**CSVPN**

# Cisco Secure Virtual Private Networks

**Version 4.7**

**Student Guide**

# Table of Contents

**1**

# Course Introduction

## Overview

This lesson includes the following topics:

- Course objectives

- Course agenda

- Participant responsibilities

- General administration

- Graphic symbols

- Participant introductions

- Cisco Security Career Certifications

- Lab topology overview

# Course Objectives

This topic introduces the course and the course objectives.

## Course Objectives

Cisco.com

**Upon completion of this course, you will be able to perform the following tasks:**

- Describe the features, functions, and benefits of Cisco VPN products.
- Explain the IPSec and IKE component technologies that are implemented in Cisco VPN products.
- Install and configure the Cisco VPN Software Client.
- Configure the Cisco VPN 3000 Series Concentrators for remote access using digital certificates.
- Configure the Cisco VPN Client for auto-initiation.
- Configure the Cisco VPN 3000 Series Concentrator firewall feature.
- Configure the Cisco VPN 3002 Hardware Client for remote access using pre-shared keys.

CSVPN 4.0—1-3

## Course Objectives (cont.)

Cisco.com

- Configure the Cisco VPN Client for software auto-update.
- Configure the Cisco VPN 3002 Hardware Client for interactive unit and individual user authentication.
- Configure the Cisco VPN Client for a backup server and load balancing.
- Configure the Cisco VPN 3000 Series Concentrator for IPSec over TCP or IPSec over UDP.
- Configure the Cisco VPN 3000 Series Concentrator for LAN-to-LAN with pre-shared keys.
- Configure the Cisco VPN 3000 Series Concentrator for LAN-to-LAN with NAT.
- Configure the Cisco VPN 3000 Series Concentrator for LAN-to-LAN with digital certificates.

CSVPN 4.0—1-4

## Course Agenda

**Day 1**
- Lesson 1—Course Introduction
- Lesson 2—Security Fundamentals
- Lesson 3—Overview of Virtual Private Networks and IPSec Technologies
- Lunch
- Lesson 4—Cisco Virtual Private Network 3000 Concentrator Series Hardware Overview
- Lesson 5—Configure the Cisco VPN 3000 Series Concentrator for Remote Access Using Pre-shared Keys

**Day 2**
- Lesson 6—Configure the Cisco VPN 3000 Series Concentrator for Remote Access Using Digital Certificates
- Lesson 7—Configure the Cisco Virtual Private Network Firewall Feature for the IPSec Software Client

CSVPN 4.0—1-5

## Course Agenda (cont.)

- Lunch
- Lesson 8—Configure the Cisco Virtual Private Network Client Auto-Initiation Feature
- Lesson 9—Monitor and Administer the Cisco VPN 3000 Series Concentrator Remote Access Networks

**Day 3**
- Lesson 10—Configure the Cisco VPN 3002 Hardware Client for Remote Access Using Pre-Shared Keys
- Lesson 11—Configure the Cisco VPN 3002 Hardware Client for Unit and User Authentication
- Lunch
- Lesson 12—Configure the Cisco Virtual Private Network 3002 Hardware Client for a Backup Server, and Load Balancing
- Lesson 13—Configure the Cisco Virtual Private Network Client for Software Auto-Update

CSVPN 4.0—1-6

## Course Agenda (cont.)

**Day 4**

- **Lesson 14—Configuring the Cisco Virtual Private Network 3000 Series Concentrator for IPSec over UDP and IPSec over TCP**
- **Lesson 15—Cisco Virtual Private Network 3000 Series Concentrator LAN-to-LAN with Pre-Shared Keys**
- **Lunch**
- **Lesson 16—Cisco Virtual Private Network 3000 Series Concentrator LAN-to-LAN with NAT**
- **Lesson 17—Configure the Cisco Virtual Private Network 3000 Series Concentrator LAN-to-LAN Using Digital Certificates**

CSVPN 4.0—1-7

---

## Participant Responsibilities

**Student responsibilities**

- **Complete prerequisites**
- **Participate in lab exercises**
- **Ask questions**
- **Provide feedback**

CSVPN 4.0—1-8

---

Copyright © 2005, Cisco Systems, Inc.

## General Administration

**Class-related**

- Sign-in sheet
- Length and times
- Break and lunch room locations
- Attire

**Facilities-related**

- Participant materials
- Site emergency procedures
- Restrooms
- Telephones/faxes

CSVPN 4.0—1-9

---

## Graphic Symbols

| | | | | | |
|---|---|---|---|---|---|
| IOS Router | PIX Firewall | VPN 3000 | IDS Sensor | Catalyst 6500 with IDS Module | IOS Firewall |
| Network Access Server | Policy Manager | CA Server | PC | Laptop | Server Web, FTP, etc. |
| Hub | Modem | Ethernet link | VPN tunnel | Network cloud | |

CSVPN 4.0—1-10

---

# Participant Introductions

- **Your name**
- **Your company**
- **Pre-requisites skills**
- **Brief history**
- **Objective**

CSVPN 4.0—1-11

---

# Cisco Security Career Certifications

**Expand Your Professional Options ——
and Advance Your Career**

**Cisco Certified Security Professional (CCSP) Certification**

**Professional-level recognition in designing
and implementing Cisco security solutions**

Expert

CCIE

Professional

CCSP

Associate

CCNA
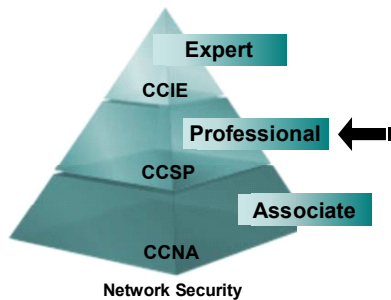
**Network Security**

| Required Exam | Recommended Training through Cisco Learning Partners |
|---|---|
| 642-501 | Securing Cisco IOS Networks |
| 642-511 | Cisco Secure Virtual Private Networks |
| 642-531 | Cisco Secure Intrusion Detection System |
| 642-521 | Cisco Secure PIX Firewall Advanced |
| 642-541 | Cisco SAFE Implementation |

**www.cisco.com/go/training**

CSVPN 4.0—1-12

# Cisco Security Career Certifications

Cisco.com

**Enhance Your Cisco Certifications ——**
**and Validate Your Areas of Expertise**
Cisco Firewall, VPN, and IDS Specialists

## Cisco Firewall Specialist

| Required Exam | Recommended Training through Cisco Learning Partners |
|---|---|
| Pre-requisite: Valid CCNA certification | |
| 642-501 | Securing Cisco IOS Networks |
| 642-521 | Cisco Secure PIX Firewall Advanced |

## Cisco VPN Specialist

| Required Exam | Recommended Training through Cisco Learning Partners |
|---|---|
| Pre-requisite: Valid CCNA certification | |
| 642-501 | Securing Cisco IOS Networks |
| 642-511 | Cisco Secure Virtual Private Networks |

## Cisco IDS Specialist

| Required Exam | Recommended Training through Cisco Learning Partners |
|---|---|
| Pre-requisite: Valid CCNA certification | |
| 642-501 | Securing Cisco IOS Networks |
| 642-531 | Cisco Secure Intrusion Detection System |

**www.cisco.com/go/training**

CSVPN 4.0—1-13

# Lab Topology Overview

This topic explains the three lab topologies that are used in this course.



**CSVPN Software Client-to-LAN Lab Visual Objective**

Cisco.com

CA server — 172.26.26.51

172.26.26.P — Student PC VPN Client

172.26.26.0 — .150

.100 — RTS

.1

192.168.P.0

.5 — Concentrator

.5

10.0.P.0

.10 — Web and FTP server

CSVPN 4.0—1-15



**CSVPN 3002 Hardware Client-to-LAN Lab Visual Objective**

Cisco.com

Hardware Client

192.168.1PP.2 — Student PC

192.168.1PP.0 — .1PP — .150

.100 — RTS

.1 — 172.26.26.0

.1

192.168.P.0

.5 — Concentrator

.5

10.0.P.0

.10 — Web and FTP server

CSVPN 4.0—1-16

CSVPN LAN-to-LAN
Lab Visual Objective

CA Server
.51
172.26.26.0
.150
Pods 1–5 .1 .1 Pods 6–10
192.168.P.0 RBB 192.168.Q.0
.5 Concentrator .5
Concentrator
.5 .5
10.0.P.0 10.0.Q.0
.10 .100 .100 .10
RTS RTS
Web and Web and
FTP server FTP server
10.0.P.15 10.0.Q.15
Student PC Student PC
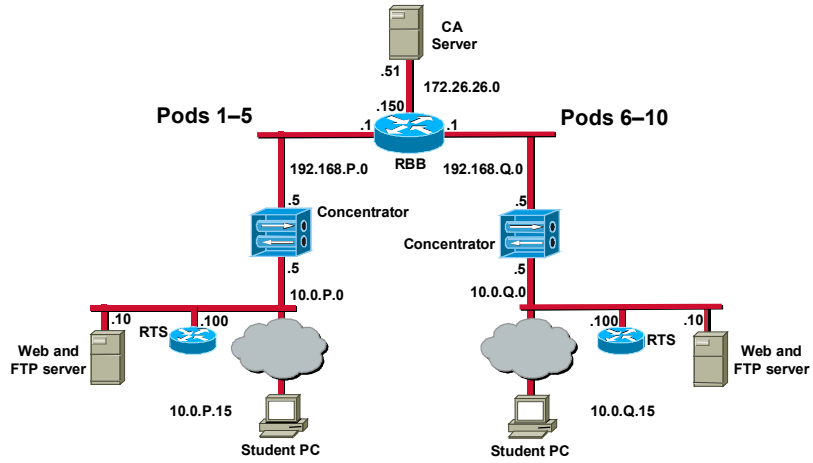
CSVPN 4.0—1-17

In this lab exercise each pair of students will be assigned a pod. In general, you will be setting up VPNs between your pod (Pod P) and your assigned peer pod (Pod Q).

| Note | The P in a command indicates your pod number. The Q in a command indicates the pod number of your peer router. |
| --- | --- |

Cisco Secure Virtual Private Networks 4.7

**2**

# Security Fundamentals

## Overview

This lesson describes security fundamentals. It includes the following topics:

- Objectives

- Need for network security

- Network security policy

- The security wheel

- Network attack taxonomy

- Management protocols and functions

- Summary

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- Describe the need for network security.
- Identify the components of a complete security policy.
- Explain how security is an ongoing process.
- Describe the four types of security threats.
- Describe common attack methods and techniques used by hackers.
- List the general recommendations for mitigating common attack methods and techniques.
- Identify the security issues implicit in common management protocols.

CSVPN 4.0—2-2

# Need for Network Security

Over the past few years, Internet-enabled business, or e-business, has drastically improved companies' efficiency and revenue growth. E-business applications such as e-commerce, supply-chain management, and remote access enable companies to streamline processes, lower operating costs, and increase customer satisfaction. Such applications require mission-critical networks that accommodate voice, video, and data traffic, and these networks must be scalable to support increasing numbers of users and the need for greater capacity and performance. However, as networks enable more and more applications and are available to more and more users, they become ever more vulnerable to a wider range of security threats. To combat those threats and ensure that e-business transactions are not compromised, security technology must play a major role in today's networks.
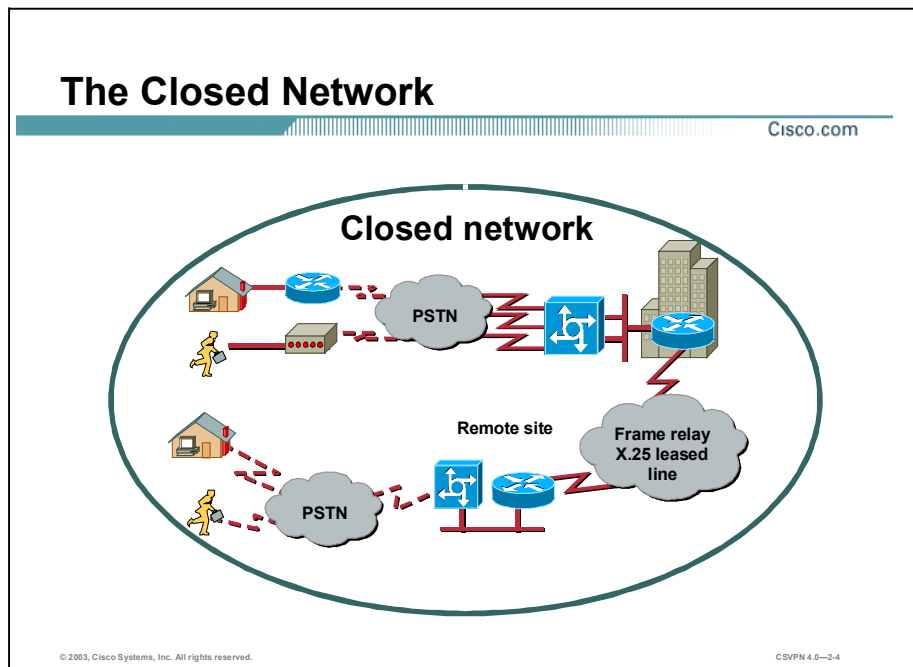


The closed network typically consists of a network designed and implemented in a corporate environment, and provides connectivity only to known parties and sites without connecting to public networks. Networks were designed this way in the past and thought to be reasonably secure because of no outside connectivity.

**The Network Today**

**Open network**

Mobile and remote users

Internet

Internet-based intranet (VPN)

Internet-based extranet (VPN)

PSTN

Remote site

Partner site
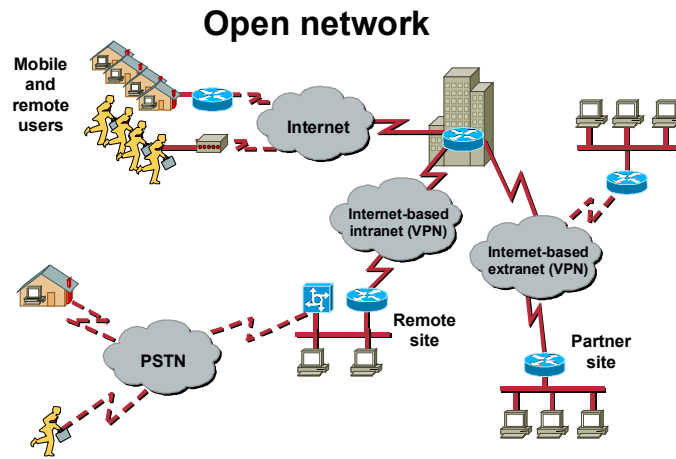
CSVPN 4.0—2-5

Networks of today are designed with availability to the Internet and public networks, which is a major requirement. Most of today's networks have several access points to other networks both public and private; therefore, securing these networks has become fundamentally important.

**Threat Capabilities—More Dangerous and Easier to Use**
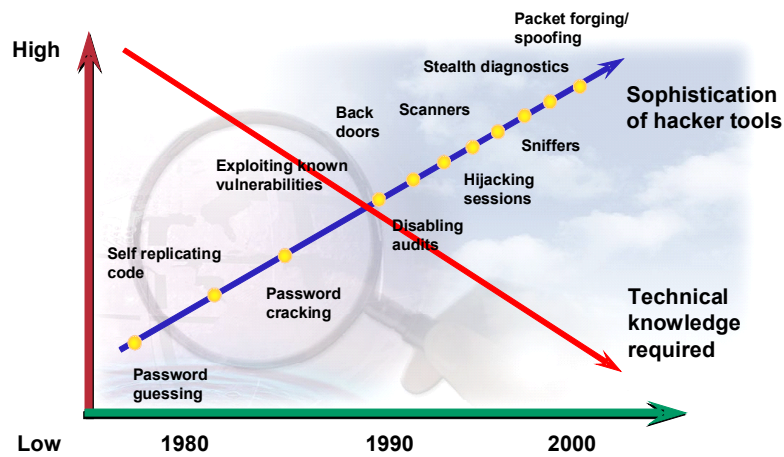
CSVPN 4.0—2-6

With the development of large open networks there has been a huge increase in security threats in the past twenty years. Not only have hackers discovered more vulnerabilities, but the tools used and technical knowledge required to hack a network have become simpler. There are downloadable applications available that require little or no hacking knowledge to implement. There are also inherent applications for troubleshooting a network that when used improperly can pose severe threats.

**The Role of Security is Changing**

Cisco.com

The need for security is becoming more important because of the following reasons:

- Required for e-business
- Required for communicating and doing business safely in potentially unsafe environments
- Result has been that networks require development and implementation of a corporate-wide security policy

CSVPN 4.0—2-7

Security has moved to the forefront of network management and implementation. It is necessary for the survival of many businesses to allow open access to network resources, and ensure that the data and resources are as secure as possible.

The need for security is becoming more important because of the following:

■ Required for e-business—The importance of e-business and the need for private data to traverse public networks has increased the need for network security.

■ Required for communicating and doing business safely in potentially unsafe environments— Today's business environment requires communication with many public networks and systems which increases the need for as much security as is possible when this type of communication is required.

■ Networks require development and implementation of a corporate-wide security policy— Establishing a security policy should be the first step in migrating a network to a secure infrastructure.

## The E-Business Challenge

Cisco.com

Internet business value

E-commerce    Supply chain    Customer care

Workforce optimization    E-learning

Business security requirements
- Defense-in-depth
- Multiple components
- Integration into e-business infrastructure
- Comprehensive blueprint

Internet presence

Corporate intranet

Internet access

**Expanded access heightened security risks**

CSVPN 4.0—2-8

Security must be a fundamental component of any e-business strategy. As enterprise network managers open their networks to more users and applications, they also expose these networks to greater risk. The result has been an increase in the business security requirements.

The Internet has radically shifted expectations of companies' abilities to build stronger relationships with customers, suppliers, partners, and employees. Driving companies to become more agile and competitive, e-business is giving birth to exciting new applications for e-commerce, supply-chain management, customer care, workforce optimization, and e-learning—applications that streamline and improve processes, speed up turnaround times, lower costs, and increase user satisfaction.

E-business requires mission-critical networks that accommodate ever-increasing constituencies and demands for greater capacity and performance. These networks also need to handle voice, video, and data traffic as networks converge into multiservice environments.

**Legal and Governmental Policy Issues**

Cisco.com

- Organizations that operate vulnerable networks will face increasing and substantial liability.
- US Federal legislation mandating security includes the following:
  - GLB financial services legislation
  - Government Information Security Reform Act
  - HIPAA

CSVPN 4.0—2-9

The legal ramifications of breaches in data confidentiality and integrity can also be extremely costly for organizations. The US Government has enacted and is currently developing regulations to control the privacy of electronic information. The existing and pending regulations generally stipulate that organizations in violation could face a range of penalties. The following are some examples:

- Gramm-Leach Bliley (GLB) Act—Includes several privacy regulations for US financial institutions. These institutions could face a range of penalties from termination of their FDIC insurance to up to US $1 million in monetary penalties.

- Government Information Security Reform Act of 2000—Agencies must undergo annual self-assessments and independent assessments of their security practices and policies, which are required for submission.

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191)—Part of a broad Congressional attempt at incremental healthcare reform. The "administrative simplification" aspect of that law requires the United States Department of Health and Human Services (DHHS) to develop standards and requirements for maintenance and transmission of health information that identifies individual patients. These standards are designed to do the following:

  — Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for specified administrative and financial transactions

  — Protect the security and confidentiality of electronic health information

Even if an external hacker is the perpetrator of an attack, the company storing that information can potentially be found negligent by the courts if the information was not adequately safeguarded. Furthermore, companies that suffer breaches in data integrity might be required to defend against lawsuits initiated by customers who are negatively affected by the incorrect or offensive data and seek monetary or punitive damages.

# Network Security Policy

A security policy can be as simple as an acceptable use policy for network resources or it can be several hundred pages in length and detail every element of connectivity and associated policies.

## What Is a Security Policy?

Cisco.com

**"A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."**

**–(RFC 2196, Site Security Handbook)**

CSVPN 4.0—2-11

According to the Site Security Handbook (RFC 2196), "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." It further states, "A security policy is essentially a document summarizing how the corporation will use and protect its computing and network resources."

**Why Create a Security Policy?**

Cisco.com

- To create a baseline of your current security posture
- To set the framework for security implementation
- To define allowed and not allowed behaviors
- To help determine necessary tools and procedures
- To communicate consensus and define roles
- To define how to handle security incidents

CSVPN 4.0—2-12

Security policies provide many benefits and are worth the time and effort needed to develop them. Developing a security policy:

■ Provides a process to audit existing network security.

■ Provides a general security framework for implementing network security.

■ Defines which behavior is and is not allowed.

■ Helps determine which tools and procedures are needed for the organization.

■ Helps communicate consensus among a group of key decision makers and define responsibilities of users and administrators.

■ Defines a process for handling network security incidents.

■ Enables global security implementation and enforcement. Computer security is now an enterprise-wide issue and computing sites are expected to conform to the network security policy.

■ Creates a basis for legal action if necessary.

- **Statement of authority and scope**
- **Acceptable use policy**
- **Identification and authentication policy**
- **Internet use policy**
- **Campus access policy**
- **Remote access policy**
- **Incident handling procedure**

The following are some of the key policy components:

- Statement of authority and scope—This topic specifies who sponsors the security policy and what areas the policy covers.

- Acceptable use policy—This topic specifies what the company will and will not allow regarding its information infrastructure.

- Identification and authentication policy—This topic specifies what technologies, equipment, or combination of the two the company will use to ensure that only authorized individuals have access to its data.

- Internet access policy—This topic specifies what the company considers ethical and proper use of its Internet access capabilities.

- Campus access policy—This topic specifies how on-campus users will use the company's data infrastructure.

- Remote access policy—This topic specifies how remote users will access the company's data infrastructure.

- Incident handling procedure—This topic specifies how the company will create an incident response team and the procedures it will use during and after and incident occurs.

# The Security Wheel

Cisco is serious about network security, and about its implications for the critical infrastructures on which this and other developed nations depend. This topic summarizes the view that network security is a continuous process.
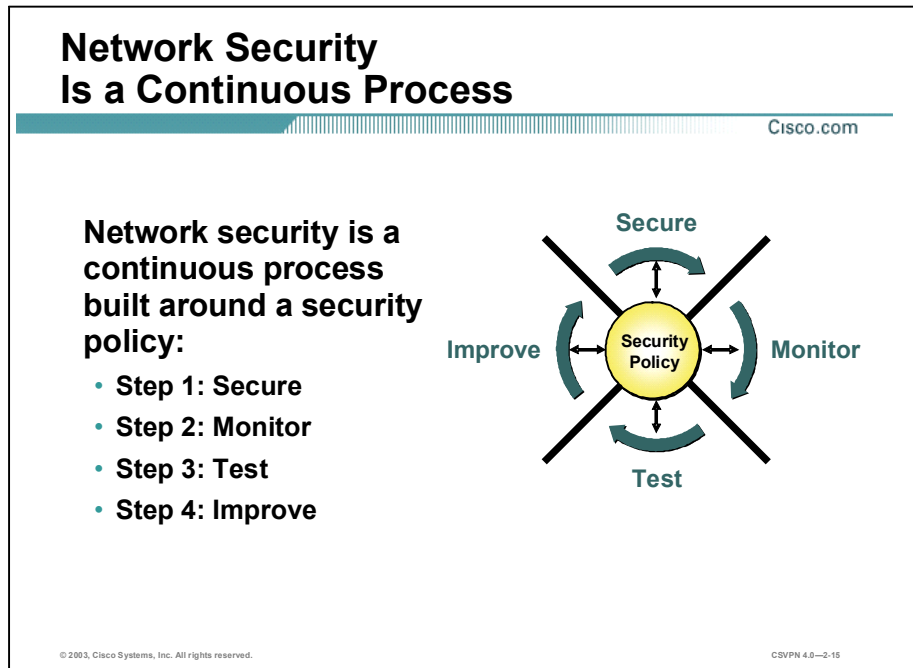


After setting appropriate policies, a company or organization must methodically consider security as part of normal network operations. This could be as simple as configuring routers to not accept unauthorized addresses or services, or as complex as installing firewalls, intrusion detection systems, centralized authentication servers, and encrypted virtual private networks.

After developing a security policy, secure your network using a variety of point products (firewalls, intrusion detection, and so on.). Before you can secure your network, however, you need to combine your understanding of your users, the assets needing protection, and the network's topology.

**Secure the Network**

Cisco.com

Implement security
solutions to stop or
prevent unauthorized
access or activities,
and to protect
information:

• Authentication

• Encryption

• Firewalls

• Vulnerability patching

Secure

Improve    Security    Monitor
           Policy

Test
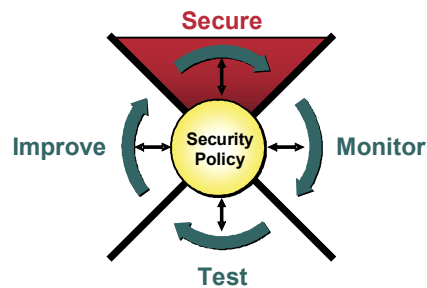
CSVPN 4.0—2-16

The following are solutions identified to secure a network:

■ Authentication—The recognition of each individual user, and the mapping of their identity,
location, and the time to policy; and the authorization of their network services and what
they can do on the network.

■ Encryption—A method for ensuring the confidentiality, integrity, and authenticity of data
communications across a network. The Cisco solution combines several standards, including
the Data Encryption Standard (DES).

■ Firewalls—A firewall is a set of related programs, located at a network gateway server, that
protects the resources of a private network from users from other networks.

■ Vulnerability patching—The identification and patching of possible security "holes" that
could compromise a network.

## Monitor Security

- **Detects violations to the security policy**
- **Involves system auditing and real-time intrusion detection**
- **Validates the security implementation in Step 1**

Secure

Improve    **Security Policy**    **Monitor**

Test
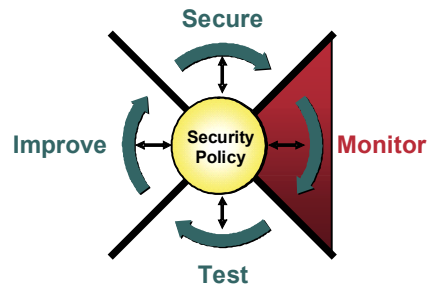
CSVPN 4.0—2-17

To ensure that a network remains secure, it is important to monitor the state of security preparation. Network vulnerability scanners can proactively identify areas of weakness, and IDSs can monitor and respond to security events as they occur. Using security monitoring solutions, organizations can obtain unprecedented visibility into both the network data stream and the security posture of the network.

**Test Security**

Cisco.com

Validates
effectiveness of
the security policy
through system
auditing and
vulnerability
scanning

Secure

Improve · Security Policy · Monitor
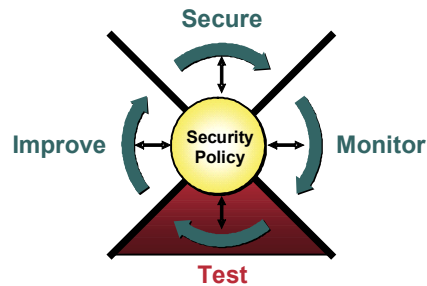
Test

CSVPN 4.0—2-18

Testing security is as important as monitoring. Without testing the security solutions in place, it is impossible to know about existing or new attacks. The hacker community is an ever-changing environment. You can perform this testing yourself or outsource it to a third party such as the Cisco Security Posture Assessment (SPA) group.

The Cisco SPA is a premium network vulnerability assessment providing comprehensive insight into the security posture of a customer's network. Delivered by highly expert Cisco Network Security Engineers (NSEs), the Cisco SPA includes an operational, granular analysis of large-scale, distributed service provider networks from the perspective of an outside "hacker."

**Improve Security**

- **Use information from the monitor and test phases to make improvements to the security implementation.**
- **Adjust the security policy as security vulnerabilities and risks are identified.**

Secure

Improve — Security Policy — Monitor
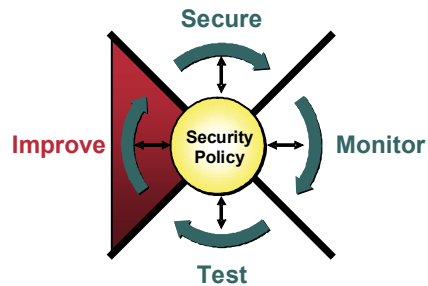
Test

CSVPN 4.0—2-19

Monitoring and testing provides the data necessary to improve network security. Administrators and engineers should use the information from the monitor and test phases to make improvements to the security implementation as well as adjust the security policy as vulnerabilities and risks are identified.

# Network Attack Taxonomy

This topic provides an overview of various network attacks and affects.
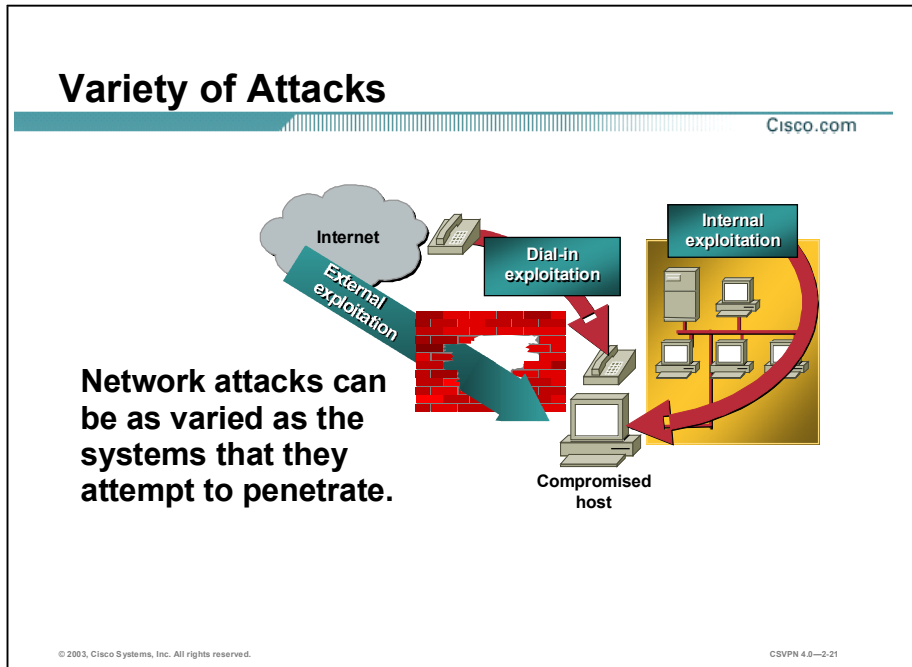


Without proper protection, any part of any network can be susceptible to attacks or unauthorized activity. Routers, switches, and hosts can all be violated by professional hackers, company competitors, or even internal employees. In fact, according to several studies, more than half of all network attacks are waged internally. The Computer Security Institute (CSI) in San Francisco estimates that between 60 and 80 percent of network misuse comes from inside the enterprises where the misuse has taken place. To determine the best ways to protect against attacks, IT managers should understand the many types of attacks that can be instigated and the damage that these attacks can cause to e-business infrastructures.

## Network Security Threats

**There are four general categories of security threats to the network:**

- **Unstructured threats**
- **Structured threats**
- **External threats**
- **Internal threats**

There are four general threats to network security:

- Unstructured threats—These threats primarily consist of random hackers using various common tools, such as malicious shell scripts, password crackers, credit card number generators, and dialer daemons. Although hackers in this category may have malicious intent, many are more interested in the intellectual challenge of cracking safeguards than creating havoc.

- Structured threats—These threats are created by hackers who are more highly motivated and technically competent. Typically, such hackers act alone or in small groups to understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies. Occasionally, such hackers are hired by organized crime, industry competitors, or state-sponsored intelligence collection organizations.

- External threats—These threats consist of structured and unstructured threats originating from an external source. These threats can have malicious and destructive intent, or simply be errors that generate a threat.

- Internal threats—These threats are typically from disgruntled former or current employees. Although internal threats may seem more ominous than threats from external sources, security measures are available for reducing vulnerabilities to internal threats and responding when attacks occur.

## Specific Attack Types

**All of the following can be used
to compromise your system:**

- Packet sniffers
- IP weaknesses
- Password attacks
- DoS or DDoS
- Man-in-the-middle attacks
- Application layer attacks
- Trust exploitation
- Port redirection
- Virus
- Trojan horse
- Operator error

CSVPN 4.0—2-23

There are many common attacks that can occur against a network. Any of the following can be used to compromise your system:

■ Packet sniffers

■ IP weaknesses

■ Password attacks

■ Denial of service (DoS) or distributed denial of service (DDoS)

■ Man-in-the-middle attacks

■ Application layer attacks

■ Trust exploitation

■ Port redirection

■ Virus

■ Trojan horse

■ Operator error

## Packet Sniffers
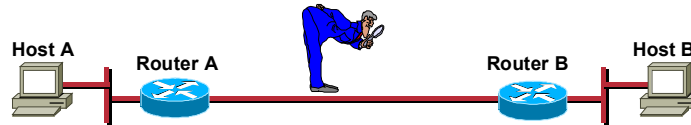
**Host A**    **Router A**    **Router B**    **Host B**

**A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets. The following are the packet sniffer features:**

- **Packet sniffers exploit information passed in clear text. Protocols that pass information in the clear include the following:**
  - **Telnet**
  - **FTP**
  - **SNMP**
  - **POP**
  - **HTTP**
- **Packet sniffers must be on the same collision domain.**

CSVPN 4.0—2-24

A packet sniffer is a software application that uses a network adapter card in promiscuous mode (a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing) to capture all network packets that are sent across a LAN.

Several network applications distribute network packets in clear text; that is, the information sent across the network is not encrypted. Because the network packets are not encrypted, they can be processed and understood by any application that can pick them up off the network and process them.

A network protocol specifies how packets are identified and labeled, which enables a computer to determine whether a packet is intended for it. Because the specifications for network protocols, such as TCP/IP, are widely published, a third party can easily interpret the network packets and develop a packet sniffer. (The real threat today results from the numerous freeware and shareware packet sniffers that are available, which do not require the user to understand anything about the underlying protocols.)

## Packet Sniffer Example

**There are two primary types of packet sniffers:**

- **General purpose sniffers**
- **Sniffers designed for attack purpose**

CSVPN 4.0—2-25

A packet sniffer can provide its user with meaningful and often sensitive information, such as user account names and passwords. If you use networked databases, a packet sniffer can provide an attacker with information that is queried from the database, as well as the user account names and passwords used to access the database. One serious problem with acquiring user account names and passwords is that users often reuse their login names and passwords across multiple applications.

In addition, many network administrators use packet sniffers to diagnose and fix network-related problems. Because in the course of their usual and necessary duties these network administrators (such as those in a payroll department) work during regular employee hours, they can potentially examine sensitive information distributed across the network.

Many users employ a single password for access to all accounts and applications. Because attackers know and use human characteristics (attack methods known collectively as social engineering attacks), such as using a single password for multiple accounts, they are often successful in gaining access to sensitive information.

There are two primary types of packet sniffers:

■ General purpose

— Captures all packets

— Included with some operating systems

— Freeware and shareware versions available

- Designed for attack purpose

  — Captures first 300 to 400 bytes

  — Typically captures login sessions (File Transfer Protocol [FTP], rlogin, and Telnet)

**Packet Sniffer Mitigation**

Cisco.com

Host A    Router A                              Router B    Host B

**The following techniques and tools can be used to mitigate sniffers:**

• **Authentication—A first option for defense against packet sniffers is to use strong authentication, such as one-time passwords.**
• **Switched infrastructure—Deploy a switched infrastructure to counter the use of packet sniffers in your environment.**
• **Antisniffer tools—Use these tools to employ software and hardware designed to detect the use of sniffers on a network.**
• **Cryptography—The most effective method for countering packet sniffers does not prevent or detect packet sniffers, but rather renders them irrelevant.**

CSVPN 4.0—2-26

The following techniques and tools can be used to mitigate packet sniffers:

■ Authentication—Using strong authentication is a first-option for defense against packet sniffers. Strong authentication can be broadly defined as a method of authenticating users that cannot easily be circumvented. A common example of strong authentication is one-time passwords (OTPs).

An OTP is a type of two-factor authentication. Two-factor authentication involves using something you have combined with something you know. Automated teller machines (ATMs) use two-factor authentication. A customer needs both an ATM card and a personal identification number (PIN) to make transactions. With OTPs you need a PIN and your token card to authenticate to a device or software application. A token card is a hardware or software device that generates new, seemingly random, passwords at specified intervals (usually 60 seconds). A user combines that random password with a PIN to create a unique password that works only for one instance of authentication. If a hacker learns that password by using a packet sniffer, the information is useless because the password has already expired. Note that this mitigation technique is effective only against a sniffer implementation that is designed to grab passwords. Sniffers deployed to learn sensitive information (such as mail messages) will still be effective.

■ Switched infrastructure—This can be used to counter the use of packet sniffers in your network environment. For example, if an entire organization deploys switched Ethernet, hackers can gain access only to the traffic that flows on the specific port to which they connect. A switched infrastructure obviously does not eliminate the threat of packet sniffers, but it can greatly reduce their effectiveness.

- Antisniffer tools—Employing software and hardware designed to detect the use of sniffers on a network. Such software and hardware does not completely eliminate the threat, but like many network security tools, they are part of the overall system. These so-called "antisniffers" detect changes in the response time of hosts to determine if the hosts are processing more traffic than their own. One such network security software tool, which is available from Security Software Technologies, is called AntiSniff.

- Cryptography—Rendering packet sniffers irrelevant, which is the most effective method for countering packet sniffers—even more effective than preventing or detecting packet sniffers. If a communication channel is cryptographically secure, the only data a packet sniffer will detect is cipher text (a seemingly random string of bits) and not the original message. The Cisco deployment of network-level cryptography is based on IPSec, which is a standard method for networking devices to communicate privately using IP. Other cryptographic protocols for network management include Secure Shell Protocol (SSH) and Secure Sockets Layer (SSL).

## IP Spoofing

- **IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.**
- **Two general techniques are used during IP spoofing:**
  - **A hacker uses an IP address that is within the range of trusted IP addresses.**
  - **A hacker uses an authorized external IP address that is trusted.**
- **Uses for IP spoofing include the following:**
  - **IP spoofing is usually limited to the injection of malicious data or commands into an existing stream of data.**
  - **If a hacker changes the routing tables to point to the spoofed IP address, then the hacker can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can.**

CSVPN 4.0—2-27

An IP spoofing attack occurs when an attacker outside your network pretends to be a trusted computer, either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you wish to provide access to specified resources on your network.

Normally, an IP spoofing attack is limited to the injection of data or commands into an existing stream of data passed between a client and server application or a peer-to-peer network connection. To enable bi-directional communication, the attacker must change all routing tables to point to the spoofed IP address. Another approach the attacker could take is to simply not worry about receiving any response from the applications. For example, if an attacker is attempting to get a system to mail him or her a sensitive file, application responses are unimportant.

However, if an attacker manages to change the routing tables to point to the spoofed IP address, he can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can. Like packet sniffers, IP spoofing is not restricted to people who are external to the network.

Although not as common, IP spoofing can also gain access to user accounts and passwords, and it can also be used in other ways. For example, an attacker can emulate one of your internal users in ways that prove embarrassing for your organization; the attacker could send e-mail messages to business partners that appear to have originated from someone within your organization. Such attacks are easier when an attacker has a user account and password, but they are possible by combining simple spoofing attacks with knowledge of messaging protocols.

The threat of IP spoofing can be reduced, but not eliminated, through the following measures:

■ Access control—The most common method for preventing IP spoofing is to properly configure access control. To reduce the effectiveness of IP spoofing, configure access control to deny any traffic from the external network that has a source address that should reside on the internal network. Note that this helps prevent spoofing attacks only if the internal addresses are the only trusted addresses. If some external addresses are trusted, this method is not effective.

■ RFC 2827 filtering—You can prevent users of your network from spoofing other networks (and be a good Internet citizen at the same time) by preventing any outbound traffic on your network that does not have a source address in your organization's own IP range.

This filtering denies any traffic that does not have the source address that was expected on a particular interface. For example, if an ISP is providing a connection to the IP address 15.1.1.0/24, the ISP could filter traffic so that only traffic sourced from address 15.1.1.0/24 can enter the ISP router from that interface. Note that unless all ISPs implement this type of filtering, its effectiveness is significantly reduced.

■ Additional Authentication—The most effective method for mitigating the threat of IP spoofing is the same as the most effective method for mitigating the threat of packet sniffers: namely, eliminating its effectiveness. IP spoofing can function correctly only when devices use IP address-based authentication; therefore, if you use additional authentication methods, IP spoofing attacks are irrelevant. Cryptographic authentication is the best form of additional authentication, but when that is not possible, strong two-factor authentication using OTP can also be effective.

**DoS**

**DoS attacks focus on making a service unavailable for normal use. They have the following characteristics:**

- **Different from most other attacks because they are generally not targeted at gaining access to your network or the information on your network**
- **Require very little effort to execute**
- **Among the most difficult to completely eliminate**

CSVPN 4.0—2-29

DoS attacks are different from most other attacks because they are not targeted at gaining access to your network or the information on your network. These attacks focus on making a service unavailable for normal use, which is typically accomplished by exhausting some resource limitation on the network or within an operating system or application. These attacks require little effort to execute because they typically take advantage of protocol weaknesses or the attacks are carried out using traffic that would normally be allowed into a network. DoS attacks are among the most difficult to completely eliminate because of the way they use protocol weaknesses and "native" traffic to attack a network.

## DDoS Example

1. Scan for systems to hack.

Client system

2. Install software to scan, compromise, and infect agents.

4. The client issues commands to handlers that control agents in a mass attack.

Handler systems

3. Agents are loaded with remote control attack software.

Agent systems

CSVPN 4.0—2-30
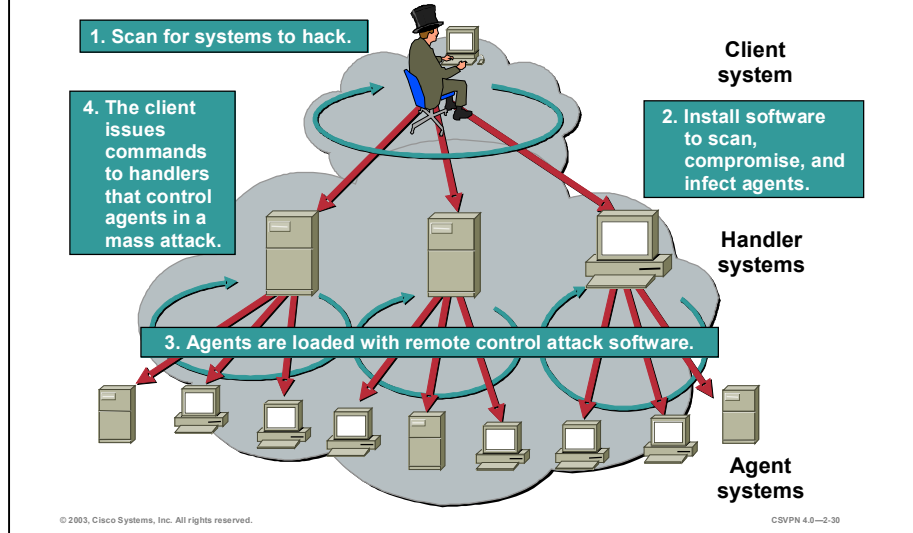
DDoS attacks are the "next generation" of DoS attacks on the Internet. This type of attack is not new—UDP and TCP SYN flooding, Internet Control Message Protocol (ICMP) echo request floods, and ICMP directed broadcasts (also known as smurf attacks) are similar—but the scope certainly is new. Victims of DDoS attacks experience packet flooding from many different sources, possibly spoofed IP source addresses, that bring their network connectivity to a grinding halt. In the past, the typical DoS attack involved a single attacker's attempt to flood a target host with packets. With DDoS tools, an attacker can conduct the same attack using thousands of systems.

In the figure the hacker uses their terminal to scan for systems to hack. When the handler systems are accessed, the hacker then installs software on them to scan for, compromise, and infect Agent systems. When the Agent systems are accessed the hacker then loads remote control attack software to carry out the DoS attack.

When involving specific network server applications, such as a HTTP server or a File Transfer Protocol (FTP) server, these attacks can focus on acquiring and keeping open all the available connections supported by that server, effectively locking out valid users of the server or service. DoS attacks can also be implemented using common Internet protocols, such as TCP and ICMP. While most DoS attacks exploit a weakness in the overall architecture of the system being attacked rather than a software bug or security hole, some attacks compromise the performance of your network by flooding the network with undesired, and often useless, network packets and by providing false information about the status of network resources.

The threat of DoS attacks can be reduced through the following three methods:

- Antispoof features—Proper configuration of antispoof features on your routers and firewalls can reduce your risk. This configuration includes RFC 2827 filtering at a minimum. If hackers cannot mask their identities, they might not attack.

- Anti-DoS features—Proper configuration of anti-DoS features on routers and firewalls can help limit the effectiveness of an attack. These features often involve limits on the amount of half-open connections that a system allows open at any given time.

- Traffic rate limiting—An organization can implement traffic rate limiting with its ISP. This type of filtering limits the amount of nonessential traffic that crosses network segments at a certain rate. A common example is to limit the amount of ICMP traffic allowed into a network because it is used only for diagnostic purposes. ICMP-based DDoS attacks are common.

**Password Attacks**

Cisco.com

**Hackers can implement password attacks using several different methods:**

- **Brute-force attacks**
- **Trojan horse programs**
- **IP spoofing**
- **Packet sniffers**

Authorization

Username  administrator

Password  ****

Connect
Options
Cancel
Help
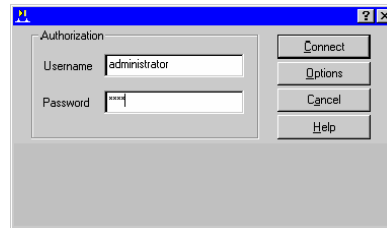
CSVPN 4.0—2-32

Password attacks can be implemented using several different methods, including brute-force attacks, Trojan horse programs (discussed later in the lesson), IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are called brute-force attacks.

Often a brute-force attack is performed using a program that runs across the network and attempts to log in to a shared resource, such as a server. When an attacker successfully gains access to a resource, he or she has the same rights as the user whose account has been compromised to gain access to that resource. If this account has sufficient privileges, the attacker can create a back door for future access, without concern for any status and password changes to the compromised user account.

## Password Attack Example

- **L0phtCrack can take the hashes of passwords and generate the clear text passwords from them.**
- **Passwords are computed using two different methods:**
  - **Dictionary cracking**
  - **Brute force computation**
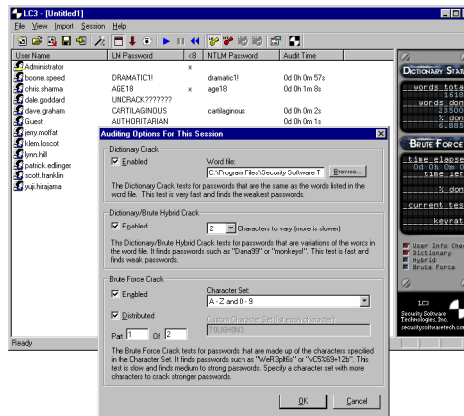
CSVPN 4.0—2-33

Just as with packet sniffers and IP spoofing attacks, a brute-force password attack can provide access to accounts that can be used to modify critical network files and services. An example that compromises your network's integrity is an attacker modifying the routing tables for your network. By doing so, the attacker ensures that all network packets are routed to him or her before they are transmitted to their final destination. In such a case, an attacker can monitor all network traffic, effectively becoming a man in the middle.

The following are the two different methods for computing passwords with L0phtCrack:

■ Dictionary cracking—The password hashes for all of the words in a dictionary file are computed and compared against all of the password hashes for the users. This method is extremely fast and finds very simple passwords.

■ Brute force computation—This method uses a particular character set such as A−Z, or A−Z plus 0−9 and computes the hash for every possible password made up of those characters. It will always compute the password if it is made up of the character set you have selected to test. The downside is that time is required for completion of this type of attack.

## Password Attacks Mitigation

**The following are mitigation techniques:**

- **Do not allow users to use the same password on multiple systems.**
- **Disable accounts after a certain number of unsuccessful login attempts.**
- **Do not use plain text passwords. An OTP or a cryptographic password is recommended.**
- **Use "strong" passwords. Strong passwords are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters.**

CSVPN 4.0—2-34

The following are password attack mitigation techniques:

- Do not allow users to have the same password on multiple systems—Most users will use the same password for each system they access, and often personal system passwords will be the same as well.

- Disable accounts after unsuccessful logins—This helps to prevent continuous password attempts.

- Do not use plain text passwords—Use of either an OTP or encrypted password is recommended.

- Use "strong" passwords—Many systems now provide strong password support and can restrict a user to only the use of strong passwords. Strong passwords are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters.

**Man-in-the-Middle Attacks**

CISCO.COM

Host A

Data in clear text

Host B

Router A

Router B

- A man-in-the-middle attack requires that the hacker have access to network packets that come across a network.
- A man-in-the-middle attack is implemented using the following:
  - Network packet sniffers
  - Routing and transport protocols
- Possible man-in-the-middle attack uses include the following:
  - Theft of information
  - Hijacking of an ongoing session
  - Traffic analysis
  - DoS
  - Corruption of transmitted data
  - Introduction of new information into network sessions

CSVPN 4.0—2-35

A man-in-the-middle attack requires that the attacker have access to network packets that come across the networks. Such attacks are often implemented using network packet sniffers and routing and transport protocols. The possible uses of such attacks are theft of information, hijacking of an ongoing session to gain access to your internal network resources, traffic analysis to derive information about your network and its users, denial of service, corruption of transmitted data, and introduction of new information into network sessions.

An example of a man-in-the-middle attack could be someone who is working for your ISP, who can gain access to all network packets transferred between your network and any other network.

**Man-in-the-Middle Mitigation**

Cisco.com

A man-in-the-middle attack
can only see cipher text

**IPSec tunnel**

Host A

Router A          ISP          Router B

Host B
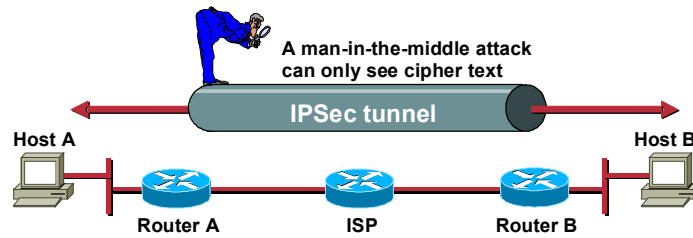
**Man-in-the-middle attacks can be effectively mitigated
only through the use of cryptography (encryption).**

CSVPN 4.0—2-36

Man-in-the-Middle attack mitigation is achieved, as shown in the figure, by encrypting traffic in an IPSec tunnel, which would only allow the hacker to see cipher text.

## Application Layer Attacks

**Application layer attacks have the following characteristics:**

- **Exploit well known weaknesses, such as protocols, that are intrinsic to an application or system (for example, sendmail, HTTP, and FTP)**
- **Often use ports that are allowed through a firewall (for example, TCP port 80 used in an attack against a web server behind a firewall)**
- **Can never be completely eliminated, because new vulnerabilities are always being discovered**

| 7 | **Application** |
| 6 | **Presentation** |
| 5 | **Session** |
| 4 | **Transport** |
| 3 | **Network** |
| 2 | **Data Link** |
| 1 | **Physical** |
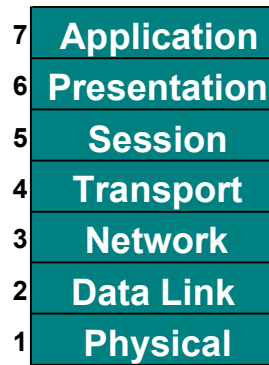
CSVPN 4.0—2-37

Application-layer attacks can be implemented using several different methods:

- One of the most common methods is exploiting well known weaknesses in software commonly found on servers, such as sendmail, PostScript, and FTP. By exploiting these weaknesses, attackers can gain access to a computer with the permissions of the account running the application, which is usually a privileged, system-level account.

- Trojan horse program attacks are implemented using programs that an attacker substitutes for common programs. These programs may provide all the functionality that the normal program provides, but also include other features that are known to the attacker, such as monitoring login attempts to capture user account and password information. These programs can capture sensitive information and distribute it back to the attacker. They can also modify application functionality, such as applying a blind carbon copy to all e-mail messages so that the attacker can read all of your organization's e-mail.

  One of the oldest forms of application-layer attacks is a Trojan horse program that displays a screen, banner, or prompt that the user believes is the valid login sequence. The program then captures the information that the user enters and stores or e-mails it to the attacker. Next, the program either forwards the information to the normal login process (normally impossible on modern systems), or simply sends an expected error to the user (for example, Bad Username/Password Combination), exits, and starts the normal login sequence. The user, believing that they have incorrectly entered the password (a common mistake experienced by everyone), re-enters the information and is allowed access.

- One of the newest forms of application-layer attacks exploits the openness of several new technologies: the HTML specification, web browser functionality, and HTTP. These attacks,

which include Java applets and ActiveX controls, involve passing harmful programs across the network and loading them through a user's browser.

## Application Layer Attacks Mitigation

Cisco.com

**Some measures you can take to reduce your risks are as follows:**

- **Read operating system and network log files, or have them analyzed by log analysis applications.**
- **Subscribe to mailing lists that publicize vulnerabilities.**
- **Keep your operating system and applications current with the latest patches.**
- **IDSs can scan for known attacks, monitor and log attacks, and in some cases, prevent attacks.**

CSVPN 4.0—2-38

The following are some measures you can take to reduce your risks for application layer attacks:

■ Read operating system and network log files or have them analyzed—It is important to review all logs and take action accordingly.

■ Subscribe to mailing lists that publicize vulnerabilities—Most application and operating system vulnerabilities are published on the Web at various sources.

■ Keep your operating system and applications current with the latest patches—Always test patches and fixes in a non-production environment. This prevents downtime and errors from being generated unnecessarily.

■ Intrusion detection systems (IDSs) can scan for known attacks, monitor and log attacks, and in some cases, prevent attacks—The use of IDSs can be essential to identifying security threats and mitigating some of those threats, and, in most cases, it can be done automatically.

# Network Reconnaissance

**Network reconnaissance refers to the overall act of learning information about a target network by using publicly available information and applications.**

Network Reconnaissance refers to the overall act of learning information about a target network by using publicly available information and applications. When hackers attempt to penetrate a particular network, they often need to learn as much information as possible about the network before launching attacks. Examples include DNS queries, ping sweeps, and port scans:

- Domain Name System (DNS) queries—Reveals such information as who owns a particular domain and what addresses have been assigned to that domain.

- Ping sweeps—Presents a picture of the live hosts in a particular environment.

- Port scans—Cycles through all well known ports to provide a complete list of all services running on the hosts.

## Network Reconnaissance Example

Cisco.com
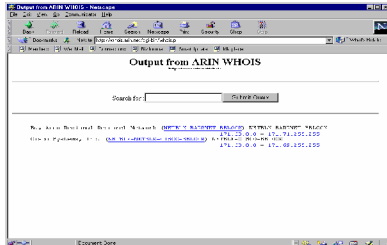
**Sample IP address query**
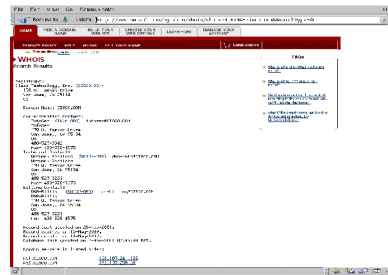
**Sample domain name query**

CSVPN 4.0—2-40

The figure demonstrates how existing Internet tools can be used for network reconnaissance (for example, an IP address query or a Domain Name query).

DNS queries can reveal such information as who owns a particular domain and what addresses have been assigned to that domain. Ping sweeps of the addresses revealed by the DNS queries can present a picture of the live hosts in a particular environment. After such a list is generated, port scanning tools can cycle through all well known ports to provide a complete list of all services running on the hosts discovered by the ping sweep. Finally, the hackers can examine the characteristics of the applications that are running on the hosts. This can lead to specific information that is useful when the hacker attempts to compromise that service.

IP address queries can reveal information such as who owns a particular IP address or range of addresses and what domain is associated to them.

## Network Reconnaissance Mitigation

- **Network reconnaissance cannot be prevented entirely.**
- **IDSs at the network and host levels can usually notify an administrator when a reconnaissance gathering attack (for example, ping sweeps and port scans) is under way.**

If ICMP echo and echo-reply is turned off on edge routers (for example, ping sweeps can be stopped, but at the expense of network diagnostic data), port scans can still be run without full ping sweeps They simply take longer because they need to scan IP addresses that might not be live.

IDSs at the network and host levels can usually notify an administrator when a reconnaissance gathering attack is underway. This allows the administrator to better prepare for the coming attack or to notify the ISP who is hosting the system that it is launching the reconnaissance probe.

**Trust Exploitation**

Cisco.com

- A hacker leverages existing trust relationships
- Several trust models exist
  - Windows
    - Domains
    - Active directory
  - Linux and UNIX
    - NFS
    - NIS+

SystemA Trusts SystemB

SystemB Trusts Everyone

SystemA Trusts Everyone

SystemA
User = psmith; Pat Smith

Hacker gains access to SystemA

SystemB – Compromised by hacker
User = psmith; Pat Smith

Hacker
User = psmith; Pat Smithson
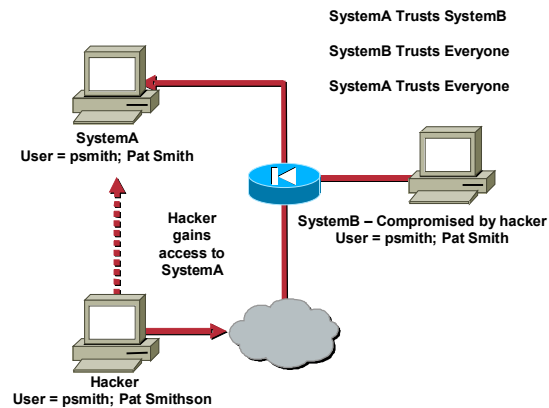
CSVPN 4.0—2-42

While not an attack in and of itself, trust exploitation refers to an attack where an individual takes advantage of a trust relationship within a network. The classic example is a perimeter network connection from a corporation. These network segments often house DNS, SMTP, and HTTP servers. Because they all reside on the same segment, a compromise of one system can lead to the compromise of other systems because they might trust other systems attached to their same network. Another example is a system on the outside of a firewall that has a trust relationship with a system on the inside of a firewall. When the outside system is compromised, it can leverage that trust relationship to attack the inside network.

**Trust Exploitation Mitigation**
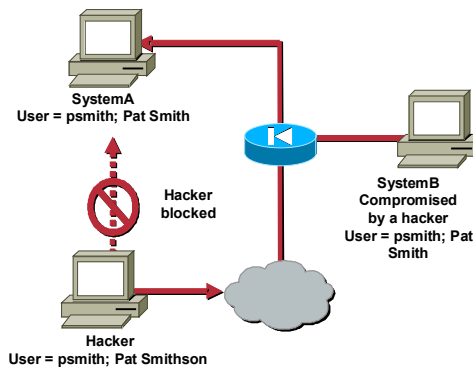
SystemA
User = psmith; Pat Smith

Hacker blocked

Hacker
User = psmith; Pat Smithson

SystemB
Compromised
by a hacker
User = psmith; Pat
Smith

- **Systems on the outside of a firewall should never be absolutely trusted by systems on the inside of a firewall.**
- **Such trust should be limited to specific protocols and should be validated by something other than an IP address where possible.**

CSVPN 4.0—2-43

You can mitigate trust and exploitation-based attacks through tight constraints on trust levels within a network. Systems on the outside of a firewall should never be absolutely trusted by systems on the inside of a firewall. Such trust should be limited to specific protocols and should be authenticated by something other than an IP address where possible.

## Port Redirection

- **Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped.**
- **It is mitigated primarily through the use of proper trust models.**
- **Antivirus software and host-based IDS can help detect and prevent a hacker installing port redirection utilities on the host.**

Attacker

Source: Attacker
Destination: A
Port: 22

Source: Attacker
Destination: B
Port: 23

Compromised
Host A

Source: A
Destination: B
Port: 23

Host B
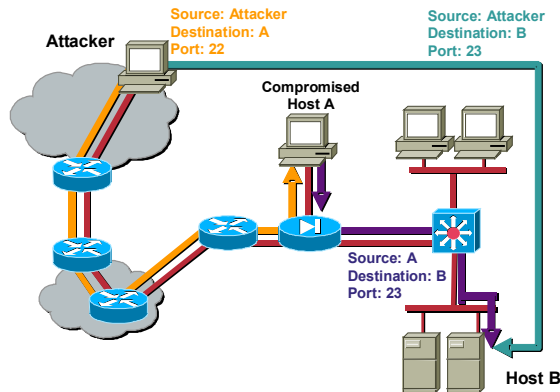
CSVPN 4.0—2-44

Port redirection attacks are a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. Consider a firewall with three interfaces and a host on each interface. The host on the outside can reach the host on the public services segment (commonly referred to as a Demilitarized Zone [DMZ]), but not the host on the inside. The host on the public services segment can reach the host on both the outside and the inside. If hackers were able to compromise the public services segment host, they could install software to redirect traffic from the outside host directly to the inside host. Though neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host. An example of an application that can provide this type of access is netcat.

Port redirection can primarily be mitigated through the use of proper trust models, which are network specific (as mentioned earlier). Assuming a system under attack, a host-based IDS can help detect and prevent a hacker installing such utilities on a host.

## Unauthorized Access

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS
PROHIBITED.

[ Disconnect ]    [ Continue ]
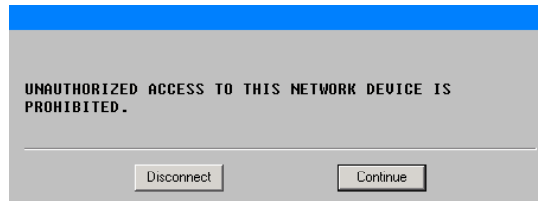
- **Unauthorized access includes any unauthorized attempt to access a private resource:**
    - **Not a specific type of attack**
    - **Refers to most attacks executed in networks today**
    - **Initiated on both the outside and inside of a network**
- **The following are mitigation techniques for unauthorized access attacks:**
    - **Eliminate the ability of a hacker to gain access to a system**
    - **Prevent simple unauthorized access attacks, which is the primary function of a firewall**

CSVPN 4.0—2-45

While not a specific type of attack, unauthorized access attacks refer to the majority of attacks executed in networks today. In order for someone to brute-force a Telnet login, they must first get the Telnet prompt on a system. Upon connection to the Telnet port, the hacker might see the message "authorization required to use this resource." If the hacker continues to attempt access, the hacker's actions become "unauthorized." These kinds of attacks can be initiated both on the outside and inside of a network.

Mitigation techniques for unauthorized access attacks are very simple. They involve reducing or eliminating the ability of a hacker to gain access to a system using an unauthorized protocol. An example would be preventing hackers from having access to the Telnet port on a server that needs to provide web services to the outside. If a hacker cannot reach that port, it is very difficult to attack it. The primary function of a firewall in a network is to prevent simple unauthorized access attacks.

## Virus and Trojan Horses

Cisco.com

- **Viruses refer to malicious software that are attached to another program to execute a particular unwanted function on a user's workstation. End-user workstations are the primary targets.**
- **A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. A Trojan horse is mitigated by antivirus software at the user level and possibly the network level.**

CSVPN 4.0—2-46

The primary vulnerabilities for end-user workstations are viruses and Trojan horse attacks. Viruses refer to malicious software that is attached to another program to execute a particular unwanted function on a user's workstation. An example of a virus is a program that is attached to command.com (the primary interpreter for windows systems), which deletes certain files and infects any other versions of command.com that it can find.

A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. Then other users receive the game and play it, thus spreading the Trojan horse.

These kinds of applications can be contained through the effective use of antivirus software at the user level and potentially at the network level. Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. Keeping up-to-date with the latest developments in these sorts of attacks can also lead to a more effective posture against these attacks. As new virus or Trojan applications are released, enterprises need to keep up-to-date with the latest antivirus software, and application versions.

# Management Protocols and Functions

The protocols used to manage your network can in themselves be a source of vulnerability. This topic examines common management protocols and how they can be exploited.

## Configuration Management

- **Configuration management protocols include SSH, SSL, and Telnet.**
- **Telnet issues include the following:**
  - **The data within a Telnet session is sent as clear text, and may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server.**
  - **The data may include sensitive information, such as the configuration of the device itself, passwords, and so on.**

CSVPN 4.0—2-48

If the managed device does not support any of the recommended protocols, such as SSH and SSL, Telnet may have to be used (although this protocol is not highly recommended). The network administrator should recognize that the data within a Telnet session is sent as clear text, and may be intercepted by anyone with a packet sniffer located along the data path between the managed device and the management server. The clear text may include important information, such as the configuration of the device itself, passwords, and other sensitive data.

## Configuration Management Recommendations

**When possible, the following practices are advised:**

- **Use IPSec, SSH, SSL, or any other encrypted and authenticated transport.**
- **ACLs should be configured to allow only management servers to connect to the device. All attempts from other IP addresses should be denied and logged.**
- **RFC 2827 filtering at the perimeter router should be used to mitigate the chance of an outside attacker spoofing the addresses of the management hosts.**

CSVPN 4.0—2-49

Regardless of whether SSH, SSL, or Telnet is used for remote access to the managed device, access control lists (ACLs) should be configured to allow only management servers to connect to the device. All attempts from other IP addresses should be denied and logged. RFC 2827 filtering at the ingress router should also be implemented to mitigate the chance of an attacker from outside the network spoofing the addresses of the management hosts.

## SNMP

- **SNMP is a network management protocol that can be used to retrieve information from a network device. The TCP and UDP ports SNMP uses are 161 and 162.**
- **The following are SNMP issues:**
  - **SNMP uses passwords, called community strings, within each message as a very simple form of security. Most implementations of SNMP on networking devices today send the community string in clear text.**
  - **SNMP messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server, and the community string may be compromised.**
  - **An attacker could reconfigure the device if read-write access via SNMP is allowed.**
- **The following are SNMP recommendations:**
  - **Configure SNMP with only read-only community strings.**
  - **Set up access control on the device you wish to manage via SNMP to allow only the appropriate management hosts access.**

CSVPN 4.0—2-50

SNMP is a network management protocol that can be used to retrieve information from a network device (commonly referred to as read-only access) or to remotely configure parameters on the device (commonly referred to as read-write access). SNMP uses passwords, called community strings, within each message as a very simple form of security. Unfortunately, most implementations of SNMP on networking devices today send the community string in clear text along with the message. Therefore, SNMP messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server, and the community string may be compromised.

When the community string is compromised, an attacker could reconfigure the device if read-write access via SNMP is allowed. Therefore, it is recommended that you configure SNMP with only read-only community strings. You can further protect yourself by setting up access control on the device you wish to manage via SNMP to allow only the appropriate management hosts access.

## Logging

**Logging issues include the following:**

- **Syslog is sent as clear text between the managed device and the management host on UDP port 514.**
- **Syslog has no packet-level integrity checking to ensure that the packet contents have not been altered in transit.**
- **There is a potential for the Syslog data to be falsified by an attacker.**
- **An attacker can send large amounts of false Syslog data to a management server in order to confuse the network administrator during an attack.**

CSVPN 4.0—2-51

Syslog, which is information generated by a device that has been configured for logging, is sent as clear text between the managed device and the management host. Syslog has no packet-level integrity checking to ensure that the packet contents have not been altered in transit. An attacker may alter Syslog data in order to confuse a network administrator during an attack.

## Logging Recommendations

**When possible, the following practices are advised:**

- **Encrypt Syslog traffic within an IPSec tunnel.**
- **When allowing Syslog access from devices on the outside of a firewall, you should implement RFC 2827 filtering at the perimeter router.**
- **ACLs should also be implemented on the firewall in order to allow Syslog data from only the managed devices themselves to reach the management hosts.**

CSVPN 4.0—2-52

Where possible, Syslog traffic may be encrypted within an IPSec tunnel in order to mitigate the chance of its being altered in transit. Where the Syslog data cannot be encrypted within an IPSec tunnel because of cost or the capabilities of the device itself, the network administrator should note that there is a potential for the Syslog data to be falsified by an attacker.

When allowing Syslog access from devices on the outside of a firewall, RFC 2827 filtering at the egress router should be implemented. This scenario will mitigate the chance of an attacker from outside the network spoofing the address of the managed device, and sending false Syslog data to the management hosts.

ACLs should also be implemented on the firewall in order to allow Syslog data from only the managed devices themselves to reach the management hosts. This scenario prevents an attacker from sending large amounts of false Syslog data to a management server in order to confuse the network administrator during an attack.

## TFTP

- **Many network devices use TFTP for transferring configuration or system files across the network. TFTP uses port 69 for both TCP and UDP.**
- **The following are TFTP issues:**
  - **TFTP uses UDP for the data stream between the device and the TFTP server.**
  - **TFTP sends data in clear text. The network administrator should recognize that the data within a TFTP session may be intercepted by anyone with a packet sniffer located along the data path between the requesting host and the TFTP server.**
- **When possible, TFTP traffic should be encrypted within an IPSec tunnel in order to mitigate the chance of its being intercepted.**

　　　　CSVPN 4.0—2-53

Many network devices use TFTP for transferring configuration or system files across the network. TFTP uses UDP for the data stream between the requesting host and the TFTP server.

As with other management protocols that send data in clear text, the network administrator should recognize that the data within a TFTP session might be intercepted by anyone with a packet sniffer located along the data path between the device and the management server. Where possible, TFTP traffic should be encrypted within an IPSec tunnel in order to mitigate the chance of its being intercepted.

## NTP

- NTP is used to synchronize the clocks of various devices across a network. It is critical for digital certificates, and for correct interpretation of events within Syslog data. NTP uses port 123 for both UDP and TCP connections.
- The following are NTP issues:
  - An attacker could attempt a DoS attack on a network by sending bogus NTP data across the Internet in an attempt to change the clocks on network devices in such a manner that digital certificates are considered invalid.
  - An attacker could attempt to confuse a network administrator during an attack by disrupting the clocks on network devices.
  - Many NTP servers on the Internet do not require any authentication of peers.
- The following are NTP recommendations:
  - Implement your own master clock for the private network synchronization.
  - Use NTP Version 3 or above as these versions support a cryptographic authentication mechanism between peers.
  - Use ACLs that specify which network devices are allowed to synchronize with other network devices.

　　　　　　CSVPN 4.0—2-54

Network Time Protocol (NTP) is used to synchronize the clocks of various devices across a network. Synchronization of the clocks within a network is critical for digital certificates, and for correct interpretation of events within Syslog data.

A secure method of providing clocking for the network is for the network administrator to implement their own master clock for the private network synchronized to Coordinated Universal Time (UTC) via satellite or radio. However, clock sources are available to synchronize to via the Internet, if the network administrator does not wish to implement their own master clock because of costs or other reasons.

An attacker could attempt a DoS attack on a network by sending bogus NTP data across the Internet in an attempt to change the clocks on network devices in such a manner that digital certificates are considered invalid. Further, an attacker could attempt to confuse a network administrator during an attack by disrupting the clocks on network devices. This scenario would make it difficult for the network administrator to determine the order of Syslog events on multiple devices.

Version 3 and above of NTP supports a cryptographic authentication mechanism between peers. The use of the authentication mechanism as well as ACLs that specify which network devices are allowed to synchronize with other network devices is recommended to help mitigate against such a scenario. The network administrator should weigh the cost benefits of pulling clock information from the Internet with the possible risk of doing so and allowing it through the firewall. Many NTP servers on the Internet do not require any authentication of peers. Therefore, the network administrator must trust that the clock itself is reliable, valid, and secure.

# Summary

This topic summarizes the information you learned in this lesson.

## Summary

Cisco.com

- **The need for network security has increased as networks have become more complex and interconnected.**
- **The following are the components of a complete security policy:**
  - **Statement of authority and scope**
  - **Acceptable use policy**
  - **Identification and authentication policy**
  - **Internet use policy**
  - **Campus access policy**
  - **Remote access policy**
  - **Incident handling procedure**
- **The Security Wheel details the view that security is an ongoing process.**
- **The Security Wheel includes four phases: secure, monitor, test, and improve.**

CSVPN 4.0—2-56

# Summary (cont.)

- **The following are the four types of security threats:**
  - **Structured**
  - **Unstructured**
  - **Internal**
  - **External**
- **The following are common attack methods and techniques used by hackers:**
  - **Packet sniffers**
  - **IP weaknesses**
  - **Password attacks**
  - **DoS or DDoS**

CSVPN 4.0—2-57

## Summary (cont.)

- – **Man-in-the-middle attacks**
- – **Application layer attacks**
- – **Trust exploitation**
- – **Port redirection**
- – **Virus**
- – **Trojan horse**
- – **Operator error**
- **Management protocols can in themselves be a source of vulnerability**

CSVPN 4.0—2-58

**3**

# Overview of Virtual Private Networks and IPSec Technologies

## Overview

This lesson teaches what Virtual Private Networks (VPNs) are, and explores fundamental IP security (IPSec) technologies. It includes the following topics:

- Objectives

- Cisco VPN products

- IPSec overview

- IPSec protocol framework

- How IPSec works

- Summary

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Define the three VPN solutions.**
- **Describe the three Cisco VPN product families and their related products.**
- **Identify IPSec and other open standards supported by Cisco VPN products.**
- **Identify the component technologies of IPSec.**
- **Explain how IPSec works.**

CSVPN 4.0—3-2

# Cisco VPN Products

Cisco products support the latest in Virtual Private Network (VPN) technology. A VPN is a service offering secure, reliable connectivity over a shared public network infrastructure such as the Internet.
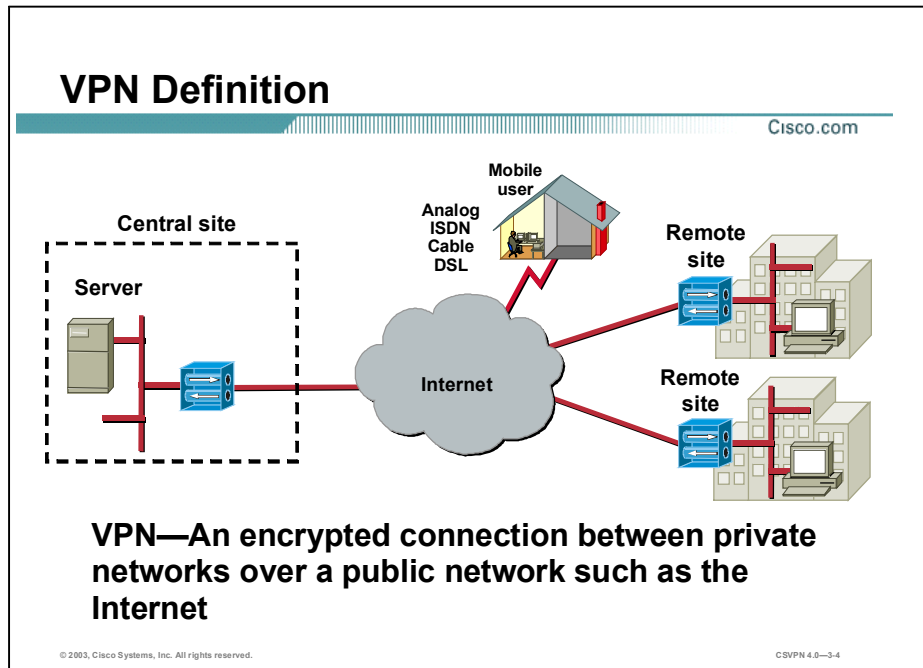


A VPN is an encrypted connection between private networks over a public network such as the Internet. The V and N stand for virtual network. The information from a private network is securely transported over a public network, an Internet, to form a virtual network. The P stands for private. To remain private, the traffic is encrypted to keep the data confidential. A VPN is a private virtual network.

There are three types of VPN networks:

■  Remote access

■  Site-to-site

■  Firewall-based

# Remote Access VPNs

Cisco.com

**Central Site**

**Remote access client**

DSL
cable

Telecommuter

POP

Internet

Router

or

or

Mobile

POP

Extranet
Consumer-to-business
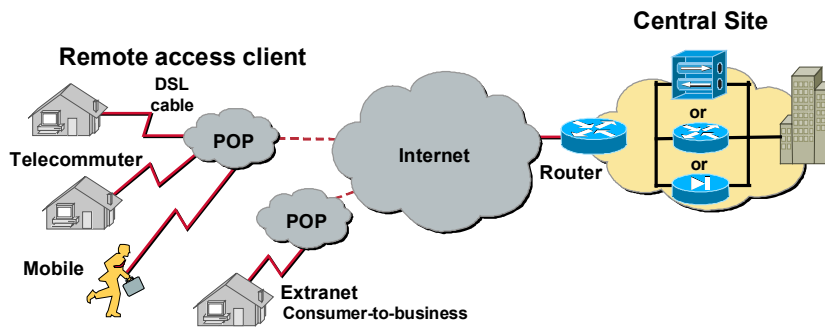
**Remote access VPN—Extension/evolution of dial**

CSVPN 4.0—3-5

The first VPN solution is remote access. Remote access is targeted to mobile users and home telecommuters. In the past, corporations supported remote users via dial-in networks. This typically necessitated a toll or toll-free call to access the corporation. With the advent of VPNs, a mobile user can make a local call to their ISP to access the corporation via the Internet wherever they may be. It is an evolution of dial networks. Remote access VPN can support the needs of telecommuters, mobile users, extranet consumer-to-business, and so on.

**Site-to-Site VPNs**

Cisco.com

Remote site

Central site

DSL cable

POP

Internet

Router

or

Extranet

Business-to-business

Intranet
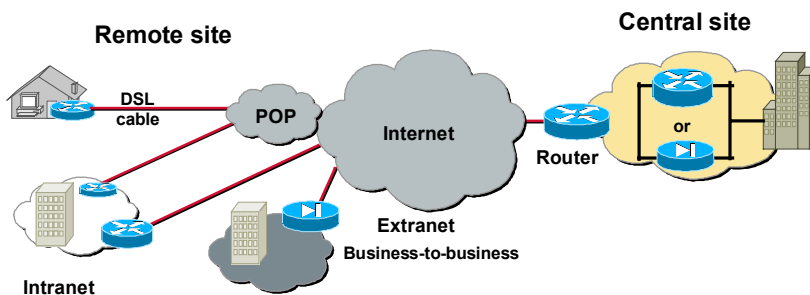
**Site-to-Site VPN—Extension of classic WAN**

CSVPN 4.0—3-6

The next VPN solution is site-to-site. VPN site-to-site can be used to connect corporate sites. In the past, a leased line or frame relay connection was required to connect sites, but now most corporations have Internet access. With Internet access, leased lines and frame relay lines can be replaced with site-to-site VPN. Use site-to-site VPN to provide the network connection. VPN can support company intranets and business partner extranets. Site-to-site VPN is an extension of classic Wide Area Network (WAN) network.

## Firewall-Based VPN Solutions

**Central site**

**Remote site**

**Internet**

**Intranet**

**Extranet**
**Business-to-business**
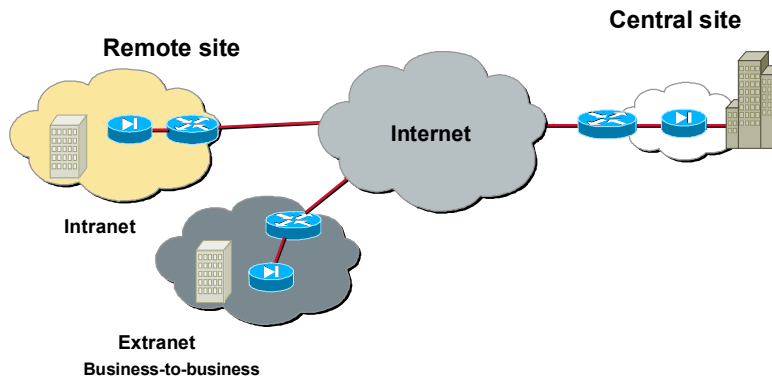
CSVPN 4.0—3-7

The last solution is firewall-based VPNs. Firewall-based VPN solutions are not a technical issue but a management issue. The question is who manages the VPN network. If corporate security manages the VPN network, a firewall-based VPN may be the VPN solution of choice. Corporations can enhance their existing firewall systems to support VPN services.

## VPN Product Function Matrix and Positioning

|  | Site-to-site VPN | Remote access VPN |
|---|---|---|
| VPN-enabled router | Primary role (full-fledged IOS) | Secondary role |
| 3000 | Secondary role | Primary role (full-fledged remote access solution) |
| PIX Firewall | Security organization owns VPN solution | Enhance existing PIX Firewall with the VPN remote access solution |

CSVPN 4.0—3-8

The VPN product function matrix compares VPN networks and Cisco products. In the top row of the table there are the two VPN applications: remote access and site-to-site. In the left column of the table, there are three product lines: VPN-enabled routers, the Concentrator, and the PIX Firewall. If the primary role of the equipment is to perform as a site-to-site VPN with a few remote access connections, the VPN-enabled router is the primary product. On the other hand, if the primary role is to perform as a remote access VPN with a few site-to-site connections, Concentrator is the product of choice. If the network is owned by the security organization, the PIX Firewall is the primary VPN product.

The following can be used as a reference for overall Cisco IP VPN positioning:

■ Dedicated VPN

— 3000 for remote access

— 7100/7200

■ VPN-enabled routers series

— SOHO/800

— 1700/2600

— 3700/3600

— 7200/7400/Cat6500

- Firewall VPN

  - PIX Firewall 5xx

**Remote Access VPNs—Concentrator**

Cisco.com

Remote access client

Central site

Telecommuter

POP    Internet

Mobile

Customer
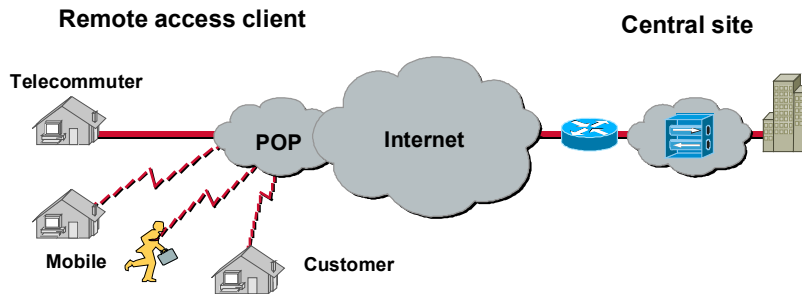
- **Connection of remote sites, users, and partners across a VPN**
- **High-density, low-bandwidth connections**

CSVPN 4.0—3-9

The Cisco VPN 3000 Concentrator Series is a family of purpose-built, remote access VPN platforms and VPN Client software that incorporates high availability, high performance, and scalability with the most advanced encryption and authentication techniques available today. With the Cisco VPN 3000 Concentrator Series, customers can take advantage of the latest VPN technology to vastly reduce their communications expenditures. Unique to the industry, it is the only scalable platform to offer field-swappable and customer-upgradeable components. These components, called Scalable Encryption Processing (SEP) modules, enable companies to easily add capacity and throughput.

With all versions of the Concentrator, the Cisco VPN Client is provided at no additional charge and includes unlimited distribution licensing. The Cisco VPN 3000 Concentrator Series is available in redundant or load-balancing configurations, enabling customers to build the most robust, reliable, and cost-effective VPNs possible.

The Cisco VPN 3002 Hardware Client is a network appliance used to connect Small Office Home Office (SOHO) LANs to the VPN. The device comes in either a single port or eight-port switch version. The Hardware Client replaces traditional VPN Client applications on individual SOHO computers.

All models in the Cisco VPN 3000 Concentrator Series support an easy-to-use management interface accessible via a web browser.

## Cisco VPN 3000 Concentrator Series

| | 3005 | 3015 | 3030 | 3060 | 3080 |
|---|---|---|---|---|---|
| Simultaneous sessions | 100 | 100 | 1500 | 5000 | 10000 |
| Site-to-site tunnels | 100 | 100 | 500 | 1000 | 1000 |
| Performance (Mbps) | 4 | 4 | 50 | 100 | 100 |
| Hardware encryption | No | No | Yes | Yes | Yes |
| Upgradeable | No | Yes | Yes | Yes | N/A |

The Cisco VPN 3000 Concentrator Series includes models to support a range of enterprise customers, from small businesses with 100 or fewer remote access sessions to large organizations with up to 10,000 simultaneous remote sessions. The Cisco VPN 3000 Concentrator Series table can be used to determine which model is best for your environment. The top row lists the five models in the Cisco VPN 3000 Concentrator Series family. The left column lists some of the VPN characteristics.

## VPN Clients

Cisco.com

Certicom PDA IPSec
VPN Client

Small office

Internet
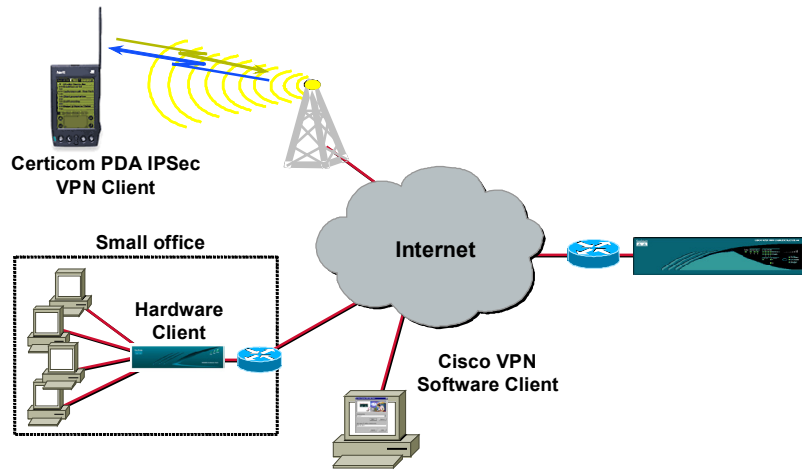
Hardware
Client

Cisco VPN
Software Client

The Concentrators can communicate with three IPSec clients: the Certicom IPSec client, the Cisco VPN Software Client, and the Hardware Client. The Certicom Client is a wireless client loaded on wireless PDAs such as the Palm operating system, HP Jornada, Compaq iPAQ, and so on. The Cisco VPN Software Client is loaded on an individual's PC. The Hardware Client is a standalone client located in small offices and home offices.

**Site-to-Site VPNs—Cisco Routers**

Cisco.com

Remote office
**1700/2600 Series**

Main office
**7100/7200/7400 Series**

Regional office
**3600/3700 Series**

Internet

Small office/ home office
**SOHO/800 Series**
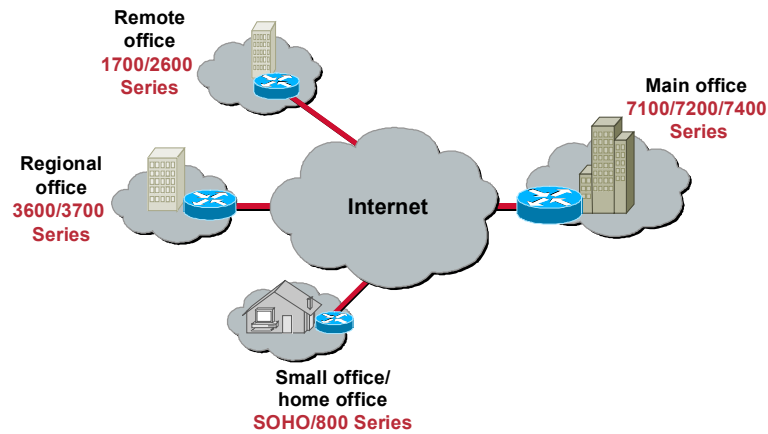
CSVPN 4.0—3-12

Site-to-site VPNs provide cost benefits relative to private WANs and also enable new applications like extranets. However, site-to-site VPNs are still an end-to-end network and are subject to the same scalability, reliability, security, multi-protocol, and so on—requirements that exist in the private WAN. In fact, because VPNs are built on a public network infrastructure, they have additional requirements such as heightened security and advanced Quality of Service (QoS) capabilities, and a set of policy management tools to manage these additional features.

Cisco provides a suite of VPN-optimized routers. Cisco IOS software running in Cisco routers combines rich VPN services with industry-leading routing, thus delivering a comprehensive solution. Cisco routing software adds scalability, reliability, multi-protocol, multi-service, management, Service Level Agreement monitoring, and QoS to site-to-site applications. The Cisco VPN software adds strong security via encryption and authentication. These Cisco VPN-enabled products provide high performance for site-to-site, intranet, and extranet VPN solutions.

**Cisco VPN Router Portfolio—SOHO and Small to Med-Sized Enterprise**

Cisco.com

Performance and Services

Cisco 3745

Cisco 3725

Cisco 3600

Cisco 2600XM/2691

Cisco 1760

Cisco 1700

Cisco 800

Teleworker/SOHO | SMB/Small Branch | Enterprise branch | Large branch | Enterprise HQ and beyond

CSVPN 4.0—3-13
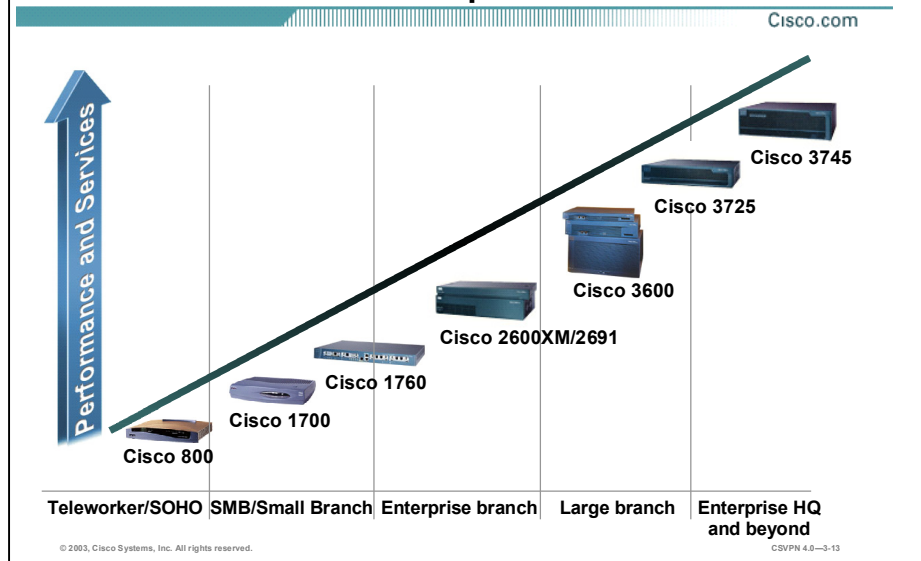
Cisco provides a suite of VPN-optimized routers. These routers run the range of VPN applications from telecommuter applications with the Cisco 800 router; to small branch office, connectivity with Cisco 1700 router; to enterprise branch with Cisco 1760 router; to the large branch with Cisco 3600 and 3725 routers; and enterprise headquarters with the Cisco 3745 router. VPN-optimized routers provide VPN solutions for hybrid VPN environments where modularity, port density, and flexibility are required for private WAN aggregation and other classic WAN applications.

## Small to Mid-Size—Cisco VPN Router Details

| | 800 | 1700 | 2600XM | 3620 | 3640A | 3660 |
|---|---|---|---|---|---|---|
| Maximum tunnels | 10 | 100 | 300 | 800 | 800 | 1300 |
| Performance (Mbps) | 0.384 | 4 | 12 | 10 | 18 | 40 |
| Hardware encryption | None | VPN module | AIM-VPN/BP | NM-VPN/MP | NM-VPN/MP | AIM-VPN/BP |

- **Hardware accelerators deliver enhanced encryption performance**

You can use the table in the figure to determine which model is best for your small- to mid-sized environment. The table identifies router platforms, and their related hardware accelerator card and maximum throughput. Lab performance numbers are based on the following configuration: Triple-Data Encryption Standard (3DES) with Hashed Message Authentication Code (HMAC)-Security Hash Algorithm 1 (SHA-1), 100% CPU use, and no other services running, such as QoS, Network Address Translation (NAT), Generic Routing Encapsulation (GRE), and so on. Actual network performance varies, depending on the services running in each router.

Hardware encryption accelerator cards provide high-performance, hardware-assisted encryption, and key generation suitable for VPN applications. Hardware encryption accelerators improve overall system performance by offloading encryption and decryption processing, thus freeing main system resources for other tasks, such as route processing, QoS, and other network services. In mid-sized routers, there are four modules available:

- AIM-VPN/BP (Base Performance)—This advanced integration module (AIM) can be added to all Cisco 2600 routers

- AIM-VPN/HP (High Performance)—High performance AIM for Cisco 3660 routers

- NM-VPN/MP (Mid Performance)—This network module is supported on all Cisco 3620 and 3640 routers

**Cisco VPN Router Portfolio—Large Enterprise and Service Provider**

Cisco.com

Performance and Services

Cat 6500

Cisco 7400

Cisco 7200

Cisco 7140

Cisco 7120

Large Enterprise/Service Provider

CSVPN 4.0—3-15
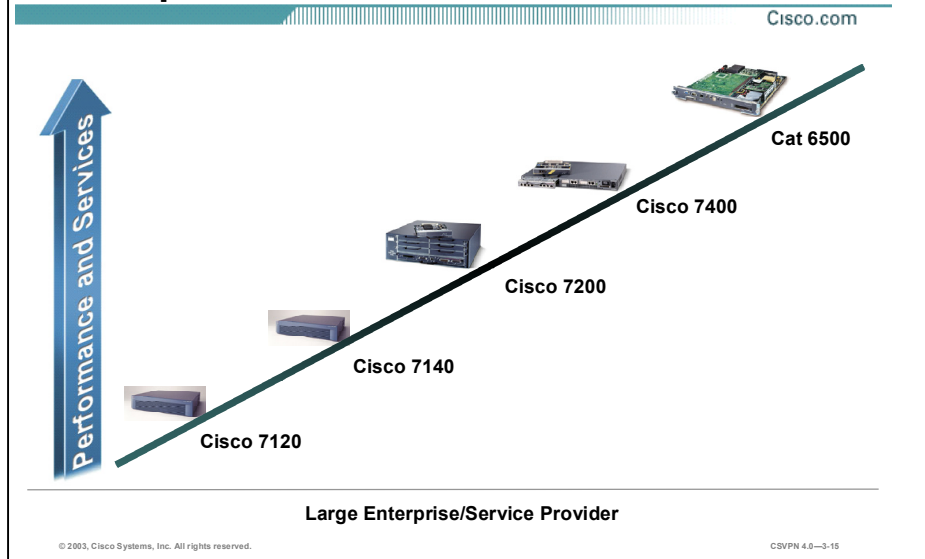
The Cisco VPN Router portfolio adds High-end VPN connectivity with Cisco 7100, 7200, 7400 series routers, and the Cisco Catalyst 6500 IPSec Services module. VPN-optimized routers and Cisco Catalyst 6500 IPSec VPN Services module provide VPN solutions for large-scale hybrid VPN environments where modularity, high performance, and flexibility are required.

## Enterprise Size and Service Provider—
## Cisco VPN Router Details

|  | 7120 | 7140 | 7140 | 7200 | 7400 | 7200 | CAT 6500 |
|---|---|---|---|---|---|---|---|
| Maximum tunnels | 2000 | 2000 | 3000 | 2000 | 5000 | 5000 | 8000 |
| Performance (Mbps) | 50 | 85 | 145 | 90 | 120 | 145 | 1.9G |
| Hardware encryption | ISM | ISM | VAM | ISA | VAM | VAM | Yes |

- **Hardware accelerators deliver enhanced encryption performance**

You can use the table in the figure to determine which enterprise model is best for your environment. The table identifies router platforms, and their related hardware encryption accelerator card and maximum throughput. Lab performance numbers are based on the following configuration: 3DES with HMAC-SHA-1, 100% CPU use, and no other services running, such as QoS, NAT, GRE, and so on. Actual network performance varies depending on the services running in each router.

Hardware encryption accelerator cards provide high-performance, hardware-assisted encryption, and key generation suitable for VPN applications. For the enterprise routers, there are three versions:

■ VPN Acceleration Module (VAM)—The VAM for Cisco 7200 and 7100 series routers provides high-performance, hardware-assisted encryption, and key generation. VAM also supports IP payload Lempel-Ziv Compression (LZS) compression services for VPN applications. There are two versions: VAM Service Adapter and VAM Service Module.

■ Integrated Service Module (ISM)—ISM uses a special slot created for offloading encryption and key generating services within the Cisco 7100 series routers (maximum of one ISM per Cisco 71XX series router).

■ Integrated Service Adapter (ISA)—ISA is a service adapter that inserts in any open port adapter slot in any Cisco 7200 router and can be used within the single port adapter of the Cisco 7140 router (up to one ISA per Cisco 7140 router or two per Cisco 7200 series routers, and not available on Cisco 7120 router).

The Cisco IPSec VPN Services Module is a high-speed module for the Cisco Catalyst 6500 Series Switch. Incorporating the latest in encryption hardware acceleration technology, the Cisco

IPSec VPN Services Module can deliver up to 1.9 Gbps of 3DES traffic and can terminate 8000 IPSec tunnels.

**Firewall-Based VPN—PIX Firewall**

Cisco.com

Remote site

Central site

Internet

Intranet

Extranet
**Business-to-business**

Remote User
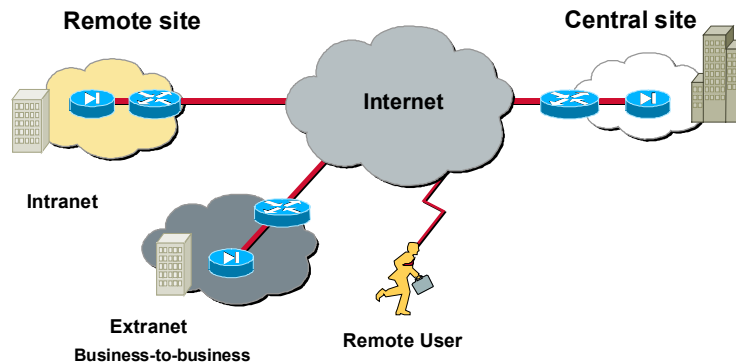
CSVPN 4.0—3-17

The PIX Firewall is a key element in the overall Cisco end-to-end security solution. The PIX Firewall is a dedicated hardware and software security solution that delivers high security without impacting network performance. If security manages the VPN, the PIX Firewall may be the VPN solution of choice. Customers may wish to enhance their existing Firewall equipment to support VPN services. Firewall-based VPN solutions support intranet, extranet, and remote user applications.

**PIX Firewall Family Overview**

Cisco.com

Performance

PIX 535

PIX 525

PIX 515E

PIX 506E

PIX 501

Gigabit Ethernet

SOHO | ROBO | SMB | Enterprise | SP

Functionality

CSVPN 4.0—3-18
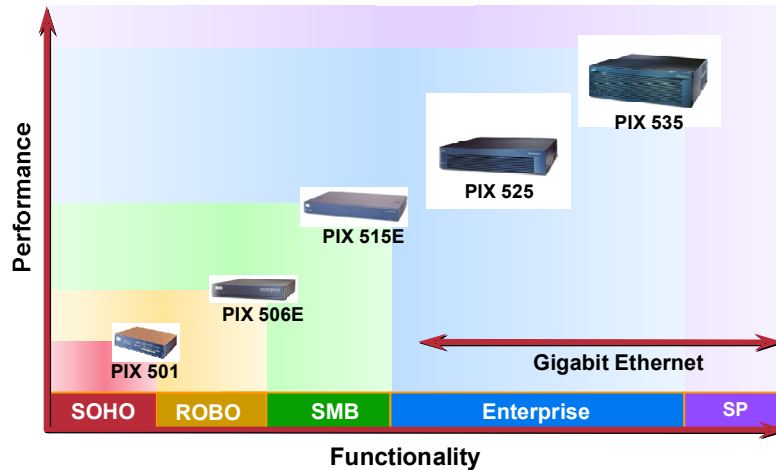
The Cisco PIX Firewall 500 series provides products that cover the entire spectrum of VPN site-to-site applications. The chart in the figure contrasts cost versus functionality. The following models are available:

■ PIX Firewall 501—Supports up to 5 tunnels

■ PIX Firewall 506E—Supports up to 25 tunnels

■ PIX Firewall 515E—Supports up to 2,000 tunnels

■ PIX Firewall 525—Supports up to 2,000 tunnels

■ PIX Firewall 535—Supports up to 2,000 tunnels

The Cisco PIX Firewall 500 series scales to meet a range of VPN requirements and network sizes.

## PIX Firewall Product Line Details

Cisco.com
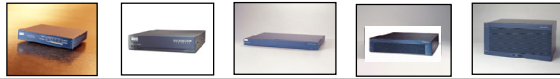
| | 501 | 506E | 515E | 525 | 535 |
|---|---|---|---|---|---|
| **Maximum tunnels** | 5 | 25 | 1,000 (SW) 2,000 (HW) | 1,000 (SW) 2,000 (HW) | 1,000 (SW) 2,000 (HW) |
| **VPN performance (Mbps)** | 3 | 16 | 22 (SW) 63 (HW) | 32 (SW) 72 (HW) | 53 (SW) 100 (HW) |
| **VPN hardware accelerator** | No | No | Yes | Yes | Yes |
| **Firewall throughput (Mbps)** | 10 | 20 | 188 | 360 | 1.7 Gbps |

CSVPN 4.0—3-19

You can use the table in the figure to determine which PIX Firewall model is best for your VPN environment. The top row lists the five models in the PIX Firewall 500 series family. The left column lists some of the VPN and PIX Firewall characteristics.

The VPN Accelerator Card (VAC) for the Cisco PIX Firewall series provides high-performance, tunneling, and encryption services suitable for site-to-site and remote access applications. This hardware-based VPN accelerator is optimized to handle repetitive but voluminous mathematical functions required for IPSec. Offloading encryption function to the card not only improves IPSec encryption processing, but also improves IPSec encryption processing. The VAC fits in a PCI slot inside the PIX Firewall chassis. The PIX Firewall is equipped with a VAC and supports as many as 2000 encrypted tunnels for concurrent sessions with mobile users or other sites. There is a limit of one VAC for each of the following PIX Firewall models: 515E, 525, and 535.

## Cisco VPN Portfolio Summary

| Customer type | Remote access | Site-to-site | Firewall-based |
|---|---|---|---|
| Large enterprise | Concentrators 3060, 3080 | CAT 6500 Routers 7100, 7200, 7400 | PIX Firewall 525, 535 |
| Medium enterprise | Concentrator 3030 | Routers 3700, 7100 | PIX Firewall 515, 525 |
| Small business or branch office | Concentrators 3005, 3015 | Routers 1700, 3600 | PIX Firewalls 506, 515 |
| SOHO market | Cisco VPN Software Client Hardware Client | Routers SOHO, 800 | PIX Firewall 501, 506 |

- **Cisco now provides the industry's broadest VPN solution set.**

Cisco now provides the industry's broadest VPN solution set. Cisco provides solutions from SOHO and small branch offices to the medium and large enterprise customers. Cisco provides solutions for remote access, site-to-site, and firewall-based VPN solutions.

The top row of the table in the figure lists the three VPN solutions. The left column of the table lists the four customer types. You can use this table to determine which model is best for your environment.

## VPN Interoperability

|  | IOS | PIX Firewall | Concentrator | Cisco VPN Client |
|---|---|---|---|---|
| **Required IOS release** | – | 12.1 | 12.1 | 12.2(8)T |
| **Required PIX Firewall release** | 5.2 | – | 5.2 | 6 |
| **Required Concentrator release** | 2.5(2) | 2.5(2) | – | 3 |

CSVPN 4.0—3-21

It is possible to interoperate between Cisco devices in a site-to-site environment. In a customer's network, there may be a PIX Firewall at one site and a Cisco router at another. A VPN tunnel can be established between the PIX Firewall and router as long as the software is at the minimum required revision. The site-to-site VPN interoperability table in the figure provides IOS, PIX Firewall, and Concentrator software revision levels.

# IPSec Overview

This topic presents an overview of the IPSec family of open standards.
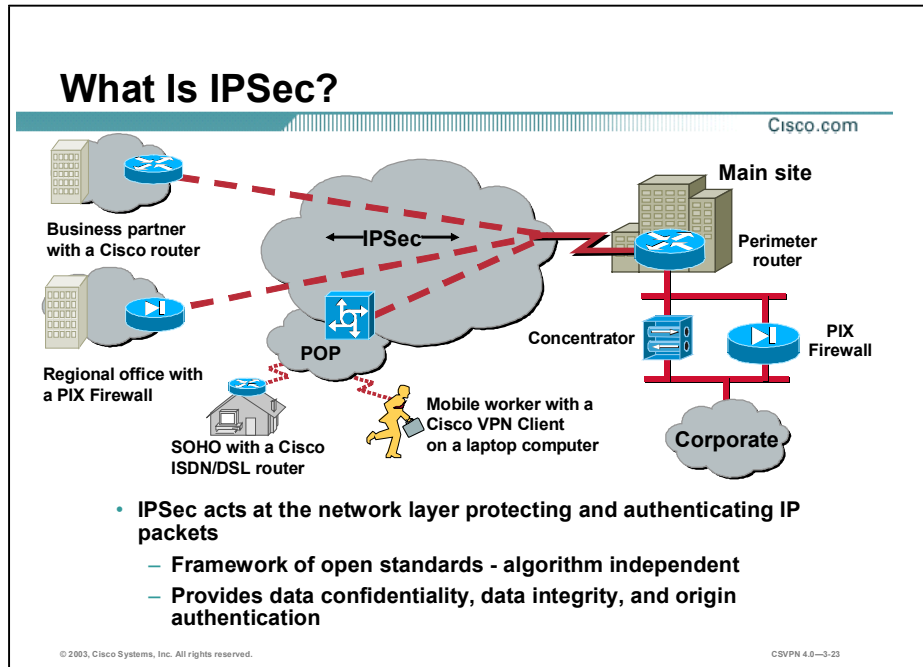


IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (peers). IPSec is not bound to any specific encryption or authentication algorithms, keying technology, or security algorithms. IPSec is a framework of open standards. By not binding IPSec to specific algorithms, IPSec allows for newer and better algorithms to be implemented without patching the existing IPSec standards. IPSec provides data confidentiality, data integrity, and origin authentication between participating peers at the IP layer. IPSec is used to secure a path between a pair of gateways, a pair of hosts, or a gateway and host.

## IPSec Security Services

- **Confidentiality**
- **Data integrity**
- **Origin authentication**
- **Anti-replay protection**

CSVPN 4.0—3-24

IPSec security services provides four critical functions:

■ Confidentiality (encryption)—The sender can encrypt the packets before transmitting them across a network. By doing so, no one can eavesdrop on the communication. If intercepted, the communications cannot be read.

■ Data integrity—The receiver can verify that the data was transmitted through the Internet without being changed or altered in any way.

■ Origin authentication—The receiver can authenticate the source of the packet, guaranteeing and certifying the source of the information.

■ Anti-replay protection—Anti-replay protection verifies that each packet is unique, not duplicated. IPSec packets are protected by comparing the sequence number of the received packets and a sliding window on the destination host, or security gateway. Packets whose sequence number is before the sliding window is considered late, or a duplicate. Late and duplicate packets are dropped.

## Confidentiality (Encryption)

Cisco.com

This quarterly report does not look so good. Hmmm . . . .

Server

Internet

Earnings off by 15%

CSVPN 4.0—3-25
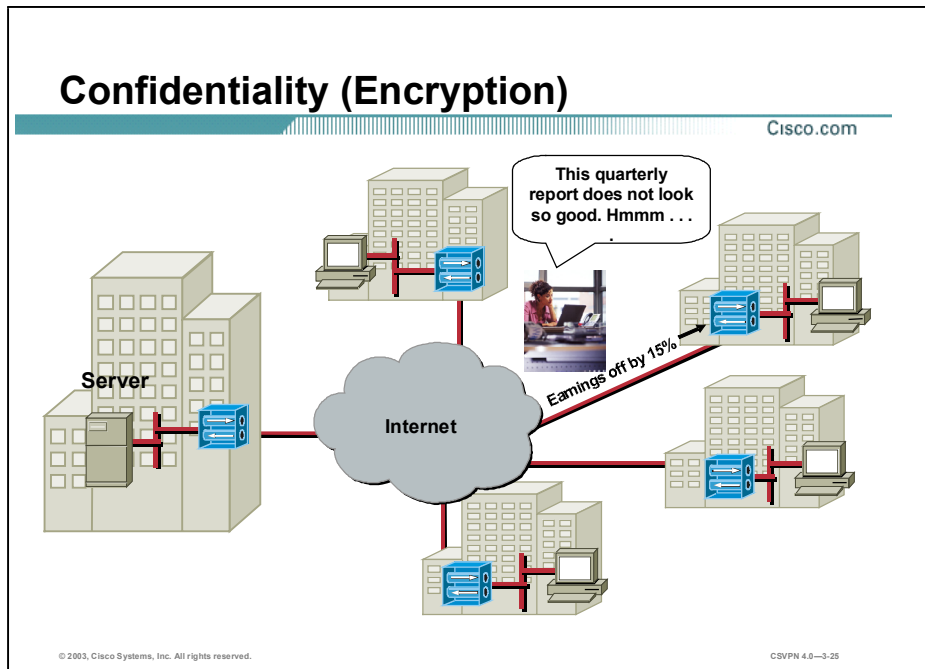
The good news is that the Internet is a public network. The bad news is that the Internet is a public network. Clear text data transported over the public Internet can be intercepted and read. In order to keep the data private, the data can be encrypted. By digitally scrambling, the data is rendered unreadable.

## Basics of Encryption

CSVPN 4.0—3-26
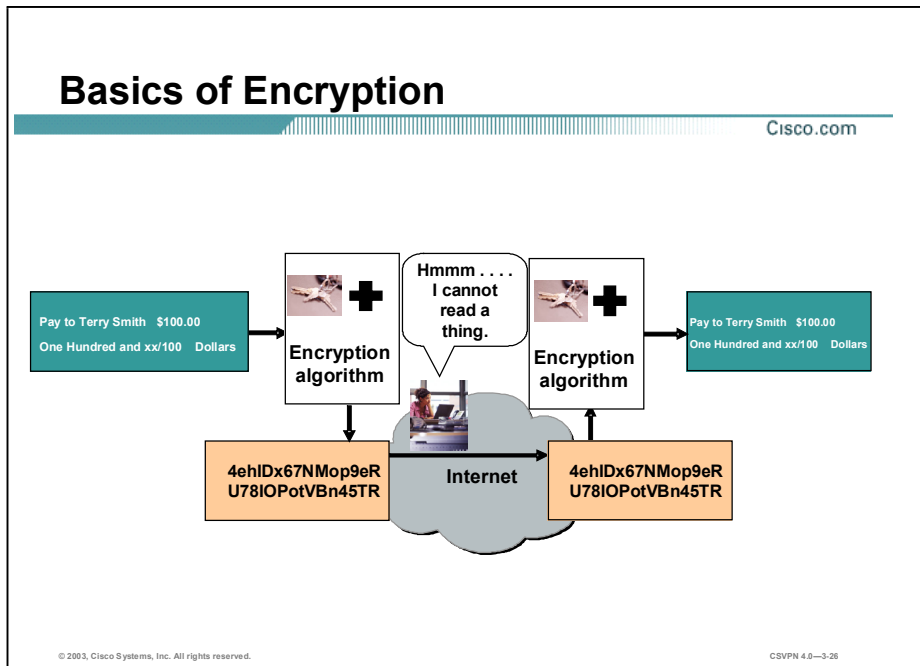
For encryption to work, both the sender and receiver need to know the rules used to transform the original message into its coded form. Rules are based on an algorithm and a key. An algorithm is a mathematical function, which combines a message, text, digits, or all three with a string of digits called a key. The output is an unreadable cipher string. Decryption is extremely difficult or impossible without the correct key.

In the example in the figure, someone wants to send a financial document across the Internet. At the local end, the document is combined with a key and run through an encryption algorithm. The output is undecipherable cyber text. The cyber text is then sent through the Internet. At the remote end, the message is recombined with a key and sent back through the encryption algorithm. The output is the original financial document.

There are two types of encryption keys:

■ Symmetric—With symmetric key encryption, each peer uses the same key to encrypt and decrypt the data.

■ Asymmetric—With asymmetric key encryption, the local end uses one key to encrypt, and the remote end uses another key to decrypt the traffic.

## DH Key Exchange

Cisco.com

Terry
**public key B**
**+ private key A**
**shared secret key (BA)**

Key = Key

Alex
**public key A**
**+ private key B**
**shared secret key (AB)**

Protocol Messages
Data Traffic
Pay to Terry Smith          $100.00
One Hundred and xx/100    Dollars

→ Decrypt

Decrypt ←

Protocol Messages
Data Traffic
Pay to Terry Smith          $100.00
One Hundred and xx/100    Dollars

4ehIDx67NMop9eR
U78IOPotVBn45TR

**Internet**

4ehIDx67NMop9eR
U78IOPotVBn45TR

CSVPN 4.0—3-27

DES, 3DES, AES, HMAC-Message Digest 5 (MD5), and HMAC-SHA require a symmetric shared secret key to perform encryption and decryption. The question is how does the encrypting and decrypting devices get the shared secret key? The keys can be sent by e-mail, courier, overnight express, or public key exchange. The easiest method is Diffie-Hellman (DH) public key exchange. The DH key agreement is a public key exchange method that provides a way for two peers to establish a shared secret key, which only they know, although they are communicating over an insecure channel.
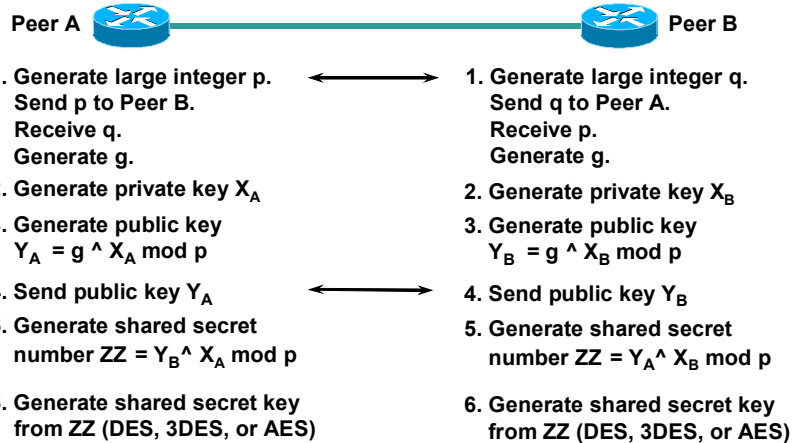
Public key cryptosystems rely on a two-key system: a public key, which is exchanged between end-users, and a private key, which is kept secret by the original owners. DH public key algorithm states that if user A and user B exchange public keys and a calculation is performed on their individual private key and one another's public key, the end result of the process is an identical shared key. The shared key is used to derive encryption and authentication keys. DH key exchange is covered in more depth later in this lesson.

There are variations of the DH key exchange algorithm, known as DH group 1 through 7. DH groups 1, 2, and 5 support exponentiation over a prime modulus with a key size of 768,1024, and 1536 respectively. Cisco VPN Clients support DH groups 1, 2, and 5. DES and 3DES encryption supports DH groups 1 and 2. AES encryption supports DH groups 2 and 5. The Certicom wireless VPN Client supports group 7. Group 7 supports elliptical curve cryptography that reduces the time needed to generate keys. During tunnel setup, VPN peers negotiate which DH group to use.

Security is not an issue with the DH key exchange. Although someone may know a user's public key, the shared secret cannot be generated because the private key never becomes public.
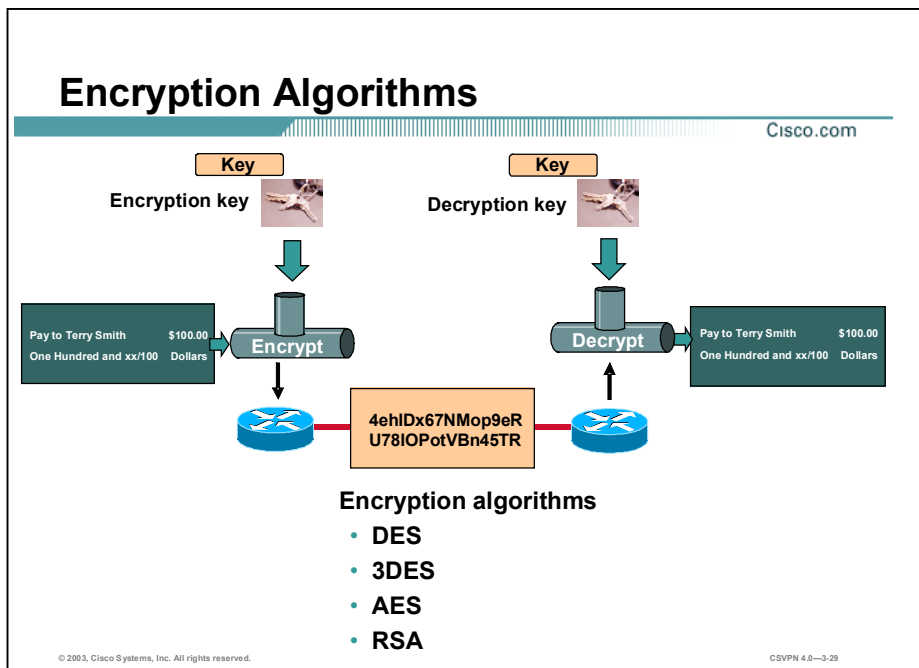
The DH key exchange is a public key exchange method that provides a way for two IPSec peers to establish a shared secret key that only they know, although they are communicating over an insecure channel.

With DH, each peer generates a public and private key pair. The private key generated by each peer is kept secret and never shared. The public key is calculated from the private key by each peer and is exchanged over the insecure channel. Each peer combines the other's public key with its own private key, and computes the same shared secret number. The shared secret number is then converted into a shared secret key. The shared secret key is never exchanged over the insecure channel.

Complete the following steps to implement the Diffie-Hellman process:

**Step 1** The DH process starts with each peer generating a large prime integer, p and q. Each peer sends the other its prime integer over the insecure channel. For example, Peer A sends p to Peer B. Each peer then uses the p and q values to generate g, a primitive root of p.

**Step 2** Each peer generates a private DH key (peer A: Xa, peer B: Xb).

**Step 3** Each peer generates a public DH key. The local private key is combined with the prime number p and the primitive root g in each peer to generate a public key, Ya for peer A and YA for peer B. The formula for peer A is $Ya = g^{Xa} \bmod p$. The formula for peer B is $Yb = g^{Xb} \bmod p$. The exponentiation is computationally expensive. The ^ character denotes exponentiation (g to the Xa power); mod denotes modulus.

**Step 4** The public keys Ya and Yb are exchanged in public.

**Step 5** Each peer generates a shared secret number (ZZ) by combining the public key received from the opposite peer with its own private key. The formula for peer A is $ZZ = (Y_b X_a) \bmod p$. The formula for peer B is $ZZ = (Y_a X_b) \bmod p$. The ZZ values are identical in each peer. Anyone who knows p or g, or the DH public keys, cannot guess or easily calculate the shared secret value—largely because of the difficulty in factoring large prime numbers.

Shared secret number ZZ is used in the derivation of the encryption and authentication symmetrical keys.

**Encryption Algorithms**

Cisco.com

Key — Encryption key

Key — Decryption key

Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars

Encrypt

Decrypt

Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars

4ehIDx67NMop9eR
U78IOPotVBn45TR

**Encryption algorithms**
- **DES**
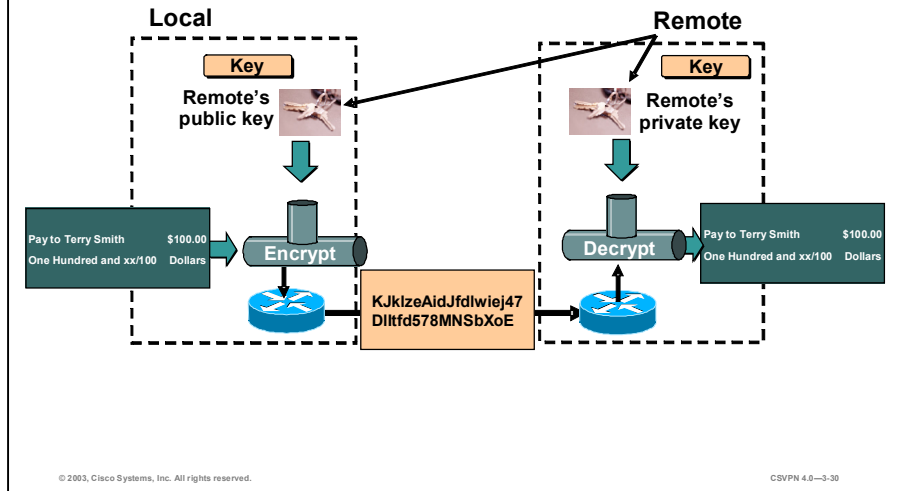- **3DES**
- **AES**
- **RSA**

CSVPN 4.0—3-29

The degree of security depends on the length of the key. If someone tries to hack the key through a brute force attack, guessing every possible combination, the number of possibilities is a function of the length of the key. The time to process all the possibilities is a function of the computing power of the computer. Therefore, the shorter the key, the easier it is to break.

Some of the encryption algorithms are as follows:

- DES algorithm—DES was developed by IBM. DES uses a 56-bit key, ensuring high performance encryption. DES is a symmetric key cryptosystem.

- 3DES algorithm—The 3DES algorithm is a variant of the 56-bit DES. 3DES operates similarly to DES, in that data is broken into 64-bit blocks. 3DES then processes each block three times, each time with an independent 56-bit key. 3DES effectively doubles encryption strength over 56-bit DES. DES is a symmetric key cryptosystem.

- Advanced Encryption Standard (AES)—The National Institute of Standards and Technology (NIST) has recently adopted a new Advanced Encryption Standard to replace existing DES encryption in cryptographic devices. AES provides stronger security than DES and computationally more efficient than 3DES. AES offers three different key strengths: 128, 192, and 256-bit keys.

- RSA—RSA is an asymmetrical key cryptosystem. It uses a key length of 512, 768, 1024, or larger. IPSec does not use RSA for data encryption. Internet Key Exchange (IKE) only uses RSA encryption during the peer authentication phase.

## RSA Encryption

Cisco.com

**Local**

Key

Remote's public key

**Remote**

Key

Remote's private key

Pay to Terry Smith    $100.00
One Hundred and xx/100    Dollars

**Encrypt**

KJklzeAidJfdlwiej47
Dlltfd578MNSbXoE

**Decrypt**

Pay to Terry Smith    $100.00
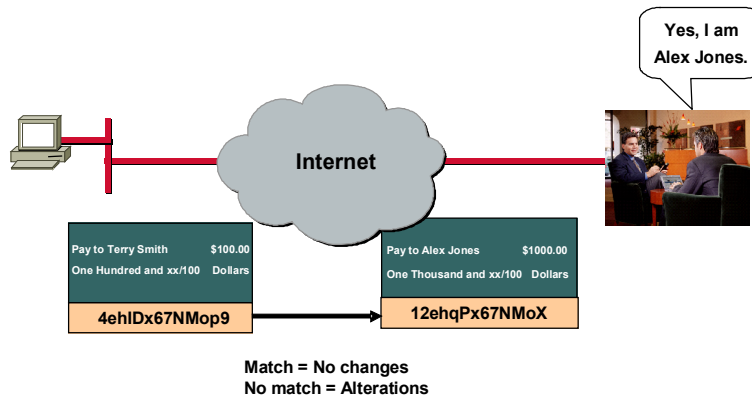One Hundred and xx/100    Dollars

CSVPN 4.0—3-30

Rivet, Shamir, and Adelman (RSA) is an encryption technique that is used for digital signatures. RSA encryption uses asymmetric keys for encryption and decryption. Each end, local and remote, generates two encryption keys: a private and public key. They keep their private key and exchange their public key with people they wish to communicate.

To send an encrypted message to the remote end, the local end encrypts the message using the remote's public key and the RSA encryption algorithm. The result is an unreadable cyber text. This message is sent through the Internet. At the remote end, the remote end uses its private key and the RSA algorithm to decrypt the cyber text. The result is the original message. The only one who can decrypt the message is the destination that owns the private key.

With RSA encryption, the opposite also holds true. The remote end can encrypt a message using its own private key. The receiver can decrypt the message using the sender's public key.

## Data Integrity

CISCO.COM

Yes, I am
Alex Jones.

Internet

Pay to Terry Smith      $100.00
One Hundred and xx/100   Dollars

4ehIDx67NMop9

Pay to Alex Jones      $1000.00
One Thousand and xx/100   Dollars

12ehqPx67NMoX

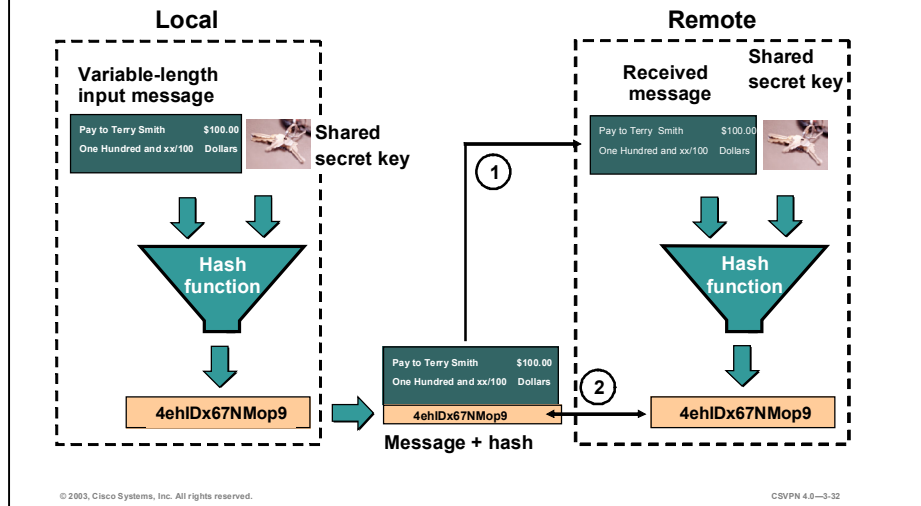**Match = No changes**
**No match = Alterations**

CSVPN 4.0—3-31

The next VPN-critical function is data integrity. VPN data is transported over the public Internet. Potentially, this data could be intercepted and modified. To guard against this, each message has a hash attached to the message. A hash guarantees the integrity of the original message. If the transmitted hash matches the received hash, the message has not been tampered with. However, if there is no match, the message was altered.

In the example in the figure, someone is trying to send Terry Smith a check for $100. At the remote end, Alex Jones is trying to cash the check for $1000. As the check progressed through the Internet, it was altered. Both the recipient and dollar amounts were changed. In this case, the hashes did not match. The transaction is no longer valid.

## HMAC

**Local**

**Variable-length input message**

Pay to Terry Smith                    $100.00
One Hundred and xx/100    Dollars

**Shared secret key**

**Hash function**

4ehIDx67NMop9

Pay to Terry Smith                    $100.00
One Hundred and xx/100    Dollars

4ehIDx67NMop9

**Message + hash**

**Remote**

**Received message**          **Shared secret key**

Pay to Terry  Smith              $100.00
One Hundred and xx/100    Dollars

**Hash function**

4ehIDx67NMop9

① ②

CSVPN 4.0—3-32

Hashed Message Authentication Codes (HMAC) guarantees the integrity of the message. At the local end, the message and a shared secret key are sent through a hash algorithm, which produces a hash value. The message and hash are sent over the network.

At the remote end, there is a two-step process. First, the received message and shared secret key are sent through the hash algorithm, resulting in a re-calculated hash value. Second, the receiver compares the re-calculated hash with the hash that was attached to the message. If the original hash and re-calculated hash match, the integrity of the message is guaranteed. If any of the original message is changed while in transit, the hash values are different.

Basically, a hash algorithm is a formula used to convert a variable length message into a single string of digits of a fixed length. It is a one-way algorithm. A message can produce a hash, but a hash cannot produce the original message. It is analogous to dropping a plate on the floor. The plate can produce a multitude of pieces, but the pieces cannot be recombined to reproduce the plate in its original form.
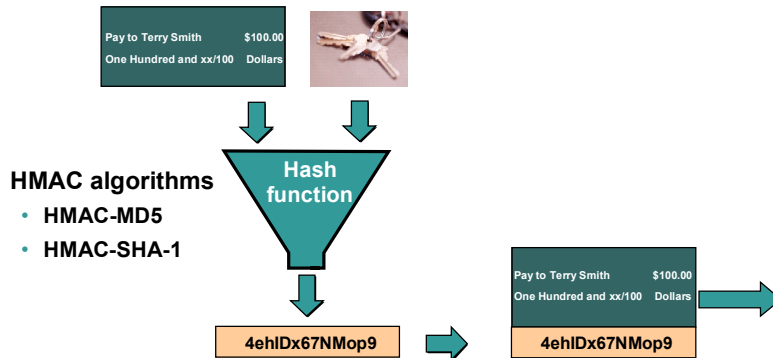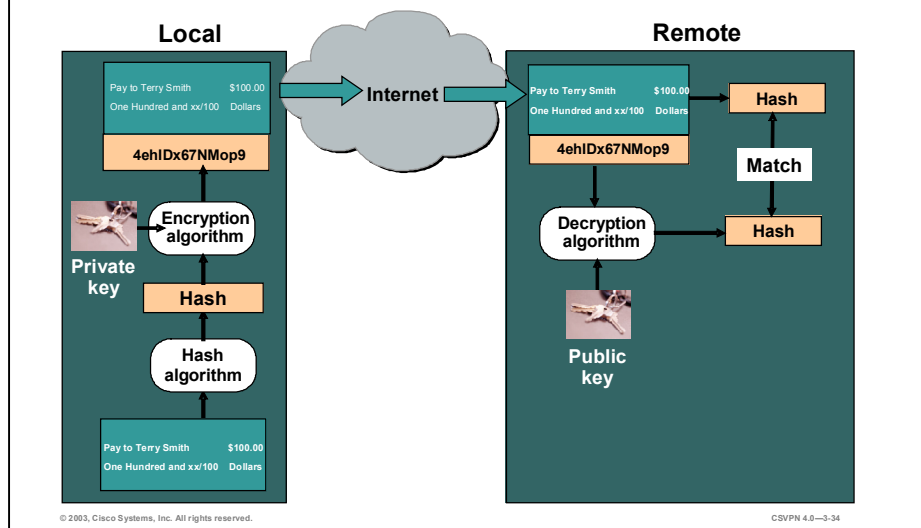
There are two common Hashed Message Authentication Codes (HMAC) algorithms:

- HMAC-MD5—Uses a 128-bit shared secret key. The variable length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.

- HMAC-SHA-1—HMAC-SHA-1 uses a 160-bit secret key. The variable length message and the 160-bit shared secret key are combined and run through the HMAC-SHA-1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

HMAC-SHA-1 is considered cryptographically stronger than HMAC-MD5. HMAC-SHA-1 is recommended when the security of HMAC-SHA-1 over HMAC-MD5 is important.

**Digital Signatures**

Cisco.com

Local

Pay to Terry Smith    $100.00
One Hundred and xx/100    Dollars

4ehIDx67NMop9

Private key → Encryption algorithm

Hash

Hash algorithm

Pay to Terry Smith    $100.00
One Hundred and xx/100    Dollars

Internet

Remote

Pay to Terry Smith    $100.00
One Hundred and xx/100    Dollars

4ehIDx67NMop9

Hash

Match

Decryption algorithm → Hash

Public key

CSVPN 4.0—3-34

The last critical function is origin authentication. In the middle ages, a seal guaranteed the authenticity of an edict. In modern times, a signed document is notarized with a seal and a signature. In the electronic era, a document is signed using the sender's private encryption key—a digital signature. A signature is authenticated by decrypting the signature with the sender's public key.

In the example in the figure, the local device derives a hash and encrypts it with its private key. The encrypted hash—digital signature—is attached to the message and forwarded to the remote end. At the remote end, the encrypted hash is decrypted using the local end's public key. If the decrypted hash matches the re-computed hash, the signature is genuine. A digital signature ties a message to a sender. The sender is authenticated. It is used during the initial establishment of a VPN tunnel to authenticate both ends to the tunnel.

There are two common digital signature algorithms: RSA and Directory System Agent (DSA). RSA is used commercially and is the most common. DSA is used by U.S. Government agencies and is not as common.

**Peer Authentication**
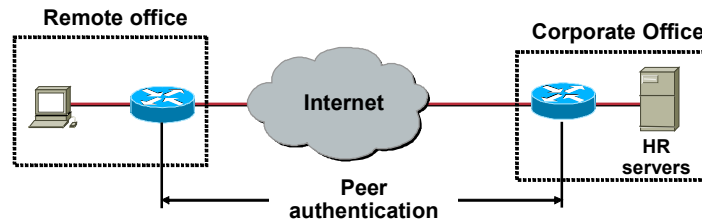
Cisco.com

Remote office

Internet

Corporate Office

HR servers

Peer authentication

**Peer authentication methods:**
- **Pre-shared keys**
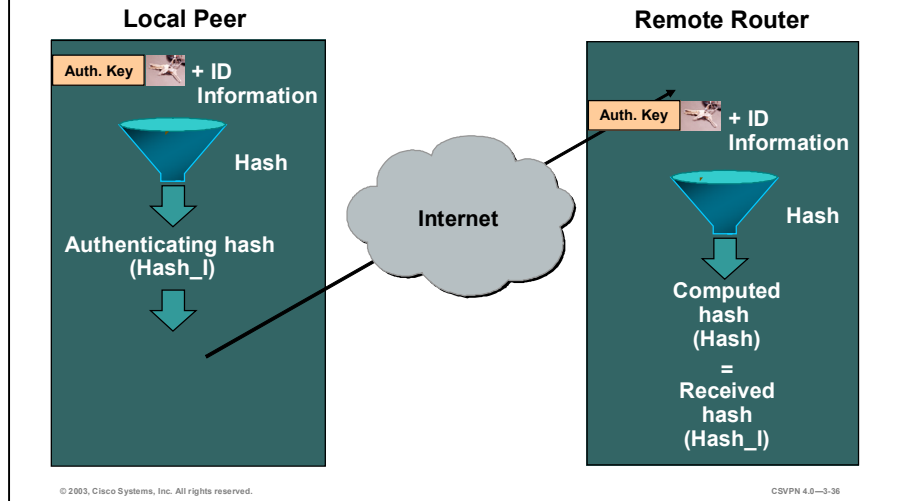- **RSA signatures**
- **RSA encrypted nonces**

CSVPN 4.0—3-35

When conducting business long distance, it is necessary to know who is at the other end of the phone, e-mail, or fax. The same is true of VPN networking. The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure. There are three peer authentication methods:

- Pre-shared keys—A secret key value entered into each peer manually used to authenticate the peer.

- RSA signatures—Uses the exchange of digital certificates to authenticate the peers.

- RSA encrypted nonces—Nonces (a random number generated by each peer) are encrypted then exchanged between peers. The two nonces are used during the peer authentication process.

## Pre-Shared Keys

Cisco.com

**Local Peer**

Auth. Key + ID Information

Hash

Authenticating hash (Hash_I)

**Internet**

**Remote Router**

Auth. Key + ID Information

Hash

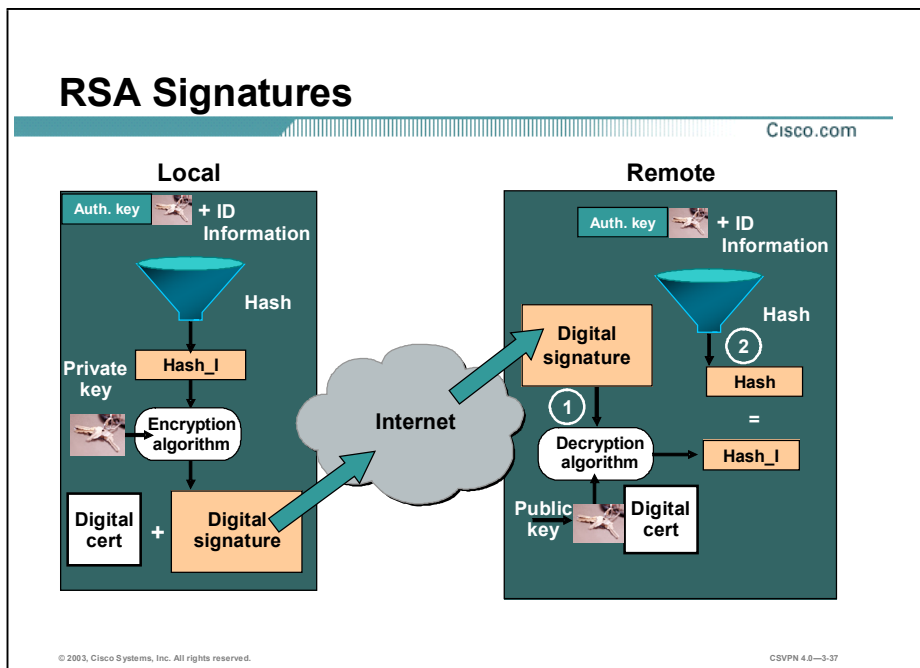Computed hash (Hash)
=
Received hash (Hash_I)

CSVPN 4.0—3-36

With pre-shared keys, the same pre-shared key is configured on each IPSec peer. At each end, the pre-shared key is combined with other information to form the authentication key. Starting at the local end, the authentication key and the identity information (device-specific information) are sent through a hash algorithm to form hash_I. The local IKE peer provides one-way authentication by sending hash_I to the remote peer. If the remote peer is able to independently create the same hash, the local peer is authenticated (shown above).

The authentication process continues in the opposite direction. The remote peer combines its identity information with the pre-shared-based authentication key and sends them through a hash algorithm to form hash_R. Hash_R is sent to the local peer. If the local peer is able to independently create the same hash from its stored information and pre-shared-based authentication key, the remote peer is authenticated. Each peer must authenticate its opposite peer before the tunnel is considered secure.Pre-shared keys are easy to configure manually, but do not scale well. Each IPSec peer must be configured with the pre-shared key of every other peer with which it communicates.

# RSA Signatures

Cisco.com

**Local**

Auth. key + ID Information

Hash

Private key → Hash_I

Encryption algorithm

Digital cert + Digital signature

**Internet**

**Remote**

Auth. key + ID Information

Hash

Digital signature

① Decryption algorithm → Hash_I

② Hash

=

Public key → Digital cert

CSVPN 4.0—3-37

With Rivest, Shamir, and Adleman (RSA) signatures, hash_I and hash_R are not only authenticated, but are also digitally signed. Starting at the local end, the authentication key and identity information (device-specific information) are sent through a hash algorithm to form hash_I. The hash_I is then encrypted using the local peer's private encryption key. The result is a digital signature. The digital signature and a digital certificate are forwarded to the remote peer. (The public encryption key for decrypting the signature is included in the digital certificate exchanged between peers.)

At the remote peer, local peer authentication is a two-step process. First, the remote peer verifies the digital signature by decrypting it using the public encryption key enclosed in the digital certificate. The result is hash_I. Next, the remote peer independently creates hash_I from stored information. If the calculated hash_I equals the decrypted hash_I, the local peer is authenticated (shown in the figure). Digital signatures and certificates are discussed in more detail later in the digital certificate lesson.

After the remote peer authenticates the local peer, the authentication process begins in the opposite direction. The remote peer combines its identity information with the authentication key and sends them through a hash algorithm to form hash_R. Hash_R is encrypted using the remote peer's private encryption key, a digital signature. The digital signature and certificate are sent to the local peer. The local peer performs two tasks: it creates the hash_R from stored information, and it decrypts the digital signature. If the calculated hash_R and the decrypted hash_R match, the remote peer is authenticated. Each peer must authenticate its opposite peer before the tunnel is considered secure.
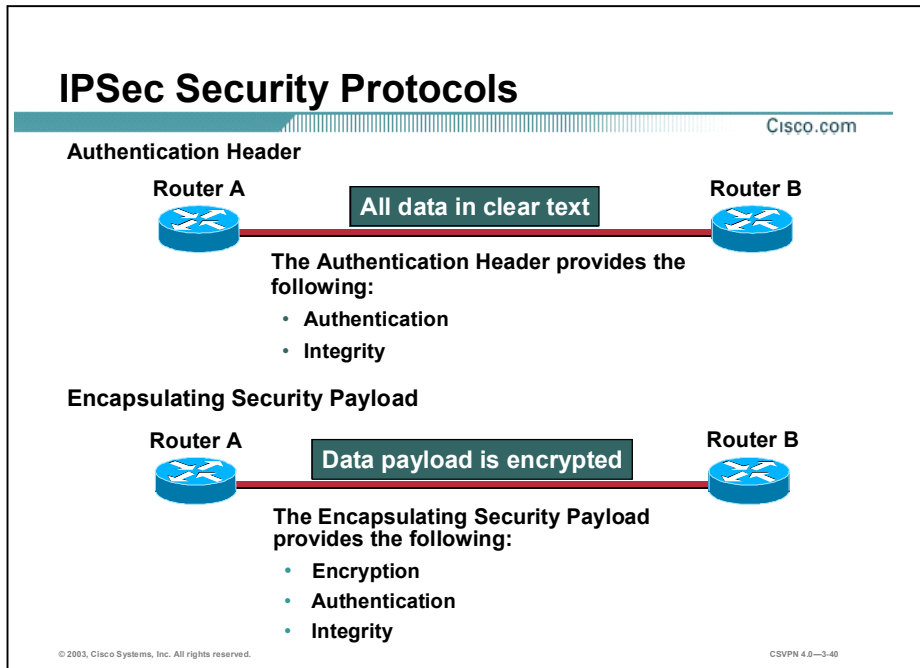
## RSA Encrypted Nonces
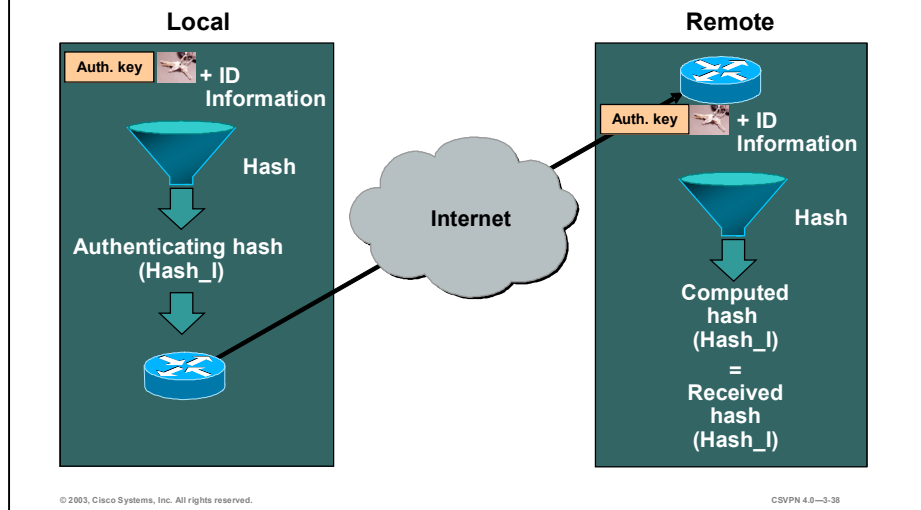
Rivest, Shamir, and Adleman (RSA) encrypted nonces require that each party generate a nonce—a pseudorandom number. The nonces are then encrypted and exchanged. Upon receipt of the nonce, each end formulates an authentication key made up of the initiator and responder nonces, the DH key, and the initiator and responder cookies. The nonce-based authentication key is combined with device-specific information and run through a hash algorithm. Where the output becomes hash_I. The local IKE peer provides one-way authentication by sending hash_I to the remote peer. If the remote peer is able to independently create the same hash from stored information and its nonce-based authentication key, the local peer is authenticated (shown above).

After the remote end authenticates the local peer, authentication process begins in the opposite direction. The remote peer combines its identity information with the nonce-based authentication key and sends them through a hash algorithm to form hash_R. Hash_R is sent to the local peer. If the local peer is able to independently create the same hash from stored information and the nonce-based key, the remote peer is authenticated. Each peer must authenticate its opposite peer before the tunnel is considered to be secure.

# IPSec Protocol Framework

The last topic discussed encryption, authentication, and integrity. This topic explains how encryption, integrity, and authentication are applied to the IPSec protocol suite.

## IPSec Security Protocols

Cisco.com

**Authentication Header**

Router A — All data in clear text — Router B

The Authentication Header provides the following:
- Authentication
- Integrity

**Encapsulating Security Payload**

Router A — Data payload is encrypted — Router B

The Encapsulating Security Payload provides the following:
- Encryption
- Authentication
- Integrity

© 2003, Cisco Systems, Inc. All rights reserved.                CSVPN 4.0—3-40

IPSec is a framework of open standards. IPSec spells out the messaging to secure the communications but relies on existing algorithms, such as DES and 3DES, to implement the encryption and authentication. The two main IPSec framework protocols are as follows:

■ Authentication Header (AH)—AH is the appropriate protocol when confidentiality is not required or permitted. It provides data authentication and integrity for IP packets passed between two systems. It is a means of verifying that any message passed from Router A to B has not been modified during transit. It verifies that the origin of the data was either Router A or B. AH does not provide data confidentiality (encryption) of packets. All text is transported in the clear.

■ Encapsulating Security Payload (ESP)—A security protocol may be used to provide confidentiality (encryption) and authentication. ESP provides confidentiality by performing encryption at the IP packet layer. IP packet encryption conceals the data payload and the identities of the ultimate source and destination. ESP provides authentication for the inner IP packet and ESP header. Authentication provides data origin authentication, and data integrity. Although both encryption and authentication are optional in ESP, at a minimum, one of them must be selected.

## Authentication Header

**Router A**                                    **Router B**

**All data in clear text**

- **Ensures data integrity**
- **Provides origin authentication (ensures packets definitely came from the peer)**
- **Uses keyed-hash mechanism**
- **Does not provide confidentiality (no encryption)**
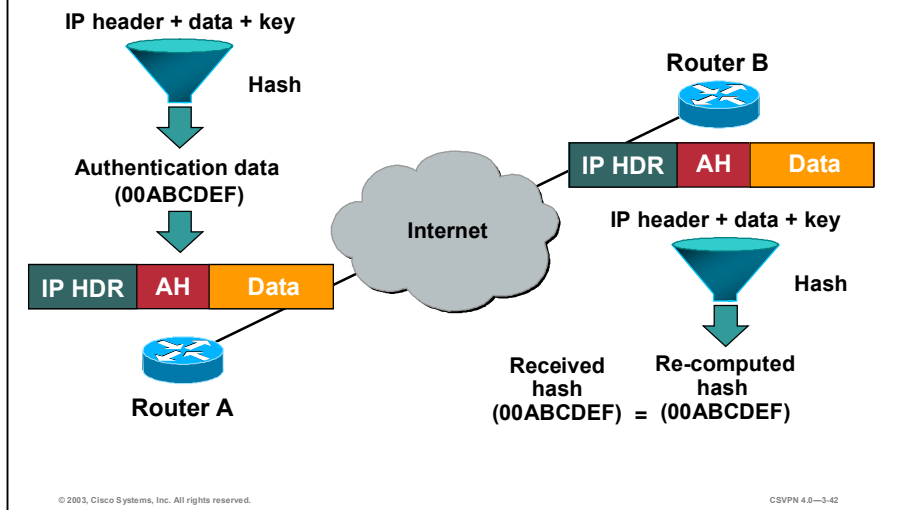- **Provides anti-replay protection**

CSVPN 4.0—3-41

Authentication is achieved by applying a keyed one-way hash function to the packet to create a hash or message digest. The hash is combined with the text and transmitted. Changes in any part of the packet that occur during transit are detected by the receiver when it performs the same one-way hash function on the received packet, and compares the value of the message digest that the sender has supplied. The fact that the one-way hash also involves the use of a symmetric key between the two systems means that authenticity is guaranteed.

# AH Authentication and Integrity

Cisco.com

IP header + data + key

Hash

Authentication data
(00ABCDEF)

IP HDR | AH | Data

Router A

Internet

Router B

IP HDR | AH | Data

IP header + data + key

Hash

Received
hash
(00ABCDEF) = 

Re-computed
hash
(00ABCDEF)

CSVPN 4.0—3-42

The Authentication Header (AH) function is applied to the entire datagram, except for any mutable IP header fields that change in transit (for example, Time To Live [TTL] fields that are modified by the routers along the transmission path). AH supports two algorithms:

■ HMAC-MD5

■ HMAC-SHA-1

AH works as follows:

**Step 1** The IP header and data payload is hashed.

**Step 2** The hash is used to build an AH header, which is appended to the original packet.

**Step 3** The new packet is transmitted to the IPSec peer.

**Step 4** The peer hashes the IP header and data payload.

**Step 5** The peer extracts the transmitted hash from the AH header.

**Step 6** The peer compares the two hashes. The hashes must exactly match. Even if one bit is changed in the transmitted packet, the hash output on the received packet will change and the AH header will not match.

.

ESP

Router A    Data payload is encrypted    Router B

- **Data confidentiality (encryption)**
- **Data integrity**
- **Data origin authentication**
- **Anti-replay protection**

CSVPN 4.0—3-43

Encapsulating Security Payload (ESP) provides confidentiality by encrypting the payload. It supports a variety of symmetric encryption algorithms. The default algorithm for IPSec is 56-bit DES. Cisco products also support the use of 3DES for stronger encryption.

ESP can be used alone or in combination with AH. ESP with AH also provides integrity, and authentication of the data grams. First, the payload is encrypted. Next, the encrypted payload is sent through a hash algorithm: HMAC-MD5 or HMAC-SHA-1. The hash provides origin authentication and data integrity for the data payload.

Alternatively, ESP may also enforce anti-replay protection by requiring that a receiving host set the replay bit in the header to indicate that the packet has been seen.

## ESP Protocol

CISCO.COM

**Internet**

Router                Router

| IP HDR | Data |                | IP HDR | Data |

| New IP HDR | ESP HDR | IP HDR | Data | ESP Trailer | ESP Auth |

← Encrypted →
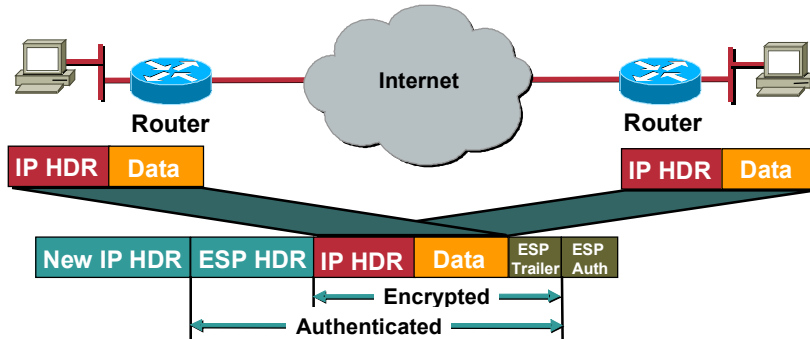
← Authenticated →

- **Provides confidentiality with encryption**
- **Provides integrity with authentication**

CSVPN 4.0—3-44

Between two security gateways, the original payload is well protected because the entire original IP data gram is encrypted. An Encapsulating Security Payload (ESP) header and trailer are added to the encrypted payload. With ESP authentication, the encrypted IP data gram and the ESP header or trailer are included in the hashing process. Last, a new IP header is appended to the front of the authenticated payload. The new IP address is used to route the packet through the Internet.

When both ESP authentication and encryption are selected, encryption is performed first before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can authenticate inbound packets. By doing this, it can detect the problems and potentially reduce the impact of denial of service (DoS) attacks.

CSVPN 4.0—3-45

## Modes of Use—Tunnel Versus Transport Mode

Cisco.com

| IP HDR | Data |
|--------|------|

**Transport mode**

| IP HDR | ESP HDR | Data | ESP Trailer | ESP Auth |
|--------|---------|------|-------------|----------|

Encrypted

Authenticated

**Tunnel mode**

| New IP HDR | ESP HDR | IP HDR | Data | ESP Trailer | ESP Auth |
|------------|---------|--------|------|-------------|----------|

Encrypted

Authenticated
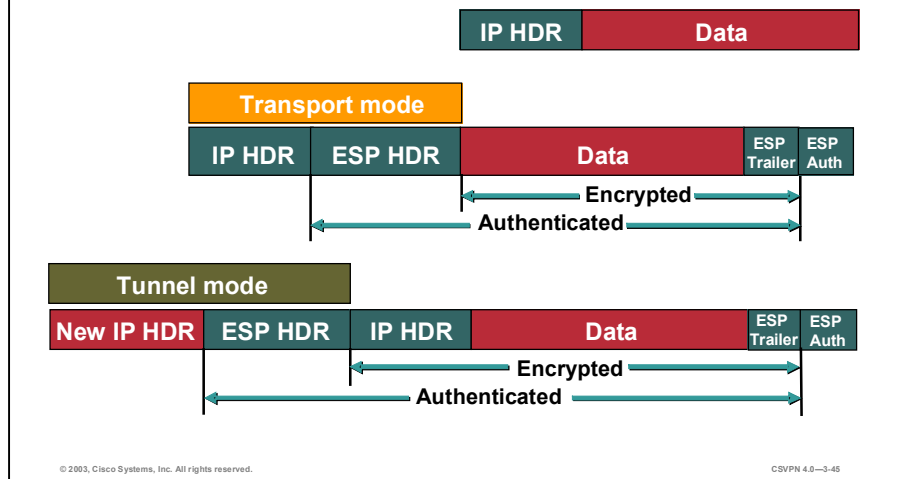
ESP and AH can be applied to IP packets in two different ways, which are referred to as modes:

■ Transport mode—Transport mode protects the payload of the packet, higher layer protocols, but leaves the original IP address in the clear. The original IP address is used to route the packet through the Internet. ESP transport mode is used between two hosts, when the final destination is the host itself. Transport mode provides security to the higher layer protocols only.

■ Tunnel mode—ESP tunnel mode is used when either end of the tunnel is a security gateway, a Concentrator, a VPN optimized router, or a PIX Firewall. Tunnel mode is used when the final destination is not a host, but a VPN gateway. The security gateway encrypts and authenticates the original IP packet. Next, a new IP header is appended to the front of the encrypted packet. The outside, new, IP address is used to route the packet through the Internet to the remote end security gateway. Tunnel mode provides security for the whole original IP packet.

# Tunnel Mode

**Remote office**

**Corporate office**

Internet

**HR servers**

**Tunnel mode**

**Home office**

**Corporate office**

Internet

**HR servers**
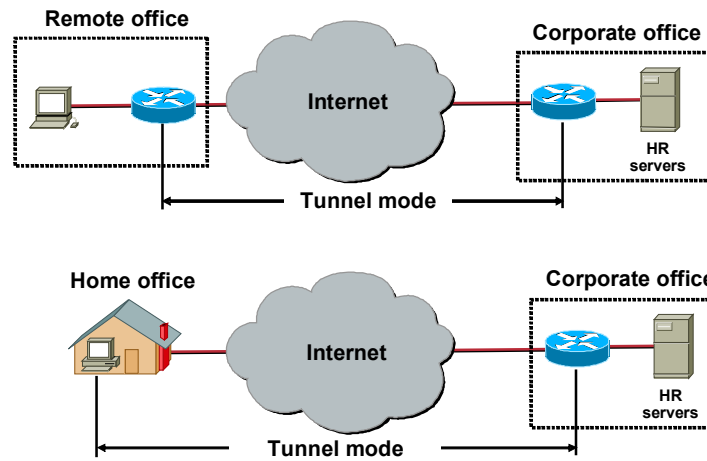
**Tunnel mode**

CSVPN 4.0—3-46

ESP tunnel mode is used between a host and a security gateway or between two security gateways. For gateway-to-gateway applications, rather than load IPSec on all the computers at the remote and corporate offices, it is easier to have the security gateways perform the IP-in-IP encryption and encapsulation.

In the IPSec remote access application, ESP tunnel mode is used. At a home office, there may be no router to perform the IPSec encapsulation and encryption. In the example in the figure, the IPSec client running on the PC performs the IPSec IP-in-IP encapsulation and encryption. At the corporate office, the router de-encapsulates and decrypts the packet.

## IPSec Protocol—Framework

Cisco.com

IPSec Framework

Choices:

| IPSec Protocol | | ESP | ESP +AH | AH |
| Encryption | | DES | 3 DES | AES |
| Authentication | | MD5 | SHA | |
| Diffie-Hellman | | DH1 | DH2 | |

CSVPN 4.0—3-47
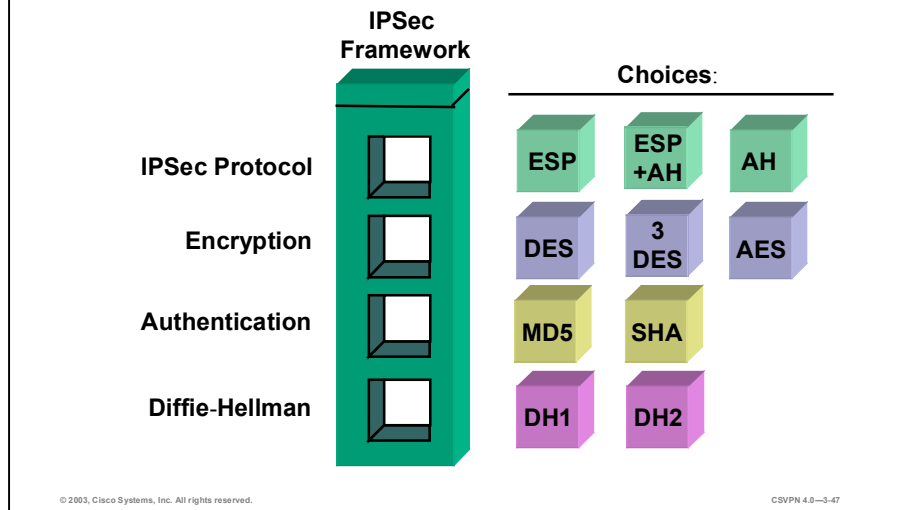
IPSec is a framework of open standards. IPSec spells out the rules for secure communications. IPSec, in turn, relies on existing algorithms to implement the encryption, authentication, and key exchange. Some of the standard algorithms are as follows:

- DES algorithm—DES is used to encrypt and decrypt packet data

- 3DES algorithm—Effectively doubles encryption strength over 56-bit DES

- AES algorithm—Faster throughput with even stronger encryption (depends on key length chosen)

- Message Digest 5 (MD5) algorithm—Used to authenticate packet data

- Secure Hash Algorithm-1 (SHA) algorithm—Authenticates packet data

- DH—A public-key cryptography protocol that allows two parties to establish a shared secret key used by encryption and hash algorithms (for example, DES and MD5) over an insecure communications channel

In the example in the figure, there are four IPSec framework squares to be filled. When configuring security services to be provided by an IPSec gateway, first, an IPSec protocol must be chosen. The choices are ESP or ESP with AH. The second square is an encryption algorithm. Choose the encryption algorithm appropriate for the level of security desired: DES or 3DES. The third square is Authentication. Choose an authentication algorithm to provide data integrity: MD5 or SHA. The last square is the DH algorithm group. Choose which group to use: DH1 or DH2. IPSec provides the framework, and the administrator chooses the algorithms used to implement the security services within that framework.

# How IPSec Works

This topic details the individual steps of IPSec.
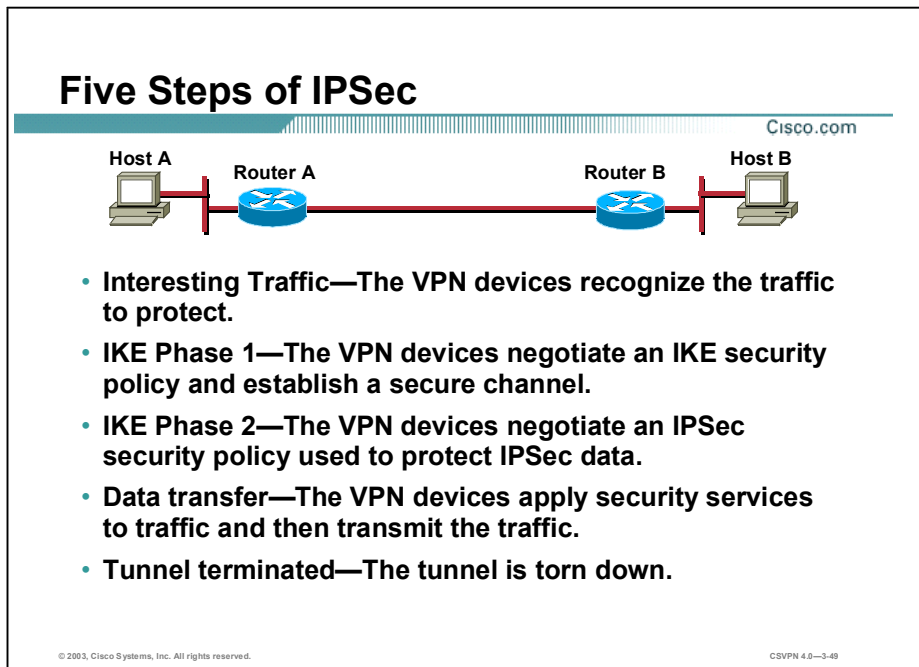


The goal of IPSec is to protect the desired data with the needed security services. IPSec's operation can be broken down into five primary steps:

**Step 1**   Interesting traffic—Traffic is deemed interesting when the VPN device recognizes that the traffic you want to send needs to be protected.

**Step 2**   IKE Phase 1—Between peers, a basic set of security services are negotiated and agreed upon. This basic set of security services protects all subsequent communications between the peers.

**Step 3**   IKE Phase 2—IKE negotiates IPSec Security Associations (SAs) parameters and sets up matching IPSec SAs in the peers. These security parameters are used to protect data and messages exchanged between endpoints. The final result of IKE phase 1 and 2 is a secure communications channel between peers.

**Step 4**   Data transfer—Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

**Step 5**   IPSec tunnel termination—IPSec SAs terminate through deletion or by timing out.

## Step 1—Interesting Traffic

Cisco.com

Host A    Router A                    Router B    Host B

10.0.1.3                                          10.0.2.3

→ Apply IPSec

→ Bypass IPSec
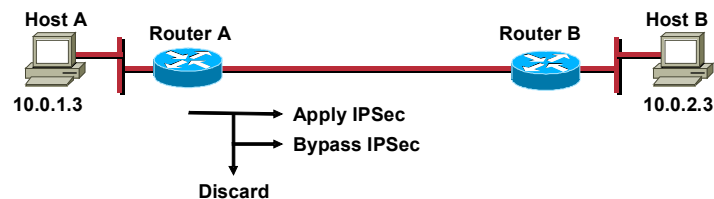
Discard

CSVPN 4.0—3-50

Determining what traffic needs to be protected is done as part of formulating a security policy for use of a VPN. The policy is used to determine what traffic needs to be protected and what traffic can be sent in the clear. For every inbound and outbound data gram, there are three choices: apply IPSec, bypass IPSec, or discard the data gram. For every data gram protected by IPSec, the system administrator must specify the security services applied to the data gram. The security policy database specifies the IPSec protocols, modes, and algorithms applied to the traffic. The services are then applied to traffic destined to each particular IPSec peer. With the VPN Client, you use menu windows to select connections that you want secured by IPSec. When interesting traffic transits the IPSec client, the client initiates the next step in the process: negotiating an IKE Phase 1 exchange.

## Step 2—IKE Phase 1

Host A    Router A                          Router B    Host B

10.0.1.3              IKE Phase 1:                  10.0.2.3
                      main mode exchange

Negotiate the                      Negotiate the
policy                             policy

DH exchange                        DH exchange

Verify the peer                    Verify the peer
identity                           identity
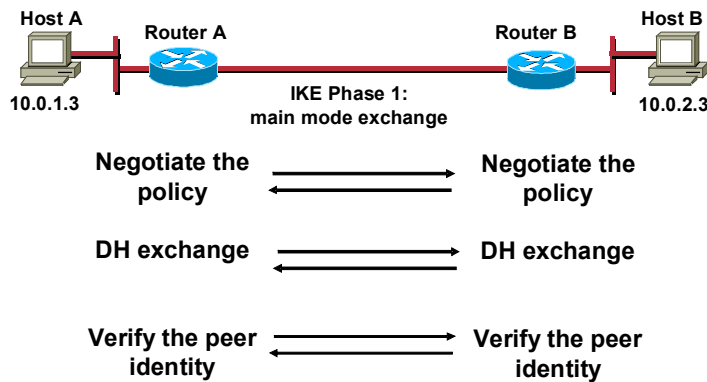
The basic purpose of Internet Key Exchange (IKE) Phase 1 is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. IKE Phase 1 occurs in two modes: main mode and aggressive mode.

Main mode has three two-way exchanges between the initiator and receiver:

■ First exchange—The algorithms and hashes used to secure the IKE communications are negotiated.

■ Second exchange—Uses a DH exchange to generate shared secret keys.

■ Third exchange—Verifies the other side's identity.

In the aggressive mode, fewer exchanges are done and with fewer packets. On the first exchange, almost everything is squeezed in: the IKE policy set negotiation; the DH public key generation; a nonce, which the other party signs; and an identity packet, which can be used to verify their identity via a third party. The receiver sends everything back that is needed to complete the exchange. The only thing left is for the initiator to confirm the exchange. While aggressive mode is faster, it does not provide identity protection and is therefore not recommended.

**First and Second Exchange—IKE Policy Sets and Establishing a Shared Secret**

Cisco.com

Host A — Router A — Router B — Host B

10.0.1.3   Negotiate IKE proposals   10.0.2.3

Transform 10
DES
MD5
pre-share
DH1
lifetime

IKE policy sets

Transform 15
DES
MD5
pre-share
DH1
lifetime

Transform 20
3DES
SHA
pre-share
DH1
lifetime
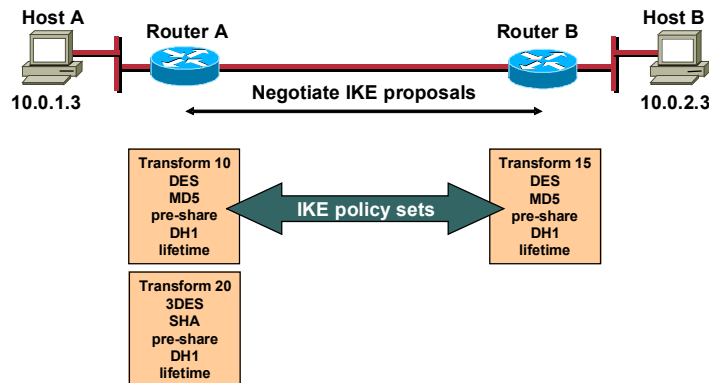
• Negotiates matching IKE transform sets to protect IKE exchange
• A DH exchange is performed to establish a shared secret

CSVPN 4.0—3-52

There are two exchanges: IKE policy sets and establishing a shared secret.

## First Exchange

During the first exchange the algorithms and hashes used to secure the IKE communications are negotiated and agreed upon between peers. When trying to make a secure connection between Host A and B through the Internet, Internet Key Exchange (IKE) security proposals are exchanged between Router A and B. The proposals identify the IPSec protocol being negotiated (for example, ESP). Under each proposal, the originator must delineate which algorithms are employed in the proposal (for example, DES with MD5). Rather than negotiate each algorithm individually, the algorithms are grouped into sets, an IKE policy set. A policy set delineates which encryption algorithm, authentication algorithm, mode, and key length are proposed. These IKE proposals and policy sets are exchanged during the IKE main mode first exchange phase. If a policy set match is found between peers, the main mode continues. If no match is found, the tunnel is torn down.

In the example in the figure, Router A sends IKE policy sets 10 and 20 to Router B. Router B compares its set, policy set 15, with those received from Router A. In this instance, there is a match: Router A's policy set 10 matches Router B's policy set 15.

In a point-to-point application, each end may only need a single IKE policy set defined. However, in a hub and spoke environment, the central site may require multiple IKE policy sets to satisfy all the remote peers.

## Second Exchange

Uses a DH exchange to generate shared secret keys and pass nonces, which are random numbers sent to the other party, signed, and returned to prove their identity. The shared secret key is used

to generate all the other encryption and authentication keys. When this step is completed, the peers have a common shared secret but the peers are not authenticated. This leads to the last step of IKE Phase 1, authenticating the peer's identity.

### Third Exchange—Authenticate Peer Identity

Cisco.com
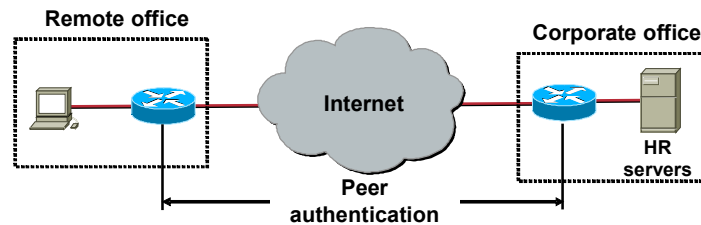
Remote office

Internet

Corporate office

HR servers

Peer authentication

**Peer authentication methods**
- **Pre-shared keys**
- **RSA signatures**
- **RSA encrypted nonces**

CSVPN 4.0—3-53

The third and last exchange is used to authenticate the remote peer. The primary outcome of main mode is a secure communication path for subsequent exchanges between the peers. Without proper authentication, it is possible to establish a secure communication channel with a hacker who is now stealing all your sensitive material. There are three data origin authentication methods:

■ Pre-shared keys—A secret key value entered into each peer manually used to authenticate the peer.

■ RSA signatures—Uses the exchange of digital certificates to authenticate the peers.

■ RSA encrypted nonces—Nonces (a random number generated by each peer) are encrypted and then exchanged between peers. The two nonces are used during peer authentication process.

# Step 3—IKE Phase 2

**Host A**

**Router A**

**Router B**

**Host B**

10.0.1.3

Negotiate IPSec
security parameters

10.0.2.3

The purpose of Internet Key Exchange (IKE) Phase 2 is to negotiate the IPSec security
parameters used to secure the IPSec tunnel. IKE Phase 2 performs the following functions:

■  Negotiates IPSec security parameters, IPSec transform sets

■  Establishes IPSec SAs

■  Periodically renegotiates IPSec SAs to ensure security

■  Optionally performs an additional DH exchange

IKE Phase 2 has one mode, called Quick mode. Quick mode occurs after IKE has established the
secure tunnel in Phase 1. It negotiates a shared IPSec transform, derives shared secret keying
material used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode
exchanges nonces that are used to generate new shared secret key material and prevent replay
attacks from generating bogus SAs.

Quick mode is also used to renegotiate a new IPSec SA when the IPSec SA lifetime expires.
Quick mode is used to refresh the keying material used to create the shared secret key based on
the keying material derived from the DH exchange in Phase 1.

IPSec Transform Sets

Host A  Router A                    Router B   Host B
10.0.1.3              Negotiate transform sets              10.0.2.3

Transform set 30                    Transform set 55
ESP                                 ESP
3DES          IPSec transform sets  3DES
SHA                                 SHA
Tunnel                              Tunnel
Lifetime                            Lifetime

Transform set 40
ESP                   • A transform set is a
DES                     combination of algorithms
MD5                     and protocols that enact a
Tunnel                  security policy for traffic.
Lifetime
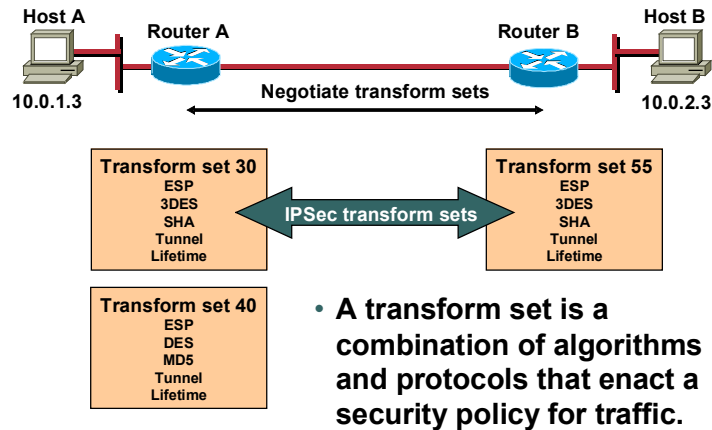
CSVPN 4.0—3-55

The ultimate goal of IKE Phase 2 is to establish a secure IPSec session between endpoints. Before that can happen, each pair of endpoints negotiates the level of security required (for example, encryption and authentication algorithms for the session). Rather than negotiate each protocol individually, the protocols are grouped into sets, an IPSec transform set. IPSec transform sets are exchanged between peers during Quick mode. If a match is found between sets, IPSec session-establishment continues. If no match is found, the session is torn down.

In the example in the figure, Router A sends IPSec transform set 30 and 40 to Router B. Router B compares its set, transform set 55, with those received from Router A. In this instance, there is a match. Router A's transform set 30 matches Router B's transform set 55. These encryption and authentication algorithms form an SA.

**SA**

Cisco.com

**SA**
**Security Policy Db**
- **Encryption Algorithm**
- **Authentication Algorithm**
- **Mode**
- **Key lifetime**

**SA Db**
- **Destination IP address**
- **SPI**
- **Protocol (ESP or AH)**

192.168.2.1
SPI–12
ESP/3DES/SHA
tunnel
28800

Internet

192.168.12.1
SPI–39
ESP/DES/MD5
tunnel
28800

CSVPN 4.0—3-56
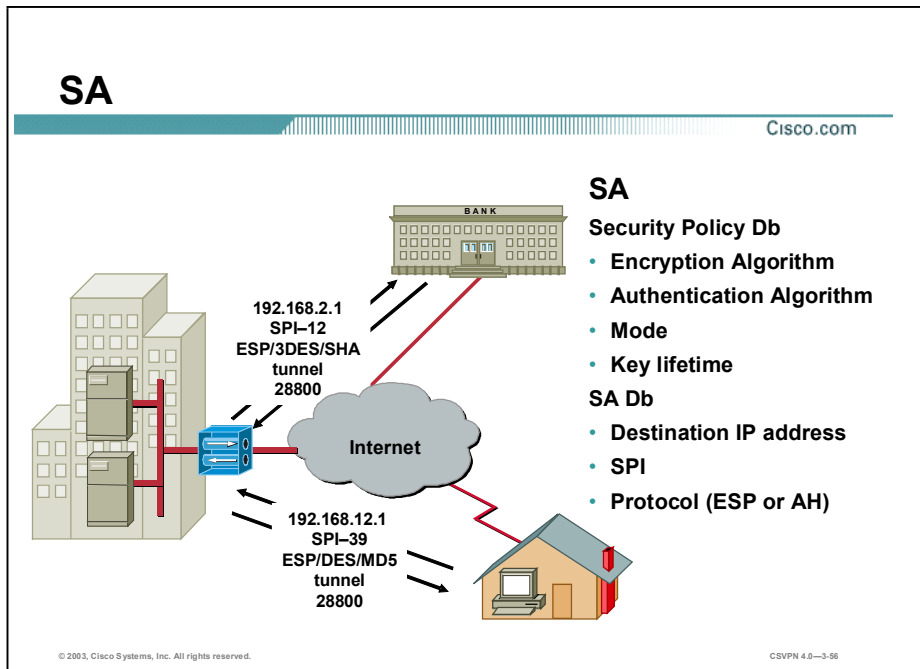
When the security services are agreed upon between peers, each VPN peer device enters the information in a Security Policy Database (SPD). The information includes the encryption and authentication algorithm, destination IP address, transport mode, key lifetime, and so on. This information is referred to as the SA. An SA is a one-way logical connection that provides security to all traffic traversing the connection. Because most traffic is bi-directional, two SAs are required: one for inbound and one for outbound traffic. The VPN device indexes the SA with a number, a Security Parameter Index (SPI). Rather than send the individual parameters of the SA across the tunnel, the source gateway, or host, inserts the SPI into the ESP header. When the IPSec peer receives the packet, it looks up the destination IP address, IPSec protocol, and SPI in its SA database (SAD), and then processes the packet according to the algorithms listed under the SPD.

The IPSec SA is a compilation of the SAD and SPD. SAD is used to identify the SA destination IP address, IPSec protocol, and SPI number. The SPD defines the security services applied to the SA, encryption and authentication algorithms, and mode and key lifetime. For example, in the corporate-to-bank connection, the security policy provides a very secure tunnel using 3DES, SHA, tunnel mode, and a key lifetime of 28800. The SAD value is 192.168.2.1, ESP, and SPI-12. For the remote user accessing e-mails, a less secure policy is negotiated using DES, MD5, tunnel mode, and a key lifetime of 28800. The SAD values are a destination IP address of 192.169.12.1, ESP, and an SPI-39.

## SA Lifetime

**Data-based**
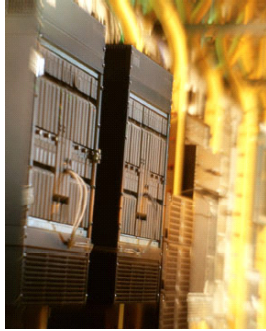
**Time-based**

CSVPN 4.0—3-57

Like passwords on your company PC, the longer you keep it, the more vulnerable it becomes. The same thing is true of keys and SAs. For good security, the SA and keys should be changed periodically. There are two parameters: lifetime type and duration. The first parameter is lifetime type. How is the lifetime measured? Is it measured by the number of bytes transmitted or the amount of time transpired? The second parameter is the unit of measure: kilobytes of data or seconds of time. Some examples are as follows: lifetime based on 10,000 kilobytes of data transmitted or 28800 seconds of time expired. The keys and SAs remain active until their lifetime expires or until some external event—the client drops the tunnel—causes them to be deleted.

## Step 4—IPSec Session

Cisco.com

Host A  Router A          Router B  Host B

IPSec session

- **SAs are exchanged between peers.**
- **The negotiated security services are applied to the traffic.**

CSVPN 4.0—3-58

After IKE Phase 2 is complete and Quick mode has established IPSec SAs, traffic is exchanged between Host A and B via a secure tunnel. Interesting traffic is encrypted and decrypted according to the security services specified in the IPSec SA.

**Step 5—Tunnel Termination**

Cisco.com

Host A    Router A                    Router B    Host B
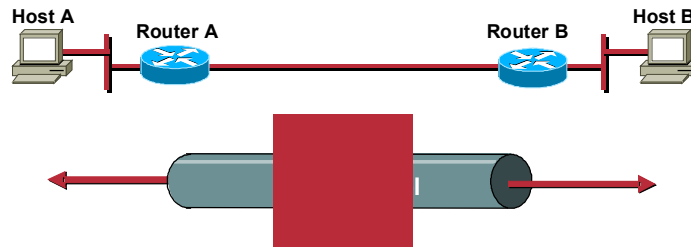
• **A tunnel is terminated**
  – **By an SA lifetime timeout**
  – **If the packet counter is exceeded**
• **Removes IPSec SA**

CSVPN 4.0—3-59

IPSec SAs terminate through deletion or by timing out. An SA can time out when a specified number of seconds has elapsed or when a specified number of bytes has passed through the tunnel. When the SAs terminate, the keys are also discarded. When subsequent IPSec SAs are needed for a flow, IKE performs a new Phase 2, and, if necessary, a new Phase 1 negotiation. A successful negotiation results in new SAs and new keys. New SAs are usually established before the existing SAs expire, so that a given flow can continue uninterrupted.

# Summary

This topic summarizes what you learned in this lesson.

## Summary

- **Cisco VPN components include Cisco VPN 3000 Series Concentrators, Cisco VPN routers, the PIX Firewall, and the Cisco VPN Client.**
- **Cisco supports the following IPSec standards: AH, ESP, DES, 3DES, AES, MD5, SHA, RSA signatures, IKE (also known as ISAKMP), DH, and CAs.**
- **There are five steps to IPSec: interesting traffic, IKE phase 1, IKE phase 2, IPSec encrypted traffic, and tunnel termination.**
- **IPSec SAs consist of a destination address, SPI, IPSec transform, mode, and SA lifetime value.**

CSVPN 4.0—3-61

**4**

# Cisco Virtual Private Network 3000 Concentrator Series Hardware Overview

## Overview

This lesson includes the following topics:

- Objectives

- Overview

- Models

- Benefits and features

- Client support

- Summary

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Describe the Cisco VPN 3000 Concentrator Series.**
- **Identify the Cisco VPN 3000 Concentrator Series models.**
- **Describe the Cisco VPN 3000 Concentrator Series features and functions.**

CSVPN 4.0—4-2

This lesson presents an overview of the Cisco Virtual Private Network (VPN) 3000 Concentrator Series. It describes the Cisco VPN 3000 Concentrator Series models, and details the major features and functions of the hardware.

# Overview

This topic presents an overview of the Cisco VPN 3000 Concentrator Series.
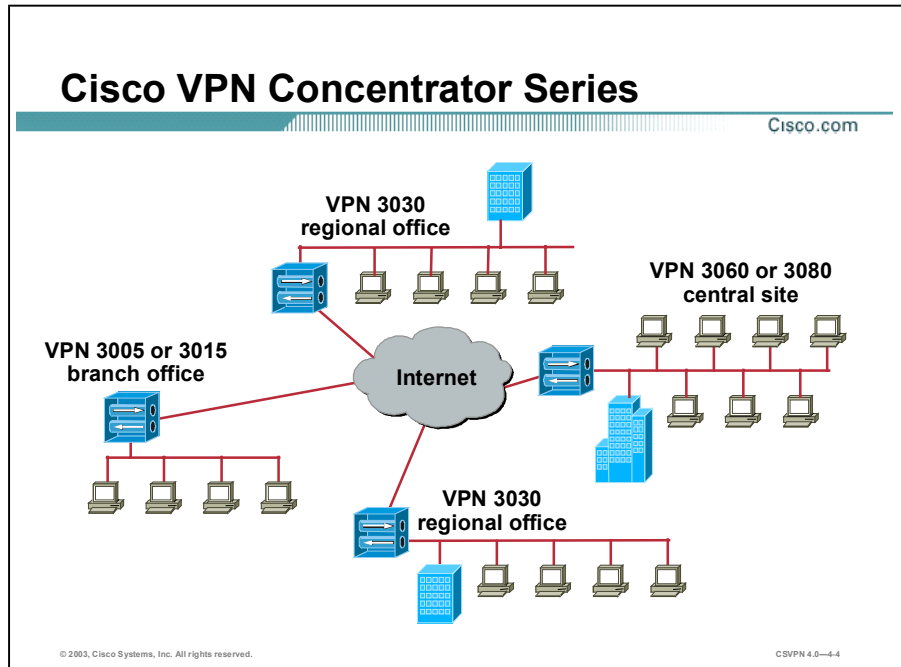


The Cisco VPN 3000 Concentrator Series consists of the following models:

■ 3005 and 3015

  — Appropriate for a small branch office

  — Supports up to 100 simultaneous sessions

■ 3030

  — Appropriate for a regional office

  — Supports up to 1,500 simultaneous sessions

■ 3060

  — Appropriate for a large central site

  — Supports up to 5,000 simultaneous sessions

■ 3080

— Appropriate for a large central site or ISP

— Supports up to 10,000 simultaneous sessions

**Product Hardware Portfolio**

Cisco.com

Cisco VPN 3000 Concentrator Series

The goal is to provide products that cover the entire spectrum of customer VPN applications, making Cisco the only choice for CPE and service providers of all sizes.
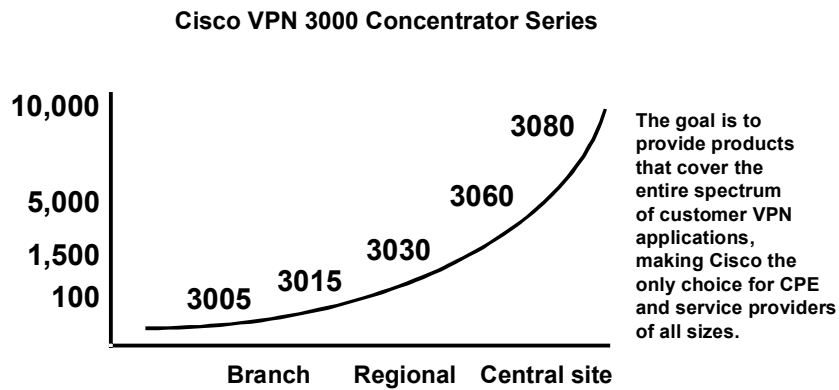
© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—4-5

The Cisco VPN 3000 Concentrator Series provides products that cover the entire spectrum of customer VPN applications. The following models are available:

■ 3005

— Supports software encryption

— Supports up to 100 simultaneous sessions

— Not upgradeable

■ 3015

— Supports software encryption

— Supports up to 100 simultaneous sessions

— Upgradeable

■ 3030

— Supports one Scalable Encryption Processor/SEP-Enhanced (SEP/SEP-E) hardware module

— Supports up to 1,500 simultaneous sessions

— Upgradeable

- 3060

    — Supports two SEP/SEP-E hardware modules

    — Supports up to 5,000 simultaneous sessions

    — Upgradeable

- 3080

    — Supports two SEP/SEP-E hardware modules

    — Supports up to 10,000 simultaneous sessions

    — Not upgradeable

# Models

This topic presents an overview of the Cisco VPN 3000 Concentrator Series models.
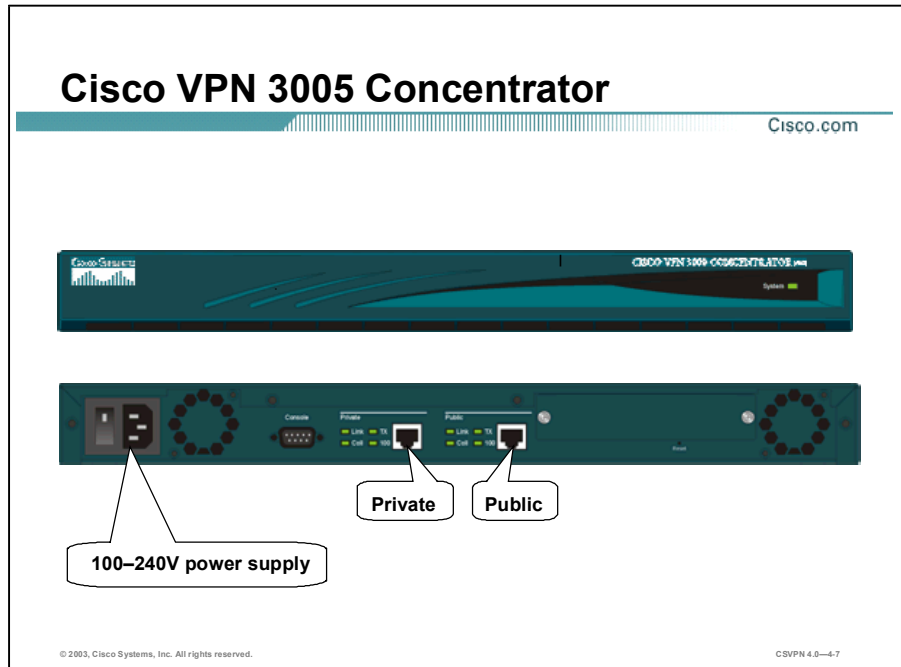
The following hardware features are supported on the Cisco VPN 3005 Concentrator:

■ Height—1U

■ Memory—32 MB SRAM, which is standard

■ Encryption—Software-based

  — Data Encryption Standard (DES)

  — 3DES

  — Advanced Encryption Standard (AES)

■ Scalability—Up to 100 simultaneous sessions

■ Network interface

  — Two auto-sensing, full duplex 10/100BaseT Ethernet interfaces.

  — The public interface connects to the Internet.

&mdash; The private interface connects to the private corporate network.

■ Power supply—AC operates at 100–240V and 50/60 Hz with universal power factor correction

■ Hardware—Not upgradeable

■ Software—Upgradeable

## Cisco VPN 3015 Concentrator

Cisco.com

SEP/SEP-E module slots

100–240V power supplies load sharing

Private

Public

External

CSVPN 4.0—4-8
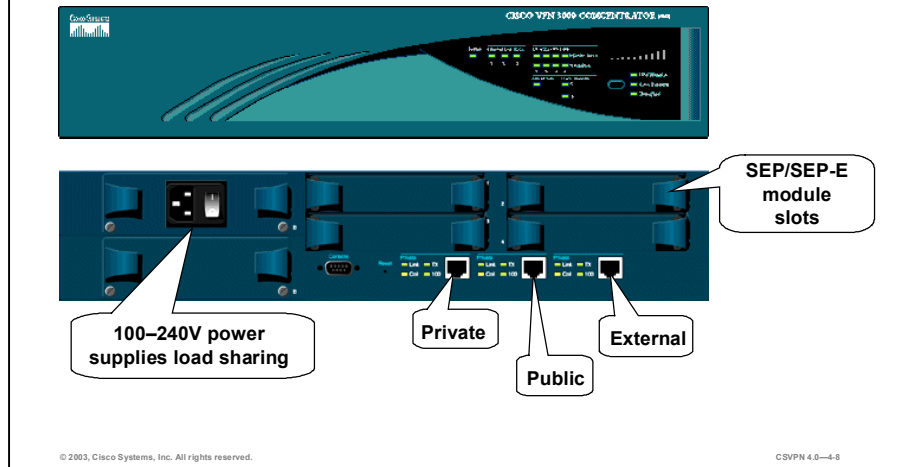
The following hardware features are supported on the Cisco VPN 3015 Concentrator:

- Memory—64 MB SRAM, which is the standard

- Encryption—Software-based

  — DES, 3DES, and AES encryption

- Scalability—Up to 100 simultaneous remote connections

- Network interface

  — Three auto-sensing, full duplex 10/100BaseT Ethernet interfaces.

  — The public interface connects to the Internet.

  — The private interface connects to the private corporate network.

  — The external interface connects to the DMZ.

- Power supply

  — AC operates at 100–240V and 50/60 Hz with universal power factor correction

  — Replaceable power supply

- Upgradeable

**Cisco VPN 3030 Concentrator**
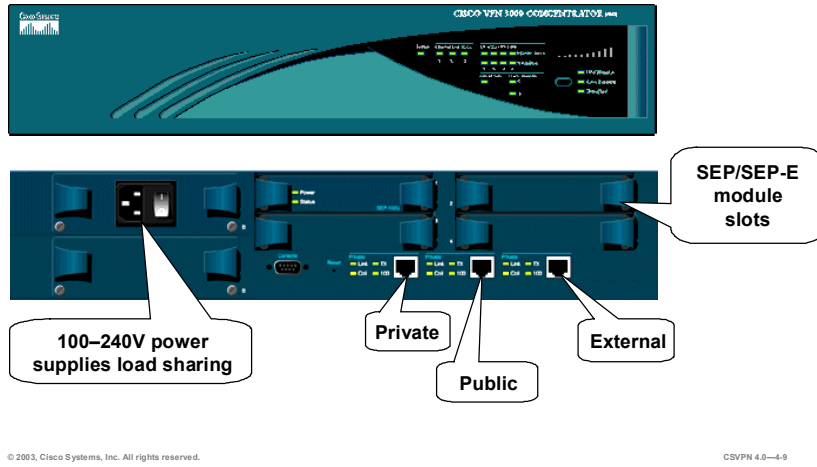
The following hardware features are supported on the Cisco VPN 3030 Concentrator:

- Memory—128 MB SRAM, which is the standard

- Encryption

  — Hardware-based encryption

    - SEP/SEP-E encryption module

    - Programmable Digital Signal Processor (DSP)-based security accelerator

    - DES, 3DES, and AES encryption

  — Software-based—AES 128, AES 192, and AES 256 encryption

- Scalability

  — Equipped with one SEP/SEP-E module

  — Up to 1,500 simultaneous remote connections

- Network interface

  — Three auto-sensing, full duplex 10/100BaseT Ethernet interfaces.

  — The public interface connects to the Internet.

- — The private interface connects to the private corporate network.

- — The external interface connects to the DMZ.

- ■ Power supply

  - — AC operates at 100–240V and 50/60 Hz with universal power factor correction

  - — Replaceable power supply

  - — Hot-swappable with optional redundant power supply

- ■ Upgradeable

## Cisco VPN 3060 Concentrator
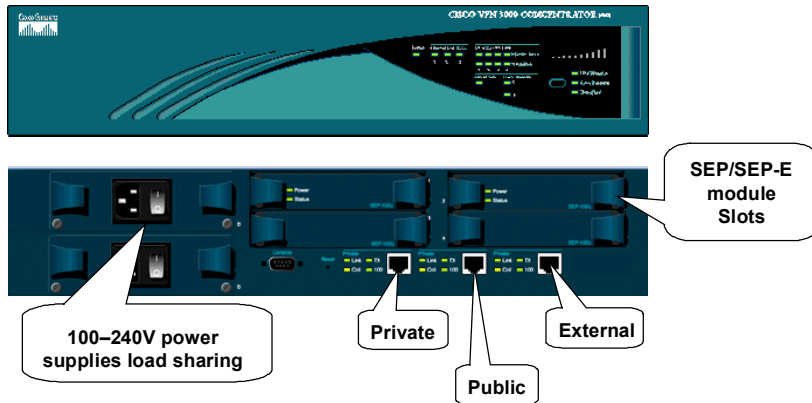
The following hardware features are supported on the Cisco VPN 3060 Concentrator:

■ Memory

— 256 MB SRAM, which is the standard

— 512 MB SRAM, upgradable

| | |
|---|---|
| **Note** | To take advantage additional memory, you must update the VPN Concentrator Manager to version 4.0, and update the VPN Concentrator Bootcode to version 4.0. |

■ Encryption

— Hardware-based encryption

■ SEP/SEP-E encryption module

■ Programmable, DSP-based security accelerator

■ DES, 3DES, and AES encryption

— Software-based encryption—AES 128, AES 192, and AES 256

■ Scalability

— Equipped with a total of two SEP/SEP-E modules

- — Up to 5000 simultaneous remote connections

- ■ Network interface

  - — Three auto-sensing, full duplex 10/100BaseT Ethernet interfaces.

  - — The public interface connects to the Internet.

  - — The private interface connects to the private corporate network.

  - — The external interface connects to the DMZ.

- ■ Power supply

  - — AC operates at 100–240V and 50/60 Hz with universal power factor correction

  - — Standard hot-swappable, redundant power supply

- ■ Upgradeable

**Cisco VPN 3080 Concentrator**

Cisco.com

SEP/SEP-E module slots

100–240V power supplies load sharing

Private

Public

External
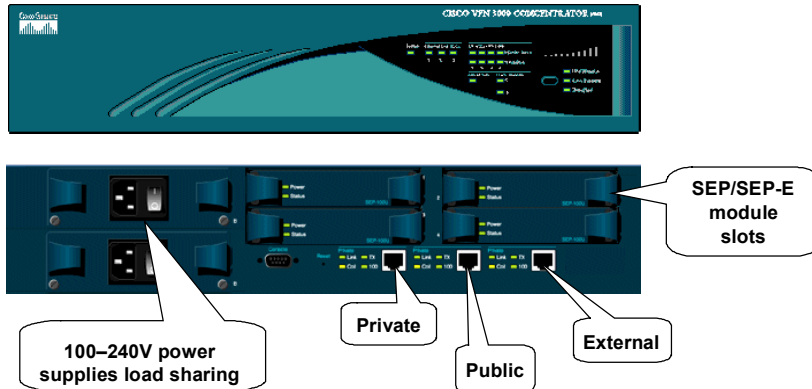
CSVPN 4.0—4-11

The following hardware features are supported on the Cisco VPN 3080 Concentrator:

- Memory

    - 256 MB SRAM, which is the standard

    - 512 MB, upgradeable

| Note | To take advantage of additional memory, you must update the VPN Concentrator Manager to version 4.0, and update the VPN Concentrator Bootcode to version 4.0. |
|------|------|

- Encryption

    - Hardware-based encryption

        - SEP/SEP-E encryption module

        - Programmable, DSP-based security accelerator

        - DES, 3DES, and AES encryption

    - Software-based encryption—AES 128, AES 192, and AES 256

- Scalability

    - Equipped with two active and two inactive SEP/SEP-E modules

- — Up to 10,000 simultaneous remote connections

- ■ Network interface

  - — Three auto-sensing, full duplex 10/100BaseT Ethernet interfaces.

  - — The public interface connects to the Internet.

  - — The private interface connects to the private corporate network.

  - — The external interface connects to the DMZ.

- ■ Power supply

  - — AC operates at 100–240V and 50/60 Hz with universal power factor correction

  - — Standard hot-swappable, redundant power supply

- ■ Migration to 3080—Factory upgrade

## Front LEDs

System    Ethernet Link Status    Expansion Modules

Insertion Status

1  2  3    Run Status

1  2  3  4

Fan Status    Power Supplies

CPU Utilization

A    Active Sessions

B    Throughput
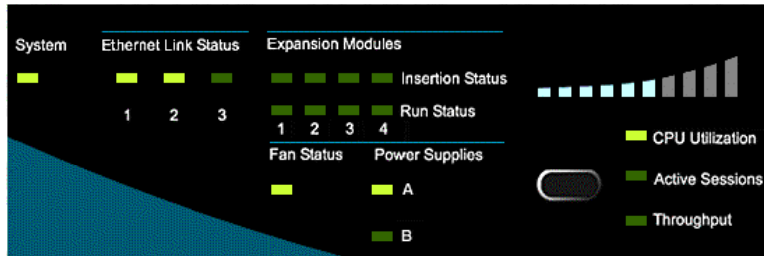
CSVPN 4.0—4-12

The following are the LEDs found on the front of the Concentrator:

| LED Indicator | Green | Amber | Off |
|---|---|---|---|
| System | Power on; normal | System has crashed and halted | Power off; all LEDs are off |
| Ethernet Link Status 1 2 3 | Steady light = Connected to the network and enabled<br><br>Blinking light = Connected and configured, but disabled | NA | Not connected to the network or not enabled |
| Expansion Modules Insertion Status | The SEP/SEP-E module is installed. | NA | SEP/SEP-E not installed in system |
| Expansion Module Run Status | The SEP/SEP-E module is operational. | NA | If installed, SEP/SEP-E failed diagnostics or the encryption is not running |
| Fan Status | Operating normally | Not running or below normal revolutions per minute (RPM) | NA |
| Power Supplies A B | Installed and operating normally | Voltage outside of normal range | Not installed |
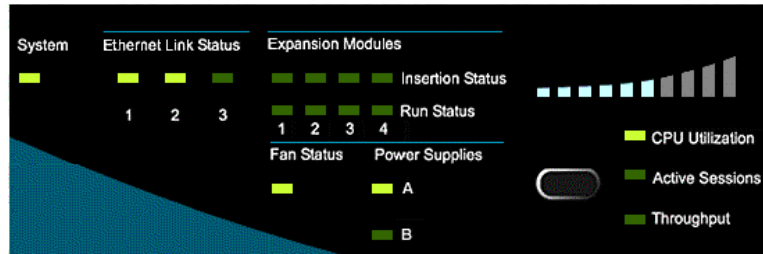
The following are additional LEDs found on the front of the Concentrator:

| LED Indicator | Green | Amber | Off |
| --- | --- | --- | --- |
| CPU Utilization | A statistic is selected for display. | NA | Not selected |
| Active Sessions | A statistic is selected for display. | NA | Not selected |
| Throughput | A statistic is selected for display. | NA | Not selected |

**Rear LEDs**

CSVPN 4.0—4-14

The following are the LEDs for the Ethernet interfaces found on the back of the Concentrator:

| LED Indicator | Green | Amber | Off |
|---|---|---|---|
| Link | Carrier detected; normal | NA | No carrier detected; error |
| Tx | Transmitting data; normal | NA | Not transmitting data; idle |
| Coll | NA | Data collisions are detected | No collisions; normal |
| 100 | The speed is set to 100 Mbps. | NA | The speed is set to 10 Mbps. |

The following are the LEDs for the SEP/SEP-E modules found on the back of the Concentrator:

| LED Indicator | Green | Amber | Off |
|---|---|---|---|
| Power | Power on; normal | NA | Power off; error |
| Status | The Encryption code is running. | NA | The module failed; diagnostics or the encryption code is not running. |

## Back Panel

SEP/SEP-E module slots

100–240V power supplies load sharing

Private

Public

External

Console
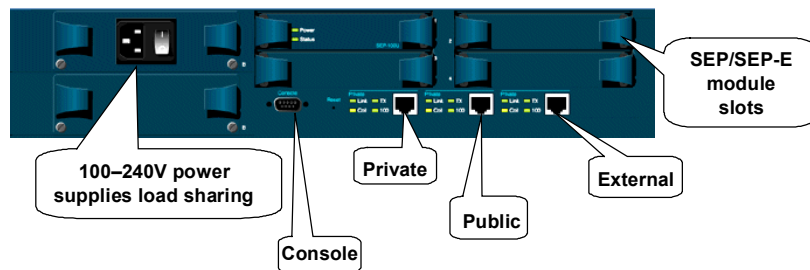
The back panel of the Concentrator has the following interfaces and features:

- Power supply

    — Replaceable power supply modules

    — AC operates at 100–240V and 50/60 Hz with universal power factor correction

    — Hot-swappable with redundant power supplies

- Network interface

    — Three auto-sensing, full duplex, 10/100BaseT Ethernet interfaces

    — The public interface connects to the Internet

    — The private interface connects to the private corporate network

    — The external interface connects to the DMZ

- Console port

    — Changes to its default setting of 9600 8N1

    — Used for the CLI

## Concentrator Product Comparison

| Feature | 3005 | 3015 | 3030 | 3060 | 3080 |
|---|---|---|---|---|---|
| Height | 1U | 2U | 2U | 2U | 2U |
| Performance | 4M | 4M | 50M | 100M | 100M |
| Simultaneous Users | 100 | 100 | 1500 | 5000 | 10000 |
| Site-to-Site Tunnels | 100 | 100 | 500 | 1000 | 1000 |
| Encryption | SW | SW | HW | HW | HW |
| Memory | 32M | 64M | 128M | 256M | 256M |
| Power Supplies | 1 | Up to 2 | Up to 2 | Up to 2 | 2 |
| SEP/SEP-E Modules | 0 | 0 | 1 | 2 | 4 |
| Upgradeable | N | Y | Y | Y | N |

CSVPN 4.0—4-16

The table can be used to determine which model is best for your environment. The top row lists the five models in the Concentrator family. The left column lists some of the Concentrator's features.
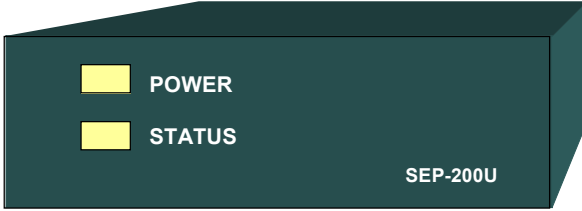
| Note | For planning purposes, a simultaneous user is considered to be a remote access VPN user connected in all tunneling modes. A session includes 1 (Internet Key Exchange) IKE Security Association (SA) and 2 unidirectional Internet Protocol Security (IPSec) SAs. For environments with rekeying or split tunneling, using a VPN remote access load-balancing environment with spare capacity is recommended since these particular sessions will utilize additional system resources that otherwise would be used to support additional users. In mixed environments where a Concentrator must support both remote access and site-to-site tunnels, the site-to-site tunnel count is subtracted from the overall simultaneous user capability. For example, a 3060, which has 50 site-to-site tunnels, cannot exceed 4950 remote access sessions. |
|---|---|

# Benefits and Features

This topic discusses the benefits and features of the Cisco VPN 3000 Concentrator Series.



**SEP/SEP-E**

Cisco.com

POWER

STATUS

SEP-200U

**DSP-based hardware encryption—1,500 to 5,000 simultaneous sessions**

- **SEP—Provides DES and 3DES hardware-based encryption**
- **SEP-E—Provides DES, 3DES, and AES hardware-based encryption**

CSVPN 4.0—4-18

The Scalable Encryption Processor (SEP/SEP-E) hardware-based encryption module enables you to offload processor-intensive DES, 3DES, and AES encryption tasks to hardware. The following features are supported:

■ DSP-based hardware encryption

— SEP/SEP-E is based on the Analog Devices DSP encryption engine.

— Encryption or decryption is offloaded to DSP-based hardware.

— DSP can be reprogrammed as existing standards change and new standards emerge.

■ SEP—DES and 3DES hardware-based encryption

■ SEP-E—DES, 3DES, and AES hardware-based encryption

■ Performance—Able to support up to 100 Mbps of encrypted throughput at wire speed

■ Sessions

— 3005 and 3015—Provides 100 simultaneous sessions using software-based encryption

— 3030—Provides 1,500 simultaneous sessions with one SEP/SEP-E module

— 3060—Provides 5,000 simultaneous sessions with two SEP/SEP-E modules

— 3080—Provides 10,000 simultaneous sessions with two SEP/SEP-E modules and an upgraded Concentrator chassis

---

| Note | The Concentrator uses either SEP or SEP-E modules, not both. Do not install both on the same device. If you install an SEP-E module on a Concentrator that already contains an SEP module, the Concentrator disables the SEP module and uses only the SEP-E module. |
|------|---|

---

## SEP/SEP-E Redundancy

Cisco.com

SEP/SEP-E redundancy

SEP/SEP-E redundancy

Failover
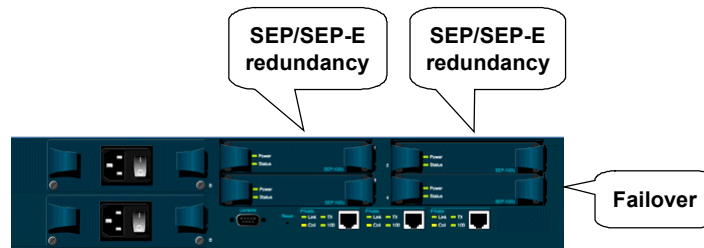
**Redundancy**

- **Top-to-bottom**
- **Side-to-side**

CSVPN 4.0—4-19

The Concentrator can contain up to four Scalable Encryption Processor (SEP/SEP-E) modules for maximum system throughput and redundancy. Two SEP/SEP-E modules are online while the other two SEP/SEP-E modules are hot-running spares. These additional modules provide redundancy in case of module failure.

SEP/SEP-E redundancy requires no configuration. It is always enabled and completely automatic; no operator intervention is required.

Redundancy is from top to bottom, which is referred to as a column. If the top SEP/SEP-E fails, the bottom SEP/SEP-E takes over. The Concentrator automatically switches all the active sessions to the redundant SEP/SEP-E. No sessions are lost.

If both SEP/SEP-Es in a column fail, the sessions are handled by the SEP/SEP-Es in the other column. In this scenario, sessions will be lost. The users need to re-establish their sessions.

**Concentrator Redundancy VRRP**

Cisco.com

Master

Slave

Server   Private   Public
         network   network

Internet
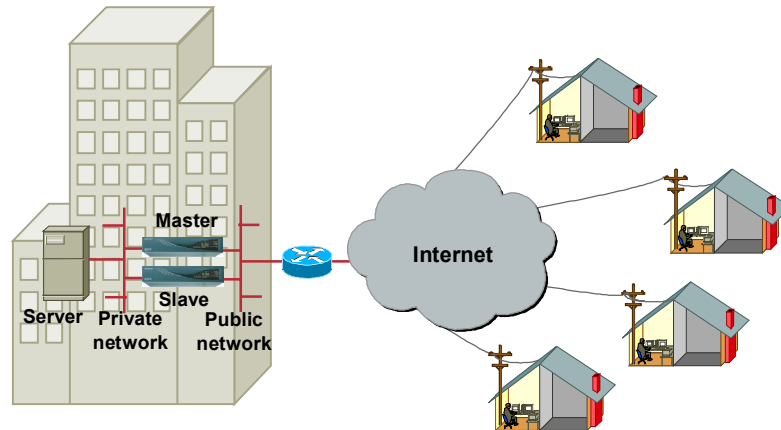
CSVPN 4.0—4-20

Concentrator redundancy applies only to installations where two or more Concentrators are in parallel. The public interfaces of all Concentrators are located on a common LAN. All private interfaces of all Concentrators are located on a different common LAN. Virtual Router Redundancy Protocol (VRRP) manages automatic switchover from one Concentrator to another in a redundant installation. Automatic switchover provides you access to the VPN even if one Concentrator is out of service for some reason (for example, system crash, power failure, physical interface failure, system shutdown, or reboot).

One Concentrator is the master system, and the others are backup systems. A backup system acts as a virtual master system when a switchover occurs. For IPSec LAN-to-LAN connections, switchover is fully automatic. A new tunnel is re-established automatically. No further action is required.

For IPSec and Point-to-Point Tunneling Protocol (PPTP) client-to-LAN connections, you are disconnected from the failing system. You are notified of the disruption and can reconnect without changing any connection parameters.

Switchover typically occurs within three to ten seconds. Switch back can be performed manually at a time that is convenient for the administrator.

## Concentrator Backup LAN-to-LAN

Cisco.com

**Remote Site**

**Central Site**
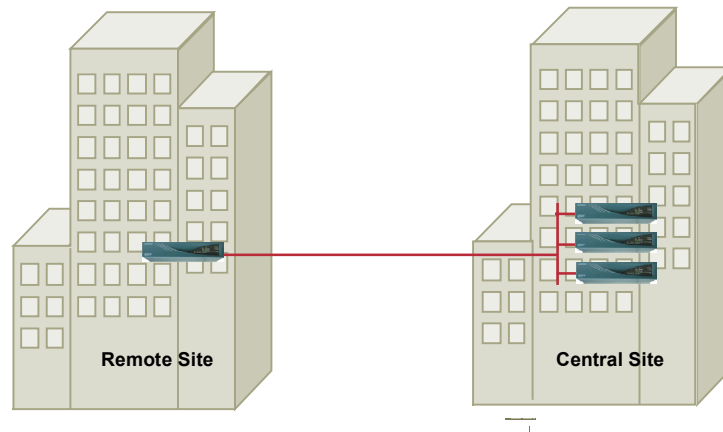
CSVPN 4.0—4-21

The Backup LAN-to-LAN feature lets you establish redundancy for your LAN-to-LAN connection. Unlike VRRP, which provides a failover for the Concentrator, Backup LAN-to-LAN provides a failover for the connection itself. Although VRRP and Backup LAN-to-LAN each provide ways of establishing continuity of service if a Concentrator fails, the Backup LAN-to-LAN feature provides certain advantages over VRRP as follows:

■ You can configure Backup LAN-to-LAN and load balancing on the same device, but you cannot configure VRRP and load balancing on the same Concentrator.

■ Redundant Backup LAN-to-LAN peers do not have to be located at the same site. VRRP backup peers cannot be geographically dispersed.

| Note | The Backup LAN-to-LAN feature does not work in conjunction with VRRP. If you set up a Backup LAN-to-LAN configuration, disable VRRP. |

## Load Balancing

Cisco.com
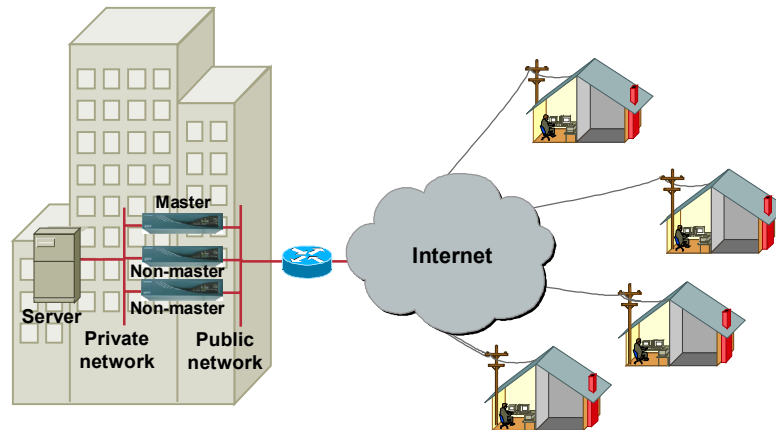
Load balancing distributes the connection load across multiple Concentrators. Rather than loading up one Concentrator at a time, load balancing spreads the connection across multiple Concentrators. In this way, individual LAN ports are used less. Each CPU is also less used, so latency and response time improves. It scales to a large number of Concentrators with no additional impact on performance. It also provides a high degree of resiliency to remote users; failure of a Concentrator does not cause a system to collapse.

Load Balancing consists of three parts:

■ Cluster—A group of Concentrators working together as a single entity. The cluster is known by one IP address to the outside client space. This virtual IP address is not tied to a specific physical device in the VPN cluster but is serviced by the cluster virtual master. The virtual IP address is a valid routable address.

■ Client—The basic strategy allows clients to initiate a connection to a known address, also known as a virtual IP address. The cluster always accepts the connection. During the second message of the IKE exchange, the cluster virtual master sends back to the client a secure, redirect notify message with the address of the least-loaded Concentrator. The client restarts IKE phase 1 with the new specified address, which is the public interface of the least-loaded Concentrator. Load balancing is performed on active sessions at connection time.

■ Load—The virtual cluster master maintains load information from all other non-masters. Each non-master sends load information in the "Keep Alive" message exchange to the master. The load is calculated as a percentage of current active sessions divided by the configured maximum allowed connections. The administrator can limit the number of connections in a Concentrator.

| **Note** | The Concentrator can perform only VRRP or load balancing, not both. |

# Client Support

This topic covers the broad client support of the Cisco VPN 3000 Concentrator Series.
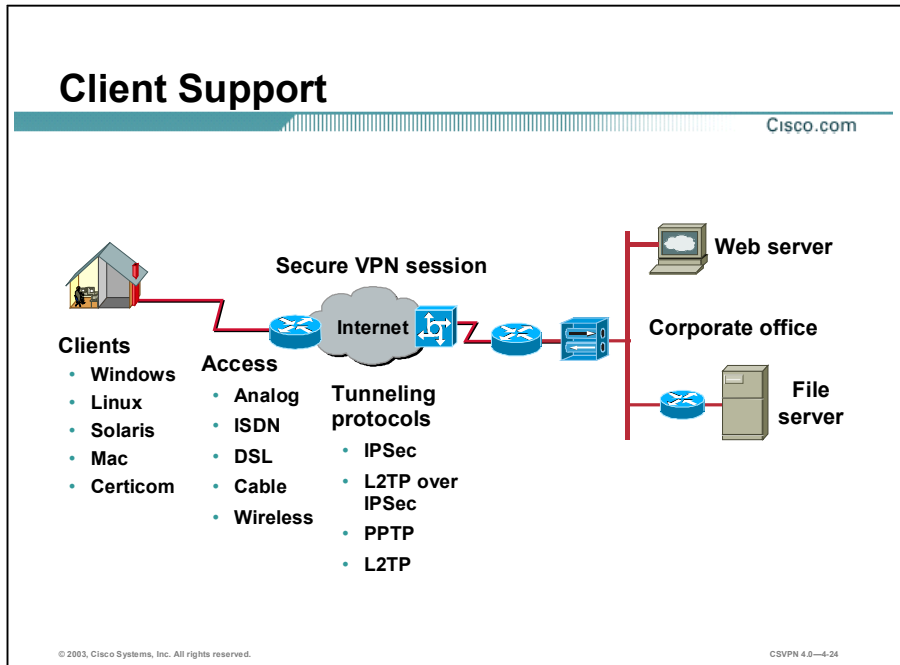


Another feature of the Cisco VPN 3000 Concentrator Series is the broad client support. The following clients and protocols are supported by the Concentrator:

■ Broad client support

— Windows client

— Linux client

— Solaris client

— Mac client

— Certicom client

■ Tunneling protocols

— IPSec client

— PPTP client in Windows Dial-up Networking 1.3

- — L2TP over IPSec client in Windows 2000

- — L2TP

- ■ Access methods

  - — Analog

  - — ISDN

  - — DSL

  - — Cable

  - — Wireless

- ■ Unlimited Cisco VPN Client software licenses

## Cisco VPN Windows Software Client
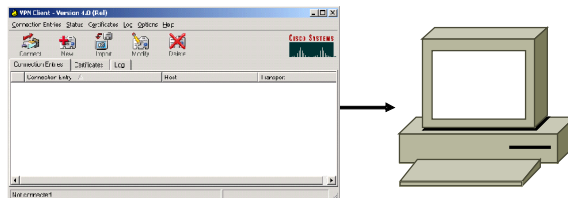
The following are system requirements for the Cisco VPN Client:

■ Operating System

— Microsoft Windows 98 or Windows 98 (second edition)

— Microsoft Windows NT 4.0—Running service pack 6 or higher

— Microsoft Windows ME

— Microsoft Windows 2000

— Microsoft Windows XP (Cisco VPN Client release 3.1 or higher)

■ Cisco VPN minimum sytem requirements

— Cisco VPN 3000 Series Concentrator (release 3.0)

— PIX Firewall (release 6.0)

— IOS 12.2(8)T

■ Hard disk space—50 MB

■ Memory

— 32 MB for Microsoft Windows 95 and 98

— 64 MB for Microsoft Windows NT

— 32–64 MB for Microsoft Windows ME

— 64 MB for Microsoft Windows 2000

— 128 MB for Microsoft Windows XP (256 MB, recommended)

# Cisco VPN Windows Client—
# Firewall Features

Cisco.com

**Are You There (AYT)?**

AYT answer

Internet

AYT

Yes

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

**Centralized Protection Policy (CPP)**

Push CPP

Internet

Push CPP

CSVPN 4.0—4-26
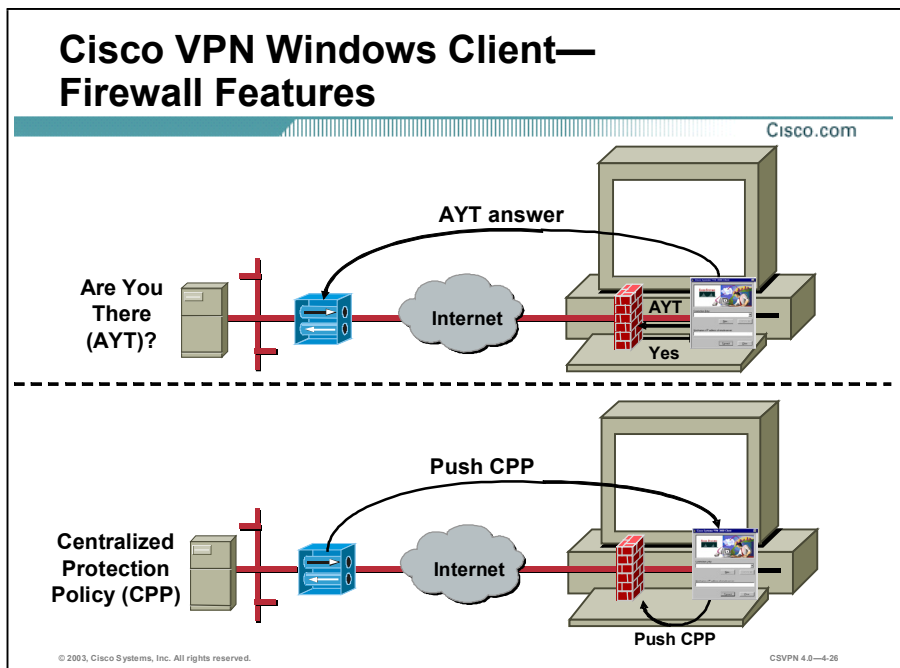
The Cisco VPN Windows client offers support for a firewall feature. The firewall feature is designed to enhance security for Microsoft Windows-based PCs running the release 3.5 and higher Cisco IPSec client. The feature is applied in one of three modes, are you there (AYT), stateful firewall (always on), and centralized protection policy (CPP):

■ AYT—For security reasons, a network administrator may require remote PCs to be running a firewall application before allowing VPN tunnels to be built. The "are you there" feature verifies the presence of a firewall and reports that information back to the concentrator. Depending on the PC's response, the Concentrator can permit or deny the PC's IPSec tunnel.

■ Stateful firewall (always on)—The stateful firewall module can only be enabled or disabled by the remote client. With this mode, a default policy is loaded on the firewall. The default firewall filter blocks all traffic inbound (to the client) that is not related to an outbound session (from the client). Once the user enables the stateful firewall, it is always on even when there are no established VPN tunnels.

■ CPP—Enables network administrators to define a set of rules (policies) to allow or drop traffic on connected VPN Clients. These policies are pushed from the concentrator to the Cisco VPN Windows Client at connection time. The VPN Client passes this policy to the firewall module on the client PC. The Concentrator can push policy to the Cisco Integrated Client (CIC) firewall and the Zonelabs, Zone Alarm and Zone Alarm-Pro, firewall applications. CPP is only enforced while the VPN Client is connected.

The Cisco VPN Windows Client firewall feature is discussed in a later lesson.

**Cisco VPN Windows Client—
Smartcard Support**

Internet
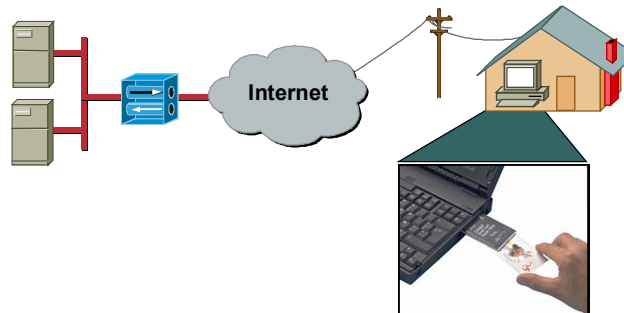
CSVPN 4.0—4-27

A Smartcard can be used to store information, such as a digital certificate. Unlike most digital certificates that are stored on a computer, with a Smartcard, you bring your authentication with you (the user, not just the computer, can be authenticated). To use a Smartcard, a user must have a Smartcard reader installed in their computer as well as driver software required to support the Smartcard reader. When a Smartcard is inserted in to the reader, the user must know a PIN in order to gain access to the card. Smartcards do not replace digital certificates; they act as a secure and portable storage mechanism for them. The Cisco VPN Windows Client supports Gemplus, Aladdin, and Activcard Smartcards.

## Cisco VPN Linux and Solaris Software Clients

CISCO.COM

**Cisco VPN Solaris and Linux client**
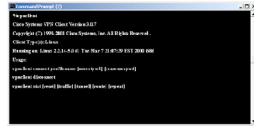
**Linux VPN client**

**Solaris VPN client**

CSVPN 4.0—4-28

The Cisco VPN software client was expanded to include Linux, Solaris, and Mac operating systems. The system requirements for Linux and Solaris client types are as follows:

■ Linux—Red Hat version 6.2 Linux (Intel), or compatible distribution, using kernel version 2.2.12 or later

— Connection type—Point-to-Point Protocol (PPP) and Ethernet

— Tunneling Protocol—IPSec

— User Authentication—RADIUS, Rivest, Shamir, and Adleman (RSA) SecurID, NT Domain, VPN Internal user list, and Public Key Infrastructure (PKI) digital certificates

— VPN Client Administration—Command line only

— Hard disk space—50 MB

— Memory—32 MB

■ Solaris UltraSPARC—32-bit or 64-bit Solaris kernal operating system version 2.6 or later

— Connection type—PPP and Ethernet

— Tunneling Protocol—IPSec

— User Authentication—RADIUS, RSA SecurID, NT Domain, VPN internal user list, and PKI digital certificates

— VPN Client Administration—Command line only

— Hard disk space—50 MB

— Memory—32 MB

**Cisco VPN Mac OS X Software Client**

Cisco.com
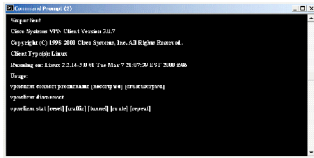
• **Cisco VPN Mac OS X Client**
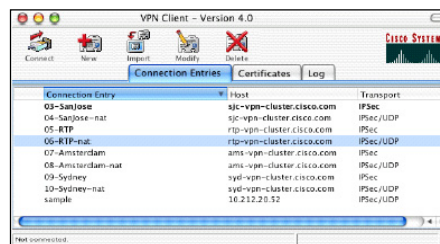
© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—4-29

The Cisco VPN Mac OS X Client supports both a command line interface (CLI) and a graphical user interface (GUI). The system requirements for the Mac OS X client are as follows:

■ Mac OS X version 10.1.0 or later

■ Connection type—Ethernet only

■ Tunneling Protocol—IPSec

■ User Authentication—RADIUS, RSA SecurID, NT Domain, VPN Internal user list, and PKI digital certificates

■ VPN Client Administration—GUI and CLI

■ Hard disk space—50 MB

The GUI enables the user to manage the VPN connections quickly and easily. The management functionality available from the GUI includes the following:

■ Certificate management

■ Profile management

■ Connection management

■ Log management

**Cisco VPN 3002 Hardware Client**

Cisco.com

VPN 3002        VPN 3002-8E

Power · Hardware reset · Console · Public · Private

Power · Hardware reset · Console · Public · Private

CSVPN 4.0—4-30
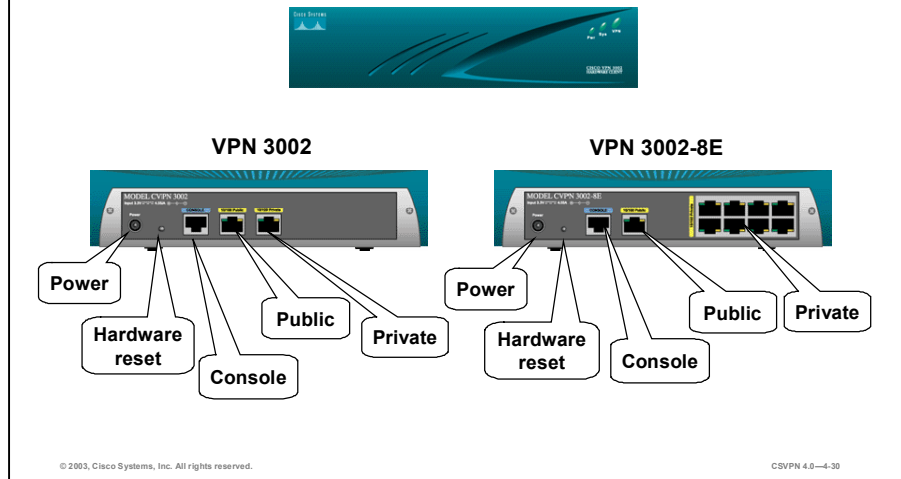
The Cisco VPN 3002 Hardware Client has the Client software built into it, enabling the Hardware Client to emulate the Cisco VPN 3000 Software Client. With the Hardware Client, you can plug remote site PCs into the Hardware Client, instead of having to load the Cisco VPN Client, or additional applications on remote site PCs.

There are two versions of the Hardware Client:

■ 3002—One private and one public interface

■ 3002-8E

— One public interface, and the private interface is a built-in 8 port 10/100BaseT Ethernet switch (switch is locked in, not configurable)

— Auto MDIX, which eliminates crossover cables

There are two modes of operation for the Hardware Client: client mode and network extension. These modes are configurable via the CLI or GUI. They can be remotely managed via IPSec tunnel or secure shell (SSH).

LEAP (Lightweight Extensible Authentication Protocol) Bypass lets LEAP packets from wireless devices behind a VPN 3002 travel across a VPN tunnel prior to individual user authentication, when enabled. This enables workstations using wireless access point devices establish LEAP authentication. Then they authenticate again per individual user authentication.

Administrators enable LEAP Bypass on a group basis at the central site, via a check box on the VPN Concentrator HW Client tab on the Group configuration page. Administrators can create a banner on the VPN 3000 Concentrator and push it to the VPN 3002. This gives organizations

the ability to provide information to users about their network, terms for use, liability, and other issues.

The Hardware Client is powered by an external power supply. It auto-senses the voltage, either 110V or 220V.

## Hardware Versus Software Client

**SOHO**

**Software client**

- **Used by a road warrior**
- **Loaded on the individual's PC**
- **Only supports an individual's device**
- **The tunnel is launched by a user.**

**Hardware client**

- **Small office or home office**
- **Built into hardware, (the end-user does not have to touch a PC)**
- **Supports multiple devices behind the hardware client**
- **The hardware client launches a tunnel automatically.**

CSVPN 4.0—4-31

You must decide which client to employ in the network, hardware, software, or both. Two fictitious companies are characterized to better explain the clients: Delicious Donuts and MetaRay System Engineers.

■ Delicious Donuts—If you have a customer who wants to take advantage of the savings of a VPN and they have 10,000 sites small office/home office (SOHO) within the US, you would want to choose the Hardware Client. The Software Client is built into the Hardware Client. Because it can be pre-configured and then sent to remote offices where it is plugged in, cabled to the local LAN, and ready to go. It supports multiple devices on the local LAN, and no applications have to be loaded to any of the local PCs. The Hardware Client is smart enough to launch a tunnel for any traffic bound for the corporate network.

■ MetaRay System Engineers—You have a company that has system engineers (road warriors) who need to call back to the home office while on the road. To do so, they would use the Software Client, because the system engineer loads the Software Client on the PC and launches it only when necessary. The Hardware Client is not feasible because the system engineer would need to use another piece of equipment.

**Certicom VPN Client Support**

Cisco.com

Internet

Tunnel

VPN 3000

Corporate network

Certicom IPSec
VPN Client
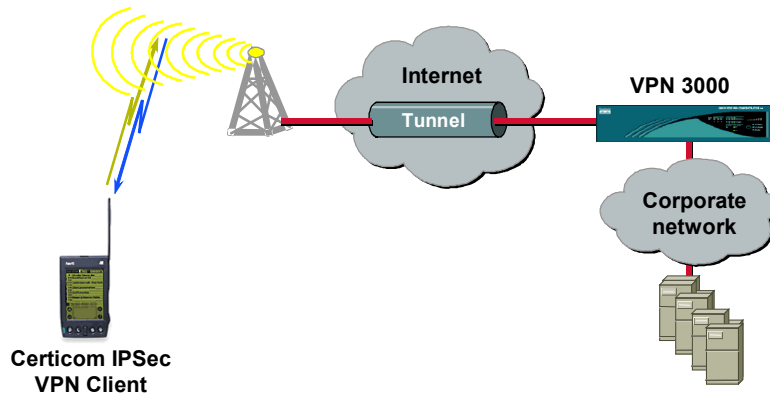
CSVPN 4.0—4-32

Certicom offers technology through the original equipment manufacturer (OEM) model, embedding security solutions in a wide variety of third-party products. They have implemented an IPSec client to run on cell phones, personal digital assistants (PDAs), and so on. When the devices perform standard IPSec, it is very CPU-intensive. Diffie-Hellman (DH) groups 1 and 2 take minutes to generate a key. Because of this, Certicom developed DH Group 7, Elliptic Curve Cryptography (ECC) support, to provide a key that can be generated in a short time (less than five seconds).

You must have the following to use Certicom VPN Client support:

■ Certicom VPN Client software

■ ECC (DH Group 7) protocol

■ Concentrator to terminate an IPSec client-to-LAN tunnel

However, the Certicom client does not support load balancing. Where load balancing requires the client to accept and interpret IKE redirect messages, the Certicom client does not support this functionality.

## Configuration Options
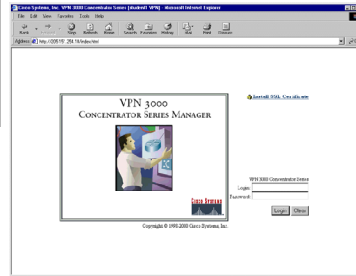
The Concentrator supports two configuration options: CLI and GUI. To use these options, they have to be configured correctly.

For the CLI configuration option, the terminal is set for the following:

■ Data bits = 8

■ Parity = N

■ Stop bits = 1

■ Speed = 9600

The web interface supports both HTTP and HTTP over secure socket layer (SSL). Operators can use either Internet Explorer or Netscape Navigator. With Internet Explorer and Netscape Navigator, the software revisions must be 4.0 or higher with both cookies and Java scripts enabled. Use either browser to configure the Concentrator with one exception—Internet Explorer must be used when programming digital certificates.

## Network Management Solutions

| Management Solution | Provisioning | SNMP | Software upgrade | Syslog |
|---|---|---|---|---|
| Cisco Info Center | | X | | X |
| Cisco View | | X | | |
| Cisco RME | | | X | X |
| Cisco VPN Monitor | | X | | |
| Cisco IP Solution Center | X | | | |

There are various Cisco network management options available to the administrator. The solutions include Simple Network Management Protocol (SNMP) monitoring, Syslog monitoring, and Cisco VPN 3000 Concentrator Series configuration. The solutions range from small to large networks and from general network to security specific management platforms. The following Cisco platforms can monitor and manage the Concentrator:

■ Cisco Info Center (CIC)—A service-level alarm monitoring and diagnostics tool that provides network fault and performance monitoring, network trouble isolation, and real-time service-level management for large networks. CIC is designed to help operators focus on important network events, offering a combination of alarm processing rules, filtering, customizable alarm viewing, and partitioning. CIC can support administrative VPNs among several Network Operations Centers (NOCs). In some networks, provincial or regional NOCs require a partial view of the network as a local network segment to facilitate local problem detection and resolution. Regional NOCs may also require a localized topological view of the local network portion. Global NOCs support regional NOCs from a central location and provide a view of the entire network and global fault monitoring. CIC focuses on fault monitoring.

■ CiscoView—A universal graphic device management application that provides real-time display and monitoring of Cisco routers, switches, hubs, concentrators, and access servers. Cisco View plugs into in third party SNMP management platforms such as HP OpenView, NetView, Whats Up Gold, and Snmpc. The Cisco View application supports graphical views of the chassis, device performance information, top ten lists, system summary, session summary (Active, Max, Total), and routing table of Cisco devices. Cisco View runs on NT and Solaris. Cisco View is a general management application.

- CiscoWorks VPN/Security Management Solution (VMS)—An integral part of the SAFE blueprint, combines web-based applications for configuring, monitoring and troubleshooting enterprise VPNs, firewalls, and network-based and host-based intrusion detection systems (IDS). VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small and large-scale VPN and security deployments. Typical devices managed include the following: PIX Firewalls, Cisco VPN 3000 Series Concentrators, 1700, 2600, 3600, 7100 and 7200 Series routers, Cisco IDS devices, Catalyst 6000 IDS Modules, and IDS for the Catalyst.

- CiscoWorks—Comprised of multiple software applications. Two of these applications are the Cisco VPN Monitor and the Cisco Resource Manager Essentials. The following provides more information on each of these software applications:

  - Cisco Resource Manager Essentials (RME)—A suite of web-based applications offering network management solutions for Cisco switches, access servers, routers, and Concentrators (NT & Solaris based). It supports the ability to collect detailed inventory, collect and report on SYSLOG messages, generate inventory reports (hardware, software, system info) and distribute software to all Concentrators in the network.

  - Cisco VPN Monitor—A web-based management tool that allows network administrators to collect, store, and view information on IPSec VPN connections for remote access or site-to-site VPN terminations. Cisco VPN Monitor manages VPNs that are configured on Cisco VPN 3000 Series Concentrators, VPN Series routers, and Cisco 7100, 1700, 2600, 3600 or 7200 Series routers. Operational status, performance, and security information can be viewed at a glance, providing status information on IPSec VPN implementations.

- Cisco IP Solution Center is an end-to-end network-management solution that scales as your organization evolves. As a unified service-management solution for Cisco routing, switching, and security products, the Cisco IP Solution Center manages the following:

  - VPNs based on Multiprotocol Label Switching (MPLS) Border Gateway Protocol (BGP), IPSec, ATM over MPLS, and Frame Relay over MPLS

  - Metro Ethernet services such as Ethernet Virtual Connection services (EVCS) transparent LAN services (TLS); and Ethernet to the home, building, or campus (ETTx)

  - MPLS traffic engineering and MPLS-based bandwidth protection solution

  - Security services such as IPSec VPNs, managed firewalls, and Network Address Translation (NAT)

# Summary

This topic summarizes the information you learned in this lesson.

## Summary

Cisco.com

- **There are five models in the Cisco VPN 3000 Concentrator Series: 3005, 3015, 3030, 3060, and 3080.**

- **The Cisco VPN 3000 Concentrator Series features include a scaleable encryption processor, strong encryption algorithms, broad client support, and broad access method support.**

CSVPN 4.0—4-36

**5**

# Configure the Cisco VPN 3000 Series Concentrator for Remote Access Using Pre-Shared Keys

## Overview

This lesson explains how to configure Cisco IOS IPSec using pre-shared keys for authentication. After presenting an overview of the process, the lesson shows you each major step of the configuration. It includes the following topics:

■  Objectives

■  Overview of remote access using pre-shared keys

■  Initial configuration of the Cisco VPN 3000 Series Concentrator for remote access

■  Browser configuration of the Cisco VPN 3000 Series Concentrator

■  Configuration of users and groups

■  In-depth configuration information

■  Configuration of the Cisco VPN Software Client for Windows

■  Summary

■  Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Configure the Cisco VPN 3000 Series Concentrator LAN interfaces via the CLI.**
- **Configure the Cisco VPN 3000 Series Concentrator Client-to-LAN application using the browser.**
- **Configure the IPSec Client.**
- **Monitor the IPSec Client-to-LAN tunnel.**

CSVPN 4.0—5-2

# Overview of Remote Access Using Pre-Shared Keys

This topic presents an overview of remote access using pre-shared keys.
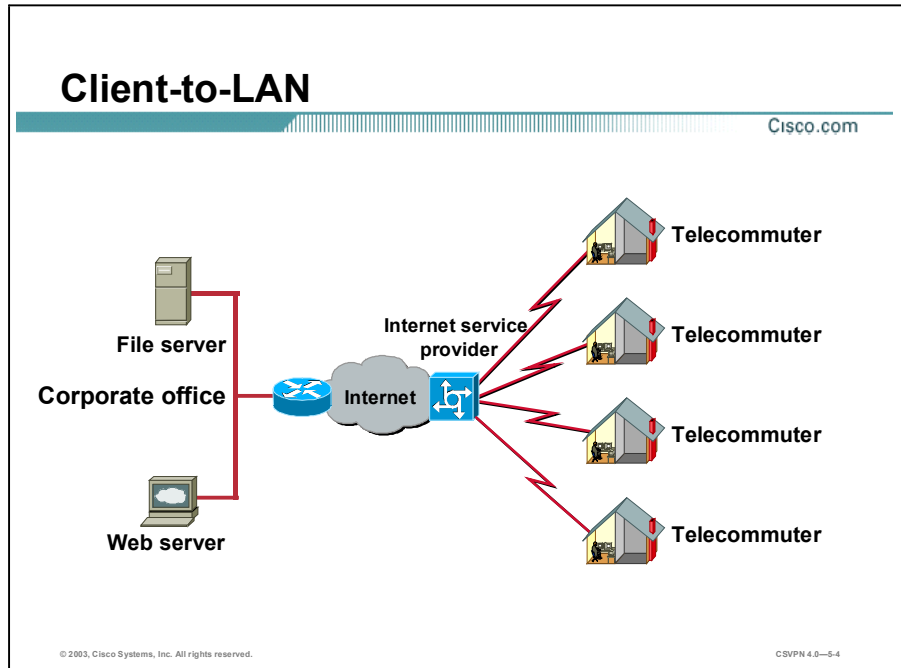


Consider the following scenario. Remote users need to dial into the corporate office and access e-mail, corporate presentations, order entry, and engineering. In addition, Corporate Information Services wants remote users to access corporate resources fast, inexpensively, and as securely as possible.

Implementing a remote-access virtual private network (VPN) with the Cisco VPN 3000 Series Concentrator and the Cisco VPN Software Client is the right choice. It enables remote users to access the corporate resources they require. Corporate Information Services meets their speed, expense, and security requirements.

IPSec Client-to-LAN Components

Cisco.com

Telecommuter
with the Cisco
VPN 3000 Series
Concentrator
Client

Application
server

Concentrator    ISP        ISP

Internet

PPP connectivity
Dial access

IPSec tunnel or session

• **Client software**

• **PPP**
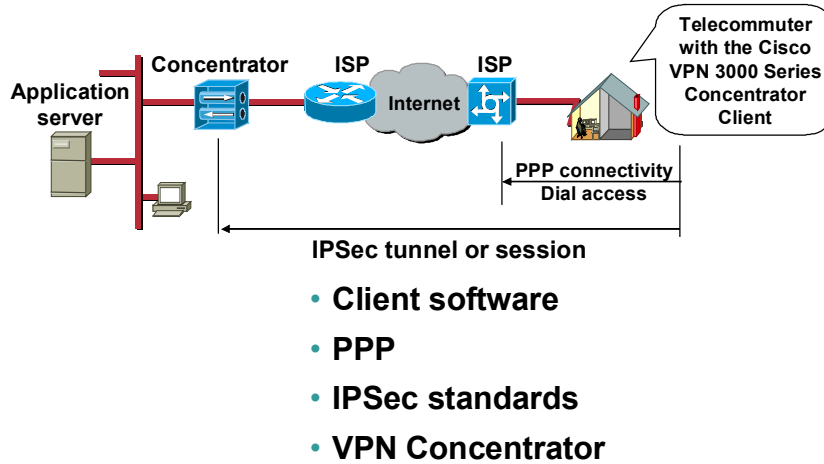
• **IPSec standards**

• **VPN Concentrator**

CSVPN 4.0—5-5

The Client-to-LAN VPN consists of four components: IPSec client software, Point-to-Point
Protocol (PPP), IPSec standards, and the Concentrator.

■  IPSec client software—The IPSec client software is not native to the Microsoft Windows
operating system and must be loaded on the PC. It is used to encrypt, authenticate, and
encapsulate data. It also terminates one end of the tunnel.

■  PPP—For remote access applications, the PC relies on PPP to establish a physical
connection to the local ISP or the Internet.

■  IPSec standards—After the ISP authenticates the remote user, the user launches the IPSec
client. IPSec establishes a secure tunnel or session through the Internet to the Concentrator.

■  Concentrator—The Concentrator terminates the opposite end of the tunnel. The
Concentrator decrypts, authenticates, and de-encapsulates the data.

**IPSec Client-to-LAN Tunneling**

Cisco.com

Telecommuter with
the Cisco VPN 3000
Series Concentrator
Client

VPN private IP
address
10.0.1.5

ISP

Internet

Application
server
10.0.1.10

VPN public IP
192.168.1.5

192.168.1.5
172.26.26.1
ESP
10.0.1.10
10.0.1.20

Data

Adapter (NIC) IP address
172.26.26.1
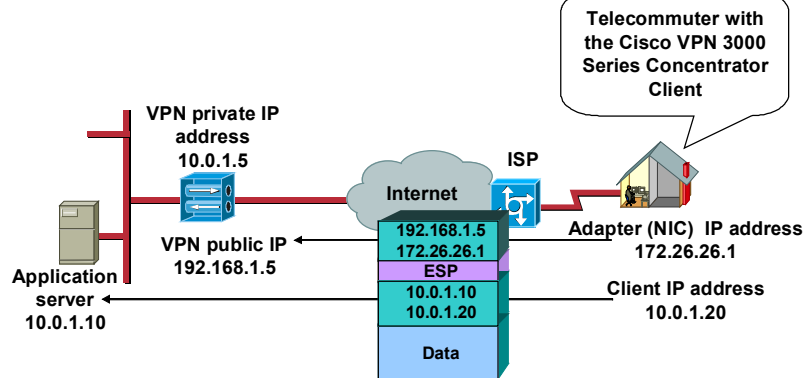
Client IP address
10.0.1.20

CSVPN 4.0—5-6

In the example in the figure, a telecommuter needs to access information on the corporate server, 10.0.1.10. The source address is the virtual IP address of the Software Client, 10.0.1.20. The Concentrator or the Dynamic Host Configuration Protocol (DHCP) server usually supplies it to the Software Client, which gives the Software Client the appearance of being resident on the VPN.

Any data flowing from the server to the Software Client must be protected as it traverses the Internet. Therefore, information flowing between the server and the Software Client is encrypted, authenticated, and encapsulated using the Encapsulating Security Payload (ESP) header to maintain confidentiality and data integrity.

However, this practice presents an issue. If the payload is encapsulated and encrypted, the routers in the Internet are unable to read the source and destination addresses of the packet. The routers are thus unable to route the packet. To solve this problem, an additional IP header is added to the ESP-encapsulated data. The outside IP header is used to route the information through the network using a routable address. The source address is the network interface card (NIC) of the Software Client. The destination address is the public interface of the Concentrator. The Software Client-to-server data is sent over the network using an IP-in-IP encapsulation. Upon receipt, the Concentrator strips the outer IP header, decrypts the data, and forwards the packet according to the inside IP address.

**Cisco VPN Software Client for Windows**

Cisco.com

**Cisco VPN Software Client for Windows**
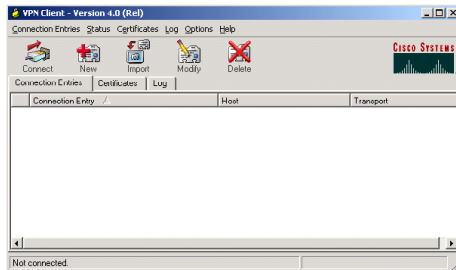
Installed on Windows system
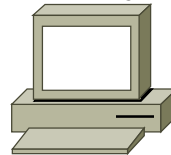
The Software Client works with the Concentrator to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Exchange (IKE) and IPSec tunneling protocols to make and manage the secure connection.

Some of the operations that the Software Client performs, which are mostly invisible to you, include the following:

■ Negotiating tunnel parameters: addresses, algorithms, lifetime, and so on

■ Establishing tunnels according to the parameters

■ Authenticating users by ensuring that users are who they say they are through usernames, group names, passwords, and digital certificates

■ Establishing user access rights: hours of access, connection time, allowed destinations, allowed protocols, and so on

■ Managing security keys for encryption and decryption

■ Establishing the IPSec session

■ Authenticating, encrypting, and decrypting data through the tunnel

# Initial Configuration of the Cisco VPN 3000 Series Concentrator for Remote Access

This topic explains how to cable the Cisco VPN 3000 Series Concentrator and establish a management session between a PC and the Concentrator.

## IPSec Server—Physical Connections

CSVPN 4.0—5-9
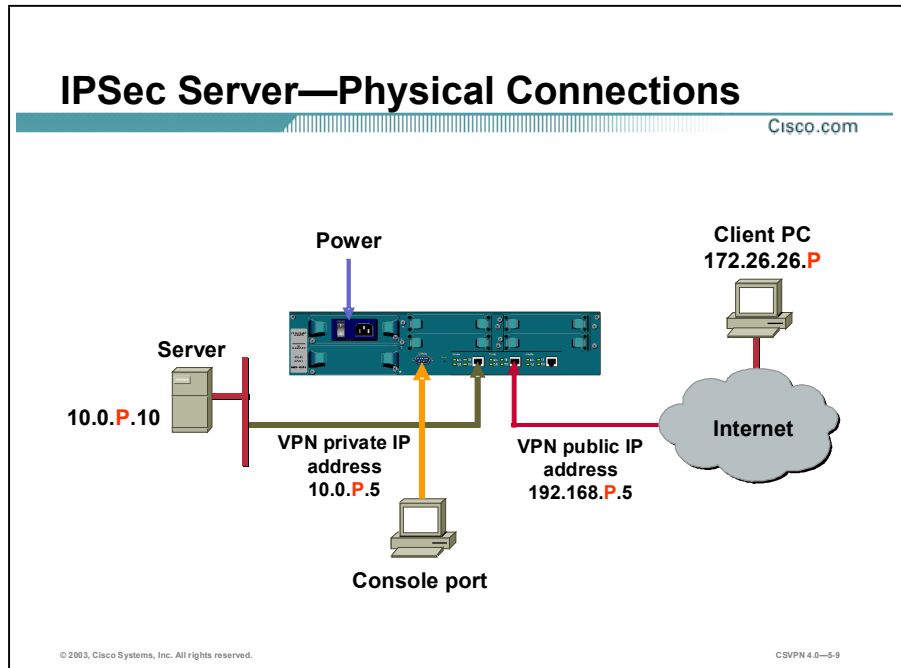
The Concentrator is equipped with universal power factor correction, 100–240 volts alternating current (VAC). A power cable with the correct plug is supplied. When the Concentrator arrives from the factory, you can plug it in and power it up. Connect the corporate LAN to the private interface of the Concentrator. Cable the Internet side of the corporate network to the public interface of the Concentrator. LAN ports can be programmed for 10-Mbps or 100-Mbps Ethernet.

IP addresses are not preprogrammed into the Concentrator at the factory. Use the console port to program in the correct IP addresses for the VPN private IP address. The serial console port needs to be configured for 9600 bps, 8 data bits, no parity, and 1 stop bit (8N1). When the addresses have been programmed, the operator can access the Concentrator via the browser.

## Configuration Options
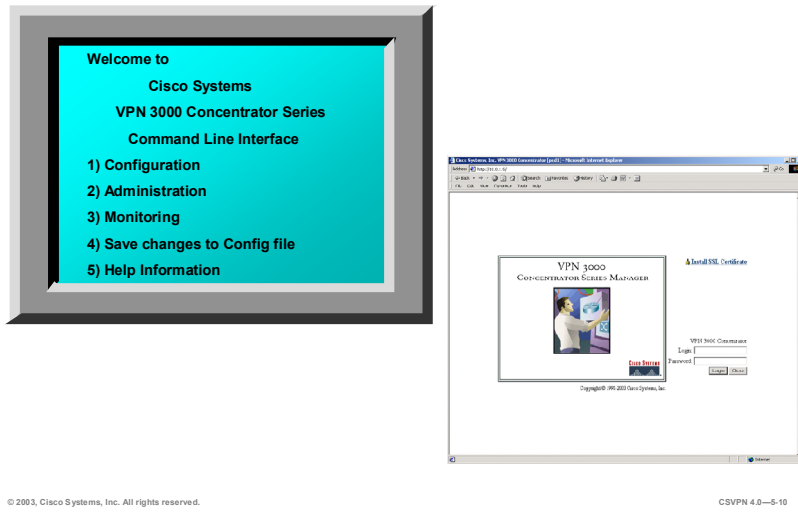
After the initial private IP address configuration, the remaining parameters can be configured in one of two ways: via the command line interface (CLI) or via a browser. For beginners, the menu-driven browser is recommended. The CLI is for those individuals who understand the menu structure. The CLI is accessed by either the direct connect console port or a LAN port Telnet session.

The web interface supports both HTTP and HTTP over Secure Sockets Layer (SSL). Operators can use either Internet Explorer or Netscape Navigator Software Revisions 4.0 or higher with both cookies and JavaScript enabled. Use either browser to configure the Concentrator, with one exception—Internet Explorer must be used when programming digital certificates.
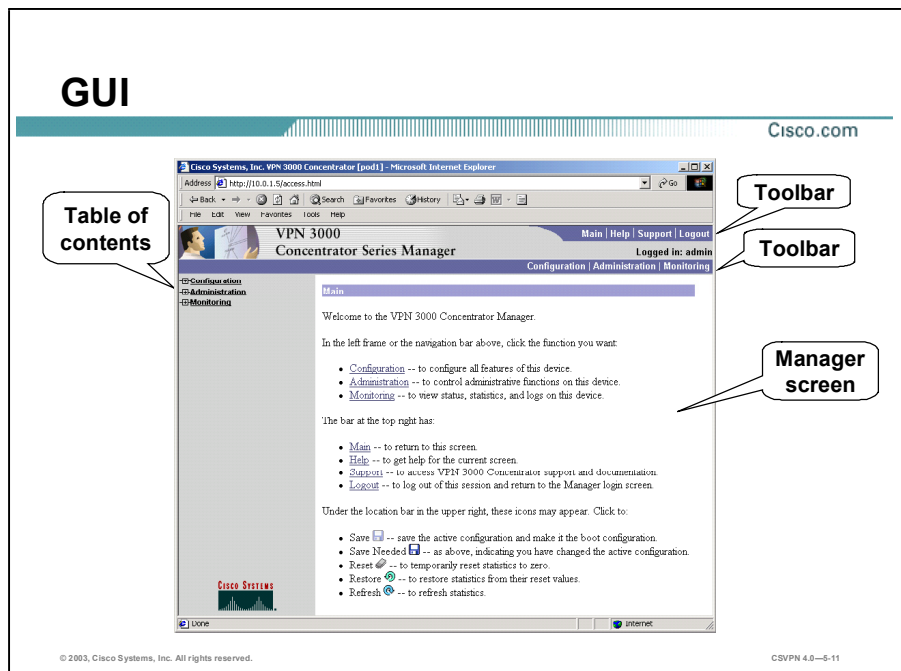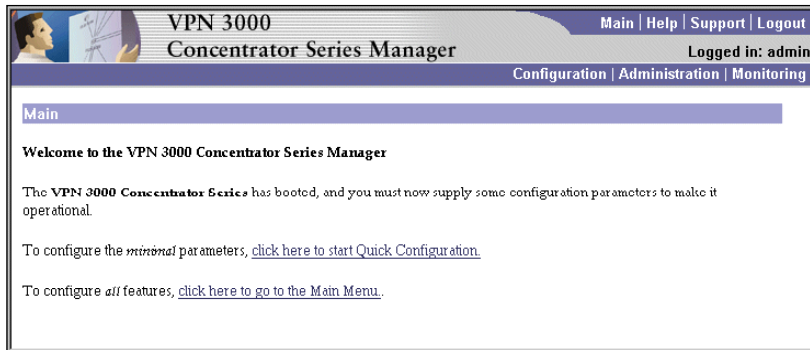
The figure shows the main window of the Concentrator, which displays after you log into the device:

■ The top frame (Cisco VPN 3000 Series Concentrator Manager toolbar) provides quick access to Manager functions.

■ The left frame (table of contents [TOC]) provides the TOC to the Manager windows.

■ The main frame (Manager window) displays the current Manager window. You can navigate the Manager using either the TOC in the left frame or the Manager toolbar at the top of the frame. To navigate from the TOC, select a title on the left frame of the window, and the Concentrator opens the Manager window for that topic in the main frame.

When you are finished with the configuration window, click **Apply**, which causes the configuration to take effect immediately. Click the **Save Needed** icon to save the changes to memory. If you reboot without saving, your configuration changes are lost.

# Quick Configuration



There are two ways to configure the Concentrator: Quick Configuration and the main menu. Quick Configuration enables you to configure the minimal parameters for operation. It automatically enables remote IPSec Client connections via an ISP for a single user group. The main menu is used to add additional IPSec user groups and to configure all features individually. Using Quick Configuration, an IPSec remote access application can be programmed by accessing six windows. Using the main menu, the same application requires the operator to access 12 or more windows. The next topics take you through an IPSec remote access configuration example.

| Note | You can run Quick Configuration only once. You must reboot to the factory default configuration to run it again. |
|------|------|

# Browser Configuration of the Cisco VPN 3000 Series Concentrator

After configuring the Cisco VPN 3000 Series Concentrator via the CLI, you can use the browser interface to configure the remaining items. This topic explains using the browser interface to configure the Concentrator.
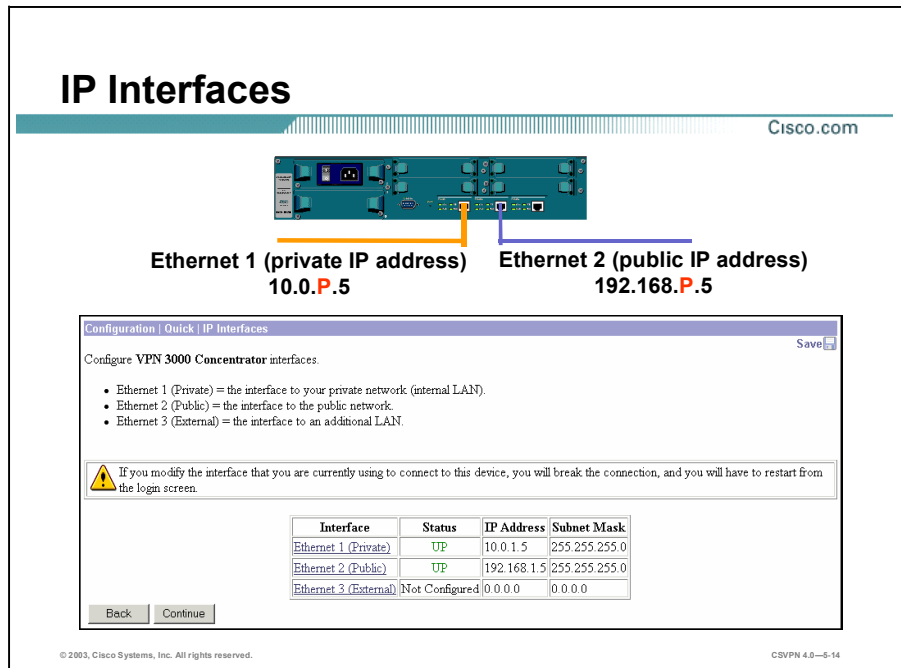


The figure contains an example of the first Quick Configuration window. It displays the current configuration of the IP interfaces:

■ Private—Interface toward the internal network

■ Public—Interface toward the public network (Internet)

■ External—Interface toward the external network or Demilitarized Zone (DMZ)

Remember, in this example, the private LAN interface was configured via the CLI. To configure the public LAN interface (toward the Internet), click the public interface hyperlink to access the public interface configuration window.

**Public IP Interface**

Cisco.com

Ethernet 1 (private IP address)
10.0.**P**.5

Ethernet 2 (public IP address)
192.168.1.5

Configuration | Quick | IP Interfaces | Ethernet 2

⚠ You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 2 (Public).

| General Parameters | | |
|---|---|---|
| **Sel** **Attribute** | **Value** | **Description** |
| ○ Disabled | | Select to disable this interface. |
| ○ DHCP Client | | |
| System Name | | Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP (System Name may be required for DHCP). |
| ⦿ Static IP Addressing | | |
| IP Address | 192.168.1.5 | |
| Subnet Mask | 255.255.255.0 | Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface. |
| Public Interface | ☑ | Check to make this interface a "public" interface. |
| MAC Address | 00.90.A4.00.17.A9 | The MAC address for this interface. |
| Filter | —None— | Select the filter for this interface. |
| Speed | 10/100 auto | Select the speed for this interface. |
| Duplex | Auto | Select the duplex mode for this interface. |
| MTU | 1500 | Enter the Maximum Transmit Unit for this interface (68 - 1500). |

Apply   Cancel

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—5-15

The window displayed in the figure is used to configure the public IP interface. The public IP interface can be configured in one of three ways: disabled, set as a DHCP client, or configured to use a static IP address. The public IP interface parameters are as follows:

■ Disabled radio button—The interface is enabled by default. Select the **Disabled** radio button to disable the interface.

■ DHCP Client radio button —Select the **DHCP Client** radio button if you want to enable this interface and use DHCP to obtain an IP address. In the System Name field, enter a name (such as VPN01 for the Concentrator). This name must uniquely identify this device on your network.

■ Static IP Addressing radio button —–Select the **Static IP Addressing** radio button if you want to enable this interface and set the static IP address. In the IP Address field, enter the IP address for this interface using dotted decimal notation (for example, 192.168.1.5). Be sure that no other device is using this address on the network. In the Subnet Mask field, enter the subnet mask for this interface using dotted decimal notation (for example, 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.1.5 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed.

■ Public Interface check box—Select the **Public Interface** check box to make this a public interface.

■ MAC Address field—This field displays the unique hardware MAC address for this interface.

- Filter drop-down menu—Click the **Filter** drop-down menu arrow and choose the public (default) filter, which allows only nonsource-routed inbound and outbound tunneling protocols and Internet Control Message Protocol (ICMP). The public filter is the default filter for Ethernet 2.

- Speed drop-down menu—Keep the default value.

- MTU field—The maximum transmission unit (MTU) value specifies the packet size, in bytes, for the interface. Valid values range from 68 through 1500. The default value, 1500, is the MTU for Ethernet.

# System Information

Cisco.com

**Configuration | Quick | System Info**

Assign a system name/hostname to this device. This may be required if you use DHCP to obtain an address.

**System Name** `student1VPN`    Enter a hostname for the system; e.g. vpn01.

Set the time on your device. The correct time is very important, so that logging and accounting entries are accurate.

The current time on this device is Friday, 23 February 2001 11:37:23.

**New Time** `11` : `38` : `10` `February ▾` / `23` / `2001` `(GMT-05:00) EST ▾`

☑ Enable DST Support

Specify a DNS server, which lets you enter hostnames rather than IP addresses in subsequent Manager fields.

**DNS Server** `0.0.0.0`    Enter the IP address of your local DNS server.

**Domain** `    `    Enter your Internet domain name; e.g. yourcompany.com.

**Default Gateway** `192.168.1.1`    Enter your default gateway. Leave at 0.0.0.0 for no default gateway.

[ Back ]  [ Continue ]

CSVPN 4.0—5-16

Use the Configuration>Quick>System Info window to configure basic information about the Cisco VPN 3000 Series Concentrator:

■ System Name field—Enter a name (such as VPN01) for the Concentrator in this field. This name must uniquely identify this device.

■ New Time fields and drop-down menus—Setting the correct time is very important so that logging and accounting entries are accurate. The fields show the current date and time on the device. The values shown in the New Time fields are the time on the browser PC, but any entries you make apply to the Concentrator. Enter the year as a four-digit number.

■ DNS Server field—Enter the IP address of your local Domain Name System (DNS) server, using dotted decimal notation (for example, 10.0.1.10). Specifying a DNS server lets you enter Internet hostnames (for example, vpn.company.com).

■ Domain field—Enter your Internet domain name.

■ Default Gateway field—Enter the IP address or hostname of the system to which the Concentrator should route packets that are not explicitly routed. In other words, if the Concentrator has no IP routing parameters (Routing Information Protocol [RIP], Open Shortest Path First [OSPF], or static routes) that specify where to send a packet, it will send it to the gateway specified in this field. This address must not be the same as the IP address configured on any Concentrator interface (for example, a default gateway may be to the perimeter router at 192.168.1.1).

**Protocols**

Cisco.com

IPSec

Internet
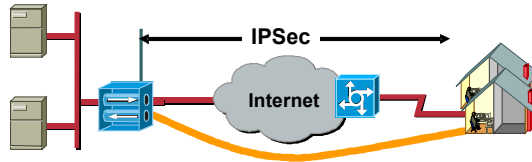
**Configuration | Quick | Protocols**

Select the tunneling protocols and encryption options that you want to enable.

☐ PPTP   ○ Require Encryption (Clients without encryption will not gain access. Requires MSCHAP.)
          ⊙ Don't Require Encryption (Clients may optionally use encryption.)

☐ L2TP   ○ Require Encryption (Clients without encryption will not gain access. Requires MSCHAP.)
          ⊙ Don't Require Encryption (Clients may optionally use encryption.)

☑ IPSec   Check to enable remote user connections via IPSec, LAN-to-LAN configurations are done outside of Quick Configuration.

[ Back ]  [ Continue ]

© 2003, Cisco Systems, Inc. All rights reserved.                                                CSVPN 4.0—5-17

Use the Configuration>Quick>Protocols window to configure the supported remote access protocols: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IPSec. The Concentrator can support all three protocols simultaneously. (However, for the sake of simplicity, only one application at a time is configured in the lab exercises.) Configure IPSec remote access, as shown in the figure, by selecting the **IPSec** check box. You cannot use Quick Configuration to configure IPSec LAN-to-LAN applications.

# Address Assignment

DHCP server
10.0.1.10

Internet
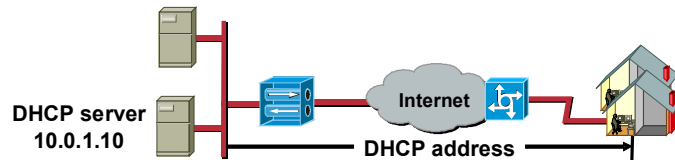
DHCP address

**Configuration | Quick | Address Assignment**

Select at least one method of assigning IP addresses to clients as a tunnel is established. The methods are tried in the order listed.

1. ☐ Client Specified  This method lets the client specify its own IP address.

2. ☐ Per User  This method assigns IP addresses on a per-user basis. If you use an authentication server (which you configure next) that has IP addresses configured, we recommend selecting this method.

3. ☑ DHCP  **Specify Server** |10.0.1.10|

4. ☐ Configured Pool  **Range Start** |_____|

   **Range End** |_____|

   This method uses this device to assign IP addresses.

[Back]  [Continue]

CSVPN 4.0—5-18

In the remote access PC, there are two IP addresses: the NIC address and the virtual IP address. The Concentrator Address Assignment window allows you to define how the remote PC receives the second IP address. There are four possible methods for obtaining the virtual IP address from which you must choose:

■ Client Specified check box—Select this check box to enable the Software Client to specify its own IP address. For maximum security, it is recommended that you control IP address assignments and not use the Software Client-specified IP addresses.

■ Per User check box—Select this check box to assign IP addresses retrieved from an authentication server on a per-user basis. If you are using an authentication server (external or internal) that has IP addresses configured, using this method is recommended.

■ DHCP check box—Select this check box to use a DHCP server to assign IP addresses.

■ Configured Pool check box—Select this check box to use the Concentrator to assign IP addresses from an internally configured pool.

# Authentication

**NT domain 10.0.1.10**

**User authentication**

**Internet**

**Cisco VPN 3000 Series Concentrator Client**

Configuration | Quick | Authentication

Specify how to authenticate users under PPTP, L2TP or IPSec. You can use the internal server or an external authentication server. If you select the *Internal Server*, you must configure the internal user database. You may configure additional servers using System Configuration.

Server Type [ NT Domain ▼ ]  Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server Address [10.0.1.10]  Enter the IP address.

Server Port [0]  Enter 0 for default port (139).

Timeout [4]  Enter the timeout for this server (seconds).

Retries [2]  Enter the number of retries for this server.

Domain Controller Name [Boston]  Enter the NT Primary Domain Controller name for this authentication server.

[ Back ] [ Continue ]

**Computer Name: BOSTON**
**Domain: Domain_BOSTON**

CSVPN 4.0—5-19

Before remote users can gain access to the private corporate network, they must be authenticated. Use the Configuration>Quick>Authentication window to define the types of authentication servers:

■ Server Type drop-down menu—Click the drop-down arrow and choose one of the following:

— RADIUS—An external Remote Authentication Dial-In User Service (RADIUS) server.

— NT domain—An external Windows NT domain server. Use the computer name, not the domain name. If you are unsure of the NT server computer name, refer to Start>Control Panel>System>Network Identification on your PC or ask your network administrator.

— Security Dynamics (SDI)—An external Rivest, Shamir, and Adleman (RSA) Security Inc. SecurID server.

— Kerberos/Active Directory—Supports authentication to Kerberos/Active Directory, which is the default authentication mechanism in Microsoft Windows 2000 and Windows XP.

— Internal server—The internal Concentrator authentication server (a maximum of 100 groups and users).

■ Authentication Server Address field—Enter the IP address of the Windows NT domain authentication server (for example, 10.0.1.10).

■ Domain Controller Name field—Enter the Windows NT primary domain controller hostname for this server (for example, Boston). Do not use the domain name.

# Configuration of Users and Groups

This topic explains how to configure users and groups on the Concentrator.
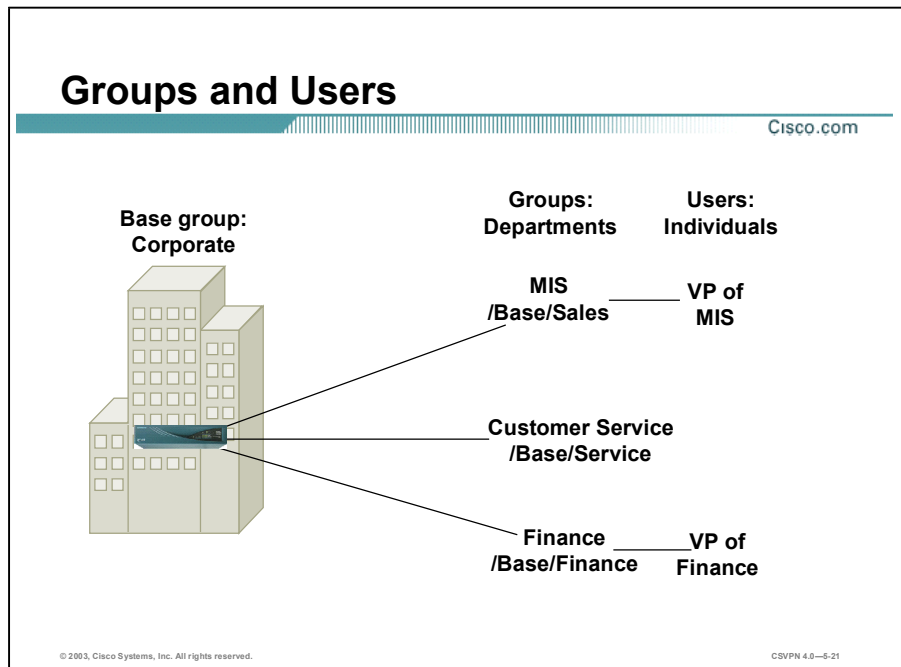


Within a corporation, not everyone has the same access requirements: customer service engineers may require seven-day, 24-hour access; sales entry personnel need five-day, eight-hour access, and contract help might need access from 9 a.m. to 5 p.m., with restricted server access. The Concentrator can accommodate different access and usage requirements. You can define different rights and privileges on a group basis. A customer service engineer, sales entry person, and contractor can be assigned to different groups. Within each group, you can configure different access hours, access protocols, idle timeouts, and server restrictions.

Within the Concentrator user management configuration tree, there are three group categories:

■ Default group—The default group is a default template. The majority of the corporation access rights and privileges are defined in this group.

■ Groups—Individual groups inherit the attributes of the default group, and you can then customize rights and privileges to meet the needs of specific groups.

■ Users—An individual user may require a unique set of privileges.

By configuring the default group first, specific groups second, and users third, you can quickly manage access and usage rights for large numbers of users.

**User and Group Policies**

Cisco.com

| Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP |

**General Parameters**

| Attribute | Value | Inherit? | Description |
|---|---|---|---|
| Access Hours | -No Restrictions- | ☑ | Select the access hours assigned to this group. |
| Simultaneous Logins | 3 | ☑ | Enter the number of simultaneous logins for this group. |
| Minimum Password Length | 8 | ☑ | Enter the minimum password length for users in this group. |
| Allow Alphabetic-Only Passwords | ☑ | ☑ | Enter whether to allow users with alphabetic-only passwords to be added to this group. |
| Idle Timeout | 30 | ☑ | (minutes) Enter the idle timeout for this group. |
| Maximum Connect Time | 0 | ☑ | (minutes) Enter the maximum connect time for this group. |
| Filter | --None-- | ☑ | Enter the filter assigned to this group. |

Access rights and privileges

CSVPN 4.0—5-22

From the Group>General window, you can configure group attributes on a group-by-group basis:

- Access Hours drop-down menu—Click the drop-down arrow and choose the named hours when group users can access the Concentrator (for example, M–F, 9–5).

- Simultaneous Logins field—Enter in this field the number of simultaneous logins that group users are permitted.

- Minimum Password Length field—Enter the minimum number of characters for group user passwords. Allow only alphabetic passwords. Select the check box to allow base-group user passwords with alphabetic characters only (the default).

- Idle Timeout field—Enter the time (in minutes). If there is no communication activity on the connection in this period, the system terminates the connection. Enter **0** to disable timeout and allow an unlimited idle period.

- Maximum Connect Time field—Enter the time in minutes. At the end of this time, the system terminates the connection. Enter **0** (the default) to allow unlimited connection time.

- Filter drop-down menu—Click the drop-down arrow and choose an option to define a filter. You can restrict the access of a group to the network based on the Software Client source address, destination address, or protocol.

- Inherit check boxes—Select the appropriate check boxes if you want the corresponding attributes to be inherited from the default group configuration. If you deselect a check box, you must enter or change any corresponding value.

**Group Database**

Cisco.com

Cisco VPN 3000 Series Concentrator Client

Internal server

Internet

Group: Training
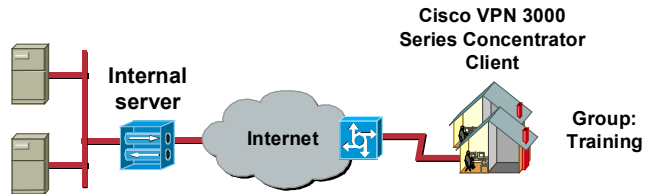
**Configuration | Quick | IPSec Group**

Select a Group Name and Password to be used by remote IPSec users. The Group Password must be at least 4 characters long.

Group Name: training
Password: ********
Verify: ********

Back   Continue

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—5-23

The Configuration>Quick>IPSec Group window enables you to enter a group name or username and password. The Software Client is authenticated by group to determine the Concentrator access and usage rights of that group. To do so, you must enter information in the following fields:

■ Group Name—Enter a unique name for this specific group. The maximum is 32 characters.

■ Password—Enter a unique password for this specific group. The minimum is 4 characters, and the maximum is 32 characters. The field displays only asterisks. The password is the IKE pre-shared key.

■ Verify—Re-enter the group password to verify it. The field displays only asterisks.

Admin Password
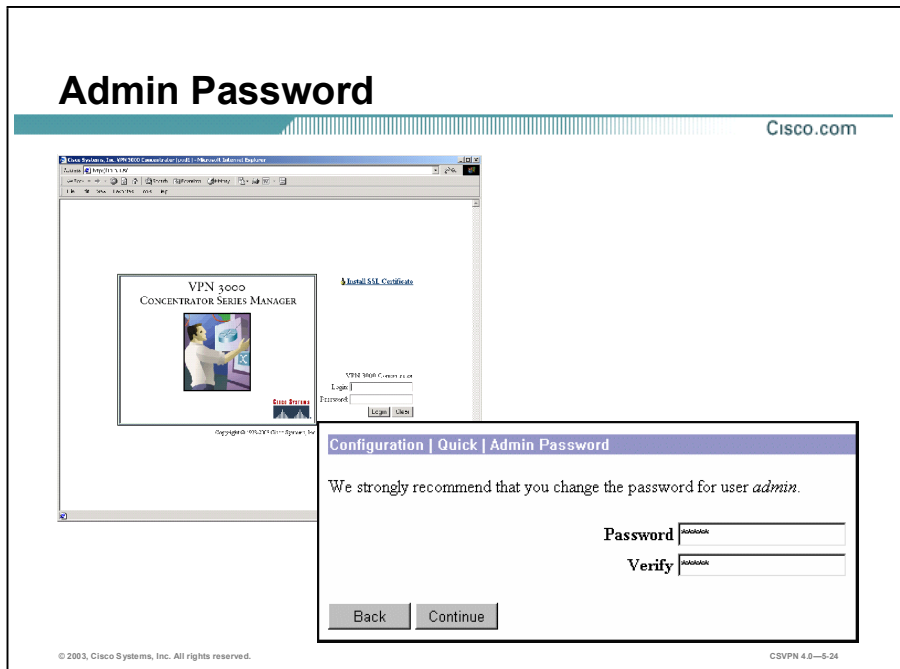
The window shown in the figure is the last Quick Configuration window. It is used to change the administrative password. Enter information in the following fields to change the administrative password:

■ Password—Enter or edit the unique password for this administrator. The maximum number of characters is 31. The field displays only asterisks.

| Caution | The default password that Cisco supplies is the same as the username. it is strongly recommended that you change this password in a production environment. (Do not change the password in the classroom environment.) |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

■ Verify—Re-enter the password to verify it. The field displays only asterisks.

# In-Depth Configuration Information

The previous topic explained how to quickly configure a single IPSec tunnel using Quick Configuration. This topic explains how to configure or modify IKE, group, and mode configuration parameters.



## Authentication

Cisco.com

**Concentrator authentication**

**Internal server**

**Internet**

**Group: Training**

**Network authentication (Xauth)**

**Cisco VPN Client (2.5)**
- **IKE Phase 1 complete**
- **Xauth**

**Cisco VPN Client (3.0 or higher)**
- **IKE Phase 1**
- **Xauth**
- **IKE Phase 1 complete**

CSVPN 4.0—5-26
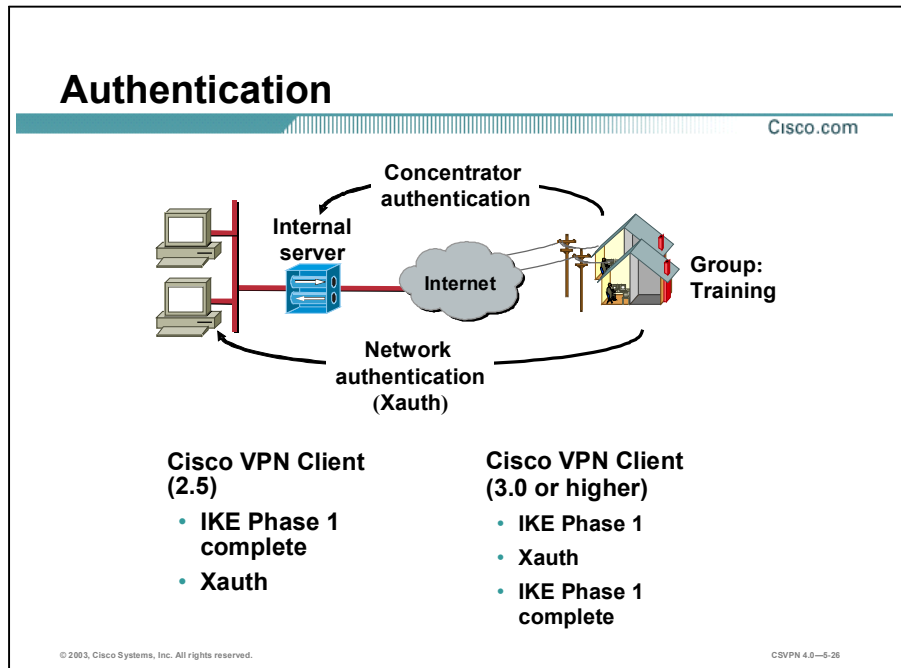
There are two types of authentication in the VPN network:

■ Concentrator authentication—Used to set up user rights and privileges as they relate to the Concentrator (for example, hours of operation, simultaneous logins, filters, and inactivity timeout).

■ Network authentication—Used to control access to the corporate network. Corporations typically require a secondary level of authentication before allowing users onto their networks—network authentications. An end user is prompted for a username and password, which in turn is verified by an authentication server. Only after being authenticated is an end user granted access to the corporate network. Network authentication is referred to as Extended Authentication (Xauth).

With the original Cisco 2.5 client, Xauth was performed after IKE Phase 1 was completed. Beginning with the Cisco VPN 3.0 Client, Xauth is performed during IKE Phase 1. In order for the Software Client to talk to the Concentrator, the correct IKE proposals must be defined for each Cisco VPN Client.

The type of Software Client resident on the remote PC is identified in the vendor identification field of an IKE message. The IKE proposal on the Concentrator must match the requirements of the Software Client.

## Activate IKE Proposal

Cisco.com

**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals**

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate.
Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.
Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by Security Associations to specify IKE parameters.

**3002, 3.x or 4.x Client**

**2.5 Client**

**Certicom client**

| Active Proposals | Actions | Inactive Proposals |
| --- | --- | --- |
| CiscoVPNClient-3DES-MD5 | << Activate | IKE-3DES-SHA-DSA |
| IKE-3DES-MD5 | Deactivate >> | IKE-3DES-MD5-RSA-DH1 |
| IKE-3DES-MD5-DH1 | Move Up | IKE-DES-MD5-DH7 |
| IKE-DES-MD5 | Move Down | CiscoVPNClient-3DES-MD5-RSA |
| IKE-3DES-MD5-DH7 | Add | CiscoVPNClient-3DES-SHA-DSA |
| IKE-3DES-MD5-RSA | Modify | CiscoVPNClient-3DES-MD5-RSA-DH5 |
| CiscoVPNClient-3DES-MD5-DH5 | Copy | CiscoVPNClient-3DES-SHA-DSA-DH5 |
| CiscoVPNClient-AES128-SHA | Delete | CiscoVPNClient-AES256-SHA |
| IKE-AES128-SHA | | IKE-AES256-SHA |

CSVPN 4.0—5-27

The Concentrator can handle several types of remote clients: the Cisco VPN 3.0 or higher Client, the Cisco VPN 2.5 Client, and the Certicom client. Before the Concentrator can interface with these clients, you must make sure that the appropriate IKE proposal is configured, activated, and prioritized.

In remote access connections, the Software Client sends IKE proposals to the Concentrator. The Concentrator functions only as the responder. As the responder, the Concentrator checks the active IKE proposal list, in priority order, to see if it can find a proposal that matches the parameters in the proposed Security Association (SA) of the Software Client. If a match is found, the tunnel establishment continues. If no match is found, the tunnel is torn down.

The IKE proposals are as follows:

■ For the Cisco VPN 3.0 Client or higher, use any of the proposals that start with CiscoVPNClient. The default is CiscoVPNClient-3DES-MD5. The Cisco VPN 3.0 Client or later proposal must be listed first under the Active Proposals list, or your Cisco VPN Client will not connect.

■ For the Cisco VPN 2.5 Client, use any of the IKE proposals except the IKE proposals that end in DH7.

■ For the Certicom client, use a proposal that ends in Diffie Hellman group 7 (DH7). The Certicom client requires a proposal that supports DH7.

Each IKE proposal in the IKE Proposals window is a template. The parameters assigned to the template are applied to the individual remote connection.

## Check IKE Proposal

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify

Modify a configured IKE Proposal.

| | | |
|---|---|---|
| **Proposal Name** | CiscoVPNClient-3DES- | Specify the name of this IKE Proposal. |
| **Authentication Mode** | Preshared Keys (XAUTH) ▼ | Select the authentication mode to use. |
| **Authentication Algorithm** | MD5/HMAC-128 ▼ | Select the packet authentication algorithm to use. |
| **Encryption Algorithm** | 3DES-168 ▼ | Select the encryption algorithm to use. |
| **Diffie-Hellman Group** | Group 2 (1024-bits) ▼ | Select the Diffie Hellman Group to use. |
| **Lifetime Measurement** | Time ▼ | Select the lifetime measurement of the IKE keys. |
| **Data Lifetime** | 10000 | Specify the data lifetime in kilobytes (KB). |
| **Time Lifetime** | 86400 | Specify the time lifetime in seconds. |

Apply     Cancel

CSVPN 4.0—5-28

As described in the previous topic, individual IKE templates were displayed under the Active Proposals column. By selecting an IKE proposal and then clicking **Modify**, the administrator can view or modify the individual parameters of the IKE proposal, or template. Use the Configuration>System>Tunneling Protocols>IPSec>IKE Proposals>Modify window to check the IKE proposals to make sure that you have the correct IKE parameters for a particular Software Client type.

■ Click the **Authentication Mode** drop-down arrow to choose the proper authentication mode:

— Pre-shared Keys (Xauth) for Cisco VPN 3.0 Client or later applications

— Pre-shared Keys for the Cisco VPN 2.5 Client

— Pre-shared Keys with DH7 for Certicom client applications

■ Click the **Diffie-Hellman Group** drop-down arrow to choose the correct DH group for each Software Client:

— Group 1 (768 bits) for Cisco VPN 2.5 Clients using digital certificates

— Group 2 (1024 bits) for Cisco VPN 2.5 Clients using pre-shared keys

— Group 5 (1536 bits) for clients using Advanced Encryption Standard (AES) encryption

— Group 7 (Elliptic Curve Cryptosystem [ECC]) for the Certicom clientClick the **Encryption Algorithm** drop-down arrow to choose the proper encryption algorithm:

— DES-56

— 3DES-168

— AES-128

— AES-192 (not supported on either the Cisco VPN Software or Hardware Client)

— AES-256

# Group Configuration—Identity

Cisco.com
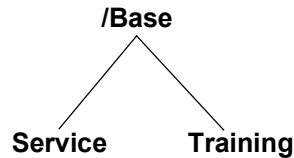
/Base

Service     Training

Configuration | User Management | Groups | Modify training

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

| Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP |

**Identity Parameters**

| Attribute | Value | Description |
|---|---|---|
| Group Name | training | Enter a unique name for the group. |
| Password | ***************** | Enter the password for the group. |
| Verify | ***************** | Verify the group's password. |
| Type | Internal | *External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database. |

Apply     Cancel

© 2003, Cisco Systems, Inc. All rights reserved.                                                      CSVPN 4.0—5-29

Within the Configuration>User Management>Groups>Modify Training window, you can view or modify individual group parameters. There are seven tabs located under Configuration>User Management>Groups>Modify Training: Identity, General, IPSec, Client Config, Client FW, HW Client, and PPTP/L2TP. Under each tab, the following information can be configured:

- Identity tab—You can configure the group name, password, and group authentication server type.

- General tab—You can configure access rights, privileges, and protocols.

- IPSec tab—You can configure the IPSec tunneling parameters.

- Client Config tab—You can configure the Software Client, Microsoft client, and common client parameters.

- Client FW tab—You can configure the Software Client firewall parameters.

- HW Client tab—You can configure the Hardware Client parameters.

- PPTP/L2TP tab—PPTP and L2TP tunneling parameters.

The identity parameters can be set as follows:

- Group Name field—Enter a unique name for this specific group. The maximum number of characters is 32.

- Password field—Enter a unique password for this specific group. The minimum number of characters is 4 and the maximum is 32. The field displays only asterisks.

- Verify field—Re-enter the group password to verify it. The field displays only asterisks.

- Type drop-down menu—Click the drop-down arrow and choose the type of group:

  - Internal—Use the internal Concentrator authentication server to authenticate groups for IPSec tunneling. The internal server is the default selection.

  - External—Use an external authentication server to verify this group (for example, a RADIUS server).

## Group Configuration—General

Cisco.com

| Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP |

**General Parameters**

| Attribute | Value | Inherit? | Description |
|---|---|---|---|
| Access Hours | -No Restrictions- | ☑ | Select the access hours assigned to this group. |
| Simultaneous Logins | 3 | ☑ | Enter the number of simultaneous logins for this group. |
| Minimum Password Length | 8 | ☑ | Enter the minimum password length for users in this group. |
| Allow Alphabetic-Only Passwords | ☑ | ☑ | Enter whether to allow users with alphabetic-only passwords to be added to this group. |
| Idle Timeout | 30 | ☑ | (minutes) Enter the idle timeout for this group. |
| Maximum Connect Time | 0 | ☑ | (minutes) Enter the maximum connect time for this group. |
| Filter | --None-- | ☑ | Enter the filter assigned to this group. |
| Primary DNS | | ☑ | Enter the IP address of the primary DNS server. |
| Secondary DNS | | ☑ | Enter the IP address of the secondary DNS server. |
| Primary WINS | | ☑ | Enter the IP address of the primary WINS server. |
| Secondary WINS | | ☑ | Enter the IP address of the secondary WINS server. |
| Tunneling Protocols | ☑ PPTP  ☑ L2TP  ☑ IPSec  ☐ L2TP over IPSec | ☑ | Select the tunneling protocols this group can connect with. |
| Strip Realm | ☐ | ☑ | Check to remove the realm qualifier of the username during authentication. |
| DHCP Network Scope | | ☑ | Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy. |

**Access rights and privileges**

**DNS and WINS**

**Tunneling protocol**

© 2003, Cisco Systems, Inc. All rights reserved.                    CSVPN 4.0—5-30

The General tab can be broken down into three sections: the top section defines access rights and privileges, the center section is for Windows Internet Name Service (WINS) and DNS information used by the Software Client, and the bottom section defines which tunneling protocols are supported by this group. Identity parameters can be set as follows:

■ Access Hours drop-down menu—Click the drop-down arrow and choose the hours when group users can access the Concentrator:

— No Restrictions—No restrictions on access hours

— Never—No access at any time

— Business Hours—Access from 9 a.m. to 5 p.m., Monday through Friday

■ Simultaneous Logins field—Enter the number of simultaneous logins that group users are permitted. The minimum is 1 and the default is 3. Although there is no maximum limit, allowing several could compromise security and affect performance.

■ Minimum Password Length field—Enter the minimum number of characters for group user passwords. The minimum is 1, the default is 8, and the maximum is 32.

■ Allow Alphabetic-Only Passwords check box—Select the check box to allow user passwords with alphabetic characters only. To maintain security, it is strongly recommended that you do not allow such passwords.

- Idle Timeout field—Enter the group idle timeout period in minutes. If there is no communication activity on the connection in this period, the system terminates the connection.

- Maximum Connect Time field—Enter the group maximum connection time in minutes. At the end of this time, the system terminates the connection.

- Filter drop-down menu—Filters can be used to restrict a group access to the network based on source address, destination address, and protocol.

---

| Note | The PC will overwrite its current values with information from the following fields. |
|------|-------------------------------------------------------------------------------------|

---

- Primary DNS field—Enter the IP address of the primary DNS server for this group.

- Secondary DNS field—Enter the IP address of the secondary DNS server for this group.

- Primary WINS field—Enter the IP address of the primary WINS server for this group.

- Secondary WINS field—Enter the IP address of the secondary WINS server for this group.

- SEP Card Assignment check boxes (depends on model)—It is recommended that you leave all four check boxes selected (for redundancy).

- Tunneling Protocols check boxes—Select the check boxes for the tunneling protocols that the user Software Clients can use. (Although the Concentrator can support all four protocols simultaneously, in the lab exercise for this lesson, you will remove the check from the PPTP and L2TP check boxes. Select IPSec only.)

- Strip Realm check box—If you select this check box, authentication is based on the username alone. The realm qualifier at the end of the username is removed (for example, "service" is stripped from "bob@service"). If this check box is not selected, authentication is based on a full string (for example, username@realm).

- DHCP Network Scope field—Enter the IP subnetwork that the DHCP server should assign to users in this group; for example, 200.0.0.0. DHCP Network Scope indicates to the DHCP server the range of IP addresses from which to assign addresses to users in this group.

**Group Configuration—IPSec**

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—5-31

The IPSec tab enables you to configure IPSec parameters that apply to this group. The window can be divided into two sections: IPSec and remote access parameters. IPSec parameters can be set as follows:

- IPSec SA drop-down menu—Click the drop-down arrow and choose the IPSec SA assigned to the IPSec clients for this group. During tunnel establishment, the IPSec client and server negotiate an SA that governs authentication, encryption, encapsulation, key management, and so on. View or modify IPSec SAs in the Configuration>Policy Management>Traffic Management>Security Associations window.

- IKE Peer Identity Validation drop-down menu—This option applies only to tunnel negotiations based on digital certificates.

- IKE Keepalives check box—Select this check box to enable the feature. (IKE keepalives are enabled by default.) This feature allows the Concentrator to monitor the continued presence of a remote peer and to report its own presence to that peer. If the peer becomes unresponsive, the Concentrator initiates removal of the connection. Enabling IKE keepalives prevents hung connections when rebooting either the host or the peer. For this feature to work, both the Concentrator and its remote peer must support IKE keepalives. The following peers support IKE keepalives:

  — Cisco VPN Client (Version 3.0)

  — Cisco VPN Client (Version 2.x)

  — Cisco VPN Hardware Client

- Concentrators (with IKE support)

- Cisco IOS software

- Cisco PIX Firewall

■ Tunnel Type drop-down menu—Click the drop-down arrow and choose the remote access tunnel type.

**IKE Keepalives—DPD**

Cisco.com

Client

Application server

Internet

Receive data

Worry timer expires

DPD message (Are you there)

DPD message (Are you there ACK)
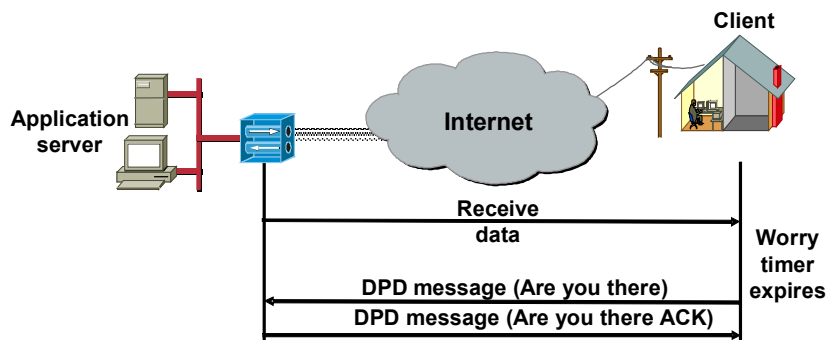
CSVPN 4.0—5-32

Dead peer detection (DPD) messages are used to enable VPN devices to detect tunnel failure on the devices located at the other end of a tunnel (for example, when you reboot one device and lose an Internet connection). A worry metric determines how often a DPD message is sent in the absence of data received from the IKE peer. When data is received, the worry timer is reset. If the worry timer expires, a DPD message is sent. The worry timers are as follows:

- In the Cisco VPN 3000 Series Concentrator Version 3.0 or later Software Client and Hardware Client, the worry timer is set for 20 seconds.

- In the Concentrator, the worry timer is set for 5 minutes.

If you are configuring a group of mixed peers, and some of those peers support IKE keepalives while others do not, enable IKE keepalives for the entire group. During IKE negotiation, each of the Software Clients will identify whether DPD messages are supported. Both ends must support the feature. The feature will have no effect on the peers that do not support it.

| Note | To reduce connectivity costs, disable IKE keepalives if this group includes any Software Clients connecting via ISDN lines. ISDN connections normally disconnect if idle, but the IKE keepalive mechanism prevents connections from idling out and, therefore, from disconnecting. |
|------|---|

**Remote Access Parameters**

CSVPN 4.0—5-33

Remote access parameters include group lock, user authentication, IP compression, and mode configuration parameters. The parameters are configured as follows:

■ Group Lock check box—Selecting this check box locks users into a specific group. (For example, RADIUS allows you to lock specific users to a group.) You can lock a user to a group based on the Organizational Unit (OU) of a certificate or by using the RADIUS Class attribute OU = group name. For example, according to the RADIUS server, Joe is a member of the Training group. If Joe tries to log in as a member of the IS group, which has different access rights, the connection fails.

■ Authentication drop-down menu—In the Concentrator, remote users are authenticated twice. This parameter pertains to the private network authentication. It determines how users within the group are authenticated and whether a Windows NT, SDI, or RADIUS server will authenticate them.

■ Authorization Type drop-down menu—If members of this group need authorization in addition to authentication, you can choose an authorization method. The following options are available:

— None—Do not authorize users in this group.

— RADIUS—Use an external RADIUS authorization server to authorize users in this group.

— Lightweight Directory Access Protocol (LDAP)—Use an external LDAP authorization server to authorize users in this group.

- Authorization Required check box—If you are using authorization, you can make it mandatory or optional.

- DN Field drop-down menu—If users in this group are authenticating by means of digital certificates and require LDAP or RADIUS authorization, you can choose which distinguished name (DN) field from the certificate uniquely identifies the user to the authorization server.

- IPComp drop-down menu—IP compression runs inside IPSec. Outbound data is compressed and then encrypted. At the remote end, data is decrypted and then decompressed. The IP compression uses fewer bytes per transmission. On a low-speed line, fewer bytes to transmit equates to faster transmission of the message. For example, you might put all modem users into a group and enable IP compression, which should speed up the transmissions. However, there is a processing penalty for compression. At higher speeds, 64 Kbps and above, IP compression tends to slow transmission due to the processing delays, compression, and decompression. Do not enable IP compression for high-speed users. Doing so would slow the performance of the PC and Concentrator.

- Reauthentication on Rekey check box—When this check box is selected, the Concentrator prompts the user for identification and a password whenever a rekey occurs. This feature is disabled by default.

- Mode Configuration check box—Selecting this check box enables the Concentrator to push information to the Software Client.

# Client Configuration Parameters

Most of the configuration issues in a remote access network originate at the remote PC. There are a large number of parameters to be programmed on the remote user PC. Not everyone could perform the needed changes. The Internet Engineering Task Force (IETF) IPSec Working Group Internet solved the issues by using mode configuration. The end user or IT department loads a minimum IPSec configuration in the end-user PC. During IPSec tunnel establishment, the Concentrator pushes the remaining information to the PC.

The administrator can program this information under the Configuration>User Management>Groups>Client Config tab. The Client Config tab has three sections: one for parameters specific to Cisco Clients, one for Microsoft client parameters, and one for common client parameters.

**Cisco Client Parameters**

Cisco.com

During IPSec tunnel establishment, the Concentrator pushes the Software Client information to the PC. These parameters include a login banner, split tunneling, IPSec over UDP, and so on.

Cisco VPN Client parameters can be set from the Client Config tab as follows:

■ Banner field—When a Software Client logs into the VPN, the banner that you enter in this field is displayed. It can be up to 510 characters and can consist of multiple lines of text instead of a single line (the text wraps). Enter a period (**.**) in the CLI to finish the entry and set the banner. If you enter more than 510 characters, the Software Client will see an error during login.

| **Note** | Each line break uses two characters. |
| --- | --- |

■ Allow Password Storage on Client check box—Password storage on the Client is not recommended for security purposes.

■ IPSec over UDP check box—IPSec packets are wrapped in UDP so firewalls and routers can perform Network Address Translation (NAT).

■ IPSec over UDP Port field—To enable IPSec over UDP, a UDP port number must be assigned.

■ IPSec Backup Servers drop-down menu—You can enable a Hardware Client to connect to the central site when its primary central-site Concentrator is unavailable. Configure backup servers for a Hardware Client either on the Hardware Client or on a group basis at the primary central-site Concentrator. If you configure backup servers on the central-site

Concentrator, that Concentrator pushes the backup server policy to the Hardware Client in the group.

**Tunneling Options**

Cisco.com

Tunnel everything

Encrypt everything — Client

Tunnel everything except local LAN traffic

Clear text

Encrypted — Client

www.news.com

Clear text

Split tunneling

Clear text

Encrypted — Client
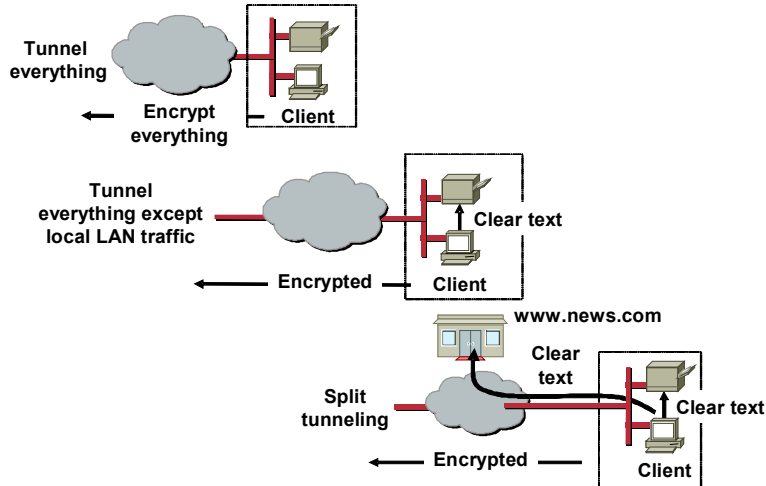
CSVPN 4.0—5-36

There are three tunneling options available to the network administrator: tunnel everything, tunnel everything except local LAN traffic, and split tunneling. The administrator must decide which option is correct for each group of remote Software Clients:

■ Tunnel everything—Once an IPSec tunnel is established, all traffic is encrypted and sent down the tunnel.

■ Tunnel everything except local LAN traffic—Everything is encrypted and sent through the tunnel except traffic destined for the local LAN. There are occasions when the remote user needs to print out spreadsheets locally. For this group of users, tunneling everything except local LAN traffic is the correct option.

■ Split tunneling—A remote user can simultaneously send clear text to a printer, download images from a web site, and send an encrypted report to headquarters, for example.

The default is to tunnel everything.

**Split Tunneling Policy—
Tunnel Everything**
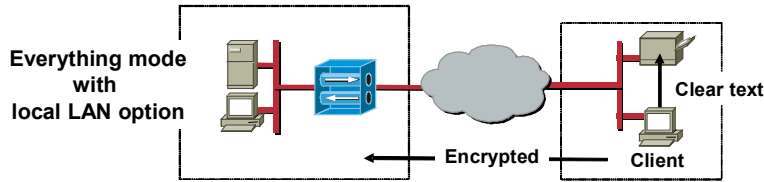
After the VPN tunnel is launched, all traffic is directed through the VPN tunnel. The VPN tunnel everything option allows only IP traffic to and from the secure gateway, prohibiting any IP traffic to and from resources on a local network (for example, printer, fax, and shared files on another system). While the IPSec tunnel is established, any Internet-bound traffic is forced through the tunnel to the central site.

Select the **Group>Client Config** tab to enable the tunnel everything option. Within this tab, select the **Tunnel everything** radio button within the Split Tunneling Policy row.

# Split Tunneling Policy—Local LAN Option

Everything mode with local LAN option

Clear text

Client

Encrypted

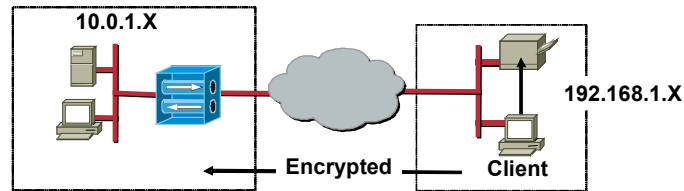| Common Client Parameters | | | |
|---|---|---|---|
| Split Tunneling Policy | ○ Tunnel everything ☑ Allow the networks in list to bypass the tunnel ○ Only tunnel networks in the list | ☐ | Select the method and network list to be used for Split Tunneling. **Tunnel Everything**: Send all traffic through the tunnel. **Allow the networks in the list to bypass the tunnel:** The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client. |
| Split Tunneling Network List | VPN Client Local LAN (Default) ▾ | ☐ | **Tunnel networks the in list:** Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN. |
| Default Domain Name | | ☑ | Enter the default domain name given to users of this group. |
| Split DNS Names | cisco.com | ☐ | Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel. |

Apply  Cancel

CSVPN 4.0—5-38

The local LAN access option, on the other hand, provides access to resources on a local LAN while the VPN tunnel is established. The local LAN addresses are pushed to the Software Client. These IP addresses are added to the access control list (ACL) of the Software Client driver. These bypass addresses route ahead of the VPN tunnel encryption algorithm. Any data bound for, or received from, the addresses specified in the mode configuration message is sent or received in the clear. This practice allows access to the local LAN while the IPSec tunnel is running. All other traffic is encrypted and forwarded to the central site. For security purposes, the user has the ability to disable local LAN access when using an unsecured local network (for example, in a hotel).

Two steps are required to configure the option:

**Step 1**  Enable the feature. Select the **Allow the networks in the list to bypass the tunnel** radio button within the Split Tunneling Policy row.

**Step 2**  Supply the referenced IP address list. Choose **VPN Client Local LAN (Default)** from the Split Tunneling Network List drop-down menu.
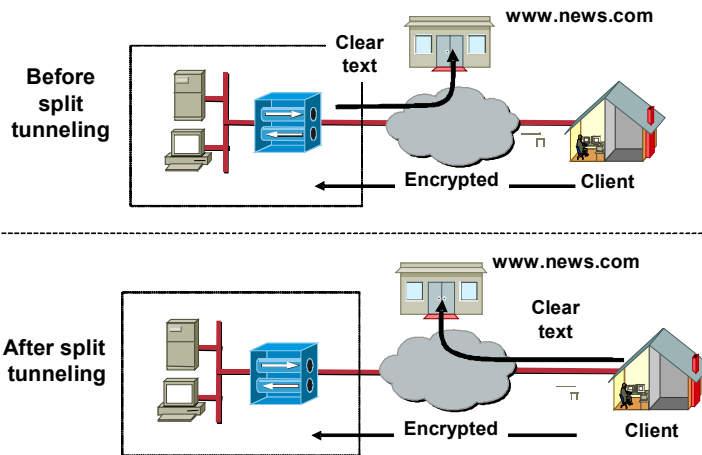
**Local LAN Option—Network List**

A local LAN network address list is required for the local LAN option. Go to the Configuration>Policy Management>Traffic Management>Network Lists window to configure the LAN address. The address list pushed to the Software Client is 0.0.0.0/0.0.0.255. This is a special case. It directs the Software Client to interpret the network address or subnet mask of the LAN interface over which the VPN connection is being made as the local LAN address. Route all locally addressed LAN packets in clear text. The 0.0.0.0/0.0.0.255 network address list is referred to as the Software Client LAN (default) list.

In the example in the figure, the Software Client resides on the 192.168.1.0 network. Having received a 0.0.0.0/0.0.0.255 network list, the Software Client routes all 192.168.1.0 traffic in clear text. All other traffic is encrypted and sent down the tunnel.

## Split Tunneling—Before and After

Cisco.com

**Before split tunneling**

Clear text

www.news.com

Encrypted — Client

**After split tunneling**
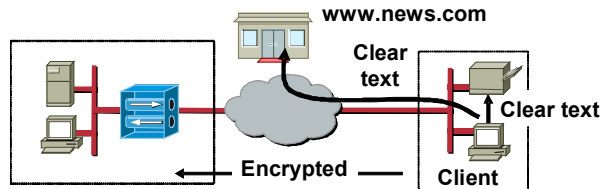
www.news.com

Clear text

Encrypted — Client

CSVPN 4.0—5-40

Split tunneling enables remote users to access Internet networks without requiring them to tunnel through the corporate network. Before split tunneling is enabled, all traffic originating from the Software Client is encrypted and routed through the secure tunnel. This traffic includes both secure and Internet browsing traffic. The secure traffic is terminated, while Internet traffic is routed back out to the Internet. A large percentage of the corporate backbone bandwidth is used for redirected web browsing traffic from remote users.

Split tunneling addresses the redirect issue, because split tunneling routes secure, encrypted traffic through the tunnel. Nonsecure traffic (for example, web browsing) is sent in the clear. The ISP can route the traffic accordingly (for example, secure traffic goes to the corporate network, and web browsing goes to the ISP).

**Split Tunneling Policy—
Split Tunneling**

Cisco.com

www.news.com

Clear
text

Clear text

Encrypted

Client

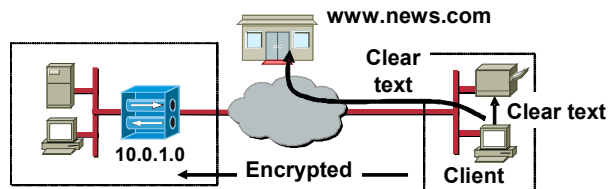| Common Client Parameters | | | |
|---|---|---|---|
| **Split Tunneling Policy** | ○ Tunnel everything<br>☐ Allow the networks in list to bypass the tunnel<br>◉ Only tunnel networks in the list | ☐ | Select the method and network list to be used for Split Tunneling.<br>**Tunnel Everything:** Send all traffic through the tunnel.<br>**Allow the networks in the list to bypass the tunnel:** The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client. |
| **Split Tunneling Network List** | pod 1 network list | ☐ | **Tunnel networks the in list:** Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN |
| **Default Domain Name** | | ☑ | Enter the default domain name given to users of this group. |
| **Split DNS Names** | cisco.com | ☐ | Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel. |

Apply   Cancel

CSVPN 4.0—5-41

The Concentrator pushes specific IP addresses to the Software Client to implement split tunneling. Traffic bound for one of these addresses is encrypted and sent to the Concentrator. If the IP address is different from the pushed addresses, the message is sent in the clear and, therefore, is routable by the ISP.

Configuring split tunneling requires two steps:

**Step 1**  Enable split tunneling by clicking the **Only tunnel networks in list** radio button within the Split Tunneling Policy row.

**Step 2**  Choose the appropriate list from the Split Tunneling Network List drop-down menu. This menu presents a predefined list of secure network addresses.

Split Tunneling—Network List

The Concentrator pushes specific IP addresses to the Cisco VPN Client. Traffic bound for one of these addresses is encrypted and sent to the Concentrator. These addresses are defined under Configuration>Policy Management>Traffic Management-Network Lists. In the List Name field, enter a name for the list. In the Network List field, supply the network and wildcard mask. In the example in the figure, the administrator wants to send clear text to the Internet and local printer. The administrator also wants to send encrypted traffic to the headquarters: the 10.0.1.0 network. In the Network List field, the administrator defines a network list name (Pod 1 network list) and configures the private network IP address and wildcard mask (10.0.1.0/0.0.0.255). As a result, any traffic bound for a host on the 10.0.1.0 network is encrypted and sent down the IPSec tunnel. All other traffic is sent in plain text.

Split DNS

CSVPN 4.0—5-43
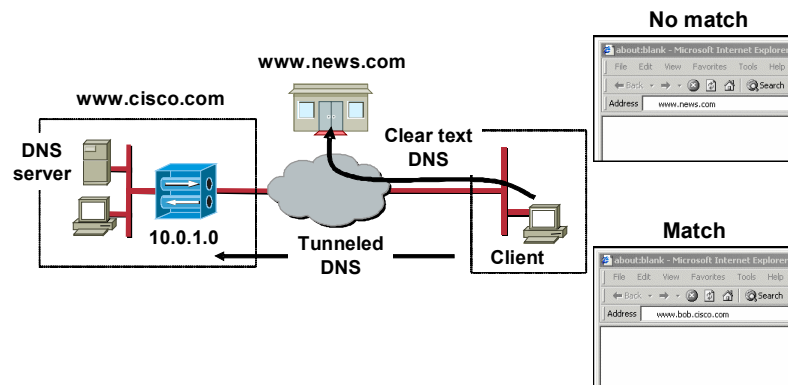
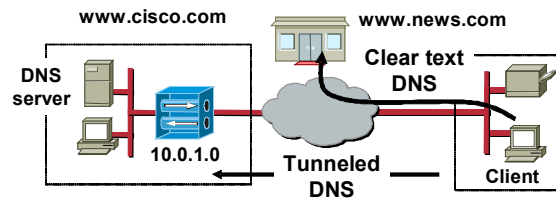Split DNS is used in split-tunneling connections. The Software Client will resolve whether a DNS query packet is to be sent in clear text or is to be encrypted and sent down the tunnel. If the packet is encrypted and sent down the tunnel, a corporate DNS server resolves the DNS query. Clear text DNS requests are resolved by ISP-assigned DNS servers.

The client will receive a comma-delimited list of split-DNS names from the Concentrator via mode configuration. When the Software Client receives a DNS query packet, the domain name is compared and sequentially checked against the split-DNS names. Case-insensitive domain name comparison will start at the end of each domain name string and continue toward the beginning of each string, resulting in a match or no match. Query packets passing the comparison will have their destination IP address rewritten and tunneled using the primary DNS IP address configured on the concentrator. As an example, the query bob.cisco.com is compared against the split-DNS name of cisco.com and results in a match. The cisco.com portion of bob.cisco.com matches the split-DNS string of cisco.com. The bob.cisco.com DNS query is encrypted and sent to the primary DNS server. The primary DNS server will resolve the IP address of bob.cisco.com. Failover in the case of an unreachable primary split-DNS server will result in the secondary split-DNS server being used to resolve further queries. Packets not matching the split-DNS list will pass through the client untouched and transmitted in clear text. As an example, the query news.com, when compared against the split-DNS name cisco.com, results in a mismatch. The news.com DNS query is sent in clear text. The ISP-assigned DNS servers will resolve the IP address.

## Split DNS Configuration

In the figure, the corporate DNS server will resolve all cisco.com DNS name requests. The ISP-assigned DNS server resolves all clear text DNS requests. Complete the following five-step process to configure split DNS:

**Step 1**  Define a list of secure networks. The network list is defined under Configuration>Traffic Management>Policy Management>Network Lists.

**Step 2**  Configure the Concentrator for split tunneling from the Configuration>User Management> Groups>Client Config tab. Click the **Only tunnel networks in the list** radio button to enable split tunneling.

**Step 3**  From the Configuration>User Management>Groups>Client Config tab, select the newly defined network list from the Split Tunneling Network List drop-down menu.

**Step 4**  From the Configuration>User Management>Groups>Client Config tab, enter the names of the corporate DNS servers in the Split DNS Names field (for example, cisco.com). Use commas, without spaces, to separate the names for multiple entries.

**Step 5**  From the Configuration>User Management>Groups>General tab, define the primary and secondary DNS server IP addresses. The primary and secondary DNS servers resolve the encrypted DNS queries.

**DDNS**

Cisco.com
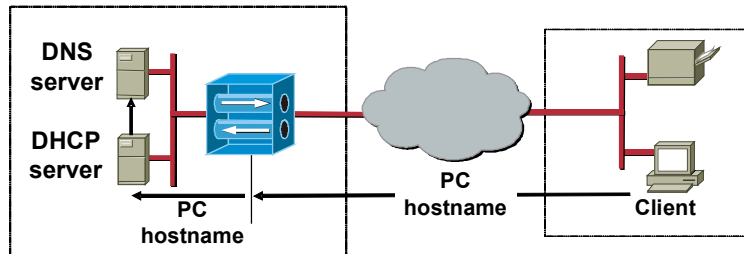
DNS servers were originally used in a static environment. As a new host was added to the network, an administrator would add the host to the DNS database. When remote hosts dynamically attach and detach from the network, static remote host information updates to DNS database become impossible. The dynamic DNS (DDNS) feature is often used in networks to coordinate hostname information between DHCP and DNS servers in an attempt to accurately reflect the current network configuration. DHCP clients and servers use dynamic updates to send updated remote hostname information from the DHCP client to the DHCP server. The DHCP server forwards the hostname to the DNS server. The DDNS feature enables DNS servers to accept hostname and IP address updating information.

Prior to Version 3.6, the Software Client did not supply its hostname to the DHCP server. The DDNS feature was not supported. In Version 3.6 and above, the Software Client was modified to send its hostname to the Concentrator as part of mode configuration messages. The Concentrator forwards the Software Client hostname to the DHCP server. The DHCP server forwards the information to the DNS server. This practice enables the DNS server to dynamically populate its records. The DDNS feature applies to Software Client connections only when a DHCP server assigns the Software Client IP address.

**Mode Configuration**

Cisco.com

Push

Internet

NT
domain
server
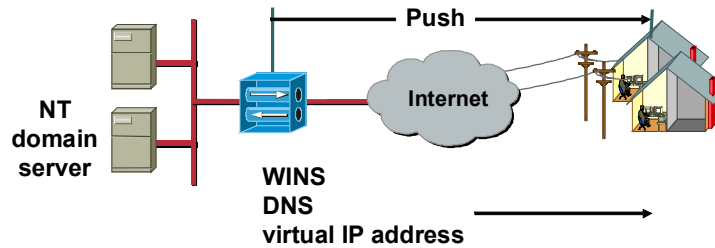
WINS
DNS
virtual IP address

CSVPN 4.0—5-46

Additional information passed to the Software Client includes WINS and DNS IP address information and virtual IP addresses. The WINS and DNS information is programmed in the Groups>General tab. The virtual IP address and network mask originate at the Concentrator, a DHCP server, or a RADIUS server. The virtual IP address source is configurable in the Configuration>System>Address Management window.

## Modifying Groups

Configuration | User Management | Groups

Save

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, select a group and click the appropriate button.

Actions | Current Groups | Modify

training (Internally Configured)

Add Group
Modify Group
Delete Group

Authentication Servers
Authorization Servers
Accounting Servers
Address Pools
Client Update
Bandwidth Assignment

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—5-47

Until Version 2.5 of the Cisco VPN 3000 Series Concentrator software, the authentication servers, address pools, and accounting servers were defined on a global basis. In later versions, the administrator can define specific attributes on a group-by-group basis. For example, one group can use RADIUS, while another group uses Windows NT.

| Note | Quick Configuration enables you to define attributes only on a global basis. |

## Setting Up Group Attributes

Cisco.com

**Finance group**

RADIUS 5

**Engineering group**

RADIUS 2

• **Global**
  – NT
  – 10.0.1.10–60
• **Engineering**
  – RADIUS 2
  – 10.0.20.60–90
• **Finance**
  – RADIUS 5
  – 10.0.30.50–80

Internet

• **HR**
  – NT
  – 10.0.1.21

• **Finance**
  – RADIUS 5
  – 10.0.30.51

• **Engineering**
  – RADIUS 2
  – 10.0.20.71

CSVPN 4.0—5-48

In Version 2.5 of the Concentrator, you set up global parameters, such as address pools, authentication, IP addressing, and so on. All Software Clients access the global parameters. Global parameters do not allow for customization.

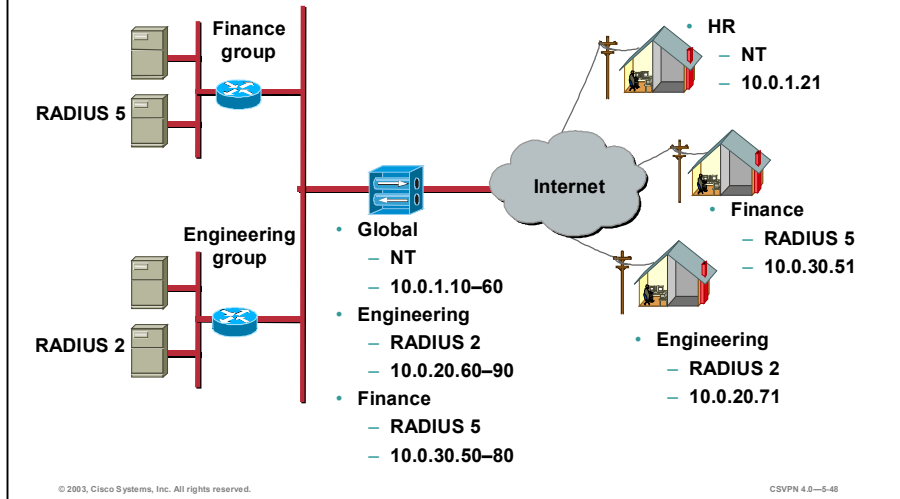Later versions allow you to set authentication and assign IP addressing on a group-by-group basis. For example, if you have remote users using different clients (Cisco VPN 2.5 Client, Cisco VPN 3.0 Client, and Certicom clients), you can program different groups for each client type. This feature enables the administrator to define different address pools, authentication server types (RADIUS, NT domain, SDI, and internal), and authentication servers for each group. If you run out of address pools under a group setting, or if the Concentrator cannot contact the authentication server for the group, the Concentrator defaults to global settings.

The figure shows three groups: HR, Finance, and Engineering. Each group has a different range of IP addresses and authentication servers. When an HR Software Client tunnels into the Concentrator, it is authenticated by a Windows NT server and assigned an address from the global IP address pool. When an Engineering Software Client establishes a tunnel to the Concentrator, it receives an IP address from a group pool, 10.0.20.60–90, and is authenticated by the RADIUS 2 server. Finance Software Clients receive attributes according to their group parameters.

## Types of Authentication

Software Clients are authenticated twice: once by the Concentrator and once by an authentication server. In the example in the figure, the Software Client is first authenticated against the internal group database of the Concentrator. Next, a Windows NT server, 10.0.1.10, authenticates the Software Client before access to the private network is allowed.

The Software Client authentication can be assigned by group. A different server type (NT, SDI, or RADIUS) can conceivably authenticate each group. When the group needs to be authenticated, the Concentrator goes down the authentication server list until it finds the first instance of the assigned authentication server. The Concentrator then tests for communication with that server. If communication is good, Software Client authentication is determined. If the Concentrator cannot communicate with the first server, it will go down the list to the next instance of that server type and retest for communications. The administrator can reorder the priority of the server list by selecting a server under the Authentication Server window and clicking the **Move Up** or **Move Down** buttons. The administrator can also check the communications between the Concentrator and the server. By clicking the **Test** button under the Actions column, the administrator can test the ability of the Concentrator to reach a specific server.

## Testing Authentication Server

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation to complete or timeout.**

User Name student1

Password ********

OK    Cancel

**Success**

Authentication Successful

Continue

CSVPN 4.0—5-50

In a remote access network, there are three main trouble spots: at the Cisco VPN Client, between the Software Client and the Concentrator, and between the Concentrator and the authentication server. Using the Test button, you can check communication between the Concentrator and the authentication server. Enter the Software Client username and password for the authentication server in the corresponding fields to complete a user authentication test. Click **OK**. The Concentrator attempts to log into the authentication server. If successful, an Authentication Successful message displays. If unsuccessful, an Authentication Failed message displays. The authentication test can verify communication between the Concentrator and the authentication server.

## Public Interface— IPSec Fragmentation

Configuration | Interfaces | Ethernet 2

Configuring Ethernet Interface 2 (Public).

General | RIP | OSPF | Bandwidth

### General Parameters

| Sel | Attribute | Value | Description |
|---|---|---|---|
| ○ | Disabled | | Select to disable this interface. |
| ○ | DHCP Client | | Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP. |
| ● | Static IP Addressing | | |
| | IP Address | 192.168.1.5 | Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface. |
| | Subnet Mask | 255.255.255.0 | |
| | Public Interface | ✓ | Check to make this interface a "public" interface. |
| | MAC Address | 00.90.A4.00.17.A9 | The MAC address for this interface. |
| | Filter | 2. Public (Default) | Select the filter for this interface. |
| | Speed | 10/100 auto | Select the speed for this interface. |
| | Duplex | Auto | Select the duplex mode for this interface. |
| | MTU | 1500 | Enter the Maximum Transmit Unit for this interface (68 - 1500). |
| | Public Interface IPSec Fragmentation Policy | ● Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission<br>○ Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)<br>○ Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit) | |

Apply    Cancel

CSVPN 4.0—5-51

IPSec fragmentation policy specifies how to treat packets that exceed the MTU setting when tunneling traffic through the public interface. This feature provides a way to handle cases where a router or NAT device between the Concentrator and the client rejects or drops IP fragments. For example, suppose a client wants to run the FTP **GET** command from an FTP server behind the Concentrator. The FTP server transmits packets that when encapsulated would exceed the Concentrator MTU size on the public interface. IPSec fragmentation is not configurable from the Quick Configuration menu. It can be configured from Configuration>Interface menu. The following options determine how the Concentrator processes these packets:

■ Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission—
The Concentrator encapsulates all tunneled packets. After encapsulating the packets, the Concentrator fragments packets that exceed the MTU setting before transmitting them through the public interface. This policy is the default for the Concentrator. This option works for situations where fragmented packets are allowed through the tunnel without hindrance. In the FTP example, large packets are encapsulated and then fragmented at the IP layer.

■ Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)—The Concentrator fragments tunneled packets that would exceed the MTU setting during encapsulation. For this option, the Concentrator drops large packets that have the Don't Fragment (DF) bit set and sends an ICMP message, "Packet needs to be fragmented but DF is set," to the packet initiator. The ICMP message includes the maximum MTU size allowed. The Path MTU Discovery message means that an intermediate device (in this case the Concentrator) informs the source of the MTU permitted to reach the destination. If a large packet does not have the DF bit set, the Concentrator fragments prior to encapsulating, thus creating two independent nonfragmented IP packets, and transmits them out the public interface. This policy is the default for the Hardware Client. In this example,

the FTP server may use Path MTU Discovery to adjust the size of the packets it transmits to this destination.

■ Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)—The Concentrator fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the Concentrator clears the DF bit, fragments the packets, and then encapsulates them. This action creates two independent nonfragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site. In this example, the Concentrator overrides the MTU and allows fragmentation by clearing the DF bit.

# Configuration of the Cisco VPN Software Client for Windows

This topic explains how to configure and use the Cisco VPN Software Client for Windows on the Concentrator.
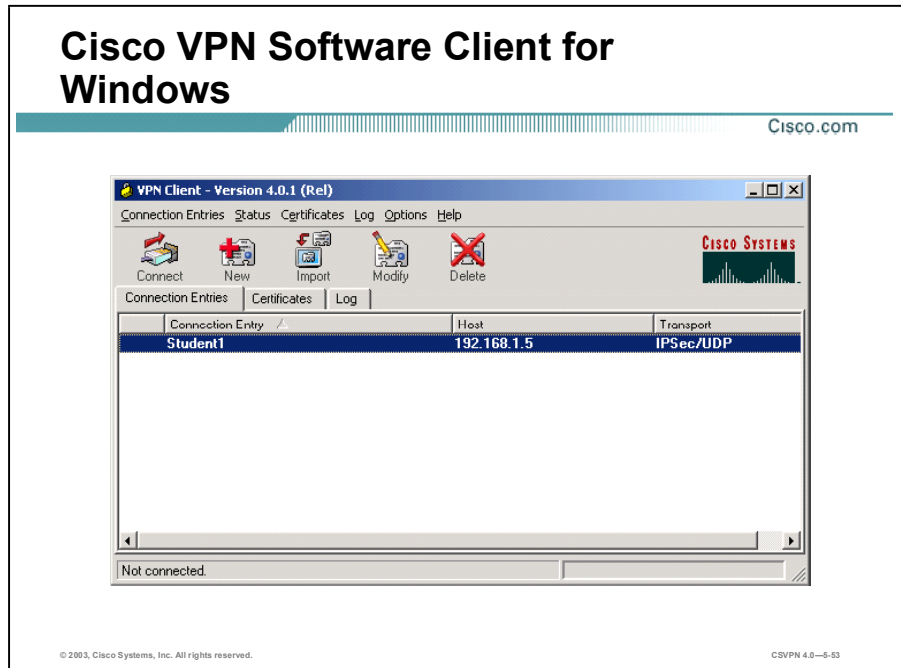


The Cisco VPN Software Client for Windows is a software program that runs on Windows 95, 98, ME, 2000, XP, and NT 4.0. The Software Client on a remote PC, communicating with a Concentrator at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user.

The figure shows the Software Client window. From this window, you can launch the new-connection wizard, change or set optional parameters, and launch the Software Client.

**Cisco VPN Software
Client for Windows Run Mode**
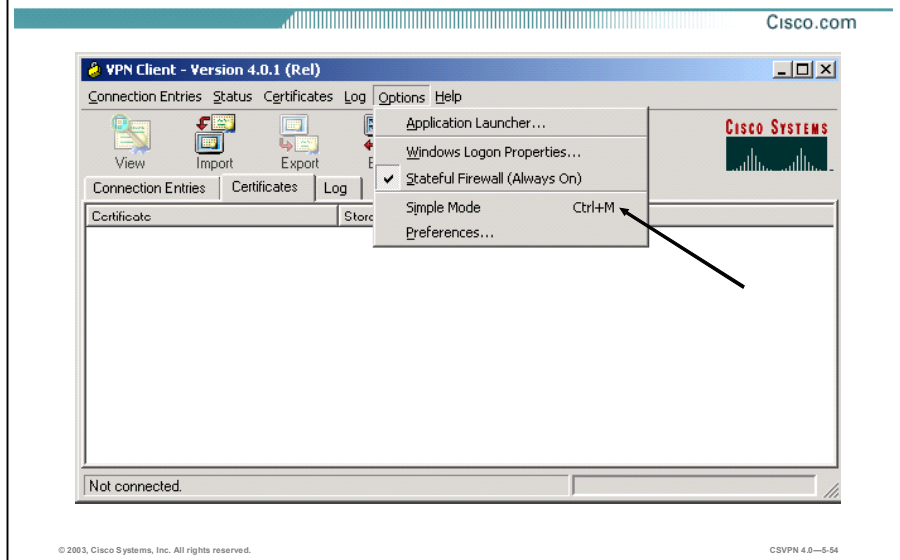
You can run the Cisco VPN Client in simple mode or in advanced mode. The default is advanced mode, although your network administrator might have configured simple mode as the default.

Use simple mode if you want only to start the Cisco VPN Client application and connect to a VPN device using the default connection entry.

Use advanced mode for the following tasks:

■ Managing the Cisco VPN Client

■ Configuring connection entries

■ Enrolling for and managing certificates

■ Viewing and managing event logging

■ Viewing tunnel routing data

To toggle between advanced mode and simple mode, press **Ctrl-M**. Alternatively, you can choose your mode from the Options menu.
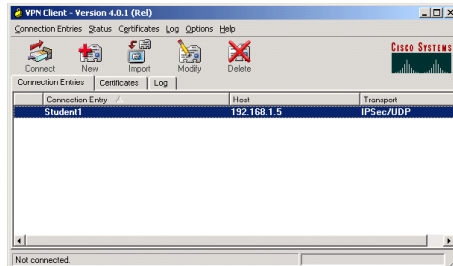
The following are the main tabs:

■ Connection Entries tab—Displays the list of current connection entries, the host, which is the VPN device that each connection entry uses to gain access to the private network, and the transport properties that are set for each connection entry.

■ Certificates tab—Displays the list of certificates in the VPN Client certificate store. Use this tab to manage certificates.

■ Log tab—Displays event messages from all processes that contribute to the client-peer connection: enabling logging, clearing the event log, viewing the event log in an external window, and setting logging levels.
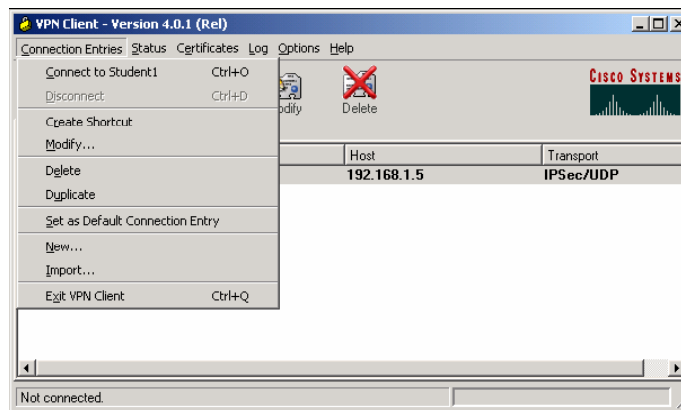
Use the Connection Entries menu as a shortcut to frequently used connection entry operations. The following commands are available:

■ Connect to—Connect to a VPN device using the selected connection entry. If the Connections tab is not selected, a submenu, which lists all available connection entries, is displayed.

■ Disconnect—Disconnect your current VPN session.

■ Create Shortcut—Create a shortcut on your desktop for the current connection entry.

■ Modify—Edit the current connection entry.

■ Delete—Delete the current connection entry.

■ Duplicate—Duplicate the selected connection entry. This menu choice lets you create a new connection entry using the configuration from a current connection entry as a template.

■ Set as Default Connection Entry—Make the current connection entry the default.

■ New—Create a new connection entry.

■ Import—Bring in a new connection entry profile from a file.

■ Exit VPN Client—Close the Cisco VPN Client application.

**Menus—Status**
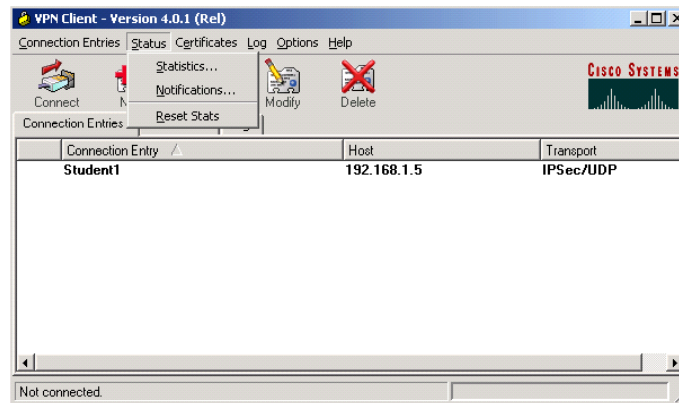
Use the Status menu to display routes and notifications and to reset the statistics display. The following commands are available:

- Statistics—View tunnel details, route details, and firewall information for the current VPN session.

- Notifications—View notices from the VPN device you are currently connected to.

- Reset Stats—Clear the statistics from the statistics displays and start over.

## Menus—Certificates

Cisco.com

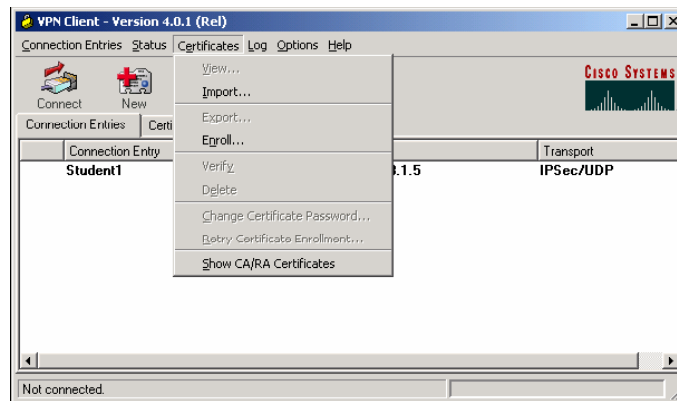VPN Client - Version 4.0.1 (Rel)

Connection Entries  Status  Certificates  Log  Options  Help

View...
Import...
Export...
Enroll...
Verify
Delete
Change Certificate Password...
Retry Certificate Enrollment...
Show CA/RA Certificates

CISCO SYSTEMS

Connect   New

Connection Entries | Certi

| Connection Entry | | Transport |
|---|---|---|
| Student1 | 1.1.5 | IPSec/UDP |

Not connected.

CSVPN 4.0—5-58

Use the Certificates menu to enroll and manage certificates. The following commands are available:

■ View—Display the properties of the selected certificate.

■ Import—Import a certificate file from a specified file location.

■ Export—Export the selected certificate to a specified file location.

■ Enroll—Enroll with a Certificate Authority (CA) to obtain a certificate.

■ Verify—Verify that a certificate is still valid.

■ Delete—Remove the selected certificate.

■ Change Certificate Password—Change the password that protects the selected certificate in the Cisco VPN Client certificate store.

■ Retry Certificate Enrollment—Retry a previously attempted certificate enrollment.

■ Show CA/RA Certificates—Display digital certificates issued by either a CA or a Registration Authority (RA).
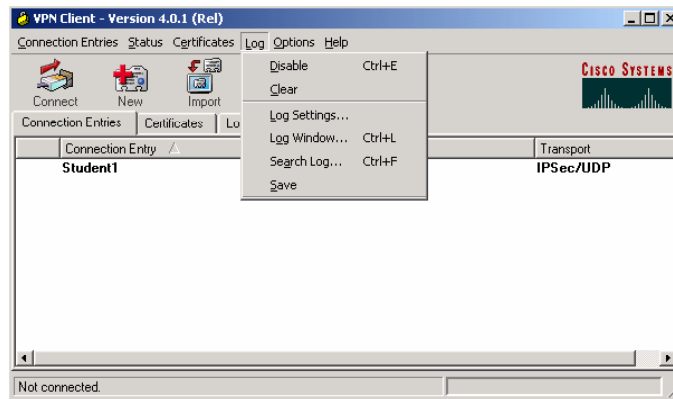
Use the Log menu to manage the log. The following commands are available:

■ Enable/Disable—Start collecting events (Enable); stop collecting events (Disable).

■ Clear—Erase the events displayed on the log tab (and log window).

■ Log Settings—Change the logging levels of event classes.

■ Log Window—Display a separate window that shows events. From this window you can save the display, edit logging levels by event class, and clear both log displays. This window shows more events than the display area of the main advanced mode window.

■ Search Log—Display a dialog box into which you enter the exact string to be matched. The search string is not case sensitive, and wild cards are not supported. Matched instances are highlighted on the log tab, not the log window.

■ Save—Store the current log in a specified log file.

## Menus—Options

Cisco.com

**VPN Client - Version 4.0.1 (Rel)**

Connection Entries  Status  Certificates  Log  Options  Help

Connect    New    Import

Application Launcher...
Windows Logon Properties...
✓ Stateful Firewall (Always On)
Simple Mode          Ctrl+M
Preferences...

Connection Entries | Certificates | Log

Connection Entry        Transport
  Student1              IPSec/UDP

Not connected.

© 2003, Cisco Systems, Inc. All rights reserved.                    CSVPN 4.0—5-60

Use the Options menu to perform actions such as launching an application. The following commands are available:

■ Application Launcher—Start an application before connecting to a VPN device.

■ Windows Logon Properties—Control logon features for the Windows NT platform. The following logon features are available:

— Ability to start a connection before logging on to a Windows NT system

— Permission to launch a third-party application before logging on to a Windows NT system

— Control of autodisconnect behavior when logging off

■ Stateful Firewall (Always On)—Enable and disable the internal stateful firewall.

■ Simple Mode—Switch to simple mode.

■ Preferences—Sets the following features:

— Save window settings—Save any changes you make to the Cisco VPN Client window.

— Hide upon connect—Place the Cisco VPN Client window in the dock when the VPN connection is established.

— Enable tool tips—Enable tool tips for the toolbar action buttons.

**Creating a New Connection—Authentication**

Clicking **New** from the toolbar or the Connection Entries menu displays the Create New VPN Connection Entry window. The following parameters need to be entered:
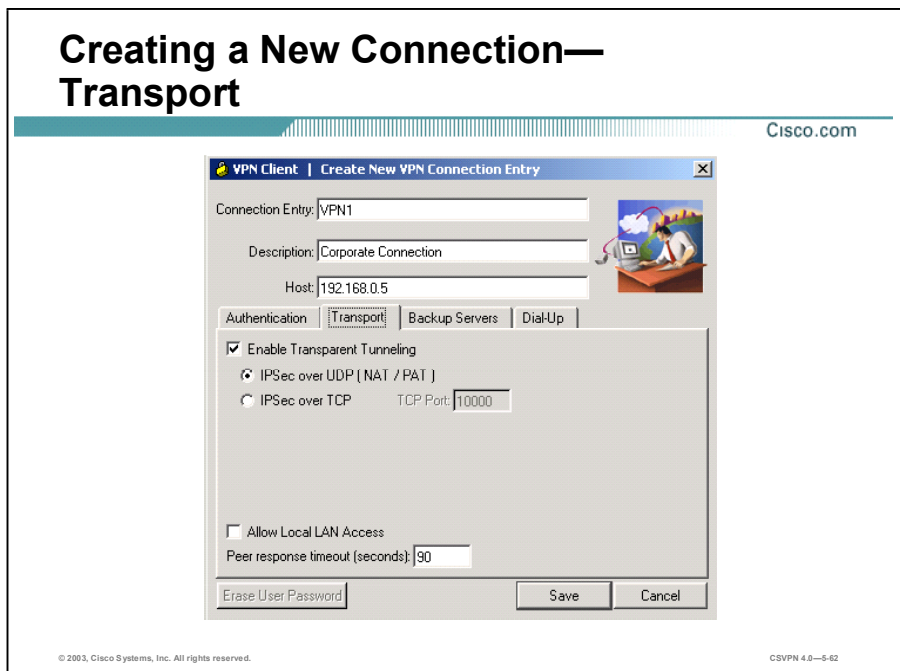
■ Enter a unique name for this new connection. You can use any name to identify this connection; for example, Engineering. This name can contain spaces, and it is not case sensitive.

■ Enter a description of this connection. This field is optional, but it helps further identify this connection. For example, Connection to Engineering remote server.

■ Enter the hostname or IP address of the remote VPN device you want to access.

Under the Authentication tab, you must choose whether you are going to be using group or certificate authentication and fill in the required fields as follows:

■ In the Name field, enter the name of the IPSec group to which you belong. This entry is case sensitive.

■ In the Password field, enter the password (which is also case sensitive) for your IPSec group. The field displays only asterisks.

■ Verify your password by entering it again in the Confirm Password field.

For certificates to be exchanged, the Certificate radio button must be selected. In the Name drop-down menu, any personal certificates loaded on your PC are listed. Choose the certificate to be exchanged with the Concentrator during connection establishment. If no personal certificates are loaded in your PC, the drop-down menu is blank. Use the Validate Certificate button to check the validity of the Software Client certificate.

**Creating a New Connection—
Transport**

Cisco.com

VPN Client | Create New VPN Connection Entry

Connection Entry: VPN1

Description: Corporate Connection

Host: 192.168.0.5

Authentication | Transport | Backup Servers | Dial-Up

☑ Enable Transparent Tunneling
  ⦿ IPSec over UDP ( NAT / PAT )
  ◯ IPSec over TCP    TCP Port: 10000

☐ Allow Local LAN Access
Peer response timeout (seconds): 90

Erase User Password    Save    Cancel

CSVPN 4.0—5-62

## Transparent Tunneling

Transparent tunneling allows secure transmission between the Cisco VPN Client and a secure
gateway through a router serving as a firewall, which may also be performing NAT or Port
Address Translation (PAT). Transparent tunneling encapsulates Protocol 50 (ESP) traffic
within UDP packets and can allow for both IKE (UDP 500) and Protocol 50 traffic to be
encapsulated in TCP packets before it is sent through the NAT or PAT devices or firewalls. The
most common application for transparent tunneling is behind a home router performing PAT.
The central-site group in the Cisco VPN device must be configured to support transparent
tunneling. This parameter is enabled by default. To disable this parameter, deselect the **Enable
Transparent Tunneling** check box under the Transport tab. It is recommended that you
always keep this parameter selected.

| Note | Not all devices support multiple simultaneous connections behind them. Some cannot map additional sessions to unique source ports. Be sure to check with the vendor of your device to verify whether this limitation exists. Some vendors support Protocol 50 (ESP) PAT (IPSec pass-through), which might let you operate without enabling transparent tunneling. |
|------|------|

You must choose a mode of transparent tunneling, over UDP or over TCP. The mode you use
must match that used by the secure gateway to which you are connecting. Either mode operates
properly through a PAT device. Multiple simultaneous connections might work better with
TCP. If you are in an extranet environment, then in general, TCP mode is preferable. UDP does
not operate with stateful firewalls, so in that case, you should use TCP.

The following transport tunneling options are available:

- Using IPSec over UDP (NAT/PAT)—To enable IPSec over UDP (NAT/PAT), select the **IPSec over UDP (NAT/PAT)** radio button. With UDP, the port number is negotiated. UDP is the default mode.

- Using IPSec over TCP (NAT/PAT/Firewall)—To enable IPSec over TCP, select the **Using IPSec over TCP** radio button. When using TCP, you must also enter the port number for TCP in the TCP port field. This port number must match the port number configured on the secure gateway. The default port number is 10000.

## Allowing Local LAN Access

In a multiple-NIC configuration, local LAN access pertains only to network traffic on the interface on which the tunnel was established. The Allow Local LAN Access parameter gives you access to the resources on your local LAN (printer, fax, shared files, and other systems) when you are connected through a secure gateway to a central-site VPN device. When this parameter is enabled and your central site is configured to permit it, you can access local resources while connected. When this parameter is disabled, all traffic from your Cisco VPN Client system goes through the IPSec connection to the secure gateway.

To enable this feature, select the **Allow Local LAN Access** check box; to disable it, deselect the check box. If the local LAN you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport.

A network administrator at the central site configures a list of networks at the VPN Client side that you can access. You can access up to ten networks when this feature is enabled. When local LAN access is allowed and you are connected to a central site, all traffic from your system goes through the IPSec tunnel except traffic to the networks excluded from doing so (in the network list).

When this feature is enabled and configured on the Cisco VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking at the Routes table.

## Adjusting the Peer Response Timeout Value

The Cisco VPN Client uses a keepalive mechanism called dead peer detection (DPD) to check the availability of the VPN device on the other side of an IPSec tunnel. If the network is unusually busy or unreliable, you might need to increase the number of seconds to wait before the Cisco VPN Client decides that the peer is no longer active. The default number of seconds to wait before terminating a connection is 90 seconds. The minimum number you can configure is 30 seconds, and the maximum is 480 seconds.

To adjust the setting, enter the number of seconds in the Peer response timeout (seconds) field. The Cisco VPN Client continues to send DPD requests every 5 seconds, until it reaches the number of seconds specified by the peer response timeout value.

# Creating a New Connection—Backup Servers

The private network may include one or more backup VPN servers to use if the primary server is not available. Your system administrator tells you whether to enable backup servers. Information on backup servers can download automatically from the Concentrator, or you can manually enter this information.

**Creating a New Connection—Dial-Up**

Cisco.com
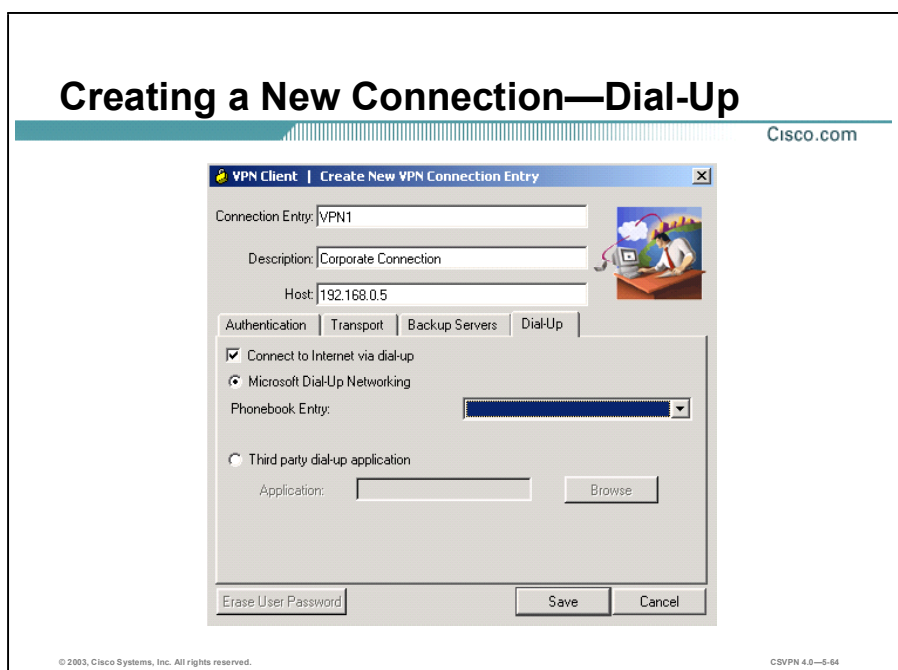
To enable and configure a connection to the Internet through dial-up networking, select the **Connect to Internet via dial-up** check box. This feature is not selected by default.

You can connect to the Internet using the Cisco VPN Client application in either of the following ways:

■ Microsoft Dial-Up Networking (DUN)—If you have DUN phonebook entries and have enabled the Connect to Internet via dial-up feature, Microsoft DUN is enabled by default. To link your Cisco VPN Client connection entry to a DUN entry, click the **Phonebook Entry** drop-down arrow and choose an entry from the menu. The Cisco VPN Client then uses this DUN entry to automatically dial into the Microsoft network before making the VPN connection to the private network.

■ Third-party dial-up program—If you have no DUN phonebook entries and have enabled the Connect to Internet via dial-up feature, then the third-party dial-up application is enabled by default. Click the **Browse** button to enter the name of the program in the Application field. This application launches the connection to the Internet. This string you choose or enter in this field is the path name to the command that starts the application and the name of the command; for example: c:\isp\ispdialer.exe dialEngineering. Your network administrator might have set this up for you. If not, consult your network administrator.

Pre-configure Client for Remote Users

An administrator has the ability to preconfigure Software Clients. A folder is placed on the remote user PC. Inside the folder is a copy of the Cisco VPN Client software plus three additional files:

- oem.ini—Installs the Software Client without user intervention.

- vpnclient.ini—A global profile that you use to set certain standards for all profiles. If this file is bundled with the Software Client software, it automatically configures the Software Client global parameters when it is first installed.

- .pcf—Creates connection entries within the dialer application. If this file is bundled with the Software Client software, it automatically configures the Cisco VPN Client connection parameters when it is first installed. There is one user profile for each .pcf file.

The administrator creates these files using a text editor and places them in the local file system of the remote user. The files must be located in the same folder as the Software Client setup.exe file.

| Note | The easiest way to create a profile for the Windows platforms is to run the Cisco VPN Client and use the Cisco VPN Client GUI to configure the parameters. When you have created a profile in this way, you can copy the .pcf file to a distribution disk for your remote users. This approach eliminates errors you might introduce by typing the parameters, and the group password is automatically converted to an encrypted format. |
| --- | --- |

.pcf File

.pcf file—User profile

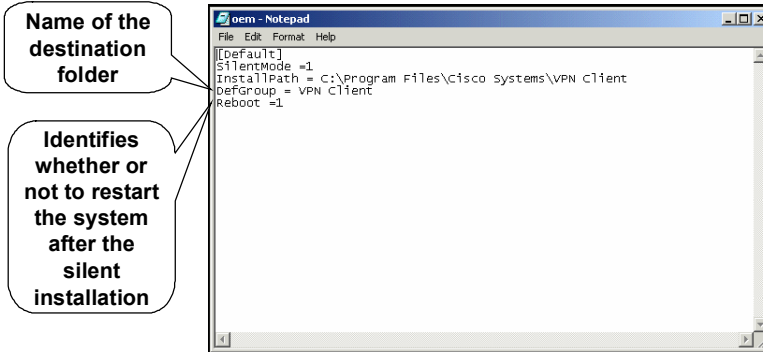The .pcf file contains all the Software Client configuration parameters. Profiles are created in two ways:

■ The remote user creates connection entries via the new-connection wizard. The output of the new-connection wizard is a .pcf file.

■ The administrator creates .pcf files using a text editor and places them in the local file system of the remote user: C:\ProgramFiles\CiscoSystems\VPN Client\Profiles directory.

Each connection has its own .pcf file. It can be viewed and edited in Notepad. If this file is bundled with the Software Client software, the installer automatically configures the Software Client when the Software Client is first installed.

To make a parameter read-only so that the Software Client user cannot change it within the GUI, put an exclamation mark (!) before the parameter name.

## Silent Mode

Name of the destination folder

Identifies whether or not to restart the system after the silent installation

```
[Default]
SilentMode =1
InstallPath = C:\Program Files\Cisco Systems\VPN Client
DefGroup = VPN Client
Reboot =1
```

**oem.ini—Installing the Cisco VPN Client without user intervention**

CSVPN 4.0—5-67

The oem.ini file installs the Software Client without user intervention. The administrator can create an oem.ini file in Notepad. Under SilentMode, enter **0** or **1**:

■  1—Activates silent installation (do not prompt user)

■  0—Prompts the user during installation

After the oem.ini file is created, identify the path name and folder to contain the Software Client software. The default path name to the Cisco VPN Client software is C:\ProgramFiles\CiscoSystems\VPN Client.

Last, reboot the system. Under Reboot, enter **1** or **2**:

■  If silent mode is on (1) and reboot is 1, the system automatically reboots after installation.

■  If silent mode is on (1) and reboot is 2, the system does not reboot after the installation.

**Client Program Menu**
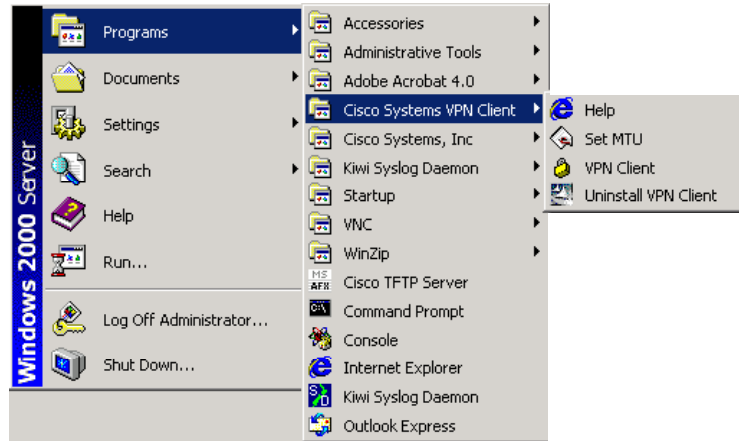
After the Software Client has been installed, access the Software Client program menu by choosing **Start>Programs>Cisco Systems VPN Client**. Under the Cisco Systems VPN Client menu, a number of options are available:

■ Help—Accesses Software Client help text. Help is also available by doing the following:

— Press **F1** at any window while using the Cisco VPN Client.

— Click the **Help** button on windows that display it.

— Click the logo in the title bar.

■ Set MTU—The Software Client automatically sets the MTU size to approximately 1420 bytes. For specific applications, Set MTU can change the MTU size to fit a specific scenario.

■ Uninstall Software Client—Only one Software Client can be loaded at a time. When you are upgrading, you must uninstall the old Software Client before installing the new Software Client. Choose **Uninstall VPN Client** to remove the old Software Client.

## Setting MTU Size

Cisco.com
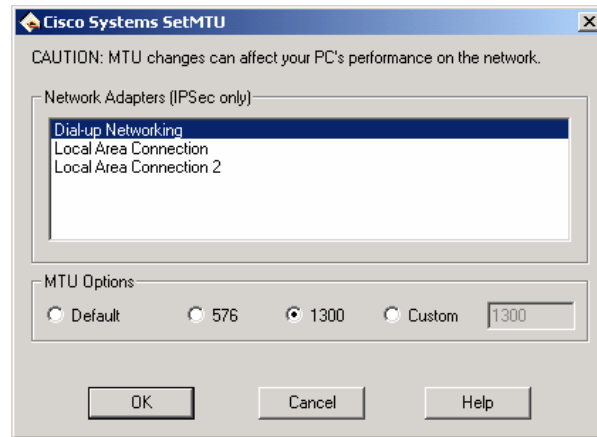
The Set MTU option is used primarily for troubleshooting connectivity problems. For specific applications where fragmentation is still an issue, Set MTU can change the MTU size to fit the specific scenario. The Cisco VPN Client automatically adjusts the MTU size to suit your environment, so running this application should not be necessary.

The MTU parameter determines the largest packet size in bytes that the client application can transmit through the network. If the MTU size is too large, the packets may not reach their destination. Adjusting the size of the MTU affects all applications that use the network adapter. Therefore, the MTU setting you use can affect the performance of your PC on the network. MTU sizing affects fragmentation of IPSec and IPSec through NAT mode packets to your connection destination. A large size (for example, more than 1300) can increase fragmentation. Using a size of 1300 or smaller usually prevents fragmentation. Fragmentation and reassembly of packets at the destination causes slower tunnel performance. Also, many firewalls do not let fragments through.

To implement a different MTU size, select the network adapter in the Network Adapters (IPSec only) field. In the example in the figure, Dial-up Networking is selected. In the MTU Options group box, set the MTU option size by clicking the appropriate radio button. You must reboot for MTU changes to take effect.

# Virtual Adapter

CSVPN 4.0—5-70
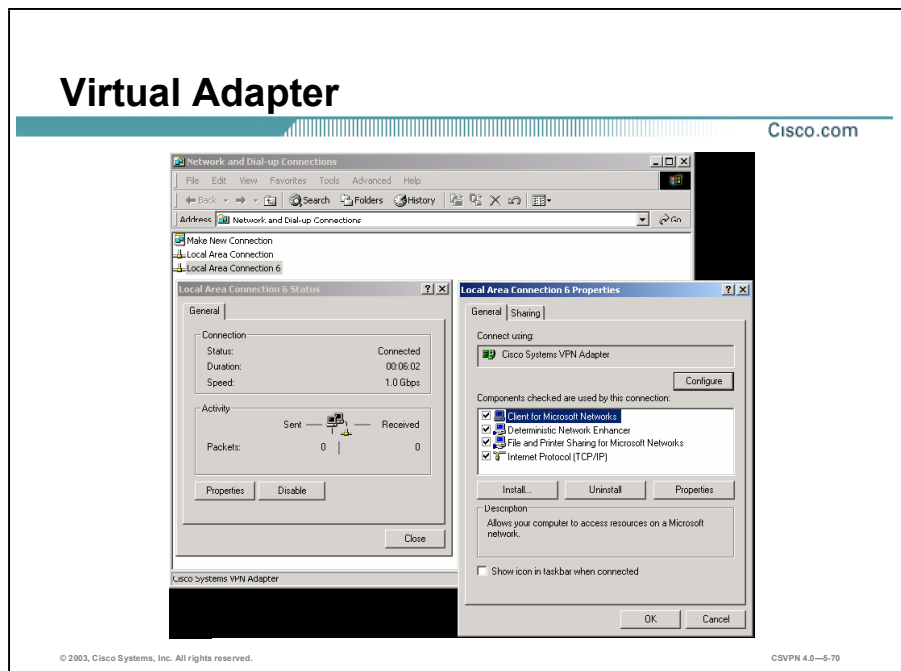
A virtual adapter is a software-only driver that acts as a valid interface in the system. Its purpose is to solve protocol incompatibility problems. The virtual adapter appears in the network properties list just like a physical adapter and displays all the information you would usually find under any other network adapter that is installed. It is available on Windows 2000 and XP only.

**Viewing Connected Clients—
Concentrator Connection Status**

The Monitor>Sessions window can be divided into four topics:

- Session Summary—Gives you an overview of all the sessions as well as total active, peak concurrent, and total concurrent sessions.

- LAN-to-LAN Sessions—Displays individual LAN-to-LAN sessions. In the example in the figure, there are currently no LAN-to-LAN sessions.

- Remote Access Sessions—Displays statistics on all the remote access sessions. In the example in the figure, there is currently one active session. The username is student1, and it belongs to the Training group. The virtual IP address assigned is 10.0.1.70, and the tunneling protocol is IPSec, using Triple-Data Encryption Standard (3DES) for encryption.

- Management Sessions—Displays information on all the current management users. In the example in the figure, the IP address of the admin user is 10.0.1.70.

**Viewing Connected Clients—Status Details**

The Monitor>Sessions window displays basic information about an individual session; however, more in-depth statistics may be required. By double-clicking the remote access username, the administrator can access session details. Session details provide specific IKE and IPSec session information and bandwidth statistics. They also provide a breakdown of the authentication modes, encryption and hash algorithms, DH groups, and rekey intervals for both the IKE and IPSec sessions.

# Summary

This topic summarizes what you learned in this lesson.

## Summary

- **The initial configuration of the Cisco VPN 3000 Series Concentrator occurs via the CLI.**
- **Subsequent configuration of the Cisco VPN 3000 Series Concentrator can be performed using a browser.**
- **Groups and users are used to assign access and usage rights.**
- **IPSec policies are assigned to groups.**

CSVPN 4.0—5-74

# Summary (cont.)

- **Mode configuration enables the Cisco VPN 3000 Series Concentrator to push the network information to the Cisco VPN Software Client.**

- **The Cisco VPN 3000 Series Concentrator can use several different types of authentication servers.**

- **The Cisco VPN 3000 Series Concentrator provides extensive monitoring capabilities.**

CSVPN 4.0—5-75

# Lab Exercise—Configure the Cisco VPN 3000 Series Concentrator for Remote Access Using Pre-Shared Keys

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to install and configure the Cisco VPN Client and the Cisco VPN 3000 Series Concentrator to enable IPSec-encrypted tunnels using pre-shared keys. Work with your lab exercise partner to complete the following tasks:

- Complete the lab exercise setup.

- Install the Cisco VPN Client.

- Configure the Cisco VPN Client.

- Verify the Cisco VPN Client properties.

- Return the Concentrator to factory settings.

- Configure the Concentrator private interface using the CLI.

- Configure the Concentrator public interface using the CLI.

- Configure the Concentrator default gateway using the CLI.

- Configure the Concentrator using the Cisco VPN 3000 Series Concentrator Manager.

- Verify the Concentrator IKE proposal.

- Verify the Concentrator group parameters.

- Modify the Concentrator public filter.

- Apply the Concentrator public filter.

- Launch the Cisco VPN Client.

- Verify the Cisco VPN connection status.

- Monitor the Concentrator statistics.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



### Lab Visual Objective

Cisco.com

CSVPN 4.0—5-1
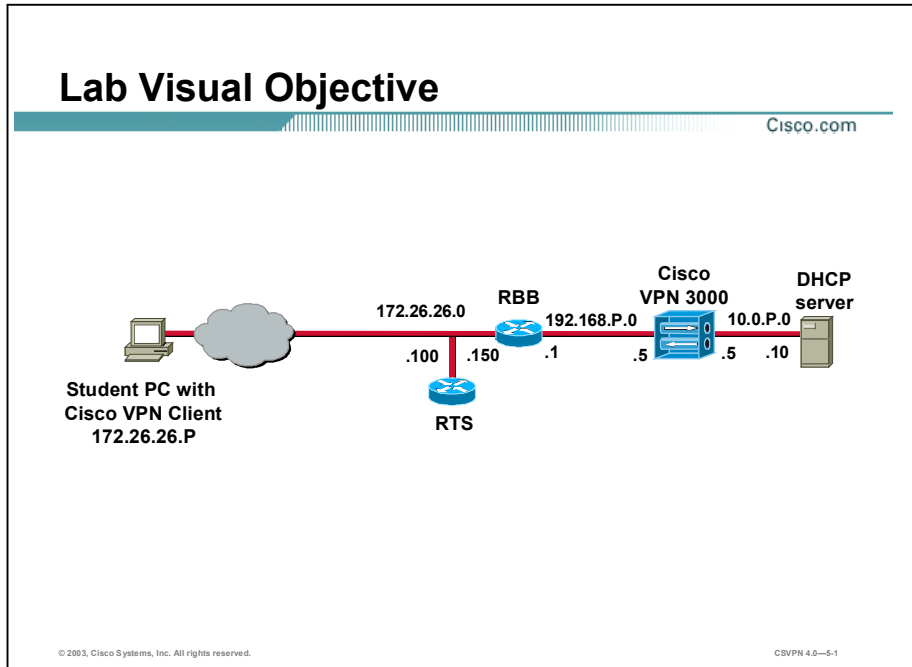
## Scenario

Your company wants to implement a VPN using remotely located Cisco VPN Clients terminating at centrally located Concentrators. You must configure both the remote Cisco VPN Clients and the Concentrators for remote access using pre-shared keys for authentication.

## Network Parameters Used in this Lab Exercise

The table contains the recommended device and interface IP addresses and subnet masks used in this lab exercise. Verify these values with your instructor before proceeding with the lab exercise.

| Parameter | IP Address | Subnet Mask |
|---|---|---|
| Student PC primary | 172.26.26.P | 255.255.255.0 |
| Student PC default gateway | 172.26.26.150 | |
| Concentrator public interface | 192.168.P.5 | 255.255.255.0 |
| Concentrator private interface | 10.0.P.5 | 255.255.255.0 |
| DHCP server | 10.0.P.10 | |
| Remote terminal server | 172.26.26.100 | |
| Backbone router | 192.168.P.1 | |
| Backbone router | 172.26.26.150 | |

(where P = pod number)

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify that your equipment is set up as follows:

■ Ensure that your student PC is powered on.

■ Ensure that your student IP addresses are configured correctly:

— Primary IP address—172.26.26.P
(where P = pod number)

— Default gateway IP address—172.26.26.150

■ Ensure that your Concentrator is powered on.

■ Uninstall the Cisco VPN Client if it is installed. Choose **Start>Programs>Cisco Systems VPN Client>Uninstall VPN Client** to remove the Cisco VPN Client. Respond to the questions appropriately.

## Task 2—Install the Cisco VPN Client

The Cisco VPN Client is typically installed from the Cisco VPN 3000 Series Concentrator CD-ROM, using the instructions supplied with the CD-ROM. In this lab exercise, the source files for the Cisco VPN Client already reside on the hard disk drive of the student PC. Complete the following steps to install the Cisco VPN Client:

**Step 1** Open the Cisco VPN Client folder found on the student PC desktop.

**Step 2** Double-click the **setup.exe** file from the Cisco VPN Client folder. If this is the first time that the Cisco VPN Client is being installed on this PC, a window opens and displays the following message: Do you want the installer to disable the IPSec Policy Agent?

**Step 3** If the disable IPSec policy agent message appears, click **Yes**. The Welcome window opens.

**Step 4** Read the Welcome window and click **Next**. The License Agreement window opens.

**Step 5** Read the license agreement and click **Yes**. The Destination Folder Location window opens.

**Step 6**  Accept the defaults by clicking **Next**. The Program Folders window opens.

**Step 7**  Accept the defaults by clicking **Next**. The Start Copying Files window opens.

**Step 8**  The files are copied to the hard disk drive of the student PC and the InstallShield Wizard Complete window opens.

**Step 9**  Select **Yes, I want to restart my computer now,** and click **Finish**. The student PC restarts.

**Step 10**  Log in to the student PC.

**Step 11**  Close the Cisco VPN Client folder.

## Task 3—Configure the Cisco VPN Client

Complete the following steps to configure the networking parameters of the new Cisco VPN Client:

| Note | This procedure assumes that Windows 2000 is already running on the student PC. |
|------|-------------------------------------------------------------------------------|

**Step 1**  Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.

**Step 2**  Click **New**. The Create New VPN Connection Entry window opens.

**Step 3**  Enter **studentP** in the Connection Entry field.
(where P = pod number)

**Step 4**  Leave the description field blank.

**Step 5**  Enter a Concentrator public interface IP address in the Host field: **192.168.P.5**.
(where P = pod number).

**Step 6**  Verify that the **Group Authentication** radio button is selected and complete the substeps listed here.

The following entries are always case sensitive. Use lowercase characters for this lab exercise.

1.  Enter a group name: training.

2.  Enter a group password: training.

3.  Confirm the password: training.

**Step 7**  Click **Save** and leave the Cisco Systems VPN Client window open.

## Task 4—Verify the Cisco VPN Client Properties

Complete the following steps to verify the Cisco VPN Client parameters you just configured:

**Step 1**  Ensure that the Cisco VPN Client window is open. If the Cisco VPN Client window is not open, choose: **Start>Programs>Cisco Systems VPN Client> VPN Client**.

**Step 2**  Select **studentP** within the Connection Entry group box and click **Modify**.
(where P = pod number)

**Step 3**  Verify that the IP address of the remote server is set to a Concentrator public interface IP address: **192.168.P.5**.
(where P = pod number)

**Step 4** Select the **Authentication** tab and verify the spelling of the group name. If necessary, you can edit the group name and password here.

**Step 5** Select the **Transport** tab and view the available options. Do not make any changes to the default settings.

**Step 6** Click **Save** if you have made any changes.

**Step 7** Close the Cisco Systems VPN Client window.

## Task 5—Return the Concentrator to Factory Settings

The instructor will provide you with the procedures for access to the Concentrator console port, because this procedure will vary according to your connectivity. After you access the Concentrator console port, the Concentrator login prompt will appear. Complete the following steps to return the Concentrator to the factory settings:

| Note | This procedure assumes that Windows 2000 is already running on the student PC. |
|------|--------------------------------------------------------------------------------|

**Step 1** Log in to the Concentrator CLI using the administrator account:

```
Login: admin

Password: admin
```

If you get a Quick prompt for the system time or date parameters, the device has already been rebooted to factory defaults. In that case, skip this task and proceed directly to Task 6.

**Step 2** Access the Administration menu:

```
Main -> 2
```

**Step 3** Access the System Reboot menu:

```
Admin -> 3
```

**Step 4** Access the Schedule Reboot menu:

```
Admin -> 2
```

**Step 5** Select Reboot ignoring the Configuration file:

```
Admin -> 3
```

**Step 6** Select Reboot Now:

```
Admin -> 2
```

The Reboot scheduled immediately message appears, followed by the Rebooting VPN 3000 Series Concentrator now message. Do not attempt to log in to the first login prompt you see because it takes several moments for the Concentrator to complete the reboot function. A login prompt appears when the reboot is complete.

**Step 7** Leave the CLI session open.

## Task 6—Configure the Concentrator Private Interface Using the CLI

Complete the following steps to configure the Concentrator private LAN interface using the CLI Quick Configuration mode:

| | Note | This procedure assumes that the CLI session is still active from the previous task. If the CLI session is not active, complete steps 1–6 of the previous task before proceeding. |

**Step 1** Log in to the Concentrator CLI using the administrator account:

```
Login: admin
Password: admin
```

| | Note | When an administrator reboots a Concentrator CLI, as in the previous task, menus open in a slightly different order. If the system parameters prompt appears, press **Enter** through the time, date, time zone, and Daylight Savings Time (DST) prompts to accept the default values. |

**Step 2** Enter the Concentrator private interface IP address:

```
Quick Ethernet 1 -> [0.0.0.0] 10.0.P.5
```

(where P = pod number)

**Step 3** Enter the Concentrator private interface subnet mask:

```
Quick Ethernet 1-> [255.0.0.0] 255.255.255.0
```

**Step 4** Accept the default Ethernet speed of 10/100 Mbps Auto Detect:

```
Quick Ethernet 1-> [3] <Enter>
```

**Step 5** Accept the default duplex mode of Auto:

```
Quick Ethernet 1-> [1] <Enter>
```

**Step 6** Accept the default MTU size:

```
Quick Ethernet 1-> [1500] <Enter>
```

**Step 7** Save the changes to the configuration file:

```
Quick -> 3
```

**Step 8** Exit the CLI:

```
Quick -> 5
```

If you do not exit, the CLI continues its quick configuration script. You will use the standard CLI menus for the remaining parameters.

**Step 9** Leave the CLI session open.

## Task 7—Configure the Concentrator Public Interface Using the CLI

Complete the following steps to configure the Concentrator public interface:

**Step 1** Log in to the Concentrator CLI using the administrator account:

```
Login: admin
Password: admin
```

**Step 2** Select the Configuration menu:

```
Main -> 1
```

**Step 3** Select the Interface Configuration menu:

```
Config -> 1
```

**Step 4**    Select the Configure Ethernet #2 (Public) menu:

```
Interfaces -> 2
```

**Step 5**    Select the Interface Setting menu:

```
Ethernet Interface 2 -> 1
```

**Step 6**    Accept the default setting to Enable using Static IP Addressing:

```
Ethernet Interface 2 -> [3] <Enter>
```

**Step 7**    Enter the Concentrator public interface IP address:

```
Ethernet Interface 2 -> [0.0.0.0] 192.168.P.5
```

(where P = pod number)

**Step 8**    Accept the default setting for the subnet mask:

```
Ethernet Interface 2 -> [255.255.255.0] <Enter>
```

---

| **Note** | Several messages appear, indicating the condition of the Ethernet #2 (public) interface. Disregard the messages. |
|---|---|

---

**Step 9**    Select the Select IP Filter menu:

```
Ethernet Interface 2-> 3
```

**Step 10**    Select **0** (no filter) on the Ethernet #2 (public) interface:

```
Ethernet Interface 2 -> [Public (Default)] 0
```

---

| **Note** | In this lab exercise, you have disabled filtering on the public LAN interface to allow access to the HTTP-based Cisco VPN 3000 Series Concentrator Manager from your student PC. Never select **0** (no filter) in a live network, because doing so could facilitate a security breach. |
|---|---|

---

**Step 11**    Return to the top-level menu by using the following shortcut:

```
Ethernet Interface 2 -> h
```

**Step 12**    Save changes to the configuration file:

```
Main -> 4
```

**Step 13**    Do not exit the CLI. Leave the Command Prompt window open, because it will be used to complete the tasks that follow.

## Task 8—Configure the Concentrator Default Gateway Using the CLI

Complete the following steps, starting from the CLI top-level menu, to set the default gateway parameter of the Concentrator to the IP address of the backbone router:

**Step 1**    Select the Configuration menu:

```
Main -> 1
```

**Step 2**    Select the System Management menu:

```
Config -> 2
```

**Step 3**    Select the IP Routing menu:

```
System -> 4
```

**Step 4**  Select the Default Gateways menu:

```
Routing -> 2
```

**Step 5**  Select the Set Default Gateway menu:

```
Routing -> 1
```

**Step 6**  Enter the backbone router IP address:

```
Routing -> 192.168.P.1
```

(where P = pod number)

**Step 7**  Select the Set Default Gateway Metric menu:

```
Routing -> 2
```

**Step 8**  Accept the Default Gateway Routing Metric of 1:

```
Routing -> [1] <Enter>
```

**Step 9**  Return to the top-level menu by using the following shortcut:

```
Routing -> h
```

**Step 10**  Save changes to the configuration file:

```
Main -> 4
```

**Step 11**  Exit the CLI session:

```
Main -> 6
```

**Step 12**  Close the Command Prompt window.

# Task 9—Configure the Concentrator Using the Cisco VPN 3000 Series Concentrator Manager

Earlier you configured both the private and public interfaces using the CLI feature of the Concentrator. Complete the following steps to finish the Concentrator configuration using the Cisco VPN 3000 Series Concentrator Manager:

---

| **Note** | This procedure assumes that Windows 2000 is already running on the student PC. |
| --- | --- |

---

**Step 1**  Launch Internet Explorer by double-clicking the desktop icon.

**Step 2**  Enter a Concentrator public interface IP address in the Internet Explorer Address field: **192.168.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Series Concentrator Manager.

**Step 3**  Log in to the Cisco VPN 3000 Series Concentrator Manager using the administrator account:

```
Login: admin
Password: admin
```

---

| **Note** | The username (login) and password are always case sensitive. |
| --- | --- |

---

**Step 4**  In the main window, click the **click here to start Quick Configuration** link.

**Step 5**  From the Configuration>Quick>IP Interfaces window, complete the following substeps:

1. Verify the IP addresses of Ethernet 1, **10.0.P.5**, and Ethernet 2, **192.168.P.5**, which you configured via the CLI (where P = pod number).

2. Click **Apply** if you have made changes to either interface 1 or 2; otherwise, click **Continue**.

**Step 6** From the Configuration>Quick>System Info window, complete the following substeps:

1. Enter **vpnP** in the System Name field.
(where P = pod number)

Your instructor will provide you with the values to complete the following table:

| Parameter | Value |
| --- | --- |
| Time (Hour:Minute:Second AM/PM) (for example, 2:45:00 PM.) | |
| Date (Month/Day/Year) (for example, July/6/2001.) | |
| Time zone (offset in hours from GMT) (for example, (GMT–05:00) EST.) | |
| Enable DST Support? (circle one) | SELECT          DE-SELECT |

2. In the System Info window, enter the correct time, date, and time zone from the previous table.

3. Check or uncheck the **Enable DST Support** check box, depending on which action has been circled in the previous table.

4. Leave the DNS Server IP Address field set to: **0.0.0.0**.

5. Enter **cisco.com** in the Domain field.

6. Leave a backbone router IP address in the Default Gateway field: **192.168.P.1**.
(where P = pod number)

7. Click **Continue**.

**Step 7** From the Configuration>Quick>Protocols window, complete the following substeps:

1. Uncheck the **PPTP** check box.

2. Uncheck the **L2TP** check box.

3. Check the **IPSec** check box.

4. Click **Continue**.

**Step 8** From the Configuration>Quick>Address Assignment window, complete the following substeps:

1. Select **DHCP**.

2.  Enter a DHCP server IP address in the Specify Server field: **10.0.P.10**.
    (where P = pod number)

3.  Click **Continue**.

**Step 9**  From the Configuration>Quick>Authentication window, complete the following:

1.  Verify that **Internal Server** is selected from the Server Type drop-down menu.

2.  Click **Continue**.

**Step 10**  From the Configuration>Quick>User Database window, complete the following substeps:

| | |
|---|---|
| **Note** | These entries are all case sensitive. Create all entries in lowercase form only. |

1.  Enter **studentP** in the User Name field.
    (where P = pod number)

2.  Enter **studentP** in the Password field.
    (where P = pod number)

3.  Enter **studentP** in the Verify field.
    (where P = pod number)

4.  Click **Add** to add the new user to the database. The new username should appear in the
    Current Users window.

5.  Click **Continue**.

**Step 11**  From the Configuration>Quick>IPSec Group window, complete the following substeps:

| | |
|---|---|
| **Note** | These entries are all case sensitive. Create all entries in lowercase form only. |

1.  Enter **training** in the Group Name field.

2.  Enter **training** in the Password field.

3.  Enter **training** in the Verify field.

4.  Click **Continue**.

**Step 12**  From the Configuration>Quick>Admin Password window, click **Continue**. Normally you would
change your password, but for lab exercise consistency, leave the password at the default value.

**Step 13**  From the Configuration>Quick>Done window, complete the following substeps:

1.  Click the **Save Needed** icon, in the upper right corner of the window. The Save Successful
    window opens.

2.  Click **OK**.

**Step 14**  Leave Internet Explorer open and continue to the next task.

## Task 10—Verify the Concentrator IKE Proposal

Complete the following steps to verify the IPSec IKE proposal:

**Step 1**    From the Configuration menu tree, choose **System>Tunneling Protocols>IPSec>IKE Proposals**.

**Step 2**    Ensure that the **CiscoVPNClient-3DES-MD5** proposal appears first under the Active Proposals list.

**Step 3**    If you need to make changes, click the **Save Needed** icon. Always select **CiscoVPNClient-3DES-MD5** when using the Cisco VPN 3.x or 4.x Client. Always select **IKE-3DES-MD5** when using the Cisco VPN 2.5 Client.

**Step 4**    Leave Internet Explorer open and continue to the next task.

## Task 11—Verify the Concentrator Group Parameters

Complete the following steps to verify the Concentrator group parameters you set earlier:

**Step 1**    From the Configuration menu tree, choose **User Management>Groups**.

**Step 2**    Choose **training** from the Current Groups list.

**Step 3**    Click **Modify Group**. It may take a few moments for the text to appear.

**Step 4**    Select the **Identity** tab.

**Step 5**    Verify that Group Name is set to **training**.

**Step 6**    Select the **IPSec** tab.

**Step 7**    Verify that Authentication is set to **Internal**.

**Step 8**    Scroll to the bottom of the window, and click **Cancel**.

**Step 9**    Leave Internet Explorer open and continue to the next task.

## Task 12—Modify the Concentrator Public Filter

Filtering must be enabled on the public interface in order for the Cisco VPN Client to connect to the Concentrator. By definition, the filter permits only tunnel and ICMP traffic to pass through the interface. This filter excludes any HTTP traffic from your student PC. However, for this lab exercise, the public filter can be modified to permit HTTP traffic to travel both inbound and outbound. With a modified filter, you can configure and monitor the network from the public side of the network. Complete the following steps to modify the public filter of the Concentrator:

| | |
|---|---|
| **Note** | This task is for lab exercise purposes only. For security reasons, this task should never be completed in a production environment. |

**Step 1**    From the Configuration menu tree, choose **Policy Management>Traffic Management>Filters**.

**Step 2**    Choose the **Public (Default)** filter from the Filter list.

**Step 3**    Click **Assign Rules to Filter** within the Actions group box.

**Step 4**    Choose **Incoming HTTP In (forward/in)** from the Available Rules list.

**Step 5**    Click **Add**.

**Step 6**  Choose **Incoming HTTP Out (forward/out)** from the Available Rules list.

**Step 7**  Click **Add**.

**Step 8**  Click **Done**.

## Task 13—Apply the Concentrator Public Filter

For the Cisco VPN Client to connect to the Concentrator, filtering must be applied to the public interface. Earlier you temporarily set the public interface filter to 0 (none) so you could configure the Concentrator via HTTP. Complete the following steps to configure the public interface in the same way with one exception: instead of setting the IP filter to **0** (none), set it to **2** (public):

**Step 1**  From the Configuration menu tree, choose **Interfaces>Ethernet 2 (Public)**.

**Step 2**  Select the **General** tab.

**Step 3**  Choose **Public (Default)** from the Filter drop-down menu.

**Step 4**  Click **Apply**.

**Step 5**  Save the changes to the configuration.

**Step 6**  Log out of the Concentrator.

**Step 7**  Close Internet Explorer.

## Task 14—Launch the Cisco VPN Client

Complete the following steps to launch the Cisco VPN Client on your student PC and create an IPSec tunnel:

**Step 1**  Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 2**  Verify that the connection entry is **studentP**.
(where P = pod number)

**Step 3**  Verify that the IP address of the remote server is set to that of a Concentrator public interface IP address: **192.168.P.5**.
(where P = pod number)

**Step 4**  Click **Connect**. Complete the following substeps:

1.  When prompted for a username, enter **studentP**.
(where P = pod number)

2.  When prompted to enter a password, enter **studentP**.
(where P = pod number)

**Step 5**  Click **OK**. The following messages flash by quickly at the bottom of the window:

```
Initializing the connection
Contacting the security gateway at
Authenticating user
```

The window closes and a Cisco VPN Client icon appears in the system tray.

## Task 15—Verify the Cisco VPN Connection Status

A Cisco VPN Client Connection Status window is available to the end user. By double-clicking the Cisco VPN Client icon, the end user can view general connection information and connection statistics. Complete the following steps to view the Cisco VPN Client connection information:

**Step 1**  Double-click the Cisco VPN Client icon in the system tray and answer the following questions:

Q1)  What window opened?

A)  _____

**Step 2**  Select the **Status>Statistic**s**…** menu option and answer the following questions.

Q2)  What encryption scheme was used?

A)  _____

Q3)  What authentication method was used?

A)  _____

Q4)  What client IP address was assigned to you?

A)  _____

**Step 3**  Click **Close**.

## Task 16—Monitor the Concentrator Statistics

Remote access information is available on the Concentrator. The administrator can view event messages that detail the connection process from start to finish. Once established, the administrator can view session statistics. Complete the following steps to monitor the Concentrator statistics:

**Step 1**  Launch Internet Explorer.

**Step 2**  Enter a Concentrator private interface IP address in the Internet Explorer Address field: **10.0.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Series Concentrator Manager.

**Step 3**  Log in to the Cisco VPN 3000 Series Concentrator Manager using the administrator account:

```
Login: admin
Password: admin
```

**Step 4**  From the Monitoring menu, choose **Routing Table**.

Q5)  Which networks are visible?

A)  _____

**Step 5**  From the Monitoring menu, choose **Filterable Event Log**.

**Step 6**  Click **Clear Log**.

**Step 7**  Disconnect your VPN session if it is still active by using the Cisco VPN Client icon in the system tray of the student PC.

**Step 8**  Re-establish your VPN session.

**Step 9**  From the Monitoring menu, choose **Filterable Event Log**.

**Step 10**  Click the |<< button and answer the following questions:

Q6)  What is the group name of the remote client?

A)  _____

Q7)  What is the username of the remote client?

A)  _____

Q8)  What SA is the IKE remote peer configured for?

A)  _____

**Step 11**  From the Monitoring menu, choose **Sessions** and answer the following question:

Q9)  Fill in the blanks:

A)  Username _____

B)  Assigned IP address _____

C)  Public IP address _____

D)  Group _____

E)  Protocol _____

F)  Encryption _____

G)  Login time _____

H)  Duration _____

I)  Client type _____

J)  Client version _____

**Step 12**  Select **studentP** (where P = pod number). More information is displayed. Use this information to answer the following questions:

Q10)  The IKE session used:

A)  Encryption algorithm: _____

B)  Hashing algorithm: _____

Q11)    The IPSec session identification (ID2) used:

    A)    Remote address: _____

    B)    Local address: _____

    C)    Encryption algorithm: _____

    D)    Hashing algorithm: _____

**Step 13**  Log out of the Concentrator.

**Step 14**  Disconnect your VPN session if it is still active by using the Cisco VPN Client icon in the student PC system tray).

**Step 15**  Close Internet Explorer.

---

| **Warning** | It is very important that you log out of the Cisco VPN 3000 Series Concentrator Manager when finished. Failing to log out before exiting the manager interface leaves an administrator session open. Eventually, all possible administrator sessions will be used, and you will not be allowed to log in again. Also, only the first administrator session has read and write access. The remaining administrator sessions have read-only access. |
| --- | --- |

**6**

# Configure the Cisco Virtual Private Network 3000 Series Concentrator for Remote Access Using Digital Certificates

## Overview

This lesson teaches how to configure the Cisco Virtual Private Network (VPN) 3000 Series Concentrator for remote access using digital certificates for authentication. After presenting an overview of the process, the lesson shows you each major step of the configuration. It includes the following topics:

■ Objectives

■ CA support overview

■ Certificate generation

■ Validating certificates

■ Configuring the Cisco VPN 3000 Series Concentrator for CA support

■ Summary

■ Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

Cisco.com

**Upon completion of this lesson, you will be able to perform the following tasks:**

- Explain the purpose of digital certificates.
- Generate a PKCS #10 for the Cisco VPN Client and Concentrator.
- Install certificates in the Cisco VPN Client and Concentrator.
- Explain how digital certificates are validated and maintained.
- Configure the Cisco VPN Client and Concentrator for certificate-based remote access.

CSVPN 4.0—6-2

# CA Support Overview

The topic presents an overview of how Certificate Authority (CA) support works.

## CA Server Fulfilling Requests from IPSec Peers

**Each IPSec peer individually enrolls with the CA server.**

**CA server**

CSVPN 4.0—6-4
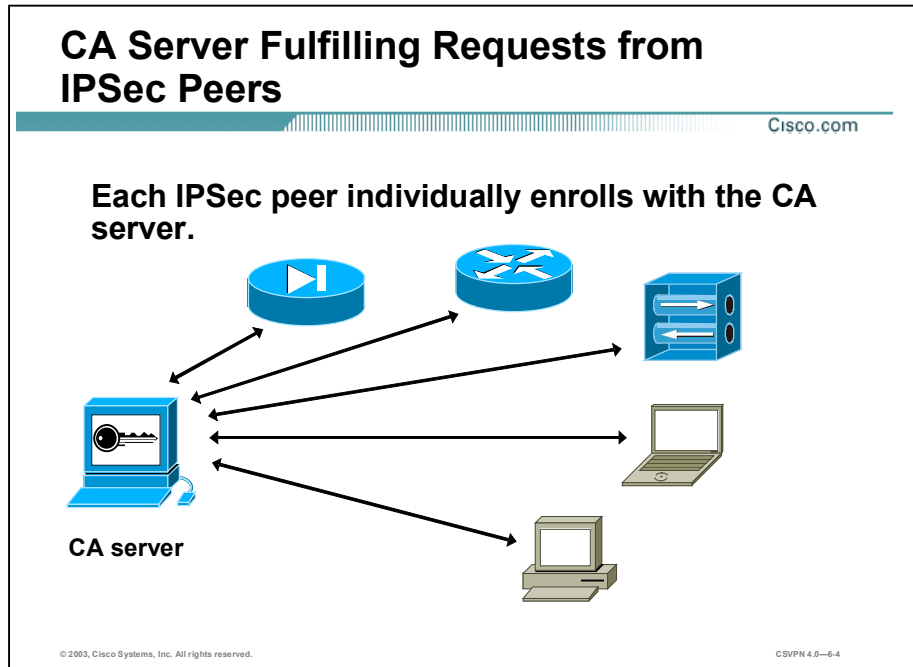
With a CA, you do not need to configure keys between all of the encrypting IPSec peers. Instead, you individually enroll each participating peer with the CA and request a certificate. When this has been accomplished, each participating peer can dynamically authenticate all of the other participating peers. To add a new IPSec peer to the network, you need to configure only that new peer to request a certificate from the CA, instead of making multiple key configurations with all the other existing IPSec peers.

## Digital Signature

Cisco.com

**Local**

Pay to Terry Smith
$100.00
One Hundred and
xx/100   Dollars

4ehIDx67NMop9

**Internet**

**Encryption algorithm**

**Private key**

**Hash**

**Hash algorithm**

Pay to Terry Smith
$100.00
One Hundred and
xx/100   Dollars

**Remote**

Pay to Terry Smith
$100.00
One Hundred and
xx/100   Dollars

**Hash**

4ehIDx67NMop9

**Match**

**Decryption algorithm**

**Hash**

**Public key**

CSVPN 4.0—6-5
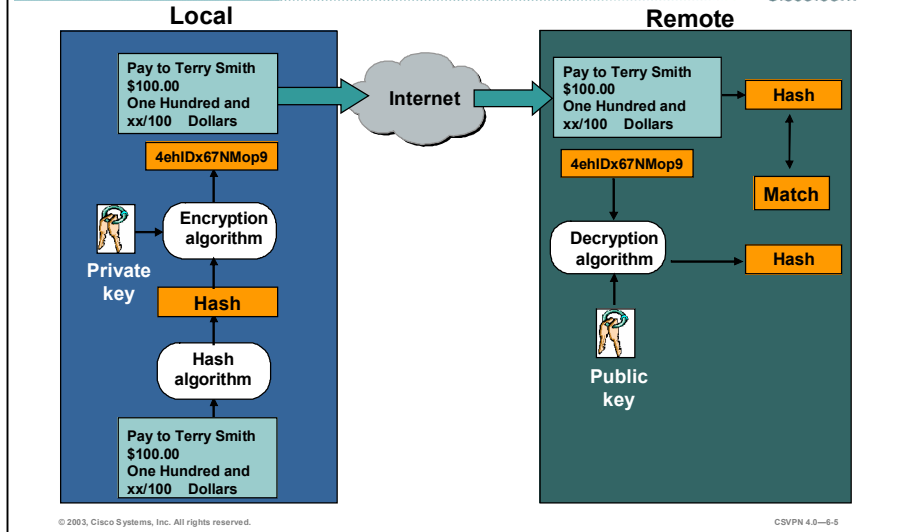
The digital signature provides a form of digital credentials that authenticate the identity of the sending party. Digital signatures are used to link data with the holder of a specific private key and consist of the following:

■ At the local end, a private key is used to encrypt the hash.

■ At the remote end:

— Running the original message through a hash algorithm produces the hash.

— The hash that was appended to the original message is decrypted using the sender's public key.

■ If the hashes match, the message was signed with the sender's private key.

■ Only a specific private key can produce the digital signature.

## Why Digital Certificates

Cisco.com
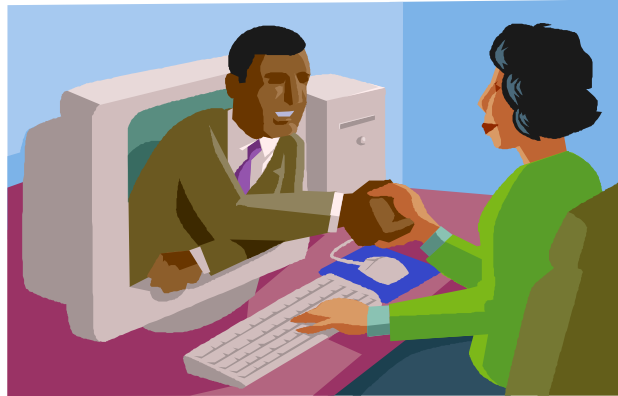
© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—6-6

A key pair has no intrinsic ties to any person or entity. A solution is necessary to reliably tie a person or entity to a key pair. The solution is digital signatures and digital certificates, which provide a way to guarantee the source of the message:

■ Digital signatures—Tie a message to a sender's private key, and the hash can be decrypted by only the sender's public key.

■ Digital certificates—Bind a person or entity to a private key. This is analogous to buying an item in a department store with a credit card. Typically, the cashier asks for a two items: a credit card and a picture identification. The credit card is swiped through the register to confirm that the account is valid, that it has not expired, and that it was not revoked. The picture identification is used to tie the customer to the credit card. Similarly, a digital certificate is used to bind a person or entity to a digital signature.

## Certificate-Based Authentication

Cisco.com

**CA trusted third party**

Terry — Request certificate → ← Request certificate — Alex

Issue certificates

Terry

Digital certificates

Alex

CSVPN 4.0—6-7
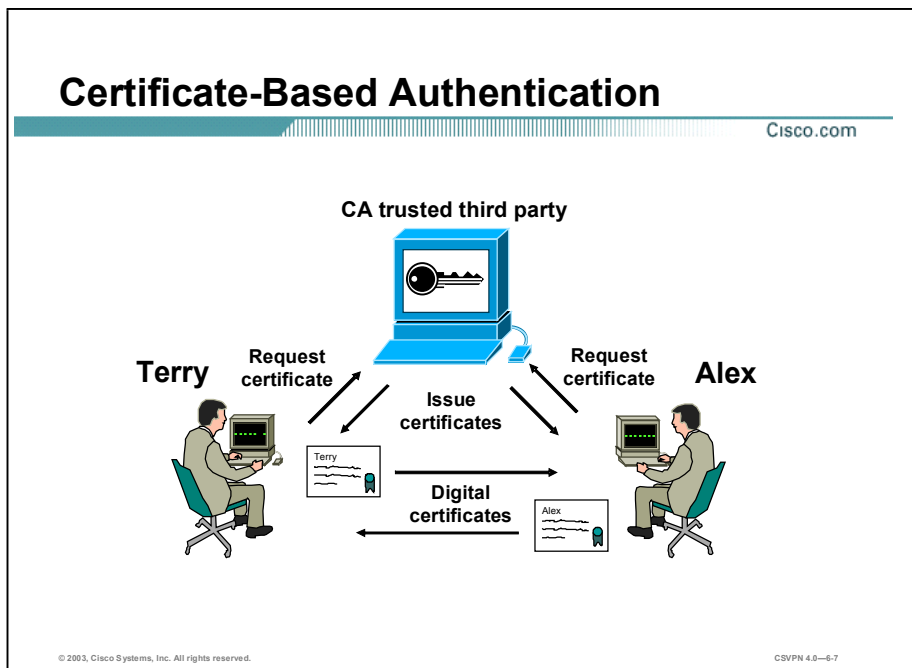
Digital certificates are used to authenticate users. They can be used to identify a person, company, or server. They are the equivalent of a passport or driver's license. The following example illustrates how this works:

**Step 1** User A and B register separately with the CA:

■ Each user generates a public and private key.

■ Certificate requests are completed by both users and forwarded to the CA.

■ A CA issues separate certificates and digitally signs them with its private key, thereby certifying the authenticity of the user.

■ Certificates are loaded and verified on both users PCs.

**Step 2** User A sends the certificate to user B.

**Step 3** User B checks the authenticity of the CA signature on the certificate:

■ The CA public key is used to verify the CA signature on the certificate.

■ If it passes validation, it is safe to assume you are who you say you are; therefore, the message is valid.

**Step 4** User B sends the certificate to user A:

■ The CA public key is used to verify the CA signature on the certificate.

■ When verified, all subsequent communications can be accepted.

| **Note** | Certificates are exchanged during the IPSec negotiations. |
| --- | --- |

# CA

**CA responsibilities:**
- **Create certificates**
- **Administer certificates**
- **Revoke invalid certificates**

CSVPN 4.0—6-8

Certification Authorities (CAs) hold the key to the Public Key Infrastructure (PKI). A CA is a trusted third party whose job is to certify the authenticity of users to ensure that you are who you say you are.

The CA digital signature, created with the CA private key, guarantees authenticity. You can verify a digital signature using the CA public key. Only the CA public key can de-crypt the digital certificate. The CA creates, administers, and revokes invalid certificates.

The CA can be a corporate network administrator or a recognized third party. Trusted sources supported by the Cisco VPN 3000 Series Concentrator include the following:

■ Entrust

■ RSA Security

■ Network Associates PGP

■ Baltimore

■ Microsoft

■ Verisign

**PKI**

CSVPN 4.0—6-9
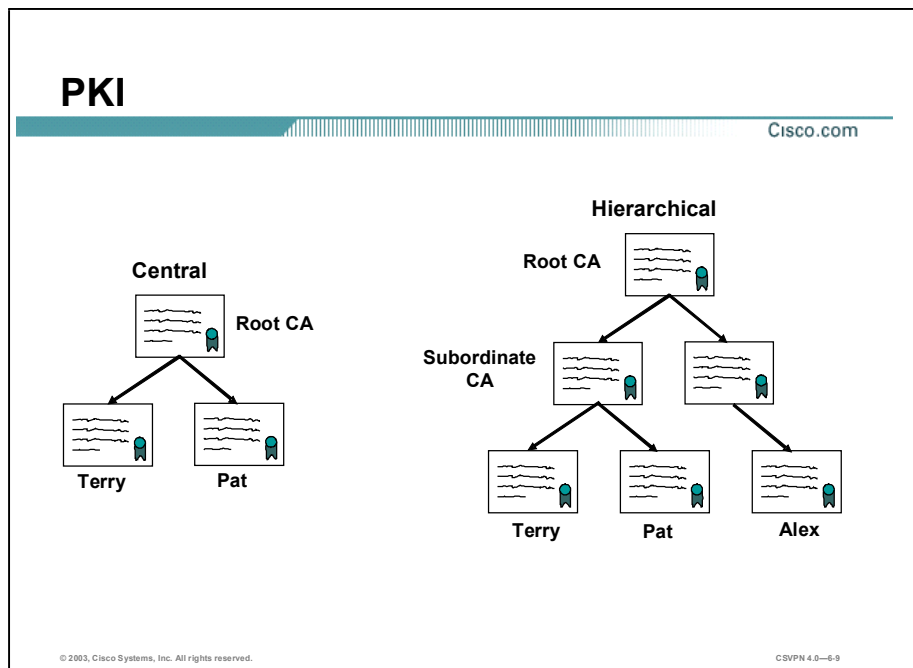
PKI is the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. PKI makes it possible to generate and distribute keys within a secure domain and enables CAs to issue keys, associated certificates, and certificate revocation lists (CRLs) in a secure manner. The two PKI models are central and hierarchical authorities:

■   Central—A flat network design. A single authority, root CA, signs all certificates. Each employee who needs a certificate sends a request to the root CA. Small companies with several hundred employees may use central CA.

■   Hierarchical authority—A tiered approach. The ability to sign a certificate is delegated through a hierarchy. The top of the hierarchy is the root CA. It signs certificates for subordinate authorities. Subordinate CAs sign certificates for lower level CAs or employees. Large geographically dispersed corporations (for example, Cisco Systems) use hierarchical CAs. The root CA is located in San Jose, the company headquarters. Rather than having more than 30,000 employees making certificate requests back to San Jose, subordinate CAs are placed strategically around the world. Local employees request a CA from the local subordinate CA.

# Certificate Generation

This topic discusses how certificates are generated and transferred between a CA and the Cisco VPN 3000 Series Concentrator.
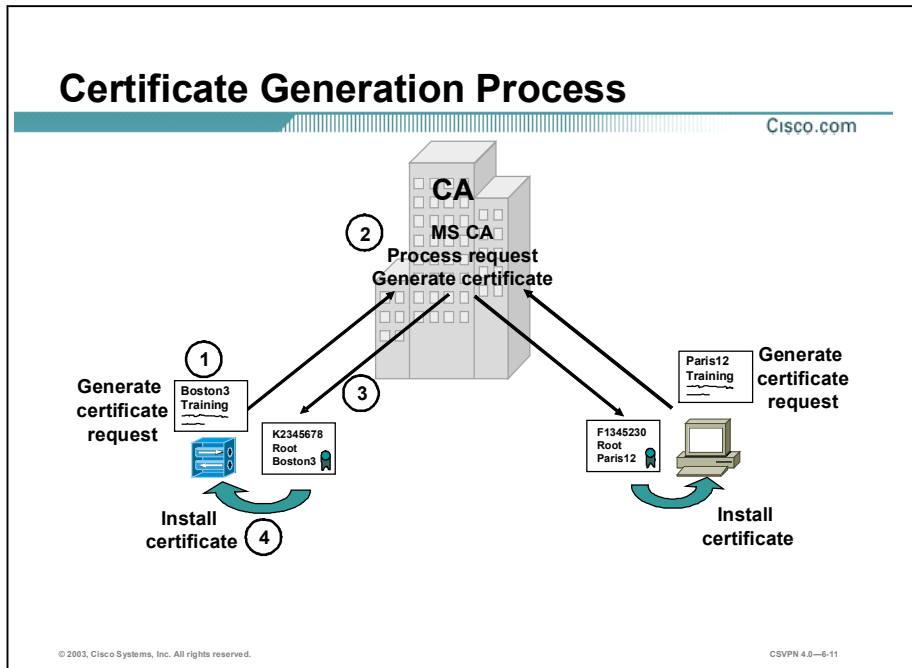


An end-user (or end-entity) must obtain a digital certificate from the CA to participate in a certificate exchange. This is known as the enrollment process. It requires three steps:

**Step 1** Each user generates a private and public key pair.

**Step 2** The requestor generates a certificate request and sends it to the CA.

**Step 3** The CA transforms the certificate request into a digital certificate and returns both a root and identity digital certificate to the requestor.

**Step 4** The requestor installs the root certificate into the Concentrator first. While installing the identity certificate, the Concentrator uses the public key from the root certificate to validate the signature of the identity certificate.

# Generating a Certificate Request

Cisco.com

**Concentrator or PC**

**CA**

PKCS #10

CA Information

Hash algorithm

Hash

CA private key

Encryption algorithm

Certificate: 123456

| Lynn | K2345678 |
|------|----------|

4ehIDx67NMop9

PKCS #10

Digital certificate

CSVPN 4.0—6-12
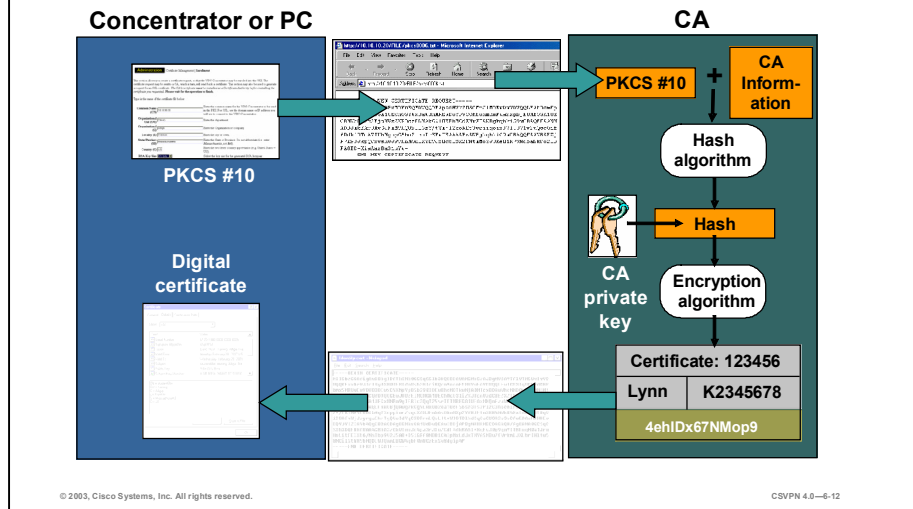
In the certificate generation process, first you generate a certificate request known as a Public Key Cryptography Standards (PKCS)#10. User information such as a common name, organizational unit, organization, locality, state, country, and public key is requested. After the information is supplied, the Concentrator generates a certificate request: a PKCS#10. The request is formatted as an Abstract Syntax Notation One (ASN.1) message and sent to the CA.

## Certificate Request Message— PKCS #10

Cisco.com

**Administration | Certificate Management | Enroll | Identity Certificate | PKCS10**

Enter the information to be included in the certificate request. *The CA's certificate* ***must*** *be installed as a Certificate Authority before installing the certificate you requested.* **Please wait for the operation to finish.**

| Field | Value | Description |
|---|---|---|
| Common Name (CN) | student1 | Enter the common name for the VPN 3000 Concentrator to be used in this PKI. |
| Organizational Unit (OU) | training | Enter the department. |
| Organization (O) | Cisco Systems | Enter the Organization or company. |
| Locality (L) | Austin | Enter the city or town. |
| State/Province (SP) | Texas | Enter the State or Province. |
| Country (C) | US | Enter the two-letter country abbreviation (e.g. United States = US). |
| Subject AlternativeName (FQDN) | | Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI. |
| Subject AlternativeName (E-Mail Address) | | Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI. |
| Key Size | RSA 512 bits | Select the key size for the generated RSA/DSA key pair. |

Enroll    Cancel

CSVPN 4.0—6-13

The figure shows a sample certificate request form completed on the Concentrator. The information for a certificate request is as follows:

■ Common Name (CN) field—A unique name for the Concentrator.

■ Organizational Unit (OU) field—The Concentrator uses the organizational unit as the group name. By default, the OU field of the certificate must match the group attribute data based in the Concentrator.

■ Organization (O) field—The company name.

■ Locality (L)—City or town where the company resides.

■ State/Province (SP)—State or province where the company resides.

■ Country (C)—Country where the company resides.

■ Subject Alternative Name—Fully qualified domain name for the Concentrator, to be used in this PKI.

■ Key Size drop-down menu—The following options are available:

— RSA 512 bits—This key size provides sufficient security and is the default selection. It is the most common and requires the least processing.

— RSA 768 bits—This key size provides normal security. It requires approximately two to four times more processing than the 512-bit key.

— RSA 1024 bits—This key size provides high security, and it requires approximately four to eight times more processing than the 512-bit key.

After the information is entered, the Concentrator generates a certificate request. The output is a new certificate request, a PKCS#10, in the ASN.1 message format.

# Generating an Identity Certificate

Cisco.com

**Concentrator or PC**

**CA**

PKCS #10

Digital certificate

PKCS #10 + CA inform-ation

Hash algorithm

Hash

CA private key → Encryption algorithm

Certificate: 123456

| Lynn | K2345678 |

4ehIDx67NMop9

CSVPN 4.0—6-14
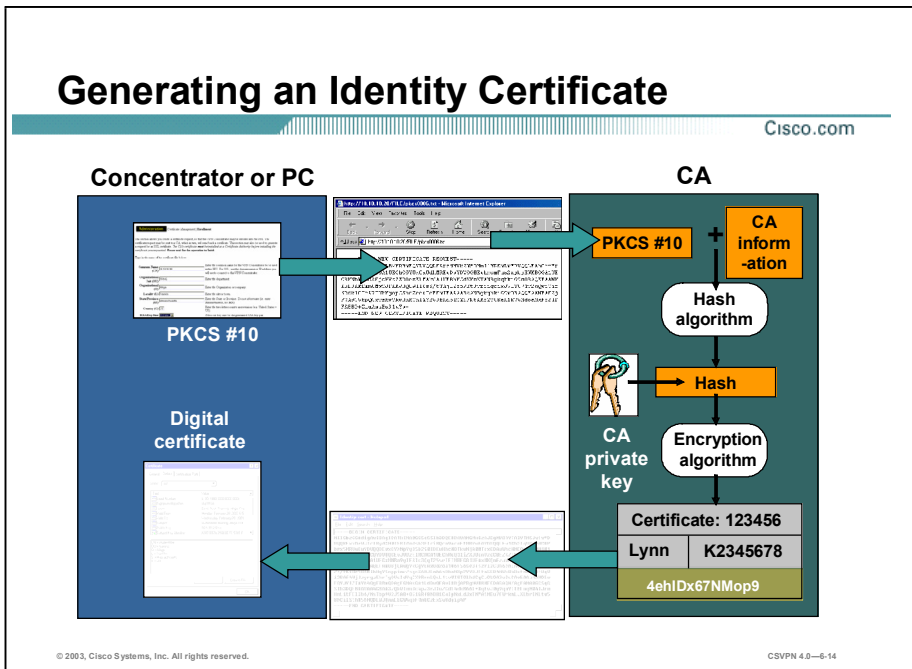
Upon receipt of the PKCS#10, the CA verifies the authenticity of the PKCS#10. The CA decrypts the digital signature with the requestor's public key to validate it. If valid, PKCS#10 is transformed into an identity certificate. The identity certificate is a composite of information supplied from the PKCS#10 and the CA. For security, a hash algorithm is performed on the combined attributes. The hash value is encrypted using the CA's private key, and is attached to the certificate. The identity certificate is then sent to the Concentrator as an ASN.1 formatted message.

## Digital Certificates
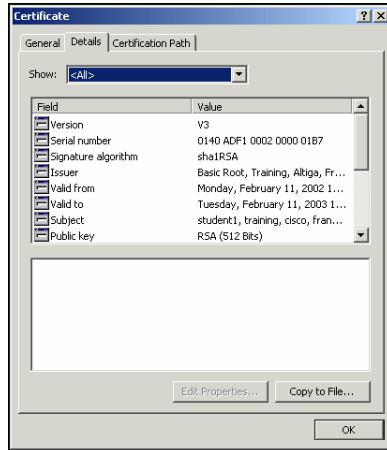
**Digital certificates contain:**

- **Serial number**
- **Validity dates**
- **Issuer name**
- **Subject name**
- **Subject public key information**
- **CA signature**

CSVPN 4.0—6-15

The X.509 certificate consists of specific fields and values. The figure shows an example of a Microsoft CA certificate. The certificate information displays the following:

■ Certificate format version—Currently, it is X.509 version 1, 2, or 3.

■ Certificate serial number—Unique certificate numerical identifier in the CA domain. When a certificate is revoked, it is the certificate number that is listed on the CRL.

■ Signature algorithm—Identifies the CA's public key and hashing algorithm.

■ Issuer—The distinguished name of the CA.

■ Validity period—Specifies the start and expiration dates for the certificate.

■ Subject X.500 name—The distinguished name of the entity holding the private key.

■ Subject public key information—Specifies the subject's public key and hashing algorithm.

■ Extensions—Extends the certificate to allow additional information.

■ CRL-Distribution Points (DPs)—Location of the CRL list for this certificate.

■ CA signature—The CA performs a hash function on the certificate contents; the hash is then signed with the CA's private key to ensure authenticity.

# Digital Certificate Encoding

Cisco.com

**CA**
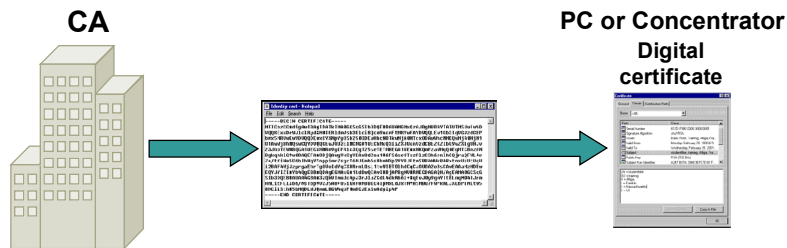
**PC or Concentrator**
**Digital certificate**

CSVPN 4.0—6-16

When a certificate is sent between a CA and Concentrator or PC, the ASN.1 formatted message is encoded. The digital certificate encoding can be one of two types: Distinguished Encoding Rules (DER) data (raw binary format) or Privacy Enhanced Mail (PEM) format (binary converted to base 64 format). Typically when you request a certificate, the CA prompts you for the encoding type: DER or base 64 encoding. This may be an issue if the sender or receiver can support only one encoding type. The Concentrator can support both types.

The CA can send certificates individually using identify and root certificates. You can also request an all-inclusive CA certificate path, PKCS#7. PKCS#7 is a message syntax that allows multiple certificates to be enveloped within one message (the same concept as PKZIP storing multiple files in a .zip file).
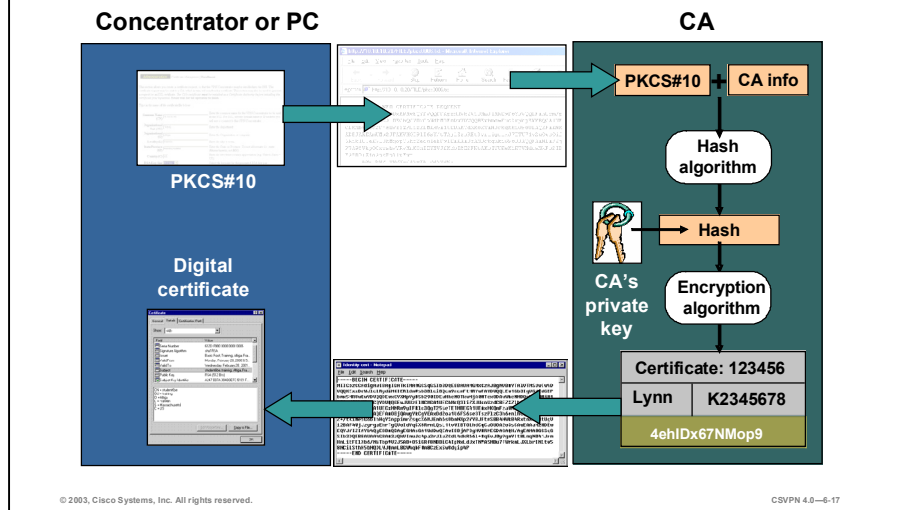
Before an identity certificate is installed, the Concentrator must validate it. The Concentrator checks the following to validate the identity certificate:

■ Is the identity certificate verified with the CA's public key?

■ Has the identity certificate expired?

■ Has the identity certificate been revoked?
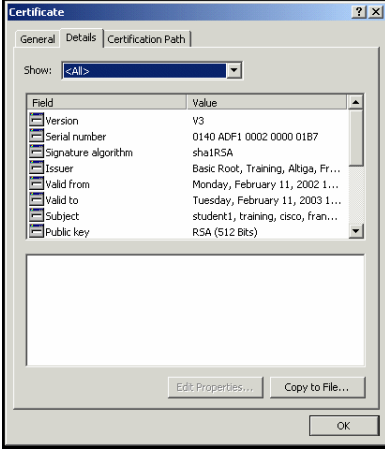
When validated, the certificate is installed on the Concentrator. The identity certificate can now be exchanged with a peer during IPSec tunnel establishment.

# Validating Certificates

This topic discusses how digital certificates are validated and maintained.



Digital certificate validation is based on trust relationships within the PKI. If you trust A, and A says that B is valid, then you should trust B. This is the underlying premise when validating certificates. When enrolling into a PKI, you must first obtain and install the CA certificates on the Concentrator. In doing so, you implicitly establish a trust relationship where any documents signed by those CAs are considered to be valid.

During Internet Key Exchange (IKE) negotiations, when an identity certificate is received from an IKE peer, the Concentrator validates the certificate by determining that the certificate:

■ Has been signed by a CA that is trusted (checks the signature).

■ Has not expired.

■ Has not been revoked.

**Signature Validation**
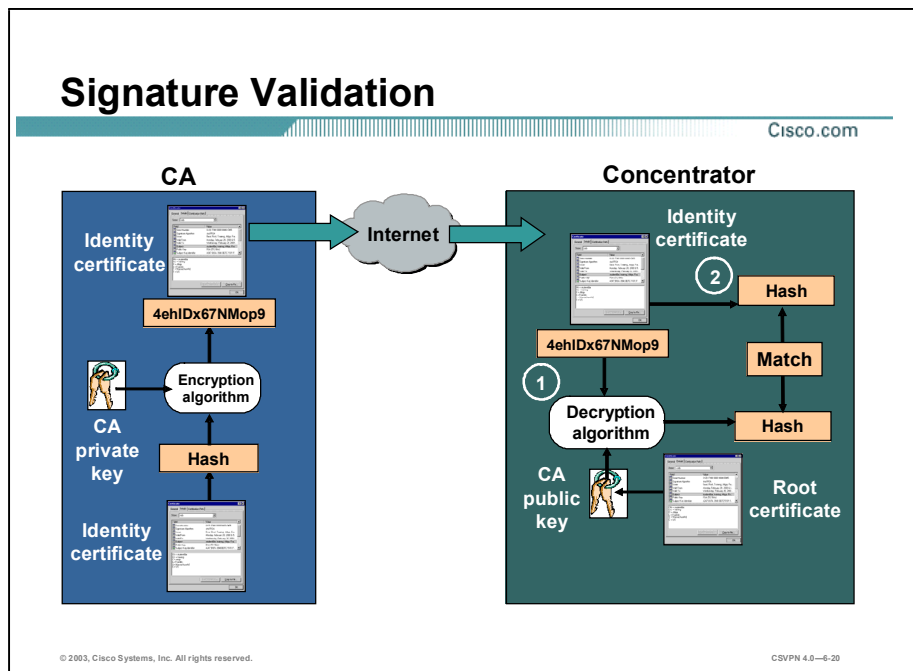
The first step in validating a digital certificate is to validate the signature. Signature validation consists of the following steps:

**Step 1**   At the CA, the original identity certificate is put through a hash algorithm, the output hash is encrypted by the CA's private key, and the hash is appended to the end of the certificate.

**Step 2**   At the remote end, there is a two-step process:

- The receiver uses the CA's public key to decrypt the hash. The result is the original hash value.

- The received message is sent through the hash algorithm to produce a second hash.

**Step 3**   The CA-generated hash and Concentrator-generated hash are compared:

- If they match, the identity certificate is genuine.

- If they do not match, the certificate is invalid; there is an invalid signature or identity certificate.

**Certification Chain**

CISCO.COM

**Central**

Root certificate

Identity certificate

Terry          Pat

**Hierarchical**

Root certificate

Subordinate CA certificate

Identity certificate

Terry          Pat          Alex
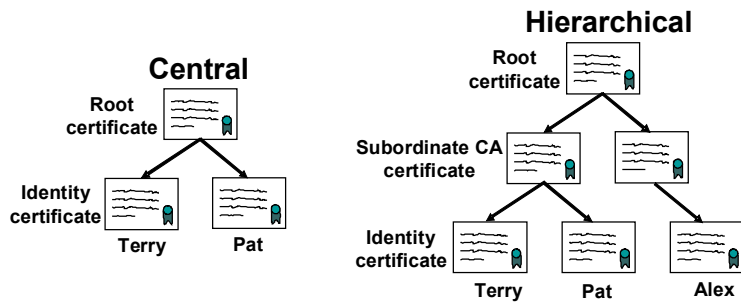
CSVPN 4.0—6-21

Previously, it was stated that the Concentrator needs a copy of the CA's public key to decrypt the hash. The question is where does the Concentrator find a copy of that key. The answer is it depends on the CA environment, central or hierarchical. In a central, or flat, CA, the root CA signs the identity certificate. The root certificate must be installed before trying to install the identity certificate so the Concentrator has access to the root's public key. One of the root CA fields is a copy of the CA's public key. In the example in the figure, using the public key of the root certificate checks the signature of Terry's certificate.

In a hierarchical environment, the ability to sign is delegated through the hierarchy. The top is the root CA; it signs certificates for subordinate CAs. The subordinate CA signs certificates for lower level CAs. Ultimately, a subordinate CA will sign the user's identity certificate. The certificate must be validated up the chain of authority. In the example in the figure, Alex's certificate is validated with the public key of the subordinate CA. The subordinate CA is validated with the public key of the root CA.

**Validity Period**

CISCO.COM

| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 0EB6 76C4 E265 A990 4793 9... |
| Signature algorithm | sha1RSA |
| Issuer | Basic Root, Training, Altiga, Fr... |
| Valid from | Monday, February 11, 2002 7... |
| Valid to | Thursday, February 12, 2004 ... |
| Subject | Basic Root, Training, Altiga, Fr... |
| Public key | RSA (1024 Bits) |

CSVPN 4.0—6-22
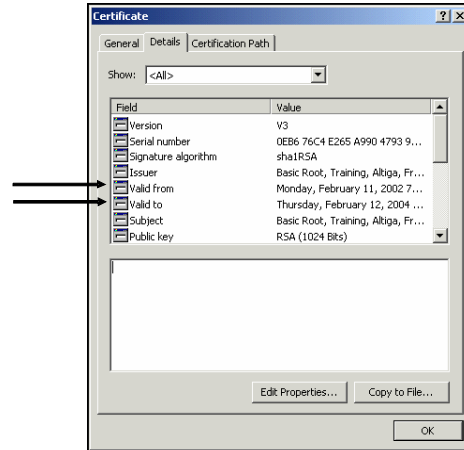
The next step is to check the validation period. A certificate is valid for a specific period of time. The validity period (range) is set by the CA and consists of valid from and valid to fields. On the Concentrator, when you try to add a certificate, the validity range is compared against the system clock. If the system clock is not within the validity range—either too early or too late—you receive an error message.

**CRL**

- **List of revoked certificates signed by the CA**
- **Stored on the CA or CRL Distribution Point**
- **No requirement on devices to ensure that CRL is current**

**Revoked**
**Cert 12345**
**Cert 12241**
**Cert 22333**

*CA Server*
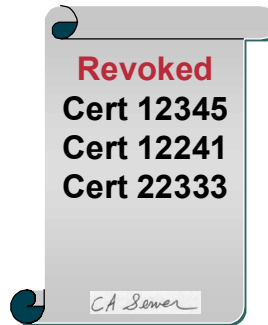
CSVPN 4.0—6-23

Checking the CRL is the last validation step. A CRL is a list issued by the CA that contains certificates that are no longer valid. CRLs are signed by the CA and are released periodically or on demand. CRLs are valid for a specific amount of time, depending on the CA vendor used. Some reasons a certificate might be invalidated are as follows:

■ User data changes (for example, the username).

■ A key is compromised.

■ An employee leaves the organization.

The CRL must be consulted by anyone using a certificate, to ensure that it is still valid. There is no requirement on devices to ensure that the CRL is current.

# CRL—General

**Certificate Revocation List**

General | Revocation List

**Certificate Revocation List Information**

| Field | Value |
|---|---|
| Version | V2 |
| Issuer | Basic Root, Training, Altiga, Frankl... |
| Effective date | Tuesday, February 26, 2002 9:03... |
| Next update | Tuesday, March 05, 2002 9:23:45... |
| Signature algorithm | sha1RSA |
| Authority Key Ident... | KeyID=4D6D 441A 6B80 2963 8A... |
| CA Version | V2.2 |

Value:

OK

CSVPN 4.0—6-24
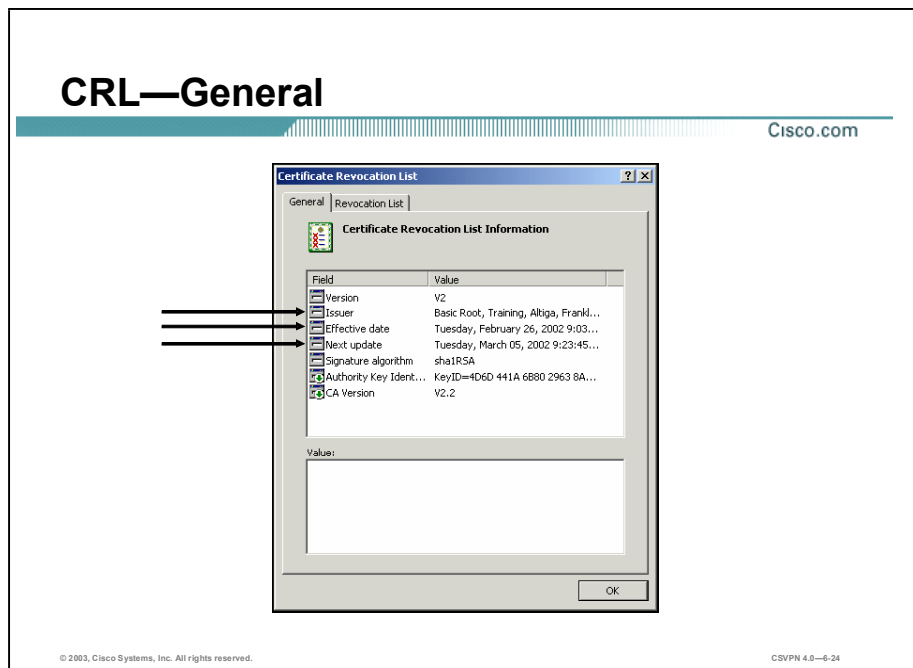
The figure contains an example of a CRL. The CRL has two tabs: General and Revocation List. The general tab includes information about the CRL itself, such as the name of the CA that issued the list, the date the list was issued, the date of the next publication. The date of the next publication could be hourly, daily, weekly, and so on, as defined by the revocation list, which includes all the revoked certificates. The certificates are listed by certificate serial number and revocation date.

# CRL—Revocation List
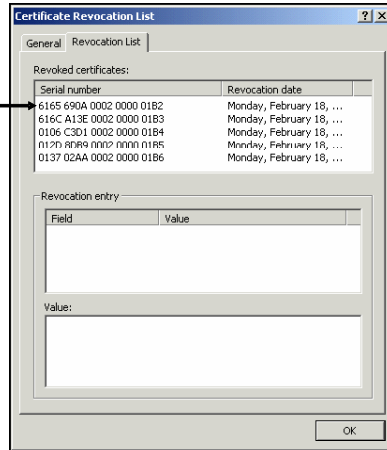


The figure contains an example of the CRL. The certificate serial number and revocation date and time are listed.

# CRL Distribution Point Location
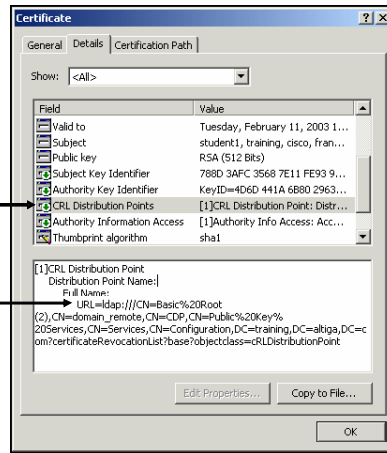
A number of CRL-DPs are accessible from the Web. Because the Web is a large place, it is difficult for the Concentrator to check a particular certificate to see if it is valid or revoked. As part of the X.509 certificate, the CRL extension includes the CRL-DP. The CRL-DP information is included in the X.509 extension fields. If you double-click the CRL-DPs icon in the certificate, the URL of the CRL-DP is included.

**Certificate Authentication Process**

Cisco.com

**Headquarters**
Entrust

Entrust Root D134TA30 | Hdqtrs3 Entrust K2345678

Hdqtrs3 Entrust K2345678

Internet

LDAP server

Boston3 Entrust K2345678

Boston3 Entrust K2345678 | Entrust Root D134TA30

**Home**
Entrust
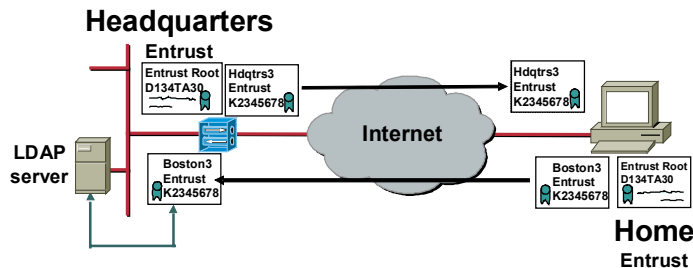
**Load and validate identity certificate**
- **Exchange the identity certificates during IKE negotiations.**
- **Verify the identity certificate signature via the stored root certificate.**
- **Verify that the certificate validity period has not expired.**
- **Verify that the identity certificate has not been revoked.**

CSVPN 4.0—6-27

During certificate exchange, identity certificates must be validated. Identity certificates are exchanged during IKE Phase 1 negotiation to authenticate the peers. The PC sends its identity certificate to the Concentrator. The Concentrator validates the certificate as follows:

**Step 1** Validate the signature. The Concentrator uses the public key stored on its root certificate to decrypt the identity certificates hash. The Concentrator also re-computes a hash of the received identity certificate. If the decrypted and re-computed hashes match, the certificate is valid.

**Step 2** Check the validity period of the certificate against the system clock of the Concentrator. If the Concentrator's system clock falls within the validity period of the identity certificate, the test is successful. The validity range can be found on the identity certificate.

**Step 3** (Optional.) If enabled, the Concentrator locates the CRL and determines whether the identity certificate serial number is on the list. If present, the certificate is revoked. If absent, the certificate is valid.

If the received identity certificate passes the validation process, the Concentrator authenticates the PC. In turn, the Concentrator sends its identity certificate to the PC. The PC performs the same validation process for the Concentrator's identity certificate.

# Configuring the Cisco VPN 3000 Series Concentrator for CA Support

This topic discusses how to install digital certificates on Cisco VPN 3000 Series Concentrator.
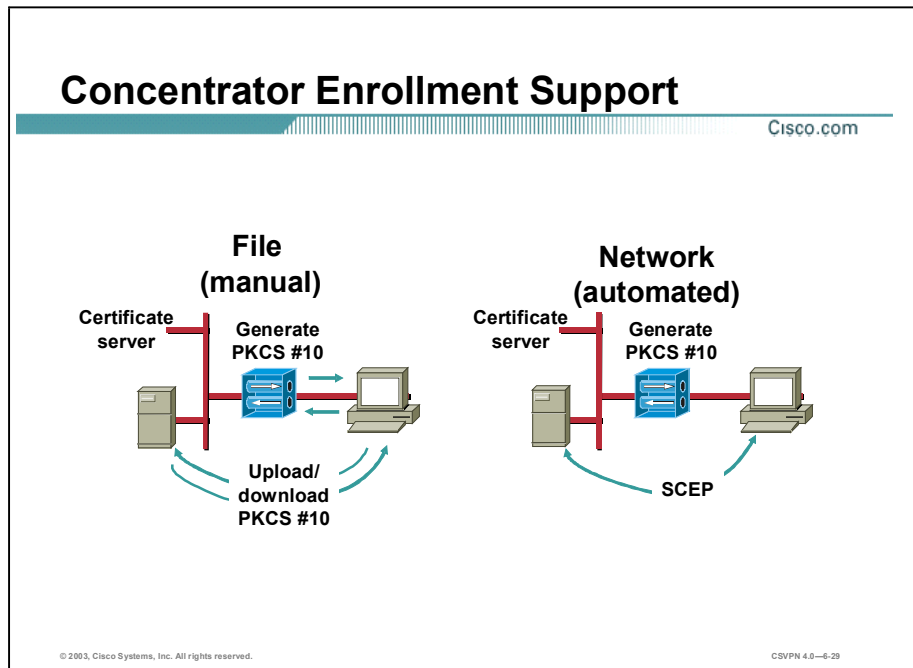


For the Concentrator to participate in the certificate exchange, a certificate needs to be loaded on the Concentrator, which is called Concentrator certificate enrollment. There are two types of Concentrator certificate enrollments:

■ File based enrollment—This is a manual process. You can enroll by creating a request file, PKCS#10. When you have created a request file, you can either e-mail it to the CA and receive a certificate back, or you can access the CA's web site and cut and paste the enrollment request in the area that the CA provides. When generated by the CA, identity and root certificates are downloaded to the PC. The certificates must then be imported onto the Concentrator.

■ Network-based enrollment—This is an automated process which enables you to connect directly to a CA via Simple Certificate Enrollment Protocol (SCEP). Complete the enrollment form to connect to a CA via SCEP. The Concentrator contacts the CA via SCEP and the CA returns a CA certificate. When the CA certificate is verified, the Concentrator uses SCEP to send the enrollment request to the CA, where the CA issues an identity certificate. The CA then returns the identity back to the Concentrator. For network-based enrollment to work, both the Concentrator and the CA must support SCEP. There will be further discussion of SCEP-based enrollment later in this lesson.

The Concentrator certificate manual loading process consists of the following:
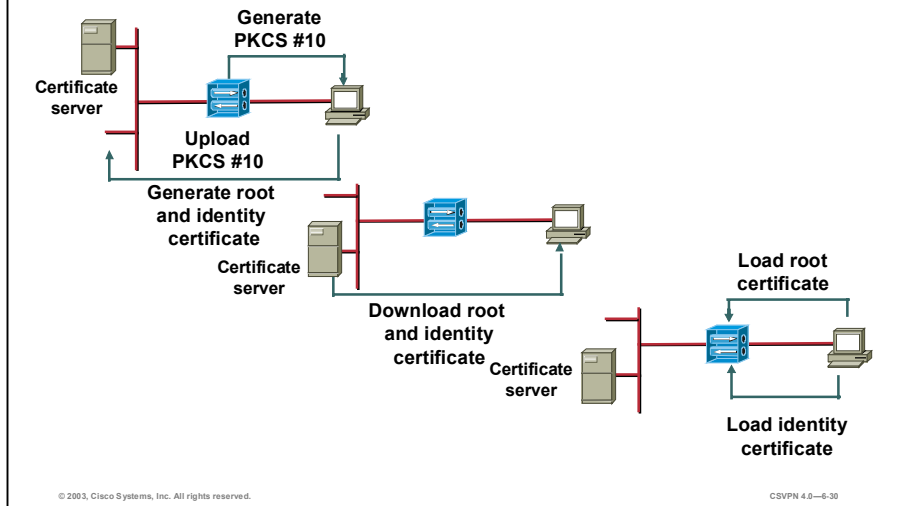
**Step 1** Generate the certificate request and upload it to a CA.

**Step 2** The CA generates the identity and root certificates. Each is downloaded to a PC.

**Step 3** The certificates are loaded onto the Concentrator.

**Manual Enrollment—Generate a Certificate Request**

The first step in the Concentrator certificate manual loading process is to generate a certificate request. Complete the following steps to accomplish the task:

**Step 1**  Choose **Administration>Certificate Management>Enroll**. The Enroll window opens. Click the **Identity certificate** link. The choice is between creating an SSL or identity certificate, choose **identity certificate**.

**Step 2**  Choose **Administration>Certificate Management>Enroll>Identity Certificate**. The Identity Certificate window opens. Click the **Enroll via PKCS10 Request (Manual)** link. You can enroll with a CA manually via a PKCS10 or automatically via SCEP. In this instance, you choose the manual process.

**Step 3**  Choose **Administration>Certificate Management>Enroll>Identity Certificate>PKCS10**. The PKCS10 window opens. Fill out the PKCS10 form. There is further discussion of the PKCS10 form later in this lesson.

## Group Matching Policy

**Identity certificate**

**Administration | Certificate Management | View**

| Subject | Issuer |
|---|---|
| CN=student1sh | CN=AUSTIN |
| OU=training | OU=VSEC |
| O=Cisco Systems | O=TRAINING |
| L=Austin | L=AUSTIN |
| SP=Texas | SP=TX |
| C=US | C=US |

Serial Number 61122D7200060000004A
Signing Algorithm SHA1WithRSA
Public Key Type RSA (512 bits)
MD5 Thumbprint 8A:09:19:01:45:B7:2D:94:5B:2E:5E:BC:63:B2:03:DB
SHA1 Thumbprint 39:9F:9B:BF:8E:FC:9D:36:31:C6:78:FE:D9:44:F8:F2:B6:D2:84:D5
Validity 6/3/2003 at 15:43:57 to 6/3/2004 at 15:53:57
CRL Distribution Point http://austin/CertEnroll/AUSTIN(6).crl

**Group matching policy**

**Configuration | Policy Management | Certificate Group Matching | Policy**

Configure the policy for certificate group matching. The VPN Concentrator processes the policies in the order listed below until it finds a match.

☑ Match Group from Rules    Check to use configured rules to match a certificate to a group.

☑ Obtain Group from OU    Check to use the certificate OU field to determine the group.

☑ Default to Group  –Base Group– ▾   Check to use a default group for certificate users. Choose the default group from the drop down menu.

[ Apply ]   [ Cancel ]

CSVPN 4.0—6-32

When a certificate arrives at the concentrator during IKE phase one, the Concentrator authenticates the remote peer and extracts the group information from the certificate. The Concentrator attempts to match the extracted information with the Concentrator's group name database. The group name identifies the remote user's concentrator access privileges. If a match is found, the remote user is afforded the access rights and privileges of the matching group. By default, the Concentrator uses the OU field for group matching. Configuration-Policy Management-Certificate Group Matching-Policy windows enables the administrator to configure alternative group matching options. For example, an administrator may choose to use the organization and organizational unit or organizational unit and locality.

Configuring certificate group matching consists of two steps, configure the matching policy and configure the rules. There are three group matching policy options to choose from:

■ Match Group from Rules—Use the rules you have defined for certificate group matching (for example, organizational unit and organization). If the administrator plans to use match group from rules policy, define the rules before selecting the policy.

■ Obtain Group from OU—Use the organizational unit in the certificate to specify the group to match. This choice is enabled by default.

■ Default to Group—Use a default group or the Base Group for certificate matching. Use the group matching rules set up for this group.

The Concentrator processes the policies in the order they are enabled until it finds a match. Group matching rules will be discussed later in this lesson.

## Group Matching Rules

**Administration | Certificate Management | View**

| Subject | Issuer |
|---|---|
| CN=student1 | CN=AUSTIN |
| OU=training | OU=VSEC |
| O=Cisco | O=TRAINING |
| L=Franklin | L=AUSTIN |
| SP=Massachusetts | SP=TX |
| C=US | |

Serial

Signing Al

Public K

MD5 Thu

SHA1 Thu

**Configuration | Policy Management | Certificate Group Matching | Rules | Add**

Create a new rule for certificate group matching from the fields below. A rule contains a group name and matching criteria that define the group. The VPN Concentrator checks the information in the certificate against these criteria; all the criteria must match the certificate to establish the group.

Note that the Value string must be enclosed in double quotes. These quotes are added automatically.

You can also create a rule by entering its text directly in the **Matching Criterion** box. If you create a rule in this way, separate the components with commas. Also, be sure to add double quotes around the value. If the value itself contains double quotes, replace them with two double quotes. For example, enter the value *"Tech" Eng* as: """Tech"" Eng". An example of a matching criterion is: OU="Engineering",ISSUER-O="Cisco"

**Enable** ☑     Check to enable the rule.

**Group** |training  ▼|  Select the group to which this rule applies.

| Distinguished Name | Operator | Value | |
|---|---|---|---|
| |Subject ▼| |CommonName (CN) ▼| | |Equals (=) ▼| | [        ] | Append |

**Matching Criterion**

|OU="training",O="Cisco"                        |

| Add | | Cancel |

CSVPN 4.0—6-33

The Configuration>Policy Management>Certificate Group Matching window enables an administrator to define rules to match an identity certificate to a permission group based on fields in the identity certificate. You can apply a combination of certificate fields. For a user to be identified as belonging to a certain group, specific fields of the received certificate must match the rules defined for that group. In the figure, the bottom window defines the rules. The top window displays a received identity certificate. In the bottom window, for a user to be recognized as being a member of the training group, the following rules must be met: the received identity certificates OU = training and O = Cisco. In the top window, the identity certificates OU field = training and the O field = Cisco.

Define the rules and enable each rule for the selected group to specify a policy for group matching by rules. A group must already exist in the configuration before you can create a rule to apply to it. You can assign multiple rules to the same group. Rules assigned to the same group are combined and a match results when all rules test true. Also, you must configure a matching policy. You can define rules and matching policies in any order.
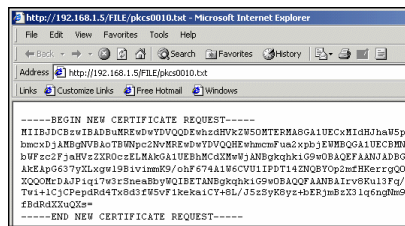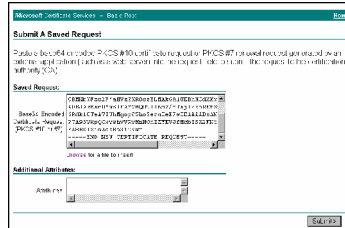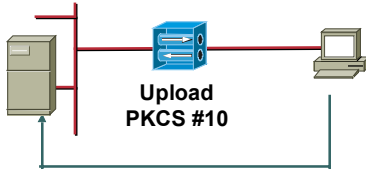
Upload the Public-Key Cryptography Standard (PKCS) #10 to the CA after the Concentrator generates the PKCS#10:

**Step 1**  Manually copy the PKCS#10 output and paste it into the CA. The figure displays an example of a Microsoft CA. The process is virtually the same for the other CAs but the CA windows and commands will vary.

**Step 2**  The CA validates the request. Validation may be automatic or may require CA administrator intervention. With automatic approval, the identity certificate is generated with no delay. With required administrator approval, the identity certificate generation is delayed until approved. The approval process varies by CA and company account.

**Step 3**  The CA produces an identity and root certificate.

Download Certificates
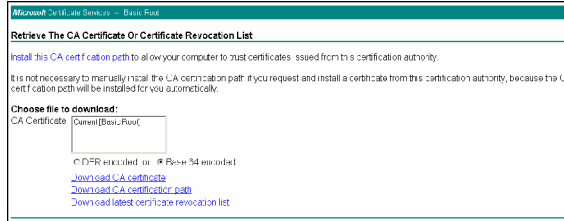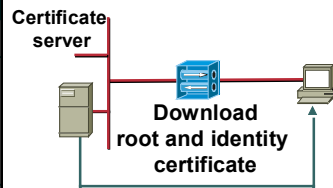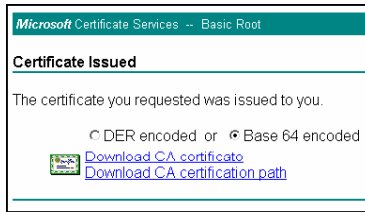
The CA generates the certificate when the CA approves the certificate request. The root and identity certificates need to be downloaded to the PC. In the figure, the Microsoft CA provides prompts to guide you through the process.

## Install Root Certificate
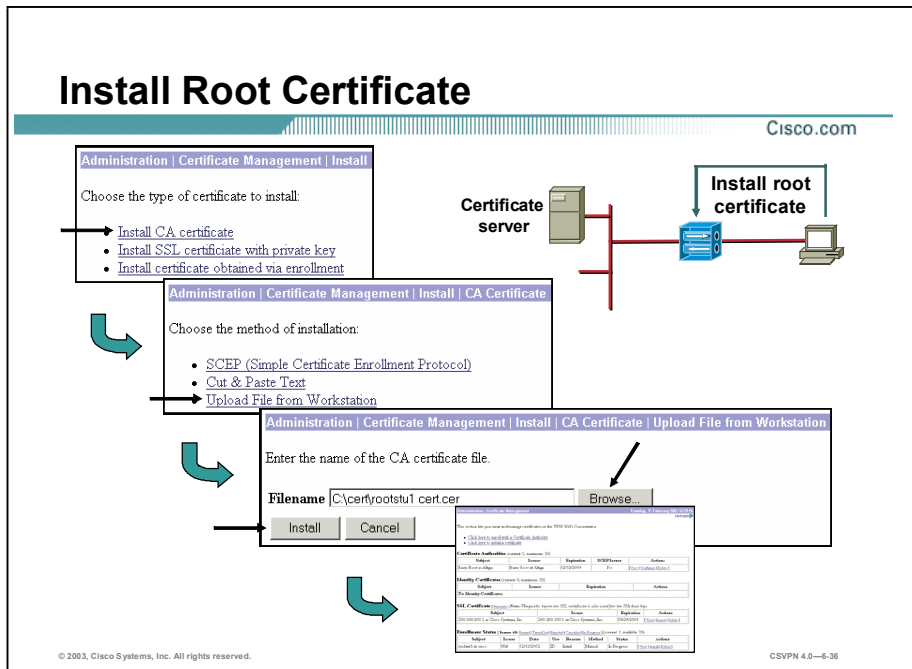
The certificates are transferred from the PC to the Concentrator. The certificates must be loaded in order. The root certificate is loaded first, followed by the identity certificate.

Complete the following steps to install the root certificate:

**Step 1** Choose **Administration>Certificate Management>Install**. The Install window opens. Click the **Install CA certificate** link.

**Step 2** Choose **Administration>Certificate Management>Install>CA Certificate**. The CA Certificate window opens. Click **Upload File from the Workstation**.

**Step 3** Choose **Administration>Certificate Management>Install>CA Certificate>Upload File** from the Workstation window and click **Browse** to browse to the root certificate file on the workstation.

**Step 4** Click **Install** to install the root certificate.

When the root certificate is loaded, it is validated. To be valid, the signature on the certificate must be valid and the certificate must not have expired. A CRL lookup is optional. By default, it is disabled.

---

**Note** If you receive an expiration error when loading your root certificate, ensure that the Concentrator's date and time is correctly set.

---

**Root Installed**

Cisco.com

CSVPN 4.0—6-37

The Administration>Certificate Management window displays the root certificate in the Certificate Authority section. Under the Certificate Authorities section, there are five fields. They are as follows:

■ Subject—The Common Name plus the Organization (O) in the Subject field of the certificate.

■ Issuer—The Common Name plus the Organization (O) in the Issuer field of the certificate.

■ Expiration—The expiration date of the certificate.

■ SCEP Issuer—In order for an identity certificate to be available for SCEP enrollment, the root must first be installed via SCEP. This field indicates if the certificate is SCEP-enabled. The two variables are as follows:

— Yes—This certificate was installed via SCEP.

— No—This certificate was not installed via SCEP.

■ Actions—This column allows you to manage particular certificates. The actions available vary with the type and status of the certificate. The following are the actions:

— View—View details of this certificate.

— Configure—Enable CRL checking for this CA certificate, modifies SCEP parameters, or enable acceptance of subordinate CA certificates.

— Delete—Delete this certificate from the Concentrator. Certificates cannot be deleted if they are in use. To remove them from use, first remove the identity certificate from any pre-existing Security Associations (SA). Then delete the certificate.

## View Root Certificate

Administration | Certificate Management | View

| Subject | Issuer |
|---|---|
| CN=student1sh | CN=AUSTIN |
| OU=training | OU=VSEC |
| O=Cisco Systems | O=TRAINING |
| L=Austin | L=AUSTIN |
| SP=Texas | SP=TX |
| C=US | C=US |

Serial Number 61122D7200060000004A
Signing Algorithm SHA1WithRSA
Public Key Type RSA (512 bits)
MD5 Thumbprint 8A:09:19:01:45:B7:2D:94:5B:2E:5E:BC:63:B2:03:DB
SHA1 Thumbprint 39:9F:9B:BF:8E:FC:9D:36:31:C6:78:FE:D9:44:F8:F2:B6:D2:84:D5
Validity 6/3/2003 at 15:43:57 to 6/3/2004 at 15:53:57
CRL Distribution Point http://austin/CertEnroll/AUSTIN(6).crl

CSVPN 4.0—6-38

The Administration>Certificate Management>Certificates>View window enables the administrator to view the installed root certificate. The root certificate contains the following information:

■ Subject—Identifies the common name of the subject.

■ Issuer—The CA or other entity (jurisdiction) that issued the certificate.

■ Issuer—Identifies the common name of the issuer. If the common name and issuer name match, this is a copy of the root certificate.

■ Serial Number—Identifies the certificate serial number.

■ Signing Algorithm—The cryptographic algorithm that the CA or other issuer used to sign this certificate.

■ Public Key Type—The algorithm and size of the certified public key.

■ Certificate Usage—The purpose of the key contained in the certificate, for example: digital signature, certificate signing, nonrepudiation, key or data encipherment, and so on.

■ MD5 Thumbprint—A 128-bit Message Digest 5 (MD5) hash of the complete certificate contents, shown as a 16-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a root certificate's authenticity, you can check this value with the issuer.

- SHA1 Thumbprint—A 160-bit Secure Hash Algorithm – 1 (SHA-1) hash of the complete certificate contents, shown as a 20-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.

- Validity—The time period during which this certificate is valid. The Manager checks the validity against the Concentrator's system clock, and it flags expired certificates by issuing event log entries.

- Subject Alternative Name (FQDN)—The FQDN for this Concentrator that identifies it in this PKI. The alternative name is an optional additional data field in the certificate, and it provides interoperability with many Cisco IOS and PIX Firewall systems in LAN-to-LAN connections.

- CRL Distribution Point—The DP for CRLs from the issuer of this certificate. If this information is included in the certificate in the proper format, and you enable CRL checking, you do not have to provide it on the Administration-Certificate Management-Configure CA Certificate window.

# Install Identity Certificate
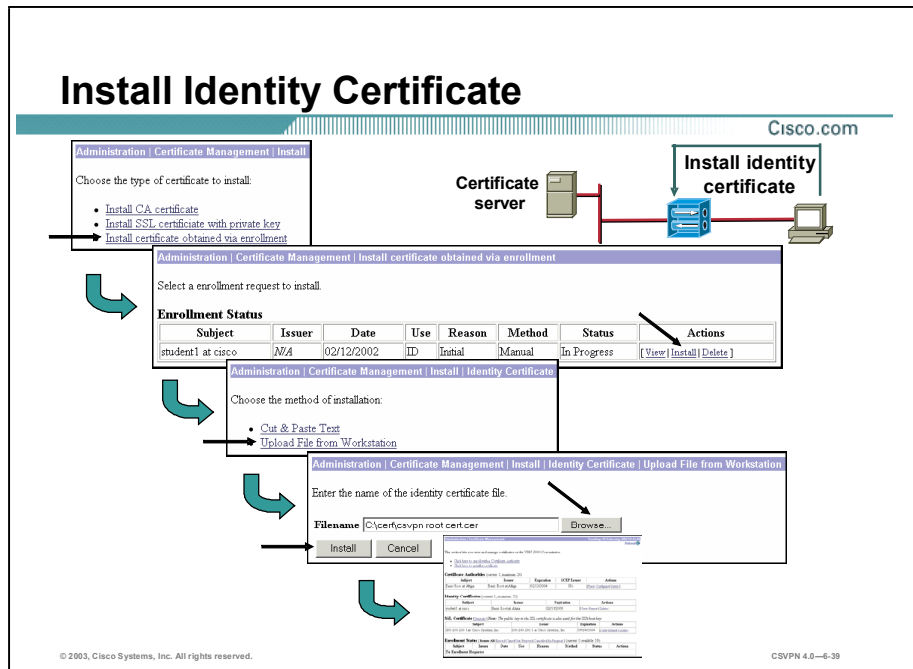
Identity certificate installation is a four-step process. The steps are as follows:

**Step 1** Choose **Administration>Certificate Management>Install**. The Install window opens. Click the **Install certificate obtained via enrollment** link.

**Step 2** Choose **Administration>Certificate Management>Install certificate obtained via enrollment**. The Install Certificate Obtained Via Enrollment window opens. Click the **Install link** in the Actions column within the Enrollment Status section.

**Step 3** Choose **Administration>Certificate Management>Install>Identity Certificate**. The Identity Certificate window opens. Click the **Upload File from Workstation** link.

**Step 4** Choose **Administration>Certificate Management>Install>Identity certificate>Upload file** from the Workstation window and click the **Browse** button to browse to the identity certificate on the PC. Click **Install**.

When the identity certificate is loaded, it is validated. To be valid, the signature on the certificate must be valid and the certificate must not have expired. A CRL lookup is optional. By default, it is disabled.

| Note | If you receive an expiration error when loading your identity certificate, ensure that the Concentrator's date and time is set correctly. |

# Identity Certificate Installed

| Administration | Certificate Management | | | Wednesday, 04 June 2003 12:35:55 |
|---|---|---|---|---|

Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- Click here to enroll with a Certificate Authority
- Click here to install a certificate

**Certificate Authorities** [ View All CRL Caches | Clear All CRL Caches ] (current: 1, maximum: 6)

| Subject | Issuer | Expiration | SCEP Issuer | Actions |
|---|---|---|---|---|
| AUSTIN at TRAINING | AUSTIN at TRAINING | 06/04/2005 | No | View | Configure | Delete |

**Identity Certificates** (current: 1, maximum: 2)

| Subject | Issuer | Expiration | Actions |
|---|---|---|---|
| student1sh at Cisco Systems | AUSTIN at TRAINING | 06/03/2004 | View | Renew | Delete |

**SSL Certificate** [ Generate ] *Note: The public key in the SSL certificate is also used for the SSH host key.*

| Subject | Issuer | Expiration | Actions |
|---|---|---|---|
| 10.0.1.5 at Cisco Systems, Inc. | 10.0.1.5 at Cisco Systems, Inc. | 05/19/2006 | View | Renew | Delete |

**Enrollment Status** [ Remove All: Errored | Timed-Out | Rejected | Cancelled | In-Progress ] (current: 0 available: 2)

| Subject | Issuer | Date | Use | Reason | Method | Status | Actions |
|---|---|---|---|---|---|---|---|
| No Enrollment Requests | | | | | | | |

CSVPN 4.0—6-40

The Administration>Certificate Management>Certificates window enables the administrator to view installed certificates. Under Identity Certificates, there are four fields. They are as follows:

■ Subject—The subjects Common Name plus the Organization (O) in the Subject field of the certificate.

■ Issuer—The issuers Common Name plus the Organization (O) in the Issuer field of the certificate.

■ Expiration—The expiration date of the certificate.

■ Actions—This column allows you to manage particular certificates. The actions available vary with type and status of the certificate. The following are the actions:
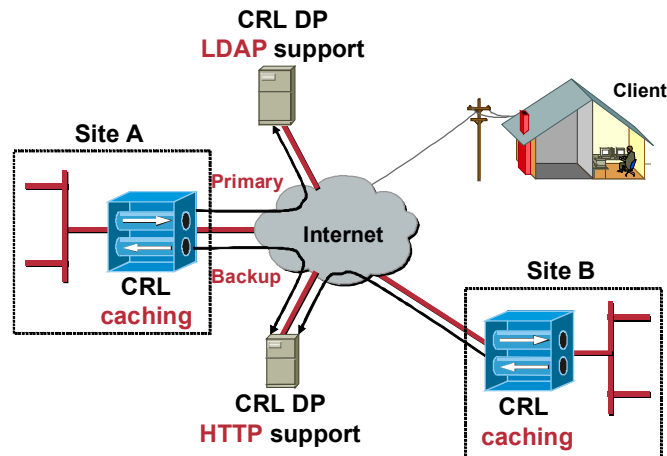
— View—View details of this certificate.

— Renew—A shortcut that allows you to generate an enrollment request based on the content of an existing certificate.

— Delete—Delete this certificate from the Concentrator.

The number of enrollment requests you can make at any given time is limited to the Concentrator's identity certificate capacity. Most Concentrator models allow a maximum of 20 identity certificates. For example, if you already have 5 identity certificates installed, you will be able to create only up to 15 enrollment requests. The Cisco VPN 3005 Concentrator is an exception, supporting only 2 identity certificates. On the Cisco VPN 3005 Concentrator only, you can request a third certificate, even if two certificates are already installed, but the

Concentrator does not install this certificate immediately. First you must delete one of the existing certificates. Then, activate the new certificate to replace the one you just deleted. The Concentrator automatically deletes entries that have the status Timed out, Failed, Cancelled, or Error and are older than one week.

## View Identity Certificate

Cisco.com

Administration | Certificate Management | View

**Subject**
CN=student1sh
OU=training
O=Cisco Systems
L=Austin
SP=Texas
C=US

**Issuer**
CN=AUSTIN
OU=VSEC
O=TRAINING
L=AUSTIN
SP=TX
C=US

Serial Number 61122D7200060000004A
Signing Algorithm SHA1WithRSA
Public Key Type RSA (512 bits)
MD5 Thumbprint 8A:09:19:01:45:B7:2D:04:5B:2E:5E:BC:69:B2:09:DB
SHA1 Thumbprint 39:9F:9B:BF:8E:FC:9D:36:31:C6:78:FE:D9:44:F8:F2:B6:D2:84:D5
Validity 6/3/2003 at 15:43:57 to 6/3/2004 at 15:53:57
CRL Distribution Point http://austin/CertEnroll/AUSTIN(6).crl

CSVPN 4.0—6-41

The Administration>Certificate Management>Certificates>View window enables the administrator to view the installed identity certificate. The end-user certificate contains the following information:

■ Issuer—Identifies the common name of the issuer (for example, Basic Root).

■ Subject—Identifies the common name of the subjects (for example, student1be).

■ Serial Number—Identifies the certificate serial number. This is used when revoking the certificate.

■ Signing Algorithm—The cryptographic algorithm that the CA or other issuer used to sign this certificate.

■ Public Key Type—The algorithm and size of the certified public key.

■ MD5 Thumbprint—A 128-bit MD5 hash of the complete certificate contents, shown as a 16-byte string. This value is unique for every certificate, and it positively identifies the certificate.

■ SHA1 Thumbprint—A 160-bit SHA-1 hash of the complete certificate contents, shown as a 20-byte string. This value is unique for every certificate, and it positively identifies the certificate.

■ Validity—Defines the period of time during which the certificate is valid (for example, from 7/23/02 to 7/23/03).

■ CRL Distribution Point—Identifies the location of the CRL. The CRL list can be retrieved and put in cache for future reference.

## Certificate Renewal



Certificate renewal is a shortcut that allows you to generate an enrollment request based on the content of an existing certificate. Use this screen to re-enroll or re-key a certificate. If you re-enroll the certificate, the new certificate uses the same key pair as the expiring certificate. If you re-key the certificate, it uses a new key pair.

- Certificate—The type of certificate you are re-enrolling or re-keying is displayed here.

- Renewal Type radio button—Specify the type of request:

  — Re-enrollment—Use the same key pair as the expiring certificate.

  — Re-key—Use a new key pair.

- Enrollment Method drop-down menu—Choose an enrollment method:

  — PKCS10 Request (manual)—Enroll using the manual process.

  — Certificate Name via SCEP—Enroll automatically using this SCEP CA.

- Challenge Password field—Your CA might have given you a password as a means of verifying your identity. If you have a password from your CA, enter it here.

- Verify Challenge Password field—Re-enter the challenge password you just entered.

- Renew button—Click **Renew** to renew the certificate.

- Cancel button—Click **Cancel** to stop the certificate renewal.

## Configure CA—CRL Caching, Backup, and HTTP Support

CRL DP
**LDAP** support

Site A

**Primary**

Client

Internet

**Backup**

CRL
**caching**

Site B

CRL DP
**HTTP** support

CRL
**caching**

CSVPN 4.0—6-43

CRLs are issued by Certificate Authorities (CAs) to identify revoked certificates. A CRL-DP specifies the location of a CRL on a server from which it can be downloaded. In order to verify the revocation status, the Concentrator retrieves the CRL from the primary or one of the backup CRL-DPs. The Concentrator checks the peer certificate serial number against the list of serial numbers in the CRL. If none of the serial numbers match, it is assumed that the peer certificate has not been revoked.

Since the system has to fetch and examine the CRL from a network DP, enabling CRL checking might slow system response times. Also, if the network is slow or congested, CRL checking might timeout. Enable CRL caching to mitigate these potential problems. This stores the retrieved CRLs in local volatile memory, thus allowing the Concentrator to verify the revocation status of certificates more quickly. There is more on configuring CRL-DPs and CRL caching later in this lesson.

# Configuring CA Certificates

There are three sections to the Administration>Certificate Management>Configure CA Certificate window: CRL retrieval policy, CRL caching, and CRL-DPs. Enabling CRL checking means that every time the Concentrator uses the certificate for authentication, it also checks the latest CRL to ensure that the certificate has not been revoked. The CRL retrieval policy defines where to find the CRL-DP location. The choices are as follows: on a CA certificate, statically defined on the Concentrator, a combination of both, or disable CRL checking.

The next section is CRL caching. Since the Concentrator has to fetch and examine the CRL from a network-based DP, CRL checking might slow system response times or cause the IPSec tunnel to fail due to IKE timeout issues. Enable CRL caching to mitigate these potential problems. CRL caching stores the retrieved CRLs in local volatile memory. This enables the Concentrator to verify the revocation status of certificates more quickly.

The last section is configuring the location of CRL-DPs. One of the responsibilities of a CA is to create a database of all revoked certificates. This is referred to as a CRL. CAs locate CRLs at network-based DPs, or CRL-DPs. Many certificates include the location of theses CRL-DPs. If the CRL-DP is present in the certificate and in the proper format, you do not need to configure any CRL-DP fields in this window. If a CRL-DP is not present or you choose to define additional CRL-DPs, define the CRL-DP addresses in the Static CRL-DP window.

There is more discussion of configuring CAs later in this lesson.

## Configuring CRL Retrieval Policy

Cisco.com

**Administration | Certificate Management | Configure CA Certificate**

Certificate AUSTIN at TRAINING

**CRL Retrieval Policy**

○ Use CRL distribution points from the certificate being checked
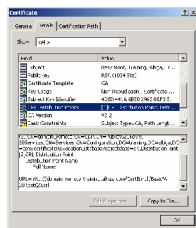
○ Use static CRL distribution points

○ Use CRL distribution points from the certificate being checked or else use static CRL distribution points
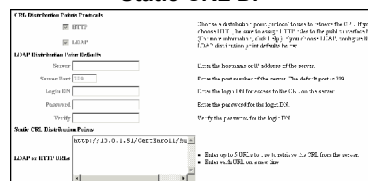
○ No CRL checking

Choose the method to use to retrieve the CRL.

**Certificate CRL DP**

**Static CRL DP**

CSVPN 4.0—6-45

During IKE phase 1 negotiation, if CRL checking is enabled, the Concentrator verifies the revocation status of the IKE peer certificate before allowing the IPSec tunnel to be established. CRLs exist on external servers maintained by CAs. The Concentrator retrieves the CRL using one of the available CRL-DPs and checks the peer certificate serial number against the list of serial numbers in the CRL to verify the revocation status. If there are no matches, the Concentrator assumes that the peer certificate has not been revoked. The CRL retrieval options are as follows:

■ Use CRL Distribution Points from the certificate being checked—The Concentrator retrieves up to five CRL-DPs from the CRL-DP extension of the certificate being verified. The Concentrator also augments the CRL-DP's information with the configured default values, if necessary. If the Concentrator's attempt to retrieve a CRL using the primary CRL-DP fails, the Concentrator retries using the next available CRL-DP in the list. This process continues until either a CRL is retrieved or the list is exhausted.

■ Use static CRL Distribution Points—Use up to five static CRL-DPs, as specified on this window. If you choose this option, you must enter at least one, and no more than five, static CRL-DPs.

■ Use CRL Distribution Points from the certificate being checked, or else use static DPs—If the Concentrator cannot find five CRL-DPs in the certificate, it adds static CRL-DPs, up to a limit of five. If you choose this option, be sure to choose a CRL-DP Protocol. If you choose a LDAP protocol, be sure to set the LDAP DP defaults as well. You also must enter at least one, and no more than five, static CRL-DPs.

■ No CRL Checking—Do not enable CRL checking.

## Configuring CRL Caching

**Certificate Authorities** [ View All CRL Caches | Clear All CRL Caches ] (current: 1, maximum: 6)

| Subject | Issuer | Expiration | SCEP Issuer | Actions |
|---|---|---|---|---|
| AUSTIN at TRAINING | AUSTIN at TRAINING | 06/04/2005 | No | View | Configure | Delete |

Administration | Certificate Management | Configure CA Certificate

**Certificate** AUSTIN at TRAINING

**CRL Retrieval Policy**

- ○ Use CRL distribution points from the certificate being checked
- ● Use static CRL distribution points
- ○ Use CRL distribution points from the certificate being checked or else use static CRL distribution points        Choose the method to use to retrieve the CRL.
- ○ No CRL checking

**CRL Caching**

**Enabled** ☑        Check to enable CRL caching. Disabling will clear CRL cache.

**Refresh Time** 5        Enter the refresh time in minutes (5 - 1440). Enter 0 to use the Next Update field in the cached CRL.

CSVPN 4.0—6-46

With CRL Caching enabled, when the Concentrator verifies a certificate's revocation status, it first verifies whether the required CRL exists in the cache and verifies the certificate's serial number against the CRL's list of serial numbers. The certificate is considered revoked if its serial number is found. The Concentrator retrieves a CRL from an external server either when it does not find the required CRL in the cache, or when the validity period of the cached CRL has expired. When the Concentrator receives a new CRL from an external server, it updates the cache with the new CRL.

The administrator must decide whether to enable CRL caching, and if so, what the cache refresh period is. The caching configuration options are as follows:

- Enabled—Select the Enabled check box to allow the Concentrator to cache retrieved CRLs. The default is not to enable CRL caching. Disabling CRL caching, by deselecting the check box, clears the CRL cache.

- Refresh Time—Specify the refresh time in minutes for the CRL cache. The range is 5 to 1440 minutes; the default value is 60 minutes. Enter **0** to use the Next Update field, if specified, in the cached CRL.

The total memory allocated for all combined CRL caches varies by Concentrator model and is as follows:

- Cisco VPN 3005 Concentrator—Can cache up to 128 KB

- Cisco VPN 3015 Concentrator—Can cache up to 256 MB

- Cisco VPN 3030 Concentrator—Can cache up to 256 MB

- Cisco VPN 3060 Concentrator—Can cache up to 1 MB

- Cisco VPN 3080 Concentrator—Can cache up to 1 MB

The CRL cache exists in memory. Rebooting the Concentrator clears the CRL cache. The Concentrator re-populates the CRL cache with updated CRLs as it processes new peer authentication requests. The embedded management enables the user to delete cached CRLs issued by a particular CA. This will enable the user to force a CRL update to be performed with the next IPSec tunnel establishment attempt.

## Configuring CRL DPs

Cisco.com

**LDAP** support    **HTTP** support

Site A

Primary

Backup

Client

**CRL Distribution Points Protocols**
☑ HTTP
☑ LDAP

Choose a distribution point protocol to use to retrieve the CRL. If you choose HTTP, be sure to assign HTTP rules to the public interface filter. (For more information, click Help.) If you choose LDAP, configure the LDAP distribution point defaults below.

**LDAP Distribution Point Defaults:**
Server _____      Enter the hostname or IP address of the server.
Server Port 389        Enter the port number of the server. The default port is 389.
Login DN _____   Enter the login DN for access to the CRL on the server.
Password _____   Enter the password for the login DN.
Verify _____     Verify the password for the login DN.

**Static CRL Distribution Points**
http://10.0.1.51/CertEnroll/Au

LDAP or HTTP URLs
• Enter up to 5 URLs to use to retrieve the CRL from the server.
• Enter each URL on a new line.

© 2003, Cisco Systems, Inc. All rights reserved.                CSVPN 4.0—6-47

CRL Distribution Points Protocols—Choose a DP protocol to use to retrieve the CRL if the primary CRL-DP is unavailable. If you choose HTTP, be sure to assign HTTP rules to the public interface filter. If you choose LDAP, configure the LDAP DP defaults as follows:

■ LDAP Distribution Point Defaults—If you specified LDAP as the CRL-DP protocol, enter the following information. If the DP extension of the peer's certificate is missing any of the following fields, the Concentrator enters these values:

— Server—Enter the IP address or hostname of the CRL-DP server (LDAP server). The maximum field length is 32 characters.

— Server Port—Enter the port number for the CRL server. Enter **0** (the default) to have the system supply the default port number: 389 (LDAP).

— Login DN—Enter the login DN (Distinguished Name)), which defines the directory path to access this CRL database (for example, cn=crl, ou=certs, o=CANam, c=US). The maximum field length is 128 characters.

— Password—Enter the password for the Login DN. The maximum field length is 128 characters.

— Verify—Re-enter the password to verify it. The maximum field length is 128 characters.

■ Static CRL Distribution Points—Enter the HTTP or LDAP address of the external servers where the CRLs are located. If you chose a CRL Retrieval Policy that uses static DPs, you must enter at least one, but not more than five, valid URLs. Enter each URL on a single line. (Scroll right to enter longer values.)

The following are examples of valid URLs:

■ HTTP URL: http://10.0.1.51/CertEnroll/AUSTIN.cri

■ LDAP URL: ldap://100.199.7.6:389/CN=TestCA68,CN=2KPDC,CN=CDP, CN=Public Key
Services,CN=Services,CN=Configuration,DC=qa2000,
DC=com?certficateRevocationList?base?objectclass=cRLDistributionPoint

**Step 1—Check the Active IKE Proposal List**

You must complete the following before the Client-to-LAN with digital certificates tunnel can be configured:

**Step 1**  Check the Active Internet Key Exchange (IKE) proposal list. For Client-to-LAN with digital certificates to work, the Concentrator requires the use of a RSA IKE proposal.

**Step 2**  Check the IKE proposal.

**Step 3**  Modify or add an SA.

## Step 2—Check the IKE Proposal

Cisco.com

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify

Modify a configured IKE Proposal.

| | | |
|---|---|---|
| Proposal Name | CiscoVPNClient-3DES- | Specify the name of this IKE Proposal. |
| Authentication Mode | RSA Digital Certificate (XAUTH) ▾ | Select the authentication mode to use. |
| Authentication Algorithm | MD5/HMAC-128 ▾ | Select the packet authentication algorithm to use. |
| Encryption Algorithm | 3DES-168 ▾ | Select the encryption algorithm to use. |
| Diffie-Hellman Group | Group 2 (1024-bits) ▾ | Select the Diffie Hellman Group to use. |
| Lifetime Measurement | Time ▾ | Select the lifetime measurement of the IKE keys. |
| Data Lifetime | 10000 | Specify the data lifetime in kilobytes (KB). |
| Time Lifetime | 86400 | Specify the time lifetime in seconds. |

Apply    Cancel

CSVPN 4.0—6-49

Check the activated RSA Internet Key Exchange (IKE) proposal to ensure that it meets the authentication, encryption, Diffie-Hellman (DH), and lifetime requirements. In the figure, the RSA IKE proposal supports the following:

- Authentication mode—RSA digital certificates

- Authentication algorithm—MD5

- Encryption algorithm—3DES

- DH group—DH group 2

- Lifetime measurement and lifetime—Time and 86400 seconds

---

| | |
|---|---|
| **Note** | For the IPSec Client-to-LAN applications, the authentication mode is changed from pre-shared keys to digital certificates. |

---

**Step 3—Modify or Add an SA**

Cisco.com

Configuration | Policy Management | Traffic Management | Security Associations

Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IKE Proposals to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs    Actions

ESP-DES-MD5
ESP-3DES-MD5
ESP/IKE-3DES-MD5
ESP-3DES-NONE
ESP-L2TP-TRANSPORT
ESP-3DES-MD5-DH7
ESP-3DES-MD5-DH5
ESP-AES128-SHA

Add
Modify
Delete

CSVPN 4.0—6-50

Modify or add a Security Association (SA). The SA is a template that defines IPSec and IKE attributes. There are two choices: modify an existing SA, or add a new one. If you modify an existing SA, you change it from pre-shared keys, which is the default, to RSA signed digital certificates. By changing it, you may be enabling the Client-to-LAN with digital certificates tunnels but disabling the use of pre-shared keys for someone else. The best choice is to add an SA. Click **Add** to add an SA.

## IPSec SA



CSVPN 4.0—6-51
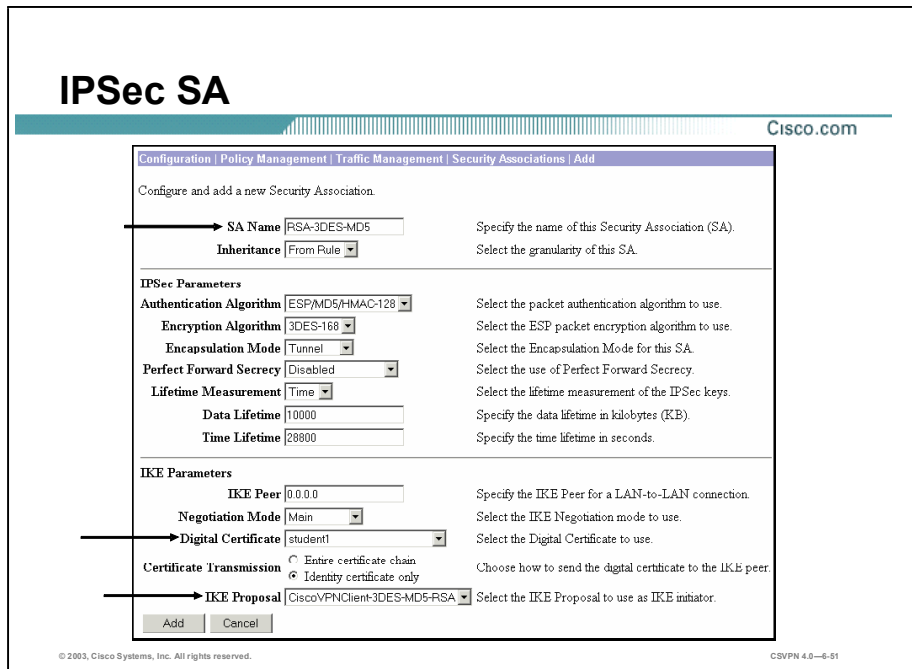
When adding a Security Association (SA), give the SA a descriptive name, such as RSA-3DES-MD5. Next, there are two sections to check: IKE and IPSec. In the IPSec parameter section of the window, verify the authentication, encryption, DH, and lifetime parameters. In the figure, the IPSec proposal supports the following:

■ Authentication algorithm—MD5

■ Encryption algorithm—3DES

■ Encapsulation mode—Tunnel

■ DH group—DH group 2

■ Lifetime measurement and lifetime—Time and 28800 seconds

Choose the IKE parameters that will be applied to this SA in the IKE Parameters section. Choose the correct certificate from the Digital Certificate drop-down menu to do this. In the figure, the student1 certificate was chosen. This certificate is used during the certificate exchange. Next, choose **CiscoVPNClient-3DES-MD5-RSA** from the IKE Parameters drop-down menu. Click **Apply**.

## Types of VPN Client Enrollment

Cisco.com

**File (manual)**

Certificate server

Generate PKCS #10

Upload PKCS #10

Download identity and root certificate

**Network (automated)**

Certificate server

SCEP
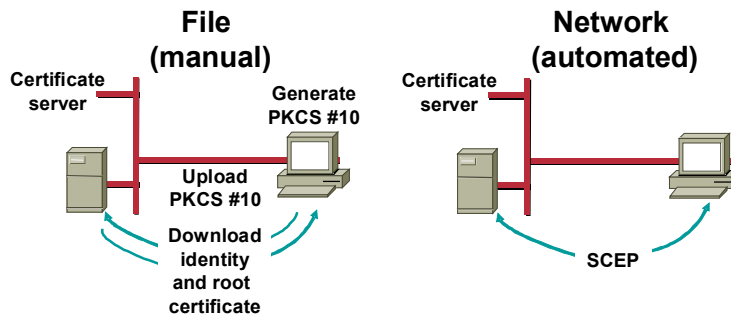
CSVPN 4.0—6-52

For the VPN Client to participate in the certificate exchange, a certificate needs to be loaded on the PC, which is called VPN Client enrollment. There are two types of VPN Client enrollment:

- File-based enrollment—This is a manual process. You can enroll by creating a request file, PKCS#10. When you have created a request file, you can either e-mail it to the CA and receive a certificate, or you can access the CA's web site and cut and paste the enrollment request in the area that the CA provides. When generated by the CA, identity and root certificates are downloaded to the PC. The certificates must then be imported into the certificate manger.

- Network-based enrollment—This is an automated process, which enables you to connect directly to a CA via SCEP. Complete the enrollment form to connect to a CA via SCEP. The Certificate Manager uses SCEP to send the request to the CA, where the CA issues an identity certificate. The CA then returns both the identity and CA certificates back to the Certificate Manager. In order for network-based enrollment to work, both the end device and the CA must support SCEP.

# Certificate Tab

Cisco.com

**Certificate tab used to enroll and manage personal certificates**

CSVPN 4.0—6-53
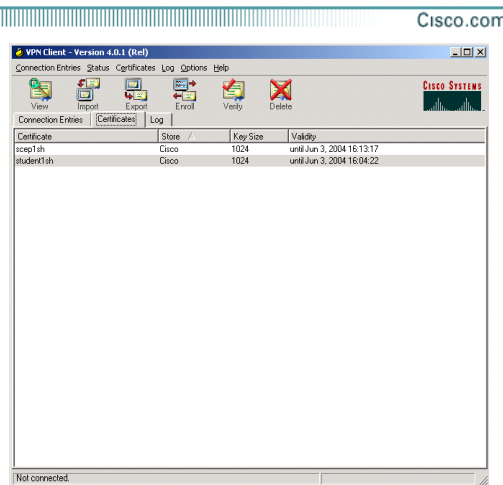
You can use the Certificate Tab to enroll and manage personal certificates. Specifically, you can use the Certificate Tab to do the following:

■ Import certificates.

■ Manage certificates by viewing, verifying, deleting, or exporting them.

■ Manage enrollment requests.

Obtain personal certificates through enrollment with a CA. You can enroll automatically through the network or manually via a file exchange.

**Certificate Store**

A certificate store is a
location in your local
file system that contains
personal certificates.
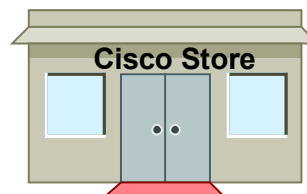
Cisco Store

A certificate store is a location in your local file system that contains personal certificates. The major store for the VPN Client is the Cisco store, which contains certificates you have enrolled for through the Simple Certificate Enrollment Protocol (SCEP). Your system also includes a Microsoft certificate store that may contain certificates that your organization provides or that you have installed previously. You can manage them just like the certificates in your Cisco store, or you can import them to your Cisco store. New certificates obtained through enrollment or importing go into the Cisco store.

# File Enrollment

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—6-55
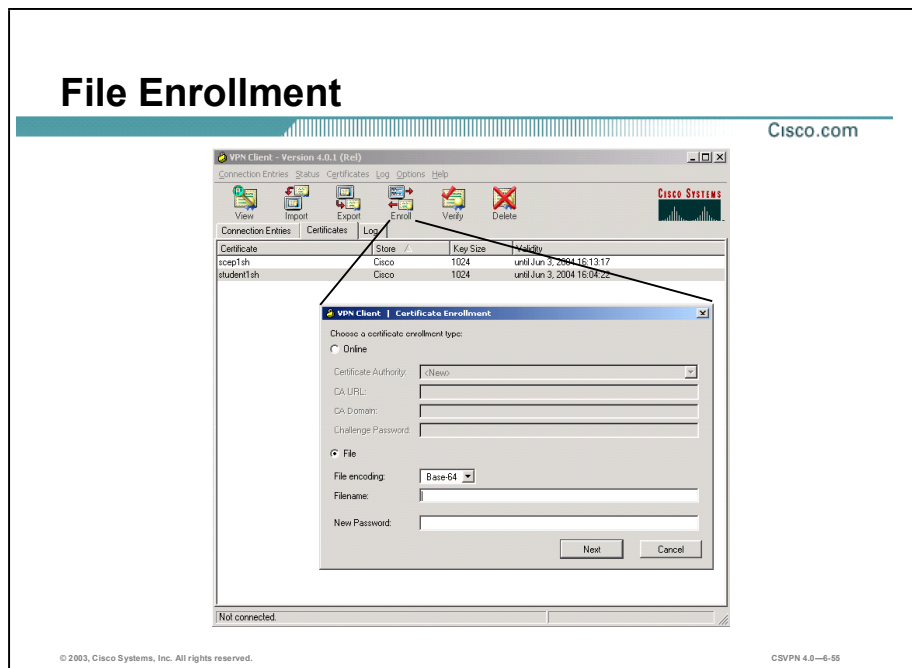
You can enroll by creating a file using the Certificate Enrollment form. Once you have created a request file, you can either e-mail it to the CA and receive a certificate back or you can access the CA's Web site and cut and paste the enrollment request in the area that the CA provides.

Yu must choose one of the following file types:

■ Binary encoded—A base-2 PKCS10 file (Public Key Cryptography Standard; for example, an X.509 DER file). You cannot display a binary-encoded file.

■ Base 64 encoded—An ASCII-encoded PKCS10 file that you can display in text format Choose this type when you want to cut and paste the text into the CA Web site.

In the Filename field, enter the full pathname for the file request.

In the New Password field, enter the password that protects this certificate. If your connection entry requires certificate authentication, you must enter this password each time you connect. The password can be up to 32 characters in length.

Clicking **Next** displays page two of the enrollment request.

## Enrollment Form

**VPN Client | Certificate Enrollment**

Enter certificate fields, "*" denotes a required field:

Name [CN]*:

Department [OU]:

Company [O]:

State [ST]:

Country [C]:

Email [E]:

IP Address:

Domain:

Back    Enroll    Cancel

CSVPN 4.0—6-56

Before you can build a certificate request, the administrator must supply some enrollment information. There are eight fields in the enrollment form:

- Common Name—The unique name used for this certificate. This field is required. It will become the name of the certificate (for example, student1).

- Dept—The name of the department to which you belong (for example, training). This field correlates to the OU. For example, the OU is the same as the group name configured in a Concentrator.

- Company—The name of the company or organization to which you belong (for example, Cisco).

- State—The name of your state (for example, Massachusetts).

- Country—The two-letter country code for your country (for example, US).

- Email—Your e-mail address (for example, asmith@cisco.com).

- IP Address—The IP address of your system (for example, 172.26.26.1).

- Domain—The name of the domain your system is in (for example, cisco.com). It can be a FQDN (for example, training.cisco.com).

After completing the form, click **Enroll**. The VPN Client displays a message to let you know whether your request succeeded. If successful, the message contains the name of the file.

# Paste Certificate Request

Cisco.com

Certificate server

Generate PKCS #10

Upload PKCS #10

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—6-57

When an enrollment request file is generated, the enrollment request file is saved on the PC hard drive. You access the enrollment request file, copy its contents, and paste it into the appropriate window on the Microsoft CA. To do this, complete the following:

**Step 1**  Locate the enrollment request file on the PC. Double click the file. The file should resemble a Notepad file.

**Step 2**  Select the contents of the file by selecting **Edit**>**Select All**. Copy the contents by selecting **Edit**>**Copy**.

**Step 3**  Copy the contents of the enrollment request file into the appropriate window on the CA. Select the CA window and press **Ctrl+V**. This pastes the contents of the paste buffer into the area provided by the CA. The CA now creates an identity certificate.

Download Root and Identity Certificates
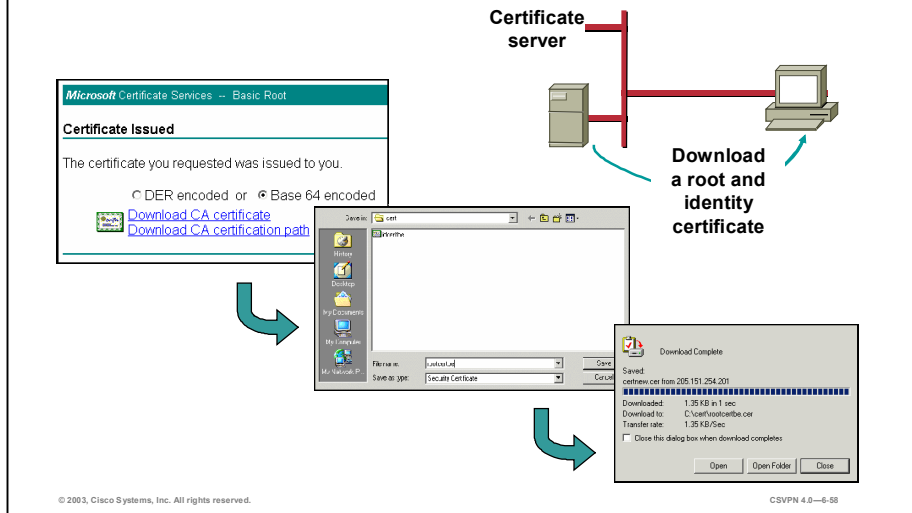
From an enrollment form, the Certificate Manager creates an enrollment request. The contents of the request file are transferred to the CA via cut and paste. The CA issues a new identity certificate. After the CA generates an identity certificate, the identity and root certificates are downloaded to the PC. Complete the following steps to download the certificates:

**Step 1**   Choose an encoding scheme: DER or Base 64 encoding. Either will work and the client can handle both schemes.

**Step 2**   Select the type of download: CA certificate or CA certificate path. The CA certificate downloads the identity certificate only. The root certificate is downloaded next or the CA certificate path is selected. The CA certificate path downloads both the identity and root certificate, PKCS#7. Selecting the download type starts the download.

**Step 3**   The Save-in window opens. Choose the destination folder from the Save In drop-down menu. In the file name window, enter the name of the file; the default file name is certnew. Re-name the file to something more descriptive such as PC new_york. Make note of the destination folder and file name; you will need them when the certificates are imported. Click **Save**.

**Step 4**   The Download Complete window opens. Click **Close**. The process is complete. The certificates are on the PC's hard drive.

## Import Certificates

Cisco.com

**VPN Client | Import Certificate**

- Import from File

Import Path: [_____] Browse

Import Password: [_____]

- Import from Microsoft Certificate store

Import Certificate: [_____▼]

Entering a new password is optional. It is recommended to password protect identity certificates.

New Password: [_____]

Confirm Password: [_____]

[ Import ] [ Cancel ]

© 2003, Cisco Systems, Inc. All rights reserved.          CSVPN 4.0—6-89

The last step is to import the identity and root certificates into the certificate store. Clicking on the **Import** button brings up the Import Certificate Window. You choose whether you are going to import from a file or from a Microsoft Certificate Store and browse to the appropriate file.

The following fields are available:

- Import Path—The complete pathname for the certificate. You can type the name or browse your file system to locate the file.

- Import Password—This password must exactly match the password given during enrollment (online) or given when exported (if a file), including upper and lower case letters. For example, sKate8 is not exactly the same as Skate8. In online enrollment, this password is kept with the certificate; in file enrollment, this password is not retained.

- New Password—The password to be stored with the certificate. Use this password to protect the certificate while it is in the certificate store. This password is optional but we recommend that you always protect your certificate with a password.

- Confirm Password—The password that you enter here must match what you entered in the New Password field.

To complete the import request, click the **Import** button.

# Viewing Certificates
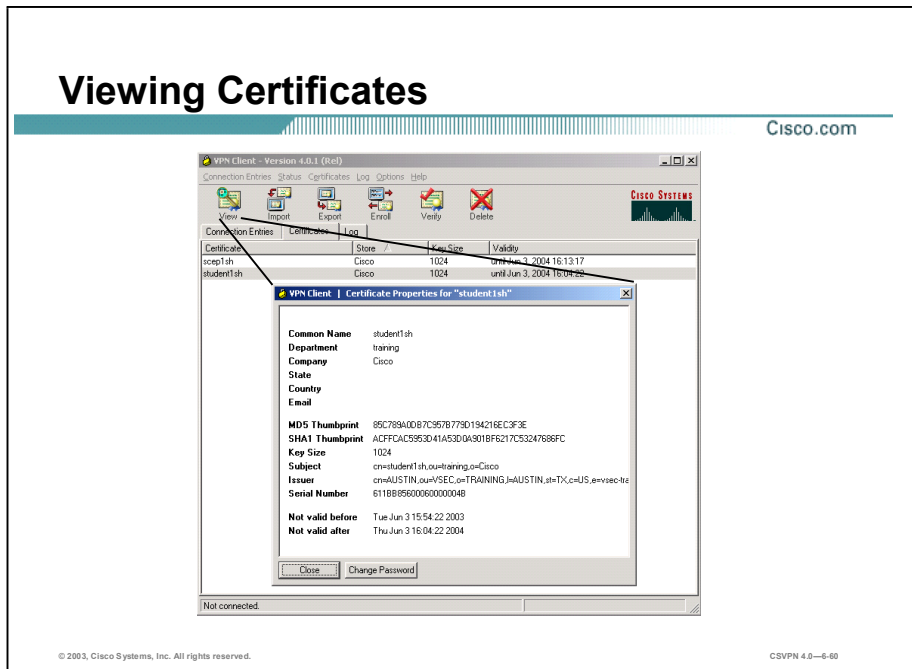
To display a certificate, select it in the certificate store, then do one of the following:

- Open the Certificates menu and choose **View**.

- Click **View** on the toolbar above the Certificates tab.

- Double-click the certificate.

**Network-Based Enrollment**

Network
(automated)

Certificate
server

SCEP

CSVPN 4.0—6-61
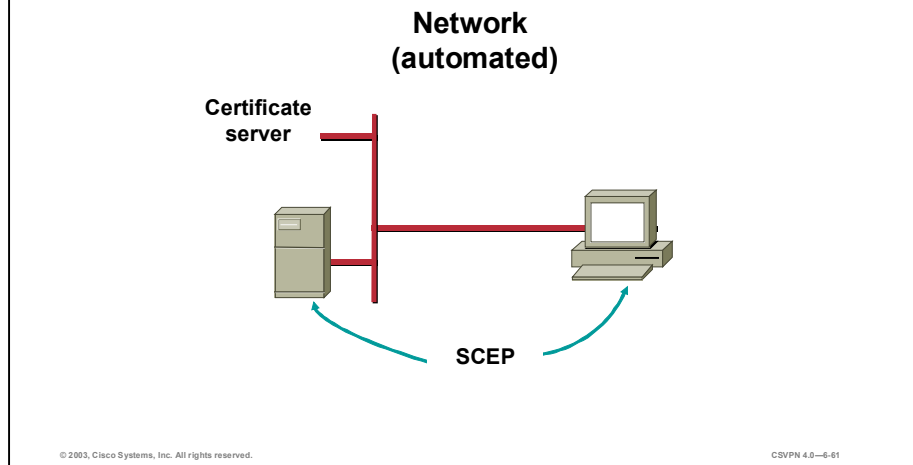
File-based enrollment is a file transfer-intensive process; however, network-based enrollment is an automatic process, which enables you to connect directly to a CA via SCEP. Complete the enrollment form to connect to a CA via SCEP. The Certificate Manager uses SCEP to send the request to the CA, where the CA issues an identity certificate. The CA then returns both the CA or RA and identity certificates back to the Certificate Manager. For network-based enrollment to work, both the end device and the CA must support SCEP.

**SCEP**

Cisco.com

Certificate manager                SCEP                Certificate server

Request CA or RA certificate → Return CA or RA certificate

Verify CA or RA certificate generation keys

Generate certificate request
Send request → Process request
- If approved, generate identity certificate
– or –
Store certificate ← - If pending approval

Request pending
Send polling request ← (Approved)

Store certificate ←

CSVPN 4.0—6-62
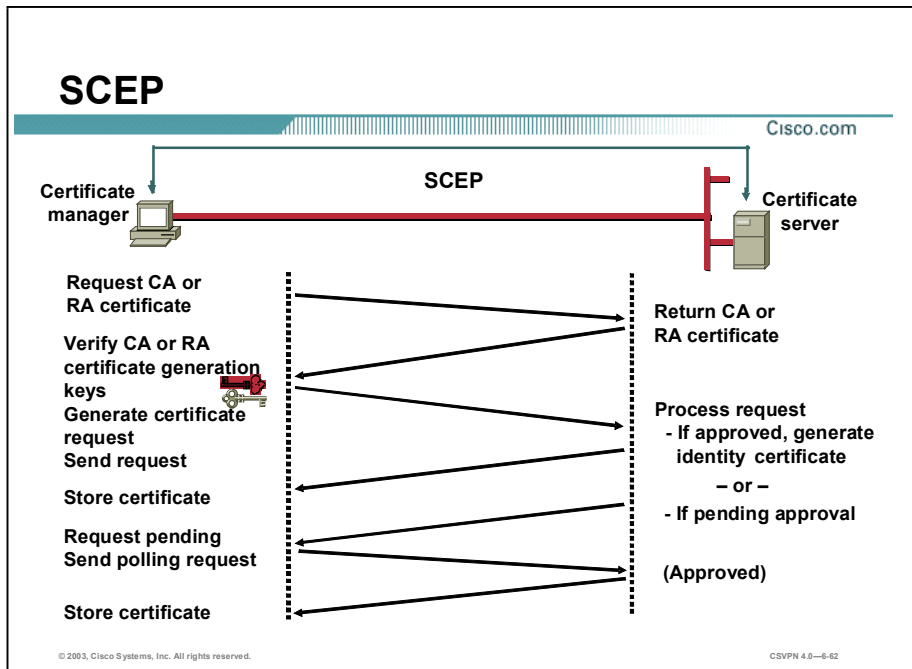
The SCEP operates between the client and the Certificate server. The certificate request process is always the same, but the approval process varies depending upon whether the identity certificate is automatically or manually approved. The approval process varies between CAs. In a private network where the corporation owns the CA, the approval process may be set to automatic: the user makes a request, the CA approves the request, and an identity certificate is generated. If the user is making the request of a public CA, the request may be delayed pending a manual approval process. The following is the SCEP process:

■ Send the CA or RA certificate request to the CA.

■ The CA returns a CA or RA certificate.

■ The Certificate Manager:

— Verifies the CA or RA.

— Generates keys.

— Generates the certificate request.

— Sends the certificate request to the CA.

■ The CA processes the request, generates an identity certificate, and returns the identity certificate to the Certificate Manager.

■ Or, the CA places the request in a pending (approval) file and returns the pending message to Certificate Manager.

— The Certificate Manager will periodically send a poll to the CA.

If the identity certificate is approved, the CA sends it to the Certificate Manager.

**Network Enrollment**

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—6-63
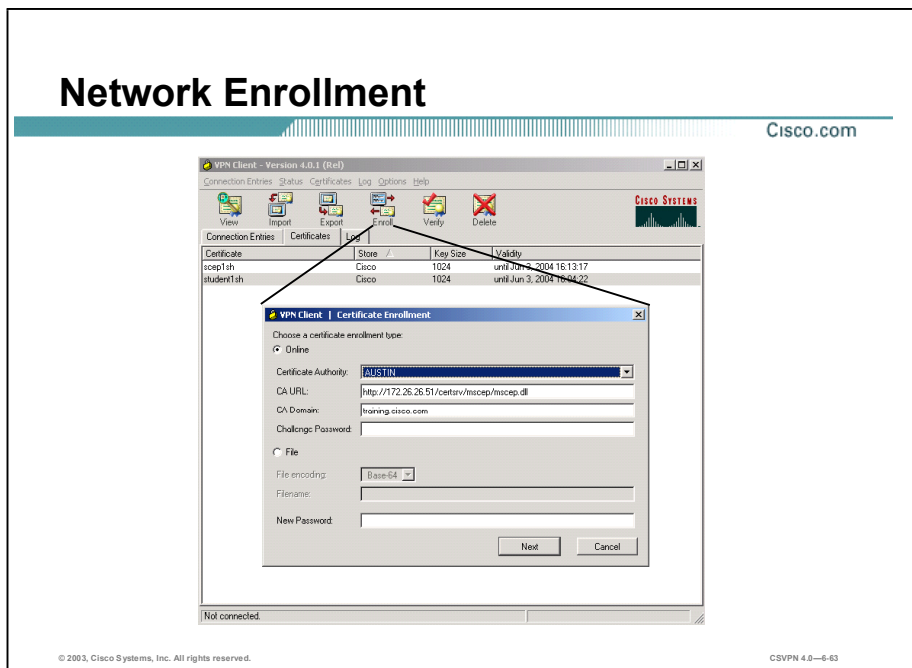
Choosing Online in the Certificate Enrollment windows allows you to request your certificates via the network. Network-based enrollment is an automatic process, which enables you to connect directly to a CA via SCEP. Fill out the enrollment form to connect to a CA via SCEP. The Certificate Manager uses SCEP to send the request to the CA, where the CA issues an identity certificate. The CA then returns both the CA and RA and identity certificates to the Certificate Manager. The file exchange process is automatic. For network-based enrollment to work, both the end device and the CA must support SCEP.

The following fields are available:

■ CA URL—The URL or network address of the CA. This parameter is required.

■ CA Domain—The CA's domain name. This parameter is required.

■ Challenge Password—Some CA's require a password to access their site. If such is the case with this CA, enter the password in the Challenge Password field. To find out the password, contact the CA or your network administrator.

■ New Password—The password that protects this certificate. If your connection entry requires certificate authentication, you must enter this password each time you connect. The password can be up to 32 characters in length. Passwords are case sensitive. For example, *sKate8* and *Skate8* are different passwords.

Clicking **Next** displays page two of the enrollment request.

**Enrollment Form**

Cisco.com

VPN Client | Certificate Enrollment

Enter certificate fields. "*" denotes a required field:

Name [CN]*:

Department [OU]:

Company [O]:

State [ST]:

Country [C]:

Email [E]:

IP Address:

Domain:

VPN Client

Certificate enrollment is now pending.

To continue the current enrollment, select the certificate being enrolled and do one of the following:

- Choose Retry from the Certificates menu.
OR
- Right-click the selected certificate and choose Retry.

OK

CSVPN 4.0—6-64

As with File based enrollment, before you can build a certificate request, the administrator must supply some enrollment information. There are eight fields in the enrollment form:

■ Common Name—The unique name used for this certificate. This field is required. It will become the name of the certificate (for example, student1).

■ Dept—The name of the department to which you belong (for example, training). This field correlates to the OU. For example, the OU is the same as the group name configured in a Concentrator.

■ Company—The name of the company or organization to which you belong (for example, Cisco).

■ State—The name of your state (for example, Massachusetts).

■ Country—The two-letter country code for your country (for example, US).

■ Email—Your e-mail address (for example, asmith@cisco.com).

■ IP Address—The IP address of your system (for example, 172.26.26.1).

■ Domain—The name of the domain your system is in (for example, cisco.com). It can be a FQDN (for example, training.cisco.com).

To complete the enrollment, click **Enroll**. (Or to edit the form click **Back**).

What happens next depends on your CA.

- Some CAs provide an immediate response. If so, you see a message that your enrollment succeeded. You can view and manage the certificate under the Certificates tab.

- If the enrollment status is Request pending, your CA does not immediately approve your request. You see a status pending pop up window.

# Summary

This topic summarizes what you learned in this lesson.

## Summary

- **Digital certificates bind a person or entity to a private key.**
- **The Cisco VPN Client and Concentrator create PKCS #10s.**
- **PKCS #10s are sent to the CA to be verified.**
- **The CA issues VPN Client and Concentrator X.509 certificates.**
- **Certificates are loaded on the VPN Client and Concentrator.**
- **Certificates are exchanged during IKE negotiations.**
- **Certificates are validated by the receiving device.**

CSVPN 4.0—6-66

# Lab Exercise—Configure the Cisco VPN 3000 Series Concentrator for Remote Access Using Digital Certificates

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to install and configure the Cisco Virtual Private Network (VPN) Client and the Cisco VPN 3000 Series Concentrator to enable Internet Protocol Security (IPSec) encrypted tunnels using digital certificates. In this lab exercise, you will work with your lab exercise partner to complete the following tasks:

■ Complete lab exercise setup.

■ Return the Concentrator to factory settings.

■ Configure the Concentrator private interface using the CLI.

■ Configure the Concentrator public interface using the CLI.

■ Configure the Concentrator default gateway using the CLI.

■ Configure the Concentrator using the Cisco VPN 3000 Concentrator Series Manager.

■ Modify the Concentrator public filter.

■ Enable the Concentrator public filter.

■ Generate the PKCS#10 certificate request.

■ Send the PKCS#10 certificate request to the certificate server.

■ Download a new identity certificate to the student PC.

■ Generate a root certificate and download it to the student PC.

■ Load the root certificate into the Concentrator.

■ Load the identity certificate into the Concentrator.

■ Activate the Concentrator IKE proposal.

■ Modify the Concentrator Security Associations.

- Verify the Concentrator IPSec Client-to-LAN group parameters.

- Create a certificate request on the Cisco VPN Client.

- Copy the request file to the paste buffer.

- Copy PKCS#10 to the certificate server.

- Download the Cisco VPN Client identity certificate.

- Retrieve the Cisco VPN Client root certificate.

- Import the Cisco VPN Client root certificate into the certificate store.

- Import the Cisco VPN Client identity certificate into the certificate store.

- Configure the Cisco VPN Client for digital certificates.

- Launch the Cisco VPN Client.

- Configure the certificate manager for network-based certificates.

- Create a new Cisco VPN Client connection record.

- Launch the Cisco VPN Client.

- Configure DN matching rules.

- Launch the Cisco VPN Client.

- Launch the Cisco VPN Client.

- Return the Cisco VPN Client and Concentrator to pre-shared keys.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
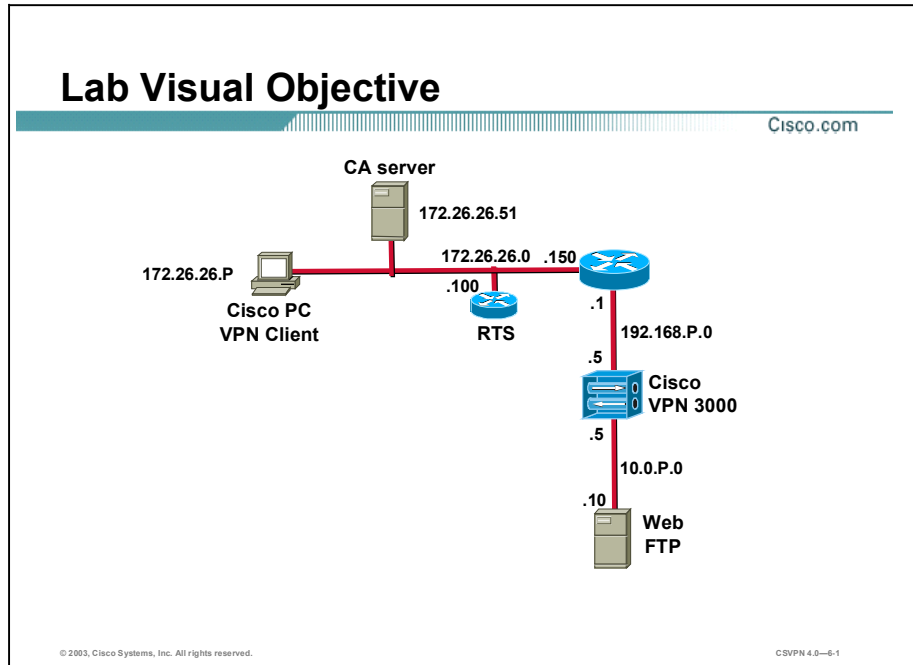


## Scenario

Your company wants you to implement a VPN using remotely located Cisco VPN Clients terminating at centrally located Concentrators. You must configure both the remote Cisco VPN Clients and the Concentrators for remote access using digital certificates for authentication.

## Task 1—Complete Lab Exercise Setup

Before starting this lab exercise, verify your equipment is setup as follows:

- Ensure that your student PC is powered on.

- Ensure that your student IP addresses are configured correctly:

  — Primary IP address—172.26.26.P
  (where P = pod number)

  — Default gateway IP address—172.26.26.150

- Ensure that your Concentrator is powered on.

- Ensure you can ping the certificate server, 172.26.26.51.

## Task 2—Return the Concentrator to Factory Settings

The instructor will provide you with procedures to access the Concentrator's console port, as this procedure will vary according to your connectivity. After accessing the Concentrator's console port, the Concentrator prompt will appear. Complete the following steps to return the Concentrator to the factory settings:

| Note | This procedure assumes that Windows 2000 is already running on the student PC. |
| --- | --- |

**Step 1** Log in to the Concentrator's command line interface (CLI) using the administrator account:

```
Login: admin
Password: admin
```

| Caution | If you get a Quick prompt for the system time and date parameters, the device has already been rebooted to factory defaults. Proceed directly to Task 3. |
| --- | --- |

**Step 2** Access the Administration menu:

```
Main -> 2
```

**Step 3** Access the System Reboot menu:

```
Admin -> 3
```

**Step 4** Access the Schedule Reboot menu:

```
Admin -> 2
```

**Step 5** Select Reboot ignoring the Configuration file:

```
Admin -> 3
```

**Step 6** Select Reboot Now:

```
Admin -> 2
```

The Reboot scheduled immediately message appears, followed by the Rebooting VPN 3000 Concentrator Series now message. Do not attempt to log in to the first login prompt you see as it takes several moments for the Concentrator to complete the reboot function. A login prompt appears when the reboot is complete.

**Step 7** Leave the Command Prompt window open.

## Task 3—Configure the Concentrator Private Interface Using the CLI

Complete the following steps to configure the Cisco VPN 3000 Series Concentrator private local area network (LAN) interface using the CLI quick configuration mode. This procedure assumes that the CLI session is still active. If it is not active, follow steps 1−7 of Task 2 before proceeding.

**Step 1** Log in to the Concentrator's CLI using the administrator account and complete the following actions, starting from the CLI top-level menu:

```
Login: admin
```

```
        Password: admin
```

When an administrator reboots a Concentrator, as in the previous task, CLI menus open in a slightly different order. If you get the Quick prompt for the system parameters, press **Enter** through the time, date, time zone, DST prompts. Complete the following steps:

**Step 2**    Enter the Concentrator's private interface IP address:

```
Quick Ethernet 1 -> [0.0.0.0] 10.0.P.5
```

(where P = pod number)

**Step 3**    Enter the Concentrator's private interface subnet mask:

```
Quick Ethernet 1-> [255.0.0.0] 255.255.255.0
```

**Step 4**    Accept the default Ethernet speed of 10/100 Mbps Auto Detect:

```
Quick Ethernet 1-> [3] <Enter>
```

**Step 5**    Accept the default duplex mode of Half/Full/Auto:

```
Quick Ethernet 1-> [1] <Enter>
```

**Step 6**    Accept the default maximum transmission unit (MTU) size:

```
Quick Ethernet 1-> [1500] <Enter>
```

**Step 7**    Save changes to the configuration file:

```
Quick -> 3
```

**Step 8**    Exit the CLI:

```
Quick -> 5
```

If you do not exit, the CLI continues its quick configuration script. You will use the standard CLI menus for the remaining parameters.

**Step 9**    Leave the command prompt window open.

## Task 4—Configure the Concentrator Public Interface Using the CLI

Complete the following steps to configure the Concentrator's public interface:

**Step 1**    Log in to the Concentrator's CLI using the administrator account and complete the following actions starting from the CLI top-level menu:

```
Login: admin
Password: admin
```

**Step 2**    Select the Configuration menu:

```
Main -> 1
```

**Step 3**    Select the Interface Configuration menu:

```
Config -> 1
```

**Step 4**    Select the Configure Ethernet #2 (Public) menu:

```
Interfaces -> 2
```

**Step 5**    Select the Interface Setting menu:

```
Ethernet Interface 2 -> 1
```

**Step 6**  Accept the default setting of Enable using Static IP Addressing:

```
Ethernet Interface 2 -> [3] <Enter>
```

**Step 7**  Enter the Concentrator's public interface IP address:

```
Ethernet Interface 2 -> [0.0.0.0] 192.168.P.5
```

(where P = pod number)

**Step 8**  Accept the default setting for the subnet mask:

```
Ethernet Interface 2 -> [255.255.255.0] <Enter>
```

Several messages appear indicating the condition of the Ethernet #2 (public) interface.

**Step 9**  Select the Select IP Filter menu:

```
Ethernet Interface 2-> 3
```

**Step 10**  Select **0** (no filter) on the Ethernet #2 (public) interface:

```
Ethernet Interface 2 -> [Public (Default)] 0
```

In this lab exercise, you disable filtering on the public LAN interface to allow access to the HTTP-based Cisco VPN 3000 Concentrator Series Manager from your student PC. Never select 0 (no filter) in a live network, as this could facilitate a security breach.

**Step 11**  Return to the top-level menu:

```
Ethernet Interface 2 -> h
```

**Step 12**  Save changes to the configuration file:

```
Main -> 4
```

**Step 13**  Remain logged in to the CLI and leave the Command Prompt window open.

## Task 5—Configure the Concentrator Default Gateway Using the CLI

Complete the following steps to set the Concentrator's default gateway parameter to the IP address of the perimeter router, starting from the CLI top-level menu:

**Step 1**  Select the Configuration menu:

```
Main -> 1
```

**Step 2**  Select the System Management menu:

```
Config -> 2
```

**Step 3**  Select the IP Routing menu:

```
System -> 4
```

**Step 4**  Select the Default Gateways menu:

```
Routing -> 2
```

**Step 5**  Select the Set Default Gateway menu:

```
Routing -> 1
```

**Step 6**  Enter the perimeter router IP address:

```
             Routing -> 192.168.P.1
```

(where P = pod number)

**Step 7**  Select the Set Default Gateway Metric menu:

```
             Routing -> 2
```

**Step 8**  Accept the Default Gateway Routing Metric of 1:

```
             Routing -> [1] <Enter>
```

**Step 9**  Return to the top-level menu:

```
             Routing -> h
```

**Step 10** Save changes to the configuration file:

```
             Main -> 4
```

**Step 11** Exit the CLI session:

```
             Main -> 6
```

**Step 12** Close the Command Prompt window.

# Task 6—Configure the Concentrator Using the Cisco VPN 3000 Concentrator Series Manager

Earlier you configured both the private and public interfaces using the CLI feature of the Concentrator. Complete the following steps to finish the configuration using the Cisco VPN 3000 Concentrator Series Manager.

---

**Note**        This procedure assumes that Windows 2000 is already running on the student PC.

---

**Step 1**  Launch Internet Explorer by double-clicking the desktop icon.

**Step 2**  Enter the Concentrator's public interface IP address of **192.168.P.5** in the Internet Explorer Address field (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 3**  Log in to the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

The username (login) and password are always case sensitive.

**Step 4**  In the main window, click **click here to start Quick Configuration**.

**Step 5**  Complete the following steps starting from the Configuration>Quick>IP Interfaces window:

1.  Verify the IP addresses of Ethernet 1 (10.0.P.5) and Ethernet 2 (192.168.P.5), which you configured via CLI.
    (where P = pod number)

2.  Click **Apply** if you have made changes to either Interface 1 or 2; otherwise click **Continue**.

**Step 6**  Complete the following sub-steps starting from the Configuration>Quick>System Info window:

---

1. Enter **podP** in the System Name field.
   (where P = pod number)

Your instructor will provide you with the values to complete the following table:

| Parameter | Value |
|---|---|
| Time (Hour:Minute:Second AM/PM)<br><br>(for example, 2:45:00 PM) | |
| Date (Month/Day/Year)<br><br>(for example, July/6/2001) | |
| Time Zone (offset in hours from GMT)<br><br>(for example, (GMT–05:00) EST) | |
| Enable DST Support? (circle one) | SELECT      DE-SELECT |

2. Enter the correct time, date, and time zone from the previous table.

3. Select or de-select the **Enable DST Support** check box from the previous table.

4. Leave the DNS server IP address set to 0.0.0.0.

5. Enter **cisco.com** in the Domain field.

6. Leave the perimeter router IP address in the Default Gateway field.

7. Click **Continue**.

**Step 7** Complete the following sub-steps starting from the Configuration>Quick>Protocols window:

1. De-select the **PPTP** check box.

2. De-select the **L2TP** check box.

3. Select the **IPSec** check box.

4. Click **Continue**.

**Step 8** Complete the following sub-steps starting from the Configuration>Quick>Address Assignment window:

1. Select **DHCP**.

2. Enter a DHCP server IP address in the Specify Server field: **10.0.P.10**.
   (where P = pod number)

3. Click **Continue**.

**Step 9** Complete the following sub-steps starting from the Configuration>Quick> Authentication window:

1. Select **Internal Server** from the Server Type drop-down menu.

2. Click **Continue**.

**Step 10** Complete the following sub-steps starting from the Configuration>Quick>User Database window:

These entries are all case-sensitive. Use lower case.

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

3. Enter **studentP** in the Verify field.
   (where P = pod number)

4. Click **Add** to add the new user to the database.

5. The new username should appear in the Current Users list box.

6. Click **Continue**.

**Step 11** Complete the following sub-steps starting from the Configuration>Quick>IP Sec Group window:

These entries are all case-sensitive and must be entered in lower case.

1. Enter **training** in the Group Name field.

2. Enter **training** in the Password field.

3. Enter **training** in the Verify field.

4. Click **Continue**.

**Step 12** Click **Continue** from the Configuration>Quick>Admin Password window.

Normally you would change your password, but for lab consistency, leave the password at the default value.

**Step 13** Complete the following sub-steps starting from the Configuration>Quick>Done window:

1. Click the **Save Needed** icon (in the upper right of the window). The Save Successful window opens.

2. Click **OK** and leave the Internet Explorer window open.

## Task 7—Modify the Concentrator Public Filter

Filtering must be enabled on the Concentrator's public interface to allow the Cisco VPN Client to connect to the Concentrator. By definition, the public (default) filter permits only tunnel and Internet Control Message Protocol (ICMP) traffic to pass through the interface. This filter excludes any HTTP traffic from your student PC. For this lab exercise, the public filter can be modified to permit HTTP traffic to travel both inbound and outbound. Complete the following steps to configure and monitor the Concentrator from the public side of the network:

| Note | This is for lab exercise purposes only. For security reasons, HTTP In and Out should never be enabled on the public interface in a production environment. |
|---|---|

**Step 1** From the Configuration menu tree, drill down to **Policy Management>Traffic Management> Filters**.

**Step 2** Choose the **Public (default)** filter from the Filter list.

**Step 3** Click **Assign Rules to Filter** within Actions.

**Step 4** Choose **Incoming HTTP In (forward/in)** from the Available Rules list.

**Step 5** Click **Add**.

**Step 6** Choose **Incoming HTTP Out (forward/out)** from the Available Rules list.

**Step 7** Click **Add**.

**Step 8** Click **Done**.

## Task 8—Enable the Concentrator Public Filter

Filtering must be enabled on the public interface to allow the Cisco VPN Client to connect to the Concentrator. Earlier you temporarily set the public interface filter to 0 (none) so you could configure the Concentrator via HTTP. Complete the following steps to configure the public interface filter:

**Step 1** From the Configuration menu tree, drill down to **Interfaces>Ethernet 2 (Public)**.

**Step 2** Select the **General** tab.

**Step 3** Choose **Public (default)** from the Filter drop-down menu.

**Step 4** Click **Apply**.

**Step 5** Click the **Save Needed** icon to save your configuration changes.

## Task 9—Generate the PKCS#10 Certificate Request

When using the Cisco VPN Client for remote access with digital certificates, IPSec establishes a secure tunnel. During the IPSec tunnel establishment process, the Concentrator and the Cisco VPN Client must exchange digital certificates. Before digital certificates can be exchanged, a digital certificate must be loaded into both the Cisco VPN Client and the Concentrator. The next few tasks will lead you through the process of loading a digital certificate into the Concentrator. Complete the following steps to create a Concentrator generated certificate request form:

**Step 1** From the Administration menu tree, drill down to **Certificate Management**. View the Identity Certificates and Certificate Authorities sections of the window. If there are Identity and Root certificates present, complete the following sub-steps to delete them. (Otherwise continue on with the next step.)

1. Click **Delete** from the Identity Certificates Actions column. The Administration>Certificate Management>Delete window appears.

2. Click **Yes**. The Administration>Certificate Management window appears.

3.  Click **Delete** from the Certificate Authority Actions column. The Administration>Certificate Management>Delete window appears.

4.  Click **Yes**. The Administration>Certificate Management window appears.

**Step 2**    Select **Click here to enroll with a Certificate Authority**. The Administration> Certificate Management>Enroll window appears.

**Step 3**    Select **Identity certificate**. The Administration>Certificate Management> Enroll>Identity Certificate window appears.

**Step 4**    Select **Enroll via PKCS10 Request (Manual)**. The Administration>Certificate Management >Enroll>Identity Certificate>PKCS10 window appears.

**Step 5**    Complete the following sub-steps to fill out the enrollment form:

1.  Enter a common name: **studentPX**.
    (where P = pod number, and X = your first and last initials)

2.  Enter an organizational unit: **training**.

The Concentrator uses this as the group password. This parameter must match end-to-end.

3.  Enter an organization: **Cisco Systems**.

4.  Enter a locality: **Austin**.

5.  Enter a state/province: **Texas**.

Do not abbreviate the state/province name.

6.  Enter a country: **US**.

7.  Leave subject alternative name fields blank.

8.  Select a key size: **RSA 512 bits**.

9.  Click **Enroll**. After a moment, a new Internet Explorer window opens containing the certificate request. Leave the Internet Explorer window open and proceed to the next task.

## Task 10—Send the PKCS#10 Certificate Request to the Certificate Server

The certificate request must be sent to the certificate server so an identity certificate can be generated. The transport method used in this lab exercise is to perform a copy and paste function. First, you will copy the certificate request generated by the Concentrator and then you will paste the certificate request directly into the certificate server via a web interface. Complete the following steps to send the PKCS#10 certificate request to the certificate server:

**Step 1**    Return to the Internet Explorer window containing the PKCS#10 and complete the following sub-steps:

1.  Select **Edit>Select all**. The contents of the PKCS#10 are highlighted.

2.  Select **Edit>Copy**. The contents of the PKCS#10 are copied to the student PC's paste buffer.

3.  Close the Internet Explorer window containing the PKCS#10.

**Step 2**  Return to the Cisco VPN 3000 Concentrator Series Manager window and complete the following sub-steps:

1.  Drill down to **File Management** from the Administration menu tree.

2.  Verify that a new PKCS000N.TXT file exists.
    (where N = any integer)

3.  Locate the PKCS000N.TXT row and click **View**. A new Internet Explorer window opens, displaying a copy of the PKCS#10.
    (where N = any integer)

4.  Close the new Internet Explorer window.

**Step 3**  Logout of the Concentrator. Do not close the Internet Explorer window.

**Step 4**  Enter a certificate server IP address, **172.26.26.51/certsrv,** in the Internet Explorer Address field. The Microsoft Certificate Services window opens.

---

| **Note** | You need to append /certsrv to the certificate server IP address (for example, 172.26.26.51/certsrv). |
|---|---|

---

**Step 5**  Select **Request a Certificate** from the menu and click **Next**.

**Step 6**  Select **Advanced Request** from the menu and click **Next**.

**Step 7**  Select **Submit a certificate request using base 64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS #7 file** from the Advanced Certificate Requests menu and click **Next**.

**Step 8**  Press **Ctrl>v** to paste the PKCS#10 contents into the Saved Request box.

**Step 9**  Click **Submit**. The certificate issued window opens. Remain logged in to the certificate server and proceed to the next task.

## Task 11—Download a New Identity Certificate to the Student PC

In the previous task, the certificate request was pasted into the certificate server and the certificate server issued the identity certificate. Complete the following steps to download the identity certificate to your student PC:

**Step 1**  Select **Base 64 encoded** from the Certificate Issued window.

**Step 2**  Click **Download CA Certificate**. The File Download window opens.

**Step 3**  Select **Save this file to disk** and click **OK**. The Save As window appears.

**Step 4**  Complete the following sub-steps from the Save As window:

1.  Click **Save in:** from the drop-down menu and search for the Certs folder. Select the **Certs** folder.

2.  Enter a file name in the File Name field: **ID cert X**.
    (where X = your first and last initials)

---

3. Click **Save**. The Download Complete window opens.

**Step 5**  Click **Close**.

**Step 6**  Click **Home** in the upper right portion of the window of the Microsoft Certificate Services window. The Welcome window opens. Leave the Welcome window open and proceed to the next task.

# Task 12—Generate a Root Certificate and Download it to the Student PC

In the prior task, the identity certificate was downloaded to the student PC. Complete the following steps to retrieve a root certificate and load it on the student PC:

**Step 1**  Select **Retrieve the CA certificate or certificate revocation list**.

**Step 2**  Click **Next**. The Retrieve the CA Certificate or Certificate Revocation List window opens.

**Step 3**  Highlight the current CA certificate. (If you are unsure of which CA certificate is the current CA certificate, ask the instructor for help.)

**Step 4**  Select **Base 64 encoded**.

**Step 5**  Click **Download CA Certificate**. The File Download window opens.

**Step 6**  Select **Save this file to disk** and click **OK**. The Save As window opens.

**Step 7**  From the Save As window, complete the following sub-steps:

1. Click **Save in:** drop-down menu and search for the certificates folder. Select the **Certs** folder.

2. Enter a file name in the File Name field: **root cert X**.
   (where X = your first and last initials)

3. Click **Save**. The Download Complete window opens.

**Step 8**  Click **Close**. The root certificate is installed on your student PC. Leave the Internet Explorer window open and proceed to the next task.

# Task 13—Load the Root Certificate Into the Concentrator

Complete the following steps to load the Root certificate into the Concentrator:

**Step 1**  Enter the Concentrator's public interface IP address in the Internet Explorer address field: **192.168.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 2**  Log in to the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

Login: **admin**

Password: **admin**

**Step 3**  Drill down to **Certificate Management** from the Administration menu tree**.** Select **Click here to install a CA certificate**. The Administration>Certificate Management>Install>CA Certificate window opens.

**Step 4**  Select **Upload File from Workstation**. The Administration>Certificate Management>Install>CA Certificate>Upload File from workstation window opens.

**Step 5** Click **Browse**. The Choose file window opens.

**Step 6** From the Choose file window, locate the root certificate in the student PC's Certs folder.

**Step 7** Highlight the root certificate file and click **Open**. The Administration>Certificate Management>Install>CA Certificate>Upload File from workstation window opens.

**Step 8** Click **Install**. The Administration>Certificate Management window opens.

**Step 9** Choose the Certificate Authorities section and complete the following sub-steps:

    1.   Under the Actions column, click **View** and answer the following questions:

        Q1)     Under Subject, what is the CN?

            A)    _____

        Q2)     Under Issuer, what is the CN?

            A)    _____

        Q3)     What signing algorithm was used?

            A)    _____

        Q4)     What was the public key type?

            A)    _____

        Q5)     What are the validity dates?

            A)    _____

    2.   Click **Back**. The Root certificate was successfully installed.

## Task 14—Load the Identity Certificate into the Concentrator

Complete the following steps to load the Identity certificate into the Concentrator:

**Step 1** From the Administration>Certificate Management window, select **Click here to install a certificate**. The Administration>Certificate Management>Install window appears.

**Step 2** Select **Install certificate obtained via enrollment**. The Administration>Certificate Management>Install certificate obtained via enrollment window opens.

**Step 3** Under the Actions column, select **Install**. The Administration>Certificate Management>Install>Identity Certificate window opens.

**Step 4** Select **Upload file from workstation**. The Administration>Certificate Management>Install>Identity Certificate>Upload from workstation window opens.

**Step 5** Click **Browse**. The Choose file window opens.

**Step 6** From the Choose file window, locate the identity certificate in the student PC's Certs folder.

**Step 7** Highlight the identity certificate file and click **Open**. The Administration>Certificate Management>Install>Certificate>Upload File from workstation window opens.

**Step 8** Click **Install**. The Administration>Certificate Management window opens. A new identity certificate is present under the Identity Certificate section.

**Step 9**  Choose the Identity Certificate section. Under the Actions column, click **View** and answer the following questions:

Q6)  Under Subject, what is the CN?

A)  _____

Q7)  Under Issuer, what is the CN?

A)  _____

Q8)  What signing algorithm was used?

A)  _____

Q9)  What was the public key type?

A)  _____

Q10)  What are the validity dates?

A)  _____

**Step 10**  Click **Back**. Remain logged into the Concentrator, leave the Internet Explorer window open, and proceed to the next task.

## Task 15—Activate the Concentrator IKE Proposal

By default, there are no digital certificate IKE proposals listed in the Concentrator under the IKE Active Proposals column. Complete the following steps to activate a digital certificate IKE proposal:

**Step 1**  From the Configuration menu tree, drill down to **System>Tunneling Protocols> IPSec>IKE Proposals**.

**Step 2**  Select the **CiscoVPNClient-3DES-MD5-RSA** proposal in the Inactive Proposals list.

**Step 3**  Click **Activate**.

**Step 4**  Select the **CiscoVPNClient-3DES-MD5-RSA** proposal in the Active Proposals list.

**Step 5**  Select **Modify** and complete the following sub-steps:

1. Verify the authentication mode is set to: RSA Digital Certificate (XAUTH).

2. Verify the authentication algorithm is set to: MD5/HMAC-128.

3. Verify the encryption algorithm is set to: 3DES-168.

4. Verify the Diffie-Hellman Group is set to: Group2 (1024-bits).

**Step 6**  Click **Apply**.

**Step 7**  Select the **CiscoVPNClient-3DES-MD5-RSA** proposal in the Active Proposals list. Under the Actions column, click **Move Up.** Click **Move up** until the CiscoVPNClient-3DES-MD5-RSA proposal is at the top of the Active Proposals list.

**Step 8**  Save your configuration changes.

## Task 16—Modify the Concentrator Security Associations

Security Associations (SAs) define the IKE and IPSec parameters that are negotiated when the IPSec remote access tunnel is established. Since we are migrating from a pre-shared key exchange to a digital certificate exchange, a digital certificate IKE template needs to be applied to the negotiation. Complete the following steps to add a digital certificate SA:

**Step 1**  From the Configuration menu tree, drill down to **Policy Management>Traffic Management> SAs**. The Configuration>Policy Management>Traffic Management>Security Associations window opens.

**Step 2**  Click **Add** under the Actions column. The Configuration>Policy Management>Traffic Management>Security Associations>Add window opens.

**Step 3**  Complete the following sub-steps:

1.  Enter in the SA Name field: **ESP-3DES-MD5-RSA**.

2.  In the IKE Parameters section of the window, select **studentPX** from the Digital Certificate drop-down menu.
    (where P = pod number, and X = your first and last initials)

3.  Choose **CiscoVPNClient-3DES-MD5-RSA** from the IKE proposal drop-down menu.

4.  Click **ADD**.

## Task 17—Configure the Concentrator IPSec Client-to-LAN Group Parameters

In the previous task, a pre-shared keys SA was configured for the training remote access group. In this task, the new digital certificate SA is assigned to the training remote access group. Complete the following steps to modify the group IPSec SA parameter:

**Step 1**  From the Configuration menu tree, drill down to **User Management>Groups**. The Configuration>User Management>Groups window opens.

**Step 2**  Select **training (Internally Configured)** and click **Modify Group**. The Configuration>User Management>Groups>Modify training window opens.

**Step 3**  Select the **IPSec** tab.

**Step 4**  Choose the IPSec SA from the drop-down menu: **ESP-3DES-MD5-RSA**.

**Step 5**  Click **Apply**.

**Step 6**  Save your configuration changes.

**Step 7**  Log out of the Concentrator.

**Step 8**  Close Internet Explorer.

## Task 18—Create a Certificate Request on the Cisco VPN Client

In previous tasks, you created and loaded an identity and root certificate on the Concentrator. In the next few steps, you will create and load an identity and root certificate on the Cisco VPN

Client. In this task, you will generate a certificate request. Complete the following steps to create a certificate request for the Cisco VPN Client:

**Step 1** Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco VPN Client window opens.

**Step 2** Select the **Certificates** tab.

**Step 3** Click **Enroll**. The Certificate Enrollment window opens.

**Step 4** Select an enrollment type of **File**.

**Step 5** Select a file type: **Base 64**.

**Step 6** Enter a file name in the Filename field: **requestPX**.
(where P = pod number, and X = your first and last initials)

**Step 7** Leave the Password field blank.

**Step 8** Click **Next**. The Certificate Enrollment window opens.

**Step 9** Complete the enrollment form using the following sub-steps:

1. Enter a Common Name: **studentPX**.
   (where P = pod number, and X = your first and last initials)

2. Enter a Department Name: **training**.

3. Enter a Company: **Cisco**.

4. Leave all other fields blank.

**Step 10** Click **Enroll**. The Creation of the Enrollment Request File was Successful window opens.

**Step 11** Click **OK**.

## Task 19—Copy the Request file to the Paste Buffer

Complete the following steps to make a copy of the request:

**Step 1** Open the C:\Program Files\Cisco Systems\VPN Client folder.

**Step 2** Double-click the **request PX** file and open it using Notepad. The file opens in a Notepad window.
(where P = pod number, and X = your first and last initials)

**Step 3** Choose **Edit>Select All**. The contents of the request file are highlighted.

**Step 4** Select **Edit>Copy**.

**Step 5** Close the Notepad window.

**Step 6** Close the C:\Program Files\Cisco Systems\VPN Client folder window.

## Task 20—Copy PKCS#10 to the Certificate Server

Complete the following steps to paste the PKCS#10 into the certificate server:

**Step 1** Launch Internet Explorer by double-clicking the desktop icon.

**Step 2** Enter a certificate server IP address (**172.26.26.51/certsrv**) in the Internet Explorer Address field. The Microsoft Certificate Services window opens.

| Note | When connecting to the certificate server, you need to append /certsrv to the certificate server IP address (for example, 172.26.26.51/certsrv). |
|------|---|

**Step 3**   Click **Request a Certificate** under Select a Task.

**Step 4**   Click **Next**.

**Step 5**   Select **Advanced Request** under Choose Request Type.

**Step 6**   Click **Next**.

**Step 7**   Click **Submit a certificate request using a base 64 encoded PKCS#10 file or a renewal request using a base64 PKCS#7 file** under Advanced Certificate Requests.

**Step 8**   Click **Next**. The Submit a Saved Request window opens.

**Step 9**   Use the **Ctrl>V** keys to paste the contents of the new certificate into the Saved Request box.

**Step 10**  Click **Submit**. The Certificate Issued window opens. Do not close the Certificate Server window. Proceed to the next task.

## Task 21—Download the Cisco VPN Client Identity Certificate

In the previous tasks, the Cisco VPN Client certificate request was pasted into the certificate server and the certificate server issued the Cisco VPN Client identity certificate. Complete the following steps to download the Cisco VPN Client identity certificate to the student PC:

**Step 1**   Select **Base 64 encoded** in the Certificate Issued window.

**Step 2**   Select **Download CA certificate**. The File Download window opens.

**Step 3**   Select **Save this file to disk**.

**Step 4**   Click **OK**. The Save As window opens.

**Step 5**   Select the save in folder: **Certs**.

**Step 6**   Enter a file name: **client ID cert X**.
(where X = your first and last initials)

**Step 7**   Click **Save**. The Download Complete window opens.

**Step 8**   Click **Close**. The Certificate Issued window opens.

**Step 9**   Click the certificate server located in the upper right portion of the window: **Home**. The Welcome window opens. Leave the Internet Explorer window open and proceed to the next task.

## Task 22—Retrieve the Cisco VPN Client Root Certificate

Complete the following steps to retrieve the root certificate from the Certificate Authority (CA) and load it on the student PC:

**Step 1**   Select **Retrieve the CA Certificate or certificate revocation list**.

**Step 2**   Click **Next**. The Choose file to download window opens.

**Step 3**   Highlight the current CA certificate. (If you are unsure of which CA certificate is the current CA certificate, ask the instructor for help.)

**Step 4**   Select **Base 64 encoded**.

**Step 5**   Click **Download CA Certificate**. The File Download window opens.

**Step 6**    Select **Save this file to disk**.

**Step 7**    Click **OK**. The Save As dialog box opens.

**Step 8**    Click **Browse** and search for the Certs folder. Select the save in folder: **Certs**.

**Step 9**    Enter a file name: **client root X**.
(where X = your first and last initials)

**Step 10**   Click **Save**. The Download Complete window opens.

**Step 11**   Click **Close**.

**Step 12**   Close Internet Explorer.

## Task 23—Import the Cisco VPN Client Root Certificate into the Certificate Store

In previous tasks, identity and root certificates were generated and then downloaded to the student PC. Complete the following steps to import the client root certificate into the certificate store on the student PC:

**Step 1**    If the Cisco VPN client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 2**    Select the **Certificates** tab.

**Step 3**    Click **Import** and complete the following sub-steps within the VPN Client>Import Certificate window:

    1.   Select the **Import from File** button.

    2.   Click **Browse**. The Open window opens.

    3.   Look in the **Certs** folder.

    4.   Select **client root X**.
       (where X = your first and last initials)

    5.   Click **Open**. The Import Certificate>Source window opens.

    6.   Click **Import**. The Certificate successfully imported window opens.

    7.   Click **OK**.

## Task 24—Import the Cisco VPN Client Identity Certificate into the Certificate Store

Complete the following steps to load the client identity certificate into the certificate store:

**Step 1**    Select the **Certificates** tab.

**Step 2**    Click **Import** and complete the following sub-steps within the VPN Client>Import Certificate window.

    1.   Select the **Import from File** button.

    2.   Click **Browse**. The Open window opens.

3.  Look in the **Certs** folder.

4.  Select **client ID cert X**.
    (where X = your first and last initials)

5.  Click **Open**. The Import Certificate>Source window opens.

6.  Click **Import**. The Certificate successfully imported window opens.

7.  Click **OK**.

## Task 25—Configure the Cisco VPN Client for Digital Certificates

In the last tasks, root and identity certificates were created for the client. In this task, enable the Cisco VPN Client to use digital certificates for IKE authentication. Complete the following steps to edit the authentication parameters of the studentP Cisco VPN Client.

| Note | This procedure assumes Windows 2000 is already running on the student PC. |
| --- | --- |

**Step 1**  If the Cisco VPN client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.

The **studentP** entry from the previous lab must be edited before establishing a new connection.

**Step 2**  Click the **Connection Entries** tab.

**Step 3**  Highlight **studentP** and select **Modify**. The Properties for StudentP window opens.
(where P = pod number)

**Step 4**  Select the **Authentication tab**.

**Step 5**  Select **Certificate Authentication** and complete the following sub-steps:

1.  Select **studentPX (Cisco)** from the Name drop-down menu.
    (where P = pod number, and X = your first and last initials)

2.  Click **Save**.

## Task 26—Launch the Cisco VPN Client

Complete the following steps to launch the Cisco VPN Client:

**Step 1**  If the Cisco VPN client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 2**  Click **Connect**. The VPN Certificate Authentication window opens. Do not enter a password.

**Step 3**  Click **OK**. The User Authentication window opens.

**Step 4**  Enter a username: **studentP**.
(where P = pod number)

**Step 5**  Enter a password: **studentP**.
(where P = pod number)

**Step 6**  Click **OK**. The Cisco VPN Client icon appears in the student PC system tray.

**Step 7** Launch Internet Explorer by double-clicking the desktop icon.

**Step 8** Enter the Concentrator private interface IP address in the Internet Explorer Address field: **10.0.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 9** Log in to the Cisco VPN Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

**Step 10** From the Monitoring menu tree, drill down to **Sessions**.

**Step 11** From the Remote Access Sessions section, select **studentP**. The Monitoring> Sessions>Detail window appears.
(where P = pod number)

**Step 12** Answer the following question by referring to the IKE Session section of the window:

Q11) What authentication mode was used for this tunnel?

A) _____

**Step 13** Log out of the Concentrator.

**Step 14** Double-click the Cisco VPN Client icon in the student PC's system tray and disconnect any existing Client-to-LAN sessions.

**Step 15** Close Internet Explorer.

# Task 27—Configure the Certificate Manager for Network-Based Certificates

In the previous topic, you used file-based certificate (manual) enrollment and installation of certificates. In this topic you will use the Cisco VPN Client Certificate Manager to create a network-based certificate, which is an automated process for enrolling, creating, installing, viewing and verifying certificates. Use this task to enroll and manage certificates via the network-based method. Complete the following steps to configure the Certificate Manager for network-based certificates:

**Step 1** If the Cisco VPN client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 2** Select the **Certificates** tab.

**Step 3** Click **Enroll**. The Certificate Enrollment window opens.

**Step 4** Select **Online**.

**Step 5** Complete the following sub-steps:

1. Select a Certificate Authority: **<New>**.

2. Enter the following URL: **http://172.26.26.51/certsrv/mscep/mscep.dll**

3. Enter a Domain: **cisco.com**.

4. Leave the Challenge Password blank.

**Step 6** Click **Next.** The Certificate Enrollment window opens.

**Step 7** Complete the following sub-steps from within the Enrollment>Form window:

1. Enter a Common Name: **scepPX**.
   (where P = pod number, and X = your first and last initials)

2. Enter a Department: **training**. Use lower-case text, text must exactly match the configuration of the Concentrator.

3. Enter a Company: **ABCD**. (Be careful of the spelling, you will enter this name later in the DN matching topic of the lab exercise.)Leave the remaining fields blank.

4. Click **Enroll**. The Certificate enrollment completed successfully dialog box opens.

**Step 8** View the enrollment status message and click **OK**.

**Step 9** Select the new **scepPX** certificate.
(where P = pod number, and X = your first and last initials)

**Step 10** Click **Verify**. A Certificate is valid message should appear.

**Step 11** Click **OK**.

# Task 28—Create a New Cisco VPN Client Connection Record

In the previous task you exported client certificates and loaded them on the Concentrator. Your current Cisco VPN Client connection reflects the certificate obtained via file enrollment method. You need to make a new connection entry based on the Simple Certificate Enrollment Protocol (SCEP) generated certificate. It is best if you make a new connection profile. Complete the following steps to create a new Cisco VPN Client connection record:

**Step 1** If the Cisco VPN client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.

**Step 2** Select the **Connection Entries** tab.

**Step 3** Click **New**. The Create New VPN Connection Entry wizard opens.

**Step 4** Enter the name for the new connection entry in the Connection Entry field: **scepP**.
(where P = pod number)

**Step 5** Enter a Concentrator public interface IP address in the Host field: **192.168.P.5**.
(where P = pod number)

**Step 6** Select **Certificate Authentication**.

**Step 7** Select the **scepPX** certificate from the Name drop-down menu.
(where P = pod number, and X = your first and last initials)

**Step 8** Click **Save**.

# Task 29—Launch the Cisco VPN Client

Verify the certificates and the Cisco VPN Client configuration by establishing a VPN tunnel to the Concentrator. Complete the following steps to launch the Cisco VPN Client:

**Step 1** If the Cisco VPN Client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 2** Ensure that the connection entry is **scepP**.
(where P = pod number)

**Step 3** Click **Connect**. The VPN Certificate Authentication window opens. Do not enter a password.

**Step 4** Click **OK**. The User Authentication window opens.

**Step 5** Enter a username: **studentP**.
(where P = pod number)

**Step 6** Enter a password: **studentP**.
(where P = pod number)

**Step 7** Click **OK**. The Cisco VPN Client icon should appear in the system tray.

**Step 8** Launch Internet Explorer using the desktop icon.

**Step 9** Enter a Concentrator private interface IP address in the Internet Explorer Address field: **10.0.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 10** Log in to the Cisco VPN 3000 Concentrator Series Manager:

Login: **admin**

Password: **admin**

**Step 11** From the Monitoring menu tree, drill down to **Sessions**.

**Step 12** From the Remote Access Sessions section, select **studentP**. The Monitoring>Sessions>Detail window appears.
(where P = pod number)

**Step 13** From the IKE Session section of the window, answer the following question:

Q12)   What authentication mode was used for this tunnel?

A)   _____

**Step 14** Logout of the Concentrator. Do not close Internet Explorer.

**Step 15** Disconnect the Client-to-LAN connection using the Cisco VPN Client icon.

## Task 30—Configure DN Matching Rules

Earlier you configured both file and SCEP-based client certificates. You entered the same department name for each certificate, training, but used a different organizational name for each, Cisco and ABCD. In this topic of the lab, you will configure group matching rules to accept certificates from training and Cisco. DN matching will reject non-matching certificates, training and ABCD. Complete the following steps to configure DN matching using the Cisco VPN 3000 Concentrator Series Manager.

**Step 1** Enter a Concentrator public interface IP address in the Internet Explorer Address field: **192.168.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 2** Log in to the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

Login: **admin**

Password: **admin**

The username (login) and password are always case sensitive.

**Step 3** From the Configuration menu tree, drill down to **Policy Management>Group Matching>Rules**.

**Step 4** Click **Add** under the Actions column.

**Step 5** From the Configuration menu tree, drill down to **Policy Management>Certificate Group Matching>Rules>Add window**, complete the following sub-steps:

1. Select **training** from the Group drop-down menu.

2. Choose **Organizational Unit (OU)** from the Distinguished Name drop-down menu.

3. Verify Operator field is **Equals (=)**.

4. Enter **training** in the Value field.

5. Click **Append**.

6. Choose **Organization (O)** from the Distinguished Name drop-down menu.

7. Enter **Cisco** in the Value field. (Value is not case sensitive.) To be accepted by the Concentrator, a client certificate's OU field must equal training and the O field must equal Cisco.

8. Click **Append**.

9. Click **Add**. The Configuration>Policy Management>Traffic Management>Certificate Group Matching>Rules window opens.

**Step 6** From the Configuration menu tree, drill down to **Policy Management>Group Matching>Policy**.

**Step 7** Select **Match Group from Rules**.

**Step 8** De-select **Obtain Group from OU**.

**Step 9** Click **Apply**.

**Step 10** Save the changes.

**Step 11** From the Monitoring menu tree, drill down to **Filterable Event Log**.

**Step 12** Clear the filterable log and leave Internet Explorer open.

## Task 31—Launch the Cisco VPN Client

In this task, you will attempt to establish a tunnel using a non-rule matching certificate. The connection will fail. Complete the following steps to launch the Cisco VPN Client:

**Step 1** If the Cisco VPN Client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 2** Ensure that the connection entry is **scepP**.
(where P = pod number)

**Step 3** Click **Connect**. The VPN Certificate Authentication window opens. Do not enter a password.

**Step 4** Click **OK**.

**Step 5** A remote peer is no longer responding message appears. Click **OK**.

**Step 6**    Return to Internet Explorer.

**Step 7**    If the Filterable Event Log window is not open, go to the Monitoring menu tree and drill down to **Filterable Event Log**.

**Step 8**    If no events appear, retrieve the log.

**Step 9**    From the filterable event log, find the message group match for cert peer 172.26.26.P failed using rule ou=training, o=cisco.
(where P = pod number)

**Step 10**    Find the filterable event log message, cert group from OU feature is disabled.

**Step 11**    Clear the filterable event log.

**Step 12**    Logout of the Concentrator and close Internet Explorer.

## Task 32—Launch the Cisco VPN Client

In this task, you will attempt to establish a tunnel using a rule-matching certificate. Complete the following steps to launch the Cisco VPN Client:

**Step 1**    If the Cisco VPN Client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 2**    Ensure that the connection entry is **studentPX**.
(where P = pod number)

**Step 3**    Click **Connect**. The VPN Certificate Authentication window opens. Do not enter a password.

**Step 4**    Click **OK**. The User Authentication window opens.

**Step 5**    Enter a username: **studentP**.
(where P = pod number)

**Step 6**    Enter a password: **studentP**.
(where P = pod number)

**Step 7**    Click **OK**. The Cisco VPN Client icon should appear.

**Step 8**    If Internet Explorer is not open, launch Internet Explorer using the desktop icon. Enter a Concentrator private interface IP address in the Internet Explorer Address field: **10.0.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 9**    Log in to the Cisco VPN 3000 Concentrator Series Manager:

```
Login: admin
Password: admin
```

**Step 10**    From the Monitoring menu tree, drill down to **Filterable Event Log**.

**Step 11**    If no events appear, retrieve the filterable log. From the filterable event log, find the message group match for cert peer 172.26.26.P succeeded using rule ou=training, o=cisco.
(where P = pod number)

**Step 12**    Find the filterable event log message: validation of certificate successful.

**Step 13**    From the Configuration menu tree, drill down to **Policy Management>Group Matching>Policy**.

**Step 14**    De-select **Match Group from Rules**.

**Step 15** Select **Obtain Group from OU**.

**Step 16** Click **Apply**.

**Step 17** Save the changes.

**Step 18** Do not logout. Do not close Internet Explorer.

# Task 33—Return the Cisco VPN Client and Concentrator to Pre-shared Keys

In the previous tasks, the Concentrators used digital certificates. In the next few lab exercises, you will use pre-shared keys. For a VPN session using pre-shared keys to authenticate, the Concentrator and Cisco VPN Client must be re-configured. Complete the following steps to modify the Cisco VPN Client and Concentrator settings:

**Step 1** From the Configuration menu tree, drill down to **User Management>Groups**. The Configuration>User Management>Groups window opens.

**Step 2** Choose **training** from the Current Groups list and click **Modify Group**. The Configuration>User Management>Groups>Modify training window opens.

**Step 3** Select the **IPSec** tab.

**Step 4** From the IPSec Security Association (SA) drop-down menu, choose the **ESP-3DES-MD5** proposal.

**Step 5** Click **Apply** then save the changes.

**Step 6** Log out of the Concentrator and close Internet Explorer.

**Step 7** Disconnect the Client-to-LAN connection using the Cisco VPN Client icon.

**Step 8** If the Cisco VPN Client is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.

**Step 9** Choose **studentP** from Connection Entry drop-down menu.
(where P = pod number)

**Step 10** Click **Modify**. The Properties for studentP window opens.
(where P = pod number)

**Step 11** Select the **Authentication tab**.

**Step 12** Select **Group Authentication** radio button and complete the following sub-steps:

Verify the following entries:

1. Group name: **training**.

2. Group password: **training**.

3. Password: **training**.

**Step 13** Click **Save**.

**Step 14** Close the VPN Client window.

**7**

# Configure the Cisco Virtual Private Network Firewall Feature for the IPSec Software Client

## Overview

This lesson includes the following topics:

- Objectives

- Overview of the Software Client's firewall feature

- The Software Client's AYT feature

- The Software Client's Stateful Firewall feature

- The Software Client's CPP feature

- Software Client firewall statistics

- Customizing firewall policy

- Summary

■ Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Configure the AYT feature.**
- **Configure the Stateful Firewall feature.**
- **Configure the CPP feature.**
- **Monitor the firewall feature on the Cisco VPN Client.**

CSVPN 4.0—7-2

# Overview of the Software Client's Firewall Feature

This topic presents an overview of the Cisco Virtual Private Network (VPN) Software Client's firewall feature.
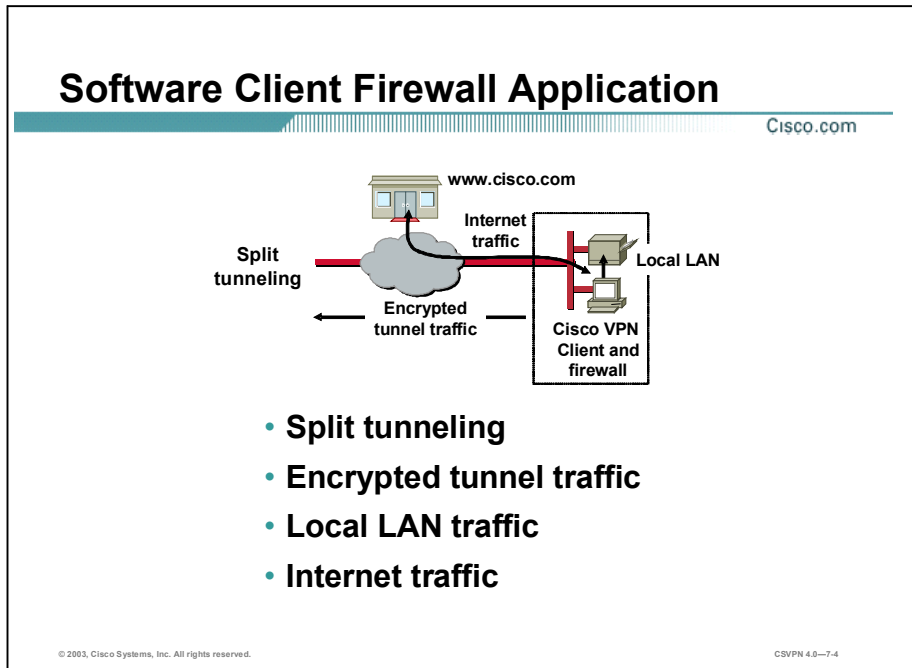


The Software Client is designed for split tunneling, Internet traffic, and applications. In split tunneling, there are three types of traffic:

■ Encrypted tunnel—All traffic bound for the corporate office is encrypted and sent down a tunnel, which is relatively safe.

■ Local LAN—Local LAN traffic is typically between a remote user's PC and a printer under their desk, which is also relatively safe.

■ Internet traffic—Internet traffic is between the remote user and sites on the Internet. By enabling split tunneling, the ability to raise a tunnel and talk to the Internet in clear text raises security issues. The Software Client firewall feature is designed to address the Internet traffic security issue.

**Windows-Based Software Client—Firewall Features**

Cisco.com

- Are you there (AYT)
- Stateful Firewall
- Central Policy Protection (CPP)
- Cisco Integrated Client (CIC) firewall

CSVPN 4.0—7-5

The Cisco VPN 3000 Series Concentrator contains four firewall features designed to enhance system security for Microsoft Windows-based PCs running the VPN Software Client:

■ Are You There (AYT) feature—This feature verifies that a specific firewall product is operational on a client PC before any tunnels are allowed.

■ Stateful Firewall feature—Pre-defined stateful firewall that is turned on or off at the remote Software Client. If enabled, it is active for both tunneled and non-tunneled traffic.

■ Central Policy Protection (CPP) feature—CPP provides network administrators with the ability to centrally define firewall policies for connected VPN Clients. This policy is pushed down to the Software Client at connection time.

■ Cisco Integrated Client (CIC) Firewall feature—As of the Cisco VPN 3000 Series Concentrator release 3.5, the Microsoft Windows-based Software Client now contains a CIC Firewall module. The CIC Firewall feature supports the Stateful Firewall feature and the CPP feature.

# The Software Client's AYT Feature

This topic presents an overview of the Software Client's Are You There (AYT) feature.
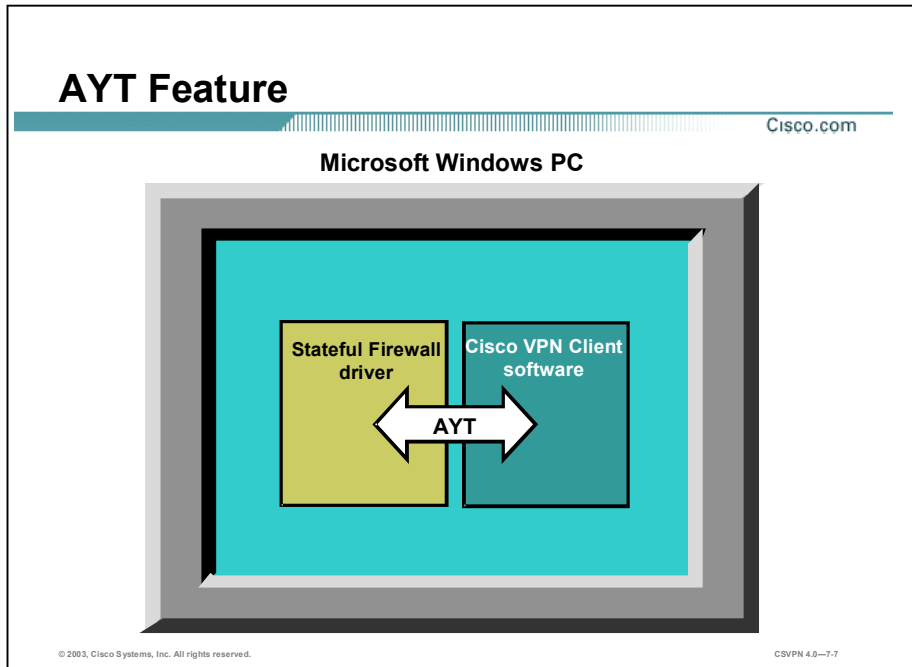


Often network administrators require remote access PCs to run a firewall application before allowing VPN tunnels to be built. The network administrator can configure the Concentrator to require all Software Clients in a group to have a specific firewall operating on the PC.

The Software Client monitors the firewall to ensure that it is running. If the firewall stops running, the Software Client drops the connection to the Concentrator. This firewall policy is also called AYT because the Software Client polls the firewall periodically to determine if it is still there. If there is no reply from the firewall, the Software Client knows that the firewall is down and terminates its connection to the Concentrator.

## Configuring the AYT Feature
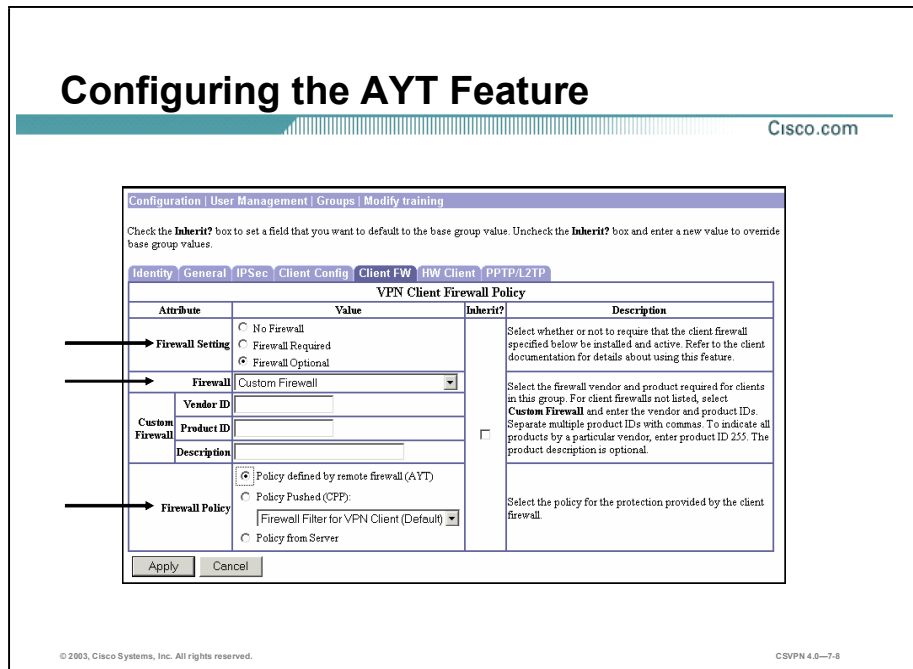
Go to the Configuration>User Management>Groups>Modify window and select the **Client FW** tab. AYT, CIC, and CPP features are configurable from this window. Over the next topics, you will configure each feature individually.

AYT is the first feature you will configure. Complete the following steps to configure the AYT feature:

**Step 1**   Select a firewall setting from the Firewall Setting row.

**Step 2**   Identify a firewall from the Firewall row.

**Step 3**   Configure a custom firewall from the Custom Firewall row.

**Step 4**   Select the Firewall policy from the Firewall Policy row.

The following figures further discuss the four steps used to configure the AYT feature.

# Step 1—Select a Firewall Setting



When configuring the AYT feature, you must first select a firewall setting. By default, no firewall is required for remote users in this group, so the No Firewall radio button is already selected. If you, as the administrator, want users in this group to be firewall-protected, select either **Firewall Required** or **Firewall Optional**:

■ No Firewall setting—This is the default. If you leave this radio button selected, then no firewall is required for remote users in this group.

■ Firewall Required setting—If you select this radio button, then all remote users in this group must use a firewall. Only those users with the designated firewall can connect to the Concentrator. The Concentrator drops any session that attempts to connect without the designated firewall installed and running. If you require a firewall for a group, make sure that the group does not include any Software Clients without the designated firewall or that the group does not include any non-Windows Software Clients, because they will be unable to connect.

■ Firewall Optional setting—If you select this radio button, then all remote users in this group can connect to the Concentrator. Those who have the designated firewall must use it. Those without the required firewall can still connect but will receive a notification message. This setting is useful if you have a group that is in gradual transition, in which some members have set up firewall capacity and others have not.

## Step 2—Identify a Firewall



After establishing the firewall setting, the second step is to identify a firewall. To do this, choose a firewall from the firewall drop-down menu:

■ Cisco Integrated Client Firewall—The firewall built into the Software Client

■ Network ICE BlackICE Defender—The Network ICE BlackICE Agent or Defender Firewall

■ Zone Labs ZoneAlarm—The Zone Labs ZoneAlarm firewall

■ Zone Labs ZoneAlarm Pro—The Zone Labs ZoneAlarm Pro firewall

■ Zone Labs ZoneAlarm or ZoneAlarm Pro—Either the Zone Labs ZoneAlarm firewall or the Zone Labs ZoneAlarm Pro firewall

■ Zone Labs Integrity—The Zone Labs Integrity Client

■ Sygate Personal Firewall—The Sygate Personal Firewall

■ Sygate Personal Firewall Pro—The Sygate Personal Firewall Pro

■ Sygate Security Agent—The Sygate Security Agent personal firewall

■ Cisco Intrusion Prevention Security Agent—Cisco Systems security agent

■ Custom Firewall—For future use (there is further discussion of this option later in this lesson)

**Step 3—Configure a Custom Firewall**

An optional step when configuring the AYT feature is to configure a custom firewall. Currently, every supported firewall is selectable from the Firewall drop-down menu. In the future this may not be true. For example, an additional firewall is supported in a future Concentrator software release, firewall brand XYZ for instance. The customer would like to support the new XYZ firewall, but they are not ready to migrate the to the new Concentrator software release. The new firewall can be supported on the older version of Concentrator software by configuring the custom firewall field. To support the new XYZ firewall, the administrator must configure the new vendor code and product code in the Vendor ID and Product ID fields. An optional description of the new firewall can also be added in the Description field.

Each vendor has a unique vendor identity and firewall product identity.

The following table lists the currently supported firewall vendors and their firewall products:

| Vendor | Vendor Code | Products | Product Code |
|---|---|---|---|
| Cisco Systems | 1 | CIC | 1 |
| | 5 | Cisco Intrusion Prevention Security Agent | 1 |
| Zone Labs | 2 | ZoneAlarm | 1 |
| | | ZoneAlarm Pro | 2 |
| | | Zone Labs Integrity | 3 |
| Network Ice | 3 | BlackIce Defender/Agent | 1 |
| Sygate | 4 | Personal Firewall | 1 |
| | | Personal Firewall Pro | 2 |
| | | Security Agent | 3 |

In the example in the figure, the administrator defines a custom firewall with a vendor identification of 2, Zone Labs, and a product identity of 2, ZoneAlarm Pro. Future vendor and product identifications will be available in the Cisco VPN 3000 product release notes.

# Step 4—Select the Firewall Policy

The last step when configuring the AYT feature is to select the firewall policy. There are three policies available. For the AYT feature, select the **Policy defined by remote firewall (AYT)** radio button. The AYT policy choice is sent to the Software Client in ModeCFG messages at connection time.

CSVPN 4.0—7-13
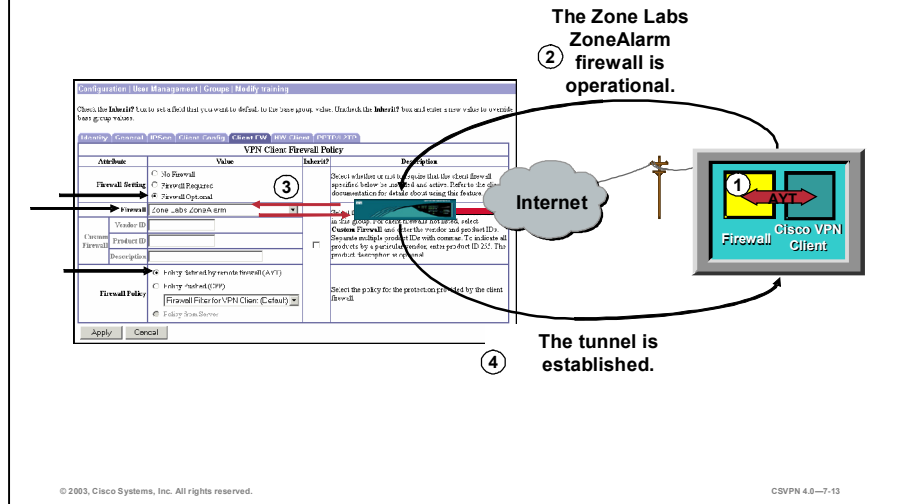
The administrator configures the Concentrator to require a particular firewall to be present on the remote Software Client's PC. At the Software Client connection time, the following steps occur:

**Step 1**  The Software Client polls the firewall.

**Step 2**  The Software Client reports the presence of a specific firewall to the Concentrator via ModeCFG messages.

**Step 3**  The Concentrator checks the reported firewall information against the VPN Client's group firewall settings.

**Step 4**  Depending on how the firewall parameters are set, the Concentrator's actions are as follows:

■  No Firewall setting—No firewall is required, so the tunnel establishment is continued.

■  Firewall Required setting—If the designated firewall is installed and running, the connection is allowed. When the connection is established, the Software Client polls the firewall every thirty seconds to ensure that it is still running. If the firewall stops running, the Software Client terminates the session.

■  Firewall Optional setting—Those VPN Clients that have the designated firewall may connect if the firewall is running. Those VPN Clients without the designated firewall may still connect but will receive a notification message. Notification messages are discussed later in the lesson.

# Firewall Optional—Warning

| Identity | General | IPSec | Client Config | Client FW | HW Clie |
|---|---|---|---|---|---|

**VPN Client Fire**

| Attribute | Value |
|---|---|
| Firewall Setting | ○ No Firewall<br>○ Firewall Required<br>◉ Firewall Optional ◄ |
| Firewall | Network ICE BlackICE Defender |

**VPN Client | Notifications**

Notifications:

| Title |
|---|
| [ 1 - Jun 6, 2003 13:55:44]  Connect History |
| [ 2 - Jun 6, 2003 13:55:42]  Client Error Notification |

Message:

The client did not match the firewall policy configured on the central site VPN device.  NetworkICE BlackICE Defender should be enabled or installed on your computer.

Launch        Close

CSVPN 4.0—7-14

When the Firewall Optional radio button is selected, Software Clients that are not running with a designated firewall are allowed to connect but will receive a Software Client notification message. The message informs the Software Client that the Software Client did not match any of the Concentrator's firewall configurations. The message also defines the expected firewall.

The particular notification text shown in the figure warns the remote user that the Software Client does not match the Concentrator's configuration. The Concentrator expects the Network ICE, BlackICE Defender firewall application to be running on the PC. If the remote user is not running BlackICE Defender and they receive a notification message, the tunnel is still established.

# The Software Client's Stateful Firewall Feature

This topic presents an overview of the Software Client's Stateful Firewall feature.

## Stateful Firewall Feature

**Microsoft Windows PC**

Stateful Firewall
(Always On)
enabled

Tunneled
traffic

Nontunneled
traffic

CSVPN 4.0—7-16
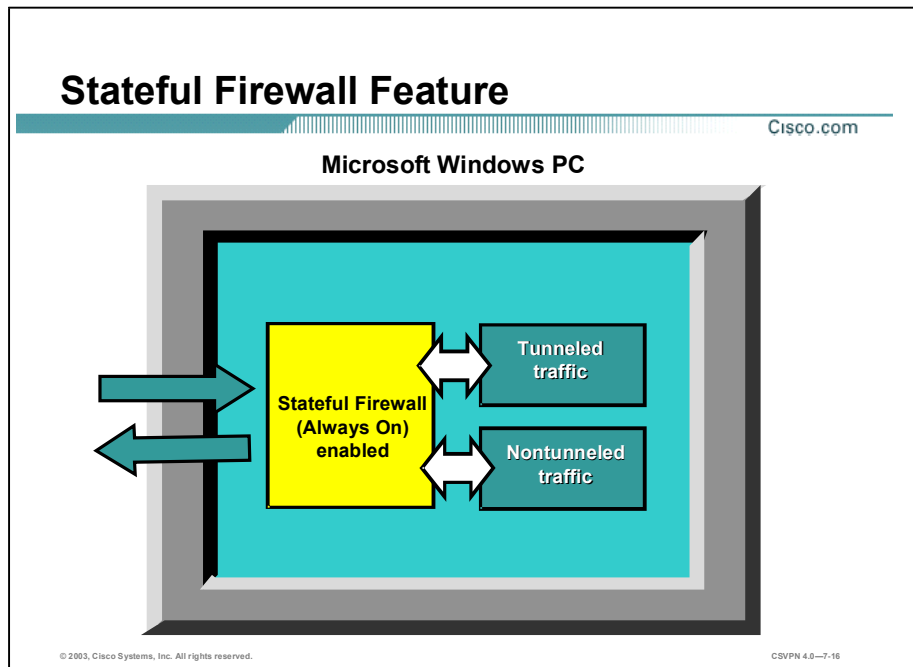
The Software Client 3.5 and higher releases contain an integrated stateful firewall module licensed from Zone Labs called the CIC firewall. Components of this feature include a dynamic link library (DLL) combined with a Zone Labs stateful firewall module driver. The DLL acts as an interface between the traditional Software Client and the firewall driver.

A default stateful firewall policy is loaded on CIC firewall. The stateful, CIC, firewall blocks all inbound traffic that is not related to an outbound session. The two exceptions to this rule are Dynamic Host Configuration Protocol (DHCP) and Acknowledge Response Protocol (ARP) traffic, where inbound packets are allowed through specific holes in the stateful firewall. When the user enables the stateful firewall, it is always on. The firewall is active for both tunneled and non-tunneled traffic.

The administrator can accept the default policy or they can customize the firewall policy. To alter the firewall policies, the administrator can use the CPP feature. CPP enables the Concentrator's administrator to centrally define a set of rules for the CIC firewall. This policy is pushed to the CIC firewall module. There is further discussion of CPP later in the lesson.

Enabling the Stateful Firewall Feature
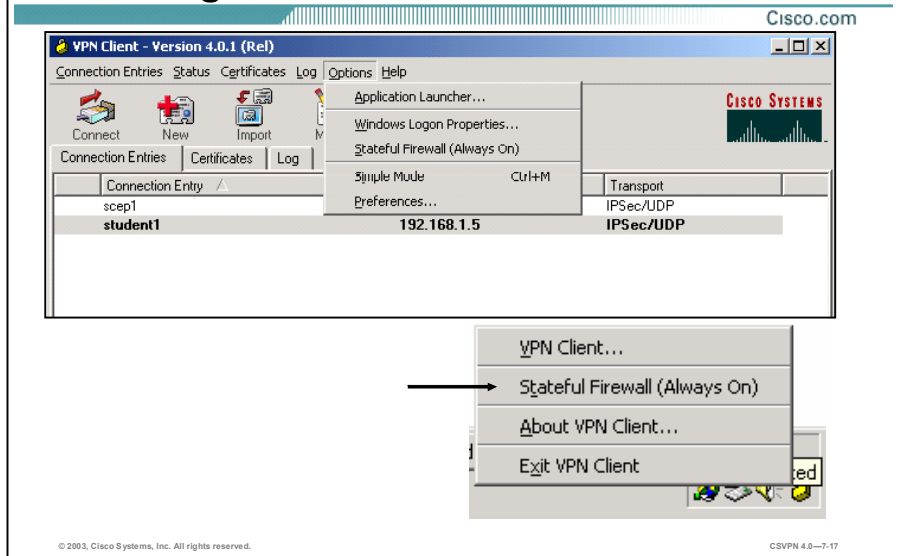
The remote client controls the stateful firewall feature. By default, the Stateful Firewall feature is disabled, or unchecked, on the Software Client. There are two ways to enable the Stateful Firewall feature. From the main Software Client window, remote users can click the **Options** button and choose **Stateful Firewall**. They can also access the Stateful Firewall option by right-clicking the lock icon from the system tray. When enabled, the Stateful Firewall feature filters both tunneled and non-tunneled traffic.

# The Software Client's CPP Feature

This topic presents an overview of the Software Client's Central Policy Protection (CPP) feature.
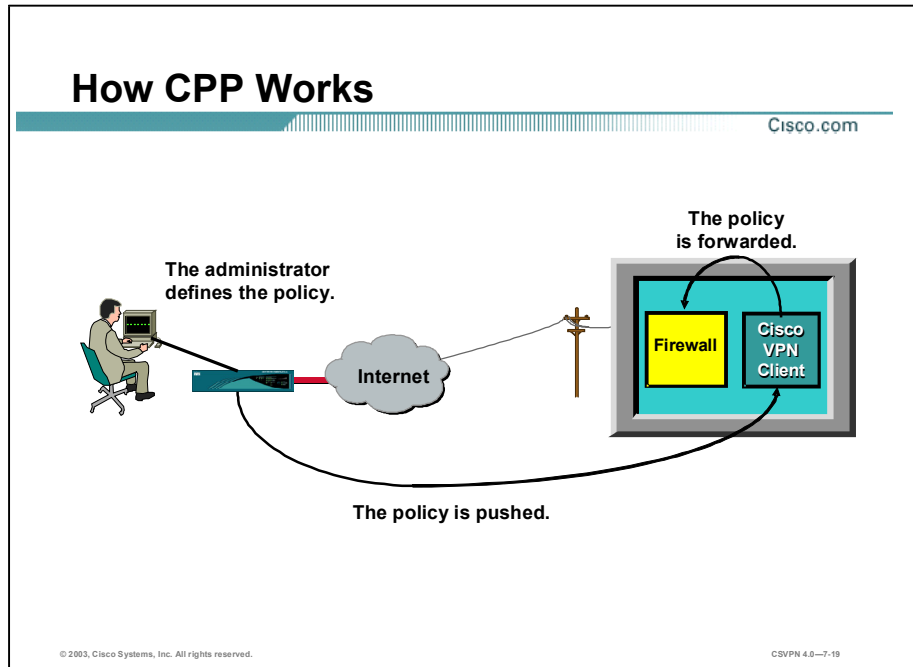


Some administrators prefer to enforce a more centralized firewall policy approach. They do this by first defining a policy—a set of rules to allow or drop traffic—on the Concentrator. When the connection is made, these policies are pushed from the Concentrator to the Software Client using ModeCFG messages. The Software Client, in turn, forwards the policy to the local firewall, which enforces it.

## CPP Supported Firewalls

| Firewall | CPP |
|----------|-----|
| Cisco Integrated Client | X |
| Zone Labs ZoneAlarm | X |
| Zone Labs ZoneAlarm Pro | X |

CSVPN 4.0—7-20

The Software Client can forward policy to the following firewalls:

■ CIC—Concentrator and Software Client release 3.5 and higher.

■ ZoneLabs—Minimum version of 2.6.357.

**Configure CPP**

Cisco.com

Configuration | User Management | Groups | Modify training

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

| Identity | General | IPSec | Client Config | **Client FW** | HW Client | PPTP/L2TP |

**VPN Client Firewall Policy**

| Attribute | Value | Inherit? | Description |
|---|---|---|---|
| **Firewall Setting** | ○ No Firewall<br>● Firewall Required<br>○ Firewall Optional | | Select whether or not to require that the client firewall specified below be installed and active. Refer to the client documentation for details about using this feature. |
| Firewall | Zone Labs ZoneAlarm Pro ▾ | | Select the firewall vendor and product required for clients in this group. For client firewalls not listed, select **Custom Firewall** and enter the vendor and product IDs. Separate multiple product IDs with commas. To indicate all products by a particular vendor, enter product ID 255. The product description is optional. |
| Custom Firewall — Vendor ID | | ☐ | |
| Product ID | | | |
| Description | | | |
| **Firewall Policy** | ○ Policy defined by remote firewall (AYT)<br>● Policy Pushed (CPP):<br>Firewall Filter for VPN Client (Default) ▾<br>○ Policy from Server | | Select the policy for the protection provided by the client firewall. |

| Apply | Cancel |

© 2003, Cisco Systems, Inc. All rights reserved.                                     CSVPN 4.0—7-21

Configuring CPP is a two-step process:

**Step 1**  The administrator selects a firewall—From the Firewall drop-down menu, choose a CPP-supported firewall: either CIC or a Zone Labs firewall.

**Step 2**  The administrator selects a policy—From the Firewall Policy row, select **Policy Pushed (CPP)**. From the Policy Pushed (CPP) drop-down menu, choose a filter to push to the firewall. The default policy is Firewall Filter for VPN Client (Default).

In the example in the figure, the administrator has selected the ZoneAlarm Pro as the required firewall, with the default CPP policy of Firewall Filter for VPN Client (Default). The default policy forwards all inbound and outbound encrypted tunnel traffic. It blocks all Internet inbound traffic that is not related to an outbound session. There is a discussion of firewall policy later in this lesson.

# Software Client Firewall Statistics

This topic discusses the Software Client firewall statistics.
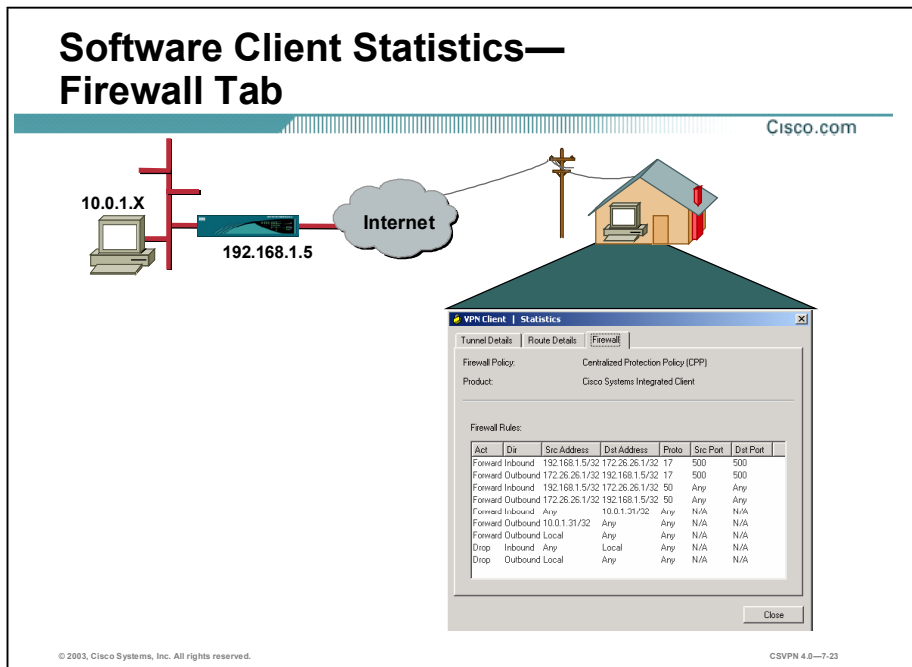
The Firewall tab displays information about the VPN Client's firewall configuration, including the firewall policy and the configured firewall product. The remaining contents of the Firewall tab depend on these two configured options. The information shown on this tab varies according to your firewall policy as follows:

■ AYT—When the AYT is the supported capability, the Firewall tab shows only the firewall policy and the name of the firewall product. AYT enforces the use of a specific personal firewall but does not require you to have a specific firewall policy.

■ Centralized Protection Policy (CPP)—When CPP is the supported capability, the Firewall tab includes the firewall policy, the firewall in use, and firewall rules.

■ Client/Server—When the Client/Server is the supported capability, the Firewall tab displays the firewall policy as Client/Server, the name of the product as ZoneLabs Integrity Agent, the user ID, session ID, and the addresses and port numbers of the firewall servers.

## Software Client Firewall Rules

Cisco.com

**VPN Client | Statistics**

Tunnel Details | Route Details | Firewall

Firewall Policy:   Centralized Protection Policy (CPP)

Product:   Cisco Systems Integrated Client

Firewall Rules:

| Act | Dir | Src Address | Dst Address | Proto | Src Port | Dst Port |
|-----|-----|-------------|-------------|-------|----------|----------|
| Forward | Inbound | 192.168.1.5/32 | 172.26.26.1/32 | 17 | 500 | 500 |
| Forward | Outbound | 172.26.26.1/32 | 192.168.1.5/32 | 17 | 500 | 500 |
| Forward | Inbound | 192.168.1.5/32 | 172.26.26.1/32 | 50 | Any | Any |
| Forward | Outbound | 172.26.26.1/32 | 192.168.1.5/32 | 50 | Any | Any |
| Forward | Inbound | Any | 10.0.1.31/32 | Any | N/A | N/A |
| Forward | Outbound | 10.0.1.31/32 | Any | Any | N/A | N/A |
| Forward | Outbound | Local | Any | Any | N/A | N/A |
| Drop | Inbound | Any | Local | Any | N/A | N/A |
| Drop | Outbound | Local | Any | Any | N/A | N/A |

Close

CSVPN 4.0—7-24

The Firewall Rules section shows all of the firewall rules currently in effect on the VPN Client. Rules are in order of importance from highest to lowest level. The rules at the top of the table allow inbound and outbound traffic between the VPN Client and the secure gateway and between the VPN Client and the private networks with which it communicates. For example, there are two rules in effect for each private network that the VPN Client connects to through a tunnel (one rule that allows traffic outbound and another that allows traffic inbound). These rules are part of the VPN Client software. Since they are at the top of the table, the VPN Client enforces them before examining CPP rules. This approach lets the traffic flow to and from private networks.

CPP rules (defined on the VPN Concentrator) are only for nontunneled traffic and appear next in the table. A default rule "Firewall Filter for VPN Client (Default)" on the VPN Concentrator lets the VPN Client send any data out, but permits return traffic in response only to outbound traffic.

Finally, there are two rules listed at the bottom of the table. These rules, defined on the VPN Concentrator, specify the filter's default action, either drop or forward. If not changed, the default action is drop. These rules are used only if the traffic does not match any of the preceding rules in the table. Each firewall rule includes the following fields:

■ Action—The action taken if the data traffic matches the rule:

— Drop—Discard the session.

— Forward—Allow the session to go through.

■ Direction—The direction of traffic to be affected by the firewall:

- Inbound—Traffic coming into the PC, also called local machine, from the public network while the Software Client is connected to a secure gateway through the secure tunnel.

- Outbound—Traffic going out from the PC to all networks while the Software Client is connected to a secure gateway.

■ Source Address—The address of the traffic that this rule affects:

- Any—All traffic (for example, drop any inbound traffic). This field can also contain a specific IP address and subnet mask.

- Local—The local machine. If the direction is outbound, then the source address is local.

■ Destination Address—The packet's destination address that this rule checks (the address of the recipient):

- Any—All traffic (for example, forward any outbound traffic).

- Local—The local machine. If the direction is inbound, the destination address is local.

■ Protocol—The Internet Assigned Number Authority (IANA) number of the protocol that this rule concerns (6 for TCP; 17 for UDP, and so on):

- Source Port—Source port used by TCP or UDP.

- Destination Port—Destination port used by TCP or UDP.

# Customizing Firewall Policy

This topic explains how to create a custom firewall policy.
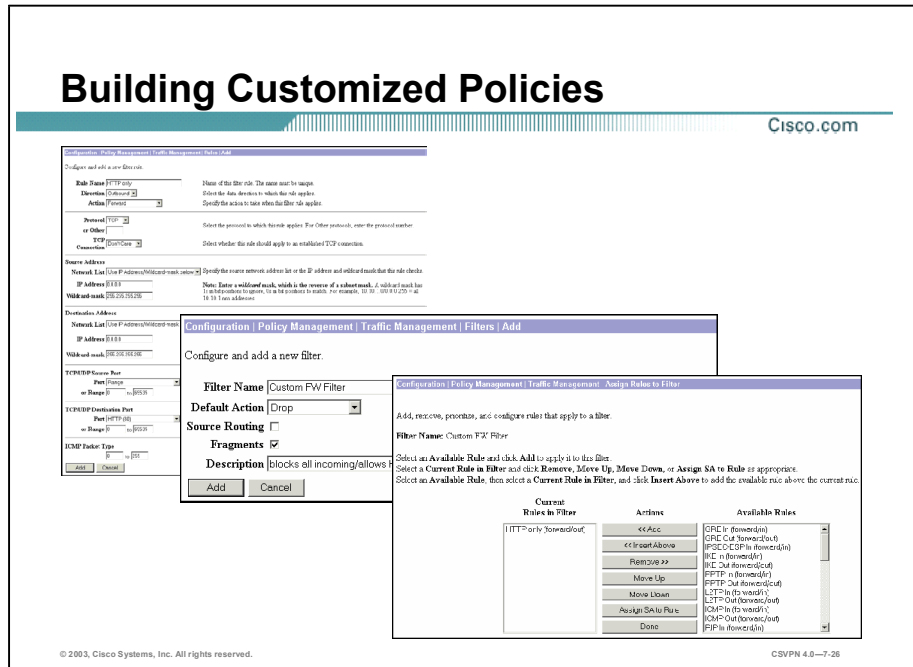


Most of the time the default policy works fine. However, if the administrator needs to restrict the outbound clear text traffic to a few protocols or a handful of remote locations, the administrator should create a new policy. Building custom CPP policies is a four-step process. On the Concentrator complete the following steps:

**Step 1**  Define rules to restrict traffic.

**Step 2**  Add a new policy.

**Step 3**  Associate the new rules with the newly created policy.

**Step 4**  Assign the new policy to the CPP.

There is further discussion of each of these steps later in the lesson.

## Step 1—Define Rules to Restrict Traffic

A firewall policy is comprised of rules. These rules are used to shape the traffic. The rules define whether the firewall should forward or drop the traffic. In creating a new policy, the administrator first has to create new rules. To create the new rules, complete the following steps:

**Step 1** Go to the Configuration>Policy Management>Traffic Management>Rules window.

**Step 2** From the Actions column, click **Add**.

**Step 3** From the Configuration>Policy Management>Traffic Management>Rules>Add window, define the new rule.

The following is a description of the rule parameters:

■ Rule Name field—Enter the name of the filter rule.

■ Direction drop-down menu—Choose the data direction to which this rule applies:

— Inbound—Into the Software Client.

— Outbound—Out of the Software Client.

■ Action drop-down menu—Choose the action to take if the data traffic (packet) matches all parameters that follow:

— Drop—Discard the packet. This is the default choice.

— Forward—Allow the packet to pass.

- Protocol drop-down menu—This parameter refers to the IANA (Internet Assigned Numbers Authority) assigned protocol number in an IP packet. The descriptions include the IANA number, in brackets, for reference. Click the **Protocol or Other** drop-down menu button and choose the protocol to which this rule applies.

  - Any—Any protocol [255] (the default choice).

  - ICMP—Internet Control Message Protocol [1] (used by ping). If you choose this protocol, you should also configure ICMP Packet Type.

  - TCP—Transmission Control Protocol [6] (connection-oriented, for example: FTP, HTTP, SMTP, and Telnet). If you choose this protocol, you should configure TCP Connection and TCP/UDP Source Port or Destination Port.

  - EGP—Exterior Gateway Protocol [8] (used for routing to exterior networks).

  - IGP—Interior Gateway Protocol [9] (used for routing within a domain).

  - UDP—User Datagram Protocol [17] (connectionless, for example: SNMP). If you choose this protocol, you should also configure TCP/UDP Source Port or Destination Port.

  - ESP—Encapsulation Security Payload [50] (applies to IPSec).

  - AH—Authentication Header [51] (applies to IPSec).

  - GRE—Generic Routing Encapsulation [47] (used by PPTP).

  - RSVP—Resource Reservation Protocol [46] (reserves bandwidth on routers).

  - IGMP—Internet Group Management Protocol [2] (used in multicasting).

  - OSPF—Open Shortest Path First [89] (interior routing protocol).

  - Other—Other protocol not listed here. If you choose **Other** here, you must enter the IANA-assigned protocol number in the Other field.

- TCP Connection drop-down menu—Do not configure this field if you are using this rule for a client firewall filter.

- Source Address—Specify the packet source address that this rule checks.

  - Network List drop-down menu—Click the **Network List** drop-down menu button and choose the configured network list that specifies the source addresses. A network list is a list of network addresses that are treated as a single object.

— IP Address field—Enter the source IP address in dotted decimal notation. The default is 0.0.0.0.

— Wildcard-mask field—Enter the source address wildcard mask in dotted decimal notation. The default is 255.255.255.255.

■ Destination Address—Specify the packet destination address that this rule checks:

— Network List drop-down menu—Click the **Network List** drop-down menu button and choose the configured network list that specifies the destination addresses. A network list is a list of network addresses that are treated as a single object.

— IP Address field—Enter the destination IP address in dotted decimal notation. The default is 0.0.0.0.

— Wildcard-mask field—Enter the destination address wildcard mask in dotted decimal notation. The default is 255.255.255.255.

■ TCP/UDP Source Port—If you chose TCP or UDP from the Protocol drop-down menu, choose the source port number that this rule checks. To do this, click the Port drop-down menu button and choose the process.

■ TCP/UDP Destination Port—If you chose TCP or UDP from the Protocol drop-down menu, choose the destination port number that this rule checks. To do this, click Port drop-down menu button and choose the process.

An example of a rule configuration is shown in the figure. The administrator wants to limit the remote user to using outbound HTTP traffic only when accessing the Internet. To accomplish this, the administrator configures the rule parameters as follows:

■ Rule Name—HTTP Only

■ Direction—Outbound

■ Action—Forward

■ Protocol—TCP

■ Source and destination address—Ignored. The administrator is limiting the end-user to a protocol, HTTP, not a specific address. The end user can surf the web if they are using only HTTP.

— TCP/UDP Source Port—Ignored.

— TCP/UDP Destination Port—Port 80, HTTP. The administrator is limiting the remote user to using HTTP.

Note of caution, this configuration does not allow the user to use hostnames. The firewall will not pass Domain Name System (DNS) information. Another rule allowing DNS is advisable.

Step 2—Add a New Policy

Cisco.com

Configuration | Policy Management | Traffic Management | Filters

This section lets you add, configure, modify, copy, and delete filters, and assign rules to filters.

Click **Add Filter** to add a filter, or select a filter and click **Modify, Copy, Delete,** or **Assign Rules to Filter**.

Filter List | Actions

Private (Default)
Public (Default)
External (Default)
Firewall Filter for VPN Client (Default)

Add Filter
Assign Rules to Filter
Modify Filter
Copy Filter
Delete Filter

Configuration | Policy Management | Traffic Management | Filters | Add

Configure and add a new filter.

Filter Name | Custom FW Filter | Name of the filter you are adding. The name must be unique.
Default Action | Drop | Select the default action to take when no rules on this filter apply.
Source Routing | □ | Check to have this filter allow IP source routed packets to pass.
Fragments | ☑ | Check to have this filter allow fragmented IP packets to pass.
Description | blocks all incoming/allows HTTP outbound

Add    Cancel

© 2003, Cisco Systems, Inc. All rights reserved.                     CSVPN 4.0—7-28

After the rules are defined, a new filter is added. Complete the following steps to create the new filter:

**Step 1**  Go to Configuration>Policy Management>Traffic Management>Filters window.

**Step 2**  Under the Actions column, click **Add**.

**Step 3**  In the Configuration>Policy Management>Traffic Management>Filter>Add window, create the new filter.

The following is a description of the new filter parameters:

■   Filter Name field—Enter a unique name for this filter. Maximum is 48 characters.

■   Default Action drop-down menu—Click the **Default Action** drop-down menu button and choose the action that this filter takes if a data packet does not match any of the rules on this filter. The choices are:

—   Drop = Discard the packet (the default choice).

—   Forward = Allow the packet to pass.

—   Drop and Log = Discard the packet and log a filter debugging event (FILTERDBG event class). See the following note.

—   Forward and Log = Allow the packet to pass and log a filter debugging event (FILTERDBG event class). See the following note.

| Note | The Log actions are intended for use only while debugging filter activity. Since they generate and log an event for every matched packet, they consume significant system resources and might seriously degrade performance. |
|------|---|

- Source Routing check box—Ignored. Check the **Source Routing** check box to allow IP source routed packets to pass. A source-routed packet specifies its own route through the network and does not rely on the system to control forwarding. This box is unchecked by default.

- Fragments check box—Ignored. Check the **Fragments** check box to allow fragmented IP packets to pass. Large data packets might be fragmented on their journey through networks, and the destination system reassembles them. This box is checked by default.

- Description field—Enter a description of this filter. This field is optional. It is a convenience for you or other administrators; use it to describe the purpose or use of the filter. The maximum number of characters is 255.

In the example in the figure, the administrator defines a new filter, named Custom FW Filter. The default action is to drop any packets that do not match any firewall rules.

**Step 3—Associate the New Rules with the Newly Created Policy**

The next step is to add the rules created in the first step to the new filter created in the previous step. To do this, complete the following steps:

**Step 1**  Go to Configuration>Policy Management>Traffic Management>Filters window.

**Step 2**  Within the Filter List field, select the new filter.

**Step 3**  Under the Actions column, click **Assign rules to filter**. The Configuration>Policy Management>Traffic Management>Filters>Assign Rules to Filters window opens.

**Step 4**  Scroll through the Available Rules column and select the new rules.

**Step 5**  Click **Add** under the Actions column. This action assigns the new rules to the new filter.

In the example in the figure, the administrator adds the HTTP only (forward/out) rule to the custom firewall filter.

Step 4—Assign the New Policy to the CPP

The last step is to assign the custom firewall policy to a group's firewall policy. To do this, complete the following steps:

**Step 1** Go to Configuration>User Management>Groups window and select a group.

**Step 2** Click **Modify** (which is not shown in the figure).

**Step 3** From the Firewall Policy row, select Policy Pushed (CPP).

**Step 4** From the Policy Pushed (CPP) drop-down menu, choose the new policy.

**Step 5** Click **Apply**.

The next time a Software Client belonging to this group connects to the Concentrator, the new custom firewall filter policy is downloaded to the VPN Client. The Software Client forwards the new policy to the firewall. With the new policy, the remote user has access to the Internet via HTTP. Any HTTP inbound traffic associated with an outbound session is forwarded. Any unsolicited inbound HTTP, or any other protocol, traffic is dropped using the default rule.

# Summary

This topic summarizes what you learned in this lesson.

## Summary

**The Software Client supports three firewall features:**

- **The AYT feature monitors the operation of a specific firewall.**
- **The Stateful Firewall feature is always on, even when no VPN tunnels are established.**
- **The CPP feature enables an administrator to push firewall policy to Software Clients.**

CSVPN 4.0—7-32

# Lab Exercise—Configuring Cisco VPN Client Firewall Features

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to install and configure the Cisco Virtual Private Network (VPN) Client and configure the Cisco VPN 3000 Series Concentrator to enable VPN encrypted tunnels using integrated firewall features. Work with your lab exercise partner to complete the following tasks:

- Complete the lab exercise setup.

- Configure the Concentrator user group for split tunneling.

- Configure the Concentrator user group firewall for the AYT feature.

- Test AYT with firewall required.

- Configure AYT with the optional firewall feature.

- Test AYT with the optional firewall feature.

- Configure the Concentrator user group firewall for the CPP feature.

- Test the CPP feature.

- Use the stateful firewall (Always On) feature.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
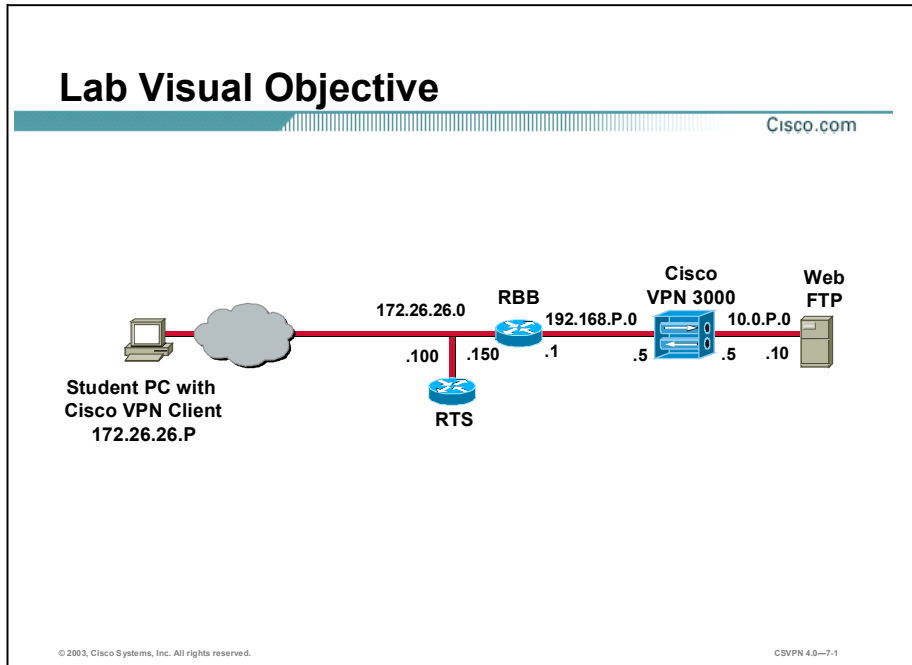


## Scenario

Your company wants to implement a Cisco VPN using split tunneling. You must configure both the remote Cisco VPN Clients and the Concentrators for remote access using integrated firewall features.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment is setup as follows:

■ Ensure that your student PC is powered on.

■ Ensure your student PC IP addresses are configured correctly:

— Primary IP address—172.26.26.P
(where P = pod number)

— Default gateway IP address—172.26.26.150

■ Ensure that your Concentrator is powered on.

## Task 2—Configure the Concentrator User Group for Split Tunneling

Split tunneling enables the remote client to browse the Internet via clear text while simultaneously accessing the corporate network via a secure tunnel. The secure tunnel protects the traffic to the corporate network. The Client Firewall application is intended to protect the Remote PC from the Internet. In this task, you will configure split tunneling in the Concentrator training user group.

| | |
|---|---|
| **Note** | This procedure assumes that Windows 2000 is already running on the student PC. |

**Step 1** Launch Internet Explorer by double-clicking the desktop icon.

**Step 2** Enter a Concentrator's public interface IP address of **192.168.P.5** in the Internet Explorer Address field. Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

(where P = pod number)

**Step 3** Log in to the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

Login: **admin**

Password: **admin**

| | |
|---|---|
| **Note** | The username (login) and password are always case-sensitive. |

**Step 4** From the Configuration menu tree, choose **Policy Management>Traffic Management> Network Lists**.

**Step 5** Click **Add**.

**Step 6** Enter a list name: **Private Network**.

**Step 7** Enter a network list: **10.0.P.0/0.0.0.255**.

(where P = pod number)

**Step 8** Click **Add**. You just created a local list for the private network.

**Step 9** From the Configuration menu tree, choose **User Management>Groups**.

**Step 10** Select the **training (Internally Configured)** group from the Current Groups list.

**Step 11** Click **Modify Group**.

**Step 12** Select the **Client Config** tab.

**Step 13** Choose the Split Tunneling Policy group box and select **Only tunnel networks in list**.

**Step 14** From the Split Tunneling Network List drop-down menu, choose **Private Network** (the network list you just created).

**Step 15** Click **Apply** and save your work.

**Step 16** Remain logged into the Concentrator, and proceed to the following task.

## Task 3—Configure the Concentrator User Group Firewall for the AYT Feature

Complete the following steps to configure the Concentrator training user group firewall for the Are You There (AYT), required firewall, feature:

**Step 1**   Choose the **training (Internally Configured)** group from the Current Groups list.

**Step 2**   Click **Modify Group**.

**Step 3**   Select the **Client FW** tab.

**Step 4**   Choose the Firewall Setting group box and select **Firewall Required**.

**Step 5**   Choose the Firewall group box and select **Network ICE BlackICE Defender** from the list.

**Step 6**   Choose the Firewall Policy group box and note that Policy defined by remote firewall (AYT) is automatically selected. This is because the BlackICE Defender Firewall is only supported for AYT not Central Policy Protection (CPP).

| **Note** | By using this configuration record, all Cisco VPN Clients become aware that they must have the BlackICE firewall running on their PC before the Concentrator will allow a tunneled connection. This also tells the VPN Client to poll for the BlackICE firewall every 30 seconds (hard-coded) and if it does not respond, to terminate the tunnel. |
| --- | --- |

**Step 7**   Scroll down and click **Apply**.

**Step 8**   Save your work by clicking the **Save Needed** icon.

**Step 9**   Log out of the Concentrator and minimize the Internet Explorer window.

## Task 4—Test AYT with Firewall Required

Complete the following steps to launch the Cisco VPN Client on your student PC to test the AYT configuration:

**Step 1**   Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco VPN Client window opens.

**Step 2**   Verify that the connection entry is **studentP**.

(where P = pod number)

**Step 3**   Verify that the IP address of the remote server is set to a Concentrator's public interface IP address: **192.168.P.5**.

(where P = pod number)

**Step 4**   Click **Connect**. The Connection History window opens and several messages flash by quickly. Disregard these messages. Complete the following sub-steps:

1. When prompted for a username, enter **studentP**.
   (where P = pod number)

2. When prompted for a password, enter **studentP**.
   (where P = pod number)

**Step 5**  Click **OK**.

You should have received an event notification. Answer the following questions:

Q1)     What is the notification text?

A)     _____

Q2)     Which firewall did the client expect to see running on the local student PC?

A)     _____

Q3)     Click **Close** to close the Cisco Systems VPN Client Notification window. Answer the following questions: Did the Cisco VPN Client actually connect?

A)     _____

The Cisco VPN Client should not have allowed the connection since the BlackICE Defender firewall specified is not installed or operational on this student PC.

## Task 5—Configure AYT with the Optional Firewall Feature

Suppose you want to use AYT with a specific firewall, but you still want people to be able to connect even if they do not have the firewall installed yet. In effect, you want to provide the remote users with a grace period in which to install a specific firewall on their PCs. Complete the following steps to enable an optional firewall:

**Step 1**  Maximize the Internet Explorer window.

**Step 2**  Enter a Concentrator public interface IP address in the Internet Explorer Address field: **192.168.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 3**  Log in to the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

---

**Note**        The username (login) and password are always case-sensitive.

---

**Step 4**  From the Configuration menu tree, choose **User Management>Groups**.

**Step 5**  Choose the **training (Internally Configured)** group from the Current Groups list.

**Step 6**  Click **Modify Group**.

**Step 7**  Select the **Client FW** tab.

**Step 8**  Choose the Firewall Setting group box and select **Firewall Optional**.

**Step 9**  Choose the Firewall group box and choose **Network ICE BlackICE Defender** from the list. By default, it should already be selected.

**Step 10**  Click **Apply** and save your work.

**Step 11**  Log out of the Concentrator and minimize the Internet Explorer window.

## Task 6—Test AYT with the Optional Firewall Feature

Complete the following steps to launch the Cisco VPN Client on your student PC to test the AYT, optional firewall configuration:

**Step 1**    Ensure that the Cisco Systems VPN Client window is open. If it is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client** from the main menu.

**Step 2**    Select **studentP** within the Connection Entry group box.

(where P = pod number)

**Step 3**    Verify that the IP address of the remote server is set to a Concentrator's public interface IP address: **192.168.P.5**.

(where P = pod number)

**Step 4**    Click **Connect**. The Connection History window opens and several messages flash by quickly. Disregard these messages. Complete the following sub-steps:

1. When prompted for a username, enter **studentP**.
(where P = pod number)

2. When prompted for a password, enter **studentP**.
(where P = pod number)

**Step 5**    Click **OK**.

You should have received an event notification. Answer the following questions:

Q4)    What is the notification text?

A)   _____

Q5)    What firewall did the Cisco VPN Client expect to see running on the local student PC?

A)   _____

Q6)    When you click **Close**, does the Cisco VPN Client still connect?

A)   _____

The Cisco VPN Client should still connect even if the firewall is not found, installed, and operational. The **Cisco VPN Client** icon in the student PCs' system tray indicates a connection.

**Step 6**    Right-click the **Cisco VPN Client** icon in the student PC's system tray.

**Step 7**    Select **Disconnect** to disconnect the client.

## Task 7—Configure the Concentrator User Group for the CPP Feature

Now that you have configured and verified the AYT feature, you need to configure and verify the Central Policy Protection (CPP) feature. Follow these instructions to configure the user group CPP feature:

**Step 1**    Maximize the Internet Explorer window.

**Step 2** Enter a Concentrator's public interface IP address in the Internet Explorer Address field: **192.168.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 3** Log in to the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

---

**Note** The username (login) and password are always case-sensitive.

---

**Step 4** From the Configuration menu tree, choose **User Management>Groups**.

**Step 5** Choose the **training (Internally Configured)** group from the Current Groups list.

**Step 6** Click **Modify Group**.

**Step 7** Select the **Client FW** tab.

**Step 8** Choose the Firewall Setting group box and select **Firewall Required**.

**Step 9** Choose the Firewall group box and choose **Cisco Integrated Client Firewall** from the list.

Choose the Firewall Policy group box and note that Policy Pushed (CPP) is automatically selected. This is because the Cisco Integrated Client (CIC) firewall only supports CPP and not AYT.

**Step 10** Choose **Firewall Filter for VPN Client (Default)** from the Firewall Policy drop-down menu.

---

**Note** This is the default Cisco VPN Client CPP policy defined in the 3.5 and higher Cisco VPN 3000 Series Concentrator software release. This policy blocks all inbound traffic on the Cisco VPN Client that is not related to any outbound traffic. This is essentially the same as the Cisco Integrated Client Stateful Firewall (Always On) policy, except this policy only applies when the Cisco VPN Client is connected and using split tunneling.

---

**Step 11** Click **Apply** and save your work.

**Step 12** Log out of the Concentrator and minimize the Internet Explorer window.

You have configured CPP for the Concentrator training user group. Because we enabled split tunneling in Task 1, the client should connect and accept the pushed CPP policy designated in the training user group record. Now you need to test your CPP configuration.

## Task 8—Test the CPP Feature

In this task you will attempt to connect to the Concentrator using the Cisco VPN Client running the Cisco Integrated Client Firewall and a pushed CPP policy. Complete the following steps:

**Step 1** Ensure that the Cisco Systems VPN Client window is open. If it is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client** from the main menu.

**Step 2** Select **studentP** within the Connection Entry group box.

(where P = pod number)

---

**Step 3**   Verify that the IP address of the remote server is set to a Concentrator's public interface IP address of **192.168.P.5**.

(where P = pod number)

**Step 4**   Click **Options**. A popup menu opens.

**Step 5**   Ensure the **Stateful Firewall (Always On)** option is off (not selected).

**Step 6**   Click **Connect**. The Connection History window opens and several messages flash by quickly. Disregard these messages. Complete the following sub-steps:

1.   When prompted for a username, enter **studentP**.
     (where P = pod number)

2.   When prompted for a password, enter **studentP**.
     (where P = pod number)

**Step 7**   Click **OK**.

The client should connect.

**Step 8**   Right-click the **Cisco VPN Client** icon in the student PC's system tray and choose **Statistics**. The Cisco Systems VPN Client Statistics window opens.

**Step 9**   Select the **Firewall** tab and view the attributes of this connection. Answer the following questions:

Q7)   What personal firewall is running on this student PC?

A)   _____

Q8)   What firewall policy is active?

A)   _____

**Step 10**   Select the **Tunnel Details** tab and leave it open.

**Step 11**   Note the number of encrypted and decrypted packets.

**Step 12**   Open a command prompt and ping your Concentrator's private interface.

View the Statistics tab again. Answer the following question:

Q9)   Did the encrypted and decrypted packets count change?

A)   _____

The encrypted number should have increased since you are connected to the Concentrator through the secure tunnel.

**Step 13**   Have one of the other training pods open a command prompt from the desktop icon and ping your student PC at 172.26.26.P.

(where P = pod number)

Answer the following question:

Q10)   Was the ping successful?

A)   _____

The other students should not be able to ping your student PC because the filter is blocking all inbound sessions.

**Step 14**   Attempt to ping 172.26.26.150 from your student PC, and answer the following question:

Q11)   Was the ping successful?

A)   _____

You should be able to ping 172.26.26.150 because the filter allows outbound sessions.

**Step 15**   Close the connection status window. Leave the client connected.

## Task 9—Use the Stateful Firewall (Always On) Feature

Complete the following steps to enable the Cisco Integrated Client Stateful Firewall (Always On) feature:

**Step 1**   Ensure that the Cisco Systems VPN Client window is open. If it is not open, choose **Start>Programs>Cisco Systems VPN Client>VPN Client** from the main menu.

**Step 2**   Click **Options**. A popup menu opens.

**Step 3**   Enable the **Stateful Firewall (Always On)** option (is selected).

**Step 4**   Disconnect the Cisco VPN Client. Now that the Cisco VPN Client connection has been terminated, you will test to see if the Stateful Firewall (Always On) policy is truly always on.

**Step 5**   Open a command prompt and ping the IP address of another pod's PC (172.26.26.Q).

(where Q = peer pod number)

---

| Note | Ensure that the other pod has disabled the Stateful Firewall feature first. |
|------|------------------------------------------------------------------------------|

---

Answer the following question:

Q12)   Were you able to ping the other pod's PC?

A)   _____

**Step 6**   You should be able to ping the other pod's PC as the Stateful Firewall (Always On) policy always allows inbound sessions that are related to outbound requests.

**Step 7**   Have another pod attempt to ping your PC at 172.26.26.P.

(where P = pod number)

Answer the following question:

Q13)   Was the other pod able to ping your PC?

---

A)      _____

The other pod should not be able to ping your PC since the Stateful Firewall (Always On) policy always drops inbound packets not related to outbound sessions. This policy applies even when the client is not operating. Continue with the following steps to see what happens when you turn off the Stateful Firewall (Always On) feature.

**Step 8** Open the Cisco VPN Client by choosing **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 9** Select **studentP** within the Connection Entry group box.

(where P = pod number)

**Step 10** Click **Options**. A popup menu opens.

**Step 11** Select the **Stateful Firewall (Always On)** option to turn it off and deselect it.

**Step 12** Close the Cisco VPN Client window.

**Step 13** Have another pod ping your PC at 172.26.26.P.

(where P = pod number)

Answer the following question:

Q14) Was the other pod able to ping your PC?

A)      _____

The other pod should be able to ping your PC since the Stateful Firewall (Always On) feature has been turned off.

**Step 14** Close all open windows.

**8**

# Configure the Cisco Virtual Private Network Client Auto-Initiation Feature

## Overview

This lesson explains how to configure the Cisco VPN Software Client auto-initiation feature. After presenting an overview of the feature, the lesson shows you each major step of the configuration. It includes the following topics:

■ Objectives

■ Overview of the Cisco VPN Software Client auto-initiation feature

■ Configure the Cisco VPN Software Client auto-initiation feature

■ Summary

■ Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Configure the vpnclient.ini file.**
- **Configure the Cisco VPN Software Client auto-initiation parameters.**
- **Pause and resume the auto-initiation feature.**
- **Monitor the progress of an auto-initiated IPSec tunnel.**

CSVPN 4.0—8-2

# Overview of the Cisco VPN Software Client Auto-Initiation Feature

This topic presents an overview of the Cisco Virtual Private Network (VPN) Software Client auto-initiation feature.

## Auto-Initiation Feature

### ABC Corporation WLAN

**Encrypted**

10.0.1.10

**Cisco VPN 3000 Series Concentrator**

**Auto-initiation IPSec tunnel**

CSVPN 4.0—8-4
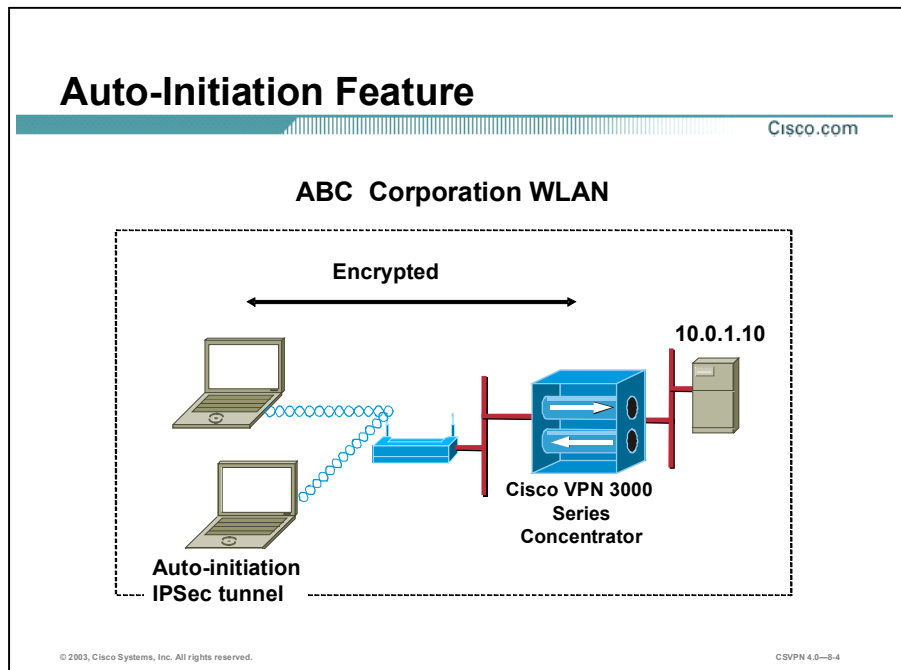
Wireless LAN connections are often insecure. Using a Software Client to connect to the concentrator over an encrypted wireless connection resolves the security problem. However, the local wireless users must be burdened with establishing the encrypted wireless VPN connection on the corporate LAN. The auto-initiation feature intends to alleviate this burden from the user by providing an automated method for establishing VPN network connections. The intent is to achieve as seamless and secure an environment as possible with the software technology currently available.
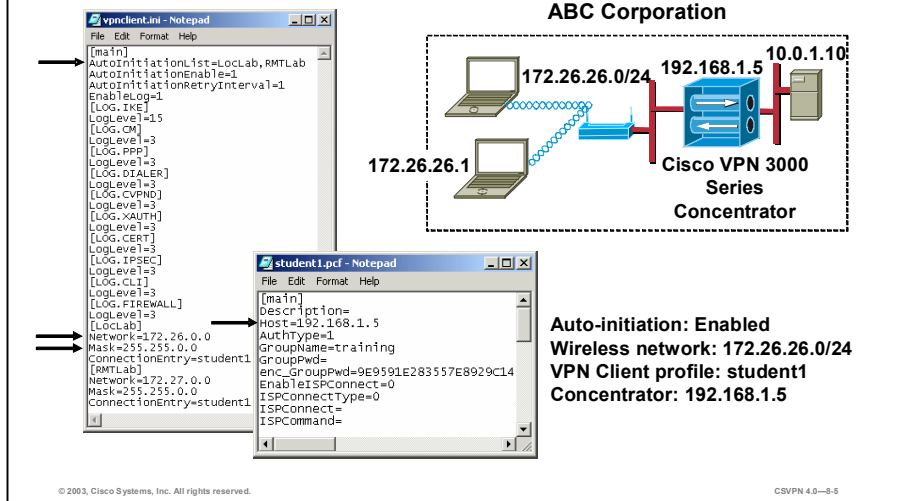
Automatic VPN initiation (auto-initiation) provides secure connections within an on-site wireless LAN (WLAN) environment through a Concentrator. When auto-initiation is configured on the Software Client, the Software Client:

■ Reads the VPNClient.ini file after one of the following:

— System startup

— PC standby or hibernation

— Auto-initiation configuration changes

— IP address changes

— IPSec tunnel disconnect

■ Detects by reading the VPNClient.ini file if the auto-initiation feature is enabled.

■ Determines whether the PC resides on one of the networks defined in the VPNClient.ini file auto-initiation network list.

■ Determines which Software Client attributes to use when establishing an IPSec tunnel. The VPNClient.ini file defines where to find the attributes, via the .PCF file listed in the connection entry field. The .PCF file defines the Software Client connection attributes.

■ Initiates a VPN connection using the attributes found in the connection .PCF file.

- Prompts the user to authenticate, and allows that user network access.

In the figure, there is a wireless PC located on the ABC Corporation WLAN. After system startup, the Software Client checks the VPNClient.ini file. First, the Software Client detects that the auto-initiation feature is enabled. Next, the Software Client checks the IP address of the NIC card, 172.26.26.1. From the NIC IP address, the Software Client determines that the PC resides on a network defined in the VPNClient.ini file, 172.26.26.0/24. The last step is to establish an IPSec tunnel using the information found in the connection entry profile. In this instance, the connection entry is student1.PCF. Using the information found in the student1.PCF file, the Software Client establishes an IPSec tunnel to the Concentrator at IP address 192.168.1.5.

# Configure the Cisco VPN Software Client Auto-Initiation Feature
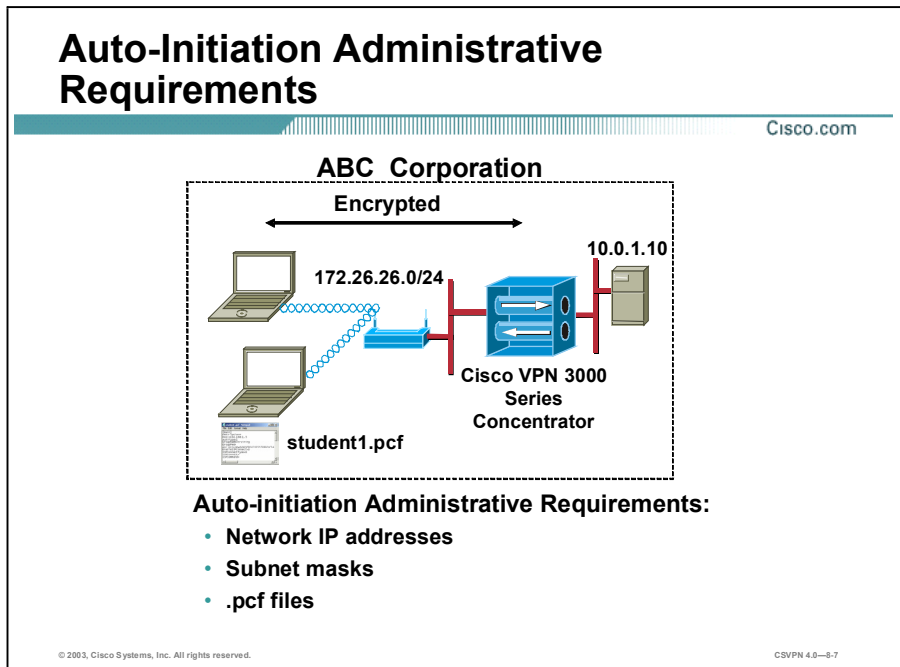


In the VPNClient.ini file, the network administrator can configure a list of up to 64 matched networks (IP address/subnet masks) and corresponding connection profiles (.pcf files). Typically, the administrator enters one network address and .PCF filename per site. When the Software Client detects that the PC resides on one of the networks in the auto-initiation network list, it automatically establishes a VPN connection using the profile listed for that network.

Before the auto-initiation user begins, the administrator should gather the information they need to configure auto-initiation:

■ The network IP addresses for the client network, 172.26.26.0.

■ The subnet mask for the client network, 255.255.255.0.

■ The filenames for all VPN connection entries, .PCF filenames, which users are using for their auto-initiation connections, student1.PCF.

A user might always report to the same office. This probably requires one network address and .PCF filename. In other instances, another user might travel between several offices. This may require a network address and .PCF file name for each office visited. That depends on the company's network-addressing scheme.

## Configuration Parameters

Cisco.com

**Global profile parameters**

**Cisco VPN Client Parameters**

CSVPN 4.0—8-8
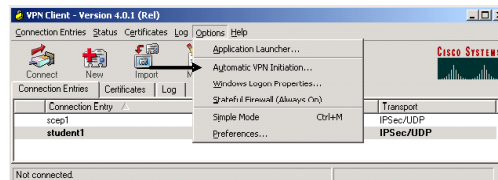
Groups of configuration parameters define the connection entries that remote users use to connect to a VPN device. There are two files: a global settings file and an individual connection profile. A global settings file defines the rules for all remote users; it contains parameters for the Software Client as a whole and auto-initiation parameters. The name of the global settings file is vpnclient.ini. Individual connection profiles contain the parameter settings for each VPN connection and are unique to that connection entry. Individual profiles have a .pcf extension (not shown).

The administrator must edit the global settings file to enable the feature on the VPN client to configure auto-initiation for users on the network. By default, auto-initiation parameters are not present on the global settings file (vpnclient.ini). The administrator must add parameters to the vpnclient.ini file via a text editor.

Through the Software Client graphical user interface (GUI) application, the administrator has the ability to enable or disable auto-initiation and to change the retry interval. The administrator must choose Start>Programs>Cisco Systems VPN Client>VPN Client to access these GUI parameters. Administrators select Automatic VPN Initiation from the Options drop-down menu.

| Note | When auto-initiation is not present in the global settings file, the automatic VPN Initiation menu option does not appear in the Options drop-down menu. |

## VPNClient.ini File Parameters

Cisco.com

Auto-initiation parameters

Auto-initiation section

**Default vpnclient.ini**

**Auto-initiate vpnclient.ini**

CSVPN 4.0—8-9

The global settings file is created in one of two ways: when an administrator or a remote user creates connection entries using the VPN Client application (connection wizard) or when the administrator creates global settings using a text editor. In the first case, the remote user is also creating a file that can be edited by a text editor. The administrator can start with a global settings file generated through the GUI and then edit it. This approach lets you control some parameters that are not available in the Software Client GUI application such as the auto-initiation feature. The default location for the global settings file is C:\Program Files\Cisco Systems\VPN Client.

There are two sets of auto-initiation fields, auto-initiation parameters and auto-initiation sections. The VPNClient.ini file auto-initiation parameters are as follows:

■ AutoInitiationList—A list of auto-initiation related section names within the INI file. Each of these sections contains a network address, subnet mask, and ConnectionEntry. If the PC is resident on one of these listed networks, the Software Client performs auto-initiation, if enabled. The auto-initiation list is evaluated in the order in which it was entered. In the above example, LocLab section is evaluated first, RMTLab section tested second, and so on. The VPNClient.ini file can contain a maximum of 64 entries.

■ AutoInitiationEnable—Enables auto-initiation, which is an automated method for establishing a wireless VPN connection in a LAN environment. The values are 0 = Disable and 1 = Enable.

■ AutoInitiationRetryInterval—Specifies the time to wait, in minutes, before retrying auto-initiation after a connection attempt failure. The allowable range of retry values is one to ten minutes, with a default value of one minute.

The VPNClient.ini auto-initiation section defines the auto-initiation networks and related .PCF file. If a PC resides on the defined network and auto-initiation is enabled, the Software Client will establish an IPSec tunnel automatically. The connection entry defines which connection profile, .PCF file, to use when making the VPN connection. Entries from the .PCF file are used to pre-configure the VPN Client. The .PCF parameters define such values as the Concentrator IP address and users group name.VPNClient.ini file auto-initiation section parameters are as follows:

- [section name]—Identifies one of the names listed in the AutoInitiationList field. Each section contains a network address, subnet mask, and connection entry.

- Network—Specifies the IP address of a network the PC may reside on.

- Mask—Specifies the subnet mask for that network.

- ConnectionEntry—Identifies the connection entry profile to be used if the PC resides on the preceding network.

In the figure, there are two VPNClient.ini files, a default and an edited version. The left hand one is the result of adding an IPSec tunnel via the connection wizard. Notice there are no auto-initiation parameters. On the right is a text-edited version of the file. The top three auto-initiation parameters enable the feature. The Auto-initiation section parameters define the network address, subnet mask, and .pcf file name, student1. The network address of the local network is 172.26.0.0/255.255.0.0. The individual profile (.PCF) file linked to this address is student1. When auto-initiation is enabled, if the PC is resident on the 172.26.26.0/24 network, the Software Client will attempt to establish an IPSec tunnel using the attributes contained in the student1.PCF file.

# Cisco VPN Software Client Parameters
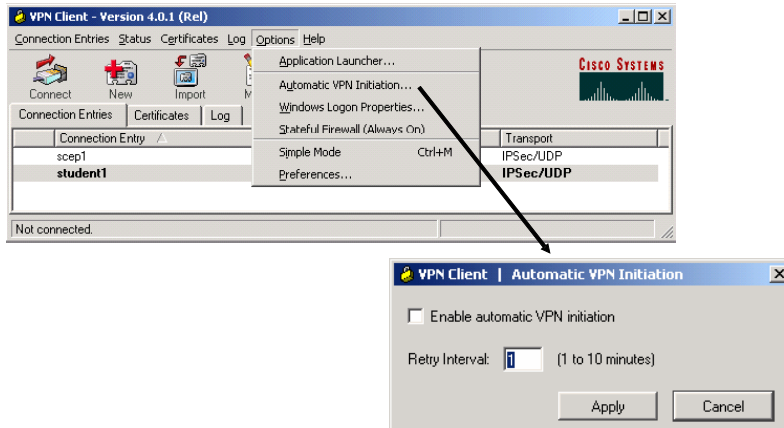
The Options pop-up menu has an Automatic VPN Initiation dialog menu item. The Automatic VPN Initiation menu allows the user to enable or disable the auto-initiation feature, as well as modify the retry interval. The retry interval specifies, in minutes, the amount of time the client will wait before retrying an auto-initiation connection attempt. Both values are stored in the vpnclient.ini file.
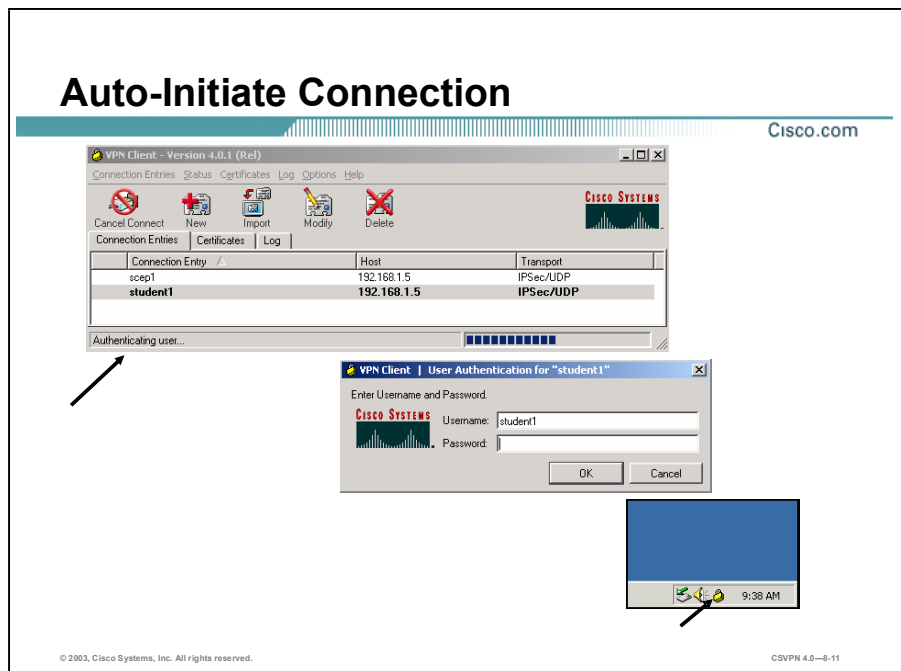
When the Software Client detects the PC resides on one of the networks in the auto-initiation network list, it automatically tries to establish a VPN connection using the linked profile for that network. The Software Client informs you when the VPN connection is auto initiating and at various stages of the auto-initiated connection process.

In the example above, when the PC launches an IPSec tunnel, the auto-initiating VPN connection window opens. In the connection history window, the Software Client provides progress updates messages. When it is time to authenticate the remote user, the user authentication window will open and prompt the remote user for a username and password. When successfully established, a closed yellow lock appears in the system tray. When auto-initiation is configured, some Software Client status displays and dialog boxes differ slightly from standard connection dialog boxes to indicate to the user that auto-initiation is occurring.

# Auto-Initiation Termination

**Auto-initiation
termination message**
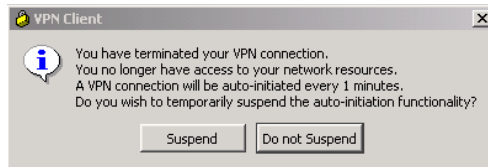


**Cisco VPN
Client menu**
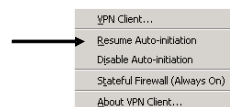


CSVPN 4.0—8-12

When a user disconnects via the Lock icon in the system tray or via the connection status dialog box, the Software Client will behave differently than manually established IPSec tunnels by displaying a Cisco Systems Software Client termination message box. If the user selects Do Not Suspend in the message box, the Software Client will terminate and auto-initiation will be retried later. The retry interval is user configurable. If the user selects Yes, the Software Client enters the suspended auto-initiation state, and an open yellow Lock icon is displayed in the system tray. Auto-initiation is temporarily suspended.

The VPN Client menu is displayed when the user right clicks the open yellow Lock icon in the system tray. The VPN Client menu choices are Resume Auto-initiation or Disable Auto-initiation. The Resume Auto-initiation menu item will cause the Software Client to immediately auto-initiate a VPN connection. The Disable Auto-initiation menu item will cause the Software Client to disable auto-initiation in the vpnclient.ini file. The remote user can also disable auto-initiation from the Software Client GUI>Options>Automatic VPN Initiation window by de-selecting the Enable check box. Once disabled, the Software Client no longer automatically attempts to launch the VPN Client. It remains disabled until the feature is manually re-enabled.

# Cisco VPN Software Client Event Log

```
VPN Client | Log Window                                      _ □ ×

Cisco Systems VPN Client Version 4.0.1 (Rel)                      ▲
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

193    11:44:50.501  06/09/03  Sev=Info/6        GUI/0x63B00003
Auto-initiation has been resumed.

194    11:44:50.812  06/09/03  Sev=Info/4        CM/0x63100002
Begin connection process

195    11:44:50.822  06/09/03  Sev=Info/4        CM/0x63100004
Establish secure connection using Ethernet

196    11:44:50.822  06/09/03  Sev=Info/4        CM/0x63100024
Attempt connection with server "192.168.1.5"

197    11:44:50.822  06/09/03  Sev=Info/6        IKE/0x6300003B
Attempting to establish a connection with 192.168.1.5.             ▼

 [ Save ]  [ Log Settings ]  [ Clear ]              [ Close ]
```

CSVPN 4.0—8-13

The administrator can verify the progress of the auto-initiated tunnel by accessing the Cisco Systems IPSec Log viewer. In the figure, auto-initiation was resumed. The IPSec tunnel attempted to connect to the destination IP address, 192.168.1.5. The destination IP address was located in the PC's .PCF file.

# Summary

This topic summarizes what you learned in this lesson.

## Summary

Cisco.com

- **Auto-initiation enables a Cisco VPN Software Client to establish an IPSec tunnel automatically.**
- **Auto-initiation is initiated after system restart, standby or hibernation mode, IP address change, auto-initiation configuration change, or IPSec tunnel disconnect.**
- **Auto-initiation parameters are added to the vpnclient.ini file via a text editor.**
- **A .pcf filename, network address, and subnet mask are needed for each site.**

CSVPN 4.0—8-15

# Lab Exercise—Configure the Cisco VPN Client Auto-Initiation Feature

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to configure and monitor the Cisco Virtual Private Network (VPN) client auto-initiation. Work with your lab partner to complete the following tasks:

- Complete the lab exercise setup.

- Manually launch the Cisco VPN Client.

- Verify the auto-initiation feature is not enabled.

- Enable the auto-initiation feature.

- Establish an IPSec tunnel using the auto-initiation feature.

- Disconnect and re-establish the IPSec tunnel.

- Suspend and resume the auto-initiation feature.

- Disable the auto-initiation feature.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
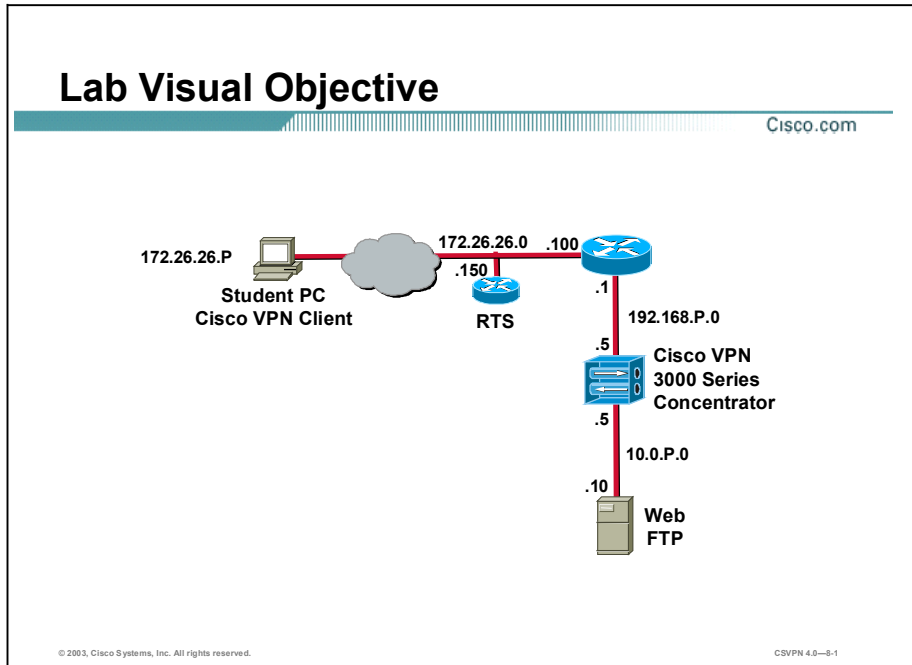


## Scenario

Your employer has asked you to provide better security for your wireless users. You will configure users for the Cisco VPN Client auto-initiation.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment as follows:

■ Ensure that your student PC is powered on.

■ Ensure your student PC IP addresses are configured correctly:

— Primary IP address—172.26.26.P
(where P = pod number)

— Default gateway IP address–172.26.26.150

■ Ensure that your Concentrator is powered on.

## Task 2—Manually Launch the Cisco VPN Client

In this task, verify you can establish an IPSec tunnel manually. Complete the following steps to launch the Cisco VPN Client on your student PC:

**Step 1**   Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.

**Step 2**   Verify that the connection entry is **studentP**.

(where P = pod number)

**Step 3**   Verify that the IP address of remote server is set to a Cisco VPN 3000 Series Concentrator's public interface IP address of **192.168.P.5**.

(where P = pod number)

**Step 4**   Click **Connect**. The Connection History window opens and several messages flash by quickly. Complete the following sub-steps:

   1.   Enter **studentP** when you are prompted for a username.
        (where P = pod number)

   2.   Enter **studentP** when you are prompted to enter a password.
        (where P = pod number)

**Step 5**   Click **OK**. The window closes and a Cisco VPN Client icon appears in the system tray.

**Step 6**   Disconnect the IPSec tunnel.

## Task 3—Verify the Auto-Initiation Feature is Not Enabled

The auto-initiation feature is configured manually on the Cisco VPN Client. Complete the following steps to view the default vpnclient.ini file:

**Step 1**   Go to the My Computer>Local Disk (C:)>Program Files >Cisco Systems >VPN Client folder on the student PC. The Cisco VPN Client folder opens.

**Step 2**   Select the **vpnclient.ini** file in the Cisco VPN Client window, and open it with Notepad. Examine the contents.

**Step 3**   Close the Notepad window and minimize the Cisco VPN Client window.

**Step 4**   Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.

**Step 5**   Select **Options** from the drop-down menu and verify that the Automatic VPN Initiation menu selection is not present.

**Step 6**   Close the Cisco Systems VPN Client window.

## Task 4—Enable the Auto-Initiation Feature

Complete the following steps to configure the vpnclient.ini file for auto-initiation:

**Step 1**   Maximize the Cisco VPN Client folder.

---

**Note**     If the VPN Client folder contains a file called internal.ini, copy the contents of this file to the beginning of the vpnclient.ini file before continuing.

---

**Step 2**   Select the **vpnclient.ini** file from the Cisco VPN Client window, and open it with Notepad.

**Step 3**   Using the text edit feature of Notepad, add the auto-initiation parameters to the vpnclient.ini file. Directly after [main], add the following lines:

**AutoInitiationList=studentP**

**AutoInitiationEnable=0**

**AutoInitiationRetryInterval=1**

(where P = pod number, do not add this line to the file)

**Step 4**   Using the text-editing feature of Notepad, add the auto-initiation list parameters to the vpnclient file. Add the following lines at the bottom of the file:

**[studentP]**

**Network=172.26.26.0**

**Mask=255.255.255.0**

**ConnectionEntry=studentP**

(where P = pod number, do not add this line to the file)

**Step 5**   Select **File>Save** from the Notepad tool bar.

**Step 6**   Close Notepad and the Cisco VPN Client.

**Step 7**   Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.

**Step 8**   Select **Options**.

**Step 9**   Select **Automatic VPN Initiation** from the Options drop-down menu.

**Step 10**  Select the **Enable** check box from the Automatic VPN Initiation window.

**Step 11**  Click **Apply** from the Automatic VPN Initiation window.

## Task 5—Establish an IPSec Tunnel Using the Auto-Initiation Feature

Upon closing the Cisco Systems VPN Client window, you started the auto-initiation process. The Cisco VPN Client re-reads the vpnclient file. Due to the editing completed in the last task, auto-initiation is now enabled with a re-try timer of 1 minute. In approximately one minute, an auto-initiating VPN connection window should appear. The auto-initiating VPN connection to 192.168.P.5 message window opens. This window is followed closely by the User authentication of studentP window. Complete the following steps in the User authentication of studentP window:

**Step 1**   Enter **studentP** when you are prompted for a username.

(where P = pod number)

**Step 2**   Enter **studentP** when you are prompted for a password.

(where P = pod number)

**Step 3**   Click **OK**.

The window closes, the Cisco VPN Client icon appears in the system tray and the auto-initiated VPN connection is successfully established.

## Task 6—Disconnect and Re-establish the IPSec Tunnel

Upon disconnecting an IPSec tunnel, you are prompted to resume or suspend the auto-initiation feature. If you answer No, the auto-initiation feature resumes. Complete the following steps to disconnect and resume the auto-initiation:

**Step 1**  Disconnect your VPN connection using the Cisco VPN Client icon in the student PC's system tray. The VPN Client window opens.

**Step 2**  Answer the following questions from the Cisco Systems VPN Client window:

Q1)  If you click Suspend, what will happen? (Do not click Suspend at this time.)

A)  _____

**Step 3**  Click **Do not Suspend**.

Q2)  By clicking Do not Suspend, what happens?

A)  _____

**Step 4**  The auto-initiating process resumes. After approximately 1 minute, the auto-initiating VPN connection to 192.168.P.5 message window opens. This window is followed closely by the User authentication of studentP window. Complete the following sub-steps in the User authentication of studentP window:

1.  Enter **studentP** when you are prompted for a username.
    (where P = pod number)

2.  Enter **studentP** when you are prompted for a password.
    (where P = pod number)

3.  Click **OK**.

The window closes, the Cisco VPN Client icon appears in the system tray, and the auto-initiated VPN connection is successfully established.

## Task 7—Suspend and Resume the Auto-Initiation Feature

In this task, you will disconnect the IPSec tunnel, and suspend auto-initiation.

**Step 1**  Disconnect your VPN connection using the Cisco VPN Client icon in the student PC's system tray. The VPN Client window opens.

**Step 2**  Click **Suspend** in the Cisco Systems VPN Client window, and answer the following questions:

Q3)  What happens to the VPN auto-initiation?

A)  _____

**Step 3**  Right click the Cisco VPN Client icon. The Cisco VPN Client menu is displayed.

**Step 4**  Select **Resume Auto-initiation** and answer the following question.

Q4)  What happens?

A)  _____

**Step 5**  Complete the following sub-steps in the User authentication of studentP window:

1.  Enter **studentP** when you are prompted for a username.
    (where P = pod number)

2.  Enter **studentP** when you are prompted for a password.
    (where P = pod number)

3.  Click **OK**. The window disappears and the Cisco VPN Client icon appears in the system tray.

# Task 8—Disable the Auto-Initiation Feature

In this task, you will disable then manually re-enable auto-initiation.

**Step 1**  Disconnect your VPN connection using the Cisco VPN Client icon in the student PC's system tray). The VPN Client window opens.

**Step 2**  Click **Suspend** in the VPN Client window. The Auto-initiation feature is suspended.

**Step 3**  Right click the Cisco VPN Client icon on the system tray. The Cisco VPN Client menu is displayed.

**Step 4**  Select **Disable Auto-initiation.** The VPN Client window opens**.** From the VPN Client window, answer the following questions:

Q5)  If you click Disable, what will happen?

A)  _____

**Step 5**  Click **Disable**.

**Step 6**  Go to the My Computer>Local Disk (C:)>Program Files >Cisco Systems >VPN Client folder on the student PC. The Cisco VPN Client folder opens.

**Step 7**  Select the **vpnclient.ini** file from the Cisco VPN Client window, and open it with Notepad. Answer the following questions after you have viewed the file:

Q6)  AutoInitiationEnable field equals 0. What does this mean?

A)  _____

**Step 8**  Close Notepad.

**Step 9**  Close the Cisco VPN Client window. The auto-initiation feature is disabled.

**Step 10**  Once auto-initiate is disabled, you must re-enable it manually. Choose **Start>Programs>Cisco Systems VPN Client>VPN Client** to re-enable auto-initiation. The Cisco Systems VPN Client window opens.

**Step 11**  Click **Options**. The Options drop-down menu opens.

**Step 12**  Select **Automatic VPN Initiation**. The Automatic VPN Initiation window opens.

Q7)      What is the status of Automatic VPN Initiation?

A)      _____

**Step 13**  Select **Enable** and click **Apply**.

**Step 14**  Close the Cisco Systems VPN Client window. Auto-initiation is re-enabled. The auto-initiation process should begin immediately.

**Step 15**  Complete the following sub-steps in the User Authentication of StudentP window:

1. Enter **studentP** when you are prompted for a username.
   (where P = pod number)

2. Enter **studentP** when you are prompted for a password.
   (where P = pod number)

3. Click **OK**.

**Step 16**  The window closes and the Cisco VPN Client icon appears in the system tray. Auto-initiation has resumed.

**Step 17**  Complete the following sub-steps to disable auto-initiation:

1. Double click the Cisco VPN Client icon in the student PC's system tray. The VPN Client window opens.

2. Click **Disconnect**. The Cisco Systems VPN Client window opens.

3. Click **Suspend**.

4. Right click the Cisco VPN Client icon in the student PC's system tray.

5. Select **Disable Auto-initiation**. The Cisco Systems VPN Client window opens.

6. Click **Disable**.

**9**

# Monitor and Administer the Cisco VPN 3000 Series Concentrator Remote Access Networks

## Overview

This lesson teaches how to monitor and administer Cisco Virtual Private Network (VPN) 3000 Series Concentrator remote access networks. It includes the following topics:

■ Objectives

■ Monitoring

■ Administration

■ Bandwidth Management

■ Summary

■ Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Configure monitoring for the Cisco VPN 3000 Series Concentrator.**
- **Perform basic administrative tasks such as configuring access control, event classes, file management, and the AAA server and updating the software on the Cisco VPN 3000 Series Concentrator.**
- **Configure bandwidth management.**

CSVPN 4.0—9-2

# Monitoring

This topic presents an overview of monitoring.



The Concentrator tracks many statistics and the status of many items essential to system administration and management. Monitoring enables you to view Concentrator status, sessions, statistics, and event logs, including the following:

■ Routing table—Current valid routes, protocols, and metrics

■ Dynamic filters—Current dynamic filters and their associated rules

■ Event logs—Current event log in memory

■ System status—Current software revisions, uptime, system power supplies, Ethernet interfaces, front-panel LEDs, and hardware sensors

■ Sessions—Currently active sessions sorted by protocol, Scalable Encryption Processing (SEP), and encryption; and top ten sessions sorted by data, duration, and throughput

■ Statistics—Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IPSec, HTTP, events, Telnet, Domain Name System (DNS), authentication, accounting, filtering, Virtual Router Redundancy Protocol (VRRP), Secure Sockets Layer (SSL), load balancing, and compression; and Management Information Base (MIB)-II objects for

interfaces, TCP/UDP, IP, Internet Control Message Protocol (ICMP), and Address Resolution Protocol (ARP)

**Monitor System Status**

Cisco.com

Monitoring | System Status — Monday, 16 June 2003 16:49:28
Refresh

Software →

VPN Concentrator Type: 3005
Serial Number:
Bootcode Rev: Cisco Systems, Inc./VPN 3000 Concentrator Series Version 2.5.Rel Jun 21 2000 18:57:52
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 4.0.1.Rel May 06 2003 13:13:03
Up For: 0:55:09
Up Since: 06/16/2003 15:54:19
RAM Size: 32 MB (Memory Status: Green)

Hardware →

In the back-panel picture below, select and click a module for status details.

| Fan 1 | Fan 2 | | CPU |
|---|---|---|---|
| 6308 RPM | 6308 RPM | | 20°C/68°F |

CPU Utilization    Active Sessions    Throughput

© 2003, Cisco Systems, Inc. All rights reserved.    CSVPN 4.0—9-5

The Monitoring>System Status window enables the administrator to view information on both the hardware and software. The system status display enables you to view the following:

■ Boot code revision and software revision

■ Uptime

■ Fan speed

■ RAM size

■ Temperature

■ CPU use

■ Active sessions

■ Aggregate throughput

The system status display can be used for quick and easy checks of the basic systems operations.

Besides the Monitoring>System Status window, you can also access and view the hardware and software status via the command line interface (CLI) or through Simple Network Management Protocol (SNMP).

**Monitor Interface Statistics**

Cisco.com

| Interface | 1 |
|---|---|
| IP Address | 10.0.1.1 |
| Status | UP |
| Rx Unicast | 0 |
| Tx Unicast | 0 |
| Rx Multicast | 1 |
| Tx Multicast | 0 |
| Rx Broadcast | 3794 |
| Tx Broadcast | 30 |

CSVPN 4.0—9-6

The Monitor System Status>Interface window enables the administrator to view all Ethernet interfaces. Place the mouse cursor over the Ethernet interface and click it to view real-time port statistics. The interface statistics displays the following:

■ IP address

■ Status

■ Receive unicast

■ Transmit unicast

■ Receive multicast

■ Transmit multicast

■ Receive broadcast

■ Transmit broadcast

The Monitor System Status>Power window enables the administrator to view all power supplies. Place the mouse cursor over the power supply and click it to view real-time statistics. By doing this, you can also view the Concentrator's power supply status. The power supply status indicates the following:

■ One or both power supplies, voltages, and status

■ Main board voltages and status

■ CPU voltages and status

| Note | Most of these items are available through CLI and SNMP monitoring. |

## Monitor Routing Table

| Monitoring | Routing Table | | | | | Friday, 13 April 2001 10:36:14 | |
| --- | --- | --- | --- | --- | --- | --- | --- |

Refresh

**Clear Routes**

Valid Routes: 3

| Address | Mask | Next Hop | Interface | Protocol | Age | Metric |
| --- | --- | --- | --- | --- | --- | --- |
| 0.0.0.0 | 0.0.0.0 | 192.168.1.1 | 2 | Default | 0 | 1 |
| 10.0.1.0 | 255.255.255.0 | 0.0.0.0 | 1 | Local | 0 | 1 |
| 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 2 | Local | 0 | 1 |

CSVPN 4.0—9-8

The Monitoring>Routing Table window enables an administrator to view the Concentrator's routing table. The IP routing subsystem examines the destination IP address of packets coming through the Concentrator and forwards or drops them according to the routing table.

The table includes all routes that the IP routing subsystem knows about, from whatever source: static routes learned via IP and Open Shortest Path First (OSPF) routing protocols, interface addresses, and so on. The Monitoring>Routing Table window enables you to view the following:

- Valid routes

- Addresses and masks

- The next hop

- Interface

- Protocol

- Age

- Metric

---

**Note**        This information is available through the CLI also.

---

**Monitor General Statistics**

Cisco.com

**Monitoring | Statistics**

This section shows statistics for VPN 3000 Concentrator tunneled sessions, traffic, connection activity, and standard MIB-II objects.

In the left frame, or in the list of links below, click the statistics you want to view:

- Accounting
- Address Pools
- Administrative AAA
- Authentication
- Bandwidth Management
- Compression
- DHCP
- DNS
- Events
- Filtering

- HTTP
- IPSec
- L2TP
- Load Balancing
- NAT
- PPTP
- SSH
- SSL
- Telnet
- VRRP

- MIB-II -- interfaces, TCP/UDP, IP, RIP, OSPF, ICMP, ARP table, etc.

CSVPN 4.0—9-9

The Monitoring>Statistics window displays statistics for traffic and activity on the Concentrator since it was last booted or reset. The following can be monitored:

■ PPTP—Total tunnels, sessions, received and transmitted control, data packets, and detailed current session data

■ L2TP—Total tunnels, sessions, received and transmitted control, data packets, and detailed current session data

■ IPSec—Tunnels, received and transmitted packets, and session details

■ HTTP—Total data traffic and connection statistics

■ Events—Total events sorted by class, number, and count

■ Telnet—Total sessions, and current session inbound and outbound traffic

■ DNS—Total requests, responses, timeouts, and so on

■ Authentication—Total requests, accepts, rejects, challenges, timeouts, and so on

■ Accounting—Total requests, responses, timeouts, and so on

■ Filtering—Total inbound and outbound filtered traffic by the interface

■ VRRP—Total advertisements, master router roles, errors, and so on

- SSL—Sessions, and encrypted versus decrypted traffic

- DHCP—Leases and durations

- Address Pools—Configured pools and allocated addresses

- SSH—Sessions, inbound and outbound

- Load Balancing—Load, state, peers, and so on

- Compression—Precompressed, postcompressed, ratios, and so on

- Administrative AAARequests, accepts, rejects, challenges, timeouts, and so on

- NAT—Sessions, inbound and outbound packets, and so on

- MIB-II Stats—Interfaces, TCP and UDP, IP, ICMP, and ARP

# Monitor Statistics IPSec

CSVPN 4.0—9-10

The Monitoring>Statistics>IPSec window displays statistics for IPSec activity, including Internet Key Exchange (IKE) and IPSec statistics.

## Monitor Sessions

Monitoring | Sessions                                                Monday, 29 July 2002 14:14:30
Reset ⊘ Refresh ®

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group ─All─ ▼

**Session Summary**

| Active LAN-to-LAN Sessions | Active Remote Access Sessions | Active Management Sessions | Total Active Sessions | Peak Concurrent Sessions | Concurrent Sessions Limit | Total Cumulative Sessions |
|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 2 | 4 | 100 | 37 |

**LAN-to-LAN Sessions**                           [ Remote Access Sessions | Management Sessions ]

| Connection Name | IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx |
|---|---|---|---|---|---|---|---|
| No LAN-to-LAN Sessions | | | | | | | |

**Remote Access Sessions**                        [ LAN-to-LAN Sessions | Management Sessions ]

| Username | Assigned IP Address Public IP Address | Group | Protocol Encryption | Login Time Duration | Client Type Version | Bytes Tx Bytes Rx |
|---|---|---|---|---|---|---|
| student1 | 10.0.1.70 192.168.1.6 | training | IPSec 3DES-168 | Jul 29 15:14:19 0:00:18 | WinNT 3.6 (Beta_2) | 37928 32304 |

**Management Sessions**                           [ LAN-to-LAN Sessions | Remote Access Sessions ]

| Administrator | IP Address | Protocol | Encryption | Login Time | Duration |
|---|---|---|---|---|---|
| admin | 10.0.1.70 | HTTP | None | Jul 29 14:14:33 | 0:00:05 |

© 2003, Cisco Systems, Inc. All rights reserved.                                      CSVPN 4.0—9-11

The Monitoring>Sessions window displays comprehensive data for currently active user and administrator sessions on the Concentrator. The following session information is available:

■ Refresh button—Click **Refresh** to update the window and its session information. The date and time indicate when the window was last updated.

■ Session Summary table—Shows summary totals for LAN-to-LAN, remote access, and management sessions.

■ LAN-to-LAN Sessions table—Shows parameters and statistics for all active IPSec LAN-to-LAN sessions. Each session identifies only the outer LAN-to-LAN connection or tunnel, not individual host-to-host sessions within the tunnel.

■ Remote Access Sessions table—Shows parameters and statistics for all active, remote-access sessions. Each session is a single-user connection from a remote client to the Concentrator.

■ Management Sessions table—Shows parameters and statistics for all active administrator management sessions on the Concentrator.

# Monitor Sessions—Protocols

Monitoring | Sessions | Protocols

Group  –All–

**Active Sessions:** 2
**Total Sessions:** 37

| Protocol | Sessions | | Percentage |
|---|---|---|---|
| Other | 0 | | 0.0% |
| PPTP | 0 | | 0.0% |
| L2TP | 0 | | 0.0% |
| IPSec | 1 | | 50.0% |
| HTTP | 1 | | 50.0% |
| FTP | 0 | | 0.0% |
| Telnet | 0 | | 0.0% |
| SNMP | 0 | | 0.0% |
| TFTP | 0 | | 0.0% |
| Console | 0 | | 0.0% |
| Debug/Telnet | 0 | | 0.0% |
| Debug/Console | 0 | | 0.0% |
| L2TP/IPSec | 0 | | 0.0% |
| IPSec/LAN-to-LAN | 0 | | 0.0% |
| IPSec/UDP | 0 | | 0.0% |
| SSH | 0 | | 0.0% |
| VCA/IPSec | 0 | | 0.0% |
| IPSec/TCP | 0 | | 0.0% |
| IPSec/NAT-T | 0 | | 0.0% |
| IPSec/LAN-to-LAN/NAT-T | 0 | | 0.0% |
| L2TP/IPSec/NAT-T | 0 | | 0.0% |

CSVPN 4.0—9-12

The Monitoring>Sessions>Protocols window displays the protocols used by the active user. The following information is available:

■ Refresh button—Click **Refresh** to update the window and its session information. The date and time indicate when the window was last updated.

■ Active Sessions—The number of currently active sessions.

■ Total Sessions—The total number of sessions since the Concentrator was last booted or reset.

■ Protocol column—The protocol that the session is using.

■ Sessions column—The number of active sessions using this protocol. The sum of this column equals the total number of active sessions listed in the top left part of the window.

■ Bar graph column—The percentage of sessions using this protocol, relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25 percent.

■ Percentage column—The percentage of sessions using this protocol relative to the total active sessions, as a number. The sum of this column equals 100%.

# Monitor Events

Configuration | System | Events

Save

This section of the Manager lets you configure how the VPN 3000 Concentrator Series handles events: alarms, traps, error conditions, status changes, etc.

In the left frame, or in the list of links below, click the option you want to configure:

- General -- general (default) event handling.
- FTP Backup -- FTP backup of event log files.
- Classes -- special handling of specific event classes.
- Trap Destinations -- SNMP trap message destinations.
- Syslog Servers -- UNIX syslog message servers.
- SMTP Servers -- SMTP servers for event notification.
- Email Recipients -- recipients for event notification via email.

CSVPN 4.0—9-13

The Configuration>System>Events window enables you to configure how the Concentrator handles events. Events provide information for system monitoring, auditing, management, accounting, and troubleshooting.

## Configure System Events



The Configuration>System>Events>General window enables you to configure the default, or general, handling of all events. These defaults apply to all event classes. The following options can be configured in this window:

■ Save Log on Wrap check box—Select this check box to automatically save the event log when it is full. (The check box is deselected by default.) The event log holds 2048 entries. When the log is full, the entries wrap; that is, entry 2049 overwrites entry 1, and so on.

■ Save Log Format drop-down menu—Click the drop-down menu button to choose the format of the saved log files.

■ FTP Saved Log on Wrap check box—Select this check box to automatically send the saved event log file, when it wraps, via FTP to a remote computer.

■ Email Source Address field—Enter the address to put in the **From:** field of an e-mailed event message.

■ Syslog Format drop-down menu—Click the drop-down menu button and choose the format for all events sent to UNIX Syslog servers.

■ Severity to Log drop-down menu—Click the drop-down menu to select the range of severity value to enter on the log. The default is 1–5, which means that all events of severity level 1 through severity level 5 are entered in the event log.

■ Severity to Console drop-down menu—Click the drop-down menu to select the range of severity value to display on the console. The default is 1–3, which means that all events of severity level 1 through severity level 3 are displayed on the console.

- Severity to Syslog drop-down menu—Click the drop-down menu button and choose the range of event severity levels to send to a Syslog server. By default, no events are sent.

- Severity to Email drop-down menu—Click the drop-down menu button and choose the range of event severity levels for e-mail to recipients.

- Severity to Trap drop-down menu—Click the drop-down menu button and choose the range of event severity levels to send to an SNMP network management system.

**Monitor Live Event Log**

Cisco.com

```
Monitoring | Live Event Log

110 02/08/2002 08:44:11.200 SEV=4 IKE/120 RPT=43 192.168.1.6
Group [service] User [student2]
PHASE 2 COMPLETED (msgid=482dc2ce)

111 02/08/2002 08:44:11.200 SEV=4 AUTOUPDATE/19 RPT=16
Sending IKE Notify: AutoUpdating clients in group [service]
Client delay: 0, instID: 000003FE

113 02/08/2002 08:44:11.270 SEV=4 IKE/49 RPT=44 192.168.1.6
Group [service] User [student2]
Security negotiation complete for User [student2]
Responder, Inbound SPI = 0x71b3406b, Outbound SPI = 0x085feef1

116 02/08/2002 08:44:11.270 SEV=4 IKE/120 RPT=44 192.168.1.6
Group [service] User [student2]
PHASE 2 COMPLETED (msgid=b525d793)

117 02/08/2002 08:45:31.130 SEV=5 AUTH/36 RPT=37
User [ admin ] Protocol [ HTTP ] attempted ADMIN logon..
Status: <ACCESS GRANTED> !

119 02/08/2002 08:45:31.130 SEV=4 AUTH/22 RPT=58
User admin connected

120 02/08/2002 08:45:31.130 SEV=4 HTTP/47 RPT=33 10.0.1.12
New administrator login: admin.
```

[ Pause Display ] [ Clear Display ] [ Restart ]  5

*Warning: This session will not time out.*

CSVPN 4.0—9-15

The Monitoring>Live Event Log window displays events in the current event log and automatically updates the display every five seconds. The events might take a few seconds to load when you first open the window. The window always displays the most recent event at the bottom. Use the scroll bar to view earlier events. To filter and display events by various criteria, choose the **Monitoring>Filterable Event Log** window. If you keep this Concentrator Manager window open, your administrative session does not time out. Each automatic window update resets the inactivity timer. The buttons at the bottom of the Live Event Log window are as follows:

■ Pause Display—To pause the display, click **Pause Display**. While paused, the window does not display new events, the button changes to Resume display, and the timer counts down to 0 and stops. You can still scroll through the event log.

■ Resume Display button—After you have clicked the Pause Display button, the button changes to Resume display, and the timer counts down to 0 and stops. Click **Resume** to resume the display of new events and restart the timer.

■ Clear Display button—To clear the event display, click **Clear Display**. This action does not clear the event log; it only clears the display of events on this window.

■ Restart button—To clear the event display and reload the entire event log in the display, click **Restart**. This action does not clear the event log; it only clears the display of events on this window.

■ Timer—The timer counts 5, 4, 3, 2, and 1 to show where it is in the 5-second refresh cycle. The Receiving message at the bottom of the Live Event Log window indicates receipt of new events. A steady 0 indicates the display has been paused.

The live event log requires Microsoft Internet Explorer release 4.0 or higher, or Netscape versions 4.5-4.7 or 6.0.

**Monitor Event Log**

Cisco.com

**Monitoring | Filterable Event Log**

Select Filter Options

Event Class: All Classes / AUTH / AUTHDBG / AUTHDECODE    Severities: ALL / 1 / 2 / 3

Client IP Address: 0.0.0.0    Events/Page: 100

Group: --All--    Direction: Oldest to Newest

[ |◄◄ ] [ ◄◄ ] [ ►► ] [ ►►| ] [ Get Log ] [ Save Log ] [ Clear Log ]

```
1 04/12/2001 13:35:05.820 SEV=3 AUTH/5 RPT=1 192.168.1.6
Authentication rejected: Reason = User was not found
handle = 1, server = Internal, user = student5, domain = <not specified>

3 04/12/2001 13:35:14.850 SEV=4 IKE/52 RPT=1 192.168.1.6
Group [training] User [student1]
User (student1) authenticated.

4 04/12/2001 13:35:15.870 SEV=4 AUTH/21 RPT=7
User student1 connected

5 04/12/2001 13:35:15.070 SEV=4 IKE/119 RPT=1 192.168.1.6
Group [training] User [student1]
PHASE 1 COMPLETED

6 04/12/2001 13:35:15.870 SEV=5 IKE/25 RPT=1 192.168.1.6
Group [training] User [student1]
Received remote Proxy Host data in ID Payload:
Address 10.0.1.30, Protocol 0, Port 0

9 04/12/2001 13:35:15.870 SEV=5 IKE/24 RPT=1 192.168.1.6
Group [training] User [student1]
Received local Proxy Host data in ID Payload:
Address 192.168.1.5, Protocol 0, Port 0
```

CSVPN 4.0—9-16

The Monitoring>Filterable Event Log window enables graphical user interface (GUI) access for viewing events in the current event log. The log holds up to 2048 events and wraps when full. The ability to manage the event log file is also provided. The administrator can select any or all of the following four options for filtering and displaying the event log:

■ Event Class drop-down menu—Click the drop-down menu button and choose the event class to display all the events in a single event class.

■ Severities drop-down menu—Click the drop-down menu button and choose the severity level to display all the events of a single severity level.

■ Client IP Address field—Displays all the events relating to a single IP address. The specific IP address is entered manually.

■ Events/Page drop-down menu—Click the drop-down menu button and select the number to display a given number of events per manager screen (page).

After selecting the options, click any one of the four Page buttons to retrieve events.

The event log can be retrieved from the Concentrator via the following:

■ Telnet

■ FTP

■ HTTP

## Configure Event Classes

Configuration | System | Events | Classes

Save Needed

This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Modify** or **Delete**.

Click here to configure general event parameters.

Configured
Event Classes   Actions

IKEDBG
MIB2TRAP

Add

Modify

Delete

   CSVPN 4.0—9-17

The Configuration>System>Events>Classes window enables you to add, configure, modify, and delete specific event classes for special handling. You can override the general or default handling of event classes. This is good for debugging special cases, such as problems with IPSec client-to-LAN handshaking because it allows you to look at all alarms, not just high-level alarms.

For example, a remote client is not able to connect to the Concentrator using digital certificates. The administrator looks at the filterable event log and notices that the remote client's digital certificate is invalid. With the event level set at the default of 1−5, the log tells the administrator there is a problem, but it does not give the administrator enough information. For that, the administrator needs information contained in event messages level 7−13, debug and engineering messages. With the IKEDECODE event modified to include levels 1−13, the administrator is able to look at the received digital certificate. From this information, the administrator ascertained that the remote client's digital certificate organizational unit OU field is set for Training while the Concentrator is expecting a value of training (lowercase "t"). The Configuration>System>Events>Classes window enables the administrator is set specific events at lower levels in order to aid in the troubleshooting of a problem. When the issue is resolved, the increased event level can be disabled and returned to the default level value of 1−5.

## Modify Classes



In the Configuration>System>Events>Classes>Add window, there are three things an administrator needs to do:

■ Select the event class to configure for special handling.

■ Enable or disable special handling of this event.

■ Select the range of severity levels.

The event class handling parameters are as follows:

■ Events to Log —Click the **Events to Log** drop-down menu button and choose the range of event severity levels to enter in the event log.

■ Events to Console—Click the **Events to Console** drop-down menu button and choose the range of event severity levels to display on the console.

■ Events to Syslog—Click the **Events to Syslog** drop-down menu button and choose the range of event severity levels to send to a Syslog server. The default is None. Using the default means that no events are sent to a Syslog server.

■ Events to Email—Click the **Events to Email** drop-down menu button and choose the range of event severity levels to send to recipients via e-mail. If you select any event severity levels to e-mail, you must also configure an Simple Mail Transfer Protocol (SMTP) server on the Configuration>System>Events>SMTP Servers window, and you must configure e-mail recipients on the Configuration>System>Events>E-mail Recipients window. You

should also configure the e-mail source address on the Configuration>System>Events>
General window.

■   Events to Trap—Click the **Events to Trap** drop-down menu button and choose the range of
    event severity levels to send to an SNMP network management system. If you select any
    event severity levels to send, you must also configure SNMP destination system parameters
    on the Configuration>System>Events>Trap Destinations window.

# Administration

This topic covers how to configure and perform basic administration on the Cisco VPN 3000 Series Concentrator.



## Administration Index

**Administration**

Save 🖫

This section of the Manager lets you control VPN 3000 Concentrator administrative functions.

In the left frame, or in the list of links below, click the function you want:

- Administer Sessions -- statistics and logout for all sessions.
- Software Update -- update concentrator and client software.
- System Reboot -- system reboot options.
- Reboot Status -- active sessions, disconnected sessions, etc.
- Ping -- use ICMP ping to determine connectivity.
- Monitoring Refresh -- enable automatic refresh of Monitoring screens.
- Access Rights -- configure administrator profiles, access, and sessions.
- File Management -- view, save, delete, swap, and transfer files.
- Certificate Management -- install and manage digital certificates.

CSVPN 4.0—9-20

The Administration window in the Manager enables you to control administrative functions on the Concentrator. The following functions are available:

- Administer Sessions—View statistics for logout, and ping sessions.

- Software Update—Upload and update the Concentrator software image, and upload and update the VPN Client software image.

- System Reboot—Set options for the Concentrator shutdown and reboot.

- Reboot Status—Display information about system reboots.

- Ping—Use ICMP ping to determine connectivity.

- Monitoring Refresh—Enable an automatic refresh of status and statistics in the monitoring section of the Manager.

- Access Rights—The Administrator can customize user profiles, access control lists (ACLs), and administration session parameters:

— ACL—Configure IP addresses for workstations with access rights.

— Administrators—Configure administrator usernames, passwords, and rights.

— Access settings—Set the administrative session idle timeout and limits.

■ File Management—Configuration, event log, and certificate request files are stored in Flash memory. File Management enables the administrator to manage these files in Flash memory:

— Files—Copy, view, and delete system files.

— Swap Configuration Files—Swap backup and boot configuration files.

— TFTP transfer—Transfer files to and from the Concentrator.

— File upload—Transfer files to the Concentrator.

■ Certificate Management—Install and manage digital certificates. The following Certificate Management submenu items are available:

— Enrollment—Create a certificate request to send to a Certificate Authority (CA).

— Installation—Install digital certificates.

— Certificates—View, modify, and delete digital certificates.

# Administrators

**Administration | Access Rights | Administrators**

This section presents administrator users. Any changes you make take effect immediately.

| Group Number | Username | Properties | Administrator | Enabled |
|---|---|---|---|---|
| 1 | admin | Modify | ⦿ | ☑ |
| 2 | config | Modify | ○ | ☐ |
| 3 | isp | Modify | ○ | ☐ |
| 4 | mis | Modify | ○ | ☐ |
| 5 | user | Modify | ○ | ☑ |

Apply    Cancel

Administrators are special users who can access and change the configuration, administration, and monitoring functions on the Concentrator. Only administrators can use the Concentrator Manager. Cisco provides five predefined administrators:

■ Admin—System administrator with access to, and the rights to change, all areas. This is the only administrator enabled by default (this is the only administrator who can log into, and use the Concentrator Manager as supplied by Cisco).

■ Config—Configuration administrator with all rights except SNMP access.

■ ISP—Internet Service Provider administrator with limited general configuration rights.

■ MIS—Management Information Systems administrator with the same rights as the configuration administrator.

■ User—Users have limited rights. They have view and read privileges only.

## Administration—Access Rights

Cisco.com

**Administration | Access Rights | Administrators | Modify Properties**

This section lets you modify the properties for administrators. Any changes you make take effect immediately.

Username [admin]
Password [******]     A password is required.
Verify [******]     The password must be verified.
**Access Rights**
Authentication [Modify Config ▾]
General [Modify Config ▾]
SNMP [Modify Config ▾]
Files [Read/Write Files ▾]  Includes Configuration Files
AAA Access
Level [0 ▾]     Select the Privilege Level for this administrator. An administrator logging in using
AAA will need to have a Privilege Level equal to one of the administrators.

[Apply]  [Default]  [Cancel]

CSVPN 4.0—9-22

The Administration>Access Rights window enables the administrator to configure access to and rights in the Concentrator Manager functional areas (Authentication or General), or via SNMP. Click the **Authentication**, **General**, and **SNMP** drop-down menus and choose from the following access rights:

- None—No access or rights.

- Stats Only—Access to only the Monitoring section of the Concentrator Manager. No rights to change parameters.

- View Config—Access to permitted functional areas of the Concentrator Manager, but no rights to change parameters.

- Modify Config—Access to permitted functional areas of the Concentrator Manager, and rights to change parameters.

Click the **Files** drop-down menu and choose from the following access rights:

- None—No file access or management rights.

- List Files—See a list of files in the Concentrator Flash memory.

- Read Files—Read (view) files in Flash memory.

- Read/Write Files—Read and write files in Flash memory, clear or save the event log, and save the active configuration to a file.

The Authentication, Authorization, and Accounting (AAA) Access Level drop-down menu enables you to govern the level of access for administrators authenticated by a Terminal Access Controller Access Control System (TACACS+) server. You set this AAA access level parameter to one of the levels configured on the TACACS+ server.

TACACS+ Authentication and
Authorization Process

Cisco.com

Username + password

Authentication
Pass or fail
Authorization
Privilege level 1

Modify configuration + read/write files
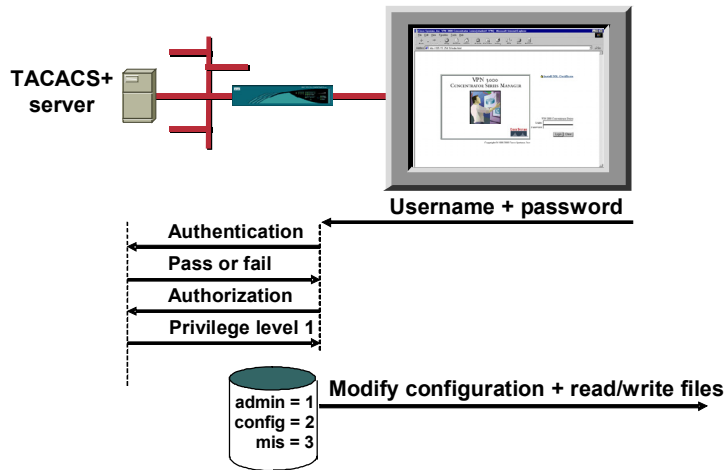
admin = 1
config = 2
mis = 3

CSVPN 4.0—9-23

In Release 3 and higher of the Concentrator, the Concentrator or a Terminal Access Controller
Access Control System (TACACS+) server can authenticate an administrator trying to access
the web interface of the Concentrator. In the example in the figure, a user tries to access the web
interface of the Concentrator. They are prompted for a username and password. With TACACS+
enabled, the Concentrator forwards the username and password to the TACACS+ server. The
server returns a pass or fail authentication message. If a pass message is returned, the
Concentrator requests a level of authorization. The server searches the database for the level
associated with that user, in this case a number 1. The server sends an authorization level of 1
back to the Concentrator. The Concentrator searches its access rights database to see which
group is assigned an AAA access level of 1. In this case, the admin group is configured as a 1.
The user is granted whatever access rights are defined under admin group.

| Note | If TACACS+ fails, the only way to get back in is via the console port using CLI. |
|------|----------------------------------------------------------------------------------|

## TACACS+ Server Configuration

Cisco.com

**Administration | Access Rights | AAA Servers | Authentication | Add**

Configure and add a TACACS+ administrator authentication server.

Authentication Server 10.0.1.10 — Enter IP address or hostname.

Server Port 0 — Enter the server TCP port number (0 for default).

Timeout 4 — Enter the timeout for this server (seconds).

Retries 2 — Enter the number of retries for this server.

Server Secret ****** — Enter the server secret.

Verify ****** — Re-enter the server secret.

[Add] [Cancel]

© 2003, Cisco Systems, Inc. All rights reserved.    CSVPN 4.0—9-24

The Administration>Access Rights>AAA Servers>Authentication window enables the administrator to add or modify TACACS+ servers:

■ Authentication Server field—Enter the IP address or hostname of the AAA authentication server.

■ Server Port field—Enter the TCP port number by which you access the server.

■ Timeout field—Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again.

■ Retries field—Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the Concentrator declares this server inoperative and uses the next TACACS+ authentication server in the list.

■ Server Secret field—Enter the TACACS+ server secret key (also called the shared secret) (for example, C8z077f).

■ Verify field—Re-enter the TACACS+ server secret key to verify it. The field shows only asterisks.

## AAA Servers

**Administration | Access Rights | AAA Servers | Authentication**

This section lets you configure parameters for TACACS+ administrator authentication servers.

Be sure that any servers you reference are properly configured.

Click the **Add** button to add a server, or select a server and click **Modify, Delete, Move,** or **Test**.

**Authentication Servers**          **Actions**

10.0.1.10

| Add |
| Modify |
| Delete |
| Move Up |
| Move Down |
| Test |

CSVPN 4.0—9-25

The Administration>Access Rights>AAA Servers>Authentication window displays the configured TACACS+ servers in priority order. It is very important that you test the communications between the Concentrator and the TACACS+ server. If you log out of the Concentrator and communications do not exist between the Concentrator and the TACACS+ server, you are locked out of the GUI. To test the communications, click **Test**.

## Test AAA Server Communications

Administration | Access Rights | AAA Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation to complete or timeout.**

User Name | student1

Password | ××××××××

OK    Cancel

Error

An error has occurred while attempting to perform the operation.

**Authentication Error: No active server found**

Retry the operation    or    Go to main menu

CSVPN 4.0—9-26
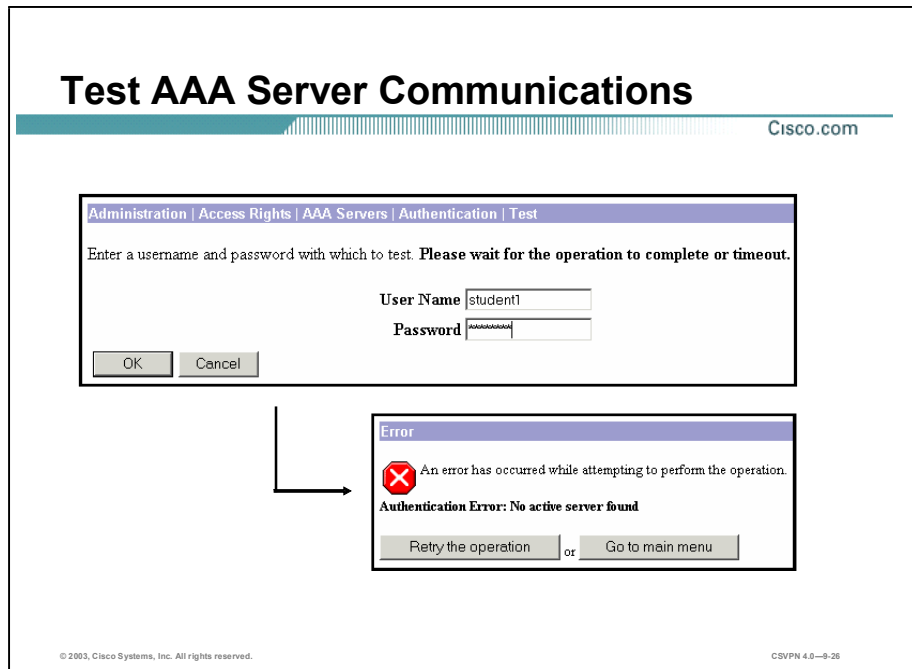
When the test window opens, enter your username and password. Click **OK**. After a short delay, the Concentrator returns an authenticated window. It is now safe to log out of the Concentrator and log back in using your TACAS+ login username and password. However, if the Authentication Error window opens, do not log out of the Concentrator. If you do, you are locked out of the GUI. The only way to access the GUI again is to fix the communication problem or turn off AAA in the Concentrator via the CLI.

## ACL

**Administration | Access Rights | Access Control List**

Save

This section presents administrator access control list options. Only those IP addresses listed will have access to manage this VPN 3000 Concentrator. If no addresses are listed, then anybody with the proper username/password combination can access this VPN 3000 Concentrator. If you do not add your IP address to the list first, you will be unable to access this VPN 3000 Concentrator.

**Manager Workstations**          **Actions**

— Empty —

Add

Modify

Delete

Move Up

Move Down

CSVPN 4.0—9-27

The Administration>Access Rights>Access Control List window enables you to configure the systems (workstations) that are allowed to access the Concentrator Manager. For example, you might want to allow access only from one or two PCs that are in a locked room. If no systems are listed, then anyone who knows the Concentrator IP address and the administrator username and password combination can gain access.

## ACL—Add

**Administration | Access Rights | Access Control List | Add**

Add a manager address to the access list.

IP Address [                    ]

IP Mask [255.255.255.255]    The mask specifies the part of the address to match. Use 255.255.255.255 to match the whole address. Use 0.0.0.0 to match any address.

Access Group
- ⦿ Group 1 (admin)
- ○ Group 2 (config)
- ○ Group 3 (isp)
- ○ Group 4 (mis)
- ○ Group 5 (student1)
- ○ No Access

[ Add ]  [ Cancel ]

CSVPN 4.0—9-28

The Administration>Access Rights>Access Control List>Add window enables you to add a PC to the ACL. Each PC requires an IP address and a subnet mask. To add a PC to the ACL, you must enter information in the following fields:

■ IP Address field—Enter the IP address of the workstation in dotted decimal notation (for example, 10.10.1.35).

■ IP Mask field—Enter the mask for the IP address in dotted decimal notation. This mask enables you to restrict access to a single IP address, a range of addresses, or all addresses. Enter **255.255.255.255** (the default) to restrict access to a single IP address. Enter **0.0.0.0** to allow all IP addresses. Enter the appropriate mask to allow a range of IP addresses.

Each individual PC is assigned to an access group or denied access. Click the appropriate radio button from the Access Group radio buttons to assign the rights of an administrator group to this IP address. The default is Group 1 (admin). You can assign only one group, or you can specify no access.

# Access Settings

**Administration | Access Rights | Access Settings**

This section presents General Access options.

**Session Idle Timeout** `600` (seconds) Enter the administrative session idle timeout. Limit is 1800 seconds.

**Session Limit** `10` Enter the maximum number of administrative sessions.

**Config File Encryption**
- ⦿ RC4
- ○ None    Select configuration file encryption.
- ○ DES

[ Apply ]   [ Cancel ]

CSVPN 4.0—9-29

The Administration>Access Rights>Access Settings window enables an administrator to customize the Concentrator web access sessions. The following access settings can be configured in the Access Settings window:

- Session Idle Timeout field—Enter the timeout period in seconds for administrative sessions. If there is no activity for this period, the Concentrator Manager session terminates. The default is 600 seconds, and there is no maximum limit.

- Session Limit field—Enter the maximum number of simultaneous administrative sessions allowed. The default is 10, and there is no limit.

- Config File Encryption radio button—To encrypt sensitive entries in the configuration file, such as passwords and keys, select either the **RC4** or **DES** radio button. Select the **None** radio button to use clear text for all configuration file entries. For maximum security, it is recommended that you do not use the None option.

# Administration Sessions

Cisco.com

**Administration | Administer Sessions** — Monday, 29 July 2002 14:20:30
Reset / Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name. To log out a session, click **Logout** in the table below. To test the network connection to a session, click **Ping**.

Group –All–
Logout All: PPTP User | L2TP User | IPSec User | IPSec LAN-to-LAN

**Session Summary**

| Active LAN-to-LAN Sessions | Active Remote Access Sessions | Active Management Sessions | Total Active Sessions | Peak Concurrent Sessions | Concurrent Sessions Limit | Total Cumulative Sessions |
| --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 1 | 2 | 4 | 100 | 37 |

**LAN-to-LAN Sessions** [ Remote Access Sessions | Management Sessions ]

| Connection Name | IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx | Actions |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | | | No LAN-to-LAN Sessions | | | | | |

**Remote Access Sessions** [ LAN-to-LAN Sessions | Management Sessions ]

| Username | Assigned IP Address / Public IP Address | Group | Protocol / Encryption | Login Time / Duration | Client Type / Version | Bytes Tx / Bytes Rx | Actions |
| --- | --- | --- | --- | --- | --- | --- | --- |
| student1 | 10.0.1.70 / 192.168.1.6 | training | IPSec / 3DES-168 | Jul 29 15:14:19 / 0:06:11 | WinNT / 3.6 (Beta_2) | 238736 / 177752 | [ Logout | Ping ] |

**Management Sessions** [ LAN-to-LAN Sessions | Remote Access Sessions ]

| Administrator | IP Address | Protocol | Encryption | Login Time | Duration | Actions |
| --- | --- | --- | --- | --- | --- | --- |
| admin | 10.0.1.70 | HTTP | None | Jul 29 14:14:33 | 0:05:57 | [ Logout | Ping ] |

CSVPN 4.0—9-30

The Administration>Administer Sessions window provides the following information:

- Session Summary table—Shows the summary totals for LAN-to-LAN, remote access, and management sessions.

- LAN-to-LAN Sessions table—Shows parameters and statistics for all active IPSec LAN-to-LAN sessions. Each session in this table identifies only the outer LAN-to-LAN connection or tunnel, not individual host-to-host sessions within the tunnel.

- Remote Access Sessions table—Shows parameters and statistics for all active remote-access sessions. Each session is a single-user connection from a remote client to the Concentrator.

- Management Sessions table—Shows parameters and statistics for all active administrator management sessions on the Concentrator. If there are multiple concurrent management sessions running, the first session has read and write capabilities. Each additional management session has read capabilities only. The additional users can view configuration screens but are unable to affect any changes.

## File Management—Files

| | |
|---|---|
| **Administration | File Management** | **Tuesday, 05 February 2002 09:21:37** |
| | Refresh |

This screen lets you manage files on the VPN 3000 Concentrator. Select a file from the list and click the appropriate **Action**, or choose an action from the list below.

- Swap Config File -- swap the backup and boot configuration files.
- TFTP Transfer -- transfer files via TFTP.
- File Upload -- send a file via HTTP.
- XML Export -- export the configuration to an XML file.

Total: 12368KB, Used: 322KB, Free: 12046KB

| Filename | Size (bytes) | Date/Time | Actions |
|---|---|---|---|
| CL2LBOS | 34577 | 10/25/2001 11:32:12 | [ View | Delete | Copy ] |
| CONFIG.BAK | 21444 | 01/23/2002 14:15:00 | [ View | Delete | Copy ] |
| CONFIG | 21676 | 01/25/2002 08:08:48 | [ View | Delete | Copy ] |
| CRSHDUMP.TXT | 19223 | 12/07/2000 12:11:00 | [ View | Delete | Copy ] |
| SAVELOG.TXT | 155304 | 01/23/2002 13:58:54 | [ View | Delete | Copy ] |

CSVPN 4.0—9-31

The Administration>File Management window enables you to manage files in the Concentrator Flash memory. From the top section of the window, management actions available to the administrator are as follows:

- Swap Config File link—Enables you to swap the backup and boot configuration files.

- TFTP Transfer link—Enables you to transfer files to and from the Concentrator via Trivial File Transport Protocol (TFTP).

- File Upload link—Enables you to use HTTP to transfer files from your PC to the Concentrator Flash memory.

- XML Export link—Exports the configuration to an XML file stored on the Concentrator.

The bottom of the window shows a table listing all files in the Flash memory—one file per table row. Such files include CONFIG, CONFIG.BAK, SAVELOG.TXT, and CRSHDUMP.TXT, and copies of the files that you have saved under different names such as CL2LBOS. The following file information is available:

- Filename column—The name of the file in Flash memory. The Concentrator stores filenames as uppercase names in the ≤8.3 naming convention.

- Size (bytes) column—The size of the file in bytes.

- Date/Time column—The date and time the file was created. The format is MM/DD/YY HH:MM:SS, with time in 24-hour notation.

■ Actions column—For a selected file, click the desired action link. The actions available to you depend on your access rights to files:

　— View—Click **View** to view the selected file. The Manager opens a new browser window to display the file.

　— Delete—Click **Delete** to delete the selected file from Flash memory.

　— Copy—Click **Copy** to copy a selected file within Flash memory.

## Swap Configuration

Save the configuration → Configuration (boot) → Config.bak (backup)

Swap the configuration
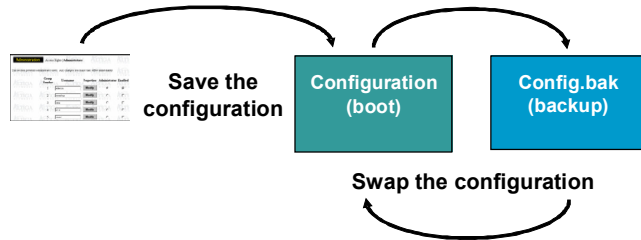
**Administration | File Management | Swap Configuration Files**

Every time the active configuration is saved, a backup is made of the configuration file. By clicking OK, you can swap the backup configuration file with the boot configuration. To reload the boot configuration, you must then reboot the device. **You will be sent to the System Reboot screen after the configuration files have been swapped.**

[ OK ] [ Cancel ]

The Administration>File Management>Swap Configuration Files window enables you to swap the boot configuration file with the backup configuration file. Every time you save the active configuration, the system writes it to the configuration file, which is the boot configuration file. It also saves the previous configuration file as config.bak, the backup configuration file. You must reboot the system to reload the boot configuration file and make it the active configuration. Click the highlighted **reboot the device** link to choose the **Administration>System Reboot** window and reboot the system.

## Reboot



**Administration | System Reboot**

This section presents reboot options.

⚠ If you reboot, the browser may appear to hang as the device is rebooted.

**Action**
- Reboot
- Shutdown without automatic reboot
- Cancel a scheduled reboot/shutdown

**Configuration**
- Save the active configuration at time of reboot
- Reboot without saving the active configuration
- Reboot ignoring the configuration file

**When to Reboot/Shutdown**
- Now
- Delayed by 10 minutes
- At time 15:04 (24 hour clock)
- Wait for sessions to terminate (don't allow new sessions)

Apply | Cancel

CSVPN 4.0—9-33

The Administration>System Reboot window enables you to reboot or shut down (halt) the Concentrator with the various options listed below:

| Note | If you are logged in to the Manager when the system reboots or halts, it automatically logs you out and displays the main login window. |
|------|---|

- Reboot radio button—Terminates all sessions, resets the hardware, loads and verifies the software image, executes system diagnostics, and initializes the system. A reboot takes approximately 60–75 seconds.

- Shutdown without automatic reboot radio button—Shuts down the Concentrator; that is, it brings the system to a halt so you can turn off the power. Shutdown terminates all sessions and prevents new user sessions (but not administrator sessions).

- Cancel a scheduled reboot/shutdown radio button—Cancels a reboot or shutdown that is waiting for a certain time, or for sessions to terminate.

- Save the active configuration at time of reboot radio button—Saves the active configuration to the configuration file, and reboots using that new file.

- Reboot ignoring the configuration file radio button—Reboots ignoring the existing configuration file and without saving the active configuration. It sets the Concentrator back to factory defaults (that is, it starts the system as if it had no configuration file).

## Software Update

**Concentrator**                    **Hardware client**
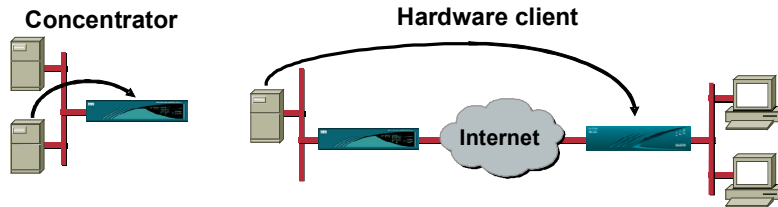
**Internet**

**Administration | Software Update**

This section of the Manager lets you update software on the **VPN 3000 Concentrator Series** or clients.

In the left frame, or in the list of links below, click the function you want:

- Concentrator -- update **VPN 3000 Concentrator Series** software.
- Clients -- update hardware and software clients.

CSVPN 4.0—9-34

The Administration>Software Update window enables you to update executable system software on both the Concentrator and Cisco VPN clients. Select the Concentrator that you want to update the Concentrator software. Choose **Clients** to update the hardware and Windows software client. Client software update is discussed later in this lesson.

**Concentrator—Software Update**

Cisco.com

① Software update

Online image → New image

② Reboot

**Administration | Software Update | Concentrator**

This section lets you update the software on your VPN 3000 Concentrator. The VPN 3000 Concentrator will verify the integrity of the software image that you download. It will take a few minutes for the upload and verification to take place. **Please wait for the operation to finish.**

**Current Software Revision:**
Cisco Systems, Inc./VPN 3000 Concentrator Version 3.6.Beta_2 Jun 26 2002 13:32:36 (DEBUG_MASK 0, NDEBUG off)

Type in the name of the image file below. The current image file is **vpn3000d-3.6.Beta_2-k9.bin**.

[ C:\rel 3_6 sw\vpn3005-3_6_Rel-k9.bin ]  [ Browse... ]

[ Upload ]  [ Cancel ]

CSVPN 4.0—9-35

The Administrator>Software Update>Concentrator window enables you to update the Concentrator executable system software (the software image). The new image file must be accessible by the workstation you are using to manage the Concentrator. This process uploads the file to the Concentrator, which then verifies the integrity of the file. It takes a few minutes to upload and verify the software, and the system displays the progress. Wait for the operation to finish.

You must reboot the Concentrator to run the new software image. The system prompts you to reboot when the update is finished.

---

| **Caution** | While the system is updating the image, do not perform any other operations that affect Flash memory (listing, viewing, copying, deleting, or writing files). Doing so may corrupt memory. |

---

**Client—Software Update**

CISCO.COM

Update notification

Internet

Training group

Engineering group
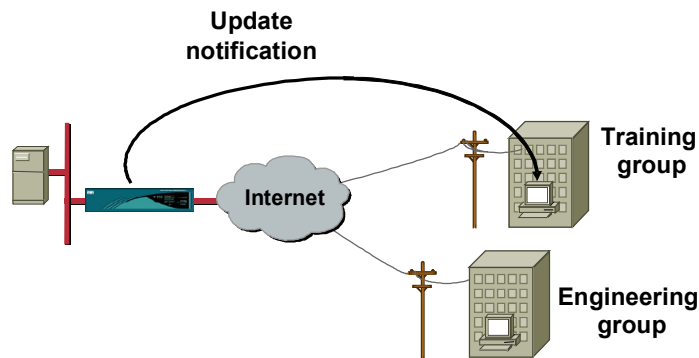
CSVPN 4.0—9-36

Network administrators of remote access VPNs are looking for Cisco to help them push client software upgrades to their users in some type of automated, informed fashion. To that end, the Concentrator has provided a client update notification feature to notify the software client when update software is available.

Updating client software in an environment with a large number of devices in different locations can be a formidable task. For this reason, the Concentrator includes a client update feature that simplifies the software update process. This feature works differently for Cisco VPN Software Clients and Cisco VPN 3002 Hardware Clients. The Hardware Client and Software Client update processes are as follows:

■ Software Clients—The client update feature enables administrators at a central location automatically notify Software Client users when it is time to update the Software Client. When you enable Client Update, during tunnel establishment the central-site Concentrator sends an IKE packet that notifies Cisco VPN Clients about acceptable versions of Software Client. It includes a location that contains the new version of software for the Cisco VPN Client to download. The administrator for that Software Client can then retrieve the new software version, and update the client at a time of their choosing.

■ Hardware Clients—When you enable Client Update for the Hardware Client, during tunnel establishment the central-site Concentrator sends an IKE packet that notifies Hardware Clients about acceptable versions of executable system software and their locations. If the Hardware Client is not running an acceptable version, it automatically attempts to download the new revision of code via TFTP. There will be further discussion of the Hardware Client update in a later lesson.

Windows Client—Enable Update Process

Configuration | System | Client Update

This section of the Manager lets you configure Client Update.

In the left frame, or in the list of links below, click the function you want:

- Enable -- enable Client Update.
- Entries -- configure the client type and URL entries for Client Update.

Configuration | System | Client Update | Enable

Check the box to enable Client Update functionality.

Enabled ☑

[Apply] [Cancel]

Configuring the VPN Windows Software client auto update is a two-step process:

**Step 1** Enable client update functionality (disabled by default) on the Concentrator.

1. Choose the **Configuration>System>Client Update** window and click the Enable link.

2. When enabled, the administrator has to decide how to update the clients: globally or by group.

- With a global update, all clients are updated to specific releases of software from a specific server. Choose the **Configuration>System>Client Update>Entries** window and enter the appropriate information to configure a global update.

- If a more systematic, group-by-group approach is preferred, different servers can update different groups at different times to different releases of software. Choose the **Configuration>User Management>Groups** window and enter the appropriate information to configure a group update.

**Step 2** Set the update parameters (for example, client type, URL, and Revisions).

**Windows Client—Global Update Process**

© 2003, Cisco Systems, Inc. All rights reserved.                                    CSVPN 4.0—9-38
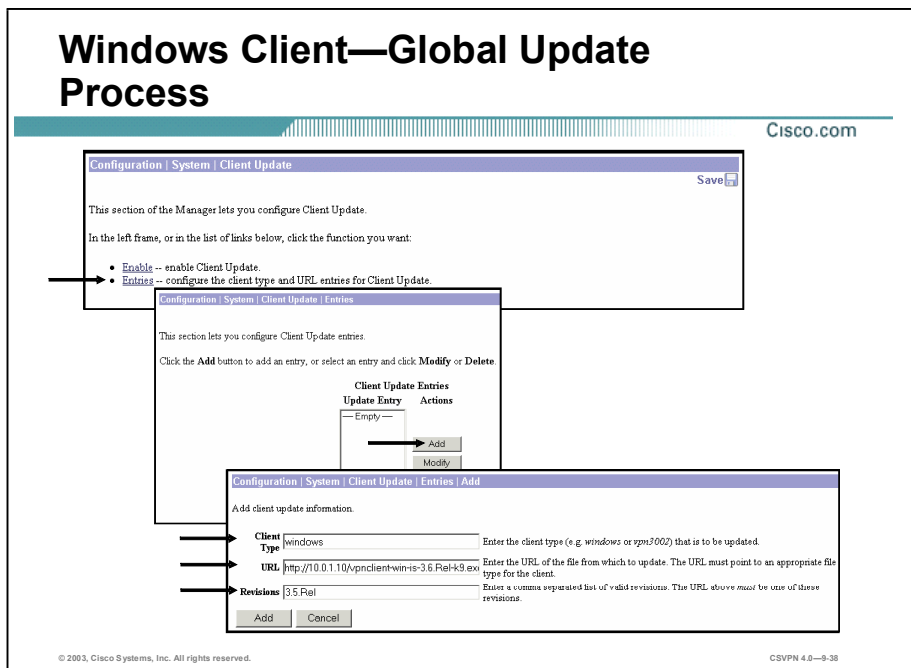
Global software update configuration is defined under the Configuration>System>Client Update tree. Complete the following steps to configure the VPN Windows Software Client update:

**Step 1**  Choose the **Configuration>System>Client Update** window and click the **Entries** link.

**Step 2**  From the Configuration>System>Client Update>Entries window, click **Add** to access the update information window.

**Step 3**  In the Configuration>System>Client Update>Entries>Add window, enter the client update information. The client update fields are as follows:

■ Client Type—The VPN Client identifiers are as follows:

— Windows—All Microsoft Windows-based platforms (95, 98, ME, NT 4.0, 2000, and XP). The following are the Microsoft Windows subset identifiers:

■ Windows 9X—All Microsoft Windows 9X-based platforms (95, 98, and ME)

■ Windows NT—All Microsoft Windows NT-based platforms (NT 4.0, 2000, and XP)

■ URL—Enter the URL for the software image. For the VPN Client to activate the Launch button on the VPN Client notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format is http(s)://*server_address:port* /*directory* /*filename* (for example, http://10.0.1.10/ clientupdate). All parts of the URL are optional except for the protocol (HTTP or HTTPS), and the server address.

■ Revisions—Enter a comma-separated list of software or firmware images appropriate for this client. Your entries must match exactly those on the VPN Windows Software Client, or the Hardware Client. For example, if the administrator wants all the clients to be upgraded to the released software version for 3.5, enter **3.5.Rel** in the revision field. For the exact spelling, open the Monitoring>System Status window. If the client is already running a software version on the list, it does not need a software update. If the client is not running a software version on the list, an update is in order. To do this, a VPN Windows Software Client user must download an appropriate software version from the URL listed in the notification message. The URL is defined in the previous URL field.
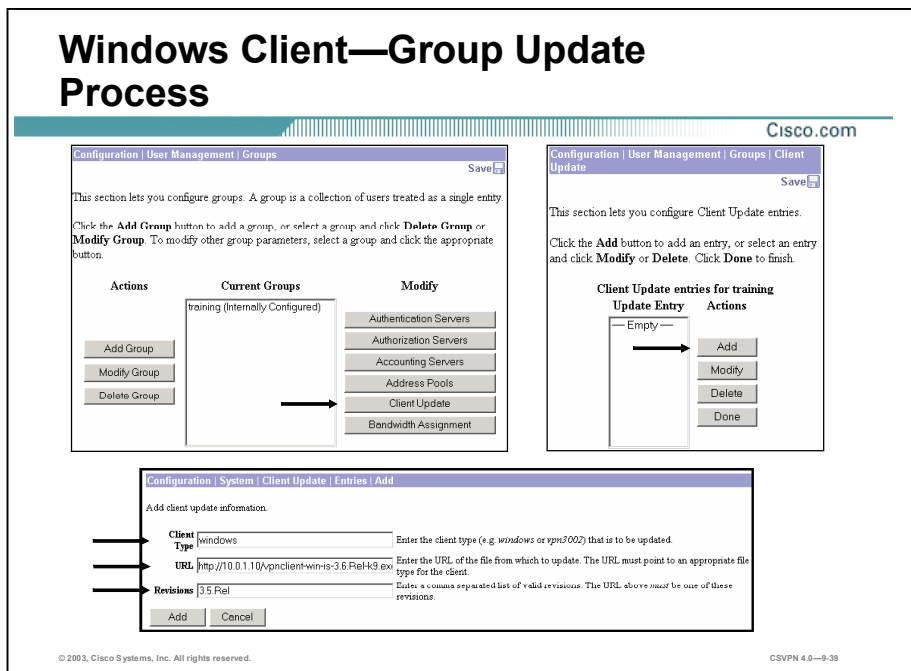
Complete the following steps to configure an update on a group-by-group basis:

**Step 1**   Choose the **Configuration>User Management>Groups** window.

**Step 2**   Select the group in the Current Groups field.

**Step 3**   Click **Client Update**.

**Step 4**   In the Configuration>User Management>Groups>Client Update>Add window, enter the client update information. The group client update fields are as follows:

■   Client Type—The VPN Windows Software Client identifiers are as follows:

— Windows—All Microsoft Windows-based platforms (95, 98, ME, NT 4.0, 2000, and XP). The following are the Microsoft Windows subset identifiers:

— Windows 9X—All Microsoft Windows 9X-based platforms (95, 98, and ME)

— Windows NT—All Microsoft Windows NT-based platforms (NT 4.0, 2000, and XP)

■   URL—Enter the URL for the software image. For the VPN Client to activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format is http(s)://*server_address:port*/*directory* /*filename* (for example, http://10.0.1.10/ clientupdate). All parts of the URL are optional except the protocol (HTTP or HTTPS) and the server address.

■   Revisions—Enter a comma-separated list of software or firmware images appropriate for this client. Your entries must match exactly those on the VPN Windows Software Client or the Hardware Client. For example, if the administrator wants all the clients to be upgraded to

the released software version for 3.5, enter **3.5.Rel** in the revision field. For the exact spelling, open the Monitoring>System Status window. If the client is already running a software version on the list, it does not need a software update. If the client is not running a software version on the list, an update is in order. To perform the update, a VPN client user must download an appropriate software version from the URL listed in the notification message. The URL is defined in the previous URL parameter field.

## Update Notification Message
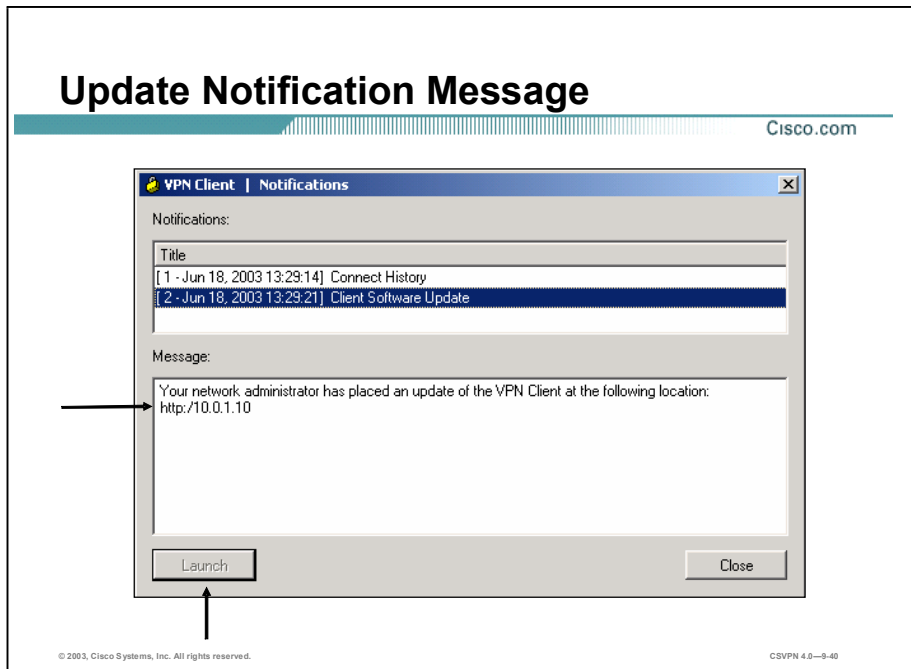
The notification message informs a remote user that it is time to upgrade the VPN Client software. The notification includes the location where the remote user can obtain the upgrade. When you receive an upgrade notification that includes a URL, click **Launch** to choose the site and retrieve the upgrade software. You will receive an upgrade notification every time you connect until you have installed the upgrade software.

# Client Statistics—Notification Button

Cisco.com

**VPN Client - Version 4.0.1 (Rel)**

Connection Entries  Status  Certificates  Log  Options  Help

Statistics...
Notifications...
Reset Stats

Disconnect        Modify        Delete

CISCO SYSTEMS

Connection Entries

| Connection Entry | Host | Transport |
|---|---|---|
| scep1 | 192.168.1.5 | IPSec/UDP |
| **student1** | **192.168.1.5** | **IPSec/UDP** |

Connected to "student1".        Connected Time: 0 day(s), 00:02.07

CSVPN 4.0—9-41
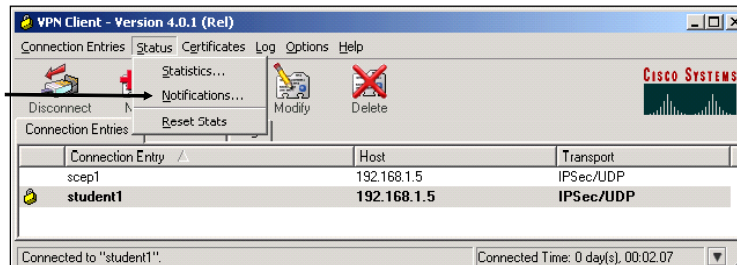
While connected, you can view the notification message by clicking **Notifications** on the VPN Client Status menu.

# Bandwidth Management
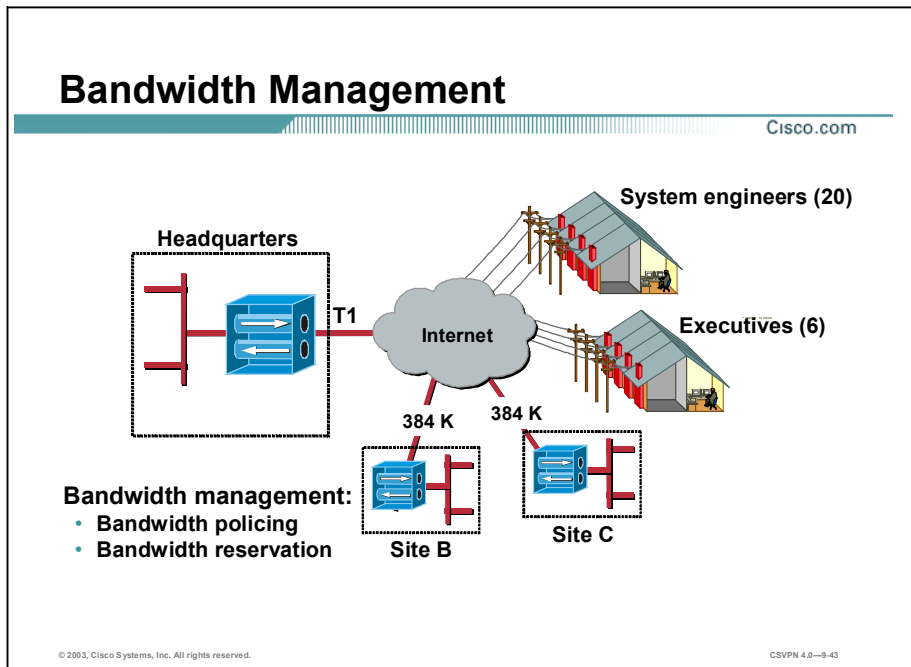


By default, the Concentrator line does not equitably manage packet traffic on a per-group or per-user basis. This means that any one group or user, given infinite bandwidth capability, could effectively steal almost all available bandwidth capacity of a Concentrator. This can cause all other logged in users to experience slower connections. In the figure, the customer has a T1, 1.544 Mbps, of bandwidth at the central site. There are two remote sites, site B and C, with 384 K of bandwidth respectively. There are two sets of remote users, system engineers and executives. The remote users have DSL and Cable access to headquarters. If all 26 remote users connect at the same time and decide to download a large file, their actions could conceivably slow down connections between the headquarters and site B and C.

The bandwidth management feature could be enabled on the Concentrator to distribute the bandwidth more equitably. One option is bandwidth reservation. The administrator could configure a minimum reserved bandwidth rate per session to prevent connection slow down. For example, each remotely connected system engineer has a configured minimum bandwidth reservation of 56 Kbps. For another option, if the administrator is concerned about over utilization, the Concentrator could be configured for bandwidth policing. The Concentrator can place a bandwidth ceiling on data transfers (for example, a maximum transfer rate of 128 Kbps per session). The last option is aggregation. The administrator could choose to reserve a pool of bandwidth, an aggregation, for a group of users, or a site-to-site link. During peak periods, this site-to-site link, or group of users, can access bandwidth from this dedicated pool of bandwidth. The pool is reserved for their exclusive use. There is further discussion of these bandwidth management options later in this lesson.

## Bandwidth Policing Overview

Cisco.com

Headquarters

System engineers

T1

Internet

Frames

Policing rate

Frames

Within burst size

Exceed policing rate

**Bandwidth policing:**
- **Policing rate**
- **Burst size**

Exceed burst size

CSVPN 4.0—9-44
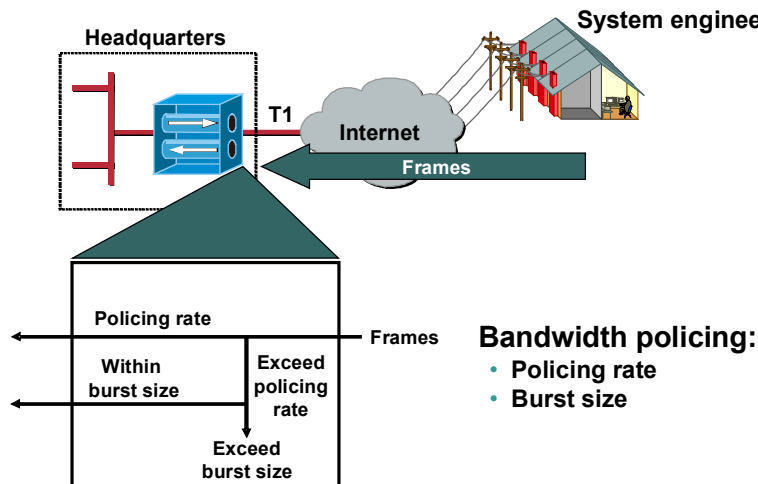
For the bandwidth policing feature, the Concentrator provides a maximum data transfer rate. Bandwidth policing sets a maximum limit, a cap, on the rate of tunneled traffic. For example, all system engineers can transfer data up to a sustained rate of 56 Kbps while remotely accessing the Concentrator. The Concentrator transmits traffic it receives below this rate; it drops traffic above this rate. Because traffic is bursty, some flexibility is built into policing. Policing involves two thresholds: the policing rate and the burst size. The policing rate is the maximum limit on the rate of sustained tunneled traffic. The burst size indicates the maximum size of an instantaneous burst of bytes allowed before traffic is capped back to the policing rate. The Concentrator allows for instantaneous bursts of traffic greater than the policing rate up to the burst rate. But should traffic burst consistently and exceed the burst rate, the Concentrator enforces the policing rate threshold. The Concentrator starts to drop frames.

Bandwidth policing is configurable on both a system and group basis. If group policing is configured, every member of the specified group can transmit data according to the group bandwidth policing policy. If a remote user is not a member of a predefined group, the remote user can transmit data up to the system-wide policing rate. For example, there are two groups of remote users, system engineers and executives. The executives have a group policing rate defined at 128 Kbps. The system engineers do not have their own group policing rate defined. When executives connect to the Concentrator, they can transmit data up to 128 Kbps. When system engineers connect, they do not have a policing policy specifically defined for their group. They can transmit data up to the system wide policing rate, or in this example, 56 Kbps.

**Bandwidth Policing Policies**

Cisco.com

Configuring the bandwidth policing feature is a two-step process. First, the policing policy, or policies, is defined. Next, the policies are assigned to an interface, and optionally to groups. To configure policing policies, choose the **Configuration>Policy Management>Traffic Management>Bandwidth Policies** window. The bandwidth policy consists of two parts, bandwidth reservation on the top half, and policing on the bottom half. (Bandwidth reservation will be discussed later in the lesson.) Policing involves two thresholds: the policing rate and the burst size. The policing rate is the maximum limit on the rate of sustained tunneled traffic. The burst size indicates the maximum size of an instantaneous burst of bytes allowed before traffic is capped back to the policing rate. The Concentrator allows for instantaneous bursts of traffic greater than the policing rate up to the burst rate. The policing policy parameters are as follows:

■ Policy Name—Enter a unique policy name that helps you remember the policy you are configuring. For example, if this policy focuses on the executive group, you could name it executive.

■ Policing—Select the **Enable Policing** check box to enable the policing feature.

■ Policing Rate—Enter a value for Policing Rate and select the unit of measurement. The Concentrator transmits traffic that is moving below the policing rate and drops all traffic that is moving above the policing rate. The range is between 56 Kbps and 100 Mbps. The default is 56K (bps). Policing rate is defined in units as follows:

— bps—Bits per second

— Kbps—Thousands of bits per second

— Mbps—Millions of bits per second

- Normal Burst Size—Enter a value for the normal burst size. The normal burst size is the amount of instantaneous burst that the Concentrator can send at any given time. Use the following formula to set the burst size: (Policing Rate/8) * 1.5. For example, if you want to limit users to 250 Kbps of bandwidth, set the police rate to 250 Kbps and set the burst size to 46875, that is: (250000 bps/8) * 1.5. Enter the Normal Burst Size and select the unit of measurement. The default is a normal burst size of 10500 bytes. Normal burst size is defined in units as follows:

  - Bytes—Unit of adjacent bits

  - Kbytes—Thousands of bytes

  - Mbytes—Millions of bytes

  For example, a policy named normal policy is configured for a policing rate of 56 Kbps and a normal burst size of 10500 bytes. Any remote user assigned this policy has a maximum limit on the rate of sustained tunneled traffic of 56 Kbps. The Concentrator can support an instantaneous burst of 10500 bytes before it starts to limit traffic by dropping packets.

**Bandwidth Policing Configuration**

Bandwidth policing policies:
- **Normal – 56 Kbps**
- **Executive – 128 Kbps**
- **LAN-to-LAN – 384 Kbps**

CSVPN 4.0—9-46

In a Concentrator, there may be multiple policies defined. In this example, the administrator defined the three policing rates, normal, executive, and LAN-to-LAN. A normal policy assigns a baseline bandwidth allocation while the executive policy allocates higher thresholds for the policing rate and burst size. The LAN-to-LAN policing policy applies to site-to-site tunnels. Normal policing policy users are allocated a maximum of 56Kbps of bandwidth with a normal burst size of 10500 bytes. This could be the default bandwidth reservation policy for the Concentrator. The executive policing policy users are allotted a maximum of 128 Kbps of bandwidth with a normal burst size of 24 Kbps. This is a custom policy for remote users who need more bandwidth than the reserve bandwidth provided by the normal, default, policy. The LAN-to-LAN policing policy allocates a maximum of 384 Kbps of bandwidth with a normal burst size of 72 Kbps for a site-to-site tunnel. The administrator can assign a bandwidth threshold of 384Kbps to site-to-site tunnels.

**Interface Policing Configuration**

Once policies are defined, they are assigned to a Concentrator interface, public or private, or a user group. The interface policy defines the default-policing rate for the Concentrator. If a remote user belongs to a group that is not specifically defined a policing rate, the remote user is assigned the policing rate defined for the interface. Choose the **Configuration>Interfaces> Ethernet2>Bandwidth Parameters** window to assign a policing policy to the interface. In the Configuration>Interfaces>Ethernet2>Bandwidth Parameters Tab window, enable bandwidth management on the selected interface, define the link rate for the interface, and assign the policy to be used on the interface. The interface bandwidth management parameters are as follows:

■ Bandwidth Management—Select the Bandwidth Management check box to enable bandwidth management on this interface.

■ Link Rate—Enter a value for the link rate, and select a unit of measurement. The defined link rate must be based on the available Internet bandwidth and not the physical LAN connection rate. The default is 1.544 Mbps. If the link rate is less than the sum of the policed rates, it is possible that some remote users will never reach the police rate.

■ Bandwidth Policy—Select a policy from the drop-down list. If there are no policies in this list, you must choose **Configuration>Policy Management>Traffic Management> Bandwidth Policies** window and define one or more policies.

| Note | If bandwidth policing is required in a network, a policing policy must be defined and applied to an interface before applying group policing policies. The Concentrator will not allow a group policy to be applied first. If an administrator attempts to apply a group policy first, the Concentrator will return an error message. |
|------|---|

In this example, the Internet link is a T1, 1.544 Mbps. The default policy for the interface is normal reservation. The normal reservation provides a maximum bandwidth allocation of 56 Kbps and a burst size of 10500 bytes. System engineers are assigned a policing rate of 56 Kbps.

**Group Policing Configuration**

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.                    CSVPN 4.0—9-48
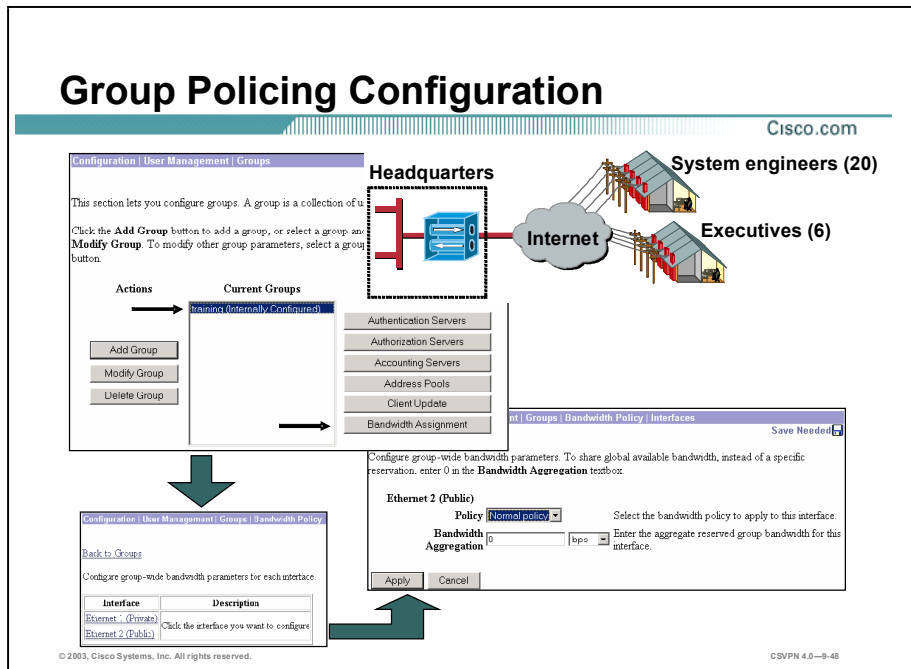
Choose the **Configuration>User Management Groups** window, select a group and select the Assign Bandwidth Policy to assign a policing policy to a group of remote users. From the Configuration>User Management>Bandwidth Policy> Interfaces window, configure the following group bandwidth policy parameters:

■ Policy—Select a policy from the Policy drop-down menu for the group. If you do not want to select a policy here, select none.

■ Bandwidth Aggregation—Enter a value for the aggregate group bandwidth to reserve for this group and select a unit of measurement. This parameter is discussed later in this lesson.

If the administrator assigns a policing policy to a group, remote users who belong to this group participate in the policing policy applied to the group. If you do not configure a bandwidth-policing policy for a group and bandwidth management is enabled on the interface, remote users participate in the policy applied to the interface, which is the default policy for the Concentrator as a whole.

In the figure, there is a multigroup remote access scenario, system engineers and executives. The administrator assigns different policing policies to each group. The executives group is assigned the executive policing policy. The system engineers are not assigned a group policing policy. As remote access executives connect to the Concentrator, they are assigned the group policing rate of 128 Kbps and a burst size of 24 Kbps. No policing policy is assigned to the system engineers group. As remote system engineers connect, they participate in the default policy for the interface, 56 Kbps policing rate and a burst size of 10500 bps.

**Bandwidth Management—Bandwidth Reservation**
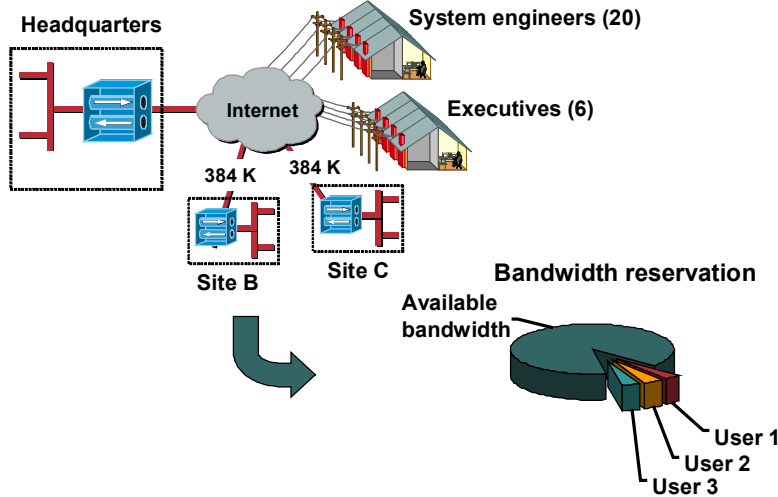
Bandwidth reservation reserves a minimum amount of bandwidth per session for tunneled traffic. As they connect to the Concentrator, each remote user receives a minimum amount of bandwidth. When there is little traffic on the box, users receive more than their allocated minimum of bandwidth. When the box becomes busy, they receive at least the minimum amount. When the combined total of the reserved bandwidth amounts of all active tunnels on an interface approaches the limit of the total bandwidth available on that interface, the Concentrator refuses further connections to users who demand more reserved bandwidth than is available.

Suppose the link rate on your public interface is 1.544 Mbps. And suppose you apply a reserved bandwidth policy to that interface that sets the reserved bandwidth to 64 Kbps per user. With this link rate and policy setting, only a total of 24 concurrent users can connect to the Concentrator at one time. (1.544 Mbps per interface divided by 64 Kbps per user equals 24 connections.)

■ The first user who logs on to the Concentrator reserves 64 Kbps of bandwidth plus the remainder of the bandwidth (1,480 Kbps).

■ The second user who logs on to the Concentrator reserves 64 Kbps of bandwidth and shares the remainder of the bandwidth (1,416 Kbps) with the first user.

■ When the twenty-fourth concurrent user connects, all users are limited to their minimum of 64 Kbps of bandwidth per connection.

■ When the twenty-fifth user attempts to connect, the Concentrator refuses the connection. It does not allow any additional connections since it cannot supply the minimum 64 Kbps reservation of bandwidth to more users.

One can think of bandwidth reservation as pieces of a pie. Each remote user is assigned a slice of pie, reserve bandwidth. As tunnels are established, each user is assigned a slice of the pie until the pie is completely divided. At that point, any new connections requesting a slice of the pie are refused the opportunity to establish a connection.

**Bandwidth Reservation Policy Configuration—System Wide**

Configuring bandwidth reservation is a two-step process. First, the bandwidth reservation policies are defined. Next, the policies are assigned to an interface, a LAN-to-LAN connection, and optionally to groups. Choose the **Configuration>Policy Management>Traffic Management>Bandwidth Policies** window to configure bandwidth reservation policies. The bandwidth policy window consists of two parts, bandwidth reservation on the top half, and policing on the bottom half. Under bandwidth reservation, the administrator is setting the minimum bandwidth assigned per session for remote users. The bandwidth reservation parameters are as follows:

- Policy Name—Enter a policy name.

- Bandwidth Reservation—Select the **Bandwidth Reservation** check box to enable the feature.

- Minimum Bandwidth—Enter the amount of bandwidth reserved per user during periods of congestion. Enter a value for the minimum bandwidth and select one of the following units of measure:

    — Bps—Bits per second

    — Kbps—Thousands of bits per second

    — Mbps—Millions of bits per second

In this example, the administrator created a policy called normal reservation. This reservation allocates a minimum of 64 Kbps to each remote access session.

**Bandwidth Reservation Policy Configuration—Group**

Not all remote users have the same bandwidth requirements. The administrator can configure additional policies with different bandwidth reservations. In the figure, the administrator created a policy for the executive group. Each member of the executive group requires more bandwidth than the minimum allocation of 64 Kbps. A policy was defined which allocates 128 Kbps of bandwidth upon connection to the Concentrator.

In the figure, as each executive connects, they are allocated part of the available bandwidth. The amount of bandwidth allocated to each executive is defined by the assigned policy, executive reservation. In this policy, each executive receives a minimum of 128 Kbps of reserved bandwidth.

**Bandwidth Reservation Policy Configuration—LAN-to-LAN**

In mixed environments where there are both remote access and site-to-site connections, it is also possible to reserve bandwidth for the site-to-site tunnels. For site-to-site policies, the minimum bandwidth field assigns the bandwidth reservation to the site-to-site tunnel rather than allocating bandwidth per user connecting through the tunnel.

In the LAN-to-LAN policy example above, when a site-to-site tunnel is established, the bandwidth reservation for the tunnel is 384 Kbps. The 384 Kbps of bandwidth will then be assigned on a tunnel basis, not on a per user basis.

Bandwidth Reservation—Public
Interface Configuration

Cisco.com

**Configuration | Policy Management | Traffic Management | Bandwidth Policies | Modify**

Configure bandwidth policy parameters. To create a bandwidth policy, you must enable at least one of the checkboxes.

Policy Name    normal reservation    Enter a unique name for this policy.

☑  Bandwidth Reservation    Check to reserve a minimum bandwidth per session.

Minimum Bandwidth 64    kbps ▾    Enter the minimum bandwidth.

Traffic policing allows you to control a policing rate or size of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.

☐  Policing    Check to enable Policing.

Policing Rate  56

Normal Burst Size  10500

Apply    Cancel

**Configuration | Interfaces | Ethernet 2**

**Configuring Ethernet Interface 2 (Public).**

General | RIP | OSPF | Bandwidth

| Bandwidth Management Parameters | | |
|---|---|---|
| Attribute | Value | Description |
| Bandwidth Management | ☑ | Check to enable bandwidth management. |
| Link Rate | 1544    kbps ▾ | Set the link rate that will be applied to all tunneled traffic. The defined link rate must be based on available Internet bandwidth and not the physical LAN connection rate. |
| Bandwidth Policy | normal reservation ▾ | This policy is applied to all VPN tunnels that do not have a group based Bandwidth Management policy. Policies are configured at Configuration | Policy Management | Traffic Management | Bandwidth Policies. |

Apply    Cancel

© 2003, Cisco Systems, Inc. All rights reserved.    CSVPN 4.0—9-53

First, the administrator defines bandwidth reservation policies. Next, the policies are applied to interfaces, groups, and site-to-site tunnels. Choose the **Configuration>Interfaces>Ethernet 1 2 3** window, **Bandwidth Parameters** tab to apply a policy to an interface. The Bandwidth tab parameters are as follows:

■ Bandwidth Management—Select the **Bandwidth Management** check box to enable the feature on the interface.

■ Link Rate—Set the link rate applied to all tunneled traffic. The defined link rate must be based on the available Internet bandwidth and not the physical LAN connection rate. The default is 1.544 Mbps.

■ Bandwidth Policy—Select a bandwidth policy for this interface. This policy is applied to all VPN tunnels that do not have a group based bandwidth management policy.

If bandwidth reservation is required in a network, a bandwidth reservation policy must be defined and applied to an interface before applying group bandwidth reservation policies. The Concentrator will not allow a group policy to be applied first. If an administrator attempts to apply a group policy first, the Concentrator will return an error message.

In this example, each remote user not assigned to a group bandwidth reservation policy will receive the minimum bandwidth reservation defined by the normal reservation policy. In this example, the user would be assigned 64 Kbps of bandwidth.

**Bandwidth Reservation—Group Configuration**

Cisco.com
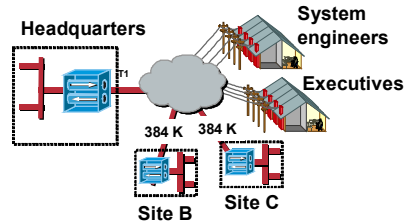
Headquarters

System engineers

Executives

T1

384 K    384 K

Site B    Site C

Configuration | User Management | Groups | Bandwidth Policy | Interfaces

Configure group-wide bandwidth parameters. To share global available bandwidth, instead of a specific reservation, enter 0 in the **Bandwidth Aggregation** textbox.

**Ethernet 2 (Public)**

Policy [exec reservation ▼]    Select the bandwidth policy to apply to this interface.

Bandwidth Aggregation [384]    [kbps ▼]    Enter the aggregate reserved group bandwidth for this interface.

[Apply]  [Cancel]

CSVPN 4.0—9-54

For those groups that have different bandwidth requirements, the administrator can define group-based bandwidth requirements. Choose the **Configuration>User Management>Groups** window, select a group, and select **Bandwidth Assignmen**t. From the Policy drop-down menu, select the appropriate policy. In the figure, the policy assigned to the interface reserved 64 Kbps of bandwidth for each remote user. This is fine for the system engineers, but the executives require a larger bandwidth reservation. From the Policy drop-down menu, the administrator selected the executive policy. With this policy, each member of the executive group is allocated a minimum bandwidth reservation of 128 Kbps.

**Bandwidth Aggregation**

Cisco.com

**Bandwidth reservation**
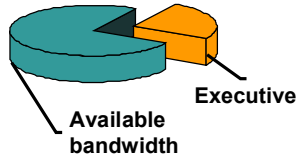
**Executive**

**Available bandwidth**

Configuration | User Management | Groups | Bandwidth Policy | Interfaces

Configure group-wide bandwidth parameters. To share global available bandwidth, instead of a specific reservation, enter 0 in the **Bandwidth Aggregation** textbox.

**Ethernet 2 (Public)**

Policy `exec reservation` ▼ Select the bandwidth policy to apply to this interface.

Bandwidth Aggregation `512` `bps` ▼ Enter the aggregate reserved group bandwidth for this interface.

[Apply] [Cancel]

© 2003, Cisco Systems, Inc. All rights reserved.  CSVPN 4.0—9-55

Choose the **Configuration>System>Tunneling Protocols>IPSec>IPSec LAN-to-LAN** window and select the connection you wish to modify by choosing the **Modify** button. From the bandwidth policy drop-down menu, select a bandwidth policy to apply to this IPSec LAN-to-LAN connection from the drop-down list. If you do not want to select a policy here, select none. When the bandwidth reservation policy is applied to a LAN-to-LAN connection, the Concentrator automatically aggregates the bandwidth. The minimum bandwidth is applied to the tunnel rather than on a per user basis. This allows you to reserve a specific amount of bandwidth for the site-to-site connection.

In the figure, the LAN-to-LAN policy was defined with a minimum bandwidth of 384 Kbps. This policy was applied to the LAN-to-LAN tunnel configurations (only the Site B tunnel configuration is shown). Once applied, the Concentrator will aggregate 384 Kbps of bandwidth to each LAN-to-LAN tunnel.

| Note | If the bandwidth reservation is enabled and the administrator selects None from the LAN-to-LAN Bandwidth Policy drop-down menu, the LAN-to-LAN tunnel contends for system wide bandwidth, a default user. If no reservation is applied and the tunnel drops, there is no guarantee that the LAN-to-LAN tunnel can reconnect if other default remote users make a connection before the LAN-to-LAN tunnel reestablishes its connection. It is suggested that, if bandwidth reservation is applied to the network, a LAN-to-LAN bandwidth reservation policy should be defined and applied. |

## LAN-to-LAN Bandwidth Reservation Configuration

Cisco.com

**Bandwidth reservation**

Configuration | Policy Management | Traffic Management | Bandwidth Policies | Mod

Configure bandwidth policy parameters. To create a bandwidth policy, you must enable a

Policy Name   LAN-to-LAN reservation   Enter a unique name for

☑ Bandwidth Reservation       Check to reserve a min
Minimum Bandwidth  384      kbps ▾   Enter the minimum bandwidth.

Traffic policing allows you to control a policing rate or size of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.
☐ Policing                    Check to enable Policing.
Policing Rate  56        kbps ▾   Enter the policing rate. Traffic below this rate will be transmitted; traffic above this rate will be dropped.
Normal Burst Size  10500    bytes ▾  Enter the amount of data allowed in a burst before excess packets will be dropped.

Apply   Cancel

Site B
Site C
Available bandwidth

CSVPN 4.0—9-56

Configuring bandwidth reservation alone may lead to a scenario in which high priority, high bandwidth, users are unable to connect to a congested Concentrator because of their bandwidth requirements. In this example, the Concentrator provides a feature called bandwidth aggregation. Bandwidth aggregation allows a particular group to reserve a fixed portion of the total bandwidth on the interface. (This fixed portion is known as an aggregation.) Then, as users from that group connect, each receives a part of the total bandwidth allocated for that group. When one group makes a reserved bandwidth aggregation, it does not affect the bandwidth allocated to users who are not in that group. However, other users are now sharing a smaller amount of the total bandwidth. Fewer users can connect. One can think of bandwidth reservation as pieces of a pie. Each group is assigned a slice of pie, aggregate bandwidth. As tunnels are established, each user is assigned part of the slice until the slice is completely divided. At that point, any new connections requesting a slice of the piece are refused a connection. Choose the **Configuration>User Management>Groups>Bandwidth Policy>Interfaces** window to assign a bandwidth aggregation. Configure the following parameters:

■ Policy—Select a bandwidth policy from the Policy drop-down menu.

■ Bandwidth Aggregation—Enter a value for the minimum bandwidth to reserve for this group and select a unit of measure.

In the figure, the executive group is assigned a bandwidth aggregation of 512 Kbps. As each executive connects, they are allocated part of the 512 Kbps aggregated bandwidth. The amount of bandwidth allocated to each executive is defined by the assigned policy. In this case, each executive reserves bandwidth of 128Kbps. Executive users are allocated bandwidth until their 512 Kbps slice of the bandwidth pie has been allocated.

# Bandwidth Session Statistics

| Administration | Administer Sessions | Detail | | | Tuesday, 17 September 2002 09:43:34 |
| --- | --- | --- | --- | --- | --- |

Reset ⟋ Refresh ⟳

Back to Sessions

| Connection Name | IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx |
| --- | --- | --- | --- | --- | --- | --- | --- |
| pod6 | 192.168.1.5 | IPSec/LAN-to-LAN | 3DES-168 | Sep 17 09:37:17 | 0:06:17 | 32496 | 728 |

**Bandwidth Statistics**

| User Name | Interface | Traffic Rate (kbps) | | Traffic Volume (bytes) | |
| --- | --- | --- | --- | --- | --- |
| | | Conformed | Throttled | Conformed | Throttled |
| pod6 (In) | Ethernet 2 (Public) | 0 | 0 | 1534 | 0 |
| pod6 (Out) | Ethernet 2 (Public) | 0 | 0 | 43470 | 0 |

IKE Sessions: 1
IPSec Sessions: 2

| IKE Session | | | |
| --- | --- | --- | --- |
| Session ID | 1 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Diffie-Hellman Group | Group 2 (1024-bit) |
| Authentication Mode | Pre-Shared Keys | IKE Negotiation Mode | Main |
| Rekey Time Interval | 86400 seconds | | |

| IPSec Session | | | |
| --- | --- | --- | --- |
| Session ID | 2 | Remote Address | 192.168.1.5 |
| Local Address | 192.168.6.5 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Encapsulation Mode | Tunnel |
| Rekey Time Interval | 28800 seconds | | |
| Bytes Received | 728 | Bytes Transmitted | 672 |

CSVPN 4.0—9-57

Choose the **Administration>Administer Sessions>Detail** window to view individual session bandwidth management statistics. This window shows details of the effects of bandwidth management policies on each tunnel. Only tunnels on which bandwidth management policies are enabled appear on this screen. The bandwidth statistics parameters are as follows:

- User Name—The user name identifying a tunnel using a bandwidth management policy

- Traffic Rate—The rate at which traffic is transmitted. Measured in kilobits per second

  - Conformed—The current rate of session traffic (as set by the bandwidth management policy)

  - Throttled—The rate at which packets are being constrained to maintain the conformed rate

- Traffic Volume—Measured in bytes

  - Conformed—The number of bytes of session traffic (as set by the bandwidth management policy)

  - Throttled—The number of bytes being throttled to maintain the conformed rate

## Bandwidth Monitoring Statistics

| Monitoring \| Statistics \| Bandwidth Management | | | | | | Tuesday, 17 September 2002 09:40:38 |

Reset ✎ Refresh⟳

This screen shows bandwidth management information. To refresh the statistics, click **Refresh**. Select a **Group** to filter the users.

Group --All-- ▼

| User Name | Interface | Traffic Rate (kbps) | | Traffic Volume (bytes) | |
|---|---|---|---|---|---|
| | | Conformed | Throttled | Conformed | Throttled |
| pod6 (In) | Ethernet 2 (Public) | 0 | 0 | 826 | 0 |
| pod6 (Out) | Ethernet 2 (Public) | 7 | 0 | 42432 | 0 |

CSVPN 4.0—9-58

Choose the **Monitoring>Statistics>Bandwidth Management** window to view bandwidth management session statistics. This window shows details of the effects of bandwidth management policies on each tunnel. Only active tunnels on which bandwidth management policies are enabled appear in this window. The bandwidth management statistics parameters are as follows:

■ User Name—The user name identifying a tunnel using a bandwidth management policy

■ Traffic Rate—Measured in kilobits per second

  — Conformed—The current rate of session traffic (as set by the bandwidth management policy)

  — Throttled—The rate at which packets are being throttled to maintain the conformed rate

■ Traffic Volume—Measures in bytes

  — Conformed—The number of bytes of session traffic (as set by the bandwidth management policy)

  — Throttled—The number of bytes being throttled to maintain the conformed rate

# Administration—Ping

**Administration | Ping**

This screen lets you test network connectivity. **Please wait for the operation to complete.**

Address/Hostname to Ping | 192.168.1.5 |

[ Ping ]   [ Cancel ]

**Success**

(i) 192.168.1.5 is alive.

[ Continue ]

CSVPN 4.0—9-89

The Administration>Ping window enables you to use the ICMP ping utility to test network connectivity. Specifically, the Concentrator sends an ICMP Echo Request message to a designated host. If the host is reachable, it returns an echo reply message and the Manager displays a Success window. If the host is not reachable, the Manager displays an Error window.

## TFTP Transfer

**Administration | File Management | TFTP Transfer**

This screen lets you transfer files to/from the **VPN 3000 Concentrator Series**. **Please wait for the operation to finish.**

| Concentrator File | Action | TFTP Server | TFTP Server File |
| --- | --- | --- | --- |
| | GET << ▾ | | |

OK    Cancel

CSVPN 4.0—9-60
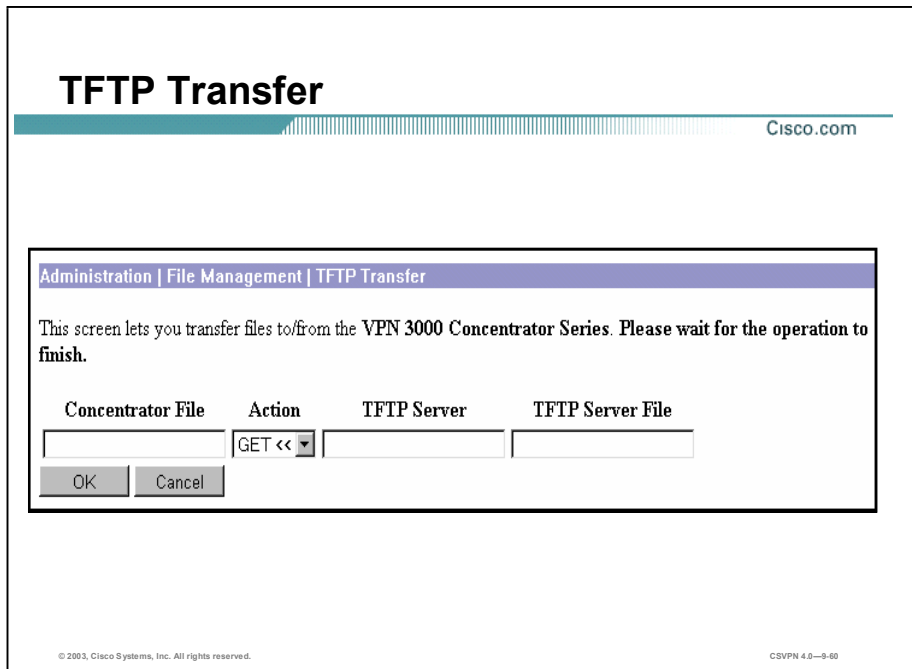
The Administrator>File Management>TFTP Transfer window enables you to use TFTP to transfer files to and from the Concentrator Flash memory. The Concentrator acts as a TFTP client for these functions, accessing a TFTP server running on a remote system. All transfers are made in binary mode, and they copy, rather than move, files.

To use the TFTP functions, complete the following fields (you must have access rights to read and write files):

■ TFTP Get—Get a file from the remote system (that is, copy a file from the remote system to the Concentrator).

■ TFTP Put—Put a file on the remote system (that is, copy a file from the Concentrator to the remote system).

■ TFTP Server—Enter the IP address or host name of the remote system running the TFTP server. (If you configured a DNS server, you can enter a host name; otherwise, enter an IP address.)

■ Concentrator File—Enter the name of the file on the Concentrator.

---

**Caution**    If either filename is the same as an existing file, TFTP overwrites the   existing file without asking for confirmation.

---

# Summary

This topic summarizes what you learned in this lesson.

## Summary

- **Many items can be monitored, including system status, interface statistics, power supply status, and statistics on the various protocols in use.**
- **Administration consists of configuring access rights, configuring ACLs, updating the software image, and performing file management.**
- **Bandwidth management can be enabled to distribute bandwidth more equitably.**

CSVPN 4.0—9-62

**Summary (cont.)**

Cisco.com

- **An administrative ping can be used to test connectivity.**
- **TFTP transfer is available for file transfers.**

CSVPN 4.0—9-63

# Lab Exercise—Cisco VPN 3000 Series Concentrator Monitoring and Administration

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

In this lab exercise you will monitor and administer newly installed Cisco Virtual Private Network (VPN) 3000 Series Concentrators. Work with your lab exercise partner to complete the following tasks:

■ Complete the lab exercise setup.

■ Monitor the Cisco VPN 3000 Series Concentrator system status.

■ Monitor the Cisco VPN 3000 Series Concentrator system events.

■ Modify and test a new Cisco VPN 3000 Series Concentrator user account.

■ Restore the original Cisco VPN 3000 Series Concentrator user account settings.

■ Update the Cisco VPN 3000 Series Concentrator software.

■ View and copy configuration files.

■ Configure bandwidth management policies.

■ Add bandwidth management policies.

■ Monitor bandwidth management statistics.

■ Configure the Cisco VPN 3000 Series Concentrator for TACACS+ administration account authentication.

■ Restore the original administrator account and disable TACACS+ administrator account authorization.

■ Disable Split Tunneling and firewall required.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



Lab Visual Objective
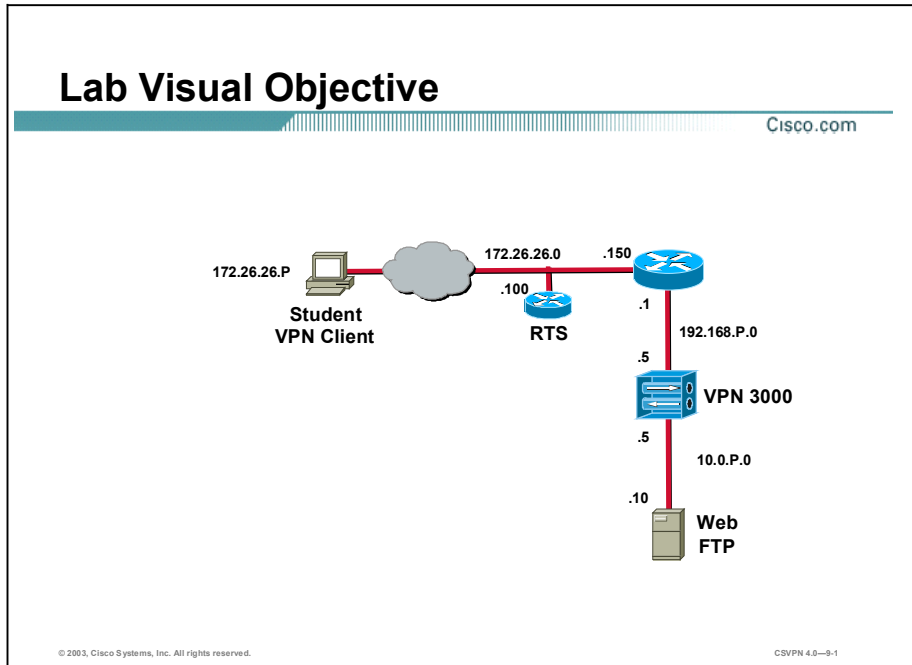
Scenario

Your employer has asked you to administer the newly installed Concentrators in your network.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment is setup as follows:

■ Ensure that your student PC is powered on.

■ Ensure that your student PC IP addresses are configured correctly:

— Primary IP address—172.26.26.P
(where P = pod number)

— Default gateway IP address—172.26.26.150

■ Ensure that your Concentrator is powered on.

## Task 2—Monitor the Cisco VPN 3000 Series Concentrator System Status

Complete the following steps to log in and monitor the Concentrator system status:

**Step 1**  Launch Internet Explorer by double-clicking the desktop icon.

**Step 2**  Enter the Concentrator's public interface IP address of **192.168.P.5** in the Internet Explorer Address field. Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

(where P = pod number)

**Step 3**  Log in to the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

The username (login) and password are always case sensitive.

**Step 4**  From the Monitoring menu tree, drill down to **System Status** and answer the following questions:

Q1)  What is the Software Rev?

A)  _____

Q2)  What is the RAM size?

A)  _____

Q3)  The system has been up since when (last time booted)?

A)  _____

**Step 5**  Click the Concentrator power supply graphic and answer the following question:

Q4)  Are the voltages OK?

A)  _____

**Step 6**  Click **Back**.

**Step 7**  Click the Concentrator private interface port graphic and answer the following questions:

Q5)  What is the IP address of the port?

A)  _____

Q6)  What is the status of the port?

A)  _____

**Step 8**  Click **Back**.

**Step 9**  Click the Concentrator public interface port graphic and answer the following questions:

Q7)  What is the IP address of the port?

A)    _____

Q8)    What is the status of the port?

A)    _____

**Step 10**  Click **Back**.

**Step 11**  View the fan status and answer the following questions:

Q9)    What is the speed of fan 1?

A)    _____

Q10)   What is the speed of fan 2?

A)    _____

Q11)   What is the temperature inside the chassis?

A)    _____

The larger Concentrator models (3015 and above) enable you to drill down to System Status>LED Status from the Monitoring menu tree. This feature enables you to view the state of the front panel LEDs.

## Task 3—Monitor the Cisco VPN 3000 Series Concentrator System Events

Complete the following steps to monitor the Concentrator system events:

**Step 1**  From the Configuration menu tree, drill down to **System>Events>General** and answer the following questions:

Q12)   Is Save Log on Wrap enabled?

A)    _____

Q13)   What are the three Save Log formats?

A)    _____

B)    _____

C)    _____

Q14)   Is FTP saved log on wrap enabled?

A)    _____

Q15)   What is the range of severity captured to the log?

A)    _____

Q16)   What is the range of severity captured to the console?

A) _____

Q17) Are there any logged events sent to Syslog, E-mail, or SNMP traps?

A) _____

**Step 2** Click **Cancel**.

**Step 3** From the Monitoring menu tree, drill down to **Filterable Event Log**.

**Step 4** In the Client IP Address field, enter your student PC's primary IP address.

**Step 5** Click |<< and answer the following question:

Q18) What, if anything, did you see?

A) _____

**Step 6** Click **Get Log**. Answer the following question:

Q19) What happened?

A) _____

**Step 7** Close the log Internet Explorer window.

**Step 8** Set the Client IP address back to **0.0.0.0**.

**Step 9** Click **Save Log**. The Internet Explorer user prompt window opens.

**Step 10** Enter a filename: **LOG2**.

**Step 11** Click **OK**.

**Step 12** From the Administration menu tree, drill down to **File Management**. Answer the following question:

Q20) Is LOG2 listed as one of the files?

A) _____

**Step 13** For LOG2 under the actions column, click **View**.

**Step 14** Close the window.

**Step 15** For LOG2 under the actions column, click **Delete** (delete only the LOG2 file). The Are you sure you want to delete LOG2 message opens.

**Step 16** Click **OK**.

**Step 17** From the Administration>File Management window, select **XML Export**. The Administration>File Management>XML Export window opens.

**Step 18** In the File Name field, enter **FILEXML** and click **Export**. The Success window opens.

**Step 19** Click **Continue**. The Administration>File Management window opens.

**Step 20** For FILEXML under the Actions column, click **View**. An Internet Explorer window opens.

**Step 21** From the Internet Explorer tool bar in the window, select **Edit>Find (on this page)**. The Internet Explorer Find window opens.

**Step 22** In the Find what field**,** enter **Ethernet** and click **Find Next**. From the Ethernet category, answer the following questions:

    Q21)    What is the <index> number?

        A)    _____

    Q22)    What is the <addr_setting>?

        A)    _____

    Q23)    What is the <ipaddr> setting?

        A)    _____

    Q24)    What is the <subnet> address?

        A)    _____

**Step 23** In the Find window, click **Cancel**.

**Step 24** Close the FILEXML Internet Explorer window.

**Step 25** Under the actions column of the FILEXML row, click **Delete** (delete only the FILEXML file). The Are you sure you want to delete FILEXML message opens.

**Step 26** Click **OK**.

## Task 4—Modify and Test a New Cisco VPN 3000 Series Concentrator User Account

In this task, modify the access rights of a default user account and test new access capabilities. Complete the following steps to modify and test a default user account using the Cisco VPN 3000 Concentrator Series Manager:

**Step 1** From the Administration menu tree, drill down to **Access Rights>Administrators**.

**Step 2** Go to the user account line and click **Modify**.

**Step 3** Change User Name to **userP**.

  (where P = pod number)

**Step 4** Change Password to **userP**.

  (where P = pod number)

**Step 5** Change Verify to **userP**.

  (where P = pod number)

**Step 6** Change Authentication to View Config.

**Step 7** Change General to View Config.

**Step 8** Change SNMP to View Config.

**Step 9** Leave Files at Read Files.

**Step 10** Click **Apply**.

**Step 11** Enable the userP account by selecting the **Enabled** check box.

(where P = pod number)

**Step 12** Click **Apply**.

**Step 13** Log out of the Concentrator.

**Step 14** Log in to the Cisco VPN 3000 Concentrator Series Manager using the new userP account:

Login: **userP**

Password: **userP**

(where P = pod number)

**Step 15** From the Configuration menu tree, drill down to **Interfaces>DNS Server(s)**.

**Step 16** De-select the **Enabled** check box.

**Step 17** Click **Apply**.

Q25) What message did you receive? Why?

A) _____

**Step 18** From the Administration menu tree, drill down to **Access Rights** and answer the following question:

Q26) What message did you receive? Why?

A) _____

**Step 19** Log out of the Concentrator.

You have successfully modified and tested the user account. Now restore the original account settings. Resetting the Concentrator to factory defaults does not return the original access account settings. Returning accounts to their original settings must be done manually.

## Task 5—Restore the Original Cisco VPN 3000 Series Concentrator User Account Settings

In this task, return the modified user account back to its default values. Complete the following steps to restore the original settings for the user account:

**Step 1** Log into the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

Login: **admin**

Password: **admin**

**Step 2** From the Administration menu tree, drill down to **Access Rights>Administrators**.

**Step 3** Locate the userP account line and click **Modify**.

(where P = pod number)

**Step 4** Click **Default**. Answer the following question:

Q27) What happened to the Enabled check box?

A) _____

When you click **Default**, two things happen: the account is disabled and the access rights are reset to Stats Only.

**Step 5**  Locate the userP account line and click **Modify**. Answer the following question:

(where P = pod number)

Q28)  What happened to the access rights?

A) _____

**Step 6**  Change the username to **user**.

**Step 7**  Change the password to **user**.

**Step 8**  Change verify to **user**.

**Step 9**  Click **Apply**.

**Step 10**  From the Administration menu tree, drill down to **Access Rights>Access Settings** and answer the following questions:

Q29)  What is the session idle timeout setting?

A) _____

Q30)  By default, the Concentrator allows a maximum of how many administration sessions?

A) _____

Q31)  By default, does the Concentrator configuration file contain encrypted data?

A) _____

When configuration file encryption is selected (the default), it does not apply to the entire contents of the configuration file. Only passwords and other security-related parameters within the configuration file are encrypted.

**Step 11**  Click **Cancel**.

## Task 6—Update the Cisco VPN 3000 Series Concentrator Software

Complete the following steps to practice using the Cisco VPN 3000 Series Concentrator software update utility:

**Step 1**  From the Administration menu tree, drill down to **Software Update**.

**Step 2**  Select **Concentrator**. The Administration>Software Update>Concentrator window opens.

**Step 3**  Click **Browse** and open the desktop TFTP folder.

**Step 4**  Select the **Cisco VPN 3005 release 4.0.x.Rel** binary (.bin) file.

**Step 5**  Click **Open**.

**Step 6**  Click **Upload**. The Software Update Progress message window opens, followed by the Software Update Success window. Wait until the software update is completed before continuing.

**Step 7**     Select **Click here to go to the reboot options**. The Administration>System Reboot window opens.

**Step 8**     Select the action to take: **Reboot**.

**Step 9**     Select the type of reboot to perform: **Reboot without saving active configuration**.

**Step 10**    Select the time to perform the reboot or shutdown: **Now**.

**Step 11**    Click **Apply** and wait for the reboot to complete.

**Step 12**    Log into the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

**Step 13**    From the Monitoring menu tree, drill down to **System Status** and answer the following question:

Q32)     What is the current software revision?

A)     _____

## Task 7—View and Copy Configuration Files

Complete the following steps to make copies of the Concentrator configuration files:

**Step 1**     From the Administration menu tree, drill down to **File Management**.

**Step 2**     Locate the CONFIG file and click **View**. A new Internet Explorer window opens displaying the contents of the CONFIG file. Answer the following questions:

Q33)     What is the [system] name?

A)     _____

Q34)     What is the [Access] timeout setting?

A)     _____

Q35)     What is [Access] maxsession setting?

A)     _____

**Step 3**     Locate the password parameter using **Edits>Find** under the Internet Explorer Toolbar, and answer the following question:

Q36)     Is the password encrypted?

A)     _____

Remember that the default setting for configuration files is to encrypt all passwords and security-related parameter values.

**Step 4**     Close the Internet Explorer window containing the CONFIG file contents.

**Step 5**     Locate the CONFIG file and click **Copy**. The Enter filename to copy to message window opens.

**Step 6**     Enter a filename: **backup1**. Filenames must meet the standard ≤8.3 notation rule.

**Step 7**   Click **OK** and answer the following question:

Q37)   Is the backup1 file listed in the Administration>File Management window?

A)   _____

**Step 8**   Locate the backup1 file and click **Delete**. The Are you sure you want to delete Backup1 message box opens.

**Step 9**   Click **OK**.

## Task 8—Configure Bandwidth Management Policies

Configuring bandwidth management is a two-step process. First, configure the bandwidth management policy. Second, apply the policy to the interface and groups. Complete the following steps to configure the policy:

**Step 1**   From the Configuration menu tree, drill down to **Policy Management>Traffic Management>BW Policies**. The Policy Management>Traffic Management> Bandwidth Policies window opens.

**Step 2**   Click **Add** under the Actions column. The Policy Management>Traffic Management>Bandwidth Policies>Add window opens. Complete the following sub-steps to add a bandwidth reservation policy:

1.   In the Policy Name field, enter **normal reservation**.

2.   Select the **Bandwidth Reservation** check box.

Q38)   What is the default minimum bandwidth?

A)   _____

3.   Click **Add**.

**Step 3**   Click **Add** under the Actions column to create a second policy for the training group. The Policy Management>Traffic Management>Bandwidth Policies>Add window opens. Complete the following sub-steps to add a bandwidth reservation policy:

1.   In the Policy Name field, enter **training**.

2.   Select the **Bandwidth Reservation** check box.

3.   In the Minimum Bandwidth field, enter **64**. The units should be Kbps.

4.   Click **Add**.

## Task 9—Add Bandwidth Management Policies

In the previous task, you configured the bandwidth management policies. In this task, apply the policies to the public interface and training group. Complete the following steps to add the policies:

**Step 1**   Complete the following sub-steps to add the bandwidth reservation policy to the public interface:

1. From the Configuration menu, drill down to **Interfaces**.

2. In the Configuration>Interfaces window, click **Ethernet 2 (Public)**. The Configuration>Interfaces>Ethernet2 window opens.

3. Select the **Bandwidth** tab.

4. Select the **Bandwidth Management** check box.

Q39) What is the default link rate?

A) _____

5. From the Bandwidth Policy drop-down menu, select **normal reservation**.

6. Click **Apply**.

**Step 2** Complete the following sub-steps to add the bandwidth reservation policy to the training group:

1. From the Configuration menu, drill down to **User Management>Groups**.

2. Under Current Groups, select **training**.

3. Under the Modify column, click **Bandwidth Assignment**. The Configuration>User Management>Groups>Bandwidth Policy window opens.

4. Under the Interface column, click **Ethernet 2 (Public)**. The Configuration>User Management>Groups>Bandwidth>Interfaces window opens.

5. From the Policy drop-down menu, select **training**.

6. Click **Apply**.

7. Save your work.

**Step 3** Log out of the Concentrator.

**Step 4** Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. Verify that the connection entry is studentP.

(where P = pod number)

**Step 5** Verify that the IP address of remote server is set to a Cisco VPN 3000 Series Concentrator's public interface IP address of **192.168.P.5**.

(where P = pod number)

**Step 6** Click **Connect**. The Connection History window opens and several messages flash by quickly. Complete the following sub-steps:

1. Enter **studentP** when you are prompted for a username.
   (where P = pod number)

2. Enter **studentP** when you are prompted to enter a password.
   (where P = pod number)

**Step 7** Click **OK**.

---

**Step 8**   The window closes and a Cisco VPN Client icon appears in the system tray.

# Task 10—Monitor Bandwidth Management Statistics

In the previous task, you configured the bandwidth management policies and applied the policies to the public interface and training group. In this task, you will monitor the bandwidth management statistics. Complete the following steps to monitor bandwidth management statistics:

**Step 1**   Log in to the Cisco VPN 3000 Concentrator Series Manager private interface using the administrator account:

Login: **admin**

Password: **admin**

The username (login) and password are always case sensitive.

**Step 2**   From the Monitoring menu, drill down to **Statistics>Bandwidth Mgmt**. The Monitoring> Statistics>Bandwidth Management window opens.

Q40)   Under User Name column, what name is listed?

A)   _____

Q41)   What Interface is listed?

A)   _____

**Step 3**   Click **Reset** to clear the statistics.

**Step 4**   Click **Refresh** three or four times. From the StudentP (Out) row, provide the following information:

Q42)   What is the conformed traffic rate?

A)   _____

Q43)   What is the throttled traffic rate?

A)   _____

Q44)   What is the conformed traffic volume?

A)   _____

Q45)   What is the throttled traffic volume?

A)   _____

**Step 5**   From the Monitoring menu, drill down to **Remote Access Sessions** under Sessions.

**Step 6**   In the Monitoring>Sessions window, select **StudentP**.

(where P = pod number)

**Step 7**   From the Bandwidth Statistics for studentP (Out) row, answer the following questions:

Q46)     What is the conformed traffic rate?

A)      _____

Q47)     What is the throttled traffic rate?

A)      _____

Q48)     What is the conformed traffic volume?

A)      _____

Q49)     What is the throttled traffic volume?

A)      _____

## Task 11—Configure the Cisco VPN 3000 Series Concentrator for TACACS+ Administration Account Authentication

As a Terminal Access Control Access Control System (TACACS+) administrator, you need to know how to administer the Concentrator administration accounts. Complete the following steps to administer the Concentrator administrator accounts using the Cisco VPN Concentrator Series 3000 Manager and TACACS+:

**Step 1**   From the Administration menu tree, drill down to **Access Rights>Administrators**.

**Step 2**   Locate the Admin username line and click **Modify**. Complete the following sub-steps:

1. Set AAA Access Level to **3**. The AAA access level must match the privilege level set on the TACACS+ server.

2. Click **Apply**. The Administration>Access Rights>Administrator window opens.

3. Click **Apply**.

**Step 3**   From the Administration menu tree, drill down to **Access Rights>AAA Servers> Authentication** and complete the following sub-steps:

1. Click **Add**.

2. Enter the authentication server IP address 10.0.P.10.
   (where P = pod number)

3. Enter the server secret: **secretkey**. Server secrets are always case sensitive and must be entered exactly as shown here.

4. Verify the server secret: **secretkey**.

5. Click **Add**. The Access Rights>AAA Servers>Authentication window opens.

**Step 4**   From the Administration>Access Rights>AAA Servers>Authentication window, complete the following sub-steps to test the ability of the Concentrator to reach the TACACS+ authentication server:

1. Select the IP address of the authentication server 10.0.P.10.
   (where P = pod number)

2. Click **Test**.

3. Enter the username: **studentP**.
   (where P = pod number)

4. Enter the password: **training**.

5. Click **OK**. The process may take several moments to complete. Answer the following question:

Q50) What message did you receive?

A) _____

---

**Caution**    The test must be successful before you proceed.

---

**Step 5**   From the Monitoring menu tree, drill down to **Filterable Event Log**.

**Step 6**   Click **Clear Log**.

**Step 7**   Log out of the Concentrator.

**Step 8**   Log in to the Cisco VPN 3000 Concentrator Series Manager using the TACACS+ studentP (where P = pod number) account. This administrator account resides on the TACACS+ server and is not the same account as any Concentrator studentP account used previously. During this login attempt, the Concentrator will verify the login and password with the TACACS+ server.

```
Login: studentP
Password: training
```

(where P = pod number)

It takes a few moments for the authentication to complete.

**Step 9**   From the Monitoring menu tree, drill down to **Filterable Event Log**. Answer the following question:

Q51) Did the TACACS+ authentication server authenticate the studentP (where P = pod number) account?

A) _____

# Task 12—Restore the Original Administrator Account and Disable TACACS+ Administrator Account Authorization

Complete the following steps to set the administration settings for the Concentrator back to their defaults:

**Step 1**   From the Administration menu tree, drill down to **Access Rights>Administrators**.

**Step 2**   Locate the administrative account line and click **Modify**. Complete the following sub-steps:

---

1. Set the AAA access level to **0**. Setting the AAA access level to 0 tells the Concentrator to authenticate the administrator user locally. This disables TACACS+ authentication of the selected administrator account.

2. Click **Apply**. The Administration>Access Rights>Administrator window opens.

3. Click **Apply**.

**Step 3**   From the Administration menu tree, drill down to **Access Rights>AAA Servers> Authentication** and complete the following sub-steps:

1. Select the IP address of the authentication server.

2. Click **Delete**. This removes the TACACS+ authentication server from the Concentrator configuration.

3. Save the configuration changes.

## Task 13—Disable Split Tunneling and Firewall Required

In the previous tasks, the Concentrators used split tunneling and a firewall. For the next lab exercise, you will disable split tunneling and a firewall is not required. For a VPN tunnel to connect, the Concentrator must be reconfigured. Complete the following steps to modify the VPN tunnel and firewall settings:

**Step 1**   From the Configuration menu tree, drill down to **User Management>Groups**. The Configuration>User Management>Groups window opens.

**Step 2**   Choose **training** from the Current Groups list and click **Modify Group**. The Configuration>User Management>Groups>Modify training window opens.

**Step 3**   Select the **Client FW** tab.

**Step 4**   Select **No Firewall** in the Firewall setting group box.

**Step 5**   Select the **Client Config** tab.

**Step 6**   Go to the Split Tunneling group box and select **Tunnel Everything**.

**Step 7**   Scroll down to the bottom of the window and click **Apply**.

**Step 8**   Save the changes.

**Step 9**   Log out of the Concentrator, and close Internet Explorer.

**10**

# Configure the Cisco VPN 3002 Hardware Client for Remote Access Using Pre-Shared Keys

## Overview

This lesson includes the following topics:

■ Objectives

■ Cisco VPN 3002 Hardware Client remote access with pre-shared keys

■ Summary

■ Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- Configure the Cisco VPN 3002 Hardware Client for client mode remote access.
- Configure the Cisco VPN 3002 Hardware Client for network extension mode remote access.
- Monitor the status of the Cisco VPN 3002 Hardware Client.

CSVPN 4.0—10-2

# Cisco VPN 3002 Hardware Client Remote Access with Pre-Shared Keys

This lesson explains how to configure the Cisco Virtual Private Network (VPN) 3002 Hardware Client for remote access.
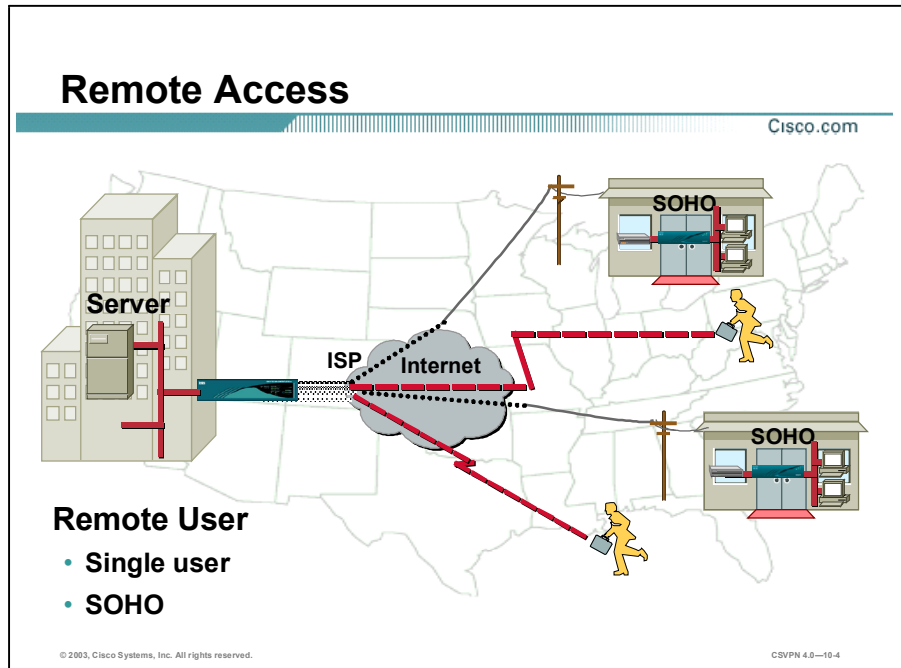


If a single remote user wants the ability to dial into the corporate network, typically the VPN software client is loaded onto the PC, which enables the remote user to establish secure communications with the central site. With the client resident on the PC, the user does not have to carry any external hardware. The caveat is that the software client works for only the single PC on which it is installed.

Small Office/Home Office (SOHO) is better positioned to use the Hardware Client. Just plug the SOHO PCs into the Hardware Client. The Hardware Client establishes secure communications for all the SOHO PCs. The Hardware Client supports up to 253 users. There is no need to add any VPN applications to the SOHO PC. The Hardware Client takes care of all the tunneling requirements.

**Remote Access Tunnel**

Cisco.com

Application server

Concentrator

Internet

Hardware Client

IPSec tunnel or session
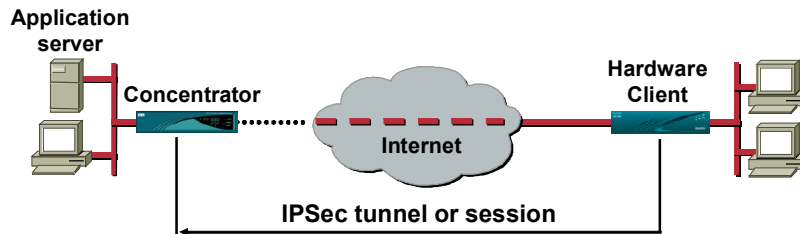
CSVPN 4.0—10-5

In the example, the Cisco VPN software client was ported over to the Hardware Client. The Hardware Client provides the VPN software client functionality on a hardware platform. The Hardware Client works with the Cisco VPN 3000 Series Concentrator to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Management (IKE) and IPSec tunneling protocols to make and manage the secure connection. No applications need to be added to the SOHO PC to perform the tunneling.

Client and network extension modes are the two modes of operation in the Hardware Client:

■ The client mode is for those who want to deploy a VPN quickly and easily in small remote offices. If there is no need to see the devices behind the Hardware Client, and ease of use and installation is the key, then client mode should be implemented. In client mode, the Hardware Client uses Port Address Translation (PAT) to isolate its private network from the public network. SOHO PCs behind the Hardware Client are invisible to the outside world. PAT causes all traffic from the SOHO PCs to appear on the private network as a single source IP address. In the above example, the Hardware Client receives a virtual IP address, 10.0.1.12 or 10.0.1.22 respectively, from the Concentrator during tunnel establishment. All remote PCs addresses in the client mode section have their IP address translated to either 10.0.1.12 or 10.0.1.22, depending on which network they reside on.

■ In network extension mode, all SOHO PCs on the Hardware Client network are uniquely addressable via the tunnel. This allows direct connection to devices behind the Hardware Client. It enables Management Information Systems (MIS) personnel at the central site to directly address devices behind the Hardware Client over the IPSec tunnel. Most companies use the Hardware Client in network extension mode.

**Remote Access Tunneling—Hardware Client Mode**

Cisco.com

VPN private IP
10.0.1.5

Internet  ISP  Hardware Client

VPN public IP
192.168.1.5

NIC IP address
172.26.26.1

192.168.1.5
172.26.26.1
ESP
10.0.1.10
10.0.1.12
Data

Application
server
10.0.1.10

Client IP
address
10.0.1.12

PC IP address
192.168.10.2

PAT

CSVPN 4.0—10-7

In the figure, there is a small remote office with a Hardware Client and a PC. The remote PC needs to access information on the application server. To provide secure communications, the information is sent over an IPSec tunnel using an IP-in-IP encapsulation. There are three components to the IP-in-IP encapsulation:

■ Outside header—Used to route the information through the network. The addresses used represent the two ends of the tunnel. The source address is the Hardware Client NIC card: 172.26.26.1. The destination address is the Concentrator's public interface: 192.168.1.5. These two addresses are used to route the traffic through the Internet.

■ Inside header—The inside header represents the two end points of the conversation. In this case, a PC at the remote office is accessing a server on the corporate LAN. The source address is the Hardware Client virtual IP address: 10.0.1.12. The Concentrator or Dynamic Host Configuration Protocol (DHCP) server usually supplies this address to the Hardware Client. The Hardware Client translates the SOHO PC's address, 192.168.10.2, to the virtual IP address, 10.0.1.12 port 10000 via PAT. This gives the client the appearance of being a resident on the private network. PAT hides the actual PC address from the outside world. The destination address is the application server on the customer's private network: 10.0.1.10.

■ Encapsulating Security Protocol (ESP) header—To keep the payload private, the inner header and data payload is encrypted and encapsulated via an ESP header. The ESP header indicates to the receiver that the payload is IPSec-encapsulated data. At the central site, the Concentrator strips the outer header, decrypts the data, and forwards the packet according to the inside IP address.

**Hardware Client—Physical Connections**

Cisco.com

**Hardware reset switch**

**Power**

MODEL CVPN 3002

**Internet**

VPN public IP
172.26.26.1

VPN private IP
192.168.10.5

192.168.10.11

**Console port**

CSVPN 4.0—10-8

The Hardware Client is equipped with a universal power factor correction, 100-240 VAC, external power supply. A power cord with the correct plug is supplied. When the Hardware Client arrives from the factory, plug it in and power it up. Connect the SOHO PC or local LAN to the Hardware Client's private interface. Cable the Internet side of the network to the public interface of the Hardware Client. Plug a PC into the console port. The serial port needs to be configured for 9600 8N1.

**Hardware Client—Configuration Options**

When the Hardware Client physical hardware is connected, the administrator must gain access to the Hardware Client manager. The Hardware Client comes from the factory with a private interface IP address of 192.168.10.1. Hook up a PC to the private port and configure the PC's TCP/IP address. To gain access to the Hardware Client, point the browser to the IP address of the private interface, http//192.168.10.1. Log in using **admin/admin**. No CLI intervention is required.

However, if you would rather configure the Hardware Client via CLI or if you need to change the default address on the private LAN interface, you can use the CLI. The default serial port setting is 9600 8N1.

GUI
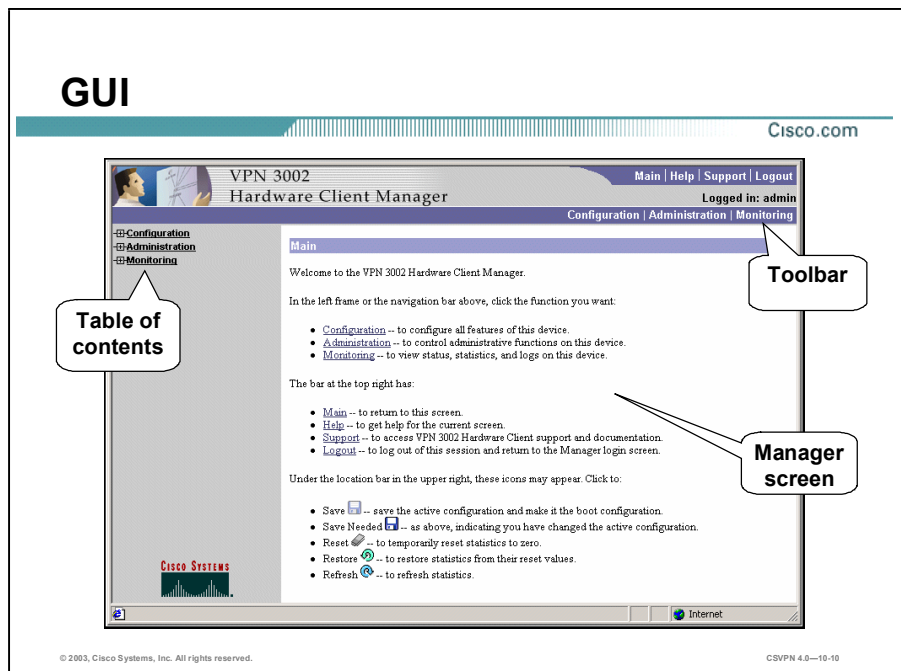
The main window of the Hardware Client manager after logging into the device is made up of the following:

■ The top frame (Hardware Client Manager toolbar) provides quick access to manager functions, configuration, administration, and monitoring.

■ The left frame (table of contents) provides the table of contents to the Manager's windows.

■ The main frame (Manager's) displays the current Hardware Client Manager window. From here you can navigate the Manager using either the table of contents in the left frame or the toolbar at the top of the frame. Select a title on the left frame of the window and the Hardware Client will introduce the manager window for the selected title.

■ Under the location bar, the Save Needed icons may appear. When finished with a configuration window, click **Apply**. Apply allows the configuration to take effect immediately. Click **Save Needed** to save the changes to memory. If you reboot without saving, your configuration changes are lost.

# Quick Configuration

**Configuration | Quick**

| Time | Upload Config | Private Intf | Public Intf | IPSec | PAT | DNS | Static Routes | Admin | Done |

Quick Configuration lets you quickly configure the VPN 3002 for basic connectivity. Use the Main Configuration menu to set advanced options.

You can go through Quick Configuration multiple times. It consists of these steps. You can go through them sequentially, or use the menu bar above.

1. Set the system time, date and time zone.
2. Configure the Ethernet interface to your Private Interface. To use LAN Extension mode, you must configure an IP address other than the default.
3. Optionally upload an already existing configuration file.
4. Configure the Public Interface to a public network.
5. Specify a method for assigning IP addresses.
6. Configure the IPSec tunneling protocol with group and user names and passwords and encryption options.
7. Set the VPN 3002 to use either PAT or LAN Extension mode.
8. Configure DNS.
9. Configure static routes.
10. Change the admin password for security.
11. You're done!

Click to start Quick Configuration

　　　　CSVPN 4.0—10-11

There are two ways to configure the Hardware Client: quick configuration and the main menu. The goal of quick configuration is to provide the minimal parameters needed for operation. Quick configuration guides you through the windows necessary to get a single tunnel up and running. Use the main menu to tune an application or configure features individually. The next windows take you through a sample Hardware Client remote access configuration example using quick configuration. You can access quick configuration from the Configuration>Quick window.

| **Note** | Hardware Client quick configuration can be run multiple times. |

## System Information

Cisco.com

**Configuration | Quick | Time and Date**

Time    Upload Config    Private Intf    Public Intf    IPSec    PAT    DNS    Static Routes    Admin    Done

Set the time on your device. The correct time is very important, so that logging entries are accurate.

The current time on this device is Monday, 18 February 2002 12:48:30.

New Time 12 : 37 : 42  February ▼ / 18 / 2002  (GMT-05:00) EST ▼

☑ Enable DST Support

↵ Click to go back without saving changes

↵ Click to save changes and continue

[ Back ]  [ Continue ]

© 2003, Cisco Systems, Inc. All rights reserved.                    CSVPN 4.0—10-12

There are ten menu selections under quick configuration. The selections can be viewed along the top of the window. The first selection is Time. This window enables the operator to set the time and date on the Hardware Client. The correct time is very important so that logging, certificate verification, and accounting entries are accurate. The window shows the current date and time on the device. The values shown in the New Time fields are the time on the browser PC, but any entries you make apply to the Hardware Client. Enter the year as a four-digit number.

When you click **Continue**, the values are saved to the run time configuration, but not saved in Flash memory. If you remove power from the Hardware Client, the values are lost.

When you click **Done** at the end of the quick configuration menu, the values are automatically saved to the flash memory.

**Configuration Upload**

Cisco.com

The next window, Upload Config, enables you to upload a previously saved configuration file. Browse to the location of the file, and click **Upload**. The Hardware Client checks the file to make sure it is a VPN configuration file. Once the file has been uploaded, reboot the Hardware Client without saving the active configuration, and the uploaded configuration will be loaded as the new run time configuration.

**Private IP Address Interface**

Cisco.com

Ethernet 2 (public IP address)
172.26.26.1

Ethernet 1 (private IP address)
192.168.10.1

Configuration | Quick | Private Interface

Time ✓    Upload Config ✓    **Private Intf**    Public Intf    IPSec    PAT    DNS    Static Routes    Admin    Done

⚠ You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

IP Address 192.168.10.1/ 255.255.255.0
DHCP Server Disabled

**Do you want to configure the IP address of the Private Interface?**
○ Yes
⊙ No

**Do you want to use the DHCP server on Interface 1 to provide addresses for the local LAN?**
○ Yes, and configure the DHCP server parameters.
○ Yes, but leave the DHCP server parameters as is.
⊙ No, do not use the DHCP server to provide addresses.

⤶ Click to go back without making any changes
⤶ Click to make changes and continue

[ Back ] [ Continue ]

© 2003, Cisco Systems, Inc. All rights reserved.      CSVPN 4.0—10-14

The next window is Private Interface. The top of the window displays the current IP address and status of the DHCP server. In this case, the default private IP address is used, 192.168.10.1, and the DHCP server is disabled.

The middle section of the window deals with the IP address of the private interface. For the question, "Do you want to configure the IP address of Interface 1 (Private)?" you can change the interface address by selecting **Yes**. Modifying the address breaks the management connection. You can accept the IP address by selecting **No**. The default IP address is 192.168.10.1.

The bottom section of the window prompts you for the DHCP server parameters. For the question "Do you want to use DHCP server on Interface 1 to provide addresses for the local LAN?", you can select one of the following choices:

■ Yes, and configure the DHCP server parameters—Enables the Hardware Client to act as a DHCP server and enables you to change the DHCP address pool.

■ Yes, but leave the DHCP server parameters as is—Enables you to use the Hardware Client as a DHCP server without changing the default pool. If enabled, the default pool can be viewed at the top of the figure above (for example, DHCP Server Enabled [192.168.10.1-192.168.10.128]).

■ No, do not use the DHCP server to provide addresses—Disables the DHCP server on the Hardware Client.

**Public IP Address Interface**
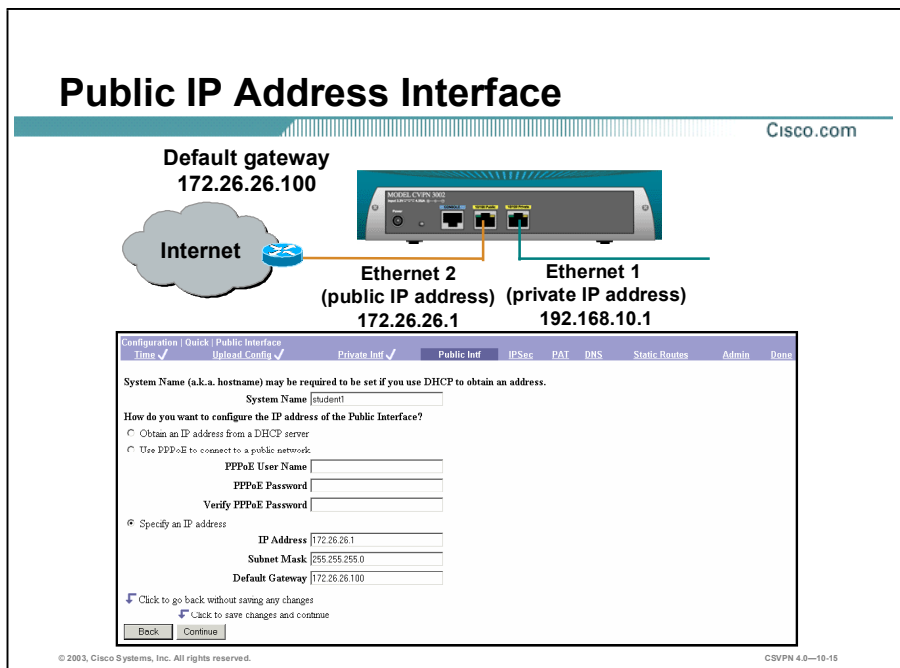
The fourth window is used to define a system name for the Hardware Client and obtain an IP address for the public interface. There are three ways to configure the IP address for the public interface: get an address from a DHCP server, use Point-to-Point Tunneling Protocol (PPP) over Ethernet (PPPoE) to connect, or define a static IP address. The configuration options of the public interface IP address are as follows:

- DHCP Client—The Hardware Client can act as a DHCP client. Select **obtain an IP address from a DHCP server** to receive an address from a DHCP server.

- PPPoE Client—If you want to connect to your Internet provider using PPPoE, select **use PPPoE to connect to a public network** and then enter information in the following fields:

  — PPPoE User Name—Enter a valid PPPoE username.

  — PPPoE Password—Enter the PPPoE password for the username you entered above.

  — Verify PPPoE Password—Enter the PPPoE password again to verify it.

- Static IP Address—Select **specify an IP address** to use a static IP Address, and enter the information in the following fields:

  — IP Address—Enter the IP address for this interface, using dotted decimal notation (for example, 172.26.26.1). Note that 0.0.0.0 is not allowed.

  — Subnet Mask—Enter the subnet mask for this interface using dotted decimal notation (for example, 255.255.255.0). The Manager automatically supplies a standard subnet

mask appropriate for the IP address you just entered. You can accept this entry or change it. Note that 0.0.0.0 is not allowed.

— Default Gateway—Enter the IP address of the system to which the Hardware Client should route packets that are not explicitly routed. In other words, if the Hardware Client has no IP routing parameters that specify where to send a packet, it will send it to this gateway. This address must not be the same as the IP address configured on any Hardware Client private interface.
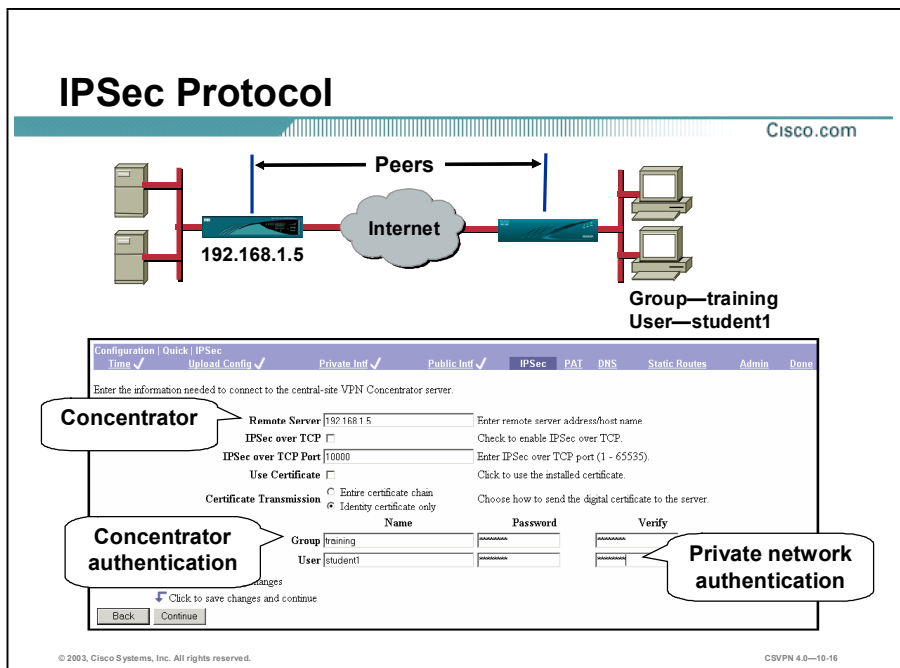
The IPSec window enables you to configure the IPSec parameters, which allows the Hardware Client to connect to the Concentrator over a secure VPN tunnel. The IPSec fields are configured as follows:

■ Remote Server field—Enter the IP address of the Concentrator to which this Hardware Client connects (for example, 192.168.1.5).

■ IPSec over TCP—Encapsulates encrypted data traffic within TCP packets. This feature enables the Hardware Client to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or IKE (UDP 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and enables secure tunneling through both Network Address Translation (NAT) and PAT devices and firewalls.

— IPSec over TCP—Enables IPSec connections using TCP encapsulation. This feature must also be enabled on the Concentrator to which this Hardware Client connects.

— IPSec over TCP Port—Enter the IPSec over TCP port number. You can enter one port. The port that you configure on the Hardware Client must also be configured on the Concentrator to which this Hardware Client connects.

■ Use certificate field—Select the **Use Certificate** check box to use digital certificates for authentication. If you are using digital certificates, there is no need to enter a group name and group password. The Hardware Client checks certificates loaded in the Hardware Client. If no certificate is loaded, an error message opens after you click the **Continue** button.

- ■ Certificate Transmission field—If you configured authentication using digital certificates, choose the type of certificate transmission.

  - — Entire certificate chain—Sends the identity certificate and all issuing certificates to the peer. Issuing certificates include the root certificate and any subordinate CA certificates.

  - — Identity certificate only—Sends only the identity certificate to the peer.

- ■ Group Fields—If you are not using digital certificates, in the Group fields, enter a unique name and password for this group. This is the same group name and password that you configured for this Hardware Client on the central-site Concentrator (for example, training). If the Hardware Client group name and password matches the entries in the Concentrator database, the user gains entrance to the Concentrator.

- ■ User field—In the User Name and Password field, enter a unique name and password for the Hardware Client user. This is the same username and password that you configured in the authentication server (for example, student1). If the Hardware Client username and password matches the entries in the authentication server database, the user gains entrance to the corporate network.

PAT

Cisco.com
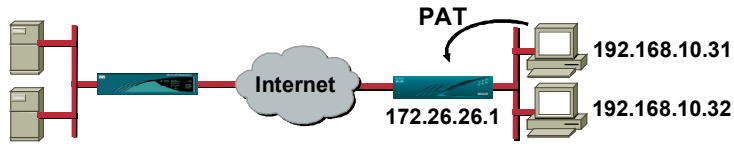
You use this window to configure this Hardware Client to use either Port Address Translation (PAT) or network extension mode. In the example within the figure, because the operator did not change the IP address of the private interface, the interface requires that PAT be enabled over the tunnel.

| Note | You cannot disable PAT if you have not changed the IP address for the private interface. |
| --- | --- |

# DNS

Cisco.com

boston01 — Internet — ISP — DNS

192.168.10.31
192.168.10.32
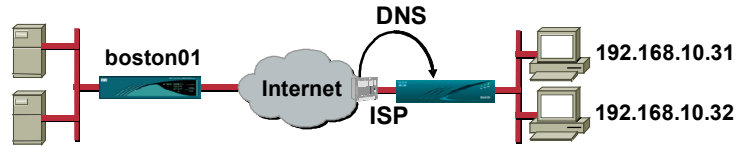
Configuration | Quick | DNS
Time ✓   Upload Config ✓   Private Intf ✓   Public Intf ✓   IPSec ✓   PAT ✓   DNS   Static Routes   Admin   Done

Configure the ISP's DNS server IP address. Enter 0.0.0.0 to not use DNS.

DNS Server [0.0.0.0]
Domain [          ]

⌐ Click to go back without making any changes
   ⌐ Click to make changes and continue

[ Back ]  [ Continue ]

CSVPN 4.0—10-18

This window enables you to specify a Domain Name System (DNS) server. This enables you to enter Internet hostnames (for example, boston01), rather than IP addresses for servers as you configure and manage the Hardware Client. While hostnames are easier to remember, using IP addresses avoids problems that might arise if the DNS server goes offline, gets congested, and so on. If you use a hostname to identify the central-site Concentrator, you must configure a DNS server.

## Static Routes

Cisco.com
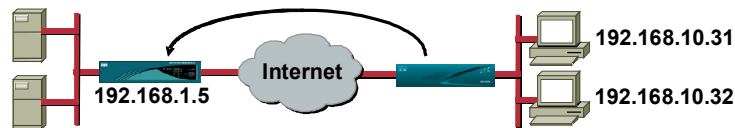
**192.168.10.31**

**192.168.10.32**

**192.168.1.5**

Internet

Configuration | Quick | Static Routes

Time ✓     Upload Config ✓     Private Intf ✓     Public Intf ✓     IPSec ✓     PAT   DNS   **Static Routes**   Admin   Done

This section lets you configure static routes for IP routing.

**Static Routes**          **Actions**

Default -> 192.168.1.5

| Add | a route to the routing table. |
| Delete | a route from the routing table. |
| Back | to the previous section. |
| Continue | to the next section. |

© 2003, Cisco Systems, Inc. All rights reserved.                    CSVPN 4.0—10-19

This section enables you to configure static routes for IP routing. The Hardware Client does not support Routing Information Protocol (RIP) or Open Shortest Path First (OSPF). A static route must be supplied. This window displays current static route as defined under the IPSec— remote server parameter. In the example in the figure, all Hardware Client traffic is routed to 192.168.1.5, the Concentrator's public interface.

In this window, you can take the following possible actions:

■ Add—Click **Add** to add a route to the routing table.

■ Delete—Select a route in the Static Routers field, and click **Delet**e to delete a route.

■ Back—Go to the previous quick configuration window.

■ Forward—Go to the next quick configuration window.

# Admin Password
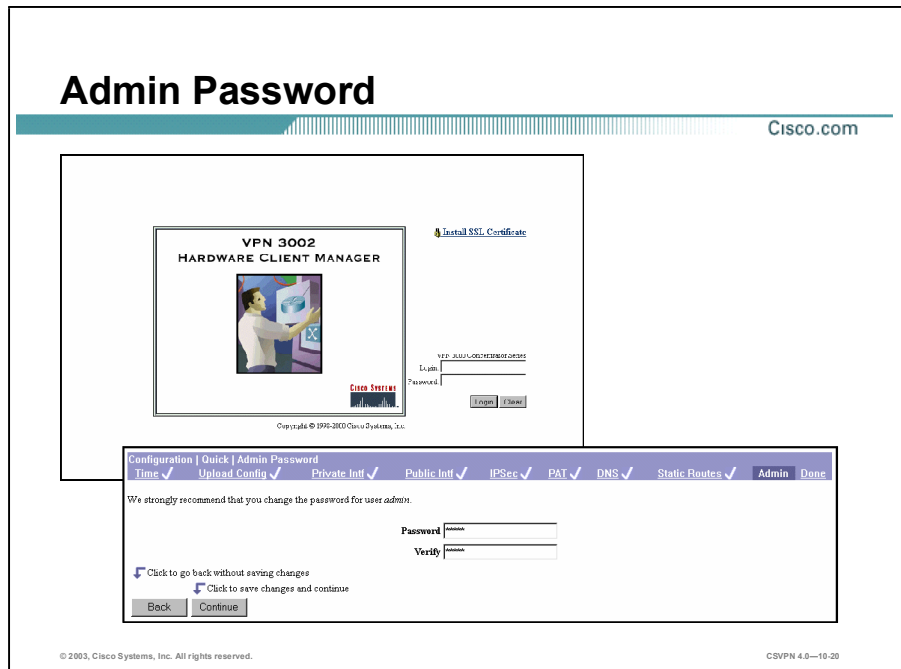


This window enables you to change the password for the administrator. For ease of use during startup, the default administrator password supplied with the Hardware Client is admin. Because the administrator has full access to all management and administration functions on the device, it is strongly recommended that you change this password to improve device security. The administrator parameters are as follows:

■ Password—Enter or edit the unique password for this administrator. The field displays only asterisks. The default password that Cisco supplies is the same as the username. It is strongly recommended that you change this password.

■ Verify—Re-enter the password to verify it. The field displays only asterisks.

There is a reset password utility, which enables you to reset the password to the default. After you reboot the system and the diagnostic check is complete, a line of three dots (…) appears on the console. Clicking **Control Break** within three seconds after seeing the three dots displays a new menu that enables you to reset the system passwords back to the default.

**Access Rights**

Cisco.com

Hardware
Client

Administration | Access Rights | Administrators

This section presents administrator users. Any changes you make take effect immediately.

Administrator *admin*    Password
                         Verify
Administrator *config*   Enabled ☐
                         Password
                         Verify
Administrator *monitor*  Enabled ☐
                         Password
                         Verify

Apply    Cancel

© 2003, Cisco Systems, Inc. All rights reserved.                                CSVPN 4.0—10-21

You can further configure all administrators under main menu in the Configuration>Access
Rights>Administrators window. The Hardware Client has three levels of graphical user
interface (GUI) access: admin, config, and monitor. Within these three levels, a user can do the
following:

- Administrator Admin—Can do everything

- Administrator Config—Quick configuration and monitoring (by default it is disabled)

- Administrator Monitor—Monitoring windows only (by default it is disabled)

The Configuration>Access Rights>Administrators window enables the administrator to enable
or disable access levels and change passwords. By default, the only enabled level is admin.
Selecting the **Enabled** check box and entering a password can activate additional levels.

Launching the Client
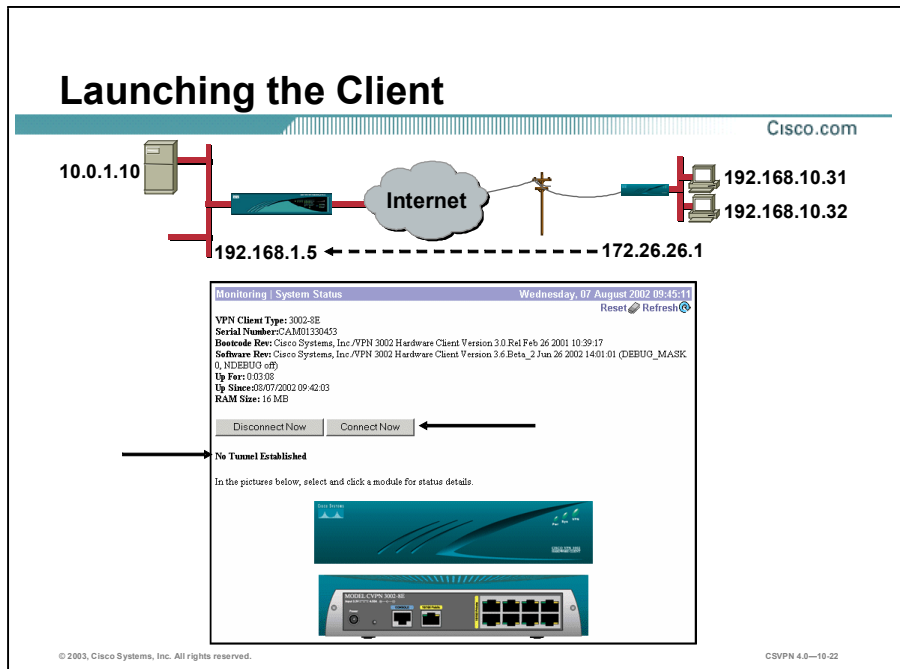
In the figure, the Hardware Client mode is complete. It is time to launch the tunnel. By default in client mode, no tunnel is established. You must manually initiate the tunnel. There are two ways to do this:

■ Click **Connect Now** in the Monitoring>System Status window.

■ Sending traffic to the hardware client destined for the remote end.

You can verify that the tunnel is established by trying to ping an interface on the remote Concentrator. The Hardware Client recognizes the remote-bound traffic and attempts to establish a tunnel. If a tunnel is established, it is viewable on this window. If the tunnel does not appear in the window, check the event log of the Hardware Client and the Concentrator.

**Hardware Client—Monitoring System Status**
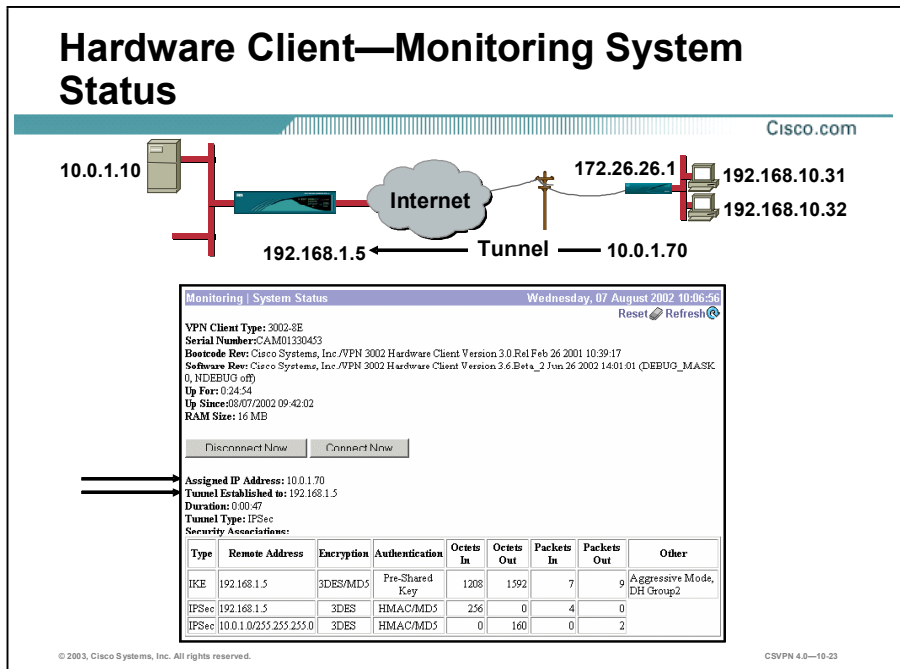
The Monitoring>System Status window on the Hardware Client enables the administrator to launch the tunnel, check the status of the tunnel and Hardware Client hardware. The top portion of the window displays the Hardware Client hardware information, such as software revision, RAM size, and up time information. The middle portion enables the administrator to connect and disconnect the tunnel by clicking the **Connect Now** and **Disconnect Now** buttons. If a tunnel is established, the bottom portion of the window displays tunnel information, such as the assigned IP address, the tunnel established, the duration time, and security associations (SAs).

In the example within the figure, a tunnel was established to a Concentrator whose public interface address is 192.168.1.5. The virtual address assigned to the client by the Concentrator is 10.0.1.70. The tunnel has been up for 47 seconds. In the SA table, the encryption method is Triple Data Encryption Standard (3DES) while the authentication method is Message Digest 5 (MD5).

The session information is also available on the Concentrator by going to the Monitoring>Sessions window.

The Monitoring>Sessions window enables the administrator to view session information. In the third portion of the window, Remote Access Sessions, you can view statistics for the Hardware Client-to-Concentrator tunnel. The following information is included:

■ Username—The username or login name for the session.

■ Public IP address—The public IP address of the client for this remote access session. This is also known as the outer IP address.

■ Assigned IP address—The private IP address assigned to the remote client for this session. This is also known as the "inner "or virtual IP address.

■ Group—The user's group.

■ Protocol—The protocol this session is using.

■ Encryption—The data encryption algorithm this session is using.

■ Login Time—The date and time (MM DD HH:MM:SS) that the session logged in.

■ Duration—The elapsed time (HH:MM:SS) between the session login time and the last window refresh.

■ Client Type—The client type of connected.

■ Version—The software version number (for example, 3.6.Rel) for connected clients.

■ Bytes Transmitted and Received—The total number of bytes transmitted to and received from the remote peer by the Concentrator.

Click the username, in this example the username is student3, to get more detailed information on the session.

Cisco.com

10.0.1.10

192.168.10.31
192.168.10.32

Internet

172.26.26.1
10.0.1.70

192.168.1.5 ← Tunnel

| Username | Public IP Address | Assigned IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx |
|---|---|---|---|---|---|---|---|---|
| student1 | 172.26.26.1 | 10.0.1.70 | IPSec | 3DES-168 | Aug 07 08:18:25 | 0:04:09 | 109840 | 31936 |

IKE Sessions: 1
IPSec Sessions: 2

| IKE Session | | | |
|---|---|---|---|
| Session ID | 1 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Diffie-Hellman Group | Group 2 (1024-bit) |
| Authentication Mode | Pre-Shared Keys (XAUTH) | IKE Negotiation Mode | Aggressive |
| Rekey Time Interval | 86400 seconds | | |

| IPSec Session | | | |
|---|---|---|---|
| Session ID | 2 | Remote Address | 172.26.26.1 |
| Local Address | 192.168.1.5 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Idle Time | 0:02:05 |
| Encapsulation Mode | Tunnel | Rekey Time Interval | 28800 seconds |
| Bytes Received | 144 | Bytes Transmitted | 400 |

| IPSec Session | | | |
|---|---|---|---|
| Session ID | 3 | Remote Address | 10.0.1.70 |
| Local Address | 10.0.1.0/0.0.0.255 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Encapsulation Mode | Tunnel |
| Rekey Time Interval | 28800 seconds | | |
| Bytes Received | 31792 | Bytes Transmitted | 112048 |

CSVPN 4.0—10-25

The administrator can also monitor VPN-to-Concentrator sessions from the Concentrator. The Monitoring>Session>Details window enables the administrator to get more in-depth information about the session, such as the hashing algorithm, authentication mode, encryption algorithm, and Diffie-Hellman (DH) group. The top line is a repetition of the remote access session entry. Below the remote entry session, the window is divided into IKE and IPSec sessions.

The first session is the IKE session. This session displays the details of the IKE tunnel establishment. It displays such details as hashing algorithm, encryption algorithm, authentication method, rekey interval, Diffie-Hellman group, and IKE negotiation mode. The next sessions detail the IPSec sessions. Displayed are the attributes of the IPSec session to include the local and remote IP address, hashing and encryption algorithms, encapsulation mode, rekey interval, and so on.

In the figure above, the tunnel is established between the public interfaces of the Concentrator, 192.168.1.5 and the Hardware Client, 172.26.26.1. When traffic flows, it flows between the central site LAN, 10.0.1.0, to a PAT address on the Hardware Client's private network, 10.0.1.70. The remote PC's IP address is changed to 10.0.1.70 and given a UDP port number. The remote PC's IP address is hidden from the outside. Hosts on the Hardware Client are not directly addressable from the central site.

# Network Extension Mode

**Network extension mode**

Internet

192.168.1.5

10.0.1.10

172.26.26.10

192.168.10.10

192.168.10.12
192.168.10.13

172.26.26.20

192.168.20.10

192.168.20.12
192.168.20.13
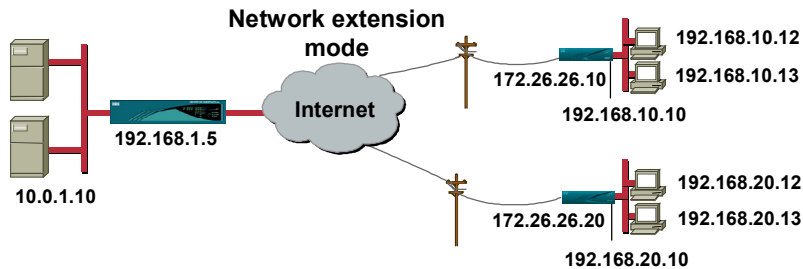
CSVPN 4.0—10-26

In network extension mode, all PCs on the Hardware Client are uniquely addressable via the tunnel. This enables MIS personnel at the central site to directly address devices behind the Hardware Client over the IPSec tunnel.

To implement network extension mode, the Hardware Client must be reconfigured. Programming network extension mode is a three-step process. First, network extension mode must be enabled on the Concentrator. Next, the IP address of the Hardware Client's private interface must be changed from the factory default. (If it is left in default, the network extension mode is disabled.). Lastly, network extension must be enabled on the Hardware Client.

# Concentrator—Hardware Client Tab

Cisco.com

10.0.1.10

Internet

172.26.26.1

192.168.10.31
192.168.10.32
192.168.10.10

**Configuration | User Management | Groups | Modify training**

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

| Hardware Client Parameters | | | |
|---|---|---|---|
| Attribute | Value | Inherit? | Description |
| Require Interactive Hardware Client Authentication | ☐ | ☐ | Check to require the hardware client to be interactively authenticated at each connection attempt. |
| Require Individual User Authentication | ☐ | ☐ | Check to require users behind a hardware client to be authenticated. |
| User Idle Timeout | 30 | ☑ | Enter the session idle timeout in minutes. Use 0 for no timeout. |
| Cisco IP Phone Bypass | ☐ | ☑ | Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client. |
| Allow Network Extension Mode | ☑ | ☐ | Check to allow hardware clients using Network Extension Mode to connect. |

Apply    Cancel

© 2003, Cisco Systems, Inc. All rights reserved.    CSVPN 4.0—10-27

By default, a Hardware Client cannot automatically connect to a Concentrator. The administrator must allow remote Hardware Clients using network extension to connect to a Concentrator on a group-by-group basis. From the Concentrator, go to **Configuration>User Management>Groups>Modify** to enable network extension mode. Under the HW Client tab, select the **Allow Network Extension Mode** check box. The feature is disabled by default.

## Quick Configuration—IP Address

Cisco.com
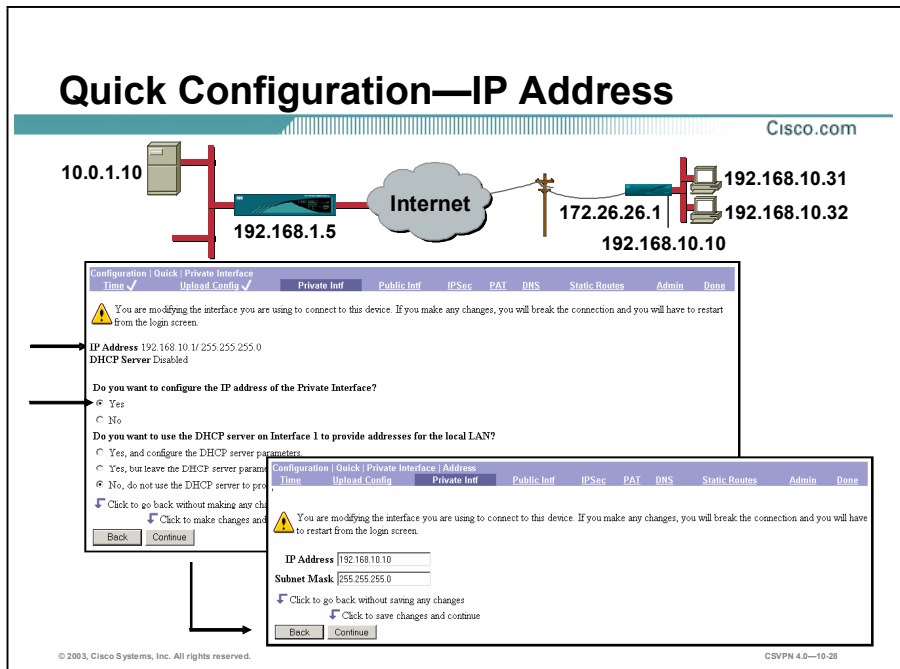
The next step in configuring network extension mode is to change the IP address of the private interface. Choose the Configuration>Quick>Private Interface window to reconfigure the IP address. Notice near the top of the window, the current IP address is 192.168.10.1, which is the default. When the GUI prompts you with the question, "Do you want to configure the IP address of the Private interface?" you have the following choices:

■ You can accept the default IP address. If you do this, you are locked into the client mode.

■ You can change the IP address. If you change the IP address of the private interface, you can choose between client or network extension modes (configured under the Quick Configuration>PAT window). In the figure, Yes because we want to use network extension mode is selected. Click **Continue**.

A window opens and prompts you for the new IP address and subnet mask. Fill in the new values and click **Continue**. If you make changes, you will break the connection. Make the necessary changes to the gateway value of your PC and restart the GUI from the login window.

**Quick Configuration—Network Extension Mode**

The last step is to configure the Hardware Client for network extension mode. In the Configuration>Quick>Public Interface, the address of the interface was changed. Use the Configuration>Quick>PAT window to enable either PAT or network extension modes. If you select **Yes**, you get PAT and client mode. If you select **No**, you opt for network extension mode. In this case, **No** was selected, which enables network extension mode. When the IPSec session is established, the data flows between the Concentrator and the private interface of the Hardware Client: 192.168.10.1.5 to 192.168.10.10.

# Hardware Client—Monitor Status

Cisco.com

10.0.1.10

Internet

192.168.1.5

172.26.26.1

192.168.10.31
192.168.10.32
192.168.10.10

Tunnel

| Monitoring | System Status | Wednesday, 07 August 2002 10:16:59 |
| Reset 🖉 Refresh 🔄 |

**VPN Client Type:** 3002-8E
**Serial Number:** CAM01330453
**Bootcode Rev:** Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.0.Rel Feb 26 2001 10:39:17
**Software Rev:** Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.6.Beta_2 Jun 26 2002 14:01:01 (DEBUG_MASK 0, NDEBUG off)
**Up For:** 0:34:57
**Up Since:** 08/07/2002 09:42:02
**RAM Size:** 16 MB

[ Disconnect Now ]   [ Connect Now ]

**Tunnel Established to:** 192.168.1.5
**Duration:** 0:00:22
**Tunnel Type:** IPSec
**Security Associations:**

| Type | Remote Address | Encryption | Authentication | Octets In | Octets Out | Packets In | Packets Out | Other |
|------|----------------|------------|----------------|-----------|------------|------------|-------------|-------|
| IKE | 192.168.1.5 | 3DES/MD5 | Pre-Shared Key | 1192 | 1592 | 7 | 9 | Aggressive Mode, DH Group2 |
| IPSec | 192.168.1.5 | 3DES | HMAC/MD5 | 0 | 0 | 0 | 0 | |
| IPSec | 10.0.1.0/255.255.255.0 | 3DES | HMAC/MD5 | 192 | 192 | 3 | 3 | |

CSVPN 4.0—10-30

When the private IP address is changed and the network extension mode is enabled, the tunnel is automatically established. You can view the tunnel status from the Monitoring>System Status window on the Hardware Client. A tunnel was established between the Concentrator, 192.168.1.5, and the Hardware Client, 192.168.10.10. The duration is the time the tunnel has been up. To update the window and its data, click **Refresh**.

For SAs, the following information is available:

- IKE SA—The SA establishes secure communications between the Hardware Client and the Concentrator.

- IPSec SA—From the public port on the Hardware Client to the public port of the Concentrator.

- IPSec SA—There is one more SA for any data streams between PCs on the corporation's private network. This last SA is only viewable if traffic is passing between the Hardware Client and the Concentrator. In the figure above, there is no data traffic.

---

**Note**    In Client mode, the Concentrator passes an assigned address to the Hardware Client during IPSec tunnel establishment. This address is the remote IP address. This assigned address is viewable from the Monitoring>System Status window. In Network Extension mode, the Hardware Client uses the private IP network address as the remote IP address. An assigned address is not applicable in this mode and is not present in the Monitoring>System Status window.

---

# Concentrator—Monitor Session

Cisco.com

10.0.1.10

192.168.1.5

Internet

172.26.26.1

192.168.10.10

192.168.10.31
192.168.10.32

**Session Summary**

| Active LAN-to-LAN Sessions | Active Remote Access Sessions | Active Management Sessions | Total Active Sessions | Peak Concurrent Sessions | Concurrent Sessions Limit | Total Cumulative Sessions |
|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 2 | 3 | 100 | 18 |

**LAN-to-LAN Sessions**     [ Remote Access Sessions | Management Sessions ]

| Connection Name | IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx |
|---|---|---|---|---|---|---|---|
| No LAN-to-LAN Sessions | | | | | | | |

**Remote Access Sessions**     [ LAN-to-LAN Sessions | Management Sessions ]

| Username | Assigned IP Address Public IP Address | Group | Protocol Encryption | Login Time Duration | Client Type Version | Bytes Tx Bytes Rx |
|---|---|---|---|---|---|---|
| student1 | 192.168.10.0 172.26.26.1 | training | IPSec 3DES-168 | Aug 7 9:28:52 0:01:44 | VPN 3002 3.6.Beta_2 | 39560 12096 |

**Management Sessions**     [ LAN-to-LAN Sessions | Remote Access Sessions ]

| Administrator | IP Address | Protocol | Encryption | Login Time | Duration |
|---|---|---|---|---|---|
| admin | 172.26.26.1 | HTTP | None | Aug 07 08:30:28 | 0:00:07 |

It is also possible to view the session information from the Concentrator's end of the tunnel. Choose the Monitoring>Sessions window to view the tunnel status. Under the Remote Access Sessions group window, the following IPSec tunnel information is available:

■ User Name—The username or login name for the session.

■ Public IP Address—The IP address of the public interface of the Hardware Client.

■ Assigned IP Address—The private virtual IP address assigned to Hardware Client for this session. In Network Extension mode, the assigned IP address is the Hardware Client's private network address, 192.168.10.0.

■ Group—The group assigned to the Client.

■ Protocol—The protocol this session is using.

■ Encryption—The data encryption algorithm this session is using.

■ Login Time—The date and time (MM DD HH:MM:SS) that the session logged in.

■ Duration—The elapsed time (HH:MM:SS) between the session login time and the last window refresh.

■ Client Type—The type of client that is connected.

■ Version—The software version number (for example, 3.6.Rel) for connected clients.

- Bytes Transmitted and Received—The total number of bytes transmitted to and received from the remote peer by the Concentrator.

An administrator can receive more details on the sessions by selecting a specific username.

10.0.1.10

192.168.1.5

Internet

172.26.26.1

192.168.10.10

192.168.10.31
192.168.10.32

| Username | Public IP Address | Assigned IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx |
|---|---|---|---|---|---|---|---|---|
| student1 | 172.26.26.1 | 192.168.10.0 | IPSec | 3DES-168 | Aug 07 08:28:52 | 0:02:35 | 48448 | 17848 |

IKE Sessions: 1
IPSec Sessions: 2

### IKE Session

| | | | |
|---|---|---|---|
| Session ID | 1 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Diffie-Hellman Group | Group 2 (1024-bit) |
| Authentication Mode | Pre-Shared Keys (XAUTH) | IKE Negotiation Mode | Aggressive |
| Rekey Time Interval | 86400 seconds | | |

### IPSec Session

| | | | |
|---|---|---|---|
| Session ID | 2 | Remote Address | 172.26.26.1 |
| Local Address | 192.168.1.5 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Idle Time | 0:02:35 |
| Encapsulation Mode | Tunnel | Rekey Time Interval | 28800 seconds |
| Bytes Received | 0 | Bytes Transmitted | 0 |

### IPSec Session

| | | | |
|---|---|---|---|
| Session ID | 3 | Remote Address | 192.168.10.0/0.0.0.255 |
| Local Address | 10.0.1.0/0.0.0.255 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Encapsulation Mode | Tunnel |
| Rekey Time Interval | 28800 seconds | | |
| Bytes Received | 17848 | Bytes Transmitted | 51808 |

CSVPN 4.0—10-32

The Monitoring>Session>Details window enables the administrator to view more in-depth information about the session, such as the hashing algorithm, authentication mode, encryption algorithm, and DH group. The top line is the remote access session entry from the previous window, Monitoring>Sessions> Remote Access Sessions. Below the remote entry session, the window is divided into IKE and IPSec sessions.

The first session is the IKE session. This part displays the details of the IKE tunnel establishment. It displays such details as hashing algorithm, encryption algorithm, authentication method, rekey interval, DH group, and IKE negotiation mode. The next two sections detail the IPSec sessions. Displayed are the attributes of the IPSec session to include the local and remote IP address, hashing and encryption algorithms, encapsulation mode, Rekey interval, and so on.

In the figure, the tunnel is established between the public interfaces of the Concentrator and the Hardware Client as documented under the first IPSec session. When traffic flows, it flows between any address on the central site LAN and hosts on the Hardware Client private network, 192.168.10.10/0.0.0.255, as documented under the second IPSec session. In this case, any hosts on the Hardware Client are addressable from the central site.

# Summary

This topic summarizes what you learned in this lesson.

## Summary

Cisco.com

- **The Cisco VPN 3002 Hardware Client supports two modes: client and network extension.**
- **Client mode will translate the PC IP address via PAT. All traffic from private networks appears as a single-source IP address.**
- **In network extension mode, all PCs are uniquely addressable via the tunnel.**

© 2003, Cisco Systems, Inc. All rights reserved.　　　　　　　　　　　　　　　　CSVPN 4.0—10-34

# Lab Exercise—Configuring Cisco VPN 3002 Hardware Client Remote Access

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to install and configure the Cisco Virtual Private Network (VPN) 3002 Hardware Client and configure the Cisco VPN 3000 Series Concentrator to enable VPN encrypted tunnels. Work with your lab exercise partner to complete the following tasks:

■ Reconfigure the student PC networking parameters.

■ Return the Cisco VPN 3002 Hardware Client to factory settings.

■ Configure the Cisco VPN 3002 Hardware Client using the VPN 3002 Hardware Client Manager.

■ Configure the Cisco VPN 3002 Hardware Client event monitoring.

■ Launch the Cisco VPN 3002 Hardware Client VPN tunnel.

■ Update the Cisco VPN 3002 Hardware Client system software.

■ Monitor the Cisco VPN 3000 Series Concentrator statistics.

■ Return the Cisco VPN 3002 Hardware Client to factory settings.

■ Configure the Cisco VPN 3002 Hardware Client private interface.

■ Configure the Cisco VPN 3002 Hardware Client for network extension mode.

■ Launch the Cisco VPN 3002 Hardware Client VPN tunnel.

■ Monitor the Cisco VPN 3000 Series Concentrator statistics.

# Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
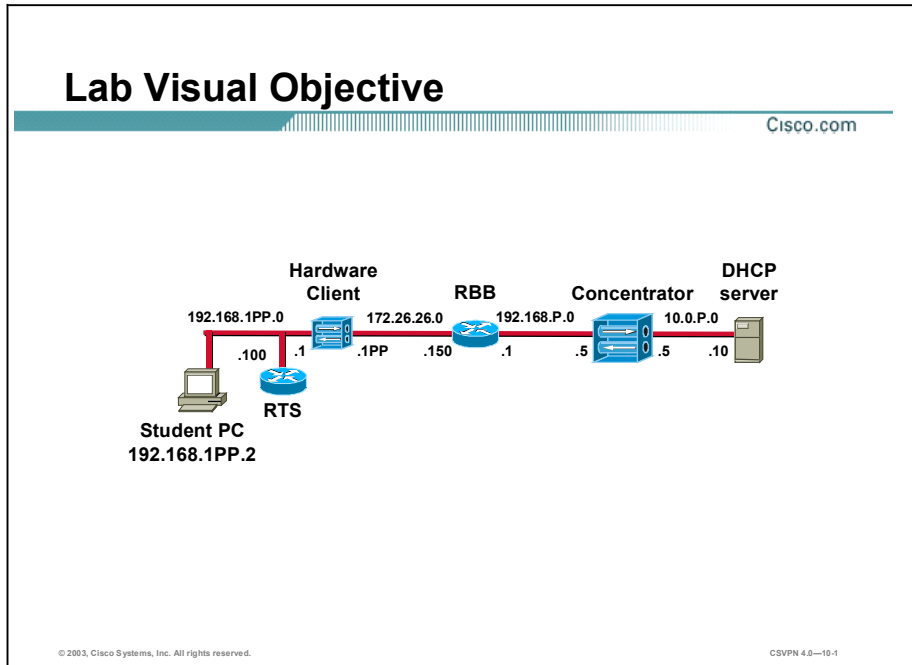


# Scenario

Your company wants you to implement a Cisco VPN using remotely located Hardware Clients terminating at centrally located Concentrators. You must configure both the Concentrator and the Hardware Client for remote access using both client mode and network extension mode.

# Task 1—Reconfigure the Student PC Networking Parameters

Certain networking parameters must be reconfigured before your student PC will communicate with a Hardware Client. Use the following information to reconfigure your student PC networking parameters.

(If you are not sure which IP addresses to use, ask your instructor.)

■ Primary IP address—**192.168.1PP.2**
(where PP = two-digit pod number [for example, Pod 1 is 01])

■ Default gateway IP address—**192.168.1PP.1**
(where PP = two-digit pod number [for example, Pod 1 is 01])

## Task 2—Return the Cisco VPN 3002 Hardware Client to Factory Settings

The instructor will provide you with the procedures for access to the Hardware Client console port, as this will vary according to your lab connectivity. After you access the Hardware Client console port, the Hardware Client login prompt will appear. Complete the following steps to return the Hardware Client to the factory settings:

| Note | This procedure assumes that Windows 2000 is already running on the student PC. |
|------|------|

**Step 1** Log in to the Hardware Client command line interface (CLI) using the administrator account:

```
Login: admin
Password: admin
```

**Step 2** Complete the following sub-steps starting from the CLI top-level menu:

1. Access the Administration menu:

```
Main -> 2
```

2. Access the System Reboot menu:

```
Admin -> 2
```

3. Access the Schedule Reboot menu:

```
Admin -> 2
```

4. Select Reboot ignoring the Configuration file:

```
Admin -> 3
```

5. Select Reboot Now:

```
Admin -> 2
```

It takes several moments for the Hardware Client to reboot. You are automatically logged out of the unit.

**Step 3** Log in to the Hardware Client using the administrator account:

```
Login: admin
Password: admin
```

**Step 4** Complete the following sub-steps, starting from the CLI top-level menu. Ignore the recurring "IP interface 2 was unable to acquire an address via DHCP" message and complete the following steps:

1. Select the Configuration menu:

```
Main -> 1
```

2. Select the Interface Configuration menu:

```
Config -> 2
```

3. Select the Configure the Private Interface menu:

```
Interfaces -> 1
```

4. Select interface setting (Disable or Static IP):

```
Private Interface -> 1
```

5. Select Enable using Static IP Addressing:

```
Private Interface -> 2
```

6. Enter the Cisco VPN 3002 Hardware Client private interface IP address:

```
Private Interface -> [192.168.10.1] 192.168.1PP.1
```

(where PP = two-digit pod number [for example, Pod 1 is 01])

Several messages appear, indicating the condition of the Ethernet #1 (private) interface. Disregard these messages.

7. Enter the Hardware Client private interface mask:

```
Enter Subnet Mask -> [255.255.255.0] Enter
```

8. Return to the top-level menu:

```
Ethernet Interface 1 -> h
```

9. Save changes to the configuration file:

```
Main -> 4
```

10. Exit the CLI:

```
Main -> 6
```

**Step 5**  Close the CLI session.

## Task 3—Configure the Cisco VPN 3002 Hardware Client Using the VPN 3002 Hardware Client Manager

Complete the following steps to finish the Hardware Client configuration using the Hardware Client Manager.

**Step 1**  Launch Internet Explorer by double-clicking the Internet Explorer desktop icon.

**Step 2**  Enter a Hardware Client private interface IP address in the Internet Explorer Address field: **192.168.1PP.1**.
(where PP = two-digit pod number [for example, Pod 1 is 01])

**Step 3**  Log in to the Hardware Client using the administrator account:

Login: **admin**

Password: **admin**

The username (login) and password are always case sensitive.

**Step 4**  In the main window, click the **click here to start Quick Configuration** hyperlink. The Configuration>Quick>Time and Date window opens.

**Step 5**  Complete the following sub-steps from the Configuration>Quick>Time and Date window:

1. View the contents of the window.

2. Click **Continue**.

**Step 6**  Complete the following sub-steps from the Configuration>Quick>Upload Config window:

1. View the contents of the window.

2. Click **No**.

**Step 7**  Complete the following sub-steps from the Configuration>Quick>Private Interface window:

1. Select **No** when you are asked if you wish to configure the IP address of the private interface.

2. Select **No, do not use DHCP server to provide addresses** when you are asked if you want to use DHCP server on the private interface.

3. Click **Continue**.

**Step 8**  Complete the following sub-steps from the Configuration>Quick>Public Interface window:

1. Enter the system name: **studentP**.
   (where P = pod number)

2. Select **Specify an IP address**.

3. Enter a Hardware Client public interface IP address in the IP Address field: **172.26.26.1PP**.
   (where PP = two-digit pod number [for example, Pod 1 is 01])

4. Enter a Hardware Client public interface subnet mask in the Subnet Mask field: **255.255.255.0**.

5. Enter a backbone router IP address in the default gateway field: **172.26.26.150**.

6. Click **Continue**.

**Step 9**  Complete the following sub-steps from the Configuration>Quick>IPSec window:

1. In the Remote Server IP Address field, enter the Concentrator's public interface IP address: **192.168.P.5**.
   (where P = pod number)

2. Verify that Use Certificate is deselected.

3. Enter the group name: **training**.

4. Enter the group password: **training**.

5. Verify the group password: **training**.

6. Enter the username: **studentP**.
   (where P = pod number)

7. Enter the user password: **studentP**.
   (where P = pod number)

8. Verify the user password: **studentP**.
   (where P = pod number)

9. Click **Continue**. It may take a few moments to complete.

**Step 10** Complete the following sub-steps from the Configuration>Quick>Port Address Translation (PAT) window:

1. View the contents of the window. Answer the following question:

Q1) What is the default mode, PAT or Network Extension?

A) _____

2. Click **Continue**.

**Step 11** Complete the following sub-steps from the Configuration>Quick>DNS window:

1. View the contents of the window.

2. Click **Continue**.

**Step 12** Complete the following sub-steps from the Configuration>Quick>Static Routes window:

1. View the contents of the window.

2. Click **Continue**.

**Step 13** Complete the following sub-steps from the Configuration>Quick>Admin Password window:

1. View the contents of the window.

2. Click Continue.

**Step 14** Do not log out of the Hardware Client Manager window, and do not close Internet Explorer.

## Task 4—Configure the Cisco VPN 3002 Hardware Client Event Monitoring

Complete the following steps to configure event monitoring on the Hardware Client:

**Step 1** From the Configuration menu tree, drill down to **System>Events>Classes**.

**Step 2** Click **Add**. The Classes>Add window opens.

**Step 3** Enable logging for the AUTHDBG event class by completing the following sub-steps:

1. Select class name: **AUTHDBG**.

2. Set the Severity to Log: **1–9**.

3. Leave all other fields at their default values.

4. Click **Add**.

**Step 4** Enable logging for the IKEDBG event class by completing the following sub-steps:

1. Click **Add**.

2. Select class name: **IKEDBG**.

3. Set the Severity to Log: **1–9**.

4. Leave all other fields at their default values.

5. Click **Add**.

**Step 5** Enable logging for the **IPSECDBG** event class by completing the following sub-steps:

1. Click **Add**.

2. Select class name: **IPSECDBG**.

3. Set the Severity to Log: **1–9**.

4. Leave all other fields at their default values.

5. Click **Add**.

**Step 6** Save the configuration.

**Step 7** From the Monitoring menu tree, drill down to **Filterable Event Log**.

**Step 8** Click **Clear Log**.

**Step 9** Set Events/page to **ALL**.

**Step 10** Do not logout of the Hardware Client. Do not close Internet Explorer.

## Task 5—Launch the Cisco VPN 3002 Hardware Client VPN Tunnel

Complete the following steps to launch and monitor the Hardware Client VPN tunnel:

**Step 1** From the Monitoring menu tree, drill down to **System Status**. A VPN tunnel should already be established to the Concentrator. If a VPN tunnel is not established, click **Connect Now**. Answer the following questions:

Q2) How can you tell if the tunnel is established?

A) _____

Q3) How many Internet Key Exchange (IKE) sessions were established?

A) _____

Q4) How many IPSec sessions were established?

A) _____

**Step 2** Ping a Concentrator private interface IP address of **10.0.P.5** using the Administration menu tree ping function.

(where P = pod number)

**Step 3** Return to the System Status window and click **Refresh**. Answer the following question:

Q5) Which IPSec tunnel was used to transmit the pings?

A) _____

**Step 4** Do not log out of the Hardware Client. Do not close Internet Explorer.

## Task 6—Update the Cisco VPN 3002 Hardware Client System Software

Complete the following steps to update the Hardware Client system software:

**Step 1** From the Administration menu tree, drill down to **Software Update**. The Administration> Software Update window opens.

**Step 2** Click **Browse**. The Choose File window opens.

**Step 3** Open the desktop TFTP folder.

**Step 4** Select the Cisco VPN 3002 Software file, **vpn3002-4.0.1.Rel-k9.bin**. (If you are unsure which software file to select, ask your instructor for help.)

**Step 5** Click **Open**.

**Step 6** Click **Upload**. The Software Update Progress window opens, followed by the Software Update Success window. Wait until the software update is complete before continuing.

**Step 7** Select **Click here to go to the reboot options**. The Administration>System Reboot window opens.

**Step 8** Select the action to take: **Reboot**.

**Step 9** Select the type of reboot to perform: **Reboot without saving active configuration**.

**Step 10** Select the time to perform the reboot or shutdown: **Now**.

**Step 11** Click **Apply** and wait approximately two minutes for the reboot to complete.

**Step 12** Log in to the Hardware Client Manager using the administrator account:

```
Login: admin
Password: admin
```

**Step 13** From the Monitoring menu tree, drill down to **System Status** and answer the following question:

Q6)    What is the current software revision?

A)    _____

**Step 14** Log out of the Hardware Client Manager.

## Task 7—Monitor the Cisco VPN 3000 Series Concentrator Statistics

Complete the following steps to monitor Concentrator statistics:

**Step 1** Enter a Concentrator's public interface IP address in the Internet Explorer Address field: **192.168.P.5** (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 2** Log in to the Concentrator using the administrator account:

```
Login: admin
Password: admin
```

**Step 3** From the Monitoring menu tree, drill down to **Routing Table**. Answer the following question:

Q7)    Which networks are visible?

---

A) _____

**Step 4**   From the Monitoring menu tree, drill down to **Sessions**, view the Remote Access Sessions window, and complete the following:

1. User name:

   _____

2. Assigned IP address:

   _____

3. Public IP address:

   _____

4. Group:

   _____

5. Protocol:

   _____

6. Encryption:

   _____

7. Login time:

   _____

8. Duration:

   _____

9. Client Type:

   _____

10. Version:

   _____

**Step 5**   Select **studentP** (where P = pod number). More information is displayed.

**Step 6**   View the IKE Session fields and answer the following questions:

Q8)    The encryption algorithm is type?

    A) _____

Q9)    The hashing algorithm is type?

    A) _____

Q10)   The Diffie-Hellman group is?

    A) _____

Q11)   The IKE negotiation mode is?

    A) _____

**Step 7** View the IPSec Session fields and answer the following questions:

Q12) The IPSec session ID 2 was established between what two addresses?

A) Local address:

_____

B) Remote address:

_____

Q13) What is the encryption algorithm type?

A) _____

Q14) What is the hashing algorithm type?

A) _____

Q15) The IPSec session ID 3 was established between what two addresses?

A) Local address:

_____

B) Remote address:

_____

Q16) Ping your student PC. Was it successful?

A) _____

**Step 8** From the Configuration menu tree, drill down to **User Management>Groups**. The Configuration>User Management>Groups window opens.

**Step 9** Choose **training** from the Current Groups list and click **Modify Group**. The Modify Training window opens.

**Step 10** Select the **HW Client** tab.

**Step 11** Select **Allow Network Extension Mode.** If you do not select Allow Network Extension mode, the Concentrator will not permit the Hardware Client to connect via network extension mode. This will result in the next task of the lab exercise not working correctly.

**Step 12** Click **Apply**.

**Step 13** Save the changes.

**Step 14** Log out of the Concentrator.

**Step 15** Close Internet Explorer.

# Task 8—Return the Cisco VPN 3002 Hardware Client to Factory Settings

The instructor will provide you with the procedures for access to the Hardware Client console port, as this will vary according to your lab connectivity. After you access the Hardware Client console port, the Hardware Client login prompt will appear. Complete the following steps to return the Hardware Client to the factory settings:

**Step 1**    Log in to the Hardware Client CLI using the administrator account:

```
Login: admin
Password: admin
```

**Step 2**    Complete the following sub-steps starting from the CLI top-level menu:

1.  Access the Administration menu:

```
Main -> 2
```

2.  Access the System Reboot menu:

```
Admin -> 2
```

3.  Access the Schedule Reboot menu:

```
Admin -> 2
```

4.  Select Reboot ignoring the Configuration file:

```
Admin -> 3
```

5.  Select Reboot Now:

```
Admin -> 2
```

It takes several moments for the Hardware Client to reboot. You are automatically logged out of the unit.

**Step 3**    Leave the CLI session open. Ignore the recurring IP interface 2 was unable to acquire an address via DHCP message.

## Task 9—Configure the Cisco VPN 3002 Hardware Client Private Interface

You must first change the private interface IP address to use the Hardware Client network extension mode. If you accept the factory default IP address, 192.168.10.1, you will never be able to select the network extension mode. Complete the following steps to alter the IP address of the Hardware Client private interface using the CLI:

**Step 1**    Log in to the Hardware Client CLI using the administrator account:

```
Login: admin
Password: admin
```

**Step 2**    Complete the following sub-steps, starting from the CLI top-level menu. Ignore the recurring IP interface 2 was unable to acquire an address via DHCP message and complete all of the following steps:

1.  Select the Configuration menu:

```
Main -> 1
```

2.  Select the Interface Configuration menu:

```
Config -> 2
```

3.  Select the Configure the Private Interface menu:

```
Interfaces -> 1
```

4.  Select the interface setting (Disable or Static IP):

```
Private Interface -> 1
```
5.  Select Enable using Static IP Addressing:

```
Private Interface -> 2
```
6.  Enter the Hardware Client private interface (network extension mode) IP address:

```
Private Interface -> [0.0.0.0] 192.168.1PP.1
```
(where PP = two-digit pod number [for example, Pod 1 is 01])

Several messages appear, indicating the condition of the Ethernet #1 (private) interface.

7.  Enter the Hardware Client private interface mask:

```
Enter Subnet Mask -> [255.255.255.0] Enter
```
8.  Return to the top-level menu:

```
Ethernet Interface 1 -> h
```
9.  Save changes to the configuration file:

```
Main -> 4
```
10. Exit the CLI:

```
Main -> 6
```

**Step 3**   Close the session.

## Task 10—Configure the Cisco VPN 3002 Hardware Client for Network Extension Mode

Complete the following steps to finish the Hardware Client network extension mode configuration using the Hardware Client Manager:

**Step 1**   Launch Internet Explorer by double-clicking the desktop icon.

**Step 2**   Enter a Hardware Client private interface (network extension mode) IP address in the Internet Explorer Address field: **192.168.1PP.1**.

(where PP = two-digit pod number [for example, Pod 1 is 01])

**Step 3**   Log in to the Hardware Client using the administrator account:

Login: **admin**

Password: **admin**

The username (login) and password are always case sensitive.

**Step 4**   In the main window, click the **click here to start Quick Configuration** hyperlink.

**Step 5**   Complete the following sub-steps from the Configuration>Quick>Time and Date window:

1.  View the contents of the window.

2.  Click **Continue**.

**Step 6**   Complete the following sub-steps from the Configuration>Quick>Upload Config window:

1.  View the contents of the window.

2. Select **No, continue on with quick configuration**.

**Step 7** Complete the following sub-steps from the Configuration>Quick>Private Interface window:

1. Select **No** when you are asked if you wish to configure the IP address of the private interface.

2. Select **No, do not use DHCP server to provide addresses** when you are asked if you want to use the DHCP server on the private interface.

3. Click **Continue**.

**Step 8** Complete the following sub-steps from the Configuration>Quick>Public Interface window:

1. Enter the system name: **studentP**.
   (where P = pod number)

2. Select **Specify an IP address**.

3. Enter a Hardware Client public interface IP address of **172.26.26.1PP**.
   (where PP = two-digit pod number [for example, Pod 1 is 01])

4. Enter a Hardware Client public interface subnet mask of **255.255.255.0**.

5. Enter a backbone router IP address of **172.26.26.150** in the Default Gateway field.

6. Click **Continue**.

**Step 9** Complete the following sub-steps from the Configuration>Quick>IPSec window:

1. In the Remote Server IP Address field, enter the Concentrator's public interface IP address: **192.168.P.5**.
   (where P = pod number)

2. Verify that **Use Certificate** is deselected.

3. Enter the group name: **training**.

4. Enter the group password: **training**.

5. Verify the group password: **training**.

6. Enter the username: **studentP**.
   (where P = pod number)

7. Enter the user password: **studentP**.
   (where P = pod number)

8. Verify the user password: **studentP**.
   (where P = pod number)

9. Click **Continue**. It may take a few moments to complete.

**Step 10** Complete the following sub-steps from the Configuration>Quick>PAT window:

1. Select **No, use Network Extension Mode**.

2. Click **Continue**.

**Step 11** Complete the following sub-steps from the Configuration>Quick>DNS window:

1. View the contents of the window.

2. Click **Continue**.

**Step 12** Complete the following sub-steps from the Configuration>Quick>Static Routes window:

1. View the contents of the window.

2. Click **Continue**.

**Step 13** Complete the following sub-steps from the Configuration>Quick>Admin Password window:

1. View the contents of the window.

2. Click **Continue**.

**Step 14** Do not log out of the Hardware Client Manager window, and do not close Internet Explorer.

# Task 11—Launch the Cisco VPN 3002 Hardware Client VPN Tunnel

Complete the following steps to launch and monitor the Hardware Client VPN tunnels:

**Step 1** Return to the Hardware Client Manager Internet Explorer window.

**Step 2** From the Monitoring menu tree, drill down to **System Status**. A VPN tunnel should already be established to the Concentrator. If not, click **Connect** now. Answer the following questions:

Q17) How can you tell if the VPN tunnel is established?

A) _____

Q18) Which IKE encryption type is used?

A) _____

Q19) Which IKE authentication type is used?

A) _____

Q20) Which IPSec encryption type is used?

A) _____

Q21) Which IPSec authentication type is used?

A) _____

Q22) Under other, which IKE mode is used?

A) _____

Q23) Which Diffie-Hellman group is used?

A) _____

**Step 3**  Log out of the Hardware Client Manager.

## Task 12—Monitor the Cisco VPN 3000 Series Concentrator Statistics

Complete the following steps to monitor the Concentrator statistics:

**Step 1**  Enter a Concentrator private interface IP address of **192.168.P.5** in the Internet Explorer Address field (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 2**  Log in to the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

**Step 3**  From the Monitoring menu tree, drill down to **Routing Table**. Answer the following question:

Q24)  Which networks are visible?

A)  _____

**Step 4**  From the Monitoring menu tree, drill down to **Sessions**.

**Step 5**  In the Remote Access Sessions window, select **studentP** (where P = pod number). More information is displayed.

**Step 6**  View the Session fields and answer the following questions:

Q25)  How many sessions are displayed?

A)  _____

Q26)  The IPSec session ID 2 supports a session between what two public interfaces?

A)  Local address:
_____

B)  Remote address:
_____

Q27)  The IPSec session ID 3 supports a session between what two addresses?

A)  Local address:
_____

B)  Remote address:
_____

Q28)  What is the difference between Client and Network Extension mode IPSec session ID 3? (refer to Task 9, Step 7 for Client mode IPSec session information)

A)  In Client mode, the session is between the Concentrator's private and the Hardware Clients:
_____

B)  In Network Extension mode, the session is between the Concentrator's private and the Hardware Clients: _____

Q29)  Ping your student PC. Was it successful?

---

A)    _____

**Step 7**   Log out of the Concentrator.

**Step 8**   Close any open Internet Explorer sessions.

# 11

# Configure the Cisco Virtual Private Network 3002 Hardware Client for Unit and User Authentication

## Overview

This lesson includes the following topics:

- Objectives

- Overview of the Hardware Client interactive unit and user authentication features

- Configuring the Hardware Client interactive unit authentication feature

- Configuring the Hardware Client user authentication feature

- Monitoring the Hardware Client user statistics

- Summary

- Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Describe the Hardware Client interactive unit and user authentication feature.**
- **Configure the Hardware Client for interactive unit authentication.**
- **Configure the Hardware Client for user authentication.**
- **Monitor the Hardware Client user statistics.**

CSVPN 4.0—11-2

# Overview of the Hardware Client Interactive Unit and User Authentication Features

This topic presents an overview of the Cisco Virtual Private Network (VPN) 3002 Hardware Client interactive unit and user authentication feature.
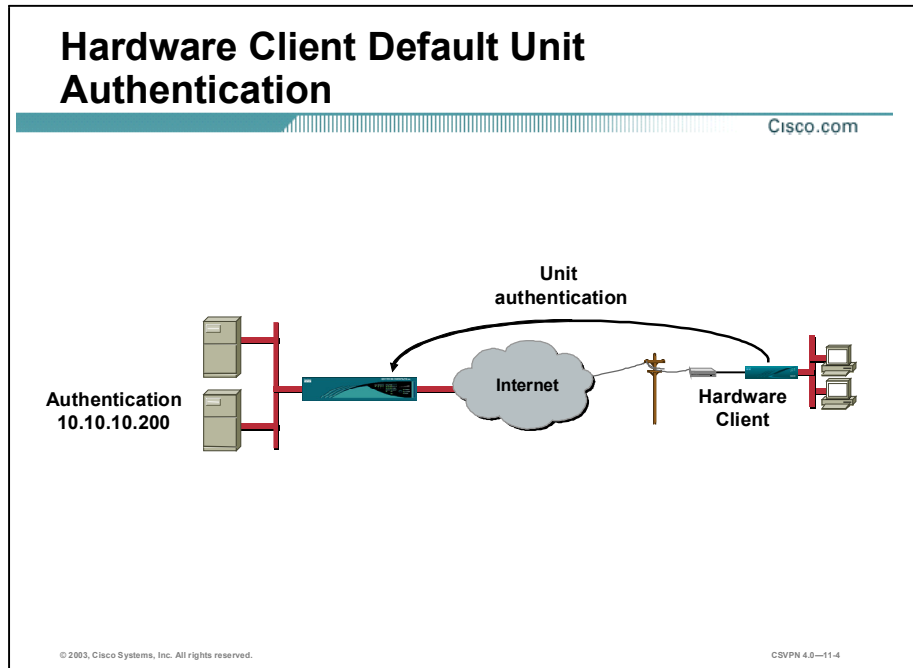


The Hardware Client allows up to 253 devices to be logged in behind it. Unlike the Cisco VPN Software Client, the Hardware Client, using the default unit authentication, saves the username and password permanently. During tunnel establishment, the Hardware Client automatically forwards the authentication information to the central site. When the tunnel is established, anyone can gain access to the corporate network. No remote site user intervention is required. Unfortunately, this can be viewed as a security weakness. This prevents administrators from requiring a Hardware Client user to enter a password before gaining access to the central site network. This is the default method used to authenticate the unit.

**Hardware Client Authentication Options**
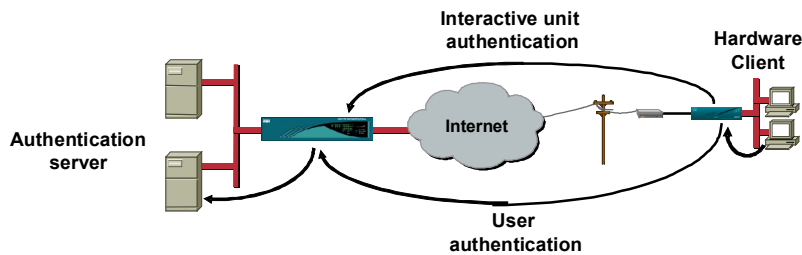
The administrator has three authentication options:

■ Unit authentication—The Hardware Client stores the username and password and forwards them automatically to the central site when the tunnel is established. This is the default.

■ Interactive unit authentication—The user password is no longer stored in memory on the Hardware Client. When launching a tunnel, a user behind the Hardware Client must supply the username and password each time a tunnel is established. When the tunnel is established, anyone on the Hardware Client private LAN can gain access to the corporate network.

■ User authentication—The first time users attempt to gain access to corporate networks over the tunnels, they are prompted for their authentication credentials. User authentication addresses unauthorized user access.

# Configuring the Hardware Client Interactive Unit Authentication Feature

This topic presents an overview of how to configure the Hardware Client interactive unit authentication feature.



The interactive unit authentication feature is enabled and disabled on the Cisco VPN Concentrator. You can do this by selecting or deselecting the **Require Interactive Hardware Client Authentication** check box within the Configuration>User Management>Groups>HW Client tab:

■ If selected, the Hardware Client does not save the user password. A remote user must supply the username and password before the tunnel is established.

■ If deselected, the Hardware Client supplies the username and password from memory when the tunnel is established. This is the default setting.

---

| Note | There is a check box labeled Allow Password Storage on Client within the Mode Config tab. This check box enables and disables password storage on the software client only. |
|------|------------|

---

# Interactive Unit Authentication—
# Hardware Client Configuration

The interactive unit authentication feature is enabled and disabled from the central site Concentrator. This information is communicated to the Hardware Client in mode configuration messages each time the tunnel is established. When the Hardware Client is first turned on without an existing configuration file, the GUI enables the user to enter a username and password as part of the quick configuration process. This initial username and password is used the first time a tunnel is established to the central site Concentrator as shown in the figure. If the Concentrator enables the interactive unit authentication feature during the tunnel negotiation, the Hardware Client removes the password from local memory and configuration files. Subsequent tunnel establishment will require the user to enter a password manually.
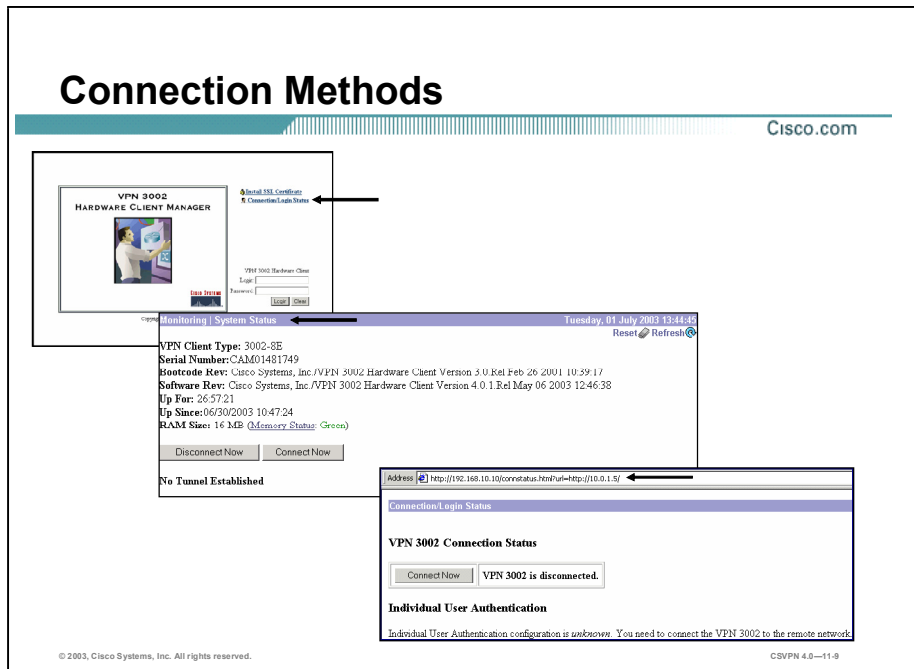
**Connection Methods**

When the Hardware Client interactive unit authentication feature is enabled on the Concentrator, a username and password must be supplied to the Hardware Client before a tunnel can be established. There are three methods in which to access the username password prompt:

■ Connect via the Hardware Client manager.

■ Connect via the System Status window.

■ Connect via the redirect message.

**Method 1—Connect via the Hardware Client Manager**
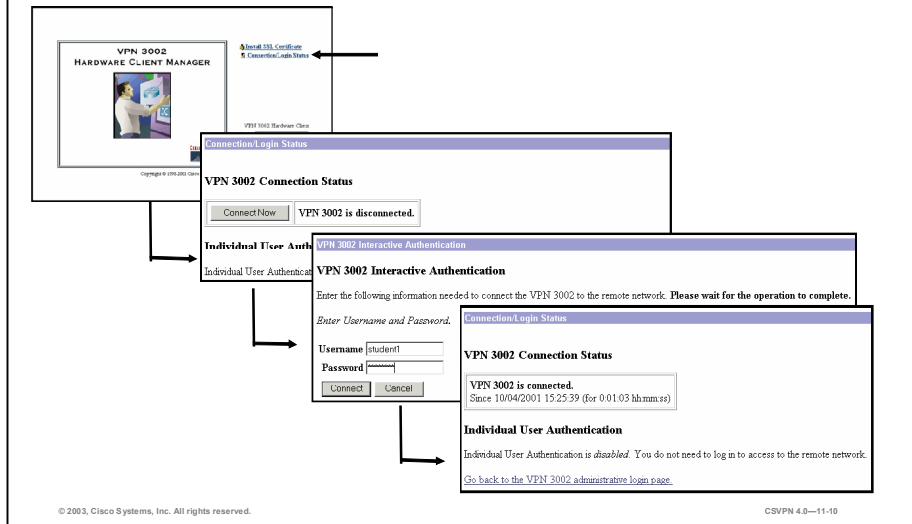
The first method for accessing the username and password is through the Hardware Client manager. There are three steps in this process:

**Step 1** Click the **Connection/Login** link in the manager window to start the login process. The Connection/Login Status window opens.

**Step 2** The Connection/Login Status window displays the current status of the Hardware Client tunnel. The Hardware Client is disconnected message indicates that the tunnel is currently down. To continue the process, click **Connect Now**. The Hardware Client interactive authentication window opens.

**Step 3** In the Hardware Client interactive authentication window, enter a username password in the corresponding fields, and click **Connect**. Clicking **Connect** initiates Internet Key Exchange (IKE) tunnel negotiation, while clicking **Cancel** sends the user back to the Hardware Client interactive authentication. If interactive unit authentication is disabled, clicking **Connect** immediately establishes a tunnel to the central site network.

If tunnel negotiation is successful, the Hardware Client is connected message is returned. If tunnel negotiations fail, a message is posted and the user is sent back to the same page to re-enter a new username and password combination.

---

**Note** If the remote host tears down the tunnel or if the system reboots, the Hardware Client must be authenticated again before the tunnel can be re-established.

---

**Method 2—Connect via the System Status Window**

Cisco.com

Monitoring | System Status                    Tuesday, 01 July 2003 13:44:45
                                                        Reset Refresh

**VPN Client Type:** 3002-8E
**Serial Number:** CAM01481749
**Bootcode Rev:** Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.0.Rel Feb 26 2001 10:39:17
**Software Rev:** Cisco Systems, Inc./VPN 3002 Hardware Client Version 4.0.1.Rel May 06 2003 12:46:38
**Up For:** 26:57:21
**Up Since:** 06/30/2003 10:47:24
**RAM Size:** 16 MB (Memory Status: Green)

[ Disconnect Now ]   [ Connect Now ]

**No Tunnel Established**

Monitoring | System Status | Connect Now

**VPN 3002 Interactive Authentication**

Enter the following information needed to connect the VPN 3002 to the remote network. **Please wait for the operation to complete.**

*Enter Username and Password.*

**Username** student1
**Password** ********

[ Connect ]   [ Cancel ]

© 2003, Cisco Systems, Inc. All rights reserved.                    CSVPN 4.0—11-11

Another way to access the login prompt is from the Hardware Client Manager Monitoring>System Status window:

**Step 1**   Determine if the tunnel is established.

**Step 2**   If no tunnel is established, click **Connect Now** to access the username and password prompts.

**Step 3**   When a username and password is provided, click **Connect** to establish the tunnel. Clicking Connect initiates the IKE tunnel negotiation.

**Method 3—Connect via the Redirect Message**
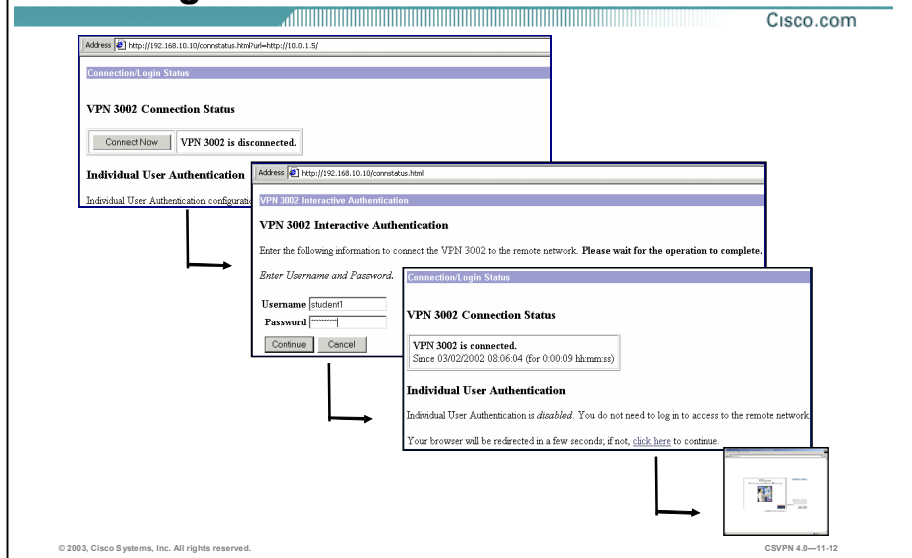
The last method for obtaining a login prompt is through message redirection. For example, a remote user powers up the Hardware Client and then attempts to connect to a corporate server via a web browser. Because the interactive unit authentication feature is enabled and the tunnel is not established, the Hardware Client redirects the remote user's web browser to the Hardware Client Connection/Login Status window. If the Hardware Client interactive unit authentication is successful, the remote user's web browser is redirected to the original destination. The Hardware Client unit authentication feature is a four-step process:

**Step 1**  You, as the remote user, try to make an HTTP connection through the Hardware Client tunnel, but the tunnel is down. With the Hardware Client interactive unit authentication feature enabled, the Hardware Client redirects the user to the Hardware Client Connection/Login Status window.

**Step 2**  The window displays the status of the window as being disconnected. Click **Connect Now** to continue the process.

**Step 3**  Enter the username and password in the corresponding fields within the Hardware Client Interactive Authentication window to connect the Hardware Client to the remote network.

**Step 4**  Click **Continue** to initiate an IKE tunnel negotiation. If successful, the Hardware Client opens the Connection/Login Status window. The Connection/Login Status window supplies you with the following information: the Hardware Client is connected and individual user authentication is disabled. After about 10 seconds, the original destination window replaces the connection/login status window.

## Hardware Client IPSec Parameters

Cisco.com

Configuration | System | Tunneling Protocols | IPSec

Enter the information needed to connect to the central-site VPN Concentrator server.

Remote Easy VPN Server: 192.168.1.5 — Enter remote server address/host name.

Backup Easy VPN Servers:
- Enter up to 10 backup server addresses/host names from high priority to low.
- Enter each backup server address/host name on a single line.

Alert when disconnecting ☐ — Inform VPN Concentrator server before the system shuts down or reboots.

IPSec over TCP ☐ — Check to enable IPSec over TCP.
IPSec over TCP Port: 10000 — Enter IPSec over TCP port (1-65535).
Use Certificate ☐ — Click to use the installed certificate.
Certificate Transmission: ○ Entire certificate chain  ⦿ Identity certificate only — Choose how to send the digital certificate to the server.

| | Name | Password | Verify |
|---|---|---|---|
| Group | training | ************ | ************ |
| User | student1 | | |

[ Apply ]  [ Cancel ]

© 2003, Cisco Systems, Inc. All rights reserved.                                    CSVPN 4.0—11-13

If the central site network enables the interactive unit authentication feature during the tunnel negotiation, the Hardware Client removes the password from the local memory and configuration files.

In the figure, notice the password and verify that the password fields are blank.

# Configuring the Hardware Client User Authentication Feature

This topic presents an overview of configuring the Hardware Client user authentication feature.
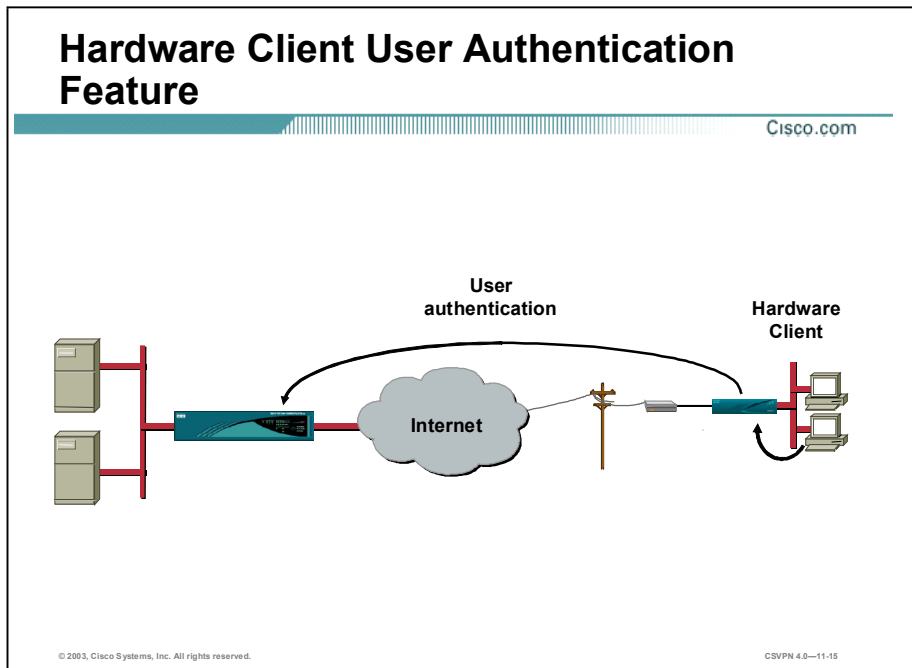


Many corporations such as banks, investment houses, and manufacturers envision using the Hardware Client to grant employees access to their corporate networks from home. By default, the Hardware Client saves the password and username permanently. This prevents corporations from requiring a user to enter a password before gaining access to the central site network. In addition, this does not allow prompted authentication, such as token cards; therefore, only fixed password authentication can be used (for example, Remote Access Dial-In User Service [RADIUS], NT Domain). Without some level of user authentication, the Hardware Client represents a substantial risk if placed in an unsecured environment, such as an employee's home.

The user authentication feature enables the authentication of users behind each Hardware Client. When a user attempts to gain access to the corporate network over the tunnel, their usernames, and IP and MAC addresses are checked. If no record of the user is present on the Hardware Client, they are prompted for authentication credentials. This protects the central site from unauthorized users, such as friends and family members, on the same LAN as the Hardware Client.

User Authentication Feature—
Concentrator Configuration

The user authentication feature is enabled and disabled on the Concentrator. You can do this by selecting the **Require Individual User Authentication** check box in the Hardware Client tab of the Configuration>User Management>Groups>Modify training window.

There are also three other parameters in this window:

- User Idle Timeout field—Enables the administrator to set an idle timeout value, in seconds, for all users behind the Hardware Client. If the remote user's keyboard remains idle for a specific period of time, the Hardware Client will log out of the remote user.

- Cisco IP Phone Bypass check box—IP phones do not support a user interface. By checking Cisco IP Phone Bypass check box, Cisco IP phones can bypass the Hardware Client individual user authentication. This option works only with user authentication.

- LEAP Bypass—Lightweight Extensible Authentication Protocol (LEAP) Bypass lets LEAP packets from devices behind a Hardware Client travel across a VPN tunnel prior to individual user authentication. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per individual user authentication (if enabled).

- Allow Network Extension Mode check box—Select this check box to allow the Hardware Client using network extension mode to connect.

**User Authentication Feature—
Hardware Client Configuration**

The user authentication feature is enabled and disabled from the central site Concentrator. This information is communicated to the Hardware Client each time the tunnel is established via mode configuration messages. When the Hardware Client is turned on without an existing configuration file, the GUI enables the user to enter a username and password for the unit as part of this quick configuration process. This initial username and password is used the first time a tunnel is established to the central site Concentrator. If the central site network enables the user authentication feature during the tunnel negotiation, the Hardware Client removes the password from the local memory and configuration files, as shown in the figure. Subsequent tunnel establishment and logins will require the user to enter a password manually.

**Connection Methods**

Cisco.com

VPN 3002
HARDWARE CLIENT MANAGER

Install SSL Certificate
Connection/Login Status

VPN 3002 Hardware Client
Login:
Password:

Login  Clear

**Monitoring | System Status**    Monday, 08 October 2001 10:06:50
Refresh

**VPN Client Type:** 3002-8E
**Bootcode Rev:** Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.0.Rel Feb 26 2001 10:39:17
**Software Rev:** Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.5.int_72 Oct 04 2001 00:14:21
**Up For:** 3d 2:06:34
**Up Since:** 10/05/2001 08:00:24
**RAM Size:** 16 MB

Disconnect Now   Connect Now

No Tunnel Established

Address  http://192.168.10.10/connstatus.html?url=http://10.0.1.5/

**Connection/Login Status**

**VPN 3002 Connection Status**

Connect Now   VPN 3002 is disconnected.

**Individual User Authentication**

Individual User Authentication configuration is *unknown*. You need to connect the VPN 3002 to the remote network.

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—11-18

When the Hardware Client individual user authentication feature is enabled on the Concentrator, a username and password must be supplied to the Hardware Client before an individual can access the Hardware Client tunnel. There are three methods in which an end user can gain access to the individual user authentication process:

■  Connect via the Hardware Client manager.

■  Connect via the System Status window.

■  Connect via the redirect message.

**Method 1—Connect via the Hardware Client Manager**

Cisco.com

VPN 3002 HARDWARE CLIENT MANAGER

**Connection/Login Status**

**VPN 3002 Connection Status**

VPN 3002 is connected.
Since 10/04/2001 15:36:03 (for 0:04:07 hh:mm:ss)

**Individual User Authentication**

Individual User Authentication is *required*. You need to log in to access to the remote network.

Log In Now | **You are not logged in.**
IP: 192.168.10.11
MAC: 00:50:DA:5A:04:07

**Individual User Authentication**

Enter the following information needed to log in to the remote

Username student1
Password ********

Login | Cancel

**Connection/Login Status**

**VPN 3002 Connection Status**

VPN 3002 is connected.
Since 03/02/2002 08:24:29 (for 0:03:02 hh:mm:ss)

**Individual User Authentication**

Log Out Now | **You are logged in.**
Username: student1
IP: 192.168.10.16
MAC: 00:50:DA:5A:04:07
Since: Mar 02 08:27:31 (for 0:00:00 hh:mm:ss)

Your browser will be redirected in a few seconds; if not, click here to continue.

CSVPN 4.0—11-19

The first method for accessing the username and password is through the Hardware Client Hardware Client manager. There are three steps in this process:

**Step 1**  Click the **Connection/Login** link in the manager window to start the login process. The Connection/Login Status window opens.

**Step 2**  The Connection/Login Status window displays the Hardware Client tunnel status and individual user authentication. The Hardware Client tunnel status indicates that the tunnel is connected but the individual user is not logged in. To continue the process, click **Log In Now**. The Hardware Client interactive authentication window opens.

**Step 3**  In the Hardware Client interactive authentication window, enter a username password in the corresponding fields, and click **Connect**. Clicking **Connect** initiates IKE tunnel negotiation, while clicking **Cancel** sends the user back to the Hardware Client interactive authentication. If tunnel negotiation is successful, a logged in message is returned along with the remote user's MAC and IP address. The Hardware Client tracks successfully logged-in remote users by their MAC and IP address.

**Method 2—Connect via the System Status Window**

Another way to access the login prompt is from the Hardware Client Manager System Status window:

**Step 1**   Click **Connect Now** in the Monitoring>System Status window. The Monitoring>System Status>Connect Now window opens.

**Step 2**   Enter a username and password in the corresponding fields, and click **Connect** to establish the tunnel. Clicking **Connect** initiates IKE tunnel negotiations.

**Method 3—Connect via the Redirect Message**

Cisco.com

Connection/Login Status

**VPN 3002 Connection Status**

VPN 3002 is connected.
Since 03/02/2002 08:24:29 (for 0:00:08 hh:mm:ss)

**Individual User Authentication**

Individual User Authentication is *required*. You need to log in to access the remote network.

| Log In Now | You are not logged in.<br>IP: 192.168.10.16<br>MAC: 00:50:DA:5A:04:07 |

Individual User Authentication

**Individual User Authentication**

Enter the following information needed to log in to the remote network. **Please wait for the operation to complete.**

Username student1
Password ********

Login    Cancel

Connection/Login Status

**VPN 3002 Connection Status**

VPN 3002 is connected.
Since 03/02/2002 08:24:29 (for 0:03:02 hh:mm:ss)

**Individual User Authentication**

| Log Out Now | You are logged in.<br>Username: student1<br>IP: 192.168.10.16<br>MAC: 00:50:DA:5A:04:07<br>Since: Mar 02 08:27:31 (for 0:00:00 hh:mm:ss) |

Your browser will be redirected in a few seconds; if not, click here to con

CSVPN 4.0—11-21

If individual user authentication is required, any attempt to access the central site network via HTTP immediately redirects the user's web browser to the user's Connection Login Status window. The "You are not logged in" message opens. To access the original central site website, the user must first login successfully.

If individual user authentication is enabled and the source IP and MAC addresses associated with the user's browser access are not authenticated, the Connection Login Status window indicates that the user is not logged in. By clicking **Log In Now**, the user is transferred to the Individual User Authentication window where they have to enter a username and password into the corresponding fields and click **Login**. The Hardware Client initiates an authentication sequence.

During user authentication the central site Concentrator determines if the username specified in the Individual User Authentication window was used to authenticate another machine. If the current authentication exceeds the simultaneous user login count for this group, the authentication fails and the user's browser is transferred back to the Connection Login Status window with an error message. If the user authentication is successful, the Hardware Client returns a Connection/Login Status window with a You are logged in message. The source IP and MAC address, and the username is saved as an authenticated machine.

If individual user authentication is disabled and the IKE tunnel has been established, the user does not need to log in to access the remote network.

# Monitoring the Hardware Client User Statistics

This topic presents an overview of monitoring the Hardware Client user status.



## Hardware Client User Status

Cisco.com

**Connection/Login Status**

**VPN 3002 Connection Status**

VPN 3002 is connected.
Since 10/04/2001 15:26:02 (for 0:06:24 hh:mm:ss)

**Individual User Authentication**

| | You are logged in. |
|---|---|
| Log Out Now | Username: student1 |
| | IP: 192.168.10.11 |
| | MAC: 00:50:DA:5A:04:07 |
| | Since: Oct 04 15:42:37 (for 0:00:00 hh:mm:ss) |

Go back to the VPN 3002 administrative login page.

- Configuration
- Administration
- Monitoring
  - Routing Table
  - Filterable Event Log
  - System Status
  - User Status
  - Statistics

**Monitoring | User Status**                 Thursday, 04 October 2001 15:44:02
Refresh

*Cisco IP Phone Bypass is disabled.*

| Username | IP Address | MAC Address | Login Time | Duration (hh:mm:ss) | Actions |
|---|---|---|---|---|---|
| student1 | 192.168.10.11 | 00.50.DA.5A.04.07 | Oct 04 15:42:37 | 0:01:25 | [ Logout ] |

© 2003, Cisco Systems, Inc. All rights reserved.                 CSVPN 4.0—11-23

Individual user statistics are available in the Hardware Client within Connection Login Status and Monitoring>User Status windows. In the Connection Login Status window, you can view your username, IP and MAC address, and login time and duration.

Under the Monitoring>User Status window, a new authenticated user's window is added on the Hardware Client. This window displays the IP address, MAC address, username, login time and duration, and logout function for currently authenticated users. If the individual user authentication feature is disabled, this window is displayed under the Monitoring>User Status window. In place of the user authentication information, this page displays a message indicating that individual user authentication is disabled.

# Concentrator User Status

IKE Sessions: 1
IPSec Sessions: 2

| IKE Session | | | |
|---|---|---|---|
| Session ID | 1 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Diffie-Hellman Group | Group 2 (1024-bit) |
| Authentication Mode | Pre-Shared Keys (XAUTH) | IKE Negotiation Mode | Aggressive |
| Rekey Time Interval | 86400 seconds | | |

| IPSec Session | | | |
|---|---|---|---|
| Session ID | 2 | Remote Address | 192.168.1.6 |
| Local Address | 192.168.1.5 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Idle Time | 0:25:53 |
| Encapsulation Mode | Tunnel | Rekey Time Interval | 28800 seconds |
| Bytes Received | 0 | Bytes Transmitted | 0 |

| IPSec Session | | | |
|---|---|---|---|
| Session ID | 3 | Remote Address | 192.168.10.10/0.0.0.255 |
| Local Address | 0.0.0.0/255.255.255.255 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Encapsulation Mode | Tunnel |
| Rekey Time Interval | 28800 seconds | | |
| Bytes Received | 124936 | Bytes Transmitted | 106728 |

| Authenticated Users | | |
|---|---|---|
| Username | Login Time | Duration |
| student1 | Oct 09 11:23:58 | 0:02:59 |

CSVPN 4.0—11-24

On the Concentrator, individual user information is added to the Administration>Sessions> Detail display window. When multiple authentications execute for a given IKE tunnel, the central site Concentrator displays the username and login duration information. The user's MAC and IP addresses are visible only on the Hardware Client.

# Summary

This topic summarizes the information presented in this lesson.

## Summary

- **There are three authentication options available on the Hardware Client: unit authentication, interactive unit authentication, and individual user authentication.**

- **Interactive unit and individual user authentication are enabled or disabled on the Concentrator.**

- **There are three ways to access interactive unit and individual user authentication prompts: connect via the Hardware Client Manager, connect via the system status window, or connect via the redirect message.**

CSVPN 4.0—11-26

# Lab Exercise—Configure the Cisco VPN 3002 Hardware Client Interactive Unit and Individual User Authentication

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to install and configure the Cisco Virtual Private Network (VPN) 3002 Hardware Client and the Cisco VPN 3000 Series Concentrator to enable IPSec encrypted tunnels. Work with your lab partner to complete the following tasks:

■ Complete the lab exercise setup.

■ Launch a Cisco VPN 3002 Hardware Client IPSec tunnel using default unit authentication.

■ Configure the Cisco VPN 3000 Series Concentrator for interactive unit authentication.

■ Authenticate the Cisco VPN 3002 Hardware Client via Connect Now.

■ Authenticate the Cisco VPN 3002 Hardware Client using the Connection/Login status link.

■ Authenticate the Cisco VPN 3002 Hardware Client using HTTP re-direction.

■ Configure the Cisco VPN 3000 Series Concentrator for individual user authentication.

■ Launch an IPSec tunnel using both the interactive unit and individual user authentication.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
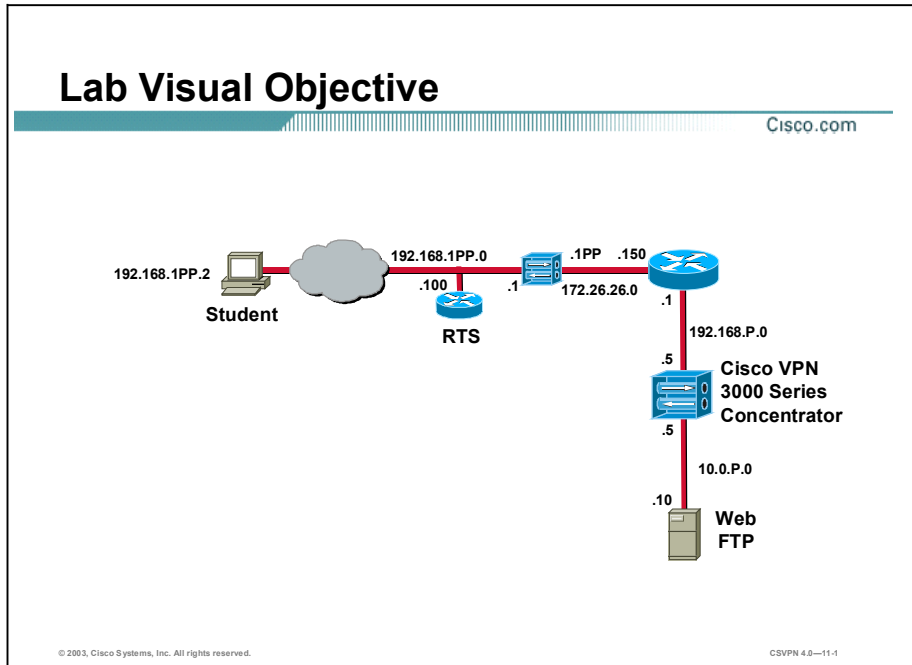


## Scenario

Your company wants you to implement a VPN using remotely located Hardware Clients terminating at centrally located Concentrators. You must configure the Concentrator to support Hardware Client interactive unit and individual user authentication.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment is setup as follows:

■   Ensure that your student PC is powered on.

■   Ensure that your student IP addresses are configured correctly:

— Primary IP address—192.168.1PP.2
(where PP = two-digit pod number [for example, Pod 1 is 01])

— Default gateway IP address—192.168.1PP.1
(where PP = two-digit pod number)

■   Ensure that your Hardware Client is powered on.

## Task 2—Launch a Cisco VPN 3002 Hardware Client IPSec Tunnel Using Default Unit Authentication

Complete the following steps to launch and monitor the Hardware Client IPSec tunnel:

**Step 1** Launch Internet Explorer by double-clicking the desktop icon.

**Step 2** Enter a Hardware Client private interface (Client mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field.

(where PP = double digit pod number)

**Step 3** Log into the Hardware Client using the administrator account:

```
Login: admin
Password: admin
```

Both the username (login) and password are always case sensitive.

**Step 4** From the Monitoring menu tree, drill down to **System Status**. An IPSec tunnel should already be established to the Concentrator. If not, click **Connect Now**.

**Step 5** Verify an IPSec tunnel is present.

**Step 6** Log out of the Cisco VPN 3002 Hardware Client Manager. Do not close Internet Explorer.

## Task 3—Configure the Cisco VPN 3000 Series Concentrator for Interactive Unit Authentication

With interactive unit authentication, the user password is no longer stored in the memory of the Hardware Client. When launching an IPSec tunnel, a user behind the Hardware Client must supply a username and password each time an IPSec tunnel is established. By default the feature is disabled. Complete the following steps to enable interactive unit authentication:

**Step 1** Enter a Concentrator public interface IP address of **192.168.P.5** in the Internet Explorer Address field (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 2** Log into the Concentrator using the administrator account:

```
Login: admin
Password: admin
```

**Step 3** From the Configuration menu tree, drill down to **User Management>Groups**.

**Step 4** Choose **training** from the Current Groups list.

**Step 5** Click **Modify Group**. It may take a few moments for the text to appear.

**Step 6** Select the **HW Client** tab.

**Step 7** Select the **Require Interactive Hardware Client Authentication** check box.

**Step 8** Click **Apply**.

**Step 9** Save the configuration.

**Step 10** Log out of the Concentrator. Do not close Internet Explorer.

# Task 4—Authenticate the Cisco VPN 3002 Hardware Client Via Connect Now

With interactive unit authentication enabled, the unit must be authenticated before an IPSec tunnel is established. There are three ways to access the Interactive Unit Authentication Login window. The first way is to access the login via Monitoring>System Status>Connect Now. Complete the following steps to authenticate the Hardware Client interactively via connect now:

**Step 1** Enter a Hardware Client private interface (Client mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field.

(where PP = double digit pod number)

**Step 2** Log into the Hardware Client using the administrator account:

Login: **admin**

Password: **admin**

Both the username (login) and password are always case sensitive.

**Step 3** From the Monitoring menu tree, drill down to **System Status**. If a tunnel is connected, click **Disconnect Now**. It takes several moments for the Hardware Client IPSec tunnel to disconnect.

**Step 4** Click **Connect Now** to re-connect the tunnel using interactive unit authentication. The Monitoring>System Status>Connect Now window opens.

**Step 5** From the Monitoring>System Status>Connect Now window, complete the following sub-steps:

---

| Note | The following entries are case sensitive and should be entered in all lower case. |
|------|-----------------------------------------------------------------------------------|

---

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

3. Click **Continue** to authenticate the unit and establish the IPSec tunnel. The Monitoring>System Status window opens.

**Step 6** View the IPSec tunnel information.

**Step 7** From the Configuration menu tree, drill down to **System>Tunneling Protocols>IPSec** window, and answer the following question:

Q1)    What is listed in the user password and verify fields?

A)    _____

**Step 8** Return to the Monitoring>System Status window and click **Disconnect Now** to disconnect the IPSec tunnel. It takes several moments for the Hardware Client IPSec tunnel to disconnect.

**Step 9** Log out of the Hardware Client Manager.

**Step 10** Do not close Internet Explorer.

---

## Task 5—Authenticate the Cisco VPN 3002 Hardware Client using the Connection/Login Status Link

The second way to access the login prompt is by using the Connection/Login Status link. Complete the following steps to authenticate the Hardware Client interactively using the Connection/Login Status link:

**Step 1**  From the Hardware Client Manager window, select **Connection/Login Status** link.

**Step 2**  From the Connection/Login Status window, answer the following questions:

Q2)  What is the connection status of the Hardware Client?

A)  _____

Q3)  What is the individual user authentication status?

A)  _____

**Step 3**  Click **Connect Now** to re-connect the tunnel.

**Step 4**  Complete the following sub-steps from the Hardware Client Interactive Authentication window:

---

**Note**  The following entries are case sensitive and should be entered in all lower case.

---

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

3. Click **Continue** to establish the IPSec tunnel to the remote Concentrator.

**Step 5**  From the Connection/Login Status window, answer the following questions:

Q4)  What is the connection status of the Hardware Client?

A)  _____

Q5)  What is the individual user authentication status?

A)  _____

**Step 6**  From the Connection/Login Status window, select **Go back to the VPN 3002 administrative login page**.

**Step 7**  Log into the Hardware Client using the administrator account:

Login: **admin**

Password: **admin**

Both the username (login) and password are always case sensitive.

**Step 8** From the Monitoring menu tree, drill down to **System Status**. If an IPSec tunnel is connected, click **Disconnect Now**. It takes several moments for the Hardware Client IPSec tunnel to disconnect.

**Step 9** Log out of the Hardware Client Manager.

**Step 10** Do not close Internet Explorer.

# Task 6—Authenticate the Cisco VPN 3002 Hardware Client Using HTTP Re-direction

The last method is HTTP re-direction. The user attempts to access a URL at the central site. Because the unit has not been authenticated, the Hardware Client re-directs the connection to the Interactive Authentication window for authentication. Complete the following steps to authenticate the Hardware Client via HTTP re-direction:

**Step 1** Enter a Concentrator public interface IP address of **192.168.P.5** in the Internet Explorer Address field (where P = pod number). The Hardware Client Connection/Login Status window opens.

Answer the following question:

Q6) What IP address was the Internet Explorer window re-directed to?

A) _____

**Step 2** Click **Connect Now**. The Hardware Client Interactive Authentication window opens.

**Step 3** Complete the following sub-steps from the Hardware Client Interactive Authentication window:

| | |
|---|---|
| **Note** | The following entries are case sensitive and should be entered in all lower case. |

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

3. Click **Continue** to establish an IPSec tunnel to the remote Concentrator. The connection Login/Status window opens for four seconds.

**Step 4** From the Connection/Login Status window, answer the following questions (you must be fast since the window only stays open for approximately four seconds):

Q7) What is the connection status of the Hardware Client?

A) _____

Q8) What is the individual user authentication status?

A) _____

The Cisco VPN 3000 Concentrator Series Manager window opens.

**Step 5**    Do not disconnect the IPSec tunnel. Do not close Internet Explorer.

# Task 7—Configure the Cisco VPN 3000 Series Concentrator for Individual User Authentication

With user authentication, each user behind the Hardware Client must be individually authenticated before they are allowed to use the IPSec tunnel. Each user behind the Hardware Client is prompted for a username and password. By default, the individual user authentication feature is disabled. Complete the following steps to enable individual user authentication on the Concentrator:

**Step 1**    If the Cisco VPN 3000 Concentrator Series Manager is not visible, enter the Concentrator's public interface IP address of **192.168.P.5** in the Internet Explorer Address field (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 2**    Log into the Concentrator using the administrator account:

Login: **admin**

Password: **admin**

**Step 3**    From the Configuration menu tree, drill down to **User Management>Groups**.

**Step 4**    Choose **training** from the Current Groups list.

**Step 5**    Click **Modify Group**. It may take a few moments for the text to appear.

**Step 6**    Select the **HW Client** tab.

**Step 7**    Select the **Require Individual User Authentication** check box. Leave the Require Interactive Hardware Client Authentication check box selected.

**Step 8**    Click **Apply**.

**Step 9**    Save the configuration.

**Step 10**   Log out of the Concentrator.

**Step 11**   Enter a Hardware Client private interface (Client mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field.

(where PP = double digit pod number)

**Step 12**   Log into the Hardware Client using the administrator account:

Login: **admin**
Password: **admin**

Both the username (login) and password are always case sensitive.

**Step 13**   From the Monitoring menu tree, drill down to **System Status**. If an IPSec tunnel is connected, click **Disconnect Now**. It takes several moments for the Hardware Client IPSec tunnel to disconnect.

**Step 14**   Log out of the Cisco VPN 3002 Hardware Client Manager and leave Internet Explorer open.

# Task 8—Launch an IPSec Tunnel Using Both the Interactive Unit and Individual User Authentication

With both the interactive unit and individual user authentication enabled, the user must authenticate twice. Complete the following steps to establish an IPSec tunnel:

**Step 1**   Enter a Concentrator's public interface IP address of **192.168.P.5** in the IP Address field. The Connection/Login Status window opens.

(where P = pod number)

**Step 2**   From the Connection/Login Status window, answer the following questions:

Q9)   What is the Hardware Client Connection status?

A)   _____

Q10)   What is the individual user authentication connection status?

A)   _____

**Step 3**   Click **Connect Now** to connect the IPSec tunnel. The Hardware Client Interactive Authentication window opens.

**Step 4**   Complete the following sub-steps from the Hardware Client Interactive Authentication window:

1.   Enter **studentP** in the User Name field.
(where P = pod number)

2.   Enter **studentP** in the Password field.
(where P = pod number)

3.   Click **Continue** to establish the IPSec tunnel to the remote Concentrator. It takes several moments for the Hardware Client IPSec tunnel to connect.

**Step 5**   From the Connection/Login Status window, answer the following questions:

Q11)   What is the connection status of the Hardware Client?

A)   _____

Q12)   What is the individual user authentication status?

A)   _____

Q13)   What is the user's PC IP address?

A)   _____

Q14)   What is the user's MAC address?

A)   _____

**Step 6**   Click **Login In Now** under Individual User Authentication.

**Step 7**   Complete the following sub-steps from the Hardware Client Interactive Authentication window:

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

3. Click **Continue** to establish the IPSec tunnel to the remote Concentrator. The Hardware Client Connection/Login Status window will quickly open and then be replaced by the Cisco VPN 3000 Concentrator Series Manager.

**Step 8**  Log into the Concentrator using the administrator account:

Login: **admin**

Password: **admin**

**Step 9**  From the Monitoring menu tree, drill down to **Sessions**.

**Step 10**  Select **studentP** in the Remote Access Sessions summary section.

(where P = pod number)

**Step 11**  From the Monitoring>Sessions>Detail window, answer the following question:

Q15)  At the bottom of the Monitoring>Sessions>Detail window, which user was authenticated?

A) _____

Q16)  What other authenticated user information was supplied?

A) _____

**Step 12**  From the Configuration menu tree, drill down to **User Management>Groups**.

**Step 13**  Choose **training** from the Current Groups list.

**Step 14**  Click **Modify Group**. It may take a few moments for the text to appear.

**Step 15**  Select the **HW Client** tab.

**Step 16**  Deselect the **Require Individual User Authentication** check box. Leave the Require Interactive Hardware Client Authentication check box selected.

**Step 17**  Click **Apply**.

**Step 18**  Save the configuration.

**Step 19**  Log out of the Concentrator. Do not close Internet Explorer.

**Step 20**  Enter a Hardware Client private interface (network extension mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field.

(where PP = double digit pod number)

**Step 21**  Log into the Hardware Client using the administrator account:

Login: **admin**

Password: **admin**

Both the username (login) and password are always case sensitive.

**Step 22**  From the Monitoring menu tree, drill down to **User Status**. Answer the following questions:

    Q17)    Which user is authenticated?

        A)    _____

    Q18)    What is the IP address of the authenticated user?

        A)    _____

    Q19)    What is the MAC address of the authenticated user?

        A)    _____

    Q20)    What is the login time and duration of the connection?

        A)    _____

**Step 23**  From the Monitoring menu tree, drill down to **System Status**.

**Step 24**  Click **Disconnect Now**. It takes several moments for the Hardware Client IPSec tunnel to disconnect.

**Step 25**  Log out of the Hardware Client and close Internet Explorer.

# Configure the Cisco Virtual Private Network Client Backup Server, and Load Balancing

## Overview

This lesson includes the following topics:

- Objectives

- Configuring the Cisco VPN Client backup server feature

- Configuring the Cisco VPN Client load-balancing feature

- Overview of the Cisco VPN Client Reverse Route Injection feature

- Summary

- Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

Cisco.com

**Upon the completion of this lesson, you will be able to perform the following tasks:**

- **Describe the Cisco VPN Client reverse route injection, backup server, and load-balancing features.**
- **Configure the VPN Client for a backup server.**
- **Configure the Cisco VPN Client for load balancing.**
- **Configure the Concentrator for reverse route injection.**

CSVPN 4.0—12-2

# Configuring the Cisco VPN Client Backup Server Feature

This topic presents an overview of how to configure the Cisco Virtual Private Network (VPN) Client backup server.



**Backup Server**

Primary server
192.168.1.5
Backup server
192.168.2.5

192.168.1.5

192.168.2.5

192.168.3.5

192.168.1.5

192.168.2.5

Internet

SOHO

CSVPN 4.0—12-4
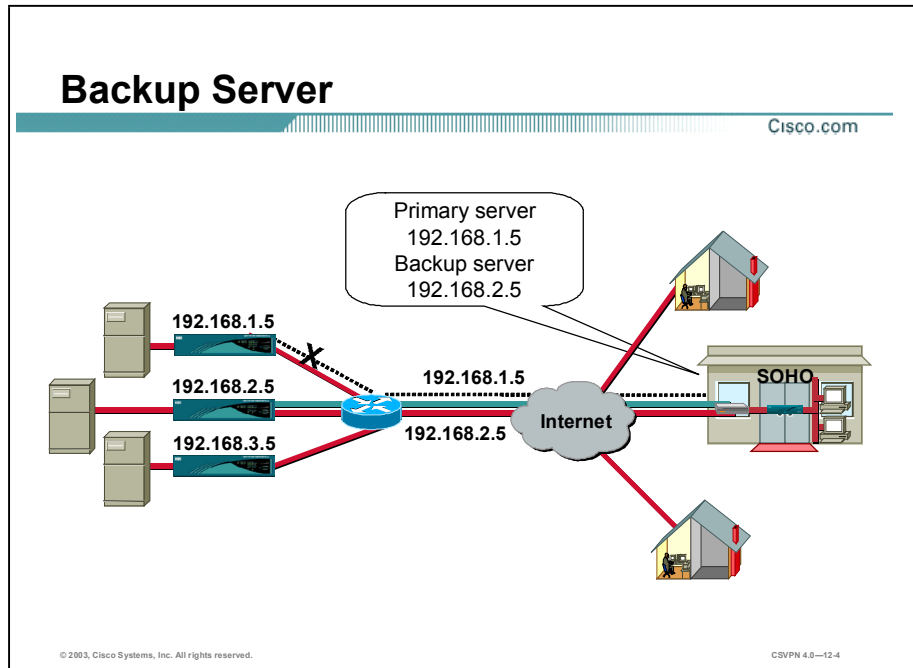
IPSec backup servers enable a Hardware Client and a VPN Software Client to connect to a backup Concentrator when its primary Concentrator is unavailable. You configure backup servers, either on the Hardware Client and the VPN Software Client, or on a group-basis on the Concentrator.

The following is an example of what happens when you configure a backup server:

**Step 1**   The Hardware Client attempts to contact the primary peer.

**Step 2**   If the Hardware Client does not receive an Internet Key Exchange (IKE) reply packet from the primary Concentrator within eight seconds, the Hardware Client declares the packet lost and logs the event.

**Step 3**   After four seconds, the Hardware Client attempts a connection with a backup server. A backup server list is traversed from top to bottom. If the bottom of the list is reached with no connection, the tunnel establishment process is terminated. The Hardware Client does not automatically begin again from the top.

Backup Server—Concentrator Configuration

Drop-down menu choices:
- Use Client Configured List
- Disable and Clear Configured List
- Use List Below

CSVPN 4.0—12-5
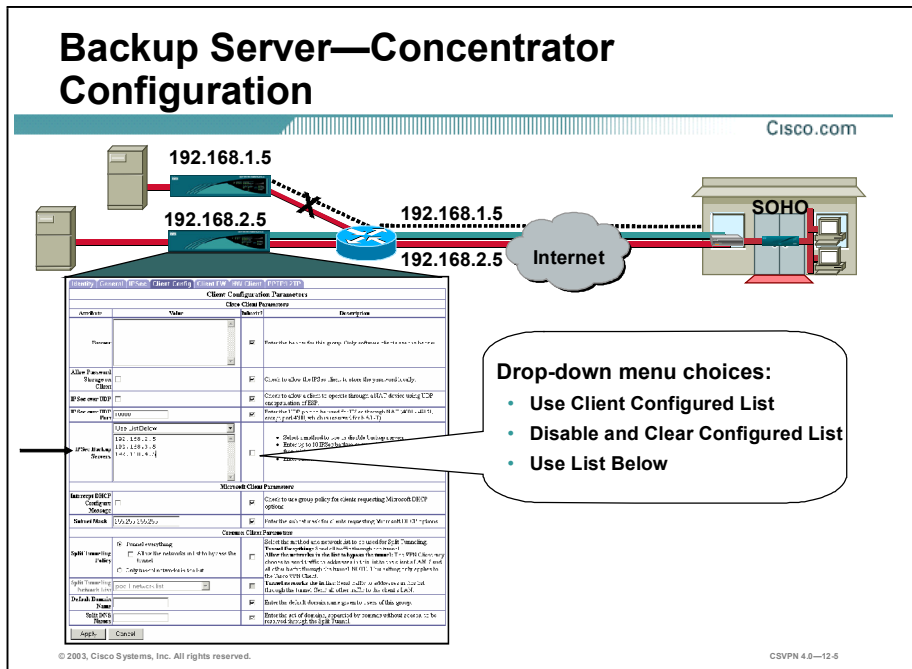
The IPSec backup server feature enables a Hardware Client and VPN Software Client to connect to a backup Concentrator when its primary Concentrator is unavailable. During tunnel negotiation, the VPN Clients ask for a policy from the Concentrator. The Concentrator responds to the request via a Mode Config policy message. The VPN Clients check the policy message and respond appropriately. There are three backup server options available:

■ Use Client Configured List—Instructs the VPN Clients to use its own backup server list.

■ Disable and Clear Configured List—Disables and clears the configured list, and instructs the VPN Clients to clear their own backup server list and disable the feature.

■ Use List Below—Instructs the VPN Clients to use the list of backup servers supplied by the Concentrator. The list is pushed down to the VPN Clients in a proprietary Mode Config message replacing any backup list on the VPN Clients.

In the example in the figure, from the IPSec Backup Server drop-down menu, the Use List Below option is chosen for the training group. Beneath the drop-down menu, there are four backup server addresses listed. This information is pushed down to the Hardware Client during tunnel setup. The IPSec backup server is configured on a group-by-group basis.

**Backup Server—Hardware Client Configuration**
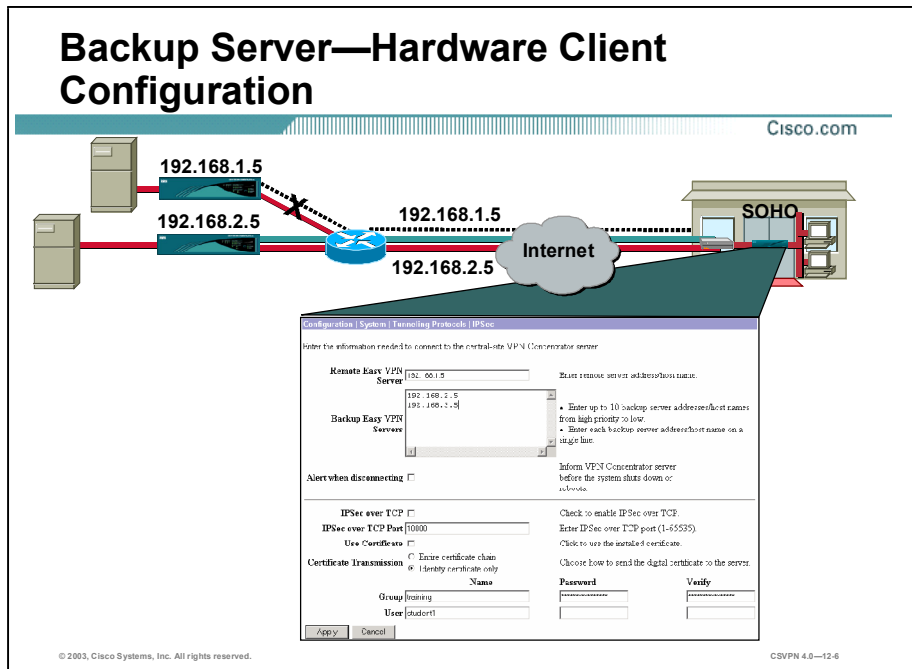
If the Concentrator IPSec backup server option is set for Use Client Configured List, the Hardware Client uses the backup server addresses configured in the Hardware Client. To configure backup servers on a Hardware Client, go to the Configuration>System>Tunneling Protocols>IPSec window. In the backup server window, enter up to ten backup servers listed from high to low priority. If the Concentrator sends a backup server list to the client, Hardware Client adds the down loaded list replacing any entries currently on the backup list.

The PC needs accurate Windows Internet Naming Service (WINS) and Domain Name System (DNS) information to navigate through the central site. Typically the WINS and DNS information is sent to the Hardware Client during tunnel establishment. In turn, the Hardware Client passes the WINS and DNS information to the remote PC in Dynamic Host Configuration Protocol (DHCP) offer messages. To update the WINS and DNS information, you may have to release and then renew the IP address of the PC. By doing so, the PC contacts the Hardware Client for a new IP address. In the resulting DHCP offer message, the PC receives an IP address, and WINS and DNS information .To enable the WINS and DNS update process, the Hardware Client is configured as a DHCP server and the PC is set to obtain IP address via DHCP.

Backup Server—Software Client Configuration
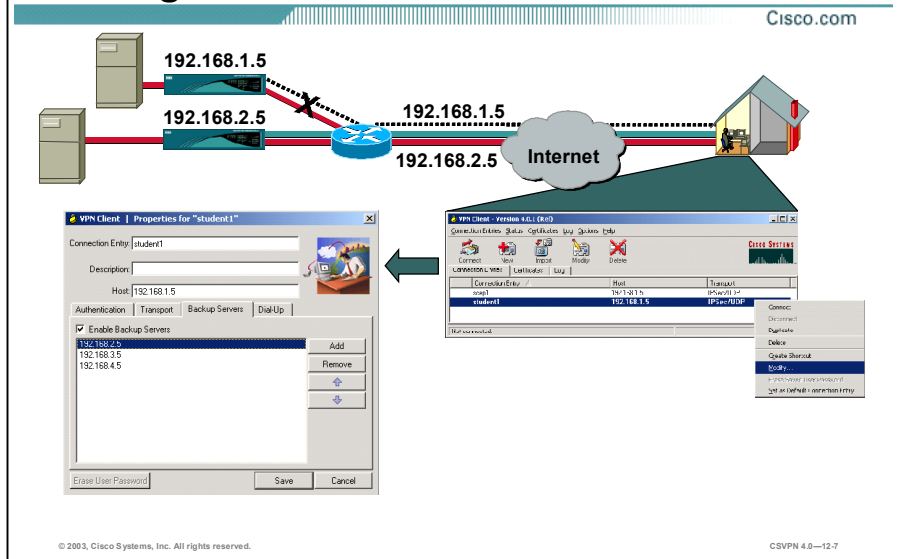
If the Concentrator IPSec backup server option is set to Use Client Configured List, the VPN Software Client uses the backup server addresses configured in the VPN Software Client. Go to **Start>Programs>Cisco Systems VPN Client>VPN Client** to configure backup servers on a VPN Client. The VPN Software Client window opens. Right-click the connection entry you wish to configure and choose **Modify** from the menu. The Properties window opens. Choose the **Backup Servers** tab. In the resulting window, click the **Enable Backup Servers** check box and then enter up to ten backup servers, listed from high to low priority. If the Concentrator sends a backup server list to the client, the VPN Software Client adds the downloaded list, replacing any entries currently on the backup list.

# Configuring the Cisco VPN Client Load-Balancing Feature

This topic presents an overview of how to configure Cisco VPN Client load balancing.



**Load-Balancing Cluster**

Cisco.com

VPN virtual cluster
IP address
192.168.1.150

192.168.1.5
**Master**

192.168.1.6
**Secondary**

192.168.1.7
**Secondary**

Internet

SOHO

SOHO

CSVPN 4.0—12-9
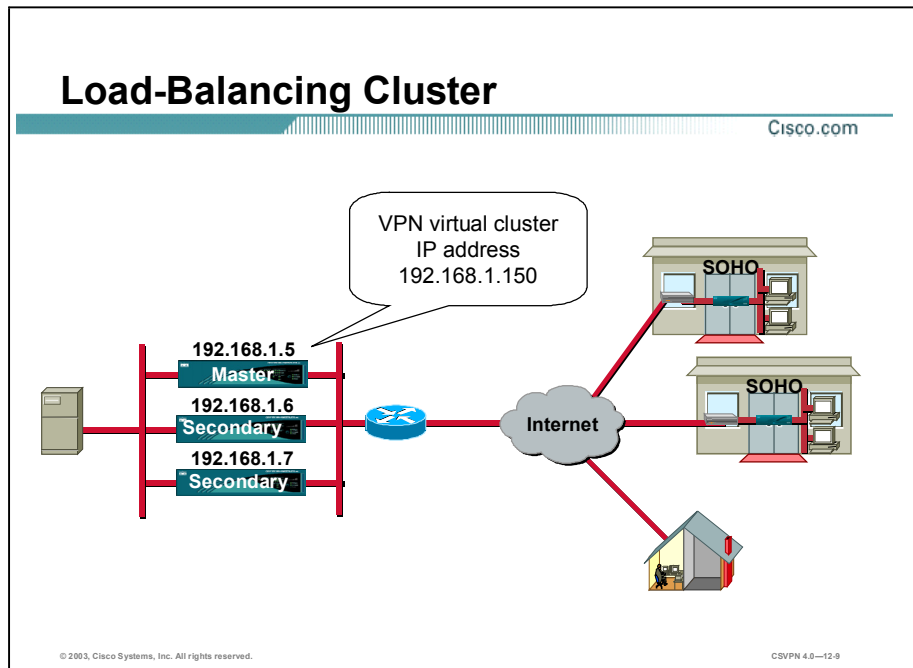
If you have a Concentrator configuration in which you are using two or more Concentrators connected on the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called load balancing. Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.

In load balancing, a group of Concentrators work together as a single entity, a cluster. The cluster is known by one IP address, a virtual address, to the outside client space. This virtual IP address is not tied to a specific physical device in the VPN cluster but will be serviced by the cluster virtual cluster master. The virtual IP address is a valid, routable address. When remote clients attempt to establish a tunnel, the clients route the IKE messages to the IP address of the cluster—the virtual IP address. The virtual cluster master responds to the messages.

Connections to the load-balancing cluster are based on the load.The designated virtual cluster master Concentrator maintains load information from all secondary Concentrators in the cluster. Each secondary Concentrator periodically sends load information in a "Keep Alive" message exchange to the master Concentrator. Load is calculated as a percentage of current active sessions divided by the configured max-allowed connections. When a VPN Client makes a connection request, the master Concentrator checks the load list for the least-loaded Concentrator. The master Concentrator directs the VPN Client toward the least-loaded Concentrator in the cluster. The least-loaded Concentrator terminates the new tunnel.

Load balancing is supported on the following VPN Client versions:

■ VPN Software Client Release 3 and above

■ Hardware Client release 3.5 and above

**Load-Balancing Connection Process**

Cisco.com

VPN virtual cluster
IP address
192.168.1.150

192.168.1.5
Master

192.168.1.150

SOHO

192.168.1.6
Secondary

192.168.1.6

Internet

SOHO

192.168.1.7
Secondary

CSVPN 4.0—12-10
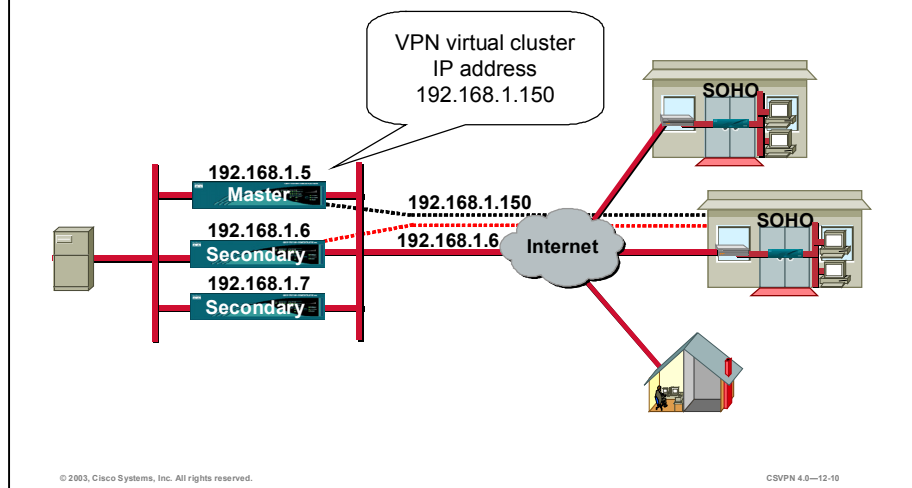
When a VPN Client is launched, it will attempt to establish an IKE tunnel to the VPN virtual cluster IP address: 192.168.1.150. The cluster master responds to the IKE messages by sending a re-direct message to the VPN Client. In the re-direct message is the physical IP address of the least-loaded Concentrator within the cluster. The cluster master determines the least-loaded Concentrator by consulting its load table. The load table is continuously updated with the secondary Concentrator's current load information. At the IKE tunnel connection time, the cluster master consults its load table and picks the least-loaded secondary Concentrator at that time. The cluster master Concentrator forwards the IP address of the least-loaded secondary Concentrator to the remote client. In the example in the figure, the IP address of the least-loaded Concentrator within the cluster is 192.168.1.6.

The VPN Client in turn attempts to establish a new tunnel to the least-loaded Concentrator: 192.168.1.6. The original tunnel to the cluster master's virtual IP address is torn down.

Load balancing is only performed during tunnel establishment.
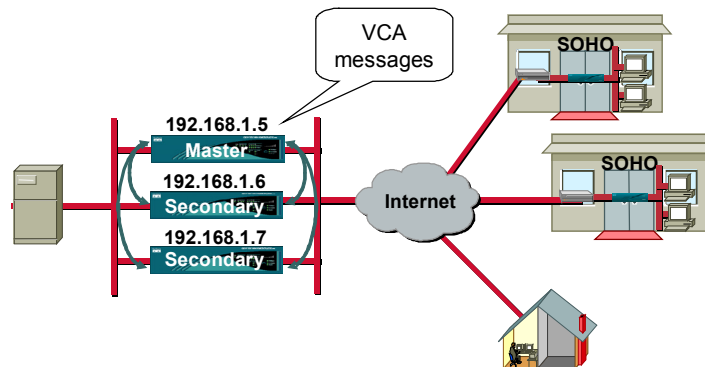
For load balancing to operate, a new application must be added to the Concentrator. The application is called Virtual Cluster Agent (VCA). VCA is the process executing on each Concentrator in the cluster. VCA is responsible for the following:

- Joining and exiting the virtual cluster

- Establishing IPSec connections between peers in the cluster

- Calculating the load

- Sending periodic load and health check information to the cluster master

- Determining a failed cluster master

- Participating in a virtual master election process

In order for the VCA messages to flow between cluster Concentrators, a VCA filter must be enabled on each Concentrator's public and private interface.

## Load-Balancing Configuration Process

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.                                      CSVPN 4.0—12-12

Load balancing is a three-step process:

**Step 1**   Add VCA capability to the Concentrator's public and private interfaces.

**Step 2**   Configure each Concentrator within the cluster for load balancing.

**Step 3**   Configure each client with the virtual address of the cluster.

**Add Rules to Filter**

Cisco.com

The first step of load balancing is to enable VCA message transmissions between Concentrators in the cluster. To do this, you must add a rule to the public and private interface of each Concentrator in the cluster:

**Step 1** On each Concentrator in the cluster, go to the Configuration>Policy Management> Traffic Management>Filters window.

**Step 2** From the Configuration>Policy Management>Traffic Management>Filters window choose **Public** from the Current Rules in Filter list and then click **Assign Rules to Filter**. The Configuration>Policy Management>Traffic Management>Assign Rules to Filter-Assign Rules to Filter window opens.

**Step 3** In the Available Rules list, choose **VCA In** and then click **Add**. VCA In moves to the Current Rules in Filter list.

**Step 4** In the Available Rules list, choose **VCA Out** and then click **Add**. VCA Out moves to the Current Rules in Filter list.

**Step 5** Add VCA in and VCA out filters to both Concentrator's public and private interfaces.

The functions of VCA In and VCA Out are as follows:

■ VCA In (forward/in)—Forwards any inbound (to this VPN 3000) UDP packet with a destination port of 9023 (VCA port).

■ VCA Out (forward/out)—Forwards any outbound (from this VPN 3000) UDP packet originating from source port 9023 (VCA port).

**Concentrator Load-Balancing Configuration**

The second step in load balancing is to configure each Concentrator in the cluster for load balancing. There are two parts to the configuration: cluster and device configuration. Cluster configuration must be the same for all Concentrators in the cluster. Device configuration parameters can vary across the cluster. The device parameters are Concentrator specific.

To configure load balancing on the Concentrator, go to the Configuration>System> Load Balancing window and complete the following parameters:

■ VPN Virtual Cluster IP Address field—Enter the single IP address that represents the entire virtual cluster. Choose an IP address that is within the public subnet address range shared by all the Concentrators in the virtual cluster.

■ VPN Virtual Cluster UDP Port field—9023 is the default UDP port address. If another application is using this port, enter the UDP destination port number you want to use for load balancing.

■ Encryption check box—The Concentrators in the virtual cluster communicate via LAN-to-LAN tunnels using IPSec. To ensure that all load-balancing information communicated between the Concentrators is encrypted, select this check box.

■ IPSec Shared Secret field—This option is available only if you have selected the preceding Encryption check box. Enter the IPSec shared secret for the virtual cluster. The shared secret is a common password that authenticates members of the cluster. IPSec uses the shared secret as a pre-shared key to establish secure tunnels between virtual cluster peers.

■ Verify Shared Secret field—Re-enter the IPSec shared secret.

- Load Balancing Enable check box—Select this check box to include this Concentrator in the virtual cluster.

- Priority field—Enter a priority for this VPN Concentrator within the virtual cluster. The priority is a number from 1 to 10 that indicates the likelihood of this device becoming the cluster master either at startup or when an existing cluster master fails. The higher you set the priority (for example 10), the more likely this device becomes the cluster master. If your cluster includes different models of Concentrators, it is recommended that you choose the device with the greatest load capacity to be the cluster master. For this reason, priority defaults are hardware dependent. If your cluster is made up of identical devices (for example, if all the devices in the virtual cluster are Concentrator 3060s), set the priority of every device to 10. Setting all identical devices to the highest priority shortens the length of time needed to select the virtual cluster master. The default priorities are as follows:

  — Concentrator 3005—1

  — Concentrator 3015—3

  — Concentrator 3030—5

  — Concentrator 3060—7

  — Concentrator 3080—9

- NAT Assigned IP Address field—If this Concentrator is behind a firewall using Network Address Translation (NAT), NAT has assigned it a public IP address. Enter the NAT IP address. If this device is not using NAT, enter **0.0.0.0**. The default setting is 0.0.0.0.

**Hardware Client Load-Balancing Configuration**

This is final step in configuring load balancing in the Hardware Client. In the Hardware Client, go to the Configuration>System>Tunneling Protocols>IPSec window. In the Remote Server field, verify the cluster virtual IP address is specified. If not, modify the Remote Server IP address to reflect the virtual, rather than a physical, IP address of the Master Concentrator. In the example in the figure, the cluster virtual IP address is 192.168.1.150.

To support the load-balancing feature, the Hardware Client must use release 3.5 software or later. In prior releases, the Hardware Client does not support redirect messages.

# Hardware Client System Status

**192.168.1.5**
Master

**192.168.1.6**
Secondary

**192.168.1.7**
Secondary

**192.168.1.5**

Internet

SOHO

Monitoring | System Status      Monday, 15 October 2001 14:21:04
     Refresh

**VPN Client Type:** 3002-8E
**Serial Number:** CAM01481749
**Bootcode Rev:** Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.0.Rel Feb 26 2001 10:39:17
**Software Rev:** Cisco Systems, Inc./VPN 3002 Hardware Client Version 4.0.1.Rel May 06 2003 12:46:38
**Up For:** 48:02:57
**Up Since:** 06/30/2003 10:47:24
**RAM Size:** 16 MB (Memory Status: Green)

[ Disconnect Now ]   [ Connect Now ]

**Tunnel Established to:** 192.168.1.5
**Duration:** 0:00:48
**Tunnel Type:** IPSec
**Security Associations:**

| Type | Remote Address | Encryption | Authentication | Octets In | Octets Out | Packets In | Packets Out | Other |
|------|----------------|-----------|----------------|-----------|-----------|-----------|-----------|-------|
| IKE | 192.168.1.5 | 3DES/MD5 | Pre-Shared Key | 1024 | 1140 | 7 | 9 | Aggressive Mode, DH Group2 |
| IPSec | 192.168.1.5 | 3DES | HMAC/MD5 | 0 | 0 | 0 | 0 | |
| IPSec | 0.0.0.0/0.0.0.0 | 3DES | HMAC/MD5 | 0 | 288 | 0 | 2 | |

     CSVPN 4.0—12-16

When the VCA filters are added, the Concentrator load balancing parameters are configured and the Hardware Client remote server address is added, you can launch the tunnel. In the example in the figure, the Cisco VPN 3002 attempted to connect to the cluster master, 192.168.1.150. From the cluster master, the Hardware Client received a re-direct message to connect to 192.168.1.5. In the Hardware Client Monitoring>System Status window, notice that the tunnel was established with 192.168.1.5.

# VPN Software Client Load-Balancing Configuration

CSVPN 4.0—12-17
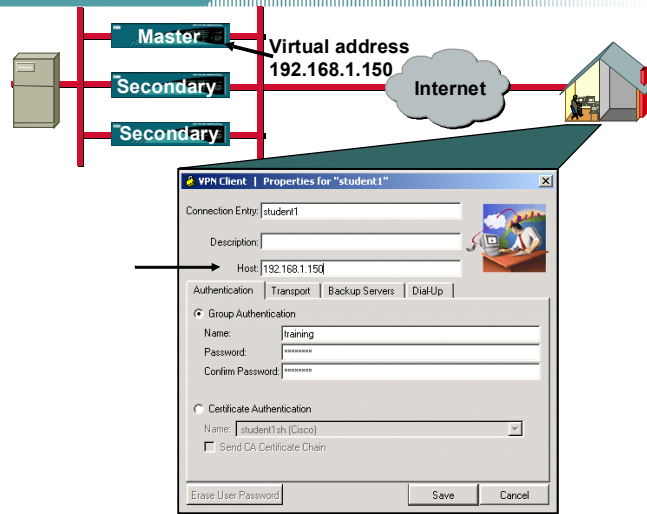
This is the final step in configuring load balancing in the Software Client. In the Software Client, go to the Start>Programs>Cisco Systems VPN Client>VPN Client window. In the Host name or IP address of remote server field, add the cluster virtual IP address. In the example in the figure, the cluster virtual IP address is 192.168.1.150.

# Overview of the Cisco VPN Client Reverse Route Injection Feature

This topic presents an overview of the Cisco Virtual Private Network (VPN) Client Reverse Route Injection (RRI) feature.
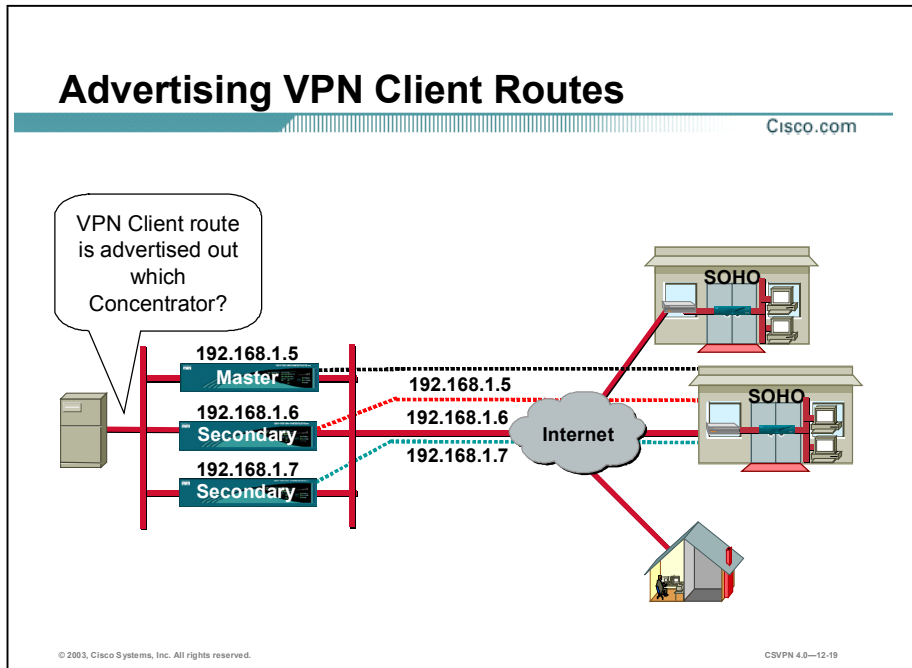


Load balancing enables the VPN client to connect to the least loaded Concentrator. The good news is the VPN client load is shared across multiple Concentrators. The bad news is how does a headend device connect to the client when it is connected to a different Concentrator each time a tunnel is established. The answer is RRI. Each time the VPN Client connects to a Concentrator, the Concentrator advertises the IP address of the VPN Client through its private interface. When the tunnel is disconnected, the Concentrator will cease to advertise the route. RRI enables a central site device to connect to the client regardless of which Concentrator the VPN Client is attached to at the time.

## RRI Feature

**Advertise host route**

**Tunnel established**

SOHO

Internet
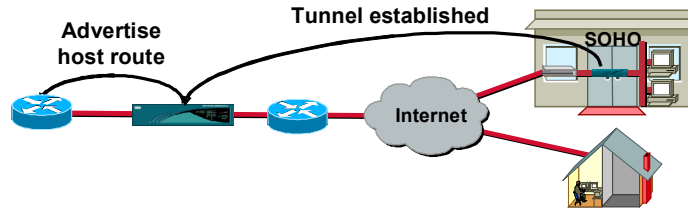
The following are the VPN Client RRI features:

• Client RRI
• Network extension RRI

Configuration | System | IP Routing | Reverse Route Injection

Configure system-wide *Reverse Route Injection* parameters. This feature adds specific routes to the routing table for distribution via RIP or OSPF to neighbouring routers for path discovery. Click on **Generate Hold Down Routes** to generate hold down routes based on configured address pools.

Client Reverse Route Injection ☐
Check to add non-local (to the private interface) client host routes to the routing table.

Network Extension Reverse Route Injection ☐
Check to add hardware client network extension connection routes to the routing table.

Address Pool Hold Down Routes
• Add or modify network address and subnet mask using the following standard format: n.n.n.n/n.n.n.n (e.g. 192.168.90.64/255.255.255.192).
• Enter each network address and subnet mask pair on a single line.
• If you are using the natural subnet mask, you may omit the subnet mask.

[Apply] [Cancel] [Generate Hold Down Routes]

CSVPN 4.0—12-20

After a VPN Client tunnel is established, the Concentrator can now add static or host routes to the routing table and announce these routes using OSPF or outbound RIP. There are two VPN Client applications within the RRI feature: client RRI and network extension RRI. (Address pool hold-down routes pertain to LAN-to-LAN applications and are not discussed in this lesson.)

Client RRI

Cisco.com

**Advertise host route**

**Tunnel established**

**Client mode**

Internet

Configuration | System | IP Routing | Reverse Route Injection

Configure system-wide *Reverse Route Injection* parameters. This feature adds specific routes to the routing table for distribution via RIP or OSPF to neighbouring routers for path discovery. Click on **Generate Hold Down Routes** to generate hold down routes based on configured address pools.

Client Reverse Route Injection ☑   Check to add non-local (to the private interface) client host routes to the routing table.

Network Extension ☐   Check to add hardware client network extension connection routes to the
Reverse Route Injection   routing table.

Address Pool
Hold Down Routes

• Add or modify network address and subnet mask using the
  following standard format: **n.n.n.n/n.n.n.n** (e.g.
  192.168.90.64/255.255.255.192).
• Enter each network address and subnet mask pair on a single line.
• If you are using the natural subnet mask, you may omit the
  subnet mask.

Apply   Cancel   Generate Hold Down Routes

© 2003, Cisco Systems, Inc. All rights reserved.                                    CSVPN 4.0—12-21

The VPN Client RRI feature applies to all VPN software and Hardware Clients using Port Address Translation (PAT) mode. To enable it, go to the Configuration>System>IP Routing>Reverse Route Injection window and select the **Client Reverse Route Injection** check box.

After the client tunnel is established, the Concentrator adds a host route to its routing table. The host route is advertised through the private interface providing OSPF, or outbound RIP is enabled on the private interface. The Concentrator deletes the route when the client disconnects.

# Client RRI—Routing Table

Cisco.com
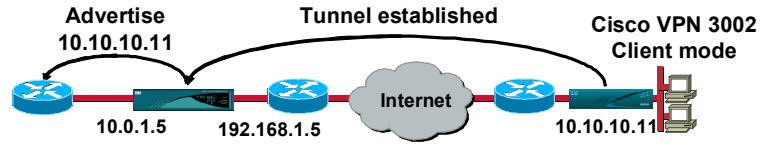
**Advertise 10.10.10.11**   **Tunnel established**   **Cisco VPN 3002 Client mode**

**Internet**

10.0.1.5   192.168.1.5   10.10.10.11

**Monitoring | Routing Table**

Clear Routes

Valid Routes: 4

**Tunnel established**

| Address | Mask | Next Hop | Interface | Protocol | Age | Metric |
|---|---|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.1.6 | 2 | Default | 0 | 1 |
| 10.0.1.0 | 255.255.255.0 | 0.0.0.0 | 1 | Local | 0 | 1 |
| 10.10.10.11 | 255.255.255.255 | 192.168.1.6 | 2 | Static | 0 | 1 |
| 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 2 | Local | 0 | 1 |

**No tunnel**

| Address | Mask | Next Hop | Interface | Protocol | Age | Metric |
|---|---|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.1.6 | 2 | Default | 0 | 1 |
| 10.0.1.0 | 255.255.255.0 | 0.0.0.0 | 1 | Local | 0 | 1 |
| 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 2 | Local | 0 | 1 |

CSVPN 4.0—12-22

In the example in the figure, Client RRI is enabled at the Concentrator and the Hardware Client is running in PAT mode. When the tunnel is launched, the Concentrator assigns the Hardware Client a virtual IP address: 10.10.10.11. Notice in the top routing table, 10.10.10.11 is listed and is advertised through the private interface on the Concentrator. When the tunnel is disconnected, the host entry is deleted from the routing table. Notice in the bottom routing table, the 10.10.10.11 host route was deleted because the tunnel was dropped.

## Network Extension RRI

Cisco.com

**Advertise host routes**

**Tunnel established**

**Cisco VPN 3002 Network Extension mode**

Internet

**192.168.201.2**

Configuration | System | IP Routing | Reverse Route Injection

Configure system-wide *Reverse Route Injection* parameters. This feature adds specific routes to the routing table for distribution via RIP or OSPF to neighbouring routers for path discovery. Click on **Generate Hold Down Routes** to generate hold down routes based on configured address pools.

Client Reverse Route Injection ☐          Check to add non-local (to the private interface) client host routes to the routing table.

Network Extension ☑
Reverse Route Injection          Check to add hardware client network extension connection routes to the routing table.

Address Pool
Hold Down Routes

- Add or modify network address and subnet mask using the following standard format: **n.n.n.n/n.n.n.n** (e.g. 192.168.90.64/255.255.255.192).
- Enter each network address and subnet mask pair on a single line.
- If you are using the natural subnet mask, you may omit the subnet mask.

[Apply]  [Cancel]  [Generate Hold Down Routes]

CSVPN 4.0—12-23

The Network Extension RRI feature applies only to a Hardware Client using Network Extension mode. To enable it, go to the Configuration>System>IP Routing> Reverse Route Injection window and select the **Network Extension Reverse Route Injection** check box.

When the tunnel is established, the Concentrator adds host routes to its routing table. The host routes are advertised through the private interface providing OSPF, or outbound RIP is enabled on the private interface. The routes are deleted when the client disconnects.

**Network Extension RRI—Routing Table**

Advertise 192.168.201.0 — Tunnel established — Cisco VPN 3002 Network Extension mode

10.0.1.5    192.168.1.5    Internet    192.168.201.2
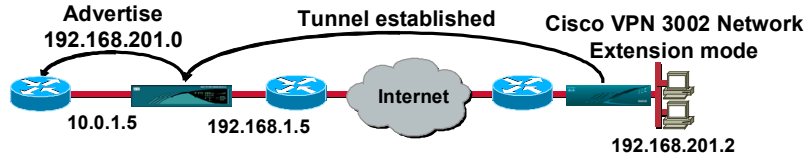
**Tunnel established**

Monitoring | Routing Table

Clear Routes

Valid Routes: 4

| Address | Mask | Next Hop | Interface | Protocol | Age | Metric |
|---|---|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.1.6 | 2 | Default | 0 | 1 |
| 10.0.1.0 | 255.255.255.0 | 0.0.0.0 | 1 | Local | 0 | 1 |
| 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 2 | Local | 0 | 1 |
| 192.168.201.0 | 255.255.255.0 | 192.168.1.6 | 2 | Static | 0 | 1 |

**No tunnel**

| Address | Mask | Next Hop | Interface | Protocol | Age | Metric |
|---|---|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.1.6 | 2 | Default | 0 | 1 |
| 10.0.1.0 | 255.255.255.0 | 0.0.0.0 | 1 | Local | 0 | 1 |
| 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 2 | Local | 0 | 1 |

CSVPN 4.0—12-24

In the example in the figure, Network Extension RRI is enabled at the Concentrator, and the Hardware Client is running in network extension mode. When the tunnel is launched, the Concentrator adds a route for the network behind the Hardware Client, 192.168.201.0, and advertises it through the private interface (the top routing table). When the tunnel is disconnected, the network address entry is deleted from the routing table (the bottom routing table).

# Summary

This topic summarizes the information that was presented in this lesson.

## Summary

- **The Concentrator can be configured to advertise routes as VPN Clients connect.**
- **The VPN Client can be configured to connect to a backup Concentrator if the primary Concentrator is unavailable.**
- **The Concentrators can be configured for load balancing to spread the connection load between co-located Concentrators.**

CSVPN 4.0—12-26

# Lab Exercise—Configuring Cisco VPN 3002 Hardware Client Reverse Route Injection

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to install and configure the Cisco Virtual Private Network (VPN) 3002 Hardware Client and configure the Cisco VPN 3000 Concentrator to enable IPSec encrypted tunnels. Work with your lab exercise partner to complete the following tasks:

■ Complete the lab exercise setup.

■ Configure the Cisco VPN 3000 Series Concentrator for Network Extension Reverse Route Injection.

■ Monitor the routing table in the Cisco VPN 3000 Series Concentrator with Network Extension Reverse Route Injection enabled.

■ Configure the Cisco VPN 3000 Series Concentrator for Client Reverse Route Injection.

■ Configure the Cisco VPN 3002 Hardware Client for client mode.

■ Monitor the Routing Table in the Cisco VPN 3000 Series Concentrator with Client Reverse Route Injection enabled.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



**Lab Visual Objective**
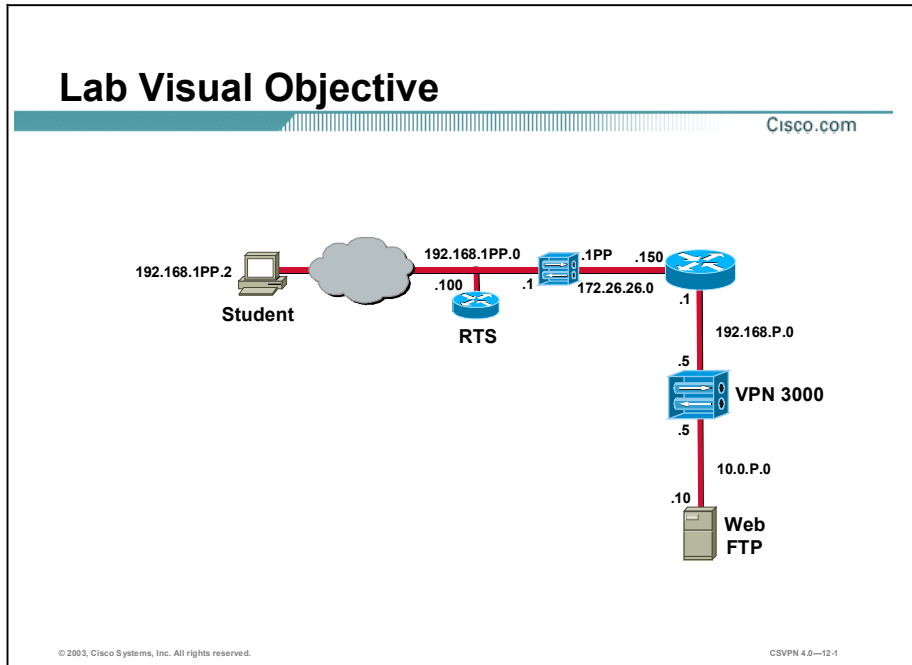
## Scenario

Your company wants you to implement a VPN using remotely located Hardware Clients terminating at centrally located Concentrators. You want the IP address of the remote client to be advertised by the private interface of the Concentrator.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment is setup as follows:

■ Ensure that your student PC is powered on.

■ Ensure that your student PC IP addresses are configured correctly:

— Primary IP address—192.168.1PP.2
(where PP = two-digit pod number [for example, Pod 1 is 01])

— Default gateway IP address—192.168.1PP.1
(where PP = two-digit pod number)

■ Ensure that your Concentrator is powered on.

■ Ensure that your Hardware Client is powered on.

# Task 2—Configure the Cisco VPN 3000 Series Concentrator for Network Extension Reverse Route Injection

With Network Extension Reverse Route Injection (RRI), the feature is enabled on the Concentrator. Once enabled, a new route is added to the routing table every time an IPSec tunnel is established. Complete the following steps to configure the Concentrator for Network Extension RRI:

**Step 1** Launch Internet Explorer by double-clicking the desktop icon.

**Step 2** Enter a Concentrator's public interface IP address of **192.168.P.5** in the IP Address field of Internet Explorer (where P = pod number). The Connection/Login Status window opens.

**Step 3** Click **Connect Now** to connect the IPSec tunnel.

**Step 4** Complete the following sub-steps from the Hardware Client Interactive Authentication window:

| Note | The following entries are case sensitive and should be entered in all lower case. |
| --- | --- |

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

3. Click **Continue** to establish the IPSec tunnel to the remote Concentrator. The Hardware Client Connection/Login Status window opens and is replaced by the Cisco VPN 3000 Concentrator Series Manager.

**Step 5** Log into the Concentrator using the administrator account:

```
Login: admin
Password: admin
```

**Step 6** From the Monitoring menu tree, drill down to **Routing Table**.

**Step 7** From the Monitoring>Routing Table window, answer the following question:

Q1)     What three routes are listed?

A)     _____

**Step 8** From the Configuration menu tree, drill down to **System>IP Routing>Reverse Route Injection**.

**Step 9** Select the **Network Extension Reverse Route Injection** check box and click **Apply**.

**Step 10** Save the changes.

**Step 11** Log out of the Concentrator. Do not close Internet Explorer.

**Step 12** Enter a Hardware Client private interface (network extension mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field (where PP = double digit pod number).

**Step 13** Log into the Hardware Client using the administrator account:

```
Login: admin
Password: admin
```

Both the username (login) and password are always case sensitive.

**Step 14** From the Monitoring menu tree, drill down to **System Status**.

**Step 15** Click **Disconnect Now**. It may take several moments for the Hardware Client to disconnect.

**Step 16** Log out of the Hardware Client. Do not close Internet Explorer.

# Task 3—Monitor the Routing Table in the Cisco VPN 3000 Series Concentrator with Network Extension Reverse Route Injection Enabled

Complete the following steps to re-connect the IPSec tunnel and monitor the changes to the Concentrator's routing table:

**Step 1** Enter a Concentrator's public interface IP address of **192.168.P.5** in the IP Address field (where P = pod number). The Connection/Login Status window opens.

**Step 2** Click **Connect Now** to connect the IPSec tunnel.

**Step 3** Complete the following sub-steps from the Hardware Client Interactive Authentication window.

| Note | The following entries are case sensitive and should be entered in all lower case. |
|------|-----------------------------------------------------------------------------------|

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

3. Click **Continue** to establish the IPSec tunnel to the remote Concentrator. The Hardware Client Connection/Login Status window opens and is replaced by the Cisco VPN 3000 Concentrator Series Manager.

**Step 4** Log into the Concentrator using the administrator account:

```
Login: admin
Password: admin
```

**Step 5** From the Monitoring menu tree, drill down to **Routing Table**.

**Step 6** From the Monitoring>Routing Table window, answer the following question and fill in the blanks:

Q2) What four routes are listed?

A) _____

Q3) With Network Extension RRI enabled, if the Hardware Client establishes an IPSec tunnel, a route is _____(added, deleted) to the routing table. When the IPSec tunnel is disconnected, the route is _____ (added, deleted) from the routing table.

**Step 7**     Do not log out of the Concentrator.

# Task 4—Configure the Cisco VPN 3000 Series Concentrator for Client Reverse Route Injection

The IPSec tunnel from the Hardware Client to the Concentrator should still be established. Complete the following steps to configure the Concentrator for Client RRI:

**Step 1**     From the Configuration menu tree, drill down to **System>IP Routing>Reverse Route Injection**.

**Step 2**     Select the **Client Reverse Route Injection** check box.

**Step 3**     Deselect the **Network Extension Reverse Route Injection** check box.

**Step 4**     Click **Apply**.

**Step 5**     Save the changes.

**Step 6**     From the Monitoring menu tree, drill down to **Routing Table**.

**Step 7**     From the Monitoring>Routing Table window, answer the following question:

Q4)     What three routes are listed?

A)     _____

**Step 8**     Log out of the Concentrator. Do not close Internet Explorer.

# Task 5—Configure the Cisco VPN 3002 Hardware Client for Client Mode

Complete the following steps to configure the Hardware Client for Client Mode:

**Step 1**     Enter a Hardware Client private interface (network extension mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field.

(where PP = two-digit pod number)

**Step 2**     Log into the Hardware Client using the administrator account:

```
Login: admin
Password: admin
```

Both the username (login) and password are always case sensitive.

**Step 3**     In the main window, choose **Configuration>Quick Configuration>PAT**, and complete the following sub-steps:

1.  Select **Yes**.

2.  Click **Continue**.

**Step 4**     From the Quick Configuration toolbar, click **Done**.

**Step 5**     Log out of the Hardware Client.

# Task 6—Monitor the Routing Table in the Cisco VPN 3000 Series Concentrator with Client Reverse Route Injection Enabled

Complete the following steps to re-connect the IPSec tunnel and monitor the Concentrator's routing table:

**Step 1** Enter a Concentrator's public interface IP address of **192.168.P.5** in the IP Address field (where P = pod number). The Connection/Login Status window opens.

**Step 2** Click **Connect Now** to connect the IPSec tunnel.

**Step 3** Complete the following sub-steps from the Hardware Client Interactive Authentication window. These entries are all case sensitive. Use lower case.

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

3. Click **Continue** to establish the IPSec tunnel to the remote Concentrator. The Hardware Client Connection/Login Status window opens and is replaced by the Cisco VPN 3000 Concentrator Series Manager.

**Step 4** Log into the Concentrator using the administrator account:

```
Login: admin
Password: admin
```

**Step 5** From the Monitoring menu tree, drill down to **Routing Table**.

**Step 6** From the Monitoring>Routing Table window, answer the following question and fill in the blanks:

Q5) What three routes are listed? (The Hardware Client assigned address is part of the 10.0.P.0 network.)

A) _____

---

**Note** The Concentrator assigns an IP address to the Hardware Client during IPSec tunnel establishment. The assigned IP address is part of the 10.0.P.0 network. When viewing the routing table, the Hardware Client's assigned address is part of the 10.0.P.0 address space and does not appear as a separate entry in the table.

---

Q6) When the Client RRI is enabled, if the Hardware Client establishes an IPSec tunnel, a host route is _____ (added, deleted) to the routing table. When the IPSec tunnel is disconnected, the host route is _____ (added, deleted) from the routing table.

**Step 7** Log out of the Concentrator.

**Step 8** Enter a Hardware Client private interface (network extension mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field.

(where PP = two-digit pod number)

---

**Step 9** Log into the Hardware Client using the administrator account:

```
Login: admin
Password: admin
```

Both the username (login) and password are always case sensitive.

**Step 10** From the Monitoring menu tree, drill down to **System Status**.

**Step 11** Click **Disconnect Now**. It may take several moments for the Hardware Client to disconnect.

**Step 12** Log out of the Hardware Client and close Internet Explorer.

**13**

# Configure the Cisco Virtual Private Network 3002 Hardware Client for Software Auto-Update

## Overview

This lesson includes the following topics:

■ Objectives

■ Overview and configuration of the Cisco VPN 3002 Hardware Client software auto-update feature

■ Monitoring the Cisco VPN 3002 Hardware Client software auto-update feature

■ Summary

■ Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Describe the Hardware Client software auto-update feature.**
- **Configure the Hardware Client for software auto-update.**
- **Monitor the Hardware Client software auto-update.**

CSVPN 4.0—13-2

# Overview and Configuration of the Cisco VPN 3002 Hardware Client Software Auto-Update Feature

This topic presents an overview of the Cisco Virtual Private Network (VPN) 3002 Hardware Client software auto-update feature.
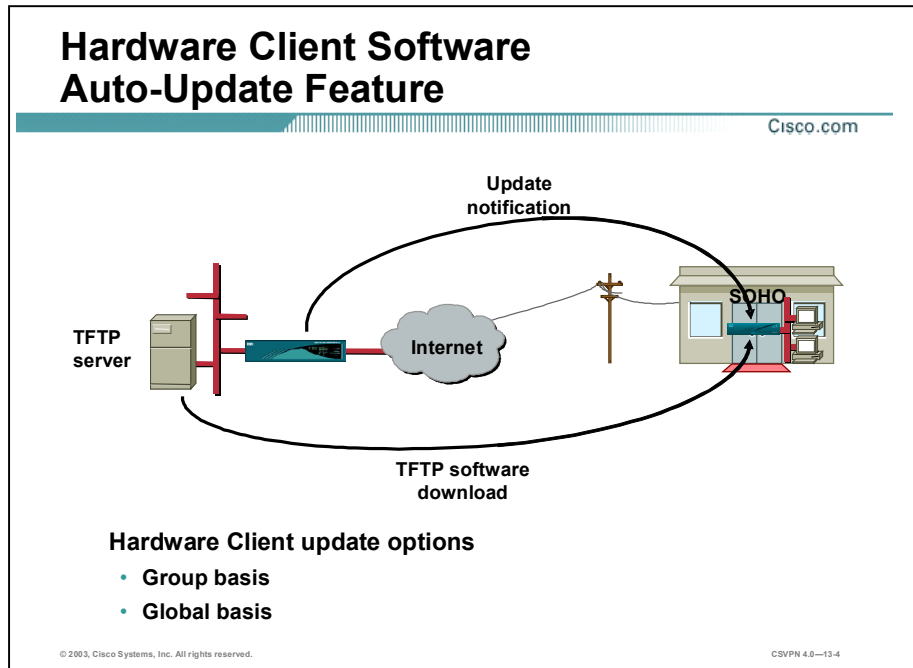


The Cisco VPN 3002 Hardware Client update feature enables administrators at a central location automatically update software for Hardware Clients deployed in diverse locations. When you enable Hardware Client update, upon connection, the central-site Cisco VPN Concentrator sends an Internet Key Exchange (IKE) packet that contains an encrypted message, which notifies the VPN 3002 about acceptable versions of executable system software and their locations. If the Hardware Client is not running an acceptable version, its software is automatically updated via TFTP. During the update process, the Hardware Client logs event messages at the start of the update. When the update completes, the Hardware Client reboots automatically.

If the Hardware Client is already connected to the Concentrator, the administrator has the option of sending an update notification message. The update message notifies the Hardware Client about acceptable versions of software and their locations. If the Hardware Client is not running an acceptable version, its software is automatically updated via TFTP. The administrator may choose to update all the Hardware Client in their network all at once. Or, the administrator may choose to update VPN 3002s on a group-by-group basis. This lesson discusses both options.

**Three-Step Group Update Process**

Cisco.com

Configuration | System | Client Update | Enable

Check the box to enable Client Update functionality.

Enabled ☑

[Apply] [Cancel]

Configuration | User Management | Groups | Client Update | Add

Add client update information.

Client Type: vpn3002 — Enter the client type (e.g. *windows* or *vpn3002*) that is to be updated.

URL: ftp://10.0.1.10/vpn3002-4.0.1.Rel-k9.bin — Enter the URL of the file from which to update. The URL must point to an appropriate file type for the client.

Revisions: 4.01 Release — Enter a comma separated list of valid revisions. The URL above *must* be one of these revisions.

[Add] [Cancel]

Success

The connected clients in that group will receive a notice that they need to update their software.

[Continue]

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—13-5

Configuring the Hardware Client software auto-update feature is a three-step process:

**Step 1**   Enable Hardware Client update functionality on the Concentrator.

**Step 2**   Set the group update parameters (for example, Hardware Client and Software Client type, URL, and revisions).

**Step 3**   (Optional.) Send an update notice to active clients. Update notice is explained later in this lesson.

**Step 1—Enable the Software Auto-Update Feature**

Cisco.com

**Configuration | System | Client Update**                                        Save⊟

This section of the Manager lets you configure Client Update.

In the left frame, or in the list of links below, click the function you want:

- Enable -- enable Client Update.
- Entries -- configure the client type and URL entries for Client Update.

**Configuration | System | Client Update | Enable**

Check the box to enable Client Update functionality.

Enabled ☑

[ Apply ]  [ Cancel ]
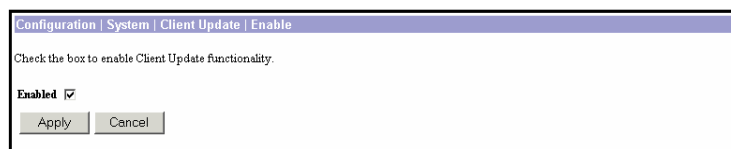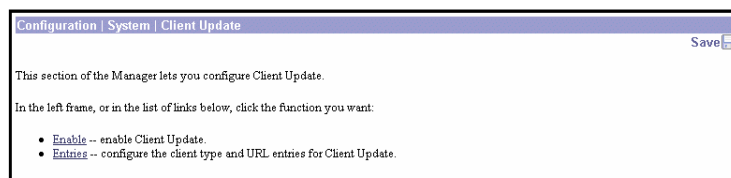
CSVPN 4.0—13-6

Complete the following steps to enable the auto-update feature:

**Step 1**   Choose the **Configuration>System>Client Update** window and click the **Enable** link. The Configuration>System>Client Update>Enable window opens.

**Step 2**   Select the **Enabled** check box.

**Step 3**   Click **Apply**.

When enabled, the administrator must decide how to update the Cisco VPN clients: globally or by group. With a global update, all clients will be updated to a specific release of software from a specific server. If a more systematic, group-by-group approach is preferred, different servers can update different groups, at different times, to different releases of software. There is further discussion of global and group configurations later in the lesson.

## Modifying Group Updates

Configuration | User Management | Groups

Save Needed

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, select a group and click the appropriate button.

**Actions** | **Current Groups** | **Modify**

training (Internally Configured)

Add Group
Modify Group
Delete Group

Authentication Servers
Authorization Servers
Accounting Servers
Address Pools
Client Update
Bandwidth Assignment

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—13-7

When updating the Hardware Client, the administrator must decide whether a system-wide update or a systematic update is in order. Complete the following steps to configure a group update:

**Step 1**  Choose the Configuration>User Management>Groups window and select the appropriate group in the Current Groups field.

**Step 2**  Click **Client Update** in the Modify column.

# Step 2—Set the Group Update Parameters

In the previous step, the administrator selected the Client Update button. In this step, the administrator configures group-specific VPN Client auto-update parameters. Choose the **Configuration>System>Client Update>Entries** window to view the Client Update Entries list. Because no updates have been configured, the list displays Empty. Click **Add** under the Actions column to add a new VPN Client update entry. The Manager opens the Configuration> System>Client Update>Entries>Add window. The entries are as follows:

■ Client Type—For the VPN 3002, the entry must be vpn3002 (case- and space-sensitive).

■ URL—The format is tftp://*server_address/directory/filename*. The server address can be either an IP address or a hostname if you have configured a DNS server (for example, tftp://10.0.1.10/vpn3002-4.0.1.Rel-k9.bin, where 10.0.1.10 is the server address and vpn3002-4.0.1.Rel-k9.bin is the filename on the TFTP server).

■ Revisions—Enter a comma-separated list of software images appropriate for the Hardware Client (for example, 4.0.1 Release). The entries are case sensitive. The Hardware Client considers 4.0.1 Release and 4.0.1 release different versions of software.

If the VPN Client is already running a software version on the list, it does not need a software update. If the Hardware Client is not running a software version on the list, an update is needed. The Hardware Client software is automatically updated via TFTP.

# Group Update Entries

**Configuration | User Management | Groups | Client Update**

Save Needed

This section lets you configure Client Update entries.

Click the **Add** button to add an entry, or select an entry and click **Modify** or **Delete**. Click **Done** to finish.

**Client Update entries for training**

| Update Entry | Actions |
|---|---|
| vpn3002 (4.01 Release) | Add |
| | Modify |
| | Delete |
| | Done |

CSVPN 4.0—13-9

The Configuration>User Management>Groups>Client Update window displays the entries for the training group. Each entry shows the platform and acceptable software version. In the example in the figure, vpn3002 (4.01 Release) is listed; vpn3002 is the Hardware Client type, and 4.01 Release is the preferred software revision.

## Step 3—Send an Update Notice

Cisco.com

**Administration | Software Update**

This section of the Manager lets you update software on the VPN 3000 Concentrator or clients.

In the left frame, or in the list of links below, click the function you want:

- Concentrator -- update the VPN 3000 Concentrator software.
- Clients -- update hardware and software clients.

**Administration | Software Update | Clients**

This screen allows you to update software on clients. Select a group to only update clients in that group.

Please refer to your product documentation to determine which versions of the software client support this feature.

Group [ training ]

[ Upgrade Clients Now ]  [ Cancel ]

**Success**

The connected clients in that group will receive a notice that they need to update their software.

[ Continue ]

CSVPN 4.0—13-10

The last step is to send an optional update notification to the Hardware Client:

**Step 1**  Choose the **Administration>Software Update** window, and click the **Clients** link. The Administration>Software Update>Clients window opens.

**Step 2**  Choose the Hardware Client group for this update from the Group drop-down menu. The default is All, which lets you update the software for all groups. The Concentrator updates VPN clients by group, in batches of ten, at five-minute intervals.

**Step 3**  Click **Upgrade Clients Now** to send the update notification. If sent successfully, the Success window opens.

In the example in the figure, the training group is selected to get an update notification. When the user clicked **Upgrade Clients Now**, the Success window opened. The connected VPN Clients in the training group will receive an update notification message. This is a proactive, forceful attempt to update clients without waiting for the client to drop the IPSec tunnel and reconnect. This process may be necessary in cases where an update is immediately required for functionality, for security reasons, or for clients that have "always on" connections. The disconnected members of the training group will receive an update message the next time they connect to the Concentrator.

**Global Update Parameters**
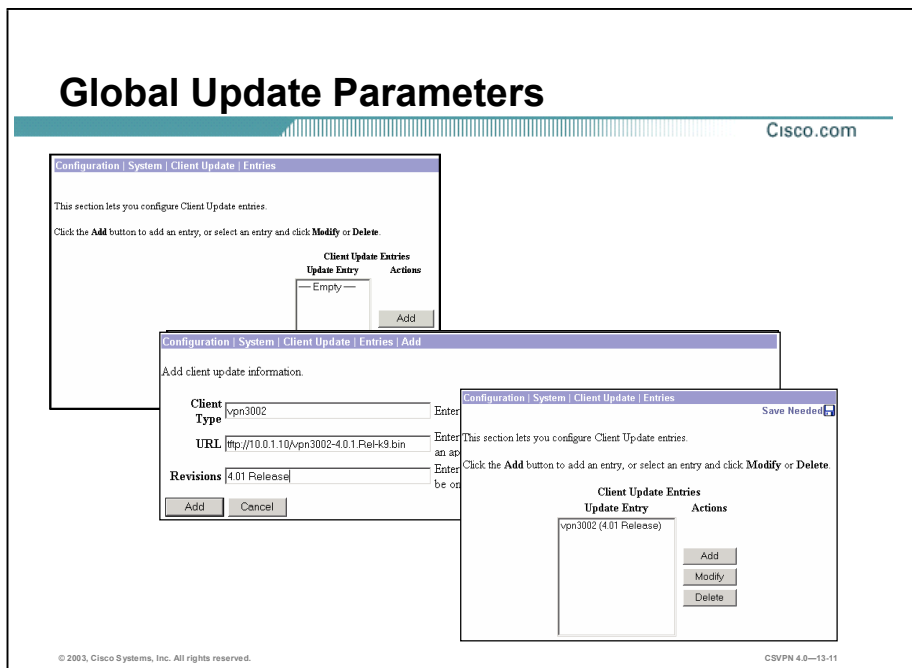
Parameters can be updated on a global basis. With global updates, all groups upgrade to the same software from the same TFTP server. Complete the following steps to define global update parameters:

**Step 1**  Choose the **Configuration>System>Client Update>Entries** window, and click **Add**. The Configuration>System>Client Update>Entries>Add window opens.

**Step 2**  Configure the global VPN Client type, URL, and revision number by entering the information in the corresponding fields.

**Step 3**  Click **Apply**. The final results are viewable in Configuration>System>Client Update>Entries window.

In the example in the figure, the VPN Client type is the VPN 3002. The Hardware Client software file vpn3002-4.0.1.Rel-k9.bin is available for download from the TFTP server 10.0.1.10. The valid revision level is set to 4.01 Release. This information can be sent to a specific group, or all groups. Choose the Administration>Software Update>Clients window to send the update notification message.

# Monitoring the Cisco VPN 3002 Hardware Client Software Auto-Update Feature

When the update notification is sent, the administrator can monitor the status of the upgrade on the Hardware Client.



In the Monitoring>Filterable Event Log window, the administrator can view the Hardware Client update information. To only view the update-specific information, scroll down in the Event Class window and select **AUTOUPDATE**. In the example in the figure, there are two versions. In the event log on the left, the Hardware Client received a notification message. The software version on the Hardware Client is up to date. No upgrade was necessary.

In the event log on the right, the Hardware Client software version does not match the software version in the notification message. The Hardware Client software is updated from 3.5.1.Rel to 3.5.2.Rel. The software file vpn3002-3_5_2_Rel-k9.bin is downloaded from the TFTP server 10.0.1.10. The image was successfully loaded and the Hardware Client automatically rebooted.

The Hardware Client stores image files in two locations: the active location, which stores the image currently running on the system, and the backup location. Updating the image overwrites the stored image file in the backup location and makes it the active location for the next reboot. The client auto-update process includes a test to validate the updated image. In the unlikely event that a VPN Client auto-update is unsuccessful, the VPN Client does not reboot, and the invalid image does not become active. The auto-update feature retries up to twenty times at three-minute intervals. If an auto-update is unsuccessful, the log files contain information indicating TFTP failures.

# Release Is Case Sensitive

**Monitoring | Filterable Event Log**

Select Filter Options

Event Class [All Classes / AUTH / AUTHDBG / AUTHDECODE]   Severities [ALL / 1 / 2 / 3]

Client IP Address [0.0.0.0]   Events/Page [100]

Direction [Oldest to Newest]

[|◄◄] [◄◄] [►►] [►►|]   [Get Log]   [Clear Log]

```
18 03/05/2002 13:34:10.510 SEV=4 AUTOUPDATE/6 RPT=1
Current version 3.5.2.Rel does not match 3.5.2.rel.

19 03/05/2002 13:34:10.510 SEV=4 AUTOUPDATE/7 RPT=1
Updating firmware to 3.5.2.rel from 3.5.2.Rel.

20 03/05/2002 13:34:10.510 SEV=4 AUTOUPDATE/12 RPT=1
Update firmware will now begin using file vpn3002-3_5_2_Rel-k9.bin on server 10.
0.1.10 [0A00010A].
```

[|◄◄] [◄◄] [►►] [►►|]

CSVPN 4.0—13-14

The auto-update event log messages are used to troubleshoot the Hardware Client software upgrade. In the example in the figure, the administrator misspelled the software version number, 3.5.2.rel. The proper, case-sensitive spelling is 3.5.2.Rel. The software version is case and space sensitive. In this example, every time a notification message is sent or the Hardware Client reconnects to the Concentrator, an update takes place.

# Summary

This topic summarizes the information that was presented in this lesson.

## Summary

- **Hardware Client operating software can be updated automatically.**
- **The auto-update feature is configured in the Concentrator.**
- **Update notification is sent to the Hardware Client automatically at connection time or manually by the administrator.**
- **If the Hardware Client release version in the notification message does not match the Hardware Client running version, the Hardware Client upgrades its software.**

CSVPN 4.0—13-16

# Lab Exercise—Configure the Cisco VPN 3002 Hardware Client Auto-Update Feature

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to install and configure the Cisco Virtual Private Network (VPN) 3002 Hardware Client and the Cisco VPN 3000 Series Concentrator to enable IPSec encrypted tunnels. Work with your lab exercise partner to complete the following tasks:

■ Complete the lab exercise setup.

■ Configure the Cisco VPN 3002 Hardware Client auto-update feature.

■ Automatically update the Cisco VPN 3002 Hardware Client system software.

■ Edit the auto-update revisions field.

■ Force the Cisco VPN 3002 Hardware Client to automatically update its software.

■ Disable the Cisco VPN 3002 Hardware Client auto-update feature.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
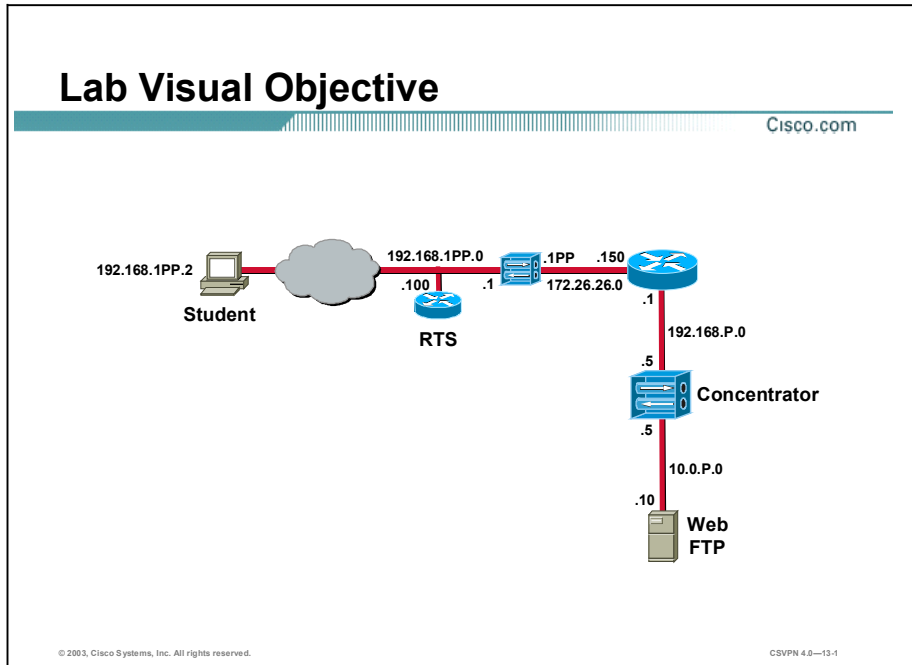


## Scenario

Your company wants you to implement an automatic update strategy for your remotely located Hardware Clients. You must configure the Concentrator to use the Hardware Client auto-update feature. You must monitor the auto-update to make sure it was completed successfully.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment is setup as follows:

■ Ensure that your student PC is powered on.

■ Ensure that your student PC IP addresses are configured correctly:

— Primary IP address—192.168.1PP.2
(where PP = two-digit pod number [for example, Pod 1 is 01])

— Default gateway IP address—192.168.1PP.1
(where PP = two-digit pod number)

■ Ensure that your Concentrator is powered on.

- Ensure that your Hardware Client is powered on.

- Ensure that the Trivial File Transfer Protocol (TFTP) server is loaded with the correct version of the Hardware Client operating software.

Your instructor will provide you with the correct username and password to log into the student PC.

## Task 2—Configure the Cisco VPN 3002 Hardware Client Auto-Update Feature

Complete the following steps to configure the Hardware Client auto-update feature:

| Note | This procedure assumes that Windows 2000 is already running on the student PC. |

**Step 1** Launch Internet Explorer by double-clicking the desktop icon.

**Step 2** Enter a Concentrator's public interface IP address of **192.168.P.5** in the Internet Explorer Address field (where P = pod number). The Connection/Login Status window opens.

**Step 3** Click **Connect Now** to connect the IPSec tunnel.

**Step 4** Complete the following sub-steps from the Concentrator Interactive Authentication window:

These entries are all case-sensitive. Use lower case.

1. Enter **studentP** in the User Name field.
(where P = pod number)

2. Enter **studentP** in the Password field.
(where P = pod number)

3. Click **Continue** to establish the tunnel to the remote Concentrator. The Hardware Client Connection/Login Status window will appear and then be replaced by the Cisco VPN 3000 Concentrator Series Manager.

**Step 5** Log into the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

Login: **admin**

Password: **admin**

The username (login) and password are always case sensitive.

**Step 6** From Configuration menu, drill down to **System>Client Update**. The Configuration>System>Client Update window opens.

**Step 7** Select **Enable.** The Configuration>System>Client Update>Enable window opens.

**Step 8** Verify the **Enabled** check box is selected.

**Step 9** Click **Apply**.

**Step 10** From Configuration menu, drill down to **User Management>Groups**.

**Step 11** Choose **training** from the Current Group list.

**Step 12** Click **Client Update**. The Configuration>User Management>Groups> Client Update window opens.

**Step 13** Click **Add**. The Configuration>User Management>Groups>Client Update>Add window opens.

**Step 14** Complete the following sub-steps from the Configuration>User Management> Groups>Client Update>Add window:

    1. Enter **vpn3002** in the Client Type field.

    2. Enter **tftp://10.0.P.10/vpn3002-4.0.1.Rel-k9.bin** in the URL field.

    3. Enter **4.0.1.Rel** in the Revisions field.

    4. Click **Add**.

**Step 15** Save the changes.

**Step 16** Logout of the Concentrator and do not close Internet Explorer.

# Task 3—Automatically Update the Cisco VPN 3002 Hardware Client System Software

During tunnel establishment, the Concentrator sends a message to the Hardware Client that a specific revision of operating software is required. If the revision in the message matches the current operating software, the event log will log the event. The Hardware Client will not try to update the system software. Complete the follow steps to receive an auto-update message:

**Step 1** Enter a Hardware Client private interface (Client mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field.

(where PP = two-digit pod number)

**Step 2** Log into the Hardware Client using the administrator account:

```
Login: admin
Password: admin
```

Both the username (login) and password are always case sensitive.

**Step 3** From the Monitoring menu, drill down to **System Status**.

**Step 4** Click **Disconnect Now**. It takes several moments for the Hardware Client tunnel to disconnect.

**Step 5** Click **Connect Now** to connect the tunnel. The Hardware Client Interactive Authentication window opens.

**Step 6** Complete the following sub-steps from the Hardware Client Interactive Authentication window:

| Note | These entries are all case-sensitive. Use lower case. |
|------|-------------------------------------------------------|

    1. Enter **studentP** in the User Name field.
       (where P = pod number)

    2. Enter **studentP** in the Password field.
       (where P = pod number)

**Step 7**   Click **Continue** to establish the tunnel to the remote Concentrator. It takes several moments for the IPSec tunnel to connect.

**Step 8**   From the Monitoring menu, drill down to **Filterable Event Log**.

**Step 9**   Complete the following sub-steps from the Monitoring>Filterable Event Log window:

1. Choose **Auto Update** from the Event Classes list.

2. Click |<< to retrieve the log. Repeat as needed until you see the auto-update event message.

**Step 10**  Answer the following question from the event log:

Q1)   Is the current version of the Hardware Client software up to date?

A)   _____

**Step 11**  Click **Clear Log** after you finish viewing the Filterable Event Log.

**Step 12**  Logout of the Hardware Client and do not close Internet Explorer.

## Task 4—Edit the Auto-Update Revisions Field

In the last task, no update was performed since the Hardware Client software was up to date. In this task, you will edit the revision field to force an update. Complete the follow steps to modify the revision field:

**Step 1**   Enter a Concentrator's public interface IP address of **192.168.P.5** in the Internet Explorer Address field (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 2**   Log into the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

Login: **admin**

Password: **admin**

The username (login) and password are always case sensitive.

**Step 3**   From Configuration menu, drill down to **User Management>Groups**.

**Step 4**   Choose **training** from the Current Group list.

**Step 5**   Click **Client Update**. The Configuration>User Management>Groups> Client Update window opens.

**Step 6**   Select **vpn3002 (4.0.1.Rel)** from the Update Entry column.

**Step 7**   Click **Modify**. The Configuration>User Management>Groups>Client Update> Modify window opens.

**Step 8**   Complete the following sub-steps from the Configuration>User Management> Groups>Client Update>Modify window:

1. In the Revisions field, change the field to read **4.0.0.Rel**. (In this case, you will force an update since the Hardware Client current release, 4.0.0.Rel, does not match the download update release name, 4.0.1.Rel.)

2. Click **Apply**.

**Step 9**   Save the changes.

**Step 10** Log out of the Concentrator and do not close Internet Explorer.

## Task 5—Force the Cisco VPN 3002 Hardware Client to Automatically Update its Software

During tunnel establishment, the Concentrator sends an update message to the Hardware Client that a specific revision of operating software is required. In the prior task, you modified the revision name. This will force the Hardware Client to update its operating software. Complete the follow steps to force a software update:

**Step 1** Enter a Hardware Client private interface (Client mode) IP address of **192.168.1PP.1** in the Internet Explorer Address field.

(where PP = two-digit pod number)

**Step 2** Log into the Hardware Client using the administrator account:

```
Login: admin
Password: admin
```

Both the username (login) and password are always case sensitive.

**Step 3** From the Monitoring menu, drill down to **System Status**.

**Step 4** Click **Disconnect Now**. It takes several moments for the Hardware Client tunnel to disconnect.

**Step 5** Click **Connect Now** to connect the tunnel. The Hardware Client Interactive Authentication window opens.

**Step 6** Complete the following sub-steps from the Hardware Client Interactive Authentication window.

| Note | These entries are all case sensitive. Use lower case. |
| --- | --- |

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. **Enter studentP** in the Password field.
   (where P = pod number)

**Step 7** Click **Continue** to establish the tunnel to the remote Concentrator. It takes several moments for the Hardware Client tunnel to connect.

**Step 8** From the Monitoring menu, drill down to **Filterable Event Log**.

**Step 9** Complete the following sub-steps from the Monitoring>Filterable Event Log window:

1. Choose **Auto Update** from the Event Classes list.

2. Click **<<** to retrieve the log. Repeat as needed to see all of the auto-update messages.

**Step 10** Answer the following questions and fill in the blanks from the Event log:

Q2) Does the Hardware Client's current version of software match the downloaded request?

A) _____

Q3) The Hardware Client will upgrade its software to version _____ from version
_____.

Q4) Which file will the Hardware TFTP download?

A) _____

Q5) What is the IP address of the TFTP server?

A) _____

Q6) Was the updated image successfully downloaded?

A) _____

Q7) The update process took approximately how many minutes?

A) _____

**Step 11** Log out of the Hardware Client and do not close Internet Explorer.

## Task 6—Disable the Cisco VPN 3002 Hardware Client Auto-Update Feature

Complete the following steps to disable the Hardware Client auto-update feature:

**Step 1** Enter a Concentrator private interface IP address of **192.168.P.5** in the Internet Explorer Address field (where P = pod number). The Connection/Login Status window opens.

**Step 2** Click **Connect Now** to connect the tunnel.

**Step 3** Complete the following sub-steps from the Hardware Client Interactive Authentication window.

---

**Note** These entries are all case sensitive. Use lower case.

---

1. Enter **studentP** in the User Name field.
   (where P = pod number)

2. Enter **studentP** in the Password field.
   (where P = pod number)

---

**Note** When re-establishing the IPSec tunnel, the Concentrator sends an update message to the Hardware Client. You have approximately 2 minutes after clicking Continue to disable the Client Update feature before the Hardware Client performs another update and re-boot. If you miss the 2-minute window, wait for the Hardware Client to re-boot, and then try to complete the disable commands again.

---

3. Click Continue to establish the tunnel to the remote Concentrator. The Hardware Client Connection/Login Status window opens and is then replaced by the Cisco VPN 3000 Concentrator Series Manager.

**Step 4** Log into the Concentrator using the administrator account:

---

```
Login: admin

Password: admin
```

**Step 5**   From Configuration menu, drill down to **System>Client Update**. The Configuration>System> Client Update window opens.

**Step 6**   Select **Enable**. The Configuration>System>Client Update>Enable window opens.

**Step 7**   Deselect the Enabled check box.

**Step 8**   Click **Apply**.

**Step 9**   From Configuration menu, drill down to **User Management>Groups**.

**Step 10**   Choose **training** from the Current Group list.

**Step 11**   Click **Client Update**. The Configuration>User Management>Groups> Client Update window opens.

**Step 12**   Select **vpn3002 (4.0.0.Rel)** from the Update Entry column, and then click **Delete**.

**Step 13**   Click **Done**.

**Step 14**   Save the changes.

**Step 15**   Log out of the Concentrator and close Internet Explorer.

# 14

# Configuring the Cisco Virtual Private Network 3000 Series Concentrator for IPSec over UDP and IPSec over TCP

## Overview

This lesson includes the following topics:

- Objectives

- Overview of Port Address Translation

- Configuring IPSec over UDP

- Configuring NAT Traversal

- Configuring IPSec over TCP

- Monitoring session statistics

- Summary

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon the completion of this lesson, you will be able to perform the following tasks:**

- **Describe how address translation works at the port level.**
- **Explain the IPSec address translation issue.**
- **Describe the three Concentrator translation options.**
- **Configure the Concentrator for IPSec over UDP.**
- **Configure the Concentrator for NAT Traversal.**
- **Configure the Concentrator for IPSec over TCP.**
- **Monitor session statistics.**

CSVPN 4.0—14-2

# Overview of Port Address Translation

This topic presents an overview of Port Address Translation (PAT).
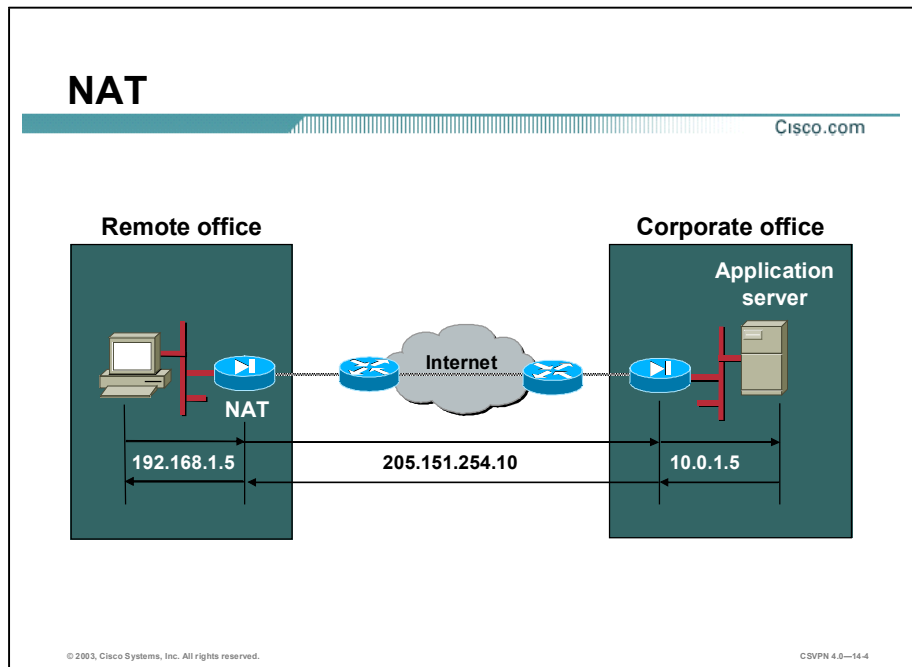


Before IPSec over UDP or IPSec over TCP is discussed, the issues surrounding IPSec through PAT or Network Address Translation (NAT) devices must first be discussed.

Internet Assigned Numbers Authority (IANA) created nonroutable private address space:

■ Class A 10.0.0.0 to 10.255.255.255

■ Class B 172.16.0.0 to 172.31.255.255

■ Class C 192.168.0.0 to 192.168.255.255

Nonroutable private address space gives companies more addresses to use within their companies, such as the company Intranet. These private addresses are easily routed within the company space. The issue is how does a company route the information between campuses or companies over the Internet. These addresses are not globally unique; the Internet cannot route them. Only globally unique addresses can be routed through the Internet. NAT enables nonroutable address space to be translated into routable, globally unique addresses. A NAT device translates a nonroutable address into one of the globally unique addresses assigned to the company. The newly addressed frame is routable through the Internet.

In the example in the figure, at the remote end, the PC has been assigned a nonroutable address space of 192.168.1.5. The end-user wants to communicate with the corporate server at a different location. The frame must travel through the Internet to travel between sites. Unfortunately, with

the current private addressing scheme, the frame cannot be routed through the Internet. The issue is solved by first sending the frame to a NAT device. By using a NAT device, the nonroutable address can be translated into a routable address of 205.151.254.10. The frame is now routable and is sent through the Internet. The corporate applications server receives the data, formulates a response, and returns a response to 205.151.254.10, the NAT device. The NAT device translates the frame address from 205.151.254.10 back to 192.168.1.5.

NAT works on a one-for-one relationship: one nonroutable address in, and one routable address out. A problem develops when the company has a large number of nonroutable source addresses that need to translate into a finite number of Class C routable addresses. The routable address pool may soon dry up.

NAT (cont.)

Cisco.com

Remote office

Corporate office

Application server

Internet

NAT

192.168.1.5     205.151.254.10     10.0.1.5

192.168.1.6     205.151.254.10     10.0.1.5

?

    CSVPN 4.0—14-5
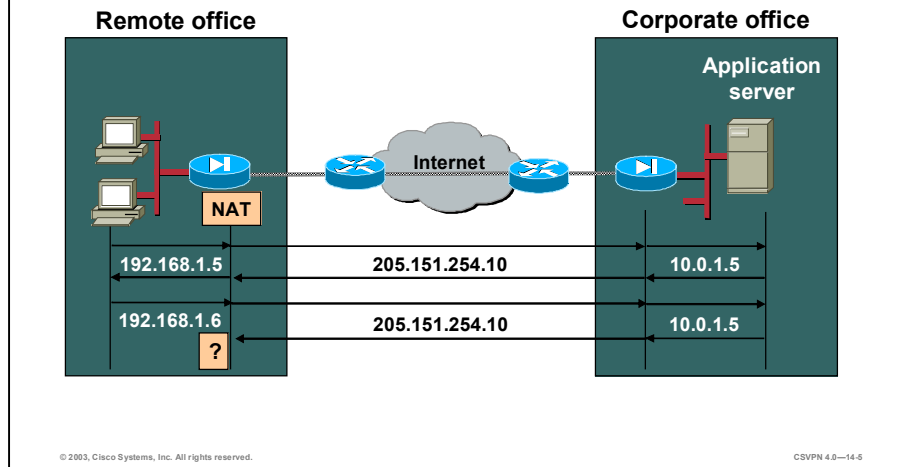
The challenge comes in when there are multiple devices at the remote end. In the example in the figure, there are two computers with separate nonroutable addresses of 192.168.1.5 and 192.168.1.6. Both devices need to talk to the application server through a Network Address Translation (NAT) device. The issue is there is only one available globally unique IP address.

In the first instance, 192.168.1.5 sends a message to the NAT device, which translates the source address from 192.168.1.5 to 205.151.254.10. The message is routed through the Internet. The corporate application server receives the message, formulates a response, and sends a reply back to 205.151.254.10 address, the NAT device. The NAT device in turn translates the routable address back to 192.168.1.5.

When the second of the two PCs tries to send a frame, 192.168.1.6 sends a message to the application server. The PC forwards the frame to the NAT device, which translates the source address from 192.168.1.6 to 205.151.254.10. The message is sent through the Internet. The corporate application server receives the message, formulates a response, and sends a reply via the 205.151.254.10 address. The NAT device will be confused. Who is the recipient of the frame, PC one, or PC two? The NAT device cannot differentiate between the two remote PCs.

This is where a PAT device fits.

PAT

Cisco.com

Remote office

Corporate office

Application server

Internet

PAT

| 192.168.1.5 - Port 10000 | 205.151.254.10 – Port 600 | 10.0.1.5 |
| 192.168.1.6 - Port 10000 | 205.151.254.10 – Port 601 | 10.0.1.5 |
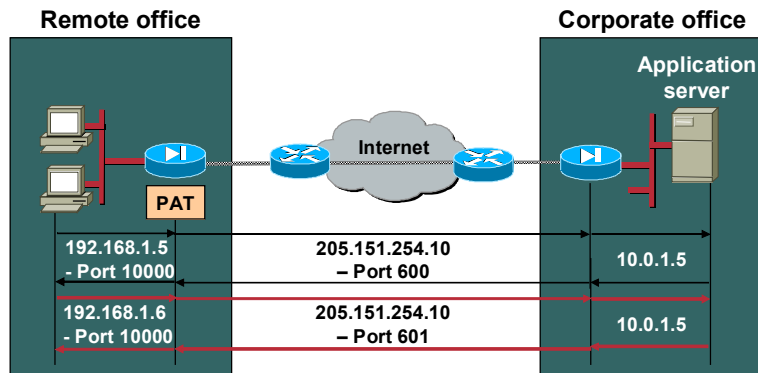
CSVPN 4.0—14-6

Port Address Translation (PAT) works at the TCP and UDP port level. It enables multiple devices to be multiplexed over one globally unique IP address. Each time the PAT device receives a frame; it translates the frame into an IP address and a port number. A unique port number supports each device. One IP address can support multiple devices using different port numbers for each device.

In the example in the figure, during the first instance, the first PC, 192.168.1.5, sends a message to the PAT device, which translates the address from 192.168.1.5 port 10000, to 205.151.254.10 port 600. The message is routed through the Internet. The corporate application server receives the message, formulates a response, and sends a reply via the 205.151.254.10 port 600. The PAT device receives the message and in turn translates the response address back to 192.168.1.5 port 10000.

In the next instance, the second PC, 192.168.1.6, sends a message to the PAT device, which translates the address from 192.168.1.6 port 10000, to 205.151.254.10 port 601. The message is sent through the Internet. The corporate application server receives the message, formulates a response, and sends a reply via 205.151.254.10 port 601. The PAT device receives the message and translates the response from 205.151.254.10 port 601, to 192.168.1.6 port 10000. In this case, the information is sent to the second PC. The UDP port numbers, 600 and 601, are used to differentiate between unique remote devices.

## PAT (cont.)

Cisco.com

**Remote office**

**Corporate office**

**Application server**

Internet

PAT
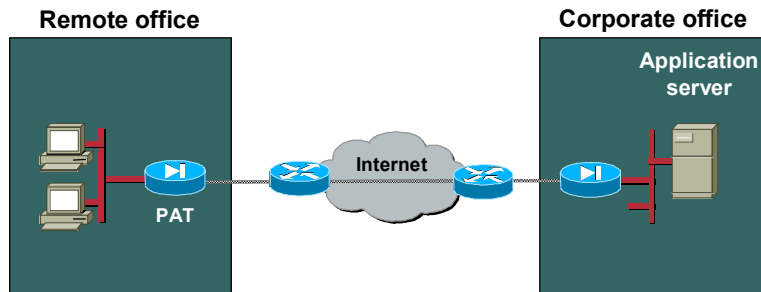
| Source Address | Port # | Source Address | Port # |
|---|---|---|---|
| 192.168.1.5 | 10000 | 205.151.254.10 | 600 |
| 192.168.1.6 | 10000 | 205.151.254.10 | 601 |

CSVPN 4.0—14-7

Within the Port Address Translation (PAT) devices, there is a translation table that is used to translate between nonroutable and routable IP addresses. In the example in the figure, a remote PC needs to send a message to the corporate office. To do so, the remote office sends the message to the PAT device. In the PAT device is a translation table. The fist entry in the table dictates that a nonroutable address and port number of 192.168.1.5 port 10000 should be translated into a routable IP address and port number of 205.151.254.10 port 600. When translated, the PAT device forwards the message to the corporate office.

PAT works well, but there is an issue with Virtual Private Network (VPN) applications.

**IKE and UDP Issue**
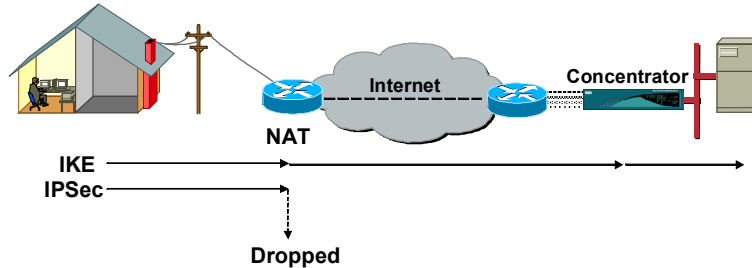
There are many situations where customers require a Cisco VPN Client to operate in an environment where standard Encapsulating Security Payload (ESP) (Protocol 50) or User Datagram Protocol (UDP) 500 Internet Key Exchange (IKE) can either not function, or not function transparently (without modification to existing firewall rules). VPN uses IKE for tunnel setup and Security Association (SA) negotiations. IKE uses UDP so a nonroutable IP address and port number can be translated into a routable public address and port number. PAT can translate IKE packets using its inherent UDP port number. The problem arises when the VPN device tries to get the IPSec session established. IPSec uses ESP encapsulation protocol. ESP does not use UDP port numbers. The PAT method of translating UDP port numbers does not work with IPSec. The translating device drops the IPSec frame.

Situations where standard ESP or UDP 500 does not work include the following:

■ A small home office router performing PAT.

■ PAT-provided IP address behind a large router. This could exist if a service provider provides non-public addresses to clients and then performs port address translation. This scenario is identical to that documented above.

**IPSec over UDP—Proprietary**

Cisco.com
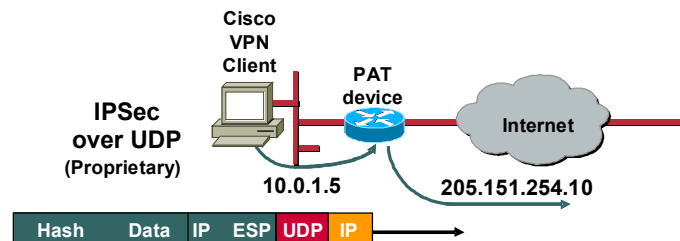
Cisco has created a proprietary fix to solve the IPSec PAT translation issue. By default, in the Cisco VPN 3000 Series Concentrator a standard IPSec datagram is wrapped in ESP and IP with no UDP port number. If the frame must traverse a NAT device, the Concentrator can be programmed to add a UDP header between the outer IP address and the ESP header. After the configuration change, when the datagram arrives at the PAT device the datagram address can be translated due to the UDP encapsulation.

IPSec over UDP is negotiated during tunnel establishment. During tunnel negotiations, if enabled in both the Cisco VPN Client and the Concentrator, IPSec is wrapped in UDP for the duration of the tunnel. This is configured on a group-by-group basis. Those groups whose frames traverse a NAT device can be configured to support IPSec over UDP. All other groups can be left at the default, with IPSec over UDP disabled. Some groups may require IPSec over UDP, while other groups may not.

**NAT Traversal—Standards-Based IPSec over UDP**

Cisco.com

Cisco VPN Client

NAT-T
(Standards-based IPSec over UDP)

PAT device

Internet

Concentrator

10.0.1.5

205.151.254.10

Initiator

Responder

UDP (X,500) … VID

UDP (500, X) …VID, NAT-D, NAT-D

UDP (X, 4500) …NAT-D, NAT-D

UDP (4500, X) …

| Hash | Data | IP | ESP | UDP | IP |

4500

CSVPN 4.0—14-10
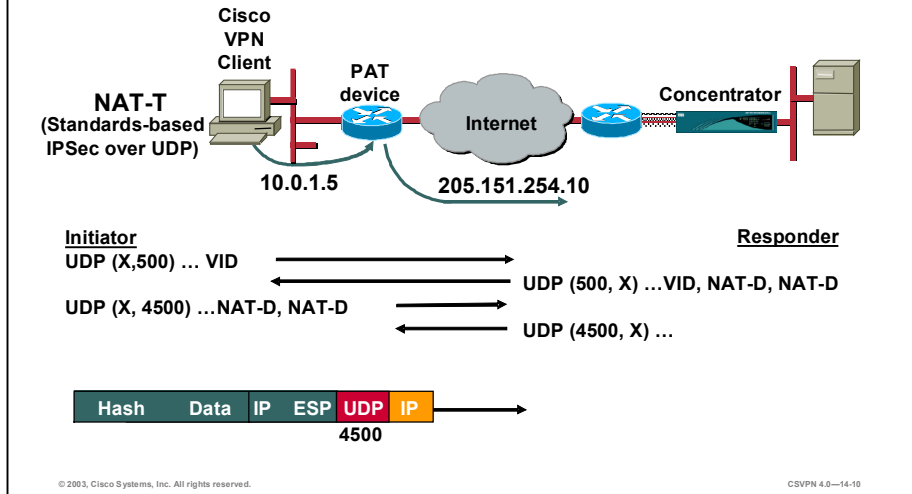
Network Address Translation Traversal (NAT-T) is a standard-based IPSec over UDP solution. NAT-T performs two tasks: detects if both ends support NAT-T and detects intermediate NAT devices along the transmission path. During IKE phase 1, the client and IPSec gateway exchange Vendor Identification (VID) packets. A NAT-T VID must be sent and received by both ends in order for the NAT-T negotiations to continue.

Next, NAT-Discovery (NAT-D) payloads are exchanged. The second task of NAT-T is to determine if there are any NAT devices along the transmission path. Intervening NAT devices will change the IP address or port numbers of the data packets. NAT-Discovery (NAT-D) payloads are exchanged to determine if there are any IP address or port number changes. There are two NAT-D payload packets sent in each direction. Each NAT-D payload is a hash of the original IP address and port number; one NAT-D packet for the source IP address and port number, and another for destination IP address and port number. After receiving the NAT-D packets, both ends compare the received address and port number with the hashed NAT-D payloads. If they match, there are no NAT devices along the transmission path. If they do not match, a NAT device translated either the IP address or port address. NAT-T should be performed. The IPSec packet is wrapped in a UDP packet with a port address of 4500.

In the example in the figure, the Cisco VPN Client and Concentrator exchange NAT-T VID packets. Both ends support NAT-T, the NAT-T negotiations continue. In packets two and three, both ends exchange NAT-D payloads. After comparing the NAT-D hashed IP address and port number with the IKE packet IP address and port number, the IP addresses and port numbers do not match. The IKE packet address was modified as the packet transited the NAT device. As a result, both ends change the UDP port number to 4500. The remaining IPSec packets are wrapped in a UDP header using port number 4500, NAT-T encapsulation. If both IPSec over UDP and NAT-T are enabled, NAT-T takes precedence.

**IPSec over TCP**

Cisco.com

Cisco
VPN
Client

PAT
device

IPSec
over TCP
(System-wide)

Internet

10.0.1.5

205.151.254.10

| Hash | Data | IP | ESP | TCP | IP |
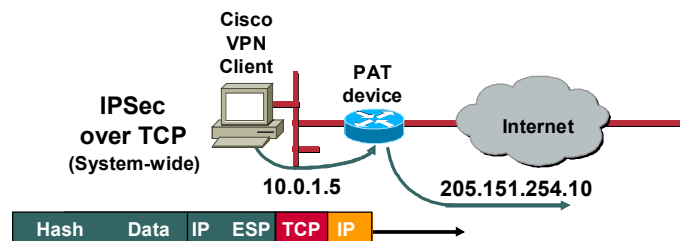
CSVPN 4.0—14-11

A third type of transparent tunneling support is IPSec over TCP. Concentrator devices support IPSec over UDP, NAT-T, or IPSec over TCP. With IPSec over TCP, there is no room for negotiation like there is in IPSec over UDP. IPSec over TCP packets are encapsulated from the start of the tunnel establishment cycle. From the very beginning, all traffic to the Concentrator is encapsulated in TCP. At the point in which IKE would normally negotiate the use of IPSec over UDP, IPSec over TCP is already active. In the Concentrator and the Cisco VPN Clients, IPSec over TCP takes precedence over both NAT-T and IPSec over UDP.

The goal of IPSec over TCP is to allow the Cisco VPN Clients to operate in the environments by using TCP to encapsulate both IKE and ESP. This takes advantage of the known fact that most firewalls allow outgoing TCP traffic and the inbound packets associated with the outbound connection. Using TCP is preferred over UDP through firewalls since state can be maintained for TCP packets resulting in higher security. The TCP implementation defaults to port 10000, but does not restrict the ability for the administrator to configure the Cisco VPN Client to listen on different ports.

Although TCP will be used to encapsulate IKE and IPSec, this feature is not intended to provide the reliability found in a fully deployed TCP implementation. The application layer (IKE) already provides much of the reliability needed.

## IPSec Through PAT Mode

Cisco.com

**Client**

**PAT**

**Internet**

**Concentrator**

| | | Data | IP | | |
|---|---|---|---|---|---|
| **IPSec** | Hash | Data | IP | ESP | IP |
| **IPSec over UDP (Proprietary)** | Hash | Data | IP | ESP | UDP IP |
| | | | | | or |
| **IPSec over UDP (NAT-T)** | Hash | Data | IP | ESP | UDP IP |
| | | | | | or |
| **IPSec over TCP (Proprietary)** | Hash | Data | IP | ESP | TCP IP |

**IPSec through PAT mode**
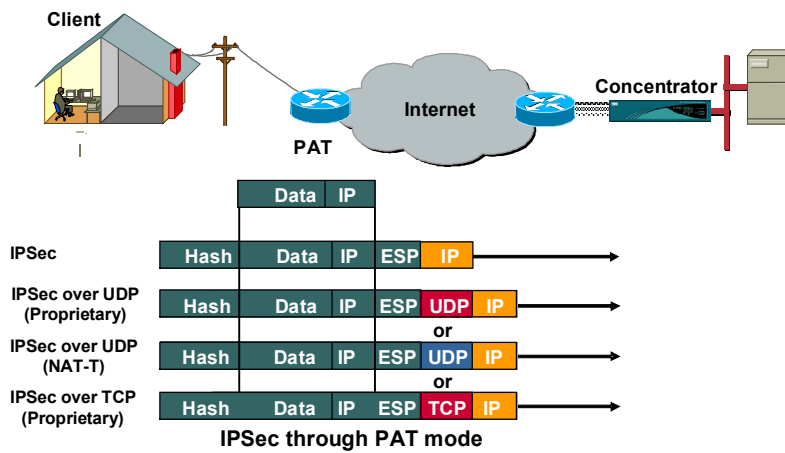
CSVPN 4.0—14-12

There are three IPSec through NAT applications: IPSec over UDP, NAT-T, and IPSec over TCP. NAT-T is a global attribute. IPSec over UDP (proprietary version) is a group attribute. The use of NAT-T or IPSec over UDP is negotiated during tunnel setup. If IPSec over UDP is enabled at both ends, and NAT-T is disabled, IPSec packets are encapsulated in proprietary UDP packets. If both IPSec over UDP and NAT-T are enabled, and a NAT device is discovered in the transmission path, IPSec packets are encapsulated using NAT-T. If no NAT device is discovered, UDP encapsulation of the IPSec packets is performed.

IPSec over TCP is a system-wide feature. Groups do not negotiate it. If enabled at both ends, it is on from the start of the IKE negotiations. If both NAT-T and IPSec over TCP are enabled, IPSec over TCP takes precedence. It is enabled globally, across all groups.

# Configuring IPSec over UDP

This topic presents an overview of configuring IPSec over UDP.



Configuring IPSec over UDP in the Concentrator is a two-step process. IPSec over UDP must be enabled first. Complete the following steps to configure IPSec over UDP:

**Step 1**  Choose **Configuration>User Management>Groups**. The Groups window opens.

**Step 2**  Select a group.

**Step 3**  Within the Client Config tab, select the **IPSec over UDP** check box.

**Step 4**  You must define an IPSec over UDP Port number by entering any UDP port number between 4001 and 49151, except for 4500, which is used for NAT-T, in the IPSec over UDP port number field. The default is 10000.

IPSec over UDP is configured on a group-by-group basis on the Concentrator. When IPSec over UDP is enabled, the defined UDP port number will be pushed down to the Cisco VPN Client via Mode configuration.

Software Client Configuration—
IPSec over UDP
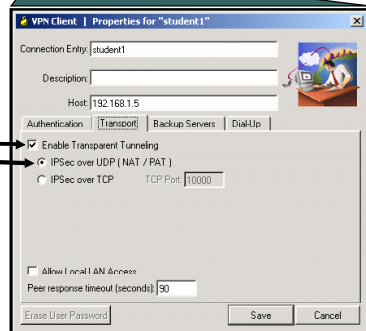
For IPSec over UDP to work, it must be enabled in both the Cisco VPN Client and the Concentrator. By default, the feature is enabled in the Cisco VPN Client but disabled in the Concentrator. To verify the Cisco VPN Client configuration, select the Cisco VPN Client **Transport** tab, and ensure that the Enable Transparent Tunneling check box and the IPSec over UDP radio button are selected. Click **Save** after you verify that IPSec over UDP is enabled in the Cisco VPN Client.

# Configuring NAT Traversal

This topic presents an overview of configuring NAT-T.



## Concentrator Configuration—NAT-T
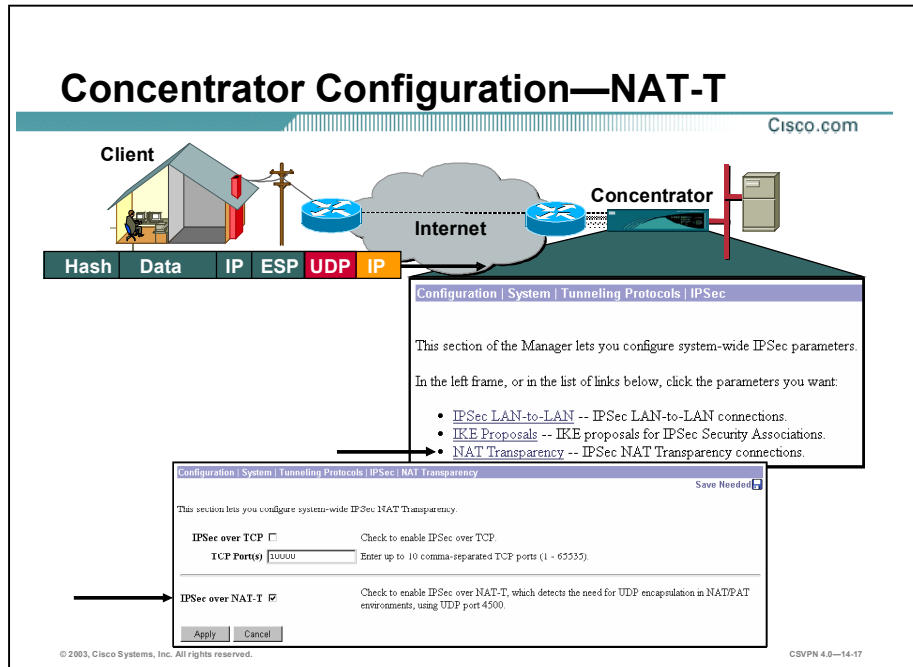
For NAT-T to work, it must be enabled in both the Cisco VPN Client and the Concentrator. Choose **Configuration>System>Tunneling Protocols**. The Tunneling Protocols window opens. Select **NAT Transparency** to enable NAT-T on the Concentrator. Select **IPSec over NAT** from the NAT Transparency window. NAT-T is enabled on a system-wide basis for all Client-to-LAN connections. NAT-T is configurable on an individual basis for LAN-to-LAN connections.

**Software Client Configuration—NAT-T**

Cisco.com

Client

Internet

Concentrator

VPN Client | Properties for "student1"

Connection Entry: student1

Description:

Host: 192.168.1.5

Authentication | Transport | Backup Servers | Dial-Up

☑ Enable Transparent Tunneling
◉ IPSec over UDP ( NAT / PAT )
○ IPSec over TCP    TCP Port: 10000

☐ Allow Local LAN Access
Peer response timeout (seconds): 90

Erase User Password    Save    Cancel
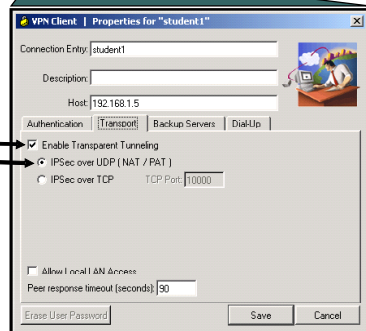
© 2003, Cisco Systems, Inc. All rights reserved.    CSVPN 4.0—14-18

Transparent tunneling must also be enabled on the Software Client for NAT-T to work. Transparent tunneling is enabled by default. Complete the following steps to view transparent tunneling in the software client:

**Step 1**  Highlight the connection entry you wish to modify.

**Step 2**  Choose **Connection Entries>Modify**. The Properties window opens.

**Step 3**  Select the **Transport** tab.

**Step 4**  View the **Enable Transparent Tunneling** check box.

**Step 5**  View the **Allow IPSec over UDP** radio button.

During IKE negotiations, the use of NAT-T and IPSec over UDP is negotiated. If both are enabled on the Concentrator, NAT-T takes precedence.

# Configuring IPSec over TCP

This topic presents an overview of configuring IPSec over TCP.
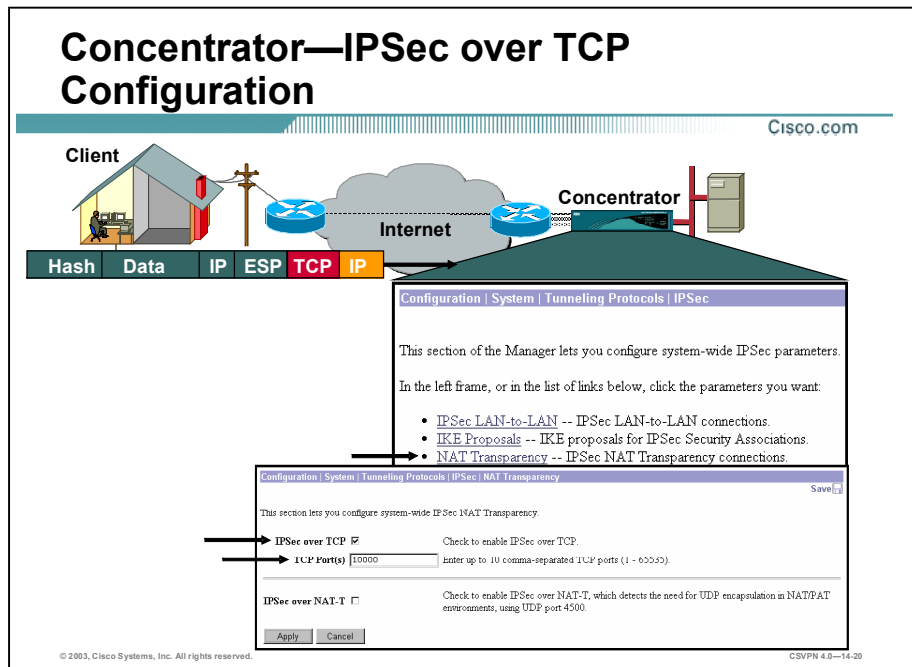


The last configuration example is IPSec over TCP. IPSec over TCP must be enabled in both the Cisco VPN Client and the Concentrator for it to work. Complete the following steps to enable IPSec over TCP in the Concentrator:

**Step 1**  Choose **Configuration>System>Tunneling Protocols>IPSec** to verify the Concentrator configuration. The IPSec window opens.

**Step 2**  Click the **NAT Transparency** link. The Configuration>System>Tunneling Protocols>IPSec> NAT Transparency window opens.

**Step 3**  From this window, ensure that the IPSec over TCP check box is selected and that the TCP port number is supplied.

Up to 10 comma-delimited port addresses can be supplied. Different remote Cisco VPN Clients can use different TCP port numbers. The pool of usable TCP port numbers is defined in the Concentrator. The port number used by each Cisco VPN Client is defined on the individual Cisco VPN Client.

This is a global parameter. If IPSec over TCP is enabled on both the Concentrator and the Cisco VPN Client, all frames are encapsulated in IPSec over TCP regardless of which group the Cisco VPN Client belongs to.

Hardware Client—IPSec over TCP Configuration

By default, NAT-T and IPSec over UDP are enabled on the Hardware Client. To enable IPSec over TCP, the IPSec over TCP feature must be enabled and a TCP port number be defined. Complete the following steps to configure the Hardware Client for IPSec over TCP:

**Step 1**    Choose Configuration>System>Tunneling Protocols>IPSec. The IPSec window opens.

**Step 2**    Select the **IPSec over TCP** check box.

**Step 3**    In the IPSec over TCP Port field, enter the correct IPSec over TCP port number. You can enter any TCP port number from 1–65535, but it must match one of the TCP port numbers programmed into the Concentrator TCP port(s) field, see the Concentrator Configuration>System>Tunneling Protocols>IPSec>NAT Transparency screen for the TCP port numbers that have been programmed.

Software Client—IPSec over TCP Configuration
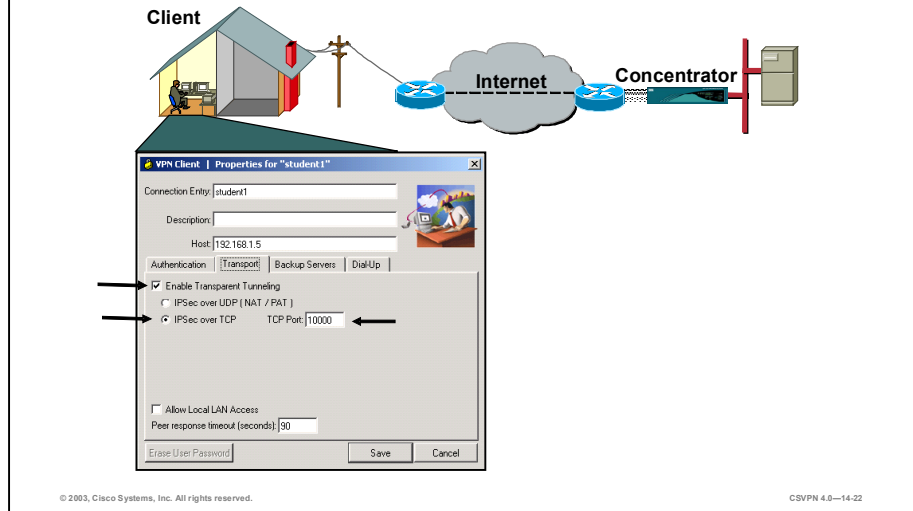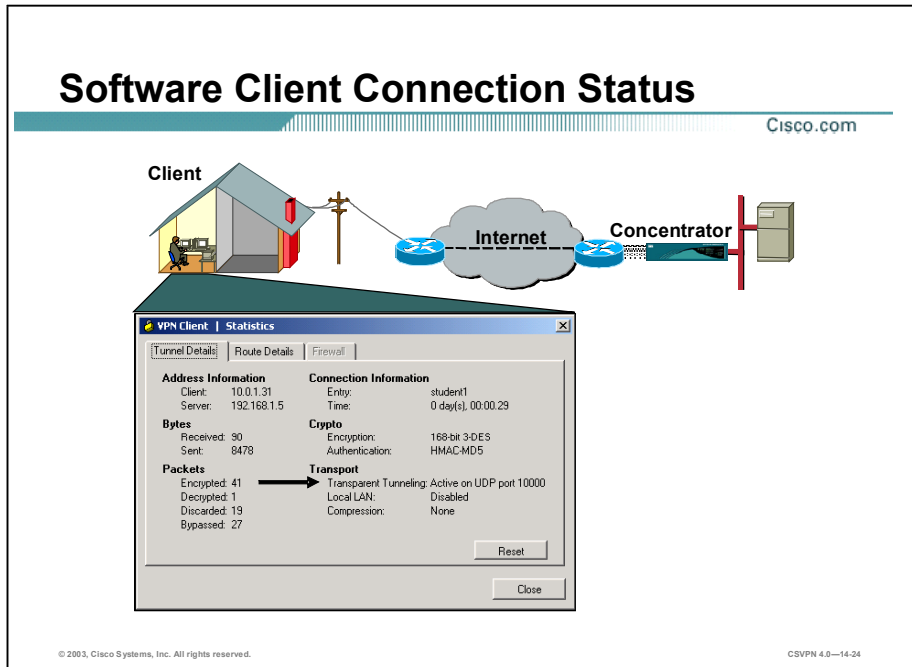
Complete the following steps to configure IPSec over TCP in the software client:

**Step 1**    Highlight the connection entry you wish to modify.

**Step 2**    Choose **Connection Entries>Modify**. The Properties window opens.

**Step 3**    Select the **Transport** tab.

**Step 4**    Select the **Enable Transparent Tunneling** check box.

**Step 5**    Select the **Use IPSec over TCP** radio button.

**Step 6**    Enter the TCP port number in the TCP port field. You can enter any TCP port number from 1–65535, but it must match one of the TCP port numbers programmed into the Concentrator TCP port(s) field, see the Concentrator Configuration>System>Tunneling Protocols>IPSec>NAT Transparency screen for the TCP port numbers that have been programmed.

# Monitoring Session Statistics

This topic presents an overview of Concentrator and Cisco VPN Client session statistics.



The administrator can check the status of the session in both the Software Client and Concentrator. Within the Statistics window, you can check whether transparent tunneling is active or inactive. If active, the encapsulation type and port number are available. In the example in the figure, transparent tunneling is active. The IPSec over UDP encapsulation is used with a port number of 10000.

# Hardware Client Connection Status

With a Hardware Client, the end user can view the session statistics by going to the Monitoring>System Status window. In the bottom part of the System Status window, you can view the tunnel type and the port number. In the example in the figure, the tunnel type is IPSec over UDP and the UDP port number is 10000. The UDP port number used is defined by the Concentrator and pushed down to the Hardware Client.

# Concentrator Monitor Session

Cisco.com

**Client**

**Internet**

**Concentrator**

| Hash | Data | | IP | ESP | TCP | IP |

**Session Summary**

| Active LAN-to-LAN Sessions | Active Remote Access Sessions | Active Management Sessions | Total Active Sessions | Peak Concurrent Sessions | Concurrent Sessions Limit | Total Cumulative Sessions |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 3 | 3 | 100 | 56 |

**LAN-to-LAN Sessions** [ Remote Access Sessions | Management Sessions ]

| Connection Name | IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx |
|---|---|---|---|---|---|---|---|
| pod1 | 192.168.6.5 | IPSec/LAN-to-LAN | 3DES-168 | Oct 14 9:26:53 | 29:34:48 | 15984 | 15864 |

**Remote Access Sessions** [ LAN-to-LAN Sessions | Management Sessions ]

| Username | Assigned IP Address Public IP Address | Group | Protocol Encryption | Login Time Duration | Client Type Version | Bytes Tx Bytes Rx |
|---|---|---|---|---|---|---|
| student1 | 10.0.1.75 172.26.26.1 | training | IPSec/TCP 3DES-168 | Oct 15 15:00:49 0:00:52 | WinNT 3.6.2 (Rel) | 0 472 |

**Management Sessions** [ LAN-to-LAN Sessions | Remote Access Sessions ]

| Administrator | IP Address | Protocol | Encryption | Login Time | Duration |
|---|---|---|---|---|---|
| admin | 10.0.1.10 | HTTP | None | Oct 15 13:33:03 | 0:28:36 |

CSVPN 4.0—14-26

The statistics can also be viewed at the Concentrator. To do this, select the **Monitoring Sessions** window. The encapsulation type is visible in the Protocol column within the Remote Access Sessions section. In the example in the figure, TCP over IPSec is used. Click the **student1** link in the Protocol column within the Remote Access Sessions section to get more information on the port number.

# Concentrator Monitor Session Detail

| Username | Public IP Address | Assigned IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx |
|---|---|---|---|---|---|---|---|---|
| student1 | 172.26.26.1 | 10.0.1.31 | IPSec/TCP | 3DES-168 | Jul 10 16:10:33 | 0:03:55 | 61520 | 29264 |

**Bandwidth Statistics**

| User Name | Interface | Traffic Rate (kbps) | | Traffic Volume (bytes) | |
|---|---|---|---|---|---|
| | | Conformed | Throttled | Conformed | Throttled |
| student1 (In) | Ethernet 2 (Public) | 0 | 0 | 36762 | 0 |
| student1 (Out) | Ethernet 2 (Public) | 2 | 0 | 69850 | 12226 |

IKE Sessions: 1
IPSec/TCP Sessions: 1

| IKE Session | | | |
|---|---|---|---|
| Session ID | 1 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Diffie-Hellman Group | Group 2 (1024-bit) |
| Authentication Mode | Pre-Shared Keys (XAUTH) | IKE Negotiation Mode | Aggressive |
| Rekey Time Interval | 86400 seconds | | |

| IPSec/TCP Session | | | |
|---|---|---|---|
| Session ID | 2 | Remote Address | 10.0.1.31 |
| Local Address | 0.0.0.0/255.255.255.255 | Encryption Algorithm | 3DES-168 |
| Hashing Algorithm | MD5 | Encapsulation Mode | Tunnel |
| TCP Source Port | 1160 | TCP Destination Port | 10000 |
| Rekey Time Interval | 28800 seconds | | |
| Bytes Received | 29264 | Bytes Transmitted | 62824 |

CSVPN 4.0—14-27

In the Monitoring>Sessions>Detail window, three sessions are listed: one IKE session and two IPSec sessions. Under the IPSec session, the encapsulation type and port numbers are available. In the example in the figure, the TCP encapsulation is used and the TCP destination port number assigned is port 10000.

# Summary

This topic summarizes the information that was presented in this lesson.

## Summary

Cisco.com

- **IPSec does not translate through a NAT or PAT device.**
- **Configure IPSec over UDP, NAT-T, or TCP in both the Concentrator and clients.**
- **For each tunnel type, an applicable port number is defined.**
- **IPSec over TCP, NAT-T, or UDP statistics are viewable on both the Concentrator and clients.**

CSVPN 4.0—14-29

**15**

# Configure the Cisco Virtual Private Network 3000 Series Concentrator for LAN-to-LAN with Pre-Shared Keys

## Overview

This lesson includes the following topics:

- Objectives

- Cisco VPN 3000 Series Concentrator IPSec LAN-to-LAN

- Configuring the Cisco VPN 3000 Series Concentrator via the Quick Configuration wizard

- LAN-to-LAN configuration

- Summary

- Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon the completion of this lesson, you will be able to perform the following tasks:**

- **Configure the Concentrator via Quick Configuration.**
- **Configure LAN-to-LAN tunnels.**
- **Monitor LAN-to-LAN tunnels.**
- **Configure network lists.**
- **Configure Network Autodiscovery.**

CSVPN 4.0—15-2

# Cisco VPN 3000 Series Concentrator IPSec LAN-to-LAN

This topic presents an overview of the Cisco Virtual Private Network (VPN) 3000 Series Concentrator LAN-to-LAN feature.
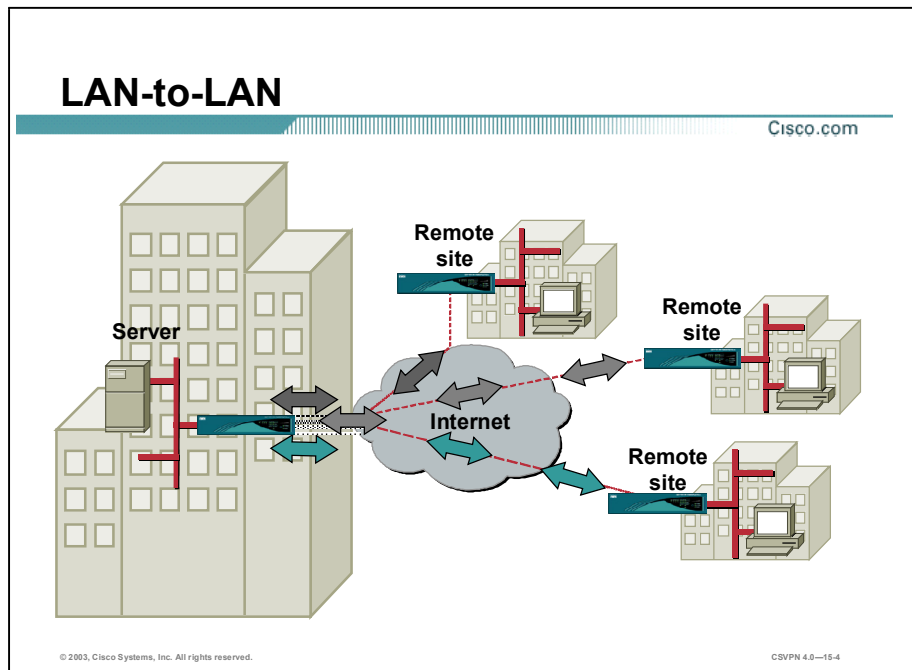


In the figure, a corporation wants to tie remote sites together via a VPN. At each remote site, there are 500 people. One option is to run a remote VPN where the VPN Client is installed on every PC. This is a logistical and administrative nightmare. The better option is to use the VPN capabilities of the Concentrator. One Concentrator is installed at each site, and all remote PC traffic is routed to the Concentrators. The Concentrators encrypt and encapsulate the traffic. The Concentrators perform all IPSec functionality, and route all interoffice VPN traffic through the Internet. This option requires that no additional software be installed on the PCs. This application is referred to as a LAN-to-LAN VPN.

**IPSec LAN-to-LAN**
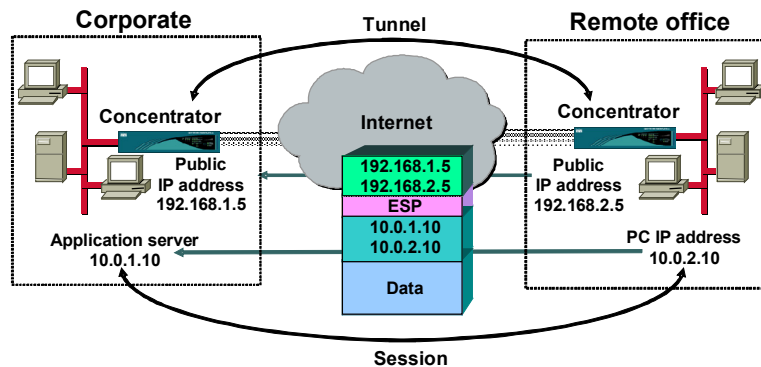
CSVPN 4.0—15-5

In the figure, the user on a remote LAN wants to access an application server at corporate headquarters. An IP packet is built with a source address of 10.0.2.3 and a destination address of 10.1.10. The packet is routed to the Concentrator. The Concentrator encrypts and encapsulates the IP packet with an Encapsulating Security Protocol (ESP) header. The packet is secure; however, the packet is non-routable due to the encrypted address. Therefore, an outside address header is added to the IP packet. The Concentrator uses the network interface card (NIC) addresses of the two Concentrators: 192.168.1.5 and 192.168.2.5. The outside address enables the IP packet to be routed through the Internet. An IPSec tunnel is established between the public interfaces of the Concentrators: 192.168.1.5 and 192.168.2.5. When the tunnel is up, a session is established between the two private networks: 10.0.1.0 and 10.0.2.0.

The Concentrator supports the following ESP options:

■ Authentication options

— None

— Hashed message algorithm code (HMAC)-Message Digest (MD5)—128-bit key

— HMAC-secure hash algorithm (SHA-1)—160-bit key

■ Data encryption options

— Data encryption standard (DES)—56-bit key

— Triple DES (3DES)—168-bit key

— AES—128-, 196-, and 256-bit key

# Concentrator—Physical Connections

Cisco.com

**Power**

**Private IP address
10.0.1.5**

**Public IP address
192.168.1.5**

**Internet**

**Console port**
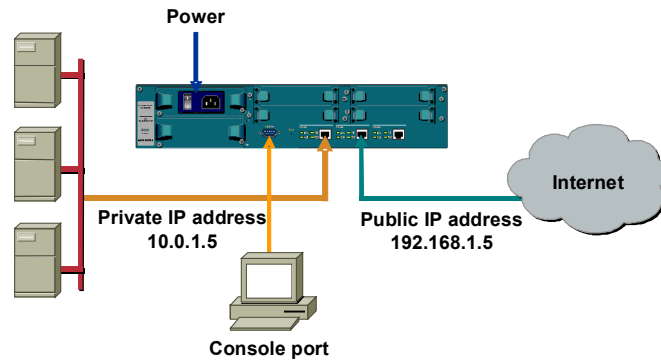
CSVPN 4.0—15-6

The Concentrator is equipped with universal power factor correction: 100–240 VAC. A power cable with the correct plug is supplied. When the Concentrator arrives from the factory, plug it in and power it up. Connect the corporate LAN to the Concentrator's private interface. Cable the Internet side of the corporate network to the public interface of the Concentrator. LAN ports can be programmed for 10M or 100M Ethernet.

The Concentrator is not pre-programmed with IP addresses at the factory. Use the console port to program the correct IP addresses for the VPN private IP address. The serial console port needs to be configured for 9600 bps 8N1. When programmed, the operator can access the Concentrator via the browser.

**Configuration Options**

Cisco.com
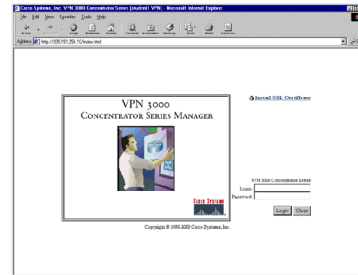
Welcome to
    Cisco Systems
    VPN 3000 Concentrator Series
    Command Line Interface
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information

VPN 3000
CONCENTRATOR SERIES MANAGER

CSVPN 4.0—15-7

After the initial private IP address configuration, the remaining parameters can be configured in one of two ways: using the command line interface (CLI) or via a browser. For beginners, the menu-driven browser is recommended. The CLI is geared for those individuals who understand the menu structure.

The web interface supports both HTTP and HTTP over Secure Sockets Layer (SSL). Operators can use either Internet Explorer or Netscape Navigator. With Internet Explorer and Netscape Navigator, the software versions must be 4.0 or higher with both cookies and Java scripts enabled. Use either browser to configure the Concentrator with one exception; Internet Explorer must be used when programming digital certificates.

GUI
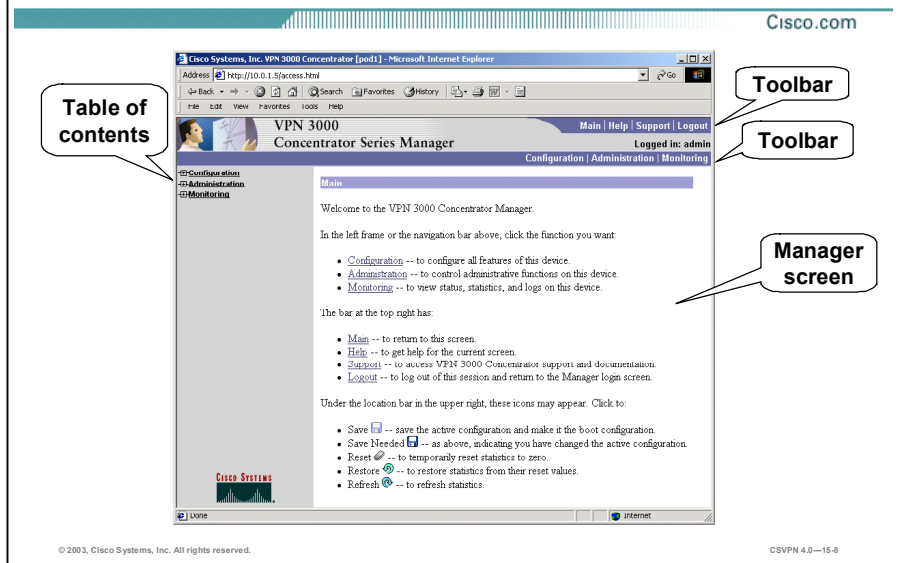
This is the main window of the Concentrator after logging into the device. In the left frame or the navigator bar in the figure above, you can click the function you want:

■ Configuration—To configure all features of this device.

■ Administration—To control administrative functions on this device.

■ Monitoring—To view status, statistics, and logs on this device.

The bar at the top right has the following options:

■ Main—Click to return to this window.

■ Help—Click to get help text for the current window.

■ Support—Click to access Concentrator support and documentation.

■ Logout—Click to log out of this session.

The following icons may be found under the location bar in the upper right part of the window:

■ Save—Save the active configuration.

■ Save Needed—Indicates you have changed the active configuration.

■ Refresh—Refresh the statistics.

| Note | When you finish with the configuration window, click **Apply**. Apply enables the configuration to take effect immediately. Click the **Save Needed** button to save the changes to memory. If you reboot without saving, your configuration changes are lost. |
|------|---|

# Quick Configuration

VPN 3000
Concentrator Series Manager

Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring

**Main**

**Welcome to the VPN 3000 Concentrator Series Manager**

The **VPN 3000 Concentrator Series** has booted, and you must now supply some configuration parameters to make it operational.

To configure the *minimal* parameters, click here to start Quick Configuration.

To configure *all* features, click here to go to the Main Menu.

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—15-9
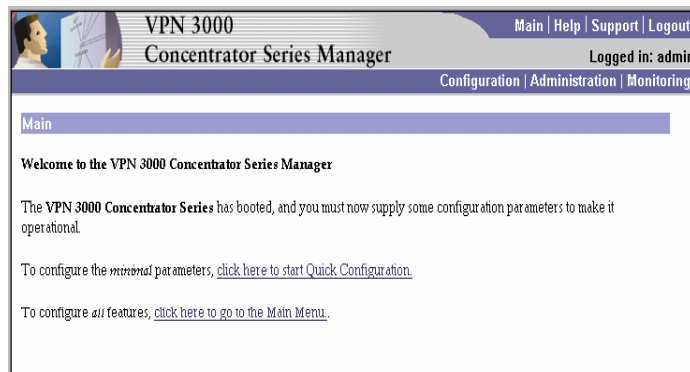
There are two ways to configure the Concentrator: Quick Configuration and the main menu. Quick Configuration enables you to configure the minimal parameters for operation. A wizard guides you through the configuration. The main menu is used to configure each feature individually. With Quick Configuration, the Concentrator can be programmed by accessing five windows. In the main menu, the same application requires the operator to access nine or more windows. The recommendation is to use Quick Configuration for the initial configuration. Use the main menu to add connections or tune existing configurations.

The next windows will take you through a LAN-to-LAN Quick Configuration sample.

---

**Note**    You can run Quick Configuration only once. You must reboot to the factory default
configuration to run it again.

---

# Configuring the Cisco VPN 3000 Series Concentrator via the Quick Configuration Wizard

This topic covers the configuration of Cisco VPN 3000 Series Concentrator via the Quick Configuration option.
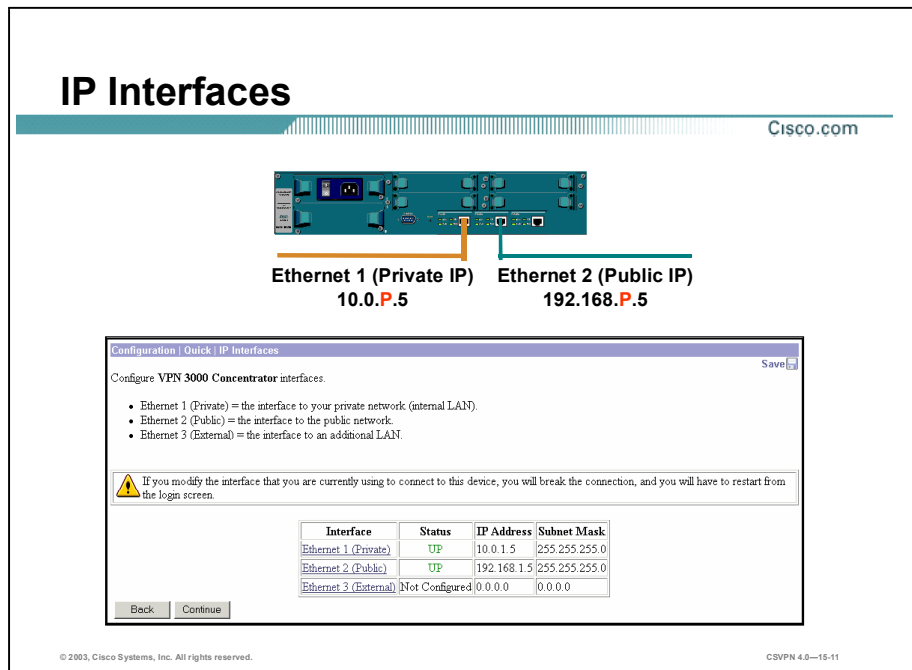


The figure shows is the first Quick Configuration window. It displays the current configuration of the IP interfaces:

■ Private—Interface toward the internal network

■ Public—Interface toward the public network (Internet)

■ External—Interface toward the external network or DMZ

If you remember, the private LAN interface was configured via the CLI. The next step is to configure the public LAN interface (toward the Internet).

Public IP Interface

Ethernet 1 (Private IP address)
10.0.P.5

Ethernet 2 (Public IP address)
192.168.1.5

The window displayed in the figure is used to configure the public interface. The public IP interface can be configured in one of three ways: disabled, set as a Dynamic Host Configuration Protocol (DHCP) client, or configured to use a static IP address. The public IP interface parameters are as follows:

■ Disable—The interface is enabled by default. Select the **Disable** check box to disable the interface.

■ DHCP Client—Select the **DHCP Client** radio button if you want to enable this interface and use DHCP to obtain an IP address. In the System Name field, enter a name (such as VPN01 for the Concentrator). This name must uniquely identify this device on your network.

■ Static IP Addressing—If you want to enable this interface and set a static IP address for it, click the **Static IP Addressing** radio button. In the IP Address field, enter the IP address for this interface using dotted decimal notation (for example, 192.168.1.5). Be sure no other device is using this address on the network. In the Subnet mask field enter the subnet mask for this interface using dotted decimal notation (for example, 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.1.5 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed.

■ Public Interface—Select the **Public Interface** check box to make this interface a public interface.

■ MAC Address—The Media Access Control (MAC) Address is the unique hardware MAC address for this interface.

- Filter—Click the Filter drop-down menu button and choose the public (default) filter, which allows only nonsource-routed inbound and outbound tunneling protocols plus Internet Control Message Protocol (ICMP). This is the default filter for Ethernet 2.

- Speed—Keep the default value.

## System Information



The Configuration>Quick>System Info window configures basic information about the Concentrator, and has the following options:

■ System Name field—Enter a name (such as VPN01) for the Concentrator. This name must uniquely identify this device.

■ New Time fields and drop-down menus—Set the time and date on the Concentrator. The correct time is very important so that logging, certificates, and accounting entries are accurate. The window shows the current date and time on the device. The values shown in the New Time fields are the time on the browser PC, but any entries you make apply to the Concentrator.

■ DNS Server field—Enter the IP address of your local DNS (Domain Name System) server, using dotted decimal notation (for example, 192.34.5.67).

■ Domain field—Enter your Internet domain name.

■ Default Gateway field—Enter the IP address or hostname of the system to which the Concentrator should route packets that are not explicitly routed. In other words, if the Concentrator has no IP routing parameters (Routing Information Protocol [RIP], Open Shortest Path First [OSPF], static routes) that specify where to send a packet, it will be sent to this gateway.

## Protocols



The Configuration>Quick>Protocols window defines the protocols used in Client-to-LAN applications. The parameters have no bearing on LAN-to-LAN applications. Look at the text next to the IPSec parameter and notice that LAN-to-LAN configuration is done outside of the Quick Configuration. The LAN-to-LAN IPSec protocol information is configured in a different window. While the Concentrator is able to handle remote access and LAN-to-LAN tunnels simultaneously, in this topic during the lab exercise, you will deselect all the remote access protocols and focus strictly on LAN-to-LAN configuration and monitoring.

**Admin Password**

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.                                                    CSVPN 4.0—15-15
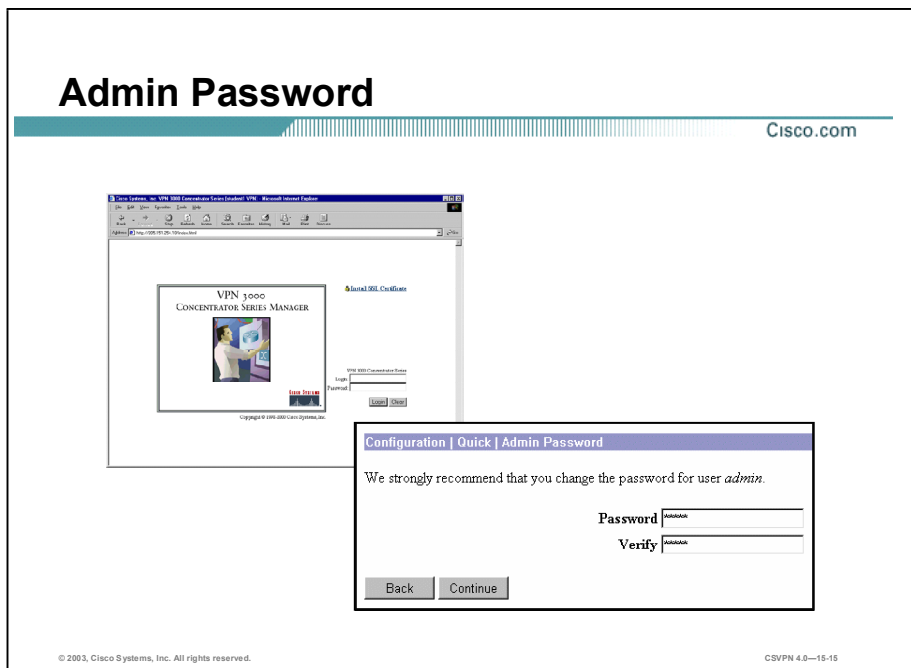
You can use the Configuration>Quick>Password window to change the password. It is highly recommended for security. Use the following options to change the password:

■ Login field—Enter or edit the unique username for this administrator.

■ Password field—Enter or edit the unique password for this administrator. The field displays only asterisks. The default password that Cisco supplies is the same as the username. It is strongly recommended that you change this password.

■ Verify field—Re-enter the password to verify it. The field displays only asterisks.

■ Reset Password utility—After you reboot the system and the diagnostic check is complete, a line of three dots ( . . . ) appears on the console. Pressing **Control-Break** within three seconds after seeing the three dots displays a new menu that enables you to reset the system password back to its default.

# LAN-to-LAN Configuration

This topic presents an overview of the Concentrator LAN-to-LAN wizard.



Configuration of LAN-to-LAN connections cannot be done in Quick Configuration. Instead, the Concentrator provides a wizard for LAN-to-LAN connections. Choose **Configuration>System>Tunneling Protocols>IPSec>LAN-to-LAN**, and click **Add** to access the LAN-to-LAN wizard. The Configuration>System>Tunneling Protocols>IPSec LAN-to-LAN>Add window opens. The LAN-to-LAN wizard presents this one window to configure a LAN-to-LAN tunnel.

**Boston IPSec LAN-to-LAN**
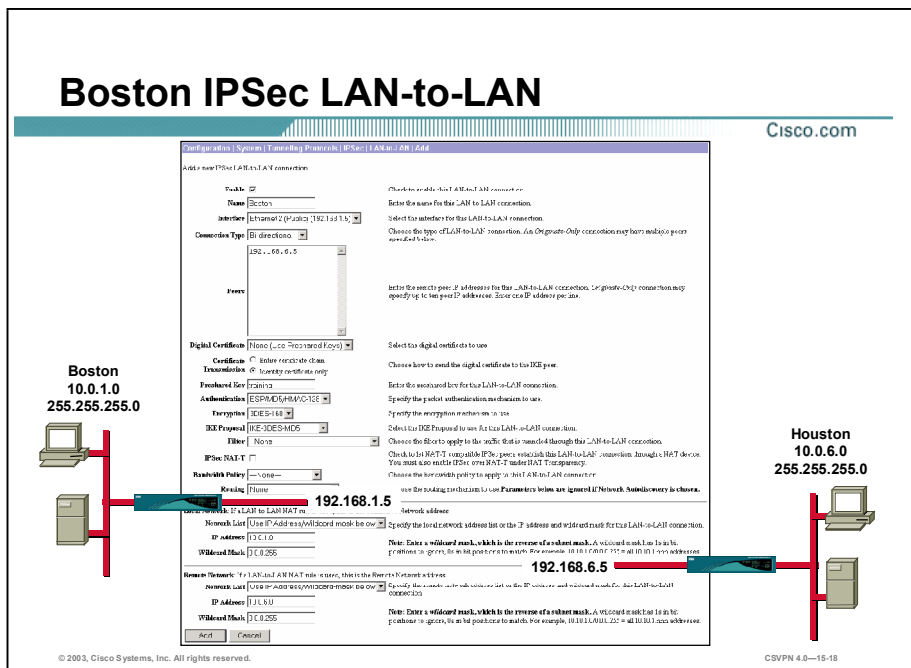
The Configuration>System>Tunneling Protocols>IPSec>LAN-to-LAN>Add window has three sections. The top section pertains to the network information; the bottom two sections deal with the two private networks at either end of the tunnel.

In the example in the figure, there is a tunnel between Boston and Houston. The administrator is currently configuring the Boston Concentrator. For the Boston network connection, the administrator needs to complete the following steps:

**Step 1** Enter the name for the LAN-to-LAN connection (local significance only) in the Name field.

**Step 2** Set the peer value as the IP address assigned to the public interface of the remote Concentrator (for example, 192.168.6.5) in the Peer field.

**Step 3** Enter an alphanumeric string value for the pre-shared key in the Preshared Key field.

There are two private networks: local and remote. The middle section of the Configuration> System>Tunneling Protocols>IPSec LAN-to-LAN window defines the local private network. When the administrator in the example programs the Boston end, the local network to Boston is 10.0.1.0. When programming the local private network, the administrator needs to complete the following steps:

**Step 1** Set the local network IP address to 10.0.1.0, which is the network and subnet address minus the host address.

**Step 2** Set the wildcard mask, 0.0.0.255. The wildcard mask is the reverse of the subnet mask.

The bottom section of the Configuration>System>Tunneling Protocols>IPSec>LAN-to-LAN>Add window defines the remote private network. In the example, the remote end is referring to the Houston private network, 10.0.6.0. When the administrator in the example programs the remote private network, the administrator needs to complete the following steps:

**Step 1** Set the remote network IP address to 10.0.6.0. It is the network and subnet address minus the host address.

**Step 2** Set the wildcard mask to 0.0.0.255. The wildcard mask is the reverse of the subnet mask.

**Step 3** Click **Add**.

## Backup LAN-to-LANs

A backup LAN-to-LAN configuration has two sides: a central side and a remote side. The central side is the endpoint of the connection where the backup VPN Concentrators reside. (If the backup VPN Concentrators reside in different geographic places, there may be more than one central side.) The endpoint of the backup VPN Concentrator's LAN-to-LAN peer is the remote side.

The remote-side VPN Concentrator has a peer list of all (up to ten) of the central-side VPN Concentrators. The peers appear on the list in their order of priority. Each central-side VPN Concentrator has a peer list of the (one) remote-side peer.

In a backup LAN-to-LAN setup, the remote peer always initiates the connection. It tries to connect to the first VPN Concentrator on its peer list. If that VPN Concentrator is unavailable, then it tries to connect to the second peer on the list. It continues in this way until it connects to one of the peers on the list. If that connection later fails, the remote-side peer again tries to connect to the first peer on its list. If that VPN Concentrator is unavailable, it tries the second, and so on. In this way, the remote VPN Concentrator re-establishes the LAN-to-LAN connection with only a brief interruption of service.

In a nonredundant LAN-to-LAN connection, the first data to travel from one peer to another brings up the Internet Key Exchange (IKE) tunnel. The tunnel exists for the duration of the data transmission only. When the data stops transmitting, the tunnel goes down. In a backup LAN-to-LAN configuration, the peers establish the tunnel in a different manner. During IKE tunnel establishment, the VPN Concentrator at each endpoint of the LAN has a unique role. It can either originate or accept IKE tunnels. In most cases, you configure the remote-side VPN Concentrator to originate the tunnel and the central-side VPN Concentrator to accept it. Once the IPSec tunnel is established, data travels in both directions; each side can both receive and send data. The tunnel remains up at all times, even if data transmission stops.

The unique role of the VPN Concentrator in establishing the IKE tunnel is called its connection type. There are three connection types:

■ Originate only—This VPN Concentrator originates the IKE tunnel. An originate-only endpoint is analogous to a telephone that makes only outgoing phone calls; it cannot receive calls.

■ Answer only—This VPN Concentrator accepts the IKE tunnel. An answer-only connection is analogous to a telephone that receives only incoming calls; it cannot make calls.

■ Bidirectional—This VPN Concentrator can either originate or accept the IKE tunnel. It is like a telephone that can both make calls and receive calls.

Configure the remote-side VPN Concentrator with the connection type Originate-Only; configure the central-side VPN Concentrator with the connection type Answer-Only. (A few other configurations are valid, although not recommended.)

**IPSec LAN-to-LAN Is Finished**

Boston
10.0.1.0
255.255.255.0

IPSec

Internet

Houston
10.0.6.0
255.255.255.0

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done

Save Needed

An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

Authentication Server  Internal
Group  192.168.6.5
Security Association  L2L: boston
Filter Rules  L2L: boston Out
L2L: boston In

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer.
The **Security Association** and **Filter Rules** all start with "**L2L:**" to indicate that they form a LAN-to-LAN configuration.

OK

CSVPN 4.0—15-19

If the connection was successfully configured, the IPSec LAN-to-LAN>Add>Done window opens. In this window, the Cisco VPN 3000 manager presents a synopsis of LAN-to-LAN tunnel configuration information. The LAN-to-LAN wizard automatically configures the following tables:

■ Group Name

■ Security Association (SA) Name

■ Filter Name

You can view or edit any parameters in these tables.

# IPSec LAN-to-LAN Connection

Cisco.com

IPSec

Boston
10.0.1.0
255.255.255.0

192.168.1.5

Internet

192.168.6.5

Houston
10.0.6.0
255.255.255.0

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN

Save Needed

This section lets you configure IPSec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPSec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to User Management and configure a Group and User. To configure NAT over LAN-to-LAN, go to LAN-to-LAN NAT Rules.

If you want to define a set of networks on the local or remote side of the LAN-to-LAN connection, configure the necessary Network Lists prior to creating the connection.

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

(D) indicates a disabled LAN-to-LAN connection.

LAN-to-LAN
Connection

Actions

Boston (192.168.6.5) on Ethernet 2 (Public)

Add
Modify
Delete

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—15-20

The Configuration>System>Tunneling Protocols>IPSec>LAN-to-LAN window lists all the LAN-to-LAN tunnels configured in the Concentrator. The example in this figure gives the listing "boston (192.168.6.5)". This means that the tunnel name is Boston and that the public interface of the remote Concentrator is 192.168.6.5.

## Houston IPSec LAN-to-LAN

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable ☑ — Check to enable this LAN-to-LAN connection.
Name: Houston — Enter the name for this LAN-to-LAN connection.
Interface: Ethernet 2 (Public) (192.168.1.5) — Select the interface for this LAN-to-LAN connection.
Connection Type: Bi-directional — Choose the type of LAN-to-LAN connection. An *Originate-Only* connection may have multiple peers specified below.

Peers: 192.168.1.5 — Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* connection may specify up to ten peer IP addresses. Enter one IP address per line.

Digital Certificate: None (Use Preshared Keys) — Select the digital certificate to use.
Certificate Transmission: ○ Entire certificate chain  ● Identity certificate only — Choose how to send the digital certificate to the IKE peer.
Preshared Key: training — Enter the preshared key for this LAN-to-LAN connection.
Authentication: ESP/MD5/HMAC-128 — Specify the packet authentication mechanism to use.
Encryption: 3DES-168 — Specify the encryption mechanism to use.
IKE Proposal: IKE-3DES-MD5 — Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter: --None-- — Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T ☐ — Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy: --None-- — Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing: None — Choose the routing mechanism to use. **Parameters below are ignored if Network Autodiscovery is chosen.**

**Local Network:** If a LAN-to-LAN NAT rule is used, this is the Translated Network address.
Network List: Use IP Address/Wildcard-mask below — Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address: 10.0.6.0
Wildcard Mask: 0.0.0.255 — **Note:** Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

**Remote Network:** If a LAN-to-LAN N... ...te Network address.
Network List: Use IP Address/Wildcard-mask below — Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address: 10.0.1.0
Wildcard Mask: 0.0.0.255 — **Note:** Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Add    Cancel

Boston
10.0.1.0
255.255.255.0

Houston
10.0.6.0
255.255.255.0

192.168.6.5

192.168.1.5

CSVPN 4.0—15-21

With LAN-to-LAN, there are two ends to the tunnel. After an administrator has configured the first end (in this example, it is "Boston"), the administrator must configure the other end (in this example, it is "Houston"). Choose **Configuration>System>Tunneling Protocols>IPSec> LAN-to-LAN** and click **Add** to access the LAN-to-LAN wizard.

There are three sections to the Configuration>System>Tunneling Protocols>IPSec>LAN-to-LAN window: the top section defines the network parameters, the middle section defines the local private network, and the bottom section defines the remote private network.

For the Houston network connection (top section) in the example, the administrator must complete the following steps:

**Step 1**  Enter the name for the LAN-to-LAN connection (local significance only) in the Name field.

**Step 2**  Set the peer value as the IP address assigned to the public interface of the remote Concentrator (for example, 192.168.1.5) in the Peer field.

**Step 3**  Enter an alphanumeric string value for the pre-shared key in the Pre-shared Key field.

In the example, there are two private networks: local and remote. When programming the Houston end (middle section), the local network to Houston is 10.0.2.0. When programming the local network, the administrator must complete the following steps:

**Step 1**  Set the local network IP address to 10.0.6.0, which is the network and subnet address minus the host address.

**Step 2**  Set the wildcard mask, 0.0.0.255. The wildcard mask is the reverse of the subnet mask.

In the example, the remote end is referring to the Boston private network (bottom section), 10.0.1.0. When programming the remote end, the administrator must complete the following steps:

**Step 1** Set the remote network IP address to 10.0.1.0. It is the network and subnet address minus the host address.

**Step 2** Set the wildcard mask to 0.0.0.255. The wildcard mask is the reverse of the subnet mask.

**Step 3** Click **Add**.

**IPSec LAN-to-LAN Is Finished**

Cisco.com

**IPSec**

Boston
10.0.1.0
255.255.255.0

Internet

Houston
10.0.6.0
255.255.255.0

192.168.1.5          192.168.6.5

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done

Save Needed

An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

**Authentication Server** Internal
**Group** 192.168.1.5
**Security Association** L2L: houston
**Filter Rules** L2L: houston Out
L2L: houston In

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer. The **Security Association** and **Filter Rules** all start with "**L2L:**" to indicate that they form a LAN-to-LAN configuration.

OK

© 2003, Cisco Systems, Inc. All rights reserved.                                                        CSVPN 4.0—15-22

If the connection was successfully configured, the IPSec LAN-to-LAN>Add>Done window opens. In this window, the Cisco VPN 3000 manager presents a synopsis of LAN-to-LAN tunnel configuration information. The LAN-to-LAN wizard automatically configures the following tables:

■    Group name

■    SA name

■    Filter name

You can view or edit any parameters in these tables.

**Administration Sessions**

Cisco.com

| Administration | Administer Sessions | | | | | | | | Thursday, 15 August 2002 15:24:05 |

Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name. To log out a session, click **Logout** in the table below. To test the network connection to a session, click **Ping**.

Group --All--

Logout All: PPTP User | L2TP User | IPSec User | IPSec LAN-to-LAN

**Session Summary**

| Active LAN-to-LAN Sessions | Active Remote Access Sessions | Active Management Sessions | Total Active Sessions | Peak Concurrent Sessions | Concurrent Sessions Limit | Total Cumulative Sessions |
|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 2 | 2 | 100 | 94 |

**LAN-to-LAN Sessions**  [ Remote Access Sessions | Management Sessions ]

| Connection Name | IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx | Actions |
|---|---|---|---|---|---|---|---|---|
| Boston | 192.168.6.5 | IPSec/LAN-to-LAN | 3DES-168 | Aug 15 6:41:45 | 7:42:24 | 51800 | 51744 | [ Logout | Ping ] |

**Remote Access Sessions**  [ LAN-to-LAN Sessions | Management Sessions ]

| Username | Assigned IP Address Public IP Address | Group | Protocol Encryption | Login Time Duration | Client Type Version | Bytes Tx Bytes Rx | Actions |
|---|---|---|---|---|---|---|---|
| | | | No Remote Access Sessions | | | | |

**Management Sessions**  [ LAN-to-LAN Sessions | Remote Access Sessions ]

| Administrator | IP Address | Protocol | Encryption | Login Time | Duration | Actions |
|---|---|---|---|---|---|---|
| admin | 10.0.1.10 | HTTP | None | Aug 15 15:24:04 | 0:00:04 | [ Logout | Ping ] |

CSVPN 4.0—15-23

Choose the **Administration>Sessions** window to verify the LAN-to-LAN tunnel. If the LAN-to-LAN tunnel is not listed, ping the private interface at the remote end (the Concentrator needs to see interesting traffic bound for the remote network before it will bring up a tunnel). LAN-to-LAN Sessions provides the following information:

- Connection name

- IP address (the public IP address of the remote Concentrator)

- Protocol

- Encryption

- Login time

- Duration

- Bytes Tx and Rx

**Multiple Subnets**

Cisco.com

Seattle

Router

Internet

Boston

Router

Router

Router

Houston

San Francisco
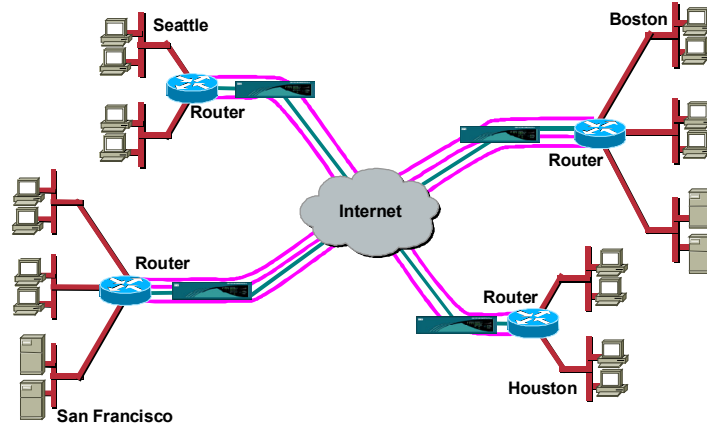
CSVPN 4.0—15-24

In the previous examples, there was one tunnel with one subnet at each end of the tunnel. This is not a real world example. In the real world, there are multiple tunnels with multiple subnets at each remote site.

Before Release 2.1 of the Concentrator, you had to define tunnels and all reachable subnets. You had to define each subnet-to-subnet connection individually. In a mesh network, that could be very time-consuming and error prone.

In Release 2.1, you can build a network list. In the network list you define all the subnets reachable at a particular site and give them a name (for example, Boston or Houston). Instead of defining individual subnet-to-subnet tunnels, you can define one tunnel between each site and apply a network list to the private network at each site. In LAN-to-LAN configuration, the Concentrator can reference the applicable network lists for subnet information.

Also in Release 2.1, Network Autodiscovery (NAD) is introduced. With NAD, you do not have to define local and remote network addresses, or network lists. You define the LAN-to-LAN network information only: name, peer, remote address, pre-shared key, and routing (NAD). As long as Inbound RIP is turned on, the Concentrator learns subnets from RIP. Each Concentrator then encrypts the RIP information and sends it through the tunnel to the remote Concentrator. (NAD is not supported with OSPF.)

**Network Lists**

Cisco.com

Configuration | Policy Management | Traffic Management | Network Lists

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List    Actions
— Empty —       Add
                Modify
                Copy
                Delete

...st. Click on **Generate Local List** to generate a network list based on routing entries

List Name [boston]

Network List
10.0.1.0/0.0.0.255

Name of the Network List you are adding. The name must be unique.
• Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
• **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
• Each Network and Wildcard mask pair must be entered on a single line.
• The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Add    Cancel    Generate Local List

CSVPN 4.0—15-25

Instead of defining individual subnet-to-subnet tunnels, you can define one tunnel between each site, define network lists for both ends, and apply a network list to each end. In the network list, you define all the subnets reachable at a particular site and give them a name (for example, Boston or Houston). The local network list is built automatically via RIP. For the remote list, all reachable private subnets are configured manually.

Generate a list for both ends of the tunnel to use network lists:

■ For the local list, click **Generate Local List**. The Concentrator generates networks from the routing table. The Concentrator uses inbound RIP, not OSPF. If necessary, edit the list. (For example, if you had a subnet that you did not want to be accessible through the tunnel, delete the networks that need to remain private). The Manager automatically generates a network list containing the first 200 private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table, and the inbound RIP must be enabled on that interface. The Manager refreshes the screen after it generates the list, and you can then edit the Network List and enter a List Name. If you click **Apply**, the generated list replaces any existing entries in the Network List. The last step is to name the list and click **Add**.

■ For the remote list in the network list window, enter the subnet/wildcard for each reachable subnet. The subnet does not include the host, and the wildcard is the reverse of the subnet mask (subnet =255.255.255.0, wildcard = 0.0.0.255).

## LAN-to-LAN Network Lists
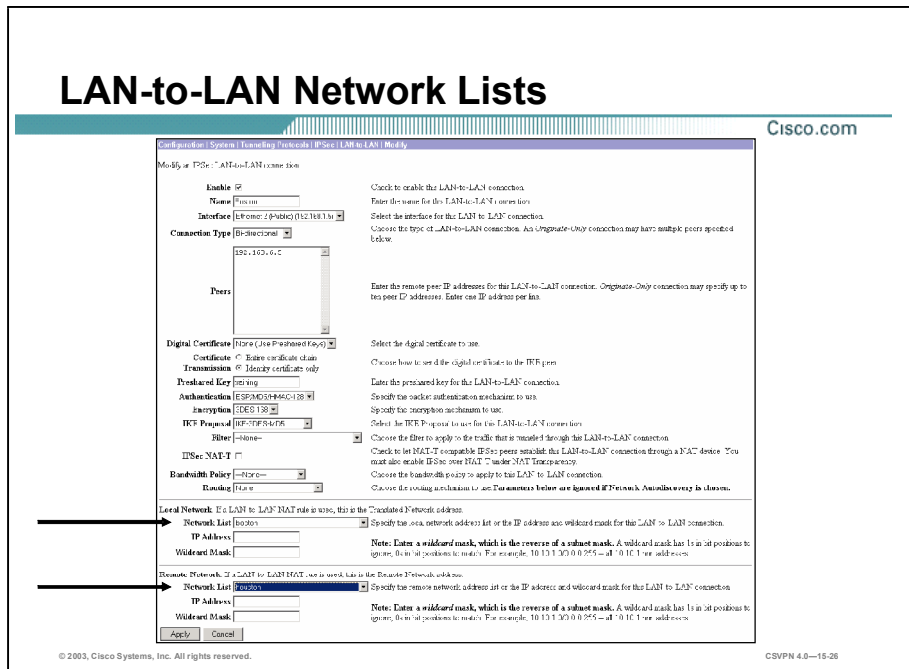
Separate network lists are built for both ends of the tunnel. The lists are then added to the LAN-to-LAN tunnel configuration as follows:

■ For local network—Under the network list drop-down menu, select the correct network list for the local end of the network.

■ For remote network—Under the network list drop-down menu, select the correct network list for the remote end of the network.

The Concentrator will build the tunnel and use the network list to determine how to route the traffic.

# LAN-to-LAN Network Autodiscovery

Cisco.com
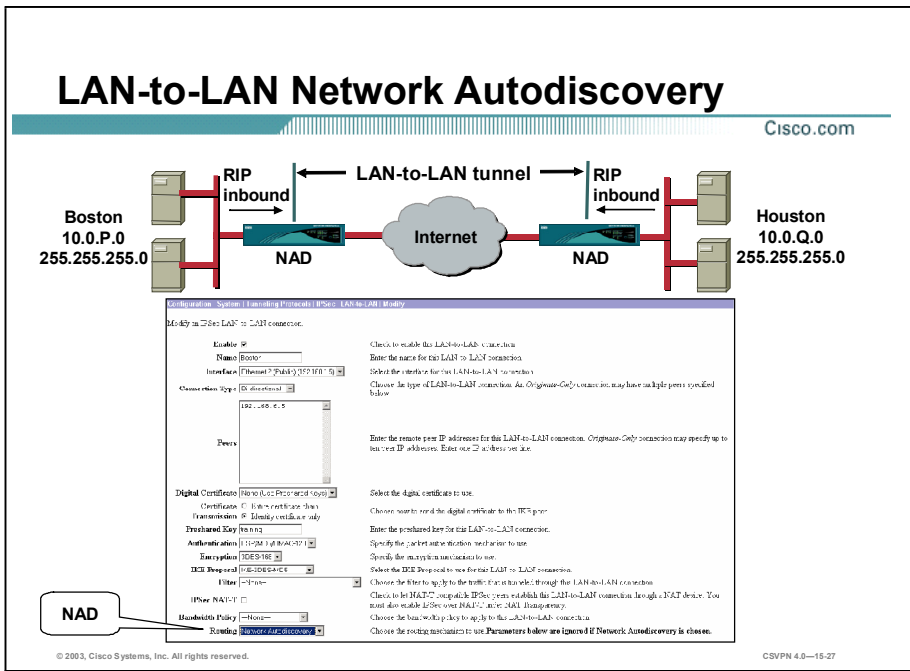
The NAD feature dynamically discovers and continuously updates the private network addresses on each side of the LAN-to-LAN connection. You do not have to define the private networks at both ends of the tunnel. The Concentrator learns local network addresses from local RIP updates. The Concentrators encrypt this information and send it through the tunnel to the remote end. From this information, the remote Concentrator learns what networks are reachable at the other end of the tunnel. For this feature to work, inbound RIP must be enabled on the private interface of both Concentrators.

Complete the following steps to configure LAN-to-LAN using NAD:

**Step 1**   Enter a name in the Name field.

**Step 2**   Choose the remote address of the peer's public interface from the Interface drop-down menu.

**Step 3**   Define the pre-shared key or certificate in the Preshared Key field.

**Step 4**   Choose **Network Autodiscovery** from the Routing drop-down menu.

**Step 5**   Click **Add**.

The Concentrator can build a LAN-to-LAN tunnel from this information.

---

**Note**      The OSPF NAD is not supported.

---

# Summary

This topic summarizes what you learned in this lesson.

## Summary

Cisco.com

- **Interface and system information is configured via Quick Configuration.**
- **LAN-to-LAN is configured via a second wizard.**
- **Network lists enable ease of configuration when dealing with multiple subnets.**
- **Network autodiscovery learns the local subnets by listening to RIP updates.**

© 2003, Cisco Systems, Inc. All rights reserved.    CSVPN 4.0—15-29

# Lab Exercise—Configure the Cisco VPN 3000 Series Concentrators for LAN-to-LAN Using Pre-Shared Keys

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to configure one end of a LAN-to-LAN Virtual Private Network (VPN) while another team completes the same tasks at a remote site. Work with your lab exercise partner to complete the following tasks on your side of the LAN-to-LAN VPN:

- Complete the lab exercise setup.

- Return the Cisco VPN 3000 Series Concentrator to factory settings.

- Configure the Cisco VPN 3000 Series Concentrator private interface using the CLI.

- Configure a static route in the Cisco VPN 3000 Series Concentrator using the CLI.

- Configure the Cisco VPN 3000 Series Concentrator using the Cisco VPN 3000 Concentrator Series Manager.

- Configure network lists.

- Configure the Cisco VPN 3000 Series Concentrator LAN-to-LAN parameters.

- Verify the Cisco VPN 3000 Series Concentrator LAN-to-LAN connectivity.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
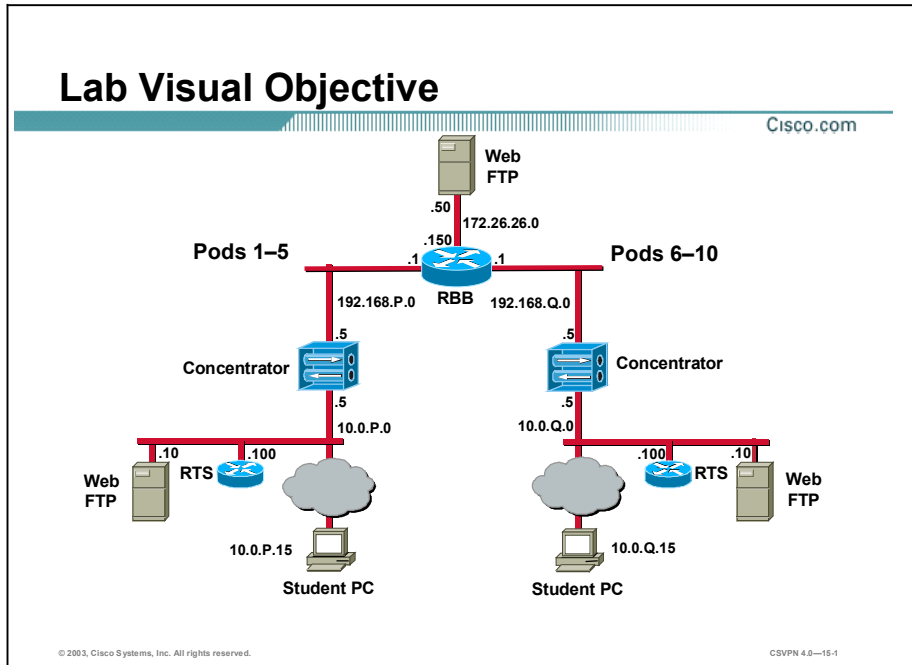


## Scenario

Your company wants you to implement a VPN between the world headquarters campus site and the remote sales offices. You must configure the Cisco VPN 3000 Series Concentrators for LAN-to-LAN tunneling using pre-shared keys for authentication.

## Task 1—Complete the Lab Exercise Setup

Certain networking parameters must be configured before your student PC can operate in the lab environment. Reconfigure your student PC networking parameters using the following IP addresses:

■ Ensure that your student PC is powered on.

■ Ensure that your student IP addresses are configured correctly:

— Primary IP address—10.0.P.15
(where P = pod number)

— Subnet mask—255.255.255.0

- Default gateway IP address—10.0.P.5
  (where P = pod number)

■ Ensure that your Concentrator is powered on.

## Task 2—Return the Cisco VPN 3000 Series Concentrator to Factory Settings

The instructor will provide you with the procedures for access to the Concentrator console port, as this will vary according to your connectivity. After you access the Concentrator console port, the Concentrator prompt will appear. Complete the following steps to return the Concentrator to the factory settings:

**Step 1**  Log into the Concentrator command line interface (CLI) using the administrator account:

```
Login: admin
Password: admin
```

If you get a Quick prompt for the system time or date parameters, the device has already been rebooted to factory defaults. Skip the remainder of this task and proceed to Task 4. If you do not get a Quick prompt for the system time or date parameters, the device has not already been rebooted to factory defaults, and you must continue with the rest of the steps in this task.

**Step 2**  Access the Administration menu:

```
Main -- 2
```

**Step 3**  Access the System Reboot menu:

```
Admin -- 3
```

**Step 4**  Access the Schedule Reboot menu:

```
Admin -- 2
```

**Step 5**  Select Reboot ignoring the Configuration file:

```
Admin -- 3
```

**Step 6**  Select Reboot Now:

```
Admin -- 2
```

The "Reboot scheduled immediately" message appears followed by the "Rebooting VPN 3000 Concentrator Series now" message. Do not attempt to log in to the first login prompt you see, as it takes several moments for the Concentrator to complete the reboot function. A login prompt appears when the reboot is completed.

**Step 7**  Leave the CLI session open.

## Task 3—Configure the Cisco VPN 3000 Series Concentrator Private Interface Using the CLI

Complete the following steps to configure the Concentrator private LAN interface using the CLI quick configuration mode:

| Note | This procedure assumes that the CLI session is still active. If not, follow steps 1–6 of the previous task before proceeding. |
| --- | --- |

**Step 1** Log in to the Concentrator using the administrator account:

```
Login: admin
Password: admin
```

When administrator reboots a Concentrator, as in the previous task, the CLI menus open in a slightly different order. If you get the Quick prompt for the system parameters, press **Enter** through the time, date, time zone, and DST prompts.

**Step 2** Enter your Concentrator private interface IP address:

```
Quick Ethernet 1-- [0.0.0.0] 10.0.P.5
```

(where P = pod number)

**Step 3** Enter your Concentrator private interface subnet mask:

```
Quick Ethernet 1-- [255.0.0.0] 255.255.255.0
```

**Step 4** Accept the default Ethernet speed of 10/100 Mbps Auto Detect:

```
Quick Ethernet 1-- [3] <Enter>
```

**Step 5** Accept the default duplex mode of Half/Full/Auto:

```
Quick Ethernet 1-- [1] <Enter>
```

**Step 6** Accept MTU default:

```
Quick Ethernet 1-- [1500] <Enter>
```

**Step 7** Save changes to the configuration file:

```
Quick -- 3
```

**Step 8** Exit the CLI:

```
Quick -- 5
```

If you do not exit, the CLI continues its quick configuration script. You will use the standard CLI menus for the remaining parameters.

## Task 4—Configure the Cisco VPN 3000 Series Concentrator Using the Cisco VPN 3000 Concentrator Series Manager

Complete the following steps to finish the configuration using the Cisco VPN 3000 Concentrator Series Manager:

| Note | This procedure assumes that Windows 2000 is already running on the student PC. |
| --- | --- |

**Step 1**  Launch Internet Explorer by double-clicking the desktop icon.

**Step 2**  Enter a Concentrator private interface IP address of **10.0.P.5** in the Internet Explorer Address field (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 3**  Log into the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

The username (login) and password are always case sensitive.

**Step 4**  In the main window, click the **click here to start Quick Configuration** hyperlink.

**Step 5**  Complete the following sub-steps from the Configuration>Quick>IP Interfaces window:

1.  Select **Ethernet 2 (Public)**. The Ethernet 2 window opens.

2.  Select **Static IP Addressing**.

3.  In the IP Address field, enter an IP address of **192.168.P.5**.
    (where P = pod number)

The subnet mask field is automatically populated with a value of 255.255.255.0.

4.  Leave all other fields at their default.

5.  Click **Apply**.

6.  Click **Continue**.

**Step 6**  Complete the following sub-steps from the Configuration>Quick>System Info window:

1.  Enter **vpnP** in the System Name field.
    (where P = pod number)

2.  Leave the DNS server set to 0.0.0.0.

3.  Enter the domain name: **cisco.com**.

4.  Enter a backbone router IP address of **192.168.P.1** in the Default Gateway field.
    (where P = pod number)

5.  Click **Continue**.

**Step 7**  Complete the following sub-steps from the Configuration>Quick>Protocols window:

1.  Deselect the **PPTP** check box.

2.  Deselect the **L2TP** check box.

3.  Select the **IPSec** check box.

4.  Click **Continue**.

**Step 8** Click **Continue** until Quick Configuration is complete.

**Step 9** Save the changes.

**Step 10** Do not close Internet Explorer. Proceed to the next topic.

## Task 5—Configure Network Lists

Configure Concentrator Network Lists. In most networks there are multiple subnets at both ends of the VPN tunnel. A network list must be configured at both ends of the tunnel to talk between subnets through the VPN tunnel. Complete the following steps to define which local and remote network IP addresses are available at each end of the tunnel:

**Step 1** Build a local network list by completing the following sub-steps:

1. From the Configuration menu tree, drill down to Policy Management>Traffic Management> Network Lists.

2. Click **Add**.

3. Click **Generate Local List** and answer the following question:

   Q1) What IP addresses appear in the Network List field?

   A) _____

4. Enter a unique name in the List Name field (for example, podP).
   (where P = pod number).

5. Click **Add**.

**Step 2** Build a remote network list by completing the following sub-steps:

1. From the Configuration menu tree, drill down to Policy Management>Traffic Management> Network Lists window, click **Add**.

2. Enter a meaningful remote city name or building name in the List Name field (for example, podQ).
   (where Q = peer pod number)

3. Enter the following IP address and wildcard mask for the remote private network:
   **10.0.Q.0/0.0.0.255**.
   (where Q = peer pod number)

4. Click **Add**.

**Step 3** Save the configuration changes.

## Task 6—Configure the Cisco VPN 3000 Series Concentrator LAN-to-LAN Parameters

In this topic you will configure the LAN-to-LAN parameters of the Concentrator using the LAN-to-LAN wizard. Complete the following steps to configure Concentrator LAN-to-LAN parameters:

**Step 1** From the Configuration menu tree, drill down to System>Tunneling Protocols> IPSec>IPSec LAN-to-LAN.

**Step 2** Click **Add**.

The IPSec LAN-to-LAN window is composed of three sections. The top section prompts you for information about the public network. The peer refers to the public interface address of a remote Concentrator (the address of the other end of the tunnel). In the middle and bottom sections of the window, you configure the addresses of the private networks at both ends of the tunnel. The local network is your private network (the host address is 0). The remote network is the private network of the remote peer (the host address is 0).

**Step 3** Complete the following sub-steps to configure the IPSec LAN-to-LAN connection:

1. Enter a name: **podP**.
   (where P = pod number)

2. Enter a peer Concentrator public interface IP address of **192.168.Q.5** (where Q = peer pod number). This is the IP address of the remote Concentrator public interface.

3. Enter a pre-shared key: **training**.

4. Leave all other fields at their defaults and go to the local network section of the window.

**Step 4** Apply the local network list previously configured in this lab. In the Local Network section of the window, choose the correct local network list from the Network List drop-down menu (for example, podP).

**Step 5** Apply the remote network list previously configured in this lab. In the Remote Network section of the window, choose the correct remote network list from the Network List drop-down menu (for example, podQ).

**Step 6** Click **Add**.

**Step 7** Click **OK**.

**Step 8** Save the configuration changes. You have successfully configured an IPSec LAN-to-LAN tunnel using the IPSec LAN-to-LAN configuration wizard. Wait for the team at the peer pod to finish before proceeding. Do not log out of the Concentrator.

## Task 7—Verify the Cisco VPN 3000 Series Concentrator LAN-to-LAN Connectivity

Complete the following steps to verify the LAN-to-LAN tunnel connections:

**Step 1** Ping your peer Concentrator private interface at **10.0.Q.5** (where Q = peer pod number) using the Administration menu tree ping function. If the LAN-to-LAN wizard was configured correctly, the Cisco VPN 3005 Concentrator will build an IPSec tunnel based on the student supplied network information and the default IKE and IPSec templates. View the results.

**Step 2** From the Monitoring menu tree, drill down to **Sessions** and answer the following questions:

Q2)     Is a LAN-to-LAN session established?

A)     _____

Q3)     What is the name of the connection?

A)    _____

Q4)    What is the IP address?

A)    _____

Q5)    What protocol is used?

A)    _____

Q6)    Which encryption scheme is used?

A)    _____

**Step 3**    Log out of the Concentrator. Close Internet Explorer.

**16**

# Configure the Cisco VPN 3000 Series Concentrator for LAN-to-LAN with NAT

## Overview

This lesson includes the following topics:

- Objectives

- LAN-to-LAN NAT overview

- Configuring the Concentrator LAN-to-LAN NAT feature

- Summary

- Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

**Upon the completion of this lesson, you will be able to perform the following tasks:**

- **Configure the static LAN-to-LAN NAT rule.**
- **Enable NAT rules.**
- **Monitor LAN-to-LAN NAT statistics.**

CSVPN 4.0—16-2

# LAN-to-LAN NAT Overview

This topic presents an overview of the LAN-to-LAN Network Address Translation (NAT) feature.
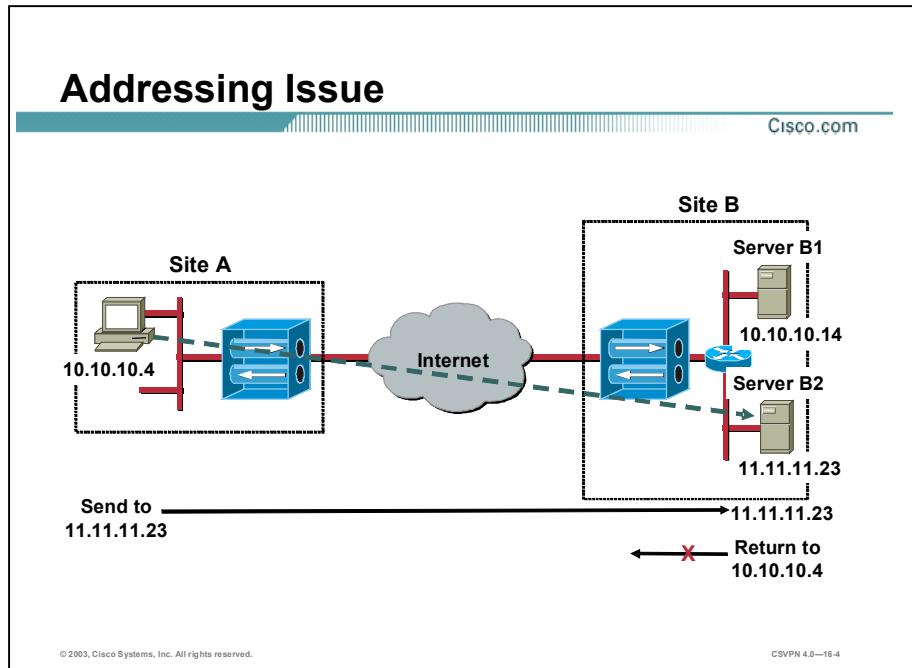


In the figure, there are two sites, site A and site B. Site A has one subnet 10.10.10.0/24. Site B has two subnets, 10.10.10.0/24 and 11.11.11.0/24. A PC at site A wants to access server B2. A PC packet is addressed to 11.11.11.23 and forwarded through the Cisco Virtual Private Network (VPN) 3000 Series Concentrators to server B2. From the remote end, the remote server responds to the PC's packet. Server B2 addresses the reply packet to 10.10.10.4/24. The issue is: what happens to server B2 reply packet. The packet is sent to the router. The router recognizes the destination IP address as a local address and sends the packet to the 10.10.10.0 network at site B. The packet is never routed to the PC at Site A.

**NAT**

Cisco.com

Site B

Server B1

Site A

10.10.10.14

10.10.10.4

Internet

Server B2

11.11.11.23

NAT

Send to
D: 11.11.11.23 → D: 11.11.11.23 → D: 11.11.11.23
S: 10.10.10.4 S: 20.20.20.4 S: 20.20.20.4

Return to
D: 10.10.10.4 ← D: 20.20.20.4 ← D: 20.20.20.4
S: 11.11.11.23 S: 11.11.11.23 S: 11.11.11.23

CSVPN 4.0—16-5
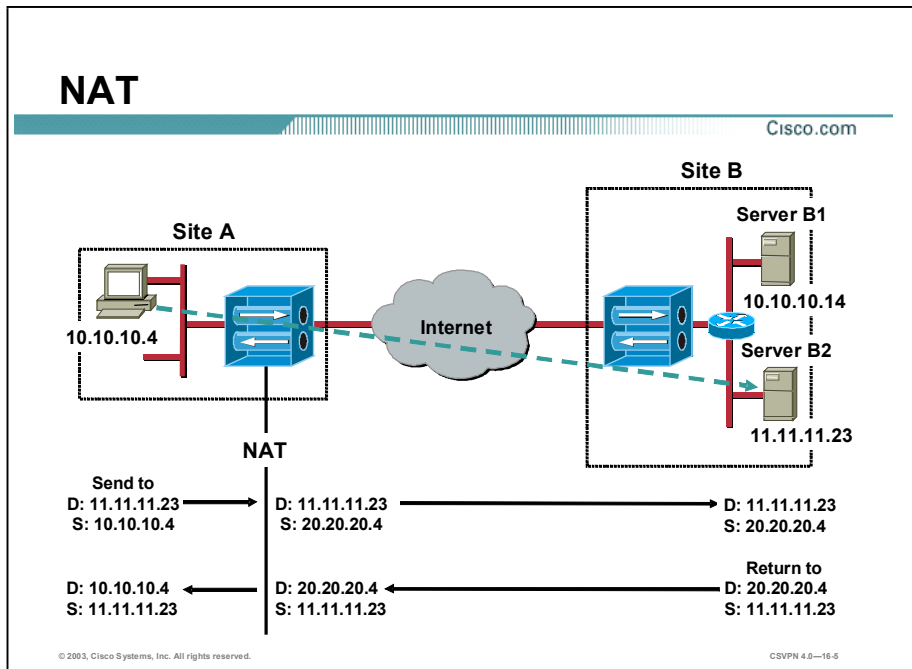
The issue can be resolved with Network Address Translation (NAT). The PC's source address is translated into a routable address. In the figure, the PC's source address is translated by Concentrator A to IP address 20.20.20.4/24 and forwarded to server B2. Server B2 replies with a packet addressed to IP address 20.20.20.4/24. The 20.20.20.4/24 IP address is routable by both site B's router and Concentrator. Back at site A, the reply packet is translated back to 10.10.10.4/24 by Concentrator A. Concentrator A then forwards the packet to the PC. NAT translation resolved the remote end routing issue by performing NAT at the local end, site A.

The next issue is: what happens if the PC on site A wants to communicate with server B1, 10.10.10.14/24. In the figure, there are overlapping addresses at both ends of the circuit.

**Overlapping Address Space**

Cisco.com

Site B

Server B1

Site A

10.10.10.14

Internet

Server B2

10.10.10.4

11.11.11.23

CSVPN 4.0—16-6
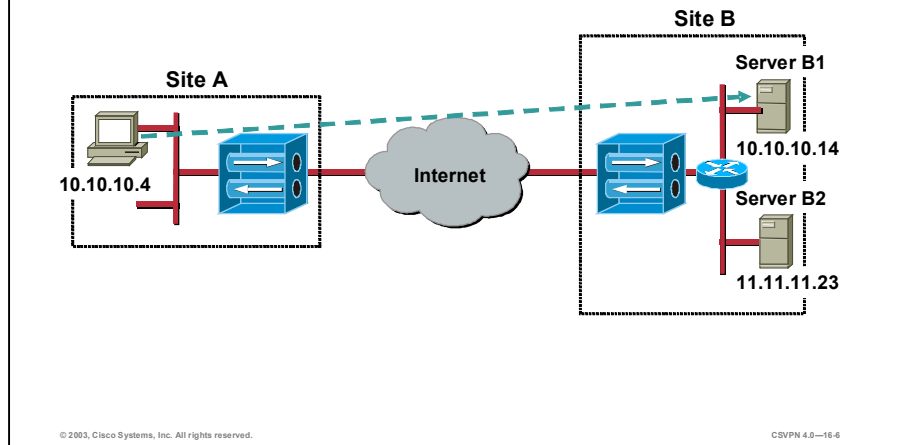
In the figure, both Site A and B are using the 10.10.10.0/24 address space. The way the network is currently configured the traffic between the Site A PC and server B2 cannot be routed. Such conflicts can be resolved by renumbering networks, but this solution is usually undesirable at best. Configure the Concentrators to perform NAT, and the Concentrators provide a solution to this problem. NAT enables the Concentrators to translate the overlapping network addresses at both ends of the tunnel. Enabling the Concentrators to route traffic between the networks.
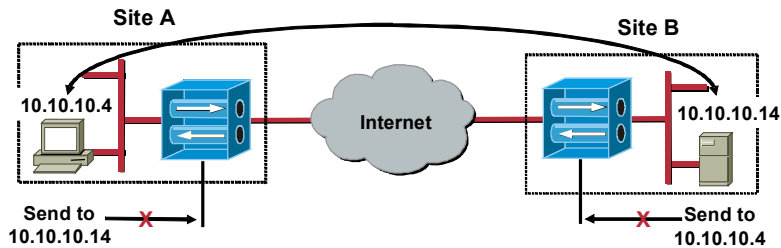
CSVPN 4.0—16-7

If the Site A PC attempts to access the server B2 using the server's IP address of 10.10.10.14/24, the attempt will fail. Concentrator A considers the destination IP address of 10.10.10.14/24 a local address and will not route the packet. The same is true at site B. If server B attempts to route a packet to the PC at IP address of 10.10.10.4/24, Concentrator B considers the destination IP address of 10.10.10.4/24 a local address and will not route the packet. The solution is NAT at both ends of the tunnel. The administrator can configure NAT rules in both Concentrators to make the routing possible. When a packet passing through the Concentrator matches a NAT rule, it is translated. A NAT session is created. Subsequent matching packets being passed are translated in accordance with this NAT session and receive the same translated IP address. The maintenance of NAT sessions allows the concentrator to maintain address and port continuity within a protocol session. NAT sessions expire and are deleted if they are not used for a period of time.

**Site A NAT**

Cisco.com

Site A

10.10.10.4

Internet

Site B

10.10.10.14

S: 10.10.10.4 → S: 20.20.20.4 → S: 20.20.20.4

NAT

D: 10.10.10.4 ← D: 20.20.20.4 ← D: 20.20.20.4

CSVPN 4.0—16-8
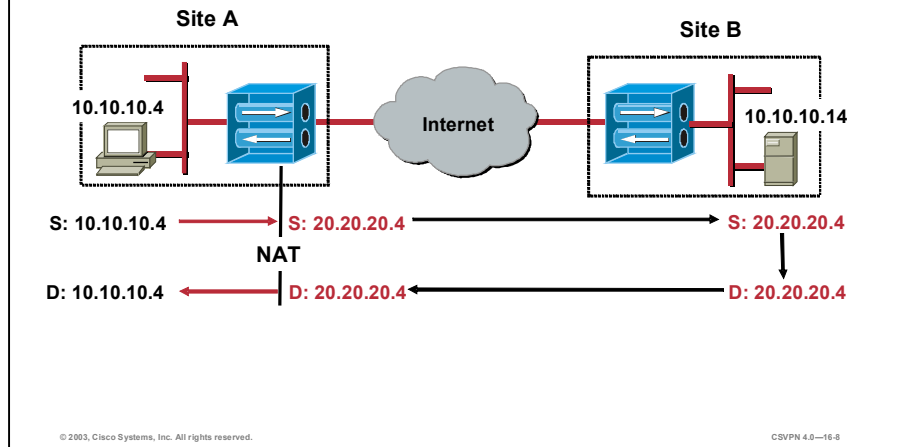
Both Concentrators implement Network Address Translation (NAT) to route the packets end-to-end. In the figure, site A Concentrator performs NAT on the PC's source IP address. Concentrator A translates the PC's source IP address of 10.10.10.4/24 to a 20.20.20.4/24 IP address. Concentrator A routes the packet to site B. Concentrator B delivers the packet to server B with a source IP address of 20.20.20.4/24. At site B, server B replies by sending a packet to the PC, destination IP address 20.20.20.4/24. Concentrator B receives the packet and routes it through the Internet to Site A. At Site A, if left un-translated, the packet is non-deliverable. The destination IP address of 20.20.20.4/24 is not located on the local LAN at Site A. The destination IP address of the packet must be translated. Concentrator A is configured to translate any packet with a destination IP address of 20.20.20.4/24 to IP address 10.10.10.4/24. After translation, the packet is successfully routed to the PC.

**Site B NAT**

Site A

Site B

10.10.10.4

Internet

10.10.10.14

D: 30.30.30.14 →       → D: 30.30.30.14 → D: 10.10.10.14

NAT

S: 30.30.30.14 ←       ← S: 30.30.30.14 ← S: 10.10.10.14
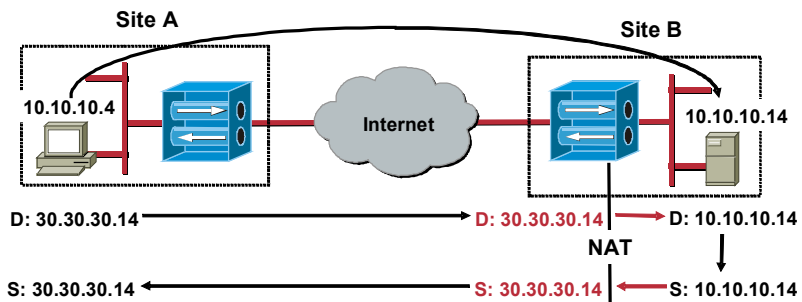
CSVPN 4.0—16-9

On the previous page, the PC's source IP address of 10.10.10.4 was translated by Concentrator A. With overlapping addresses at both ends of the network, translation is performed at both ends of the network. In this figure, server B IP address of 10.10.10.14 is translated to 30.30.30.14. If PC A attempted to send a packet to server B IP address 10.10.10.14/24, Concentrator A would drop the packet. Concentrator A considers 10.10.10.14/24 a local host. To overcome the local host issue, PC initiates a session with server B using a destination IP address of 30.30.30.14/24. The network administrator assigned an IP address of 30.30.30.14/24. Concentrator A routes the packet to site B. To deliver the packet to server B, the destination IP address of a packet, 30.30.30.14/24, must be translated to server B's IP address of 10.10.10.14/24. The translation is from a destination IP address of 30.30.30.14/24 to server B's IP address of 10.10.10.14/24. Once translated, the packet is routed to the server B2. A Network Address Translation (NAT) session is established. In the reverse direction, when a server B packet with the source address of 10.10.10.14/24 reaches Concentrator B, the source IP address is translated to 30.30.30.14/24.

# LAN-to-LAN NAT Summary

**PC A**
S: 10.10.10.4 → S: 20.20.20.4
D: 30.30.30.14 → D: 30.30.30.14

**Server B**
S: 20.20.20.4
D: 10.10.10.14

Internet

S: 30.30.30.14
D: 10.10.10.4 ← D: 20.20.20.4

S: 30.30.30.14 ← S: 10.10.10.14
D: 20.20.20.4

| Concentrator A | | | Concentrator B | | |
|---|---|---|---|---|---|
| **Concentrator Interface** | **Outbound Translation** | | **Inbound Translation** | | **Concentrator Interface** |
| S: 10.10.10.4 -> D: 30.30.30.14 | S: 20.20.20.4 D: 30.30.30.14 NAT Rule A | → | S: 20.20.20.4 D: 30.30.30.14-> NAT Rule B | D: 10.10.10.14 | S: 20.20.20.4 D: 10.10.10.14 |
| | | **Inbound Translation** | | **Outbound Translation** | |
| S: 30.30.30.14 D: 10.10.10.4 | D: 10.10.10.4 | S: 30.30.30.14 <-D: 20.20.20.4 NAT Rule A ← | | S: 30.30.30.14 D: 20.20.20.4 **NAT Rule B** | <-S: 10.10.10.14 D: 20.20.20.4 |

CSVPN 4.0—16-10

This figure summarizes the LAN-to-LAN Network Address Translations (NATs) taking place in the network. The top section displays the bidirectional traffic and the associated translations. The bottom section displays a translation table. The following table details Concentrator A and Concentrator B address translations:

| Concentrator | Native IP Address | Translated IP Address |
|---|---|---|
| Concentrator A | 10.10.10.4/24 | 20.20.20.4/24 |
| Concentrator B | 10.10.10.14/24 | 30.30.30.14/24 |

# Configuring the Concentrator LAN-to-LAN NAT Feature

This topic presents an overview of how to configure the LAN-to-LAN Network Address Translation (NAT) feature. Configuring LAN-to-LAN NAT is a three-step process: configure the LAN-to-LAN rule, enable the rule, then tie the translated addresses to the Concentrator. Configuring the LAN-to-LAN rule is covered first.
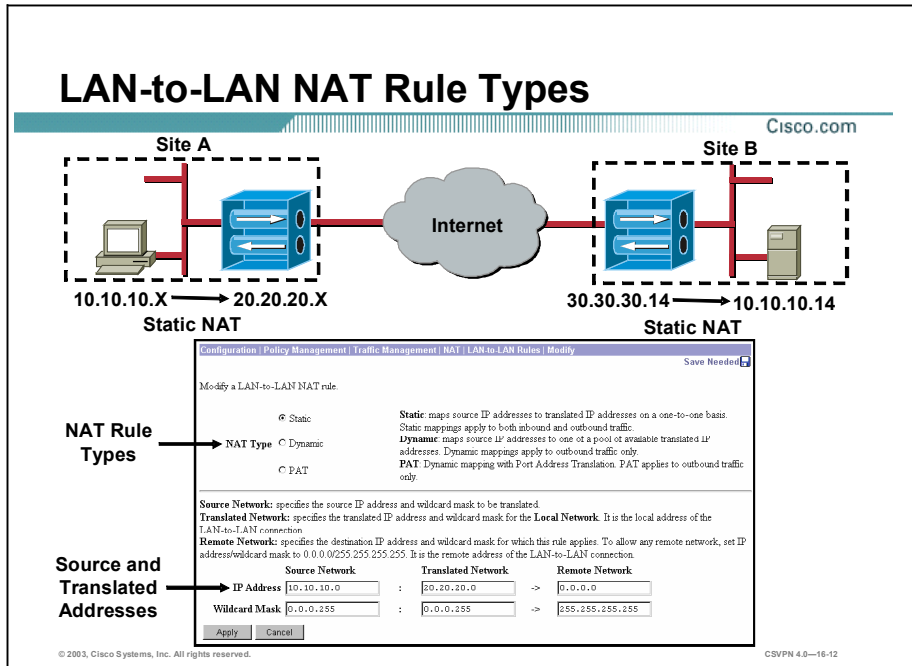


There are two elements to define to configure a LAN-to-LAN Network Address Translation (NAT) rule. The administrator defines the NAT rule type, whether the Concentrator applies a static, dynamic, or PAT rule. Once the rule is selected, the next step is to configure the source address and the translated address. What is source address and what is the translated address? NAT rule type is covered first.

There are three types of LAN-to-LAN NAT rules types, static, dynamic, and PAT. An explanation of the LAN-to-LAN rule types is as follows:

Static Translation Rules—Define one-to-one address mappings between networks. These rules have the following characteristics and restrictions:

- When the user configures a static translation rule, the specified local network must be the same class as the mapped network.

- When a packet is translated based on a static rule, port mappings are never being performed.

- In the Concentrator, all static rules are bidirectional.

Static rules are needed if servers are made available to a remote overlapping network. In the figure, at server at the site B is made available to PCs at site A. One-to-one NAT is performed. At the local end, a PC address of 10.10.10.X/24 is translated to an IP address of 20.20.20.X/24. At the remote end, an IP address of 30.30.30.14/24 is translated to 10.10.10.14/24, one-to-one mapping (not shown).

Dynamic translation rules—Map a local network to either a smaller network or to a single address. Dynamic translation may also alter the source or destination port of the packet being translated. These rules are most often applied to outbound traffic. Since, a remote host could not predict the mapped address of a dynamically mapped local host, inbound rules are generally not useful. Dynamic rules are usually applied to networks in which local and mapped addresses are of different classes, (for example, Class B and C IP addresses).

PAT translation rules—PAT LAN-to-LAN NAT rules are dynamic rules with Port Address Translation (PAT). PAT rules apply to outbound traffic only.

Notice that in this example, translation happens at both ends of the LAN-to-LAN connection. LAN-to-LAN NAT rules are configured in both Concentrators. There is one rule and set of addresses configured at one end and another rule with addresses configured at the opposite end.

NAT rule addressing is discussed later in this lesson.

## Site A LAN-to-LAN NAT Configuration
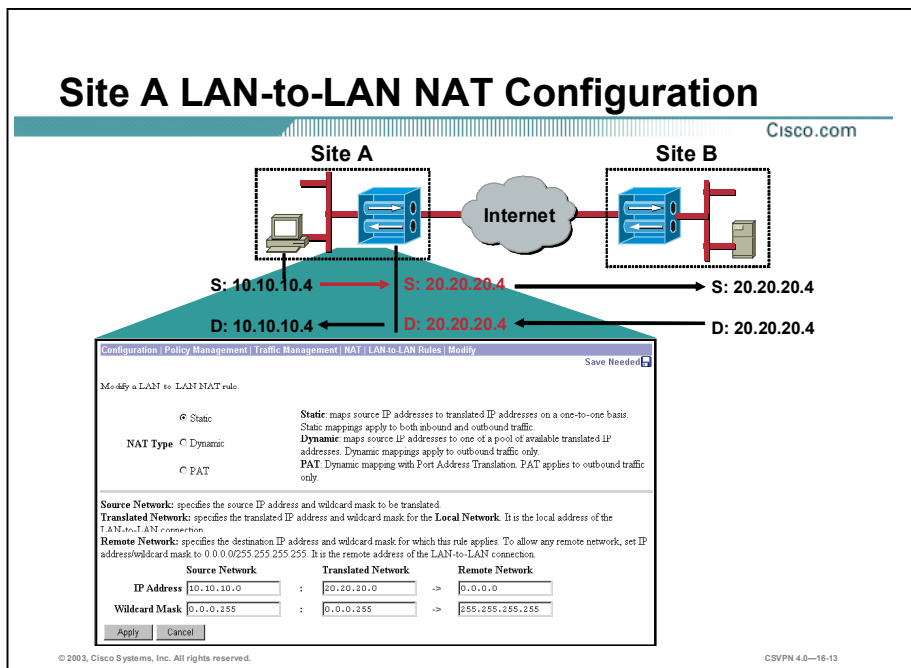
Once a NAT rule type is selected, the source and translated IP address are configured. The source network is the IP address of the local network. It is the source IP address and wildcard mask. The translated network is the address the source IP address is translated to. This is the translated IP address and wildcard mask. In the figure, a PC user on Site A is accessing a server on Site B. There is address overlap between the two private networks. The administrator is defining LAN-to-LAN NAT addressing rules for Concentrator A. The Concentrator is configured to translate the PC's 10.10.10.4/24 IP address to 20.20.20.4/24. Concentrator A's LAN-to-LAN NAT rule configuration is as follows:

■ NAT Type—Static LAN-to-LAN NAT rules map source IP addresses to translated IP addresses on a one-to-one basis. Static rules apply both to inbound traffic, which is traffic received over a tunnel and outbound traffic, which is traffic entering the tunnel.

■ Source Network—Local IP address, 10.10.10.0, and wildcard mask, 0.0.0.255. All the hosts on the 10.10.10.0 network.

■ Translated Network—Translated IP address, 20.20.20.0 and wildcard mask, 0.0.0.255. The source address is translated one-to-one. For example, source IP address 10.10.10.4/24 is translated to 20.20.20.4/24.

■ Remote Network—Destination IP network and wildcard mask for this LAN-to-LAN connection. This is the destination IP address for a specific remote LAN-to-LAN connection. This rule is applied only to packets bound for this address space. For example, there are multiple remote sites in a network sites B, C, and D. If the LAN-to-LAN NAT rule only applied to packets bound for site C. The administrator would define the address of site C in the remote network field. Remote network is not used in this example.

## Site B LAN-to-LAN NAT Configuration
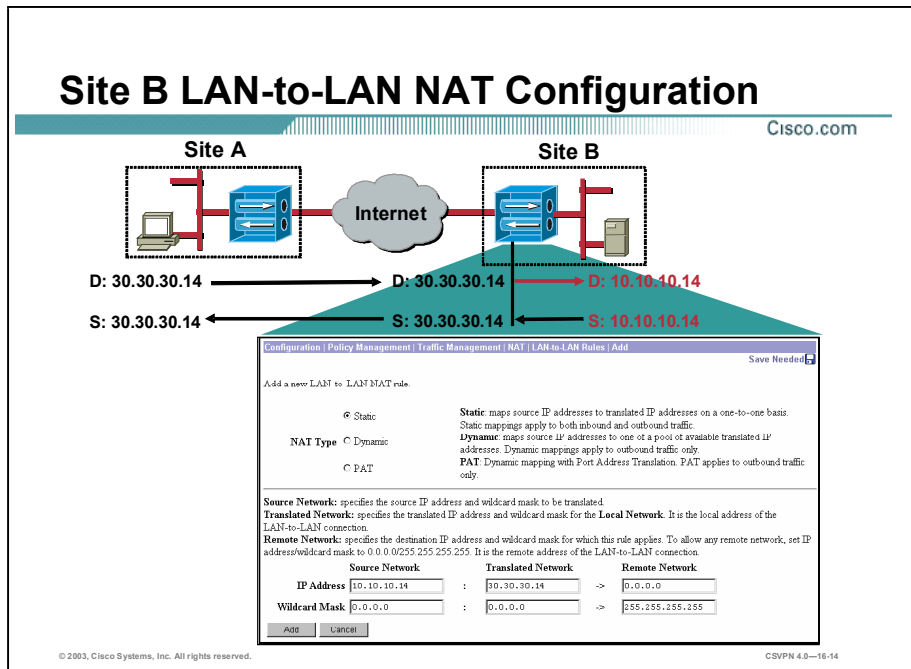
In the figure, translation takes place at both ends of the LAN-to-LAN connection. The Concentrator A's Network Address Translation (NAT) rules were configured on a previous page. The administrator is now defining LAN-to-LAN NAT rules for Concentrator B. The Concentrator is configured to translate a destination IP address of 30.30.30.14/24 to IP address 10.10.10.14/24. Concentrator B's LAN-to-LAN NAT rule configuration is as follows:

■ NAT Type—Static LAN-to-LAN NAT rules map source IP addresses to translated IP addresses on a one-to-one basis, 10.10.10.14/24 to 30.30.30.14/24. Static rules apply both to inbound traffic, which is traffic received over a public interface and outbound traffic, which is traffic bound for a public interface.

■ Source Network—Server B IP address, 10.10.10.4/24, and wildcard mask, 0.0.0.0. A specific server on the 10.10.10.0/24 network is referenced.

■ Translated Network—Translated IP address, 30.30.30.14 and wildcard mask, 0.0.0.0. IP address 30.30.30.14/24 is the translated IP address for server B.

■ Remote Network—A destination IP network and wildcard mask for this LAN-to-LAN connection is not used.

## Enable NAT

Cisco.com

**Configuration | Policy Management | Traffic Management | NAT | Enable**

This section lets you enable system-wide NAT rules.

**Interface NAT Rules Enabled** ☐ Check to enable NAT rules on interfaces.
**LAN-to-LAN Tunnel NAT Rule Enabled** ☑ Check to enable NAT rules on LAN-to-LAN tunnels.

[ Apply ] [ Cancel ]

CSVPN 4.0—16-15

The second step is to enable LAN-to-LAN Network Address Translation (NAT). Choose
**Configuration>Policy Management>Traffic Management>NAT>Enable**. The Enable
window opens. Select the **LAN-to-LAN Tunnel NAT Rule Enabled** check box to enable NAT
rules for LAN-to-LAN connections, or deselect it to disable these NAT rules. By default, the
check box is deselected. It is recommended that you configure LAN-to-LAN NAT rules before
you enable the function. The administrator can change NAT rules while NAT is enabled. Doing
so affects subsequent sessions, but not current sessions, as long as the changed rule still allows
current sessions; if it does not, traffic will stop.

**Concentrator Network Lists—Site A**
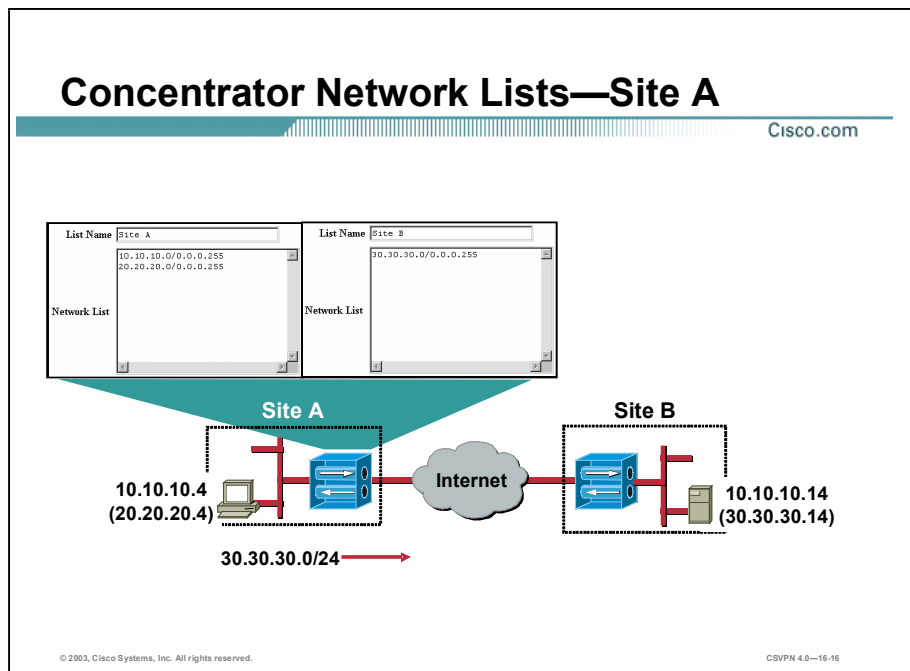
The NAT rule types were selected, NAT rules were defined, and the LAN-to-LAN Tunnel NAT rule was enabled. The last step is to tie the translated addresses to the Concentrator. The Concentrator must know how to route the translated addresses. The translated addresses are defined at their respective ends of the tunnel with network lists. Concentrator A needs to know that 10.10.10.0/24 and 20.20.20.0/24 are considered to be local addresses. 30.30.30.0/24 is considered to be a remote address. To reach 30.30.30.0/24 from site A, traffic is routed down a LAN-to-LAN tunnel between site A and site B. The two network lists are defined and applied to the IPSec LAN-to-LAN tunnel. Once defined, PC packets can be routed from site A to the server on site B.

In the figure, two network lists are defined. At site A, local and remote network address lists are defined. The local list includes network 10.10.10.0 and 20.20.20.0. A remote network list includes network 30.30.30.0. These lists aid the Concentrator in making LAN-to-LAN tunnel routing decisions. Which networks are local and which networks can be reached through the tunnel, remote network list?

The network information is also configured at site B (not shown). Site B network list information is discussed later in this lesson.

Concentrator Network Lists—Site B
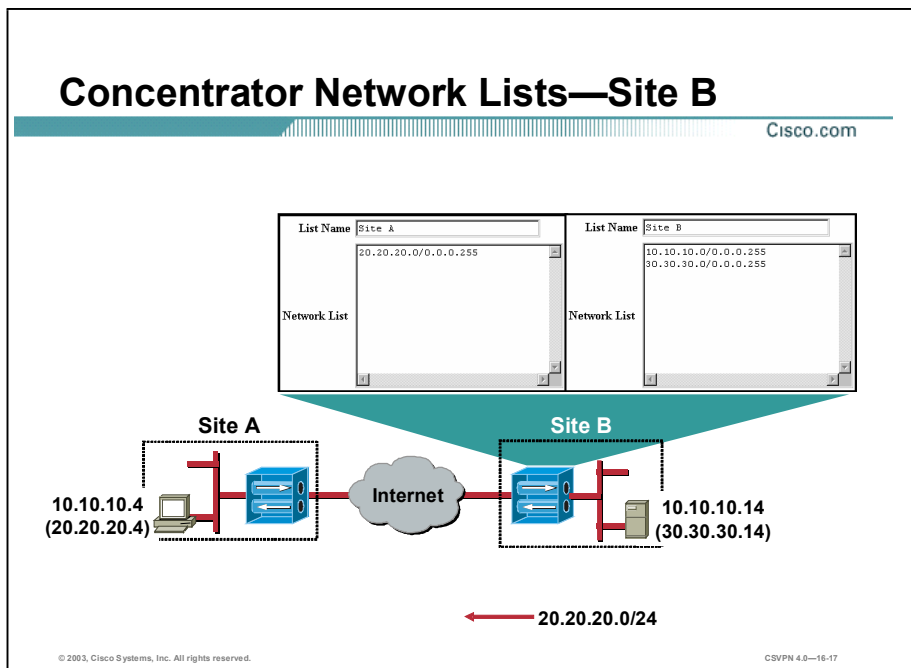
The NAT rule types were selected, NAT rules were defined, and the LAN-to-LAN Tunnel NAT rule was enabled. The last step is to tie the translated addresses to the Concentrator B. Concentrator B must know how to route the translated addresses. Concentrator B needs to know that 10.10.10.0/24 and 30.30.30.0/24 are considered to be local addresses. 20.20.20.0/24 is considered to be a remote address. To reach 20.20.20.0/24 from site B, traffic is routed down a LAN-to-LAN tunnel between site B and site A. The two network lists are defined and applied to the IPSec LAN-to-LAN tunnel. Once defined, PC packets can be routed from site B to the PC on site A.

In the figure, two network lists are defined at each end of the tunnel. At site B, local and remote network address lists are defined. The local list includes network 10.10.10.0 and 30.30.30.0. A remote network list includes networks and 20.20.20.0. These lists aid the Concentrator in making LAN-to-LAN tunnel routing decisions. Which networks are local and which networks can be reached through the tunnel, remote network list?

## LAN-to-LAN NAT Statistics

Cisco.com

**Site A**

Ping 30.30.30.5
Reply from 30.30.30.5
Reply from 30.30.30.5
Reply from 30.30.30.5

10.0.1.15

Internet

**Site B**

S: 10.0.1.15          S: 20.20.20.15
D: 30.30.30.5          D: 30.30.30.5

Monitoring | Statistics | NAT                                    Thursday, 26 September 2002 10:50:57
                                                                 Reset⊘Restore⊛Refresh⊛

|          | Packets |
|----------|---------|
| In       | 4       |
| Out      | 4       |
|          | Translations |
| Active   | 1       |
| Peak     | 0       |
| Total    | 1       |

**NAT Sessions**

| Source | | Destination | | Translated | | | | | Translated | |
|--------|--|-------------|--|------------|--|-----------|-----|------|-------|---------|
| IP Address | Port | IP Address | Port | IP Address | Port | Direction | Age | Type | Bytes | Packets |
| 10.0.1.15 | 0 | 30.30.30.5 | 0 | 20.20.20.15 | 0 | Outbound | 2 | No Port Mapping | 480 | 8 |
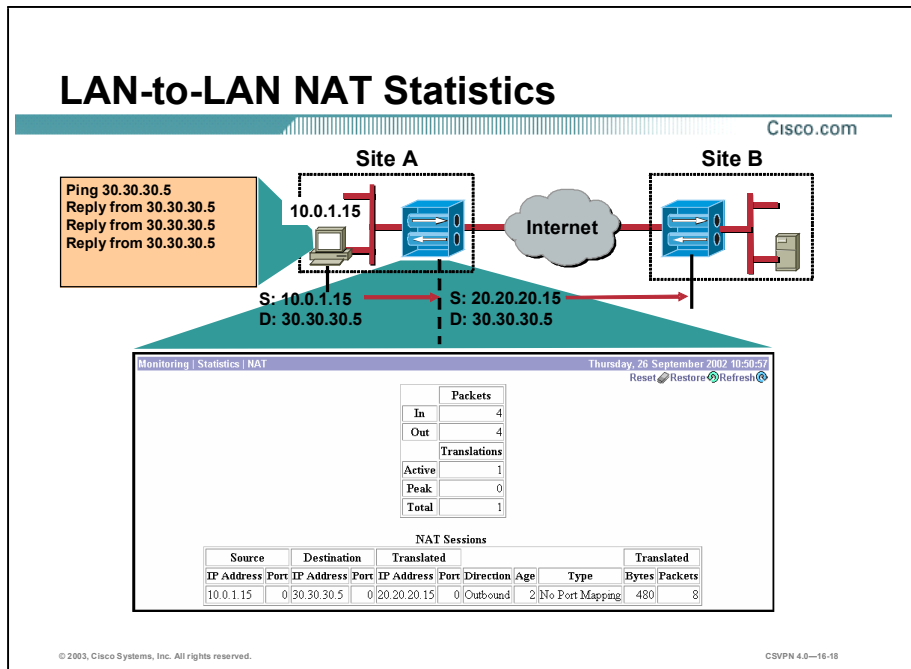
Choose **Monitoring>Statistics>NAT**. The NAT window opens to view NAT statistics. The
window displays statistics for NAT activity on the Concentrator since it was last booted or reset.
An explanation of the NAT statistics fields is as follows:

■ Packets In/Out—The total of NAT packets inbound and outbound since the last time the
Concentrator was rebooted or reset.

■ Translations Active—The number of currently active NAT sessions.

■ Translations Peak—The maximum number of NAT sessions that were simultaneously active
on the Concentrator since it was last booted or reset.

■ Translations Total—The total number of NAT sessions on the Concentrator since it was last
booted or reset.

■ NAT Sessions—The following topics provide detailed information about active NAT
sessions on the Concentrator:

— Source IP Address/Port—The source IP address and port for the NAT session.

— Destination IP Address/Port—The destination IP address and port for the NAT session.

— Translated IP Address/Port—The translated IP address and port for the NAT session.
The Concentrator uses this port number to keep track of which devices initiate data
transfer; by keeping this record, the Concentrator is able to correctly route responses.

— Direction—The direction, inbound or outbound, of the data transferred for the NAT session.

— Age—The number of half seconds remaining until the NAT session times out.

In the figure, the PC is pinging the remote server, 10.0.6.5. The PC needs to address packets to 30.30.30.5 to access the remote server. This is the address supplied by the network administrator. In the statistics window, there are 4 packets in and 4 packets out. This represents 1 NAT session. In the NAT session statistics at the bottom of the window, the address of the PC is the source address, 10.0.1.15. The destination address of the server is the address supplied by the IT administrator, 30.30.30.5. Concentrator A will translate the PC source address of 10.0.1.15 to 20.20.20.15. Therefore, the translated address is 20.20.20.15. The translation occurs in the outbound direction, from PC to Concentrator A.

# Summary

This topic summarizes what you learned in this lesson.

## Summary

- **LAN-to-LAN NAT translates overlapping private network address spaces.**
- **There are two translation rule types: static and dynamic.**
- **LAN-to-LAN rules should be configured first.**
- **LAN-to-LAN rules should be enabled next.**
- **Tie a translated address to a Concentrator.**

CSVPN 4.0—16-20

# Lab Exercise—Configure the Cisco VPN 3000 Series Concentrators for NAT over LAN-to-LAN

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to configure one end of a LAN-to-LAN Virtual Private Network (VPN) while another team completes the same tasks at a remote site. Work with your lab partner to complete the following tasks on your side of the LAN-to-LAN VPN:

- Complete the lab exercise setup.

- Verify the Cisco VPN 3000 Series Concentrator LAN-to-LAN connectivity.

- Configure the LAN-to-LAN NAT rules.

- Configure network lists.

- Verify the Cisco VPN 3000 Series Concentrator LAN-to-LAN connectivity.

- Create and monitor a LAN-to-LAN NAT session.

---

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
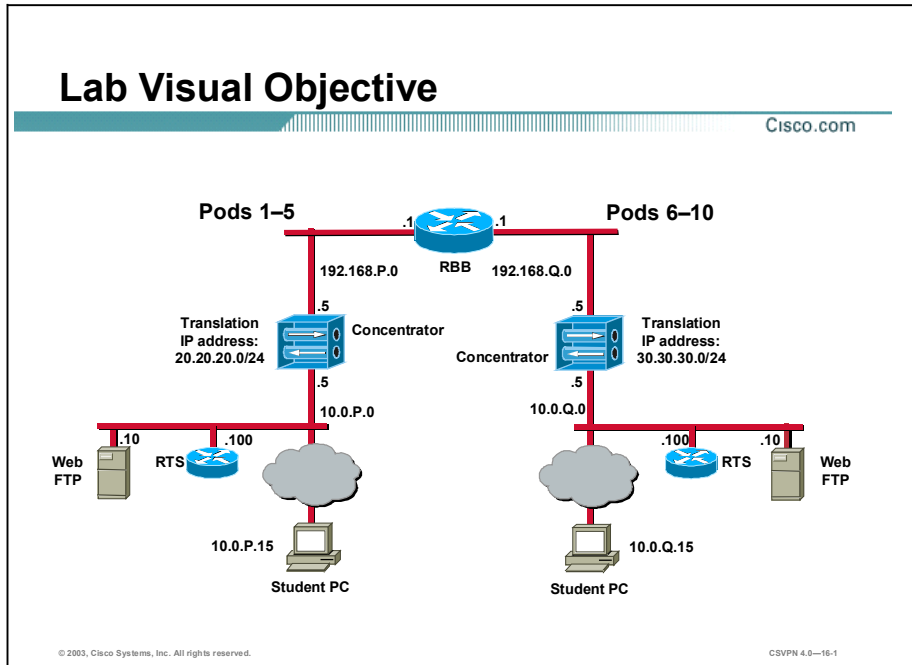


## Scenario

Your company wants you to implement a VPN between the world headquarters campus site and the remote sales offices using Network Address Translation (NAT) over a LAN-to-LAN tunnel. You must configure the Cisco VPN 3000 Series Concentrators for LAN-to-LAN tunneling using NAT.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment is setup as follows:

■ Ensure that your student PC is powered on.

■ Ensure that your student IP addresses are configured correctly:

— Primary IP address—10.0.P.15
(where P = pod number)

— Subnet mask—255.255.255.0

— Default gateway IP address—10.0.P.5
(where P = pod number)

- Ensure that your Concentrator is powered on.

## Task 2—Verify the Cisco VPN 3000 Series Concentrator LAN-to-LAN Connectivity

Before configuring the LAN-to-LAN NAT rules, verify a tunnel can be established between Concentrators. Complete the following steps to verify the LAN-to-LAN tunnel connections:

**Step 1**    Launch Internet Explorer by double-clicking the desktop icon.

**Step 2**    Enter a Concentrator private interface IP address of **10.0.P.5** in the Internet Explorer Address field (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 3**    Log into the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

Login: **admin**

Password: **admin**

The username (login) and password are always case sensitive.

**Step 4**    Ping your peer Concentrator private interface at **10.0.Q.5** (where Q = peer pod number) using the Administration menu tree ping function. If the LAN-to-LAN wizard was configured correctly, the VPN 3005 will build an IPSec tunnel based on the student supplied network information and the default IKE and IPSec templates. View the results.

**Step 5**    From the Monitoring menu tree, drill down to **Sessions** and answer the following questions:

Q1)    Is the LAN-to-LAN session established?

A)    _____

## Task 3—Configure the LAN-to-LAN NAT Rules

In this lab exercise, translation is performed at both ends of the tunnel. To accomplish this, NAT rules must be defined, NAT rules must be enabled, and translation addresses applied to LAN-to-LAN tunnel. The first step is to configure LAN-to-LAN NAT rules. One NAT rule is configured in each Concentrator. The exact IP addresses to enter depends on the location of the Concentrator. Pods 1–5 enter a translation IP address of 20.20.20.0/0.0.0.255. You will perform step 1. Pods 6–10, use translation IP address of 30.30.30.0/0.0.0.255. You will perform step 2. Configure and enable the LAN-to-LAN rule for your pod.

- For pods 1–5, complete step 1.

- For pods 6–10, complete step 2.

**Step 1**    For pods 1–5, complete the following sub-steps to build the correct NAT rule. From the Configuration menu, drill down to **Policy Management>Traffic Management>NAT>LAN-to-LAN NAT Rules**. The Configuration>Policy Management>Traffic Management>NAT>LAN-to-LAN Rules window opens.

    1.    Under the Actions column click **Add**. The Configuration>Policy Management>Traffic Management>NAT>LAN-to-LAN Rules>Add window opens.

2. Under NAT type, select **Static**.

3. Configure the Source Network IP address and wildcard mask fields.

- IP address—10.0.P.0
  (where P = pod number)

- Wildcard mask—0.0.0.255

4. Configure the correct translation IP address for your end of the tunnel. If you are located at pods 1–5, enter the following in the Translated IP address and wildcard mask fields:

- IP address—20.20.20.0

- Wildcard mask—0.0.0.255

5. Click **Add**.

6. From Configuration, drill down to **Policy Management>Traffic Management>NAT> Enable**. The Enable window opens.

7. Select LAN-to-LAN Tunnel NAT Rule Enabled.

8. Click **Apply**.

9. Save the changes.

10. Proceed to Task 4.

**Step 2**    For pods 6–10, complete the following sub-steps to build the correct NAT rule. From the Configuration menu, drill down to **Policy Management>Traffic Management>NAT>LAN-to-LAN NAT Rules**. Configuration>Policy Management>Traffic Management>NAT>LAN-to-LAN Rules window opens.

1. Under the Actions column click **Add**. The Configuration>Policy Management>Traffic Management>NAT>LAN-to-LAN Rules>Add window opens.

2. Under NAT type, select **Static**.

3. Configure the Source Network IP address and wildcard mask fields.

- IP address—10.0.P.0
  (where P = pod number)

- Wildcard mask—0.0.0.255

4. Configure the correct translation IP address for your end of the tunnel. If you are located at pods 6–10, enter the following in the Translated IP address and wildcard mask fields:

- IP address—30.30.30.0

- Wildcard mask—0.0.0.255

5. Click **Add**.

6. From Configuration, drill down to **Policy Management>Traffic Management>NAT> Enable**. The Enable window opens.

7. Select LAN-to-LAN Tunnel NAT Rule Enabled.

8. Click **Apply**.

9. Save the changes.

10. Proceed to task 4.

## Task 4—Configure Network Lists

In a previous lab, you defined network lists for both ends of the LAN-to-LAN tunnel. In this task, modify each list to include the translation IP address. The two translation addresses are 20.20.20.0 and 30.30.30.0. It is important to add each IP address to the correct network list. For pods 1–5, IP address 20.20.20.0 is a local address and 30.30.30.0 is a remote address. For pods 6–10, IP address 30.30.30.0 is a local address and 20.20.20.0 is a remote address (If confused, viewing the visual objective at the beginning of this lab may help.) Complete the following steps to add the local and remote translation addresses to the proper network list:

■ For pods 1–5, complete step 1.

■ For pods 6–10, complete step 2.

**Step 1** For pods 1–5, complete the following sub-steps to build a local network list:

1. From the Configuration menu tree, drill down to Policy Management>Traffic Management> Network Lists.

2. Under Network List column, select **podP** (your local network list).
   (where P = pod number)

   ■ Click **Modify**.

   ■ Under Network Lists, enter **20.20.20.0/0.0.0.255**.

   ■ Click **Apply**.

3. Under Network List column, select **podQ** (your remote network list).
   (where Q = peer pod number)

   ■ Click **Modify**.

   ■ Under Network Lists, enter **30.30.30.0/0.0.0.255**.

   ■ Click **Apply**.

- Save the configuration changes.

4. Proceed to task 5.

**Step 2** For pods 6–10, complete the following sub-steps to build a local network list:

5. From the Configuration menu tree, drill down to **Policy Management>Traffic Management>Network Lists**.

6. Under the Network List column, select **podP** (your local network list).
   (where P = pod number)

- Click **Modify**.

- Under Network Lists, enter **30.30.30.0/0.0.0.255**.

- Click **Apply**.

7. Under Network List column, select **podQ** (your remote network list).
   (where Q = peer pod number)

- Click **Modify**.

- Under Network Lists, enter **20.20.20.0/0.0.0.255**.

- Click **Apply**.

- Save the configuration changes.

8. Proceed to task 5.

# Task 5—Verify the Cisco VPN 3000 Series Concentrator LAN-to-LAN Connectivity

After completing the LAN-to-LAN NAT configuration changes, verify a tunnel can still be established between Concentrators. Complete the following steps to check the LAN-to-LAN tunnel connections:

**Step 1** Open a Command Prompt from the desktop icon on your student PC and ping the translated address of your peer's student PC continuously.

| Note | If necessary, disconnect any previously established LAN-to-LAN tunnels. |
|------|-----------------------------------------------------------------------|

- For pods 1-5, use the following: C:\ ping 30.30.30.15 -t

- For pods 6-10, use the following: C:\ ping 20.20.20.15 -t

**Step 2** View the results.

**Step 3** From the Monitoring menu tree, drill down to **Sessions** and answer the following questions:

Q2)     Is a LAN-to-LAN session established?

A)     _____

## Task 6—Monitor a LAN-to-LAN NAT Session

In this task, you will open a LAN-to-LAN NAT session with your peer's student PC. By continuously pinging your peer's student PC address, you create a NAT session through the LAN-to-LAN tunnel. Complete the following steps to create and monitor a LAN-to-LAN NAT session:

**Step 1**   From Monitoring menu tree, drill down to **Statistics>NAT**. The Monitoring> Statistics>NAT window opens.

**Step 2**   Click **Reset** in the Monitoring>Statistics>NAT window. Leave this Internet Explorer window open.

**Step 3**   Click **Refresh** in the Monitoring>Statistics>NAT window. NAT session statistics appear.

**Step 4**   Answer the following questions from the Packets and Translations statistics fields:

Q3)     How many packets went in and out?

A)     _____

Q4)     How many total translations were there?

A)     _____

**Step 5**   Answer the following questions from the NAT Sessions statistics fields:

Q5)     What is the Source IP address?

A)     _____

Q6)     What is the Destination IP address?

A)     _____

Q7)     What is the Translated IP address?

A)     _____

Q8)     What is the NAT Session Direction?

A)     _____

**Step 6**   Return to the Command Prompt window and stop the continuous ping by clicking **Control + C** on the student PC.

**Step 7**   Return to the local Cisco VPN 3000 Concentrator Series Manager window. From Configuration, drill down to **Policy Management>Traffic Management> NAT>Enable**. The Configuration> Policy Management>Traffic Management> NAT>Enable window opens.

**Step 8**   Deselect **LAN-to-LAN Tunnel NAT Rule Enabled**.

**Step 9**   Click **Apply**.

**Step 10** Save the changes.

**17**

# Configure the Cisco Virtual Private Network 3000 Series Concentrator for LAN-to-LAN Using Digital Certificates

## Overview

This lesson discusses how to configure the Cisco Virtual Private Network (VPN) 3000 Series Concentrator for LAN-to-LAN using the Simple Certificate Enrollment Protocol (SCEP). After presenting an overview of the SCEP process, the lesson shows you each major step of the configuration. This lesson includes the following topics:

■ Objectives

■ SCEP support overview

■ Root certificate installation

■ Identity certificate installation

■ Summary

■ Lab exercise

# Objectives

This topic lists the lesson's objectives.

## Objectives

Cisco.com

**Upon completion of this lesson, you will be able to perform the following tasks:**

- **Explain the purpose of SCEP.**
- **Explain how root certificates are installed via SCEP.**
- **Explain how identity certificates are installed via SCEP.**
- **Configure the Concentrator for LAN-to-LAN support with digital certificates.**

© 2003, Cisco Systems, Inc. All rights reserved.

CSVPN 4.0—17-2

# SCEP Support Overview

With a certificate authority (CA), you do not need to configure keys between all of the encrypting IPSec peers. Instead, each individual peer enrolls with the CA and requests a certificate. When this has been accomplished, the peers can exchange certificates during tunnel establishment.

In the Cisco Virtual Private Network (VPN) 3000 Series Concentrator, there are two enrollment methods: manual and automated. With the manual process, there are a significant number of steps to perform before a certificate can finally be imported into the Concentrator. Using the Simple Certificate Enrollment Protocol (SCEP), the process is streamlined and simplified.



**CA Server Fulfilling Requests from IPSec Peers**

Cisco.com

**Each IPSec peer individually enrolls with the CA server.**

**CA server**
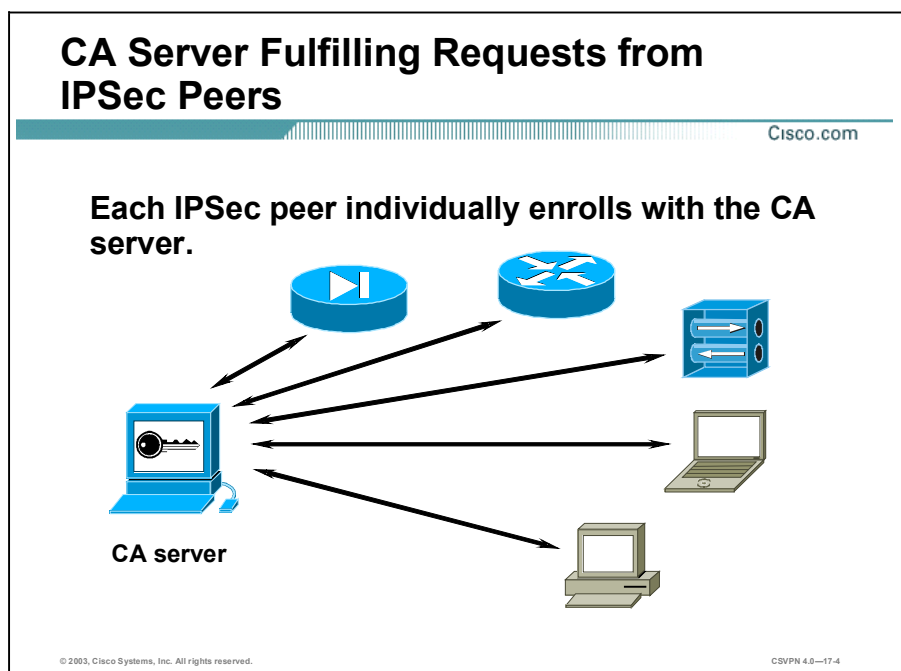
CSVPN 4.0—17-4

This topic covers how certificates are generated and transferred between a CA and the Concentrator via SCEP.

**SCEP-Based Enrollment**

Cisco.com

Certificate
server

SCEP
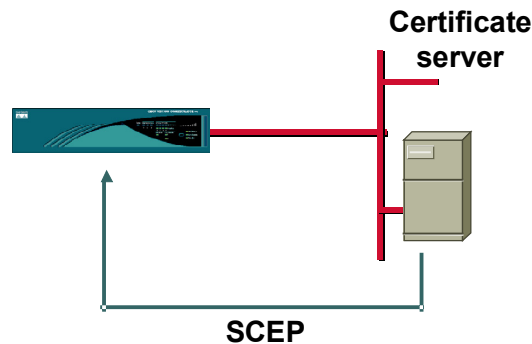
CSVPN 4.0—17-5

Public key technology is becoming more widely deployed. With the use of public key certificates in network security protocols, comes the need for a certificate management protocol that Public Key Infrastructure (PKI) clients and CA servers can use to support automated certificate enrollment. The goal of the Simple Certificate Enrollment Protocol (SCEP) is to support the secure issuance of certificates to network devices in a scalable, more streamlined manner. SCEP supports automated CA public key distribution and certificate enrollment. (SCEP is a secure messaging protocol that requires minimal user intervention).

This method is quicker and allows you to enroll and install certificates using only the Concentrator Manager, but is only available if you are both enrolling with a CA that supports SCEP and enrolling via the web. If your CA does not support SCEP or if you do not have network connectivity to your CA, then you cannot use the automatic method; you must use the manual method.

**SCEP Loading Process**

Certificate server

Load root certificate via SCEP

Certificate server

Load identity certificate via SCEP

CSVPN 4.0—17-6
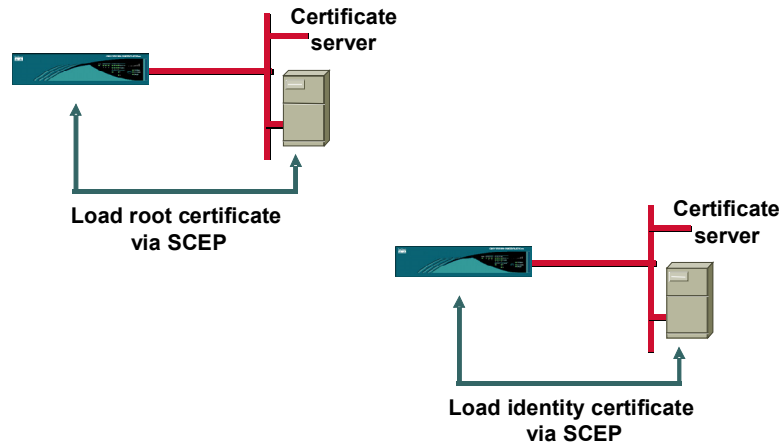
Whether you use the automatic or manual method, you follow the same overall certificate management procedure:

**Step 1**   Install one or more CA certificates.

**Step 2**   (Optional.) Enable certificate revocation list (CRL) checking.

**Step 3**   Enroll and install identity certificates.

**Step 4**   Enable digital certificates on the Concentrator.

If you have trouble enrolling or installing digital certificates via SCEP, enable a Certificate (CERT) event class to assist in troubleshooting.

# Root Certificate Installation

This topic explains how to install a root certificate on the Concentrator via SCEP.
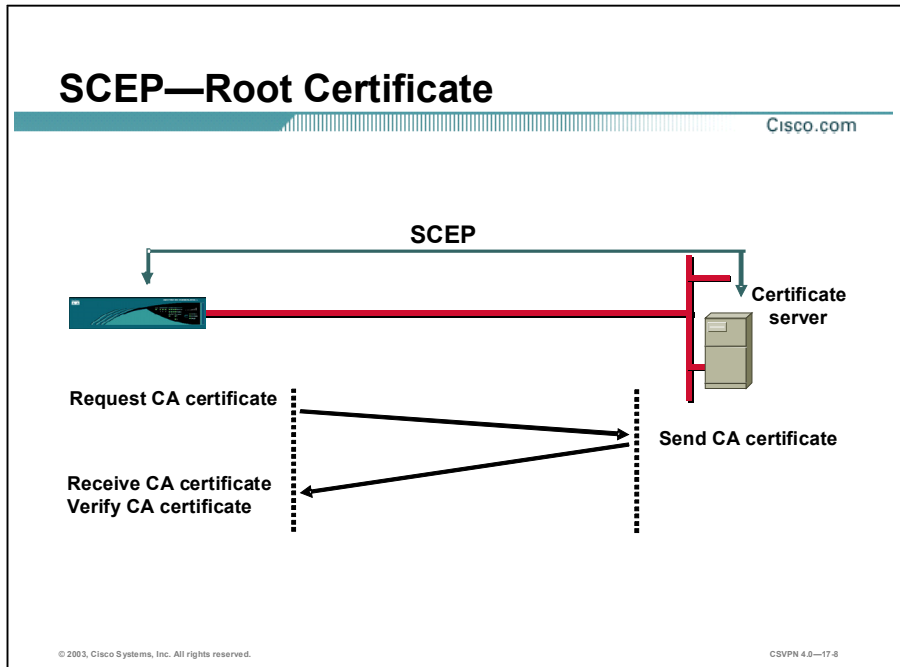


Before any PKI operation can be started, the Concentrator needs to install the CA certificates. Complete the following steps to install the CA certificate:

**Step 1**  The Concentrator sends a Get CA message to the CA.

**Step 2**  The CA returns a CA certificate to the Concentrator.

**Step 3**  After the Concentrator receives the CA certificate, the Concentrator authenticates the CA certificate. The administrator can also verify the CA certificate out-of-band by comparing the Concentrator's root certificate hash with the root certificate hash registered with the CA administrator. When comparing the two hashes, they should match.

# Certificate Management

Cisco.com

| Administration | Certificate Management | | | Monday, 28 July 2003 15:49:26 |
| | | | | Refresh |

This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.

- Click here to install a CA certificate
- Click here to enroll with a Certificate Authority
- Click here to install a certificate

**Certificate Authorities** [ View All CRL Caches | Clear All CRL Caches ] (current: 0, maximum: 6)

| Subject | Issuer | Expiration | SCEP Issuer | Actions |
|---------|--------|------------|-------------|---------|
| No Certificate Authorities | | | | |

**Identity Certificates** (current: 0, maximum: 2)

| Subject | Issuer | Expiration | Actions |
|---------|--------|------------|---------|
| No Identity Certificates | | | |

**SSL Certificate** [ Generate ] *Note: The public key in the SSL certificate is also used for the SSH host key.*

| Subject | Issuer | Expiration | Actions |
|---------|--------|------------|---------|
| 10.0.1.5 at Cisco Systems, Inc. | 10.0.1.5 at Cisco Systems, Inc. | 05/19/2006 | View | Renew | Delete |

**Enrollment Status** [ **Remove All:** Errored | Timed-Out | Rejected | Cancelled | In-Progress ] (current: 0 available: 3)

| Subject | Issuer | Date | Use | Reason | Method | Status | Actions |
|---------|--------|------|-----|--------|--------|--------|---------|
| No Enrollment Requests | | | | | | | |

CSVPN 4.0—17-9

The Certificate Manager enables you to manage digital certificates. The links at the top of the Certificate Management window guide you step-by-step through the process of enrolling and installing certificates:

■ Click the **Click here to install a CA certificate** link to install a CA certificate (via SCEP or manually). The Click here to install a CA certificate option is only available from this window when no CA certificates are installed on the Concentrator.

■ Click the **Click here to enroll with a Certificate Authority** link to create an identity certificate enrollment request.

■ Click the **Click here to install a certificate** link to install the certificate obtained via enrollment.

The bottom section of the Certificate Management window shows all the certificates installed in the Concentrator and lets you view, enable revocation checking, and delete certificates. The following four tables are displayed:

■ Certificate Authorities table—Shows root and subordinate CA certificates installed on the Concentrator.

■ Identity Certificates table—Shows installed server identity certificates.

■ SSL Certificate table—Shows the Secure Sockets Layer (SSL) server certificate installed on the Concentrator. The system can have only one SSL server certificate installed: either a self-signed certificate or one issued in a PKI context.

- Enrollment Status table—Tracks the status of active enrollment requests. The number of enrollment requests you can make at any given time is limited to the Concentrator's identity certificate capacity. Most Concentrator models allow a maximum of 20 identity certificates. For example, if you already have 5 identity certificates installed, you are able to create only up to 15 enrollment requests. The Cisco VPN 3005 Concentrator is an exception, supporting only 2 identity certificates. Only on the Cisco VPN 3005 Concentrator can you request a third certificate—even if there are already two certificates installed. But the Concentrator does not install this certificate immediately. First, you must delete one of the existing certificates. Then you must activate the new certificate to replace the one you just deleted. The Concentrator notifies you (by issuing a severity 3 CERT class event) if any of the installed certificates are within one month of expiration.

# Concentrator—SCEP Enrollment Procedure

There are three steps to generate a CA certificate via the Simple Certificate Enrollment Protocol (SCEP):

**Step 1**  In the Administration>Certificate management window, click the **Click here to install a CA certificate** link to install a CA certificate via SCEP. The **Click here to install a CA certificate** option is available from this window only when no CA certificates are installed on the Concentrator. If you do not see this option, click the **Click here to install a certificate** link.

**Step 2**  In the Administration>Certificate Management>Install>CA Certificate window, click the **SCEP (Simple Certificate Enrollment Protocol)** link.

**Step 3**  In the Administration>Certificate Management>Install>CA Certificate>SCEP window, enter the URL information of the CA. There is further discussion of the URL field later in this lesson. Click **Retrieve** to retrieve and install a root certificate. If all goes well, the result is an installed root certificate.

**SCEP URL**

Cisco.com

**Certificate server**
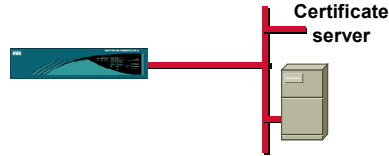
**CA server information:**
- **What is the URL of the CA server?**
- **Is a descriptor required?**

Administration | Certificate Management | Install | CA Certificate | SCEP

Enter the information needed to retrieve the CA certificate via SCEP. **Please wait for the operation to complete.**

URL http://10.0.1.10/certsrv/mscep/mscep

CA Descriptor [_____]  Required for some PKI configurations.

[Retrieve]  [Cancel]

CSVPN 4.0—17-11

In the Administration>Certificate Management>Install>CA Certificate>SCEP window, enter the URL location of the CA.

■ URL field—Enter the URL of the CA's SCEP interface.

■ CA Descriptor field—Some CAs use descriptors to further identify the certificate. If your CA gave you a descriptor, enter it here. Otherwise enter a descriptor of your own. Most CAs require something in this field, something as simple as xxx. With a Microsoft CA, a non-descript entry is required.

■ Retrieve button—Click **Retrieve** to retrieve a CA certificate from the CA.

■ Cancel—Click **Cancel** to discard your entries and cancel the request.

Once the Retrieve button is clicked, the Concentrator sends a get CA message to the CA whose location is defined in the URL field. In turn, the CA returns a root certificate to the concentrator. Upon receipt of the root certificate, the Concentrator authenticates and installs the root certificate. The administrator can view the root certificate from the Administration>Certificate Management window.

## Root Installed



The Administration>Certificate Management window displays the root certificate in the Certificate Authorities section. Under the Certificate Authorities section, there are five columns:

■ Subject—A combination of both the Common Name and the Organization (O) from the root certificate.

■ Issuer—A combination of both the Common Name and the Organization (O) from the root certificate.

■ Expiration—The expiration date of the certificate.

■ SCEP Issuer—For an identity certificate to be available for SCEP enrollment, the root must first be installed via SCEP. This cell indicates if the certificate is SCEP-enabled:

  — Yes—This certificate can issue identity certificates via SCEP.

  — No—This certificate cannot issue identity certificates via SCEP. If you want to use a root certificate for SCEP enrollment, but that certificate is not SCEP-enabled, reinstall it using SCEP.

■ Actions—Enables you to manage particular certificates. The available actions vary with type and status of the certificate:

  — View—View details of this certificate.

— Configure—Enable CRL checking for this CA certificate, modify SCEP parameters, or enable acceptance of subordinate CA certificates.

— Delete—Delete this certificate from the Concentrator.

— SCEP—View or configure SCEP parameters for this certificate.

— Show RAs—SCEP-enabled CA certificates sometimes have supporting Registration Authority (RA) certificates.

— Hide RAs—Hide the details of the RA certificates.

**View the Root Certificate**

Administration | Certificate Management | View

**Subject**                              **Issuer**
CN=AUSTIN                                 CN=AUSTIN
OU=VSEC                                   OU=VSEC
O=TRAINING                               O=TRAINING
L=AUSTIN                                  L=AUSTIN
SP=TX                                     SP=TX
C=US                                      C=US

Serial Number 63F833F002E5E88845598082B73ED249
Signing Algorithm SHA1WithRSA
Public Key Type RSA (1024 bits)
Certificate Usage Digital Signature,Non Repudiation,Certificate Signature,CRL Signature
MD5 Thumbprint 38:5F:42:5E:C0:4F:CE:5A:2E:47:29:48:9C:4D:44:17
SHA1 Thumbprint 10:03:73:53:F5:48:F7:31:B4:23:40:29:C3:FD:F3:FB:8B:F4:8A:93
Validity 7/28/2003 at 17:29:38 to 7/29/2005 at 17:10:38
CRL Distribution Point http://austin/CertEnroll/AUSTIN(9).crl

CSVPN 4.0—17-13

You can view the root certificate from the Administration>Certificate Management> Certificates>View window. The root certificate contains the following information:

■ Subject—The system that uses the certificate, Austin. For a root certificate, the subject and issuer are the same.

■ Issuer—The CA that issued the certificate, Austin.

■ Serial Number—Identifies the certificate.

■ Signing Algorithm—The cryptographic algorithm that the CA or other issuer used to sign this certificate.

■ Public Key Type—The algorithm and size of the certified public key.

■ Certificate Usage—The purpose of the key contained in the certificate (for example, digital signature, certificate signing, non-repudiation, key or data encryption).

■ Thumbprint—A hash of the complete certificate contents. This value is unique for every certificate, and it positively identifies the certificate. If you question the authenticity of a root certificate, you can check this value with the issuer.

■ Validity Period—Just like credit cards, certificates are valid from the date of issue to the date of expiration. In the example in the figure, the certificate is valid from 2/23/00 to 2/23/02.

■ CRL Distribution Point—All CRL distribution points from the issuer of this certificate.

# Identity Certificate Installation

This topic explains how to install an identity certificate on the Concentrator via SCEP.
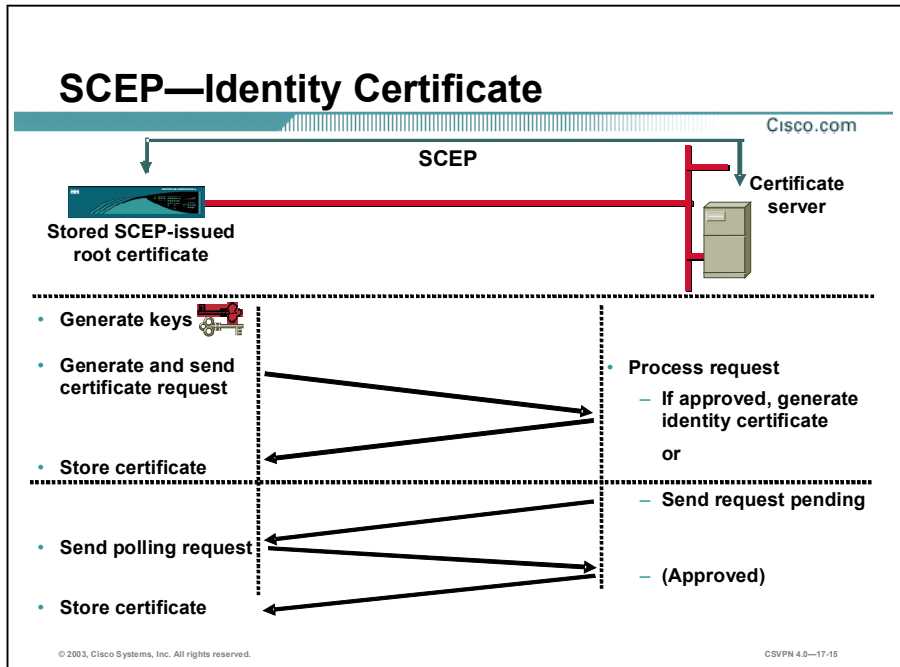


Before a Concentrator can start a PKI transaction, it first generates asymmetric key pairs, using the selected algorithm the Rivest, Shamir, and Adelman (RSA) algorithm is required in Simple Certificate Enrollment Protocol (SCEP). After generating a public and private key, the Concentrator starts an enrollment transaction. The Concentrator creates a certificate request using Public Key Cryptography Standard #10 (PKCS#10) and sends it to the CA enveloped using the PKCS#7. At the CA, the certificate request is processed, and hopefully approved, in one of two ways: automatically or manually. The two processes are as follows:

■ Automated approval process—After the CA receives the request, it automatically approves the request and sends the certificate back. In the automatic mode, the transaction consists of one PKCS Req PKI Message from the Concentrator, and one Cert Rep PKI message to the Concentrator.

■ Manual approval process—The CA requires the end Concentrator to wait until the CA administrator can manually authenticate the identity of the requesting end entity. In the manual mode, the Concentrator enters into polling mode by periodically sending GetCertInitial PKI message to the CA, until the CA administrator completes the manual authentication. After this, the CA will respond to GetCertInitial by returning the issued certificate.

# Identity Certificate Enrollment

Cisco.com

| Administration | Certificate Management | | | Wednesday, 30 July 2003 09:27:05 |
|---|---|---|---|---|
| | | | | Refresh |

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- Click here to enroll with a Certificate Authority
- Click here to install a certificate

**Certificate Authorities** [ View All CRL Caches | Clear All CRL Caches ] (current: 3, maximum: 6)

| Subject | Issuer | Expiration | SCEP Issuer | Actions |
|---|---|---|---|---|
| AUSTIN at TRAINING | AUSTIN at TRAINING | 07/29/2005 | Yes | View | Configure | Delete | SCEP | Show RAs |

**Identity Certificates** (current: 0, maximum: 2)

| Subject | Issuer | Expiration | Actions |
|---|---|---|---|
| No Identity Certificates | | | |

**SSL Certificate** [ Generate ] *Note: The public key in the SSL certificate is also used for the SSH host key.*

| Subject | Issuer | Expiration | Actions |
|---|---|---|---|
| 10.0.1.5 at Cisco Systems, Inc. | 10.0.1.5 at Cisco Systems, Inc. | 05/19/2006 | View | Renew | Delete |

**Enrollment Status** [ **Remove All:** Errored | Timed-Out | Rejected | Cancelled | In-Progress ] (current: 0 available: 3)

| Subject | Issuer | Date | Use | Reason | Method | Status | Actions |
|---|---|---|---|---|---|---|---|
| No Enrollment Requests | | | | | | | |

CSVPN 4.0—17-16

The first step of the process is to install a root certificate in the Concentrator via SCEP. In the example in the figure, the root certificate was issued via SCEP and installed on the Concentrator. The next step of the process is to install an identity certificate via SCEP. In the example in the figure, notice there is no identity certificate installed.

There are four steps to generate an identity certificate via SCEP:

**Step 1** Click the **Click here to enroll with a Certificate Authority** link in the Administration> Certificate Management window.

**Step 2** Click the **Identity certificate** link in the Administration>Certificate Management>Enroll window.

**Step 3** Click the **Enroll via SCEP at XXX at XXX** link (where XXX is the name of the SCEP issuing the CA) in the Administration>Certificate Management>Enroll>Identity Certificate window.

**Step 4** In the Administration>Certificate Management>Enroll>Identity Certificate>SCEP window, fill out the PKCS#10 enrollment form and click **Enroll**. There is further discussion of the PKCS#10 form later in this lesson.

   If the SCEP enrollment was successful, the Concentrator returns a SCEP status installed message.

# Identity Enrollment Form

Cisco.com

**Administration | Certificate Management | Enroll | Identity Certificate | SCEP**

Enter the information to be included in the certificate request. **Please wait for the operation to finish.**

| | | |
|---|---|---|
| Common Name (CN) | student1 | Enter the common name for the VPN 3000 Concentrator to be used in this PKI. |
| Organizational Unit (OU) | training | Enter the department. |
| Organization (O) | Cisco | Enter the Organization or company. |
| Locality (L) | Austin | Enter the city or town. |
| State/Province (SP) | Texas | Enter the State or Province. |
| Country (C) | US | Enter the two-letter country abbreviation (e.g. United States = US). |
| Subject AlternativeName (FQDN) | | Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI. |
| Subject AlternativeName (E-Mail Address) | | Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI. |
| Challenge Password | | Enter and verify the challenge password for this certificate request. |
| Verify Challenge Password | | |
| Key Size | RSA 512 bits | Select the key size for the generated RSA key pair. |

Enroll    Cancel

CSVPN 4.0—17-18

Part of the enrollment process is to fill out an enrollment request form. The following are the enrollment request fields:

■ Common Name (CN) field—The primary identity of the entity associated with the certificate.

■ Organizational Unit (OU) field—The name of the department or other organizational unit. It must match the group name configured in the destination Concentrator.

■ Organization (O) field—The name of the company or organization.

■ Locality (L) field—The city or town where this Concentrator is located.

■ State/Province (S/P) field—The state or province where this Concentrator is located.

■ Country (C) field—The country where this Concentrator is located (for example, US). Use two characters, no spaces, and no periods.

■ Subject Alternative Name (FQDN) field—The fully qualified domain name that identifies this Concentrator in this PKI (for example, vpn3030.cisco.com). This field is optional. The alternative name is an additional data field in the certificate that provides interoperability with many Cisco IOS and PIX Firewall systems in LAN-to-LAN connections.

■ Subject Alternative Name (E-Mail Address) field—The e-mail address of the Concentrator administrator.

- Challenge Password field—This field appears if you are requesting a certificate using SCEP. Use this field according to the policy of your CA:

  — Your CA might have given you a password. If so, enter it here in order to be authenticated.

  — Your CA might allow you to provide your own password to use to identify yourself to the CA in the future. If so, create your password here.

  — Your CA might not require a password. If so, leave this field blank.Verify Challenge Password field—Re-enter the challenge password.

- Key Size drop-down menu—The algorithm for generating the public and private key pair and the key size. The following options are available:

  — RSA 512 bits—Generates 512-bit key using the RSA (Rivest, Shamir, Adelman) algorithm. This key size provides sufficient security and is the default selection. It is most common, and requires the least processing.

  — RSA 768 bits—Generates 768-bit key using the RSA algorithm. This key size provides normal security. It requires approximately 2 to 4 times more processing than the 512-bit key.

  — RSA 1024 bits—Generates 1024-bit key using the RSA algorithm. This key size provides high security. It requires approximately 4 to 8 times more processing than the 512-bit key.

# Identity Certificate Installed

**Administration | Certificate Management**  Wednesday, 30 July 2003 10:20:49
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- Click here to enroll with a Certificate Authority
- Click here to install a certificate

**Certificate Authorities** [ View All CRL Caches | Clear All CRL Caches ] (current: 3, maximum: 6)

| Subject | Issuer | Expiration | SCEP Issuer | Actions |
|---|---|---|---|---|
| AUSTIN at TRAINING | AUSTIN at TRAINING | 07/29/2005 | Yes | View | Configure | Delete | SCEP | Show RAs |

**Identity Certificates** (current: 1, maximum: 2)

| Subject | Issuer | Expiration | Actions |
|---|---|---|---|
| student1 at Cisco | AUSTIN at TRAINING | 07/29/2004 | View | Renew | Delete |

**SSL Certificate** [ Generate ] *Note: The public key in the SSL certificate is also used for the SSH host key.*

| Subject | Issuer | Expiration | Actions |
|---|---|---|---|
| 10.0.1.5 at Cisco Systems, Inc. | 10.0.1.5 at Cisco Systems, Inc. | 05/19/2006 | View | Renew | Delete |

**Enrollment Status** [ **Remove All:** Errored | Timed-Out | Rejected | Cancelled | In-Progress ] (current: 0 available: 2)

| Subject | Issuer | Date | Use | Reason | Method | Status | Actions |
|---|---|---|---|---|---|---|---|
| No Enrollment Requests | | | | | | | |

CSVPN 4.0—17-19

After you fill out the enrollment request form and click enroll, an identity certificate is loaded on the Concentrator. Choose the **Administration>Certificate Management** window to view the identity certificate. The identity certificate entry columns are as follows:

- Subject—A combination of the Common Name (CN) or Organizational Unit (OU), if present, and the Organization (O) in the Subject column of the certificate.

- Issuer—A combination of both the Common Name (CN) or Organizational Unit (OU), if present, and the Organization (O) in the Issuer column of the certificate.

- Expiration—The expiration date of the certificate.

- Actions—This column enables you to manage particular certificates. The actions available vary by the type and status of the certificate:

  — View—View this certificate.

  — Renew—A shortcut that enables you to generate an enrollment request based on the content of an existing certificate.

  — Delete—Delete this certificate from the Concentrator.

## View the Identity Certificate

Cisco.com

Administration | Certificate Management | View

→ **Subject**
CN=student1
OU=training
O=Cisco
L=Austin
SP=Texas
C=US

→ **Issuer**
CN=AUSTIN
OU=VSEC
O=TRAINING
L=AUSTIN
SP=TX
C=US

→ **Serial Number** 03F42112000A00000062
**Signing Algorithm** SHA1WithRSA
**Public Key Type** RSA (512 bits)
**MD5 Thumbprint** FB:90:6E:83:95:11:C9:65:C1:A7:8B:0B:74:68:E9:0F
**SHA1 Thumbprint** 61:00:73:BD:3F:42:3A:DC:CE:45:A7:54:F4:0A:72:3F:D1:6E:FF:67
→ **Validity** 7/29/2003 at 12:09:51 to 7/29/2004 at 12:19:51
**CRL Distribution Point** http://austin/CertEnroll/AUSTIN(9).crl

CSVPN 4.0—17-20

You can view the identity certificate from the Administration>Certificate Management> Certificates>View window. The identity certificate contains the following information:

■ Issuer—The CA that issued the certificate.

■ Subject—File name of the identity certificate.

■ Serial Number—Identifies the certificate.

■ Signing Algorithm—The cryptographic algorithm that the CA or other issuer used to sign this certificate.

■ Public Key Type—The algorithm and size of the certified public key.

■ Thumbprint—A hash of the complete certificate contents. This value is unique for every certificate, and it positively identifies the certificate. If you question the authenticity of a root certificate, you can check this value with the issuer.

■ Validity Period—Just like credit cards, certificates are valid from the date of issue to the date of expiration. In the example in the figure, the certificate is valid from 2/25/00 to 2/25/01.

■ CRL Distribution Point—All CRL distribution points from the issuer of this certificate.

## Enrollment Status

Cisco.com

The enrollment status table tracks the status of active enrollment requests. The different parts of the enrollment status table are as follows:

- Subject column—A combination of the Common Name (CN) or Organizational Unit (OU), if present, and the Organization (O) in the Subject column of the certificate.

- Issuer column—A combination of the Common Name (CN) or Organizational Unit (OU), if present, and the Organization (O) in the Subject column of the certificate.

- Date column—Date the enrollment request was issued.

- Use column—Identity or SSL.

- Reason column—Initial, re-enrollment, or re-key.

- Method column—SCEP or manual.

- Status column—Shows the status of the recent enrollment requests.

  - Errored link—An internal error occurred during the enrollment process; therefore, enrollment was stopped.

  - Timed Out link—The SCEP polling cycle has ended after reaching the configured maximum number of retries. This value is used only for enrollment requests created using SCEP.

— Rejected link—The CA refused to issue the certificate. This value is used only for enrollment requests created using SCEP.

— Cancelled link—The certificate request was cancelled while the Concentrator was in polling mode.

■ In-Progress link—The request has been created, but the requested certificate has not yet been installed. This value is used only for PKCS#10 (manual) enrollment requests.

■ Actions column—Enables you to manage enrollments requests:

— View link—View details of this enrollment request.

— Resubmit link—Reinitiate SCEP communications with the CA or RA using the previously entered request information.

— Delete link—Delete an enrollment request from the Concentrator.

# Certificate Renewal

**Administration | Certificate Management | Renewal**

This section allows you to re-enroll or re-key a certificate, so that the VPN 3000 Concentrator updates its certificate. The certificate request can be sent to a CA, which in turn, sends back a certificate. **Please wait for the operation to finish.**

| | |
|---|---|
| **Certificate** | SSL Certificate |
| **Renewal Type** | ⦿ Re-enrollment ○ Re-key — Select the type of renewal. A *re-enrollment* uses the same key for the certificate. A *re-key* generates a new key for the certificate. |
| **Enrollment Method** | AUSTIN at TRAINING via SCEP ▾ — Select the renewal method for this certificate. |
| **Challenge Password** | |
| **Verify Challenge Password** | Enter and verify the challenge password for this certificate request. |

[Renew] [Cancel]

CSVPN 4.0—17-22

SCEP does not provide for an automatic certificate renewal process. Approximately one month before a certificate expires, the Concentrator alerts you with an event message. It is up to you to renew the certificate. Certificate renewal is a shortcut that enables you to generate an enrollment request based on the content of an existing certificate. When you renew a certificate via SCEP, the new certificate does not automatically overwrite the original certificate. It remains in the Enrollment Request table until the administrator manually activates it. The different parts of the Renewal window are as follows:

■ Certificate field—Displays the type of certificate that you are re-enrolling or re-keying.

■ Renewal Type radio buttons—Specifies the type of request:

— Re-enrollment radio button—Use the same key pair as the expiring certificate.

— Re-key radio button—Use a new key pair as the expiring certificate.

■ Enrollment Method drop-down menu—Choose an enrollment method:

— PKCS10 Request (Manual)—Enroll using the manual process.

— [certificate name] via SCEP—Enroll automatically using this SCEP CA.

■ Challenge Password field—Your CA might have given you a password as a means of verifying your identity. If you have a password from your CA, enter it here.

■ Verify Challenge Password field—Enter the challenge password here.

# Configuring Certificate Authority

Cisco.com

**Certificate Authorities** [ View All CRL Caches | Clear All CRL Caches ] (current: 3, maximum: 6)

| Subject | Issuer | Expiration | SCEP Issuer | Actions |
|---|---|---|---|---|
| AUSTIN at TRAINING | AUSTIN at TRAINING | 07/29/2005 | Yes | View | Configure | Delete | SCEP | Show RAs |

**CRL retrieval policy**

**CRL caching**

**CRL distribution points**

There are three sections to the Administration>Certificate Management>Configure CA Certificate window: CRL retrieval policy, CRL caching, and CRL-distribution points (CRL-DPs). Enabling CRL checking means that every time the Concentrator uses the certificate for authentication, it also checks the latest CRL to ensure that the certificate has not been revoked. CRL retrieval policy defines where to find the CRL-DP location. The choices are as follows: on a CA certificate, statically defined on the Concentrator, a combination of both, or disable CRL checking.

The next section is CRL caching. Since the Concentrator has to fetch and examine the CRL from a network-based DP, CRL checking might slow system response times or cause the tunnel to fail due to Internet Key Exchange (IKE) timeout issues. Enable CRL caching to mitigate these potential problems. CRL caching stores the retrieved CRLs in local volatile memory. This enables the Concentrator to verify the revocation status of certificates more quickly.

The last section is configuring the location of CRL-DPs. CAs provide CRLs through network-based DPs, or CRL-DPs. Many certificates include the location of theses CRL-DPs. If the CRL-DP is present in the certificate and in the proper format, you need not configure any CRL-DP fields in this window. If a CRL-DP is not present or you choose to define additional CRL-DPs, define the CRL-DP addresses in the Static CRL-DP window.

**Concentrator SCEP Configuration**

To configure or modify the SCEP parameters, choose the **Administration>Certificate Management** window and select **SCEP** under the Certificate Authorities actions column. The Administration>Certificate Management>Configure SCEP window opens. The administrator can set the SCEP polling parameters or modify the SCEP URL information from the Administration>Certificate Management>Configure SCEP window.

If the CA does not issue the certificate immediately (some CAs require manual verification of credentials and this can take time), the certificate request could enter pending mode. In pending mode, the Concentrator polls the CA a specified number of times at regular intervals until the CA responds or the process times out. The following options govern the polling application:

■ Enrollment URL field—Enter the URL where the Concentrator should send SCEP enrollment requests. The default value of this field is the URL used to download this CA certificate.

■ Polling Interval field—If the CA does not issue the certificate immediately, the certificate request could enter polling mode. Enter the number of minutes the Concentrator should wait between re-sends. The minimum number of minutes is 1; the maximum number of minutes is 60, and the default value is 1.

■ Polling Limit field—Enter the number of times the Concentrator should re-send an enrollment request if the CA does not issue the certificate immediately. The minimum number of re-sends is 0; the maximum number is 100. If you do not want any polling limit (in other words you want infinite re-sends), enter **none**.

**Activate the IKE Proposal**

Cisco.com

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate.
Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.
Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by Security Associations to specify IKE parameters.

| Active Proposals | Actions | Inactive Proposals |
|---|---|---|
| CiscoVPNClient-3DES-MD5 | << Activate | IKE-3DES-SHA-DSA |
| CiscoVPNClient-3DES-MD5-RSA | Deactivate >> | IKE-3DES-MD5-RSA-DH1 |
| IKE-3DES-MD5 | Move Up | IKE-DES-MD5-DH7 |
| IKE-3DES-MD5-DH1 | | CiscoVPNClient-3DES-SHA-DSA |
| IKE-DES-MD5 | Move Down | CiscoVPNClient-3DES-MD5-RSA-DH5 |
| IKE-3DES-MD5-DH7 | Add | CiscoVPNClient-3DES-SHA-DSA-DH5 |
| IKE-3DES-MD5-RSA | | CiscoVPNClient-AES256-SHA |
| CiscoVPNClient-3DES-MD5-DH5 | Modify | IKE-AES256-SHA |
| CiscoVPNClient-AES128-SHA | Copy | |
| IKE-AES128-SHA | Delete | |

CSVPN 4.0—17-25

You must check the following three items before the LAN-to-LAN with digital certificates tunnel can be configured:

■ Active Internet Key Exchange (IKE) proposal list

■ IKE proposal

■ Security Association (SA)

Check the Active Proposals list. By default, an RSA proposal should be present. The Concentrator requires the use of a RSA IKE proposal for LAN-to-LAN with digital certificates to work.

**IKE Proposal**

Cisco.com

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify

Modify a configured IKE Proposal.

| | | |
|---|---|---|
| Proposal Name | IKE-3DES-MD5-RSA | Specify the name of this IKE Proposal. |
| Authentication Mode | RSA Digital Certificate | Select the authentication mode to use. |
| Authentication Algorithm | MD5/HMAC-128 | Select the packet authentication algorithm to use. |
| Encryption Algorithm | 3DES-168 | Select the encryption algorithm to use. |
| Diffie-Hellman Group | Group 2 (1024-bits) | Select the Diffie Hellman Group to use. |
| Lifetime Measurement | Time | Select the lifetime measurement of the IKE keys. |
| Data Lifetime | 10000 | Specify the data lifetime in kilobytes (KB). |
| Time Lifetime | 86400 | Specify the time lifetime in seconds. |

Apply    Cancel

CSVPN 4.0—17-26

Check the activated RSA Internet Key Exchange (IKE) proposal to ensure that it meets the authentication, encryption, Diffie-Hellman (DH), and lifetime requirements. In the example in the figure, the RSA IKE proposal supports the following:

■ Authentication mode—RSA digital certificates

■ Authentication algorithm—Message Digest 5 (MD5)

■ Encryption algorithm—Triple-Data Encryption Standard (3DES)

■ DH group—DH group 2

■ Key length and lifetime—Time and 86400 seconds

# Add RSA SA

**Configuration | Policy Management | Traffic Management | Security Associations**

Save 🖫

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IKE Proposals to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

**IPSec SAs**          **Actions**

| ESP-3DES-MD5 |
| ESP-3DES-MD5-DH5 |
| ESP-3DES-MD5-DH7 |
| ESP-3DES-NONE |
| ESP-AES128-SHA |
| ESP-DES-MD5 |
| ESP-L2TP-TRANSPORT |
| ESP/IKE-3DES-MD5 |
| L2L: pod1 |

Add

Modify

Delete

CSVPN 4.0—17-27

Select the Security Association (SA). The SA is a template that defines IPSec and IKE attributes. There are two choices: modify an existing SA or add a new one. If you modify an existing SA, you change it from pre-shared keys (the default) to Rivest, Shamir, and Adelman (RSA)-signed digital certificates. By changing it, you may enable the LAN-to-LAN with digital certificates tunnels, but disable the use of pre-shared keys for someone else. The best option is to add an SA. Click **Add** to do this.

**Configure RSA SA**

Configuration | Policy Management | Traffic Management | Security Associations | Add

Configure and add a new Security Association.

SA Name [RSA 3DES MD5]  Specify the name of this Security Association (SA).
Inheritance [From Rule ▾]  Select the granularity of this SA.

**IPSec Parameters**
Authentication Algorithm [ESP/MD5/HMAC-128 ▾]  Select the packet authentication algorithm to use.
Encryption Algorithm [3DES-168 ▾]  Select the ESP packet encryption algorithm to use.
Encapsulation Mode [Tunnel ▾]  Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy [Disabled ▾]  Select the use of Perfect Forward Secrecy.
Lifetime Measurement [Time ▾]  Select the lifetime measurement of the IPSec keys.
Data Lifetime [10000]  Specify the data lifetime in kilobytes (KB).
Time Lifetime [28800]  Specify the time lifetime in seconds.

**IKE Parameters**
IKE Peer [0.0.0.0]  Specify the IKE Peer for a LAN-to-LAN connection.
Negotiation Mode [Main ▾]  Select the IKE Negotiation mode to use.
Digital Certificate [student1kc ▾]  Select the Digital Certificate to use.
Certificate Transmission ○ Entire certificate chain  Choose how to send the digital certificate to the IKE peer.
                         ○ Identity certificate only
IKE Proposal [IKE-3DES-MD5-RSA ▾]  Select the IKE Proposal to use as IKE initiator.

[Add]  [Cancel]

CSVPN 4.0—17-28

The Configuration>Policy Management>Traffic Management>Security Associations window has two sections: IPSec Parameters and IKE Parameters. In the IPSec parameter section, verify the authentication, encryption, DH, and lifetime parameters. In the example in the figure, the IPSec proposal supports the following:

■ Authentication algorithm—MD5

■ Encryption algorithm—3DES

■ Encapsulation mode—Tunnel

■ Diffie-Hellman group—DH group 2

■ Key length and lifetime—Time and 86400 seconds

In the IKE parameter section, choose which IKE parameters are to be applied to this Security Association (SA). Complete the following to do this:

**Step 1**  Choose **IKE-3DES-MD5-RSA** from the IKE proposal drop-down menu.

**Step 2**  Choose the correct certificate from the Digital Certificate drop-down menu. In the example in the figure, the student1 certificate was chosen. This certificate is used during the certificate exchange.

**Step 3**  Click **Add**.

**Add IPSec LAN-to-LAN**

Cisco.com

The Concentrator provides a wizard for LAN-to-LAN connections. It is found in the Configuration>System>Tunneling Protocols>IPSec LAN-to-LAN window. Click **Add** to access the wizard.

**Boston IPSec LAN-to-LAN**

Cisco.com

Boston
10.0.1.0
255.255.255.0

Houston
10.0.6.0
255.255.255.0

192.168.1.5

192.168.6.5

CSVPN 4.0—17-30

The LAN-to-LAN wizard is divided into three sections. The top section provides Concentrator-to-Concentrator parameters. The middle section defines attributes at the local private network, while the bottom section deals with the remote private network.

In the top section, there are four parameters that must be defined:

- Name field—Enter a unique descriptive name for this connection.

- Peer field—Enter the IP address of the remote peer in the LAN-to-LAN connection. This must be the IP address of the public interface on the peer VPN Concentrator.

- Digital Certificate drop-down menu—Click the drop-down menu button and choose from a list of installed digital certificates.

- IKE Proposal drop-down menu—Specifies the set of attributes for Phase 1 IPSec negotiations, which are known as IKE proposals. You already activated the digital certificate IKE proposals before configuring LAN-to-LAN connections. Click the drop-down menu button and choose the **IKE-3DES-MD5-RSA** proposal. The list shows only active IKE proposals.

The middle and bottom sections define the addresses of the local and remote private networks. The term defined refers to the network address on the private interface of the Concentrator, not the host address. The local IP address is 10.0.1.0. Next is the wildcard mask, which is the opposite of a subnet mask (for example, the wildcard mask for 255.255.255.0 is 0.0.0.255).

IPSec LAN-to-LAN Is Finished
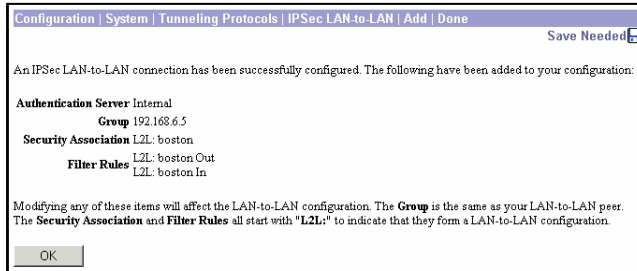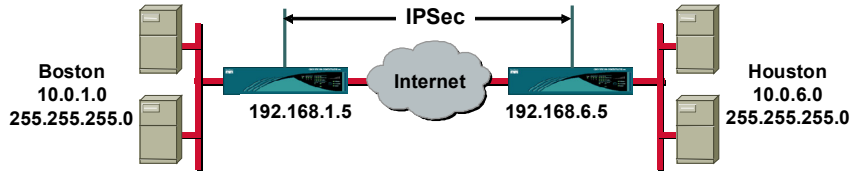
The window in the figure is a synopsis of the tunnel attributes defined by the wizard to include group, SA, and filter parameters. For more in-depth information, go to each record individually. Where appropriate, the parameters can be edited.

## IPSec LAN-to-LAN Connection

Cisco.com

**Boston**
10.0.1.0
255.255.255.0

IPSec

Internet

192.168.1.5

192.168.6.5

**Houston**
10.0.6.0
255.255.255.0

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN

Save Needed

This section lets you configure IPSec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPSec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to User Management and configure a Group and User. To configure NAT over LAN-to-LAN, go to LAN-to-LAN NAT Rules.

If you want to define a set of networks on the local or remote side of the LAN-to-LAN connection, configure the necessary Network Lists prior to creating the connection.

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

(D) indicates a disabled LAN-to-LAN connection.

LAN-to-LAN
Connection                                    Actions

Boston (192.168.6.5) on Ethernet 2 (Public)

Add

Modify

Delete

CSVPN 4.0—17-32

When finished, the new tunnel is defined as Boston (192.168.6.5) on Ethernet 2 (Public). Boston is the name of the tunnel. 192.168.6.5 is the public interface of the remote Concentrator. Ethernet 2 (Public) is the local termination point of the tunnel.

There are two ends to every tunnel. The local end was defined earlier. The remote end needs to be defined. At the remote end, click **Add** and define the remote end LAN-to-LAN wizard.

# Summary

This topic summarizes the tasks you learned to complete in this lesson.

## Summary

Cisco.com

- SCEP certificate generation is a two-step process:
  - CA certificate requests are sent to and CA certificates are received from the CA.
  - Identity certificate requests are sent to and identity certificates are received from the CA.
- CA and identity certificates are validated before being loaded on a Concentrator.
- For CA support you configure the Concentrator much the same as you would for pre-shared keys, substituting the digital certificates when necessary.
- Add, verify, and delete certificates in the Administration-Certificate Management window.

CSVPN 4.0—17-34

# Lab Exercise—Configure Cisco VPN 3000 Series Concentrators for LAN-to-LAN Using Digital Certificates

Complete the following lab exercise to practice what you learned in this lesson.

## Objectives

Your task in this lab exercise is to configure one end of a LAN-to-LAN Virtual Private Network (VPN) while another team completes the same tasks at a remote site. Work with your lab partner to complete the following tasks on your side of the LAN-to-LAN VPN:

■ Complete the lab exercise setup.

■ Delete the Cisco VPN 3000 Series Concentrator pre-existing PKCS#10 requests.

■ Delete the Cisco VPN 3000 Series Concentrator pre-existing identity and root certificates.

■ Generate a new root certificate via SCEP.

■ Generate a new identity certificate via SCEP.

■ Verify the Cisco VPN 3000 Series Concentrator IKE proposal.

■ Modify the Cisco VPN 3000 Series Concentrator SAs.

■ Verify the Cisco VPN 3000 Series Concentrator IPSec LAN-to-LAN parameters.

■ Drop the IPSec LAN-to-LAN tunnel.

■ Monitor Cisco VPN 3000 Series Concentrator events.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



**Lab Visual Objective**
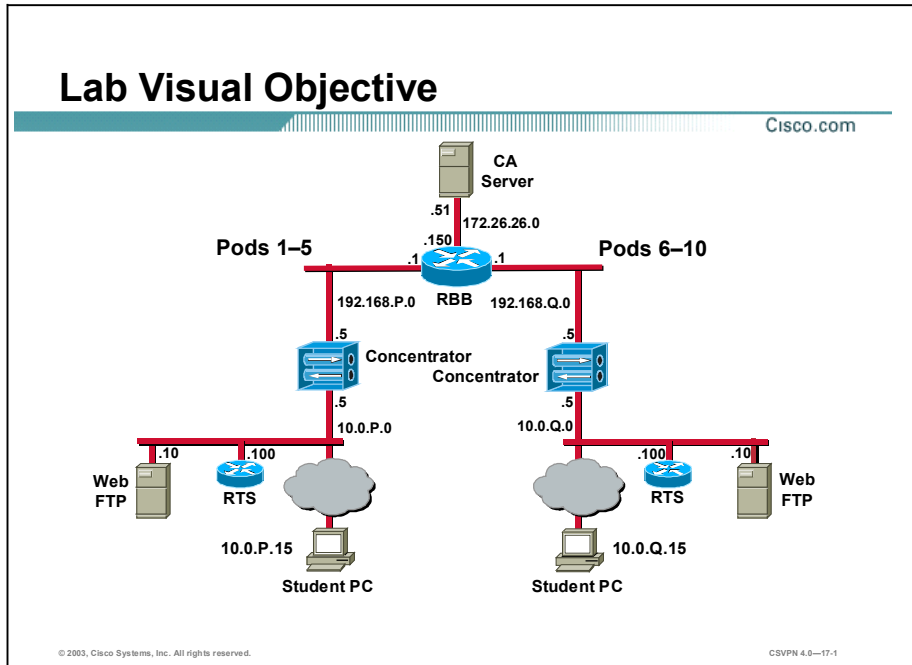
## Scenario

Your company wants you to implement a VPN between the world headquarters campus site and the remote sales offices. You must configure the Cisco VPN 3000 Series Concentrators for LAN-to-LAN tunneling using digital certificates for authentication.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment is setup as follows:

■ Ensure that your student PC is powered on.

■ Ensure your student PC IP addresses are configured correctly:

— Primary IP address—10.0.P.15
(where P = pod number)

— Default gateway IP address—10.0.P.5
(where P = pod number)

■ Ensure that your Concentrator is powered on.

## Task 2—Delete the Cisco VPN 3000 Series Concentrator Pre-Existing PKCS#10 Requests

Complete the following steps to ensure that all previous certificate requests are removed from the Concentrator:

**Step 1**   Launch Internet Explorer by double-clicking the desktop icon.

**Step 2**   Enter a Concentrator private interface IP address of **10.0.P.5** in the Internet Explorer Address field (where P = pod number). Internet Explorer connects to the Cisco VPN 3000 Concentrator Series Manager.

**Step 3**   Log into the Cisco VPN 3000 Concentrator Series Manager using the administrator account:

```
Login: admin
Password: admin
```

The username (login) and password are always case sensitive.

**Step 4**   From the Administration menu tree, drill down to **File Management**.

**Step 5**   Locate any existing PKCSN.TXT files and click **Delete**. Click **OK**, in the Are you sure you want to delete PKCSN.TXT message box.

(where N = any number)

**Step 6**   Do not log out of the Concentrator.

---

| **Warning** | Delete only those files named PKCSN.TXT (where N = any number string). Deleting any other listed files may result in unpredictable operation of the Concentrator. |

---

## Task 3—Delete the Cisco VPN 3000 Series Concentrator Pre-Existing Identity and Root Certificates

Complete the following steps to ensure that all previous certificates are removed from the Concentrator:

**Step 1**   From the Administration menu tree, drill down to **Certificate Management**.

**Step 2**   Under the Identity Certificates section, locate any existing identity certificates. Complete the following sub-steps to delete any existing identity certificate:

1.   Click **Delete** under the Identity Certificates actions column.

2.   Click **Yes** when you are asked if you are sure you want to delete this certificate.

**Step 3**   Locate any existing root certificate under the Certificate Authorities section.

**Step 4**   Complete the following sub-steps to delete any existing root certificates:

1.   Click **Delete** under the Certificate Authorities actions column.

2.   Click **Yes** when you are asked if you are sure you want to delete this certificate.

## Task 4—Generate a New Root Certificate via SCEP

Complete the following steps to create a new root certificate using Simple Certificate Enrollment Protocol (SCEP):

**Step 1** From the Administration menu tree, drill down to **Certificate Management**. The Administration>Certificate Management window opens.

**Step 2** Select **Click here to install a CA certificate**. The Administration>Certificate Management> Install>CA Certificate window opens.

**Step 3** Select **SCEP (Simple Certificate Enrollment Protocol)**. The Administration>Certificate Management>Install>CA Certificate>SCEP window opens.

**Step 4** Enter the CA information in the URL field as follows: **http://172.26.26.51/certsrv/mscep/mscep.dll**

**Step 5** Enter **99** in the CA Descriptor field.

**Step 6** Click **Retrieve**. It may take several moments for the certificate to be retrieved. The Administration>Certificate Management window opens. The new root certificate should be present and the value in the SCEP Issuer field should be Yes.

**Step 7** Choose the Certificate Authorities section and click **View**.

**Step 8** Answer the following questions under the Actions column:

Q1)    Under Subject, what is CN?

   A)    _____

Q2)    Under Issuer, what is CN?

   A)    _____

Q3)    What is the signing algorithm?

   A)    _____

Q4)    What is the public key type?

   A)    _____

Q5)    What is the validity period?

   A)    From _____
   B)    To _____

**Step 9** Click **Back**.

## Task 5—Generate a New Identity Certificate via SCEP

Complete the following steps to create a new identity certificate using SCEP:

**Step 1** From the Administration menu tree, drill down to **Certificate Management**. The Administration>Certificate Management window opens.

**Step 2**    Select **Click here to enroll with a Certificate Authority**. The Administration> Certificate Management>Enroll window opens.

**Step 3**    Select **Identity certificate**. The Administration>Certificate Management>Enroll> Identity Certificate window opens.

**Step 4**    Select **Enroll via SCEP at XXXX** (where XXXX = name of the CA authority). The Administration>Certificate Management>Enroll>Identity Certificate>SCEP window opens.

**Step 5**    Complete the following sub-steps to fill out the CA enrollment:

1.  Enter a common name: **studentPX**.
    (where P = pod number, and X = your first and last initials)

2.  Enter an organizational unit: **training**. (The Concentrator uses this as the group password. This parameter must match end-to-end.)

3.  Enter an organization: **Cisco**.

4.  Leave the rest of the empty fields blank.

5.  Choose a key size: **RSA 512 bits**.

6.  Click **Enroll**. It may take several moments for the SCEP enrollment to finish. When successfully completed, a SCEP status installed message opens.

7.  Click **Go To Certificate Management**. The Administration>Certificate Management window opens.

**Step 6**    Go to the Identity Certificates section and click **View** under the Actions column.

**Step 7**    Answer the following questions:

Q6)    Under Subject, what is CN?

    A)    _____

Q7)    Under Issuer, what is CN?

    A)    _____

Q8)    What is the signing algorithm?

    A)    _____

Q9)    What is the public key type?

    A)    _____

Q10)    What is the validity period?

    A)    From _____
    B)    To _____

**Step 8**    Click **Back**.

## Task 6—Verify the Cisco VPN 3000 Series Concentrator IKE Proposal

Complete the following steps to verify an Internet Key Exchange (IKE) proposal is active:

**Step 1** From the Configuration menu tree, drill down to **System>Tunneling Protocols> IPSec>IKE Proposals**.

**Step 2** Verify the **IKE-3DES-MD5-RSA** proposal in the Active Proposals list.

**Step 3** Choose the **IKE-3DES-MD5-RSA** proposal from the Active Proposals list.

**Step 4** Select **Modify** and complete the following sub-steps:

1. Verify that the Authentication Mode is set to **RSA Digital Certificate**.

2. Verify that the Authentication Algorithm is set to **MD5/HMAC-128**.

3. Verify that the Encryption Algorithm is set to **3DES-168**.

4. Verify that the Diffie-Hellman Group is set to **Group2 (1024-bits)**.

**Step 5** Click **Cancel**.

## Task 7—Modify the Cisco VPN 3000 Series Concentrator SAs

Security Associations (SA) define the IKE and IPSec parameters that are negotiated when the IPSec LAN-to-LAN tunnel is established. Because you are migrating from a pre-shared key exchange to a digital certificate exchange, a digital certificate IKE template needs to be applied to the negotiation. Complete the following steps:

**Step 1** From the Configuration menu tree, drill down to **Policy Management>Traffic Management> SAs**.

**Step 2** Select the **L2L:podP** SA and click **Modify**. The Modify window opens.

(where P = pod number)

**Step 3** From the digital certificate drop-down menu, choose **studentPX**.

(where P = pod number, and X = your first and last initials)

**Step 4** From the IKE Proposal drop-down menu, choose **IKE-3DES-MD5-RSA**.

**Step 5** Click **Apply**.

**Step 6** Save the configuration changes.

## Task 8—Verify the Cisco VPN 3000 Series Concentrator IPSec LAN-to-LAN Parameters

Complete the following steps to verify the IPSec LAN-to-LAN group parameters:

**Step 1** From the Configuration menu tree, drill down to **System>Tunneling Protocols> IPSec>LAN-to-LAN**.

**Step 2** Select **podP**.

(where P = pod number)

**Step 3**    Click **Modify**.

**Step 4**    Verify the digital certificate: **studentPX**.

(where P = pod number, and X = your first and last initials)

**Step 5**    Verify the IKE proposal: **IKE-3DES-MD5-RSA**.

**Step 6**    Click **Apply**.

**Step 7**    Save the configuration changes. Wait for the remote end to reach this point before continuing.

## Task 9—Drop the IPSec LAN-to-LAN Tunnel

Complete the following steps to disconnect the LAN-to-LAN tunnel session:

**Step 1**    From the Administration menu tree, drill down to **Administer Sessions**.

**Step 2**    Choose the LAN-to-LAN Sessions section.

**Step 3**    If a LAN-to-LAN session exists, click **Logout** to disconnect the tunnel.

**Step 4**    Wait a few seconds and click **Refresh**. The LAN-to-LAN tunnel should re-establish a connection. If it does not, ping your peer's PC.

## Task 10—Monitor Cisco VPN 3000 Series Concentrator Events

Complete the following steps to complete an in-depth examination of the IKE and Certificate (CERT) event messages:

**Step 1**    From the Configuration menu tree, drill down to **System>Events>Classes**.

**Step 2**    Click **Add**. The Classes>Add window opens.

**Step 3**    Enable logging for the IKEDECODE event class by completing the following sub-steps:

1.  Select a class name: **IKEDECODE**.

2.  Set the Events to Log: **1–13**.

3.  Leave all other fields at their default values.

4.  Click **Add**. The Classes>Add window opens.

**Step 4**    Enable logging for the CERT event class by completing the following sub-steps:

1.  Click **Add**.

2.  Select a class name: **CERT**.

3.  Set the Events to Log: **1–13**.

4.  Leave all other fields at their default values.

5.  Click **Add**. The Classes>Add window opens.

**Step 5**    From the Monitoring menu tree, drill down to **Filterable Event Log**.

**Step 6**    Click **Clear Log**.

**Step 7**    From the Administration menu tree, drill down to **Administer Sessions**.

**Step 8**  Disconnect and re-establish the LAN-to-LAN tunnel to view the events generated by completing the following sub-steps:

1.  Choose the **LAN-to-LAN Sessions** section and select **Logout**.

2.  Wait a few seconds and click **Refresh**. The LAN-to-LAN tunnel should re-establish itself. If it does not, ping your peer's PC.

**Step 9**  From the Monitoring menu tree, drill down to **Filterable Event Log** and complete the following sub-steps:

1.  In the Event Class group box, scroll down and select **IKEDECODE**.

2.  While holding down the **Ctrl** key on your PC, select **CERT**.

3.  In the Events/Page combo window, select **ALL**.

4.  Click |<<.

**Step 10**  Scroll through the event messages.

**Step 11**  View the event shown and answer the following question:

```
127 03/01/2000 09:41:23.510 SEV=8 IKEDECODE/0 RPT=305
Phase 1 SA Attribute Decode for Transform # 1:

Encryption Alg:     Triple-DES (5)
Hash Alg     :      MD5 (1)
Group        :      Oakley Group 1 (1)
Auth Method  :      RSA signature with Certificates (3)
Life Time    :      86400 seconds
```

Q11)  What is the authentication method for this IKE tunnel?

A)  _____

**Step 12**  View the event shown and answer the following questions:

```
DER_ASN1_DN ID received, len 58
0000: 3038310E 300C0603 55040A13 05636973     081.0...U....cis
0010: 636F3111 300F0603 55040B13 08747261     co1.0...U....tra
0020: 696E696E 67311330 11060355 0403130A     ining1.0...U....
0030: 73747564 656E7431 6265                  student1be
```

Q12)  What is the company name?

A)  _____

Q13)  What is the organizational unit?

A)  _____

Q14)  The organizational unit name must match what name on the Concentrator?

A)  _____ name

**Step 13**  View the events shown and answer the following question:

```
235 03/01/2000 09:41:23.680 SEV=7 CERT/1 RPT=10
Certificate is valid: session = 35
```

Q15)   Is the certificate valid?

A)   _____

**Step 14**   Log out of the Concentrator.

**Step 15**   Close Internet Explorer.

**18**

# Using Cisco VPN 3000 Concentrator v4.7

## Overview

Organizations are increasingly expected to provide access to the corporate network to a diverse mix of users. Employees working at remote locations need secure access to the corporate network from any non-corporate or public owned system. There can also be situations when these users need access without having preinstalled VPN software, which is not a secure method. In addition, the users can require access from a system with simple configuration and Internet connectivity. Therefore, to extend secure access to this diverse mix of users, organizations need to provide secure connectivity from a Web browser.

The Cisco VPN 3000 Concentrator running version 4.7 provides a robust VPN infrastructure and a unique remote-access architecture that supports remote-access application requirements of organizations. The Cisco SSL VPN Client and Cisco Secure Desktop features in Cisco VPN 3000 Concentrator v4.7 deliver extensive application access, endpoint security, data integrity protection, infrastructure access, and network compliant validation controls.

## Module Objectives

Upon completing this module, you will be able to perform the following tasks:

■ Install Cisco SSL VPN Client and configure Cisco VPN 3000 Series Concentrator v4.7

■ Install, enable, and configure the Cisco Secure Desktop

**NOTE:** Cisco Secure Virtual Private Networks (CSVPN) v4.7 is an add-on, optional module, consisting of 2 lessons. The CSVPN exam #642-511 will not be refreshed and this new content in v4.7 will not be in the CSVPN exam.

# Lesson 1

# Using Cisco SSL VPN Client

## Overview

This chapter describes the procedure to install Cisco SSL VPN Client, and how to configure Cisco VPN 3000 Series Concentrator v4.7. It includes the following topics:

- Objectives

- Cisco SSL VPN Client—An Overview

- Installing Cisco SSL VPN Client

- Configuring Cisco VPN 3000 Series Concentrator v4.7

- Summary

- Lab Exercise

# Objectives

This section lists the chapter's objectives.

## Objectives

**Upon completion of this course, you will be able to perform the following tasks:**

- **Explain how Cisco SSL VPN Client works.**
- **Identify the administrative requirements for installing Cisco SSL VPN Client.**
- **Install Cisco SSL VPN Client.**
- **Configure Cisco VPN 3000 Series Concentrator v4.7.**

CSVPN v1.0—1

# Cisco SSL VPN Client—An Overview

This topic provides an overview of Cisco SSL VPN Client.
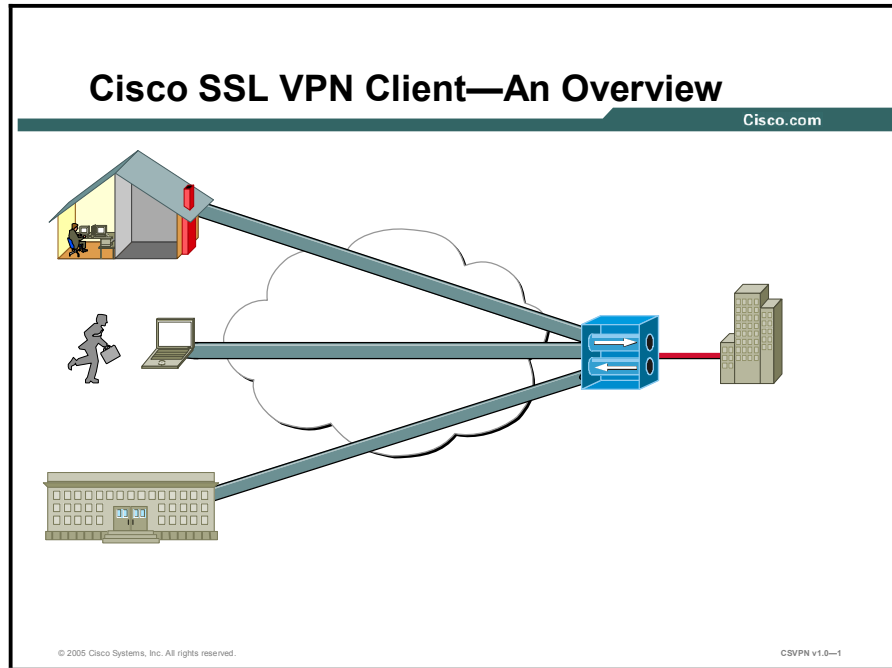
Cisco SSL VPN Client is an application that is dynamically downloaded on a remote system when a user attempts to connect to the corporate network through Cisco VPN 3000 Concentrator. Cisco SSL VPN Client provides secure access to the corporate network by establishing end-to-end, encrypted VPN tunnels. This enables a user to gain secure access to the corporate network without preinstalling any VPN client software on the remote system.

| Note | Using Cisco SSL VPN Client, users gain network-layer connectivity to virtually any IP application on the corporate network. |
| --- | --- |

The following table lists the features of Cisco SSL VPN Client.

**Features of Cisco SSL VPN Client**

| Feature | Description |
|---------|-------------|
| Universal Application Access | ■ Provides full client capabilities over SSL, including access to Cisco IP SoftPhone and voice over IP (VoIP) support, thus increasing remote-user productivity. |
| Ease of Download and Installation | ■ Dynamic download and multiple delivery methods ensure seamless download and distribution with Java, ActiveX, or .exe.<br><br>■ Small download size ensures rapid delivery.<br><br>■ No reboot required after installation. |
| Increased Security | ■ Cisco SSL VPN Client can be removed at the end of a session or can be installed permanently. |
| Zero-Touch Remote Administration | ■ Central site configuration provides integration, with no administration required on the remote client side. |

# Example: Cisco SSL VPN Client

The figure shows how users access a corporate network by using Cisco SSL VPN Client.



## Connecting to Corporate Network

Cisco.com

Step 1. Users connect to the corporate network via web browser.

Step 2. A security certificate is displayed.

Step 3. User provides authentication details.

Step 4. Cisco SSL VPN Client software is installed after successful login.

Step 5. User system obtains an IP address from the VPN 3000 Series Concentrator.

192.168.1.1

CSVPN v1.0—1
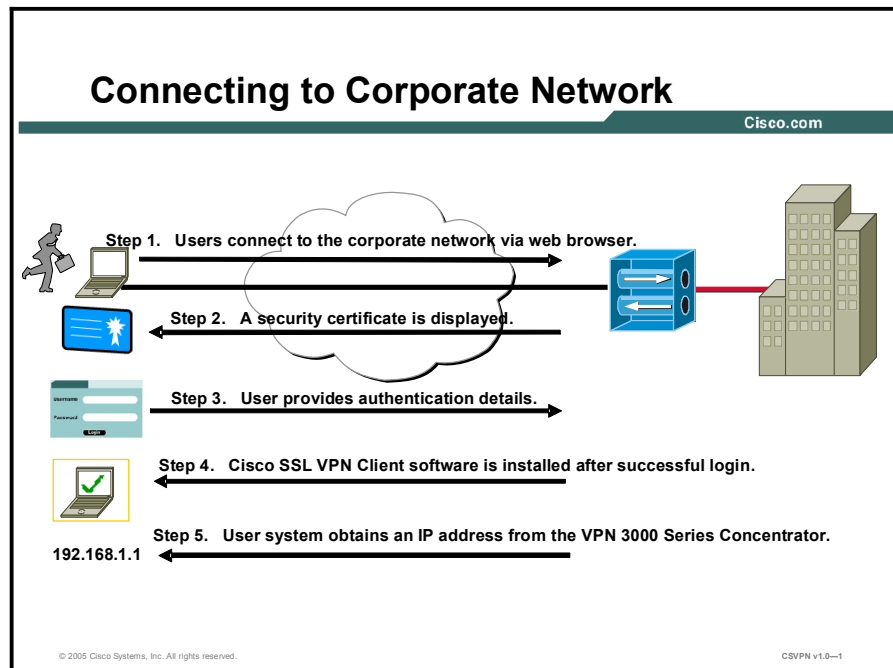
When a remotely placed user connects to the corporate network through a Web browser, a security certificate is displayed. The user then enters the login and password details. Cisco VPN 3000 Concentrator validates the login and the Cisco SSL VPN Client software is automatically installed on the remote system. Finally, Cisco SSL VPN 3000 Concentrator assigns an IP address to the remote system.

The remote system appears as a workstation within the corporate network and the traffic between Cisco VPN 3000 Concentrator and the remote system is encrypted through the SSL tunnel.

# Installing Cisco SSL VPN Client

This topic explains the administrative requirements and the procedure for installing Cisco SSL VPN Client.



Before installing a Cisco SSL VPN Client on the VPN 3000 Concentrator, you need to ensure that the remote system and the VPN 3000 Concentrator meet the recommended administrative requirements.

# Administrative Requirements for Installing Cisco SSL VPN Client



The following table lists the administrative requirements for installing Cisco SSL VPN Client on the VPN 3000 Concentrator.

### Administrative Requirements for Installing Cisco SSL VPN Client

| Administrative Requirement | Description |
|---|---|
| Hardware | ■ Cisco VPN 3000 Concentrator running version 4.7 or later<br>■ Altiga Networks VPN Concentrator running version 4.7 or later |
| Operating System | Windows XP or Windows 2000 only. |
| Privileges | Administrator privileges |

However, there can be instances where a user does not have administrator privileges on the remote system to install Cisco SSL VPN Client. In such a case, an install enabler utility, STCIE.EXE needs to be installed on the system.

| Note | STCIE.EXE preloads a client service that allows non-privileged users to load Cisco SSL VPN Client. STCIE.EXE is included in the sslclient-win-1.0.1.116.zip file. |
|---|---|

STCIE.EXE creates or updates the Cisco SSL VPN Client in the Program Files > Cisco System folder, which the VPN 3000 Concentrator pushes to the remote system.

The following table lists the switches available with the STCIE.EXE utility:

**STCIE.EXE Command Line Switches**

| Command Line Switch | Description |
|---|---|
| STCIE.EXE/? | Displays the available command options. |
| STCIE.EXE/HELP | Displays the available command options. |
| STCIE.EXE/NODLG | Suppresses dialog boxes except for errors. |
| STCIE.EXE/NODLGNOERROR | Suppresses all dialog boxes, including errors. |

# Installing Cisco SSL VPN Client

You can install Cisco SSL VPN Client on a client PC by performing the following steps:
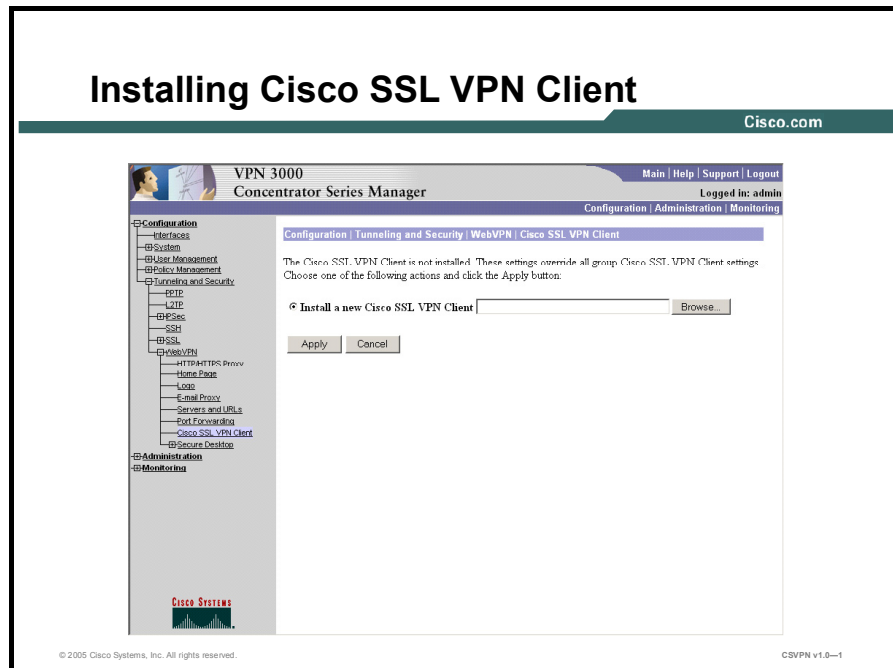


**Step 1**  Download the sslclient-win*.pkg file from the Cisco Web site by using the Cisco.com login to any location on the PC.

**Step 2**  On the Web browser window, enter the IP address of the VPN 3000 Concentrator, for example https://128.107.245.51/admin.htm. A security alert certificate dialog box is displayed.

**Step 3**  Click the **Yes** button to gain access to VPN 3000 Concentrator Series Manager.

**Step 4**  Enter the Username and Password in the Login and Password text boxes for authentication. Click the **Login** button. After successful authentication, the Main Page on the VPN 3000 Concentrator Series Manager window is displayed.

**Step 5**  Click **Configuration** to display the Configuration page. This page displays the features that can be configured.

**Step 6**  Click **Tunneling and Security**.

**Step 7**  Click **WebVPN.** This displays the options for WebVPN remote access sessions. The additional configuration options for WebVPN are SSL Encryption, HTTP, HTTPS, Interfaces, Base Groups, and Groups.

**Step 8**  Click **Cisco SSL VPN Client**.

**Step 9**  Click the **Browse** button to open the **Choose File** dialog box. Locate the Cisco SSL VPN Client package file, and then click the **Open** button**.**

**Step 10**  Click the **Apply** button to display the File Upload window. When the Upload Complete message appears, click **Save Needed** to save the configuration.

---

**Step 11** On the **Save Successful** dialog box, click the **OK** button.

To verify the installation of Cisco SSL VPN Client, click **Cisco SSL VPN Client**.
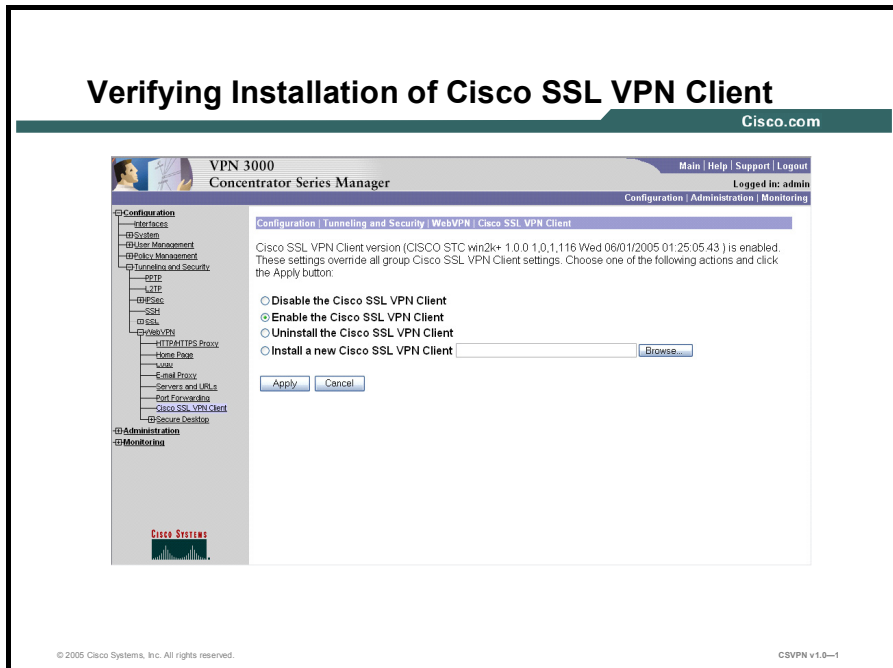


Note that the options listed in the following table are displayed on the Web browser window:

### Cisco SSL VPN Client Options

| Option | Description |
|---|---|
| Disable the Cisco SSL VPN Client | Select this radio button to disable the Cisco SSL VPN Client. |
| Enable the Cisco SSL VPN Client | Select this radio button to enable the Cisco SSL VPN Client. |
| Uninstall the Cisco SSL VPN Client | Select this radio button to remove the Cisco SSL VPN Client software image from the Cisco VPN 3000 Concentrator. |
| Install the Cisco SSL VPN Client | Select this radio button to install a new Cisco SSL VPN Client application. |

# Configuring VPN 3000 Series Concentrator v 4.7

This topic describes the several options that can be configured on the VPN 3000 Series Concentrator v 4.7.
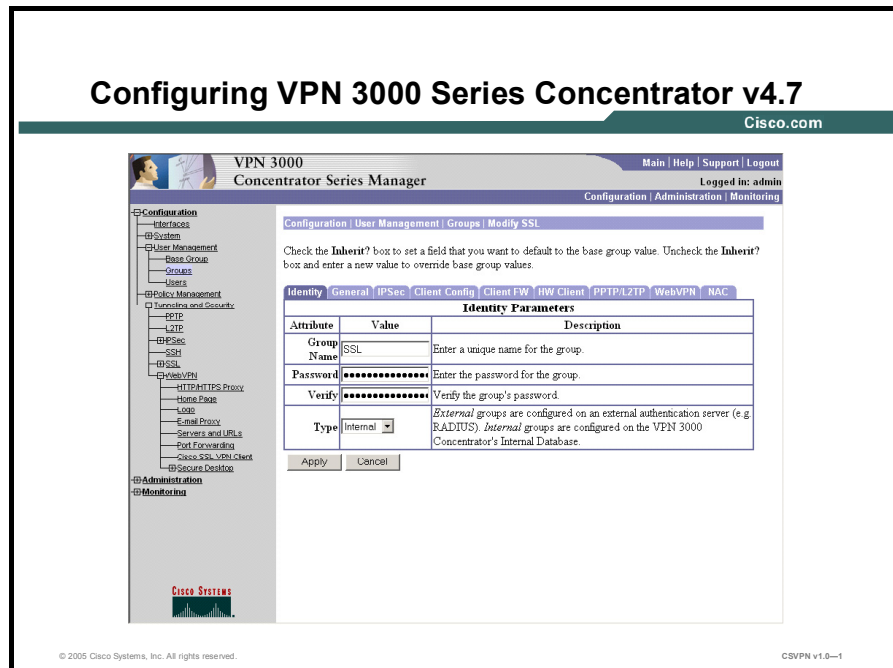


Cisco VPN 3000 Series Concentrator v 4.7 provides several options that can be configured to meet customized requirements. For example, to enhance security, you can restrict a remote user to access the corporate network only during business hours or restrict the number of simultaneous logins to the corporate network from a remote user. To meet these requirements, you can configure the global parameters and options available on the General, Client Config and WebVPN tabs of the Cisco VPN 3000 Series Concentrator v 4.7.

# Configuring Group Options on General Tab

The General tab can be divided into three sections. The first section enables you to configure the access rights and privileges. In the second section, you can configure DNS and the WINS information used by the client. The third section enables you to configure the tunneling protocols supported by the group.
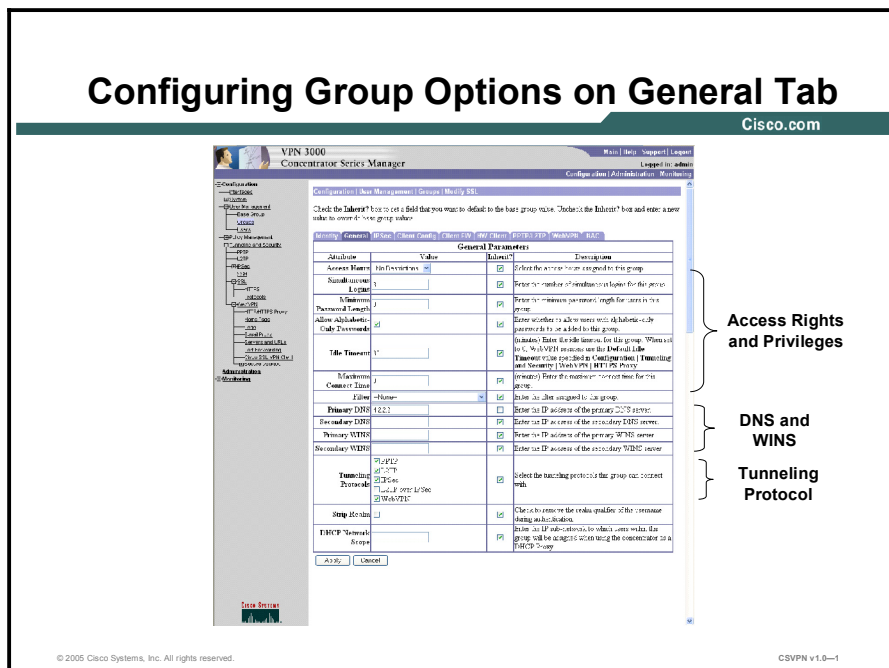


The following table lists the components of the General tab.

### Components of the General Tab

| Components | Description |
|---|---|
| Access Hours | Click this drop-down arrow and depending on your requirement, select any of the following option :<br><br>■ No Restrictions: No restrictions on access hours<br><br>■ Never: No access at any time<br><br>■ Business Hours: Access from 9 a.m. to 5 p.m., Monday to Friday |
| Simultaneous Logins | Enter the number of simultaneous logins provided for a single internal user. The default is 3, the minimum is 0, and there is no limit for maximum number of simultaneous logins. |

| Components | Description |
|---|---|
| Minimum Password Length | Enter the user password. The minimum number of characters is 1, the default is 8, and the maximum is 32. |
| Allow Alphabetic-Only Passwords | Select this check box to allow user passwords with alphabetic characters only. This option applies only to users who are authenticated by the VPN 3000 Concentrator internal authentication server. However, it is recommended to set passwords that contain alphabetic characters, numbers, and symbols. |
| Idle Timeout | Enter the idle timeout period in minutes for terminating system connection when there is no communication activity. The minimum time is 1 minute, the maximum is 10080 minutes, and the default time is 30 minutes. To disable timeout and allow an unlimited idle period, enter 0. |
| Maximum Connect Time | Enter the maximum user connection time in minutes at the end of which the system terminates the connection. The minimum time is one minute, and the maximum time is 2147483647 minutes. To allow unlimited connection time, enter 0. |
| Filter | Select the filter of the base group from the drop-down arrow. This component determines whether to allow or reject tunneled data packets coming through the VPN Concentrator based on criteria, such as source address, destination address, and protocol. You can choose None, Private, Public, or External. Moreover, additional filters that you configure also appear on this list. |
| Primary DNS | Enter the IP address of the primary DNS server for base-group users. The system sends this address to the client as the first DNS server to use for resolving host names. |
| Secondary DNS | Enter the IP address of the secondary DNS server for base-group users. The system sends this address to the client as the second DNS server to use for resolving host names. |
| Primary WINS | Enter the IP address of the primary WINS server for base-group users. The system sends this address to the client as the first WINS server to use for resolving host names under Windows NT. If the base group does not use WINS, leave this field blank. |
| Secondary WINS | Enter the IP address of the secondary WINS server for base-group users. The system sends this address to the client as the second WINS server to use for resolving host names under Windows NT. |
| SEP Card Assignment | Select the check boxes to assign a user to a given SEP or SEP-E module. By default, all the check boxes are selected. |
| Tunneling Protocols | Select the desired Tunneling Protocol check boxes to select the VPN tunneling protocols that users in this group can use. The WebVPN check box has been included in VPN 3000 Concentrator v4.7. WebVPN does not require a software or hardware client to establish a remote-access tunnel. |
| Strip Realm | Select this check box to remove the realm qualifier of the username during authentication. On selecting this check box, authentication is based on the username |

| | |
|---|---|
| | only. Otherwise, authentication is based on the full username@realm string. You need to select this check box if your server is unable to parse delimiters. |
| DHCP Network Scope | Enter the IP sub-network that the DHCP server should assign to users in the group. To use this feature, the VPN 3000 Concentrator must be using a DHCP server for address assignment. |

# Configuring Group Options on Client Config Tab

On this tab, you can set client configuration parameters separately for Cisco clients, Microsoft clients, and for clients common to Microsoft and Cisco.



The following table lists the components of Cisco Clients Parameters that are on the Client Config tab.

## Cisco Client Parameters

| Components | Description |
| --- | --- |
| Allow Password Storage on Client | Select this check box to allow IPSec clients to store their login passwords on their local client systems. If you do not allow password storage (the default), IPSec users must enter their password each time they seek access to the VPN. |
| IPSec over UDP | Select this check box for Cisco VPN Client (IPSec client) or VPN 3002 hardware client to connect to the VPN Concentrator through UDP through a firewall or router. This check box is not selected by default. |
| IPSec over UDP Port | Enter the UDP port number to use on the VPN Concentrator if you allow IPSec through NAT. Enter a number ranging from 4001 to 49151; default is 10000. |

| Components | Description |
|---|---|
| IPSec Backup Servers | Select the appropriate backup server configuration. You can enter either the IP addresses or the hostnames of the VPN Concentrators that are to be configured as the backup servers. |

**Configuring Group Options on Client Config Tab**

The following table lists the components of the Microsoft Clients Parameters on the Client Config tab.

### Microsoft Client Parameters

| Components | Description |
| --- | --- |
| Intercept DHCP Configure Message | Select this check box to enable DHCP Intercept. DHCP Intercept allows Microsoft XP clients to implement split-tunneling with a VPN Concentrator. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask. |
| Subnet Mask | Enter the subnet masks for clients requesting Microsoft DHCP options. |

| Components | Description |
|---|---|
| IE Proxy Server Policy | Choose from the following options:<br><br>■ **Do not modify proxy settings**: Leave the HTTP proxy server setting in Internet Explorer unchanged for the client PC.<br><br>■ **No Proxy**: Disable the HTTP proxy server, if any, configured in Internet Explorer on client PCs.<br><br>■ **Auto Detect Proxy**: Set Internet Explorer on the client PCs to use the automatic proxy detection feature.<br><br>■ **Use proxy server/port listed below**: Set the HTTP proxy server setting in Internet Explorer on client PCs according to values that you configure in the IE Proxy Server field on this configuration screen. |
| IE Proxy Server | Enter the proxy server name or IP address and port number for use by Internet Explorer on Windows client PCs. The name or IP address must be separated from the number using a colon (:). Ensure that the **Use proxy server/port listed below** radio button is selected. |
| IE Proxy Server Exception List | Enter a list of domain names or specific addresses that should not be accessed through a proxy server, if desired. |
| Bypass Proxy Server for Local Addresses | Select the check box to allow local requests (addresses inside the enterprise network) bypass the proxy server. |

The following table lists the components of the Common Client Parameters on the Client Config tab.

## Common Client Parameters

| Components | Description |
|---|---|
| Banner | Enter the welcome text that this group's IPSec clients see when they log in. The maximum length is 510 characters. You can use ASCII characters.<br><br>In addition, you can also display a banner to VPN Clients, WebVPN users, and VPN 3002 hardware clients that are configured for individual user authentication. |
| Split Tunneling Policy | Choose from the following options:<br><br>■ **Tunnel everything**: This radio button is selected by default, it disables split tunneling. When Tunnel everything is configured, all traffic from remote clients in the group travels over the secure IPSec tunnel in encrypted form. In addition, the network traffic goes only to the VPN Concentrator. Remote users in this group reach internet networks through the corporate network and do not have access to local networks.<br><br>If users in a group need access to local networks, select **Allow networks in list to bypass tunnel** check box. This allows you to send all data through the secure IPSec tunnel except for data to addresses on the network list. This option is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.<br><br>■ **Only tunnel networks in list**: Select this radio button to send network traffic for addresses in the list in the secure IPSec tunnel. The network traffic to all other addresses is sent in unencrypted form. The purpose of this option is to allow remote users to access internet networks without requiring them to be tunneled through the corporate network. |
| Split Tunneling Network List | From the drop-down arrow, select the split tunneling address list to use with this group's remote-access IPSec clients. Both the Allow Networks in List to Bypass Tunnel option and the Only Tunnel Networks in List option make split tunneling decisions on the basis of a network list. |
| Default Domain Name | Enter the default domain name that the VPN Concentrator passes to the IPSec client. |
| Split DNS Names | Enter each domain name to be resolved by the internal server. Use commas but no spaces to separate the names. The VPN Concentrator does not support split-DNS for Microsoft VPN Clients; however, it does support split DNS for the Cisco VPN Client operating on Microsoft Windows Operating Systems. |

# Configuring Group Options on WebVPN Tab

By using this tab, you can configure access to network resources for WebVPN users.
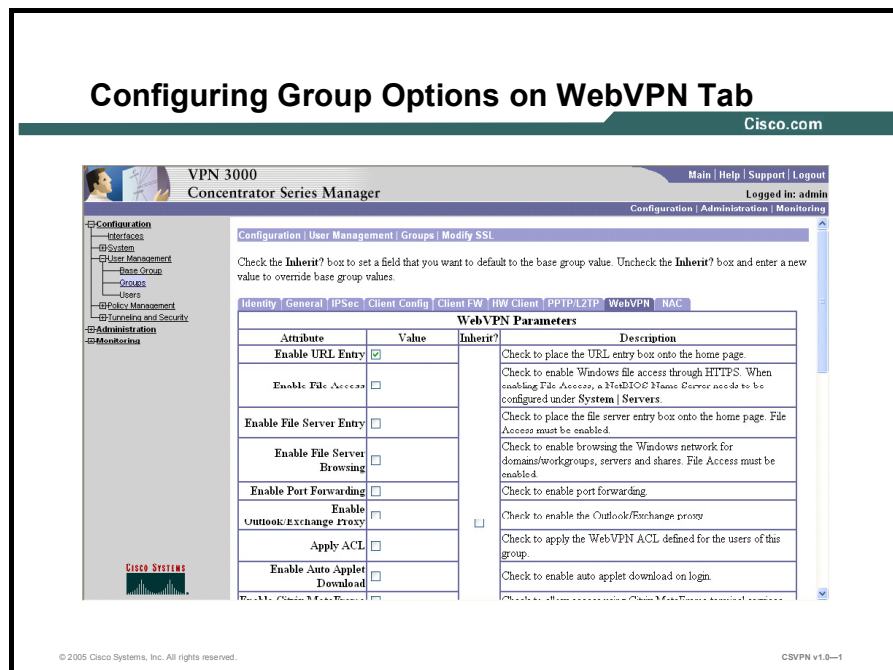


You can perform the following steps to enable Cisco SSL VPN Client for Web VPN:

**Step 1**   After logging on to VPN 3000 Series Concentrator Manager, click the **Configuration** menu. This displays the features that can be configured, which are Interfaces, System, User Management, Policy Management, and Tunneling and Security.

**Step 2**   Click **User Management**. This section allows you to configure group and user parameters, including IPSec, PPTP, and L2TP.

**Step 3**   Click **Groups.** You can configure groups in this section. A group is a collection of users treated as a single entity. A list of existing groups is displayed in the **Current Groups** option in this section. You also have the option of adding new groups to already existing ones, deleting groups, and also modifying groups by modifying the parameters.

**Step 4**   Select a group from the **Current Groups** list and click the **Modify Group** button. This opens the Modify SSL page. This section contains the General, IPSec, Client Config, Client FW, HW Client, PPTP/L2TP, WebVPN, and NAC tabs. You can click any of the tabs and modify the default parameters by not selecting the Inherit? check box. Select the Inherit? check box to set the field that you need to use as the default setting for the base group.

**Step 5**   Click **WebVPN** to modify the default parameters on the WebVPN tab.

**Step 6**   Select the **Enable Cisco SSL VPN Client** check box to enable Cisco SSL VPN Client. Click the **Apply** button to save the changes made**.**

**Step 7**   Click **Save Needed** to save the configuration.

**Step 8** On the **Save Successful** dialog box, click the **OK** button.

To log on to the Cisco SSL VPN Client, log on to the WebVPN URL, enter Username and Password. Notice that Cisco SSL VPN client is automatically installed on your system and a key icon appears on the taskbar.

The following table lists the components of the WebVPN tab.

| Component | Description |
|---|---|
| Enable URL Entry | Select this check box to allow users to enter Web addresses in the URL entry box, and to use WebVPN to access those websites. You can limit the Internet access to WebVPN users by not selecting the Enable URL Entry check box. This prevents WebVPN users from surfing the Internet during a WebVPN connection. |
| Enable File Access | Select this check box to allow users to access Windows files on the network. They can download, edit, delete, rename, and move files. If you enable only this parameter for WebVPN file sharing, users can access only the servers that you configure in the Tunneling and Security page. |
| Enable File Server Entry | Select this check box to allow users to enter path names of Windows files directly. Users may need to be authenticated before accessing files. |
| Enable File Server Browsing | Select this check box to allow users to browse the Windows network for domains/workgroups, servers, and shares. Users can select domains and workgroups, and can browse servers and shares within those domains. Users may need to be required to authenticate before accessing servers. |
| Enable Port Forwarding | Select this check box to allow users to access client/server applications by mapping local TCP ports on the system to remote ports. |
| Enable Outlook/Exchange Proxy | Select this check box to enable the Outlook/Exchange mail forwarding (MAPI) proxy. |
| Apply ACL | Select this check box to apply the WebVPN Access Control List that is defined for the users of this group. |
| Enable Auto Applet Download | If WebVPN is enabled for the group. Select this check box to automatically start the port forwarding or Outlook/Exchange Proxy Java applet when users log on through WebVPN. |
| Enable Citrix MetaFrame | Select this check box to enable support for Citrix MetaFrame services through WebVPN. |
| Enable Cisco SSL VPN Client | Select this check box to enable Cisco SSL VPN Client (SVC). |
| Require Cisco SSL VPN Client | Select this check box to make the SSL VPN Client available for members of this group. When this is check box is selected, standard WebVPN connections are not permitted. This setting does not apply if the Enable Cisco SSL VPN Client check box is not selected. This check box is not selected by default. |
| Keep Cisco SSL VPN Client | Select this check box to allow clients to retain the Cisco SSL VPN Client software installed in their PCs, which speeds up access for subsequent connections. |
| Port Forwarding Name | Enter the display name that users see when using TCP Port Forwarding. |
| Homepage | Enter the default Web page that is displayed to users when they connect for the first time. |
| Filter Java/Active X | Select this check box to remove <applet>, <embed> and <object> tags from HTML. |

| | |
|---|---|
| | HTML. |
| Filter Scripts | Select this check box to remove <script> tags from HTML. |
| Filter Images | Select this check box to remove <img> tags from HTML. |
| Filter Cookies from Images | Select this check box to remove cookies that are delivered with images. |

# Configuring Global Parameters

The topic describes the process involved in configuring system-wide parameters.
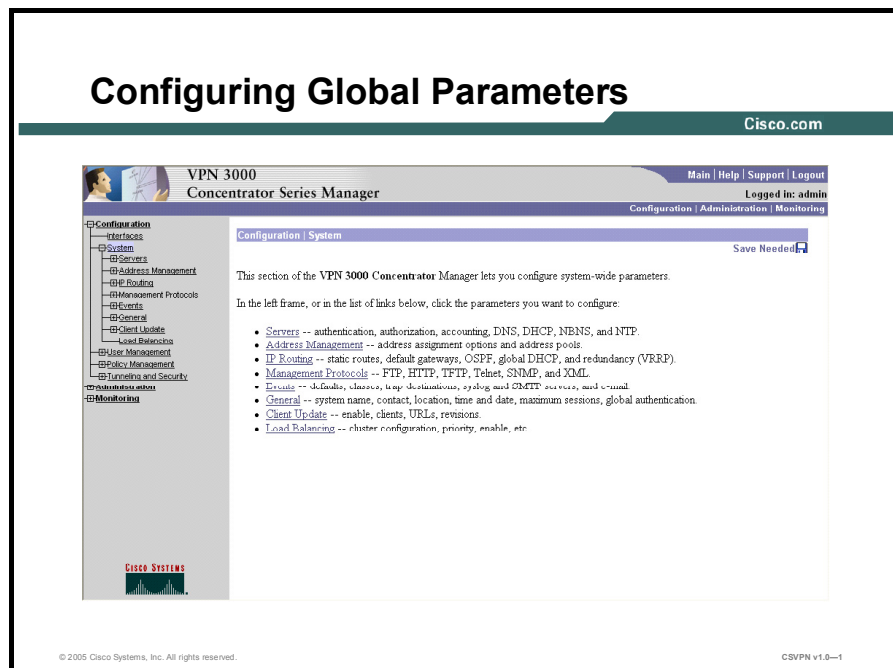


You can configure several global parameters on the sections available in **Configuration > System**. Using these sections you can configure servers, address management, IP routing, management protocols, and load balancing.

■ **Servers**—This section enables you to configure parameters for servers that authenticate users. The key servers include:

— **Authentication**: You can configure Cisco VPN 3000 Series Concentrator internal server and external RADIUS, NT Domain, and SDI servers for authenticating users. Ensure that you configure at least one authentication server type, and one method of authenticating users.

— **Authorization**: You can configure parameters for servers that authorize users. Authorization can be configured on a global or group basis.

— **Accounting**: You can configure parameters for external RADIUS user accounting servers. You can configure and prioritize up to ten servers. The first server is the primary, and the rest are backup servers. Ensure that the servers you reference are properly configured.

The other servers include DNS Server, DHCP Server, Firewall Server, NBNS Server, and NTP Server.

■ **Address Management**—This section enables you to configure options for assigning addresses to clients when a tunnel is established. A client must have an IP address to function as a tunnel endpoint. This section includes Assignment and Pools components:

— **Assignment**: This component enables you to configure options for assigning addresses to clients while establishing a tunnel.

— **Pools**: This component enables you to configure IP address pools from which Cisco VPN 3000 Series Concentrator assigns addresses to clients. You can also add and modify an IP address pool.

■ **IP Routing**—This section includes Static Routes, Default Gateways, Open Shortest Path First (OSPF), OSPF Areas, DHCP, Redundancy, and Reverse Route Injection components. In this section, you can configure several system-wide IP routing parameters. For example, in the Default Gateways component, you can configure the default gateway for IP routing, and tunneled traffic. When you configure a tunnel default gateway, Cisco VPN 3000 Series Concentrator forwards the tunnel-to-tunnel traffic to the tunnel default gateway. The gateway redirects the traffic back through Cisco VPN 3000 Series Concentrator to its destination. You can also override the default gateway by selecting the Override Default Gateway check box.

■ **Management Protocol**—This section allows you to configure and enable built-in VPN Concentrator servers that provide management functions using FTP, HTTP, TFTP, Telnet, SNMP, SNMP Communities, and XML.

■ **Events**—This section enables you to configure how the VPN 3000 Concentrator handles several events, such as alarms, traps, and error conditions.

■ **General**—This section enables you to configure several general parameters for Cisco VPN 3000 Series Concentrator, such as Identification, Time and Date, Sessions, and Global Authentication Parameters.

■ **Client Update**—This section enables you to configure the client update feature. The client update feature is included in the VPN 3000 Concentrator to simplify the software update process.

■ **Load Balancing**—This section enables you to share the session load when you use two or more VPN Concentrators connected on the same network to handle remote sessions.

You can also configure global parameters on the sections available in **Configuration**>**Tunneling and Security**>**SSL**>**HTTPS** and **Configuration**>**Tunneling and Security**>**SSL**>**Protocols**.

■ The SSL section allows you to set the Secure Socket Layer (SSL) options for management and WebVPN remote access sessions. A secure session between the remote user, also called a client, and the VPN Concentrator is created by SSL after successful authentication by the user. The components of SSL include:

— **HTTPS**: You can configure HTTPS (HTTP over SSL) that allows you to use a Web browser over a secure and encrypted connection to manage the VPN 3000 Concentrator. The following table lists the components of HTTPS section.

## Components of HTTPS

| Component | Description |
|---|---|
| Enable HTTPS | Select this check box for enabling the HTTPS server. The check box is selected by default. |
| HTTPS Port | Enter the port number that the HTTPS server uses. The default value is 443. |
| Client Authentication | Select this check box to enable SSL client authentication with digital certificates. This check box is not selected by default |

— **Protocols**: You can configure the encryption algorithms and SSL versions that the VPN Concentrator SSL server can negotiate with a client and use for encrypting a session. The following table lists the components of Protocols section.

## Components of Protocols

| Component | Description |
|---|---|
| Encryption Protocols | Select the check boxes for the encryption algorithms that the VPN Concentrator SSL server can negotiate with a client and use for session encryption. The check boxes are selected by default. Select at least one algorithm to enable SSL. if all the algorithms are not selected, SSL is disabled. |
| SSL Version | Click the drop-down arrow and select the SSL version. The version selected must match both sides of the connection. The options available are: Negotiate SSL V3/TLS V1, Negotiate SSL V3, SSL V3 Only, TLS V1 Only, and Negotiate TLS V1. |
| SSL Re-Key Interval | Enter the number of seconds between renegotiations of the SSL connection. This value applies to Cisco SSL VPN Clients. The range is 300 seconds (5 minutes) to 604,800 seconds (one week). The default time is 86,400 seconds (one day). |

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- **Cisco VPN 3000 Series Concentrator running version 4.7 or later offers extensive application support through its dynamically downloaded Cisco SSL VPN client for WebVPN.**
- **Cisco SSL VPN Client provides secure access to the corporate network by establishing end-to-end, encrypted VPN tunnels.**
- **STCIE.EXE utility enables a non-privileged users to install Cisco SSL VPN client on a system.**
- **Configure the global parameters and options available on the General, Client Config and WebVPN tabs of Cisco VPN 3000 Series Concentrator v 4.7 to meet customized requirements.**

CSVPN v1.0—1

# Lab-Exercise––Install Cisco SSL VPN Client and Configure VPN 3000 Series Concentrator v4.7

Complete the following lab exercise to practice what you learned in this chapter.

## Objectives

Your task in this lab exercise is to install Cisco SSL VPN Client and configure the VPN 3000 Series Concentrator v4.7. Work with your lab partner to complete the following tasks:

■ Complete the lab exercise setup.

■ Install Cisco SSL VPN Client

■ Configure the VPN 3000 Series Concentrator v4.7

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
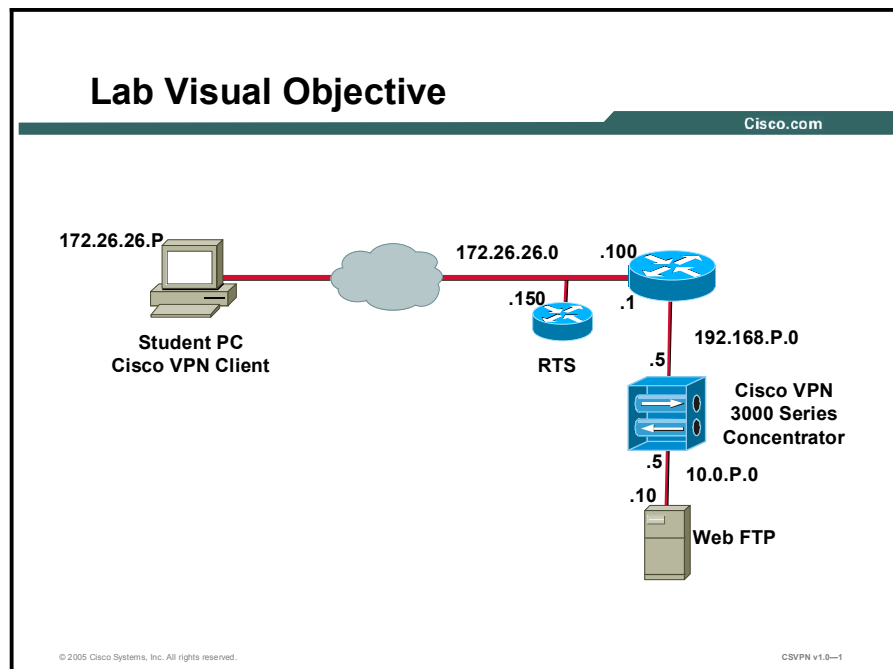


## Scenario

You are working as a network administrator in your organization. The senior network administrator has assigned you the task of installing Cisco SSL VPN Client and configuring the VPN 3000 Series Concentrator v 4.7 to enhance network security.

## Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment as follows:

■ Ensure that your student PC is powered on.

- Ensure your student PC IP addresses are configured correctly:

  — Primary IP address—172.26.26.P (where P = pod number)

  — Default gateway IP address—172.26.26.150

- Ensure that your Concentrator is powered on.

# Task 2—Install Cisco SSL VPN Client

Complete the following steps to install Cisco SSL VPN Client.

**Step 1**  Download the sslclient-win*.pkg file from Cisco Web site by using the Cisco.com login to any location on the PC.

**Step 2**  On the Web browser window, enter the IP address of the VPN 3000 Concentrator.

**Step 3**  When a security alert certificate dialog box is displayed, click the **Yes** button to gain access to the VPN 3000 Concentrator Series Manager window.

**Step 4**  Enter the username and password the Login and Password text boxes for authentication. Click the **Login** button.

**Step 5**  Click **Configuration > Tunneling and Security** > **WebVPN.**

**Step 6**  Click **Cisco SSL VPN Client**.

**Step 7**  Click the **Browse** button to open the **Choose File** dialog box. Locate the Cisco SSL VPN Client package file, and then click the **Open** button**.**

**Step 8**  Click the **Apply** button to display the File Upload window. When the Upload complete message appears, click **Save Needed**.

**Step 9**  Click the **OK** button on the **Save Successful** dialog box.

**Step 10**  Click **Cisco SSL VPN Client** to verify the installation of Cisco SSL VPN Client. Note that the four options, Enable Cisco SSL VPN Client, Disable Cisco SSL VPN Client, Install Cisco SSL VPN Client, and Uninstall Cisco SSL VPN Client appear on the Web page.

# Task 3—Configure VPN 3000 Series Concentrator v 4.7

Complete the following steps to configure VPN 3000 Series Concentrator.

**Step 1**  Log on to the VPN 3000 Series Concentrator Manager window.

**Step 2**  Click **Configuration** > **User Management > Groups.**

**Step 3**  Select a group from the **Current Groups** list and click the **Modify Group** button.

**Step 4**  Click **WebVPN**.

**Step 5**  Select the **Enable Cisco SSL VPN Client** check box.

**Step 6**  Click the **Apply** button**.**

**Step 7**  Click **Save Needed**.

**Step 8**  Click the **OK** button on the **Save Successful** dialog box.

## Lesson 2

# Installing and Configuring Cisco Secure Desktop

## Overview

This chapter explains how the Cisco Secure Desktop (CSD) works, and also describes the procedure to install and configure it. It includes the following topics:

- Objectives

- Cisco Secure Desktop—An Overview

- Installing Cisco Secure Desktop

- Identifying Secure Desktop Manager Options

- Configuring Secure Desktop Manager Options

- Enabling Cisco Secure Desktop

- Summary

- Lab Exercise

# Objectives

This section lists the chapter's objectives.

## Objectives

**Cisco.com**

**Upon completion of this course, you will be able to perform the following tasks:**

- **Explain how Cisco Secure Desktop works.**
- **Install Cisco Secure Desktop on the VPN 3000 Concentrator.**
- **Identify the Secure Desktop Manager options.**
- **Configure the Secure Desktop Manager options.**
- **Enable Cisco Secure Desktop on the VPN 3000 Concentrator.**

© 2005 Cisco Systems, Inc. All rights reserved.

CSVPN v1.0—2-1

# Cisco Secure Desktop—An Overview

This topic describes how the CSD works.
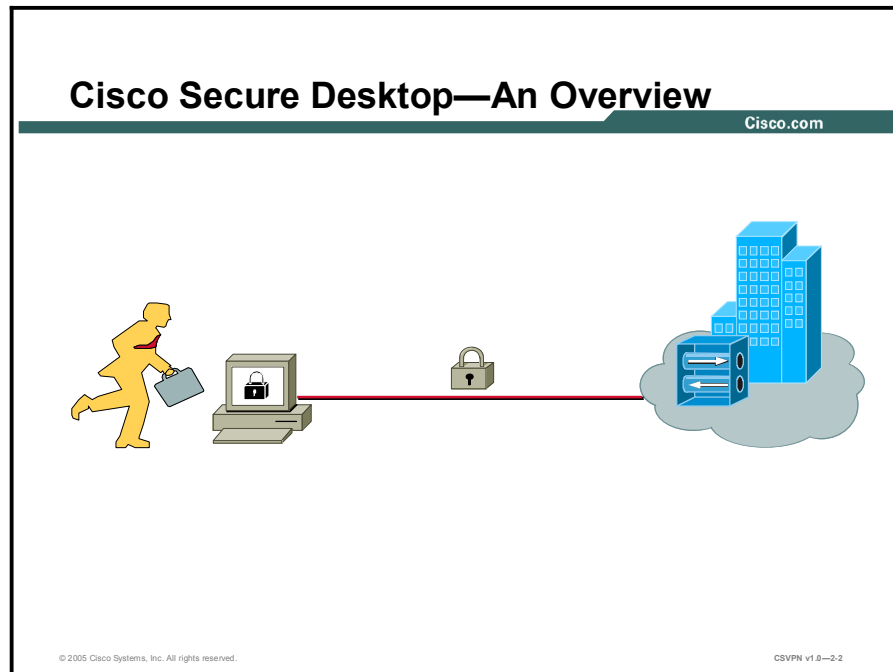


Enterprises are increasingly expected to provide secure remote access to the corporate network for a diverse mix of users. It is also essential that this access to the corporate network is secure for both the remote user and the corporate network. WebVPN is used to securely extend the corporate network to an authorized user. The main advantage of WebVPN is that users can securely access their corporate network from any supported browser. This means that they are not required to install any VPN client software on their system.

However, this extension of network also entails an increase in the points for potential network security attacks. These WebVPN endpoint security issues are addressed with the use of CSD. CSD is an endpoint security solution that offers data theft prevention, so that confidential data does not remain unprotected on a remote system. CSD ensures complete data protection by offering an encrypted space for users throughout an SSL session. CSD provides preconnection security state or "posture" assessment of the connecting device. It also offers security during the session by creating a secure virtual desktop that protects sensitive data. Finally, CSD also provides postconnection "clean-up" that eliminates all traces of sensitive session information.

When a remote user attempts to connect to the corporate network, CSD is downloaded to the user's desktop via Active X, Java or .exe. The CSD Host Integrity Verification feature performs preconnection posture assessment to certify that the endpoint seeking access possesses the particular antivirus, firewall, and OS or service pack features that are required. It also detects installed malware before granting access to the network. CSD then creates a secure vault for all session information by generating a virtual desktop, on the user system. During the session, all information is encrypted and written onto the CSD partition on the hard drive.

At the close of the session, the secure vault is eradicated and all session information including cache files, history, cookies, file downloads, and passwords are encrypted real time. This

ensures that all data is protected from the start of the session. The automatic timeout feature of CSD ensures that session information is erased, when the session times out.

# Installing Cisco Secure Desktop

This topic describes how to install CSD on the VPN 3000 concentrator.
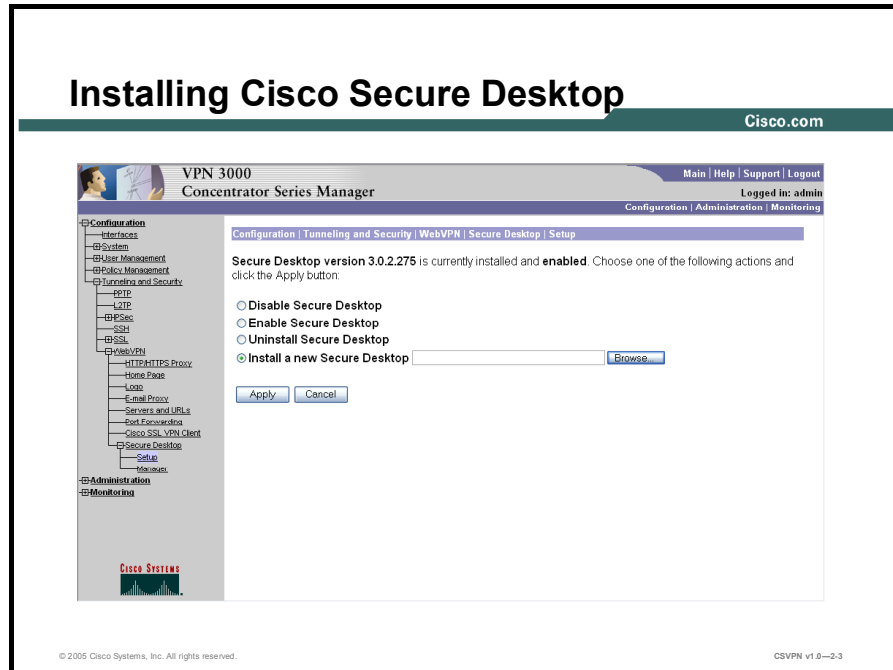


To install CSD, you need to first download the securedesktop*.pkg file. You can then install the securedesktop*.pkg file in the VPN 3000 Concentrator Series Manager application, and then configure the settings before you enable it for remote users over WebVPN.

---

**Note**     Before you start the installation process, download the CSD installation file and then copy it to any location on your management PC.

---

[0]To install CSD, do the following:

**Step 1**     Connect to the VPN 3000 Series Concentrator, and log on to the VPN Concentrator Manager application.

**Step 2**     In the home page of VPN Concentrator Manager, click **Configuration** > **Tunneling and Security** > **WebVPN** > **Secure Desktop** > **Setup** window.

**Step 3**     Click the **Install a new Secure Desktop** radio button.

**Step 4**     Click the **Browse** button and then locate the CSD installation file on your management PC.

**Step 5**     Click the **Apply** button. The CSD is installed in the VPN Concentrator Manager and a Secure Desktop Package Upload Success window is displayed.

**Step 6**     Click **Save Needed** to save the settings.

---

**Step 7** Click the **OK** button when the **Save Successful** message box appears.

---

| | |
|---|---|
| **Tip** | Users having a valid Cisco.com login ID with privileges to download the VPN software can click http://www.cisco.com/cgi-bin/tablebuild.pl/vpn3000-3des to download the securedesktop*.pkg file. |

---

# Identifying Secure Desktop Manager Options

This topic describes the different Secure Desktop Manager options that you can configure.
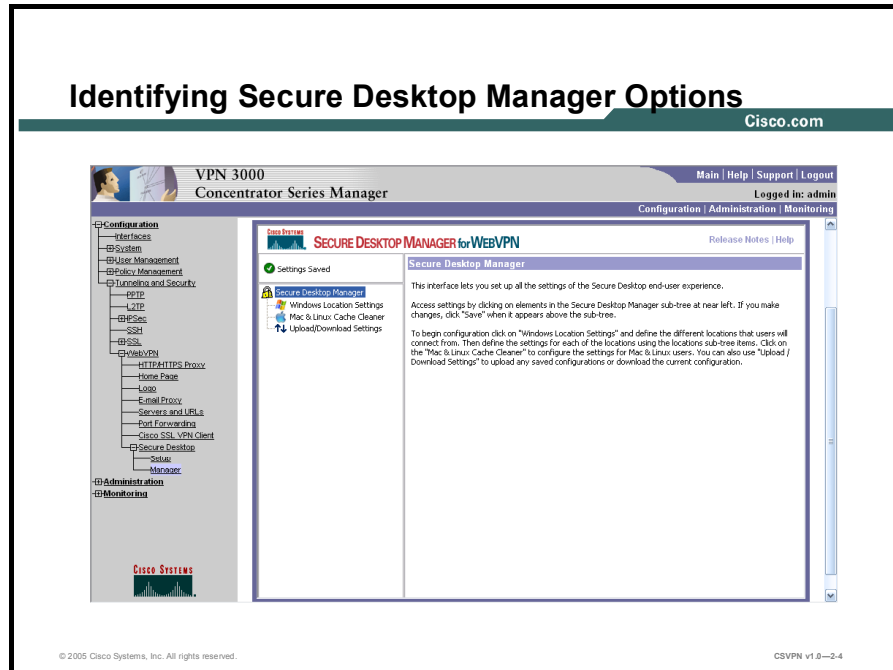


CSD contains a customizable suite of security tools that you can configure for various deployment scenarios. By doing this, you can secure remote systems and enforce your company's network security policies. You can configure these options in Secure Desktop Manager software for WebVPN that runs within the VPN Concentrator Manager application. To configure CSD settings for client computers, you need to navigate to the **Configuration >Tunneling and Security > WebVPN > Secure Desktop > Manager** window. The Secure Desktop Manager window initially has these options:

- Windows Location Settings

- Mac & Linux Cache Cleaner

- Upload/Download Settings

# Configuring Secure Desktop Manager Options

This topic describes how to configure the Secure Desktop Manager options.
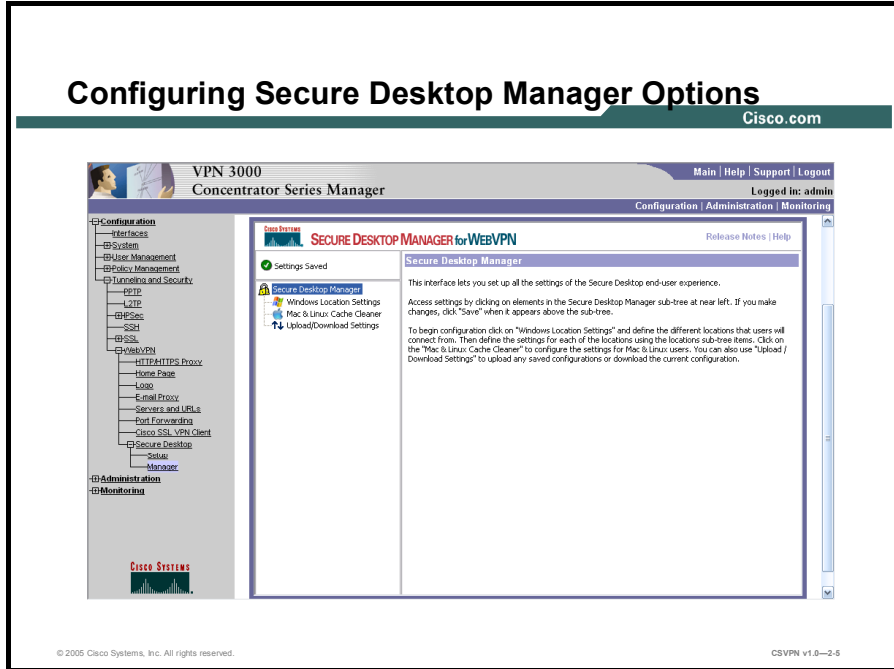


To configure the secure desktop manager options, you need to click **Windows Location Settings** and define the different locations that users will connect from. Then define the settings for each of the locations using the locations subtree items. Click **Mac & Linux Cache Cleaner** to configure the settings for Mac & Linux users. To upload any saved configurations or download the current configuration, click **Upload/Download Settings**.

# Configuring the Windows Location Settings

By configuring the Windows locations, you can allow CSD to deploy an appropriate secure environment for the hosts that connect through the VPN. It is in the administrator's best interests to increase security on hosts that are likely to be insecure, while offering flexibility to hosts that are deemed secure.
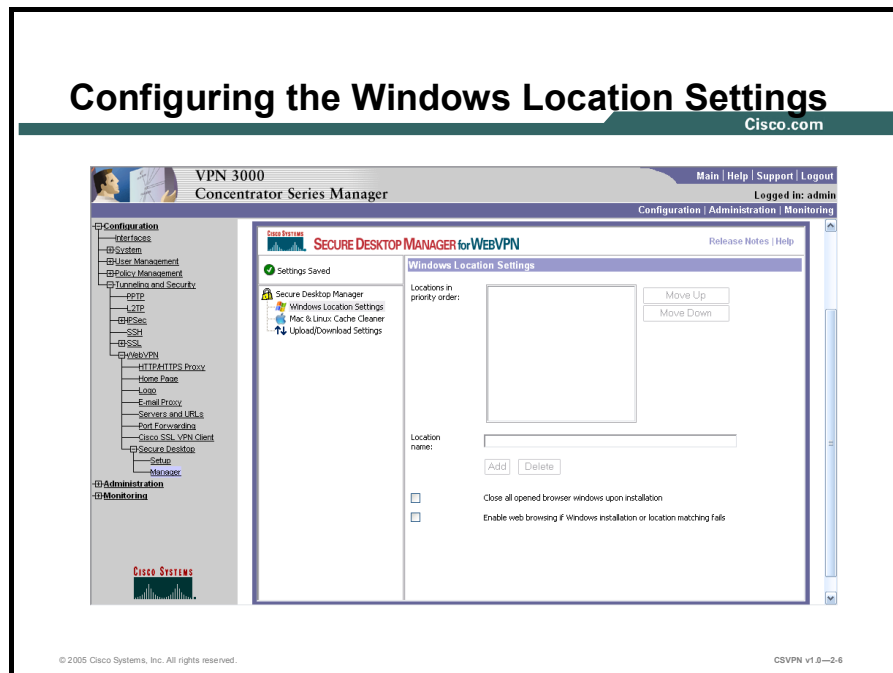


You can use the Windows Location settings option to create a group of settings for Windows clients connecting from a particular type of location, such as Work, Home, or an Internet Cafe. For example, clients connecting from within a workplace LAN on a 10.x.x.x network behind a NAT device are not at risk for exposing confidential information. For these clients, a network administrator might set up a CSD Windows Location named Work that is specified by IP addresses on the 10.x.x.x network, and disable both the Cache Cleaner and the Secure Desktop function for this location.

In contrast, users' home PCs might be considered more at risk to viruses due to their mixed use. For these clients, you might set up a location named Home that is specified by a corporate-supplied certificate that employees install on their home PCs. This location would require the presence of antivirus software and specific, supported operating systems to grant full access to the network.

After you create a Windows location name, you can also configure other options such as VPN Feature Policy, Cache Cleaner, and Secure Desktop features for that location. Network administrators need to first consider the different hosts that will connect through the VPN and then consider what modules and criteria are needed to secure these hosts. When you configure multiple Windows location names, CSD checks locations in the order listed on the Windows Location Settings window. CSD then grants privileges to a client PC based on the first location definition it matches. You can view the Lists the locations that you have configured in the order

of priority. However, you can change this priority order for locations by choosing a location name and clicking the **Move Up** and **Move Down** button.

---

| Note | Begin configuring CSD by defining Windows Locations. Windows Locations apply to supported Microsoft Windows clients only; they do not apply to Macintosh and Linux clients. |
|------|------|

---

To create a Windows location name, do the following:

**Step 1** Connect to the VPN 3000 Series Concentrator, and log in to the VPN Concentrator Manager application.

**Step 2** In the home page of VPN Concentrator Manager, click **Configuration** > **Tunneling and Security** > **WebVPN** > **Secure Desktop** > **Manager** window.

**Step 3** Click **Windows Location Settings** in the subtree on the left panel of the Secure Desktop Manager window.

**Step 4** Enter the location name in the **Location name** text box, and then click **Add.**

**Step 5** Click **Save** to save the changes.

You can remove unsecured Web browser sessions when CSD is installed by selecting the **Close all opened browser windows upon installation** check box. This option applies to all the Windows locations. You can also configure the Windows location settings to allow Windows clients use the VPN to browse the Web as a minimal connection option, if the client PC does not match any of the configured locations criteria. This is done by selecting the **If Windows installation or location matching fails, enable web browsing** check box.

# Identifying the Windows Location Name

To define and configure the settings for a window location, click the location name. When you click location name, the identification window opens. This window enables you to specify the criterion that defines the location. A location can be based on a certificate, an IP address range, the presence or the absence of a particular file or registry entry.
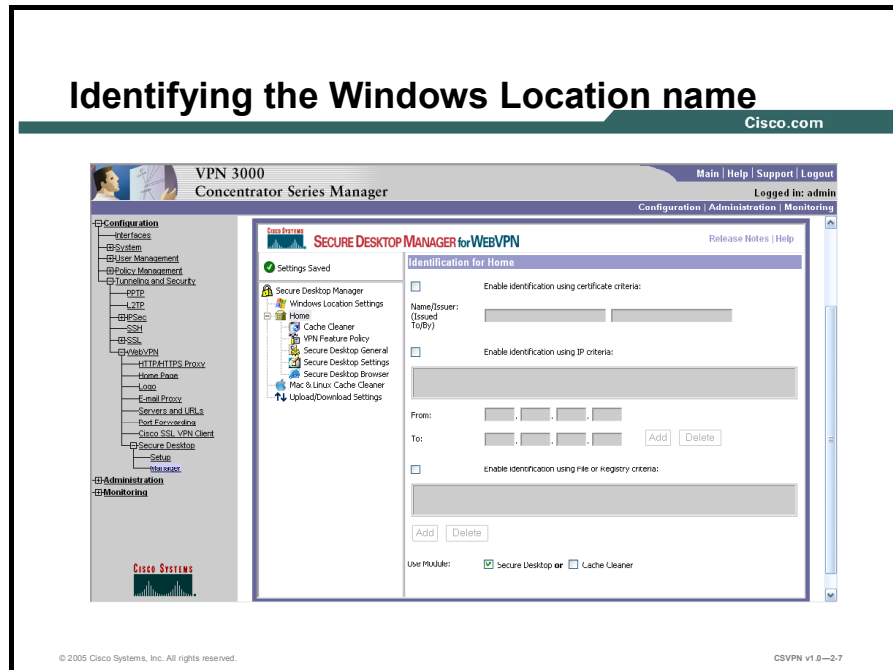


There are three identification criteria that you can provide for a Windows location name. They are:

- **Enable identification using certificate criteria**—You can select this option to allow CSD to identify the client computer by the certificate. If you select this option you must provide the certificate information with the Name (company) and Issuer (certificate).

- **Enable identification using IP criteria**—You can select this option to allow CSD search the IP addresses of the client trying to connect. If the client has an address within the specified range, CSD will validate the location. If the client has more than one network card, CSD will use only the address of the first card that has been detected. If you select this option, you must enter one or more IP Address ranges, by clicking the Add button.

- **Enable identification using File or Registry criteria**—You can select this option to allow CSD to identify the clients trying to connect to the specified files or registry keys. If the client has these files or registry keys, CSD will validate the location. If you select this option, you must enter one or more file or registry names and strings by clicking the **Add** button. You can enter the file or registry key information and set the condition by using a number of check boxes and drop down items.

- **Use Module** — You can use this option to select the CSD module that you need for a particular location. The options from which you can choose are **Cache Cleaner,**

**Secure Desktop,** or neither. You cannot use the Cache Cleaner and Secure Desktop at the same time. If neither is selected, the VPN Feature Policy will be applied.

CSD considers the three locations criteria in a logical "AND" relationship. For example, you can specify an IP address range under **Enable identification using IP criteria.** You can also specify "File company_software.exe #does exist#" under **Enable identification using File or Registry criteria.** Therefore the client must meet both these conditions to match the location. However, within each area, only one of the criteria you specify must match. This is because CSD considers the criteria in a logical "OR" relationship. Hence, if you specify several files under **Enable identification using File or Registry criteria,** only one of these files will be present.

| Note | If you need to install CSD to all the clients regardless of their status, you can configure only one location without specifying a certificate, an IP address, a file or registry criteria. This default location will enable all your remote users to connect from any computer. |
| --- | --- |

# Configuring the Cache Cleaner Options

The Cache Cleaner option erases all data that a user downloaded, inserted, or created in the browser, including cached files, configuration changes, cached browser information, passwords entered, and auto completed information.
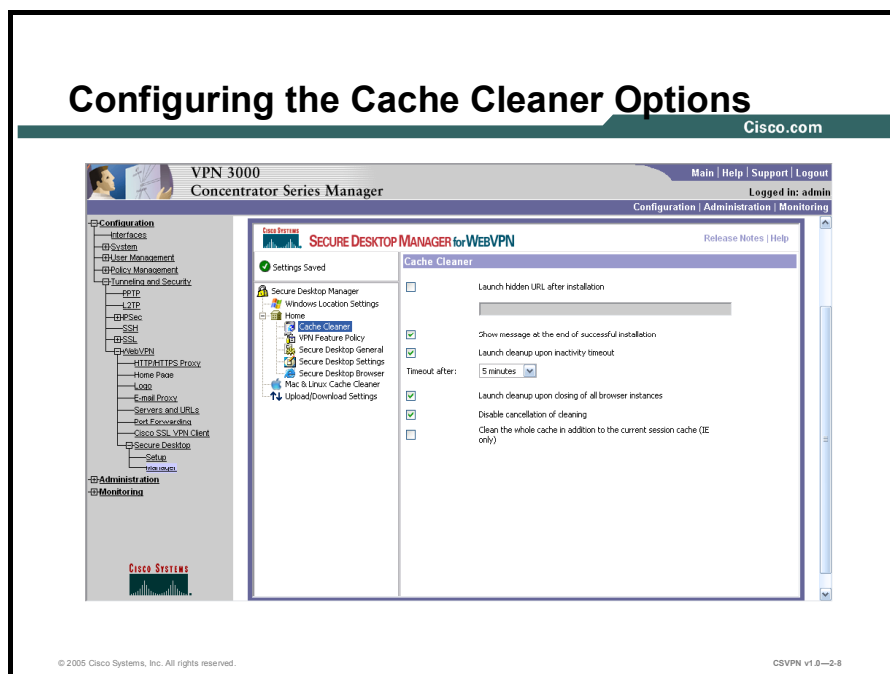
While configuring the Cache Cleaner option, you can configure the following options based on your network requirements:

- **Launch hidden URL after installation** —Select this option to enter the URL that you use for administrative purposes, to know if the client has the Cache Cleaner installed. For example, you can place a cookie file on the client's computer, and then check for the presence of that cookie.

- **Show message at the end of successful installation** —Select this option to display a message box on client's computer.

- **Launch cleanup upon inactivity timeout** —Select this option to set a specific timeout period at which the cleanup would begin. You can set the timeout period in the **Timeout after** option. This option is an inactivity timer.

- **Launch cleanup upon closing of all browser instances** —Select this option to enable a cleanup after all the browser windows are closed.

- **Disable cancellation of cleaning** —Select this option to disable the cancel feature.

- **Clean the whole cache** —Select this option to remove all the data from the Internet Explorer cache. This will remove all the data from the time of activation including all the files that were generated before the client's CSD session began.

| Note | The Cache Cleaner works with Microsoft Internet Explorer 5.0 or later on Windows 98, ME, NT 4, 2000, and XP; Internet Explorer 5.2 or later, or Safari 1.0 or later, on Macintosh (MacOS X); and Mozilla 1.1 or later on Red Hat Linux v9. |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

# Configuring the VPN Feature Policy

By using the VPN Feature Policy option in the Secure Desktop Manager, you can conditionally or unconditionally enable a feature for the Windows location. As a network administrator, you need to secure enterprise networks and data by configuring the system detection. By using System Detection, you can confirm the presence of antivirus software, personal firewall software, and Windows service packs in the client's computer as a condition to enable particular features.
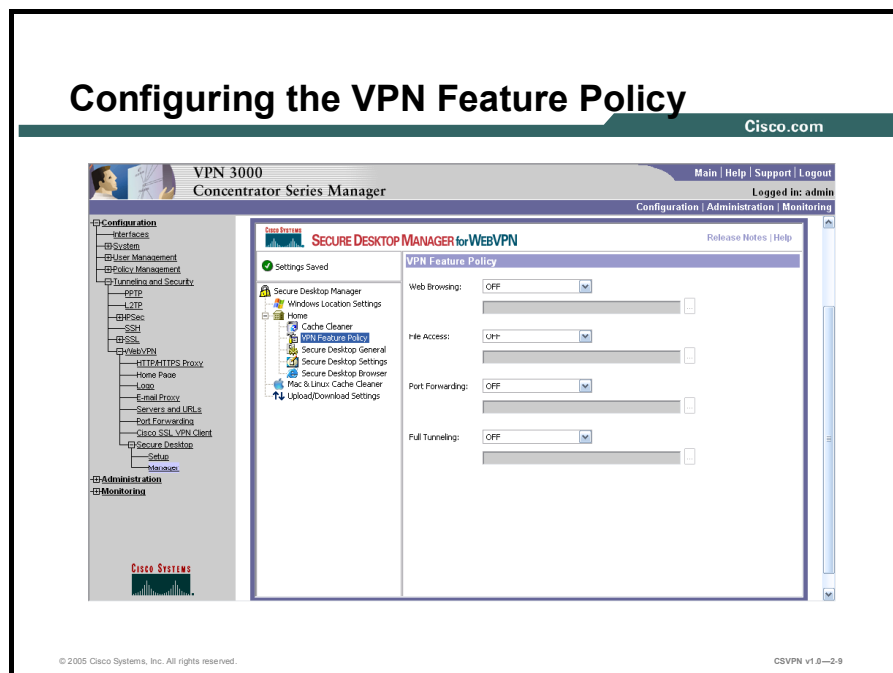


To enable a feature for the location unconditionally, you can select the **ON** option from the drop down list next to the name of the feature. If you require specified software or security to be present for the client, you can select the **ON if criteria are matched** option from the drop down list. You can then click the associated ellipsis (...) button to open the dialog window.

In this window, you can enable System Detection for antivirus software, personal firewall, service packs, and Secure Desktop or Cache Cleaner. You can click one or more of the security categories to require their presence as a condition. Then, you can enable the features selected in the previous window. For each enabled security category, you can select one of the options or multiple options. The browser will highlight the options as you select. However, you can select only one option next to the Feature category.

CSD considers the criteria within each category in a logical "OR" relationship. For example, if you specify several antivirus programs, only one of these antivirus programs will be present. The relationship between categories is an "AND" relationship, so you can select only one category. The selected category must pass the System Detection check. If you select all categories, then the client has to meet all the conditions set by the criteria. Therefore the client must have anti-virus software, a personal firewall, a service pack and a Secure Desktop feature that matches the options selected in this window.

The categories and options available in this window are as follows:

■ **Anti-Virus**—Select this option to enable System Detection for the anti-virus software. You can specify any of the anti-virus software in the list, and if one of them is available, this criterion will be met. The options among the anti-virus programs have an "OR" relationship, therefore the client's computer has to run any one of the anti-virus software programs that you have selected. System Detection checks for the following anti-virus software programs:

— eTrust Antivirus (7.0 through 2005)

— F-Secure Antivirus (2003 through 2005)

— McAfee VirusScan (8.0 through 9.0, Enterprise 7.0 through 8.0)

— Norton AntiVirus For Windows (Corporate 8.0 through 9.0, Professional 2004 through 2005)

— Panda AntiVirus Platinum (7.0 through 8.0) or Titanium 2004

— PC-cillin 2003 or 2004

— Trend Micro PC-cillin Internet Security 2004

— Microsoft Windows AntiSpyware (beta1)

■ **Firewall** — Select this option to enable System Detection for personal firewall. You can specify any personal firewall in the list, and if one of them is running, this criterion will be met. The choices among personal firewalls have an "OR" relationship. Therefore, the client's computer must be running any one of the personal firewalls that you have selected. The personal firewall software that the System Detection checks for are as follows:

— Cisco Security Agent (4.0 through 4.5)

— Internet Connection Firewall (ICF) (Windows XP through XP SP2)

— ISS BlackICE PC Protection (3.6)

— McAfee Personal Firewall (4.0 through 5.0)

— Norton Personal Firewall (2003 through 2005)

— Sygate Personal Firewall (5.0 through 5.5)

— ZoneAlarm Personal Firewall (4.0 through 5.0)

■ **OS**—Select this option to enable System Detection for a particular operating system and service pack. The choices among service packs have an "OR" relationship. Therefore, the client's computer has to run one of the operating system and service pack combination that you have selected. The operating systems and service packs that System Detection checks for are as follows:

— Windows XP

— Windows XP Service Pack 1

— Windows XP Service Pack 2

— Windows 2000

— Windows 2000 Service Pack 1

— Windows 2000 Service Pack 2

- — Windows 2000 Service Pack 3

- — Windows 2000 Service Pack 4

- — Windows NT Service Pack 6

- — Windows Millennium Edition

- — Windows 98

- ■ **Feature**—Select this option to enable System Detection for one of the two core CSD features, Secure Desktop or Cache Cleaner. You can select one of these features from the drop down list. If the CSD feature is not active in other components the client will fail when the VPN Feature Policy criteria check is performed.

# Configuring Secure Desktop General

You can configure this setting for a location name, to either enable or disable the Secure Desktop features to customize the user experience.
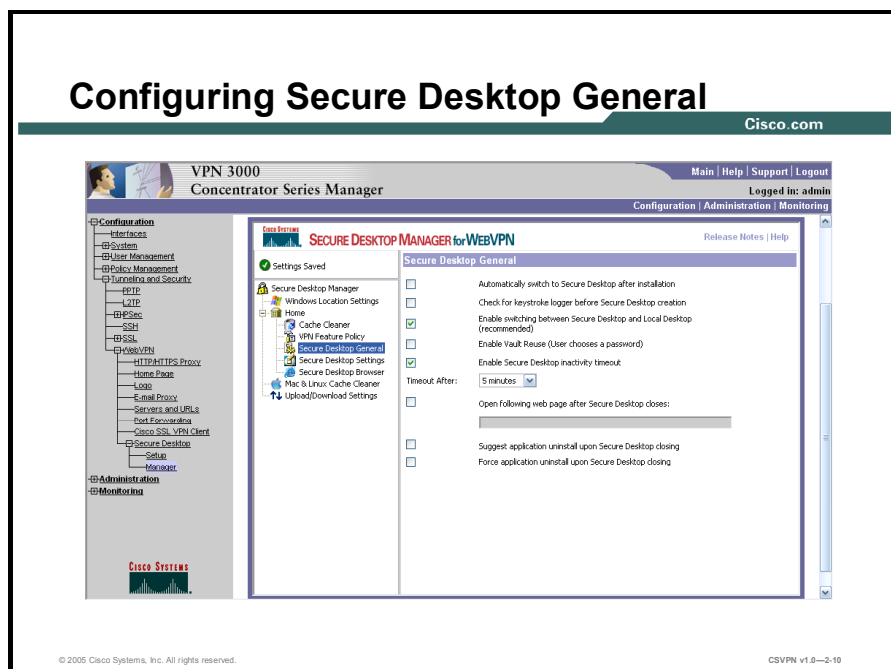


You can select the following options as required by your network:

■ **Automatically switch to Secure Desktop after Installation**—Select this option to enable Secure Desktop to load automatically after the installation.

■ **Check for keystroke logger before Secure Desktop creation**—Select this option to check if a keystroke logging application is not running on the client's computer before the Secure Desktop space is created. This feature can be enabled only in hosts, where the client has administrator privileges.

■ **Enable switching between Secure Desktop and Local Desktop**—Select this option to enable your clients to switch between the Secure Desktop and the untrusted desktop. This is known as desktop switching. This provides the clients with the flexibility of responding to a prompt from another application. To enable the CSD to continue processing your client, click the **OK** button.

---

**Note**    Deselecting this attribute eliminates the potential security risk posed by a user who leaves traces on the untrusted desktop. Thus, you may choose to deselect this option if the security risk is a bigger issue than the deployment advantages of the alternative.

---

■ **Enable Vault Reuse**—Select this option to allow users to close the Secure Desktop and open it again at a later time, creating a persistent desktop that is available from one session to the next. If you enable this option, users must enter a password (up to 127 characters in length) when CSD creates the Secure Desktop. This is useful if users are running the

Secure Desktop on computers that are likely to be reused; for example, a home computer. When a user closes the Secure Desktop, the Vault is not wiped out. If you do not enable this option, CSD automatically destroys the Vault at the end of each Secure Desktop session.

- **Enable Secure Desktop inactivity timeout**—Select this option to specify the duration of inactivity after which CSD automatically closes the Secure Desktop. Choose a value from the **Timeout After** drop down menu. Because CSD is running on the client machine, it can detect inactivity and close the Secure Desktop. Note that this works only if the **Enable switching between Secure Desktop and Local Desktop** option is checked.

- **Open following Web page after Secure Desktop closes**—Select this option and type a URL in the text box to allow CSD automatically open a web page when the Secure Desktop closes.

- **Suggest application uninstall upon Secure Desktop closing**—Select this option to prompt the user and recommend that the Secure Desktop be uninstalled when it closes. However, the user has the choice to refuse the uninstallation.

---

**Note**     Leave this option disabled for users to be able to use the Vault. By selecting this option, you can uninstall the Vault from the user's computer when the Secure Desktop closes.

---

- **Force Uninstall of application when Secure Desktop closes**—Select this option, to disable the Secure Desktop application on untrusted computers after users are done using it. CSD uninstalls when it closes.

---

**Note**     Leave this option disabled for the users to be able to use the Vault. Selecting this option uninstalls the Vault from the user's computer when the Secure Desktop closes.

---

# Configuring Secure Desktop Settings

You can click the **Secure Desktop Settings** icon for a particular location to place restrictions on the Secure Desktop experience. The **Secure Desktop Settings** window appears.
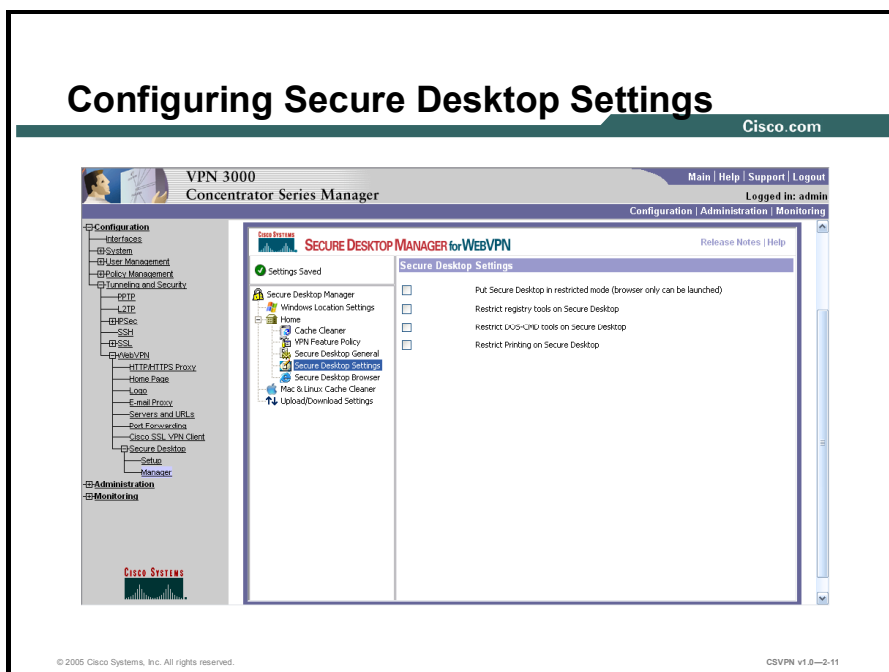


You can select the following options in this window to apply the associated restrictions:

- **Put Secure Desktop in restricted mode**—Select this option to enable only the originating browser run on the Secure Desktop. Therefore, the browser that started CSD (Internet Explorer, Netscape, Firefox, etc.) will be the only browser permitted to run in the Secure Desktop mode. By selecting this option, you can limit the client's ability to use other applications, thereby providing high security.

- **Restrict Registry tools on Secure Desktop**—Select this option to prevent the client from modifying the registry within the Secure Desktop.

- **Restrict DOS-CMD tools on Secure Desktop**—Select this option to prevent the client from running the DOS command prompt within the Secure Desktop.

- **Restrict Printing on Secure Desktop**—Select this option to prevent the client from printing while using the Secure Desktop space. By selecting this option, you can ensure that the sensitive information is always secure.

# Configuring Secure Desktop Browser Settings

You can click the **Secure Desktop Browser** icon for a particular location to customize the settings for the Secure Desktop browser.
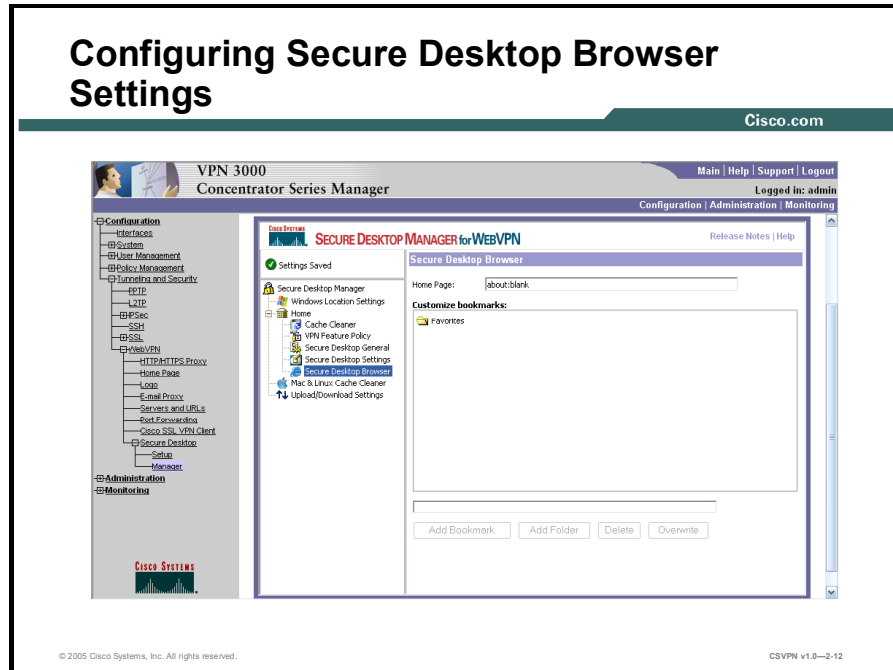


You can customize the browser settings by changing the default home page and customizing bookmarks by adding favorite URLs to the default **Favorites** folder. You can also create subfolders under the default **Favorites** folder to add a bookmark of the URLs.

# Configuring the Mac & Linux Cache Cleaner

To set up CSD for Macintosh and Linux clients, you need to configure the **Mac & Linux Cache Cleaner** option.
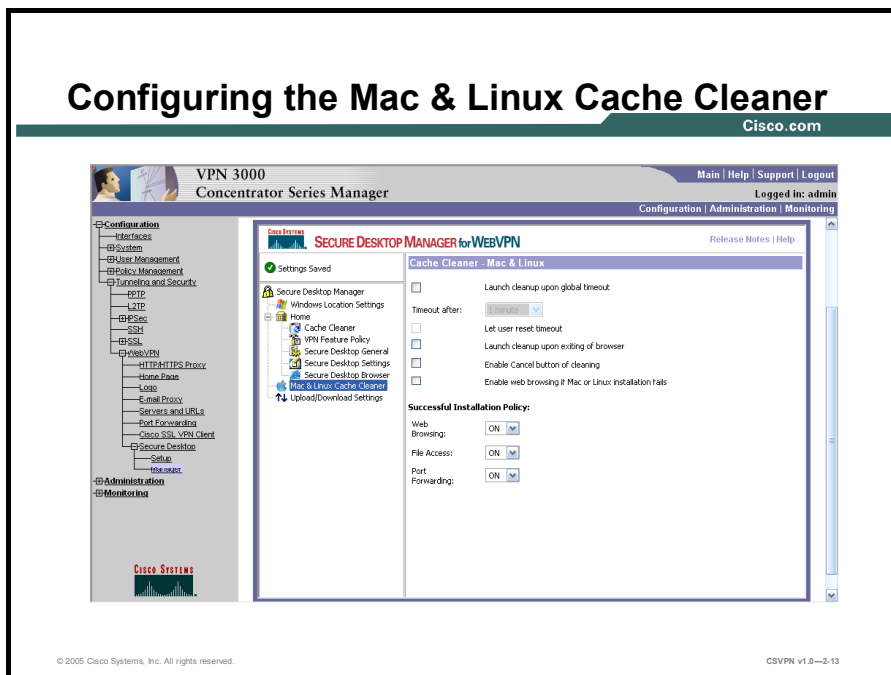


To configure the cache cleaner option for Macintosh and Linux clients, click **Mac & Linux Cache Cleaner** in the subtree on the left. The **Cache Cleaner—Mac & Linux** window appears.

In this Window, you can set the following attributes:

- **Launch cleanup upon global timeout/Timeout after** — Select this option to set a global timeout after which CSD will launch the Cache Cleaner. You can also set the timeout period from the drop-down list.

- **Let user reset timeout**—Select this option to enable your client to reset the timeout period.

- **Launch cleanup upon exiting of browser**—Select this option to launch a cache cleaning after the client closes all the browser instances.

- **Enable Cancel button of cleaning**—Select this option to enable your client to cancel the cache cleaning.

- **Enable web browsing if Mac or Linux installation fails**—Select this option to enable the remote clients to browse the web (with other remote access features disabled), if the Cache Cleaner installation fails.

- **Web Browsing/File Access/Port Forwarding**—Select ON or OFF to enable or disable these features. These attributes allows you to set the VPN Feature Policy for Macintosh and Linux users. This is similar to the way you set the VPN Feature Policy for Windows users, but without criteria checking and not on a location specific basis.

# Reusing the Configuration Settings

To reuse the Secure Desktop settings in configurations for additional secure gateways, click the **Upload/Download Settings** in the Secure Desktop Manager menu. The **Upload/Download Configuration** window appears.
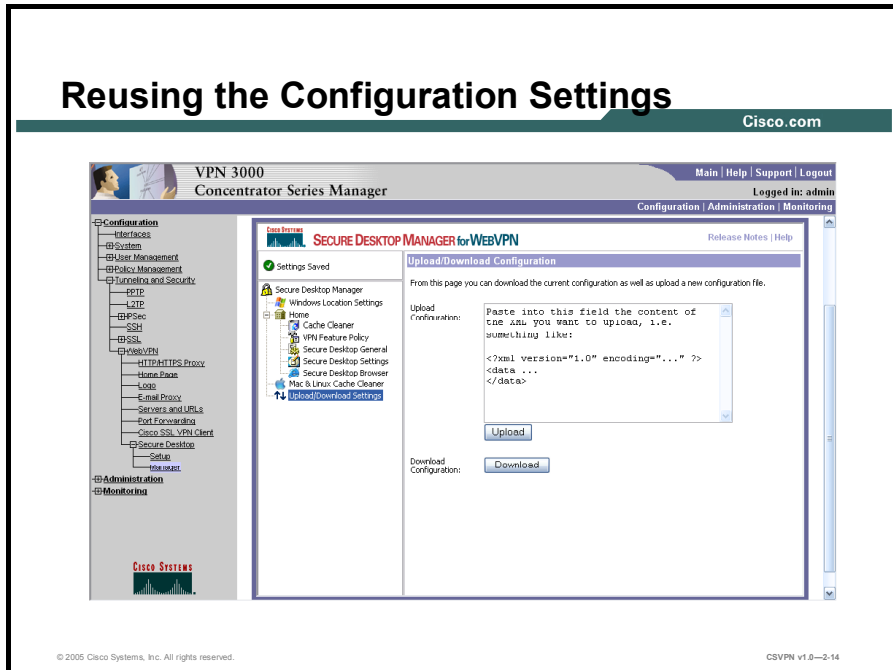


If you want to retain the Secure Desktop configuration for later retrieval for the development of additional secure gateway configurations, click the **Download** button to save the current CSD configuration in an XML format. In response, another browser window opens, displaying the current configuration as an XML file. Save the file to your local computer.

To reuse the configuration settings, Copy the contents of an XML file containing a previously saved configuration and paste it in the Upload Configuration text box, then click on the Upload button. The CSD loads the settings into the current configuration.

# Enabling Cisco Secure Desktop

This topic describes how to enable CSD in the VPN 3000 series concentrator.
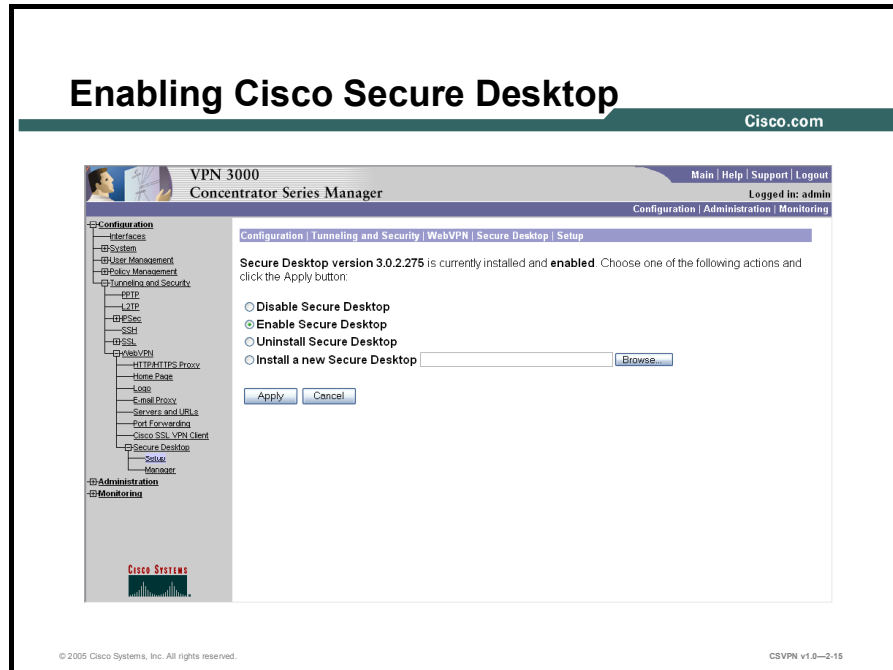


For security reasons, after you install CSD, it is not enabled by default. The threat of potential network attacks is very high, if you allow anybody to use CSD without specifying the access criteria such as antivirus, Operating System, and IP based location settings. Hence it is recommended, that you configure the Secure Desktop security policies before enabling it for the users.

To enable CSD, do the following:

**Step 1**     Connect to the VPN 3000 Series Concentrator, and log in to the VPN Concentrator Manager application.

**Step 2**     In the home page of VPN Concentrator Manager, click **Configuration** > **Tunneling and Security** > **WebVPN** > **Secure Desktop** > **Setup** window.

**Step 3**     In the **Secure Desktop window**, click the **Enable Secure Desktop** radio button.

**Step 4**     Click **Apply** and then click the **Save Needed** button to save the changes.

# Summary

This section summarizes the information you learned in this chapter.

## Summary

- **Cisco WebVPN solution offers Cisco Secure Desktop (CSD) to create a secure and customizable SSL VPN session for data theft prevention at the endpoint.**

- **CSD provides preconnection security state or "posture" assessment of the connecting device. It also offers security during the session by creating a secure virtual desktop that protects sensitive data.**

- **You need to install the securedesktop*.pkg file on the VPN 3000 concentrator, and then configure the settings before you enable it for remote users over WebVPN.**

CSVPN v1.0—2-16

# Lab Exercise—Installing and Configuring Cisco Secure Desktop

Complete the following lab exercise to practice what you learned in this chapter.

## Objectives

Your task in this lab exercise is to install and configure the Cisco Secure Desktop (CSD). Work with your lab partner to complete the following tasks:

- Complete the lab exercise setup.
- Install Cisco Secure Desktop on VPN 3000 concentrator.
- Create a Windows location.
- Configure the identification criteria for the Windows location.
- Configure the VPN Feature Policy for the Windows location.
- Enable Cisco Secure Desktop on VPN 3000 concentrator.

## Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



**Lab Visual Objective**

Cisco.com

172.26.26.P

**Student PC
Cisco VPN Client**

172.26.26.0   .100

.150   .1

**RTS**

192.168.P.0

.5

**Cisco VPN
3000 Series
Concentrator**

.5   10.0.P.0

.10

**Web FTP**

CSVPN v1.0—2-17
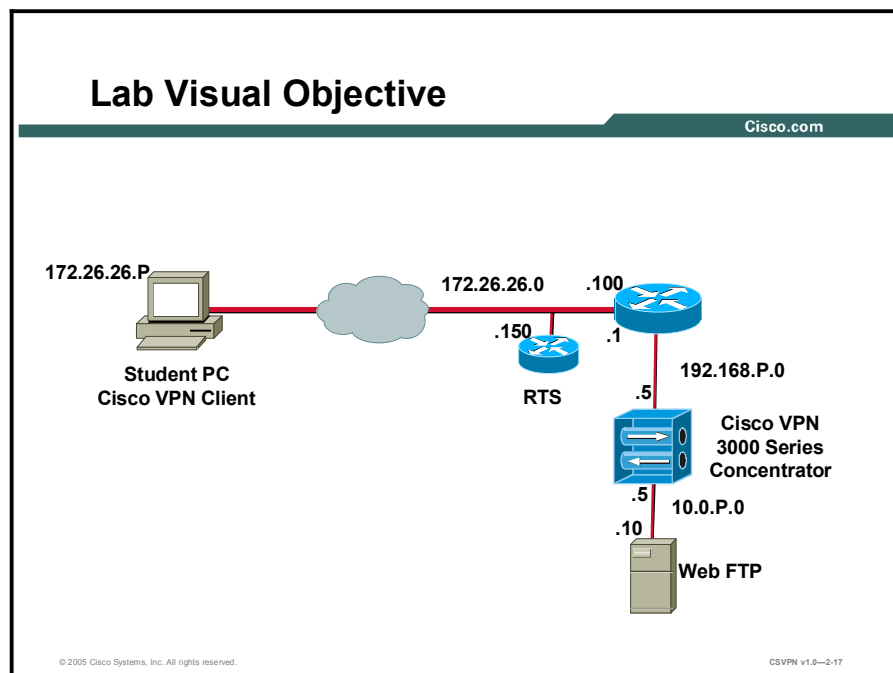
## Scenario

Your employer has asked you to provide better security for your wireless users. You will install the Cisco Secure Desktop on the VPN 3000 concentrator and configure it for the employees connecting through the wireless network.

# Task 1—Complete the Lab Exercise Setup

Before starting this lab exercise, verify your equipment as follows:

- Ensure that your student PC is powered on.

- Ensure your student PC IP addresses are configured correctly:

  — Primary IP address—172.26.26.P (where P = pod number)

  — Default gateway IP address–172.26.26.150

- Ensure that your Concentrator is powered on.

# Task 2—Installing Cisco Secure Desktop on VPN 3000 Concentrator

Complete the following steps to install CSD.

**Step 1**    Connect to the VPN 3000 Series Concentrator, and log in to the VPN Concentrator Manager application. The home page of the VPN Concentrator Manager application is displayed.

**Step 2**    In the home page of VPN Concentrator Manager, choose **Configuration** > **Tunneling and Security** > **WebVPN** > **Secure Desktop** > **Setup**.

**Step 3**    Click the **Install a new Secure Desktop** radio button.

**Step 4**    Click the **Browse** button and then locate the CSD installation file on your management PC.

**Step 5**    Click the **Apply** button. The File Upload window is displayed.

**Step 6**    When the upload success message appears, Click **Save Needed**.

**Step 7**    Click the **OK** button when the **Save Successful** message box appears.

# Task 3—Creating a Windows Location

Complete the following steps to create a new Windows location.

**Step 1**    In the home page of VPN Concentrator Manager, choose **Configuration** > **Tunneling and Security** > **WebVPN** > **Secure Desktop** > **Manager**. The **Secure Desktop Manager for WebVPN** window appears.

**Step 2**    Select the **Windows Location Settings** link.

**Step 3**    In the **Location name** textbox, type **Working Users**.

**Step 4**    Click the **Add** button. Notice that the location name is displayed in the **Locations in priority order** list.

**Step 5**    Select the **Close all opened browser windows upon installation** check box to remove unsecured Web browser sessions when CSD is installed.

**Step 6**    Click **Save**. The **Secure Desktop Manager for WebVPN** message box appears.

**Step 7**    Click the **OK** button.

## Task 4—Configuring the Identification for the Windows Location

Complete the following steps to configure the identification for the Windows location.

**Step 1**    In the **Secure Desktop Manager for WebVPN** window, select the **Working Users** link. The **Identification for Working Users** page is displayed.

**Step 2**    Select the **Enable Identification Using IP criteria** checkbox.

**Step 3**    In the **From** textbox, type **192.168.1.1**.

**Step 4**    In the **To** textbox, type **192.168.1.254**.

**Step 5**    Click the **Add** button.

**Step 6**    Uncheck the **Secure Desktop** check box from the **Use Module** options at the bottom of the window.

**Step 7**    Click **Save**. The **Secure Desktop Manager for WebVPN** message box appears.

**Step 8**    Click the **OK** button.

## Task 5—Configuring the VPN Feature Policy for the Windows Location

Complete the following steps to configure the VPN Feature Policy for the Windows location.

**Step 1**    In the **Secure Desktop Manager for WebVPN** window, select the **VPN Feature Policy** link for the **Working Users** location. The **VPN Feature Policy** page is displayed.

**Step 2**    Set all the attributes to **ON** to ensure that users connecting from the office environment have access to all the VPN features.

**Step 3**    Click **Save** to save the changes. The **Secure Desktop Manager for WebVPN** message box appears.

**Step 4**    Click the **OK** button.

## Task 6—Enabling Cisco Secure Desktop

Complete the following steps to enable CSD in the VPN 3000 concentrator.

**Step 1**    In the home page of VPN 3000 Concentrator Manager, choose **Configuration > Tunneling and Security > WebVPN > Secure Desktop > Setup**.

**Step 2**    Click the **Enable Secure Desktop** radio button.

**Step 3**    Click the **Apply** button.

**Step 4**    Click **Save Needed**. The **Save Successful** message box appears.

**Step 5**    Click the **OK** button.

# Module Summary

This topic summarizes the key points that were discussed in this module.

## Module Summary

- **Cisco VPN 3000 Series Concentrator running version 4.7 or later offers extensive application support through its dynamically downloaded Cisco SSL VPN client for WebVPN.**
- **Cisco SSL VPN Client provides secure access to the corporate network by establishing end-to-end, encrypted VPN tunnels.**
- **Cisco Secure Desktop (CSD) provides endpoint security, when a remote user accesses the corporate network through WebVPN.**
- **After installing the CSD, you need to configure the Secure Desktop Manager options before you enable it for the remote clients.**

HIPS v2.0—3-1

This module covered how Cisco VPN 3000 Series Concentrator running version 4.7 or later offers extensive application support through its dynamically downloaded Cisco SSL VPN client for WebVPN. This module first presented how to install Cisco SSL VPN Client and configure the Cisco SSL VPN Client for remote users. This module also covered how the Cisco Secure Desktop (CSD) provides endpoint security, when a remote user accesses the corporate network through WebVPN. This module then presented how to install the CSD on VPN 3000 concentrator. The module then covered how to install the CSD on VPN 3000 concentrator and how to configure options such as Windows location for different user groups, VPN Feature Policy, and Secure Desktop settings. Finally, the module ended with how to enable the CSD on VPN 3000 concentrator, after you configure the different secure desktop manager options.

## References

For additional information, refer to these resources:

- http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00803ee1f0.html#wp1756983

- http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/4_7/471con3k.htm

- http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/tsd_products_support_configure.html

- http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_chapter09186a00803ef68a.html

# Module Self-Check

Use the questions here to review what you learned in this lesson. The correct answers and solutions are found in the Lesson Self-Check Answer Key.

Q1)     Which of the following options are components of the Client Config Tab. (Choose two.) (Source: Configuring Group options Client Config Tab)

A)      Split Tunneling Policy
B)      IE Proxy Server
C)      Enable Citrix Metaframe
D)      DHCP Network Scope

Q2)     You need VPN 3000 Series Concentrator running version _____ or later for installing Cisco SSL VPN Client. (Source: Administrative Requirements for Installing Cisco SSL VPN Client)

Q3) Match each component with the appropriate tab. (Source: Configuring Group options on General Tab, Configuring Group options on Client Config Tab, Configuring Group options on WebVPN Tab)

A) Secondary DNS
B) Subnet Mask
C) Strip Realm
D) Banner
E) Apply ACL
F) Filter Script

_____ 1. General Tab

_____ 2. Client Config Tab

_____ 3. WebVPN Tab

Q4) You are a remote user, and Cisco SSL VPN Client has not been installed in the client PC. How would you go about installing the same? Arrange the steps involved in Installing Cisco SSL VPN Client in the correct order.

Enter the IP address of the VPN 3000 Series Concentrator on the web browser.
Download the sslclient-win*.pkg file to any location on your PC.
Login to the VPN 3000 Series Concentrator Manager by entering the Username and Password.
A security alert certificate dialog box is displayed. Click **Yes.**
Click **Tunneling and Security**.
Click **Configuration** menu.
Click, **Browse** button to open the **Choose File** dialog box and then click **Open** after locating the Cisco SSL VPN package file.
Click **Cisco SSL VPN Client** link to install it**.**
Click the **Install a new Cisco SSLVPN Client** option button.

A) Click, **Apply** to display the File upload window. When the **Upload complete** message appears, click **Save Needed** to save the configuration.

B) Click, **OK** button on the **Save Successful** dialog box.

C) Click **WebVPN.**

Q5) To install the CSD you will have to do the following. Arrange the steps in the correct order. (Source: Installing and Enabling the Cisco Secure Desktop.)

> Click the **Browse** button and then locate the CSD installation file on your management PC.
> In the home page of VPN Concentrator Manager, click **Configuration** > **Tunneling and Security** > **WebVPN** > **Secure Desktop** > **Setup** window.
> Connect to the VPN 3000 Series Concentrator, and log in to the VPN Concentrator Manager application.
> Click the **Install a new Secure Desktop** radio button.
> Click the **Save Needed** link on top of the page to save the settings.
> Click the **Apply** button. The CSD is installed in the VPN Concentrator Manager and a Secure Desktop Package Upload Success window is displayed.

Q6) Match the options that appear in the CSD Manager window with their settings. (Source: Secure Desktop manager Options)

A) Windows Location Settings

B) Mac & Linux Cache Cleaner

C) Upload/Download Settings

_____1.To configure the settings for Mac & Linux Users

_____2.To upload saved configurations or download the current configuration

_____3.To define the different locations that users will connect from.

Q7) A location can be based on_____. (Choose four.)(Source: Secure Desktop Manager options)

A)      Passwords entered.
         Configuration setting
         A certificate
         An IP address range.
         The presence or absence of a particular file.
         A registry entry.

Q8) Which of the following features does Cisco Secure Desktop provides. (Choose Three.) (Source: Cisco Secure Desktop-An Overview)

A) Data theft prevention.
B) Data protection.
C) Post-connection clean up.
D) Securely extends the corporate network to an authorized user.

E) Access to the corporate network from any supported browser.

# Module Self-Check Answer Key

Q1)     A, B

Q2)     4.7

Q3)     1-A, C
        2-B, D

         3-E, F

Q4)     B,  A, D, C, F, E, L, H,  I, G, J, K

Q5)     C, B, D, A, F, E

Q6)     A-3

        B-1

        C-2

Q7)     C, D, E, F

Q8)     A, B and C

---