Copyright Information

Disclaimer

The following publication, ***CCIE Security Lab Workbook Volume I***, is designed to assist candidates in the preparation for Cisco Systems' CCIE Routing & Switching Lab exam. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Internetwork Expert, Inc. assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this workbook.

This workbook was developed by Internetwork Expert, Inc. and is an original work of the aforementioned authors. Any similarities between material presented in this workbook and actual CCIE™ lab material is completely coincidental.

Table of Contents

VPN 1

COMMON CONFIGURATIONS 1
IOS Router and the PIX/ASA 1
IOS Router and VPN3k 6
GRE and DMVPN 24
VPN3k Easy VPN/WebVPN 27
IOS Easy VPN 42
PIX/ASA Easy VPN/WebVPN 46

IPSEC LAN-TO-LAN 50
IOS and the PIX/ASA with PSK 50
IOS and the PIX/ASA with PSK and NAT on the Firewall 55
IOS and the PIX/ASA with Digital Certificates 57
IOS and the PIX/ASA: Matching Name in Certificate 65
IOS and IOS with PSK Across the PIX/ASA 68
IOS and IOS with PSK Across the PIX/ASA and NAT 74
IOS and IOS with PSK Across the PIX/ASA with Overlapping Subnets 80
IOS and IOS with PSK Across the PIX/ASA and NAT with IKE AM 87
IOS and IOS with Digital Certificates Across the PIX/ASA 96
IOS and VPN3k with PSK 103
IOS and VPN3k with PSK using CLI only 113
IOS and VPN3k with Digital Certificates 131
IOS and VPN3k with PSK: Tuning IPsec Parameters 148
IOS and VPN3k: Filtering Tunneled Traffic 159

GRE AND DMVPN 168
GRE Tunnels over IPsec with Static Crypto Maps 168
GRE Tunnels over IPsec with Crypto Profiles 175
DMVPN with PSK 182

EASY VPN 189
VPN3k and Cisco VPN Client 189
VPN3k and Cisco VPN Client with Split-Tunneling 201
VPN3k and Cisco VPN Client with Hold-Down Route 206
VPN3k and Cisco VPN Client with RRI 212
VPN3k and Cisco VPN Client with DHCP Server 219
VPN3k and Cisco VPN Client with RADIUS Authentication 224
VPN3k and Cisco VPN Client with External Group 244
VPN3k and Cisco VPN Client with Digital Certificates 256
VPN3k and IOS ezVPN Remote Client Mode with Split-Tunneling 284
VPN3k and IOS ezVPN Remote NW Extension Mode with RRI 298
IOS and IOS ezVPN Remote Client Mode with Xauth/RRI 308
IOS and IOS ezVPN Remote NW Extension Mode with Xuath/RRI 315
PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI 318
PIX/ASA and Cisco VPN Client with External Policy 324

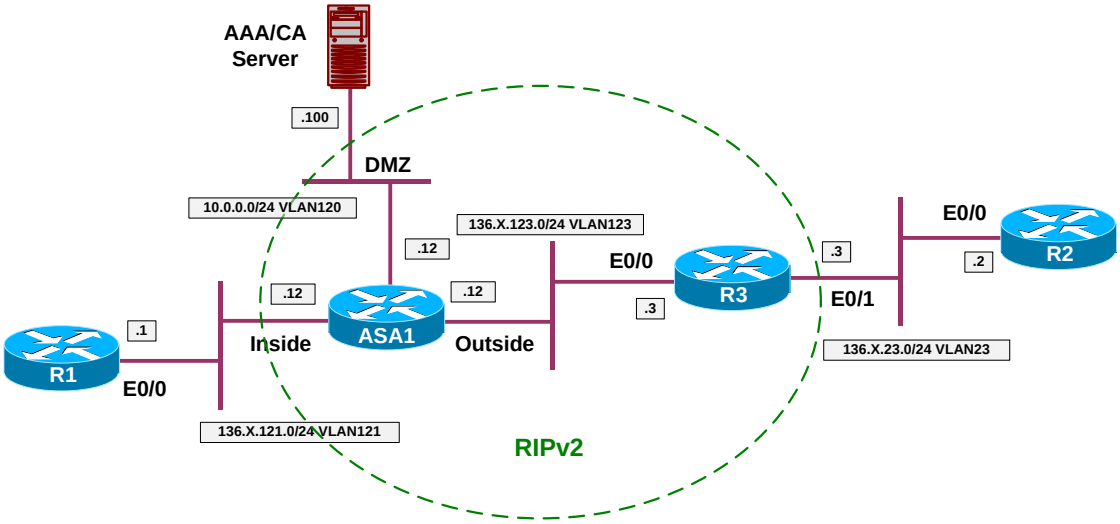
PIX/ASA and Cisco VPN Client with RADIUS....339
PIX/ASA and Cisco VPN Client with Digital Certificates....345
The PIX/ASA and IOS ezVPN Remote NW Extension Mode....362
WEBVPN AND SSL VPN....367
ASA and WebVPN Client....367
ASA and WebVPN Port Forwarding....374
ASA and SSL VPN Client....380
VPN3k and WebVPN Client....383
VPN3k and WebVPN Port Forwarding....397
VPN QOS....407
IOS and the PIX/ASA: Policing the L2L IPsec tunnel....407
IOS and VPN3k: QoS for L2L Tunnel....410
PIX/ASA and Cisco VPN Client: Per-Flow Policing....417
QoS Pre-Classify for IPsec Tunnel....421
ADVANCED VPN TOPICS....425
Decoding IPsec Debugging Output on VPN3k....425
IPsec and Fragmentation Issues....440
ISAKMP Pre-Shared Keys via AAA....443
IPsec NAT-T: L2L Tunnel with VPN3k and IOS Box....459
IKE Tunnel Endpoint Discovery (TED)....466
IPsec VPN High-Availability with HSRP....470
IPsec High Availability with NAT and HSRP....479
IPsec Pass-Through Inspection on the PIX/ASA....483
L2TP over IPsec between the ASA and Windows 2000 PC....485
VPN3k and PPTP Client....494
Using ISAKMP Profiles....506
IOS FIREWALL....518
Common Configuration....518
Basic Access-Lists....521
Reflexive Access-Lists....527
Dynamic Access-Lists....531
Stateful Inspection with CBAC....534
CBAC Port-to-Application Mapping....537
Preventing DoS Attacks with CBAC....539
CBAC Performance Tuning....542
Authentication Proxy with RADIUS....544
Content Filtering with IOS Firewall....556

VPN

Common Configurations

IOS Router and the PIX/ASA

Objective: Configure common L2/L3 settings for IOS & the PIX/ASA VPN scenarios.



Directions

- Create VLANs, configure trunk and access-ports to reflect the diagram topology.
- Configure IP addressing as per the diagram.
- Configure RIP on the ASA Firewall and R3. Advertise all the connected interfaces.
- Configure static default route on R1 and R2 to point at ASA/R3 respectively.
- Permit outside access to AAA/CA server via HTTP/NTP, as well as ICMP traffic from outside.

Final Configuration

```
ASA1:
!
! IP addressing
!
interface Ethernet0/0
 no shut
 nameif outside
```

```
 security-level 0
 ip address 136.1.123.12 255.255.255.0
!
interface Ethernet0/1
 no shut
 nameif inside
 security-level 100
 ip address 136.1.121.12 255.255.255.0
!
interface Ethernet0/2
 no shut
 nameif dmz
 security-level 50
 ip address 10.0.0.12 255.255.255.0
!
! RIP configuration
!
router rip
 version 2
 no auto-summary
 network 10.0.0.0
 network 136.1.0.0
!
! Access-Control: permit HTTP/NTP and ICMP
!
access-list OUTSIDE_IN permit tcp any host 10.0.0.100 eq 80
access-list OUTSIDE_IN permit udp any host 10.0.0.100 eq 123
access-list OUTSIDE_IN permit icmp any any
!
access-group OUTSIDE_IN in interface outside
```

SW1 & SW2:

```
!
! create VLANs and configure trunk links
!
vlan 23,120,121,123
!
interface range Fa 0/21 - 23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shut
```

SW1:

```
!
!  Configure switchports
!
interface Fa 0/1
 switchport host
 switchport access vlan 121
!
interface Fa 0/2
 switchport host
 switchport access vlan 23
!
interface Fa 0/3
 switchport host
 switchport access vlan 123
!
interface Fa 0/13
 switchport host
 switchport access vlan 121
!
interface Fa 0/20
```

```
 switchport host
 switchport access vlan 120
```

SW2:

```
!
!  Configure switchports
!
interface Fa 0/3
 switchport host
 switchport access vlan 23
!
interface Fa 0/12
 switchport host
 switchport access vlan 123
```

R1:

```
interface E 0/0
 no shut
 ip add 136.1.121.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 136.1.121.12
```

R2:

```
interface E 0/0
 no shut
 ip add 136.1.23.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 136.1.23.3
```

R3:

```
interface E 0/0
 no shut
 ip add 136.1.123.3 255.255.255.0
!
interface E 0/1
 no shut
 ip add 136.1.23.3 255.255.255.0
!
router rip
 version 2
 no auto-summary
 network 136.1.0.0
```

Verification

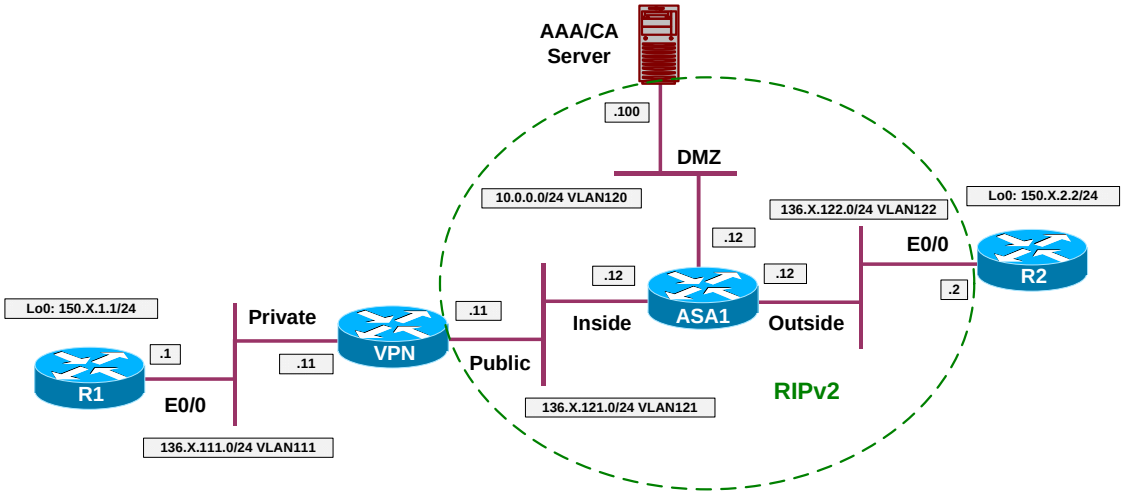
```
ASA1(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    136.1.23.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:06, outside
C    136.1.121.0 255.255.255.0 is directly connected, inside
C    136.1.123.0 255.255.255.0 is directly connected, outside
C    10.0.0.0 255.255.255.0 is directly connected, dmz
```

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     136.1.0.0/24 is subnetted, 3 subnets
C       136.1.23.0 is directly connected, Ethernet0/1
R       136.1.121.0 [120/1] via 136.1.123.12, 00:00:17, Ethernet0/0
C       136.1.123.0 is directly connected, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/1] via 136.1.123.12, 00:00:17, Ethernet0/0

ASA1(config)# ping 10.0.0.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R2#ping 136.1.23.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.23.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/5 ms

R1#ping 136.1.121.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#telnet 136.1.23.2
Trying 136.1.23.2 ... Open



User Access Verification

Password:
R2>

R3#ping 10.0.0.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R3#telnet 10.0.0.100 80
Trying 10.0.0.100, 80 ... Open


HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 12 Jan 2007 09:54:11 GMT
```

```
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect.
</body></html>
[Connection to 10.0.0.100 closed by foreign host]
```

IOS Router and VPN3k

Objective: Configure common L2/L3 settings for IOS & VPN3k scenarios.



Directions

- Create VLANs, configure trunk and access-ports to reflect the diagram topology.
- Configure IP addressing as per the diagram.
- Configure RIP on the ASA Firewall, VPN3k and R2. Advertise all the connected interfaces.
- Configure static route for 150.X.1.0/24 on VPN3k.
- Configure static default route on R1 to point at VPN3k.
- Permit outside access to AAA/CA server via HTTP/NTP, as well as ICMP traffic from outside.
- Permit acess from DMZ to VPN3k via HTTPs.

Final Configuration

ASA1:

```
!
! IP addressing
!
interface Ethernet0/0
 no shut
 nameif outside
 security-level 0
 ip address 136.1.122.12 255.255.255.0
!
interface Ethernet0/1
 no shut
 nameif inside
 security-level 100
 ip address 136.1.121.12 255.255.255.0
!
interface Ethernet0/2
 no shut
```

```
 nameif dmz
 security-level 50
 ip address 10.0.0.12 255.255.255.0
!
! RIP configuration
!
router rip
 version 2
 no auto-summary
 network 10.0.0.0
 network 136.1.0.0
!
! Access-Control: permit HTTP/NTP and ICMP
!
access-list OUTSIDE_IN permit tcp any host 10.0.0.100 eq 80
access-list OUTSIDE_IN permit udp any host 10.0.0.100 eq 123
access-list OUTSIDE_IN permit icmp any any
!
access-group OUTSIDE_IN in interface outside
!
! HTTPs to VPN3k
!
access-list DMZ_IN extended permit tcp any any eq https
access-group DMZ_IN in interface dmz
```

SW1 & SW2:

```
!
! create VLANs and configure trunk links
!
vlan 111,120,121,122
!
interface range Fa 0/21 - 23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shut
```

SW1:

```
!
!  Configure switchports
!
interface Fa 0/1
 switchport host
 switchport access vlan 111
!
interface Fa 0/2
 switchport host
 switchport access vlan 122
!
interface Fa 0/11
 switchport host
 switchport access vlan 111
!
interface Fa 0/13
 switchport host
 switchport access vlan 121
!
interface Fa 0/20
 switchport host
 switchport access vlan 120
```

SW2:

```
!
!  Configure switchports
```

```
!
interface Fa 0/11
 switchport host
 switchport access vlan 121
!
interface Fa 0/12
 switchport host
 switchport access vlan 122
```

R1:

```
interface E 0/0
 no shut
 ip add 136.1.111.1 255.255.255.0
!
interface Loopback0
 ip add 150.1.1.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 136.1.111.11
```

R2:

```
interface E 0/0
 no shut
 ip add 136.1.122.2 255.255.255.0
!
router rip
 version 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
!
interface Loopback 0
 ip address 150.1.2.2 255.255.255.0
```

VPN3k:

Reboot with clean config:

```
                Welcome to
               Cisco Systems
       VPN 3000 Concentrator Series
          Command Line Interface
Copyright (C) 1998-2005 Cisco Systems, Inc.



1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 2

1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Traceroute
7) Access Rights
8) File Management
9) Certificate Management
```

```
10) Back

VPN3k: Admin -> 3

1) Cancel Scheduled Reboot/Shutdown
2) Schedule Reboot
3) Schedule Shutdown
4) Back

VPN3k: Admin -> 2

1) Save active Configuration and use it at Reboot
2) Reboot without saving active Configuration file
3) Reboot ignoring the Configuration file
4) Back

VPN3k: Admin -> 3

1) Cancel Scheduled Reboot/Shutdown
2) Reboot Now
3) Reboot in X minutes
4) Reboot at time X
5) Reboot wait for sessions to terminate
6) Back

VPN3k: Admin -> 2


41 01/15/2007 19:47:44.160 SEV=1 REBOOT/1 RPT=1
Reboot scheduled immediately.
Done
```

Perform initial setup:

```
                Welcome to
               Cisco Systems
       VPN 3000 Concentrator Series
          Command Line Interface
Copyright (C) 1998-2005 Cisco Systems, Inc.



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

 -- : Enter the system time in the following format:
 -- :       HH:MM:SS.  Example  21:30:00  for 9:30 PM

> Time

Quick -> [ 19:52:27 ]

 -- : Enter the date in the following format.
 -- : MM/DD/YYYY  Example 06/12/1999  for June 12th 1999.

> Date

Quick -> [ 01/15/2007 ]

 -- :  Set the time zone on your device. The correct time zone is very
```

```
 -- :  important so that logging and accounting entries are accurate.

 -- :  Enter the time zone using the hour offset from GMT:
 -- :  -12 : Kwajalein   -11 : Samoa      -10 : Hawaii         -9 : Alaska
 -- :   -8 : PST          -7 : MST         -6 : CST            -5 : EST
 -- :   -4 : Atlantic     -3 : Brasilia  -3.5 : Newfoundland   -1 : Mid-
Atlantic
 -- :   -1 : Azores        0 : GMT         +1 : Paris          +2 : Cairo
 -- :   +3 : Kuwait     +3.5 : Tehran      +4 : Abu Dhabi    +4.5 : Kabul
 -- :   +5 : Karachi    +5.5 : Calcutta +5.75 : Kathmandu      +6 : Almaty
 -- : +6.5 : Rangoon      +7 : Bangkok     +8 : Singapore      +9 : Tokyo
 -- : +9.5 : Adelaide    +10 : Sydney     +11 : Solomon Is.   +12 : Marshall
Is.

> Time Zone

Quick -> [ -8 ]

1) Enable Daylight Savings Time Support
2) Disable Daylight Savings Time Support

Quick -> [ 1 ]

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|Not Configured|        0.0.0.0/0.0.0.0        |
Ether2-Pub|Not Configured|        0.0.0.0/0.0.0.0        |
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

** An address is required for the private interface. **

> Enter IP Address

Quick Ethernet 1 -> [ 0.0.0.0 ] 136.1.111.11

Waiting for Network Initialization...

> Enter Subnet Mask

Quick Ethernet 1 -> [ 255.255.0.0 ] 255.255.255.0

> Enter Interface Name

Quick Ethernet 1 -> Private

1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick Ethernet 1 -> [ 3 ]

1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick Ethernet 1 -> [ 1 ]

> MTU (68 - 1500)
```

```
Quick Ethernet 1 -> [ 1500 ]

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 2

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|Not Configured|        0.0.0.0/0.0.0.0        |
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

> Enter IP Address

Quick Ethernet 2 -> [ 0.0.0.0 ] 136.1.121.11

> Enter Subnet Mask

Quick Ethernet 2 -> [ 255.255.0.0 ] 255.255.255.0

> Enter Interface Name

Quick Ethernet 2 -> Public

1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick Ethernet 2 -> [ 3 ]

1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick Ethernet 2 -> [ 1 ]

> MTU (68 - 1500)

Quick Ethernet 2 -> [ 1500 ]

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 4

 -- : Assign a System Name (hostname) to this device.
 -- : This may be required for DHCP.

> System Name
```

```
Quick -> VPN3K

 -- : Specify a local DNS server, which lets you enter hostnames
 -- : rather than IP addresses while configuring.

> DNS Server

VPN3K: Quick -> [ 0.0.0.0 ]

 -- : Enter your Internet domain name; e.g., yourcompany.com

> Domain

VPN3K: Quick ->

> Default Gateway

VPN3K: Quick ->

-- : Configure protocols and encryption options.
-- : This table shows current protocol settings

         PPTP         |        L2TP         |
----------------------------------------------
|       Enabled       |       Enabled       |
|  No Encryption Req  |  No Encryption Req  |
----------------------------------------------

1) Enable  PPTP
2) Disable PPTP

VPN3K: Quick -> [ 1 ]

1) PPTP Encryption Required
2) No Encryption Required

VPN3K: Quick -> [ 2 ]

1) Enable  L2TP
2) Disable L2TP

VPN3K: Quick -> [ 1 ]

1) L2TP Encryption Required
2) No Encryption Required

VPN3K: Quick -> [ 2 ]

1) Enable  IPSec
2) Disable IPSec

VPN3K: Quick -> [ 1 ]

1) Enable  WebVPN
2) Disable WebVPN

VPN3K: Quick -> [ 1 ] 2

-- : Configure address assignment for PPTP, L2TP and IPSec.

1) Enable Client Specified Address Assignment
2) Disable Client Specified Address Assignment
```

```
VPN3K: Quick -> [ 2 ]

1) Enable Per User Address Assignment
2) Disable Per User Address Assignment

VPN3K: Quick -> [ 2 ]

1) Enable DHCP Address Assignment
2) Disable DHCP Address Assignment

VPN3K: Quick -> [ 2 ]

1) Enable Configured Pool Address Assignment
2) Disable Configured Pool Address Assignment

VPN3K: Quick -> [ 2 ]

-- : Specify how to authenticate users

1) Internal
2) RADIUS
3) NT Domain
4) SDI
5) Kerberos/Active Directory
6) Continue

VPN3K: Quick -> [ 1 ]

                                    Current Users
-------------------------------------------------------------------------------
                                      No Users
-------------------------------------------------------------------------------

1) Add a User
2) Delete a User
3) Continue

VPN3K: Quick -> 3

> IPSec Group Name

VPN3K: Quick ->

-- : We strongly recommend that you change the password for user admin.

> Reset Admin Password

VPN3K: Quick -> [ ***** ]

Verify ->

1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit

VPN3K: Quick -> 2

1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit

VPN3K: Quick -> 1
```

```
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config ->h
```

Now configure RIP routing:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|      UP      |   136.1.121.11/255.255.255.0  | 00.03.A0.88.BD.2A
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

VPN3K: Interfaces -> 2

1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Set Interface Name
4) Select IP Filter
5) Select Ethernet Speed
6) Select Duplex
7) Set MTU
8) Set Port Routing Config
9) Set Bandwidth Management
10) Set Public Interface IPSec Fragmentation Policy
11) Set Interface WebVPN Parameters
12) Back

VPN3K: Ethernet Interface 2 -> 8
```

```
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3K: Ethernet Interface 2 -> 1

1) Disable Inbound RIP
2) Enable RIP V1 Inbound
3) Enable RIP V2 Inbound
4) Enable RIP V2/V1 Inbound

VPN3K: Ethernet Interface 2 -> [ 1 ] 3

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3K: Ethernet Interface 2 -> 2

1) Disable Outbound RIP
2) Enable RIP V1 Outbound
3) Enable RIP V2 Outbound
4) Enable RIP V2/V1 Outbound

VPN3K: Ethernet Interface 2 -> [ 1 ] 3

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3K: Ethernet Interface 2 ->
```

Permit RIP through the Public Filter:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 4

1) Access Hours
2) Traffic Management
```

```
3) Group Matching
4) Network Admission Control
5) Back

VPN3K: Policy -> 2

1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back

VPN3K: Traffic -> 4

                             Current Active Filters
-------------------------------------------------------------------------------
| 1. Private (Default)                 | 2. Public (Default)                  |
| 3. External (Default)                | 4. Firewall Filter for VPN Client (De|
-------------------------------------------------------------------------------

1) Add a Filter
2) Modify a Filter
3) Delete a Filter
4) Assign Rules to a Filter
5) Copy a Filter
6) Back

VPN3K: Filters -> 4

> Which Filter to assign Rules to

VPN3K: Filters -> 2

                       The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. GRE In                            | IN FORWARD                           |
| 2. IPSEC-ESP In                      | IN FORWARD                           |
| 3. IKE In                            | IN FORWARD                           |
| 4. PPTP In                           | IN FORWARD                           |
| 5. L2TP In                           | IN FORWARD                           |
| 6. ICMP In                           | IN FORWARD                           |
| 7. VRRP In                           | IN FORWARD                           |
| 8. NAT-T In                          | IN FORWARD                           |
| 9. GRE Out                           | OUT FORWARD                          |
| 10. IKE Out                          | OUT FORWARD                          |
| 11. PPTP Out                         | OUT FORWARD                          |
| 12. L2TP Out                         | OUT FORWARD                          |
| 13. ICMP Out                         | OUT FORWARD                          |
| 14. VRRP Out                         | OUT FORWARD                          |
| 15. NAT-T Out                        | OUT FORWARD                          |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3K: Filters -> 1
```

```
                              Current Filter Rules
-------------------------------------------------------------------------------
| 1. GRE In                              | 2. GRE Out                          |
| 3. IPSEC-ESP In                        | 4. IKE In                           |
| 5. IKE Out                             | 6. PPTP In                          |
| 7. PPTP Out                            | 8. L2TP In                          |
| 9. L2TP Out                            | 10. ICMP In                         |
| 11. ICMP Out                           | 12. RIP In                          |
| 13. RIP Out                            | 14. OSPF In                         |
| 15. OSPF Out                           | 16. Incoming HTTP In                |
| 17. Incoming HTTP Out                  | 18. VRRP In                         |
| 19. VRRP Out                           | 20. Any In                          |
| 21. Any Out                            | 22. Incoming HTTPS In               |
| 23. Incoming HTTPS Out                 | 24. LDAP In                         |
| 25. LDAP Out                           | 26. Telnet/SSL In                   |
| 27. Telnet/SSL Out                     | 28. Outgoing HTTP In                |
| 29. Outgoing HTTP Out                  | 30. Outgoing HTTPS In               |
| 31. Outgoing HTTPS Out                 | 32. CRL over LDAP In                |
| 33. CRL over LDAP Out                  | 34. SSH In                          |
| 35. SSH Out                            | 36. VCA In                          |
| 37. VCA Out                            | 38. NAT-T In                        |
| 39. NAT-T Out                          | 40. DHCP In                         |
| 41. DHCP Out                           |                                     |
-------------------------------------------------------------------------------

> Which Rule to add

VPN3K: Filters -> 12

                        The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. GRE In                              | IN FORWARD                          |
| 2. IPSEC-ESP In                        | IN FORWARD                          |
| 3. IKE In                              | IN FORWARD                          |
| 4. PPTP In                             | IN FORWARD                          |
| 5. L2TP In                             | IN FORWARD                          |
| 6. ICMP In                             | IN FORWARD                          |
| 7. VRRP In                             | IN FORWARD                          |
| 8. NAT-T In                            | IN FORWARD                          |
| 9. GRE Out                             | OUT FORWARD                         |
| 10. IKE Out                            | OUT FORWARD                         |
| 11. PPTP Out                           | OUT FORWARD                         |
| 12. L2TP Out                           | OUT FORWARD                         |
| 13. ICMP Out                           | OUT FORWARD                         |
| 14. VRRP Out                           | OUT FORWARD                         |
| 15. NAT-T Out                          | OUT FORWARD                         |
| 16. RIP In                             | IN FORWARD                          |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3K: Filters -> 1

                              Current Filter Rules
-------------------------------------------------------------------------------
| 1. GRE In                              | 2. GRE Out                          |
| 3. IPSEC-ESP In                        | 4. IKE In                           |
| 5. IKE Out                             | 6. PPTP In                          |
```

```
| 7. PPTP Out                          | 8. L2TP In                          |
| 9. L2TP Out                          | 10. ICMP In                         |
| 11. ICMP Out                         | 12. RIP In                          |
| 13. RIP Out                          | 14. OSPF In                         |
| 15. OSPF Out                         | 16. Incoming HTTP In                |
| 17. Incoming HTTP Out                | 18. VRRP In                         |
| 19. VRRP Out                         | 20. Any In                          |
| 21. Any Out                          | 22. Incoming HTTPS In               |
| 23. Incoming HTTPS Out               | 24. LDAP In                         |
| 25. LDAP Out                         | 26. Telnet/SSL In                   |
| 27. Telnet/SSL Out                   | 28. Outgoing HTTP In                |
| 29. Outgoing HTTP Out                | 30. Outgoing HTTPS In               |
| 31. Outgoing HTTPS Out               | 32. CRL over LDAP In                |
| 33. CRL over LDAP Out                | 34. SSH In                          |
| 35. SSH Out                          | 36. VCA In                          |
| 37. VCA Out                          | 38. NAT-T In                        |
| 39. NAT-T Out                        | 40. DHCP In                         |
| 41. DHCP Out                         |                                     |
-------------------------------------------------------------------------------

> Which Rule to add

VPN3K: Filters -> 13

                       The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. GRE In                            | IN FORWARD                          |
| 2. IPSEC-ESP In                      | IN FORWARD                          |
| 3. IKE In                            | IN FORWARD                          |
| 4. PPTP In                           | IN FORWARD                          |
| 5. L2TP In                           | IN FORWARD                          |
| 6. ICMP In                           | IN FORWARD                          |
| 7. VRRP In                           | IN FORWARD                          |
| 8. NAT-T In                          | IN FORWARD                          |
| 9. GRE Out                           | OUT FORWARD                         |
| 10. IKE Out                          | OUT FORWARD                         |
| 11. PPTP Out                         | OUT FORWARD                         |
| 12. L2TP Out                         | OUT FORWARD                         |
| 13. ICMP Out                         | OUT FORWARD                         |
| 14. VRRP Out                         | OUT FORWARD                         |
| 15. NAT-T Out                        | OUT FORWARD                         |
| 16. RIP In                           | IN FORWARD                          |
| 17. RIP Out                          | OUT FORWARD                         |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3K: Filters ->
```

Configure static route to 150.1.0.0/24:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
```

```
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 2

1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back

VPN3K: System -> 3

1) Static Routes
2) Default Gateways
3) OSPF
4) OSPF Areas
5) DHCP Parameters
6) Redundancy
7) Reverse Route Injection
8) DHCP Relay
9) Back

VPN3K: Routing -> 1

Static Routes
-------------
Destination     Mask            Metric Destination
------------------------------------------------------------
No Static Routes Configured

1) Add Static Route
2) Modify Static Route
3) Delete Static Route
4) Back

VPN3K: Routing -> 1

> Net Address

VPN3K: Routing -> 150.1.1.0

> Subnet Mask

VPN3K: Routing -> 255.255.255.0

1) Destination is Router
2) Destination is Interface

VPN3K: Routing -> 1
```

```
> Router Address

VPN3K: Routing -> 136.1.111.1

> Route Metric (1 - 16)

VPN3K: Routing -> [ 1 ]

Static Routes
-------------
Destination     Mask            Metric Destination
------------------------------------------------------------
150.1.1.0       255.255.255.0        1 136.1.111.1

1) Add Static Route
2) Modify Static Route
3) Delete Static Route
4) Back

VPN3K: Routing ->
```

Permit management from outside via HTTPs:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|      UP      |   136.1.121.11/255.255.255.0  | 00.03.A0.88.BD.2A
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

VPN3K: Interfaces -> 2

1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
```

```
3) Set Interface Name
4) Select IP Filter
5) Select Ethernet Speed
6) Select Duplex
7) Set MTU
8) Set Port Routing Config
9) Set Bandwidth Management
10) Set Public Interface IPSec Fragmentation Policy
11) Set Interface WebVPN Parameters
12) Back

VPN3K: Ethernet Interface 2 -> 11

1) Enable/Disable HTTP and HTTPS Management
2) Enable/Disable HTTPS WebVPN
3) Enable/Disable POP3S
4) Enable/Disable IMAP4S
5) Enable/Disable SMTPS
6) Enable/Disable HTTP Redirect
7) Back

VPN3K: Ethernet Interface 2 -> 1

1) Enable HTTP and HTTPS Management
2) Disable HTTP and HTTPS Management

VPN3K: Ethernet Interface 2 -> [ 2 ] 1


You may save current config for further reference:


1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 2

1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Traceroute
7) Access Rights
8) File Management
9) Certificate Management
10) Back

VPN3K: Admin -> 8

List of Files
-------------
SAVELOG.TXT  CONFIG       CONFIG.SAV   CRSHDUMP.TXT CONFIG.BAK

1) Delete File
2) Copy File
3) View File
4) Put File via TFTP
5) Get File via TFTP
```

```
6) Swap Config Files
7) Export XML File
8) Import XML File
9) Reformat Filesystem
10) Back

VPN3K: File -> 2

> Which File to copy

VPN3K: File -> CONFIG

> File name to copy to

VPN3K: File -> CONFIG.SAV

List of Files
-------------
SAVELOG.TXT  CONFIG       CONFIG.SAV   CRSHDUMP.TXT CONFIG.BAK

1) Delete File
2) Copy File
3) View File
4) Put File via TFTP
5) Get File via TFTP
6) Swap Config Files
7) Export XML File
8) Import XML File
9) Reformat Filesystem
10) Back
```

Verification

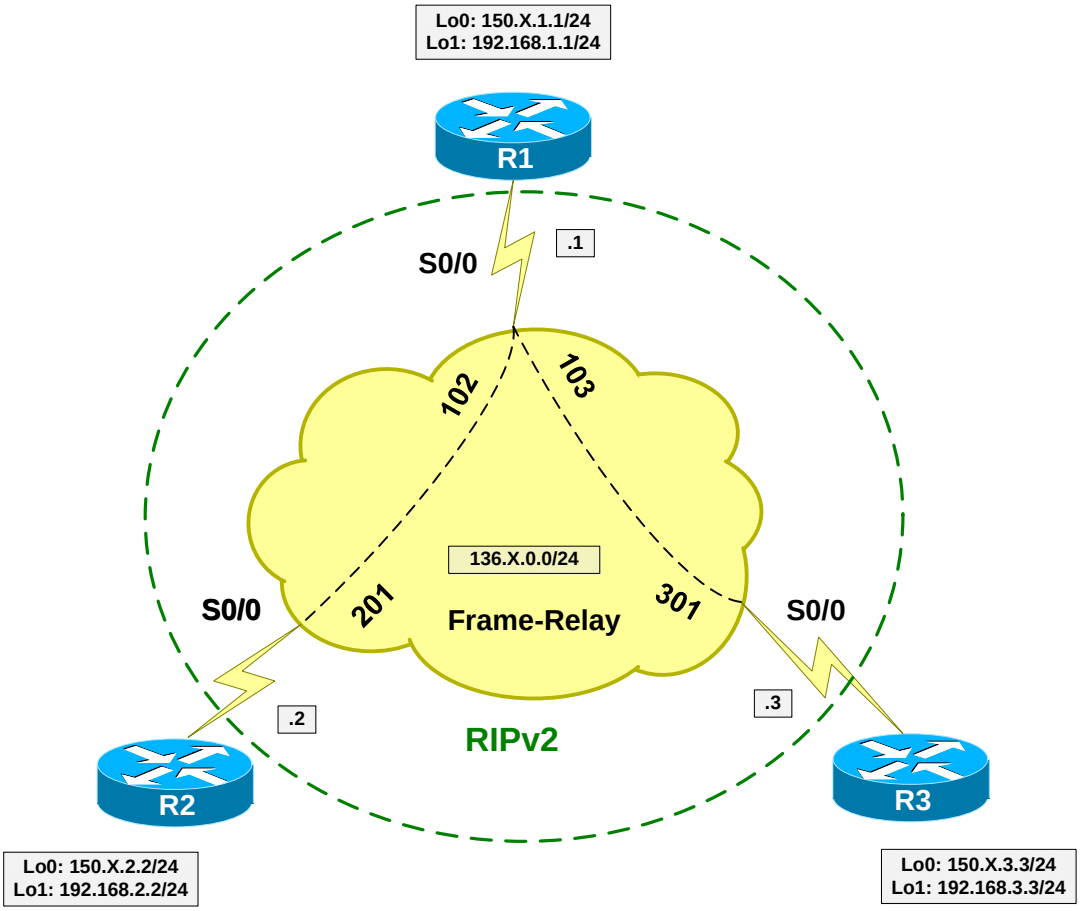
VPN3k:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 3

1) Routing Table
2) Event Log
3) System Status
4) Sessions
5) General Statistics
6) Dynamic Filters
7) Back

VPN3K: Monitor -> 1

Routing Table
-------------
Number of Routes: 5
   IP Address         Mask          Next Hop    Intf Protocol Age Metric
-----------------------------------------------------------------------
10.0.0.0        255.255.255.0   136.1.121.12       2 RIP       28      2
```

```
136.1.111.0     255.255.255.0   0.0.0.0            1 Local      0      1
136.1.121.0     255.255.255.0   0.0.0.0            2 Local      0      1
136.1.122.0     255.255.255.0   136.1.121.12       2 RIP       28      2
150.1.1.0       255.255.255.0   136.1.111.1        1 Static     0      1

1) Refresh Routing Table
2) Clear Routing Table
3) Back

VPN3K: Routing ->

ASA1(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    136.1.111.0 255.255.255.0 [120/1] via 136.1.121.11, 0:00:19, inside
C    136.1.121.0 255.255.255.0 is directly connected, inside
C    136.1.122.0 255.255.255.0 is directly connected, outside
C    10.0.0.0 255.255.255.0 is directly connected, dmz
R    150.1.1.0 255.255.255.0 [120/1] via 136.1.121.11, 0:00:19, inside

R2#show ip route rip
     136.1.0.0/24 is subnetted, 3 subnets
R       136.1.111.0 [120/2] via 136.1.122.12, 00:00:27, Ethernet0/0
R       136.1.121.0 [120/1] via 136.1.122.12, 00:00:27, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/1] via 136.1.122.12, 00:00:27, Ethernet0/0
     150.1.0.0/24 is subnetted, 1 subnets
R       150.1.1.0 [120/2] via 136.1.122.12, 00:00:27, Ethernet0/0

R1#ping 136.1.111.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.111.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 150.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

GRE and DMVPN

Objective: Configure common L2/L3 settings for DMVPN and GRE scenarios.



Directions

- Configure Loopback interfaces as per the diagram.
- Configure Frame-Relay interfaces. Use physical interfaces and static mappings on every router.
- R2 should be able to reach R3 via R1. Provide static mappings to make this possible.
- Configure RIP as routing protocol on FR cloud.
- Advertise Loopback0 interfaces into RIP.

Final Configuration

```
R1:
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
```

```
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
!
interface Serial 0/0
  encaps frame
  no frame inverse
  no shut
  frame map ip 136.1.0.2 102 broad
  frame map ip 136.1.0.3 103 broad
  ip add 136.1.0.1 255.255.255.0
!
router rip
  ver 2
  no auto
  net 136.1.0.0
  net 150.1.0.0
```

R2:

```
interface Loopback0
 ip address 150.1.2.2 255.255.255.0
!
interface Loopback1
 ip address 192.168.2.2 255.255.255.0
!
interface Serial 0/0
  encaps frame
  no frame inverse
  no shut
  frame map ip 136.1.0.1 201 broad
  frame map ip 136.1.0.3 201
  ip add 136.1.0.2 255.255.255.0
!
router rip
  ver 2
  no auto
  net 136.1.0.0
  net 150.1.0.0
```

R3:

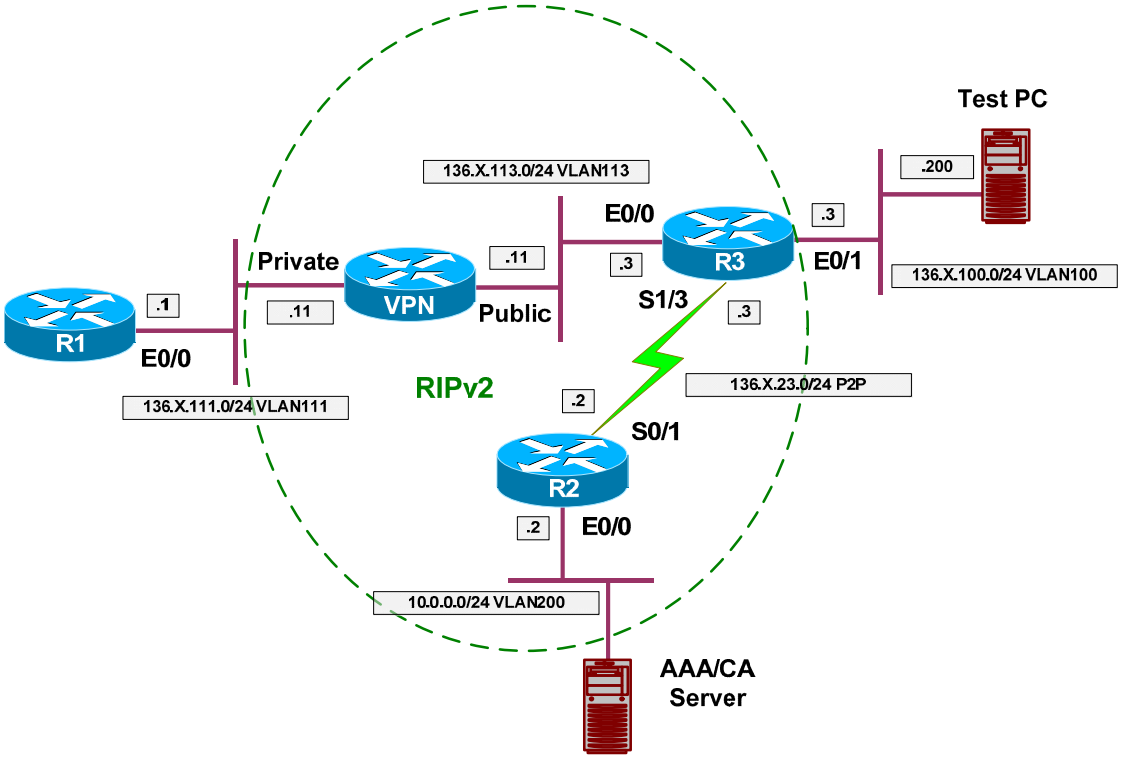
```
interface Loopback0
 ip address 150.1.3.3 255.255.255.0
!
interface Loopback1
 ip address 192.168.3.3 255.255.255.0
!
interface Serial 1/0
  encaps frame
  no frame inverse
  no shut
  frame map ip 136.1.0.1 301 broad
  frame map ip 136.1.0.2 301
  ip add 136.1.0.3 255.255.255.0
!
router rip
  ver 2
  no auto
  net 136.1.0.0
  net 150.1.0.0
```


Verification

```
R1#ping 136.1.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

R1#ping 136.1.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

R1#show ip route rip
     150.1.0.0/24 is subnetted, 3 subnets
R       150.1.3.0 [120/1] via 136.1.0.3, 00:00:13, Serial0/0
R       150.1.2.0 [120/1] via 136.1.0.2, 00:00:06, Serial0/0

R3#show ip route rip
     150.1.0.0/24 is subnetted, 3 subnets
R       150.1.2.0 [120/2] via 136.1.0.2, 00:00:28, Serial1/0
R       150.1.1.0 [120/1] via 136.1.0.1, 00:00:28, Serial1/0

R3#ping 150.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/40 ms
```


VPN3k Easy VPN/WebVPN

Objective: Configure common L2/L3 settings for VPN3k Easy VPN/WebVPN scenarios.



Directions

- Create VLANs 100,111,113, 200 on SW1 and SW2.
- Configure the switchports into respective VLANs.
- Configure HDLC link between R2 and R3.
- Configure IP addressing on routers and VPN3k as per the diagram.
- Configure IP addressing on Test PC.
- Confiture RIP routing on VPN3k. Permit RIP to pass through the Public filter.
- Configure a static default route on R1 and Test PC to point at VPN3k and R3 respectively.
- Configure RIP routing on R2 and R3.

Final Configuration

```
SW1 & SW2:
!
! create VLANs and configure trunk links
!
vlan 100,111,113,200
```

```
!
interface range Fa 0/21 - 23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shut
```

SW1:

```
!
!  Configure switchports
!
interface Fa 0/1
 switchport host
 switchport access vlan 111
!
interface Fa 0/2
 switchport host
 switchport access vlan 200
!
interface Fa 0/3
 switchport host
 switchport access vlan 113
!
interface Fa 0/11
 switchport host
 switchport access vlan 111
!
interface Fa 0/20
 switchport host
 switchport access vlan 200
```

SW2:

```
!
!  Configure switchports
!
interface Fa 0/3
 switchport host
 switchport access vlan 100
!
interface Fa 0/11
 switchport host
 switchport access vlan 113
!
interface Fa 0/20
 switchport host
 switchport access vlan 100
```

R1:

```
interface E 0/0
 no shut
 ip add 136.1.111.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 136.1.111.11
```

R2:

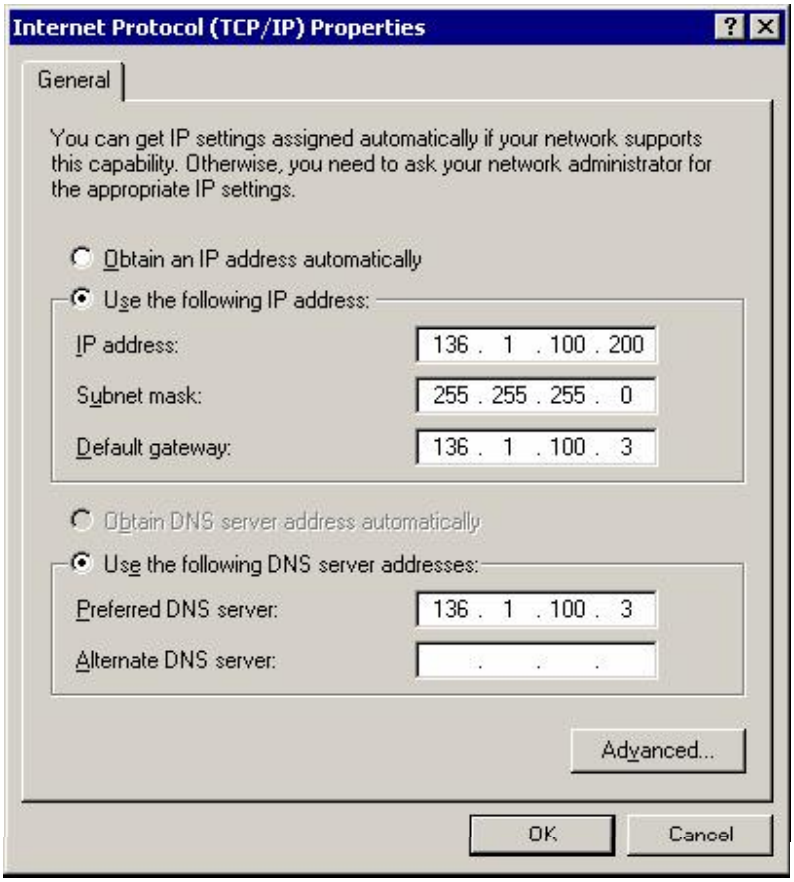
```
interface E 0/0
 no shut
 ip add 10.0.0.2 255.255.255.0
!
interface Ser 0/1
 no shut
 ip address 136.1.23.2 255.255.255.0
!
router rip
```

```
 ver 2
 no auto
 network 136.1.0.0
 network 10.0.0.0
```

R3:

```
interface E 0/0
 no shut
 ip add 136.1.113.3 255.255.255.0
!
interface E 0/1
 no shut
 ip add 136.1.100.3 255.255.255.0
!
interface Ser 1/3
 no shut
 clock rate 64000
 ip address 136.1.23.3 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
```

Test PC:



VPN3k CLI:

Erase present configuration:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 2

1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Traceroute
7) Access Rights
8) File Management
9) Certificate Management
10) Back

VPN3K: Admin -> 3

1) Cancel Scheduled Reboot/Shutdown
2) Schedule Reboot
3) Schedule Shutdown
4) Back

VPN3K: Admin -> 2

1) Save active Configuration and use it at Reboot
2) Reboot without saving active Configuration file
3) Reboot ignoring the Configuration file
4) Back

VPN3K: Admin -> 3

1) Cancel Scheduled Reboot/Shutdown
2) Reboot Now
3) Reboot in X minutes
4) Reboot at time X
5) Reboot wait for sessions to terminate
6) Back

VPN3K: Admin -> 2
```

VPN3k Initial configuration:

```
                Welcome to
               Cisco Systems
       VPN 3000 Concentrator Series
          Command Line Interface
Copyright (C) 1998-2005 Cisco Systems, Inc.



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

 -- : Enter the system time in the following format:
```

```
 -- :       HH:MM:SS.  Example  21:30:00  for 9:30 PM

> Time

Quick -> [ 23:53:38 ]

 -- : Enter the date in the following format.
 -- : MM/DD/YYYY  Example 06/12/1999  for June 12th 1999.

> Date

Quick -> [ 01/17/2007 ]

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

 -- :  Enter the time zone using the hour offset from GMT:
 -- :  -12 : Kwajalein   -11 : Samoa      -10 : Hawaii         -9 : Alaska
 -- :   -8 : PST          -7 : MST         -6 : CST            -5 : EST
 -- :   -4 : Atlantic     -3 : Brasilia  -3.5 : Newfoundland   -1 : Mid-
Atlantic
 -- :   -1 : Azores        0 : GMT         +1 : Paris          +2 : Cairo
 -- :   +3 : Kuwait     +3.5 : Tehran      +4 : Abu Dhabi    +4.5 : Kabul
 -- :   +5 : Karachi    +5.5 : Calcutta +5.75 : Kathmandu      +6 : Almaty
 -- : +6.5 : Rangoon      +7 : Bangkok     +8 : Singapore      +9 : Tokyo
 -- : +9.5 : Adelaide    +10 : Sydney     +11 : Solomon Is.   +12 : Marshall
Is.

> Time Zone

Quick -> [ -8 ]

1) Enable Daylight Savings Time Support
2) Disable Daylight Savings Time Support

Quick -> [ 1 ]

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|Not Configured|        0.0.0.0/0.0.0.0        |
Ether2-Pub|Not Configured|        0.0.0.0/0.0.0.0        |
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

** An address is required for the private interface. **

> Enter IP Address

Quick Ethernet 1 -> [ 0.0.0.0 ] 136.1.111.11

Waiting for Network Initialization...

> Enter Subnet Mask

Quick Ethernet 1 -> [ 255.255.0.0 ] 255.255.255.0

> Enter Interface Name

Quick Ethernet 1 -> Private
```

```
1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick Ethernet 1 -> [ 3 ]

1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick Ethernet 1 -> [ 1 ]

> MTU (68 - 1500)

Quick Ethernet 1 -> [ 1500 ]

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 2

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|Not Configured|        0.0.0.0/0.0.0.0        |
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

> Enter IP Address

Quick Ethernet 2 -> [ 0.0.0.0 ] 136.1.113.11

> Enter Subnet Mask

Quick Ethernet 2 -> [ 255.255.0.0 ] 255.255.255.0

> Enter Interface Name

Quick Ethernet 2 -> Public

1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick Ethernet 2 -> [ 3 ]

1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick Ethernet 2 -> [ 1 ]

> MTU (68 - 1500)

Quick Ethernet 2 -> [ 1500 ]
```

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 4

 -- : Assign a System Name (hostname) to this device.
 -- : This may be required for DHCP.

> System Name

Quick -> VPN3k

 -- : Specify a local DNS server, which lets you enter hostnames
 -- : rather than IP addresses while configuring.

> DNS Server

VPN3k: Quick -> [ 0.0.0.0 ]

 -- : Enter your Internet domain name; e.g., yourcompany.com

> Domain

VPN3k: Quick ->

> Default Gateway

VPN3k: Quick ->

-- : Configure protocols and encryption options.
-- : This table shows current protocol settings

         PPTP         |        L2TP         |
----------------------------------------------
|       Enabled       |       Enabled       |
|  No Encryption Req  |  No Encryption Req  |
----------------------------------------------

1) Enable  PPTP
2) Disable PPTP

VPN3k: Quick -> [ 1 ]

1) PPTP Encryption Required
2) No Encryption Required

VPN3k: Quick -> [ 2 ]

1) Enable  L2TP
2) Disable L2TP

VPN3k: Quick -> [ 1 ]

1) L2TP Encryption Required
2) No Encryption Required

VPN3k: Quick -> [ 2 ]

1) Enable  IPSec
```

```
2) Disable IPSec

VPN3k: Quick -> [ 1 ]

1) Enable  WebVPN
2) Disable WebVPN

VPN3k: Quick -> [ 1 ] 2

-- : Configure address assignment for PPTP, L2TP and IPSec.

1) Enable Client Specified Address Assignment
2) Disable Client Specified Address Assignment

VPN3k: Quick -> [ 2 ]

1) Enable Per User Address Assignment
2) Disable Per User Address Assignment

VPN3k: Quick -> [ 2 ]

1) Enable DHCP Address Assignment
2) Disable DHCP Address Assignment

VPN3k: Quick -> [ 2 ]

1) Enable Configured Pool Address Assignment
2) Disable Configured Pool Address Assignment

VPN3k: Quick -> [ 2 ]

-- : Specify how to authenticate users

1) Internal
2) RADIUS
3) NT Domain
4) SDI
5) Kerberos/Active Directory
6) Continue

VPN3k: Quick -> [ 1 ]

                                   Current Users
-------------------------------------------------------------------------------
                                     No Users
-------------------------------------------------------------------------------

1) Add a User
2) Delete a User
3) Continue

VPN3k: Quick -> 3

> IPSec Group Name

VPN3k: Quick ->

-- : We strongly recommend that you change the password for user admin.

> Reset Admin Password

VPN3k: Quick -> [ ***** ]
```

```
Verify ->

1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit

VPN3k: Quick -> 1
```

Permit RIP to pass through Public traffic filter:

```
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3k: Config -> 4

1) Access Hours
2) Traffic Management
3) Group Matching
4) Network Admission Control
5) Back

VPN3k: Policy -> 2

1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back

VPN3k: Traffic -> 4

                            Current Active Filters
-------------------------------------------------------------------------------
| 1. Private (Default)                 | 2. Public (Default)                  |
| 3. External (Default)                | 4. Firewall Filter for VPN Client (De|
-------------------------------------------------------------------------------

1) Add a Filter
2) Modify a Filter
3) Delete a Filter
4) Assign Rules to a Filter
5) Copy a Filter
6) Back

VPN3k: Filters -> 4

> Which Filter to assign Rules to

VPN3k: Filters -> 2

                       The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. GRE In                            | IN FORWARD                           |
| 2. IPSEC-ESP In                      | IN FORWARD                           |
| 3. IKE In                            | IN FORWARD                           |
| 4. PPTP In                           | IN FORWARD                           |
| 5. L2TP In                           | IN FORWARD                           |
```

```
| 6. ICMP In                          | IN FORWARD                          |
| 7. VRRP In                          | IN FORWARD                          |
| 8. NAT-T In                         | IN FORWARD                          |
| 9. GRE Out                          | OUT FORWARD                         |
| 10. IKE Out                         | OUT FORWARD                         |
| 11. PPTP Out                        | OUT FORWARD                         |
| 12. L2TP Out                        | OUT FORWARD                         |
| 13. ICMP Out                        | OUT FORWARD                         |
| 14. VRRP Out                        | OUT FORWARD                         |
| 15. NAT-T Out                       | OUT FORWARD                         |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3k: Filters -> 1

                            Current Filter Rules
-------------------------------------------------------------------------------
| 1. GRE In                           | 2. GRE Out                          |
| 3. IPSEC-ESP In                     | 4. IKE In                           |
| 5. IKE Out                          | 6. PPTP In                          |
| 7. PPTP Out                         | 8. L2TP In                          |
| 9. L2TP Out                         | 10. ICMP In                         |
| 11. ICMP Out                        | 12. RIP In                          |
| 13. RIP Out                         | 14. OSPF In                         |
| 15. OSPF Out                        | 16. Incoming HTTP In                |
| 17. Incoming HTTP Out               | 18. VRRP In                         |
| 19. VRRP Out                        | 20. Any In                          |
| 21. Any Out                         | 22. Incoming HTTPS In               |
| 23. Incoming HTTPS Out              | 24. LDAP In                         |
| 25. LDAP Out                        | 26. Telnet/SSL In                   |
| 27. Telnet/SSL Out                  | 28. Outgoing HTTP In                |
| 29. Outgoing HTTP Out               | 30. Outgoing HTTPS In               |
| 31. Outgoing HTTPS Out              | 32. CRL over LDAP In                |
| 33. CRL over LDAP Out               | 34. SSH In                          |
| 35. SSH Out                         | 36. VCA In                          |
| 37. VCA Out                         | 38. NAT-T In                        |
| 39. NAT-T Out                       | 40. DHCP In                         |
| 41. DHCP Out                        |                                     |
-------------------------------------------------------------------------------

> Which Rule to add

VPN3k: Filters -> 12

                       The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. GRE In                           | IN FORWARD                          |
| 2. IPSEC-ESP In                     | IN FORWARD                          |
| 3. IKE In                           | IN FORWARD                          |
| 4. PPTP In                          | IN FORWARD                          |
| 5. L2TP In                          | IN FORWARD                          |
| 6. ICMP In                          | IN FORWARD                          |
| 7. VRRP In                          | IN FORWARD                          |
| 8. NAT-T In                         | IN FORWARD                          |
| 9. GRE Out                          | OUT FORWARD                         |
| 10. IKE Out                         | OUT FORWARD                         |
| 11. PPTP Out                        | OUT FORWARD                         |
```

```
| 12. L2TP Out                          | OUT FORWARD                          |
| 13. ICMP Out                          | OUT FORWARD                          |
| 14. VRRP Out                          | OUT FORWARD                          |
| 15. NAT-T Out                         | OUT FORWARD                          |
| 16. RIP In                            | IN FORWARD                           |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3k: Filters -> 1

                              Current Filter Rules
-------------------------------------------------------------------------------
| 1. GRE In                             | 2. GRE Out                           |
| 3. IPSEC-ESP In                       | 4. IKE In                            |
| 5. IKE Out                            | 6. PPTP In                           |
| 7. PPTP Out                           | 8. L2TP In                           |
| 9. L2TP Out                           | 10. ICMP In                          |
| 11. ICMP Out                          | 12. RIP In                           |
| 13. RIP Out                           | 14. OSPF In                          |
| 15. OSPF Out                          | 16. Incoming HTTP In                 |
| 17. Incoming HTTP Out                 | 18. VRRP In                          |
| 19. VRRP Out                          | 20. Any In                           |
| 21. Any Out                           | 22. Incoming HTTPS In                |
| 23. Incoming HTTPS Out                | 24. LDAP In                          |
| 25. LDAP Out                          | 26. Telnet/SSL In                    |
| 27. Telnet/SSL Out                    | 28. Outgoing HTTP In                 |
| 29. Outgoing HTTP Out                 | 30. Outgoing HTTPS In                |
| 31. Outgoing HTTPS Out                | 32. CRL over LDAP In                 |
| 33. CRL over LDAP Out                 | 34. SSH In                           |
| 35. SSH Out                           | 36. VCA In                           |
| 37. VCA Out                           | 38. NAT-T In                         |
| 39. NAT-T Out                         | 40. DHCP In                          |
| 41. DHCP Out                          |                                      |
-------------------------------------------------------------------------------

> Which Rule to add

VPN3k: Filters -> 13

                        The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. GRE In                             | IN FORWARD                           |
| 2. IPSEC-ESP In                       | IN FORWARD                           |
| 3. IKE In                             | IN FORWARD                           |
| 4. PPTP In                            | IN FORWARD                           |
| 5. L2TP In                            | IN FORWARD                           |
| 6. ICMP In                            | IN FORWARD                           |
| 7. VRRP In                            | IN FORWARD                           |
| 8. NAT-T In                           | IN FORWARD                           |
| 9. GRE Out                            | OUT FORWARD                          |
| 10. IKE Out                           | OUT FORWARD                          |
| 11. PPTP Out                          | OUT FORWARD                          |
| 12. L2TP Out                          | OUT FORWARD                          |
| 13. ICMP Out                          | OUT FORWARD                          |
| 14. VRRP Out                          | OUT FORWARD                          |
| 15. NAT-T Out                         | OUT FORWARD                          |
| 16. RIP In                            | IN FORWARD                           |
```

```
| 17. RIP Out                          | OUT FORWARD                          |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3k: Filters -> h
```

Configure RIP on Public interface:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3k: Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|      UP      |   136.1.113.11/255.255.255.0  | 00.03.A0.88.BD.2A
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

VPN3k: Interfaces -> 2

1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Set Interface Name
4) Select IP Filter
5) Select Ethernet Speed
6) Select Duplex
7) Set MTU
8) Set Port Routing Config
9) Set Bandwidth Management
10) Set Public Interface IPSec Fragmentation Policy
11) Set Interface WebVPN Parameters
```

```
12) Back

VPN3k: Ethernet Interface 2 -> 8

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 2 -> 1

1) Disable Inbound RIP
2) Enable RIP V1 Inbound
3) Enable RIP V2 Inbound
4) Enable RIP V2/V1 Inbound

VPN3k: Ethernet Interface 2 -> [ 1 ] 3

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 2 -> 2

1) Disable Outbound RIP
2) Enable RIP V1 Outbound
3) Enable RIP V2 Outbound
4) Enable RIP V2/V1 Outbound

VPN3k: Ethernet Interface 2 -> [ 1 ] 3

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 2 ->
```

Enable management on Public interface:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3k: Config -> 1

This table shows current IP addresses.
```

```
  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|      UP      |   136.1.113.11/255.255.255.0  | 00.03.A0.88.BD.2A
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

VPN3k: Interfaces -> 2

1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Set Interface Name
4) Select IP Filter
5) Select Ethernet Speed
6) Select Duplex
7) Set MTU
8) Set Port Routing Config
9) Set Bandwidth Management
10) Set Public Interface IPSec Fragmentation Policy
11) Set Interface WebVPN Parameters
12) Back

VPN3k: Ethernet Interface 2 -> 11

1) Enable/Disable HTTP and HTTPS Management
2) Enable/Disable HTTPS WebVPN
3) Enable/Disable POP3S
4) Enable/Disable IMAP4S
5) Enable/Disable SMTPS
6) Enable/Disable HTTP Redirect
7) Back

VPN3k: Ethernet Interface 2 -> 1

1) Enable HTTP and HTTPS Management
2) Disable HTTP and HTTPS Management

VPN3k: Ethernet Interface 2 -> [ 2 ] 1

1) Enable/Disable HTTP and HTTPS Management
2) Enable/Disable HTTPS WebVPN
3) Enable/Disable POP3S
4) Enable/Disable IMAP4S
5) Enable/Disable SMTPS
6) Enable/Disable HTTP Redirect
7) Back

VPN3k: Ethernet Interface 2 ->
```

Verification

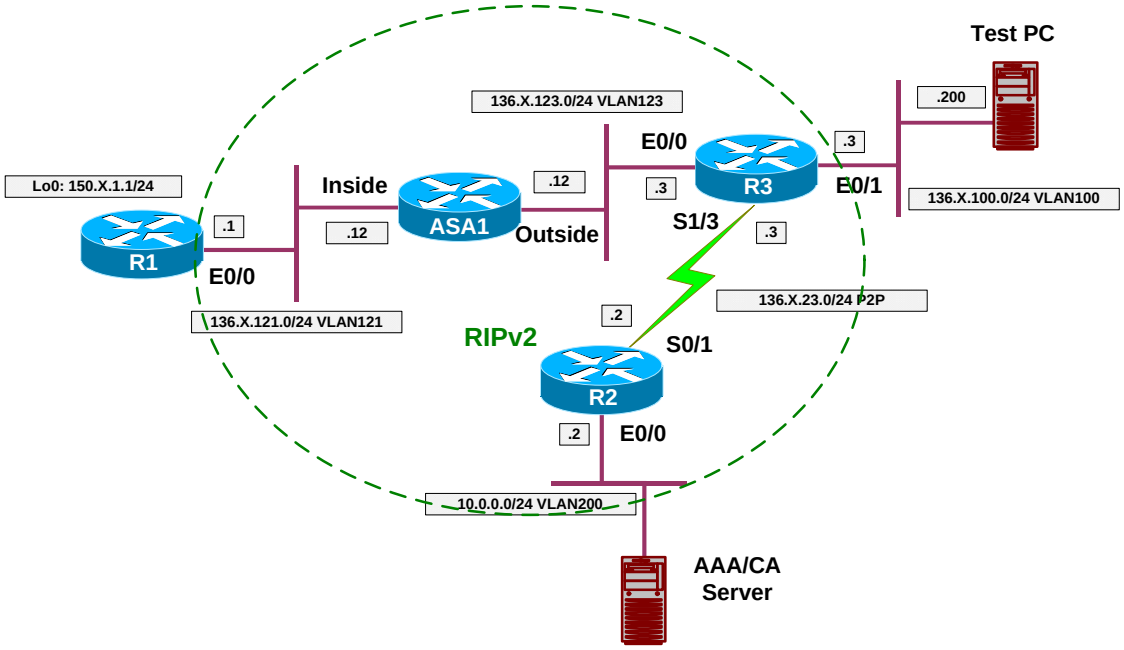
```
R3#ping 136.1.113.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.113.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R3#show ip route rip
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/1] via 136.1.23.2, 00:00:00, Serial1/3
R       136.1.111.0 [120/1] via 136.1.113.11, 00:00:05, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/1] via 136.1.23.2, 00:00:00, Serial1/3
     150.1.0.0/24 is subnetted, 1 subnets
R       150.1.2.0 [120/1] via 136.1.23.2, 00:00:00, Serial1/3
```

VPN3k CLI:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 3

1) Routing Table
2) Event Log
3) System Status
4) Sessions
5) General Statistics
6) Dynamic Filters
7) Back

VPN3k: Monitor -> 1

Routing Table
-------------
Number of Routes: 7
   IP Address         Mask          Next Hop    Intf Protocol Age Metric
-----------------------------------------------------------------------------
10.0.0.0        255.255.255.0   136.1.113.3        2 RIP       13      3
136.1.0.0       255.255.255.0   136.1.113.3        2 RIP       13      3
136.1.23.0      255.255.255.0   136.1.113.3        2 RIP       13      2
136.1.100.0     255.255.255.0   136.1.113.3        2 RIP       13      2
136.1.111.0     255.255.255.0   0.0.0.0            1 Local      0      1
136.1.113.0     255.255.255.0   0.0.0.0            2 Local      0      1
150.1.2.0       255.255.255.0   136.1.113.3        2 RIP       13      3

1) Refresh Routing Table
2) Clear Routing Table
3) Back

VPN3k: Routing ->
```

IOS Easy VPN

Objective: Configure common L2/L3 setting for IOS Easy VPN scenarios.



Directions

- Create VLANs 100,200,121,123 on SW1 & SW2.
- Configure the switchports into respective VLANs.
- Configure serial HDLC link between R2 and R3.
- Configure IP addressing as per the diagram.
- Configure RIP as routing protocol on R1, R2, R3, and ASA1.
- Configure the ASA to permit inbound IKE/ESP.

Final Configuration

```
SW1 & SW2:
!
! create VLANs and configure trunk links
!
vlan 100,121,123,200
!
interface range Fa 0/21 - 23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shut

SW1:
!
!  Configure switchports
!
interface Fa 0/1
```

```
 switchport host
 switchport access vlan 121
!
interface Fa 0/2
 switchport host
 switchport access vlan 200
!
interface Fa 0/3
 switchport host
 switchport access vlan 123
!
interface Fa 0/12
 switchport host
 switchport access vlan 121
!
interface Fa 0/20
 switchport host
 switchport access vlan 200
```

SW2:

```
!
!  Configure switchports
!
interface Fa 0/3
 switchport host
 switchport access vlan 100
!
interface Fa 0/12
 switchport host
 switchport access vlan 123
!
interface Fa 0/20
 switchport host
 switchport access vlan 100
```

R1:

```
interface E 0/0
 no shut
 ip add 136.1.121.1 255.255.255.0
!
interface Loopback0
 ip add 150.1.1.1 255.255.255.0
!
router rip
 version 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
```

R2:

```
interface E 0/0
 no shut
 ip add 10.0.0.2 255.255.255.0
!
interface Ser 0/1
 no shut
 ip address 136.1.23.2 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 10.0.0.0
```

```
R3:
interface E 0/0
 no shut
 ip add 136.1.123.3 255.255.255.0
!
interface E 0/1
 no shut
 ip add 136.1.100.3 255.255.255.0
!
interface Ser 1/3
 no shut
 clock rate 64000
 ip address 136.1.23.3 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0

ASA1:
!
! IP addressing
!
interface Ethernet0/0
 no shut
 nameif outside
 security-level 0
 ip address 136.1.123.12 255.255.255.0
!
interface Ethernet0/1
 no shut
 nameif inside
 security-level 100
 ip address 136.1.121.12 255.255.255.0
!
! RIP configuration
!
router rip
 version 2
 no auto-summary
 network 136.1.0.0
!
! Permit Inbound IKE/ESP
!
access-list OUTSIDE_IN permit udp any any eq 500
access-list OUTSIDE_IN permit esp any any
!
access-group OUTSIDE_IN in interface outside
```

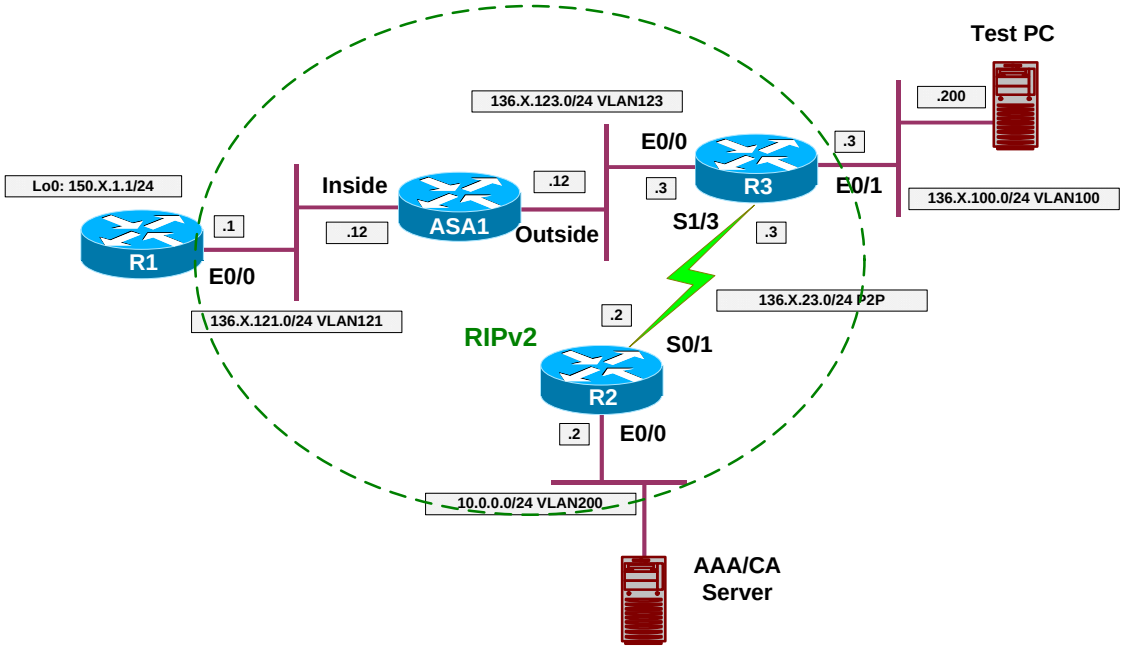
Verification

```
R1#show ip route  rip
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/3] via 136.1.121.12, 00:00:21, Ethernet0/0
R       136.1.23.0 [120/2] via 136.1.121.12, 00:00:21, Ethernet0/0
R       136.1.100.0 [120/2] via 136.1.121.12, 00:00:21, Ethernet0/0
R       136.1.123.0 [120/1] via 136.1.121.12, 00:00:21, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/3] via 136.1.121.12, 00:00:21, Ethernet0/0
```

```
R3#show ip route rip
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/1] via 136.1.23.2, 00:00:11, Serial1/3
R       136.1.121.0 [120/1] via 136.1.123.12, 00:00:23, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/1] via 136.1.23.2, 00:00:11, Serial1/3
     150.1.0.0/24 is subnetted, 1 subnets
R       150.1.1.0 [120/2] via 136.1.123.12, 00:00:23, Ethernet0/0

R2#show ip route  rip
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.100.0 [120/1] via 136.1.23.3, 00:00:21, Serial0/1
R       136.1.121.0 [120/2] via 136.1.23.3, 00:00:21, Serial0/1
R       136.1.123.0 [120/1] via 136.1.23.3, 00:00:21, Serial0/1
     150.1.0.0/24 is subnetted, 2 subnets
R       150.1.1.0 [120/3] via 136.1.23.3, 00:00:04, Serial0/1
```


PIX/ASA Easy VPN/WebVPN

Objective: Configure common L2/L3 setting for the PIX/ASA Easy VPN/WebVPN scenarios.



Directions

- Create VLANs 100,200,121,123 on SW1 & SW2.
- Configure the switchports into respective VLANs.
- Configure serial HDLC link between R2 and R3.
- Configure IP addressing as per the diagram.
- Configure RIP as routing protocol on R1, R2, R3, and ASA1.

Final Configuration

```
SW1 & SW2:
!
! create VLANs and configure trunk links
!
vlan 100,121,123,200
!
interface range Fa 0/21 - 23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shut

SW1:
!
!  Configure switchports
!
interface Fa 0/1
```

```
 switchport host
 switchport access vlan 121
!
interface Fa 0/2
 switchport host
 switchport access vlan 200
!
interface Fa 0/3
 switchport host
 switchport access vlan 123
!
interface Fa 0/12
 switchport host
 switchport access vlan 121
!
interface Fa 0/20
 switchport host
 switchport access vlan 200
```

SW2:

```
!
!  Configure switchports
!
interface Fa 0/3
 switchport host
 switchport access vlan 100
!
interface Fa 0/12
 switchport host
 switchport access vlan 123
!
interface Fa 0/20
 switchport host
 switchport access vlan 100
```

R1:

```
interface E 0/0
 no shut
 ip add 136.1.121.1 255.255.255.0
!
interface Loopback0
 ip add 150.1.1.1 255.255.255.0
!
router rip
 version 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
```

R2:

```
interface E 0/0
 no shut
 ip add 10.0.0.2 255.255.255.0
!
interface Ser 0/1
 no shut
 ip address 136.1.23.2 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 10.0.0.0
```

```
R3:
interface E 0/0
 no shut
 ip add 136.1.123.3 255.255.255.0
!
interface E 0/1
 no shut
 ip add 136.1.100.3 255.255.255.0
!
interface Ser 1/3
 no shut
 clock rate 64000
 ip address 136.1.23.3 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0

ASA1:
!
! IP addressing
!
interface Ethernet0/0
 no shut
 nameif outside
 security-level 0
 ip address 136.1.123.12 255.255.255.0
!
interface Ethernet0/1
 no shut
 nameif inside
 security-level 100
 ip address 136.1.121.12 255.255.255.0
!
! RIP configuration
!
router rip
 version 2
 no auto-summary
 network 136.1.0.0
```

Verification

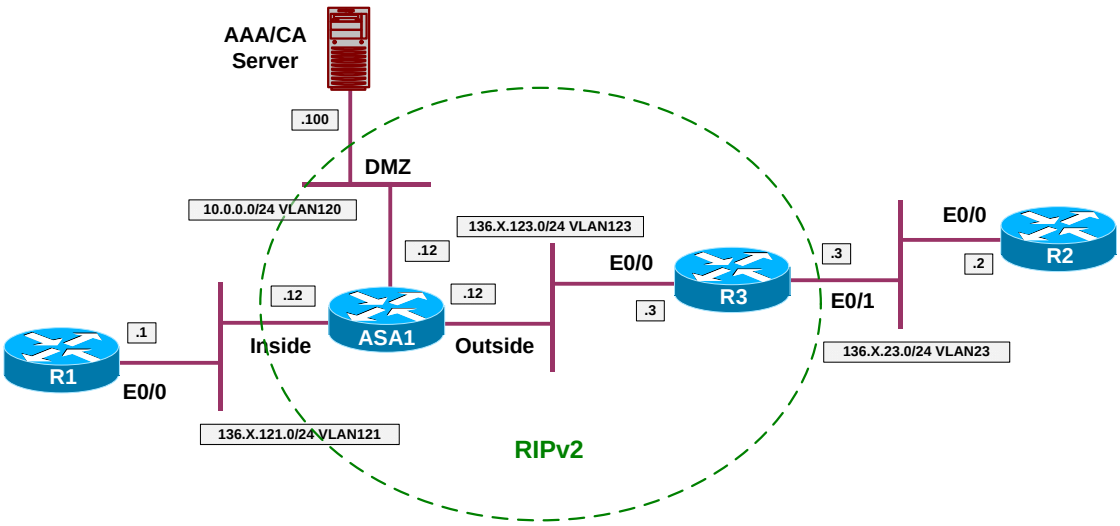
```
R1#show ip route  rip
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/3] via 136.1.121.12, 00:00:21, Ethernet0/0
R       136.1.23.0 [120/2] via 136.1.121.12, 00:00:21, Ethernet0/0
R       136.1.100.0 [120/2] via 136.1.121.12, 00:00:21, Ethernet0/0
R       136.1.123.0 [120/1] via 136.1.121.12, 00:00:21, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/3] via 136.1.121.12, 00:00:21, Ethernet0/0

R3#show ip route rip
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/1] via 136.1.23.2, 00:00:11, Serial1/3
R       136.1.121.0 [120/1] via 136.1.123.12, 00:00:23, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/1] via 136.1.23.2, 00:00:11, Serial1/3
     150.1.0.0/24 is subnetted, 1 subnets
```

```
R       150.1.1.0 [120/2] via 136.1.123.12, 00:00:23, Ethernet0/0

R2#show ip route  rip
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.100.0 [120/1] via 136.1.23.3, 00:00:21, Serial0/1
R       136.1.121.0 [120/2] via 136.1.23.3, 00:00:21, Serial0/1
R       136.1.123.0 [120/1] via 136.1.23.3, 00:00:21, Serial0/1
     150.1.0.0/24 is subnetted, 2 subnets
R       150.1.1.0 [120/3] via 136.1.23.3, 00:00:04, Serial0/1
```


IPsec LAN-to-LAN

IOS and the PIX/ASA with PSK

Objective: Configure IPsec L2L tunnel between the ASA firewall and IOS router using pre-shared key for authentication.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "IOS Router and the PIX/ASA".
- Configure L2L VPN on the ASA Firewall.
    - Create ISAKMP policy with priority 10 as follows:
        - Use 3DES encryption.
        - Use MD5 hash.
        - Use DH Group2.
        - Use Pre-Shared keys authentication.
    - Enable ISAKMP policy on the outside interface.
    - Create L2L tunnel-group with name "136.1.123.3" and configure pre-shared key "CISCO".
    - Create access-list VLAN121_TO_VLAN23 to match traffic from VLAN23 to VLAN121.
    - Create transform-set 3DES_MD5 as follows:
        - Use 3DES cipher

        - Use MD5 hash

    - Create crypto map VPN of type IPsec-ISAKMP as follows:

        - Match access-list VLAN121_TO_VLAN23.
        - Set peer ip 136.1.123.3.
        - Set transform-set 3DES_MD5.

    - Apply crypto map VPN to outside interface.
    - Enable VPN traffic to bypass ACL check.

- Configure L2L VPN on R3 as follows:

    - Create ISAKMP policy with priority 10 as follows.

        - Use 3DES encryption.
        - Use MD5 hash.
        - Use DH Group2.
        - Use Pre-Shared keys authentication.

    - Configure pre-shared ISAKMP key “CISCO” for IP 136.1.123.3.
    - Create access-list VLAN23_TO_VLAN121 to match traffic from VLAN23 to VLAN121
    - Create transform-set 3DES_MD5 as follows:

        - Use 3DES cipher
        - Use MD5 hash

    - Create crypto map VPN of type IPsec-ISAKMP as follows:

        - Match access-list VLAN23_TO_VLAN121
        - Set peer ip 136.1.123.12
        - Set transform-set 3DES_MD5

    - Apply crypto map VPN to interface Eth 0/0.

Final Configuration

```
ASA1:
!
! Configure & Enable ISAKMP policy
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
!
crypto isakmp enable outside
```

```
!
! Configure tunnel group for L2L tunnel
!
tunnel-group 136.1.123.3 type ipsec-l2l
tunnel-group 136.1.123.3 ipsec-attributes
 pre-shared-key CISCO
!
! Configure transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-list to classify traffic for encryption
!
access-list VLAN121_TO_VLAN23 permit ip 136.1.121.0 255.255.255.0 136.1.23.0
255.255.255.0
!
! Configure crypto-map
!
crypto map VPN 10 match address VLAN121_TO_VLAN23
crypto map VPN 10 set peer 136.1.123.3
crypto map VPN 10 set transform-set 3DES_MD5
!
! Apply crypto-map and enable VPN traffic to bypass ACLs
!
crypto map VPN interface outside
sysopt connection permit-vpn
```

R3:

```
!
! Configure ISAKMP policy
!
crypto isakmp policy 10
 encryption 3des
 auth pre-share
 hash md5
 group 2
!
crypto isakmp key CISCO address 136.1.123.12
!
! Create transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Create access-list to classify traffic for encryption
!
ip access-list extended VLAN23_TO_VLAN121
 permit ip 136.1.23.0 0.0.0.255 136.1.121.0 0.0.0.255
!
! Create & apply crypto map
!
crypto map VPN 10 ipsec-isakmp
 match address VLAN23_TO_VLAN121
 set transform 3DES_MD5
 set peer 136.1.123.12
!
interface E 0/0
 crypto map VPN
```


Verification

```
R2#ping 136.1.121.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 100/166/189 ms

R3#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
2     136.1.123.3     136.1.123.12             3des md5  psk  2  23:54:52

R3#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.123.3

   protected vrf:
   local  ident (addr/mask/prot/port): (136.1.23.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
   current_peer: 136.1.123.12:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 21, #recv errors 0

     local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.123.12
     path mtu 1500, media mtu 1500
     current outbound spi: 482D0576

     inbound esp sas:
      spi: 0xB0A78AA3(2963770019)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4455492/3285)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x482D0576(1210910070)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4455492/3285)
        IV size: 8 bytes
        replay detection support: Y
```

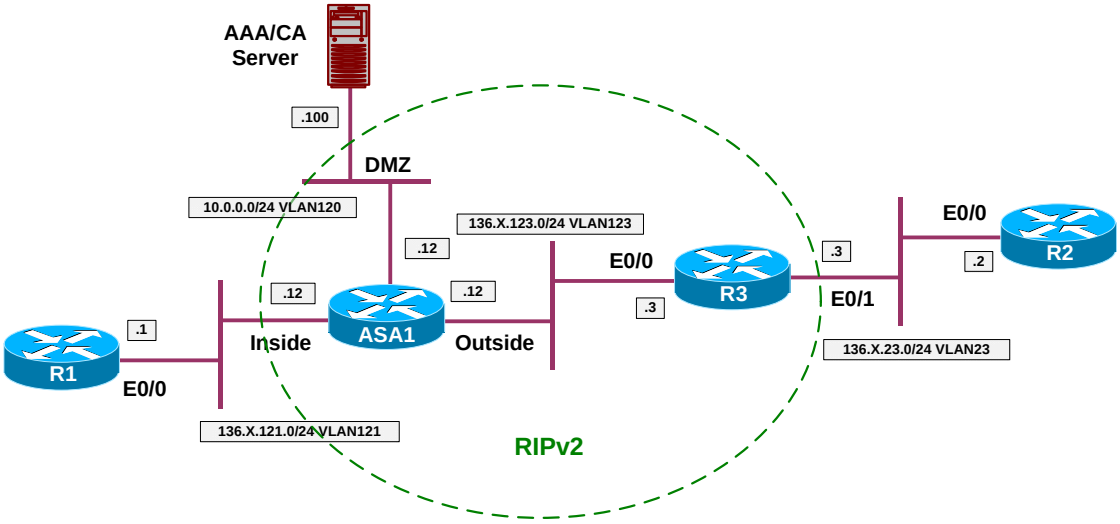
```
     outbound ah sas:

     outbound pcp sas:

ASA1(config)# 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: 136.1.123.3
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

ASA1(config)# show cry ipsec sa
interface: outside
    Crypto map tag: VPN, seq num: 10, local addr: 136.1.123.12

      access-list VLAN121_TO_VLAN23 permit ip 136.1.121.0 255.255.255.0
136.1.23.0 255.255.255.0
      local ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (136.1.23.0/255.255.255.0/0/0)
      current_peer: 136.1.123.3

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 136.1.123.12, remote crypto endpt.: 136.1.123.3

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: B0A78AA3

    inbound esp sas:
      spi: 0x482D0576 (1210910070)
         transform: esp-3des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: VPN
         sa timing: remaining key lifetime (kB/sec): (4274999/3132)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xB0A78AA3 (2963770019)
         transform: esp-3des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: VPN
         sa timing: remaining key lifetime (kB/sec): (4274999/3132)
         IV size: 8 bytes
         replay detection support: Y
```

📖 Further Reading

Configuring LAN-to-LAN IPSec VPNs

IOS and the PIX/ASA with PSK and NAT on the Firewall

Objective: Configure IPsec L2L tunnel between the ASA firewall and IOS router using pre-shared key for authentication. Consider NAT configured for users behind the ASA firewall.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and the PIX/ASA with PSK".
- Enable NAT control on the firewall.
- Configure NAT for inside users, use outside IP for PAT.
- When using NAT with VPN configuration, remember to exempt VPN traffic from NAT.
- Configure NAT exemption for IPsec VPN traffic.
- Use access-list EXEMPT to match traffic from VLAN121 to VLAN23.

Final Configuration

ASA1:

```
nat-control
!
! NAT for inside users
!
nat (inside) 1 0 0
global (outside) 1 interface
!
! Exemption access-list
!
access-list EXEMPT permit ip 136.1.121.0 255.255.255.0 136.1.23.0 255.255.255.0
nat (inside) 0 access-list EXEMPT
```

Verification

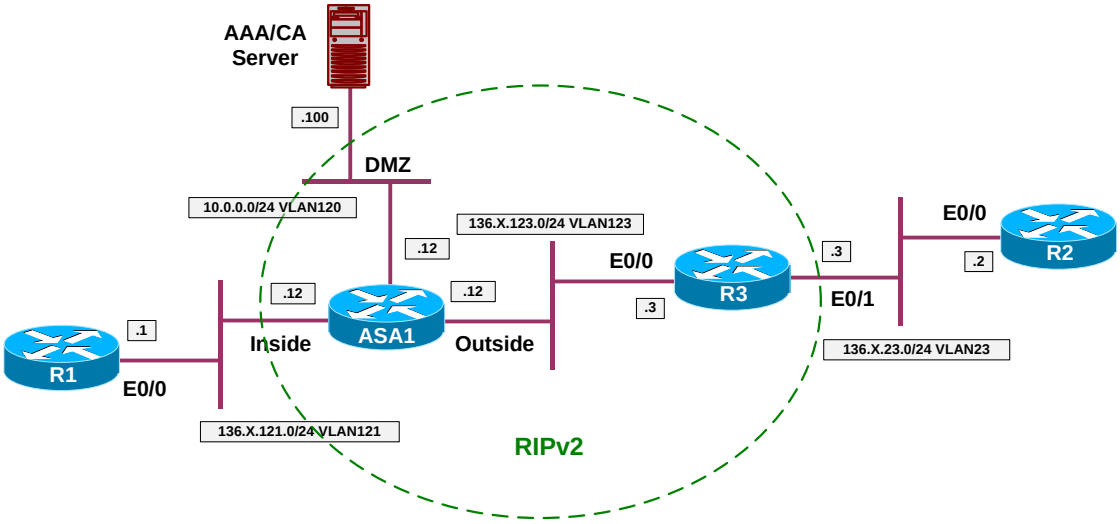
```
R1#telnet 136.1.123.3
Trying 136.1.123.3 ... Open


User Access Verification

Password:
R3>
Rack1AS>12
[Resuming connection 12 to asa1 ... ]

ASA1(config)# show x
1 in use, 10 most used
PAT Global 136.1.123.12(1024) Local 136.1.121.1(11072)

R1#ping 136.1.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.23.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 96/165/189 ms

R1#telnet 136.1.23.2
Trying 136.1.23.2 ... Open


User Access Verification

Password:
R2>

ASA1(config)# show x
0 in use, 10 most used

ASA1(config)# show conn
5 in use, 43 most used
TCP out 136.1.23.2:23 in 136.1.121.1:11073 idle 0:00:52 bytes 111 flags UIO
```

Further Reading

Configuring LAN-to-LAN IPSec VPNs

IOS and the PIX/ASA with Digital Certificates

Objective: Configure L2L VPN tunnel between R3 and the ASA. Use digital certificates for authentication.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "IOS Router and the PIX/ASA".
- Configure CA Truspoint with name IE1 on the ASA as follows:
    - Use enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
    - CRL is optional.
- Enroll the ASA with CA as follows:
    - Configure NTP server to 10.0.0.100.
    - Authenticate the CA.
    - Configure domain-name and create RSA key-pair.
    - Enroll with CA finally.
- Configure L2L VPN on the ASA Firewall as follows.
    - Create ISAKMP policy with priority 10 as follows:
        - Use 3DES encryption.
        - Use MD5 hash.
        - Use DH Group2.
        - Use RSA-SIG authentication.

- Enable ISAKMP policy on the outside interface.
- Create L2L tunnel-group with name “136.1.123.3” and configure trustpoint “IE1”.
- Create access-list VLAN121_TO_VLAN23 to match traffic from VLAN23 to VLAN121.
- Create transform-set 3DES_MD5 as follows:
    - Use 3DES cipher.
    - Use MD5 hash.
- Create crypto map VPN of type IPsec-ISAKMP as follows:
    - Match access-list VLAN121_TO_VLAN23.
    - Set peer ip 136.1.123.3.
    - Set transform-set 3DES_MD5.
- Apply crypto map VPN to outside interface.
- Enable VPN traffic to bypass ACL check.

- Configure CA Truspoint with name IE1 on R3 as follows:
    - Use enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
    - CRL is optional.

- Enroll R3 with CA as follows:
    - Configure NTP server to 10.0.0.100.
    - Authenticate the CA.
    - Configure domain-name and create RSA key-pair.
    - Enroll with CA finally.

- Configure L2L VPN on R3 as follows:
    - Create ISAKMP policy with priority 10 as follows:
        - Use 3DES encryption.
        - Use MD5 hash.
        - Use DH Group2.
        - Use RSA-Sig authentication.
    - Create access-list VLAN23_TO_VLAN121 to match traffic from VLAN23 to VLAN121
    - Create transform-set 3DES_MD5 as follows:
        - Use 3DES cipher.

- Use MD5 hash.

o Create crypto map VPN of type IPsec-ISAKMP as follows:

- Match access-list VLAN23_TO_VLAN121.
- Set peer ip 136.1.123.12.
- Set transform-set 3DES_MD5.

o Apply crypto map VPN to interface Eth 0/0.

Final Configuration

ASA1:

```
!
! Trustpoint configuration
!
crypto ca trustpoint IE1
 enrollment url http://10.0.0.100:80/certsrv/mscep/mscep.dll
 crl optional
!
ntp server 10.0.0.100
!
crypto ca auth IE1
domain-name internetworkexpert.com
crypto key generate rsa general-keys modulus 512
crypto ca enroll IE1

!
! L2L VPN. ISAKMP Configuration
!
crypto isakmp policy 10
 authentication rsa-sig
 encryption 3des
 hash md5
!
crypto isakmp enable outside
!
! Configure tunnel group for L2L tunnel
!
tunnel-group 136.1.123.3 type ipsec-l2l
tunnel-group 136.1.123.3 ipsec-attributes
  trust-point IE1
!
! Configure transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-list to classify traffic for encryption
!
access-list VLAN121_TO_VLAN23 permit ip 136.1.121.0 255.255.255.0 136.1.23.0
255.255.255.0
!
! Configure crypto-map
!
crypto map VPN 10 match address VLAN121_TO_VLAN23
crypto map VPN 10 set peer 136.1.123.3
crypto map VPN 10 set transform-set 3DES_MD5
!
```

```
! Apply crypto-map and enable VPN traffic to bypass ACLs
!
crypto map VPN interface outside
sysopt connection permit-vpn
```

R3:

```
!
! Configure trustpoint
!
crypto ca trustpoint IE1
 enrollment url http://10.0.0.100:80/certsrv/mscep/mscep.dll
 crl optional
!
! Generate keypair and enroll
!
ip domain name internetworkexpert.com
crypto key generate rsa general-keys modulus 512
ntp server 10.0.0.100
crypto ca authenticate IE1
crypto ca enroll IE1
!
! L2L VPN:
! Configure ISAKMP policy
!
crypto isakmp policy 10
 encryption 3des
 auth rsa-sig
 hash md5
 group 2
!
crypto isakmp key CISCO address 136.1.123.12
!
! Create transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Create access-list to classify traffic for encryption
!
ip access-list extended VLAN23_TO_VLAN121
 permit ip 136.1.23.0 0.0.0.255 136.1.121.0 0.0.0.255
!
! Create & apply crypto map
!
crypto map VPN 10 ipsec-isakmp
 match address VLAN23_TO_VLAN121
 set transform 3DES_MD5
 set peer 136.1.123.12
!
interface Eth 0/0
 crypto map VPN
```

Verification

Enroll the ASA with CA:

```
ASA1(config)# crypto ca authenticate IE1

INFO: Certificate has the following attributes:
Fingerprint:     74f95e93 4f8c8af3 5fd15364 8efbb479
Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.

ASA1(config)# crypto key generate rsa general-keys modulus 512
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...

ASA1(config)# crypto ca enroll IE1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco
Re-enter password: cisco


% The fully-qualified domain name in the certificate will be:
ASA1.internetworkexpert.com

% Include the device serial number in the subject name? [yes/no]: no

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ASA1(config)# The certificate has been granted by CA!

ASA1(config)# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 2358cad2000100000026
  Certificate Usage: General Purpose
  Public Key Type: RSA (512 bits)
  Issuer Name:
    cn=IESERVER1
    o=Internetwork Expert
    l=Reno
    st=NV
    c=US
    ea=bmcgahan@internetworkexpert.com
  Subject Name:
    hostname=ASA1.internetworkexpert.com
  CRL Distribution Points:
    [1]  http://ieserver1/CertEnroll/IESERVER1(1).crl
    [2]  file://\\IESERVER1\CertEnroll\IESERVER1(1).crl
  Validity Date:
    start date: 10:07:47 UTC Jan 12 2007
    end   date: 10:17:47 UTC Jan 12 2008
  Associated Trustpoints: IE1

CA Certificate
  Status: Available
  Certificate Serial Number: 6a8b964c37f91bb245b01de2a6363745
  Certificate Usage: Signature
  Public Key Type: RSA (1024 bits)
  Issuer Name:
    cn=IESERVER1
    o=Internetwork Expert
    l=Reno
    st=NV
    c=US
    ea=bmcgahan@internetworkexpert.com
```

```
  Subject Name:
    cn=IESERVER1
    o=Internetwork Expert
    l=Reno
    st=NV
    c=US
    ea=bmcgahan@internetworkexpert.com
  CRL Distribution Points:
    [1]  http://ieserver1/CertEnroll/IESERVER1(1).crl
    [2]  file://\\IESERVER1\CertEnroll\IESERVER1(1).crl
  Validity Date:
    start date: 09:01:58 UTC Jul 21 2006
    end   date: 09:09:34 UTC Jul 21 2008
  Associated Trustpoints: IE1
```

Enroll R3 with CA:

```
R3(config)#crypto ca authenticate IE1
Certificate has the following attributes:
Fingerprint: 74F95E93 4F8C8AF3 5FD15364 8EFBB479
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

R3(config)#crypto ca enroll IE1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: cisco
Re-enter password: cisco

% The fully-qualified domain name in the certificate will be:
R3.internetworkexpert.com
% The subject name in the certificate will be: R3.internetworkexpert.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

R3(config)#    Fingerprint:  4913AF72 E8D4DEC9 01526382 C936CF4D

Jan 12 11:07:54.762: %CRYPTO-6-CERTRET: Certificate received from Certificate
Authority

R3#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 23869E24000100000027
  Certificate Usage: General Purpose
  Issuer:
    CN = IESERVER1
     O = Internetwork Expert
     L = Reno
     ST = NV
     C = US
     EA = bmcgahan@internetworkexpert.com
  Subject:
    Name: R3.internetworkexpert.com
```

```
    OID.1.2.840.113549.1.9.2 = R3.internetworkexpert.com
  CRL Distribution Point:
    http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 10:57:52 UTC Jan 12 2007
    end   date: 11:07:52 UTC Jan 12 2008
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: IE1

CA Certificate
  Status: Available
  Certificate Serial Number: 6A8B964C37F91BB245B01DE2A6363745
  Certificate Usage: Signature
  Issuer:
    CN = IESERVER1
     O = Internetwork Expert
     L = Reno
     ST = NV
     C = US
     EA = bmcgahan@internetworkexpert.com
  Subject:
    CN = IESERVER1
     O = Internetwork Expert
     L = Reno
     ST = NV
     C = US
     EA = bmcgahan@internetworkexpert.com
  CRL Distribution Point:
    http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 09:01:58 UTC Jul 21 2006
    end   date: 09:09:34 UTC Jul 21 2008
  Associated Trustpoints: IE1

R2#ping 136.1.121.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 12/30/48 ms

R3#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.123.3     136.1.123.12             3des md5  rsig 2  23:58:57

R3#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.123.3

   protected vrf:
   local  ident (addr/mask/prot/port): (136.1.23.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
   current_peer: 136.1.123.12:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify 2
```

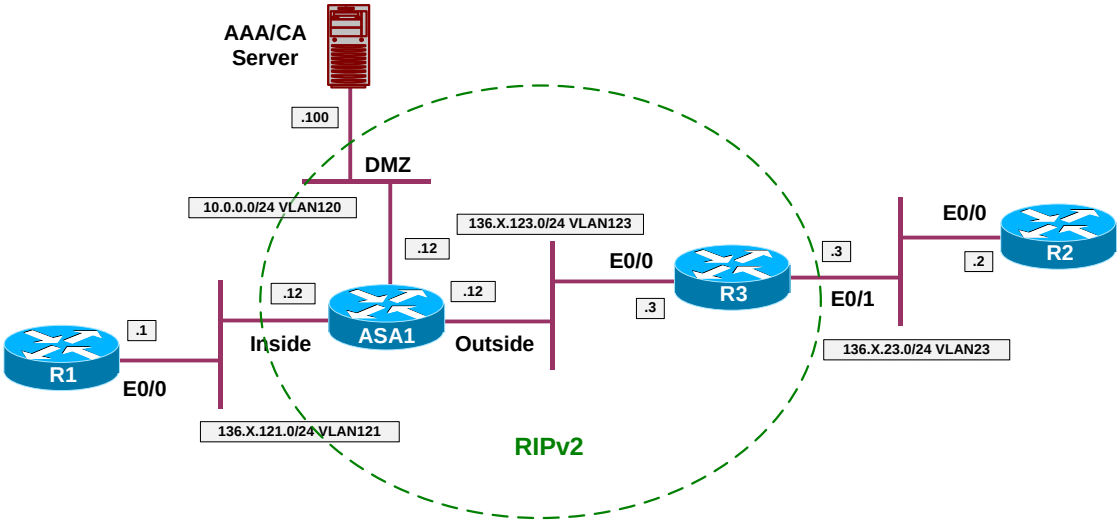
```
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.123.12
     path mtu 1500, media mtu 1500
     current outbound spi: 4A807DEA

     inbound esp sas:
      spi: 0xED9B3EDE(3986374366)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4403363/3534)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4A807DEA(1249934826)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4403363/3534)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

Further Reading

Configuring LAN-to-LAN IPSec VPNs
Configuring Certificates

IOS and the PIX/ASA: Matching Name in Certificate

Objective: Match remote L2L endpoint by hostname in certificate on the PIX/ASA firewall.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and the PIX/ASA with Digital Certificates"
- Clear existing tunnel group "136.1.123.3".
- Create new tunnel-group as follows:
    - Base group-name on FQDN: "R3.internetworkexpert.com".
    - Use trustpoint IE1 for this group.
- Configure ASA1 and R3 to use hostname as identity.

Final Configuration

```
ASA1:
crypto isakmp identity hostname
clear configure tunnel-group
!
tunnel-group R3.internetworkexpert.com type ipsec-l2l
tunnel-group R3.internetworkexpert.com ipsec-attributes
 trust-point IE1

R3:
crypto isakmp identity hostname
```

Verification

Snip from ASA debug output:

```
ASA1# debug crypto isakmp 9

Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, processing ID payload
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, processing cert payload
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, processing RSA signature
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, Computing hash for ISAKMP
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, processing notify payload
Jan 12 13:09:17 [IKEv1]: IP = 136.1.123.3, Trying to find group via OU...
Jan 12 13:09:17 [IKEv1]: IP = 136.1.123.3, No Group found by matching OU(s)
from ID payload:   Unknown
Jan 12 13:09:17 [IKEv1]: IP = 136.1.123.3, Trying to find group via IKE ID...
Jan 12 13:09:17 [IKEv1]: IP = 136.1.123.3, Connection landed on tunnel_group
R3.internetworkexpert.com
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, peer ID type 2 received (FQDN)
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, constructing ID payload
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, constructing cert payload
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, constructing RSA signature
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, Computing hash for ISAKMP

R3#ping 136.1.121.1 source ethernet 0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
Packet sent with a source address of 136.1.23.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms

R3#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.123.3     136.1.123.12             3des md5  rsig 2  23:52:24

R3#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.123.3

   protected vrf:
   local  ident (addr/mask/prot/port): (136.1.23.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
   current_peer: 136.1.123.12:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 12, #recv errors 0
```

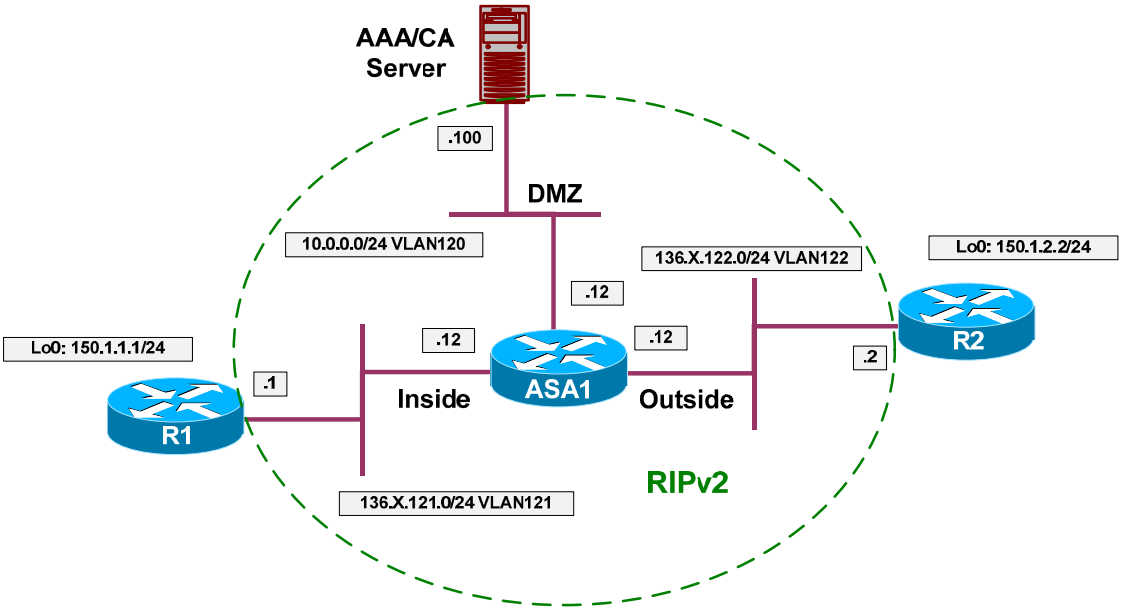
```
local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.123.12
path mtu 1500, media mtu 1500
current outbound spi: A45F614E

inbound esp sas:
 spi: 0xF77C2C21(4152110113)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4546831/3141)
   IV size: 8 bytes
   replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0xA45F614E(2757714254)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4546831/3141)
   IV size: 8 bytes
   replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

📖 Further Reading

Configuring LAN-to-LAN IPSec VPNs
Configuring Certificates

IOS and IOS with PSK Across the PIX/ASA

Objective: Configure IPsec tunnel across the PIX/ASA firewall between two IOS routers with PSK authentication.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration".
- Create two additional loopback interfaces on R1 and R2 as per the diagram, advertise them into RIP.
- Configure access-control on the ASA.
- Create and apply to the outside interface access-list OUTSIDE_IN as follows:
    - Permit ISAKMP traffic from outside.
    - Permit ESP traffic from outside.
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
    - Create ISAKMP policy with priority 10 as follows:
        - Use pre-shared keys authentication.
        - Use 3DES for cipher.
        - Use MD5 for hash.
    - Create ISAKMP key CISCO for address 136.X.122.2 (R2).
    - Create transform-set 3DES_MD5 as follows:

- Use 3DES for cipher.
- Use MD5 for hash.

o Create access-list LO1_TO_LO2 as follows:

- Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.

o Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:

- Match address LO1_TO_LO2.
- Set peer 136.X.122.2.
- Set transform-set 3DES_MD5.

o Apply crypto-map VPN to interface E0/0.

- Configure R2 to mirror R1's configuration.

Final Configuration

```
R1:
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
router rip
 network 150.1.0.0

R2:
interface Loopback0
 ip address 150.1.2.2 255.255.255.0
!
router rip
 network 150.1.0.0

ASA1:
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit esp any any
!
access-group OUTSIDE_IN in interface outside

R1:
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
!
crypto isakmp key CISCO address 136.1.122.2
!
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-List to classify VPN traffic
!
```

```
ip access-list extended LO1_TO_LO2
  permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
!
! Create and apply crypto-map
!
crypto map VPN 10 ipsec-isakmp
 match address LO1_TO_LO2
 set transform 3DES_MD5
 set peer 136.1.122.2
!
interface E 0/0
 crypto map VPN
```

R2:

```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
!
crypto isakmp key CISCO address 136.1.121.1
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
ip access-list extended LO2_TO_LO1
  permit  ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
crypto map VPN 10 ipsec-isakmp
 match address LO2_TO_LO1
 set transform 3DES_MD5
 set peer 136.1.121.1
!
interface E 0/0
 crypto map VPN
```


Verification

```
R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 8/10/12 ms

R2#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.122.2     136.1.121.1              3des md5  psk  1  23:59:27

R2#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify 2
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 13, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.1
     path mtu 1500, media mtu 1500
     current outbound spi: 566119F8

     inbound esp sas:
      spi: 0xE069002C(3764977708)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4517902/3508)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x566119F8(1449204216)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4517902/3508)
        IV size: 8 bytes
```

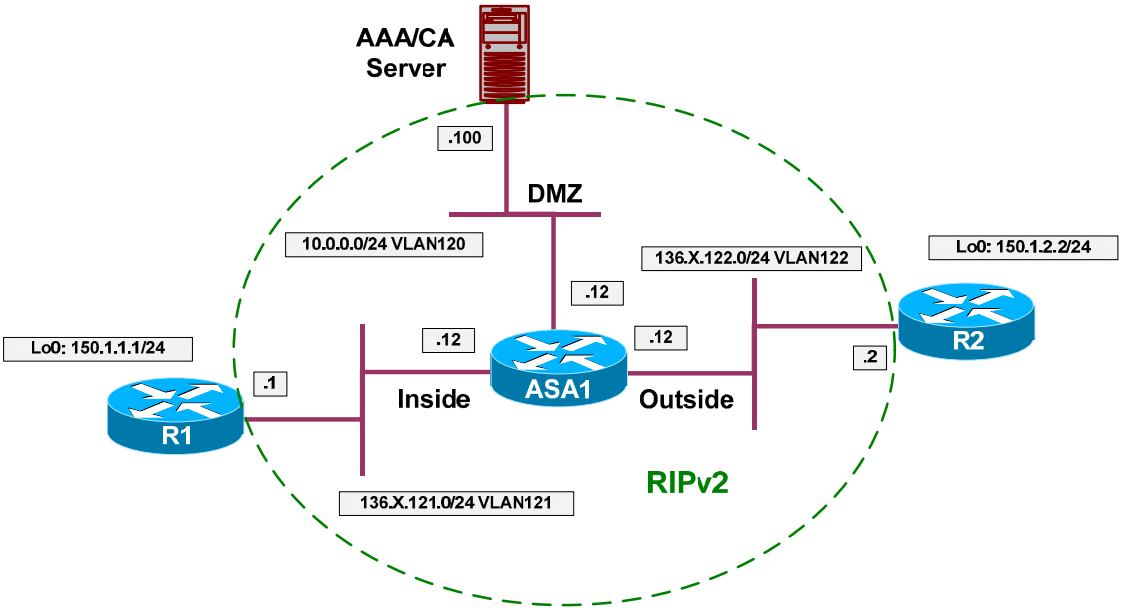
```
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

R1#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.121.1     136.1.122.2              3des md5  psk  1  23:57:54

R1#show cry ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.121.1

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.122.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify 2
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.122.2
     path mtu 1500, media mtu 1500
     current outbound spi: E069002C

     inbound esp sas:
      spi: 0x566119F8(1449204216)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4402011/3469)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xE069002C(3764977708)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4402011/3469)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

Further Reading

Configuring IPSec Network Security
Configuring Internet Key Exchange Security Protocol

IOS and IOS with PSK Across the PIX/ASA and NAT

Objective: Configure IPsec tunnel between two IOS routers across the PIX/ASA firewall with NAT setup.Use PSK for authentication.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration".
- Create two additional loopback interfaces on R1 and R2 as per the diagram, advertise them into RIP.
- Configure NAT on the PIX/ASA firewall as follows:
    - Translate inside networks as they go outside using the outside interface IP address.
    - Enable NAT-Control on the firewall.
- Configure access-control on the ASA as follows:
    - Create and apply to the outside interface access-list OUTSIDE_IN:
        - Permit ISAKMP traffic from outside.
        - Permit NAT-T traffic from outside (UDP 4500).
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
    - Create ISAKMP policy with priority 10 as follows:
        - Use pre-shared keys authentication.
        - Use 3DES for cipher.

        - Use MD5 for hash.

    - Create ISAKMP key CISCO for address 136.X.122.2 (R2).
    - Create transform-set 3DES_MD5 as follows:

        - Use 3DES for cipher.
        - Use MD5 for hash.

    - Create access-list LO1_TO_LO2 as follows:

        - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.

    - Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:

        - Match address LO1_TO_LO2.
        - Set peer 136.X.122.2.
        - Set transform-set 3DES_MD5.

- Configure IPsec L2L tunnel on R2 as follows:

    - Configure ISAKMP just like you did on R1.
    - However, configure wildcard pre-shared ISAKMP key "CISCO" for address 0.0.0.0 0.0.0.0.
    - Create transform-set 3DES_MD5 as follows:

        - Use 3DES for cipher.
        - Use MD5 for hash.

    - Create dynamic crypto-map DYNAMIC entry 10 as follows:

        - Set transform-set 3DES_MD5.

    - Create crypto-map VPN entry 10 of type IPsec-ISAKMP and attach dynamic crypt-map DYNAMIC to it.
    - Apply crypto-map VPN to interface Ethernet 0/0.

Final Configuration

```
R1:
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
router rip
 network 150.1.0.0

R2:
interface Loopback0
 ip address 150.1.2.2 255.255.255.0
!
```

```
router rip
 network 150.1.0.0
```

ASA1:

```
access-list OUTSIDE_IN permit udp any any eq 500
access-list OUTSIDE_IN permit udp any any eq 4500
!
access-group OUTSIDE_IN in interface outside
!
! NAT Configuration
!
nat-control
nat (inside) 1 0 0
global (outside) 1 interface
```

R1:

```
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
!
crypto isakmp key CISCO address 136.1.122.2
!
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-List to classify VPN traffic
!
ip access-list extended LO1_TO_LO2
  permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
!
! Create and apply crypto-map
!
crypto map VPN 10 ipsec-isakmp
 match address LO1_TO_LO2
 set transform 3DES_MD5
 set peer 136.1.122.2
!
interface E 0/0
 crypto map VPN
```

R2:

```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
!
! Wildcard pre-shared key
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Dynamic map
!
crypto dynamic-map DYNAMIC 10
 set transform 3DES_MD5
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
```



```
!
interface E 0/0
 crypto map VPN
```

Verification

```
R1#ping 150.1.2.2 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/13 ms

R1#show cry isa sa
dst             src             state          conn-id slot
136.1.122.2     136.1.121.1     QM_IDLE              1    0

R1#show cry ips sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.121.1

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.122.2:4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 6, #recv errors 0

     local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.122.2
     path mtu 1500, media mtu 1500
     current outbound spi: 652A3F6F

     inbound esp sas:
      spi: 0xE6BFA8E(241957518)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4585150/3572)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x652A3F6F(1697267567)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4585150/3572)
        IV size: 8 bytes
```

```
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

R2#sho cry isa sa
dst             src             state          conn-id slot
136.1.122.2     136.1.122.12    QM_IDLE              1    0

R2#show cry ips sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.122.12:1027
     PERMIT, flags={}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.122.12
     path mtu 1500, media mtu 1500
     current outbound spi: E6BFA8E

     inbound esp sas:
      spi: 0x652A3F6F(1697267567)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4520954/3533)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xE6BFA8E(241957518)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4520954/3533)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

ASA1(config)# show x
2 in use, 10 most used
PAT Global 136.1.122.12(1027) Local 136.1.121.1(4500)
PAT Global 136.1.122.12(1) Local 136.1.121.1(500)

ASA1(config)# show conn
```

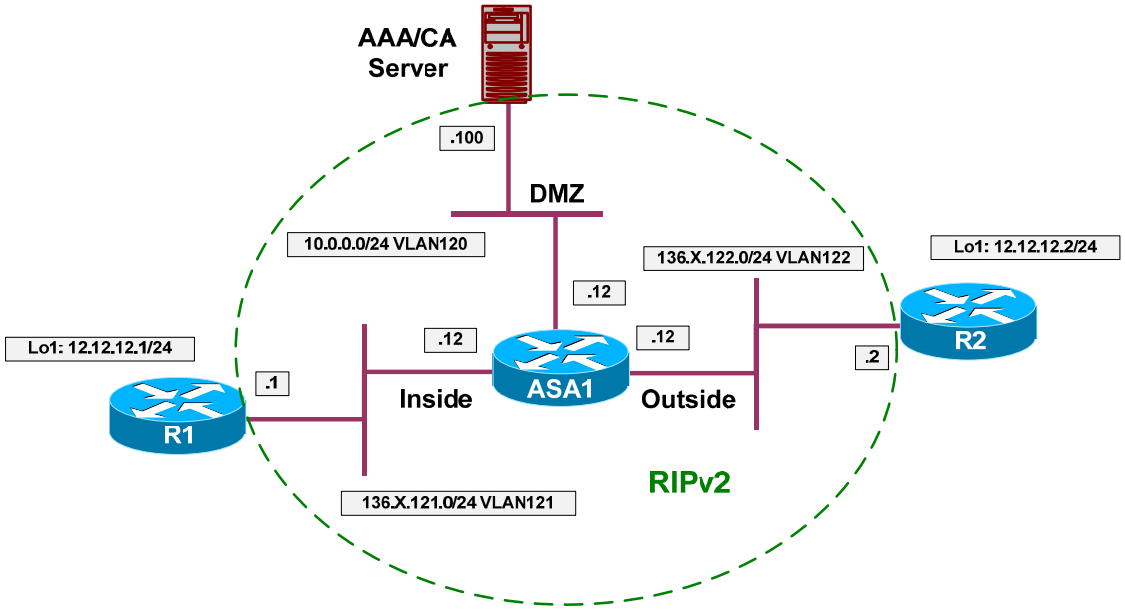
```
7 in use, 209 most used
UDP out 136.1.122.2:4500 in 136.1.121.1:4500 idle 0:00:58 flags -
UDP out 136.1.122.2:500 in 136.1.121.1:500 idle 0:01:14 flags -
```

Further Reading

Configuring IPSec Network Security
Configuring Internet Key Exchange Security Protocol

IOS and IOS with PSK Across the PIX/ASA with Overlapping Subnets

Objective: Configure IPsec tunnel across the PIX/ASA firewall between two IOS routers with PSK authentication. Handle the overlapping subnets issue.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration".
- Create two additional loopback interfaces on R1 and R2 as per the diagram, however do not advertise them into RIP.
- To handle the overlapping subnets issue a NAT configuration should be implemented.
- Configure access-control on the ASA.
- Create and apply to the outside interface access-list OUTSIDE_IN as follows:
    - Permit ISAKMP traffic from outside.
    - Permit ESP traffic from outside.
- Configure NAT on R1 as follows:
    - Configure Lo1 as inside and E0/0 as outside interface.
    - Configure static network NAT for 12.12.12.0/24 to 10.10.10.0/24.
- Configure NAT on R2 as follows:
    - Configure Lo1 as inside and E0/0 as outside interface.

  - Configure static network NAT for 12.12.12.0/24 to 20.20.20.0/24.

- Configure static routes on R1 and R2 for 20.20.20.0/24 and 10.10.10.0/24 respectively to point at the ASA.
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
  - Create ISAKMP policy with priority 10 as follows:
    - Use pre-shared keys authentication.
    - Use 3DES for cipher.
    - Use MD5 for hash.
  - Create ISAKMP key CISCO for address 136.X.122.2 (R2).
  - Create transform-set 3DES_MD5 as follows:
    - Use 3DES for cipher.
    - Use MD5 for hash.
  - Create access-list LO1_TO_LO2 as follows:
    - Permit IP traffic from 10.10.10.0/24 to 20.20.20.0/24.
  - Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
    - Match address LO1_TO_LO2.
    - Set peer 136.X.122.2.
    - Set transform-set 3DES_MD5.

- Configure R2 to mirror R1's configuration.

Final Configuration

```
ASA1:
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit esp any any
!
access-group OUTSIDE_IN in interface outside

R1:
!
! NAT Configuration
!
interface Loopback1
 ip address 12.12.12.1 255.255.255.0
 ip nat inside
!
interface E 0/0
 ip nat outside
!
ip nat inside source static network 12.12.12.0 10.10.10.0 /24
!
```

```
! Static route to peer's post-NAT network
!
ip route 20.20.20.0 255.255.255.0 136.1.121.12
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
!
crypto isakmp key CISCO address 136.1.122.2
!
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-List to classify VPN traffic
!
ip access-list extended LO1_TO_LO2
  permit ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255
!
! Create and apply crypto-map
!
crypto map VPN 10 ipsec-isakmp
 match address LO1_TO_LO2
 set transform 3DES_MD5
 set peer 136.1.122.2
!
interface E 0/0
 crypto map VPN
```

R2:

```
!
! NAT Configuration
!
interface Loopback1
 ip address 12.12.12.2 255.255.255.0
 ip nat inside
!
interface E 0/0
 ip nat outside
!
ip nat inside source static network 12.12.12.0 20.20.20.0 /24
!
! Static route to peer's post-NAT network
!
ip route 10.10.10.0 255.255.255.0 136.1.122.12
!
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
!
crypto isakmp key CISCO address 136.1.121.1
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
ip access-list extended LO2_TO_LO1
  permit  ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255
!
crypto map VPN 10 ipsec-isakmp
 match address LO2_TO_LO1
```

```
 set transform 3DES_MD5
 set peer 136.1.121.1
!
interface E 0/0
 crypto map VPN
```

Verification

```
R2#ping 10.10.10.1 source loopback 1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 12.12.12.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/12/12 ms

R2#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.121.1     136.1.122.2     QM_IDLE              1    0

R2#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer: 136.1.121.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.1
     path mtu 1500, media mtu 1500
     current outbound spi: FE66CA03

     inbound esp sas:
      spi: 0x6BD89D6B(1809358187)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4554053/3567)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xFE66CA03(4268149251)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4554053/3567)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

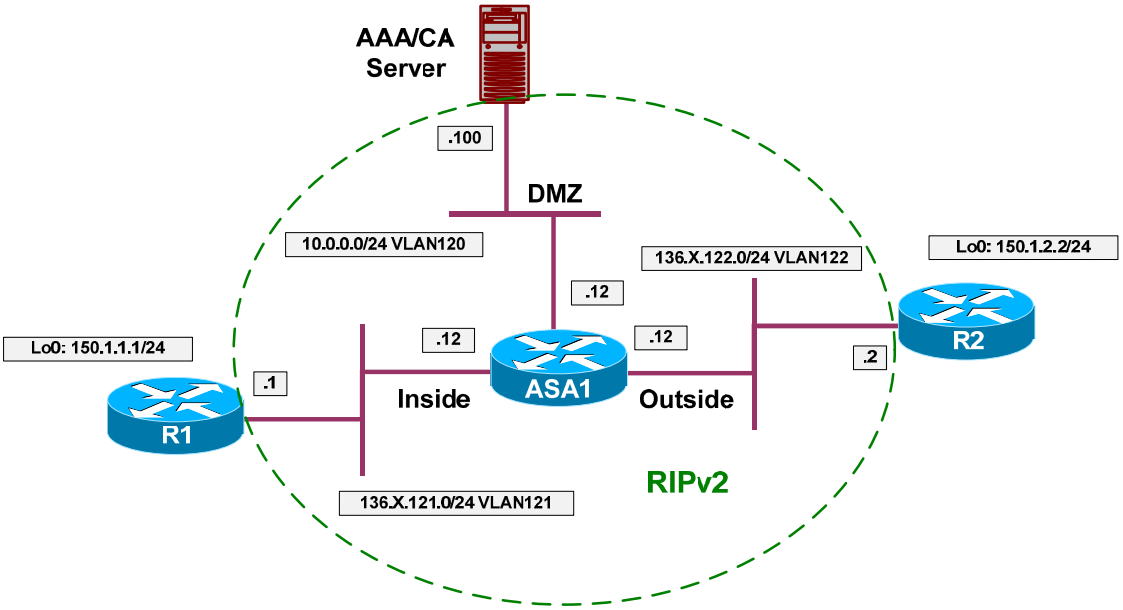
```
R2#show ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- 20.20.20.2         12.12.12.2         ---                ---

Subnet translation:
Inside global   Inside local    Outside local   Outside global /prefix
20.20.20.0      12.12.12.0      ---             ---             /24

R1#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- 10.10.10.1         12.12.12.1         ---                ---

Subnet translation:
Inside global   Inside local    Outside local   Outside global /prefix
10.10.10.0      12.12.12.0      ---             ---             /24

R1#show cry ips sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.121.1

   protected vrf:
   local  ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
   current_peer: 136.1.122.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.122.2
     path mtu 1500, media mtu 1500
     current outbound spi: 6BD89D6B

     inbound esp sas:
      spi: 0xFE66CA03(4268149251)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4466441/3540)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6BD89D6B(1809358187)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4466441/3540)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

Further Reading

Configuring IPSec Network Security
Configuring Internet Key Exchange Security Protocol
Cisco - NAT Order of Operation
Configuring Network Address Translation: Getting Started

IOS and IOS with PSK Across the PIX/ASA and NAT with IKE AM

Objective: Configure IPsec tunnel between two IOS routers across the PIX/ASA firewall with NAT setup.Use PSK for authentication and hostname for IKE identity.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration".
- The main advantage of IKE Agressive Mode (IKE AM) with PSK is that identity is present at IKE initiation phase, allowing for flexible policy lookup.
- In this lab the hostname will be used as router's identity, to avoid configuring the wildcard pre-shared key on the "hub" site (R2).
- Create two additional loopback interfaces on R1 and R2 as per the diagram, advertise them into RIP.
- Configure domain-name "internetworkexpert.com" on R1 and R2, as well as hostnames R1 and R2.
- Configure NAT on the PIX/ASA firewall as follows:
    - Translate inside networks as they go outside using the outside interface IP address.
    - Enable NAT-Control on the firewall.
- Configure access-control on the ASA as follows:
    - Create and apply to the outside interface access-list OUTSIDE_IN:

        - Permit ISAKMP traffic from outside.
        - Permit NAT-T traffic from outside (UDP 4500).

- Configure IPsec LAN-to-LAN tunnel on R1 as follows:

    - Configure ISAKMP profile AGGRESSIVE as follows:

        - Initiate IKE aggressive mode.
        - Use FQDN as self-identity.
        - Use global keyring.

    - Configure host entry for host “R2.internetworkexpert.com” to IP 136.1.122.2. This way you attach a “peer IP” in crypto map to it’s hostname for key lookup.
    - Create ISAKMP policy with priority 10 as follows:

        - Use pre-shared keys authentication.
        - Use 3DES for cipher.
        - Use MD5 for hash.

    - Create ISAKMP key CISCO for host “R2.internetworkexpert.com”.
    - Create transform-set 3DES_MD5 as follows:

        - Use 3DES for cipher.
        - Use MD5 for hash.

    - Create access-list LO1_TO_LO2 as follows:

        - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.

    - Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:

        - Match address LO1_TO_LO2.
        - Set peer 136.X.122.2
        - Set transform-set 3DES_MD5.

- Configure IPsec L2L tunnel on R2 as follows:

    - Configure ISAKMP just like you did on R1.
    - Configure ISAKMP identity “hostname”.
    - However, configure pre-shared ISAKMP key “CISCO” for hostname “R1.internetworkexpert.com”.
    - Create transform-set 3DES_MD5 as follows:

        - Use 3DES for cipher.

- Use MD5 for hash.

- Create dynamic crypto-map DYNAMIC enry 10 as follows:
  - Set transform-set 3DES_MD5.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP and attach dynamic crypto-map DYNAMIC to it.
- Apply crypto-map VPN to interface Ethernet 0/0.

Final Configuration

```
R1:
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
router rip
 network 150.1.0.0

R2:
interface Loopback0
 ip address 150.1.2.2 255.255.255.0
!
router rip
 network 150.1.0.0

ASA1:
access-list OUTSIDE_IN permit udp any any eq 500
access-list OUTSIDE_IN permit udp any any eq 4500
!
access-group OUTSIDE_IN in interface outside
!
! NAT Configuration
!
nat-control
nat (inside) 1 0 0
global (outside) 1 interface

R1:
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
!
! ISAKMP profile
!
crypto isakmp profile AGGRESSIVE
 initiate mode aggressive
 self-identity fqdn
 keyring default
!
! Domain-name & host mapping
!
hostname R1
ip domain-name internetworkexpert.com
```

```
ip host R2.internetworkexpert.com 136.1.122.2
!
! Hostname pre-shared key
!
crypto isakmp key CISCO host R2.internetworkexpert.com
!
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-List to classify VPN traffic
!
ip access-list extended LO1_TO_LO2
  permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255

!
! Create and apply crypto-map
! Apply ISAKMP profile to crypto map
!
crypto map VPN isakmp-profile AGGRESSIVE
crypto map VPN 10 ipsec-isakmp
 match address LO1_TO_LO2
 set transform 3DES_MD5
 set peer 136.1.122.2
!
interface E 0/0
 crypto map VPN
```

R2:

```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
!
crypto isakmp identity hostname
!
! Host pre-shared key
!
hostname R2
ip domain-name internetworkexpert.com
crypto isakmp key CISCO host R1.internetworkexpert.com
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Dynamic map
!
crypto dynamic-map DYNAMIC 10
 set transform 3DES_MD5
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
!
interface E 0/0
 crypto map VPN
```


Verification

```
R1#debug crypto isakmp
Crypto ISAKMP debugging is on

R1#ping 150.1.2.2 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
R1#

ISAKMP: received ke message (1/1)
ISAKMP (0:0): SA request profile is AGGRESSIVE
ISAKMP: local port 500, remote port 500
ISAKMP: set new node 0 to QM_IDLE
ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa = 8256C708
ISAKMP (0:3): Found HOST key in keyring default
ISAKMP (0:3): constructed NAT-T vendor-03 ID
ISAKMP (0:3): constructed NAT-T vendor-02 ID
ISAKMP (0:3): SA is doing pre-shared key authentication using id type ID_FQDN
ISAKMP (3): ID payload
        next-payload : 13
        type         : 2
        FQDN name    : R1.internetworkexpert.com
        protocol     : 17
        port         : 0
        length       : 29
ISAKMP (3): Total payload length: 33
ISAKMP (0:3): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_AM
ISAKMP (0:3): Old State = IKE_READY  New State = IKE_I_AM1
ISAKMP (0:3): beginning Aggressive Mode exchange
ISAKMP (0:3): sending packet to 136.1.122.2 my_port 500 peer_port 500 (I)
AG_INIT_EXCH
ISAKMP (0:3): received packet from 136.1.122.2 dport 500 sport 500 Global (I)
AG_INIT_EXCH
ISAKMP (0:3): processing SA payload. message ID = 0
ISAKMP (0:3): processing ID payload. message ID = 0
ISAKMP (3): Process ID payload
        type         : 2
        FQDN name    : R2.internetworkexpert.com
        protocol     : 17
        port         : 0
        length       : 25
ISAKMP (0:3): processing vendor id payload
ISAKMP (0:3): vendor ID is Unity
ISAKMP (0:3): processing vendor id payload
ISAKMP (0:3): vendor ID is DPD
ISAKMP (0:3): processing vendor id payload
ISAKMP (0:3): speaking to another IOS box!
ISAKMP (0:3): Found HOST key in keyring default
ISAKMP (0:3) local preshared key found
ISAKMP : Scanning profiles for xauth ... AGGRESSIVE
ISAKMP (0:3): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
```

```
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:3): atts are acceptable. Next payload is 0
ISAKMP (0:3): vendor ID is NAT-T v3
ISAKMP (0:3): processing KE payload. message ID = 0
ISAKMP (0:3): processing NONCE payload. message ID = 0
ISAKMP (0:3): Found HOST key in keyring default
ISAKMP (0:3): SKEYID state generated
ISAKMP (0:3): processing HASH payload. message ID = 0
ISAKMP:received payload type 17
ISAKMP (0:3): Detected NAT-D payload
ISAKMP (0:3): NAT does not match MINE hash
hash received: 76 26 A8 59 D9 6E F6 8 20 A7 A9 25 2E 60 5A 89
my nat hash  : E C6 37 A2 9A BB 13 5D F1 C5 96 3 31 E6 12 B4
ISAKMP:received payload type 17
ISAKMP (0:3): Detected NAT-D payload
ISAKMP (0:3): NAT match HIS hash
ISAKMP (0:3): SA has been authenticated with 136.1.122.2
ISAKMP: Locking peer struct 0x82E737F0, IKE refcount 2 for from
crypto_ikmp_udp_enc_ike_init
ISAKMP (0:3): Setting UDP ENC peer struct 0x82E73A58 sa= 0x8256C708
ISAKMP (0:3): Send initial contact
ISAKMP (0:3): constructed HIS NAT-D
ISAKMP (0:3): recalc his hash for NAT-D
ISAKMP (0:3): constructed MINE NAT-D
ISAKMP (0:3): sending packet to 136.1.122.2 my_port 4500 peer_port 4500 (I)
AG_INIT_EXCH
ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:3): Old State = IKE_I_AM1  New State = IKE_P1_COMPLETE

ISAKMP: sending nat keepalive packet to 136.1.122.2(4500)
ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -785375327
ISAKMP (0:3): sending packet to 136.1.122.2 my_port 4500 peer_port 4500 (I)
QM_IDLE
ISAKMP (0:3): Node -785375327, Input = IKE_MESG_INTERNAL, IKE_INIT_QM
ISAKMP (0:3): Old State = IKE_QM_READY  New State = IKE_QM_I_QM1
ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:3): Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

ISAKMP (0:3): received packet from 136.1.122.2 dport 4500 sport 4500 Global (I)
QM_IDLE
ISAKMP (0:3): processing HASH payload. message ID = -785375327
ISAKMP (0:3): processing SA payload. message ID = -785375327
ISAKMP (0:3): Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 61443
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 3600
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (0:3): atts are acceptable.
ISAKMP (0:3): processing NONCE payload. message ID = -785375327
ISAKMP (0:3): processing ID payload. message ID = -785375327
ISAKMP (0:3): processing ID payload. message ID = -785375327
ISAKMP: Locking peer struct 0x82E737F0, IPSEC refcount 1 for for stuff_ke
ISAKMP (0:3): Creating IPSec SAs
        inbound SA from 136.1.122.2 to 136.1.121.1 (f/i)  0/ 0
        (proxy 150.1.2.0 to 150.1.1.0)
        has spi 0x2127CD37 and conn_id 2000 and flags 400
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
        has client flags 0x10
```

```
        outbound SA from 136.1.121.1     to 136.1.122.2     (f/i)  0/ 0 (proxy
150.1.1.0       to 150.1.2.0      )
        has spi -847945563 and conn_id 2001 and flags 408
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
        has client flags 0x10
ISAKMP (0:3): sending packet to 136.1.122.2 my_port 4500 peer_port 4500 (I)
QM_IDLE
ISAKMP (0:3): deleting node -785375327 error FALSE reason ""
ISAKMP (0:3): Node -785375327, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP (0:3): Old State = IKE_QM_I_QM1  New State = IKE_QM_PHASE2_COMPLETE

R1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
3     136.1.121.1     136.1.122.2              3des md5  psk  1  23:57:42 N

R1#show cry ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.121.1

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.122.2:4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.122.2
     path mtu 1500, media mtu 1500
     current outbound spi: CD7560A5

     inbound esp sas:
      spi: 0x2127CD37(556256567)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4458262/3456)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCD7560A5(3447021733)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4458262/3456)
        IV size: 8 bytes
```

```
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

R2#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.122.2     136.1.122.12    QM_IDLE              3    0

R2#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
3     136.1.122.2     136.1.122.12             3des md5  psk  1  23:56:43 N

R2#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.122.12:1027
     PERMIT, flags={}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.122.12
     path mtu 1500, media mtu 1500
     current outbound spi: 2127CD37

     inbound esp sas:
      spi: 0xCD7560A5(3447021733)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4449442/3395)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x2127CD37(556256567)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4449442/3395)
        IV size: 8 bytes
        replay detection support: Y
```

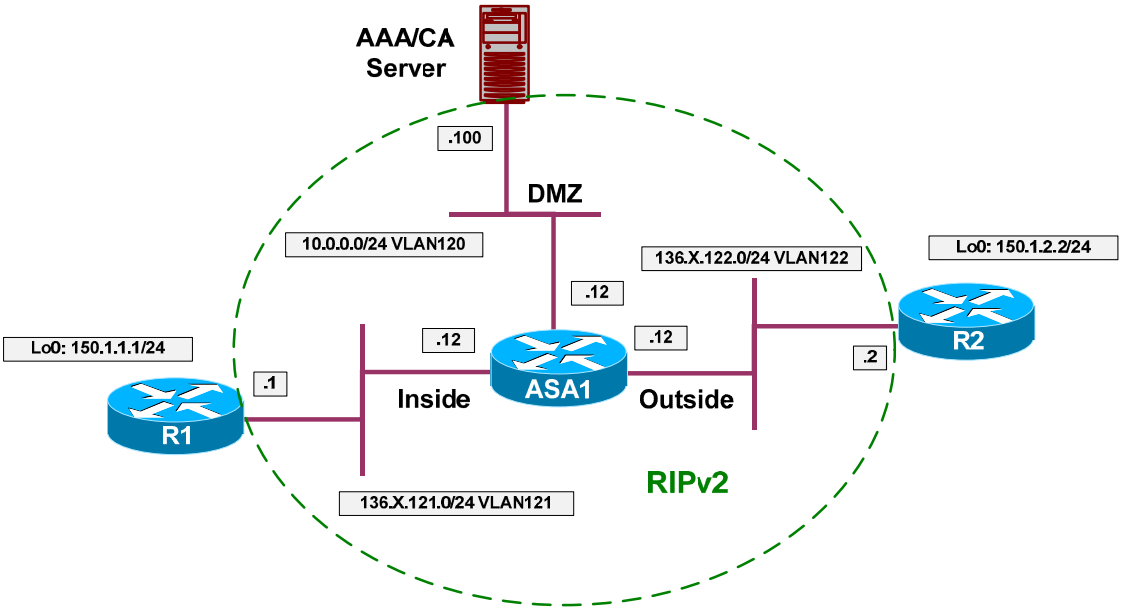
```
outbound ah sas:

outbound pcp sas:
```

Further Reading

Configuring IPSec Network Security
Configuring Internet Key Exchange Security Protocol

IOS and IOS with Digital Certificates Across the PIX/ASA

Objective: Configure IPsec tunnel between two IOS routers across the PIX/ASA firewall, with digital certificates based authentication.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration".
- Create two additional loopback interfaces on R1 and R2 as per the diagram, advertise them into RIP.
- Configure access-control on the ASA.
- Create access-list OUTSIDE_IN as follows:
    - Permit ISAKMP traffic from outside.
    - Permit ESP traffic from outside.
    - Permit HTTP to 10.0.0.100.
    - Permit NTP to 10.0.0.100.
- Apply this access-group to the outside interface
- Configure R1, R2 and the ASA to synchronize time with the AAA/CA server via NTP.
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
    - Create ISAKMP policy with priority 10 as follows:
        - Use RSA-sig authentication.
        - Use 3DES for cipher.

        - Use MD5 for hash.

    - Enroll R1 with CA:

        - Configure domain-name “internetworkexpert.com”
        - Generate RSA key-pair.
        - Configure CA Trustpoint IE1 as follows:

            - Use enrollment URL: http://10.0.0.100/certsrv/mscep/mscep.dll
            - Use RA mode.
            - Set CRL as optional.

        - Authenticate the CA and Enroll.
    - Create transform-set 3DES_MD5 as follows:

        - Use 3DES for cipher.
        - Use MD5 for hash.

    - Create access-list LO1_TO_LO2 as follows:

        - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.

    - Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:

        - Match address LO1_TO_LO2.
        - Set peer 136.X.122.2.
        - Set transform-set 3DES_MD5.

- Configure R2 to mirror R1’s configuration.

Final Configuration

```
R1:
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
router rip
 network 150.1.0.0

R2:
interface Loopback0
 ip address 150.1.2.2 255.255.255.0
!
router rip
 network 150.1.0.0

ASA1:
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit tcp any host 10.0.0.100 eq 80
```

```
access-list OUTSIDE_IN permit udp any host 10.0.0.100 eq 123
access-list OUTSIDE_IN permit esp any any
!
access-group OUTSIDE_IN in interface outside
!
ntp server 10.0.0.100
```

R1:

```
ntp server 10.0.0.100
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
 authentication rsa-sig
 hash md5
 encryption 3des
!
crypto ca trustpoint IE1
 enrollment url http://10.0.0.100/certsrv/mscep/mscep.dll
 crl optional
 enrollment mode ra
 exit

!
! Generate RSA key, authenticate CA and enroll
!
ip domain-name internetworkexpert.com
hostname R1
crypto key generate rsa general modulus 512
crypto ca authenticate IE1
crypto ca enroll IE1
!
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-List to classify VPN traffic
!
ip access-list extended LO1_TO_LO2
  permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
!
! Create and apply crypto-map
!
crypto map VPN 10 ipsec-isakmp
 match address LO1_TO_LO2
 set transform 3DES_MD5
 set peer 136.1.122.2
!
interface E 0/0
 crypto map VPN
```

R2:

```
ntp server 10.0.0.100
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
 authentication rsa-sig
 hash md5
 encryption 3des
!
crypto ca trustpoint IE1
 enrollment url http://10.0.0.100/certsrv/mscep/mscep.dll
```

```
 crl optional
 enrollment mode ra
 exit
!
! Generate RSA key, authenticate CA and enroll
!
ip domain-name internetworkexpert.com
hostname R2
crypto key generate rsa general modulus 512
crypto ca authenticate IE1
crypto ca enroll IE1
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
ip access-list extended LO2_TO_LO1
  permit  ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
crypto map VPN 10 ipsec-isakmp
 match address LO2_TO_LO1
 set transform 3DES_MD5
 set peer 136.1.121.1
!
interface E 0/0
 crypto map VPN
```

Verification

Enroll R1 and R2 with CA, check certificates:

```
R2(config)#do sho cry ca cert
Certificate
  Status: Available
  Certificate Serial Number: 32D2CA1D00010000002A
  Certificate Usage: General Purpose
  Issuer:
    CN = IESERVER1
     O = Internetwork Expert
     L = Reno
     ST = NV
     C = US
     EA = bmcgahan@internetworkexpert.com
  Subject:
    Name: R2.internetworkexpert.com
    OID.1.2.840.113549.1.9.2 = R2.internetworkexpert.com
  CRL Distribution Point:
    http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 10:16:14 UTC Jan 15 2007
    end   date: 10:26:14 UTC Jan 15 2008
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: IE1

CA Certificate
  Status: Available
  Certificate Serial Number: 6A8B964C37F91BB245B01DE2A6363745
  Certificate Usage: Signature
  Issuer:
    CN = IESERVER1
     O = Internetwork Expert
```

```
      L = Reno
      ST = NV
      C = US
      EA = bmcgahan@internetworkexpert.com
  Subject:
    CN = IESERVER1
      O = Internetwork Expert
      L = Reno
      ST = NV
      C = US
      EA = bmcgahan@internetworkexpert.com
  CRL Distribution Point:
    http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 09:01:58 UTC Jul 21 2006
    end   date: 09:09:34 UTC Jul 21 2008
  Associated Trustpoints: IE1

R1(config)#do sh cry ca cert
Certificate
  Status: Available
  Certificate Serial Number: 32CEEFC6000100000028
  Certificate Usage: General Purpose
  Issuer:
    CN = IESERVER1
      O = Internetwork Expert
      L = Reno
      ST = NV
      C = US
      EA = bmcgahan@internetworkexpert.com
  Subject:
    Name: R1.internetworkexpert.com
    OID.1.2.840.113549.1.9.2 = R1.internetworkexpert.com
  CRL Distribution Point:
    http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 10:12:01 UTC Jan 15 2007
    end   date: 10:22:01 UTC Jan 15 2008
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: IE1

CA Certificate
  Status: Available
  Certificate Serial Number: 6A8B964C37F91BB245B01DE2A6363745
  Certificate Usage: Signature
  Issuer:
    CN = IESERVER1
      O = Internetwork Expert
      L = Reno
      ST = NV
      C = US
      EA = bmcgahan@internetworkexpert.com
  Subject:
    CN = IESERVER1
      O = Internetwork Expert
      L = Reno
      ST = NV
      C = US
      EA = bmcgahan@internetworkexpert.com
  CRL Distribution Point:
    http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 09:01:58 UTC Jul 21 2006
```

```
    end   date: 09:09:34 UTC Jul 21 2008
  Associated Trustpoints: IE1

R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/12 ms

R2#show cry isa sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.122.2     136.1.121.1              3des md5  rsig 1  23:59:29

R2#show cry ips sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 3, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.1
     path mtu 1500, media mtu 1500
     current outbound spi: 24ADFE7A

     inbound esp sas:
      spi: 0x8ADF82D(145618989)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4480341/3568)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x24ADFE7A(615382650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4480341/3568)
        IV size: 8 bytes
        replay detection support: Y
```

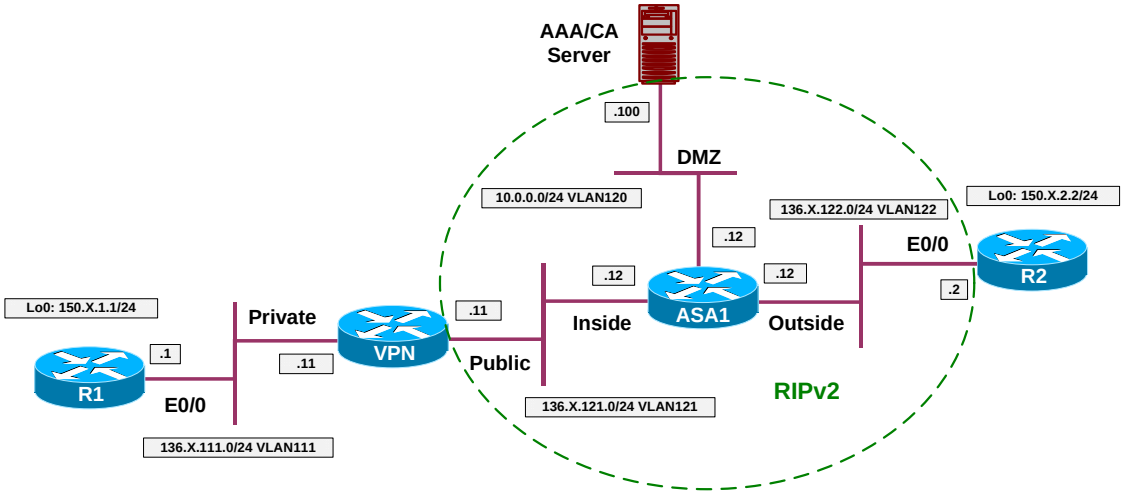
```
outbound ah sas:

outbound pcp sas:
```

🕮 Further Reading

Configuring IPSec Network Security
Configuring Internet Key Exchange Security Protocol
Configuring Certification Authority Interoperability

IOS and VPN3k with PSK

Objective: Configure L2L IPsec tunnel between IOS router and VPN3k across the PIX/ASA Firewall. Use pre-shared keys for authentication.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "IOS Router and VPN3k".
- Configure access-control on the ASA. Add rules to the access-list OUTSIDE_IN as follows:
    - Permit ISAKMP traffic from outside.
    - Permit ESP traffic from outside.
- Configure IPsec LAN-to-LAN tunnel on R2 as follows:
    - Create ISAKMP policy with priority 10 as follows:
        - Use pre-shared keys authentication.
        - Use 3DES for cipher.
        - Use MD5 for hash.
        - Use DH Group 2.
    - Create ISAKMP key CISCO for address 136.X.121.11 (VPN3k).
    - Create transform-set 3DES_MD5 as follows:
        - Use 3DES for cipher.
        - Use MD5 for hash.
    - Create access-list LO2_TO_LO1 as follows:

        - Permit IP traffic from 150.X.2.0/24 to 150.X.1.0/24.

    - Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:

        - Match address LO2_TO_LO1.
        - Set peer 136.X.121.11.
        - Set transform-set 3DES_MD5.

    - Apply crypto-map VPN to interface E0/0.

- Configure IPsec LAN-to-LAN tunnel on VPN3k as follows:

    - Use L2L tunnel wizard to complete to configuration steps.

Final Configuration

R2:

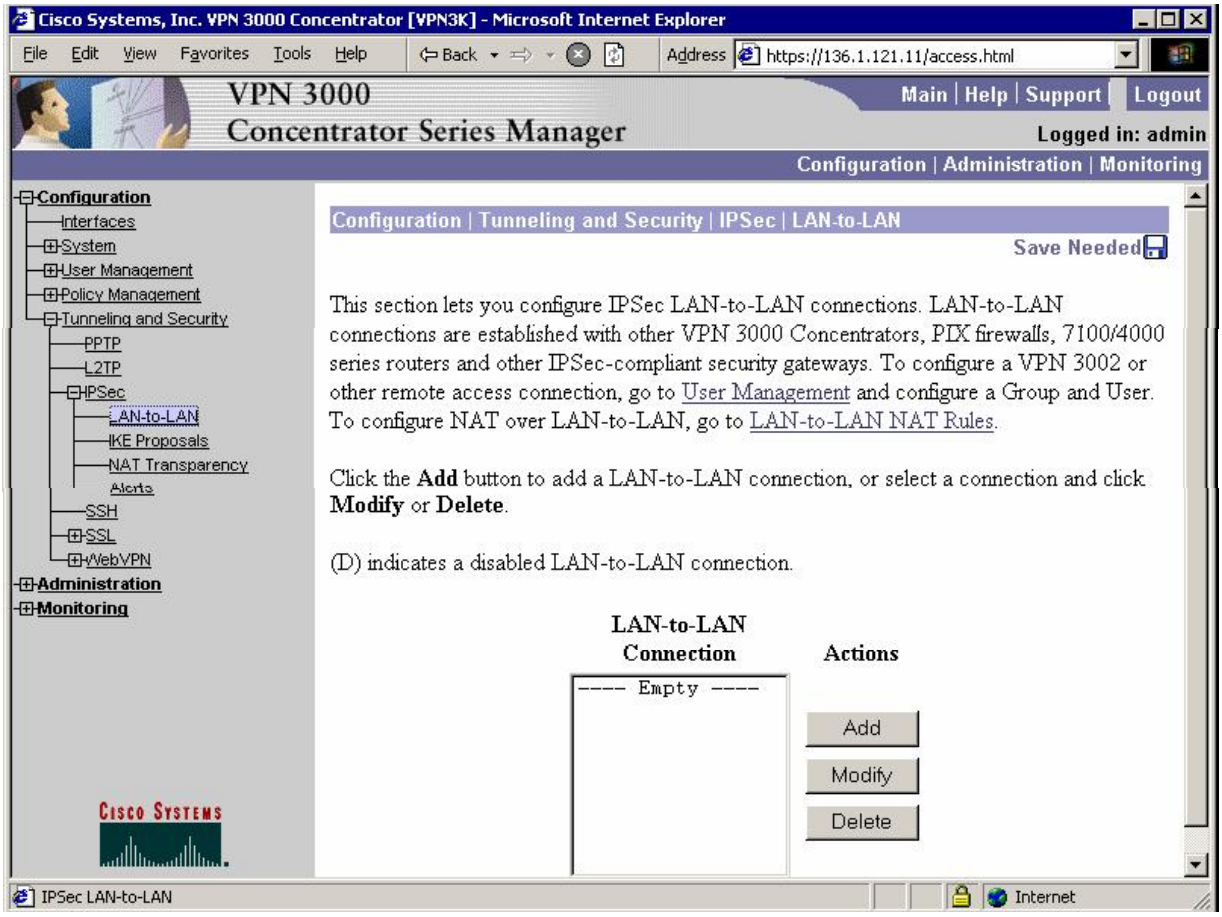
```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 group 2
 encryption 3des
!
crypto isakmp key CISCO address 136.1.121.11
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
ip access-list extended LO2_TO_LO1
  permit  ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
crypto map VPN 10 ipsec-isakmp
 match address LO2_TO_LO1
 set transform 3DES_MD5
 set peer 136.1.121.11
!
interface E 0/0
 crypto map VPN
```

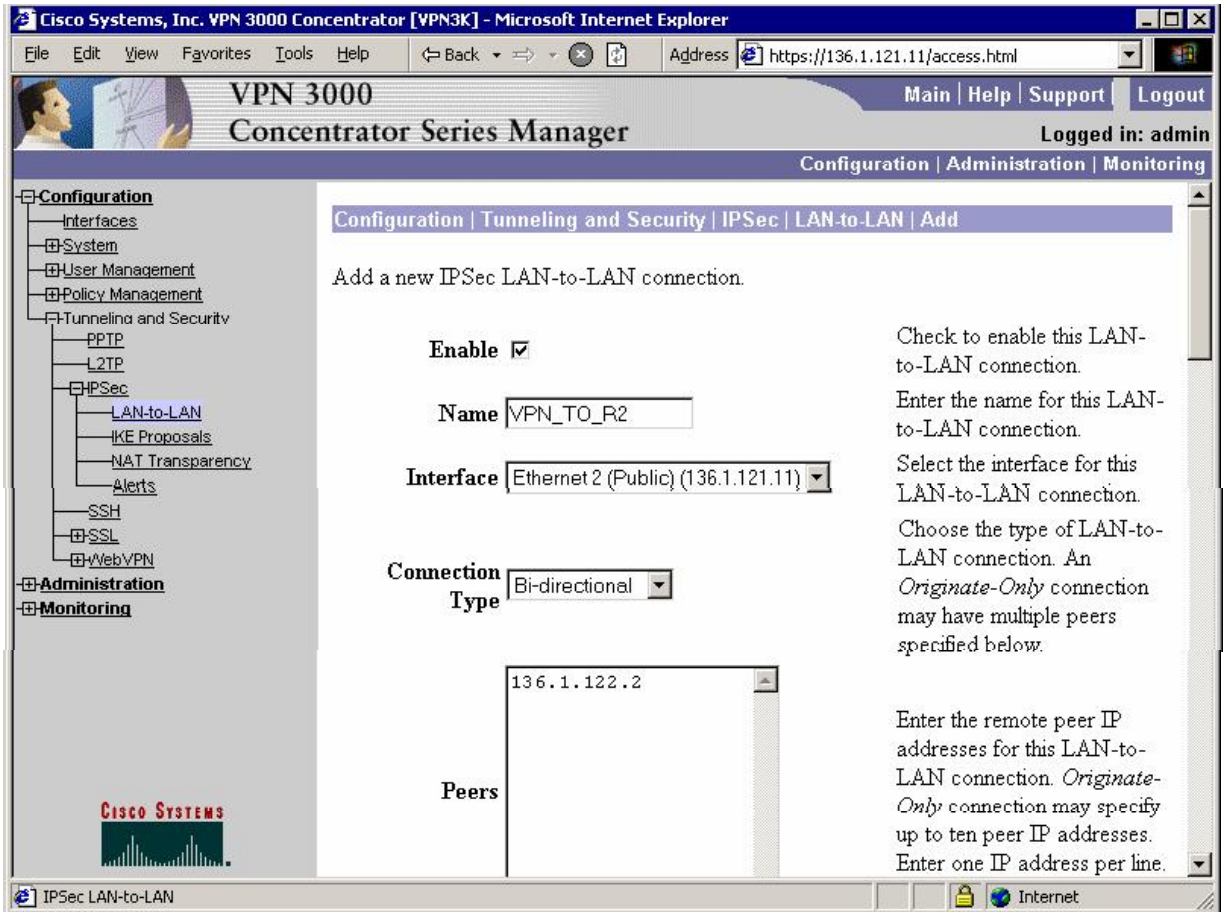
ASA1:

```
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit esp any any
```

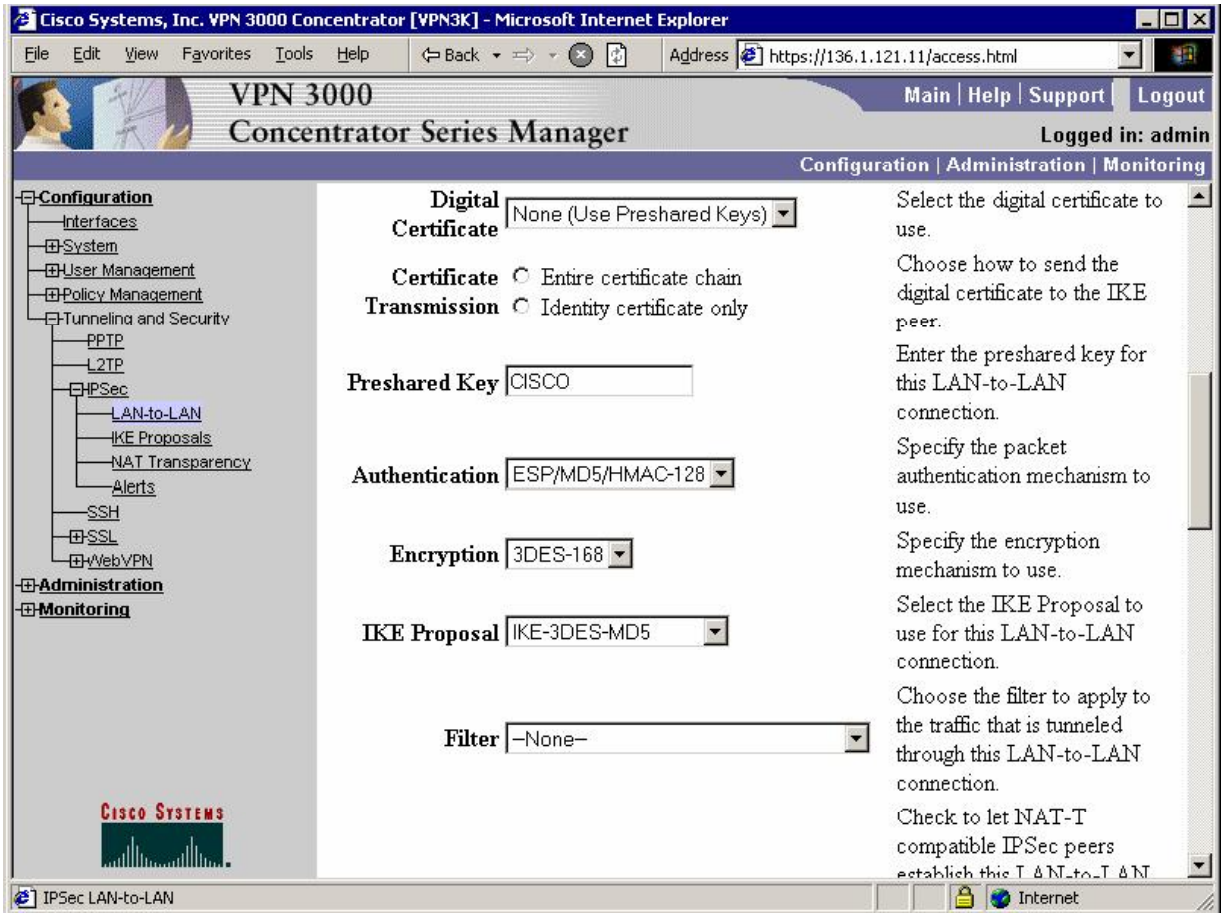
VPN3k:

Add new L2L Tunnel: Add peer IP address.

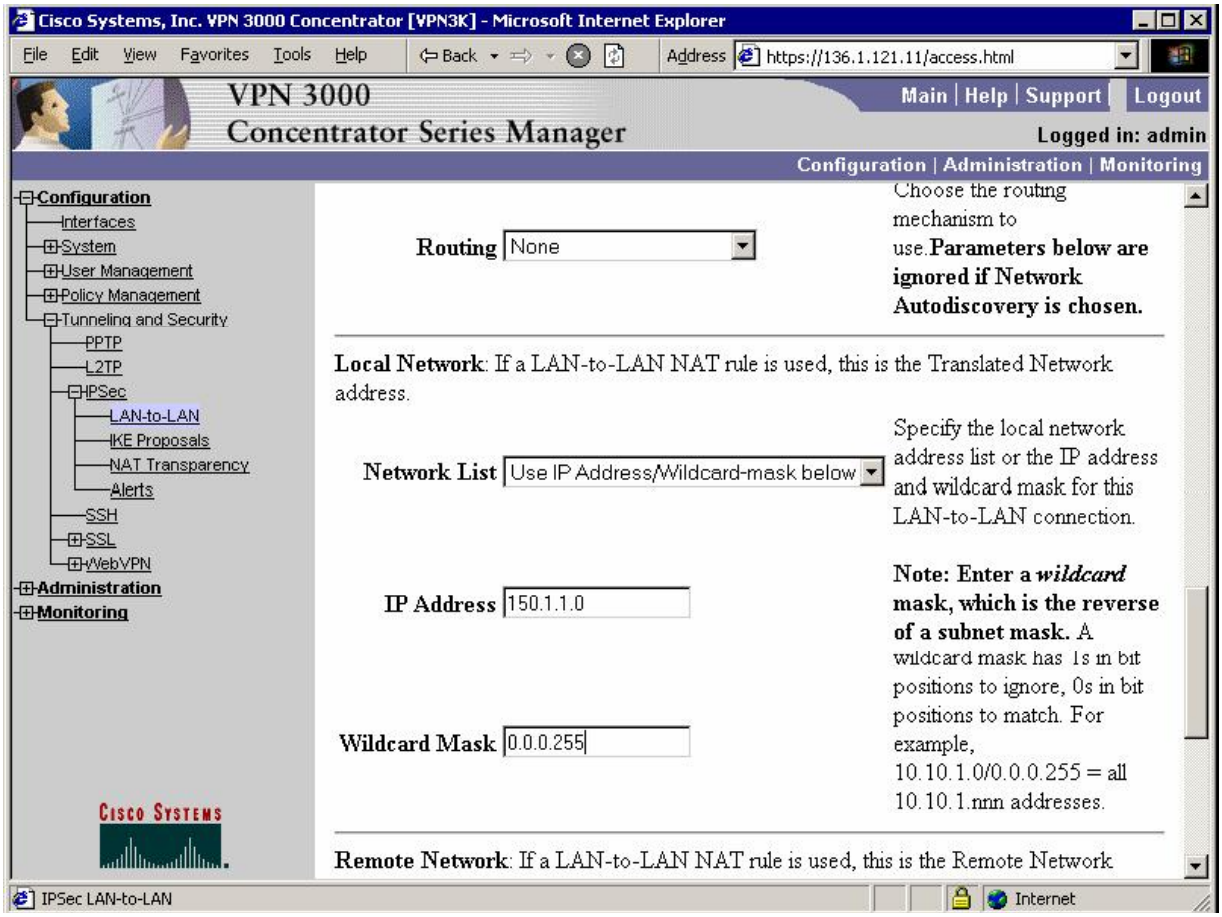

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support
Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Tunneling and Security
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
NAT Transparency
Alerts
SSH
SSL
WebVPN
Administration
Monitoring
Configuration | Tunneling and Security | IPSec | LAN-to-LAN
Save Needed
This section lets you configure IPSec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPSec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to User Management and configure a Group and User. To configure NAT over LAN-to-LAN, go to LAN-to-LAN NAT Rules.
Click the Add button to add a LAN-to-LAN connection, or select a connection and click Modify or Delete.
(D) indicates a disabled LAN-to-LAN connection.
LAN-to-LAN Connection
Actions
---- Empty ----
Add
Modify
Delete
Cisco Systems
IPSec LAN-to-LAN
Internet

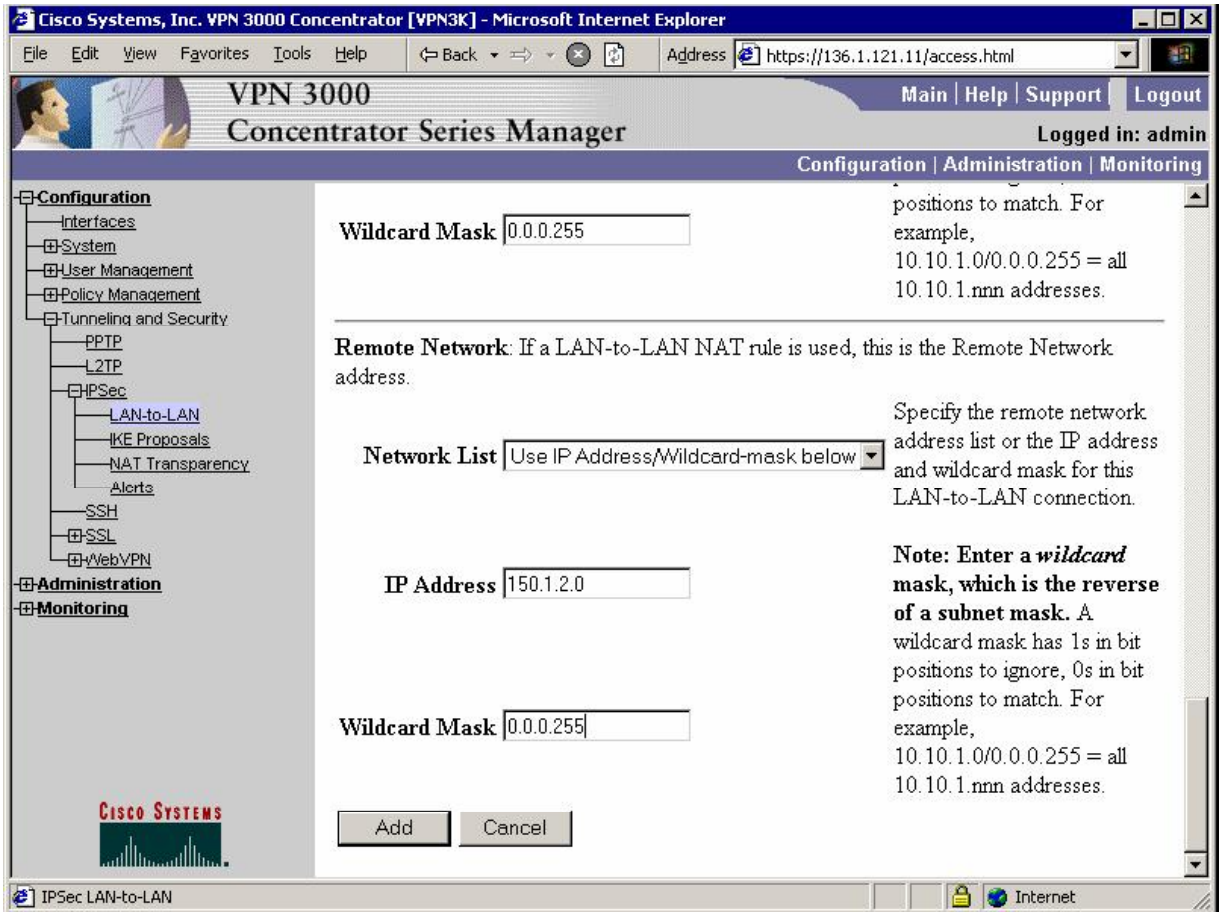

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Tunneling and Security
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
NAT Transparency
Alerts
SSH
SSL
WebVPN
Administration
Monitoring
Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add
Add a new IPSec LAN-to-LAN connection.
Enable
Check to enable this LAN-to-LAN connection.
Name
VPN_TO_R2
Enter the name for this LAN-to-LAN connection.
Interface
Ethernet 2 (Public) (136.1.121.11)
Select the interface for this LAN-to-LAN connection.
Connection Type
Bi-directional
Choose the type of LAN-to-LAN connection. An Originate-Only connection may have multiple peers specified below.
Peers
136.1.122.2
Enter the remote peer IP addresses for this LAN-to-LAN connection. Originate-Only connection may specify up to ten peer IP addresses. Enter one IP address per line.
Cisco Systems
IPSec LAN-to-LAN
Internet

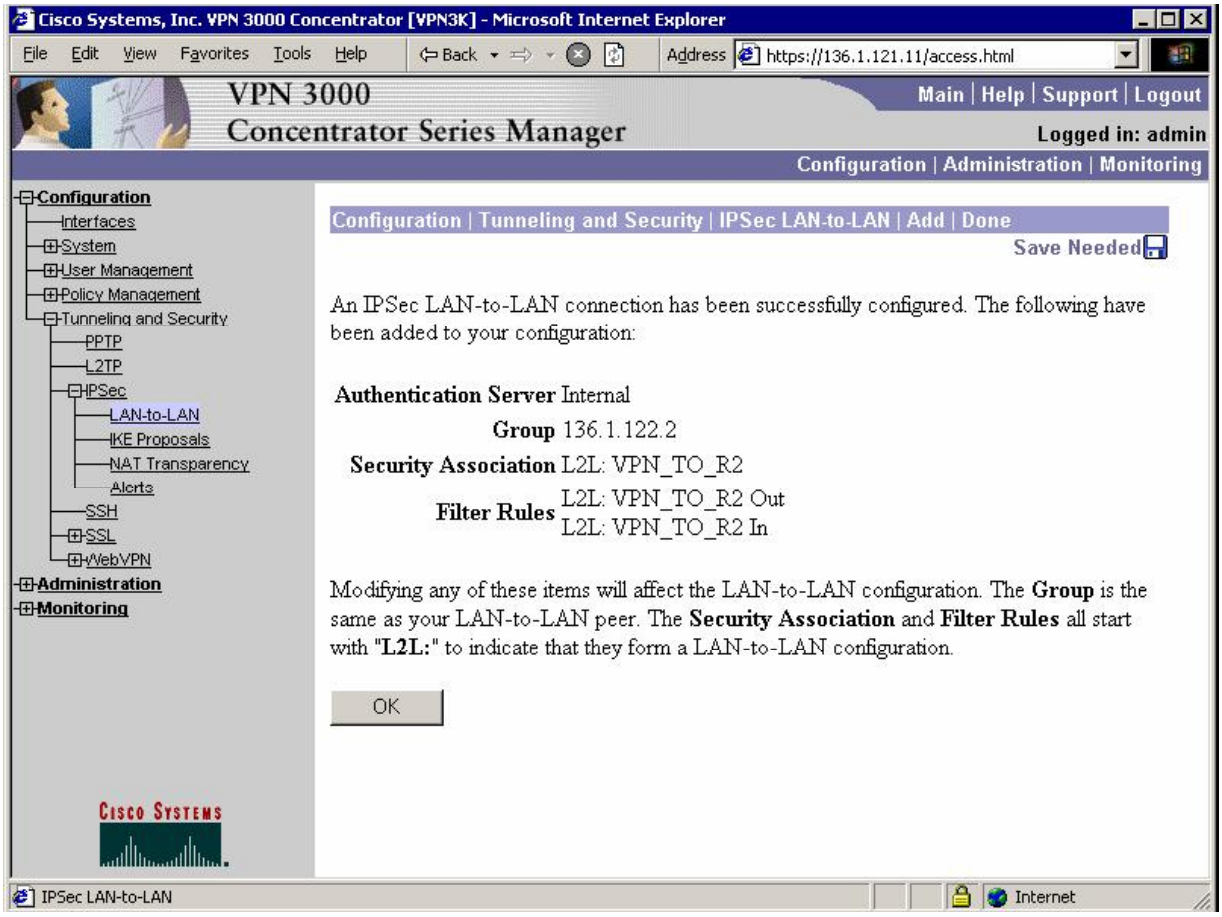
Set pre-shared key:



Designate protected networks:




Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Tunneling and Security
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
NAT Transparency
Alerts
SSH
SSL
WebVPN
Administration
Monitoring
Wildcard Mask 0.0.0.255
positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.
Network List Use IP Address/Wildcard-mask below
Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 150.1.2.0
Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask 0.0.0.255
Add
Cancel
Cisco Systems
IPSec LAN-to-LAN
Internet


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Tunneling and Security
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
NAT Transparency
Alerts
SSH
SSL
WebVPN
Administration
Monitoring
Configuration | Tunneling and Security | IPSec LAN-to-LAN | Add | Done
Save Needed
An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:
Authentication Server Internal
Group 136.1.122.2
Security Association L2L: VPN_TO_R2
Filter Rules L2L: VPN_TO_R2 Out
L2L: VPN_TO_R2 In
Modifying any of these items will affect the LAN-to-LAN configuration. The Group is the same as your LAN-to-LAN peer. The Security Association and Filter Rules all start with "L2L:" to indicate that they form a LAN-to-LAN configuration.
OK
Cisco Systems
IPSec LAN-to-LAN
Internet

Verification

```
R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/8/8 ms

R2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.122.2     136.1.121.11             3des md5  psk  2  23:59:32

R2#show cry ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.11:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 26, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.11
     path mtu 1500, media mtu 1500
     current outbound spi: 3EE679DF

     inbound esp sas:
      spi: 0xFE812159(4269875545)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4474125/3567)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x3EE679DF(1055291871)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4474125/3567)
        IV size: 8 bytes
```

```
        replay detection support: Y
    outbound ah sas:
    outbound pcp sas:
```

VPN3k:

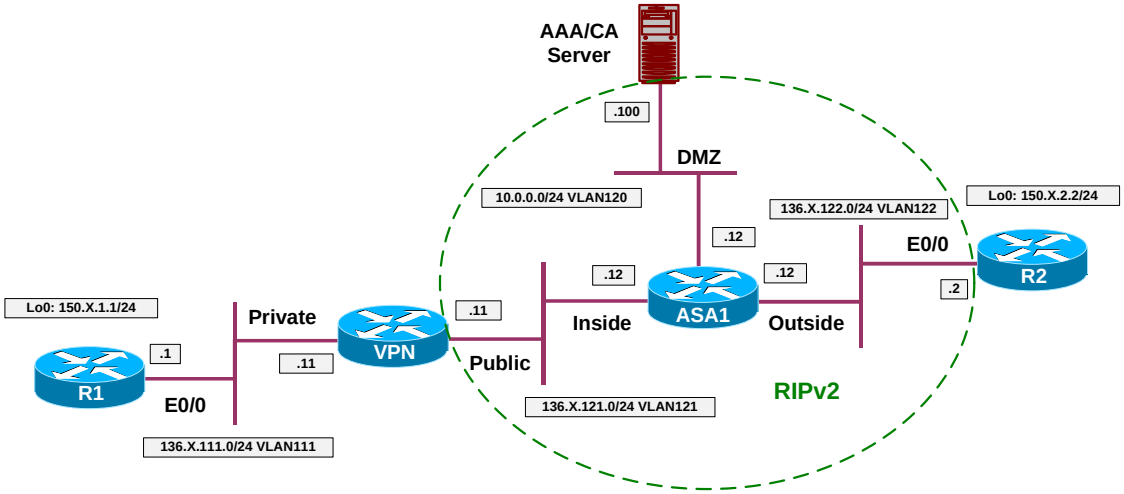
Admininstration > Administer Session:

Further Reading

Tunneling and Security: IPsec LAN-to-LAN

IOS and VPN3k with PSK using CLI only

Objective: Configure L2L IPsec tunnel between IOS router and VPN3k across the PIX/ASA Firewall. Use pre-shared keys for authentication. Use CLI to configure VPN3k.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "IOS Router and VPN3k".
- Configure access-control on the ASA. Add rules to the access-list OUTSIDE_IN as follows:
    - Permit ISAKMP traffic from outside.
    - Permit ESP traffic from outside.
- Configure IPsec LAN-to-LAN tunnel on R2 as follows:
    - Create ISAKMP policy with priority 10 as follows:
        - Use pre-shared keys authentication.
        - Use 3DES for cipher.
        - Use MD5 for hash.
        - Use DH Group 2.
    - Create ISAKMP key CISCO for address 136.X.121.11 (VPN3k).
    - Create transform-set 3DES_MD5 as follows:
        - Use 3DES for cipher.
        - Use MD5 for hash.

- Create access-list LO2_TO_LO1 as follows:
    - Permit IP traffic from 150.X.2.0/24 to 150.X.1.0/24.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
    - Match address LO2_TO_LO1.
    - Set peer 136.X.121.11.
    - Set transform-set 3DES_MD5.
- Apply crypto-map VPN to interface E0/0.

- Configure IPsec LAN-to-LAN tunnel on VPN3k using CLI as follows:
    - Create new IPsec SA: “L2L:VPN_TO_R2” as follows:
        - Use 3DES as cipher.
        - Use MD5 as hash.
        - Use IKE-3DES-MD5 IKE proposal.
    - Create access-list rule “L2L:VPN_TO_R2 In” as follows:
        - Match traffic from 150.1.2.0/24 to 150.1.1.0/24.
        - Configure “apply IPsec” as rule action.
    - Create access-list rule “L2L:VPN_TO_R2 Out” as follows:
        - Match traffic from 150.1.1.0/24 to 150.1.2.0/24.
        - Configure “apply IPsec” as rule action.
    - Assign rules “L2L:VPN_TO_R2 Out” and “L2L:VPN_TO_R2 In” to Public filter.
        - Apply IPsec SA “L2L:VPN_TO_R2” to this rules.
    - Create new group as follows:
        - Name “136.1.122.2”
        - Password “CISCO”
        - IPsec Parameters:
            - IPsec SA: “L2L:VPN_TO_R2”.
            - Tunnel Type: LAN-to-LAN.

Final Configuration

R2:
```
crypto isakmp policy 10
 authentication pre-share
 hash md5
 group 2
 encryption 3des
!
crypto isakmp key CISCO address 136.1.121.11
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
ip access-list extended LO2_TO_LO1
  permit  ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
crypto map VPN 10 ipsec-isakmp
 match address LO2_TO_LO1
 set transform 3DES_MD5
 set peer 136.1.121.11
!
interface E 0/0
 crypto map VPN
```

ASA1:
```
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit esp any any
```

VPN3k:

Create IPsec SA, based on existing "stock" SA:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 4

1) Access Hours
2) Traffic Management
3) Group Matching
4) Network Admission Control
5) Back

VPN3K: Policy -> 2

1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
```

```
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back

VPN3K: Traffic -> 3

                         Current Security Associations
-------------------------------------------------------------------------------
| 1. ESP-DES-MD5                       | 2. ESP-3DES-MD5                      |
| 3. ESP/IKE-3DES-MD5                  | 4. ESP-3DES-NONE                     |
| 5. ESP-L2TP-TRANSPORT                | 6. ESP-3DES-MD5-DH7                  |
| 7. ESP-3DES-MD5-DH5                  | 8. ESP-AES128-SHA                    |
-------------------------------------------------------------------------------

1) Add Security Associations
2) Modify Security Association
3) Delete Security Association
4) Copy Security Association
5) Back

VPN3K: Security Associations -> 4

> Copy which SA

VPN3K: Security Associations -> 2

> SA Name

VPN3K: Security Associations -> L2L:VPN_TO_R2

1) Modify SA Name
2) Modify the SA's Inheritance
3) Modify the IPSec Parameters
4) Modify the IKE Parameters
5) Back

VPN3K: Security Associations -> 4

1) Modify IKE Peer
2) Modify Negotiation Mode
3) Modify Authentication Method
4) Modify IKE Proposal
5) Back

VPN3K: Security Associations (IKE) -> 1

> IKE Peer

VPN3K: Security Associations (IKE) -> [ 0.0.0.0 ] 136.1.122.2

1) Modify IKE Peer
2) Modify Negotiation Mode
3) Modify Authentication Method
4) Modify IKE Proposal
5) Back

VPN3K: Security Associations (IKE) ->
```

Create rule to match outgoing traffic:

```
1) Configuration
2) Administration
3) Monitoring
```

```
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 4

1) Access Hours
2) Traffic Management
3) Group Matching
4) Network Admission Control
5) Back

VPN3K: Policy -> 2

1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back

VPN3K: Traffic -> 2

                             Current Filter Rules
-------------------------------------------------------------------------------
| 1. GRE In                            | 2. GRE Out                           |
| 3. IPSEC-ESP In                      | 4. IKE In                            |
| 5. IKE Out                           | 6. PPTP In                           |
| 7. PPTP Out                          | 8. L2TP In                           |
| 9. L2TP Out                          | 10. ICMP In                          |
| 11. ICMP Out                         | 12. RIP In                           |
| 13. RIP Out                          | 14. OSPF In                          |
| 15. OSPF Out                         | 16. Incoming HTTP In                 |
| 17. Incoming HTTP Out                | 18. VRRP In                          |
| 19. VRRP Out                         | 20. Any In                           |
| 21. Any Out                          | 22. Incoming HTTPS In                |
| 23. Incoming HTTPS Out               | 24. LDAP In                          |
| 25. LDAP Out                         | 26. Telnet/SSL In                    |
| 27. Telnet/SSL Out                   | 28. Outgoing HTTP In                 |
| 29. Outgoing HTTP Out                | 30. Outgoing HTTPS In                |
| 31. Outgoing HTTPS Out               | 32. CRL over LDAP In                 |
| 33. CRL over LDAP Out                | 34. SSH In                           |
| 35. SSH Out                          | 36. VCA In                           |
| 37. VCA Out                          | 38. NAT-T In                         |
| 39. NAT-T Out                        | 40. DHCP In                          |
| 41. DHCP Out                         |                                      |
-------------------------------------------------------------------------------

1) Add Filter Rule
2) Modify Filter Rule
3) Delete Filter Rule
4) Copy Filter Rule
5) Back
```

```
VPN3K: Filter Rules -> 1

> Rule Name

VPN3K: Filter Rules -> L2L:VPN_TO_R2 Out

1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back

VPN3K: Filter Rules -> 3

1) Use Single Address/Wildcard
2) Use Network List
3) Back

VPN3K: Filter Rules (Source) -> 1

> Source IP Address for this rule

VPN3K: Filter Rules (Source) -> [ 0.0.0.0 ] 150.1.1.0

> Wildcard Mask for this rule

VPN3K: Filter Rules (Source) -> [ 255.255.255.255 ] 0.0.0.255

1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back

VPN3K: Filter Rules -> 4

1) Use Single Address/Wildcard
2) Use Network List
3) Back

VPN3K: Filter Rules (Destination) -> 1

> Destination IP Address for this rule

VPN3K: Filter Rules (Destination) -> [ 0.0.0.0 ] 150.1.2.0

> Wildcard Mask for this rule

VPN3K: Filter Rules (Destination) -> [ 255.255.255.255 ] 0.0.0.255

1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
```

```
7) Modify ICMP Packet type
8) Back

VPN3K: Filter Rules -> 2

1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back

VPN3K: Filter Rules -> 1

1) Apply Rule to inbound data
2) Apply Rule to outbound data

VPN3K: Filter Rules -> [ 1 ] 2

1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back

VPN3K: Filter Rules -> 2

1) Drop
2) Forward
3) Drop and log
4) Forward and log
5) Apply IPSec
6) Apply IPSec and log
7) Override Tunnel Default Gateway
8) Override Tunnel Default Gateway and log

VPN3K: Filter Rules -> [ 1 ] 5

1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back
```

Create rule for inbound traffic (for policy matching):

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 4

1) Access Hours
2) Traffic Management
```

```
3) Group Matching
4) Network Admission Control
5) Back

VPN3K: Policy -> 2

1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back

VPN3K: Traffic -> 2

                             Current Filter Rules
-------------------------------------------------------------------------------
| 1. GRE In                            | 2. GRE Out                           |
| 3. IPSEC-ESP In                      | 4. IKE In                            |
| 5. IKE Out                           | 6. PPTP In                           |
| 7. PPTP Out                          | 8. L2TP In                           |
| 9. L2TP Out                          | 10. ICMP In                          |
| 11. ICMP Out                         | 12. RIP In                           |
| 13. RIP Out                          | 14. OSPF In                          |
| 15. OSPF Out                         | 16. Incoming HTTP In                 |
| 17. Incoming HTTP Out                | 18. VRRP In                          |
| 19. VRRP Out                         | 20. Any In                           |
| 21. Any Out                          | 22. Incoming HTTPS In                |
| 23. Incoming HTTPS Out               | 24. LDAP In                          |
| 25. LDAP Out                         | 26. Telnet/SSL In                    |
| 27. Telnet/SSL Out                   | 28. Outgoing HTTP In                 |
| 29. Outgoing HTTP Out                | 30. Outgoing HTTPS In                |
| 31. Outgoing HTTPS Out               | 32. CRL over LDAP In                 |
| 33. CRL over LDAP Out                | 34. SSH In                           |
| 35. SSH Out                          | 36. VCA In                           |
| 37. VCA Out                          | 38. NAT-T In                         |
| 39. NAT-T Out                        | 40. DHCP In                          |
| 41. DHCP Out                         | 42. L2L:VPN_TO_R2 Out                |
'q' to Quit, '<SPACE>' to Continue ->
-------------------------------------------------------------------------------

1) Add Filter Rule
2) Modify Filter Rule
3) Delete Filter Rule
4) Copy Filter Rule
5) Back

VPN3K: Filter Rules -> 1

> Rule Name

VPN3K: Filter Rules -> L2L:VPN_TO_R2 In

1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back
```

```
VPN3K: Filter Rules -> 3

1) Use Single Address/Wildcard
2) Use Network List
3) Back

VPN3K: Filter Rules (Source) -> 1

> Source IP Address for this rule

VPN3K: Filter Rules (Source) -> [ 0.0.0.0 ] 150.1.2.0

> Wildcard Mask for this rule

VPN3K: Filter Rules (Source) -> [ 255.255.255.255 ] 0.0.0.255

1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back

VPN3K: Filter Rules -> 4

1) Use Single Address/Wildcard
2) Use Network List
3) Back

VPN3K: Filter Rules (Destination) -> 1

> Destination IP Address for this rule

VPN3K: Filter Rules (Destination) -> [ 0.0.0.0 ] 150.1.1.0

> Wildcard Mask for this rule

VPN3K: Filter Rules (Destination) -> [ 255.255.255.255 ] 0.0.0.255

1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back

VPN3K: Filter Rules -> 2

1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back

VPN3K: Filter Rules -> 1

1) Apply Rule to inbound data
2) Apply Rule to outbound data

VPN3K: Filter Rules -> [ 1 ] 1
```

```
1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back

VPN3K: Filter Rules -> 2

1) Drop
2) Forward
3) Drop and log
4) Forward and log
5) Apply IPSec
6) Apply IPSec and log
7) Override Tunnel Default Gateway
8) Override Tunnel Default Gateway and log

VPN3K: Filter Rules -> [ 1 ] 5

1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back

VPN3K: Filter Rules -> 4
```

Assign rules to the Public traffic filer:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 4

1) Access Hours
2) Traffic Management
3) Group Matching
4) Network Admission Control
5) Back

VPN3K: Policy -> 2

1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back

VPN3K: Traffic -> 4
```

```
                              Current Active Filters
--------------------------------------------------------------------------------
| 1. Private (Default)                 | 2. Public (Default)                  |
| 3. External (Default)                | 4. Firewall Filter for VPN Client (De|
--------------------------------------------------------------------------------

1) Add a Filter
2) Modify a Filter
3) Delete a Filter
4) Assign Rules to a Filter
5) Copy a Filter
6) Back

VPN3K: Filters -> 4

> Which Filter to assign Rules to

VPN3K: Filters -> 2

                        The Current Rules for this Filter
--------------------------------------------------------------------------------
| 1. GRE In                            | IN FORWARD                           |
| 2. IPSEC-ESP In                      | IN FORWARD                           |
| 3. IKE In                            | IN FORWARD                           |
| 4. PPTP In                           | IN FORWARD                           |
| 5. L2TP In                           | IN FORWARD                           |
| 6. ICMP In                           | IN FORWARD                           |
| 7. VRRP In                           | IN FORWARD                           |
| 8. NAT-T In                          | IN FORWARD                           |
| 9. GRE Out                           | OUT FORWARD                          |
| 10. IKE Out                          | OUT FORWARD                          |
| 11. PPTP Out                         | OUT FORWARD                          |
| 12. L2TP Out                         | OUT FORWARD                          |
| 13. ICMP Out                         | OUT FORWARD                          |
| 14. VRRP Out                         | OUT FORWARD                          |
| 15. NAT-T Out                        | OUT FORWARD                          |
--------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3K: Filters -> 1

                              Current Filter Rules
--------------------------------------------------------------------------------
| 1. GRE In                            | 2. GRE Out                           |
| 3. IPSEC-ESP In                      | 4. IKE In                            |
| 5. IKE Out                           | 6. PPTP In                           |
| 7. PPTP Out                          | 8. L2TP In                           |
| 9. L2TP Out                          | 10. ICMP In                          |
| 11. ICMP Out                         | 12. RIP In                           |
| 13. RIP Out                          | 14. OSPF In                          |
| 15. OSPF Out                         | 16. Incoming HTTP In                 |
| 17. Incoming HTTP Out                | 18. VRRP In                          |
| 19. VRRP Out                         | 20. Any In                           |
| 21. Any Out                          | 22. Incoming HTTPS In                |
| 23. Incoming HTTPS Out               | 24. LDAP In                          |
| 25. LDAP Out                         | 26. Telnet/SSL In                    |
```

```
| 27. Telnet/SSL Out                    | 28. Outgoing HTTP In                  |
| 29. Outgoing HTTP Out                 | 30. Outgoing HTTPS In                 |
| 31. Outgoing HTTPS Out                | 32. CRL over LDAP In                  |
| 33. CRL over LDAP Out                 | 34. SSH In                            |
| 35. SSH Out                           | 36. VCA In                            |
| 37. VCA Out                           | 38. NAT-T In                          |
| 39. NAT-T Out                         | 40. DHCP In                           |
| 41. DHCP Out                          | 42. L2L:VPN_TO_R2 Out                 |
'q' to Quit, '<SPACE>' to Continue ->
| 43. L2L:VPN_TO_R2 In                  |                                       |
-------------------------------------------------------------------------------

> Which Rule to add

VPN3K: Filters -> 42

                        The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. L2L:VPN_TO_R2 Out                  | OUT IPSEC                             |
| 2. GRE In                             | IN FORWARD                            |
| 3. IPSEC-ESP In                       | IN FORWARD                            |
| 4. IKE In                             | IN FORWARD                            |
| 5. PPTP In                            | IN FORWARD                            |
| 6. L2TP In                            | IN FORWARD                            |
| 7. ICMP In                            | IN FORWARD                            |
| 8. VRRP In                            | IN FORWARD                            |
| 9. NAT-T In                           | IN FORWARD                            |
| 10. GRE Out                           | OUT FORWARD                           |
| 11. IKE Out                           | OUT FORWARD                           |
| 12. PPTP Out                          | OUT FORWARD                           |
| 13. L2TP Out                          | OUT FORWARD                           |
| 14. ICMP Out                          | OUT FORWARD                           |
| 15. VRRP Out                          | OUT FORWARD                           |
| 16. NAT-T Out                         | OUT FORWARD                           |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3K: Filters -> 1

                              Current Filter Rules
-------------------------------------------------------------------------------
| 1. GRE In                             | 2. GRE Out                            |
| 3. IPSEC-ESP In                       | 4. IKE In                             |
| 5. IKE Out                            | 6. PPTP In                            |
| 7. PPTP Out                           | 8. L2TP In                            |
| 9. L2TP Out                           | 10. ICMP In                           |
| 11. ICMP Out                          | 12. RIP In                            |
| 13. RIP Out                           | 14. OSPF In                           |
| 15. OSPF Out                          | 16. Incoming HTTP In                  |
| 17. Incoming HTTP Out                 | 18. VRRP In                           |
| 19. VRRP Out                          | 20. Any In                            |
| 21. Any Out                           | 22. Incoming HTTPS In                 |
| 23. Incoming HTTPS Out                | 24. LDAP In                           |
| 25. LDAP Out                          | 26. Telnet/SSL In                     |
| 27. Telnet/SSL Out                    | 28. Outgoing HTTP In                  |
| 29. Outgoing HTTP Out                 | 30. Outgoing HTTPS In                 |
| 31. Outgoing HTTPS Out                | 32. CRL over LDAP In                  |
```

```
| 33. CRL over LDAP Out                | 34. SSH In                           |
| 35. SSH Out                          | 36. VCA In                           |
| 37. VCA Out                          | 38. NAT-T In                         |
| 39. NAT-T Out                        | 40. DHCP In                          |
| 41. DHCP Out                         | 42. L2L:VPN_TO_R2 Out                |
'q' to Quit, '<SPACE>' to Continue ->
| 43. L2L:VPN_TO_R2 In                 |                                      |
-------------------------------------------------------------------------------

> Which Rule to add

VPN3K: Filters -> 43

                        The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. L2L:VPN_TO_R2 In                  | IN IPSEC                             |
| 2. L2L:VPN_TO_R2 Out                 | OUT IPSEC                            |
| 3. GRE In                            | IN FORWARD                           |
| 4. IPSEC-ESP In                      | IN FORWARD                           |
| 5. IKE In                            | IN FORWARD                           |
| 6. PPTP In                           | IN FORWARD                           |
| 7. L2TP In                           | IN FORWARD                           |
| 8. ICMP In                           | IN FORWARD                           |
| 9. VRRP In                           | IN FORWARD                           |
| 10. NAT-T In                         | IN FORWARD                           |
| 11. GRE Out                          | OUT FORWARD                          |
| 12. IKE Out                          | OUT FORWARD                          |
| 13. PPTP Out                         | OUT FORWARD                          |
| 14. L2TP Out                         | OUT FORWARD                          |
| 15. ICMP Out                         | OUT FORWARD                          |
| 16. VRRP Out                         | OUT FORWARD                          |
| 17. NAT-T Out                        | OUT FORWARD                          |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3K: Filters -> 5

> Enter the Rule

VPN3K: Filters -> 1

                          Current Security Associations
-------------------------------------------------------------------------------
| 1. ESP-DES-MD5                       | 2. ESP-3DES-MD5                      |
| 3. ESP/IKE-3DES-MD5                  | 4. ESP-3DES-NONE                     |
| 5. ESP-L2TP-TRANSPORT                | 6. ESP-3DES-MD5-DH7                  |
| 7. ESP-3DES-MD5-DH5                  | 8. ESP-AES128-SHA                    |
| 9. L2L:VPN_TO_R2                     |                                      |
-------------------------------------------------------------------------------

> Enter the Security Association

VPN3K: Filters -> 9

                        The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. L2L:VPN_TO_R2 In                  | IN IPSEC L2L:VPN_TO_R2               |
```

```
| 2. L2L:VPN_TO_R2 Out                    | OUT IPSEC                          |
| 3. GRE In                               | IN FORWARD                         |
| 4. IPSEC-ESP In                         | IN FORWARD                         |
| 5. IKE In                               | IN FORWARD                         |
| 6. PPTP In                              | IN FORWARD                         |
| 7. L2TP In                              | IN FORWARD                         |
| 8. ICMP In                              | IN FORWARD                         |
| 9. VRRP In                              | IN FORWARD                         |
| 10. NAT-T In                            | IN FORWARD                         |
| 11. GRE Out                             | OUT FORWARD                        |
| 12. IKE Out                             | OUT FORWARD                        |
| 13. PPTP Out                            | OUT FORWARD                        |
| 14. L2TP Out                            | OUT FORWARD                        |
| 15. ICMP Out                            | OUT FORWARD                        |
| 16. VRRP Out                            | OUT FORWARD                        |
| 17. NAT-T Out                           | OUT FORWARD                        |
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back

VPN3K: Filters -> 5

> Enter the Rule

VPN3K: Filters -> 2

                         Current Security Associations
-------------------------------------------------------------------------------
| 1. ESP-DES-MD5                        | 2. ESP-3DES-MD5                    |
| 3. ESP/IKE-3DES-MD5                   | 4. ESP-3DES-NONE                   |
| 5. ESP-L2TP-TRANSPORT                 | 6. ESP-3DES-MD5-DH7                |
| 7. ESP-3DES-MD5-DH5                   | 8. ESP-AES128-SHA                  |
| 9. L2L:VPN_TO_R2                      |                                    |
-------------------------------------------------------------------------------

> Enter the Security Association

VPN3K: Filters -> 9

                       The Current Rules for this Filter
-------------------------------------------------------------------------------
| 1. L2L:VPN_TO_R2 In                   | IN IPSEC L2L:VPN_TO_R2             |
| 2. L2L:VPN_TO_R2 Out                  | OUT IPSEC L2L:VPN_TO_R2            |
| 3. GRE In                             | IN FORWARD                         |
| 4. IPSEC-ESP In                       | IN FORWARD                         |
| 5. IKE In                             | IN FORWARD                         |
| 6. PPTP In                            | IN FORWARD                         |
| 7. L2TP In                            | IN FORWARD                         |
| 8. ICMP In                            | IN FORWARD                         |
| 9. VRRP In                            | IN FORWARD                         |
| 10. NAT-T In                          | IN FORWARD                         |
| 11. GRE Out                           | OUT FORWARD                        |
| 12. IKE Out                           | OUT FORWARD                        |
| 13. PPTP Out                          | OUT FORWARD                        |
| 14. L2TP Out                          | OUT FORWARD                        |
| 15. ICMP Out                          | OUT FORWARD                        |
| 16. VRRP Out                          | OUT FORWARD                        |
| 17. NAT-T Out                         | OUT FORWARD                        |
```

```
-------------------------------------------------------------------------------

1) Add a Rule to this Filter
2) Remove a Rule from this Filter
3) Move the Rule Up
4) Move the Rule Down
5) Assign Security Assoc. to Rule
6) Back
```

Create Tunnel Group:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 3

1) Base Group
2) Groups
3) Users
4) Back

VPN3K: User Management -> 2

                                Current User Groups
-------------------------------------------------------------------------------
                                  No User Groups
-------------------------------------------------------------------------------

1) Add a Group
2) Modify a Group
3) Delete a Group
4) Back

VPN3K: Groups -> 1

> Group Name

VPN3K: Groups -> 136.1.122.2

> Password

VPN3K: Groups -> CISCO

Verify -> CISCO

1) Group Type - Internal
2) Group Type - External

VPN3K: Groups -> 1
```

```
1) Identification
2) General Parameters
3) Servers
4) IPSec Parameters
5) VPN Client Firewall Parameters
6) Hardware Client Parameters
7) PPTP/L2TP Parameters
8) Address Pools
9) Client Update
10) Assign Bandwidth Policies
11) WebVPN Parameters
12) NAC Parameters
13) Back

VPN3K: Groups -> 4

1) Select IPSec SA
2) Select IKE Peer Validation
3) Enable/Disable IKE Keepalives
4) Set Confidence Interval
5) Set Tunnel Type
6) Back

VPN3K: Groups -> 1

                          Current Security Associations
-------------------------------------------------------------------------------
| 0. Use '0' for no selection          | 1. ESP-DES-MD5                       |
| 2. ESP-3DES-MD5                      | 3. ESP/IKE-3DES-MD5                  |
| 4. ESP-3DES-NONE                     | 5. ESP-L2TP-TRANSPORT                |
| 6. ESP-3DES-MD5-DH7                  | 7. ESP-3DES-MD5-DH5                  |
| 8. ESP-AES128-SHA                    | 9. L2L:VPN_TO_R2                     |
-------------------------------------------------------------------------------

> IPSec SA

VPN3K: Groups -> [ (inherited) ESP-3DES-MD5 ] 9

1) Select IPSec SA
2) Select IKE Peer Validation
3) Enable/Disable IKE Keepalives
4) Set Confidence Interval
5) Set Tunnel Type
6) Back

VPN3K: Groups -> 5

1) LAN-to-LAN
2) Remote Access

VPN3K: Groups -> [ (inherited) 2 ] 1

1) Select IPSec SA
2) Select IKE Peer Validation
3) Enable/Disable IKE Keepalives
4) Set Confidence Interval
5) Set Tunnel Type
6) Back

VPN3K: Groups ->
```

Verification

```
R2#ping 150.1.1.1 so lo 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms

R2#sho crypto isakmp sa
dst             src             state          conn-id slot
136.1.121.11    136.1.122.2     QM_IDLE              1    0

R2#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.11:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.11
     path mtu 1500, media mtu 1500
     current outbound spi: 49A180DF

     inbound esp sas:
      spi: 0x380D5231(940397105)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4433672/3564)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x49A180DF(1235321055)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4433672/3564)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

Monitor session at VPN3k:

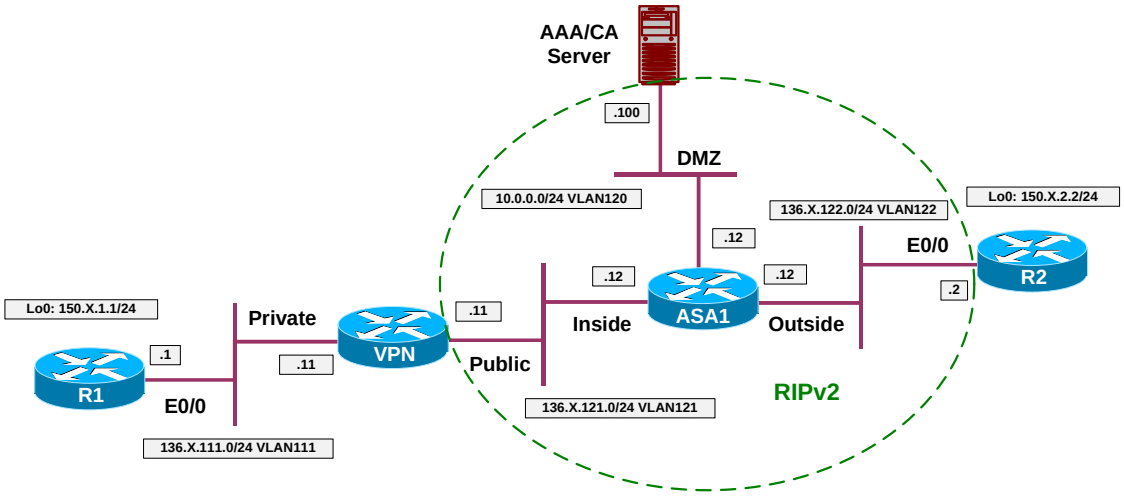
```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 3

1) Routing Table
2) Event Log
3) System Status
4) Sessions
5) General Statistics
6) Dynamic Filters
7) Back

VPN3K: Monitor -> 4

1) View Session Statistics
2) View Top Ten Lists
3) View Session Protocols
4) View Session Encryption
5) Filter Sessions on Group
6) Back

VPN3K: Sessions -> 1

Active Sessions
---------------
Active LAN-to-LAN Sessions:    1
Active Remote Access Sessions: 0
Active Management Sessions:    1
Total Active Sessions:         2
Weighted Active Load:          1
Percent Session Load:          1.00%
Total Active Sessions:         2
Peak Concurrent Sessions:      2
Total Cumulative Sessions:     8

 Num   Username   IP Address    Protocol  Encrypt  Duration  Data Tx   Data Rx
-------------------------------------------------------------------------------
    1 admin     Local           Console  None      0:10:44        N/A       N/A
    2 Auth'ing  136.1.122.2     IPSecL2L 3DES168   0:02:45        936       936

1) Refresh Session Statistics
2) Reset Session Statistics
3) Restore Session Statistics
4) Session Details
5) Back

VPN3K: Sessions ->
```

📖 Further Reading

Tunneling and Security: IPsec LAN-to-LAN

IOS and VPN3k with Digital Certificates

Objective: Configure L2L IPsec tunnel between IOS and VPN3k using authentication based on Digital Certificates.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and VPN3k with PSK".
- Enroll VPN3k with CA:
  - Set up clock synchronization via NTP with CA server.
    - Configure Public traffic filter to permit Outgoing NTP as follows:
      - Configure two rules: inbound and outbound.
      - Assign them to Public traffic filter.
  - Retrieve CA Certificate via SCEP:
    - Configure Public traffic filter to permit:
      - Ougoing HTTP traffic In and Out.
      - Use the pre-configured rules for this task.
    - Use enrollment URL http://10.0.0.100/certsrv/mscep/mscep.dll
  - Generate Certificate Request.
- Enroll R2 with CA:
  - Configure domain-name and generate key-pair.

- o Synchronize clock via NTP with CA Server.
- o Configure CA Trustpoint as follows:
    - Use enrollment URL: http://10.0.0.100/certsrv/mscep/mscep.dll
    - Configure CRL as optional.
    - Use RA mode.

- Modify L2L Tunnel settings on VPN3k as follows:
    - o Use IKE Proposal with “RSA” keyword (RSA-Sig authentication).
    - o Chose certificate you have requested to be used for authentication.

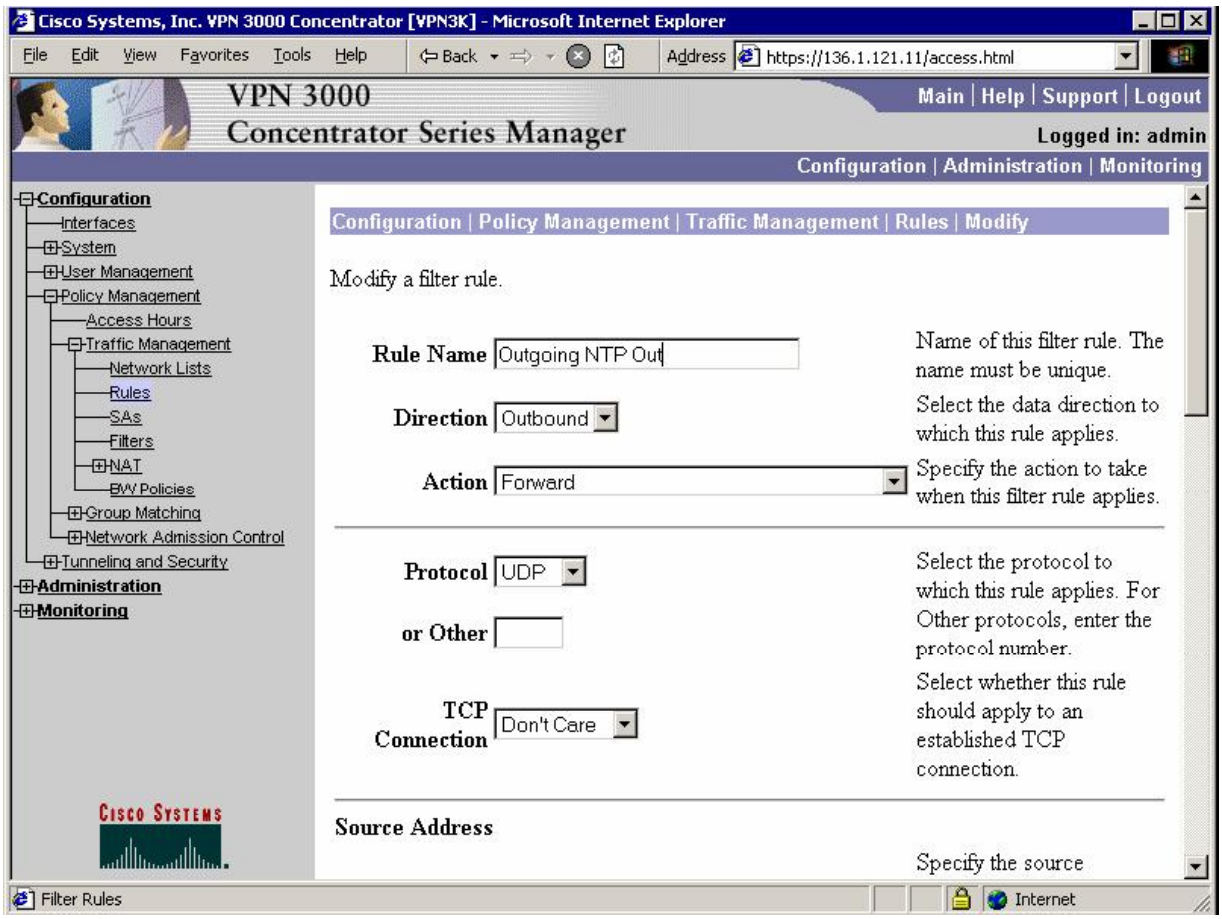
- Modify ISAKMP policy at R2 to use RSA-sig authentication.

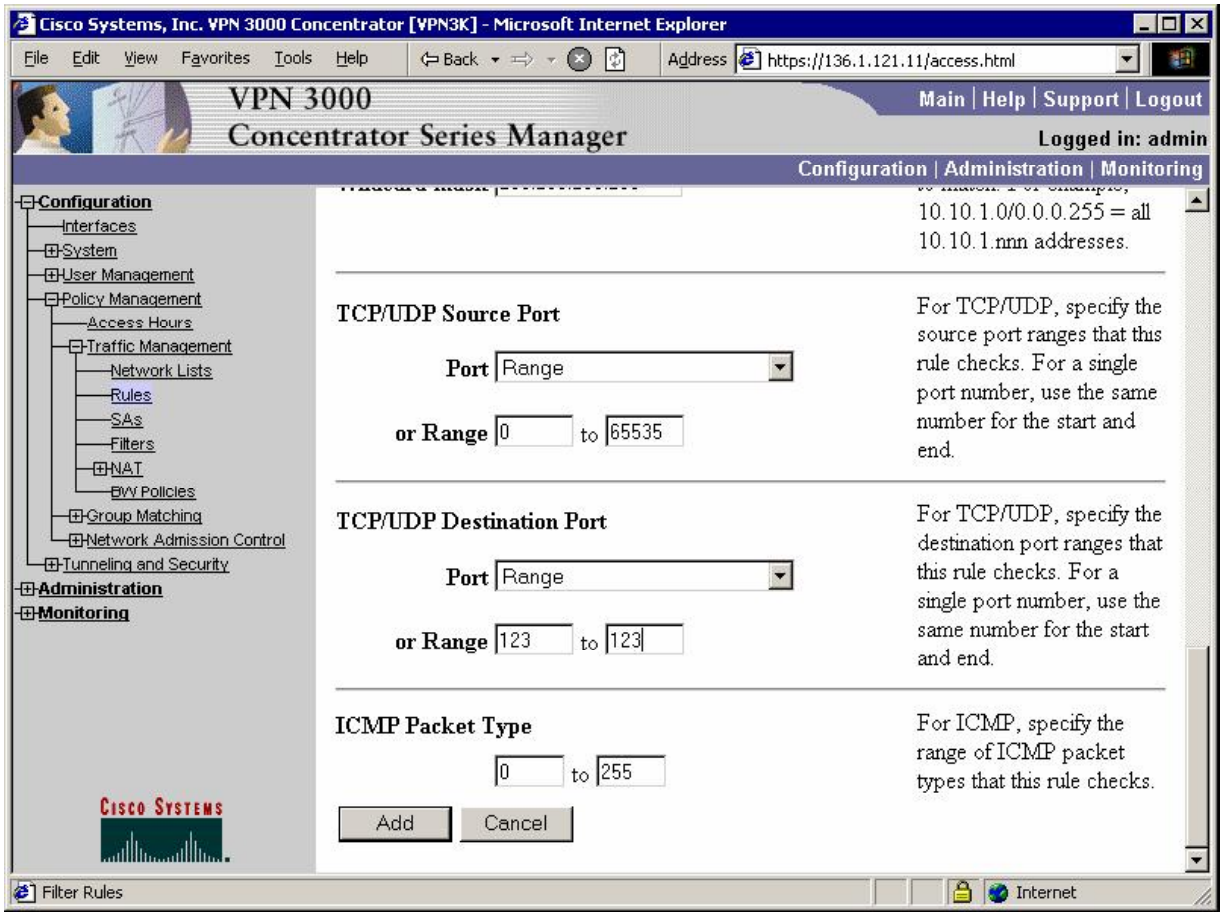
Final Configuration

```
R2:
crypto isakmp policy 10
 authentication rsa-sig
!
crypto ca trustpoint IE1
 enrollment url http://10.0.0.100/certsrv/mscep/mscep.dll
 crl optional
 enrollment mode ra
 exit
!
! Configure NTP server
!
ntp server 10.0.0.100
!
! Generate RSA key, authenticate CA and enroll
!
ip domain-name internetworkexpert.com
hostname R2
crypto key generate rsa general modulus 512
crypto ca authenticate IE1
crypto ca enroll IE1
```

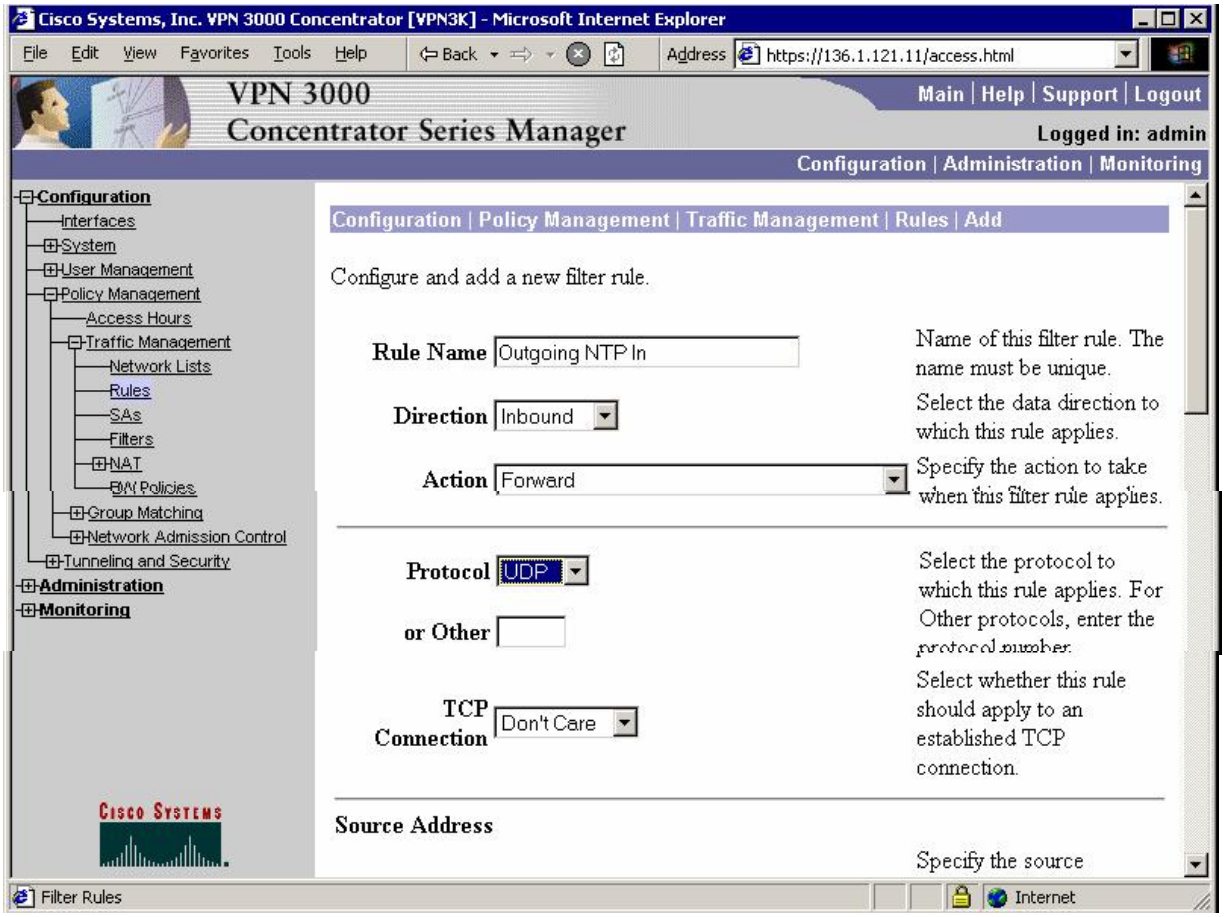
VPN3k:

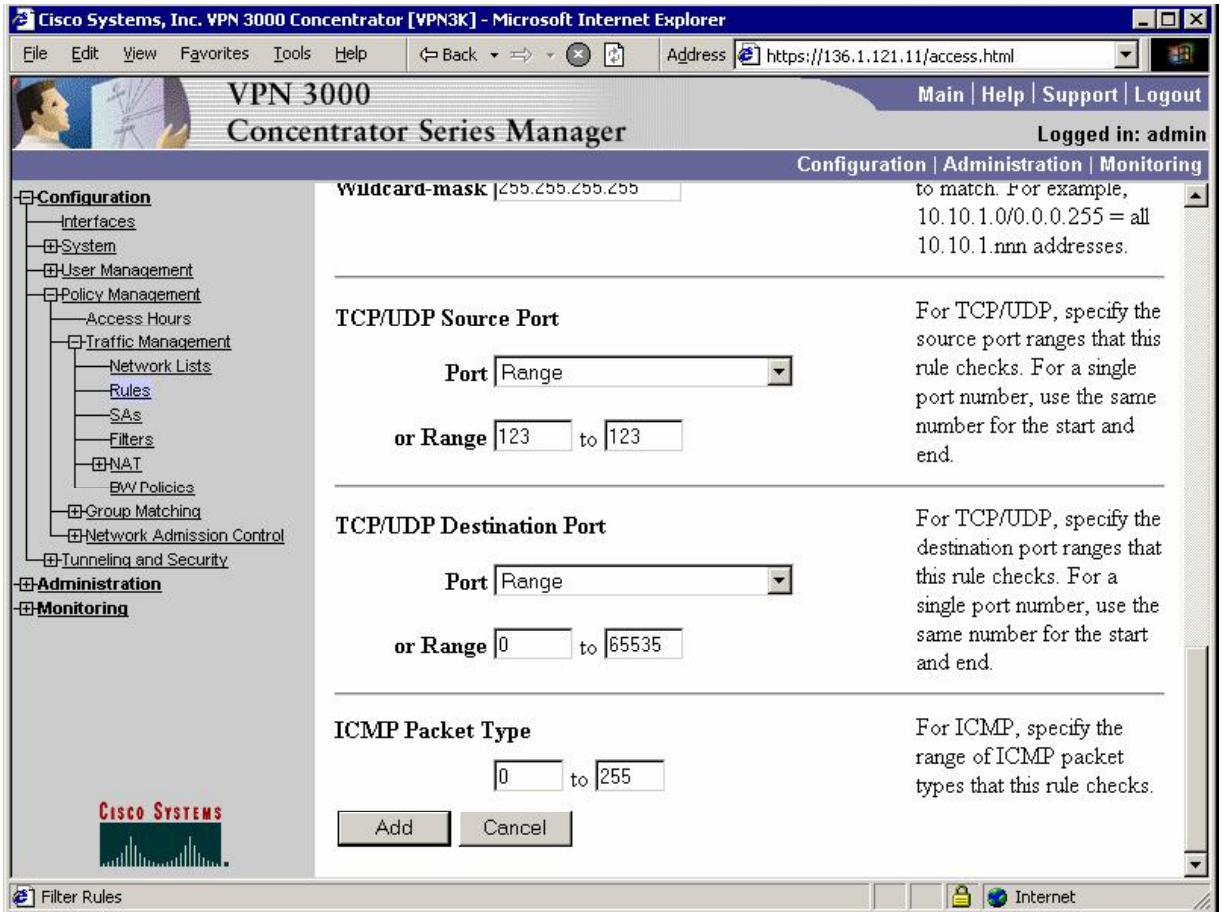
Create rule for Outgoing NTP Out:



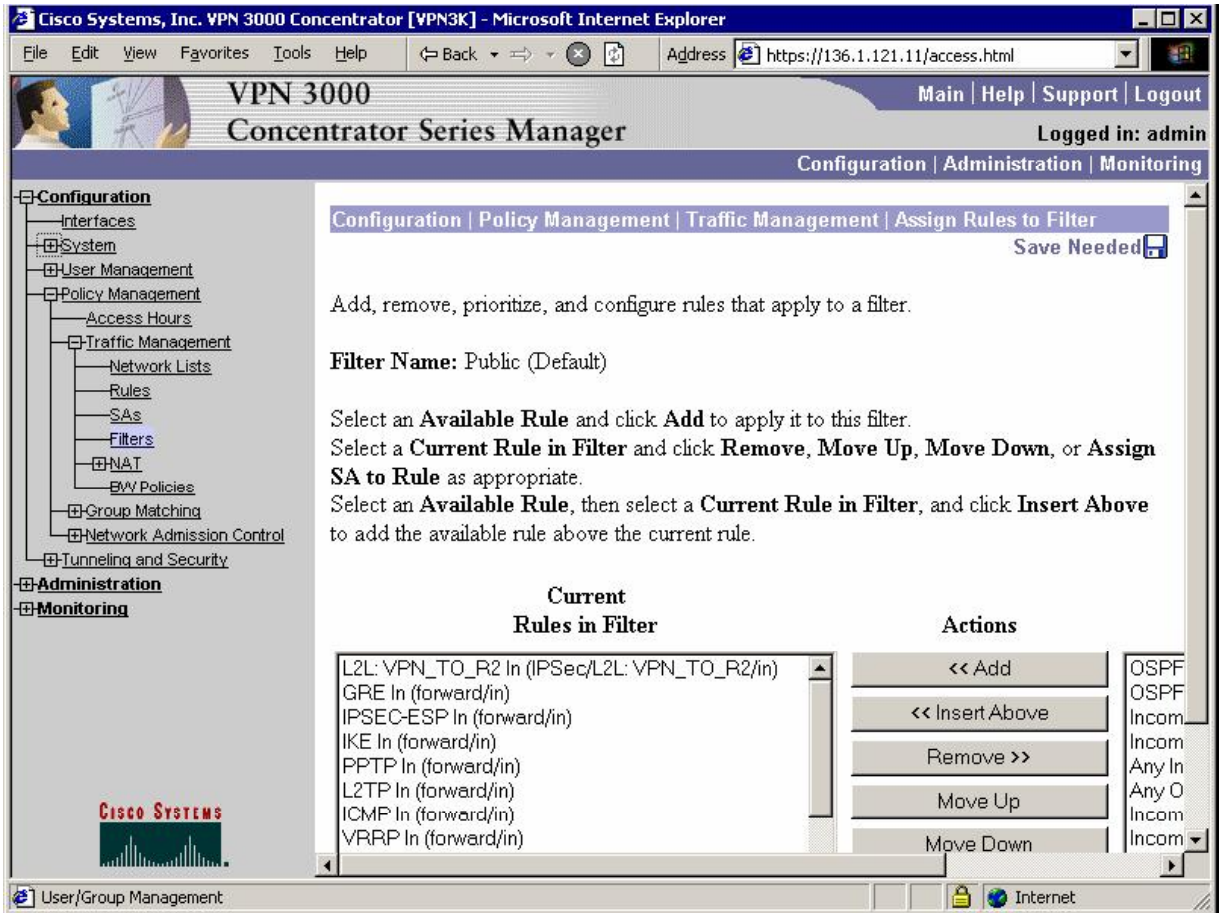

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
TCP/UDP Source Port
Port Range
or Range 0 to 65535
For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.
TCP/UDP Destination Port
Port Range
or Range 123 to 123
For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.
ICMP Packet Type
0 to 255
For ICMP, specify the range of ICMP packet types that this rule checks.
Add
Cancel
Cisco Systems
Filter Rules
Internet

Create rule for Outgoing NTP in:



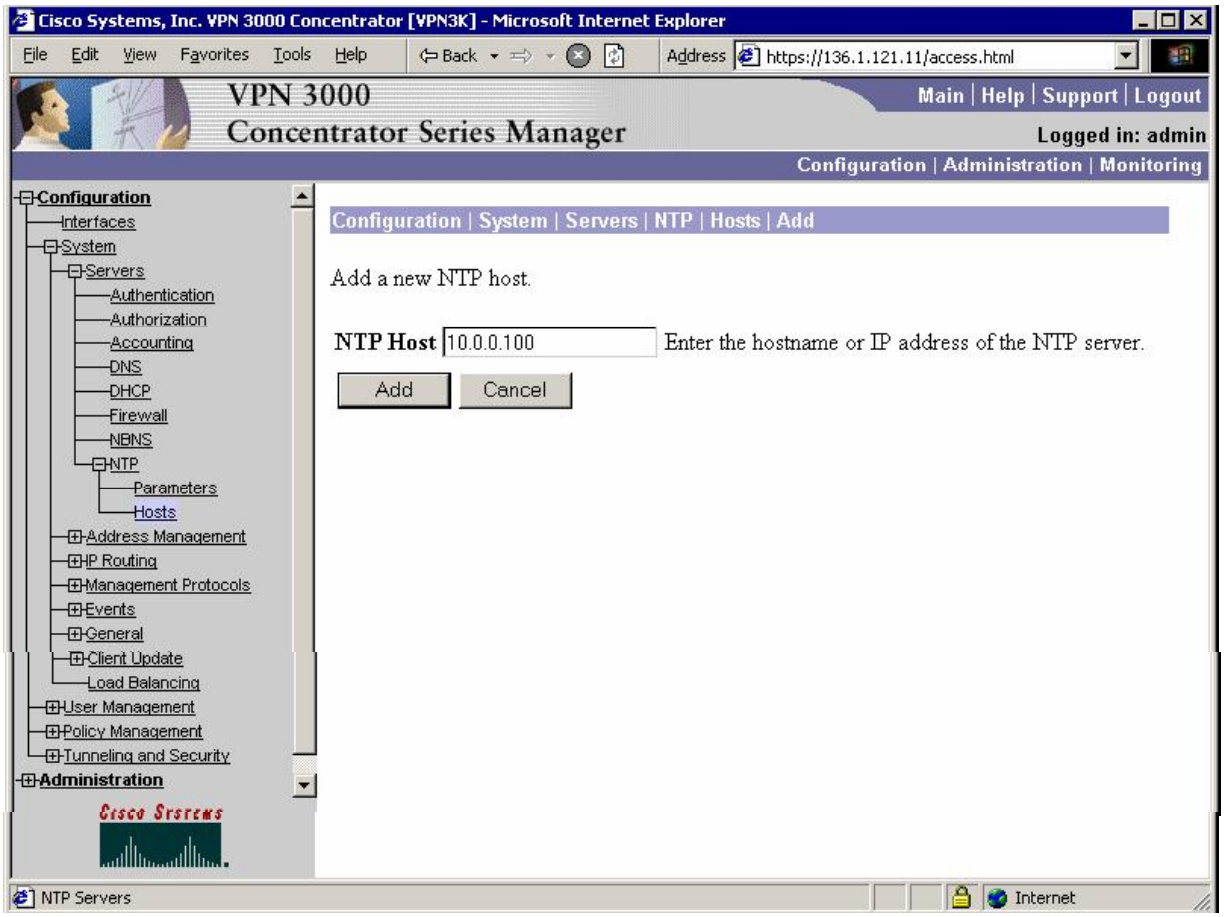

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Wildcard-mask 255.255.255.255
to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
TCP/UDP Source Port
Port Range
or Range 123 to 123
For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.
TCP/UDP Destination Port
Port Range
or Range 0 to 65535
For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.
ICMP Packet Type
0 to 255
For ICMP, specify the range of ICMP packet types that this rule checks.
Add
Cancel
Cisco Systems
Filter Rules
Internet

Add rules to Public filter, permitting outgoing NTP:



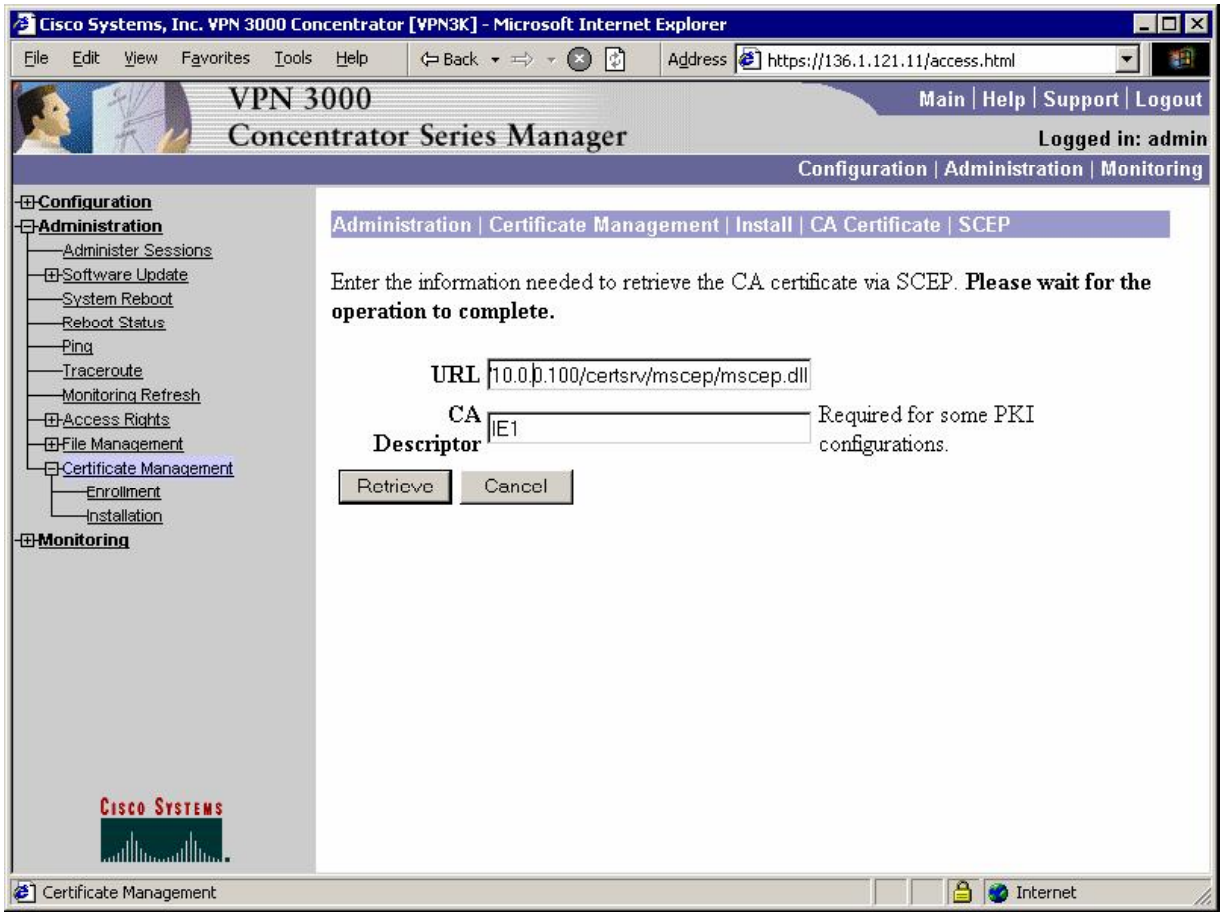

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Filter Name: Public (Default)
Select an Available Rule and click Add to apply it to this filter.
Select a Current Rule in Filter and click Remove, Move Up, Move Down, or Assign SA to Rule as appropriate.
Select an Available Rule, then select a Current Rule in Filter, and click Insert Above to add the available rule above the current rule.
Current Rules in Filter
Actions
Outgoing NTP In (forward/in)
L2L: VPN_TO_R2 Out (IPSec/L2L: VPN_TO_R2/out)
GRE Out (forward/out)
IKE Out (forward/out)
PPTP Out (forward/out)
L2TP Out (forward/out)
ICMP Out (forward/out)
VRRP Out (forward/out)
NAT-T Out (forward/out)
RIP Out (forward/out)
Outgoing HTTP Out (forward/out)
Outgoing NTP Out (forward/out)
<< Add
<< Insert Above
Remove >>
Move Up
Move Down
Assign SA to Rule
Done
Cisco Systems
User/Group Management
Internet

Configure NTP Server:

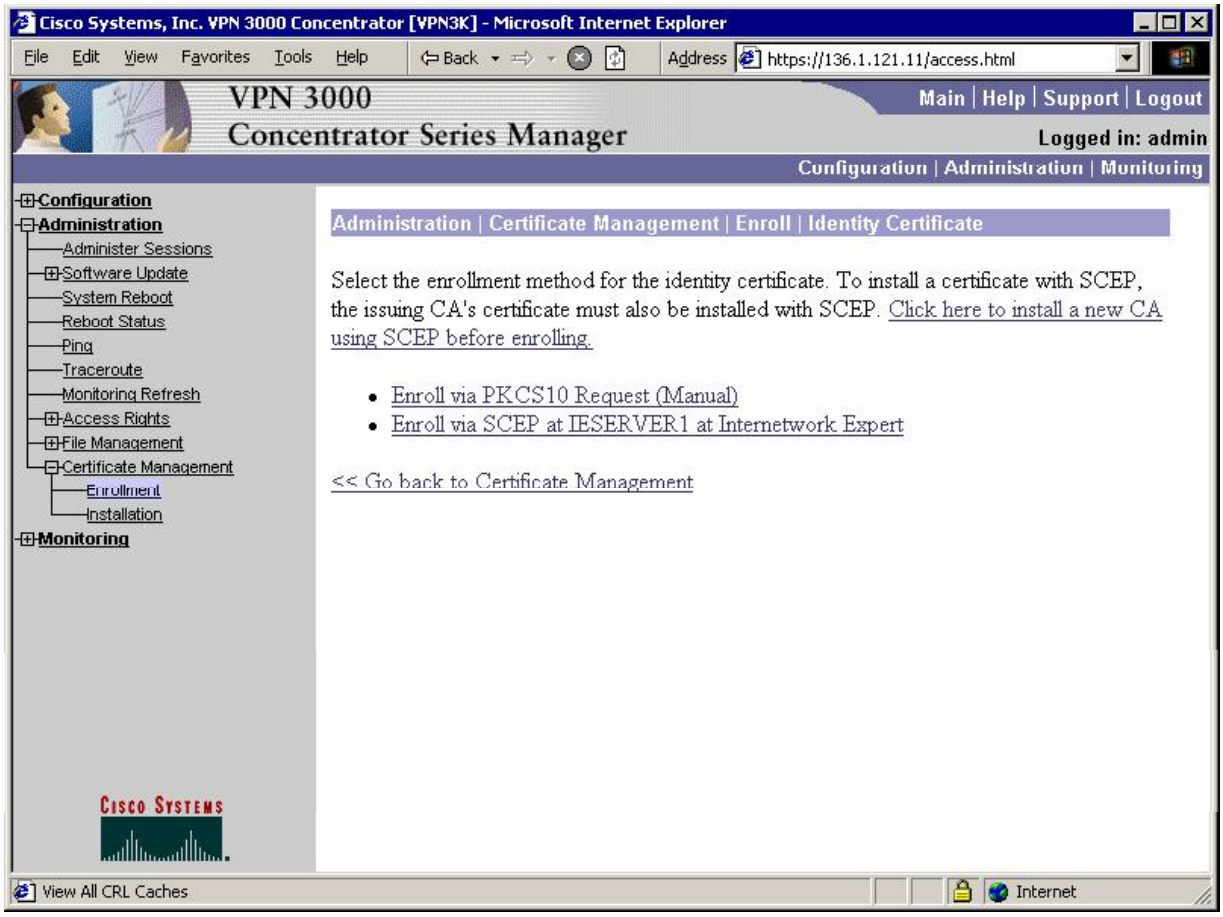


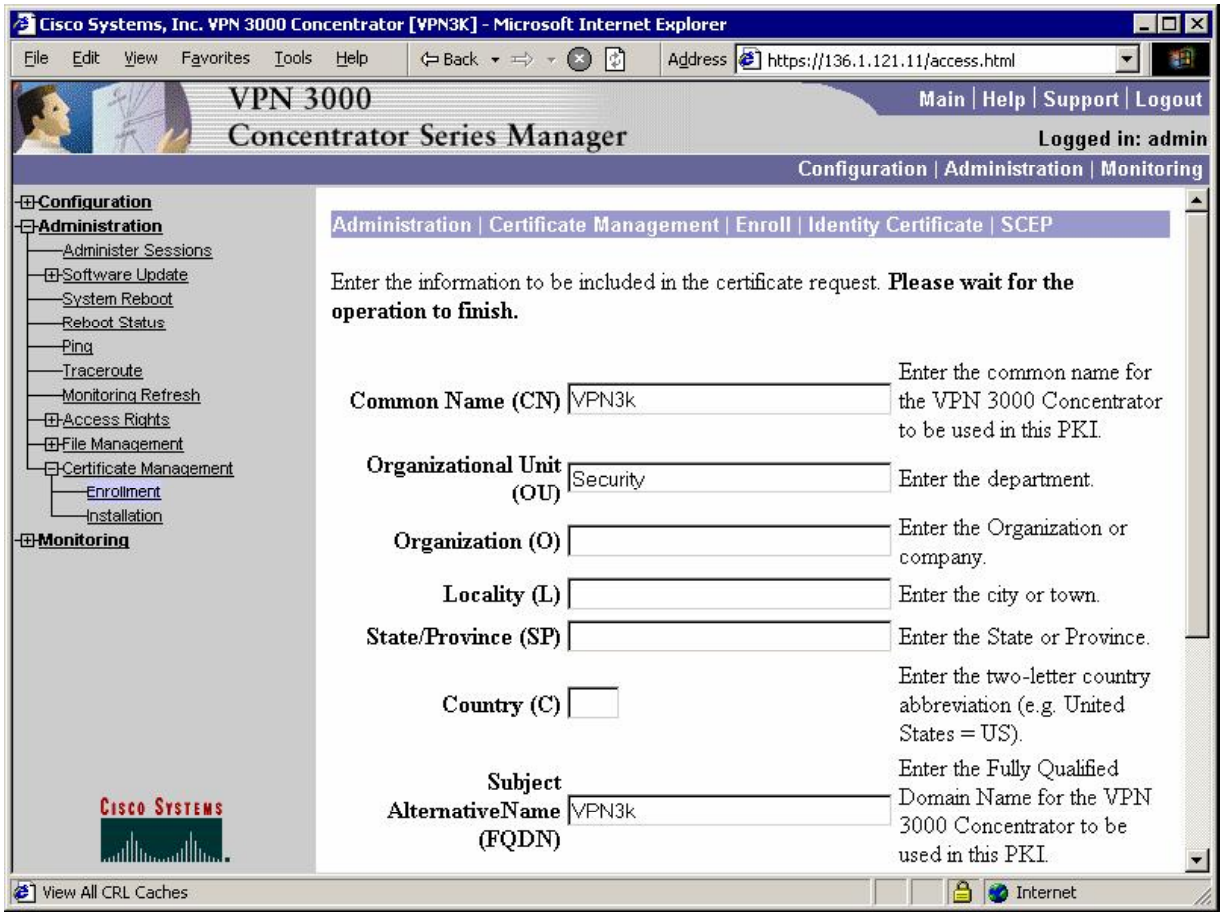
Add rules to Public filter, permitting Outgoing HTTP In/Out (for SCEP):

Install CA Certificate:


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Traceroute
Monitoring Refresh
Access Rights
File Management
Certificate Management
Enrollment
Installation
Monitoring
Administration | Certificate Management | Install | CA Certificate | SCEP
Enter the information needed to retrieve the CA certificate via SCEP. Please wait for the operation to complete.
URL 10.0.0.100/certsrv/mscep/mscep.dll
CA Descriptor IE1
Required for some PKI configurations.
Retrieve
Cancel
Cisco Systems
Certificate Management
Internet

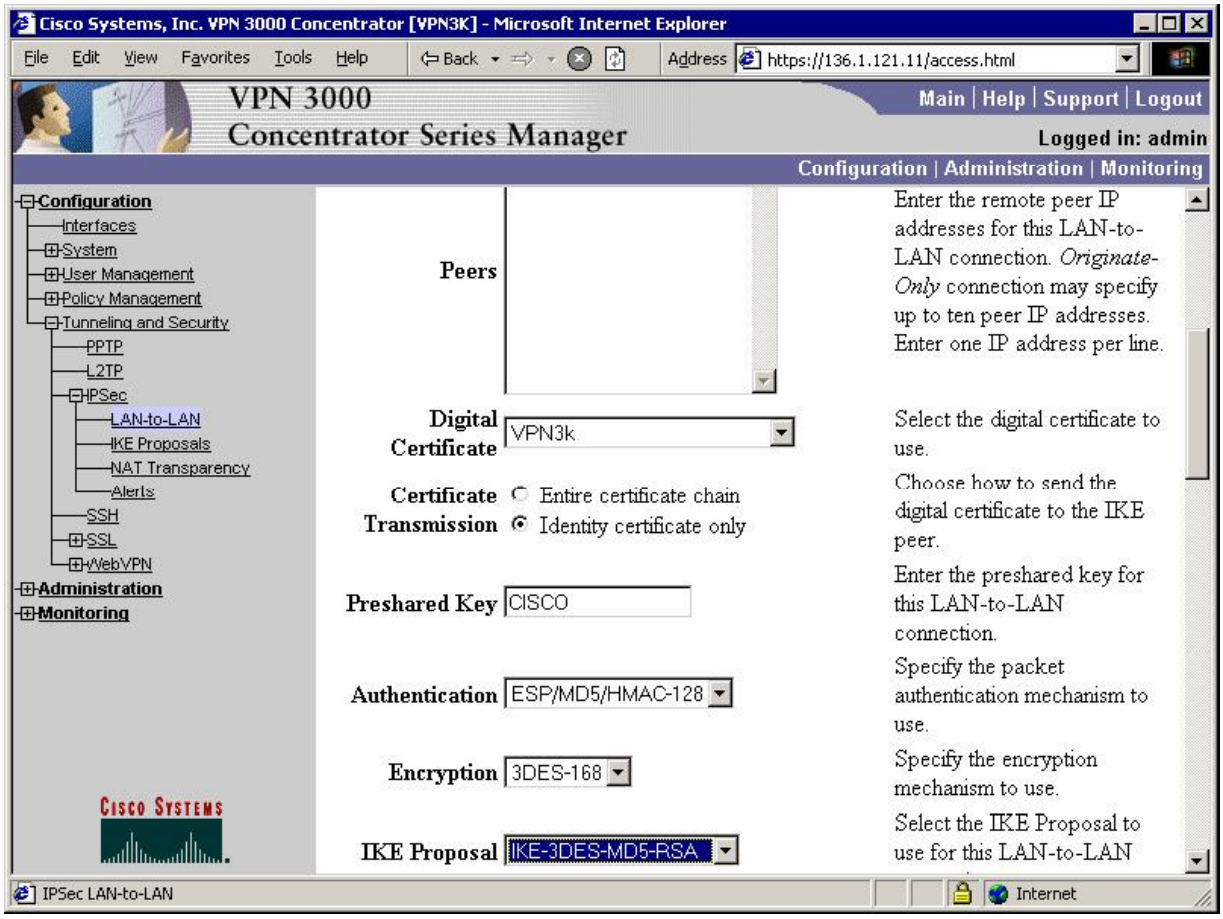
Enroll with certification authority:




Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Traceroute
Monitoring Refresh
Access Rights
File Management
Certificate Management
Enrollment
Installation
Monitoring
Administration | Certificate Management | Enroll | Identity Certificate | SCEP
Enter the information to be included in the certificate request. Please wait for the operation to finish.
Common Name (CN)
VPN3k
Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)
Security
Enter the department.
Organization (O)
Enter the Organization or company.
Locality (L)
Enter the city or town.
State/Province (SP)
Enter the State or Province.
Country (C)
Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)
VPN3k
Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Cisco Systems
View All CRL Caches
Internet


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Traceroute
Monitoring Refresh
Access Rights
File Management
Certificate Management
Enrollment
Installation
Monitoring
Administration | Certificate Management | Enrollment | Request Generated
A certificate request has been generated.
SCEP Status: Installed
Go to Certificate Management
Go to Certificate Enrollment
Go to Certificate Installation
Cisco Systems
View All CRL Caches
Internet

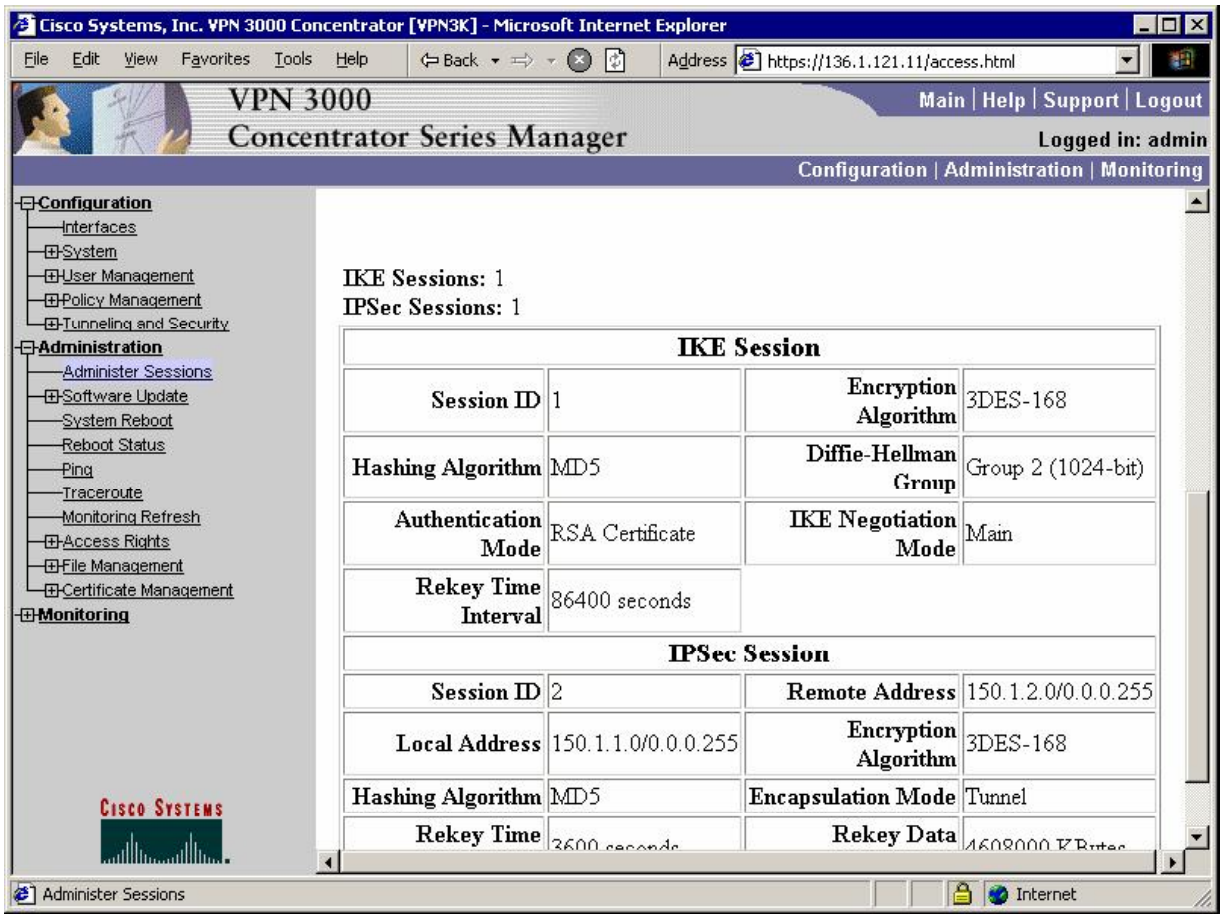
Modify L2L tunnel settings:



Verification

```
R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 8/9/12 ms

R2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.122.2     136.1.121.11             3des md5  rsig 2  23:59:18
```

Check Authentication mode for IPsec session on VPN3k:

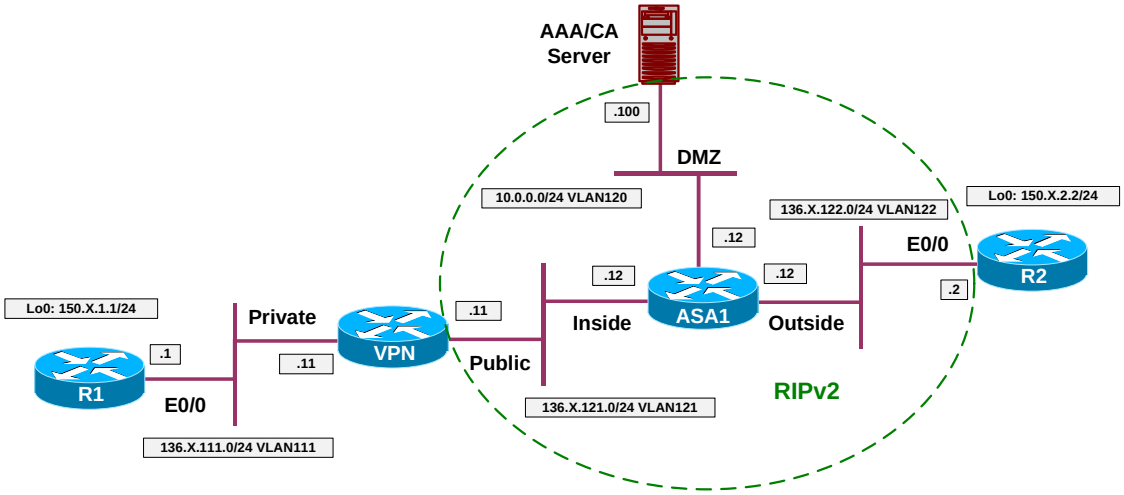


🕮 Further Reading

[VPN3k: Certificate Management]

IOS and VPN3k with PSK: Tuning IPsec Parameters

Objective: Fine-Tune IPsec parameters for L2L tunnel between IOS and VPN3k.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and VPN3k with PSK".
- Re-Configure IPsec L2L on R2 as follows:
  - Re-Configure ISAKMP policy to use DH Group 1 for authentication.
  - Create IPsec transform-set 3DES_SHA on R2 as follows:
    - Use 3DES cipher.
    - Use SHA hash.
  - Re-configure crypto-map VPN as follows:
    - Use transform-set 3DES_SHA.
    - Use PFS DH Group 2.
- Re-Configure IPsec L2L on VPN3k as follows:
  - Create new IKE Proposal named "IKE_3DES_MD5_DH1" as follows:
    - Use DH Group 1.
    - Use 3DES as cipher.
    - Use MD5 as hash.
  - Modify L2L tunnel to use new IKE Proposal.

- Modify exististing IPsec SA for the L2L Tunnel:
  - Use SHA hash
  - Use PFS Group 2

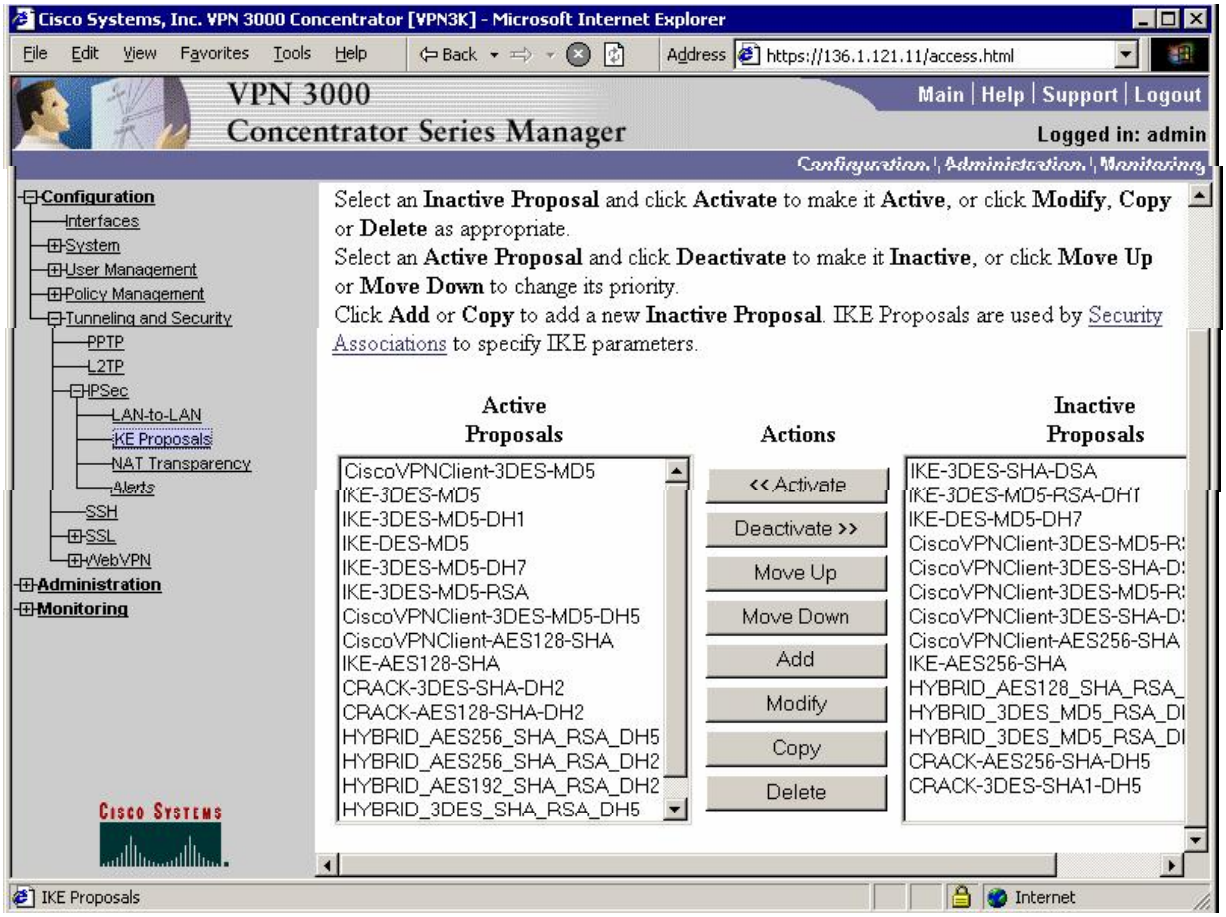
Final Configuration

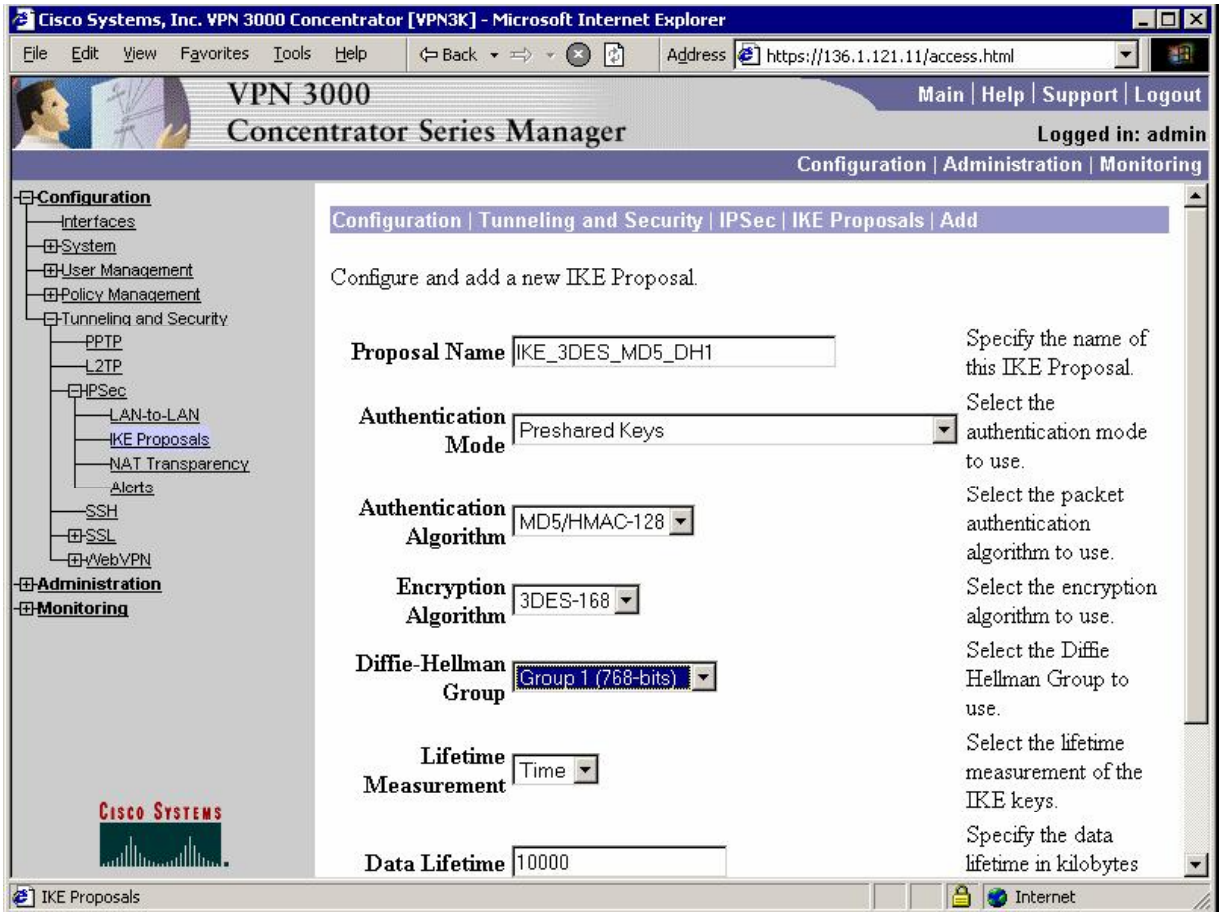
R2:

```
crypto isakmp policy 10
 group 1
!
crypto ipsec transform-set 3DES_SHA esp-3des esp-sha-hmac
!
crypto map VPN 10
 set transform-set 3DES_SHA
 set pfs group2
```

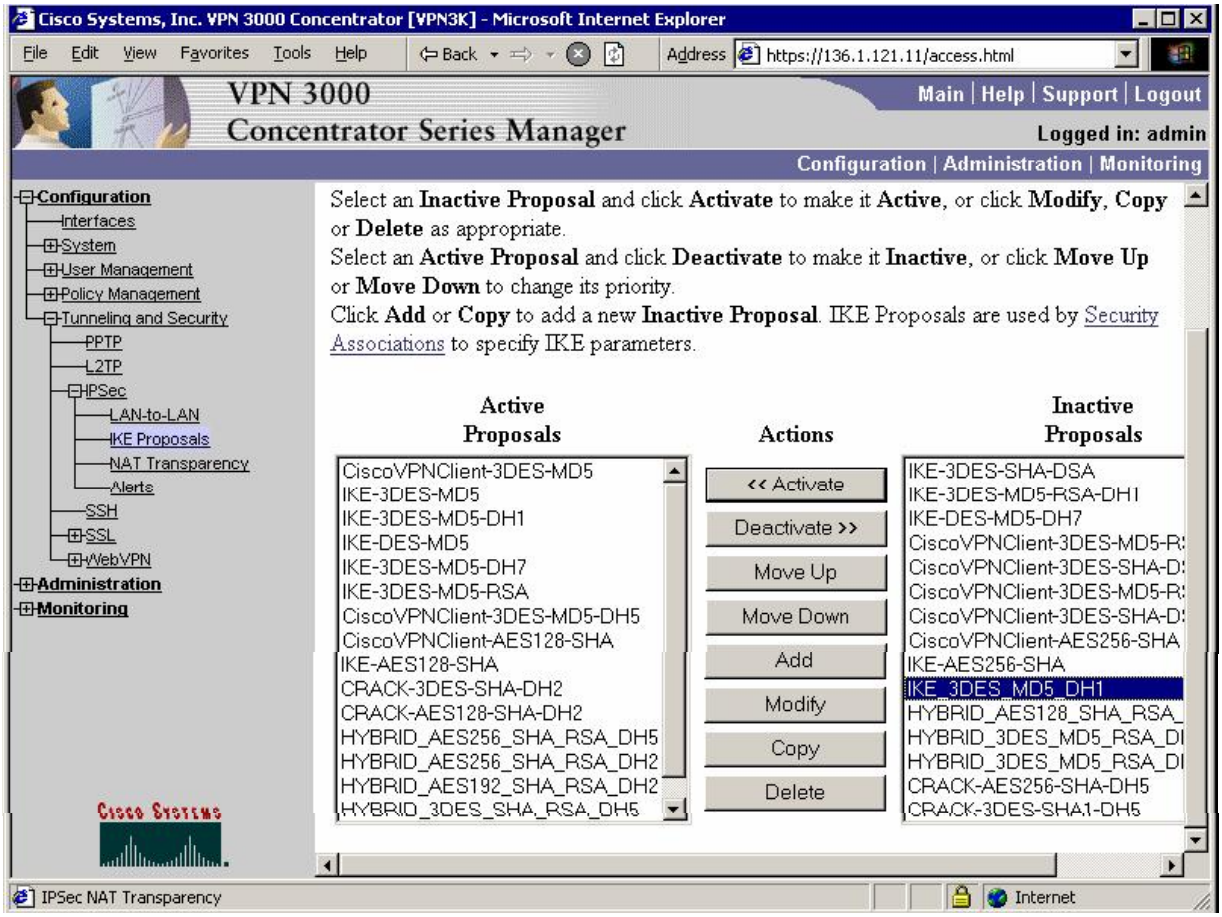
VPN3k:

Add new IKE proposal:

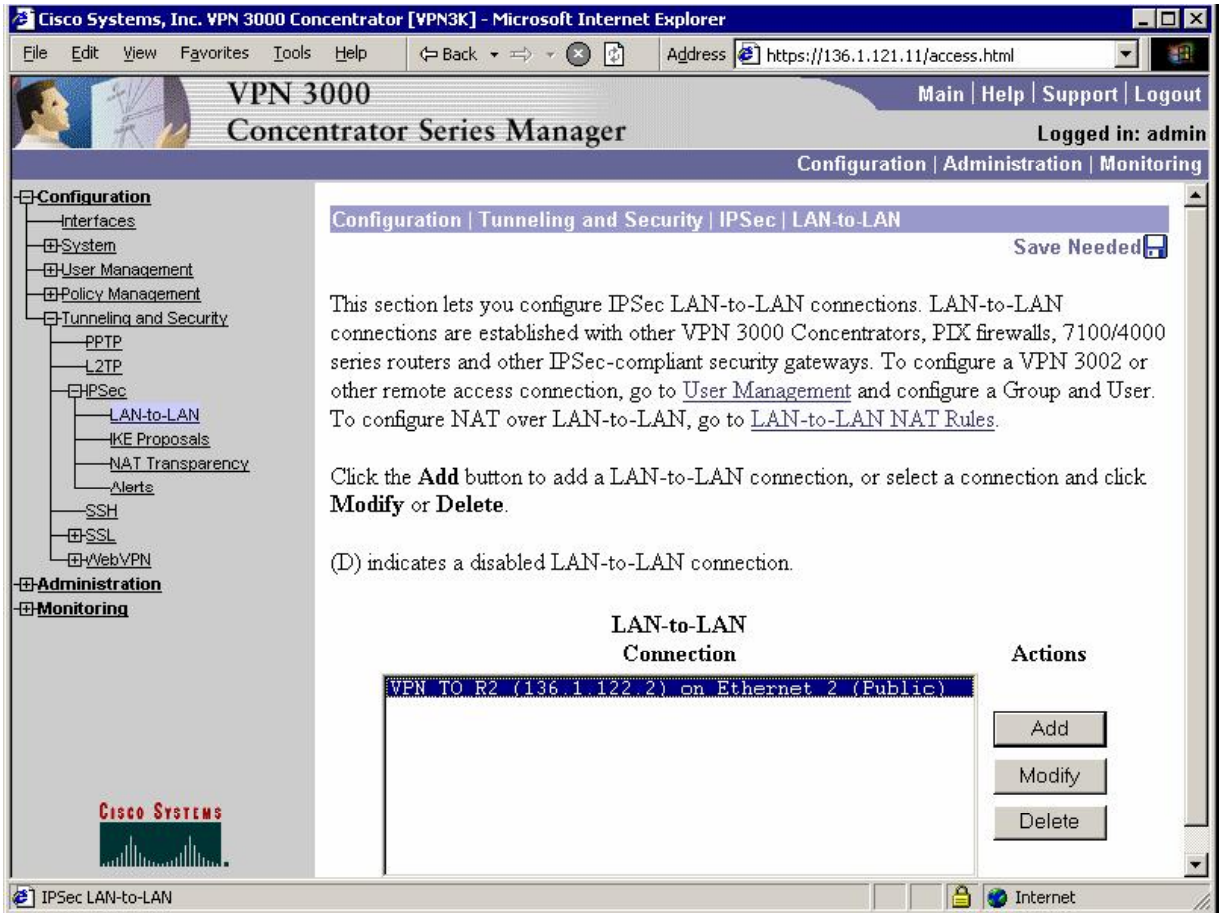


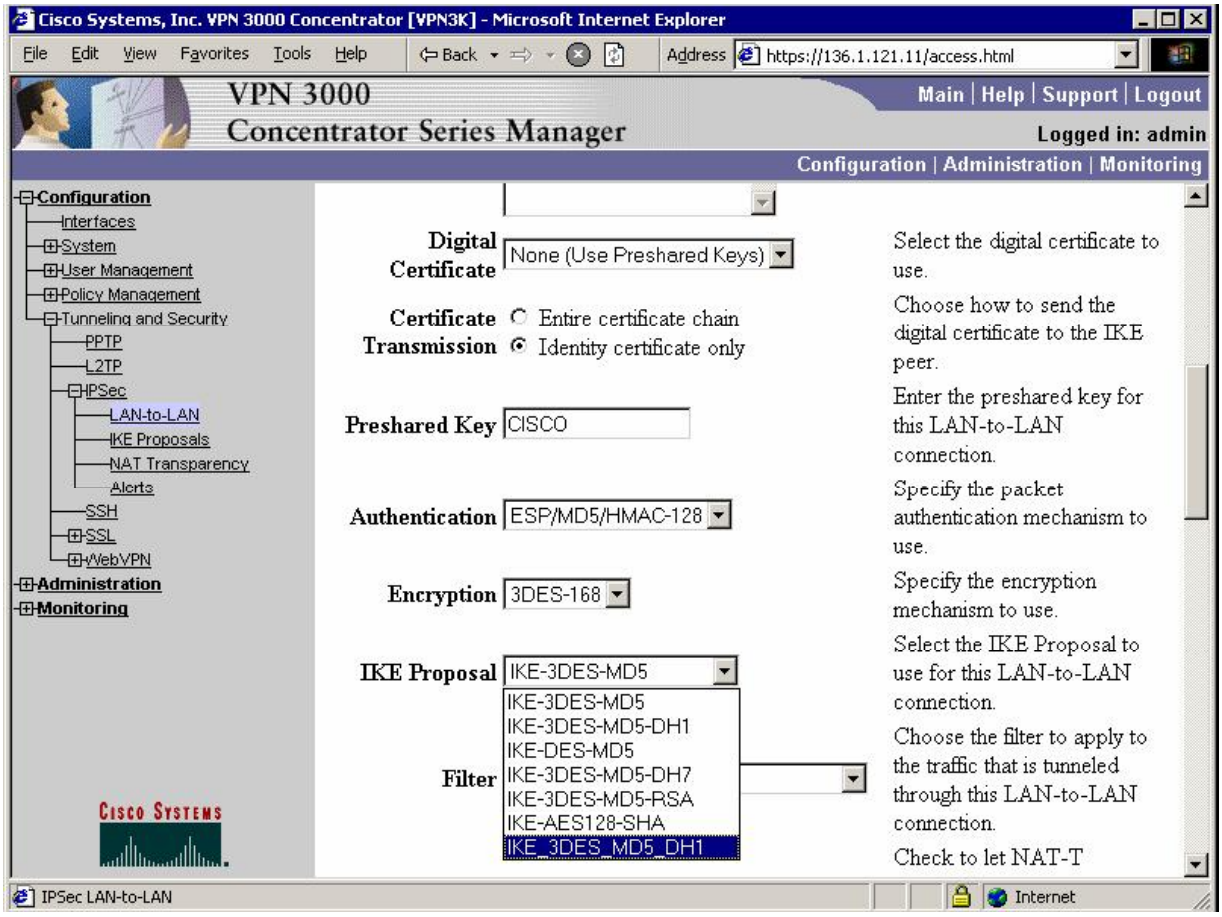

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Tunneling and Security
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
NAT Transparency
Alerts
SSH
SSL
WebVPN
Administration
Monitoring
Configuration | Tunneling and Security | IPSec | IKE Proposals | Add
Configure and add a new IKE Proposal.
Proposal Name
IKE_3DES_MD5_DH1
Specify the name of this IKE Proposal.
Authentication Mode
Preshared Keys
Select the authentication mode to use.
Authentication Algorithm
MD5/HMAC-128
Select the packet authentication algorithm to use.
Encryption Algorithm
3DES-168
Select the encryption algorithm to use.
Diffie-Hellman Group
Group 1 (768-bits)
Select the Diffie Hellman Group to use.
Lifetime Measurement
Time
Select the lifetime measurement of the IKE keys.
Data Lifetime
10000
Specify the data lifetime in kilobytes
Cisco Systems
IKE Proposals
Internet

Activate this proposal:

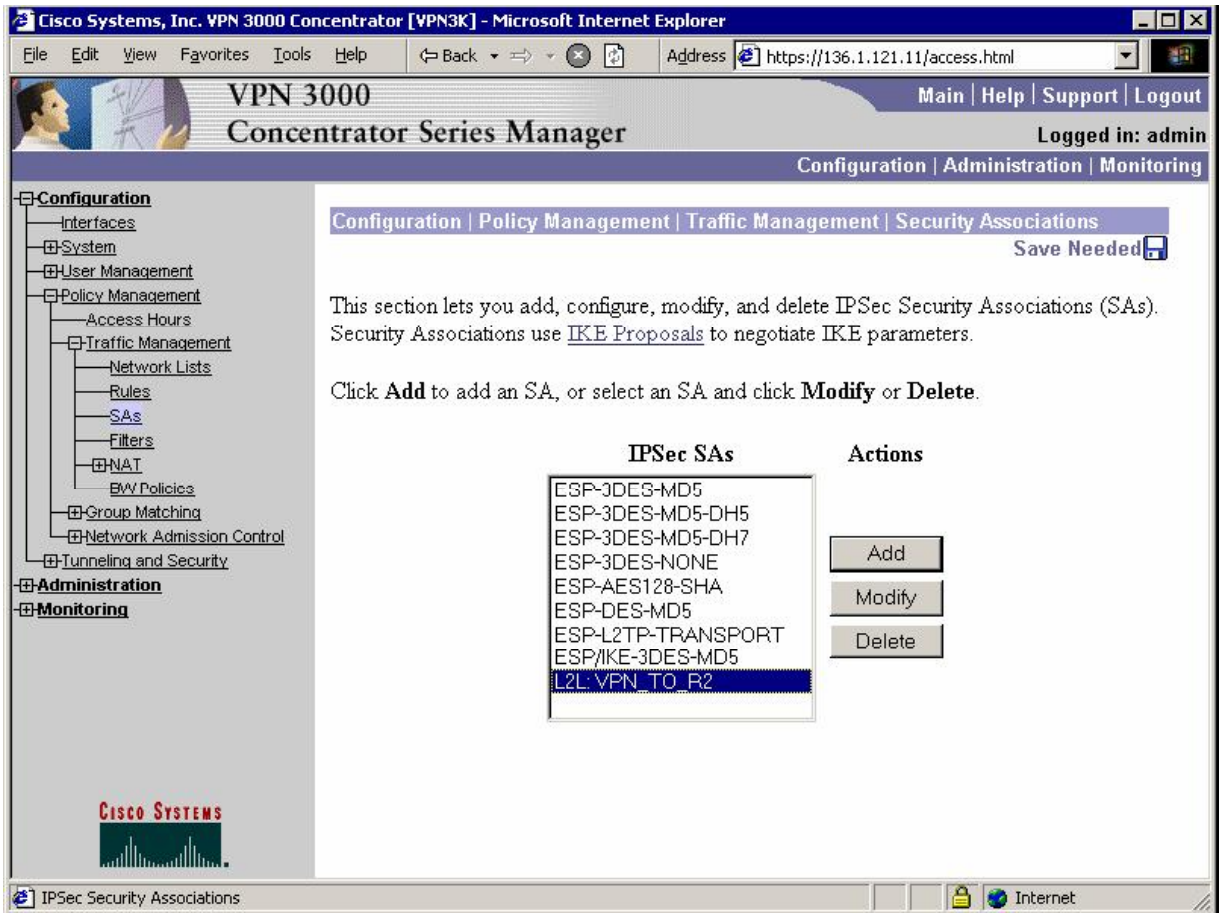


Modify L2L tunnel settings:

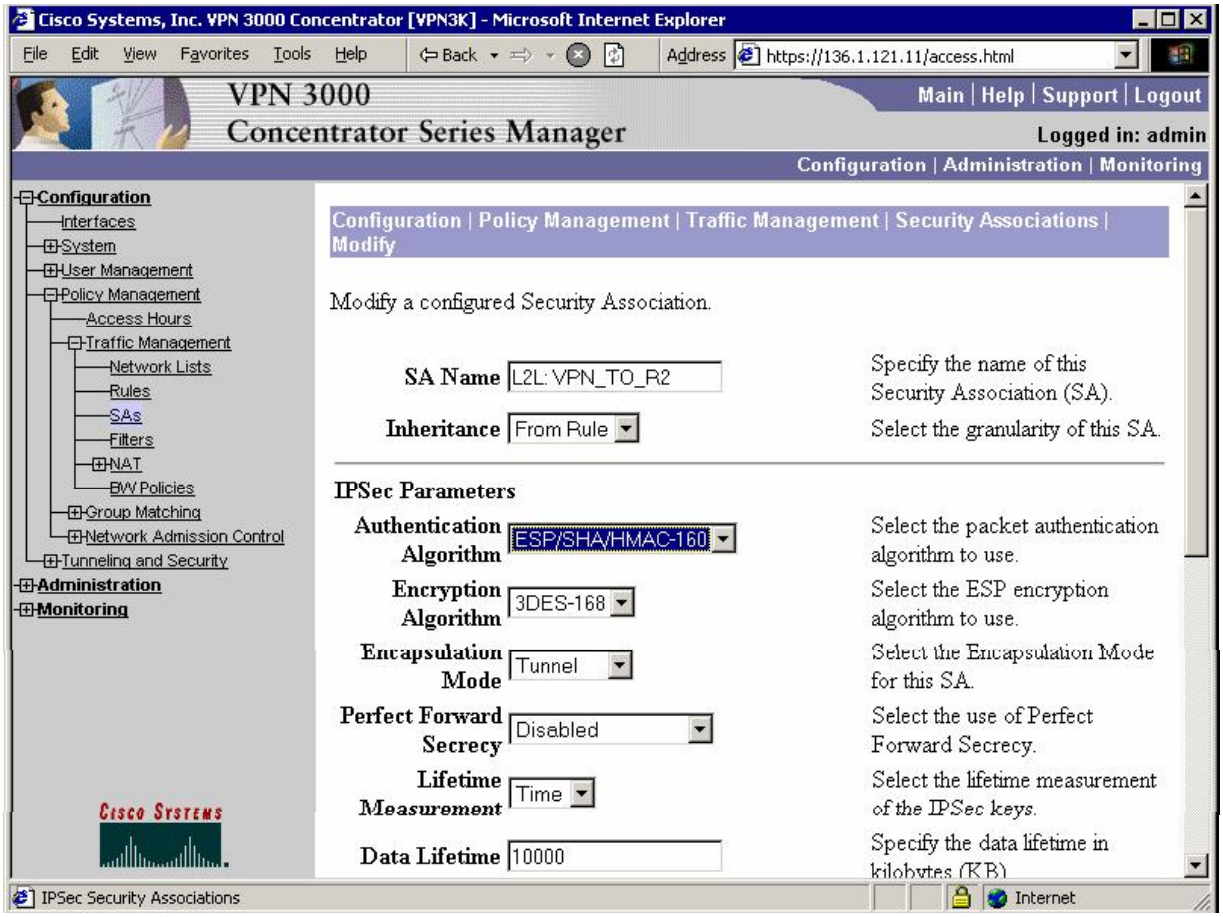



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Tunneling and Security
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
NAT Transparency
Alerts
SSH
SSL
WebVPN
Administration
Monitoring
Digital Certificate
None (Use Preshared Keys)
Select the digital certificate to use.
Certificate Transmission
Entire certificate chain
Identity certificate only
Choose how to send the digital certificate to the IKE peer.
Preshared Key
CISCO
Enter the preshared key for this LAN-to-LAN connection.
Authentication
ESP/MD5/HMAC-128
Specify the packet authentication mechanism to use.
Encryption
3DES-168
Specify the encryption mechanism to use.
IKE Proposal
IKE-3DES-MD5
IKE-3DES-MD5
IKE-3DES-MD5-DH1
IKE-DES-MD5
IKE-3DES-MD5-DH7
IKE-3DES-MD5-RSA
IKE-AES128-SHA
IKE_3DES_MD5_DH1
Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter
Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
Check to let NAT-T
Cisco Systems
IPSec LAN-to-LAN
Internet

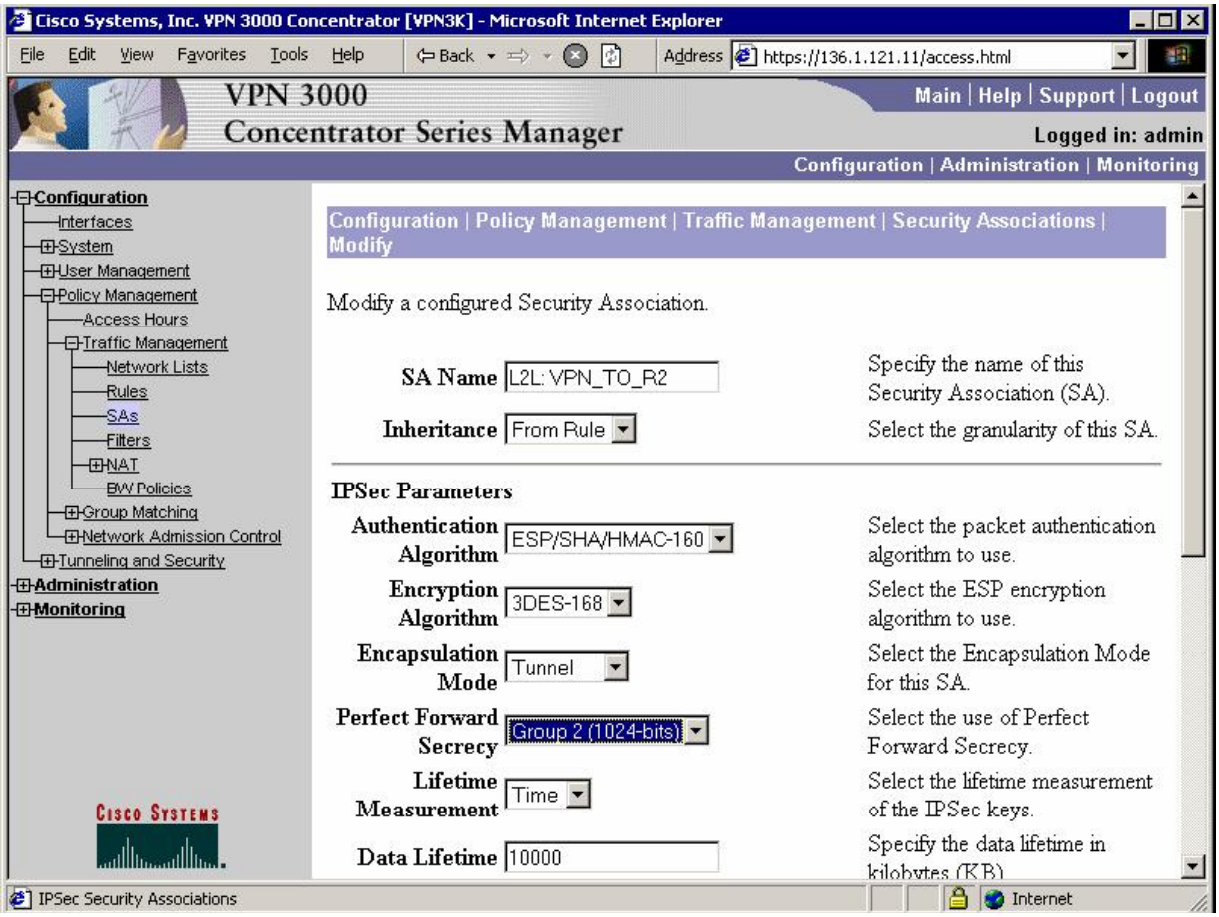
Modify L2L tunnel's IPsec SA:



Change authentication:



Change PFS group:



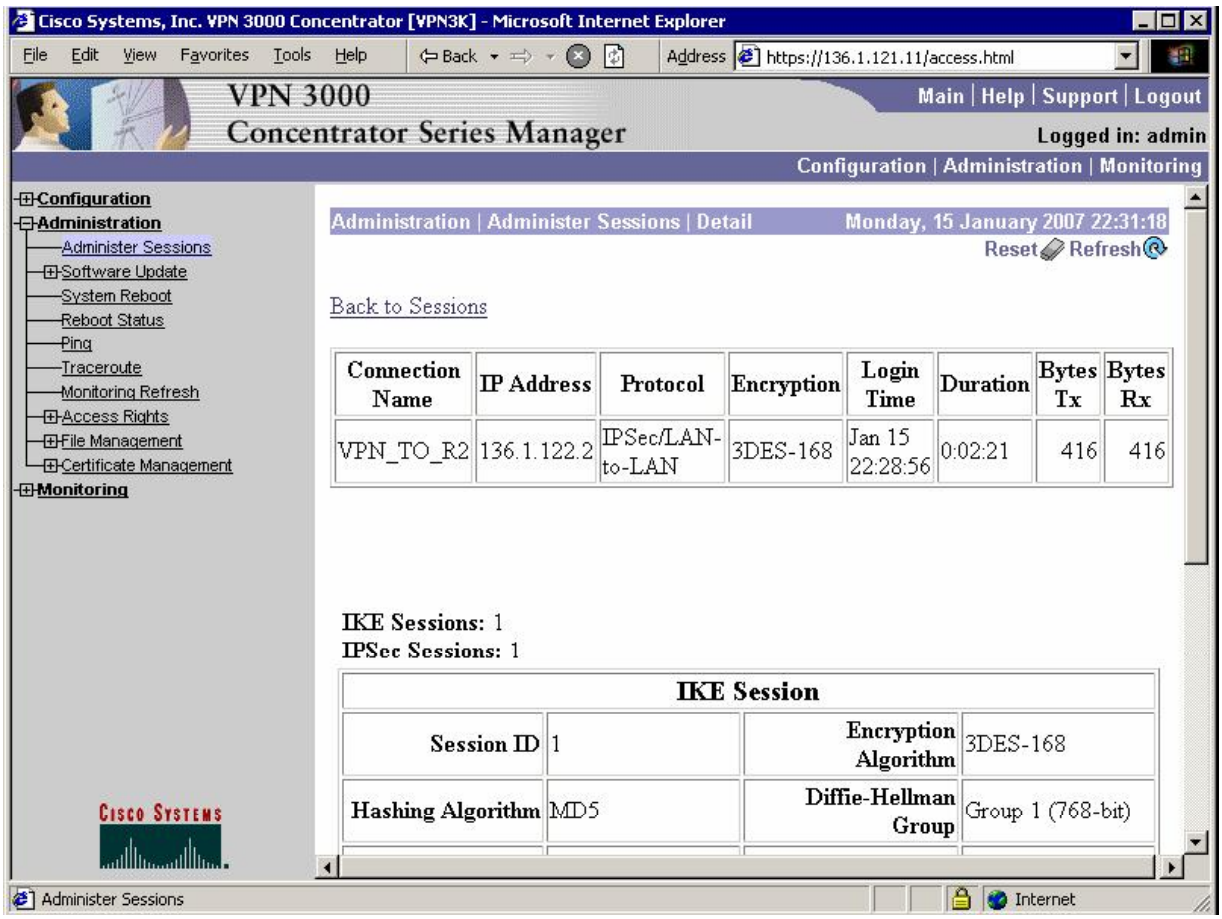
Verification

```
R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/9/12 ms

R2#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.122.2     136.1.121.11             3des md5  psk  1  23:59:24

R2#show crypto ipsec sa

interface: Ethernet0/0
```

```
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.11:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 6, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.11
     path mtu 1500, media mtu 1500
     current outbound spi: 4BBCC626

     inbound esp sas:
      spi: 0x5553683(89470595)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4401657/3547)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4BBCC626(1270662694)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4401657/3547)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

VPN3k:

Administration > Administer Sessions > VPN_TO_R2:

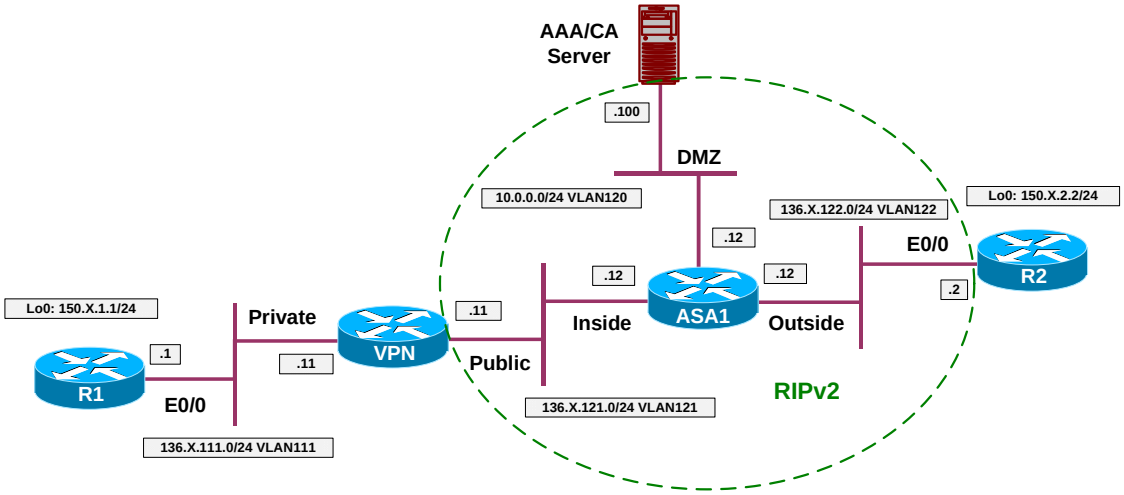


Further Reading

[VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7]

IOS and VPN3k: Filtering Tunneled Traffic

Objective: Configure VPN3k to filter tunneled traffic.



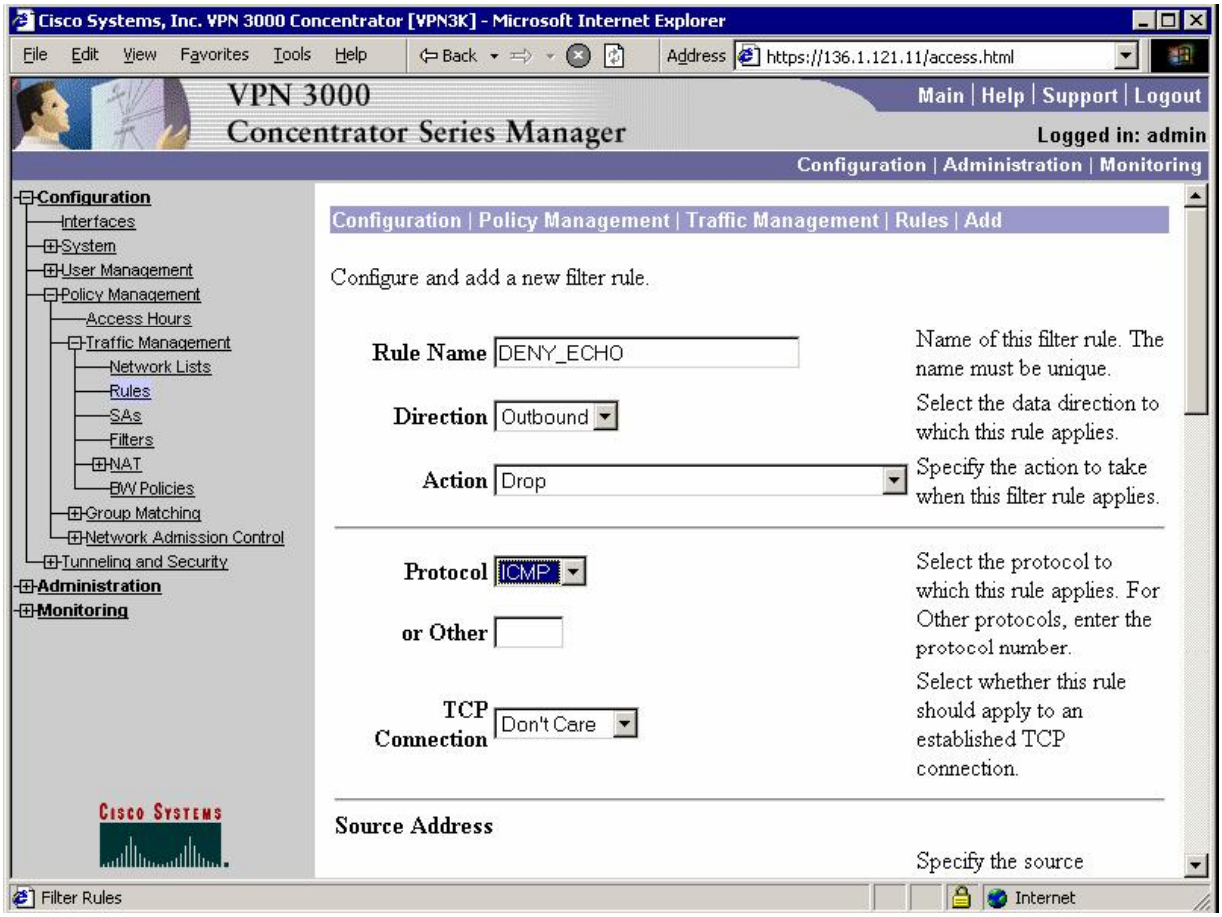
Directions

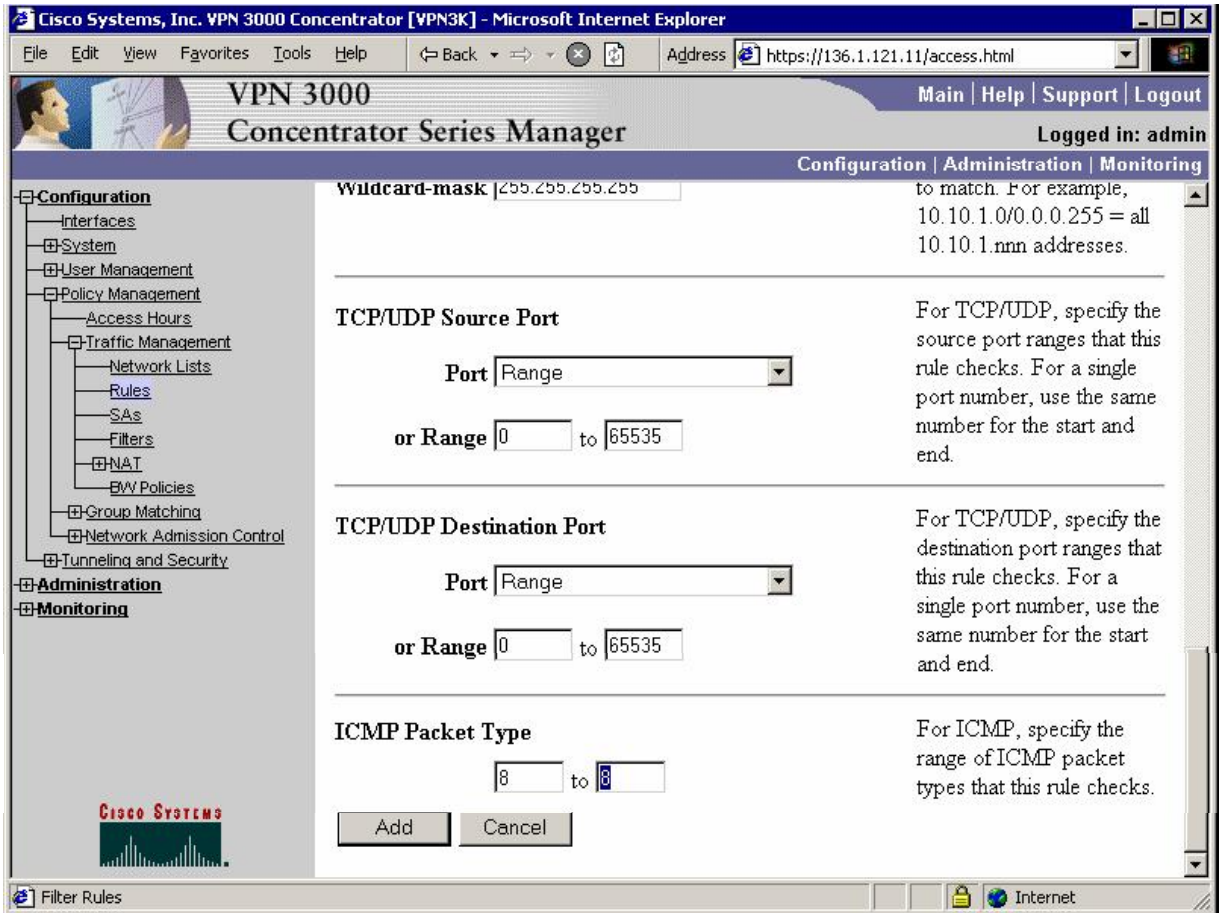
- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and VPN3k with PSK".
- The goal is to deny ICMP echo and echo-replay message to flow in the tunnel.
- Configure VPN3k as follows:
    - Create Fitler Rule DENY_ECHO to deny ICMP Echo Outbound.
    - Create Filter Rule DENY_ECHO_REPLY to deny ICMP Echo-Reply Inbound.
    - Create Filter VPN_TO_R2_FILTER as follows:
        - Permit traffic by default with this filter.
        - Assign rules "DENY_ECHO" and "DENY_ECHO_REPLY" to this filter.
    - Assign Filter VPN_TO_R2_FILTER to L2L Tunnel VPN_TO_R2.

Final Configuration

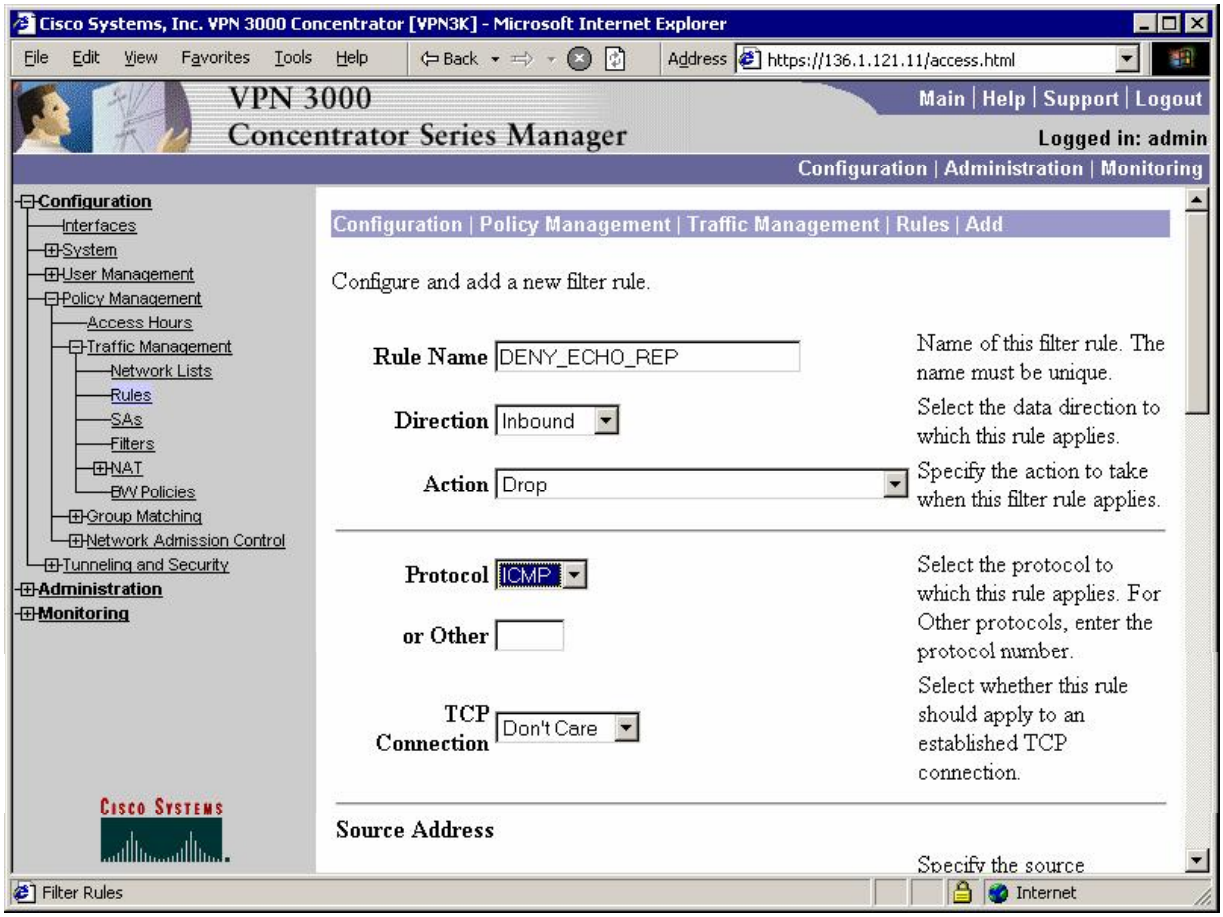
VPN3k:

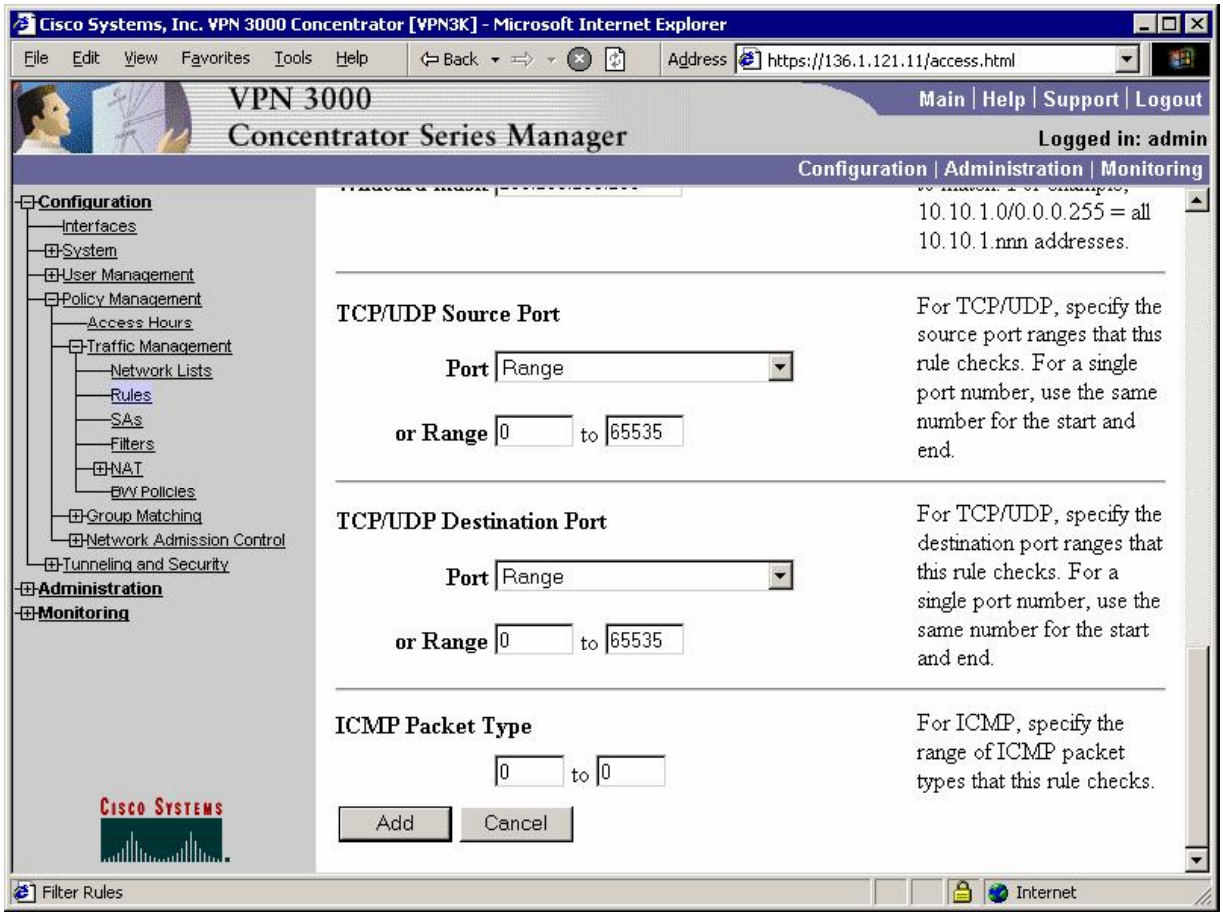
Create "DENY_ECHO" Rule:



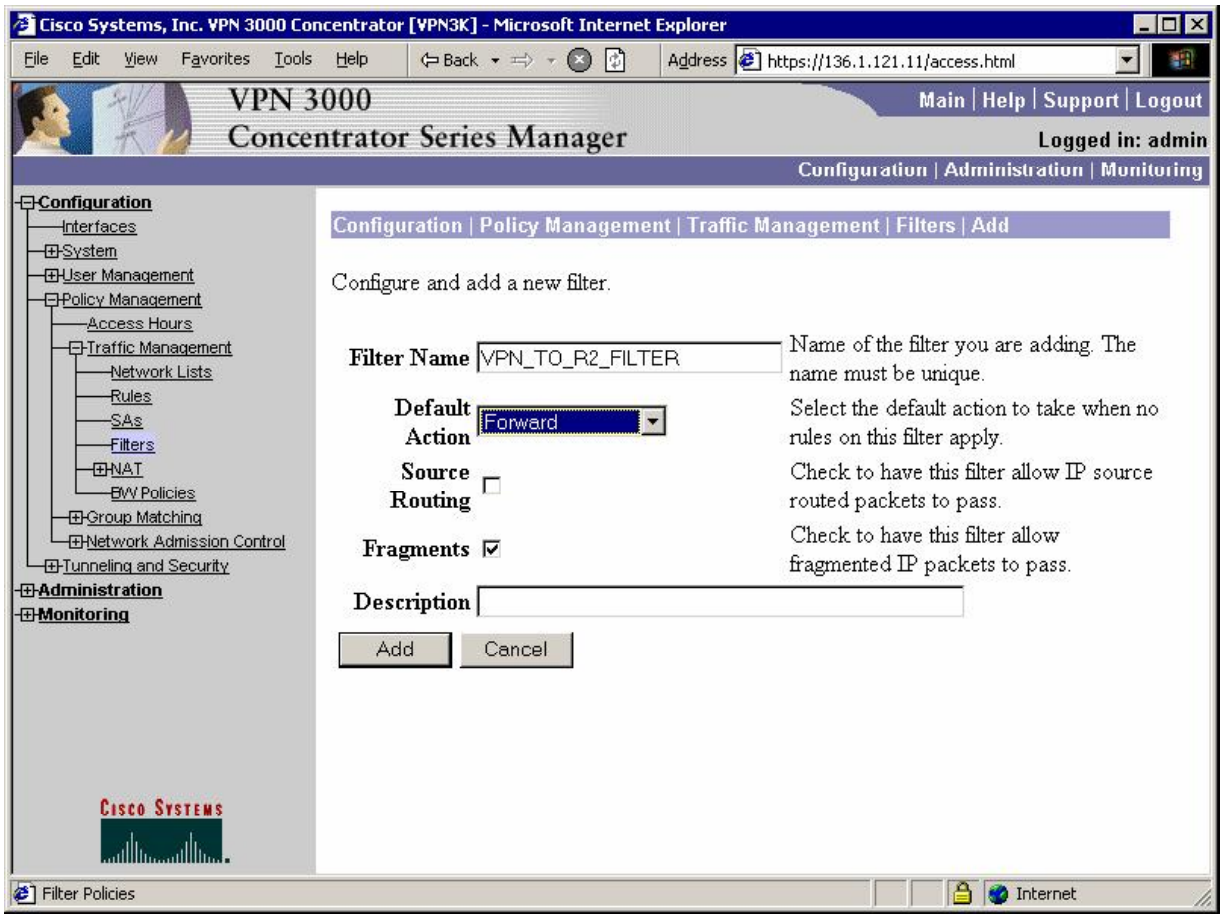

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Wildcard-mask 255.255.255.255
to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
TCP/UDP Source Port
Port Range
or Range 0 to 65535
For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.
TCP/UDP Destination Port
Port Range
or Range 0 to 65535
For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.
ICMP Packet Type
8 to 8
For ICMP, specify the range of ICMP packet types that this rule checks.
Add
Cancel
Cisco Systems
Filter Rules
Internet

Create "DENY_ECHO_REP" rule:



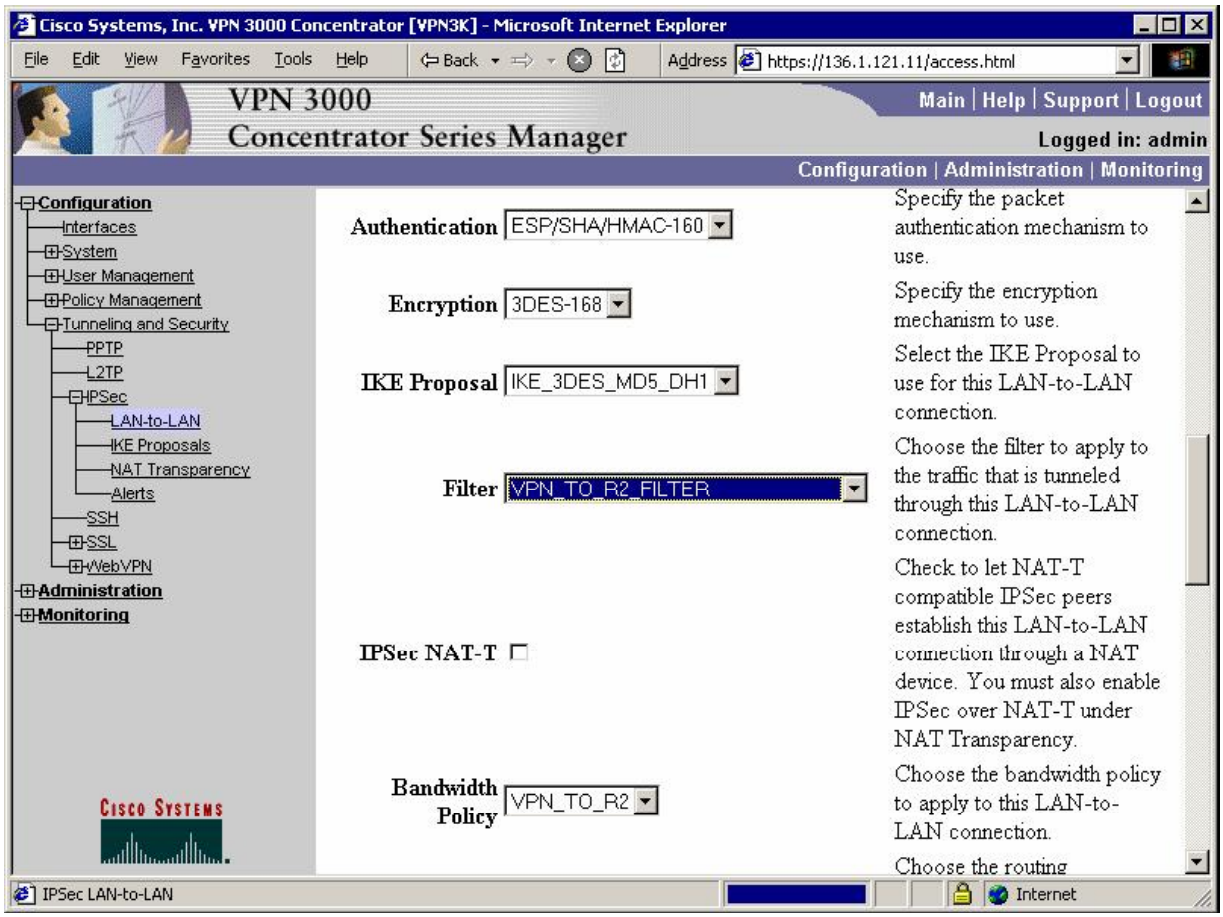

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
TCP/UDP Source Port
Port Range
or Range 0 to 65535
For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.
TCP/UDP Destination Port
Port Range
or Range 0 to 65535
For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.
ICMP Packet Type
0 to 0
For ICMP, specify the range of ICMP packet types that this rule checks.
Add
Cancel
Cisco Systems
Filter Rules
Internet

Add new traffic filter named "VPN_TO_R2_FILTER":



Assign previously created rules to filter:

Assign filter to L2L tunnel:



Verification

```
R1#telnet 150.1.2.2 /source-interface loopback 0
Trying 150.1.2.2 ... Open


Password required, but none set

[Connection to 150.1.2.2 closed by foreign host]

R1#ping 150.1.2.2 so lo 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
.....
Success rate is 0 percent (0/5)
```

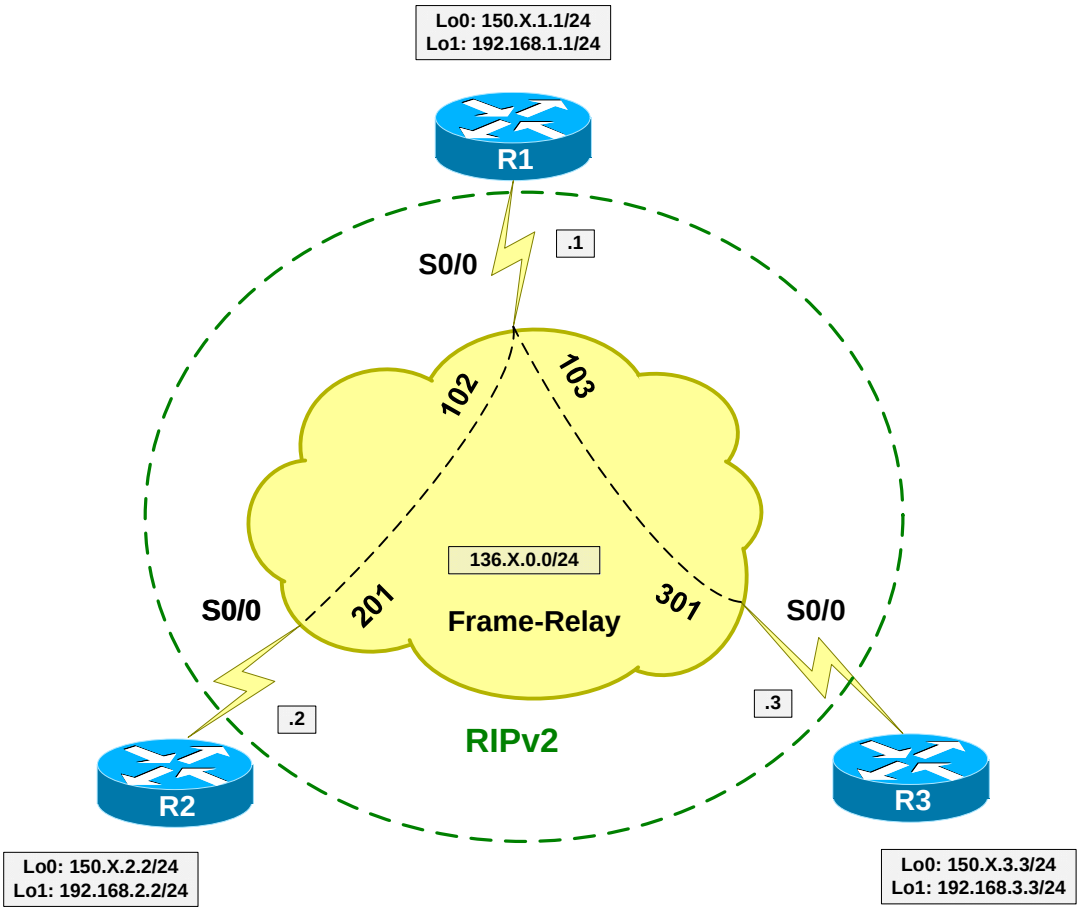
🕮 Further Reading

VPN3k: Policy Management

GRE and DMVPN

GRE Tunnels over IPsec with Static Crypto Maps

Objective: Configure GRE tunnels and encrypt them using static crypto maps.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "DMVPN".
- Configure GRE tunnels between R2 and R1 , R1 and R3 as follows:
    - Use Loopback0 interface as tunnel sources.
    - Use IP addresses from subnet 12.12.12.0/24 for R1/R2.
    - Use IP addresses from subnet 13.13.13.0/24 for R1/R3.
- Configure R1 for encryption of Tunnel0 as follows:

- Create ISAKMP policy with priority 10 as follows:
    - Use 3DES/MD5 as cipher/hash.
    - Use pre-shared keys authentication.
- Create ISAKMP key CISCO for host 136.1.0.2
- Create IPsec transform-set 3DES_MD5_TRANS as follows:
    - Use 3DES cipher.
    - Use MD5 hash.
    - Use transport mode for minimum overhead.
- Create access-list R1_TO_R2 as follows:
    - Match GRE traffic from 150.1.1.1 to 150.1.2.2
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
    - Match address R1_TO_R2.
    - Set transform-set 3DES_MD5_TRANS.
    - Set peer 136.X.0.2.

- Configure encryption of Tunnel1 (R1-R3) on R1 the same way:
    - Create ISAKMP key CISCO for address 136.X.0.3
    - Create crypto-map VPN entry 20 of type IPsec-ISAKMP:
        - Match address R1_TO_R2.
        - Set transform-set 3DES_MD5_TRANS
        - Set peer 136.X.0.2
- Apply crypto-map VPN to interface Serial 0/0.
- Configure R2 and R3 to mirror R1's configuration.
- Configure VPN routing as follows:
    - Enable EIGRP process 100 on R1, R2, R3:
        - Include networks 12.12.12.0/24 and 13.13.13.0/24 into EIGRP
        - Include Loopback1 interfaces into EIGRP

Final Configuration

Tunnels & IPsec:

R1:

```
!
! Tunnel to R2
!
interface Tunnel0
 tunnel source Loopback0
 tunnel destination 150.1.2.2
 ip address 12.12.12.1 255.255.255.0
!
! Tunnel to R3
!
interface Tunnel1
tunnel source Loopback0
 tunnel destination 150.1.3.3
 ip address 13.13.13.1 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
! Pre-shared keys
!
crypto isakmp key CISCO address 136.1.0.2
crypto isakmp key CISCO address 136.1.0.3
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
! Access-list to match tunnels' traffic
!
ip access-list extended R1_TO_R2
 permit gre host 150.1.1.1 host 150.1.2.2
!
ip access-list extended R1_TO_R3
 permit gre host 150.1.1.1 host 150.1.3.3
!
! Crypto map to encrypto traffic to R2
!
crypto map VPN 10 ipsec-isakmp
 set peer 136.1.0.2
 set transform-set 3DES_MD5_TRANS
 match address R1_TO_R2
!
! Crypto map to encrypto traffic to R3
!
crypto map VPN 20 ipsec-isakmp
 set peer 136.1.0.3
 set transform-set 3DES_MD5_TRANS
 match address R1_TO_R3

interface Se 0/0
 crypto map VPN
```

R2:

```
!
! Tunnel to R1
```

```
!
interface Tunnel0
 tunnel source Loopback0
 tunnel destination 150.1.1.1
 ip address 12.12.12.2 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
! Pre-shared key
!
crypto isakmp key CISCO address 150.1.1.1
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
ip access-list extended R2_TO_R1
 permit gre host 150.1.2.2 host 150.1.1.1
!
! Crypto map to encrypto traffic to R1
!
crypto map VPN 10 ipsec-isakmp
 set peer 136.1.0.1
 set transform-set 3DES_MD5_TRANS
 match address R2_TO_R1
!
interface Serial0/0
 crypto map VPN
```

R3:

```
!
! Tunnel to R1
!
interface Tunnel0
 tunnel source Loopback0
 tunnel destination 150.1.1.1
 ip address 13.13.13.3 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
! Pre-shared key
!
crypto isakmp key CISCO address 150.1.1.1
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
! Access-list to match tunnel traffic
!
ip access-list extended R3_TO_R1
```

```
 permit gre host 150.1.3.3 host 150.1.1.1
!
! Crypto map to encrypt traffic to R1
!
crypto map VPN 10 ipsec-isakmp
 set peer 136.1.0.1
 set transform-set 3DES_MD5_TRANS
 match address R3_TO_R1
!
interface Serial 1/0
 crypto map VPN
```

VPN Routing:

R1:

```
router eigrp 100
 no auto-summary
 network 12.12.12.0 0.0.0.255
 network 13.13.13.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
```

R2:

```
router eigrp 100
 no auto-summary
 network 12.12.12.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
```

R3:

```
router eigrp 100
 no auto-summary
 network 13.13.13.0 0.0.0.255
 network 192.168.3.0 0.0.0.255
```

Verification

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
Type
                                            (sec)         (ms)       Cnt Num
1   12.12.12.2              Tu0               10 00:12:17   92  5000  0  13
0   13.13.13.3              Tu1               11 00:16:21  113  5000  0  11

R1#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.0.2       136.1.0.1       QM_IDLE             45    0
136.1.0.3       136.1.0.1       QM_IDLE             44    0

R3#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/76/80 ms

R1#show crypto ipsec sa

interface: Serial0/0
    Crypto map tag: VPN, local addr. 136.1.0.1
```

```
protected vrf:
local  ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (150.1.2.2/255.255.255.255/47/0)
current_peer: 136.1.0.2:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 121, #pkts encrypt: 121, #pkts digest 121
 #pkts decaps: 120, #pkts decrypt: 120, #pkts verify 120
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 1, #recv errors 0

  local crypto endpt.: 136.1.0.1, remote crypto endpt.: 136.1.0.2
  path mtu 1500, media mtu 1500
  current outbound spi: 15AF12C4

  inbound esp sas:
   spi: 0x2A1EEF14(706670356)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2002, flow_id: 3, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4382403/3058)
     IV size: 8 bytes
     replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x15AF12C4(363795140)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2003, flow_id: 4, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4382403/3058)
     IV size: 8 bytes
     replay detection support: Y

  outbound ah sas:

  outbound pcp sas:

protected vrf:
local  ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (150.1.3.3/255.255.255.255/47/0)
current_peer: 136.1.0.3:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 118, #pkts encrypt: 118, #pkts digest 118
 #pkts decaps: 117, #pkts decrypt: 117, #pkts verify 117
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 1, #recv errors 0

  local crypto endpt.: 136.1.0.1, remote crypto endpt.: 136.1.0.3
  path mtu 1500, media mtu 1500
  current outbound spi: C50B2425

  inbound esp sas:
   spi: 0x6DB01774(1840256884)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
```

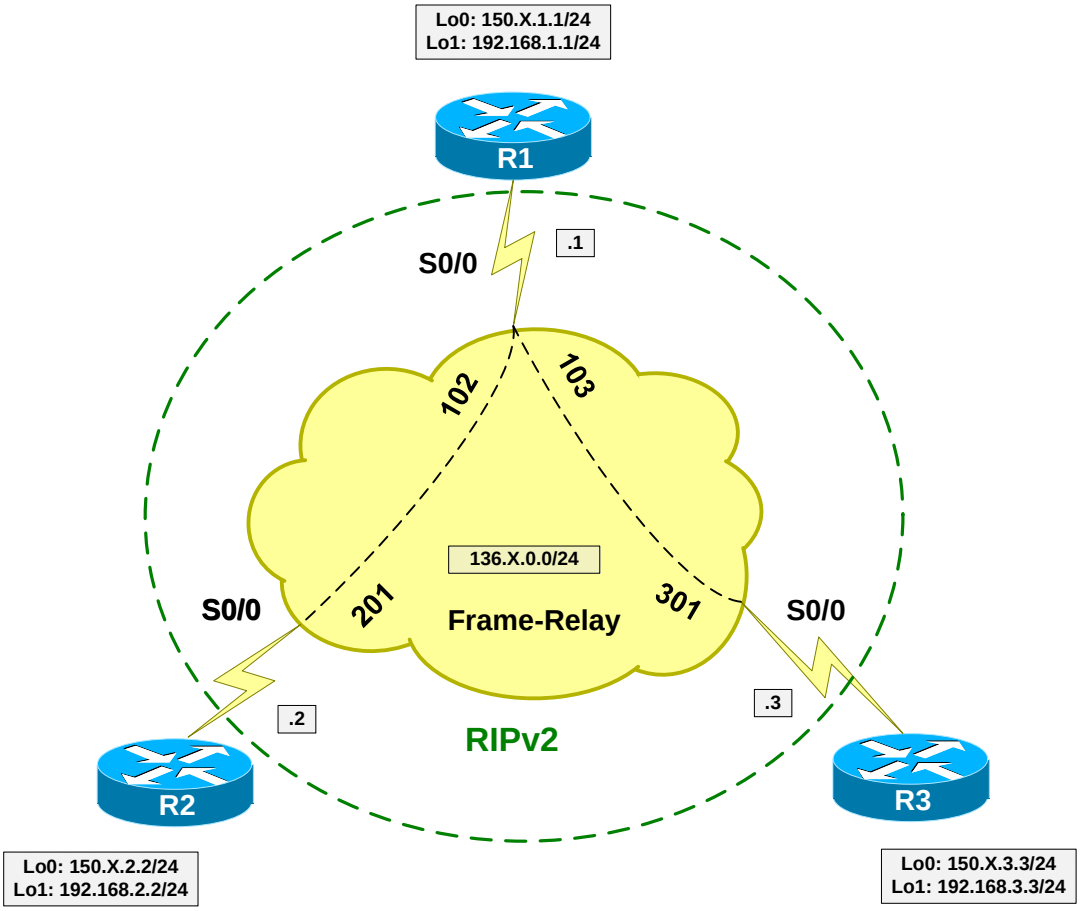
```
        sa timing: remaining key lifetime (k/sec): (4399740/3055)
        IV size: 8 bytes
        replay detection support: Y

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xC50B2425(3305841701)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4399740/3052)
        IV size: 8 bytes
        replay detection support: Y

    outbound ah sas:

    outbound pcp sas:
```

🕮 Further Reading

GRE over IPSec with EIGRP to Route Through a Hub and Multiple Remote Sites

GRE Tunnels over IPsec with Crypto Profiles

Objective: Configure GRE tunnels and encrypt them using crypto profiles.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "DMVPN".
- Configure GRE tunnels between R2 and R1 , R1 and R3 as follows:
    - Use Loopback0 interface as tunnel sources.
    - Use IP addresses from subnet 12.12.12.0/24 for R1/R2.
    - Use IP addresses from subnet 13.13.13.0/24 for R1/R3.
- The difference with profiles is that IPsec is initiated from Loopbacks, hence you need to configure ISAKMP keys for Loopback addresses.
- Configure R1 for encryption of Tunnel0 as follows:

- Create ISAKMP policy with priority 10 as follows:
    - Use 3DES/MD5 as cipher/hash.
    - Use pre-shared keys authentication.
- Create ISAKMP key CISCO for host 150.X.2.2.
- Create IPsec transform-set 3DES_MD5_TRANS as follows:
    - Use 3DES cipher.
    - Use MD5 hash.
    - Use transport mode for minimum overhead.
- Create crypto profile VPN as follows:
    - Apply transform set 3DES_MD5_TRANS.
- Apply crypto profile VPN to Tunnel0.

- Configure encryption of Tunnel1 (R1-R3) on R1 the same way:
    - Create ISAKMP key CISCO for host 150.X.2.2.
    - Apply crypto profile VPN to Tunnel1.
- Configure R2 and R3 to mirror R1's configuration.
- Configure VPN routing as follows:
    - Enable EIGRP process 100 on R1, R2, R3:
        - Include networks 12.12.12.0/24 and 13.13.13.0/24 into EIGRP.
        - Include Loopback1 interfaces into EIGRP.

Final Configuration

Tunnels & IPsec:

R1:

```
!
! Tunnel to R2
!
interface Tunnel0
 tunnel source Loopback0
 tunnel destination 150.1.2.2
 ip address 12.12.12.1 255.255.255.0
!
! Tunnel to R3
!
interface Tunnel1
tunnel source Loopback0
```

```
 tunnel destination 150.1.3.3
 ip address 13.13.13.1 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
! Pre-shared keys
!
crypto isakmp key CISCO address 150.1.3.3
crypto isakmp key CISCO address 150.1.2.2
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
! Create IPsec profile
!
crypto ipsec profile VPN
  set transform-set 3DES_MD5_TRANS
!
! Apply crypto profile to tunnels
!
interface Tunnel0
 tunnel protection ipsec profile VPN
!
interface Tunnel1
 tunnel protection ipsec profile VPN
```

R2:

```
!
! Tunnel to R1
!
interface Tunnel0
 tunnel source Loopback0
 tunnel destination 150.1.1.1
 ip address 12.12.12.2 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
! Pre-shared key
!
crypto isakmp key CISCO address 150.1.1.1
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
! Create IPsec profile
!
crypto ipsec profile VPN
  set transform-set 3DES_MD5_TRANS
!
```



```
! Apply crypto profile to tunnels
!
interface Tunnel0
 tunnel protection ipsec profile VPN
```

R3:

```
!
! Tunnel to R1
!
interface Tunnel0
 tunnel source Loopback0
 tunnel destination 150.1.1.1
 ip address 13.13.13.3 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
! Pre-shared key
!
crypto isakmp key CISCO address 150.1.1.1
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
! Create IPsec profile
!
crypto ipsec profile VPN
  set transform-set 3DES_MD5_TRANS
!
! Apply crypto profile to tunnels
!
interface Tunnel0
 tunnel protection ipsec profile VPN
```

VPN Routing:

R1:

```
router eigrp 100
 no auto-summary
 network 12.12.12.0 0.0.0.255
 network 13.13.13.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
```

R2:

```
router eigrp 100
 no auto-summary
 network 12.12.12.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
```

R3:

```
router eigrp 100
 no auto-summary
 network 13.13.13.0 0.0.0.255
 network 192.168.3.0 0.0.0.255
```


Verification

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
Type
                                            (sec)         (ms)       Cnt Num
1   13.13.13.3              Tu1               12 00:01:34  261  5000  0  5
0   12.12.12.2              Tu0               13 00:01:47   73  5000  0  7

R1#show ip ro ei
D    192.168.2.0/24 [90/297372416] via 12.12.12.2, 00:01:52, Tunnel0
D    192.168.3.0/24 [90/297372416] via 13.13.13.3, 00:01:38, Tunnel1

R1#sho crypto isakmp sa
dst             src             state          conn-id slot
150.1.1.1       150.1.3.3       QM_IDLE              4    0
150.1.1.1       150.1.2.2       QM_IDLE              3    0

R3#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/69/72 ms

R1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr. 150.1.1.1

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (150.1.2.2/255.255.255.255/47/0)
   current_peer: 150.1.2.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 32, #pkts encrypt: 32, #pkts digest 32
    #pkts decaps: 33, #pkts decrypt: 33, #pkts verify 33
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 225, #recv errors 0

     local crypto endpt.: 150.1.1.1, remote crypto endpt.: 150.1.2.2
     path mtu 1500, media mtu 1500
     current outbound spi: 60AAA69E

     inbound esp sas:
      spi: 0xFD7661D(265774621)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4532966/3472)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

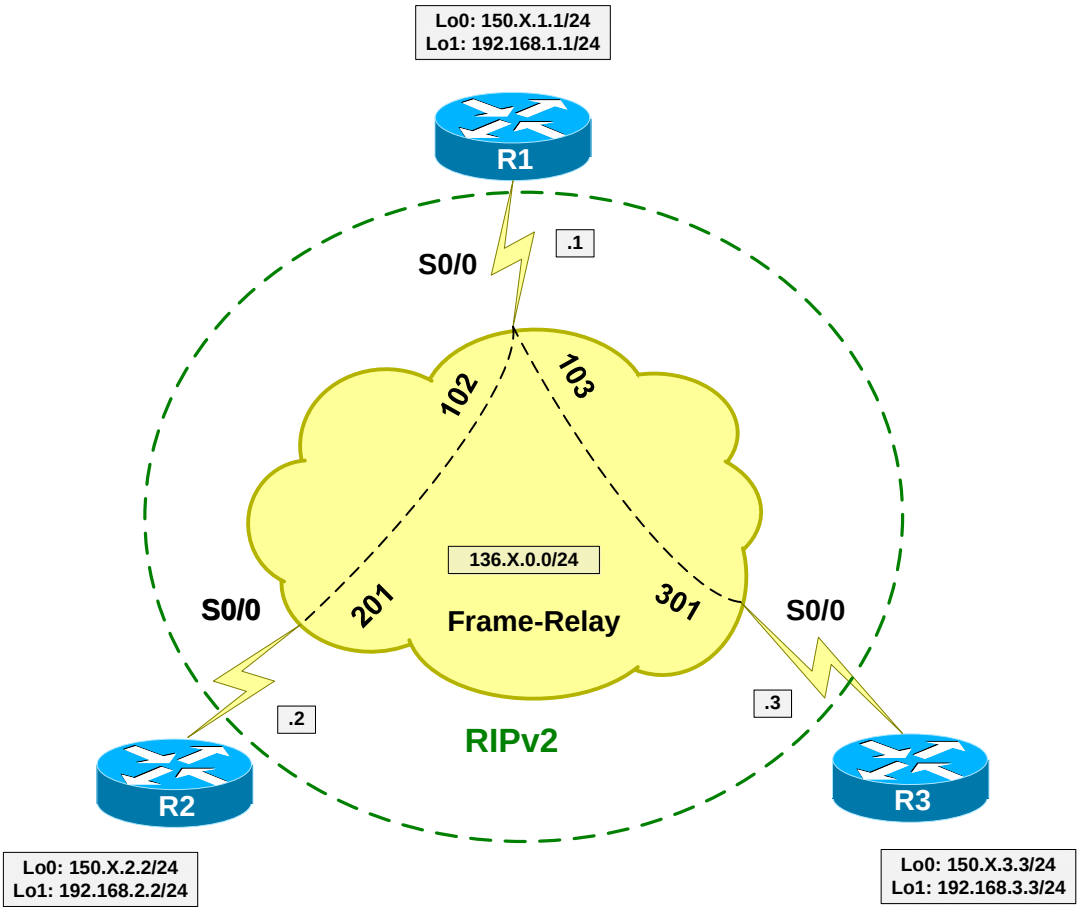
```
      spi: 0x60AAA69E(1621796510)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4532966/3472)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:


interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr. 150.1.1.1

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (150.1.3.3/255.255.255.255/47/0)
   current_peer: 150.1.3.3:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 31, #pkts encrypt: 31, #pkts digest 31
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify 30
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 225, #recv errors 0

     local crypto endpt.: 150.1.1.1, remote crypto endpt.: 150.1.3.3
     path mtu 1500, media mtu 1500
     current outbound spi: A1C5A428

     inbound esp sas:
      spi: 0xD0532A43(3495111235)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 2002, flow_id: 3, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4402696/3481)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA1C5A428(2714084392)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Transport, }
        slot: 0, conn id: 2003, flow_id: 4, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4402696/3481)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

🕮 Further Reading

GRE over IPSec with EIGRP to Route Through a Hub and Multiple Remote Sites

DMVPN with PSK

Objective: Configure Dynamic Multopoint VPN with EIGRP routing.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "DMVPN".
- The key idea behind DMVPN is to use NHRP for dynamic next-hop resolution, and establish direct spoke-to-spoke tunnels on demand, as opposed to "static" Hub-And-Spoke model.
- NHRP uses client-server model, where server (usually the hub router) responds to NHRP next-hop queries, providing spokes with "best" next-hop available.
- NHRP is used in combination with multipoint GRE encapsulation, thereby allowing a tunnel to be connected to multiple remote endpoints simultaneously.
- Multipoint GRE is combined with IPsec profiles to allow for dynamic IPsec session establishment. Altogether mGRE+NHRP+IPsec provides the three building blocks of DMVPN technology.

- Create Tunnel0 interfaces at R1, R2, R3 as follows:
    - Use multipoint GRE encapsulation.
    - Use tunnel source Loopback0.
    - Use tunnel key 123.
    - Use addresses 123.123.123.Y/24 where Y is router number.
    - Configure bandwidth of 1024Kbps (to override defaults).
    - Configure delay value of 100.
- Configure common NHRP settings on R1, R2, R3 as follows:
    - Use network-id 123.
    - Use authentication-key “CISCO”.
    - Use Hold-Time of 60 seconds.
- Configure IPsec at Hub & Spokes router as follows:
    - Create ISAKMP policy.
    - Configure wildcard pre-shared key “CISCO”.
    - Create IPsec transform-set 3DES_MD5_TRANS as follows:
        - Encryption 3DES.
        - Hash MD5.
        - Mode Transport.
    - Create IPsec Profile DMVPN as follows:
        - Apply transform-set 3DES_MD5_TRANS.
    - Apply IPsec Profile DMVPN to Tunnel0 interfaces.
- Configure NHRP specific settings for R1 (Hub) as follows:
    - Map multicast traffic to dynamic NHRP entries.
- Configure NHRP specific settings for R2, R3 (Spokes) as follows:
    - Map 123.123.123.1 to 150.X.1.1
    - Map multicast to 150.X.1.1.
    - Use 123.123.123.1 as NHS server.
- Configure EIGRP 100 for VPN routing on R1, R2, R3 as follows:
    - Include network 123.123.123.0/24.
    - Include networks 192.168.Y.0/24 on R2, and R3.
    - Disable EIGRP split horizon on interface Tunnel0 of R1.

Final Configuration

R1:

```
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
! Wildcard pre-shared key to authenticate any valid peer
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
!
! Transport mode transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5
  mode tunnel
!
! IPsec profile
!
crypto ipsec profile DMVPN
  set transform 3DES_MD5_TRANS
!
! DMVPN Hub
!
interface Tunnel0
 ip address 123.123.123.1 255.255.255.0
 tunnel source Loopback0
 tunnel mode gre multi
 tunnel key 123
 ip nhrp network-id 123
 ip nhrp authentication CISCO
 ip nhrp hold 30
 ip nhrp map multicast dynamic
 !
 ! Override default bw/delay for tunnel
 !
 bandwidth 1024
 delay 100
 !
 ! Apply IPsec
 !
 tunnel protection ipsec profile DMVPN
```

R2:

```
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5
  mode tunnel
!
crypto ipsec profile DMVPN
  set transform 3DES_MD5_TRANS
!
! DMVPN Spoke
!
interface Tunnel0
 ip address 123.123.123.2 255.255.255.0
```

```
 tunnel source Loopback0
 tunnel mode gre multi
 tunnel key 123
 ip nhrp network-id 123
 ip nhrp authentication CISCO
 ip nhrp hold 30
 ip nhrp map 123.123.123.1 150.1.1.1
 ip nhrp map multicast 150.1.1.1
 ip nhrp nhs 123.123.123.1
 !
 ! Override default bw/delay for tunnel
 !
 bandwidth 1024
 delay 100
 !
 tunnel protection ipsec profile DMVPN
```

R3:

```
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5
  mode tunnel
!
crypto ipsec profile DMVPN
  set transform 3DES_MD5_TRANS
!
! DMVPN Spoke
!
interface Tunnel0
 ip address 123.123.123.3 255.255.255.0
 tunnel source Loopback0
 tunnel mode gre multi
 tunnel key 123
 ip nhrp network-id 123
 ip nhrp authentication CISCO
 ip nhrp hold 30
 ip nhrp map 123.123.123.1 150.1.1.1
 ip nhrp map multicast 150.1.1.1
 ip nhrp nhs 123.123.123.1
 !
 ! Override default bw/delay for tunnel
 !
 bandwidth 1024
 delay 100
 !
 tunnel protection ipsec profile DMVPN
```

VPN Routing:

R1:

```
router eigrp 100
 no auto-summary
 network 123.123.123.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
!
interface Tunnel0
 no ip split-horizon eigrp 100
```

```
R2:
router eigrp 100
 no auto-summary
 network 123.123.123.0 0.0.0.255
 network 192.168.2.0 0.0.0.255

R3:
router eigrp 100
 no auto-summary
 network 123.123.123.0 0.0.0.255
 network 192.168.3.0 0.0.0.255
```

Verification

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
Type
                                            (sec)         (ms)       Cnt Num
1   123.123.123.3           Tu0               12 00:01:22   56   336  0  2
0   123.123.123.2           Tu0               12 00:01:33   17   200  0  3

R1#show ip nhrp
123.123.123.2/32 via 123.123.123.2, Tunnel0 created 00:35:30, expire 00:00:12
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 150.1.2.2
123.123.123.3/32 via 123.123.123.3, Tunnel0 created 00:35:10, expire 00:00:13
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 150.1.3.3

R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
Type
                                            (sec)         (ms)       Cnt Num
0   123.123.123.1           Tu0               10 00:01:44   20   200  0  4

R2#show ip route eigrp
D    192.168.1.0/24 [90/2653440] via 123.123.123.1, 00:01:49, Tunnel0
D    192.168.3.0/24 [90/2679040] via 123.123.123.1, 00:01:41, Tunnel0

R2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/17/20 ms

R2#ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 76/77/80 ms

R2#show ip nhrp
123.123.123.1/32 via 123.123.123.1, Tunnel0 created 00:35:05, never expire
  Type: static, Flags: authoritative used
  NBMA address: 150.1.1.1
192.168.3.0/24 via 192.168.3.3, Tunnel0 created 00:00:00, expire 00:00:29
```

```
  Type: dynamic, Flags: router unique
  NBMA address: 150.1.3.3

R2#show crypto isakmp sa
dst             src             state          conn-id slot
150.1.2.2       150.1.3.3       QM_IDLE              2    0
150.1.1.1       150.1.2.2       QM_IDLE              1    0

R2#ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/72/80 ms

R2#show cry ips sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr. 150.1.2.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0)
   current_peer: 150.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 150.1.2.2, remote crypto endpt.: 150.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 52678822

     inbound esp sas:
      spi: 0xC26D47B9(3261941689)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 5, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4564366/3567)
        IV size: 8 bytes
        replay detection support: Y
      spi: 0x9A04BA4D(2584001101)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2006, flow_id: 7, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4579606/3567)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xD33C8295(3543958165)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2005, flow_id: 6, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4564366/3567)
        IV size: 8 bytes
```

```
        replay detection support: Y
      spi: 0x52678822(1382516770)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 8, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4579606/3565)
        IV size: 8 bytes
        replay detection support: Y

    outbound ah sas:

    outbound pcp sas:

  protected vrf:
  local  ident (addr/mask/prot/port): (150.1.2.2/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (150.1.3.3/255.255.255.255/47/0)
  current_peer: 150.1.3.3:500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
   #pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 150.1.2.2, remote crypto endpt.: 150.1.3.3
    path mtu 1500, media mtu 1500
    current outbound spi: 138EA870

    inbound esp sas:
     spi: 0x50C4E27E(1355080318)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2008, flow_id: 9, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4592139/3581)
        IV size: 8 bytes
        replay detection support: Y

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x138EA870(328116336)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2009, flow_id: 10, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4592140/3579)
        IV size: 8 bytes
        replay detection support: Y

    outbound ah sas:

    outbound pcp sas:
```

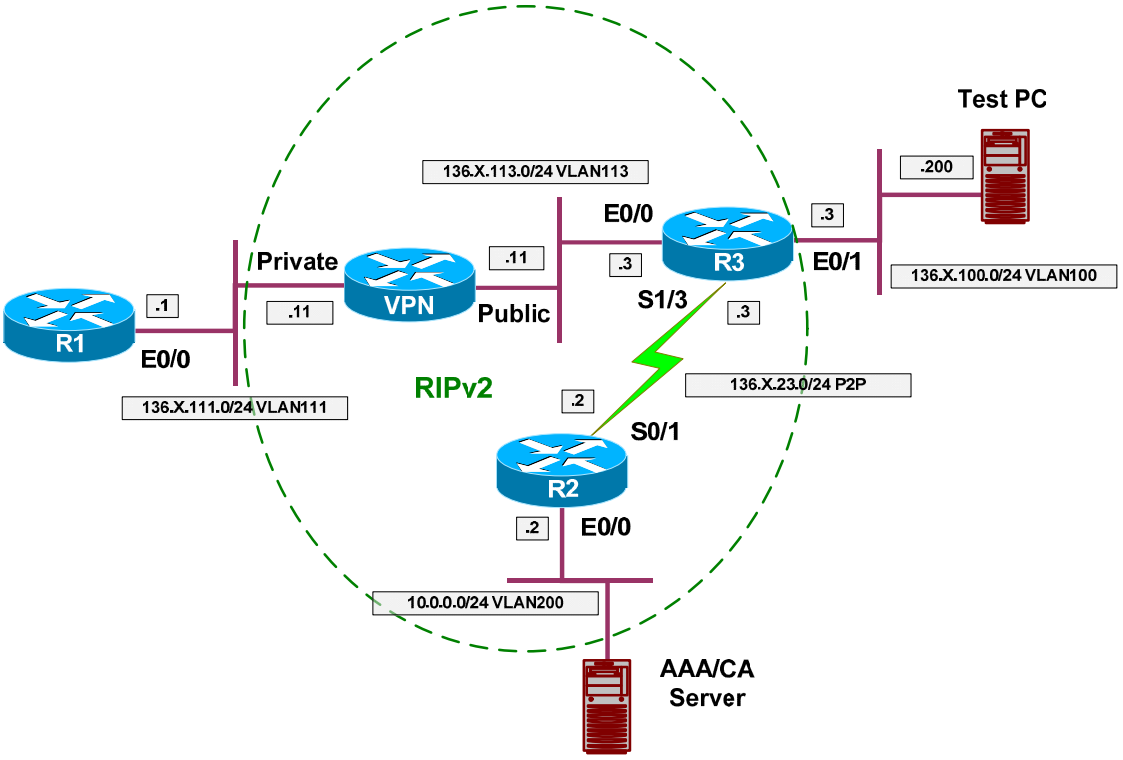
Further Reading

Dynamic Multipoint VPN (DMVPN)

Easy VPN

VPN3k and Cisco VPN Client

Objective: Configure VPN3k to accept remote VPN Client connections.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "VPN3k ezVPN".
- Create new Group on VPN 3000 Concentrator as follows:
    - Name EZVPN password CISCO.
    - Configure IPsec as the only tunneling protocol.
    - Configure IPsec Remote Access Tunnel Type.
    - Configure IPsec Xauth.
- Assign Address Pool "20.0.0.1-20.0.0.254" to group EZVPN.
- Create new User on VPN 3000:
    - Name CISCO password CISCO1234

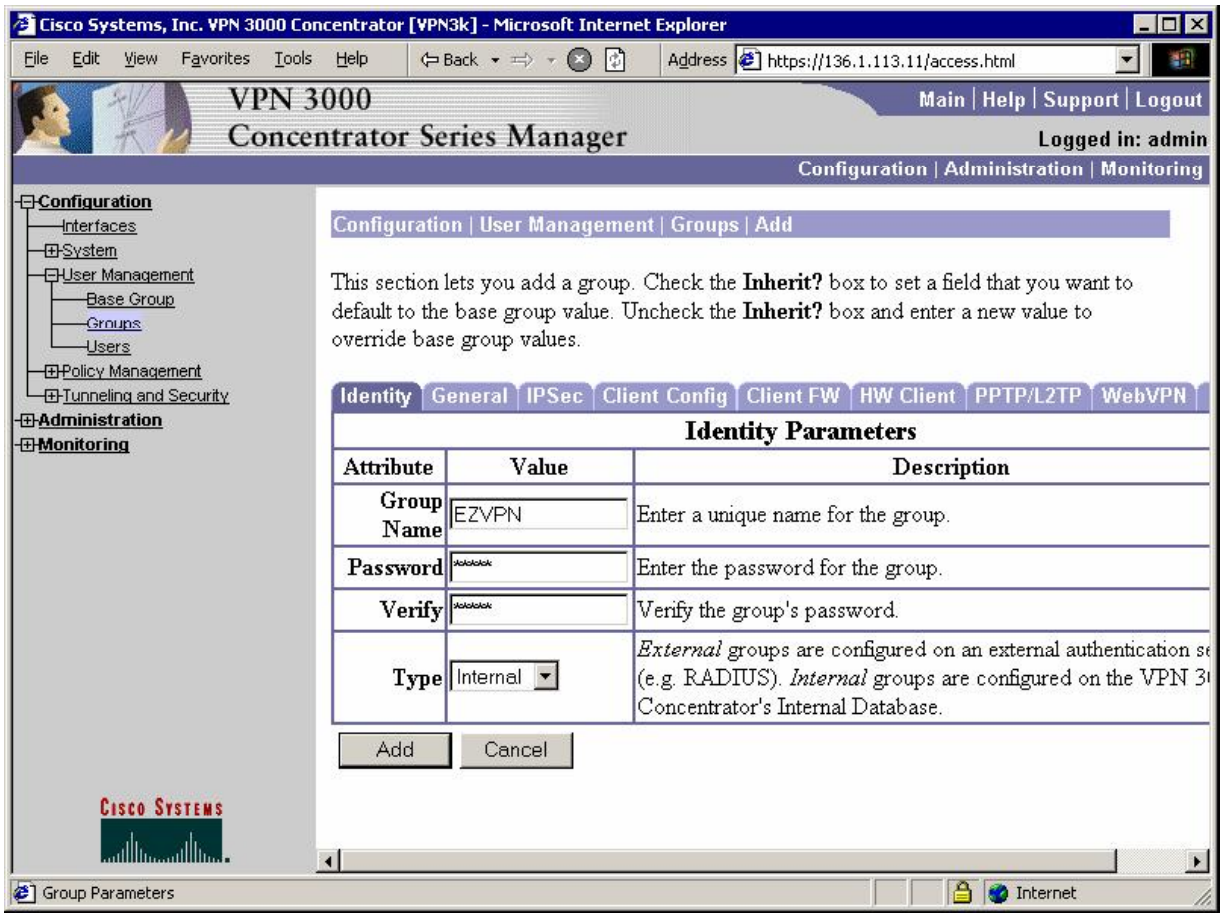
- o Group EZVPN

- Permit address allocation from Address Pools.
- Configure Cisco VPN Client to connect to VPN3000.

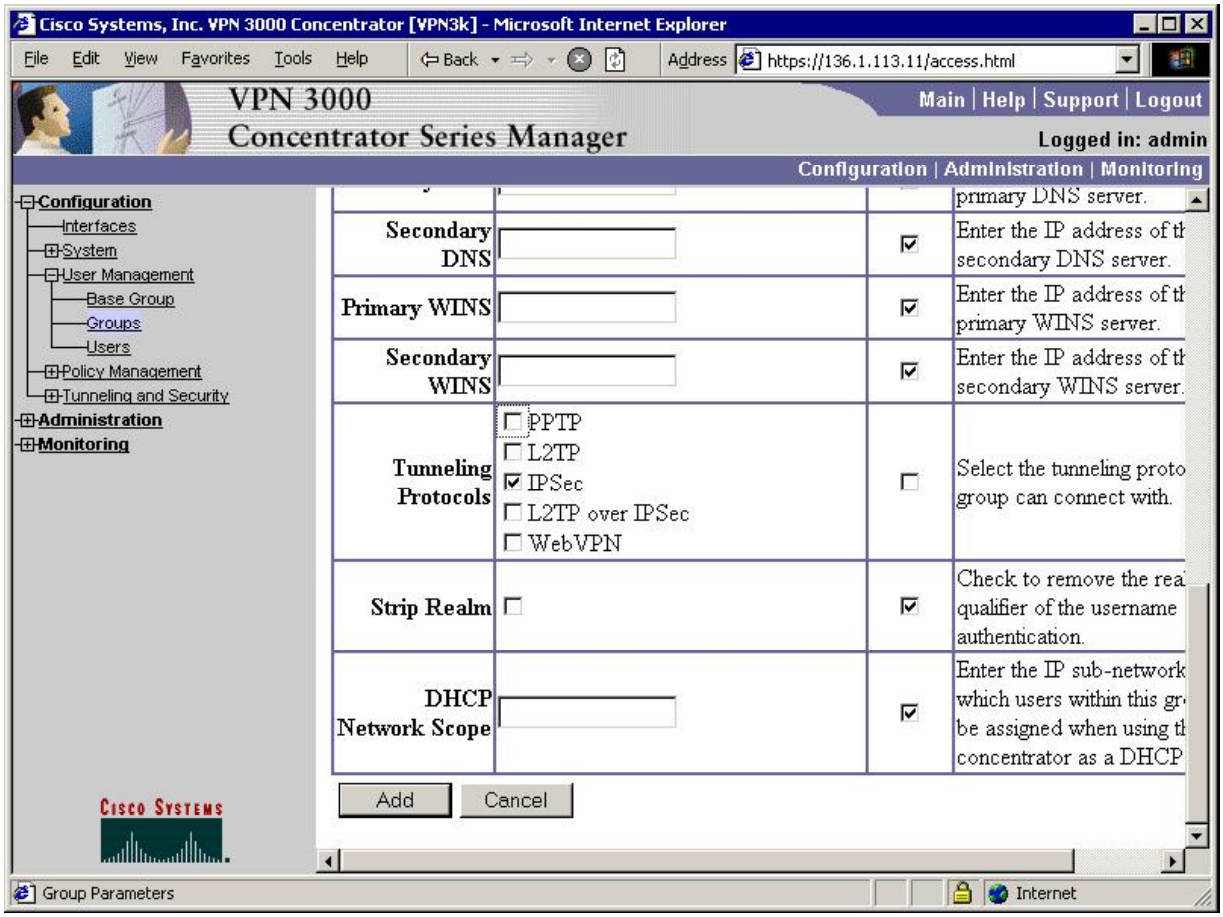
Final Configuration

VPN3k:

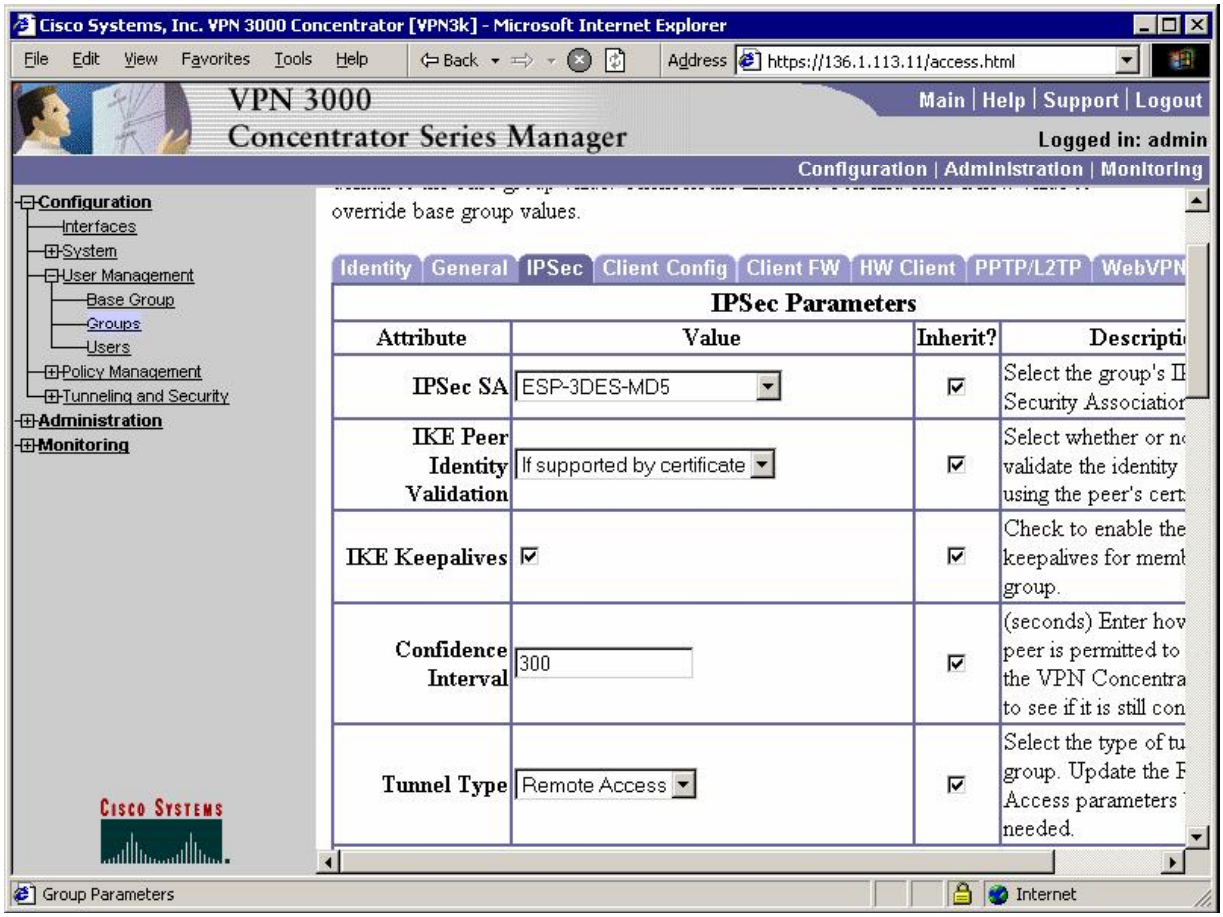
Create new group:



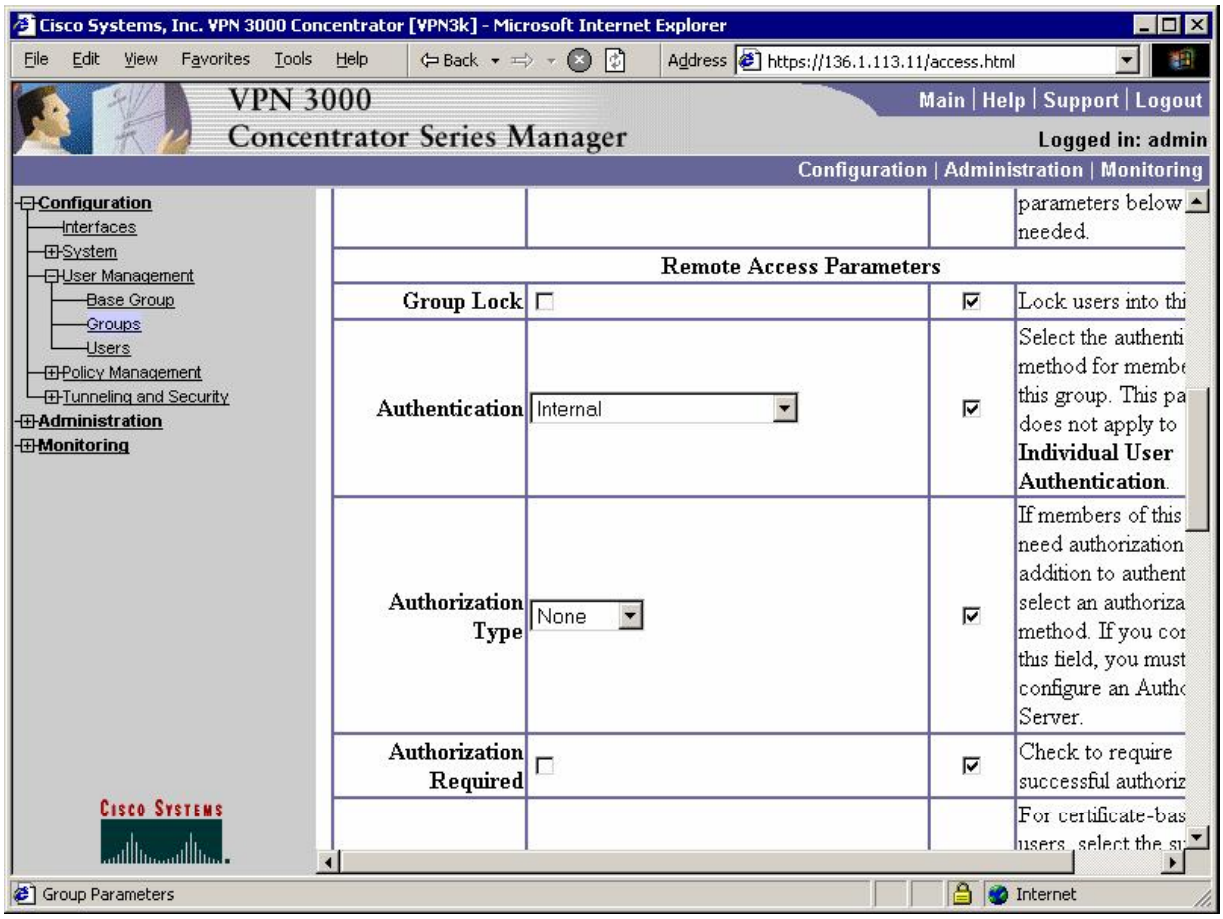
Permit IPsec as the only tunneling protocol in General Tab:



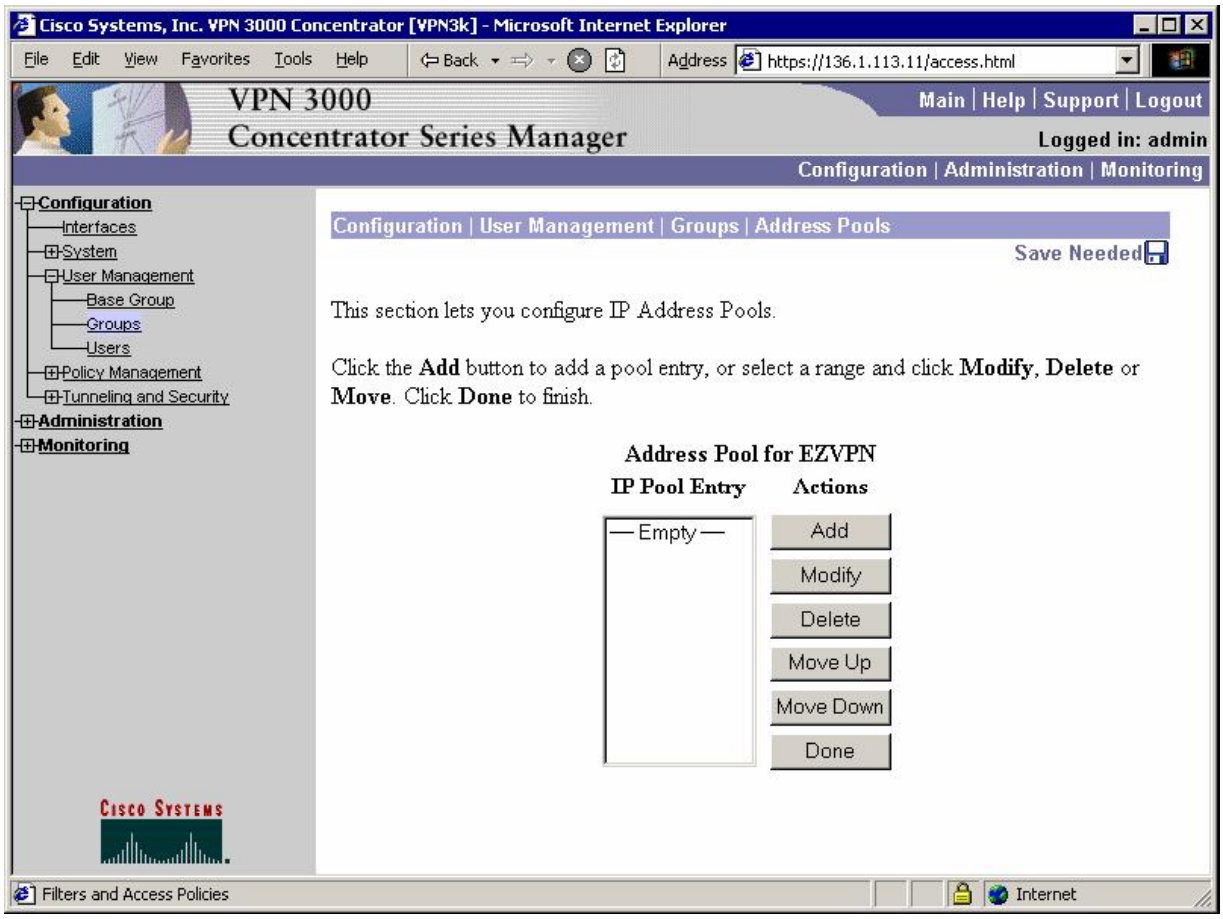
Make sure you group have "Remote Access" IPSec "Tunnel type":

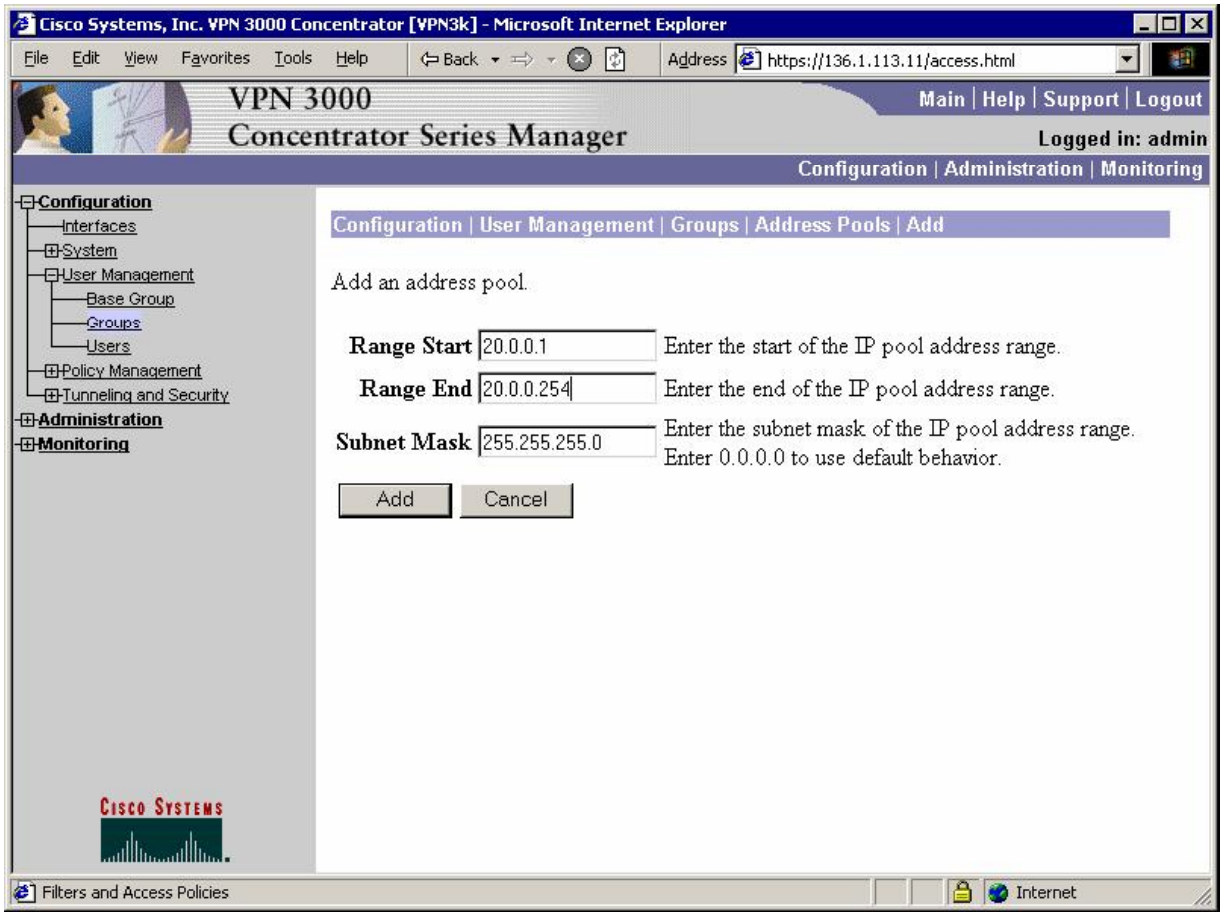


And that you have authentication (Xauth) enabled in IPsec Tab:



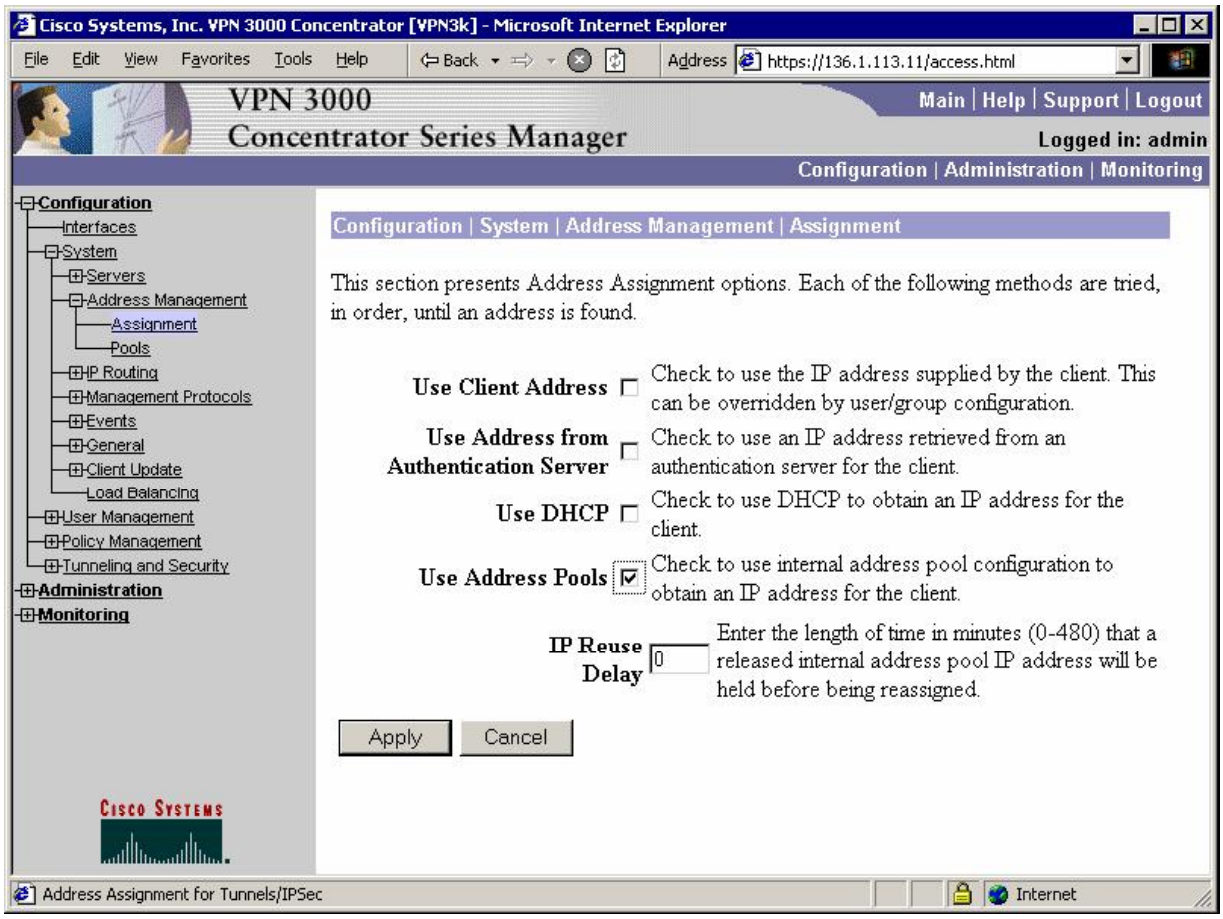
Modify address pools for a Group:




Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Tunneling and Security
Administration
Monitoring
Configuration | User Management | Groups | Address Pools | Add
Add an address pool.
Range Start 20.0.0.1
Enter the start of the IP pool address range.
Range End 20.0.0.254
Enter the end of the IP pool address range.
Subnet Mask 255.255.255.0
Enter the subnet mask of the IP pool address range.
Enter 0.0.0.0 to use default behavior.
Add
Cancel
Cisco Systems
Filters and Access Policies
Internet

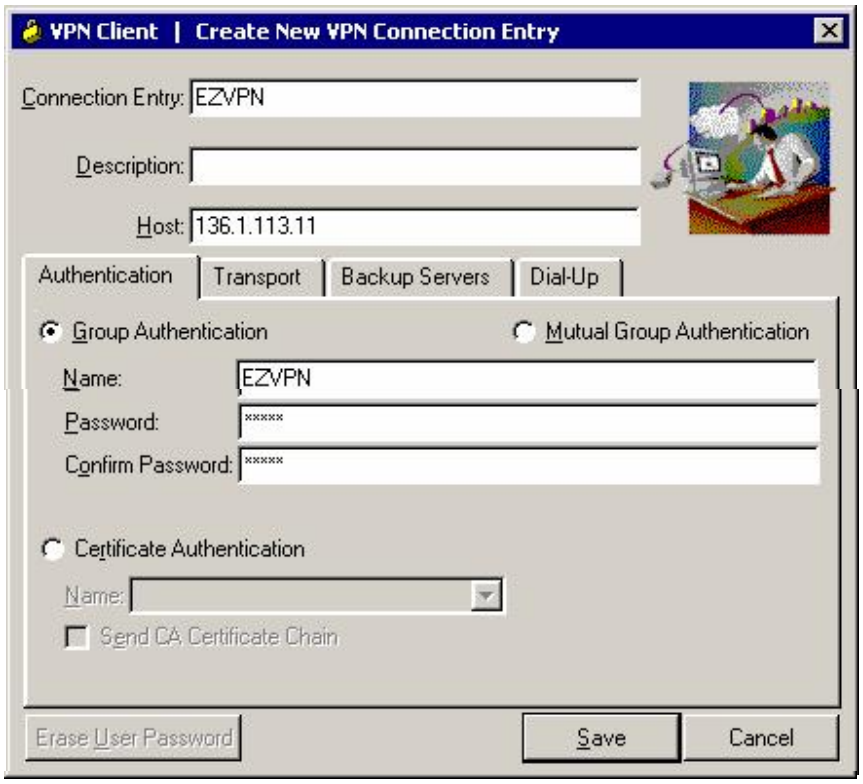
Add new user "CISCO/CISCO1234" to the group "EZVPN":

Allow IP address Assignment from Address Pools:



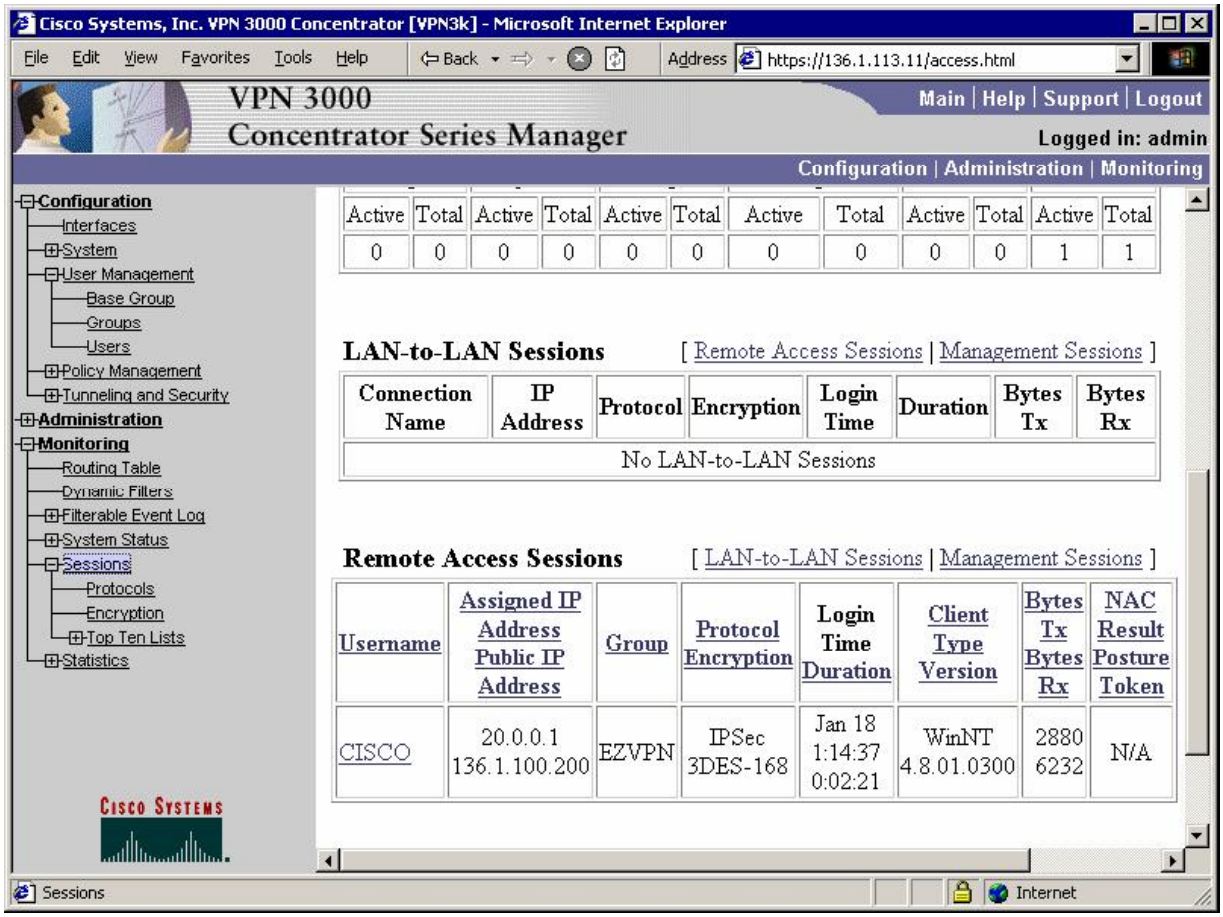
Verification

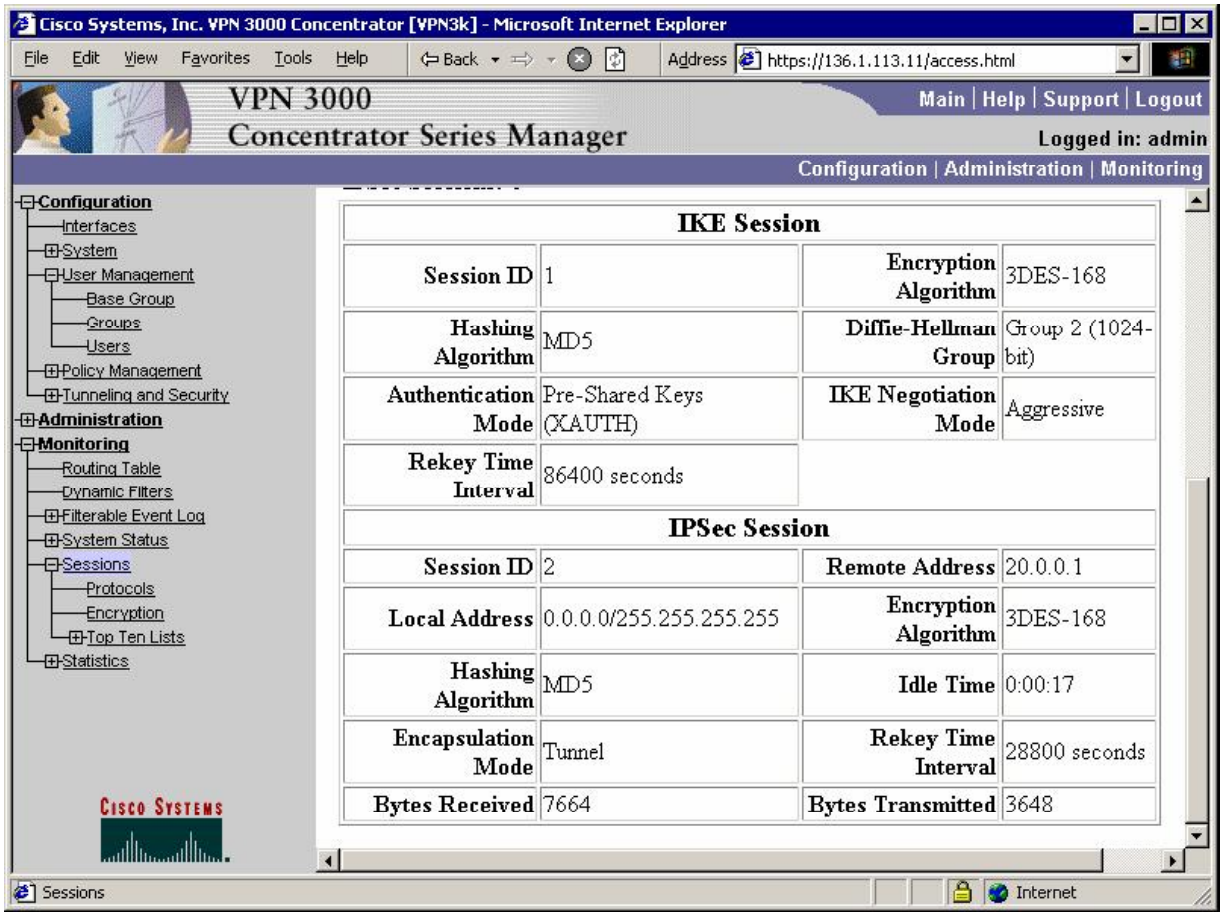
Configure Cisco VPN Client on Test PC, use key "CISCO":



Connect the VPN Client and enter CISCO/CISCO1234 when prompted for Xauth.

Verify connected Remote Sessions at VPN3k:



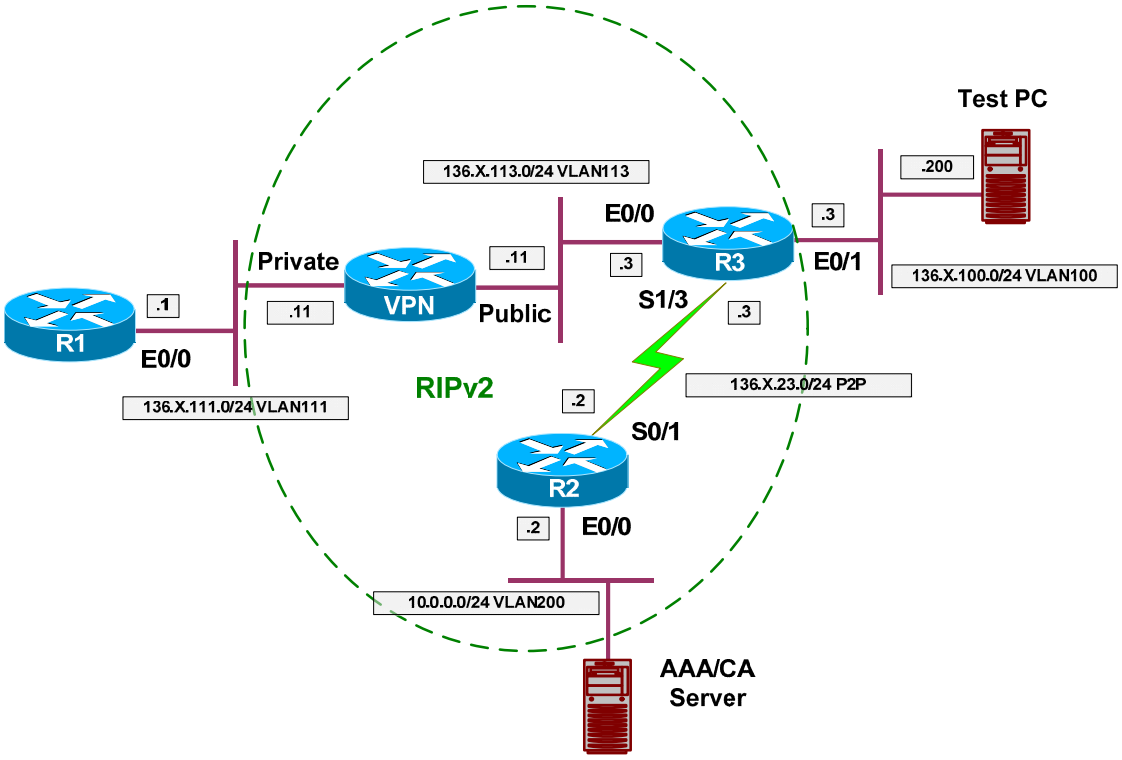


Further Reading

[IPsec with VPN Client to VPN 3000 Concentrator Configuration Example]

VPN3k and Cisco VPN Client with Split-Tunneling

Objective: Configure VPN3k and Cisco VPN Client for split-tunneling.



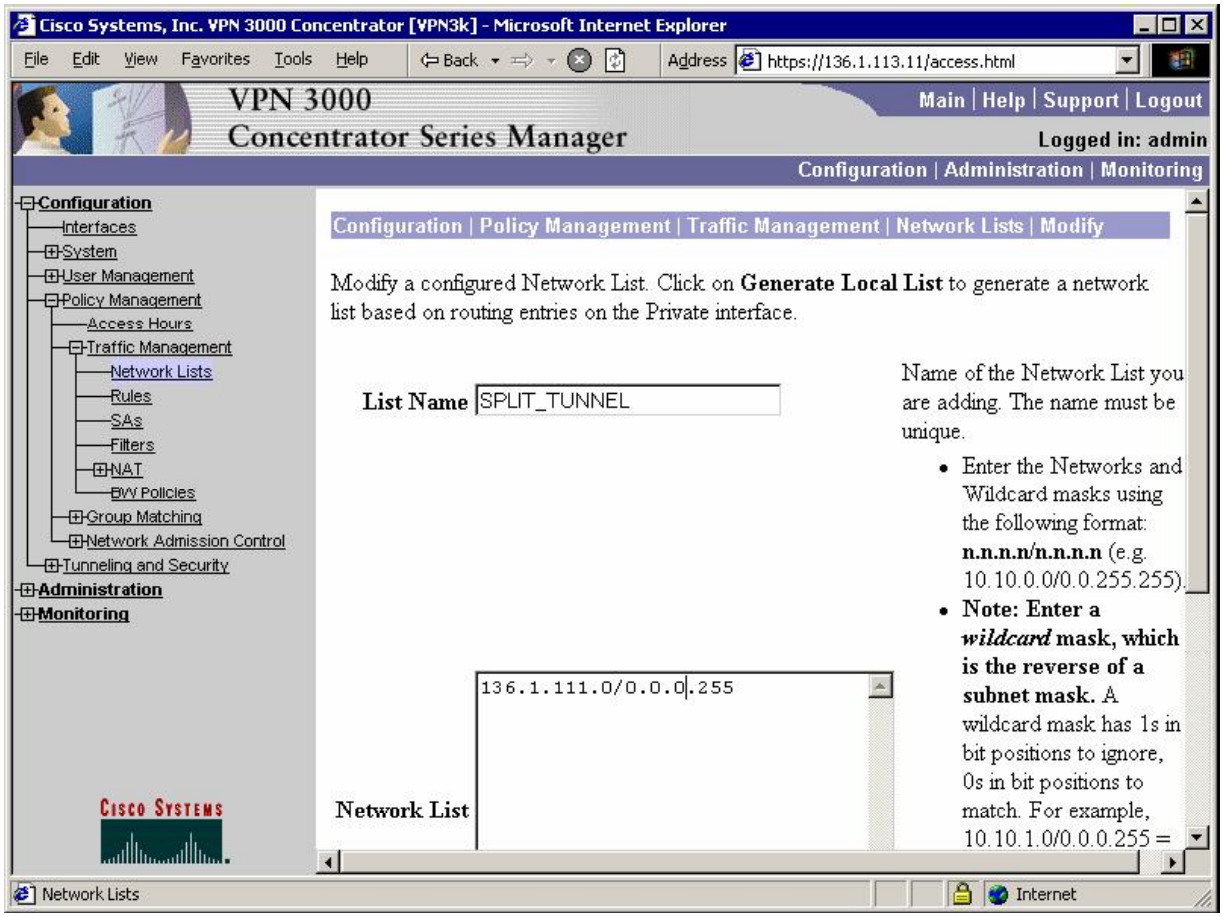
Directions

- Configure devices as per the scenario " VPN/ezVPN" "VPN3k and Cisco VPN Client".
- The goal to encrypt only traffic from client to network 136.1.111.0/24.
- First, create network list to distinguish network 136.1.111.0/24, name it SPLIT_TUNNEL.
- Next, modify group EZVPN, changing split-tunneling settings under "Client Config" Tab.

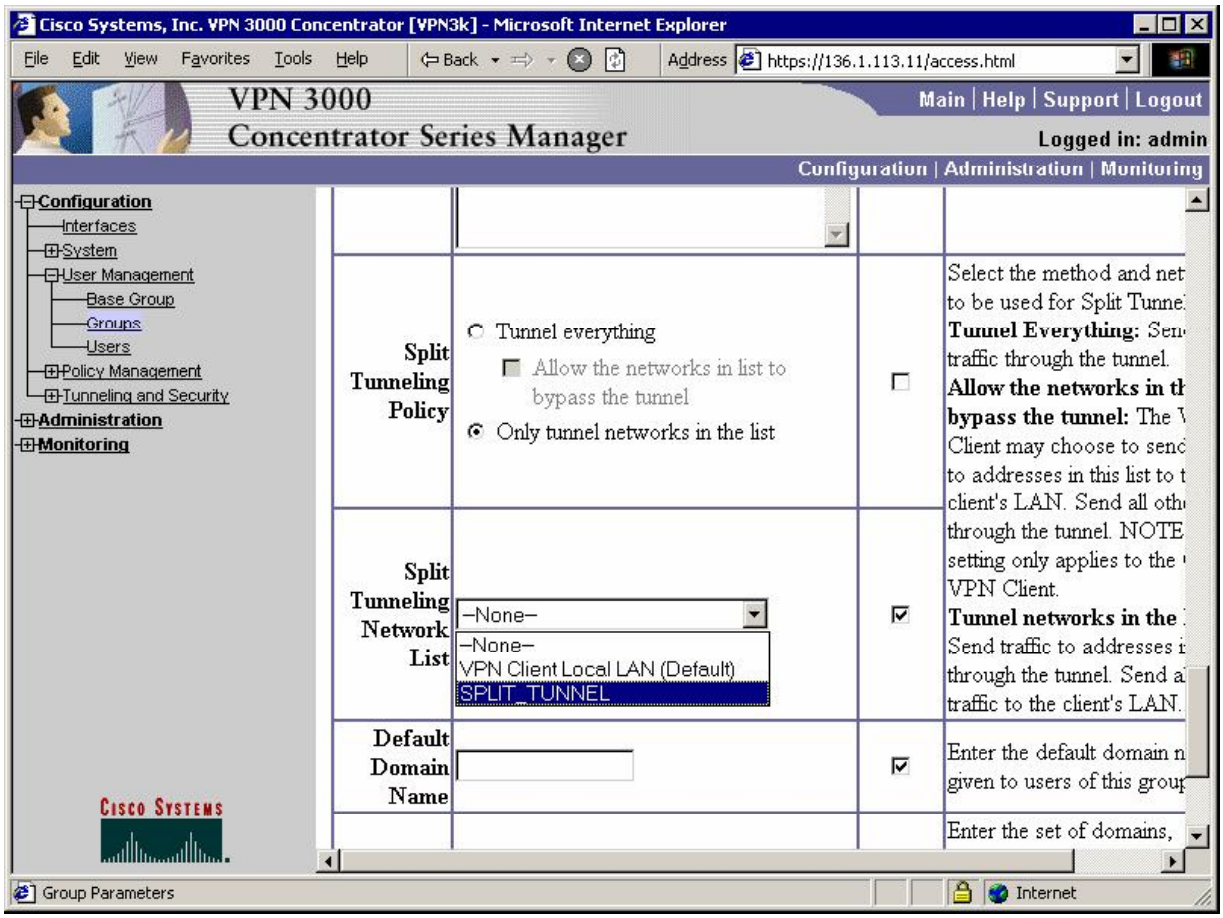
Final Configuration

VPN3k:

Create Network List for split-tunneling:



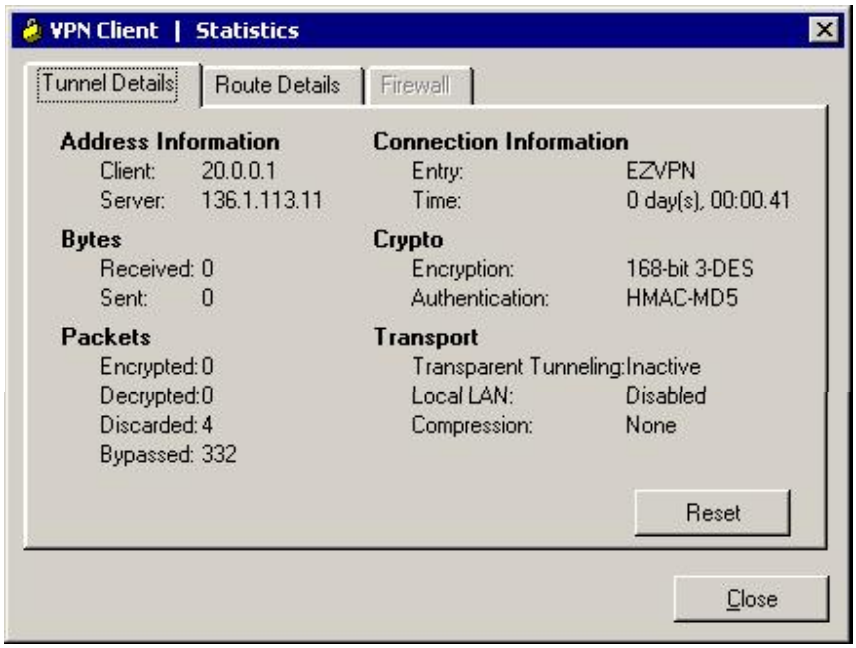
Modify group "EZVPN", "Client Config" Tab. Chose "Only tunnel networks in the list":

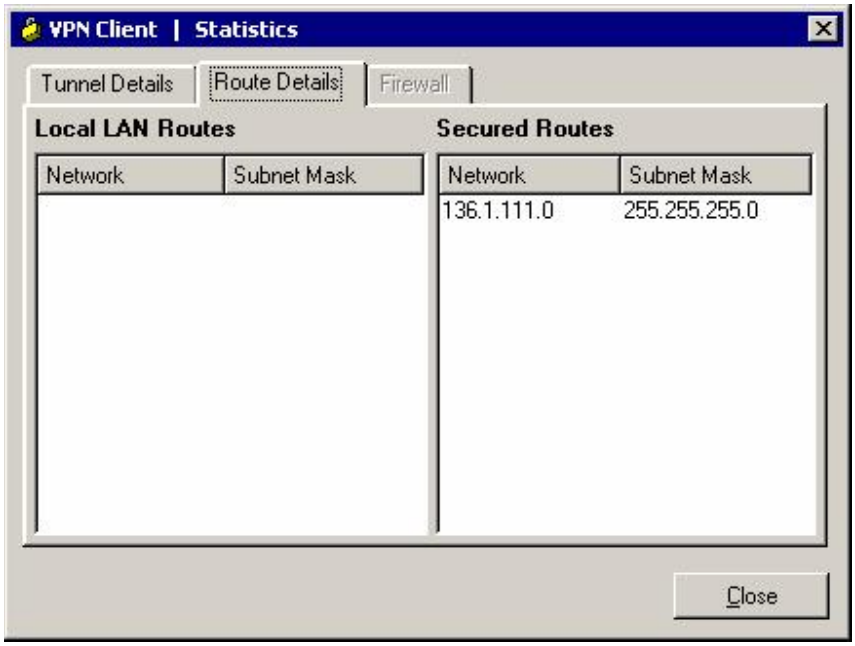


Verification

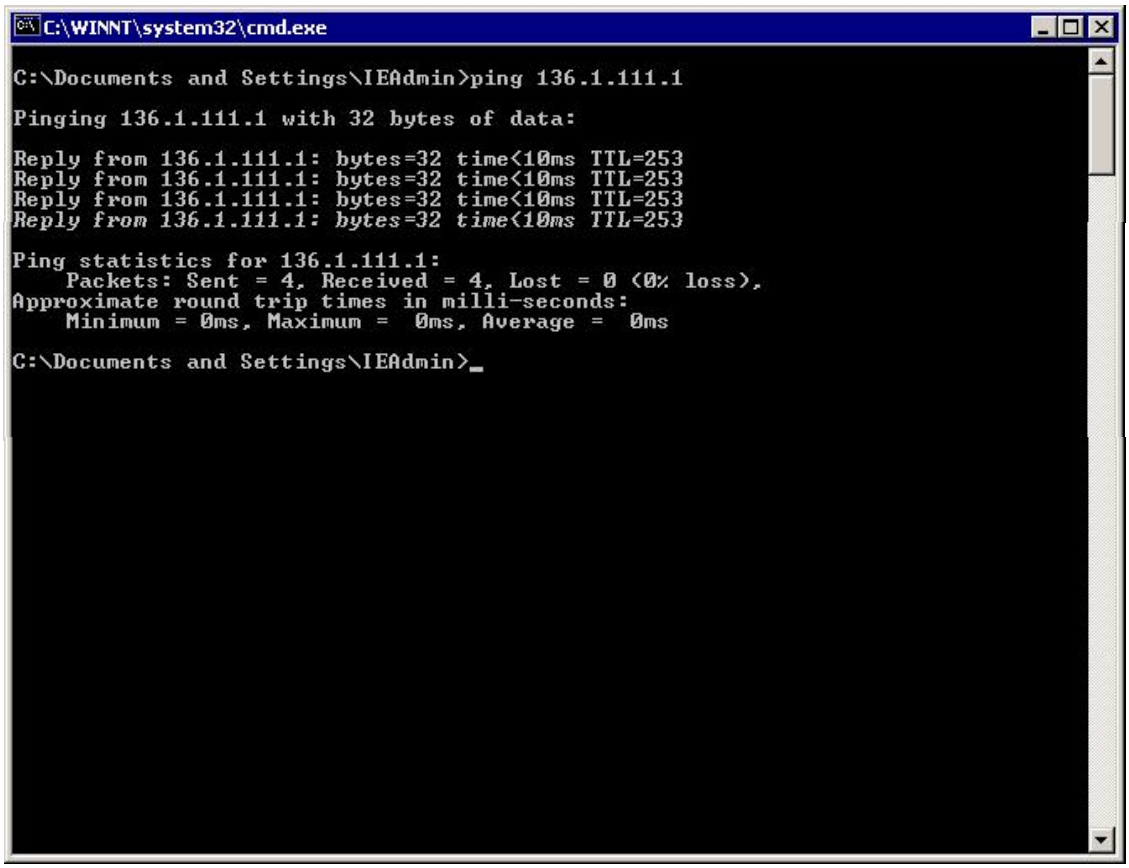
Connect Cisco VPN Client on Test PC:

Check VPN Client Statistics:



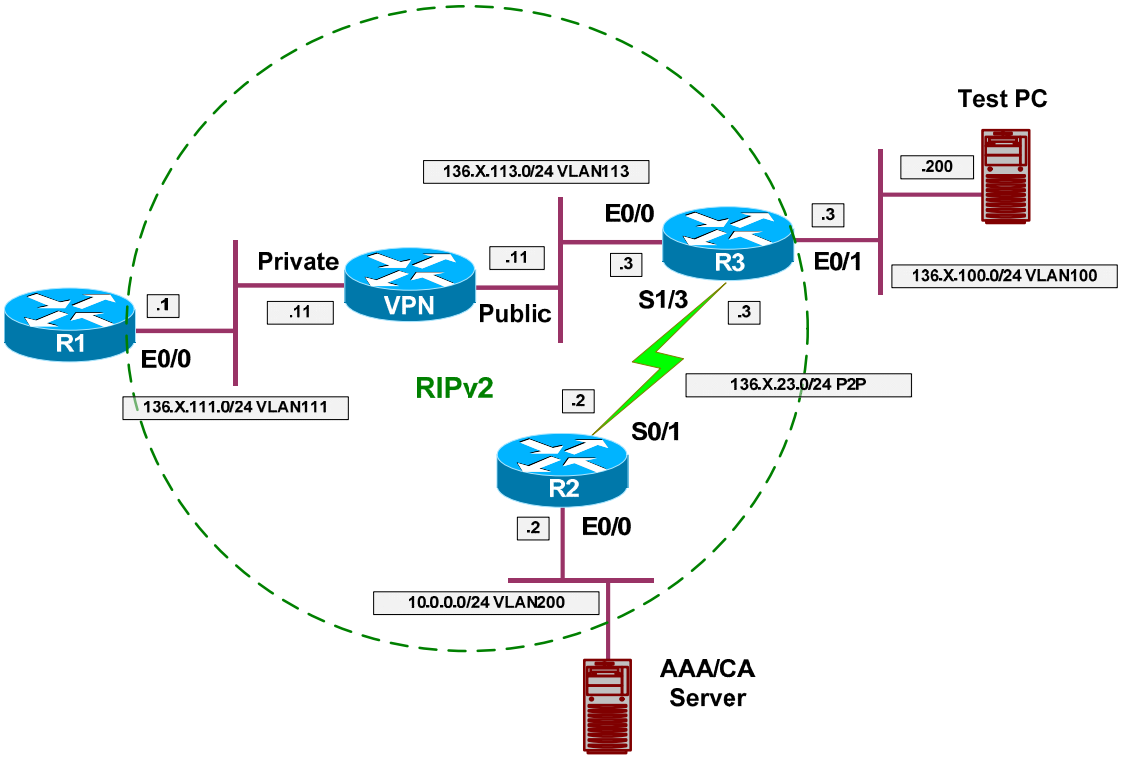


Test connectivity:



VPN3k and Cisco VPN Client with Hold-Down Route

Objective: Configure VPN3k to advertise Hold-Down route via RIP.



Directions

- Configure devices as per the scenario " VPN/ezVPN" "VPN3k and Cisco VPN Client with Split Tunneling".
- The idea of hold-down route is to advertise the network corresponding to the locally configure address pool.
- Remove static default route on R1, and configure RIP routing.
- Note that inbound RIP is enabled by default on VPN3k Private Interface.
- Configure outbound RIPv2 on Private Interface of VPN3k.
- Create Hold-Down routes on VPN3k by generating them based on pre-configured Address-Pools.

Final Configuration

```
R1:
no ip route 0.0.0.0 0.0.0.0 136.1.111.11
router rip
 ver 2
 no auto
 network 136.1.0.0

VPN3k CLI:
```

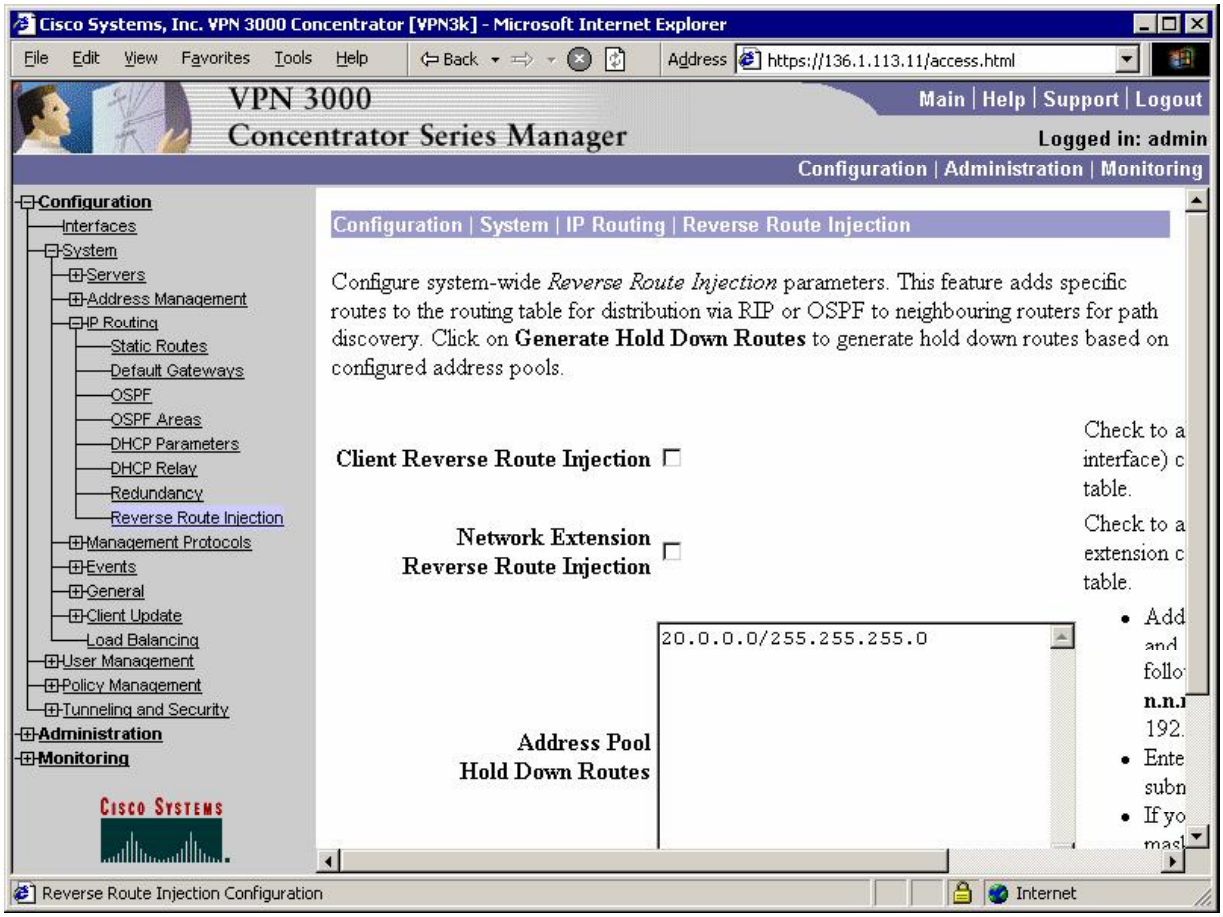
Enable RIP outbound on Private Interface:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3k: Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|      UP      |   136.1.113.11/255.255.255.0  | 00.03.A0.88.BD.2A
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

VPN3k: Interfaces -> 1

1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Set Interface Name
4) Select IP Filter
5) Select Ethernet Speed
6) Select Duplex
7) Set MTU
8) Set Port Routing Config
9) Set Bandwidth Management
10) Set Public Interface IPSec Fragmentation Policy
11) Set Interface WebVPN Parameters
12) Back

VPN3k: Ethernet Interface 1 -> 8

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 1 -> 1

1) Disable Inbound RIP
```

```
2) Enable RIP V1 Inbound
3) Enable RIP V2 Inbound
4) Enable RIP V2/V1 Inbound

VPN3k: Ethernet Interface 1 -> [ 4 ]

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 1 -> 2

1) Disable Outbound RIP
2) Enable RIP V1 Outbound
3) Enable RIP V2 Outbound
4) Enable RIP V2/V1 Outbound

VPN3k: Ethernet Interface 1 -> [ 1 ] 4

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 1 ->
```


VPN3k GUI:

Configure Hold-Down Route on VPN3k: Choose "Generate Hold Down Routes":



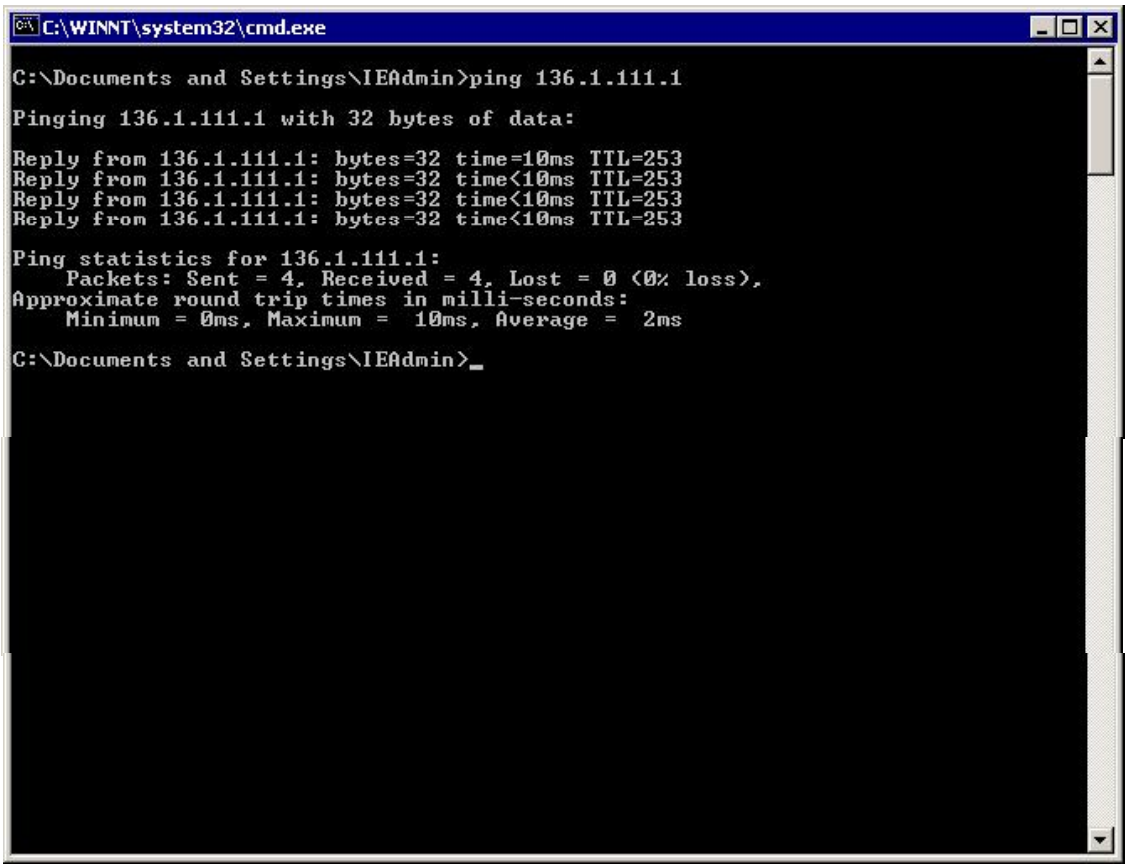
Verification

VPN3k:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 3

1) Routing Table
2) Event Log
3) System Status
4) Sessions
5) General Statistics
6) Dynamic Filters
7) Back

VPN3k: Monitor -> 1

Routing Table
-------------
Number of Routes: 7
   IP Address         Mask           Next Hop    Intf Protocol Age Metric
-----------------------------------------------------------------------------
10.0.0.0        255.255.255.0   136.1.113.3        2 RIP       17      3
20.0.0.0        255.255.255.0   136.1.113.11       2 Static     0      1
136.1.0.0       255.255.255.0   136.1.113.3        2 RIP       17      3
136.1.23.0      255.255.255.0   136.1.113.3        2 RIP       17      2
136.1.100.0     255.255.255.0   136.1.113.3        2 RIP       17      2
136.1.111.0     255.255.255.0   0.0.0.0            1 Local      0      1
136.1.113.0     255.255.255.0   0.0.0.0            2 Local      0      1

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/3] via 136.1.111.11, 00:00:22, Ethernet0/0
R       136.1.23.0 [120/2] via 136.1.111.11, 00:00:22, Ethernet0/0
C       136.1.111.0 is directly connected, Ethernet0/0
R       136.1.100.0 [120/2] via 136.1.111.11, 00:00:22, Ethernet0/0
R       136.1.113.0 [120/1] via 136.1.111.11, 00:00:22, Ethernet0/0
R    20.0.0.0/8 [120/1] via 136.1.111.11, 00:00:22, Ethernet0/0
R    10.0.0.0/8 [120/3] via 136.1.111.11, 00:00:22, Ethernet0/0

R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/1] via 136.1.23.2, 00:00:24, Serial1/3
C       136.1.23.0 is directly connected, Serial1/3
R       136.1.111.0 [120/1] via 136.1.113.11, 00:00:10, Ethernet0/0
C       136.1.100.0 is directly connected, Ethernet0/1
C       136.1.113.0 is directly connected, Ethernet0/0
     20.0.0.0/24 is subnetted, 1 subnets
R       20.0.0.0 [120/1] via 136.1.113.11, 00:00:10, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/1] via 136.1.23.2, 00:00:26, Serial1/3
```

Connect VPN Client and ping R1 from Test PC:

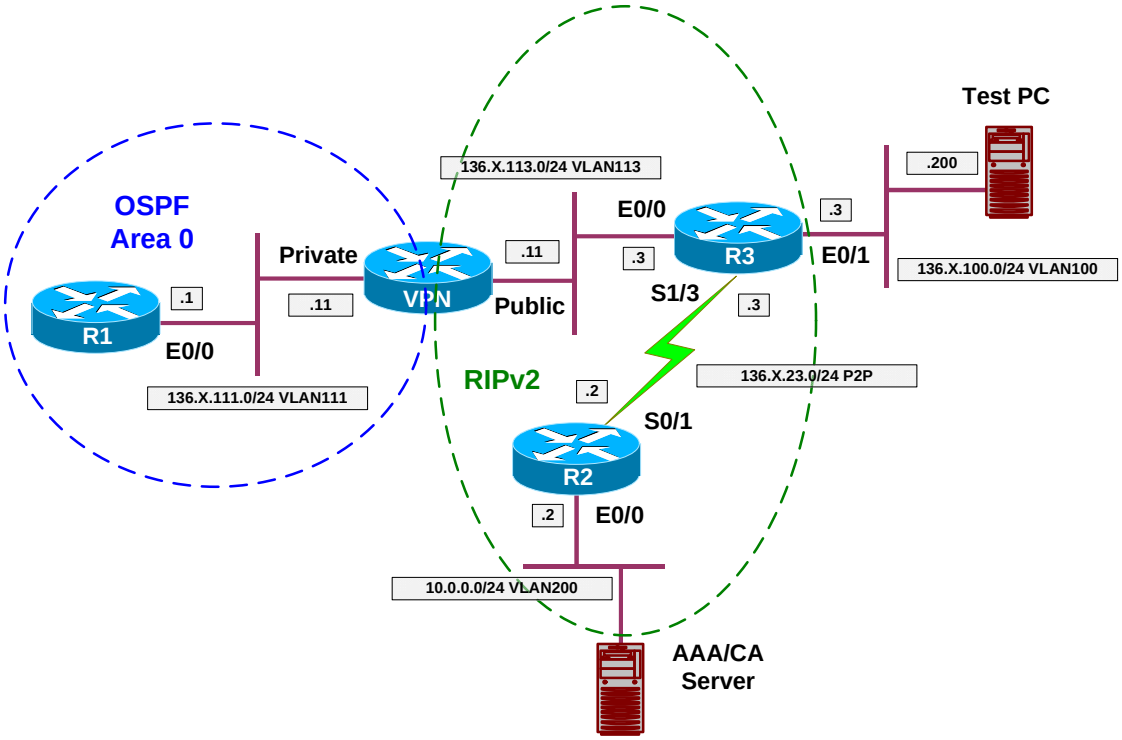


Further Reading

[How to Populate Dynamic Routes Using Reverse Route Injection]

VPN3k and Cisco VPN Client with RRI

Objective: Configure VPN3k for RRI with OSPF routing.



Directions

- Configure devices as per the scenario " VPN/Easy VPN" "VPN3k and Cisco VPN Client with Split Tunneling".
- The key point with RRI into OSPF is to configure ASBR feature on the VPN3k, so that it starts advertising external routes into OSPF.
- Remove static default route on R1 and configure OSPF routing as per the diagram.
- Enable OSPF process on VPN3k as follows:
    - Use router-id 150.X.11.11.
    - Permit ASBR feature.
- Enable OSPF on the Private interface of the VPN3k. Use Area 0.

Final Configuration

```
R1:
no ip route 0.0.0.0 0.0.0.0 136.1.111.11
!
router ospf 1
 network 136.1.111.0 0.0.0.255 area 0
```

VPN3k CLI:

Configure OSPF on the Private Interface:

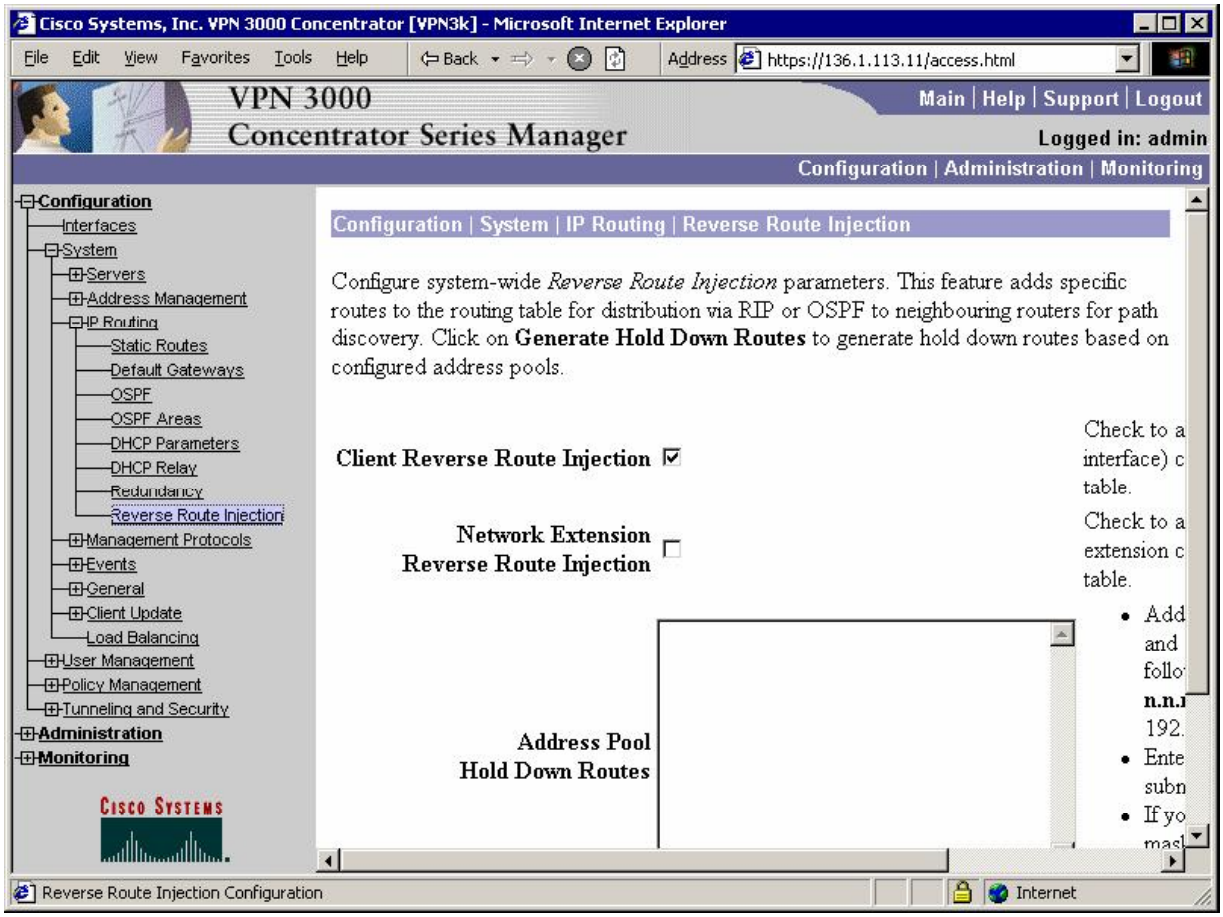
```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3k: Config -> 2

1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back

VPN3k: System -> 3

1) Static Routes
2) Default Gateways
3) OSPF
4) OSPF Areas
5) DHCP Parameters
6) Redundancy
7) Reverse Route Injection
8) DHCP Relay
9) Back

VPN3k: Routing -> 3

1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back

VPN3k: OSPF -> 2

> Router ID

VPN3k: OSPF -> [ 0.0.0.0 ] 150.1.11.11

1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
```

```
VPN3k: OSPF -> 1

1) Enable OSPF
2) Disable OSPF

VPN3k: OSPF -> [ 2 ] 1

1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back

VPN3k: OSPF -> 3

1) Enable Autonomous System
2) Disable Autonomous System

VPN3k: OSPF -> [ 2 ] 1

1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back

VPN3k: OSPF -> h

1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3k: Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
--------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|      UP      |   136.1.113.11/255.255.255.0  | 00.03.A0.88.BD.2A
--------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

VPN3k: Interfaces -> 1

1) Interface Setting (Disable, DHCP or Static IP)
```

```
2) Set Public Interface
3) Set Interface Name
4) Select IP Filter
5) Select Ethernet Speed
6) Select Duplex
7) Set MTU
8) Set Port Routing Config
9) Set Bandwidth Management
10) Set Public Interface IPSec Fragmentation Policy
11) Set Interface WebVPN Parameters
12) Back

VPN3k: Ethernet Interface 1 -> 8

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 1 -> 3

1) Enable OSPF
2) Disable OSPF

VPN3k: Ethernet Interface 1 -> [ 2 ] 1

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 1 -> 4

1) Set OSPF Area ID
2) Set OSPF Priority
3) Set OSPF Metric
4) Set OSPF Retransmit Interval
5) Set OSPF Hello Interval
6) Set OSPF Dead Interval
7) Set OSPF Transit Delay
8) Set OSPF Authentication
9) Back

VPN3k: Ethernet Interface 1 -> 1

> OSPF Area ID

VPN3k: Ethernet Interface 1 -> [ 0.0.0.0 ] 0.0.0.0

1) Set OSPF Area ID
2) Set OSPF Priority
3) Set OSPF Metric
4) Set OSPF Retransmit Interval
5) Set OSPF Hello Interval
6) Set OSPF Dead Interval
7) Set OSPF Transit Delay
8) Set OSPF Authentication
9) Back

VPN3k: Ethernet Interface 1 ->
```

VPN3k GUI:

Configure Client Reverse Route Injection:

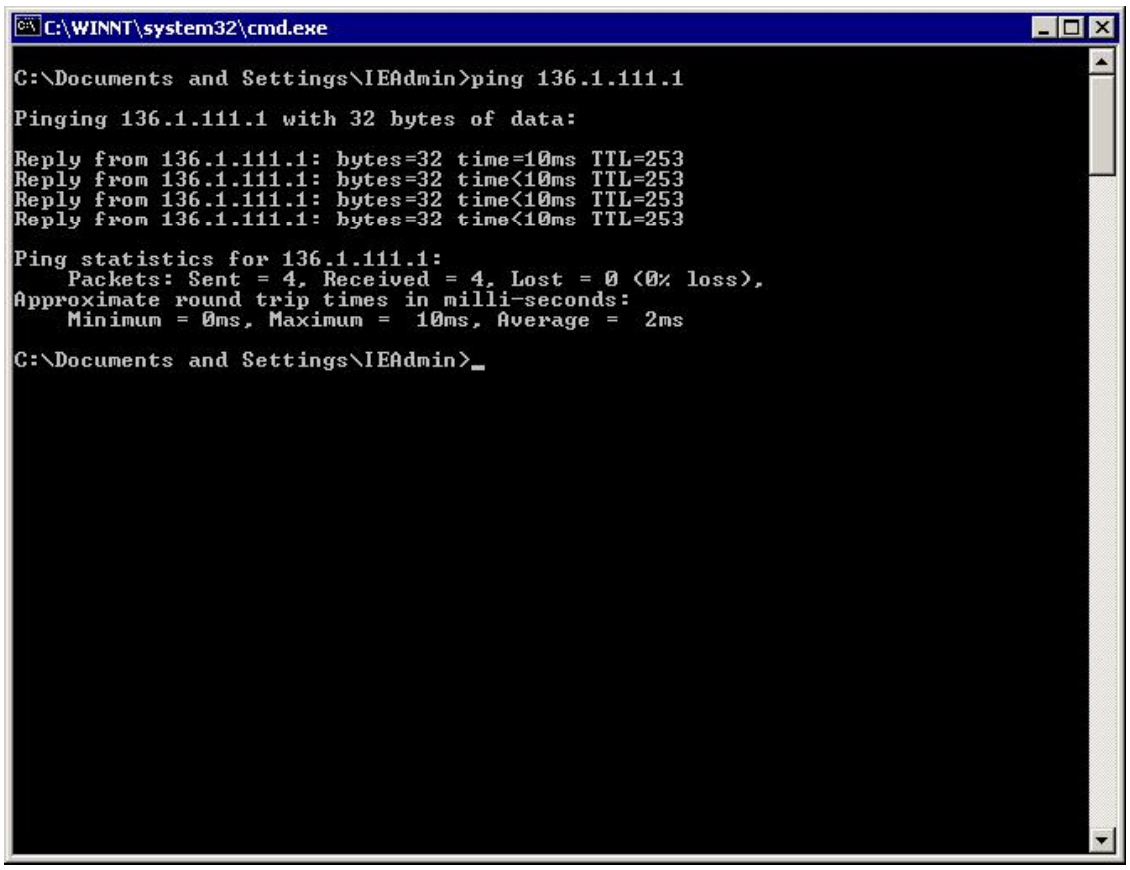


Verification

Connect Cisco VPN Client from Test PC to the VPN3k:

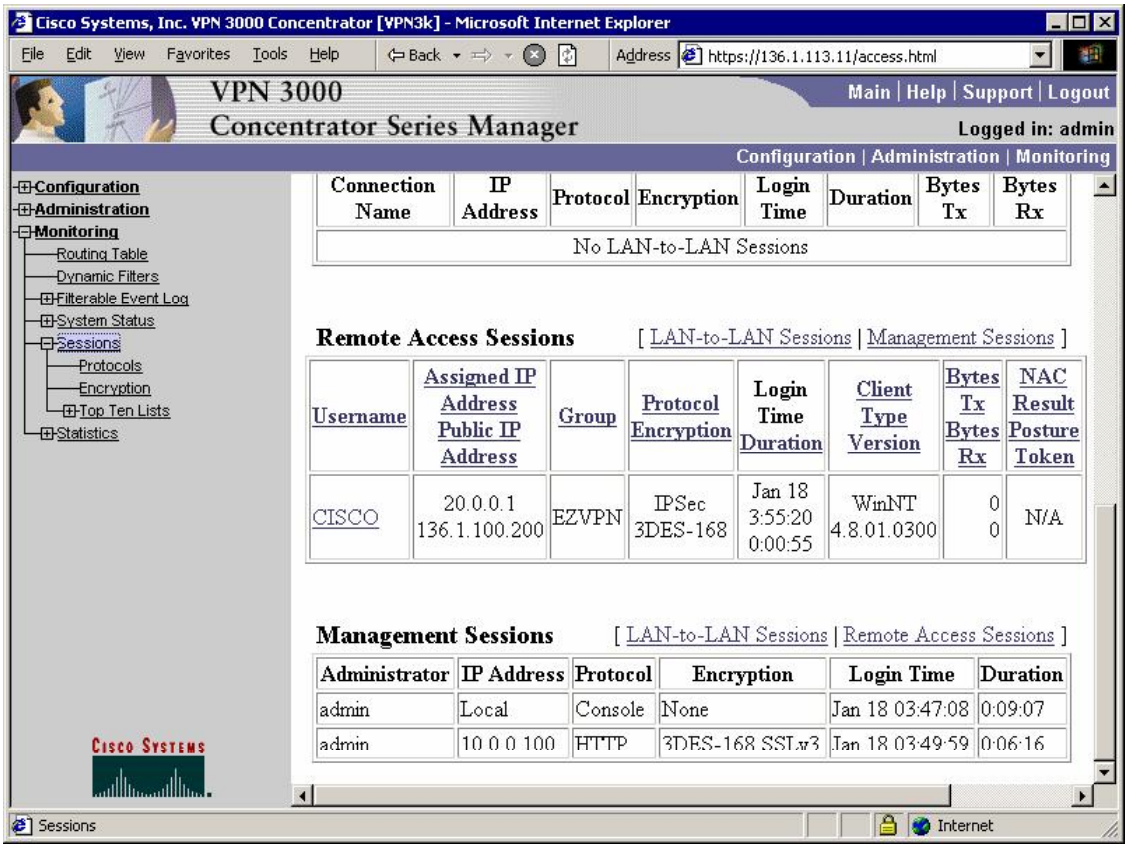
```
R1#show ip route ospf
     136.1.0.0/24 is subnetted, 4 subnets
O E2    136.1.0.0 [110/20] via 136.1.111.11, 00:08:09, Ethernet0/0
O E2    136.1.23.0 [110/20] via 136.1.111.11, 00:08:09, Ethernet0/0
O E2    136.1.100.0 [110/20] via 136.1.111.11, 00:08:09, Ethernet0/0
     20.0.0.0/32 is subnetted, 1 subnets
O E2    20.0.0.1 [110/20] via 136.1.111.11, 00:00:32, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
O E2    10.0.0.0 [110/20] via 136.1.111.11, 00:08:09, Ethernet0/0

R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
```

```
       P - periodic downloaded static route

Gateway of last resort is not set

     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/1] via 136.1.23.2, 00:00:01, Serial1/3
C       136.1.23.0 is directly connected, Serial1/3
R       136.1.111.0 [120/1] via 136.1.113.11, 00:00:07, Ethernet0/0
C       136.1.100.0 is directly connected, Ethernet0/1
C       136.1.113.0 is directly connected, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/1] via 136.1.23.2, 00:00:01, Serial1/3
```



VPN3k GUI:

Monitor connected sessions:

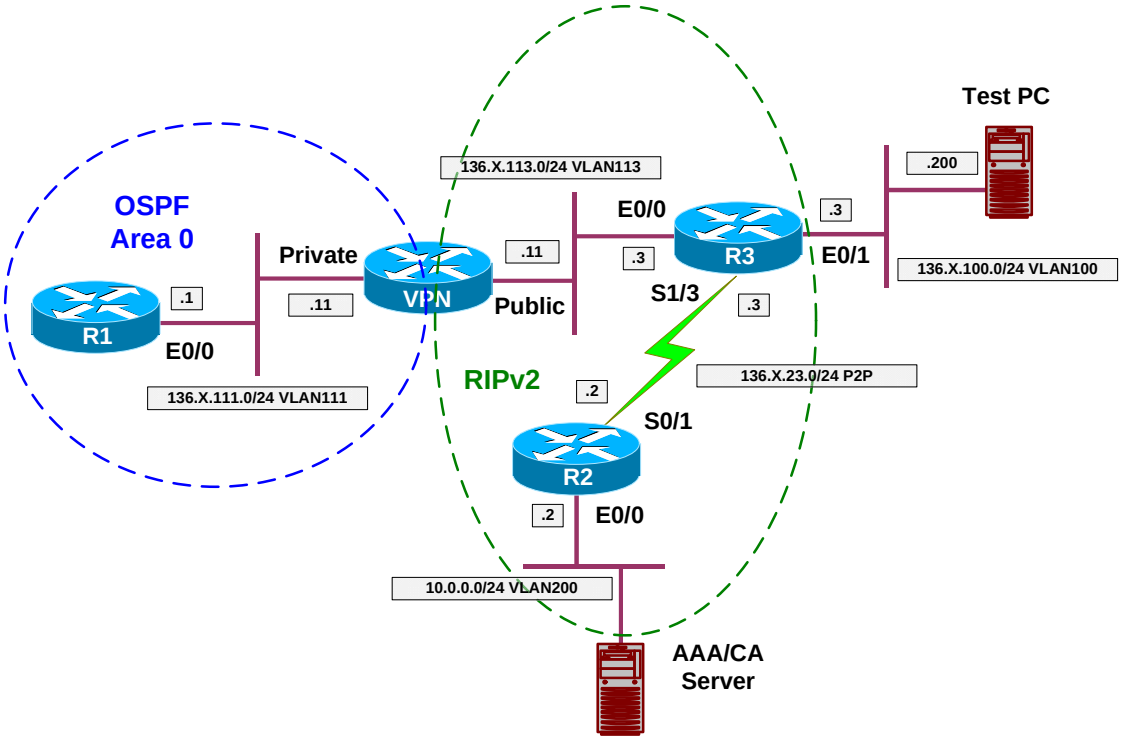


Further Reading

How to Populate Dynamic Routes Using Reverse Route Injection

VPN3k and Cisco VPN Client with DHCP Server

Objective: Configure VPN3k to allocate addresses from DHCP server.



Directions

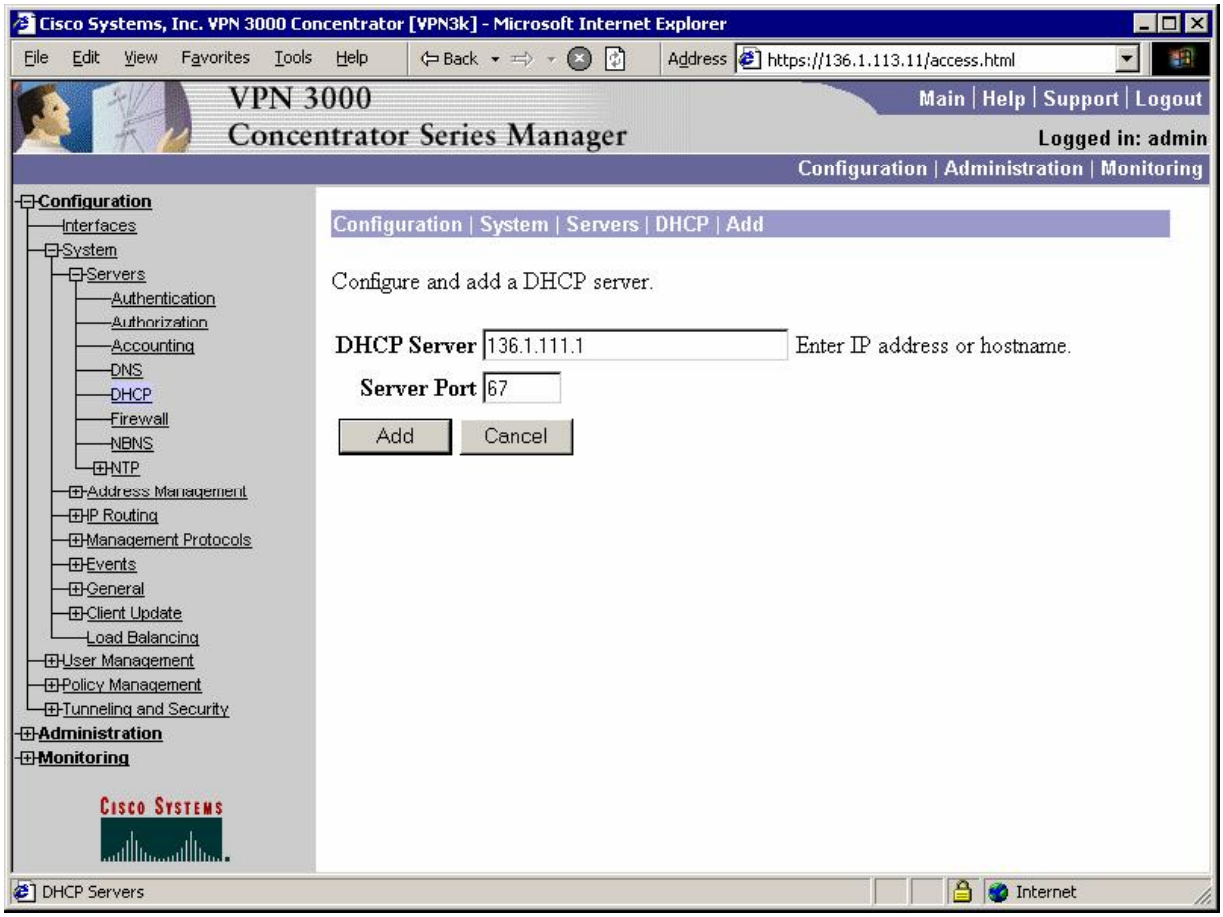
- Configure devices as per the scenario "VPN/ezVPN" "VPN3k and Cisco VPN Client with RRI".
- VPN3k could allocate client IPs using external DHCP server, acting as DHCP client itself (proxing).
- Do not confuse this with DHCP Relay feature, where VPN3k transparenty passes the DHCP requests from Public interface.
- Configure DHCP pool EZVPN on R1 as follows:
    - Use address pool 20.0.0.0/24
    - Configure static route for 20.0.0.0/24 to 136.1.111.11
    - The latter route is required since VPN3k proxies the DHCP request, sending it from IP address in network 20.0.0.0.
- Configure VPN3k to permit address allocation via DHCP
- Configure VPN3k to disable adderss allocation via Address Pools.
- Configure DHCP server 136.1.111.1 on the VPN3k.
- Configure DHCP network scope 20.0.0.0 under group EZVPN "General" Tab.

Final Configuration

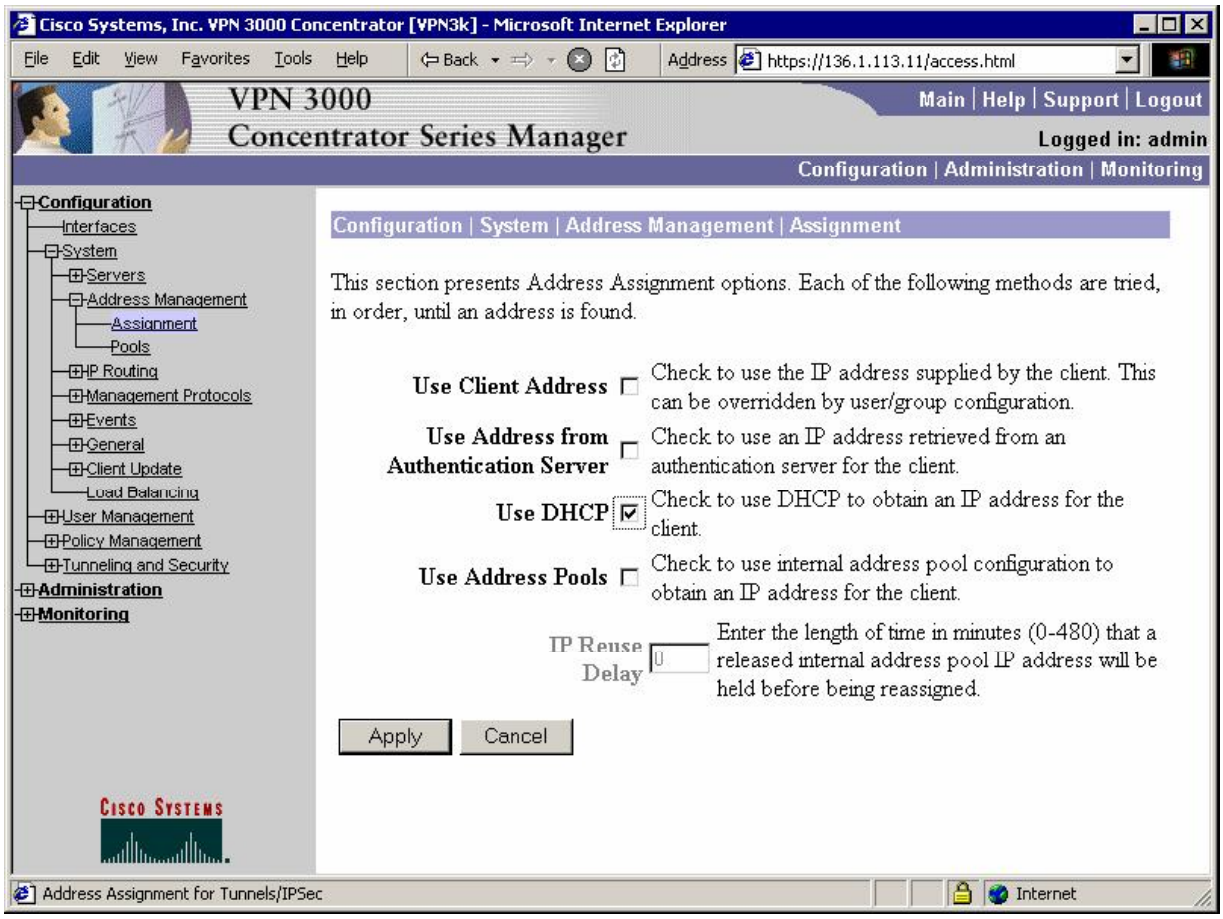
```
R1:
ip dhcp pool EZVPN
   network 20.0.0.0 /24
!
ip route 20.0.0.0 255.255.255.0 136.1.11.11
```

VPN3k GUI:

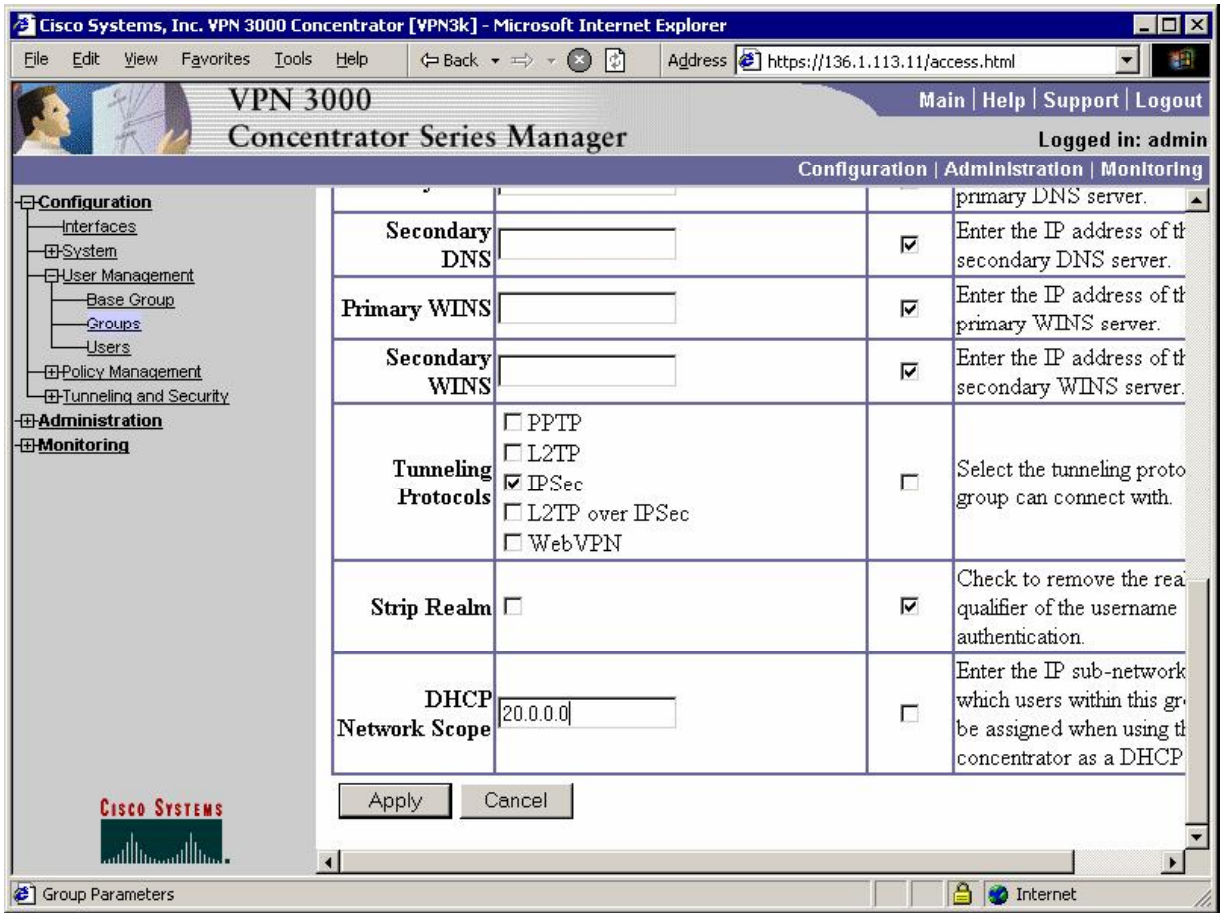
Configure DHCP Server:



Configure Address Allocation via DHCP:



Modify group "EZVPN" settings to use DHCP Network Scope:

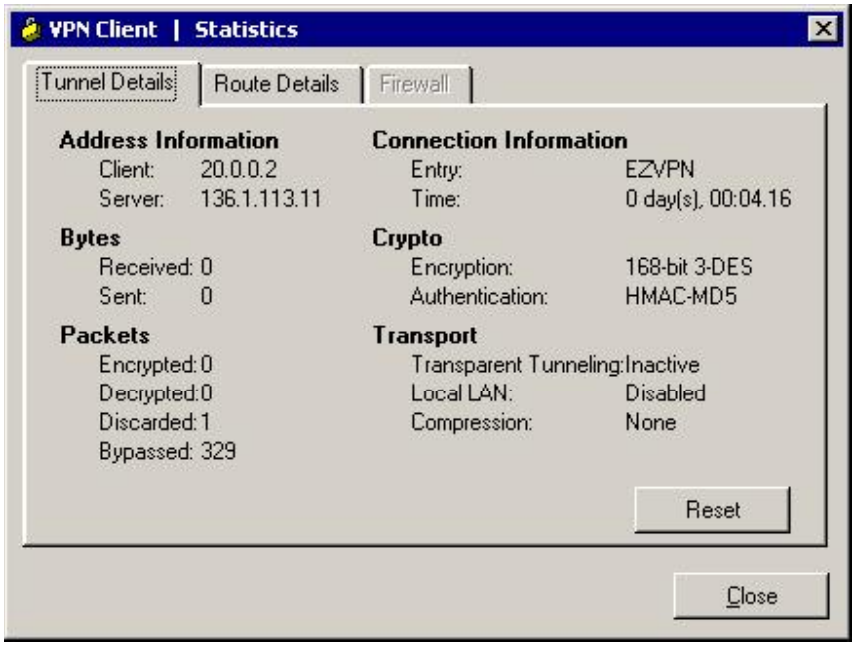


Verification

Connect the VPN Client to VPN3k:

```
R1#debug ip dhcp server events
R1#debug ip dhcp server packet
R1#
*Mar  1 05:18:51.793: DHCPD: assigned IP address 20.0.0.2 to client
0000.03a0.88bd.2900.004b.9447.ad08.df00.
*Mar  1 05:18:51.793: DHCPD: Sending DHCPOFFER to client
0000.03a0.88bd.2900.004b.9447.ad08.df00 (20.0.0.2).
*Mar  1 05:18:51.793: DHCPD: unicasting BOOTREPLY for client 0003.a088.bd29 to
relay 20.0.0.0.
*Mar  1 05:18:51.801: DHCPD: DHCPREQUEST received from client
0000.03a0.88bd.2900.004b.9447.ad08.df00.
*Mar  1 05:18:51.801: DHCPD: Sending DHCPACK to client
0000.03a0.88bd.2900.004b.9447.ad08.df00 (20.0.0.2).
*Mar  1 05:18:51.801: DHCPD: unicasting BOOTREPLY for client 0003.a088.bd29 to
relay 20.0.0.0.
```

Check VPN Client statistics:



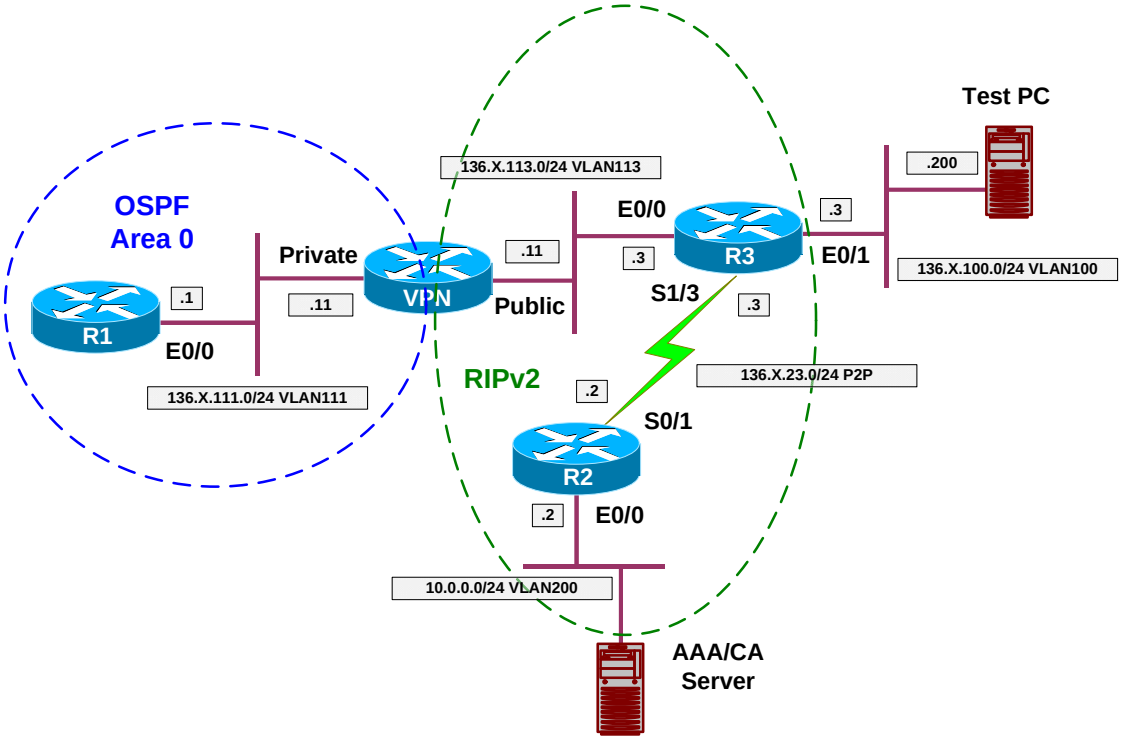

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     136.1.0.0/24 is subnetted, 4 subnets
O E2    136.1.0.0 [110/20] via 136.1.111.11, 01:16:12, Ethernet0/0
O E2    136.1.23.0 [110/20] via 136.1.111.11, 01:16:12, Ethernet0/0
C       136.1.111.0 is directly connected, Ethernet0/0
O E2    136.1.100.0 [110/20] via 136.1.111.11, 01:16:12, Ethernet0/0
     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       20.0.0.0/24 [1/0] via 136.1.111.11
O E2    20.0.0.2/32 [110/20] via 136.1.111.11, 00:04:29, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
O E2    10.0.0.0 [110/20] via 136.1.111.11, 01:16:13, Ethernet0/0

R1#ping 20.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

📖 Further Reading

VPN3k: Configuring DHCP Server

VPN3k and Cisco VPN Client with RADIUS Authentication

Objective: Configure VPN3k for authentication and address allocation via RADIUS.



Directions

- Configure devices as per the scenario "VPN/ezVPN" "VPN3k and Cisco VPN Client with RRI".
- The goal is to authenticate users and allocate addresses using RADIUS server.
- Configure VPN3k to communicate with RADIUS server as follows:
    - First, create two filter rules, to permit outgoing RADIUS traffic IN and OUT.
    - Name these rules "Outgoing RADIUS In" and "Outgoing RADIUS Out".
    - Permit UDP packets from/to port 1645 of host 10.0.0.100.
    - Configure VPN3k to use RADIUS Authentication Server with IP 10.0.0.100.
    - Use key "CISCO" to secure communications.

- Configure ACS server:
    - Add network client for VPN3k as follows:

        - Use IP 136.1.113.11.
        - Use key CISCO.
        - Use RADIUS server type specific for VPN3000.

    - Add user “CISCO” with password “CISCO1234”

        - Configure this user’s profile to allocate static IP “20.0.0.1”

- Configure VPN3k as follows:

    - Modify group EZVPN as follows:

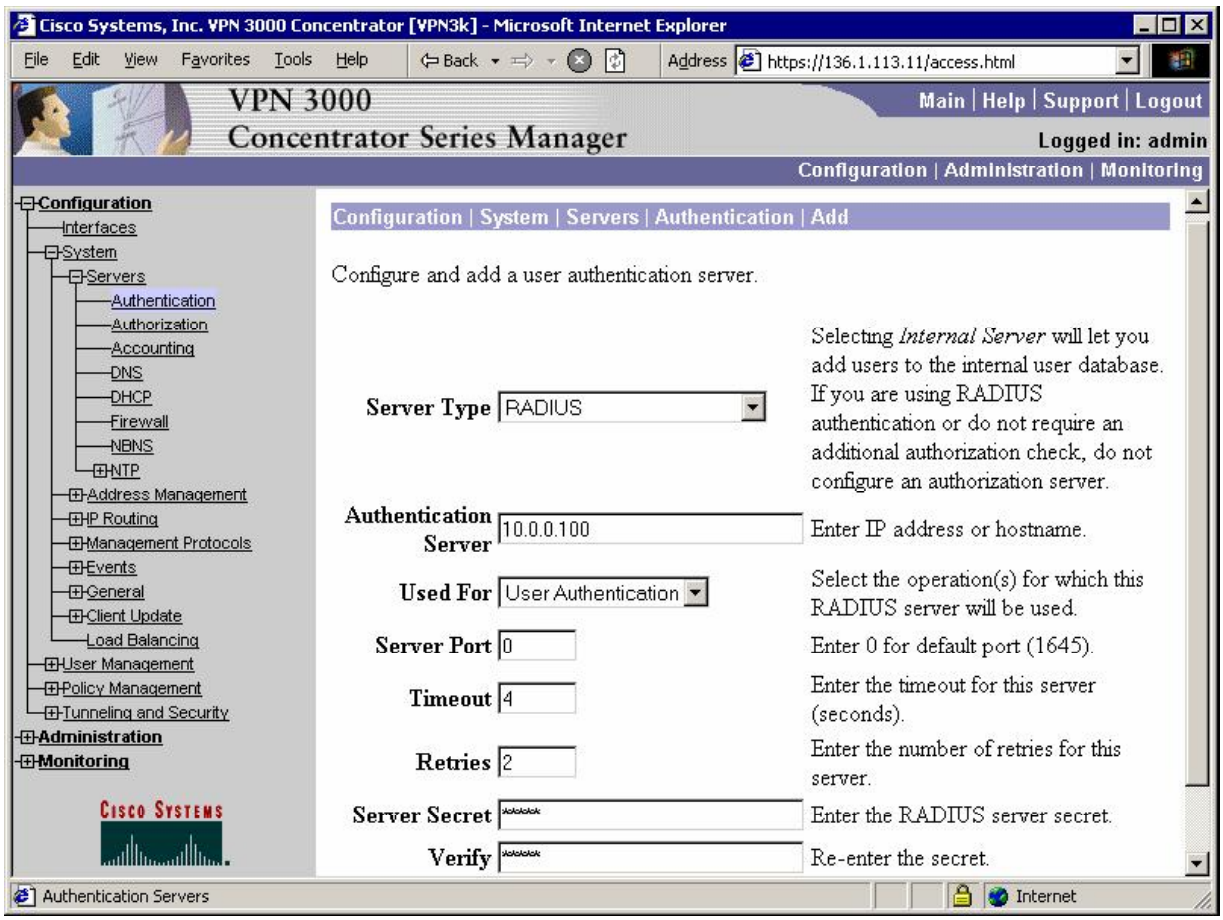
        - With IPsec Tab set authentication to “RADIUS”.

    - Modify address allocation policy, permitting address allocation by Authentication Server.

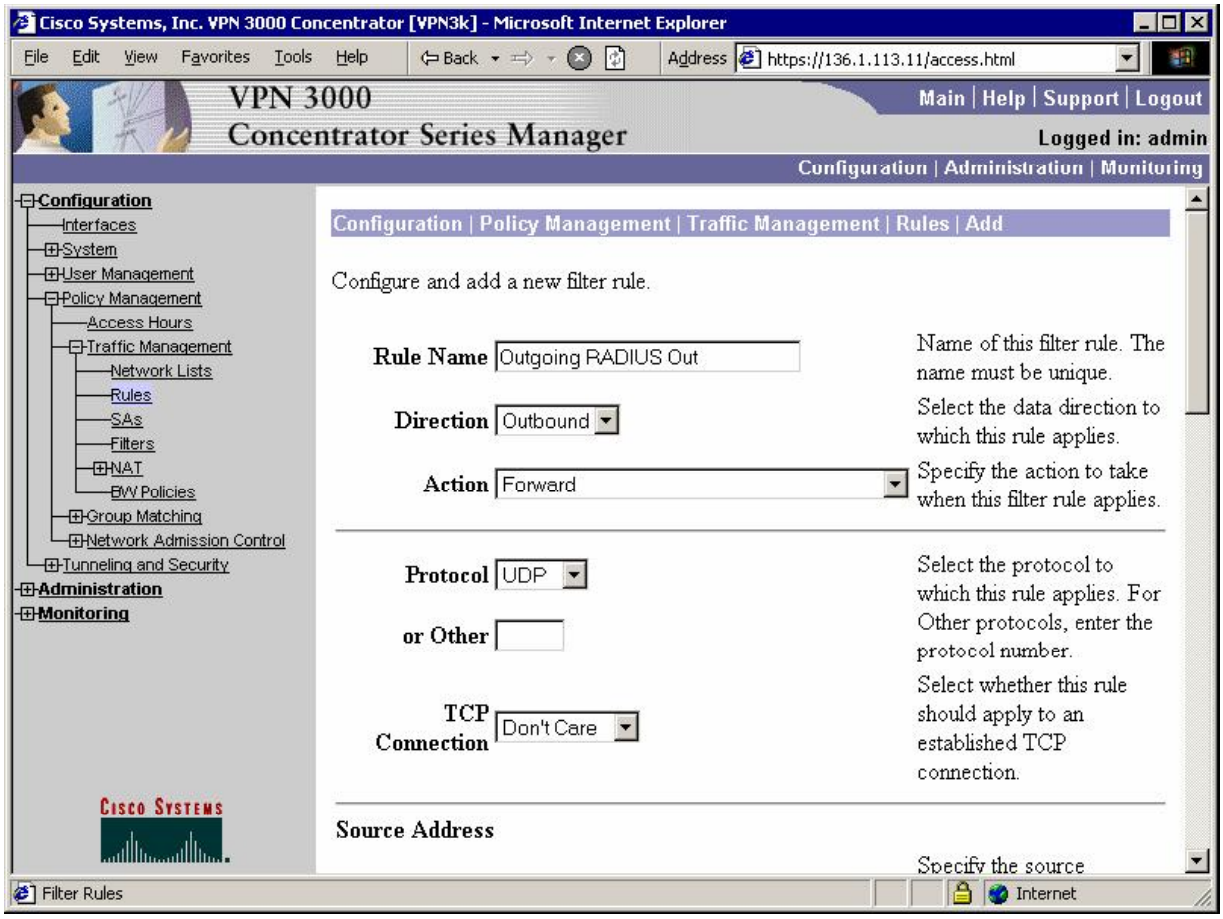
Final Configuration

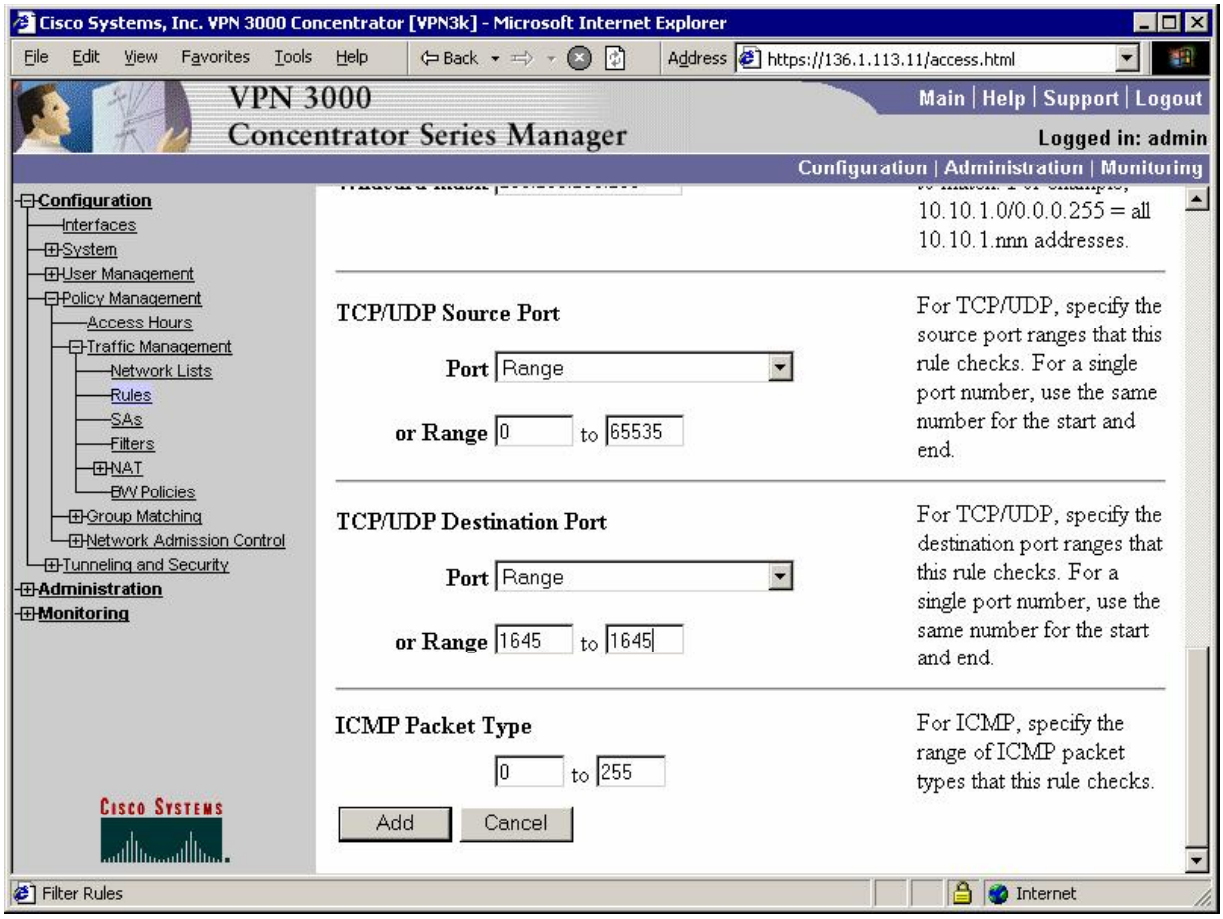
VPN3k GUI:

Configure RADIUS Authentication Server:

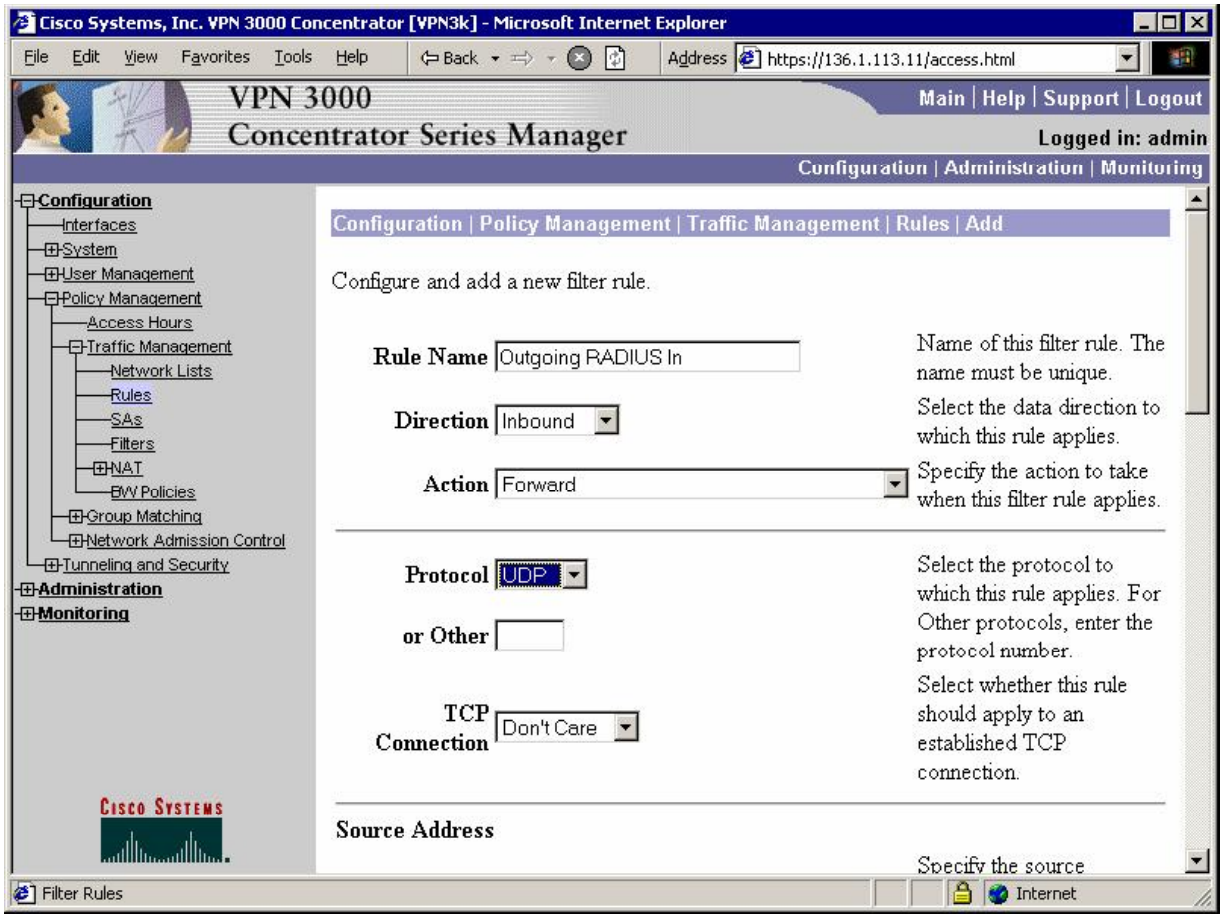


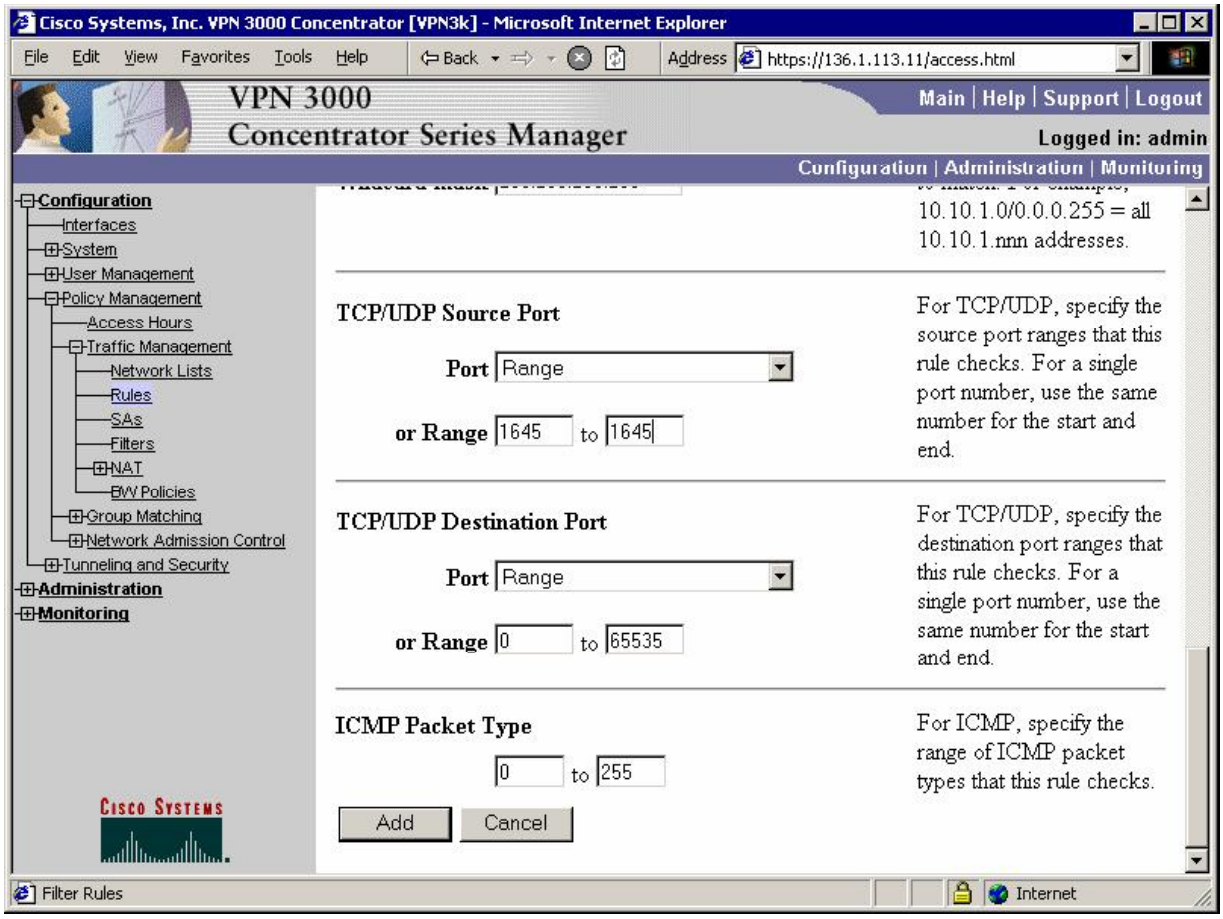
Configure Rule for Outgoing RADIUS traffic Out:


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Configuration | Policy Management | Traffic Management | Rules | Add
Configure and add a new filter rule.
Rule Name
Outgoing RADIUS Out
Name of this filter rule. The name must be unique.
Direction
Outbound
Select the data direction to which this rule applies.
Action
Forward
Specify the action to take when this filter rule applies.
Protocol
UDP
or Other
Select the protocol to which this rule applies. For Other protocols, enter the protocol number.
TCP Connection
Don't Care
Select whether this rule should apply to an established TCP connection.
Source Address
Filter Rules
Internet



Configure Rule for Outgoing RADIUS traffic In:

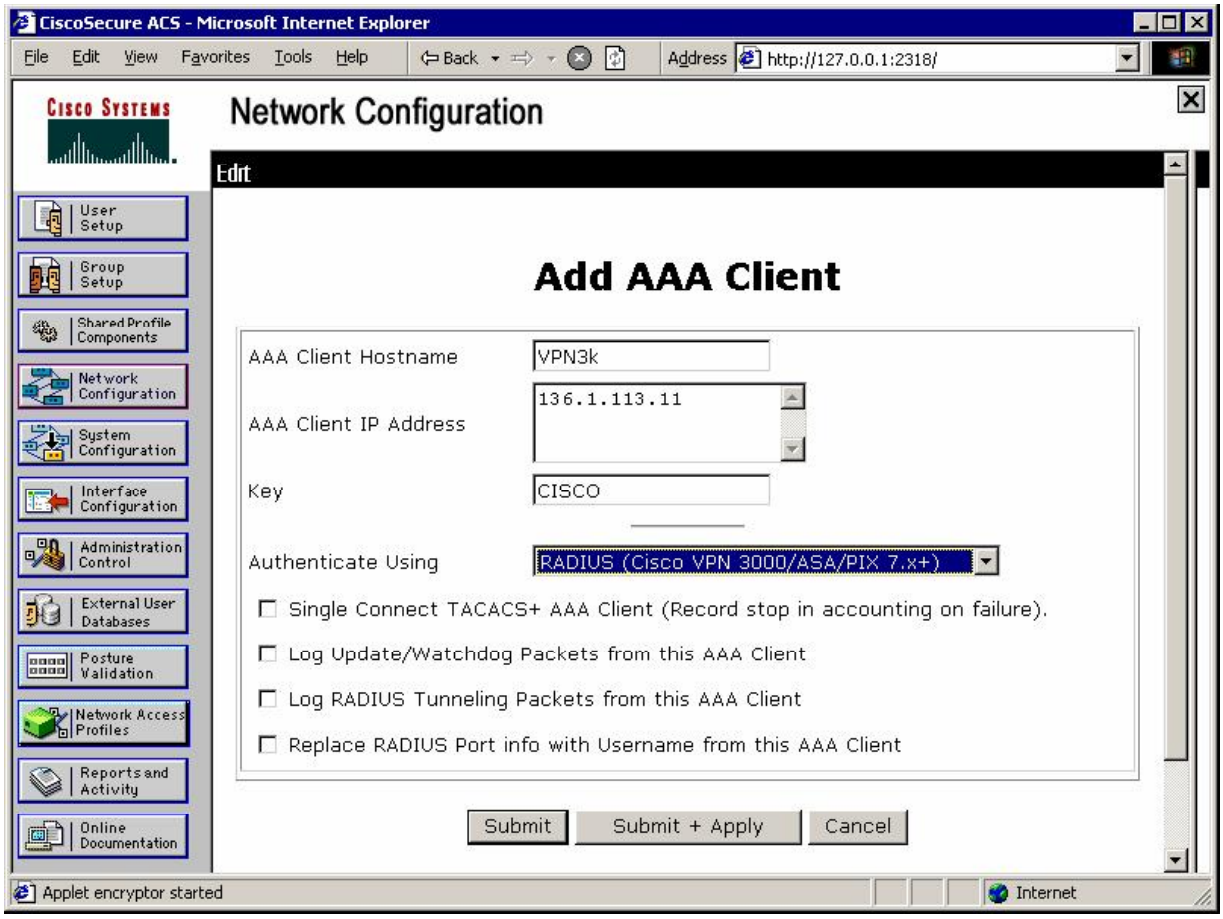

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Configuration | Policy Management | Traffic Management | Rules | Add
Configure and add a new filter rule.
Rule Name
Outgoing RADIUS In
Name of this filter rule. The name must be unique.
Direction
Inbound
Select the data direction to which this rule applies.
Action
Forward
Specify the action to take when this filter rule applies.
Protocol
UDP
or Other
Select the protocol to which this rule applies. For Other protocols, enter the protocol number.
TCP Connection
Don't Care
Select whether this rule should apply to an established TCP connection.
Source Address
Filter Rules
Internet


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
TCP/UDP Source Port
Port Range
or Range 1645 to 1645
For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.
TCP/UDP Destination Port
Port Range
or Range 0 to 65535
For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.
ICMP Packet Type
0 to 255
For ICMP, specify the range of ICMP packet types that this rule checks.
Add
Cancel
Cisco Systems
Filter Rules
Internet

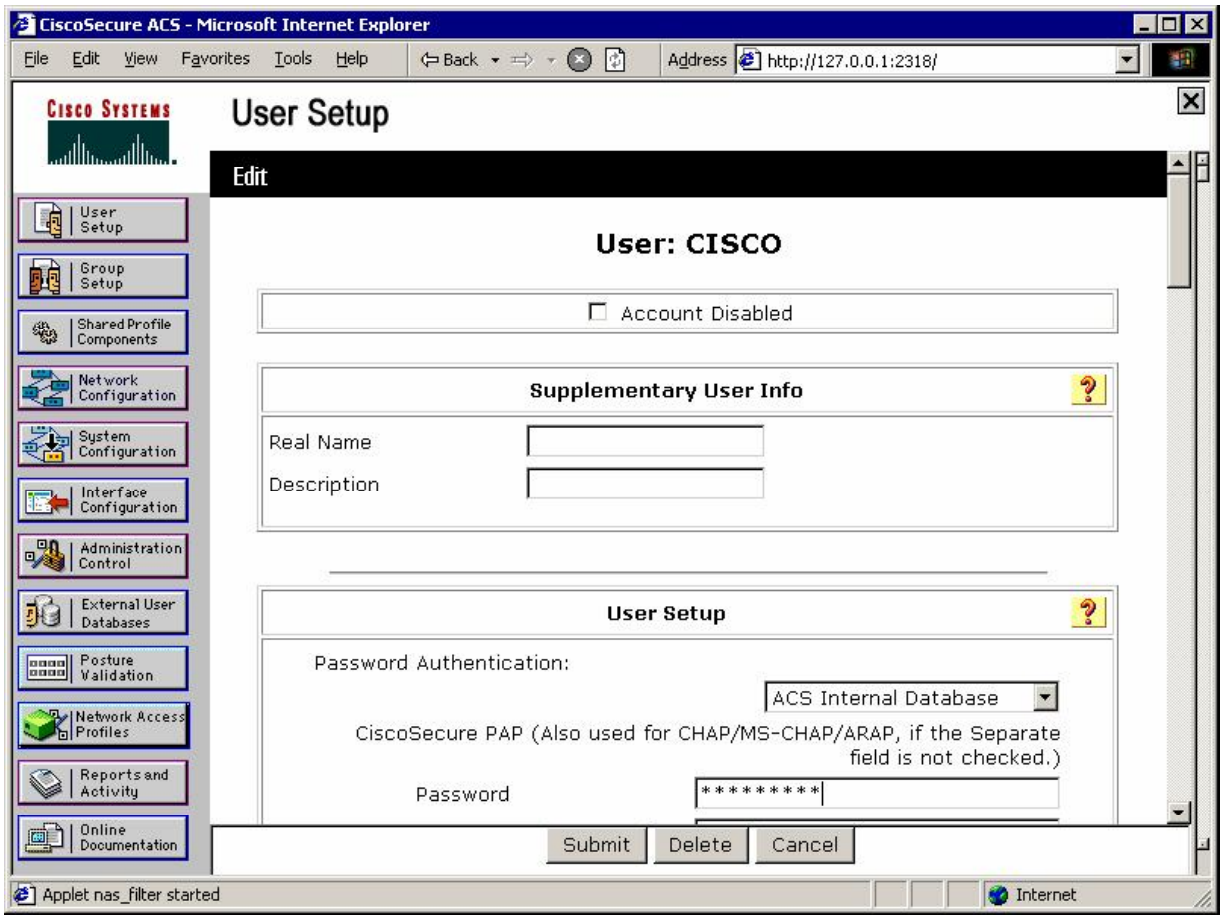
Assign both rules to the Public filter:

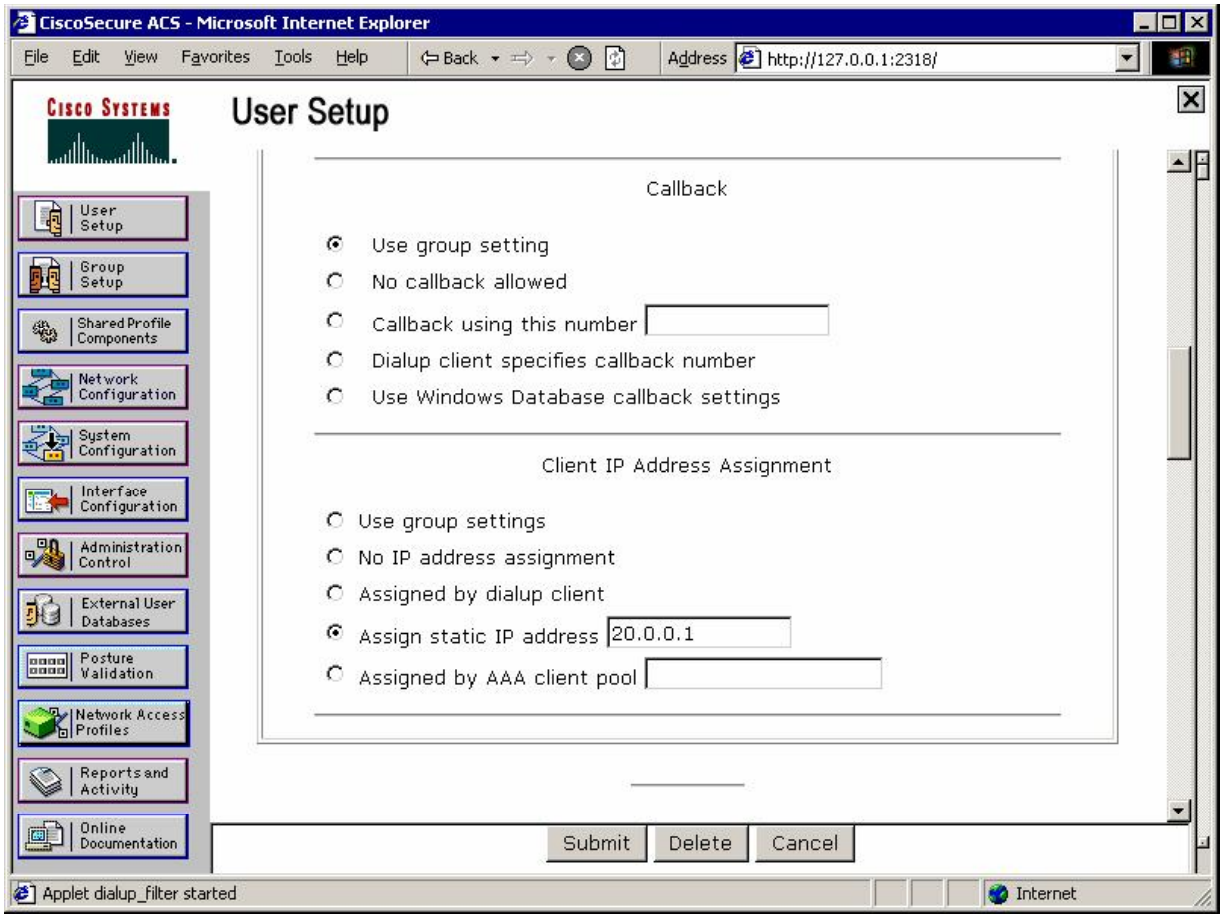

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Filter Name: Public (Default)
Select an Available Rule and click Add to apply it to this filter.
Select a Current Rule in Filter and click Remove, Move Up, Move Down, or Assign SA to Rule as appropriate.
Select an Available Rule, then select a Current Rule in Filter, and click Insert Above to add the available rule above the current rule.
Current Rules in Filter
Actions
Available R
NAT-T In (forward/in)
RIP In (forward/in)
Outgoing RADIUS In (forward/in)
GRE Out (forward/out)
IKE Out (forward/out)
PPTP Out (forward/out)
L2TP Out (forward/out)
ICMP Out (forward/out)
VRRP Out (forward/out)
NAT-T Out (forward/out)
RIP Out (forward/out)
Outgoing RADIUS Out (forward/out)
<< Add
<< Insert Above
Remove >>
Move Up
Move Down
Assign SA to Rule
Done
OSPF In (forward/in)
OSPF Out (forward/out)
Incoming HTTP In (forv
Incoming HTTP Out (fo
Any In (forward/in)
Any Out (forward/out)
Incoming HTTPS In (fo
Incoming HTTPS Out (
LDAP In (forward/in)
LDAP Out (forward/out)
Telnet/SSL In (forward/
Telnet/SSL Out (forwar
Cisco Systems
Filter Policies
Internet

Configure ACS Server – Add VPN3k as network client:

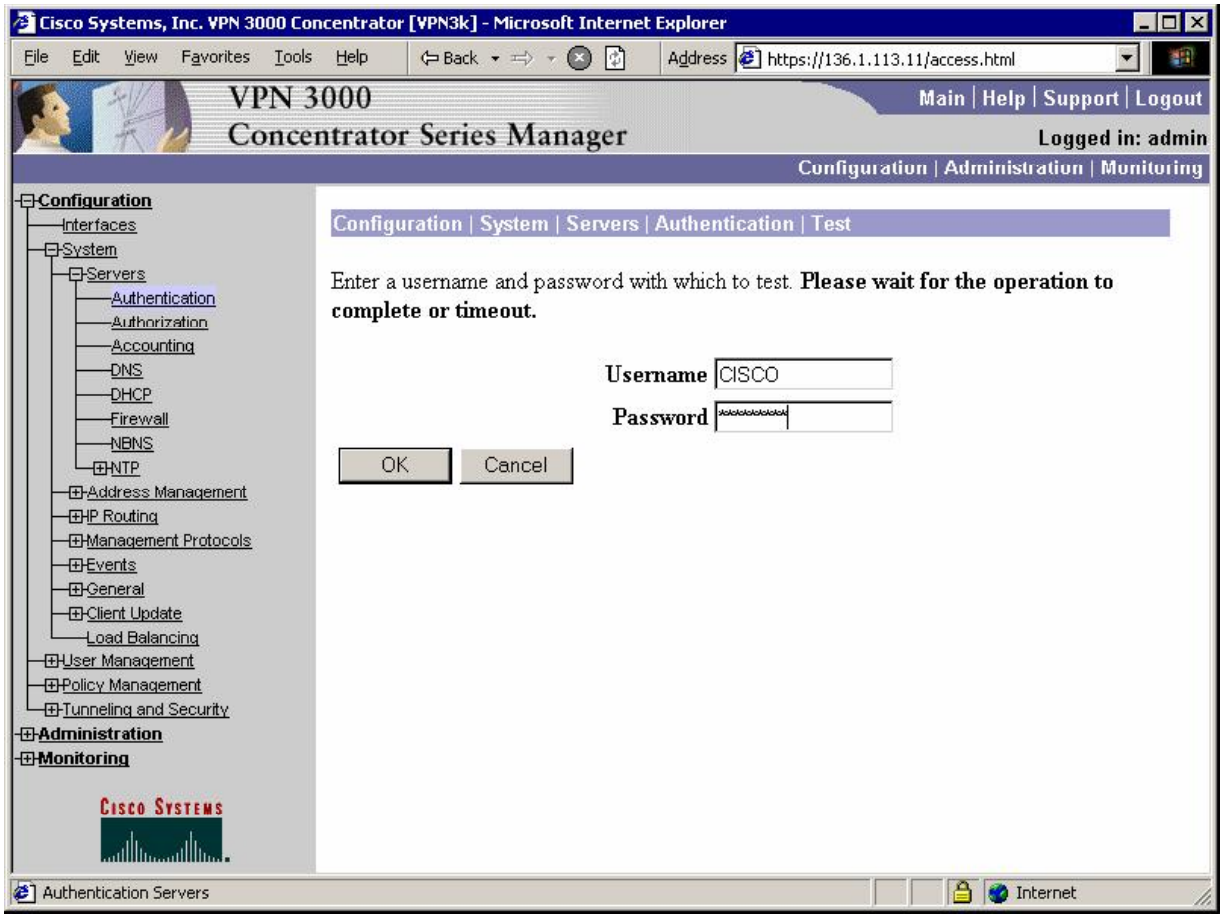


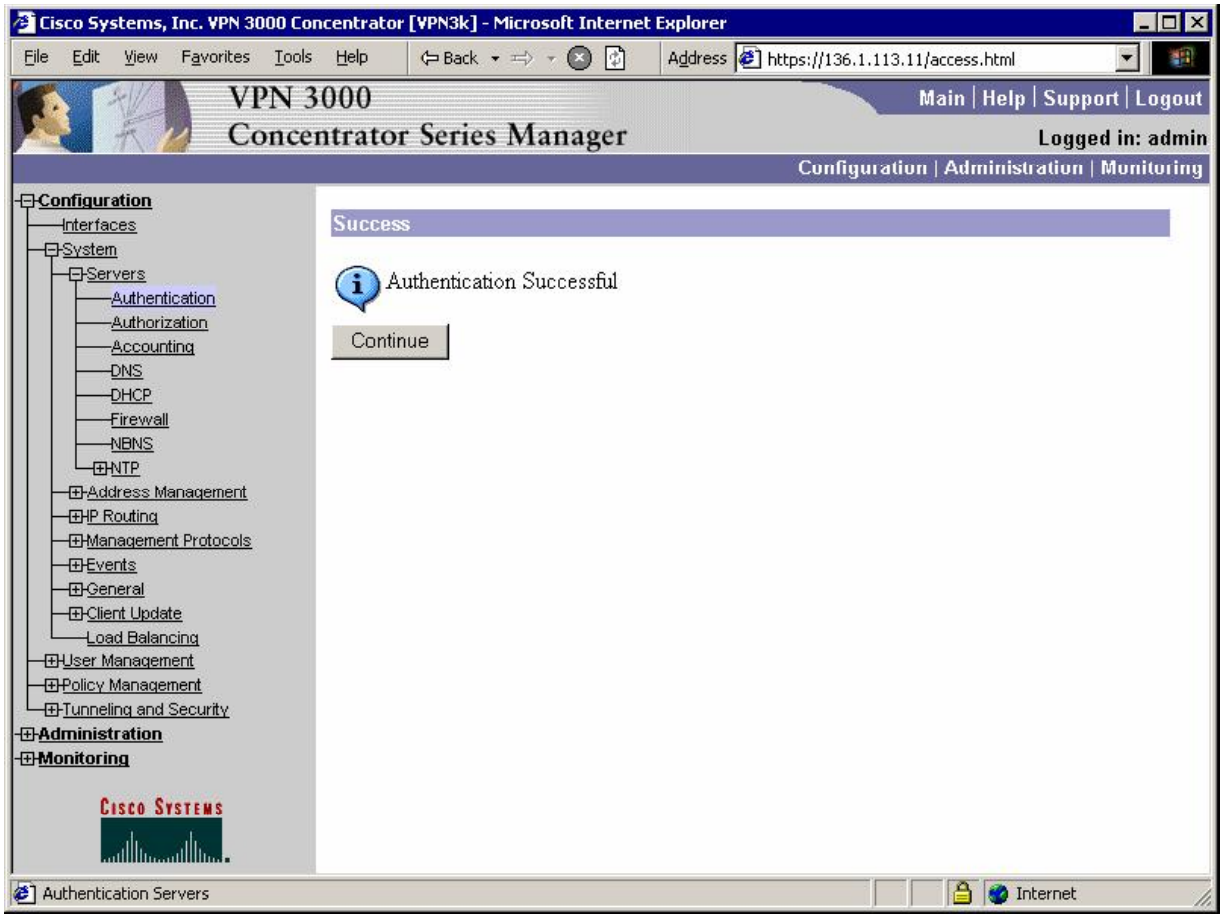
Create user CISCO with password CISCO1234 and configure address allocation:



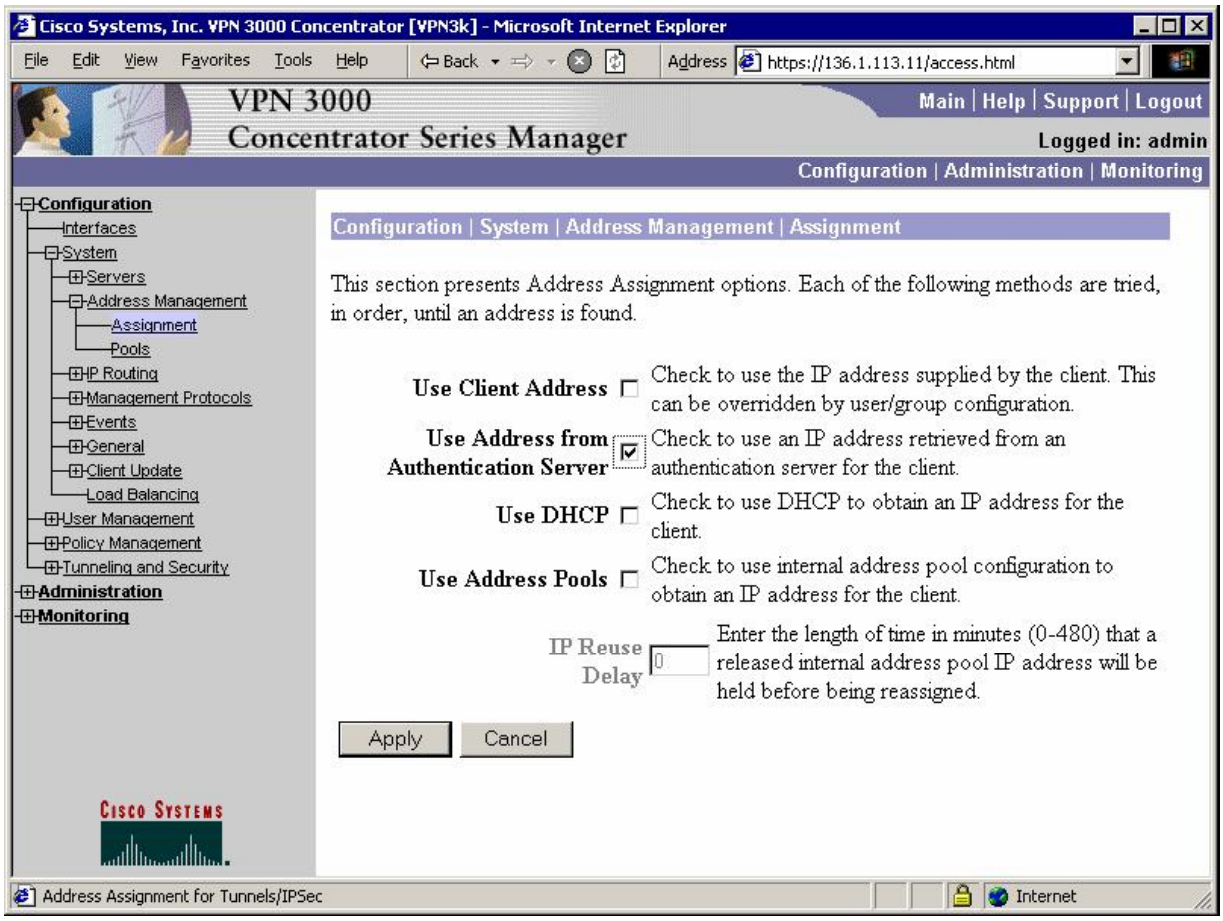

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:2318/
Cisco Systems
User Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Callback
Use group setting
No callback allowed
Callback using this number
Dialup client specifies callback number
Use Windows Database callback settings
Client IP Address Assignment
Use group settings
No IP address assignment
Assigned by dialup client
Assign static IP address
20.0.0.1
Assigned by AAA client pool
Submit
Delete
Cancel
Applet dialup_filter started
Internet

Test AAA server on VPN3k:

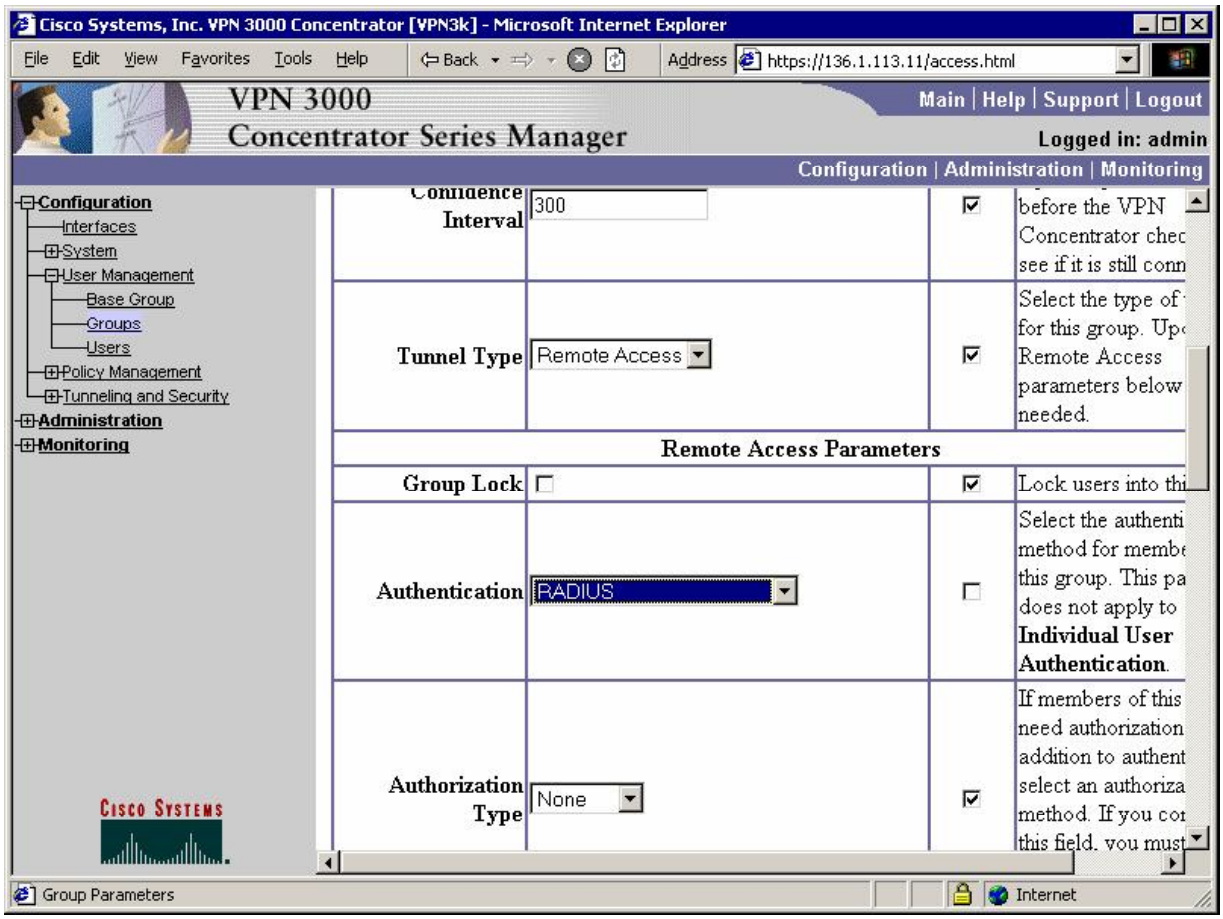



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Authentication
Authorization
Accounting
DNS
DHCP
Firewall
NBNS
NTP
Address Management
IP Routing
Management Protocols
Events
General
Client Update
Load Balancing
User Management
Policy Management
Tunneling and Security
Administration
Monitoring
Cisco Systems
Success
Authentication Successful
Continue
Authentication Servers
Internet

Configure Address allocation by Authentication Server:

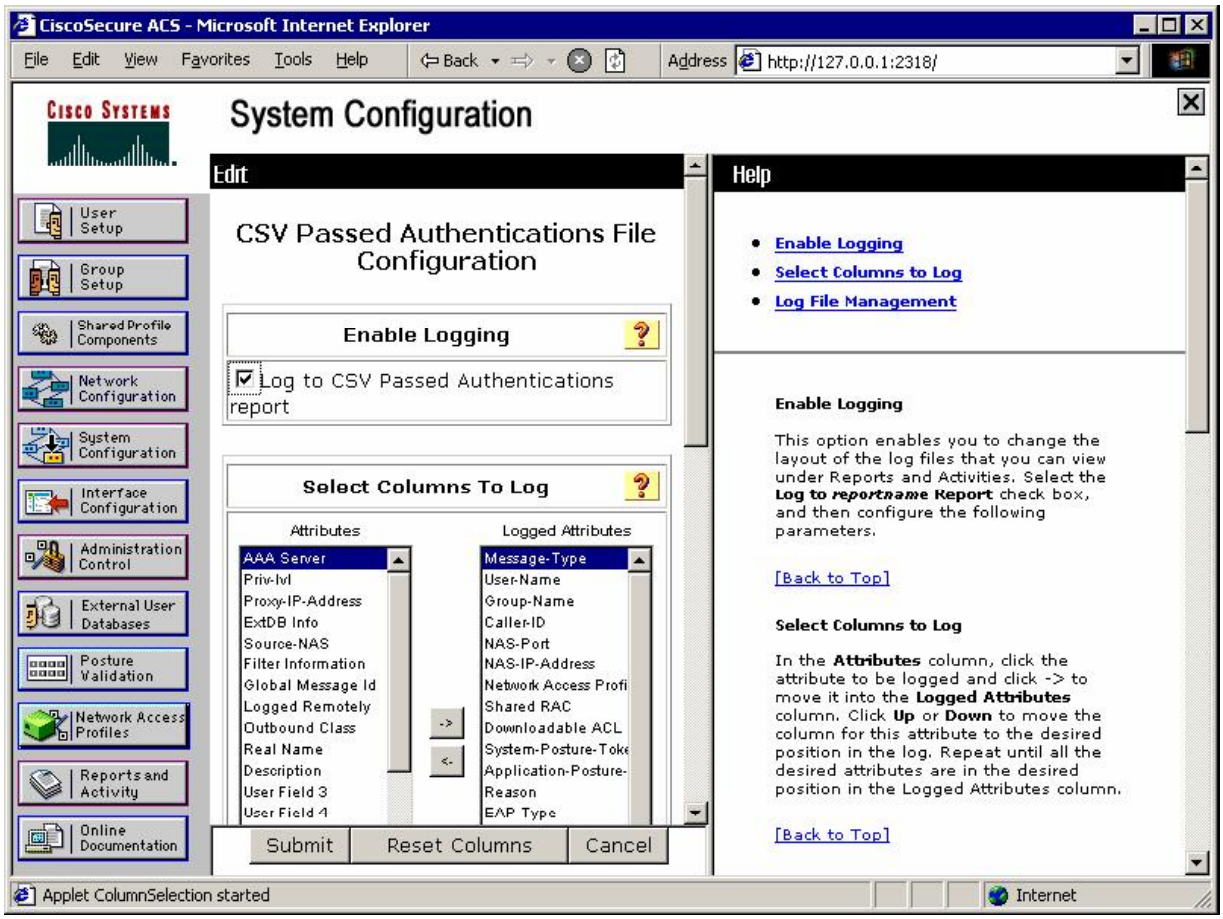


Configure group EZVPN to authenticate users via RADIUS:

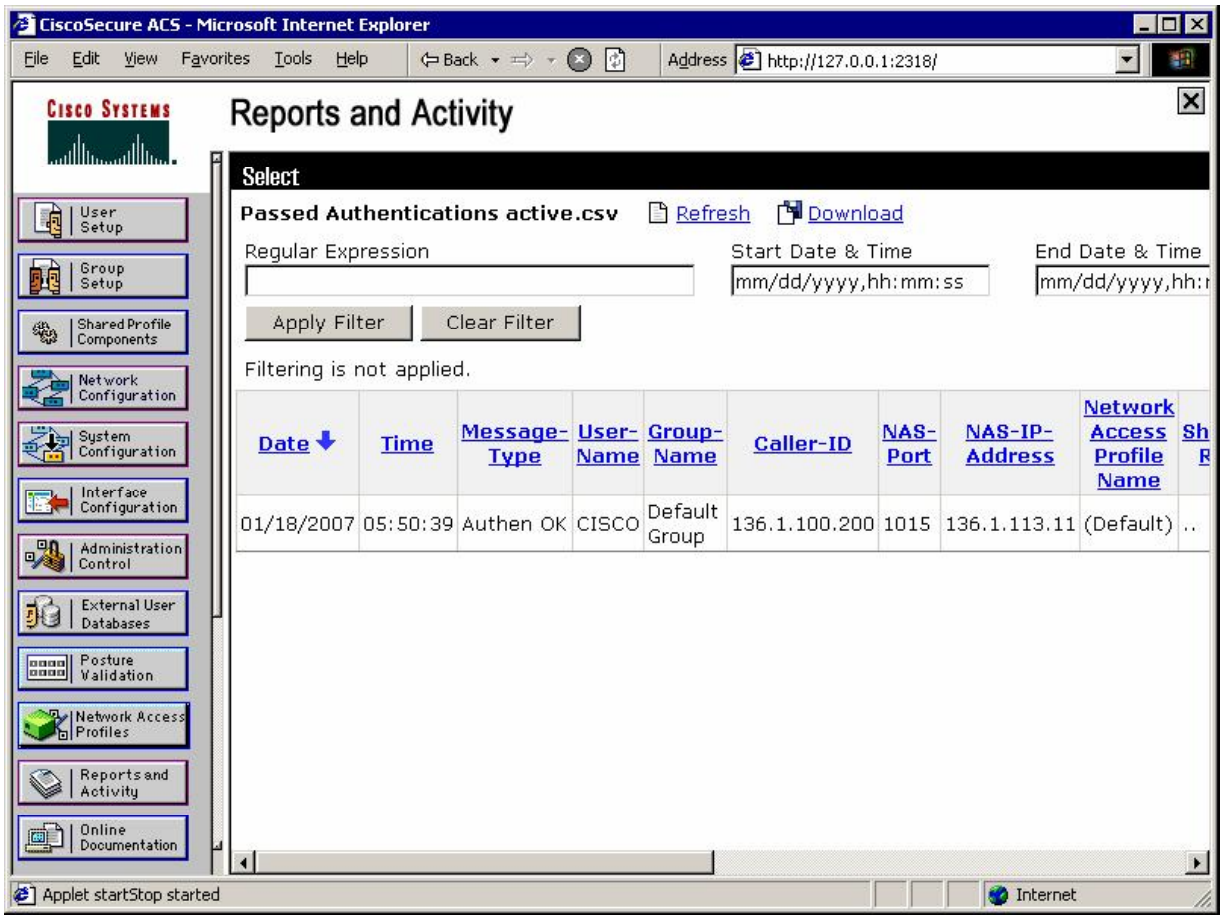


Verification

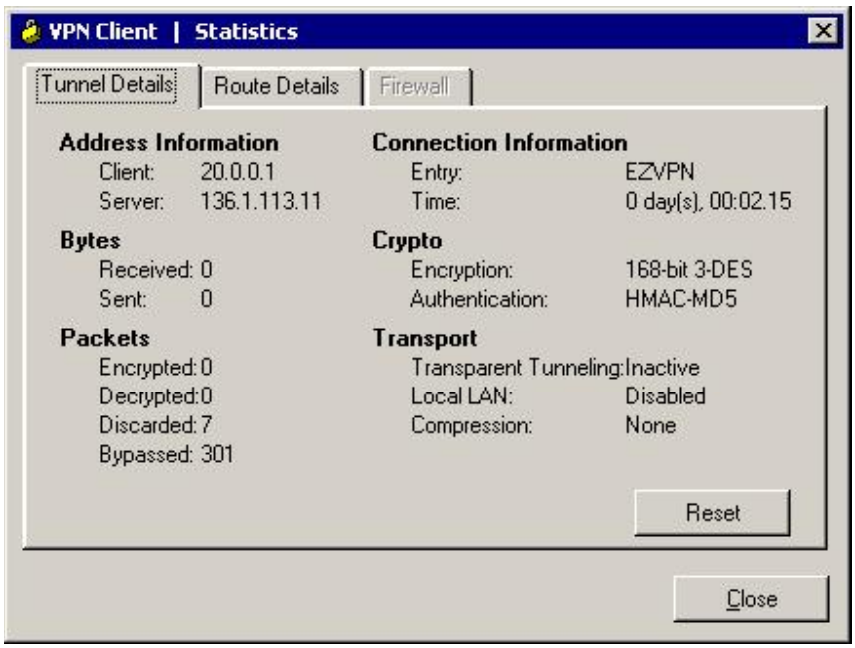
Enable logging of passed authentications under System Configuration on ACS:



Connect Cisco VPN Client and check Passed Authentications on ACS:



Check Client Statistics:



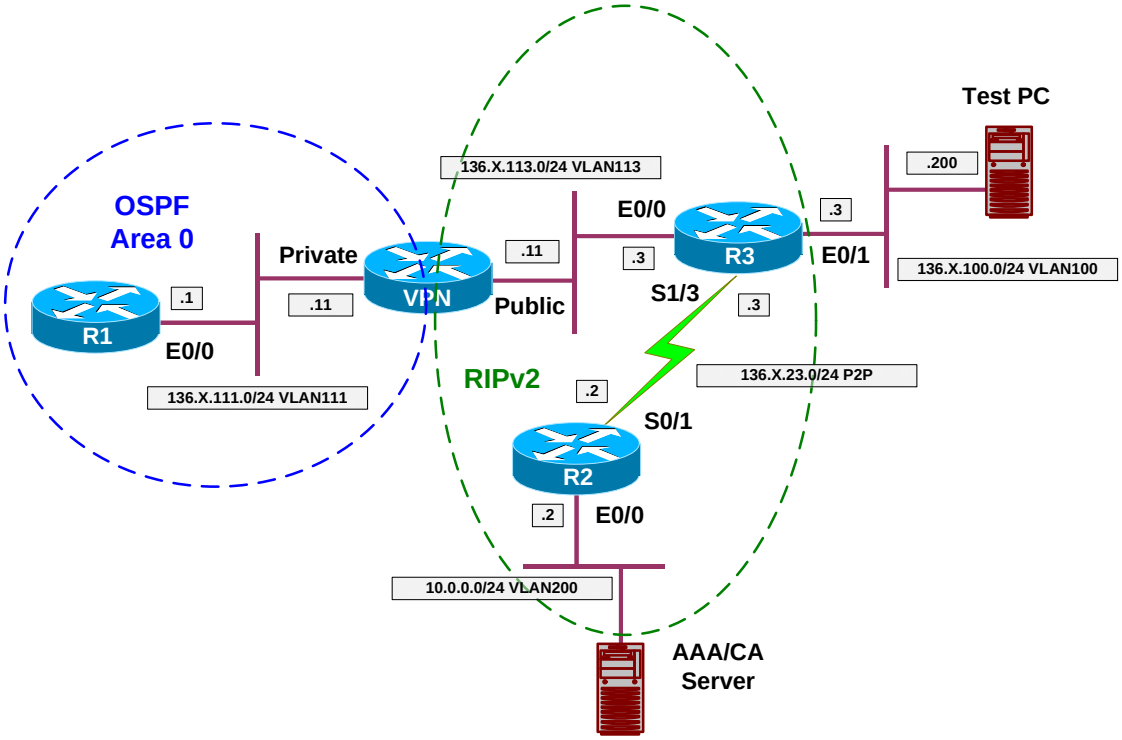

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     136.1.0.0/24 is subnetted, 4 subnets
O E2    136.1.0.0 [110/20] via 136.1.111.11, 02:06:12, Ethernet0/0
O E2    136.1.23.0 [110/20] via 136.1.111.11, 02:06:12, Ethernet0/0
C       136.1.111.0 is directly connected, Ethernet0/0
O E2    136.1.100.0 [110/20] via 136.1.111.11, 02:06:12, Ethernet0/0
     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       20.0.0.0/24 [1/0] via 136.1.111.11
O E2    20.0.0.1/32 [110/20] via 136.1.111.11, 00:03:20, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
O E2    10.0.0.0 [110/20] via 136.1.111.11, 02:06:13, Ethernet0/0

R1#ping 20.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/10/32 ms
```

Further Reading

Using Cisco Secure ACS for Windows with the VPN 3000 Concentrator - IPSec

VPN3k and Cisco VPN Client with External Group

Objective: Configure VPN3k to authenticate and apply attributes receieved for external group via RADIUS.



Directions

- Configure devices as per the scenario "VPN/ezVPN" "VPN3k and Cisco VPN Client with RADIUS Authentication".
- VPN3000 has capability of downloading all group attributes from RADIUS server.
- When you configure a group on VPN3000, you specify it as a "external" one, and configue a group password. This password will be used to authenticate against the RADIUS server.
- Take the previously configured group "EZVPN" and configure it as external.
- On the RADIUS server you need first to enable certain RADIUS attributes, used for group configuration. At least, these should be attributes to specify user's authentication.
- Configure ACS Interface, and activate these RADIUS attributes.
- Create group EZVPN and configure the following VPN3000 attributes:

    - Tunneling-Protocols = "IPsec".
    - IPsec-Authentication = "RADIUS".

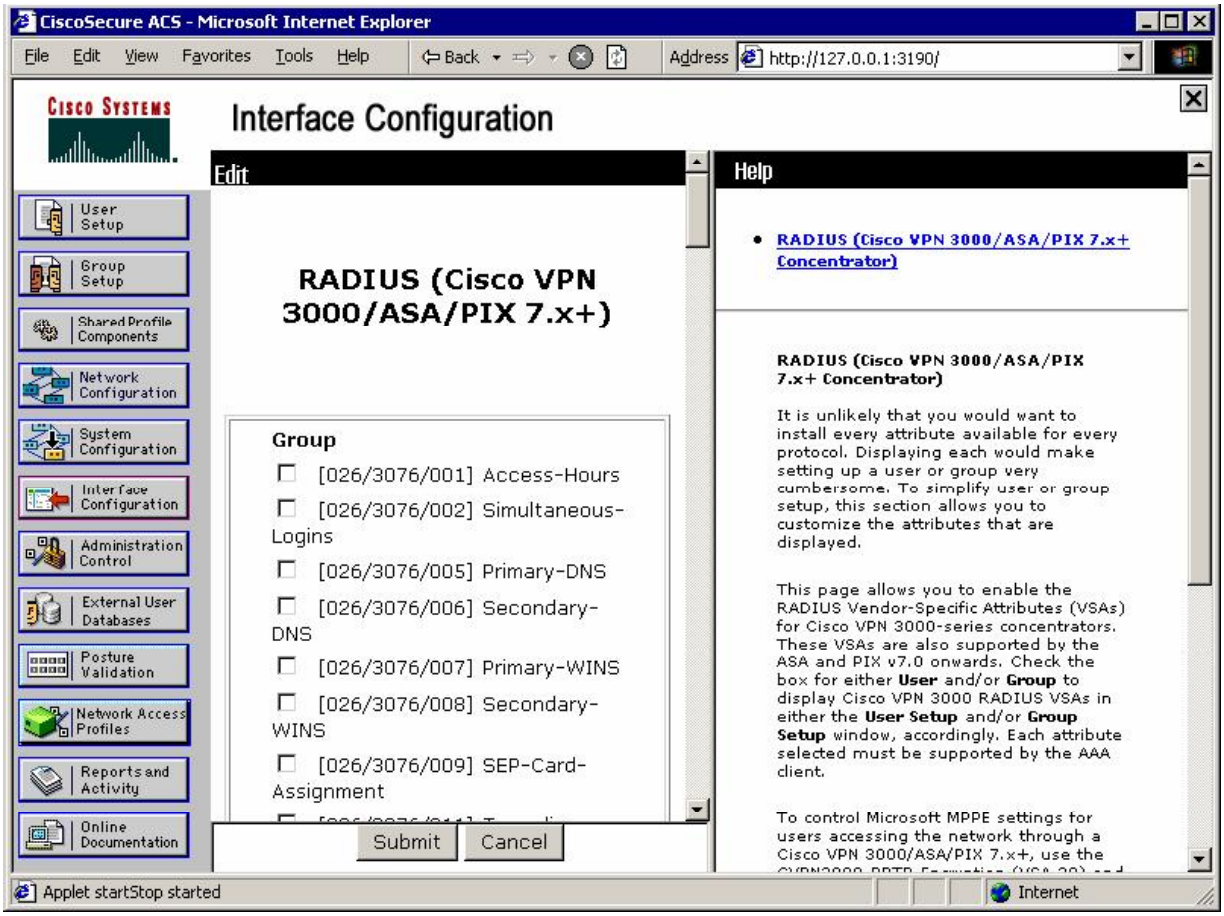
- o Split-Tunneling-Policy = “Only Tunnel networks in the List”.
- o Split-Tunneling-List = “SPLIT_TUNNEL”.

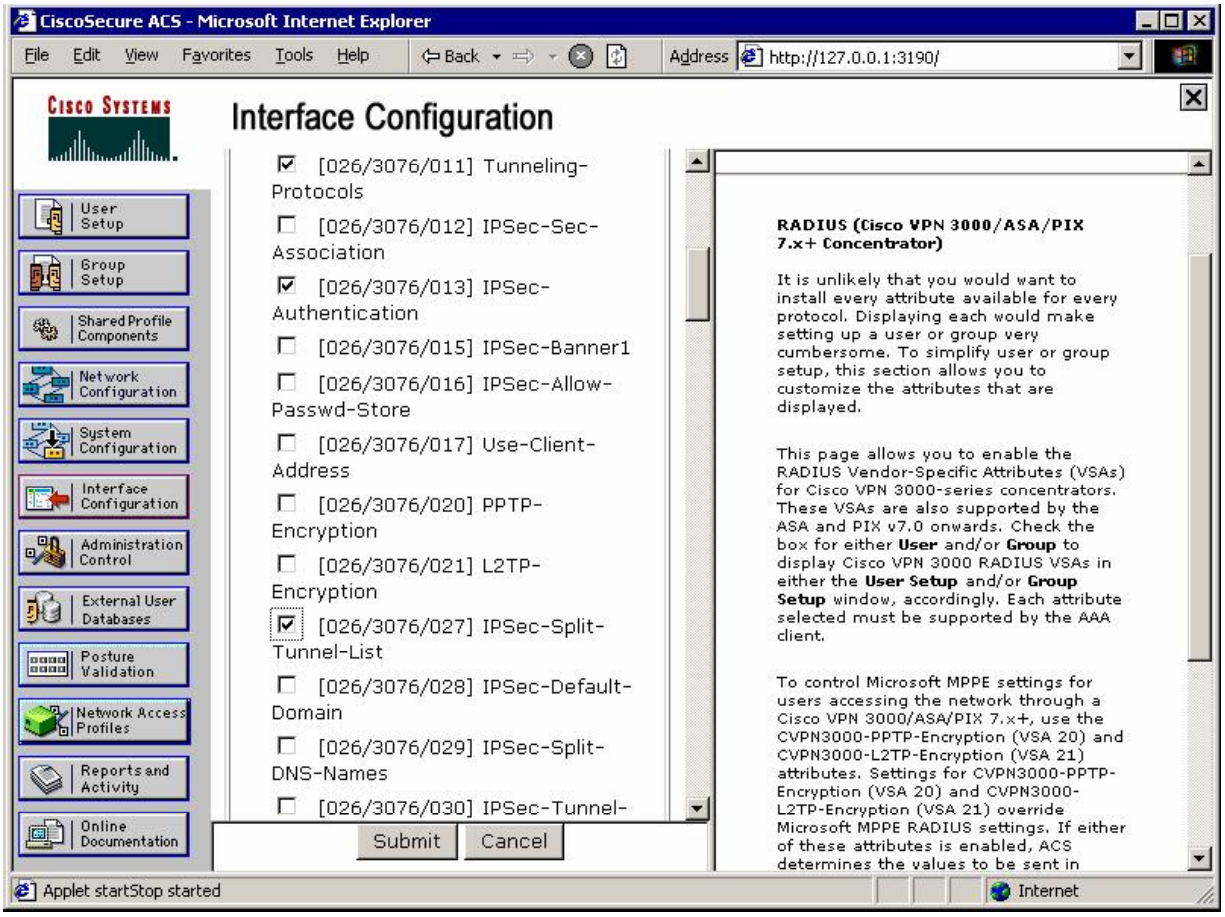
- On the RADIUS server you need to create a user with a name matching the group name. Create user named EZVPN with password “CISCO”.
- Assign this use to group EZVPN.
- On the VPN3000 you should have RADIUS server already configured for authentication. It will be used to download group attributes as well.

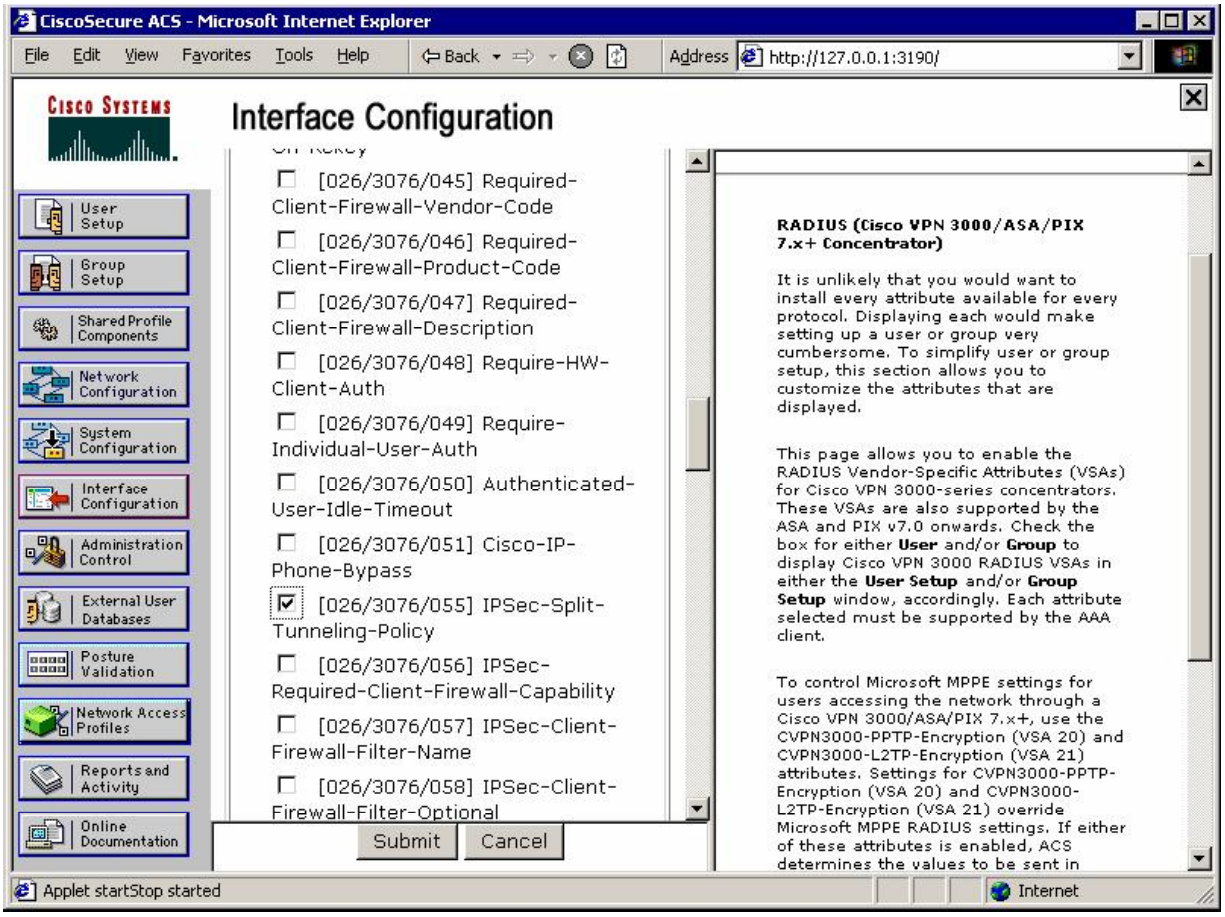
Final Configuration

ACS:

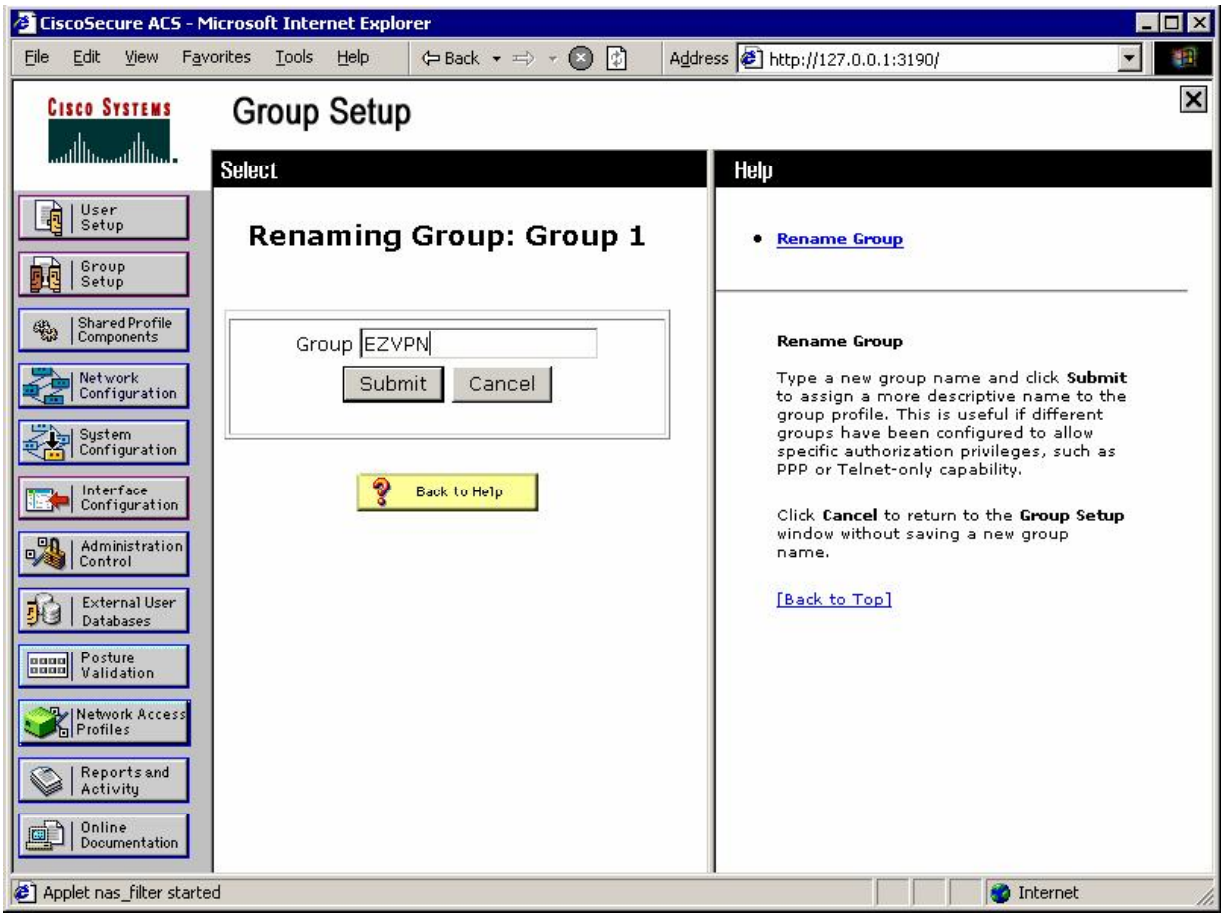
Enable VPN3000 RADIUS attributes under Interface Configuration:



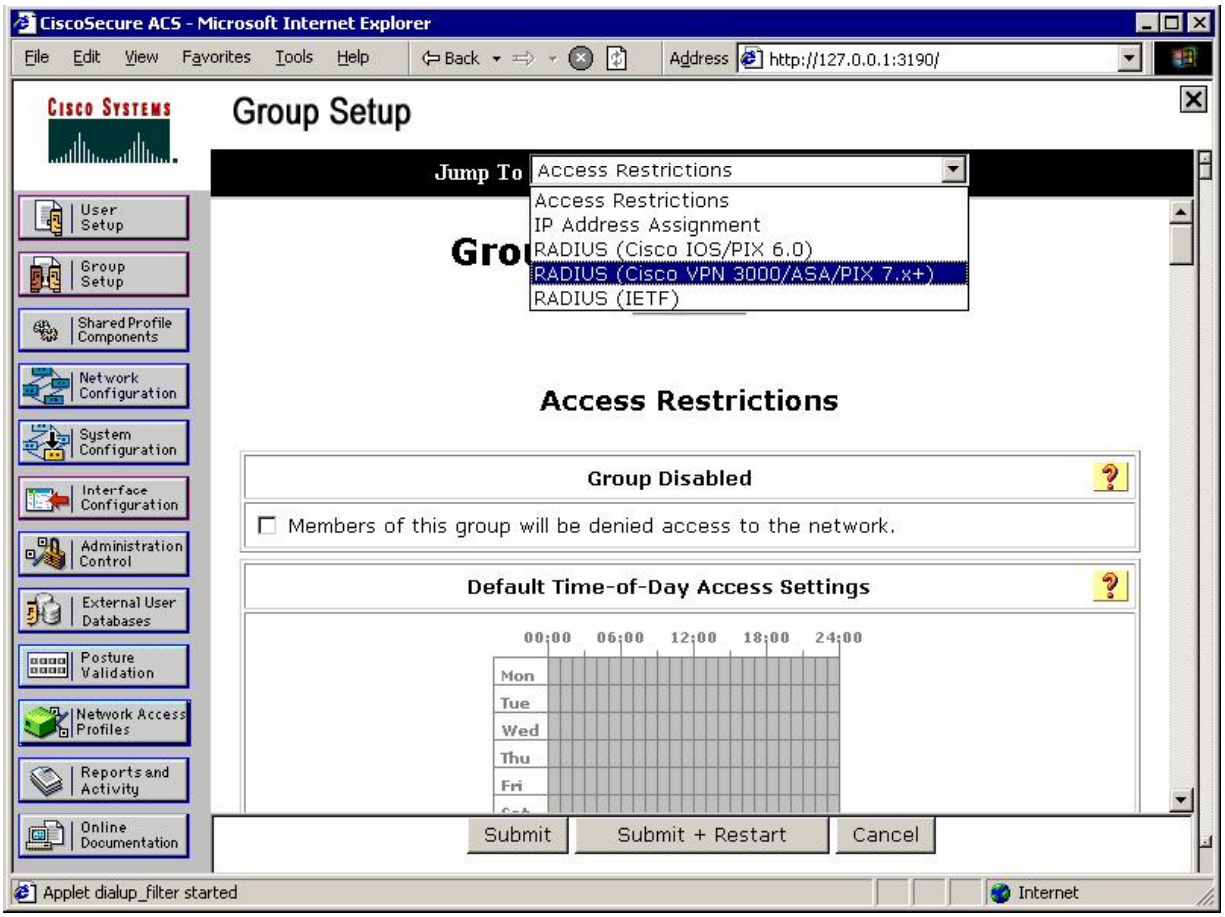

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:3190/
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
[026/3076/011] Tunneling-Protocols
[026/3076/012] IPSec-Sec-Association
[026/3076/013] IPSec-Authentication
[026/3076/015] IPSec-Banner1
[026/3076/016] IPSec-Allow-Passwd-Store
[026/3076/017] Use-Client-Address
[026/3076/020] PPTP-Encryption
[026/3076/021] L2TP-Encryption
[026/3076/027] IPSec-Split-Tunnel-List
[026/3076/028] IPSec-Default-Domain
[026/3076/029] IPSec-Split-DNS-Names
[026/3076/030] IPSec-Tunnel-
Submit
Cancel
RADIUS (Cisco VPN 3000/ASA/PIX 7.x+ Concentrator)
It is unlikely that you would want to install every attribute available for every protocol. Displaying each would make setting up a user or group very cumbersome. To simplify user or group setup, this section allows you to customize the attributes that are displayed.
This page allows you to enable the RADIUS Vendor-Specific Attributes (VSAs) for Cisco VPN 3000-series concentrators. These VSAs are also supported by the ASA and PIX v7.0 onwards. Check the box for either User and/or Group to display Cisco VPN 3000 RADIUS VSAs in either the User Setup and/or Group Setup window, accordingly. Each attribute selected must be supported by the AAA client.
To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000/ASA/PIX 7.x+, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in
Applet startStop started
Internet

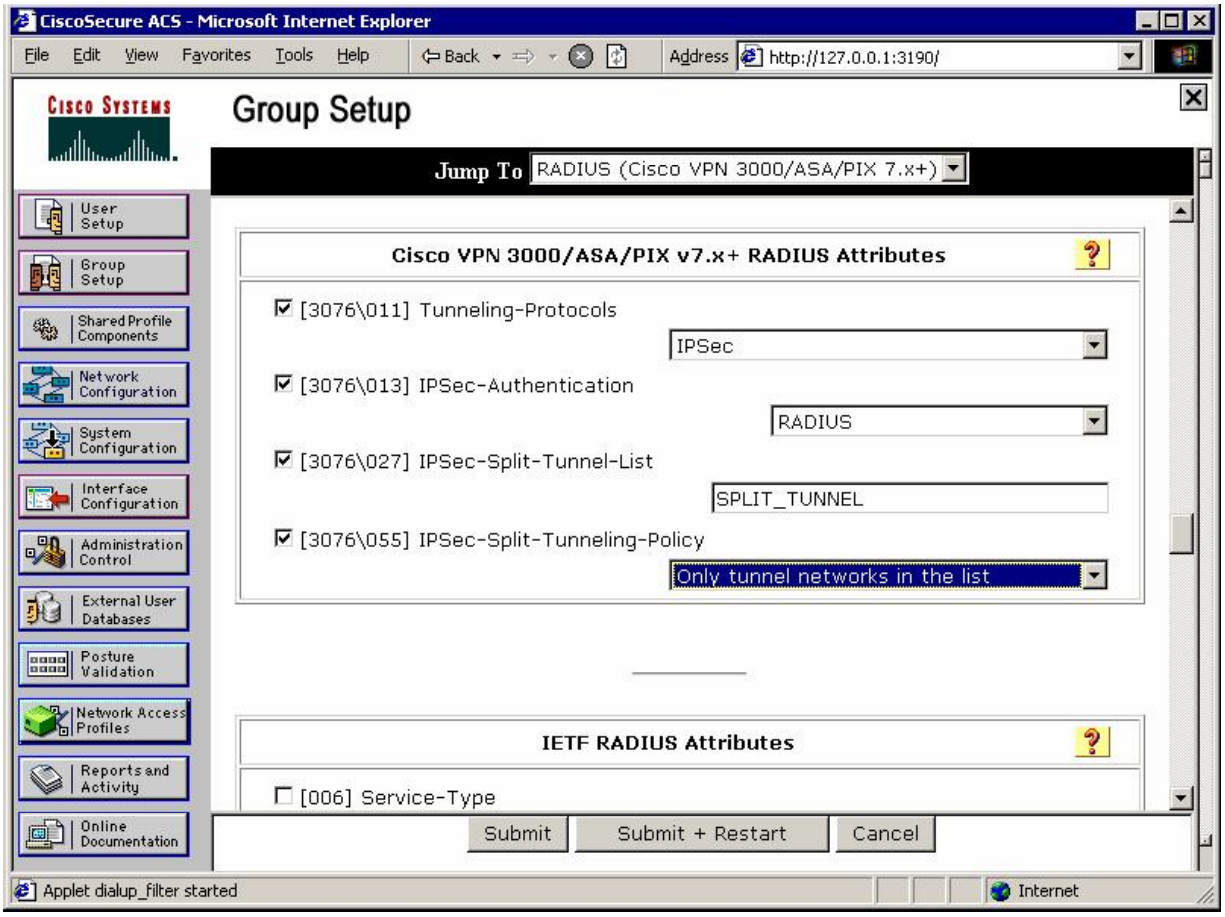

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:3190/
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
[026/3076/045] Required-Client-Firewall-Vendor-Code
[026/3076/046] Required-Client-Firewall-Product-Code
[026/3076/047] Required-Client-Firewall-Description
[026/3076/048] Require-HW-Client-Auth
[026/3076/049] Require-Individual-User-Auth
[026/3076/050] Authenticated-User-Idle-Timeout
[026/3076/051] Cisco-IP-Phone-Bypass
[026/3076/055] IPSec-Split-Tunneling-Policy
[026/3076/056] IPSec-Required-Client-Firewall-Capability
[026/3076/057] IPSec-Client-Firewall-Filter-Name
[026/3076/058] IPSec-Client-Firewall-Filter-Optional
Submit
Cancel
RADIUS (Cisco VPN 3000/ASA/PIX 7.x+ Concentrator)
It is unlikely that you would want to install every attribute available for every protocol. Displaying each would make setting up a user or group very cumbersome. To simplify user or group setup, this section allows you to customize the attributes that are displayed.
This page allows you to enable the RADIUS Vendor-Specific Attributes (VSAs) for Cisco VPN 3000-series concentrators. These VSAs are also supported by the ASA and PIX v7.0 onwards. Check the box for either User and/or Group to display Cisco VPN 3000 RADIUS VSAs in either the User Setup and/or Group Setup window, accordingly. Each attribute selected must be supported by the AAA client.
To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000/ASA/PIX 7.x+, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in
Applet startStop started
Internet

Create group EZVPN:

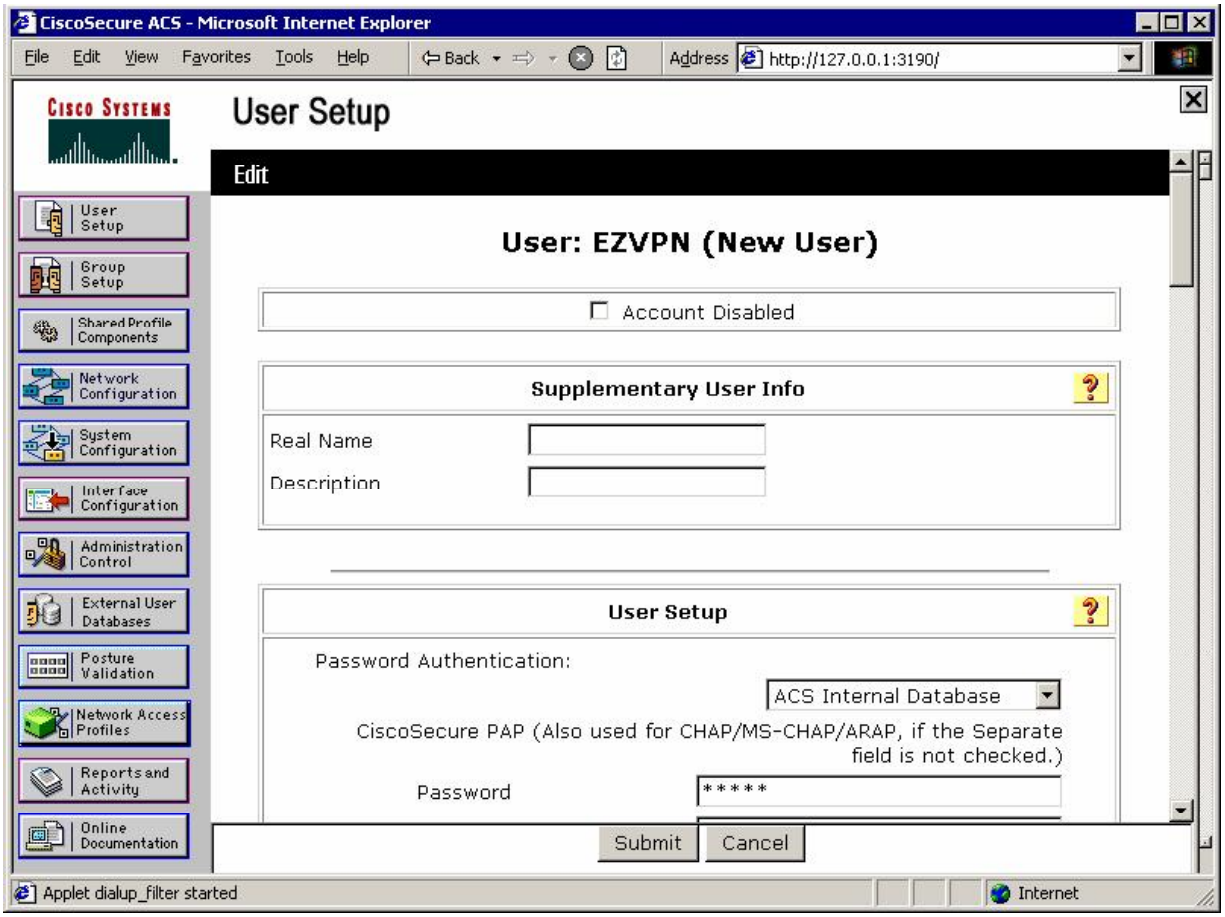


Set values for VPN3000 RADIUS attributes:

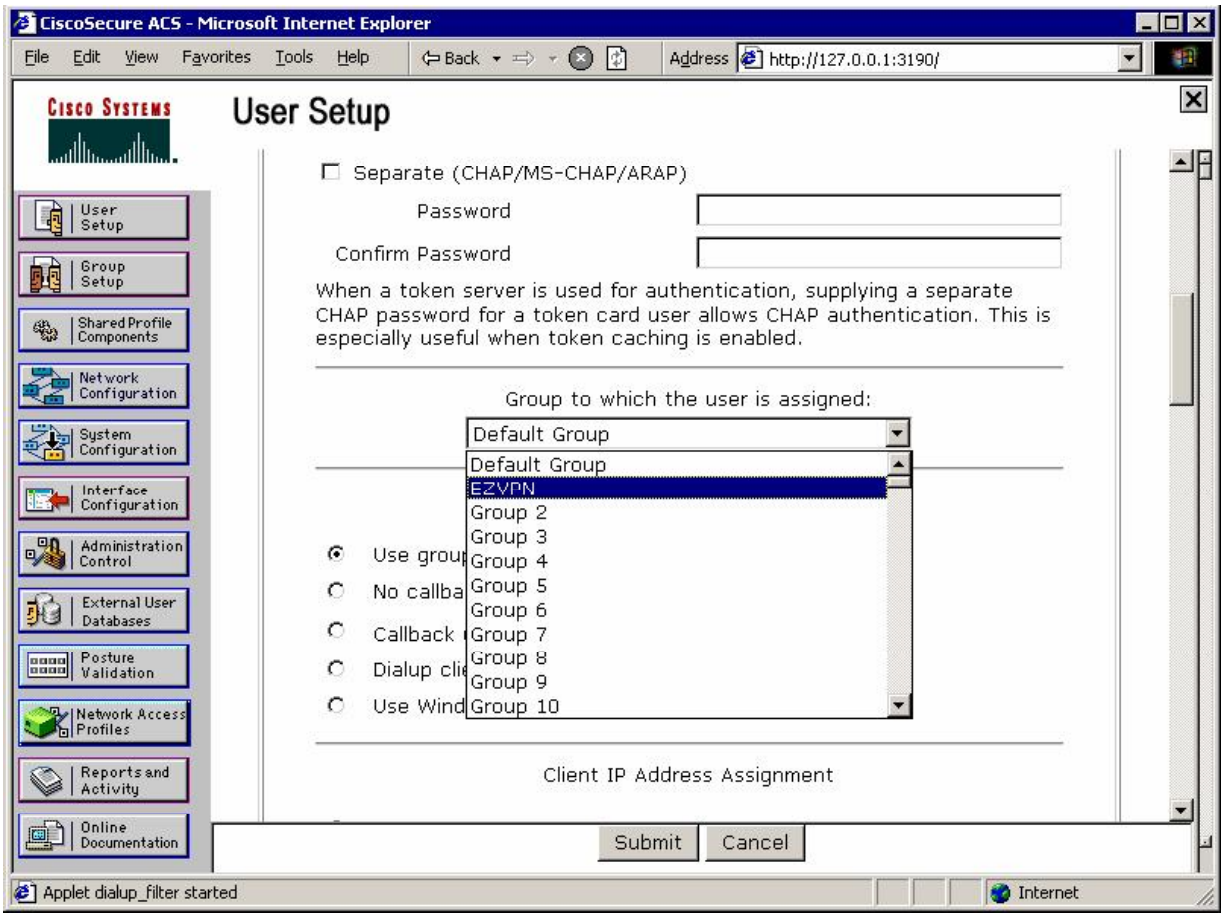



CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:3190/
Cisco Systems
Group Setup
Jump To RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes
[3076\011] Tunneling-Protocols
IPSec
[3076\013] IPSec-Authentication
RADIUS
[3076\027] IPSec-Split-Tunnel-List
SPLIT_TUNNEL
[3076\055] IPSec-Split-Tunneling-Policy
Only tunnel networks in the list
IETF RADIUS Attributes
[006] Service-Type
Submit
Submit + Restart
Cancel
Applet dialup_filter started
Internet

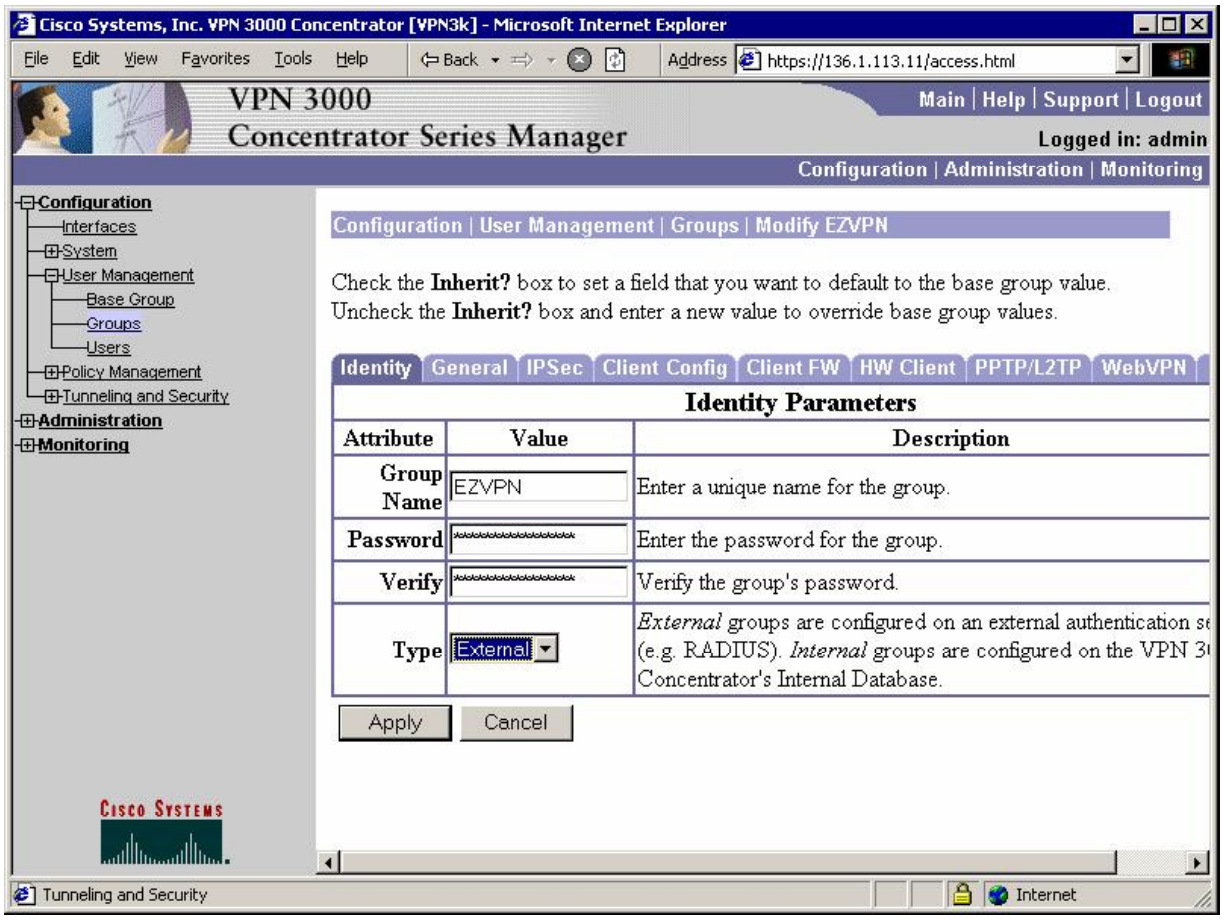
Create user EZVPN with password, matching the group's password configured on VPN3000 ("CISCO"):



Assign it to group EZVPN:

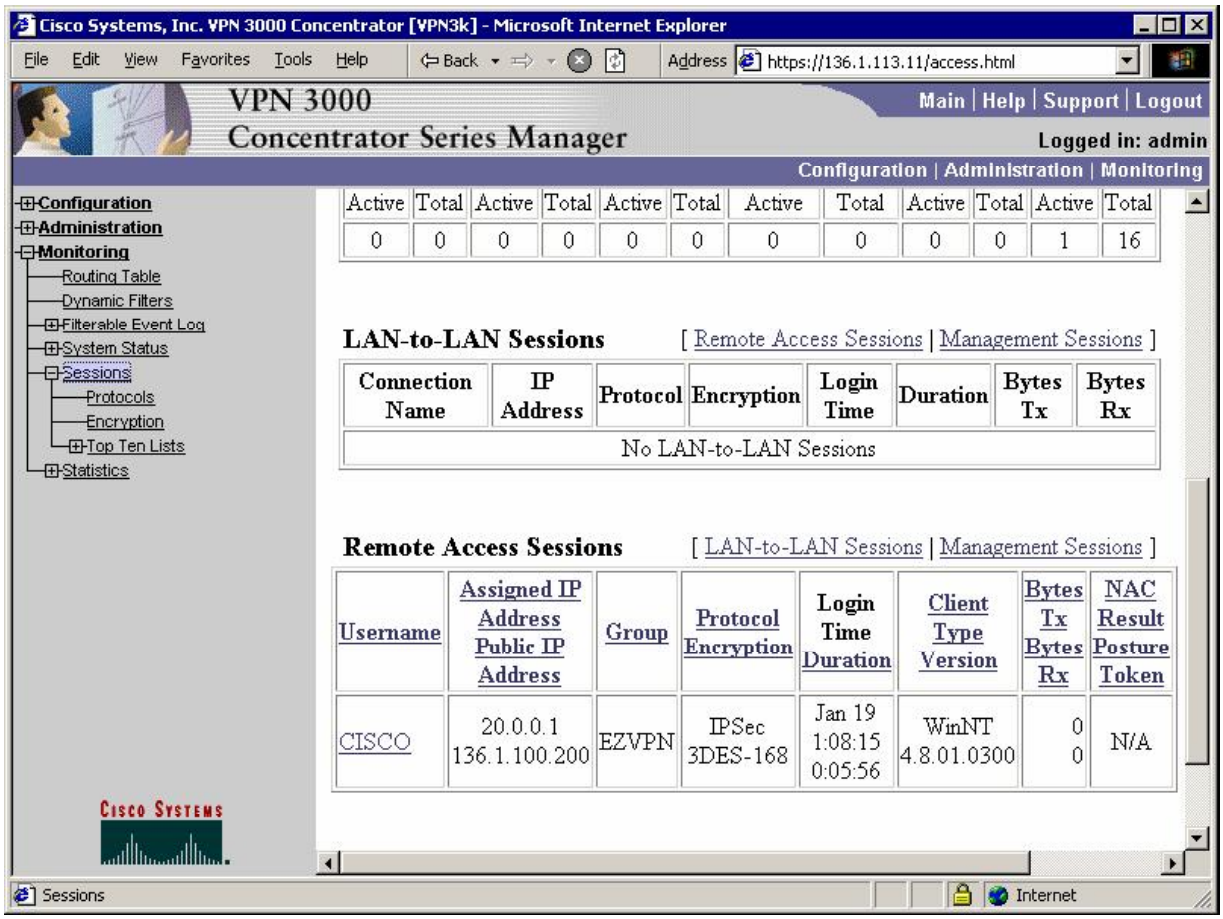


Configure group EZVPN on VPN3k as External:

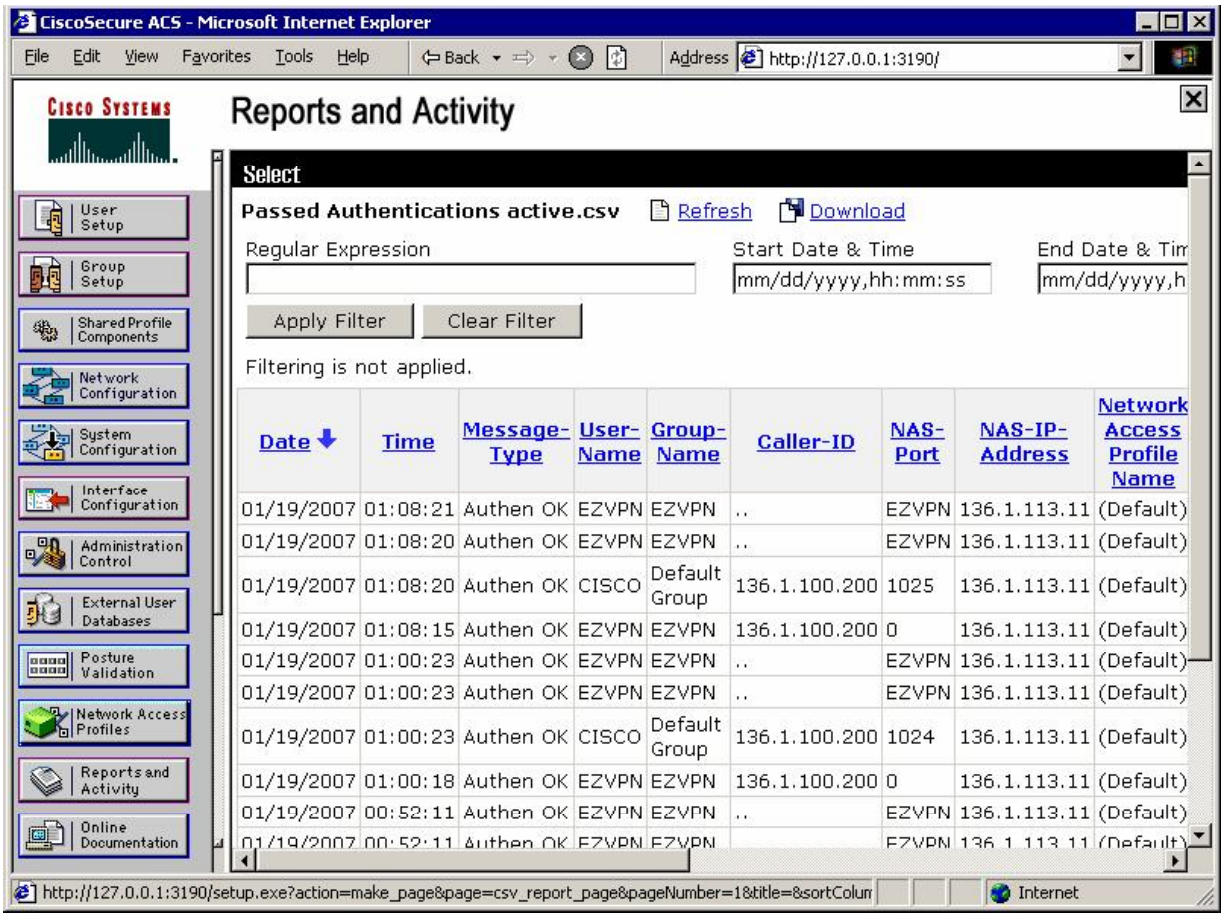


Verification

Connect Cisco VPN Client and check session status at VPN3000:



Check the passed authentications on ACS server:

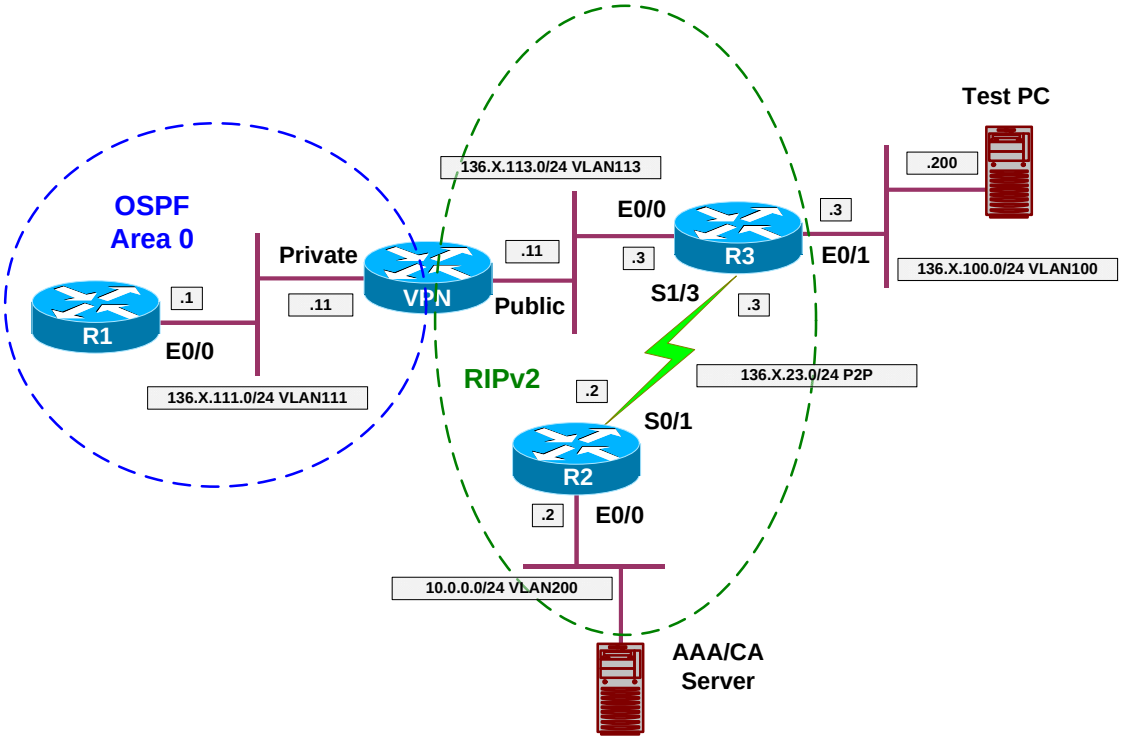


🕮 Further Reading

Cisco VPN Client User and Group Attribute Processing on the VPN 3000 Concentrator

VPN3k and Cisco VPN Client with Digital Certificates

Objective: Configure VPN3k and Cisco VPN client for group authentication using digital certificates.



Directions

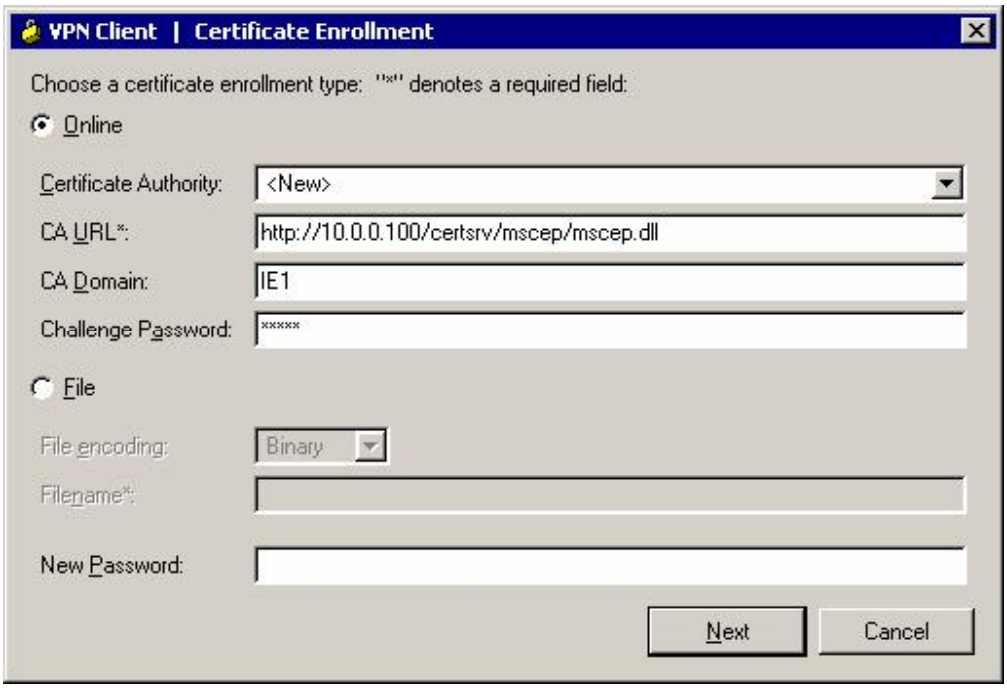
- Configure devices as per the scenario "VPN/ezVPN" "VPN3k and Cisco VPN Client with RRI".
- Start by configuring VPN Client:
  - First, enroll VPN client with CA via SCEP.
    - Use enrollment URL http://10.0.0.100/certsrv/mscep/mscep.dll
    - Specify "OU=EZVPN" to be used for group matching on VPN3k.
  - Next, use Internet Explorer to retreive and install CA Root Certificate into Windows trusted certificates store.
  - After that, download CA certificate and import it into VPN client Store.
  - Modify VPN connection setting, and choose authentication based on certificates.
- Enroll VPN3k with CA:
  - Set up clock synchronization via NTP with CA server.
    - Configure Public traffic filter to permit Outgoing NTP.

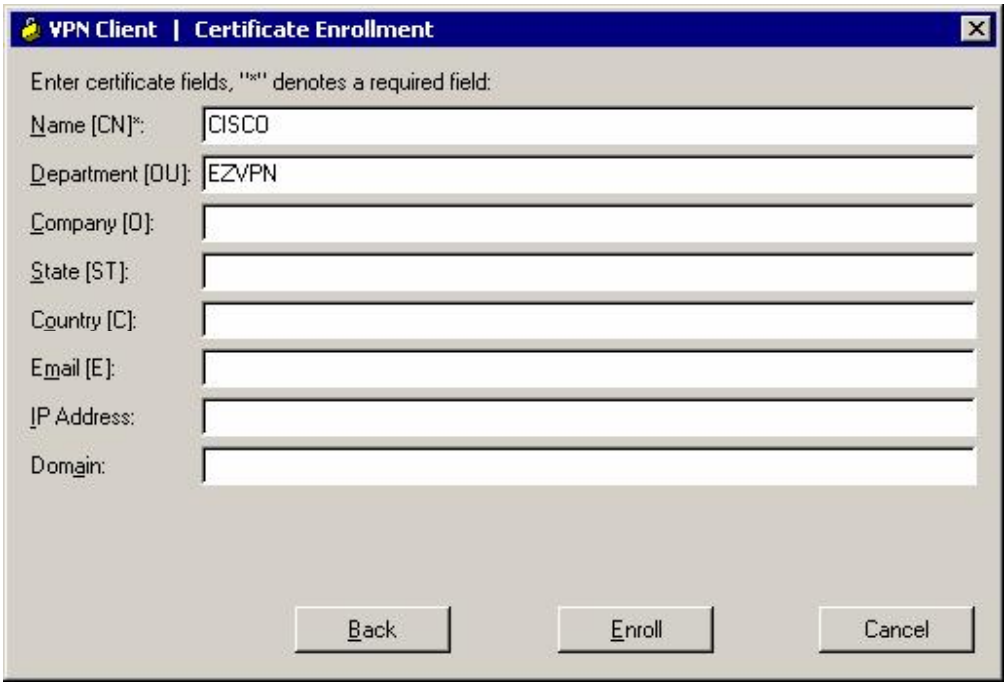
        - Configure two rules: inbound and outbound.
        - Assign them to Public traffic filter.
    - Retrieve CA Certificate via SCEP:
        - Configure Public traffic filter to permit:
            - Ougoing HTTP traffic In and Out.
            - Use the pre-configured rules for this task.
        - Use enrollment URL http://10.0.0.100/certsrv/mscep/mscep.dll
    - Generate Certificate Request.
- Configure VPN3k for Group authentication with certificates.
    - Activate “CiscoVPN” IKE proposal that uses RSA-Sig authentication.
    - Make it top priority.
- Modify the default IPsec SA “ESP-3DES-MD5”
    - Configure it to use digital certificates for authentication.
    - Chose certificate you have obtained from CA for identity.
- Check group “EZVPN” to make sure you have assigned IPsec SA “ESP-3DES-MD5” in “IPsec” Tab.

Final Configuration

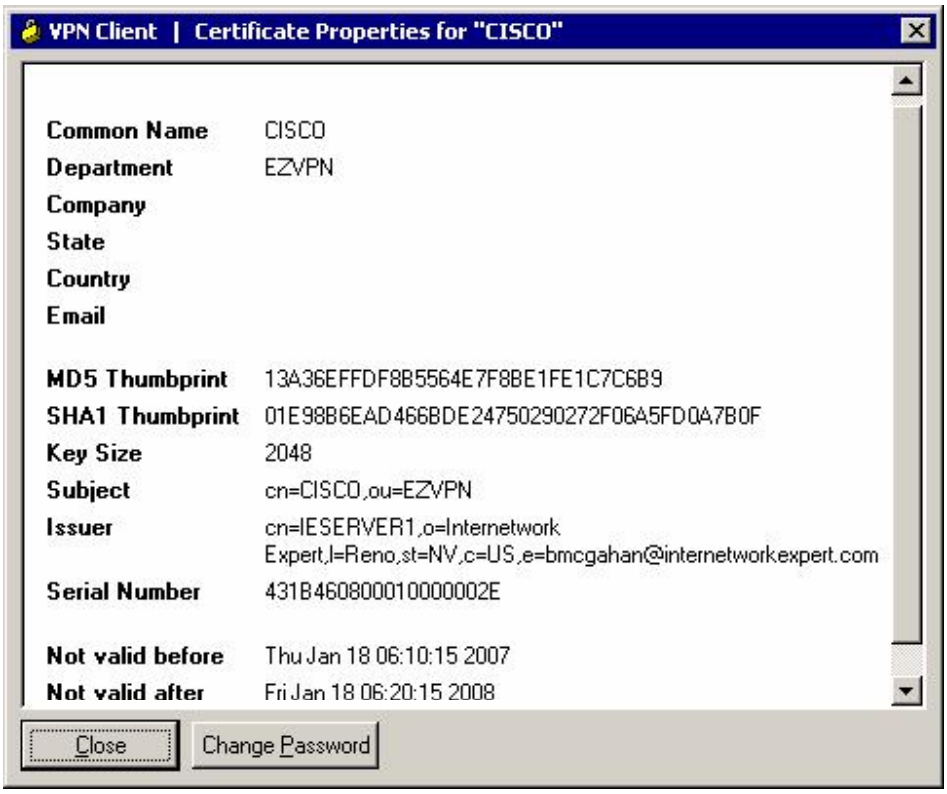
Test PC/VPN Client:

Choose Certificates/Enroll:

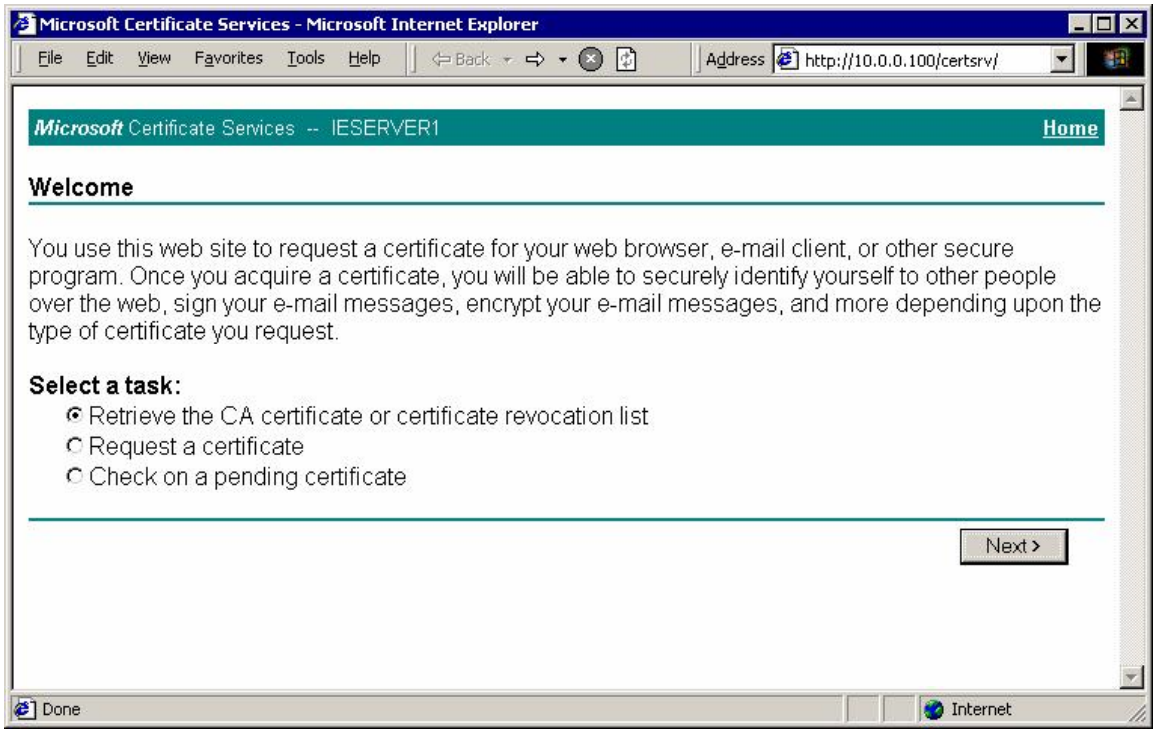




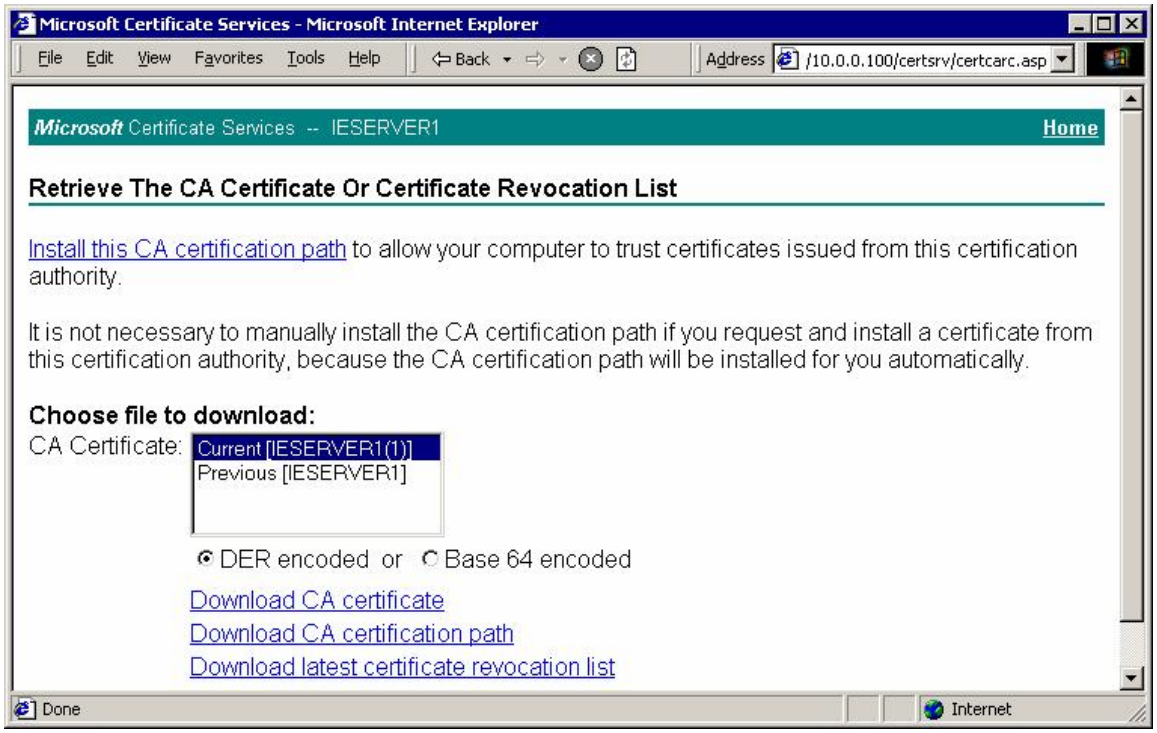
View your certificate:

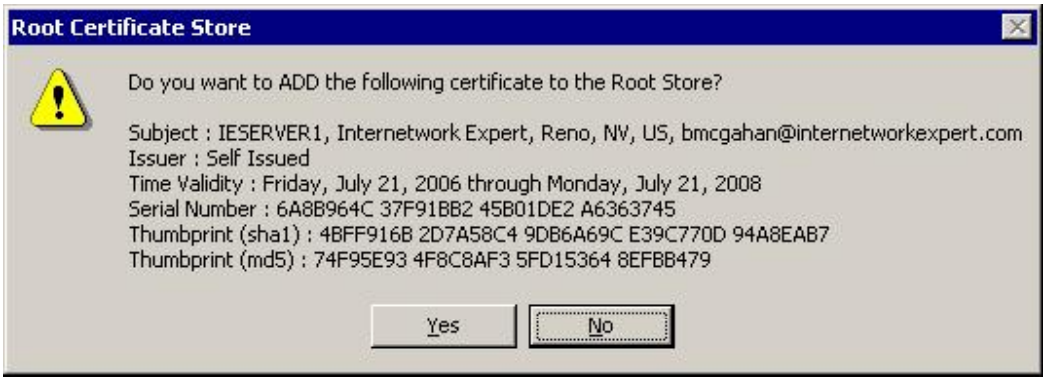


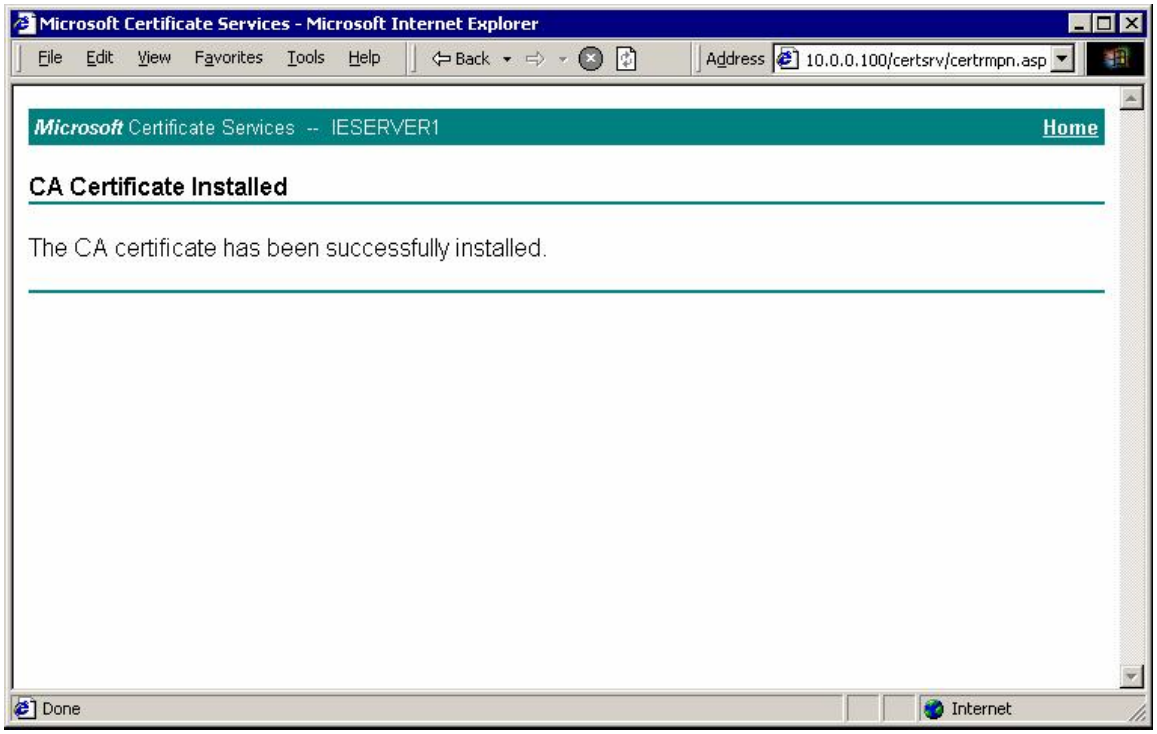
Retreive CA certificate and install it into Trusted Roots store:



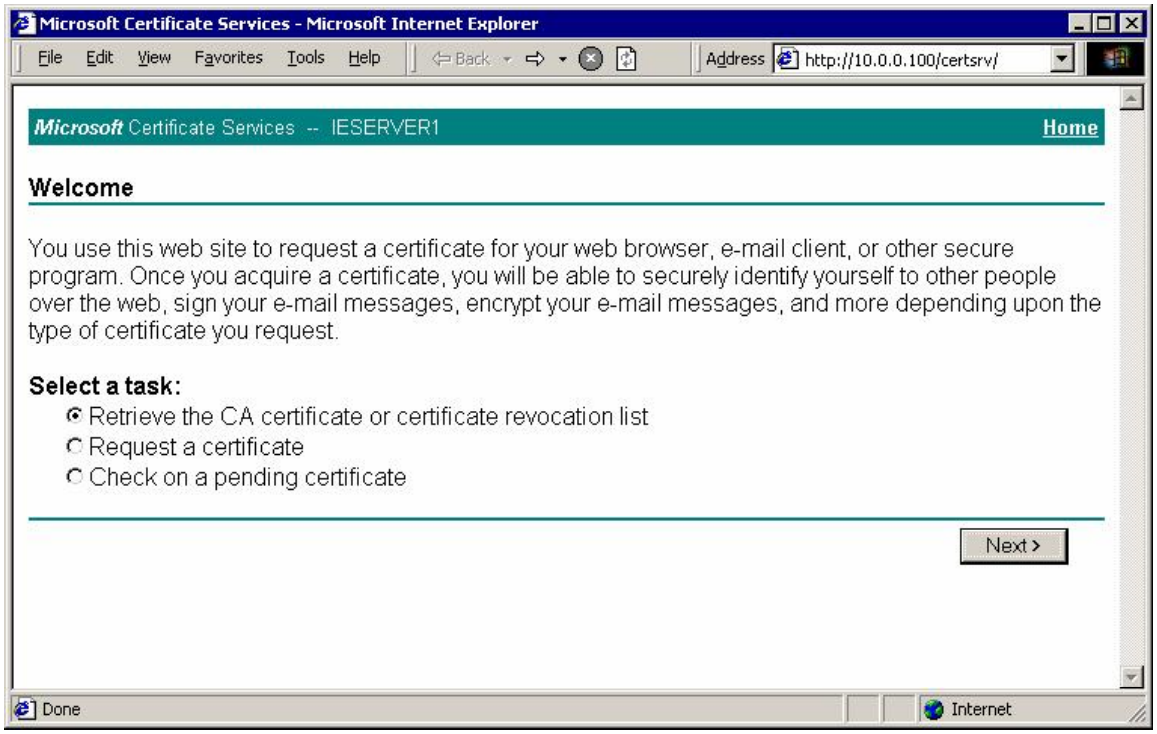
Choose "Install this CA certification path":



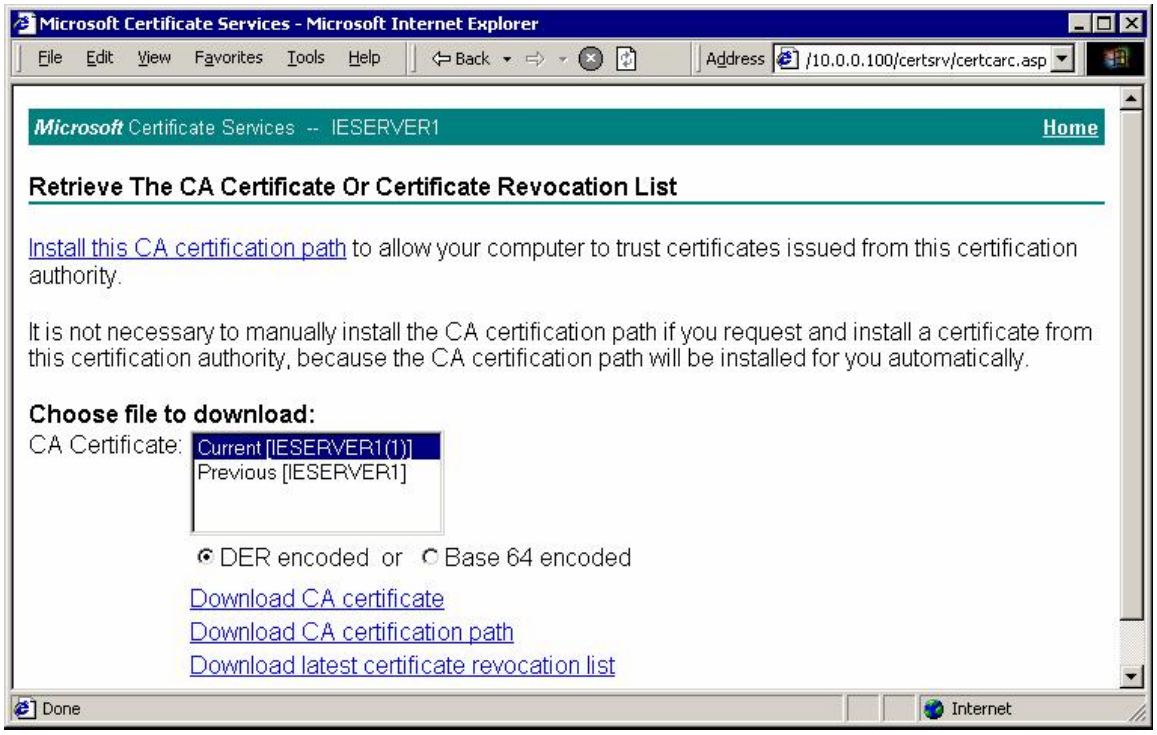

Root Certificate Store
Do you want to ADD the following certificate to the Root Store?
Subject : IESERVER1, Internetwork Expert, Reno, NV, US, bmcgahan@internetworkexpert.com
Issuer : Self Issued
Time Validity : Friday, July 21, 2006 through Monday, July 21, 2008
Serial Number : 6A8B964C 37F91BB2 45B01DE2 A6363745
Thumbprint (sha1) : 4BFF916B 2D7A58C4 9DB6A69C E39C770D 94A8EAB7
Thumbprint (md5) : 74F95E93 4F8C8AF3 5FD15364 8EFBB479
Yes
No

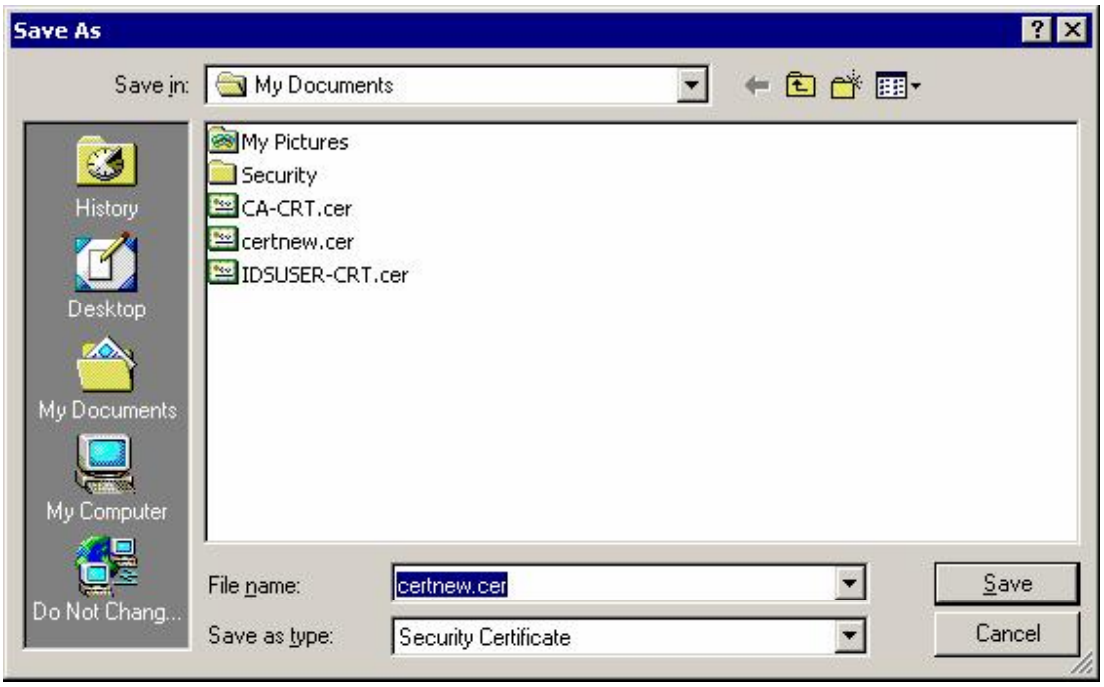

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address 10.0.0.100/certsrv/certrmpn.asp
Microsoft Certificate Services -- IESERVER1
Home
CA Certificate Installed
The CA certificate has been successfully installed.
Done
Internet

Download CA certificate for installation into Cisco VPN Client certificate store:

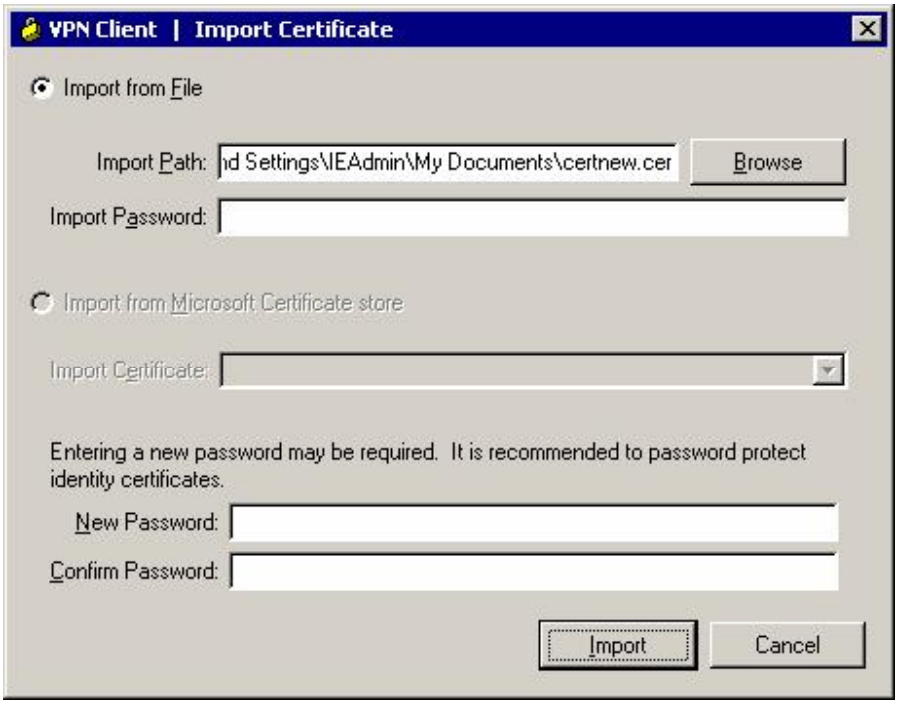


Choose "Download CA Certificate":

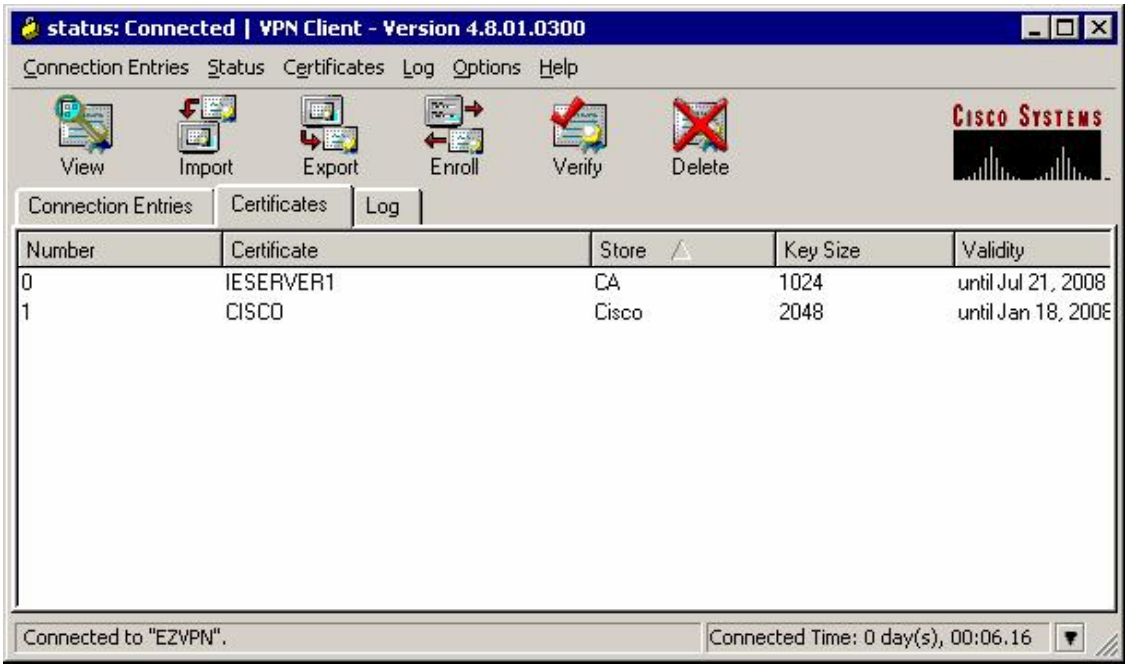




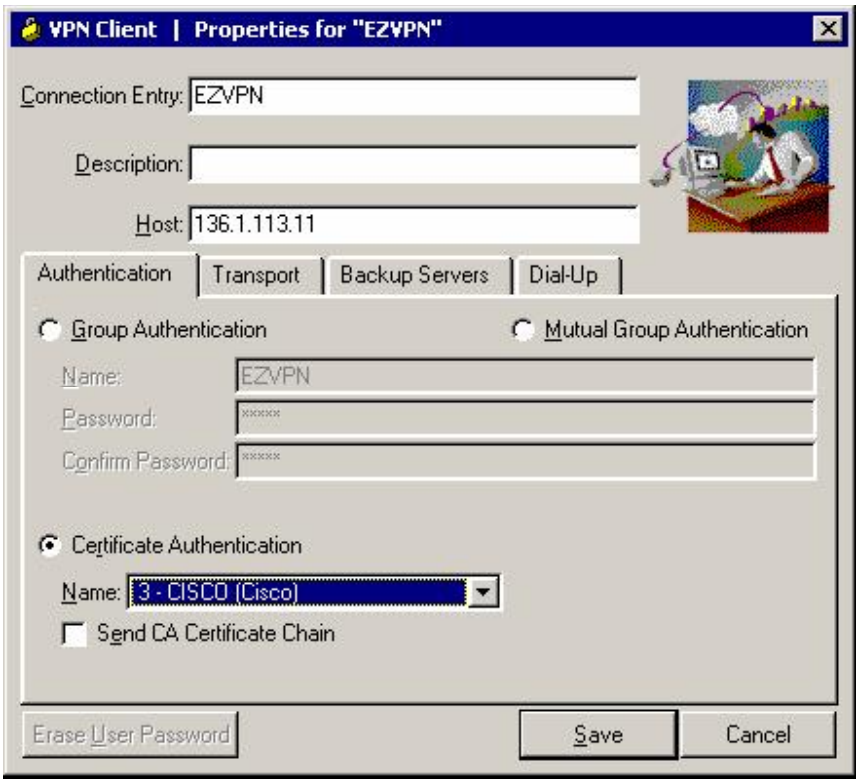
Next choose "Import" in Certificate Menu of Cisco VPN Client, and browse to downloaded file:



You should now have identity ceritificate and CA certificate into Cisco VPN Client Store:

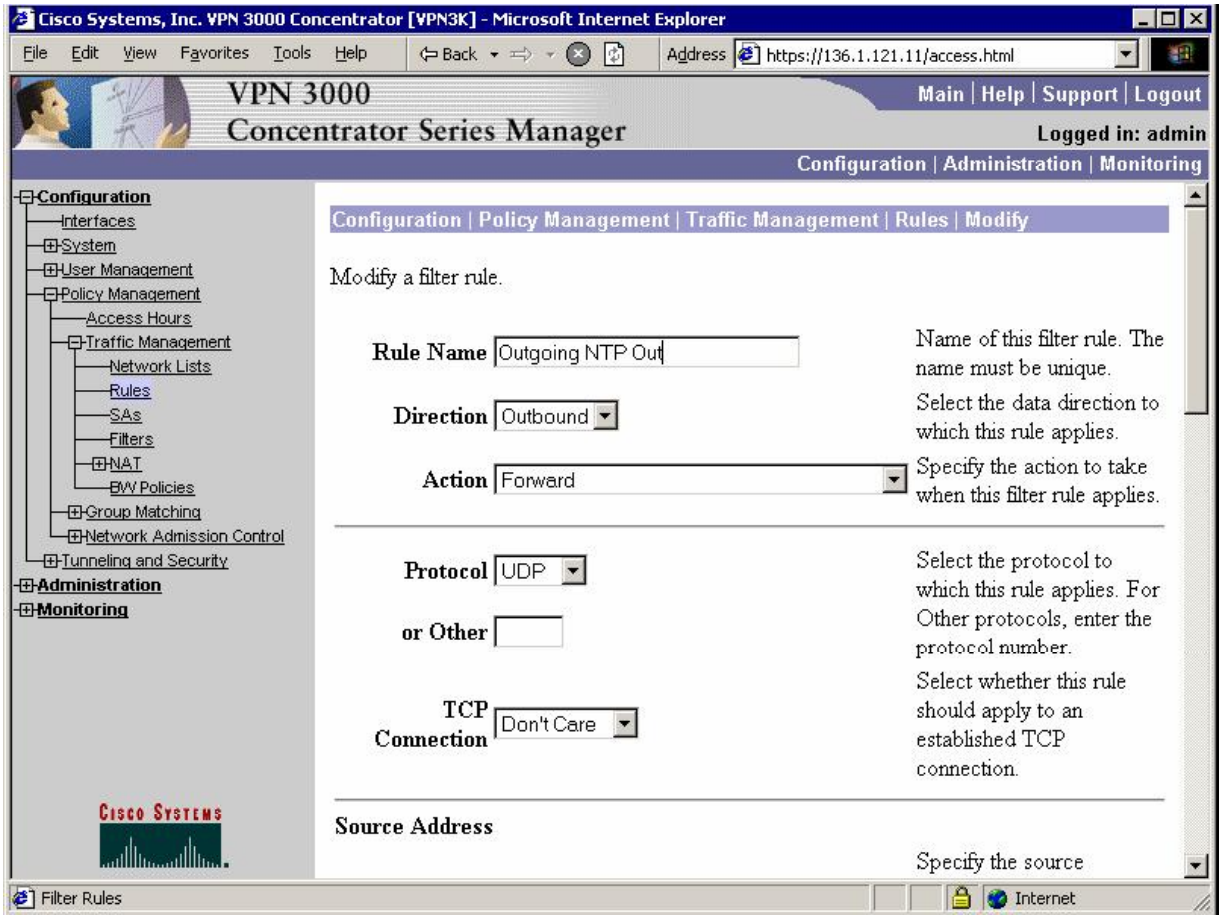


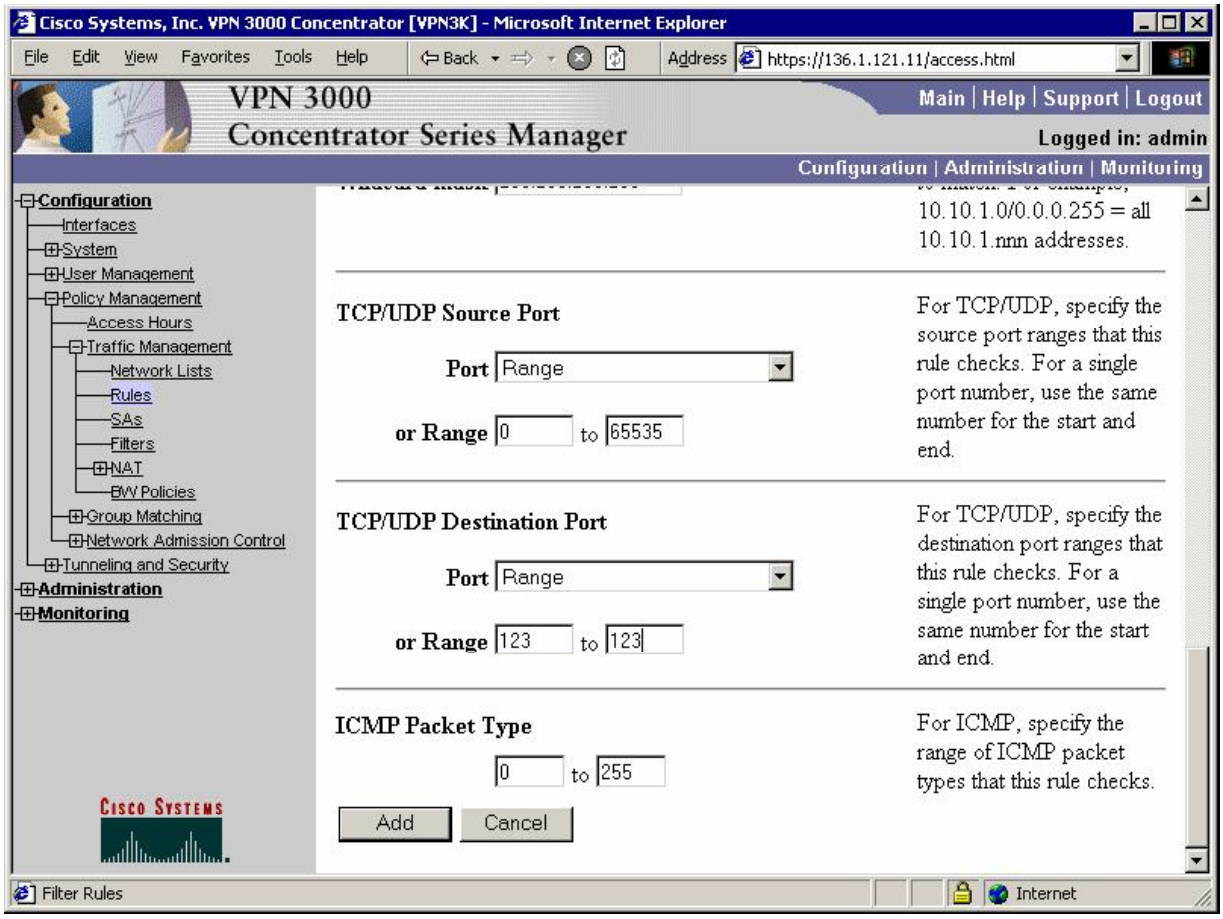
Modify connection Settings to use Certificates for authentication:



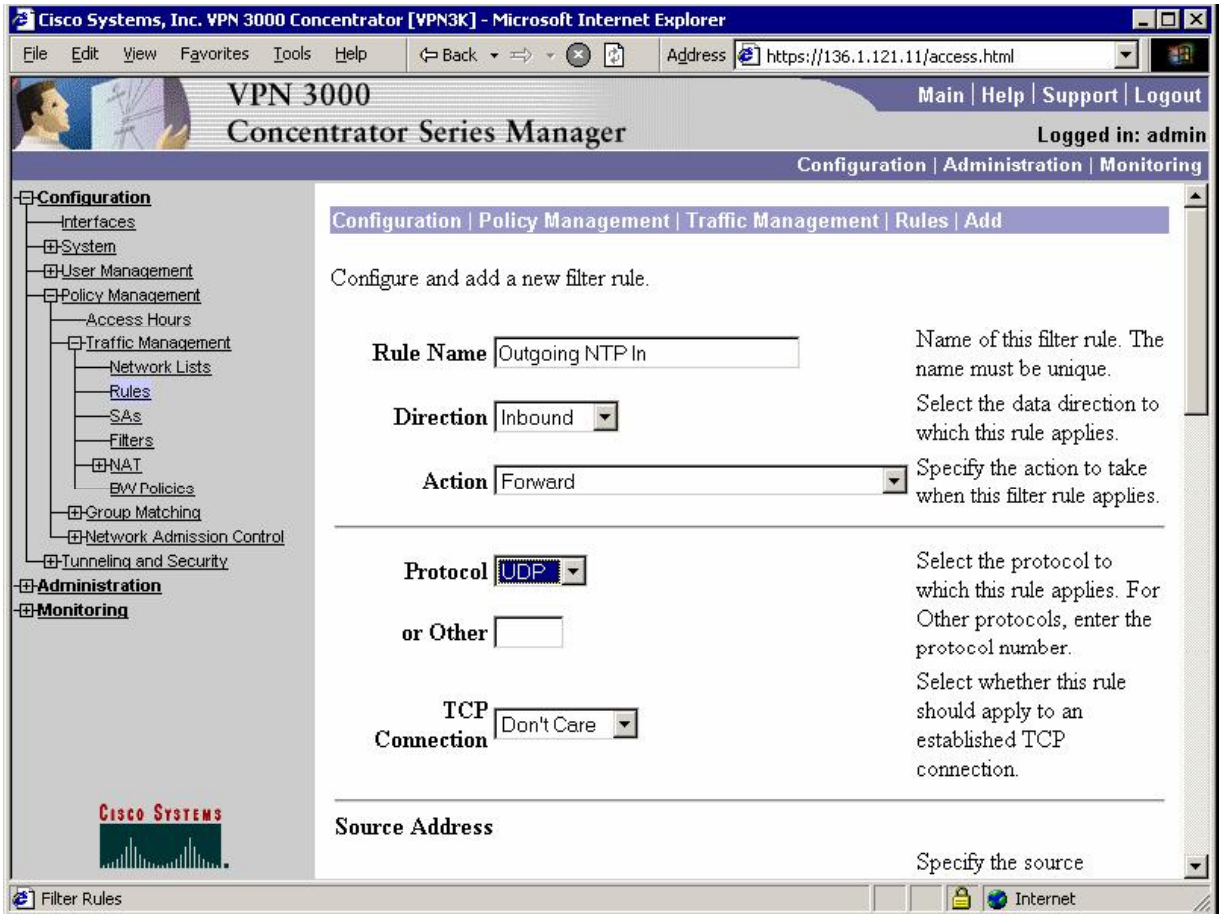
VPN3k:

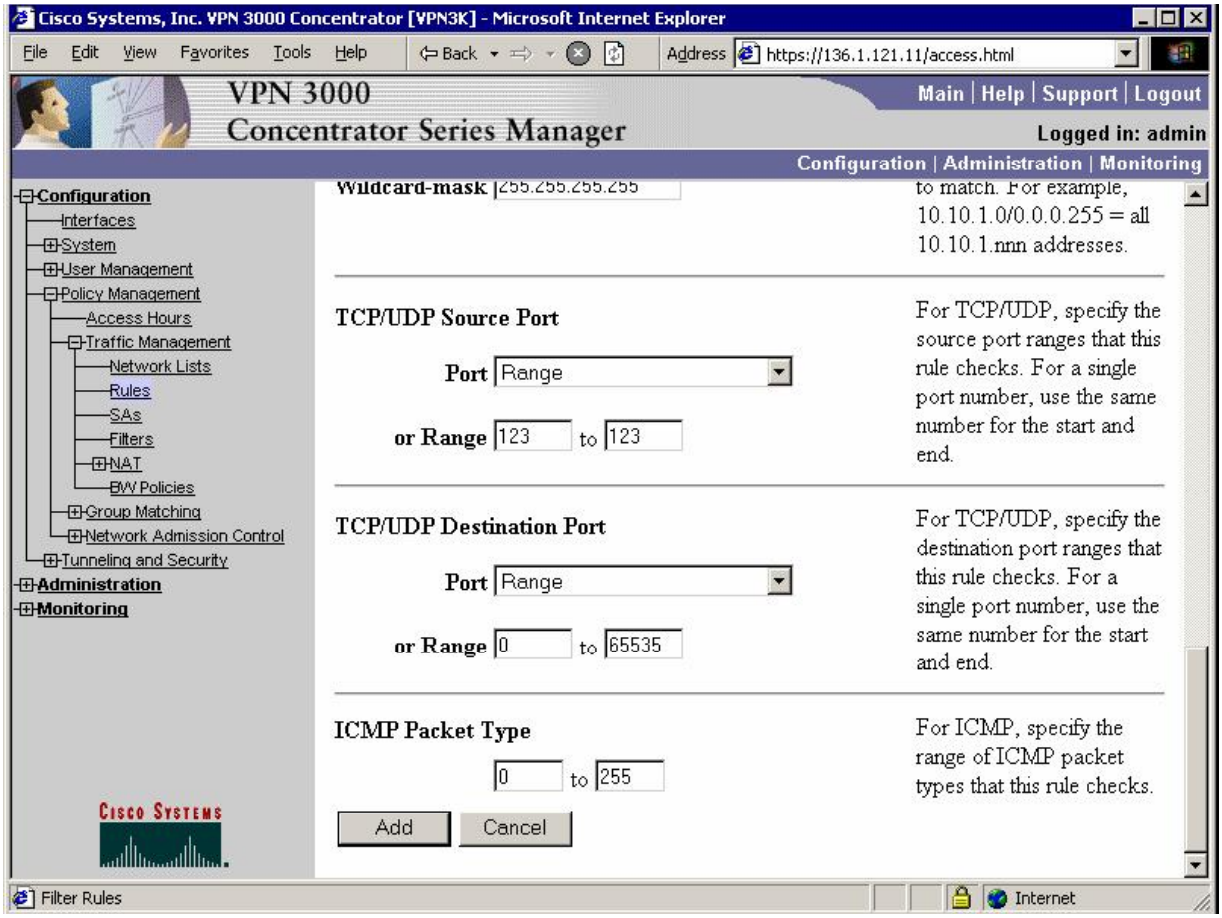
Create rule for Outgoing NTP Out:



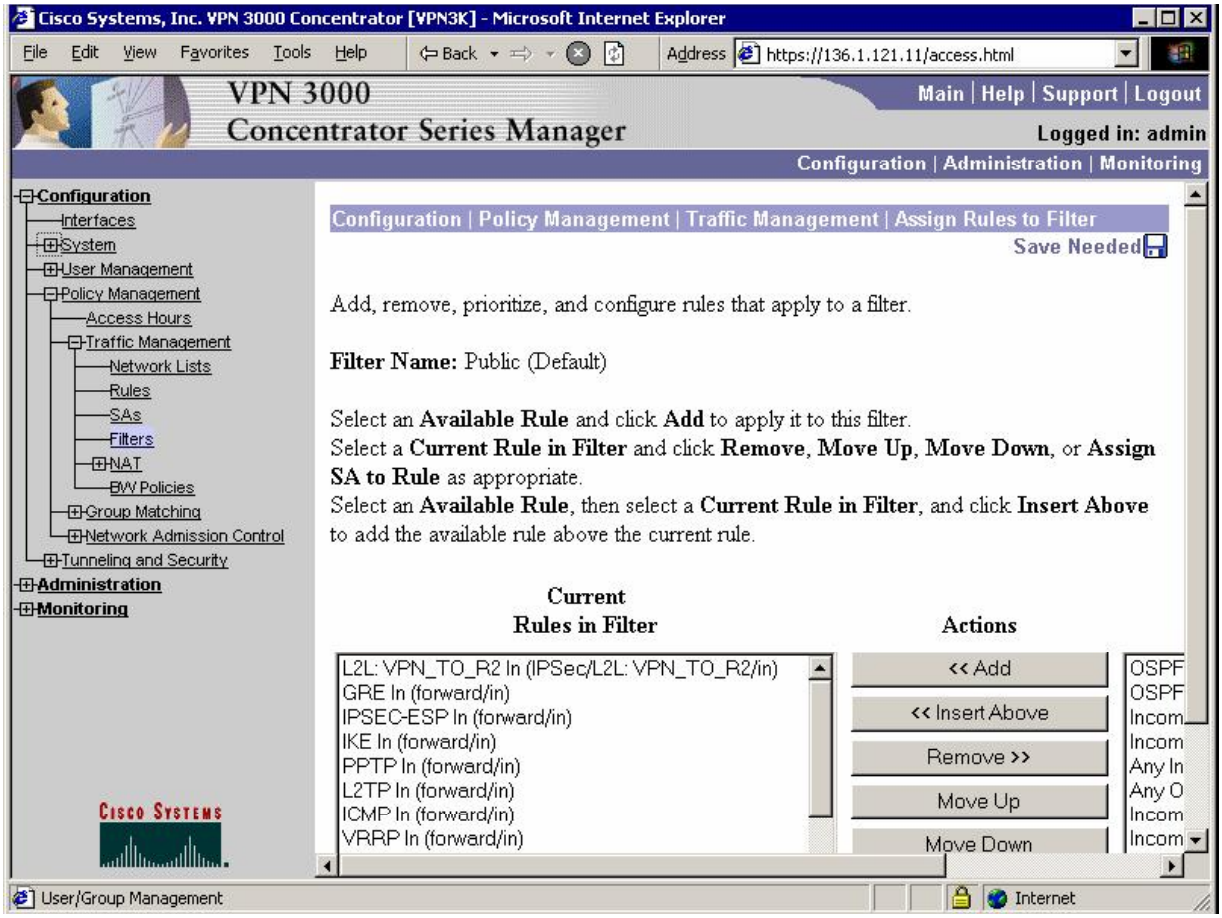

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
TCP/UDP Source Port
Port Range
or Range 0 to 65535
For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.
TCP/UDP Destination Port
Port Range
or Range 123 to 123
For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.
ICMP Packet Type
0 to 255
For ICMP, specify the range of ICMP packet types that this rule checks.
Add
Cancel
Cisco Systems
Filter Rules
Internet

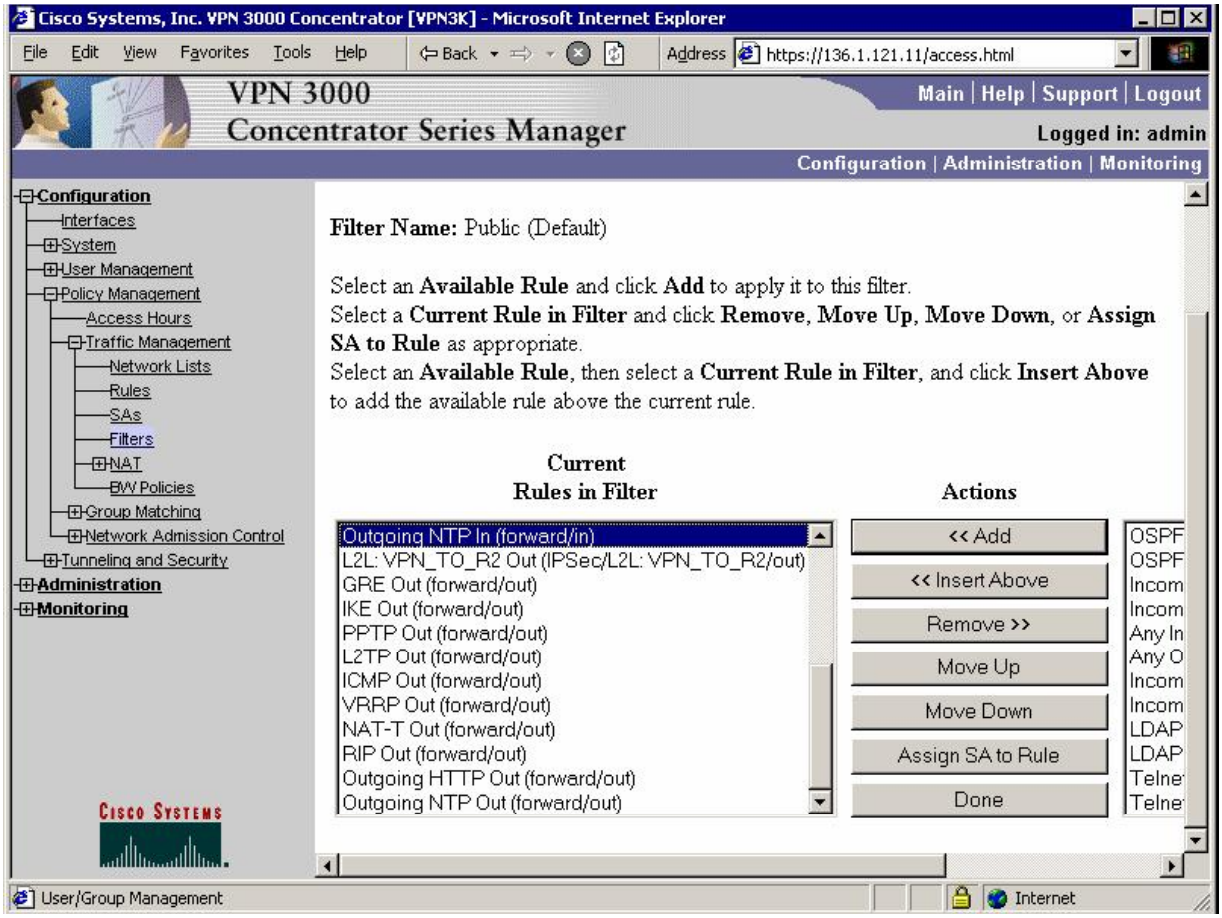
Create rule for Outgoing NTP inbound:



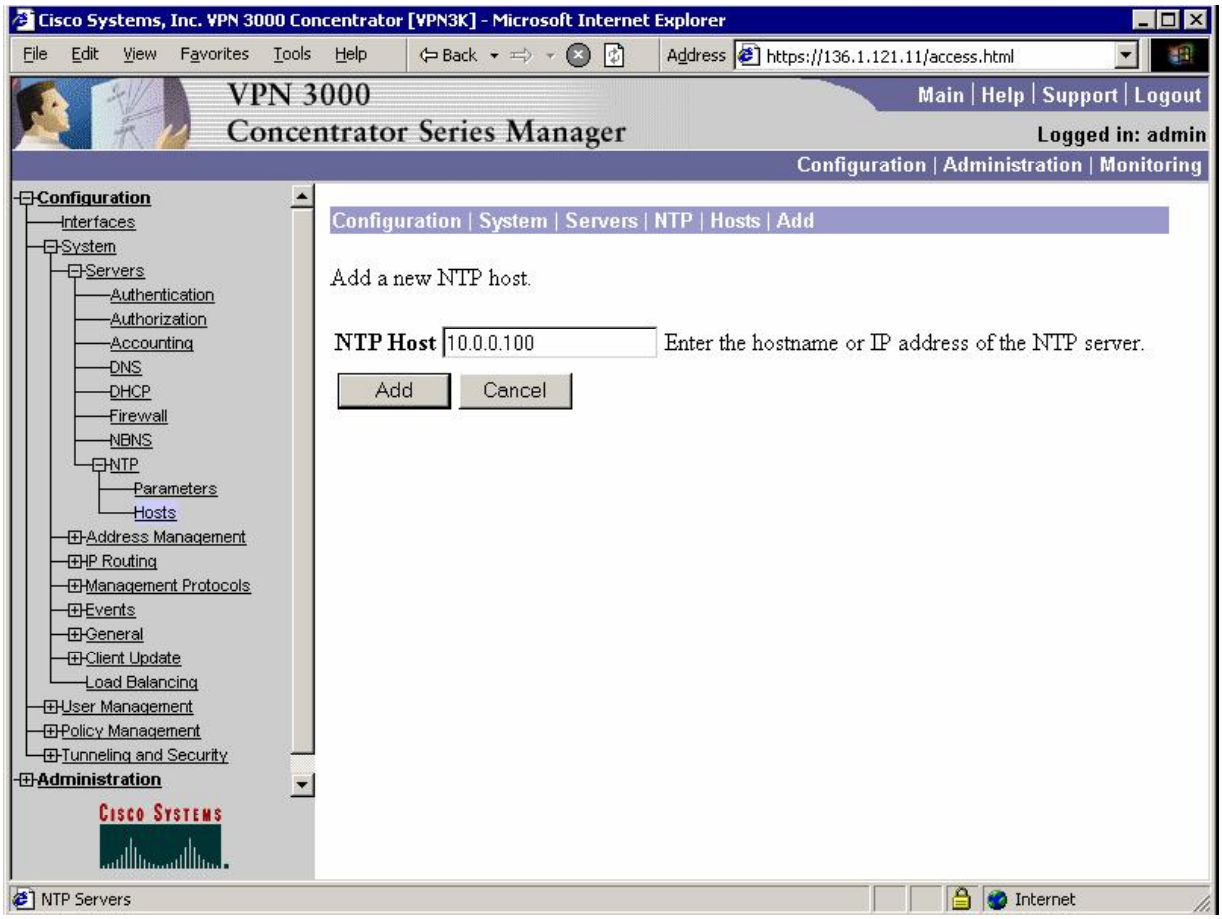


Add rules to Public filter, permitting outgoing NTP:


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Configuration | Policy Management | Traffic Management | Assign Rules to Filter
Save Needed
Add, remove, prioritize, and configure rules that apply to a filter.
Filter Name: Public (Default)
Select an Available Rule and click Add to apply it to this filter.
Select a Current Rule in Filter and click Remove, Move Up, Move Down, or Assign SA to Rule as appropriate.
Select an Available Rule, then select a Current Rule in Filter, and click Insert Above to add the available rule above the current rule.
Current Rules in Filter
Actions
L2L: VPN_TO_R2 In (IPSec/L2L: VPN_TO_R2/in)
GRE In (forward/in)
IPSEC-ESP In (forward/in)
IKE In (forward/in)
PPTP In (forward/in)
L2TP In (forward/in)
ICMP In (forward/in)
VRRP In (forward/in)
<< Add
<< Insert Above
Remove >>
Move Up
Move Down
Cisco Systems
User/Group Management
Internet

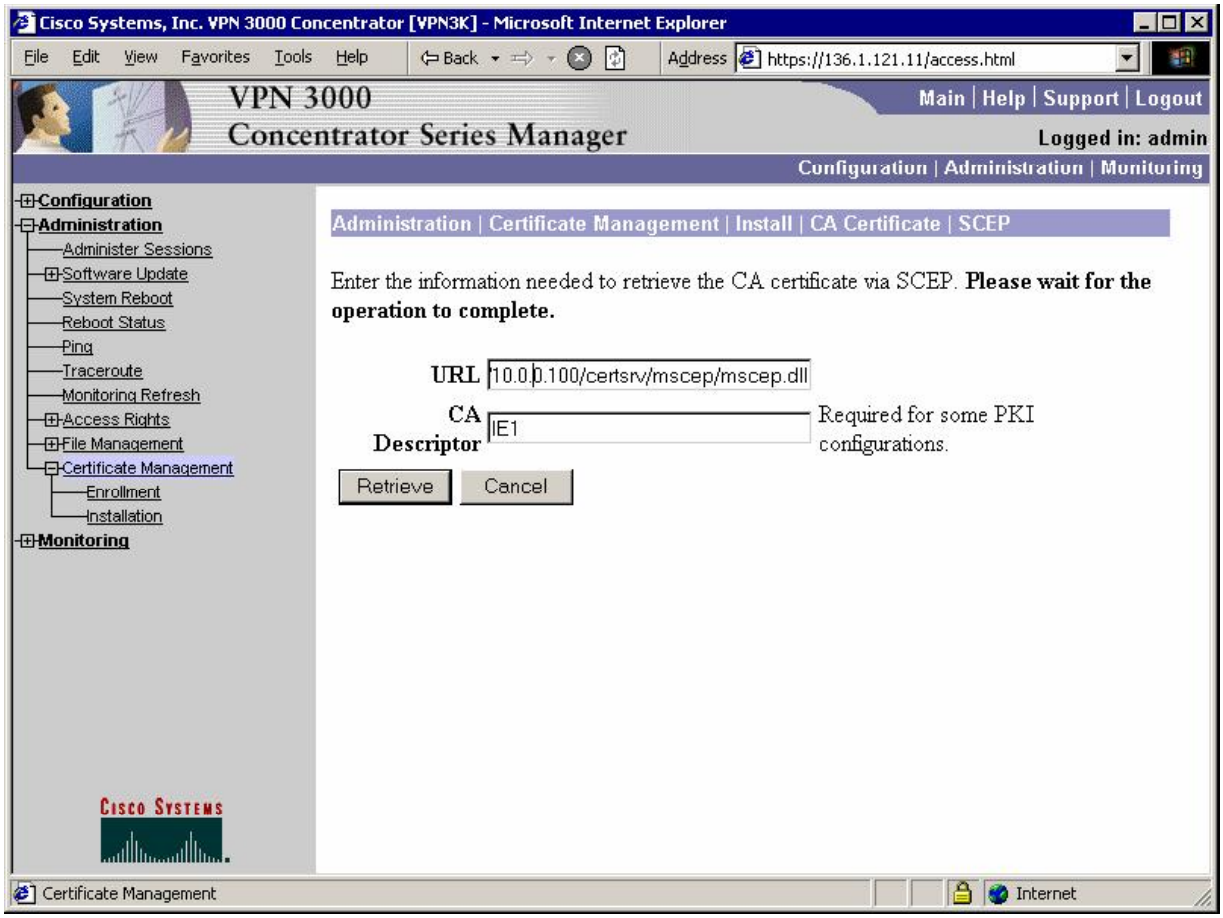

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Filter Name: Public (Default)
Select an Available Rule and click Add to apply it to this filter.
Select a Current Rule in Filter and click Remove, Move Up, Move Down, or Assign SA to Rule as appropriate.
Select an Available Rule, then select a Current Rule in Filter, and click Insert Above to add the available rule above the current rule.
Current Rules in Filter
Actions
Outgoing NTP In (forward/in)
L2L: VPN_TO_R2 Out (IPSec/L2L: VPN_TO_R2/out)
GRE Out (forward/out)
IKE Out (forward/out)
PPTP Out (forward/out)
L2TP Out (forward/out)
ICMP Out (forward/out)
VRRP Out (forward/out)
NAT-T Out (forward/out)
RIP Out (forward/out)
Outgoing HTTP Out (forward/out)
Outgoing NTP Out (forward/out)
<< Add
<< Insert Above
Remove >>
Move Up
Move Down
Assign SA to Rule
Done
Cisco Systems
User/Group Management
Internet

Configure NTP Server:

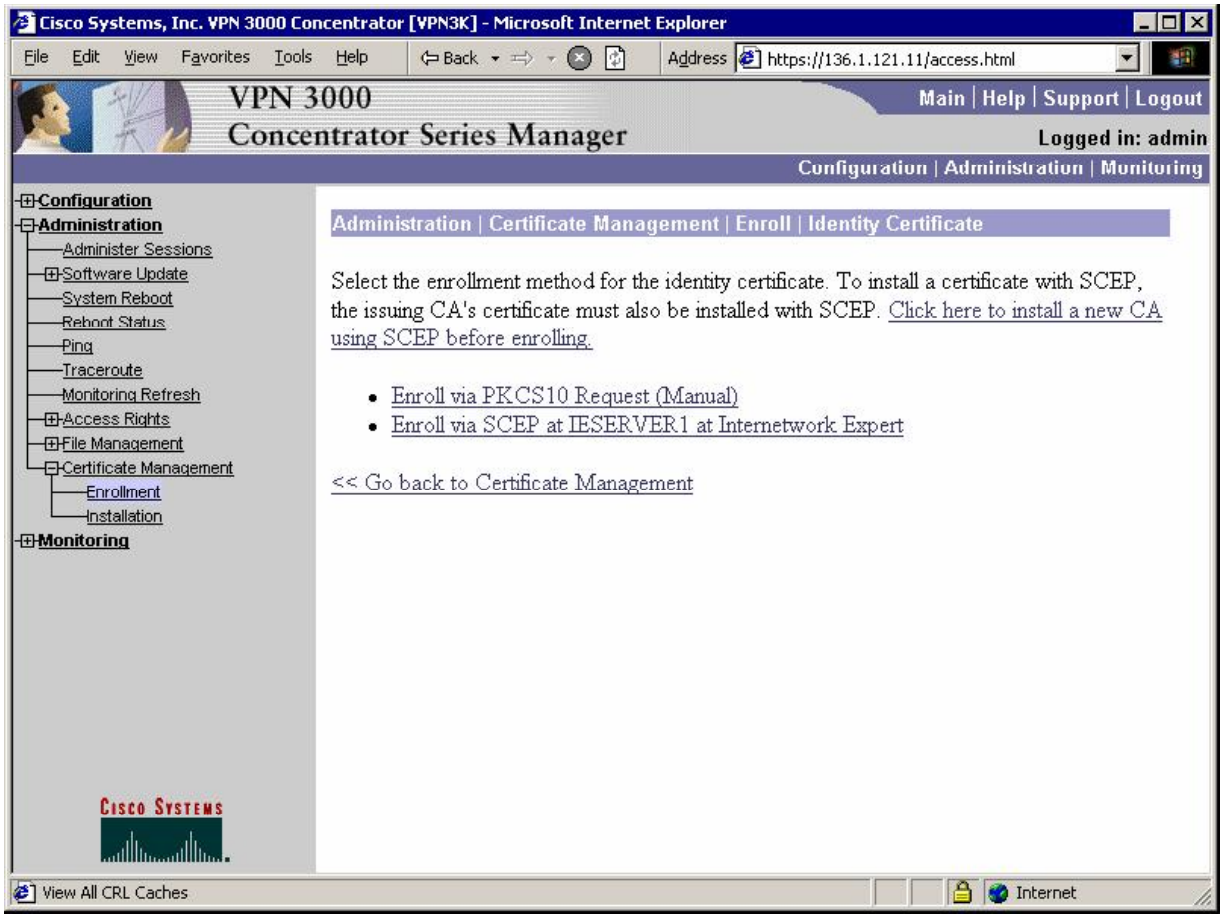


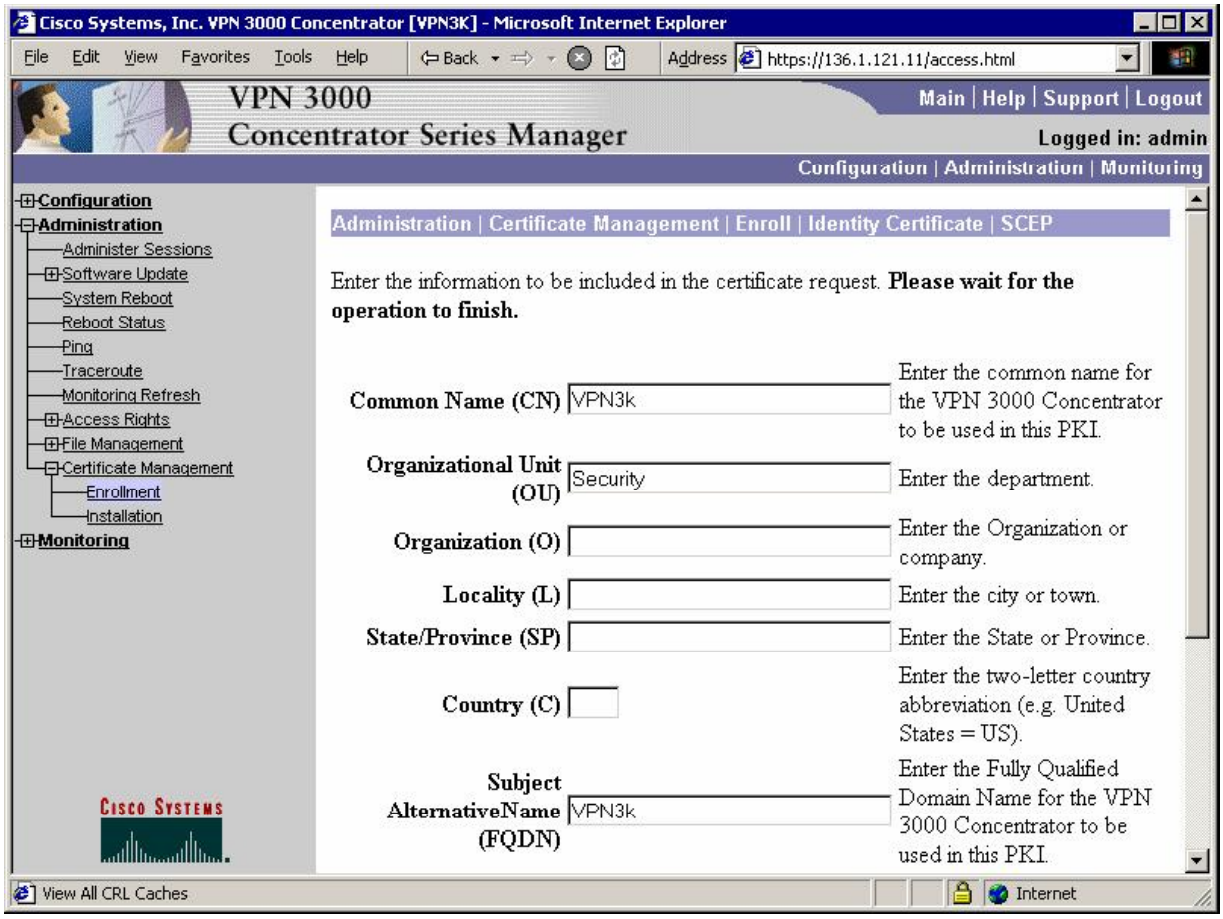
Add rules to Public filter, permitting Outgoing HTTP In/Out (for SCEP):

Install CA Certificate:


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Traceroute
Monitoring Refresh
Access Rights
File Management
Certificate Management
Enrollment
Installation
Monitoring
Administration | Certificate Management | Install | CA Certificate | SCEP
Enter the information needed to retrieve the CA certificate via SCEP. Please wait for the operation to complete.
URL 10.0.0.100/certsrv/mscep/mscep.dll
CA Descriptor IE1
Required for some PKI configurations.
Retrieve
Cancel
Cisco Systems
Certificate Management
Internet

Enroll with certification authority:

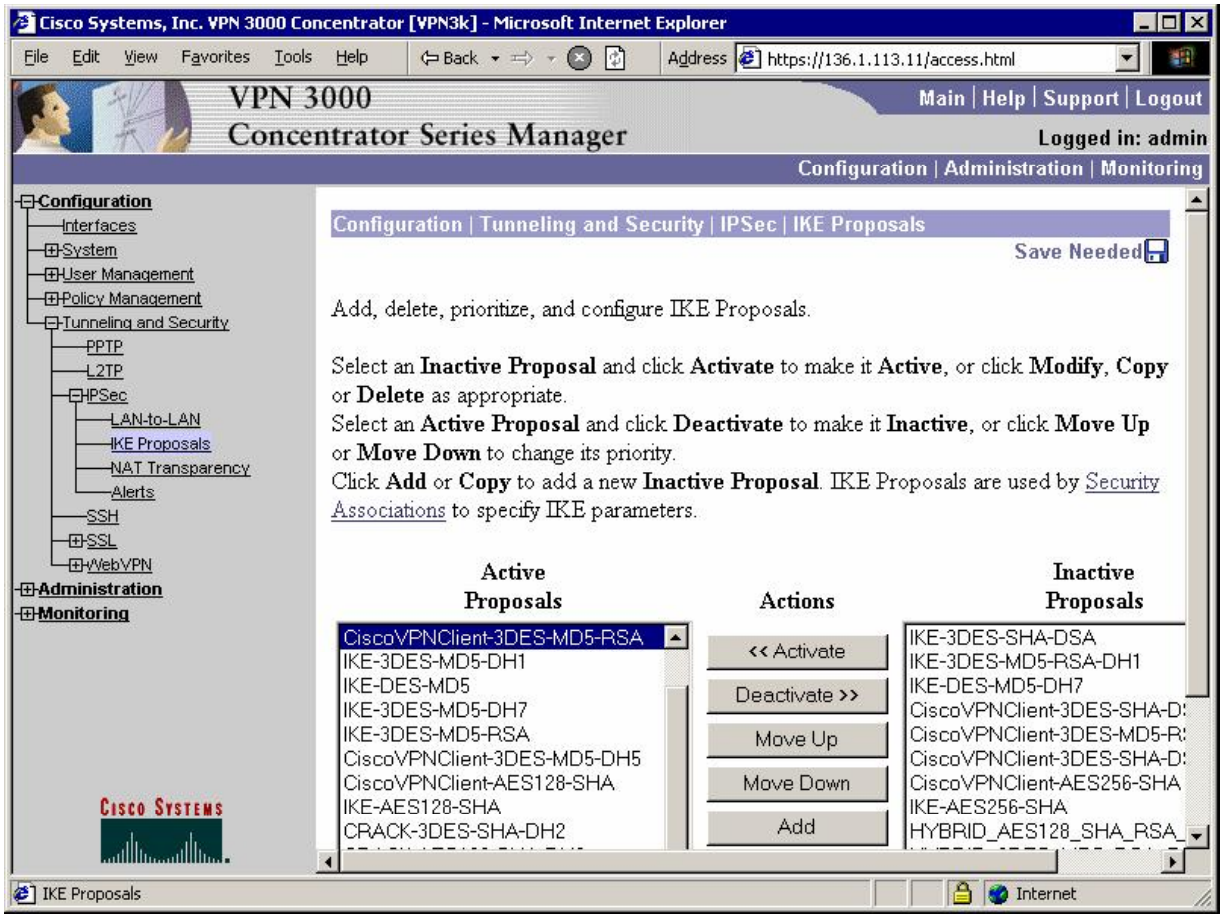



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Traceroute
Monitoring Refresh
Access Rights
File Management
Certificate Management
Enrollment
Installation
Monitoring
Administration | Certificate Management | Enroll | Identity Certificate | SCEP
Enter the information to be included in the certificate request. Please wait for the operation to finish.
Common Name (CN)
VPN3k
Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)
Security
Enter the department.
Organization (O)
Enter the Organization or company.
Locality (L)
Enter the city or town.
State/Province (SP)
Enter the State or Province.
Country (C)
Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)
VPN3k
Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Cisco Systems
View All CRL Caches
Internet


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.121.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Traceroute
Monitoring Refresh
Access Rights
File Management
Certificate Management
Enrollment
Installation
Monitoring
Administration | Certificate Management | Enrollment | Request Generated
A certificate request has been generated.
SCEP Status: Installed
Go to Certificate Management
Go to Certificate Enrollment
Go to Certificate Installation
Cisco Systems
View All CRL Caches
Internet

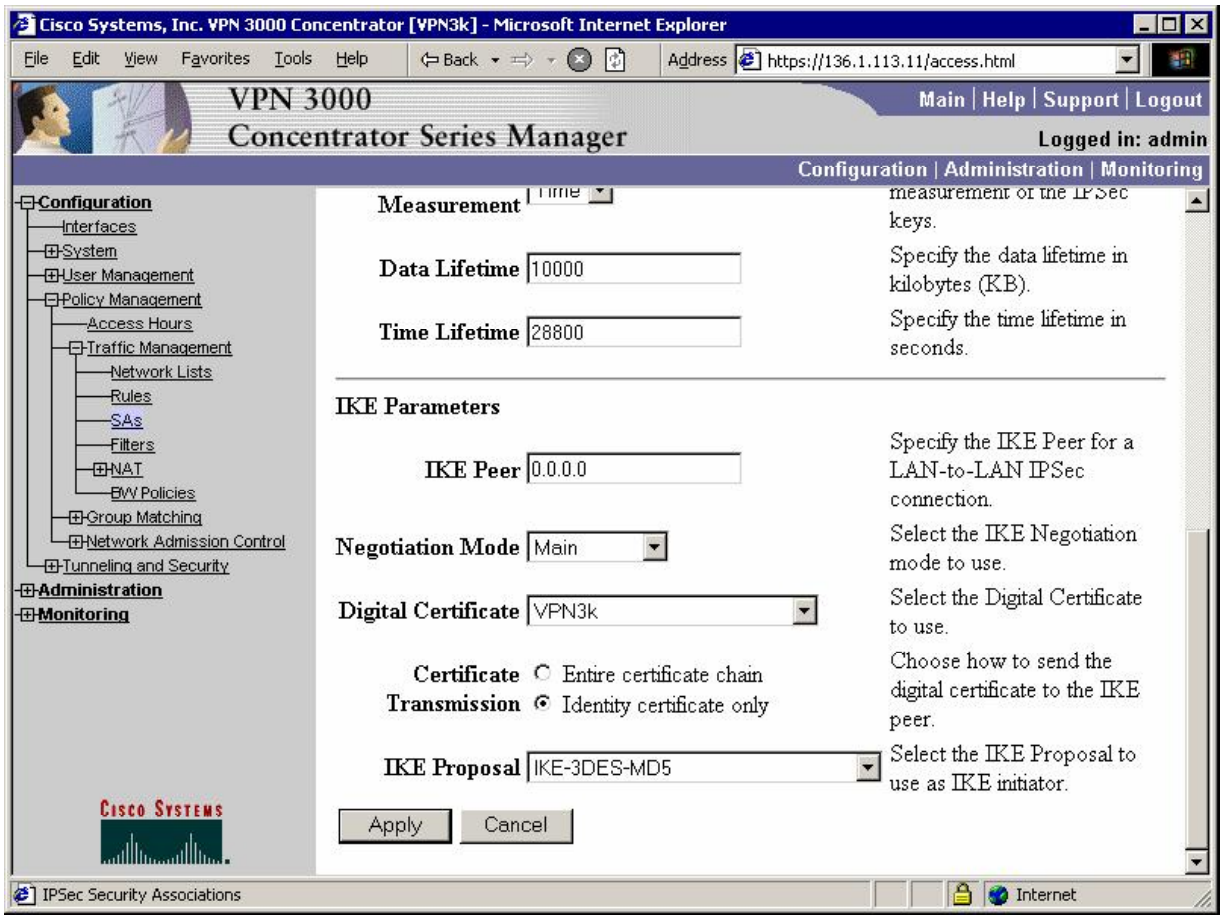
Activate IKE Proposal that uses RSA-Sig authentication:

Make it top priority:

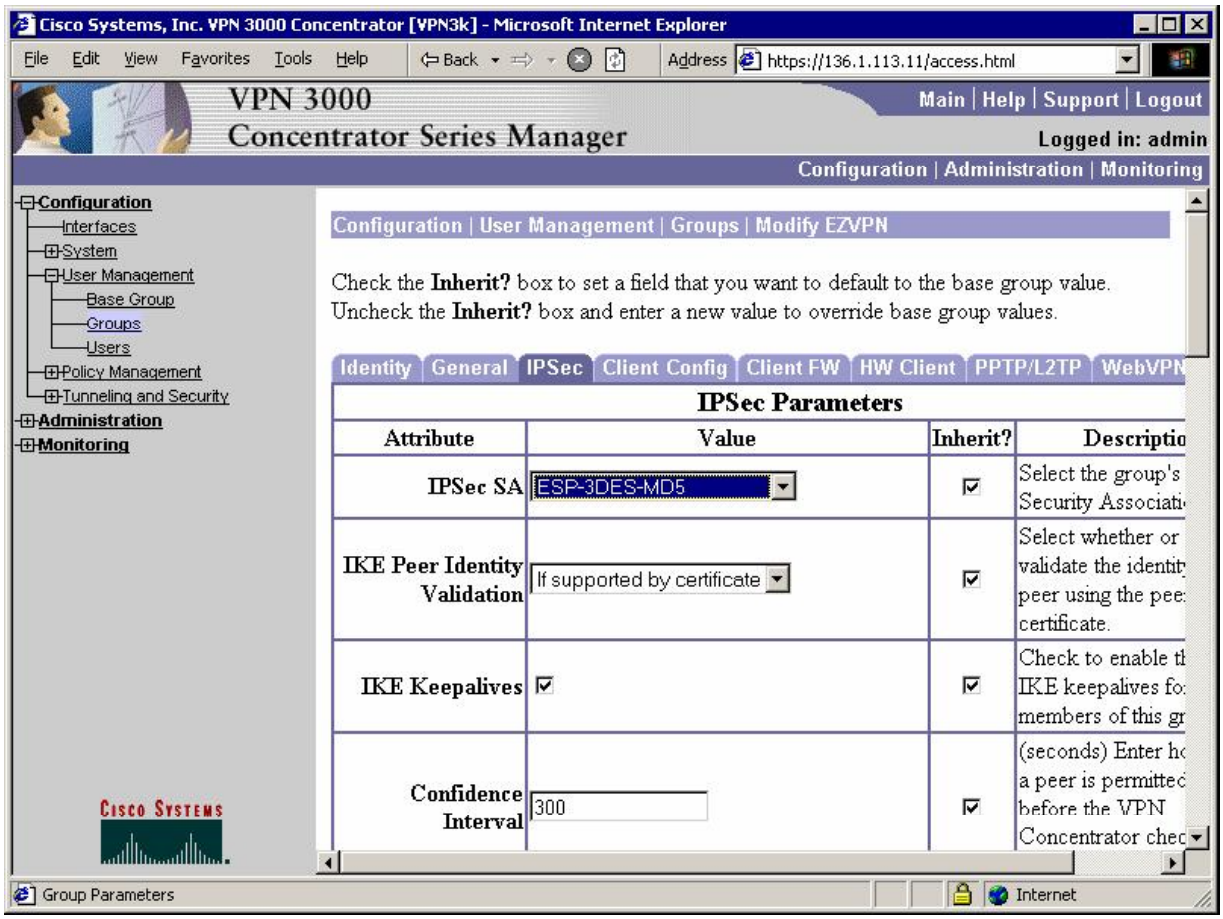


Modify the default IPsec SA "ESP-3DES-MD5":

Choose the digital certificate you have obtained for authentication:

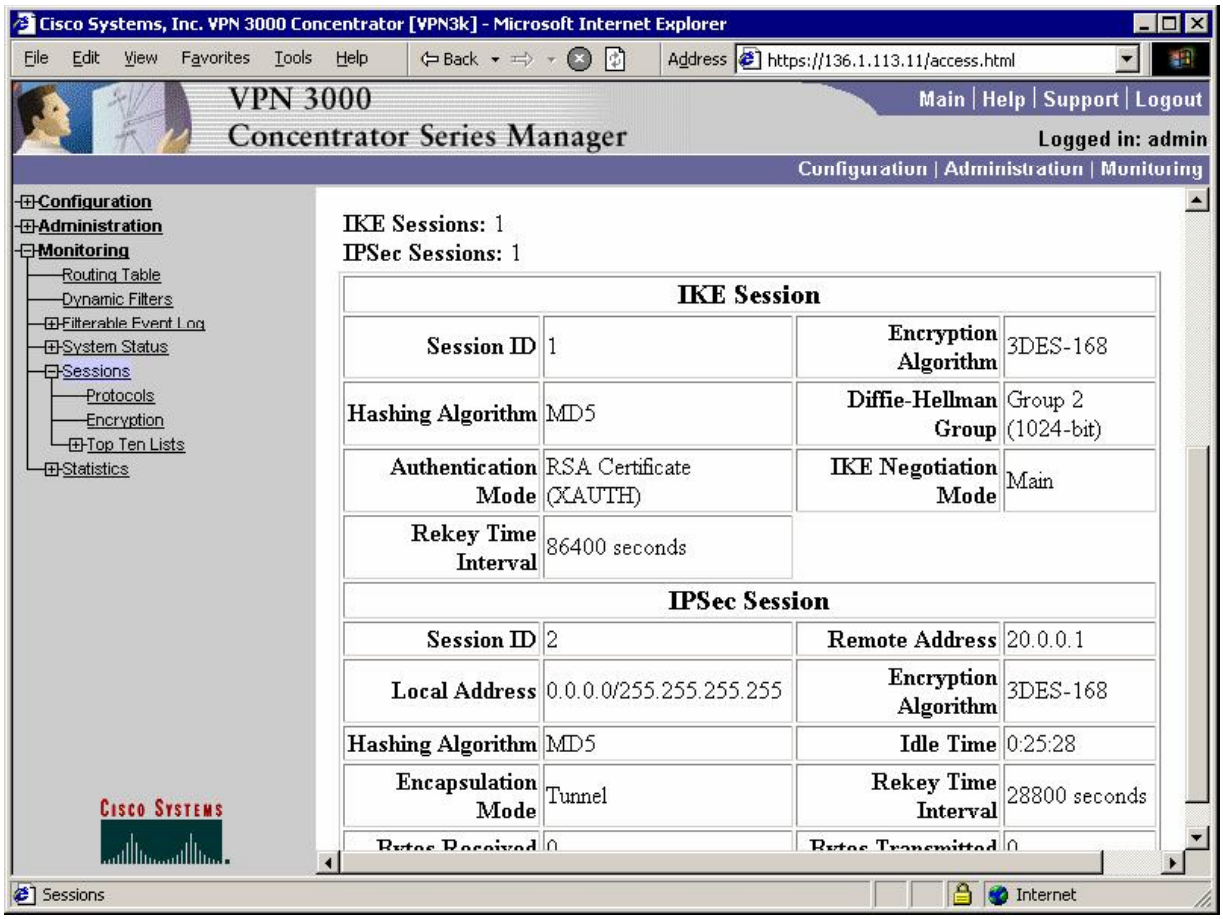


Make sure this SA is assigned to group EZVPN:



Verification

Connect Cisco VPN Client and monitor session on VPN3k:

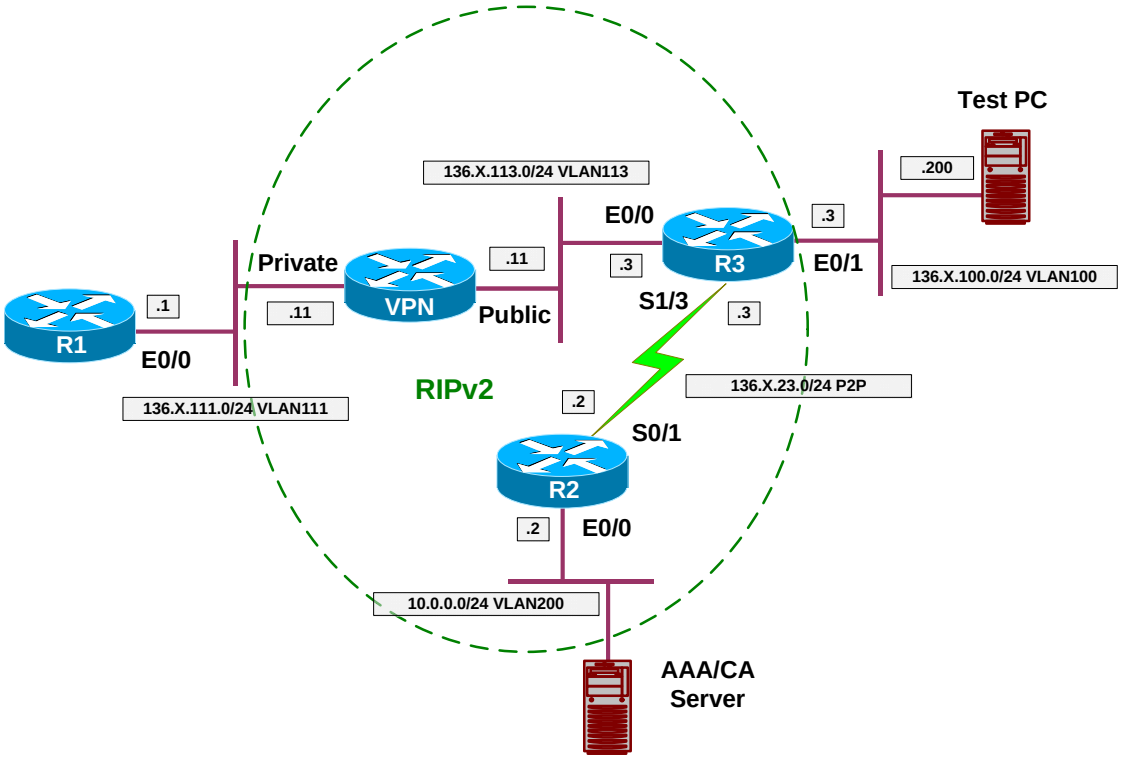


Further Reading

[Cisco - Configuring the VPN 3000 Concentrator to Communicate with the VPN Client Using Certificates]

VPN3k and IOS ezVPN Remote Client Mode with Split-Tunneling

Objective: Configure VPN3k to support IOS ezVPN Remote feature in Client mode.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "VPN3k ezVPN".
- In this task, R3 will be configured as ezVPN Remote device in Client mode. That is, it will simulate VPN Client behavior, requesting new IP address from VPN3k server.
- Create ezVPN client group on R3:
  - Use group name EZVPN with key CISCO.
  - Use peer 136.1.113.11.
  - Specify connect mode manual.
  - Specify client mode.
  - Configure E0/0 as outside interface.
  - Configure E0/1 as inside interface.
- Create network list to distinguish network 136.1.111.0/24, name it SPLIT_TUNNEL.
- Create new Group on VPN 3000 Concentrator:
  - Name EZVPN password CISCO.

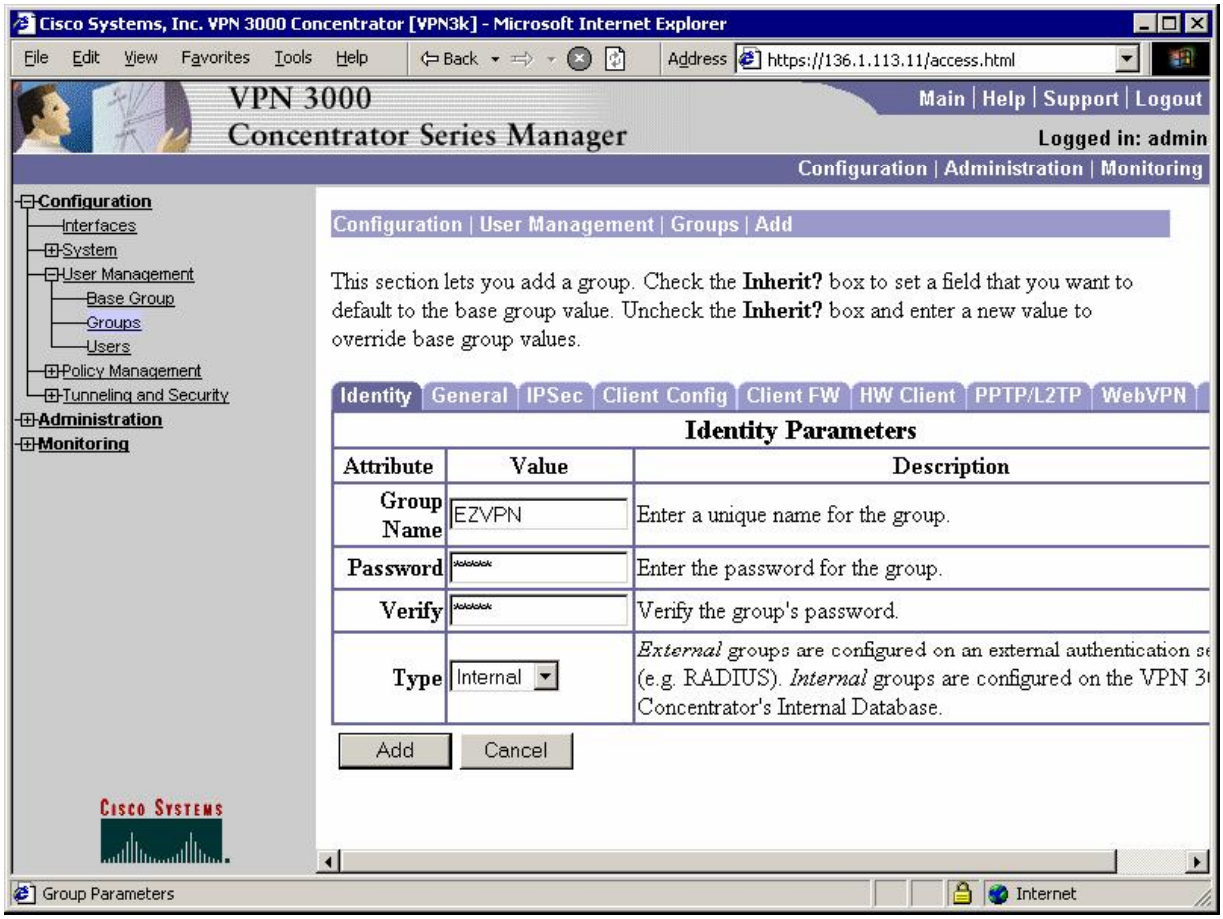
    - Configure IPsec as the only tunneling protocol.
    - Configure IPsec Remote Access Tunnel Type.
    - Configure IPsec Xauth.
- Modify group EZVPN, changing split-tunneling settings under “Client Config” Tab:
    - Tunnel only to networks in list.
    - Use network list SPLIT_TUNNEL.
- Assign Address Pool “20.0.0.1-20.0.0.254” to group EZVPN.
- Create new User on VPN 3000:
    - Name CISCO password CISCO1234
    - Group EZVPN
- Permit address allocation from Address Pools.

Final Configuration

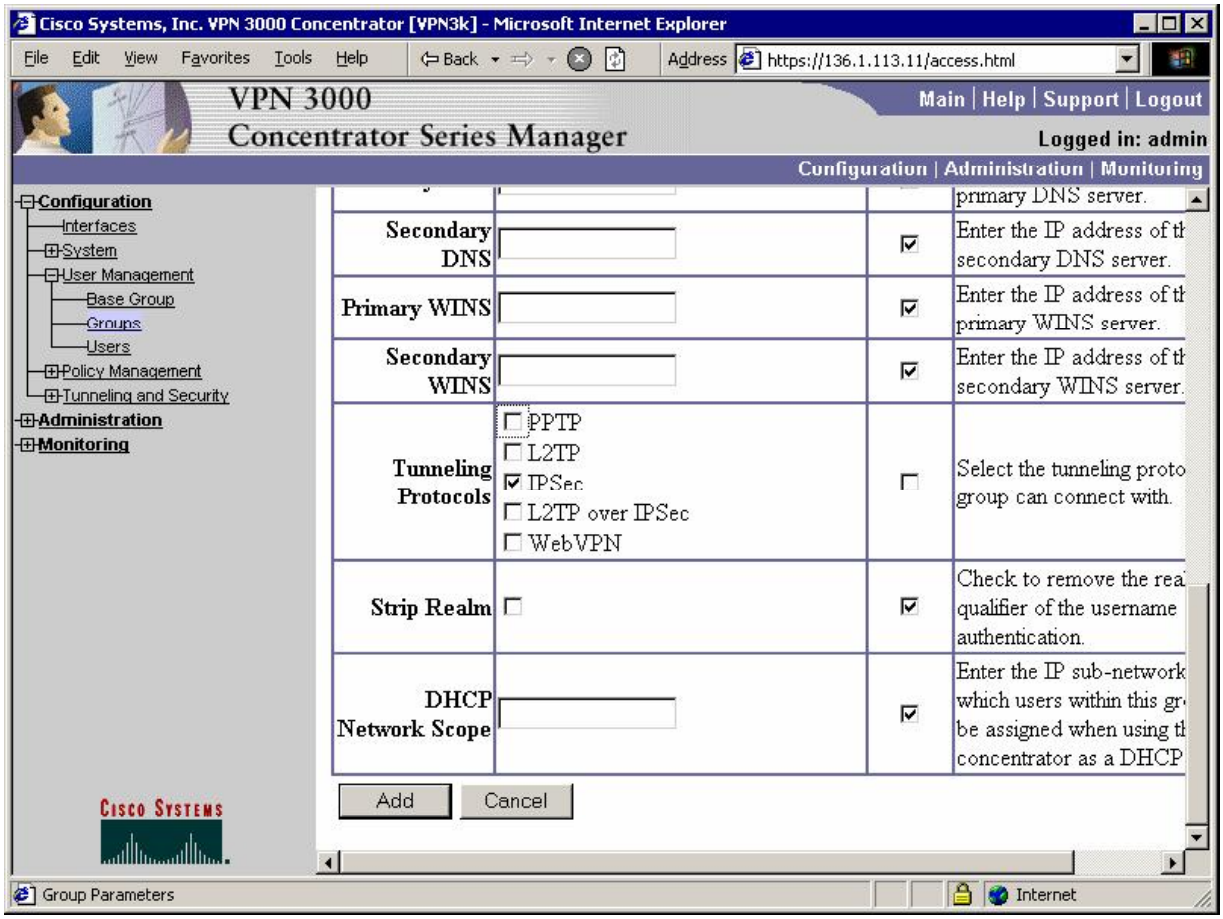
```
R3:
crypto ipsec client ezvpn EZVPN
 connect manual
 group EZVPN key CISCO
 mode client
 peer 136.1.113.11
!
interface Ethernet0/0
 crypto ipsec client ezvpn EZVPN
!
interface Ethernet0/1
 crypto ipsec client ezvpn EZVPN inside
```


VPN3k:

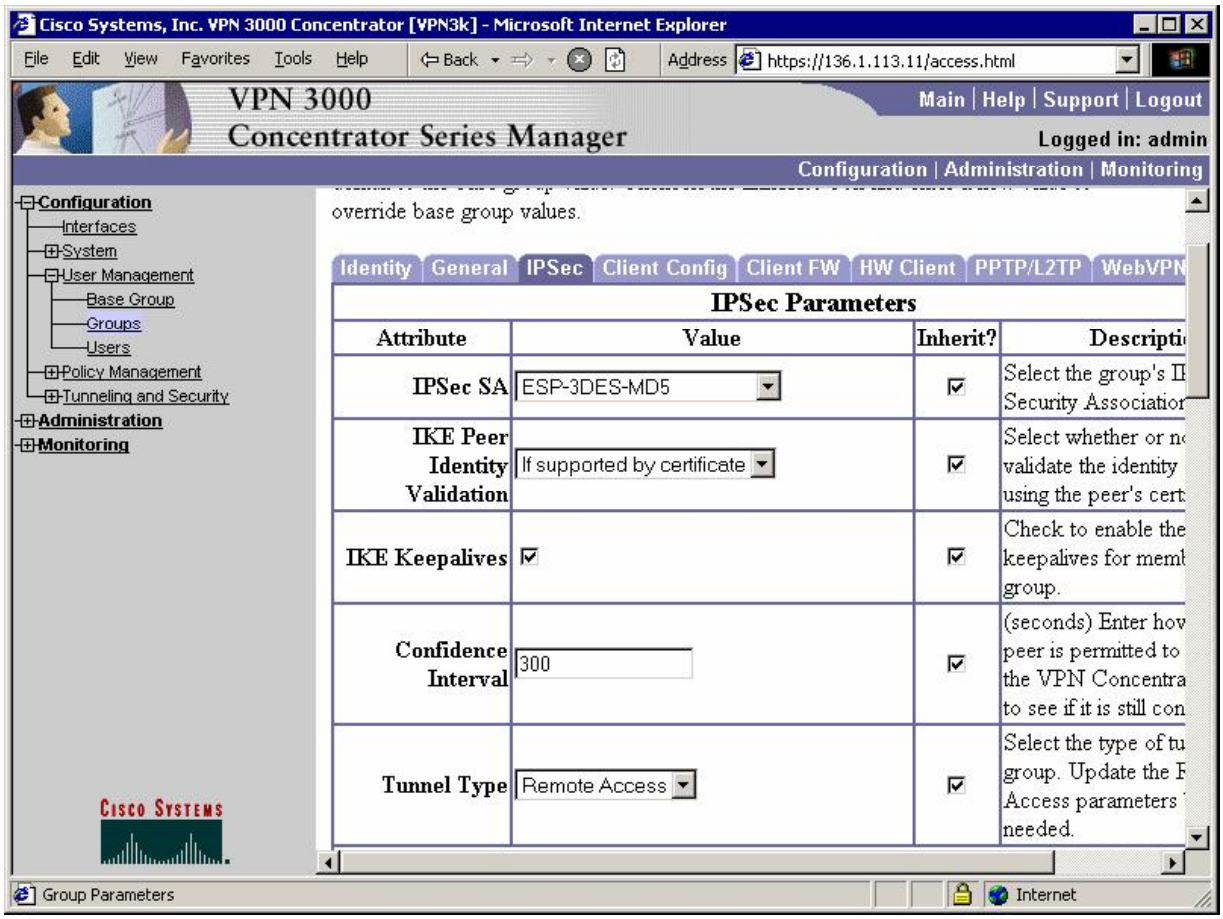
Create new group:



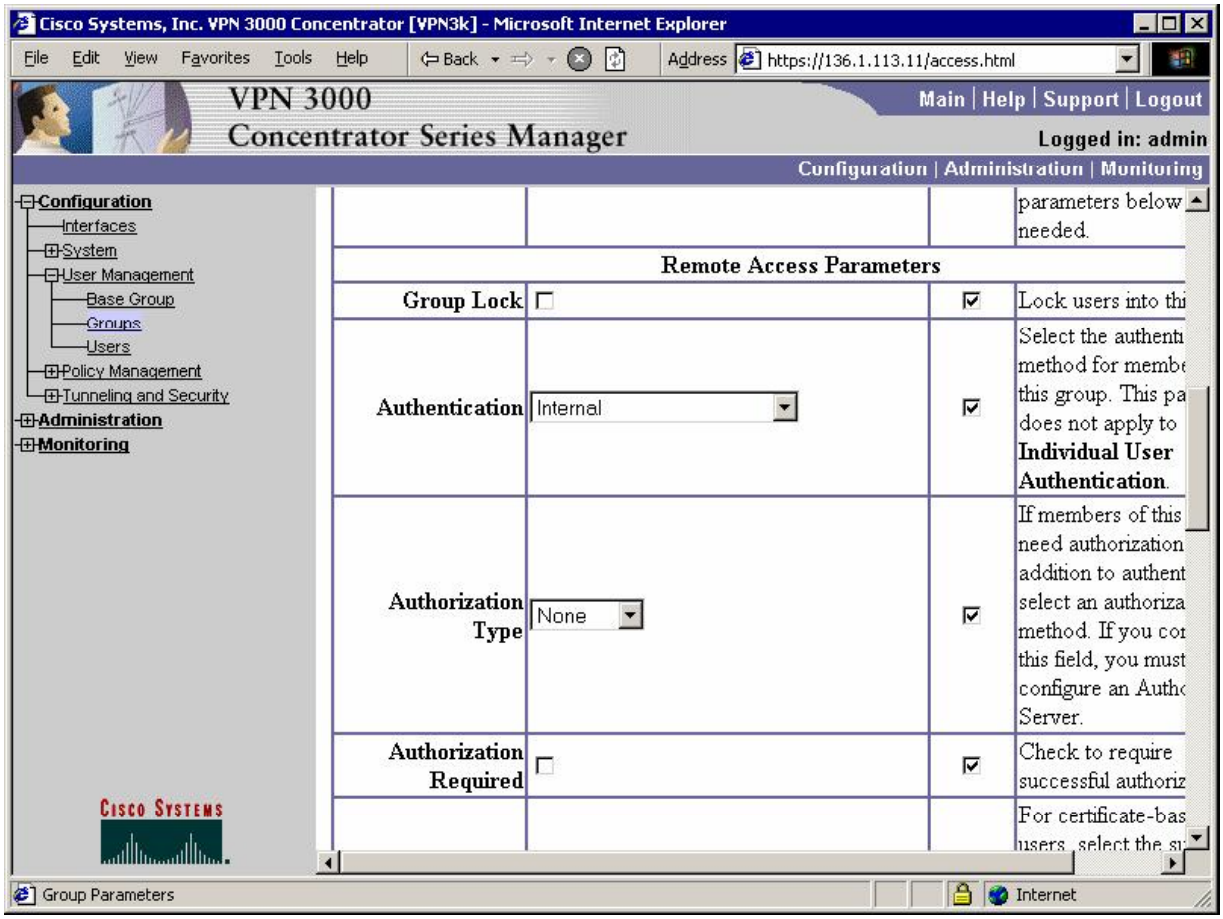
Permit IPsec as the only tunneling protocol in General Tab:



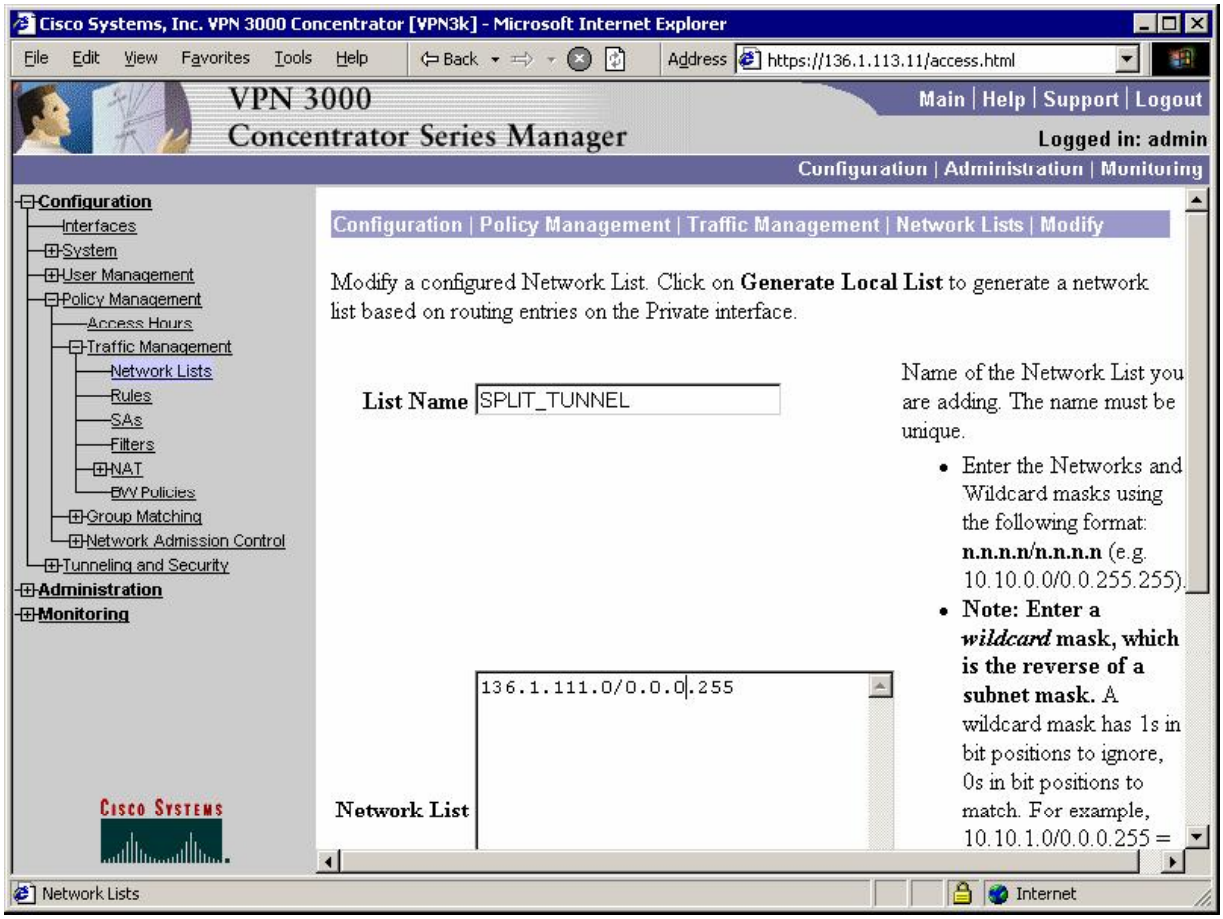
Make sure yoru group has Remote Access IPSec tunnel type:



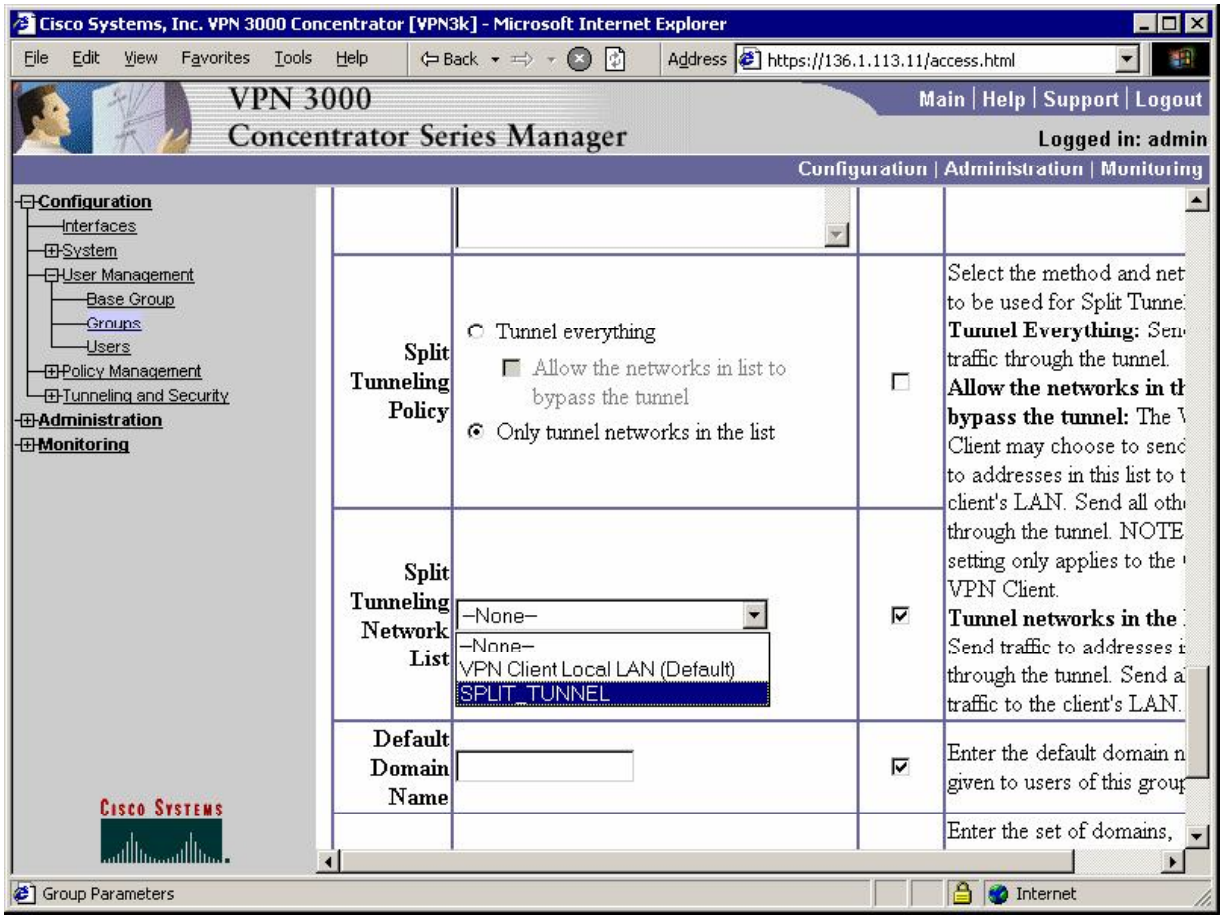
And that you have authentication (Xauth) enabled in IPsec Tab:



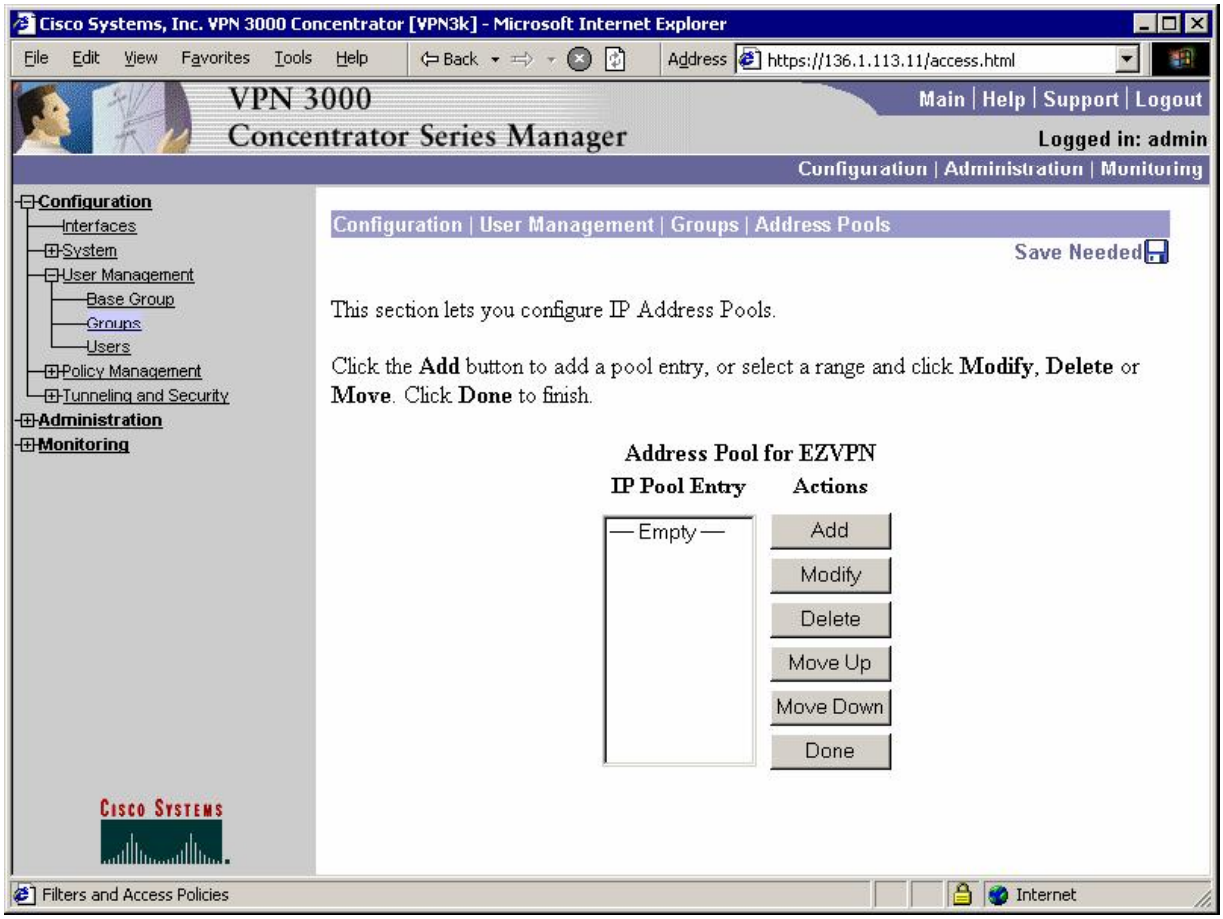
Create Network List for split-tunneling:

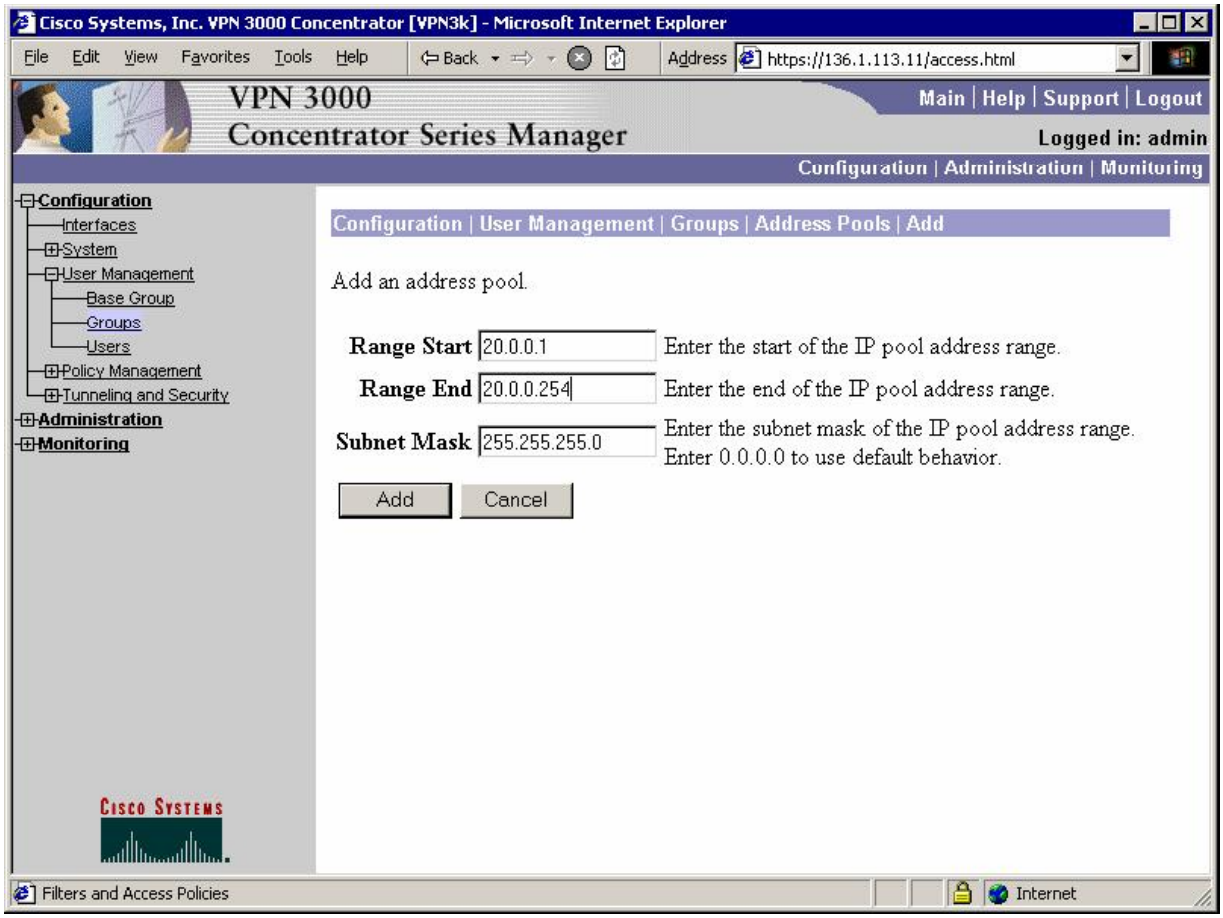


Modify group "EZVPN", "Client Config" Tab. Chose "Only tunnel networks in the list":

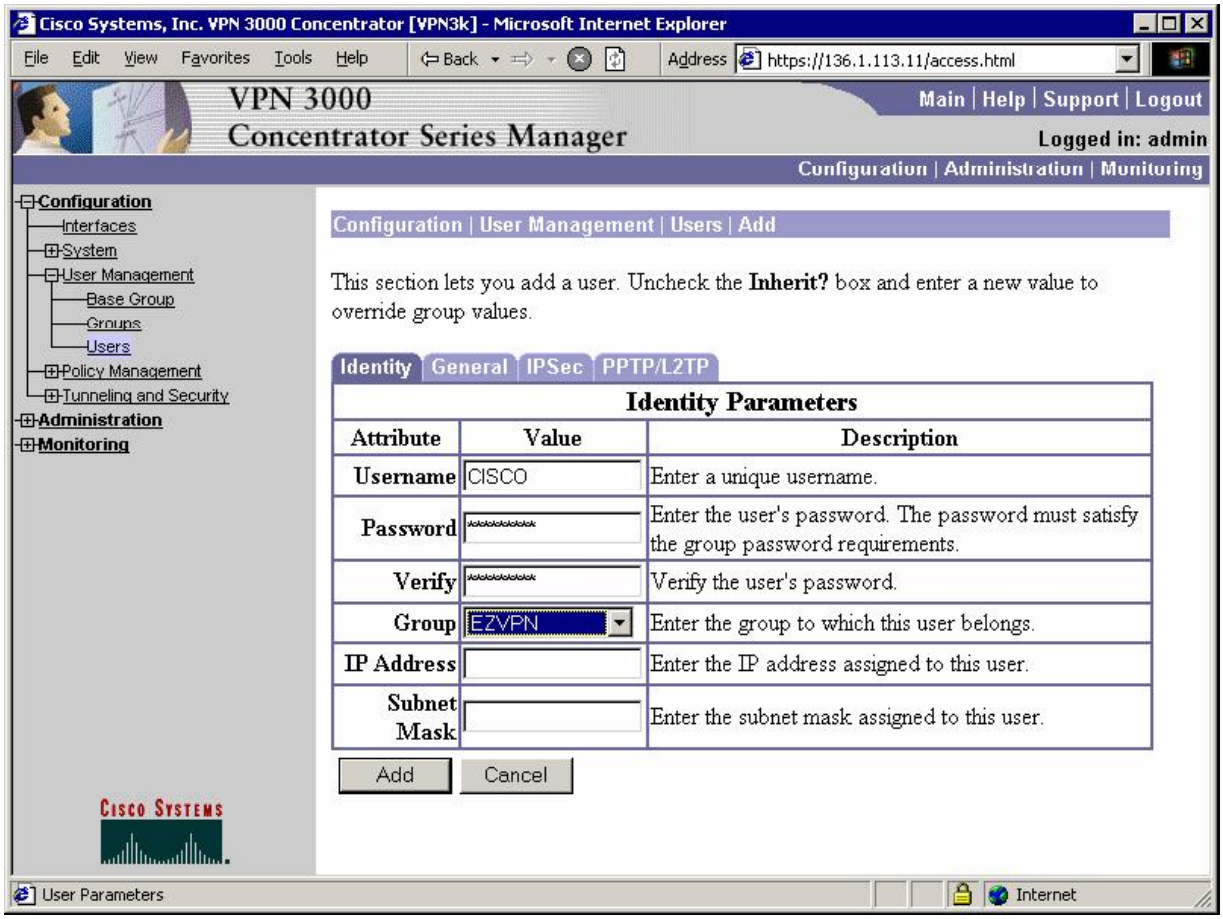


Modify address pools for a Group:

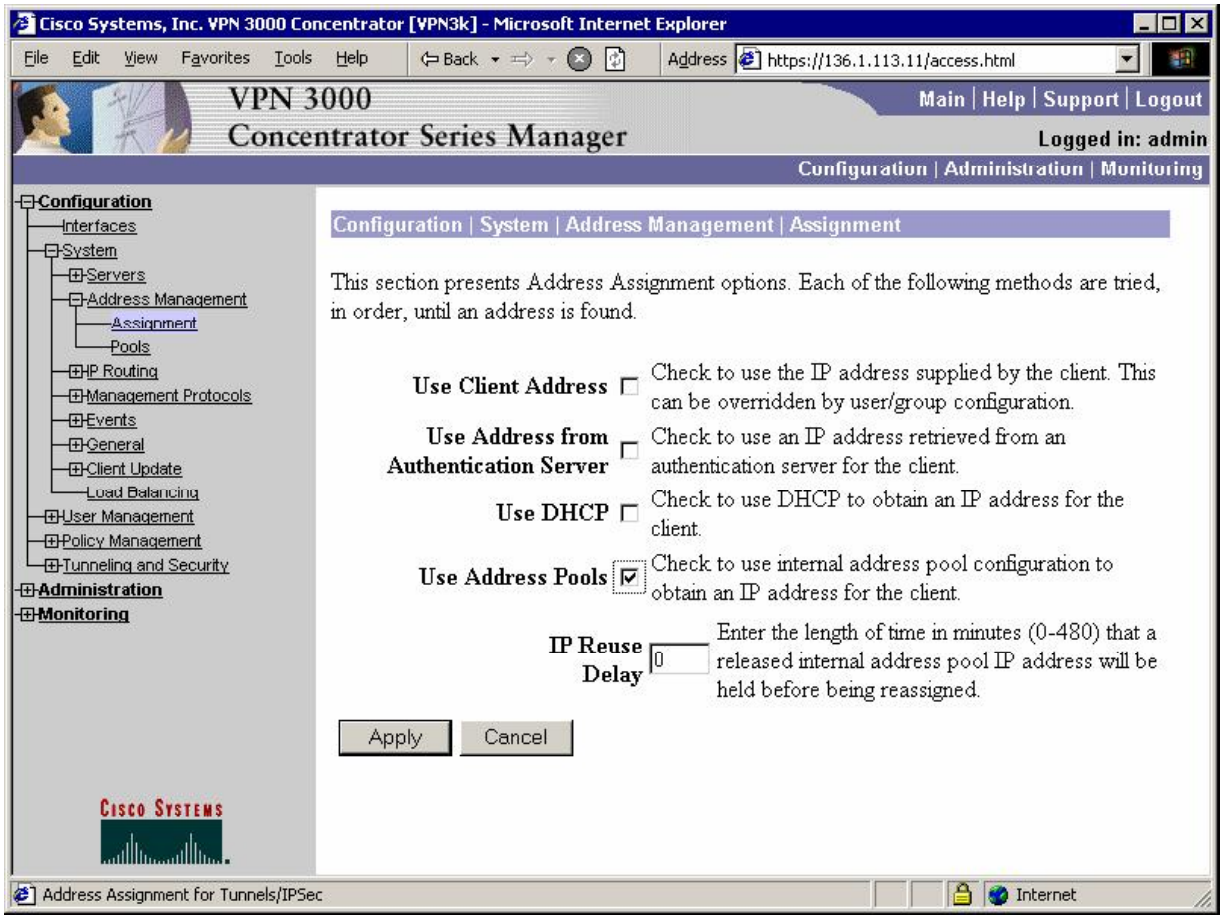



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Tunneling and Security
Administration
Monitoring
Configuration | User Management | Groups | Address Pools | Add
Add an address pool.
Range Start 20.0.0.1 Enter the start of the IP pool address range.
Range End 20.0.0.254 Enter the end of the IP pool address range.
Subnet Mask 255.255.255.0 Enter the subnet mask of the IP pool address range. Enter 0.0.0.0 to use default behavior.
Add
Cancel
Cisco Systems
Filters and Access Policies
Internet

Add new user "CISCO/CISCO1234" to group "EZVPN":



Allow IP address Assignment from Address Pools:



Verification

```
R3#crypto ipsec client ezvpn connect
R3#
*Mar  2 02:30:23.220: EZVPN(EZVPN): Pending XAuth Request, Please enter the
following command:
*Mar  2 02:30:23.220: EZVPN: crypto ipsec client ezvpn xauth

R3#crypto ipsec client ezvpn xauth
Enter Username and Password.: CISCO
Password: : CISCO1234

R3#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : EZVPN
Inside interface list: Ethernet0/1,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 20.0.0.1
Mask: 255.255.255.255
Split Tunnel List: 1
```

```
       Address    : 136.1.111.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0

R3#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list internet-list interface Ethernet0/0 refcount 0
[Id: 1] access-list enterprise-list pool EZVPN refcount 0
 pool EZVPN: netmask 255.255.255.0
        start 20.0.0.1 end 20.0.0.1
        type generic, total addresses 1, allocated 0 (0%), misses 0

R3#ping 136.1.111.1 source ethernet 0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.111.1, timeout is 2 seconds:
Packet sent with a source address of 136.1.100.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms

R3# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 20.0.0.1:8471     136.1.100.3:8471   136.1.111.1:8471   136.1.111.1:8471
icmp 20.0.0.1:8472     136.1.100.3:8472   136.1.111.1:8472   136.1.111.1:8472
icmp 20.0.0.1:8473     136.1.100.3:8473   136.1.111.1:8473   136.1.111.1:8473
icmp 20.0.0.1:8474     136.1.100.3:8474   136.1.111.1:8474   136.1.111.1:8474
icmp 20.0.0.1:8475     136.1.100.3:8475   136.1.111.1:8475   136.1.111.1:8475

R3#sh cry isakmp sa
dst             src             state          conn-id slot
136.1.113.11    136.1.113.3     QM_IDLE              1    0

R3#show cry ipsec sa

interface: Ethernet0/0
    Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.113.3

   protected vrf:
   local  ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (136.1.111.0/255.255.255.0/0/0)
   current_peer: 136.1.113.11:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.113.3, remote crypto endpt.: 136.1.113.11
     path mtu 1500, media mtu 1500
     current outbound spi: 31B8C3A
```

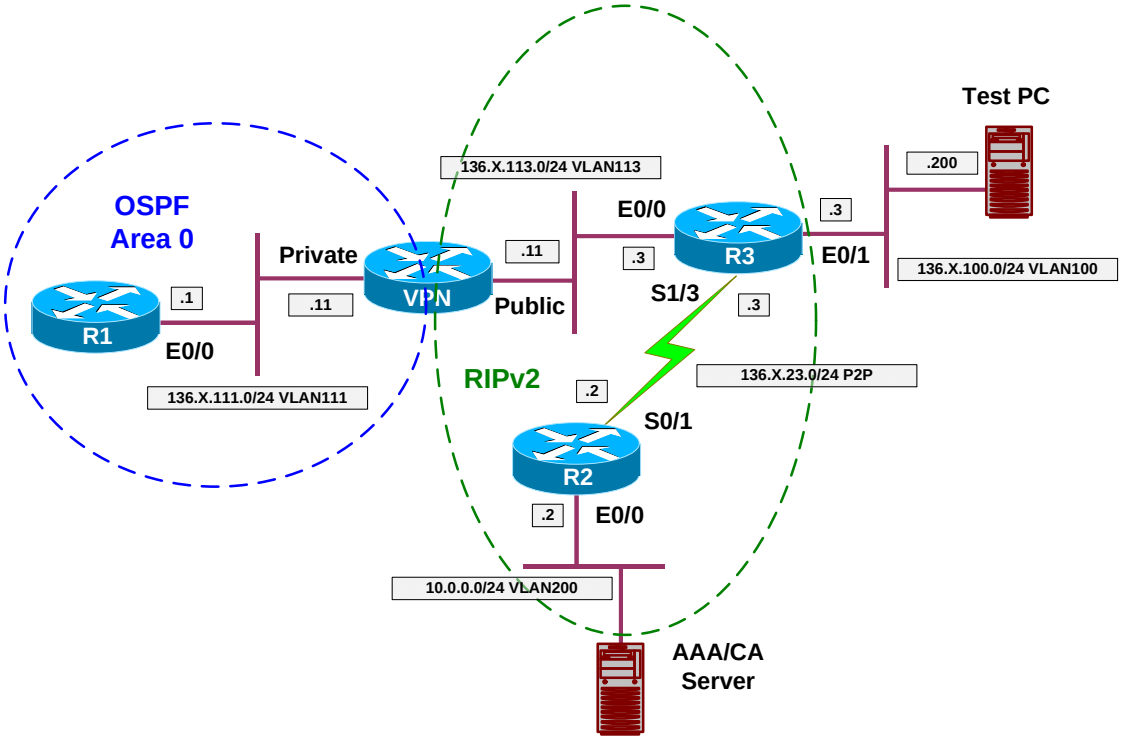
```
inbound esp sas:
 spi: 0xC5A8C13C(3316171068)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
   sa timing: remaining key lifetime (k/sec): (4539243/27495)
   IV size: 8 bytes
   replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x31B8C3A(52137018)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
   sa timing: remaining key lifetime (k/sec): (4539243/27495)
   IV size: 8 bytes
   replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

Further Reading

ezVPN Remote Phase I

VPN3k and IOS ezVPN Remote NW Extension Mode with RRI

Objective: Configure VPN3k for ezVPN Remote in network extension mode with RRI into OSPF.



Directions

- Configure devices as per the scenario " VPN/ezVPN" "VPN3k and IOS ezVPN Remote Client Mode with Split Tunneling".
- Re-configure R3, and change ezVPN mode to "network-extension".
- Network Extension mode does not need an additional IP address from VPN 3000, and router does not enable NAT automatiacally.
- Therefore, you may disable IP address allocation in global Configuration.
- Additionally, you need to permit network extenstion mode, under "HW Client" Tab of group "EZVPN".
- The key point with RRI into OSPF is to configure ASBR feature on the VPN3k, so that it starts advertising external routes into OSPF.
- Also, you have to enable Network Extension RRI under IP Routing Configuration.
- Configure R1:
    - Remove static default route on R1 and configure OSPF routing as per the diagram.
- Enable OSPF process on VPN3k
    - Use router-id 150.X.11.11.

  - Permit ASBR feature
- Enable OSPF on the Private interface of the VPN3k. Use Area 0.

Final Configuration

```
R1:
no ip route 0.0.0.0 0.0.0.0 136.1.111.11
!
router ospf 1
 network 136.1.111.0 0.0.0.255 area 0

VPN3k CLI:

Configure OSPF on the Private Interface:

1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3k: Config -> 2

1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back

VPN3k: System -> 3

1) Static Routes
2) Default Gateways
3) OSPF
4) OSPF Areas
5) DHCP Parameters
6) Redundancy
7) Reverse Route Injection
8) DHCP Relay
9) Back

VPN3k: Routing -> 3

1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
```

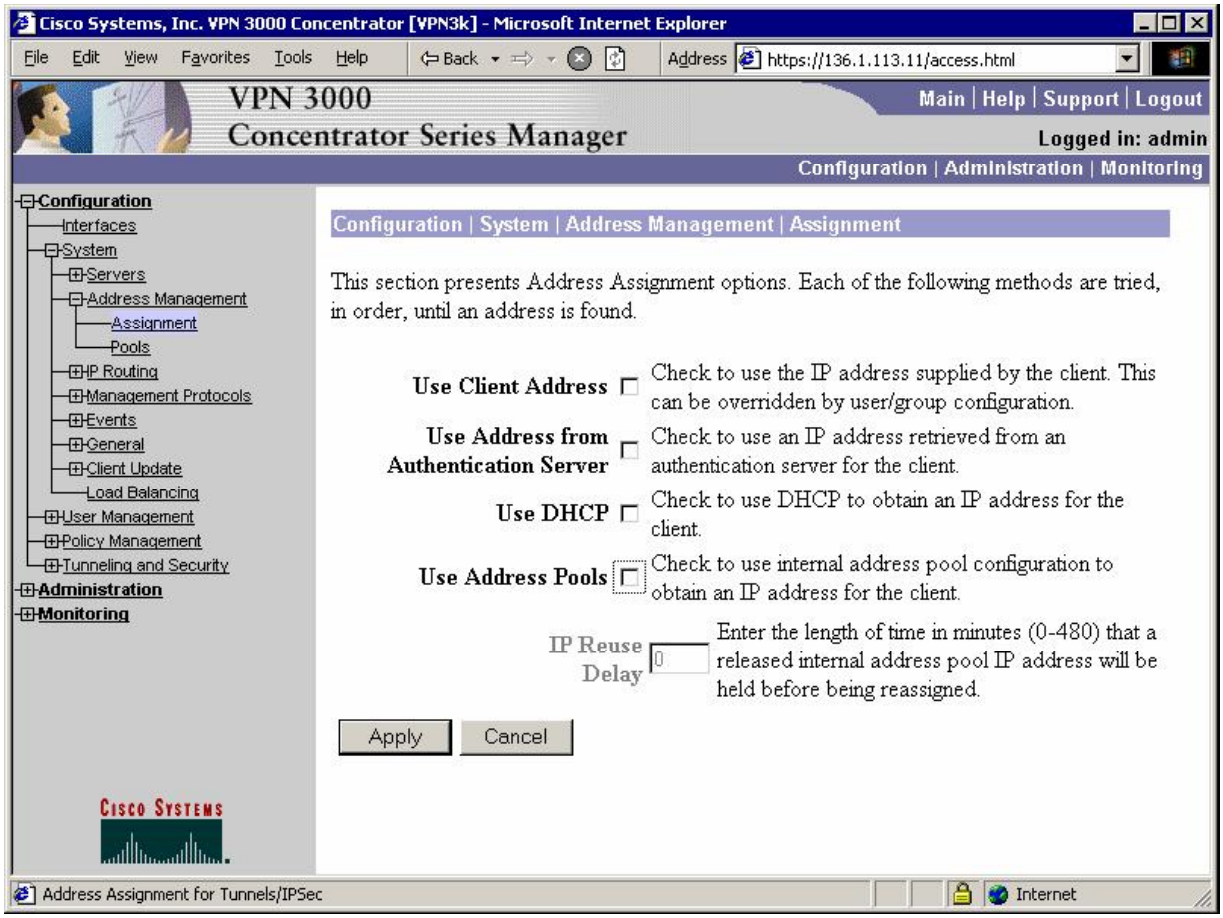
```
VPN3k: OSPF -> 2

> Router ID

VPN3k: OSPF -> [ 0.0.0.0 ] 150.1.11.11

1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back

VPN3k: OSPF -> 1

1) Enable OSPF
2) Disable OSPF

VPN3k: OSPF -> [ 2 ] 1

1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back

VPN3k: OSPF -> 3

1) Enable Autonomous System
2) Disable Autonomous System

VPN3k: OSPF -> [ 2 ] 1

1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back

VPN3k: OSPF -> h

1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3k: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

VPN3k: Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Ether1-Pri|      UP      |   136.1.111.11/255.255.255.0  | 00.03.A0.88.BD.29
Ether2-Pub|      UP      |   136.1.113.11/255.255.255.0  | 00.03.A0.88.BD.2A
-------------------------------------------------------------------------------
```

```
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

VPN3k: Interfaces -> 1

1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Set Interface Name
4) Select IP Filter
5) Select Ethernet Speed
6) Select Duplex
7) Set MTU
8) Set Port Routing Config
9) Set Bandwidth Management
10) Set Public Interface IPSec Fragmentation Policy
11) Set Interface WebVPN Parameters
12) Back

VPN3k: Ethernet Interface 1 -> 8

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 1 -> 3

1) Enable OSPF
2) Disable OSPF

VPN3k: Ethernet Interface 1 -> [ 2 ] 1

1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back

VPN3k: Ethernet Interface 1 -> 4

1) Set OSPF Area ID
2) Set OSPF Priority
3) Set OSPF Metric
4) Set OSPF Retransmit Interval
5) Set OSPF Hello Interval
6) Set OSPF Dead Interval
7) Set OSPF Transit Delay
8) Set OSPF Authentication
9) Back

VPN3k: Ethernet Interface 1 -> 1

> OSPF Area ID

VPN3k: Ethernet Interface 1 -> [ 0.0.0.0 ] 0.0.0.0
```

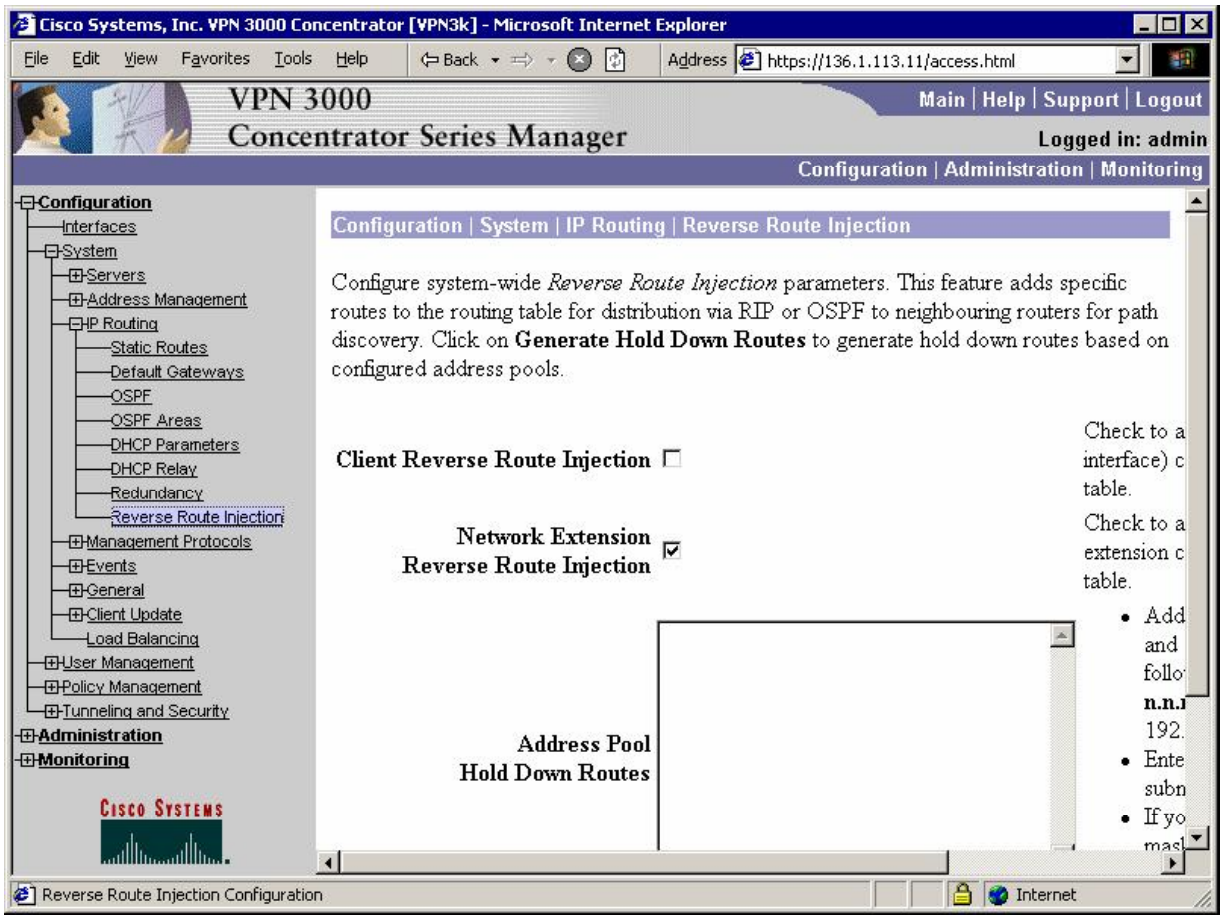
```
1) Set OSPF Area ID
2) Set OSPF Priority
3) Set OSPF Metric
4) Set OSPF Retransmit Interval
5) Set OSPF Hello Interval
6) Set OSPF Dead Interval
7) Set OSPF Transit Delay
8) Set OSPF Authentication
9) Back

VPN3k: Ethernet Interface 1 ->
```

VPN3k GUI:

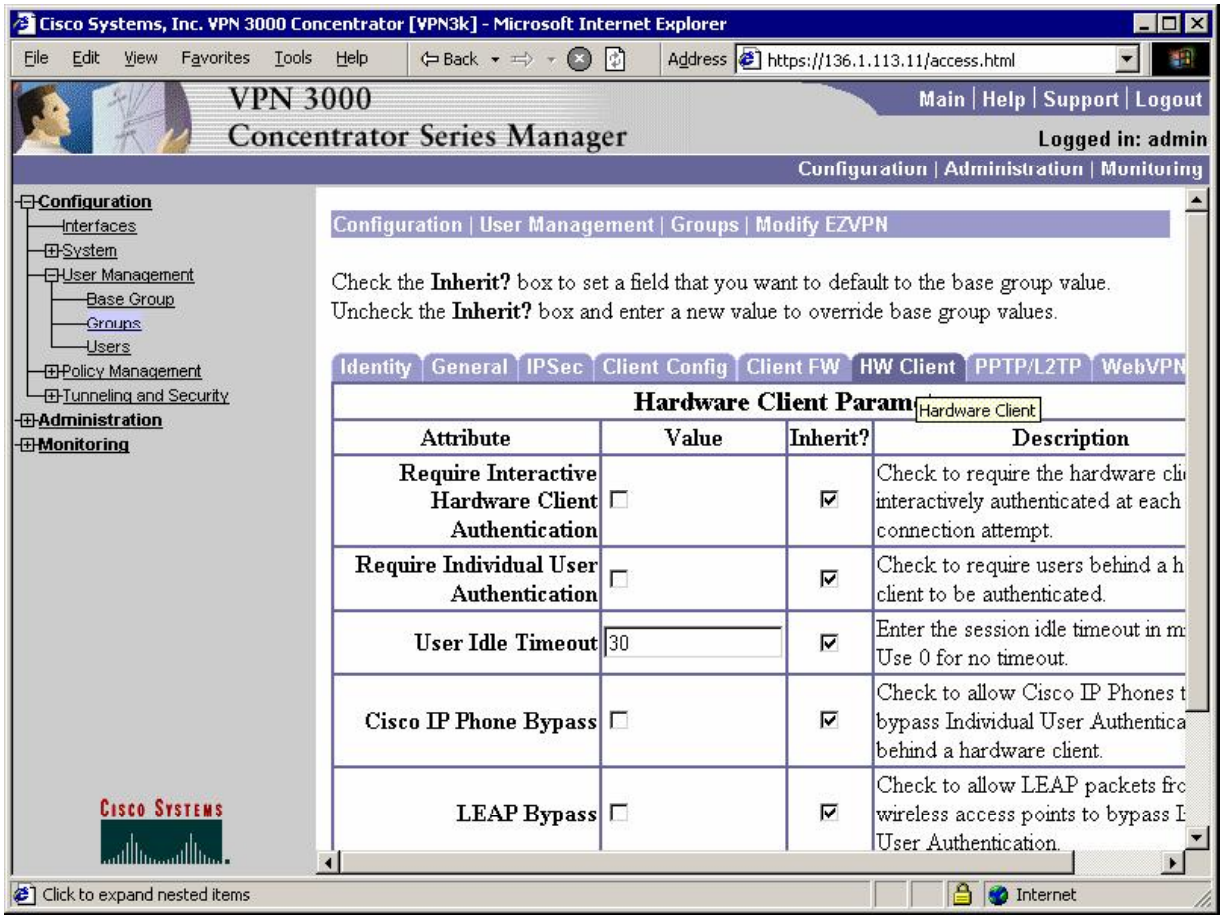
Disable address assignment:

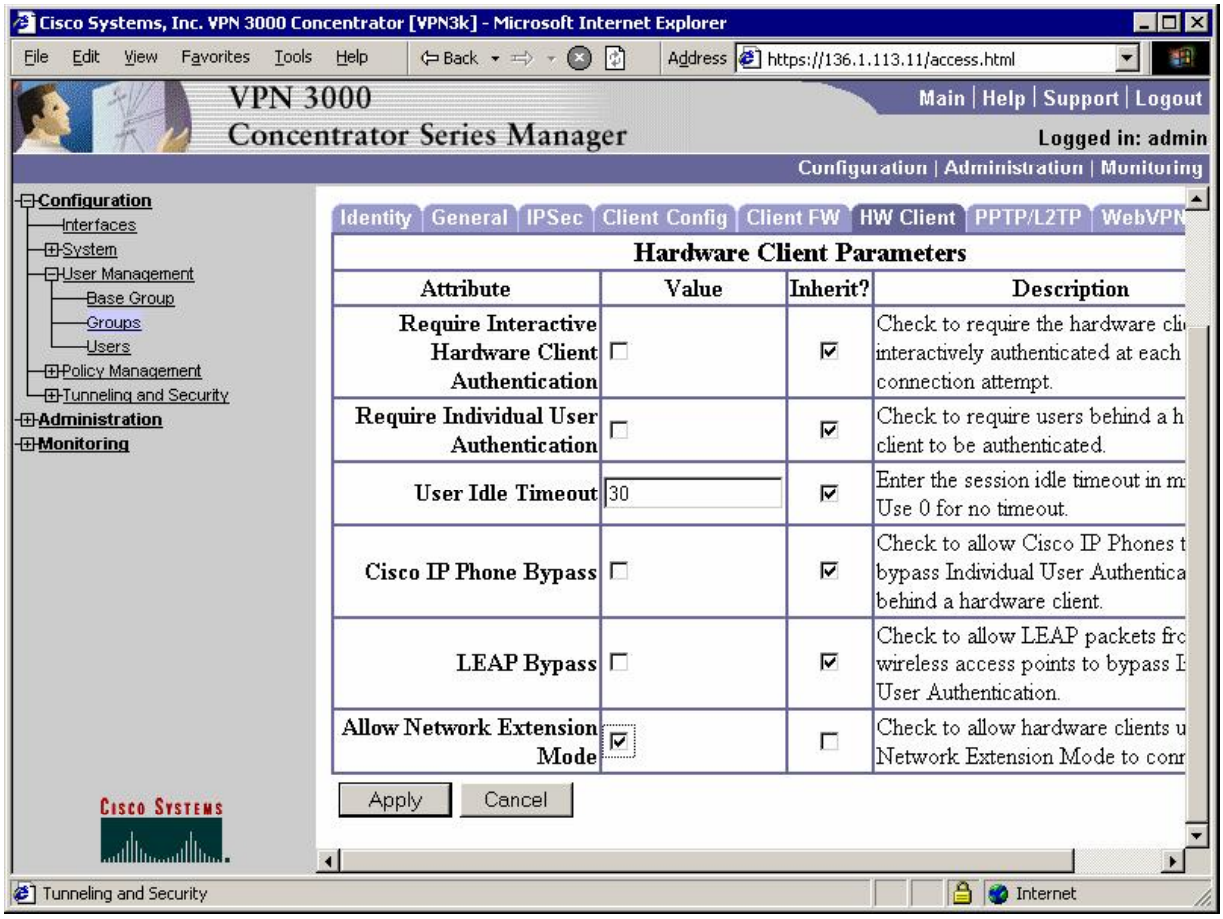


Enable RRI for Network Extension Prefixes:



Allow Network Extenstion mode for the group "EZVPN":





Verification

```
R3#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : EZVPN
Inside interface list: Ethernet0/1,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Split Tunnel List: 1
       Address    : 136.1.111.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0

R3#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 10  Misses: 10
Expired translations: 10
Dynamic mappings:
```

```
-- Inside Source
[Id: 3] access-list internet-list interface Ethernet0/0 refcount 0
```

Check for RRI-injected route:

```
R1#show ip route ospf
     136.1.0.0/24 is subnetted, 4 subnets
O E2    136.1.0.0 [110/20] via 136.1.111.11, 23:54:52, Ethernet0/0
O E2    136.1.23.0 [110/20] via 136.1.111.11, 23:54:52, Ethernet0/0
O E2    136.1.100.0 [110/20] via 136.1.111.11, 00:00:27, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
O E2    10.0.0.0 [110/20] via 136.1.111.11, 23:54:52, Ethernet0/0

R1#ping 136.1.100.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.100.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
R1#

R3#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.113.11    136.1.113.3     QM_IDLE              1    0

R3#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.113.3

   protected vrf:
   local  ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.111.0/255.255.255.0/0/0)
   current_peer: 136.1.113.11:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.113.3, remote crypto endpt.: 136.1.113.11
     path mtu 1500, media mtu 1500
     current outbound spi: 1D1B61D3

     inbound esp sas:
      spi: 0xCA9D083A(3399288890)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4434055/28659)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1D1B61D3(488333779)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
```

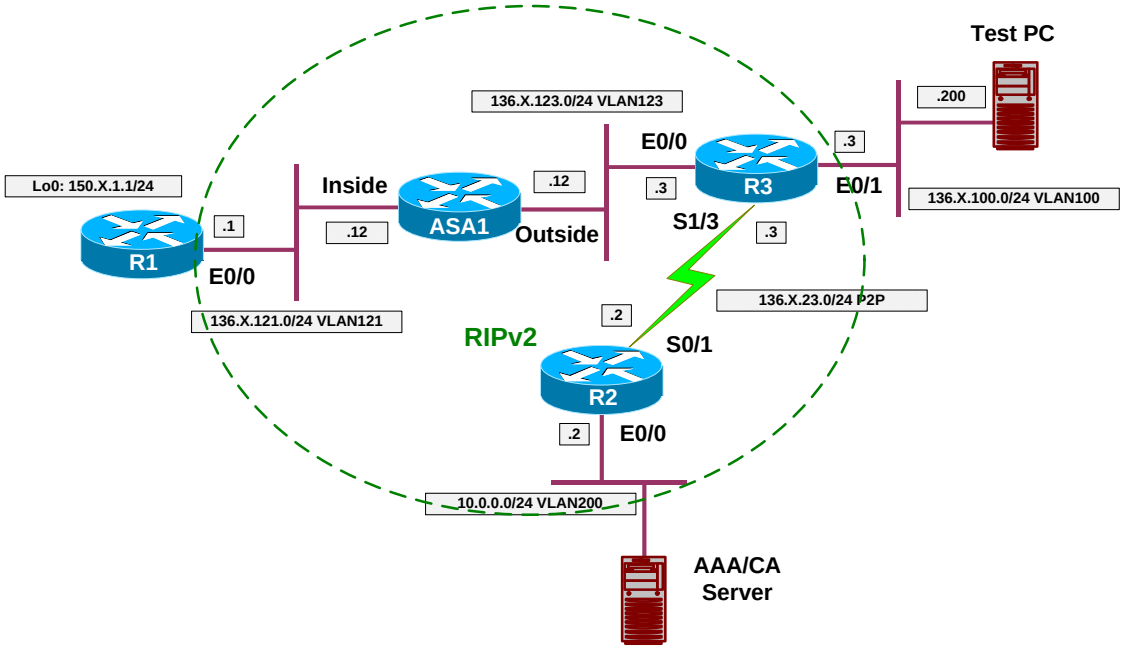
```
        slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4434055/28659)
        IV size: 8 bytes
        replay detection support: Y

    outbound ah sas:

    outbound pcp sas:
```

Further Reading

Configuring the Cisco EzVPN Client on Cisco IOS with the VPN 3000 Concentrator

IOS and IOS ezVPN Remote Client Mode with Xauth/RRI

Objective: Configure IOS router to support ezVPN Remote connections and redistribute connected host routes.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "IOS ezVPN".
- Configure R3 as ezVPN Server:
  - Enable AAA and make sure console is unaffected.
  - Configure ISAKMP Policy.
    - Use DH Group 2.
    - Use 3DES cipher.
    - Use MD5 hash.
    - Use Pre-Shared authentication.
  - Configure IP addressing for remote clients.
    - Create local IP address pool EZVPN: 20.0.0.1-20.0.0.254.
    - Configure ISAKMP to use this pool.
  - Configure split-tunneling ACL, name it "SPLIT_TUNNEL":
    - Permit network 136.X.100.0/24 to be tunneled.
  - Configure ISAKMP Authorization parameters.
    - Configure network AAA authorization list named EZVPN, user local database.
    - Create ISAKMP configuration group "EZVPN":
      - Specify key "CISCO".

            - Use local pool “EZVPN”.
            - Use split-tunnel list “SPLIT_TUNNEL”.
        - Configure crypto-map VPN to use ISAKMP authorization list “EZVPN”.
        - Configure crypto-map VPN to respond to IKE configuration requests.
    - Configure client authentication:
        - Configure AAA authentication list for login named “EZVPN”, use local database.
        - Create local username CISCO with password CISCO1234.
        - Configure crypto-map VPN to use client authentication AAA list EZVPN. This will activate Xauth.
    - Configure crypto:
        - Create crypto transform-set 3DES_MD5:
            - Use 3DES cipher.
            - Use MD5 hash.
        - Create dynamic crypto-map DYNAMIC:
            - Apply 3DES_MD5 transform-set.
            - Enable reverse-route injection
        - Configure crypto-map VPN entry 10:
            - Use type IPsec-ISAKMP.
            - Use dynamic crypt-map DYNAMIC.
            - Apply crypto-map to interface Eth0/0.
    - Redistribute static routes into RIP. This way you make remote router visible in the routing domain.
- Configure R1 as ezVPN Remote in client mode:
    - Create ezVPN group named “EZVPN”:
        - Use group name “EZVPN” and key CISCO.
        - Specify manual connect mode.
        - Specify peer 136.X.123.3
    - Configure interface Ethernet 0/0 as ezVPN outside
    - Configure interface Loopback0 as ezVPN inside.

Final Configuration

```
R3:
aaa new-model
aaa authentication login CONSOLE none
!
! ezVPN Authorization & Authentication
!
aaa authorization network EZVPN local
aaa authentication login EZVPN local
!
! Local username for Xauth
!
username CISCO pass CISCO1234
!
line con 0
```

```
  login authentication CONSOLE
!
! Configure ISAKMP policy
! Note the pre-shared key and group 2
! DH Group 2 should be used for ezVPN Remote
!
crypto isakmp policy 10
 authentication pre-share
 encr 3des
 hash md5
 group 2
!
! Configure local address pool
! Configure ISAKMP to use this address pool
!
ip local pool EZVPN 20.0.0.1 20.0.0.254
crypto isakmp client configuration address-pool local EZVPN
!
! Split-tunnel ACL
!
ip access-list extended SPLIT_TUNNEL
 permit ip 136.1.100.0 0.0.0.255 any
!
!  Configure ISAKMP Group
!
crypto isakmp client configuration group EZVPN
  key CISCO
  pool EZVPN
  acl SPLIT_TUNNEL
!
! Configure IPsec transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Dynamic crypto map
!
crypto dynamic-map DYNAMIC  10
  set transform-set 3DES_MD5
  reverse-route
!
! RRI into RIP
!
router rip
 redistribute static
!
! Configure crypto-map for authorization & authentication
!
crypto map VPN isakmp authorization list EZVPN
!
! Activating client authentication enables Xauth
!
crypto map VPN client authentication list EZVPN
crypto map VPN client configuration address respond
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
!
! Attach crypto-map to an interface
!
interface E 0/0
 crypto map VPN
```

R1:

```
crypto ipsec client ezvpn EZVPN
```

```
  group EZVPN key CISCO
  connect manual
  peer 136.1.123.3
!
interface E 0/0
 crypto ipsec client ezvpn EZVPN
!
interface Loopback0
 crypto ipsec client ezvpn EZVPN  inside
```

Verification

```
R1#crypto ipsec client ezvpn connect

*Mar  1 00:09:10.577: EZVPN(EZVPN): Pending XAuth Request, Please enter the
following command:
*Mar  1 00:09:10.577: EZVPN: crypto ipsec client ezvpn xauth

R1#crypto ipsec client ezvpn xauth
Username: : CISCO
Password: : CISCO1234

R1#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : EZVPN
Inside interface list: Loopback0,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 20.0.0.2
Mask: 255.255.255.255
Split Tunnel List: 1
       Address    : 136.1.100.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0

R1#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Loopback0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list internet-list interface Ethernet0/0 refcount 0
[Id: 1] access-list enterprise-list pool EZVPN refcount 0
 pool EZVPN: netmask 255.255.255.0
        start 20.0.0.2 end 20.0.0.2
        type generic, total addresses 1, allocated 0 (0%), misses 0

R1#ping 136.1.100.3 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.100.3, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/12 ms

R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 20.0.0.2:3391     150.1.1.1:3391     136.1.100.3:3391   136.1.100.3:3391
icmp 20.0.0.2:3392     150.1.1.1:3392     136.1.100.3:3392   136.1.100.3:3392
icmp 20.0.0.2:3393     150.1.1.1:3393     136.1.100.3:3393   136.1.100.3:3393
icmp 20.0.0.2:3394     150.1.1.1:3394     136.1.100.3:3394   136.1.100.3:3394
icmp 20.0.0.2:3395     150.1.1.1:3395     136.1.100.3:3395   136.1.100.3:3395

R1#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.121.1

   protected vrf:
   local  ident (addr/mask/prot/port): (20.0.0.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
   current_peer: 136.1.123.3:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.123.3
     path mtu 1500, media mtu 1500
     current outbound spi: 953B01EC

     inbound esp sas:
      spi: 0x734BD2AE(1934348974)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4588571/3570)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x953B01EC(2503672300)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4588571/3570)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

R3#show ip route static
     20.0.0.0/32 is subnetted, 1 subnets
S       20.0.0.2 [1/0] via 136.1.121.1

R2#show ip route rip
```

```
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.100.0 [120/1] via 136.1.23.3, 00:00:18, Serial0/1
R       136.1.121.0 [120/2] via 136.1.23.3, 00:00:18, Serial0/1
R       136.1.123.0 [120/1] via 136.1.23.3, 00:00:18, Serial0/1
     20.0.0.0/32 is subnetted, 1 subnets
R       20.0.0.2 [120/1] via 136.1.23.3, 00:00:18, Serial0/1
     150.1.0.0/24 is subnetted, 2 subnets
R       150.1.1.0 [120/3] via 136.1.23.3, 00:00:18, Serial0/1

R3#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
1     136.1.123.3     136.1.121.1              3des md5       2  23:55:49 CX

R3#show crypto ipsec sa

interface: Ethernet0/0
   Crypto map tag: VPN, local addr. 136.1.123.3

   protected vrf:
   local  ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (20.0.0.2/255.255.255.255/0/0)
   current_peer: 136.1.121.1:500
     PERMIT, flags={}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.121.1
     path mtu 1500, media mtu 1500
     current outbound spi: 734BD2AE

     inbound esp sas:
      spi: 0x953B01EC(2503672300)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4384197/3348)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x734BD2AE(1934348974)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4384197/3348)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
```

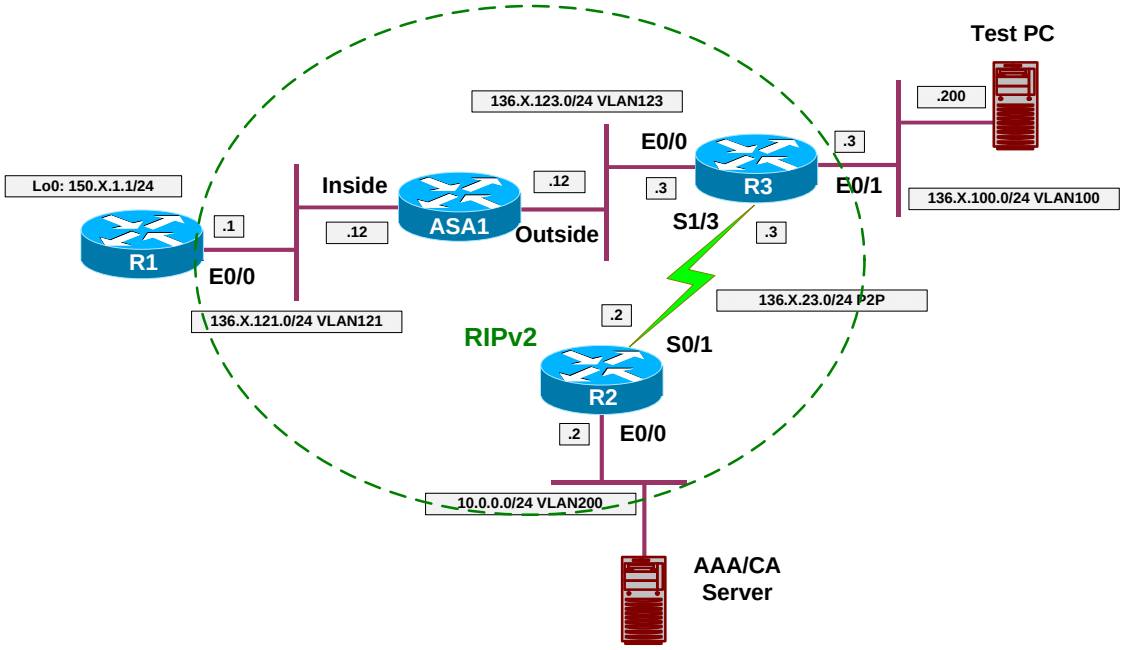
```
    outbound pcp sas:
```

📖 Further Reading

Cisco Easy VPN Remote Feature
Easy VPN Server

IOS and IOS ezVPN Remote NW Extension Mode with Xuath/RRI

Objective: Configure ezVPN server to accept ezVPN Remote in network-extension mode.



Directions

- Configure devices as per the scenario "VPN/ezVPN" "IOS and IOS ezVPN Remote Client Mode with Xauth/RRI".
- In network extension mode, remote client does not need new IP address to be allocated.
- Hence, you may remove the following from R3's configuration:
  - Reference to local address pool EZVPN from group EZVPN.
  - ISAKMP reference to address-pool EZVPN.
  - Local IP pool EZVPN.
  - "client configuration address respond" statement from crypto-map VPN.
- Configure ezVPN client on R1 to use network-extension mode.

Final Configuration

```
R3:
crypto isakmp client config group EZVPN
 no pool EZVPN
!
no crypto isakmp client configuration address-pool local EZVPN
no crypto map VPN client configuration address respond
no ip local pool EZVPN
```

```
R1:
crypto ipsec client ezvpn EZVPN
 mode network-extension
```

Verification

```
R1#crypto ipsec client ezvpn connect
R1#
.Jan 19 17:54:52.206: EZVPN(EZVPN): Pending XAuth Request, Please enter the
following command:
.Jan 19 17:54:52.206: EZVPN: crypto ipsec client ezvpn xauth

R1#crypto ipsec client ezvpn xauth
Username: : CISCO
Password: : CISCO1234

R1#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : EZVPN
Inside interface list: Loopback0,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Split Tunnel List: 1
       Address    : 136.1.100.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0

R1#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Loopback0
Hits: 5  Misses: 5
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 5] access-list internet-list interface Ethernet0/0 refcount 0

R1#ping 136.1.100.3 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.100.3, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/13 ms

R1#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.123.3     136.1.121.1     QM_IDLE            122    0

R1#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.121.1
```

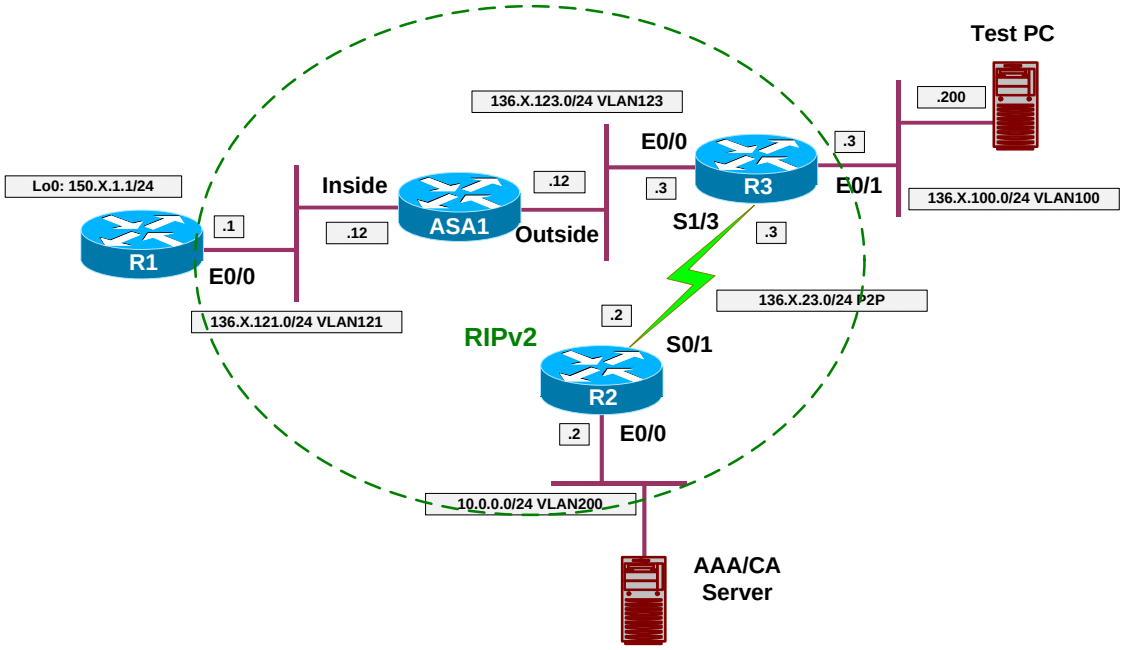
```
   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
   current_peer: 136.1.123.3:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.123.3
     path mtu 1500, media mtu 1500
     current outbound spi: CA5E3CB

     inbound esp sas:
      spi: 0x2FBDC4BD(800965821)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4457618/3396)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCA5E3CB(212198347)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4457618/3396)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

R3#show ip route static
     150.1.0.0/24 is subnetted, 1 subnets
S       150.1.1.0 [1/0] via 136.1.121.1
```

Further Reading

Cisco Easy VPN Remote Feature
Easy VPN Server

PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI

Objective: Configure the PIX/ASA firewall to support Cisco VPN Clients.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "The PIX/ASA Easy VPN/WebVPN".
- The PIX/ASA VPN configuration borrowed many concepts from IOS and VPN 3000. You configure crypto maps and ISAKMP policy just like you do on IOS (and older PIX).
- However you define tunnel group, group policy and attributes similar to VPN3000.
- Like with VPN3000 group attributes inherit their default values from default system groups. Take this in consideration, while configuring VPN.
- If you'd like to see the defaults, simply issue the following:

  "show run all tunnel-group"
  "show run all group-policy".

- Configure ISAKMP as follows:
  - Enable ISAKMP on the outside interface.
  - Configure ISAKMP policy with priority 10:
    - Use Pre-Shared authentication.
    - Use 3DES cipher.
    - Use MD5 hash.

        - Use DH group 2.

- Configure VPN addressing:
    - Enable address allocation from local pools.
    - Create local-pool EZVPN with address range:
        - 20.0.0.1-20.0.0.254
- Create access-list SPLIT_TUNNEL:
    - Permit network 136.X.121.0/24.
- Add a local user for Xauth:
    - Create local user “CISCO” with password “CISCO1234”.
- Define group-policy named EZVPN as internal:
    - Configure IPsec as the tunneling protocol.
    - Configure DNS server 10.0.0.100.
    - Specify split-tunneling policy “only tunnel networks in the list”.
    - Assign split-tunnel network-list SPLIT_TUNNEL
- Define tunnel group:
    - Create tunnel group “EZVPN” of type Remote-Access.
    - Group General Attributes:
        - Set authentication-server group to “LOCAL” (it’s the default value, inherited from default group).
        - Specify address pool “EZVPN”.
        - Assign group-policy “EZVPN”.
    - Group IPSec Attributes:
        - Specify pre-shared key “CISCO”.
- Configure crypto:
    - Create transform-set 3DES_MD5:
        - Cipher 3DES.
        - Hash MD5.
    - Create dynamic crypto-map DYNAMIC entry 10:
        - Set transform-set 3DES_MD5
        - Set reverse-route
    - Create crypto-map VPN entry 10 to use dynamic crypto-map DYNAMIC.
    - Attach crypto-map VPN to interface outside.
    - Explicitly permit VPN traffic to pass through acess-lists.
- Redistribute static routes into RIP (this will redistribute RRI routes).

Final Configuration

```
ASA1:
!
! ISAKMP configuration
!
crypto isakmp enable outside
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
```

```
 group 2
!
! Enable VPN address allocation from local pools
! Note that it's enabled by default with the PIX/ASA
!
vpn-addr-assign local
!
! Local address pool
!
ip local pool EZVPN 20.0.0.1-20.0.0.254
!
! Split-tunneling ACL
!
access-list SPLIT_TUNNEL permit ip 136.1.121.0 255.255.255.0 any
!
! Local username for Xauth
!
username CISCO password CISCO1234
!
! Tunnel-group policy
!
group-policy EZVPN internal
group-policy EZVPN attributes
 vpn-tunnel-protocol IPSec
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_TUNNEL
 dns-server value 10.0.0.100
!
! Tunnel-group definition
! Note that "authentication-server-group"
! is LOCAL by default
!
tunnel-group EZVPN type ipsec-ra
tunnel-group EZVPN general-attributes
  authentication-server-group LOCAL
  address-pool EZVPN
  default-group-policy EZVPN
tunnel-group EZVPN ipsec-attributes
  pre-shared-key CISCO
!
! IPsec transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Dynamic crypto-map
!
crypto dynamic-map DYNAMIC 10 set transform-set 3DES_MD5
crypto dynamic-map DYNAMIC 10 set reverse-route
!
! Define crypto-map
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
!
! Attach crypto map to the interface
!
crypto map VPN interface outside
!
! Permit VPN traffic to bypass ACLs
!
sysop connection permit-vpn
!
! Redistribute static routes into RIP
!
```

```
router rip
 redistribute static
```

Verification

Configure Cisco VPN client to connect to the ASA:

- ***Use group name EZVPN and password "CISCO".***
- ***Use username/password CISCO/CISCO1234 when prompted for Xauth.***

Check connected sessions:

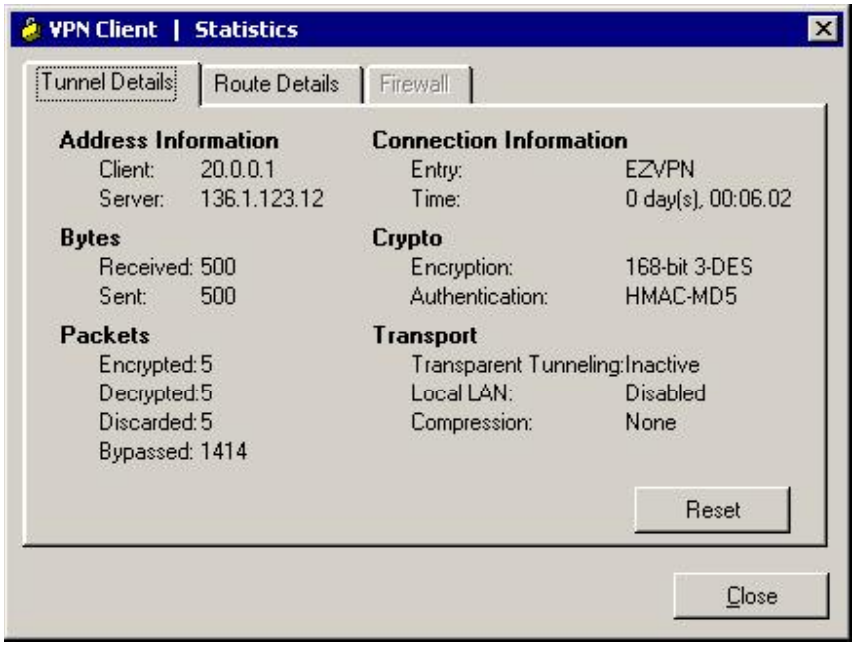
```
ASA1(config)# show vpn-sessiondb remote

Session Type: Remote

Username     : CISCO
Index        : 1
Assigned IP  : 20.0.0.1              Public IP    : 136.1.100.200
Protocol     : IPSec                 Encryption   : 3DES
Hashing      : MD5
Bytes Tx     : 978500                Bytes Rx     : 978500
Client Type  : WinNT                 Client Ver   : 4.8.01.0300
Group Policy : EZVPN
Tunnel Group : EZVPN
Login Time   : 07:10:40 UTC Mon Jan 22 2007
Duration     : 0h:09m:50s
Filter Name  :
NAC Result   : N/A
   Posture Token:
```

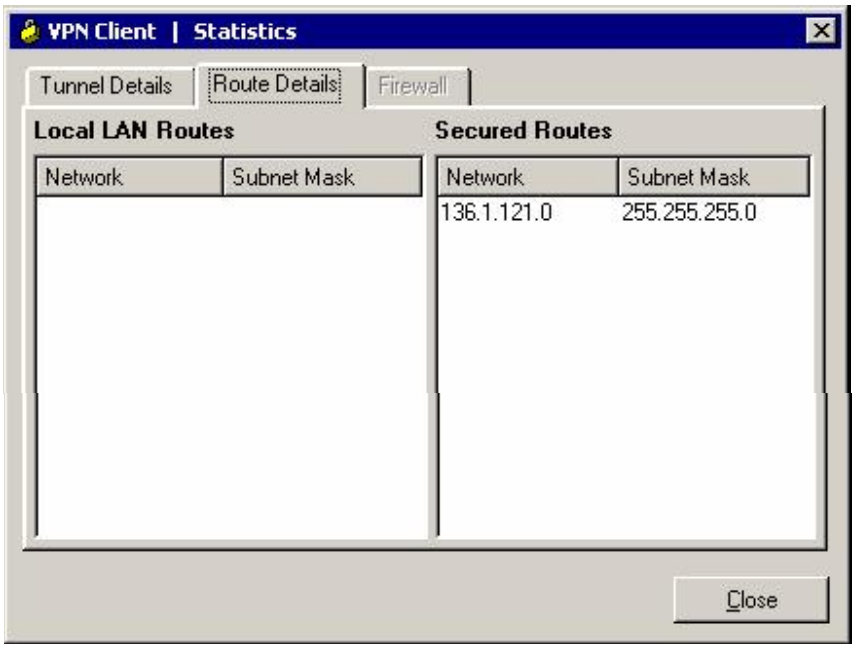
Check the ASA's routing table after connection has been established:

```
ASA1(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    136.1.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:22, outside
R    136.1.23.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:22, outside
R    136.1.100.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:22, outside
C    136.1.121.0 255.255.255.0 is directly connected, inside
C    136.1.123.0 255.255.255.0 is directly connected, outside
S    20.0.0.1 255.255.255.255 [1/0] via 136.1.123.3, outside
R    10.0.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:22, outside
R    150.1.1.0 255.255.255.0 [120/1] via 136.1.121.1, 0:00:23, inside

R1#sho ip route  rip
     136.1.0.0/24 is subnetted, 5 subnets
R       136.1.0.0 [120/3] via 136.1.121.12, 00:00:12, Ethernet0/0
R       136.1.23.0 [120/2] via 136.1.121.12, 00:00:12, Ethernet0/0
R       136.1.100.0 [120/2] via 136.1.121.12, 00:00:12, Ethernet0/0
R       136.1.123.0 [120/1] via 136.1.121.12, 00:00:12, Ethernet0/0
     20.0.0.0/32 is subnetted, 1 subnets
```

```
R       20.0.0.1 [120/1] via 136.1.121.12, 00:00:12, Ethernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.0.0 [120/3] via 136.1.121.12, 00:00:12, Ethernet0/0

R1#ping 20.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/10/36 ms

ASA1(config-router)# 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: 136.1.100.200
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE

ASA1(config-router)# show crypto ipsec sa
interface: outside
    Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
      current_peer: 136.1.100.200, username: CISCO
      dynamic allocated peer ip: 20.0.0.1

      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 136.1.123.12, remote crypto endpt.: 136.1.100.200

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 010C3FDC

    inbound esp sas:
      spi: 0xA17A46D4 (2709145300)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 6, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28402
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x010C3FDC (17579996)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 6, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28402
         IV size: 8 bytes
         replay detection support: Y
```

Check VPN Client Statistics:



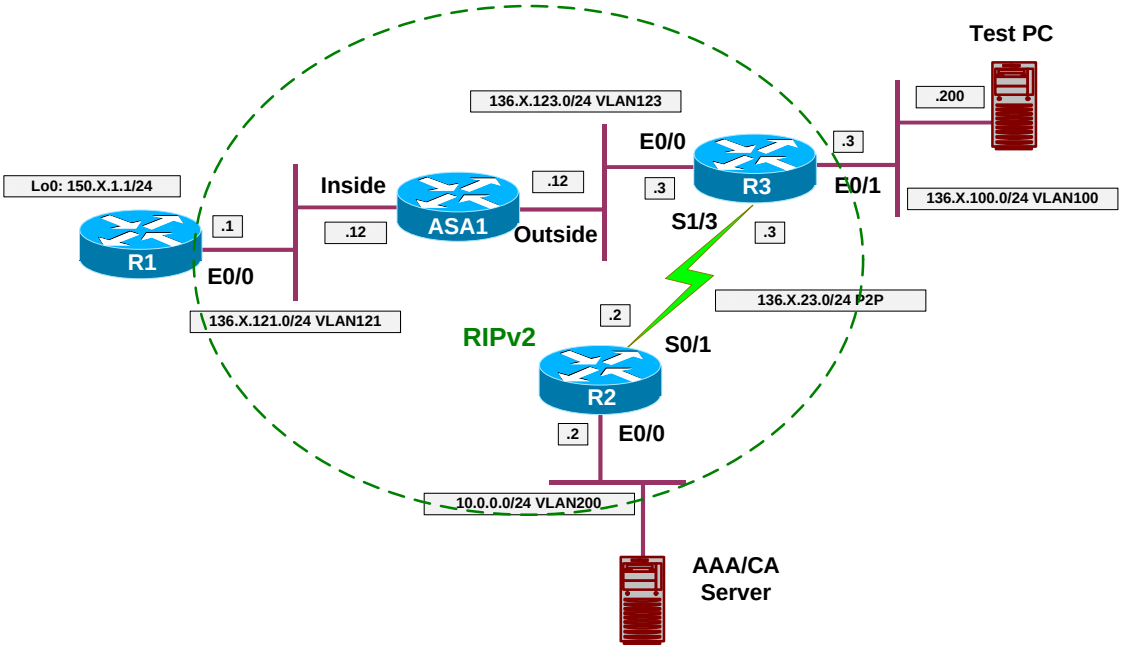


🕮 Further Reading

Configuring Remote Access VPNs

PIX/ASA and Cisco VPN Client with External Policy

Objective: Configure the PIX/ASA to apply external group policy from RADIUS server to remote-access VPN connections.



Directions

- Configure devices as per the scenario "VPN/ezVPN" "The PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI".
- The concept of group policy is decoupled from group definition with the PIX/ASA configuration. This makes it easy to change policy, retaining the group attributes.
- Note that with VPN3000 group policy is bound to a group itself, and VPN3000 uses the group password when retreiving group attributes.
- What we want, is to authenticate user locally on the firewall, yet download policy from RADIUS server.
- First, define a RADIUS server on the firewall:
  - Define server protocol to be RADIUS.
  - Define server to reside on the "outside":
    - Use CISCO as communication key.
    - Use CISCO as key for authorization transactions.
- Delete previously configured internal group-policy EZVPN.
- Configure external group-policy EZVPN to use server-group RADIUS and password CISCO.
- ACS Configuration:
  - Configure ACS server to support new RADIUS client.
  - Configure ACS Interface and permit ASA RADIUS attributes.

- Create group EZVPN and set values for ASA RADIUS attributes:
  - Tunneling-Protocols = “IPsec”.
  - IPsec-Authentication = “Internal”.
  - Split-Tunneling-Policy = “Only Tunnel networks in the List”.
  - Split-Tunneling-List = “SPLIT_TUNNEL”.
- Create user with name “EZVPN” and password matching the password you specified for group policy.
- Assign user “EZVPN” to group “EZVPN”.

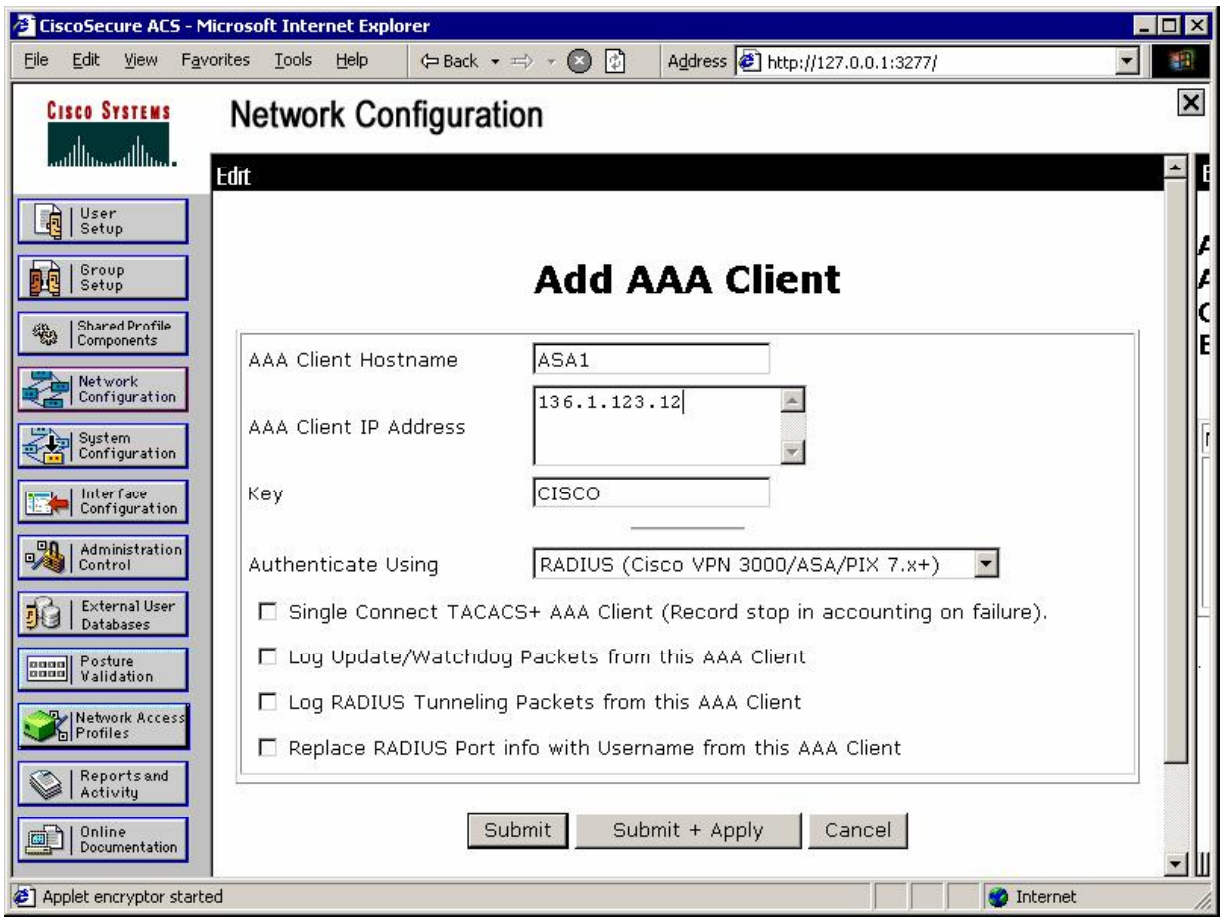
Final Configuration

ASA1:

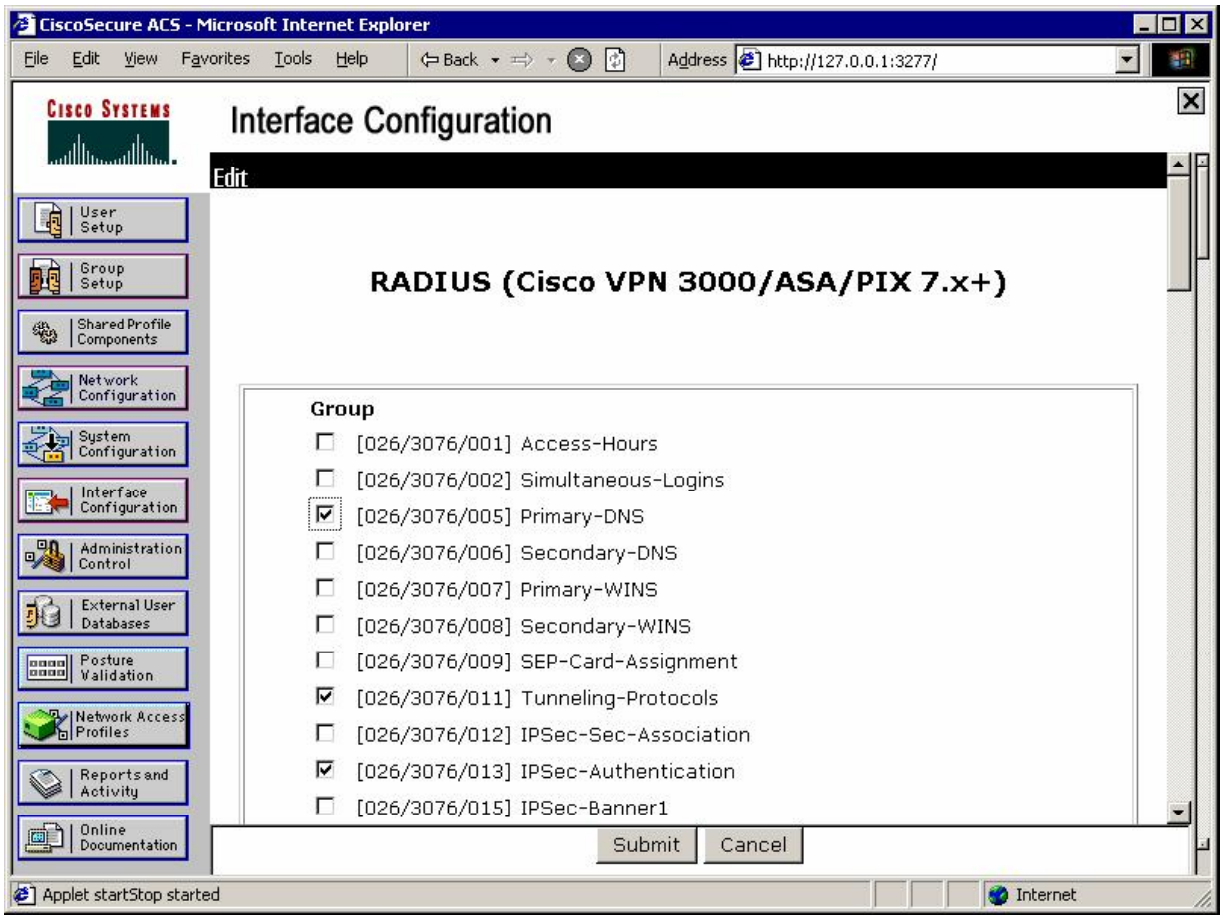
```
aaa-server RADIUS protocol radius
aaa-server RADIUS (outside) host 10.0.0.100
 key CISCO
 radius-common-pw CISCO
!
clear configure group-policy EZVPN
group-policy EZVPN external server-group RADIUS password CISCO
```

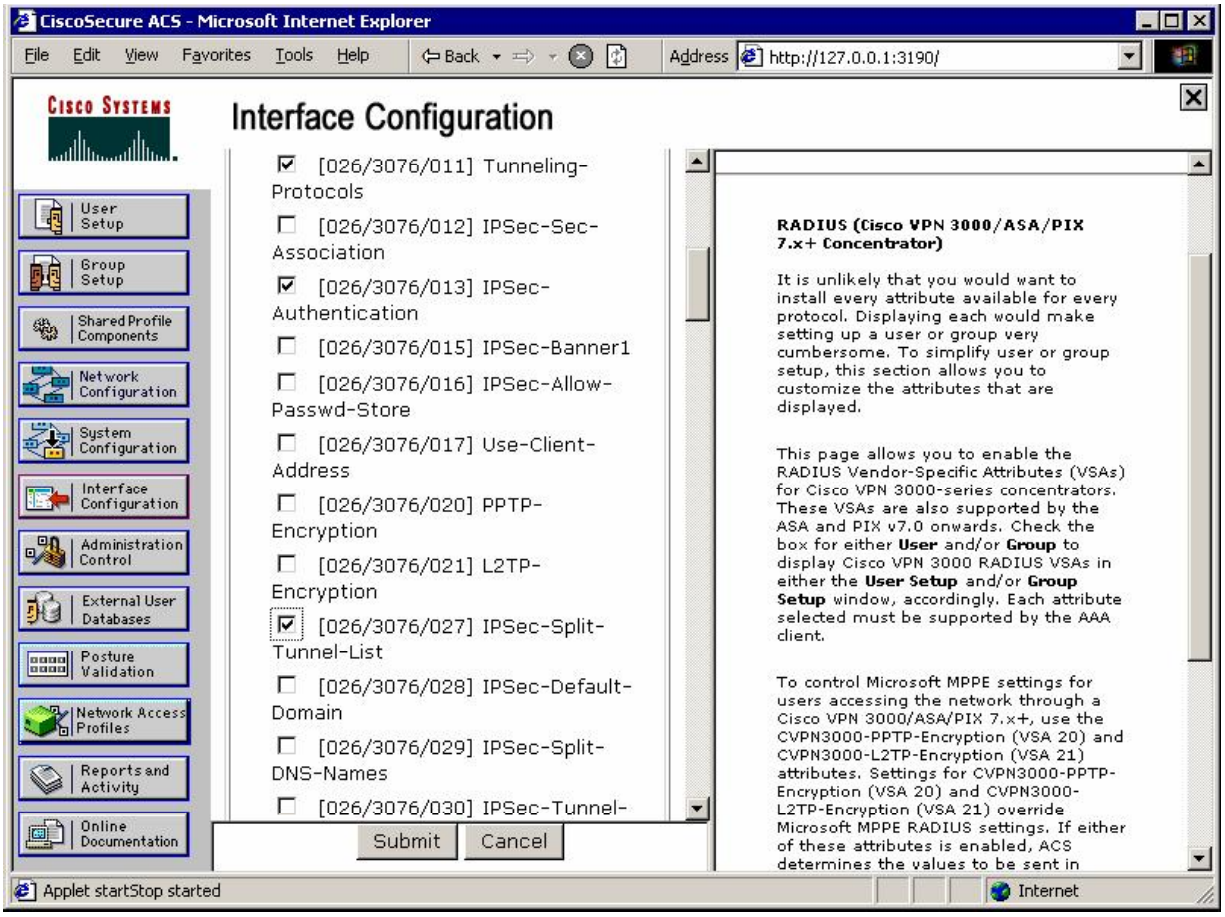
ACS:

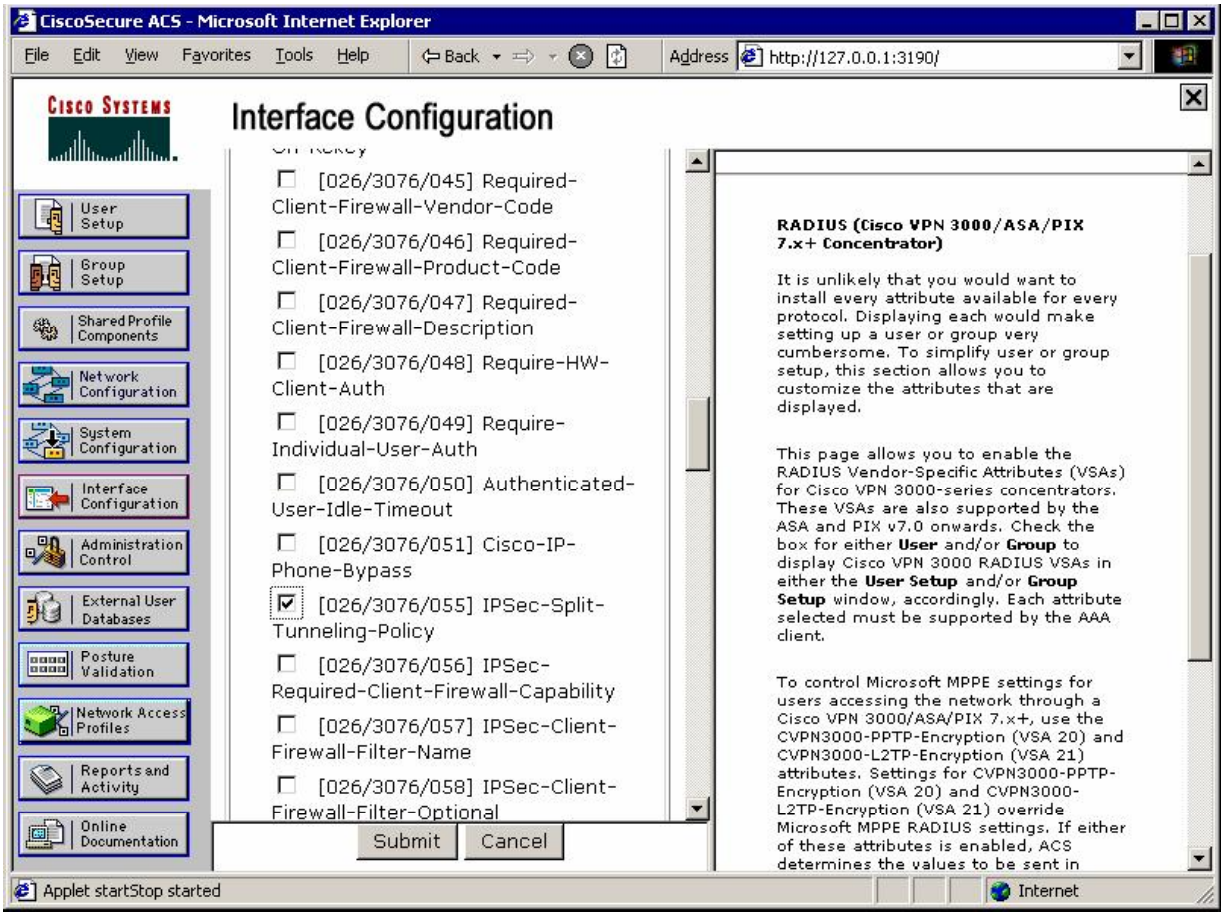
Add new AAA client:



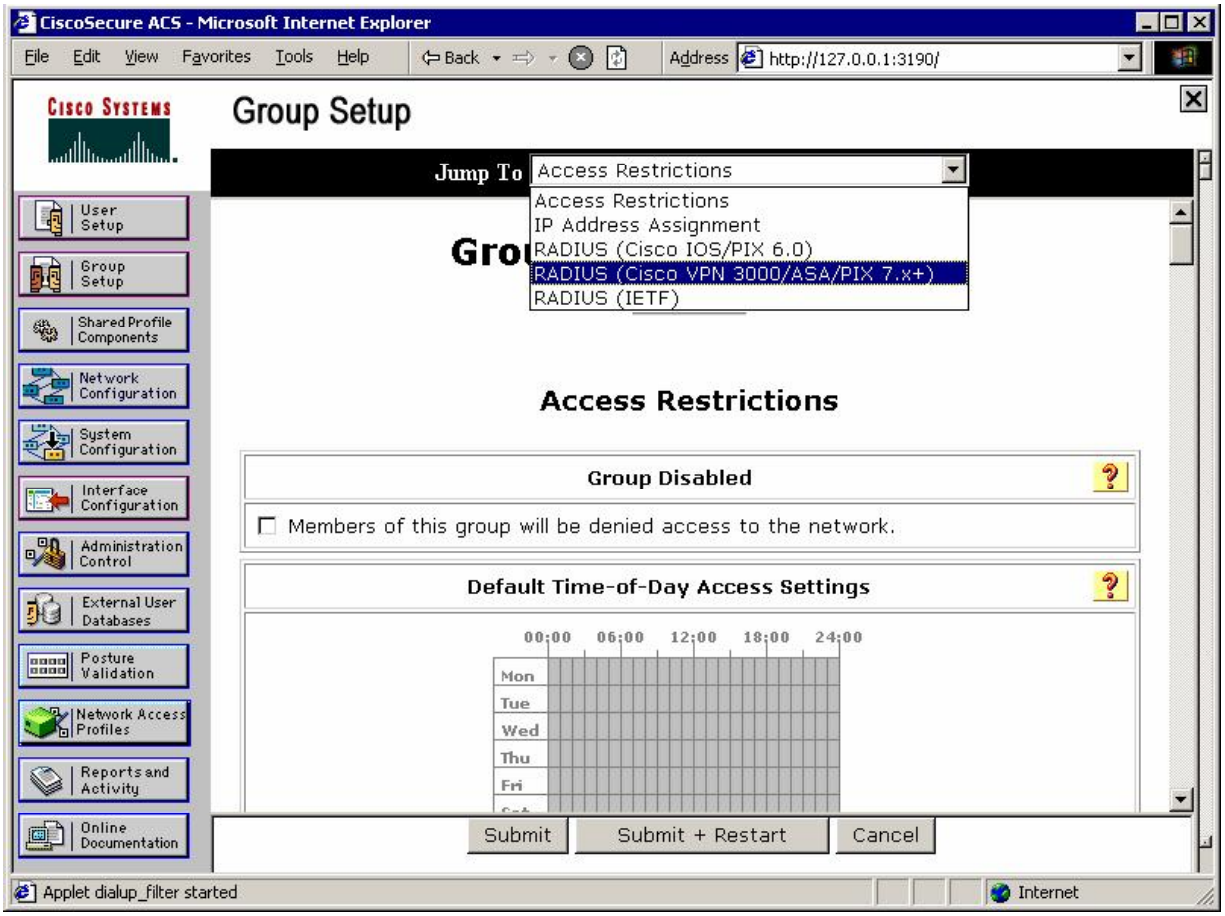
Configure ACS Interface to enable some of VPN3k/ASA RADIUS attributes:

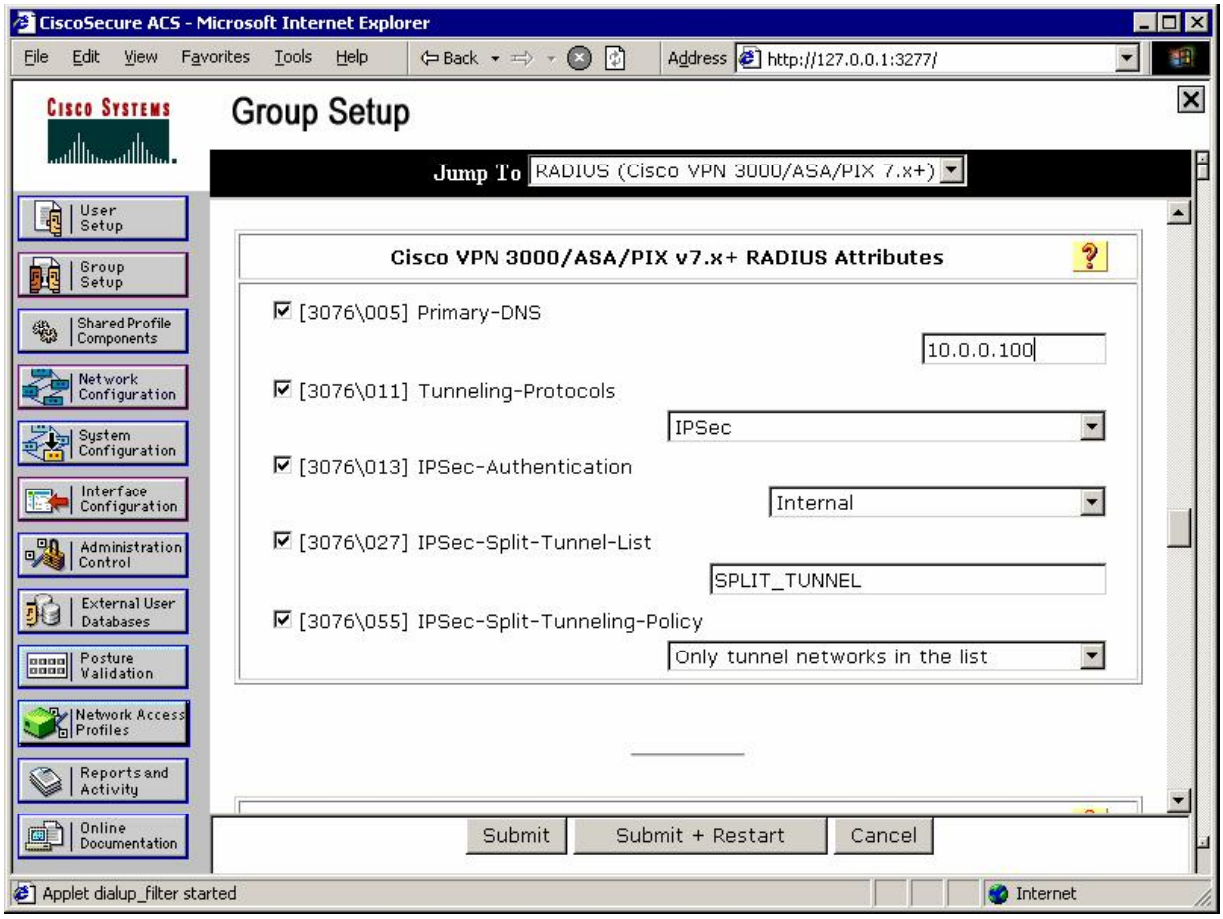



CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:3190/
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
[026/3076/011] Tunneling-Protocols
[026/3076/012] IPSec-Sec-Association
[026/3076/013] IPSec-Authentication
[026/3076/015] IPSec-Banner1
[026/3076/016] IPSec-Allow-Passwd-Store
[026/3076/017] Use-Client-Address
[026/3076/020] PPTP-Encryption
[026/3076/021] L2TP-Encryption
[026/3076/027] IPSec-Split-Tunnel-List
[026/3076/028] IPSec-Default-Domain
[026/3076/029] IPSec-Split-DNS-Names
[026/3076/030] IPSec-Tunnel-
Submit
Cancel
RADIUS (Cisco VPN 3000/ASA/PIX 7.x+ Concentrator)
It is unlikely that you would want to install every attribute available for every protocol. Displaying each would make setting up a user or group very cumbersome. To simplify user or group setup, this section allows you to customize the attributes that are displayed.
This page allows you to enable the RADIUS Vendor-Specific Attributes (VSAs) for Cisco VPN 3000-series concentrators. These VSAs are also supported by the ASA and PIX v7.0 onwards. Check the box for either User and/or Group to display Cisco VPN 3000 RADIUS VSAs in either the User Setup and/or Group Setup window, accordingly. Each attribute selected must be supported by the AAA client.
To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000/ASA/PIX 7.x+, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in
Applet startStop started
Internet

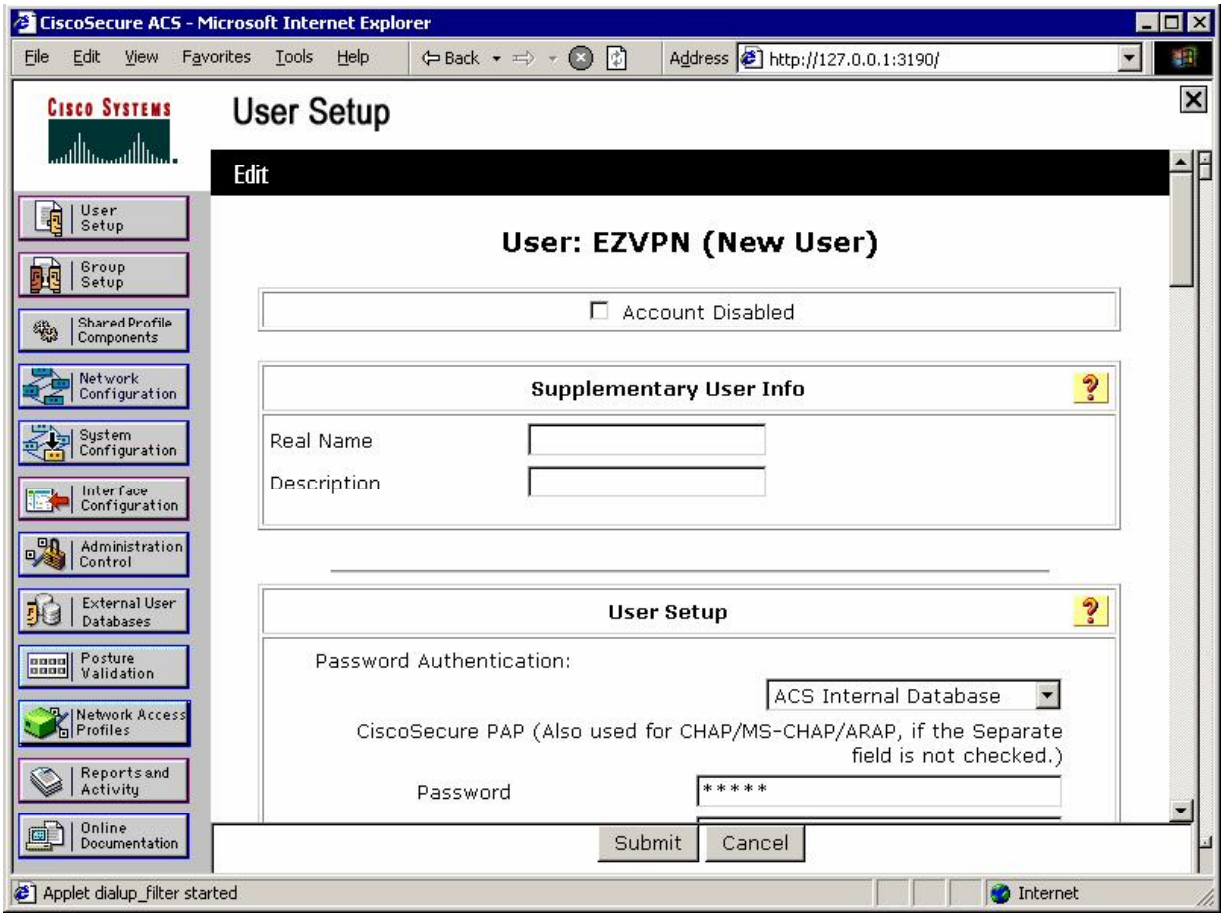

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:3190/
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
[026/3076/045] Required-Client-Firewall-Vendor-Code
[026/3076/046] Required-Client-Firewall-Product-Code
[026/3076/047] Required-Client-Firewall-Description
[026/3076/048] Require-HW-Client-Auth
[026/3076/049] Require-Individual-User-Auth
[026/3076/050] Authenticated-User-Idle-Timeout
[026/3076/051] Cisco-IP-Phone-Bypass
[026/3076/055] IPSec-Split-Tunneling-Policy
[026/3076/056] IPSec-Required-Client-Firewall-Capability
[026/3076/057] IPSec-Client-Firewall-Filter-Name
[026/3076/058] IPSec-Client-Firewall-Filter-Optional
Submit
Cancel
RADIUS (Cisco VPN 3000/ASA/PIX 7.x+ Concentrator)
It is unlikely that you would want to install every attribute available for every protocol. Displaying each would make setting up a user or group very cumbersome. To simplify user or group setup, this section allows you to customize the attributes that are displayed.
This page allows you to enable the RADIUS Vendor-Specific Attributes (VSAs) for Cisco VPN 3000-series concentrators. These VSAs are also supported by the ASA and PIX v7.0 onwards. Check the box for either User and/or Group to display Cisco VPN 3000 RADIUS VSAs in either the User Setup and/or Group Setup window, accordingly. Each attribute selected must be supported by the AAA client.
To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000/ASA/PIX 7.x+, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in
Applet startStop started
Internet

Create new group named "EZVPN":

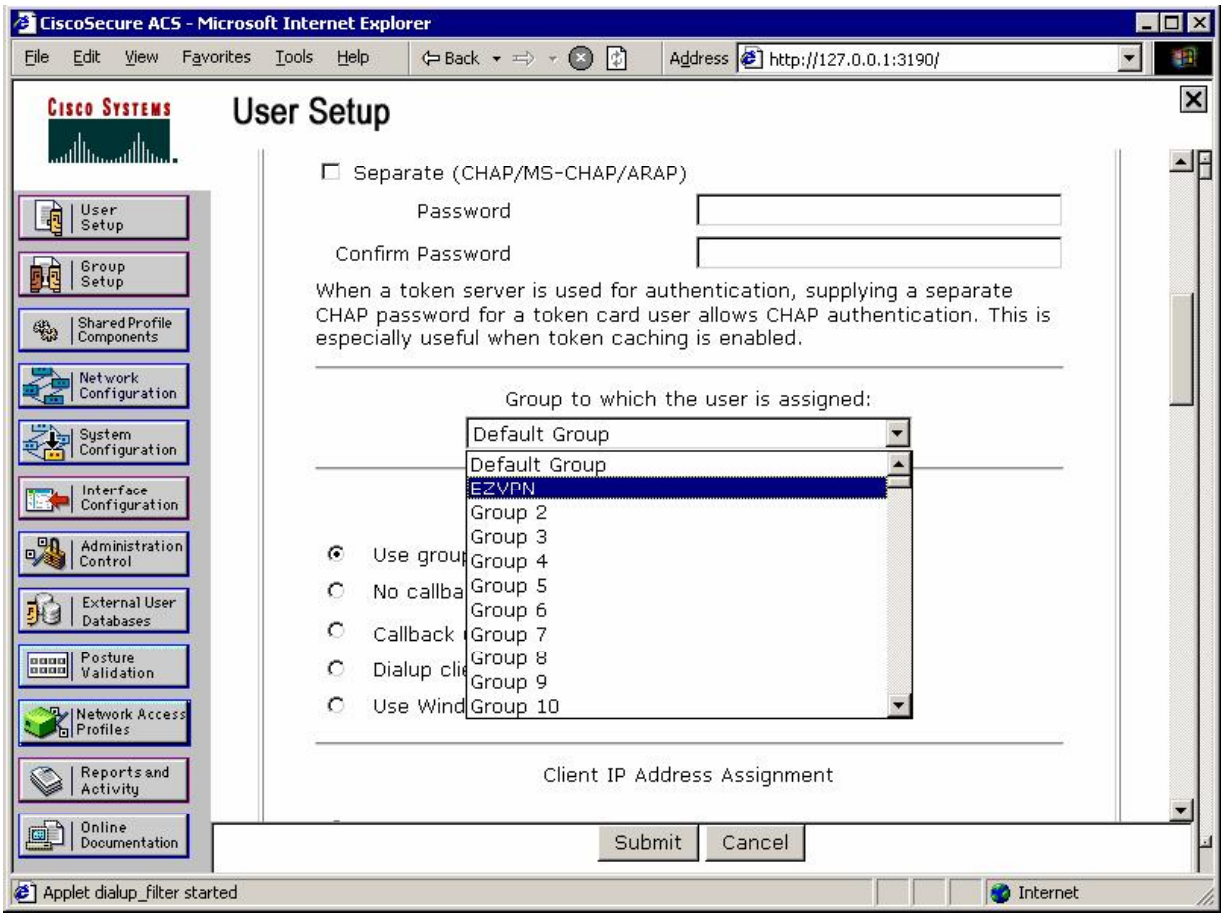



CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:3277/
Cisco Systems
Group Setup
Jump To RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes
[3076\005] Primary-DNS
10.0.0.100
[3076\011] Tunneling-Protocols
IPSec
[3076\013] IPSec-Authentication
Internal
[3076\027] IPSec-Split-Tunnel-List
SPLIT_TUNNEL
[3076\055] IPSec-Split-Tunneling-Policy
Only tunnel networks in the list
Submit
Submit + Restart
Cancel
Applet dialup_filter started
Internet

Create user EZVPN with password, matching the common RADIUS authorization password on the ASA ("CISCO"):



Assign this user to group EZVPN:



Verification

Enable debugging on the ASA, and connect Cisco VPN Client to the ASA:
(use group password "CISCO" and "CISCO/CISCO1234" for Xauth):

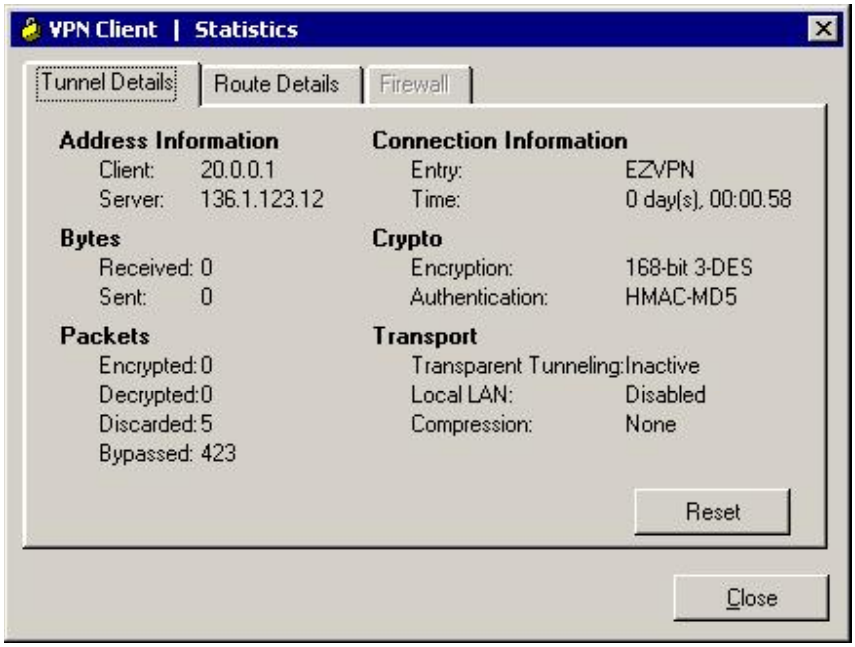
```
ASA1(config)# debug radius
ASA1(config)# debug aaa authentication
debug aaa authentication enabled at level 1
ASA1(config)# debug aaa authorization
debug aaa authorization enabled at level 1

radius mkreq: 0xe
alloc_rip 0x41ed900
    new request 0xe --> 3 (0x41ed900)
got user ''
got password
add_req 0x41ed900 session 0xe id 3
RADIUS_REQUEST
radius.c: rad_mkpkt

RADIUS packet decode (authentication request)
```

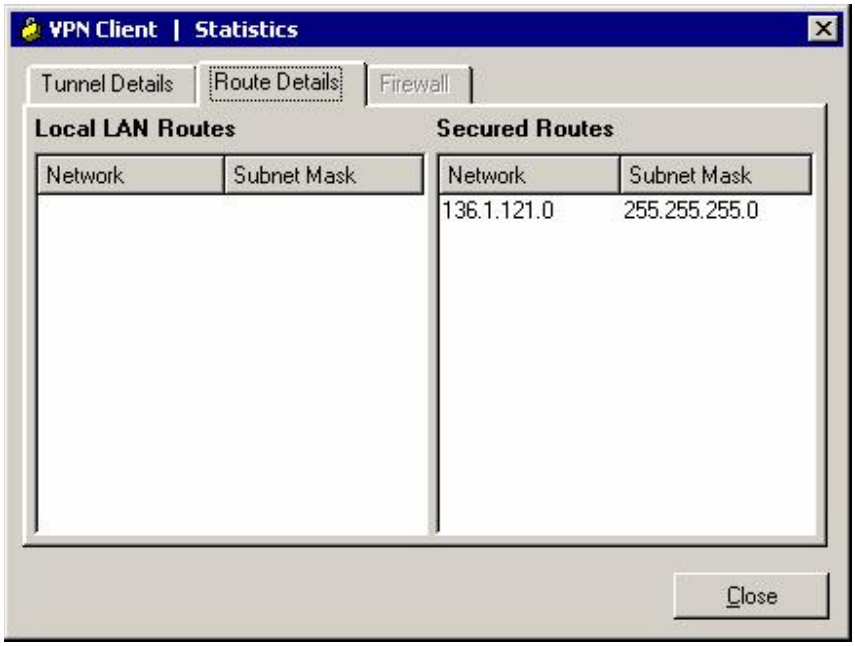
```
----------------------------------------
Raw packet data (length = 155).....
01 03 00 9b f9 3e 9f ec b5 4a bb d8 31 16 97 84    |  .....>...J..1...
6d a2 33 f0 01 07 45 5a 56 50 4e 02 12 18 68 ef    |  m.3...EZVPN...h.
c0 3b 69 3b a5 75 28 66 7a f4 d5 a0 e5 05 06 00    |  .;i;.u(fz.......
00 00 09 06 06 00 00 00 02 07 06 00 00 00 01 1e    |  ................
0e 31 33 36 2e 31 2e 31 32 33 2e 31 32 1f 0f 31    |  .136.1.123.12..1
33 36 2e 31 2e 31 30 30 2e 32 30 30 3d 06 00 00    |  36.1.100.200=...
00 05 42 0f 31 33 36 2e 31 2e 31 30 30 2e 32 30    |  ..B.136.1.100.20
30 04 06 88 01 7b 0c 1a 24 00 00 00 09 01 1e 69    |  0....{..$......i
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 33 36 2e    |  p:source-ip=136.
31 2e 31 30 30 2e 32 30 30 d9 1e                   |  1.100.200..

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 3 (0x03)
Radius: Length = 155 (0x009B)
Radius: Vector: F93E9FECB54ABBD8311697846DA233F0
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
45 5a 56 50 4e                                     |  EZVPN
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
18 68 ef c0 3b 69 3b a5 75 28 66 7a f4 d5 a0 e5    |  .h..;i;.u(fz....
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x9
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 14 (0x0E)
Radius: Value (String) =
31 33 36 2e 31 2e 31 32 33 2e 31 32                |  136.1.123.12
Radius: Type = 31 (0x1F) Calling-Station-Id
Radius: Length = 15 (0x0F)
Radius: Value (String) =
31 33 36 2e 31 2e 31 30 30 2e 32 30 30             |  136.1.100.200
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 15 (0x0F)
Radius: Value (String) =
31 33 36 2e 31 2e 31 30 30 2e 32 30 30             |  136.1.100.200
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 136.1.123.12 (0x88017B0C)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 36 (0x24)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 30 (0x1E)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 33 36    |  ip:source-ip=136
2e 31 2e 31 30 30 2e 32 30 30 d9 1e                |  .1.100.200..
send pkt 10.0.0.100/1645
```

```
rip 0x41ed900 state 7 id 3
rad_vrfy() : response message verified
rip 0x41f02c8
 : chall_state ''
 : state 0x7
 : timer 0x0
 : reqauth:
     f9 3e 9f ec b5 4a bb d8 31 16 97 84 6d a2 33 f0
 : info 0xe
     session_id 0xe
     request_id 0x3
     user 'EZVPN'
     response '***'
     app 0
     reason 0
     skey 'CISCO'
     sip 10.0.0.100
     type 1

RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 118).....
02 03 00 76 2b 96 dd 0f 10 d9 50 76 a2 38 04 78    |  ...v+.....Pv.8.x
87 60 fc 89 1a 0c 00 00 0c 04 05 06 0a 00 00 64    |  .`............d
1a 0c 00 00 0c 04 0b 06 00 00 00 04 1a 0c 00 00    |  ................
0c 04 0d 06 00 00 00 05 1a 14 00 00 0c 04 1b 0e    |  ................
53 50 4c 49 54 5f 54 55 4e 4e 45 4c 1a 0c 00 00    |  SPLIT_TUNNEL....
0c 04 37 06 00 00 00 01 08 06 ff ff ff ff 19 18    |  ..7.............
43 41 43 53 3a 30 2f 35 31 65 61 2f 38 38 30 31    |  CACS:0/51ea/8801
37 62 30 63 2f 39                                  |  7b0c/9

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 3 (0x03)
Radius: Length = 118 (0x0076)
Radius: Vector: 2B96DD0F10D95076A23804788760FC89
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 5 (0x05) Primary-DNS
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.0.0.100 (0x0A000064)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 11 (0x0B) Tunnelling-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 4 (0x0004)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 13 (0x0D) IPSec-Authentication
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 5 (0x0005)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 20 (0x14)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 27 (0x1B) Split-Tunnel-Inclusion-List
Radius: Length = 14 (0x0E)
Radius: Value (String) =
53 50 4c 49 54 5f 54 55 4e 4e 45 4c                |  SPLIT_TUNNEL
Radius: Type = 26 (0x1A) Vendor-Specific
```

```
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 55 (0x37) Split-Tunneling-Policy
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 1 (0x0001)
Radius: Type = 8 (0x08) Framed-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 255.255.255.255 (0xFFFFFFFF)
Radius: Type = 25 (0x19) Class
Radius: Length = 24 (0x18)
Radius: Value (String) =
43 41 43 53 3a 30 2f 35 31 65 61 2f 38 38 30 31    |  CACS:0/51ea/8801
37 62 30 63 2f 39                                  |  7b0c/9
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x41ed900 session 0xe id 3
free_rip 0x41ed900
radius: send queue empty
```

Check Cisco VPN Client statistics:






```
ASA1(config)# 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: 136.1.100.200
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE

R1#ping 20.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/24 ms
R1#

ASA1(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
      current_peer: 136.1.100.200, username: CISCO
      dynamic allocated peer ip: 20.0.0.1

      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 136.1.123.12, remote crypto endpt.: 136.1.100.200
```

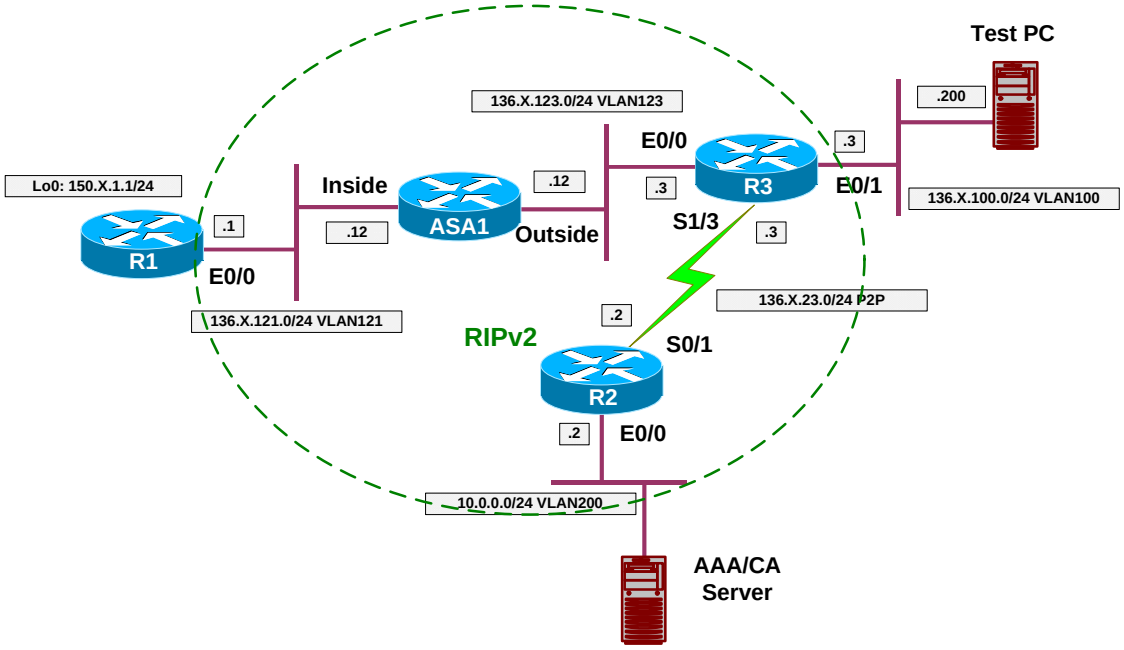
```
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: E7392AD9

    inbound esp sas:
      spi: 0xD7D854C0 (3621278912)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 9, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 27808
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xE7392AD9 (3879283417)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 9, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 27808
         IV size: 8 bytes
         replay detection support: Y
```

📖 Further Reading

Migrating to ASA 7.2 for VPN 3000 Concentrator Administrators

PIX/ASA and Cisco VPN Client with RADIUS

Objective: Configure the to authenticate remote user and download group policy from RADIUS server. Additionally, specify a group ACL on RADIUS server to be applied to user's session.



Directions

- Configure devices as per the scenario "VPN/Easy VPN" "The PIX/ASA and Cisco VPN Client with External Policy"
- We want to force group "EZVPN" member to be authenticated against the RADIUS server, not the local database.
- To make that possible, configure group EZVPN" general-attributes to use RADIUS server group for authentication.
- Note that user's authentication is performed before the external policy is retreived from RADIUS server. This allows you to specify different policy name in user's profile.
- Create user "CISCO" with password "CISCO1234" on ACS. This entry will be used to authenticate remote client via Xauth.
- Additionally, we want all group members to have simple ACL applied. The ACL should permit only ICMP traffic to group members.
- Configure group EZVPN on ACS server, and add Cisco AV-Pair:
    - "ip:inacl#1="permit icmp any any"

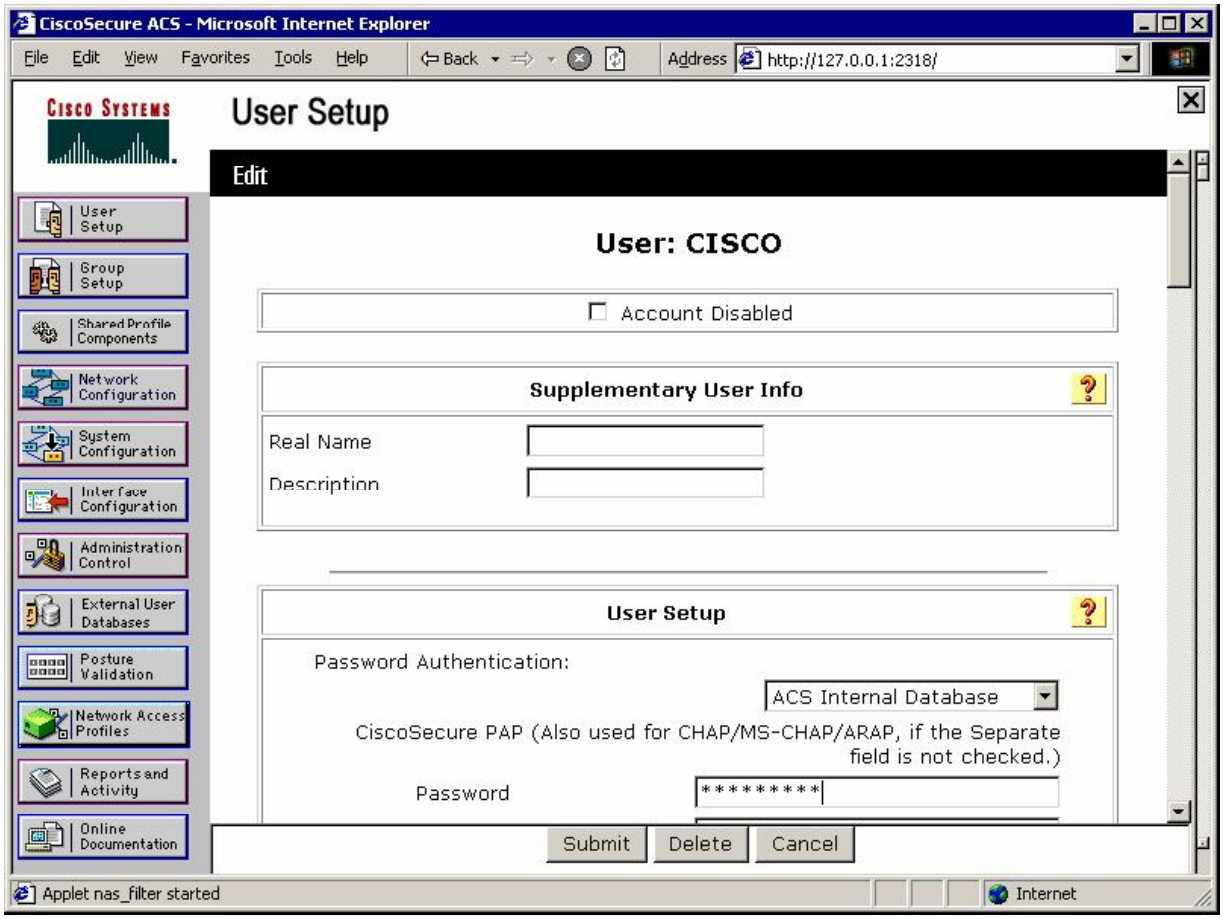
Final Configuration

ASA1:

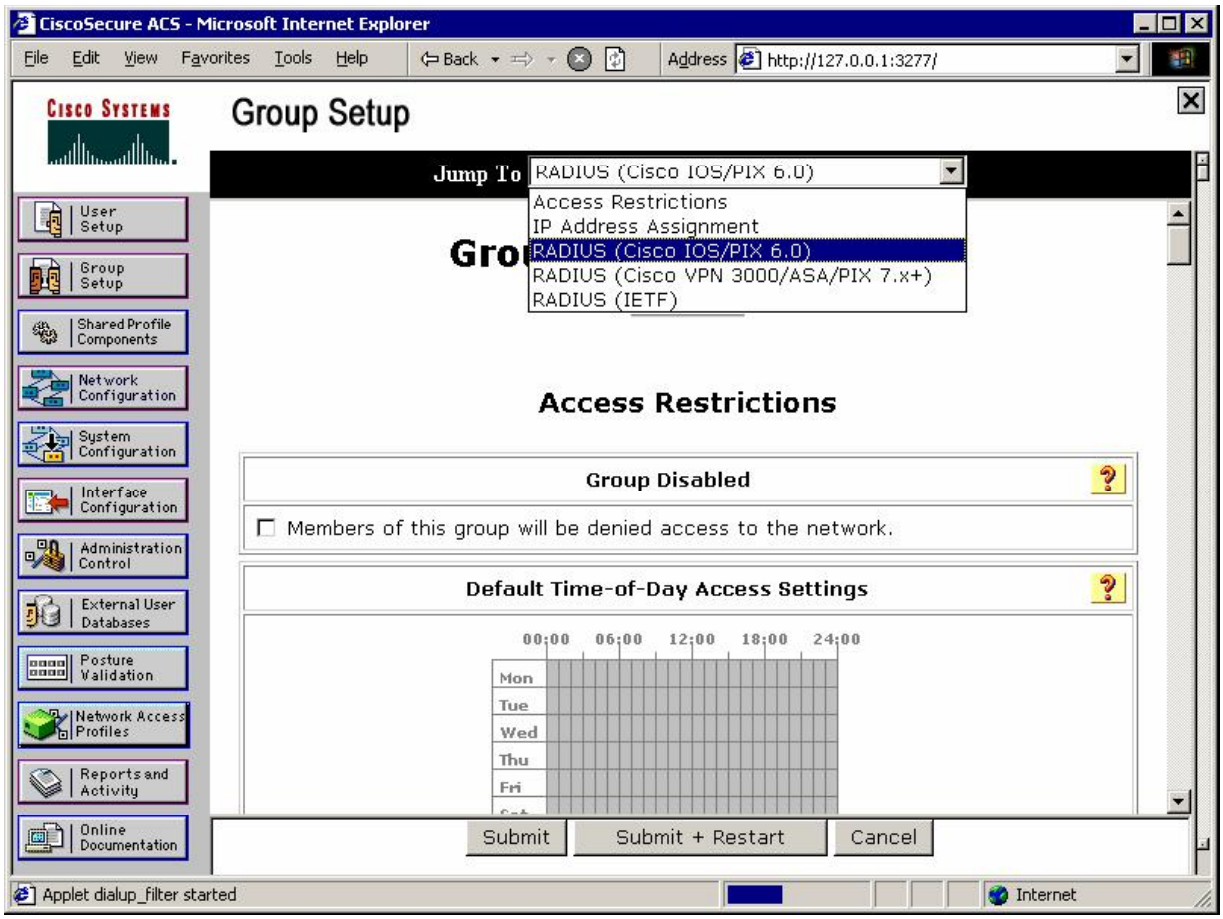
```
tunnel-group EZVPN general-attributes
 authentication-server-group RADIUS
```

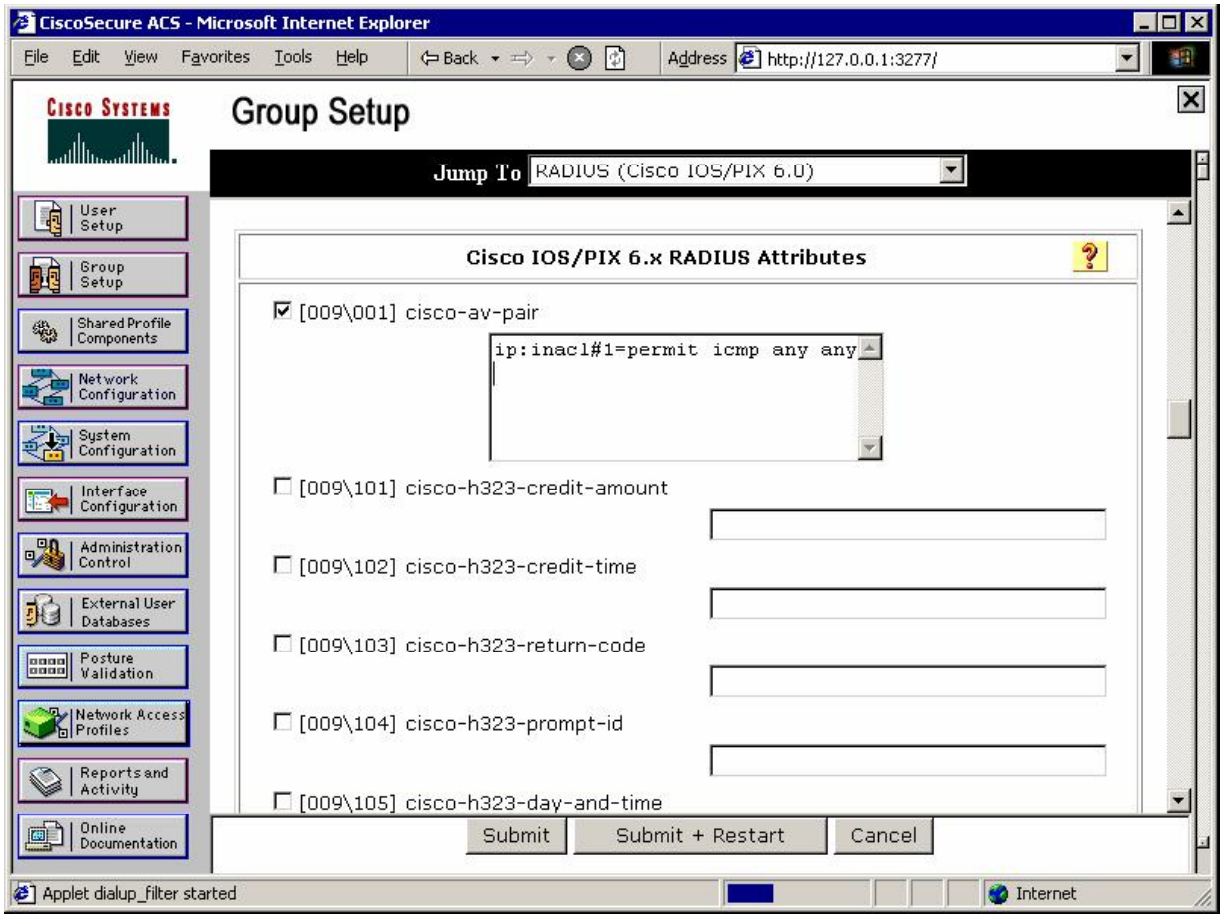
ACS:

Create user "CISCO" with password "CISCO1234":



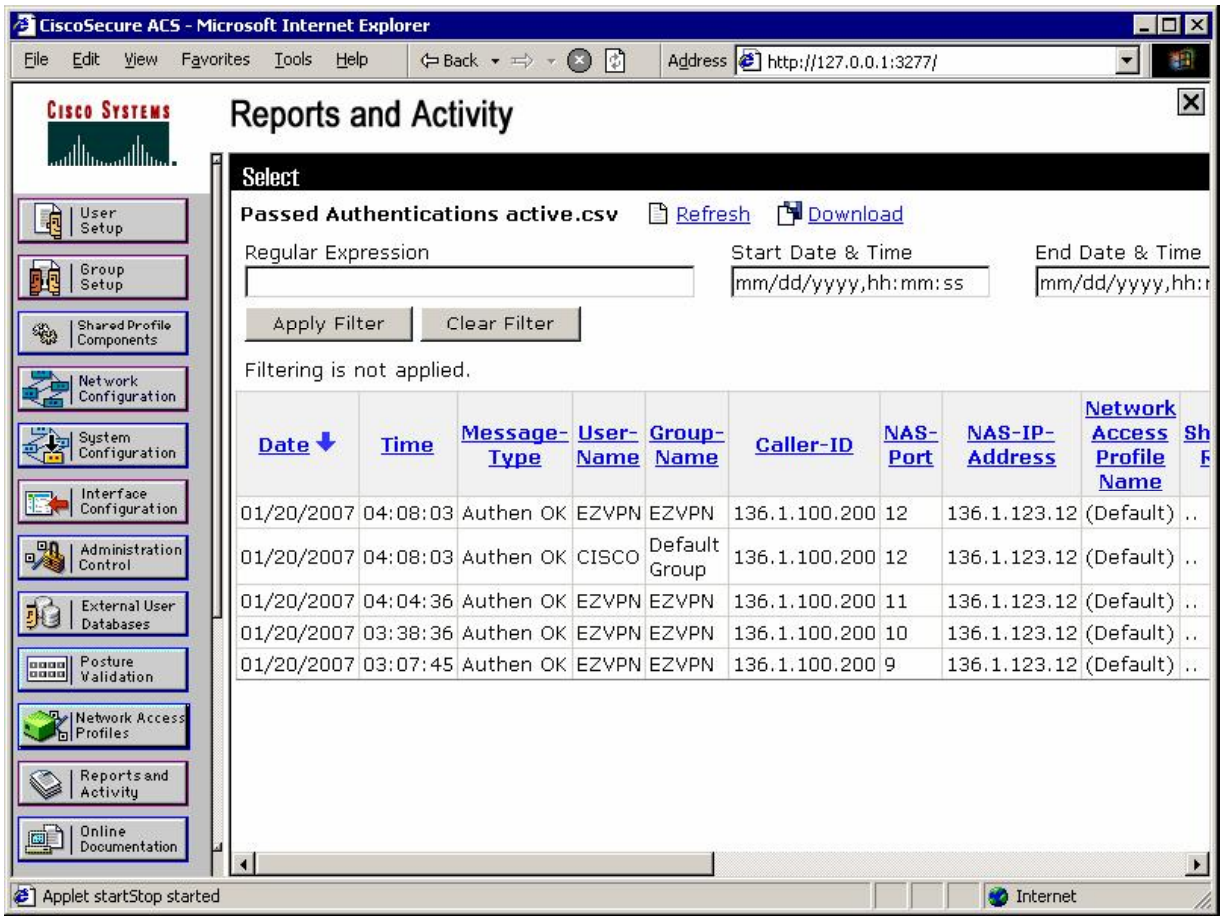
Add group attribute "Cisco AV-Pair" to specify downloadble ACL:




CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:3277/
Cisco Systems
Group Setup
Jump To RADIUS (Cisco IOS/PIX 6.0)
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Cisco IOS/PIX 6.x RADIUS Attributes
[009\001] cisco-av-pair
ip:inacl#1=permit icmp any any
[009\101] cisco-h323-credit-amount
[009\102] cisco-h323-credit-time
[009\103] cisco-h323-return-code
[009\104] cisco-h323-prompt-id
[009\105] cisco-h323-day-and-time
Submit
Submit + Restart
Cancel
Applet dialup_filter started
Internet

Verification

Connect Cisco VPN Client, and check "Passed Authentication" on ACS:



Note that user was authenticated first, before the policy retreival.

Check access-list at the ASA:

```
ASA1(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list SPLIT_TUNNEL; 1 elements
access-list SPLIT_TUNNEL line 1 extended permit ip 136.1.121.0 255.255.255.0
any (hitcnt=0) 0x71544147
access-list AAA-user-EZVPN-29666A08; 1 elements (dynamic)
access-list AAA-user-EZVPN-29666A08 line 1 extended permit icmp any any
(hitcnt=0) 0x836519eb

R1#ping 20.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/28 ms
```

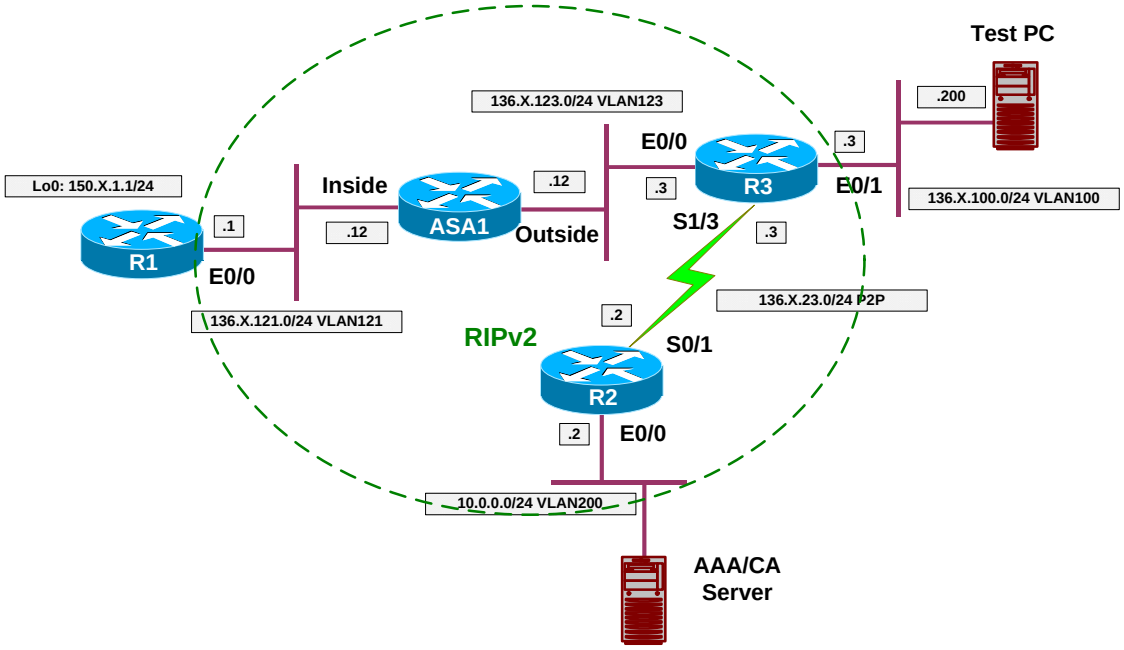
```
R1#telnet 20.0.0.1 139
Trying 20.0.0.1, 139 ...
% Connection refused by remote host

ASA1(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
      current_peer: 136.1.100.200, username: CISCO
      dynamic allocated peer ip: 20.0.0.1

      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 136.1.123.12, remote crypto endpt.: 136.1.100.200

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: ACE45F0C

    inbound esp sas:
      spi: 0xDDC0489C (3720366236)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 12, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28278
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xACE45F0C (2900647692)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 12, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28278
         IV size: 8 bytes
         replay detection support: Y
```

Further Reading

Cisco VPN Client User and Group Attribute Processing on the VPN 3000 Concentrator

PIX/ASA and Cisco VPN Client with Digital Certificates

Objective: Configure the ASA to authenticate remote VPN Client connections using digital certificates.



Directions

- Configure devices as per the scenario "VPN/Easy VPN" "The PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI".
- Start by configuring VPN Client as follows:
  - First, enroll VPN client with CA via SCEP.
    - Use enrollment URL http://10.0.0.100/certsrv/mscep/mscep.dll
    - Specify "OU=EZVPN" to be used for group matching on the ASA.
  - Next, use Internet Explorer to retreive and install CA Root Certificate into Windows trusted certificates store.
  - After that, download CA certificate and import it into VPN client Store.
  - Modify VPN connection setting and choose authentication based on certificates.
- Enroll the ASA with CA:
  - Configure NTP server to 10.0.0.100.
  - Configure CA trustpoint IE1:
    - Use enrollment URL: http://10.0.0.100/certsrv/mscep/mscep.dll

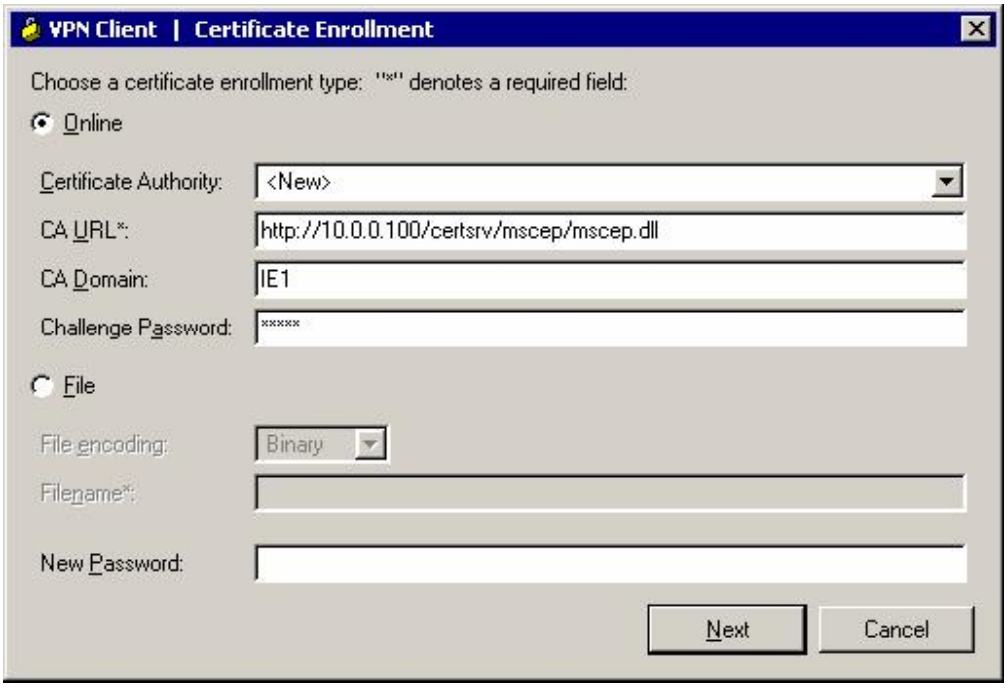
        - Set revocation-check to none.
    - Authenticate the CA trustpoint.
    - Configure domain-name and create RSA key-pair.
    - Enroll with CA finally.
- Change ISAKMP policy entry 10 on the ASA
    - Specify RSA-Sig authentication.
- Change tunnel-group EZVPN ipsec-attributes settings on the ASA:
    - Use trustpoint IE1

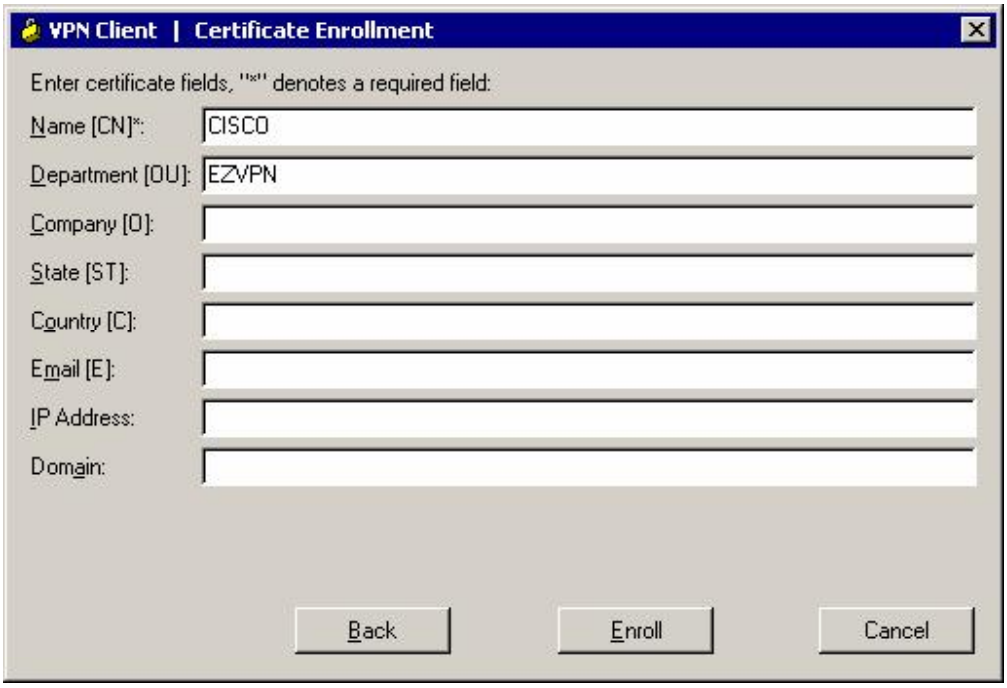
Final Configuration

```
ASA1:
!
! Sync time, set domain-name, generate key
!
ntp server 10.0.0.100
domain-name internetworkexpert.com
crypto key generate rsa general-keys modulus 512
!
! Trustpoint config
!
crypto ca trustpoint IE1
 enrollment url http://10.0.0.100:80/certsrv/mscep/mscep.dll
 crl configure
!
! Authenticate and enroll
!
crypto ca authenticate IE1
crypto ca enroll IE1
!
! Change ISAKMP policy to use RSA-Sig Auth
!
crypto isakmp policy 10
 authentication rsa-sig
!
! Configure IE1 as trustpoint for group EZVPN
!
tunnel-group EZVPN ipsec-attr
  trust-point IE1
```

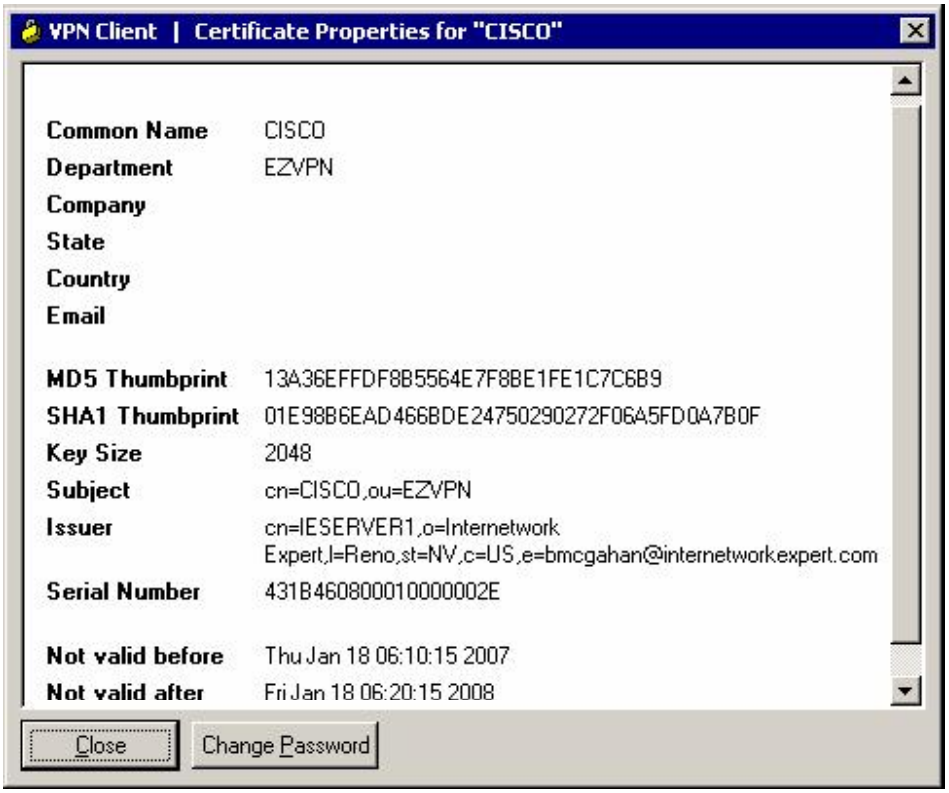
Test PC/VPN Client:

Choose Certificates/Enroll:

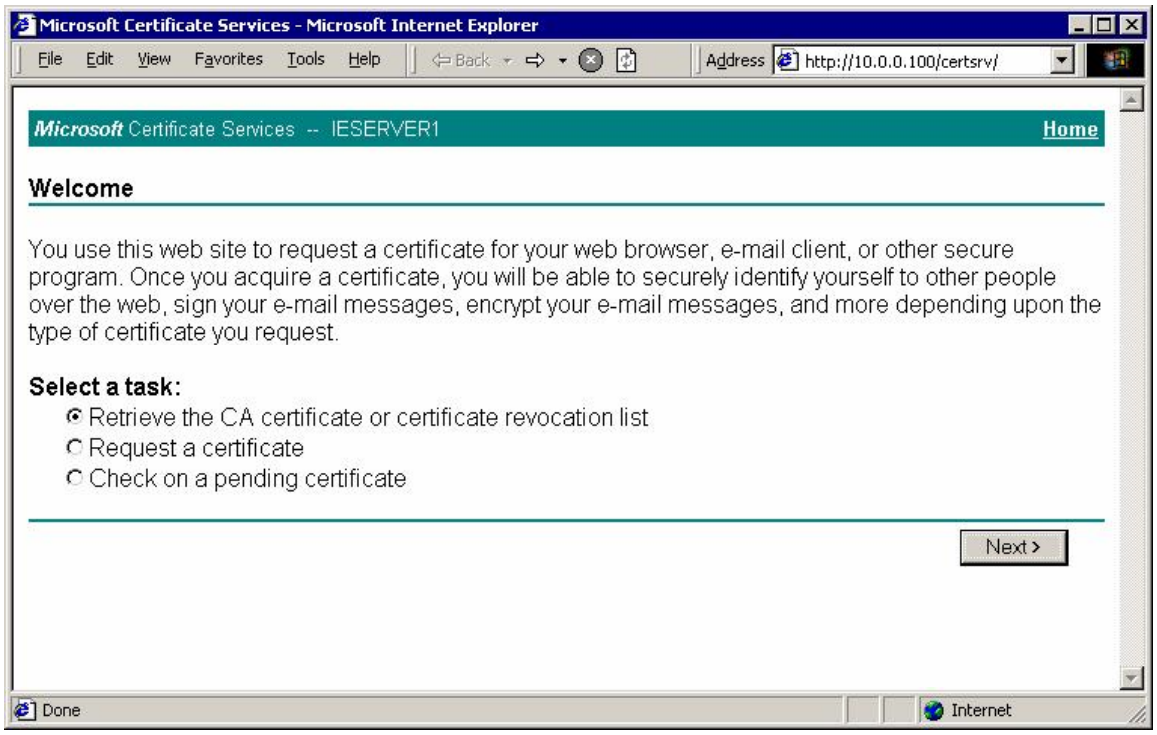




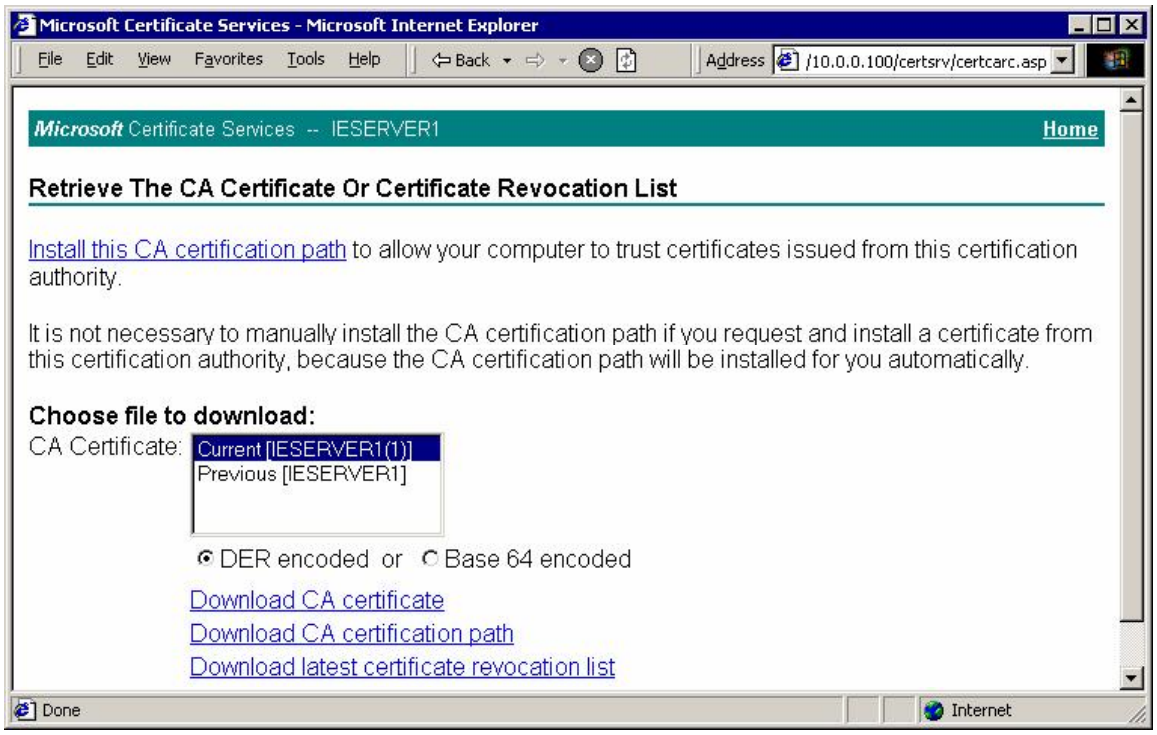
Review your certificate:

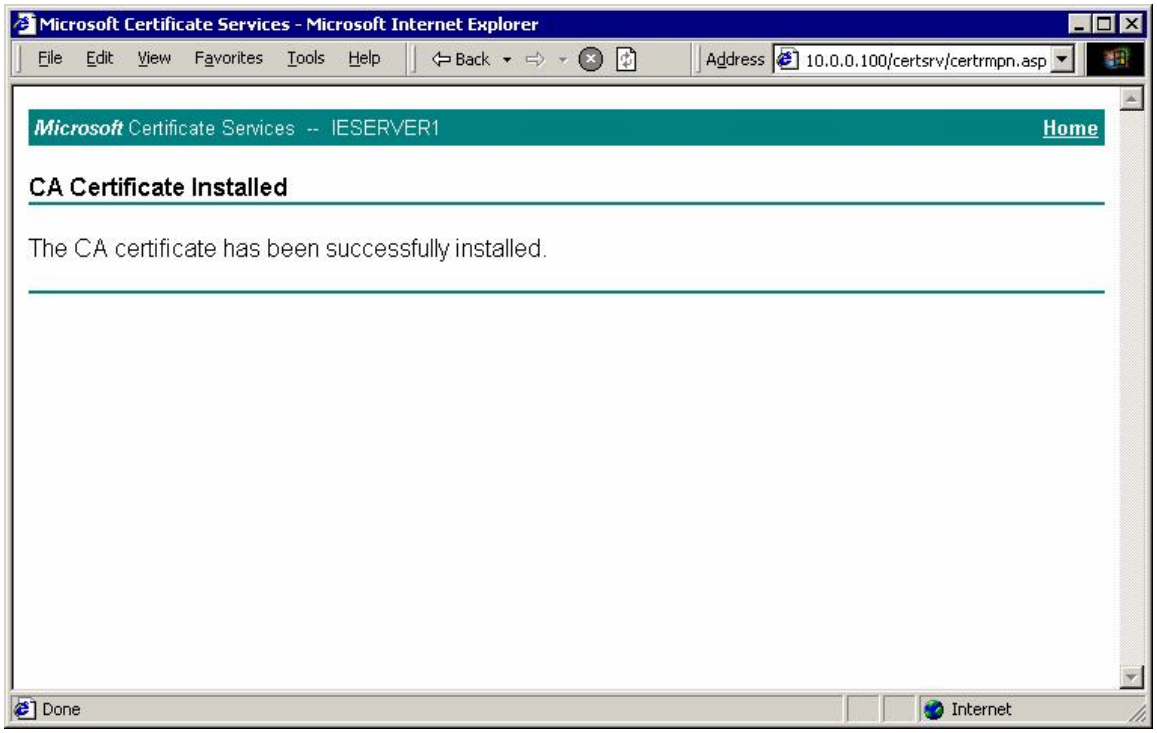


Retreive CA certificate and install it into trusted store:

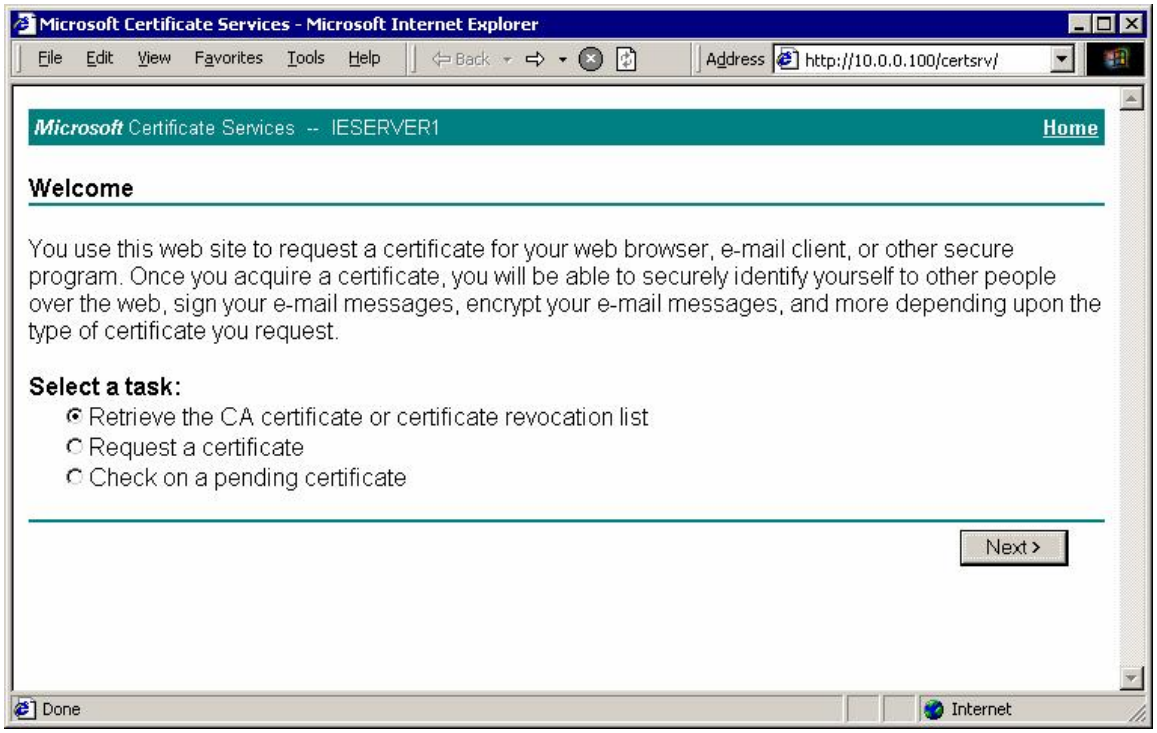


Choose "Install this CA certification path":

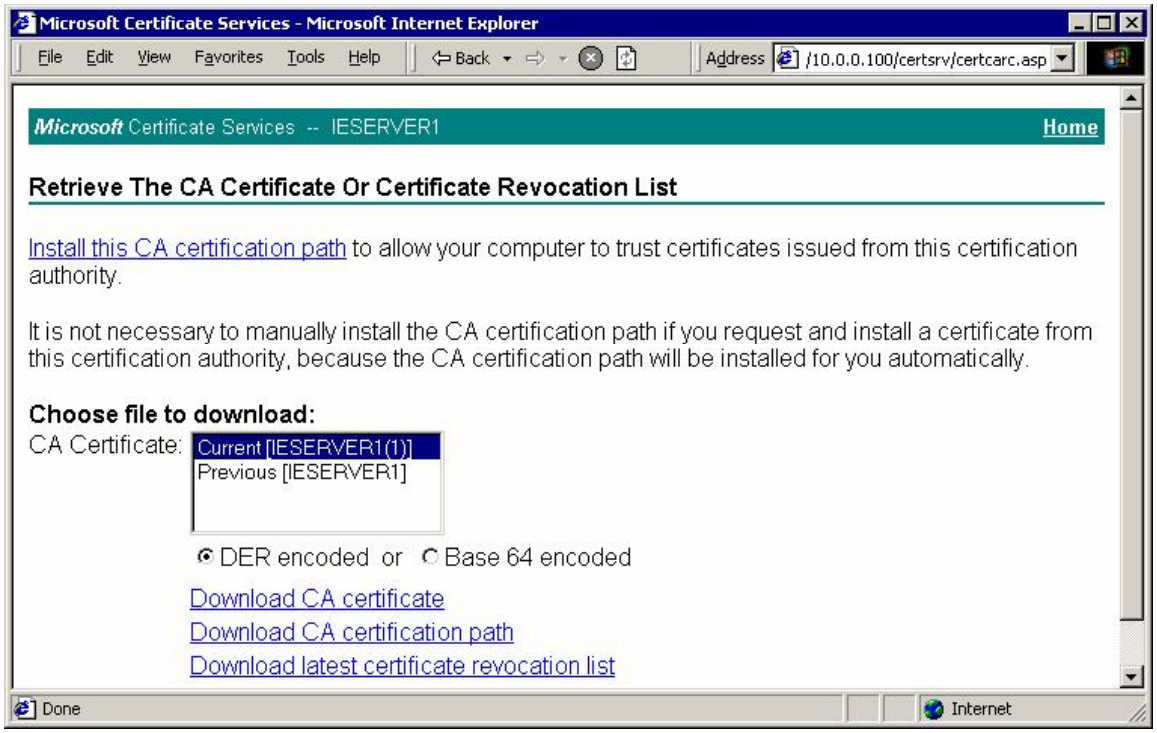


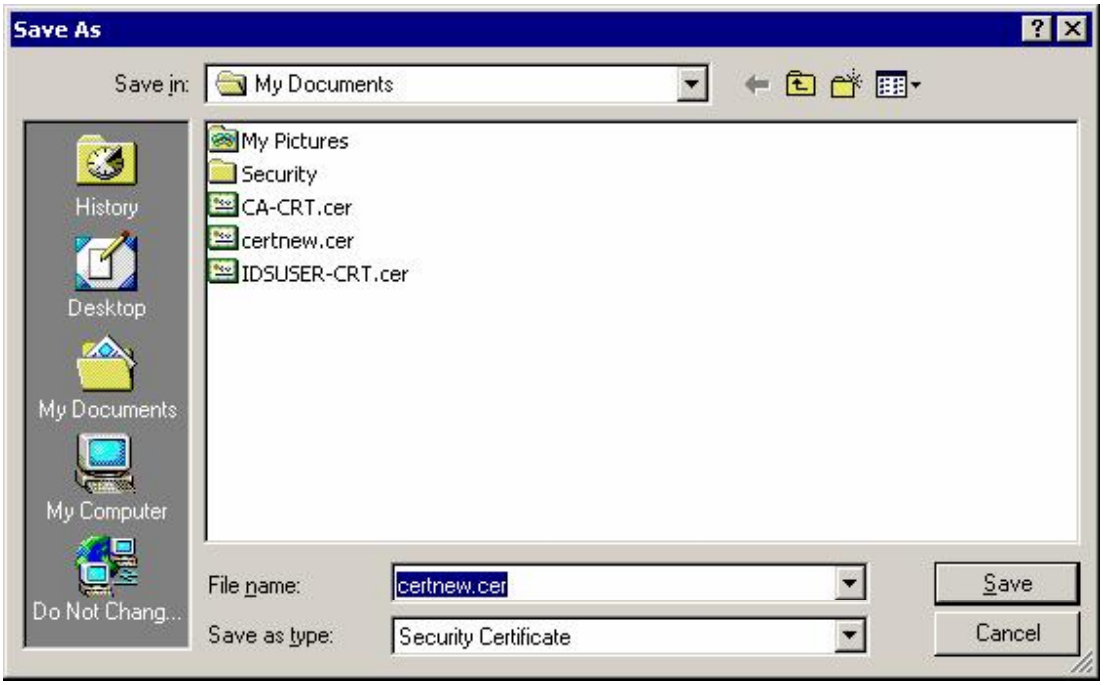


Download CA certificate for installation into Cisco VPN client store:

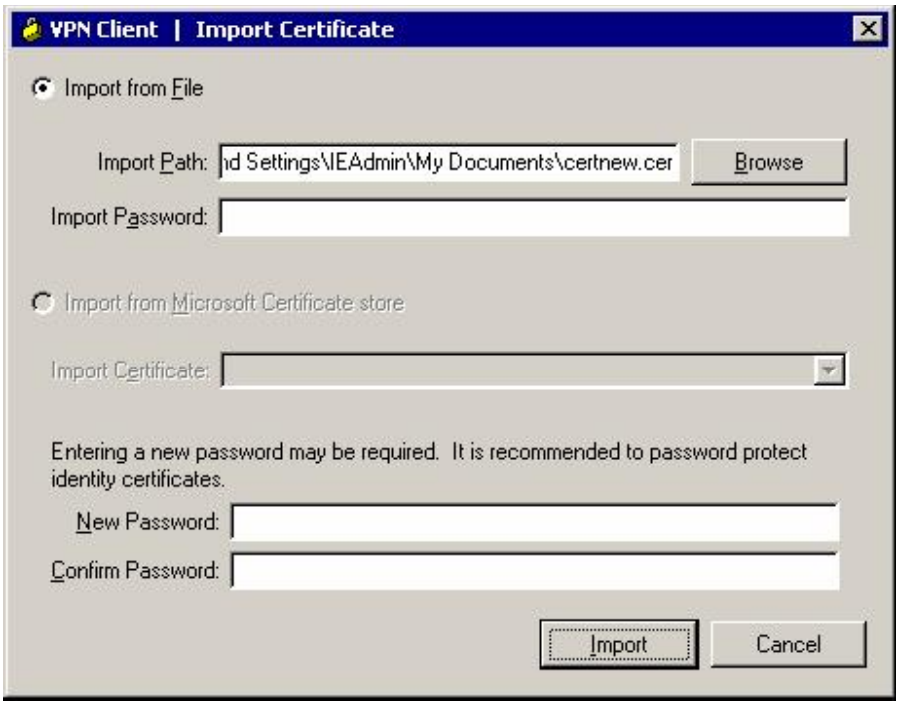


Choose "Download CA Certificate":

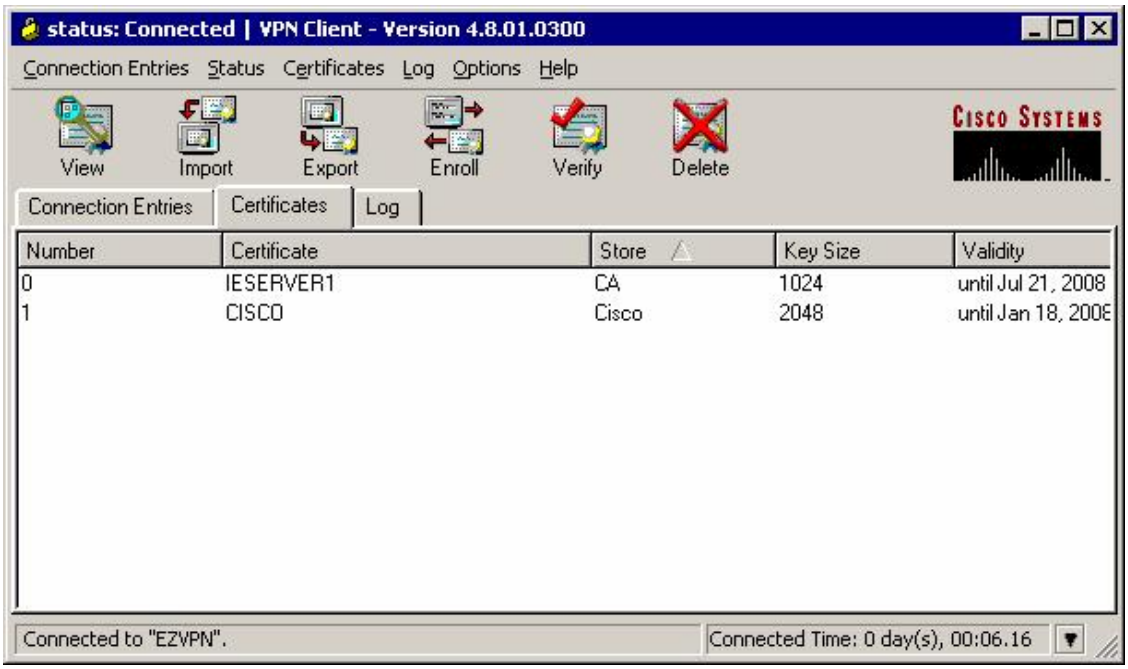




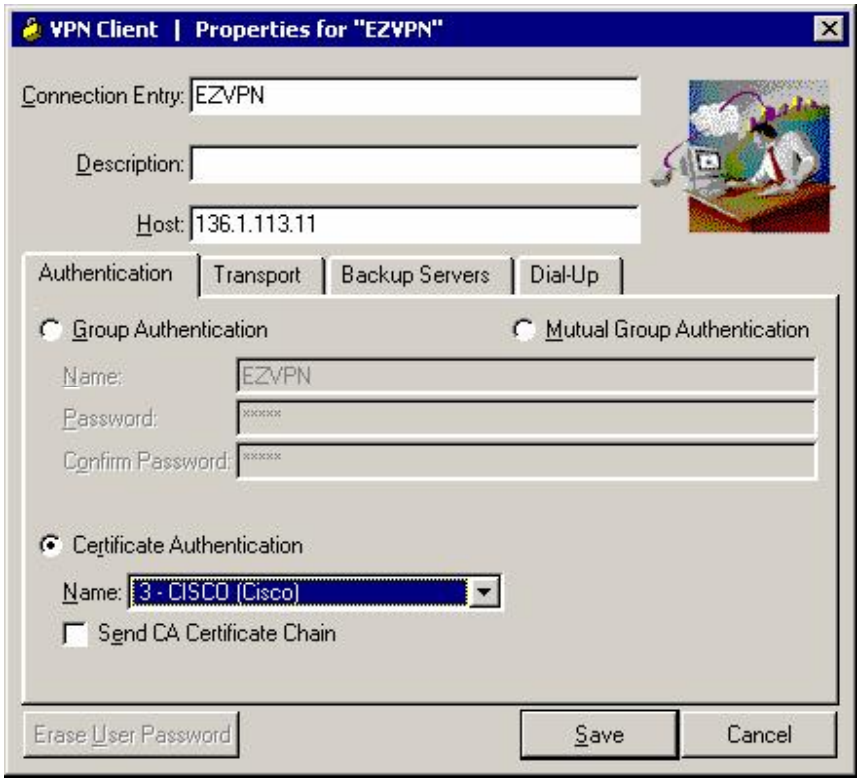
Next choose "Import" in Certificate Menu of Cisco VPN Client:



You should have identity ceritificate and CA certificate into Cisco VPN Client Store:



Modify connection Settings to use Certificates for authentication:

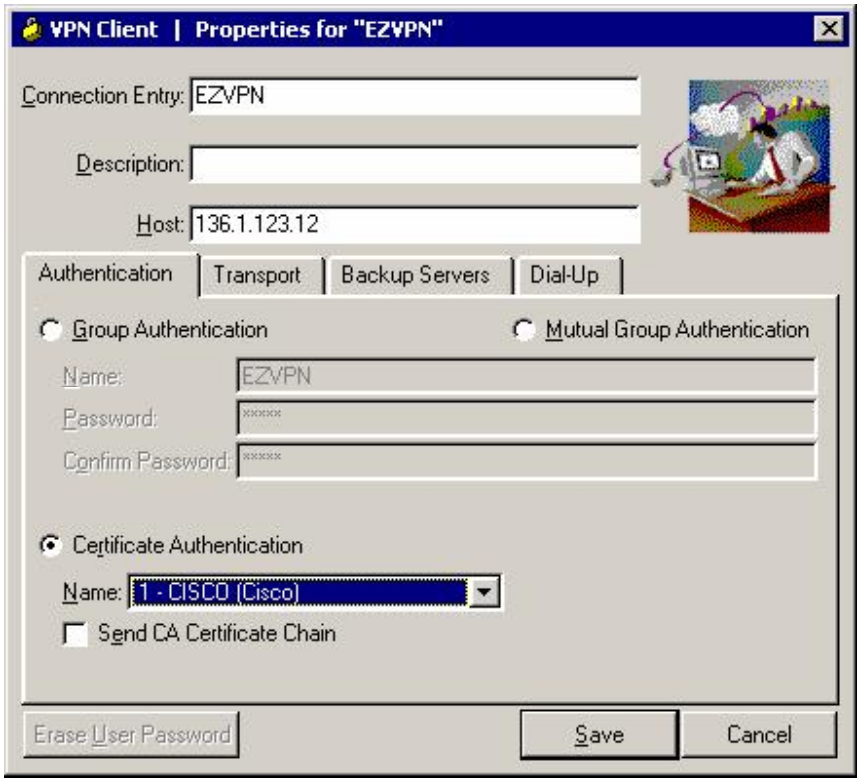


Verification

```
ASA1(config)# crypto ca enroll IE1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco
Re-enter password: cisco


% The fully-qualified domain name in the certificate will be:
ASA1.internetworkexpert.com

% Include the device serial number in the subject name? [yes/no]: no

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ASA1(config)# The certificate has been granted by CA!
```

VPN Client:

Change connection settings to use Digital Certificate:



Enable debugging at the ASA and connect VPN Client:

```
ASA1(config)# debug crypto isakmp 9
ASA1(config)#
Jan 20 13:45:40 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 1144
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing SA payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Oakley proposal is
acceptable
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received xauth V6 VID
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received DPD VID
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received Fragmentation VID
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, IKE Peer included IKE
fragmentation capability flags:  Main Mode:        True  Aggressive Mode:
False
```

With certificates connection occurs in IKE Main Mode

```
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received NAT-Traversal ver
02 VID
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received Cisco Unity client
VID
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing IKE SA payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, IKE SA Proposal # 1,
Transform # 22 acceptable  Matches global IKE entry # 1
```

ISAKMP Policy match found

```
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing ISAKMP SA
payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing Fragmentation
VID + extended capabilities payload
Jan 20 13:45:40 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length :
108
Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
+ NONE (0) total length : 224
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing ke payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing ISA_KE payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing nonce payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Processing IOS/PIX Vendor ID
payload (version: 1.0.0, capabilities: 00000408)
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Received Cisco Unity client
VID
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing ke payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing nonce payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing certreq payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing Cisco Unity VID
payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing xauth V6 VID
payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Send IOS VID
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Constructing ASA spoofing
IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing VID payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Send Altiga/Cisco
VPN3000/Cisco ASA GW VID
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Generating keys for
Responder...
Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=0) with payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 403
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Rcv'd fragment from a new
fragmentation set. Deleting any old fragments.
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Successfully assembled an
encrypted pkt from rcv'd fragments!
Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + CERT (6) + CERT_REQ (7) + SIG (9) +
NOTIFY (11) + NONE (0) total length : 1714
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing ID payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing cert payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing cert request
payload
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing RSA signature
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Computing hash for ISAKMP
Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing notify payload
```

Group name is taken from the OU field in the certificate:

```
Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, Trying to find group via OU...
Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, Connection landed on tunnel_group
EZVPN

Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, peer ID type
9 received (DER_ASN1_DN)
Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing
```

```
ID payload
Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing
cert payload
Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing
RSA signature
Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, Computing
hash for ISAKMP
Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing
dpd vid payload
Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=0) with payloads : HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) +
NONE (0) total length : 1244
Jan 20 13:45:42 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing
blank hash payload
Jan 20 13:45:42 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing
qm hash payload
Jan 20 13:45:42 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=ed5985ad) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total
length : 68
Jan 20 13:45:47 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=ed5985ad) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total
length : 82
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200,
process_attr(): Enter!
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, Processing
MODE_CFG Reply attributes.
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: primary DNS = 10.0.0.100
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: secondary DNS = cleared
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: primary WINS = cleared
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: secondary WINS = cleared
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: split tunneling list = SPLIT_TUNNEL
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: IP Compression = disabled
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: Split Tunneling Policy = Split Network
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: Browser Proxy Setting = no-modify
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKEGetUserAttributes: Browser Proxy Bypass Local = disable
Jan 20 13:45:47 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
User (CISCO) authenticated.
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing blank hash payload
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing qm hash payload
Jan 20 13:45:47 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=e2adfc00) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total
length : 60
Jan 20 13:45:47 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=e2adfc00) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total
length : 56
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, process_attr(): Enter!
Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Processing cfg ACK attributes
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=f10a41b4) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total
length : 188
```

```
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, process_attr(): Enter!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Processing cfg Request attributes
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for IPV4 address!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for IPV4 net mask!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for DNS server address!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for WINS server address!
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Received unsupported transaction mode attribute: 5
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for Banner!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for Save PW setting!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for Default Domain Name!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for Split Tunnel List!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for Split DNS!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for PFS setting!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for Client Browser Proxy Setting!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for backup ip-sec peer list!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for Application Version!
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Client Type: WinNT  Client Application Version: 4.8.01.0300
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for FWTYPE!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for DHCP hostname for DDNS is: ie-
server3!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, MODE_CFG: Received request for UDP Port!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Obtained IP addr (20.0.0.1) prior to initiating Mode Cfg (XAuth
enabled)
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Assigned private IP address 20.0.0.1 to remote user
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing blank hash payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Send Client Browser Proxy Attributes!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Browser Proxy set to No-Modify. Browser Proxy data will NOT be
included in the mode-cfg reply
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing qm hash payload
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=f10a41b4) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total
length : 184
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
```

```
PHASE 1 COMPLETED
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, Keep-alive type for this
connection: DPD
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Starting P1 rekey timer: 82080 seconds.
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, sending notify message
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing blank hash payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing qm hash payload
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=926c5df3) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total
length : 88
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=be168033) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5)
+ ID (5) + NONE (0) total length : 1022
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing hash payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing SA payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing nonce payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing ID payload
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Received remote Proxy Host data in ID Payload:  Address 20.0.0.1, Protocol 0,
Port 0
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing ID payload
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Received local IP Proxy Subnet data in ID Payload:   Address 0.0.0.0, Mask
0.0.0.0, Protocol 0, Port 0
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
QM IsRekeyed old sa not found by addr
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
IKE Remote Peer configured for crypto map: DYNAMIC
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing IPSec SA payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IPSec SA Proposal # 11, Transform # 1 acceptable  Matches global
IPSec SA entry # 10
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
IKE: requesting SPI!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKE got SPI from key engine: SPI = 0xd9191a19
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, oakley constucting quick mode
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing blank hash payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing IPSec SA payload
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing IPSec nonce payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing proxy ID
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Transmitting Proxy Id:
  Remote host: 20.0.0.1  Protocol 0  Port 0
  Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
```

```
136.1.100.200, Sending RESPONDER LIFETIME notification to Initiator
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing qm hash payload
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=be168033) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5)
+ ID (5) + NOTIFY (11) + NONE (0) total length : 176
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=be168033) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing hash payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, loading all IPSEC SAs
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Generating Quick Mode Key!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Generating Quick Mode Key!
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Security negotiation complete for User (CISCO)  Responder, Inbound SPI =
0xd9191a19, Outbound SPI = 0x70ec9942
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKE got a KEY_ADD msg for SA: SPI = 0x70ec9942
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Pitcher: received KEY_UPDATE, spi 0xd9191a19
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Starting P2 rekey timer: 27360 seconds.
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Adding static route for client address: 20.0.0.1
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
PHASE 2 COMPLETED (msgid=be168033)

R1#ping 20.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/11/40 ms

ASA1(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
      current_peer: 136.1.100.200, username: CISCO
      dynamic allocated peer ip: 20.0.0.1

      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 136.1.123.12, remote crypto endpt.: 136.1.100.200

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 70EC9942

    inbound esp sas:
      spi: 0xD9191A19 (3642300953)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
```

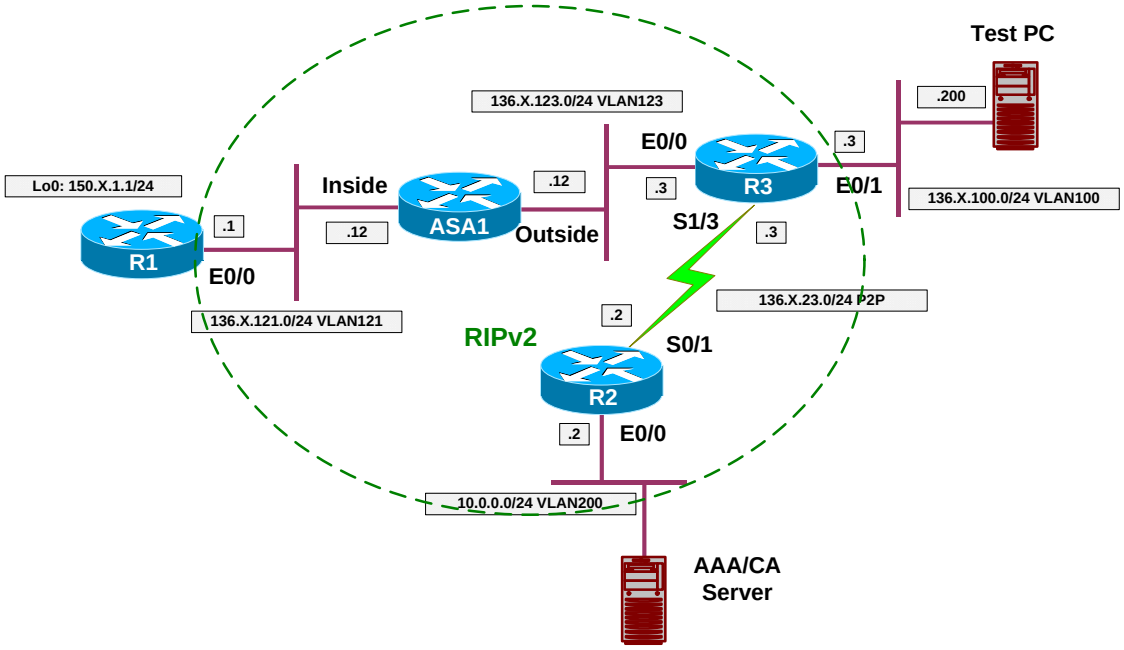
```
        slot: 0, conn_id: 14, crypto-map: DYNAMIC
        sa timing: remaining key lifetime (sec): 28540
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0x70EC9942 (1894553922)
        transform: esp-3des esp-md5-hmac none
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 14, crypto-map: DYNAMIC
        sa timing: remaining key lifetime (sec): 28540
        IV size: 8 bytes
        replay detection support: Y
```

Further Reading

Configuring the VPN Client 3.x to Get a Digital Certificate

The PIX/ASA and IOS ezVPN Remote NW Extension Mode

Objective: Configure the PIX/ASA to support IOS hardware clients in network extension mode.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "The PIX/ASA ezVPN".
- Configure ISAKMP:
  - Enable ISAKMP on the outside interface.
  - Configure ISAKMP policy with priority 10:
    - Use Pre-Shared authentication.
    - Use 3DES cipher.
    - Use MD5 hash.
    - Use DH group 2.
- With Network-Extension mode you do not need to configure any VPN addressing, since remote router does not need it.
- Create access-list SPLIT_TUNNEL:
  - Permit network 136.X.121.0/24.
- Add a local user for Xauth:
  - Create local user "CISCO" with password "CISCO1234".
- Define group-policy named EZVPN as internal:
  - Configure IPsec as the tunneling protocol.
  - Configure DNS server 10.0.0.100.
  - Specify split-tunneling policy "only tunnel networks in the list".
  - Assign split-tunnel network-list SPLIT_TUNNEL.

    - Allow network-extension mode (NEM).
- Define tunnel group:
    - Create tunnel group “EZVPN” of type Remote-Access.
    - Group General Attributes:
        - Set authentication-server group to “LOCAL” (it’s the default value, inherited from default group).
        - Assign group-policy “EZVPN”.
    - Group IPSec Attributes:
        - Specify pre-shared key “CISCO”.
- Configure crypto:
    - Create transform-set 3DES_MD5:
        - Cipher 3DES.
        - Hash MD5.
    - Create dynamic crypto-map DYNAMIC entry 10:
        - Set transform-set 3DES_MD5
        - Set reverse-route
    - Create crypto-map VPN entry 10 to use dynamic crypto-map DYNAMIC.
    - Attach crypto-map VPN to interface outside.
    - Explicitly permit VPN traffic to pass through acess-lists.
- Redistribute static routes into RIP (this will redistribute RRI routes).

Final Configuration

```
ASA1:
!
! ISAKMP configuration
!
crypto isakmp enable outside
crypto isakmp policy 10
 auth pre-share
 encr 3des
 hash md5
 group 2
!
! Split-tunneling ACL
!
access-list SPLIT_TUNNEL permit ip 136.1.121.0 255.255.255.0 any
!
! Local username for Xauth
!
username CISCO password CISCO1234
!
! Tunnel-group policy
!
group-policy EZVPN internal
group-policy EZVPN attributes
 vpn-tunnel-protocol IPSec
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_TUNNEL
 dns-server value 10.0.0.100
 nem enable
!
! Tunnel-group definition
```

```
! Note that "authentication-server-group"
! is LOCAL by default
!
tunnel-group EZVPN type ipsec-ra
tunnel-group EZVPN general-attributes
  authentication-server-group LOCAL
  default-group-policy EZVPN
tunnel-group EZVPN ipsec-attributes
  pre-shared-key CISCO
!
! IPsec transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Dynamic crypto-map
!
crypto dynamic-map DYNAMIC 10 set transform-set 3DES_MD5
crypto dynamic-map DYNAMIC 10 set reverse-route
!
! Define crypto-map
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
!
! Attach crypto map to the interface
!
crypto map VPN interface outside
!
! Permit VPN traffic to bypass ACLs
!
sysop connection permit-vpn
!
! Redistribute static routes into RIP
!
router rip
 redistribute static
```

R3:

```
crypto ipsec client ezvpn EZVPN
 connect manual
 group EZVPN key CISCO
 mode network-extension
 peer 136.1.123.12
!
interface E0/0
 crypto ipsec client ezvpn EZVPN
!
interface E0/1
 crypto ipsec client ezvpn EZVPN inside
```

Verification

Connect R3 to the ASA:

```
R3#crypto ipsec client ezvpn connect
R3#crypto ipsec client ezvpn

Jan 20 16:36:01.429: EZVPN(EZVPN): Pending XAuth Request, Please enter the
following command:
Jan 20 16:36:01.429: EZVPN: crypto ipsec client ezvpn xauth
```

```
R3#crypto ipsec client ezvpn xauth
Username: : CISCO
Password: : CISCO1234

R3#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : EZVPN
Inside interface list: Ethernet0/1,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 10.0.0.100
Split Tunnel List: 1
       Address    : 136.1.121.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
```

Verify RRI:

```
ASA1(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    136.1.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:20, outside
R    136.1.23.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:20, outside
S    136.1.100.0 255.255.255.0 [1/0] via 136.1.123.3, outside
C    136.1.121.0 255.255.255.0 is directly connected, inside
C    136.1.123.0 255.255.255.0 is directly connected, outside
R    10.0.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:20, outside
R    150.1.1.0 255.255.255.0 [120/1] via 136.1.121.1, 0:00:09, inside

R1#ping 136.1.100.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.100.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms

R3#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.123.3

   protected vrf:
   local  ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
   current_peer: 136.1.123.12:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

```
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.123.12
     path mtu 1500, media mtu 1500
     current outbound spi: BA77E350

     inbound esp sas:
      spi: 0x6FD779C7(1876392391)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4501355/28260)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xBA77E350(3128419152)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4501355/28260)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

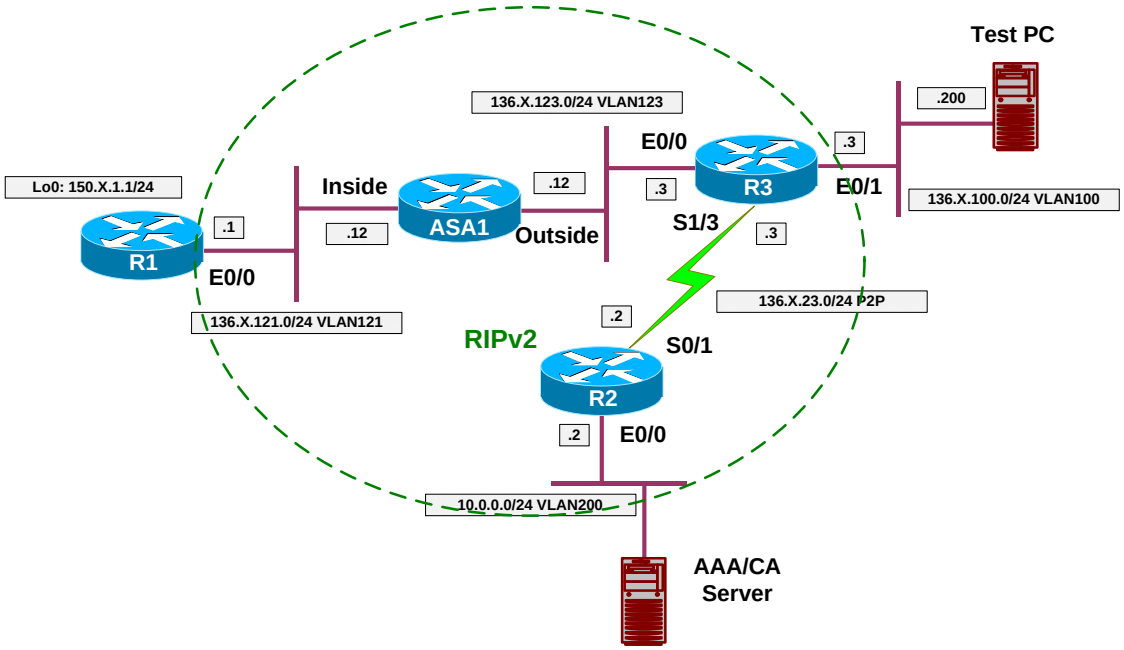
Further Reading

PIX/ASA 7.x Easy VPN with an ASA 5500 as the Server and Cisco 871 as the Easy VPN Remote Configuration Example

WebVPN and SSL VPN

ASA and WebVPN Client

Objective: Configure the PIX/ASA to accept WebVPN connections and authenticate users internally.



Directions

- Configure devices as per the scenario "VPN/Common Configuration" "PIX/ASA Easy VPN/WebVPN".
- We would like to set up basic WebVPN functionality, permitting WebVPN users from outside to access the inside servers.
- At the same time, we would like to permit selected outside users to access ASDM from the outside interace.
- Configure WebVPN globally:
  - Configure WebVPN to run on port 444 instead of default 443.
  - Enable WebVPN on the outside interface.
  - Permit user to choose among the WebVPN tunnel groups.
  - Create URL-List named "LIST":
    - Add entry "R1" with value http://136.1.121.1
- Configure WebVPN Policy:
  - Create access-list "WEBACCESS" of type "webtype":
    - Permit http connections on ports 80 and 443.

    - Create group-policy WEBVPN:
        - Specify WebVPN attributes:
            - Permit URL entry and WebFilter functions.
            - Apply WEBACCESS filter.
            - Specify URL List “LIST”.
- Create local user “CISCO” with password “CISCO1234”
- Configure WebVPN tunnel-group named “WEBVPN”:
    - General Attributes:
        - Specify LOCAL authentication.
        - Apply WEBVPN group-policy.
    - WebVPN Attributes:
        - Authenticate via AAA.
        - Specify group-alias “WEBVPN” so that users may choose group upon signon.
- Lock use “CISCO” in group “WEBVPN”.
- Enable ASDM on the outside interface.
    - Permit HTTPS connections from any host

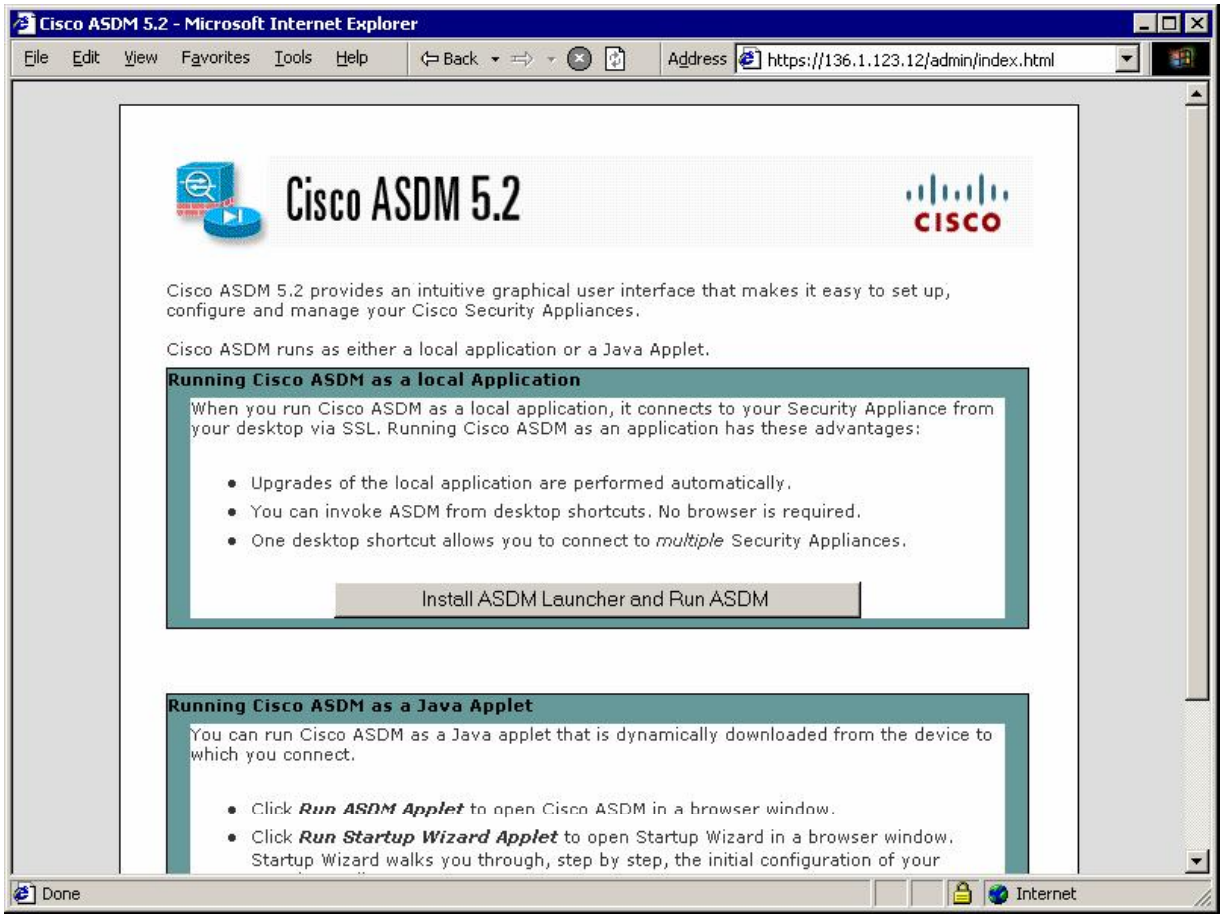
Final Configuration

```
ASA1:
webvpn
 port 444
 enable outside
 url-list LIST "R1" http://136.1.121.1
 tunnel-group-list enable
!
! Web-type access-list to permit only ports 80/443
!
access-list WEBACCESS webtype permit tcp any eq www
access-list WEBACCESS webtype permit tcp any eq https
!
! Group-policy to apply web-type access-list
!
group-policy WEBVPN internal
group-policy WEBVPN attributes
 webvpn
  functions url-entry filter
  filter value WEBACCESS
  url-list value LIST
!
! Local username to authenticate remote users
!
username CISCO password CISCO1234
!
! Lock this user into WEBVPN group only
!
username CISCO attributes
 group-lock value WEBVPN
!
! Tunnel-group definition
!
tunnel-group WEBVPN type webvpn
tunnel-group WEBVPN general-attributes
 default-group-policy WEBVPN
```

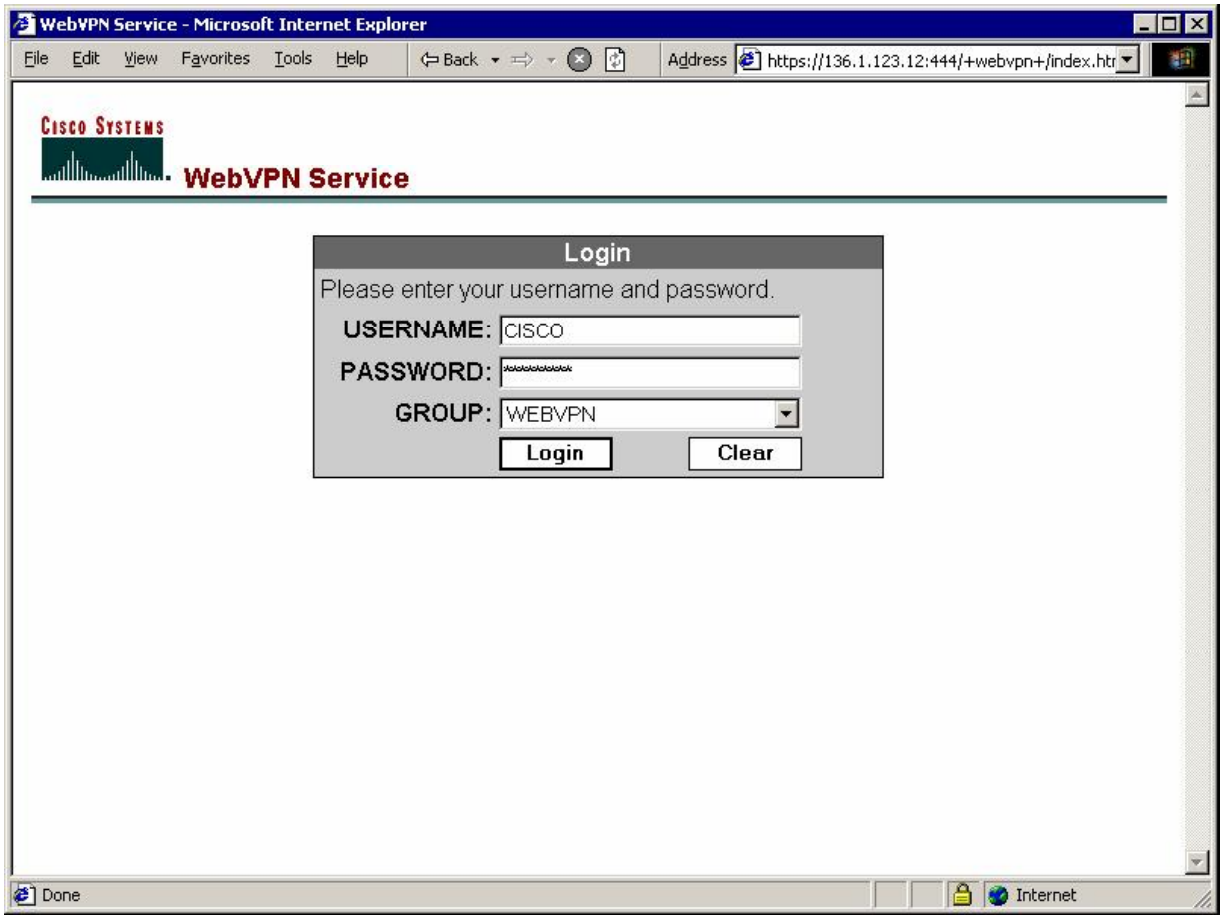
```
!
tunnel-group WEBVPN webvpn-attributes
 group-alias WEBVPN enable
 authentication aaa
!
! Enable ASDM on the outside
!
asdm image disk0:/asdm-522.bin
http server enable
http 0 0 outside
```

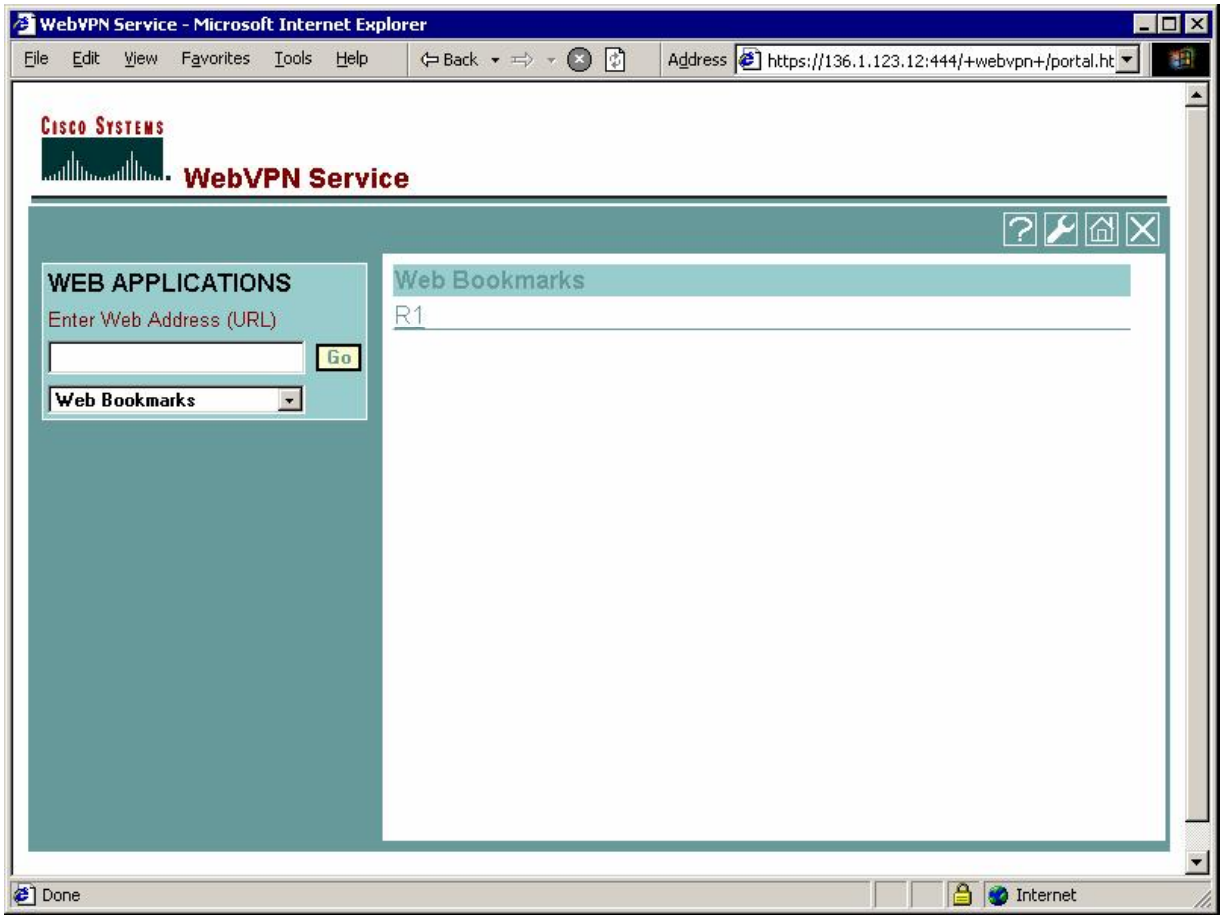
Verification

Initiate connection to the ASA, default port 443:

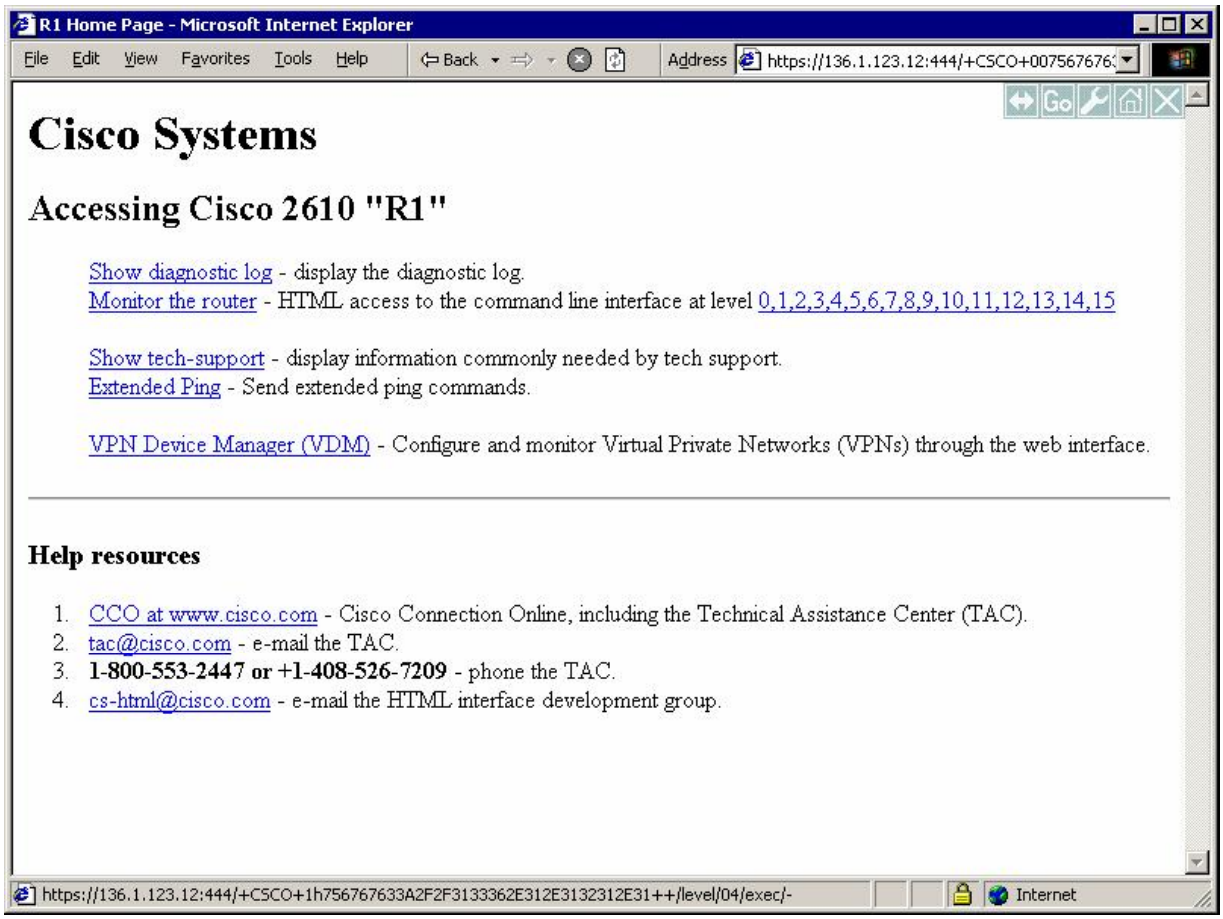


Connect to port 444 and login to WebVPN:


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.123.12:444/+webvpn+/index.htr
Cisco Systems
WebVPN Service
Login
Please enter your username and password.
USERNAME: CISCO
PASSWORD:
GROUP: WEBVPN
Login
Clear
Done
Internet


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.123.12:444/+webvpn+/portal.ht
CISCO SYSTEMS
WebVPN Service
WEB APPLICATIONS
Enter Web Address (URL)
Go
Web Bookmarks
Web Bookmarks
R1
Done
Internet

Click the bookmark URL "R1":

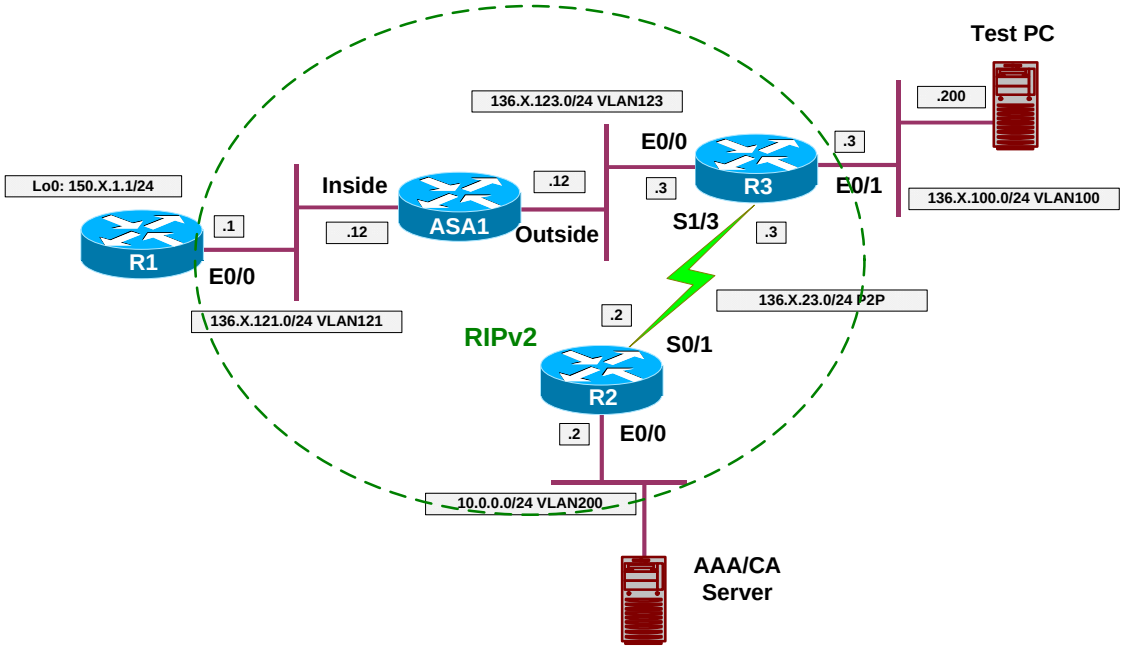


Further Reading

ASA with WebVPN and Single Sign-on using ASDM and NTLMv1 Configuration Example

ASA and WebVPN Port Forwarding

Objective: Configure the PIX/ASA to accept WebVPN connections and forward local connections on specific port to the remote host.



Directions

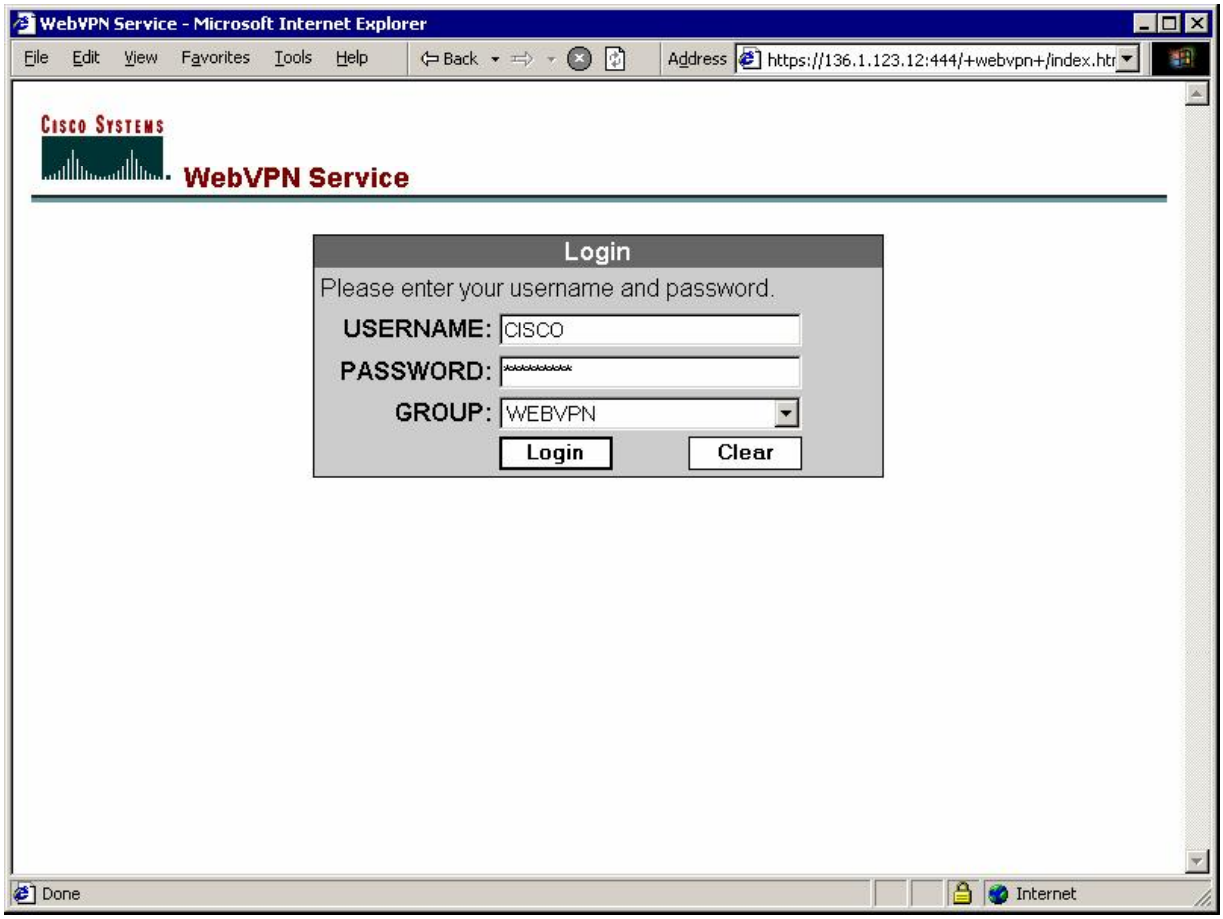
- Configure devices as per the scenario "VPN/WebVPN and SSL VPN" "ASA and WebVPN Clients".
- As the added function, we will permit users to use application port forwarding.
- The way it works is that user's browser dowloads Java applet, which listens on specified port, and forward connections to remote host via SSL connection.
- Change group-policy WEBVPN:
  - Permit port-forward.
  - Enable applet auto-download.
- Change webtype access-list WEBACCESS:
  - Permit access via telnet.
- Configure WebVPN forward rule named TELNET_R3:
  - Forward port 20023 to host R1 port 23.
- Assign this rule to group-policy WEBVPN.

Final Configuration

```
ASA1:
group-policy WEBVPN attributes
 webvpn
  functions url-entry port-forward filter auto-download
  port-forward value TELNET_R3
  port-forward-name value Port Forwarding
  exit
 exit
!
! Permit telnet access in WebACL
!
access-list WEBACCESS webtype permit tcp any eq 23
!
! Port-forwarding config is global
!
webvpn
 port-forward TELNET_R3 20023 136.1.121.1 telnet
```

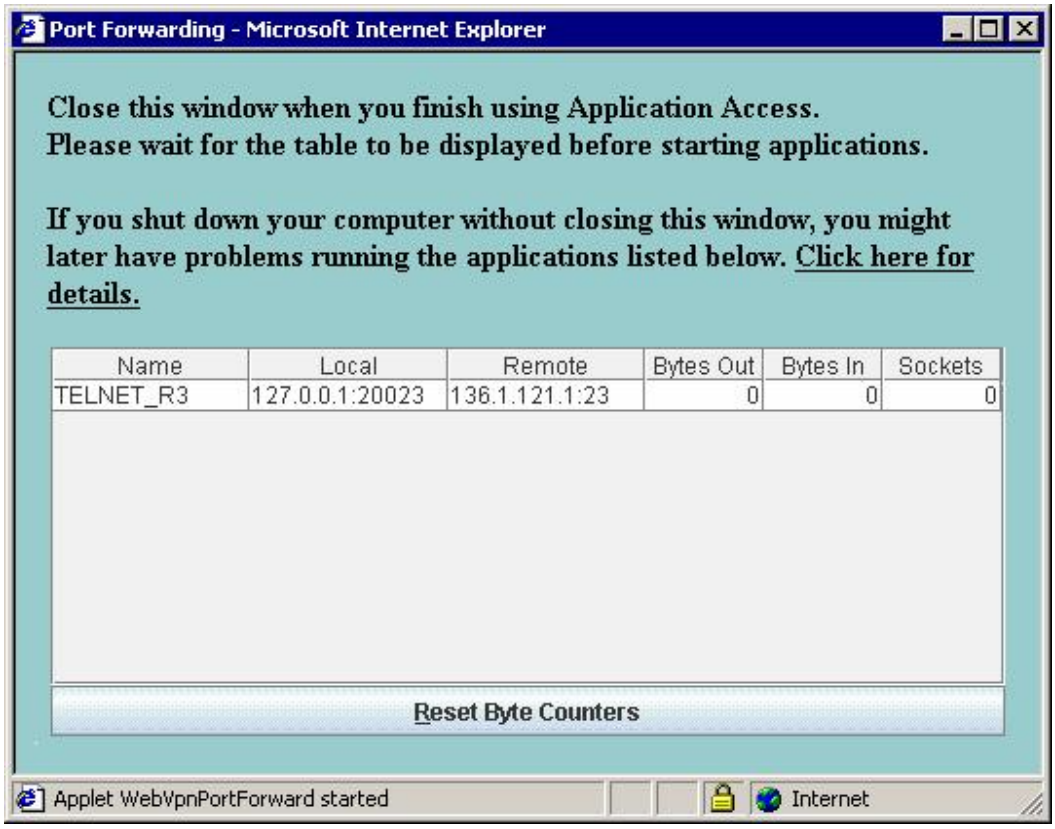
Verification

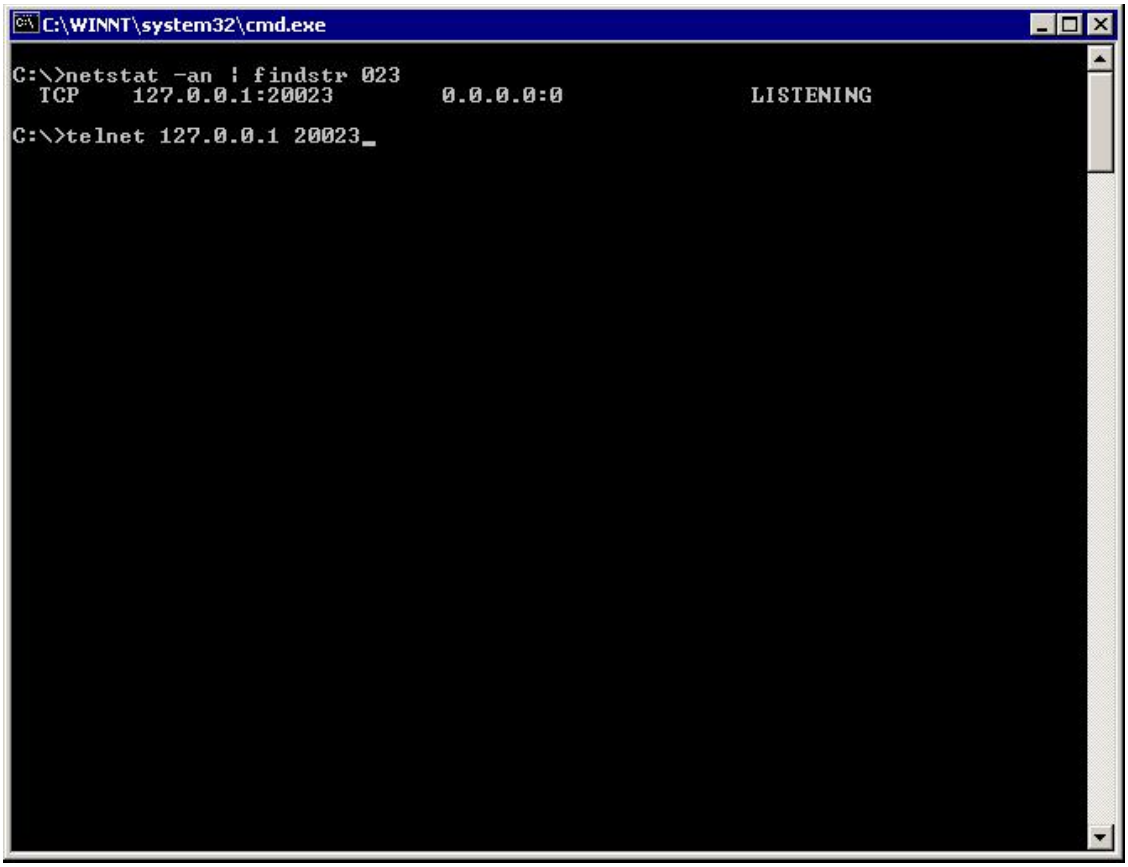
Connect to port 444 and login to WebVPN services:

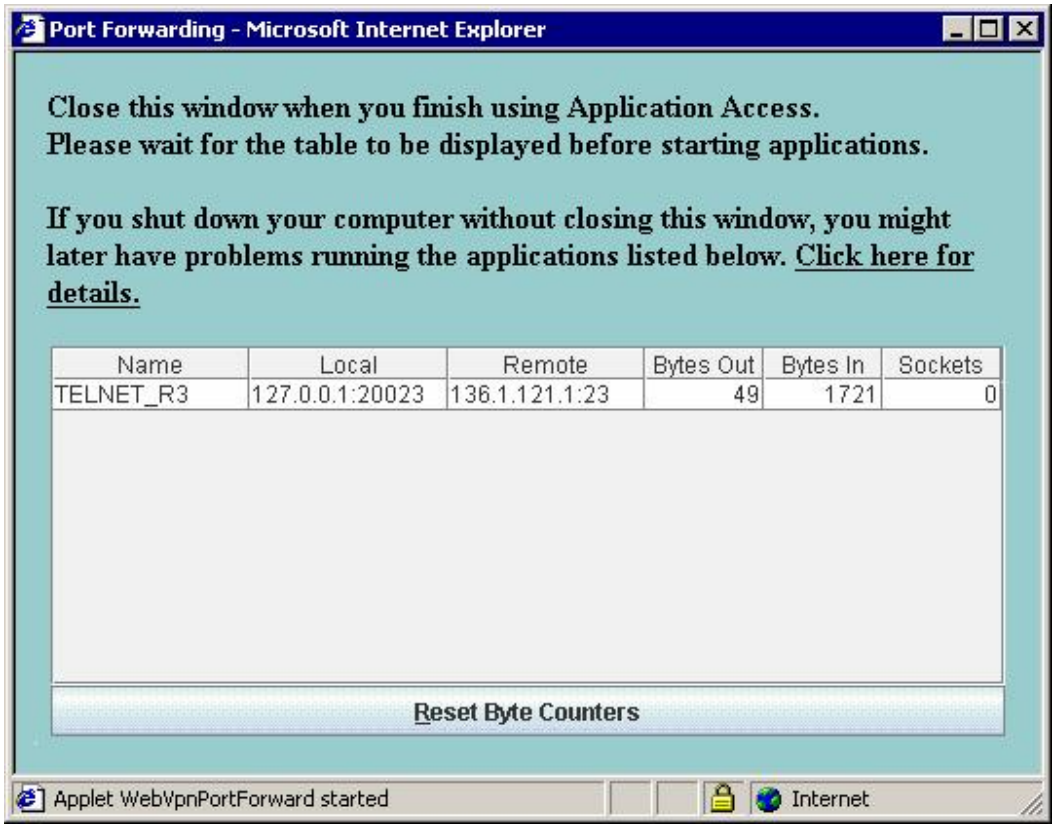



WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.123.12:444/+webvpn+,
Links
Cisco Systems
WebVPN Service
WEB APPLICATIONS
Enter Web Address (URL)
Go
Web Bookmarks
PORT FORWARDING
Start Application Client
Go
Web Bookmarks
R1
Done
Internet

Application forwarding is started automatically:




C:\WINNT\system32\cmd.exe
C:\>netstat -an | findstr 023
TCP 127.0.0.1:20023 0.0.0.0:0 LISTENING
C:\>telnet 127.0.0.1 20023_

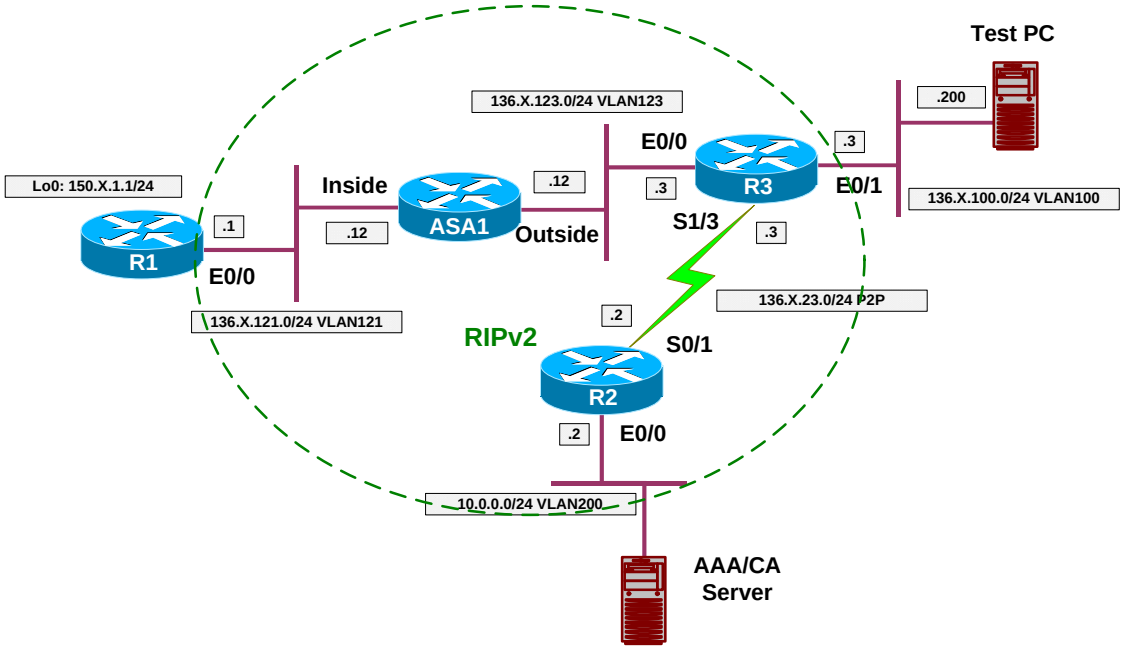


Further Reading

Thin-Client SSL VPN (WebVPN) on ASA with ASDM Configuration Example

ASA and SSL VPN Client

Objective: Configure the ASA to support remote SSL VPN Client connections.



Directions

- Configure devices as per the scenario "VPN/Common Configuration" "PIX/ASA Easy VPN/WebVPN".
- by
- step
- directions
- on
- how
- to
- complete
- objective

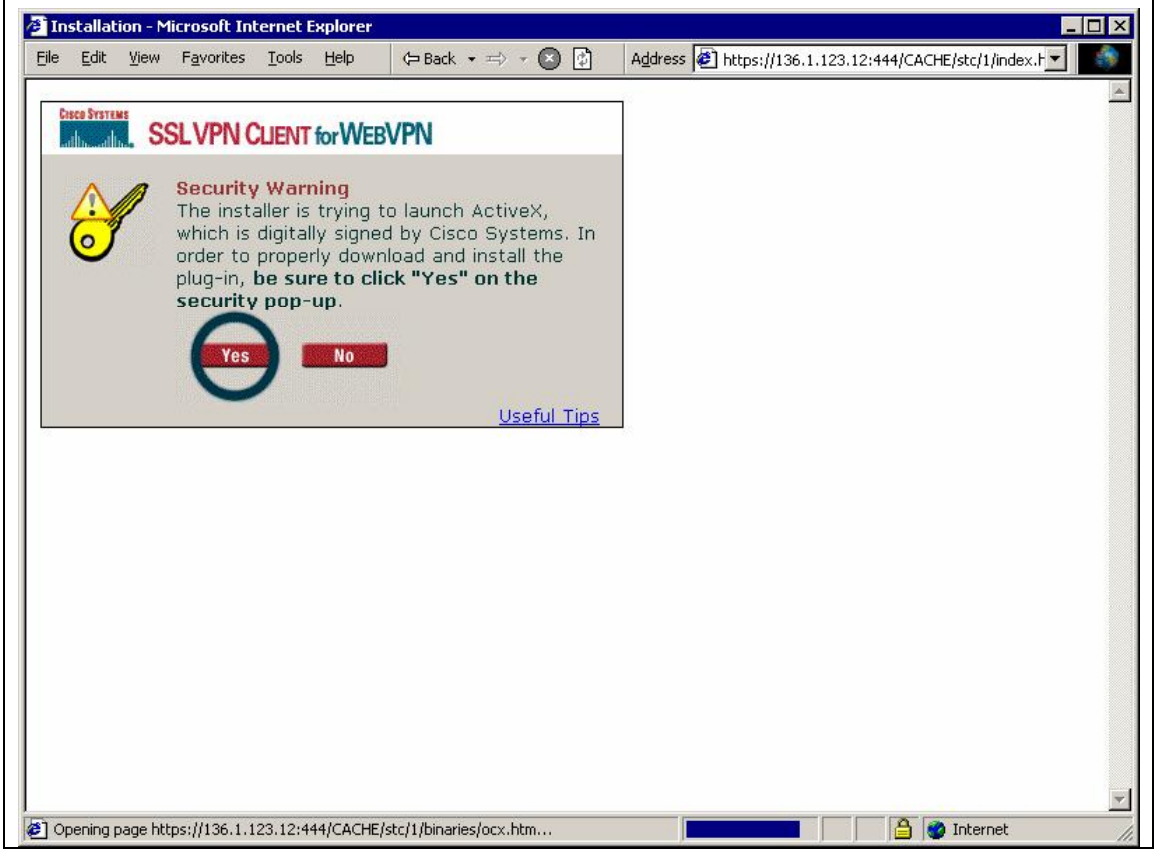
Final Configuration

ASA1 :

```
webvpn
 port 444
 webvpn enable outside
 svc image disk0:/sslclient-win-1.1.3.173.pkg 1
 svc enable
!
ip local pool SSLVPN 20.0.0.1-20.0.0.254
username CISCO password CISCO1234
!
!
```

```
!
group-policy SSLVPN internal
group-policy SSLVPN attributes
 vpn-tunnel-protocol webvpn
 webvpn
  svc required
  svc keep-installer installed
!
!
!
tunnel-group SSLVPN type webvpn
tunnel-group SSLVPN general-attributes
 address-pool SSLVPN
 default-group-policy SSLVPN
!
!
!
username CISCO attributes
 vpn-group-policy SSLVPN
```

Verification

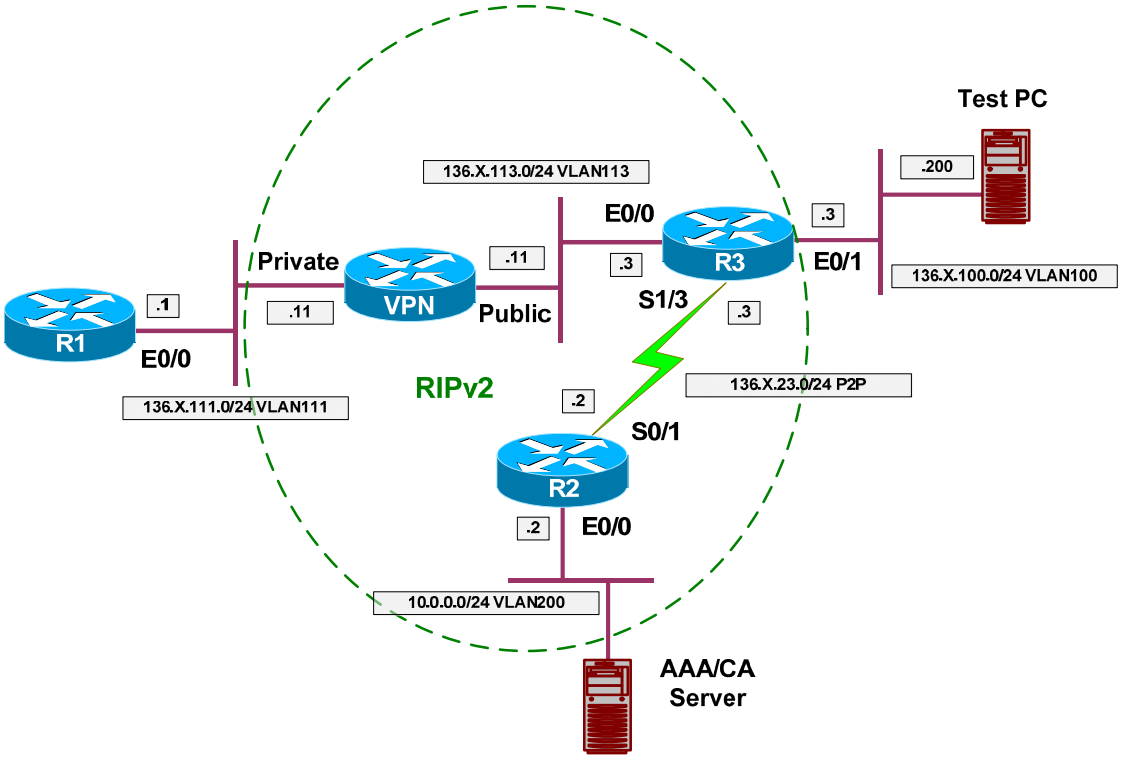


Further Reading

Release Notes for Cisco SSL VPN Client, Release 1.1.0
SSL VPN Client (SVC) on ASA with ASDM Configuration Example

VPN3k and WebVPN Client

Objective: Configure VPN3k concentrator to accept WebVPN client sessions.



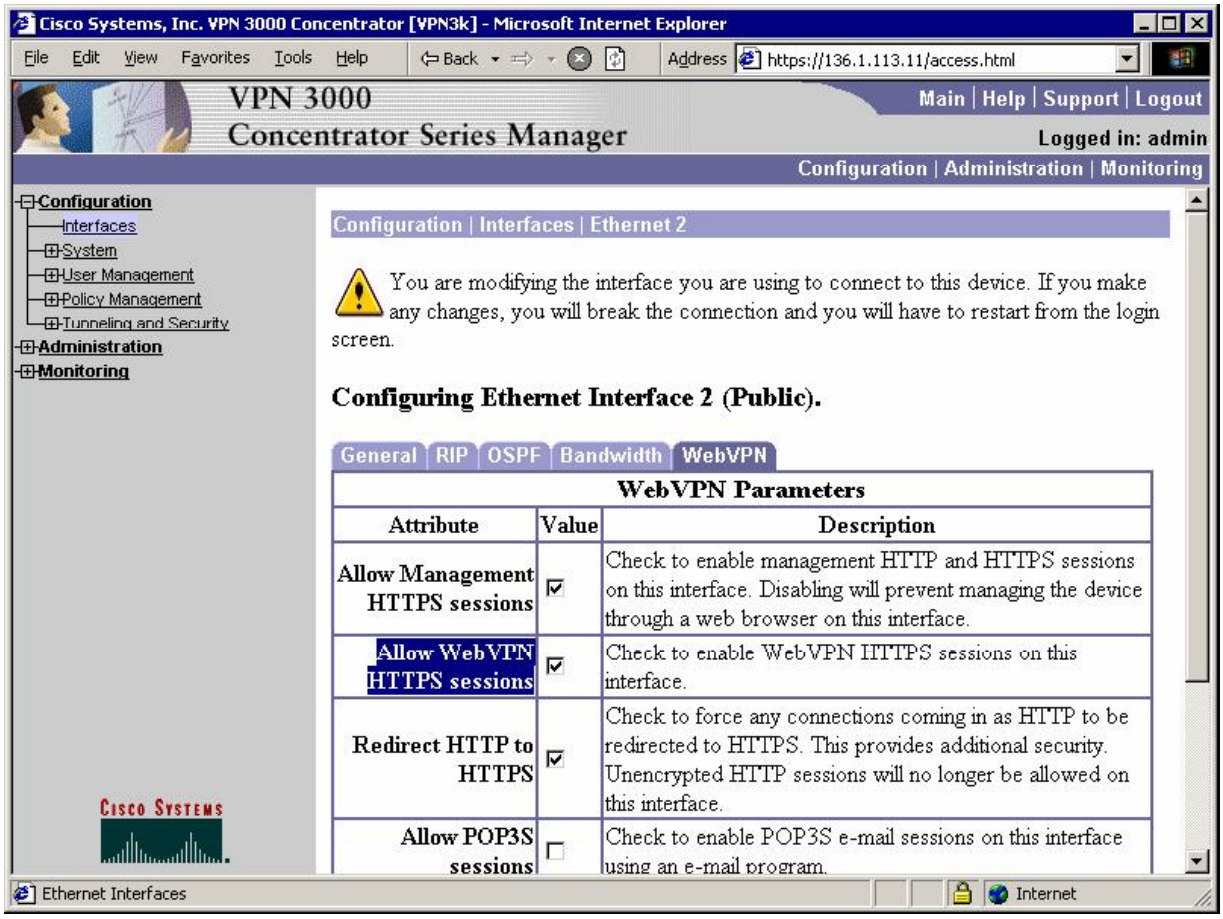
Directions

- Configure devices as per the scenario "VPN/Common Configurations" "VPN3k Easy VPN/WebVPN".
- Enable WebVPN services on the Public interface.
- Configure WebVPN settings:
  - Create URL entry "R1" to "http://136.1.111.1"
- Create group WebVPN:
  - Specify password "CISCO".
  - Permit WebVPN as the only tunneling protocol.
  - Configure WebVPN Attribute:
    - Disable URL entry.
    - Apply WebACL.
    - Configure WebACL to permit only access to URL "http://136.1.111.1"
- Create user "CISCO" with password "CISCO1234" and assign it to group "WEBVPN".

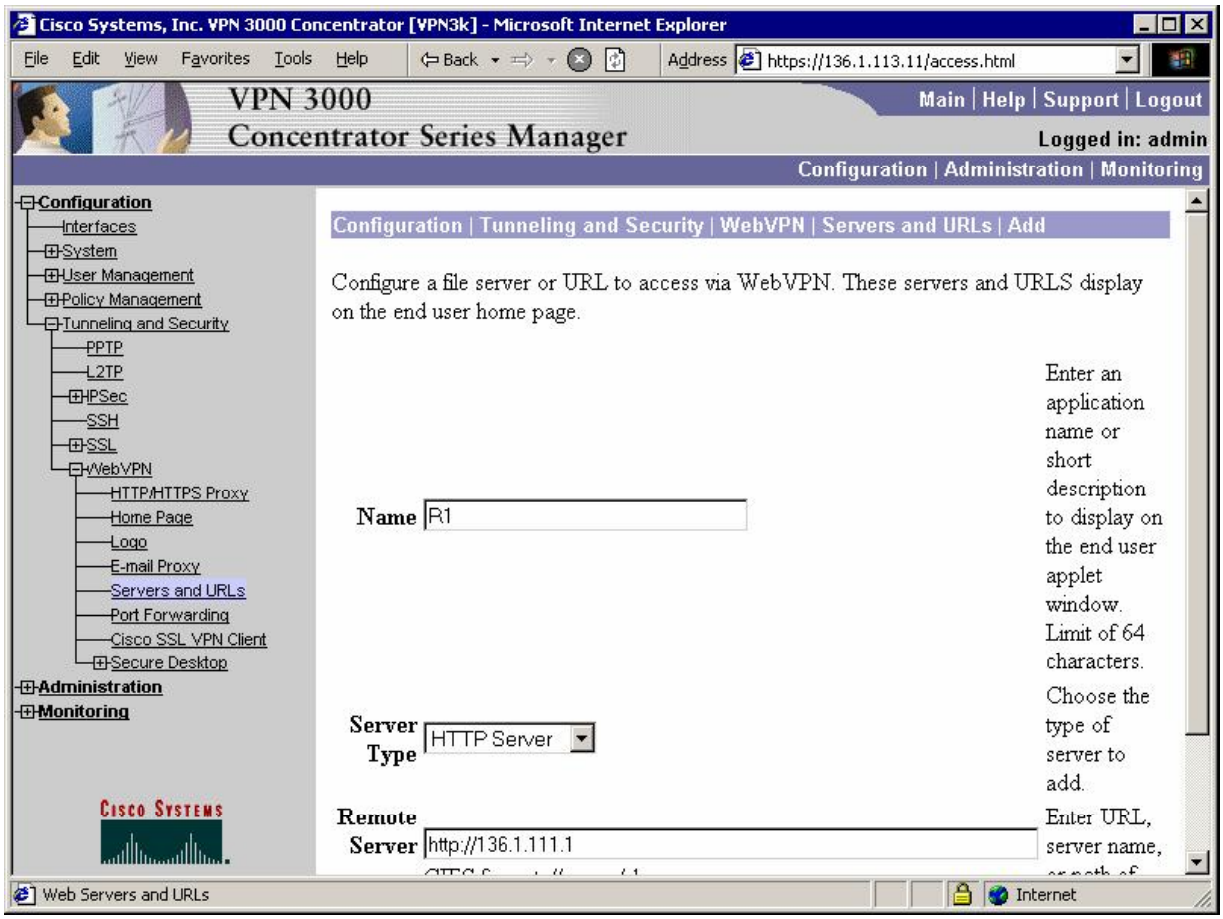
Final Configuration

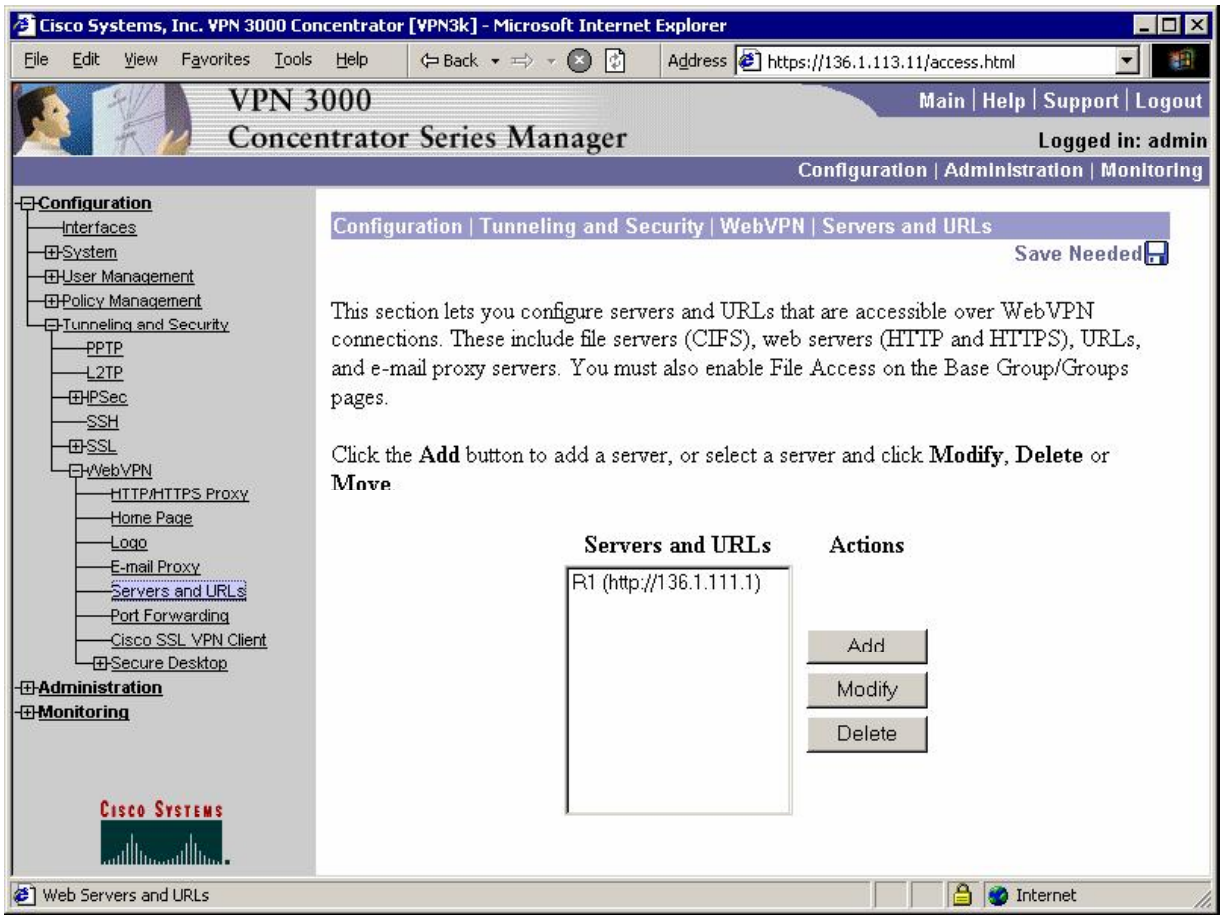
VPN3k CLI:

Enable WebVPN on Public Interface:

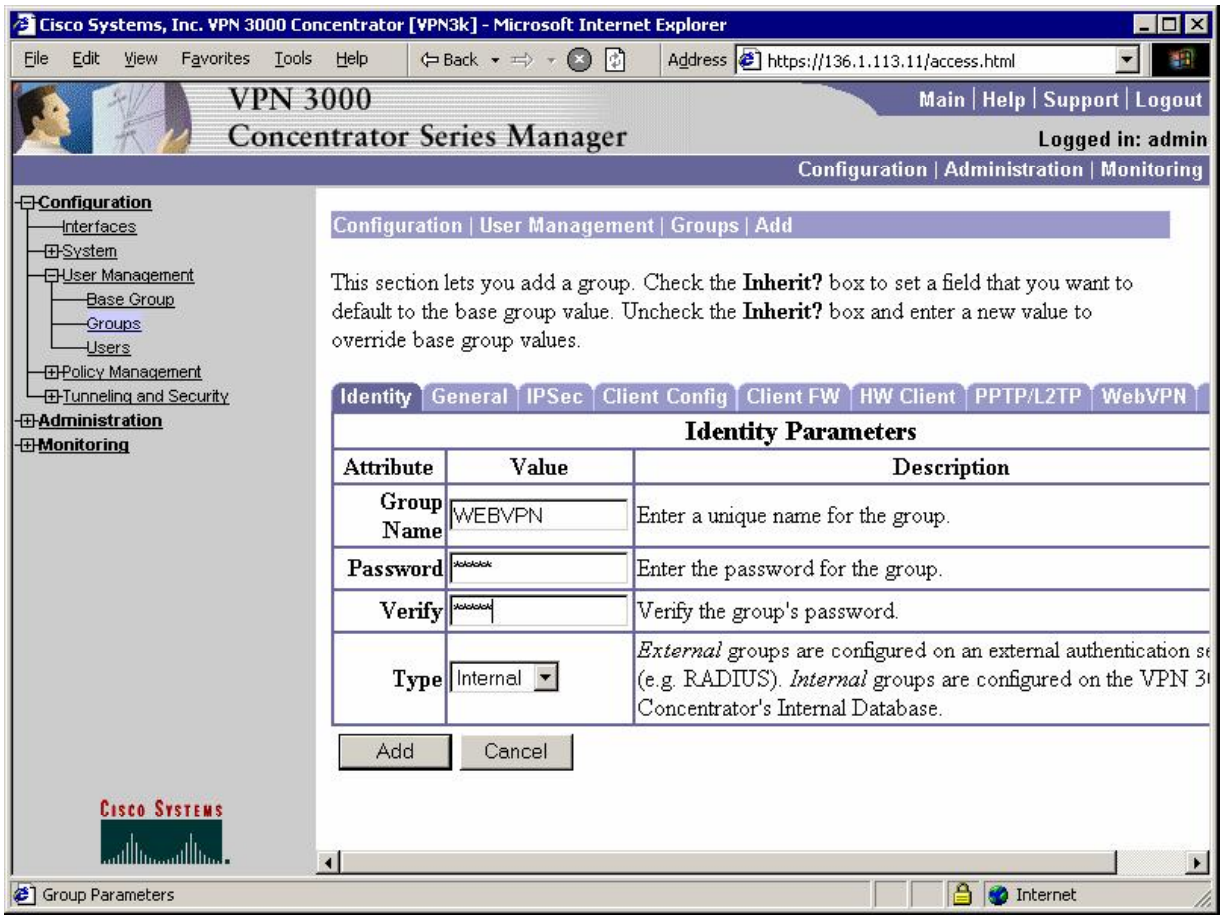


Create static URL entry for R1:

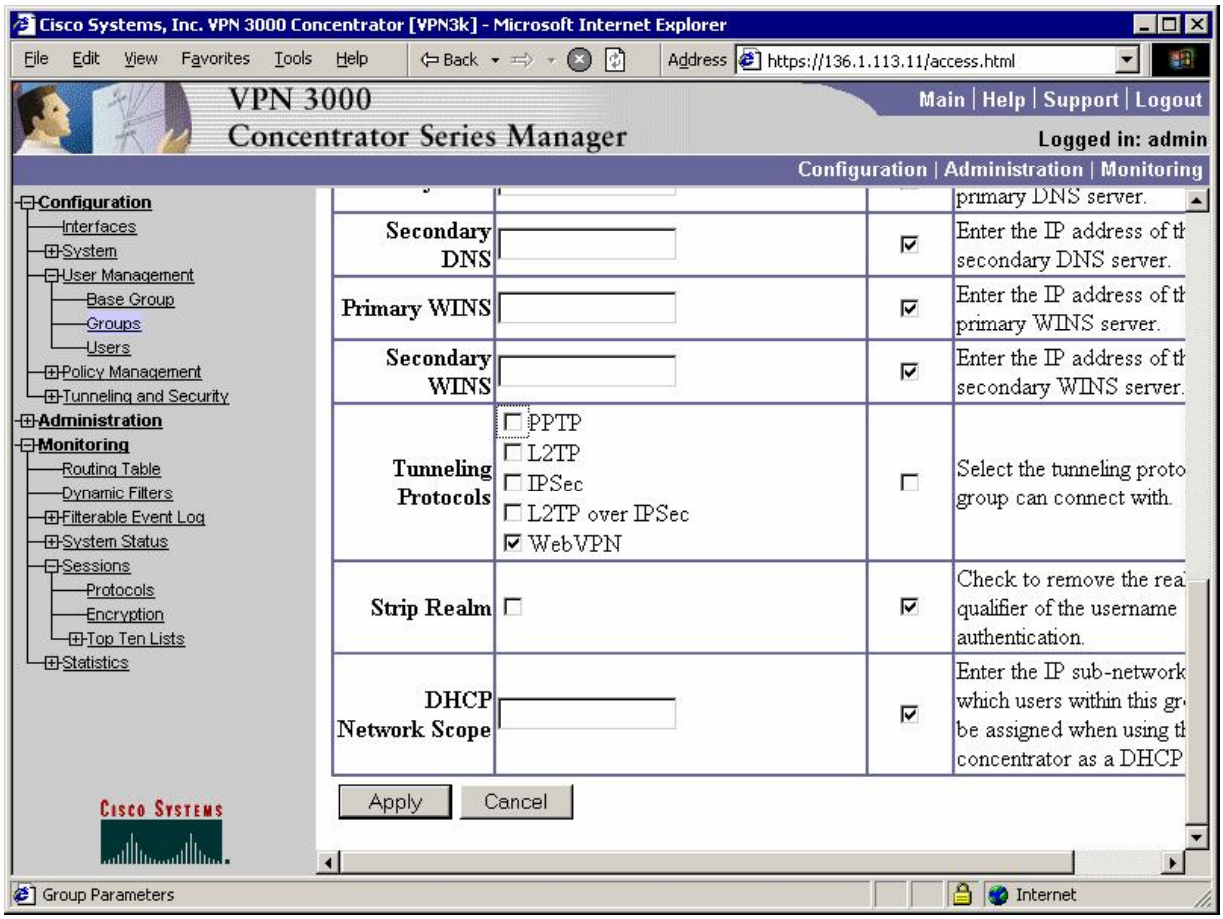



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Tunneling and Security
PPTP
L2TP
IPSec
SSH
SSL
WebVPN
HTTP/HTTPS Proxy
Home Page
Logo
E-mail Proxy
Servers and URLs
Port Forwarding
Cisco SSL VPN Client
Secure Desktop
Administration
Monitoring
Configuration | Tunneling and Security | WebVPN | Servers and URLs
Save Needed
This section lets you configure servers and URLs that are accessible over WebVPN connections. These include file servers (CIFS), web servers (HTTP and HTTPS), URLs, and e-mail proxy servers. You must also enable File Access on the Base Group/Groups pages.
Click the Add button to add a server, or select a server and click Modify, Delete or Move
Servers and URLs
Actions
R1 (http://136.1.111.1)
Add
Modify
Delete
Web Servers and URLs
Internet

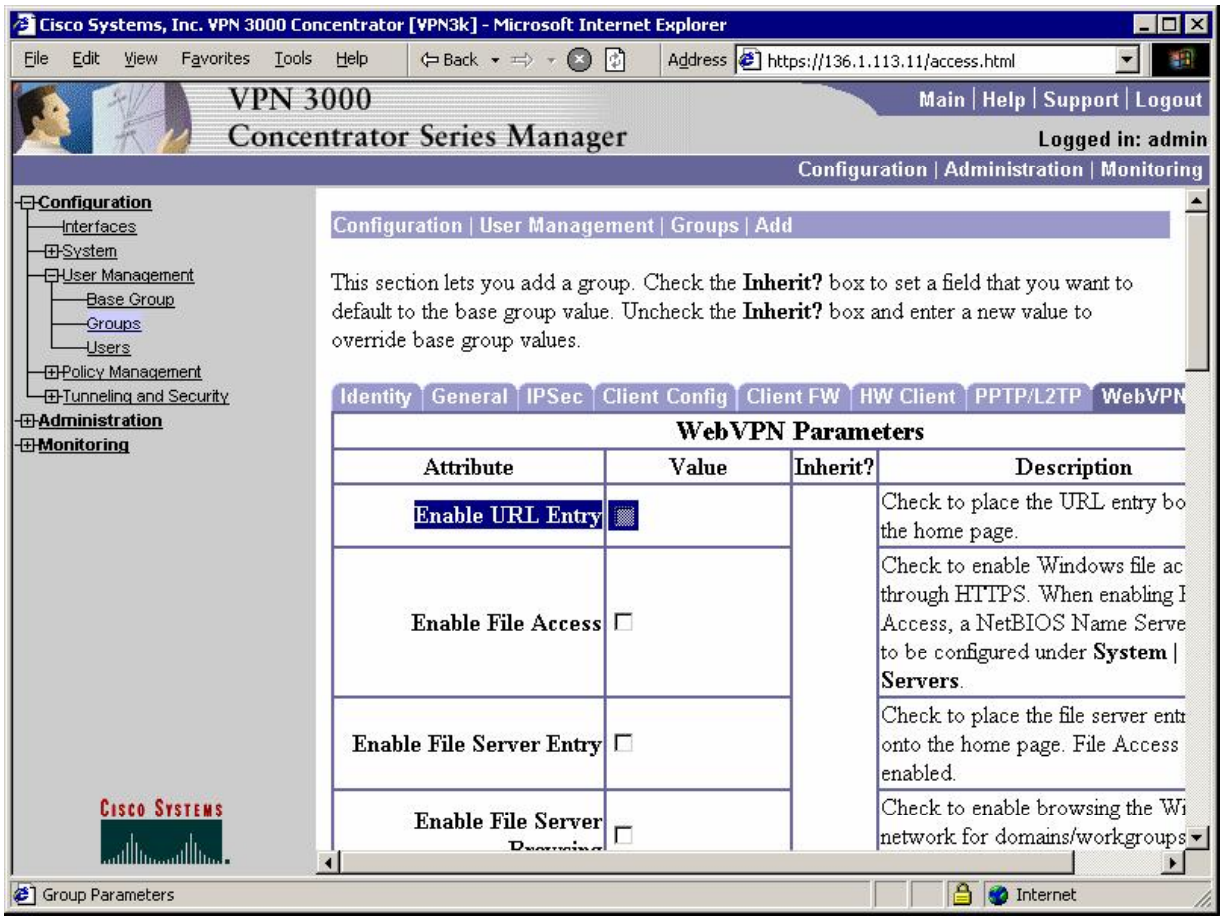
Create group "WEBVPN" with password "CISCO":



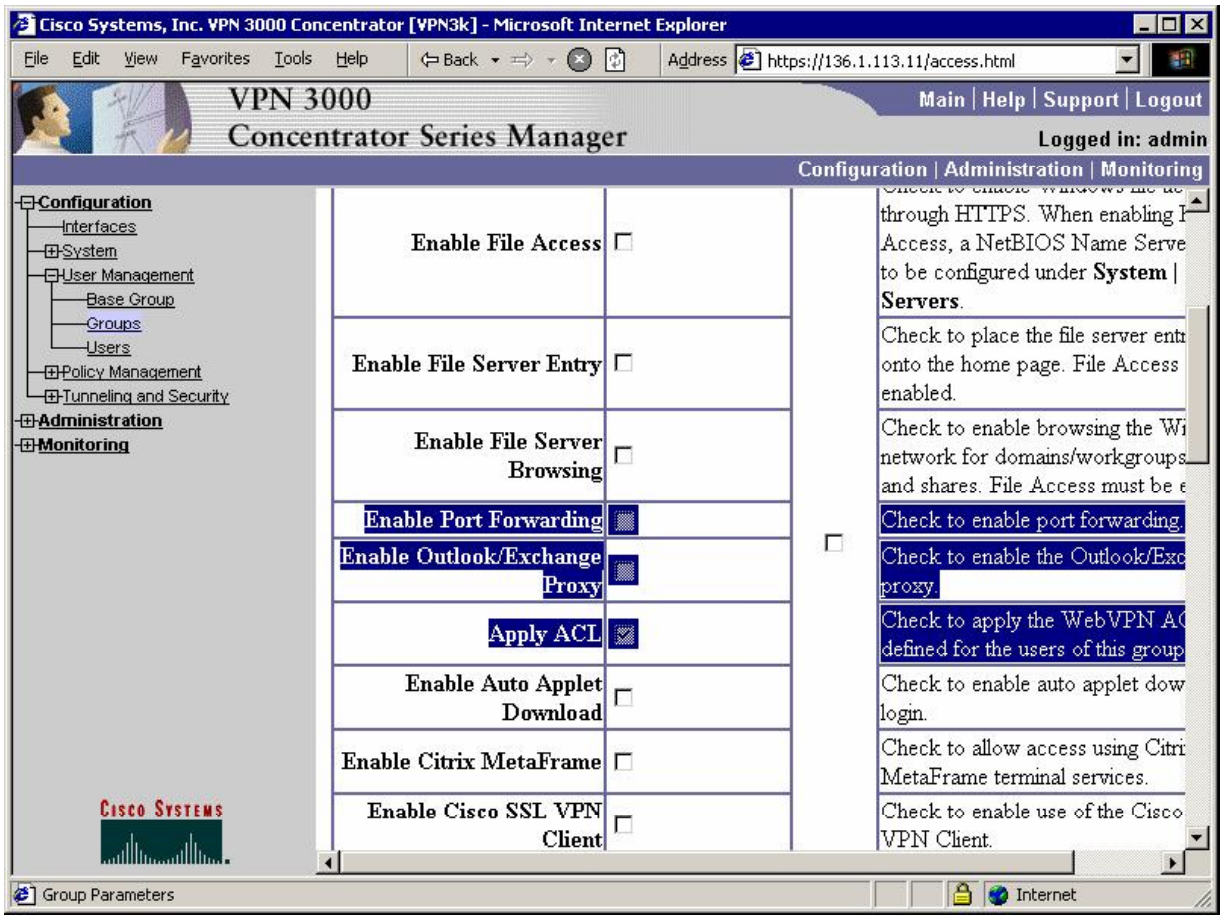
Enable WebVPN as the tunneling protocol:



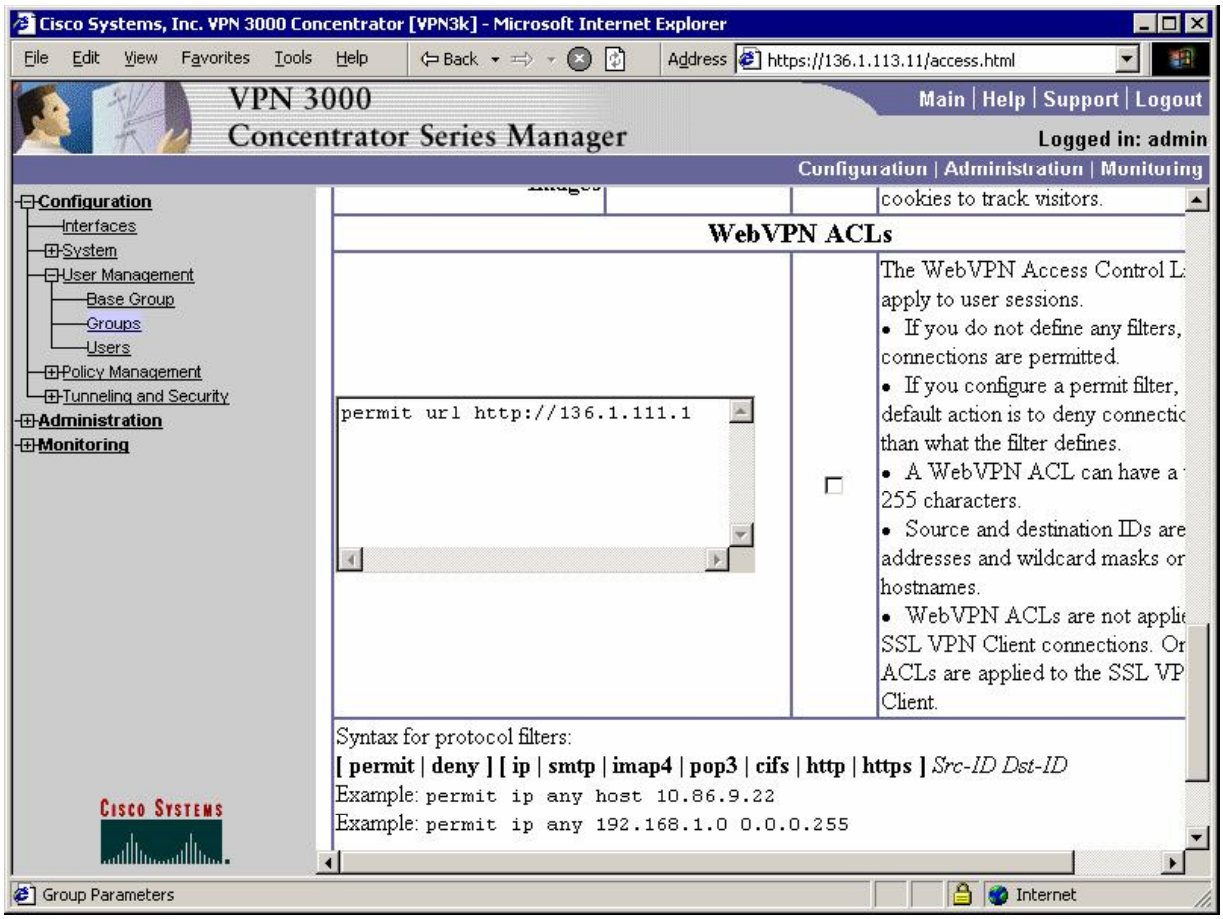
Disable client URL entry:



Permit WebACL Application:



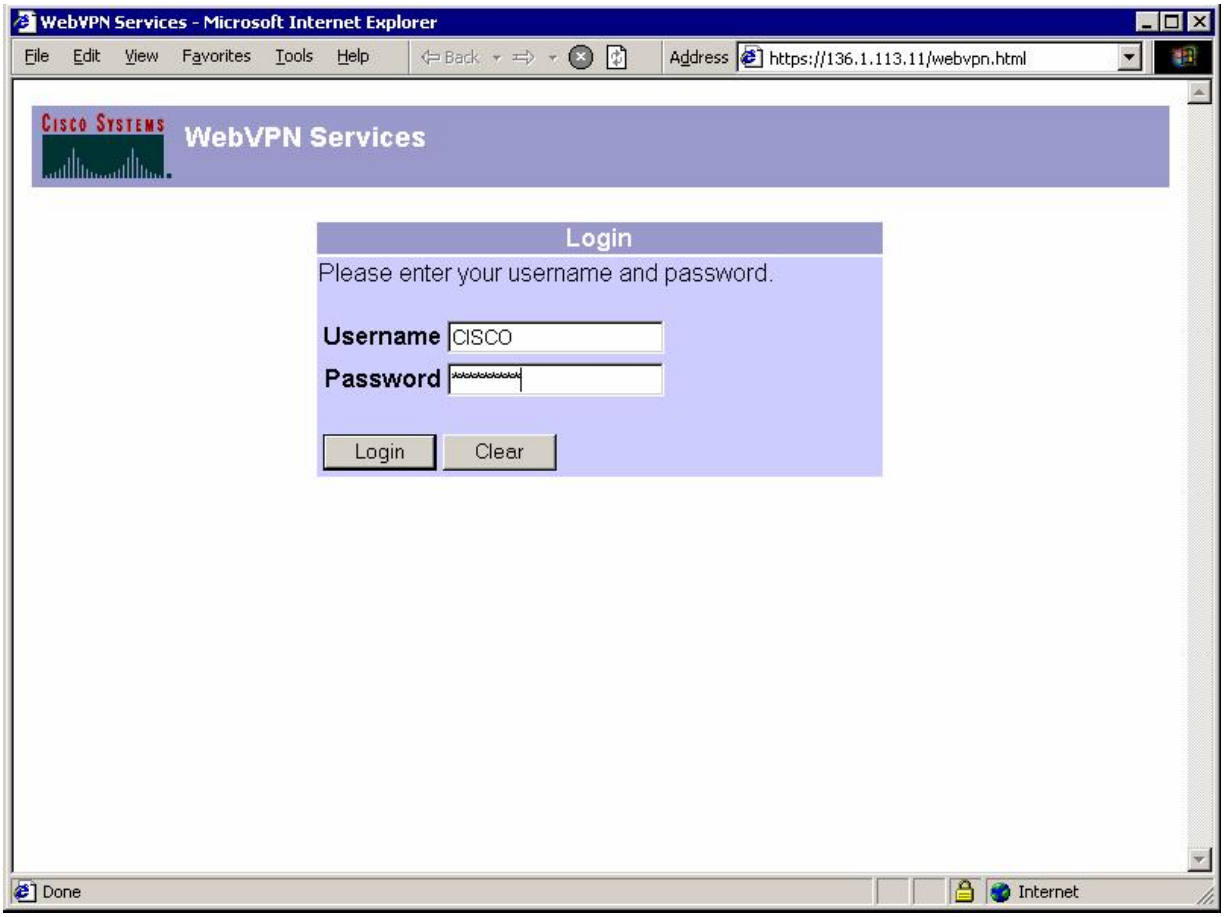
Configure WebACL:

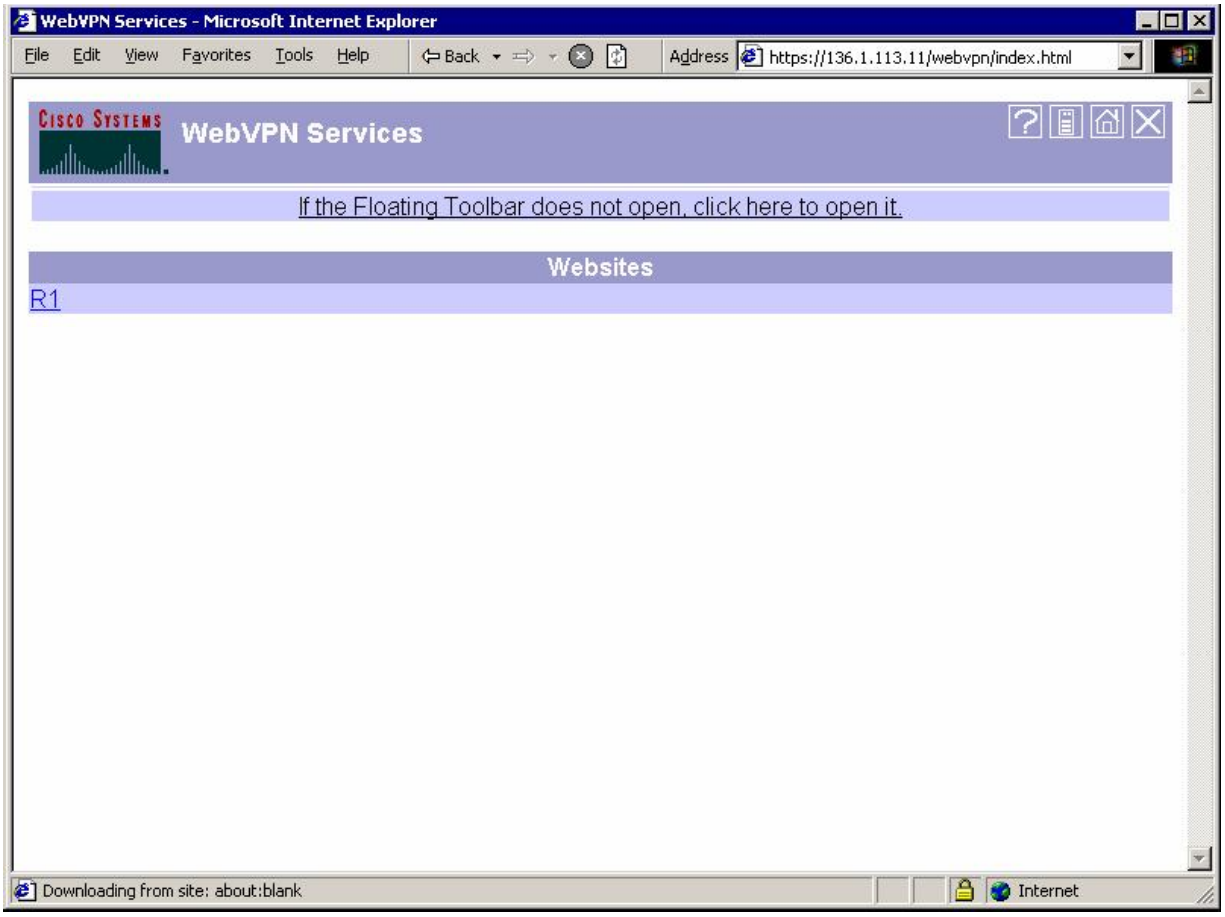


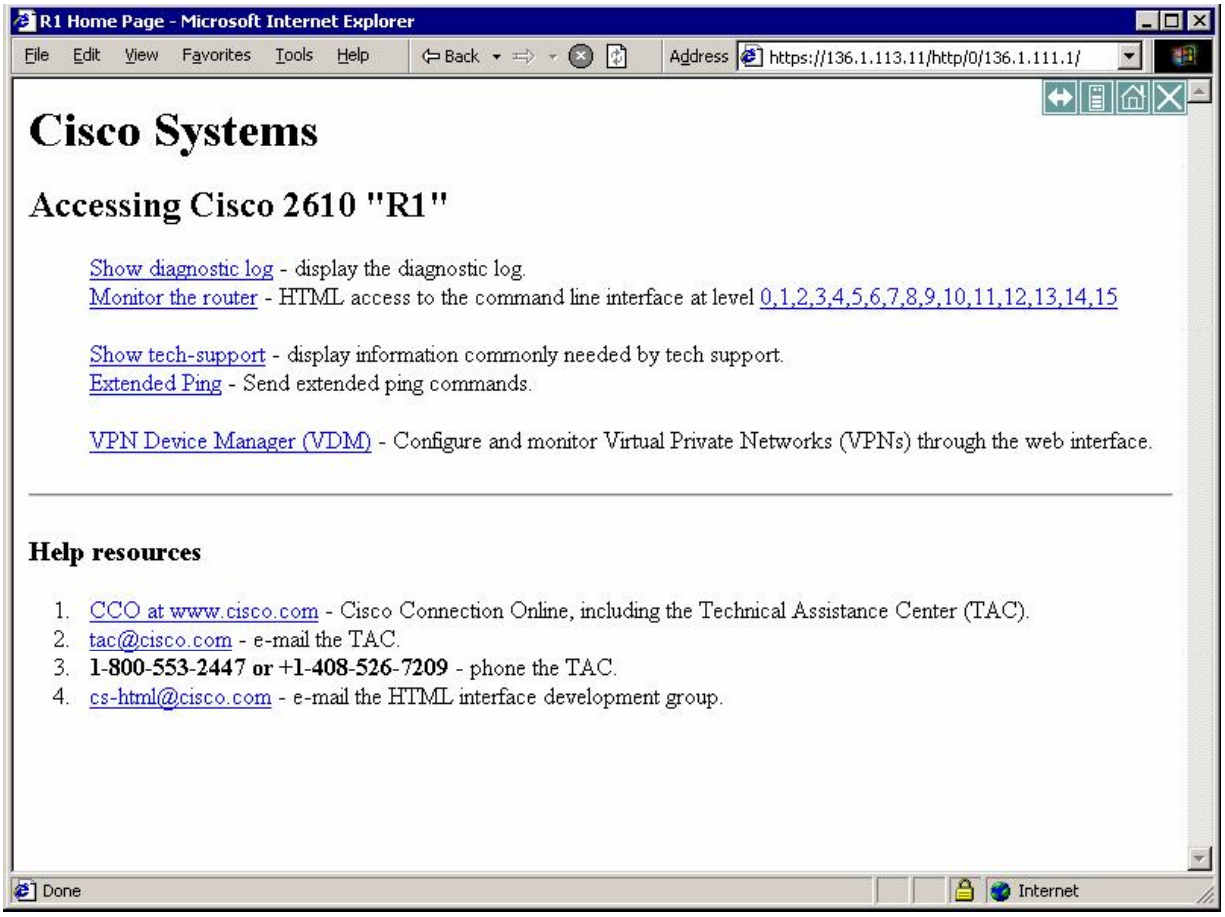
Create user "CISCO" with password "CISCO1234" and add it to group "WEBVPN":

Verification

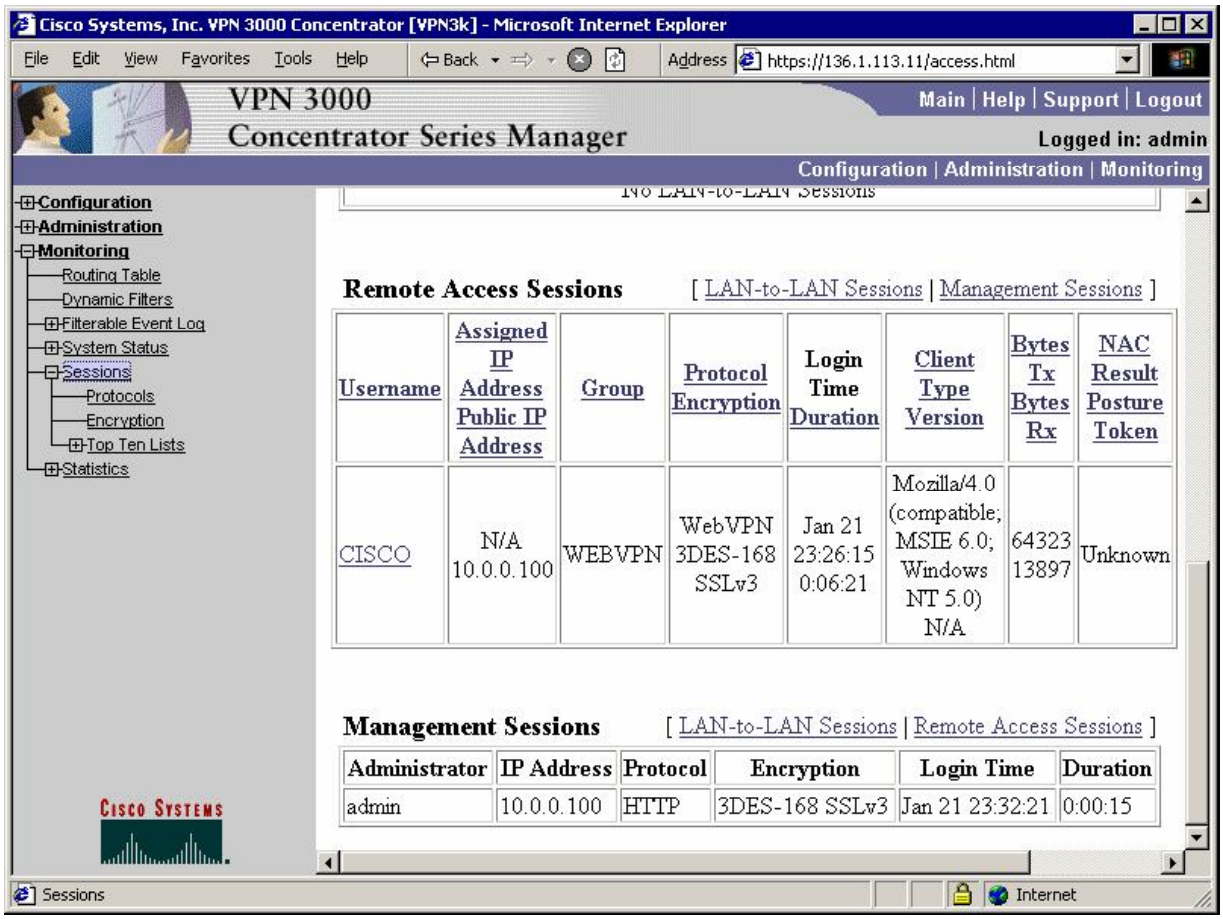
Connect to the public interface of VPN3k:




WebVPN Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/webvpn/index.html
CISCO SYSTEMS
WebVPN Services
If the Floating Toolbar does not open, click here to open it.
Websites
R1
Downloading from site: about:blank
Internet


R1 Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/http/0/136.1.111.1/
Cisco Systems
Accessing Cisco 2610 "R1"
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.
VPN Device Manager (VDM) - Configure and monitor Virtual Private Networks (VPNs) through the web interface.
Help resources
1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.
Done
Internet

Check statistics on the VPN3k:

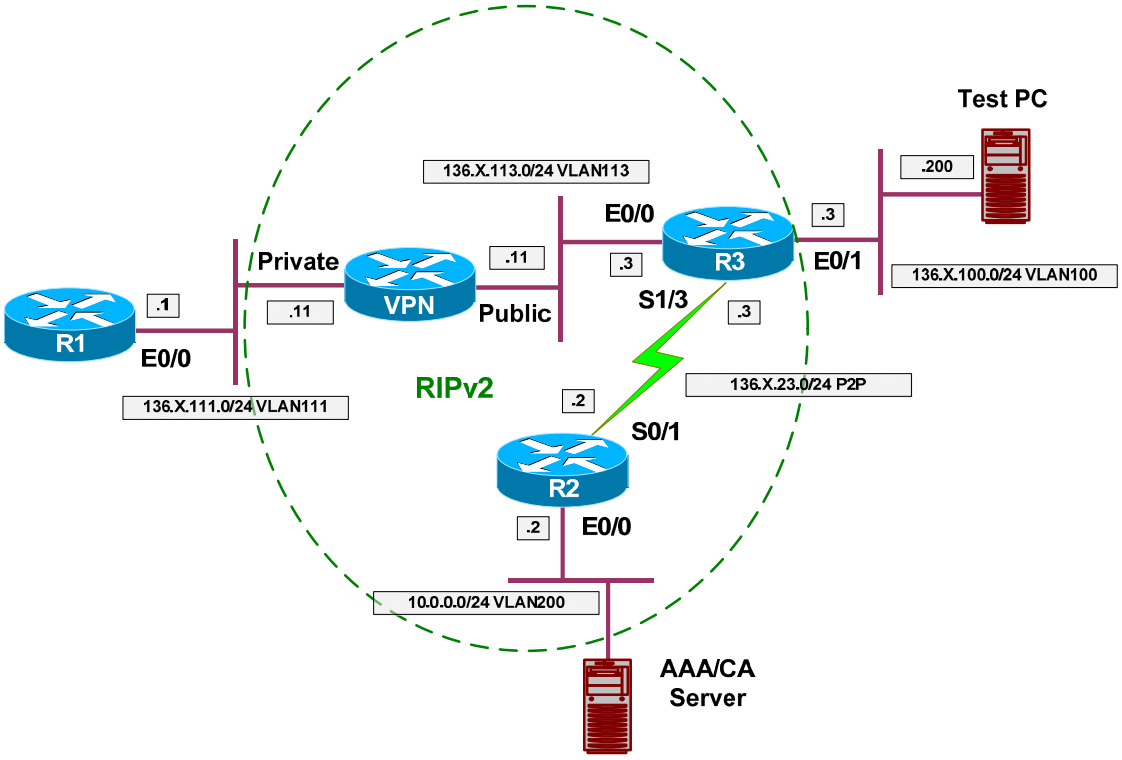


Further Reading

Configuring the VPN Concentrator for WebVPN

VPN3k and WebVPN Port Forwarding

Objective: Configure VPN3k to provide port-forwarding service to WebVPN clients.



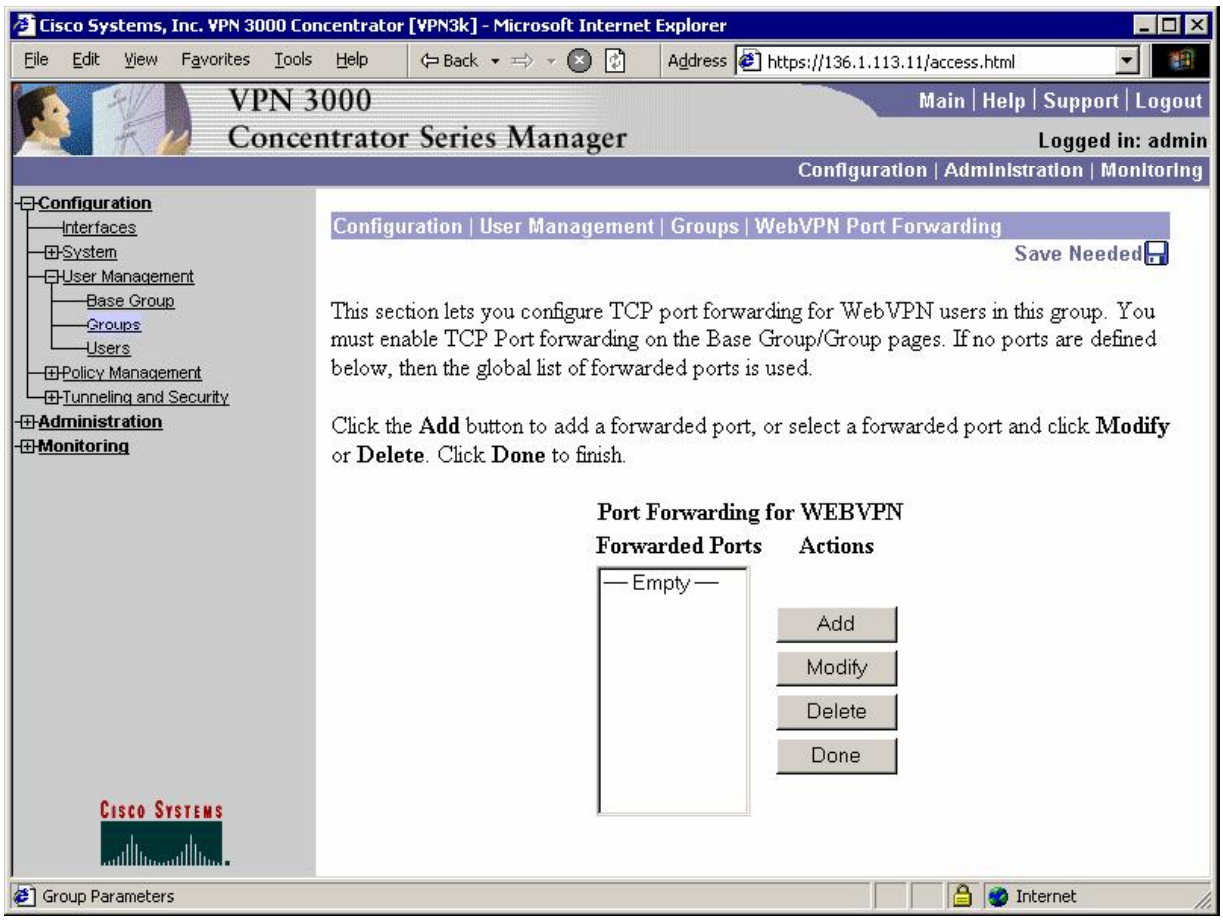
Directions

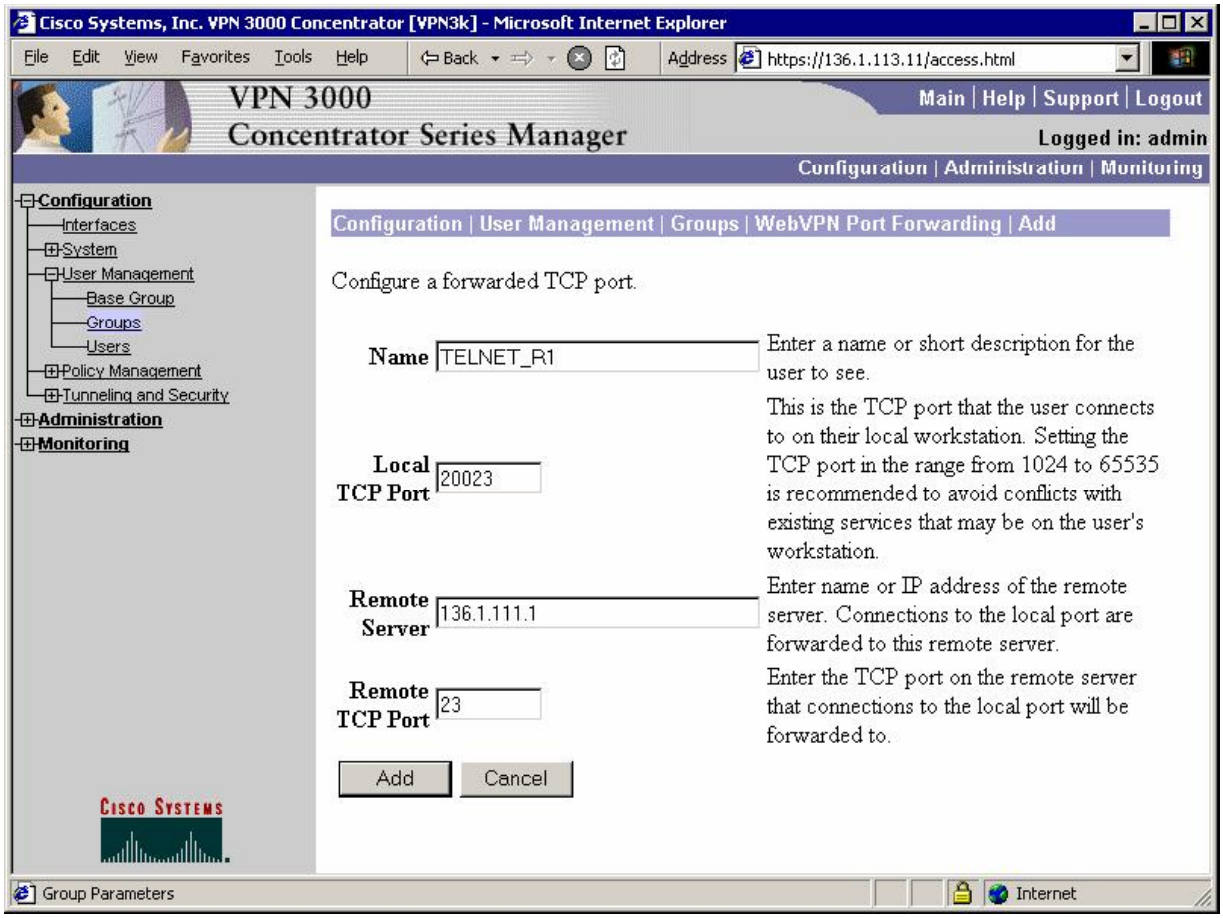
- Configure devices as per the scenario "VPN/WebVPN and SSL VPN" "VPN3k and WebVPN Client".
- We would like to tunnel local connection to port 20023 to remote router R1 port 23.
- Configure group WEBVPN
  - Set up port-forwarding:
    - Use name TELNET_R1.
    - Specify local port 20023
    - Specify remote server 136.1.111.1
    - Specify remote port 23
  - Enable port-forwarding under group's WebVPN attributes.
  - Modify WebACL to permit any type of access to host 136.1.111.1

Final Configuration

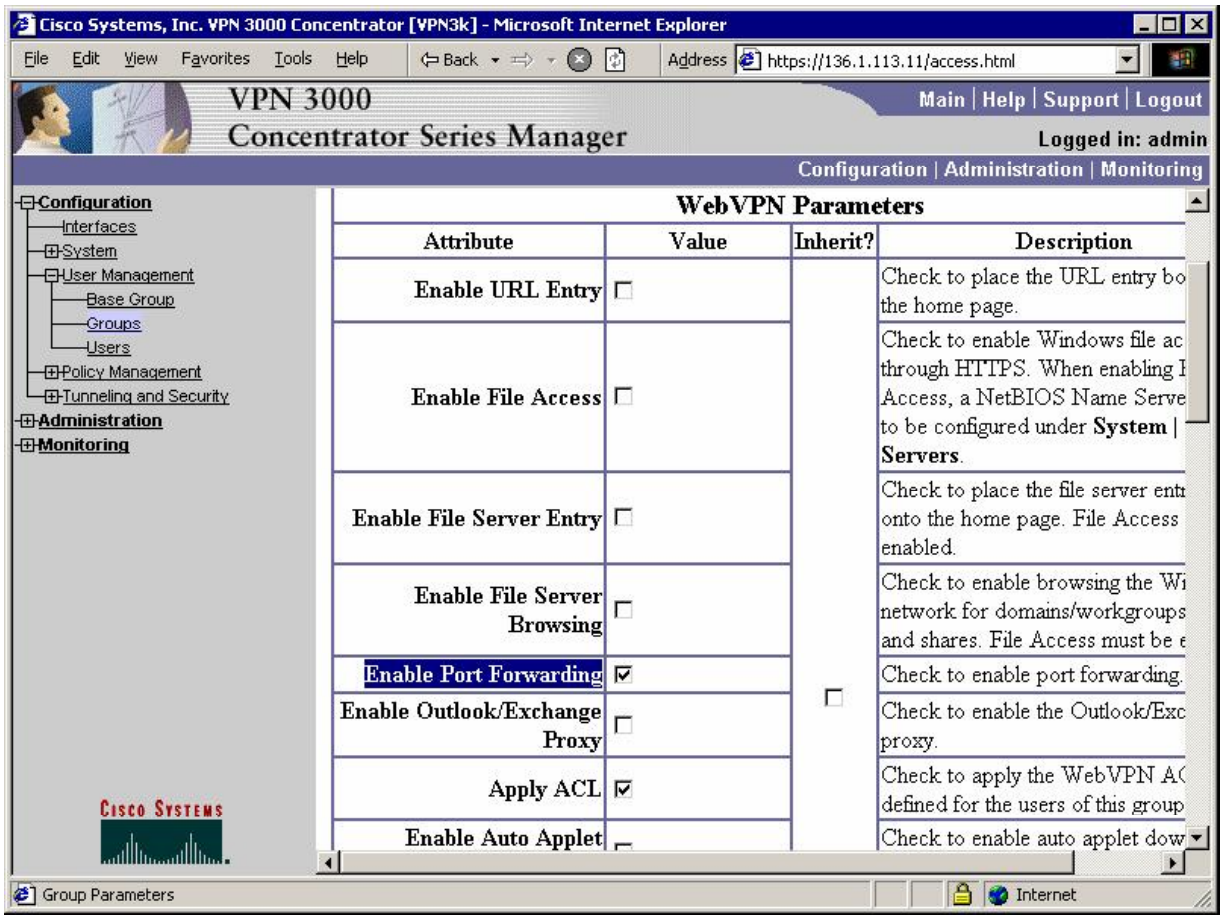
VPN3k GUI:

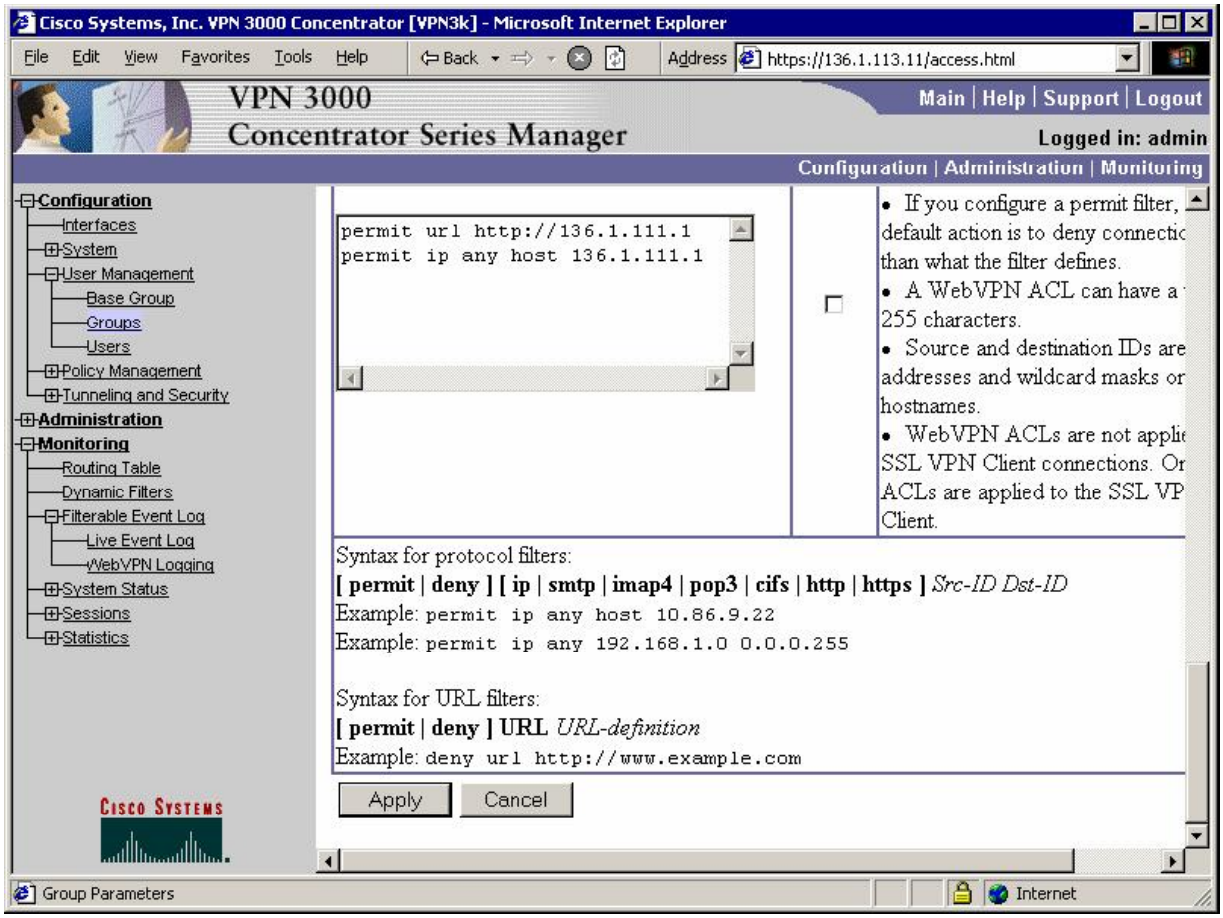
Configure port-forwarding settings for group "WEBVPN":




Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Tunneling and Security
Administration
Monitoring
Configuration | User Management | Groups | WebVPN Port Forwarding | Add
Configure a forwarded TCP port.
Name
TELNET_R1
Enter a name or short description for the user to see.
Local TCP Port
20023
This is the TCP port that the user connects to on their local workstation. Setting the TCP port in the range from 1024 to 65535 is recommended to avoid conflicts with existing services that may be on the user's workstation.
Remote Server
136.1.111.1
Enter name or IP address of the remote server. Connections to the local port are forwarded to this remote server.
Remote TCP Port
23
Enter the TCP port on the remote server that connections to the local port will be forwarded to.
Add
Cancel
Cisco Systems
Group Parameters
Internet

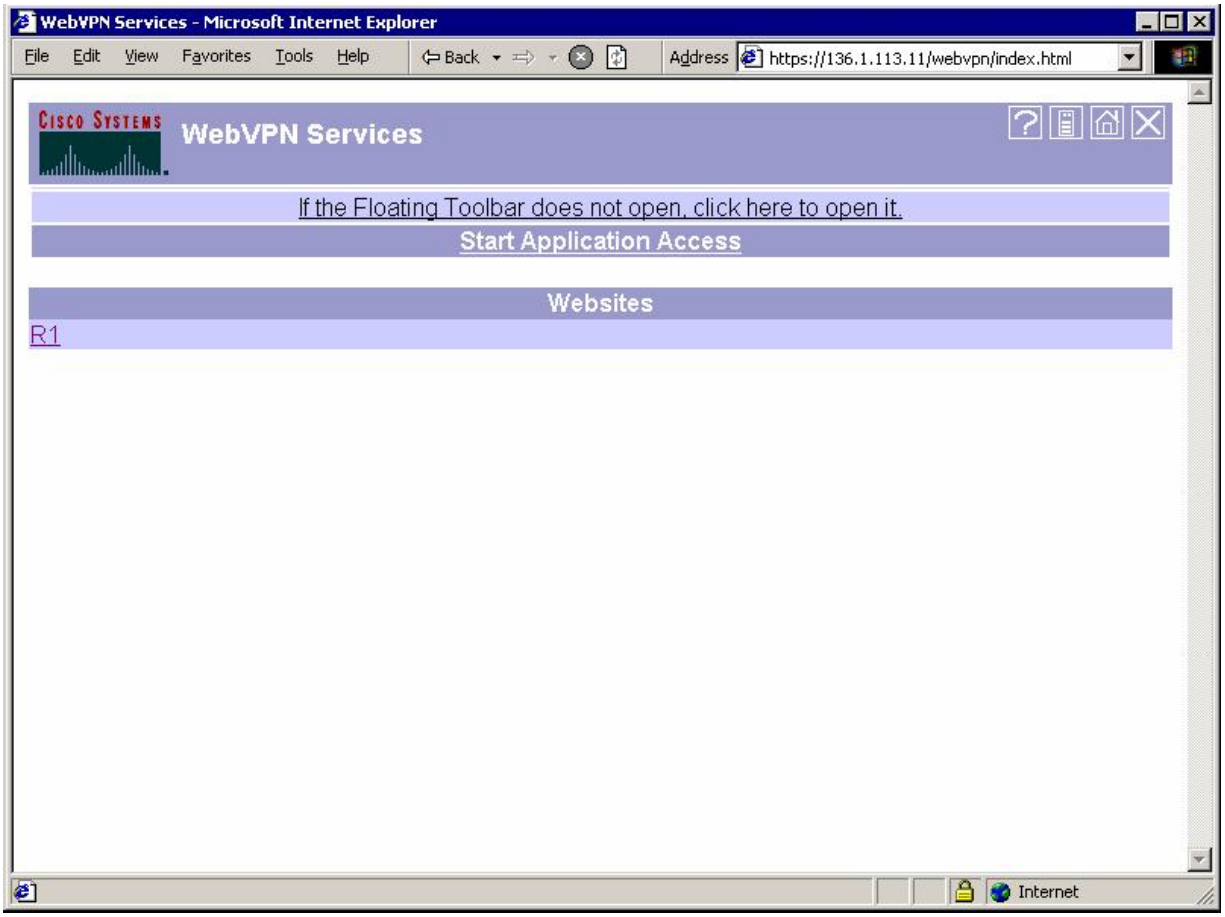
Enable port forwarding under WebVPN tab and permit it with WebACL:

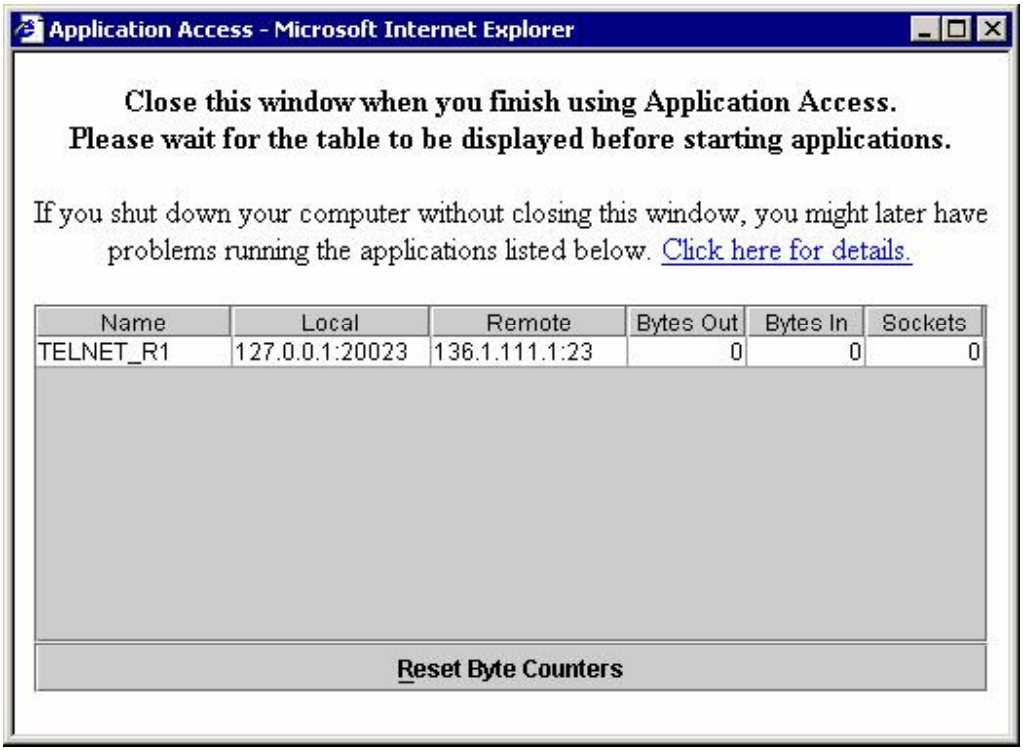



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Tunneling and Security
Administration
Monitoring
Routing Table
Dynamic Filters
Filterable Event Log
Live Event Log
WebVPN Logging
System Status
Sessions
Statistics
permit url http://136.1.111.1
permit ip any host 136.1.111.1
• If you configure a permit filter,
default action is to deny connectic
than what the filter defines.
• A WebVPN ACL can have a
255 characters.
• Source and destination IDs are
addresses and wildcard masks or
hostnames.
• WebVPN ACLs are not applie
SSL VPN Client connections. Or
ACLs are applied to the SSL VP
Client.
Syntax for protocol filters:
[permit | deny] [ip | smtp | imap4 | pop3 | cifs | http | https] Src-ID Dst-ID
Example: permit ip any host 10.86.9.22
Example: permit ip any 192.168.1.0 0.0.0.255
Syntax for URL filters:
[permit | deny] URL URL-definition
Example: deny url http://www.example.com
Apply
Cancel
Cisco Systems
Group Parameters
Internet

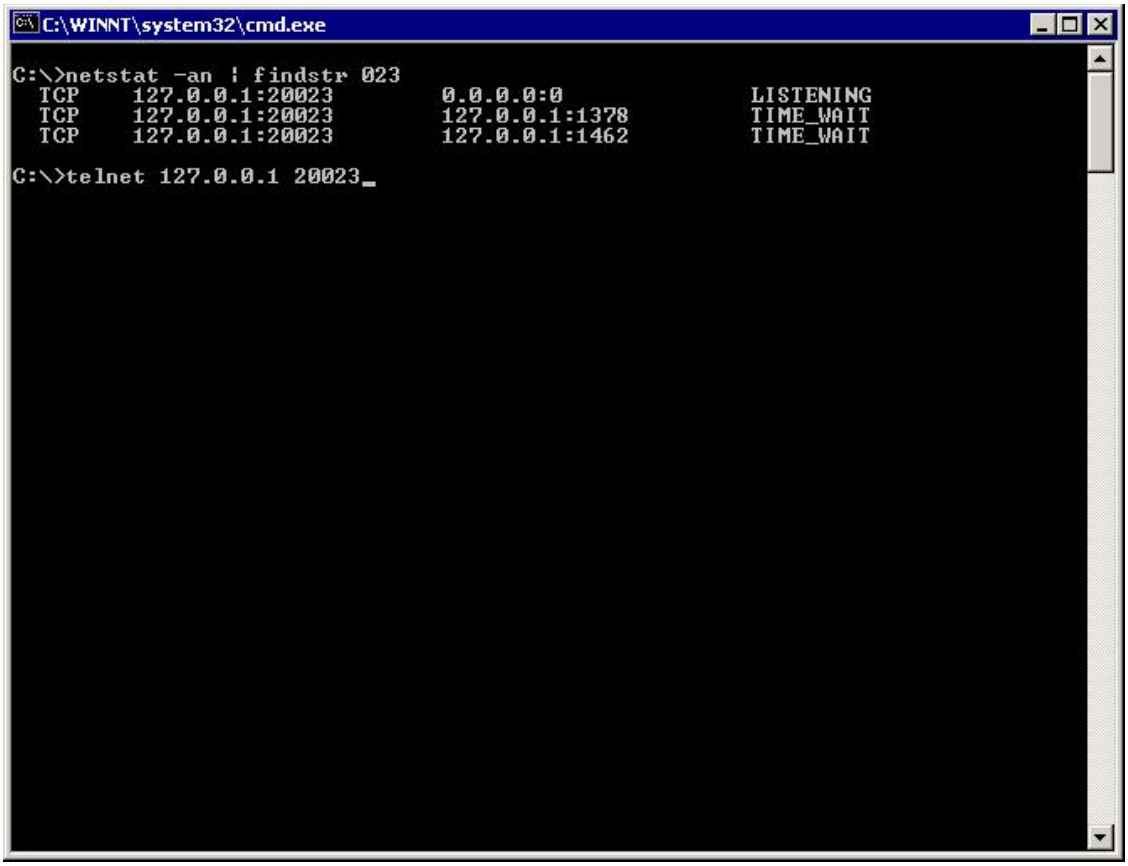
Verification

Connect to VPN3k & start application access:




Application Access - Microsoft Internet Explorer
Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.
If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details.
Name
Local
Remote
Bytes Out
Bytes In
Sockets
TELNET_R1
127.0.0.1:20023
136.1.111.1:23
0
0
0
Reset Byte Counters

Verify local port 20023:



```
C:\WINNT\system32\cmd.exe - telnet 127.0.0.1 20023

R1>show  ver
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.2(15)T17, RELEASE SOFTWARE
 (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Fri 12-Aug-05 15:49 by kehsiao
Image text-base: 0x80008098, data-base: 0x81942FEC

ROM: System Bootstrap, Version 11.3(2)XA3, PLATFORM SPECIFIC RELEASE SOFTWARE (f
c1)
ROM: C2600 Software (C2600-IK9O3S3-M), Version 12.2(15)T17, RELEASE SOFTWARE (fc
1)

R1 uptime is 2 hours, 40 minutes
System returned to ROM by reload
System image file is "flash:c2600-ik9o3s3-mz.122-15.T17.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 2610 (MPC860) processor (revision 0x202) with 59392K/6144K bytes of memory
.
Processor board ID JAB03040BW9 (1247782719)
M860 processor: part number 0, mask 49
Bridging software.
```

Check session statistics on VPN3k:

Application Access - Microsoft Internet Explorer

Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details.

Name	Local	Remote	Bytes Out	Bytes In	Sockets
TELNET_R1	127.0.0.1:20023	136.1.111.1:23	85	1718	1

Reset Byte Counters

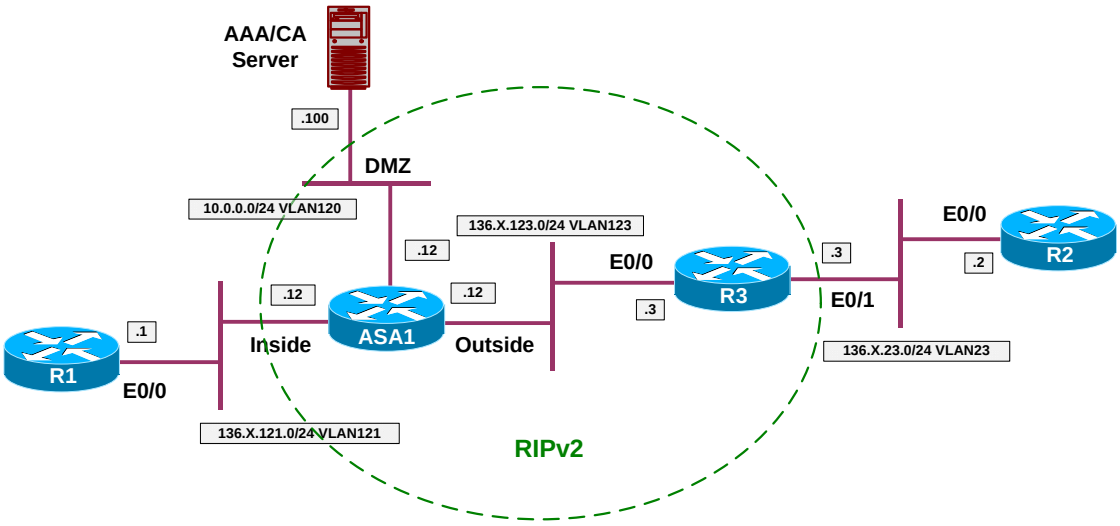
🕮 Further Reading

Configuring the VPN Concentrator for WebVPN

VPN QoS

IOS and the PIX/ASA: Policing the L2L IPsec tunnel

Objective: Configure policing for L2L IPsec tunnel on the ASA firewall.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and the PIX/ASA with PSK".
- Create class-map L2L_TO_R3_DATA and match tunnel group "136.1.123.3". Match flow based on destination IP.
- Create class-map L2L_TO_R3_VOICE and match tunnel group "136.1.123.3". Match DSCP EF.
- Create policy-map OUTSIDE:
  - Match class L2L_TO_R3_DATA. Police up to 128Kbps with default burst.
  - Match class L2L_TO_R3_VOICE. Provide LLQ service for this class.
  - For class-default police to 2000000 bps
- Apply policy-map OUTSIDE to outside interface.

Final Configuration

```
ASA1:
class-map L2L_TO_R3_DATA
  match tunnel-group 136.1.123.3
  match flow ip destination
!
class-map L2L_TO_R3_VOICE
  match tunnel-group 136.1.123.3
  match dscp ef
```

```
!
policy-map OUTSIDE
  class L2L_TO_R3_DATA
    police out 128000
  class L2L_TO_R3_VOICE
    priority
  class class-default
    police out 2000000
!
service-policy OUTSIDE interface outside
```

Verification

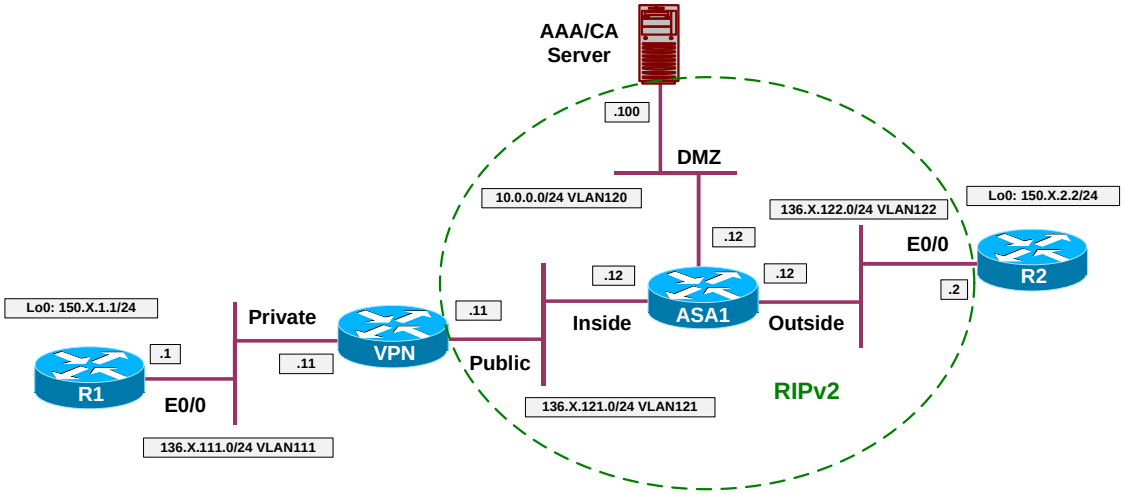
```
R1#ping 136.1.23.2 repeat 1000 size 1000

Type escape sequence to abort.
Sending 1000, 1000-byte ICMP Echos to 136.1.23.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!
!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!
!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!
!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!
!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!
!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!.!!!!!!!
Success rate is 96 percent (967/1000), round-trip min/avg/max = 28/34/621 ms

ASA1(config)# show service-policy interface outside

Interface outside:
  Service-policy: OUTSIDE
    Class-map: L2L_TO_R3_VOICE
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 0
    Class-map: L2L_TO_R3_DATA
      Output police Interface outside:
        cir 128000 bps, bc 4000 bytes
        conformed 967 packets, 1034690 bytes; actions:  transmit
        exceeded 33 packets, 35310 bytes; actions:  drop
        conformed 0 bps, exceed 0 bps
    Class-map: class-default
      Output police Interface outside:
        cir 2000000 bps, bc 62500 bytes
        conformed 367 packets, 59649 bytes; actions:  transmit
        exceeded 0 packets, 0 bytes; actions:  drop
        conformed 0 bps, exceed 0 bps
```

Further Reading

Applying QoS Policies

IOS and VPN3k: QoS for L2L Tunnel

Objective: Configure VPN3k to provide minimum bandwidth and maximum allowed rate for a tunnel.



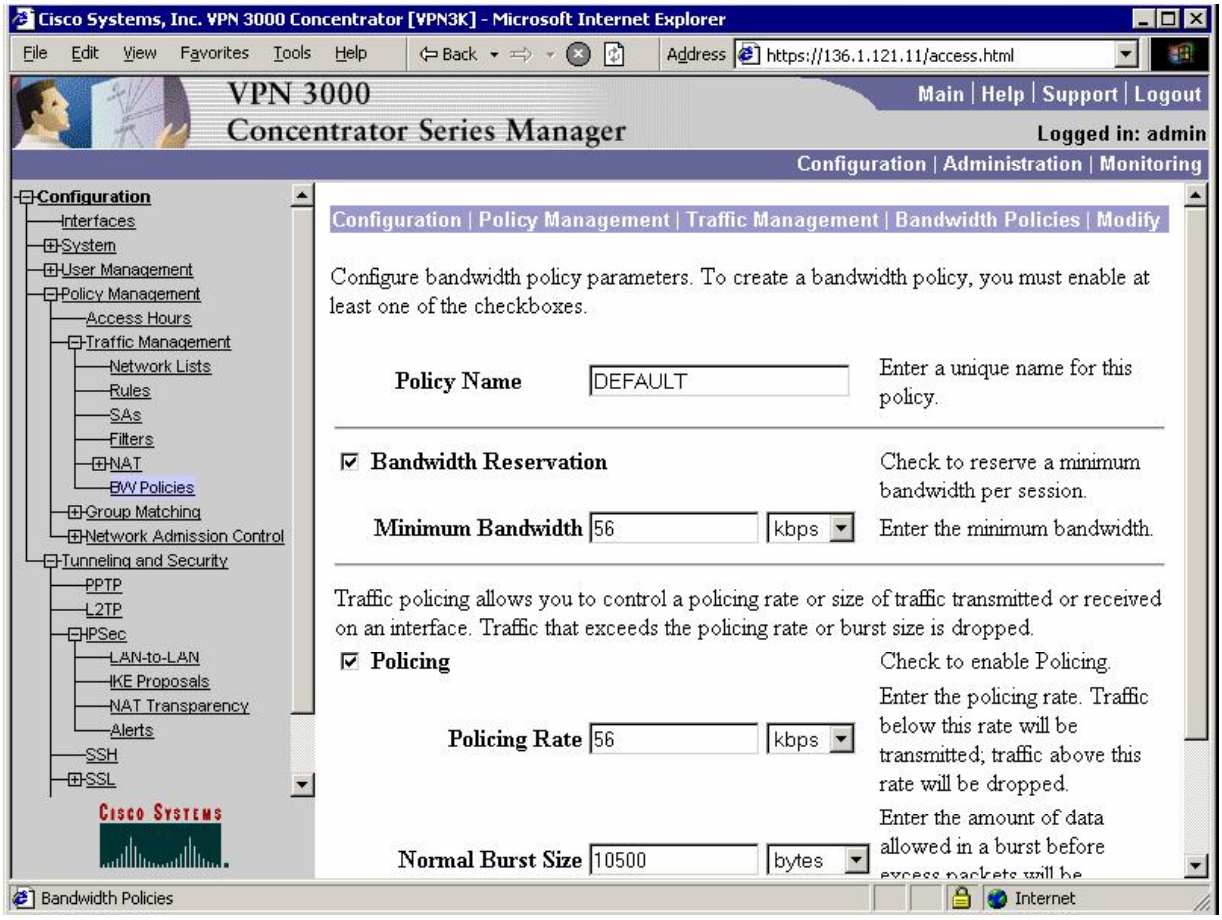
Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and VPN3k with PSK".
- Create Bandwidth Policy named DEFAULT:
  - Reserve 56Kbps
  - Policy to 56Kbps
- Create Bandwidth Policy named "VPN_TO_R2":
  - Use bandwidth of 128Kbps
  - Police up to 256Kbps
- Consider the minimum bandwidth along the path to VPN3k to be 2Mbps. Configure Public interface bandwidth accordingly.
- Assign "DEFAULT" policy as default Public interface bandwidth policy.
- Configure L2L Tunnel "VPN_TO_R2" to use bandwidth policy "VPN_TO_R2".

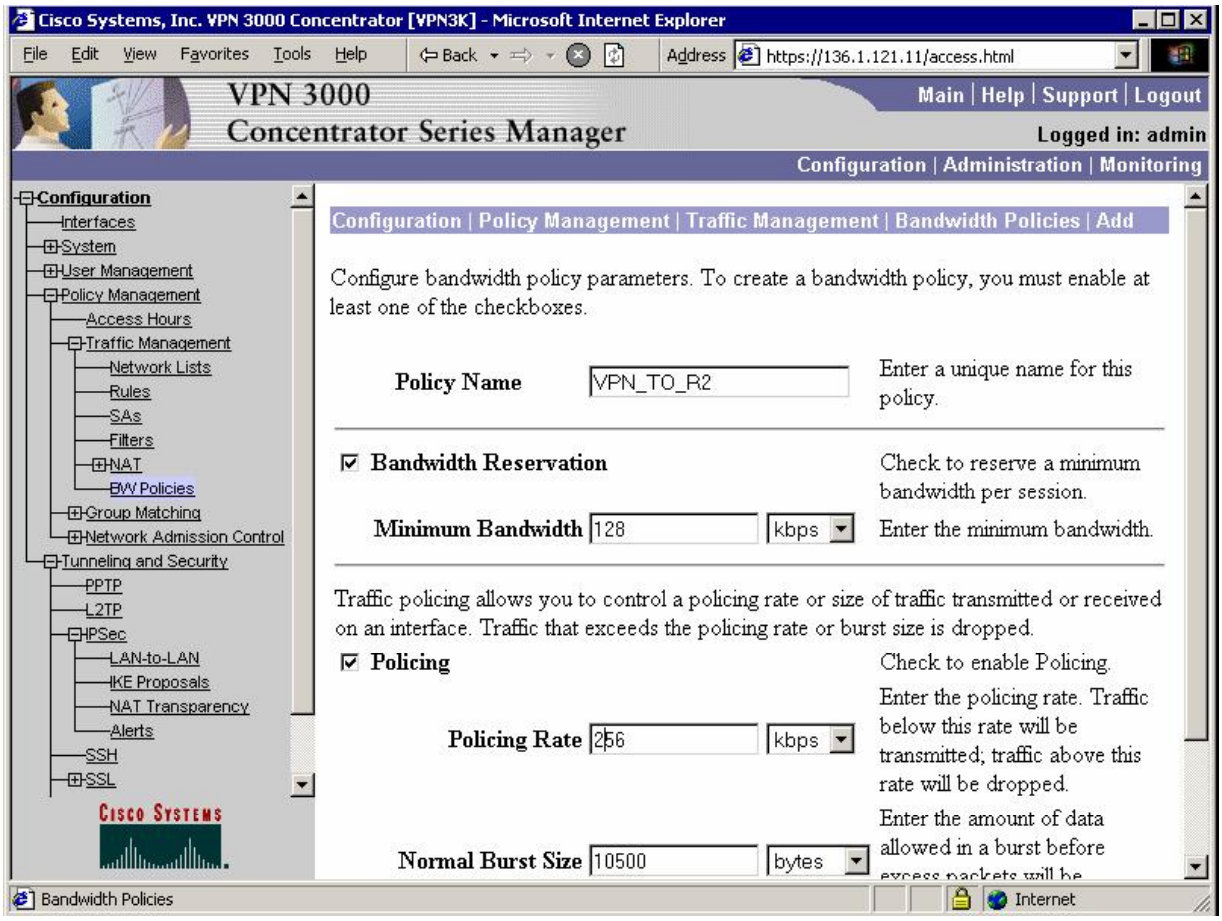
Final Configuration

VPN3k:

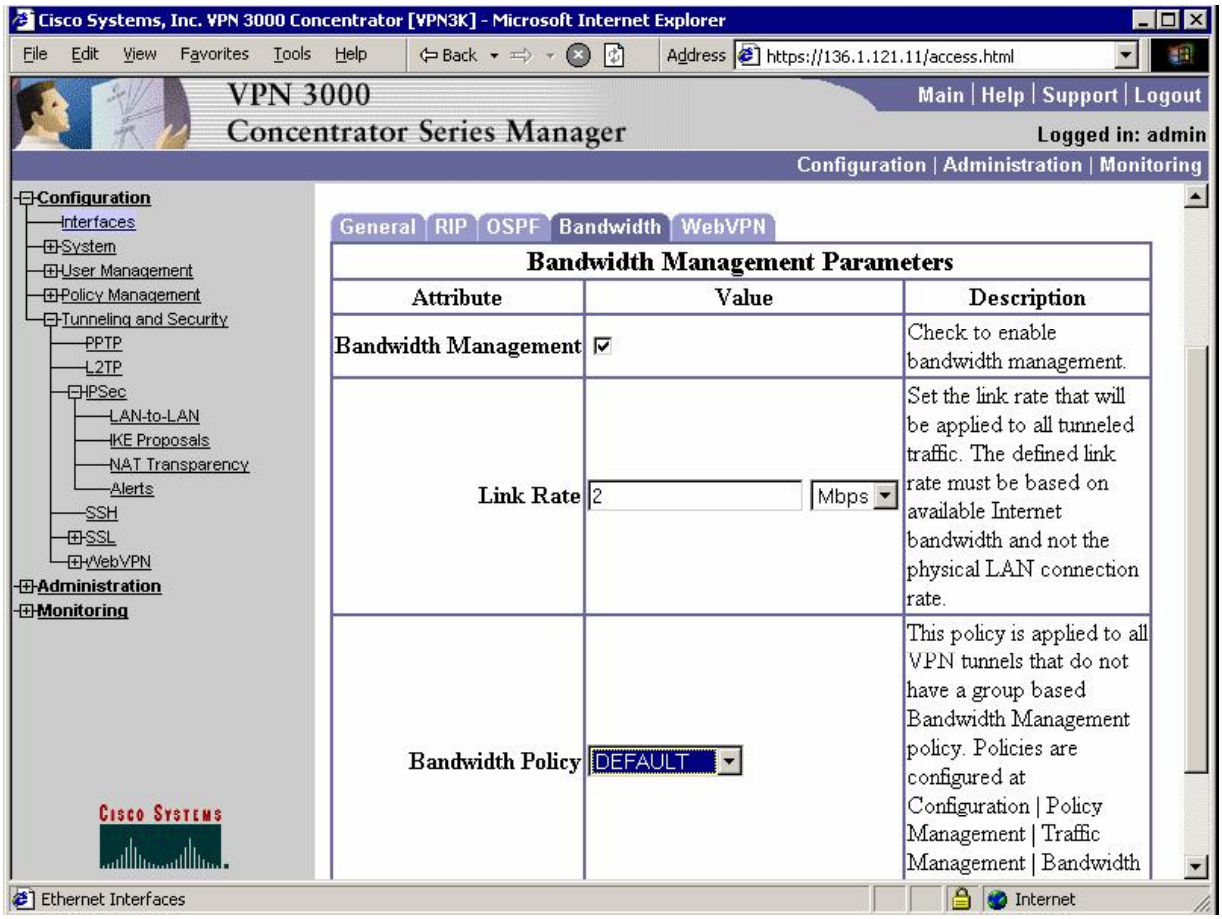
Create default bandwidth policy:



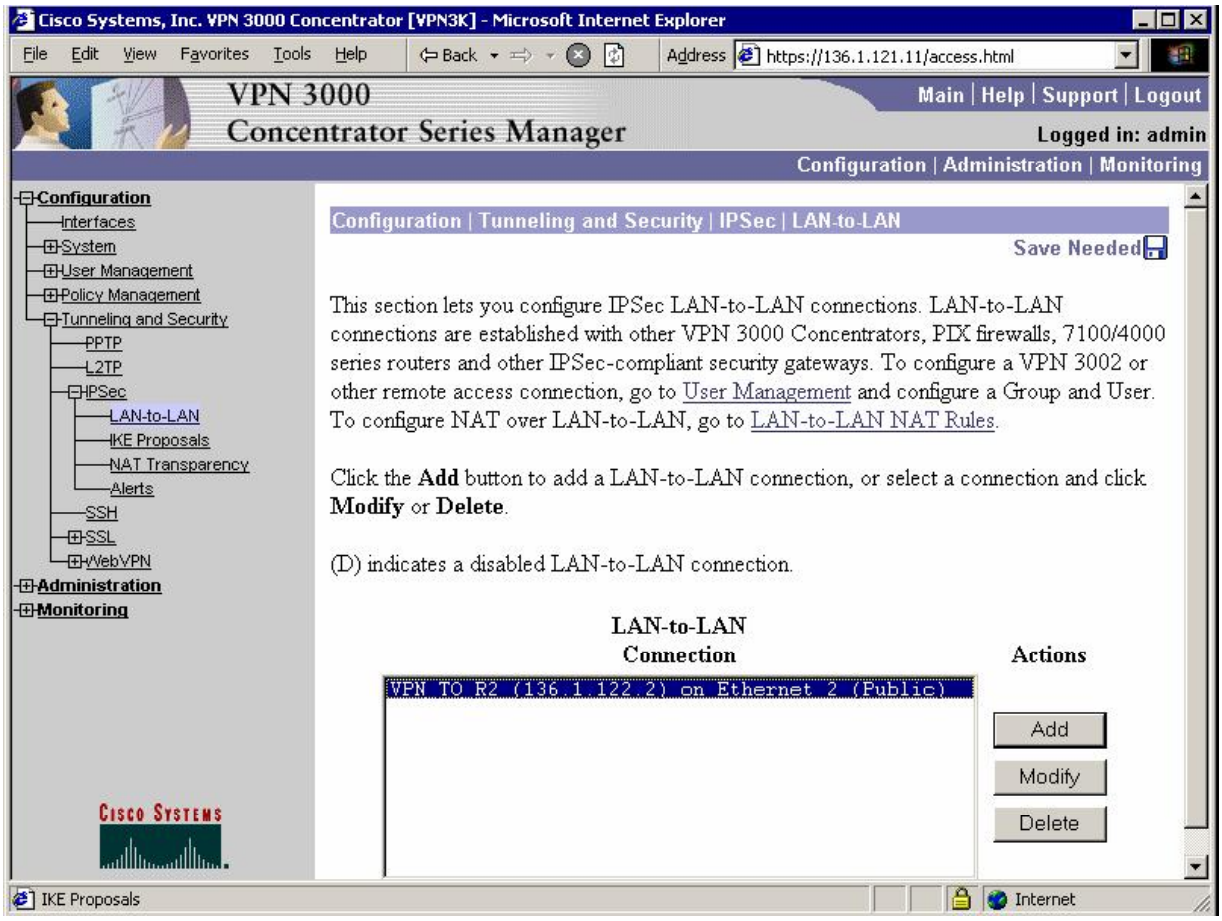
Create bandwidth policy for L2L tunnel:

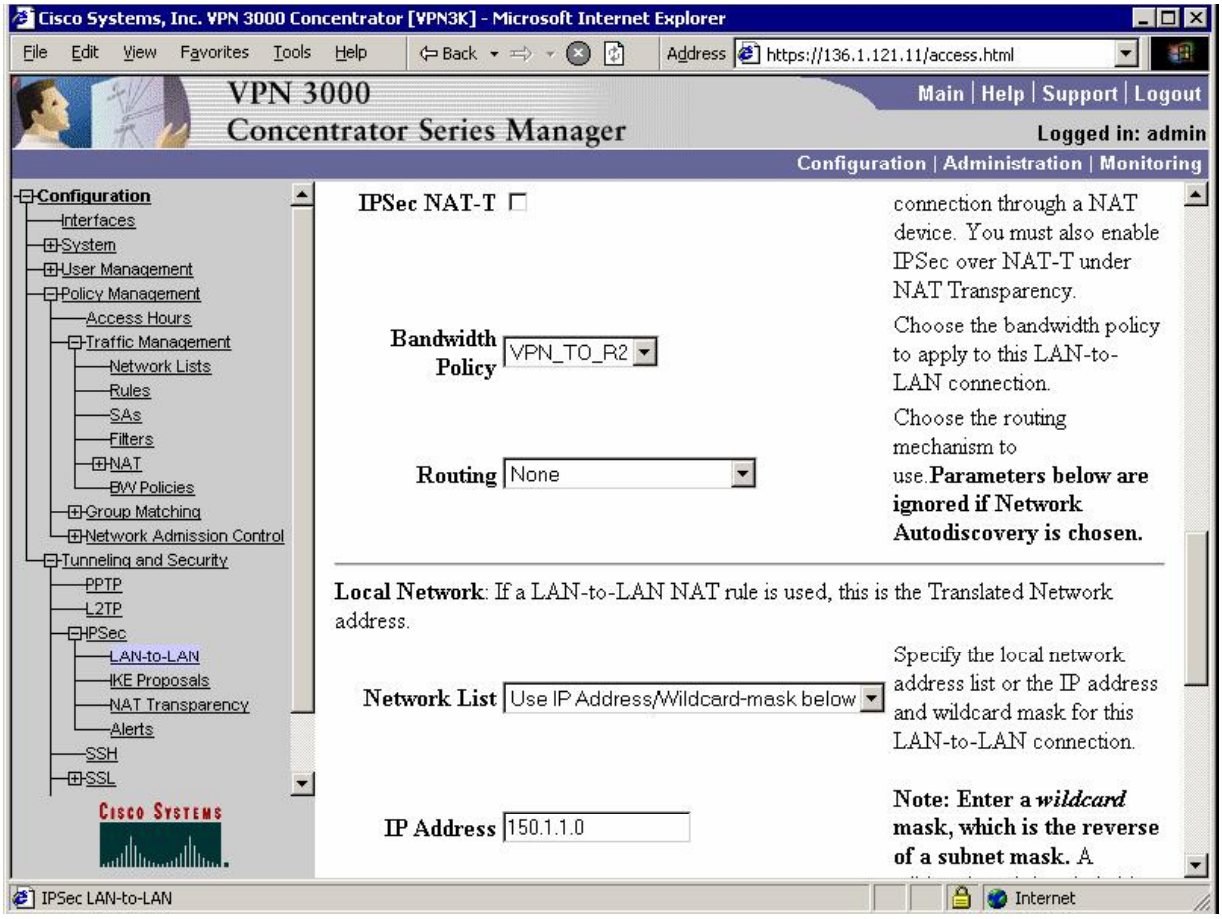


Configure Public interface:



Apply bandwidth policy to L2L Tunnel:



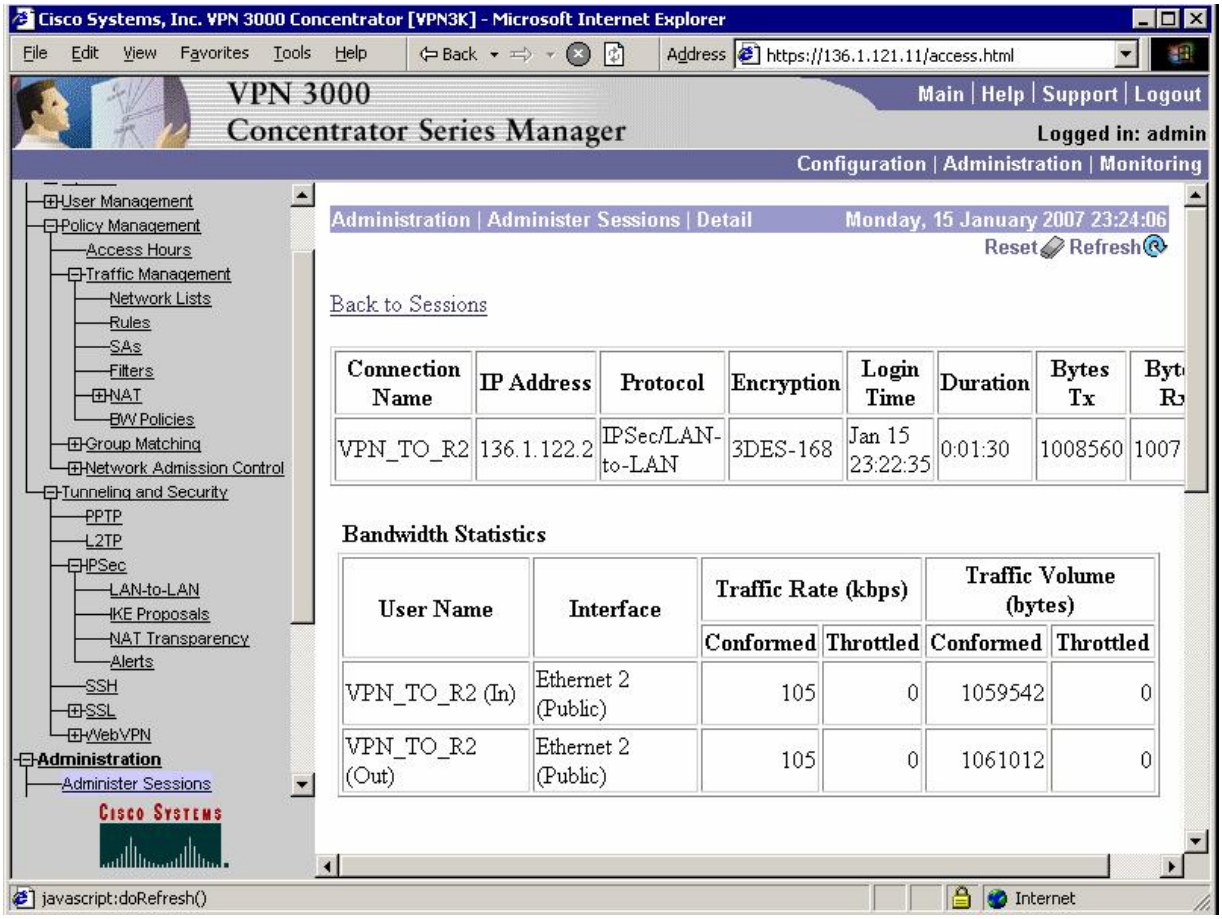


Verification

```
R1#ping 150.1.2.2 source loopback 0 repeat 1000 size 1400 timeout 1

Type escape sequence to abort.
Sending 1000, 1400-byte ICMP Echos to 150.1.2.2, timeout is 1 seconds:
Packet sent with a source address of 150.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<snip>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 44/111/180 ms
```

VPN3k:

Administration > Administer Session > Detail

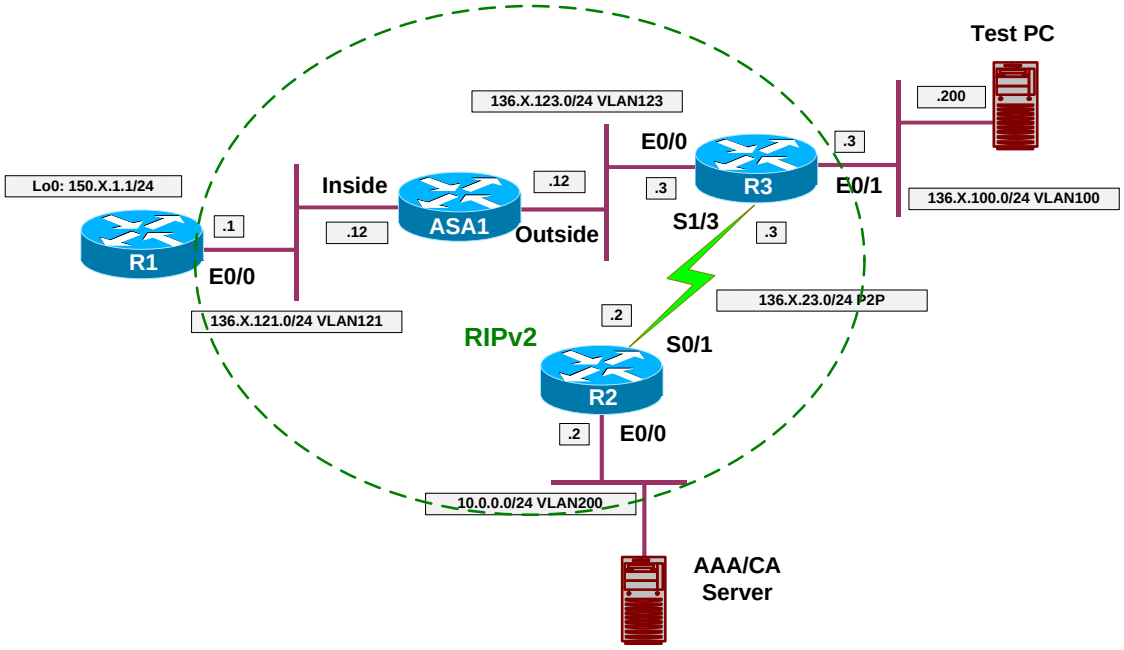


Further Reading

VPN3k: Policy Management

PIX/ASA and Cisco VPN Client: Per-Flow Policing

Objective: Configure the firewall to limit maximum permitted per-flow rate for remote-access VPN group users.



Directions

- Configure devices as per the scenario "VPN/ezVPN" "The PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI".
- Create class-map VPN_DATA and match tunnel group "EZVPN". Match flow based on destination IP.
- Create class-map L2L_TO_R3_VOICE and match tunnel group "EZVPN". Match DSCP EF.
- Create policy-map OUTSIDE:
  - Match class VPN_DATA. Police up to 256Kbps with default burst.
  - Match class VPN_VOICE. Provide LLQ service for this class.
  - For class-default police to 2000000 bps
- Apply policy-map OUTSIDE to outside interface.

Final Configuration

```
ASA1:
!
! Tunneled voice traffic, marked by DSCP EF
!
class-map VPN_VOICE
 match dscp ef
 match tunnel-group EZVPN
!
```

```
! Tunneled data flows
!
class-map VPN_DATA
 match flow ip destination-address
 match tunnel-group EZVPN
!
! Outside interface policy
!
policy-map OUTSIDE
 class VPN_VOICE
  priority
 class VPN_DATA
  police output 256000
 class class-default
  police output 2000000
!
service-policy OUTSIDE interface outside
```

Verification

Connect Cisco VPN Client to the ASA:

```
ASA1(config)# show vpn-sessiondb remote

Session Type: Remote

Username     : CISCO
Index        : 1
Assigned IP  : 20.0.0.1               Public IP    : 136.1.100.200
Protocol     : IPSec                  Encryption   : 3DES
Hashing      : MD5
Bytes Tx     : 978500                 Bytes Rx     : 978500
Client Type  : WinNT                  Client Ver   : 4.8.01.0300
Group Policy : EZVPN
Tunnel Group : EZVPN
Login Time   : 07:10:40 UTC Mon Jan 22 2007
Duration     : 0h:09m:50s
Filter Name  :
NAC Result   : N/A
Posture Token:

R1#ping 20.0.0.1 repeat 1000 size 1000

Type escape sequence to abort.
Sending 1000, 1000-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!.!!
```

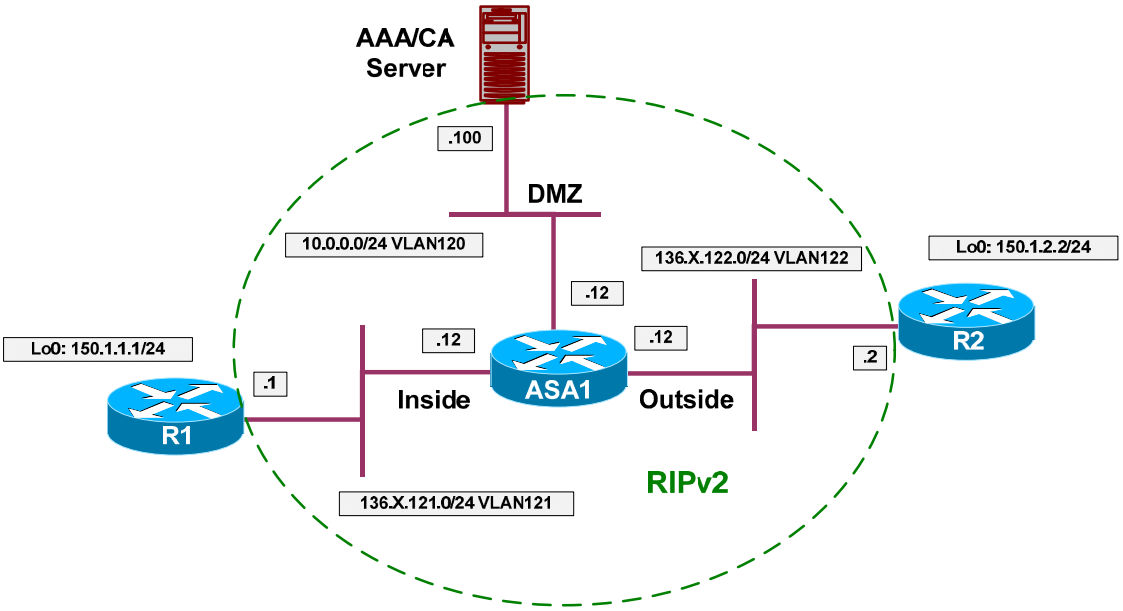
```
Success rate is 97 percent (978/1000), round-trip min/avg/max = 8/9/24 ms
R1#

ASA1(config)# show ipsec sa
interface: outside
    Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
      current_peer: 136.1.100.200, username: CISCO
      dynamic allocated peer ip: 20.0.0.1

      #pkts encaps: 983, #pkts encrypt: 983, #pkts digest: 983
      #pkts decaps: 983, #pkts decrypt: 983, #pkts verify: 983
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 983, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 136.1.123.12, remote crypto endpt.: 136.1.100.200

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 457752CA

    inbound esp sas:
      spi: 0x3A8E8CC1 (982420673)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28691
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x457752CA (1165447882)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 2, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28691
         IV size: 8 bytes
         replay detection support: Y

ASA1(config)# show service-policy interface outside

Interface outside:
  Service-policy: OUTSIDE
    Class-map: VPN_VOICE
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 0
    Class-map: VPN_DATA
      Output police Interface outside:
        cir 256000 bps, bc 8000 bytes
        conformed 983 packets, 1041412 bytes; actions:  transmit
        exceeded 22 packets, 23408 bytes; actions:  drop
        conformed 14408 bps, exceed 320 bps
    Class-map: class-default
      Output police Interface outside:
        cir 2000000 bps, bc 62500 bytes
        conformed 983 packets, 1047290 bytes; actions:  transmit
        exceeded 0 packets, 0 bytes; actions:  drop
        conformed 14488 bps, exceed 0 bps
```

🕮 Further Reading

Applying QoS Policies

QoS Pre-Classify for IPsec Tunnel

Objective: Configure IOS router for QoS pre-classify feature with IPsec tunnel.



Directions

- Configure devices as per the "VPN/IPsec LAN-to-LAN" scenario "IOS and IOS with PSK Across the PIX/ASA".
- QoS pre-classify feature permits classification on an interface to occur before the actual data encryption. In turn, this feature is useful to apply QoS policies to tunnel-encapsualted traffic.
- Configure class-map VPN_VOICE:
  - Match traffic with DSCP value EF.
  - Match access-list LO1_TO_LO2.
- Configure class-map VPN_DATA:
  - Match access-list LO1_TO_LO2.
  - Match traffic with DSCP value any besides EF.
- Configure policy-map VPN_QOS:
  - For class VPN_VOICE provide prioriy queue with 64Kbps
  - For class VPN_DATA police traffic up to 256Kbps
- Create policy-map INTERFACE_QOS:
  - Shape class-default up to 384Kbps
  - Apply policy-map VPN_QOS inside class-default.
- Configure crypto-map VPN:
  - Enable QoS pre-classify.

Final Configuration

```
R1:
!
! VPN voice traffic
!
class-map VPN_VOICE
  match access-group  name LO1_TO_LO2
  match dscp ef
!
! VPN regular data
!
class-map VPN_DATA
 match access-group name LO1_TO_LO2
 match not dscp ef
!
! Configure VPN QoS Policy
!
policy-map VPN_QOS
  class VPN_VOICE
    priority 64
  class VPN_DATA
    police 256000
!
policy-map INTERFACE_QOS
  class class-default
    shape average 384000
    service-policy VPN_QOS
!
! Apply service policy to an interface
!
interface E0/0
  service-policy output INTERFACE_QOS
!
! Enable QoS pre-classify under crypto map
!
crypto map VPN 10
  qos pre-classify
```

Verification

```
R1#ping 150.1.2.2 source loopback 0 size 1000 repeat 200 timeout 1

Type escape sequence to abort.
Sending 200, 1000-byte ICMP Echos to 150.1.2.2, timeout is 1 seconds:
Packet sent with a source address of 150.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (200/200), round-trip min/avg/max = 40/42/52 ms

R1#show policy-map interface ethernet 0/0
 Ethernet0/0

  Service-policy output: INTERFACE_QOS

    Class-map: class-default (match-any)
      203 packets, 214186 bytes
```

```
      5 minute offered rate 8000 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
           384000/384000    2400   9600      9600      25        1200

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         203       214186    0         0         no

      Service-policy : VPN_QOS

        Class-map: VPN_DATA (match-all)
          200 packets, 214000 bytes
          5 minute offered rate 8000 bps, drop rate 0 bps
          Match: access-group name LO1_TO_LO2
          Match: not  dscp ef
          police:
              cir 256000 bps, bc 8000 bytes
            conformed 200 packets, 214000 bytes; actions:
              transmit
            exceeded 0 packets, 0 bytes; actions:
              drop
            conformed 8000 bps, exceed 0 bps

        Class-map: VPN_VOICE (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match:  dscp ef
          Match: access-group name LO1_TO_LO2
          Queueing
            Strict Priority
            Output Queue: Conversation 40
            Bandwidth 64 (kbps) Burst 1600 (Bytes)
            (pkts matched/bytes matched) 0/0
            (total drops/bytes drops) 0/0

        Class-map: class-default (match-any)
          3 packets, 186 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any
```

Send traffic with DSCP EF value; note that EF corresponds to DSCP value 46 and ToS byte 46*4=184:

```
R1#ping
Protocol [ip]:
Target IP address: 150.1.2.2
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]: 1
Extended commands [n]: y
Source address or interface: 150.1.1.1
Type of service [0]: 184
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 150.1.2.2, timeout is 1 seconds:
Packet sent with a source address of 150.1.1.1
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 8/11/13 ms

R1#show policy-map interface ethernet 0/0
 Ethernet0/0

  Service-policy output: INTERFACE_QOS

    Class-map: class-default (match-any)
      825 packets, 301562 bytes
      5 minute offered rate 2000 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
           384000/384000    2400   9600      9600      25        1200

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         825       301562    0         0         no

      Service-policy : VPN_QOS

        Class-map: VPN_DATA (match-all)
          500 packets, 263800 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: access-group name LO1_TO_LO2
          Match: not  dscp ef
          police:
              cir 256000 bps, bc 8000 bytes
            conformed 500 packets, 263800 bytes; actions:
              transmit
            exceeded 0 packets, 0 bytes; actions:
              drop
            conformed 0 bps, exceed 0 bps

        Class-map: VPN_VOICE (match-all)
          100 packets, 16600 bytes
          5 minute offered rate 2000 bps, drop rate 0 bps
          Match:  dscp ef
          Match: access-group name LO1_TO_LO2
          Queueing
            Strict Priority
            Output Queue: Conversation 40
            Bandwidth 64 (kbps) Burst 1600 (Bytes)
            (pkts matched/bytes matched) 0/0
            (total drops/bytes drops) 0/0

        Class-map: class-default (match-any)
          225 packets, 21162 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any
```

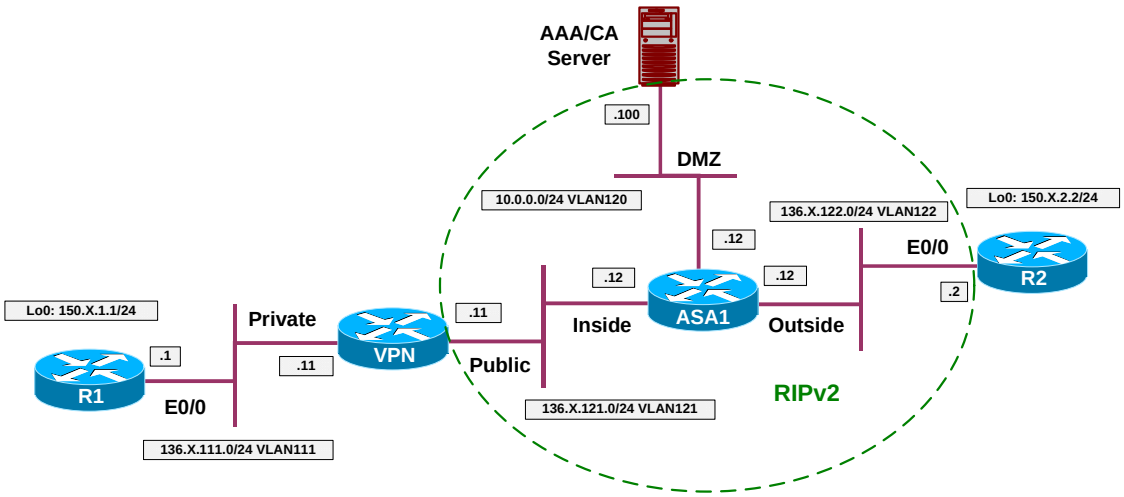
Further Reading

Reference Guide to Implementing Crypto and QoS
Quality of Service Options on GRE Tunnel Interfaces

Advanced VPN Topics

Decoding IPsec Debugging Output on VPN3k

Objective: Configure VPN3k debugging for IPsec/IKE events.



Directions

- Configure devices as per the scenario " VPN/IPsec LAN-to-LAN" "IOS and VPN3k with PSK using CLI".
- Activate logging for the following systems Events:
  - IKE, IKEDBG, IKEDECODE.
  - IPSEC, IPSECDBG, IPSEDECODE.
  - Log events with severity up to 9.
- Configure Monitor Log to display up to 100 events per page.
- Filter only events for group 136.1.122.2

Final Configuration

ASA1 :

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 1

1) Interface Configuration
2) System Management
3) User Management
```

```
4) Policy Management
5) Tunneling and Security
6) Back

VPN3K: Config -> 2

1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back

VPN3K: System -> 5

1) General
2) FTP Backup
3) Classes
4) Trap Destinations
5) Syslog Servers
6) SMTP Servers
7) E-mail Recipients
8) Back

VPN3K: Event -> 3

                           The Active Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP                          |                                      |
-------------------------------------------------------------------------------

1) Add an Event Class
2) Modify an Event Class
3) Delete an Event Class
4) Back

VPN3K: Event Class -> 1

                              The Event Classes
-----------------------------------------------------------------------------
| 1. MIB2TRAP      | 2. PSOS          | 3. SYSTEM        | 4. QUEUE         |
| 5. EVENT         | 6. EVENTDBG      | 7. SMTP          | 8. RM            |
| 9. DM            | 10. IP           | 11. TCP          | 12. PPP          |
| 13. L2TP         | 14. HTTP         | 15. AUTH         | 16. AUTHDBG      |
| 17. AUTHDECODE   | 18. PPTP         | 19. PPTPDBG      | 20. PPTPDECODE   |
| 21. GRE          | 22. GREDBG       | 23. GREDECODE    | 24. PSH          |
| 25. CONFIG       | 26. L2TPDBG      | 27. L2TPDECODE   | 28. TELNET       |
| 29. TELNETDBG    | 30. TELNETDECODE | 31. FTPD         | 32. DNS          |
| 33. DNSDBG       | 34. IPSEC        | 35. IPSECDBG     | 36. IPSECDECODE  |
| 37. IKE          | 38. IKEDBG       | 39. IKEDECODE    | 40. HARDWAREMON  |
| 41. IPDBG        | 42. CAPI         | 43. IPDECODE     | 44. PPPDBG       |
| 45. PPPDECODE    | 46. DNSDECODE    | 47. DHCP         | 48. DHCPDBG      |
| 49. DHCPDECODE   | 50. FILTER       | 51. FILTERDBG    | 52. EVENTMIB     |
| 53. REBOOT       | 54. SNMP         | 55. OSPF         | 56. VRRP         |
| 57. SSL          | 58. CERT         | 59. GENERAL      | 60. TIME         |
| 64. EXPANSIONCARD| 67. FSM          | 68. SSH          | 69. LBSSF        |
| 71. PPPOE        | 72. PPPOEDBG     | 73. PPPOEDECODE  | 74. NETBIOS      |
| 75. CLIENT       | 76. XML          | 77. FW           | 78. FWDBG        |
| 79. FWDECODE     | 82. BMGT         | 83. BMGTDBG      | 84. FIPS         |
| 85. FIPSDIAG     | 86. WEBVPN       | 87. EMAILPROXY   | 88. CIFS         |
```

```
| 89. CIFSDBG      | 90. STC          | 91. CSTP         | 92. NAC          |
'q' to Quit, '<SPACE>' to Continue ->
| 93. EAP          | 94. EAPOUDP      |                  |                  |
-------------------------------------------------------------------------------

> Enter the Event Class to Add

VPN3K: Event Class -> 34

1) Enable this Class
2) Disable this Class

VPN3K: Event Class -> [ 1 ]

> Events to Log

VPN3K: Event Class -> [ 5 ] 9

> Events to Console

VPN3K: Event Class -> [ 3 ]

> Events to Syslog

VPN3K: Event Class -> [ 0 ]

> Events to E-mail

VPN3K: Event Class -> [ 0 ]

> Events to SNMP Trap

VPN3K: Event Class -> [ 0 ]

                           The Active Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP                           | 34. IPSEC                            |
-------------------------------------------------------------------------------

1) Add an Event Class
2) Modify an Event Class
3) Delete an Event Class
4) Back

VPN3K: Event Class -> 1

                              The Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP      | 2. PSOS          | 3. SYSTEM        | 4. QUEUE         |
| 5. EVENT         | 6. EVENTDBG      | 7. SMTP          | 8. RM            |
| 9. DM            | 10. IP           | 11. TCP          | 12. PPP          |
| 13. L2TP         | 14. HTTP         | 15. AUTH         | 16. AUTHDBG      |
| 17. AUTHDECODE   | 18. PPTP         | 19. PPTPDBG      | 20. PPTPDECODE   |
| 21. GRE          | 22. GREDBG       | 23. GREDECODE    | 24. PSH          |
| 25. CONFIG       | 26. L2TPDBG      | 27. L2TPDECODE   | 28. TELNET       |
| 29. TELNETDBG    | 30. TELNETDECODE | 31. FTPD         | 32. DNS          |
| 33. DNSDBG       | 34. IPSEC        | 35. IPSECDBG     | 36. IPSECDECODE  |
| 37. IKE          | 38. IKEDBG       | 39. IKEDECODE    | 40. HARDWAREMON  |
| 41. IPDBG        | 42. CAPI         | 43. IPDECODE     | 44. PPPDBG       |
| 45. PPPDECODE    | 46. DNSDECODE    | 47. DHCP         | 48. DHCPDBG      |
| 49. DHCPDECODE   | 50. FILTER       | 51. FILTERDBG    | 52. EVENTMIB     |
| 53. REBOOT       | 54. SNMP         | 55. OSPF         | 56. VRRP         |
| 57. SSL          | 58. CERT         | 59. GENERAL      | 60. TIME         |
```

```
| 64. EXPANSIONCARD| 67. FSM          | 68. SSH          | 69. LBSSF        |
| 71. PPPOE        | 72. PPPOEDBG     | 73. PPPOEDECODE  | 74. NETBIOS      |
| 75. CLIENT       | 76. XML          | 77. FW           | 78. FWDBG        |
| 79. FWDECODE     | 82. BMGT         | 83. BMGTDBG      | 84. FIPS         |
| 85. FIPSDIAG     | 86. WEBVPN       | 87. EMAILPROXY   | 88. CIFS         |
| 89. CIFSDBG      | 90. STC          | 91. CSTP         | 92. NAC          |
'q' to Quit, '<SPACE>' to Continue ->
| 93. EAP          | 94. EAPOUDP      |                  |                  |
-------------------------------------------------------------------------------

> Enter the Event Class to Add

VPN3K: Event Class -> 35

1) Enable this Class
2) Disable this Class

VPN3K: Event Class -> [ 1 ] 1

> Events to Log

VPN3K: Event Class -> [ 5 ] 9

> Events to Console

VPN3K: Event Class -> [ 3 ]

> Events to Syslog

VPN3K: Event Class -> [ 0 ]

> Events to E-mail

VPN3K: Event Class -> [ 0 ]

> Events to SNMP Trap

VPN3K: Event Class -> [ 0 ]

                           The Active Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP                          | 34. IPSEC                            |
| 35. IPSECDBG                         |                                      |
-------------------------------------------------------------------------------

1) Add an Event Class
2) Modify an Event Class
3) Delete an Event Class
4) Back

VPN3K: Event Class -> 1

                               The Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP      | 2. PSOS          | 3. SYSTEM        | 4. QUEUE         |
| 5. EVENT         | 6. EVENTDBG      | 7. SMTP          | 8. RM            |
| 9. DM            | 10. IP           | 11. TCP          | 12. PPP          |
| 13. L2TP         | 14. HTTP         | 15. AUTH         | 16. AUTHDBG      |
| 17. AUTHDECODE   | 18. PPTP         | 19. PPTPDBG      | 20. PPTPDECODE   |
| 21. GRE          | 22. GREDBG       | 23. GREDECODE    | 24. PSH          |
| 25. CONFIG       | 26. L2TPDBG      | 27. L2TPDECODE   | 28. TELNET       |
| 29. TELNETDBG    | 30. TELNETDECODE | 31. FTPD         | 32. DNS          |
| 33. DNSDBG       | 34. IPSEC        | 35. IPSECDBG     | 36. IPSECDECODE  |
```

```
| 37. IKE          | 38. IKEDBG       | 39. IKEDECODE    | 40. HARDWAREMON  |
| 41. IPDBG        | 42. CAPI         | 43. IPDECODE     | 44. PPPDBG       |
| 45. PPPDECODE    | 46. DNSDECODE    | 47. DHCP         | 48. DHCPDBG      |
| 49. DHCPDECODE   | 50. FILTER       | 51. FILTERDBG    | 52. EVENTMIB     |
| 53. REBOOT       | 54. SNMP         | 55. OSPF         | 56. VRRP         |
| 57. SSL          | 58. CERT         | 59. GENERAL      | 60. TIME         |
| 64. EXPANSIONCARD| 67. FSM          | 68. SSH          | 69. LBSSF        |
| 71. PPPOE        | 72. PPPOEDBG     | 73. PPPOEDECODE  | 74. NETBIOS      |
| 75. CLIENT       | 76. XML          | 77. FW           | 78. FWDBG        |
| 79. FWDECODE     | 82. BMGT         | 83. BMGTDBG      | 84. FIPS         |
| 85. FIPSDIAG     | 86. WEBVPN       | 87. EMAILPROXY   | 88. CIFS         |
| 89. CIFSDBG      | 90. STC          | 91. CSTP         | 92. NAC          |
'q' to Quit, '<SPACE>' to Continue ->
| 93. EAP          | 94. EAPOUDP      |                  |                  |
-------------------------------------------------------------------------------

> Enter the Event Class to Add

VPN3K: Event Class -> 36

1) Enable this Class
2) Disable this Class

VPN3K: Event Class -> [ 1 ] 1

> Events to Log

VPN3K: Event Class -> [ 5 ] 9

> Events to Console

VPN3K: Event Class -> [ 3 ]

> Events to Syslog

VPN3K: Event Class -> [ 0 ]

> Events to E-mail

VPN3K: Event Class -> [ 0 ]

> Events to SNMP Trap

VPN3K: Event Class -> [ 0 ]

                           The Active Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP                          | 34. IPSEC                            |
| 35. IPSECDBG                         | 36. IPSECDECODE                      |
-------------------------------------------------------------------------------

1) Add an Event Class
2) Modify an Event Class
3) Delete an Event Class
4) Back

VPN3K: Event Class -> 1

                              The Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP      | 2. PSOS          | 3. SYSTEM        | 4. QUEUE         |
| 5. EVENT         | 6. EVENTDBG      | 7. SMTP          | 8. RM            |
| 9. DM            | 10. IP           | 11. TCP          | 12. PPP          |
```

```
| 13. L2TP          | 14. HTTP          | 15. AUTH          | 16. AUTHDBG       |
| 17. AUTHDECODE    | 18. PPTP          | 19. PPTPDBG       | 20. PPTPDECODE    |
| 21. GRE           | 22. GREDBG        | 23. GREDECODE     | 24. PSH           |
| 25. CONFIG        | 26. L2TPDBG       | 27. L2TPDECODE    | 28. TELNET        |
| 29. TELNETDBG     | 30. TELNETDECODE  | 31. FTPD          | 32. DNS           |
| 33. DNSDBG        | 34. IPSEC         | 35. IPSECDBG      | 36. IPSECDECODE   |
| 37. IKE           | 38. IKEDBG        | 39. IKEDECODE     | 40. HARDWAREMON   |
| 41. IPDBG         | 42. CAPI          | 43. IPDECODE      | 44. PPPDBG        |
| 45. PPPDECODE     | 46. DNSDECODE     | 47. DHCP          | 48. DHCPDBG       |
| 49. DHCPDECODE    | 50. FILTER        | 51. FILTERDBG     | 52. EVENTMIB      |
| 53. REBOOT        | 54. SNMP          | 55. OSPF          | 56. VRRP          |
| 57. SSL           | 58. CERT          | 59. GENERAL       | 60. TIME          |
| 64. EXPANSIONCARD| 67. FSM           | 68. SSH           | 69. LBSSF         |
| 71. PPPOE         | 72. PPPOEDBG      | 73. PPPOEDECODE   | 74. NETBIOS       |
| 75. CLIENT        | 76. XML           | 77. FW            | 78. FWDBG         |
| 79. FWDECODE      | 82. BMGT          | 83. BMGTDBG       | 84. FIPS          |
| 85. FIPSDIAG      | 86. WEBVPN        | 87. EMAILPROXY    | 88. CIFS          |
| 89. CIFSDBG       | 90. STC           | 91. CSTP          | 92. NAC           |
'q' to Quit, '<SPACE>' to Continue ->
| 93. EAP           | 94. EAPOUDP       |                   |                   |
-------------------------------------------------------------------------------

> Enter the Event Class to Add

VPN3K: Event Class -> 38

1) Enable this Class
2) Disable this Class

VPN3K: Event Class -> [ 1 ] 1

> Events to Log

VPN3K: Event Class -> [ 5 ] 9

> Events to Console

VPN3K: Event Class -> [ 3 ]

> Events to Syslog

VPN3K: Event Class -> [ 0 ]

> Events to E-mail

VPN3K: Event Class -> [ 0 ]

> Events to SNMP Trap

VPN3K: Event Class -> [ 0 ]

                           The Active Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP                          | 34. IPSEC                            |
| 35. IPSECDBG                         | 36. IPSECDECODE                      |
| 38. IKEDBG                           |                                      |
-------------------------------------------------------------------------------

1) Add an Event Class
2) Modify an Event Class
3) Delete an Event Class
4) Back
```

```
VPN3K: Event Class -> 1

                              The Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP      | 2. PSOS          | 3. SYSTEM        | 4. QUEUE         |
| 5. EVENT         | 6. EVENTDBG      | 7. SMTP          | 8. RM            |
| 9. DM            | 10. IP           | 11. TCP          | 12. PPP          |
| 13. L2TP         | 14. HTTP         | 15. AUTH         | 16. AUTHDBG      |
| 17. AUTHDECODE   | 18. PPTP         | 19. PPTPDBG      | 20. PPTPDECODE   |
| 21. GRE          | 22. GREDBG       | 23. GREDECODE    | 24. PSH          |
| 25. CONFIG       | 26. L2TPDBG      | 27. L2TPDECODE   | 28. TELNET       |
| 29. TELNETDBG    | 30. TELNETDECODE | 31. FTPD         | 32. DNS          |
| 33. DNSDBG       | 34. IPSEC        | 35. IPSECDBG     | 36. IPSECDECODE  |
| 37. IKE          | 38. IKEDBG       | 39. IKEDECODE    | 40. HARDWAREMON  |
| 41. IPDBG        | 42. CAPI         | 43. IPDECODE     | 44. PPPDBG       |
| 45. PPPDECODE    | 46. DNSDECODE    | 47. DHCP         | 48. DHCPDBG      |
| 49. DHCPDECODE   | 50. FILTER       | 51. FILTERDBG    | 52. EVENTMIB     |
| 53. REBOOT       | 54. SNMP         | 55. OSPF         | 56. VRRP         |
| 57. SSL          | 58. CERT         | 59. GENERAL      | 60. TIME         |
| 64. EXPANSIONCARD| 67. FSM          | 68. SSH          | 69. LBSSF        |
| 71. PPPOE        | 72. PPPOEDBG     | 73. PPPOEDECODE  | 74. NETBIOS      |
| 75. CLIENT       | 76. XML          | 77. FW           | 78. FWDBG        |
| 79. FWDECODE     | 82. BMGT         | 83. BMGTDBG      | 84. FIPS         |
| 85. FIPSDIAG     | 86. WEBVPN       | 87. EMAILPROXY   | 88. CIFS         |
| 89. CIFSDBG      | 90. STC          | 91. CSTP         | 92. NAC          |
'q' to Quit, '<SPACE>' to Continue ->
| 93. EAP          | 94. EAPOUDP      |                  |                  |
-------------------------------------------------------------------------------

> Enter the Event Class to Add

VPN3K: Event Class -> 39

1) Enable this Class
2) Disable this Class

VPN3K: Event Class -> [ 1 ]

> Events to Log

VPN3K: Event Class -> [ 5 ] 9

> Events to Console

VPN3K: Event Class -> [ 3 ]

> Events to Syslog

VPN3K: Event Class -> [ 0 ]

> Events to E-mail

VPN3K: Event Class -> [ 0 ]

> Events to SNMP Trap

VPN3K: Event Class -> [ 0 ]

                            The Active Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP                          | 34. IPSEC                            |
| 35. IPSECDBG                         | 36. IPSECDECODE                      |
| 38. IKEDBG                           | 39. IKEDECODE                        |
```

```
-------------------------------------------------------------------------------

1) Add an Event Class
2) Modify an Event Class
3) Delete an Event Class
4) Back

VPN3K: Event Class -> 1

                              The Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP      | 2. PSOS          | 3. SYSTEM        | 4. QUEUE         |
| 5. EVENT         | 6. EVENTDBG      | 7. SMTP          | 8. RM            |
| 9. DM            | 10. IP           | 11. TCP          | 12. PPP          |
| 13. L2TP         | 14. HTTP         | 15. AUTH         | 16. AUTHDBG      |
| 17. AUTHDECODE   | 18. PPTP         | 19. PPTPDBG      | 20. PPTPDECODE   |
| 21. GRE          | 22. GREDBG       | 23. GREDECODE    | 24. PSH          |
| 25. CONFIG       | 26. L2TPDBG      | 27. L2TPDECODE   | 28. TELNET       |
| 29. TELNETDBG    | 30. TELNETDECODE | 31. FTPD         | 32. DNS          |
| 33. DNSDBG       | 34. IPSEC        | 35. IPSECDBG     | 36. IPSECDECODE  |
| 37. IKE          | 38. IKEDBG       | 39. IKEDECODE    | 40. HARDWAREMON  |
| 41. IPDBG        | 42. CAPI         | 43. IPDECODE     | 44. PPPDBG       |
| 45. PPPDECODE    | 46. DNSDECODE    | 47. DHCP         | 48. DHCPDBG      |
| 49. DHCPDECODE   | 50. FILTER       | 51. FILTERDBG    | 52. EVENTMIB     |
| 53. REBOOT       | 54. SNMP         | 55. OSPF         | 56. VRRP         |
| 57. SSL          | 58. CERT         | 59. GENERAL      | 60. TIME         |
| 64. EXPANSIONCARD| 67. FSM          | 68. SSH          | 69. LBSSF        |
| 71. PPPOE        | 72. PPPOEDBG     | 73. PPPOEDECODE  | 74. NETBIOS      |
| 75. CLIENT       | 76. XML          | 77. FW           | 78. FWDBG        |
| 79. FWDECODE     | 82. BMGT         | 83. BMGTDBG      | 84. FIPS         |
| 85. FIPSDIAG     | 86. WEBVPN       | 87. EMAILPROXY   | 88. CIFS         |
| 89. CIFSDBG      | 90. STC          | 91. CSTP         | 92. NAC          |
'q' to Quit, '<SPACE>' to Continue ->
| 93. EAP          | 94. EAPOUDP      |                  |                  |
-------------------------------------------------------------------------------

> Enter the Event Class to Add

VPN3K: Event Class -> 37

1) Enable this Class
2) Disable this Class

VPN3K: Event Class -> [ 1 ]

> Events to Log

VPN3K: Event Class -> [ 5 ] 9

> Events to Console

VPN3K: Event Class -> [ 3 ]

> Events to Syslog

VPN3K: Event Class -> [ 0 ]

> Events to E-mail

VPN3K: Event Class -> [ 0 ]

> Events to SNMP Trap
```

```
VPN3K: Event Class -> [ 0 ]

                           The Active Event Classes
-------------------------------------------------------------------------------
| 1. MIB2TRAP                          | 34. IPSEC                            |
| 35. IPSECDBG                         | 36. IPSECDECODE                      |
| 37. IKE                              | 38. IKEDBG                           |
| 39. IKEDECODE                        |                                      |
-------------------------------------------------------------------------------

1) Add an Event Class
2) Modify an Event Class
3) Delete an Event Class
4) Back

VPN3K: Event Class ->
```

Configure events monitor:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

VPN3K: Main -> 3

1) Routing Table
2) Event Log
3) System Status
4) Sessions
5) General Statistics
6) Dynamic Filters
7) Back

VPN3K: Monitor -> 2

1) Configure Log viewing parameters
2) View Event Log
3) Save Log
4) Clear Log
5) Configure WebVPN Logging
6) Back

VPN3K: Log -> 4

1) Configure Log viewing parameters
2) View Event Log
3) Save Log
4) Clear Log
5) Configure WebVPN Logging
6) Back

VPN3K: Log -> 1

> Events per page

VPN3K: Log -> [ 5 ] 100

                              The Event Classes
-----------------------------------------------------------------------------
| 1. MIB2TRAP      | 2. PSOS          | 3. SYSTEM        | 4. QUEUE         |
```

```
| 5. EVENT          | 6. EVENTDBG       | 7. SMTP           | 8. RM             |
| 9. DM             | 10. IP            | 11. TCP           | 12. PPP           |
| 13. L2TP          | 14. HTTP          | 15. AUTH          | 16. AUTHDBG       |
| 17. AUTHDECODE    | 18. PPTP          | 19. PPTPDBG       | 20. PPTPDECODE    |
| 21. GRE           | 22. GREDBG        | 23. GREDECODE     | 24. PSH           |
| 25. CONFIG        | 26. L2TPDBG       | 27. L2TPDECODE    | 28. TELNET        |
| 29. TELNETDBG     | 30. TELNETDECODE  | 31. FTPD          | 32. DNS           |
| 33. DNSDBG        | 34. IPSEC         | 35. IPSECDBG      | 36. IPSECDECODE   |
| 37. IKE           | 38. IKEDBG        | 39. IKEDECODE     | 40. HARDWAREMON   |
| 41. IPDBG         | 42. CAPI          | 43. IPDECODE      | 44. PPPDBG        |
| 45. PPPDECODE     | 46. DNSDECODE     | 47. DHCP          | 48. DHCPDBG       |
| 49. DHCPDECODE    | 50. FILTER        | 51. FILTERDBG     | 52. EVENTMIB      |
| 53. REBOOT        | 54. SNMP          | 55. OSPF          | 56. VRRP          |
| 57. SSL           | 58. CERT          | 59. GENERAL       | 60. TIME          |
| 64. EXPANSIONCARD| 67. FSM           | 68. SSH           | 69. LBSSF         |
| 71. PPPOE         | 72. PPPOEDBG      | 73. PPPOEDECODE   | 74. NETBIOS       |
| 75. CLIENT        | 76. XML           | 77. FW            | 78. FWDBG         |
| 79. FWDECODE      | 82. BMGT          | 83. BMGTDBG       | 84. FIPS          |
| 85. FIPSDIAG      | 86. WEBVPN        | 87. EMAILPROXY    | 88. CIFS          |
| 89. CIFSDBG       | 90. STC           | 91. CSTP          | 92. NAC           |
'q' to Quit, '<SPACE>' to Continue ->
| 93. EAP           | 94. EAPOUDP       |                   |                   |
-------------------------------------------------------------------------------

For multiple classes, separate numbers with spaces.

> Event classes to view (0 for all Classes)

VPN3K: Log -> 0

     The following is a description of the Event Severity Levels

Severities  1 - 3 are Warning :   1  - Fault    2  - Warning1   3 - Warning2
Severities  4 - 6 are Info    :   4  - Info1    5  - Info2      6 - Info3
Severities  7 - 9 are Debug   :   7  - Debug1   8  - Debug2     9 - Debug3
Severities  10, 11 are Decodes:   10 - Hdecode  11 - Ldecode
Severities  12, 13 are Dumps  :   12 - HdrDump  13 - PktDump

For multiple severities, separate numbers with spaces.

> Event severities to view (0 for all Severities)

VPN3K: Log -> 0

> Client Address to view (0.0.0.0 for all addresses)

VPN3K: Log -> [ 0.0.0.0 ]

                              Current User Groups
-------------------------------------------------------------------------------
| 1. 136.1.122.2                      |                                     |
-------------------------------------------------------------------------------

> Group to view (-1 for All Groups, 0 for Base Group)

VPN3K: Log -> 1

1) Configure Log viewing parameters
2) View Event Log
3) Save Log
4) Clear Log
5) Configure WebVPN Logging
6) Back
```

```
VPN3K: Log -> 2

    No more Events

1) First Page
2) Previous Page
3) Next Page
4) Last Page
5) Back

VPN3K: Log ->
```

Verification

```
R2#ping 150.1.1.1 so lo 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/8/8 ms

1) Configure Log viewing parameters
2) View Event Log
3) Save Log
4) Clear Log
5) Configure WebVPN Logging
6) Back

VPN3K: Log -> 2

IKE Main Mode Exchange begins:

191 01/17/2007 01:14:45.150 SEV=9 IKEDBG/1 RPT=15 136.1.122.2
Group [136.1.122.2]
Processing ID

192 01/17/2007 01:14:45.150 SEV=9 IKEDBG/0 RPT=46 136.1.122.2
Group [136.1.122.2]
processing hash

193 01/17/2007 01:14:45.150 SEV=9 IKEDBG/0 RPT=47 136.1.122.2
Group [136.1.122.2]
computing hash

194 01/17/2007 01:14:45.150 SEV=9 IKEDBG/0 RPT=48 136.1.122.2
Group [136.1.122.2]
Processing Notify payload

Looking for a match by peer's IP (it's Main Mode):

201 01/17/2007 01:14:45.150 SEV=9 IKEDBG/23 RPT=2 136.1.122.2
Group [136.1.122.2]
Starting group lookup for peer 136.1.122.2

202 01/17/2007 01:14:45.260 SEV=7 IKEDBG/80 RPT=3 136.1.122.2
Group [136.1.122.2]
Found Phase 1 Group (136.1.122.2)

Group found, extracting authentication attributes:
```

```
203 01/17/2007 01:14:45.260 SEV=7 IKEDBG/14 RPT=3 136.1.122.2
Group [136.1.122.2]
Authentication configured for Internal

204 01/17/2007 01:14:45.260 SEV=9 IKEDBG/19 RPT=2 136.1.122.2
Group [136.1.122.2]
IKEGetUserAttributes: IP Compression = reset

205 01/17/2007 01:14:45.260 SEV=9 IKEDBG/78 RPT=3 136.1.122.2
Group [136.1.122.2]
IKEGetUserAttributes: Browser Proxy Setting = 1

206 01/17/2007 01:14:45.260 SEV=9 IKEDBG/78 RPT=4 136.1.122.2
Group [136.1.122.2]
IKEGetUserAttributes: Browser Proxy Bypass Local = 0
```

Respond with IKE message, presenting our ID and authenticationg:

```
207 01/17/2007 01:14:45.260 SEV=9 IKEDBG/1 RPT=16 136.1.122.2
Group [136.1.122.2]
constructing ID

208 01/17/2007 01:14:45.260 SEV=9 IKEDBG/0 RPT=49
Group [136.1.122.2]
construct hash payload

209 01/17/2007 01:14:45.260 SEV=9 IKEDBG/0 RPT=50 136.1.122.2
Group [136.1.122.2]
computing hash

211 01/17/2007 01:14:45.260 SEV=9 IKEDBG/46 RPT=10 136.1.122.2
Group [136.1.122.2]
constructing dpd vid payload

215 01/17/2007 01:14:45.260 SEV=4 IKE/119 RPT=4 136.1.122.2
Group [136.1.122.2]
PHASE 1 COMPLETED
```

Phase 1 has been completed, after authentication and attributes negotiation

```
217 01/17/2007 01:14:45.260 SEV=7 IKEDBG/82 RPT=3 136.1.122.2
Group [136.1.122.2]
Starting phase 1 rekey timer: 82080000 (ms)

218 01/17/2007 01:14:45.260 SEV=4 AUTH/22 RPT=4 136.1.122.2
User [136.1.122.2] Group [136.1.122.2] connected, Session Type: IPSec/LAN-to-
LAN
```

Phase2 begins:

```
230 01/17/2007 01:14:45.280 SEV=9 IKEDBG/0 RPT=52 136.1.122.2
Group [136.1.122.2]
processing hash

231 01/17/2007 01:14:45.280 SEV=9 IKEDBG/0 RPT=53 136.1.122.2
Group [136.1.122.2]
processing SA payload

245 01/17/2007 01:14:45.280 SEV=9 IKEDBG/1 RPT=17 136.1.122.2
Group [136.1.122.2]
processing nonce payload
```

Received proxy id:

```
246 01/17/2007 01:14:45.280 SEV=9 IKEDBG/1 RPT=18 136.1.122.2
Group [136.1.122.2]
Processing ID

247 01/17/2007 01:14:45.280 SEV=5 IKE/35 RPT=4 136.1.122.2
Group [136.1.122.2]
Received remote IP Proxy Subnet data in ID Payload:
 Address 150.1.2.0, Mask 255.255.255.0, Protocol 0, Port 0

250 01/17/2007 01:14:45.280 SEV=9 IKEDBG/1 RPT=19 136.1.122.2
Group [136.1.122.2]
Processing ID

251 01/17/2007 01:14:45.280 SEV=5 IKE/34 RPT=4 136.1.122.2
Group [136.1.122.2]
Received local IP Proxy Subnet data in ID Payload:
 Address 150.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0

254 01/17/2007 01:14:45.280 SEV=8 IKEDBG/83 RPT=3 136.1.122.2
Group [136.1.122.2]
QM IsRekeyed old sa not found by addr
```

Applying SA attributes:

```
255 01/17/2007 01:14:45.280 SEV=5 IKE/66 RPT=4 136.1.122.2
Group [136.1.122.2]
IKE Remote Peer configured for SA: L2L:VPN_TO_R2

256 01/17/2007 01:14:45.280 SEV=9 IKEDBG/1 RPT=20 136.1.122.2
Group [136.1.122.2]
processing IPSEC SA
```

Phase2 Proposal match found:

```
258 01/17/2007 01:14:45.280 SEV=7 IKEDBG/27 RPT=3 136.1.122.2
Group [136.1.122.2]
IPSec SA Proposal # 1, Transform # 1 acceptable
Matches global IPSec SA entry # 9 Proposal (L2L:VPN_TO_R2)
```

Generating SPI:

```
261 01/17/2007 01:14:45.280 SEV=7 IKEDBG/85 RPT=3 136.1.122.2
Group [136.1.122.2]
IKE: requesting SPI!  (Protocol=ESP)

268 01/17/2007 01:14:45.290 SEV=8 IKEDBG/6 RPT=3 136.1.122.2
Group [136.1.122.2]
IKE got SPI from key engine: SPI = 0x55b6504a

269 01/17/2007 01:14:45.290 SEV=9 IKEDBG/0 RPT=54 136.1.122.2
Group [136.1.122.2]
oakley constucting quick mode

270 01/17/2007 01:14:45.290 SEV=9 IKEDBG/0 RPT=55 136.1.122.2
Group [136.1.122.2]
constructing blank hash

271 01/17/2007 01:14:45.290 SEV=9 IKEDBG/0 RPT=56 136.1.122.2
Group [136.1.122.2]
constructing ISA_SA for ipsec
```

```
272 01/17/2007 01:14:45.290 SEV=9 IKEDBG/1 RPT=21 136.1.122.2
Group [136.1.122.2]
constructing ipsec nonce payload

273 01/17/2007 01:14:45.290 SEV=9 IKEDBG/1 RPT=22 136.1.122.2
Group [136.1.122.2]
constructing proxy ID
```

Transmitting our proxies:

```
274 01/17/2007 01:14:45.290 SEV=7 IKEDBG/91 RPT=3 136.1.122.2
Group [136.1.122.2]
Transmitting Proxy Id:
  Remote subnet: 150.1.2.0  Mask 255.255.255.0 Protocol 0  Port 0
  Local subnet:  150.1.1.0  mask 255.255.255.0 Protocol 0  Port 0

278 01/17/2007 01:14:45.290 SEV=9 IKEDBG/0 RPT=57 136.1.122.2
Group [136.1.122.2]
constructing qm hash

290 01/17/2007 01:14:45.310 SEV=9 IKEDBG/0 RPT=58 136.1.122.2
Group [136.1.122.2]
processing hash

291 01/17/2007 01:14:45.310 SEV=9 IKEDBG/0 RPT=59 136.1.122.2
Group [136.1.122.2]
loading all IPSEC SAs
```

Generating QM keying material:

```
292 01/17/2007 01:14:45.310 SEV=9 IKEDBG/1 RPT=23 136.1.122.2
Group [136.1.122.2]
Generating Quick Mode Key!

293 01/17/2007 01:14:45.320 SEV=9 IKEDBG/1 RPT=24 136.1.122.2
Group [136.1.122.2]
Generating Quick Mode Key!

294 01/17/2007 01:14:45.320 SEV=7 IKEDBG/93 RPT=3 136.1.122.2
Group [136.1.122.2]
Loading subnet:
  Dst: 150.1.1.0  mask: 255.255.255.0
  Src: 150.1.2.0  mask: 255.255.255.0
```

SAs have been negotiated:

```
297 01/17/2007 01:14:45.320 SEV=4 IKE/49 RPT=4 136.1.122.2
Group [136.1.122.2]
Security negotiation complete for LAN-to-LAN Group (136.1.122.2)
Responder, Inbound SPI = 0x55b6504a, Outbound SPI = 0xbf527809

322 01/17/2007 01:14:45.330 SEV=8 IKEDBG/86 RPT=3 136.1.122.2
Group [136.1.122.2]
pitcher: rcv KEY_UPDATE, spi 0x55b6504a

323 01/17/2007 01:14:45.330 SEV=4 IKE/120 RPT=4 136.1.122.2
Group [136.1.122.2]
PHASE 2 COMPLETED (msgid=022fd181)

326 01/17/2007 01:14:46.270 SEV=8 IKEDBG/87 RPT=3 136.1.122.2
Group [136.1.122.2]
pitcher: recv KEY_SA_ACTIVE spi 0x55b6504a
```

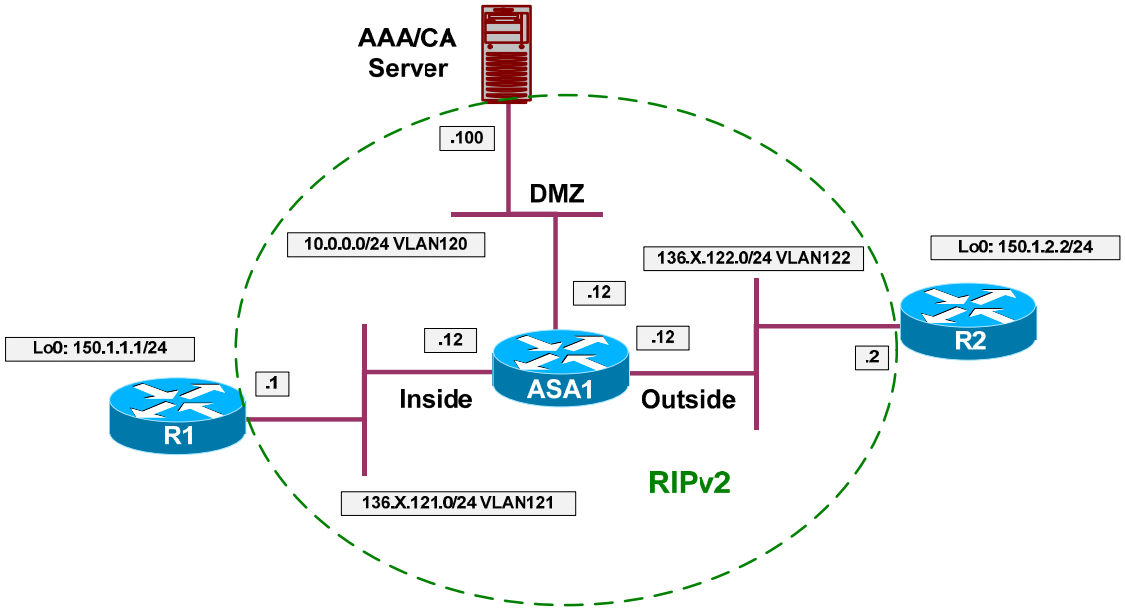
```
1) First Page
2) Previous Page
3) Next Page
4) Last Page
5) Back

VPN3K: Log ->
```

Further Reading

VPN3k: System Configuration/Events

IPsec and Fragmentation Issues

Objective: Configure IOS router for packet fragmentation prior to encryption.



Directions

- Configure devices as per the "VPN/IPsec LAN-to-LAN" scenario "IOS and IOS with PSK Across the PIX/ASA".
- IPsec termination router permormace may be severely affected, if encrypted packets are fragmented along the way.
- This is due to the fact the fragments re-assembly takes place at the process level, severely degrading overall performance.
- To avoid this issue, a near-MTU sized packet may be pre-fragmented by sending router before encryption.
- Configure R1 for IPsec pre-fragmentation, and verify how it changes encryption behavior.
- Configure access-list on R2 to match fragmented ESP packets, and see if they apper after the pre-fragmentation is enabled.

Final Configuration

```
R2:
access-list 100 permit esp any any fragments
access-list 100 permit ip any any
!
interface E 0/0
 ip access-group 100 in

R1:
interface E0/0
 crypto ipsec fragmentation before-encryption
```

Verification

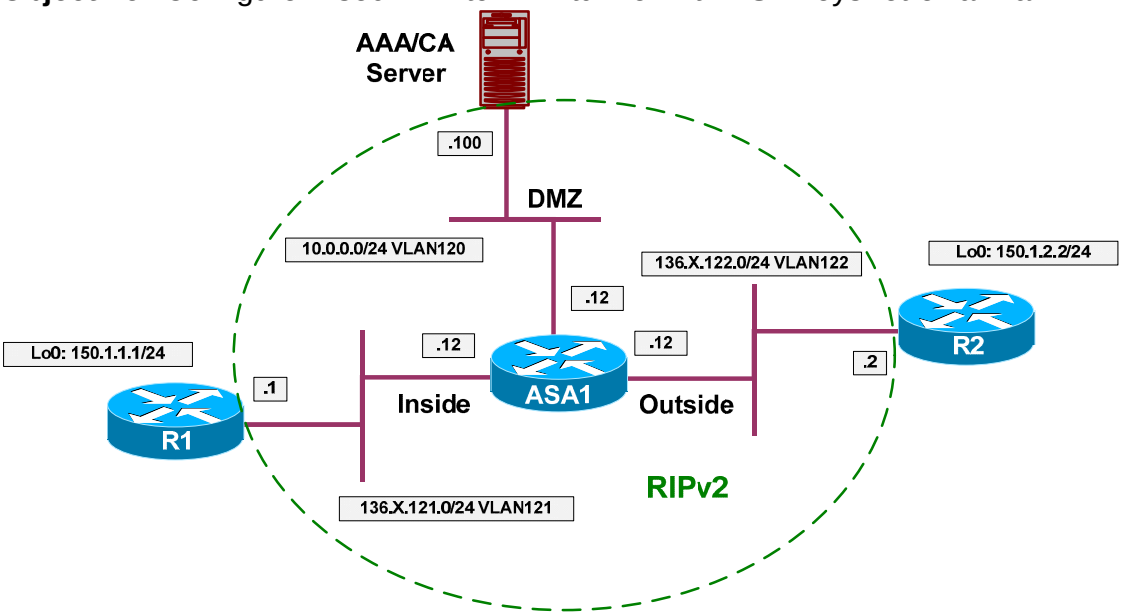
```
R2#show ip access-lists 100
Extended IP access list 100
    10 permit esp any any fragments
    20 permit ip any any (6 matches)

R1#sh running-config interface ethernet 0/0
Building configuration...

Current configuration : 141 bytes
!
interface Ethernet0/0
 ip address 136.1.121.1 255.255.255.0
 half-duplex
 crypto map VPN
 crypto ipsec fragmentation after-encryption
end

R1#ping 150.1.2.2 source loopback 0 size 1500 repeat 10

Type escape sequence to abort.
Sending 10, 1500-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 64/65/68 ms

R2#show ip access-lists 100
Extended IP access list 100
    10 permit esp any any fragments (20 matches)
    20 permit ip any any (44 matches)

R1#sh running-config interface ethernet 0/0
Building configuration...

Current configuration : 142 bytes
!
interface Ethernet0/0
 ip address 136.1.121.1 255.255.255.0
 half-duplex
 crypto map VPN
 crypto ipsec fragmentation before-encryption
end

R2#clear access-list counters

R1#ping 150.1.2.2 source loopback 0 size 1500 repeat 10

Type escape sequence to abort.
Sending 10, 1500-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 60/61/64 ms

R2#show ip access-lists 100
Extended IP access list 100
    10 permit esp any any fragments
    20 permit ip any any (40 matches)
```

Further Reading

Pre-Fragmentation for IPSec VPNs

ISAKMP Pre-Shared Keys via AAA

Objective: Configure IPsec LAN-to-LAN tunnel with PSK keys retreival via AAA.



Directions

- Configure devices as per the "VPN/IPsec LAN-to-LAN" scenario "IOS and IOS with PSK Across the PIX/ASA".
- IOS router could retreive ISAKMP attributes from RADIUS server. To make this possible, it sends remote peer ID as login name, along with password "cisco" (hardcoded value). The attributes returned in reply are used to extract pre-shared key for IKE, and to deduce various other attributes.
- Configure the ASA1 to permit inbound RADIUS traffic.
  - Add an entry to access-list OUTSIDE_IN to permit UDP traffic to host 10.0.0.100 port 1645
- Configure ISAKMP peer 136.1.122.2 policy on R1:
  - Set aggressive mode with password "CISCO".
  - Use self-id FQDN "R1".
- Enable AAA on R2 and safeguard console authentication.
- Configure authorization list ISAKMP to use RADIUS server.
- Configure RADIUS server 10.0.0.100 with key CISCO.
- Delete pre-shared key "CISCO" for address 136.1.121.1
- Configure crypto map VPN for ISAKMP authorization with list ISAKMP.
- Configure ACS:
  - Add new RADIUS network client corresponding to R2 with IP 136.1.122.2
  - Create new group ISAKMP.

- Disable IP address assignment.
- Add Cisco AV-Pair “ipsec:key-exchange=IKE”.
- Set IETF RADIUS attribute “Service” to value “Outbound”.
- Set IETF RADIUS attribute “Tunnel-Type” to value “IP ESP”.
- Set IETF RADIUS attribute “Tunnel-Password” to value “CISCO”. This is the actual pre-shared key.

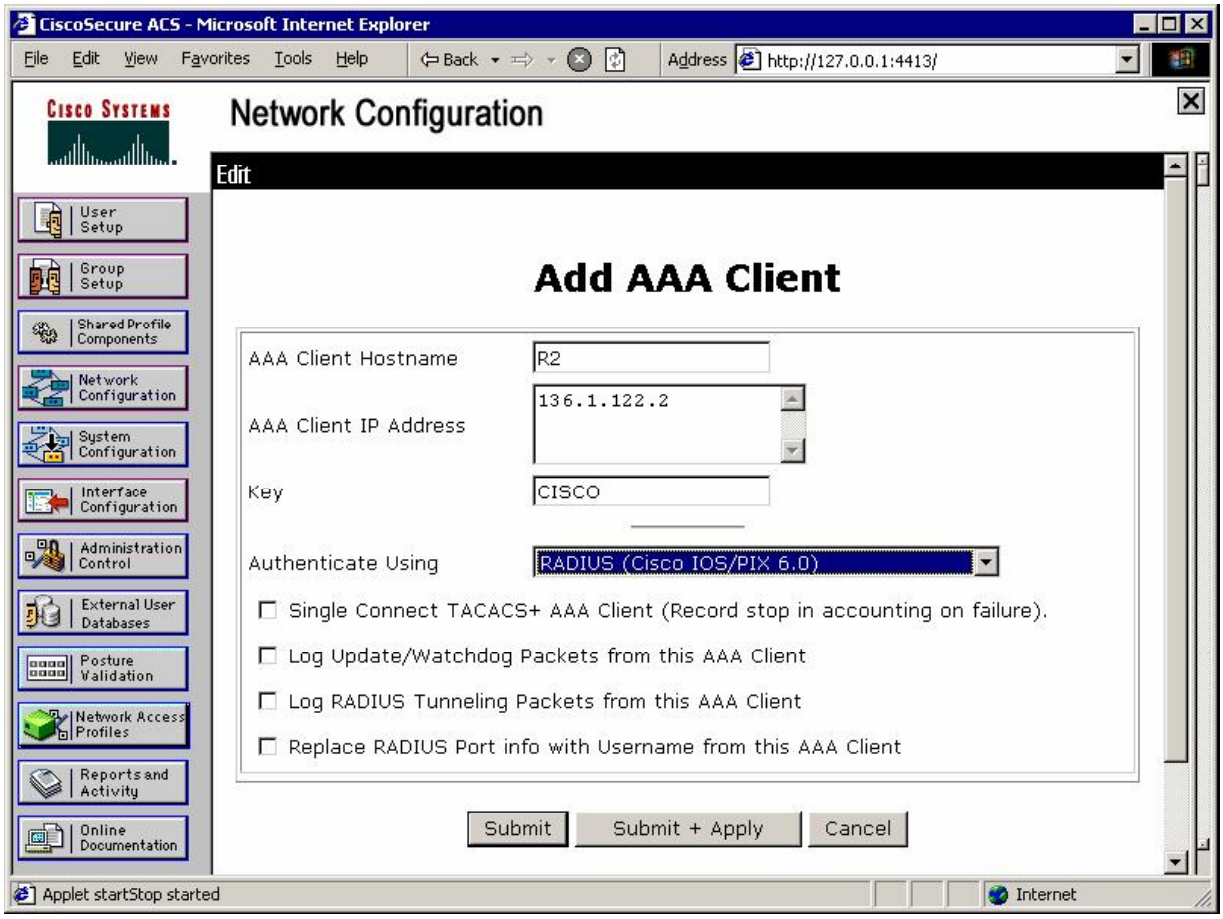
o Add new user with name “R1” and password “cisco”
  - Assign this user to group “ISAKMP”.

Final Configuration

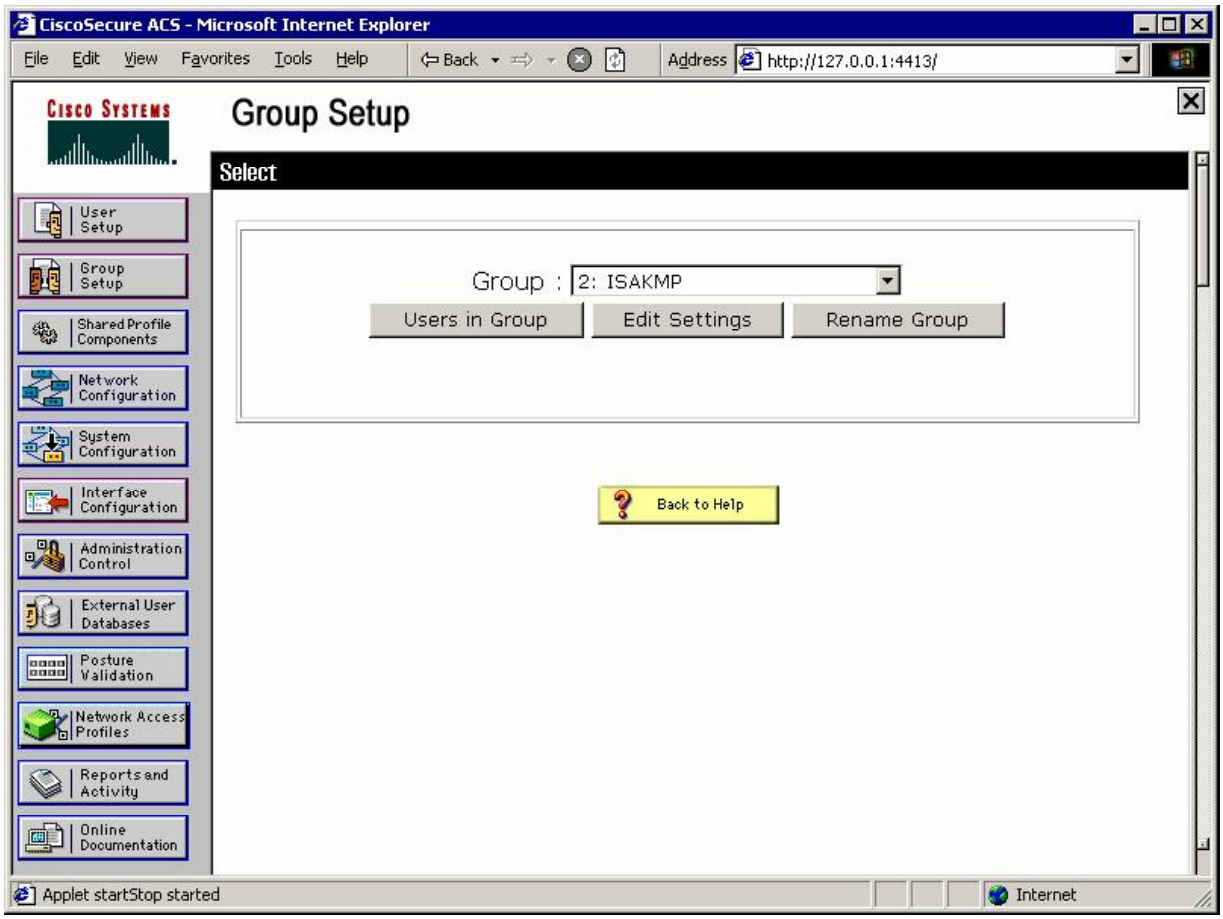
```
ASA1:
access-list OUTSIDE_IN permit udp any any eq 1645

R2:
aaa-new model
aaa authentication login CONSOLE none
aaa authorization network ISAKMP group radius
!
line console 0
  login authentication CONSOLE
!
radius-server host 10.0.0.100 key CISCO

no crypto isakmp key CISCO address 136.1.121.1
crypto map VPN isakmp authorization list ISAKMP

R1:
crypto isakmp peer address 136.1.122.2
 set aggressive-mode password CISCO
 set aggressive-mode client-endpoint fqdn R1
```

ACS:

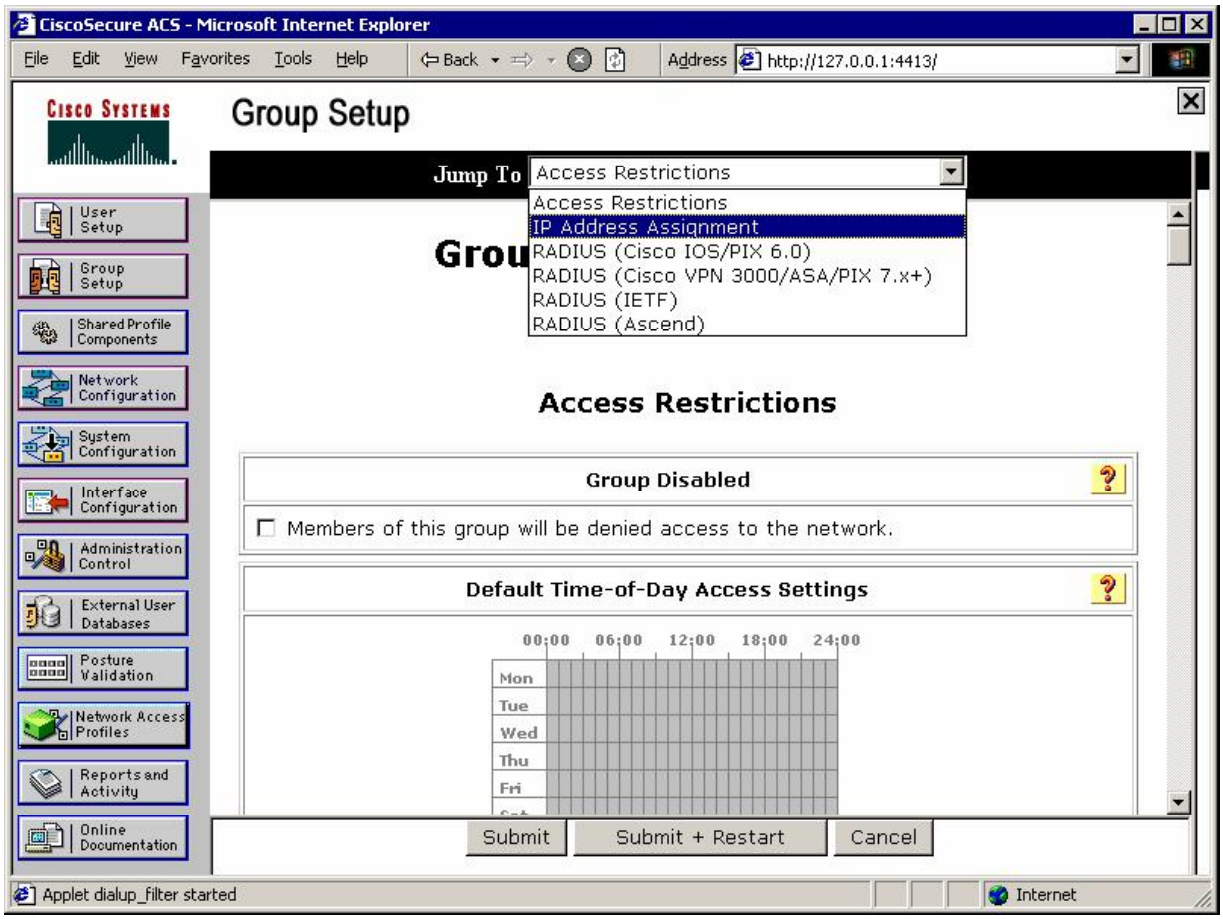
Add new AAA client for to R2:

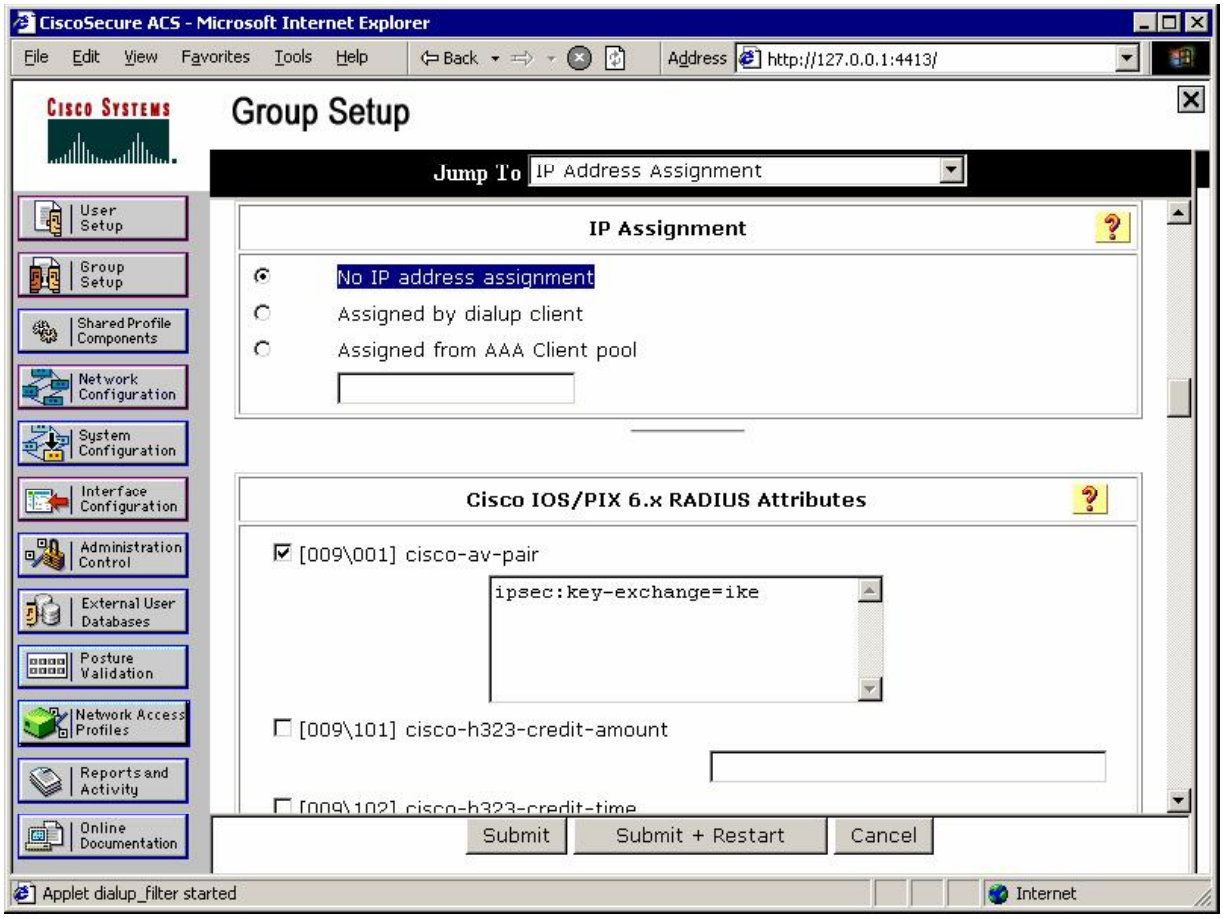


Create new group named "ISAKMP":

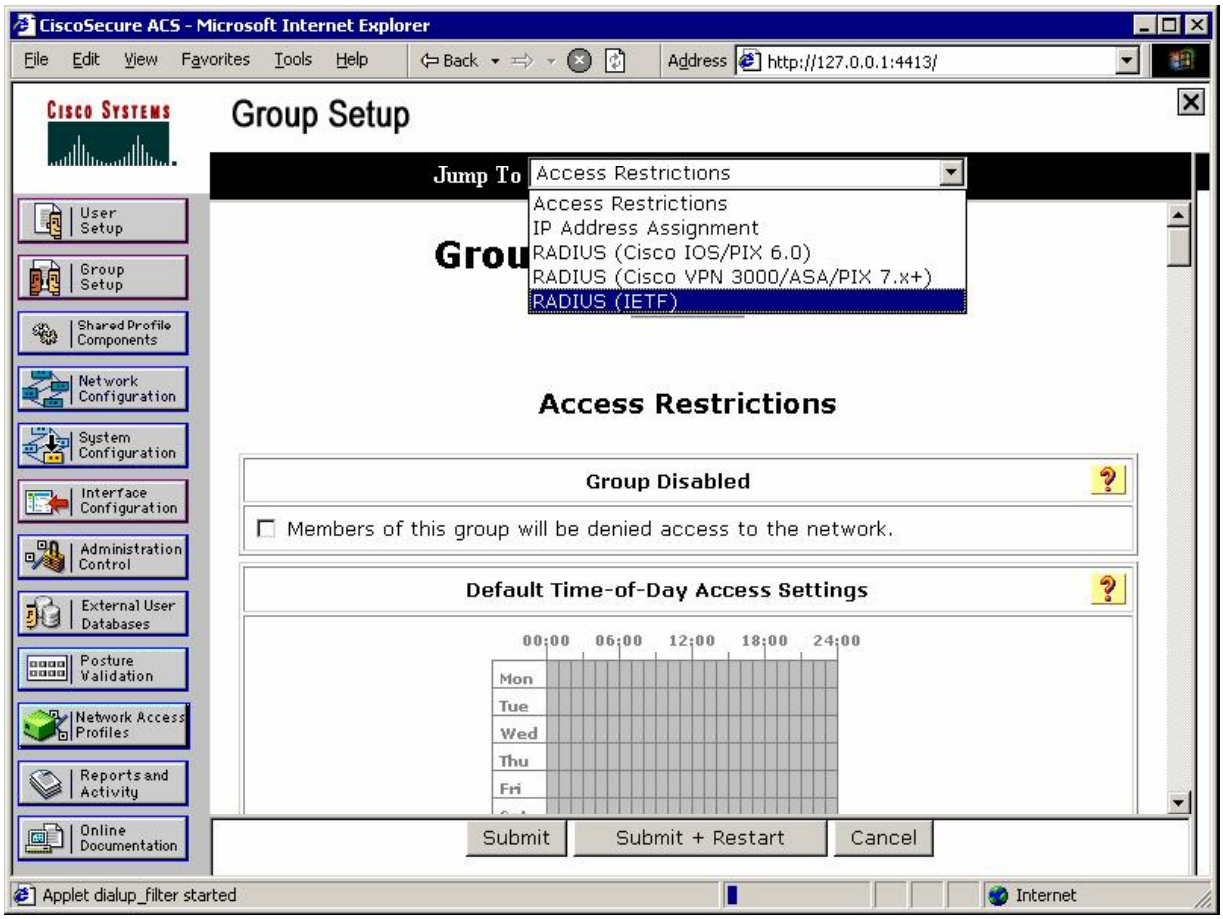


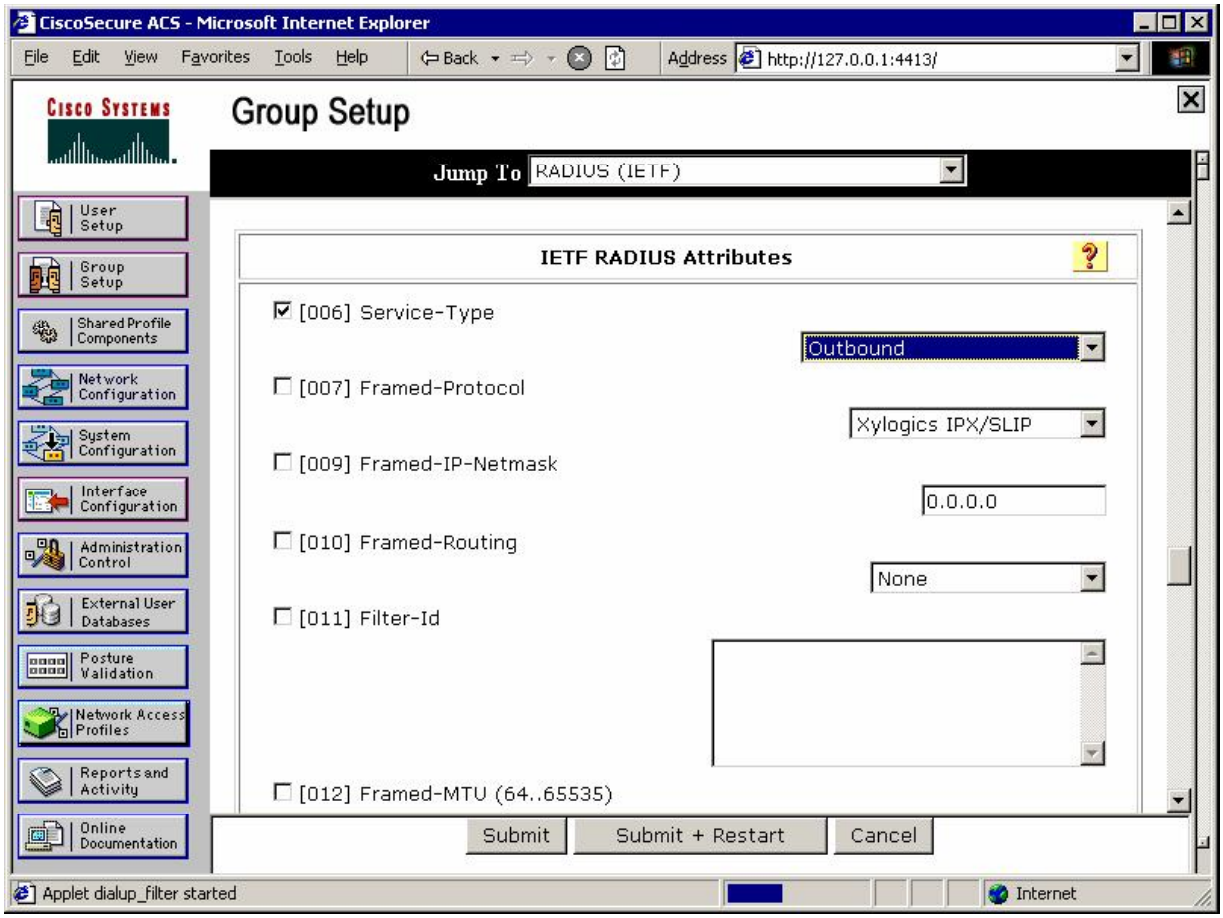
Configure IP address assignment (disable it actually) and Cisco AV-Pair:

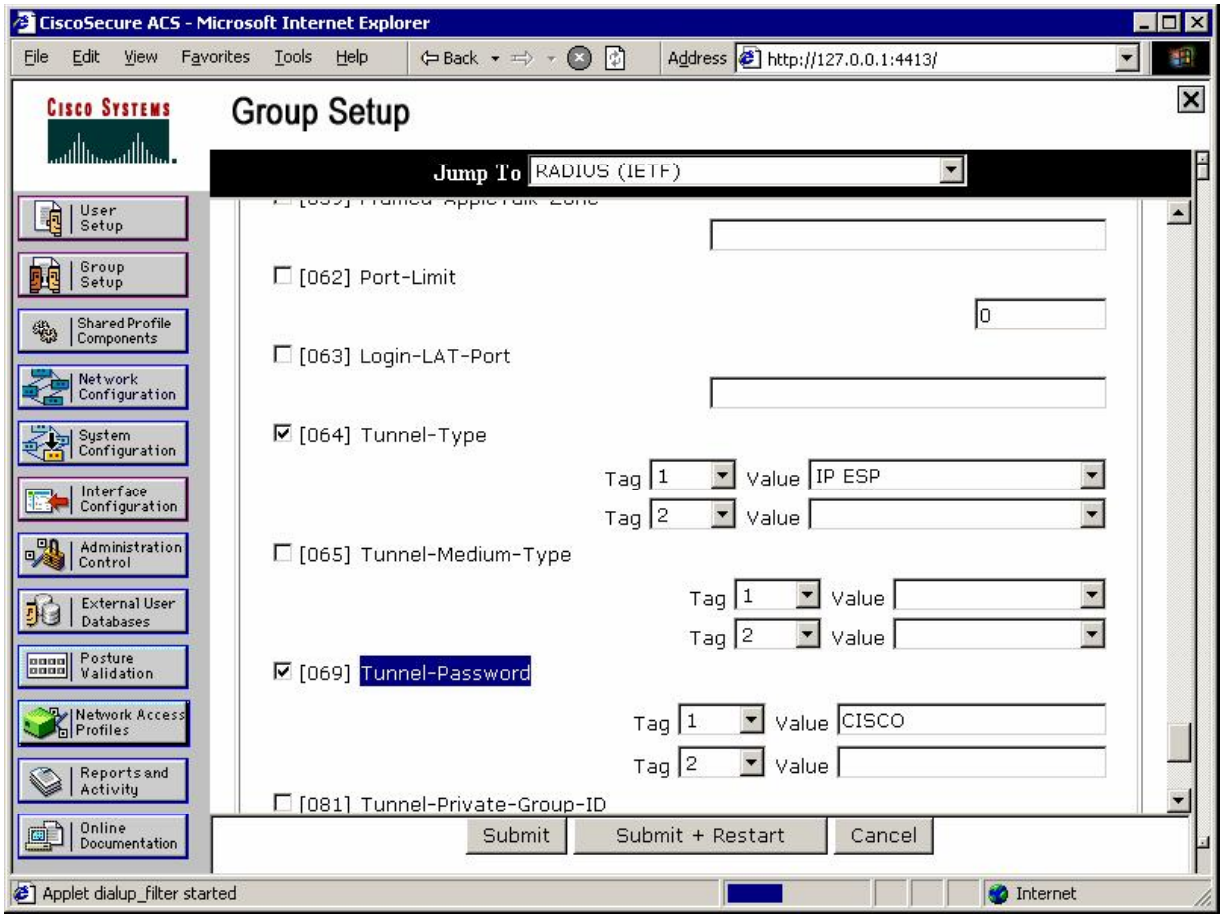



CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:4413/
Cisco Systems
Group Setup
Jump To IP Address Assignment
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
IP Assignment
No IP address assignment
Assigned by dialup client
Assigned from AAA Client pool
Cisco IOS/PIX 6.x RADIUS Attributes
[009\001] cisco-av-pair
ipsec:key-exchange=ike
[009\101] cisco-h323-credit-amount
Submit
Submit + Restart
Cancel
Applet dialup_filter started
Internet

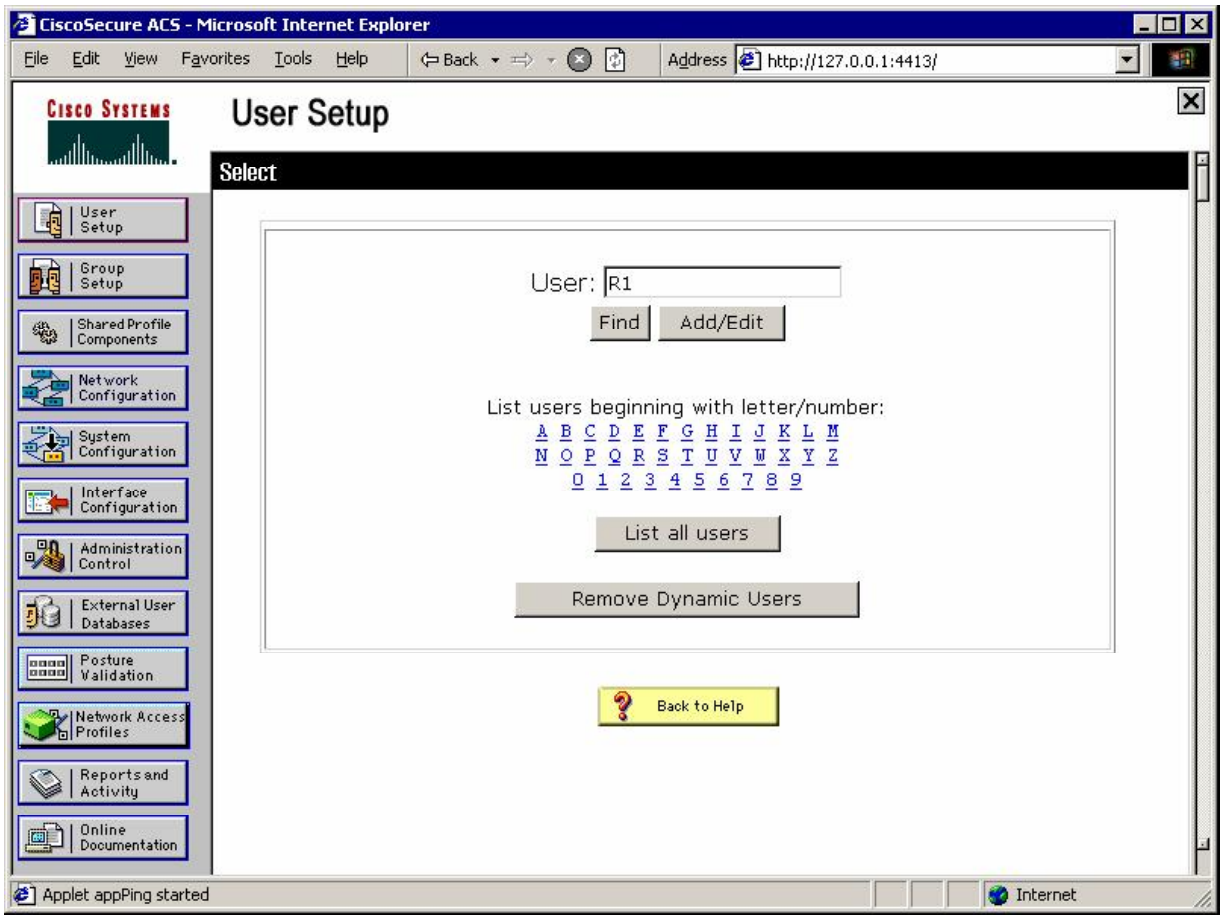
Configure IETF RADIUS attributes:

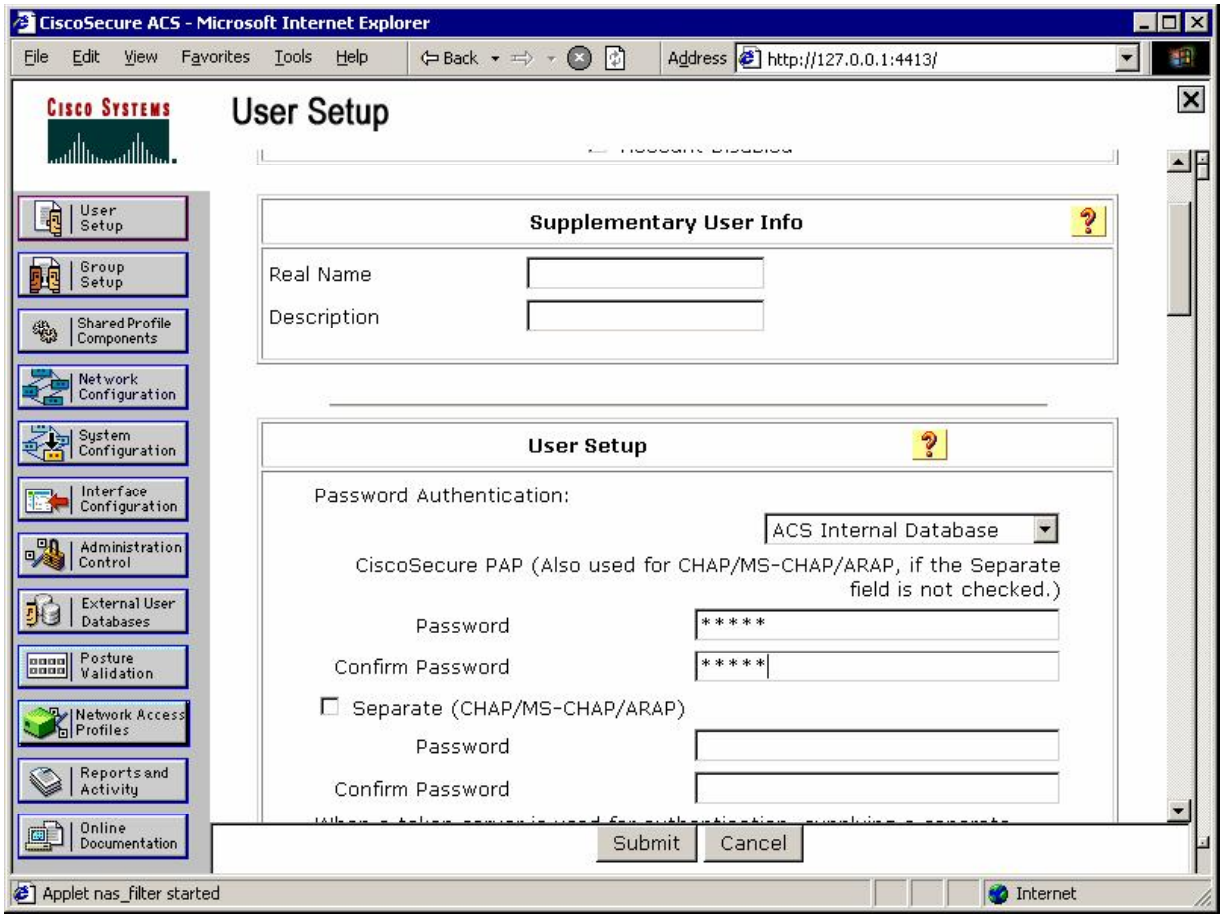


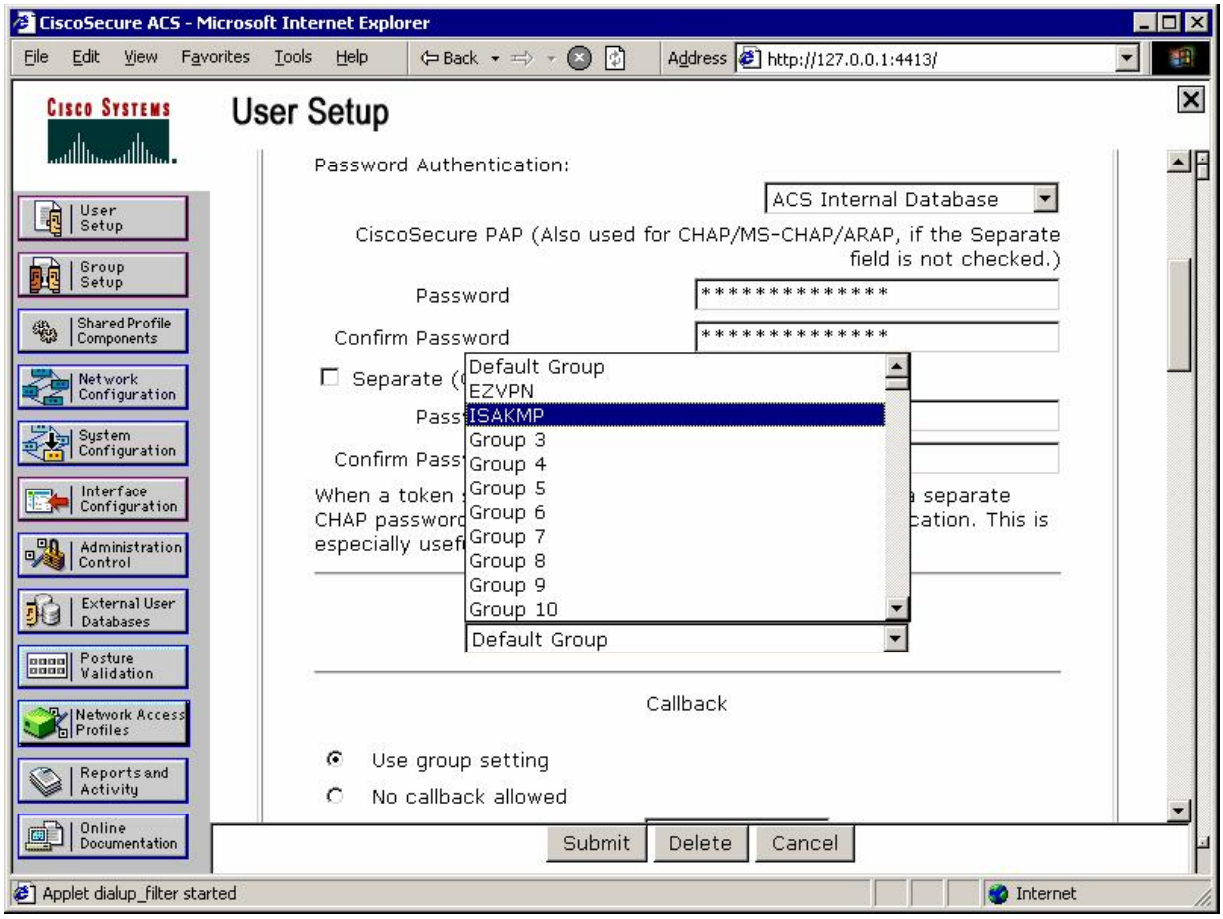

CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:4413/
Cisco Systems
Group Setup
Jump To RADIUS (IETF)
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
IETF RADIUS Attributes
[006] Service-Type
Outbound
[007] Framed-Protocol
Xylogics IPX/SLIP
[009] Framed-IP-Netmask
0.0.0.0
[010] Framed-Routing
None
[011] Filter-Id
[012] Framed-MTU (64..65535)
Submit
Submit + Restart
Cancel
Applet dialup_filter started
Internet


CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:4413/
Cisco Systems
Group Setup
Jump To RADIUS (IETF)
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
[062] Port-Limit
0
[063] Login-LAT-Port
[064] Tunnel-Type
Tag 1 Value IP ESP
Tag 2 Value
[065] Tunnel-Medium-Type
Tag 1 Value
Tag 2 Value
[069] Tunnel-Password
Tag 1 Value CISCO
Tag 2 Value
[081] Tunnel-Private-Group-ID
Submit
Submit + Restart
Cancel
Applet dialup_filter started
Internet

Add new user with name "R1" and password "cisco":




CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://127.0.0.1:4413/
Cisco Systems
User Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Supplementary User Info
Real Name
Description
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
*****
Confirm Password
*****
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
Submit
Cancel
Applet nas_filter started
Internet



Verification

```
R2#debug aaa authentication
AAA Authentication debugging is on
R2#debug radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
R2#deb aaa authorization
AAA Authorization debugging is on
R2#debug crypto isakmp
Crypto ISAKMP debugging is on

R1#ping 150.1.2.2 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/10/12 ms
```

```
R1#

*Mar  1 10:23:30.797: ISAKMP (0:0): received packet from 136.1.121.1 dport 500
sport 500 Global (N) NEW SA
*Mar  1 10:23:30.797: ISAKMP: Created a peer struct for 136.1.121.1, peer port
500
*Mar  1 10:23:30.797: ISAKMP: Locking peer struct 0x8291ACFC, IKE refcount 1
for crypto_ikmp_config_initialize_sa
*Mar  1 10:23:30.797: ISAKMP (0:0): Setting client config settings 82D89EB0
*Mar  1 10:23:30.797: ISAKMP: local port 500, remote port 500
*Mar  1 10:23:30.801: ISAKMP: insert sa successfully sa = 82BC5CA0
*Mar  1 10:23:30.801: ISAKMP (0:1): processing SA payload. message ID = 0
*Mar  1 10:23:30.801: ISAKMP (0:1): processing ID payload. message ID = 0
*Mar  1 10:23:30.801: ISAKMP (1): Process ID payload
        type         : 2
        FQDN name    : R1
        protocol     : 17
        port         : 0
        length       : 2
*Mar  1 10:23:30.801: ISAKMP (0:1): peer matches *none* of the profiles
```

R2 received aggressive-mode message with FQDN id of R1:

```
*Mar  1 10:23:30.805: ISAKMP (0:1): processing vendor id payload
*Mar  1 10:23:30.805: ISAKMP (0:1): vendor
R2#show de b ID seems Unity/DPD but major 157 mismatch
*Mar  1 10:23:30.805: ISAKMP (0:1): vendor ID is NAT-T v3
*Mar  1 10:23:30.805: ISAKMP (0:1): processing vendor id payload
*Mar  1 10:23:30.805: ISAKMP (0:1): vendor ID seems Unity/DPD but major 123
mismatch
*Mar  1 10:23:30.805: ISAKMP (0:1): vendor ID is NAT-T v2
*Mar  1 10:23:30.805: ISAKMP (0:1): Looking for a matching key for R1 in
default
*Mar  1 10:23:30.805: ISAKMP: no pre-shared key based on hostname R1!
*Mar  1 10:23:30.809: ISAKMP : Scanning profiles for xauth ...
*Mar  1 10:23:30.809: ISAKMP (0:1): Checking ISAKMP transform 1 against
priority 10 policy
*Mar  1 10:23:30.809: ISAKMP:      encryption 3DES-CBC
*Mar  1 10:23:30.809: ISAKMP:      hash MD5
*Mar  1 10:23:30.809: ISAKMP:      default group 1
*Mar  1 10:23:30.809: ISAKMP:      auth pre-share
*Mar  1 10:23:30.809: ISAKMP:      life type in seconds
*Mar  1 10:23:30.809: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Mar  1 10:23:30.813: ISAKMP (0:1): atts are acceptable. Next payload is 0
```

ISAKMP policy match found:

```
*Mar  1 10:23:30.982: ISAKMP (0:1): processing vendor id payload
*Mar  1 10:23:30.982: ISAKMP (0:1): vendor ID seems Unity/DPD but major 157
mismatch
*Mar  1 10:23:30.986: ISAKMP (0:1): vendor ID is NAT-T v3
*Mar  1 10:23:30.986: ISAKMP (0:1): processing vendor id payload
*Mar  1 10:23:30.986: ISAKMP (0:1): vendor ID seems Unity/DPD but major 123
mismatch
*Mar  1 10:23:30.986: ISAKMP (0:1): vendor ID is NAT-T v2
*Mar  1 10:23:30.986: ISAKMP (0:1): processing KE payload. message ID = 0
*Mar  1 10:23:31.194: ISAKMP (0:1): processing NONCE payload. message ID = 0
*Mar  1 10:23:31.198: ISAKMP (0:1): processing vendor id payload
*Mar  1 10:23:31.198: ISAKMP (0:1): vendor ID is DPD
*Mar  1 10:23:31.198: ISAKMP (0:1): processing vendor id payload
*Mar  1 10:23:31.198: ISAKMP (0:1): vendor ID seems Unity/DPD but major 242
mismatch
*Mar  1 10:23:31.202: ISAKMP (0:1): vendor ID is XAUTH
```

```
*Mar  1 10:23:31.202: ISAKMP (0:1): processing vendor id payload
*Mar  1 10:23:31.202: ISAKMP (0:1): vendor ID is Unity
*Mar  1 10:23:31.202: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
*Mar  1 10:23:31.202: AAA/MEMORY: create_user (0x82E8C6B8) user='R1'
ruser='NULL' ds0=0 port='ISAKMP-ID-AUTH' rem_addr='136.1.121.1'
authen_type=NONE service=LOGIN priv=0 initial_task_id='0', vrf= (id=0)
*Mar  1 10:23:31.206: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Mar  1 10:23:31.206: ISAKMP (0:1): Old State = IKE_READY  New State =
IKE_R_AM_AAA_AWAIT

*Mar  1 10:23:31.206: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877):
Port='ISAKMP-ID-AUTH' list='ISAKMP' service=NET
*Mar  1 10:23:31.206: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(3753740877)
user='R1'
*Mar  1 10:23:31.210: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877): send AV
service=ike
*Mar  1 10:23:31.210: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877): send AV
protocol=ipsec
*Mar  1 10:23:31.210: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877): found
list "ISAKMP"
*Mar  1 10:23:31.210: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877):
Method=radius (radius)
```

Next R2 queries RADIUS server to authorize incoming connection and obtain ISAKMP attributes:

```
*Mar  1 10:23:31.210: RADIUS: authenticating to get author data
*Mar  1 10:23:31.210: RADIUS: Pick NAS IP for u=0x82E8C6B8 tableid=0
cfg_addr=0.0.0.0 best_addr=136.1.122.2
*Mar  1 10:23:31.210: RADIUS: ustruct sharecount=3
*Mar  1 10:23:31.214: Radius: radius_port_info() success=0 radius_nas_port=1
```

R2 sends Access-Reques method with FQDN ID of R1 ans password "cisco" (default value, hardcoded):

```
*Mar  1 10:23:31.214: RADIUS(00000000): Send Access-Request to 10.0.0.100:1645
id 21645/5, len 73
*Mar  1 10:23:31.214: RADIUS:  authenticator 8D E0 1F 1A A6 0F 06 ED - 7F F5 4F
AD 18 04 93 3F
*Mar  1 10:23:31.218: RADIUS:  NAS-IP-Address      [4]   6   136.1.122.2
*Mar  1 10:23:31.218: RADIUS:  NAS-Port-Type       [61]  6   Async
[0]
*Mar  1 10:23:31.218: RADIUS:  User-Name           [1]   4   "R1"
*Mar  1 10:23:31.218: RADIUS:  Calling-Station-Id  [31]  13  "136.1.121.1"
*Mar  1 10:23:31.218: RADIUS:  User-Password       [2]   18  *
*Mar  1 10:23:31.218: RADIUS:  Service-Type        [6]   6   Outbound
[5]
```

Access-Accept with a set of attributes received:

```
*Mar  1 10:23:31.286: RADIUS: Received from id 21645/5 10.0.0.100:1645, Access-
Accept, len 108
*Mar  1 10:23:31.290: RADIUS:  authenticator E2 DC 27 9D C7 FF 16 72 - 71 FE 30
CC 6F 4C A8 42
*Mar  1 10:23:31.290: RADIUS:  Vendor, Cisco       [26]  30
```

Key-exchange protocol:

```
*Mar  1 10:23:31.290: RADIUS:   Cisco AVpair       [1]   24  "ipsec:key-
exchange=ike"
*Mar  1 10:23:31.290: RADIUS:  Service-Type        [6]   6   Outbound
[5]
```

Tunnel-type:

```
*Mar  1 10:23:31.290: RADIUS:  Tunnel-Type         [64]  6   01:ESP
[9]
```

Tunnel-password (pre-shared key actually):

```
*Mar  1 10:23:31.294: RADIUS:  Tunnel-Password     [69]  21  *
*Mar  1 10:23:31.294: RADIUS:  Class               [25]  25
*Mar  1 10:23:31.294: RADIUS:   43 41 43 53 3A 30 2F 35 63 61 63 2F 38 38 30 31
[CACS:0/5cac/8801]
*Mar  1 10:23:31.294: RADIUS:   37 61 30 32 2F 52 31
[7a02/R1]
*Mar  1 10:23:31.298: RADIUS: saved authorization data for user 82E8C6B8 at
8291AE94
*Mar  1 10:23:31.298: RADIUS: cisco AVPair "ipsec:key-exchange=ike"
*Mar  1 10:23:31.298: RADIUS: Tunnel-Type, [01] 00 00 09
*Mar  1 10:23:31.302: RADIUS: TAS(1) created and enqueued.
*Mar  1 10:23:31.302: RADIUS: Tunnel-Password decrypted, [01] CISCO
*Mar  1 10:23:31.302: RADIUS: TAS(1) takes precedence over tagged attributes,
tunnel_type=esp
*Mar  1 10:23:31.302: RADIUS: free TAS(1)
*Mar  1 10:23:31.302: AAA/AUTHOR (3753740877): Post authorization status =
PASS_ADD
*Mar  1 10:23:31.306: ISAKMP: got callback 1
*Mar  1 10:23:31.306:
AAA/AUTHOR/IKE: Processing AV service=ike
*Mar  1 10:23:31.306:
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
*Mar  1 10:23:31.306:
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
*Mar  1 10:23:31.306:
AAA/AUTHOR/IKE: Processing AV tunnel-type*esp
*Mar  1 10:23:31.306:
AAA/AUTHOR/IKE: Processing AV tunnel-password=CISCO
*Mar  1 10:23:31.310:
AAA/AUTHOR/IKE: Processing AV tunnel-tag*1
*Mar  1 10:23:31.310: ISAKMP (0:1): SKEYID state generated
*Mar  1 10:23:31.314: ISAKMP (0:1): constructed NAT-T vendor-03 ID
*Mar  1 10:23:31.314: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
```

Sending our ID, in this case – IP address:

```
*Mar  1 10:23:31.314: ISAKMP (1): ID payload
        next-payload : 10
        type         : 1
        addr         : 136.1.122.2
        protocol     : 17
        port         : 0
        length       : 8
*Mar  1 10:23:31.314: ISAKMP (1): Total payload length: 12
*Mar  1 10:23:31.318: ISAKMP (0:1): constructed HIS NAT-D
*Mar  1 10:23:31.318: ISAKMP (0:1): constructed MINE NAT-D
*Mar  1 10:23:31.318: ISAKMP (0:1): sending packet to 136.1.121.1 my_port 500
peer_port 500 (R) AG_INIT_EXCH
*Mar  1 10:23:31.318: ISAKMP (0:1): Input = IKE_MESG_FROM_AAA,
PRESHARED_KEY_REPLY
*Mar  1 10:23:31.322: ISAKMP (0:1): Old State = IKE_R_AM_AAA_AWAIT  New State =
IKE_R_AM2

*Mar  1 10:23:31.322: AAA/MEMORY: free_user (0x82E8C6B8) user='R1' ruser='NULL'
port='ISAKMP-ID-AUTH' rem_addr='136.1.121.1' authen_type=NONE service=LOGIN
```

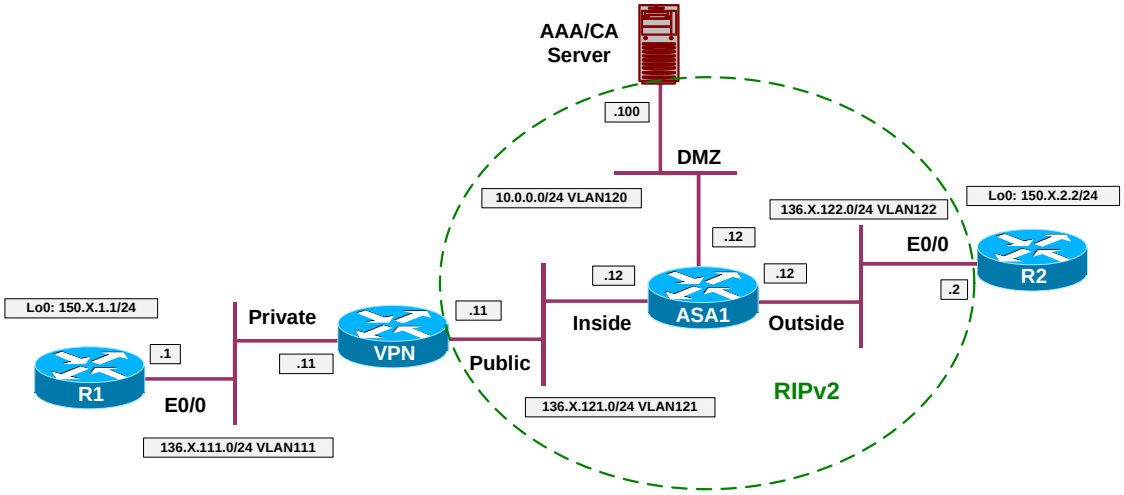
```
priv=0 vrf= (id=0)

*Mar  1 10:23:31.538: ISAKMP (0:1): received packet from 136.1.121.1 dport 500
sport 500 Global (R) AG_INIT_EXCH
*Mar  1 10:23:31.542: ISAKMP (0:1): processing HASH payload. message ID = 0
*Mar  1 10:23:31.542: ISAKMP:received payload type 17
*Mar  1 10:23:31.546: ISAKMP (0:1): Detected NAT-D payload
*Mar  1 10:23:31.546: ISAKMP (0:1): recalc my hash for NAT-D
*Mar  1 10:23:31.546: ISAKMP (0:1): NAT match MINE hash
*Mar  1 10:23:31.546: ISAKMP:received payload type 17
*Mar  1 10:23:31.546: ISAKMP (0:1): Detected NAT-D payload
*Mar  1 10:23:31.546: ISAKMP (0:1): recalc his hash for NAT-D
*Mar  1 10:23:31.546: ISAKMP (0:1): NAT match HIS hash
*Mar  1 10:23:31.546: ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol
1
        spi 0, message ID = 0, sa = 82BC5CA0
*Mar  1 10:23:31.546: ISAKMP (0:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local 136.1.122.2 remote
136.1.121.1 remote port 500
*Mar  1 10:23:31.550: ISAKMP (0:1): returning IP addr to the address pool
*Mar  1 10:23:31.550: ISAKMP (0:1): SA has been authenticated with 136.1.121.1
```

📖 Further Reading

Configuring IKE Shared Secret Using AAA Server
IKE: Initiate Aggressive Mode

IPsec NAT-T: L2L Tunnel with VPN3k and IOS Box

Objective: Configure IPsec L2L tunnel between IOS and VPN3k across the NAT.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and VPN3k with PSK".
- The way we are going to change scenario is to make VPN3k to connect to R2 across the PAT configuration on the ASA.
- This way only VPN3k is able to initiate connection to R2.
- Enable NAT-control on the ASA, and translate inside network 136.1.121.0/24 using the outside IP address of the firewall.
- Re-configure IPsec L2L tunnel on R2:
  - Change pre-shared key to match outside IP address of the firewall: 136.1.122.12
  - Create dynamic crypto-map DYNAMIC:
    - Set transform-set 3DES_MD5.
    - Match address LO2_TO_LO1.
  - Detach crypto-map VPN from interface E0/0 and delete it.
  - Create crypto map VPN and attach dynamic crypt-map DYNAMIC to it.
  - Apply crypto map VPN to interface E0/0.
- VPN3k:
  - Re-configure LAN-to-LAN tunnel "VPN_TO_R2":
    - Set tunnel type to initiate-only
    - Enable NAT-T in tunnel settings
  - Enable NAT-T globally

Final Configuration

ASA1:

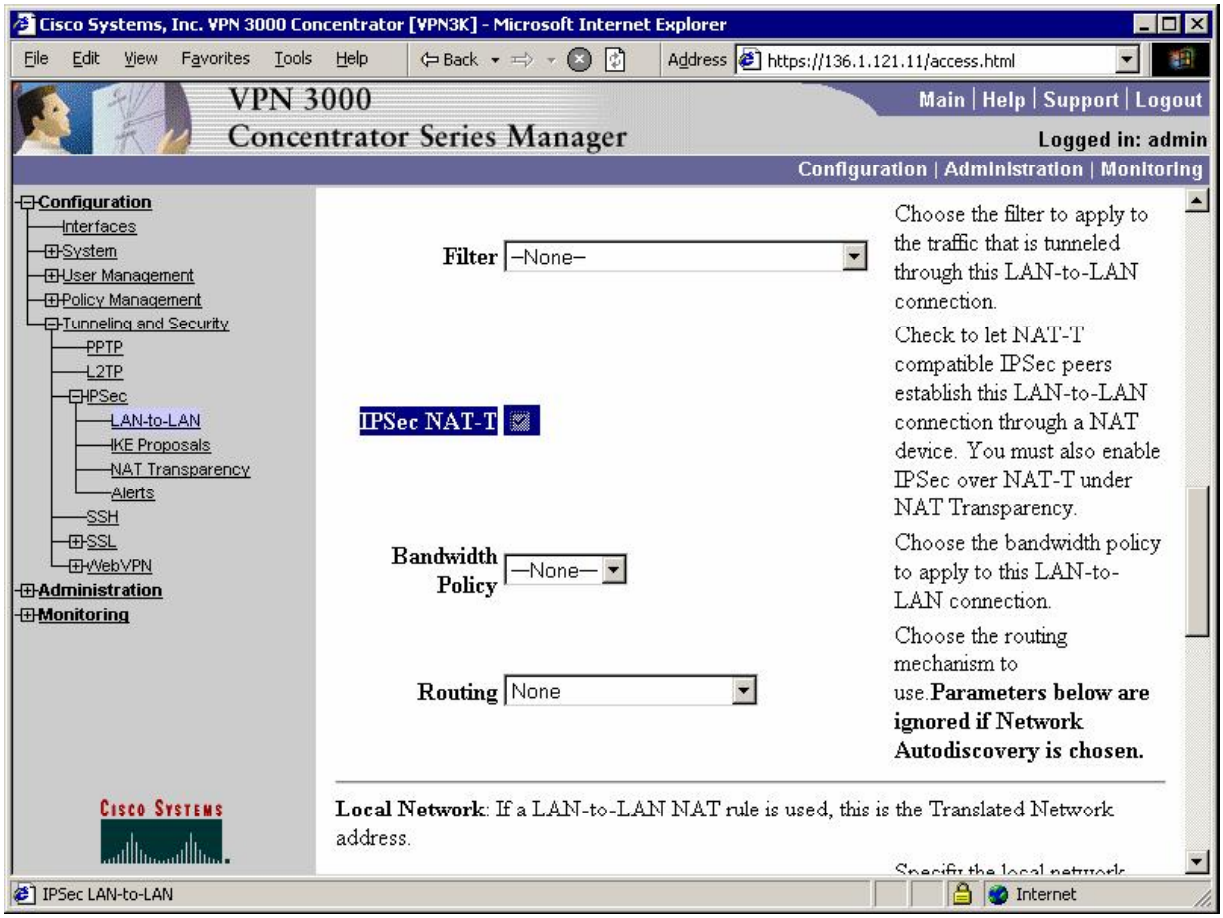
```
nat-control
nat (inside) 1 136.1.121.0 255.255.255.0
global (outside) 1 interface
!
! Static NAT to manage VPN3k
!
static (i,dmz) 136.1.121.11 136.1.121.11
```

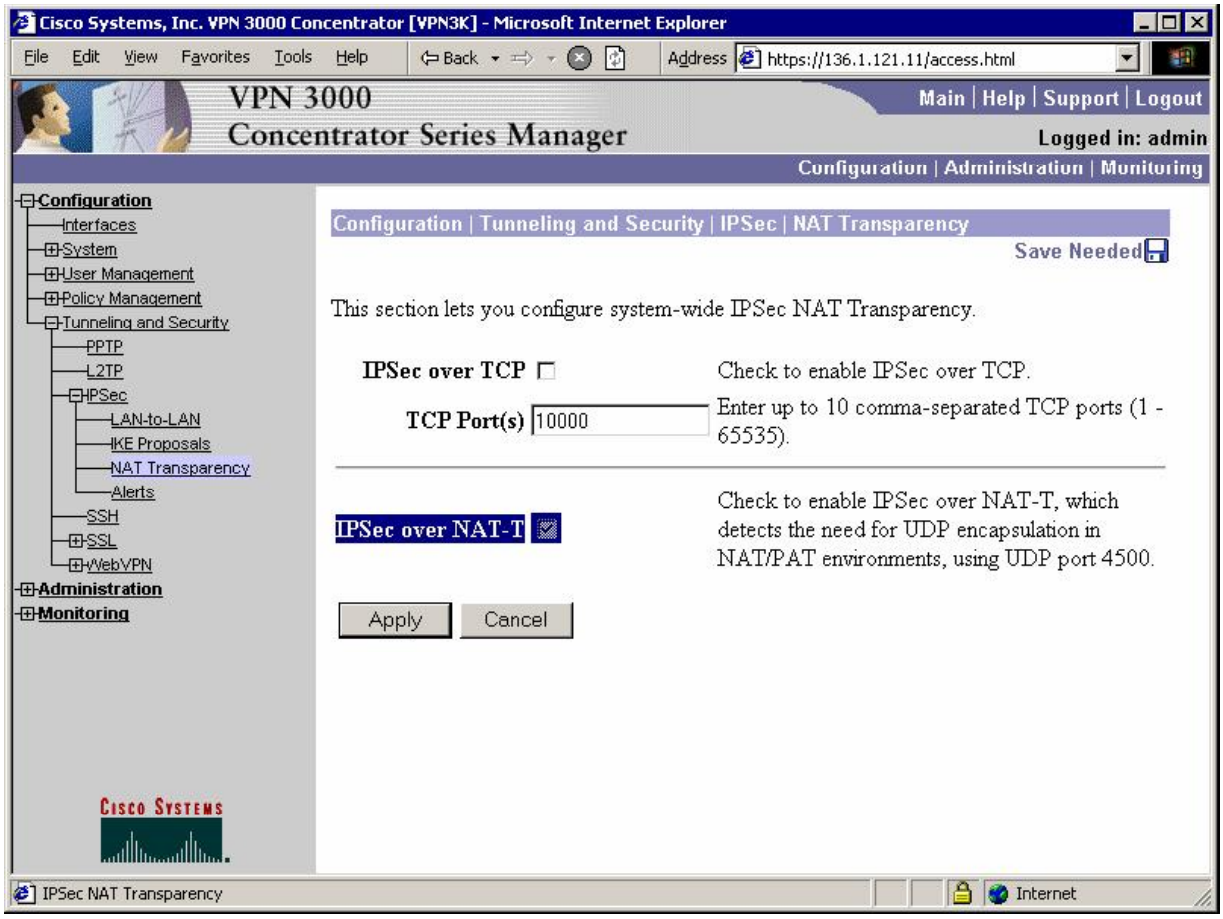
R2:

```
no crypto isakmp key CISCO address 136.1.121.11
crypto isakmp key CISCO address 136.1.122.12
!
! Delete existing crypto-map
!
interface E 0/0
 no crypto map VPN
!
no crypto map VPN
!
! Create dynamic crypto-map
!
crypto dynamic-map DYNAMIC 10
 set transform-set 3DES_MD5
 match address LO2_TO_LO1
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
!
! Apply new crypto-map
!
interface E0/0
 crypto map VPN
```


VPN3k GUI:

Modify settings for L2L tunnel "VPN_TO_R2":





Verification

```
R1#ping 150.1.2.2 so lo 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms

R2#debug crypto isakmp
Crypto ISAKMP debugging is on

<output omitted>

*Mar  1 22:50:31.399: ISAKMP (0:4): processing SA payload. message ID = 0
*Mar  1 22:50:31.399: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:31.399: ISAKMP (0:4): vendor ID seems Unity/DPD but major 123
mismatch
*Mar  1 22:50:31.399: ISAKMP (0:4): vendor ID is NAT-T v2
*Mar  1 22:50:31.399: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:31.399: ISAKMP (0:4): vendor ID seems Unity/DPD but major 157
mismatch
*Mar  1 22:50:31.399: ISAKMP (0:4): vendor ID is NAT-T v3
*Mar  1 22:50:31.399: ISAKMP (0:4): processing vendor id payload
```

```
*
R2#Mar  1 22:50:31.403: ISAKMP (0:4): vendor ID seems Unity/DPD but major 194
mismatch
*Mar  1 22:50:31.403: ISAKMP: Looking for a matching key for 136.1.122.12 in
default : success
*Mar  1 22:50:31.403: ISAKMP (0:4): found peer pre-shared key matching
136.1.122.12
*Mar  1 22:50:31.403: ISAKMP (0:4) local preshared key found
*Mar  1 22:50:31.403: ISAKMP : Scanning profiles for xauth ...
*Mar  1 22:50:31.403: ISAKMP (0:4): Checking ISAKMP transform 1 against
priority 10 policy
*Mar  1 22:50:31.403: ISAKMP:      encryption 3DES-CBC
*Mar  1 22:50:31.407: ISAKMP:      hash MD5
*Mar  1 22:50:31.407: ISAKMP:      default group 2
*Mar  1 22:50:31.407: ISAKMP:      auth pre-share
*Mar  1 22:50:31.407: ISAKMP:      life type in seconds
*Mar  1 22:50:31.407: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Mar  1 22:50:31.407: ISAKMP (0:4): atts are acceptable. Next payload is 0
*Mar  1 22:50:31.683: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:31.687: ISAKMP (0:4): vendor ID seems Unity/DPD but major 123
mismatch
*Mar  1 22:50:31.687: ISAKMP (0:4): vendor ID is NAT-T v2
*Mar  1 22:50:31.687: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:31.687: ISAKMP (0:4): vendor ID seems Unity/DPD but major 157
mismatch
*Mar  1 22:50:31.687: ISAKMP (0:4): vendor ID is NAT-T v3
*Mar  1 22:50:31.687: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:31.687: ISAKMP (0:4): vendor ID seems Unity/DPD but major 194
mismatch
*Mar  1 22:50:31.691: ISAKMP (0:4): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Mar  1 22:50:31.691: ISAKMP (0:4): Old State = IKE_R_MM1  New State =
IKE_R_MM1

*Mar  1 22:50:31.699: ISAKMP (0:4): constructed NAT-T vendor-03 ID
*Mar  1 22:50:31.699: ISAKMP (0:4): sending packet to 136.1.122.12 my_port 500
peer_port 2 (R) MM_SA_SETUP
*Mar  1 22:50:31.699: ISAKMP (0:4): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Mar  1 22:50:31.703: ISAKMP (0:4): Old State = IKE_R_MM1  New State =
IKE_R_MM2

*Mar  1 22:50:31.811: ISAKMP (0:4): received packet from 136.1.122.12 dport 500
sport 2 Global (R) MM_SA_SETUP
*Mar  1 22:50:31.815: ISAKMP (0:4): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Mar  1 22:50:31.815: ISAKMP (0:4): Old State = IKE_R_MM2  New State =
IKE_R_MM3

*Mar  1 22:50:31.819: ISAKMP (0:4): processing KE payload. message ID = 0
*Mar  1 22:50:32.156: ISAKMP (0:4): processing NONCE payload. message ID = 0
*Mar  1 22:50:32.168: ISAKMP: Looking for a matching key for 136.1.122.12 in
default : success
*Mar  1 22:50:32.172: ISAKMP (0:4): found peer pre-shared key matching
136.1.122.12
*Mar  1 22:50:32.172: ISAKMP (0:4): SKEYID state generated
*Mar  1 22:50:32.176: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:32.176: ISAKMP (0:4): vendor ID is Unity
*Mar  1 22:50:32.176: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:32.176: ISAKMP (0:4): vendor ID seems Unity/DPD but major 39
mismatch
*Mar  1 22:50:32.176: ISAKMP (0:4): vendor ID is XAUTH
*Mar  1 22:50:32.176: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:32.180: ISAKMP (0:4): speaking to another IOS box!
```

```
*Mar  1 22:50:32.180: ISAKMP (0:4): processing vendor id payload
*Mar  1 22:50:32.180: ISAKMP (0:4): vendor ID seems Unity/DPD but major 4
mismatch
*Mar  1 22:50:32.180: ISAKMP:received payload type 17
*Mar  1 22:50:32.180: ISAKMP (0:4): Detected NAT-D payload
*Mar  1 22:50:32.180: ISAKMP (0:4): NAT match MINE hash
*Mar  1 22:50:32.180: ISAKMP:received payload type 17
*Mar  1 22:50:32.180: ISAKMP (0:4): Detected NAT-D payload
*Mar  1 22:50:32.184: ISAKMP (0:4): NAT does not match HIS hash
*Mar  1 22:50:32.184: hash received: E8 A0 28 25 68 19 1D CB A9 A9 12 CD 33 18
D7 E
*Mar  1 22:50:32.184: his nat hash : D 74 46 B9 F4 14 42 22 B5 7F 97 AD 5C 98 C
EC
*Mar  1 22:50:32.188: ISAKMP (0:4): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Mar  1 22:50:32.188: ISAKMP (0:4): Old State = IKE_R_MM3  New State =
IKE_R_MM3

R2#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.122.12:1025
     PERMIT, flags={}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 21
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.122.12
     path mtu 1500, media mtu 1500
     current outbound spi: 49FC5761

     inbound esp sas:
      spi: 0xC8A87211(3366482449)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4414001/2862)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x49FC5761(1241274209)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4414004/2862)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
```

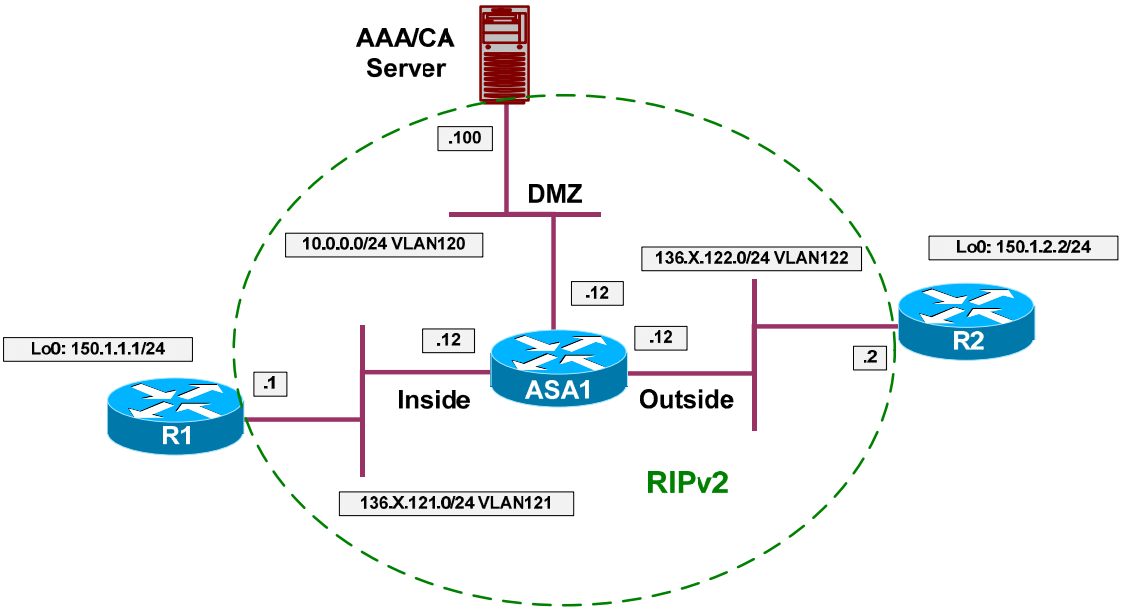
```
     outbound pcp sas:

ASA1(config)# show xlate
2 in use, 4 most used
Global 136.1.121.11 Local 136.1.121.11
PAT Global 136.1.122.12(1025) Local 136.1.121.11(4500)

ASA1(config)# show conn
7 in use, 98 most used
TCP out 10.0.0.100:2415 in 136.1.121.11:443 idle 0:00:40 bytes 1205 flags UIOB
UDP out 136.1.122.2:4500 in 136.1.121.11:4500 idle 0:00:02 flags -
```

Further Reading

Configuring NAT Transparent Mode for IPSec on the VPN 3000 Concentrator

IKE Tunnel Endpoint Discovery (TED)

Objective: Configure IOS routers for tunnel end-point discovery.



Directions

- Configure devices as per the "VPN/IPsec LAN-to-LAN" scenario "IOS and IOS with PSK across the PIX/ASA".
- Detach crypto map VPN from Ethernet interfaces. Delete crypto map VPN.
- Create dynamic crypto map DISCOVER on R1 and R2:
  - Match access-list LO1_TO_LO2 and LO2_TO_LO1 respectively.
  - Set transform-set 3DES_MD5
- Create crypto map VPN entry 10 of type IPsec-ISAKMP:
  - Attach dynamic crypto-map DISCOVER and enable peer IP discovery.
- Apply crypto map VPN to ethernet interfaces.

Final Configuration

```
R1:
!
! Delete existing crypto map
!
interface E0/0
  no crypto map VPN
  exit
!
no crypto map VPN
!
! Create dynamic crypto map
!
crypto dynamic-map DISCOVER 10
  match address LO1_TO_LO2
```

```
  set transform-set 3DES_MD5
!
! Enable TED
!
crypto map VPN 10 ipsec-isakmp dynamic DISCOVER discover
!
! Apply crypto map to the interface
!
interface E0/0
  crypto map VPN
```

R2:

```
!
! Delete existing crypto map
!
interface E0/0
  no crypto map VPN
  exit
!
no crypto map VPN
!
! Create dynamic crypto map
!
crypto dynamic-map DISCOVER 10
  match address LO2_TO_LO1
  set transform-set 3DES_MD5
!
crypto map VPN 10 ipsec-isakmp dynamic DISCOVER discover
!
! Apply crypto map to the interface
!
interface E0/0
  crypto map VPN
```

Verification

```
R1#debug crypto isakmp
Crypto ISAKMP debugging is on

R1#ping 150.1.2.2 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/20 ms

*Mar  1 12:35:08.364: ISAKMP: received ke message (1/1)
*Mar  1 12:35:08.364: ISAKMP: GOT A PEER DISCOVERY MESSAGE FROM THE SA
MANAGER!!!
*Mar  1 12:35:08.364: src = 150.1.1.1 to 150.1.2.2, protocol 3, transform 3,
hmac 1
*Mar  1 12:35:08.364: proxy source is 150.1.1.0/255.255.255.0 and my address
(not used now) is 136.1.121.1
*Mar  1 12:35:08.368: ISAKMP (0:0): no idb in request
*Mar  1 12:35:08.368: ISAKMP (0:0): SA request profile is (NULL)
*Mar  1 12:35:08.368: ISAKMP: local port 500, remote port 500
*Mar  1 12:35:08.372: ISAKMP: set new node 0 to QM_IDLE
*Mar  1 12:35:08.372: ISAKMP: Find a dup sa in the avl tree during calling
isadb_insert sa = 82E2EF64
```

```
*Mar  1 12:35:08.372: ISAKMP (0:19): SA is doing unknown authentication!
*Mar  1 12:35:08.372: ISAKMP (19): ID payload
        next-payload : 5
        type         : 1
        addr         : 136.1.121.1
        protocol     : 17
        port         : 500
        length       : 8
*Mar  1 12:35:08.372: ISAKMP (19): Total payload length: 12
*Mar  1 12:35:08.376: 1st ID is 136.1.121.1
*Mar  1 12:35:08.376: 2nd ID is 150.1.1.0/255.255.255.0
*Mar  1 12:35:08.376: ISAKMP (0:19): Input = IKE_MESG_FROM_IPSEC, IKE_TED_REQ
*Mar  1 12:35:08.376: ISAKMP (0:19): Old State = IKE_READY  New State =
IKE_I_TED_RESP

*Mar  1 12:35:08.376: ISAKMP (0:19): beginning peer discovery exchange
*Mar  1 12:35:08.376: ISAKMP (0:19): sending packet to 150.1.2.2 my_port 500
peer_port 500 (I) PEER_DISCOVERY via Ethernet0/0:136.1.121.12
*Mar  1 12:35:08.396: ISAKMP (0:19): received packet from 136.1.122.2 dport 500
sport 500 Global (I) PEER_DISCOVERY
*Mar  1 12:35:08.400: ISAKMP (0:19): processing vendor id payload
*Mar  1 12:35:08.400: ISAKMP (0:19): speaking to another IOS box!
*Mar  1 12:35:08.400: ISAKMP (0:19): processing ID payload. message ID = 0
*Mar  1 12:35:08.400: ISAKMP:received payload type 16
*Mar  1 12:35:08.400: ISAKMP (0:19): received response to my peer discovery
probe!
*Mar  1 12:35:08.404: ISAKMP (0:19): ted negotiated proxies: 0
150.1.1.0/255.255.255.0:0, 150.1.2.0/255.255.255.0:0
*Mar  1 12:35:08.404: ISAKMP (0:19): initiating IKE to 136.1.122.2 in response
to probe.

R1# show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
20    136.1.121.1     136.1.122.2              3des md5  psk  1  23:53:14

R1#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.121.1

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.122.2:500
     PERMIT, flags={}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.122.2
     path mtu 1500, media mtu 1500
     current outbound spi: A1315146

     inbound esp sas:
```

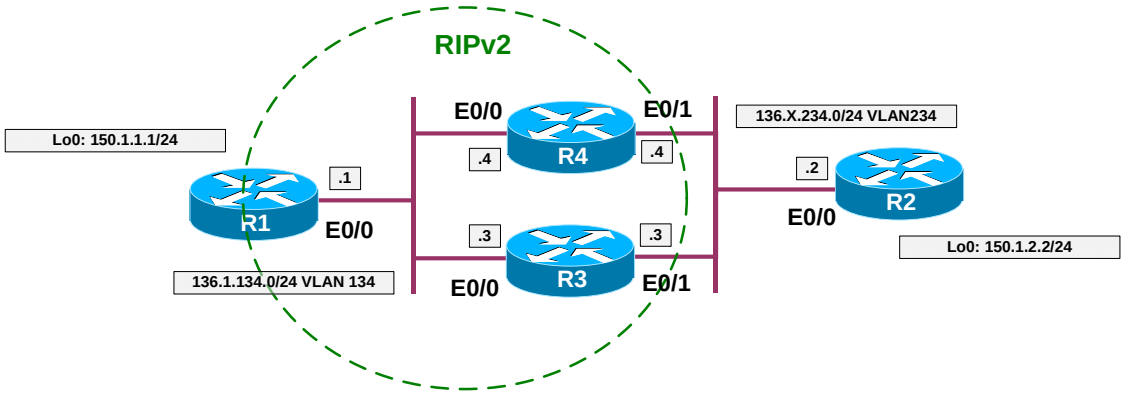
```
 spi: 0xCE62E629(3462587945)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4418894/3170)
   IV size: 8 bytes
   replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0xA1315146(2704363846)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4418894/3170)
   IV size: 8 bytes
   replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

Further Reading

Configuring IPSec Tunnel End-Point Discovery

IPsec VPN High-Availability with HSRP

Objective: Configure IPsec tunnel high-availability using HSRP.



Directions

- Pre-configuration steps:
  - Create necessary VLANs on SW1 & SW2, and configure trunk ports.
  - Configure IP addressing as per the diagram.
  - Configure RIP as routing protocol on R2, R3, and R4.
  - Configure HSRP on R3, R4 VLAN 234 (interfaces E0/0):
    - Use virtual IP 136.X.234.254
    - Use HSRP name HSRP1
    - Configure preemption.
    - Track interface E0/1.
    - R3 should be primary.
  - Configure static default route to 136.X.234.254 on R2.
- The idea behind the high-availability is to use HSRP virtual IP address for IPsec tunnel establishment. Whether one of peers fails, the other will automatically take the active role.
- IPsec HA Configuration:
  - Configure ISAKMP policy on R2, R3, R4:
    - Use 3DES cipher.
    - Use MD5 hash.
    - Use Pre-shared keys for authentication.
  - Set ISAKMP keepalive interval to minimum value.
  - Create pre-shared keys on R3 and R4 for IP address 136.X.234.2 of R2.
  - Create pre-shared key on R2 for HSRP virtual IP address 136.X.234.254
  - Create transform-set 3DES_MD5 on R3, R4, and R2.
    - Use 3DES cipher.
    - Use MD5 hash.
  - Create access-list R1_TO_R2 on R3 and R4:

        - Match IP traffic from 150.1.1.0/24 to 150.1.2.0/24.
    - Create access-list R2_TO_R1 on R2:
        - Match IP traffic from 150.1.2.0/24 to 150.1.1.0/24.
    - On R3 and R4 create crypto map VPN entry 10, type IPsec ISAKMP:
        - Match IP address R1_TO_R2.
        - Set peer 136.X.234.2
        - Set transform-set 3DES_MD5.
        - Enable RRI
    - Assign crypto map VPN to interface E0/1 on R3 and R4 and attach it to HSRP group HSRP1.
    - On R3 and R4 redistribute static subnets into RIP.
    - On R2 create crypto map VPN entry 10 type IPsec-ISAKMP:
        - Match IP address R2_TO_R1.
        - Set peer 136.X.234.254
        - Set transform-set 3DES_MD5.
    - Set up RIP timers on R1, R3, and R4 for faster convergence. Divide all timers by value of ten.

Final Configuration

```
Pre-Configuration:

SW1 & SW2:
vlan 234,134
!
interface range Fa 0/21 - 23
 no shut
 switchport trunk encaps dot1q
 switchport mode trunk

SW1:
interface Fa 0/1
  switchport mode access
  switchport access vlan 134
!
interface Fa 0/2
  switchport mode access
  switchport access vlan 234
!
interface Fa 0/3
  switchport mode access
  switchport access vlan 134
!
interface Fa 0/4
  switchport mode access
  switchport access vlan 134

SW2:
interface Fa 0/3
  switchport mode access
  switchport access vlan 234
!
interface Fa 0/4
  switchport mode access
```

```
  switchport access vlan 234
```

R1:

```
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
interface E 0/0
 ip address 136.1.134.1 255.255.255.0
 no shutdown
!
router rip
  ver 2
  no auto
  network 136.1.0.0
  network 150.1.0.0
```

R2:

```
interface Loopback0
 ip address 150.1.2.2 255.255.255.0
!
interface E 0/0
 ip address 136.1.234.2 255.255.255.0
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 136.1.234.254
```

R3:

```
interface E 0/0
 ip address 136.1.134.3 255.255.255.0
 no shutdown
!
! Configure HSRP
!
interface E 0/1
 ip address 136.1.234.3 255.255.255.0
 standby 1 ip 136.1.234.254
 standby 1 preempt
 standby 1 track E 0/0 20
 standby 1 priority 110
 standby 1 name HSRP1
 no shutdown
!
router rip
  ver 2
  no auto
  network 136.1.0.0
  network 150.1.0.0
```

R4:

```
interface E 0/0
 ip address 136.1.134.4 255.255.255.0
 no shutdown
!
! Configure HSRP
!
interface E 0/1
 ip address 136.1.234.4 255.255.255.0
 standby 1 ip 136.1.234.254
 standby 1 preempt
 standby 1 name HSRP1
 no shutdown
!
router rip
```

```
  ver 2
  no auto
  network 136.1.0.0
  network 150.1.0.0
```

R3 & R4:

```
crypto isakmp policy 10
 auth pre
 hash md5
 encr 3des
!
! Configure pre-shared key
!
crypto isakmp key CISCO address 136.1.234.2
!
! Shorten keepalive interval
!
crypto isakmp keepalive 10
!
! Configure access-list to match traffic
!
ip access-list ext R1_TO_R2
  permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
!
! Create transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Configure crypto map with RRI
!
crypto map VPN 10 ipsec-isakmp
  match address R1_TO_R2
  set transform 3DES_MD5
  set peer 136.1.234.2
  reverse
!
! Apply crypto-map and enable redundancy
!
interface E0/1
  crypto map VPN redundancy HSRP1
!
! Redistribute static routes from RRI
!
router rip
 redistribute static
```

R2:

```
crypto isakmp policy 10
 auth pre
 hash md5
 encr 3des
!
!
!
crypto isakmp key CISCO address 136.1.234.254
!
!
!
crypto isakmp keepalive 10
!
!
!
ip access-list ext R2_TO_R1
```

```
  permit ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
!
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
!
!
crypto map VPN 10 ipsec-isakmp
  match address R2_TO_R1
  set transform 3DES_MD5
  set peer 136.1.234.254
!
!
!
interface E0/0
  crypto map VPN
```

Tune up RIP convergence:

R1, R3, R4:

```
router rip
 timers basic 3 18 18 24
```

Verification

Primary path:

```
R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/12/12 ms

R2#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.234.254   136.1.234.2     QM_IDLE              1    0

R2#show crypto ips sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.234.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.234.254:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 136.1.234.2, remote crypto endpt.: 136.1.234.254
     path mtu 1500, media mtu 1500
```

```
     current outbound spi: ABB177EC

     inbound esp sas:
      spi: 0x6BBA47F9(1807370233)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4499195/3565)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xABB177EC(2880534508)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4499195/3565)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

R3#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.234.254   136.1.234.2     QM_IDLE              1    0

R3#show crypto ipsec sa

interface: Ethernet0/1
    Crypto map tag: VPN, local addr. 136.1.234.254

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.234.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.234.254, remote crypto endpt.: 136.1.234.2
     path mtu 1500, media mtu 1500
     current outbound spi: 6BBA47F9

     inbound esp sas:
      spi: 0xABB177EC(2880534508)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4604708/3508)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
```

```
     inbound pcp sas:

     outbound esp sas:
      spi: 0x6BBA47F9(1807370233)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4604708/3508)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

R3#show standby
Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:31:02
  Virtual IP address is 136.1.234.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.333 secs
  Preemption enabled
  Active router is local
  Standby router is 136.1.234.4, priority 100 (expires in 9.523 sec)
  Priority 110 (configured 110)
    Track interface Ethernet0/0 state Up decrement 20
  IP redundancy name is "HSRP1" (cfgd)

R3#show cry map tag VPN
Redundancy Group: HSRP1

Crypto Map "VPN" 10 ipsec-isakmp
        Peer = 136.1.234.2
        Extended IP access list R1_TO_R2
            access-list R1_TO_R2 permit ip 150.1.1.0 0.0.0.255 150.1.2.0
0.0.0.255
        Current peer: 136.1.234.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                3DES_MD5,
        }
        Reverse Route Injection Enabled
        Interfaces using crypto map VPN:
                Ethernet0/1

R1#show ip route rip
     136.1.0.0/24 is subnetted, 2 subnets
R       136.1.234.0 [120/1] via 136.1.134.3, 00:00:07, Ethernet0/0
                    [120/1] via 136.1.134.4, 00:00:24, Ethernet0/0
     150.1.0.0/24 is subnetted, 2 subnets
R       150.1.2.0 [120/1] via 136.1.134.3, 00:00:07, Ethernet0/0

Shutdown E0/0 on R3 to make primary path fail:

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface ethernet 0/0
R3(config-if)#shut
```

```
R3#show standby
Ethernet0/1 - Group 1
  State is Standby
    4 state changes, last state change 00:00:29
  Virtual IP address is 136.1.234.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.836 secs
  Preemption enabled
  Active router is 136.1.234.4, priority 100 (expires in 9.836 sec)
  Standby router is local
  Priority 90 (configured 110)
    Track interface Ethernet0/0 state Down decrement 20
  IP redundancy name is "HSRP1" (cfgd)

R2#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.234.254   136.1.234.2     MM_NO_STATE          1    0 (deleted)

R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/12/12 ms

R4#show crypto isakmp sa
dst             src             state          conn-id slot
136.1.234.254   136.1.234.2     QM_IDLE              1    0

R4#show cry ips sa

interface: Ethernet0/1
    Crypto map tag: VPN, local addr. 136.1.234.254

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.234.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.234.254, remote crypto endpt.: 136.1.234.2
     path mtu 1500, media mtu 1500
     current outbound spi: 30B73525

     inbound esp sas:
      spi: 0x7AAA7507(2057991431)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4472014/3552)
        IV size: 8 bytes
        replay detection support: Y
```

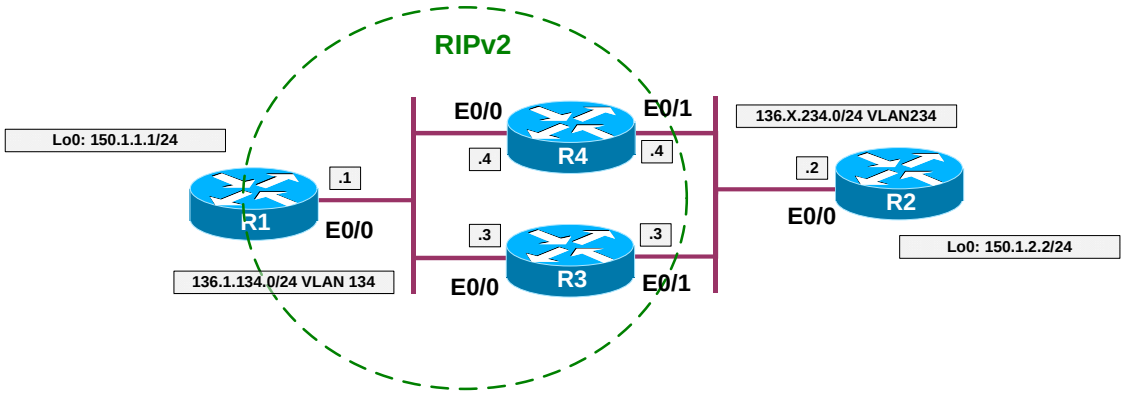
```
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x30B73525(817313061)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4472014/3552)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

R1#show ip route rip
     136.1.0.0/24 is subnetted, 2 subnets
R       136.1.234.0 [120/1] via 136.1.134.4, 00:00:02, Ethernet0/0
     150.1.0.0/24 is subnetted, 2 subnets
R       150.1.2.0 [120/1] via 136.1.134.4, 00:00:02, Ethernet0/0
```

Further Reading

IPsec High Availability

IPsec High Availability with NAT and HSRP

Objective: Configure IPsec tunnel across NAT enabling bi-directional tunnel initiation.



Directions

- Configure devices as per the scenario "VPN/Advanced Topics" "IPsec High Availability with HSRP".
- Remove IPsec configuration from R3/R4.
- Configure NAT on R3 and R4:
  - Make E0/1 outside interface and E0/0 inside
  - Configure static mapping for IP 136.X.134.1 to 136.X.234.1 with redundancy via HSRP group HSRP1.
- Re-configure IPsec on R2 to use peer IP address 136.X.234.1. Re-configure ISAKMP key accordingly.
- Configure IPsec on R1:
  - Configure ISAKMP policy:
    - Use pre-shared keys for authentication.
    - Use 3DES cipher.
    - Use MD5 hash.
  - Configure ISAKMP pre-shared key for IP address 136.X.234.2
  - Create IPsec transform-set 3DES_MD5:
    - Use 3DES cipher.
    - Use MD5 hash.
  - Create dynamic crypto map DYNAMIC entry 10
    - Apply transform-set 3DES_MD5
    - Enable RRI
  - Create crypto map VPN entry 10 and attach dynamic crypto map DYNAMIC.
  - Apply crypto-map VPN to interface E0/0.

Final Configuration

```
R3 & R4:
interface E0/1
  no crypto map VPN
!
! Static NAT mapping with HSRP redundancy support
!
ip nat inside source static 136.1.134.1 136.1.234.1 red HSRP1
!
inter E0/1
 ip nat outside
!
inter E0/0
 ip nat inside

R2:
crypto map VPN 10
 no set peer 136.1.234.254
 set peer 136.1.234.1
!
! Change ISAKMP peer IP address
!
crypto isakmp key CISCO addr 136.1.234.1

R1:
crypto isakmp policy 10
 auth pre
 hash md5
 encr 3des
!
crypto isakmp key CISCO addr 136.1.234.2
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5
!
crypto dynamic-map DYNAMIC 10
 set transform 3DES_MD5
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
!
interface E0/0
  crypto map VPN
```

Verification

```
R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/16 ms

R3#show standby
Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:09:59
  Virtual IP address is 136.1.234.254
```

```
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.880 secs
  Preemption enabled
  Active router is local
  Standby router is 136.1.234.4, priority 100 (expires in 8.874 sec)
  Priority 110 (configured 110)
    Track interface Ethernet0/0 state Up decrement 20
  IP redundancy name is "HSRP1" (cfgd)

R2#sho ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  136.1.234.3           187   0050.5476.4101  ARPA   Ethernet0/0
Internet  136.1.234.2             -   0003.e335.1240  ARPA   Ethernet0/0
Internet  136.1.234.1            14   0050.5476.4101  ARPA   Ethernet0/0
Internet  136.1.234.4           187   0050.8004.8b61  ARPA   Ethernet0/0
Internet  136.1.234.254          15   0000.0c07.ac01  ARPA   Ethernet0/0

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface ethernet 0/0
R3(config-if)#shutdown

136.1.234.1 ARP entry was replaced by gratituous ARP from R4:

R2#sho ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  136.1.234.3           189   0050.5476.4101  ARPA   Ethernet0/0
Internet  136.1.234.2             -   0003.e335.1240  ARPA   Ethernet0/0
Internet  136.1.234.1             0   0050.8004.8b61  ARPA   Ethernet0/0
Internet  136.1.234.4           189   0050.8004.8b61  ARPA   Ethernet0/0
Internet  136.1.234.254           0   0000.0c07.ac01  ARPA   Ethernet0/0

R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms

No IPsec re-negotiation took place since IPsec endpoint neve changed.

R2#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.234.2

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.234.1:4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 136.1.234.2, remote crypto endpt.: 136.1.234.1
     path mtu 1500, media mtu 1500
```

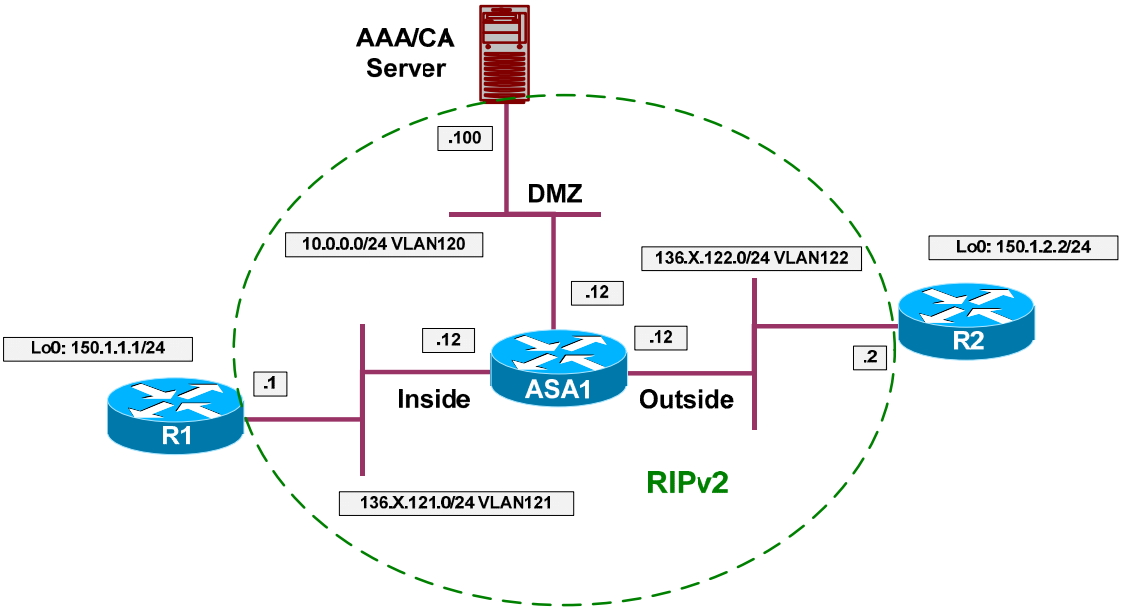
```
current outbound spi: B57901EF

inbound esp sas:
 spi: 0xAF5F4F7C(2942259068)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel UDP-Encaps, }
   slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4490451/2831)
   IV size: 8 bytes
   replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0xB57901EF(3044606447)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel UDP-Encaps, }
   slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4490451/2831)
   IV size: 8 bytes
   replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

Further Reading

NAT - Static Mapping Support with HSRP for High Availability

IPsec Pass-Through Inspection on the PIX/ASA

Objective: Configure the ASA firewall to inspect IKE sessions and open pinholes in ACLs dynamically.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and IOS with Digital Certificates across the PIX/ASA".
- Remove access-list line permitting ESP traffic from the acl OUTSIDE_IN.
- Configure L3/L4 class-map IKE_TRAFFIC and match udp port 500 with it.
- Configure policy-map "global_policy":
  - For class IKE_TRAFFIC configure IPsec inspection.

Final Configuration

```
ASA1:
class-map IKE_TRAFFIC
 match port udp eq isakmp
!
policy-map global_policy
 class IKE_TRAFFIC
  inspect ipsec-pass-thru
!
no access-list OUTSIDE_IN permit esp any any
```

Verification

```
R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
```

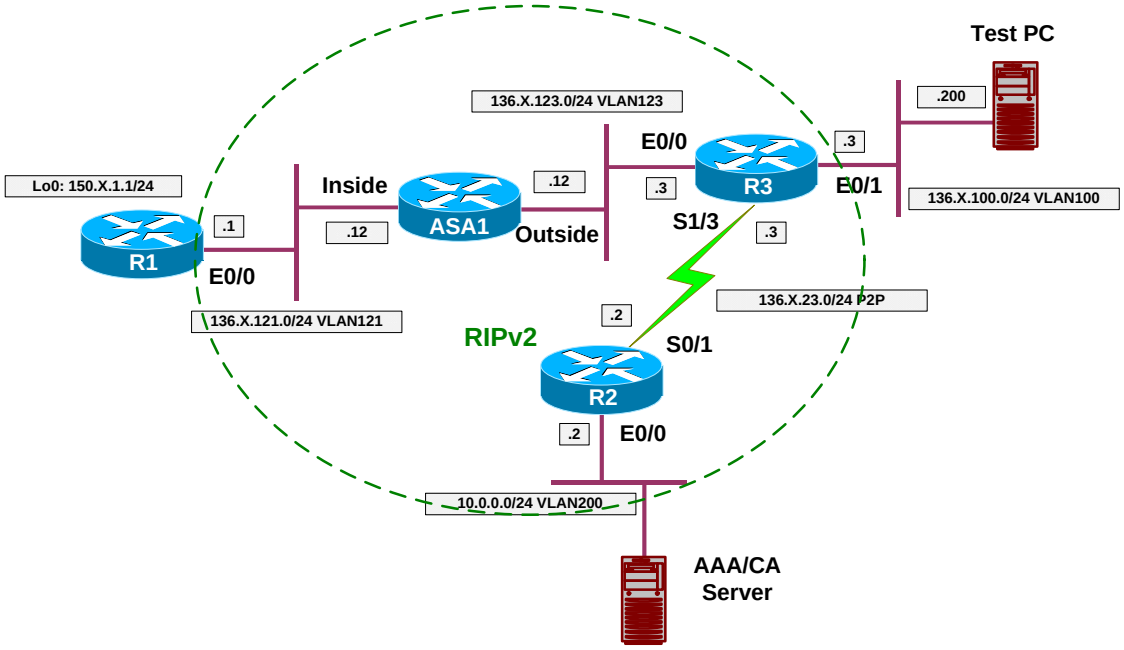
```
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 8/8/8 ms

ASA1(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTSIDE_IN; 3 elements
access-list OUTSIDE_IN line 1 extended permit udp any any eq isakmp (hitcnt=2)
0x468d7962
access-list OUTSIDE_IN line 2 extended permit tcp any host 10.0.0.100 eq www
(hitcnt=8) 0x59f08b76
access-list OUTSIDE_IN line 3 extended permit udp any host 10.0.0.100 eq ntp
(hitcnt=6) 0x8189f120

ASA1(config)# show service-policy global

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
      Inspect: ftp, packet 0, drop 0, reset-drop 0
      Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
      Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
      Inspect: rsh, packet 0, drop 0, reset-drop 0
      Inspect: rtsp, packet 0, drop 0, reset-drop 0
      Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
      Inspect: sqlnet, packet 0, drop 0, reset-drop 0
      Inspect: skinny, packet 0, drop 0, reset-drop 0
      Inspect: sunrpc, packet 0, drop 0, reset-drop 0
      Inspect: xdmcp, packet 0, drop 0, reset-drop 0
      Inspect: sip, packet 0, drop 0, reset-drop 0
      Inspect: netbios, packet 0, drop 0, reset-drop 0
      Inspect: tftp, packet 0, drop 0, reset-drop 0
    Class-map: IKE_TRAFFIC
      Inspect: ipsec-pass-thru _default_ipsec_passthru_map, packet 10, drop 0,
reset-drop 0

ASA1(config)# show conn
13 in use, 209 most used
UDP out 10.0.0.100:123 in 136.1.121.1:123 idle 0:00:53 flags -
ESP out 136.1.122.2 in 136.1.121.1 idle 0:01:22 bytes 248
ESP out 136.1.122.2 in 136.1.121.1 idle 0:01:30 bytes 0
ESP out 136.1.122.2 in 136.1.121.1 idle 0:01:22 bytes 248
ESP out 0.0.0.0 in 0.0.0.0 idle 0:01:30 bytes 0
UDP out 136.1.122.2:500 in 136.1.121.1:500 idle 0:01:22 flags -
UDP out 136.1.122.2:123 in 10.0.0.100:123 idle 0:00:34 flags -
```

Further Reading

Using Modular Policy Framework
Configuring Application Layer Protocol Inspection

L2TP over IPsec between the ASA and Windows 2000 PC

Objective: Configure the ASA firewall to support remote L2TP over IPsec connections.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" "The PIX/ASA Easy VPN/WebVPN".
- The goal of this lab is to set up remote VPN connection using L2TP over IPsec as tunneling protocol. For IPsec part, authentication is performed using the pre-shared keys.
- Configure the workstation using the guide: "How to configure an L2TP/IPSec connection by using Preshared Key Authentication" at http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q240262
- Configure the ASA firewall as follows:

    - IPsec settings:

        - Enable ISAKMP on the outside interface of the ASA
        - Create an ISAKMP policy to use pre-shared keys for authentication and 3DES/SHA1/Group2 as cipher/hash/DH group.
        - Create a wildcard pre-shared key CISCO
        - Create an IPSec transform-set 3DES_MD5_TRANS as follows:

        - Use 3DES/MD5 as cipher/hash
        - Configure transport mode

    - Create an access-list L2TP and match UDP traffic from the outside interface to any host port 1701 (L2TP)
    - Create a dynamic crypto map DYNAMIC as follows:

        - Match access-list L2TP
        - Set transform-set 3DES_MD5_TRANS

    - Create a crypto map VPN and assign the dynamic crypto map DYNAMIC_VPN to it.
    - Assign the crypto map VPN to outside interface.

- IP addressing and username:

    - Create an IP local address pool L2TP with the address range 20.0.0.1 – 20.0.0.254
    - Create local username CISCO with password CISCO1234, specify MSCHAP keyword with it. This way it will be hashed to be used with MSCHAP authentication.

- Create group-policy “L2TP” as follows:

    - Configure IPsec and L2TP-IPsec as the tunneling protocols.
    - Configure default-domain value “internetworkexpert.com”.
    - Use DNS server IP address 10.0.0.100.

- Assign group-policy “L2TP” to user “CISCO”, and configure “L2TP-over-IPsec” as user’s tunneling protocol.

- Modify the built-in default tunnel-group “DefaultRAGroup” general-attributes as follows:

    - Assign local address pool L2TP to the group.
    - Use LOCAL authentication server group.
    - Apply default group policy “L2TP”.

- Modify the built-in default tunnel-group “DefaultRAGroup” ppp-attributes to use “MS-CHAP-v2” as the authentication protocol.
- Modify the built-in default tunnel-group “DefaultRAGroup” ipsec-attributes to use pre-shared key “CISCO”.

Final Configuration

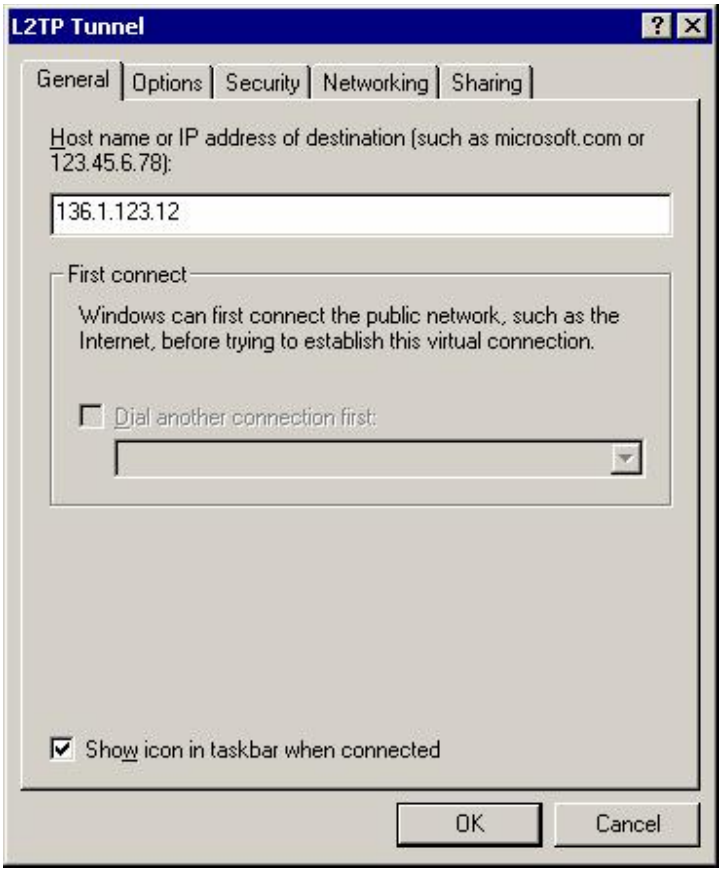
ASA1:

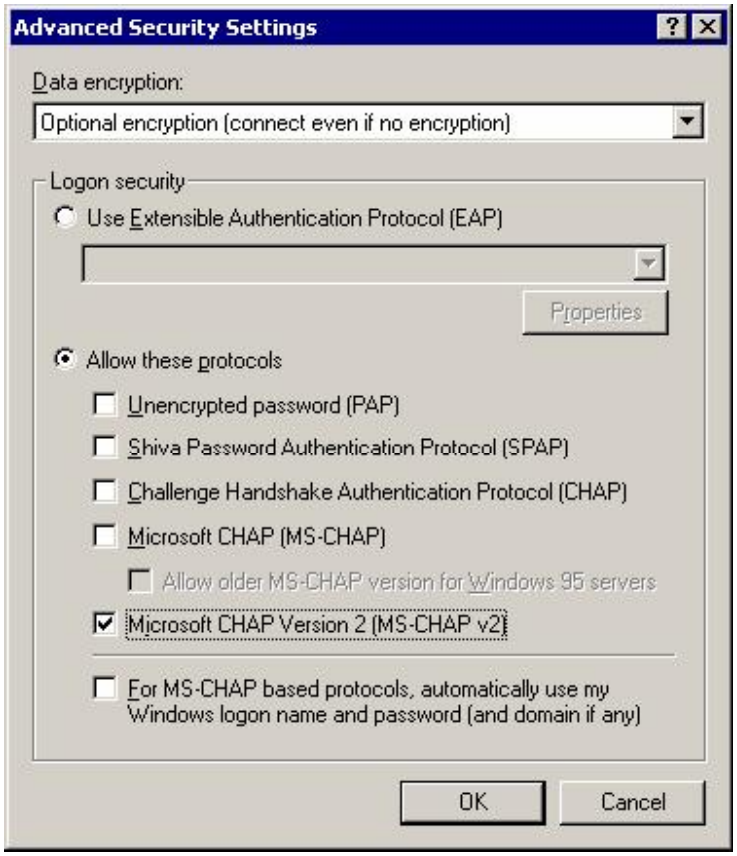
```
!
! Define a new group policy for L2TP connections
!
group-policy L2TP internal
group-policy L2TP attributes
 dns-server value 10.0.0.100
 vpn-tunnel-protocol IPSec l2tp-ipsec
 default-domain value internetworkexpert.com
!
! Create local user and apply the group policy to it
!
username CISCO password CISCO1234 mschap
!
! Note that user's tunneling protocol is L2TP over IPsec
!
username CISCO attributes
 vpn-group-policy L2TP
 vpn-tunnel-protocol l2tp-ipsec
!
! Modify built-in default tunnel-group
! Apply the L2TP group-policy within
!
tunnel-group DefaultRAGroup general-attributes
 address-pool L2TP
 default-group-policy L2TP
 authentication-server-group LOCAL
!
! Define PPP attributes
!
tunnel-group DefaultRAGroup ppp-attributes
 authentication ms-chap-v2
!
! Define a pre-share ISAKMP key
!
tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key CISCO
!
! Enable and configure ISAKMP on the outside
!
crypto isakmp enable outside
crypto isakmp identity address
crypto isakmp policy 10
  auth pre-share
  encr 3des
  hash sha1
  group 1
!
crypto ipsec transform-set DES_MD5_TRANS esp-des esp-md5-hmac
crypto ipsec transform-set DES_MD5_TRANS mode transport
!
access-list L2TP extended permit udp any any eq 1701
!
crypto dynamic-map DYNAMIC 10 match address L2TP
crypto dynamic-map DYNAMIC 10 set transform-set DES_MD5_TRANS
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
crypto map VPN interface outside
!
```

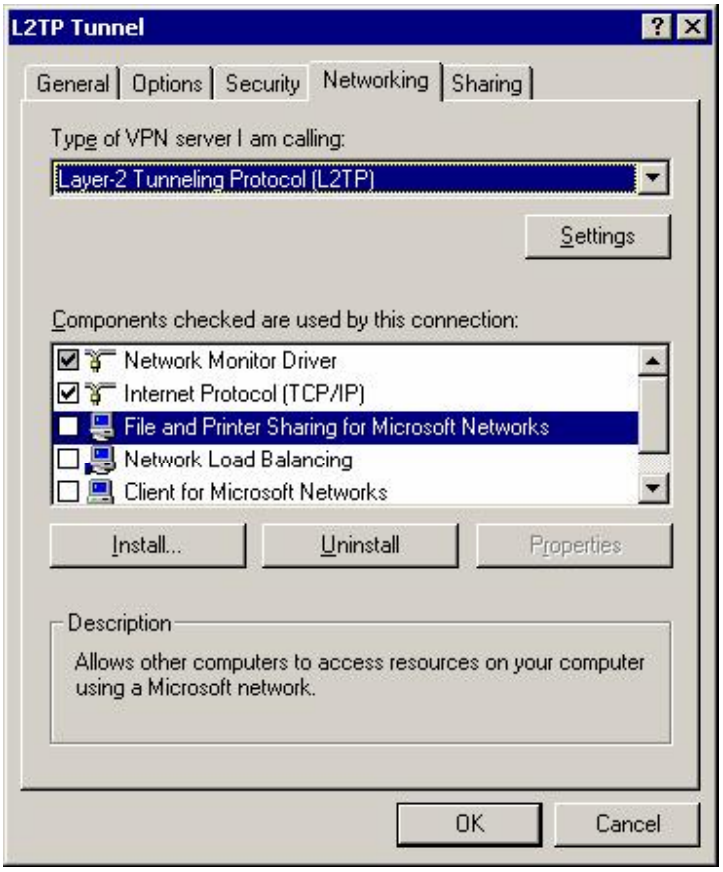
```
sysopt connection permit-vpn
```

Verification

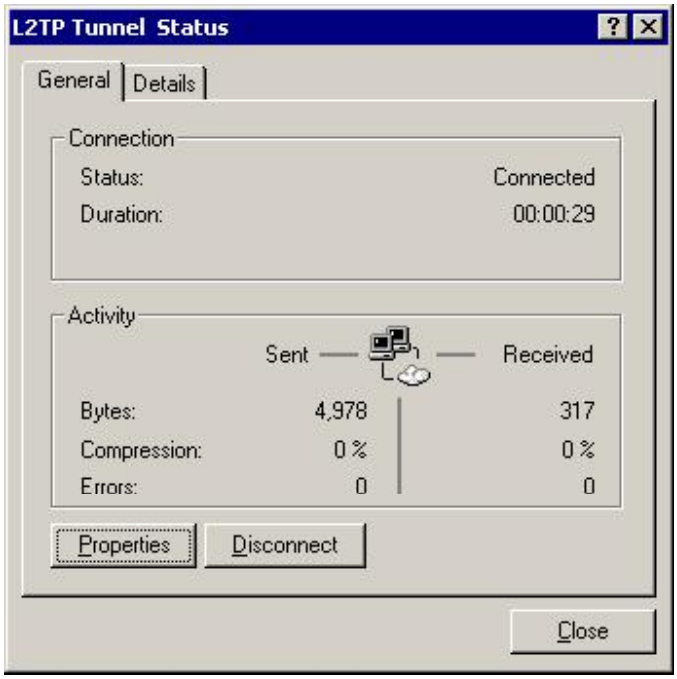
Create new L2TP VPN connection:

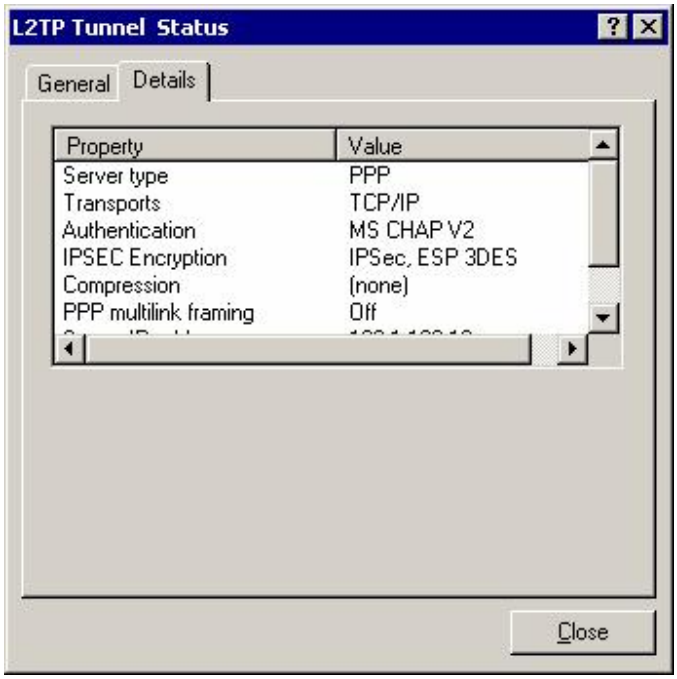



Advanced Security Settings
Data encryption:
Optional encryption (connect even if no encryption)
Logon security
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
Unencrypted password (PAP)
Shiva Password Authentication Protocol (SPAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP (MS-CHAP)
Allow older MS-CHAP version for Windows 95 servers
Microsoft CHAP Version 2 (MS-CHAP v2)
For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)
OK
Cancel



Connect to the ASA:






```
ASA1(config)# 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: 10.0.0.100
    Type    : user             Role    : responder
    Rekey   : no               State   : MM_ACTIVE
```

```
ASA1(config)# show cry ips sa
interface: outside
    Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12

      access-list L2TP permit udp any any eq 1701
      local ident (addr/mask/prot/port): (136.1.123.12/255.255.255.255/17/0)
      remote ident (addr/mask/prot/port): (10.0.0.100/255.255.255.255/17/1701)
      current_peer: 10.0.0.100, username: CISCO
      dynamic allocated peer ip: 20.0.0.1

      #pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
      #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 24, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 136.1.123.12, remote crypto endpt.: 10.0.0.100

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: A5D2904C

    inbound esp sas:
      spi: 0x9A975A34 (2593610292)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 125, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (kB/sec): (92766/712)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xA5D2904C (2782040140)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 125, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (kB/sec): (92771/712)
         IV size: 8 bytes
         replay detection support: Y

ASA1(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    136.1.23.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:19, outside
R    136.1.100.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:19, outside
C    136.1.121.0 255.255.255.0 is directly connected, inside
C    136.1.123.0 255.255.255.0 is directly connected, outside
S    20.0.0.1 255.255.255.255 [1/0] via 136.1.123.3, outside
R    10.0.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:19, outside
R    150.1.2.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:19, outside
R    150.1.1.0 255.255.255.0 [120/1] via 136.1.121.1, 0:00:03, inside

ASA1(config)# show vpn-sessiondb remote
```

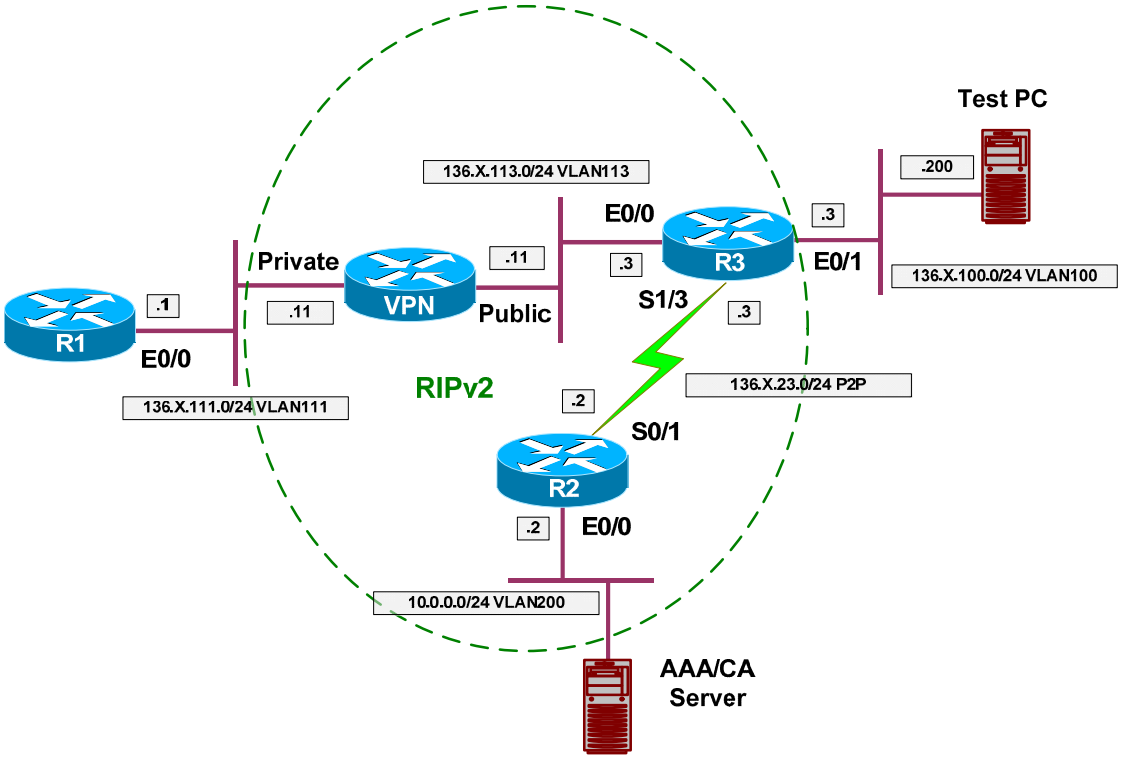
```
Session Type: Remote

Username     : CISCO
Index        : 1
Assigned IP  : 20.0.0.1              Public IP    : 10.0.0.100
Protocol     : L2TPOverIPSec         Encryption   : 3DES
Hashing      : MD5
Bytes Tx     : 1460                  Bytes Rx     : 6572
Client Type  : Microsoft             Client Ver   : 5.0
Group Policy : L2TP
Tunnel Group : DefaultRAGroup
Login Time   : 10:27:36 UTC Fri Jan 26 2007
Duration     : 0h:05m:02s
Filter Name  :
NAC Result   : N/A
Posture Token:

ASA1(config)# ping 20.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
```

Further Reading

Configuring L2TP over IPSec
L2TP Over IPsec Between Windows 2000/XP PC and PIX/ASA 7.2 Using Pre-shared Key

VPN3k and PPTP Client

Objective: Configure VPN3k to support users connecting via PPTP.



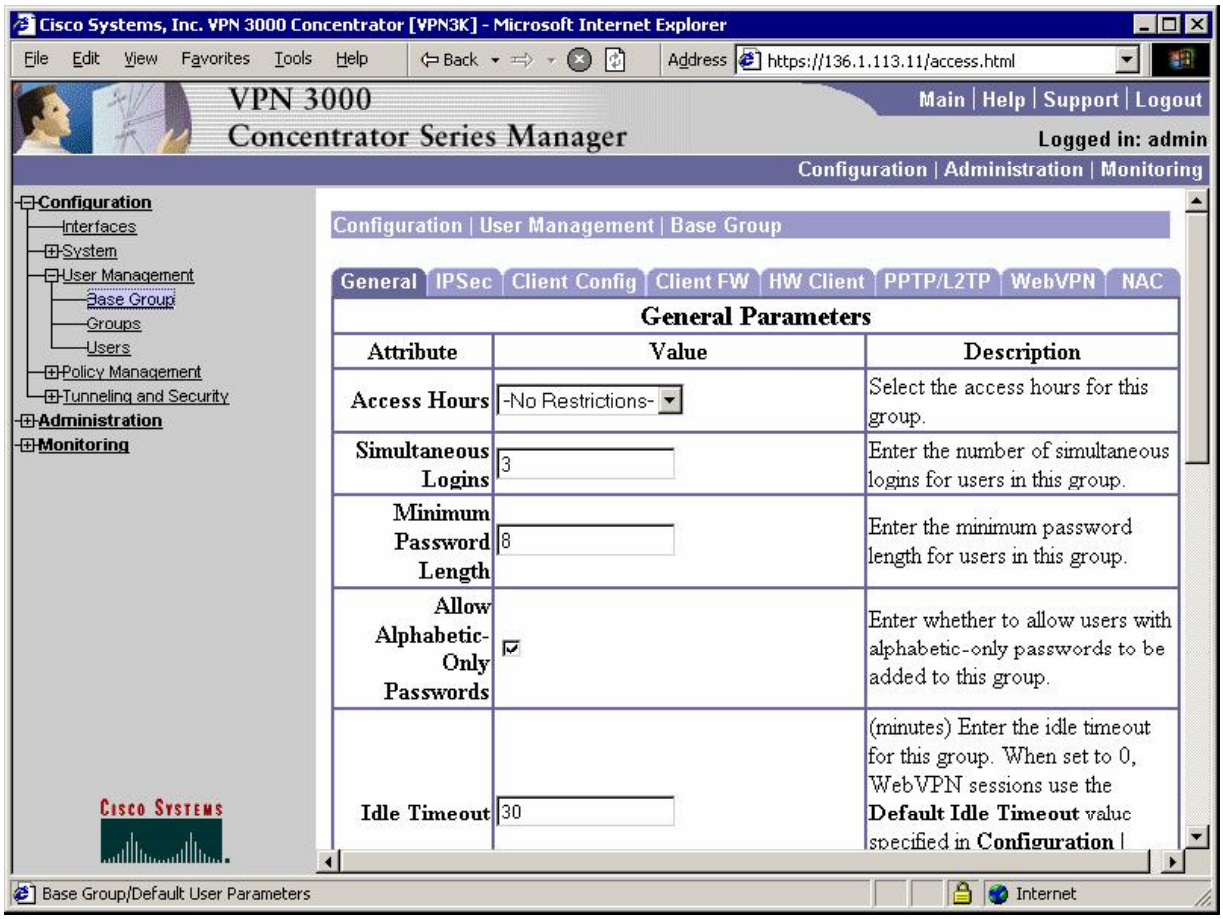
Directions

- Configure devices as per the scenario "VPN/Common Configurations" "VPN3k Easy VPN/WebVPN".
- Create an IP address pool globally on VPN3k with address range "20.0.0.1-20.0.0.254".
- Configure default group to accept PPTP connections.
- Additionally, enable MSCAP for PPP authentication.
- Create a local user named "CISCO" with password "CISCO1234".
- Configure address assignment policy to use local address pools.
- Enable client reverse route injection.
- Configure PPTP client on Windows PC.

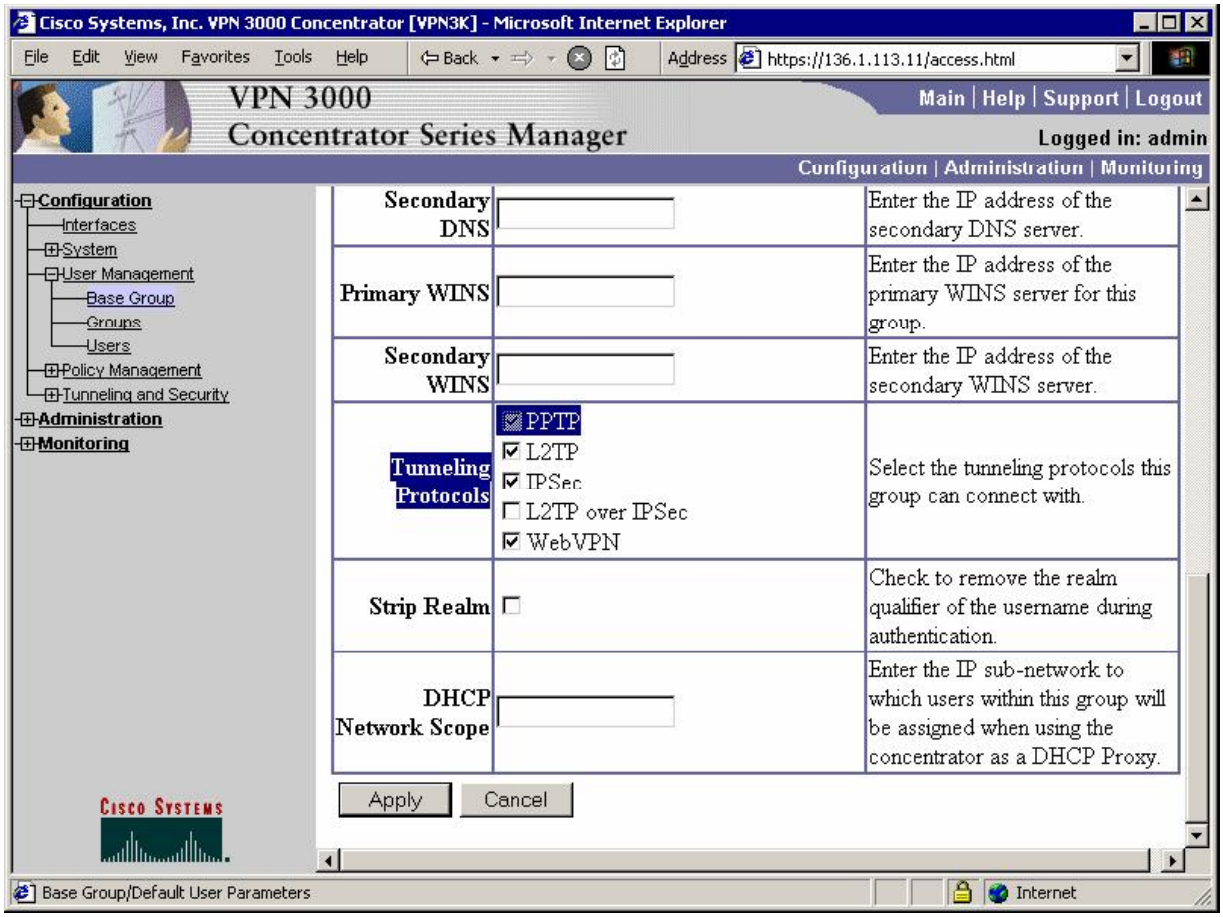
Final Configuration

VPN3k:

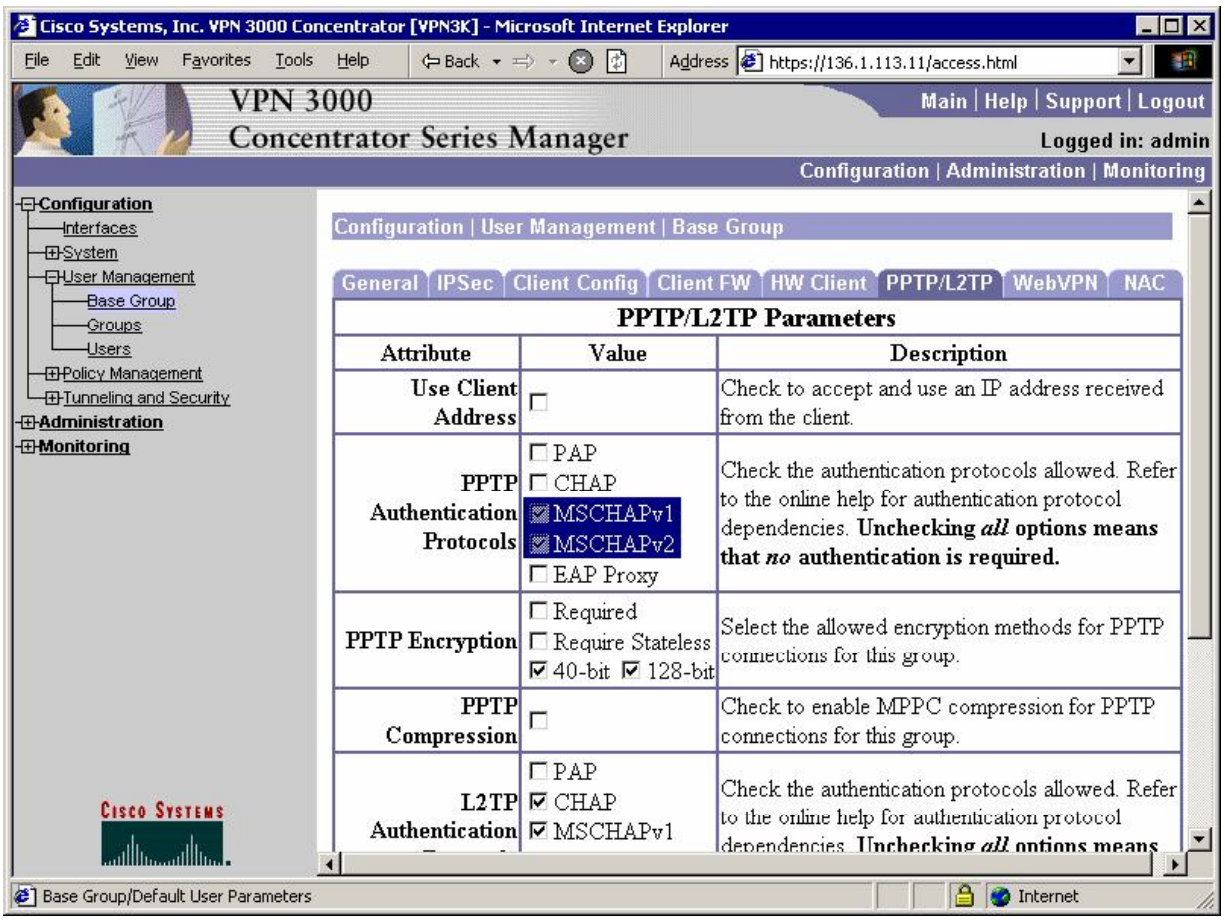
Change Base group settings:



Enable PPTP as tunneling protocol

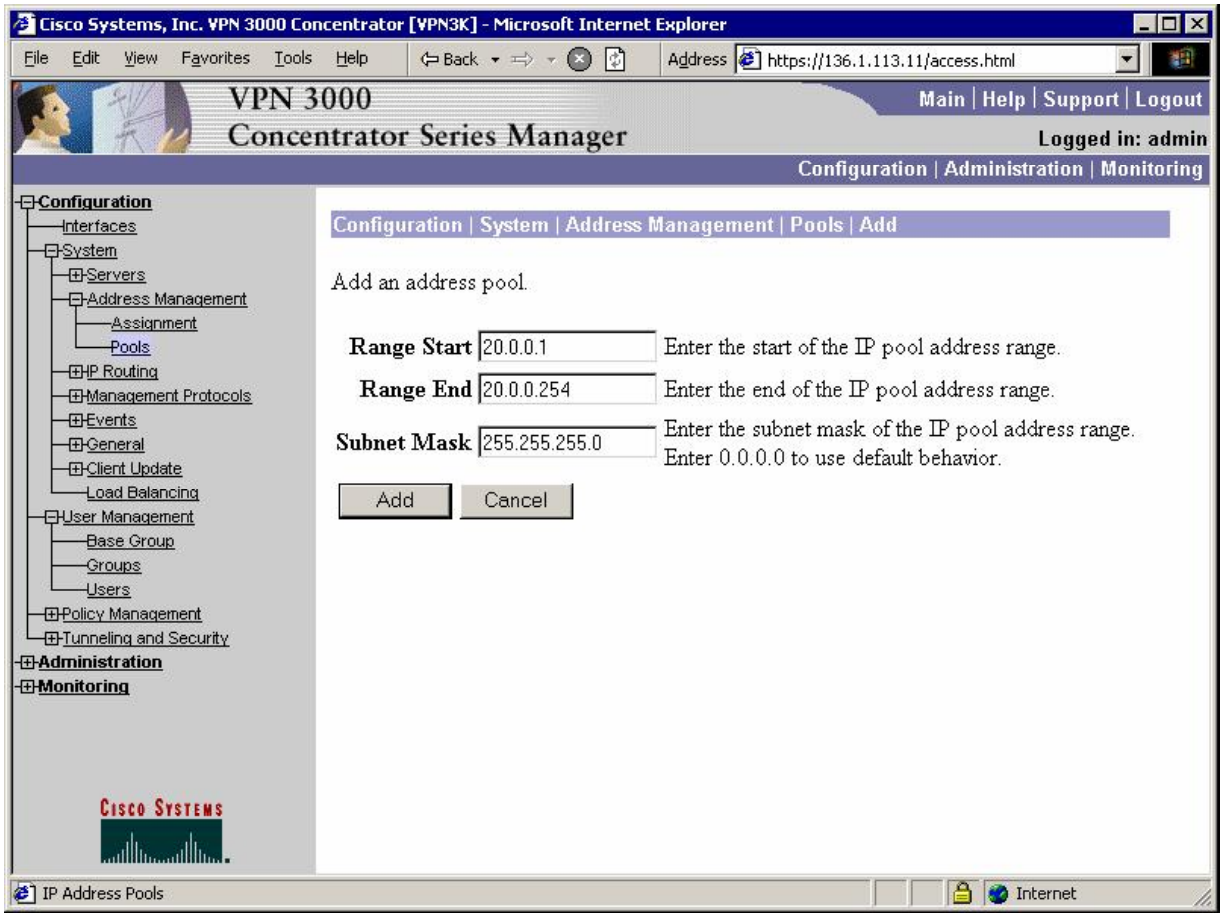


Configure PPP Authentication:

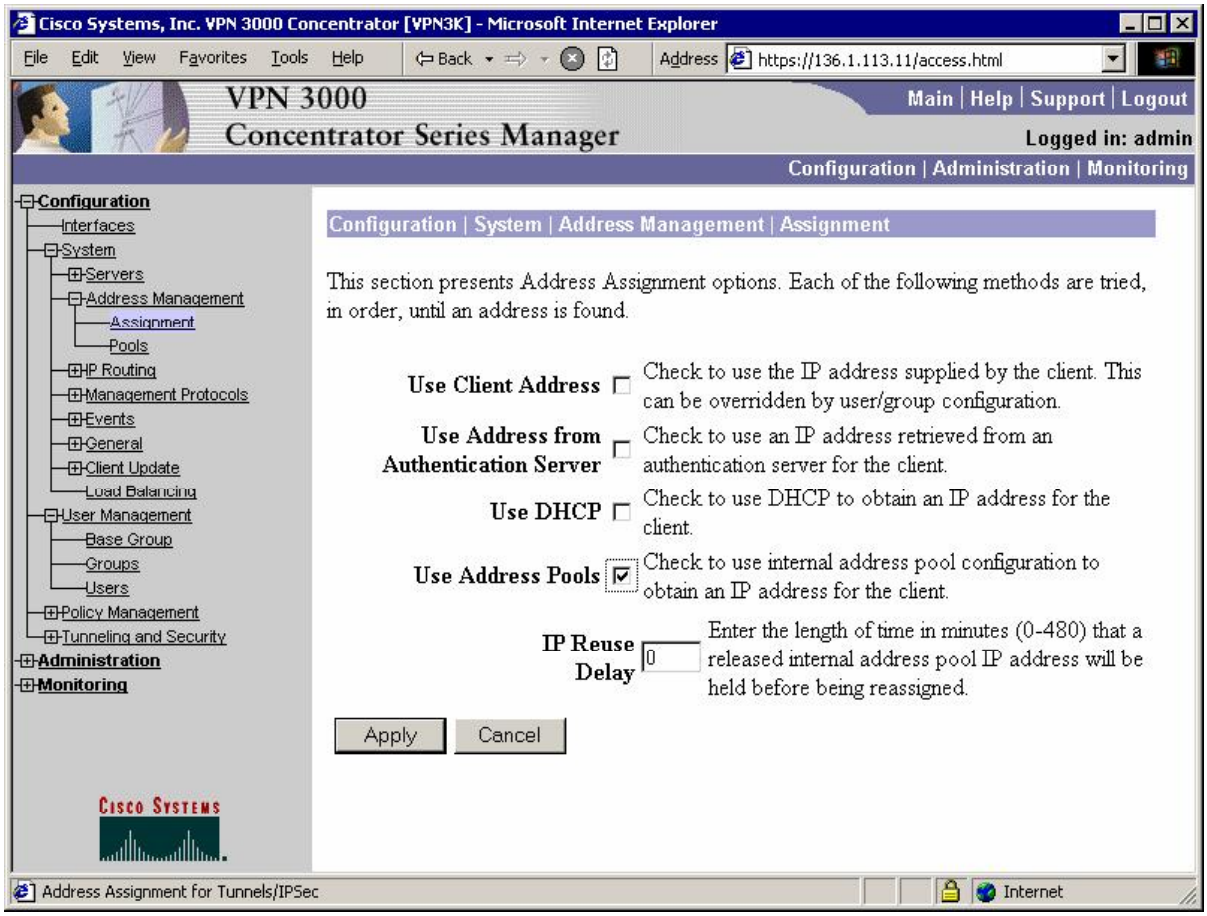


Add new user "CISCO" with password "CISCO1234":

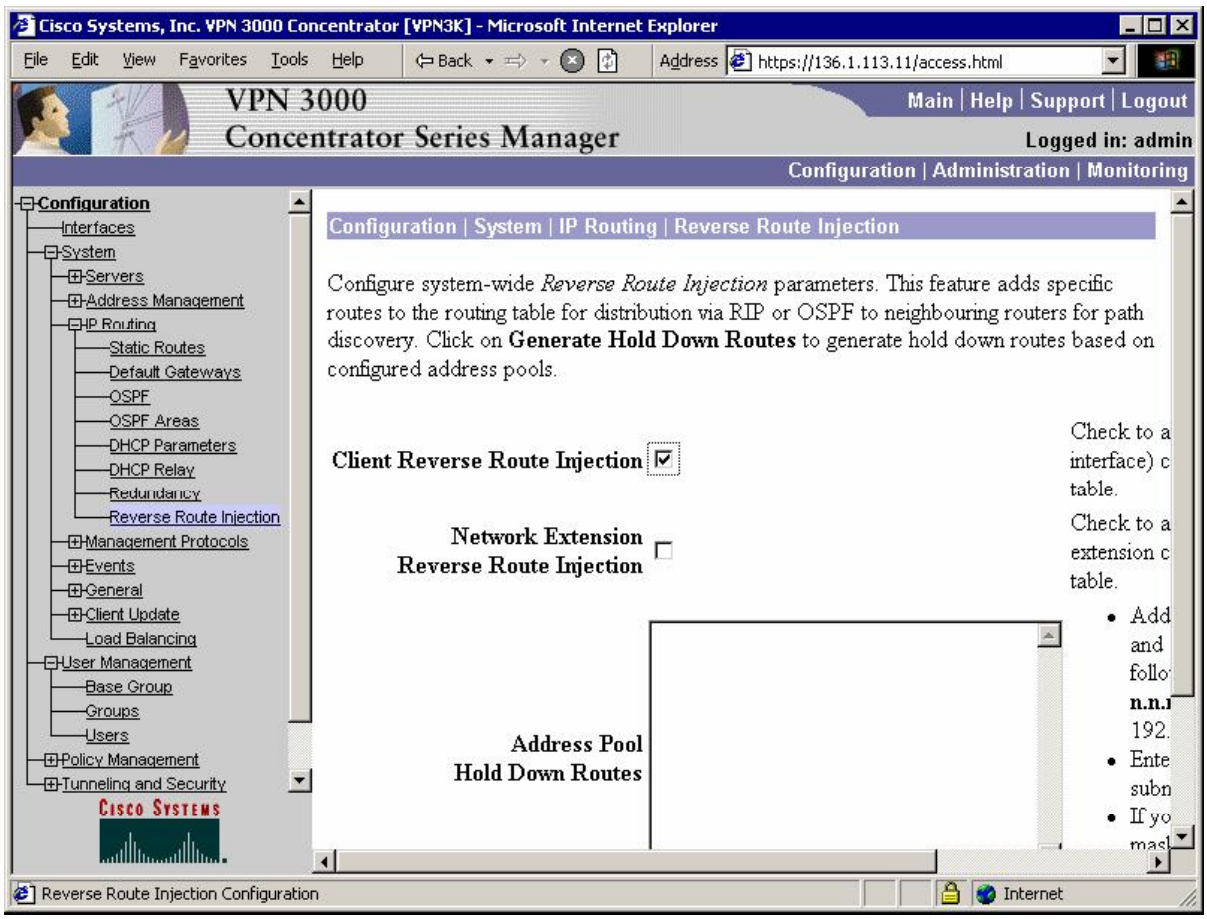
Create an IP address pool (global):



Configure address assignment from local pools:

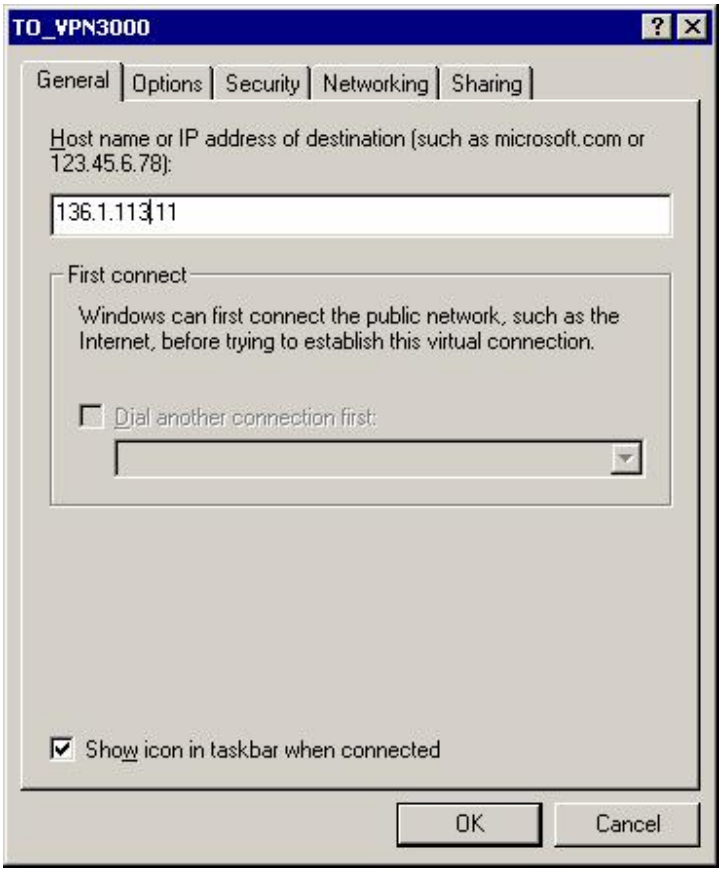


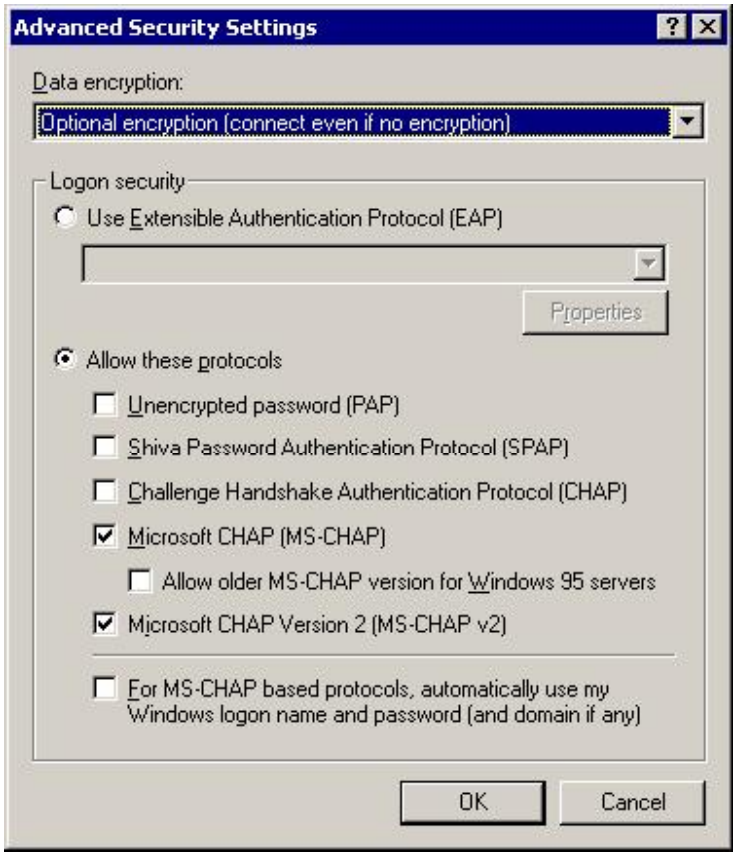
Enable Client RRI:

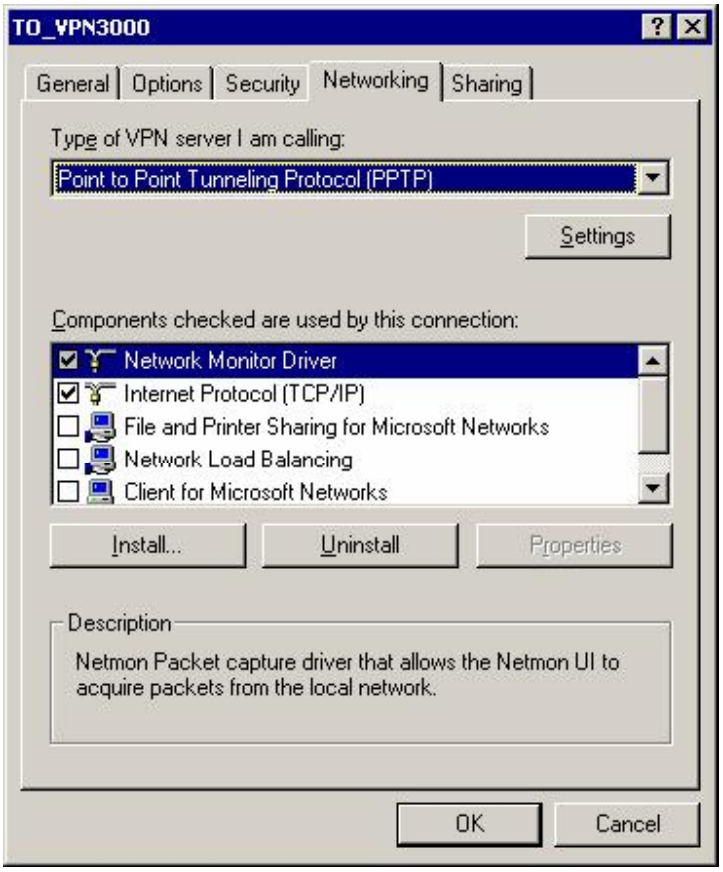


Verification

Configure PPTP client on VPN3k:

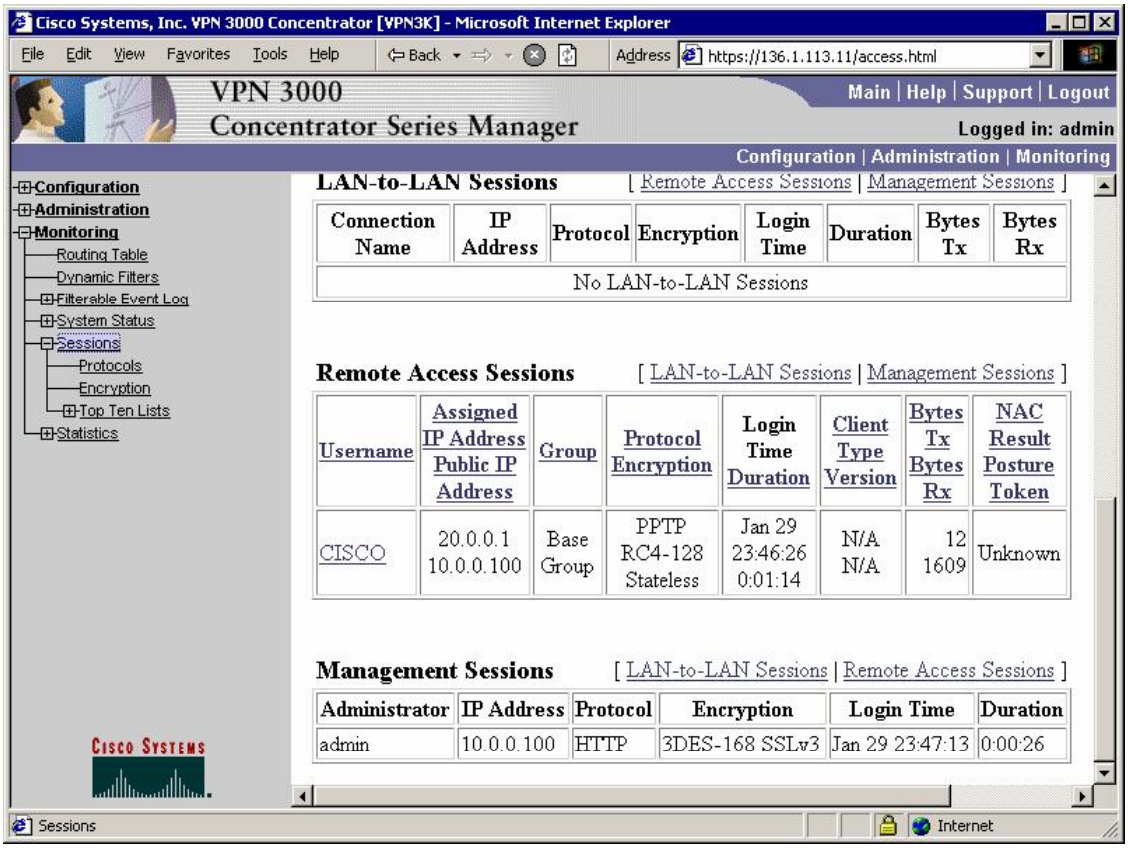



Advanced Security Settings
Data encryption:
Optional encryption (connect even if no encryption)
Logon security
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
Unencrypted password (PAP)
Shiva Password Authentication Protocol (SPAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP (MS-CHAP)
Allow older MS-CHAP version for Windows 95 servers
Microsoft CHAP Version 2 (MS-CHAP v2)
For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)
OK
Cancel


TO_VPN3000
General
Options
Security
Networking
Sharing
Type of VPN server I am calling:
Point to Point Tunneling Protocol (PPTP)
Settings
Components checked are used by this connection:
Network Monitor Driver
Internet Protocol (TCP/IP)
File and Printer Sharing for Microsoft Networks
Network Load Balancing
Client for Microsoft Networks
Install...
Uninstall
Properties
Description
Netmon Packet capture driver that allows the Netmon UI to acquire packets from the local network.
OK
Cancel


Connect TO_VPN3000
User name:
CISCO
Password:
Save Password
Connect
Cancel
Properties
Help

Check connected sessions on VPN3k:

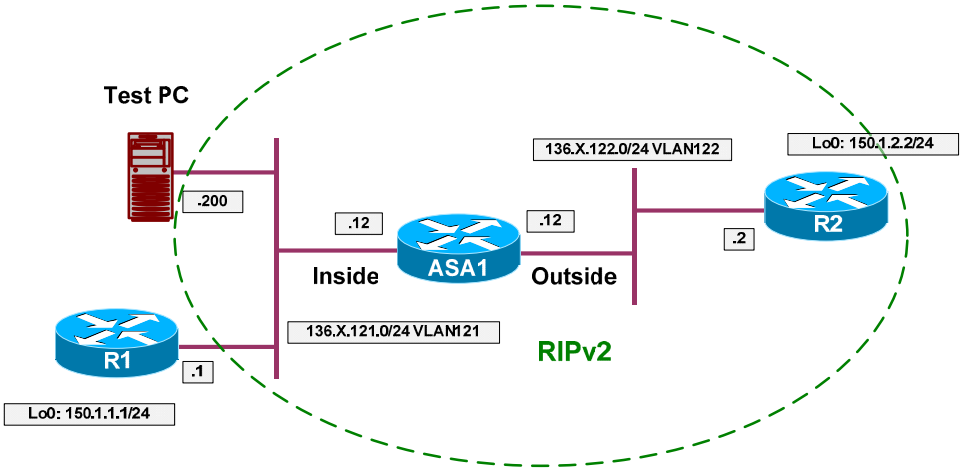


Further Reading

[Configuring the VPN 3000 Concentrator PPTP With Cisco Secure ACS for Windows RADIUS Authentication]

Using ISAKMP Profiles

Objective: Configure router to support ezVPN client connections and IPsec LAN-to-LAN connections simultaneously.



Directions

- Pre-configure devices as follows:
    - Create the necessary VLANs, and configure the switchports respectively as per the diagram.
    - Configure IP addressing as per the diagram.
    - Configure RIP as routing protocol on all devices.
    - Advertise Loopback interfaces on R1 and R2 into RIP.
- The goal is to provide support for remote ezVPN clients as well as L2L connections terminating on the same router and the same interface.
- This is possible withf "ISAKMP profiles" feature. As soon as ISAKMP negotiations reveal client's identity, it is possible to apply certain ISAKMP policies to a given client.
- Specifically you may decide to enable Xauth and Mode Config for a client group.
- Configure access-control on the ASA to permit IPsec traffic as follows:
    - Create and apply to the outside interface access-list OUTSIDE_IN:
        - Permit ISAKMP traffic from outside.
        - Permit ESP traffic from outside.
- We are going to configure L2L tunnel on R1 to use IKE Aggressive mode along with hostname identity.
- Configure an IPsec LAN-to-LAN tunnel on R1 as follows:

- Configure hostname “R1” and domain-name “internetworkexpert.com”.
- Create ISAKMP profile named “AGGRESSIVE”:
    - Initiate aggressive mode.
    - Use hostname (FQDN) for identity.
    - Use the default keyring.
- Create ISAKMP policy with priority 10:
    - Use pre-shared keys authentication.
    - Use 3DES for cipher.
    - Use MD5 for hash.
    - Use DH Group 2.
- Create ISAKMP key “LAN2LAN” for address 136.X.122.2 (R2).
- Create transform-set 3DES_MD5
    - Use 3DES for cipher.
    - Use MD5 for hash.
- Create access-list “LO1_TO_LO2”:
    - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP
    - Match address LO1_TO_LO2.
    - Set peer 136.X.122.2.
    - Set transform-set 3DES_MD5.
- Associate ISAKMP profile “AGGRESSIVE” with crypto map “VPN”.
- Apply crypto-map “VPN” to interface E0/0.

- Configure common IPsec settings on R2 as follows:
    - Create ISAKMP policy as follows:
        - Authentication via pre-shared key.
        - Encryption 3DES.
        - Hash MD5.
        - DH Group 2 (to match DH group of ezVPN client).
    - Create IPsec transform-set 3DES_MD5 as follows:

        - Use 3DES cipher.
        - Use MD5 hash.

- Configure IPsec settings for ezVPN server on R2 as follows:

    - Enable and configure AAA as follows:

        - Disable authentication on the console line.
        - Create AAA list “EZVPN” for local login authentication.
        - Create AAA list “EZVPN” for local network authorization.
        - Create local username “CISCO” with password “CISCO1234”.

    - Create local address pool named “EZVPN” with address range “20.0.0.1-20.0.0.254”.
    - Assign this pool to the ISAKMP client configuration process.
    - Create ISAKMP profile named “EZVPN” as follows:

        - Match remote group named “EZVPN”.
        - Enable client authentication via AAA list “EZVPN”.
        - Enable ISAKMP authorization using AAA list “EZVPN”.
        - Respond to configuration mode requests.

    - Create split access-list named “SPLIT_TUNNEL” and permit only network “136.1.0.0/16” within.
    - Create ISAKMP client configuration group named “EZVPN” as follows:

        - Configure pre-shared key “EZVPN”.
        - Use local address pool “EZVPN”.
        - Use split access-list “SPLIT_TUNNEL”.

    - Create dynamic crypto map named “DYNAMIC” as follows:

        - Set transform-set 3DES_MD5.
        - Enable RRI.

- Configure IPsec settings for L2L tunnel on R2 as follows:

    - Create crypto keyring named “LAN2LAN”:

        - Assign key “LAN2LAN” to host “R1.internetworkexpert.com”

    - Create ISAKMP profile “LAN2LAN” as follows:

- Match identity based on domain-name "internetworkexpert.com".
- Use address as self-identity.
- Use keyring "LAN2LAN".

o Create access-list "LO2_TO_LO1" to match traffic from Loopback0 of R2 to Loopback0 of R1.

- Create crypto-map named "VPN" entry 10 on R2 as follows:

  o Match address "LO2_TO_LO1".
  o Set transform-set "3DES_MD5".
  o Set peer 136.1.121.1

- Create crypto-map named "VPN" entry 20 on R2 to use dynamic crypto map named "DYNAMIC".
- Apply crypto map VPN to interface Ethernet 0/0.

Final Configuration

Pre-Configuration

ASA1:

```
!
! IP addressing
!
interface Ethernet0/0
 no shut
 nameif outside
 security-level 0
 ip address 136.1.122.12 255.255.255.0
!
interface Ethernet0/1
 no shut
 nameif inside
 security-level 100
 ip address 136.1.121.12 255.255.255.0
!
! RIP configuration
!
router rip
 version 2
 no auto-summary
 network 136.1.0.0
```

SW1 & SW2:

```
!
! create VLANs and configure trunk links
!
vlan 121,122
!
interface range Fa 0/21 - 23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shut
```

SW1:

```
!
!  Configure switchports
!
interface Fa 0/1
 switchport host
 switchport access vlan 121
!
interface Fa 0/2
 switchport host
 switchport access vlan 122
```

SW2:

```
!
!  Configure switchports
!
interface Fa 0/12
 switchport host
 switchport access vlan 122
!
interface Fa 0/20
 switchport host
 switchport access vlan 121
```

R1:

```
interface E 0/0
 no shut
 ip add 136.1.121.1 255.255.255.0
!
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
```

R2:

```
interface E 0/0
 no shut
 ip add 136.1.122.2 255.255.255.0
!
interface Loopback0
 ip address 150.1.2.2 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
```

ASA1:

```
access-list OUTSIDE_IN extended permit udp any any eq isakmp
access-list OUTSIDE_IN extended permit esp any any
!
access-group OUTSIDE_IN in interface outside
```

ISAKMP Profiles:

R1:

```
hostname R1
ip domain-name internetworkexpert.com
!
! Create ISAKMP profile for aggressive mode
!
crypto isakmp profile AGGRESSIVE
  self-identity fqdn
  initiate mode aggressive
  keyring default
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
 group 2
!
crypto isakmp key LAN2LAN address 136.1.122.2
!
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-List to classify VPN traffic
!
ip access-list extended LO1_TO_LO2
  permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
!
! Create crypto-map
!
crypto map VPN 10 ipsec-isakmp
 match address LO1_TO_LO2
 set transform 3DES_MD5
 set peer 136.1.122.2
!
! Associate profile with crypto map
!
crypto map VPN isakmp-profile AGGRESSIVE
!
! Apply the crypto map
!
interface E 0/0
 crypto map VPN
```

R2:

```
!
! COMMON CONFIG
!

!
! Create ISAKMP policy (Phase 1) common to L2L and ezVPN clients
!
crypto isakmp policy 10
 authentication pre-share
 hash md5
 encryption 3des
 group 2

!
!
! Create transform set
!
```

```
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac

!
! EZVPN CONFIG
!
!

! Configure AAA stuff required for ezVPN
!
aaa new-model
!
! Disable console auth
!
aaa authentication login CONSOLE none
!
! Define AAA lists we referenced in ezVPN ISAKMP profile
!
aaa authentication login EZVPN local
aaa authorization network EZVPN local
!
! Create a user for Xauth
!
username CISCO password CISCO1234
!
! Configure local address pool for remote users
! Configure ISAKMP to use this address pool
!
ip local pool EZVPN 20.0.0.1 20.0.0.254
crypto isakmp client configuration address-pool local EZVPN

!
! ISAKMP policy specific for ezVPN clients (they have group ID)
! Note Mode Config and Xauth configuration
!
crypto isakmp profile EZVPN
   match identity group EZVPN
   client authentication list EZVPN
   isakmp authorization list EZVPN
   client configuration address respond
!
! Split-tunnel ACL for remote ezVPN users
!
ip access-list extended SPLIT_TUNNEL
 permit ip 136.1.0.0 0.0.0.255 any
!
! ISAKMP group policy for ezVPN group named "EZVPN"
!
crypto isakmp client configuration group EZVPN
  key EZVPN
  pool EZVPN
  acl SPLIT_TUNNEL
!
! Dynamic crypto map for ezVPN clients
!
crypto dynamic-map DYNAMIC 10
  set transform-set 3DES_MD5
  reverse-route

!
! LAN2LAN TUNNEL CONFIG
!

!
```

```
! Create a keyring for L2L connections
!
crypto keyring LAN2LAN
  pre-shared-key hostname R1.internetworkexpert.com  key LAN2LAN
!
! Create a profile to match incoming L2L connection
!
crypto isakmp profile LAN2LAN
   keyring LAN2LAN
   self-identity address
   match identity host domain internetworkexpert.com
!
! Access-List to classify L2L VPN traffic
!
ip access-list extended LO2_TO_LO1
  permit ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255

!
! COMMON CONFIG
!

!
! Create crypto-map
!
crypto map VPN 10 ipsec-isakmp
 match address LO2_TO_LO1
 set transform 3DES_MD5
 set peer 136.1.121.1
!
! Dynamic entry
!
crypto map VPN 20 ipsec-isakmp dynamic DYNAMIC
!
! Apply crypto map to Ethernet interface
!
interface E 0/0
 crypto map VPN
```

Verification

Initiate L2L tunnel from R1:

```
R1#ping 150.1.2.2 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/12 ms
```

Snip from the output of "debug crypto isakmp" command on R1:

```
*Mar  1 01:32:47.040: ISAKMP: received ke message (1/1)
*Mar  1 01:32:47.040: ISAKMP (0:0): SA request profile is AGGRESSIVE
*Mar  1 01:32:47.040: ISAKMP: local port 500, remote port 500
*Mar  1 01:32:47.040: ISAKMP: set new node 0 to QM_IDLE
*Mar  1 01:32:47.044: ISAKMP: insert sa successfully sa = 82E36154
*Mar  1 01:32:47.044: ISAKMP (0:1): Found ADDRESS key in keyring default
*Mar  1 01:32:47.044: ISAKMP (0:1): constructed NAT-T vendor-03 ID
*Mar  1 01:32:47.044: ISAKMP (0:1): constructed NAT-T vendor-02 ID
```

```
*Mar  1 01:32:47.321: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_FQDN
*Mar  1 01:32:47.325: ISAKMP (1): ID payload
        next-payload : 13
        type         : 2
        FQDN name    : R1.internetworkexpert.com
        protocol     : 17
        port         : 0
        length       : 29
```

Snip of output from the "debug crypto isakmp" command on R2:

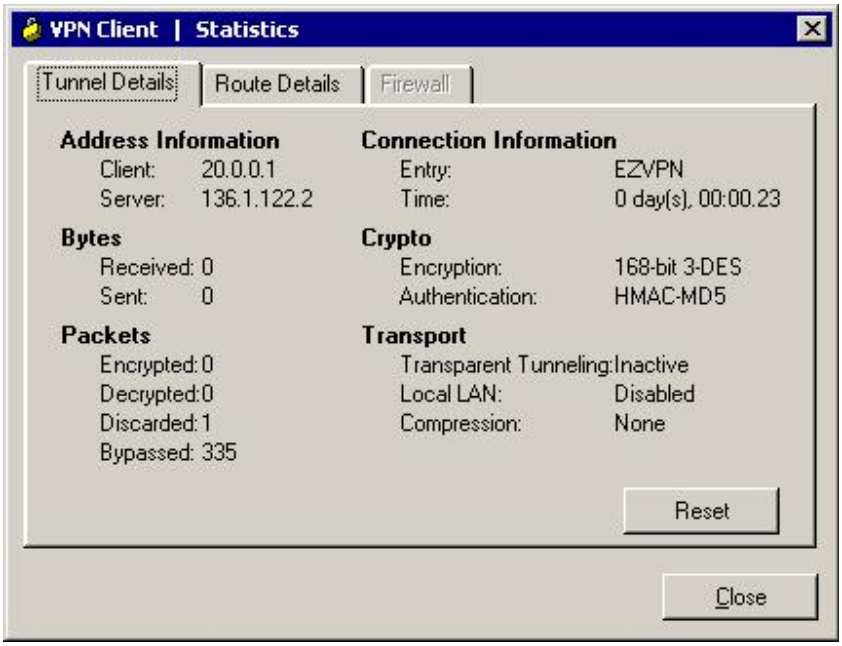
```
*Mar  1 01:34:05.725: ISAKMP (5): Process ID payload
        type         : 2
        FQDN name    : R1.internetworkexpert.com
        protocol     : 17
        port         : 0
        length       : 25
*Mar  1 01:34:05.725: ISAKMP (0:5): peer matches LAN2LAN profile
*Mar  1 01:34:05.725: ISAKMP: Looking for a matching key for 136.1.121.1 in
default
*Mar  1 01:34:05.729: ISAKMP: Looking for a matching key for 136.1.121.1 in
LAN2LAN
*Mar  1 01:34:05.729: ISAKMP: Looking for a matching key for 136.1.121.1 in
EZVPN : success
*Mar  1 01:34:05.729: ISAKMP (0:5): processing vendor id payload
*Mar  1 01:34:05.729: ISAKMP (0:5): vendor ID seems Unity/DPD but major 157
mismatch
*Mar  1 01:34:05.729: ISAKMP (0:5): vendor ID is NAT-T v3
*Mar  1 01:34:05.729: ISAKMP (0:5): processing vendor id payload
*Mar  1 01:34:05.729: ISAKMP (0:5): vendor ID seems Unity/DPD but major 123
mismatch
*Mar  1 01:34:05.733: ISAKMP (0:5): vendor ID is NAT-T v2
*Mar  1 01:34:05.733: ISAKMP (0:5): Found HOST key in keyring LAN2LAN
*Mar  1 01:34:05.733: ISAKMP (0:5) local preshared key found
*Mar  1 01:34:05.733: ISAKMP : Scanning profiles for xauth ... LAN2LAN EZVPN
```

Self-ID on R2. Note that R1 and R2 use different ID types!

```
*Mar  1 01:34:06.367: ISAKMP (5): ID payload
        next-payload : 10
        type         : 1
        addr         : 136.1.122.2
        protocol     : 17
        port         : 0
        length       : 8
*Mar  1 01:34:06.367: ISAKMP (5): Total payload length: 12
*Mar  1 01:34:06.367: ISAKMP (0:5): constructed HIS NAT-D
*Mar  1 01:34:06.367: ISAKMP (0:5): constructed MINE NAT-D
*Mar  1 01:34:06.367: ISAKMP (0:5): sending packet to 136.1.121.1 my_port 500
peer_port 500 (R) AG_INIT_EXCH
*Mar  1 01:34:06.371: ISAKMP (0:5): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Mar  1 01:34:06.371: ISAKMP (0:5): Old State = IKE_READY  New State =
IKE_R_AM2

*Mar  1 01:34:06.747: ISAKMP (0:5): received packet from 136.1.121.1 dport 500
sport 500 Global (R) AG_INIT_EXCH
*Mar  1 01:34:06.751: ISAKMP (0:5): processing HASH payload. message ID = 0
*Mar  1 01:34:06.751: ISAKMP:received payload type 17
*Mar  1 01:34:06.751: ISAKMP (0:5): Detected NAT-D payload
*Mar  1 01:34:06.751: ISAKMP (0:5): recalc my hash for NAT-D
*Mar  1 01:34:06.751: ISAKMP (0:5): NAT match MINE hash
```

```
*Mar  1 01:34:06.751: ISAKMP:received payload type 17
*Mar  1 01:34:06.755: ISAKMP (0:5): Detected NAT-D payload
*Mar  1 01:34:06.755: ISAKMP (0:5): recalc his hash for NAT-D
*Mar  1 01:34:06.755: ISAKMP (0:5): NAT match HIS hash
*Mar  1 01:34:06.755: ISAKMP (0:5): processing NOTIFY INITIAL_CONTACT protocol
1
        spi 0, message ID = 0, sa = 82BD41BC
*Mar  1 01:34:06.755: ISAKMP (0:5): Process initial contact,
bring down existing phase 1 and 2 SA's with local 136.1.122.2 remote
136.1.121.1 remote port 500
*Mar  1 01:34:06.767: ISAKMP (0:5): SA has been authenticated with 136.1.121.1
```

Connect Cisco VPN client on Test PC to R2, using group name "EZVPN" with key "CISCO" along with Xauth username/password "CISCO/CISCO1234":




```
R2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
6     136.1.122.2     136.1.121.200            3des md5       2  23:56:53 CX
5     136.1.122.2     136.1.121.1              3des md5  psk  2  22:11:34

R2#show cry ipsec sa

interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2

   protected vrf:
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
   current_peer: 136.1.121.200:500
```

```
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.200
     path mtu 1500, media mtu 1500
     current outbound spi: 868AECA9

     inbound esp sas:
      spi: 0x74428D90(1950518672)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2004, flow_id: 5, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4462340/3457)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x868AECA9(2257251497)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2005, flow_id: 6, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4462340/3457)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

   protected vrf:
   local  ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 13, #pkts encrypt: 13, #pkts digest 13
    #pkts decaps: 13, #pkts decrypt: 13, #pkts verify 13
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.1
     path mtu 1500, media mtu 1500
     current outbound spi: FBC85DAB

     inbound esp sas:
      spi: 0xD81A6A49(3625609801)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 3, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4449378/646)
        IV size: 8 bytes
        replay detection support: Y
```

```
inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0xFBC85DAB(4224212395)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2003, flow_id: 4, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4449378/644)
   IV size: 8 bytes
   replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

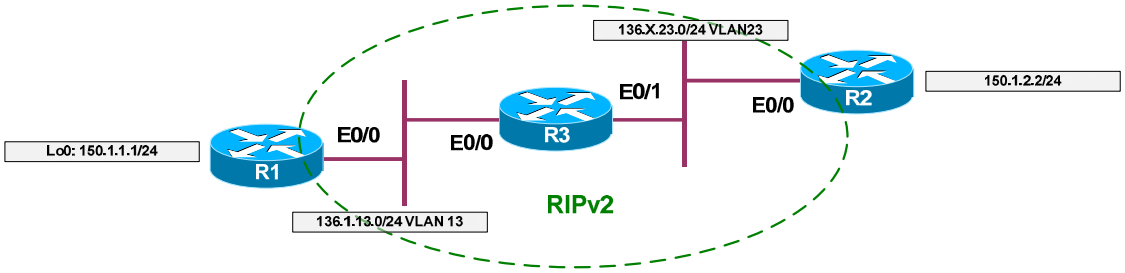
Further Reading

Cisco - DMVPN and Easy VPN Server with ISAKMP Profiles

IOS Firewall

Common Configuration

Objective: Pre-configure devices for IOS firewall scenarios.



Directions

- Create VLANs 13, 23 on SW1 and SW2 and assign switchports to respective VLANs.
- Configure IP addressing as per the diagram, create Loopback0 interfaces on R1 and R2.
- Configure RIP as routing protocol between R1, R2, and R3. Advertise Loopback0 interfaces on R1 and R2 into RIP.

Final Configuration

```
SW1 & SW2:
vlan 13,23
!
! Configure trunks
!
interface range Fa0/21 - 23
 switchport trunk encaps dot1q
 switchport mode trunk

SW1:
interface Fa0/1
 switchport host
 switchport access vlan 13
!
interface Fa0/2
 switchport host
 switchport access vlan 23
!
interface Fa0/3
 switchport host
 switchport access vlan 13

SW2:
interface Fa0/3
```

```
 switchport host
 switchport access vlan 23

R1:
interface E0/0
 no shut
 ip address 136.1.13.1 255.255.255.0
!
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0

R2:
interface E0/0
 no shut
 ip address 136.1.23.2 255.255.255.0
!
interface Loopback0
 ip address 150.1.2.2 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0

R3:
interface E0/0
 no shut
 ip address 136.1.13.3 255.255.255.0
!
interface E0/1
 no shut
 ip address 136.1.23.3 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
```

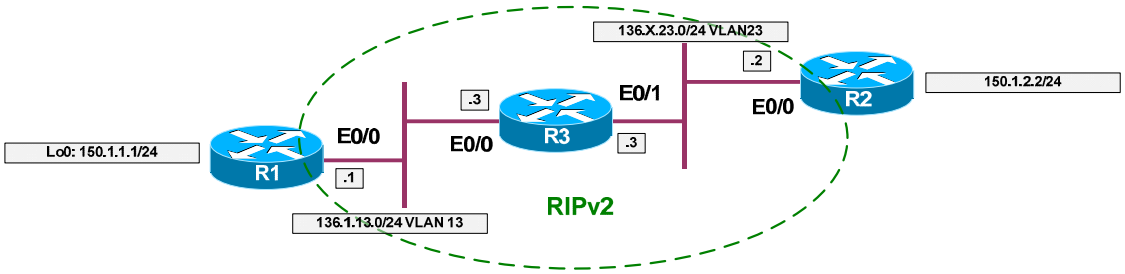
Verification

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set

     136.1.0.0/24 is subnetted, 2 subnets
C       136.1.13.0 is directly connected, Ethernet0/0
R       136.1.23.0 [120/1] via 136.1.13.3, 00:00:01, Ethernet0/0
     150.1.0.0/24 is subnetted, 2 subnets
R       150.1.2.0 [120/2] via 136.1.13.3, 00:00:01, Ethernet0/0
C       150.1.1.0 is directly connected, Loopback0

R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     136.1.0.0/24 is subnetted, 2 subnets
R       136.1.13.0 [120/1] via 136.1.23.3, 00:00:09, Ethernet0/0
C       136.1.23.0 is directly connected, Ethernet0/0
     150.1.0.0/24 is subnetted, 2 subnets
C       150.1.2.0 is directly connected, Loopback0
R       150.1.1.0 [120/2] via 136.1.23.3, 00:00:09, Ethernet0/0

R2#ping 150.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 4/4/4 ms
```

Basic Access-Lists

Objective: Configure router to implement basic filtering policy using extended access-lists.



Directions

- Configure devices as per the scenarion "IOS Firewall/Access Lists" "Common Configuration".
- Conside R1 to be on the inside of the firewall, and R2 on the outside.
- Apply ingress and egress access-lists to interface E0/1 of R3.
- The security policy states the following permissions for inside networks:
    - Permit access to WWW applications.
    - Permit remote access to outside servers via standard virtual terminal access protocols.
    - Permit access to e-mail send/receive services.
    - Inside users should be able use outside DNS and access outside FTP servers by means of active FTP mode.
    - Inside users should be able to traceroute and ping to outside.
- The security policy states the following permissions for outside networks:
    - Inside server at IP address "150.1.1.1" should be accessible from outside via HTTP and active FTP.
    - Inside server should be protected from "fragmented" attacks.
    - Packets for sessions initiated from inside should be permitted. For TCP sessions, use only one line of access-list configuration.
    - Make sure pMTU discovery process works.
- The key problem with basic access-list is that they have no idea of sessions tracking, i.e. they are stateless. So if you permit a packet from inside wint egress ACL, you should make sure that there is a mirrored entry within ingress ACL.
- Rememember the common protocols port numbers.

- Also, keep in mind that popular FTP protocol has two functional modes:
    - Active, where client connects to server on port 21, and server opens data connection source from port 20 back to client on port specified by client.
    - Passive, where client connects to server, server tells client the port number for data connection, and client initiates data connection on that port.

- Know that common UNIX and IOS traceroute implementation sends out UDP packets on port range “33434-33464” by default, and awaits two kinds of ICMP messages in reply “Time-Exceeded” or “Port-Unreachable”.
- Additionally, pMTU discovery process needs ICMP message type 3 with code 4 “Packet too Big” to be permitted from outside.
- Remember that you may permit packets from established TCP session using keyword “established” in access-list entry. It actually matches any packets having “ACK” or “RST” bits set.
- You can match non-initial fragments of IP traffic using “fragments” keyword. Remember tht non-initial fragments have no information about upper level protocol, such as ports.
- Always remember that router-generated traffic is not inspected by egress access-lists. However, the returning traffic is subject to check by ingress ACL, so make sure you permitted any routing and management traffic.
- Make a useful habit of adding an explicit “deny ip any any log” at the end of your access-lists. This may greatly easy the troubleshooting on your lab exam.
- Bearing this in mind, create an extended access-list OUTBOUND to reflect security policy as follows:
    - Permit TCP from any to ports 80, 443, 23, 22, 25, 110/143 (HTTP, HTTPs, Telnet, SSH, SMTP, POP3/IMAP)
    - Permit UDP from any to port 53 (DNS)
    - Permit TCP from any to ports 21, 20 (Active FTP)
    - Permit UDP from any to port range 33434 33464 (UNIX style traceroute)
    - Permit ICMP echo from any to any
    - Permit TCP from host 150.1.2.100 ports 80 and 20, 21 to any (HTTP/Active FTP traffic returning from internal server)

- Create an extended access-list INBOUND as follows:
    - Permit RIP traffic
    - Deny any non-initial fragments to internal servers’ global address
    - Permit TCP from any to 150.1.2.100 ports 80 and 20, 21 (HTTP, FTP)
    - Permit TCP established sessions from any

- Permit returning DNS traffic
- Permit inbound ICMP echo-reply, port-unreachable, and time-exceeded (Ping-reply, Traceroute)
- Permit inbound ICMP packet-too-big (pMTU discovery)

Final Configuration

```
R3:
!
! Egress ACL
!
ip access-list extended OUTBOUND

 remark == HTTP/HTTPs
 remark == SSH/Telnet

 permit tcp any any eq 80
 permit tcp any any eq 443
 permit tcp any any eq 22
 permit tcp any any eq 23

 remark == SMTP POP3/IMAP DNS

 permit tcp any any eq 25
 permit tcp any any eq 110
 permit tcp any any eq 143
 permit udp any any eq 53

 remark == FTP, Traceroute, Pings

 permit tcp any any range 20 21
 permit udp any any range 33434 33464
 permit icmp any any echo

 remark == Traffic from internal server (HTTP/FTP)

 permit tcp host 150.1.1.1 eq 80 any
 permit tcp host 150.1.1.1 range 20 21 any

 deny ip any any log
!
! Ingress ACL
!
ip access-list extended INBOUND

 remark == Permit inbound RIP updates

 permit udp any any eq rip

 remark == Block non-initial frags to server

 deny ip any host 150.1.1.1 fragments

 remark == Permit HTTP/Active FTP to server

 permit tcp any host 150.1.1.1 eq 80
 permit tcp any host 150.1.1.1 range 20 21

 remark == Returning TCP traffic for inside TCP session
```

```
 permit tcp any any established

 remark == Active FTP data channel

 permit tcp any eq 20 any

 remark == Returning DNS traffic

 permit udp any eq 53 any

 remark == Pings, Traceroute and pMTU disc returning traffic

 permit icmp any any echo-reply
 permit icmp any any port-unreachable
 permit icmp any any time-exceeded
 permit icmp any any packet-too-big

 deny ip any any log

!
! Apply access-lists
!
interfac  E0/1
  ip access-group OUTBOUND out
  ip access-group INBOUND in
```

Verification

```
R3#show ip access-lists
Extended IP access list INBOUND
    10 permit udp any any eq rip (8 matches)
    20 deny ip any host 150.1.1.1 fragments
    30 permit tcp any host 150.1.1.1 eq www
    40 permit tcp any host 150.1.1.1 range ftp-data ftp
    50 permit tcp any any established
    60 permit tcp any eq ftp-data any
    70 permit udp any eq domain any
    80 permit icmp any any echo-reply
    90 permit icmp any any port-unreachable
    100 permit icmp any any time-exceeded
    110 permit icmp any any packet-too-big
    120 deny ip any any log

Extended IP access list OUTBOUND
    10 permit tcp any any eq www
    20 permit tcp any any eq 443
    30 permit tcp any any eq 22
    40 permit tcp any any eq telnet
    50 permit tcp any any eq smtp
    60 permit tcp any any eq pop3
    70 permit tcp any any eq 143
    80 permit udp any any eq domain
    90 permit tcp any any range ftp-data ftp
    100 permit udp any any range 33434 33464
    110 permit icmp any any echo
    120 permit tcp host 150.1.1.1 eq www any
    130 permit tcp host 150.1.1.1 range ftp-data ftp any
    140 deny ip any any log

R1#ping 150.1.2.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

R1#trace 150.1.2.2

Type escape sequence to abort.
Tracing the route to 150.1.2.2

  1 136.1.13.3 4 msec 0 msec 0 msec
  2 136.1.23.2 4 msec *  0 msec

R1#telnet 150.1.2.2
Trying 150.1.2.2 ... Open


Password required, but none set

[Connection to 150.1.2.2 closed by foreign host]
R1#telnet 150.1.2.2 80
Trying 150.1.2.2, 80 ... Open

R1#disc 1
Closing connection to 150.1.2.2 [confirm]

R1#telnet 150.1.2.2 8080
Trying 150.1.2.2, 8080 ...
% Destination unreachable; gateway or host down

R3#show ip access-lists
Extended IP access list INBOUND
    10 permit udp any any eq rip (34 matches)
    20 deny ip any host 150.1.1.1 fragments
    30 permit tcp any host 150.1.1.1 eq www
    40 permit tcp any host 150.1.1.1 range ftp-data ftp
    50 permit tcp any any established (16 matches)
    60 permit tcp any eq ftp-data any
    70 permit udp any eq domain any
    80 permit icmp any any echo-reply (11 matches)
    90 permit icmp any any port-unreachable (2 matches)
    100 permit icmp any any time-exceeded
    110 permit icmp any any packet-too-big
    120 deny ip any any log
Extended IP access list OUTBOUND
    10 permit tcp any any eq www (12 matches)
    20 permit tcp any any eq 443
    30 permit tcp any any eq 22
    40 permit tcp any any eq telnet (20 matches)
    50 permit tcp any any eq smtp
    60 permit tcp any any eq pop3
    70 permit tcp any any eq 143
    80 permit udp any any eq domain
    90 permit tcp any any range ftp-data ftp
    100 permit udp any any range 33434 33464 (3 matches)
    110 permit icmp any any echo (10 matches)
    120 permit tcp host 150.1.1.1 eq www any
    130 permit tcp host 150.1.1.1 range ftp-data ftp any
    140 deny ip any any log (1 match)

R2>ping 150.1.1.1

Type escape sequence to abort.
```

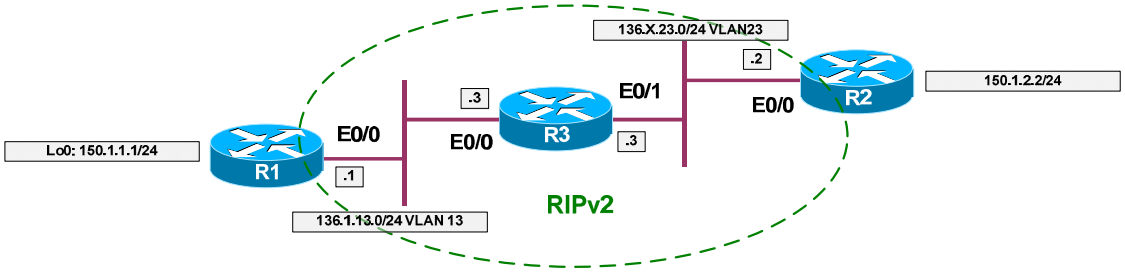
```
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

R2>telnet 150.1.1.1 80
Trying 150.1.1.1, 80 ... Open

R2>disc 1
Closing connection to 150.1.1.1 [confirm]
```

Further Reading

Transit Access Control Lists: Filtering at Your Edge
Path Maximum Transmission Unit (PMTU) Black Hole-Router
Cisco - Access Control Lists and IP Fragments

Reflexive Access-Lists

Objective: Configure router to filter traffic using reflexive access-lists.



Directions

- Configure devices as per the scenario "IOS Firewall/Access Lists" "Common Configuration".
- The goal is to permit TCP/UDP/ICMP traffic from R1 to R2, but not vice versa. This could be achieved using the concept of reflective ACL.
- The idea of reflexive ACL is pretty simple: take a packet flow, extract session information (src/dst IP and ports) and create dynamic entry in access-list that is applied in opposite direction, to permit the "mirrored" traffic flow.
- This basic "session" idea works well with most simple protocols, like HTTP and Telnet. However, complex protocols like FTP has more complex behavior, which could not be interpreted properly by simply reflecting a traffic flow.
- Additionally, reflexive ACLs scales poorly, since router open all the pinholes temporarily and needs to age them out, constantly keeping the track of every new "session".
- Also, by default a router-originated traffic is not subject to "reflection", unless you use local policy routing to divert it into loopback interface, therefore making it "ingress".
- Create access-list OUTBOUND on R3 as follows:
    - Permit TCP traffic from any to any, and reflect sessions into access-list named "MIRROR".
    - Configure the same behavior for ICMP and UDP traffic.
- Create access-list INBOUND on R3 as follows:
    - Evaluate the access list named "MIRROR", i.e. permit only the mirrored sessions.

- Additionally, in order to “reflect” the local router RIP updates, create local policy routing as follows:
    - Create named access-list “RIP” and match UDP traffic from any to any port 520.
    - Create interface Loopback0 with arbitraty IP address.
    - Create route-map named “LOCAL”:
        - Match access-list “RIP” and set interface Loopback0
        - Apply this route-map as local policy.

Final Configuration

R3:

```
!
! Outbound access-list, mirror all outbound sessions
!
ip access-list extended OUTBOUND
 permit tcp any any reflect MIRROR
 permit udp any any reflect MIRROR
 permit icmp any any reflect MIRROR
!
! Ingress ACL, permit only the “returning” packets
!
ip access-list extended INBOUND
 evaluate MIRROR
!
! Select RIP traffic
!
ip access-list extended RIP
 permit udp any any eq rip
!
! Create loopback for PBR
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.0
!
! Create route-map to divert RIP traffic to loopback
!
route-map LOCAL 10
 match ip address RIP
 set interface Loopback0
!
ip local policy route-map LOCAL
!
! Apply ACLs
!
interface E0/1
 ip access-group OUTBOUND out
 ip access-group INBOUND in
```


Verification

With some IOS versions, local policy routing may refuse to route multicast packets. Configure static RIP neighbors in such case:

```
R3:
router rip
 neighbor 136.1.23.2
 passive E0/1

R2:
router rip
 neighbor 136.1.23.3
 passive E0/0

R3#show ip access-lists
Extended IP access list INBOUND
    10 evaluate MIRROR
Reflexive IP access list MIRROR
     permit udp host 136.1.23.2 eq rip host 136.1.23.3 eq rip (13 matches)
(time left 297)
Extended IP access list OUTBOUND
    10 permit tcp any any reflect MIRROR
    20 permit udp any any reflect MIRROR
    30 permit icmp any any reflect MIRROR
Extended IP access list RIP
    10 permit udp any any eq rip (15 matches)


R1>telnet 150.1.2.2
Trying 150.1.2.2 ... Open

R2>

R3#show ip access-lists
Extended IP access list INBOUND
    10 evaluate MIRROR
Reflexive IP access list MIRROR
     permit tcp host 150.1.2.2 eq telnet host 136.1.13.1 eq 11009 (31 matches)
(time left 294)
     permit udp host 136.1.23.2 eq rip host 136.1.23.3 eq rip (18 matches)
(time left 295)
Extended IP access list OUTBOUND
    10 permit tcp any any reflect MIRROR
    20 permit udp any any reflect MIRROR
    30 permit icmp any any reflect MIRROR
Extended IP access list RIP
    10 permit udp any any eq rip (19 matches)

R1>ping 150.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R1>

R3#show ip access-lists MIRROR
Reflexive IP access list MIRROR
     permit icmp host 150.1.2.2 host 136.1.13.1  (19 matches) (time left 292)
     permit udp host 136.1.23.2 eq rip host 136.1.23.3 eq rip (25 matches)
```

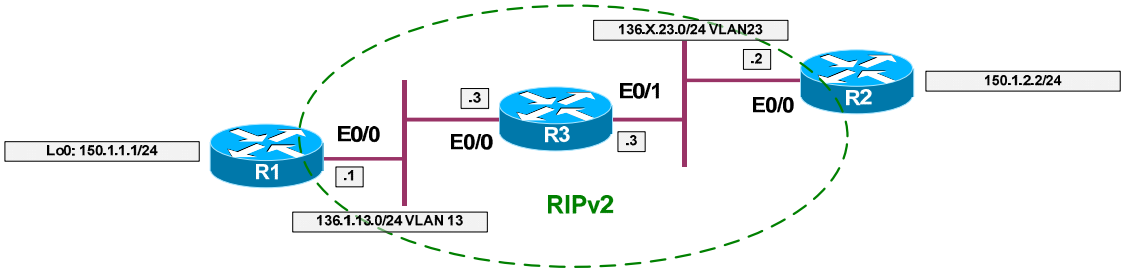
```
(time left 291)
```

Further Reading

Configuring IP Session Filtering (Reflexive Access Lists)
Cisco - Configuring Commonly Used IP ACLs

Dynamic Access-Lists

Objective: Configure router for lock & key security with local AAA.



Directions

- Configure devices as per the scenario "IOS Firewall/Access Lists" "Common Configuration".
- Dynamic access-list is a type of access policy which is activated by a user logging into router.
- The key factor here is "access-enable" command, which activates all dynamic access entries in all access-lists.
- This command may be assigned to a particular user's profile, or be attached to a virtual terminal line.
- You may pass two optional arguments to "access-enable" command:
    - The "host" keyword, which create dynamic ACL entry ONLY for a host that triggered the authentication session.
    - The "timeout" keyword, which specifies inactivity timeout to remove the dynamic ACL entry.
- While creating dynamic template entry in access-list you may also specify "absolute" timeout with "timeout" keyword.
- If you have configured AAA on a router, remember to configure "exec" authorization appropriately, as by default exec commands are not authorized.
- To apply the dynamic ACL feature with AAA configure as follows:
    - Enable AAA, configure and apply AAA list to disable console authentication.
    - Configure local "exec" authorization.
    - Create user named "CISCO" with password "CISCO1234" and assign it autocommand "access-enable host timeout 10".
    - Create access-list "INBOUND" as follows:
        - Permit telnet traffic to IP address 136.X.23.3 (E0/1 of R3).
        - Permit RIP updates inbound.

- With dynamic entry named ACCESS permit ICMP traffic from any to any. Specify absolute timeout of 30 minutes.
- Deny and log everything else.

o Apply acess-list INBOUND to interface Ethernet 0/1 of R3.

- By configuring global command “access-list dynamic-extended” you permit users to extend absolute timeout by fixed value every time they re-authenticate with router.

Final Configuration

```
R3:
aaa new-model
aaa authentication login CONSOLE none
aaa authorization exec default local
!
username CISCO password CISCO1234
username CISCO autocommand access-enable host timeout 10
!
line con 0
 login authentication CONSOLE
!
! Ingress ACL with dynamic templates
!
ip access-list extended INBOUND
 permit tcp any host 136.1.23.3 eq 23
 permit udp any any eq 520
 dynamic ACCESS timeout 30 permit icmp any any
 deny ip any any log
!
!
!
interface E0/1
 ip access-group INBOUND in
```

Verification

```
R3#show ip access-lists
Extended IP access list INBOUND
    10 permit tcp any host 136.1.23.3 eq telnet
    20 permit udp any any eq rip (48 matches)
    30 Dynamic ACCESS permit icmp any any
    40 deny ip any any log
Extended IP access list RIP
    10 permit udp any any eq rip (271 matches)

R2#telnet 136.1.23.3
Trying 136.1.23.3 ... Open


User Access Verification

Username: CISCO
Password: CISCO1234
```

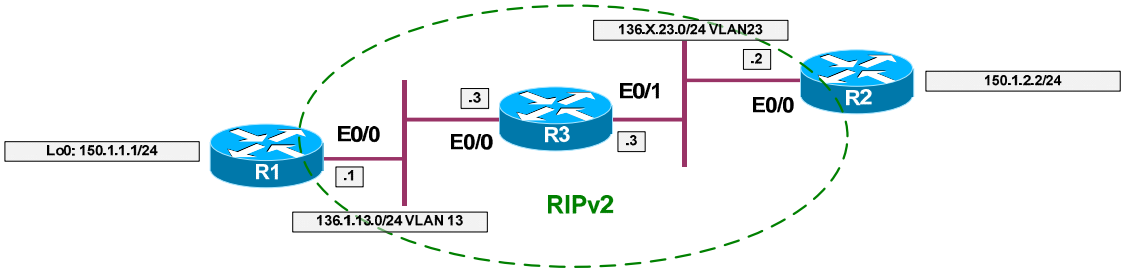
```
[Connection to 136.1.23.3 closed by foreign host]

R3#show ip access-lists
Extended IP access list INBOUND
    10 permit tcp any host 136.1.23.3 eq telnet (723 matches)
    20 permit udp any any eq rip (93 matches)
    30 Dynamic ACCESS permit icmp any any
       permit icmp host 136.1.23.2 any
    40 deny ip any any log
Extended IP access list RIP
    10 permit udp any any eq rip (291 matches)

R2#ping 150.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R2#

R3#show ip access-lists
Extended IP access list INBOUND
    10 permit tcp any host 136.1.23.3 eq telnet (723 matches)
    20 permit udp any any eq rip (96 matches)
    30 Dynamic ACCESS permit icmp any any
       permit icmp host 136.1.23.2 any (5 matches) (time left 595)
    40 deny ip any any log
Extended IP access list RIP
    10 permit udp any any eq rip (291 matches)
```

📖 Further Reading

Configuring Lock-and-Key Security (Dynamic Access Lists)

Stateful Inspection with CBAC

Objective: Configure router for stateful inspection of session traffic.



Directions

- Configure devices as per the scenario "IOS Firewall" "Common Configuration".
- CBAC is a stateful IOS firewall feature. Unlike reflexive ACL is has more intelligence, inspecting session traffic and parsing protocol operations.
- The way CBAC originally worked was as follows:
    - Apply pre-configured inspection rule to egress/ingress traffic (depends on configuration). Find out if there are any additional sessions that a protocol intiates (like FTP).
    - If there is an access-list configured in direction opposite to traffic flow, open a temporaty pinhole in it, permitting session traffic to come back.
    - Additionally, parse the protocol state-machine to find any misbehavior.
- With recent IOS versions, CBAC no longer "patch" access-lists, rather returning traffic is matched directly against state-table. This speed up the actual firewall traffic processing, but you won't see any more "pinholes" in access-lists.
- In this task we are going to apply the simple form of traffic inspection, processing generic TCP, UDP and ICMP sessions. Note that ICMP inspection as a new 12.2T feature, that was unavailable in original CBAC. With 12.3T an inspection of router-generated traffic was also added.
- Create inspection rule named INSPECT as follows:
    - Inspect TCP, UDP, ICMP traffic.
    - Additionally, inspect FTP traffic.
- Create access-list named "INBOUND" as follows:
    - Permit RIP routing updates
    - Deny & log everything else.

- Apply access-group “INBOUND” to E0/1 ingress direction.
- Apply inspection rule “INSPECT” to egress direction on interface E0/1.

Final Configuration

```
R3:
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
ip inspect name INSPECT icmp
!
! FTP-specific inspection
! Uses port-map to apply the rule
!
ip inspect name INSPECT ftp

ip access-list extended INBOUND
 permit udp any any eq rip
 deny ip any any log

interface E0/1
 ip access-group INBOUND in
 ip inspect INSPECT out
```

Verification

```
R3#show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name INSPECT
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    ftp alert is on audit-trail is off timeout 3600

Interface Configuration
 Interface Ethernet0/1
  Inbound inspection rule is not set
  Outgoing inspection rule is INSPECT
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    ftp alert is on audit-trail is off timeout 3600
  Inbound access list is INBOUND
  Outgoing access list is not set

R3#show ip access-lists
Extended IP access list INBOUND
    10 permit udp any any eq rip (21 matches)
    20 deny ip any any log

R3#show ip port-map ftp
```

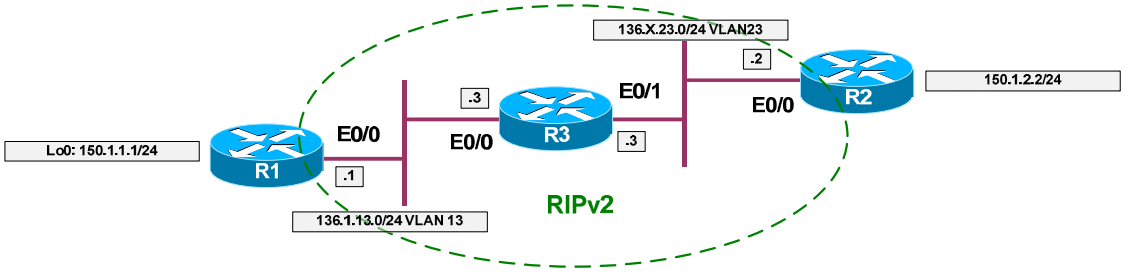
```
Default mapping: ftp              port 21                  system defined

Inspection is not applied to route-generated traffic:

R3#ping 150.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:

*Mar  1 17:01:17.914: %SEC-6-IPACCESSLOGDP: list INBOUND denied icmp 150.1.2.2
-> 136.1.23.3 (0/0), 1 packet.....
Success rate is 0 percent (0/5)

R1#ping 150.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
R1#

R3#sh ip acce
Extended IP access list INBOUND
     permit icmp any host 136.1.13.1 time-exceeded
     permit icmp any host 136.1.13.1 unreachable
     permit icmp any host 136.1.13.1 timestamp-reply
     permit icmp any host 136.1.13.1 echo-reply (5 matches)
    10 permit udp any any eq rip (99 matches)
    20 deny ip any any log (5 matches)

R1#telnet 150.1.2.2
Trying 150.1.2.2 ... Open

R2>

R3#show ip inspect sessions
Established Sessions
 Session 82C79F24 (136.1.13.1:11010)=>(150.1.2.2:23) tcp SIS_OPEN

R3#sh ip acce
Extended IP access list INBOUND
     permit tcp host 150.1.2.2 eq telnet host 136.1.13.1 eq 11010 (8 matches)
    10 permit udp any any eq rip (105 matches)
    20 deny ip any any log (5 matches)
```

📖 Further Reading

Configuring Context-Based Access Control

CBAC Port-to-Application Mapping

Objective: Configure router to use non-standard ports for traffic inspection.



Directions

- Configure devices as per the scenario "IOS Firewall" "Stateful Inspection with CBAC".
- Imagine we have a web-server at 150.X.2.2 listening on port 21 and FTP server somewhere on outside network listening on port 8080.
- To inspect an application traffic, CBAC has a table of port-mappings. There are some system defined ports, like "21,80,25". You can not map HTTP service to port 21 directly, since it's system-defined. However, you can use an acess-list to specify list of "server" which have standard port re-mapped.
- Create a standard access-list number 99 and permit host 150.X.2.2 with it.
- Map application "HTTP" to port 21 for servers in access-list 99.
- Map FTP protocol to port 8080 globally.
- Add protocol HTTP to inspection rule "INSPECT".

Final Configuration

```
R3:
access-list 99 permit host 150.1.2.2
!
ip port-map http port 21 list 99
ip port-map ftp port 8080
!
ip inspect name INSPECT http
```

Verification

```
R3(config)#ip port-map http port 21
Command fail: the port 21 has already been defined for ftp by the system.
              No change can be made to the system defined port mappings.

R3(config)#ip port-map http port 21 list 99

R3#show ip port-map | inc http
Host specific:   http            port 21     in list 99   user defined
```

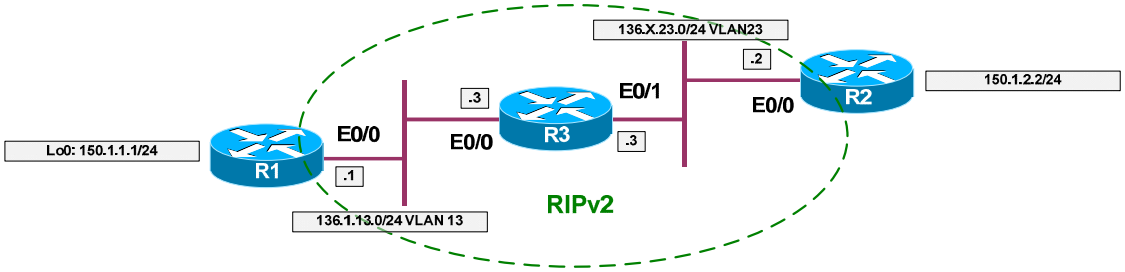
```
Default mapping: http             port 80                  system defined

R3#show ip port-map | inc ftp
Default mapping: tftp             port 69                  system defined
Default mapping: ftp              port 21                  system defined
Default mapping: ftp              port 8080                user defined
```

Further Reading

Configuring Port to Application Mapping

Preventing DoS Attacks with CBAC

Objective: Configure router limit number of half-open sessions with CBAC feature.



Directions

- Configure devices as per the scenario "IOS Firewall" "Common Configuration".
- In addition to protocol inspection CBAC has built-in DoS prevention feature, similar to TCP intercept.
- However, in contrast to TCP intercept, CBAC intercept works with any inspected session, even UDP.
- The only supported mode, in comparsion with TCP intercept, is "watch" mode: sessions are not proxied and are rather monitored. The equivalent to TCP Intercept "watch-timeout" is "tcp synwait-time" with CBAC.
- CBAC cessions are limited using two basic rate-limiting features:
    - Total number of half-open (non-established) session.
    - One-minute half-open sessions rate.
    - There are high and low limits for both limits.
- For TCP you may specify additional parameters as follows:
    - Connection establishment/inactivity/teardown timeouts.
    - Per-host limits & block time.
- You may also specify UDP sessions timeout and DNS session timeout separately.
- CBAC intercept feature is usually implemented to protect servers, rather than control users sessions, though there may be exceptions.
- Create inspection rule "PROTECT" as follows:
    - Inspect TCP, UDP and ICMP traffic.
- Configure global CBAC intercept parameters as follows:
    - Start clamping when total number of half-open sessions reaches 1000, and stop when it falls below 900.

- o Start clamping when one-minute rate reaches 100 and stop when it falls below 90.
- o Set per-host limit of half-open sessions to 50. Block a host for 5 minutes when the threshold is reached.
- o Set number of seconds spent in connection establishment phase for TCP to 15 seconds.

- Create an extended access-list named “INBOUND” as follows:
  - o Permit RIP updates.
  - o Deny and log everything else.

- Apply inspection rule named “PROTECT” outbound on E0/0.
- Apply access-list “INBOUND” ingress on E0/0.

Final Configuration

```
R3:
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1000
ip inspect one-minute low 90
ip inspect one-minute high 100
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 50 block-time 5
!
ip inspect name PROTECT tcp
ip inspect name PROTECT udp
ip inspect name PROTECT icmp
!
ip access-list extended INBOUND
 permit udp any any eq rip
 deny ip any any log
!
interface E0/0
 ip inspect PROTECT out
 ip access-group INBOUND in
```

Verification

```
R3#show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [90:100] connections
max-incomplete sessions thresholds are [900:1000]
max-incomplete tcp connections per host is 50. Block-time 5 minutes.
tcp synwait-time is 15 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name PROTECT
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
```



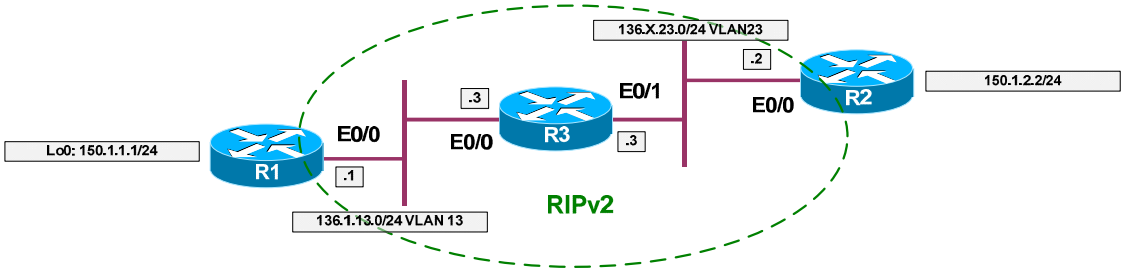
```
Interface Configuration
 Interface Ethernet0/0
  Inbound inspection rule is not set
  Outgoing inspection rule is PROTECT
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
  Inbound access list is INBOUND
  Outgoing access list is not set

Check to see if TCP SYN Wait timeout works:

R3#debug ip inspect events
INSPECT special events debugging is on
R3#

R2#telnet 150.1.1.100 3030
Trying 150.1.1.100, 3030 ...
% Connection timed out; remote host not responding

R3#
*Mar  1 18:54:42.877: CBAC 136.1.23.2:11011 <- RST (150.1.1.100:3030) seq 0 wnd
4128
*Mar  1 18:54:42.877: CBAC (136.1.23.2:11011) RST -> 150.1.1.100:3030 seq
3660436220 wnd 0
```

Further Reading

Configuring Context-Based Access Control

CBAC Performance Tuning

Objective: Tune CBAC for effective router performance.



Directions

- Configure devices as per the scenario "IOS Firewall" "Stateful Inspection with CBAC".
- The core of CBAC algorithm is formed by protocol inspection logic and session state table. In order to make CBAC more effective under heavy load conditions, you should take in accountint the following:
    - State table is hashed structured, with configurable number of entries. Try to make hashtable size close to the average number of concurrect sessions passing through the firewall.
    - By default, protocol inspection logic generates alerts when it finds inconsistence in protocol tracking. This may cause additional CPU load under inensive traffic. Consider disable the alerts globally or per protocol in order to improve performance.
- There's also an additional CBAC feature called session audit. It permits you to log every session statistics for accounting or audit purposes naturally. Audit may be enable globally or per-protocol.
- In order to improve performance, disable CBAC alerts, but retain alerting for ICMP sessions.
- Keeping CBAC audit globally disabled, enable it for TCP sessions only.
- Change hashtable size to 4096, in order to accommodate to intensive traffic flow.

Final Configuration

```
R3:
ip inspect alert-off
!
ip inspect name INSPECT icmp alert on
!
! Audit trails
!
no ip inspect audit-trail
ip inspect name INSPECT tcp audit-trail on
```

Verification

```
R3#show ip inspect all
Session audit trail is disabled
Session alert is dlsabled
one-minute (sampling period) thresholds are [90:100] connections
max-incomplete sessions thresholds are [900:1000]
max-incomplete tcp connections per host is 50. Block-time 5 minutes.
tcp synwait-time is 15 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name INSPECT
    tcp alert is off audit-trail is on timeout 3600
    udp alert is off audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    ftp alert is off audit-trail is off timeout 3600

Interface Configuration
 Interface Ethernet0/1
  Inbound inspection rule is not set
  Outgoing inspection rule is INSPECT
    tcp alert is off audit-trail is on timeout 3600
    udp alert is off audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    ftp alert is off audit-trail is off timeout 3600
  Inbound access list is INBOUND
  Outgoing access list is not set
```

Verify audit trails:

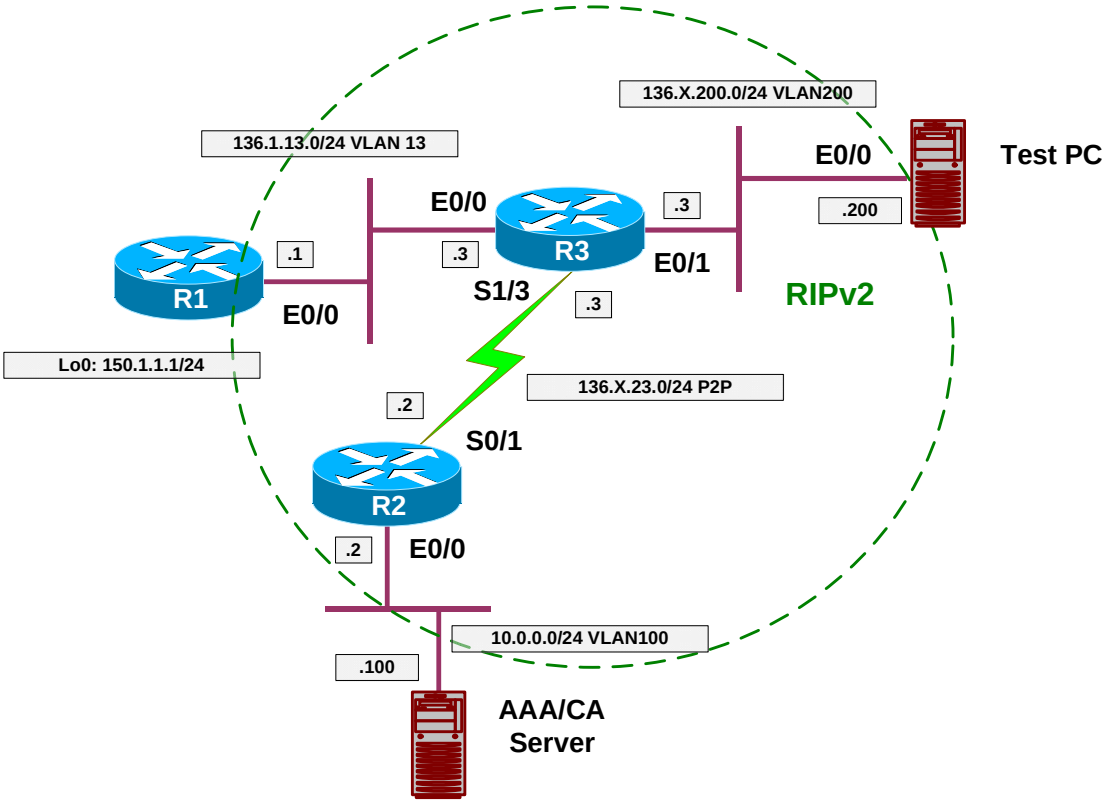
```
R1#telnet 150.1.2.2
Trying 150.1.2.2 ... Open

R2>exit

R3#
*Mar  1 20:34:34.483: %FW-6-SESS_AUDIT_TRAIL: tcp session initiator
(136.1.13.1:11011) sent 36 bytes -- responder (150.1.2.2:23) sent 44 bytes
```

Further Reading

Cisco IOS Firewall Performance Improvements
Configuring Context-Based Access Control

Authentication Proxy with RADIUS

Objective: Configure router to filter traffic based on application-level criteria.



Directions

- Pre-configure devices as follows:
  - Create VLANs 13, 23 and 100.
  - Configure IP addressing on Ethernet interfaces.
  - Configure Serial link between R3 and R2.
  - Configure RIP as routing protocol.
  - Create and advertise into RIP interface Loopback0 on R1.

- The idea behind Authentication Proxy is to download per-user access profile (ACL rules) and merge it with interface access-group.
- To authenticate user, an HTTP session is intercepted and authentication is performed by router.
- Configure Authentication Proxy settings on R3 as follows:
  - Enable AAA; configure & apply AAA list to disable console line authentication. This may have implications with some IOS versions, where HTTP server uses AAA list assigned to console for HTTP

authentication. If this is the case, configure console line in sync with HTTP authentication requirements.
- Configure RADIUS server 10.0.0.100 with key CISCO.
- Configure default login authentication via RADIUS.
- Configure auth-proxy authorization via RADIUS.
- Enable local HTTP server, and configure it to use AAA authentication.
- Create an authentication proxy rule named “PROXY” and apply it to interface E0/1.
- Create access-list 100 as follows:
    - Permit RIP updates.
    - Deny and log everythig else.
    - Apply access-group ingress to interface E0/1

- Configure ACS as follows:
    - Add R3 as RADIUS client.
    - Enable per-user RADIUS attributes and permit “Cisco AV-Pair” in user profiles.
    - Create user “PROXY” with password “CISCO1234” and create the following Cisco AV-Pair attributes:
        - auth-proxy:priv-lvl=15
        - auth-proxy:proxyacl#1=permit icmp any any
        - auth-proxy:proxyacl#2=permit tcp any any

Final Configuration

Pre-Configuration:

SW1 & SW2:
```
vlan 13,200,100
!
! Configure trunks
!
interface range Fa0/21 - 23
 switchport trunk encaps dot1q
 switchport mode trunk
```

SW1:
```
interface Fa0/1
 switchport host
 switchport access vlan 13
!
interface Fa0/2
 switchport host
 switchport access vlan 100
!
interface Fa0/3
 switchport host
 switchport access vlan 13
!
```

```
interface Fa0/20
 switchport host
 switchport access vlan 100
```

SW2:

```
interface Fa0/3
 switchport host
 switchport access vlan 200
!
interface Fa0/20
 switchport host
 switchport access vlan 200
```

R1:

```
interface E0/0
 no shut
 ip address 136.1.13.1 255.255.255.0
!
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
```

R2:

```
interface E 0/0
 no shut
 ip add 10.0.0.2 255.255.255.0
!
interface Ser 0/1
 no shut
 ip address 136.1.23.2 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 10.0.0.0
```

R3:

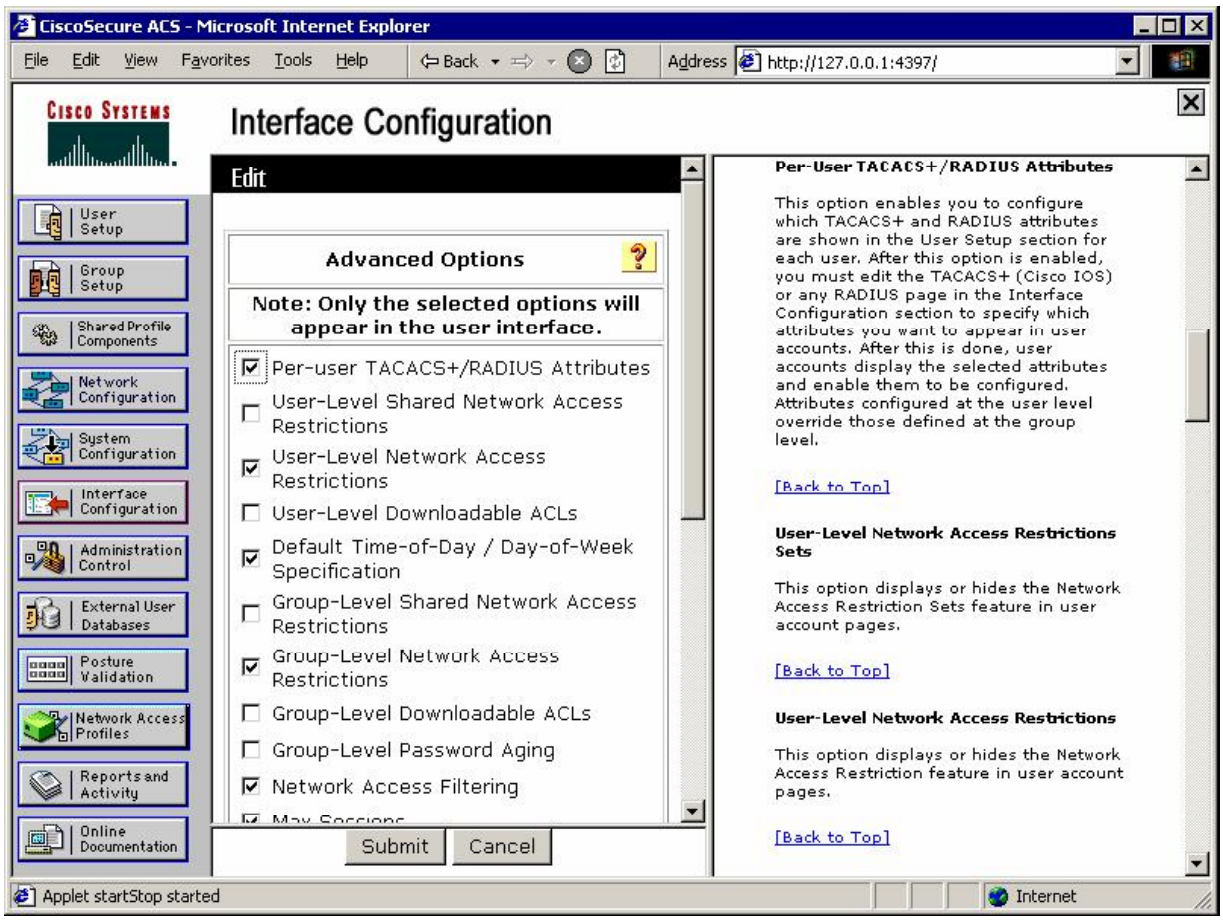
```
interface E 0/0
 no shut
 ip add 136.1.13.3 255.255.255.0
!
interface E 0/1
 no shut
 ip add 136.1.200.3 255.255.255.0
!
interface Serial 1/3
 no shut
 clockrate 64000
 ip address 136.1.23.3 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
```

Auth Proxy:

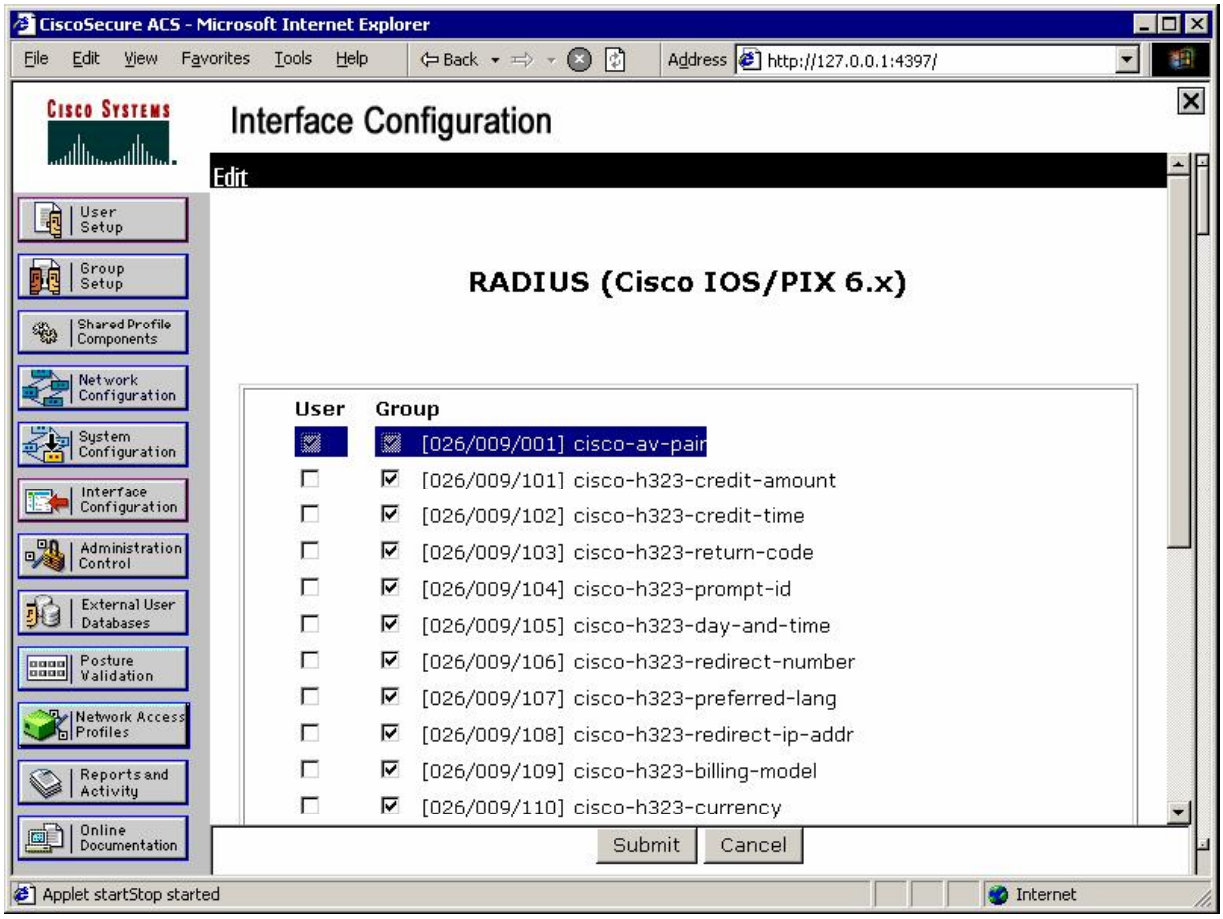
```
R3:
aaa new-model
!
! Safeguard console
!
aaa authentication login CONSOLE none
!
line console 0
 login authentication CONSOLE
!
! Configure AAA settings for auth-proxy
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
!
radius-server host 10.0.0.100 key CISCO

!
! Configure HTTP server & HTTP auth via AAA
!
ip http server
ip http authentication aaa

!
! Auth proxy rule
!
ip auth-proxy name PROXY http

!
! Inbound access-list
!
ip access-list extended 100
 permit udp any any eq RIP
 remark == permit TACACS+/RADIUS traffic
 remark == if you have them on outside interface
 deny ip any any log

interface E0/1
 ip access-group 100 in
 ip auth-proxy PROXY
```


ACS:

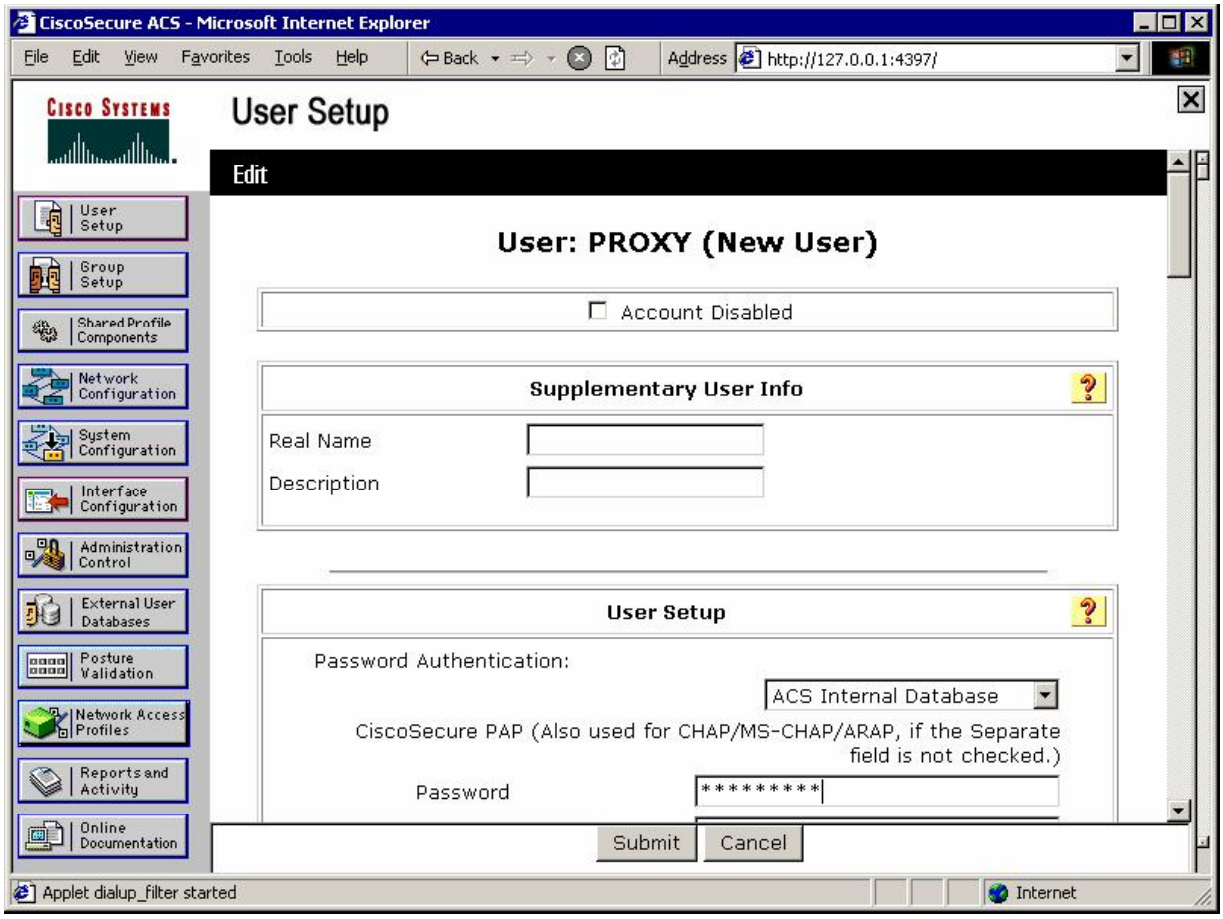
Within Interface Configuration permit per-user TACACS+/RADIUS Attributes:



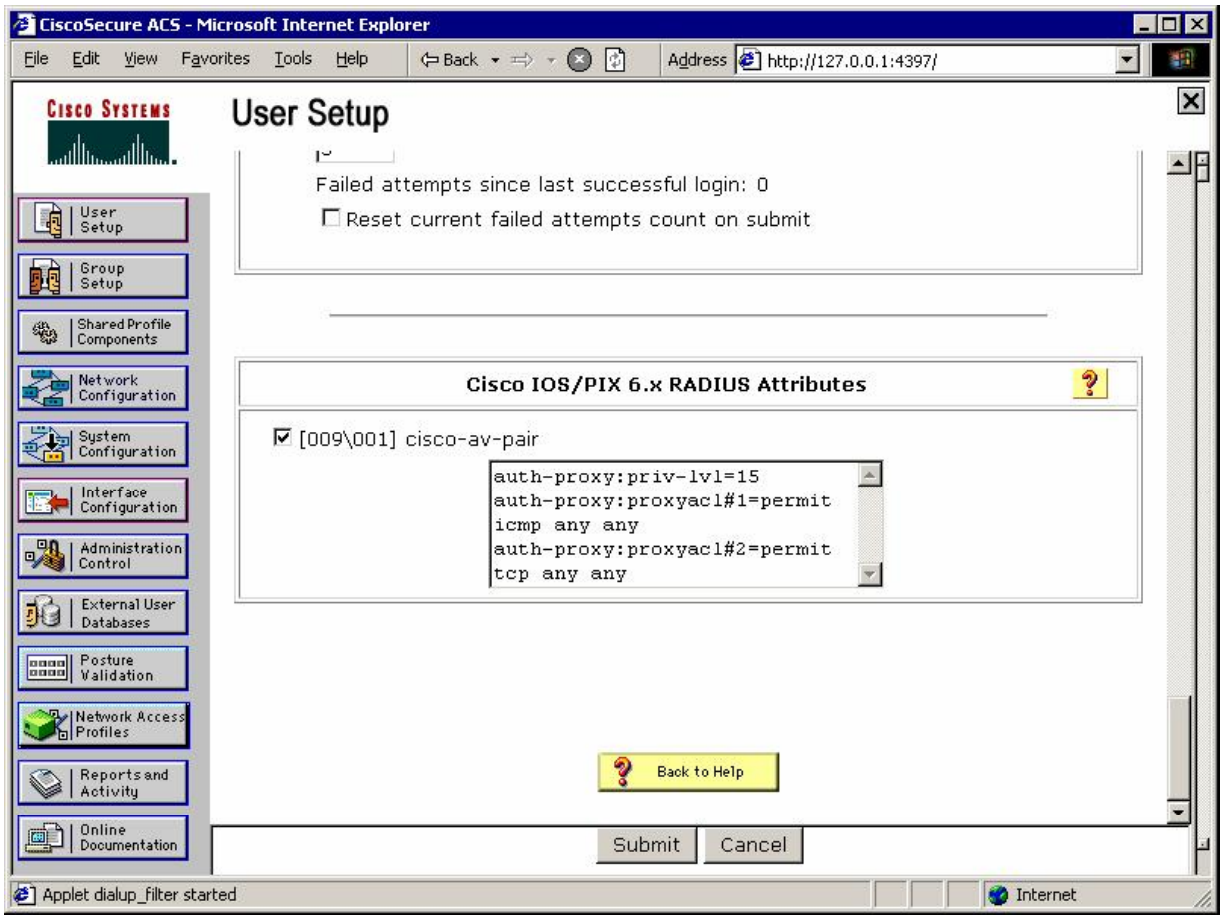
Permit "cisco av-pair" attribute in user profile:



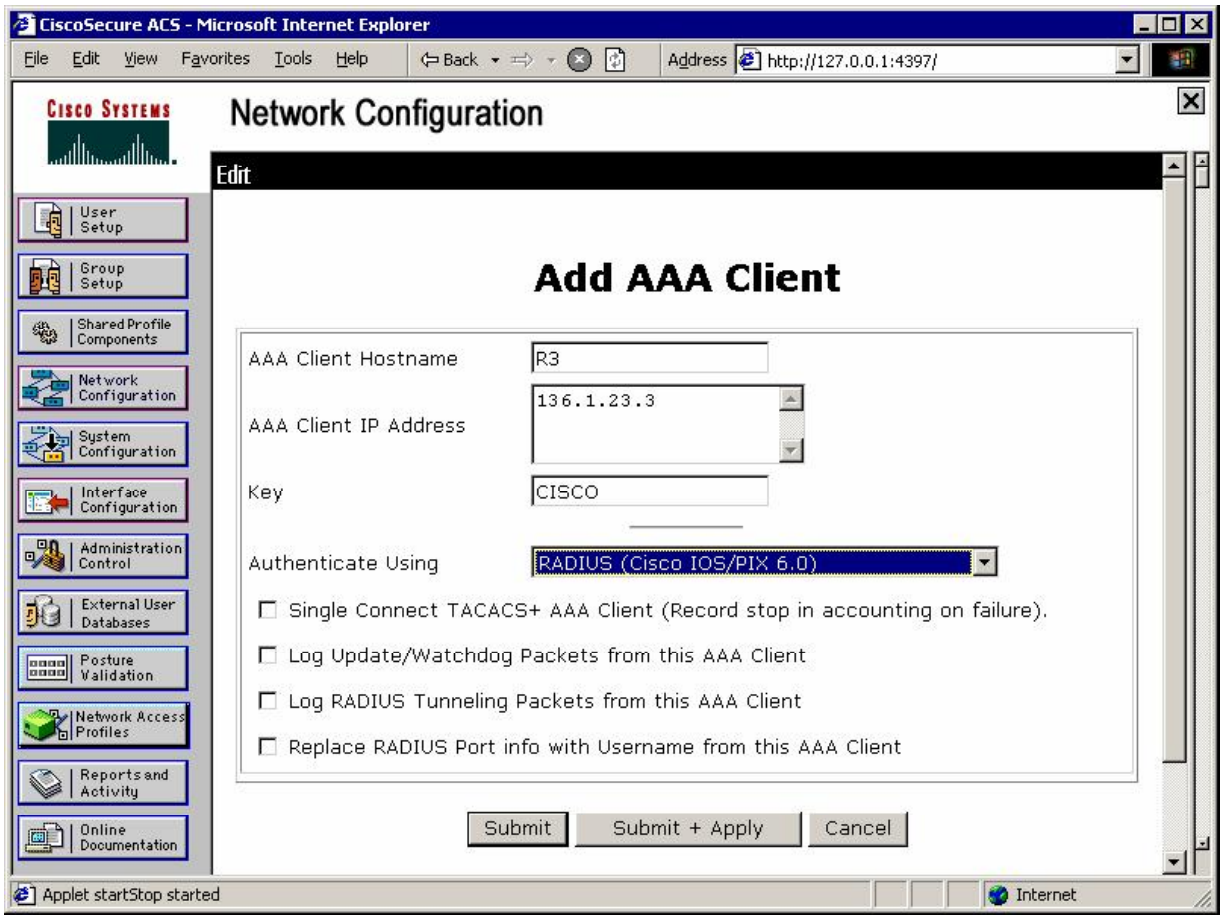
Add new user "PROXY" with password "CISCO1234":



Configure auth-proxy attributes in user profile:



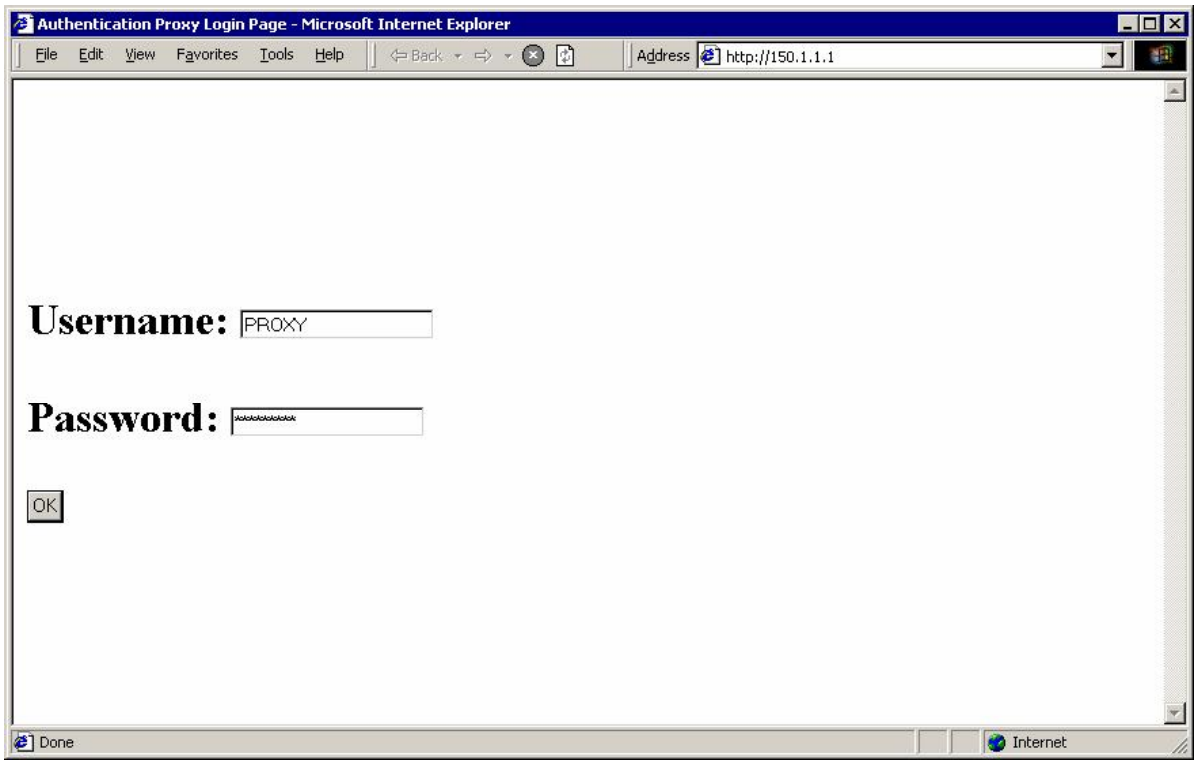
Add R3 as RADIUS client on ACS:

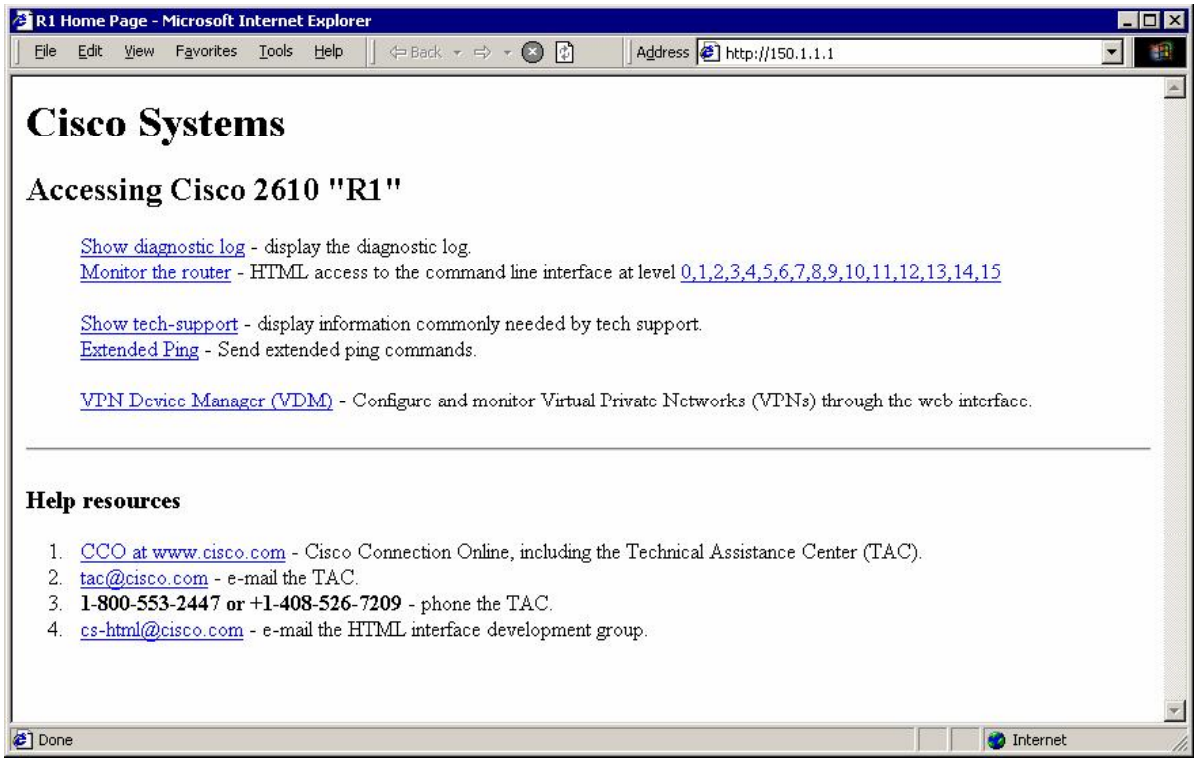


Verification

```
R3#debug aaa authentication
AAA Authentication debugging is on
R3#debug aaa authorization
AAA Authorization debugging is on
R3#debug radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
```

Test PC:






```
<snip>

*Mar  1 22:28:31.315: AAA/AUTHEN/START (4167353654): port='Ethernet0/1'
list='default' action=LOGIN service=LOGIN
*Mar  1 22:28:31.315: AAA/AUTHEN/START (4167353654): found list default
*Mar  1 22:28:31.315: AAA/AUTHEN/START (4167353654): Method=radius (radius)
*Mar  1 22:28:31.319: AAA/AUTHEN(4167353654): Status=GETUSER
*Mar  1 22:28:31.319: AAA/AUTHEN/CONT (4167353654): continue_login
(user='(undef)')
*Mar  1 22:28:31.319: AAA/AUTHEN(4167353654): Status=GETUSER
*Mar  1 22:28:31.319: AAA/AUTHEN(4167353654): Method=radius (radius)
*Mar  1 22:28:31.319: AAA/AUTHEN(4167353654): Status=GETPASS
*Mar  1 22:28:31.319: AAA/AUTHEN/CONT (4167353654): continue_login
(user='PROXY')
*Mar  1 22:28:31.319: AAA/AUTHEN(4167353654): Status=GETPASS
*Mar  1 22:28:31.323: AAA/AUTHEN(4167353654): Method=radius (radius)
*Mar  1 22:28:31.323: RADIUS: Pick NAS IP for u=0x82ECC30C tableid=0
cfg_addr=0.0.0.0 best_addr=136.1.23.3
*Mar  1 22:28:31.323: RADIUS: ustruct sharecount=1
*Mar  1 22:28:31.323: Radius: radius_port_info() success=1 radius_nas_port=1
*Mar  1 22:28:31.323: RADIUS(00000000): Send Access-Request to 10.0.0.100:1645
id 21645/9, len 84
*Mar  1 22:28:31.327: RADIUS:  authenticator BB ED AA B9 32 98 61 51 - A5 9F A7
29 CF 38 AD F0
*Mar  1 22:28:31.327: RADIUS:  NAS-IP-Address      [4]   6   136.1.23.3
*Mar  1 22:28:31.327: RADIUS:  NAS-Port            [5]   6   60001
*Mar  1 22:28:31.327: RADIUS:  NAS-Port-Type       [61]  6   Virtual
[5]
*Mar  1 22:28:31.327: RADIUS:  User-Name           [1]   7   "PROXY"
*Mar  1 22:28:31.331: RADIUS:  Calling-Station-Id  [31]  15  "136.1.200.200"
*Mar  1 22:28:31.331: RADIUS:  User-Password       [2]   18  *
*Mar  1 22:28:31.331: RADIUS:  Service-Type        [6]   6   Outbound
[5]
```

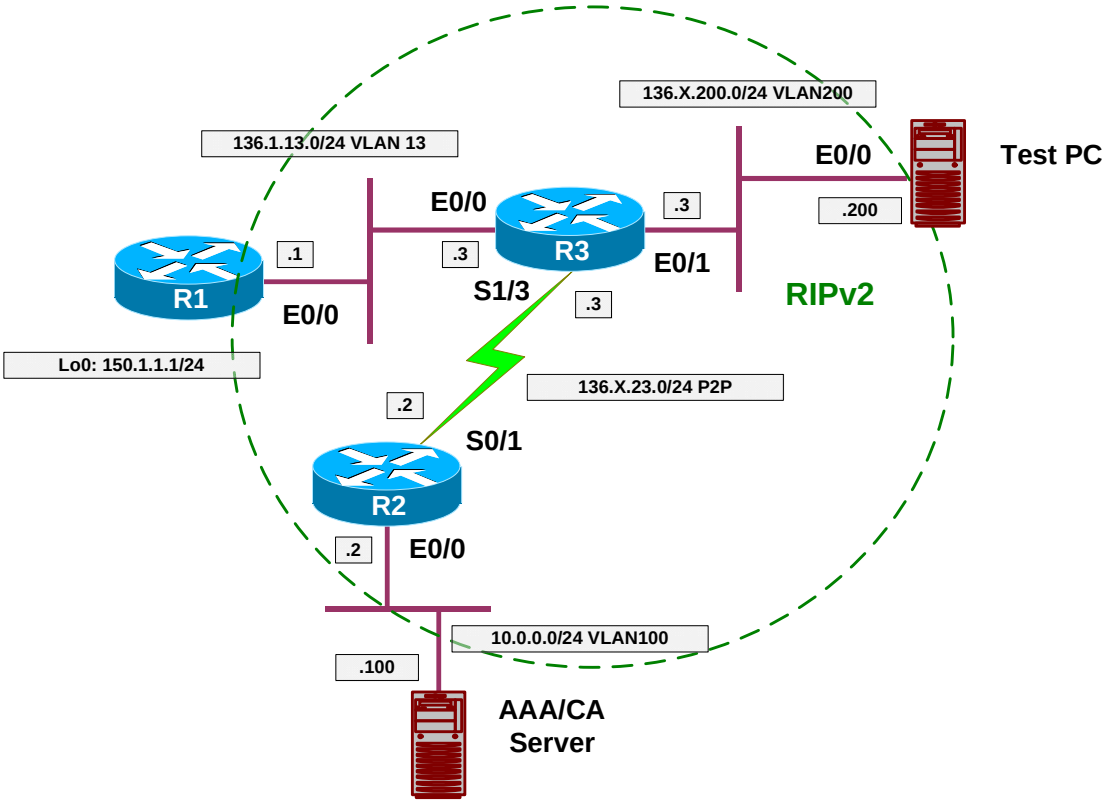
```
*Mar  1 22:28:31.411: RADIUS: Received from id 21645/9 10.0.0.100:1645, Access-
Accept, len 181
*Mar  1 22:28:31.415: RADIUS:  authenticator 35 55 0E 8A 76 28 14 EF - 90 82 89
E1 B6 3D D8 EF
*Mar  1 22:28:31.415: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
*Mar  1 22:28:31.415: RADIUS:  Vendor, Cisco       [26]  30
*Mar  1 22:28:31.415: RADIUS:   Cisco AVpair       [1]   24  "auth-proxy:priv-
lvl=15"
*Mar  1 22:28:31.415: RADIUS:  Vendor, Cisco       [26]  49
*Mar  1 22:28:31.415: RADIUS:   Cisco AVpair       [1]   43  "auth-
proxy:proxyacl#1=permit icmp any any"
*Mar  1 22:28:31.419: RADIUS:  Vendor, Cisco       [26]  48
*Mar  1 22:28:31.419: RADIUS:   Cisco AVpair       [1]   42  "auth-
proxy:proxyacl#2=permit tcp any any"
*Mar  1 22:28:31.419: RADIUS:  Class               [25]  28
*Mar  1 22:28:31.419: RADIUS:   43 41 43 53 3A 30 2F 36 66 31 64 2F 38 38 30 31
[CACS:0/6f1d/8801]
*Mar  1 22:28:31.423: RADIUS:   31 37 30 33 2F 36 30 30 30 31
[1703/60001]
*Mar  1 22:28:31.423: RADIUS: saved authorization data for user 82ECC30C at
82BC2E78
*Mar  1 22:28:31.427: AAA/AUTHEN(4167353654): Status=PASS
*Mar  1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236):
Port='Ethernet0/1' list='default' service=AUTH-PROXY
*Mar  1 22:28:31.427: AAA/AUTHOR/HTTP: Ethernet0/1(476008236) user='PROXY'
*Mar  1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236): send AV
service=auth-proxy
*Mar  1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236): send AV cmd*
*Mar  1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236): found list
"default"
*Mar  1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236): Method=radius
(radius)
*Mar  1 22:28:31.431: RADIUS: cisco AVPair "auth-proxy:priv-lvl=15"
*Mar  1 22:28:31.431: RADIUS: cisco AVPair "auth-proxy:proxyacl#1=permit icmp
any any"
*Mar  1 22:28:31.431: RADIUS: cisco AVPair "auth-proxy:proxyacl#2=permit tcp
any any"
*Mar  1 22:28:31.431: AAA/AUTHOR (476008236): Post authorization status =
PASS_ADD

R3#show ip access-lists
Extended IP access list 100
     permit icmp host 136.1.200.200 any
     permit tcp host 136.1.200.200 any (7 matches)
    10 permit udp any any eq rip
    20 deny ip any any log (20 matches)

R3#show ip auth-proxy cache
Authentication Proxy Cache
 Client IP 136.1.200.200 Port 1248, timeout 60, state HTTP_ESTAB
```

Further Reading

Implementing Authentication Proxy

Content Filtering with IOS Firewall

Objective: Configure router for URL filtering using Websense application.



Directions

- Pre-configure devices as follows:
  - Create VLANs 13, 23 and 100.
  - Configure IP addressing on Ethernet interfaces.
  - Configure Serial link between R3 and R2.
  - Configure RIP as routing protocol.
  - Create and advertise into RIP interface Loopback0 on R1.
- The goal of the task is to configure HTTP application filtering to achieve the following:
  - Filter all java applets from HTTP responses.
  - Filter URLs using Websense server.
  - Permit domain 'cisco.com' to be accessed at any time.
  - In case if Websense server fails, router should permit any HTTP request.

- Configure R3 as follows:
    - Create access-list number 1, and deny everything with it. It will be used for java filtering.
    - Configure URL server at 10.0.0.100, use vendor “Websense”.
    - Configure inspection rule named INSPECT as follows:
        - Inspect HTTP traffic and enable java filtering with access-list 1 as well as URL filtering.
    - Configure URL filtering to exempt domain “cisco.com” from filtering and always permit it.
    - Configure url-filtering allow-mode, which instructs router to bypass filtering if filtering server is unavailable.
    - Apply inspection rule “INSPECT” ingress to interface E0/1.

Final Configuration

```
Pre-Configuration:

SW1 & SW2:
vlan 13,200,100
!
! Configure trunks
!
interface range Fa0/21 - 23
 switchport trunk encaps dot1q
 switchport mode trunk

SW1:
interface Fa0/1
 switchport host
 switchport access vlan 13
!
interface Fa0/2
 switchport host
 switchport access vlan 100
!
interface Fa0/3
 switchport host
 switchport access vlan 13
!
interface Fa0/20
 switchport host
 switchport access vlan 100

SW2:
interface Fa0/3
 switchport host
 switchport access vlan 200
!
interface Fa0/20
 switchport host
 switchport access vlan 200
```


R1:
```
interface E0/0
 no shut
 ip address 136.1.13.1 255.255.255.0
!
interface Loopback0
 ip address 150.1.1.1 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
```

R2:
```
interface E 0/0
 no shut
 ip add 10.0.0.2 255.255.255.0
!
interface Ser 0/1
 no shut
 ip address 136.1.23.2 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 10.0.0.0
```

R3:
```
interface E 0/0
 no shut
 ip add 136.1.13.3 255.255.255.0
!
interface E 0/1
 no shut
 ip add 136.1.200.3 255.255.255.0
!
interface Serial 1/3
 no shut
 clockrate 64000
 ip address 136.1.23.3 255.255.255.0
!
router rip
 ver 2
 no auto
 network 136.1.0.0
```

Content Filtering:

R3:
```
!
! Access-list for java-filtering
!
access-list 1 deny any

!
! Websense Server
!
ip urlfilter server vendor websense 10.0.0.100

!
! Inspection rule to activate filtering
```

```
!
ip inspect name INSPECT http java-list 1 urlfilter

!
! Configure cisco.com as 'exclusively permitted' domain
!
ip urlfilter exclusive-domain permit cisco.com

!
! Enable allow-mode
!
ip urlfilter allow-mode on

!
! Apply inspection rule
!
interface Ethernet 0/1
 ip inspect INSPECT in
```

Verification

If you have functional Websense server you should see something like this on your console:

```
R3(config)#ip urlfilter server vendor websense 10.0.0.100
R3(config)#
*Mar  1 23:03:46.566: %URLF-5-SERVER_UP: Connection to an URL filter
server(10.0.0.100) is made, the router is returning from ALLOW MODE

R3#show ip inspect all
Session audit trail is disabled
Session alert is dlsabled
one-minute (sampling period) thresholds are [90:100] connections
max-incomplete sessions thresholds are [900:1000]
max-incomplete tcp connections per host is 50. Block-time 5 minutes.
tcp synwait-time is 15 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name INSPECT
    http java-list 1 url-filter is on alert is off audit-trail is off timeout
3600

Interface Configuration
 Interface Ethernet0/1
  Inbound inspection rule is INSPECT
    http java-list 1 url-filter is on alert is off audit-trail is off timeout
3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
```

Check urlfilter configuration, note the server port. Sometimes you may need to open a pinhole for it in access-lists:

```
R3#show ip urlfilter config
Websense URL Filtering is ENABLED

Primary Websense server configurations
========================================
```

```
Websense server IP address: 10.0.0.100
Websense server port: 15868
Websense retransmission time out: 6 (in seconds)
Websense number of retransmission: 2

Secondary Websense servers configurations
=========================================
Other configurations
====================
Allow Mode: ON
System Alert: ENABLED
Audit Trail: DISABLED
Log message on Websense server: DISABLED
Maximum number of cache entries: 5000
Maximum number of packet buffers: 200
Maximum outstanding requests: 1000
```

Further Reading

Firewall Websense URL Filtering