SECURE

# Lab Guide

## Overview

This guide presents the instructions and other information required to complete the lab activities for this course. You can find the solutions in the lab activity Answer Key.

## Outline

This guide includes these activities:

- Lab 1-1: Configuring Advanced Switched Data Plane Security Controls
- Lab 1-2: Configuring Advanced Infrastructure Security Controls
- Lab 2-1: Configuring Basic Zone-Based Policy Firewall Features
- Lab 2-2: Configuring Advanced Zone-Based Policy Firewall Features
- Lab 2-3: Configuring Cisco IOS Software IPS
- Lab 3-1: Configuring a PKI-Enabled Site-to-Site IPsec VPN
- Lab 3-2: Configuring Cisco IOS Software DMVPN Spokes
- Lab 3-3: Configuring GET VPN Group Members
- Lab 4-1: Configuring a Cisco IOS Software SSL VPN Gateway
- Lab 4-2: Configuring Cisco Easy VPN
- Answer Key

# Lab 1-1: Configuring Advanced Switched Data Plane Security Controls

Complete this lab activity to practice what you learned in the related module.

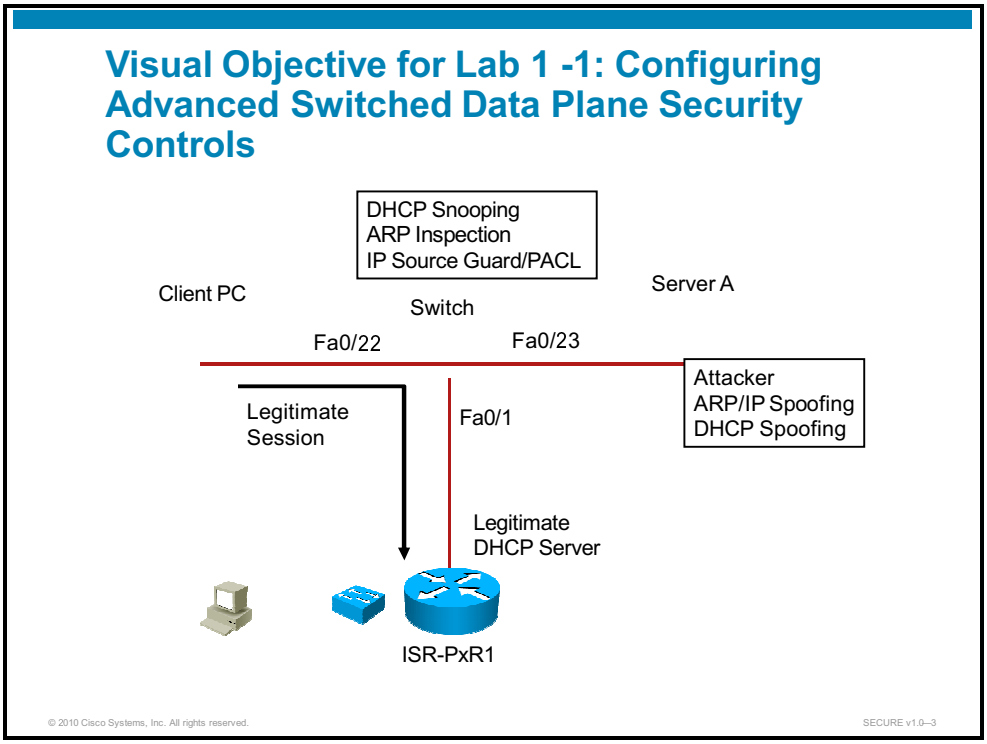
## Activity Objective

In this activity, you will configure common Cisco Catalyst IOS Software-switched infrastructure protection controls in a basic scenario. After completing this activity, you will be able to meet these objectives:

- Verify DHCP spoofing vulnerability
- Configure DHCP snooping
- Configure dynamic and static ARP inspection
- Configure IP Source Guard and PACLs
- Configure PVLAN Edge

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops or PCs)
- Pod ISR router
- Pod Catalyst switch
- Pod client PC and Server A systems

# Command List

The table describes the commands that are used in this activity.

### Configuring Advanced Switched Data Plane Security Controls Commands

| Command | Description |
|---|---|
| **arp access-list** *name* | Configures an ARP ACL for ARP inspection. |
| **ip access-group** *access-list-name* **{in \| out}** | Applies an IP ACL to an interface. |
| **ip access-list {standard \| extended}** *access-list-name* | Defines an IP ACL by name. |
| **ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* | Permits ARPs from hosts that are configured for static IP when Dynamic ARP Inspection (DAI) is enabled, and defines an ARP access list and applies it to a VLAN. |
| **ip arp inspection vlan** *vlan-range* | Enables DAI on a per-VLAN basis. |
| **ip dhcp snooping** | Globally enables DHCP snooping. |
| **ip dhcp snooping trust** | Configures the interface as DHCP-snooping trusted. |
| **ip dhcp snooping vlan** {*number* \| *vlan-list*} | Enables DHCP snooping on a VLAN or a group of VLANs. |
| **ip verify source port-security** | Configures the IP Source Guard feature on an interface with IP and MAC address verification. |
| **ipconfig /release** | Releases the IP address on the PC. |
| **ipconfig /renew** | Renews the IP address on the PC. |
| **permit** *ip-address* | Sets conditions in the named IP ACL that will permit packets. |
| **permit ip host** *ip-address* **mac host** *mac-address* | Permits ARP packets inside the ARP access list with the IP address specified, bound to a specific MAC address. |
| **ping** *ip-address* | Determines if another IP address is accessible. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding entries. |
| **show running-config** | Displays the configuration that is currently running on the device. |

# Job Aids

These job aids are available to help you complete the lab activity:

- The instructor will provide you with your pod number and other pod access information. Please log this information in this table.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |

| Parameter | Value |
|---|---|
| Username on the router and switch | |
| Password on the router and switch | |
| Username on Server A | Administrator |
| Password on Server A | admin |
| Username on the client PC | Administrator |
| Password on the client PC | admin |
| VLAN ID for the VLAN hosting the client and server | |

- The IP addressing scheme in the table lists the IP addresses of the devices that are used in this lab exercise.

## Pod Addressing

| Device | Interface | IP Address and Mask |
|---|---|---|
| Router | Loopback 0 | 192.168.x.1/32 |
| Router | FastEthernet0/0 | 10.x.1.1/24 |
| Client PC | LAB | Assigned via DHCP |
| Server A | LAB | 10.x.1.11/24 |

 © 2010 Cisco Systems, Inc.

# Task 1: Verify DHCP Spoofing Vulnerability

The router in the lab is the legitimate DHCP server for the subnet on which the client PC system is located. Server A in the lab is configured as a rogue DHCP server that will attempt to misconfigure the client PC to perform man-in-the-middle attacks against it.

In this task, you will verify the effects of DHCP spoofing in the lab LAN.

## Activity Procedure

Complete these steps:

**Step 1** Log in to the client PC system.

**Step 2** Right-click the network icon in the system tray and choose **Open Network Connections**. The Network Connections window opens.

**Step 3** Right-click the LAB interface and choose **Properties**. The LAB Properties window opens.

**Step 4** In the This Connection Uses the Following Items section, choose **Internet Protocol (TCP/IP)** and click **Properties**. The Internet Protocol (TCP/IP) Properties window opens.

**Step 5** Click the **Obtain an IP Address Automatically** radio button and click **OK**.

**Step 6** Click **OK** and close the window.

**Step 7** Open a command prompt and verify the DHCP configuration using the **ipconfig /all** command. In the output for the LAB adapter, you should see Server A (10.1.1.11) as the DHCP server. The default gateway IP address should be 10.1.1.11 (that is, Server A acting as a rogue default gateway).

---

**Note** Although the router is configured as the legitimate DHCP server, the client PC has received the IP configuration from server A, which is a rogue DHCP server. The server can now act as a man-in-the-middle and can capture all traffic from the client PC to the Internet because it has configured itself as the default gateway of the client.

If the client PC did not receive an IP configuration from the server, try to release and renew the IP address on the client PC.

---

**Step 8** Log in to the Server A system and run the Wireshark network analyzer.

**Step 9** In the menu bar**,** click **Capture**, select **Interfaces**, and select the first (top) interface as the capture interface by clicking **Start** at the interface name.

---

**Note** All traffic from the client PC goes through the Server A system now, where it can be captured using the appropriate software.

---

**Step 10** From the client PC, attempt to ping the IP address of the loopback 0 interface on the router (192.168.1.1).

**Step 11** In the Wireshark network analyzer windows on Server A, you will notice intercepted PING packets that are sourced by the client, because Server A has configured the client PC to use as the default gateway.

### Activity Verification

You have completed this task when you attain these results:

- On the client PC, verify the DHCP configuration that is provided by the rogue DHCP server on the server.

```
C:\Documents and Settings\Administrator>ipconfig

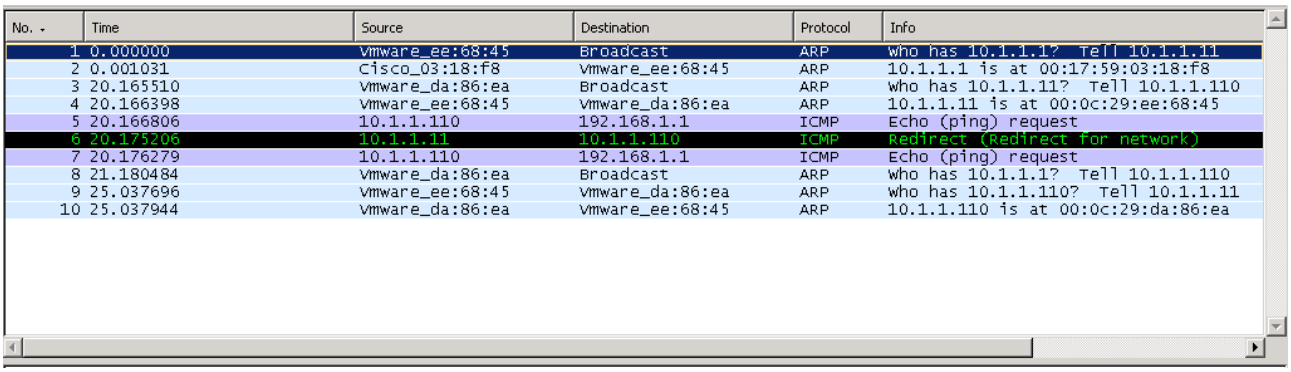
Windows IP Configuration

Ethernet adapter LAB:

        Connection-specific DNS Suffix  . : cisco.com
        IP Address. . . . . . . . . . . . : 10.1.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.1.1.11
```

**Note** You may be assigned a different (but similar) IP address on the LAB adapter.

- On the Server A system, verify the interception of the ICMP packets of the client PC.



| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | Vmware_ee:68:45 | Broadcast | ARP | Who has 10.1.1.1? Tell 10.1.1.11 |
| 2 | 0.001031 | Cisco_03:18:f8 | Vmware_ee:68:45 | ARP | 10.1.1.1 is at 00:17:59:03:18:f8 |
| 3 | 20.165510 | Vmware_da:86:ea | Broadcast | ARP | Who has 10.1.1.11? Tell 10.1.1.110 |
| 4 | 20.166398 | Vmware_ee:68:45 | Vmware_da:86:ea | ARP | 10.1.1.11 is at 00:0c:29:ee:68:45 |
| 5 | 20.166806 | 10.1.1.110 | 192.168.1.1 | ICMP | Echo (ping) request |
| 6 | 20.175206 | 10.1.1.11 | 10.1.1.110 | ICMP | Redirect (Redirect for network) |
| 7 | 20.176279 | 10.1.1.110 | 192.168.1.1 | ICMP | Echo (ping) request |
| 8 | 21.180484 | Vmware_da:86:ea | Broadcast | ARP | Who has 10.1.1.1? Tell 10.1.1.110 |
| 9 | 25.037696 | Vmware_ee:68:45 | Vmware_da:86:ea | ARP | Who has 10.1.1.110? Tell 10.1.1.11 |
| 10 | 25.037944 | Vmware_da:86:ea | Vmware_ee:68:45 | ARP | 10.1.1.110 is at 00:0c:29:da:86:ea |

# Task 2: Configure DHCP Snooping

In this task, you will enable DHCP snooping on the switch to prevent server spoofing attacks against the DHCP infrastructure.

### Activity Procedure

Complete these steps:

**Step 1** Access the console of the switch. Examine the configuration and note the number of the VLAN hosting the client PC (connected to the FastEthernet0/22 interface), router (connected to the FastEthernet0/1 interface), and Server A (connected to the FastEthernet0/23 interface) devices that are used in the lab exercise.

Q1) What is your VLAN number?

**Step 2** On the switch, globally enable DHCP snooping.

**Step 3** On the switch, configure DHCP snooping to use a file in the root folder of the flash file system as the DHCP snooping database. You can use any name for the database file.

 © 2010 Cisco Systems, Inc.

**Step 4** On the switch, enable DHCP snooping inside the specific VLAN that you noted before.

**Step 5** On the switch, enter the interface configuration mode on the FastEthernet0/1 port that connects to the legitimate DHCP server (router). Configure this port as trusted for DHCP snooping.

| **Note** | All interfaces are labeled as untrusted by default. |
|---|---|

**Step 6** On the client PC, renew the IP address of the client PC using the **ipconfig /renew** command in a command-line session.

**Step 7** In the Wireshark application on the server, click **Capture** and **Restart** to start capturing traffic again.

**Step 8** From the client PC, ping the IP address of the loopback 0 interface on the router.

**Step 9** In the Wireshark application on Server A, you will notice that there are no intercepted ICMP packets anymore.

**Step 10** Close the Wireshark application on Server A.

| **Note** | Traffic from the client PC to the loopback interface on the router goes through the router now, which is the intended behavior. |
|---|---|

### Activity Verification

No additional verification steps are needed for this task.

## Task 3: Configure Dynamic and Static ARP Inspection

In this task, you will first perform an ARP spoofing attack against the client PC from the Server A system. Then you will configure dynamic and static ARP inspection to mitigate the ARP spoofing attack.

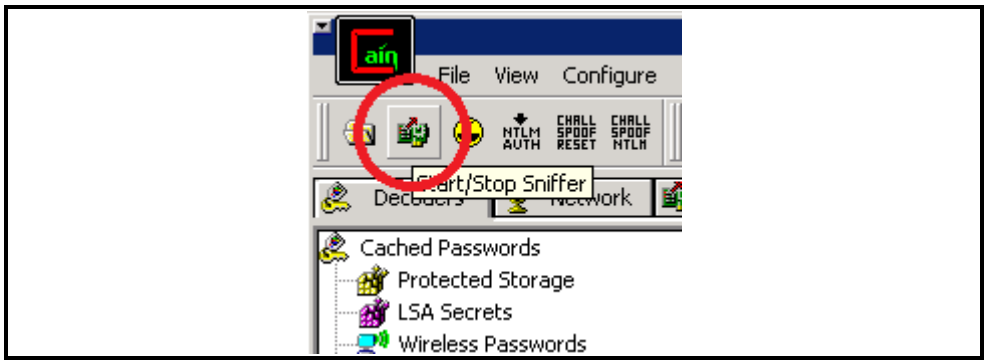
### Activity Procedure

Complete these steps:

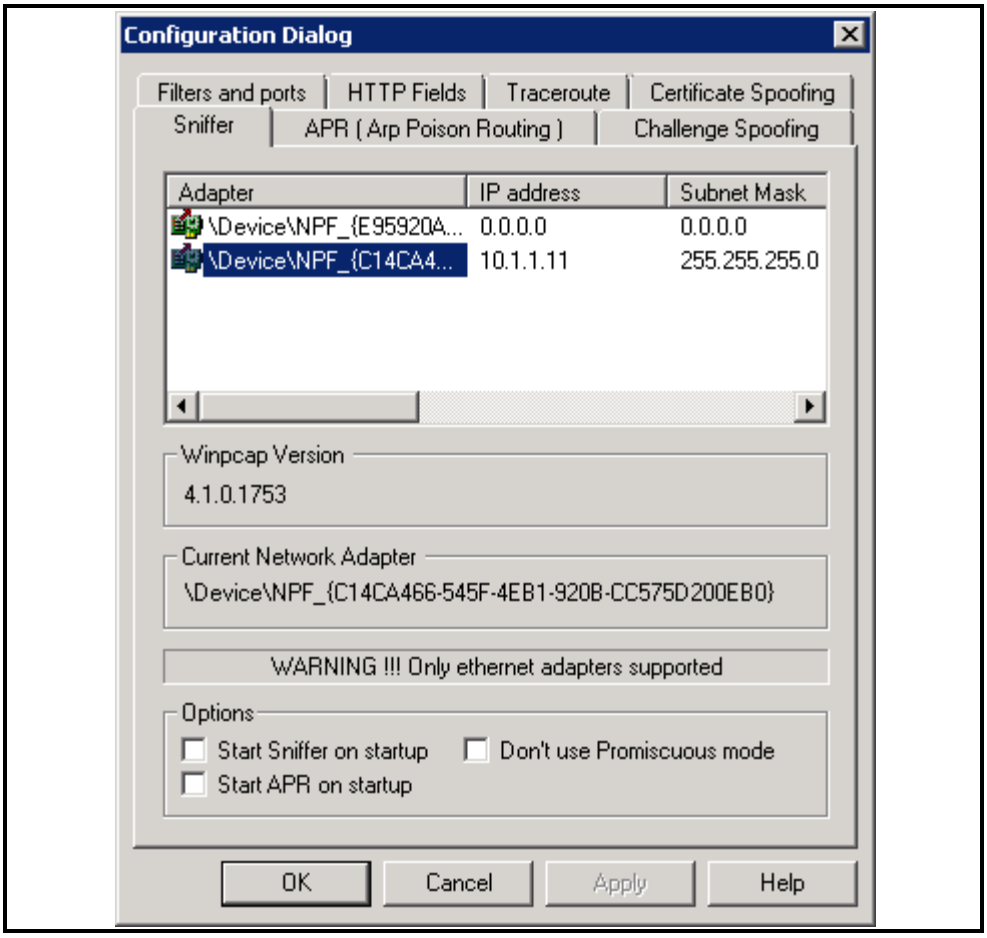
**Step 1** Log in to the Server A system and test basic connectivity by pinging the router (10.1.1.1) and client PC from the Server A CLI.

**Step 2** Double-click the **Cain** icon on the desktop of Server A.

**Step 3** When the Cain application window opens, click the **Start/Stop Sniffer** button (second button in the taskbar, next to the folder icon) to start the sniffer. This is the first step of hijacking the session from the client PC to the router.

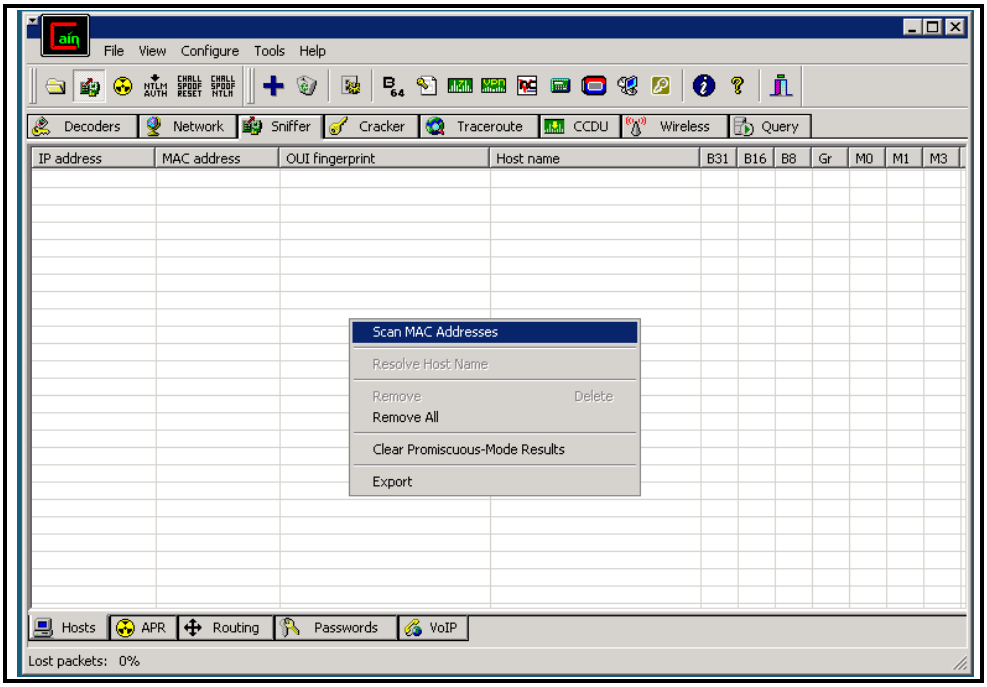


**Step 4** When you see a list of network adapters, select the one with the IP address of 10.1.1.11 and click **OK**.



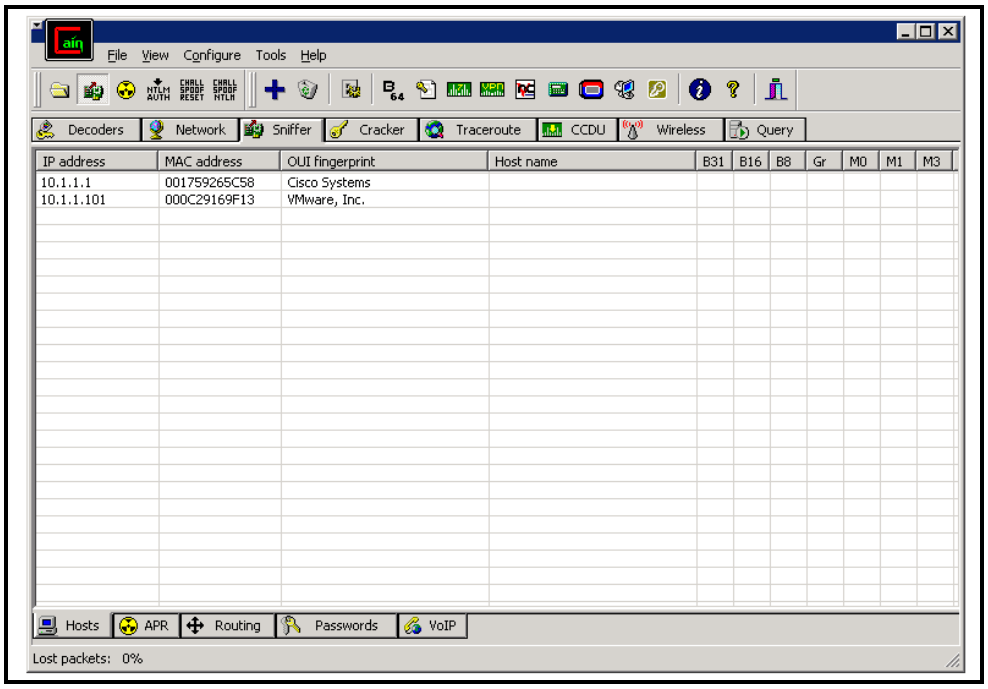

**Step 5** Click the **Sniffer** tab. If the table is not empty, right-click the table, choose **Remove All**, and click **OK** when asked to delete all entries.

**Step 6** Right-click inside the empty table and choose the **Scan MAC Addresses** option.

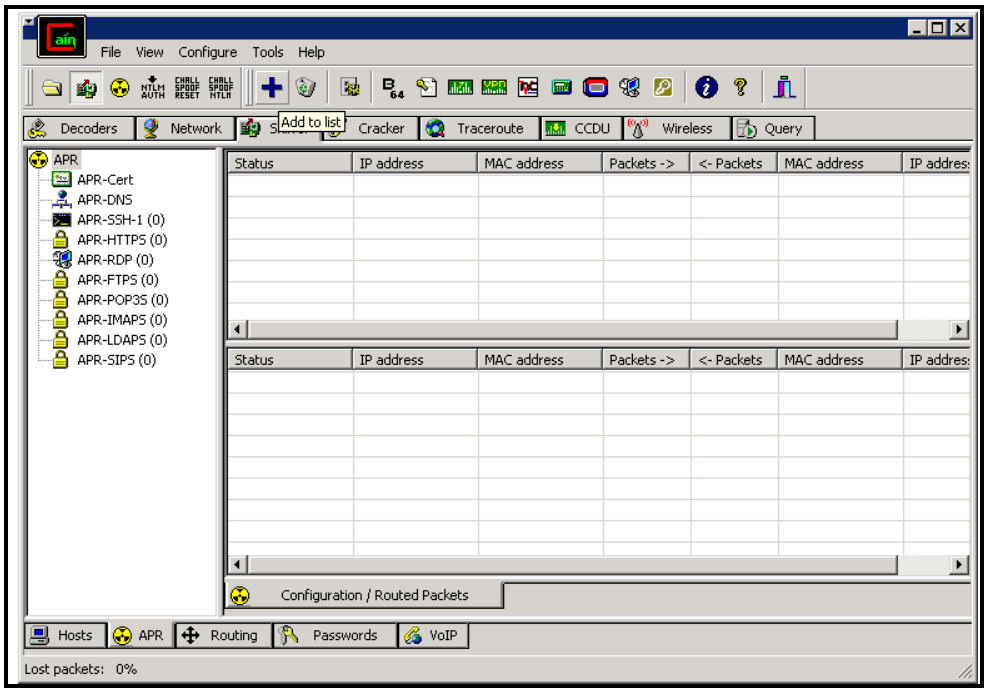



 © 2010 Cisco Systems, Inc.

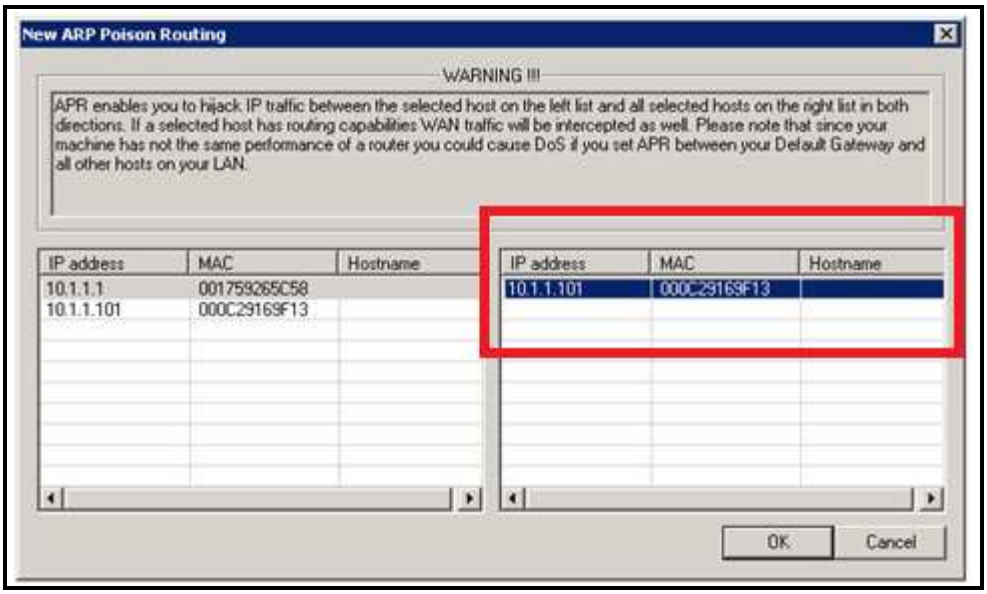
**Step 7** Click **OK** in the **MAC Address Scanner** window. You should see at least two MAC addresses, among them one for the router (10.1.1.1) and one for the client PC host (DHCP-assigned in the 10.1.1.101–10.1.1.254 range).




**Step 8** Scroll to the bottom of the window and click the **ARP Poison Routing (APR)** tab. Click the upper table, and click the Plus sign (+) in the toolbar.

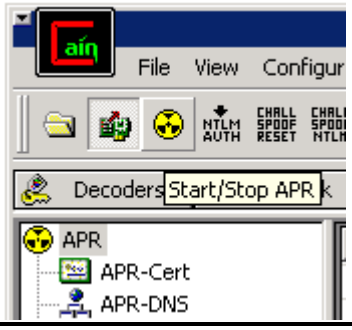


**Step 9** You are going to hijack a session between the client PC host and the router. Choose the IP address of the router from the table on the left by clicking **10.1.1.1.** Choose the IP address of the client PC by clicking the IP address that was assigned to the client in the table on the right (in this example, the IP address of the client host is 10.1.1.101, but your IP address may differ).




**Note** Ensure that the entry in the right pane is highlighted or selected, as shown in the preceding figure.

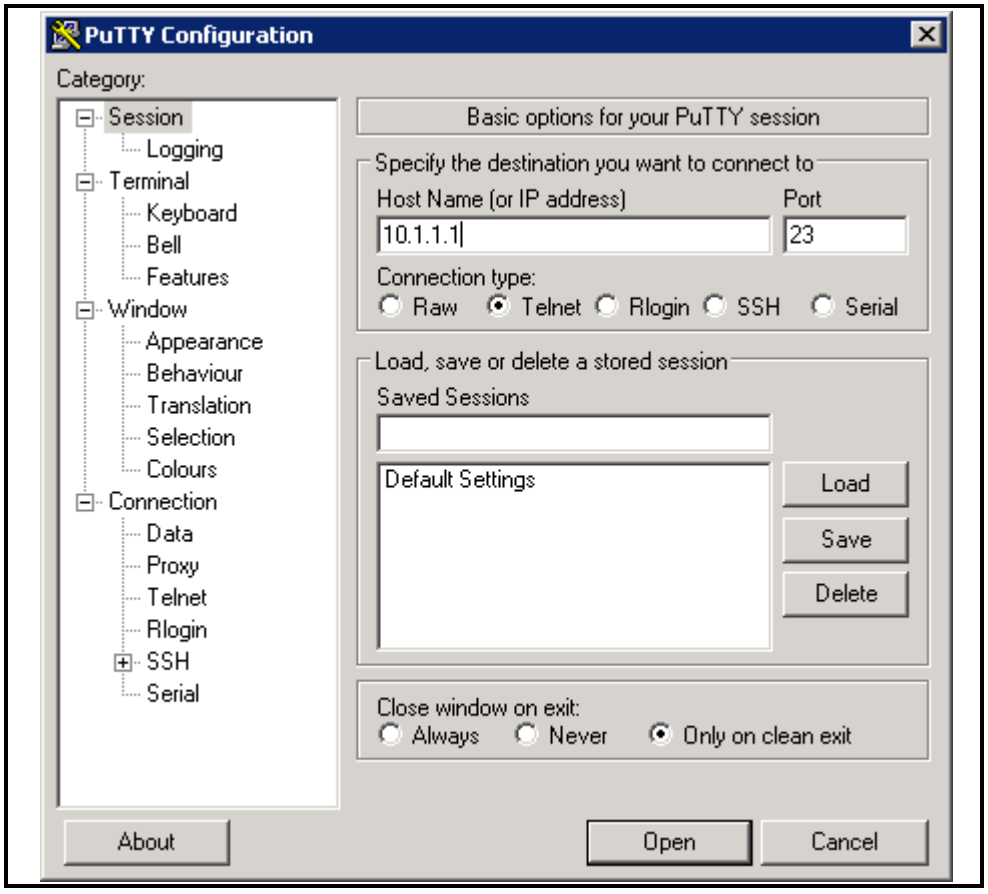
**Step 10** Click the **Start/Stop APR** button (the third button in the taskbar, next to the sniffer icon) to start the ARP poisoning process and session interception.




**Step 11** Log in to the client PC and start the PuTTY Telnet/SSH terminal emulator by clicking the **PuTTY** icon on the desktop.

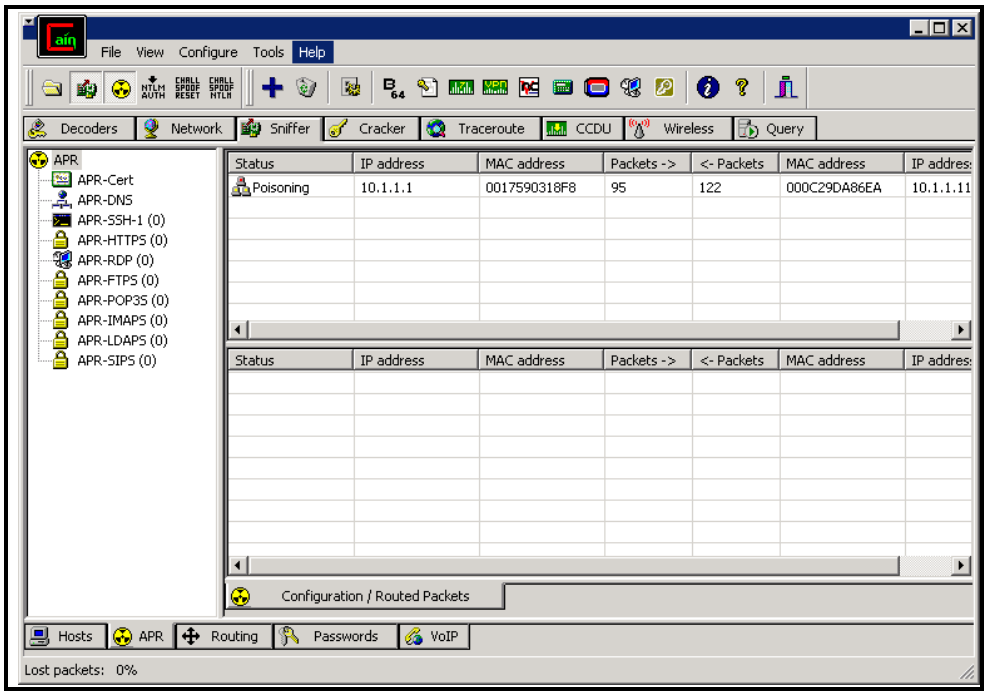
 © 2010 Cisco Systems, Inc.

**Step 12** Use the PuTTY Configuration window to select Telnet for connecting to the router at 10.1.1.1. Log in to the router vty using the password **cisco**.

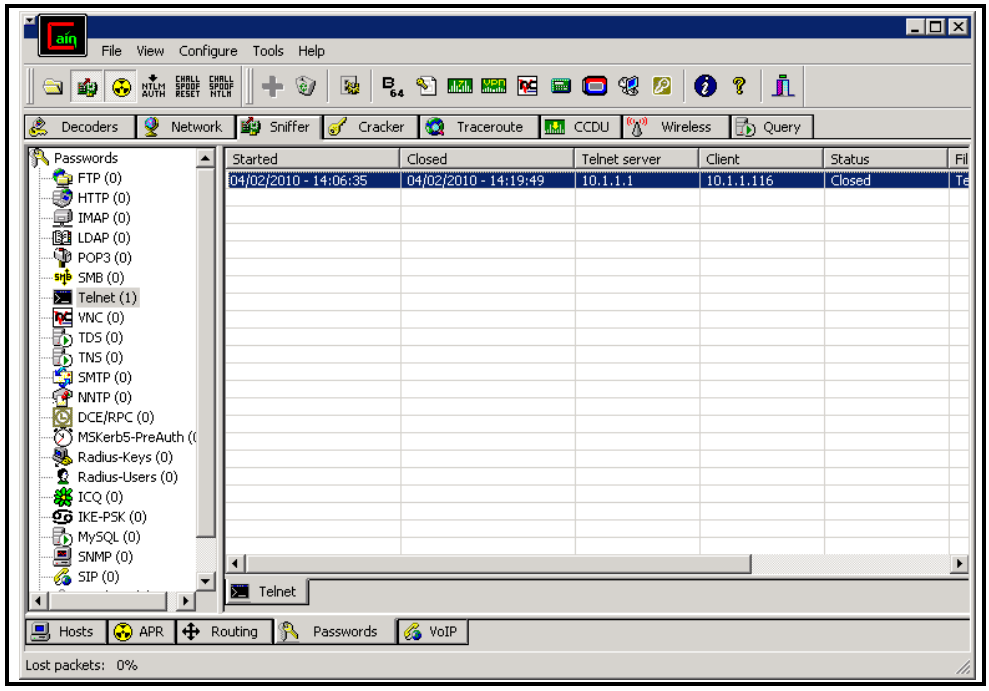



**Step 13** Display the entire configuration that is currently running on the router device. Close the Telnet session to the router.

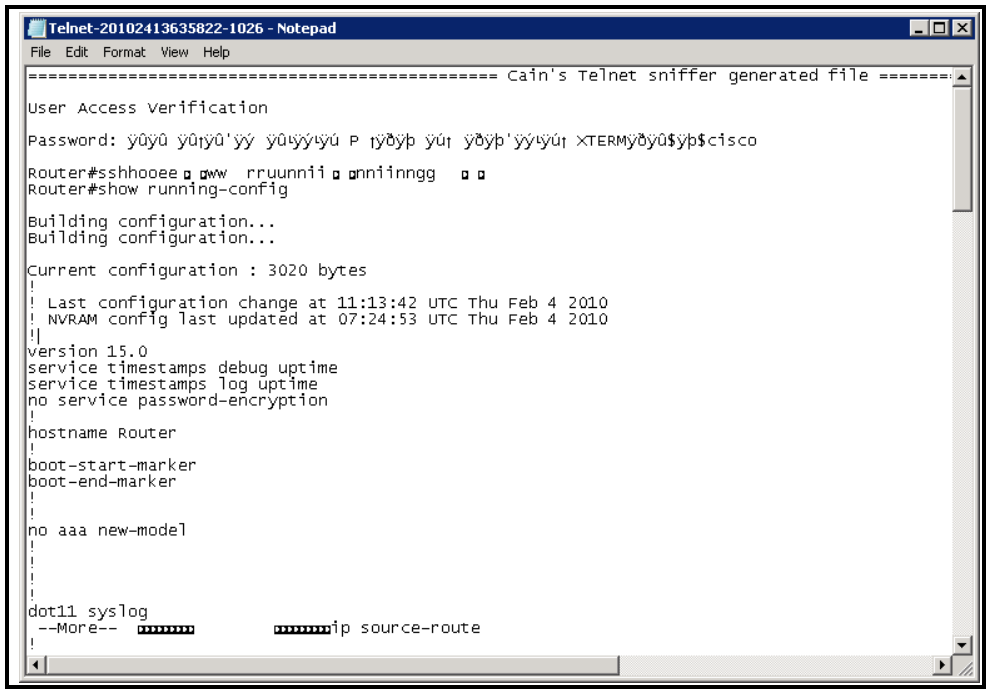
**Step 14** Go back to the Server A desktop and notice that the Cain application has captured some data between the router and the server by noting the captured packets counter.



**Step 15** Click the **Passwords** tab at the bottom of the window. Click **Telnet** in the list on the left side of the window.




**Step 16** Right-click the session that you just intercepted (based on the Started and Closed dates and times) and choose **View**. Notice that you intercepted the administrative session and that the entire router configuration was captured in plaintext. Notice that any characters that you entered are recorded twice because of the Telnet echo feature.




 © 2010 Cisco Systems, Inc.

**Step 17** On Server A, inside the Cain tool, click the **Start/Stop APR** button (the third button in the taskbar, next to the sniffer icon) to stop the ARP poisoning process and session interception.

**Step 18** On the router, verify the MAC address of the FastEthernet0/0 interface facing the switch and record it here:

_____

**Step 19** On the switch, configure static ARP inspection to protect the IP-to-MAC mapping for the FastEthernet0/0 interface of the router.

**Step 20** Enable dynamic ARP inspection in the specific VLAN hosting the client, server, and router devices. The ARP inspection rule should also check the static ARP ACL. All ports on the switch should be labeled as untrusted for ARP inspection.

**Step 21** On the server, try to hijack a session between the client PC and the server again by clicking the **Start/Stop APR** in the Cain application. Your attempt should fail because of ARP inspection that is configured on the switch. Note that Cisco IOS Software on the switch displays violations of ARP inspection security filters as system log messages.

**Step 22** Stop ARP poisoning in the Cain application by clicking the **Start/Stop APR** button again.

**Step 23** Disable ARP inspection on the VLAN hosting the client, server, and router devices.

### Activity Verification

You have completed this task when you attain these results:

- On the switch, you receive system log message with violations of the ARP inspection security filter:

```
01:45:38: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/23, vlan
661.([000c.29ee.6845/10.1.1.1/000c.29da.86ea/10.1.1.116/01:45:37 UTC Mon Mar 1
1993])
```

## Task 4: Configure IP Source Guard and Port Access Lists

In this task, you will configure IP Source Guard and PACLs to prevent IP spoofing from hosts on switch ports. You will try to change the IP address of the client PC and the server, but the switch will not allow traffic from these IP addresses because of the configured IP Source Guard and port access list.

### Activity Procedure

Complete these steps:

**Step 1** On the client PC, ping the server at 10.1.1.11. The ping should be successful.

**Step 2** On the switch, configure the IP Source Guard feature with IP and MAC address verification on the FastEthernet 0/22 interface facing the client PC.

**Step 3** On the client PC, change the IP address of the LAB adapter to a static IP address of 10.1.1.10/24.

**Step 4** From the client PC, ping the server at 10.1.1.11 again. The ping should fail because the IP Source Guard feature filters packets with an unknown IP source address.

**Step 5** On the switch, verify the current source address mappings and IP-Source-Guard-enabled ports.

**Step 6** On the client PC, change the IP address of the LAB adapter to be obtained automatically from the DHCP server.

**Step 7** On the server, ping the router at 10.1.1.1. The ping test should be successful.

**Step 8** On the switch, configure a standard access control list permitting only the authorized source IP address of 10.1.1.11. Apply this access control list to the FastEthernet0/23 interface facing the server in the input direction.

**Step 9** On the server, change the IP address of the LAB interface to a static IP address of 10.1.1.12/24.

**Step 10** From the server, ping the router at 10.1.1.1. The ping should fail because the configured static PACL denies packets with unexpected IP source addresses.

**Step 11** On the switch, remove the port access list on the FastEthernet0/23 interface facing the server.

**Step 12** On the server, change the IP address of the LAB interface back to its original static IP address of 10.1.1.11/24.

### Activity Verification

No additional verification steps are needed for this task.

## Task 5: Configure PVLAN Edge

In this task you will configure the PVLAN Edge feature, which is a Cisco IOS Software feature like PVLANs. The switch does not forward any traffic from one protected port to any other protected port.

### Activity Procedure

Complete these steps:

**Step 1** From the server, ping the router at 10.1.1.1. The ping should be successful.

**Step 2** On the switch, configure the PVLAN Edge feature on the FastEthernet0/1 and FastEthernet0/23 interfaces facing the router and the server, respectively.

**Step 3** Verify that the FastEthernet0/1 and FastEthernet0/23 interfaces are configured as protected ports.

**Step 4** From the server, ping the router at 10.1.1.1. The ping should fail because the PVLAN Edge feature does not allow communication between two protected ports.

**Step 5** Remove the protected port feature from both configured ports.

### Activity Verification

No additional verification steps are needed for this task.

 © 2010 Cisco Systems, Inc.

# Lab 1-2: Configuring Advanced Infrastructure Security Controls

Complete this lab activity to practice what you learned in the related module.

## Activity Objective

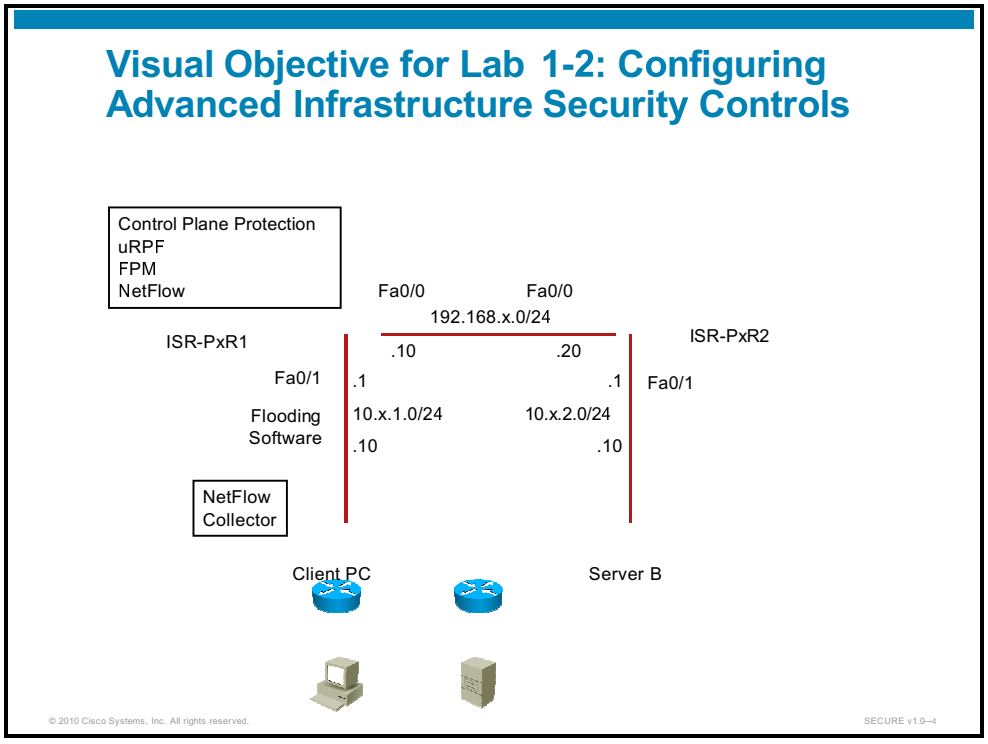
In this activity, you will configure common Cisco Catalyst IOS Software-switched infrastructure protection controls in a basic scenario.

After completing this activity, you will be able to meet these objectives:

- Configure Control Plane Protection
- Configure Management Plane Protection
- Configure uRPF
- Configure FPM
- Configure Flexible NetFlow

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Two pod Cisco ISR routers
- Pod client PC and Server B systems

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **access-list** *access-list-number* **{deny \| permit}** *protocol source source-wildcard destination destination-wildcard* **[ [log [word] \| log-input [word]]** | Defines an extended IP access list with an option that includes the input interface and source MAC address or virtual circuit in the logging output. |
| **class** *class-name* | Inside policy-map configuration, specifies the name of the class that you want to create or change before you configure its policy. |
| **class-map [type {stack \| access-control \| port-filter \| queue-threshold \| logging** *log-class***}] [match-all \| match-any]** *class-map-name* | Creates a class map to be used for matching packets to a specified class. |
| **control-plane [host \| transit \| cef-exception]** | Enters control-plane configuration mode. |
| **copy tftp: flash:** | Copies file from TFTP server to the flash of the network device. |
| **drop** | Configures a traffic class to discard packets belonging to a specific class. |
| **interface** *type* | Enters interface configuration mode. |
| **ip access-group** *access-list-name* **{***in* **\|** *out***}** | Applies an IP access list to an interface. |
| **ip access-list {standard \| extended} {***access-list-name* **\|** *access-list-number***}** | Defines an IP access list by name or number. |
| **ip cef** | Enables Cisco Express Forwarding (CEF) on the route processor card. |
| **ip verify source port-security** | Configures the IP Source Guard feature on the interface with IP and MAC address verification. |
| **ip verify unicast source reachable-via {rx \| any} [allow-default] [allow-self-ping] [***list***]** | Enables Unicast Reverse Path Forwarding (uRPF) in interface configuration mode. |
| **load protocol** *location*:*filename* | Loads a PHDF onto a router. |
| **match access-group {***access-group* **\| name** *access-group-name***}** | Configures the match criteria for a class map that is based on the specified access control list. |
| **match field** *protocol protocol-field* **{eq [***mask***] \| neq [***mask***] \| gt \| lt \| range** *range* **\| regex** *string***}** *value* **[next** *next-protocol***]** | Configures the match criteria for a class map that is based on the fields that are defined in the PHDFs. |

 © 2010 Cisco Systems, Inc.

| Command | Description |
|---|---|
| **match start {l2-start \| l3-start} offset** *number* **size** *number* **{eq \| neq \| gt \| lt \| range** *range* **\| regex** *string***} {***value* **[***value2***] \| [***string***]}** | Configures the match criteria for a class map that is based on the datagram header (Layer 2) or the network header (Layer 3). |
| **permit** | Sets conditions in the named IP access list that will permit packets. |
| **permit ip host** *ip-address* **host** *mac-address* | Permits ARP packets inside the ARP access-list with IP address specified, bound to a specific MAC address. |
| **permit** *protocol source_address destination_address* **eq** *port* | Sets conditions in the named IP access list that will permit packets. |
| **ping** | Determines if other IP addresses are accessible. |
| **police rate** *units* **pps [conform-action** *action***]** | Configures traffic policing for traffic that is destined for the control plane in QoS policy-map class configuration mode. |
| **policy-map [type {stack \| access-control \| port-filter \| queue-threshold \| logging** *log-policy***}]** *policy-map-name* | Specifies the name of the policy map to be created, added to, or modified before you configure policies for classes whose match criteria are defined in a class map. |
| **service-policy {input \| output}** *policy-map-name* | Attaches a policy map to a control plane for aggregate or distributed control plane services. |
| **service-policy** *type* **access-control {input \| output}** *policy-map-name* | Applies a policy map to the interface in interface configuration mode. |
| **show running-config** | Displays the configuration that is currently running on the adaptive security appliance. |
| **snmp-server community** *string* **[ro \| rw]** | Sets up the community access string to permit access to the SNMP. |

# Job Aids

These job aids are available to help you complete the lab activity.

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username that is used to log in to the Server system | |
| Password that is used to log in to the Server system | |

# Task 1: Configure Control Plane Protection

In this task, you will configure the Control Plane Protection feature on a Cisco ISR to mitigate the risk of control plane flooding denial-of-service attacks.

## Activity Procedure

Complete these steps:

**Step 1** Log in to the ISR-PxR1 router and observe its CPU utilization using the **show processes cpu** command; it should be very low.

```
ISR-PxR1#show processes cpu
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(uS)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1        8000          14        571  0.00%  0.00%  0.00%   0 Chunk Manager
   2        4000         406          9  0.00%  0.00%  0.00%   0 Load Meter
   3           0           1          0  0.00%  0.00%  0.00%   0 LICENSE AGENT
   4     2012000         304       6618  0.00%  0.12%  0.09%
```

**Step 2** Log in to the client PC host. Double-click the **SNMP-flood** batch file inside the SECURE folder on the desktop, which will start flooding the ISR-PxR1 router with 2500 UDP packets per second on destination port 161 (SNMP polling).

**Step 3** Observe the CPU utilization of the ISR-PxR1 router again. It should now be very high because of UDP flooding.

```
ISR-PxR1#show processes cpu
CPU utilization for five seconds: 98%/35%; one minute: 21%; five minutes: 6%
 PID Runtime(uS)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1        8000          14        571  0.00%  0.00%  0.00%   0 Chunk Manager
   2        8000         428         18  0.00%  0.01%  0.00%   0 Load Meter
   3           0           1          0  0.00%  0.00%  0.00%   0 LICENSE AGENT
```

**Step 4** Stop the flooding process on the client PC by closing the **udpc.exe** command-line window.

**Step 5** On the ISR-PxR1 router, configure a Control Plane Protection policy, which will rate-limit all SNMP packets to the control plane to 200 p/s.

**Step 6** Log in to the client PC host. Double-click the **SNMP-flood** batch file inside the SECURE folder on the desktop, which will again start flooding the ISR-PxR1 router with 2500 UDP p/s.

**Step 7** Examine statistics from the control plane protection feature. You should see packets being dropped in the CPPR-SNMP-CLASS class, which matches SNMP traffic and is policed to 200 p/s.

**Step 8** Stop the flooding process on the client PC by closing the **udpc.exe** command-line window.

## Activity Verification

You have completed this task when you have completed all the steps listed in the Activity Procedure section.

- Examine statistics from the control plane protection feature.

```
ISR-PxR1#show policy-map control-plane host
 Control Plane Host

  Service-policy input: CPPR-POLICY

    Class-map: CPPR-SNMP-CLASS (match-all)
```

 © 2010 Cisco Systems, Inc.

```
      963680 packets, 977171520 bytes
      5 minute offered rate 21809000 bps, drop rate 32000 bps
      Match: access-group name CPPR-SNMP
      police:
          rate 200 pps, burst 48 packets
        conformed 16440 packets; actions:
          transmit
        exceeded 947250 packets; actions:
          drop
        conformed 184 pps, exceed 10449 pps

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

# Task 2: Configure Management Plane Protection

In this task, you will enable the MPP feature to only allow management traffic on a dedicated router interface.

## Activity Procedure

Complete these steps:

**Step 1** Log in to the Server B system. From the Server B system, attempt to use Telnet to connect to the ISR-PxR2 router FastEthernet0/1 (10.x.2.1) interface using the PuTTY client on the desktop. Your Telnet session should succeed.

**Step 2** Log in to the client PC. From the client PC, attempt to use Telnet to connect to the ISR-PxR2 router FastEthernet0/1 (10.x.2.1) interface using the PuTTY client on the desktop. Your Telnet session should succeed.

**Step 3** On the ISR-PxR2 router, configure the FastEthernet0/1 interface as a dedicated management interface using the MPP feature. Allow only the Telnet and SSH management protocols. This should allow only the Server B system to manage the router, over the FastEthernet0/1 management interface.

**Step 4** From the Server B system, attempt to use Telnet to connect to the ISR-PxR2 router FastEthernet0/1 interface. Your Telnet session should succeed.

**Step 5** From the client PC, attempt to use Telnet to connect to the ISR-PxR2 router FastEthernet0/1 interface. Your Telnet session should fail.

## Activity Verification

You have completed this task when you attain these results:

- Verify the MPP feature using the **show management-interface** command. Confirm that the FastEthernet0/1 interface of PxR2 is configured as a dedicated management interface.

```
ISR-PxR2#show management-interface
Management interface FastEthernet0/1
        Protocol        Packets processed
             ssh                0
          telnet                179
```

- You are able to use Telnet to connect to the ISR-PxR2 FastEthernet0/1 interface from the Server B host only when the MPP feature is enabled on the PxR2 FastEthernet0/1 interface.

# Task 3: Configure Unicast Reverse Path Forwarding

In this task, you will configure strict uRPF, which verifies that the packet is coming through the expected interface. Packets coming from unexpected (from the RIB and FIB perspective) interfaces will be dropped.

## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR2 router, remove the MPP feature from the control plane.

**Step 2** On the ISR-PxR1 router, enable Cisco Express Forwarding, or verify that Cisco Express Forwarding has already been enabled.

**Step 3** On the ISR-PxR1 router, configure a numbered extended access list, which denies IP traffic from any source to any destination and logs all denied traffic. The uRPF feature, when it decides to deny a packet that is based on FIB lookup, will compare the offending packet to this ACL.

**Note** This access list is used only to log all packets that are denied by strict uRPF.

**Step 4** Configure the strict uRPF feature on the FastEthernet0/0 interface of the ISR-PxR1 router. Allow local ping tests to this interface, and specify the configured extended access list as its argument.

**Step 5** On the ISR-PxR2 router, create a loopback interface and configure it with the 10.1.1.11 IP address and a mask of 255.255.255.255. This is a spoofed address, representing, for example, a management host on the network where the client PC resides.

**Step 6** On the ISR-PxR2 router, try to ping the 192.168.1.10 IP address of router ISR-PxR1 with the spoofed source IP address configured on the loopback interface.

**Note** You should see packets, which are rejected by the uRPF logging access list, on ISR-PxR1.

**Step 7** On ISR-PxR1, verify the configuration and operation of uRPF on interface FastEthernet0/0 and the number of drops.

## Activity Verification

You have completed this task when you attain these results:

- On the ISR-PxR2, try to ping the 192.168.1.10 IP address of the ISR-PxR1 router with the spoofed source IP address configured on the loopback interface, and receive the log of denied packets on ISR-PxR1:

```
ISR-PxR2#ping 192.168.1.10 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2
seconds:
Packet sent with a source address of 10.1.1.11
.....
Success rate is 0 percent (0/5)
```

 © 2010 Cisco Systems, Inc.

```
ISR-PxR1(config-if)#
06:55:35: %SEC-6-IPACCESSLOGDP: list 199 denied icmp 10.1.1.11
(FastEthernet0/0 0017.5926.3e78) -> 192.168.1.10 (0/0), 1
packet
```

- Verify the configuration and operation of uRPF on interface FastEthernet0/0 and the number of drops:

```
ISR-PxR1#show ip interfaces FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.10 255.255.255.0
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: uRPF, MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  IP verify source reachable-via RX, allow self-ping, ACL 199
   5 verification drops
   0 suppressed verification drops
```

```
                0 verification drop-rate
```

# Task 4: Configure Cisco FPM

In this task, you will configure Cisco FPM, which is another traffic filtering option that is more flexible and granular than ACLs, but less performance-demanding than IPS functionality. You will provide a filtering defense against a worm that uses HTTP to infect other endpoints using an attack that can be characterized by the **cmd.exe** string inside the HTTP request URI or arguments.

## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR2 router, remove the loopback interface that was created in the previous task.

**Step 2** On the client PC, click the TFTP server icon (TFTPSRV.EXE) on the desktop.

**Note** You will configure FPM after transferring PHDF files from the client PC to the flash file system of the ISR-PxR1 router.

**Step 3** On the client PC, choose the **Options > Server Root Directory** option to set the TFTP server root directory to C:/Secure, in which PHDF files are located.

**Step 4** On the ISR-PxR1 router, copy the **ip.phdf** and **tcp.phdf** files from the TFTP server on the client PC (10.1.1.10) to the flash file system of the ISR-PxR1 router.

**Step 5** On the ISR-PxR1 router, load PHDF files from the flash file system to the running memory of the router.

**Step 6** On the ISR-PxR1 router, create FPM policy on the FastEthernet0/1 interface. This policy should drop all packets containing the “cmd.exe” string in the first 256 bytes of any TCP segment.

## Activity Verification

You have completed this task when you attain these results:

- On the ISR-PxR1 router, ensure that the **ip.phdf** and **tcp.phdf** files have been transferred to flash:

```
ISR-PxR1#show flash:
-#- --length-- -----date/time------ path
1     51130820 Dec 17 2009 18:08:44 c2800nm-advipservicesk9-
mz.124-15.T5.bin
2         1823 Dec 17 2009 18:13:58 sdmconfig-2811.cfg
3         1826 Dec 17 2009 18:14:04 sdmconfig-28xx.cfg
4         1038 Dec 17 2009 18:14:08 home.shtml
5       527849 Dec 17 2009 18:14:16 128MB.sdf
6      6036480 Dec 17 2009 18:14:42 sdm.tar
7       861696 Dec 17 2009 18:14:50 es.tar
8       113152 Dec 17 2009 18:14:56 home.tar
9      1164288 Dec 17 2009 18:15:04 common.tar
10      793739 Dec 17 2009 18:15:12 256MB.sdf
11        2679 Mar 18 2010 12:35:34 ip.phdf
12        2444 Mar 18 2010 12:51:02 tcp.phdf
```

 © 2010 Cisco Systems, Inc.

**Step 7** On the client PC, open the Internet Explorer browser. Paste the content of the C:\Secure\Directory-traversal.txt file to the Internet Explorer address bar. Inside the address bar, replace x with your pod number and press **Enter**.

**Note** In this step, you are simulating a directory traversal attack against the 10.x.2.10 HTTP server. The HTTP query includes the "**cmd.exe**" string, which simulates a worm attack.

- On the ISR-PxR1 router, check the number of packets that are matched by your access-control class map:

```
ISR-PxR1#show policy-map type access-control interface
FastEthernet 0/1
 FastEthernet0/1

  Service-policy access-control input: WAN-POLICY

    Class-map: IP-TCP (match-all)
      58 packets, 8825 bytes
      5 minute offered rate 0 bps
      Match: field IP protocol eq 0x6 next TCP

      Service-policy access-control : HTTP-WORM-POLICY

        Class-map: HTTP-WORM-CLASS (match-all)
          2 packets, 1072 bytes
          5 minute offered rate 0 bps
          Match: field TCP dest-port eq 80
          Match: start TCP payload-start offset 0 size 256
string "cmd.exe"
      drop

        Class-map: class-default (match-any)
          56 packets, 7753 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

    Class-map: class-default (match-any)
      12 packets, 888 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

- If you repeat your simulation of a directory traversal attack, the number of packets that are matched should increase. Check the number of packets that are matched to the access-control class after your second simulation of the directory traversal attack:

```
ISR-PxR1#show policy-map type access-control interface
FastEthernet 0/1

 FastEthernet0/1

  Service-policy access-control input: WAN-POLICY
```

```
    Class-map: IP-TCP (match-all)
      62 packets, 10017 bytes
      5 minute offered rate 0 bps
      Match: field IP protocol eq 0x6 next TCP

      Service-policy access-control : HTTP-WORM-POLICY

        Class-map: HTTP-WORM-CLASS (match-all)
          4 packets, 2144 bytes
          5 minute offered rate 0 bps
          Match: field TCP dest-port eq 80
          Match: start TCP payload-start offset 0 size 256
string "cmd.exe"
      drop

        Class-map: class-default (match-any)
          58 packets, 7873 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

    Class-map: class-default (match-any)
      12 packets, 888 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

# Task 5: Configure Flexible NetFlow

In this task, you will configure Flexible NetFlow on the ISR-PxR1 router and observe information on collected flows on the NetFlow collector that is installed on the client PC system.

## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR1 router, create a Flexible NetFlow exporter. Inside the flow exporter object:

- Define the export destination as the IP address of the client PC system.
- Specify UDP as the transport protocol and the UDP destination port number, which is 9996.
- Configure NetFlow Version 5 export as the export protocol.

**Step 2** On the ISR-PxR1 router, create a named Flexible NetFlow monitor. Inside the flow monitor object:

- Specify that the default traditional NetFlow data set should be monitored and exported.
- Specify the configured exporter for this monitor.

**Step 3** On the ISR-PxR1 router, apply the configured flow monitor to the FastEthernet0/1 interface facing to client PC in the input direction.

 © 2010 Cisco Systems, Inc.

**Step 4** On the client PC, double-click the **Solarwinds Real-Time NetFlow Analyzer** icon on the desktop to start the NetFlow analyzer application.

**Step 5** On the client PC, inside the Solarwinds Real-Time NetFlow Analyzer application, in the lower part of its main window, change the listening port to **9996** and click **Apply**.

**Step 6** On the client PC, inside the Solarwinds Real-Time NetFlow Analyzer application, add the ISR-PxR1 device in the application toolbar by clicking **Tools > Add NetFlow Device**. Set the IP address to 10.x.1.1, in which x is your pod number, and set its SNMP community to **public**.

**Step 7** On the client PC, inside the Solarwinds Real-Time NetFlow Analyzer application, the ISR-PxR1 device should appear in the lower part of the window. Ensure that the green check box appears for FastEthernet0/1 in the "Sending NetFlow" column. By clicking the + sign next to the name of the router, you can obtain the list of all interfaces in the ISR-PxR1 router.

**Step 8** On the client PC, inside the Solarwinds Real-Time NetFlow Analyzer application, select the FastEthernet0/1 interface and click **Start Flow Capture**.

**Step 9** On the client PC, ping the IP address of the Server B system (10.x.2.10).

**Step 10** On the client PC, using the PuTTY Telnet client, initiate a Telnet session for ISR-PxR1 (10.x.1.1).

**Step 11** On the ISR-PxR1 router, verify that NetFlow data is being exported to the configured NetFlow export destination.

**Step 12** On the ISR-PxR1 router, examine the NetFlow caches created by the NetFlow flow monitor.

| **Note** | Nonempty caches are a good indication that NetFlow is working properly. |
|---|---|

**Step 13** On the client PC, inside the Solarwinds Real-Time NetFlow Analyzer application, in the panel on the left side, examine the Applications, Conversations, and Protocols panes. You should discover that Telnet and ICMP traffic was seen flowing in the ingress direction on the ISR-PxR1 FastEthernet0/1 interface.

**Step 14** When you are finished, on the client PC, inside the Solarwinds Real-Time NetFlow Analyzer application, select the FastEthernet0/1 interface and click **Stop Flow Capture**.

## Activity Verification

You have completed this task when you attain these results:

- On the ISR-PxR1 router, verify that NetFlow data has been exported to the NetFlow collector:

```
ISR-PxR1#show flow exporter statistics
Flow Exporter MYEXPORTER:
  Packet send statistics (last cleared 02:46:17 ago):
    Successfully sent:         162                    (16728
bytes)

  Client send statistics:
    Client: Flow Monitor MYMONITOR
      Records added:           26
```

```
    - sent:                 26
  Bytes added:              1248
    - sent:                 1248
```

- On the ISR-PxR1 router, examine the NetFlow cache that is created by the NetFlow flow monitor while traffic is being switched by the router:

```
ISR-PxR1#show flow monitor name MYMONITOR cache format table
  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                               3
  High Watermark:                                4

  Flows added:                                  40
  Flows aged:                                   37
    - Active timeout      (  1800 secs)          4
    - Inactive timeout    (    15 secs)         33
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0

IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT
INTF INPUT            FLOW SAMPLER ID  IP TOS  IP PROT  ip src
as  ip dst as  ipv4 next hop addr  ipv4 src mask  ipv4 dst
mask  tcp flags  intf output               bytes        pkts
time first     time last
===============  ===============  =============  =============
====================  ===============  ======  =======
=========  =========  ==================  =============
=============  =========  ====================  ==========
==========  ============  ============
10.1.1.10        10.1.2.10                     0           2048
Fa0/1                                 0  0x00          1
0          0  192.168.1.20                /24           /24
0x00       Fa0/0                       240           4
10:52:34.271  10:52:37.287
10.1.1.10        10.1.1.1                   1160            23
Fa0/1                                 0  0x00          6
0          0  0.0.0.0                     /24           /0
0x1B       Null                         645           15
10:52:39.143  10:52:42.291
```

 © 2010 Cisco Systems, Inc.

# Lab 2-1: Configuring Basic Zone-Based Policy Firewall Features

Complete this lab activity to practice what you learned in the related module.

## Activity Objective

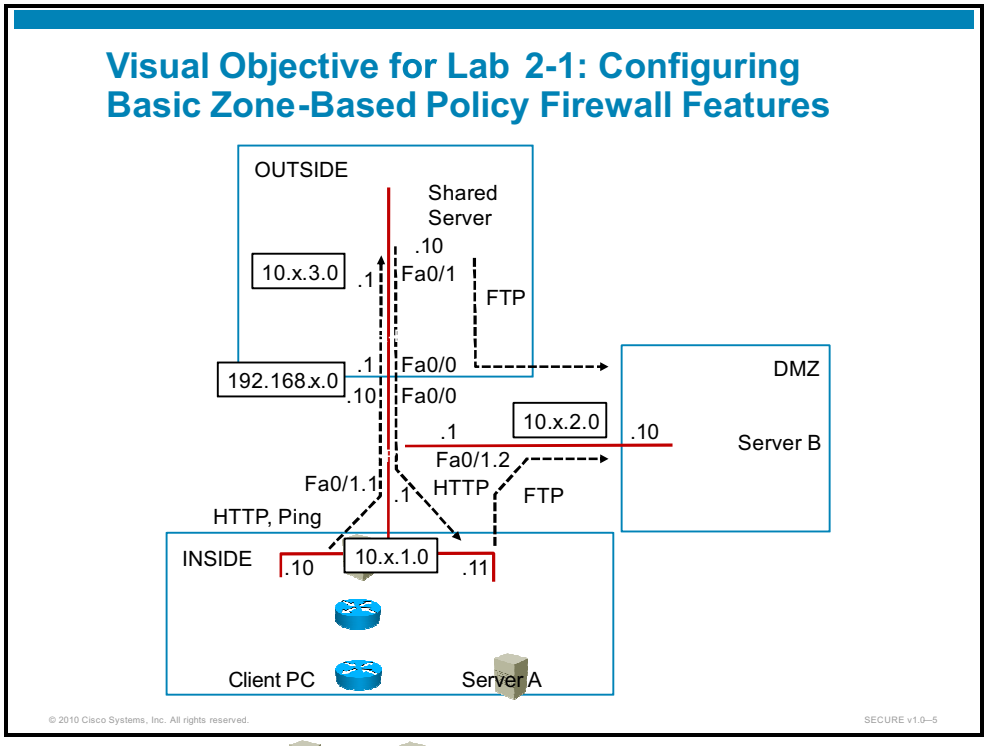
In this activity, you will configure and verify the OSI Layer 3–4 access control features of the Zone-Based Policy Firewall. You will configure three zones and configure access control between them.

After completing this activity, you will be able to meet these objectives:

- Configure zones
- Configure access between the internal and external zones
- Configure access between the internal and DMZ zones
- Configure access between the external and DMZ zones
- Configure inspection of local (self-zone) traffic

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Pod ISR routers
- Pod client PC, Server A, and Server B systems

- Shared backbone ISR router

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **auto-summary** | Allows automatic summarization of subnet routes into network-level routes. To disable this function and send subprefix routing information across classful network boundaries, use the no form of this command. |
| **ip access-list extended** *access-list-name* | Defines the extended IP access list. |
| **ip address** *ip-address* **port** *port-number* | Configures a proxy IP address on an SSL VPN gateway and specifies the port number for proxy traffic. |
| **ip host** *hostname ip-address* | Defines static hostname-to-address mappings in the DNS hostname cache. |
| **network** *ip-address* [*wildcard-mask*] | Specifies the network for an EIGRP routing process. |
| **peer** *ip-address* | Sets the peer IP address for the VPN connection. |
| **permit** *source* [*source-wildcard*] **permit** *protocol source source-wildcard destination destination-wildcard* | Sets conditions to allow a packet to pass a named IP access list in access list configuration mode. |
| **ping** | Determines if other IP addresses are accessible. |
| **router eigrp** *autonomous-system-number* | Configures the EIGRP routing process. |
| **show running-config** | Displays the configuration that is currently running on the adaptive security appliance. |
| **username** *name* **privilege** *level* **password** *password* | Establishes a username-based authentication system with privilege level specified. |
| **zone security** *zone-name* | Creates a security zone. |
| **zone-member security** *zone-name* | Attaches an interface to a security zone in interface configuration mode. |
| **zone-pair security** *zone-pair-name* **source** {*source-zone-name* \| **self** \| default} **destination** {*destination-zone-name* \| **self** \| **default**} | Creates a zone pair in global configuration mode. |
| **show zone security** *security-zone-name* | Displays zone security information. |
| **class-map type inspect** [**match-any** \| **match-all**] *class-map-name* | Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type class map. |
| **match access-group** {*access-group* \| **name** *access-group-name*} | Configures the match criteria for a class map based on the specified ACL. |

 © 2010 Cisco Systems, Inc.

| Command | Description |
|---|---|
| **match protocol** *protocol-name* | Configures the match criterion for a class map based on the specified protocol. |
| **policy-map type inspect** *policy-map-name* | Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map. |
| **inspect** | Enables Cisco IOS stateful packet inspection in policy-map-class configuration mode. |
| **drop [log]** | Drops packets that are sent to the router in policy-map-class configuration mode. |
| **class type inspect** *class-map-name* | Specifies the traffic (class) on which an action is to be performed in policy-map configuration mode. |
| **service-policy type inspect** *policy-map-name* | Attaches a firewall policy map to a zone-pair in zone-pair configuration mode. |
| **show policy-map type inspect [***policy-map-name***] [class** *class-map-name***]** | Displays a specified policy map. |
| **show policy-map type inspect zone-pair [***zone-pair-name***] [sessions]** | Displays the runtime inspect-type policy map statistics and other information such as sessions existing on a specified zone pair. |
| **telnet** *host* | Logs in to a host that supports Telnet. |

# Job Aids

These job aids are available to help you complete the lab activity.

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username | |
| Password | |

# Task 1: Configure Zones

In this task, you will create three named zones, assign router interfaces to zones, and create zone pairs that require interaction.

## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR2 router, globally create zones named INSIDE, DMZ, and OUTSIDE.

**Step 2** On the ISR-PxR2 router, assign interfaces to zones:

- Assign the FastEthernet0/0 interface to zone OUTSIDE.
- Assign the FastEthernet0/1.1 subinterface to zone INSIDE.
- Assign the FastEthernet0/1.2 subinterface to zone DMZ.

**Step 3** Create zone pairs that will require interaction:

- INSIDE to OUTSIDE
- OUTSIDE to INSIDE
- OUTSIDE to DMZ

## Activity Verification

You have completed this task when you attain these results:

- On ISR-PxR2 display, the zone descriptions and interfaces that are associated with the three zones are the following:

```
ISR-PxR2#show zone security
zone self
  Description: System defined zone

zone INSIDE
  Member Interfaces:
    FastEthernet0/1.1

zone DMZ
  Member Interfaces:
    FastEthernet0/1.2

zone OUTSIDE
  Member Interfaces:
    FastEthernet0/0
```

 © 2010 Cisco Systems, Inc.

# Task 2: Configure Access Control Between the INSIDE and OUTSIDE Zones

In this task, you will configure access control between the INSIDE and OUTSIDE zones.

## Activity Procedure

Complete these steps:

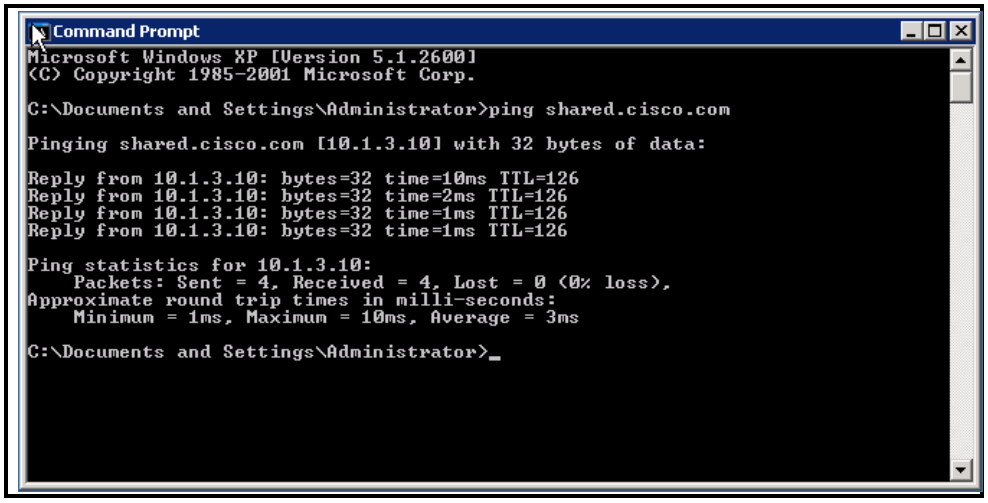
**Step 1** On the ISR-PxR2 router, configure the following access policy using the Zone-Based Policy Firewall configuration language:

- Any host in the INSIDE zone should be allowed access any host in the OUTSIDE zone, using the HTTP and ping (ICMP echo) protocols.
- Any host in the OUTSIDE zone should be allowed to send any ICMP *destination unreachable* message to hosts in the INSIDE zone. These messages should be *statelessly* passed to the INSIDE zone.
- All denied traffic should be logged.

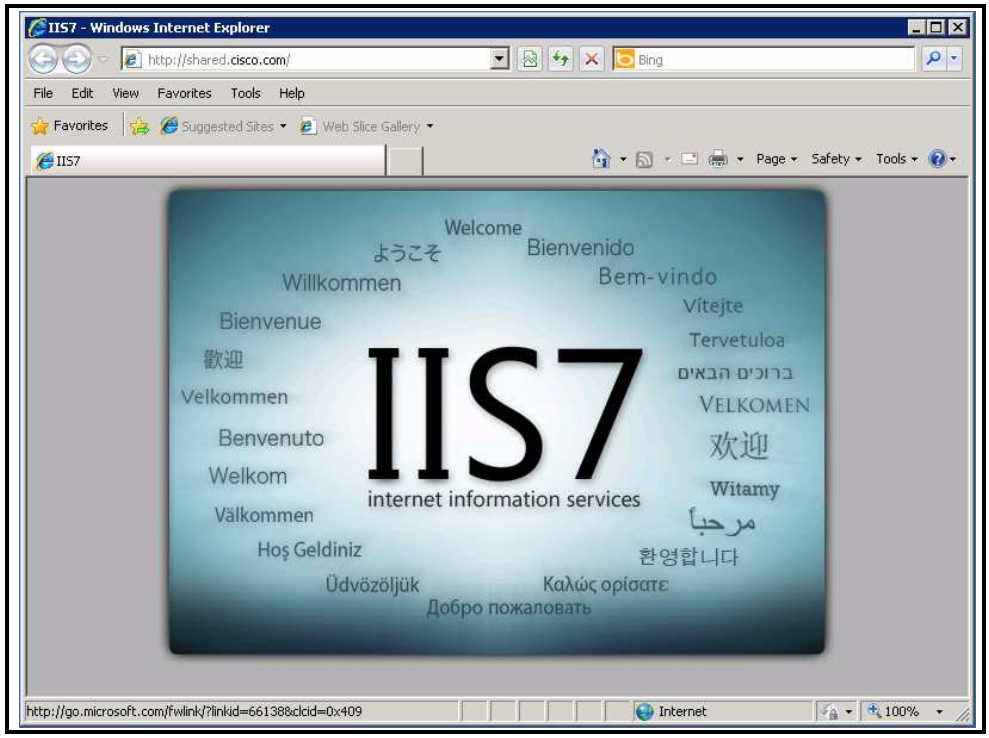
## Activity Verification

You have completed this task when you attain these results:

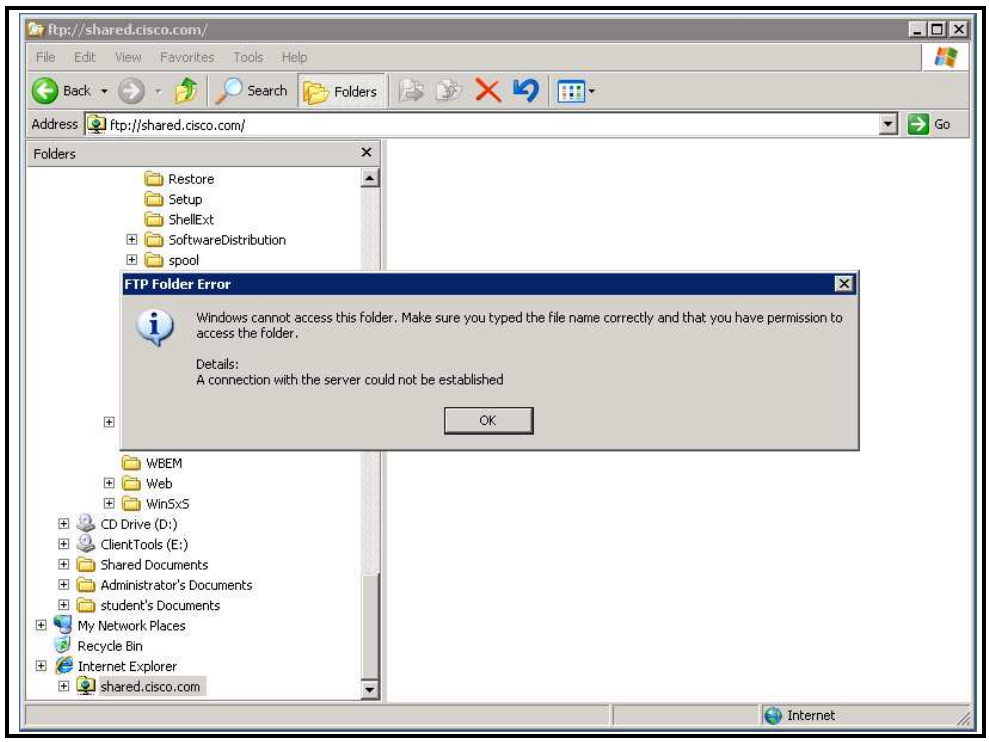
- From the client PC, ping the shared server (10.x.3.10) in the OUTSIDE zone, which is accessible using the shared.cisco.com hostname. Your attempt should be successful.




- From the client PC, verify HTTP connectivity over the firewall to the shared server in the OUTSIDE, which is accessible at **http://shared.cisco.com**. Your attempt should be successful.




- From the client PC, verify FTP connectivity to the shared server. Your attempt should fail, because FTP packets are dropped because of default-deny policy settings.




- Observe the syslog messages that you receive on the console of the ISR-PxR2 router:

```
04:52:09: %FW-6-DROP_PKT: Dropping tcp session 10.1.1.10:1038
10.1.3.10:21 on zone-pair IN-TO-OUT class class-default due to
DROP action found in policy-map with ip ident 0
```

```
04:53:04: %FW-6-LOG_SUMMARY: 3 packets were dropped from
10.1.1.10:1038 => 10.1.3.10:21 (target:class)-(IN-TO-
OUT:class-default)
```

 © 2010 Cisco Systems, Inc.

```
04:53:04: %FW-6-LOG_SUMMARY: 3 packets were dropped from
10.1.1.10:1039 => 10.1.3.10:21 (target:class)-(IN-TO-
OUT:class-default)
04:53:04: %FW-6-LOG_SUMMARY: 3 packets were dropped from
10.1.1.10:1040 => 10.1.3.10:21 (target:class)-(IN-TO-
OUT:class-default)
```

- Display a policy map along with its class maps, and display session statistics, including the number of dropped packets in its class-default class:

```
ISR-PxR2#show policy-map type inspect zone-pair
No policy attached on zp OUT-TO-DMZ
No policy attached on zp OUT-TO-IN

policy exists on zp IN-TO-OUT
 Zone-pair: IN-TO-OUT

  Service-policy inspect : IN-TO-OUT-POLICY

    Class-map: IN-TO-OUT-CLASS (match-all)
      Match: access-group name IN-TO-OUT-ACL

   Inspect
        Packet inspection statistics [process switch:fast
switch]
        tcp packets: [0:11]
        icmp packets: [0:16]

        Session creations since subsystem startup or last
reset 3
        Current session counts (estab/half-open/terminating)
[0:0:0]
        Maxever session counts (estab/half-open/terminating)
[1:1:0]
        Last session created 00:19:44
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0


    Class-map: class-default (match-any)
      Match: any
      Drop
        9 packets, 252 bytes

policy exists on zp OUT-TO-IN
 Zone-pair: OUT-TO-IN
```

```
  Service-policy inspect : OUT-TO-IN-POLICY

    Class-map: OUT-TO-IN-CLASS (match-all)
      Match: access-group name OUT-TO-IN-ACL

   Inspect
        Packet inspection statistics [process switch:fast
switch]
        tcp packets: [0:10]

        Session creations since subsystem startup or last
reset 1
        Current session counts (estab/half-open/terminating)
[0:0:0]
        Maxever session counts (estab/half-open/terminating)
[1:1:0]
        Last session created 00:15:23
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0


    Class-map: class-default (match-any)
      Match: any
      Drop
        12 packets, 480 bytes
```

# Task 3: Configure Access Control Between the OUTSIDE and DMZ Zones

In this task, you will configure access between the OUTSIDE and DMZ zones. Hosts in the OUTSIDE zone should be able to access Server B inside the DMZ zone, using the FTP protocol.

## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR2 router, configure the following access policy using the Zone-Based Policy Firewall configuration language:

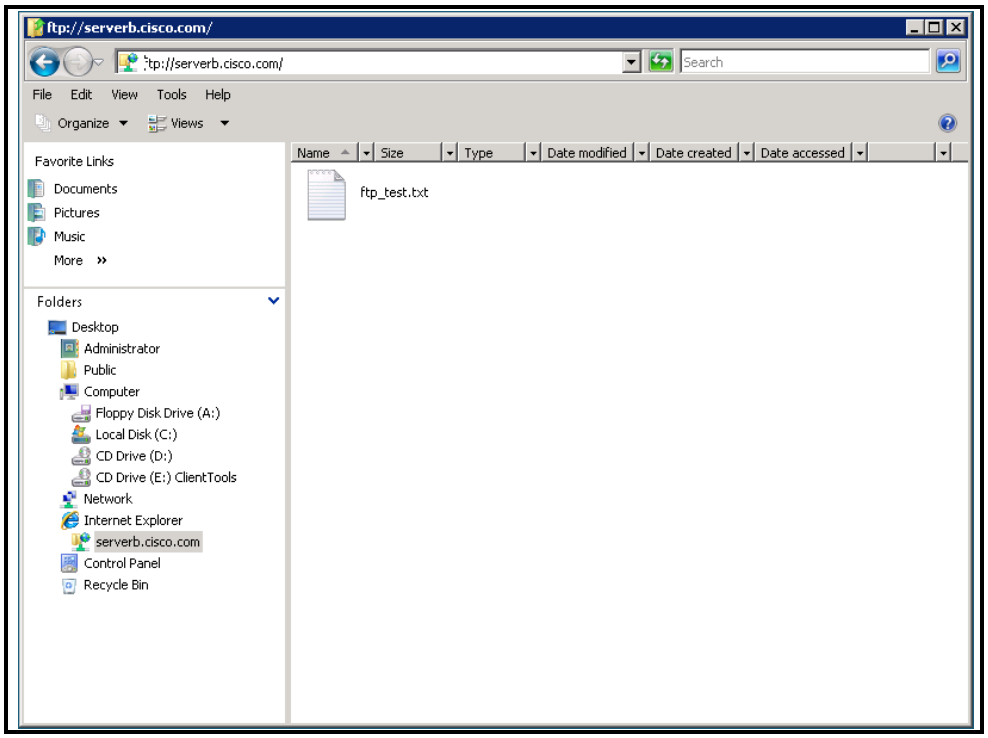
- Any host in the OUTSIDE zone should be allowed FTP access to Server B in the DMZ zone.
- All denied traffic should be logged.

 © 2010 Cisco Systems, Inc.

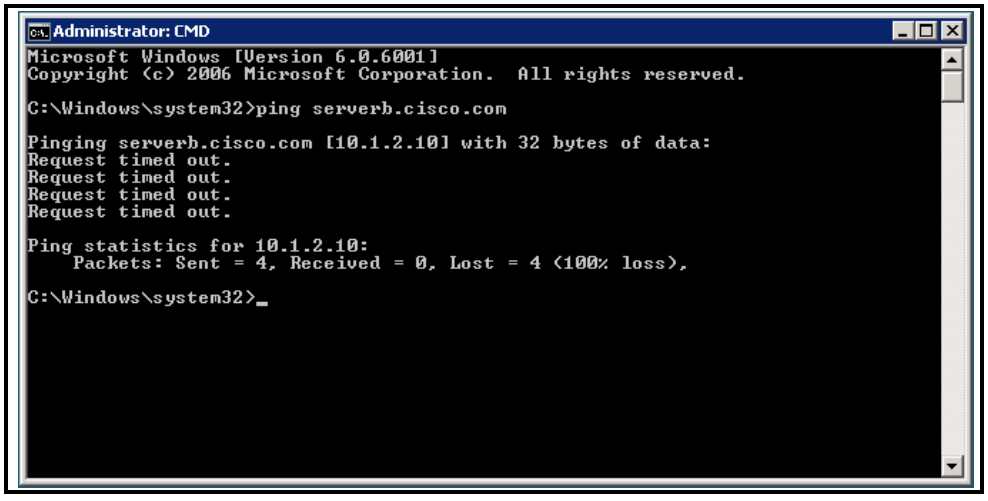
## Activity Verification

You have completed this task when you attain these results:

- From the shared server, verify FTP connectivity to Server B, which is accessible at **ftp://serverb.cisco.com**. Your attempt should be successful.




- From the shared server, ping the Server B host. Your attempt should fail. ICMP ping packets are dropped because of the default-deny policy between zones.




- Observe the log messages that you will receive on the ISR-PxR2 console:

```
07:31:31: %FW-6-DROP_PKT: Dropping icmp session 10.1.3.10:0
10.1.2.10:0 on zone-pair OUT-TO-DMZ class class-default due to
DROP action found in policy-map with ip ident 0
07:32:04: %FW-6-LOG_SUMMARY: 4 packets were dropped from
10.1.3.10:8 => 10.1.2.10:0 (target:class)-(OUT-TO-DMZ:class-
default)
```

- Display a policy map OUT-TO-DMZ, along with its class maps, and display session statistics, including the number of dropped packets in its class-default class:

**Note** You should see a nonzero number of packets being inspected for zone pair OUT-TO-DMZ. You should also see a nonzero number of packets being dropped for zone pairs OUT-TO-DMZ.

```
ISR-PxR2#show policy-map type inspect zone-pair OUT-TO-DMZ

policy exists on zp OUT-TO-DMZ
 Zone-pair: OUT-TO-DMZ

  Service-policy inspect : OUT-TO-DMZ-POLICY

    Class-map: OUT-TO-DMZ-CLASS (match-all)
      Match: access-group name OUT-TO-DMZ-ACL
      Match: protocol ftp

   Inspect
        Packet inspection statistics [process switch:fast
switch]
        tcp packets: [5:33]

        Session creations since subsystem startup or last
reset 2
        Current session counts (estab/half-open/terminating)
[0:0:0]
        Maxever session counts (estab/half-open/terminating)
[2:1:1]
        Last session created 00:11:44
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 2
        Last half-open session total 0
        TCP reassembly statistics
        received 1 packets out-of-order; dropped 0
        peak memory usage 1 KB; current usage: 0 KB
        peak queue length 1


    Class-map: class-default (match-any)
      Match: any
      Drop
        4 packets, 160 bytes
```

# Task 4: Configure Inspection of Local Traffic

In this task, you will configure access control between the INSIDE and "self" zones of the ISR-PxR2 router.

 © 2010 Cisco Systems, Inc.

## Activity Procedure

Complete these steps:

**Step 1** On ISR-PxR2, inside the EIGRP routing process, configure interface FastEthernet0/1.1 as a passive interface using the **passive-interface FastEthernet 0/1.1** command, to eliminate the log messages because of denied EIGRP packets in the lab infrastructure.

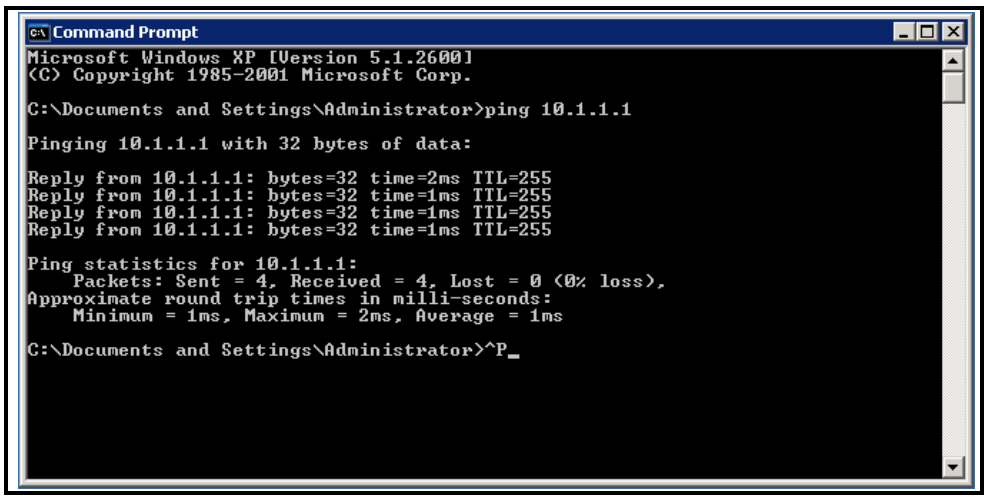
**Step 2** On the ISR-PxR2 router, configure the following access policy using the Zone-Based Policy Firewall configuration language:

- All hosts in the INSIDE zone should be able to use Telnet to connect to the ISR-PxR2 router (10.x.2.1).
- All hosts in the INSIDE zone should be able to ping the ISR-PxR2 router (10.x.2.1).
- All denied traffic should be logged.

## Activity Verification

You have completed this task when you attain these results:

- From the client PC, verify Telnet connectivity to the ISR-PxR2 router (10.x.2.1). Your attempt should be successful.
- From the client PC, ping the ISR-PxR2 router (10.x.2.1). Your attempt should be successful.




- Display a policy map IN-TO-SELF along with its class maps, and display session statistics, including the number of dropped packets in its class-default class:

**Note** You should see a nonzero number of packets being inspected for zone pair IN-TO-SELF. You should also see a nonzero number of packets being dropped for zone pairs IN-TO-SELF.

```
ISR-PxR2#show policy-map type inspect zone-pair IN-TO-SELF

policy exists on zp IN-TO-SELF
 Zone-pair: IN-TO-SELF

  Service-policy inspect : IN-TO-SELF-POLICY
```

```
    Class-map: IN-TO-SELF-CLASS (match-all)
      Match: access-group name IN-TO-SELF-ACL

   Inspect
        Packet inspection statistics [process switch:fast
switch]
        tcp packets: [16:19]
        icmp packets: [4:4]

        Session creations since subsystem startup or last
reset 2
        Current session counts (estab/half-open/terminating)
[0:0:0]
        Maxever session counts (estab/half-open/terminating)
[1:1:1]
        Last session created 00:17:42
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0


    Class-map: class-default (match-any)
      Match: any
      Drop
        18 packets, 2584 bytes
```

 © 2010 Cisco Systems, Inc.

# Lab 2-2: Configuring Advanced Zone-Based Policy Firewall Features

Complete this lab activity to practice what you learned in the related module.

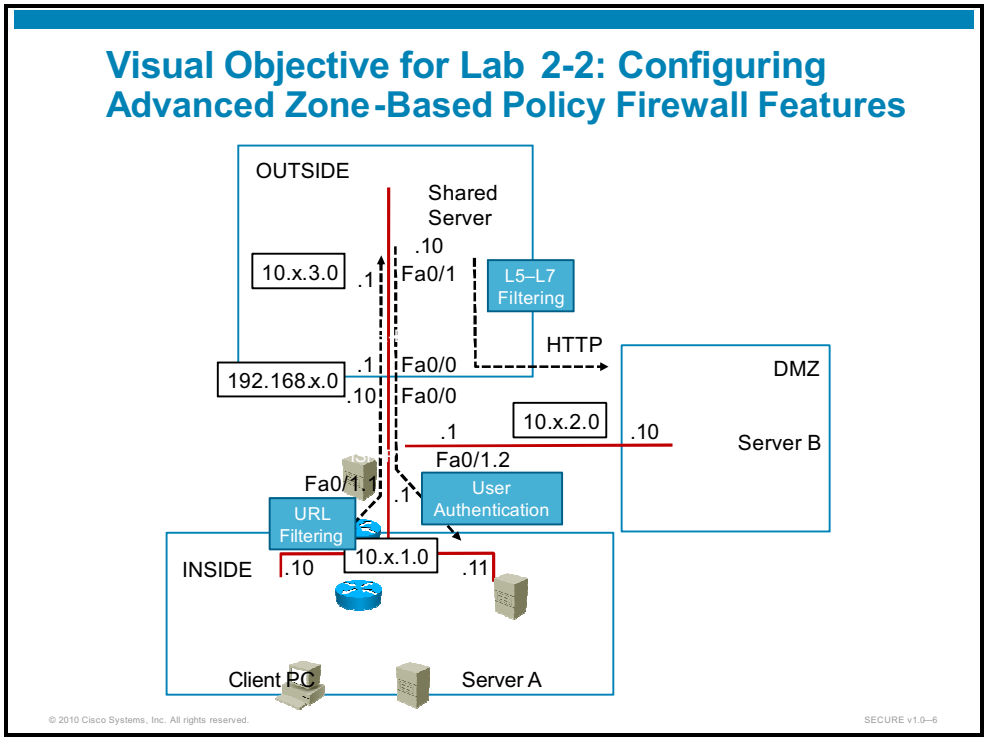
## Activity Objective

In this activity, you will configure and verify application-layer (OSI Layers 5–7) filtering, user-based access control, and content filtering controls. After completing this activity, you will be able to meet these objectives:

- Configure and verify application-layer filtering on the Zone-Based Policy Firewall
- Configure and verify URL filtering
- Configure and verify user-based firewalling

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Pod ISR routers
- Pod client PC, Server A, and Server B systems
- Shared backbone ISR router

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **aaa attribute list** *list-name* | Defines an AAA attribute list locally on a router. |
| **aaa authentication login {default \|** *list-name***} {passwd-expiry** *method1* **[***method2***...]}** | Sets AAA at login. |
| **aaa authorization auth-proxy {default \|** *list-name***} [***method1* **[method2...]]** | Configures the authentication proxy feature to use local authorization. |
| **aaa new-model** | Enables the AAA access control model in global configuration mode. |
| **attribute type supplicant-group** *user-group-name* | Defines an attribute type supplicant group that is to be added to an attribute list locally on a router. |
| **class type inspect** *class-map-name* | Specifies the traffic (class) on which an action is to be performed in policy-map configuration mode. |
| **class type urlfilter** *class-map-name* | Associates a URL filter class with a URL filtering policy map. |
| **class-map type inspect [match-any \| match-all]** *class-map-name* | Creates a Layer 3 and Layer 4 inspect-type class map. |
| **class-map type inspect** *protocol-name* **{match-any \| match-all}** *class-map-name* | Creates a Layer 7 (application-specific) inspect-type class map. |
| **class-map type urlfilter** *class-map-name* | Creates or modifies a URL filter class map. |
| **drop [log]** | Drops packets that are sent to the router in policy-map-class configuration mode. |
| **inspect** | Enables Cisco IOS stateful packet inspection in policy-map-class configuration mode. |
| **ip access-list extended** *access-list-name* | Defines the extended IP access list. |
| **ip admission** *admission-name* | Creates a Layer 3 NAC rule to be applied to the interface. |
| **ip admission name** *admission-name* **proxy {ftp \| http \| telnet} inactivity-time** *minutes* | Creates an IP NAC rule that intercepts FTP, HTTP, or Telnet sessions. |
| **log** | Logs the session matching the inspection class. |
| **match access-group {***access-group* **\| name** *access-group-name***}** | Configures the match criteria for a class map, based on the specified ACL. |
| **match protocol** *protocol-name* | Configures the match criterion for a class map, based on the specified protocol. |

 © 2010 Cisco Systems, Inc.

| Command | Description |
|---|---|
| **match req-resp protocol-violation** | Allows HTTP messages to pass through the firewall or to reset the TCP connection when HTTP noncompliant traffic is detected in class-map configuration mode. |
| **match request {uri \| arg} regex** *parameter-map-name* | Configures an HTTP firewall policy to permit or deny HTTP traffic, based on request messages of which the Uniform Resource Identifier (URI) or arguments (parameters) match a defined regular expression. |
| **match url-keyword urlf-glob** *parameter-map-name* | Configures the match criteria for a local URL filtering class map based on the URL keyword in class-map configuration mode. |
| **match user-group** *group-name* | Configures the match criterion for a class map based on the specified user group. |
| **parameter-map type regex** *parameter-map-name* | Configures a parameter-map type to match a specific traffic pattern. |
| **parameter-map type urlf-glob** *parameter-map-name* | Creates or modifies a parameter map that specifies the list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering and to place the system in parameter map configuration mode. |
| **pattern** | Specifies the regular expression that will match data inside parameter-map configuration mode. |
| **permit** *source* **[***source-wildcard***] permit** *protocol source source-wildcard destination destination-wildcard* | Sets conditions to allow a packet to pass a named IP access list in access list configuration mode. |
| **policy-map type inspect** *policy-map-name* | Creates a Layer 3 and Layer 4 inspect-type policy map. |
| **policy-map type inspect** *protocol-name policy-map-name* | Creates a Layer 7 inspect-type policy map. |
| **policy-map type inspect urlfilter** *policy-map-name* | Creates or modifies a URL filter type inspect policy map in global configuration mode. |
| **reset** | Resets the session matching the inspection class. |
| **service-policy** *protocol-name policy-map-name* | Attaches a Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map in policy-map-class configuration mode. |
| **service-policy type inspect** *policy-map-name* | Attaches a firewall policy map to a zone-pair in zone-pair configuration mode. |
| **show class-map type inspect [***protocol-name***] [***class-map-name***]** | Displays Layer 3 and Layer 4 or Layer 7 (application-specific) inspect-type class maps and their matching criteria. |
| **show epm session ip** *ip-address* | Displays information about EPM sessions specifically for an IP address. |
| **show ip admission cache** | Displays the current list of network admission entries. |
| **show policy-map type inspect [***policy-map-name***] [class** *class-map-name***]** | Displays a specified policy map, |
| **show policy-map type inspect [***policy-map-name***] [class** *class-map-name***]** | Displays a specified policy map. |

| Command | Description |
|---|---|
| **show user-group [***group-name* **\| count]** | Displays information about user groups in privileged EXEC mode. |
| **telnet** *host* | Logs in to a host that supports Telnet. |
| **username** *name* **privilege** *level* **password** *password* | Establishes a username-based authentication system with privilege level specified. |

# Job Aids

These job aids are available to help you complete the lab activity.

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username | |
| Password | |

 © 2010 Cisco Systems, Inc.

# Task 1: Configure Application-Layer Filtering on the Zone-Based Policy Firewall

In this task, you will configure application-layer filtering for HTTP traffic from the OUTSIDE zone to a server in the DMZ zone. For these flows, the ISR-PxR2 router should drop all requests that contain the pattern “cmd.exe” inside HTTP arguments.

## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR2 router, reconfigure the existing policy from the OUTSIDE zone to the DMZ zone to inspect HTTP traffic instead of FTP.

**Step 2** On the ISR-PxR2 router, create a regular expression for argument matching. You should match any capitalization of the CMD.EXE string, which represents one particular signature of malicious data in the HTTP arguments field.

**Step 3** On the ISR-PxR2 router, reconfigure the existing policy from the OUTSIDE zone to the DMZ zone to add an HTTP inspection policy that will reset and log:

- HTTP sessions containing the malicious pattern CMD.EXE in HTTP request arguments field
- HTTP sessions violating the HTTP protocol

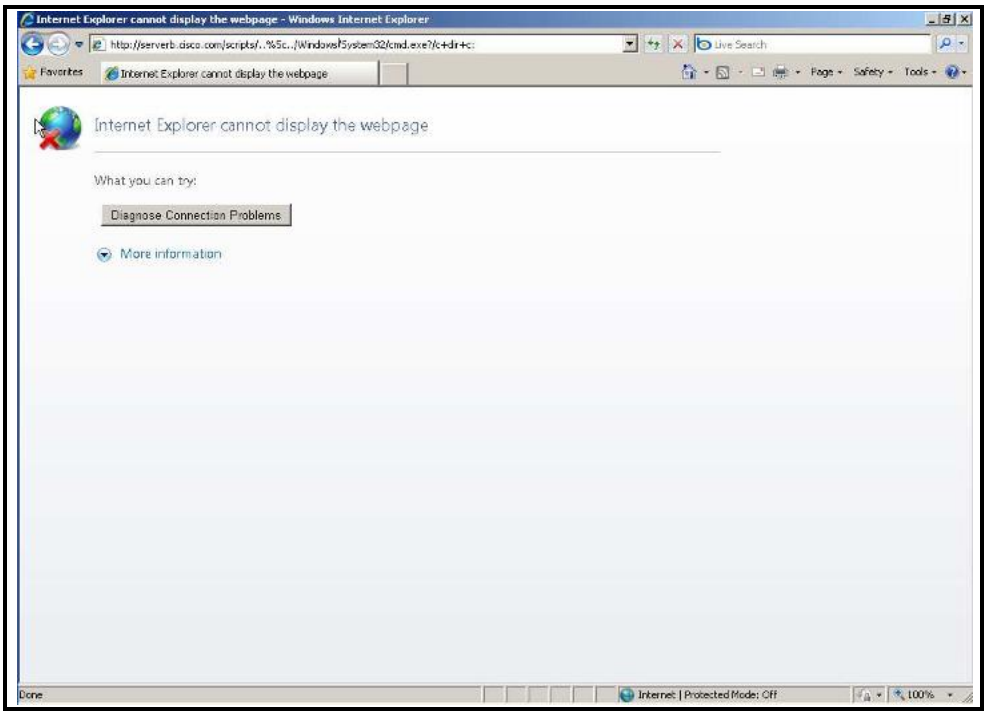
## Activity Verification

You have completed this task when you attain these results:

- From the shared server, verify HTTP connectivity to Server B, which is accessible at **http://serverb.cisco.com**. Your basic connectivity attempt should be successful.



- From the shared server, simulate a directory traversal attack against Server B by accessing the **http://serverb.cisco.com/scripts/..%5c../windows/system32/cmd.exe?/c+dir+c:** URL. Your attempt should fail, because HTTP arguments include the "cmd.exe" pattern.




- Observe the log message you will receive on the ISR-PxR2 console regarding denied traffic:

```
03:23:40: %APPFW-4-HTTP_DEOBFUSCATION: Deobfuscation signature
(15) detected - resetting session 10.1.3.10:53068 10.1.2.10:80
on zone-pair OUT-TO-DMZ class OUT-TO-DMZ-CLASS appl-class OUT-
TO-DMZ-APPLICATION-CLASS
```

- On the ISR-PxR2 router, display the configuration of the HTTP inspection class map:

```
ISR-PxR2#show class-map type inspect http
 Class Map type inspect http match-any OUT-TO-DMZ-APPLICATION-
CLASS (id 50)
   Match  request arg regex CMD-REGEX
   Match  req-resp protocol-violation
```

- On the ISR-PxR2 router, display the policy actions that are configured for the HTTP inspection class map:

```
ISR-PxR2#show policy-map type inspect http
  Policy Map type inspect http OUT-TO-DMZ-APPLICATION-POLICY
    Class OUT-TO-DMZ-APPLICATION-CLASS
      Log
      Reset
```

 © 2010 Cisco Systems, Inc.

# Task 2: Configure URL Filtering

In this task, you will use a local blacklist on the router to deny access from the INSIDE zone to sites in the OUTSIDE zone that contain the “gambling” string in their domain name.

## Activity Procedure

Complete these steps:

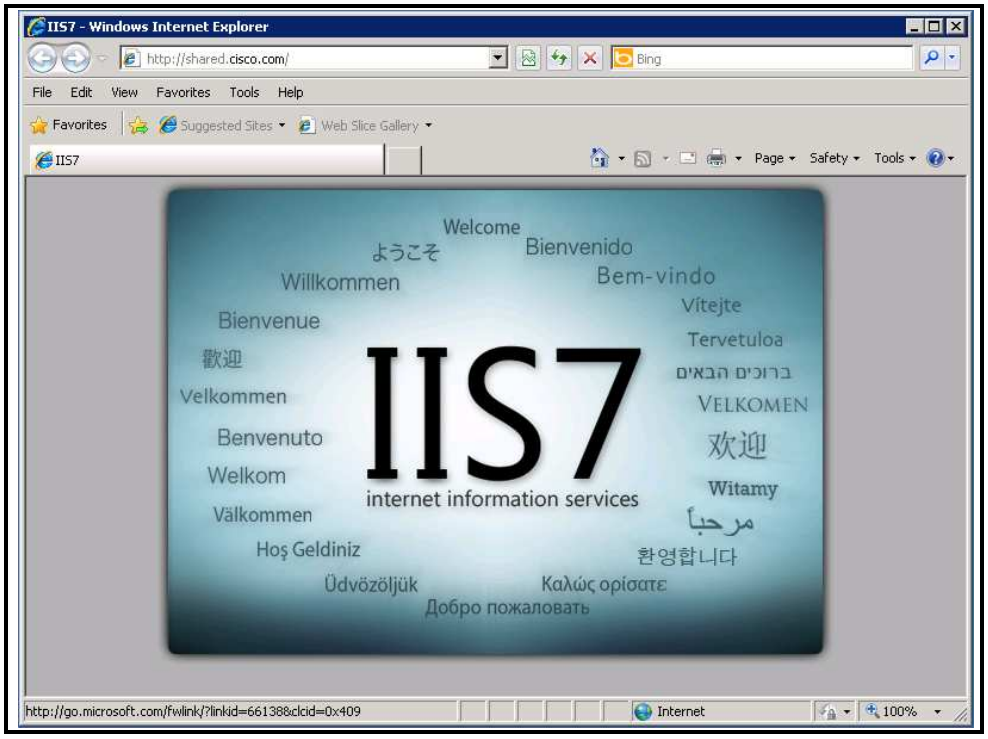
**Step 1** On the ISR-PxR2 router, define the “gambling” pattern for server domain name matching.

**Step 2** On the ISR-PxR2 router, define a local URL filtering policy that will deny access from all hosts in the INSIDE zone to sites in the OUTSIDE zone that contain the “gambling” string in their domain name.

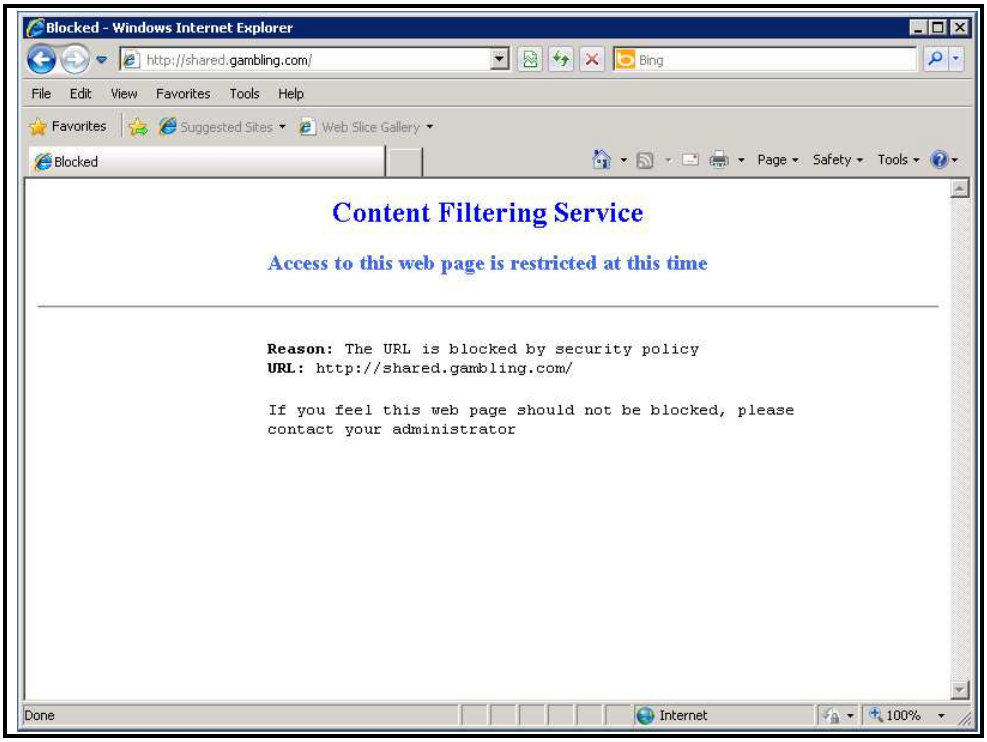
## Activity Verification

You have completed this task when you attain these results:

- From the client PC, verify HTTP connectivity to the shared server, which is accessible at **http://shared.cisco.com**. Your attempt should be successful.




- From the client PC, verify HTTP connectivity to the server accessible at the **http://shared.gambling.com** URL. Your attempt should fail, and the Content Filtering window should appear.




# Task 3: Configure User-Based Firewalling

In this task, you will configure user-based firewalling on the ISR-PxR2 router, which should intercept user sessions from the OUTSIDE zone to the DMZ zone and authenticate users before allowing access. Only users that belong to the ENGINEERING user group will be allowed to access Server B using FTP.

## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR2 router, configure a local user (enguser) and a local user group (ENGINEERING) to which the local user will belong.

**Step 2** On the ISR-PxR2 router, configure the user-based firewall with the following policy:

- The user-based firewall feature will intercept Telnet and FTP sessions on the FastEthernet0/0 interface.
- Set the caching inactivity time for user credentials to 60 minutes.
- Allow access to the DMZ Server B host using FTP for authenticated users of the ENGINEERING group.

## Activity Verification

You have completed this task when you attain these results:

- From the shared server, use Telnet to connect to Server A. The ISR-PxR2 firewall router should intercept your session and attempt to authenticate you. Authenticate as user enguser.
- From the shared server, verify FTP connectivity over the firewall to Server B. Your connection should succeed, if you are authenticated to the firewall router.
- Display the contents of the authentication proxy cache and therefore all authenticated users (along with their IP addresses) known to the ISR-PxR2 router:

 © 2010 Cisco Systems, Inc.

```
ISR-PxR2#show ip admission cache
Authentication Proxy Cache
 Client Name enguser, Client IP 10.1.3.10, Port 64099, timeout
60, Time Remaining 51, state ESTAB
```

- Display all known users belonging to user group ENGINEERING:

```
ISR-PxR2#show user-group
Usergroup : ENGINEERING
----------------------------------------------------------------
----------
User Name       Type     Interface              Learn
Age (min)
----------------------------------------------------------------
----------
10.1.3.10       IPv4     FastEthernet0/0        Dynamic
9
```

- Display user information that is associated with the IP address of the shared server:

```
ISR-PxR2#show epm session ip 10.1.3.10
Admission feature       : Authproxy
AAA Policies            :
Supplicant-Group        : ENGINEERING
```

# Lab 2-3: Configuring Cisco IOS Software IPS

Complete this lab activity to practice what you learned in the related module.

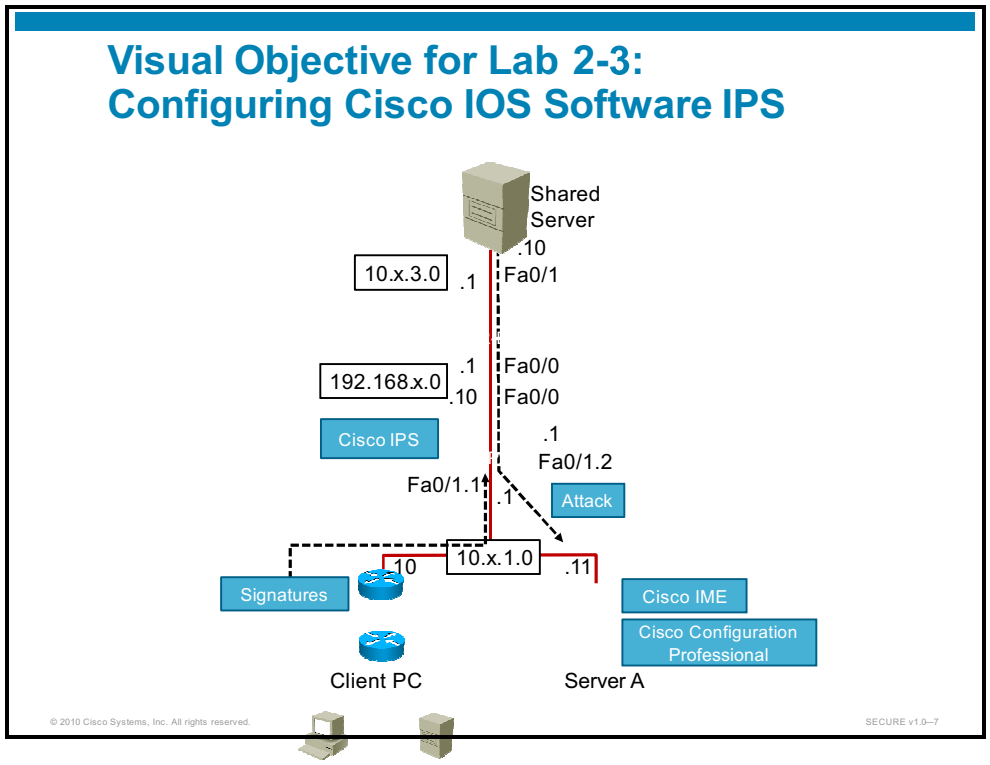
## Activity Objective

In this activity, you will configure and verify a basic Cisco IOS Software IPS sensor. You will initialize IPS functionality and configure IPS policies on the ISR-PxR2 router. After completing this activity, you will be able to meet these objectives:

- Initialize Cisco IOS Software IPS
- Configure an IPS policy
- Tune an IPS policy using SEAP
- Configure Cisco IME
- Verify signature triggering and dropping actions
- Verify IME IPS events

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Pod ISR routers
- Pod client PC and Server A systems
- Shared backbone ISR router

 © 2010 Cisco Systems, Inc.

- The shared server

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **crypto key pubkey-chain rsa** | Enters public key configuration mode. |
| **named-key** *key-name* **signature** | Indicates that the RSA public key to be specified will be a signature special-usage key. |
| **key-string** *key-string* | Specifies the RSA public key of the remote peer. |
| **ip ips config location** *url* | Specifies the location in which the router will save signature information. |
| **ip ips name** *ips-name* | Specifies an IPS rule. |
| **ip ips** *ips-name* **{in \| out}** | Applies an IPS rule to an interface. |
| **show ip ips signatures [count]** | Verifies the number of signatures active (enabled and not retired) on the router. |
| **show ip ips interfaces** | Verifies the router interfaces on which IPS functionality has been enabled. |
| **username** *name* **privilege** *level* **password** *password* | Establishes a username-based authentication system with privilege level specified. |

# Job Aids

These job aids are available to help you complete the lab activity.

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username | |
| Password | |

# Task 1: Initialize Cisco IOS Software IPS and Configure IPS Policy

In this task, you will import a known RSA public key, the corresponding private key of which is used by Cisco IPS engineering to digitally sign all signature packages. You will also load an IPS signature package to the ISR-PxR2 router.

## Activity Procedure

Complete these steps:

**Step 1** Copy the content of the **C:\SECURE\Public-crypto-key-IPS.txt** file on the client PC to the public key chain of the ISR-PxR2 router. This is the Cisco RSA public key, which is used to verify the digital signature of IPS signature packages that are loaded on the router.

**Step 2** On the ISR-PxR2 router, create a folder named **iosips** in the local file system and designate this folder as the location in which the router will save its IPS settings.

**Step 3** On the ISR-PxR2 router, create a named IPS ruleset, and apply it on the input and output of the FastEthernet0/0 interface.

**Step 4** On the client PC desktop, click the **ftpdmin.exe** desktop shortcut to start the FTP server.

**Step 5** On the ISR-PxR2 router, load the signature package from the client PC using the **ftp://10.1.1.10/SECURE/IOS-S480-CLI.pkg** URL of the signature package. It will take a while for the router to load the signature package.

**Note** Immediately after the signature package is loaded to the router, the signature compiling process will begin. When signatures in categories other than "Cisco IPS Basic" and "Cisco IPS Advanced" are unretired as a category, compilation of some signatures and engines could fail because they may not be supported by the Cisco IPS engine. All other successfully compiled (unretired) signatures will be used by Cisco IPS to scan traffic.

## Activity Verification

You have completed this task when you attain these results:

- Verify that the signature package has compiled:

```
ISR-PxR2#show ip ips signatures count

Cisco SDF release version S480.0
Trend SDF release version V0.0

Signature Micro-Engine: atomic-ip: Total Signatures 386
      atomic-ip enabled signatures: 95
      atomic-ip retired signatures: 183
      atomic-ip compiled signatures: 101
      atomic-ip Inactive - compile failure: 102
      atomic-ip obsoleted signatures: 3

Signature Micro-Engine: normalizer: Total Signatures 9
      normalizer enabled signatures: 8
      normalizer compiled signatures: 8
```

 © 2010 Cisco Systems, Inc.

```
Signature Micro-Engine: service-http-v2 (INACTIVE)

Signature Micro-Engine: service-http: Total Signatures 820
      service-http enabled signatures: 142
      service-http retired signatures: 657
      service-http compiled signatures: 80
      service-http inactive signatures - invalid params: 7
      service-http Inactive - compile failure: 76

Signature Micro-Engine: service-smb-advanced: Total Signatures
52
      service-smb-advanced enabled signatures: 43
      service-smb-advanced retired signatures: 8
      service-smb-advanced compiled signatures: 27
      service-smb-advanced Inactive - compile failure: 17
      service-smb-advanced disallowed signatures: 3

Signature Micro-Engine: service-msrpc: Total Signatures 35
      service-msrpc enabled signatures: 17
      service-msrpc retired signatures: 20
      service-msrpc compiled signatures: 14
      service-msrpc inactive signatures - invalid params: 1
      service-msrpc obsoleted signatures: 2

Signature Micro-Engine: service-smtp-v1 (INACTIVE)

Signature Micro-Engine: state: Total Signatures 37
      state enabled signatures: 16
      state retired signatures: 19
      state compiled signatures: 14
      state inactive signatures - invalid params: 3
      state Inactive - compile failure: 1
```

- Verify that the IPS ruleset is active on the FastEthernet0/0 interface:

```
ISR-PxR2#show ip ips interfaces
    Interface Configuration
      Interface FastEthernet0/0
        Inbound IPS rule is MY-IPS
        Outgoing IPS rule is MY-IPS
```

# Task 2: Prepare the Cisco IME and Cisco Configuration Professional Software

In this task, you will prepare the Cisco IME and Cisco Configuration Professional tools for later use. You will connect to the ISR-PxR2 router sensor using both tools. In the next tasks, you will use the Cisco IME application to monitor IPS events that are generated by the ISR-PxR2 sensor, and use the Cisco Configuration Professional application to tune IPS signatures.

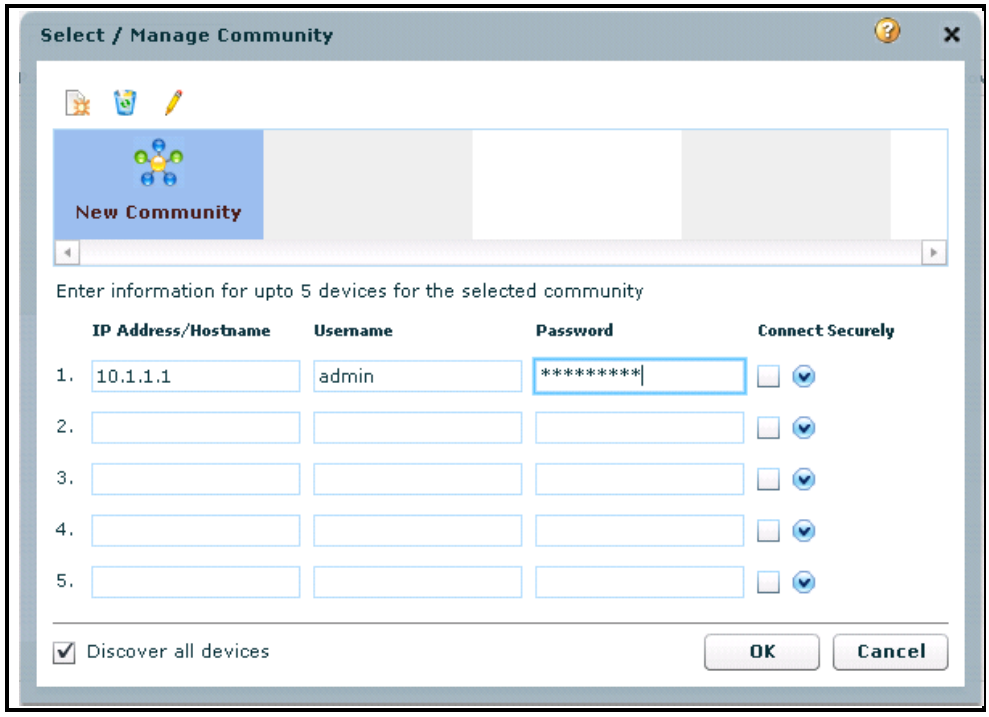
## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR2 router, enable IPS SDEE event notifications and enable the Cisco IOS HTTP server.

**Step 2** Log in to Server A, and start the Cisco IME user interface using the Cisco IME shortcut on the desktop. Add the ISR-PxR2 router as a sensor, using the username **admin** and password **adminpass** that the Cisco IME will use to log on to the router using SDEE. This username and password pair is already configured on the ISR-PxR2 router.

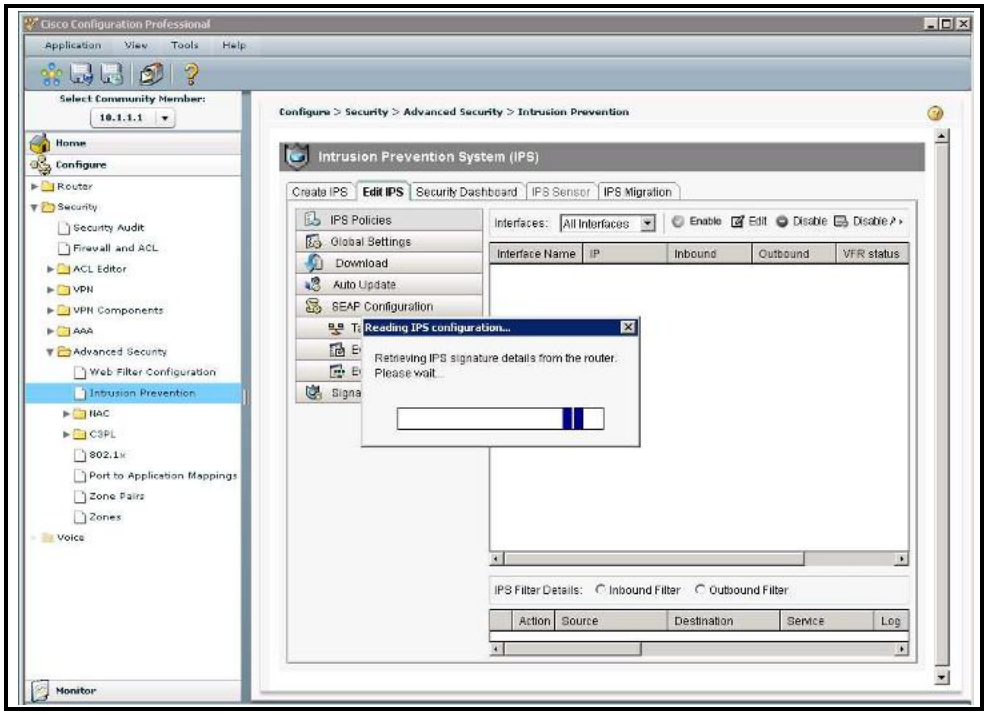
**Step 3** On Server A, start the Cisco Configuration Professional using its icon on the desktop, and add IPS to the ISR-PxR2 router using the **admin** username and **adminpass** password to the new community. Check the **Discover All Devices** check box of the Cisco Configuration Professional Select/Manage Community window.




**Step 4** On Server A, inside the Cisco Configuration Professional application, click **OK** to start discovering the router. It will take a while to discover all configuration settings.

**Step 5** On Server A, inside the Cisco Configuration Professional application, navigate to **Configure > Security > Advanced Security > Intrusion Prevention > Edit IPS** to retrieve IPS signature details from the ISR-PxR2 router.

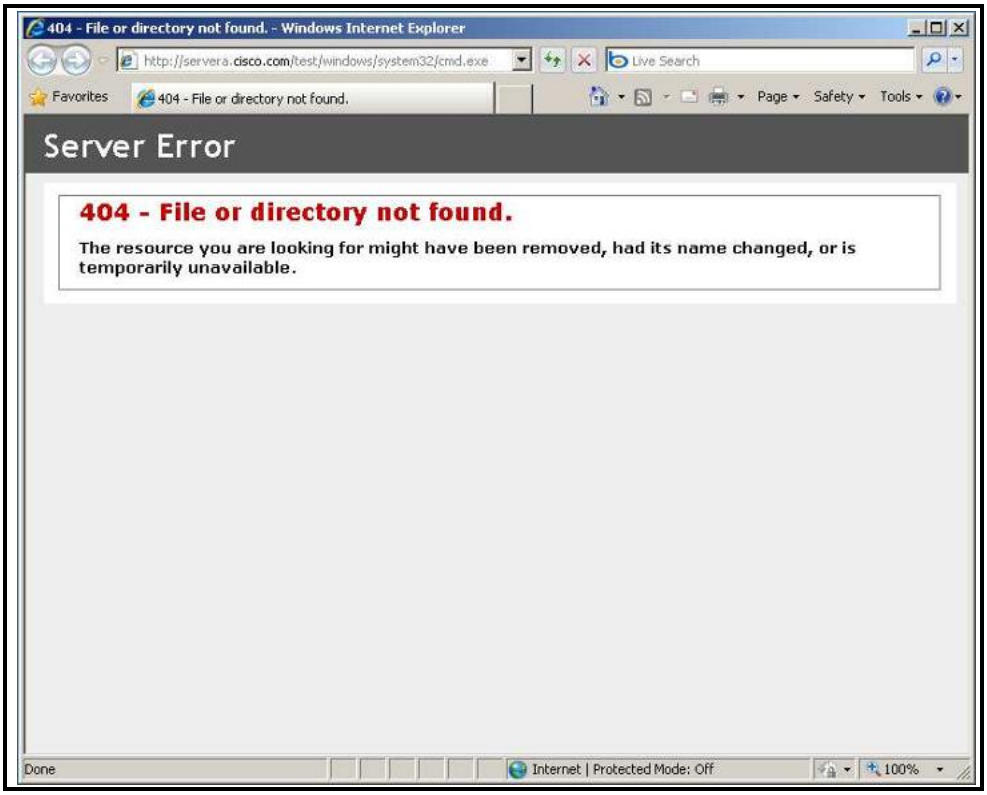
 © 2010 Cisco Systems, Inc.




## Activity Verification

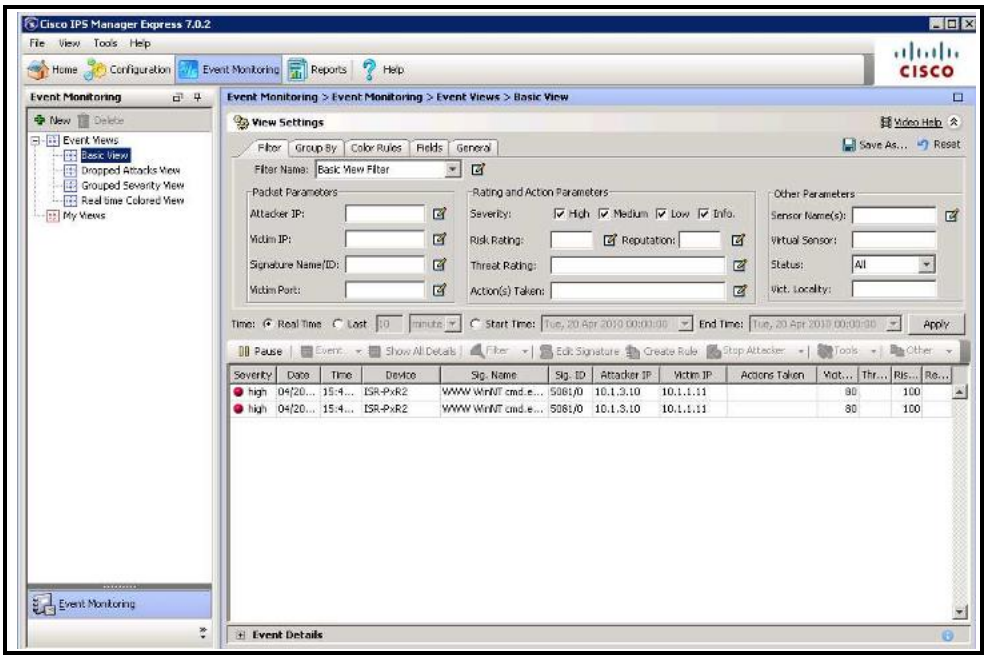
You have completed this task when you attain these results:

- On Server A, inside the Cisco IME application, inside the **Event Monitoring** window, select IPS events to be presented in real time and click **Apply**.
- Log in to the shared server, and simulate an attack against Server A by visiting the **http://servera.cisco.com/test/windows/system32/cmd.exe** URL using a web browser. You should receive a *File or directory not found* message, indicating that this traffic was not yet dropped by the ISR-PxR2 IPS feature.




- On Server A, inside the Cisco IME application, inside the Event Monitoring window, observe messages that you receive regarding current IPS events. Notice the signature ID, risk rate, and action that are taken by the signature that was triggered.

**Note** The triggered signature does not, by default, have any aggressive (IPS) action that is associated with it and only produces intrusion alerts.




 © 2010 Cisco Systems, Inc.

# Task 3: Tune the Cisco IOS Software IPS Policy Using SEAP

In this task, you will tune the router IPS policy using SEAP, which is configured using the Cisco Configuration Professional application.

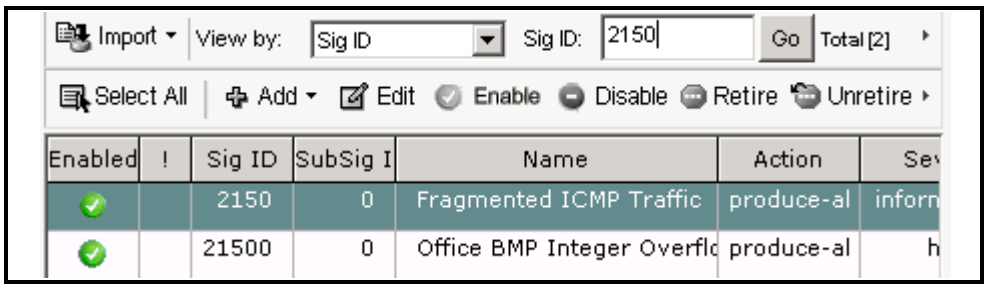
## Activity Procedure

Complete these steps:

**Step 1** On Server A, inside the Cisco Configuration Professional application, navigate to **Configure > Security > Advanced Security > Intrusion Prevention > Edit IPS > SEAP Configuration > Event Action Overrides.**

**Step 2** On Server A, inside the Cisco Configuration Professional application, add the **Deny Packet Inline** and **Reset TCP Connection** actions for events in which the event-risk rating exceeds 75. Apply your changes.

**Step 3** On Server A, inside the Cisco Configuration Professional application, enable the **Fragmented ICMP Traffic** signature.




**Step 4** On Server A, ping the shared server with 2000-byte ICMP packets using the **ping shared.cisco.com –l 3000** command. These packets will be fragmented, causing the Fragmented ICMP Traffic signature to fire.

**Step 5** On Server A, in the Cisco IME Event Monitoring window, observe the messages that you receive regarding IPS events. You should observe alerts that are caused by the Fragmented ICMP Traffic signature.

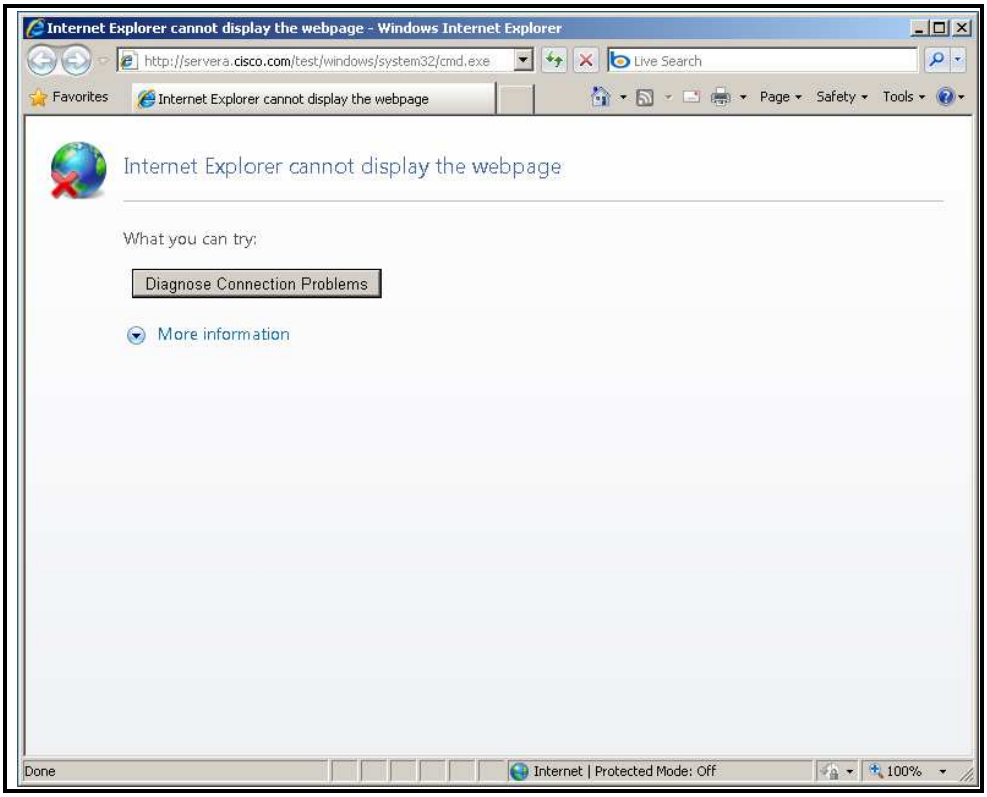
**Step 6** On Server A, clear the Event Monitor events by selecting the **Other > Clear All Events** option.

**Step 7** You have decided that such fragmented traffic from Server A to the shared server is legitimate and do not want to receive warnings for this event. Create a SEAP event action filter and filter the Fragmented ICMP Traffic signature (signature ID 2150) to not trigger (by subtracting all of its actions) if traffic is sourced from the 10.1.1.11 host or destined from the 10.1.1.11 host. (You have to create two event action filter rules).

## Activity Verification

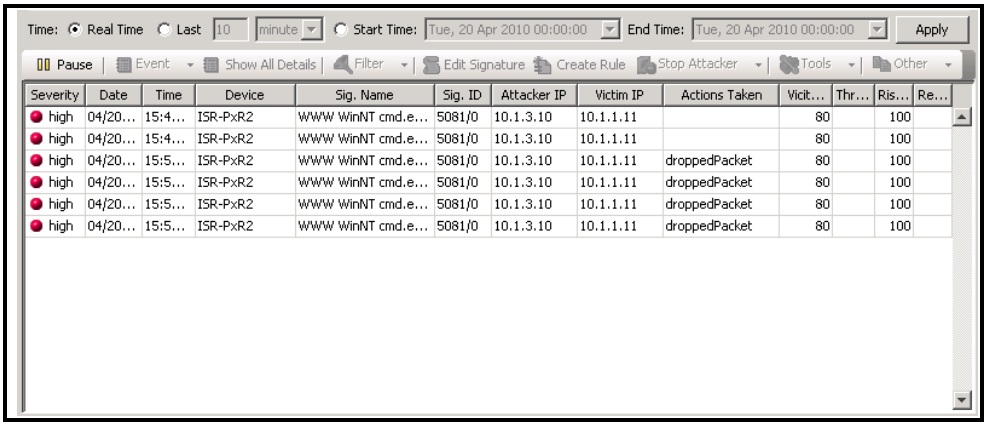
You have completed this task when you attain these results:

- Log in to the shared server, and simulate an attack against Server A by visiting the **http://servera.cisco.com/test/windows/system32/cmd.exe** URL again. You should not receive any reply from Server A (the session should time out), indicating that this traffic was dropped by the ISR-PxR2 router sensor.



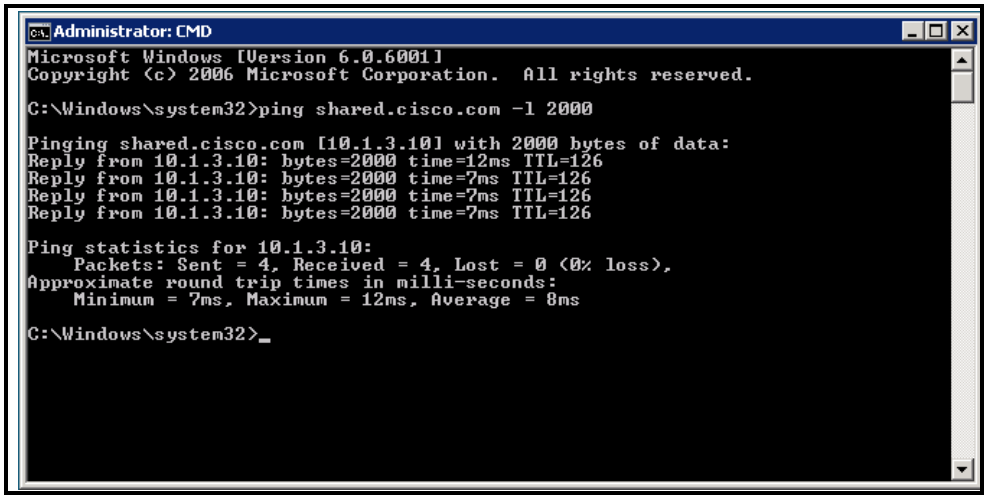

- On Server A, inside the Cisco IME Event Monitoring window, observe messages that you receive regarding IPS events. Notice the signature ID, event risk rating, and the action that is taken by the signature that was triggered.

**Note** Packets were dropped because the action taken is the droppedPacket IPS action.




- On Server A, inside the Cisco IME Event Monitoring window, clear all displayed Event Monitor events by selecting the **Other > Clear All Events** option.
- From Server A, ping the shared server with 2000 bytes using the **ping shared.cisco.com –l 3000** command.

 © 2010 Cisco Systems, Inc.




- On Server A, in the Cisco IME Event Monitoring window, you should not receive any events because the event action filters are in place for this traffic:



# Lab 3-1: Configuring a PKI-Enabled Site-to-Site IPsec VPN

Complete this lab activity to practice what you learned in the related module.

## Activity Objective

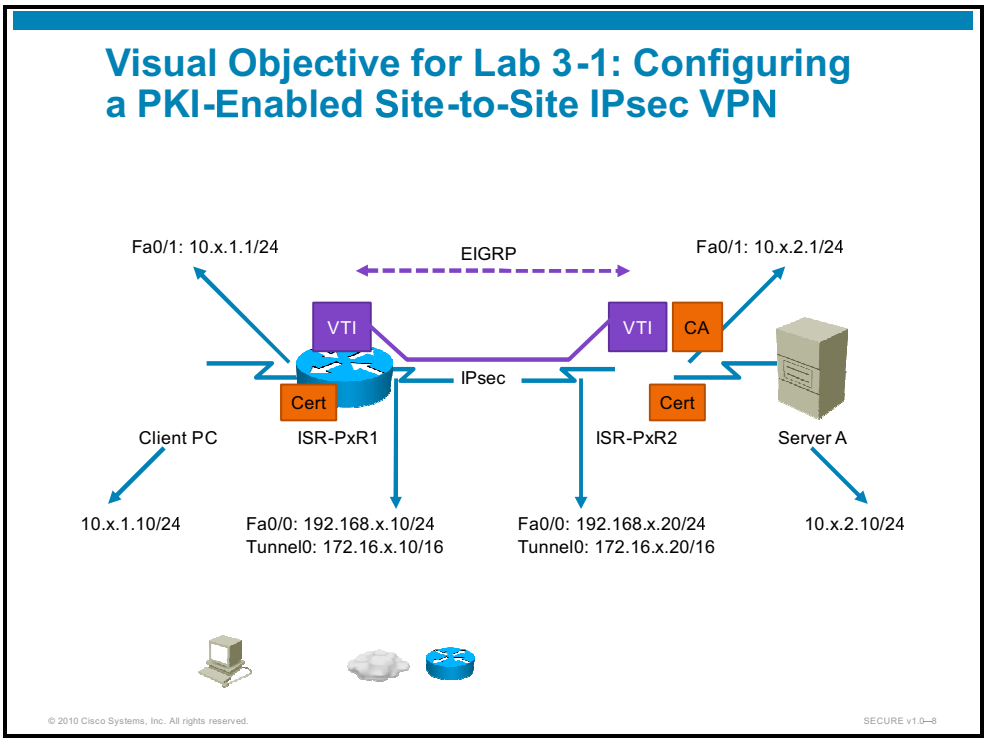
In this activity, you will configure PKI integration in site-to-site IPsec VPNs and verify its operation using the CLI. The ISR-PxR2 router will act as a CA server.

After completing this activity, you will be able to meet these objectives:

- Configure a certificate server on a router
- Enroll a router into a PKI
- Configure a VTI-based point-to-point IPsec VPN tunnel
- Configure basic EIGRP over the point-to-point IPsec VPN tunnel
- Test and verify IKE peering between the routers
- Verify routing protocol peering between the routers
- Verify connectivity between sites

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Pod ISR routers (ISR-PxR1 and ISR-PxR2)

 © 2010 Cisco Systems, Inc.

- Pod client PC and Server A systems

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **auto-summary** | Allows automatic summarization of subnet routes into network-level routes. To disable this function and send subprefix routing information across classful network boundaries, use the no form of this command. |
| **crypto ca authenticate** | Authenticates the certification authority (by getting the certificate of the CA). |
| **crypto ca enroll** | Obtains the certificates for your router from the CA. |
| **crypto ipsec profile** *name* | Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers. |
| **crypto key generate rsa label** *key-label* **modulus** *modulus-size* **exportable** | Generates RSA key pairs with specified label and modulus size. |
| **crypto pki authenticate** | Authenticates the certification authority (by getting the certificate of the CA). |
| **crypto pki certificate map** *label sequence-number* | Defines certificate-based access control lists in ca-certificate-map configuration mode. |
| **crypto pki enroll** | Obtains the certificates for your router from the CA. |
| **crypto pki server** *cs-label* | Enables a Cisco IOS certificate server and enters certificate server configuration mode. |
| **crypto pki server** *cs-label* **grant** *{all \| req-id}* | Grants all or certain SCEP requests. |
| **crypto pki trustpoint** *name* | Declares the trustpoint that your router should use. |
| **database url** *root-url* | Specifies in certificate server configuration mode the location where database entries for the CS will be stored. |
| **enrollment url** *url* | Specifies the enrollment parameters of a CA. |
| **hash** *{md5 \| sha1 \| sha256 \| sha384 \| sha512}* | Specifies the cryptographic hash function the Cisco IOS client will use for self-signed certificates. |
| **interface** *interface* | Enters the interface configuration mode. |
| **ip http server** | Enables the HTTP server on the router. |
| **issuer-name** *DN-string* | Specifies the DN as the CA issuer name for the certificate server. |
| **lifetime ca-certificate** *days* | Specifies that the lifetime applies to the CA certificate of the certificate server. |
| **lifetime certificate** *days* | Specifies that the lifetime applies to the certificate of the certificate server. The maximum certificate lifetime is 1 month less than the expiration date of the lifetime of the CA certificate. |
| **match certificate** *certificate-map* | Assigns an ISAKMP profile to a peer based on the contents of arbitrary fields in the certificate. |

| Command | Description |
| --- | --- |
| **network** *ip-address* **[***wildcard-mask***]** | Specifies the network for an EIGRP routing process. |
| **no shutdown** | Allows a certificate server to be disabled in certificate server configuration mode. |
| **ping** | Determines if other IP addresses are accessible. |
| **router eigrp** *autonomous-system-number* | Configures the EIGRP routing process. |
| **rsakeypair** *key-label* | Specifies which RSA key pair to associate with the certificate in ca-trustpoint configuration mode. |
| **set isakmp-profile** *profile-name* | Sets the ISAKMP profile name in IPsec profile configuration mode. |
| **show crypto ipsec sa** | Displays the settings that are used by current SAs. |
| **show crypto isakmp policy** | Displays the parameters for each IKE policy. |
| **show crypto isakmp sa** | Displays current IKE SAs. |
| **show crypto pki server** | Displays the current state and configuration of the certificate server. |
| **show ip eigrp neighbors** | Displays neighbors that are discovered by EIGRP. |
| **show ip route** | Displays the routing table. |
| **show running-config** | Displays the configuration that is currently running on the adaptive security appliance. |
| **subject-name** *x.500-name* | Specifies the subject name in the certificate request. |
| **tunnel destination {***ip-address* \| *interface-type interface-number***}** | Sets the destination address for a tunnel interface. |
| **tunnel protection ipsec profile** *name* | Associates a tunnel interface with an IPsec profile. |
| **tunnel source {***ip-address* \| *interface-type interface-number***}** | Sets the source address for a tunnel interface. |

 © 2010 Cisco Systems, Inc.

# Job Aids

These job aids are available to help you complete the lab activity.

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username | |
| Password | |

# Task 1: Configure a Certificate Server on a Router

The Cisco IOS Software Certificate Server is a powerful and capable certification authority for dedicated VPN applications, and it contains several features that can significantly improve network manageability. In this task, you will configure the ISR-PxR2 router as a certificate server.

## Activity Procedure

Complete these steps:

**Step 1** On the ISR-PxR2 router, create a 2048-bit RSA key pair, assign a label to it, and mark it as exportable.

**Step 2** On the ISR-PxR2 router, create a named PKI trustpoint, and inside it, reference the label of the newly created, dedicated Certificate Server key pair.

**Step 3** On the ISR-PxR2 router, create a directory in the local flash file system. You will store all certificate server-related files in this folder.

**Step 4** On the ISR-PxR2 router, create a certificate server and assign it the same name that you used for the named PKI trustpoint in the previous step.

**Step 5** On the ISR-PxR2 router, inside the certificate server, specify an X.500 name for the certificate server:

- Set its canonical name (CN) to CA
- Set organization unit (OU) to VPN
- Set organization (O) to Cisco
- Set country (C) to US

**Step 6** On the ISR-PxR2 router, configure the location for Certificate Server files to be stored in its flash memory, in the folder that is configured in Step 3.

**Step 7** On the ISR-PxR2 router, specify SHA-1 as the hash algorithm used in the certificate signing process.

**Step 8** On the ISR-PxR2 router, set the lifetime of issued identity certificates to two years.

**Step 9** On the ISR-PxR2 router, set the lifetime of the Certificate Server signing (CA) certificate to 10 years. After this lifetime expires, the Certificate Server will need to re-regenerate its self-signed certificate.

**Step 10** On the ISR-PxR2 router, enable the SCEP interface on the certificate server by enabling the Cisco IOS Software HTTP server to provide a SCEP server to PKI clients.

**Step 11** Enable the certificate server on the ISR-PxR2 router. When asked, enter a long and random password to protect the Certificate Server RSA private key.

## Activity Verification

You have completed this task when you have completed all the steps listed in the Activity Procedure section.

- On the ISR-PxR2 router, verify the status of the certificate server and check the CA certificate fingerprint:

```
ISR-PxR2#show crypto pki server MY-CS
Certificate Server MY-CS:
```

 © 2010 Cisco Systems, Inc.

```
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock
it)
    Issuer name: CN=CA, OU=VPN, O=Cisco, C=US
    CA cert fingerprint: 0E53DE23 7AC1AEFB E8CF46D0 FE87DBC2
    Granting mode is: manual
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 08:52:35 UTC Jan 24 2020
    CRL NextUpdate timer: 14:52:35 UTC Jan 26 2010
    Current primary storage dir: flash://my-cs
    Database Level: Minimum - no cert data written to storage
```

# Task 2: Enroll Two VPN Peers into a PKI

In this task, you will enroll both the ISR-PxR2 and the ISR-PxR1 routers into a PKI. PKI enrollment is the procedure of adding a PKI user (router in this case) to the PKI by providing it with an identity certificate. Despite the fact that ISR-PxR2 also acts as a certificate server, you have to enroll both ISR-PxR1 and ISR-PxR2 to a PKI for them to obtain their respective identity certificates.

## Activity Procedure

Complete these steps:

**Step 1** On both the ISR-PxR2 and the ISR-PxR1 routers, verify the system clock and synchronize it to the time of ISR-PxR2, if required.

**Step 2** On both the ISR-PxR2 and the ISR-PxR1 routers, create a 2048-bit RSA key pair, and assign it a label.

**Step 3** On both the ISR-PxR2 and the ISR-PxR1 routers, create a named PKI trustpoint (on ISR-PxR2, use a name that is different from the name used for the certificate server trustpoint). In trustpoint configuration, configure the following:

- Specify the location of the CA (enrollment URL), which is **http://192.168.1.20** (the web server is ISR-PxR2).
- Specify the FQDN of the peer to be **R1.vpn.cisco.com** for the ISR-PxR1 router and **R2.vpn.cisco.com** for the ISR-PxR2 router.
- Specify the X.500 subject name of the peer to be **CN=R1, OU=VPN, O=Cisco, C=US** for the ISR-PxR1 router, and **CN=R2, OU=VPN, O=Cisco, C=US** for the ISR-PxR2 router.
- Reference the named RSA key pair configured in Step 1 of this task.

**Step 4** On both the ISR-PxR2 and the ISR-PxR1 routers, authenticate the PKI CA by obtaining its self-signed certificate. To verify that the correct CA certificate has been received, the local PKI client calculates a local hash (fingerprint) of received information. You must compare this fingerprint to the true CA certificate fingerprint observed in the verification section of the previous task.

**Step 5** On both the ISR-PxR2 and the ISR-PxR1 routers, create an enrollment request by submitting your name and public key to the CA and obtaining the identity certificate of the router from the CA. Enter a revocation password of your choice that the CA administrator may require in the future, if you attempt to revoke this certificate. Choose not to include one of the IP addresses of the device as the identifier and not to include the serial number of the device.

**Step 6** On the ISR-PxR2 certificate server, verify all currently pending enrollment requests. Validate the fingerprint of pending requests against the fingerprints of the client.

**Step 7** On the ISR-PxR2 certificate server, grant both requests from ISR-PxR1 and ISR-PxR2 routers. After you have granted the identity certificates, the certificates will be automatically downloaded by a SCEP-enabled PKI client and installed (saved) on the requesting devices (ISR-PxR1 and ISR-PxR2).

## Activity Verification

You have completed this task when you attain these results:

- On the ISR-PxR1 router, verify that the CA certificate and an identity certificate have been successfully installed (using the name of your trustpoint as the argument):

```
ISR-PxR1#show crypto pki certificates VPN-PKI
Certificate
  Status: Available
  Certificate Serial Number (hex): 03
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
    ou=VPN
    o=Cisco
    c=US
  Subject:
    Name: R1.vpn.cisco.com
    hostname=R1.vpn.cisco.com
    cn=R2
    ou=VPN
    o=Cisco
    c=US
  Validity Date:
    start date: 10:21:12 UTC Jan 26 2010
    end   date: 10:21:12 UTC Jan 26 2012
  Associated Trustpoints: VPN-PKI

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA
    ou=VPN
    o=Cisco
    c=US
  Subject:
    cn=CA
    ou=VPN
    o=Cisco
    c=US
  Validity Date:
```

 © 2010 Cisco Systems, Inc.

```
    start date: 08:52:35 UTC Jan 26 2010
    end   date: 08:52:35 UTC Jan 24 2020
  Associated Trustpoints: VPN-PKI
```

- On the ISR-PxR2 router, verify that the CA certificate and an identity certificate have been successfully installed (using the name of your trustpoint as the argument):

```
ISR-PxR2#show crypto pki certificates VPN-PKI
Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
    ou=VPN
    o=Cisco
    c=US
  Subject:
    Name: R2.vpn.cisco.com
    hostname=R2.vpn.cisco.com
    cn=R2
    ou=VPN
    o=Cisco
    c=US
  Validity Date:
    start date: 10:21:04 UTC Jan 26 2010
    end   date: 10:21:04 UTC Jan 26 2012
  Associated Trustpoints: VPN-PKI

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA
    ou=VPN
    o=Cisco
    c=US
  Subject:
    cn=CA
    ou=VPN
    o=Cisco
    c=US
  Validity Date:
    start date: 08:52:35 UTC Jan 26 2010
    end   date: 08:52:35 UTC Jan 24 2020
  Associated Trustpoints: VPN-PKI MY-CS
```

# Task 3: Configure VTI-Based Point-to-Point IPsec VPN Peering

In this task, you will configure a VTI-based point-to-point IPsec VPN tunnel, using default policies for IKE and default IPsec transform sets.

## Activity Procedure

Complete these steps:

**Step 1** On both the ISR-PxR2 and the ISR-PxR1 routers, verify that some ISAKMP policies are preconfigured by default in Cisco IOS Software.

**Step 2** On both the ISR-PxR2 and the ISR-PxR1 routers, configure an IPsec protection profile name and leave it blank (that is, the default IPsec transform sets will be used).

**Step 3** On both the ISR-PxR2 and the ISR-PxR1 routers, configure a VTI tunnel interface and use the interface parameters that are listed here:

- Assign an appropriate IP address to the tunnel interface, based on the lab addressing data.
- Specify the tunnel source interface as the physical interface to the untrusted network (that is, the interface pointing to the other VPN peer).
- Specify the tunnel destination IP address (that is, the tunnel source interface IP address of the other peer).
- Enable IPsec encapsulation.
- Specify an IPsec traffic protection policy by referencing the configured IPsec profile.

## Activity Verification

You have completed this task when you attain these results:

- On the ISR-PxR1 router, verify that some ISAKMP policies are preconfigured by default in Cisco IOS Software:

```
ISR-PxR1#show crypto isakmp policy

Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit
keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit
keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit
keys
).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
```

 © 2010 Cisco Systems, Inc.

```
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit
keys
).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

- On the ISR-PxR2 router, verify that some ISAKMP policies are preconfigured by default in Cisco IOS Software:

```
ISR-PxR1#show crypto isakmp policy

Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit
keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit
keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit
keys
).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit
keys
).
        hash algorithm:         Message Digest 5
```

```
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

- On the ISR-PxR1 router, verify that ISAKMP security association is established with the ISR-PxR2 router:

```
ISR-PxR1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.20    192.168.1.10    QM_IDLE           1001 ACTIVE
```

- On the ISR-PxR2 router, verify that ISAKMP security association is established with the ISR-PxR1 router:

```
ISR-PxR2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.20    192.168.1.10    QM_IDLE           1001 ACTIVE
```

- On the ISR-PxR1 router, ping the inner tunnel IP address of the remote ISR-PxR2 router:

```
ISR-PxR1#ping 172.16.1.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.20, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/4 ms
```

 © 2010 Cisco Systems, Inc.

# Task 4: Configure IKE on Both Peers Using Peer Canonical Name Verification

In this task, you will configure certificate-based authorization of remote peers to limit the authenticated identities of remote peers that can use a particular VPN association.

## Activity Procedure

Complete these steps:

**Step 1** On both the ISR-PxR1 and the ISR-PxR2 routers, limit the peers with which the local peer is willing to establish a VPN session by creating an appropriate certificate map:

- On ISR-PxR1 ensure that you are always establishing the IKE session with the ISR-PxR2 peer, which has its CN set to R2.
- On ISR-PxR2 ensure that you are always establishing the IKE session with the ISR-PxR1 peer, which has its CN set to R1.

## Activity Verification

You have completed this task when you attain these results:

- On the ISR-PxR1 router, shut down the VTI tunnel interface. Bring it back up again to reinitialize the IKE and IPsec associations of the VTI tunnel.
- On the ISR-PxR1 router, ensure that the tunnel reinitialized with CN verification by pinging the inner tunnel IP address of the remote ISR-PxR2 router:

```
ISR-PxR1#ping 172.16.1.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.20, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/4 ms
```

# Task 5: Configure EIGRP Over the Point-to-Point IPsec VPN Peering

In this task, you will configure the EIGRP routing protocol over the point-to-point IPsec VPN peering. You will verify that traffic from the client PC to the Server A host flows through the configured VTI tunnel.

## Activity Procedure

Complete these steps:

**Step 1** On both the ISR-PxR1 and the ISR-PxR2 routers, enable an EIGRP routing process with an autonomous system number of 200.

**Step 2** On the ISP-PxR1 router, specify the networks for EIGRP as those belonging to the tunnel subnet and the subnet of the client PC.

**Step 3** On the ISP-PxR2 router, specify the networks for EIGRP as those belonging to the tunnel subnet and the subnet of the Server A host.

**Step 4** On both the ISR-PxR1 and the ISR-PxR2 routers, disable EIGRP autosummarization.

**Step 5** On router ISR-PxR1, check the current number of encrypted and decrypted IPsec packets so far.

## Activity Verification

You have completed this task when you attain these results:

- On both the ISR-PxR1 and the ISR-PxR2 routers, verify that an EIGRP adjacency across the VTI tunnel is successfully established:

```
ISR-PxR1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(200)
H   Address                 Interface       Hold Uptime   SRTT
RTO  Q  Seq
                                            (sec)         (ms)
Cnt Num
0   172.16.1.20             Tu0               13 00:00:10   11
1398  0  3

ISR-PxR2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(200)
H   Address                 Interface       Hold Uptime   SRTT
RTO  Q  Seq
                                            (sec)         (ms)
Cnt Num
0   172.16.1.10             Tu0               11 00:01:21   10
1398  0  3
```

- On the ISR-PxR1 router, verify that an EIGRP-learned route exists to the subnet hosting the server system:

```
ISR-PxR1#show ip route eigrp
Codes: L - local, 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, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

      10.0.0.0 255.0.0.0 is variably subnetted, 3 subnets, 2 masks
D        10.1.2.0 255.255.255.0
           [90/26882560] via 172.16.1.20, 00:00:12, Tunnel0
```

- On the ISR-PxR2 router, verify that an EIGRP-learned route exists to subnet hosting the client PC:

```
ISR-PxR2#show ip route eigrp
Codes: L - local, 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, su - IS-IS summary, 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, + - replicated route

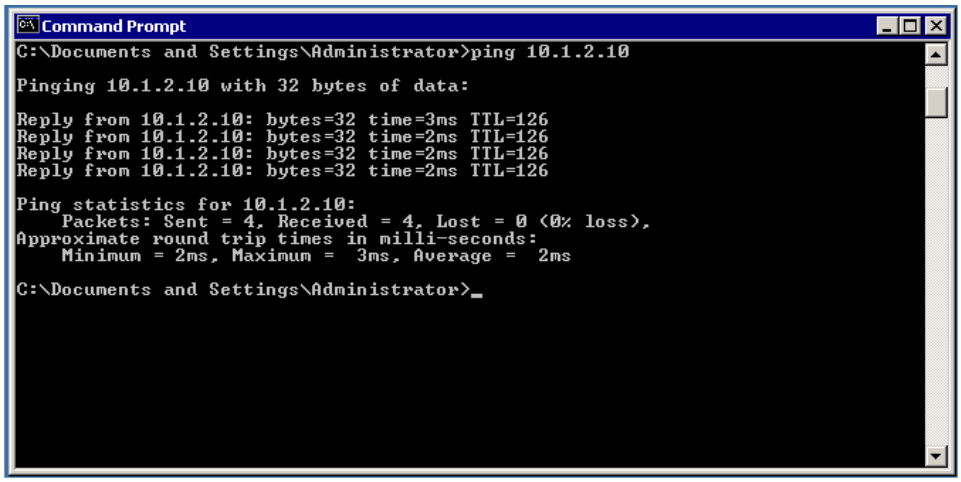
Gateway of last resort is not set

      10.0.0.0 255.0.0.0 is variably subnetted, 3 subnets, 2 masks
```

 © 2010 Cisco Systems, Inc.

```
D        10.1.1.0 255.255.255.0
           [90/26882560] via 172.16.1.10, 00:00:13, Tunnel0
```

- Log in to the client PC, and ping the Server A host (over the VPN tunnel):




- On the ISR-PxR1 router, check the current number of encrypted and decrypted IPsec packets:

```
ISR-PxR1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.1.10

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.168.1.20 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 240, #pkts encrypt: 240, #pkts digest: 240
    #pkts decaps: 234, #pkts decrypt: 234, #pkts verify: 234
    #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.: 192.168.1.10, remote crypto endpt.: 192.168.1.20
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xAD27B086(2905059462)
     PFS (Y/N): N, DH group: none

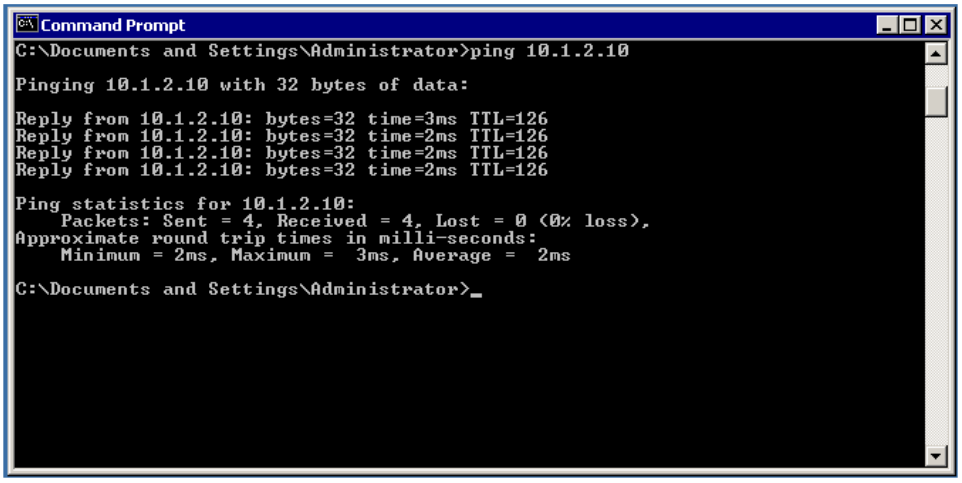
     inbound esp sas:
      spi: 0xA7B82DB1(2813865393)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4390183/348)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xAD27B086(2905059462)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map:
Tunnel0-head-0
```

```
        sa timing: remaining key lifetime (k/sec): (4390183/348)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

      outbound ah sas:
      outbound pcp sas:
```

- From the client PC, ping the Server A host again:




- On the ISR-PxR1 router, verify that the number of encrypted and decrypted packets is increasing with traffic:

```
ISR-PxR1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.1.10

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.168.1.20 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 247, #pkts encrypt: 247, #pkts digest: 247
    #pkts decaps: 241, #pkts decrypt: 241, #pkts verify: 241
    #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.: 192.168.1.10, remote crypto endpt.: 192.168.1.20
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xAD27B086(2905059462)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xA7B82DB1(2813865393)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4390182/339)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
```

 © 2010 Cisco Systems, Inc.

```
     outbound esp sas:
      spi: 0xAD27B086(2905059462)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4390182/339)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

# Lab 3-2: Configuring Cisco IOS Software DMVPN Spokes

Complete this lab activity to practice what you learned in the related module.

## Activity Objective

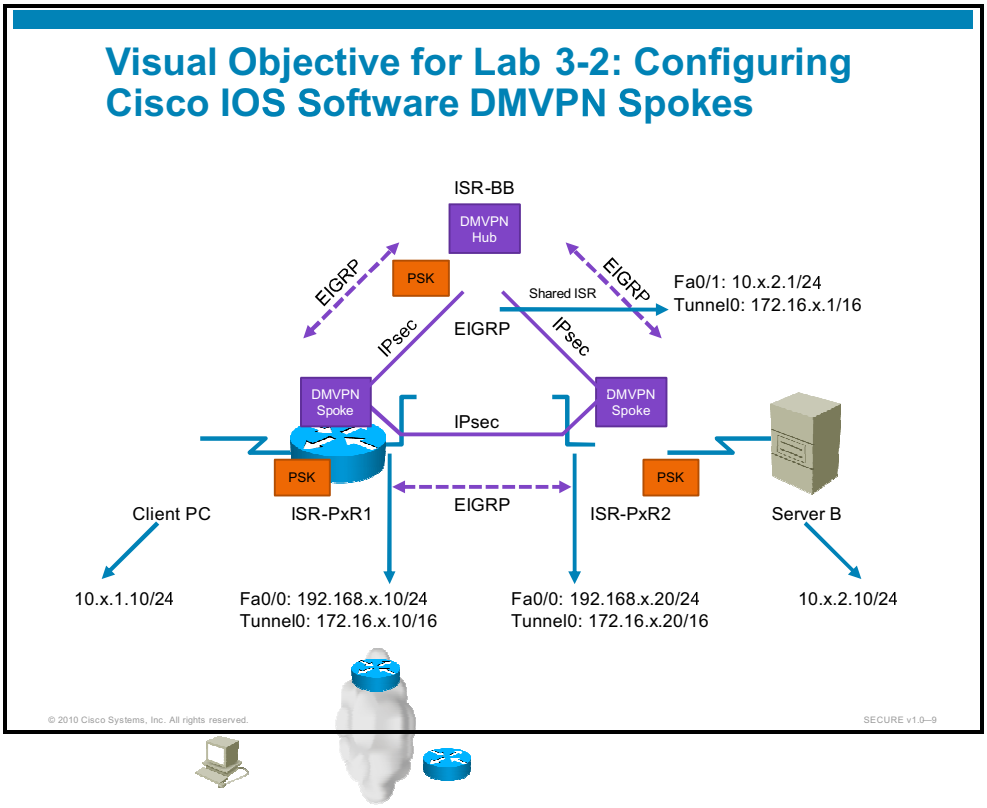
In this activity, you will configure and verify two DMVPN spokes using the CLI. You will use the spoke-to-spoke (full mesh) deployment model, which requires each spoke to be configured with an mGRE interface, in which dynamic spoke-to-spoke tunnels are used for spoke-to-spoke traffic. The ISR-BB router, which is the DMVPN hub, has been preconfigured by the instructor.

After completing this activity, you will be able to meet these objectives:

- Verify and evaluate the preconfigured DMVPN hub configuration
- Configure two DMVPN spokes
- Configure EIGRP routing protocol support on DMVPN spokes
- Verify spoke-to-hub tunnel establishment
- Verify spoke-to-spoke tunnel establishment
- Verify EIGRP adjacencies
- Verify spoke-to-spoke connectivity

## Visual Objective

The figure illustrates what you will accomplish in this activity.



# Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Pod ISR routers
- Pod client PC and Server B systems
- Shared backbone ISR router

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **authentication** *method* | Specifies the authentication method within an IKE policy. |
| **auto-summary** | Allows automatic summarization of subnet routes into network-level routes. To disable this function and send subprefix routing information across classful network boundaries, use the no form of this command. |
| **crypto ca authenticate** | Authenticates the CA (by getting the certificate of the CA). |
| **crypto ca enroll** | Obtains the certificates for your router from the CA. |
| **crypto ipsec profile** *name* | Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers. |
| **crypto ipsec transform-set** *name transform1 [transform2] …* | Defines a transform set—an acceptable combination of security protocols and algorithm. |
| **crypto isakmp policy** *priority* | Defines an IKE policy in global configuration mode. |
| **crypto pki authenticate** | Authenticates the certification authority (by getting the certificate of the CA). |
| **crypto pki enroll** | Obtains the certificates for your router from the CA. |
| **crypto pki trustpoint** *name* | Declares the trustpoint that your router should use. |
| **encryption** *algorithm* | Specifies the encryption algorithm within an IKE policy. |
| **enrollment url** *url* | Specifies the enrollment parameters of a CA. |
| **group** *identifier* | Specifies the Diffie-Hellman group identifier within an IKE policy. |
| **interface** *interface* | Enters the interface configuration mode. |
| **ip mtu** *bytes* | Sets the MTU size of IP packets that are sent on an interface. |
| **ip nhrp authentication** *string* | Configures the authentication string for an interface using the NHRP. |
| **ip nhrp map** *ip-address nbma-address* | Statically configure the IP-to- NBMA address mapping of IP destinations that are connected to an NBMA network. |
| **ip nhrp map multicast** *nbma-address* | Configures NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network |

| Command | Description |
|---|---|
| **ip nhrp network-id** *number* | Enables the NHRP on an interface. |
| **ip nhrp nhs** *nhs-address* | Specifies the address of one or more NHRP servers. |
| **Ip tcp adjust-mss** *max-segment-size* | Adjusts the MSS value of TCP synchronize/start (SYN) packets going through a router. |
| **network** *ip-address* **[***wildcard-mask***]** | Specifies the network for an EIGRP routing process. |
| **ping** | Determines if other IP addresses are accessible. |
| **revocation-check crl** | CRL checks the revocation status of a certificate. |
| **router eigrp** *autonomous-system-number* | Configures the EIGRP routing process. |
| **set transform-set** *name* | Specifies which transform sets can be used with the cryptography IPsec profile. |
| **show crypto ipsec sa** | Displays the settings that are used by current SAs. |
| **show crypto isakmp policy** | Displays the parameters for each IKE policy. |
| **show crypto isakmp sa** | Displays current IKE SAs. |
| **show crypto pki server** | Displays the current state and configuration of the certificate server. |
| **show ip eigrp neighbors** | Displays neighbors that are discovered by EIGRP. |
| **show ip nhrp** | Displays NHRP mapping information. |
| **show ip route** | Displays the routing table. |
| **show running-config** | Displays the configuration that is currently running on the adaptive security appliance. |
| **subject-name** *x.500-name* | Specifies the subject name in the certificate request. |
| **tunnel key** *key-number* | Enables an ID key for a tunnel interface. |
| **tunnel mode gre multipoint** | Sets the global encapsulation mode on the interface to multipoint GRE. |
| **tunnel protection ipsec profile** *name* | Associates a tunnel interface with an IPsec profile. |
| **tunnel source {***ip-address* \| *interface-type interface-number***}** | Sets the source address for a tunnel interface. |

 © 2010 Cisco Systems, Inc.

# Job Aids

These job aids are available to help you complete the lab activity.

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username | |
| Password | |

# Task 1: Verify Preconfigured DMVPN Hub Configuration

In this task, you will verify and evaluate the existing DMVPN hub configuration on ISR-BB. The ISR-BB router has been preconfigured with basic IKE parameters and as the DMVPN hub by your instructor.

## Activity Procedure

Complete these steps:

**Step 1** Log into the console of your ISR-PxR1 router, and from this router, use Telnet to connect to the loopback address (172.31.1.1) of the ISR-BB router. Log in to ISR-BB as user **admin** with the password of **admin**.

**Step 2** Verify the IKE (ISAKMP) policies that are configured on the ISR-BB router.

**Note** Note the settings of the highest priority IKE (ISAKMP) policy. You will have to configure a matching policy on the two-spoke DMVPN group members.

**Step 3** ISR-BB is preconfigured as a certificate server. Verify the status of the certificate server.

**Step 4** ISR-BB is preconfigured as a DMVPN hub. Verify the configuration of its DMVPN tunnel (mGRE) interface.

## Activity Verification

You have completed this task when you attain these results:

- Display ISAKMP policy on the ISR-BB router:

```
ISR-BB#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman
Signature
        Diffie-Hellman group:   #14 (1536 bit)
        lifetime:               86400 seconds, no volume limit
```

- Verify the status of the certificate server:

```
ISR-BB#sh crypto pki server
Certificate Server MY-CS:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock
it)
    Issuer name: CN=Hub, OU=VPN, O=Cisco, C=US
    CA cert fingerprint: 5DAEBFEC 775780AD 1C77F3CD 5F03961E
    Granting mode is: auto
    Last certificate issued serial number (hex): 2
    CA certificate expiration timer: 08:06:17 UTC Jan 27 2020
```

 © 2010 Cisco Systems, Inc.

```
    CRL NextUpdate timer: 14:06:19 UTC Jan 29 2010
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
```

- Verify the configuration of the hub mGRE interface:

```
Hub#show running-config interface tunnel 0
Building configuration...

Current configuration : 444 bytes
!
interface Tunnel0
 bandwidth 1000
 ip address 172.16.1.1 255.255.0.0
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 200
 ip nhrp authentication DMVPN_NW
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 200
 delay 1000
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile MY-IPSEC-PROFILE
end
```

# Task 2: Configure Two DMVPN Spokes

In this task, you will create a PKI trustpoint, authenticate the PKI CA, and create an enrollment request for the identity certificate of the spoke on the ISR-PxR1 and ISR-PxR2 routers. You will also configure and verify two DMVPN spokes (the ISR-PxR1 and ISR-PxR2 routers).

## Activity Procedure

Complete these steps:

**Step 1** Log in to the ISR-BB router and examine its system clock.

**Step 2** Log in to the ISR-PxR1 router. Manually sync its system clock to the ISR-BB router if required.

**Step 3** On the ISR-PxR1 router, create a PKI trustpoint with an enrollment URL of the DMVPN hub HTTP server. Configure CRL revocation checking for this trustpoint.

**Step 4** On the ISR-PxR1 router, return to the global configuration mode and authenticate the CA.

**Step 5** On the ISR-PxR1 router, create an enrollment request using the configured trustpoint parameters. Obtain an identity certificate.

**Step 6** On the ISR-PxR1 router, configure an ISAKMP policy that will match the highest-priority ISAKMP (IKE) policy of the DMVPN hub.

| Note | By default, RSA signatures are set as the authentication method. |
|---|---|

**Step 7** On the ISR-PxR1 router, create an IPsec profile that matches the IPsec profile that is used by the DMVPN hub.

**Step 8** On the ISR-PxR1 router, create a multipoint GRE tunnel interface. Set the source interface of the tunnel to the physical interface pointing towards the DMVPN hub, and specify a tunnel key, which should match the tunnel key that is configured on the DMVPN hub.

**Step 9** On the ISR-PxR1 router, configure an NHRP client:

- Match the NHRP network ID and authentication string of the DMVPN hub.
- Configure the DMVPN hub router ISR-BB as the NHRP next-hop server.
- Enable the use of dynamic multicast between the spoke and the hub. Enable the sending of multicast packets to the hub router.
- Configure a static NHRP mapping of the hub tunnel interface IP address to the hub physical interface IP address.

**Step 10** On the ISR-PxR1 router, assign an IP address on the tunnel interface according to the lab addressing scheme, and lower the MTU and TCP MSS of the tunnel interface to avoid fragmentation of GRE and IPsec packets.

**Step 11** On the ISR-PxR1 router, apply the IPsec profile to the tunnel interface.

**Step 12** Repeat all steps in Task 2 for the second spoke router ISR-PxR2.

## Activity Verification

You have completed this task when you attain these results:

- Verify spoke-to-hub IKE security associations on both spoke routers:

```
ISR-PxR1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
status
192.168.1.1     192.168.1.10    QM_IDLE           1010    0
ACTIVE


ISR-PxR2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
status
192.168.1.1     192.168.1.20    QM_IDLE           1001    0
ACTIVE
```

- Verify IPsec spoke-to-hub tunnel establishment. You should be able to ping the tunnel interface of the hub router from the spoke routers. Verify that the number of packets being encrypted and decrypted is increasing.

```
ISR-PxR1#show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.1.10

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)
   current_peer 192.168.1.1 port 500
     PERMIT, flags={origin_is_acl,}
```

 © 2010 Cisco Systems, Inc.

```
     #pkts encaps: 125, #pkts encrypt: 125, #pkts digest: 125
     #pkts decaps: 127, #pkts decrypt: 127, #pkts verify: 127
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 2526, #recv errors 0

      local crypto endpt.: 192.168.1.10, remote crypto endpt.: 192.168.1.1
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
      current outbound spi: 0x11435859(289626201)

      inbound esp sas:
       spi: 0x682F0BBA(1747913658)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4407356/3070)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0x11435859(289626201)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4407357/3063)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE


ISR-PxR2#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.1.20

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)
   current_peer 192.168.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
    #pkts decaps: 232, #pkts decrypt: 232, #pkts verify: 232
    #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.: 192.168.1.20, remote crypto endpt.: 192.168.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x341D93A2(874353570)

     inbound esp sas:
      spi: 0x6527821B(1697088027)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: NETGX:1, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4486629/2629)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
```

```
inbound pcp sas:

outbound esp sas:
 spi: 0x341D93A2(874353570)
   transform: esp-3des esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 2002, flow_id: NETGX:2, crypto map: Tunnel0-head-0
   sa timing: remaining key lifetime (k/sec): (4486654/2622)
   IV size: 8 bytes
   replay detection support: Y
   Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

**Step 13** On both spokes, verify the static NHRP mapping for the hub router:

```
ISR-PxR1#show ip nhrp
172.16.1.1 255.255.255.255 via 172.16.1.1, Tunnel0 created
03:23:24, never expire
  Type: static, Flags: used
  NBMA address: 192.168.1.1


ISR-PxR2#show ip nhrp
172.16.1.1 255.255.255.255 via 172.16.1.1, Tunnel0 created
00:28:15, never expire
  Type: static, Flags: used
  NBMA address: 192.168.1.1
```

# Task 3: Configure EIGRP Support on DMVPN Spokes

In this task, you will configure the EIGRP routing protocol across the DMVPN to enable a fully meshed DMVPN.

## Activity Procedure

Complete these steps:

**Step 1** On spoke router ISR-PxR1, configure the EIGRP routing protocol on the DMVPN mGRE tunnel interface and on the FastEthernet0/1 interface connecting to the client PC. Disable EIGRP autosummarization.

**Step 2** On spoke router ISR-PxR2, configure the EIGRP routing protocol on the DMVPN mGRE tunnel interface and on the FastEthernet0/1 interface connecting to the Server B host. Disable EIGRP autosummarization.

## Activity Verification

You have completed this task when you attain these results:

- On ISR-PxR1, verify its EIGRP adjacency with the ISR-BB hub router:

```
ISR-PxR1#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   172.16.1.1              Tu0               13 00:41:58    1  4476  0  34
```

- On ISR-PxR2, verify its EIGRP adjacency with the ISR-BB hub router:

```
ISR-PxR2#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
```

 © 2010 Cisco Systems, Inc.

```
                                                  (sec)         (ms)       Cnt Num
0   172.16.1.1              Tu0                   14 01:09:56    1  5000  0  37
```

- Verify the routing table on ISR-PxR1:

```
ISR-PxR1#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, su - IS-IS summary, 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

C    172.16.0.0 255.255.0.0 is directly connected, Tunnel0
     172.31.0.0 255.255.255.255 is subnetted, 1 subnets
D       172.31.1.1 [90/297372416] via 172.16.1.1, 00:02:58, Tunnel0
     10.0.0.0 255.255.255.0 is subnetted, 2 subnets
D       10.1.2.0 [90/297502976] via 172.16.1.20, 01:06:07, Tunnel0
C       10.1.1.0 is directly connected, FastEthernet0/1
C    192.168.1.0 255.255.255.0 is directly connected, FastEthernet0/0
```

- Verify the routing table on ISR-PxR2:

```
ISR-PxR2#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, su - IS-IS summary, 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

C    172.16.0.0 255.255.0.0 is directly connected, Tunnel0
     172.31.0.0 255.255.255.255 is subnetted, 1 subnets
D       172.31.1.1 [90/297372416] via 172.16.1.1, 00:01:29, Tunnel0
     10.0.0.0 255.255.255.0 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, FastEthernet0/1
D       10.1.1.0 [90/297502976] via 172.16.1.10, 00:39:57, Tunnel0
C    192.168.1.0 255.255.255.0 is directly connected, FastEthernet0/0
```

- Log in to the client PC system, and ping the Server B system (10.x.2.10). The ping test should succeed. This will trigger the creation of the dynamic spoke-to-spoke tunnel.
- Verify IKE sessions on ISR-PxR1. You should now see an additional IKE session between the two spokes:

```
ISR-PxR1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.1     192.168.1.10    QM_IDLE           1001 ACTIVE
192.168.1.20    192.168.1.10    QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA
```

- Verify NHRP mappings on ISR-PxR1:

```
ISR-PxR1#show ip nhrp
172.16.1.1 255.255.255.255 via 172.16.1.1, Tunnel0 created 05:41:29, never
expire
  Type: static, Flags: used
  NBMA address: 192.168.1.1
172.16.1.20 255.255.255.255 via 172.16.1.20, Tunnel0 created 00:00:30, expire
01:59:29
  Type: dynamic, Flags: router implicit
  NBMA address: 192.168.1.20
    (no-socket)
```

- Verify NHRP mappings on ISR-PxR2:

```
ISR-PxR2#show ip nhrp
172.16.1.1 255.255.255.255 via 172.16.1.1, Tunnel0 created 01:58:26, never
expire
  Type: static, Flags: used
  NBMA address: 192.168.1.1
172.16.1.10 255.255.255.255 via 172.16.1.10, Tunnel0 created 00:01:40, expire
00:05:58
  Type: dynamic, Flags: router implicit
  NBMA address: 192.168.1.10
    (no-socket)
```

 © 2010 Cisco Systems, Inc.

# Lab 3-3: Configuring GET VPN Group Members

Complete this lab activity to practice what you learned in the related module.

## Activity Objective

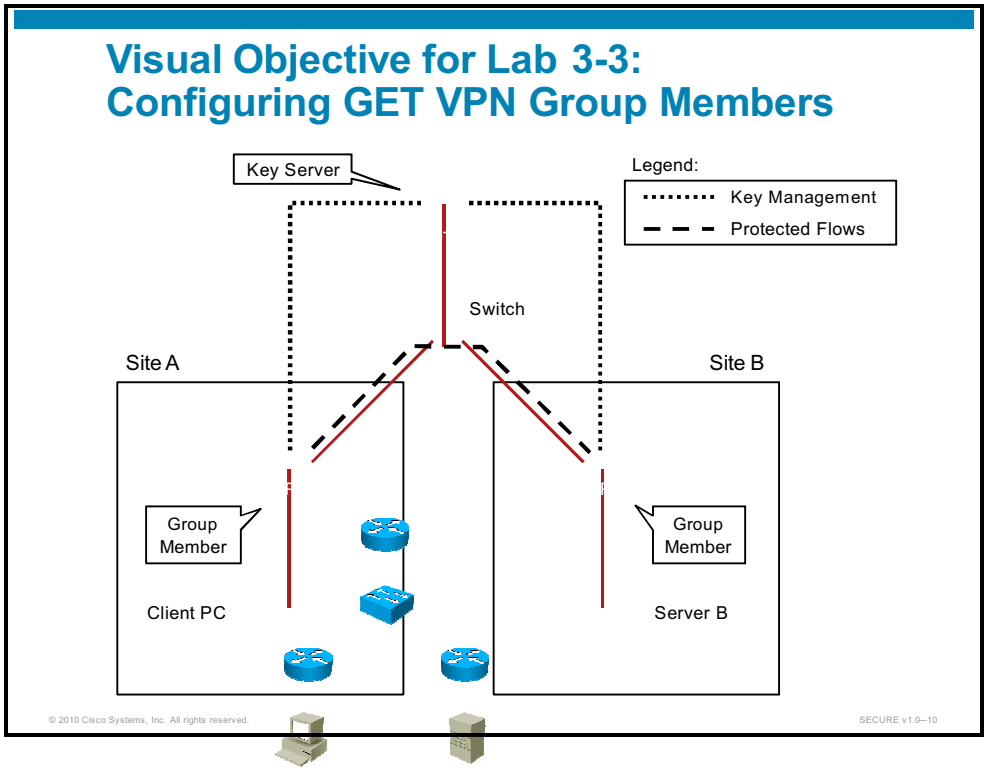
In this activity, you will configure a GET VPN between two member routers and verify its operation using the CLI. The ISR-BB router has been preconfigured by the instructor as the key server.

After completing this activity, you will be able to meet these objectives:

- Verify and evaluate the preconfigured GET VPN key server configuration
- Configure GET VPN group members with a fail-closed traffic policy
- Configure IKE sessions between GET VPN group members and the key server
- Register GET VPN group members to the key server
- Test and verify GET VPN member configuration and registration

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Pod ISR routers
- Pod client PC and Server B systems
- Shared backbone ISR router

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **authentication pre-share** | Specifies PSKs as the authentication method. |
| **crypto gdoi group** *group-name* | Identifies a GDOI group and enters GDOI group configuration mode. |
| **crypto isakmp key password address** *ip-address* | Configures a preshared authentication key. |
| **crypto isakmp policy** *number* | Defines an IKE policy. |
| **crypto map** *map-name* | Applies a crypto map to an interface. |
| **crypto map** *map-name* **number gdoi** | Enters crypto map configuration mode and creates or modifies a crypto map entry. Indicates that the key management mechanism is GDOI. |
| **crypto map** *map-name* **gdoi fail-close** | Sets the crypto map to operate in fail-close mode. |
| **encryption algorithm [ keylength ]** | Sets the IKE encryption type. |
| **group** *number* | Sets the IKE Diffie-Hellman group. |
| **identity number** *number* | Identifies a GDOI group number. |
| **lifetime** *seconds* | Specifies the lifetime of an IKE SA. |
| **server address ipv4** *ip-address* | Specifies the address of the server that a GDOI group is trying to reach. |
| **set group** *group-name* | Sets the GDOI crypto map to the GDOI group that has already been defined. |
| **show crypto gdoi** | Displays information about a GDOI configuration. |
| **show crypto gdoi ipsec sa** | Displays information about the IPsec SA for all group members. |
| **show crypto isakmp policy** | Displays all configured IKE policies. |

# Job Aids

These job aids are available to help you complete the lab activity.

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username | |
| Password | |

 © 2010 Cisco Systems, Inc.

| Parameter | Value |
| --- | --- |
| Username on the Server B | Administrator |
| Password on the Server B | admin |
| Username on the client PC | Administrator |
| Password on the client PC | admin |

# Task 1: Verify Preconfigured GET VPN Key Server Configuration

In this task, you will verify and evaluate the existing IKE and GET VPN key server configuration on ISR-BB. The ISR-BB router has been preconfigured with basic IKE parameters and as the GET VPN key server by your instructor.

## Activity Procedure

Complete these steps:

**Step 1** Log into the console of your ISR-PxR1 router, and from this router, use Telnet to connect to the loopback address (172.31.1.1) of the ISR-BB router. Log in to ISR-BB as user **admin** with the password of **admin**.

**Step 2** On the ISR-BB router, examine the IKE (ISAKMP) policies that are configured on the ISR-BB key server.

| **Note** | Note the settings of the highest priority IKE (ISAKMP) policy. You will have to configure a matching policy on the two GET VPN group members. |
|---|---|

**Step 3** On the ISR-BB router, examine the GET VPN key server policy that is configured on the ISR-BB router.

**Step 4** On the ISR-BB router, observe the contents of the traffic-protecting ACL. Verify that it includes a rule that will protect traffic between your two pod sites bidirectionally.

## Activity Verification

You have completed this task when you have completed all the tasks in the Activity Procedure section.

# Task 2: Configure GET VPN Group Members Including a Fail-Closed Policy

In this task, you will configure and verify a GET VPN member, including a fail-closed policy on your two group members. A fail-closed policy prevents communication through untrusted interfaces until GET VPN IPsec SAs have been established and hence prevents data leakage into the untrusted network.

## Activity Procedure

Complete these steps:

**Step 1** Log into the console of your ISR-PxR1 router.

**Step 2** On the ISR-PxR1 router, configure an IKE (ISAKMP) policy of high priority that will match the highest-priority policy of the key server. As recommended in the course, configure a lower IKE SA lifetime of 300 seconds on the spoke.

**Step 3** On the ISR-PxR1 router, configure an authentication key of **secretpassword** for the key server. The key server uses its loopback address (172.31.1.1) for IKE peering. In real life, make sure that you use long and random PSKs.

**Step 4** On ISR-PxR1, configure a GDOI group with the following parameters:

- The name of the group should be MYGETVPNGROUP.
- The group identity should be based on a number; set it to 12345.

 © 2010 Cisco Systems, Inc.

- The key server is located at 172.31.1.1.

**Step 5** On the ISR-PxR1 router, configure a crypto map entry of type GDOI, low priority (10). Inside it, set the GET VPN group to MYGETVPNGROUP.

**Step 6** On the ISR-PxR1 router, configure the MYCRYPTOMAP crypto map as a fail-close crypto map and activate its fail-closed status.

**Step 7** Apply the crypto map to the untrusted interface (the interface inside the 192.168.1.0/24 network).

**Note** Note that the router will not be able to authenticate and register to the key server, because the key server does not have a PSK that is configured for the group member. Do not configure the pre-shared key on the key server yet, because you have to test the fail-closed policy on the group member.

**Step 8** Repeat all Task 2 steps on the ISR-PxR2 router.

## Activity Verification

You have completed this task when you attain these results:

- On the ISR-PxR1 router, verify that the IKE (ISAKMP) policy has been correctly configured using the **show crypto isakmp policy** command:

```
ISR-PxR1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption
Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
        lifetime:               300 seconds, no volume limit
```

- Repeat the last step on the ISR-PxR2 router. You should observe the same output.
- On the ISR-PxR1 router, verify that the GET VPN policy has been correctly configured using the **show crypto gdoi** command:

```
ISR-PxR1#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPNGROUP
    Group Identity           : 12345
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 172.31.1.1

    Group member             : 192.168.1.2      vrf: None
       Registration status   : Registering
       Registering to        : 172.31.1.1
       Re-registers in       : 35 sec
       Succeeded registration: 0
```

```
        Attempted registration: 3
        Last rekey from       : 0.0.0.0
        Last rekey seq num    : 0
        Multicast rekey rcvd  : 0

      Rekeys cumulative
        Total received        : 0
        After latest register : 0
        Rekey Received        : never

   ACL Downloaded From KS UNKNOWN:

  TEK POLICY for the current KS-Policy ACEs Downloaded:
```

- Repeat the last step on the ISR-PxR2 router. You should observe the same output, except for a different local IP address.
- On the ISR-PxR1 router, verify that the crypto map has been correctly applied to the interface using the **show crypto map** command:

```
ISR-PxR1#show crypto map
Crypto Map "MYCRYPTOMAP" 10 gdoi
        Group Name: MYGETVPNGROUP
            identity number 12345
            server address ipv4 172.31.1.1
        Interfaces using crypto map MYCRYPTOMAP:
                GigabitEthernet0/0
```

- Repeat the last step on the ISR-PxR2 router. You should observe the same output.
- Verify that the fail-closed policy is working properly. Log in to the client PC, open a command prompt window, and attempt to ping an address in the lab Internet (172.16.1.1). You should not succeed, because the group member is dropping all outbound traffic.

```
C:\Windows\system32>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

# Task 3: Configure Group Member IKE Credentials on the Key Server and Establish Secure Site-to-Site Connectivity

In this task, you will configure member authentication credentials on the key server, which should allow group member authentication and registration. After the group members have registered, you will verify site-to-site connectivity with both group members protecting traffic using GET VPN IPsec encapsulation.

 © 2010 Cisco Systems, Inc.

## Activity Procedure

Complete these steps:

**Step 1** Log in to the ISR-PxR1 router, and from this router, use Telnet to connect to the loopback address (172.31.1.1) of the ISR-BB router. Log in as user **admin** with the password of **admin**.

**Step 2** On the ISR-BB router, configure two ISAKMP keys with the key string of **secretpassword** for both your group members. Your group members use IP addresses 192.168.x.10 (ISR-PxR1) and 192.168.x.20 (ISR-PxR2) to register with the key server.

## Activity Verification

You have completed this task when you attain these results:

- Log into the console of your ISR-PxR1 router. Verify that it has registered with the key server and has created the IPsec SAs:

```
ISR-PxR1#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPNGROUP
    Group Identity           : 12345
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 172.31.1.1

    Group member             : 192.168.1.2      vrf: None
       Registration status   : Registered
       Registered with       : 172.31.1.1
       Re-registers in       : 3419 sec
       Succeeded registration: 1
       Attempted registration: 19
       Last rekey from       : 0.0.0.0
       Last rekey seq num    : 0
       Unicast rekey received: 0
       Rekey ACKs sent       : 0
       Rekey Received        : never

    Rekeys cumulative
       Total received        : 0
       After latest register : 0
       Rekey Acks sents      : 0

 ACL Downloaded From KS 172.31.1.1:
   access-list  permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 86399
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 2048

TEK POLICY for the current KS-Policy ACEs Downloaded:
  GigabitEthernet0/0:
    IPsec SA:
        spi: 0xB8B5CB91(3098921873)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (3590)
        Anti-Replay :  Disabled
```

- Repeat the previous verification step on ISR-PxR2.

- Verify intersite connectivity, which should now be protected by IPsec. Log in to the client PC, open a command prompt window, and attempt to ping an address of Server B in the other site (10.1.2.10). You should succeed.

```
C:\Windows\system32>ping 10.1.2.10

Pinging 10.1.2.10 with 32 bytes of data:
Reply from 10.1.2.10: bytes=32 time=1ms TTL=127
Reply from 10.1.2.10: bytes=32 time=1ms TTL=127
Reply from 10.1.2.10: bytes=32 time=1ms TTL=127
Reply from 10.1.2.10: bytes=32 time=1ms TTL=127
```

- On the ISR-PxR1, verify that the IPsec SA counters are increasing using the **show crypto ipsec sa** command.

```
ISR-PxR1#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: MYCRYPTOMAP, local addr 192.168.1.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
   current_peer 0.0.0.0 port 848
     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

<...rest of output omitted...>
```

 © 2010 Cisco Systems, Inc.

# Lab 4-1: Configuring a Cisco IOS Software SSL VPN Gateway

Complete this lab activity to practice what you learned in the related module.

## Activity Objective

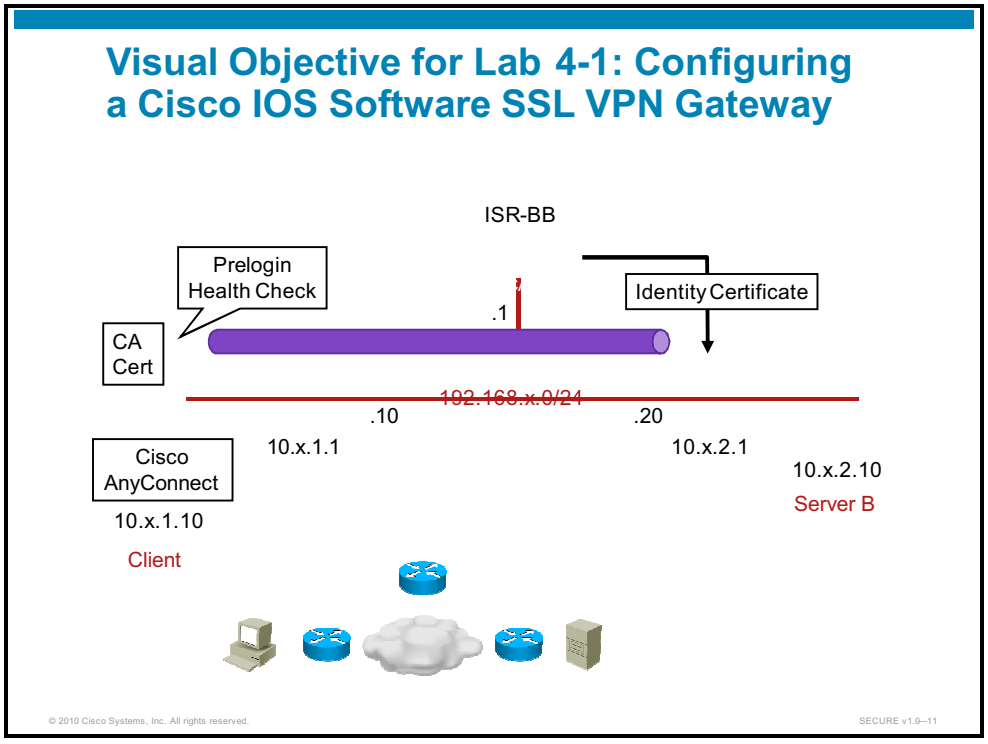
In this activity, you will configure the ISR-PxR2 router as an SSL VPN gateway.

After completing this activity, you will be able to meet these objectives:

- Provision a certificate to the SSL VPN gateway
- Import the root CA certificate into the client certificate store
- Configure a router as a full tunneling SSL VPN gateway
- Install the Cisco AnyConnect client and establish a full tunneling SSL VPN
- Configure a router as a clientless SSL VPN gateway
- Configure basic Cisco Secure Desktop features for a clientless SSL VPN

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Pod ISR routers
- Pod client PC and Server B systems

- Shared backbone ISR-BB router

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **aaa authentication login {default \| *list-name*} { method1 [method2...]}** | Sets AAA at login. |
| **aaa new-model** | Enables the AAA access control mode. |
| **auto-summary** | Allows automatic summarization of subnet routes into network-level routes. To disable this function and send subprefix routing information across classful network boundaries, use the no form of this command. |
| **banner** *string* | Configures a banner to be displayed after a successful login in WebVPN group policy. |
| **copy tftp: flash:** | Copies a file from the TFTP server to flash. |
| **crypto ca authenticate** | Authenticates the certification authority (by getting the certificate of the CA). |
| **crypto ca enroll** | Obtains the certificates for your router from the CA. |
| **crypto pki authenticate** | Authenticates the certification authority (by getting the certificate of the CA). |
| **crypto pki enroll** | Obtains the certificates for your router from the CA. |
| **crypto pki export** *trustpoint* **pem {terminal \| url** *url***} {3des \| des}** *passphrase* | Exports certificate and RSA keys that are associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file. |
| **crypto pki trustpoint** *name* | Declares the trustpoint that your router should use. |
| **csd enable** | Enables Cisco Secure Desktop support for SSL VPN sessions in WebVPN context configuration mode. |
| **default-group-policy** *name* | Associates a policy group with an SSL VPN context configuration in WebVPN context configuration mode. |
| **enrollment url** *url* | Specifies the enrollment parameters of a CA. |
| **functions svc-enabled** | Enables full tunneling for a policy group. |
| **gateway** *webvpn-gateway-name* | Binds context to a gateway inside context configuration mode. |
| **inservice** | Enables an SSL VPN gateway or context process. |
| **ip address** *ip-address* **port** *port-number* | Configures a proxy IP address on an SSL VPN gateway and specifies the port number for proxy traffic. |
| **ip host** *hostname ip-address* | Defines static hostname-to-address mappings in the DNS hostname cache. |
| **ip local pool {default \|** *poolname***} [***low-ip-address* **[***high-ip-address***]]** | Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface. |
| **logging enable** | Enables syslog logging of SSL VPN gateway-related messages. |

 © 2010 Cisco Systems, Inc.

| Command | Description |
| --- | --- |
| **network** *ip-address* [*wildcard-mask*] | Specifies the network for an EIGRP routing process. |
| **ping** | Determines if other IP addresses are accessible. |
| **policy group** | Enters WebVPN group policy configuration mode to configure a group policy. |
| **router eigrp** *autonomous-system-number* | Configures the EIGRP routing process. |
| **show ip route** | Displays the routing table. |
| **show running-config** | Displays the configuration that is currently running on the adaptive security appliance. |
| **show webvpn gateway** | Display the status of an SSL VPN gateway. |
| **show webvpn session context** *context-name* | Displays SSL VPN user session information for context. |
| **ssl trustpoint** *name* | Configures the certificate trustpoint on an SSL VPN gateway. |
| **svc address-pool** | Configures a pool of IP addresses to assign to end users in a policy group. |
| **svc keep-client-installed** | Configures the end user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled. |
| **svc split include** *ip-address mask* | Enables split tunneling for Cisco AnyConnect VPN Client tunnel clients in WebVPN group policy configuration mode. |
| **url-list** *name* | Enters WebVPN URL list configuration mode to configure a list of URLs to which a user has access on the portal page of an SSL VPN and to attach the URL list to a policy group. |
| **url-text {***name* **url-value** *url***}** | Adds an entry to a URL list in URL list configuration mode. |
| **username** *name* **privilege** *level* **password** *password* | Establishes a username-based authentication system with privilege level specified. |
| **webvpn context** *name* | Enters WebVPN context configuration mode to configure the SSL VPN context. |
| **webvpn gateway** *name* | Enters WebVPN gateway configuration mode to configure an SSL VPN gateway. |
| **webvpn install [csd** *location-name* **\| svc** *location-name***]** | Installs a Cisco Secure Desktop or Cisco AnyConnect VPN Client package file to an SSL VPN gateway. |

# Job Aids

These job aids are available to help you complete the lab activity.

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username on the Server B | Administrator |
| Password on the Server B | admin |
| Username on the client PC | Administrator |
| Password on the client PC | admin |

 © 2010 Cisco Systems, Inc.

# Task 1: Provision a Certificate to the SSL VPN Gateway

In this task, you will provision a certificate to the PxR2 router, which will act as an SSL VPN gateway to support full tunneling and clientless SSL VPN users. You will create a PKI trustpoint, authenticate the PKI CA, and create an enrollment request for a certificate to obtain an identity certificate. The ISR-BB router has been preconfigured as a CA server.

## Activity Procedure

Complete these steps:

**Step 1** Log in to the console of your ISR-PxR2 router.

**Step 2** Create a PKI trustpoint with the following properties.

- Specify the enrollment URL as the web server of router ISR-BB (**http://192.168.1.1**).
- Set the router FQDN to **vpn.cisco.com**.
- Set the CN field of the X.500 subject name of the router to **vpn.cisco.com**.

**Step 3** Authenticate the CA

**Step 4** Create an enrollment request and enroll in the CA.

**Note** If your enrollment fails, ensure that the clock on the ISR-PxR2 is set to the same time as the clock of the ISR-BB router.

# Task 2: Import the Root CA Certificate into the Client Certificate Store

In this task, you will export the (root) CA certificate of the ISR-BB router, which acts as a CA server, from the certificate store of the ISR-PxR2 router (which obtained it during the CA authentication process). You will import this CA certificate into the certificate store of the client PC. The client PC will use this certificate to validate the authenticity of the certificate of the SSL VPN gateway when establishing the SSL connection to the gateway.

## Activity Procedure

Complete these steps:

**Step 1** Log in to the console of your ISR-PxR2 router.

**Step 2** Use **crypto pki export** *trustpoint_name* **pem terminal** to export the ISR-BB CA certificate to the console, in which *trustpoint_name* is the name of the trustpoint that was configured in Task 1.

**Step 3** In the output, copy the first section (starting with the string **% CA certificate**) from (and including) the -----BEGIN CERTIFICATE----- line to (and including) the -----END CERTIFICATE----- line to the clipboard.

**Step 4** Log in to the client PC, open the Notepad editor, and paste the contents of the clipboard into it. Save the file as **root.cer** on the client PC desktop.

**Step 5** On the client PC, double-click the **root.cer** file on the desktop**.** Click **Install Certificate** and click **Next** twice, which will automatically select the certificate store that is based on the certificate type. Click **Finish** and then **OK** to confirm that import was successful.

# Task 3: Configure a Router as a Full Tunneling SSL VPN Gateway

In this task, you will configure the ISR-PxR2 router as a full tunneling SSL VPN Gateway.

## Activity Procedure

Complete these steps:

**Step 1** Configure EIGRP on the ISR-PxR1 and ISR-PxR2 routers. ISR-PxR1 should advertise networks 192.168.x.0/24 and 10.x.1.0/24. ISR-PxR2 should advertise only the 192.168.x.0/24 network.

**Note** ISR-PxR2 does not advertise network 10.x.2.0/24, so the client PC cannot reach network 10.x.2.0/24 without the SSL VPN being established.

**Step 2** On the ISR-PxR2, create an SSL VPN gateway object with the following properties:

- The gateway should bind to the IP address of the FastEthernet0/0 interface and use the default HTTPS TCP port of 443.
- The gateway should use the identity certificate that is associated with the trustpoint configured in Task 1
- You should enable SSL VPN related logging.

**Step 3** On the client PC, start the TFTP server by clicking its icon (**TFTPSRV.EXE**) on the desktop, and set the TFTP root directory to C:\SECURE.

**Step 4** On the ISR-PxR2, copy the Cisco AnyConnect client image file to the flash file system from the **tftp://10.1.1.10/anyconnect-win-2.2.0134-k9.pkg** URL, and install the Cisco AnyConnect VPN Client package file.

**Step 5** On ISR-PxR2, create an SSL VPN context that is associated with the configured gateway, with the following properties:

- The context should authenticate users against the local database. You should create at least one user who will be able to log in to SSL VPN.

**Step 6** The context should enforce the following access policy:

- It should display the “Welcome to SSL VPN” banner to remote full tunneling users upon login.
- It should allow full tunneling (Cisco AnyConnect) sessions.
- The Cisco AnyConnect client should not be uninstalled after logout,
- The policy should assign IP addresses in the 172.16.0.1- 172.16.0.10 range to remote full tunneling users.
- Only traffic between the client and the 10.1.2.0/24 network should be routed through the VPN tunnel.

## Activity Verification

You have completed this task when you attain these results:

- Check the status of an SSL VPN gateway. It should indicate *up* as its administrative and operational status:

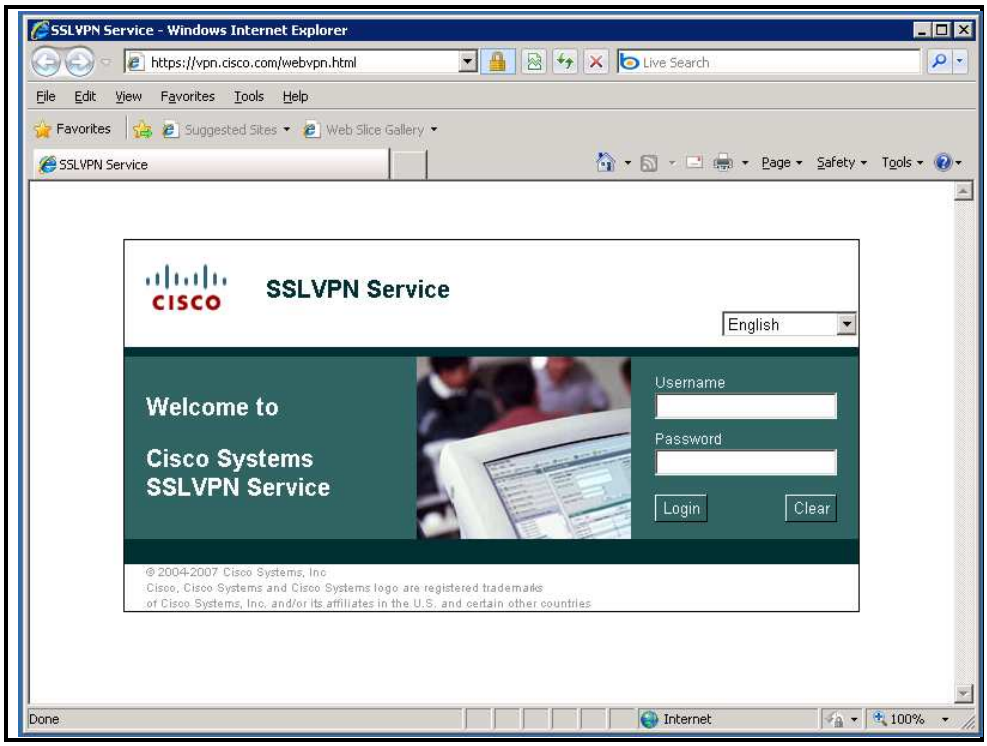
```
ISR-PxR2#show webvpn gateway
```

 © 2010 Cisco Systems, Inc.

```
Gateway Name                    Admin  Operation
------------                    -----  ---------
MY-GATEWAY                      up     up
```

- On the client PC, use a browser to navigate to the URL of the SSL VPN gateway **https://vpn.cisco.com,** in which a default SSL VPN portal login page should open.

**Note** If you have properly imported the CA certificate, you should receive no certificate warnings.



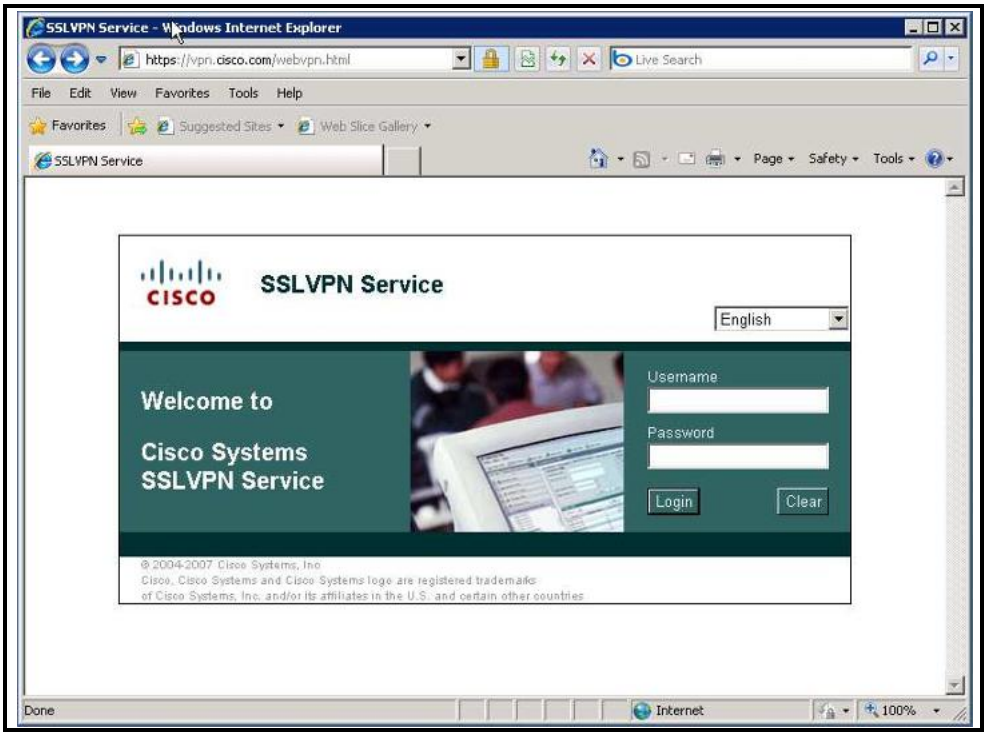

# Task 4: Install the Cisco AnyConnect Client and Establish a Full Tunneling SSL VPN

In this task, you will install the Cisco AnyConnect client on the client PC. You do not need an offline installation file on the client PC, because you will use the Cisco AnyConnect VPN Client package file inside the ISR-PxR2 flash file system. You will also verify connectivity over a full tunneling SSL VPN connection.

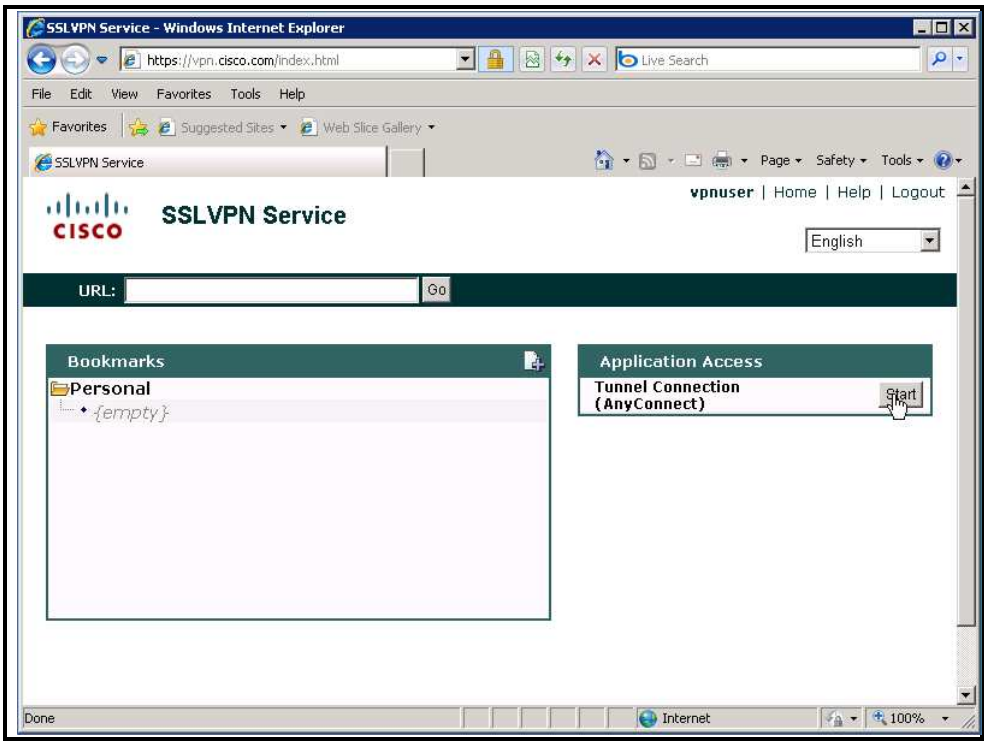
## Activity Procedure

Complete these steps:

**Step 1** On the client PC, open a browser and navigate to the **https://vpn.cisco.com** URL, which is the home page of the SSL VPN gateway. Log in to the VPN portal using the VPN username and password that was configured in the local database of ISR-PxR2 in the previous task.

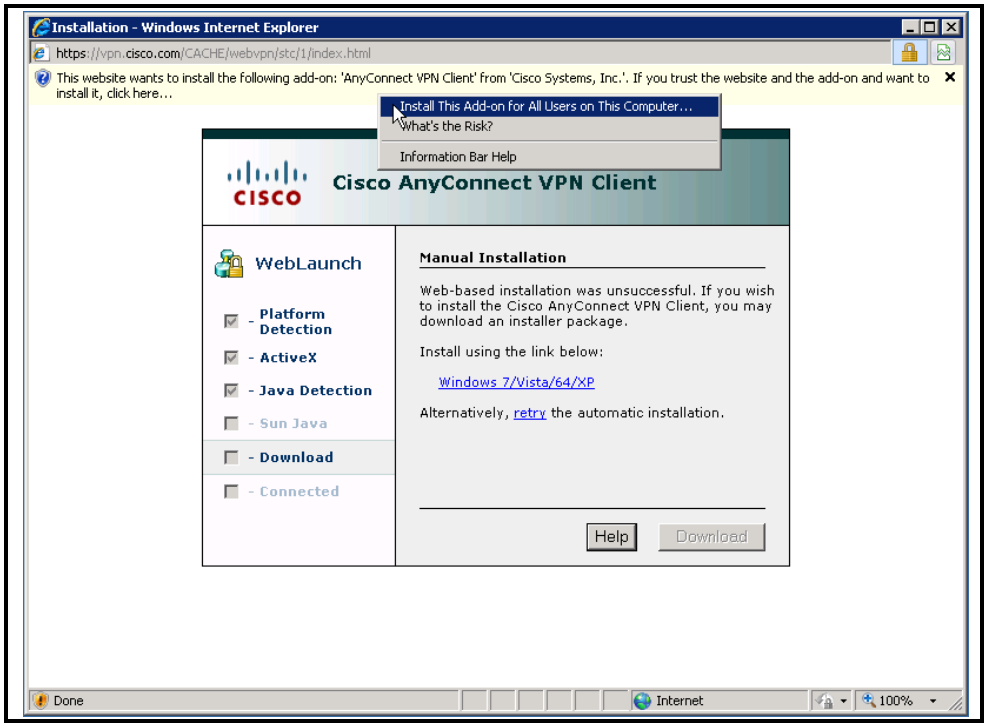



**Step 2** Install the Cisco AnyConnect client by clicking the **Start** button in the **Application Access** portal section.

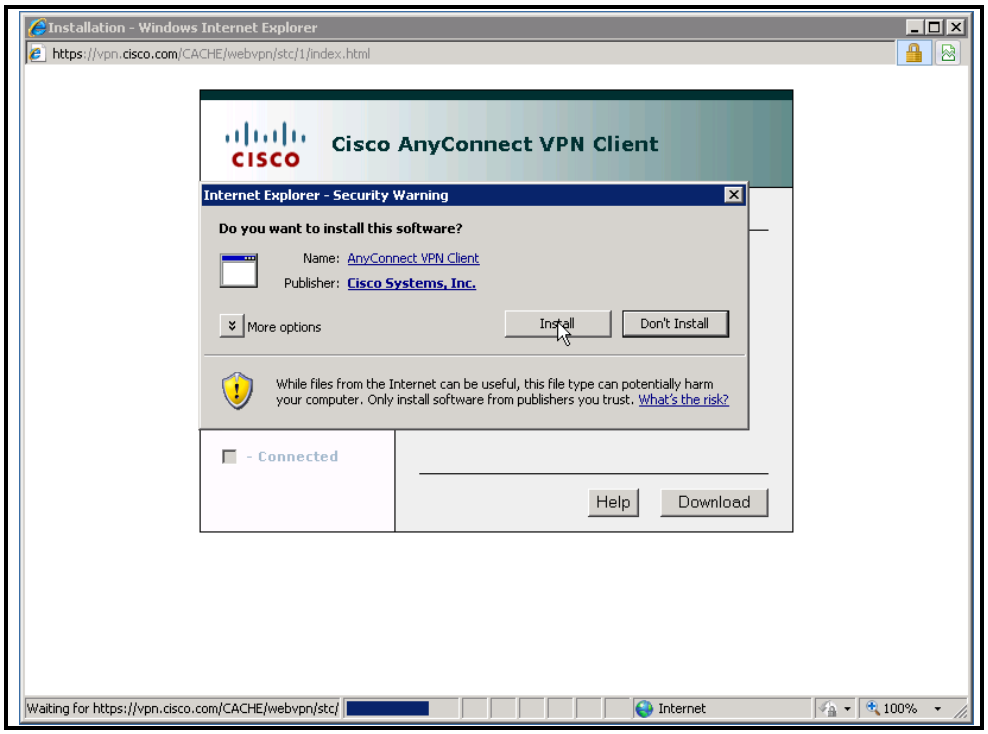



**Step 3** Install the AnyConnect VPN Client add-on (installation helper application) into the browser.

 © 2010 Cisco Systems, Inc.




**Step 4** Click **Install** when prompted to install the Cisco AnyConnect VPN Client.




**Note** In a few moments, a full tunneling SSL VPN connection should be established and the Cisco AnyConnect icon should appear in the system tray of the client PC.




**Step 5** Right-click the **Cisco AnyConnect** icon in the system tray, and click **Open AnyConnect**. Explore various options:

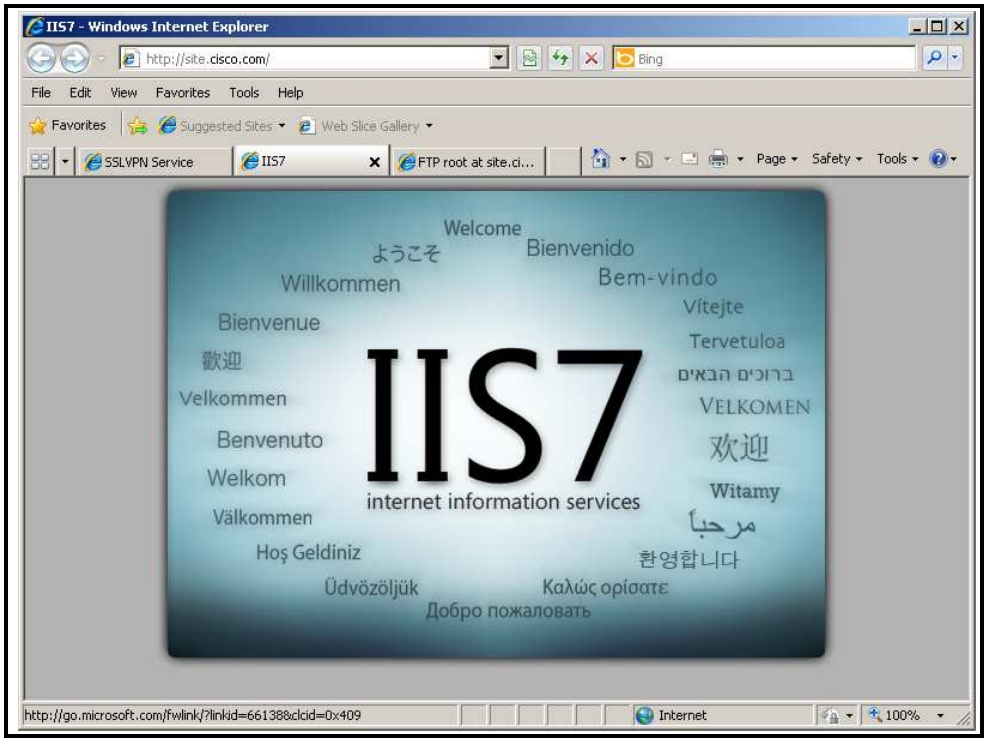
- Connection tab
- Statistics tab
- Check statistical details by opening the Statistics tab and clicking **Details**
- Within Statistic Details, select the **Route Details** tab

## Activity Verification

You have completed this task when you attain these results:

- On the client, use the Internet Explorer browser to verify the HTTP to the server, which is accessible behind the SSL VPN gateway as **http://site.cisco.com**. Your connection should be successful.

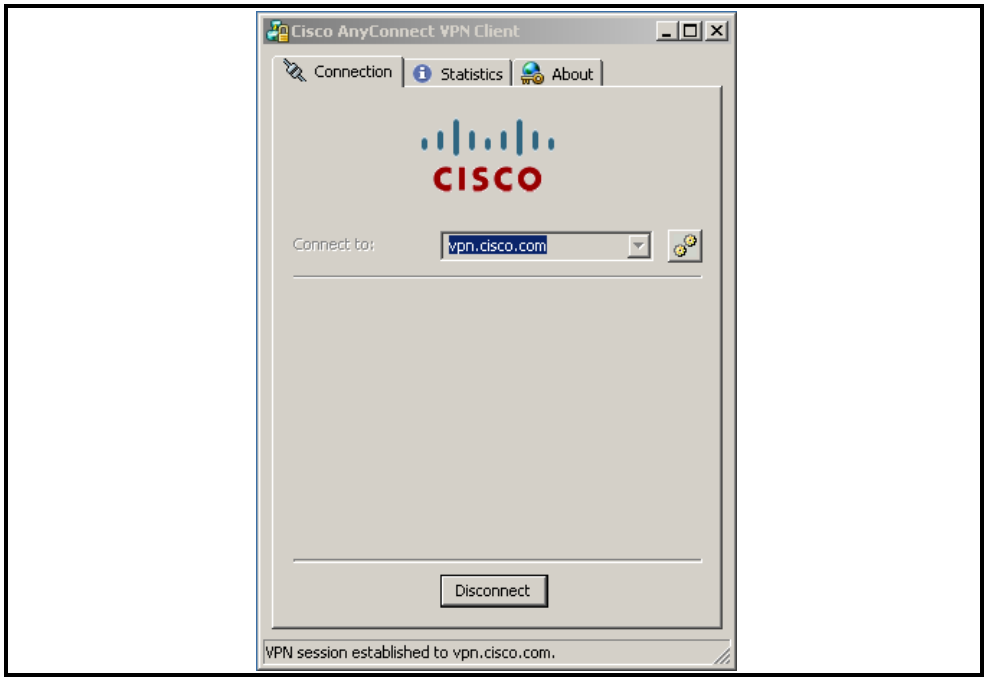
 © 2010 Cisco Systems, Inc.



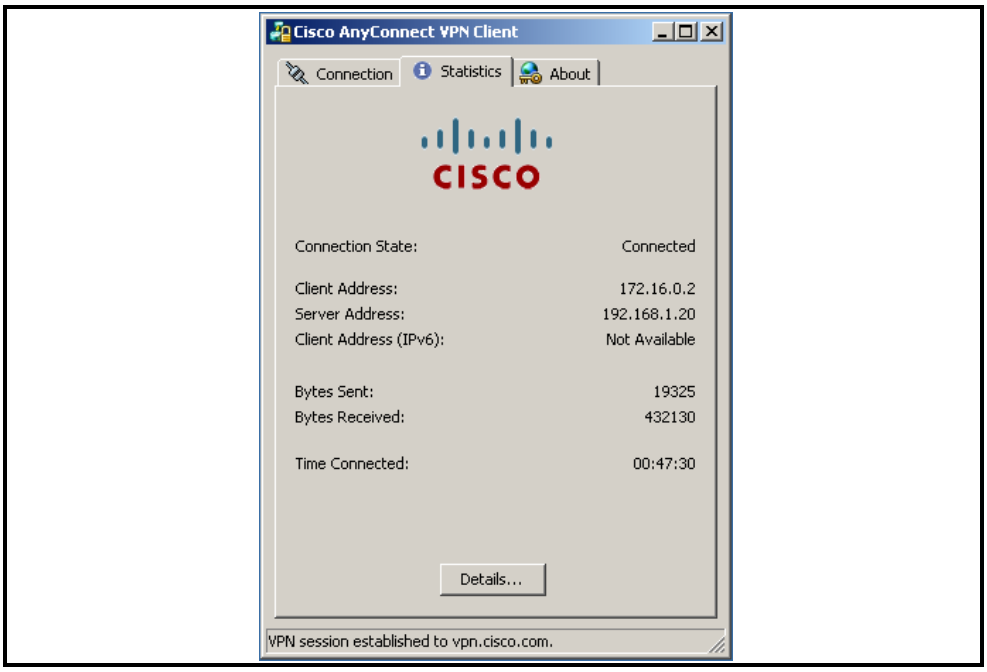

- On ISR-PxR2, verify that an SSL VPN session with the client PC is established inside your SSL VPN context:

```
ISR-PxR2#show webvpn session context MY-CONTEXT
WebVPN context name: MY-CONTEXT
Client_Login_Name  Client_IP_Address  No_of_Connections
Created  Last_Used
vpnuser            10.1.1.10                 1
00:08:57  00:08:39
```

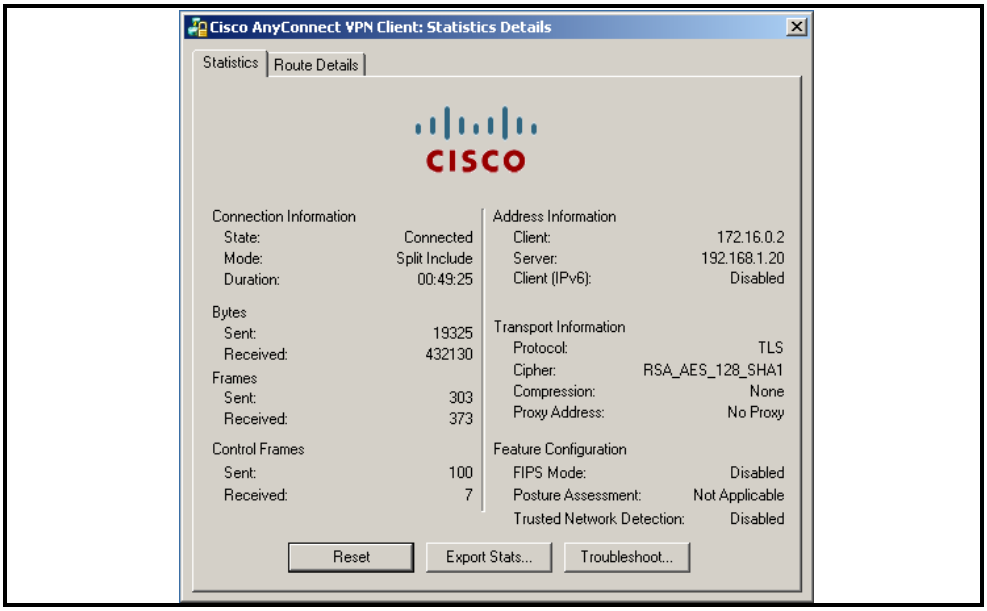
- On the client PC, open the Cisco AnyConnect client by double-clicking its icon in the system tray. Examine the **Connection** tab:



- Examine the **Statistics** tab:

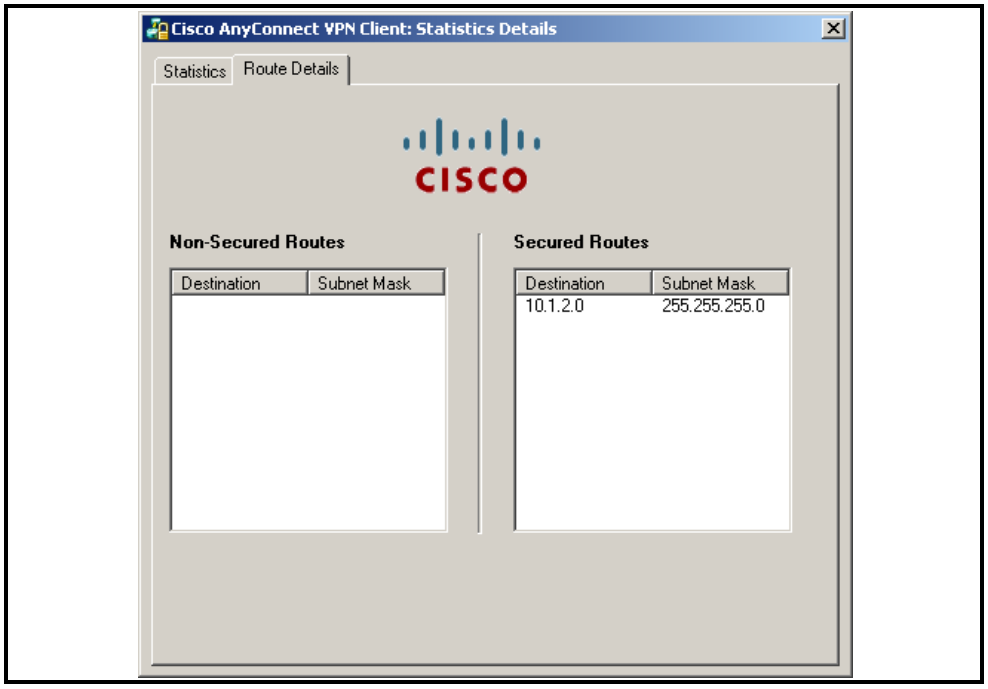



- Check statistics details by clicking the **Details** button in the Statistics tab:




- Verify the **Route Details** tab in the **Statistic Details** window. You should see a specific (split tunneling) route to the remote 10.x.2.0/24 network):

 © 2010 Cisco Systems, Inc.




# Task 5: Configure a Router as a Clientless SSL VPN Gateway

In this task, you extend the SSL VPN gateway configuration to provide clientless access, which allows remote users to access internal resources using only a supported browser.

## Activity Procedure

Complete these steps:

**Step 1** On the client PC, disconnect from the full tunneling VPN by right-clicking the **Cisco AnyConnect** icon in the system tray and selecting **Disconnect**.

**Step 2** On the ISR-PxR2 router, configure your SSL VPN context with the following clientless portal features:

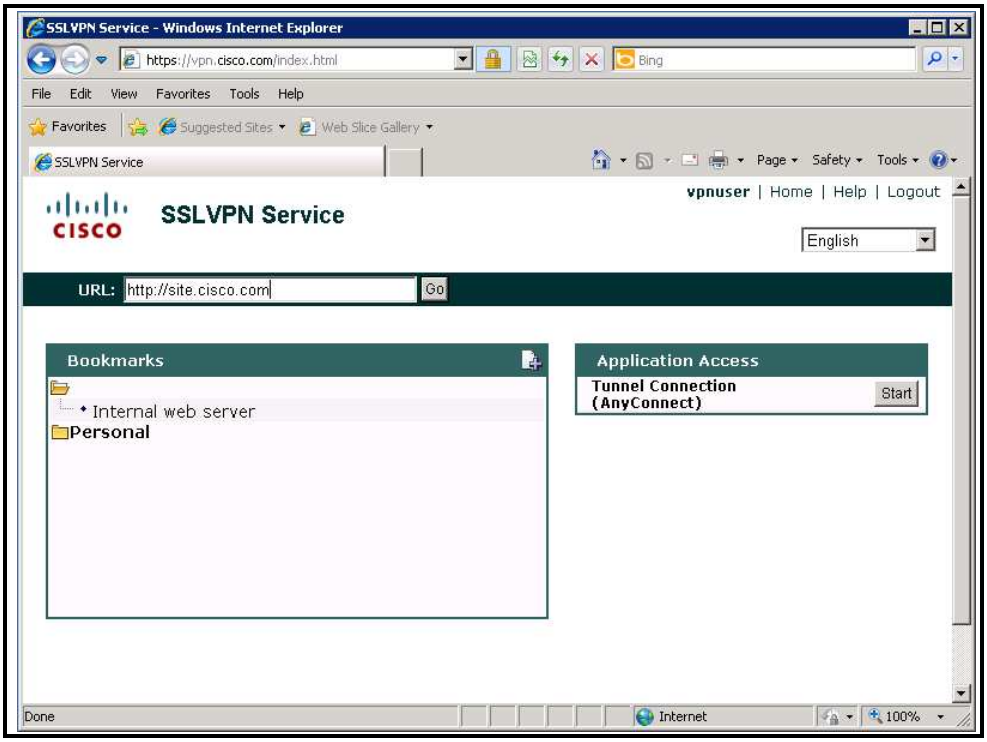
- Create a bookmark list containing a bookmark for the **http://site.cisco.com** internal web server.
- Enable this bookmark list for all SSL VPN users.

**Step 3** On the ISR-PxR2 router, define a static hostname-to-address mapping to map the site.cisco.com hostname to the IP address of your server host (10.x.2.10).

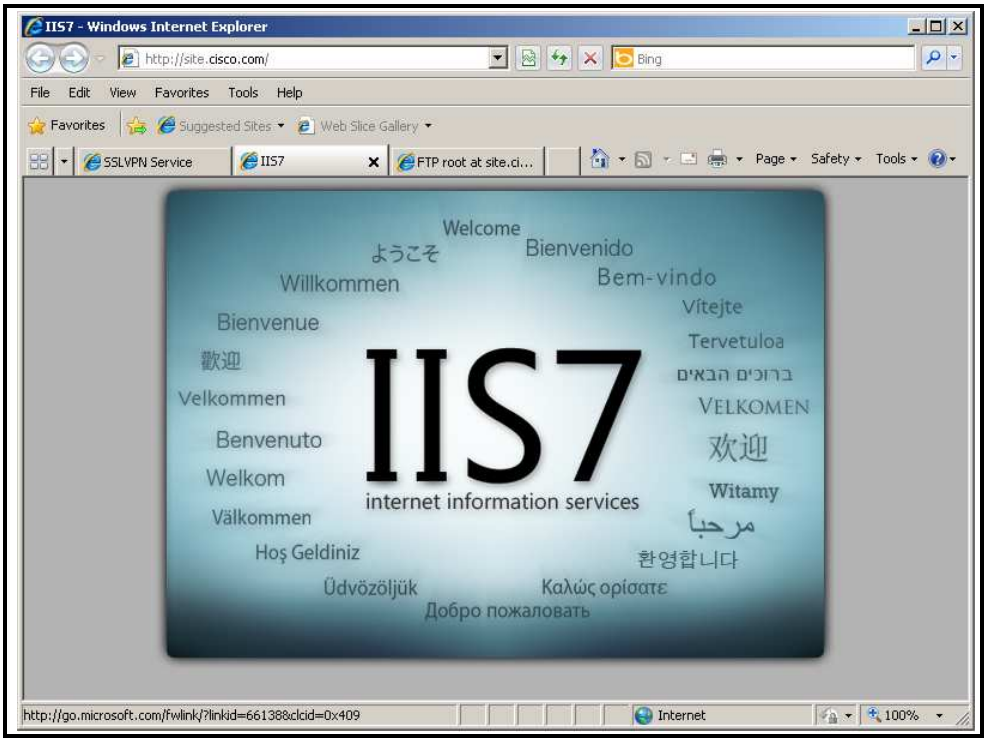
## Activity Verification

You have completed this task when you attain these results:

- On the client PC, open a browser and navigate to the **https://vpn.cisco.com** URL, which is the home page of the SSL VPN gateway. Log in to the VPN portal using the VPN username and password that are configured in the local database of ISR-PxR2 in the previous task.
- Verify that the configured bookmark list is present on the portal.




- Click the configured bookmark to verify HTTP connectivity to the server.




- Navigate back to the home page of the portal using SSL VPN portal controls (hovering at the top of the browser content window). Type **http://site.cisco.com** into the URL window on SSL VPN Service portal. HTTP connectivity to the server should also work using the URL entry option.

 © 2010 Cisco Systems, Inc.

# Task 6: Configure Basic Cisco Secure Desktop Features for a Clientless SSL VPN

In this task, you will deploy a basic Cisco Secure Desktop environment to clientless SSL VPN users.

## Activity Procedure

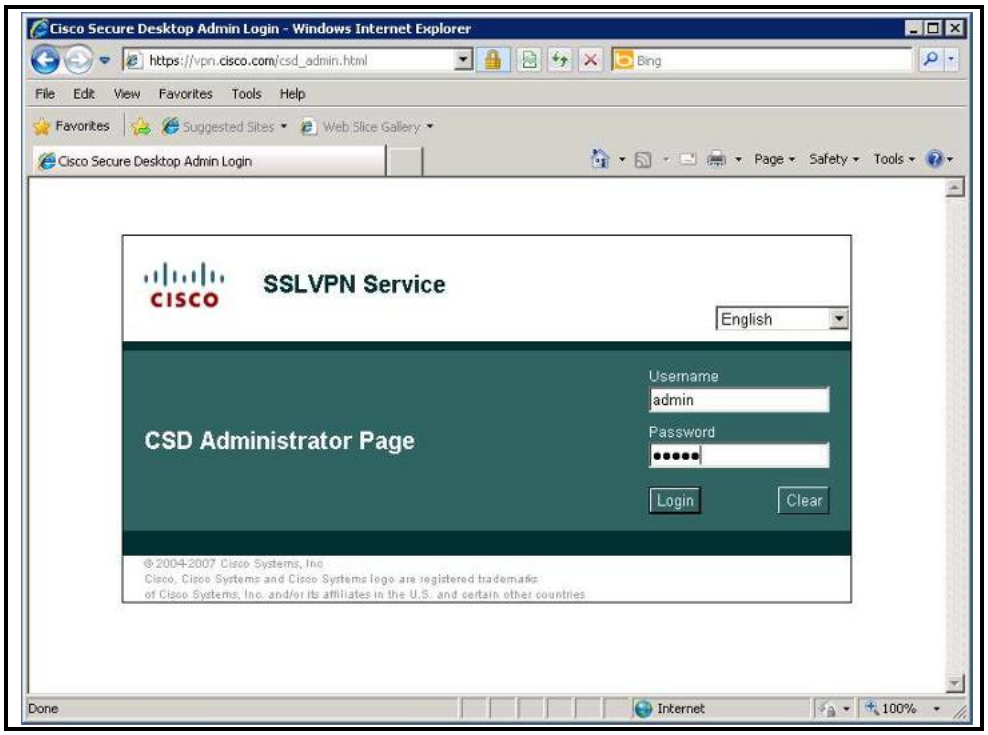
Complete these steps:

**Step 1** On the ISR-PxR2 router, copy the Cisco Secure Desktop image to the flash file system from the **tftp://10.1.1.10/securedesktop-ios-3.1.1.45-k9.pkg** URL. Install the Cisco Secure Desktop package file.

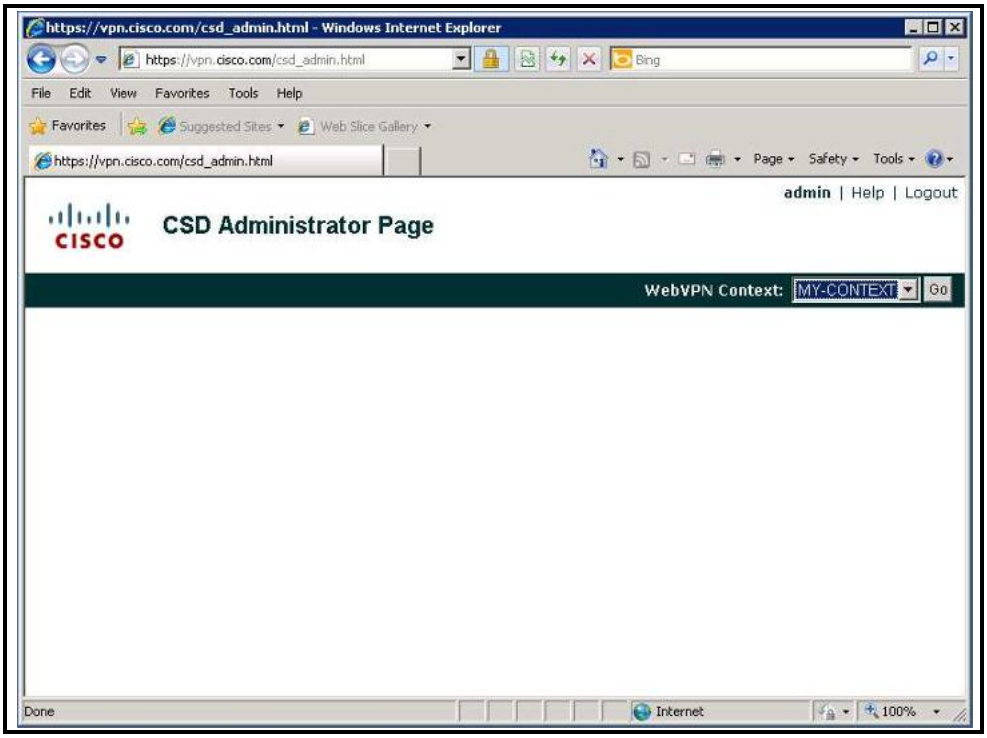
**Step 2** Enable Cisco Secure Desktop in your SSL VPN context.

**Step 3** On the ISR-PxR2 router, create an enable secret of **cisco**.

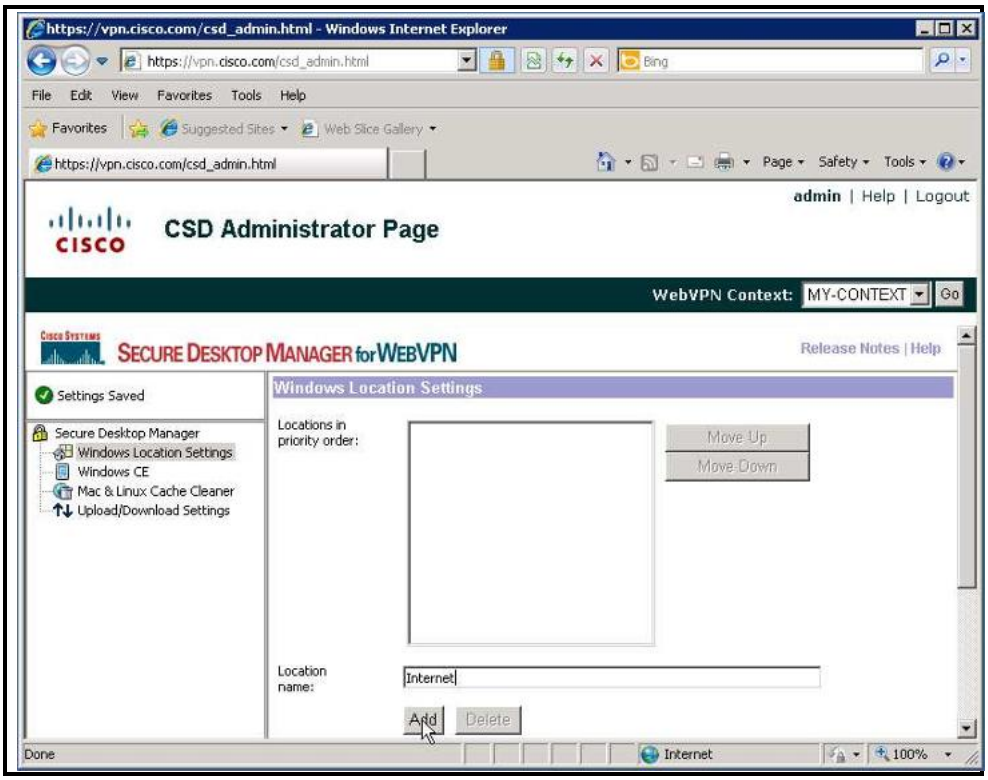
**Step 4** From the client, configure Cisco Secure Desktop by navigating to the **https://vpn.cisco.com/csd_admin.html** URL. Log in using the username **admin** and password **cisco**.




**Step 5** Select the WebVPN context that is configured in Task 2 and click the **Go** button.



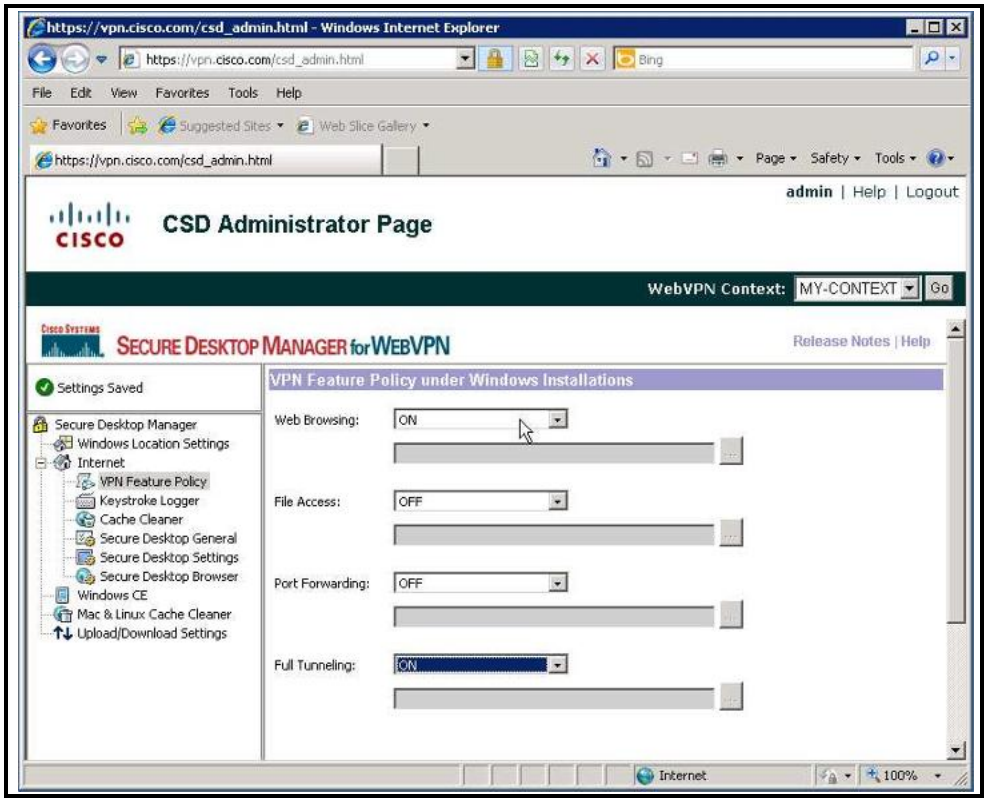

**Step 6** Select **Windows Location Settings** and add a Location named **Internet**.



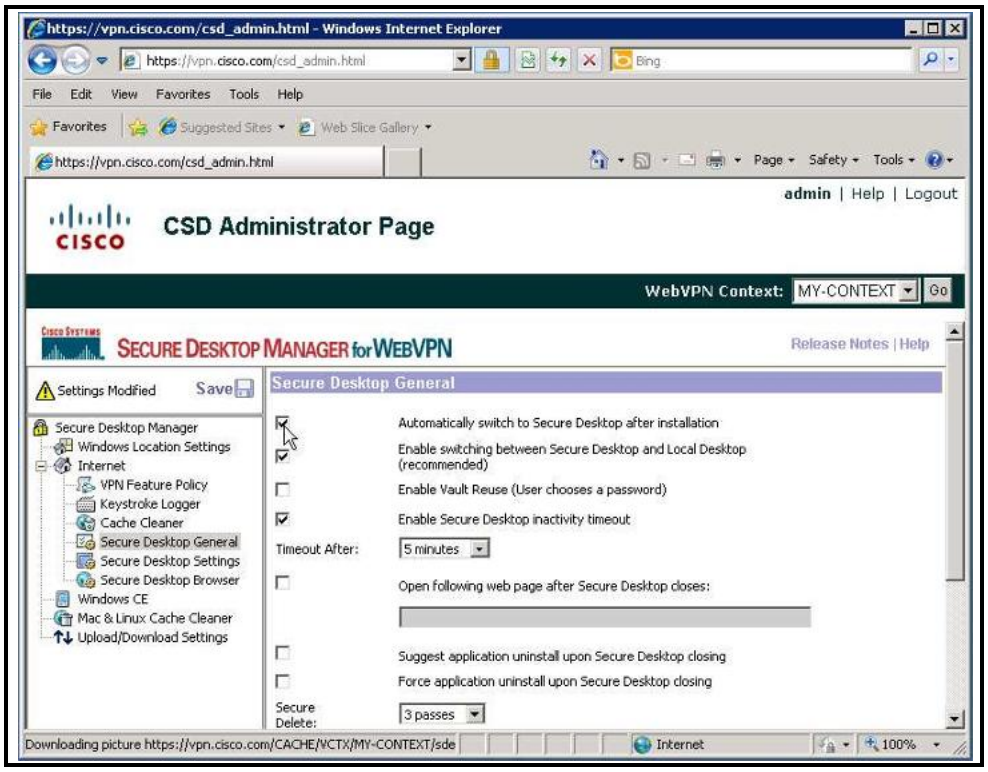

**Step 7** The location “Internet” should now appear in the left pane. Expand it and choose the **VPN Feature Policy** option, then complete these tasks:

- Enable web browsing for remote users using Cisco Secure Desktop.
- Enable full tunneling for remote users using Cisco Secure Desktop.

 © 2010 Cisco Systems, Inc.

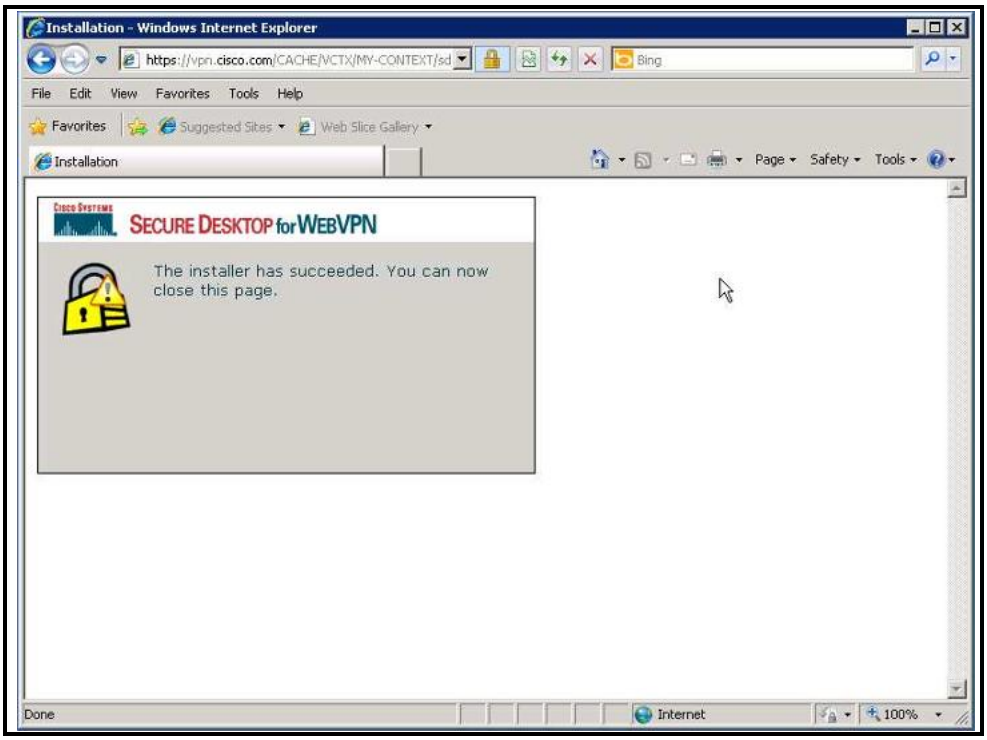



**Step 8** Under location Internet, choose the **Secure Desktop General** option, and enable the option **Automatically Switches to Secure Desktop After Installation**. Click **Save** when you are finished.

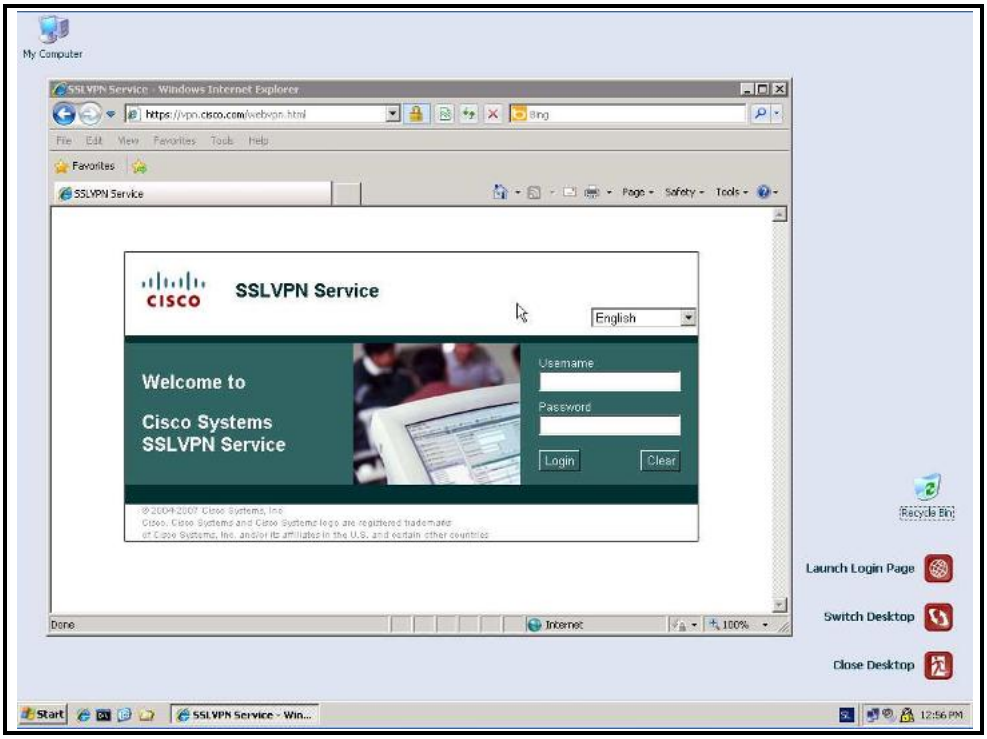



**Step 9** On the client PC, close all browsers.

**Step 10** On the client PC, use a web browser to navigate to the **https://vpn.cisco.com** URL to log in to the VPN. The installation of Cisco Secure Desktop will begin automatically.

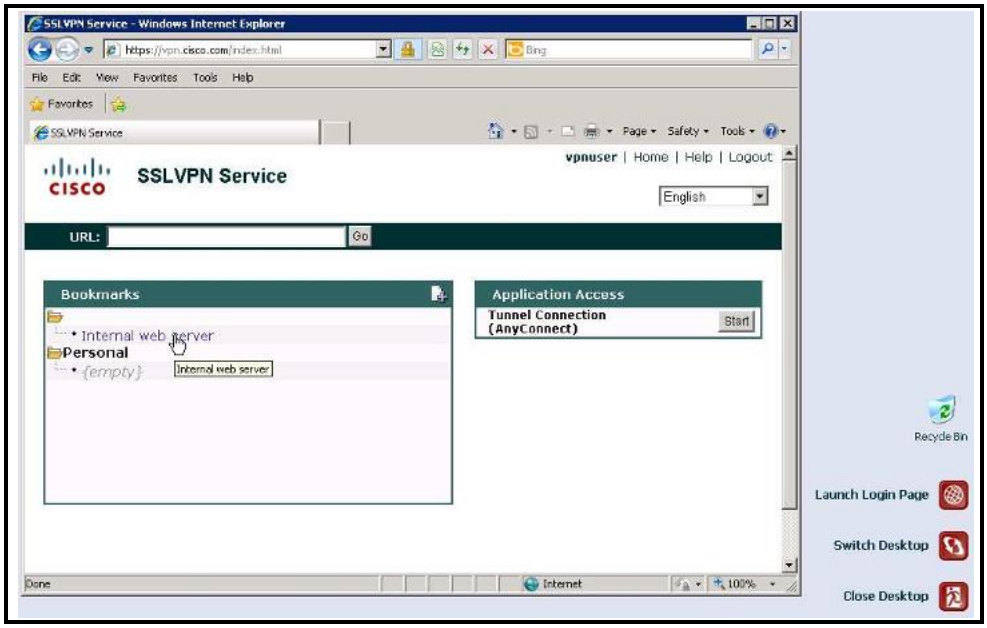



**Step 11** The Cisco Secure Desktop virtual desktop will start and will include a browser running inside the virtual environment. Log in to the VPN using your configured VPN username and password.

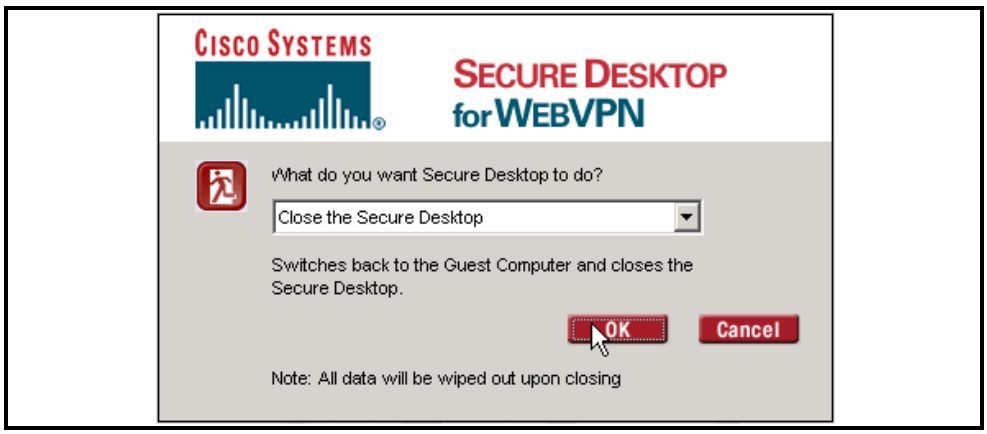



**Step 4** Check your connectivity to the internal web server using the configured bookmark. HTTP access to the server host should work.

 © 2010 Cisco Systems, Inc.




**Step 12** Click **Close Desktop** on the Cisco Secure Desktop virtual desktop and confirm your selection by clicking **OK**.




## Activity Verification

No additional verification is required for this task.

# Lab 4-2: Configuring Cisco Easy VPN

Complete this lab activity to practice what you learned in the related module.

## Activity Objective

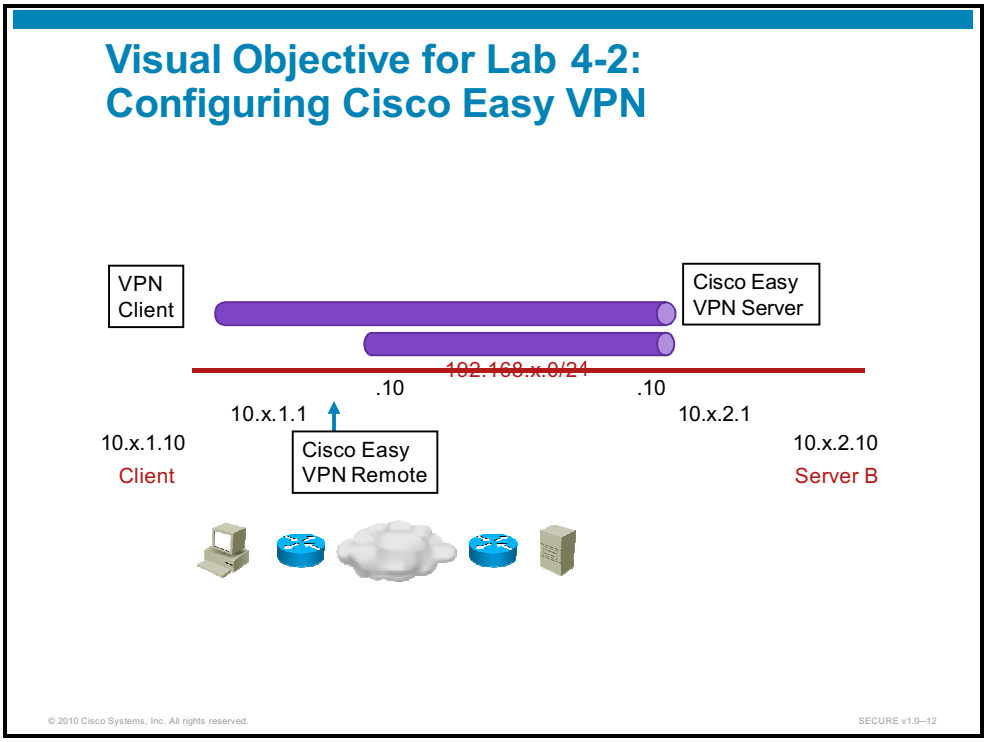
In this activity, you will configure the ISR-PxR2 router as a Cisco Easy VPN server and establish a remote access IPsec tunnel from the client PC to ISR-PxR2. In addition, you will also configure the ISR-PxR1 router as a Cisco Easy VPN Remote hardware client.

After completing this activity, you will be able to meet these objectives:

- Configure the Cisco Easy VPN server feature using VTIs and remote AAA
- Install and configure the Cisco VPN Client and establish a remote access IPsec VPN tunnel
- Configure a Cisco Easy VPN Remote device using VTIs

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Required Resources

These are the resources and equipment that are required to complete this activity:

- Student terminals (laptops, PCs)
- Pod ISR routers (ISR-PxR1 and ISR-PxR2)
- Pod client PC and Server B systems
- Shared backbone ISR-BB router

 © 2010 Cisco Systems, Inc.

# Command List

The table describes the commands that are used in this activity.

### Cisco IOS Commands

| Command | Description |
|---|---|
| **aaa authentication login {default \|** *list-name*} **{ method1 [method2...]}** | Sets AAA at login. |
| **aaa authorization network** | Sets parameters that restrict user access to a network and runs authorization for all network-related services. |
| **aaa new-model** | Enables the AAA access control mode. |
| acl *number* | Configures split tunneling in ISAKMP group configuration mode. |
| **auto-summary** | Allows automatic summarization of subnet routes into network-level routes. To disable this function and send subprefix routing information across classful network boundaries, use the no form of this command. |
| **banner** *string* | Configures a banner to be displayed after a successful login in WebVPN group policy. |
| **client authentication list** *list-name* | Configures IKE XAUTH in an ISAKMP profile. |
| **client configuration address {initiate \| respond}** | Configures IKE configuration mode in the ISAKMP profile. |
| **client configuration group** *group-name* | Associates a group with the peer that has been assigned an ISAKMP profile. |
| **copy tftp: flash:** | Copies file from TFTP server to flash. |
| **crypto ipsec client ezvpn** *name* | Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN remote configuration mode. |
| **crypto ipsec client ezvpn** *name* **[outside \| inside]** | Assigns a Cisco Easy VPN remote configuration to an interface other than a virtual interface, to specify whether the interface is outside or inside. |
| **crypto ipsec profile** *profile-name* | Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and to enter IPsec profile configuration mode. |
| **crypto ipsec transform-set t***ransform-set-name transform1* **[***transform2***] [***transform3***] [***transform4***]** | Defines a transform set—an acceptable combination of security protocols and algorithm. |
| **crypto isakmp client configuration group** *group-name* | Creates a named ISAKMP client configuration group. |
| **crypto isakmp profile** *profile-name* | Creates a named ISAKMP profile. |
| **default-group-policy** *name* | Associates a policy group with an SSL VPN context configuration in WebVPN context configuration mode. |
| **functions svc-enabled** | Enables full tunneling for a policy group. |
| **gateway** *webvpn-gateway-name* | Binds context to a gateway inside context configuration mode. |

| Command | Description |
|---|---|
| **group** *group-name* **key** *group-key* | Specifies the group name and key value for the VPN connection. |
| **inservice** | Enables an SSL VPN gateway or context process. |
| **interface virtual-template** *number* **type tunnel** | Creates a virtual template interface type tunnel and enters interface configuration mode. |
| **ip access-list extended** *access-list-name* | Defines an extended IP access list. |
| **ip address** *ip-address* **port** *port-number* | Configures a proxy IP address on an SSL VPN gateway and specifies the port number for proxy traffic. |
| **ip host** *hostname ip-address* | Defines static hostname-to-address mappings in the DNS hostname cache. |
| **ip local pool {default \|** *poolname***} [***low-ip-address* **[***high-ip-address***]]** | Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface. |
| **ip unnumbered** *type number* | Enables IP processing on an interface without assigning an explicit IP address to the interface. |
| **isakmp authorization list** *list-name* | Configures an IKE shared secret using the AAA server in an ISAKMP profile. |
| **key** *name* | Specifies the IKE PSK for group policy attribute definition in ISAKMP group configuration mode. |
| **logging enable** | Enables syslog logging of SSL VPN gateway-related messages. |
| **match identity group** *group-name* | Identifies the group name that the ISAKMP profile will select. |
| **mode client** | Specifies the VPN mode of operation of the router for the client, which automatically configures the router for Cisco Easy VPN client mode operation. |
| **network** *ip-address* **[***wildcard-mask***]** | Specifies the network for an EIGRP routing process. |
| **peer** *ip-address* | Sets the peer IP address for the VPN connection. |
| **permit** *source* **[***source-wildcard***] permit** *protocol source source-wildcard destination destination-wildcard* | Sets conditions to allow a packet to pass a named IP access list in access list configuration mode. |
| **ping** | Determines if other IP addresses are accessible. |
| **policy group** | Enters WebVPN group policy configuration mode to configure a group policy. |
| **pool** *name* | Defines a local pool address in ISAKMP group configuration mode. |
| **router eigrp** *autonomous-system-number* | Configures the EIGRP routing process. |
| **save-password** | Enables saving your XAUTH password locally on your PC or router in ISAKMP group configuration mode. |
| **set isakmp-profile** *profile-name* | Sets the ISAKMP profile name in IPsec profile configuration mode. |

 © 2010 Cisco Systems, Inc.

| Command | Description |
|---|---|
| **set transform-set** *transform-set-name* | Specifies which transform sets can be used with the IPsec profile. |
| **show crypto session username** *username* | Displays status information for active cryptography sessions for a specific username. |
| **show running-config** | Displays the configuration that is currently running on the adaptive security appliance. |
| **show webvpn session context** *context-name* | Displays SSL VPN user session information for the context. |
| **tunnel mode ipsec ipv4** | Sets the encapsulation mode for the tunnel interface to IPsec. |
| **tunnel protection ipsec profile** *profile-name* | Associates a tunnel interface with an IPsec profile and enables GRE encryption via IPsec. |
| **url-list** *name* | Enters WebVPN URL list configuration mode to configure a list of URLs to which a user has access on the portal page of an SSL VPN and to attach the URL list to a policy group. |
| **url-text {***name* **url-value** *url***}** | Adds an entry to a URL list in URL list configuration mode. |
| **username** *name* **privilege** *level* **password** *password* | Establishes a username-based authentication system with the privilege level specified. |
| **virtual-interface** *virtual-template-number* | Specifies a virtual interface for a Cisco Easy VPN remote device. |
| **virtual-template** *template-number* | Associates a group with the peer that has been assigned an ISAKMP profile. |
| **webvpn install [csd** *location-name* **\| svc** *location-name***]** | Installs a Cisco Secure Desktop or Cisco AnyConnect VPN Client package file to an SSL VPN gateway. |

# Job Aids

These job aids are available to help you complete the lab activity:

- The instructor will provide you with your pod number and other pod access information.

### Pod Access Information

| Parameter | Value |
|---|---|
| Pod number | |
| Terminal server IP address and port number | |
| Username on the Server B | Administrator |
| Password on the Server B | admin |
| Username on the client PC | Administrator |
| Password on the client PC | admin |

# Task 1: Configure the Cisco Easy VPN Server Feature Using VTIs and Remote AAA

In this task, you will configure the ISR-PxR2 router with basic VTI-based Cisco Easy VPN server features, including configuring the appropriate IKE and IPsec policies, dynamic VTIs, and IPsec profiles.

## Activity Procedure

Complete these steps:

**Step 1** Configure EIGRP on the ISR-PxR1 and ISR-PxR2 routers. The ISR-PxR1 router should advertise networks 192.168.x.0/24 and 10.x.1.0/24. ISR-PxR2 should only advertise the 192.168.x.0/24 network.

**Step 2** On the ISR-PxR2 router, configure a custom IPsec transform set that uses ESP encapsulation with the 128-bit AES and SHA-1 HMAC transforms.

**Step 3** On the ISR-PxR2 router, create an IPsec profile and associate it with the configured transform set.

**Step 4** On the ISR-PxR2 router, create a dynamic VTI template with the following properties:

- Use IP unnumbered addressing.
- Use IPsec tunnel encapsulation referencing the configured IPsec profile.

**Step 5** On the ISR-PxR2 router, create a client configuration group with the following properties:

- A group password of **cisco**.
- An address assignment pool using addresses from the 172.16.0.1–172.16.0.10 range.
- Split tunneling that protects traffic between clients and the 10.x.2.0/24 network.

**Step 6** On the ISR-PxR2 router, create an ISAKMP profile named MY-ISAKMP-PROFILE with the following settings:

- Associate the profile with the previously configured configuration group.
- A local user authentication method (XAUTH). Configure a local user account that will be able to log in to the VPN.
- A local authorization method.
- The ability to respond to address configuration requests.
- The ability to create virtual access interfaces that are based on the configured dynamic VTI template.

**Step 7** On the ISR-PxR2 router, associate the configured ISAKMP profile to the configured IPsec profile.

 © 2010 Cisco Systems, Inc.

# Task 2: Configure the Cisco VPN Client

In this task, you will configure the Cisco VPN Client and establish an IPsec remote access VPN tunnel between the Cisco VPN Client that is installed on the client PC and the Cisco Easy VPN server on the ISR-PxR2 router.

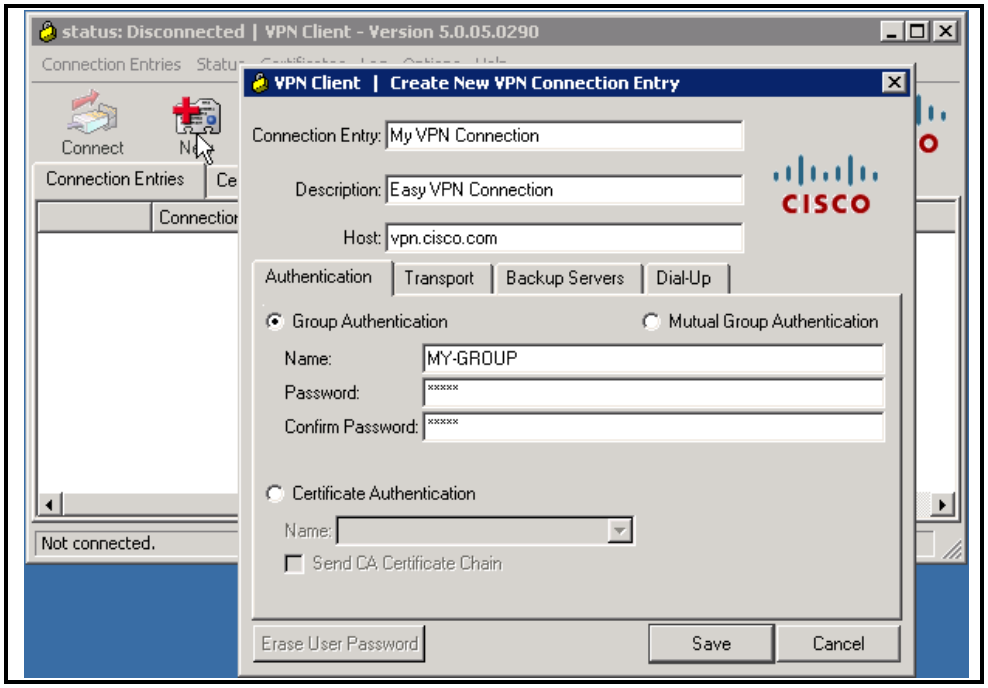
## Activity Procedure

Complete these steps:

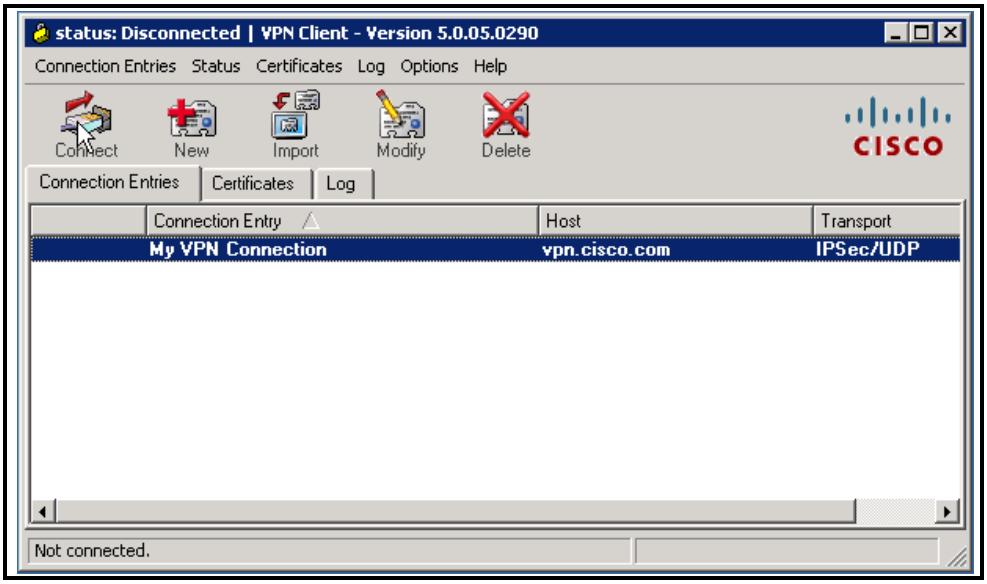
**Step 1** On the client PC, start the Cisco VPN Client by double-clicking its shortcut on the client PC desktop.

**Step 2** On the client PC, create a new VPN connection entry by clicking the **New** button in the Cisco VPN Client toolbar. Fill in all required profile information:

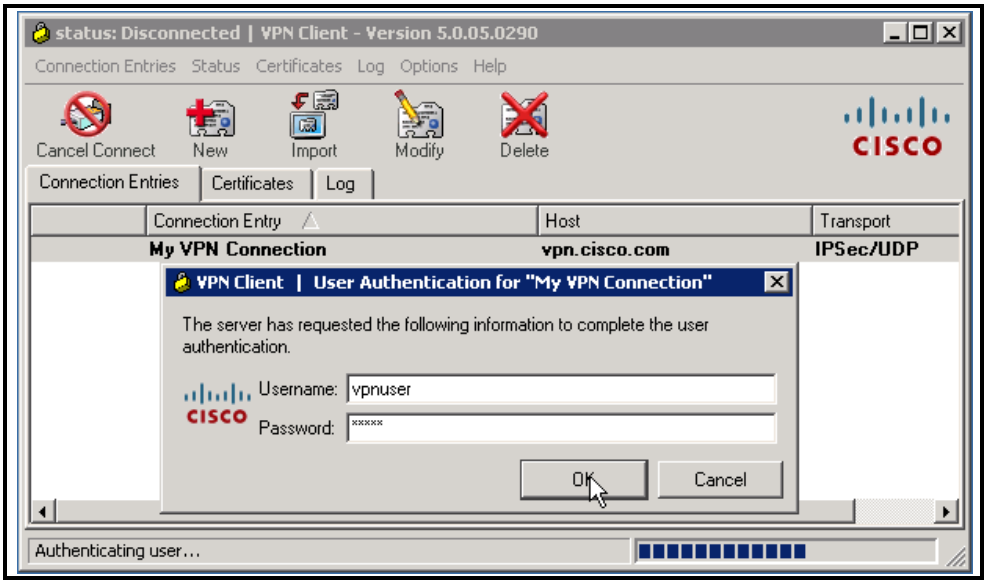
- The host with which the tunnel should be established is **vpn.cisco.com** (the ISR-PxR2 router).
- The group authentication name is the group name that you have specified in this task.
- The group authentication password is **cisco**.




**Step 3** On the client PC, in the Cisco VPN Client application, select the connection entry that you have created in the previous step. Click the **Connect** button in the toolbar to establish an IPsec tunnel between the client PC and the ISR-PxR2 router.




**Step 4** In the user authentication window, use the VPN username and password that you have configured on ISR-PxR2.



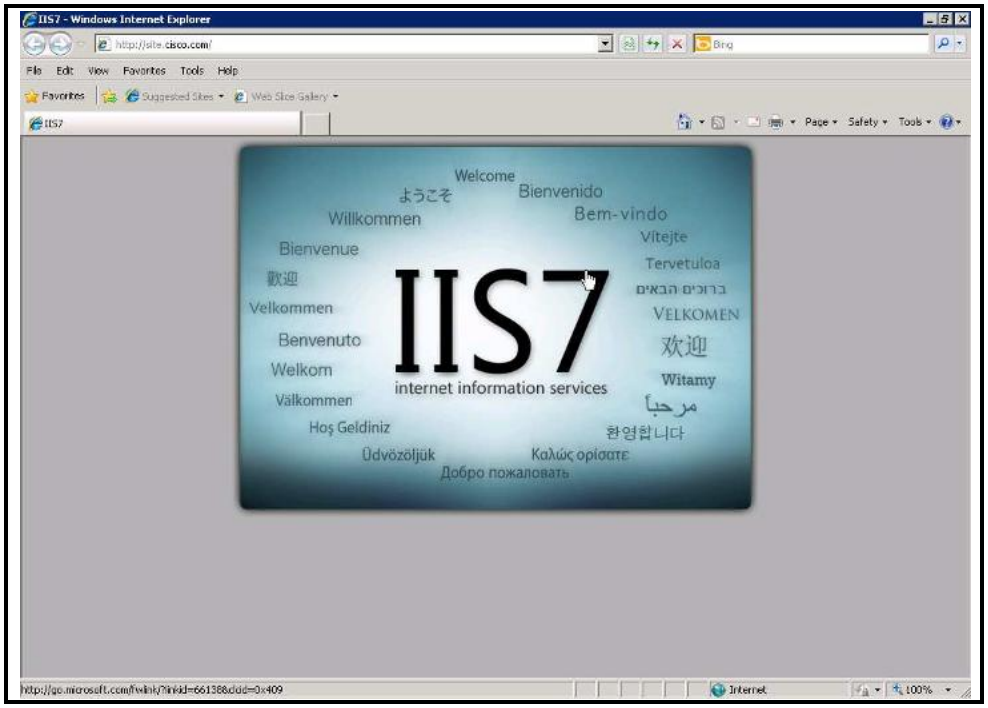

**Step 5** The IPsec tunnel should successfully establish, and the Cisco VPN Client icon should appear in the system tray.

## Activity Verification

You have completed this task when you attain these results:

- On the client PC, open a browser and navigate to the internal Server B system (**http://site.cisco.com**). Your connection over the VPN tunnel should succeed.

 © 2010 Cisco Systems, Inc.




- On the ISR-PxR2 router, verify the status of the remote access session for the configured username (vpnuser in this printout):

```
ISR-PxR2#show crypto session username vpnuser
Crypto session current status

Interface: Virtual-Access2
Username: vpnuser
Profile: MY-ISAKMP-PROFILE
Group: MY-GROUP
Assigned address: 172.16.0.2
Session status: UP-ACTIVE
Peer: 10.1.1.10 port 1049
  IKE SA: local 192.168.1.20/500 remote 10.1.1.10/1049 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 172.16.0.2
        Active SAs: 2, origin: crypto map
```

# Task 3: Configure a Cisco Easy VPN Remote Device Using VTI

In this task, you will configure the PxR1 router to act as a hardware Cisco Easy VPN Remote VPN Client, using minimal local configuration to connect to the VPN and enable the entire remote network to communicate with the central site network behind ISR-PxR2. You will configure the remote ISR-PxR1 router with authentication credentials and the IP address of its Easy VPN server (ISR-PxR2). The router will receive most of its network configuration from the Easy VPN server client configuration group settings.

## Activity Procedure

Complete these steps:

**Step 1** On the client PC, disconnect your Cisco VPN Client session by bringing up the Cisco VPN Client interface (double-click its tray icon), and clicking the **Disconnect** button.

**Step 2** On the ISR-PxR1 router, create a VTI template, and configure the template with IPsec tunneling mode.

**Step 3** On the ISR-PxR1 router, create an Easy VPN Remote connection profile with the following settings:

- Use the same group name and password that were used for the software Cisco VPN Client in the previous task.
- Use the configured VTI template to create a tunnel interface for the Easy VPN connection.
- Specify the IP address of ISR-PxR2 as the Easy VPN server.
- Specify that the client will use the Easy VPN Client mode when connecting to the Easy VPN server.
- Specify the VPN username and password (configured in the ISR-PxR2 local database) to additionally authenticate to the Easy VPN server.

**Step 4** On the ISR-PxR2 router, inside its VPN access policy, allow the saving of client XAUTH passwords locally on remote devices to fully automate the Easy VPN Remove device connection.

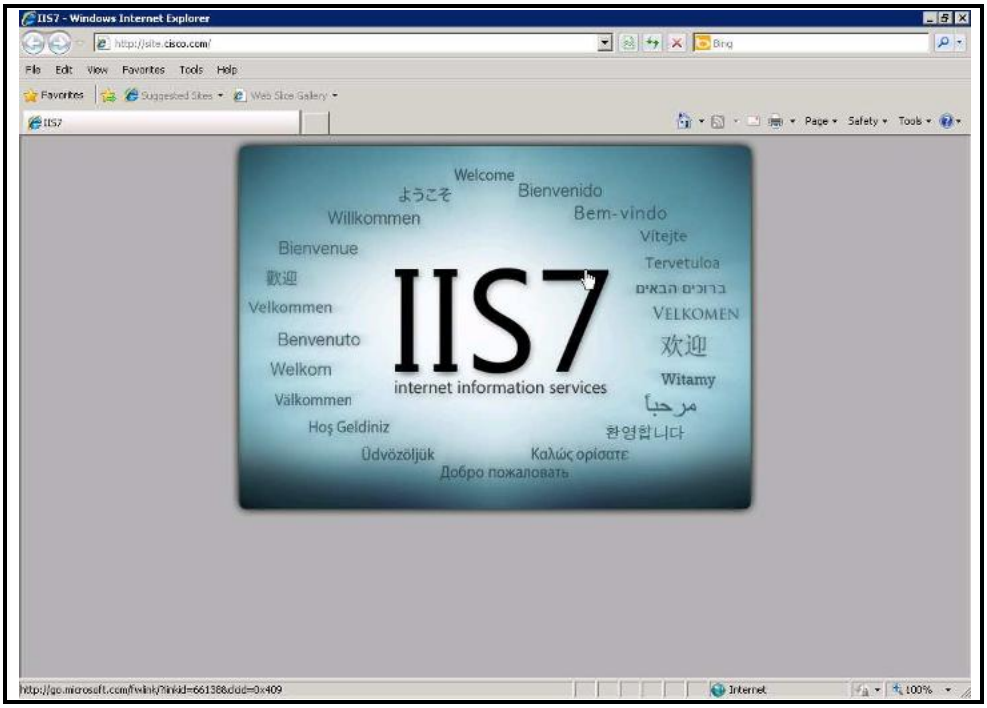
**Step 5** On the ISR-PxR1 router, designate the internal (trusted) interface (FastEthernet0/1) as the Cisco Easy VPN Remote "inside" interface.

**Step 6** On the ISR-PxR1 router, designate the external (untrusted) interface (FastEthernet0/0) as the Cisco Easy VPN Remote "outside" interface.

## Activity Verification

You have completed this task when you attain these results:

- Log in to the client PC again. On the client PC, open a browser and navigate to the internal Server B system (**http://site.cisco.com**). Your connection over the Cisco Easy VPN Remote VPN tunnel should succeed.




 © 2010 Cisco Systems, Inc.

- On the ISR-PxR2 router, verify the status of the Easy VPN Remote session for the configured username (vpnuser in this printout):

```
ISR-PxR2#show crypto session username vpnuser
Crypto session current status

Interface: Virtual-Access2
Username: vpnuser
Profile: MY-ISAKMP-PROFILE
Group: MY-GROUP
Assigned address: 172.16.0.6
Session status: UP-ACTIVE
Peer: 192.168.1.10 port 500
  IKE SA: local 192.168.1.20/500 remote 192.168.1.10/500
Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

# Answer Key

The correct answers and expected solutions for the activities that are described in this guide appear here.

## Lab 1-1 Answer Key: Configuring Advanced Switched Data Plane Security Controls

To complete this activity, configure the following tasks.

### Task 1: Verify DHCP Spoofing Vulnerability

No configuration commands are needed in this task.

### Task 2: Configure DHCP Snooping

Q1) What is your VLAN number?

Your VLAN number varies. Please enter it into the Job Aids table.

The following commands need to be configured on the switch:

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping database flash:/dhcp-
snooping.db
Switch(config)#ip dhcp snooping vlan 661
Switch(config)#interface fastethernet 0/1
Switch(config-if)#ip dhcp snooping trust
```

On the switch, verify DHCP snooping configuration:

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
661
DHCP snooping is operational on following VLANs:
661
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0017.0e6c.8e80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following
Interfaces:

Interface       Trusted    Allow option    Rate limit (pps)
-------------   -------    ------------    ----------------
FastEthernet0/1 yes        yes             unlimited
  Custom circuit-ids:
```

On the client PC, release and renew the IP address:

```
C:\Documents and Settings\Administrator>ipconfig /release
```

 © 2010 Cisco Systems, Inc.

```
Windows IP Configuration

Ethernet adapter LAB:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>ipconfig /renew

Windows IP Configuration

Ethernet adapter LAB:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.1.1.1
```

On the switch, verify the DHCP snooping binding database:

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress   Lease(sec) Type           VLAN Interface
------------------ ----------- ---------- ------------- ---- --------------------
00:0C:29:DA:86:EA  10.1.1.101  86228      dhcp-snooping 661  FastEthernet0/22
Total number of bindings: 1
```

## Task 3: Configure Dynamic and Static ARP Inspection

On the router, check the MAC address of the FastEthernet0/0 interface facing the switch:

```
Router#show interfaces fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 0017.5903.18f8 (bia 0017.5903.18f8)
  Internet address is 10.1.1.1 255.255.255.0
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:23, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     254 packets input, 31831 bytes
     Received 158 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     414 packets output, 43851 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     67 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following commands need to be configured on the switch:

```
Switch(config)#arp access-list STATIC
Switch(config-arp-nacl)#permit ip host 10.1.1.1 mac host
0017.5903.18f8
Switch(config-arp-nacl)#exit
Switch(config)#ip arp inspection filter STATIC vlan 661
Switch(config)#ip arp inspection vlan 661
```

The following commands need to be configured on the switch:

```
Switch(config)#no ip arp inspection vlan 661
```

## Task 4: Configure IP Source Guard and Port Access Lists

From the client PC, ping the server at 10.1.1.11 before enabling the IP Source Guard feature:

```
C:\Documents and Settings\Administrator>ping 10.1.1.11

Pinging 10.1.1.11 with 32 bytes of data:

Reply from 10.1.1.11: bytes=32 time=1ms TTL=128
Reply from 10.1.1.11: bytes=32 time=1ms TTL=128
Reply from 10.1.1.11: bytes=32 time<1ms TTL=128
Reply from 10.1.1.11: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

The following commands need to be configured on the switch:

```
Switch(config)#interface fastethernet 0/22
Switch(config-if)#ip verify source port-security
```

Ping the server at 10.1.1.11 again after enabling the IP Source Guard feature and changing its IP address:

```
C:\Documents and Settings\Administrator>ping 10.1.1.11

Pinging 10.1.1.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

On the switch, verify the current source address mappings and IP Source Guard-enabled ports:

```
Switch#show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/22     ip-mac       active       10.1.1.101       permit-all         661
```

The following commands need to be configured on the switch:

```
Switch(config)#interface fastethernet 0/22
Switch(config-if)#no ip verify source port-security
```

 © 2010 Cisco Systems, Inc.

From the server, ping the router at 10.1.1.1 before enabling the static IP Source Guard rule:

```
C:\Windows\system32>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Reply from 10.1.1.1: bytes=32 time=2ms TTL=128
Reply from 10.1.1.1: bytes=32 time=1ms TTL=128
Reply from 10.1.1.1: bytes=32 time=1ms TTL=128
Reply from 10.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.116:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

The following commands need to be configured on the switch:

```
Switch(config)#ip access-list standard PACL
Switch(config-std-nacl)#permit 10.1.1.11
Switch(config-std-nacl)#exit
Switch(config)#interface fastethernet 0/23
Switch(config-if)#ip access-group PACL in
Switch(config-if)#no ip access-group PACL in
```

From the server, ping the router at 10.1.1.1 again after enabling the port access control list:

```
C:\Windows\system32>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The following commands need to be configured on the switch:

```
Switch(config)#interface fastethernet 0/23
Switch(config-if)#no ip access-group PACL in
```

## Task 5: Configure PVLAN Edge

From the server, ping the router at 10.1.1.1 before enabling the PVLAN Edge feature:

```
C:\Windows\system32>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Reply from 10.1.1.1: bytes=32 time=2ms TTL=128
Reply from 10.1.1.1: bytes=32 time=1ms TTL=128
Reply from 10.1.1.1: bytes=32 time=1ms TTL=128
Reply from 10.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

The following commands need to be configured on the switch:

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport protected
Switch(config)#interface fastethernet 0/23
Switch(config-if)#switchport protected
```

On the switch, verify that the FastEthernet0/1 and FastEthernet0/23 interfaces are configured as protected ports:

```
Switch#show interfaces fastethernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled

<...part of the output omitted...>

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Switch#show interfaces FastEthernet 0/23 switchport
Name: Fa0/23
Switchport: Enabled

<...part of the output omitted...>

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

From the server, ping the router at 10.1.1.1 after enabling PVLAN Edge feature:

```
C:\Windows\system32>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The following commands need to be configured on the switch:

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#no switchport protected
Switch(config)#interface fastethernet 0/23
```

 © 2010 Cisco Systems, Inc.

```
Switch(config-if)#no switchport protected
```

# Lab 1-2 Answer Key: Configuring Advanced Infrastructure Security Controls

To complete this activity, configure the following tasks.

## Task 1: Configure Control Plane Protection

The following commands are needed on ISR-PxR1:

```
ISR-PxR1(config)#ip access-list extended CPPR-SNMP
ISR-PxR1(config-ext-nacl)#permit udp any any eq snmp
ISR-PxR1(config-ext-nacl)#exit
ISR-PxR1(config)#class-map CPPR-SNMP-CLASS
ISR-PxR1(config-cmap)#match access-group name CPPR-SNMP
ISR-PxR1(config)#policy-map CPPR-POLICY
ISR-PxR1(config-pmap)#class CPPR-SNMP-CLASS
ISR-PxR1(config-pmap-c)#police rate 200 pps conform-action
transmit exceed-action drop
ISR-PxR1(config)#control-plane host
ISR-PxR1(config-cp-host)#service-policy input CPPR-POLICY
01:00:31: %CP-5-FEATURE: Control-plane Policing feature
enabled on Control plane host path
```

## Task 2: Configure Management Plane Protection

The following commands are needed on ISR-PxR2:

```
ISR-PxR2(config)#control-plane host
ISR-PxR2(config-cp-host)# management-interface FastEthernet
0/1 allow telnet ssh
```

## Task 3: Configure Unicast Reverse Path Forwarding

The following commands are needed on ISR-PxR2:

```
ISR-PxR2(config)#control-plane host
ISR-PxR2(config-cp-host)# no management-interface FastEthernet
0/1 allow telnet ssh
```

The following commands are needed on ISR-PxR1:

```
ISR-PxR1(config)#ip cef
ISR-PxR1(config)#access-list 199 deny ip any any log-input
ISR-PxR1(config)#interface fastEthernet 0/0
ISR-PxR1(config-if)#ip verify unicast source reachable-via rx
allow-self-ping 199
```

The following commands are needed on ISR-PxR2:

```
ISR-PxR2(config)#interface loopback 0
ISR-PxR2(config-if)#ip address 10.1.1.11 255.255.255.255
```

## Task 4: Configure FPM

The following commands are needed on ISR-PxR2:

```
ISR-PxR2(config)#no interface loopback 0
```

The following commands are needed on the PxR1 router:

```
ISR-PxR1#copy tftp://10.1.1.10/tcp.phdf flash:
Destination filename [tcp.phdf]?
Accessing tftp://10.1.1.10/tcp.phdf...
Loading tcp.phdf from 10.1.1.10 (via FastEthernet0/1): !

ISR-PxR1#copy tftp://10.1.1.10/ip.phdf flash:
Destination filename [ip.phdf]?
Accessing tftp://10.1.1.10/tcp.phdf...
Loading tcp.phdf from 10.1.1.10 (via FastEthernet0/1): !

ISR-PxR1(config)#load protocol flash:ip.phdf
ISR-PxR1(config)#load protocol flash:tcp.phdf
ISR-PxR1(config)#class-map type stack match-all IP-TCP
ISR-PxR1(config-cmap)#match field ip protocol eq 0x6 next tcp
ISR-PxR1(config-cmap)#exit
ISR-PxR1(config)#class-map type access-control match-all HTTP-
WORM-CLASS
ISR-PxR1(config-cmap)#match field tcp dest-port eq 80
ISR-PxR1(config-cmap)#match start tcp payload-start offset 0
size 256 string "cmd.exe"
ISR-PxR1(config-cmap)#exit
ISR-PxR1(config)#policy-map type access-control HTTP-WORM-
POLICY
ISR-PxR1(config-pmap)#class HTTP-WORM-CLASS
ISR-PxR1(config-pmap-c)#drop
ISR-PxR1(config-pmap-c)#exit
ISR-PxR1(config-pmap)#exit
ISR-PxR1(config)#policy-map type access-control WAN-POLICY
ISR-PxR1(config-pmap)#class IP-TCP
ISR-PxR1(config-pmap-c)#service-policy HTTP-WORM-POLICY
ISR-PxR1(config-pmap-c)#exit
ISR-PxR1(config-pmap)#exit
ISR-PxR1(config)#interface FastEthernet 0/1
ISR-PxR1(config-if)#service-policy type access-control input
WAN-POLICY
```

## Task 5: Configure Flexible NetFlow

The following commands are needed on the PxR1 router:

```
ISR-PxR1(config)#flow exporter MYEXPORTER
ISR-PxR1(config-flow-exporter)#destination 10.1.1.10
ISR-PxR1(config-flow-exporter)#transport udp 9996
ISR-PxR1(config-flow-exporter)#export-protocol netflow-v5
ISR-PxR1(config-flow-exporter)#exit
ISR-PxR1(config)#flow monitor MYMONITOR
ISR-PxR1(config-flow-monitor)#record netflow ipv4 original-
input
ISR-PxR1(config-flow-monitor)#exporter MYEXPORTER
ISR-PxR1(config-flow-monitor)#exit
```

 © 2010 Cisco Systems, Inc.

```
ISR-PxR1(config)#interface FastEthernet 0/1
ISR-PxR1(config-if)#ip flow monitor MYMONITOR input
```

# Lab 2-1 Answer Key: Configuring Basic Zone-Based Policy Firewall Features

To complete this activity, configure the following tasks.

## Task 1: Configure Zones

The following commands are needed on PxR2 router:

```
ISR-PxR2(config)#zone security INSIDE
ISR-PxR2(config-sec-zone)#exit
ISR-PxR2(config)#zone security DMZ
ISR-PxR2(config-sec-zone)#exit
ISR-PxR2(config)#zone security OUTSIDE
ISR-PxR2(config-sec-zone)#exit
ISR-PxR2(config)#int FastEthernet 0/0
ISR-PxR2(config-if)#zone-member security OUTSIDE
ISR-PxR2(config-if)#exit
ISR-PxR2(config)#interface FastEthernet 0/1.1
ISR-PxR2(config-subif)#zone-member security INSIDE
ISR-PxR2(config-subif)#exit
ISR-PxR2(config)#interface FastEthernet 0/1.2
ISR-PxR2(config-subif)#zone-member security DMZ
ISR-PxR2(config-subif)#exit
ISR-PxR2(config)#zone-pair security IN-TO-OUT source INSIDE
destination OUTSIDE
ISR-PxR2(config-sec-zone-pair)#exit
ISR-PxR2(config)#zone-pair security OUT-TO-IN source OUTSIDE
destination INSIDE
ISR-PxR2(config-sec-zone-pair)#exit
ISR-PxR2(config)#zone-pair security OUT-TO-DMZ source OUTSIDE
destination DMZ
ISR-PxR2(config-sec-zone-pair)#exit
```

## Task 2: Configure Access Control Between the INSIDE and OUTSIDE Zones

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#ip access-list extended IN-TO-OUT-ACL
ISR-PxR2(config-ext-nacl)#permit tcp 10.1.1.0 0.0.0.255 any eq
www
ISR-PxR2(config-ext-nacl)#permit icmp 10.1.1.0 0.0.0.255 any
echo
ISR-PxR2(config)#ip access-list extended OUT-TO-IN-ACL-ICMP
ISR-PxR2(config-ext-nacl)#permit icmp any 10.1.1.0 0.0.0.255
unreachable
ISR-PxR2(config)#class-map type inspect OUT-TO-IN-CLASS-ICMP
ISR-PxR2(config-cmap)#match access-group name OUT-TO-IN-ACL-
ICMP
ISR-PxR2(config-cmap)#exit
ISR-PxR2(config)#class-map type inspect IN-TO-OUT-CLASS
```

```
ISR-PxR2(config-cmap)#match access-group name IN-TO-OUT-ACL
ISR-PxR2(config)#policy-map type inspect IN-TO-OUT-POLICY
ISR-PxR2(config-pmap)#class type inspect IN-TO-OUT-CLASS
ISR-PxR2(config-pmap-c)#inspect
ISR-PxR2(config-pmap-c)#exit
ISR-PxR2(config-pmap)#class class-default
ISR-PxR2(config-pmap-c)#drop log
ISR-PxR2(config-pmap-c)#exit
ISR-PxR2(config-pmap)#exit
ISR-PxR2(config)#policy-map type inspect OUT-TO-IN-POLICY
ISR-PxR2(config-pmap)#class type inspect OUT-TO-IN-CLASS-ICMP
ISR-PxR2(config-pmap-c)#pass
ISR-PxR2(config-pmap-c)#class class-default
ISR-PxR2(config-pmap-c)#drop log
ISR-PxR2(config-pmap-c)#exit
ISR-PxR2(config-pmap)#
ISR-PxR2(config)#zone-pair security IN-TO-OUT source INSIDE
destination OUTSIDE
ISR-PxR2(config-sec-zone-pair)#service-policy type inspect IN-
TO-OUT-POLICY
ISR-PxR2(config-sec-zone-pair)#exit
ISR-PxR2(config)#zone-pair security OUT-TO-IN source OUTSIDE
destination INSIDE
ISR-PxR2(config-sec-zone-pair)#service-policy type inspect
OUT-TO-IN-POLICY
```

## Task 3: Configure Access Control Between the OUTSIDE and DMZ Zones

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#ip access-list extended OUT-TO-DMZ-ACL
ISR-PxR2(config-ext-nacl)#permit tcp any host 10.1.2.10 eq ftp
ISR-PxR2(config-ext-nacl)#exit
ISR-PxR2(config)#class-map type inspect OUT-TO-DMZ-CLASS
ISR-PxR2(config-cmap)#match access-group name OUT-TO-DMZ-ACL
ISR-PxR2(config-cmap)#exit
ISR-PxR2(config)#policy-map type inspect OUT-TO-DMZ-POLICY
ISR-PxR2(config-pmap)#class type inspect OUT-TO-DMZ-CLASS
ISR-PxR2(config-pmap-c)#inspect
ISR-PxR2(config-pmap-c)#exit
ISR-PxR2(config-pmap)#class class-default
ISR-PxR2(config-pmap-c)#drop log
ISR-PxR2(config-pmap-c)#exit
ISR-PxR2(config-pmap)#exit
ISR-PxR2(config)#$zone-pair security OUT-TO-DMZ source OUTSIDE
destination DMZ
ISR-PxR2(config-sec-zone-pair)#service-policy type inspect
OUT-TO-DMZ-POLICY
```

 © 2010 Cisco Systems, Inc.

## Task 4: Configure Inspection of Local Traffic

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#router eigrp 200
ISR-PxR2(config-router)#passive-interface FastEthernet 0/1.1
ISR-PxR2(config)#ip access-list extended IN-TO-SELF-ACL
ISR-PxR2(config-ext-nacl)#permit icmp 10.1.1.0 0.0.0.255 any
echo
ISR-PxR2(config-ext-nacl)#permit tcp 10.1.1.0 0.0.0.255 any eq
telnet
ISR-PxR2(config-ext-nacl)#exit
ISR-PxR2(config)#class-map type inspect IN-TO-SELF-CLASS
ISR-PxR2(config-cmap)#match access-group name IN-TO-SELF-ACL
ISR-PxR2(config-cmap)#exit
ISR-PxR2(config)#policy-map type inspect IN-TO-SELF-POLICY
ISR-PxR2(config-pmap)#class type inspect IN-TO-SELF-CLASS
ISR-PxR2(config-pmap-c)#inspect
ISR-PxR2(config-pmap-c)#exit
ISR-PxR2(config-pmap)#class class-default
ISR-PxR2(config-pmap-c)#drop log
ISR-PxR2(config-pmap-c)#exit
ISR-PxR2(config-pmap)#exit
ISR-PxR2(config)#zone-pair security IN-TO-SELF source INSIDE
destination self
ISR-PxR2(config-sec-zone-pair)#service-policy type inspect IN-
TO-SELF-POLICY
```

When you complete the lab, your configuration will be like the results here, with differences that are specific to your workgroup:

```
version 15.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ISR-PxR2
!
boot-start-marker
boot system usbflash0:c2800nm-advsecurityk9-mz.150-1.M1.bin
boot-end-marker
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
license udi pid CISCO2811 sn FCZ100770VQ
username admin privilege 15 password 0 adminpass
!
redundancy
!
!
ip tcp synwait-time 5
!
```

```
class-map type inspect match-all OUT-TO-IN-CLASS-ICMP
 match access-group name OUT-TO-IN-ACL-ICMP
class-map type inspect match-all IN-TO-OUT-CLASS
 match access-group name IN-TO-OUT-ACL
 match protocol http
class-map type inspect match-all IN-TO-SELF-CLASS
 match access-group name IN-TO-SELF-ACL
class-map type inspect match-all SELF-TO-IN-CLASS
 match access-group name SELF-TO-IN-ACL
class-map type inspect match-all OUT-TO-DMZ-CLASS
 match access-group name OUT-TO-DMZ-ACL
 match protocol ftp
!
!
policy-map type inspect OUT-TO-DMZ-POLICY
 class type inspect OUT-TO-DMZ-CLASS
  inspect
 class class-default
  drop log
policy-map type inspect IN-TO-SELF-POLICY
 class type inspect IN-TO-SELF-CLASS
  inspect
 class class-default
  drop log
policy-map type inspect IN-TO-OUT-POLICY
 class type inspect IN-TO-OUT-CLASS
  inspect
 class class-default
  drop log
policy-map type inspect OUT-TO-IN-POLICY
 class type inspect OUT-TO-IN-CLASS-ICMP
  pass
class class-default
  drop log
!
zone security INSIDE
zone security DMZ
zone security OUTSIDE
zone-pair security OUT-TO-DMZ source OUTSIDE destination DMZ
 service-policy type inspect OUT-TO-DMZ-POLICY
zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE
 service-policy type inspect IN-TO-OUT-POLICY
zone-pair security OUT-TO-IN source OUTSIDE destination INSIDE
 service-policy type inspect OUT-TO-IN-POLICY
zone-pair security IN-TO-SELF source INSIDE destination self
 service-policy type inspect IN-TO-SELF-POLICY
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.10 255.255.255.0
 zone-member security OUTSIDE
 duplex auto
 speed auto
 !
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 !
!
interface FastEthernet0/1.1
 encapsulation dot1Q 511
```

 © 2010 Cisco Systems, Inc.

```
 ip address 10.1.1.1 255.255.255.0
 zone-member security INSIDE
!
interface FastEthernet0/1.2
 encapsulation dot1Q 513
 ip address 10.1.2.1 255.255.255.0
 zone-member security DMZ
!
interface Serial0/0/0
 no ip address
 shutdown
 !
!
interface Serial0/1/0
 no ip address
 shutdown
 !
!
interface Serial0/1/1
 no ip address
 shutdown
 !
!
!
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 10.1.2.0 0.0.0.255
 network 192.168.1.0
 passive-interface FastEthernet0/1.1
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
ip access-list extended IN-TO-OUT-ACL
 permit tcp 10.1.1.0 0.0.0.255 any eq www
 permit icmp 10.1.1.0 0.0.0.255 any echo
ip access-list extended IN-TO-SELF-ACL
 permit icmp 10.1.1.0 0.0.0.255 any echo
 permit tcp 10.1.1.0 0.0.0.255 any eq 22
ip access-list extended OUT-TO-DMZ-ACL
 permit tcp any host 10.1.2.10 eq ftp
ip access-list extended OUT-TO-IN-ACL-ICMP
 permit icmp any 10.1.1.0 0.0.0.255 unreachable
!
control-plane
 !
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 ip netmask-format decimal
line aux 0
line vty 0 4
 privilege level 15
 logging synchronous
 login local
!
no scheduler allocate
end
```

# Lab 2-2 Answer Key: Configuring Advanced Zone-Based Policy Firewall Features

To complete this activity, configure the following tasks.

## Task 1: Configure Application-Layer Filtering on the Zone-Based Policy Firewall

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#ip access-list extended OUT-TO-DMZ-ACL
ISR-PxR2(config-ext-nacl)#no permit tcp any host 10.1.2.10 eq
ftp
ISR-PxR2(config-ext-nacl)#permit tcp any host 10.1.2.10 eq www
ISR-PxR2(config-ext-nacl)#exit
ISR-PxR2(config)#class-map type inspect match-all OUT-TO-DMZ-
CLASS
ISR-PxR2(config-cmap)#no match protocol ftp
ISR-PxR2(config-cmap)#match protocol http
ISR-PxR2(config-cmap)#end
ISR-PxR2#
ISR-PxR2(config)#parameter-map type regex CMD-REGEX
ISR-PxR2(config-profile)#pattern [cC][mM][dD]\.[eE][xX][eE]
ISR-PxR2(config-profile)#exit
ISR-PxR2(config)#class-map type inspect http match-any OUT-TO-
DMZ-APPLICATION-CLASS
ISR-PxR2(config-cmap)#match request arg regex CMD-REGEX
ISR-PxR2(config-cmap)#match req-resp protocol-violation
ISR-PxR2(config)#policy-map type inspect http OUT-TO-DMZ-
APPLICATION-POLICY
ISR-PxR2(config-pmap)#class type inspect http OUT-TO-DMZ-
APPLICATION-CLASS
ISR-PxR2(config-pmap-c)#log
ISR-PxR2(config-pmap-c)#reset
ISR-PxR2(config)#policy-map type inspect OUT-TO-DMZ-POLICY
ISR-PxR2(config-pmap)#class type inspect OUT-TO-DMZ-CLASS
ISR-PxR2(config-pmap-c)#service-policy http OUT-TO-DMZ-
APPLICATION-POLICY
```

## Task 2: Configure URL Filtering

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#parameter-map type urlf-glob BAD-KEYWORD
ISR-PxR2(config-profile)#pattern gambling
ISR-PxR2(config-profile)#exit
ISR-PxR2(config)#class-map type urlfilter BAD-KEYWORD-CLASS
ISR-PxR2(config-cmap)#match url-keyword urlf-glob BAD-KEYWORD
ISR-PxR2(config-cmap)#exit
ISR-PxR2(config)#policy-map type inspect urlfilter URL-POLICY
ISR-PxR2(config-pmap)#class type urlfilter BAD-KEYWORD-CLASS
ISR-PxR2(config-pmap-c)#reset
ISR-PxR2(config)#policy-map type inspect IN-TO-OUT-POLICY
ISR-PxR2(config-pmap)#class type inspect IN-TO-OUT-CLASS
```

 © 2010 Cisco Systems, Inc.

```
ISR-PxR2(config-pmap-c)#service-policy urlfilter URL-POLICY
ISR-PxR2(config-pmap-c)#exit
ISR-PxR2(config-pmap)#exit
```

### Task 3: Configure User-Based Firewalling

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#aaa new-model
ISR-PxR2(config)#aaa authentication login default local
ISR-PxR2(config)#aaa authorization auth-proxy default local
ISR-PxR2(config)#aaa attribute list MY-ATTRS
ISR-PxR2(config-attr-list)#attribute type supplicant-group
"ENGINEERING"
ISR-PxR2(config-attr-list)#exit
ISR-PxR2(config)#username enguser privilege 15 password
engineer
ISR-PxR2(config)#username enguser aaa attribute list MY-ATTRS
ISR-PxR2(config)#ip admission name MY-USER-FW proxy telnet
inactivity-time 60
ISR-PxR2(config)#ip admission name MY-USER-FW proxy ftp
inactivity-time 60
ISR-PxR2(config)#interface FastEthernet 0/0
ISR-PxR2(config-if)#ip admission MY-USER-FW
ISR-PxR2(config)#class-map type inspect match-all OUT-TO-DMZ-
CLASS
ISR-PxR2(config-cmap)#match user-group ENGINEERING
ISR-PxR2(config-cmap)#exit
```

## Lab 2-3 Answer Key: Configuring Cisco IOS Software IPS

To complete this activity, configure the following tasks.

### Task 1: Initialize Cisco IOS Software IPS and Configure IPS Policy

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#crypto key pubkey-chain rsa
ISR-PxR2(config-pubkey-chain)# named-key realm-cisco.pub
signature
ISR-PxR2(config-pubkey-key)#  key-string
Enter a public key as a hexidecimal number ....
ISR-PxR2(config-pubkey)#$70D0101 01050003 82010F00 3082010A
02820101
ISR-PxR2(config-pubkey)#$097A975 206BE3A2 06FBA13F 6F12CB5B
4E441F16
ISR-PxR2(config-pubkey)#$7FDD9C8 11FC7AF7 DCDD81D9 43CDABC3
6007D128
ISR-PxR2(config-pubkey)#$59C189E F30AF10A C0EFB624 7E0764BF
3E53053E
ISR-PxR2(config-pubkey)#$ED7A5B8 9479039D 20F30663 9AC64B93
C0112A35
ISR-PxR2(config-pubkey)#$A9E481D F65875D6 85EAF974 6D9CC8E3
F0B08B85
ISR-PxR2(config-pubkey)#$C189CB9 69C46F9C A84DFBA5 7A0AF99E
AD768C36
```

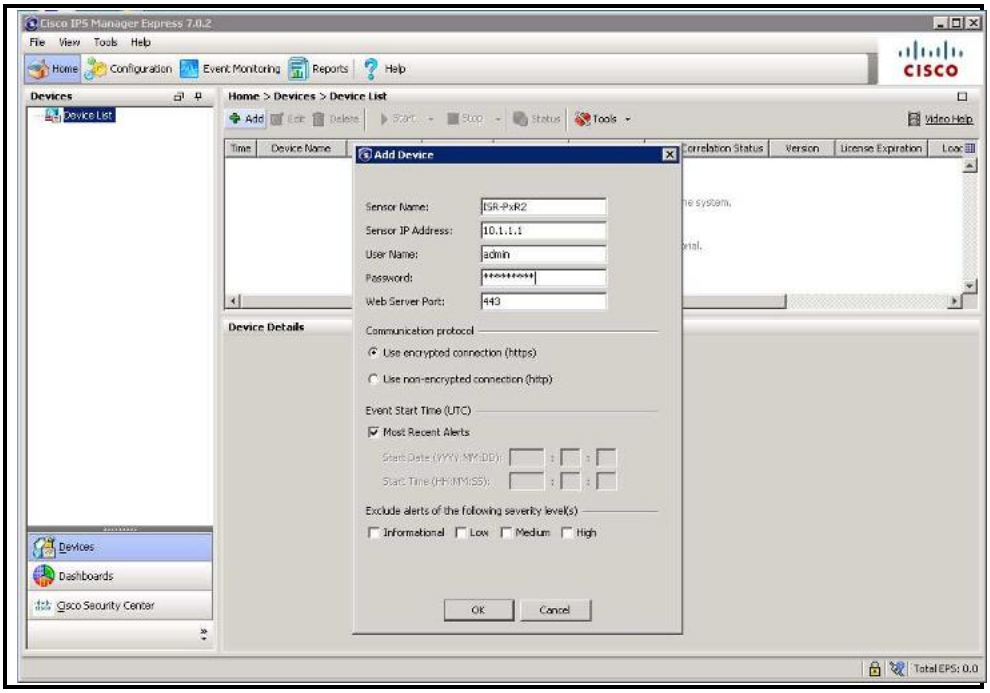
```
ISR-PxR2(config-pubkey)#$FB7B3CB 5539E1D1 9693CCBB 551F78D2
892356AE
ISR-PxR2(config-pubkey)#$7BFCA3B BFF668E9 689782A5 CF31CB6E
B4B094D3
ISR-PxR2(config-pubkey)#   F3020301 0001
ISR-PxR2(config-pubkey)# quit
ISR-PxR2(config-pubkey-key)# exit
ISR-PxR2(config-pubkey-chain)# exit
ISR-PxR2#mkdir iosips
Create directory filename [iosips]?
Created dir flash:iosips
ISR-PxR2(config)#ip ips config location flash:/iosips
ISR-PxR2(config)#ip ips name MY-IPS
ISR-PxR2(config)#interface FastEthernet 0/0
ISR-PxR2(config-if)#ip ips MY-IPS in
ISR-PxR2(config-if)#ip ips MY-IPS out
ISR-PxR2(config-if)#end
ISR-PxR2# copy ftp://anonymous:anonymous@10.1.1.10/SECURE/IOS-
S480-CLI.pkg idconf
```

## Task 2: Prepare the Cisco IME and Cisco Configuration Professional Software

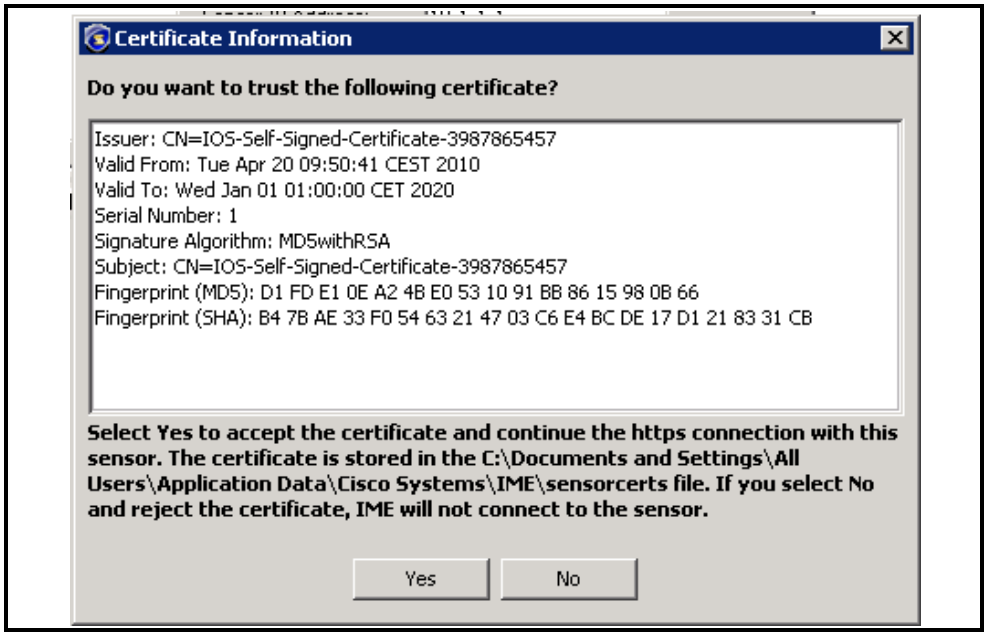
The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#ip ips notify sdee
ISR-PxR2(config)#ip http server
```

Add the router as a sensor in Cisco IME.




 © 2010 Cisco Systems, Inc.

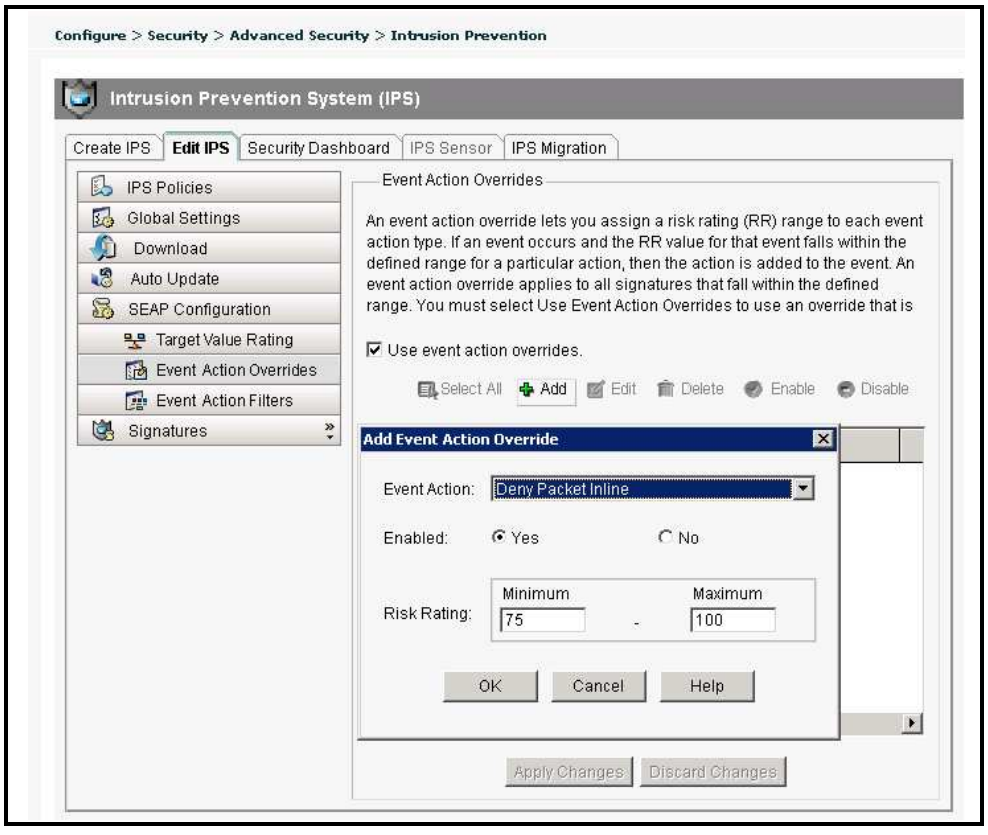



Click **Yes** to trust the router certificate.

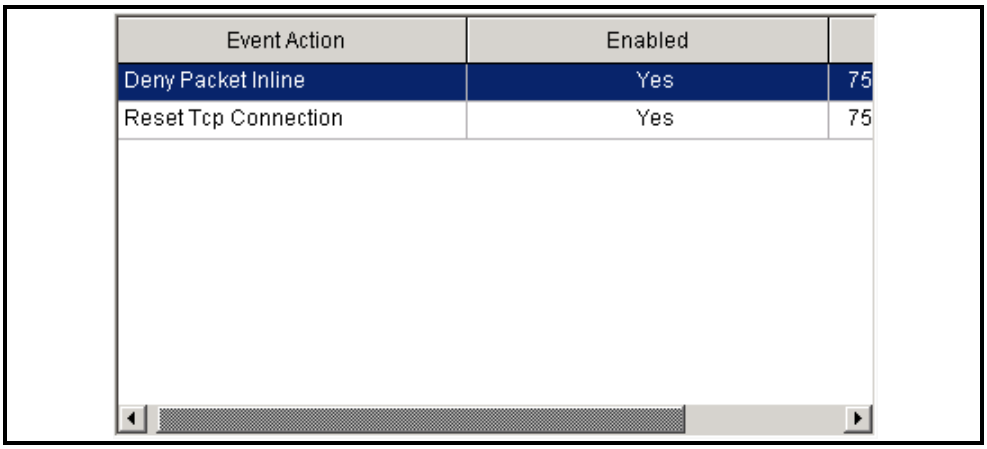
## Task 3: Tune the Cisco IOS Software IPS Policy Using SEAP

On Server A, inside the Cisco Configuration Professional application, navigate to **Configure > Security > Advanced Security > Intrusion Prevention > Edit IPS > SEAP Configuration > Event Action Overrides.**

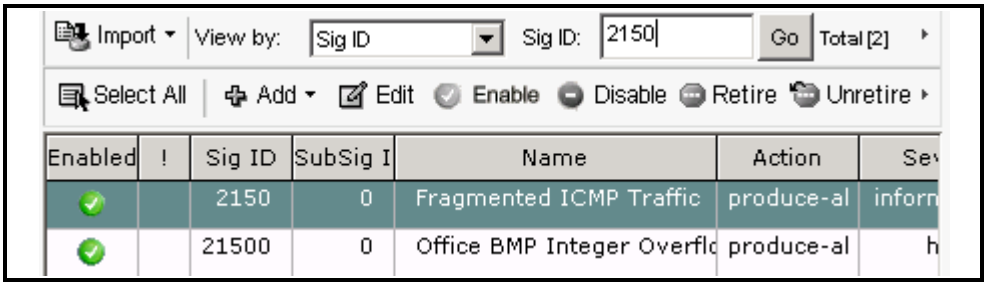
Add the **Deny packet inline** and **Reset TCP connection** actions for events in which the event-risk rating exceeds 75 by clicking the **Add** button. Then, select **Apply changes**.



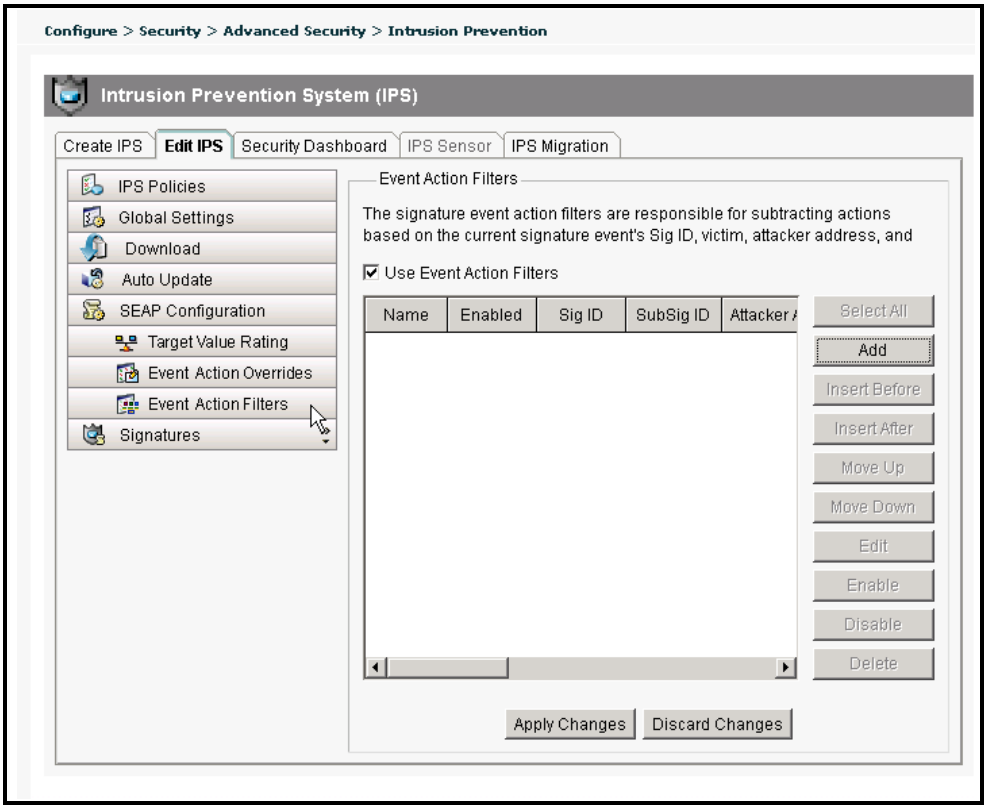
This is the resulting Event Action Overrides rule window.




On Server A, inside the Cisco Configuration Professional application, enable the Fragmented ICMP Traffic signature.

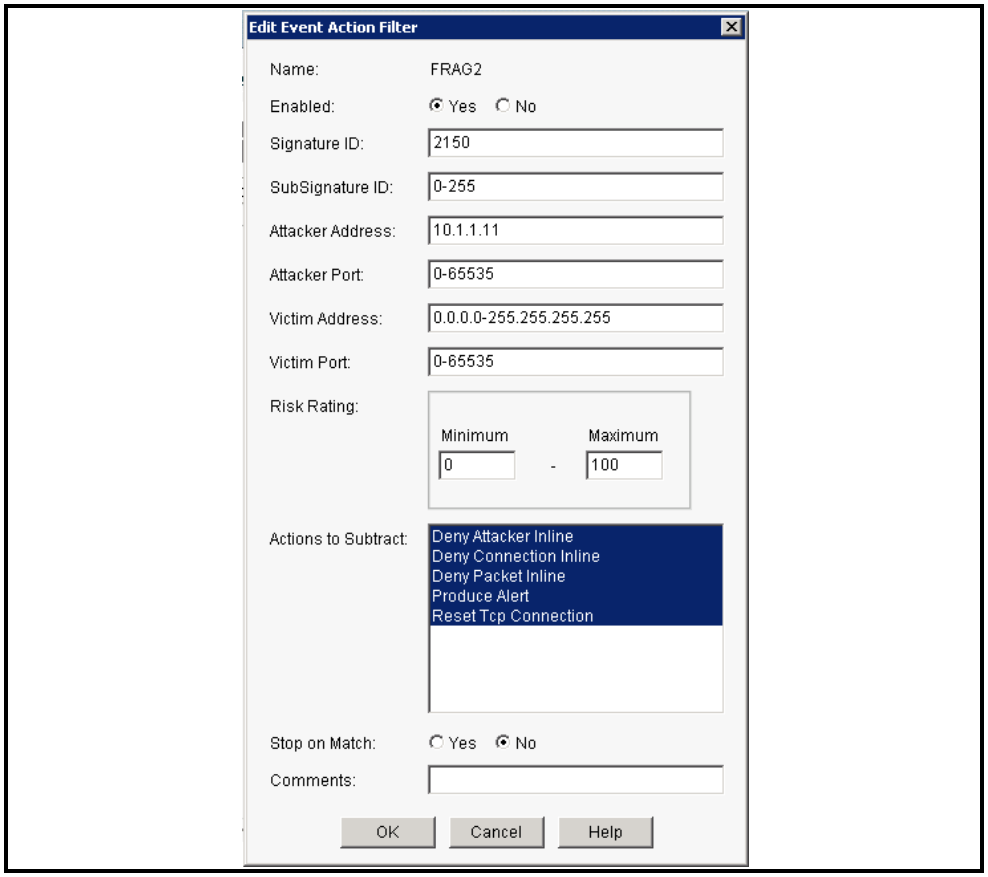



On Server A, inside the Cisco Configuration Professional application, navigate to **Configure > Security > Advanced Security > Intrusion Prevention > Edit IPS > SEAP Configuration > Event Action Filters**.




 © 2010 Cisco Systems, Inc.

Check the **Use Event Action Filters** box and filter the Fragmented ICMP Traffic signature (signature ID 2150) to not trigger (by subtracting all of its actions) if traffic is sourced from the 10.1.1.11 host or destined from the 10.1.1.11 host—you have to create two event action filter rules.




# Lab 3-1 Answer Key: Configuring a PKI-Enabled Site-to-Site IPsec VPN

To complete this activity, configure the following tasks.

## Task 1: Configure a Certificate Server on a Router

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#crypto key generate rsa label CS-KEYS modulus
2048 exportable
ISR-PxR2(config)#crypto pki trustpoint MY-CS
ISR-PxR2(ca-trustpoint)#rsakeypair CS-KEYS
ISR-PxR2(ca-trustpoint)#exit
ISR-PxR2(config)#exit
ISR-PxR2#mkdir my-cs
ISR-PxR2#configure terminal
ISR-PxR2(config)#crypto pki server MY-CS
ISR-PxR2(cs-server)#issuer-name CN=CA, OU=VPN, O=Cisco, C=US
ISR-PxR2(cs-server)#database url flash://my-cs
ISR-PxR2(cs-server)#hash sha1
ISR-PxR2(cs-server)#lifetime certificate 730
ISR-PxR2(cs-server)#lifetime ca-certificate 3650
```

```
ISR-PxR2(cs-server)#exit
ISR-PxR2(config)#ip http server
ISR-PxR2(config)#crypto pki server MY-CS
ISR-PxR2(cs-server)#no shutdown
```

## Task 2: Enroll Two VPN Peers into a PKI

The following commands are needed on the PxR1 router:

```
ISR-PxR1(config)#crypto key generate rsa label VPN-KEYS
modulus 2048 exportable
ISR-PxR1(config)#crypto pki trustpoint VPN-PKI
ISR-PxR1(ca-trustpoint)#enrollment url http://192.168.1.20
ISR-PxR1(ca-trustpoint)#fqdn R1.vpn.cisco.com
ISR-PxR1(ca-trustpoint)#subject-name CN=R1,OU=VPN, O=Cisco,
C=US
ISR-PxR1(ca-trustpoint)#rsakeypair VPN-KEYS
ISR-PxR1(ca-trustpoint)#exit
ISR-PxR1(config)#crypto pki authenticate VPN-PKI
Spoke1(config)#crypto pki enroll VPN-PKI
```

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#crypto key generate rsa label VPN-KEYS
modulus 2048 exportable
ISR-PxR2(config)#crypto pki trustpoint VPN-PKI
ISR-PxR2(ca-trustpoint)#enrollment url http://192.168.1.20
ISR-PxR2(ca-trustpoint)#fqdn R2.vpn.cisco.com
ISR-PxR2(ca-trustpoint)#subject-name CN=R2, OU=VPN, O=Cisco,
C=US
ISR-PxR2(ca-trustpoint)#rsakeypair VPN-KEYS
ISR-PxR2(ca-trustpoint)#exit
ISR-PxR2(config)#crypto pki authenticate VPN-PKI
ISR-PxR2(config)#crypto pki enroll VPN-PKI
ISR-PxR2#crypto pki server MY-CS grant 1
ISR-PxR2#crypto pki server MY-CS grant 2
```

## Task 3: Configure VTI-Based Point-to-Point IPsec VPN Peering

The following commands are needed on the PxR1 router:

```
ISR-PxR1(config)#crypto ipsec profile MYPROFILE
ISR-PxR1(ipsec-profile)#exit
ISR-PxR1(config)#interface tunnel 0
ISR-PxR1(config-if)#ip address 172.16.1.10 255.255.0.0
ISR-PxR1(config-if)#tunnel source FastEthernet 0/0
ISR-PxR1(config-if)#tunnel destination 192.168.1.20
ISR-PxR1(config-if)#tunnel mode ipsec ipv4
ISR-PxR1(config-if)#tunnel protection ipsec profile MYPROFILE
```

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#crypto ipsec profile MYPROFILE
ISR-PxR2(ipsec-profile)#exit
ISR-PxR2(config)#interface tunnel 0
ISR-PxR2(config-if)#ip address 172.16.1.20 255.255.0.0
```

 © 2010 Cisco Systems, Inc.

```
ISR-PxR2(config-if)#tunnel source FastEthernet 0/0
ISR-PxR2(config-if)#tunnel destination 192.168.1.10
ISR-PxR2(config-if)#tunnel mode ipsec ipv4
ISR-PxR2(config-if)#tunnel protection ipsec profile MYPROFILE
```

### Task 4: Configure IKE on Both Peers Using Peer Canonical Name Verification

The following commands are needed on the PxR1 router:

```
ISR-PxR1(config)#crypto pki certificate map MY-CERT-MAP 10
ISR-PxR1(ca-certificate-map)#subject-name co cn=R2
ISR-PxR1(ca-certificate-map)#exit
ISR-PxR1(config)#crypto isakmp profile MY-ISAKMP-PROFILE
ISR-PxR1(conf-isa-prof)#match certificate MY-CERT-MAP
ISR-PxR1(conf-isa-prof)#exit
ISR-PxR1(config)#crypto ipsec profile MYPROFILE
ISR-PxR1(ipsec-profile)#set isakmp-profile MY-ISAKMP-PROFILE
```

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#crypto pki certificate map MY-CERT-MAP 10
ISR-PxR2(ca-certificate-map)#subject-name co CN=R1
ISR-PxR2(ca-certificate-map)#exit
ISR-PxR2(config)#crypto isakmp profile MY-ISAKMP-PROFILE
ISR-PxR2(conf-isa-prof)#match certificate MY-CERT-MAP
ISR-PxR2(conf-isa-prof)#exit
ISR-PxR2(config)#crypto ipsec profile MYPROFILE
ISR-PxR2(ipsec-profile)#set isakmp-profile MY-ISAKMP-PROFILE
```

### Task 5: Configure EIGRP Over the Point-to-Point IPsec VPN Peering

The following commands are needed on the PxR1 router:

```
ISR-PxR1(config)#router eigrp 200
ISR-PxR1(config-router)#network 10.0.0.0
ISR-PxR1(config-router)#network 172.16.0.0
ISR-PxR1(config-router)#no auto-summary
```

The following commands are needed on the PxR2 router:

```
ISR-PxR2(config)#router eigrp 200
ISR-PxR2(config-router)#network 10.0.0.0
ISR-PxR2(config-router)#network 172.16.0.0
ISR-PxR2(config-router)#no auto-summary
```

## Lab 3-2 Answer Key: Configuring Cisco IOS Software DMVPN Spokes

To complete this activity, configure the following tasks.

### Task 1: Verify Preconfigured DMVPN Hub Configuration

No commands are needed in this task.

### Task 2: Configure Two DMVPN Spokes

The following commands are needed on the PxR1 spoke router:

```
ISR-PxR1(config)#crypto pki trustpoint VPN-PKI
```

```
ISR-PxR1(ca-trustpoint)#enrollment url http://192.168.1.1
ISR-PxR1(ca-trustpoint)#revocation-check crl
ISR-PxR1(config)#crypto ca authenticate VPN-PKI
ISR-PxR1(config)#crypto ca enroll VPN-PKI
ISR-PxR1(config)#crypto isakmp policy 10
ISR-PxR1(config-isakmp)#encryption 3des
ISR-PxR1(config-isakmp)#authentication rsa-sig
ISR-PxR1(config-isakmp)#group 14
ISR-PxR1(config)#crypto ipsec transform-set ESP-3DES-SHA esp-
3des esp-sha-hmac
ISR-PxR1(cfg-crypto-trans)#exit
ISR-PxR1(config)#crypto ipsec profile Profile
ISR-PxR1(ipsec-profile)#set transform-set ESP-3DES-SHA
ISR-PxR1(ipsec-profile)#exit
ISR-PxR1(config)#interface tunnel 0
ISR-PxR1(config-if)#tunnel mode gre multipoint
ISR-PxR1(config-if)#tunnel source FastEthernet0/0
ISR-PxR1(config-if)#tunnel key 100000
ISR-PxR1(config-if)#ip nhrp authentication DMVPN_NW
ISR-PxR1(config-if)#ip nhrp nhs 172.16.1.1
ISR-PxR1(config-if)#ip nhrp network-id 100000
ISR-PxR1(config-if)#ip nhrp map multicast 192.168.1.1
ISR-PxR1(config-if)#ip nhrp map 172.16.1.1 192.168.1.1
ISR-PxR1(config-if)#ip address 172.16.1.10 255.255.0.0
ISR-PxR1(config-if)#ip mtu 1400
ISR-PxR1(config-if)#ip tcp adjust-mss 1360
ISR-PxR1(config-if)#tunnel protection ipsec profile Profile
```

The following commands are needed on the PxR2 spoke router:

```
ISR-PxR2(config)#crypto pki trustpoint VPN-PKI
ISR-PxR2(ca-trustpoint)#enrollment url http://192.168.1.1
ISR-PxR2(ca-trustpoint)#revocation-check crl
ISR-PxR2(config)#crypto ca authenticate VPN-PKI
ISR-PxR2(config)#crypto ca enroll VPN-PKI
ISR-PxR2(config)#crypto isakmp policy 10
ISR-PxR2(config-isakmp)#encryption 3des
ISR-PxR2(config-isakmp)#authentication rsa-sig
ISR-PxR2(config-isakmp)#group 14
ISR-PxR2(config)#crypto ipsec transform-set ESP-3DES-SHA esp-
3des esp-sha-hmac
ISR-PxR2(cfg-crypto-trans)#exit
ISR-PxR2(config)#crypto ipsec profile Profile
ISR-PxR2(ipsec-profile)#set transform-set ESP-3DES-SHA
ISR-PxR2(ipsec-profile)#exit
ISR-PxR2(config)#interface tunnel 0
ISR-PxR2(config-if)#tunnel mode gre multipoint
ISR-PxR2(config-if)#tunnel source FastEthernet0/0
ISR-PxR2(config-if)#tunnel key 100000
ISR-PxR2(config-if)#ip nhrp authentication DMVPN_NW
```

 © 2010 Cisco Systems, Inc.

```
ISR-PxR2(config-if)#ip nhrp nhs 172.16.1.1
ISR-PxR2(config-if)#ip nhrp network-id 100000
ISR-PxR2(config-if)#ip nhrp map multicast 192.168.1.1
ISR-PxR2(config-if)#ip nhrp map 172.16.1.1 192.168.1.1
ISR-PxR2(config-if)#ip address 172.16.1.20 255.255.0.0
ISR-PxR2(config-if)#ip mtu 1400
ISR-PxR2(config-if)#ip tcp adjust-mss 1360
ISR-PxR2(config-if)#tunnel protection ipsec profile Profile
ISR-PxR1(config-if)#end
```

### Task 3: Configure EIGRP Support on DMVPN Spokes

The following commands are needed on the PxR1 spoke router:

```
ISR-PxR1(config)#router eigrp 200
ISR-PxR1(config-router)#network 10.0.0.0
ISR-PxR1(config-router)#network 172.16.0.0
ISR-PxR1(config-router)#no auto-summary

ISR-PxR1#ping 10.1.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/5/8 ms
```

The following commands are needed on the PxR2 spoke router:

```
ISR-PxR1(config)#router eigrp 200
ISR-PxR1(config-router)#network 10.0.0.0
ISR-PxR1(config-router)#network 172.16.0.0
ISR-PxR1(config-router)#no auto-summary

ISR-PxR2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/6/8 ms
```

## Lab 3-3 Answer Key: Configuring GET VPN Group Members

To complete this activity, configure the following tasks.

### Task 1: Verify Preconfigured GET VPN Key Server Configuration

The following commands are needed on the ISR-BB key server router:

```
ISR-BB#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
```

```
        encryption algorithm:   AES - Advanced Encryption
Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
        lifetime:               86400 seconds, no volume limit


ISR-BB#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPNGROUP (Unicast)
    Group Identity           : 12345
    Group Members            : 0
    IPSec SA Direction       : Both
    Group Rekey Lifetime     : 86400 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2

      IPSec SA Number        : 10
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : MYIPSECPROFILE
      Replay method          : Count Based
      Replay Window Size     : 64
      ACL Configured         : access-list VPNACL
      Group Server list       : Local

ISR-BB#show ip access-list
Extended IP access list VPNACL
    10 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
```

## Task 2: Configure GET VPN Group Members Including a Fail-Closed Policy

The following commands are needed on the PxR1 member router:

```
ISR-PxR1#configure terminal
ISR-PxR1(config)#crypto isakmp policy 10
ISR-PxR1(config-isakmp)#authentication pre-share
ISR-PxR1(config-isakmp)#encryption aes 128
ISR-PxR1(config-isakmp)#hash sha
ISR-PxR1(config-isakmp)#group 14
ISR-PxR1(config-isakmp)#lifetime 300
ISR-PxR1(config-isakmp)#exit
ISR-PxR1(config)#crypto isakmp key secretpassword address
172.31.1.1
ISR-PxR1(config)#crypto gdoi group MYGETVPNGROUP
ISR-PxR1(config-gdoi-group)#identity number 12345
ISR-PxR1(config-gdoi-group)#server address ipv4 172.31.1.1
ISR-PxR1(config-gdoi-group)#exit
ISR-PxR1(config)#crypto map MYCRYPTOMAP 10 gdoi
ISR-PxR1(config-crypto-map)#set group MYGETVPNGROUP
```

 © 2010 Cisco Systems, Inc.

```
ISR-PxR1(config-crypto-map)#exit
ISR-PxR1(config)#crypto map MYCRYPTOMAP gdoi fail-close
ISR-PxR1(config-crypto-map-fail-close)#activate
ISR-PxR1(config-crypto-map-fail-close)#exit
ISR-PxR1(config)#interface FastEthernet 0/0
ISR-PxR1(config-if)#crypto map MYCRYPTOMAP
ISR-PxR1(config-if)#
```

The following commands are needed on the PxR2 member router:

```
ISR-PxR2#configure terminal
ISR-PxR2(config)#crypto isakmp policy 10
ISR-PxR2(config-isakmp)#authentication pre-share
ISR-PxR2(config-isakmp)#encryption aes 128
ISR-PxR2(config-isakmp)#hash sha
ISR-PxR2(config-isakmp)#group 14
ISR-PxR2(config-isakmp)#lifetime 300
ISR-PxR2(config-isakmp)#exit
ISR-PxR2(config)#crypto isakmp key secretpassword address
172.31.1.1
ISR-PxR2(config)#crypto gdoi group MYGETVPNGROUP
ISR-PxR2(config-gdoi-group)#identity number 12345
ISR-PxR2(config-gdoi-group)#server address ipv4 172.31.1.1
ISR-PxR2(config-gdoi-group)#exit
ISR-PxR2(config)#crypto map MYCRYPTOMAP 10 gdoi
ISR-PxR2(config-crypto-map)#set group MYGETVPNGROUP
ISR-PxR2(config-crypto-map)#exit
ISR-PxR2(config)#crypto map MYCRYPTOMAP gdoi fail-close
ISR-PxR2(config-crypto-map-fail-close)#activate
ISR-PxR2(config-crypto-map-fail-close)#exit
ISR-PxR2(config)#interface FastEthernet 0/0
ISR-PxR2(config-if)#crypto map MYCRYPTOMAP
ISR-PxR2(config-if)#
```

### Task 3: Configure Group Member IKE Credentials on the Key Server and Establish Secure Site-to-Site Connectivity

The following commands are needed on the ISR-BB key server router:

```
ISR-BB#configure terminal
ISR-BB(config)#crypto isakmp key secretpassword address
192.168.1.10
ISR-BB(config)#crypto isakmp key secretpassword address
192.168.1.20
```

## Lab 4-1 Answer Key: Configuring a Cisco IOS Software SSL VPN Gateway

To complete this activity, configure the following tasks.

### Task 1: Provision a Certificate to the SSL VPN Gateway

The following commands are needed on the ISR-PxR2 router:

```
ISR-PxR2(config)#crypto pki trustpoint MY-TRUSTPOINT
```

```
ISR-PxR2(ca-trustpoint)#enrollment url http://192.168.1.1
ISR-PxR2(ca-trustpoint)#fqdn vpn.cisco.com
ISR-PxR2(ca-trustpoint)#subject-name cn=vpn.cisco.com
ISR-PxR2(ca-trustpoint)#exit
ISR-PxR2(config)#crypto ca authenticate MY-TRUSTPOINT
ISR-PxR2(config)#crypto ca enroll MY-TRUSTPOINT
ISR-PxR2(config)#crypto pki export trustpoint_name pem
terminal
```

## Task 2: Import the Root CA Certificate into the Client Certificate Store

The following command is needed on the ISR-PxR2 router:

```
ISR-PxR2(config)#crypto pki export MY-TRUSTPOINT pem terminal
```

## Task 3: Configure a Router as a Full Tunneling SSL VPN Gateway

The following commands are needed on the PxR1 spoke router:

```
ISR-PxR1(config)#router eigrp 200
ISR-PxR1(config-router)#network 10.1.1.0 0.0.0.255
ISR-PxR1(config-router)#network 192.168.1.0 0.0.0.255
ISR-PxR1(config-router)#no auto-summary
```

The following commands are needed on the PxR2 spoke router:

```
ISR-PxR2(config)#router eigrp 200
ISR-PxR2(config-router)#network 192.168.1.0 0.0.0.255
ISR-PxR2(config-router)#no network 10.1.2.0 0.0.0.255
ISR-PxR2(config)#webvpn gateway MY-GATEWAY
ISR-PxR2(config-webvpn-gateway)#ip address 192.168.1.20 port
443
ISR-PxR2(config-webvpn-gateway)#ssl trustpoint MY-TRUSTPOINT
ISR-PxR2(config-webvpn-gateway)#logging enable
ISR-PxR2(config-webvpn-gateway)#inservice
ISR-PxR2(config)#webvpn context MY-CONTEXT
ISR-PxR2(config-webvpn-context)#gateway MY-GATEWAY
ISR-PxR2(config-webvpn-context)#inservice
ISR-PxR2#copy tftp://10.1.1.10/anyconnect-win-2.2.0134-k9.pkg
flash:
ISR-PxR2(config)#webvpn install svc flash://anyconnect-win-
2.2.0134-k9.pkg
ISR-PxR2(config)#aaa new-model
ISR-PxR2(config)#aaa authentication login LOCAL-AUTHEN local
ISR-PxR2(config)#username vpnuser privilege 0 password cisco
ISR-PxR2(config)#ip local pool MY-POOL 172.16.0.1 172.16.0.10
ISR-PxR2(config)#webvpn context MY-CONTEXT
ISR-PxR2(config-webvpn-context)#default-group-policy MY-POLICY
ISR-PxR2(config-webvpn-context)#aaa authentication list LOCAL-
AUTHEN
ISR-PxR2(config-webvpn-context)#policy group MY-POLICY
ISR-PxR2(config-webvpn-group)#banner "Welcome to SSL VPN"
ISR-PxR2(config-webvpn-group)#functions svc-enabled
ISR-PxR2(config-webvpn-group)#svc keep-client-installed
ISR-PxR2(config-webvpn-group)#svc address-pool MY-POOL
```

 © 2010 Cisco Systems, Inc.

```
ISR-PxR2(config-webvpn-group)#svc split include 10.1.2.0
255.255.255.0
```

### Task 4: Install the Cisco AnyConnect Client and Establish a Full Tunneling SSL VPN

No commands are needed in this task.

### Task 5: Configure a Router as a Clientless SSL VPN Gateway

The following commands are needed on the PxR2 spoke router:

```
ISR-PxR2(config)#ip host site.cisco.com 10.1.2.10
ISR-PxR2(config)#webvpn context MY-CONTEXT
ISR-PxR2(config-webvpn-context)#url-list "MY-WEB-BOOKMARKS"
ISR-PxR2(config-webvpn-url)#url-text "Internal web server"
url-value "http://site.cisco.com"
ISR-PxR2(config-webvpn-url)#exit
ISR-PxR2(config-webvpn-context)#policy group MY-POLICY
ISR-PxR2(config-webvpn-group)#url-list "MY-WEB-BOOKMARKS"
```

### Task 6: Configure Basic Cisco Secure Desktop Features for a Clientless SSL VPN

The following commands are needed on the PxR2 spoke router:

```
ISR-PxR2#copy tftp://10.1.1.10/securedesktop-ios-3.1.1.45-
k9.pkg flash:
ISR-PxR2(config)#webvpn install csd flash://securedesktop-ios-
3.1.1.45-k9.pkg
ISR-PxR2(config)#webvpn context MY-CONTEXT
ISR-PxR2(config-webvpn-context)#csd enable
```

## Lab 4-2 Answer Key: Configuring Cisco Easy VPN

To complete this activity, configure the following tasks.

### Task 1: Configure the Cisco Easy VPN Server Feature Using VTIs and Remote AAA

The following commands are needed on the ISR-PxR1 router:

```
ISR-PxR1(config)#router eigrp 200
ISR-PxR1(config-router)#network 192.168.1.0 0.0.0.255
ISR-PxR1(config-router)network 10.1.1.0 0.0.0.255
ISR-PxR1(config-router)#no auto-summary
```

The following commands are needed on the ISR-PxR2 router:

```
ISR-PxR2(config)#router eigrp 200
ISR-PxR2(config-router)#network 192.168.1.0 0.0.0.255
ISR-PxR2(config-router)#no network 10.1.2.0 0.0.0.255
ISR-PxR2(config-router)#no auto-summary
ISR-PxR2(config)#crypto ipsec transform-set MY-SET esp-aes
esp-sha-hmac
ISR-PxR2(cfg-crypto-trans)#exit
ISR-PxR2(config)#crypto ipsec profile MY-PROFILE
ISR-PxR2(ipsec-profile)#set transform-set MY-SET
ISR-PxR2(config)#interface virtual-template 1 type tunnel
ISR-PxR2(config-if)#ip unnumbered fastEthernet 0/0
ISR-PxR2(config-if)#tunnel mode ipsec ipv4
```

```
ISR-PxR2(config-if)#tunnel protection ipsec profile MY-PROFILE
ISR-PxR2(config-if)#
ISR-PxR2(config)#ip local pool MY-POOL 172.16.0.1 172.16.0.10
ISR-PxR2(config)#ip access-list extended MY-SPLIT-TUNNEL
ISR-PxR2(config-ext-nacl)#permit ip 10.1.2.0 0.0.0.255 any
ISR-PxR2(config-ext-nacl)#exit
ISR-PxR2(config)#crypto isakmp client configuration group MY-
GROUP
ISR-PxR2(config-isakmp-group)#key cisco
ISR-PxR2(config-isakmp-group)#pool MY-POOL
ISR-PxR2(config-isakmp-group)#acl MY-SPLIT-TUNNEL
ISR-PxR2(config)#aaa new-model
ISR-PxR2(config)#aaa authentication login LOCAL-AUTHEN local
ISR-PxR2(config)#aaa authorizatoin network LOCAL-AUTHOR local
ISR-PxR2(config)#username vpnuser privilege 0 password cisco
ISR-PxR2(config)#crypto isakmp profile MY-ISAKMP-PROFILE
ISR-PxR2(conf-isa-prof)#match identity group MY-GROUP
ISR-PxR2(conf-isa-prof)#client authentication list LOCAL-
AUTHEN
ISR-PxR2(conf-isa-prof)#isakmp authorization list LOCAL-AUTHOR
ISR-PxR2(conf-isa-prof)#client configuration address respond
ISR-PxR2(conf-isa-prof)#client configuration group MY-GROUP
ISR-PxR2(conf-isa-prof)#virtual-template 1
ISR-PxR2(conf-isa-prof)#exit
ISR-PxR2(config)#crypto ipsec profile MY-PROFILE
ISR-PxR2(ipsec-profile)#set isakmp-profile MY-ISAKMP-PROFILE
```

## Task 2: Configure the Cisco VPN Client

No commands are needed in this task.

## Task 3: Configure a Cisco Easy VPN Remote Device Using VTI

The following commands are needed on the ISR-PxR1 router:

```
ISR-PxR1(config)#router eigrp 200
ISR-PxR1(config-router)#network 10.1.1.0 0.0.0.255
ISR-PxR1(config-router)#network 192.168.1.0 0.0.0.255
ISR-PxR1(config-router)#no auto-summary
ISR-PxR1(config-if)#interface virtual-template 1 type tunnel
ISR-PxR1(config-if)#tunnel mode ipsec ipv4
ISR-PxR1(config-if)#exit
ISR-PxR1(config)#crypto ipsec client ezvpn MY-EZVPN-CLIENT
ISR-PxR1(config-crypto-ezvpn)#group MY-GROUP key cisco
ISR-PxR1(config-crypto-ezvpn)#virtual-interface 1
ISR-PxR1(config-crypto-ezvpn)#peer 192.168.1.20
ISR-PxR1(config-crypto-ezvpn)#mode client
ISR-PxR1(config-crypto-ezvpn)#username vpnuser password cisco
ISR-PxR1(config)#interface FastEthernet 0/1
ISR-PxR1(config-if)#crypto ipsec client ezvpn MY-EZVPN-CLIENT
inside
ISR-PxR1(config-if)#exit
```

 © 2010 Cisco Systems, Inc.

```
ISR-PxR1(config)#interface FastEthernet 0/0
ISR-PxR1(config-if)#crypto ipsec client ezvpn MY-EZVPN-CLIENT
outside
ISR-PxR1(config-if)#exit
```

The following commands are needed on the ISR-PxR2 router spoke router:

```
ISR-PxR2(config)#router eigrp 200
ISR-PxR2(config-router)#network 192.168.1.0 0.0.0.255
ISR-PxR2(config-router)#no network 10.1.2.0 0.0.0.255
ISR-PxR2(config)#crypto isakmp client configuration group MY-
GROUP
ISR-PxR2(config-isakmp-group)#save-password
```

 © 2010 Cisco Systems, Inc.