

VPN

---

# Deploying Cisco ASA VPN Solutions

---

**Volume 1**

Version 1.0

**Student Guide**

Text Part Number: 97-2922-01




**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

**DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.**



*Students, this letter describes important course evaluation access information!*

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco Systems is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions; therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. We would appreciate a few minutes of your time to complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL directing you to a short post-course evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,

*Cisco Systems Learning*



# Table of Contents

## Volume 1

<b><u>Course Introduction</u></b>	<b>1</b>
Overview	1
Learner Skills and Knowledge	1
Course Goal and Objectives	2
Course Flow	3
Additional References	4
Cisco Glossary of Terms	4
Your Training Curriculum	5
<b><u>Evaluation of the Cisco ASA Adaptive Security Appliance VPN Subsystem</u></b>	<b>1-1</b>
Overview	1-1
Module Objectives	1-1
<b><u>Evaluating the Cisco ASA Adaptive Security Appliance Software Architecture</u></b>	<b>1-3</b>
Overview	1-3
Objectives	1-3
Cisco ASA Adaptive Security Appliance Access Control Model Refresher	1-4
Cisco ASA Adaptive Security Appliance Packet Routing Refresher	1-12
Cisco ASA Adaptive Security Appliance NAT Refresher	1-16
Cisco ASA Adaptive Security Appliance AAA Refresher	1-19
Summary	1-22
References	1-22
<b><u>Evaluating the Cisco ASA Adaptive Security Appliance VPN Subsystem Architecture</u></b>	<b>1-23</b>
Overview	1-23
Objectives	1-23
PKI Technology	1-24
The Public Key of the CA	1-32
Certificate Revocation Lists	1-34
Online Certificate Status Protocol	1-35
AAA-Based Certificate Authorization	1-35
Public Key Exchange Scalability	1-36
What Does a PKI Enable?	1-37
Comparison of Cisco ASA Adaptive Security Appliance VPN Technologies	1-38
IPsec Security Associations	1-42
IKE Phases	1-43
IKE Main and Aggressive Mode	1-43
SSL/TLS Session Establishment and Key Management	1-46
Cisco Secure Desktop	1-54
IPsec and NAT	1-59
VPN Termination on Cisco ASA Adaptive Security Appliance Network Interfaces	1-61
Packet Flow in Cisco ASA Adaptive Security Appliance VPN Functions	1-64
Cisco ASA Adaptive Security Appliance VPN Access Control Model	1-74
Cisco ASA Adaptive Security Appliance VPN Licensing	1-80
Summary	1-102
References	1-102

## **Applying Common Cisco ASA Adaptive Security Appliance Remote Access VPN**

### **Configuration Concepts** **1-103**

Overview	1-103
Objectives	1-103
Cisco ASA Adaptive Security Appliance VPN Policy Configuration	1-104
Connection Profiles	1-107
Group Policies	1-123
External Policy Storage	1-132
RADIUS Attribute Reference	1-132
Summary	1-139
References	1-139
Module Summary	1-141

### **Deployment of Cisco ASA Adaptive Security Appliance IPsec VPN Solutions** **2-1**

Overview	2-1
Module Objectives	2-1

#### **Deploying Basic Site-to-Site IPsec VPNs** **2-3**

Overview	2-3
Objectives	2-3
Configuration Choices, Basic Procedures, and Required Input Parameters	2-4
Configuring Basic Peer Authentication	2-9
Configuring Transmission Protection	2-21
Troubleshooting a Cisco ASA Adaptive Security Appliance Site-to-Site VPN	2-31
Summary	2-36

#### **Deploying Certificate Authentication in Site-to-Site IPsec VPNs** **2-37**

Overview	2-37
Objectives	2-37
Configuration Choices, Basic Procedures, and Required Input Parameters	2-38
Deploying Certificate-Based Authentication	2-42
Configuring PKI-Based Peer Authentication	2-53
Summary	2-70

#### **Deploying the Cisco VPN Client** **2-71**

Overview	2-71
Objectives	2-71
Evaluating Cisco VPN Client Features	2-72
Installing Cisco VPN Client Software	2-77
Configuring Cisco VPN Client Profiles	2-81
Adjusting the Peer Response Timeout Value	2-86
Configuring Advanced Profile Settings	2-89
Summary	2-96

#### **Deploying Basic Cisco Easy VPN Solutions** **2-97**

Overview	2-97
Objectives	2-97
Configuration Choices, Basic Procedures, and Required Input Parameters	2-98
Configuring Basic Cisco ASA Adaptive Security Appliance Cisco Easy VPN Server Features	2-101
Cisco VPN Client and IKE Policies	2-104
Crypto Maps	2-106
Configuring Group PSK Authentication	2-110
Configuring Extended User Authentication	2-116
Configuring Client Network Settings	2-123
Configuring Basic Access Control and Split Tunneling	2-133
Configuring the Cisco VPN Client	2-147
Troubleshooting Basic Cisco Easy VPN Operation	2-153
Summary	2-160

<b><u>Deploying Advanced Authentication in Cisco Easy VPN Solutions</u></b>	<b>2-161</b>
Overview	2-161
Objectives	2-161
Configuration Choices, Basic Procedures, and Required Input Parameters	2-162
Deploying Cisco VPN Client Certificate Authentication	2-164
Configuring Hybrid Authentication	2-172
Deploying Advanced PKI Integration	2-177
Troubleshooting PKI Integration	2-190
Summary	2-193
<b><u>Deploying the Cisco ASA 5505 Adaptive Security Appliance as Cisco Easy VPN Remote</u></b>	<b>2-195</b>
Overview	2-195
Objectives	2-195
Choosing Cisco Easy VPN Remote Modes	2-196
Deploying a Basic Cisco Easy VPN Remote Profile	2-201
Configuring Advanced Cisco Easy VPN Remote Features	2-208
Cisco Easy VPN Remote Side	2-217
Cisco Easy VPN Server Side	2-217
Troubleshooting the Cisco Easy VPN Remote	2-221
Summary	2-226
Module Summary	2-227





# Course Introduction

---

## Overview

The *Deploying Cisco ASA VPN Solutions (VPN) 1.0* course is a five-day instructor-led course that is aimed at providing network security engineers with the knowledge and skills that are needed to deploy virtual private network (VPN) solutions based on Cisco ASA adaptive security appliances.

## Learner Skills and Knowledge

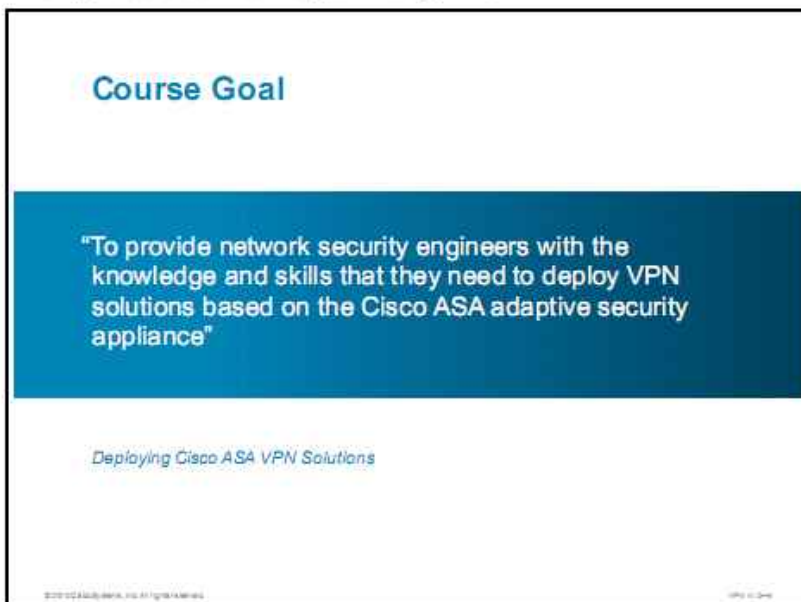
This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.

### Learner Skills and Knowledge

- Cisco CCNA certification:
  - *Interconnecting Cisco Network Devices, Part 1 (ICND1)*
  - *Interconnecting Cisco Network Devices, Part 2 (ICND2)*
- Cisco CCNA Security certification:
  - *Implementing Cisco IOS Network Security (IINS)*
- Familiarity with networking and security terms and concepts:
  - *Securing Networks with Cisco Routers and Switches (SECURE)*
- Working knowledge of the Microsoft Windows operating system

# Course Goal and Objectives

This topic describes the course goal and objectives.

A slide titled "Course Goal" with a blue header. The main content is a dark blue box containing the text: "To provide network security engineers with the knowledge and skills that they need to deploy VPN solutions based on the Cisco ASA adaptive security appliance". Below this box, the text "Deploying Cisco ASA VPN Solutions" is displayed in a smaller font. At the bottom left, there is a small copyright notice: "© 2010 Cisco Systems, Inc. All rights reserved." and at the bottom right, the text "VPN v1.0".

**Course Goal**

**"To provide network security engineers with the knowledge and skills that they need to deploy VPN solutions based on the Cisco ASA adaptive security appliance"**

*Deploying Cisco ASA VPN Solutions*

© 2010 Cisco Systems, Inc. All rights reserved. VPN v1.0

Upon completing this course, you will be able to meet these objectives:

- Evaluate the Cisco ASA adaptive security appliance VPN subsystem
- Deploy Cisco ASA adaptive security appliance IPsec VPN solutions
- Deploy Cisco ASA adaptive security appliance Cisco AnyConnect remote-access VPN solutions
- Deploy Cisco ASA adaptive security appliance clientless remote-access VPN solutions
- Deploy advanced Cisco ASA adaptive security appliance VPN solutions

# Course Flow

This topic presents the suggested flow of the course materials.

		Day 1	Day 2	Day 3	Day 4	Day 5
A M		Course Introduction	Module 2 (Cont.)	Module 3: Deployment of Cisco ASA Adaptive Security Appliance Cisco AnyConnect Remote-Access VPN Solutions	Module 4: Deployment of Cisco ASA Adaptive Security Appliance Clientless Remote-Access VPN Solutions	Module 5: Deployment of Advanced Cisco ASA Adaptive Security Appliance VPN Solutions
		Module 1: Evaluation of the Cisco ASA Adaptive Security Appliance VPN Subsystem				
Lunch						
P M		Module 1 (Cont.)	Module 2 (Cont.)	Module 3 (Cont.)	Module 4 (Cont.)	Module 5 (Cont.)
		Module 2: Deployment of Cisco ASA Adaptive Security Appliance IPsec VPN Solutions				

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

## Additional References

This topic presents the Cisco icons and symbols that are used in this course, as well as information on where to find additional technical references.



## Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at

[http://docwiki.cisco.com/wiki/Category:Internetworking\\_Terms\\_and\\_Acronyms\\_%28ITA%29](http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_%28ITA%29)

# Your Training Curriculum

This topic presents the training curriculum for this course.



You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE<sup>®</sup>, CCNA<sup>®</sup>, CCDA<sup>®</sup>, CCNP<sup>®</sup>, CCDP<sup>®</sup>, CCIP<sup>®</sup>, CCVP<sup>®</sup>, or CCSP<sup>®</sup>). It provides a gathering place for Cisco certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit <http://www.cisco.com/go/certifications>.



# Evaluation of the Cisco ASA Adaptive Security Appliance VPN Subsystem

---

## Overview

The Cisco ASA adaptive security appliance supports a wide range of network integration and access control options. The Cisco ASA adaptive security appliance also supports different types of virtual private network (VPN) features, which can be used to provide secure remote access to enterprise networks. This module provides a refresher of network integration and access control features, and provides an overview of VPN technologies that are supported by the Cisco ASA adaptive security appliance. The module also describes scalable and flexible configuration mechanisms that are available on the Cisco ASA adaptive security appliance to configure VPNs for larger numbers of users.

## Module Objectives

Upon completing this module, you will be able to assess the general properties of the Cisco ASA adaptive security appliance VPN subsystem. This ability includes being able to meet these objectives:

- Describe the operations of Cisco ASA adaptive security appliance networking functions that are needed in VPN deployments
- Describe the Cisco ASA adaptive security appliance VPN subsystem architecture
- Apply configuration functions common to all Cisco ASA adaptive security appliance remote access architectures





# Evaluating the Cisco ASA Adaptive Security Appliance Software Architecture

---

## Overview

The Cisco ASA adaptive security appliance provides a rich set of network integration, access control, and virtual private network (VPN) features that work in concert to provide multifunction security functions to an organization. As this course focuses on the VPN aspects of the Cisco ASA adaptive security appliance software and hardware, this lesson provides a refresher of baseline access control and network integration features that are required when implementing VPN functionality.

## Objectives

Upon completing this lesson, you will be able to describe the operations of Cisco ASA adaptive security appliance networking functions that are needed in VPN deployments. This ability includes being able to meet these objectives:

- Explain the Cisco ASA adaptive security appliance access control model, including security levels, NAT control, ACLs, object groups, and policies based on Cisco MPF
- Describe static and dynamic routing on the Cisco ASA adaptive security appliance
- Describe Cisco ASA adaptive security appliance NAT functionality
- Describe Cisco ASA adaptive security appliance AAA functionality

# Cisco ASA Adaptive Security Appliance Access Control Model Refresher

This topic reviews the principles of the Cisco ASA adaptive security appliance access control model.

## Cisco ASA Adaptive Security Appliance Access Control

- Cisco ASA adaptive security appliance uses a stateful packet filtering engine that supports AIC.
- Network traffic crossing the firewall is controlled through:
  - Interface security levels
  - IP routing
  - Interface ACLs
  - Service policies (configured through Cisco MPF)
  - Optionally, NAT
  - Security service modules
- Network traffic to the security appliance control plane is subject to a separate set of rules.

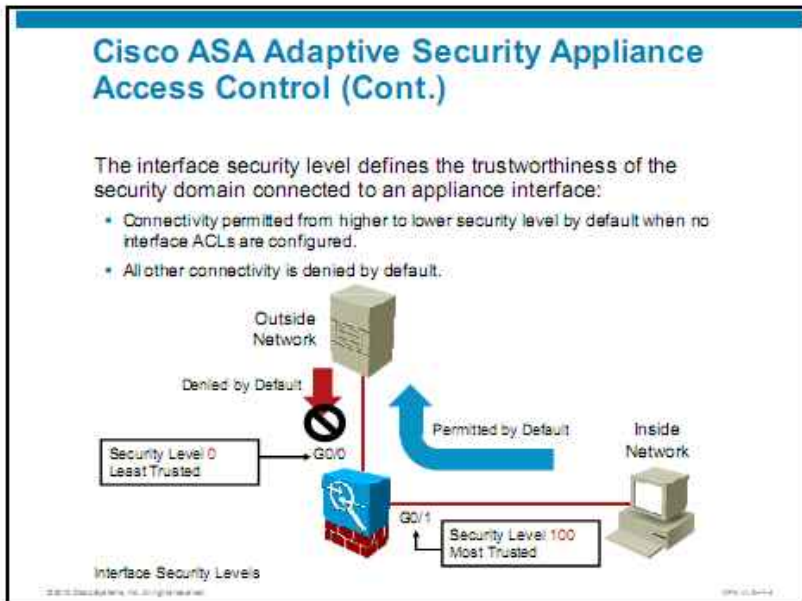
The Cisco ASA adaptive security appliance is a multifunction security appliance that primarily uses a stateful packet filtering engine that also supports Application Inspection and Control (AIC). The stateful packet filtering functionality allows the Cisco ASA adaptive security appliance to intelligently filter network traffic on Open Systems Interconnection (OSI) Layers 3 and 4 (that is, it controls which network endpoints can communicate using which applications). The AIC functionality allows the Cisco ASA adaptive security appliance to analyze application layer protocols, verify their adherence to standards, and enforce access control based on application layer protocol messages and their content.

In terms of configuration, the Cisco ASA adaptive security appliance filters network traffic that is forwarded across the appliance using the following concepts:

- Interface security levels, which define the default access policy and optional interface isolation.
- IP routing configuration, where only networks that are listed in the IP routing table are potentially accessible.
- Interface access control lists (ACLs), which define the permitted flows that are then tracked by the stateful filtering engine of the appliance.
- Service policies, configured through the Cisco Modular Policy Framework (MPF) interface, which define advanced traffic inspection features, including application layer filtering policies.
- Optionally, the Network Address Translation (NAT) functions, which can act as a layer of access control, if enabled. NAT control is disabled by default.

- Security services module, which you can optionally add to the security appliance to extend its functionality with advanced intrusion prevention and content inspection features.

Note that these features only inspect network traffic across the appliance. All management traffic that terminates on the Cisco ASA adaptive security appliance control plane is subject to a different set of controls that can limit access to the appliance itself to the minimum.



The access control model of the Cisco ASA adaptive security appliance is fundamentally based on security levels that are applied to security appliance interfaces. The higher the security level, the more trustworthy are the networks (the security domain) that are reachable over that network interface. The security level is a numerical tag that ranges from 0 (least trusted) to 100 (most trusted).

If you do not apply an ACL to a network interface, all outbound sessions (that is, sessions to all networks on lower-security-level interfaces) from the higher-security-level interface are permitted. At the same time, all inbound sessions (that is, sessions to all networks on higher-security-level interfaces) from the lower-security-level interfaces are denied. ACLs will override this default access policy once they are applied to the interfaces, and the interfaces will only permit what is specifically authorized by the ACL.

## Cisco ASA Adaptive Security Appliance Access Control (Cont.)

- Traffic between interface with the same security level is denied by default, but can be enabled.
- Useful to additionally isolate interfaces.
- Allow with the **same-security-traffic permit inter-interface** command.



By default, hosts that are reachable over different security appliance network interfaces that are tagged with the same security level cannot communicate with one another. This feature can be used to isolate several security domains from one another, if they should not be enabled to exchange traffic. While you can accomplish this action by using ACLs, the security level mechanism provides you with an independent isolation method that works even if ACLs are accidentally misconfigured (that is, if they are a defense-in-depth feature).

There are situations, however, where multiple interfaces with the same security level need to exchange traffic.

One example is an enterprise that has multiple network zones with the same level of trust. If you assign two interfaces to the same level, you can allow them to communicate (subject to ACLs) by using the **same-security-traffic permit inter-interface** command. Also, if you enable NAT control, you do not need to configure NAT between same-security-level interfaces. Another example is a security appliance that is configured with more than 101 network interfaces, where at least 2 interfaces will have the same security level.

## Cisco ASA Adaptive Security Appliance Access Control (Cont.)

- Traffic returning via the source interface is denied by default, but can be globally enabled.
- Enabled with the **same-security-traffic permit intra-interface** command.
- This is needed in special scenarios, such as VPNs (spoke-to-spoke communication via a Cisco ASA adaptive security appliance hub) and private VLANs.



Same-Interface Connectivity

By default, the Cisco ASA adaptive security appliance will not forward packets arriving at a specific interface back via the same interface, even if the IP routing table dictates such forwarding. You can disable this behavior by using the **same-security-traffic permit intra-interface** command. This is most commonly done to allow a spoke VPN client to communicate with another spoke VPN client while both VPN connections of the spoke are terminated on the same interface on the hub Cisco ASA adaptive security appliance. By allowing such traffic in and out of the same interface, or “hairpinning,” this configuration supports a hub-and-spoke VPN, with the VPNs as spokes connecting through a security appliance that is acting as a VPN hub.

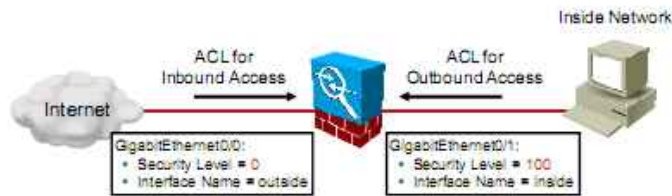
This configuration is also used to redirect incoming VPN traffic out through the same interface as unencrypted traffic. This routing is needed when the VPN client that does not have split tunneling enabled but wants to access an Internet website while connected to the VPN. If internal private address space is being used and unencrypted traffic is allowed back out the same interface where it arrived, NAT must map the internal private address to a public routable address.

Apart from VPN scenarios, this feature is used in some special cases, in which the traffic between two hosts is forced to flow via the security appliance for inspection, such as with private VLANs (PVLANS).

## Cisco ASA Adaptive Security Appliance Access Control (Cont.)

Interface ACLs control transit traffic over the Cisco ASA adaptive security appliance on OSI Layers 3 and 4:

- Interface ACLs can be assigned in both the incoming and outgoing directions on an interface.
- An ACL must describe only the initial packet of an application.
- All subsequent traffic is automatically permitted by the connection table.



Interface ACLs

ACLs, once applied to interfaces, override the default behavior that permits outbound and denies inbound traffic. When you create an ACL, the security appliance automatically applies an implicit rule at the end of the ACL. This implicit rule denies all traffic that is not explicitly permitted. ACLs can be applied in the inbound or outbound direction on an interface.

ACLs are made up of one or more access control entries (ACEs). An ACE is a single entry in an ACL that specifies a permit or deny rule and is applied to a protocol, a source and destination IP address or network, and, optionally, the source and destination ports. After an ACL is configured, it must be activated and applied to an interface with an **access-group** command.

The Cisco ASA adaptive security appliance checks only the first packet of a TCP or User Datagram Protocol (UDP) flow against its ACL configuration. Once the packet is permitted, the flow description is entered into the connection table, which can be viewed with the **show conn** command. All subsequent packets of that flow are permitted through the appliance based on the connection entry.

---

**Note** With each new connection, you see only one hit count on the corresponding ACE.

---

## Cisco ASA Adaptive Security Appliance Access Control (Cont.)

- Allows flexible configuration of advanced firewall features.
- Achieves modularity by class maps and policy maps:
  - Class maps define traffic flows:
    - Layers 3 and 4, Layers 5–7
  - Policy maps apply actions to the traffic flows:
    - Layers 3 and 4, Layers 5–7
- Service policies apply policy maps to interfaces or globally.



Cisco MPF is a configuration language that provides the granularity and flexibility to configure advanced traffic management features. This framework enables the administrator to define traffic classes at the desired granularity and apply actions (policies) to them. For examples, the administrator can identify and prioritize voice traffic, perform intrusion prevention system (IPS) inspection on specific flows of traffic, and use the default global inspection policy to perform deep packet inspection on traffic traversing the security appliance.

Cisco MPF consists of three main components:

- **Class maps:** These components are used to identify a traffic flow. A traffic flow is a set of traffic that is identifiable by its packet content and can be defined either on Layers 3 and 4 (Layer 3 and 4 class map) and, optionally, on Layers 5 through 7 (Layer 5–7 class map). For example, voice traffic from the headquarters to the branch office can be defined as one traffic flow (traffic class). Class maps are assigned to policy maps.
- **Policy maps:** These components are used to associate one or more actions with a class of traffic. For example, all voice traffic coming from headquarters to the branch office can be associated with low latency queuing. To associate an action with a specific class of traffic, create a policy map, assign a class map to the policy map, and associate an action with the class of traffic. Policy maps are applied to and activated by service policies.
- **Service policy:** These components are used to activate the policies. A service policy is not actually a policy at all; instead, it activates a policy map on a targeted interface, or globally on all interfaces. For example, a voice priority queuing policy can be applied to the outside interface.

## Cisco ASA Adaptive Security Appliance Access Control (Cont.)

### MPF Supported Features

These actions can be applied to a traffic flow:

- TCP normalization
- TCP and UDP connection limits and timeouts
- TCP sequence number randomization
- Stateful inspection and Layers 5–7 application inspection
- Forward to Cisco Content Security and Control (CSC) Security Services Module (SSM)
- Forward to Cisco Advanced Inspection and Prevention (AIP) SSM
- QoS traffic policing and shaping
- QoS priority queuing
- NetFlow export

A Layer 3 and 4 policy identifies a traffic flow via a previously defined class map and then associates an action with each traffic flow. A policy map can contain multiple policies. The security appliance supports one policy map per interface and one default global policy that is applied to all interfaces. The Layer 3 and 4 policy action options are as follows:

- Perform TCP normalization. This feature consists of advanced TCP connection settings that are designed to drop packets that do not appear normal.
- Apply configured connection constraints to TCP and User Datagram Protocol (UDP) traffic.
- Randomize TCP initial sequence number (ISN) and the resulting sequence numbers for protected servers.
- Perform a specified protocol inspection.
- Forward the traffic flow to the respective security services module for intrusion prevention or content security.
- Police and shape the bandwidth that is used by the specified flow.
- Direct the flow to the low latency queue by creating a quality-of-service (QoS) priority policy.
- Export NetFlow accounting records for specific flows.



## Cisco ASA Adaptive Security Appliance Access Control (Cont.)

### MPF Directionality

Layer 3 and 4 Action	Single Interface Direction	Global Direction
TCP normalization	Bidirectional	Ingress
TCP and UDP limits and timeouts	Bidirectional	Ingress
TCP sequence number randomization	Bidirectional	Ingress
Application inspection	Bidirectional	Ingress
CSC SSM	Bidirectional	Ingress
AIP-SSM	Bidirectional	Ingress
Input policing	Ingress	Ingress
Output policing	Egress	Egress
Shaping	Egress	—
Priority queuing	Egress	Egress

The order in which different types of actions in a policy map are performed is independent of the order in which the actions appear in the policy map. The table shows the order in which the actions are performed and the direction in which they apply once the policy is applied to an interface, or globally by using the **service-policy** command.

**Note** The **service-policy** command applies a policy map to an interface, or globally without defining the direction. The direction is implicit and depends on the action type, as shown in the table.

- In most instances, policy actions are applied to traffic as follows:
- If the policy is applied globally, actions are applied to traffic in the ingress direction only.
- If the policy is applied to a specific interface, actions are applied to traffic bidirectionally. All traffic that enters or exits the interface is affected if the traffic matches the class map for both directions.

# Cisco ASA Adaptive Security Appliance Packet Routing Refresher

This topic reviews the routing features of the Cisco ASA adaptive security appliance.

## Cisco ASA Adaptive Security Appliance Packet Routing

- The Cisco ASA adaptive security appliance supports static IP routing, which is recommended over dynamic routing in most scenarios.
- Static route appears in the routing table if the interface is up.
- Administrative distance enables floating static routes and route tracking.

Static Routing

The routing table of the security appliance can be populated by static routes and by dynamic routing protocols. Static routes appear in the routing only if the interface to which they point is up. The **route** global configuration command includes the administrative distance parameter (metric), with the default value of 1. The administrative distance (metric) can be used to configure floating (or backup) static routes. Floating static routes offer a fallback when the primary routing information is invalid and occurs typically in these two scenarios:

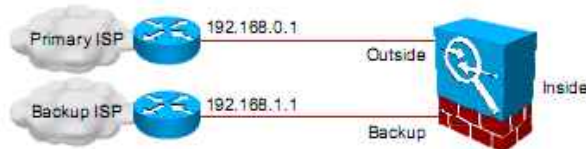
- A dynamic routing protocol is used but no routing updates are received.
- Route tracking detected that the primary route is unavailable.

In both cases, the floating (backup) static route is configured with a worse administrative distance (numerically higher than the administrative distance of the primary routing source) and is installed in the routing table only when the primary information becomes unavailable.

The Cisco ASA adaptive security appliance also supports stub multicast routing or Protocol Independent Multicast (PIM) multicast routing. However, you cannot configure both concurrently on a single adaptive security appliance.

## Cisco ASA Adaptive Security Appliance Packet Routing (Cont.)

- Static route tracking is a method for tracking the availability of the primary static route and using the backup route if the primary route fails.
- The primary static route is associated with a monitoring target.
- Target reachability is tested with ICMP echo requests.
- Uses the Cisco SLA technology.
- Can be used for monitoring DHCP and PPPoE default routes.



Static Route Tracking

One of the pitfalls that is associated with static routes is that there is no mechanism to determine whether the route is up or down. The static routes remain in the security appliance routing table even if the next hop is unavailable. Static routes on the security appliance are removed only if the interface with which they are associated goes down.

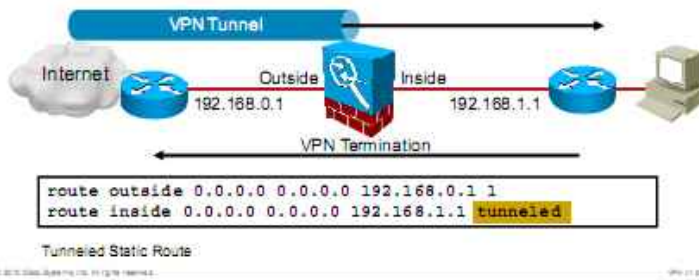
The static route tracking feature provides a method for tracking the availability of a static route and for making a secondary route available if the primary route fails. In order to achieve this redundancy, the security appliance associates a static route with a monitoring target that you define. The service level agreement (SLA) operation monitors the target with periodic Internet Control Message Protocol (ICMP) echo requests. If an echo reply is not received within a specified period, the object is considered down, and the associated route for that target is removed from the routing table. A previously configured backup route is used in place of the route that is removed. While the backup route is in use, the SLA monitor operation continues to try to reach the monitoring target. Once the target is available again, the first route is returned to the routing table and the backup route is removed.

When selecting a target, you must be sure that the monitoring target is always available to receive echo requests so that the tracked route is not unnecessarily removed. In addition, ensure that the state of your monitoring target (whether the target is reachable) is closely tied to the state of the primary ISP connection. If you choose a monitoring target that is farther away than the ISP gateway, another link along that route may fail, or another device may interfere. This configuration may cause the SLA monitoring operation to conclude that the connection to the primary ISP has failed and cause the security appliance to unnecessarily fail over to the secondary ISP link.

You can configure static route tracking for statically defined routes or default routes that are obtained through DHCP or PPP over Ethernet (PPPoE).

## Cisco ASA Adaptive Security Appliance Packet Routing (Cont.)

- A separate default route for traffic emerging from a tunnel terminating on the Cisco ASA adaptive security appliance that cannot be routed using more specific routes, learned or static.
- For traffic emerging from a tunnel, this route overrides any other configured or learned routes.
- Does not work with uRPF on the specified interface.
- Only one tunneled default route is supported.



The tunneled static route is an additional default route for managing tunneled traffic. When you create a default route with the tunneled option, all tunnel traffic that terminates on the adaptive security appliance that cannot be routed by using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides any other configured or learned default routes.

The following restrictions apply to default routes with the tunneled option:

- Unicast Reverse Path Forwarding (uRPF) using the **ip verify reverse-path** command on the egress interface of the tunneled route is not supported.
- The TCP Intercept feature on the egress interface of the tunneled route is not supported.
- You cannot define more than one default route with the tunneled option.

## Cisco ASA Adaptive Security Appliance Packet Routing (Cont.)

### Dynamic Routing Support

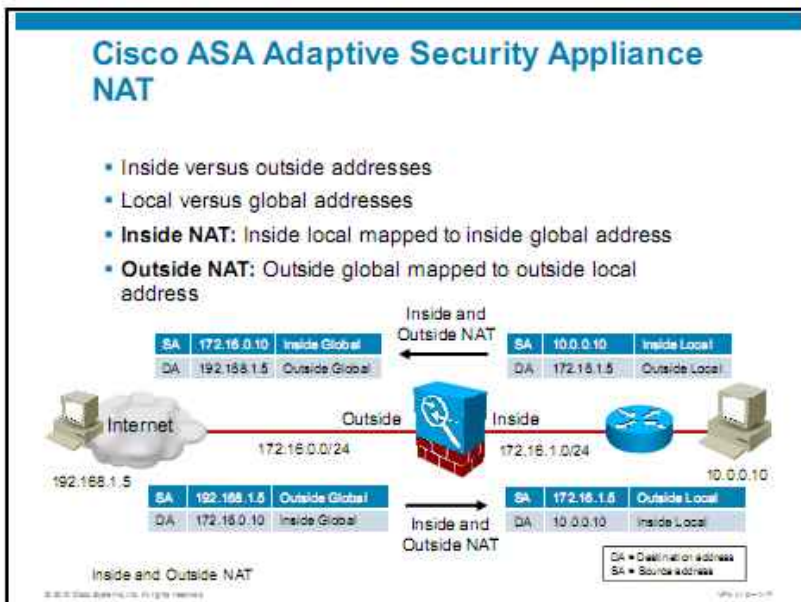
RIP	OSPF	EIGRP
Distance-vector routing protocol	Link-state routing protocol	Hybrid routing protocol that builds a topology table
Single RIP process supported	Two concurrent OSPF processes supported	Single EIGRP process supported
Supports authentication in RIP version 2 (RIPv2)	Supports authentication	Supports authentication
Supports automatic summarization only	Supports manual route summarization	Supports automatic and manual route summarization
Supports route information filtering	Supports route information filtering	Supports route information filtering
Supported only in routed single-context mode	Supported only in routed single-context mode	Supported only in routed single-context mode

The Cisco ASA adaptive security appliance supports three dynamic routing protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

# Cisco ASA Adaptive Security Appliance NAT Refresher

This topic reviews the principles of NAT on the Cisco ASA adaptive security appliance.

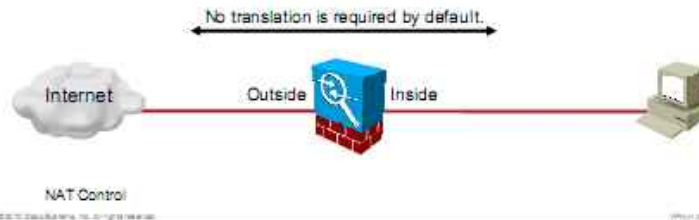


The Cisco ASA adaptive security appliance supports both inside and outside translation. The terms “inside” and “outside” describe the position of the system whose address is translated. The terms “local” and “global” define the perspective from which that system is viewed. A local address indicates that the system is seen from the inside. A global address means that it is viewed from outside. Inside translation defines a mapping between a local and global address of a system that is located in the inside network. Outside translation describes a mapping between a global and local address of a system that is located in the outside network.

The term “real address” is often used when discussing NAT. It can refer either to an inside local or to an outside global address. The term “mapped address” is also often used when discussing NAT. It can refer either to an inside global or to an outside local address. Because inside translation is far more common, real addresses are most typically the inside local addresses, and the mapped addresses are most typically the inside global addresses.

## Cisco ASA Adaptive Security Appliance NAT (Cont.)

- By default, NAT control is disabled:
  - Hosts can communicate without NAT (if ACLs permit)
  - As on a Cisco IOS router
- With NAT control enabled, traffic requires translation of inside addresses.
- With NAT control disabled, translation is still possible.

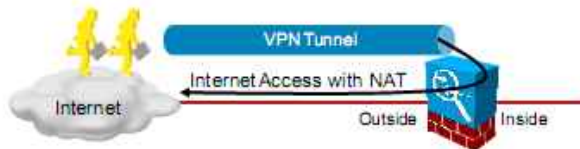


The **nat-control** global configuration command defines whether inside translation is mandatory. By default, NAT control is disabled, so the security appliance does not require inside NAT. With NAT control disabled, if a NAT rule matches the traffic, the security appliance performs the translation and forwards the packet; if no NAT rule matches, the security appliance forwards the packet anyway.

- **NAT control and inside interfaces:** If enabled, NAT control requires that packets traversing from an inside interface to an outside interface match a NAT rule. For any host on the inside network to access a host on the outside network, you must configure NAT to translate the inside host address.
- **NAT control and outside dynamic NAT:** If outside dynamic NAT or Port Address Translation (PAT) is enabled, then all outside traffic must match a NAT rule when it accesses an inside interface.
- **NAT control and same security interfaces:** Interfaces at the same security level are not required to use NAT to communicate, even if NAT control is enabled. However, if dynamic NAT or PAT is configured on a same-security interface, then all traffic from the interface to a same-security interface or an outside interface must match a NAT rule.

## Cisco ASA Adaptive Security Appliance NAT (Cont.)

- The Cisco ASA adaptive security appliance also allows NAT on a single interface (traffic enters and leaves on the same interface).
- Useful in VPN scenarios to provide Internet connectivity to remote VPN sites and users.



Same-Interface NAT

Same-interface NAT is needed in certain VPN scenarios. In the example, the security appliance terminates remote access VPN connections. The VPN clients obtain internal IP addresses from the private range, such as 192.168.0.10–192.168.0.250. The VPN clients are permitted, upon decryption, to access public servers that are located in the Internet. These features are needed for the same-interface NAT:

- The **same-security-traffic permit intra-interface** command disables the split-horizon rule for network traffic arriving on and leaving the same interface.
- A dynamic NAT configuration (the **nat** and **global** commands) is attached to just one interface, making it both the inside and outside interface at the same time.
- NAT exemption (the **nat 0 access-list** command) identifies the address ranges in the VPN sites to prevent inter-VPN traffic and traffic to resources behind the Cisco ASA adaptive security appliance from being translated.



# Cisco ASA Adaptive Security Appliance AAA Refresher

This topic reviews the authentication, authorization, and accounting (AAA) technology on the Cisco ASA adaptive security appliance.

Cisco ASA Adaptive Security Appliance AAA Refresher		
Cisco ASA Adaptive Security Appliance AAA Overview		
Authentication Features	Authorization Features	Accounting Features
Management access authentication	Management shell and command authorization	Management shell and command accounting
Authentication of a network traffic through the appliance (cut-through proxy)	Authorization of network traffic (session authorization, downloadable ACLs)	Network traffic accounting
Authentication of VPN access	Authorization of VPN access (feature control, split tunneling)	VPN access accounting

The security appliance uses its AAA subsystem to prove user identities (authentication); to determine what the user can do (authorization); and to audit the actions of the user (accounting). You can use authentication alone or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

Three types of authentication exist:

- Management AAA enables you to require authentication for users wishing to access the security appliance management functions. Secure Shell (SSH) and HTTPS are the common protocols to remotely access the appliance.
- Cut-through proxy is a technique that requires user authentication for a session through the security appliance. The session description is embedded in the **aaa authentication** global configuration command. A user at a given IP address needs to authenticate only one time, until the authentication session expires. For example, if you configure the security appliance to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, as long as the authentication session exists, the user does not have to also authenticate for FTP. The security appliance can be configured to directly authenticate HTTP, HTTPS, Telnet, and FTP cut-through sessions.
- VPN authentication requires a remote user to authenticate before using the VPN service. Once the credentials are verified, the VPN connection is completely established and the remote user is allowed to access the enterprise resources.

Three types of authorization correspond to the three authentications, respectively:

- Management shell and command authorization controls which privilege level and which commands are available to the user in the console session.
- Network access restrictions encompass a range of techniques that control access to network resources, once the user identity is established. Examples include downloadable ACLs or per-session authorization.
- VPN access restrictions are applied to an authenticated user session. The approaches differ based on the VPN technology. Split tunneling is an ACL-based filter for IP Security (IPsec) remote access VPNs, where the ACL identifies the data that must be encrypted. Traffic that is not matched by the ACL is permitted to bypass the VPN connection and access the Internet directly in cleartext. For Secure Sockets Layer (SSL) VPNs, a number of filtering techniques exist, such as URL- and Common Internet File System (CIFS)-based ACLs.

Accounting can be also configured for three types of traffic:

- Accounting of management shell and command can track shell access and commands that are used by a specific user. Each command or commands that are entered by an administrator are recorded and sent to the accounting server or servers.
- Accounting of user traffic can track user activity over the security appliance, enabling you to have a record of user activity. If you enable authentication for that traffic, you can account for traffic per user. If you do not authenticate the traffic, you can account for traffic on a per-IP-address basis.
- Accounting of VPN traffic tracks user access over VPN tunnels.

## Cisco ASA Adaptive Security Appliance AAA Refresher (Cont.)

### AAA User Databases

- Local:
  - Easy to set up
  - Not scalable
- RADIUS:
  - Combines authentication and authorization in a user profile
  - IETF, Cisco, and Microsoft VSAs
- TACACS+:
  - Authentication and authorization are separate
- LDAP
- RSA SecurID
- Kerberos
- Microsoft Windows NT

The adaptive security appliance comes with a local database that is stored on the security appliance. A local database is the easiest to set up, but it does not scale beyond the smallest network implementations. It lacks advanced features such as high availability and integration with other user databases. Furthermore, the Cisco ASA adaptive security appliance supports these server types:

- RADIUS is an extensible Internet Engineering Task Force (IETF) protocol that combines authentication and authorization in a user profile. In other words, authorization is always performed in the same step as authentication. RADIUS uses attribute-value pairs to carry data in both the request and the response for the authentication, authorization, and accounting transactions. RADIUS is extensible; many vendors of RADIUS hardware and software implement their own variants by using vendor-specific attributes (VSAs). VSA definitions from many other companies remain proprietary and ad hoc. The security appliance supports RFC VSAs, Cisco VSAs, and Microsoft VSAs.
- TACACS+ is a Cisco proprietary enhancement to the original TACACS specification that is now publicly available in the form of a developer kit. Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates the two operations. TACACS+ offers multiprotocol support, such as IP and AppleTalk. Normal operation fully encrypts the body of the TACACS+ packets for more secure communications.
- Lightweight Directory Access Protocol (LDAP) is a ubiquitous directory access protocol that is used, among others, by Microsoft Active Directory.
- RSA SecurID one-time password (OTP) solution uses two-factor authentication that is based on something you know (a password or PIN) and something you have (an authenticator), providing a more reliable level of user authentication compared to reusable passwords.
- Kerberos is a secure authentication protocol that is used in heterogeneous UNIX environments, and in Microsoft Windows networking functions.
- Microsoft Windows NT-based authentication enables the security appliance to verify user credentials against existing Microsoft Windows NT servers.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- Interface security levels and ACLs control access through the Cisco ASA adaptive security appliance, and Cisco MPF allows scalable configuration of advanced firewall features.
- The Cisco ASA adaptive security appliance supports static routes, RIP, OSPF, and EIGRP.
- NAT is optional by default, and inside NAT can be made mandatory.
- Cisco ASA adaptive security appliance supports various types of NAT.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-001-02

## References

For additional information, refer to this resource:

- *Cisco ASA 5500 Series Configuration Guide Using the CLI, 8.2* at <http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/config.html>

# Evaluating the Cisco ASA Adaptive Security Appliance VPN Subsystem Architecture

---

## Overview

The Cisco ASA adaptive security appliance provides a rich set of virtual private network (VPN) features that cover a wide range of common enterprise use cases to support mobile workers and remote offices. This lesson introduces the VPN technologies and access methods that are supported by the Cisco ASA adaptive security appliance; the integration of these access methods in the Cisco ASA adaptive security appliance traffic-forwarding engine and access control model; and the VPN licensing options of Cisco ASA adaptive security appliance appliances.

## Objectives

Upon completing this lesson, you will be able to describe the Cisco ASA adaptive security appliance VPN subsystem architecture. This ability includes being able to meet these objectives:

- Describe the basic functions and features of a PKI
- Describe the VPN technologies and key features of tunnel and clientless VPNs
- Describe the termination of VPN traffic on Cisco ASA adaptive security appliance network interfaces
- Describe the packet flow in tunnel and clientless VPNs
- Explain the access control model in tunnel and clientless VPNs
- Describe the VPN feature licensing on the Cisco ASA adaptive security appliance with the 8.2.2 release

# PKI Technology

This topic provides an overview of the deployment of the public key infrastructure (PKI).

## PKI Technology

### The Public Key Cryptography Problem

- In a VPN, public key cryptosystems can provide very strong peer authentication services.
- Entities need public keys of other entities before using any RSA-based service:
  - Over untrusted channels, public keys must be exchanged securely.
  - Public key must not be intercepted and changed during key exchange.
- Authenticity of public keys of other entities is paramount.

VPNs often use public key cryptography to provide scalable peer authentication. A common public key cryptography building block, digital signatures, is the foundation for many authentication protocols that can run over untrusted networks.

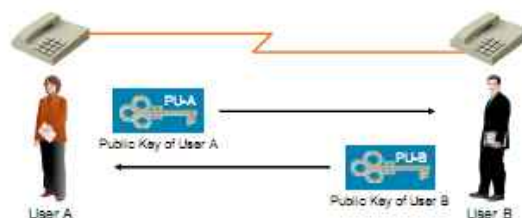
Public key cryptography, most commonly using the Rivest-Shamir-Adleman (RSA) algorithm, uses key pairs of public and private keys for its encryption and digital signature processes. Both procedures require an exchange of public keys between communicating entities. When verifying a digital signature, the verifier needs to securely obtain the public key of the signing party. If this exchange is performed over untrusted channels, the public key must not be intercepted and substituted by an attacker (a man-in-the-middle attack). While the key is public information, its authenticity and integrity must be somehow guaranteed to ensure secure transport.

## PKI Technology

### Manual Key Exchange with Verification

The simplest method for securely exchanging public keys requires OOB verification:

- Read back the received key (fingerprint) over an OOB channel (phone).
- If it matches, the key was not changed in transit.
- This method is not scalable.



One approach to solving this problem involves exchanging the public keys in the clear over an untrusted channel, but verifying the received key out-of-band (OOB) over another channel, for example, by reading the public key or its fingerprint (hash digest) back over the telephone to the sending party. This approach is rather cumbersome in practice and does not scale.

Also, public key exchanges must be made between any two communicating parties. This arrangement results in a point-to-point “mesh of trust” between parties. That is, if  $n$  parties need to communicate with each other, the amount of public key exchanges increases as a function of  $n*(n-1)$ , which means that the number of exchanges becomes too large for even a moderately sized system.

## PKI Technology

### Trusted Introduction

- Users A and B have securely exchanged public keys (with OOB verification).
- Users B and C have securely exchanged public keys (with OOB verification).
- Can users A and C exchange public keys with the help of user B?



Attempts have been made to overcome this scaling problem. Perhaps the best known is the Pretty Good Privacy (PGP) system, which is an email and file encryption system based on public key cryptography. PGP uses an interesting concept of trusted introduction, where existing point-to-point key exchanges can be tied together to soften the public key distribution problem.

In this example, users A, B, and C each have created a public and a private key pair of their own. Additionally, the following conditions exist:

- Users A and B have already securely exchanged their public keys by using the previously mentioned method (OOB verification or readback).
- Users B and C have also securely exchanged their public keys with manual verification.

At this point, users A and B (as well as users B and C) can securely exchange messages in their point-to-point relationship. They can either digitally sign them for authenticity and integrity, each with their own private key, with the other party verifying the signature with the corresponding public key; or they can encrypt them with the public key of the other party, which they already have.

Therefore, two point-to-point secure channels are provided: between users A and B, and between users B and C. Could this configuration allow the two channels to be used connect users A and C directly into their own point-to-point trust relationship?

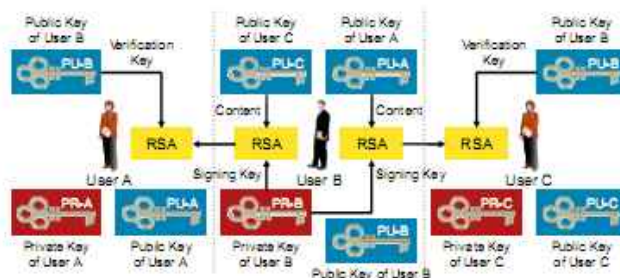


## PKI Technology

### Trusted Introduction (Cont.)

User B can act as a trusted introducer, as it is trusted by both users A and C:

- User B signs public key of user A with its own private key and sends it to user C.
- User B signs public key of user C with its own private key and sends it to user A.
- Users A and C can verify the signature, as they already had public key of user B.



It turns out that it can. User B can act as a trusted introducer, as this user has a secure channel with both users A and C. When users A and C need to exchange their public keys securely, they can do it with the help of user B, if that user is trustworthy to perform this procedure correctly.

1. User B digitally signs the public key of user A (which it has available locally) and sends it to user C.
2. User C can verify the signature of user B (as user C has the public key of user B), and can consider the public key of user A to be authentic, if user C trusts user B.
3. User B also digitally signs the public key of user C (which it has available locally) and sends it to user A.
4. User A can verify the signature of user B (as user A has the public key of user B), and can consider the public key of user C to be authentic, if user A trusts user B.

## PKI Technology

### Trusted Introduction (Cont.)

Users A and C now have the public key of each other:

- User B is their trusted introducer.



With this method, RSA public keys are signed by using RSA private keys to facilitate the secure exchange of public keys. Users A and C have now exchanged their public keys, with the help of user B. The digital signature of user B, which could be verified (as both users A and C had the public key of user B), was protecting the public keys of users A and C over an untrusted network.

This “web of trust” principle can assume various topologies of trust (combinations of point-to-point trust) and is, to some degree, scalable. However, its main pitfall lies in the fact that possibly untrained end users (users A, B, and C) make all the trust decisions and must not make any mistakes.

The next logical step, which has much better scaling properties and provides better manageability, is the use of a trusted third-party cryptographic protocol, which is a variant of the trusted introduction approach.

## PKI Technology

### Public Key Infrastructure: Certificate Authorities

PKI extends this concept and makes it scalable:

- There is only one central trusted introducer (the certificate authority).
- The certificate authority signs the public key of everyone.
- Everyone has the public key of the CA.



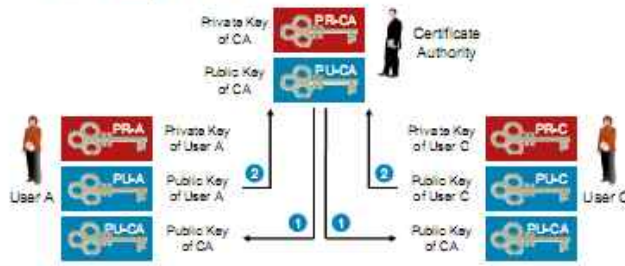
The use of a trusted third-party protocol, with public key cryptography, is also based on the digital signing of public keys and extends the concept of the trusted introducer. In this case, however, there is only one central trusted introducer (called the certificate authority, or CA) who signs all the public keys in its population (for example, servers, users, routers, and so on). Everybody trusts the CA (that is, has the public key of the CA, which is used to verify messages from the CA). The CA is a trusted third party—someone whom all participants trust and have a secure channel with, based on digital signatures.

The figure illustrates a network where each entity has a pair of asymmetric cryptographic keys, a public and a private key. Entities A and C are users who wish to communicate securely, and the CA is the trusted third party, whom all users (including users A and C) trust unconditionally. Every entity—users and the CA—has a unique pair of keys: a private and a public key, usually those of the RSA algorithm.

## PKI Technology

### Public Key Infrastructure: Certificate Authorities (Cont.)

1. Every entity gets the public key of the certificate authority ("authenticates" the certificate authority).
  2. Every entity submits its public key to the certificate authority ("enrolls into the PKI").
- This initial step must be manually authenticated, or performed over a trusted transport network.



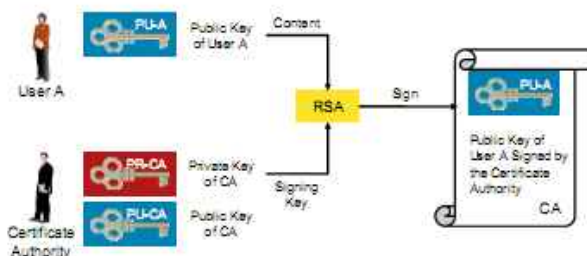
Every user in the system trusts the CA. In practice, this trust is accomplished by digital signing—what the CA signs is considered to be trusted. To verify future signatures of the CA, each user of this system must first obtain the public key of the CA, which is freely distributed among users. Users must obtain this public key in a secure manner, and be sure that the key is authentic. This step is usually called authenticating the CA.

To become a part of the system, all end users then enroll with the CA, that is, they submit their public key and their name to the CA.

## PKI Technology

### Public Key Infrastructure: Certificate Authorities (Cont.)

- The certificate authority digitally signs submitted public keys using its private key.



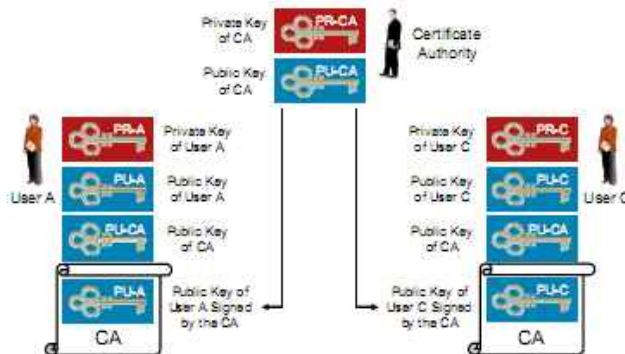
After users submit their public keys and names, the CA verifies the identity and public key of each enrolling user. If they are correct (authentic), the CA digitally signs the submitted information (name and public key) with its private key.

This process creates an identity certificate for the submitter: a piece of information that binds a name of a PKI member to its public key, packed into a standard format.

## PKI Technology

### Public Key Infrastructure: Certificate Authorities (Cont.)

- Signed public keys (**identity certificates**) are returned to entities.

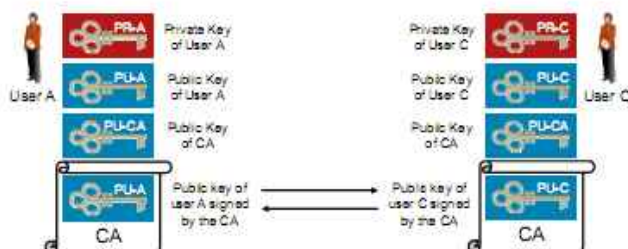


Those signed documents, identity certificates, which contain the public keys (and name) of each end user, are bound together by the signature of the CA. They are then returned to the entity, which installs them and uses them until they expire or until they are revoked.

## PKI Technology

### Public Key Infrastructure: Certificate Authorities (Cont.)

- Entities can now exchange their certificates with each other over an untrusted network.
- A received certificate is verified with the public key of the CA, which each entity must have available locally.



As every entity now has its own document (identity certificate)—containing its name and public key, signed by the certificate authority—and the public key of the certificate authority, it can verify any data that is signed by the certificate authority.

The entities can now (independently of the certificate authority) establish point-to-point relationships by exchanging information about themselves in the form of verifiable identity certificates.

In practice, this means that the end users can, after enrolling with the CA and having it sign their public keys, mutually exchange certificates over an untrusted network and use the digital signature of the CA as the protection mechanism for the public key exchange. Again, the signature of the CA is trusted because it can be verified (the entities have the public key of the certificate authority), and the certificate authority and its operations are (hopefully) secure.

Note that the exchange of identity certificates does not prove the identity of someone. Certificates only provide assurance that a particular name is connected to a particular public key. You can prove your identity by using an authentication protocol, which can in turn use certificates (and the embedded public keys) in procedures that prove the possession by the entity of the private key that corresponds to the public key in the identity certificate.

## The Public Key of the CA

The public key of the certificate authority is also distributed in the form of a certificate that is issued by the CA itself. This is also called a self-signed CA certificate, as the signer and the holder are the same entity.

## PKI Technology

- Public keys of entities, signed by the CA; certificates are public (that is, not secret) information

Certificate Format Version	Version 3
Certificate Serial Number	12457801
Signature Algorithm Identifier for CA	RSA with SHA-1
Issuer X.509 Name	C=US O=Cisco CN=CA
Validity Period	Start = 04/01/10 Expire = 04/01/15
Subject X.509 Name	C=US O=Cisco CN=CCMCluster001
Subject Public Key Information	756ECE0C9ADC7140...
Extension(s) (v3):	
CRL Distribution Points	URL=http://crl.CA.com/CACRL.crl
CA Signature	2C086C7FE0B6E90DA398AB...

X.509 Identity Certificate

An identity certificate is therefore a document, which, in its essence, binds together a name of the entity to its public key, and is signed by the certificate authority, so every other end entity will be able to verify it.

It is imperative to remember that certificates are not secret information and do not need to be encrypted in any way—their only protection is a digital signature, which proves their authenticity and integrity.

The following information is typical data that is found in an X.509 version 3 (X.509v3) identity certificate:

- The name or names of the certificate holder
- The public key of the holder
- The digital signature of the CA

Other fields include the following information:

- Certificate serial number
- Certificate expiration data
- Algorithms that are used to generate the signature
- Extensions, for example certificate revocation list (CRL) distribution points

X.509 is the ubiquitous and well-known standard, which defines basic PKI data formats, such as certificate and CRL format to enable basic interoperability.

This format is already extensively used in the infrastructure of the Internet. It is used:

- It is used with secure web servers for website authentication in the Secure Sockets Layer (SSL) protocol.
- It is used with web browsers for services that implement client certificates in the SSL or Transport Layer Security (TLS) protocols.

- It is used with user mail agents that support mail protection using the Secure/Multipurpose Internet Mail Extension (S/MIME) protocol.
- In IP Security (IPsec) VPNs where certificates can be used as a public key distribution mechanism for Internet Key Exchange (IKE) RSA-based authentication.

The figure gives an example certificate format, according to X.509v3.

PKI Technology		
Certificate Revocation Checking		
CRLs	OCSP	AAA Server Certificate Authorization
A list of revoked certificate serial numbers distributed as a time-stamped, CA-signed file	Revocation information is immediately pushed to an online database	Proprietary Cisco technology that is an alternative to OCSP
PKI entities regularly poll the CRL repository to receive the current CRL	Entities can query the OCSP server at any time to check for validity of the received certificate	Entities can query the AAA server at any time to check for validity of the received certificate
A window of opportunity for the attacker while new CRL is not yet propagated	Not widely deployed	Not integrated with the PKI—requires a separate authorization database

One of the main problems that was solved by a PKI was scalability of public key exchange. The second problem, which was also not solved by manual key exchange, was the problem of key compromise. If a certain RSA private key has been compromised, all other entities have to be signaled to no longer trust that key (and its corresponding public key).

## Certificate Revocation Lists

A PKI can offer a simple solution by using CRLs, which contain a list of all certificates that are no longer valid (that is, revoked). The CRL is signed by the CA and is time-stamped with a defined lifetime. It is stored on an HTTP server, a Lightweight Directory Access Protocol (LDAP)-accessible directory, on a Simple Certificate Enrollment Protocol (SCEP)-enabled web server, or some other available location.

It is the duty of the PKI end user to obtain a fresh CRL after the old one has expired, and to compare any certificates it wants to use against the current CRL.

A certificate is placed on a CRL if it is no longer considered trusted. A revocation of trust can be caused by many reasons:

- Private key compromise
- Contract termination for that PKI user
- Loss of private keys due to memory loss
- Device replacement



A CRL can be a single list (monolithic), which can become very large, or broken up into several smaller CRLs (multipart CRLs), accessible via different distribution points (different servers). The CRL distribution point URL for a certificate is listed in the certificate itself.

## Online Certificate Status Protocol

The main weakness of CRLs is the fact that they may contain stale information, as they are issued periodically, usually every couple of hours. If a key is compromised in the middle of that period, and a new CRL is issued soon afterward. There is a window of vulnerability when this compromised key can be used by the attacker, while the endpoints still use the old CRL (until it expires), which does not contain the compromised key.

The Online Certificate Status Protocol (OCSP) is a protocol for real-time verification of certificates against a database of revoked certificates. Upon receipt of a certificate for another user, the end user or device queries the OCSP server in real time to verify whether the received certificate has not been revoked. This approach eliminates the weakness of CRLs, but it requires a highly available OCSP server infrastructure. OCSP is not yet widely used in the network infrastructure.

## AAA-Based Certificate Authorization

Cisco supports a proprietary method using the authentication, authorization, and accounting (AAA) infrastructure, which you can use as an alternative to OCSP. By using the TACACS+ protocol, some Cisco devices can query a capable AAA server to determine revocation information in real time. This method provides real-time revocation information, but it requires the maintenance of a separate revocation database on the AAA server, as it is not integrated with common PKI revocation mechanisms.

---

**Note** Verification of certificates against a database of revoked certificates is technically not required, but it is highly recommended.

---

## PKI Technology

### Using Certificates in Network Applications

- The PKI provides a system for secure exchange of public keys:
  - Entities can establish point-to-point trust without previous mutual contact
  - Access to the CA is not required (except for revocation checking)
- Everything else is up to the application—authentic public keys can be used to:
  - Encrypt email
  - Authenticate IKE or IPsec peers
  - Authenticate web servers
  - Authenticate an IP phone to a Cisco Unified Communications Manager
  - Distribute symmetric session keys

With the introduction of the trusted third-party protocol, an efficient public key distribution model has been created. Every end entity receives its own public key that is signed by the CA, which acts as a trusted intermediary. The devised system is the underlying technical mechanism of a PKI, a service framework that is needed to support large-scale public key-based technologies.

A PKI provides a hierarchical framework for managing the digital security attributes of entities that will engage in secured communications. In addition to human users, there are encryption gateways, secure web servers, and other resources that require close control of identity and encryption.

PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Every entity (a person or device) participating in the secured communications is enrolled in the PKI in a process in which the entity generates an RSA key pair (one private key and one public key). The entity has its identity validated by a trusted entity (also known as a CA or trustpoint).

## Public Key Exchange Scalability

This system has considerably reduced the scaling complexity of public key exchange. Before this protocol was used, all possible pairs of entities needed to establish point-to-point trust, causing  $O(n^2)$  scaling properties. Now, every entity establishes point-to-point trust with the certificate authority only and trusts all other entities, which have certificates that are issued by the same authority. This process scales linearly and only requires a single procedure for each new user or device. All other relationships are automatically derived from relationship of each user to the certificate authority.

## What Does a PKI Enable?

It is extremely important to realize that a PKI is only a mechanism to securely distribute public keys between end users or entities. What you do with a particular public key of another entity is entirely up to the application itself. Applications that use PKI include the following:

- Email clients, which can look up other people certificates in a directory, verify them, extract the public key, and use it to send encrypted mail to another person without prior contact.
- VPN routers, which each have a certificate of their own and exchange them over an untrusted network when initially setting up a VPN tunnel. The public key inside a certificate is used to challenge the other peer to provide proof of the corresponding private key, and therefore authenticate it.
- Web servers, which have certificates that are issued by well-known Internet CAs. Web clients (Microsoft Windows operating system and browsers) have embedded the CA certificates of those certificate authorities. They can verify the identity of a web server by requesting its certificate at the beginning of the HTTPS session, and verify it by using an appropriate locally available (embedded) CA certificate. They can then extract its public key, and use this information to challenge the server to provide proof of its private key (usually by sending it a random piece of data that is encrypted with the public key from the certificate, and verifying that the server can decrypt it), which authenticates the server.
- In the same way as web servers, the Cisco Unified Communications Manager authenticates to the IP phone, and the IP phone to the Cisco Unified Communications Manager when using TLS-protected signaling.
- Additionally, a trusted public key from a certificate can be used to securely transport a symmetric (session) key of a symmetric algorithm (for example, Triple Data Encryption Standard [3DES], Advanced Encryption Standard [AES], and keyed Secure Hash Algorithm 1 Hashed Message Authentication Code [SHA-1 HMAC]) to the other party.

# Comparison of Cisco ASA Adaptive Security Appliance VPN Technologies

This topic describes the VPN architectures and technologies that are supported on the Cisco ASA adaptive security appliance: remote access VPNs and site-to-site VPNs, using either SSL VPN or IPsec VPN technology.

## Cisco ASA Security Appliance VPN Technologies

Remote access VPNs	Site-to-site VPNs
<ul style="list-style-type: none"><li>▪ Connect mobile users to protected resources</li><li>▪ Use client authentication and cryptographic path protection</li><li>▪ May require various user-focused security controls</li><li>▪ Must support any connectivity method and traverse any network</li></ul>	<ul style="list-style-type: none"><li>▪ Connect sites as a replacement for a classic WAN</li><li>▪ Use peer (site) authentication and cryptographic path protection</li><li>▪ Require basic network traffic controls</li><li>▪ Often work over controlled networks (MPLS) or Internet backbones</li><li>▪ Often require high availability and performance guarantees (QoS)</li></ul>

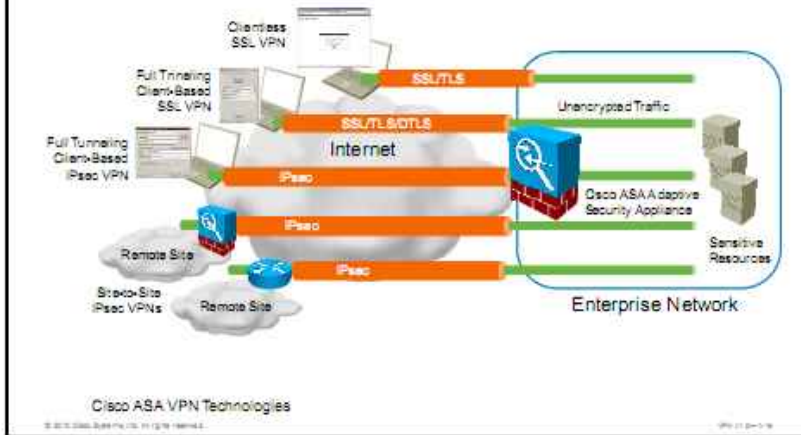
Cisco ASA VPN Services

Enterprises usually deploy VPNs in two distinct use cases: remote access VPNs and site-to-site VPNs.

Remote access VPNs generally connect individual remote users, be it enterprise employees, contractors, partners, or customers, to a set of protected resources in the enterprise internal network or a perimeter, extranet, or demilitarized zone buffer network. Remote access VPNs use strong client authentication, forcing remote users to prove their identity, and cryptographic data transmission protection across an untrusted transport network, usually the Internet. Most remote access VPNs require various security controls in addition to authentication and transmission protection. Often, VPN gateways will strictly limit access to sensitive resources; may request that remote users download additional security controls from the enterprise network; and may assess the security posture of remote clients before allowing access. Additionally, remote access VPNs must support any kind of client connectivity, as long as it has routed IP access to the VPN gateway. Remote access VPN users often operate in environments that do not natively support or allow VPN connectivity, such as behind firewalls of other enterprises.

Enterprises use site-to-site VPNs as a replacement for a classic routed WAN, to either connect geographically dispersed sites of the same enterprise, or to connect to their partners over a public network, lowering cost and providing scalable performance in the process. These site-to-site VPNs authenticate VPN peers, network devices that provide VPN functionality on behalf of an entire site, and provide transmission security between sites over an untrusted network, such as the Internet or a Multiprotocol Label Switching (MPLS) WAN. To control traffic flowing over site-to-site VPNs, VPN devices use basic firewall-like controls to limit connectivity and prevent traffic spoofing. These networks often work over more controlled transport networks, and usually do not encounter many problems with traffic filtering in transport networks between VPN endpoints. However, as these networks provide core connectivity in an enterprise network, they often have to provide high-availability and high-performance functions to critical enterprise applications.

## Cisco ASA Security Appliance VPN Technologies (Cont.)



The Cisco ASA adaptive security appliance supports various remote access VPN and site-to-site VPN technologies, differing both in the manner that these technologies encapsulate user traffic, and the way in which they provide transmission protection.

There are two major modes of user encapsulation:

- Full tunneling VPNs require VPN client software (remote access VPNs) on the remote computer, or dedicated VPN devices (site-to-site VPNs) to enable complete routed IP access to protected resources. The full-tunneling-mode VPN connections behave similarly to dedicated point-to-point links over the untrusted transport network.
- By using clientless VPNs deployment mode, available in remote access SSL VPNs, organizations have the additional flexibility of providing remote access to protected network resources even when the remote device is not managed and has no VPN client software. In clientless SSL VPN deployment, users only require a web browser acting as a VPN client, and the VPN gateway acts as a proxy device to protected network resources, providing a web portal interface with which remote users can navigate the network. Although easier to deploy than full tunneling remote access VPNs, clientless SSL VPNs provide only limited application access and may pose additional security risks to the enterprise.

There are two primary encapsulation methods for deploying VPNs: using SSL, TLS, or Datagram Transport Layer Security (DTLS), or IPsec cryptographic encapsulation protocols. Both provide comparable transmission security features.

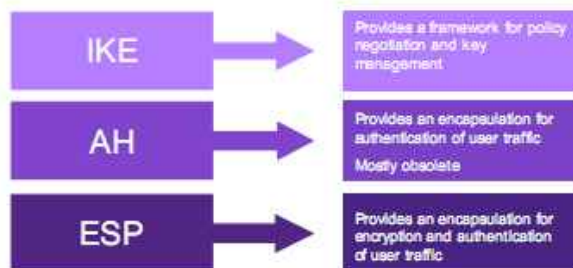
The Cisco ASA adaptive security appliance supports the following types of remote access and site-to-site VPNs:

- Clientless remote access SSL VPNs
- Full tunneling client-based remote access SSL VPNs
- Full tunneling client-based remote access IPsec VPNs
- (Full tunneling) Site-to-site IPsec VPNs

## Cisco ASA Security Appliance VPN Technologies

### IPsec VPN Building Blocks

- Defined in RFC 4301
- Combines three protocols into a cohesive security framework



IPsec is designed to provide interoperable, high-quality, and cryptographically based transmission security to IP traffic. Defined in RFC 4301, *Security Architecture for the Internet Protocol*, IPsec offers access control, connectionless integrity, data origin authentication, protection against replays, confidentiality, and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and upper-layer protocols.

IPsec provides security services at the IP layer by enabling a system that selects required security protocols, determines the algorithm (or algorithms) to use for the service (or services), and puts in place any cryptographic keys that are required to provide the requested services. IPsec can protect one or more paths between a pair of hosts, between a pair of security gateways (usually routers or firewalls), or between a security gateway and a host.

The IPsec protocol provides IP network layer encryption and defines a new set of headers to be added to IP datagrams. These new headers are placed after the IP header and before the Layer 4 protocol (typically TCP or UDP). The new headers furnish information for securing the payload of the IP packet.

IPsec combines the following security protocols:

- IKE provides key management to IPsec.
- Authentication Header (AH) defines a user traffic encapsulation that provides data integrity, data origin authentication, and protection against replay to user traffic.
- Encapsulating Security Payload (ESP) defines a user traffic encapsulation that provides data integrity, data origin authentication, protection against replays, and confidentiality to user traffic.

You can use AH and ESP independently or together, although for most applications just one of them (ESP is preferred, and AH is largely considered obsolete) is sufficient.

---

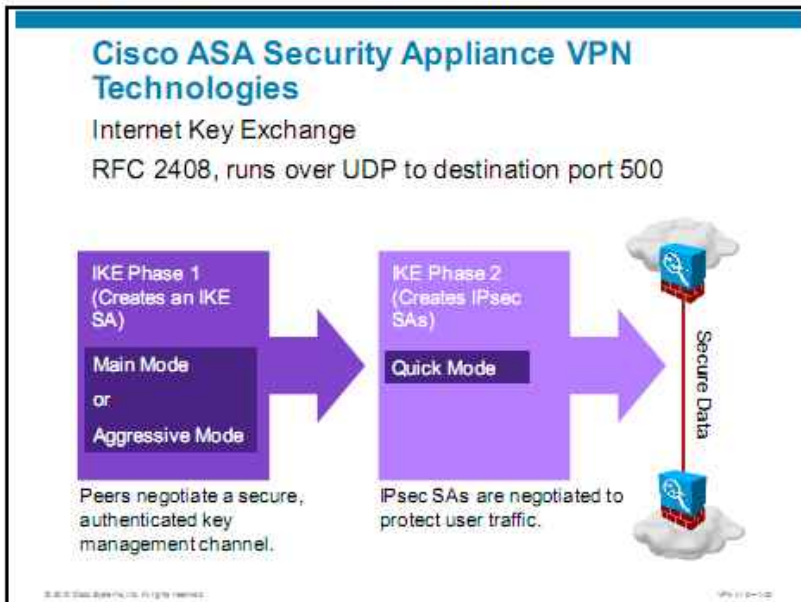
**Note** AH is not supported on the Cisco ASA adaptive security appliance.

---

## IPsec Security Associations

The concept of a security association (SA) is fundamental to IPsec. Both AH and ESP make use of SAs, and a major function of IKE is to establish and maintain SAs.

An SA is a simplex description of current traffic protection parameters (algorithms, keys, traffic specification, and so on) that are to be applied to specific user traffic flows. Security services are provided to an SA by the use of either AH or ESP. If AH or ESP protection is applied to a traffic stream, two (or more) SAs are created to provide protection to the traffic stream. To secure typical, bidirectional communication between two hosts or between two security gateways, two SAs (one in each direction) are required.



IKE is a hybrid protocol that is defined by RFC 2408 that uses parts of several other protocols (Internet Security Association and Key Management Protocol [ISAKMP], Oakley, and SKEME) to automatically establish a shared security policy and authenticated keys for services that require keys, such as IPsec. IKE creates an authenticated, secure connection (defined by a separate IKE SA that is distinct from IPsec SAs) between two entities, and then negotiates the SAs on behalf of the IPsec stack. This process requires that the two entities authenticate themselves to each other and establish shared session keys that IPsec encapsulations and algorithms will use to transform cleartext user traffic into ciphertext.

---

**Note** A potential point of confusion is that the acronyms ISAKMP and IKE are both used in Cisco IOS Software to refer to the same thing. While these two items are somewhat different, they can be considered as equivalent in this course.

---



The following are reasons to implement IKE in your IPsec configuration:

- Scalability
- Manageable manual configuration
- SA characteristics negotiation
- Automatic key generation
- Automatic key refresh

## IKE Phases

IKE operates in two distinct phases:

- **Phase 1:** The two IKE peers establish a secure, authenticated channel with which to communicate, and establish shared keying material using a Diffie-Hellman key exchange. This channel is known as the IKE (or ISAKMP) SA. Phase 1 can operate in either main mode or aggressive mode.
- **Phase 2:** In Phase 2, additional SAs are negotiated on behalf of services such as IPsec or any other service that needs key material or parameter negotiation, or both. The IPsec session keys are, by default, derived from the initial keying material that is obtained in the Phase 1 Diffie-Hellman key exchange. Optionally, they can be created by using new, independent Diffie-Hellman key exchanges if the perfect forward secrecy (PFS) feature is enabled. This Phase 2 exchange is called the IKE quick mode, which is one of two modes of IKE Phase 2. The other mode is the Group Domain of Interpretation (GDOI) mode that is used by Group Encrypted Transport (GET) VPN. It is supported on Cisco IOS routers, but not supported on the Cisco ASA adaptive security appliance.

## IKE Main and Aggressive Mode

In Phase 1, IKE can operate in either main or aggressive mode. The major characteristics of these modes are as follows:

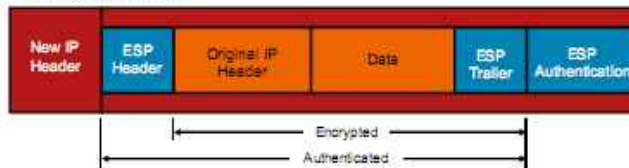
- Main mode allows for more flexible IKE protection policy negotiation, and always protects peer identity (that is, an eavesdropper cannot learn about the identity—name—of the entities that communicate by using IKE). A downside of IKE main mode is that it does not support dynamically addressed peers when performing pre-shared key (PSK) authentication, but it supports them with PKI-facilitated authentication. The only notable exception is when wildcard PSKs are used, which are strongly discouraged.
- Aggressive mode does not allow much IKE protection policy negotiation, and it does not protect peer identities—the names of communicating peers are sent over the untrusted network in the clear. The major benefit of aggressive mode is that it supports PSK authentication for dynamically addressed peers, using names (and not IP addresses) to associate credentials to a particular peer.

## Cisco ASA Security Appliance VPN Technologies

### Encapsulating Security Payload

- RFC 4303, IP protocol 50

#### Tunnel Mode ESP



The ESP encapsulation is designed to provide a mix of security services in IP version 4 (IPv4) and IP version 6 (IPv6). ESP provides confidentiality, authenticity, integrity, and antireplay by encrypting, sequencing, and authenticating the data that is to be protected, placing the encrypted data in the data portion of the IP ESP payload, and the sequencing and authentication tags at the end of the ESP-encapsulated packet.

ESP is defined in RFC 4303, *IP Encapsulating Security Payload (ESP)*.

---

**Note** Using ESP increases the IP protocol processing costs in participating systems and increases the communication latency. The increased latency is primarily due to the encryption and decryption that are generally performed for each IP datagram that contains ESP.

---

In tunnel mode, the ESP header is inserted after the tunnel IP header and before an encapsulated IP header. The Internet Assigned Numbers Authority (IANA) has assigned IP protocol 50 to ESP. The header immediately preceding an ESP header always contains the value 50 in its Next Header (IPv6) or Protocol (IPv4) field. ESP consists of an unencrypted ESP header that is followed by encrypted data.

Tunnel mode encapsulates and protects an entire IP packet. Because tunnel mode encapsulates or hides the original IP header of the packet, a new IP header must be added for the packet to be successfully forwarded. The encrypting routers own the IP addresses that are used in these new headers. Using tunnel mode leads to additional packet expansion of approximately 20 bytes that is associated with the new IP header.

## Cisco ASA Security Appliance VPN Technologies

### SSL and TLS

- Originally developed in 1994 by Netscape Communications to protect web transactions:
  - IETF enhanced SSL and named it TLS.
  - TLSv1.0 is an evolution of SSLv3.0.
  - TLSv1.0 is described in RFC 2246.
- SSL/TLS is designed to:
  - Authenticate server to client using a X.509 certificate.
  - Authenticate client to server using a X.509 certificate (optional).
  - Select common cryptographic algorithms and generate shared secrets.
  - Establish a protected SSL/TLS tunnel for TCP or UDP connections or application data.

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide transmission security for communications over networks such as the Internet. These protocols are commonly used in applications like web browsing, electronic mail, and VoIP.

The SSL protocol was originally developed by Netscape in 1994 to protect web transactions. Netscape continued the development of SSL until version 3.0, which had been released as Internet draft in 1996. In January 1999, the Internet Engineering Task Force (IETF) adopted the SSL protocol and called it Transport Layer Security, or TLS. TLS is also known as SSL version 3.1.

---

**Note** Note that TLS version 1 (TLSv1) is not compatible with SSL version 3.0 because TLS uses Diffie-Hellman and Digital Signature Standard (DSS), while SSL uses RSA. See RFC 2246 for further details.

---

Currently, almost all web browsers have implemented SSL version 3 (SSLv3) or TLSv1. Many other applications, including Cisco VPN Clients, also use SSL/TLS for transmission protection.

SSL/TLS provides endpoint authentication both for the client and the server; data encryption to ensure that it is only readable by the intended recipient; and data integrity and data authentication to ensure that the data has not been modified in transit. These services allow traffic to be protected as it traverses public network segments such as the Internet.

SSL/TLS is designed to do the following:

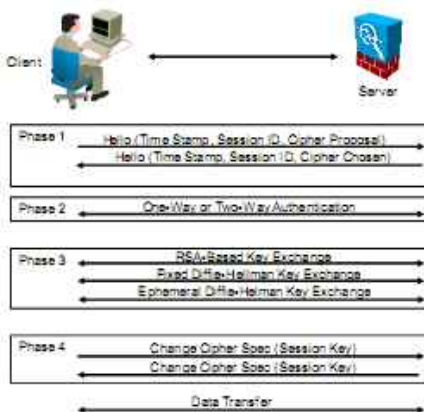
- Authenticate the server to the client
- Authenticate the client to the server (optional)
- Select joint cryptography algorithms
- Generate shared secrets
- Establish a protected path (an SSL/TLS tunnel) to provide protection to applications data or TCP and UDP connections

## Cisco ASA Security Appliance VPN Technologies

### Session and Key Management

#### SSL/TLS session establishment phases:

- Negotiation of parameters between client and server
- One-way or mutual authentication between client and server
- Creation of session key and activation of cipher suite



The SSL and TLS protocols work in two distinct planes: the session establishment phase, in which the negotiation of parameters and peer authentication takes place, and a data transfer phase that provides a protected path between the client and the server. Both of these phases occur inside the SSL/TLS Record Protocol.

## SSL/TLS Session Establishment and Key Management

### Phase 1: Establish Client-Server Security Capabilities

In phase 1 (initiated by the client), hello messages are exchanged between the client and the server to negotiate parameters, including authentication and encryption algorithms. These messages include whether RSA or Diffie-Hellman will be used as the key exchange method. The following key exchange methods are supported:

- RSA, where a shared secret is encrypted using the public key of each other.
- A fixed Diffie-Hellman key exchange, which relies on a fixed public-Diffie-Hellman value that is contained in a certificate.
- An ephemeral Diffie-Hellman key exchange, which uses the actual public-Diffie-Hellman value that is signed with the private key of the sender. This method provides the best protection because every session will have a different set of generated keys.
- An anonymous Diffie-Hellman key exchange, without certificates or signatures. This method cannot prevent man-in-the-middle attacks and should be avoided.

### Phase 2: Server Certificate and Key Exchange

In phase 2 (initiated by the server), one- or two-way authentication between the client and the server is performed. The server begins this phase by sending its certificate to the client. Unlike most other authenticated solutions where server authentication is typically optional, with HTTP and SSL, it is client authentication that is optional. A premaster key is also sent by the client using the public key of the server to start protecting the session if RSA is used.

### Phase 3: Client Certificate (If Required) and Key Exchange

In phase 3 (initiated by the client), if client authentication is required, the client sends its certificate to the server, the session key is calculated, and the cipher suite is activated. HMAC is used to protect the integrity of the data transfer using either keyed SHA-1 or keyed Message Digest 5 (MD5). Confidentiality is provided using Data Encryption Standard (DES)-40, DES-Cipher Block Chaining (CBC), 3DES-Encrypt-Decrypt-Encrypt (EDE), 3DES-CBC, RC4-40, or RC4-128.

### Phase 4: Finish

In phase 4, the data transfer starts, beginning with the exchange of session keys.

Session keys are created either using:

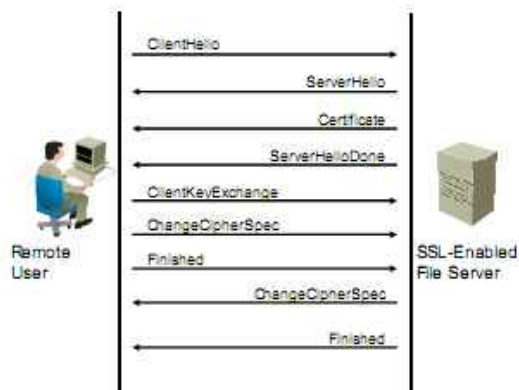
- RSA, where a shared secret is encrypted using the public key of each other.
- A fixed Diffie-Hellman key exchange, which relies on a fixed public Diffie-Hellman value that is contained in a certificate.
- An ephemeral Diffie-Hellman key exchange, which uses the actual public Diffie-Hellman value that is signed with the private key of the sender. This method provides the best protection because every session will have a different set of generated keys.
- An anonymous Diffie-Hellman key exchange, without certificates or signatures. This method cannot prevent man-in-the-middle attacks and should be avoided.

Each SSL session is uniquely identified by a session ID that is exchanged during the authentication process. The SSL session ID is used to differentiate between new and old sessions. Old sessions might exist because session IDs can be cached, but usually not longer than 24 hours.

SSL also has the ability to resume a previously negotiated session if TCP communication between a client and a server is interrupted. During the initial exchange between the SSL client and the server, the server gives the client a session ID that helps the server keep track of that SSL session. The client can ask that the server resume the SSL session without having to renegotiate parameters.

## Cisco ASA Security Appliance VPN Technologies

### Server Authentication



SSL server-side authentication is used when a client needs to verify the identity of a server. This type of authentication is commonly used for servers that require secured transactions to protect user data or account information for online purchases.

The client starts the exchange by sending a client hello message to the server to let the server know that the client wants to establish secure communications. It also proposes a list of security parameters (cipher suites) that the client would like to use.

The server sends a server hello message that informs the client of the preferred cipher suite. In addition, it tells the client that the server is willing to proceed with the SSL negotiation. The server replies immediately with a certificate message (carries the public key certificate of the server).

A trusted certificate authority (CA), such as VeriSign, typically issues this server-side certificate. The client must verify the certificate to ensure that it has been issued by a trusted CA, has not expired, or has not been revoked.

The server then sends a server hello done message to the client. This message tells the client that the server has finished its part of the initial negotiations.

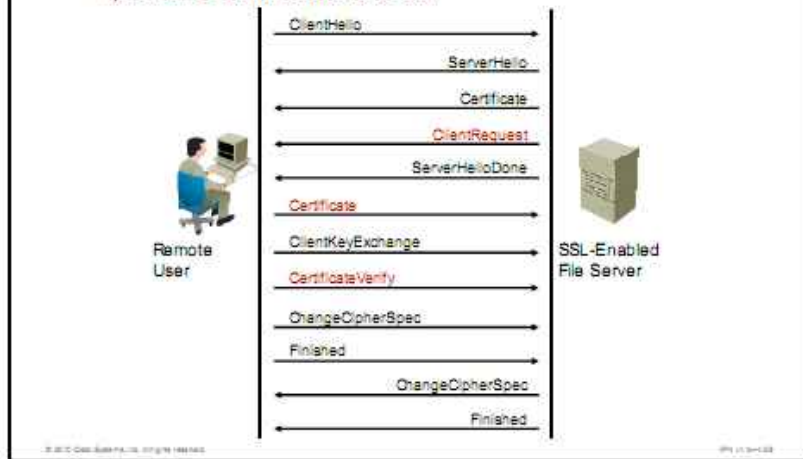
The client generates random numbers to use as a shared session key. In a client key exchange message, the client encrypts the session key with the public key of the server and sends the result to the server. The client depends on the ability of the server to decipher the client key exchange message to verify the identity of the server.

The client now sends a change cipher spec message that tells the server to activate the negotiated cipher suite. From now on, all messages from the client are encrypted using the algorithm from the server hello and the session key in the client key exchange. The client sends an encrypted finished message, which ensures that both parties use the same cryptographic algorithms and parameters. The negotiation is considered to be successful when the message that follows the change cipher spec of the client is successfully decrypted as a finished message.

The server sends a change cipher spec message that tells the client that all subsequent messages from the server will use the negotiated security. The server then sends its own finished message, which enables the client to confirm that the negotiated security is in place.

## Cisco ASA Security Appliance VPN Technologies

### Optional Client Authentication



Optionally, the server can authenticate the client, in addition to the server being authenticated. Authenticating the client ensures that the user is allowed to connect to the requested network resource. Client-side authentication is common when connecting end users to a remote access VPN using SSL.

When an SSL client must be authenticated in addition to the server, the protocol flow is almost the same. There are only a few additional required exchanges.

After the server sends its certificate to the client, the server will request that the client send its certificate in return. After the client sends the client key exchange, the client sends a certificate verify message. The client encrypts a known piece of plaintext by using its private key. The server uses the client certificate to decrypt the message. Successful decryption of the message indicates to the server that the client has the proper private key.

## Cisco ASA Security Appliance VPN Technologies

- SSL/TLS Record Protocol:
  - Partitions data stream into records.
  - Each record is protected separately.
- Each record consists of header, data, and HMAC:
  - Data and HMAC are encrypted.
  - Supports TCP or UDP (DTLS) transport.



Transmission Protection

© 2010 Cisco Systems, Inc. All rights reserved.

VPN 01-08

The SSL/TLS Record Protocol provides cryptographic envelopes to data that is transferred between the SSL/TLS client and the SSL/TLS server. Application data is split into discrete chunks that are cryptographically protected, and a header and trailer are added. A series of SSL records is then forwarded to the TCP or UDP layer that provides a transmission for the session. The UDP encapsulation is defined in the DTLS standard that provides a connectionless transport service that can efficiently transport real-time data.

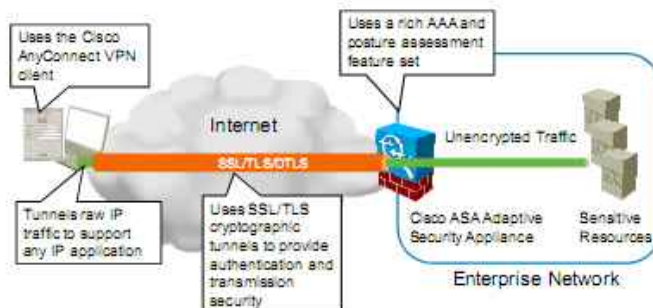
**Note** DTLS is described later in the course.

Four record types are defined to implement signaling and secure data exchange. One record contains up to 16,384 data bytes. Special record types are used for handshake, signaling cipher change, and alert messages. Each record consists of a header, a data portion, and an HMAC. Both the data and the HMAC are encrypted. Optionally, the data can also be compressed.



## Cisco ASA Security Appliance VPN Access Methods

### Full Tunneling Client-Based Remote Access SSL VPN: Features



The first remote access VPN architecture that is supported by the Cisco ASA adaptive security appliance is the full tunneling (client-based) remote access SSL VPN architecture. In this architecture, remote users use the Cisco AnyConnect VPN Client to establish an SSL/TLS tunnel with the Cisco ASA adaptive security appliance. After bidirectional authentication, the appliance applies a set of authorization and accounting rules to the user session, and may deploy advanced security controls, such as a posture assessment using Cisco Secure Desktop to the VPN session. After the security appliance establishes an acceptable VPN environment with the remote user, the user can forward raw IP traffic into the SSL/TLS tunnel, as the Cisco AnyConnect client creates a virtual network interface on the client to provide this functionality. The client can use any application to access any resource behind the Cisco ASA adaptive security appliance VPN gateway, subject to access rules applied to the VPN session.

## Cisco ASA Security Appliance VPN Access Methods

### Full Tunneling SSL VPN: Benefits and Limitations

Benefits	Limitations
Supports any IP application	Requires Cisco AnyConnect client software
Requires little user training	Requires administrative rights for the initial client installation (not for updates)
Supports low-latency operation (DTLS)	
Can traverse most firewalls and NAT devices	
Uses a typically more trustworthy managed client	
Auto updates	

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-00-000

The full tunneling remote access SSL VPN architecture has the following benefits:

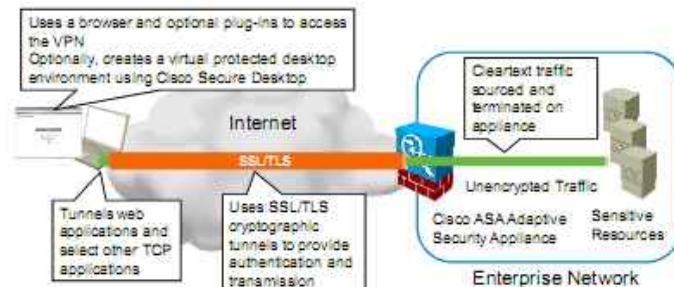
- It supports any IP application without application modification. As any full tunneling VPN, its transparency creates the illusion of being in the protected network and having unrestricted access to resources, policy permitting.
- It does not require any user training, except for initiating and terminating the VPN connection.
- It supports low-latency forwarding and enables the use of real-time applications, such as IP voice and real-time video. The use of DTLS encapsulation is recommended to support such applications.
- It can traverse most firewalls and Network Address Translation (NAT) devices, as the SSL VPN encapsulation uses the HTTPS port (TCP port 443) and is indistinguishable from an HTTPS session to the transport network operator.
- As it is limited to users having the Cisco AnyConnect VPN Client, it is mostly used on managed devices that are typically more trustworthy compared to unmanaged devices.
- The auto-update feature enables the security appliance to automatically push updates to the Cisco AnyConnect clients.

However, the full tunneling remote access SSL VPN architecture has some limitations:

- It requires that users install the Cisco AnyConnect VPN Client on their systems.
- It requires administrative privileges to initially install the VPN client application, as the VPN client needs to modify the local network interfaces and IP stack in order to work. Auto updates do not require administrative privileges.

## Cisco ASA Security Appliance VPN Access Methods

### Clientless Remote Access SSL VPN: Features



The second remote access SSL VPN architecture that is supported by the Cisco ASA adaptive security appliance is the clientless remote access SSL VPN architecture. In this architecture, remote users use the web browser to establish an SSL/TLS session with the Cisco ASA adaptive security appliance. After bidirectional authentication, the user is presented with a web portal, and the Cisco ASA adaptive security appliance applies a set of authorization and accounting rules for the user session. The appliance may also deploy advanced security controls, such as a virtual desktop or a posture assessment to the VPN session.

Clientless SSL VPNs do not offer the full network access that is provided by full tunneling VPNs. To enable remote users to access enterprise applications, the security appliance acts as a proxy. It transforms web and some nonweb applications so that they can be SSL-protected. The security appliance offers several techniques to facilitate resource and application access:

- URL and Common Internet File System (CIFS) file access is provided. When the client browser establishes the SSL session and the user authenticates, the gateway can present a page with resource bookmarks. These bookmarks allow the user to access preconfigured web pages or file shares. The user can also enter the address of the resource and be redirected to it.
- Applications plug-ins, also referred to as thin-client connections, exist for well-known applications, such as Route Discovery Protocol (RDP), Telnet, Citrix, Virtual Network Computing (VNC) and Secure Shell (SSH). They allow the user to launch a Java application plug-in inside the browser and connect to an internal server running that application.
- Port forwarding provides access to TCP-based applications by mapping application-specific ports on the remote computer to application-specific ports on internal servers. Port forwarding requires a downloaded Java applet that listens to ports on the client machine and then to forwards the connection to the gateway.
- Smart tunnels are connections between an application and a remote site, using a clientless SSL VPN session as the pathway. A successor technology to port forwarding, smart tunnels do not require administrator privileges on the remote computer. Clientless VPN users can run Winsock2 TCP applications just like full tunnel SSL VPN client access.

- The email proxy feature allows users of SSL/TLS-enabled email clients to use the security appliance as an SSL/TLS proxy, by configuring their email clients to authenticate to the security appliance, which in turn forwards their sessions to internal servers.

These techniques are covered in detail later in the course.

## Cisco Secure Desktop

The Cisco Secure Desktop is a security control that can provide virtual desktop and posture assessment features to full tunneling or clientless SSL VPNs:

- The Secure Vault feature encrypts the data and files that are associated with or downloaded during the remote session into a secure desktop partition. It also presents a graphical representation of a desktop that includes an image of a lock to signify a safe environment in which the remote user can work. Upon session termination, the partition is deleted.
- The Host Scan module installs on the remote device after the user connects to the security appliance, before the user logs in. It checks for the presence of required end-system software, including antivirus, personal firewall, and antispyware applications and updates.
- The Keystroke Logger Detection and host emulation detection module denies VPN access when it detects the presence of a suspected keystroke logging application or a host emulator.

Cisco Secure Desktop functionality is available for all types of SSL VPNs, but is not supported for IPsec VPNs.

## Cisco ASA Security Appliance VPN Access Methods

### Clientless SSL VPN: Benefits and Limitations

Benefits	Limitations
Does not require SSL VPN client software	Does not support all IP applications
Can traverse most firewalls and NAT devices	Requires some user training to access resources
Does not require administrative rights at any time	Does not support low-latency operation
Supports access from unmanaged systems	

The clientless remote access SSL VPN architecture has the following benefits:

- It can traverse most firewalls and NAT devices, as the SSL VPN encapsulation uses the HTTPS port (TCP port 443) and is indistinguishable from an HTTPS session to the transport network operator.
- It requires that users install a VPN client on their systems.
- It requires administrative privileges to install the VPN client application, as the VPN client needs to modify the local network interfaces and IP stack in order to work.
- It allows access from endpoints that are not enterprise managed.

However, the clientless remote access SSL VPN architecture has some limitations:

- It does not support all IP applications, although the majority of web-based client-server enterprise applications are supported.
- It may require user training, as the manner in which users access some resources may change.
- It does not support low-latency forwarding and the use of real-time applications due to its proxying nature.

## Cisco ASA Security Appliance VPN Access Methods

### Remote Access IPsec VPN: Features



The third remote access VPN architecture that is supported by the Cisco ASA adaptive security appliance is the full tunneling (client-based) remote access IPsec VPN architecture. In this architecture, remote users use the Cisco SSL VPN Client to establish an IPsec tunnel with the Cisco ASA adaptive security appliance. Just like with the tunneling remote access SSL VPN, after bidirectional authentication, the Cisco ASA adaptive security appliance applies a set of authorization and accounting rules to the user session. After the Cisco ASA adaptive security appliance establishes an acceptable VPN policy for the remote user, the remote user can forward raw IP traffic into the IPsec tunnel. The client can use any application to access any resource behind the Cisco ASA adaptive security appliance VPN gateway, subject to access rules that are applied to the VPN session.

## Cisco ASA Security Appliance VPN Access Methods

### Remote Access IPsec VPN: Benefits and Limitations

Benefits	Limitations
Supports any IP application	Requires IPsec VPN client software
Requires little user training	Requires administrative rights for initial installation and updates
Supports low-latency operation	Cannot traverse many firewalls with default configuration
Uses a typically more trustworthy managed client	
Free license	

The full tunneling remote access IPsec architecture has these benefits:

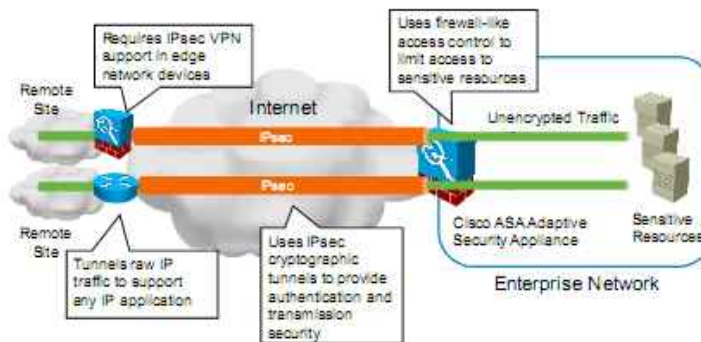
- It supports any IP application without application modification.
- It does not require any user training, except for initiating and terminating the VPN connection.
- It supports low-latency forwarding and enables the use of real-time applications, such as IP voice and real-time video, as IPsec is, by default, a connectionless protocol.
- Because it is limited to users having the IPsec VPN client, it is mostly used on managed devices that are typically more trustworthy than unmanaged devices.
- It does not require a license.

However, a full tunneling remote access IPsec VPN architecture has some limitations:

- It requires that users install a VPN client on their systems.
- It requires administrative privileges to install the initial VPN client application and for the updates.
- It has issues traversing many firewalls, as IPsec and IKE traffic may not, by default, be allowed across enterprise firewalls, behind which a remote user may be located.

## Cisco ASA Security Appliance VPN Access Methods

### Site-to-Site IPsec VPN: Features



Enterprises often want to secure the communications between different branches of the same or different organizations using (full tunneling) site-to-site VPNs. The Cisco ASA adaptive security appliance supports IPsec as the encapsulation method for site-to-site VPNs. It also interoperates with standard IKE and IPsec VPN peers, such as Cisco IOS Software routers and third-party IPsec VPN devices.

In this architecture, remote networks use an IPsec VPN device, a VPN gateway, to establish an IPsec tunnel with the Cisco ASA adaptive security appliance. The Cisco ASA adaptive security appliance applies a set of authorization and accounting rules to the VPN session, and forwards raw IP traffic from and to the IPsec tunnel. The remote network can use any application to access any resource behind the Cisco ASA adaptive security appliance VPN gateway, subject to access rules that are applied to the VPN session.

The security appliance lacks, however, the advanced functionality that is provided by Cisco IOS Software, such as virtual tunnel interfaces (VTIs), Generic Routing Encapsulation (GRE)-over-IPsec tunneling, Dynamic Multipoint VPNs (DMVPNs), or GET VPN.



## Cisco ASA Security Appliance VPN Access Methods

### Site-to-Site IPsec VPN: Benefits and Limitations

Benefits	Limitations
Supports any IP application	Cannot traverse many firewalls with default configuration
Requires no user training	
Supports low-latency operation.	

The full tunneling site-to-site IPsec architecture has the following benefits:

- It supports any IP application without application modification.
- It does not require any end-user training.
- It supports low-latency forwarding and enables the use of real-time applications, such as IP voice and real-time video, as IPsec is, by default, a connectionless protocol.

The full tunneling site-to-site IPsec VPN architecture is limited in that, like remote access IPsec VPNs, it has issues traversing many firewalls. This limitation occurs because IPsec and IKE traffic may not, by default, be allowed across enterprise firewalls.

## IPsec and NAT

VPN connections can be subject to a NAT or Port Address Translation (PAT). This translation is most common when the computer of a user or a VPN device is attached to a network where private addresses are used.

In IPsec VPNs, encrypted traffic is carried inside ESP, the IP protocol number 50. There are no port numbers in the ESP header that could be used for PAT mapping. Therefore, workarounds have been designed to overcome this limitation:

- Standards-based NAT-Transparency, also called NAT-Traversal (NAT-T), which encapsulates IKE and ESP into UDP to traverse NAT gateways, if these are detected along the VPN transport path
- UDP or TCP encapsulation from Cisco

A standards-based IPsec over UDP encapsulation, NAT-T performs two tasks: it detects whether both ends support NAT-T, and it 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, two NAT discovery (NAT-D) packets are 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 the 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, and a NAT-T should be performed. The subsequent ISAKMP packets and all IPsec packets are wrapped in a UDP header with a port address of 4500. Periodically, IKE NAT keepalives are sent out to keep the translations from timing out.

### Cisco ASA Security Appliance VPN Access Methods

VPN Access Methods: Use Cases

Scenario	Full Tunneling RA SSL VPN	Clientless RA SSL VPN	Full Tunneling RA IPsec VPN	Site-to-Site IPsec VPN
Mobile workers using managed devices requiring full network access	Yes	No	Yes	No
Mobile workers using unmanaged devices from public locations	No	Yes	No	No
Mobile partners requiring controlled transparent access with VPN client software	Yes	No	Yes	No
Mobile partners requiring controlled access without a client	No	Yes	No	No
Remote site or partner site connectivity	No	No	No	Yes

**RA: Remote access**

This table describes various VPN use cases with the corresponding best match VPN access types.

- **Mobile workers using managed devices requiring full network access:** This scenario is typical for mobile employees who use company-owned computers to access internal enterprise resources. Client software (Cisco AnyConnect VPN Client or Cisco SSL VPN Client) is installed on the computer and provides transparent network access.
- **Mobile workers using unmanaged devices from public locations:** In this situation, users access the VPN from public computers in Internet kiosks. No client software is available, and the users access the VPN using the web browser.
- **Partners requiring controlled transparent access with VPN client software:** This case is like the scenario with mobile employees who use computers with client software to access the VPN.
- **Partners requiring controlled access without a client:** In this scenario, partners access VPN resources via a web browser.
- **Remote site or partner site connectivity:** IPsec site-to-site VPNs are used to provide continuous connectivity between branches or locations of the same or of different partner organizations.

# VPN Termination on Cisco ASA Adaptive Security Appliance Network Interfaces

This topic discusses the VPN termination on Cisco ASA adaptive security appliances.

## VPN Termination on Cisco ASA Security Appliance Network Interfaces

### Cisco ASA Network Interface Requirements

- The Cisco ASA only supports VPN functionality in routed, single-context mode.
- The Cisco ASA only allows traffic to terminate on its interface closest to the traffic source:
  - All services on an interface must be explicitly enabled (VPN, management access).
  - Cisco ASA security appliance always drops packets to its other interfaces.



The Cisco ASA adaptive security appliance only supports VPN functions when running in routed, single-context mode. In order to terminate a VPN connection, the VPN connection must terminate on one of Cisco ASA adaptive security appliance routed (Open Systems Interconnection [OSI] Layer 3) interfaces. Due to Cisco ASA adaptive security appliance software design, the security application will only terminate VPN traffic on the interface that is closest to the traffic source. For example, if you have configured the outside interface to connect the Cisco ASA adaptive security appliance to the Internet, all VPN connections from the Internet can only terminate on the outside interface.

By default, the Cisco ASA adaptive security appliance denies all connections to its IP addresses (that is, the control plane) on routed interfaces. In order to allow VPN termination, or to establish remote management access, you need to specifically authorize every such network service on every Cisco ASA adaptive security appliance interface.

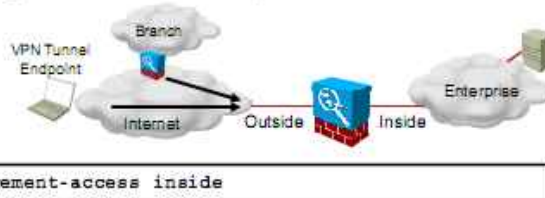
Note that the Cisco ASA adaptive security appliance does not permit the forwarding of any packets to interfaces that are not closest to the traffic source. Taking the previous example, you also cannot configure the Cisco ASA adaptive security appliance to respond to pings on any other interface than the outside interface, for clients reachable over the outside interface.

## VPN Termination on Cisco ASA Security Appliance Network Interfaces

### Management Access Exception

You may need to access a Cisco ASA security appliance interface through a VPN tunnel.

- Often, this will be an interface not closest to the traffic source.
- The "management access" feature allows such access over any supported VPN tunnel.
- Only one management access interface possible.
- Management rules still need to permit such access.



There is an exception that you can configure to change the management access behavior in one particular scenario. By default, the described behavior causes remote management traffic that arrives through a VPN tunnel (terminating on, for example, the outside interface) and is destined for the inside interface, to be dropped. Sometimes, this is unwanted, especially if you need to manage the security appliance over an untrusted network.

Such management traffic that is destined to the inside interface can be explicitly permitted to arrive through a VPN that is terminated on another interface. You can configure this setting using the **management-access** global configuration command and specifying the management interface to which connections from other interfaces are permitted, but only over a VPN tunnel. The VPN protection ensures that the traffic is protected even though it is forwarded over an untrusted network. Alternatively, you may also deploy secure management protocols, such as HTTPS or SSH, and manage the security appliance with connections to the outside interface. Only one management access interface can be configured on the appliance. The management access interface IP address should not have any static NAT translation rules applied to it.

### management-access

To allow management access to an interface other than the one from which you entered the adaptive security appliance when using VPN, use the **management-access** command in global configuration mode. To disable management access, use the **no** form of this command.

**management-access** *mgmt\_if*

#### management-access Parameters

Parameter	Description
<i>mgmt_if</i>	Specifies the name of the management interface that you want to access when entering the Cisco ASA adaptive security appliance from another interface

## VPN Termination on Cisco ASA Security Appliance Network Interfaces

### Concurrent Management and VPN Access

SSL VPN and Cisco ASDM management both use the HTTPS protocol to access the Cisco ASA security appliance:

- Supported on the same interface since Release 8.0(2).
- Management access is still subject to restrictions based on IP address.
- Cisco ASDM invoked using management URL.

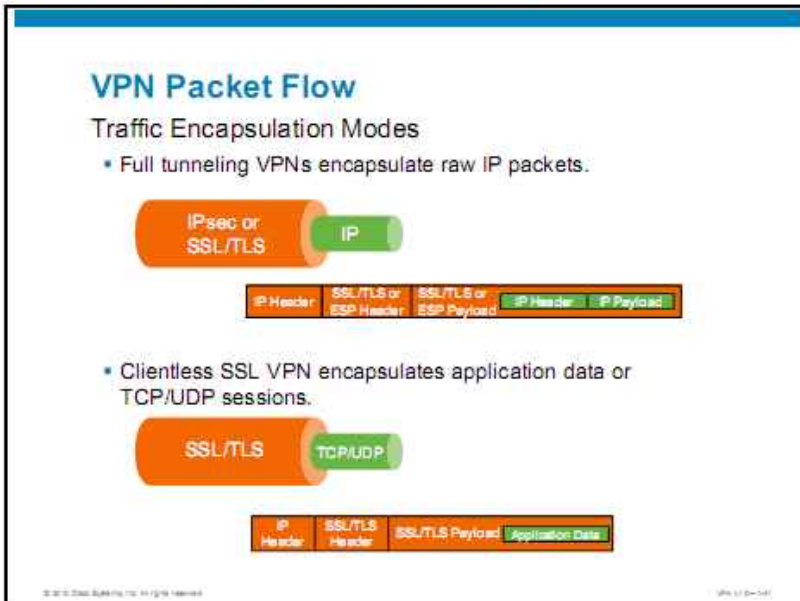


Beginning in Cisco ASA Software Release 8.0(2), the security appliance is capable of processing both SSL VPNs and management HTTPS traffic (that is, Cisco Adaptive Security Device Manager [ASDM] access) on the same interface and same port, although they use the same protocol. The connecting users must select which access type they seek and then authenticate accordingly. The Cisco ASDM is invoked by accessing the management URL at https://ASA-address/admin.

The approach that is used by earlier versions was to configure distinct port numbers for Cisco ASDM HTTPS access and for the SSL VPN. Configuring different port numbers is still supported, but no longer required.

# Packet Flow in Cisco ASA Adaptive Security Appliance VPN Functions

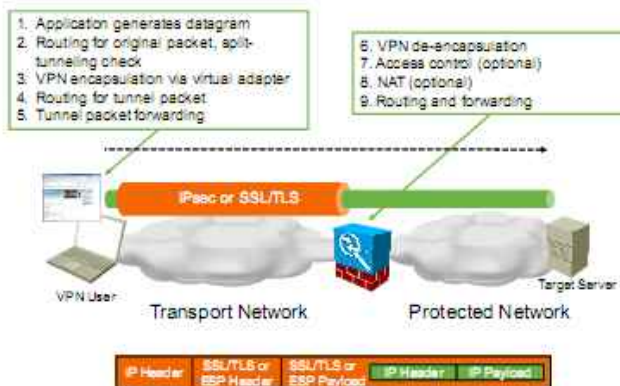
This topic explains the packet flow in tunnel and clientless VPNs.



The two modes of carrying data in VPN packets are the full tunneling mode, which encapsulates raw IP packets in a cryptographic envelope, and clientless SSL VPN mode, which encapsulates TCP or UDP sessions or application data. This topic describes how the Cisco ASA adaptive security appliance processes user traffic in both scenarios.

## Tunneling VPN Packet Flow

### Inbound Traffic

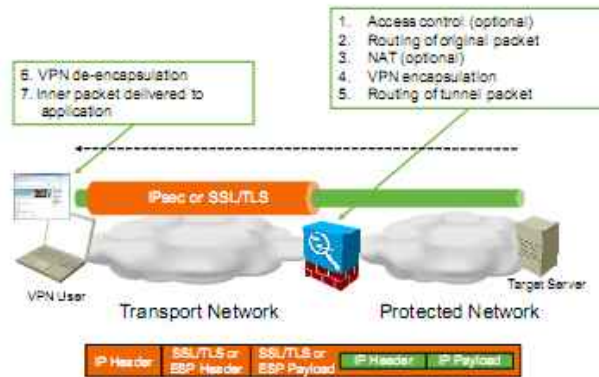


The figure depicts the life cycle of a packet in a full tunneling remote access VPN:

1. The client application generates an IP datagram that needs to be forwarded to a target server in the protected network.
2. The IP stack makes a routing decision. A split tunneling configuration can be used to influence the routing table. For networks that are reachable over the tunnel, the route points via the virtual adapter to the remote VPN gateway.
3. The VPN client encapsulates the IP datagram in a cryptographic envelope (ESP or SSL/TLS) and adds a tunnel (outer) IP header. The source IP address is set to the physical interface IP address and the destination to the VPN gateway.
4. The packet is routed to determine the output interface.
5. The packet is forwarded over the physical interface of the client into the untrusted network.
6. The VPN gateway verifies packet authenticity and decrypts it.
7. The VPN gateway checks its access policy to permit or deny the packet.
8. The VPN gateway performs NAT on the outside or inside address, if configured.
9. The cleartext packet is forwarded to the destination.

## Tunneling VPN Packet Flow

### Return Traffic



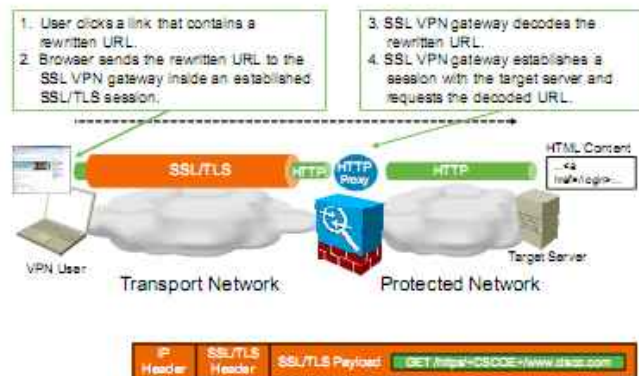
After the return packet arrives on the inside interface of the VPN gateway, the following occurs:

1. The packet is most likely matched against an existing entry in the connection table that defines an established session. The packet is inspected by the access control functions.
2. The outgoing interface is found in the routing table.
3. Address translation is optionally performed, if configured for the combination of the inside host and the client VPN address.
4. The packet is encapsulated, encrypted, and authenticated.
5. The packet is routed and forwarded out the external VPN gateway interface.
6. The client receives the packet, decrypts the content, verifies authenticity, and de-encapsulates the inner packet.
7. The datagram is delivered to the application.



## Clientless SSL VPN Data Flow

### Inbound Traffic (HTTP Request)



When a user connects to a clientless SSL VPN and uses a web (HTTP-based) application that is available on the VPN portal that connects to an internal server, these steps occur:

1. The user clicks a link on the VPN portal. The link contains a URL that is rewritten by the VPN gateway.
2. The browser sends this URL to the SSL VPN gateway inside the SSL and VPN session.
3. The original URL that identifies content in the internal network is decoded from the rewritten URL by the VPN gateway.
4. The VPN gateway opens an HTTP session to the target server and requests the target URL.

## Clientless SSL VPN Data Flow

### Return Traffic (HTTP Response)



When the internal server returns web content to the VPN gateway, the following events will take place:

1. The VPN gateway will receive the content from the target server.
2. The VPN gateway will analyze the content, and rewrite all URLs in the content in a specific manner. In this example, the original content contains a relative link to the “/login” URL on the internal server. The SSL VPN gateway will rewrite this link to a link that appears to be reachable on the SSL VPN gateway, and not the internal server (for example, <https://+CSCOE+/intra.domain.com/login>).
3. The VPN gateway forwards the modified content to the browser over the SSL/TLS session.
4. The browser will receive the modified content.
5. The browser may additionally modify content before displaying it to the user.
6. Finally, the browser renders the rewritten content to the user.

## Clientless SSL VPN Data Flow

### Inbound URL Decoding

- The SSL VPN gateway must force the client to use it as a proxy for all subsequent requests.
- The gateway rewrites all URLs in content, and references itself as the target server.
- When the client requests the rewritten URL, the gateway can decode it back to the original URL.



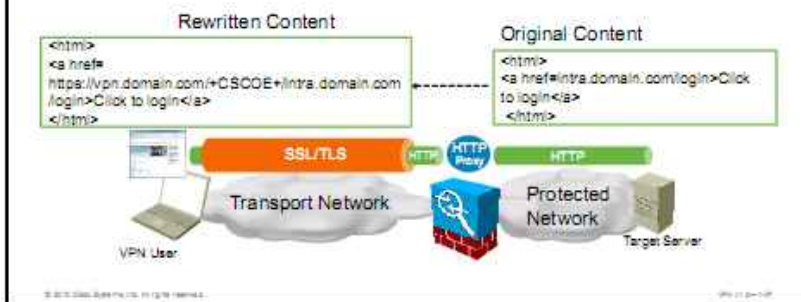
Rewriting of content is required in clientless SSL VPNs to force the browser of the VPN user to always request content from the SSL VPN gateway, and never attempt to contact the server directly. Therefore, the VPN gateway must rewrite all URLs so that they appear to be present on the VPN gateway itself. When the client requests such a URL, the VPN gateway can decode the original URL from it, as the URL was rewritten in such a manner as to include the original URL inside it. In this example, the security appliance rewrites the client request `https://vpn.domain.com/+CSCOE+/intra.domain.com` to request `http://intra.domain.com`. It then forwards the rewritten request to the internal server.

## Clientless SSL VPN Data Flow

### Outbound Content Rewriting

The SSL VPN gateway must rewrite all URLs inside delivered content that the client could potentially request:

- HTML, JavaScript, Java applets, XML, ActiveX, Flash
- Content changes when you rewrite applets, invalidating their digital signatures. The gateway must re-sign such applets.



The SSL VPN gateway rewrites all web-based content that is received from the internal server. The rewriting process changes the URL references and Java socket calls so that the requests point to the gateway instead of the internal server. The SSL VPN gateway parses web objects that may include rewriteable information—HTML, JavaScripts, Java applets, XML, ActiveX, and Flash—and replaces all found references.

When rewriting digitally signed Java applets or other digitally signed applets content, the SSL VPN gateway must also replace the Java bytecode signature that is applied to the content by a Java bytecode that is applied over the rewritten content.

All these tasks require substantial CPU and memory resources. To save the resources, the SSL VPN gateway can tag the web objects and send them to the remote browser along with JavaScript rewriting instructions. The remote browser executes the JavaScript routines to perform the content rewriting before presenting the content to the end user. This is called client-side rewriting.

## Clientless SSL VPN Data Flow

### Browser Plugins

Browser plugins are lightweight client applications that run inside the browser:

- These are Java applets loaded from the SSL VPN gateway on demand.
- Available for interactive terminal access (Telnet, SSH, Route Discovery Protocol (RDP), Citrix Independent Computing Architecture (ICA), Virtual Network Computing (VNC)).
- Do not require any reconfiguration of the client.
- Attempt to run ActiveX first, with fallback to Java.



Browser plug-ins are lightweight client applications that provide terminal access functionality inside the browser of a user. These plug-ins are downloaded on demand from the SSL VPN gateway, and all their communications are encapsulated within the SSL VPN session. The browser plug-ins use ActiveX as the primary download and invocation method. If ActiveX fails, Java is attempted as the last resort. At least one of the methods (ActiveX or Java) must be enabled in the browser for the browser plug-ins to work.

The figure illustrates plug-in-based application access:

1. A user connects and authenticates to the SSL VPN portal, and then runs an SSH plug-in that allows access to an SSH server running on `mgmt.cisco.com`.
2. The SSH client runs inside the browser, and reuses the SSL session of the browser with the SSL VPN gateway to forward a TCP connection inside it.
3. The SSL VPN gateway extracts the TCP session from the SSL VPN session, establishes a TCP connection with `mgmt.cisco.com` on port 22, and acts as a data relay between the two TCP sessions.

This approach does not require any client reconfiguration, but it may not be available for all applications needing support.

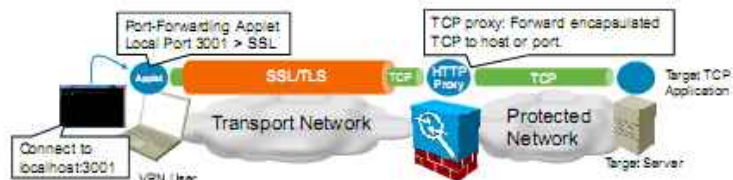
The plug-ins that are supported by Cisco are available at the Cisco Adaptive Security Appliance Software Download location on Cisco.com.

## Clientless SSL VPN Data Flow

### Port Forwarding

Port forwarding relays static TCP applications over the clientless SSL VPN session:

- Applications on the client connect to a local host socket.
- An in-browser applet listening on this socket forwards all data to the SSL VPN gateway.
- The gateway forwards all data to a preconfigured host or port.
- Require client application or operating system name resolution reconfiguration.
- Predecessor of smart tunnels.



Clientless SSL VPNs also support alternative methods that do not rely on content rewriting, but rather use browser features to enable the relaying of almost arbitrary TCP connections over the SSL/TLS session of the browser.

Port forwarding makes use of a local Java helper applet to provide access to certain TCP applications that, by default, are not supported by a clientless SSL VPN. The helper application installs on the client and acts as a connection broker to provide port-forwarding functionality. Client-side applications or the operating system must be slightly reconfigured to support operations over the port-forwarding relay.

---

**Note** Port forwarding is the predecessor technology of smart tunnels and should only be used wherever smart tunnels are not supported, such as on Linux machines.

---

The figure illustrates the port forwarding process:

1. A user application attempts to connect via Telnet to TS1.cisco.com on port 3001.
2. The local hosts file on the VPN user machine is analyzed. It has an entry for TS1.cisco.com (127.0.0.1) and directs the request at loopback (127.0.0.1 port 3001).
3. A port-forwarding Java applet has been started inside the browser that was downloaded from the SSL VPN portal. The applet intercepts connections to the loopback at port 3001 and forwards them over the SSL VPN session.
4. The VPN gateway extracts the TCP session from the SSL VPN session, establishes a TCP connection with TS1.cisco.com on port 2001, and act as a data relay between the two TCP sessions.

## Clientless SSL VPN Data Flow

### Smart Tunnels

Smart tunnels relay arbitrary TCP applications over the clientless SSL VPN session:

- Native applications on the client are unaware of the VPN session.
- A lightweight connection broker applet, downloaded from the SSL VPN gateway, intercepts sessions from designated applications and forwards them across the SSL VPN session.
- Does not require any reconfiguration of the client and its applications.



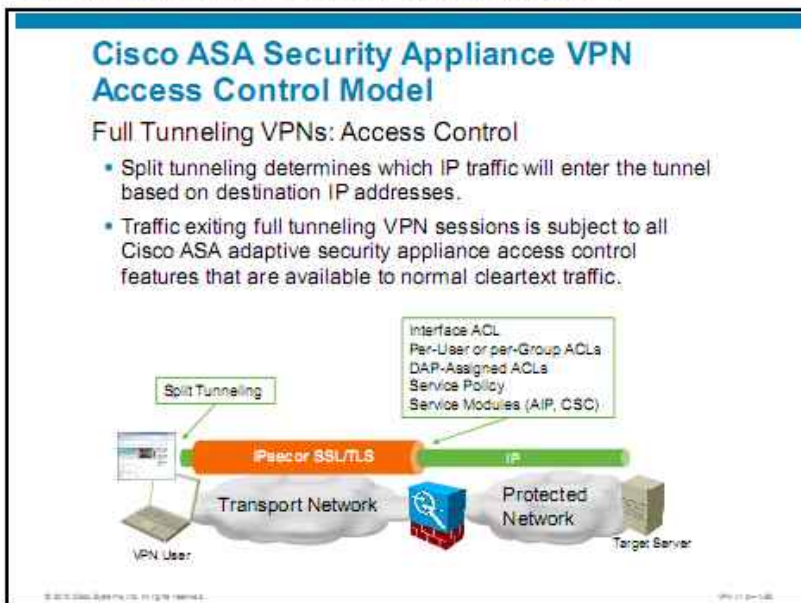
An evolution of port forwarding, smart tunnels allow clients to use many native client TCP (Winsock2) applications over the clientless SSL VPN tunnel without requiring administrative rights or application reconfiguration. Smart tunnels work by downloading a special applet to the client system. This applet intercepts all socket calls (that is, connection requests to the operating system kernel) from specific applications, and automatically redirects them into the SSL VPN session.

This figure illustrates smart-tunnel-based application access:

1. A user connects and authenticates to the SSL VPN portal. A smart tunnels configuration is in place for that user, and automatically downloads and executes on the client system. The user starts the IBM Lotus Sametime instant messaging client.
2. The smart tunnels applet intercepts the TCP connection of the Lotus Sametime client to the real server, and forwards it over the existing SSL VPN session.
3. The SSL VPN gateway extracts the TCP session from the SSL VPN session, establishes a TCP connection with the real target server, and acts as a data relay between the two TCP sessions.

# Cisco ASA Adaptive Security Appliance VPN Access Control Model

This topic describes the access control mechanisms that are available for full tunneling and clientless VPNs on the Cisco ASA adaptive security appliance.



The access control model that the Cisco ASA adaptive security appliance applies to VPN connections varies greatly depending on the use of full tunneling (SSL or IPsec) and clientless SSL VPNs.

In full tunneling (SSL or IPsec) VPNs, the Cisco ASA adaptive security appliance can apply its complete set of packet-based access control features, such as interface access control lists (ACLs), per-user or per-group ACLs, dynamic access policies (DAP)-assigned ACLs, a service policy that is configured by using Cisco Modular Policy Framework (MPF), and traffic redirection to security modules. All security controls are applied to cleartext traffic as it exits the tunnel (that is, just after de-encapsulation).



## Cisco ASA Security Appliance VPN Access Control Model

### Full Tunneling VPNs: ACL Bypass Configuration

Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Bypass Interface Access List

Enable inbound SSL VPN and IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Globally enable interface ACL bypass (enabled by default).

```
sysopt connection permit-vpn
```

Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Bypass Interface Access List

In all full tunneling (SSL or IPsec) VPNs, the Cisco ASA adaptive security appliance allows you to bypass its interface ACLs for traffic that has arrived over a VPN connection. This redirection can be useful in environments where no access control beyond VPN authentication is required to access protected resources. Note that the Cisco ASA adaptive security appliance can still apply per-user or per-group ACLs, DAP-assigned ACLs, an MPF-configured service policy, and service module redirection to this traffic, if needed.

Using Cisco ASDM, perform the following steps to enable the Cisco ASA adaptive security appliance to bypass interface ACLs for traffic that has arrived over a VPN connection:

- Step 1** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Bypass Interface Access List** (or **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options** (not shown in the figure).
- Step 2** Check the check box that enables this behavior.
- Step 3** Click **Apply** to apply this setting to the security appliance.

In the command-line interface (CLI), use the **sysopt connection permit-vpn** command in global configuration mode to allow the VPN traffic to bypass interface access lists. This setting is enabled by default as of Cisco ASA Software Release 7.0(1).

### sysopt connection permit-vpn

For traffic that enters the adaptive security appliance through a VPN tunnel and is then decrypted, use the **sysopt connection permit-vpn** command in global configuration mode to allow the traffic to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. To disable this feature, use the **no** form of this command.

### sysopt connection permit-vpn

## Cisco ASA Security Appliance VPN Access Control Model

### Clientless SSL VPN: Proxy-Mode Access Control

In proxy-mode clientless SSL VPNs, the Cisco ASA security appliance uses URL filters and selective VPN portal features to limit access to internal resources:

- Rules are implemented as webtype ACLs.
- Classic ACLs, service policies, and service module redirects are not supported.



In clientless SSL VPNs, when the Cisco ASA adaptive security appliance is acting as a proxy for HTTP traffic, traffic is inspected and controlled using a distinctly different set of access control features than those that are applied to traffic from full tunneling (SSL or IPsec) VPNs. Interface ACLs, per-user or per-group ACLs, DAP-assigned packet ACLs, an MPF-configured service policy, and traffic redirection to security modules are not available for proxy-mode clientless connections.

In a proxy-mode clientless SSL VPN, you can control user access based on URL filters to determine which URLs (objects, resources) users can access. This determination can be made based on the destination host, service, and object path or name. You can also limit the VPN portal features that are available to the users—for example, restricting them from mounting certain file shares.

AAA authorization offers a scalable approach to apply access control parameters in a centralized fashion. An external AAA server can be configured to use attribute-value pairs to enforce VPN session settings. External AAA authorization and access control are covered in a later module.

## Access Control for Clientless SSL VPN

### Selective Portal Features

Portal Feature	Description
URL entry	Allow or deny entering URLs directly into the portal page
File server entry	Allow or deny entering file server names
File server browsing	Allow or deny browsing of CIFS shares
Hidden share access	Allow or deny access to hidden CIFS shares
ActiveX relay	Enables users to launch ActiveX-based applications from the SSL VPN browser

The table shows some portal features that you can use to perform access control for clientless SSL VPN users.

## Cisco ASA Security Appliance VPN Access Control Model

Clientless SSL VPN: Port Forwarding, Browser Plugins, Smart Tunnel Access

With port forwarding, browser plug-ins, and smart tunnels, the Cisco ASA adaptive security appliance uses address- and service-based filters to limit access to internal resources:

- Classic ACLs, service policies, and service module redirects are not supported.



You can control the three alternative access methods in clientless SSL VPNs: port forwarding, browser plug-ins (thin clients), and smart tunnels using webtype ACLs that filter traffic based on the destination server and service. Therefore, you can specify exactly which applications on specific servers are available to users of these services. Interface ACLs, per-user or per-group ACLs, DAP-assigned packet ACLs, an MPF-configured service policy, and traffic redirection to security modules are also not available for port forwarding, browser plug-ins, and smart tunnels connections.

## Cisco ASA Security Appliance VPN Access Control Model

### Comparison

Criteria	Full Tunneling Client-Based Access	HTTP Proxy Access (Clientless)	Port Forwarding (Clientless)	Browser Plug-Ins (Clientless)	Smart Tunnels (Clientless)
Uses classic ACLs, service policy, modules	Yes	No	No	No	No
Uses webtype ACLs	No	Yes	Yes	Yes	Yes
Supports MPF Layer 3-4 filtering	Yes	No	No	No	No
Supports MPF Layer 5-7 filtering	Yes	No	No	No	No

The table compares the Cisco ASA adaptive security appliance access controls that are available for various remote access modes, and allows you to choose an access mode that provides adequate controls in your risk environment.

# Cisco ASA Adaptive Security Appliance VPN Licensing

This topic provides an overview of the VPN licensing model on the Cisco ASA adaptive security appliance.

## Cisco ASA Security Appliance VPN Licensing

**Base license:**

- Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580 Adaptive Security Appliances
- Two concurrent SSL VPN users
- Platform-dependant number of IPsec clients and a maximum number of all VPN users
- VPN load balancing (except ASA 5505 and ASA 5510)

**Security Plus license:**

- Only available on Cisco ASA 5505 and 5510 Adaptive Security Appliances
- Two concurrent SSL VPN users
- ASA 5505: Increased number of IPsec clients (25 instead of 10)
- ASA 5510: VPN load balancing

Feature	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580
Maximum number of concurrent IPsec and SSL VPN sessions	10 / 25	250	750	2500	5000	5000

Base and Security Plus Licensing

© 2010 Cisco Systems, Inc. All rights reserved. | 9001-11-00-1-00

The Cisco ASA adaptive security appliance license specifies the options that are enabled on a given security appliance. It is represented by an activation key that is a 160-bit (five 32-bit words) value. This value encodes the serial number (an 11-character string) and the enabled features into the activation key string.

By default, the Cisco ASA adaptive security appliance ships with a license already installed. This license might be the base license, to which you want to add more licenses, or it might already have some of required licenses installed. You may install additional licenses on all Cisco ASA adaptive security appliance models. The base license covers, among non-VPN features, two SSL VPN sessions, for trial and management purposes, and any number of IPsec VPN sessions that does not exceed the per-platform limit depicted in the table. It also covers VPN load-balancing virtual cluster functionality.

The Cisco ASA 5505 Adaptive Security Appliance and Cisco ASA 5510 Adaptive Security Appliance models differ from the other Cisco ASA adaptive security appliance models. The Cisco ASA 5505 Adaptive Security Appliance does not support VPN load balancing at all. The Cisco ASA 5510 Adaptive Security Appliance does not offer VPN load balancing within the base license, but provides it with the Security Plus license option. The Security Plus license extends the scope of the basic license by additional non-VPN features, as well as a higher number of IPsec clients on the Cisco ASA 5505 Adaptive Security Appliance, and active/standby failover support and VPN load-balancing support on the Cisco ASA 5510 Adaptive Security Appliance.

Most enterprise environments use a higher number of SSL VPN sessions and may require enhanced functionality. Such enterprises need to purchase optional VPN licenses that can be activated in addition to the base license. The security appliance offers these additional license types:

- The Cisco AnyConnect Essentials license enables lightweight Cisco AnyConnect VPN Client access to the Cisco ASA adaptive security appliance. This license does not support clientless SSL VPN access or Cisco Secure Desktop.
- The Cisco AnyConnect Premium per-user license allows both Cisco AnyConnect VPN Client software-based and clientless SSL VPN access for users with or without Cisco Secure Desktop. This license is available as a permanent or temporary activation key that can be installed locally on an appliance or shared among multiple devices.
- The Cisco AnyConnect Mobile license provides access to the Cisco AnyConnect client for touchscreen mobile devices running Windows Mobile 5.0, 6.0, or 6.1.
- The Advanced Endpoint Assessment license enables advanced endpoint assessment and remediation functionality that goes beyond the standard host scan (which includes host scan extensions for basic endpoint assessment) features of the Cisco Secure Desktop.
- The shared VPN license enables sharing of VPN licenses among security appliances based on the number of VPN connections on an individual security appliance.
- The Federal Information Processing Standards Publication (FIPS) 140-2 Level 1 validation license is necessary to use a FIPS-compliant version of the Cisco AnyConnect VPN Client (version 2.4 or later).
- A strong encryption license offers support for strong encryption algorithms 3DES and AES. It is free, but subject to export restrictions.

## Cisco AnyConnect VPN Licensing

Supports only Cisco AnyConnect VPN Client users:

- Immediately provides support for the maximum supported number of VPN users
- Does not support clientless access or Cisco Secure Desktop
- Cannot be active at the same time with Cisco AnyConnect Premium license
- Used by default, if installed



Cisco AnyConnect Essentials Licenses

© 2010 Cisco Systems, Inc. All rights reserved.

VPN 11-04-100

The Cisco AnyConnect Essentials license enables the Cisco ASA adaptive security appliance to immediately use the maximum number of allowed SSL VPN connections (as limited by the platform) using the Cisco AnyConnect VPN Client, but does not support clientless SSL VPN or Cisco Secure Desktop features with SSL VPN access. If you require these features, you must install the Cisco AnyConnect Premium SSL VPN license *instead* of the Cisco AnyConnect Essentials license. With the Cisco AnyConnect Essentials license, VPN users can only use a web browser to log in and to download and start the Cisco AnyConnect client. The Cisco AnyConnect client software offers the same set of client features, whether it is enabled by this license or a Cisco AnyConnect Premium SSL VPN license, except for its integration with Cisco Secure Desktop.

The Cisco AnyConnect Essentials license cannot be active at the same time as the Cisco AnyConnect Premium SSL VPN license. By default, the security appliance uses the Cisco AnyConnect Essentials license, if it is installed, but you can disable it using the **no anyconnect-essentials** global configuration command. You must disable it if you want to activate the Cisco AnyConnect Premium or the Advanced Endpoint Assessment license.



## Cisco AnyConnect VPN Licensing

Supports AnyConnect or clientless users:

- Supports Cisco Secure Desktop in both scenarios
- Available as temporary or permanent license
- VPN flex (temporary license for a single feature), 60-day for pandemic or business continuity
- Evaluation (temporary, can be for multiple features)
- Available as shared or local license



Cisco AnyConnect Premium Licenses

The Cisco AnyConnect Premium per-user license enables SSL VPN access for Cisco AnyConnect or clientless SSL VPN users, with or without Cisco Secure Desktop. The security appliance supports these license types:

- **Permanent license:** An unrestricted time validity.
- **Temporary licenses:** Valid for a limited time. Several subtypes exist:
  - **The VPN flex license:** A 60-day license for a single feature (SSL VPN), used to guarantee business continuity.
  - **An evaluation license:** May encompass multiple features for customer testing and proof-of-concept scenarios.
- **Local licenses:** Issued for a specific appliance (identified by the serial number) to enable SSL VPN sessions that are terminated on the licensed appliance.
- **Shared licenses:** Lets a Cisco ASA adaptive security appliance act as a shared license server for multiple client security appliances. This approach allows more effective license utilization in scenarios with distributed SSL VPN termination.

## Cisco AnyConnect VPN Licensing

- The appliance starts the time countdown when you configure the activation key.
- Pauses when you:
  - Stop using the license
  - Activate a permanent license
  - Activate a different temporary license
- Continues countdown when the security appliance is shut down.
- Reverts to the primary license after first load after expiration.
- The temporary license reacts to system clock changes to prevent misuse.



Cisco AnyConnect Premium Temporary Licensing

© 2010 Cisco Systems, Inc. All rights reserved.

VPN 11.0-148

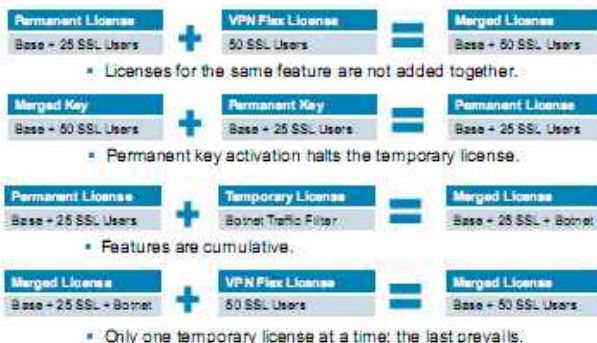
To deploy the Cisco AnyConnect Premium temporary licensing, you must understand the time measurement approach that is implemented by the temporary licenses. These are the key features:

- The timer for the temporary license starts counting down when you activate it on the security appliance.
- If you stop using the temporary license before it times out—for example, you activate a permanent license or a different temporary license—the timer halts. The timer only starts again when you reactivate the temporary license.
- If the temporary license is active, and you shut down the security appliance, then the timer continues to count down. If you intend to leave the security appliance in a shutdown state for an extended period, you should activate the permanent license before you shut down to preserve the temporary license.
- When a temporary license expires, the next time you reload the security appliance, the permanent license is used. You are not forced to perform a reload immediately when the temporary license expires.

You should not change the system clock after you install the temporary license. If you set the clock to a later date, then if you reload, the security appliance checks the system clock against the original installation time, and assumes that more time has passed than has actually been used. If you set the clock back, and the actual running time is greater than the time between the original installation time and the system clock, then the license immediately expires after a reload.

## Cisco AnyConnect VPN Licensing

### Cisco AnyConnect Premium License Interaction



These rules describe the license interaction that is represented by examples in the figure:

- When you activate a temporary license, then features from both the permanent and the temporary licenses are merged to form the running license. The security appliance only uses the highest value from each license for each feature; the values are not combined.
- When you activate a permanent license, it overwrites the currently running permanent and temporary licenses and becomes the running license.

---

**Note** If you install a new permanent license, and it is a downgrade from the temporary license, then you need to reload the security appliance to disable the temporary license and restore the permanent license. Until you reload, the temporary license continues to count down.

---

- If you reactivate the already-installed permanent license, you do not need to reload the security appliance. The temporary license does not continue to count down.
- To re-enable the features of the temporary license if you later activate a permanent license, simply re-enter the temporary activation key.

---

**Note** For a license upgrade, you do not need to reload the Cisco ASA adaptive security appliance.

---

- To switch to a different temporary license, enter the new activation key. The new license is used instead of the old temporary license and combines with the permanent license to create a new running license.

---

**Note** The security appliance can have multiple temporary licenses installed, but only one is active at any given time.

---

## Cisco AnyConnect VPN Licensing

For Cisco AnyConnect clients on devices running Microsoft Windows Mobile 5.0, 6.0, or 6.1:

- A single license that enables Microsoft Windows Mobile access
- Also requires Cisco AnyConnect Essentials or Cisco AnyConnect Premium license to specify the total number SSL VPN sessions



Cisco AnyConnect Mobile License

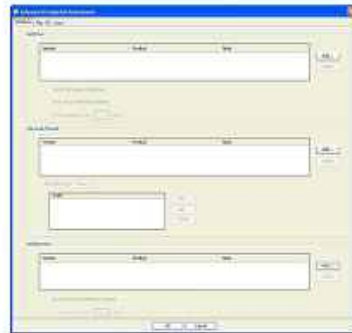
© 2010 Cisco Systems, Inc. All rights reserved.

VPN-01-00-000

The Cisco AnyConnect Mobile per-user license provides Cisco AnyConnect client access for touchscreen mobile devices running Windows Mobile 5.0, 6.0, or 6.1. This license requires activation of one of the following licenses to specify the total number SSL VPN sessions permitted: Cisco AnyConnect Essentials or Cisco AnyConnect Premium SSL VPN.

## Cisco ASA Security Appliance Additional VPN Licensing

- Provides Advanced Endpoint Assessment capabilities in SSL VPNs:
  - Autoremediation
  - Activation of disabled modules
  - Update of signature definition files
- Independent from basic host scan and endpoint assessment
- One license per device, requires Cisco AnyConnect Premium License



Advanced Endpoint Assessment License

The Advanced Endpoint Assessment per-user license enhances the Host Scan capabilities of the Cisco Secure Desktop. The Host Scan software supports three modules: Basic Scan, Endpoint Assessment, and Advanced Endpoint Assessment. The Advanced Endpoint Assessment is activated by the Advanced Endpoint Assessment license. In addition to collecting information regarding antivirus and antispymware applications, firewalls, operating systems, and associated updates, the module provides autoremediation features, such as activation of disabled components, configuring rules in supported personal firewalls, and updating host intrusion prevention system (HIPS) signature definition files.

The scan results are reported to the Cisco ASA adaptive security appliance, which can actively construct the DAP to enforce access rules based on the security posture of the client. The Advanced Endpoint Assessment license also requires a suitably sized Cisco AnyConnect Premium license to enable the advanced Cisco Secure Desktop functionality.

## Cisco ASA Security Appliance Additional VPN Licensing

Allows use of a FIPS 140-2 Level 1-compliant version of the Cisco AnyConnect VPN Client (2.4 or later):

- Provides support for a certified set of algorithm bundles
- Automatically avoids the use of weaker algorithms and key lengths
- Satisfies requirements of organizations requiring product FIPS 140-2 Level 1 compliance



FIPS 140-2 Level 1 Validation License

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-01-04-100

Cisco AnyConnect VPN Client Release 2.4 or later has been certified for compliance with Level 1 of FIPS 140-2, a U.S. government standard for specific security requirements for cryptographic modules. The FIPS 140-2 standard applies to all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems.

The security appliance requires the FIPS 140-2 Level 1 validation license to allow FIPS 140-2 Level 1-enabled Cisco AnyConnect clients to connect via the SSL VPN.

## Cisco ASA Security Appliance Additional VPN Licensing

### Failover:

- Supports single context for VPNs; only active/standby possible
- Both mates must have identical licenses

### VPN cluster:

- Members can have different capabilities and licenses
- Well suited for the shared licensing model
- Cluster master not necessarily identical with shared licensing server



You can design a redundant VPN system by configuring two identical appliances as a failover pair. For a VPN solution, you can only deploy active/standby mode, because VPNs only work in single-context mode, and active/active mode requires multiple contexts. Both failover mates must have identical licenses (for Cisco ASA Software Release 8.2 and earlier), although only one unit is actively using them. This setup supports stateful VPN failover, allowing uninterrupted VPN operations in case of device failure.

---

**Note** The Cisco ASA 5520 Adaptive Security Appliance and higher support stateful failover without any special license. The Cisco ASA 5510 Adaptive Security Appliance supports stateful failover with the Security Plus license only. The Cisco ASA 5505 Adaptive Security Appliance supports stateless failover with the Security Plus license only.

---

You can also achieve VPN high availability by grouping multiple appliances in a virtual cluster. In this scenario, the VPN sessions are load-balanced among the cluster members. The members may run on different platforms and have different licenses. When a cluster member fails, the cluster master redirects the sessions at other members, but existing sessions are not statefully taken over.

The shared licensing model suits VPN load balancing very well, because the licenses are consumed on demand. The functions of the cluster master and the VPN shared licensing server are independent from each other. VPN shared licensing is explained later in this lesson.

# Cisco ASA Security Appliance Additional VPN Licensing

## License Verification

```
ASA#show license
... part of the output omitted ...

Licensed Features for this platform:
Maximum Physical Interfaces    + Unlimited
Maximum VLANs                 + 150
Outside Hosts                 + Unlimited
Failover                      + Active/Active
VPN-SSS                      + Enabled
VPN-SSL-ASD                  + Enabled
Security Contexts             + 2
SFP/DFE                       + Disabled
SSL VPN Peers                + 2
Total VPN Peers              + 100
Shared Licenses               + Disabled
AnyConnect for Mobile        + Disabled
AnyConnect for Cisco VPN Phone + Disabled
AnyConnect Essentials        + Disabled
Advanced Endpoint Assessment + Disabled
UC Phone Proxy Sessions      + 2
Total UC Proxy Sessions      + 2
Botnet Traffic Filter         + Disabled

This platform has an ASA 5510 VPN Plus license.
```

Current Values

Serial No.: 781109107  
Running Activation Key: 0x615943 0x26c149e 0x6b7174 0x4c70985 0x823af6a  
Flash Authorization Key: 0x7098403 0x66c149e 0x6b7174 0x4c70985 0x823af6a

New Activation Key  
Configure a new activation key for the device. It will take effect after the next reload.  
New Activation Key:

Running Licenses

License	VPN Plus
Max Security Contexts	2
Max Physical Interfaces	Unlimited
Max VLANs	150
Failover	Active/Active
OTF/SFPs	Disabled
VPN SSL Encryption	Enabled
SSL VPN Peers	2
VPN Peers	100
SSL VPN Peers	2
Shared SSL VPN Licensing	Disabled
AnyConnect Mobile	Disabled
AnyConnect Essentials	Disabled
Advanced Endpoint Assessment	Disabled
UC Phone Proxy Sessions	2
Total UC Proxy Sessions	2
Botnet Traffic Filter	Disabled

Configuration > Device Management > Licensing > Activation Key

The licenses are activated using activation keys that are bound to the security appliance serial number. Activation keys are not portable. The activation key is not stored in the configuration file; it is stored as a hidden file in the Cisco ASA adaptive security appliance flash memory, and is tied to the serial number of the device. Feature licenses cannot be transferred between devices (except in the case of a hardware failure). If you have to replace your device due to a hardware failure, contact the Cisco Licensing Team to have your existing license transferred to the new serial number. The Cisco Licensing Team will ask for the Product Authorization Key (PAK) reference number and existing serial number.

You cannot combine two separate licenses for the same feature; for example, if you purchase a 50-session SSL VPN license, and later purchase a 100-session license, you cannot use 150 sessions; you can use a maximum of 100 sessions.

Although you can activate all license types, some features are incompatible with one another; for example, multiple-context mode and VPN. You can observe and upgrade the license for your security appliance from Cisco ASDM or from the CLI. The activation key and licensed features can be analyzed by choosing **Configuration > Device Management > Licensing > Activation Key**. Before you enter a new activation key, ensure that the image in flash and the running image are the same. You will also need to reboot the security appliance after you enter the new activation key for the change to take effect.

Complete the following steps to upgrade the activation key from Cisco ASDM:

- Step 1** Click **Configuration** in the Cisco ASDM toolbar.
- Step 2** Click **Device Management** in the navigation pane.
- Step 3** Expand **Licensing** menu.
- Step 4** Click **Activation Key**. The Activation Key panel is displayed.
- Step 5** Enter the new activation key in the New Activation Key field. Enter the activation key as a four- or five-element hexadecimal string with one space between each element as follows:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```



---

**Note** The leading 0x specifier is optional; all values are assumed to be hexadecimal. The key is not stored in the configuration file, and its tied to the serial number.

---

**Step 6** Click **Update Activation Key**.

**Step 7** Reload the security appliance to activate the flash activation key.

To obtain purchased activation keys, go to one of the following websites:

- If you are a registered user of Cisco.com, go to <http://www.cisco.com/go/license>.
- If you are not a registered user of Cisco.com, go to <https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet> to register.

To obtain an activation key, you will need to provide the serial number for the security appliance as it appears in the **show version** command output.

You can also obtain temporary, time-limited activation keys for demonstration or testing of new features that require a special license. Contact your Cisco account team for details.

To view your current activation key from CLI, enter the **show activation-key** command in the CLI and use the **show version** command to view all the licensed features on the Cisco ASA adaptive security appliance.

## show activation-key

To display the running activation key and licensed features in the configuration that are enabled by your activation key, including the number of contexts that are allowed, use the **show activation-key** command in privileged EXEC mode.

**show activation-key [detail]**

### show activation-key Parameters

Parameter	Description
<b>detail</b>	(Optional) Displays the permanent and temporary activation keys with their enabled features, including all previously installed temporary keys and their expiration dates

## show version

To display the software version, hardware configuration, license key, and related uptime data, use the **show version** command in user EXEC mode.

**show version**

## Cisco ASA Security Appliance Shared VPN Licensing

### Cisco AnyConnect Premium Shared Licensing

- A single pool of SSL VPN sessions shared among a cluster of appliances:
  - Licensing server uses a dedicated license
  - Optional backup server; participant license obtained from server, using serial number
  - Participant VPN gateways obtain licenses from server
- SSL-protected communications between servers and participants



© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-04-108

A shared SSL VPN license (available on Cisco ASA Software Release 8.2 and later) lets you purchase many SSL VPN sessions and share the sessions as needed among a group of security appliances. You configure one of the security appliances as a shared licensing server, another as an optional backup shared licensing server, and the rest as shared licensing participants.

You need to decide which appliance should act as the server, and obtain the shared licensing server license using the serial number of that unit. Optionally, you can designate a second security appliance as a shared licensing backup server. You can only specify one backup server. The backup server needs a regular participant license. You must configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license. All communication in the licensing cluster is protected using SSL.

## Cisco ASA Security Appliance Shared VPN Licensing

### Licensing server:

- Serves participant requests
- Participates in shared license pool
- Does not need participant license
- May use a VPN flex license in addition to the shared license pool
- VPN flex licenses available for local SSL VPN sessions only
- Cannot be added to the shared licensing pool for use by participants
- Supports active/standby failover



When the participants register at the shared licensing server, the server responds with information about how often the participant Cisco ASA adaptive security appliance should poll the server. Whenever a participant needs additional user licenses, it contacts the server and the server responds with a 50-session batch of shared licenses. If there are not enough remaining sessions in the shared license pool for the participant, then the server responds with as many sessions as available.

The shared licensing server can also participate in the shared license pool. It does not need a participant license as well as the server license to participate.

## Cisco ASA Security Appliance Shared VPN Licensing

### Backup shared licensing server:

- Acts as participant
- Receives server-to-backup updates
- Takes over server role when the server fails
- Supports active/standby failover



### Participant:

- Uses up local licenses first
- Requests licenses from server in 50-session batches
- Total number of licenses cannot exceed the maximum platform limit



The shared licensing backup server must register successfully with the main shared licensing server before it can take on the backup role. When it registers, the main shared licensing server syncs the server settings as well as the shared license information with the backup, including a list of registered participants and the current license usage. The main server and backup server sync the data at 10-second intervals. After the initial sync, the backup server can successfully perform backup duties, even after a reload.

When the main server goes down, the backup server takes over server operation. While the primary server remains inactive, the backup server can operate for up to 30 continuous days. After this time, the backup server stops issuing sessions to participants, and existing sessions time out. Critical-level syslog messages are sent at 15 days, and again at 30 days.

When the main server comes back up, it syncs with the backup server, and then takes over server operation. When the backup server is not acting as the licensing server, it acts as a regular participant to the main shared licensing server.

When you configure the security appliance as a participant, it registers with the shared licensing server by sending information about itself, including the local license and model information. When a participant uses up the sessions of the local license, it sends a request to the shared licensing server for additional sessions in 50-session increments. The total sessions that are used by a participant cannot exceed the maximum sessions for the platform model. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

## Cisco ASA Security Appliance Shared VPN Licensing

### Configuring a Shared Licensing Server

Configure the shared SSL VPN license sharing server:

Shared secret:  Specify a shared secret key.

TCP IP port:  Default is 50554.

Refresh interval:  Default is 30 seconds.

Interfaces that serve shared licenses:

Interface	Serves licenses
inside	<input checked="" type="checkbox"/>
outside	<input type="checkbox"/>
serial	<input type="checkbox"/>

Select interfaces on which participants contact the server.

Optional backup shared SSL VPN license server:

Backup server IP address:  Enter IP address of the backup server.

Primary backup server serial number:  Enter serial number of the backup server.

Secondary backup server serial number:

```
license-server secret gj20v
license-server backup 10.1.1.2 backup-id JMX0929K0AK
license-server enable inside
```

Configuration > Device Management > Licensing > Shared SSL VPN Licenses

To configure the licensing server, you must first provision the proper activation key that enables the licensing server on that particular platform.

To configure a shared licensing server using Cisco ASDM, complete the following steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Device Management > Licensing > Shared SSL VPN Licenses** (not shown in the example).
- Step 2** In the Shared Secret field, enter the shared secret as a string between 4 and 128 ASCII characters. Any participant with this secret can use the license server.
- Step 3** Optionally, in the TCP IP Port field, enter the port on which the server listens for SSL connections from participants, between 1 and 65,535. In the example, the default value, TCP port 50,554, is used.
- Step 4** Optionally, in the Refresh Interval field, enter the refresh interval between 10 and 300 seconds. This value is provided to participants to set how often they should communicate with the server. The default is 30 seconds.
- Step 5** In the Interfaces That Serve Shared Licenses area, check the **Shares Licenses** check box for any interfaces on which participants contact the server. In the example, participants contact the server on the inside interface.
- Step 6** Optionally, to identify a backup server, perform the following actions in the Optional Backup Shared SSL VPN License Server area:
  - In the Backup Server IP Address field, enter the backup server IP address. In the example, the backup server IP address is 10.1.1.2.
  - In the Primary Backup Server Serial Number field, enter the backup server serial number. In the example, the serial number of the backup shared license server is JMX0929K0AK.
  - If the backup server is part of a failover pair, identify the standby unit serial number in the Secondary Backup Server Serial Number field.

---

**Note** You can only identify one backup server and its optional standby unit.

---

**Step 7** Click **Apply** to apply the configuration.

To configure a shared licensing server using the CLI, first use the **license-server secret** command to configure a shared secret that will be used to encrypt the communication between the server, backup server, and the participants. To deploy the backup licensing server, define its address and serial number by using the **license-server backup** command. If the backup server runs in active/standby failover mode, you must provide the serial numbers of both mates. Finally, specify the interfaces on which you activate the license server feature by using the **license-server enable** command.

## license-server secret

To set the shared secret on the shared licensing server, use the **license-server secret** command in global configuration mode. To remove the secret, use the **no** form of this command.

**license-server secret** *secret*

### license-server secret Parameters

Parameter	Description
<i>secret</i>	Sets the shared secret, a string between 4 and 128 ASCII characters

## license-server backup backup-id

To identify the shared licensing backup server in the main shared licensing server configuration, use the **license-server backup backup-id** command in global configuration mode. To remove the backup server configuration, use the **no** form of this command.

**license-server backup** *address backup-id serial\_number* [**ha-backup-id** *ha\_serial\_number*]

### license-server backup backup-id Parameters

Parameter	Description
<i>address</i>	Identifies the shared licensing backup server IP address
<b>backup-id</b> <i>serial_number</i>	Identifies the shared licensing backup server serial number
<b>ha-backup-id</b> <i>ha_serial_number</i>	(Optional) If you use failover for the backup server, identifies the secondary shared licensing backup server serial number

## license-server enable

To identify this unit as a shared licensing server, use the **license-server enable** command in global configuration mode. To disable the shared licensing server, use the **no** form of this command. A shared license lets you purchase many SSL VPN sessions and share the sessions as needed among a group of adaptive security appliances by configuring one of the appliances as a shared licensing server, and the rest as shared licensing participants.

**license-server enable** *interface\_name*

## license-server enable Parameters

Parameter	Description
<code>interface_name</code>	Specifies the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

**Cisco ASA Security Appliance Shared VPN Licensing**

Configuring a Backup Shared Licensing Server

Configuration > Device Management > Licensing > Shared SSL VPN Licenses

Configure multi-site SSL VPN license sharing client.

Shared secret: \*\*\*\*\* Specify a shared secret key. Must be supplied to participate. (4-128 char)

license server IP address: 10.1.1.1 Enter IP address of the server. Must be supplied to participate.

TCP IP port: 50554 Must match server port. Defaults to 50554.

Select backup role of client:

Client only  Backup server Select backup server role.

At least one interface must be selected to participate.

Interface	Shares Licenses
inside	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>
public	<input type="checkbox"/>

Select interfaces on which participants contact the server.

```
license-server address 10.1.1.1 secret gj3Dv
license-server backup enable inside
```

Configuration > Device Management > Licensing > Shared SSL VPN Licenses

To configure a shared licensing backup server using Cisco ASDM, complete the following steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Device Management > Licensing > Shared SSL VPN Licenses** (not shown in the example).
- Step 2** In the Shared Secret field, enter the shared secret as a string between 4 and 128 ASCII characters.
- Step 3** In the License Server IP Address field, enter the IP address of the shared license server. In the example, the IP address of the shared license server is 10.1.1.1.
- Step 4** Optionally, in the TCP IP Port field, enter the port on which to communicate with the server using SSL, between 1 and 65,535. In the example, the default value, TCP port 50,554, is used.
- Step 5** To identify the participant as the backup server, in the Select Backup Role of Client area:
  - Click the **Backup Server** radio button.
  - Check the **Shares Licenses** check box for any interfaces on which participants contact the backup server. In the example, participants contact the server on the inside interface.
- Step 6** Click **Apply** to apply the configuration.

To configure a shared licensing backup server using the CLI, first define the server address and encryption key by using the **license-server address** command. Then enable interfaces for the backup licensing server feature by using the **license-server backup enable** command.

## license-server address

To identify the shared licensing server IP address and shared secret for use by a participant, use the **license-server address** command in global configuration mode. To disable participation in shared licensing, use the **no** form of this command. A shared license lets you purchase many SSL VPN sessions and share the sessions as needed among a group of adaptive security appliances. This arrangement occurs by configuring one of the adaptive security appliances as a shared licensing server, and the rest as shared licensing participants.

**license-server address** *address* **secret** *secret* [**port** *port*]

### license-server address Parameters

Parameter	Description
<i>address</i>	Identifies the shared licensing server IP address.
<b>secret</b> <i>secret</i>	Identifies the shared secret. Use the <b>license-server secret</b> command to ensure that the secret matches the secret set on the server.
<b>port</b> <i>port</i>	(Optional) If you changed the default port in the server configuration by using the <b>license-server port</b> command, set the port for the backup server to match, between 1 and 65,535. The default port is 50,554.

## license-server backup enable

To enable this unit to be the shared licensing backup server, use the **license-server backup enable** command in global configuration mode. To disable the backup server, use the **no** form of this command.

**license-server backup enable** *interface\_name*

### license-server backup enable Parameters

Parameter	Description
<i>interface_name</i>	Specifies the interface on which participants contact the backup server. You can repeat this command for as many interfaces as desired.



# Cisco ASA Security Appliance Shared VPN Licensing

## Configuring a Shared Licensing Participant

Configuration > Device Management > Licensing > Shared SSL VPN Licenses

Configure multi-site SSL VPN license sharing client.

Shared secret:  Specify a shared secret key. Must be supplied to participate. (4-128 char)

License server IP address:  Enter IP address of the server. Must be supplied to participate.

TCP IP port:  Must match server port. Defaults to 50554.

Select backup role of client:

Client only  Backup server Select client role.

Backup license server IP address:  Enter IP address of the backup server. (Optional)

```
license-server address 10.1.1.1 secret gj2Dv
license-server backup address 10.1.1.2
```

Configuration > Device Management > Licensing > Shared SSL VPN Licenses

To configure a shared licensing participant using Cisco ASDM, complete the following steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Device Management > Licensing > Shared SSL VPN Licenses** (not shown in the example).
- Step 2** In the Shared Secret field, enter the shared secret as a string between 4 and 128 ASCII characters.
- Step 3** In the License Server IP Address field, enter the IP address of the shared license server. In the example, the IP address of the shared license server is 10.1.1.1.
- Step 4** Optionally in the TCP IP Port field, enter the port on which the server uses SSL to communicate. The port number should be between 1 and 65,535. In the example, the default value, TCP port 50,554, is used.
- Step 5** To identify the participant, perform the following actions in the Select Backup Role of Client area:
  - Click the **Client Only** radio button.
  - Specify the IP address of the backup server in the Backup License Server IP Address field. In the example, the IP address of the shared license backup server is 10.1.1.2.
- Step 6** Click **Apply** to apply the configuration.

To configure a shared licensing backup server using the CLI, use the **license-server address** command to configure the server address and encryption key. Use the **license-server backup address** command, if available, to configure the backup server address.

## license-server address

To identify the shared licensing server IP address and the shared secret for use by a participant, use the **license-server address** command in global configuration mode. To disable participation in shared licensing, use the **no** form of this command. A shared license lets you purchase many SSL VPN sessions and share the sessions as needed among a group of adaptive security appliances by configuring one of the appliances as a shared licensing server, and the rest as shared licensing participants.

**license-server address** *address* **secret** *secret* [**port** *port*]

### license-server address Parameters

Parameter	Description
<i>address</i>	Identifies the shared licensing server IP address.
<b>secret</b> <i>secret</i>	Identifies the shared secret. The secret must match the <b>secret</b> set on the server by using the <b>license-server secret</b> command.
<b>port</b> <i>port</i>	(Optional) If you changed the default port in the server configuration by using the <b>license-server port</b> command, set the port for the backup server to match, between 1 and 65,535. The default port is 50,554.

## license-server backup address

To identify the shared licensing backup server IP address for use by a participant, use the **license-server backup address** command in global configuration mode. To disable use of the backup server, use the **no** form of this command.

**license-server backup address** *address*

### license-server backup address Parameters

Parameter	Description
<i>address</i>	Identifies the shared licensing backup server IP address

## Cisco ASA Security Appliance Shared VPN Licensing

### Licensing Server

```
ASA#show shared license detail
Backup License Server Info:
Device ID       : ABCD
Address        : 10.1.1.2
Registered     : NO
SA peer ID     : SPGH
Registered     : NO
c..part of the output omitted...>
Shared license utilisation:
SSLVPN:
  Total for network : 500
  Available         : 500
  Utilized          : 0
c..part of the output omitted...>
Client Info:
  Hostname        : 5540-A
  Device ID       : XXXXXXXXXXXX
  SSLVPN:
```

Verifying Shared Licensing Operation

### Participant

```
ASA#show shared license
Primary License Server : 10.1.1.1
Version               : 1
Status                : Active
Shared license utilisation:
SSLVPN:
  Total for network : 5000
  Available         : 5000
  Utilized          : 0
This Device:
  Platform limit   : 250
  Current usage    : 0
  High usage       : 0
c..part of the output omitted...>
```

You can verify the licensing server operations by using the **show shared license** command. If issued on the server, the command returns the details of the backup server and all registered participants. If run on a participant or backup server, the command provides information about the server.

### show shared license

To show shared license statistics, use the **show shared license** command in privileged EXEC mode. Optional keywords are available only for the licensing server.

**show shared license** [**detail** | **client** [*hostname*] | **backup**]

#### show shared license Parameters

Parameter	Description
<b>detail</b>	(Optional) Shows all statistics, including per participant
<b>client</b>	(Optional) Limits the display to participants
<i>hostname</i>	(Optional) Limits the display to a particular participant
<b>backup</b>	(Optional) Shows information about the backup server

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- X.509 certificates bind public keys to entity names; the PKI provides a scalable public key distribution system.
- The Cisco ASA adaptive security appliance provides site-to-site and remote access VPN features. VPN technologies that are supported are SSL and IPsec.
- The Cisco ASA allows to terminate VPN traffic on the interface that is closest to the traffic source.
- There are major differences in handling full tunneling and clientless VPN access.
- There are differences in the application of security controls between full tunneling and clientless VPN access.
- There are major differences how packets are handled in full tunneling and clientless SSL VPN access.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN 11-04-10

## References

For additional information, refer to this resource:

- *Managing Feature Licenses for Cisco ASA 5500 Version 8.2* at <http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html>

# Applying Common Cisco ASA Adaptive Security Appliance Remote Access VPN Configuration Concepts

---

## Overview

Configuring policies and network settings for many virtual private network (VPN) users requires a scalable and flexible configuration mechanism. This lesson enables you to configure connection profiles and group policies, which are the cornerstone for configuring either Secure Sockets Layer (SSL) VPN or IP Security (IPsec) remote-access policies on the Cisco ASA adaptive security appliance.

## Objectives

Upon completing this lesson, you will be able to apply configuration functions that are common to all Cisco ASA adaptive security appliance remote-access architectures. This ability includes being able to meet these objectives:

- Describe the components of Cisco ASA adaptive security appliance VPN policy configuration
- Configure connection profiles on the Cisco ASA adaptive security appliance
- Configure group policies on the Cisco ASA adaptive security appliance
- Describe external storage of policies

# Cisco ASA Adaptive Security Appliance VPN Policy Configuration

This topic provides an overview of the components of Cisco ASA adaptive security appliance VPN policy configuration.

## Cisco ASA VPN Policy Configuration

### Remote Access Configuration Requirements

The remote access VPN configuration tools require:

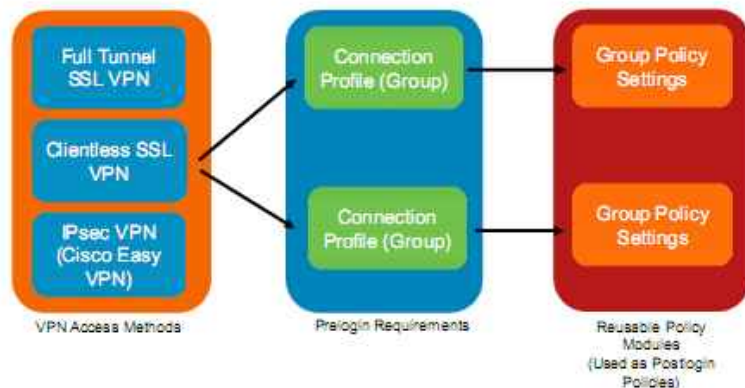
- **Flexibility:** Arbitrary network settings and security policies can apply to any user or group to implement a local policy.
- **Scalability:** Configuration of similar policies should not require duplication of effort; typically achieved through configuration modularity and hierarchical inheritance.

Remote-access VPNs involve various classes of remote users connecting to a protected network over an untrusted transport network. The policies governing security requirements for these users may be very complex, and there may be many different user groups, each with different requirements. For this reason, remote-access VPNs require a flexible and scalable configuration method to make the provisioning of such a configuration manageable.

The configuration method should allow arbitrary network settings and security policy-related rules to be applied to any specific user or user group. Additionally, it should guarantee that the configuration of similar policies to different groups, or the creation of small exceptions to group security policies, should require little effort, with no duplication of workload. And these attributes should occur through mechanisms that provide appropriate modularity of configuration, and inheritance in a configuration hierarchy.

## Cisco ASA VPN Policy Configuration

### Separation of Access Methods and Policies



To achieve this goal, the Cisco ASA adaptive security appliance uses a separation of access methods and policies. You should be aware of two major configuration constructs: connection profiles and group policies. Connection profiles define the prelogin requirements for a particular access method. Reusable group policies define the postlogin settings and security policies that need to be applied to a remote-access session after user authentication.

The Cisco ASA adaptive security appliance uses the same configuration philosophy for all three major access methods: full tunneling SSL VPNs, clientless SSL VPNs, and full tunneling IPsec VPNs (such as Cisco Easy VPN). A remote user connecting to a remote-access VPN will be classified into a connection profile, which will determine how the user should authenticate to the VPN gateway. After successful authentication, group policy settings will dictate the special VPN features or policy restrictions that apply to that user session.

---

**Note** Some documentation also refers to connection profiles as to "tunnel groups."

---

## Policy Inheritance and Aggregation

### Policy Hierarchy

- The security appliance applies user policies according to the following hierarchy:
  1. Dynamic access policy (DAP) rules
  2. User profile
  3. Group policy attached to the user profile
  4. Group policy attached to the connection profile
  5. DfltGrpPolicy settings
- All settings not specified in each level are automatically inherited from the lower-priority level.

So far, you have learned about several configuration concepts that you can combine to create manageable remote-access configurations. One of the major features that you should use as much as possible is policy inheritance, which connects all these objects to enable configuration reuse.

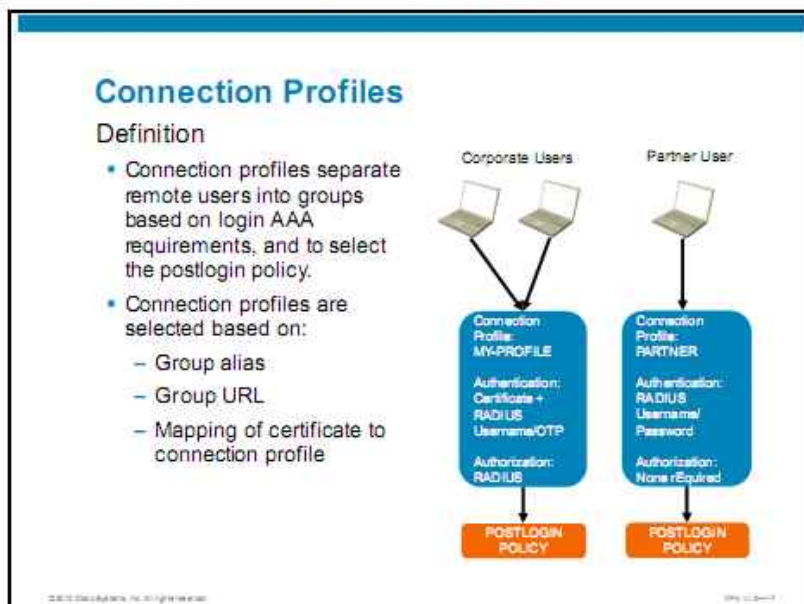
The Cisco ASA adaptive security appliance uses a hierarchical policy inheritance model, which has the following priority philosophy:

1. The most important postlogin settings and policies that are applied to the VPN connection of a remote-access user are those created by dynamic access policy (DAP) rules. DAP is covered separately later in this course, and can take into account dynamic events, such as the posture of the client to determine access rights.
2. If DAP does not configure a particular parameter, settings that are configured in the local user profile (or pushed from the authentication, authorization, and accounting [AAA] server as part of user authentication and authorization) will determine the postlogin policy.
3. If a certain parameter is not specified in the user profile, it may be specified in a group policy that is attached to a user profile.
4. If there is no group policy that is attached to a user profile, the Cisco ASA adaptive security appliance uses settings from the group policy that is attached to the connection profile of the user.
5. If the connection-profile-based group policy does not specify a particular setting, the security appliance will use the setting from the default group policy (DfltGrpPolicy).



# Connection Profiles

This topic describes how to configure connection profiles.



Connection profiles are Cisco ASA adaptive security appliance configuration entities that separate remote users into groups, based on your requirements for login AAA, and postlogin policies. Therefore, you should create different connection profiles for users who require different AAA methods, and different connection profiles for users who require different postlogin policies. Often, these are interdependent—for users who require access to more resources (or more-sensitive resources), you will typically require stronger AAA methods. For users who require only limited access, you may require weaker AAA controls.

The Cisco ASA adaptive security appliance allows you to select connection profiles based on the following:

- You can allow remote users to select the connection profile they intend to use. This can be achieved by using two methods:
  - By selecting a connection profile from a drop-down menu, a remote user then needs to successfully authenticate against the profile to obtain network access.
  - By connecting to a VPN group URL that is associated with the specific connection profile.
- Remote system identity allows you to use a property of the remote system, for example, a field in a digital (identity) certificate, to select the connection profile that is to be used for the remote client.

## Connection Profiles

### Mapping of Clients to Connection Profiles

- Connection profile selected before authentication
- Certificate-to-connection-profile maps can automate the selection process
- Connection profile determines the postlogin policy



© 2010 Cisco Systems, Inc. All rights reserved.

VPN-10108

When a remote-access VPN user initiates a VPN connection to the Cisco ASA adaptive security appliance VPN gateway, the security appliance will choose an initial connection profile that is based on the currently known remote system identity, or the selection by a remote user of the wanted connection profile.

The final connection profile of a user determines final policy settings.

## Connection Profiles

### Default Connection Profiles

If you do not define any criteria for mapping remote users to connection profiles, the Cisco ASA security appliance will map the user to a default connection profile:

- DefaultRAGroup for full tunnel IPsec VPN remote access clients.
- DefaultWEBVPNGroup for full tunnel and clientless SSL VPN remote access clients.
- Both default connection profiles are fully customizable.

The Cisco ASA adaptive security appliance includes two default connection profiles, which the security appliance uses in the absence of any connection-profile-mapping configuration.

- The default remote-access group (DefaultRAGroup) connection profile, which the Cisco ASA adaptive security appliance uses and to which it assigns a remote user if you do not configure any rules that would assign a user to a connection profile in full tunneling IPsec remote-access VPNs
- The default Cisco WebVPN group (DefaultWebVPNGroup) connection profile, to which the Cisco ASA adaptive security appliance will assign a remote user when you do not configure any connection-profile-mapping rules in full client and clientless SSL VPNs

## Connection Profile Selection

### Password Authentication

- You can select the connection profile before login (if allowed).
- Otherwise, user is initially mapped to a default connection profile.

### Client Certificate Authentication

- Custom client-certificate-field-based mapping can place the user in any connection profile.
- Otherwise, user is initially mapped to a default connection profile.
- You can then allow the user to select the connection profile (if allowed).

Remote Access SSL VPN

© 2010 Cisco Systems, Inc. All rights reserved.

VPN 11-00-110

In order to assign a remote user to a connection profile, the Cisco ASA adaptive security appliance provides a rich set of features that differ based on the access method used.

If you deploy full tunneling or clientless SSL VPN and use password (or one-time password) authentication, you can perform the following actions:

- Allow the user to select the connection profile before login. The user can choose the connection profile from a drop-down menu that appears in the browser (for clientless SSL VPNs), or a menu in the Cisco AnyConnect VPN Client interface.
- If the user does not choose a connection profile before login, the user is initially mapped to the DefaultWebVPNGroup (clientless SSL VPN) or DefaultRAGroup (full tunneling SSL VPN).

If you deploy full tunneling or clientless SSL VPN and use authentication based on a client identity certificates (or a combined authentication using client identity certificates and passwords), you can perform the following actions:

- Use rules that are based on the contents of the client identity certificate to assign a remote user to a connection profile of your choice.
- If there are no identity-certificate-based mapping rules, the user is initially mapped to the DefaultWebVPNGroup (clientless SSL VPN) or DefaultRAGroup (full tunneling SSL VPN).

## Connection Profile Selection

### Group PSK Authentication

- You must specify the connection profile (IKE identity name) as the group name in the Cisco VPN Client.
- The default connection profile is never directly used.

### Client Certificate Authentication

- You cannot specify the connection profile in the Cisco VPN Client connection entry.
- Custom client-certificate-based mapping can place the user in any connection profile.
- Otherwise, the organizational unit field is treated as the connection profile name.
- Otherwise, the client maps to the default connection profile.

Remote Access IPsec VPN

©2010 Cisco Systems, Inc. All rights reserved.

VPN-00011

If you deploy a remote-access IPsec VPN:

- You must specify the connection profile (the Internet Key Exchange [IKE] identity) as the group name in the Cisco SSL VPN Client. Depending on the authentication method, you will configure a password (group pre-shared key [PSK]) or identify a certificate that is used for authentication.
- The default connection profile (DefaultRAGroup) is never used when using group PSK authentication.

If you deploy a remote-access IPsec VPN and use certificate-based client authentication (or a combined authentication using client identity certificates and passwords), the following restrictions apply:

- You cannot specify the connection profile (group name) in the Cisco SSL VPN Client.
- Customized certificate-to-connection-profile maps can assign a remote user to a connection profile of your choice.
- If no custom mapping exists, the Cisco ASA adaptive security appliance examines the identity certificate of the client, and uses the subject organizational unit field as the connection profile name, if you have configured a connection profile by that name on the Cisco ASA adaptive security appliance.
- If no connection profile has been identified, the user is mapped to the DefaultRAGroup.

## Configuring Connection Profile Selection

### Selection Options

- Allow users to choose a connection profile before connecting in SSL VPNs.
- Configure client-certificate-based mapping to a connection profile if using certificate-based user authentication.
- Lock the connection profile in local user settings:
  - User must select the identified profile or be mapped to it.
  - Otherwise user is denied access.
- For IPsec VPNs:
  - Set the name of the connection profile to the IKE identity (group name in the Cisco VPN Client).

You can map remote clients to connection profiles in a number of ways:

- You may allow SSL VPN users to choose their connection profile manually, before logging into the SSL VPN.
- You can configure a client-certificate-based mapping of remote users to a connection profile. This option is valid if you are using authentication based on client identity certificates.
- You can configure the connection profile lock feature. This feature is available on an individual-user basis. It forces a user to use the specified connection profile, selected either through the drop-down menu, a URL link, or the certificate to a connection profile map. If the user attempts to use another connection profile, connection is denied. The usage of this option is uncommon.
- If you are using an IPsec remote-access VPN, the name of the connection profile is used as the IKE identity during IKE Phase 1 exchange. The name corresponds to the group name in the Cisco SSL VPN Client settings. IKE is discussed in the next module.

## Configuring Connection Profile Selection

### Creating a Connection Profile

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles  
Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles  
Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles

To create a connection profile using Cisco Adaptive Security Device Manager (ASDM), perform the following steps:

- Step 1** Choose **Configuration > Remote Access VPN** (not shown in the figure):
  - To create a connection profile for a *full tunneling SSL VPN*, choose **Network (Client) Access > AnyConnect Connection Profiles**.
  - To create a connection profile for a *clientless SSL VPN*, choose **Clientless SSL VPN Access > Connection Profiles**.
  - To create a connection profile for an *IPsec remote-access VPN*, choose **Network (Client) Access > IPsec Profiles**.
- Step 2** Click **Add** to create a new connection profile.
- Step 3** Assign a name to the new connection profile.
- Step 4** Specify AAA requirements for this connection profile. These functions are covered in later lessons of this course.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the connection profile to the security appliance.

## Configuring Connection Profile Selection

### Allow Users to Choose Connection Profile (SSL VPN)

The screenshot displays the Cisco ASDM configuration interface for SSL VPN Connection Profiles. It includes several callouts and annotations:

- Enable user choice of connection profile:** A callout pointing to the 'Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.' checkbox in the 'Login Page Settings' pane.
- Edit a connection profile:** A callout pointing to the 'Edit' button in the 'Connection Profiles' pane.
- In each profile, define an alias and enable the profile for user choice:** A callout pointing to the 'Add' button and the 'Enabled' checkbox in the 'Connection Aliases' table.

The 'Connection Profiles' pane shows a list of profiles: 'DefaultWebVPNGroup' (selected), 'DefaultWebVPNGroup', and 'DefaultWebVPNGroup'. The 'Edit SSL VPN Connection Profile: MY-PROFILE' pane is open, showing the 'Advanced' tab with 'SSL VPN' selected. The 'Connection Aliases' pane shows a table with one alias: 'my-workshop' (Enabled).

At the bottom, a 'Login' page is shown with fields for 'USERNAME' (containing 'my-workshop') and 'PASSWORD' (containing '1234567890').

Configuration > Remote Access > VPN > Network (Client) Access > AnyConnect Connection Profiles

To allow remote users to select the connection profile to use for their SSL VPN connection, you need to enable this functionality globally, and define aliases in connection profiles that will allow users to choose connection profiles that are based on user-friendly aliases.

For SSL VPN configurations using Cisco ASDM, perform these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** (not shown in the figure).
- Step 2** Check the **Allow User to Select Connection Profile, Identified by Its Alias, on the Login Page. Otherwise, DefaultWebVPNGroup Will Be the Connection Profile** check box.
- Step 3** In the list of the connection profiles, choose a connection profile that you wish to make user-selectable, and click the **Edit** button.
- Step 4** Inside each edit connection profile pane, choose **Advanced > SSL VPN**, and click **Add** to create an alias in the Connection Aliases pane.
- Step 5** Configure the alias name, and check the **Enable** check box.

---

**Note** Multiple aliases can be defined for each connection profile.

---

- Step 6** Click **OK** when done.
- Step 7** Click **Apply** to apply the aliases to the security appliance.



## Configuring Connection Profile Selection

### Configure Certificate to Connection Profile Maps

Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

Define rules to map certificates to desired connection profiles (tunnel groups). Use the bottom table to configure map criteria for the selected rule.

Certificate to Connection Profile Maps

Map Name	Rule Priority	Mapped to Connection Profile
MYMAP	10	MY-PROFILE
MYMAP	20	PARTNERS

Mapping Criteria

Field	Component	Operator	Value
Issuer	Common Name (CN)	Equals	My-CA
Subject	Organization (OU)	Equals	IT

Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

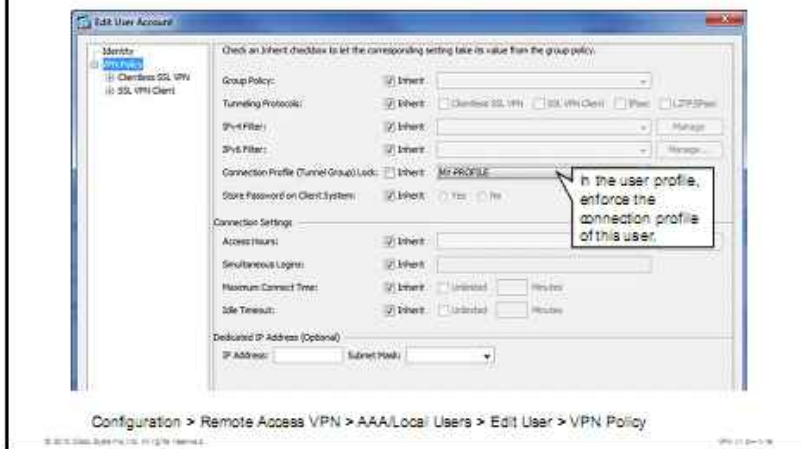
If you use authentication based on client identity certificates, you can optionally deploy connection profile mapping that is based on the contents of the client identity certificate. You can specify criteria that are based on the client certificate fields such as subject name or issuer name, and create conditions that are based on exact matching of the certificate attribute values, partial (subset) matching, or negative matching.

For SSL VPN configurations using Cisco ASDM, perform these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps** (not shown in the figure).
- Step 2** In the Certificate to Connection Profile Maps pane, click **Add** to add a connection-profile-mapping entry.
- Step 3** Choose the certificate map entry, and the connection profile to which to map matching users (not shown in the example). Click **OK**. In the example, two mapping rules are configured. MYMAP rule with priority 10 maps to MY-PROFILE connection profile. MYMAP rule with priority 20 maps to PARTNERS connection profile.
- Step 4** Choose a mapping rule in the Certificate to Connection Profile Maps pane, and click **Add** in the Mapping Criteria pane to add a certificate map entry.
- Step 5** In the new certificate map entry, configure mapping criteria that are based on certificate contents (not shown in the example). Click **OK**. In the example, mapping criteria for MYMAP rule with priority 10 is configured, where the organizational unit field of a certificate should be IT and the common name field should be My-CA.
- Step 6** Click **Apply** to apply the mapping to the security appliance.

## Configuring Connection Profile Selection

### Configuring Per-User Connection Profile Lock



The connection profile lock feature enforces usage of a connection profile to a specific user. It forces a user to use the specified connection profile, selected either through the drop-down menu, a URL link, or the certificate to a connection profile map. If the user attempts to use another connection profile, connection is denied.

To configure a per-user connection profile lock using Cisco ASDM, perform the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users** (not shown in the figure).
- Step 2** Choose a user and click the **Edit** button (not shown in the figure).
- Step 3** Choose **VPN Policy** inside the user profile.
- Step 4** Uncheck the **Inherit** check box next to the **Connection Profile (Tunnel Group) Lock** field.
- Step 5** In the **Connection Profile (Tunnel Group) Lock** field, choose the desired connection profile from a drop-down menu.
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply the connection profile to the security appliance.

## Configuring Connection Profile Selection

### CLI Commands

```
tunnel-group MY-PROFILE type remote-access
tunnel-group MY-PROFILE type webvpn-attributes
  group-alias "IT workers" enable
|
tunnel-group PARTNERS type remote-access
tunnel-group PARTNERS type webvpn-attributes
  group-alias "Company partners" enable
|
crypto ca certificate map MYMAP 10
  subject-name attr ou eq IT
  issuer-name attr cn eq My-CA
|
crypto ca certificate map MYMAP 20
  subject-name attr ou eq Partners
  issuer-name attr cn eq My-CA
|
webvpn
  certificate-group-map MYMAP 10 MY-PROFILE
  certificate-group-map MYMAP 20 PARTNERS
  tunnel-group-list enable
|
username vpmuser password * encrypted
username vpmuser attributes
  group-lock value MY-PROFILE
```

Annotations:

- Create a connection profile.
- Define alias for a connection profile and enable a profile for user choice.
- Create a mapping criteria map.
- Map users to a connection profile.
- Enable user choice of connection profile.
- Go to the attributes of a local user account.
- Map a user to a connection profile.

To configure the selection of a connection profile using the command-line interface (CLI), first create the connection profile itself. Using the CLI, create a connection profile by using the **tunnel-group** command, and create a named connection profile of type remote-access. In the example, the MY-PROFILE and PARTNERS connection profile are created.

To enable user selection of connection profiles, enter webvpn configuration mode and enable user-based profile selection by using the **tunnel-group-list enable** command. Then, inside the webvpn-attributes mode of the connection profile ("tunnel-group"), configure user-friendly names for a connection group by using the **group-alias string enable** command. These strings will be displayed to users in the connection profile drop-down menu. In the example, the "IT workers" alias is configured for the MY-PROFILE connection profile, and the "Company partners" alias is configured for the PARTNERS connection profile.

To configure mappings between certificates and connection profiles, first configure a certificate map by using the **crypto ca certificate map** command. You can create multiple certificate map entries using different sequence numbers to create multiple mapping rules to different connection profiles. In the certificate map, configure mapping criteria based on the certificate contents. Then, in the webvpn configuration mode, use the **certificate-group-map** command to assign a particular certificate map entry to a connection profile.

To configure the lock feature, enter the local user profile configuration by using the **username user attributes** command, and use the **group-lock value** command to assign a connection profile to the local user.

### tunnel-group

To create and manage the database of connection-specific records for IPsec and SSL VPN tunnels, use the **tunnel-group** command in global configuration mode. To remove a tunnel group, use the **no** form of this command.

**tunnel-group** *name* *type* *type*

**no tunnel-group** *name*

## tunnel-group Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel group. This name can be any string that you choose. If the name is an IP address, it is usually the IP address of the peer.
<i>type</i>	<p>Specifies the type of tunnel group:</p> <ul style="list-style-type: none"><li>■ <b>remote-access</b>: Allows a user to connect by using either IPsec remote access or WebVPN (portal or tunnel client)</li><li>■ <b>ipsec-l2l</b>: Specifies IPsec LAN-to-LAN, which allows two sites or LANs to connect securely across a public network like the Internet</li></ul> <hr/> <p><b>Note</b> The following tunnel group types are deprecated in Cisco ASA Software Release 8.0(2):</p> <ul style="list-style-type: none"><li>– <b>ipsec-ra</b>: IPsec remote access</li><li>– <b>webvpn</b>: WebVPN</li></ul> <p>The adaptive security appliance converts these types to the remote access type.</p>

## tunnel-group webvpn-attributes

To enter the webvpn-attributes configuration mode, use the **tunnel-group webvpn-attributes** command in global configuration mode. This mode configures settings that are common to WebVPN tunneling. To remove all WebVPN attributes, use the **no** form of this command.

**tunnel-group** *name* webvpn-attributes

### tunnel-group webvpn-attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel group
<b>webvpn-attributes</b>	Specifies the WebVPN attributes for this tunnel group

## group-alias

To create one or more alternate names (aliases) by which the user can refer to a tunnel group, use the **group-alias** command in tunnel-group webvpn configuration mode. To remove an alias from the list, use the **no** form of this command.

**group-alias** *name* [**enable** | **disable**]

### group-alias Parameters

Parameter	Description
<i>name</i>	Specifies the name of a tunnel group alias. This name can be any string that you choose, except that the string cannot contain spaces.
<b>enable</b>	Enables a previously disabled group alias.
<b>disable</b>	Disables the group alias.

## username attributes

To enter the username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure attribute-value pairs for a specified user.

**username** *name* **attributes**

### username attributes Parameters

Parameter	Description
<i>name</i>	Provides the name of the user

## group-lock

To restrict remote users to access through the tunnel group only, issue the **group-lock** command in group-policy configuration mode or username configuration mode.

To remove the **group-lock** attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy.

**group-lock** {*value tunnel-grp-name* | **none**}

### group-lock Parameters

Parameter	Description
<b>none</b>	Sets the group lock to a null value, thus allowing no group-lock restriction. Prevents inheriting a group-lock value from a default or specified group policy.
<b>value</b> <i>tunnel-grp-name</i>	Specifies the name of an existing tunnel group that the adaptive security appliance requires for the user to connect.

## crypto ca certificate map

To enter certificate authority (CA) certificate map mode, use the **crypto ca certificate map** command in global configuration mode. Executing this command places you in CA certificate map mode. Use this group of commands to maintain a prioritized list of certificate mapping rules. The sequence number orders the mapping rules. To remove a crypto CA certificate map rule, use the **no** form of the command.

**crypto ca certificate map** {*sequence-number* | *map-name* *sequence-number*}

### crypto ca certificate map Parameters

Parameter	Description
<i>map-name</i>	Specifies a name for a certificate-to-group map.
<i>sequence-number</i>	Specifies a number for the certificate map rule that you are creating. The range is 1 through 65,535. You can use this number when creating a tunnel group map, which maps a tunnel group to a certificate map rule.

## subject-name (crypto ca certificate map)

To indicate that a rule entry is applied to the subject distinguished name (DN) of the identity certificate of the client, use the **subject-name** command in crypto CA certificate map configuration mode. To remove a subject name, use the **no** form of the command.

```
subject-name [attr tag] {eq | ne |co | nc} string
```

### subject-name (crypto ca certificate map) Parameters

Parameter	Description
<b>attr tag</b>	(Optional) Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows: <ul style="list-style-type: none"><li>■ CN = Common name</li><li>■ DNQ = DN qualifier</li><li>■ EA = Email address</li><li>■ GENQ = Generational qualifier</li><li>■ GN = Given name</li><li>■ I = Initials</li><li>■ IP = IP address</li><li>■ N = Name</li><li>■ O = Organization name</li><li>■ SER = Serial number</li><li>■ SN = Surname</li><li>■ SP = State/province</li><li>■ T = Title</li><li>■ UNAME = Unstructured name</li></ul>
<b>eq</b>	Specifies that the DN string or indicated attribute must match the entire rule string.
<b>ne</b>	Specifies that the DN string or indicated attribute must not match the entire rule string.
<b>co</b>	Specifies that the rule entry string must be a substring in the DN string or indicated attribute.
<b>nc</b>	Specifies that the rule entry string must not be a substring in the DN string or indicated attribute.
<b>string</b>	Specifies the value to be matched.

## certificate-group-map

To associate a rule entry from a certificate map with a tunnel group, use the **certificate-group-map** command in webvpn configuration mode. To clear current tunnel group map associations, use the **no** form of this command.

```
certificate-group-map certificate_map_name index tunnel_group_name
```

### certificate-group-map Parameters

Parameter	Description
<b>certificate_map_name</b>	The name of a certificate map.
<b>index</b>	The numeric identifier ( <i>sequence-number</i> ) for a map entry in the certificate map. The index value can range from 1 to 65,535.
<b>tunnel_group_name</b>	The name of the tunnel group that is chosen if the map entry matches the certificate. The <i>tunnel_group_name</i> must exist.

## issuer-name

To specify the issuer name DN of all issued certificates, use the **issuer-name** command in local CA server configuration mode. To remove the subject DN from the CA certificate, use the **no** form of this command.

**issuer-name** *DN-string*

### issuer-name Parameters

Parameter	Description
<i>DN-string</i>	Specifies the distinguished name of the certificate, which is also the subject-name DN of the self-signed CA certificate. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains a comma. An issuer name must be less than 500 alphanumeric characters.

**Configuring Connection Profile Selection**

Naming Connection Profile as IKE Identity (IPsec VPN)

Configure a group key to authenticate to this connection profile.

Specify the profile name and password in the connection entry.

```
tunnel-group MY-PROFILE type remote-access
tunnel-group MY-PROFILE ipsec-attributes
pre-shared-key mg1R@Huz1vZUkyg
```

Configure a group key to authenticate to this connection profile.

Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles

In IPsec remote-access VPNs, you must set the connection profile name to the value of the IKE identity that is used in IKE Phase 1 negotiation. This name corresponds to the group name in the Cisco SSL VPN Client (IPsec).

Using the CLI, create the IPsec connection profile, and optionally create a group password for it in the tunnel-group *name* ipsec-attributes configuration mode, using the **pre-shared key** command.

Using Cisco ASDM, perform these steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**.
- Step 2** Add or edit an existing connection profile, and create a strong (long and random) group password in the Pre-shared Key field.
- Step 3** Click **OK**.
- Step 4** Click **Apply** to apply the connection profile to the security appliance.

In the Cisco SSL VPN Client (IPsec), enter the name of the connection profile in the Name field of the connection entry that uses group authentication. Enter the pre-shared key (PSK) in the Password field.

## tunnel-group ipsec-attributes

To enter the ipsec-attributes configuration mode, use the **tunnel-group ipsec-attributes** command in global configuration mode. This mode is used to configure settings that are specific to the IPsec tunneling protocol.

To remove all IPsec attributes, use the **no** form of this command.

**tunnel-group** *name* ipsec-attributes

### tunnel-group ipsec-attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel group
<b>ipsec-attributes</b>	Specifies attributes for this tunnel group

## pre-shared-key

To specify a PSK to support IKE connections that are based on PSKs, use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

**pre-shared-key** *key*

### pre-shared-key Parameters

Parameter	Description
<i>key</i>	Specifies an alphanumeric key between 1 and 128 characters



# Group Policies

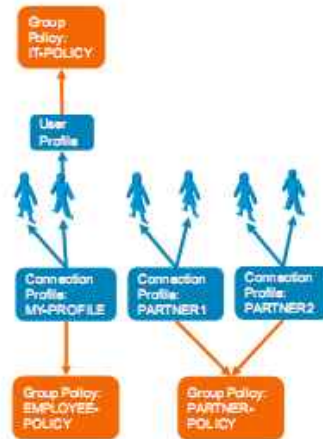
This topic describes how to configure group policies.

## Group Policies

### Definition

Group policies are reusable policy objects that:

- Can apply to connection profiles or user profiles
- Can be applied to multiple connection profiles or users to enable reuse
- Simplify configuration where reuse is required



Group policies are Cisco ASA adaptive security appliance configuration objects that define postlogin network settings and security policies that are to be applied to a remote-access VPN user. These settings and policies include IP addresses (or pools) assigned to remote users, Domain Name System (DNS) servers, access control lists, and so on.

You can apply group policies to connection profiles, or to individual locally configured user profiles when using local AAA. Group policies are reusable; therefore, you can apply the same group policy to multiple connection profiles or user profiles. Group policies can greatly simplify configuration in situations where you need to deploy the same or similar policies to different users.

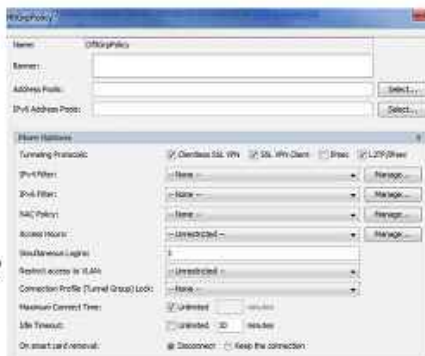
In this example, three connection profiles and two group policies are configured on the Cisco ASA adaptive security appliance. The two users on the left belong to the MY-PROFILE connection profile, and would, by default, be assigned the EMPLOYEE-POLICY group policy. However, the second user from the left is assigned into a different per-user connection profile after login, and thus is assigned a different (IT-POLICY) group policy. The two groups of users in the middle and on the right use different connection profiles, but are assigned the same (PARTNER-POLICY) group policy.

## Group Policies

### Default Group Policy

By default, the Cisco ASA security appliance includes a policy named DfltGrpPolicy:

- DfltGrpPolicy is applied to the default DefaultRAGroup and DefaultWebVPNGroup connection profiles.
- The DfltGrpPolicy is fully customizable.



Configuration > Remote Access VPN > Network (Client) Access > Group Policies

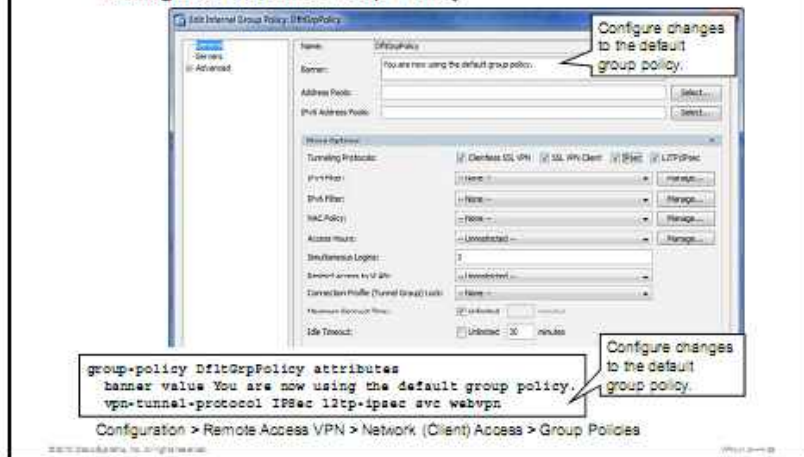
The Cisco ASA adaptive security appliance includes a default group policy called DfltGrpPolicy. This policy is, by default, assigned to the DefaultRAGroup and DefaultWebVPNGroup connection profiles. The DfltGrpPolicy group policy cannot be deleted, but you can fully customize it. You can also disassociate this policy from the two default connection profiles, and attach a group policy with a different name to default connection profiles.

However, the DfltGrpPolicy group policy plays an important role in policy inheritance. You can use policy inheritance to configure scalable complex policies without duplicating your work. In policy inheritance, your custom policies can inherit certain common parameters from the DfltGrpPolicy group policy, hence its proper configuration and tuning are paramount.

As you will see later in this lesson, policy inheritance is used simply by not specifying certain parameters in your custom policies, allowing them to be inherited from the DfltGrpPolicy group policy.

## Configuring Group Policies

### Tuning the Default Group Policy



To tune the default group policy using the CLI, use the **group-policy DfltGrpPolicy attributes banner value** You are now using the default group policy. **vpn-tunnel-protocol IPsec l2tp-ipsec svc webvpn** command in configuration mode.

For remote-access VPN configurations using Cisco ASDM, perform these steps to tune the default group policy:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** (or **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**) (not shown in the example).
- Step 2** Choose **DfltGrpPolicy** and choose **Edit** (not shown in the example).
- Step 3** Change all required settings in the DfltGrpPolicy based on your local requirements.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the changes to the security appliance DfltGrpPolicy group policy.

### group-policy attributes

To enter group-policy configuration mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, use the **no** version of this command. In group-policy configuration mode, you can configure attribute-value pairs for a specified group policy or enter group-policy webvpn configuration mode to configure WebVPN attributes for the group.

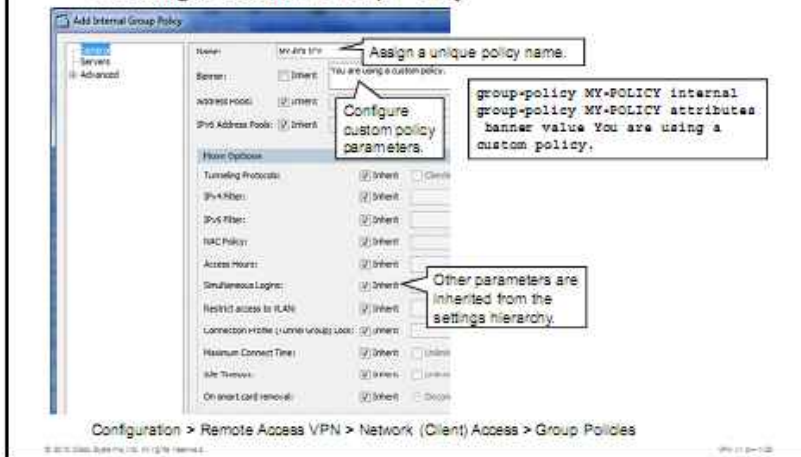
### group-policy name attributes

#### group-policy attributes Parameters

Parameter	Description
name	Specifies the name of the group policy

## Configuring Group Policies

### Creating a Custom Group Policy



To create a new, custom group policy using the CLI, use the **group-policy name internal** command, and change the default attributes of the new group policy by using the **group-policy name attributes** in the attributes configuration mode.

For remote-access VPN configurations using Cisco ASDM, perform these steps to create a new, custom group policy:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** (or **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**) (not shown in the example).
- Step 2** Click the **Add** button (not shown in the example).
- Step 3** Assign a name to the new policy, and change all required settings in the policy based on your local requirements. Note that you can use the Inherit function for almost all policy settings, and inherit their values from the DfltGrpPolicy.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to transfer the new, custom group policy to the security appliance.

### group-policy

To create or edit a group policy, use the **group-policy** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

```
group-policy name { internal [from group-policy_name] | external server-group server_group password server_password }
```

```
no group-policy name
```

## group-policy Parameters

Parameter	Description
<code>name</code>	Specifies the name of the group policy. The name can be up to 64 characters long and cannot contain spaces.
<code>internal</code>	Identifies the group policy as internal.
<code>from group-policy_name</code>	(Optional) Initializes the attributes of this internal group policy to the values of a pre-existing group policy.
<code>external server-group server_group</code>	Specifies the group policy as external and identifies the AAA server group for the adaptive security appliance to query for attributes.
<code>password server_password</code>	Provides the password to use when retrieving attributes from the external AAA server group. The password can be up to 128 characters long and cannot contain spaces.

### Configuring Group Policies

#### Assigning Group Policies to Connection Profiles

```
tunnel-group MY-PROFILE type remote-access
tunnel-group MY-PROFILE general-attributes
default-group-policy MY-POLICY
```

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Edit

Group policies do not perform any function on their own—you need to apply them to either connection profiles or local user profiles.

In order to apply a group policy (a custom group policy or the default group policy) to a connection profile using the CLI, enter the general-attributes configuration mode of a connection profile. Perform this action by using the **tunnel-group name general-attributes** command, and apply the group policy to this connection profile by using the **default-group-policy name** command.

Using Cisco ASDM, perform these steps to apply a group policy to a connection profile:

- Step 1** Choose **Configuration > Remote Access VPN**.
- To attach a group policy to a connection profile for a full tunneling SSL VPN, choose **Network (Client) Access > AnyConnect Connection Profiles**. Proceed to the next step.
  - To attach a group policy to a connection profile for a clientless SSL VPN, choose **Clientless SSL VPN Access > Connection Profiles**. Proceed to the next step.
  - To attach a group policy to a connection profile for an IPsec remote-access VPN, choose **Network (Client) Access > IPsec Connection Profiles**. Proceed to the next step.
- Step 2** Click **Edit** to edit the target connection profile
- Step 3** In the connection profile configuration, choose the appropriate group policy from the Group Policy drop-down list.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to transfer the mapping to the security appliance.

## tunnel-group general-attributes

To enter the general-attributes configuration mode, use the **tunnel-group general-attributes** command in global configuration mode. This mode is used to configure settings that are common to all supported tunneling protocols.

To remove all general attributes, use the **no** form of this command.

**tunnel-group** *name* **general-attributes**

### tunnel-group general-attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel group
<b>general-attributes</b>	Specifies attributes for this tunnel group

## default-group-policy

To specify the set of attributes that the user inherits by default, use the **default-group-policy** command in tunnel-group general-attributes configuration mode. To eliminate a default group policy name, use the **no** form of this command.

**default-group-policy** *group-name*

### default-group-policy Parameters

Parameter	Description
<i>group-name</i>	Specifies the name of the group policy to be applied to the connection profile

## Configuring Group Policies

### Assigning Group Policies to User Profiles



Finally, you can assign a group policy directly to a locally configured user profile, if connection profile-based policies are too coarse for your requirements, and you are using authentication against the local database.

In order to apply a group policy to a local user profile by using the CLI, enter the local user attributes configuration mode by using the **username** name **attributes** command. Then, apply the group policy to this local user profile by using the **vpn-group-policy** name command.

Using ASDM, perform these steps to apply a group policy to a local user profile:

- Step 1** Choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**, choose a local user, and click **Edit** (not shown in the example).
- Step 2** Choose **VPN Policy**.
- Step 3** In the user profile configuration, uncheck the **Inherit** check box next to the group policy, and choose the appropriate group policy from the Group Policy drop-down menu.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to transfer the mapping to the security appliance.

### vpn-group-policy

To have a user inherit attributes from a configured group policy, use the **vpn-group-policy** command in username configuration mode. To remove a group policy from a user configuration, use the **no** version of this command. Using this command lets users inherit attributes that you have not configured at the username level.

**vpn-group-policy** *group-policy-name*

#### vpn-group-policy Parameters

Parameter	Description
<i>group-policy-name</i>	Provides the name of the group policy

## User Profiles

### User Profile Settings

- Remote access VPNs often use username-based authentication:
  - Password or OTP authentication (Extended Authorization [XAUTH]) in IPsec VPNs
  - Password or OTP authentication in SSL VPNs
- You may need to set some parameters or policies on a per-user basis:
  - Per-user IP addresses
  - Per-user tuning (session idle time, ACL, and so on)
- Creating a group policy for a single user is a cumbersome alternative.



Most remote-access VPNs use some sort of user authentication that is based on a username and a password (or one-time password [OTP]), authenticated against the local Cisco ASA adaptive security appliance database, or against a remote AAA server. Often, you may need to set some network parameters or policies, such as a per-user IP address to simplify user tracking, or a per-user ACL, on a per-user basis.

It would be cumbersome to create separate group policies to configure such small exceptions to group policies that are applied to larger sets of users. For that purpose, the Cisco ASA adaptive security appliance allows you to configure per-user exceptions without the need for a dedicated per-user group policy.

In this example, all users shared the same group policy (either by being assigned into the same connection profile or by their different connection profile using the same group policy). However, you can override the group policy settings by specifying per-user settings, as shown in the figure for the user on the right. While per-user settings override group policy settings, all other settings that are applied to the user are inherited from the group policy of the user.

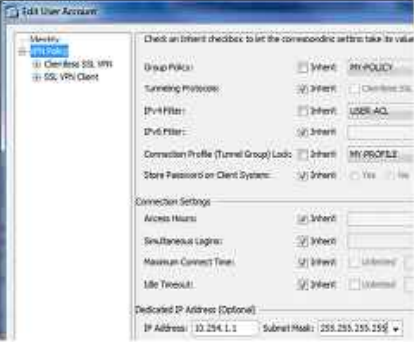


## User Profiles

### Configuring User Profiles

You configure user profiles in the local database:

- A user profile contains all settings normally available in a group policy.
- For multiple users that share the same policy exceptions, consider using a group policy instead.



```
username vpnuser attributes
vpn-filter value USER-ACL
vpn-framed-ip-address 10.254.1.1 255.255.255.255
```

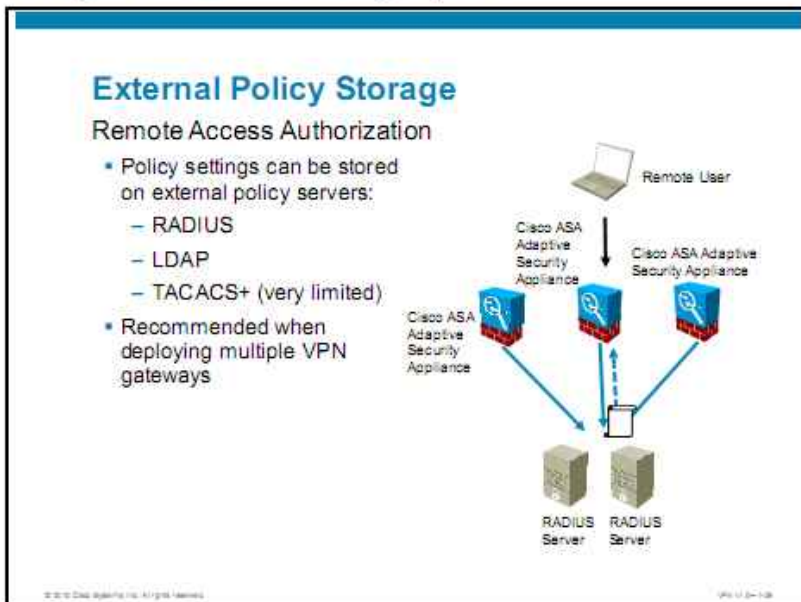
Configuration > Remote Access VPN > AAA/Local Users > Local Users

To configure such exceptions, you can simply edit local user profiles, where you will find all settings that are normally available inside a group policy. If you do not configure a particular setting in a local user profile, its value is automatically inherited from the group policy that is applied to the connection profile of the user.

Note that you should use this option only for settings that are unique to one or a very small number of users. If there are more than a few users sharing these exceptions, consider creating a group policy to cover all these users with common exceptions.

# External Policy Storage

This topic describes the external storage of policies.



Instead of configuring group policy settings locally on the security appliance, you can store these settings in an external, remotely accessible database. This option is especially attractive when you are using a cluster of Cisco ASA adaptive security appliance VPN gateways, and you need to synchronize policies that are assigned to remote users. By using an external server, you can centralize the policy database and allow all Cisco ASA adaptive security appliance VPN gateways to query this server to obtain relevant policies for remote-access VPN users upon their login.

The Cisco ASA adaptive security appliance supports RADIUS, Lightweight Directory Access Protocol (LDAP), and TACACS+ to access the remote policy (authorization) database. Note, however, that while RADIUS and LDAP support the complete set of group policy attributes on the remote server, the TACACS+ protocol only supports very basic remote authorization (assignment of an ACL and session timeouts).

## RADIUS Attribute Reference

This table lists the Cisco vendor-specific attributes and values that are supported by RADIUS and are available for remote-access VPN external authorization.

### Supported RADIUS Attributes and Values

Attribute Name	Attribute Number	Syntax or Type	Single- or Multivalued	Description or Value
Access-Hours	1	String	Single	Name of the time range, for example, Business-hours
Simultaneous-Logins	2	Integer	Single	An integer between 0 and 2,147,483,647

Attribute Name	Attribute Number	Syntax or Type	Single- or Multivalued	Description or Value
Primary-DNS	5	String	Single	An IP address
Secondary-DNS	6	String	Single	An IP address
Primary-WINS	7	String	Single	An IP address
Secondary-WINS	8	String	Single	An IP address
SEP-Card-Assignment	9	Integer	Single	Not used
Tunneling-Protocols	11	Integer	Single	1 = PPTP 2 = L2TP 4 = IPsec 8 = L2TP/IPsec 16 = WebVPN 4 and 8 are mutually exclusive; 0-11 and 16-27 are legal values.
IPSec-Sec-Association	12	String	Single	Name of the security association
IPSec-Authentication	13	Integer	Single	0 = None 1 = RADIUS 2 = LDAP (authorization only) 3 = NT Domain 4 = SDI 5 = Internal 6 = RADIUS with Expiry 7 = Kerberos/Active Directory
Banner1	15	String	Single	Banner string
IPSec-Allow-Passwd-Store	16	Boolean	Single	0 = Disabled 1 = Enabled
Use-Client-Address	17	Boolean	Single	0 = Disabled 1 = Enabled
PPTP-Encryption	20	Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Required 15 = 40/128-Encr/Stateless-Req
L2TP-Encryption	21	Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bit 4 = 128 bits 8 = Stateless-Req 15 = 40/128-Encr/Stateless-Req
Group-Policy	25	String		Sets the group policy for the remote-access VPN session. For version 8.2 and later, use this attribute instead of IETF-Radius-Class. You can use one of the three following formats: <ul style="list-style-type: none"> <li>■ &lt;group policy name&gt;</li> <li>■ OU=&lt;group policy name&gt;</li> <li>■ OU=&lt;group policy name&gt;</li> </ul>
IPSec-Split-Tunnel-List	27	String	Single	Specifies the name of the network or access list that describes the split tunnel inclusion list

Attribute Name	Attribute Number	Syntax or Type	Single- or Multivalued	Description or Value
IPSec-Default-Domain	28	String	Single	Specifies the single default domain name to send to the client (1–255 characters)
IPSec-Split-DNS-Names	29	String	Single	Specifies the list of secondary domain names to send to the client (1–255 characters)
IPSec-Tunnel-Type	30	Integer	Single	1 = LAN-to-LAN 2 = Remote access
IPSec-Mode-Config	31	Boolean	Single	0 = Disabled 1 = Enabled
IPSec-User-Group-Lock	33	Boolean	Single	0 = Disabled 1 = Enabled
IPSec-Over-UDP	34	Boolean	Single	0 = Disabled 1 = Enabled
IPSec-Over-UDP-Port	35	Integer	Single	4001–49,151 default = 10,000
Banner2	36	String	Single	A banner string that is concatenated to the Banner1 string, if configured
PPTP-MPPC-Compression	37	Integer	Single	0 = Disabled 1 = Enabled
L2TP-MPPC-Compression	38	Integer	Single	0 = Disabled 1 = Enabled
IPSec-IP-Compression	39	Integer	Single	0 = Disabled 1 = Enabled
IPSec-IKE-Peer-ID-Check	40	Integer	Single	1 = Required 2 = If supported by peer certificate 3 = Do not check
IKE-Keep-Alives	41	Boolean	Single	0 = Disabled 1 = Enabled
IPSec-Auth-On-Rekey	42	Boolean	Single	0 = Disabled 1 = Enabled
Required-Client-Firewall-Vendor-Code	45	Integer	Single	1 = Cisco (with Cisco Integrated Client) 2 = Zone Labs 3 = Network ICE 4 = Sygate 5 = Cisco (with Cisco Intrusion Prevention Security Agent)
Required-Client-Firewall-Product-Code	46	Integer	Single	Cisco products: 1 = Cisco Intrusion Prevention System Agent or Cisco Integrated Client Zone Labs Products: 1 = ZoneAlarm 2 = ZoneAlarm Pro 3 = Zone Labs Integrity Network ICE Product: 1 = BlackIce Defender/Agent Sygate Products: 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent

Attribute Name	Attribute Number	Syntax or Type	Single- or Multivalued	Description or Value
Required-Client-Firewall-Description	47	String	Single	String
Require-HW-Client-Auth	48	Boolean	Single	0 = Disabled 1 = Enabled
Required-Individual-User-Auth	49	Integer	Single	0 = Disabled 1 = Enabled
Authenticated-User-Idle-Timeout	50	Integer	Single	1–35,791,394 minutes
Cisco-IP-Phone-Bypass	51	Integer	Single	0 = Disabled 1 = Enabled
IPSec-Split-Tunneling-Policy	55	Integer	Single	0 = No split tunneling 1 = Split tunneling 2 = Local LAN permitted
IPSec-Required-Client-Firewall-Capability	56	Integer	Single	0 = None 1 = Policy defined by remote firewall Are-You-There (AYT) 2 = Policy pushed CPP 4 = Policy from server
IPSec-Client-Firewall-Filter-Name	57	String	Single	Specifies the name of the filter to be pushed to the client as firewall policy
IPSec-Client-Firewall-Filter-Optional	58	Integer	Single	0 = Required 1 = Optional
IPSec-Backup-Servers	59	String	Single	1 = Use client-configured list 2 = Disable and clear client list 3 = Use backup server list
IPSec-Backup-Server-List	60	String	Single	Server addresses (space delimited)
DHCP-Network-Scope	61	String	Single	An IP address
Intercept-DHCP-Configure-Msg	62	Boolean	Single	0 = Disabled 1 = Enabled
MS-Client-Subnet-Mask	63	Boolean	Single	An IP address
Allow-Network-Extension-Mode	64	Boolean	Single	0 = Disabled 1 = Enabled
Authorization-Type	65	Integer	Single	0 = None 1 = RADIUS 2 = LDAP
Authorization-Required	66	Integer	Single	0 = No 1 = Yes
Authorization-DN-Field	67	String	Single	Possible values: UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name
IKE-KeepAlive-Confidence-Interval	68	Integer	Single	10–300 seconds

Attribute Name	Attribute Number	Syntax or Type	Single- or Multivalued	Description or Value
WebVPN-Content-Filter-Parameters	69	Integer	Single	1 = Java ActiveX 2 = Java Script 4 = Image 8 = Cookies in images
WebVPN-URL-List	71	String	Single	URL list name
WebVPN-Port-Forward-List	72	String	Single	Port forward list name
WebVPN-Access-List	73	String	Single	Access list name
Cisco-LEAP-Bypass	75	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Homepage	76	String	Single	A URL such as http://example-portal.com
Client-Type-Version-Limiting	77	String	Single	IPsec VPN version number string
WebVPN-Port-Forwarding-Name	79	String	Single	String name (example, "Corporate-Apps"). Text replaces default string "Application Access" on clientless portal home page
IE-Proxy-Server	80	String	Single	An IP address
IE-Proxy-Server-Policy	81	Integer	Single	1 = No modify 2 = No proxy 3 = Autodetect 4 = Use concentrator setting
IE-Proxy-Exception-List	82	String	Single	Newline (\n) separated list of DNS domains
IE-Proxy-Bypass-Local	83	Integer	Single	0 = None 1 = Local
IKE-Keepalive-Retry-Interval	84	Integer	Single	2–10 seconds
Tunnel-Group-Lock	85	String	Single	Name of the tunnel group or "none"
Access-List-Inbound	86	String	Single	Access list ID
Access-List-Outbound	87	String	Single	Access list ID
Perfect-Forward-Secrecy-Enable	88	Boolean	Single	0 = No 1 = Yes
NAC-Enable	89	Integer	Single	0 = No 1 = Yes
NAC-Status-Query-Timer	90	Integer	Single	30–1800 seconds
NAC-Revalidation-Timer	91	Integer	Single	300–86,400 seconds
NAC-Default-ACL	92	String		Access list
WebVPN-URL-Entry-Enable	93	Integer	Single	0 = Disabled 1 = Enabled

Attribute Name	Attribute Number	Syntax or Type	Single- or Multivalued	Description or Value
WebVPN-File-Access-Enable	94	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-File-Server-Entry-Enable	95	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-File-Server-Browsing-Enable	96	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-Enable	97	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Outlook-Exchange-Proxy-Enable	98	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-HTTP-Proxy	99	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Auto-Applet-Download-Enable	100	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Citrix-Metaframe-Enable	101	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Apply-ACL	102	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Enable	103	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Required	104	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Keep-Installation	105	Integer	Single	0 = Disabled 1 = Enabled
SVC-Keepalive	107	Integer	Single	0 = Off 15–600 seconds
SVC-DPD-Interval-Client	108	Integer	Single	0 = Off 5–3600 seconds
SVC-DPD-Interval-Gateway	109	Integer	Single	0 = Off 5–3600 seconds
SVC-Rekey-Time	110	Integer	Single	0 = Disabled 1–10,080 minutes
WebVPN-Deny-Message	116	String	Single	Valid string (up to 500 characters).
Extended-Authentication-On-Rekey	122	Integer	Single	0 = Disabled 1 = Enabled
SVC-DTLS	123	Integer	Single	0 = False 1 = True
SVC-MTU	125	Integer	Single	MTU value 256–1406 in bytes

Attribute Name	Attribute Number	Syntax or Type	Single- or Multivalued	Description or Value
SVC-Modules	127	String	Single	String (name of a module).
SVC-Profiles	128	String	Single	String (name of a profile).
SVC-Ask	131	String	Single	0 = Disabled 1 = Enabled 3 = Enable default service 5 = Enable default clientless (2 and 4 not used)
SVC-Ask-Timeout	132	Integer	Single	5–120 seconds
IE-Proxy-PAC-URL	133	String	Single	PAC address string
Strip-Realm	135	Boolean	Single	0 = Disabled 1 = Enabled
Smart-Tunnel	136	String	Single	Name of a smart tunnel
WebVPN-ActiveX-Relay	137	Integer	Single	0 = Disabled Otherwise = Enabled
Smart-Tunnel-Auto	138	Integer	Single	0 = Disabled 1 = Enabled 2 = Autostart
Smart-Tunnel-Auto-Signon-Enable	139	String	Single	Name of a smart tunnel auto sign-on list appended by the domain name
VLAN	140	Integer	Single	0–4094
NAC-Settings	141	String	Single	Name of NAC policy
Member-Of	145	String	Single	Comma-delimited string, for example: Engineering, Sales Administrative attribute that can be used in DAP; does not set a group policy
Address-Pools	217	String	Single	Name of IP local pool
IPv6-Address-Pools	218	String	Single	Name of IP local pool IPv6
IPv6-VPN-Filter	219	String	Single	ACL value
Privilege-Level	220	Integer	Single	An integer between 0 and 15
WebVPN-Macro-Value1	223	String	Single	Unbounded. See the SSL VPN Deployment Guide for examples and use cases at this URL: <a href="http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x">http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x</a>
WebVPN-Macro-Value2	224	String	Single	Unbounded. See the SSL VPN Deployment Guide for examples and use cases at this URL: <a href="http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x">http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x</a>



# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- The Cisco ASA adaptive security appliance uses a powerful configuration model involving connection profiles, group policies, and user profiles to provide modularity and flexibility.
- Connection profiles define prelogin AAA requirements.
- Group policies define post-login policies and network settings. User profiles can override group policies when per-user exceptions are required. Group policy and user profile inheritance allows you to quickly create policies with complex requirements.
- Use external policy storage with multiple VPN gateways to simplify administration and ensure uniform policy assignment.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-1-2010-02

## References

For additional information, refer to these resources:

- *Configuring an External Server for Security Appliance User Authorization (CLI)* at [http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/ref\\_extserver.html](http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/ref_extserver.html)
- *Configuring an External Server for Authorization and Authentication (ASDM)* at [http://www.cisco.com/en/US/docs/security/asdm/6\\_2/user/guide/extservr.html](http://www.cisco.com/en/US/docs/security/asdm/6_2/user/guide/extservr.html)



# Module Summary

This topic summarizes the key points that were discussed in this module.

## Module Summary

- The Cisco ASA adaptive security appliance provides a rich set of network integration, access control, and VPN features that work in concert to provide multifunction security functions to an organization.
- Remote access VPNs involve various classes of remote users connecting to a protected network over an untrusted transport network.
- Site-to-site VPNs can connect geographically dispersed sites of the same enterprise over a public network, lowering cost and providing scalable performance.

© 2010 Cisco Systems, Inc. All rights reserved.

ASA-11-1001



# Deployment of Cisco ASA Adaptive Security Appliance IPsec VPN Solutions

---

## Overview

The Cisco ASA adaptive security appliance supports site-to-site IP Security (IPsec) virtual private networks (VPNs) and remote access IPsec VPNs, which can be managed using the Cisco Easy VPN solution. While site-to-site IPsec VPNs protect traffic between remote and central sites, remote-access IPsec VPNs protect traffic between mobile workers and a central site. This module describes how to configure basic and certificate-based site-to-site IPsec VPNs. It also describes how to deploy remote access IPsec VPNs, including preshared authentication, certificate-based authentication, and advanced public key infrastructure (PKI) integration. The module describes remote access deployments that use the Cisco VPN Client and Cisco Easy VPN Remote hardware client.

## Module Objectives

Upon completing this module, you will be able to implement and maintain site-to-site IPsec VPNs and Cisco Easy VPN solutions on the Cisco ASA adaptive security appliance VPN gateway according to policies and environmental requirements. This ability includes being able to meet these objectives:

- Deploy and manage basic site-to-site IPsec VPN features of the Cisco ASA adaptive security appliance
- Deploy and manage advanced site-to-site IPsec VPN authentication features of the Cisco ASA adaptive security appliance
- Deploy advanced Cisco VPN Client settings to support a range of end users
- Deploy and manage the basic features of the Cisco ASA adaptive security appliance Cisco Easy VPN Server feature
- Deploy advanced authentication methods of the Cisco ASA adaptive security appliance Cisco Easy VPN Server feature to support IPsec VPN clients
- Deploy advanced Cisco Easy VPN Remote setup to support a secure connection between remote and central offices



# Deploying Basic Site-to-Site IPsec VPNs

---

## Overview

The Cisco ASA adaptive security appliance supports site-to-site IP Security (IPsec) virtual private network (VPN) deployments, which can be used to protect traffic between remote and central sites. Basic deployments of site-to-site IPsec VPNs use pre-shared keys (PSKs) for authentication, which is recommended for smaller deployments. This lesson describes how to configure, verify, and troubleshoot basic site-to-site IPsec VPNs.

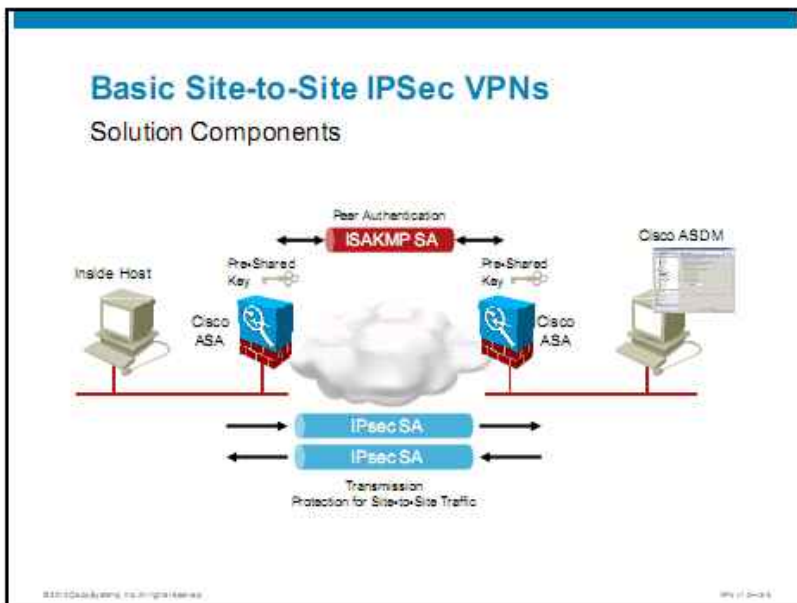
## Objectives

Upon completing this lesson, you will be able to deploy and manage basic site-to-site IPsec VPN features of the Cisco ASA adaptive security appliance. This ability includes being able to meet these objectives:

- Plan a Cisco ASA adaptive security appliance site-to-site VPN
- Configure and verify basic peer authentication in a Cisco ASA adaptive security appliance site-to-site VPN
- Configure and verify transmission protection in a Cisco ASA adaptive security appliance site-to-site VPN
- Troubleshoot the operation of a Cisco ASA adaptive security appliance site-to-site VPN

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic gives an overview of how to plan a Cisco ASA adaptive security appliance site-to-site VPN.



In site-to-site IPsec VPNs, two local networks communicate via an encrypted connection between two VPN gateways. One security appliance is installed at each site and all traffic for remote destinations is routed to the security appliance. The security appliances encrypt and encapsulate the traffic. They also perform all IPsec functionality and route all interoffice VPN traffic through the Internet. This setup does not require installation of any additional software and is referred to as a site-to-site VPN.

When conducting business over a site-to-site VPN tunnel, you must “know” or have verification of who is at the other end of the tunnel. The VPN gateway on the other end of the VPN tunnel must be authenticated before the communications path is considered secure. The last exchange of Internet Key Exchange (IKE) Phase 1 is used to authenticate the remote VPN gateway peer.

In small networks (basic site-to-site VPNs), pre-shared keys (PSKs) can be used to authenticate remote VPN peers. This authentication method is simple, but the PSK must be distributed to remote sites in advance. Using PSKs to authenticate does not scale well in large networks. The preferred method is the exchange of digital certificates to authenticate remote peers.



## Basic Site-to-Site IPsec VPNs

### Cisco ASA Site-to-Site Capacity and Performance

Cisco ASA Adaptive Security Appliance Model	AES or 3DES	Concurrent IPsec Peers	VPN Clustering
ASA 5505 with Base	100 Mb/s	10	No
ASA 5505 with Security Plus	100 Mb/s	25	No
ASA 5510	170 Mb/s	250	Yes (Sec+)
ASA 5520	225 Mb/s	750	Yes
ASA 5540	325 Mb/s	5000	Yes
ASA 5550	425 Mb/s	5000	Yes
ASA 5580-20	1 Gb/s	10,000	Yes
ASA 5580-40	1 Gb/s	10,000	Yes

The table summarizes site-to-site IPsec performance for various Cisco ASA adaptive security appliance models. The performance ranges from 100 Mb/s (and 10 concurrent IPsec peers) for the Cisco ASA 5505 Adaptive Security Appliance model to 1 Gb/s (and 10,000 concurrent IPsec peers) for high-end Cisco ASA 5580-20 Adaptive Security Appliance and Cisco 5580-40 Adaptive Security Appliance models.

## Basic Site-to-Site IPsec VPNs

### Deployment Tasks

- Configure basic peer authentication.
- Configure transmission protection.
- Verify communication over encrypted tunnel.

©2010 Cisco Systems, Inc. All rights reserved.

VPN 11-2-10

To configure a basic site-to-site IPsec VPN, complete the following overall configuration tasks:

1. Configure basic peer authentication.
2. Configure transmission protection.
3. Verify communication over an encrypted tunnel.

## Basic Site-to-Site IPsec VPNs

### Input Parameters

Parameter	Description
Peer IP address	Tunnel endpoint of the opposite adaptive security appliance, usually the outside interface
ISAKMP policy	Protection for Phase 1 ISAKMP SA: encryption, hash, authentication, DH group
PSK	Authentication method used to authenticate other endpoint
Local and remote networks	Traffic that needs to be encrypted and sent through the tunnel
Transform set	Protection for Phase 2 IPsec SA: encryption and hashing algorithm

Before configuring a site-to-site IPsec VPN, you need to collect the following input parameters:

- **Peer IP address:** The peer IP address is the IP address of the opposite Cisco ASA adaptive security appliance, usually the outside interface.
- **ISAKMP policy:** This policy provides protection for Phase 1 Internet Security Association and Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE) security association (SA), including encryption, hash, authentication, and Diffie-Hellman (DH) group.
- **Pre-shared key:** The PSK is used to authenticate the opposite tunnel endpoint.
- **Local and remote networks:** This information defines traffic that needs to be encrypted and sent through the tunnel.
- **Transform set:** The transform set provides protection for Phase 2 IPsec SA, including encryption and hashing algorithm (and optional parameters).

## Basic Site-to-Site IPsec VPNs

### Design and Implementation Guidelines

- Verify network connectivity before encryption
- Use PSKs for small VPNs
- Use separate key for each tunnel
- Avoid unnecessary complexity, which rises with  $n*(n-1)/2$
- Use strong keys against dictionary or brute force attacks (up to 128 characters, uppercase and lowercase, special characters)

© 2010 Cisco Systems, Inc. All rights reserved.

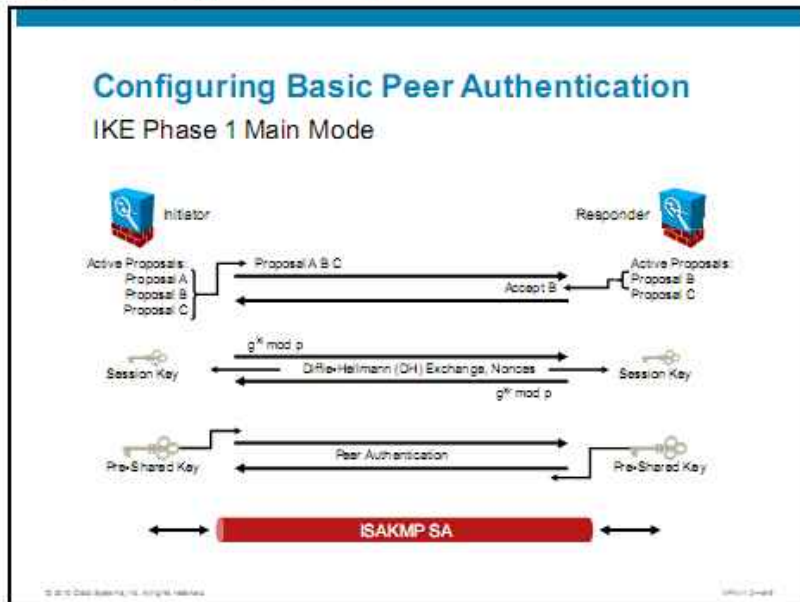
VPN 11-2-07

Consider the following design and implementation guidelines when you configure basic site-to-site IPsec VPNs:

- **Verify network connectivity before encryption:** IPsec VPN peers need to be reachable over the network before they can successfully establish IPsec SAs. You should also verify that required ports are not filtered on any intermediate firewall.
- **Use PSKs for small VPNs:** It is usually recommended to use pre-shared keys for only small VPN deployments. For larger VPN deployments, use digital certificate authentication since it easily scales to hundreds of VPN peers and beyond.
- **Avoid unnecessary complexity:** In a full mesh IPsec VPN deployment, where each IPsec gateway establishes a VPN tunnel to all other IPsec gateways, the number of tunnels grows with  $n*(n-1)/2$ . Design your VPN network connectivity properly to avoid unneeded complexity.
- **Use a separate key for each tunnel:** If you use one key for all tunnels, then IPsec authentication between all the peers is compromised as soon as the key is compromised. If you use different keys for each tunnel, only IPsec authentication for peers using this key is compromised.
- **Use strong keys against dictionary or brute force attacks:** Strong keys are the ones with up to 128 characters, upper and lower case characters, as well as special characters.

# Configuring Basic Peer Authentication

This topic describes how to configure and verify basic peer authentication in a Cisco ASA adaptive security appliance site-to-site VPN.



The basic purpose of IKE (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 or aggressive mode. Aggressive mode is faster, but it does not provide identity protection for the communicating parties like the slower main mode does. Therefore, the peers must exchange identification information before establishing a secure SA. Aggressive mode is enabled by default on the security appliance.

Main mode has six total exchanges (three in each direction) between the initiator and receiver using six packets:

- **First and second exchange:** The algorithms and hashes that are used to secure the IKE communications are negotiated and agreed upon between peers.
- **Third and fourth exchange:** This exchange uses a DH exchange to generate shared secret keys and pass nonces, which are random numbers that are 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.
- **Fifth and sixth exchange:** This exchange verifies the identity of the other side. It is used to authenticate the remote peer. The main outcome of main mode is a secure communication path for subsequent exchanges between the peers. Without proper authentication, you might establish a secure communication channel with a hacker who could be stealing all your sensitive material.

IKE and ISAKMP SA is bidirectional, in contrast to IPsec SAs, which are unidirectional.

## Configuring Basic Peer Authentication

### Configuration Tasks

1. Enable IKE on an interface.
2. Configure IKE policy.
3. Configure PSKs.

To configure basic peer authentication, complete these configuration tasks:

1. Enable IKE on an interface.
2. Configure the IKE policy.
3. Configure PSKs.

## Configuring Basic Peer Authentication

### Configuration Scenario

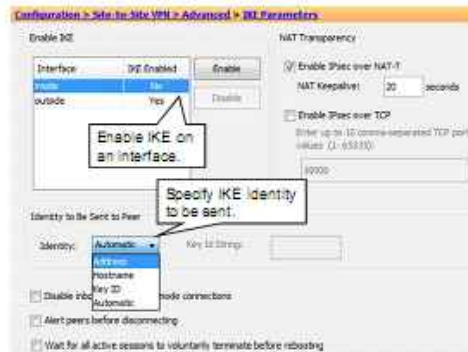


In this configuration scenario, the lesson guides you through setting up an IPsec VPN tunnel between two Cisco ASA adaptive security appliances. You will configure the headquarters (HQ in the figure) security appliance to establish a VPN tunnel over its outside interface to IP address 192.168.226.211, which belongs to the outside interface of the remote branch office security appliance. The tunnel enables direct communication between the HQ LAN (10.0.2.0/24) and the remote branch office LAN (10.0.1.0/24) over an encrypted tunnel.

## Configuring Basic Peer Authentication

### Task 1: Enable IKE on an Interface

- Optionally, specify the IKE identity that is sent to a peer device.



You must enable IKE for each interface that you want to use for VPN connections. To enable IKE on an interface using Cisco Adaptive Security Device Manager (Cisco ASDM), complete the following steps:

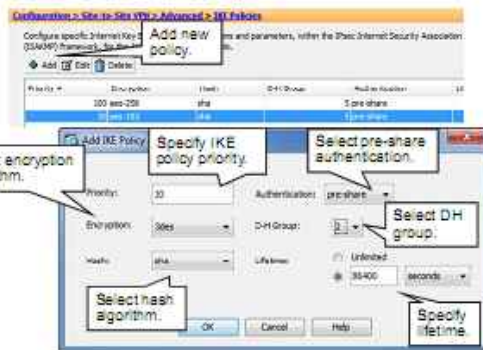
- Step 1** Inside Cisco ASDM, choose **Configuration > Site-to-Site VPN > Advanced > IKE Parameters**.
- Step 2** Select an interface, on which you want to enable IKE processing and click the **Enable** button.
- Step 3** Optionally, you can change how IPsec peers identify themselves to each other. You can choose the identification methods from the following options:
  - **Address:** Uses the IP addresses of the hosts exchanging ISAKMP identity information.
  - **Hostname:** Uses the fully-qualified domain name of the hosts that are exchanging ISAKMP identity information. (This option is the default.) This name comprises the hostname and the domain name.
  - **Key ID:** Uses the string that the remote peer uses to look up the PSK.
  - **Automatic:** Determines IKE negotiation by connection type:
    - IP address for PSK
    - Certificate distinguished name (DN) for certificate authentication
- Step 4** Click **Apply** to apply the configuration.



## Configuring Basic Peer Authentication

### Task 2: Configure IKE Policy

- IKE policies are already configured.
- You can create custom IKE policies.
- Select parameters for IKE policy.



Configuration > Site-to-Site VPN > Advanced > IKE Policies

To add an IKE policy using Cisco ASDM, complete the following steps:

**Step 1** Inside Cisco ASDM, choose **Configuration > Site-to-Site VPN > Advanced > IKE Policies**. The IKE Policy pane lists all active IKE policies and their configured priorities.

**Step 2** Click **Add**. The Add IKE Policy window appears. Select and input the desired values for the IKE policy:

- **Priority:** Type a number to set a priority for the IKE policy. The range is 1 to 65,543, with 1 being the highest priority.
- **Encryption:** Choose an encryption method. The method in this scenario is a symmetric encryption method that protects data that is transmitted between two IPsec peers. The following options in the drop-down list are available to choose from:
  - **des:** This method is 56-bit Data Encryption Standard-Cipher Block Chaining (DES-CBC). It is less secure, but faster, than the alternatives. This option is the default value.
  - **3des:** This method is 168-bit triple DES (3DES).
  - **aes:** This method is 128-bit Advanced Encryption Standard (AES).
  - **aes-192:** This method is 192-bit AES.
  - **aes-256:** This method is 256-bit AES.
- **Hash:** Choose the hash algorithm that ensures data integrity. It ensures that a packet comes from whom you think it comes from, and that it has not been modified in transit:
  - **Sha:** Secure Hash Algorithm 1 (SHA-1)
  - **md5:** Message Digest 5 (MD5)

The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. A successful (but extremely difficult) attack against MD5 has occurred; however, the Hashed Message Authentication Code (HMAC) variant that IKE uses prevents this attack.

- **Authentication:** Choose the authentication method the security appliance uses to establish the identity of each IPsec peer. PSKs do not scale well with a growing network but are easier to set up in a small network. The following options in the drop-down list are available to choose from:
  - **pre-share:** PSKs
  - **rsa-sig:** A digital certificate with keys that are generated by the Rivest, Shamir, and Adleman (RSA) signatures algorithm
  - **crack:** IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK) protocol for mobile IPsec-enabled clients that use authentication techniques other than certificates
- **D-H Group:** Choose the DH group identifier that the two IPsec peers use to derive a shared secret without transmitting it to each other. You can choose from the following:
  - **1:** Group 1 (768 bit). This is the default value.
  - **2:** Group 2 (1024 bit).
  - **5:** Group 5 (1536 bit).
- **Lifetime:** Choose **Unlimited** or type an integer for the SA lifetime. The default is 86,400 seconds or 24 hours. With longer lifetimes, the security appliance sets up future IPsec SA more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. It is recommended that you accept the default.

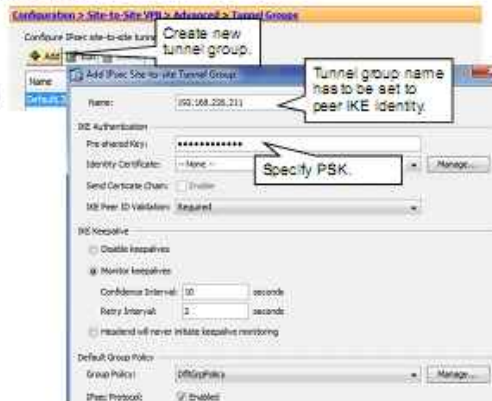
**Step 3** Click **OK**.

**Step 4** Click **Apply** to apply the configuration.

## Configuring Basic Peer Authentication

### Task 3: Configure PSKs

- Create a tunnel group.
- Specify tunnel group name and PSK.



Configuration > Site-to-Site VPN > Advanced > Tunnel Groups

The Add or Edit IPsec Site-to-Site Tunnel Group dialog box lets you specify attributes for the IPsec site-to-site connection that you are adding. In addition, you can select IKE peer and user authentication parameters, configure IKE keepalive monitoring, and select the default group policy.

To add an IPsec site-to-site tunnel group using Cisco ASDM, complete the following steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**.
- Step 2** Click the **Add** button. The Add IPsec Site-to-site Tunnel Group window appears.
- Step 3** Enter the tunnel group name into the Name field. In the example in the figure, 192.168.226.211, the IP address of the peer device, is entered as the name.
- Step 4** Enter the PSK into the Pre-shared Key field.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the configuration.

## Configuring Basic Peer Authentication

### CLI Configuration

```
crypto isakmp enable outside
|
crypto isakmp identity address
|
crypto isakmp policy 10 authen pre-share
crypto isakmp policy 10 encrypt 3des
crypto isakmp policy 10 hash sha
crypto isakmp policy 10 group 2
crypto isakmp policy 10 lifetime 86400
|
tunnel-group 192.168.226.211 type ipsec-l2l
tunnel-group 192.168.226.211 ipsec-attributes
pre-shared-key *****
isakmp keepalive threshold 10 retry 2
```

Enable IKE on the outside interface.

Use IP address as identity.

Configure IKE policy.

Configure tunnel group and attributes.

This output in the figure shows the CLI commands that are required to enable IKE processing on the outside interface, to send the interface IP address to an IPsec peer for identification. The output also shows the commands that are used to configure the IKE policy and to configure the tunnel group and PSK.

Use the **crypto isakmp enable outside** command to enable IKE on the outside interface. Use the **crypto isakmp identity address** command to use IP address as peer IPsec identification.

Use **crypto isakmp policy authen pre-share** to specify that the PSK will be used for authentication. Use the **crypto isakmp policy encrypt** command to specify the encryption algorithm. Use the **crypto isakmp policy hash** command to specify the hashing algorithm. Use the **crypto isakmp policy group** command to specify the DH group. Use the **crypto isakmp policy lifetime** command to specify the SA lifetime.

Use the **tunnel-group** command, followed by the tunnel group name and **type ipsec-l2l** keyword to create a site-to-site type of tunnel group. Use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode to specify a PSK. Use the **isakmp keepalive** command to enable IKE keepalives. IKE keepalives are used to determine whether the remote VPN peer is still up.

### crypto isakmp enable

To enable ISAKMP negotiation on the interface on which the IPsec peer communicates with the adaptive security appliance, use the **crypto isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

**crypto isakmp enable** *interface-name*

#### crypto isakmp enable Parameters

Parameter	Description
<i>interface-name</i>	Specifies the name of the interface on which to enable or disable ISAKMP negotiation

## crypto isakmp identity

To set the IKE Phase 2 ID to be sent to the peer, use the **crypto isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
crypto isakmp identity {address | hostname | key-id key-id-string | auto}
```

### crypto isakmp identity Parameters

Parameter	Description
<b>address</b>	Uses the IP address of the host that is exchanging ISAKMP identity information.
<b>auto</b>	Determines ISAKMP negotiation by connection type: IP address for PSK or certificate DN for certificate authentication.
<b>hostname</b>	Uses the fully-qualified domain name of the host that is exchanging ISAKMP identity information. (This parameter is the default). This name comprises the hostname and the domain name.
<b>key-id</b> <i>key_id_string</i>	Specifies the string that is used by the remote peer to look up the PSK.

## crypto isakmp policy authentication

To specify an authentication method within an IKE policy, use the **crypto isakmp policy authentication** command in global configuration mode. IKE policies define a set of parameters for IKE negotiation. To remove the ISAKMP authentication method, use the related **clear configure** command.

```
crypto isakmp policy priority authentication {crack | pre-share | rsa-sig}
```

### crypto isakmp policy authentication Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<b>crack</b>	Specifies IKE CRACK as the authentication method.
<b>pre-share</b>	Specifies PSKs as the authentication method.
<b>rsa-sig</b>	Specifies RSA signatures as the authentication method. RSA signatures provide nonrepudiation for the IKE negotiation. This nonrepudiation basically means that you can prove to a third party whether you had an IKE negotiation with the peer.

## crypto isakmp policy encryption

To specify the encryption algorithm that should be used within an IKE policy, use the **crypto isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, which is DES, use the **no** form of this command.

```
crypto isakmp policy priority encryption {aes | aes-192 | aes-256 | des | 3des}
```

## crypto isakmp policy encryption Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>aes</i>	Specifies that the encryption algorithm that should be used in the IKE policy is AES with a 128-bit key.
<i>aes-192</i>	Specifies that the encryption algorithm that should be used in the IKE policy is AES with a 192-bit key.
<i>aes-256</i>	Specifies that the encryption algorithm that should be used in the IKE policy is AES with a 256-bit key.
<i>des</i>	Specifies that the encryption algorithm that should be used in the IKE policy is 56-bit DES-CBC.
<i>3des</i>	Specifies that the encryption algorithm that should be used in the IKE policy is triple DES (3DES).

## crypto isakmp policy group

To specify the DH group for an IKE policy, use the **crypto isakmp policy group** command in global configuration mode. IKE policies define a set of parameters to use during IKE negotiation. To reset the DH group identifier to the default value, use the **no** form of this command.

**crypto isakmp policy *priority* group {1 | 2 | 5}**

## crypto isakmp policy group Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>group 1</i>	Specifies that the 768-bit DH group should be used in the IKE policy. This is the default value.
<i>group 2</i>	Specifies that the 1024-bit DH Group 2 (DH2) should be used in the IKE policy.
<i>group 5</i>	Specifies that the 1536-bit DH Group 5 (DH5) should be used in the IKE policy.

## crypto isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **crypto isakmp policy hash** command in global configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

**crypto isakmp policy *priority* hash {md5 | sha}**

## crypto isakmp policy hash Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>md5</i>	Specifies that MD5 (HMAC variant) should be used as the hash algorithm for the IKE policy.
<i>sha</i>	Specifies that SHA-1 (HMAC variant) should be used as the hash algorithm for the IKE policy.

## crypto isakmp policy lifetime

To specify the lifetime of an IKE security association (SA) before it expires, use the **crypto isakmp policy lifetime** command in global configuration mode. You can specify an infinite lifetime if the peer does not propose a lifetime. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command.

**crypto isakmp policy *priority* lifetime *seconds***

## crypto isakmp policy lifetime Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>seconds</i>	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2,147,483,647 sec. Use 0 sec for infinite lifetime.

## tunnel-group

To create and manage the database of connection-specific records for IPsec and Cisco WebVPN tunnels, use the **tunnel-group** command in global configuration mode. To remove a tunnel group, use the **no** form of this command.

**tunnel-group *name* *type* *type***

## tunnel-group Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel group. This can be any string that you choose. If the name is an IP address, it is usually the IP address of the peer.
<i>type</i> <i>type</i>	<p>Specifies the type of tunnel group:</p> <ul style="list-style-type: none"><li>■ <b>remote-access</b>: Allows a user to connect using either IPsec remote access or WebVPN (portal or tunnel client)</li><li>■ <b>ipsec-l2l</b>: Specifies IPsec LAN-to-LAN, which allows two sites or LANs to connect securely across a public network like the Internet</li></ul> <p><b>Note</b> The following tunnel-group types are deprecated in Release 8.0(2):</p> <ul style="list-style-type: none"><li>– <b>ipsec-ra</b>: IPsec remote access</li><li>– <b>webvpn</b>: WebVPN</li></ul> <p>The adaptive security appliance converts these to the <b>remote-access</b> type.</p>

## tunnel-group ipsec-attributes

To enter ipsec-attributes configuration mode, use the **tunnel-group ipsec-attributes** command in global configuration mode. This mode is used to configure settings that are specific to the IPsec tunneling protocol. To remove all IPsec attributes, use the **no** form of this command.

**tunnel-group** *name* ipsec-attributes

### tunnel-group ipsec-attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel group
<b>ipsec-attributes</b>	Specifies attributes for this tunnel group

## pre-shared-key

To specify a PSK to support IKE connections that are based on PSKs, use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

**pre-shared-key** *key*

### pre-shared-key Parameters

Parameter	Description
<i>key</i>	Specifies an alphanumeric key between 1 and 128 characters

## isakmp keepalive

To configure IKE DPD, use the **isakmp keepalive** command in tunnel-group ipsec-attributes configuration mode. In every tunnel group, IKE keepalives are enabled by default with default threshold and retry values. To return the keepalive parameters to enabled with default threshold and retry values, use the **no** form of this command.

**isakmp keepalive** [**threshold** *seconds*] [**retry** *seconds*] [**disable**]

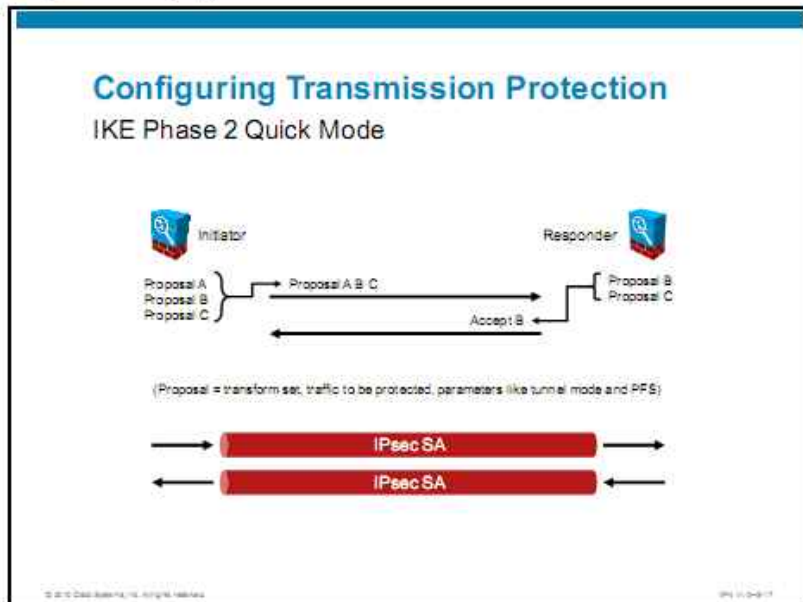
### isakmp keepalive Parameters

Parameter	Description
<b>threshold</b> <i>seconds</i>	Specifies the number of seconds the peer can idle before beginning keepalive monitoring. The range is 10 to 3600 sec. The default is 10 sec for a LAN-to-LAN group, and 300 sec for a remote access group.
<b>retry</b> <i>seconds</i>	Specifies the interval in seconds between retries after a keepalive response has not been received. The range is 2 to 10 sec. The default is 2 sec.
<b>disable</b>	Disables IKE keepalive processing, which is enabled by default.



# Configuring Transmission Protection

This topic describes how to configure and verify transmission protection in a Cisco ASA adaptive security appliance site-to-site VPN.



The purpose of IKE Phase 2 is to negotiate the IPsec security parameters that are used to secure the IPsec tunnel. IKE Phase 2 performs the following functions:

- Negotiates IPsec security parameters and IPsec transform sets
- Establishes IPsec SAs
- Periodically renegotiates IPsec SAs to ensure security
- (Optional) 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 that is 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 invalid SAs.

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

## Configuring Transmission Protection

### Configuration Tasks

1. Select transform set and remote VPN peer.
2. Select traffic for VPN.

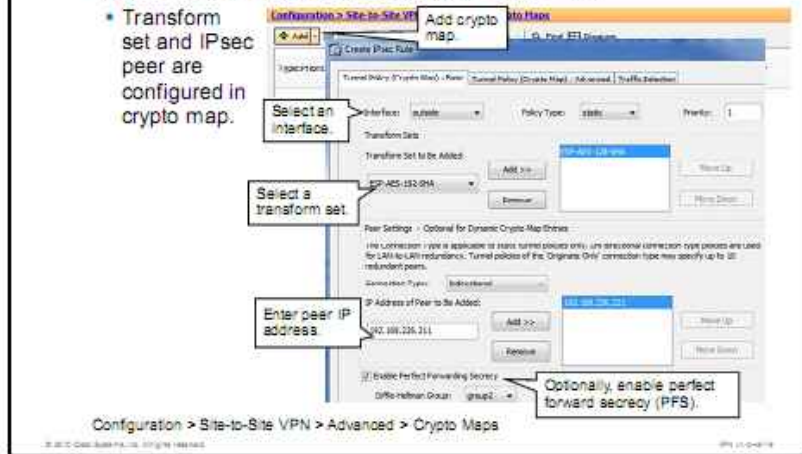
To configure transmission protection, complete these configuration tasks:

1. Select the transform set and VPN peer.
2. Select traffic for the VPN.

## Configuring Transmission Protection

### Task 1: Select Transform Set and VPN Peer

- Transform set and IPsec peer are configured in crypto map.



To create a crypto map using Cisco ASDM, complete the following steps:

- Step 1** Inside Cisco ASDM, choose **Configuration > Site-to-Site VPN > Advanced > Crypto Maps**.
- Step 2** Click **Add** to launch the Create IPsec Rule dialog box, where you can configure basic, advanced, and traffic selection parameters for a rule.
- Step 3** To select transform set and VPN peer, fill-in the necessary information in the Create IPsec Rule dialog-box. The dialog-box has the following fields and options:

- **Interface:** Choose the interface name to which this policy applies.
- **Policy Type:** Choose the type, static or dynamic, of this tunnel policy.
- **Priority:** Enter the priority of the policy.
- **Transform Set to Be Added:** Choose the transform set for the policy and click **Add** to move it to the list of active transform sets. Click **Move Up** or **Move Down** to rearrange the order of the transform sets in the list box. You can add a maximum of 11 transform sets to a crypto map entry or a dynamic crypto map entry.

In the Peer Settings area, you configure the peer settings for the policy:

- **Connection Type** (meaningful only for static tunnel policies): Choose **bidirectional**, **originate-only**, or **answer-only** to specify the connection type of this policy. For LAN-to-LAN connections, choose **bidirectional** or **answer-only** (not originate-only). Choose **answer-only** for LAN-to-LAN redundancy.
- **IP Address of Peer to Be Added:** Enter the IP address of the IPsec peer that you are adding.
- **Enable Perfect Forwarding Secrecy:** Check this check box to enable perfect forward secrecy (PFS) for the policy. PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless you specify PFS.

- **Diffie-Hellman Group:** When you enable PFS, you must also choose a DH group that the security appliance uses to generate session keys. The choices are as follows:
  - **Group 1 (768 bits):** Use PFS, and use Diffie-Hellman Group 1 (DH1) to generate IPsec session keys, where the prime and generator numbers are 768 bits. This option is more secure but requires more processing overhead.
  - **Group 2 (1024 bits):** Use PFS, and use Diffie-Hellman Group 2 (DH2) to generate IPsec session keys, where the prime and generator numbers are 1024 bits. This option is more secure than DH1 but requires more processing overhead.
  - **Group 5 (1536 bits):** Use perfect forward secrecy, and use Diffie-Hellman Group 5 (DH5) to generate IPsec session keys, where the prime and generator numbers are 1536 bits. This option is more secure than DH2 but requires more processing overhead.

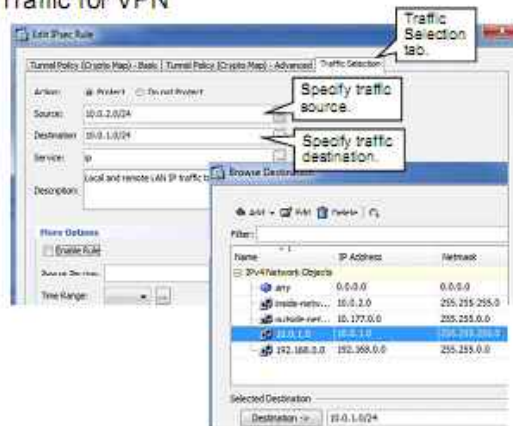
**Step 4** Click **OK**.

**Step 5** Click **Apply** to apply the configuration.

## Configuring Transmission Protection

### Task 2: Select Traffic for VPN

- Source and destination networks must be reversed at remote end.



Configuration > Site-to-Site VPN > Advanced > Crypto Maps

To select the traffic that needs to be protected by the IPsec VPN, complete the following steps:

- Step 1** Click the **Traffic Selection** tab.
- Step 2** In the Action row, you can select the action for this rule to take. There are two possible choices:
  - Protect
  - Do not Protect

In this configuration scenario, Protect has been chosen.

- Step 3** In the Source and Destination fields, list the appropriate network addresses. You can list multiple networks in each field. To select the networks, click the ... (ellipsis) button. The Browse Destination dialog-box opens. In this configuration scenario, 10.0.2.0/24 has been selected as source and 10.0.1.0/24 as destination.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration.

## Configuring Transmission Protection

### CLI Configuration

```
access-list CRYPTO_ACL line 1 remark Local and remote LAN
access-list CRYPTO_ACL line 2 extended permit ip 10.0.2.0 255.255.255.0
10.0.1.0 255.255.255.0
!
crypto map CRYPTO_MAP 1 match address CRYPTO_ACL
crypto map CRYPTO_MAP 1 set pfs group2
crypto map CRYPTO_MAP 1 set peer 192.168.226.211
crypto map CRYPTO_MAP 1 set transform-set ESP-AES-128-SHA
crypto map CRYPTO_MAP interface outside
```

ACL defines traffic to be protected.

Configure crypto map.

To configure transmission protection using the CLI, these two configuration elements are required:

- An access list, which defines the traffic that is to be protected by the IPsec
- A crypto map, which specifies the following:
  - Access list (CRYPTO\_ACL in this example)
  - DH group with optional PFS (pfs group2 in the example)
  - Crypto peer (192.168.226.211 in the example)
  - Transform set (ESP-AES-128-SHA in the example)
  - Interface to which the crypto map is applied (outside in the example)

### crypto map match address

To assign an access control list (ACL) to a crypto map entry, use the **crypto map match address** command in global configuration mode. To remove the ACL from a crypto map entry, use the **no** form of this command.

**crypto map** *map-name seq-num match address acl\_name*

#### crypto map match address Parameters

Parameter	Description
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number that you assign to the crypto map entry.
<i>acl_name</i>	Specifies the name of the encryption ACL. This name should match the <i>name</i> argument of the named encryption ACL being matched.

## crypto map set pfs

Use the **crypto map set pfs** command in global configuration mode to set IPsec to ask for PFS when IPsec requests new SAs for this crypto map entry or to indicate that IPsec requires PFS when IPsec receives requests for new security associations. To specify that IPsec should not request PFS, use the **no** form of this command.

```
crypto map map-name seq-num set pfs [group1 | group2 | group5]
```

### crypto map set pfs Parameters

Parameter	Description
<i>map-name</i>	Specifies the name of the crypto map set
<i>seq-num</i>	Specifies the number that you assign to the crypto map entry
<b>group1</b>	Specifies that IPsec should use the 768-bit DH prime modulus group when performing the new DH exchange
<b>group2</b>	Specifies that IPsec should use the 1024-bit DH prime modulus group when performing the new DH exchange
<b>group5</b>	Specifies that IPsec should use the 1536-bit DH prime modulus group when performing the new DH exchange

## crypto map set peer

To specify an IPsec peer in a crypto map entry, use the **crypto map set peer** command in global configuration mode. To remove an IPsec peer from a crypto map entry, use the **no** form of this command.

```
crypto map map-name seq-num set peer {ip_address | hostname}{...ip_address | hostname10}
```

### crypto map set peer Parameters

Parameter	Description
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number that you assign to the crypto map entry.
<b>peer</b>	Specifies an IPsec peer in a crypto map entry either by hostname or IP address.
<i>ip_address</i>	Specifies a peer by its IP address.
<i>hostname</i>	Specifies a peer by its hostname as defined by the adaptive security appliance name command.

## crypto map set transform-set

To specify the transform sets that should be used in a crypto map entry, use the **crypto map set transform-set** command in global configuration mode.

```
crypto map map-name seq-num set transform-set transform-set-name1 [...transform-set-name11]
```

To specifically remove the names of the transform sets from a crypto map entry, use the **no** form of this command with the specified transform set name.

```
no crypto map map-name seq-num set transform-set transform-set-name1 [...transform-set-name11]
```

To specify all or none of the transform sets and remove the crypto map entry, use the **no** form of the command.

**no crypto map** *map-name seq-num set transform-set*

### crypto map set transform-set Parameters

Parameter	Description
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the sequence number that corresponds to the crypto map entry.
<i>transform-set-name1</i> <i>transform-set-name11</i>	Specifies one or more names of the transform sets. Any transform sets that are named in this command must be defined in the <b>crypto ipsec transform-set</b> command. Each crypto map entry supports up to 11 transform sets.

### crypto map interface

To apply a previously defined crypto map set to an interface, use the **crypto map interface** command in global configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

**crypto map** *map-name interface interface-name*

### crypto map interface Parameters

Parameter	Description
<i>map-name</i>	Specifies the name of the crypto map set.
<i>interface-name</i>	Specifies the interface for the adaptive security appliance to use for establishing tunnels with VPN peers. If ISAKMP is enabled, and you are using a certificate authority (CA) to obtain certificates, this interface should be the interface with the address that is specified in the CA certificates.



## Alternate Configuration

### Configure Connection Profile

Configuration > Site-to-Site VPN > Connection Profiles

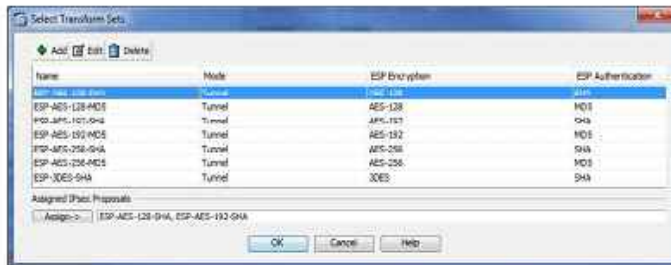
There are three basic ways to add a site-to-site IPsec VPN tunnel:

- You can use the IPsec VPN Wizard to add a site-to-site VPN.
- You can use the Site-to-Site VPN > Advanced menus to add or modify a site-to-site VPN configuration.
- You can use the Site-to-Site VPN > Connection Profiles menus to add or modify a site-to-site VPN.

To configure a site-to-site tunnel using the connection profiles, choose **Configuration > Site-to-Site VPN > Connection Profiles** to go to the site-to-site VPN navigation pane. In the Connection Profiles pane, click the **Add** button to begin configuring the connection profile.

## Alternate Configuration

### Tune IPsec Transform Sets

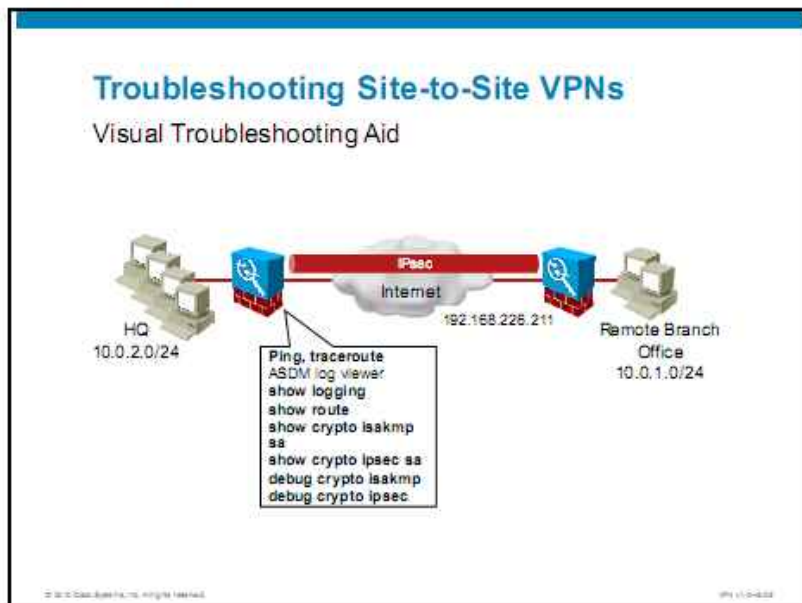


Configuration > Site-to-Site VPN > Connection Profiles

The connection profiles reference an IKE proposal and IPsec proposal (transform set). You may tune any of these entries by navigating to Configuration > Site-to-Site VPN > Advanced > IKE Policies or to Configuration > Site-to-Site VPN > Advanced > IPsec Transform Sets.

# Troubleshooting a Cisco ASA Adaptive Security Appliance Site-to-Site VPN

This topic describes how to troubleshoot the operation of a Cisco ASA adaptive security appliance site-to-site VPN.



The figure presents useful tools for troubleshooting site-to-site VPNs on the Cisco ASA adaptive security appliance. When you troubleshoot IPsec site-to-site VPN tunnels, you should troubleshoot both ends of the tunnel.

## Troubleshooting Site-to-Site VPNs

### Verification of Established ISAKMP Tunnels

```
ASA#show crypto isakmp sa detail

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during
rekey)
Total IKE SA: 1

1 IKE Peer: 192.168.226.211
  Type    : L2L           Role    : responder
  Rekey   : no          State   : MM_ACTIVE
  Encrypt : des          Hash    : SHA
  Auth    : preshared    Lifetime: 86400
  Lifetime Remaining: 86150
```

The figure shows how to verify established ISAKMP tunnels as a result of Phase 1 negotiation. The **show crypto isakmp sa detail** command shows the IP address of the IKE peer, type of connection, encryption and hashing algorithm and authentication method, role of the device and state of the connection. The desired state is **MM\_ACTIVE**. In this example, one IKE tunnel is active.

#### show crypto isakmp sa

To display the IKE run-time SA database, use the **show crypto isakmp sa** command in global configuration mode or privileged EXEC mode.

**show crypto isakmp sa [detail]**

#### show crypto isakmp sa Parameters

Parameter	Description
<b>detail</b>	Displays detailed output about the SA database

## Troubleshooting Site-to-Site VPNs

### Verification of Established IPsec Tunnels

```
ASA#show crypto ipsec sa detail
interface: outside
  Crypto map tag: outside_map0, seq num: 1, local addr: 192.168.225.211
    access-list outside_cryptomap extended permit ip 10.0.2.0 255.255.255.0
10.0.1.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.0.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)
      current_peer: 192.168.225.211
      #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
      #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    <...part of the output omitted...>
      local crypto endpt.: 192.168.225.211, remote crypto endpt.:
192.168.225.211
      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 65AAS0FB
      current inbound spi : B900E536
      inbound esp sas:
        spi: 0xB900E536 (3909150006)
          transform: esp-aes esp-sha-hmac no compression
          in use settings ={(L2L, Tunnel, )}
    <...part of the output omitted...>
      outbound esp sas:
        spi: 0x65AAS0FB (1705677051)
          transform: esp-aes esp-sha-hmac no compression
```

The figure shows how to verify the IPsec tunnels that are established as a result of Phase 2 negotiation using the **show crypto ipsec sa detail** command. When you use this command, search for the number of encrypted and decrypted and encapsulated and de-encapsulated packets for individual connection.

### show crypto ipsec sa

To display a list of IPsec SAs, use the **show crypto ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show ipsec sa**.

**show crypto ipsec sa** [*entry* | *identity* | *map map-name* | *peer peer-addr*] [*detail*]

### show crypto ipsec sa Parameters

Parameter	Description
<b>detail</b>	(Optional) Displays detailed error information on what is displayed.
<b>entry</b>	(Optional) Displays IPsec SAs sorted by peer address
<b>identity</b>	(Optional) Displays IPsec SAs sorted by identity, not including ESPs. This is a condensed form.
<b>map map-name</b>	(Optional) Displays IPsec SAs for the specified crypto map.
<b>peer peer-addr</b>	(Optional) Displays IPsec SAs for specified peer IP addresses.

## Troubleshooting Site-to-Site VPNs

### Logging Messages

```
ASA(config)#logging console ?
ASA(config)#logging enable
%ASA-5-713257: Phase 1 failure: Mismatched attribute types for class Group
Description: Rev'd: Group 2 Cfg'd: Group 1
%ASA-5-713257: Phase 1 failure: Mismatched attribute types for class Group
Description: Rev'd: Group 2 Cfg'd: Group 1
%ASA-5-713257: Phase 1 failure: Mismatched attribute types for class Group
Description: Rev'd: Group 2 Cfg'd: Group 1
%ASA-5-713257: Phase 1 failure: Mismatched attribute types for class Group
Description: Rev'd: Group 2 Cfg'd: Group 1
%ASA-7-713236: IP = 172.26.0.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + NOTIFY (11) + NONE (0) total length : 132
%ASA-7-713506: IP = 172.26.0.2, All SA proposals found unacceptable
```

- IKE Phase 1 failure due to mismatched IKE proposals

```
%ASA-4-713903: Group = 172.26.0.2, IP = 172.26.0.1, ERROR, had problems
decrypting packet, probably due to mismatched pre-shared key. Aborting
```

- IKE Phase 1 failure due to mismatched PSK

This example shows logging messages when IKE Phase 1 is not successful because of mismatched IKE proposals (different DH groups). The example also shows a logging message that is shown if PSKs are misconfigured.

## Troubleshooting Site-to-Site VPNs

### Logging Messages (Cont.)

```
ASA(config)#logging console ?
ASA(config)#logging enable
%ASA-7-715001: Group = 192.168.226.211, IP = 192.168.226.211, Generating
Quick Mode Key!
%ASA-6-602303: IPSEC: An outbound LAN-to-LAN SA (SPI= 0x6FADAB52) between
192.168.225.211 and 192.168.226.211 (user= 172.16.0.2) has been created.
%ASA-5-713049: Group = 192.168.226.211, IP = 192.168.226.211, Security
negotiation complete for LAN-to-LAN Group (192.168.226.211) Responder,
Inbound SPI = 0x93c2ea5d, Outbound SPI = 0x6fada9b2
%ASA-6-602303: IPSEC: An inbound LAN-to-LAN SA (SPI= 0x93C2EA5D) between
192.168.225.211 and 192.168.226.211 (user= 172.16.0.2) has been created.
%ASA-7-715080: Group = 192.168.226.211, IP = 192.168.226.211, Starting P2
rekey timer: 3060 seconds.
%ASA-5-713120: Group = 192.168.226.211, IP = 192.168.226.211, PHASE 2
COMPLETED
```

- Successful IKE Phase 2

The figure shows logging messages for successful creation of IPsec SAs and completed IKE Phase 2.

## Troubleshooting Site-to-Site VPNs

### Debugging

- Use these commands for advanced troubleshooting:

```
debug crypto isakmp [level]
```

- Shows debug messages for ISAKMP

```
debug crypto ipsec [level]
```

- Shows debug messages for IPsec

Use the debugging commands shown in the figure for advanced troubleshooting of IPsec VPNs. Avoid using these commands in production environments because they can produce large amounts of output.

### debug crypto isakmp

To show debug messages for ISAKMP, use the **debug crypto isakmp** command in privileged EXEC mode. To stop showing debug messages for ISAKMP, use the **no** form of this command.

**debug crypto isakmp** [timers] [level]

#### debug crypto isakmp Parameters

Parameter	Description
<code>timers</code>	(Optional) Shows debug messages for ISAKMP timer expiration.
<code>level</code>	(Optional) Sets the debug message level to display, using a number between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Levels 2 through 7 show additional information. Level 254 shows decrypted ISAKMP packets in a human readable format. Level 255 shows hexadecimal dumps of decrypted ISAKMP packets.

### debug crypto ipsec

To show debug messages for IPsec, use the **debug crypto ipsec** command in privileged EXEC mode. To stop showing debug messages for IPsec, use the **no** form of this command.

**debug crypto ipsec** [level]

#### debug crypto ipsec Parameters

Parameter	Description
<code>level</code>	(Optional) Sets the debug message level to display, using a number between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- Cisco ASA adaptive security appliance site-to-site VPNs offer a broad range of options and scale from a home office or small office to enterprise deployments.
- Basic site-to-site VPNs for Cisco ASA adaptive security appliance use PSKs for authentication. Keys are configured in tunnel groups. The algorithms for IKE Phase 1 are configured in an ISAKMP policy.
- Transmission protection is configured in crypto maps, defining source and destination as well as transform sets. A configured crypto map with a matching tunnel group creates a connection profile.
- The **show crypto** commands allow verification of the configuration and status of the components and the **debug** commands show details of cryptographic functions in progress.

© 2010 Cisco Systems, Inc. All rights reserved.

990012-06-01



# Deploying Certificate Authentication in Site-to-Site IPsec VPNs

---

## Overview

The Cisco ASA adaptive security appliance supports certificate-based authentication in site-to-site virtual private networks (VPNs), together with rich public key infrastructure (PKI) integration options. Certificates can be used to provide secure and scalable authentication among multiple sites in large site-to-site IP Security (IPsec) VPNs. This lesson describes how to enroll the Cisco ASA adaptive security appliance into a PKI and how to enable certificate-based authentication for site-to-site IPsec VPNs.

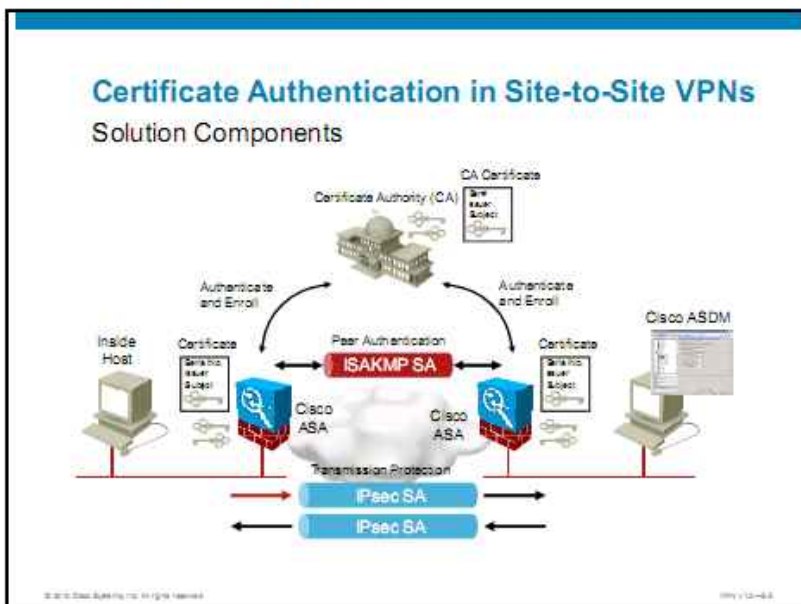
## Objectives

Upon completing this lesson, you will be able to deploy and manage advanced site-to-site IPsec VPN authentication features of the Cisco ASA adaptive security appliance. This ability includes being able to meet these objectives:

- Plan a Cisco ASA adaptive security appliance site-to-site VPN using PKI-based authentication
- Enroll Cisco ASA adaptive security appliance with an external CA and deploy certificate-based authentication
- Configure and verify PKI-based peer authentication in the Cisco ASA adaptive security appliance site-to-site VPN

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic gives an overview of how to plan a Cisco ASA adaptive security appliance site-to-site VPN using PKI-based authentication.



In large networks, the use of a pre-shared key (PSK) to authenticate a remote peer does not scale well. The preferred method is the exchange of digital certificates to authenticate remote peers.

When digital certificates are used for peer authentication, a certificate authority (CA) is needed that is trusted by all the communicating parties. Each IPsec peer needs to authenticate and enroll with the CA. In this way, each IPsec peer obtains valid private and public cryptographic keys with the corresponding certificate.

During the Internet Security Association and Key Management security association (ISAKMP SA) setup phase, the VPN peers exchange digital certificates as proof of their identity. Exchanged certificates are verified using a CA certificate by checking the signature of the received with the public key of the CA. The CA certificates have to be installed locally on both appliances. To check validity of peer certificates, each appliance also needs access to an accurate time source (such as a Network Time Protocol [NTP] server).

## Certificate Authentication in Site-to-Site VPNs

### Deployment Tasks

- Generate public and private keys on the adaptive security appliance.
- Authenticate CA (install root certificate).
- Enroll ASA with CA (install identity certificate).
- Configure ISAKMP for certificate-based authentication.
- Associate certificate with tunnel group.
- Configure transmission protection.
- Verify certificates and test the tunnel.

These tasks are the overall deployment tasks that must be completed when a site-to-site VPN using PKI-based authentication is deployed:

1. Generate public and private keys on the Cisco ASA adaptive security appliance.
2. Authenticate the CA by installing a root certificate.
3. Enroll the Cisco ASA adaptive security appliance with the CA by installing an identity certificate.
4. Configure ISAKMP for certificate-based authentication.
5. Associate the certificate with a tunnel group.
6. Configure transmission protection for user traffic.
7. Verify certificates and test the tunnel.

## Certificate Authentication in Site-to-Site VPNs

### Input Parameters

Parameter	Description
Peer IP address	Tunnel endpoint of the opposite adaptive security appliance, usually the outside interface
ISAKMP policy	Protection for Phase 1 ISAKMP SA: encryption, hash, authentication, DH group
CA URL and details	URL of the CA for network-based enrollment, CA mode of operation, CA fingerprint
Local and remote networks	Traffic that needs to be encrypted and sent through the tunnel
Transform set	Protection for Phase 2 IPsec SA: encryption and hashing algorithm

The table in the figure describes the input parameters that are used when you deploy a site-to-site VPN using PKI-based authentication:

- **Peer IP address:** The peer IP address is the IP address of the opposite Cisco ASA adaptive security appliance, usually the outside interface.
- **ISAKMP policy:** This policy provides protection for Phase 1 ISAKMP and Internet Key Exchange (IKE) SA, including encryption, hash, authentication, and Diffie-Hellman (DH) group.
- **Certificate authority URL and other details:** This information is used for certificate enrollment.
- **Local and remote networks:** This information defines traffic that needs to be encrypted and sent through the tunnel.
- **Transform set:** The transform set provides protection for Phase 2 IPsec SA, including encryption and hashing algorithm (and optional parameters).

## Certificate Authentication in Site-to-Site VPNs

### Design and Implementation Guidelines

- Verify connectivity before encryption
- Use certificates for larger VPNs
- Avoid unnecessary complexity, which rises with number of IPsec tunnels
- Use appropriately strong RSA keys inside certificates

Consider these design and implementation guidelines when you deploy a site-to-site VPN using PKI-based authentication:

- Verify the connectivity before the encryption
- Use certificates for larger VPNs
- Avoid unnecessary complexity, which rises with the number of IPsec tunnels
- Use appropriately strong Rivest, Shamir, and Adleman (RSA) keys inside certificates

# Deploying Certificate-Based Authentication

This topic describes how to enroll the Cisco ASA adaptive security appliance with an external CA and deploy certificate-based authentication.

## Deploying Certificate Authentication

Configuration Tasks

1. Retrieve CA certificate.
2. Install CA certificate.
3. Create enrollment request.
4. Save enrollment request.
5. Submit enrollment request.
6. Check status of enrollment request.
7. Save identity certificate.
8. Install identity certificate.

© 2010 Cisco Systems, Inc. All rights reserved. VPN 1-10-088

The identity certificate installation process consists of these three tasks:

1. Retrieve the CA certificate.
2. Install the CA certificate.
3. Create the enrollment request.
4. Save the enrollment request.
5. Submit the enrollment request.
6. Check the status of the enrollment request.
7. Save the identity certificate.
8. Install the identity certificate.

The next few figures take you through the complete process of configuring the Cisco ASA adaptive security appliance for digital certificates.

## Deploying Certificate Authentication

### Task 1: Retrieve CA Certificate



Complete these steps to install a CA certificate in the Cisco ASA adaptive security appliance, using a Microsoft CA server:

- Step 1** Bring up the CA certificate main page by entering **http://name or ip-address/certsrv**. The main window should appear as seen in the figure.
- Step 2** Click the **Download a CA Certificate, Certificate Chain, or CRL** link. The Download a CA Certificate window should appear as seen in the next figure.

## Deploying Certificate Authentication

### Task 1: Retrieve CA Certificate (Cont.)

Microsoft Certificate Services - MS-CA

**Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current (MS-CA) Select CA certificate.

Encoding method:

DER

Base 64 Use Base 64 format.

[Download CA certificate](#) Choose Download CA Certificate.

[Download CA certificate chain](#)

[Download latest base CRL](#)

© 2010 Cisco Systems, Inc. All rights reserved. 109 of 109

This window lets you download a CA certificate, download a certificate chain, download the latest certificate revocation list (CRL), and choose the content-transfer-encoding method. Two methods of content transfer encoding are offered.

- **DER:** A message transfer syntax that is specified by the ITU in X.690. It is a method for encoding a data object, such as an X.509 public key infrastructure (PKI) certificate, to be digitally signed or to have its signature verified.
- **Base 64:** A specific Multipurpose Internet Mail Extensions (MIME) content transfer encoding. Base 64 encoding encodes binary data by treating it numerically and translating it into a base 64 representation. The MIME specification, which is defined in RFC 2045, lists "base64" as one of several binary-to-text encoding schemes. The MIME base64 encoding is based on that of the RFC 1421 version of privacy-enhanced mail (PEM). It uses the same 64-character alphabet and encoding mechanism as PEM and uses the "=" symbol for output padding.

**Step 1** Because the Cisco ASA adaptive security appliance does not have a DER option for certificate installation, click the **Base 64** radio button.

**Step 2** Click the **Download CA Certificate** link. The File Download dialog box appears.



## Deploying Certificate Authentication

### Task 1: Retrieve CA Certificate (Cont.)



After you retrieve the certificate, you must save it to the local machine.

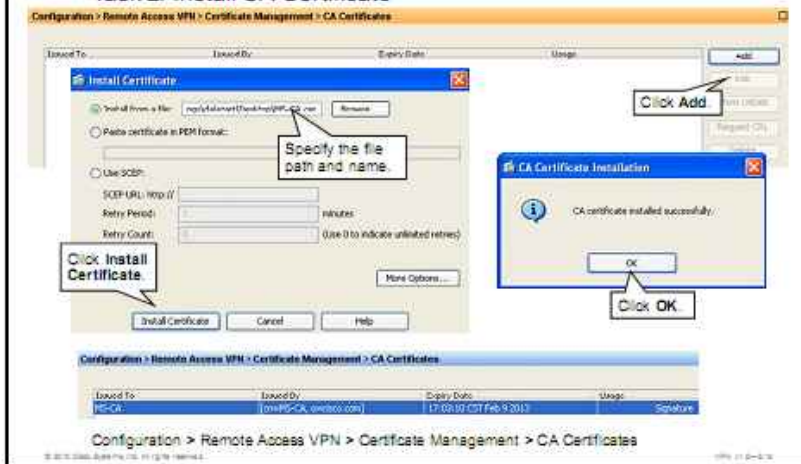
**Step 1** Click **Save** in the file download window. The Save As window appears.

**Step 2** Give the file a unique name and save it to the local machine.

After retrieving the CA certificate and storing it on the local machine, you must open the Cisco Adaptive Security Device Manager (Cisco ASDM) and install the CA certificate.

## Deploying Certificate Authentication

### Task 2: Install CA Certificate



Use the CA Certificates pane to install a new CA certificate. Complete the following steps to install a new CA certificate:

**Step 1** Choose **Configuration > Remote Access VPN > Certificate Management > CA Certificates**.

**Step 2** Click the **Add** button in the upper right corner of the pane. The Install Certificate dialog box appears as seen in the next figure.

To finish installing the CA certificate, complete the following steps:

**Step 1** Click the **Install from a File** radio button.

**Step 2** Use the Browse button or input the name of the CA certificate file that was previously saved to the local machine. In this figure, the filename is **MS\_CA.cer**.

**Step 3** Click the **Install Certificate** button. You should receive a “CA certificate installed successfully” message in the CA Certificate Installation popup window.

The newly installed CA certificate should be visible in the CA Certificates pane.

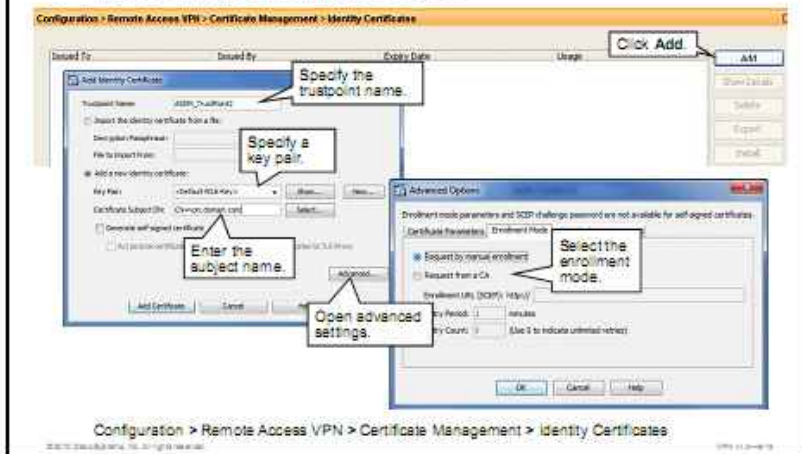
Information that is displayed in the CA Certificate pane includes these items:

- Issued To
- Issued By
- Expiry Date
- Usage

After the CA certificate has been installed, the next step in the process is enrolling with the CA. The procedure for enrolling with the CA follows.

# Deploying Certificate Authentication

## Task 3: Create Enrollment Request



To enroll with a CA, you must submit a certificate request. Then you wait for the CA administrator to grant the certificate, at which time you retrieve the identity certificate.

Complete these steps to create a certificate request:

**Step 1** Choose **Configuration > Remote Access VPN > Certificate Management > Identity Certificates**. The Identity Certificates pane should appear as seen in the figure.

**Step 2** Click the **Add** button on the right side of the pane. The Add Identity Certificate dialog box should appear as seen in the next figure.

Complete these steps to set the parameters for the certificate request using manual enrollment:

**Step 1** Enter the trustpoint name in the Trustpoint Name field. In the example, the default name that is assigned by ASDM is used.

**Step 2** Click the **Add a New Identity Certificate** radio button.

**Step 3** Choose a key pair that will be used by the certificate from the Key Pair drop-down menu. You can also create a new key pair by clicking the **New** button (not shown in the example).

**Step 4** Enter the subject name into the Certificate Subject DN field in distinguished name (DN) format. In the example, CN=vpn.domain.com is used as the subject name.

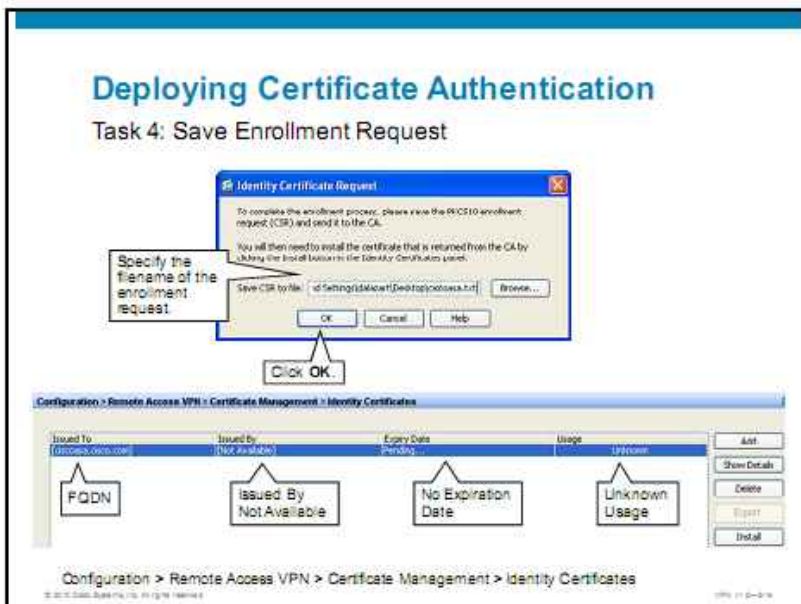
The Advanced Options dialog box allows you to set the proper parameters for a certificate request from a CA. The Advanced Options window has three tabs:

- Certificate Parameters
- Enrollment Mode
- SCEP Challenge Password

**Step 5** Click the **Advanced** button to open advanced settings.

**Step 6** Choose the **Enrollment Mode** tab.

- Step 7** Click the **Request by Manual Enrollment** radio button.
- Step 8** Click **OK**.
- Step 9** Click the **Add Certificate** button. This action enables you to save the certificate request to a file.



The Public-Key Cryptography Standard #10 (PKCS #10) certificate request is saved to the local machine so that it can be pasted into the web page of the CA when you perform a manual enrollment for the Cisco ASA adaptive security appliance. Complete the following steps to save the identity certificate request to your desktop:

- Step 1** Use the **Browse** button to choose or enter the name of the PKCS #10 file.
- Step 2** Click **OK**.

---

**Note** Save the file as a text file.

---

The bottom half of the figure shows the pending certificate request. The Identity Certificates pane now shows the following attributes for the certificate:

- **Issued To:** username.domain (ciscoasa.cisco.com in our example)
- **Issued By:** Not Available
- **Expiry Date:** Pending
- **Usage:** Unknown

The PKCS #10 certificate request has been saved and now must be presented to the CA for manual enrollment.

# Deploying Certificate Authentication

## Task 5: Submit Enrollment Request

Microsoft Certificate Services – MS-CA

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

#### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Click **Request a Certificate**

To view status, click **View the Status of a Pending Certificate Request**

The procedure for requesting a certificate from the CA is the same procedure that is used to request the Cisco IPsec VPN Client certificate. The procedure is summarized here:

- Step 1** Bring up the CA certificate main page by entering **http://name** or **ip-address/certsrv**. The main window should appear as seen in this figure.
- Step 2** Click the **Request a Certificate** link. The Request a Certificate window appears.
- Step 3** Choose the **Advanced Certificate Request** link. The Advanced Certificate Request window appears.
- Step 4** Click **Submit a Certificate Request by Using a Base-64-Encoded CMC or PKCS#10 File**, or click the **Submit a Renewal Request by Using a Base-64-Encoded PKCS#7 File** link. The Submit a Certificate or Renewal Request window appears.
- Step 5** Paste the contents of the PKCS #10 file into the Saved Request pane.
- Step 6** Click the **Submit** button. The Certificate Pending window appears.
- Step 7** The CA administrator should issue the certificate at this point.
- Step 8** After the appropriate amount of time, return to the CA server web page and check the status of the certificate.
- Step 9** Bring up the CA certificate main page by entering **http://name** or **ip-address/certsrv** again.
- Step 10** Click the **View the status of a pending certificate request** link from the main window. The Pending Certificate Request window should appear.

The preceding figure shows the links that you use to submit a request and to view the status of a request. The next figure shows the message that you receive after you make a request, but before a certificate has been issued.

## Deploying Certificate Authentication

### Task 6: Check Status of Enrollment Request

Microsoft Certificate Services — MS-CA

#### Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 8.

Please return to this web site in a day or two to retrieve your certificate.

**Note:** You must return with this web browser within 10 days to retrieve your certificate.

Microsoft Certificate Services — MS-CA

#### View the Status of a Pending Certificate Request

Select the certificate request you want to view.

[Saved-Request Certificate \(Tuesday February 12 2008 5:00:43 PM\)](#)

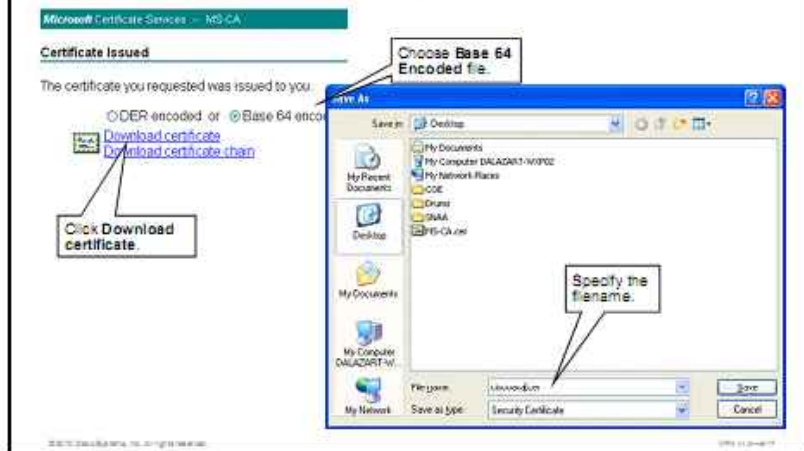
© 2010 Cisco Systems, Inc. All rights reserved. 1000 01-0-0-0

Next, you must check the status of the enrollment request to find out if it has been issued. The issued certificate must be retrieved in the proper format. Complete the following steps to retrieve the certificate:

**Step 1** Click the **Saved-Request Certificate** link. The Certificate Issued window appears.

## Deploying Certificate Authentication

### Task 7: Save Identity Certificate



**Step 2** Click the **Base 64 Encoded** radio button.

**Step 3** Click the **Download Certificate** link. The File Download security warning appears as seen in the next figure.

In the preceding figures, you see the saved certificate request link and the choice of DER or Base 64 encoding for the file MIME content transfer encoding. When you click the Download Certificate link, the file download process begins.

Give the certificate file a unique name and make a note of where you save the file. Complete the following steps to save the certificate file to the local machine:

**Step 1** Click the **Save** button in the File Download – Security Warning window. The Save As window appears.

**Step 2** Give the file a unique name and click the **Save** button in the Save As window.

The only procedure that is left to do is to install the retrieved certificate on the security appliance. That procedure is described in the following section. In the example in the figure, the file named ciscoasa.cer is saved to the desktop.





# Configuring PKI-Based Peer Authentication

This topic describes how to configure and verify PKI-based peer authentication in a Cisco ASA adaptive security appliance site-to-site VPN.

## Configuring PKI-Based Authentication

### Configuration Tasks

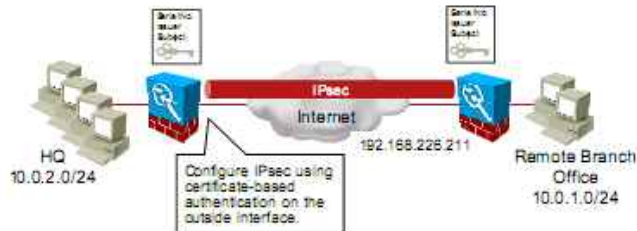
1. Create connection profile.
2. Choose identity certificate.
3. Define interesting traffic.
4. Configure IKE policy.
5. Configure transform set.
6. (Optional) Tune crypto map parameters.
7. (Optional) Tune tunnel group parameters.
8. Configure certificate map policy.
9. (Optional) Define certificate to connection profile map.

To configure certificate-based site-to-site authentication, you will perform these tasks:

1. Create a connection profile.
2. Choose the identity certificate.
3. Define interesting traffic.
4. Configure the IKE policy.
5. Configure the transform set.
6. Optionally, tune crypto map parameters.
7. Optionally, tune tunnel group parameters.
8. Configure the certificate map policy.
9. Optionally, define the certificate-to-connection profile map.

## Configuring PKI-Based Authentication

### Configuration Scenario



The figure represents the scenario that is used in this topic.

After the CA certificate and identity certificates are stored on the security appliance, the site-to-site VPN tunnel can be configured.

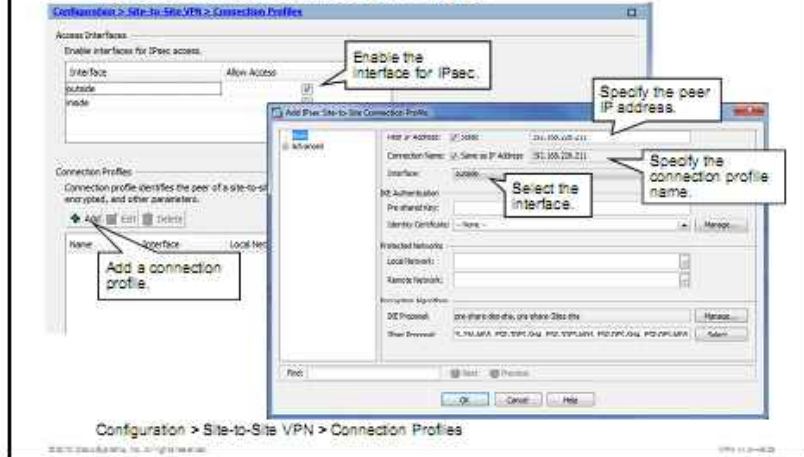
There are three basic ways to add a site-to-site IPsec VPN tunnel:

- You can use the IPsec VPN Wizard to add a site-to-site VPN.
- You can use the Site-to-Site VPN > Advanced menus to add or modify a site-to-site VPN configuration.
- You can use the Site-to-Site VPN > Connection Profiles menus to add or modify a site-to-site VPN.

This section discusses how to configure a site-to-site tunnel using the connection profiles.

# Configuring PKI-Based Authentication

## Task 1: Create Connection Profile



To start building a connection profile, you enable IPsec access on select security appliance interfaces and then add a connection profile. Complete the following steps:

- Step 1** Choose **Configuration > Site-to-Site VPN > Connection Profiles**.
- Step 2** In the **Access Interfaces** area, check the check box next to the interface on which you want to allow IPsec access. In the example, the **Outside** interface check box was checked.
- Step 3** In the **Connection Profiles** area, click the **Add** button to begin configuring the connection profile. The **Add IPsec Site-to-Site Connection Profile** dialog box appears.

By choosing the **Basic** option in the navigation pane of **Add IPsec Site-to-Site Connection Profile** window, the **Add IPsec Site-to-Site Connection Profile—Basic** dialog box opens. The fields within the **Add IPsec Site-to-Site Connection Profile—Basic** window enable you to specify:

- Peer IP address
- Connection name
- Interface choice
- IKE authentication parameters
- Protected networks
- Encryption algorithms

The next few figures and accompanying text explain how each section of the **Add IPsec Site-to-Site Connection Profile—Basic** window is completed.

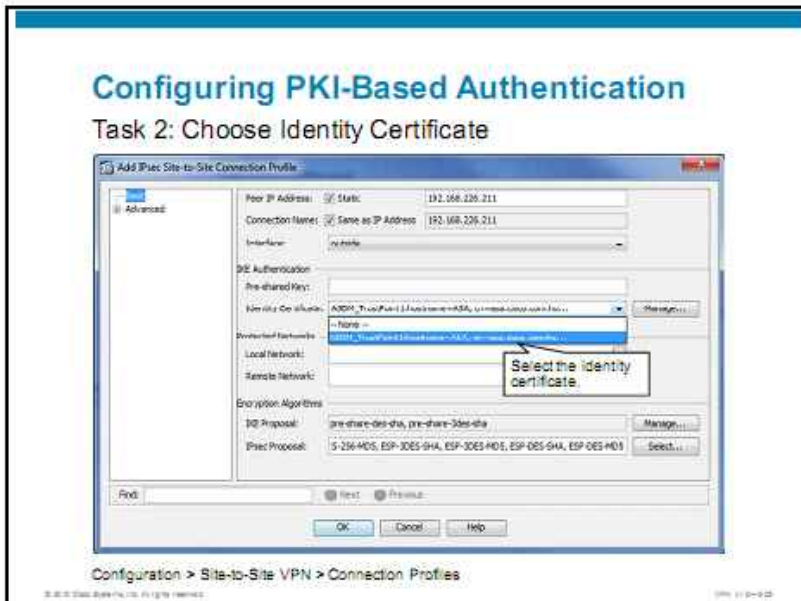
The top section of the window enables you to define the IPsec site-to-site remote peer. To configure the remote peer, complete the following steps:

- Step 1** Next to the **Peer IP Address**, check the **Static** check box. In the following field, enter the IP address of the interface on the remote peer where the tunnel terminates.

**Step 2** By checking the Same as IP Address check box, you can specify that the connection name is the same as the IP address that is specified in the Peer IP Address field.

**Step 3** In the Interface field, choose the local security appliance interface to use for this connection.

In the example in the figure, the IP address of the remote peer IPsec tunnel interface is 192.168.226.211. The tunnel terminates on the remote security appliance outside interface.

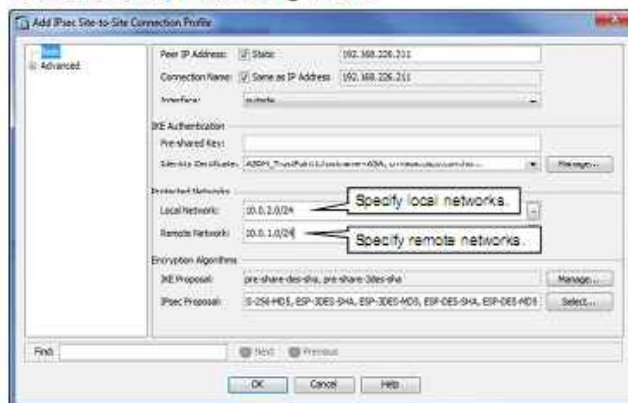


The IKE Authentication area is used to specify the pre-shared key (PSK) or identity certificate to use to authenticate an IKE peer. In this scenario, digital certificates are used to authenticate site-to-site IPsec peers.

**Step 1** From the **Identity Certificate** drop-down menu in the IKE Authentication area, choose the name of the identity certificate to use for authentication. In the example, the previously added identity certificate is chosen.

## Configuring PKI-Based Authentication

### Task 3: Define Interesting Traffic



Configuration > Site-to-Site VPN > Connection Profiles

The protected network parameters define which traffic the IPsec VPN tunnel, the traffic flow source, and the destination IP addresses will protect. In the protected network area, choose or specify the local and remote networks that are protected by this tunnel.

- Step 1** In the Local Network field, specify the IP address of the local network or click the ellipsis (...) button. It opens the Browse Local Network dialog box on which you can choose a previously defined local network.
- Step 2** In the Remote Network field, specify the IP address of the remote network or click the ... button. It opens the Browse Remote Network dialog box, on which you can choose a remote network.

In the example in the figure, the local protected network is 10.0.2.0/24. The remote protected network is 10.0.1.0/24. The IPsec site-to-site tunnel will protect any traffic that is transmitted between these two networks.

## Configuring PKI-Based Authentication

### Task 4: Configure IKE Policy



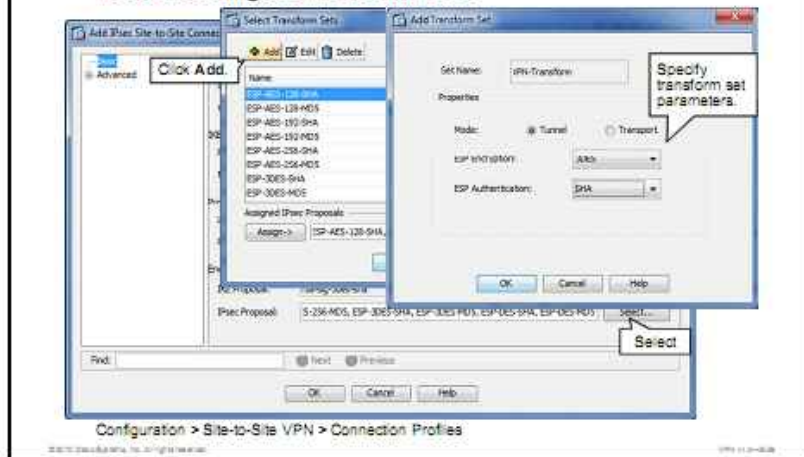
To create a custom IKE policy, click the **Manage** button in the IPsec Site-to-Site Connection Profile window and then click **Add**. The Add IKE Policy dialog box appears. In the Add IKE Policy dialog box, you can create a new IKE policy. This Add IKE Policy window enables you to add the IKE policy as follows:

- Step 1** Use the Priority field to designate a priority number.
- Step 2** Use the Encryption drop-down list to choose the encryption method that protects the data that is transmitted between the IPsec peers.
- Step 3** Use the Hash drop-down menu to choose the hash algorithm that ensures data integrity.
- Step 4** Use the Authentication drop-down list to choose the authentication method that the security appliance uses to establish the identity of each IPsec peer. In this example, digital certificates provide IKE peer authentication. To accomplish this, "rsa-sig" was chosen in the Authentication drop-down menu.
- Step 5** Use the D-H Group drop-down list to choose the Diffie-Hellman group identifier that the IPsec peers use to derive a shared secret without transmitting it to each other.
- Step 6** Use the Lifetime radio buttons and fields to specify the lifetime for the IKE security association.
- Step 7** Click **OK**.

In the example in the figure, an IKE policy using Triple Data Encryption Standard (3DES) encryption, Secure Hash Algorithm (SHA) Hash, and RSA digital certificates for authentication, Diffie-Hellman Group 2 (DH2), and a lifetime of 86,400 seconds was defined.

## Configuring PKI-Based Authentication

### Task 5: Configure Transform Set



This figure shows the Select Transform Sets window that appears if you click the Select button in the Add IPsec Site-to-Site Connection Profile window. Here you can add, edit, or delete transform sets for your site-to-site VPN. You cannot edit or delete the preconfigured transform sets.

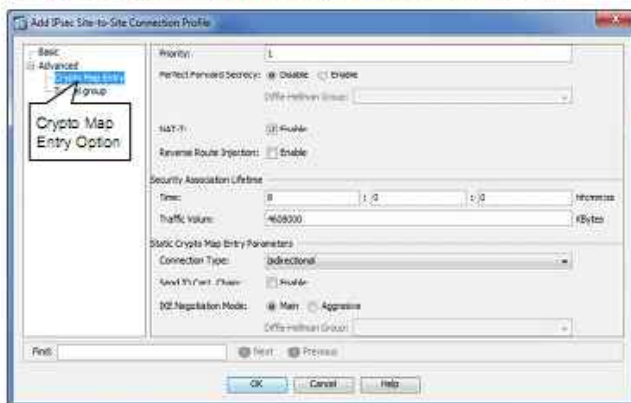
The Select Transform Sets window also allows you to create new transform sets. You might want to create new transform sets if you want to customize the names of the transform sets that you use in your configuration. To create a new transform set, complete the following steps:

- Step 1** Click the **Add** button in the Select Transform Sets window. The Add Transform Sets dialog box appears.
- Step 2** In the Edit Transform Sets window, enter a name for the new transform set in the Set Name field.
- Step 3** Verify that the Tunnel radio button is chosen in the Properties area. The Properties area contains the following mode radio buttons:
  - **Tunnel:** Applies ESP encryption and authentication to the entire original IP packet (IP header and data), thus hiding the ultimate source and destination addresses. This is the default mode.
  - **Transport:** Applies ESP encryption and authentication only to the data in the IP packet. The security appliance uses transport mode only when communicating with a Microsoft Windows 2000 L2TP/IPsec client.
- Step 4** From the ESP Encryption drop-down list, choose the ESP encryption algorithm for the transform set.
- Step 5** From the ESP Authentication drop-down list, choose the ESP authentication algorithm for the transform set.

In the example in the figure, tunnel mode with 3DES encryption with SHA-1 authentication is chosen.
- Step 6** Click **OK**. The Select Transform Sets window becomes active.

## Configuring PKI-Based Authentication

### Task 6: (Optional) Tune Crypto Map Parameters



Configuration > Site-to-Site VPN > Connection Profiles

You can use the Advanced menu items in the IPsec Site-to-Site Connection Profile window to make changes to your site-to-site VPN. By choosing the Crypto Map Entry option, you can make the following changes:

- **Priority:** A unique priority (1 through 65,543, with 1 the highest priority). When IKE negotiation begins, the peer that initiates the negotiation sends all of its policies to the remote peer, and the remote peer searches for a match with its own policies, in priority order.
- **Perfect Forward Secrecy:** Ensures that the key for a given IPsec security association (SA) was not derived from any other secret (like some other keys). With perfect forward secrecy (PFS), every time a new SA is negotiated, a new DH exchange occurs. PFS adds another level of security because if an attacker ever cracks one key, only the data that is sent with that key is compromised. If a peer initiates the negotiation and the local configuration specifies PFS, the peers must perform a PFS exchange for the negotiation to succeed. If someone breaks a key, PFS ensures that the attacker would not be able to derive any other key. If you enable PFS, the Diffie-Hellman Group list becomes active. In the figure, PFS is disabled.

---

**Note** Enabling PFS is optional. PFS provides additional security for DH key exchanges at the cost of additional processing.

---

- **Enable NAT-T:** Enables NAT Traversal (NAT-T) for this policy, which enables IPsec peers to establish both remote-access and site-to-site connections through a Network Address Translation (NAT) device. In the figure, NAT-T is disabled.
- **Enable Reverse Route Injection:** Provides the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint. In the figure, Reverse Route Injection (RRI) is disabled.
- **Security Association Lifetime:** Configures the duration of an SA. Security associations have two lifetimes, a timed lifetime and a traffic volume lifetime. The SA expires after the first of these lifetimes is reached. In the figure, the traffic volume lifetime for this VPN

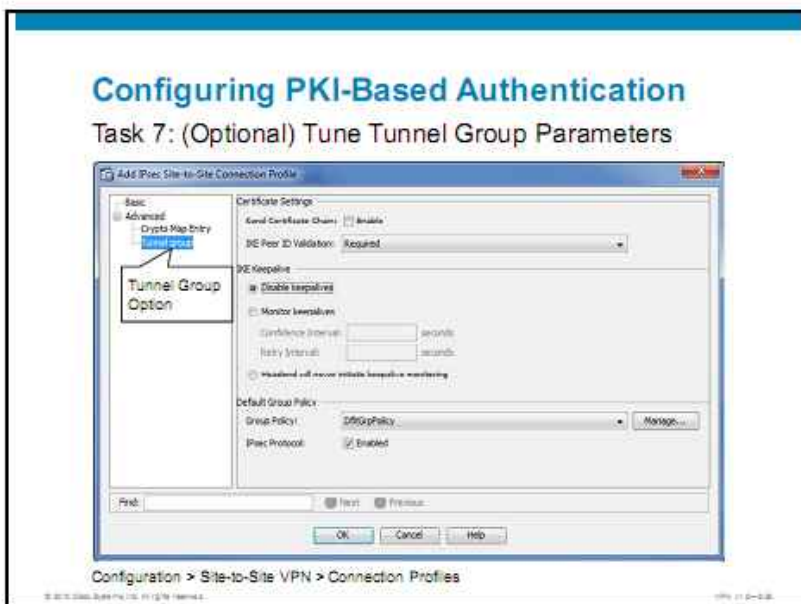


connection is 4,608,000 KB. The SA expires when traffic passing between the IPsec peers using the SA exceeds 4,608,000 KB, or when the security association lifetime exceeds the default setting of 8 hours, whichever happens first. This parameter specifies how to measure the lifetime of the IPsec SA keys by time and traffic volume.

- **Time:** Specifies the SA lifetime in terms of hours (hh), minutes (mm), and seconds (ss).
  - **Traffic Volume:** Defines the SA lifetime in terms of kilobytes of traffic. Enter the number of kilobytes of payload data after which the IPsec SA expires. Minimum is 100 KB, default is 10,000 KB, and maximum is 2,147,483,647 KB.
  - Override the global lifetime value for SAs.
- **Static Crypto Map Entry Parameters:** Configure these additional parameters when the Peer IP Address is specified as Static:
    - **Connection Type:** Specify the allowed negotiation as bidirectional, answer-only, or originate-only.
    - **Send ID Cert. Chain:** Enables transmission of the entire certificate chain.
    - **IKE Negotiation Mode:** Sets the mode for exchanging key information for setting up the SAs: Main or Aggressive. It also sets the mode that the initiator of the negotiation uses. The responder autonegotiates. Aggressive mode is faster, using fewer packets and fewer exchanges, but it does not protect the identity of the communicating parties. Main mode is slower, using more packets and more exchanges, but it protects the identities of the communicating parties. This mode is more secure and it is the default selection. If you choose Aggressive, the Diffie-Hellman Group list becomes active.

## Configuring PKI-Based Authentication

### Task 7: (Optional) Tune Tunnel Group Parameters



By choosing the **Advanced > Tunnel group** option, you can make the following changes:

- **Certificate Settings:** Sets the following certificate chain and IKE peer validation attributes:
  - **Send Certificate Chain:** Enables or disables sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
  - **IKE Peer ID Validation:** Choose whether IKE peer ID validation is ignored, required, or checked only if a certificate includes a field that is used as IKE identity (IP address or hostname).
- **IKE Keepalive:** Enables and configures IKE (ISAKMP) keepalive monitoring:
  - **Disable Keepalives:** Enables or disables IKE keepalives.
  - **Monitor Keepalives:** Enables or disables IKE keepalive monitoring. Choosing this option makes the Confidence Interval and Retry Interval fields available.
  - **Confidence Interval:** Specifies the IKE keepalive confidence interval. This value is the number of seconds the security appliance should allow a peer to idle before beginning keepalive monitoring. The minimum is 10 seconds; the maximum is 300 seconds. The default for a remote access group is 300 seconds.
  - **Retry Interval:** Specifies the number of seconds between IKE keepalive retries. The default is 2 seconds.
  - **Headend Will Never Initiate Keepalive Monitoring:** Specifies that the central-site security appliance never initiates keepalive monitoring.
- **Default Group Policy:** Specifies the following group-policy attributes:
  - **Group Policy:** Choose a group policy to use as the default group policy. The default value is DfltGrpPolicy.
  - **Manage:** Opens the Configure Group Policies dialog box.
  - **IPsec Protocol:** Enables or disables IPsec protocol use for this connection profile.

## Configuring PKI-Based Authentication

### Task 8: Configure Certificate Map Policy

Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Policy

Configure the policy for certificate group matching. The device processes the policies in the order listed below until it finds a match.

- Use the configured rules to match a certificate to a Connection Profile
- Use the certificate OU field to determine the Connection Profile
- Use the IKE identity to determine the Connection Profile
- Use the peer IP address to determine the Connection Profile
- Default to Connection Profile:

Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Policy

© 2010 Cisco Systems, Inc. All rights reserved. VPN 11-2-628

In the configuration scenario, a company with a site-to-site VPN tunnel was shown. The company wants to use a specific tunnel group for a VPN connection to the remote peer. To achieve this, the administrator can configure mapping between attributes within a certificate (the O and OU field, for instance) and tunnel group. Certificate-to-tunnel mapping enables the administrator to use different tunnel groups for different connections, based on fields within a certificate.

To match site-to-site VPN tunnels to tunnel groups based on attributes within a certificate, you must first create rules that define attribute-matching criteria and then associate each rule with the desired tunnel group. Complete the following steps to start mapping a certificate to a specific tunnel connection:

- Step 1** Choose **Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Policy**.
- Step 2** Check the **Use the Configured Rules to Match a Certificate to a Group** check box.

---

**Note** Another option is to check the **Use the Certificate OU Field to Determine the Group** check box. The OU in this option indicates that if a tunnel group is not determined, based on a certificate-to-tunnel group mapping rule lookup, then use the single value of the OU field to determine the tunnel group.

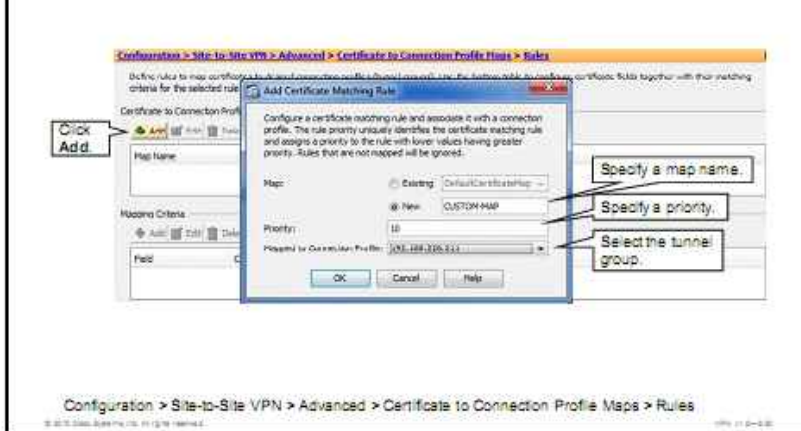
---

- Step 3** Check the **Default to Group** check box.
- Step 4** From the drop-down list, choose the **DefaultL2LGroup** tunnel group.
- Step 5** Click **Apply** at the bottom of the pane.

When the Cisco ASA adaptive security appliance receives an IKE tunnel connection request with a digital certificate, it uses a set of rules to evaluate the attributes of the certificate until it finds a match. When it finds a match, it assigns the connection profile that is associated with the matched rule to the connection. If the security appliance fails to find a match, it assigns the default DefaultL2LGroup profile to the connection.

## Configuring PKI-Based Authentication

### Task 9: (Optional) Define Certificate Map



The administrator defines a rule name, a priority, and a tunnel group. The administrator configures a rule and associates it with a connection profile (formerly called tunnel group).

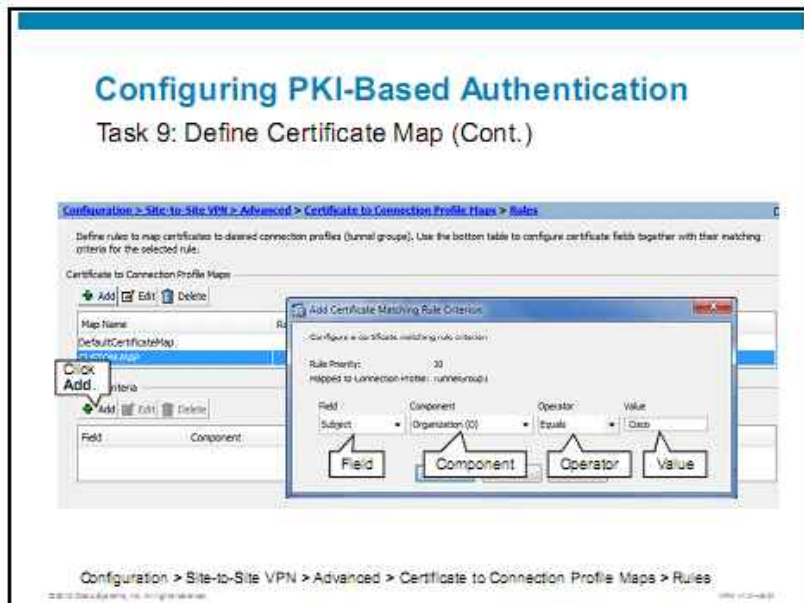
The following parameters are available in the Add Certificate Matching Rule dialog box or Edit Certificate Matching Rule dialog box.

- **Map:** Choose one of the following:
  - **Existing:** Choose an existing map name.
  - **New:** Enter a new map name for a rule. In the example, CUSTOM-MAP was chosen.
- **Priority:** Type a number to specify the sequence with which the Cisco ASA adaptive security appliance evaluates the map when it receives a connection request. The security appliance evaluates each connection against the map with the lowest priority number first. The default priority is 10.
- **Mapped to Connection Profile:** Choose the connection profile to map to this rule. In the example, a predefined connection profile, 192.168.226.211, was chosen as the tunnel group.

To configure a Certificate to Connection Profile Map, complete the following steps:

- Step 1** Choose **Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Rules**.
- Step 2** In the Certificate to Connection Profile Maps pane, click the **Add** button. The Add Certificate Matching Rule window opens.
- Step 3** Choose the **New** radio button. Enter a name into the Name field. In the example, CUSTOM-MAP was entered.
- Step 4** In the Priority field, enter a number to specify the sequence with which the security appliance evaluates the map when it receives a connection request. The number in the example is 10.

- Step 5** From the Mapped to Connection Profile drop-down menu, choose a predefined tunnel group. In the example, a predefined tunnel group, 192.168.226.211, was chosen as the tunnel group.



In the top half of the pane, the administrator defines a name, a priority, and an associated tunnel group. In the bottom half of the pane, the administrator defines the matching rule certificate attribute criteria.

The following parameters are available on the Add Certificate Matching Rule Criterion window:

- **Rule Priority** (Display only): Previously configured sequence number with which the Cisco ASA adaptive security appliance evaluates the map when it receives a connection request. The Cisco ASA adaptive security appliance evaluates each connection against the map with the lowest priority number first.
- **Mapped to Connection Profile** (Display only): Previously configured connection profile to which the rule is mapped.
- **Field**: Choose the part of the certificate to be evaluated from the drop-down list:
  - **Subject**: The person or system that uses the certificate. For a CA root certificate, the Subject and Issuer are the same.
  - **Alternative Subject**: The subject alternative names extension allows additional identities to be bound to the subject of the certificate.
  - **Issuer**: The CA or other entity (jurisdiction) that issued the certificate.
- **Component** (Applies only if Subject or Issuer is chosen.): Choose the certificate attribute that is used in the rule.

- **Operator:** Choose the operator that is used in the rule:
  - **Equals:** The distinguished name field must exactly match the value.
  - **Contains:** The distinguished name field must include the value within it.
  - **Does Not Equal:** The distinguished name field must not match the value
  - **Does Not Contain:** The distinguished name field must not include the value within it.
- **Value:** Enter up to 255 characters to specify the object of the operator.

---

**Note** If multiple criteria are entered, the criterion operation is a logical "and."

---

To configure a Certificate Matching Rule Criterion, complete the following steps:

- Step 1** Choose **Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Rules**.
- Step 2** In the Mapping Criteria area, click the **Add** button. The Add Certificate Matching Rule Criterion window opens.
- Step 3** From the Field drop-down menu, choose the part of the certificate to be evaluated: **Subject, Alternate Subject, or Issuer**.
- Step 4** From the Component drop-down menu, choose the component of the certificate to be evaluated. In the example, the Organization (O) component was chosen.
- Step 5** From the Operator drop-down menu, choose the operator. In the example, Equals was chosen.
- Step 6** From the Value drop-down menu, enter the component values in the field. In the example, "Cisco" was entered.
- Step 7** Click **OK**.
- Step 8** Click **Apply** to apply the configuration.

In the example, connections using certificates with an "O" field value of "Cisco" are assigned to the 192.168.226.211 profile. All other nonmatching connections are assigned to the default L2Lgroup profile.

## Configuring PKI-Based Authentication

### CLI Configuration

```
crypto isakmp enable outside
|
crypto isakmp policy 10 authen rsa-sig
crypto isakmp policy 10 encrypt 3des
crypto isakmp policy 10 hash sha
crypto isakmp policy 10 group 2
crypto isakmp policy 10 lifetime 86400
|
access-list CRYPTO_MAP line 1 extended permit ip 10.0.2.0
255.255.255.0 10.0.1.0 255.255.255.0
|
crypto ipsec transform-set VPN-Transform esp-3des esp-sha-hmac
|
crypto map outside_map0 1 match address outside_cryptomap
crypto map outside_map0 1 set peer 192.168.226.211
crypto map outside_map0 1 set transform-set ESP-AES-128-SHA ESP-
AES-128-MD5 VPN-Transform
|
crypto map outside_map0 interface outside
```

Enable IKE on the outside interface

Configure the IKE policy.

The ACL defines traffic to be protected

Configure a crypto map.

The figure includes the CLI configuration of the IKE policy and the site-to-site VPN tunnel. The configuration that is shown in this slide is similar to the configuration with pre-shared keys (PSKs).

## Configuring PKI-Based Authentication

### CLI Configuration (Cont.)

```
tunnel-group 192.168.226.211 type ipsec-l2l
tunnel-group 192.168.226.211 ipsec-attributes
 trust-point ASDM_TrustPoint1
|
crypto ca certificate map CUSTOM-MAP 10
 subject-name attr o eq Cisco
|
tunnel-group-map enable rules
tunnel-group-map CUSTOM-MAP 10 192.168.226.211
```

Configure tunnel group and attributes.

Configure a certificate-to-connection profile mapping rule.

Enable mapping between certificates and tunnel groups

Configure mapping between connection profile and rule.

The figure shows the CLI commands that are needed to enable certificates-based authentication. The example also shows the commands that are needed to configure mapping between the certificate that was received from the peer device and the tunnel group that should be used for the IKE session that is being established.

## trust-point

To specify the name of a trustpoint that identifies the certificate to be sent to the IKE peer, use the **trust-point** command in the tunnel-group ipsec-attributes mode. To eliminate a trustpoint specification, use the **no** form of this command.

**trust-point** *trust-point-name*

### trust-point Parameters

Parameter	Description
<i>trust-point-name</i>	Specifies the name of the trustpoint to use

## tunnel-group-map enable

The **tunnel-group-map enable** command configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. Use the **no** form of this command to restore the default values.

**tunnel-group-map** [*rule-index*] **enable** *policy*

### tunnel-group-map enable Parameters

Parameter	Description
<i>rule-index</i>	(Optional) Refers to the parameters that are specified by the <b>crypto ca certificate map</b> command. The values are 1 to 65,535.
<i>policy</i>	Specifies the policy for deriving the tunnel group name from the certificate. Policy can be one of the following: <ul style="list-style-type: none"><li>■ <b>ike-id</b>: Indicates that if a tunnel group is not determined based on a rule lookup or taken from the organizational unit, then the certificate-based IKE sessions are mapped to a tunnel group based on the content of the Phase 1 IKE ID.</li><li>■ <b>Ou</b>: Indicates that if a tunnel group is not determined based on a rule lookup, then use the value of the organizational unit in the subject distinguished name (DN).</li><li>■ <b>peer-ip</b>: Indicates that if a tunnel group is not determined based on a rule lookup or taken from the ou or ike-id methods, then use the established peer IP address.</li><li>■ <b>Rules</b>: Indicates that the certificate-based IKE sessions are mapped to a tunnel group based on the certificate map associations that are configured by this command.</li></ul>

## crypto ca certificate map

To enter CA certificate map mode, use the **crypto ca certificate map** command in global configuration mode. Executing this command places you in CA certificate map mode. Use this group of commands to maintain a prioritized list of certificate mapping rules. The sequence number orders the mapping rules. To remove a crypto CA certificate map rule, use the **no** form of the command.

**crypto ca certificate map** {*sequence-number* | *map-name sequence-number*}



## crypto ca certificate map Parameters

Parameter	Description
<i>sequence-number</i>	Specifies a number for the certificate map rule that you are creating. The range is 1 through 65,535. You can use this number when creating a tunnel-group map, which maps a tunnel group to a certificate map rule.
<i>map-name</i>	Specifies a name for a certificate-to-group map.

## subject-name (crypto ca certificate map)

To indicate that rule entry is applied to the subject DN of the IPsec peer certificate, use the **subject-name** command in crypto CA certificate map configuration mode. To remove a subject name, use the **no** form of the command.

**subject-name** [*attr tag eq | ne | co | nc string*]

## subject-name (crypto ca certificate map)Parameters

Parameter	Description
<i>attr tag</i>	Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows: <ul style="list-style-type: none"><li>■ DNQ = DN qualifier</li><li>■ GENQ = Generational qualifier</li><li>■ I = Initials</li><li>■ GN = Given name</li><li>■ N = Name</li><li>■ SN = Surname</li><li>■ IP = IP address</li><li>■ SER = Serial number</li><li>■ UNAME = Unstructured name</li><li>■ EA = Email address</li><li>■ T = Title</li><li>■ O = Organization Name</li><li>■ L = Locality</li><li>■ SP = State/Province</li><li>■ C = Country</li><li>■ OU = Organizational unit</li><li>■ CN = Common name</li></ul>
<i>eq</i>	Specifies that the DN string or indicated attribute must match the entire rule string
<i>ne</i>	Specifies that the DN string or indicated attribute must not match the entire rule string
<i>co</i>	Specifies that the rule entry string must be a substring in the DN string or indicated attribute
<i>nc</i>	Specifies that the rule entry string must not be a substring in the DN string or indicated attribute
<i>string</i>	Specifies the value to be matched

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- In large networks, the preferred method of authenticating a remote peer is the exchange of digital certificates.
- When digital certificates are used for peer authentication, a CA that is trusted by all communicating parties is needed.
- The site-to-site VPN tunnel can be configured only after the CA certificate and identity certificates are stored on the security appliance.

# Deploying the Cisco VPN Client

---

## Overview

Cisco VPN Client is software that runs on a PC. When Cisco VPN Client is installed on a remote PC and communicates with a Cisco ASA adaptive security appliance, it creates a secure connection over the Internet. Through this connection, you can access a private network as if you were an on-site user.

This lesson lists the features that are supported on Cisco VPN Client and shows you how to install the software and configure a profile. You will also learn how advanced Cisco VPN Client profile settings are configured.

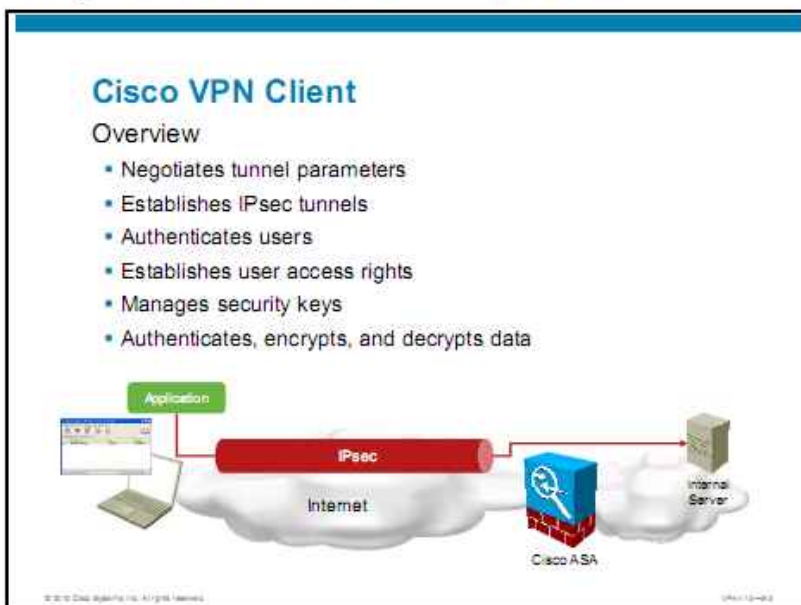
## Objectives

Upon completing this lesson, you will be able to deploy advanced Cisco VPN Client settings to support a range of end users. This ability includes being able to meet these objectives:

- Choose Cisco VPN Client features
- Install, configure, and verify the installation of Cisco VPN Client
- Configure and verify Cisco VPN Client profiles
- Configure and verify advanced Cisco VPN Client profile settings

# Evaluating Cisco VPN Client Features

This topic describes how to choose Cisco VPN Client features.



When you use Cisco VPN Client, you can access a private network through the IP Security (IPsec) virtual private network (VPN) connection as if you were an on-site user. The VPN gateway verifies that incoming connections have up-to-date policies in place before establishing those connections. The Cisco ASA adaptive security appliance can terminate the IPsec VPN connections from Cisco VPN Clients.

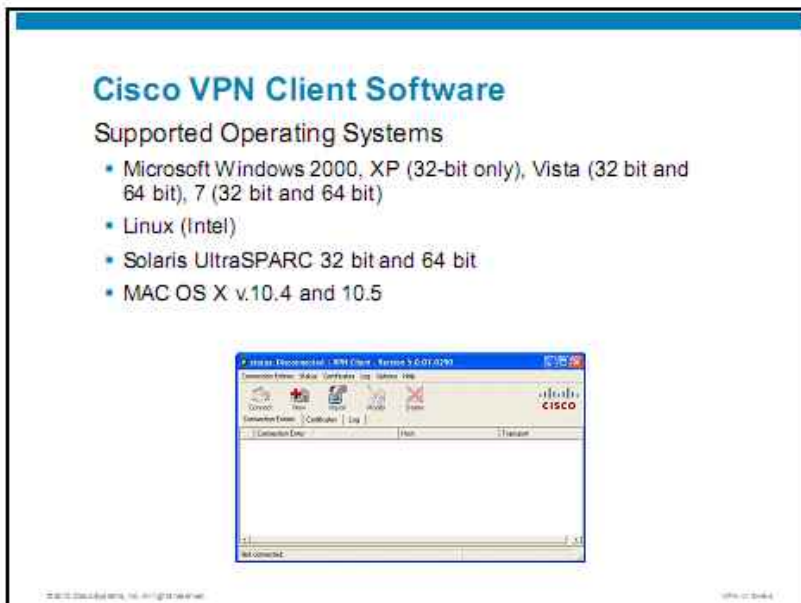
As a remote user, you first connect to the Internet. Then, you use Cisco VPN Client to securely access private enterprise networks through a VPN server that supports Cisco VPN Client.

Cisco VPN Client works with a VPN gateway (a Cisco ASA adaptive security appliance in the figure) to create a secure connection, called a tunnel, between your computer and the private network. It uses the Internet Key Exchange (IKE) and IPsec tunneling protocols to make and manage secure connections. These are some of the steps in the process of making and managing connections:

- **Negotiating tunnel parameters:** Includes addresses, algorithms, lifetime, and so on
- **Establishing tunnels:** According to the parameters
- **Authenticating users:** Making sure that users are who they say they are through the use of usernames, group names and passwords, and X.509 digital certificates
- **Establishing user access rights:** Includes hours of access, connection time, allowed destinations, allowed protocols, and so on
- **Managing security keys:** For encryption and decryption
- **Authenticating, encrypting, and decrypting data:** Through the tunnel

For example, to use a remote PC to read email at your organization, you connect to the Internet, then start the IPsec VPN client, and establish a secure connection through the Internet to the private network of your organization. When you open your email, the Cisco Easy VPN Server feature uses IPsec to encrypt the email message.

It then transmits the message through the tunnel to your Cisco VPN Client, which decrypts the message so that you can read it on your remote PC. If you reply to the email message, Cisco VPN Client uses IPsec to process and return the message to the private network through Cisco Easy VPN Server.



This figure shows the Cisco VPN Client window. You can preconfigure the connection entry (name of connection) and hostname or IP address of a remote VPN device such as the Cisco ASA adaptive security appliance.

Clicking the Connect icon initiates IKE Phase 1.

Cisco VPN Client can be preconfigured for mass deployments, and initial logins require very little user intervention. VPN access policies and configurations are downloaded from Cisco Easy VPN Server and pushed to Cisco VPN Client when a connection is established, allowing simple deployment and management.

Cisco VPN Client provides support for the following operating systems:

- Microsoft Windows 2000, XP (32 bit only), Vista (32 bit and 64 bit), 7 (32 bit and 64 bit)
- Linux (Intel)
- Solaris UltraSPARC 32 bit and 64 bit
- MAC OS X v.10.4 and 10.5

The Cisco Client is compatible with the following Cisco products:

- Platforms based on Cisco IOS Release 12.2(8)T and later
- Cisco ASA 5500 Series Adaptive Security Appliance Version 7.0 and later
- Cisco 7600/Catalyst 6500 IPsec VPN Services Module and Cisco 7600/Catalyst 6500 Series IPsec VPN Shared Port Adapter (SPA) with Cisco IOS Software Release 12.2SX and later

---

**Note** For the latest operating systems and Cisco product support, refer to Cisco.com.

---

## Cisco VPN Client Software

### Specifications

- Supported tunneling protocols
- Supported encryption and authentication
- Supported key management techniques
- Supported data compression technique
- Digital certificate support
- Authentication methodologies
- Profile management
- Policy management

© 2010 Cisco Systems, Inc. All rights reserved. VPN-12-448

The specifications for the Cisco VPN Client product are as follows:

- Supported tunneling protocols:
  - IPsec Encapsulating Security Payload (ESP)
  - Transparent tunneling:
    - IPsec over TCP (using Network Address Translation [NAT] or Port Address Translation [PAT])
    - IPsec over User Datagram Protocol (UDP) (using NAT, PAT, or a firewall)
- Supported encryption and authentication:
  - Data Encryption Standard (DES)
  - Triple DES (3DES)
  - Advanced Encryption Standard (AES)
  - Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)

- Supported key management techniques:
  - IKE, in both aggressive and main mode (digital certificates)
  - DH groups 1, 2, 5, and 7
  - Perfect forward secrecy (PFS) rekeying
- Supported data compression technique: Lempel-Ziv-Stac (LZS)
- Digital certificate support including the following:
  - Two supported enrollment mechanisms:
    - Simple Certificate Enrollment Protocol (SCEP)
    - Certificates that are enrolled with Microsoft Internet Explorer
  - Supported certificate authorities (CAs):
    - Cisco
    - Entrust
    - Netscape
    - Baltimore
    - Rivest, Shamir, and Adleman (RSA) Keon
    - VeriSign
    - Microsoft
  - Support for the Entrust Entelligence Security Provider and Entelligence client
  - Smart cards that are supported through a Microsoft CryptoAPI, CRYPT\_NOHASHOID, including the following:
    - ActivCard (Schlumberger cards)
    - Aladdin
    - Gemalto
    - Datakey Electronics
- Authentication methodologies including the following:
  - Extended Authentication (XAUTH)
  - RADIUS with support for the following:
    - Token cards (state- and reply-message attributes)
    - Kerberos and Microsoft Active Directory authentication
    - RSA Security (RSA SecurIDReady)
    - Microsoft NT domain authentication
    - Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) Windows NT password expiration
    - X.509 version 3 digital certificates
  - External user authorization information that is obtained via Lightweight Directory Access Protocol (LDAP) or RADIUS
- FIPS 140-2 Level 1 (v3.6) certifications

- Profile management: Preconfigured profile configuration files for distributing Cisco VPN Client
- Policy management: Internet Security Association and Key Management Protocol (ISAKMP)
  - Keeps track of centrally controlled policies, such as the following:
    - Domain Name System (DNS) information
    - Microsoft Windows Internet Name Service (Microsoft WINS) information
    - IP address
    - Default domain name
  - Has the ability to save the following connection attributes:
    - Password
    - Split tunneling and local LAN access control and networks
    - Remote-access load balancing
    - Centralized Protection Policy (CPP) firewall
    - Personal firewall requirement
    - Automatic software updates



# Installing Cisco VPN Client Software

This topic describes how to install, configure, and verify the installation of Cisco VPN Client.

## Installing Cisco VPN Client

### Configuration Tasks

1. Verify system requirements.
2. Install Cisco VPN Client.
3. (Optional) Change MTU size on a network adapter.

Complete the following configuration tasks to install Cisco VPN Client:

1. Installation of Cisco VPN Client varies slightly based on the type of operating system. Always review the installation instructions and system requirements that come with Cisco VPN Client before attempting any installation.
2. Install Cisco VPN Client on your system through either of two applications:
  - InstallShield
  - Microsoft Windows Installer (MSI)

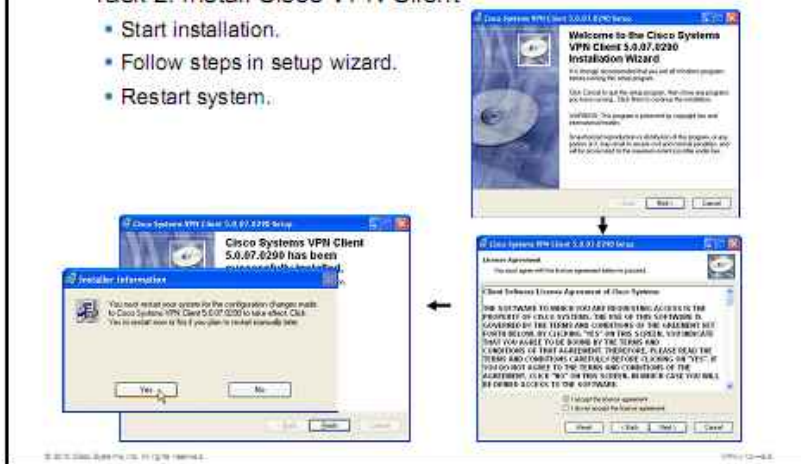
Both applications use installation wizards to walk you through the installation process. Installing Cisco VPN Client through InstallShield includes an Uninstall icon in the program group; MSI does not. In the latter case, to manually remove the Cisco VPN Client applications, you can use the Microsoft Add/Remove Programs utility.

3. Optionally, change maximum transmission unit (MTU) size on a network adapter if you have problems with fragmented IP packets.

## Installing Cisco VPN Client

### Task 2: Install Cisco VPN Client

- Start installation.
- Follow steps in setup wizard.
- Restart system.

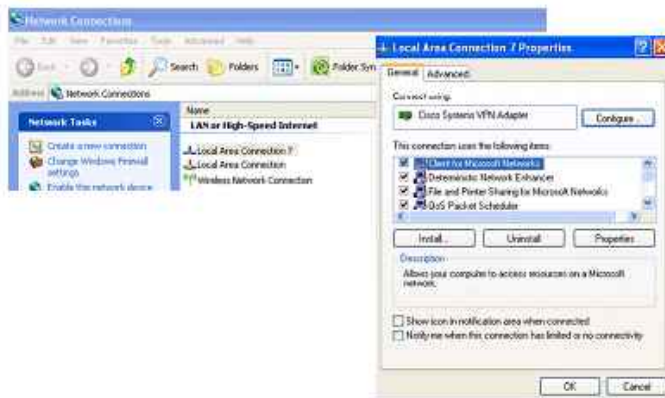


Generally, installation of the Cisco IPsec VPN Client involves the following steps:

- Step 1** Double-click the `vpnclient_setup.msi` file. The Welcome window appears.
- Step 2** Read the Welcome window and click **Next**. The License Agreement page appears.
- Step 3** Read the license agreement, click the **I Accept the License Agreement** radio button, and click **Next**. The Destination Folder page appears.
- Step 4** Click **Next** to accept the default destination folder. The Ready to Install the Application page appears.
- Step 5** Click **Next**. After the files are copied to the hard disk drive of the PC, a new page displays the “Cisco Systems VPN Client 5.0 has been successfully installed” message.
- Step 6** Click **Finish**.
- Step 7** Click **Yes** to restart system after installation is finished.

## Installing Cisco VPN Client

### Virtual Adapter



On the end-user PC, a virtual adapter is a software-only driver that is installed and acts as a valid interface in the system. Its purpose is to solve hardware incompatibility problems. The virtual adapter appears in the network properties list just like a physical adapter and displays all the information that you would usually find under any other network adapter that is installed.

## Installing Cisco VPN Client

### Task 3: Set MTU Size

- From the Start > All Programs menu, choose **Set MTU**.



- Select the proper network adapter and adjust the MTU size.



Cisco VPN Client automatically sets a maximum transmission unit (MTU) size that is optimal for your environment. However, you can also set the MTU size manually.

This figure shows the Set MTU window, which is where you set the MTU size. 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. Using an MTU size of 1300 bytes or smaller usually prevents fragmentation. Fragmentation and reassembly of packets can cause slower tunnel performance. Also, many firewalls do not let fragments through.

To implement a different MTU size using the Set MTU utility, select the network adapter in the Network Adapters (IPsec only) field. In the figure, Local Area Connection 7 is selected. In the MTU Options group box, set the MTU option size by clicking the appropriate radio button, in this example, the MTU for the chosen network adapter is set to 1400 bytes. You must reboot for MTU changes to take effect.

---

**Note** Cisco VPN Client automatically adjusts the MTU size to suit your environment, so running this application should not be necessary.

---

# Configuring Cisco VPN Client Profiles

This topic describes how to configure and verify Cisco VPN Client profiles.

## Configuring Cisco VPN Client

### Configuration Tasks

1. Gather information you need.
2. Create new connection entry.
3. Configure basic connection properties.
4. (Optional) Configure transport properties.
5. (Optional) Configure backup server properties.
6. (Optional) Configure dialup properties.

Complete the following steps to configure Cisco VPN Client:

1. Gather the information that you need.
2. Create a new connection entry.
3. Configure basic connection properties.
4. Optionally, configure transport properties.
5. Optionally, configure backup server properties.
6. Optionally, configure dialup properties.

## Configuring Cisco VPN Client

### Task 1: Gather Information

- Hostname or IP address of the adaptive security appliance
- Authentication information
- Hostnames or IP addresses of the backup servers



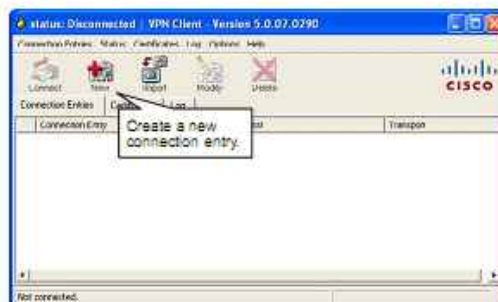
To configure and use Cisco VPN Client, you will need the following information:

- Hostname or IP address of the secure gateway to which you are connecting
- Group name (for pre-shared keys [PSKs])
- Group password (for PSKs)
- If authenticating with a digital certificate, the name of the certificate
- Username and password for user authentication
- If you are configuring backup server connections, the hostnames or IP addresses of the backup servers

Ask for this information from the system administrator of the private network that you want to access. Your system administrator might have preconfigured much of this data; if so, your administrator will tell you which items you need.

## Configuring Cisco VPN Client

### Task 2: Create Connection Entry



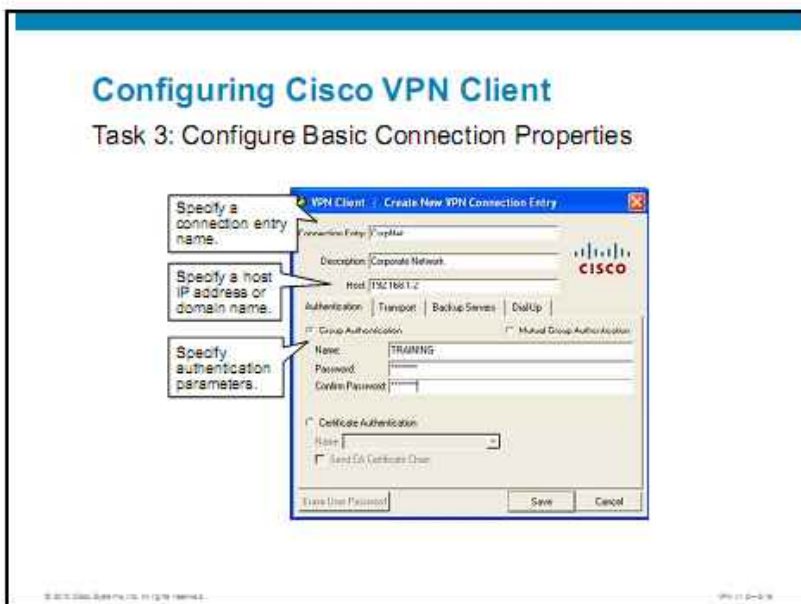
Cisco VPN Client enables users to configure multiple connection entries. Multiple connection entries enable the user to build a list of possible network connection points. For example, a corporate telecommuter may want to connect to the sales office in Boston for sales data (the first connection entry, not shown in the figure). Then, the telecommuter may want to connect to the Austin factory for inventory data (a second connection entry, not shown in the figure). Each connection contains a specific entry name and remote server hostname or IP address.

To create a new connection entry, complete the following configuration steps:

- Step 1** Choose **Start > All Programs > Cisco Systems VPN Client > VPN Client**. The VPN Client window appears.
- Step 2** Click **New**.

## Configuring Cisco VPN Client

### Task 3: Configure Basic Connection Properties



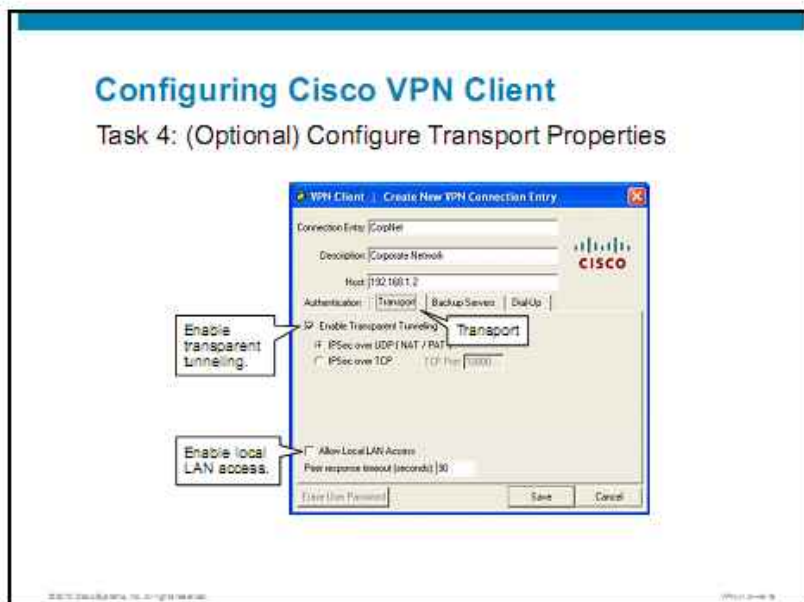
Generally, creating a new connection entry involves the following steps:

- Step 1** Enter a name for the new connection entry in the Connection Entry field. In the figure, *CorpNet* is entered.
- Step 2** Optionally, enter a description for the new connection entry in the Description field. In the figure, *Corporate Network* is entered.
- Step 3** Enter the public interface IP address or hostname of the remote Cisco Easy VPN Server in the Host field. In the figure, *192.168.1.2* is entered.
- Step 4** In the Authentication tab, click the radio button for the authentication method that you want to use. You can connect as part of a group (which must be configured on the Cisco Easy VPN Server) or by supplying an identity digital certificate. For this example, group authentication is used. Complete the following substeps to configure group authentication:
  - In the Name field, enter a group name that matches a tunnel group on the Cisco Easy VPN Server. The group name and its password must match what is configured within the Cisco Easy VPN Server. Entries are case sensitive. In the figure, *TRAINING* is entered.
  - In the Password field, enter the group password that matches the group password (key) on the Cisco Easy VPN Server. Entries are case sensitive.
  - Enter the password again in the Confirm Password field.
- Step 5** Click **Save**.



## Configuring Cisco VPN Client

### Task 4: (Optional) Configure Transport Properties



From the Transport tab, you can configure the following Cisco VPN Client options:

- Transparent tunneling
- Local LAN access
- Peer response timeout

Transparent tunneling allows secure transmission between Cisco VPN Client and a secure gateway through a router serving as a firewall, which may also be performing NAT or PAT. Transparent tunneling encapsulates Protocol 50 (which is ESP) traffic within UDP or 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. To use transparent tunneling, the central-site group in the Cisco Easy VPN Server must also be configured to support it. This parameter is enabled by default. To disable this parameter, uncheck the **Enable Transparent Tunneling** check box under the Transport tab. It is recommended that you leave this parameter enabled.

---

**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 that 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:

- **IPsec over UDP (NAT/PAT):** Click this radio button to enable IPsec over UDP (using NAT or PAT). With UDP, the port number is negotiated. UDP is the default mode.
- **IPsec over TCP:** Click this radio button to enable IPsec over TCP. 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 that is configured on the secure gateway. The default port number is 10000.

In a multiple network interface card (NIC) configuration, local LAN access pertains only to network traffic on the interface on which the tunnel was established. Allow Local LAN Access 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, check the **Allow Local LAN Access** check box; to disable it, uncheck 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 Cisco VPN Client side that you can access. You can access up to 10 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 that are excluded from doing so (in the network list).

When this feature is enabled and configured on Cisco VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs that are available by looking at the Routes table.

## Adjusting the Peer Response Timeout Value

Cisco VPN Client uses a keepalive mechanism, 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 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 that 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. Cisco VPN Client continues to send DPD requests every 5 seconds until it reaches the number of seconds that are specified by the peer response timeout value.

## Configuring Cisco VPN Client

### Task 5: (Optional) Configure Backup Server Properties



The private network may include one or more backup servers to use if the primary VPN server is not available. Information on backup servers can download automatically from a VPN server or you can manually enter this information.

To enable backup servers from Cisco VPN Client, complete the following steps:

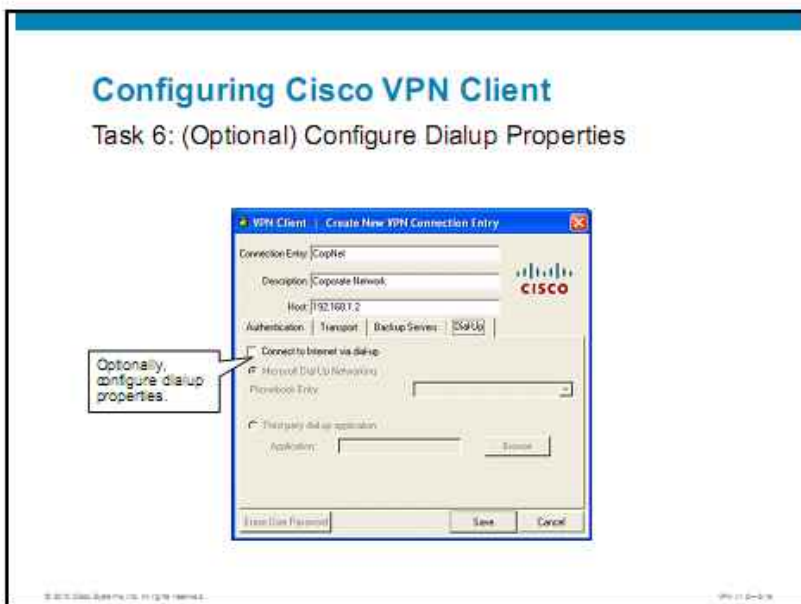
- Step 1** Check the **Enable Backup Servers** check box in the Backup Servers tab.
- Step 2** Click **Add**. The VPN Client | Enter Backup Server window appears.
- Step 3** Enter the hostname or IP address of a backup server in the Enter Backup Server Hostname or IP Address field (not shown). You can use a maximum of 255 characters.
- Step 4** Click **OK**. The hostname or IP address is displayed in the Enable Backup Servers list.
- Step 5** Click **Save**.

You can add more backup servers by repeating all but the first step (that is, steps 2, 3, 4, and 5). To remove a server from the backup list, select the server in the list, click **Remove**, and then click **Save**.

When necessary, Cisco VPN Client tries the backup servers in the order in which they appear in the backup servers list, starting at the top. To reorder the servers in the list, select a server and click the up arrow to increase the priority of the server or the down arrow to decrease the priority of the server.

## Configuring Cisco VPN Client

### Task 6: (Optional) Configure Dialup Properties



To enable and configure a connection to the Internet through dialup networking, check 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 Microsoft DUN phone book entries and have enabled the Connect to Internet via Dial-up feature, DUN is enabled by default. To link your Cisco VPN Client connection entry to a Microsoft DUN entry, click the **Phonebook Entry** drop-down arrow and choose an option from the menu. 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 dialup application:** If you have no Microsoft DUN phone book entries and have enabled the Connect to Internet via Dial-up feature, the third-party dialup application is enabled by default. Click **Browse** to enter the name of the program in the Application field. This application launches the connection to the Internet. The string that you enter in the Application field is the pathname to the command that starts the application and the name of the command. For example, `c:\isp\ispdialer.exe dialEngineering` would activate the ISP dialer using the script `dialEngineering`, which would contain the required dial information.

# Configuring Advanced Profile Settings

This topic describes how to configure advanced Cisco VPN Client profile settings.

## Configuring Advanced Profile Settings

### Profiles

Groups of parameters that control a VPN client are called profiles:

- **Global profile:** Contains parameters for the VPN client as a whole (vpnclient.ini).
- **Individual profiles:** Contain the parameter settings for each connection entry and are unique to that connection entry (.pcf).
- Profiles are created using the VPN client GUI or manually using text editor.
- You can provision these files to clients to avoid configuring each VPN client separately.

Groups of configuration parameters define the connection entries that remote users use to connect to a VPN central-site device. Together, these parameters form files called profiles. There are two profiles: a global profile and an individual profile.

- A global profile sets rules for all remote users; it contains parameters for Cisco VPN Client as a whole. The name of the global profile file is vpnclient.ini.
- Individual profiles contain the parameter settings for each connection entry and are unique to that connection entry. Individual profiles have a .pcf extension.

Profiles are created in two ways:

- When an administrator or a remote user creates connection entries using the Cisco VPN Client GUI (Windows and Macintosh only)
- When you create profiles using a text editor

In the first case, the remote user is also creating a file that can be edited through a text editor. You can start with a profile file generated through the GUI and edit it. This approach lets you control some parameters that are not available in the Cisco VPN Client GUI application such as auto initiation or the dialup time to wait for third-party dialers.

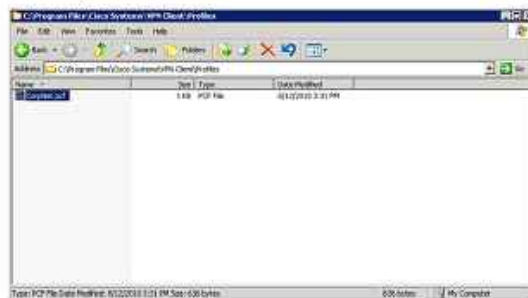
When you create these files, you can provision them to several clients to avoid configuring each VPN client individually.



## Configuring Advanced Profile Settings

### Individual Profiles

- Windows platforms: `C:\Program Files\Cisco Systems\VPN Client\Profiles\`
- Linux, Solaris, and Mac OS X platforms: `/etc/CiscoSystemsVPNClient/Profiles/`



Cisco VPN Client uses parameters that must be uniquely configured for each remote user of the private network. Together, these parameters make up a user profile, which is contained in a profile configuration file (.pcf file) in the local file system of the Cisco VPN Client user in the following directories:

- For Windows platforms: **Program Files\Cisco Systems\VPN Client\Profiles** (if the software is installed in the default location)
- For the Linux, Solaris, and Mac OS X platforms: `/etc/CiscoSystemsVPNClient/Profiles/`

These parameters include the authentication type that is used, remote server address, IPsec group name and password, use of a log file, use of backup servers, and automatic Internet connection via Microsoft DUN among many other features and requirements. Each connection entry has its own .pcf file.

## Configuring Advanced Profile Settings

### Global Profile Features

- Start before logon
- Automatically connect to the default connection entry (default profile) upon startup
- Automatically disconnect upon log off
- Control of logging services by class
- Certificate enrollment
- Identity of a proxy server for routing HTTP traffic
- Identity of an application to launch upon connect
- Missing group warning message
- Logging levels for log classes
- RADIUS SDI Extended Authentication behavior
- GUI parameters—appearance and behavior of GUI applications
- Transparent tunneling

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-0-00

The `vpnclient.ini` file controls the following features on all Cisco VPN Client platforms:

- Start Before Logon
- Automatically connect to the default connection entry (default profile) upon startup
- Automatically disconnect upon log off
- Control of logging services by class
- Certificate enrollment
- Identity of a proxy server for routing HTTP traffic
- Identity of an application to launch upon connect
- Missing group warning message
- Logging levels for log classes
- RADIUS SDI Extended Authentication behavior
- GUI parameters—appearance and behavior of GUI applications

The `vpnclient.ini` file controls the following additional features in the Windows platform:

- Location of the `Entrust.ini` file
- List of Graphical Identification and Authentication (GINA) dynamic link libraries (DLLs) that are not compatible with Cisco VPN Client
- Auto initiation
- Setting of the Stateful Firewall option
- The method to use in adding suffixes to domain names on Windows 2000 and Windows XP platforms
- When working with a third-party dialer, time to wait after receiving an IP address before initiating an IKE tunnel



- Network proxy server for routing HTTP traffic
- Application launching
- DNS suffixes
- Force Network Login, which forces a user on Windows NT, Windows 2000, or Windows XP to log out and log back in to the network without using cached credentials
- Accessibility options setting
- Setting a default connection entry
- Connecting to a default connection entry

## Configuring Advanced Profile Settings

### Individual Profile Features

<ul style="list-style-type: none"> <li>▪ Description of the connection profile</li> <li>▪ The remote server address</li> <li>▪ Authentication type</li> <li>▪ Name of IPsec group containing the remote user</li> <li>▪ Group password</li> <li>▪ Split DNS</li> <li>▪ TCP tunneling port</li> <li>▪ Enabling of IKE and ESP keepalives</li> <li>▪ Certificate parameters for a certificate connection</li> <li>▪ DH group</li> <li>▪ RADIUS SDI Extended Authentication setting</li> <li>▪ Split DNS setting</li> </ul>	<ul style="list-style-type: none"> <li>▪ Name of remote user</li> <li>▪ Password of a remote user</li> <li>▪ Backup servers</li> <li>▪ Connecting to the Internet via dialup networking</li> <li>▪ Type of dialup networking connection</li> <li>▪ Transparent tunneling</li> <li>▪ Allowing of local LAN access</li> <li>▪ Setting of peer response timeout</li> <li>▪ Setting of certificate chain</li> <li>▪ Verification of the DN of a peer certificate</li> <li>▪ Use of SDI hardware token setting</li> <li>▪ Use of legacy IKE port setting</li> </ul>
--	--

© 2010 Cisco Systems, Inc. All rights reserved. IPSec-2-93

A connection profile (.pef file) controls the following features on all platforms):

- Description of the connection profile
- The remote server address
- Authentication type
- Name of IPsec group containing the remote user
- Group password
- Connecting to the Internet via dialup networking
- Name of remote user
- Remote user password
- Backup servers
- Split DNS
- Type of dialup networking connection
- Transparent tunneling
- TCP tunneling port

- Allowing of local LAN access
- Enabling of IKE and ESP keepalives
- Setting of peer response timeout
- Certificate parameters for a certificate connection
- Setting of certificate chain
- Diffie-Hellman (DH) group
- Verification of the distinguished name (DN) of a peer certificate
- RADIUS RSA Extended Authentication setting
- Use of Rivest, Shamir, and Adleman (RSA) hardware token setting
- Split DNS setting
- Use of legacy IKE port setting

A connection profile (.pcf file) controls the following additional features on the Windows platform:

- Dialup networking phone book entry for Microsoft
- Command string for connecting through an ISP
- Windows NT domain
- Logging in to Microsoft Network and credentials
- Changing the default IKE port from 500/4500 (must be explicitly added)
- Enabling Force Network Login, which forces a user on Windows NT, Windows 2000, and Windows XP to log out and then log back in to the network without using cached credentials
- Enabling and disabling the browser proxy setting on Cisco VPN Client for all connection types

## Configuring Advanced Profile Settings

### Profile Sample Files

<pre>[main] RunAtLogon=0 EnableLog=1 DialerDisconnect=1 ConnectOnOpen=1 [LOG. IKE] LogLevel=1 [LOG. CM] LogLevel=1 [GUI] DefaultConnectionEntry=CorpNet WindowWidth=578 WindowHeight=367 WindowX=324 WindowY=112 VisibleTab=0 ConnectionAttribute=0 AdvancedView=1 MinimizeOnConnect=1</pre>	<pre>[main] Description=Corporate Network !Host=192.168.1.2 AuthType=1 GroupName=TRAINING GroupPwd= enc_GroupPwd=C9428D74E589E EnableISPConnect=0 ISPConnectType=0 ISPConnect= ISPPhonebook= ISPCommand= Username= SaveUserPassword=0 UserPassword= enc_UserPassword= NTDomain= EnableBackup=0 BackupServer= EnableMSLogon=1 MSLogonType=0</pre>
vpnclient.ini	CorpNet.pcf

The figure shows sample vpnclient.ini and pcf files. An administrator can preconfigure VPN clients by placing these files into the Cisco VPN Client installation folder:

- **vpnclient.ini:** If this file is bundled with the client software when it is first installed, it automatically configures the client global parameters during installation. To mask the configuration option from the end user, add an exclamation point (!) to the beginning of the configuration line within the vpnclient.ini field.
- **.pcf:** Creates connection entries within the dialer application. If this file is bundled with the client software when it is first installed, it automatically configures the Cisco VPN Client connection parameters during installation. Each connection has its own .pcf file. It can be viewed and edited in Notepad. To make a parameter read-only so that the client user cannot change it within the GUI, put an exclamation mark (!) before the parameter name.

**Note** The easiest way to create a profile for the Windows platforms is to run 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 that you might introduce by typing the parameters, and the group password gets automatically converted to an encrypted format.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- Cisco VPN Client enables VPN access to private network.
- Verify system requirements and gather information before installing Cisco VPN client.
- Cisco VPN Client entry parameters are remote server hostname or IP address and PSKs or certificates.
- PCF and INI files contain profile parameters (authentication type, remote server address, IPsec group name and password, and so on).

# Deploying Basic Cisco Easy VPN Solutions

---

## Overview

A basic Cisco Easy VPN solution provides client-based access to sensitive resources over a remote access IP Security (IPsec) virtual private network (VPN) gateway that is implemented on the Cisco ASA adaptive security appliance. A basic Easy VPN solution uses basic user authentication using usernames and passwords, client configuration and IP address assignment services, and a single access control policy. This lesson enables you to configure, verify, and troubleshoot a basic Easy VPN solution.

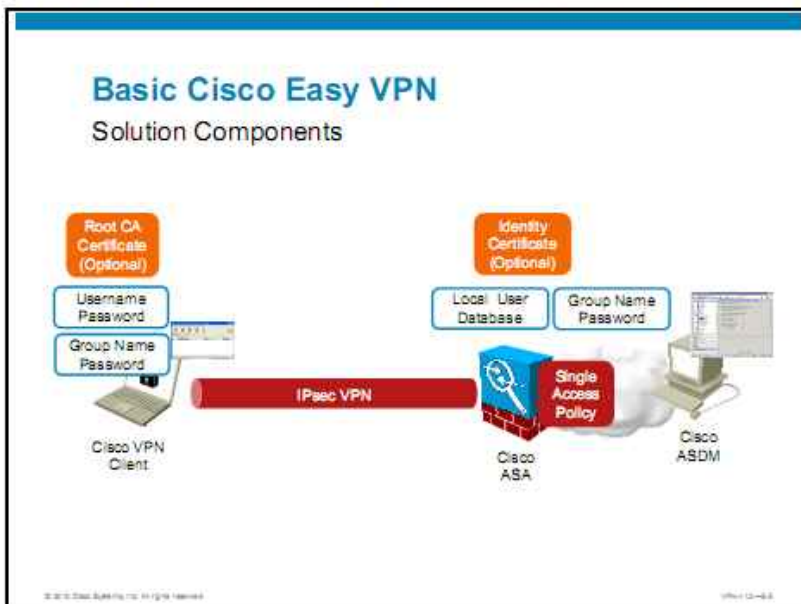
## Objectives

Upon completing this lesson, you will be able to deploy and manage the basic features of the Cisco ASA adaptive security appliance Easy VPN Server feature. This ability includes being able to meet these objectives:

- Plan the deployment of a basic Easy VPN solution
- Configure and verify basic Cisco ASA adaptive security appliance Easy VPN Server features
- Configure and verify Easy VPN group authentication
- Configure and verify Easy VPN XAUTH
- Configure and verify Easy VPN client network settings
- Configure and verify Easy VPN basic access control and split tunneling
- Configure and verify Cisco VPN Client connectivity
- Troubleshoot Easy VPN session establishment between a Cisco VPN Client and the Cisco ASA adaptive security appliance gateway

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic describes how to plan the deployment of a basic Cisco Easy VPN solution.



In a basic Cisco Easy VPN solution, remote users use the Cisco IPsec software or hardware Cisco VPN Client to establish an IPsec tunnel with the Cisco ASA adaptive security appliance.

The basic solution uses bidirectional authentication, where the client authenticates the Cisco ASA adaptive security appliance with a group-password-based authentication method, and the Cisco ASA adaptive security appliance authenticates the user based on a group password, and optionally an additional username and password method against its local user database. This authentication scheme can be extended by deploying hybrid authentication, where the client additionally authenticates the Cisco ASA adaptive security appliance using the identity certificate of the Cisco ASA adaptive security appliance, which is verifiable using a locally installed CA certificate.

After authentication, the Cisco ASA adaptive security appliance applies a set of authorization and accounting rules to the VPN session of the user. After the Cisco ASA adaptive security appliance establishes an acceptable VPN environment with the remote user, the remote user can forward raw IP traffic into the IPsec tunnel because the Cisco VPN Client creates a virtual network interface on the client. The client can use any application to access any resource behind the Cisco ASA adaptive security appliance VPN gateway, subject to access rules applied to the VPN session.

## Basic Cisco Easy VPN

### Deployment Tasks

1. Configure basic Cisco ASA adaptive security appliance Easy VPN Server features.
2. Configure group authentication.
3. (Optional) Configure basic user authentication (XAUTH).
4. Configure client network configuration.
5. Configure basic access control.
6. Configure Cisco VPN Client.

Use the following general deployment tasks to create a basic Cisco Easy VPN solution:

1. Configure the security appliance with basic Cisco Easy VPN Server features, including enabling the Internet Key Exchange (IKE) and IPsec protocols on a Cisco ASA adaptive security appliance interface.
2. Configure group pre-shared key (PSK) authentication to mutually authenticate the two IKE peers: the Cisco VPN Client and the appliance.
3. Optionally, configure basic user authentication using IKE Extended Authentication (XAUTH), using the appliance local user database to create user accounts with static passwords.
4. Optionally, in addition to basic user authentication, configure hybrid authentication to additionally authenticate the appliance to the client. As you will learn later in this lesson, this additional authentication may be required to avoid man-in-the-middle attacks in some environments.
5. Configure the client network settings (Domain Name Server [DNS] server, Microsoft Windows Internet Name Service [WINS] server, domain suffix) configuration set, and IP address assignment method, using either pools or per-user IP addresses that are configured locally on the appliance.
6. Configure basic access control, limiting access to protected resources.
7. Install the Cisco VPN Client, and configure it to connect to the Cisco Easy VPN Server for the appliance.

## Basic Cisco Easy VPN

### Input Parameters

Parameter	Description
VPN gateway addressing	Required to configure adaptive security appliance IP interfaces
User naming and credentials	Required to create the local user database
Cryptographic policy	Required to enable or disable cryptographic algorithms within IPsec
IP address ranges for client address assignment	Required to assign IP addresses to VPN virtual adapters
Access policies	Required to create separate profiles and access control policies for remote users
Client platforms	Required to provision VPN client software to remote users

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-10-433

Before implementing a basic Cisco Easy VPN solution, you will need to obtain and analyze several pieces of information that are related to the network and system environment. These input parameters include the following:

- The IP addressing plan that will dictate the VPN gateway addressing. This data is needed to assign an IP address to the appliance VPN-terminating interface.
- The enterprise policy of user naming and the enterprise password policy, to create the local user database on the appliance.
- The enterprise cryptographic policy, to choose the optimal IKE and IPsec protocol versions and algorithm bundles (Internet Security Association and Key Management Protocol [ISAKMP] policies, IPsec transform sets) for VPN sessions on the appliance.
- The IP addressing plan for remote clients. With Cisco Easy VPN, the appliance must assign IP addresses to remote clients, and these addresses must be unique and routed to the appliance for VPN connectivity to work.
- Access policies that dictate which sensitive resources remote users can access. This data is needed to configure an access control policy on the appliance that will be applied to remote access VPN sessions.
- A list of the client platforms of remote users, which is used to correctly provision the Cisco VPN Client software images to users.



# Configuring Basic Cisco ASA Adaptive Security Appliance Cisco Easy VPN Server Features

This topic describes how to configure and verify basic Cisco ASA adaptive security appliance Easy VPN Server features.

## Configuring Basic Cisco Easy VPN

### Configuration Tasks

1. Enable IKE and IPsec on an interface.
2. (Optional) Tune the IKE policy.
3. (Optional) Tune the IPsec policy.



The first deployment step to take when you configure a Cisco Easy VPN solution is to configure basic Cisco Easy VPN Server parameters on the Cisco ASA adaptive security appliance. This process includes the following configuration tasks:

1. Enabling IKE and IPsec functionality on a Cisco ASA adaptive security appliance interface. Enabling this functionality via the Cisco Adaptive Security Device Manager (Cisco ASDM) automatically creates an IKE and IPsec policy of acceptable cryptographic algorithm bundles.
2. Optionally, tune the IKE policy on the Cisco ASA adaptive security appliance, if you require specific cryptographic algorithms to be enabled or disabled for the IKE security associations.
3. Optionally, tune the IPsec policies on the Cisco ASA adaptive security appliance, if you require specific cryptographic algorithms to be enabled or disabled for the IPsec security associations.

The figure presents the configuration scenario that is used in upcoming configuration tasks. You will enable the basic Cisco Easy VPN Server functionality by enabling IKE and IPsec on the "outside" interface of the Cisco ASA adaptive security appliance.

## Configuring Basic Cisco Easy VPN

### Task 1: Enable IKE and IPsec on an Interface

In Cisco ASDM, this task also automatically:

- Enables two IKE policies
- Creates 10 IPsec transform sets
- Creates dynamic crypto map rules that use these policies and transform sets



In the first task, you will enable IKE and IPsec on a Cisco ASA adaptive security appliance interface. Perform the following steps:

- Step 1** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**.
- Step 2** In the Access Interfaces area, check a particular check box in the Allow Access column to enable IKE and IPsec on a particular interface.
- Step 3** Click **Apply** and, optionally, click **Save** to save your configuration.

When you enable IKE and IPsec on a Cisco ASA adaptive security appliance interface, the Cisco ASDM enables the IKE (ISAKMP) listener on that interface, and creates two IKE policies (that is, the allowed algorithm bundles) that it is willing to negotiate with remote peers. The following policies are the two policies that are created:

- An IKE policy entry with a priority of 5 with the following settings:
  - PSK-based peer authentication
  - Triple Data Encryption Standard (3DES) encryption
  - Secure Hash Algorithm 1 (SHA-1) hashing
  - Diffie-Hellman Group 2 (DH2) (1024 bit) key exchange strength
  - A lifetime of 24 hours
- An IKE policy entry with a priority of 10 (that is, lower than the previous policy entry) with the following settings:
  - PSK-based peer authentication
  - Data Encryption Standard (DES) encryption
  - SHA-1 hashing
  - Diffie-Hellman Group 2 (DH2) (1024 bit) key exchange strength
  - A lifetime of 24 hours

Additionally, Cisco ASDM will create an IPsec policy (crypto map) in the following manner:

- The Cisco ASA adaptive security appliance will be willing to accept any Cisco Easy VPN Client on the configured interface, as long as it authenticates using the configured methods.
- The client must support one of the following IPsec transform sets (traffic-protecting algorithm bundles) in the listed priority order:
  - Encapsulating Security Protocol (ESP) encapsulation, with 128-bit Advanced Encryption Standard (AES) encryption and Secure Hash Algorithm 1 Hashed Message Authentication Code (SHA-1 HMAC)
  - ESP encapsulation, with 128-bit AES encryption and Message Digest 5 (MD5) HMAC
  - ESP encapsulation, with 192-bit AES encryption and SHA-1 HMAC
  - ESP encapsulation, with 192-bit AES encryption and MD5 HMAC
  - ESP encapsulation, with 256-bit AES encryption and SHA-1 HMAC
  - ESP encapsulation, with 256-bit AES encryption and MD5 HMAC
  - ESP encapsulation, with 168-bit 3DES encryption and SHA-1 HMAC
  - ESP encapsulation, with 168-bit 3DES encryption and MD5 HMAC
  - ESP encapsulation, with 56-bit DES encryption and SHA-1 HMAC
  - ESP encapsulation, with 56-bit DES encryption and MD5 HMAC

## Configuring Basic Cisco Easy VPN

### Task 2: (Optional) Tune the IKE Policy

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime (seconds)
10	des	sha	2	pre-share	86400
5	3des	sha	2	pre-share	86400

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies

In Task 2, you can tune the preconfigured IKE policies to either add a policy that you want to use or remove some of the preconfigured policies. In most cases, it is recommended that you remove the preconfigured policy with priority 10 that uses DES encryption.

To delete an existing IKE policy entry, perform the following steps:

- Step 1** Using Cisco ASDM, navigate to the list of IKE policies at Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies.
- Step 2** Select the IKE policy entry that you want to delete.
- Step 3** Click the **Delete** button to delete it.
- Step 4** Click **Apply** and, optionally, click **Save** to save your configuration.

To add a new IKE policy entry, perform the following steps:

- Step 1** Using Cisco ASDM, navigate to the list of IKE policies at Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies.
- Step 2** Click the **Add** button to add a new policy entry.
- Step 3** In the Add Ike Policy window, configure the required IKE policy parameters that you wish to bundle in a policy entry.
- Step 4** Click **OK**, **Apply**, and, optionally, click **Save** to save your configuration.

## Cisco VPN Client and IKE Policies

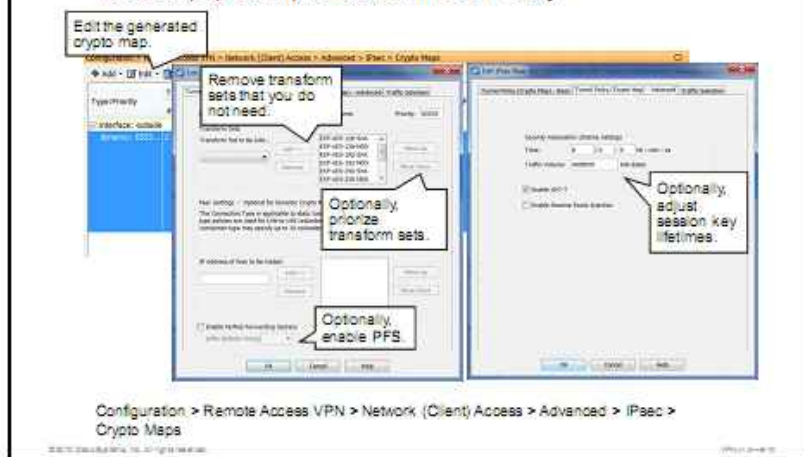
The Cisco VPN Client that is configured for PSKs uses IKE aggressive mode to connect to the Cisco ASA adaptive security appliance and is preconfigured with 14 IKE policies in priority order. All of these policies use a fixed DH2 (1024-bit) key exchange strength setting. If you need to use a stronger Diffie-Hellman (DH) group on the client—which is recommended in high-risk environments—you need to configure it inside the Cisco VPN Client connection entry file (the DHGroup parameter inside the .pcf file).

The Cisco VPN Client uses these 14 preconfigured IKE policies when it is configured with group password authentication in Cisco VPN Client Release 5.0.6:

1. 256-bit AES encryption, SHA-1 HMAC, DH2, Extended Authentication (XAUTH) enabled
2. 256-bit AES encryption, MD5 HMAC, DH2, XAUTH enabled
3. 256-bit AES encryption, SHA-1 HMAC, DH2
4. 256-bit AES encryption, MD5 HMAC, DH2
5. 128-bit AES encryption, SHA-1 HMAC, DH2, XAUTH enabled
6. 128-bit AES encryption, MD5 HMAC, DH2, XAUTH enabled
7. 128-bit AES encryption, SHA-1 HMAC, DH2
8. 128-bit AES encryption, MD5 HMAC, DH2
9. 3DES, SHA-1 HMAC, DH2, XAUTH enabled
10. 3DES, MD5 HMAC, DH2, XAUTH enabled
11. 3DES, SHA-1 HMAC, DH2
12. 3DES, MD5 HMAC, DH2
13. DES, MD5 HMAC, DH2, XAUTH enabled
14. DES, MD5 HMAC, DH2

## Configuring Basic Cisco Easy VPN

### Task 3: (Optional) Tune the IPsec Policy



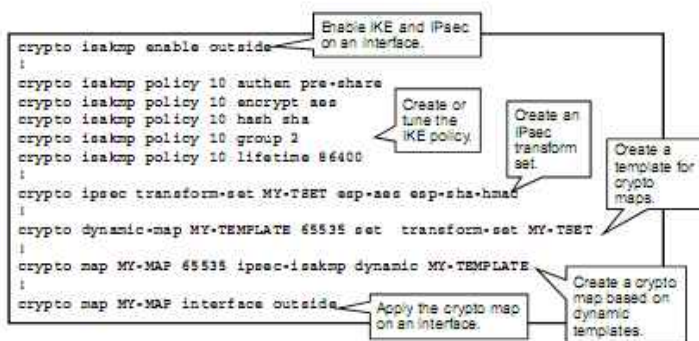
In Task 3, you can optionally tune the preconfigured IPsec policies to either add a policy that you want to use or remove some of the preconfigured policies. In most cases, it is recommended that you remove the preconfigured transform sets that use DES encryption.

To tune the existing IPsec policy, perform the following steps:

- Step 1** Using Cisco ASDM, navigate to the list of IKE policies at Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps.
- Step 2** Select the dynamic crypto map entry with priority 65,535, created by the Cisco ASDM, and click **Edit** to edit it.
- Step 3** Optionally, in the Transform Sets area, use the Add and Remove buttons to select or deselect IPsec transform sets that are used by the IPsec policy that supports dynamic Cisco Easy VPN connections.
- Step 4** Optionally, use the Move Up and Move Down buttons to change the default priority order, which the Cisco ASA adaptive security appliance uses to select the active IPsec transform set.
- Step 5** Optionally, you can enable perfect forward secrecy (PFS) for all client connections by checking the Enable Perfect Forward Secrecy check box. This setting can cause additional load on the Cisco ASA adaptive security appliance because the Cisco VPN Client and the Cisco ASA adaptive security appliance will need to perform a fresh DH exchange on each session key rekey.
- Step 6** Optionally, in the Advanced Tab, you can adjust session key lifetimes from their default values.
- Step 7** Click **OK**, **Apply**, and, optionally, click **Save** to save your configuration.

## Configuring Basic Cisco Easy VPN

### CLI Configuration



This output shows the command-line interface (CLI) commands that are required to configure the basic Cisco Easy VPN Server features.

In the CLI, use the **crypto isakmp enable** command to enable IKE on a Cisco ASA adaptive security appliance interface. Use the **crypto isakmp policy** commands to create one or more IKE policies with settings that are compatible with those of the Cisco VPN client.

Next, use the **crypto ipsec transform-set** command to define at least one IPsec transform set that is compatible with the Cisco IPsec VPN client.

Finally, create an IPsec policy by creating a crypto map and enabling the crypto map on an interface. First, create a template from which you will create crypto map entries dynamically, because clients connect to the Cisco ASA adaptive security appliance using the **crypto dynamic-map** command. In the crypto dynamic-map template, require that the clients support the configured IPsec transform set that was configured previously. Then, configure the main crypto map entity, using the **crypto map** command, to automatically create crypto map entries for authenticated clients, starting at sequence number 65,535, and using the configured template to enforce policy to clients. At the end, apply the crypto map to the VPN-terminating interface.

## Crypto Maps

A crypto map is a Cisco configuration mechanism that specifies the conditions for traffic protection. A crypto map is a collection of crypto map entries in which each entry defines a particular VPN tunnel. In site-to-site VPNs, these entries are defined statically, each entry describing the traffic and peer IP address for the tunnel. In Cisco Easy VPN, you cannot know the IP address or the exact traffic protection specification (because IP addresses are dynamically assigned to clients). You are, therefore, forced to use dynamic crypto map entries. With dynamic crypto map entries, the Cisco Easy VPN Server (Cisco ASA adaptive security appliance) creates crypto map entries in real time, based on the configured template, and fills in all required (dynamic) parameters based on the data that is obtained through IKE negotiation with the IPsec VPN clients.

## crypto isakmp enable

To enable ISAKMP negotiation on the interface on which the IPsec peer communicates with the adaptive security appliance, use the **crypto isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

**crypto isakmp enable** *interface-name*

### crypto isakmp enable Parameters

Parameter	Description
<i>interface-name</i>	Specifies the name of the interface on which to enable or disable ISAKMP negotiation.

## crypto isakmp policy authentication

To specify an authentication method within an IKE policy, use the **crypto isakmp policy authentication** command in global configuration mode. IKE policies define a set of parameters for IKE negotiation. To remove the ISAKMP authentication method, use the related **clear configure** command.

**crypto isakmp policy** *priority* **authentication** {*crack* | *pre-share* | *rsa-sig*}

### crypto isakmp policy authentication Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>crack</i>	Specifies IKE Challenge/Response for Authenticated Cryptographic (CRACK) as the authentication method.
<i>pre-share</i>	Specifies PSKs as the authentication method.
<i>rsa-sig</i>	Specifies RSA signatures as the authentication method. RSA signatures provide nonrepudiation for the IKE negotiation. This nonrepudiation means that you can prove to a third party whether you had an IKE negotiation with the peer.

## crypto isakmp policy encryption

To specify the encryption algorithm that should be used within an IKE policy, use the **crypto isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, which is DES, use the **no** form of this command.

**crypto isakmp policy** *priority* **encryption** {*aes* | *aes-192* | *aes-256* | *des* | *3des*}

## crypto isakmp policy encryption Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>aes</i>	Specifies that the encryption algorithm that should be used in the IKE policy is AES with a 128-bit key.
<i>aes-192</i>	Specifies that the encryption algorithm that should be in the IKE policy is AES with a 192-bit key
<i>aes-256</i>	Specifies that the encryption algorithm that should be used in the IKE policy is AES with a 256-bit key
<i>des</i>	Specifies that the encryption algorithm that should be used in the IKE policy is 56-bit DES-CBC
<i>3des</i>	Specifies that the encryption algorithm that should be used in the IKE policy is 3DES

## crypto isakmp policy group

To specify the DH group for an IKE policy, use the **crypto isakmp policy group** command in global configuration mode. IKE policies define a set of parameters to use during IKE negotiation. To reset the DH group identifier to the default value, use the **no** form of this command.

**crypto isakmp policy *priority* group {1 | 2 | 5}**

### crypto isakmp policy group Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>group 1</i>	Specifies that the 768-bit DH group should be used in the IKE policy. This is the default value.
<i>group 2</i>	Specifies that the 1024-bit DH2 should be used in the IKE policy.
<i>group 5</i>	Specifies that the 1536-bit DH5 should be used in the IKE policy.

## crypto isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **crypto isakmp policy hash** command in global configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

**crypto isakmp policy *priority* hash {md5 | sha}**

### crypto isakmp policy hash Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>md5</i>	Specifies that MD5 (HMAC variant) should be used as the hash algorithm for the IKE policy.
<i>sha</i>	Specifies that SHA-1 (HMAC variant) should be used as the hash algorithm for the IKE policy.



## crypto isakmp policy lifetime

To specify the lifetime of an IKE security association (SA) before it expires, use the **crypto isakmp policy lifetime** command in global configuration mode. You can specify an infinite lifetime if the peer does not propose a lifetime. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command.

**crypto isakmp policy priority lifetime seconds**

### crypto isakmp policy lifetime Parameters

Parameter	Description
<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>seconds</i>	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2,147,483,647 sec. Use 0 sec for infinite lifetime.

## Configuring Basic Cisco Easy VPN

### Implementation Guidelines

Consider the following implementation guideline:

- When tuning policies, you should carefully select IKE policies and IPsec transform sets because Cisco VPN Client has a fixed policy.

When implementing basic Cisco Easy VPN Server settings on the Cisco ASA adaptive security appliance, consider this implementation guideline:

- If you decide to tune the default IKE and IPsec settings that are configured by Cisco ASDM, or if you are configuring the Cisco ASA adaptive security appliance via the CLI, be aware that the Cisco VPN Client uses a preconfigured set of IKE and IPsec policies. Therefore, you need to configure the Cisco ASA adaptive security appliance to match one of these policy settings for connections to succeed.

# Configuring Group PSK Authentication

This topic describes how to configure and verify Cisco Easy VPN group authentication.

## Configuring Group PSK Authentication

### Configure Group PSK Authentication

- Basic Cisco Easy VPN authenticates the following:
  - The **remote peer** based on group passwords (pre-shared keys [PSKs])
  - Optionally, the **remote user** based on passwords or OTPs (XAUTH)
- Group passwords are shared by a group of users:
  - They are more vulnerable to compromise.
  - If compromised, an attacker can mount a man-in-the-middle attack against all VPN sessions of the group (even with XAUTH enabled).

© 2010 Cisco Systems, Inc. All rights reserved. VPN-11-34-010

The basic Cisco Easy VPN solution supports multiple levels of user and peer authentication. Peer authentication refers to the basic mutual authentication of two entities: the client and the Cisco ASA adaptive security appliance. In the basic Cisco Easy VPN solution, peer authentication uses group passwords that are configured on the Cisco ASA adaptive security appliance (inside each connection profile), and a group of VPN clients that typically share a common access policy. In addition to the group passwords, you can deploy Extended Authentication (XAUTH), which is an optional, one-way user authentication. This method of authentication supports passwords or one-time passwords (OTPs), with the help of an external authentication server, and can improve the reliability of VPN access authentication if group passwords are compromised.

Group passwords are secret authentication keys that are shared by a group of users and the Cisco ASA adaptive security appliance. Because of their shared nature, they are more vulnerable to compromise. For example, if one laptop of the group is stolen, the attacker will likely be able to extract the group password from its Cisco VPN Client connection entry.

If you are not using XAUTH, the attacker will be immediately able to log in to the VPN using the group password.

If you are using Extended Authentication, and if the attacker knows the group password, the attacker can mount a MITM attack, intercepting the initial negotiation between the client and the Cisco ASA adaptive security appliance, and spoofing identity of the Cisco ASA adaptive security appliance using the group password. The client has no means to distinguish between the legitimate gateway (Cisco ASA adaptive security appliance) and the attacker, and will send XAUTH credentials over the IKE session to the attacker. The attacker can then use these XAUTH credentials to log in to the VPN.

## Configuring Group PSK Authentication

### Configuration Tasks

1. Create a new group policy for Cisco Easy VPN connections
2. Create a new connection profile for Cisco Easy VPN connections, create a group password, and assign the new group policy



To configure group authentication in the basic Cisco Easy VPN solution, perform the following configuration tasks:

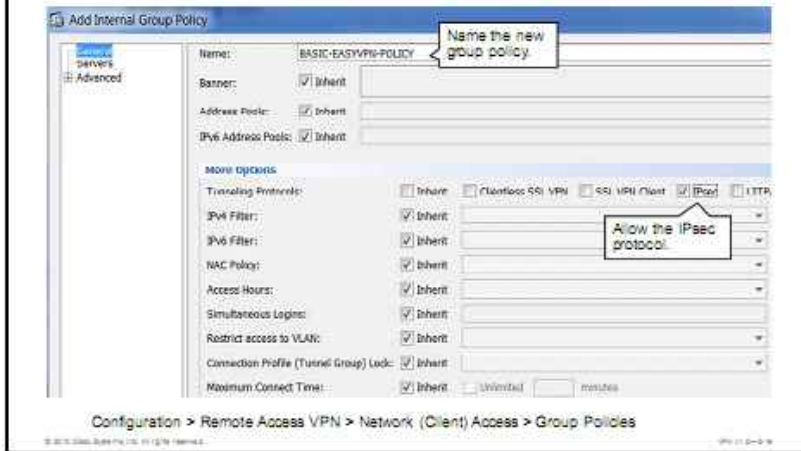
1. Create a new, custom group policy for your Cisco Easy VPN users. In this topic, you will create a single custom group policy for all users. Based on your requirements, you may need to create multiple custom group policies to differentiate users based on their access needs.
2. Create a new custom connection profile and assign the custom group policy to it. As with the custom group policy, based on your requirements, you may need to create multiple connection profiles to differentiate users based on their access needs and assign each connection profile a different group policy.

This figure presents the configuration scenario that is used in upcoming configuration tasks. On the Cisco ASA adaptive security appliance, you will create a custom connection profile named BASIC-EASYVPN-PROFILE, and a related group policy named BASIC-EASYVPN-POLICY.

In Cisco Easy VPN solutions that are based on group authentication, users explicitly configure the connection profile that they want to use inside the Cisco VPN Client, together with the group password.

## Configuring Group PSK Authentication

### Task 1: Create a New Group Policy



In the first configuration task, you create a new, custom group policy, which you will apply to VPN users via their connection profile. Perform the following steps:

- Step 1** In Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, and click **Add** to add a new policy.
- Step 2** Provide a name for the new group policy (BASIC-EASYVPN-POLICY in this example).
- Step 3** Uncheck the **Inherit** check box, then check the **IPsec** check box in the Tunneling Protocols area, and uncheck all other tunneling protocols.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration and, optionally, click **Save** to save your configuration.

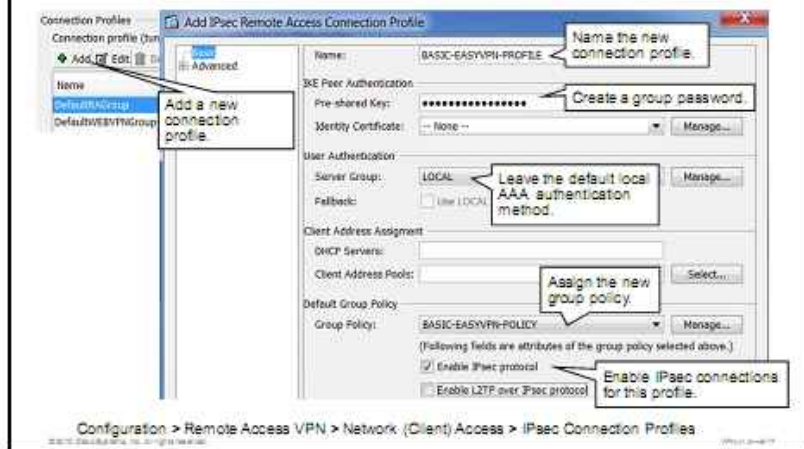
---

**Note** If your Cisco ASA adaptive security appliance supports other VPN access options that may reuse this policy, you may need to leave some of the other tunneling protocols enabled.

---

## Configuring Group PSK Authentication

### Task 2: Create a New Connection Profile



In the second configuration task, you create a new, custom connection profile to which you will assign VPN users. Perform the following steps:

- Step 1** In Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**, and click **Add** to add a new connection profile (not shown in the example).
- Step 2** Provide a name for the new connection profile (BASIC-EASYVPN-PROFILE in this example). You will need to configure this connection profile (group) name also in the connection entry of the Cisco IPsec VPN Client.
- Step 3** In the IKE Peer Authentication area, create a password (Pre-shared Key field) for this group. You will also need to configure this password in the connection entry of the Cisco IPsec VPN Client. Use a long and random group password because you are not likely to be able to change it easily after client software is deployed to client systems.
- Step 4** In the User Authentication area, leave the authentication method at its default settings (local authentication, authorization, and accounting [AAA] authentication).
- Step 5** In the Default Group Policy area, select the custom group policy (BASIC-EASYVPN-POLICY in this example) from the drop-down list.
- Step 6** Check the **Enable IPsec Protocol** check box.
- Step 7** Click **OK**.
- Step 8** Click **Apply** to apply the configuration and, optionally, click **Save** to save your configuration.

## Configuring Group PSK Authentication

### CLI Configuration

```
group-policy BASIC-EASYVPN-POLICY internal
group-policy BASIC-EASYVPN-POLICY attributes
  vpn-tunnel-protocol ipsec
!
tunnel-group BASIC-EASYVPN-PROFILE type remote-access
tunnel-group BASIC-EASYVPN-PROFILE general-attributes
  default-group-policy BASIC-EASYVPN-POLICY
tunnel-group BASIC-EASYVPN-PROFILE ipsec-attributes
  pre-shared-key Ad8gYmlOjFrPReAFiOkvpi
```

Annotations:

- Name the new group policy.
- Set the type of the connection profile.
- Enable only the IPsec protocol.
- Configure the group PSK.
- Assign the configured custom group policy.

This output shows the CLI commands that are required to configure basic Cisco ASA adaptive security appliance Cisco Easy VPN solution.

In the CLI, create a new, custom group policy using the **group-policy** command, and specify the group policy as **internal**. In the new group-policy attributes mode, enable the Cisco Easy VPN functionality for this group policy using the **vpn-tunnel-protocol ipsec** command.

Next, create a new, custom connection profile using the **tunnel-group** command, using the **type remote-access** parameter, and attach the custom BASIC-EASYVPN-POLICY group policy to this connection profile using the **default-group-policy** command. Move to the IPsec-related parameters of this connection profile using the **tunnel-group ipsec-attributes** command, and configure the group password for this connection profile using the **pre-shared-key** command.

The two commands that are seen in the figure are listed here. The command syntax for some of the commands is not shown here because those commands were already discussed in other lessons or topics.

### tunnel-group ipsec-attributes

To enter the ipsec-attributes configuration mode, use the **tunnel-group ipsec-attributes** command in global configuration mode. This mode is used to configure settings that are specific to the IPsec tunneling protocol. To remove all IPsec attributes, use the **no** form of this command.

**tunnel-group** *name* ipsec-attributes

#### tunnel-group ipsec-attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel group
<b>ipsec-attributes</b>	Specifies attributes for this tunnel group

## pre-shared-key

To specify a pre-shared key (PSK) to support IKE connections that are based on PSKs, use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

**pre-shared-key** *key*

### pre-shared-key Parameters

Parameter	Description
<i>key</i>	Specifies an alphanumeric key between 1 and 128 characters

## Configuring Group PSK Authentication

### Implementation Guidelines

Consider the following group PSK authentication implementation guidelines:

- Create groups of limited size to somewhat mitigate problems if the group key is compromised (laptop theft, and so on).
- Consider migrating to hybrid authentication to eliminate the man-in-the-middle issue.

When implement group PSK (password) authentication in a basic Cisco Easy VPN solution, consider the following implementation guidelines:

- To somewhat mitigate potential group password compromise, create user groups of limited size (that is, assign a limited number of users to a connection profile using a particular group password). With this setup, if a key is compromised, only connections of a limited number of users can be compromised, and it will be much easier to reconfigure the clients with a new group password.
- If you consider the risk of group password compromise unacceptable in your environment, you can deploy hybrid authentication to enhance the peer authentication process between the client and the Cisco ASA adaptive security appliance, making it resistant to such man-in-the-middle attacks. Hybrid authentication is discussed in an upcoming topic of this lesson.

# Configuring Extended User Authentication

This topic describes how to configure and verify Cisco Easy VPN XAUTH.

## Extended User Authentication

### Extended Authentication (XAUTH) Overview

XAUTH is additional one-way user authentication method:

- Occurs at the end of IKE Phase 1 (peer authentication) and before Phase 2
- Is configurable on a per-profile basis
- Is enabled by default for all IPsec connection profiles



IKE Extended Authentication (XAUTH) is a one-way, optional user authentication method that the Cisco ASA adaptive security appliance can use in addition to peer authentication. XAUTH occurs after IKE Phase 1 completes and before IKE Phase 2 (IPsec SA) negotiation begins. The XAUTH process uses the cryptographically protected IKE SA to send credentials from the client, to the Cisco ASA adaptive security appliance.

You should use XAUTH to enhance the authentication strength of group passwords, and to provide per-user services, such as the assignment of per-user IP addresses or access rules.

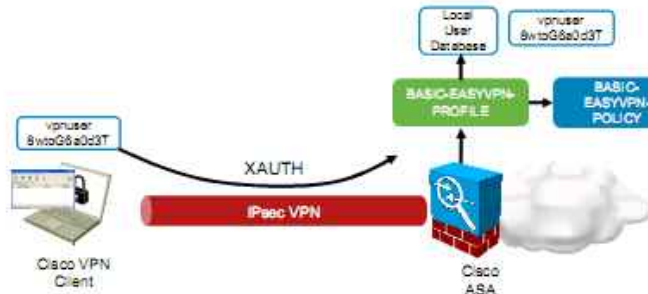
XAUTH can be enabled or disabled on a per-connection-profile basis. When you create a Cisco Easy VPN connection profile, XAUTH is enabled by default.



## Extended User Authentication

### Configuration Tasks

1. Ensure that connection profile uses XAUTH.
2. Configure local users and credentials.



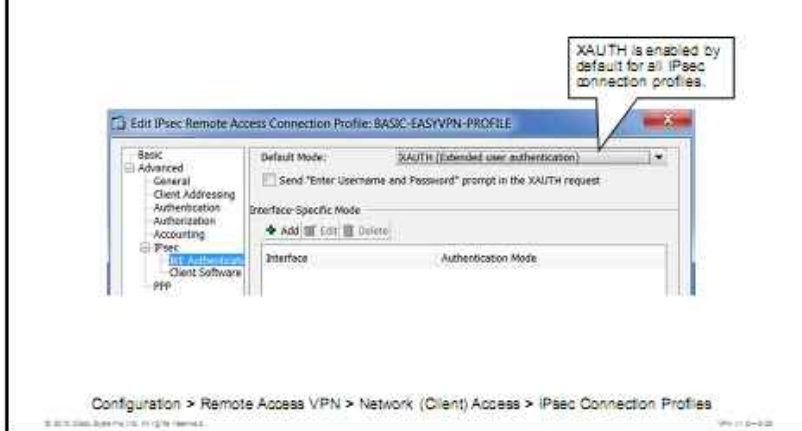
To configure basic user authentication in the basic Cisco Easy VPN solution, perform the following configuration tasks:

1. Verify that XAUTH is enabled in a connection profile.
2. Configure users and their credentials in the Cisco ASA adaptive security appliance local user database.

This figure presents the configuration scenario that is used in upcoming configuration tasks. You will create one user named "vpuser" in the local user database, and lock this user to the BASIC-EASYVPN-PROFILE connection profile.

## Extended User Authentication

### Task 1: Ensure That Connection Profile Uses XAUTH



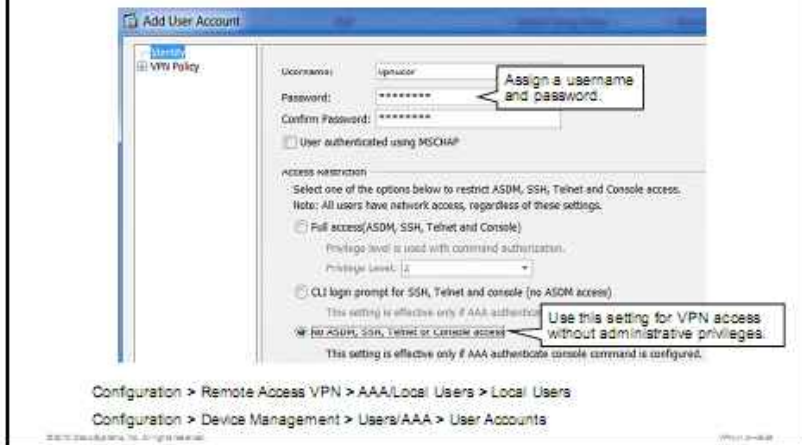
In the first task, verify that XAUTH is enabled in the connection profile or profiles that you want to use in the basic Cisco Easy VPN solution. The Cisco ASA adaptive security appliance enables XAUTH by default for all Cisco Easy VPN connection profiles.

Perform the following steps:

- Step 1** In Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**, and click **Edit** to edit the relevant connection profile (not shown in the example).
- Step 2** In the Edit IPsec Remote Access Connection Profile window, navigate to the **Advanced > IPsec > IKE Authentication Mode** pane on the left.
- Step 3** Verify that XAUTH is selected in the **Default Mode** drop-down box.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration and, optionally, click **Save** to save your configuration.

## Extended User Authentication

### Task 2: Configure Local Users and Credentials



In Task 2, you create a user account in the Cisco ASA adaptive security appliance local database. This user account must only be able to log in to the VPN, and not to the Cisco ASA adaptive security appliance management user interfaces (Cisco ASDM and the CLI). Perform the following tasks:

- Step 1** In Cisco ASDM, navigate to **Configuration > Remote Access VPN > AAA/Local Users > Local Users**, and click **Add** to add a new user account (not shown in the example).
- Step 2** Provide a name for the new user account (vpnuser in this example).
- Step 3** Create a password for the new user account.
- Step 4** In the Access Restriction area, click the **No ASDM, SSH, Telnet or Console Access** radio button. This selection will restrict the user to prevent these credentials from being accepted by device management functions.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the configuration.

## Extended User Authentication

### CLI Configuration

```
tunnel-group BASIC-EASYVPN-PROFILE ipsec-attributes
 isakmp ikev1-user-authentication xauth
!
username vpnuser password VI6esudcaYe4YjxN encrypted
username vpnuser attributes
 service-type remote-access
```

Only allow VPN access  
for this user account.

This output shows the CLI commands that are required to configure basic Cisco ASA adaptive security appliance Cisco Easy VPN user authentication.

In the CLI, use the **isakmp ikev1-user-authentication xauth** command in the tunnel-group ipsec-attributes mode to enable XAUTH in a connection profile if it has been changed from its default.

Then, create a user account in the local database, using the **username** command and assign it a password. In the username attributes mode, restrict this user to VPN access only using the **service-type remote-access** command. Also, assign this user into the BASIC-EASYVPN-PROFILE connection profile using the **group-lock value** command.

The command syntax for some of the commands is not shown here because those commands were already discussed in previous lessons.

### isakmp ikev1-user-authentication

To configure hybrid authentication during IKE, use the **isakmp ikev1-user-authentication** command in tunnel-group ipsec-attributes configuration mode. To disable hybrid authentication, use the **no** form of this command.

**isakmp ikev1-user-authentication** [*interface*] {**none** | **xauth** | **hybrid**}

#### isakmp ikev1-user-authentication Parameters

Parameter	Description
<i>interface</i>	(Optional) Specifies the interface on which the user authentication method is configured
<b>none</b>	Disables user authentication during IKE
<b>xauth</b>	Specifies XAUTH, also called extended user authentication
<b>hybrid</b>	Specifies hybrid XAUTH authentication during IKE

## username

To add a user to the adaptive security appliance database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username you want to remove. To remove all usernames, use the **no** version of this command without appending a username.

```
username name {nopassword | password password [mschap | encrypted | nt-encrypted] }  
[privilege priv_level]
```

### username Parameters

Parameter	Description
<code>name</code>	Specifies the name of the user as a string from 4 to 64 characters in length.
<code>nopassword</code>	Indicates that this user needs no password.
<code>password password</code>	Sets the password as a string from 3 to 16 characters in length.
<code>mschap</code>	Specifies that the password will be converted to Unicode and hashed using MD4 after you enter it. Use this keyword if users are authenticated using Microsoft Challenge Handshake Authentication Protocol version 1 or version 2 (MS-CHAPv1 or MS-CHAPv2).
<code>encrypted</code>	<p>Indicates that the password is encrypted (if you did not specify <code>mschap</code>). When you define a password in the <code>username</code> command, the adaptive security appliance encrypts the password when it saves the password to the configuration for security purposes. When you enter the <code>show running-config</code> command, the <code>username</code> command does not show the actual password; it shows the encrypted password that is followed by the <code>encrypted</code> keyword. For example, if you enter the password "test," the <code>show running-config</code> display would appear to be something like the following:</p> <pre>username pat password xv2dRhx0xPC6bel7s encrypted</pre> <p>The only time that you would actually enter the <code>encrypted</code> keyword at the CLI is if you are cutting and pasting a configuration to another adaptive security appliance and you are using the same password.</p>
<code>nt-encrypted</code>	<p>Indicates that the password is encrypted for use with MS-CHAPv1 or MS-CHAPv2. If you specified the <code>mschap</code> keyword when you added the user, then this keyword is displayed instead of the <code>encrypted</code> keyword when you view the configuration using the <code>show running-config</code> command.</p> <p>When you define a password in the <code>username</code> command, the adaptive security appliance encrypts the password when it saves the password to the configuration for security purposes. When you enter the <code>show running-config</code> command, the <code>username</code> command does not show the actual password; it shows the encrypted password followed by the <code>nt-encrypted</code> keyword. For example, if you enter the password "test," the <code>show running-config</code> display would appear to be something like the following:</p> <pre>username pat password DLauiaX3178ggcB5c7iVNw== nt-encrypted</pre> <p>The only time that you would actually enter the <code>nt-encrypted</code> keyword at the CLI is if you are cutting and pasting a configuration to another adaptive security appliance and you are using the same password.</p>
<code>privilege priv_level</code>	Sets a privilege level for this use from 0 to 15 (lowest to highest). The default privilege level is 2. This privilege level is used with command authorization.

## username attributes

To enter username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure attribute-value pairs for a specified user.

**username** *{name}* **attributes**

### username attributes Parameters

Parameter	Description
<i>name</i>	Provides the name of the user

# Configuring Client Network Settings

This topic describes how to configure and verify client VPN network settings.

## Configuring Client Network Settings

### Configuration Tasks

1. (Optional) Configure DNS, WINS, and domain name.
2. Configure allowed IP address assignment methods.
3. (Optional) Configure an address pool.
4. (Optional) Assign address pool to group policy.
5. Alternatively, assign IP addresses to users.

To configure client IP address assignment, you need to perform the following configuration tasks:

1. Optionally, configure client configuration parameters, such as DNS server addresses, in a group policy that is applied to your connection profile or profiles. This task is optional.
2. Globally configure the allowed IP address assignment methods on the Cisco ASA adaptive security appliance.
3. Optionally, configure an IP address pool if you decide to use pools from which users can lease client IP addresses.
4. Optionally, assign the configured IP address pool to the default or specific group policy.
5. Alternatively, assign IP addresses to individual users, if you require per-user addresses, where each user “owns” a particular IP address.

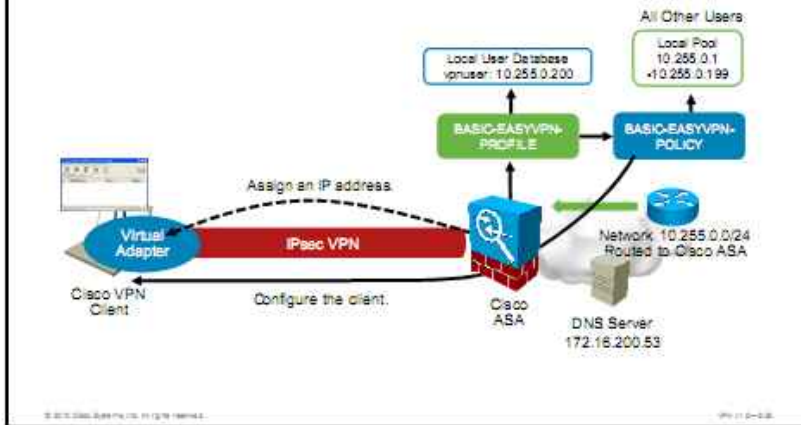
---

**Note** You need to configure either per-group-policy or per-user IP addresses. If you configure no address assignment, Cisco Easy VPN connections to the Cisco ASA adaptive security appliance will fail.

---

## Configuring Client Network Settings

### Configuration Scenario



This figure presents the configuration scenario that is used in upcoming configuration tasks. The client should be configured with the internal DNS server address of 172.16.200.53. The Cisco ASA adaptive security appliance will use IP addresses from the 10.255.0.0/24 network for client address assignment. The policy dictates that the “vpnuser” user account should always have a fixed IP address of 10.255.0.200, while all other users of the BASIC-EASYVPN-PROFILE will have IP addresses assigned from a pool starting at 10.255.0.1 and ending at 10.255.0.199. The 10.255.0.0/24 network must be routed to the Cisco ASA adaptive security appliance in the internal network.



## Configuring Client Network Settings

### Task 1: Configure DNS, WINS, and Domain Name

- Consider using the **default group policy** for basic network settings.



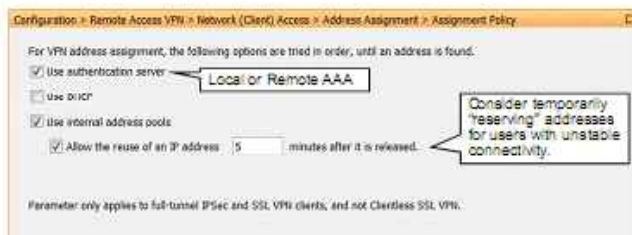
In the first task, you can optionally push some network settings to the client. These settings, such as the DNS server, allow the client to transparently access internal resources that are protected by the Cisco ASA adaptive security appliance. In this scenario, the Cisco ASA adaptive security appliance is acting similarly to a DHCP server, but using the IKE “mode configuration” functionality to configure the client.

To configure the client with internal DNS infrastructure information, and a DNS resolver suffix (the default domain name that is appended to nonqualified DNS queries) using the custom group policy, perform the following tasks:

- Step 1** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** and click **Edit** to edit the desired group policy that is applied to a particular connection profile (not shown in the example).
- Step 2** Choose **Servers** in the pane on the left.
- Step 3** Uncheck the **Inherit** check box for DNS Servers, and enter the IP address of the DNS server or servers in the DNS Servers field.
- Step 4** Uncheck the **Inherit** check box for Default Domain, and enter the default domain search suffix in the Default Domain field.
- Step 5** Click **OK**.
- Step 6** Click **Apply** to apply the configuration, and click **Save** to save your configuration.

## Configuring Client Network Settings

### Task 2: Configure Allowed Assignment Methods



Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy

© 2010 Cisco Systems, Inc. All rights reserved.

VPN 11 2-126

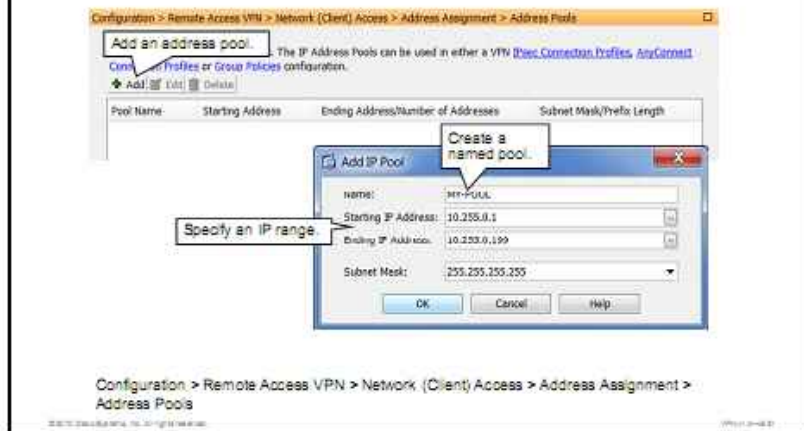
In the second task, you must globally enable all allowed IP address assignment methods on the Cisco ASA adaptive security appliance. In this example, you will enable authentication-server-assigned (by the LOCAL or remote AAA server) IP addresses, and the internal local IP address pools.

Perform the following steps:

- Step 1** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**.
- Step 2** Check the **Use Authentication Server** and **Use Internal Address Pools** check boxes. Optionally, configure the caching time to allow reuse of addresses for re-established sessions.

## Configuring Client Network Settings

### Task 3: Configure Address Pool (Optional)

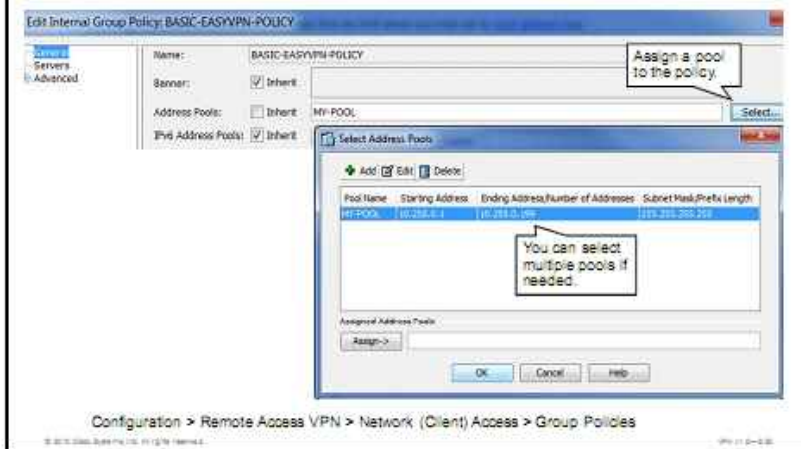


In the optional Task 3, you create IP address pools if you intend to use pool-based address assignment. Perform the following steps:

- Step 1** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**.
- Step 2** Click **Add** to add a new address pool
- Step 3** In the Add IP Pool dialog box, name the new IP pool and specify the starting and ending IP addresses of the pool range. Assign the subnet mask of 255.255.255.255 for remote access connections.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration, and click **Save** to save your configuration.

## Configuring Client Network Settings

### Task 4: Assign Address Pool to Group Policy (Optional)

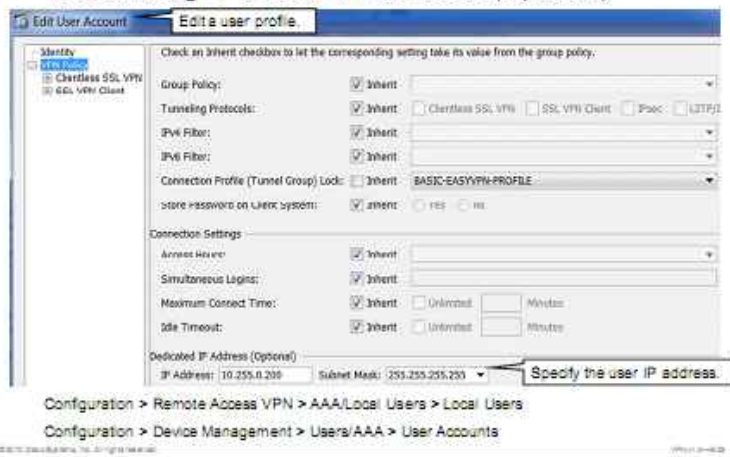


To assign an IP address pool to a connection profile via its group policy, perform the following steps:

- Step 1** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Select a group policy that you want to edit and click the **Edit** button (not shown in the example).
- Step 2** Uncheck the **Inherit** check box for Address Pools and click the **Select** button in the **Address Pools** field.
- Step 3** Select the IP address pool (or multiple pools, if needed and if configured) in the Select Address Pools dialog box, and click the **Assign** button.
- Step 4** Click **OK** twice.
- Step 5** Click **Apply** to apply the configuration, and click **Save** to save your configuration.

## Configuring Client Network Settings

### Task 5: Assign Per-User IP Addresses (Optional)



If you need to assign per-user IP addresses, you can do so in the profile of the user account. To assign a fixed IP address to a user, perform the following steps:

- Step 1** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > AAA/Local Users > Local Users**. Select a user account that you want to edit and click **Edit** (not shown in the example).
- Step 2** In the Edit User Account window, choose **VPN Policy** in the pane on the left.
- Step 3** Enter the desired IP address and a host mask (255.255.255.255) in the Dedicated IP Address area.
- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration, and click **Save** to save your configuration.

## Configuring Client Network Settings

### CLI Configuration

```
group-policy BASIC-EASYVPN-POLICY attributes
  dns-server value 172.16.200.53
  default-domain value domain.com
!
vpn-addr-assign aaa
vpn-addr-assign local
no vpn-addr-assign dhcp
vpn-addr-assign local reuse-delay 5
!
ip local pool MY-POOL 10.255.0.1-10.255.0.199 mask 255.255.255.255
!
group-policy BASIC-EASYVPN-POLICY attributes
  address-pools value MY-POOL
!
username vpnuser attributes
  vpn-framed-ip-address 10.255.0.200 255.255.255.255
```

Configure client network parameters.

Configure allowed assignment methods.

Create a named pool.

Assign a pool to the policy.

Specify the per-user IP address.

This output shows the CLI commands that are required to configure the per-policy and per-user client IP address assignment.

In the CLI, first configure the optional **client** network settings that the Cisco ASA adaptive security appliance will attempt to configure the client with. In the **group-policy attributes** section, specify the DNS server address (or multiple addresses), and the default domain suffix using the **dns-server value** and **default-domain value** commands respectively.

Next, use the **vpn-addr-assign** command to globally enable AAA server (LOCAL and remote AAA server) and pool-based IP address assignment. Then, use the **ip local pool** command to define a named local pool. Optionally, use the **vpn-add-assign local reuse-delay** command to specify the caching time of address reuse.

Inside a group policy, use the **address-pools value** command to assign a pool to a group policy. For per-user address assignment, use the **vpn-framed-ip-address** command within user account attributes.

The command syntax for some of the commands is not shown here because those commands are covered in previous lessons.

### group-policy attributes

To enter group-policy configuration mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, use the **no** version of this command. In group-policy configuration mode, you can configure attribute-value pairs for a specified group policy.

**group-policy** *name* **attributes**

#### group-policy attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the group policy

## dns-server

To set the IP address of the primary and secondary DNS servers, use the **dns-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

```
dns-server {value ip_address [ip_address] | none}
```

### dns-server Parameters

Parameter	Description
value <i>ip_address</i>	Specifies the IP address of the primary and secondary DNS servers.
none	Sets dns-servers to a null value, thereby allowing no DNS servers. Prevents inheriting a value from a default or specified group policy.

## default-domain

To set a default domain name for users of the group policy, use the **default-domain** command in group-policy configuration mode. To delete a domain name, use the **no** form of this command.

```
default-domain {value domain-name | none}
```

### default-domain Parameters

Parameter	Description
value <i>domain-name</i>	Identifies the default domain name for the group.
none	Indicates that there is no default domain name. Sets a default domain name with a null value, thereby disallowing a default domain name. Prevents inheriting a default domain name from a default or specified group policy.

## vpn-addr-assign

To specify a method for assigning IP addresses to remote access clients, use the **vpn-addr-assign** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command. To remove all configured VPN address assignment methods from the adaptive security appliance, use the **no** version of this command without arguments.

```
vpn-addr-assign {aaa | dhcp | local [reuse-delay delay]}
```

### vpn-addr-assign Parameters

Parameter	Description
aaa	Obtains IP addresses from an external or internal (LOCAL) AAA authentication server.
dhcp	Obtains IP addresses via DHCP.
local	Assigns IP addresses from an IP address pool that is configured on the adaptive security appliance and associates them with a tunnel group.
reuse-delay <i>delay</i>	(Optional) The delay before a released IP address can be reused. The range is 0 to 480 min. The default is 0 (disabled).

## ip local pool

To configure IP address pools to be used for VPN remote access tunnels, use the **ip local pool** command in global configuration mode. To delete address pools, use the **no** form of this command.

**ip local pool** *poolname first-address—last-address* [*mask mask*]

### ip local pool Parameters

Parameter	Description
<i>poolname</i>	Specifies the name of the IP address pool
<i>first-address</i>	Specifies the starting address in the range of IP addresses
<i>last-address</i>	Specifies the final address in the range of IP addresses
<i>mask mask</i>	(Optional) Specifies a subnet mask for the pool of addresses

## address-pools

To specify a list of address pools for allocating addresses to remote clients, use the **address-pools** command in group-policy attributes configuration mode. To remove the attribute from the group policy and enable inheritance from other sources of group policy, use the **no** form of this command.

**address-pools value** *address\_pool1* [...*address\_pool6*]

**address-pools none**

### address-pools Parameters

Parameter	Description
<b>value</b>	Specifies a list of up to six address pools from which to assign addresses.
<i>address_pool</i>	Specifies the name of the address pool that is configured with the <b>ip local pool</b> command. You can specify up to six local address pools.
<b>none</b>	Specifies that no address pools are configured and disables inheritance from other sources of group policy.

## vpn-framed-ip-address

To specify the IP address to assign to a particular user, use the **vpn-framed-ip-address** command in username mode. To remove the IP address, use the **no** form of this command.

**vpn-framed-ip-address** *{ip\_address}* *{subnet\_mask}*

### vpn-framed-ip-address Parameters

Parameter	Description
<i>ip_address</i>	Provides the IP address for this user
<i>subnet_mask</i>	Specifies the subnetwork mask



# Configuring Basic Access Control and Split Tunneling

This topic describes how to configure basic access control and split tunneling in a Cisco Easy VPN solution.

Configuring Basic Access Control	
Configuration Choices	
Choice	Criteria
Use interface ACL bypass	When all remote users are completely trusted (enabled by default)
Use interface ACLs	When requiring per-user or per-group access rules with contiguous client addressing
Use per-user or per-profile ACLs	When requiring per-user or per-group access rules with any client addressing (recommended over interface ACLs)
Use split tunneling	To increase performance with direct client Internet access, without access control

In all full tunneling VPNs, the Cisco ASA adaptive security appliance allows you to bypass its interface access control lists (ACLs) for traffic that has arrived over a VPN connection. This ability can be useful in environments where no access control beyond VPN authentication is required to access protected resources. Note that the Cisco ASA adaptive security appliance can still apply per-user or per-group ACLs, DAP-assigned ACLs, service policies, and service module redirection to this traffic, if needed.

Alternatively, you can disable the bypass and configure interface ACLs to permit traffic from VPN users to the protected network. You should consider this option when you require per-user or per-group access control and you have assigned contiguous IP pools or per-user address ranges to users to make interface ACLs configurations manageable.

---

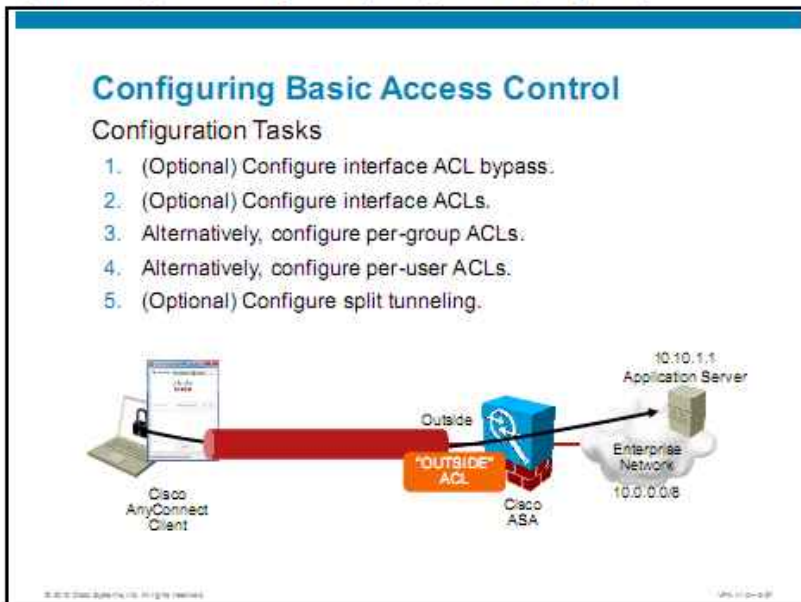
**Note**      Disabling of interface ACL bypass is a global configuration option and affects all types of VPNs that are configured on the security appliance.

---

A better alternative than interface ACLs is to deploy per-user or per-group access rules to create separate ACLs that only specify what remote users can access and apply those rules dynamically to remote access tunnels. This method is the recommended and most scalable method.

Finally, you will need to decide whether you want to allow split tunneling or not. By default, the Cisco ASA adaptive security appliance configures the client to forward all IP traffic over the VPN tunnel. Split tunneling allows you to tunnel only certain traffic to specific internal protected networks, while all other traffic bypasses the VPN tunnel. Split tunneling can improve the performance of applications that do not require the VPN tunnel (such as Internet access), but may increase risk, because the client is not protected by central site security mechanisms when connecting to the other networks. It also may increase risk because the client can be used as a relay between the external networks and the internal protected network more easily if the client is compromised by an attacker.

Split tunneling can be configured separately for each group policy.



To configure access control in a Cisco Easy VPN solution, you typically perform some of the following configuration tasks:

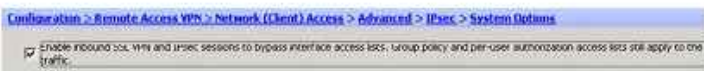
1. Configure the Cisco ASA adaptive security appliance to bypass interface ACLs for traffic arriving through the VPN. As this is a default setting, you may want to disable it. This task is optional.
2. Reconfigure the interface ACLs to allow some traffic arriving through the VPN. This task is optional, and is not required if you have configured some other access control method.
3. Alternatively, configure per-group (using a group policy) ACLs to implement per-group access control.
4. Alternatively, configure per-user ACLs to implement per-user access control.
5. Optionally, configure split tunneling to enable remote clients to directly access all networks that are not located beyond the Cisco ASA adaptive security appliance VPN gateway.

This figure presents the configuration scenario that is used in upcoming configuration tasks. Remote users will only be allowed to access a single application server (10.10.1.1) in the protected network using an interface ACL, or a per-user or per-group ACL, to control the access. Clients use addresses from the 10.255.0.0/24 network. The VPN client will perform split tunneling and only tunnel traffic that is destined for the 10.0.0.0/8 network to the Cisco ASA adaptive security appliance.

## Configuring Basic Access Control

### Task 1: Configure Interface ACL Bypass

- Interface ACL bypass disables interface ACL filtering for VPN tunnel traffic.
- Default setting of the ASA.
- Per-user or per-group ACLs will be checked.



Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options

Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Bypass Interface Access List

To configure the interface-ACL-bypass policy using Cisco ASDM, perform the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options**.
- Step 2** In this scenario, uncheck the check box that enables this behavior, because you will be configuring per-policy ACLs to control access.
- Step 3** Click **Apply** to apply this setting to the security appliance.

## Configuring Basic Access Control

### Task 2: Configure Interface ACLs

If you use the ACL of an interface for VPN filtering follow these guidelines:

- Use IP address pools or per-user addresses as source.
- Ensure that cleartext spoofing of these addresses is not possible on the adaptive security appliance VPN interface, using neighboring devices.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
inside (2 incoming rules):									
1	<input checked="" type="checkbox"/>	any	any	ip	Deny	0			
2	<input checked="" type="checkbox"/>	any	any	ip	Deny	0			Implicit rule
outside (3 incoming rules):									
1	<input checked="" type="checkbox"/>	10.255.0.0/24	10.10.1.1	http	Permit	0			Allow VPN web
2	<input checked="" type="checkbox"/>	any	any	ip	Deny	0			
3	<input checked="" type="checkbox"/>	any	any	ip	Deny	0			Implicit rule

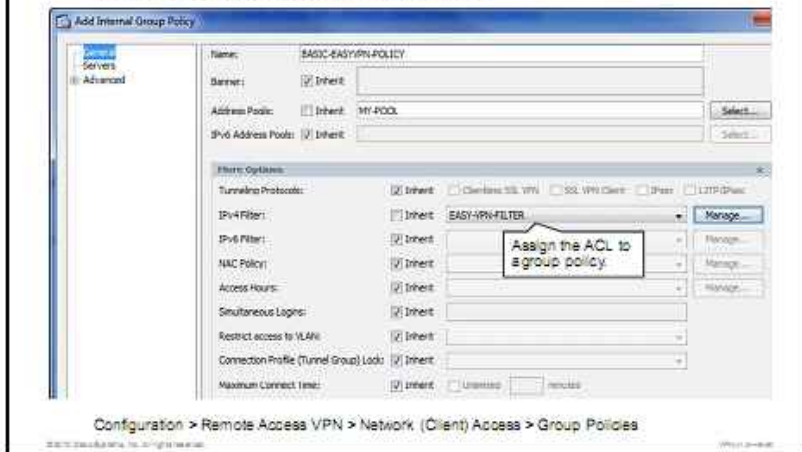
Configuration > Firewall > Access Rules

To implement the desired policy, you could configure Cisco ASA adaptive security appliance interface ACLs to permit the required traffic from remote clients. In this example, the “outside” interface (where the VPN tunnel terminates) ACL permits HTTP access from VPN clients (the clients will source their traffic from the gateway-assigned IP address in the 10.255.0.0/24 range) to the 10.10.1.1 web server.

When you configure interface ACLs to permit VPN access, make sure that packets matching the permit rules cannot arrive at the Cisco ASA adaptive security appliance in cleartext from an attacker that spoofs the assigned IP addresses. Usually, you can configure an adjacent router with appropriate ACLs to prevent this problem.

## Configuring Basic Access Control

### Task 3: Configure per-Group ACLs

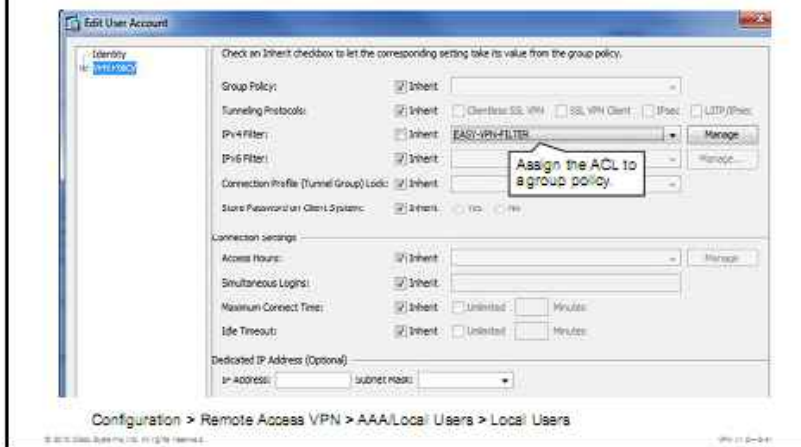


Perform the following steps to apply an access list to a user or group policy:

- Step 1** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Select a group policy that you want to edit and click the **Edit** button (not shown in the example).
- Step 2** Edit a group policy, uncheck the **Inherit** check box, and select the newly created ACL in the **IPv4 Filter** field. You can click the **Manage** button to create an ACL.
- Step 3** Click **OK**.
- Step 4** Click **Apply** to apply this setting to the security appliance.

## Configuring Basic Access Control

### Task 4: Configure per-User ACLs



Perform the following steps to apply an access list to a user or group policy:

- Step 1** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > AAA/Local Users**. Select a user account that you want to edit and click the **Edit** button (not shown in the example).
- Step 2** Uncheck the **Inherit** check box and select the newly created ACL in the **IPv4 Filter** field. You can click the **Manage** button to create an ACL.
- Step 3** Click **Apply** to apply this setting to the security appliance.

## Configuring Basic Access Control

### Task 5: Configure Split Tunneling

The screenshot displays two windows from the Cisco ASDM interface. The top window, titled 'Configuration > Firewall > Advanced > Standard ACL', shows a table with one entry: 'MY-SPLIT-TUNNEL' with ID 1, address 10.0.0.0/8, and action 'Permit'. A callout box points to this entry with the text 'Create a standard ACL describing tunneled networks.' The bottom window, titled 'Edit Internal Group Policy: BASIC-EASYVPN-POLICY', shows the 'Split Tunneling' section. The 'Policy' field has 'Inherit' unchecked and 'Tunnel Network List Below' selected. The 'Network List' field has 'Inherit' unchecked and 'MY-SPLIT-TUNNEL' selected. Callout boxes point to these fields with the text 'Enable split tunneling of specific networks.' and 'Reference the ACL.' respectively. The breadcrumb at the bottom of the second window reads 'Configuration > Firewall > Advanced > Standard ACL' and 'Configuration > Remote Access VPN > Network (Client) Access > Group Policies'.

If you want to enable split tunneling for a group policy (and therefore all connection profiles using this group policy or perhaps the default group policy to enable split tunneling in a scalable manner for all VPN users), perform the following steps:

- Step 1** Using the Cisco ASDM ACL Manager, navigate to **Configuration > Firewall > Advanced > Standard ACL** to create a standard ACL and permit all networks (the internal protected destinations) that you want to tunnel. Traffic to all networks denied by this ACL will bypass the tunnel. In this example, only traffic to the 10.0.0.0/8 internal protected network will be tunneled. All other traffic will bypass the tunnel.
- Step 2** Using Cisco ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Select a group policy that you want to edit and click the **Edit** button (not shown in the example).
- Step 3** In the Edit Internal Group Policy window, choose **Advanced > Split Tunneling** in the pane on the left.
- Step 4** Uncheck the **Inherit** check box in the **Policy** field, and choose the **Tunnel Network List Below** option.
- Step 5** Uncheck the **Inherit** check box in the **Network List** field, and choose the newly created split-tunnel ACL (MY-SPLIT-TUNNEL ACL is this example).
- Step 6** Click **OK**.
- Step 7** Click **Apply** to apply this setting to the security appliance.

## Configuring Basic Access Control

### CLI Configuration

Disable interface ACL bypass

```
no sysopt connection permit-vpn
```

Configure interface ACLs

```
access-list OUTSIDE remark Allow VPN web server access
access-list OUTSIDE extended permit tcp 10.255.0.0 255.255.255.0
    host 10.10.1.1 eq www
access-list OUTSIDE extended deny ip any any
!
access-group OUTSIDE in interface outside
```

Interface ACLs on the Cisco ASA adaptive security appliance are only applied to transient traffic. Encrypted packets that terminate on the Cisco ASA adaptive security appliance are not subject to the interface ACL. By default, the unencrypted packets are also not subject to any interface ACL. The exception to this is when the **sysopt connection permit-vpn** command is disabled, which would cause the Cisco ASA adaptive security appliance to reinject the unencrypted packets into the interface as transient packets and thereby subject the packets to the interface ACL.

These two output samples show the CLI commands that are required to configure interface ACL bypass or an interface ACL to permit the desired connectivity over the VPN tunnel. To disable the default policy that permits all connectivity over the VPN tunnels, use the **no sysopt connection permit-vpn** command.

The example in the figure also shows the ACL named OUTSIDE applied to the outside interface in the inbound direction that only permits HTTP traffic that is sourced from 10.255.0.0/24 (the IP address pool range for this scenario) to the 10.10.1.1 internal web server.

### sysopt connection permit-vpn

For traffic that enters the adaptive security appliance through a VPN tunnel and is then decrypted, use the **sysopt connection permit-vpn** command in global configuration mode to allow the traffic to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. This feature is enabled by default. To disable this feature, use the **no** form of this command. This command was changed from **sysopt connection permit-ipsec** from the Cisco ASA 5500 Series Adaptive Security Appliances Release Software Release 7.1(1) and later.

#### sysopt connection permit-vpn

### access-list remark

To specify the text of a remark to add before or after an **access-list extended** command, use the **access-list remark** command in global configuration mode. To delete the remark, use the **no** form of this command.

```
access-list id [line line-num] remark text
```



## access-list remark Parameters

Parameter	Description
<code>id</code>	Name of an access list
<code>line line-num</code>	(Optional) The line number at which to insert a remark or an access control entry (ACE)
<code>remark text</code>	Text of the remark to add before or after an <b>access-list extended</b> command

## access-list extended

To add an ACE, use the **access-list extended** command in global configuration mode. An ACL is made up of one or more ACEs with the same ACL ID. ACLs are used to control network access or to specify traffic for many features to act upon. To remove an ACE, use the **no** form of this command. To remove the entire access list, use the **clear configure access-list** command.

```
access-list id [line line-number] [extended] {deny | permit} {protocol | object-group
protocol_obj_grp_id} {src_ip_mask | interface ifc_name | object-group network_obj_grp_id}
[operator port | object-group service_obj_grp_id] {dest_ip_mask | interface ifc_name | object-
group network_obj_grp_id} [operator port | object-group service_obj_grp_id] object-group
icmp_type_obj_grp_id [log [[level] [interval secs] | disable | default]] [inactive | time-range
time_range_name]
```

## access-list extended Parameters

Parameter	Description
<code>id</code>	Specifies the access list ID, as a string or integer up to 241 characters in length. The ID is case-sensitive.  <b>Tip</b> Use all capital letters to see the access list ID better in your configuration.
<code>line line-num</code>	(Optional) Specifies the line number at which to insert the ACE. If you do not specify a line number, the ACE is added to the end of the access list. The line number is not saved in the configuration; it only specifies where to insert the ACE.
<code>extended</code>	(Optional) Adds an ACE.
<code>deny</code>	Denies a packet if the conditions are matched. In the case of network access (the <b>access-group</b> command), this keyword prevents the packet from passing through the Cisco ASA adaptive security appliance. In the case of applying application inspection to a class map (the <b>class-map</b> and <b>inspect</b> commands), this keyword exempts the traffic from inspection. Some features do not allow deny ACEs to be used, such as Network Address Translation (NAT). See the command documentation for each feature that uses an ACL for more information.
<code>permit</code>	Permits a packet if the conditions are matched. In the case of network access (the <b>access-group</b> command), this keyword lets the packet pass through the Cisco ASA adaptive security appliance. In the case of applying application inspection to a class map (the <b>class-map</b> and <b>inspect</b> commands), this keyword applies inspection to the packet.

Parameter	Description
<code>protocol</code>	Specifies the IP protocol name or number. For example, User Datagram Protocol (UDP) is 17, TCP is 6, and exterior gateway protocol (EGP) is 47.
<code>object-group protocol_obj_grp_id</code>	Specifies the identifier of a protocol object group. See the <b>object-group protocol</b> command to add an object group.
<code>src_ip</code>	Specifies the IP address of the network or host from which the packet is being sent. Enter the <b>host</b> keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the <b>any</b> keyword instead of the address and mask to specify any address.
<code>mask</code>	The subnet mask for the IP address. When you specify a network mask, the method is different from the Cisco IOS Software <b>access-list</b> command. The Cisco ASA adaptive security appliance uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
<code>interface ifc_name</code>	Specifies the interface address as the source or destination address.  <b>Note</b> You must specify the <b>interface</b> keyword instead of specifying the actual IP address in the access list when the traffic destination is a device interface.
<code>object-group network_obj_grp_id</code>	Specifies the identifier of a network object group. See the <b>object-group network</b> command to add an object group.
<code>operator</code>	(Optional) Matches the port numbers that are used by the source or destination. The permitted operators are as follows: <ul style="list-style-type: none"> <li>■ <b>lt</b>: less than</li> <li>■ <b>gt</b>: greater than</li> <li>■ <b>eq</b>: equal to</li> <li>■ <b>neq</b>: not equal to</li> <li>■ <b>range</b>: an inclusive range of values. When you use this operator, specify two port numbers, for example: <code>range 100 200</code></li> </ul>
<code>port</code>	(Optional) If you set the protocol to TCP or UDP, specifies the integer or name of a TCP or UDP port. DNS, Discard, Echo, Ident, Network Time Protocol (NTP), remote procedure call (RPC), SunRPC, and Talk protocols each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP.
<code>object-group service_obj_grp_id</code>	(Optional) If you set the protocol to TCP or UDP, specifies the identifier of a service object group. See the <b>object-group service</b> command to add an object group.
<code>dest_ip</code>	Specifies the IP address of the network or host to which the packet is being sent. Enter the <b>host</b> keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the <b>any</b> keyword instead of the address and mask to specify any address.
<code>object-group icmp_type_obj_grp_id</code>	(Optional) If the protocol is Internet Control Message Protocol (ICMP), specifies the identifier of an ICMP-type object group. See the <b>object-group icmp-type</b> command to add an object group.

Parameter	Description
<b>log</b>	(Optional) Sets logging options when an ACE matches a packet for network access (an access list that is applied with the <b>access-group</b> command). If you enter the <b>log</b> keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 sec). If you do not enter the <b>log</b> keyword, then the default system log message 106023 is generated.
<b>level</b>	(Optional) Sets the system log message 106100 severity level from 0 to 7. The default level is 6 (informational).
<b>interval secs</b>	(Optional) Specifies the log interval at which to generate system log message 106100. Valid values are from 1 to 600 sec. The default is 300.
<b>disable</b>	(Optional) Disables logging for this ACE.
<b>default</b>	(Optional) Sets logging to the default method, which is to generate system log message 106023 for each denied packet.
<b>inactive</b>	(Optional) Disables an ACE. To re-enable it, enter the entire ACE without the <b>inactive</b> keyword. This feature lets you keep a record of an inactive ACE in your configuration to make re-enabling easier.
<b>time-range</b> <i>time_range_name</i>	(Optional) Schedules each access control entry to be activated at specific times of the day and week by applying a time range to the access control entry. See the <b>time-range</b> command for information about defining a time range.

## access-group

To bind an access list to an interface, use the **access-group** command in global configuration mode. To unbind an access list from the interface, use the **no** form of this command.

**access-group** *access-list* {**in** | **out**} **interface** *interface\_name* [*per-user-override* | *control-plane*]

### access-group Parameters

Parameter	Description
<i>access-list</i>	Access list ID
<b>in</b>	Filters the inbound packets at the specified interface
<b>out</b>	Filters the outbound packets at the specified interface
<b>interface</b> <i>interface-name</i>	Name of the network interface
<i>per-user-override</i>	(Optional) Allows downloadable user access lists to override the access list that is applied to the interface
<i>control-plane</i>	(Optional) Specifies if the rule is for to-the-box traffic

## Configuring Basic Access Control

### CLI Configuration (Cont.)

Configure per-profile and per-user ACLs

```
access-list EASY-VPN-FILTER extended permit tcp any
host 10.10.1.1 eq www
|
group-policy BASIC-EASYVPN-POLICY attributes
  vpn-filter value EASY-VPN-FILTER
|
username vpnuser attributes
  vpn-filter value EASY-VPN-FILTER
```

Assign the ACL to a group policy.

Optionally, assign the ACL to a user profile.

Configure split tunneling

```
access-list MY-SPLIT-TUNNEL standard permit 10.0.0.0 255.0.0.0
|
group-policy BASIC-EASYVPN-POLICY attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value MY-SPLIT-TUNNEL
```

Create a standard ACL describing tunneled networks.

Enable split tunneling of specific networks.

These two output samples show the CLI commands that are required to configure per-profile or per-user ACLs and split tunneling respectively.

Create an extended ACL governing user access using the **access-list** command. To assign this ACL dynamically to all users of a particular connection profile, edit the group policy of the profile and assign the ACL to the policy using the **vpn-filter value** command. You can use the same command to assign the ACL to a specific user profile (if needed). Note as mentioned before, the source IP address in this ACL can be “any” and the Cisco ASA adaptive security appliance will dynamically replace this address with the assigned IP address of the user when activating this ACL on a VPN tunnel.

To configure split tunneling using the CLI, first create a standard ACL describing internal protected networks that are to be tunneled. To create a split tunneling policy for all users of a particular connection profile, edit the group policy of the profile. Use the **split-tunnel-policy tunnelspecified** command to enable split tunneling and the **split-tunnel-network-list value** to reference the standard ACL that describes tunneled networks.

### vpn-filter

To specify the name of the ACL to use for VPN connections, use the **vpn-filter** command in group-policy or username mode. To remove the ACL, including a null value that is created by issuing the **vpn-filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **vpn-filter none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **vpn-filter** command to apply those ACLs.

**vpn-filter** {value *acl-name* | none}

## vpn-filter Parameters

Parameter	Description
<code>value acl-name</code>	Provides the name of the previously configured access list.
<code>none</code>	Indicates that there is no access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.

## split-tunnel-policy

To set a split tunneling policy, use the **split-tunnel-policy** command in group-policy configuration mode. To remove the **split-tunnel-policy** attribute from the running configuration, use the **no** form of this command. Use of this command enables inheritance of a value for split tunneling from another group policy.

Split tunneling lets a remote-access IPsec client conditionally direct packets over an IPsec tunnel in encrypted form or to a network interface in cleartext form. With split-tunneling enabled, packets that are not bound for destinations on the other side of the IPsec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

This command applies this split tunneling policy to a specific network.

**split-tunnel-policy** { **tunnelall** | **tunnelspecified** | **excludespecified** }

## split-tunnel-policy Parameters

Parameter	Description
<code>split-tunnel-policy</code>	Indicates that you are setting rules for tunneling traffic.
<code>tunnelall</code>	Specifies that no traffic goes in the clear or to any other destination than the adaptive security appliance. Remote users reach Internet networks through the corporate network and do not have access to local networks.
<code>tunnelspecified</code>	Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear and is routed by the ISP of the remote user.
<code>excludespecified</code>	Defines a list of networks to which traffic goes in the clear. This feature 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. This option applies only to the Cisco VPN Client.

## split-tunnel-network-list

To create a network list for split tunneling, use the **split-tunnel-network-list** command in group-policy configuration mode. To delete a network list, use the **no** form of this command.

To delete all split tunneling network lists, use the **no split-tunnel-network-list** command without arguments. Use of this command deletes all configured network lists, including a null list that is created by issuing the **split-tunnel-network-list none** command.

When there are no split tunneling network lists, users inherit any network lists that exist in the default or specified group policy. To prevent users from inheriting such network lists, use the **split-tunnel-network-list none** command.

Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling.

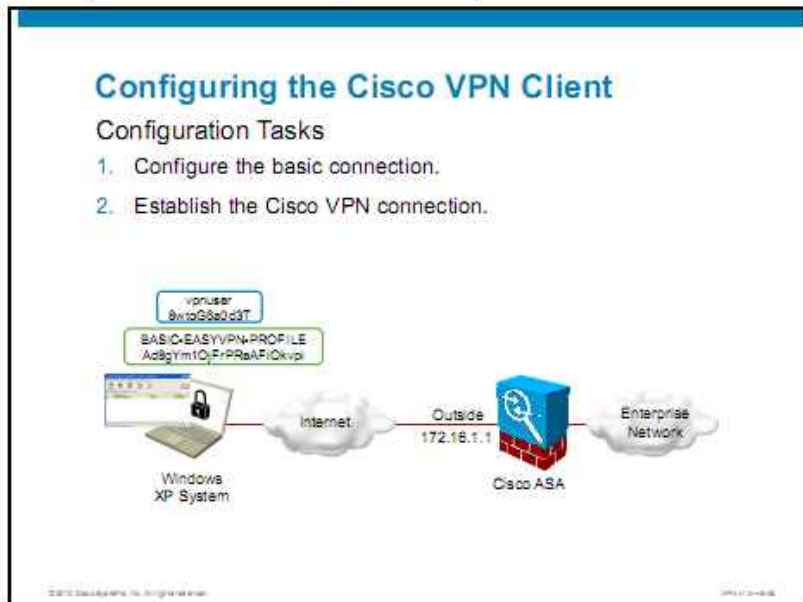
**split-tunnel-network-list** { **value access-list name** | **none** }

## split-tunnel-network-list Parameters

Parameter	Description
<b>value</b> <i>access-list name</i>	Identifies an access list that enumerates the networks to tunnel or not tunnel
<b>none</b>	Indicates that there is no network list for split tunneling; the adaptive security appliance tunnels all traffic

# Configuring the Cisco VPN Client

This topic describes how to configure and verify Cisco VPN Client connections.



To deploy Cisco VPN Client in a basic Cisco Easy VPN solution, you will perform the following configuration tasks:

1. Configure the Cisco VPN Client connection entry settings (the IP address of the Cisco ASA adaptive security appliance, the connection profile name, and the group password).
2. Establish the Cisco Easy VPN connection using the Cisco VPN Client.

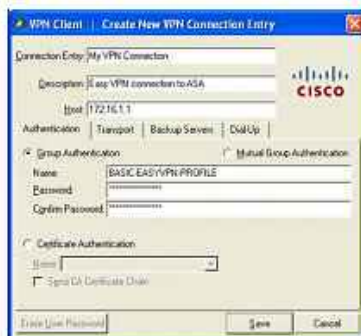
This figure presents the configuration scenario that is used in upcoming configuration tasks. You will configure the Cisco VPN Client on a Microsoft Windows XP system, and the Cisco ASA adaptive security appliance uses the 172.16.1.1 IP address on its “outside” interface. The VPN client will use the BASIC-EASYVPN-PROFILE connection profile with a strong group password. The remote user will use the “vpnuser” account to log in to the Cisco ASA adaptive security appliance.

## Configuring the Cisco VPN Client

### Task 1: Configure Basic Connection

For basic group password authentication, configure the following values:

- Local connection name
- IP address of the Cisco ASA adaptive security appliance VPN-terminating interface
- Group name
- Group password



After installing the Cisco VPN Client, you need to configure a connection entry that will describe the Cisco Easy VPN tunnel connection. Perform the following steps on the Cisco VPN Client:

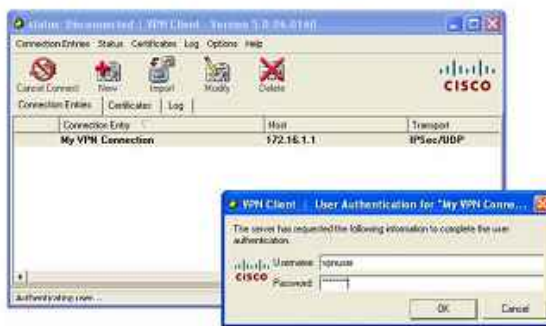
- Step 1** Start the Cisco VPN Client.
- Step 2** In the Cisco VPN Client main window, click the **New** button to create a new connection entry (not shown in this figure).
- Step 3** Specify a local name for the connection entry (“My VPN Connection” in this figure), and optionally add a description.
- Step 4** In the Host field, specify the IP address of the Cisco ASA adaptive security appliance VPN-terminating interface (172.16.1.1 in this example).
- Step 5** In the Authentication tab, select the **Group Authentication** method, and enter the group name and password. The group name must correspond to the name of the connection profile that is configured on the Cisco ASA adaptive security appliance (“BASIC-EASYVPN-PROFILE” in this example). The key must match the PSK that is configured in the connection profile on the Cisco ASA adaptive security appliance.
- Step 6** Click **Save** to save the profile.



## Configuring the Cisco VPN Client

### Task 2: Establish the Cisco VPN Connection

- Click **Connect** or double-click the entry.
- Enter the username and password if prompted.
- The policy can allow clients to save this password.



To verify the VPN connection, select the configured profile and click the Connect button. If you have configured XAUTH for this profile, the VPN client will prompt you for a username and password. In this example, you can log in with the credentials of the "vpnuser" account. You can also allow this username and password pair to be saved on the client so that users can log in without specifying a password every time. If you do not consider allowing users to log in without a password an unacceptable risk, you can configure this setting in the group policy of the connection profile.

When connected, the Cisco IPsec VPN Client will minimize by default. You can reinvoke the user interface by double-clicking or right-clicking its tray icon.

## Verifying the Cisco VPN Connection

### Client-Side Verification



After the initial connection, the Cisco ASA adaptive security appliance will push the network configuration (DNS server, domain name) to the client and assign the client the configured IP address. If you reopen the Cisco VPN Client main window, you can observe the connection status in the title and status bars.

If you right-click the Cisco VPN Client tray icon and choose to view Statistics, you can observe your connection details, including the assigned IP address (10.255.0.200 in this example), the negotiated cryptographic algorithms (IPsec transform set), and some statistics on exchanged packets and data.

# Verifying the Cisco VPN Connection

## Client-Side Verification (Cont.)

No Split Tunneling (Default)

Split Tunneling

**No Split Tunneling (Default)**

Network	Subnet Mask	Network	Subnet Mask
Tunnel all networks.		0.0.0.0	0.0.0.0

**Split Tunneling**

Network	Subnet Mask	Network	Subnet Mask
Tunnel specific networks.		10.0.0.0	255.0.0.0

© 2010 Cisco Systems, Inc. All rights reserved. VPN1-2-6-80

To verify the state of split tunneling and routing on the client, you can navigate to the Route Details tab of the Statistics window. On the left side, you can see a client that is configured with no split tunneling (that is, the default setting). In the Secured Routes pane, you can see the default network 0.0.0.0/0 instructing all traffic to enter the tunnel. On the right side, you can see a client that is configured for split tunneling. In the Secured Routes pane, you can see the default network 10.0.0.0/8 instructing only traffic to this specific network to enter the tunnel.

## Verifying the Cisco VPN Connection

### Gateway-Side Verification

The screenshot shows the Cisco ASDM interface for monitoring VPN sessions. The breadcrumb path is **Monitoring > VPN > VPN Statistics > Sessions**. The main table displays session statistics for IPsec and SSL VPN. The IPsec section is expanded to show a list of sessions. A callout box points to the 'IPsec Remote Access' filter, with the text 'Select IPsec Remote Access sessions.' Below the session list, two callout boxes point to the 'Group Policy Connection Profile' and 'Assigned IP Address' columns, with the text 'Verify the profile and policy' and 'Verify the IP address assignment.' respectively.

Remote Access	Site-to-Site	Clientless	VPN Client	Inactive	Total	E-mail Proxy	VPN Load Bal.
1	0	0	0	0	0	0	1

Username	Group Policy Connection Profile	Assigned IP Address Public(Peer) IP Address	Protocol Encryption	Login Time Duration	Client(Peer) Type Version
vpnuser	BASIC-EAS-VPN-POLICY BASIC-EAS-VPN-PROFILE	172.16.0.200 172.16.0.204	IPsec AES128	11:43:18 UTC Fri Feb 12 2010 0h:05m:56s	AnyNet 3.0.0.1108

To verify the connection of the client on the Cisco ASA adaptive security appliance, using Cisco ASDM, navigate to the **Monitoring > VPN > VPN Statistics > Session** pane. Choose **IPsec Remote Access** in the Filter by field. The VPN session should be displayed in the main pane, where you can verify all session parameters.

## Verifying the Cisco VPN Connection

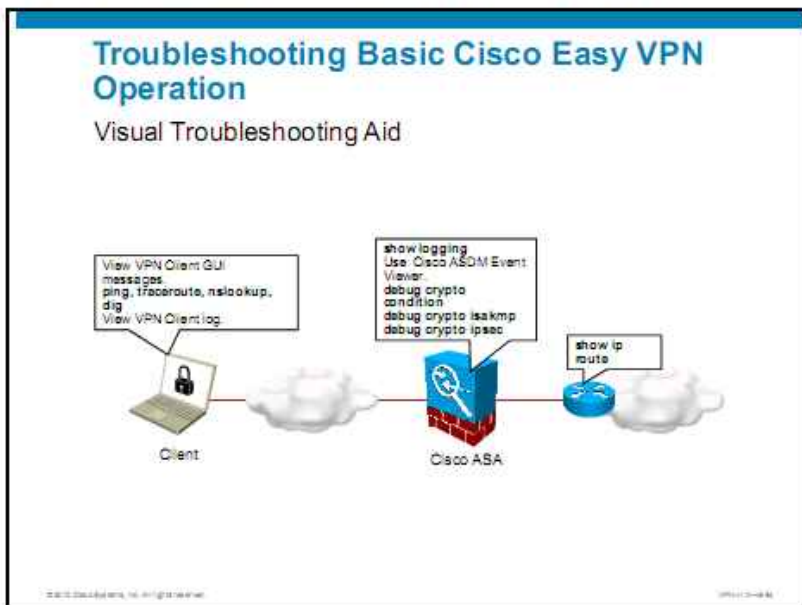
### Gateway-Side CLI Verification

```
ASA#show vpn-sessiondb remote
Session Type: IPsec
Username      : vpnuser                Index      : 27
Assigned IP   : 10.255.0.200             Public IP   : 172.16.0.204
Protocol      : IKE IPsec
License       : IPsec
Encryption    : 3DES AES128                     Hashing     : SHA1
Bytes Tx      : 7196                       Bytes Rx    : 11308
Group Policy  : BASIC-EAS-VPN-POLICY      Tunnel Group : BASIC-EAS-VPN-PROFILE
Login Time    : 11:43:18 UTC Fri Feb 12 2010
Duration      : 0h:05m:51s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                       VLAN        : none
```

In the CLI, use the **show vpn-sessiondb remote** command to obtain the same information.

# Troubleshooting Basic Cisco Easy VPN Operation

This topic describes how to troubleshoot Cisco Easy VPN session establishment between a Cisco VPN Client and a Cisco ASA adaptive security appliance gateway.

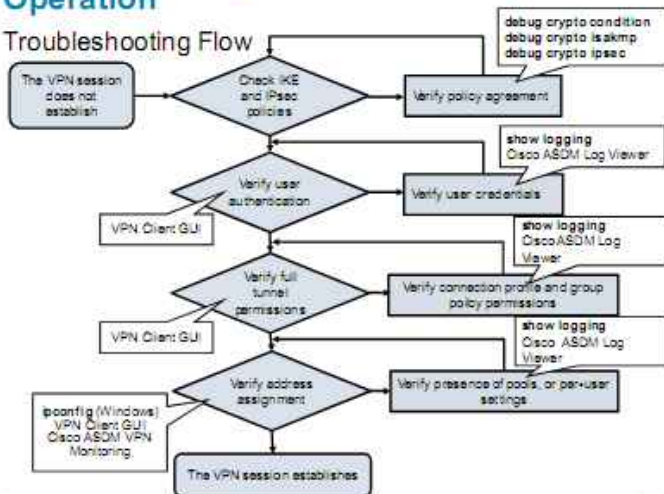


When troubleshooting Cisco Easy VPN session establishment, you should perform troubleshooting tasks on both the client and the Cisco ASA adaptive security appliance, if possible. Sometimes, you may need to also resolve routing issues on adjacent network devices. This figure shows some most useful troubleshooting commands and actions that you can use on involved components.

Note that the Cisco ASA adaptive security appliance will extensively log most issues into its syslog subsystem. Debug commands are generally not required, except for in-depth troubleshooting of IKE and IPsec negotiation issues.

## Troubleshooting Basic Cisco Easy VPN Operation

### Troubleshooting Flow



If you encounter session establishment issues, you may follow these steps to troubleshoot the issue:

- Step 1** First, verify that the IKE and IPsec protocols successfully negotiate based on matching IKE and IPsec policies on the client and the Cisco ASA adaptive security appliance. You should use the **debug crypto condition** command to limit debugging information to a particular user or IP address, and then use the **debug crypto isakmp** and **debug crypto ipsec** commands to troubleshoot policy compatibility.
- Step 2** If the IKE and IPsec negotiations complete with no errors, verify if user authentication works and the user is supplying the correct credentials. The Cisco ASA adaptive security appliance will clearly indicate these issues in its syslog messages.
- Step 3** Next, verify whether the connection profile and the associated group policy allow IPsec VPN tunnels. The Cisco ASA adaptive security appliance will clearly indicate these issues in its syslog messages.
- Step 4** Finally, verify that the Cisco ASA adaptive security appliance is able to assign an IP address to the client. The IP Address Assignment (IPAA) subsystem will extensively log to the syslog subsystem to indicate any issues.

**Note** If all these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.

### debug crypto isakmp

To show debug messages for ISAKMP, use the **debug crypto isakmp** command in privileged EXEC mode. To stop showing debug messages for ISAKMP, use the **no** form of this command.

**debug crypto isakmp** [timers] [level]

## debug crypto isakmp Parameters

Parameter	Description
<code>timers</code>	(Optional) Shows debug messages for ISAKMP timer expiration.
<code>level</code>	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Levels 2 through 7 show additional information. Level 254 shows decrypted ISAKMP packets in a human readable format. Level 255 shows hexadecimal dumps of decrypted ISAKMP packets.

## debug crypto ipsec

To show debug messages for IPsec, use the **debug crypto ipsec** command in privileged EXEC mode. To stop showing debug messages for IPsec, use the **no** form of this command.

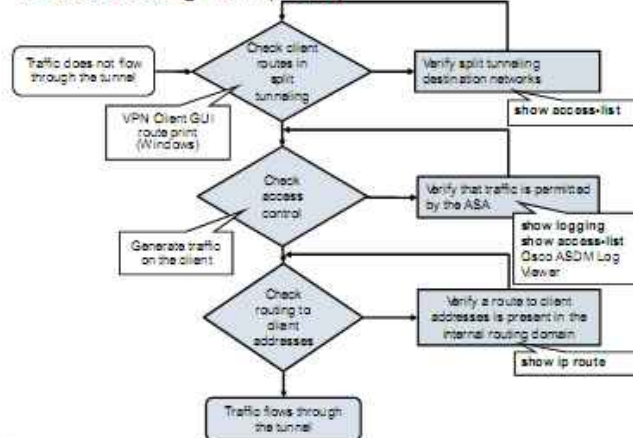
**debug crypto ipsec** [*level*]

## debug crypto ipsec Parameters

Parameter	Description
<code>level</code>	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

## Troubleshooting Basic Cisco Easy VPN Operation

### Troubleshooting Flow (Cont.)



If your Cisco Easy VPN session establishes, but there is no connectivity over the tunnel, you may follow these steps to troubleshoot the issue:

- Step 1** First, if you are using split tunneling, verify that the correct routes (networks) to the tunneled destination are present in the routing table. You can observe if the routes are present in the Cisco VPN Client GUI, or by examining the client routing table.
- Step 2** Next, verify that the Cisco ASA adaptive security appliance is not denying traffic from the VPN tunnel. Examine the Cisco ASA adaptive security appliance syslog to see messages that are about permitted or denied packets.
- Step 3** Finally, verify that the protected network has a route to the client-assigned addresses by examining routing tables in internal network routers along the path to the destination.

**Note** If all these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.



## Troubleshooting Basic Cisco Easy VPN Operation

### Gateway-Side Issues

- No shared IKE policies between client and gateway

```
asa#debug crypto condition peer 172.16.1.254
asa#debug crypto isakmp 3
[IKEv1 DEBUG]: IP = 172.16.1.254, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: False
[IKEv1]: IP = 172.16.1.254, Connection landed on tunnel_group
BASIC-EASYVPN-PROFILE
[IKEv1]: IP = 172.16.1.254, All IKE SA proposals found unacceptable!
```

- No shared IPsec transform sets between client and gateway

```
%ASA-5-713257: Phase 2 failure: Mismatched attribute types for class
Encapsulation Mode: Rcv'd: Tunnel Cfg'd: Transport
%ASA-5-713904: Group = BASIC-EASYVPN-PROFILE, Username = vpnuser,
IP = 172.16.1.254, All IPsec SA proposals found unacceptable!
%ASA-5-713259: Group = BASIC-EASYVPN-PROFILE, Username = vpnuser,
IP = 172.16.1.254, Session is being torn down. Reason: Phase 2 Mismatch
```

These output samples list the Cisco ASA adaptive security appliance debug and syslog messages that indicate two rare session establishment issues: a failed IKE negotiation that is caused by incompatible policies (note that the IKE debugging level must be set to at least 3) and a failed IPsec negotiation that is caused by incompatible IPsec policies.

## Troubleshooting Basic Cisco Easy VPN Operation

### Gateway-Side Issues (Cont.)

- IPsec VPN full tunneling not enabled or allowed in profile group policy or connection profile

```
ASA-3-713206: Group = BASIC-EASYVPN-PROFILE, Username = vpnuser, IP = 172.16.1.254, Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
```

- Client authentication failure: bad password

```
ASA-6-113015: AAA user authentication Rejected : reason = Invalid password : local database : user = vpnuser  
ASA-6-716039: Group <fltGrpPolicy> User <vpnuser> IP <172.16.1.254> Authentication: rejected
```

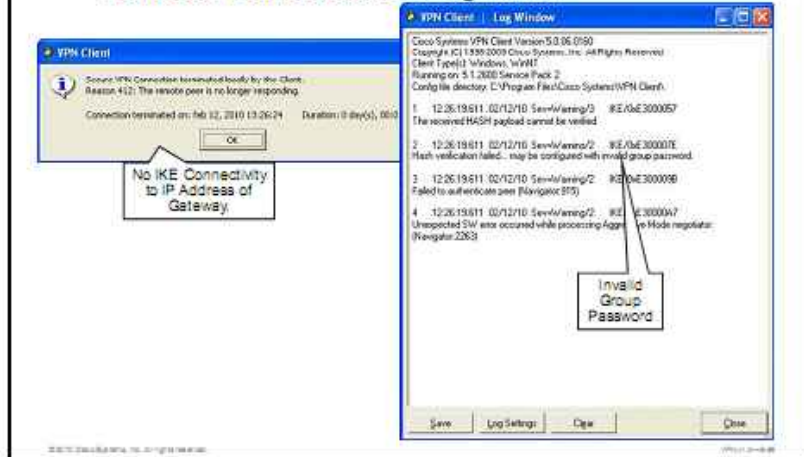
- No IP address pool assigned to a specific or default group policy

```
ASA-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools  
ASA-5-737007: IPAA: Local pool request failed for tunnel-group BASIC-EASYVPN-PROFILE  
ASA-4-737012: IPAA: Address assignment failed  
ASA-5-732006: Group <BASIC-EASYVPN-POLICY> User <vpnuser> IP <172.16.1.254> Invalid address <0.0.0.0> assigned to SVC connection.
```

These output samples list the Cisco ASA adaptive security appliance syslog messages that indicate some common session establishment issues. The issues are a session teardown that is caused by the IPsec VPN function not being enabled for a user, a connection profile, or a group policy; a failed user authentication that is caused by a bad password; and a failed IP address assignment that is caused by no IP address pools or no per-user IP addresses being configured on the Cisco ASA adaptive security appliance.

## Troubleshooting Basic Cisco Easy VPN Operation

### Client-Side Notifications and Log Viewer



On the client, the most common issues that you may observe are the following:

- The unreachability of the Cisco ASA adaptive security appliance, which the client will indicate after a one-minute timeout with a message indicating an unresponsive peer.
- A mismatch in group passwords. If you open the Cisco VPN Client Log Window, you will see hints that this issue may be the case for session setup failure.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- A basic full tunneling Cisco Easy VPN solution involves basic gateway configuration, user authentication, client configuration, and access control configuration.
- In basic gateway configuration, you should enable the IKE and IPsec protocols on a Cisco ASA adaptive security appliance interface.
- In basic Cisco Easy VPN solutions, peers are authenticated using group passwords.
- XAUTH is used to perform user authentication. In basic Cisco Easy VPN solutions, users are authenticated against the local user database.
- Configuration of basic client network settings includes configuration of DNS servers and IP address assignment method.
- You can use interface ACLs, per-user ACLs or per-profile ACLs to control access through VPN connections. Use split tunneling to specify that only certain traffic will be subject to encryption.
- Configure basic settings in the Cisco VPN Client before establishing the connection.
- Use various **show** and **debug** commands to troubleshoot basic easy VPN operations.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-10-24-000

# Deploying Advanced Authentication in Cisco Easy VPN Solutions

---

## Overview

Establishing a virtual private network (VPN) connection between an IP Security (IPsec) VPN client and the VPN gateway using the Cisco Easy VPN solution can be simple for the client and more complicated for the gateway site. Before the IPsec VPN clients establish secure connection to the VPN gateway, the IPsec client should authenticate to the VPN gateway. Typically, end users are required to coordinate their authentication setup with the network administrator on the VPN gateway site.

This lesson guides you through the different authentication methods that the IPsec VPN client can use to authenticate itself to the VPN gateway.

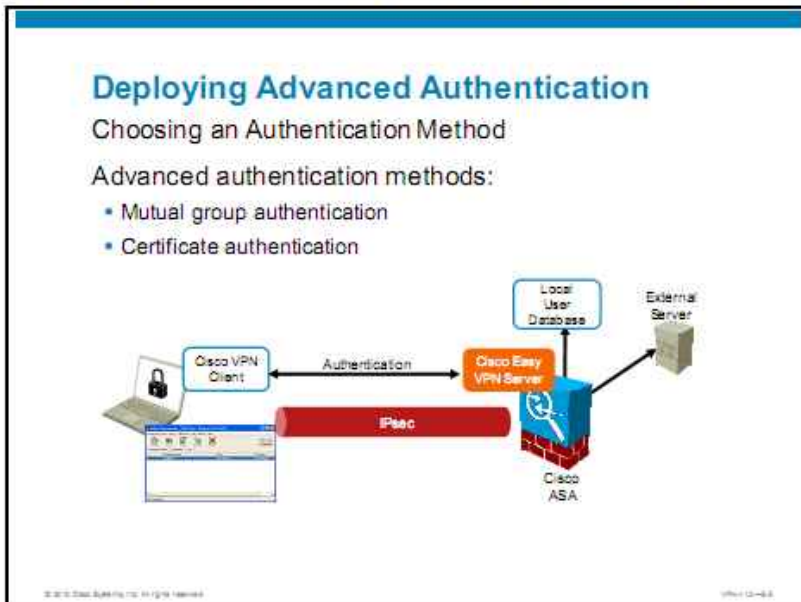
## Objectives

Upon completing this lesson, you will be able to deploy advanced authentication methods of the Cisco ASA adaptive security appliance Cisco Easy VPN Server to support IPsec VPN clients. This ability includes being able to meet these objectives:

- Plan the deployment of advanced authentication in Cisco Easy VPN
- Deploy Cisco ASA adaptive security appliance Cisco Easy VPN Server certificate authentication
- Deploy Cisco VPN Client certificate authentication
- Deploy advanced gateway PKI integration and external certificate authorization
- Troubleshoot PKI integration

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic describes how to plan the deployment of advanced client authentication.



In addition to the group authentication and Extended Authentication (XAUTH), Cisco Easy VPNs support two additional authentication methods: mutual group authentication and certificate-based client-side authentication. Both methods require installation of an identity digital certificate.

## Deploying Advanced Authentication

### Input Parameters

Parameter	Description
Group name and group PSK	Required to specify group name and password for mutual authentication
User authentication data	Required to authenticate users
PKI information	Required to enroll the ASA or the clients into a PKI; required to select CA certificate for mutual authentication
Time synchronization options	Required to synchronize time on the Cisco ASA adaptive security appliance and clients

When you deploy a Cisco Easy VPN solution, consider the following input parameters:

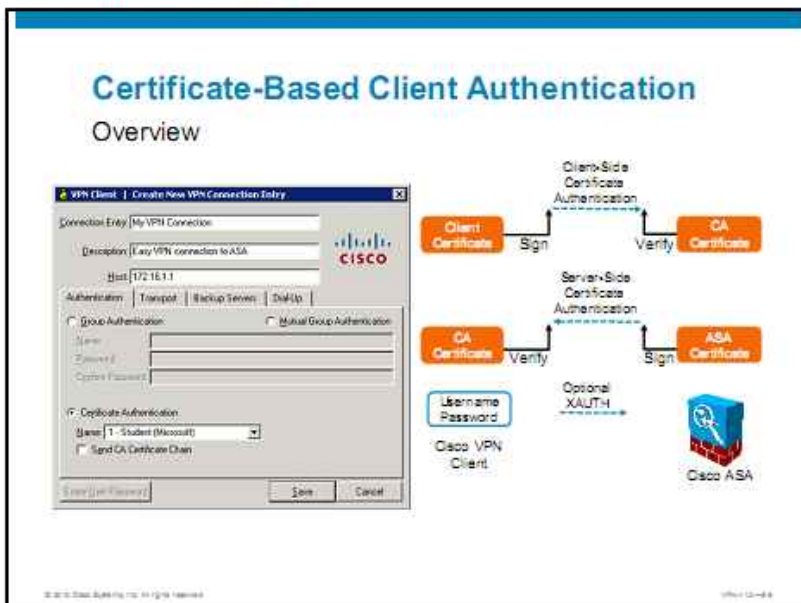
- Group name and group pre-shared key (PSK)
- User authentication data
- Public key infrastructure (PKI) information
- Time synchronization options

If you are using a smart card or electronic token to authenticate a connection, create a connection entry that defines the certificate that is provided by the smart card. For example, if you are using ActivCard Gold, an accompanying certificate is in the Microsoft Certificate Store. When you create a new connection entry for using the smart card, choose that certificate.

The Cisco VPN Client supports authentication with digital certificates through a smart card or an electronic token.

# Deploying Cisco VPN Client Certificate Authentication

This topic describes how to configure and verify the Cisco VPN Client to use an external CA and provision client certificates.



To use digital certificates, each peer enrolls with a certificate authority (CA), which is responsible for issuing digital certificates. A CA can be a trusted vendor or a private CA that you establish within an organization. When two peers want to communicate, they exchange certificates and digitally sign data to authenticate each other. When you add a new peer to the network, it enrolls with a CA.

After the Cisco VPN Client is enrolled with the PKI, you choose the Certificate Authentication option and select the client identity certificate that will be used to authenticate the client to the server.

In the second authentication stage, the client authenticates the VPN server by verifying its identity certificate using the appropriate CA certificate.

In the optional third stage, the user can be prompted for authentication using XAUTH. This optional step has already been covered previously.



## Certificate-Based Client Authentication

### Configuration Tasks

1. Enroll a client into a PKI.
2. Enroll the Cisco ASA into PKI (same as in site-to-site).
3. Enable certificate authentication in a connection profile (same as in site-to-site).
4. (Optional) Define certificate-to-connection profile map (same as in site-to-site).

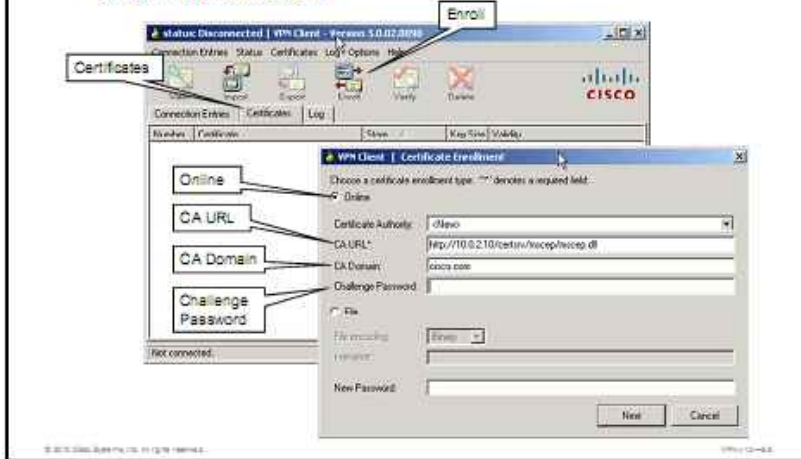


To deploy certificate-based client authentication, you will perform these tasks:

1. Enroll the Cisco VPN Client into the PKI.
2. Enroll the Cisco ASA adaptive security appliance into the PKI. This procedure is identical to the enrollment procedure that was performed in site-to-site VPNs and will therefore not be repeated.
3. Enable certificate-based authentication in the connection profile. This task is equivalent to the certificate-based authentication that was configured in site-to-site VPNs and will not be repeated.
4. Optionally, define certificate-to-connection profile map. If you do not configure mapping, then the organizational unit field of the client certificate will be used to determine the connection profile on the Cisco ASA adaptive security appliance. This task is equivalent to the mapping that was configured in site-to-site VPNs and will not be repeated.

## Certificate-Based Client Authentication

### Task 1: Enroll Client



The Cisco VPN Client can obtain a certificate by enrolling with a CA over the network or by creating a file request. There are two methods that are supported by the IPsec VPN client: online and file-based. This section describes the online process only. Refer to the latest Cisco documentation for the file-based method.

When you enroll for a personal certificate, either you go through a CA from which your system already has a root certificate or you obtain a root certificate from the CA as part of the enrollment process. The Certificates tab displays the current list of CA certificates. In the example, no certificates are displayed in the certificates panel.

To enroll online for a certificate with a CA over the network, follow this procedure:

- In advanced mode, either click the **Enroll** icon on the toolbar above the Certificates tab or choose the Certificates menu option, and then click **Enroll**.
- Click the **Online** radio button to select online as the certificate enrollment type. The VPN Client Certificate Enrollment window appears.
- In the VPN Client Certificate Enrollment form fill in the fields as follows:
  - **CA URL:** Enter the URL or network address of the CA. This parameter is required. In the example, 10.0.2.10 is the address of the CA server. The CA URL for our example Microsoft CA server is `http://10.0.2.10/certsrv/mscep/mscep.dll`.
  - **CA Domain:** Enter the CA domain name in this field. This parameter is required. In the example, the domain is `cisco.com`.
  - **Challenge Password:** Some CAs require a password to access their site. If such is the case with your CA, enter the password in the Challenge Password field. To find out the password, contact the CA or your network administrator. In the example, no password was required.
- Click the **Next** button. The Cisco VPN Client certificate enrollment form opens.

## Certificate-Based Client Authentication

### Task 1: Enroll Client (Cont.)

- Specify certificate attributes.

Enter certificate fields. \* indicates a required field.

Name (CN): David L.

Department (OU): training

Company (O): cisco

State (ST):

Country (C):

Email (E):

IP Address:

Domain:

Back Enroll Cancel

Enroll

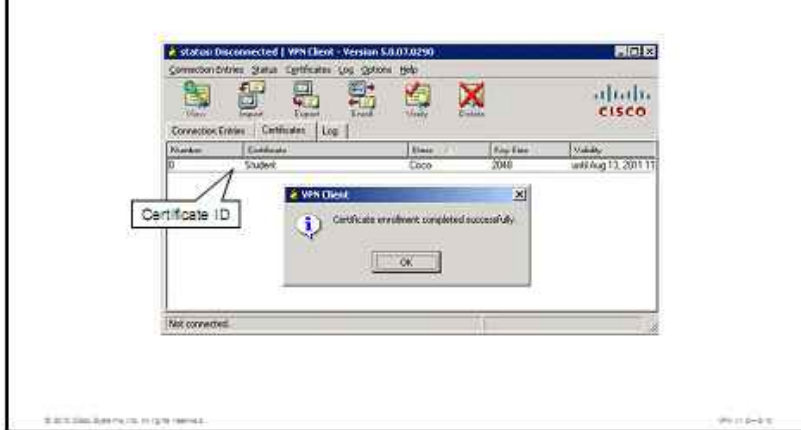
In the certificate enrollment form fields, you can fill the various attribute values to be included in the certificate as follows:

- **Name (CN):** Use your common name (CN in the certificate enrollment form), which is the unique name for this certificate. This field is required. The common name can be the name of a person, system, or other entity; it is the most specific level in the identification hierarchy. The common name becomes the name of the certificate, for example, David L.
- **Department (OU):** Use the name of the department to which you belong; for example, training. This field correlates to the organizational unit (OU in the certificate enrollment form). The organization unit is the same as the connection profile name configured on the security appliance, for example, training.
- **Company (O):** Use the name of the company or organization (O in the certificate enrollment form) to which you belong, for example, cisco.
- **State (ST):** Use the name of your state (ST in the certificate enrollment form), for example, Massachusetts.
- **Country (C):** Use the two-letter country code for your country (C in the certificate enrollment form), for example, US. This two-letter country code must conform to ISO 3166 country abbreviations.
- **Email (E):** Use your email address (E in the certificate enrollment form), for example, DL@training.cisco.com.
- **IP Address:** Use the IP address of your system, for example, 10.10.10.1.
- **Domain:** Use the fully qualified domain name (FQDN) of the host for your system.

Next, click the **Enroll** button. The SCEP enrollment process takes place.

## Certificate-Based Client Authentication

### Task 1: Enroll Client (Cont.)



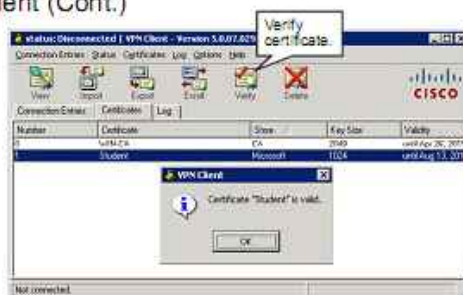
After you click the Enroll button, what happens next depends on the configuration of the CA. Either you will receive immediate approval or approval will be required.

- Some CAs provide 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 popup window.
- While you are waiting for the CA to issue the certificate, your request appears in the certificates list under the Certificates tab as a request. (The Store column shows Request.)
- When the CA issues your certificate, choose the certificate and then choose **Retry Certificate Enrollment** from the Certificates menu to complete the enrollment.
- After you have obtained the certificate, you see a message that your enrollment succeeded.
- In the example, only the identity certificate is visible, even though both the identity and CA certificates were downloaded. You can display both the CA and identity certificates by choosing **Certificates > Show CA/RA Certificates**.

## Certificate-Based Client Authentication

### Task 1: Enroll Client (Cont.)

- You can verify certificate validity.



Message	Description
Certificate is not valid yet.	Wait until the certificate becomes valid.
Certificate has expired.	Enroll for a new certificate.
Certificate signature is not valid.	Download or import the new CA certificate.
Certificate <name> is valid.	You have a working certificate enrolled.

To verify whether a certificate is valid or not, follow these steps.

- Step 1** Choose the certificate from the certificate store under the Certificates tab.
- Step 2** Display the Certificates menu, and choose **Verify** or click the **Verify** icon on the toolbar above the Certificates tab. The Cisco VPN Client displays a message indicating if the certificate is still valid.
- Step 3** Click **OK**.

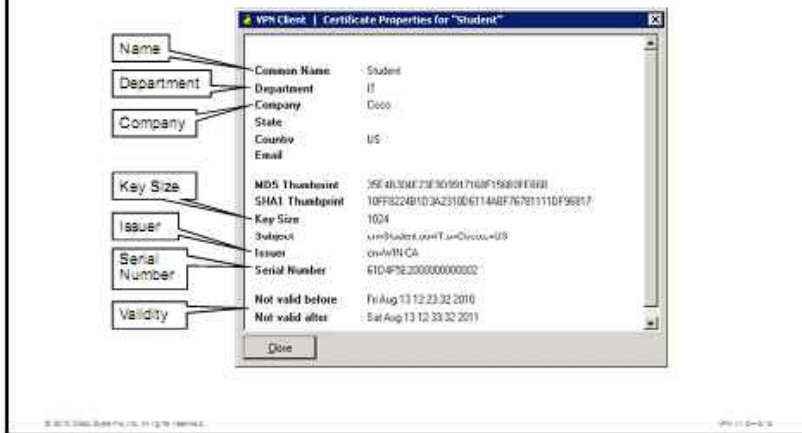
This table shows the messages that you might see when you check the validity of a certificate.

### Verification Messages

Message	Description
Certificate is not valid yet.	The current date is before the valid start date of the certificate. You must wait until the certificate becomes valid.
Certificate has expired.	The current date is after the valid end date of the certificate. You need to enroll for a new certificate.
Certificate signature is not valid.	You do not have the CA certificate, or the CA certificate that you have may have expired. You might need to download or import the CA certificate.
Certificate <name> is valid.	You have a working certificate enrolled.

## Certificate-Based Client Authentication

### Verification



To display a certificate, choose 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.

In the example is a sample certificate from a Microsoft certificate service provider. This is only an example. Not all certificates will look like this one.

A typical certificate, such as the certificate shown in the example, contains the following information.

- **Common Name:** The name of the owner, usually the first name and last name. This field identifies the owner within the public key infrastructure (PKI) organization).
- **Department:** The name of the department the owner is in, which is same as the organizational unit. Note that when you connect to a Cisco ASA adaptive security appliance, the organizational unit should generally match the group name that is configured for the owner in the Cisco ASA adaptive security appliance.
- **Company:** The organization where the owner is using the certificate.
- **State:** The state where the owner is using the certificate.
- **Country:** The two-character country code where the owner's system is located.
- **Email:** The email address of the owner of the certificate.
- **Thumbprint:** The Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) hash to the complete contents of the certificate. This identifier provides a way to validate the authenticity of the certificate. For example, if you contact the issuing CA, you can use this identifier to verify that this is the correct certificate to use.
- **Key Size:** The size of the signing key pair in bits; for example, 1024.

- **Subject:** The fully qualified distinguished name (DN) of the owner of the certificate. This specific example includes the following parts. Other items may be included, depending on the certificate type. However, these fields are fairly standard:
  - CN is the common name
  - OU is the organizational unit (department)
  - O is the organization
  - L is the locality (city or town)
  - ST is the state or province of the owner
  - C is the country, and e is the email address of the owner
- **Issuer:** The fully qualified domain name (FQDN) of the source that provided the certificate. The fields in this example are the same as for Subject.
- **Serial Number:** A unique identifier that is used for tracking the validity of the certificate on certificate revocation lists (CRLs).
- **Not Valid Before:** The beginning date that the certificate is valid.
- **Not Valid After:** The end date beyond which the certificate is no longer valid.

# Configuring Hybrid Authentication

This topic describes how to configure and verify Cisco Easy VPN hybrid authentication.

## Hybrid Authentication

### Overview

- In hybrid authentication, the Cisco ASA adaptive security appliance signs the exchange with a private RSA key:
  - Also called mutual group authentication
  - Eliminates the man-in-the-middle problem with compromised group passwords
  - Requires a CA certificate on the client
- Does not support self-signed certificates on the Cisco ASA adaptive security appliance

The diagram illustrates the hybrid authentication process between a Cisco VPN Client and a Cisco ASA. On the left, the Cisco VPN Client provides a Username Password and a Group Name Password. On the right, the Cisco ASA provides a Group Name Password and an Identity Certificate. The process involves three main steps: 1. The Cisco VPN Client sends 'Authenticate as User (XAUTH)' to the Cisco ASA. 2. The Cisco ASA sends 'Authenticate as Group' to the Cisco VPN Client. 3. The Cisco ASA sends 'Sign' to the Cisco VPN Client, which then sends 'Verify' back to the Cisco ASA. The Cisco VPN Client also has a Root CA Certificate, and the Cisco ASA has an Identity Certificate.

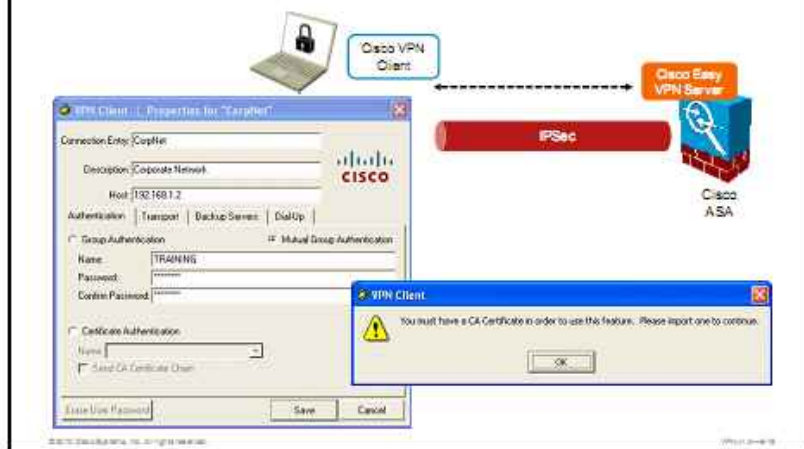
Group password authentication is a method that uses pre-shared keys (PSKs) for mutual authentication of the client and the Cisco ASA adaptive security appliance. In this method, the VPN Client and the VPN central-site device use a group name and password to validate the connection. This is a symmetrical form of authentication since both sides use the same authentication method during their negotiations.

Mutual group authentication is asymmetrical in that each side uses a different method to authenticate the other. In this method, authentication happens in two stages. During the first stage, the Cisco ASA adaptive security appliance initially authenticates the client peer using a group password. The client then authenticates the Cisco ASA adaptive security appliance using a group password, but this exchange is additionally digitally signed by a credential that is only available to the Cisco ASA adaptive security appliance—a Rivest, Shamir, and Adleman (RSA) private key. For the client to verify this digital signature, the Cisco ASA adaptive security appliance sends its identity certificate (containing the public key that corresponds to the signing private key). Then the client verifies the identity certificate of the Cisco ASA adaptive security appliance using a locally available copy of the certificate authority (CA) certificate, extracts the public key of the Cisco ASA adaptive security appliance from the identity certificate of the Cisco ASA adaptive security appliance, and verifies the digital signature in the initial authentication. Because only the Cisco ASA adaptive security appliance possesses the private RSA key, no attacker compromising the group password can spoof the identity of the Cisco ASA adaptive security appliance.



## Hybrid Authentication

### CA Certificate on Client



To use hybrid authentication (or mutual group authentication, as it is often called), the Cisco VPN Client system for the remote user must have the relevant CA certificate installed. If needed, you can install a CA certificate automatically by installing it on the Cisco VPN Client system during installation. The CA certificate must be in a file named "rootcert," with no extension, and must be placed in the installation directory for the Cisco VPN Client system of the remote user. For more information about loading a CA certificate, see the installation instructions in the user guide for the remote user's platform.

---

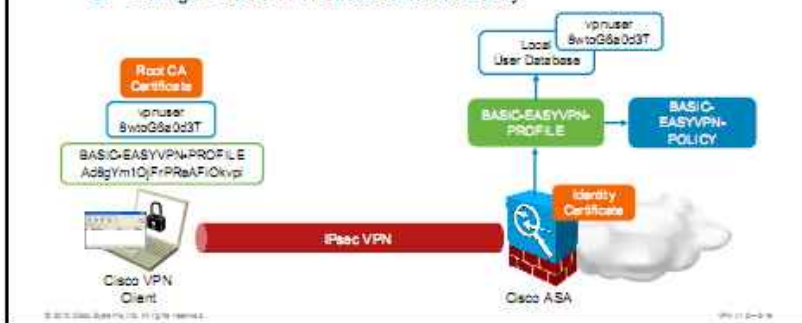
**Note** The hybrid authentication method does not support self-signed identity certificates for the Cisco ASA adaptive security appliance. The Cisco ASA adaptive security appliance must have a certificate that is signed by some other entity (typically a public key infrastructure (PKI) CA).

---

## Configuring Hybrid Authentication

### Configuration Tasks

1. Enroll the Cisco ASA into a PKI (same as site-to-site).
  - Client does not enroll to PKI.
2. Enable mutual authentication in connection profile.
3. Configure Cisco VPN Client connection entry.



To configure hybrid authentication for a connection profile, you will need to perform the following configuration tasks:

1. Enroll the Cisco ASA adaptive security appliance into a PKI to obtain the identity certificate of the Cisco ASA adaptive security appliance. Configuration guidance for this task is not part of this lesson because you have already learned to perform this task in previous lessons.

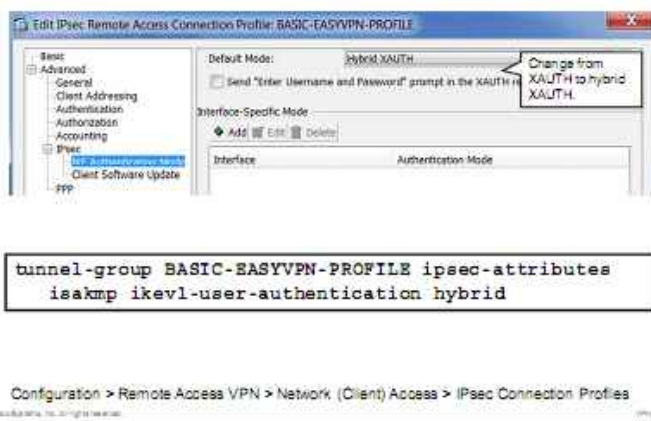
The client will be able to verify the identity certificate of the Cisco ASA adaptive security appliance by having a local, authentic copy of the relevant CA certificate.

2. Enable hybrid authentication in a specific connection profile.
3. Configure VPN Client connection entry

This figure presents the configuration scenario that is used in upcoming configuration tasks. The Cisco ASA adaptive security appliance is already configured with a local user in the user database, and the Cisco Easy VPN connection profile (BASIC-EASYVPN-PROFILE) and the custom group policy (BASIC-EASYVPN-POLICY).

## Configuring Hybrid Authentication

### Task 2: Enable Hybrid Authentication for a Profile



After installing the identity certificate of the Cisco ASA adaptive security appliance, you enable hybrid authentication in the connection profile or profiles that you want to use in the Cisco Easy VPN solution.

Perform the following steps:

- Step 1** In Cisco Adaptive Security Device Manager (Cisco ASDM), navigate to **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**, and click **Edit** to edit the relevant connection profile.
- Step 1** In the Edit IPsec Remote Access Connection Profile window, choose **Advanced > IPsec > IKE Authentication Mode** in the pane on the left.
- Step 2** Choose **Hybrid XAUTH** in the Default Mode drop-down box.
- Step 3** Click **OK** and **Apply** and, optionally, click **Save** to save your configuration.

The resulting CLI configuration is shown in the figure here. It includes the **isakmp ikev1-user-authentication hybrid** command in group-policy ipsec-attributes mode.

### isakmp ikev1-user-authentication

To configure hybrid authentication during Internet Key Exchange (IKE), use the **isakmp ikev1-user-authentication** command in tunnel-group ipsec-attributes configuration mode. To disable hybrid authentication, use the **no** form of this command.

```
isakmp ikev1-user-authentication [interface] {none | xauth | hybrid}
```

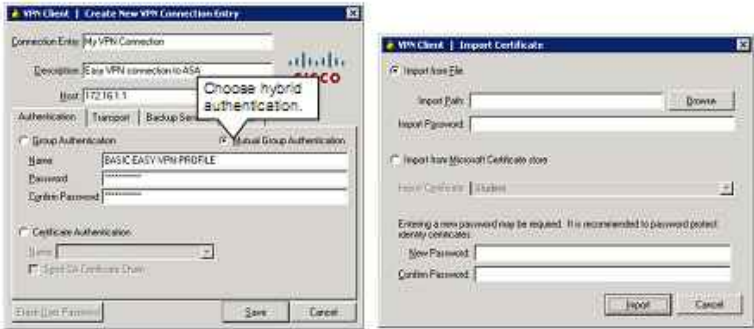
## isakmp ikev1-user-authentication Parameters

Parameter	Description
<code>interface</code>	(Optional) Specifies the interface on which the user authentication method is configured
<code>none</code>	Disables user authentication during IKE
<code>xauth</code>	Specifies XAUTH, also called extended user authentication
<code>hybrid</code>	Specifies hybrid XAUTH authentication during IKE

### Configuring Hybrid Authentication

Task 3: Configure Cisco VPN Client Connection Entry

- VPN server > Group name > Group password
- Select and import the CA certificate from a file



© 2010 Cisco Systems, Inc. All rights reserved. VPN v1.0-10

Perform the following steps on the Cisco VPN Client:

- Step 1** Start the Cisco VPN Client.
- Step 2** In the Cisco VPN Client main window, click the **New** button to create a new connection entry.
- Step 3** Specify a local name for the connection entry (“My VPN Connection” in this figure), and optionally add a description.
- Step 4** In the Host field, specify the IP address of the Cisco ASA adaptive security appliance VPN-terminating interface.
- Step 5** In the Authentication tab, click the **Mutual Group Authentication** radio button to select the mutual group authentication method.
- Step 6** At this point, the Cisco VPN Client will prompt you to import a CA certificate into the Cisco VPN Client certificate store. Provide a path to the file where you have stored the CA certificate (obtained from the PKI administrator), and click **Import**.
- Step 7** Enter the group name and password. The group name must correspond to the name of the connection profile that is configured on the Cisco ASA adaptive security appliance (“BASIC-EASYVPN-PROFILE” in this figure). The key must match the PSK that is configured in the connection profile on the Cisco ASA adaptive security appliance.
- Step 8** Click **Save** to save the profile.

# Deploying Advanced PKI Integration

This topic describes how to configure and verify integration with supporting PKI entities.

## Configuring Advanced PKI Integration

### Overview

- VPN gateway must provide a revocation method to reduce risk of compromised credentials:
  - CRLs
  - OCSP
  - AAA authorization
- VPN gateway may need to provide AAA per-user settings server for certificate users.



In some cases of certificate-based client authentication, advanced integration with existing PKI is needed. Advanced PKI integration includes configuring a revocation method to reduce a risk of compromised certificates. Certificates are considered compromised when a certificate was issued improperly by a CA or a private-key matching a public-key on the certificate is thought to be compromised. For example, if a laptop that stores a certificate and a matching private-key is lost, the certificate should be revoked. Another example would be revocation of certificates belonging to users that are not employed in an organization any more.

The certificate revocation method can be implemented in the following ways:

- **Configuring certificate revocation lists (CRLs):** A CRL is a list of the serial numbers of certificates that have been revoked and are no longer valid. A CRL is generated and published by the CA, which issues corresponding certificates and is updated periodically or immediately after a certificate has been revoked. You can configure the Cisco ASA adaptive security appliance to make CRL checks mandatory when authenticating a certificate. The Cisco ASA adaptive security appliance needs a CRL location to verify client certificates. A CRL location can be found in CRL distribution point (CDP) specified in an identity certificate. The Cisco ASA adaptive security appliance can download a CRL using HTTP, Lightweight Directory Access Protocol (LDAP), or Simple Certificate Enrollment Protocol (SCEP).
- **Configuring Online Certificate Status Protocol (OCSP):** OCSP is a protocol for obtaining the revocation status of digital certificates. OCSP messages are usually communicated over HTTP. You can configure the Cisco ASA adaptive security appliance to make OCSP checks mandatory when authenticating a certificate. The location of the OCSP server on the Cisco ASA adaptive security appliance can be configured as an OCSP URL that is defined in the match certificate rule, as a statically configured OCSP URL, or it can be specified in the Authority Information Access (AIA) field of the authenticating certificate.

---

**Note** The OCSP server is now termed the OCSP *responder*.

---

- **Configuring authentication, authorization, and accounting (AAA) authorization of the user certificate:** You can also revoke user authorization by deploying an external RADIUS server. When the Cisco ASA adaptive security appliance receives the certificate of a user, it sends a predefined field from the certificate as a username and predefined (common to all users) password to the RADIUS server, which authorizes the user. On the RADIUS server, users with a proper username (which matches a predefined field in the certificate of the user) and password have to be configured. If you want to revoke user authorization, you have to delete or disable a user account that corresponds to the certificate you want to revoke.

## Configuring Advanced PKI Integration

### Configuration Tasks

1. (Optional) Configure a certificate revocation checking policy.
2. (Optional) Configure AAA authorization revocation.

You should complete these tasks when you configure advanced PKI integration:

1. Optionally, configure a certificate revocation checking policy.
2. Optionally, configure AAA user authorization based on certificate identity.

## Configuring Advanced PKI Integration

### Configuration Choices

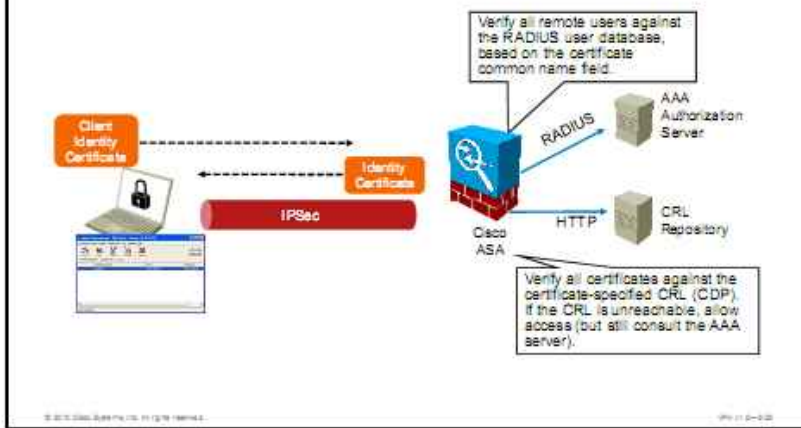
Revocation Method	Criteria
CRL	Use this method if other methods are not available.
OCSP	Use this method if you have an OCSP server available and cannot use AAA.
AAA	Use this method if you have an AAA server available. Use it if you need to also assign AAA per-user or per-group attributes (IP addresses, ACLs, and so on).

When deploying advanced PKI integration, you have various deployment options:

- **Use CRL as the certificate revocation method:** Use if other methods are not available.
- **Use OCSP as the certificate revocation method:** Use when you have an OCSP server (responder) available and the AAA server is not available.
- **Use AAA as the certificate revocation method:** Use when you have an AAA server available and you have to provide per-user or per-group attributes, such as IP addresses, downloadable access lists, and so on.

## Configuring Advanced PKI Integration

### Configuration Scenario

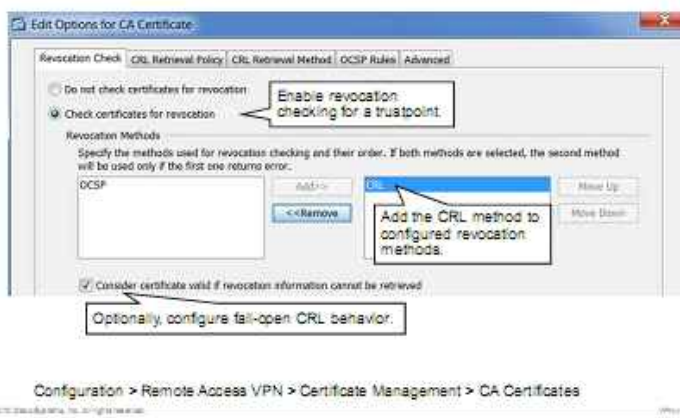


The figure presents an example, which will serve as configuration scenario for ongoing configuration tasks. You will configure the Cisco ASA adaptive security appliance to verify received certificates against the certificate-specified CRL (CDP) using the HTTP-based CRL retrieval method. If the CRL is unreachable, you will allow access, because you will also configure certificate authorization against the RADIUS server. Certificate authorization should be based on the certificate common name field. This example uses Cisco Secure Access Control Server (ACS) as the AAA authorization server.



## Configuring Advanced PKI Integration

### Task 1: Configure Revocation Checking Policy

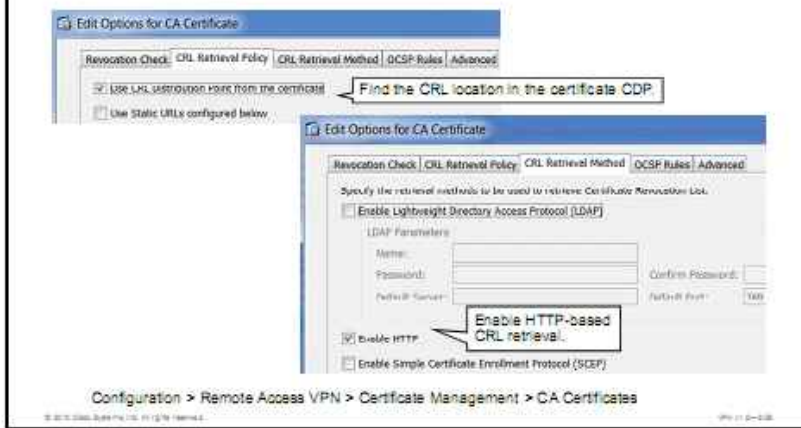


To configure a certificate revocation checking policy using Cisco ASDM, complete the following configuration steps:

- Step 1** From Cisco ASDM, choose **Configuration > Remote Access VPN > Certificate Management > CA Certificates**. The CA Certificates pane appears (not shown in the figure).
- Step 2** Choose the CA certificate that is used to verify client certificates. Click **Edit**. The Edit Options for CA Certificate window appears.
- Step 3** Verify that the Check Certificates for Revocation radio button is selected.
- Step 4** In the Revocation Method area of the window, click **CRL** and click the Add button.
- Step 5** To enable fail-open operations, check the **Consider Certificate Valid if Revocation Checking Returns Errors** check box to consider the certificate as valid if the revocation information cannot be retrieved (for instance, if the CRL distribution point is unreachable).

## Configuring Advanced PKI Integration

### Task 1: Configure Revocation Checking Policy (Cont.)



- Step 1** Click the **CRL Retrieval Policy** tab in the Edit Options for CA Certificate window.
- Step 2** Verify that the Use CRL Distribution Point from the Certificate check box is checked to direct revocation checking to the CRL distribution point from the certificate that is being checked.
- Step 3** Click the **CRL Retrieval Method** tab in the Edit Options for CA Certificate window.
- Step 4** To enable HTTP-based CRL retrieval, verify that the Enable HTTP check box is checked and that all others are unchecked.
- Step 5** Click **OK** in the Edit Options for CA Certificate window.
- Step 6** Click **Apply** to apply the configuration.

## Configuring Advanced PKI Integration

### Task 2: (Optional) Configure AAA Certificate Authorization

Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

To configure authorization using RADIUS, configure a new AAA server or edit an existing one by completing these steps:

---

**Note** This configuration example uses an existing server group and an existing server in that server group.

---

- Step 1** Choose a configured RADIUS server group from the AAA Server Groups table in the AAA Server Groups pane (not shown in the figure).
- Step 2** Choose a configured RADIUS server in the Servers in Selected Group area of the AAA Server Groups pane (not shown in the figure). Click **Edit**. The Edit AAA Server window appears.
- Step 3** Enter a common password into the Common Password field. This password will be sent, together with a username that is extracted from a certificate, to the RADIUS server as the credentials of the user.

---

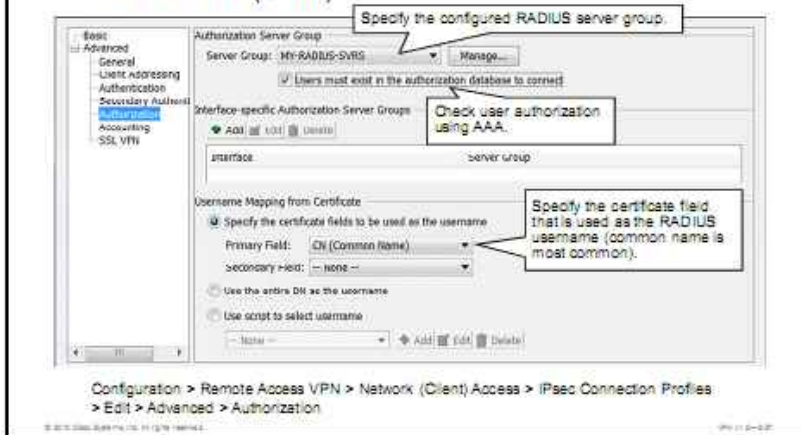
**Note** The Cisco ASA adaptive security appliance will use the same common password for all users when it authorizes certificates for them.

---

- Step 4** Click **OK**.
- Step 5** Click **Apply** to apply the configuration.

## Configuring Advanced PKI Integration

### Task 2: (Optional) Configure AAA Certificate Authorization (Cont.)



After you have configured common password for a RADIUS server, edit a connection profile to enable certificate authorization using AAA. Complete the following steps:

- Step 1** From the Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles**. Select a connection profile and click **Edit** (not shown in the example).
- Step 2** Choose **Advanced > Authorization** from the menu on the left (not shown in the example).
- Step 3** Choose a previously configured AAA server group from the Server Group drop-down menu. In the example, the MY-RADIUS-SVRS server group is selected.
- Step 4** Check the **Users Must Exist in the Authorization Database to Connect** check box.
- Step 5** Verify that the **Specify the Certificate Fields To Be Used as the Username** radio button is selected.
- Step 6** Choose **CN (Common Name)** from the Primary Field drop-down menu. That choice means that the common name field will be extracted from a certificate and sent to the AAA server as the username.

---

**Note** Recall that the previously configured common password is sent together with a username to the AAA server.

---

- Step 7** Click **OK** and **Apply** to apply the configuration.

## Configuring Advanced PKI Integration

### Task 2: (Optional) Configure AAA Certificate Authorization (Cont.)

The screenshot shows the 'User Setup' form in Cisco Secure ACS. It is divided into three main sections:

- User Setup:** Contains a 'User' field with the value 'certuser (New User)'. A callout box points to this field with the text: 'On the RADIUS server, create a new user whose identity is determined by the configured certificate field.'
- Supplementary User Info:** Contains a checkbox for 'Account Disabled' (checked). A callout box points to it with the text: 'By enabling or disabling this account, you can achieve OOSP-like functionality.'
- Password Authentication:** Contains a dropdown menu for 'Authentication' (set to 'ACS Internal Database'), a 'CostSecure PAP (Also used for CHAP/RM-CHAP/ARAP, if the separate field is not checked.)' checkbox, and 'Password' and 'Confirm Password' fields, both containing masked characters. A callout box points to these fields with the text: 'Configure the common password.'

At the bottom of the form, there are small text elements: '© 2010 Cisco Systems, Inc.' on the left and '0001-0-00' on the right.

To configure users on the RADIUS server, complete the following steps:

- Step 1** On the Cisco Secure ACS, navigate to **User Setup** (not shown in the figure).
- Step 2** Enter a username into the User field and click **Add/Edit** (not shown in the example). This username has to match a certificate field that will be used by the Cisco ASA adaptive security appliance as a username. In our example, the common name field of a certificate has been configured as a username.
- Step 3** Enter the password that has been previously configured as a common password for the RADIUS server, into the Password and Confirm Password fields.
- Step 4** Optionally, control the user authorization revocation by enabling or disabling the **Account Disabled** check box. In the example, the account is enabled and certificate authorization will be successful.
- Step 5** Click **Submit**.
- Step 6** Repeat the preceding steps to add all users that need authorization.

## Configuring Advanced PKI Integration

### CLI Configuration

```
crypto ca trustpoint MY-CA
revocation-check crl none
crl configure
  protocol http
  no protocol scep
  no protocol ldap
}
aaa-server MY-RADIUS-SVRS (inside) host 10.0.0.11
radius-common-pw *****
}
tunnel-group BASIC-EASYVPN-PROFILE general-attributes
authorization-required
username-from-certificate CN
authorization-server-group MY-RADIUS-SVRS
```

Enable CRL checking.

Use HTTP as CRL retrieval method.

Configure a common password for a RADIUS server.

Enable AAA certificate authorization.

To configure the advanced PKI integration using the CLI, use the following commands. To enable CRL checking when the Cisco ASA adaptive security appliance authenticates a certificate, first enter trustpoint configuration mode using the **crypto ca trustpoint** command. Use the **revocation-check crl** command to enable certificate revocation checking using CRL. The **none** keyword instructs the Cisco ASA adaptive security appliance to interpret the certificate status as valid, even if the CRL method returns an error (for example, server down, as opposed to finding the status as revoked). Then use the **crl configure** command to enter CRL configuration mode. Use the **protocol http** command to specify HTTP as the permitted method for retrieving a CRL. Use the **no protocol scep** and **no protocol ldap** commands to disable all other methods for retrieving a CRL.

To configure certificate authorization, first enter AAA server configuration mode using the **aaa-server** command and specify the common password using the **radius-common-pw** command. Then enter a connection profile (tunnel group) configuration mode using the **tunnel-group** command, followed by the connection profile name and **general-attributes** keyword. Use the **authorization-required** command to require the authorization of the user. Use the **username-from-certificate** command to specify a field in a certificate to use as the username for authorization. Use the **authorization-server-group** command to specify which AAA server group will be used for authorization of certificates.

### crypto ca trustpoint

To enter trustpoint configuration mode for the specified trustpoint, use the **crypto ca trustpoint** command in global configuration mode. To remove the specified trustpoint, use the **no** form of this command.

**crypto ca trustpoint** *trustpoint-name*

**no crypto ca trustpoint** *trustpoint-name* [**noconfirm**]

## crypto ca trustpoint Parameters

Parameter	Description
<code>trustpoint-name</code>	Identifies the name of the trustpoint to manage. The maximum name length is 128 characters.
<code>noconfirm</code>	Suppresses all interactive prompting.

### revocation-check

To set one or more methods for revocation checking, use the **revocation-check** command in `crypto ca trustpoint` mode. The adaptive security appliance tries the methods in the order that you configure them, trying the second and third methods only if the previous method returns an error (for example, server down), as opposed to finding the status as revoked.

You can set a revocation checking method in the client certificate validating trustpoint and also configure no revocation checking (**revocation-check none**) in the responder certificate validating trustpoint. The **match certificate** command documentation includes a step-by-step configuration example.

To restore the default revocation checking method, which is none, use the **no** version of this command.

```
revocation-check {[crl] [none] [ocsp]}
```

### revocation-check Parameters

Parameter	Description
<code>crl</code>	Specifies that the adaptive security appliance should use CRL as the revocation checking method
<code>none</code>	Specifies that the adaptive security appliance should interpret the certificate status as valid, even if all methods return an error
<code>ocsp</code>	Specifies that the adaptive security appliance should use OCSP as the revocation checking method

### crl configure

To enter CRL configuration mode, use the **crl configure** command in `crypto ca trustpoint` configuration mode.

```
crl configure
```

### protocol http

To specify HTTP as a permitted distribution point protocol for retrieving a CRL, use the **protocol http** command in CRL configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, or SCEP). To remove HTTP as the permitted method of CRL retrieval, use the **no** form of this command.

```
protocol http
```

### protocol ldap

To specify LDAP as a distribution point protocol for retrieving a CRL, use the **protocol ldap** command in CRL configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, or SCEP). To remove the LDAP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

```
protocol ldap
```

## protocol scep

To specify SCEP as a distribution point protocol for retrieving a CRL, use the **protocol scep** command in CRL configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, or SCEP). To remove the SCEP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

### protocol scep

## tunnel-group general-attributes

To enter general-attributes configuration mode, use the **tunnel-group general-attributes** command in global configuration mode. This mode is used to configure settings that are common to all supported tunneling protocols. To remove all general attributes, use the **no** form of this command.

### tunnel-group *name* general-attributes

#### tunnel-group general-attributes Parameters

Parameter	Description
<i>name</i>	Specifies the name of the tunnel-group
<b>general-attributes</b>	Specifies attributes for this tunnel-group

## username-from-certificate

To specify the field in a certificate to use as the username for authorization, use the **username-from-certificate** command in tunnel-group general-attributes mode. The DN of the peer certificate is used as the username for authorization. To remove the attribute from the configuration and restore default values, use the **no** form of this command.

### username-from-certificate {*primary-attr* [*secondary-attr*] **use-entire-name**}

#### username-from-certificate Parameters

Parameter	Description
<i>primary-attr</i>	Specifies the attribute to use to derive a username for an authorization query from a certificate. If pre-fill-username is enabled, the derived name can also be used in an authentication query.
<i>secondary-attr</i>	(Optional) Specifies an additional attribute to use with the primary attribute to derive a username for an authentication or authorization query from a digital certificate. If pre-fill-username is enabled, the derived name can also be used in an authentication query.
<b>use-entire-name</b>	Specifies that the adaptive security appliance must use the entire subject DN (RFC 1779) to derive a name for an authorization query from a digital certificate.

## authorization-required

To require users to authorize successfully before connecting, use the **authorization-required** command in various modes. To remove the attribute from the configuration, use the **no** form of this command.

### authorization-required



## authorization-server-group

To specify the set of authorization servers to use with Cisco WebVPN and email proxies, use the **authorization-server-group** command in various modes. To remove authorization servers from the configuration, use the **no** form of this command. The adaptive security appliance uses authorization to verify the level of access to network resources that users are permitted.

**authorization-server-group** *group\_tag*

### authorization-server-group Parameters

Parameter	Description
<i>group_tag</i>	Identifies the previously configured authorization server or group of servers. Use the <b>aaa-server</b> command to configure authorization servers.

### Configuring Advanced PKI Integration

Implementation Guidelines

- Deploy at least one method of revocation checking.
- With AAA authorization, use a very strong common password and ensure that these user accounts can only authenticate on VPN gateways.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Consider the following implementation guidelines when implementing advanced PKI integration:

- It is very important to verify certificate revocation. Deploy at least one method of revocation checking.
- With AAA authorization, use a very strong common password and ensure that these user accounts can only authenticate on VPN gateways.

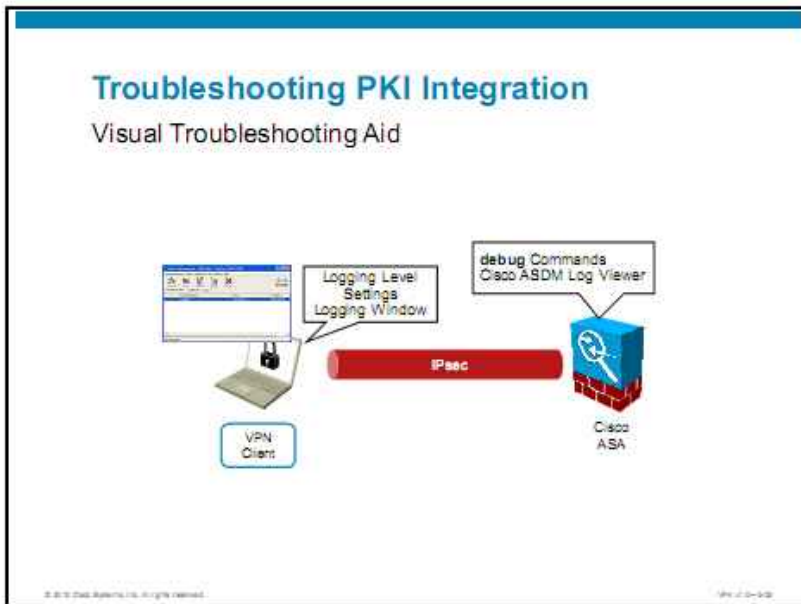
---

**Note** The RSA (formerly SDI) authentication server type cannot be used as the secondary username and password credential. It can only be used for primary authentication.

---

# Troubleshooting PKI Integration

This topic describes how to troubleshoot advanced client and server authentication in the Cisco Easy VPN solution.

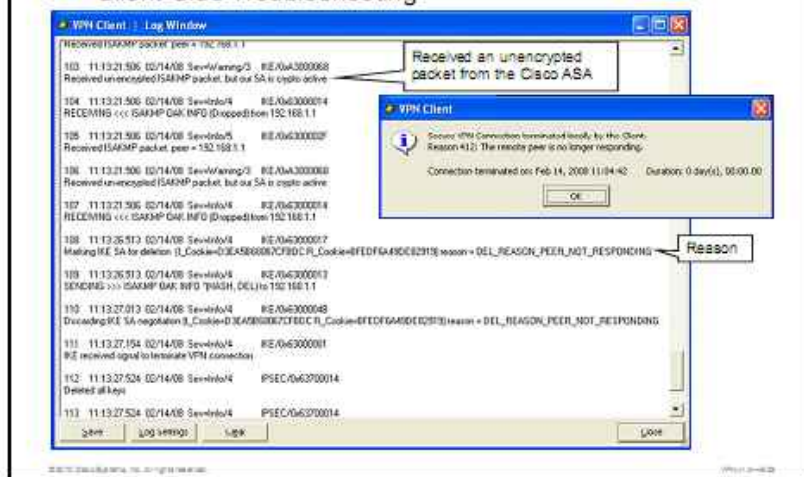


Several tools are available to troubleshoot remote-access VPNs when connectivity problems occur. When troubleshooting remote-access client connectivity issues, you will use a combination of the following:

- Cisco VPN Client logging-level settings
- Cisco VPN Client log window
- The **debug** commands
- Cisco ASA adaptive security appliance internal log buffer
- Cisco ASDM log window

## Troubleshooting PKI Integration

### Client-Side Troubleshooting



This figure shows the client error message and the log window of the client. The client error message shows that the security appliance is not responding. Notice that the client is actually responding but the client is receiving unencrypted packets from the Cisco ASA adaptive security appliance. This problem could be occurring for a number of reasons, but it does look like the problem is on the Cisco ASA adaptive security appliance side of the connection.

**Note** Logging in the Cisco VPN Client is not enabled by default. You can enable logging using the **Log > Enable** menu option.

Some reasons could include these:

- IKE Phase 1 could not complete.
- IKE Phase 2 could not complete.
- Crypto map on the Cisco ASA adaptive security appliance may be misconfigured.
- Tunnel group may be misconfigured.
- Certificate to connection profile policy may be incorrect.

The next thing to do would be to set up a syslog server, configure logging on the Cisco ASA adaptive security appliance, and enable the appropriate **debug** commands. The next section takes you through this process.

## Troubleshooting PKI Integration

### Server-Side Troubleshooting

#### Syslog output

```
15:10:03 Local7.Debug 10.0.1.1 %ASA-7-713906: Group = DefaultRAGroup, IP = 192.168.1.6, sending delete/delete with reason message
15:10:03 Local7.Debug 10.0.1.1 %ASA-7-713906: Group = DefaultRAGroup, IP = 192.168.1.6, IKE SA MM1c3d6e151 terminating: flags 0x0105c002,
15:10:03 Local7.Error 10.0.1.1 %ASA-3-713226: Connection failed with peer '192.168.1.6', no trust-point defined for tunnel-group 'DefaultRAGroup'
15:10:03 Local7.Info 10.0.1.1 %ASA-6-713905: Group = DefaultRAGroup, IP = 192.168.1.6, No valid authentication type found for the tunnel group
15:10:03 Local7.Debug 10.0.1.1 %ASA-7-713906: IP = 192.168.1.6, Connection landed on tunnel_group DefaultRAGroup
15:10:03 Local7.Debug 10.0.1.1 %ASA-7-713906: IP = 192.168.1.6, Trying to find group via default group...
15:10:03 Local7.Debug 10.0.1.1 %ASA-7-713906: IP = 192.168.1.6, Trying to find group via IP ADDR...
15:10:03 Local7.Error 10.0.1.1 %ASA-3-713020: IP = 192.168.1.6, No Group found by matching OU(s) from ID payload: Unknown
15:10:03 Local7.Debug 10.0.1.1 %ASA-7-713906: IP = 192.168.1.6, Trying to find group via IKE ID...
15:10:03 Local7.Error 10.0.1.1 %ASA-3-713020: IP = 192.168.1.6, No Group found by matching OU(s) from ID payload: Unknown
```

The figure displays the messages that are sent to the syslog server from the Cisco ASA adaptive security appliance. The error occurs as follows:

1. The Cisco ASA adaptive security appliance is trying to match a group with the incoming IPsec request.
2. The connection lands on the default remote access group.
3. The Cisco ASA adaptive security appliance finds that there is no valid authentication type found for the tunnel group.
4. There is no trustpoint defined for the default tunnel group.

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- The Cisco Easy VPN solution supports two types of advanced authentication methods: mutual group authentication and certificate authentication.
- Before installing the identity certificate on the Cisco ASA adaptive security appliance, install a CA certificate and enroll with the CA.
- There are two methods that you can use to set up Cisco VPN Client with digital certificates supported: online and file-based.
- To check certificates for revocation, you can use CRLs, OCSP, or an AAA server.
- To troubleshoot VPN connectivity, use these tools: Cisco VPN Client, **debug** commands, and the Cisco ASDM log window.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN12-68



# Deploying the Cisco ASA 5505 Adaptive Security Appliance as Cisco Easy VPN Remote

---

## Overview

Cisco Easy VPN Remote (also called the Cisco Easy VPN hardware client) enables companies with multiple sites to establish secure communications among them and share resources. A Cisco Easy VPN solution consists of a Cisco Easy VPN Server at the main site and Cisco Easy VPN Remote at the remote offices.

This lesson discusses the Cisco Easy VPN Remote and its modes of deployment. The lesson then presents how to configure the Cisco ASA 5505 Adaptive Security Appliance as a Cisco Easy VPN Client. The lesson concludes with a look at specific hardware client features and policies and how they are configured.

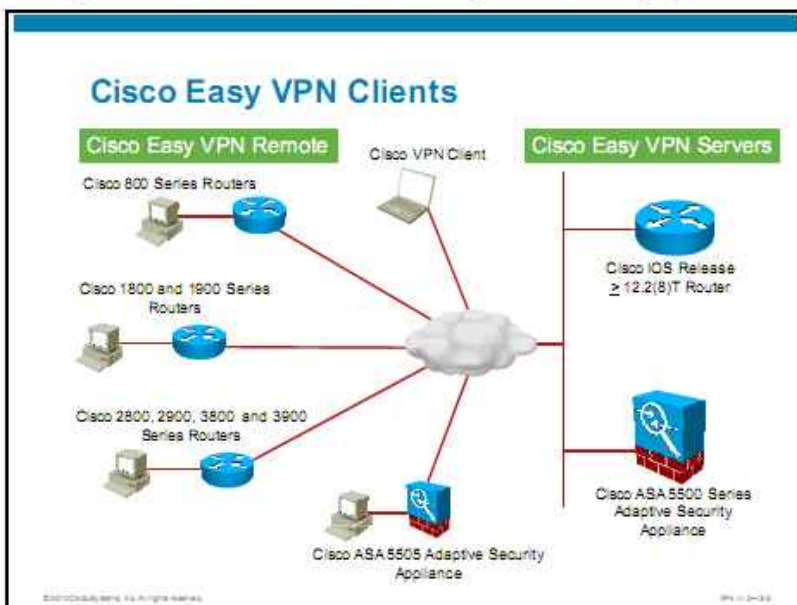
## Objectives

Upon completing this lesson, you will be able to deploy an advanced Cisco Easy VPN Remote setup to support a secure connection between remote and central offices. This ability includes being able to meet these objectives:

- Choose a Cisco Easy VPN Remote deployment mode
- Configure and verify a basic Cisco Easy VPN Remote profile
- Configure and verify advanced Cisco Easy VPN Remote features
- Troubleshoot Cisco Easy VPN Remote connections

# Choosing Cisco Easy VPN Remote Modes

This topic describes how to choose a Cisco Easy VPN Remote deployment mode.



The Cisco Easy VPN Remote feature enables Cisco security appliances and Cisco IOS routers to act as Cisco Easy VPN Clients. As such, these devices can receive security policies from a Cisco Easy VPN Server, minimizing virtual private network (VPN) configuration requirements at the remote location. This cost-effective solution is ideal for remote offices with little IT support or large customer premises equipment (CPE) deployments where it is impractical to individually configure multiple remote devices. This feature makes VPN configuration as easy as entering a password, which increases productivity and lowers costs as the need for local IT support is minimized.

The following Cisco products can act as Cisco Easy VPN Remote:

- Cisco VPN Client Version 3.x or later
- Cisco ASA 5505 Adaptive Security Appliance
- Cisco integrated services routers (ISRs):
  - Cisco 800 Series Routers and 1800 and 1900 Series Integrated Services Routers
  - Cisco 2800, 2900, 3800, and 3900 Series Integrated Services Routers

---

**Note** See Cisco.com for the latest listing of Cisco Easy VPN Remote devices and software clients.

---



## Cisco Easy VPN Remote

### Remote Modes of Operation

- Client mode:
  - Specifies the use of NAT or PAT
  - Enables the client to automatically configure NAT or PAT translations and the ACLs that are needed to implement the VPN tunnel
  - Supports split tunneling
- Network extension mode:
  - Specifies that the hosts at the client end of the VPN connection use fully routable IP addresses
  - NAT or PAT is not used
  - Supports split tunneling

The Cisco Easy VPN Remote feature supports two modes of operation:

- **Client mode:** Client mode is also called Port Address Translation (PAT) or Network Address Translation (NAT) mode. It isolates the IP address of the Cisco Easy VPN Remote client private network from those of the enterprise network. IP address management is not required for the inside interface or inside host. The Cisco Easy VPN Remote feature automatically configures the PAT translation and access control lists (ACLs) that are needed to implement the VPN connection. These configurations are automatically created when the VPN connection is initiated. When the tunnel is torn down, PAT translations and the ACL configurations are automatically deleted.

---

**Note** The PAT translation and ACL configurations that are created by the Cisco Easy VPN Remote feature are not written to either the startup configuration or running configuration files. However, you can display these configurations in Cisco routers using the **show ip nat statistics** and **show access-list** commands.

---

- **Network extension mode:** This mode specifies that the PCs and other hosts at the client end of the IP Security (IPsec) tunnel be given IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the PCs and hosts on the destination network.

Both modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the IPsec tunnel while also allowing Internet access through a connection to an ISP or other service. Split tunneling eliminates the corporate network from the path for Internet access.

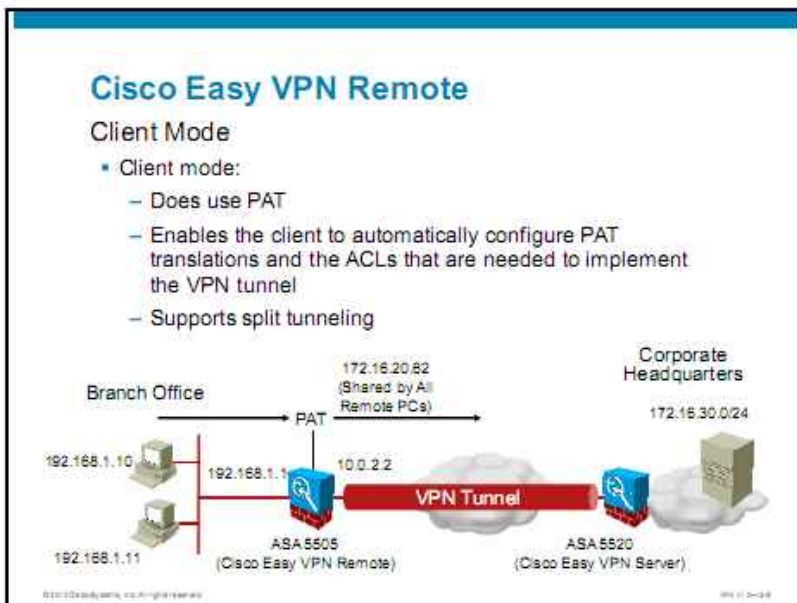
Cisco Easy VPN Remote supports interoperability with NAT. You can have a NAT configuration and a Cisco Easy VPN Remote configuration that coexist. When an IPsec VPN connection is down, the NAT configuration works.

In the Cisco Easy VPN Remote feature, the server automatically restores the previous NAT configuration when the IPsec VPN tunnel is torn down. The user-defined access lists are not disturbed. Users can continue to access nontunnel areas of the Internet when the tunnel times out or disconnects.

---

**Note** NAT interoperability is not supported in client mode with split tunneling enabled.

---



Use client mode if you want to deploy a VPN quickly and easily in a small office, home office (SOHO). If you do not need to see devices that might reside behind a VPN hardware client and ease of use and installation is essential, you should implement client mode. In client mode, a VPN hardware client, such as the Cisco ASA 5505 Adaptive Security Appliance, uses PAT to isolate its private network from the public network. SOHO PCs behind the hardware client are invisible to the outside network. PAT causes all traffic from the SOHO PCs to appear on the private network as a single-source IP address.

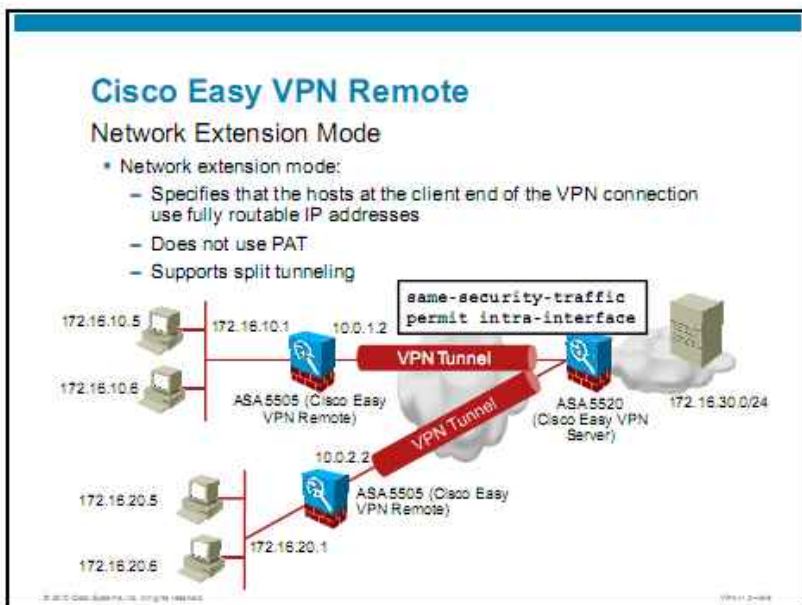
In client mode, the IP addresses of the Cisco Easy VPN Remote client private network are isolated from those of the enterprise network. IP address management is not required for the inside interface or inside host. The Cisco Easy VPN Remote feature automatically configures the PAT translation and access control lists (ACLs) that are needed to implement the VPN connection. These configurations are automatically created when the VPN connection is initiated. When the tunnel is torn down, PAT translations and the ACL configurations are automatically deleted.

---

**Note** The PAT translation and ACL configurations that are created by the Cisco Easy VPN Remote feature are not written to either the startup configuration or running configuration files. However, you can display these configurations in Cisco routers by using the **show ip nat statistics**, **show access-list**, or **show vpnclient detail** commands.

---

The figure illustrates the Cisco Easy VPN Remote client mode of operation. In this example, the Cisco ASA 5505 Adaptive Security Appliance provides access to two PCs, which have IP addresses in the 192.168.1.0 private network space. These PCs connect to the Ethernet interface on the Cisco ASA 5505 Adaptive Security Appliance. The two PC IP addresses are translated to the Cisco ASA 5505 Adaptive Security Appliance Easy Remote IP address 172.16.20.62. The Cisco ASA 5505 Adaptive Security Appliance performs PAT translation over the IPsec tunnel so that the PCs can access the destination network. If split tunneling is enabled, any traffic that is bound for networks on the outside interface and also not bound for the IPsec tunnel would be translated to the IP addresses that are found in the global pool or translated to the outside interface IP address of 10.0.2.2.



In network extension mode, all SOHO PCs that are connected to the Cisco Easy VPN remote device are uniquely addressable via the tunnel. This setup allows direct connections between hosts that are behind the Cisco Easy VPN Remote device and hosts that are behind the Cisco Easy VPN Server. The client hosts are given IP addresses that are fully routable by the destination network over the tunnel. These IP addresses can be either in the same subnet space as the destination network, or they can be in separate subnets, as long as the destination routers are configured to properly route those IP addresses over the tunnel. This setup provides a seamless extension of the remote network.

In network extension mode, the PCs and other hosts at the client end of the IPsec tunnel are given IP addresses that are fully routable and reachable by the destination network so that they form one logical network. Because PAT is not used, the client PCs and hosts have direct access to the PCs and hosts on the network of the headend.

This mode supports split tunneling, which allows secure access to corporate resources through the IPsec tunnel while also allowing Internet access through a connection to an ISP or other service—thereby eliminating the corporate network from the path for Internet access.

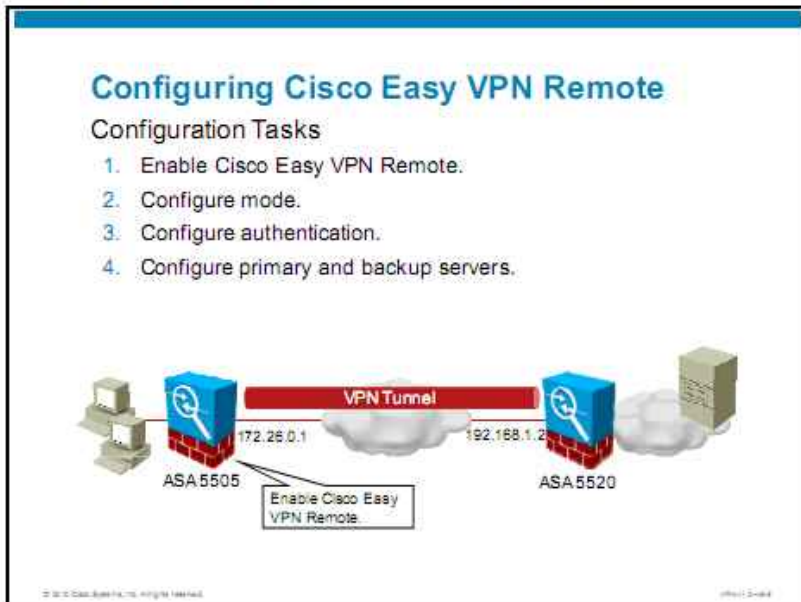
The figure illustrates the network extension mode of operation. In this example, the Cisco ASA 5505 Adaptive Security Appliance acts as Cisco Easy VPN Remote clients, connecting to the Cisco ASA 5520 Adaptive Security Appliance Cisco Easy VPN Server. Hosts at the branch offices can communicate directly with hosts on the corporate network. Hosts at corporate headquarters can also communicate directly with hosts at the branch offices. This ability enables central-site management information system personnel to directly address devices that are behind the Cisco ASA 5505 Adaptive Security Appliance over IPsec tunnels.

The client hosts are given IP addresses that are fully routable by the destination network over the tunnel. These IP addresses could be either in the same subnet space as the destination network, or they could be in separate subnets, as long as the destination routers are configured to properly route those IP addresses over the tunnel. This ability provides a seamless extension of the remote network.

By default, the Cisco ASA adaptive security appliance will not forward packets that arrive at a specific interface back via the same interface. You can disable this behavior using the **same-security-traffic permit intra-interface** command. By allowing the VPN “hairpinning” in this scenario, this configuration supports a hub-and-spoke VPN, with the VPN spokes connecting through a security appliance that is acting as a VPN hub.

# Deploying a Basic Cisco Easy VPN Remote Profile

This topic describes how to configure and verify a basic Cisco Easy VPN Remote profile.



Complete the following configuration tasks to configure Cisco Easy VPN Remote on the Cisco ASA 5505 Adaptive Security Appliance:

1. Enable Cisco Easy VPN Remote feature.
2. Configure the mode of operation.
3. Configure authentication.
4. Configure primary and backup servers.

The figure also shows a configuration scenario that will be used for ongoing configuration tasks. You will configure the Cisco Easy VPN Remote feature on the Cisco ASA 5505 Adaptive Security Appliance. You will use client mode of operation and authentication with digital certificate.

## Configuring Cisco Easy VPN Remote

### Task 1: Enable Cisco Easy VPN Remote



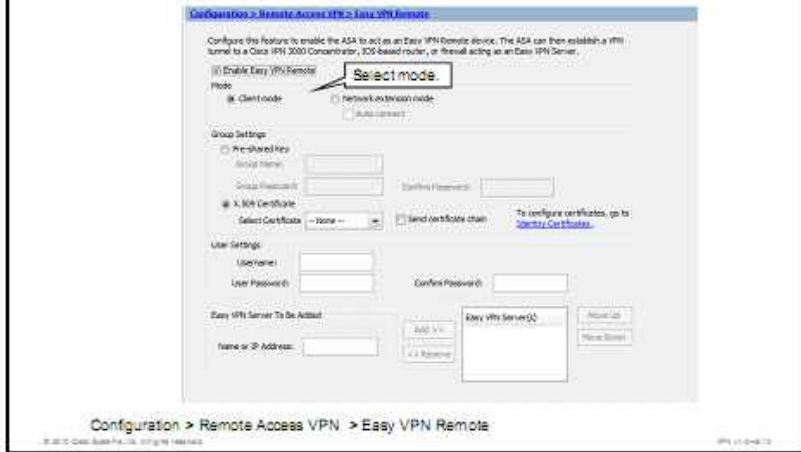
The Cisco ASA 5505 Adaptive Security Appliance is the only appliance within the Cisco ASA 5500 Series Adaptive Security Appliances that can be configured as a Cisco Easy VPN Remote. The Cisco ASA 5505 Adaptive Security Appliance can function as a Cisco Easy VPN Remote or as a server, but it cannot function in both of these modes at the same time. It does not have a default role for Cisco Easy VPN.

To configure the Cisco ASA 5505 Adaptive Security Appliance as a Cisco Easy VPN Remote, within Cisco Adaptive Security Device Manager (Cisco ASDM) for the Cisco ASA 5505 Adaptive Security Appliance, complete the following steps:

- Step 1** From Cisco ASDM, navigate to **Configuration > Remote Access VPN > Easy VPN Remote** (not shown in the example). The Easy VPN Remote pane appears.
- Step 2** Check the **Enable Easy VPN Remote** check box.

# Configuring Cisco Easy VPN Remote

## Task 2: Configure Mode



To configure the Cisco Easy VPN Remote mode of operation for the Cisco ASA 5505 Adaptive Security Appliance, complete the following step:

- Step 1** Within the Mode area of the Cisco Easy VPN Remote pane, click the radio button to choose **Client Mode** or **Network Extension Mode**. If Network Extension Mode is selected, the Auto Connect option becomes available. With this option, the Cisco Easy VPN Remote automatically initiates IPsec data tunnels to the Cisco Easy VPN Server when network extension mode and split tunnels are configured. In this example, client mode is chosen as the mode of operation.

IPsec data tunnels are automatically initiated and sustained when in network extension mode, except when split tunneling is configured. Automatic tunnel initiation is disabled if secure unit authentication (SUA) is enabled.

## Configuring Cisco Easy VPN Remote

### Task 3: Configure Authentication

#### IKE peer authentication

- Digital certificate
- Pre-shared key (PSK)

Select authentication type.

The screenshot shows the configuration interface for a Cisco Easy VPN Remote. The 'Group Settings' section is active, with the 'X.509 Certificate' radio button selected. Below this, there is a 'Select Certificate' dropdown menu and a 'Send certificate chain' checkbox. A callout box points to the 'X.509 Certificate' option with the text 'Select authentication type.'

Configuration > Remote Access VPN > Easy VPN Remote

When configuring the Cisco ASA 5505 Adaptive Security Appliance as a Cisco Easy VPN Remote, you can configure it to use a tunnel group password or a trustpoint for authentication, depending on the Cisco Easy VPN Server configuration. When you chose a tunnel group, the tunnel group name and its pre-shared key (PSK) that is configured on the Cisco Easy VPN Server are used as the group and password. If you choose trustpoint, you must configure the CA identity certificate and a device identity certificate. Certificate configuration can be found on the Certificate option of the Remote Access VPN menu. By default, if no tunnel group or trustpoint is configured, the Cisco Easy VPN Remote attempts to use Rivest, Shamir, and Adleman (RSA) certificates.

To configure the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote authentication, complete the following steps:

- Step 1** Within the Group Settings area of the Easy VPN Remote pane, click the radio button to choose **Pre-shared Key** or **x.509 Certificate**.
- Step 2** If you choose the Pre-shared Key option, the Group Name and Group Password options become available. The Group Name is the name of the VPN tunnel group that is configured on the Cisco Easy VPN Server. You must configure this tunnel group on the server before establishing a connection. The Group Password is the Internet Key Exchange (IKE) PSK that is used for authentication on the Cisco Easy VPN Server.
- Step 3** If you choose the X.509 Certificate option, the option to select a configured certificate is available from the Select Certificate drop-down list and Send Certificate Chain becomes available. A certificate chain is a sequence of certificates where the subsequent CA in the higher hierarchy signs each certificate. The last certificate in the chain is normally the self-signed certificate of the root CA.

In this example, the X.509 Certificate option is chosen, and a previously configured certificate is selected.



## Configuring Cisco Easy VPN Remote

### Task 4: Configure Primary and Backup Server

- Cisco ASA Cisco Easy VPN Remote can be configured for multiple servers.
- VPN connections are attempted based on the order of the list.
- The first server in the list is the primary.
- The remaining servers are backup servers.

The Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote can be configured for primary and secondary (backup) servers to provide it another way to the central site if the primary server becomes unavailable. The Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote can be configured for up to ten backup servers. VPN connections that are attempted to the servers are attempted in the order in which they are added to the configuration until a successful connection is made. The first server in the list is the primary server.

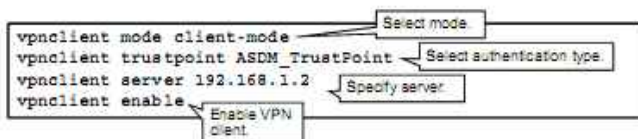
To configure primary and backup server for the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote, complete the following steps:

- Step 1** Within the Easy VPN Server to Be Added area of the Easy VPN Remote pane, enter a DNS name or an IP address in the Name or IP Address field.
- Step 2** Click the **Add** button.
- Step 3** Click **Apply** to apply the configuration.

In this example, the IP address of 192.168.1.2 was added as the primary server for the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote. After a VPN connection is initialized, any backup servers that are configured on the Cisco Easy VPN Server will be pushed to Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote.

## Configuring Cisco Easy VPN Remote

### CLI Configuration



To configure Cisco Easy VPN Remote on the Cisco ASA 5505 Adaptive Security Appliance using the command line interface (CLI), use the following commands. Use the **vpn mode client-mode** command to specify that the Cisco ASA adaptive security appliance will work in client mode. Use the **vpnclient trustpoint** command to enable authentication using digital certificates. Use the **vpnclient server** command to specify Cisco Easy VPN Servers. Finally, use the **vpnclient enable** command to enable Cisco Easy VPN Remote functionality.

### vpnclient mode

To configure the Cisco Easy VPN Remote connection for either client mode or network extension mode, use the **vpnclient mode** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

**vpnclient mode** {*client-mode* | *network-extension-mode*}

#### vpnclient mode Parameters

Parameter	Description
<b>client-mode</b>	Configures the Cisco Easy VPN Remote connection to use client mode (PAT)
<b>network-extension-mode</b>	Configures the Cisco Easy VPN Remote connection to use network extension mode

### vpnclient trustpoint

To configure the RSA identity certificate to be used by the Cisco Easy VPN Remote connection, use the **vpnclient trustpoint** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

**vpnclient trustpoint** *trustpoint\_name* [*chain*]

## vpnclient trustpoint Parameters

Parameter	Description
<i>trustpoint_name</i>	Specifies the name of a trustpoint identifying the RSA certificate to use for authentication
<i>chain</i>	Sends the entire certificate chain

## vpnclient server

To configure the primary and secondary IPsec servers, for the Cisco Easy VPN Remote connection, use the **vpnclient server** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

**vpnclient server** *ip\_primary\_address* [*ip\_secondary\_address\_1* ... *ipsecondary\_address\_10*]

## vpnclient server Parameters

Parameter	Description
<i>ip_primary_address</i>	IP address or DNS name of the primary Cisco Easy VPN (IPsec) server. Any Cisco ASA adaptive security appliance or Cisco VPN 3000 Concentrator Series can act as a Cisco Easy VPN server.
<i>ip_secondary_address_n</i>	(Optional) List of the IP addresses or DNS names of up to ten backup Cisco Easy VPN servers. Use a space to separate the items in the list.

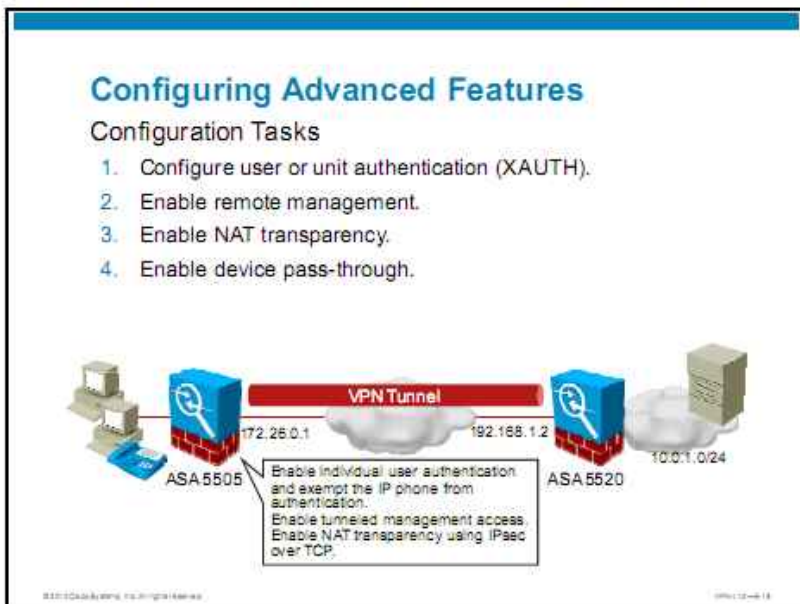
## vpnclient enable

To enable the Cisco Easy VPN Remote feature, use the **vpnclient enable** command in global configuration mode. To disable the Cisco Easy VPN Remote feature, use the **no** form of this command.

**vpnclient enable**

# Configuring Advanced Cisco Easy VPN Remote Features

This topic describes how to configure and verify advanced Cisco Easy VPN Remote features.



To configure advanced features on the Cisco ASA adaptive security appliance Cisco Easy VPN Remote, complete the following configuration tasks:

1. Configure user or unit authentication (XAUTH).
2. Enable remote management.
3. Enable NAT transparency.
4. Enable device pass-through.

The figure also shows an example that will serve as the configuration scenario for ongoing configuration tasks. You will enable individual user authentication (IUA) and exempt the IP phone from authentication. You will also enable tunneled remote management access from 10.0.1.0/24 network and NAT transparency over TCP.

## Configuring Advanced Features

### Task 1: Configure User Authentication (Client-Side)

Available user and unit authentication options:

- No extended authentication
- Unit authentication
- Secure unit authentication (enabled on server)
- Individual user authentication (enabled on server)

Configure the feature to enable the ASA to act as an Easy VPN Remote device. The ASA can then establish a VPN tunnel to a Cisco Easy VPN 3500 Concentrator, 3500-based router, or Remote Acting as an Easy VPN Server.

Enable Easy VPN Remote

Mode:  Client mode  Network extension mode

Group Settings

Disabled Site

Group Name:

Group Password:  Client Password:

Client Certificate

Select Certificate: ASA5505\_Tunnel...  Send certificate chain To configure certificates, go to: [Specify Certificates](#)

User Settings

Username:  User Password:  Certificate Password:

Easy VPN Server To Be Added

Name or IP Address:

Add

Specify user credentials for unit authentication.

Configuration > Remote Access VPN > Easy VPN Remote

The Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote configures the authentication mechanism that it uses, based on the group policy and user attributes that are pushed to it from the Cisco Easy VPN Server. The following list identifies the user authentication options that are supported by the Cisco Easy VPN Remote; however, you must configure them on the Cisco Easy VPN Server:

- **No Extended Authentication:** Does not require Extended Authentication (XAUTH) for the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote each time a tunnel initiation occurs.
- **Unit Authentication (Automatic XAUTH Authentication):** Requires only the preconfigured XAUTH for the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote to occur each time a tunnel initiation occurs. The Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote is configured with this username and password so that no other XAUTH requests happen.
- **Secure Unit Authentication (SUA)** (also called interactive unit authentication): Requires the user to authenticate the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote each time a tunnel initiation occurs, by entering a username and password. By default, SUA is not enabled. Because the policy pushed down from the Cisco Easy VPN Server overwrites the local policy on the Cisco Easy VPN Remote, SUA ignores the `vpncient username` command that is used for XAUTH if it is configured.

- **Individual User Authentication (IUA):** Requires each user behind the Cisco ASA 5505 Adaptive Security Appliance to authenticate before being granted access to the VPN network. By default, IUA is not enabled.
  - **Authentication by HTTP Redirection:** The Cisco Easy VPN Server intercepts HTTP traffic and redirects the user to a login page. HTTP redirection is automatic and does not require configuration on the Cisco Easy VPN Server. HTTP redirection happens if one of the following is true:
    - SUA or the XAUTH username and password are not configured on the Cisco Easy VPN Remote.
    - IUA is enabled.

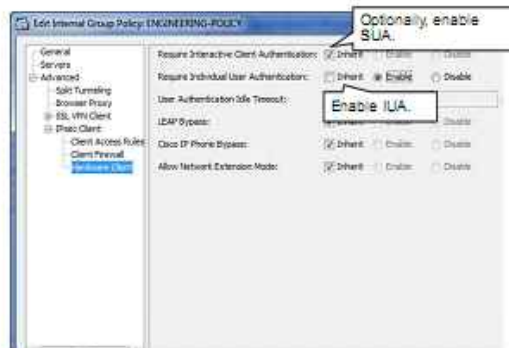
To configure the local policy of the Cisco Easy VPN Remote for unit authentication (automatic XAUTH authentication), complete the following steps:

- Step 1** Within the User Settings area of the Easy VPN Remote pane, enter a username in the Username field.
- Step 2** Enter and confirm the password in the User Password and Confirm Password fields.
- Step 3** Click **OK**.
- Step 4** Click **Apply** to apply the configuration.

## Configuring Advanced Features

### Task 1: Configure User Authentication (Server-Side)

- Secure unit authentication (SUA) is enabled on server within group policy.
- Individual user authentication (IUA) is enabled on server within group policy.



To configure the group policy on the Cisco Easy VPN Server to enable SUA or IUA, complete the following steps:

- Step 1** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** (not shown in the example).
- Step 2** Choose the appropriate group policy and click the **Edit** button.
- Step 3** In the Advanced menu in the pane on the left, choose **IPsec Clients > Hardware Client**.
- Step 4** Optionally, uncheck the **Inherit** check box for the **Require Interactive Client Authentication (SUA)** option.
- Step 5** The default is that interactive client authentication is disabled, so, optionally, click the **Enable** radio button to enable it.
- Step 6** Optionally, uncheck the **Inherit** check box for the **Require Individual User Authentication (IUA)** option.
- Step 7** The default is that IUA is disabled, so, optionally, click the **Enable** radio button to enable it.
- Step 8** Optionally, from this window, you can configure the user authentication idle timeout as well. The default timeout value is 30 minutes.
- Step 9** Click **OK**.
- Step 10** Click **Apply** to apply the configuration.

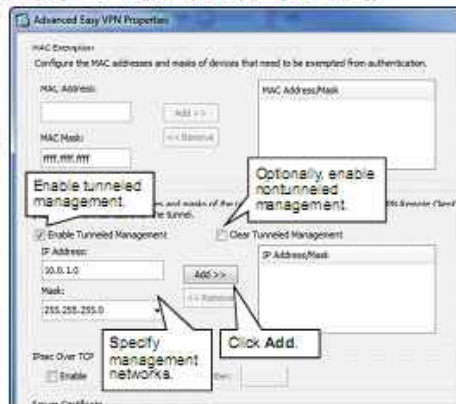
In this example, the Require Individual User Authentication option is enabled. Because this option is enabled, the XAUTH username and password configuration on the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote will be ignored.

## Configuring Advanced Features

### Task 2: Enable Remote Management (Client-Side)

Remote management types:

- Tunneled remote management
- Nontunneled remote Management
- No remote management



The Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote supports three methods of remote management access. The following methods are the three supported methods for remote management of the Cisco ASA adaptive security appliance Cisco Easy VPN Remote:

- **Tunneled:** Automates the setup of IPsec tunnels specifically for management access from the corporate network to the outside interface of the Cisco ASA 5505 Adaptive Security Appliance that is running as a Cisco Easy VPN Client. Administrative access to the client side is limited to specific hosts or networks on the corporate network.
- **Clear:** Uses normal routing to provide management access from the corporate network to the outside interface of the Cisco ASA 5505 Adaptive Security Appliance that is running as a Cisco Easy VPN Client. This option does not create management tunnels. This option should be used if a NAT device is between the Cisco Easy VPN Remote and the Server.
- **Disabled:** Prohibits management access from the Cisco Easy VPN Server side of the VPN connection unless specifically allowed in the configuration of Cisco Easy VPN Remote.

When remote management is enabled, Cisco ASDM and Secure Shell (SSH) management access is denied for the private network side of the Cisco Easy VPN Remote.

To configure remote management for the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote, complete the following steps:

- Step 1** Click the **Advanced** button in the Easy VPN Remote pane. The Advanced Easy VPN Properties window appears.
- Step 2** Within the Tunneled Management section of the Advanced Easy VPN Properties window, check the **Enable Tunneled Management** or **Clear Tunneled Management** check box.
- Step 3** When the Enable Tunneled Management check box is checked, the IP Address and Mask fields are enabled. Optionally, enter the IP address and mask in these fields for the tunneled management hosts that can access the management ports for the Cisco Easy VPN Remote.
- Step 4** Click the **Add** button.



In this example, the network IP address of 10.0.1.0 and the mask of 255.255.255.0 is entered.

## Configuring Advanced Features

### Task 3: Enable IPsec over TCP (Client-Side)

- By default, the VPN remote and server use IPsec over UDP.
- When UDP communications are not allowed, remote and server can be configured for IPsec over TCP.

Configuration > Remote Access VPN > Easy VPN Remote > Advanced

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 Internet Key Exchange (IKE) User Datagram Protocol (UDP) 500 either cannot function or cannot function transparently (without modification to existing firewall rules). VPN uses IKE for tunnel setup and security association (SA) negotiations. IKE uses UDP so that 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 or TCP port numbers. The PAT method of translating UDP port numbers does not work with IPsec. The translating device drops the IPsec frame.

The goal of IPsec over TCP is to allow the Cisco VPN Clients to operate in the various 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 that are associated with the outbound connection. Using TCP is preferred over UDP through firewalls because the state can be maintained for TCP packets, resulting in higher security. The TCP implementation defaults to port 10,000, but does not restrict the ability of the administrator to configure the Cisco VPN Client to listen on different ports.

By default, the Cisco Easy VPN Remote and server encapsulate IPsec in UDP packets. In some environments, such as those with firewall or NAT and PAT devices, UDP may be prohibited. To use standard ESP Protocol 50 or IKE UDP 500 in such environments, you must configure the client and the server to encapsulate IPsec within TCP packets to enable secure tunneling. Configuring IPsec over TCP adds unnecessary overhead to the VPN tunnel if it is not necessary. For this reason, it should not be configured unless necessary.

To configure IPsec over TCP, complete the following steps:

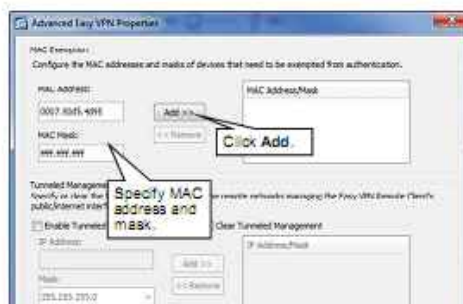
- Step 1** Within the IPsec over TCP area of the Advanced Easy VPN Properties window, check the **Enable** check box.
- Step 2** In the Enter Port Number field, enter the TCP port number to use for IPsec over TCP connections. The default TCP port number is 10000.

In this example, use of the default TCP 10000 enables IPsec over TCP. The Cisco Easy VPN Server needs to have this setting enabled within its IKE policy as well. For the VPN tunnel to come up, the TCP ports for IPsec over TCP on the client and the server must match.

## Configuring Advanced Features

### Task 4: Enable Device Pass-Through (Client-Side)

- Devices that are incapable of authenticating the VPN tunnel can be exempted from authentication.



Configuration > Remote Access VPN > Easy VPN Remote > Advanced

When the Cisco ASA 5505 Adaptive Security Appliance is deployed as a Cisco Easy VPN Remote, it can be configured to allow certain types of devices to access to the VPN tunnel without authentication because these devices are incapable of performing authentication. Cisco IP phones, network devices, and printers are examples of these types of devices.

To allow a device to pass through the VPN tunnel without authentication, the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote needs to know the MAC address of the pass-through devices. If the MAC address is not known, it assumes that the device is capable of authentication and will not allow access to the VPN tunnel until authentication is provided.

Devices such as Cisco IP phones, wireless access points (APs), and printers are incapable of performing authentication. To configure the Cisco ASA 5505 Adaptive Security Appliance Cisco Easy VPN Remote to allow devices to pass through the VPN tunnel without authentication, complete the following steps:

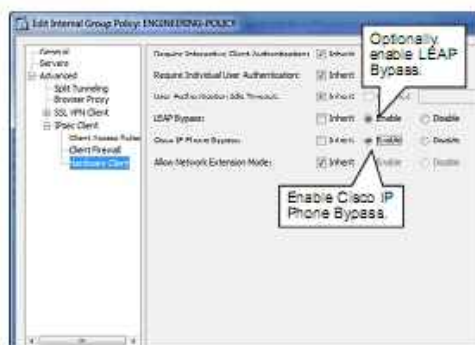
- Step 1** Within the MAC Exemption area of the Advanced Easy VPN Properties window, enter the MAC address and MAC mask in the MAC Address and MAC Mask fields. A MAC mask of `ffff.ff00.0000` matches all devices that are made by the same manufacturer. A MAC mask of `ffff.ffff.ffff` matches a single device.
- Step 2** Click the **Add** button.
- Step 3** Click **OK** to close the Advanced Easy VPN Properties window.
- Step 4** Click **Apply** to send the commands to the security appliance.

In the example, the MAC address of `0007.50d5.4d95` is entered for the IP phone with a MAC mask of `ffff.ffff.ffff` to match this specific IP phone and MAC address.

## Configuring Advanced Features

### Task 4: Enable Device Pass-Through (Server-Side)

- Bypass has to be allowed on the server within group policy.



Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Devices such as Cisco IP phones and wireless access points are incapable of performing authentication. You can allow Cisco IP phones to bypass IUA behind a hardware client. Cisco IP Phone Bypass lets IP phones behind hardware clients connect without undergoing user authentication processes. Cisco IP Phone Bypass is disabled by default.

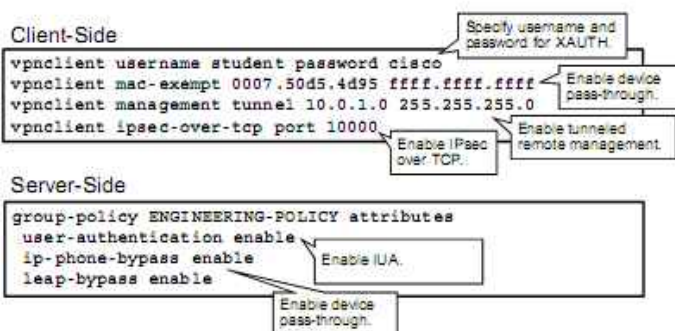
When Cisco Lightweight Extensible Authentication Protocol (LEAP) Bypass is enabled, Cisco LEAP packets from wireless devices behind a VPN hardware client travel across a VPN tunnel before user authentication. This action lets workstations using Cisco wireless access point devices establish Cisco LEAP authentication and then authenticate again per user authentication. Cisco LEAP Bypass is disabled by default.

To configure the Cisco ASA 5520 Adaptive Security Appliance Cisco Easy VPN Server to allow devices to pass through the VPN tunnel without authentication, complete the following steps:

- Step 1** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
- Step 2** Select a group policy that you want to edit and click **Edit** button.
- Step 3** Click the **Hardware Client** option from the menu in the pane on the left.
- Step 4** Uncheck the **Inherit** check box for the LEAP Bypass.
- Step 5** The default for LEAP Bypass is Disable, so click the **Enable** radio button to enable it.
- Step 6** Uncheck the **Inherit** check box for the Cisco IP Phone Bypass.
- Step 7** The default for Cisco IP Phone Bypass is Disable, so click the **Enable** radio button to enable it.
- Step 8** Click **OK** to close the Edit Internal Group Policy window.
- Step 9** Click **Apply** to send the commands to the Cisco ASA adaptive security appliance.

## Configuring Advanced Features

### CLI Configuration



To configure advanced features using CLI, use the commands described here.

## Cisco Easy VPN Remote Side

Use the **vpnclient username password** command to configure the username for XAUTH. Use the **vpnclient mac-exempt** to provide MAC addresses of devices that are eligible for pass-through. Use the **vpnclient management tunnel** command to enable tunneled remote management. Use the **vpnclient ipsec-over-tcp port** command to enable IPsec over TCP.

## Cisco Easy VPN Server Side

First enter group-policy configuration mode using the **group-policy attributes** command. Then enable IUA using the **user-authentication enable** command. Enable device pass-through using the **ip-phone-bypass enable** and **leap-bypass enable** commands respectively.

### vpnclient username

To configure the VPN username and password for the Cisco Easy VPN Remote connection, use the **vpnclient username** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

```
vpnclient username xauth_username password xauth_password
```

#### vpnclient username Parameters

Parameter	Description
<i>xauth_username</i>	Specifies the username to use for XAUTH. The maximum length is 64 characters.
<i>xauth_password</i>	Specifies the password to use for XAUTH. The maximum length is 64 characters.

## vpnclient mac-exempt

To exempt devices behind a Cisco Easy VPN Remote connection from IUA requirements, use the **vpnclient mac-exempt** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

**vpnclient mac-exempt** *mac\_addr\_1 mac\_mask\_1* [*mac\_addr\_2 mac\_mask\_2 ... mac\_addr\_n mac\_mask\_n*]

### vpnclient mac-exempt Parameters

Parameter	Description
<i>mac_mask_n</i>	Network mask for the corresponding MAC address. Use a space to separate the network mask and any subsequent MAC address and network mask pairs.
<i>mac_addr_n</i>	MAC address, in dotted hexadecimal notation, specifying a manufacturer and serial number of a device for which to exempt IUA. For more than one device, specify each MAC address, separating each with a space and the respective network mask.  The first six characters of the MAC address identify the device manufacturer, and the last six characters are the serial number. The last 24 bits are the serial number of the unit in hexadecimal format.

## vpnclient management

To generate IPsec tunnels for management access to the Cisco Easy VPN Remote, use the **vpnclient management** command in global configuration mode.

To remove the attribute from the running configuration, use the **no** form of this command, which sets up IPsec tunnels exclusively for management in accordance with the **split-tunnel-policy** and **split-tunnel-network-list** commands.

**vpnclient management tunnel** *ip\_addr\_1 ip\_mask\_1* [*ip\_addr\_2 ip\_mask\_2 ... ip\_addr\_n ip\_mask\_n*]

**vpnclient management clear**

### vpnclient management Parameters

Parameter	Description
<b>tunnel</b>	Automates the setup of IPsec tunnels specifically for management access from the corporate network to the outside interface of the Cisco ASA 5505 Adaptive Security Appliance running as a Cisco Easy VPN Client.
<i>ip_addr_n</i>	IP address of the host or network for which to build a management tunnel from the Cisco Easy VPN Remote. Use this argument with the <b>tunnel</b> keyword. Specify one or more IP addresses, separating each with a space and the respective network mask.
<i>ip_mask_n</i>	Network mask for the corresponding IP address. Use a space to separate the network mask and any subsequent IP address and network mask pairs.
<b>clear</b>	Uses normal routing to provide management access from the corporate network to the outside interface of the Cisco ASA 5505 Adaptive Security Appliance running as a Cisco Easy VPN Client. This option does not create management tunnels.  <b>Note</b> Use this option if a NAT device is operating between the client and the Internet.

## vpnclient ipsec-over-tcp

To configure the Cisco ASA 5505 Adaptive Security Appliance running as a Cisco Easy VPN Remote to use TCP-encapsulated IPsec, use the **vpnclient ipsec-over-tcp** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

```
vpnclient ipsec-over-tcp [port tcp_port]
```

### vpnclient ipsec-over-tcp Parameters

Parameter	Description
<code>port</code>	(Optional) Specifies the use of a particular port.
<code>tcp_port</code>	(Required if you specify the <b>port</b> keyword.) Specifies the TCP port number to be used for a TCP-encapsulated IPsec tunnel.

## user-authentication

To enable user authentication, use the **user-authentication enable** command in group-policy configuration mode. To disable user authentication, use the **user-authentication disable** command. To remove the user authentication attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for user authentication from another group policy.

When user authentication is enabled, it requires that individual users behind a hardware client authenticate to gain access to the network across the tunnel.

```
user-authentication {enable | disable}
```

### user-authentication Parameters

Parameter	Description
<code>enable</code>	Enables user authentication
<code>disable</code>	Disables user authentication

## ip-phone-bypass

To enable IP Phone Bypass, use the **ip-phone-bypass enable** command in group-policy configuration mode. To disable IP Phone Bypass, use the **ip-phone-bypass disable** command. To remove the IP phone Bypass attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for IP Phone Bypass from another group policy.

IP Phone Bypass lets IP phones behind hardware clients connect without undergoing user authentication processes. If enabled, SUA remains in effect.

```
ip-phone-bypass {enable | disable}
```

### ip-phone-bypass Parameters

Parameter	Description
<code>enable</code>	Enables IP Phone Bypass
<code>disable</code>	Disables IP Phone Bypass

## leap-bypass

To enable LEAP Bypass, use the **leap-bypass enable** command in group-policy configuration mode. To disable LEAP Bypass, use the **leap-bypass disable** command. To remove the LEAP Bypass attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for LEAP Bypass from another group policy.

**leap-bypass {enable | disable}**

### leap-bypass Parameters

Parameter	Description
<b>enable</b>	Enables LEAP Bypass
<b>disable</b>	Disables LEAP Bypass



# Troubleshooting the Cisco Easy VPN Remote

This topic describes how to troubleshoot Cisco Easy VPN Remote connections.

## Verifying Remote Access VPNs

IPsec		SSL VPN				IPsec Proxy	VPN Load Balancing	Total	Total Cumulative
Remote Access	Site-to-Site	Clientless	with Client	Inactive	Total				
1	0	0	0	0	0	0	0	1	5

Filter By: [IPsec Remote Access] [All Sessions] [Filter]

Username	Group Policy/Connection Profile	Assigned IP Address/Public/Private IP Address	Protocol/Encryption	Login Time/Duration	Details
pomer	ANYCONNECT-PROFILE	10.211.1.2 172.26.1.1	IPsec Open AES128	08:06:30 UTC Mon Aug 16 2010 00:00:21s	Logout Ping

Monitoring > VPN > VPN Statistics > Sessions

© 2010 Cisco Systems, Inc. All rights reserved. VPN-11-248-01

You can use Cisco ASDM and the command-line interface (CLI) commands to verify remote access VPN operation.

Complete the following steps to monitor IPsec VPN connections using Cisco ASDM:

- Step 1** Inside ASDM, navigate to **Monitoring > VPN > VPN Statistics > Sessions**.
- Step 2** Choose the **IPsec Remote Access** option from the **Filter By** drop-down menu. You should see active remote access IPsec tunnels.
- Step 3** Optionally, click the **Details** button to observe details about the connection (not shown in the example).

## Verifying Remote Access VPNs

### CLI Commands

```
ASA#show vpn-sessiondb remote

Session Type: IPsec

Index      : 697
Assigned IP : 10.0.1.0          Peer IP    : 172.16.0.1
Protocol   : IKE IPsec
License    : IPsec
Encryption : 3DES AES128      Hashing    : SHA1
Bytes Tx   : 240              Bytes Rx   : 240
Login Time : 08:04:31 UTC Mon Aug 16 2010
Duration   : 0h:25m:40s
Inactivity : 0h:00m:00s
```

### show vpn-sessiondb

To display information about VPN sessions, use the **show vpn-sessiondb** command. The command includes options for displaying information in full (streamed, untruncated output) or in detail (extended details), lets you specify the type of sessions to display, and provides options to filter and sort the information.

```
show vpn-sessiondb [detail] [full] {remote | I21 | index indexnumber | webvpn | email-proxy} [filter {name username | ipaddress IPaddr | a-ipaddress IPaddr | p-ipaddress IPaddr | tunnel-group groupname | protocol protocol-name | encryption encryption-algo}] [sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption}]
```

The figure displays the output of the **show vpn-sessiondb remote** command. This command displays remote access sessions. You can display this information for all groups or you can filter it by using the following filter options: **name**, **a-ipaddress**, **p-ipaddress**, **tunnel-group**, **protocol**, and **encryption**.

## show vpn-sessiondb Parameters

Parameter	Description
<code>detail</code>	(Optional) Displays extended details about a session. For example, using the <code>detail</code> option for an IPsec session displays additional details such as the IKE hashing algorithm, authentication mode, and rekey interval.  If you choose <code>detail</code> , and the <code>full</code> option, the adaptive security appliance displays the detailed output in a machine-readable format.
<code>filter filter_criteria</code>	(Optional) Filters the output to display only the information that you specify by using one or more of the filter options.
<code>full</code>	(Optional) Displays streamed, untruncated output. Output is delineated by   characters and a    string between records.
<code>session_type</code>	(Optional) To show data for a specific session type, enter one of the following keywords: <ul style="list-style-type: none"><li>■ <b>email-proxy</b>: Displays email-proxy sessions</li><li>■ <b>index <i>indexnumber</i></b>: Displays a single session by index number. Specify the index number for the session, 1–750</li><li>■ <b>I2I</b>: Displays VPN LAN-to-LAN session information</li><li>■ <b>ratio</b>: Displays VPN Session protocol or encryption ratios</li><li>■ <b>remote</b>: Displays IPsec remote access sessions</li><li>■ <b>summary</b>: Displays the VPN session summary</li><li>■ <b>svc</b>: Displays SSL VPN Client sessions</li><li>■ <b>vpn-lb</b>: Displays VPN Load Balancing management sessions</li><li>■ <b>webvpn</b>: Displays information about clientless SSL VPN sessions</li></ul>
<code>sort sort_criteria</code>	(Optional) Sorts the output according to the sort option that you specify.

Information from the `show vpn-sessiondb remote` command includes the following:

- Session type
- Username (the tunnel group that is created by the IPsec Connection Profile)
- Assigned address of client
- Public address of client
- Encryption algorithm
- Hash algorithm
- Tunnel group
- Login time of client

## Verifying Remote Access VPNs

### CLI Commands (Cont.)

```
ASA#show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA
during rekey)
Total IKE SA: 1

1 IKE Peer: 192.168.1.6
  Type    : user           Role    : responder
  Rekey   : no           State   : MM_ACTIVE
```

### show crypto isakmp sa

To display the IKE run-time SA database, use the **show crypto isakmp sa** command in global configuration mode or privileged EXEC mode.

**show crypto isakmp sa [detail]**

#### show crypto isakmp sa Parameters

Parameter	Description
<b>detail</b>	Displays detailed output about the SA database.

Information from the **show crypto isakmp sa** command may include the following:

- Active SAs
- Total IKE SAs
- IKE peer addresses
- State of the connection

## Verifying Remote Access VPNs

### CLI Commands (Cont.)

```
ASA#show crypto ipsec sa
Interface: outside
Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: LOCAL-CAL-SRVSRV

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.0.1.20/255.255.255.255/0/0)
current_peer: 192.168.1.6, username: david1.cisco.com
dynamic allocated peer ip: 10.0.1.20

#pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
#pkts decaps: 330, #pkts decrypt: 330, #pkts verify: 330
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 52, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#MTEs sent: 0, #MTEs rcvd: 0, #decompressed frags needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.6
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 03630655
```

### show crypto ipsec sa

To display a list of IPsec SAs, use the `show crypto ipsec sa` command. The figure displays the output of this command.

`show crypto ipsec sa [entry | identity | map map-name | peer peer-addr] [detail]`

#### show crypto ipsec sa Parameters

Parameter	Description
<code>entry</code>	(Optional) Displays IPsec SAs sorted by peer address.
<code>identity</code>	(Optional) Displays IPsec SAs sorted by identity, not including Encapsulating Security Payloads (ESPs). This form is a condensed form.
<code>map <i>map-name</i></code>	(Optional) Displays IPsec SAs for the specified crypto map.
<code>peer <i>peer-addr</i></code>	(Optional) Displays IPsec SAs for specified peer IP addresses.
<code>detail</code>	(Optional) Displays detailed error information on what is displayed.

Information in the output of this command includes the following:

- Interface that is used for the tunnel
- Crypto map
- Current peer
- Username of current peer
- Packet statistics
- Local and remote crypto endpoints

# Summary

This topic summarizes the key points that were discussed in this lesson.

## Summary

- The Cisco Easy VPN Remote feature supports client and network extension modes of operation.
- The Cisco ASA 5505 appliance can be configured as a Cisco Easy VPN Remote.
- The ASA 5505 Cisco Easy VPN Remote supports these authentication mechanisms: no extended authentication, unit authentication, SUA, and IUA.
- You may use Cisco ASDM and CLI commands to verify remote access VPN operation.

© 2010 Cisco Systems, Inc.

© 2010 Cisco

# Module Summary

This topic summarizes the key points that were discussed in this module.

## Module Summary

- To configure a basic site-to-site IPsec VPN, configure basic peer authentication and transmission protection and verify communication over the encrypted tunnel.
- Because the use of a PSK to authenticate a remote peer does not scale well in large networks, the preferred method is to exchange digital certificates.
- The Cisco VPN Client on a remote PC, communicating with a Cisco Easy VPN Server on an enterprise network or with a service provider, creates a secure connection over the Internet.
- A basic Cisco Easy VPN solution provides client-based access to sensitive resources over a remote access IPsec VPN gateway, implemented on the Cisco ASA adaptive security appliance.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-04-1

## Module Summary (Cont.)

- Before the IPsec VPN clients establish a secure connection to the VPN gateway, they should first authenticate to the VPN gateway.
- The Cisco Easy VPN Remote feature enables Cisco security appliances and Cisco IOS routers to act as Cisco Easy VPN Clients. These devices can receive security policies from a Cisco Easy VPN Server.

© 2010 Cisco Systems, Inc. All rights reserved.

VPN-11-04-2