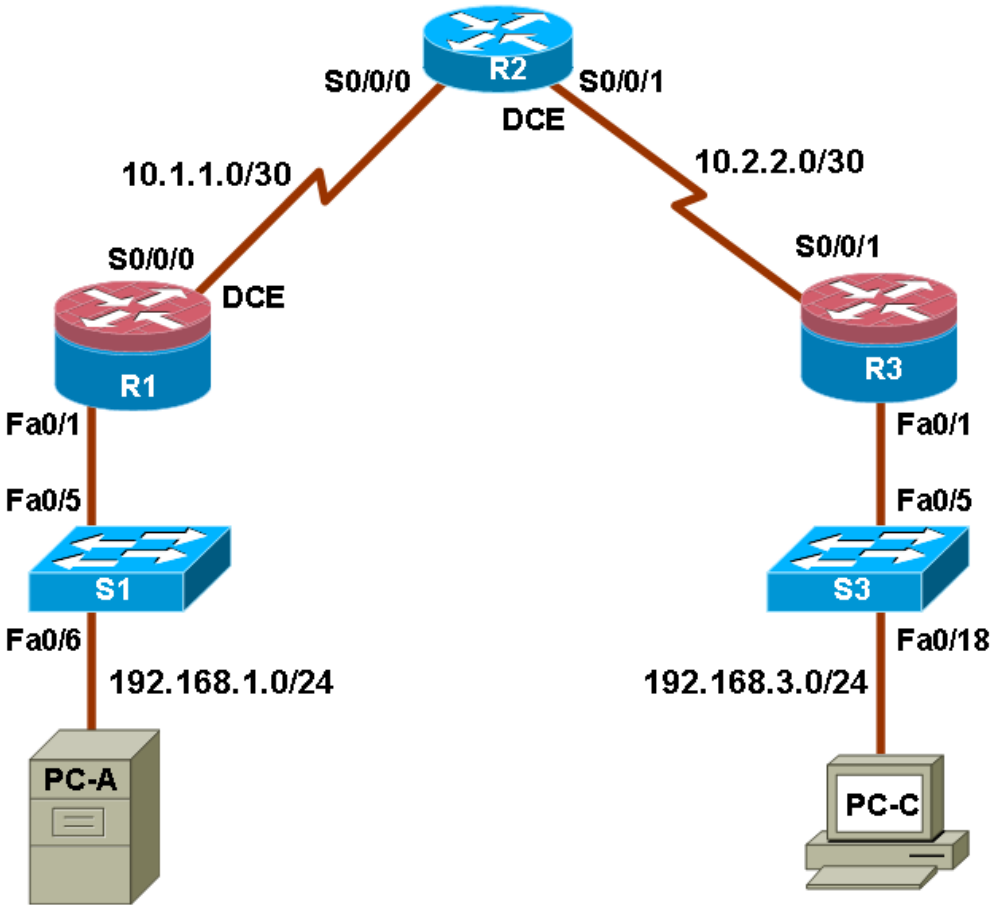
Chapter 5 Lab A: Configuring an Intrusion Prevention System (IPS) Using the CLI and CCP

Topology



Note: ISR G2 devices have Gigabit Ethernet interfaces instead of Fast Ethernet Interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Router Configuration

- Configure hostname, interface IP addresses and access passwords.
- Configure the static routing.

Part 2: Use CLI to configure an IOS Intrusion Prevention System (IPS)

- Configure IOS IPS using CLI.
- Modify IPS Signatures.
- Examine the resulting IPS configuration.
- Verify IPS functionality.
- Log IPS messages to a syslog server.

Part 3: Configuring an Intrusion Prevention System (IPS) using CCP

- Configure IPS using CCP.
- Modify IPS signatures.
- Examine the resulting IPS configuration.
- Use a scanning tool to simulate an attack.
- Use the CCP Monitor to verify IPS functionality.

Background

In this lab, you configure the Cisco IOS Intrusion Prevention System (IPS), which is part of the Cisco IOS Firewall feature set. IPS examines certain attack patterns and alerts or mitigates when those patterns occur. IPS alone is not enough to make a router into a secure Internet firewall, but in addition to other security features, it can be a powerful defense.

You will configure IPS using the Cisco IOS CLI on one router and CCP on another router, and then test IPS functionality on both routers. You will load the IPS Signature package from a TFTP server and configure the public crypto key using the Cisco IOS CLI and CCP.

Note: The router commands and output in this lab are from a Cisco 1841 using Cisco IOS Release 12.4(20)T (Advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router and Cisco IOS version, the available commands and the output produced might vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 2 routers (Cisco 1841 with Cisco IOS Release 12.4(20)T1 and 192MB DRAM or comparable routers)
- 1 router (R2) Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable
- 2 switches (Cisco 2960 or comparable)
- PC-A: Windows XP, Vista or Windows 7 with syslog and TFTP servers and the SuperScan tool (optional)
- PC-C: Windows XP, Vista or Windows 7 with Java 6 Standard Edition, CCP 2.5, syslog, and TFTP servers, and the SuperScan tool (optional)
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console
- IPS Signature package and public crypto key files on PC-A and PC-C (provided by instructor)

CCP Notes:

- Refer to Chp 00 Lab A for instructions on how to install CCP. Hardware/software recommendations for CCP include Windows XP, Vista, or Windows 7 with Java version 1.6.0_11 up to 1.6.0_21, Internet Explorer 6.0 or above and Flash Player Version 10.0.12.36 and later.
- If the PC on which CCP is installed is running Windows Vista or Windows 7, it may be necessary to right-click on the CCP icon or menu item, and choose **Run as administrator**.
- In order to run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure that all pop-up blockers are turned off in the browser.

Part 1: Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings such as host names, interface IP addresses, static routing, device access, and passwords.

Note: Perform all tasks on routers R1, R2, and R3. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology diagram and cable as necessary.

Step 2: Configure the basic settings for each router.

a. Configure the host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table.

c. Configure a clock rate for serial router interfaces with a DCE serial cable attached.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

d. To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

b. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

Step 5: Verify basic network connectivity.

a. Ping from R1 to R3.

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that the static routing protocol is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to identify routing protocol-related problems.

Step 6: Configure and encrypt passwords.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

a. Configure a minimum password length using the **security passwords** command to set a minimum password length of **10** characters.

```
R1(config)# security passwords min-length 10
```

b. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered to be a good security practice.

```
R1(config)# line console 0
```



```
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

c. Configure a password for the aux port for router R1.

```
R1(config)# line aux 0
R1(config-line)# password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

d. Configure the password on the vty lines for router R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

e. Encrypt the console, aux, and vty clear text passwords.

```
R1(config)# service password-encryption
```

f. Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not? _____

Step 7: Save the basic configurations for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1# copy running-config startup-config
```

Part 2: Configuring IPS Using the Cisco IOS CLI

In Part 2 of this lab, you configure IPS on R1 using the Cisco IOS CLI. You then review and test the resulting configuration.

Task 1: Verify Access to the R1 LAN from R2

In this task, you verify that without IPS configured, the external router R2 can ping the R1 S0/0/0 interface and PC-A on the R1 internal LAN.

Step 1: Ping from R2 to R1.

a. From R2, ping R1 interface S0/0/0 at IP address 10.1.1.1.

```
R2# ping 10.1.1.1
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Ping from R2 to PC-A on the R1 LAN.

a. From R2, ping PC-A on the R1 LAN at IP address 192.168.1.3.

```
R2# ping 192.168.1.3
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 3: Display the R1 running config prior to configuring IPS.

a. Issue the **show run** command to review the current basic configuration on R1.

b. Are there any security commands related to IPS?

_____

Task 2: Prepare the Router and TFTP Server

Step 1: Verify the availability of Cisco IOS IPS files.

To configure Cisco IOS IPS 5.x, the IOS IPS Signature package file and public crypto key file must be available on PC-A. Check with your instructor if these files are not on the PC. These files can be downloaded from Cisco.com with a valid user account that has proper authorization.

a. Verify that the IOS-S*xxx*-CLI.pkg file is in a TFTP folder. This is the signature package. The *xxx* is the version number and varies depending on which file was downloaded.

b. Verify that the realm-cisco.pub.key.txt file is available and note its location on PC-A. This is the public crypto key used by IOS IPS.

Step 2: Verify or create the IPS directory in router flash on R1.

In this step, you verify the existence of, or create a directory in, the router flash memory where the required signature files and configurations will be stored.

Note: Alternatively, you can use a USB flash drive connected to the router USB port to store the signature files and configurations. The USB flash drive needs to remain connected to the router USB port if it is used as the IOS IPS configuration directory location. IOS IPS also supports any Cisco IOS file system as its configuration location with proper write access.

a. From the R1 CLI, display the contents of flash memory using the **show flash** command and check for the **ipsdir** directory.

```
R1# show flash
```

b. If the ipsdir directory is not listed, create it in privileged EXEC mode.

```
R1# mkdir ipsdir
Create directory filename [ipsdir]? Press Enter
Created dir flash:ipsdir
```

Note: If the directory already exists, the following message displays.

```
%Error Creating dir flash:ipsdir (Can't create a file that exists)
```

c. From the R1 CLI, verify that the directory is present using the **dir flash:** or **dir flash:ipsdir** command.

```
R1# dir flash:
Directory of flash:/
```

```
        5  -rw-    37081324  Dec 17 2008 21:57:10 +00:00  c1841-
    advipservicesk9-mz.124-20.T1.bin
        6  drw-           0   Jan 6 2009 11:19:14 +00:00  ipsdir
```

or

```
R1# dir flash:ipsdir

Directory of flash:/ipsdir/

No files in directory
```

Note: The directory exists, but there are currently no files in it.

Task 3: Configuring the IPS Crypto Key

The crypto key verifies the digital signature for the master signature file (sigdef-default.xml). The contents are signed by a Cisco private key to guarantee the authenticity and integrity at every release.

Note: The following instructions use Notepad as the text editor and HyperTerminal as the terminal emulation program. Another text editor and terminal emulation program can be used.

Step 1: Locate and open the crypto key file.

On PC-A, locate the crypto key file named realm-cisco.pub.key.txt and open it using Notepad or another text editor. The contents should look similar to the following:

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
```

Step 2: Copy the contents of the text file.

a. From the Notepad menu bar, choose **Edit > Select All**.

b. Choose **Edit > Copy** (or press Ctrl+C).

Step 3: Apply the contents of the text file to the router.

a. At the R1 privileged EXEC prompt, enter global config mode using the **config t** command.

b. With the cursor at the `R1(config)#` prompt, paste the text file contents from HyperTerminal by right-clicking and selecting **Paste to Host** from the context menu. Alternatively, you can select **Edit > Paste to Host** from the HyperTerminal menu bar.

c. Exit global config mode and issue the **show run** command to confirm that the crypto key is configured.

Task 4: Configure IPS

Step 1: Create an IPS rule.

a. On R1, create an IPS rule name using the **ip ips name** *name* command in global configuration mode. Name the IPS rule **iosips**. This will be used later on an interface to enable IPS.

```
R1(config)# ip ips name iosips
```

b. You can specify an optional extended or standard access control list (ACL) to filter the traffic that will be scanned by this rule name. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

c. To see the options available for specifying an ACL with the rule name, use the **ip ips name** command and the CLI help function (**?**).

```
R1(config)# ip ips name ips list ?
  <1-199>  Numbered access list
  WORD     Named access list
```

Step 2: Configure the IPS Signature storage location in router flash memory.

The IPS files will be stored in the ipsdir directory that was created in Task 2, Step 2. Configure the location using the **ip ips config location** command.

```
R1(config)# ip ips config location flash:ipsdir
```

Step 3: Enable IPS SDEE event notification.

The Cisco Security Device Event Exchange (SDEE) server is a Simple Object Access Protocol (SOAP) based, intrusion detection system (IDS) alert format and transport protocol specification. SDEE replaces Cisco RDEP.

To use SDEE, the HTTP server must be enabled with the **ip http server** command. If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot see the requests. SDEE notification is disabled by default and must be explicitly enabled.

Note: CCP Monitor uses HTTP and SDEE to capture IPS events.

To enable SDEE, use the following command.

```
R1(config)# ip ips notify sdee
```

Step 4: Enable IPS syslog support.

IOS IPS also supports the use of syslog to send event notification. SDEE and syslog can be used independently or enabled at the same time to send IOS IPS event notification. Syslog notification is enabled by default.

a. If console logging is enabled, you see IPS syslog messages. Enable syslog if it is not enabled.

```
R1(config)# ip ips notify log
```


b. Use the **show clock** command to verify the current time and date for the router. Use the **clock set** command from privileged EXEC mode to reset the clock if necessary. The following is an example of how to set the clock.

```
R1# clock set 01:20:00 6 january 2009
```

c. Verify that the timestamp service for logging is enabled on the router using the **show run** command. Enable the timestamp service if it is not enabled.

```
R1(config)# service timestamps log datetime msec
```

d. To send log messages to the syslog server on PC-A, use the following command:

```
R1(config)# logging 192.168.1.3
```

e. To see the type and level of logging enabled on R1, use the **show logging** command.

```
R1# show logging
```

Note: Verify that you have connectivity between R1 and PC-A by pinging from PC-A to the R1 Fa0/1 interface IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.

The next step describes how to download one of the freeware syslog servers if one is not available on PC-A.

Step 5: (Optional) Download and start the syslog server.

If a syslog server is not currently available on PC-A, you can download the latest version of Kiwi from http://www.kiwisyslog.com or Tftpd32 from http://tftpd32.jounin.net/. If the syslog server is available on the PC, go to Step 6.

Note: This lab uses the Tftpd32 syslog server.

Start the syslog server software on PC-A if you want to send log messages to it.

Step 6: Configure IOS IPS to use one of the pre-defined signature categories.

IOS IPS with Cisco 5.x format signatures operates with signature categories, just like Cisco IPS appliances do. All signatures are pregrouped into categories, and the categories are hierarchical. This helps classify signatures for easy grouping and tuning.

Warning: The “all” signature category contains *all* signatures in a signature release. Because IOS IPS cannot compile and use all the signatures contained in a signature release at one time, do not unretire the “all” category. Otherwise, the router will run out of memory.

Note: When configuring IOS IPS, it is required to first retire all the signatures in the “all” category and then unretire selected signature categories.

In the following example, all signatures in the “all” category are retired, and then the “ios_ips basic” category is unretired.

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] <Enter>
```

```
Jan  6 01:32:37.983: Applying Category configuration to signatures ...
```

Step 7: Apply the IPS rule to an interface.

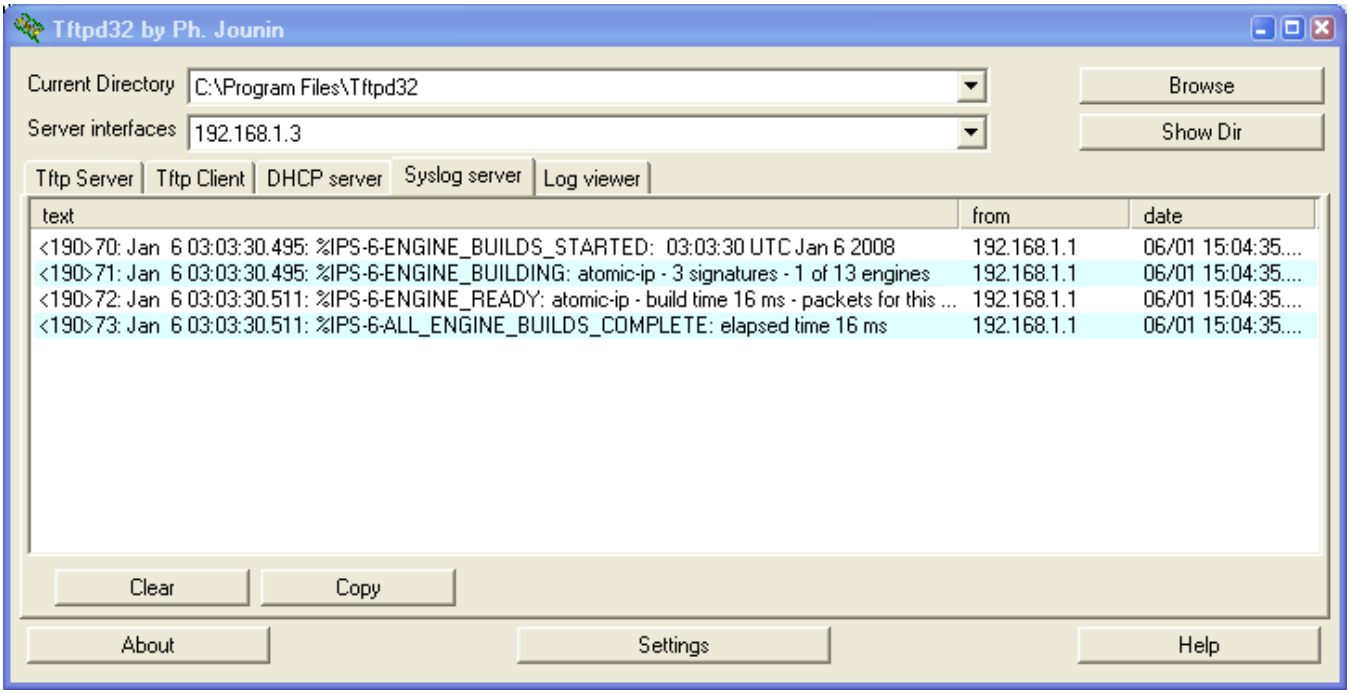
a. Apply the IPS rule to an interface with the **ip ips** *name direction* command in interface configuration mode. Apply the rule you just created inbound on the S0/0/0 interface. After you enable IPS, some log messages will be sent to the console line indicating that the IPS engines are being initialized.

Note: The direction **in** means that IPS inspects only traffic going into the interface. Similarly, **out** means only traffic going out the interface. To enable IPS to inspect both in and out traffic, enter the IPS rule name for in and out separately on the same interface.

```
R1(config)# interface serial0/0/0
R1(config-if)# ip ips iosips in

Jan  6 03:03:30.495: %IPS-6-ENGINE_BUILDS_STARTED:  03:03:30 UTC Jan 6
2008
Jan  6 03:03:30.495: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1
of 13 engines
Jan  6 03:03:30.511: %IPS-6-ENGINE_READY: atomic-ip - build time 16 ms -
packets for this engine will be scanned
Jan  6 03:03:30.511: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16 ms
```

The message also displays on the syslog server if it is enabled. The Tftpd32 syslog server is shown here.



b. Although the R1 Fa0/1 interface is an internal interface, it might be desirable to configure it with IPS to respond to internal attacks. Apply the IPS rule to the R1 Fa0/1 interface in the inbound direction.

```
R1(config)# interface fa0/1
R1(config-if)# ip ips iosips in
```

Step 8: Save the running configuration.

Enter privileged EXEC mode using the **enable** command and provide the enable password cisco12345.

```
R1# copy run start
```

Task 5: Load the IOS IPS Signature Package to the Router

The most common way to load the signature package to the router is to use TFTP. Refer to Step 4 for alternative methods for loading the IOS IPS signature package. The alternative methods include the use of FTP and a USB flash drive.

Step 1: (Optional) Download the TFTP server.

The Tftpd32 freeware TFTP server is used in this task. Many other free TFTP servers are also available. If a TFTP server is not currently available on PC-A, you can download the latest version of Tftpd32 from http://tftpd32.jounin.net/. If it is already installed, go to Step 2.

Note: This lab uses the Tftpd32 TFTP server. This software also includes a syslog server, which runs simultaneously with the TFTP server.

Step 2: Start the TFTP server on PC-A and verify the IPS file directory.

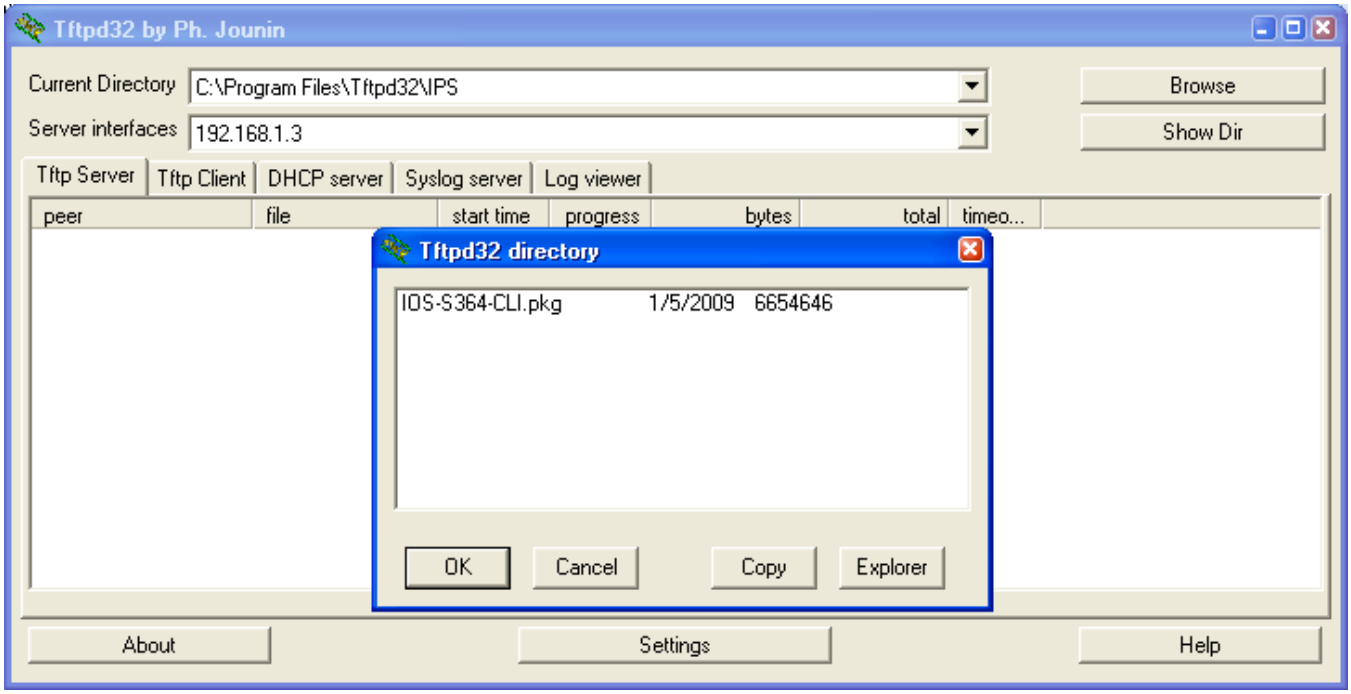
a. Verify connectivity between R1 and PC-A, the TFTP server, using the **ping** command.

b. Verify that the PC has the IPS Signature package file in a directory on the TFTP server. This file is typically named IOS-S*xxx*-CLI.pkg, where *xxx* is the signature file version.

   Note: If this file is not present, contact your instructor before continuing.

c. Start Tftpd32 or another TFTP server and set the default directory to the one with the IPS Signature package in it. The Tftpd32 screen is shown here with the C:\Program Files\Tftpd32\IPS directory contents displayed. Take note of the filename for use in the next step.

Note: It is recommended to use the latest signature file available in a production environment. However, if the amount of router flash memory is an issue in a lab environment, you may use an older version 5.x signature, which requires less memory. The S364 file is used with this lab for demonstration purposes, although newer versions are available. Consult CCO to determine the latest version.



Step 3: Copy the signature package from the TFTP server to the router.

If you do not have a TFTP server available and are using a router with a USB port, you can go to Step 5 and use the procedure described there.

a. Use the **copy tftp** command to retrieve the signature file. Be sure to use the **idconf** keyword at the end of the **copy** command.

Note: Immediately after the signature package is loaded to the router, signature compiling begins. You can see the messages on the router with logging level 6 or above enabled.

```
R1# copy tftp://192.168.1.3/IOS-S364-CLI.pkg idconf

Loading IOS-S364-CLI.pkg from 192.168.1.3 (via FastEthernet0/1):
!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6654646 bytes]

Jan  6 03:18:36.799: %IPS-6-ENGINE_BUILDS_STARTED:  03:18:36 UTC Jan 6
2008
Jan  6 03:18:36.799: %IPS-6-ENGINE_BUILDING: multi-string - 8
signatures - 1 of 13 engines
Jan  6 03:18:36.811: %IPS-6-ENGINE_READY: multi-string - build time 12
ms - packets for this engine will be scanned
Jan  6 03:18:36.831: %IPS-6-ENGINE_BUILDING: service-http - 629
signatures - 2 of 13 engines
Jan  6 03:18:46.755: %IPS-6-ENGINE_READY: service-http - build time
9924 ms - packets for this engine will be scanned
<Output omitted>
```

b. Use the **dir flash** command to see the contents of the ipsdir directory created earlier. There should be six files as shown here.

```
R1# dir flash:ipsdir
Directory of flash:/ipsdir/
```

```
16  -rw-   230621  Jan 6 2008 03:19:42 +00:00  R1-sigdef-default.xml
15  -rw-      255  Jan 6 2008 01:35:26 +00:00  R1-sigdef-delta.xml
14  -rw-     6632  Jan 6 2008 03:17:48 +00:00  R1-sigdef-typedef.xml
13  -rw-    28282  Jan 6 2008 03:17:52 +00:00  R1-sigdef-category.xml
10  -rw-      304  Jan 6 2008 01:35:28 +00:00  R1-seap-delta.xml
18  -rw-      491  Jan 6 2008 01:35:28 +00:00  R1-seap-typedef.xml
```

Step 4: Verify that the signature package is properly compiled.

a. Use the **show ip ips signature count** command to see the counts for the signature package compiled.

```
R1# show ip ips signature count

Cisco SDF release version S364.0
Trend SDF release version V0.0

Signature Micro-Engine: multi-string: Total Signatures 11
      multi-string enabled signatures: 9
      multi-string retired signatures: 11

Signature Micro-Engine: service-http: Total Signatures 662
      service-http enabled signatures: 163
      service-http retired signatures: 565
      service-http compiled signatures: 97
      service-http obsoleted signatures: 1

Signature Micro-Engine: string-tcp: Total Signatures 1148
      string-tcp enabled signatures: 622
      string-tcp retired signatures: 1031
      string-tcp compiled signatures: 117
      string-tcp obsoleted signatures: 21

<Output Omitted>

Total Signatures: 2435
   Total Enabled Signatures: 1063
   Total Retired Signatures: 2097
   Total Compiled Signatures: 338
   Total Obsoleted Signatures: 25
```

Note: If you see an error message during signature compilation, such as "`%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)`," it means the public crypto key is invalid. Refer to Task 3, Configuring the IPS Crypto Key, to reconfigure the public crypto key.

b. Use the **show ip ips all** command to see an IPS configuration status summary. To which interfaces and in which direction is the iosips rule applied? _____

```
R1# show ip ips all

IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir/
    Last signature default load time: 18:47:52 UTC Jan 6 2009
    Last signature delta load time: 20:11:35 UTC Jan 6 2009
    Last event action (SEAP) load time: -none-

    General SEAP Config:
```



```
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 339
    Total Inactive Signatures: 2096

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Interface Configuration
      Interface Serial0/0/0
        Inbound IPS rule is iosips
        Outgoing IPS rule is not set
      Interface FastEthernet0/1
              Inbound IPS rule is iosips
              Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False
```

Step 5: (Optional) Alternative methods of copying the signature package to the router.

If you used TFTP to copy the file and do not intend to use one of these alternative methods, read through the procedures described here to become familiar with them. If you use one of these methods instead of TFTP, return to Step 4 to verify that the signature package loaded properly.

FTP method: Although the TFTP method is generally adequate, the signature file is rather large and FTP provides a more positive method of copying the file. You can use an FTP server to copy the signature file to the router with this command:

copy ftp://<ftp_user:password@Server_IP_address>/<signature_package> idconf

In the following example, the user **admin** must be defined on the FTP server with a password of **cisco**.

```
R1# copy ftp://admin:cisco@192.168.1.3/IOS-S364-CLI.pkg idconf
Loading IOS-S364-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
```

USB method: If there is no access to a FTP or TFTP server, you can use a USB flash drive to load the signature package to the router.

a. Copy the signature package onto the USB drive.

b. Connect the USB drive to one of the USB ports on the router.

c. Use the **show file systems** command to see the name of the USB drive. In the following output, a 4GB USB drive is connected to the USB port on the router as file system usbflash0:.

```
R1# show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
        196600        185972     nvram     rw   nvram:
*     64012288      14811136      disk     rw   flash:#
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   pram:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    4001378304    3807461376  usbflash     rw   usbflash0:
```

d. Verify the contents of the flash drive using the **dir** command.

```
R1# dir usbflash0:
Directory of usbflash0:/
90  -rw-  6654646  Jan 5 2009 14:49:34 +00:00  IOS-S364-CLI.pkg
91  -rw-      805  Jan 5 2009 14:49:34 +00:00  realm-cisco.pub.key.txt
```

e. Use the **copy** command with the **idconf** keyword to copy the signature package to the router.

```
R1# copy usbflash0:IOS-S364-CLI.pkg idconf
```

The USB copy process can take 60 seconds or more, and no progress indicator is displayed. When the copy process is completed, numerous engine building messages display. These must finish before the command prompt returns.

Task 6: Test the IPS Rule and Modify a Signature

You can work with signatures in many ways. They can be retired and unretired, enabled and disabled, and their characteristics and actions can be changed. In this task, you first test the default behavior of IOS IPS by pinging it from the outside.

Step 1: Ping from R2 to the R1 serial 0/0/0 interface.

From the CLI on R2, ping R1 S0/0/0 at IP address 10.1.1.1. The pings are successful because the ICMP Echo Request signature 2004:0 is retired.

Step 2: Ping from R2 to PC-A.

From the CLI on R2, ping PC-A at IP address 192.168.1.3. These pings are also successful because of the retired signature. This is the default behavior of the IPS Signatures.

```
R2# ping 192.168.1.3
```



```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Step 3: Modify the signature.

You can use Cisco IOS CLI to change signature status and actions for one signature or a group of signatures based on signature categories.

The following example shows how to un-retire the echo request signature, enable it, change the signature action to alert, and drop and reset for signature 2004 with a subsig ID of 0.

```
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 2004 0
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)# retired false
R1(config-sigdef-sig-status)# enabled true
R1(config-sigdef-sig-status)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# event-action reset-tcp-connection
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>

*Jan  6 19:36:56.459: %IPS-6-ENGINE_BUILDS_STARTED:  19:36:56 UTC Jan 6 2009
*Jan  6 19:36:56.891: %IPS-6-ENGINE_BUILDING: atomic-ip - 306 signatures - 1
of 13 engines
*Jan  6 19:36:57.599: %IPS-6-ENGINE_READY: atomic-ip - build time 704 ms -
packets for this engine will be scanned
*Jan  6 19:36:57.979: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 1520 ms
```

Step 4: Ping from R2 to R1 serial 0/0/0 interface.

a. Start the syslog server.

b. From the CLI on R2 ping R1 S0/0/0 at IP address 10.1.1.1. Where the pings successful? Why or why not? _____

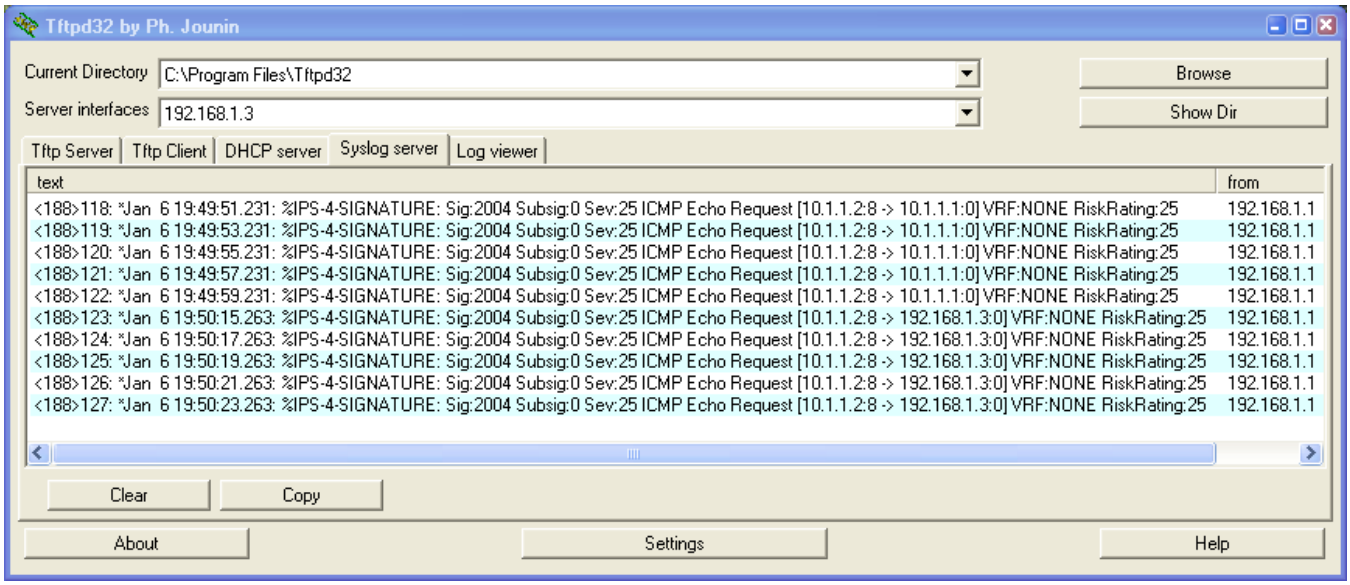
Step 5: Ping from R2 to PC-A.

a. From the CLI on R2, ping R1 S0/0/0 at IP address 192.168.1.3. Were the pings successful?
_____

```
R2# ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

b. Notice the IPS messages from R1 on the syslog server screen below. How many messages were generated from the R2 pings to R1 and PC-A? _____



Note: The ICMP echo request IPS risk rating (severity level) is relatively low at 25. Risk rating can range from 0 to 100.

Task 7: (Optional) Test IPS with SuperScan

SuperScan is a freeware scanning tool that runs with Windows XP. It can detect open TCP and UDP ports on a target host. If the SuperScan program is available on PC-A or can be downloaded, you can perform this task.

SuperScan will test the IPS capabilities on R1. You will run the scanning program from PC-A and attempt to scan open ports on router R2. The IPS rule iosips, which is set on R1 F0/1 inbound, should intercept the scanning attempts and send messages to the R1 console and syslog server.

Step 1: Download the SuperScan program.

a. If SuperScan is not on PC-A, download the SuperScan 4.0 tool from the Scanning Tools group at http://www.foundstone.com.

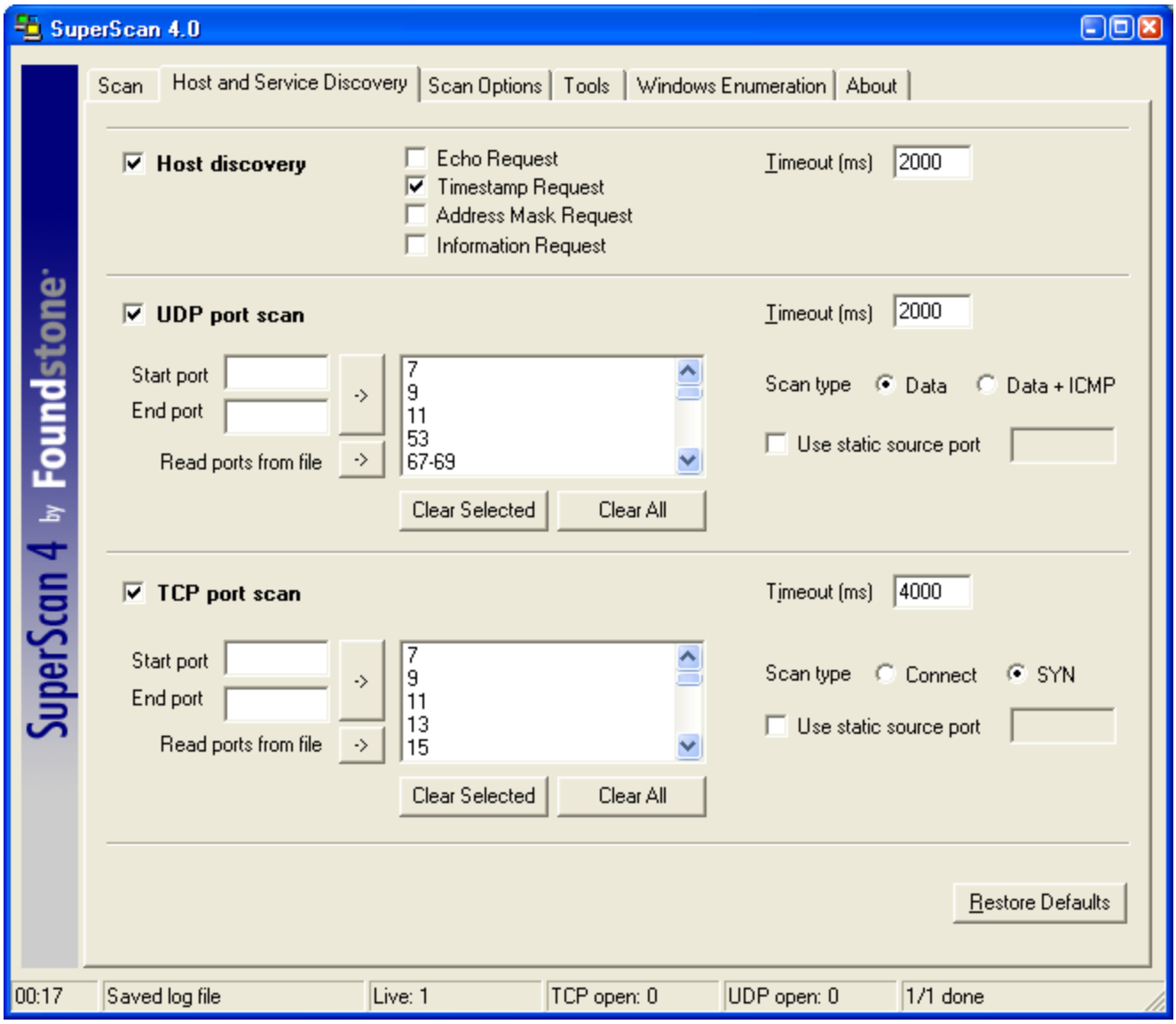
b. Unzip the file into a folder. The SuperScan4.exe file is executable and installation is not required.

Step 2: Run SuperScan and set scanning options.

a. Start the SuperScan program on PC-A.

b. Click the **Host and Service Discovery** tab. Check the **Timestamp Request** check box, and uncheck the **Echo Request** check box.

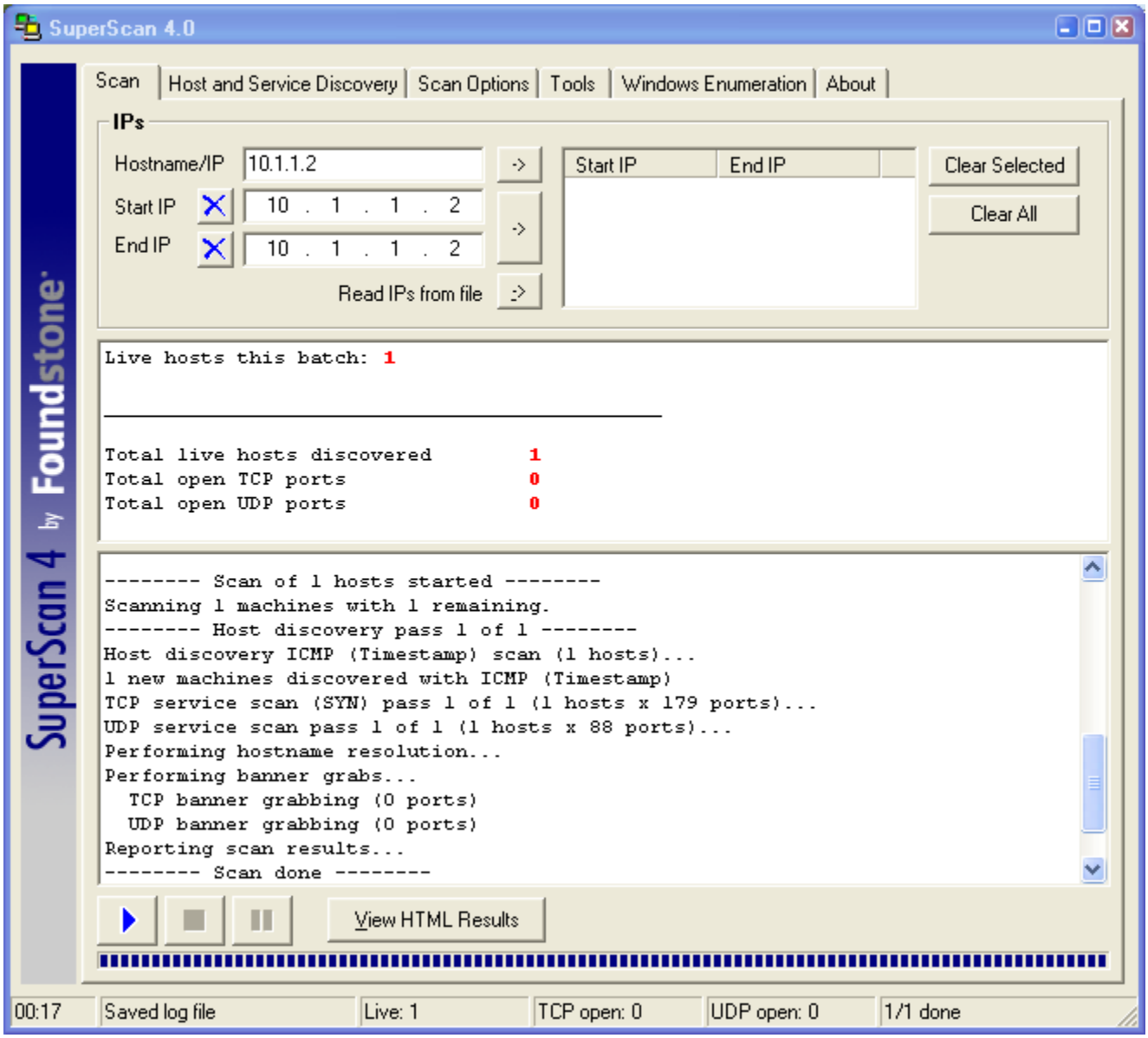
c. Scroll through the UDP and TCP port selection lists and notice the range of ports that will be scanned.



d. Click the **Scan** tab and enter the IP address of R2 S0/0/0 (**10.1.1.2**) in the Hostname/IP field.

Note: You can also specify an address range, such as 10.1.1.1 to 10.1.1.254, by entering an address in the Start IP and End IP fields. The program scans all hosts with addresses in the range specified.

e. To start the scan, click the button with the blue arrow at the bottom left of the screen. Results of the scan are shown in the SuperScan window.



f. How many open TCP and UDP ports did SuperScan find on R2? Why do you think this is?

_____

g. Exit SuperScan.

Step 3: Observe the syslog messages on R1.

a. You should see syslog entries on the R1 console and on the syslog server if it is enabled. The descriptions should include phrases such as "`Invalid DHCP Packet`" and "`DNS Version Request`."

```
R1#
*Jan  6 19:43:35.611: %IPS-4-SIGNATURE: Sig:6054 Subsig:0 Sev:50 DNS
Version Request [192.168.1.3:1076 -> 10.1.1.2:53] VRF:NONE
RiskRating:50
```

```
*Jan  6 19:43:35.851: %IPS-4-SIGNATURE: Sig:4619 Subsig:0 Sev:75
Invalid DHCP Packet [192.168.1.3:1096 -> 10.1.1.2:67] VRF:NONE
RiskRating:75
```

b. What is the IPS risk rating or severity level (Sev:) of the DNS version request, signature 6054? ___

c. What is the IPS risk rating or severity level (Sev:) of the Invalid DHCP Packet, signature 4619? ___

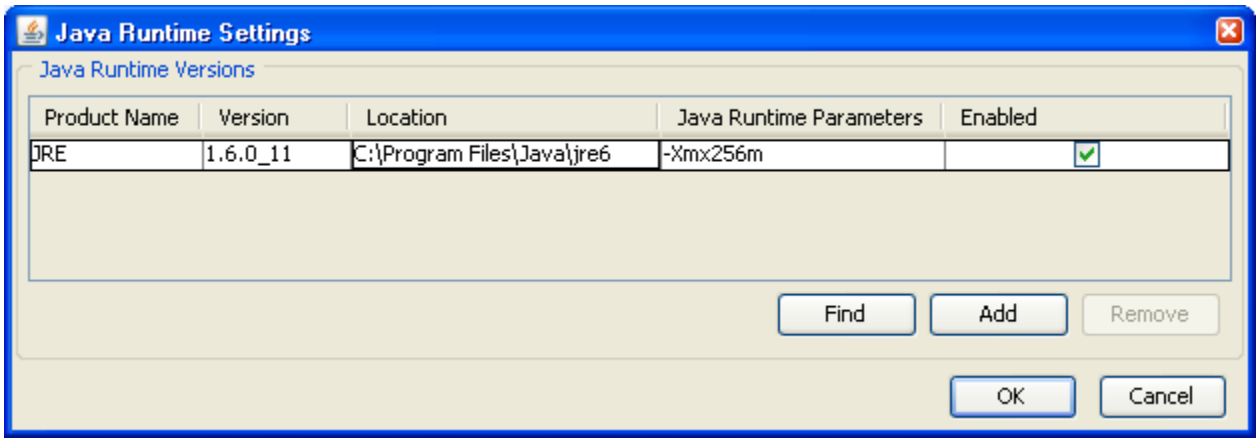
d. Which signature is considered by IPS to be more of a threat? _____

Part 3: Configuring IPS using CCP

In Part 3 of this lab, you configure IOS IPS on R3 using CCP.

Note: To support CCP configuration of IPS, PC-C should be running Java JRE version 6 or newer to set the Java heap to 256 MB. This is done using the runtime parameter –Xmx256m. The latest JRE for Windows XP can be downloaded from Oracle Corporation at http://www.oracle.com/.

The PC must have at least 512MB of RAM. From the PC Start Menu, click **Settings > Control Panel > Java** to open the Java Control Panel window. From the Java Control Panel window, click the **Java** tab and click the **View** button to enter or change the Java Applet Runtime Settings. The following screenshot shows setting the heap size to 256MB using the Runtime Parameter –Xmx256m.



Task 1: Verify Access to the R3 LAN from R2

In this task, you verify that, without IPS configured, external router R2 can access the R3 S0/0/1 interface and PC-C on the R3 internal LAN.

Step 1: Ping from R2 to R3.

a. From R2, ping the R3 interface S0/0/1 at IP address 10.2.2.1.

```
R2# ping 10.2.2.1
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Ping from R2 to PC-C on the R3 LAN.

a. From R2, ping PC-C on the R3 LAN at IP address 192.168.3.3.

```
R2# ping 192.168.3.3
```

b. Were the results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 3: Display the R3 running config prior to starting CCP.

a. Issue the **show run** command to review the current basic configuration on R3.

b. Verify the R3 basic configuration as performed in Part 1 of the lab. Are there any security commands related to IPS? _____

Task 2: Prepare the Router for CCP and IPS

Step 1: Configure the enable secret password and HTTP router access prior to starting CCP.

a. From the CLI, configure the enable secret password for use with CCP on R3.

```
R3(config)# enable secret cisco12345
```

b. Enable the HTTP server on R3.

```
R3(config)# ip http server
```

c. Add admin user to the local database.

```
R3(config)# username admin privilege 15 secret cisco12345
```

d. Have CCP use the local database to authenticate web sessions.

```
R3(config)# ip http authentication local
```

Step 2: Verify or create the IPS directory in router flash.

a. From the R3 CLI, display the content of flash memory using the **show flash** command and check for the ipsdir directory.

```
R3# show flash
```

b. If this directory is not listed, create it by entering the command **mkdir ipsdir** in privileged EXEC mode.

```
R3# mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir
```

c. From the R3 CLI, verify that the directory is present using the **dir flash:ipsdir** command.

```
R3# dir flash:ipsdir

Directory of flash:/ipsdir/

No files in directory
```

Note: The directory exists, but there are currently no files in it.

Task 3: Prepare the TFTP Server

Step 1: Download the TFTP server.

The Tftp32 freeware TFTP server is used in this task. Many other free TFTP servers are also available. If a TFTP server is not currently available on PC-C, you can download the latest version of Tftpd32 from http://tftpd32.jounin.net/. If it is already installed, go to Step 2.

This lab uses the Tftpd32 TFTP server. This software also includes a syslog server that runs simultaneously with the TFTP server.

Step 2: Start the TFTP server on PC-C and verify the IPS file directory.

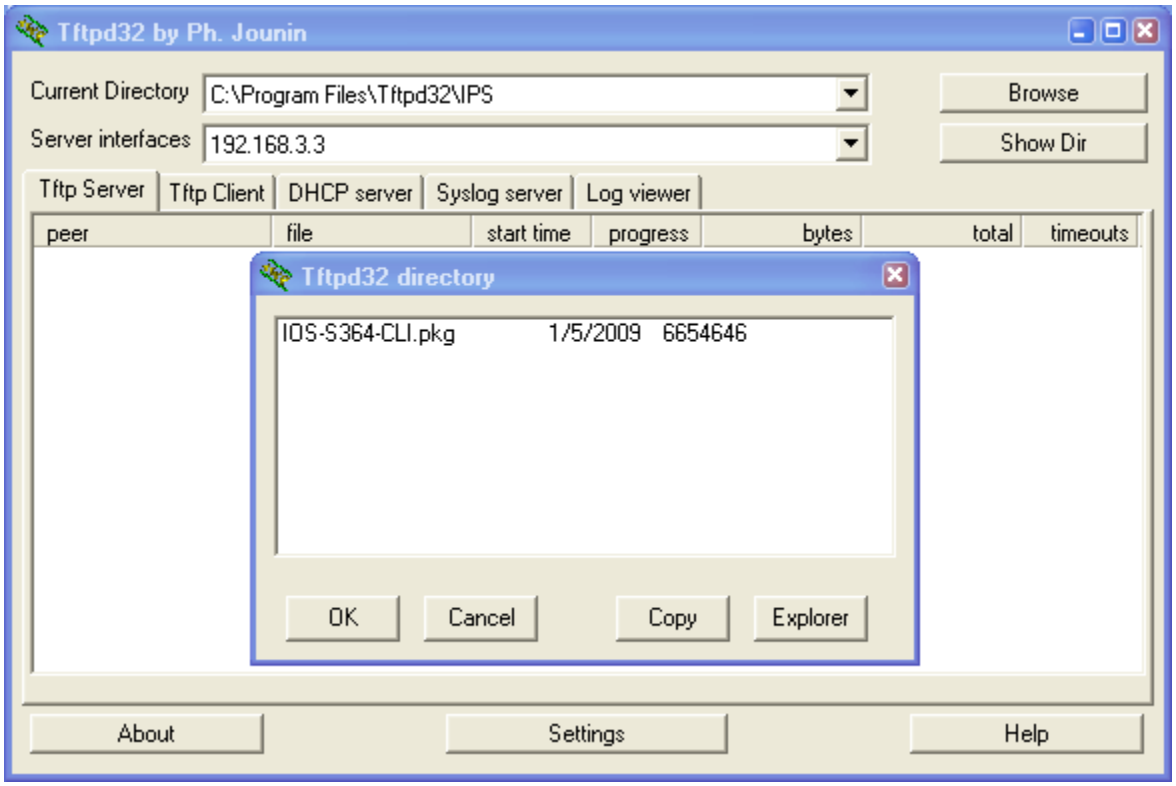
a. Verify connectivity between R3 and PC-C, the TFTP server, using the **`ping`** command.

b. Verify that the PC has the IPS Signature package file in a directory on the TFTP server. This file is typically named IOS-S*xxx*-CLI.pkg, where *xxx* is the signature file version.

Note: If this file is not present, contact your instructor before continuing.

c. Start Tftpd32 or another TFTP server and set the default directory to the one with the IPS Signature package. The Tftpd32 screen is shown here with the C:\Program Files\Tftpd32\IPS directory contents displayed. Take note of the filename for use in the next step.

d. What is the name of the signature file? _____



Task 4: Use CCP to Configure IPS

Step 1: Access CCP and discover R3.

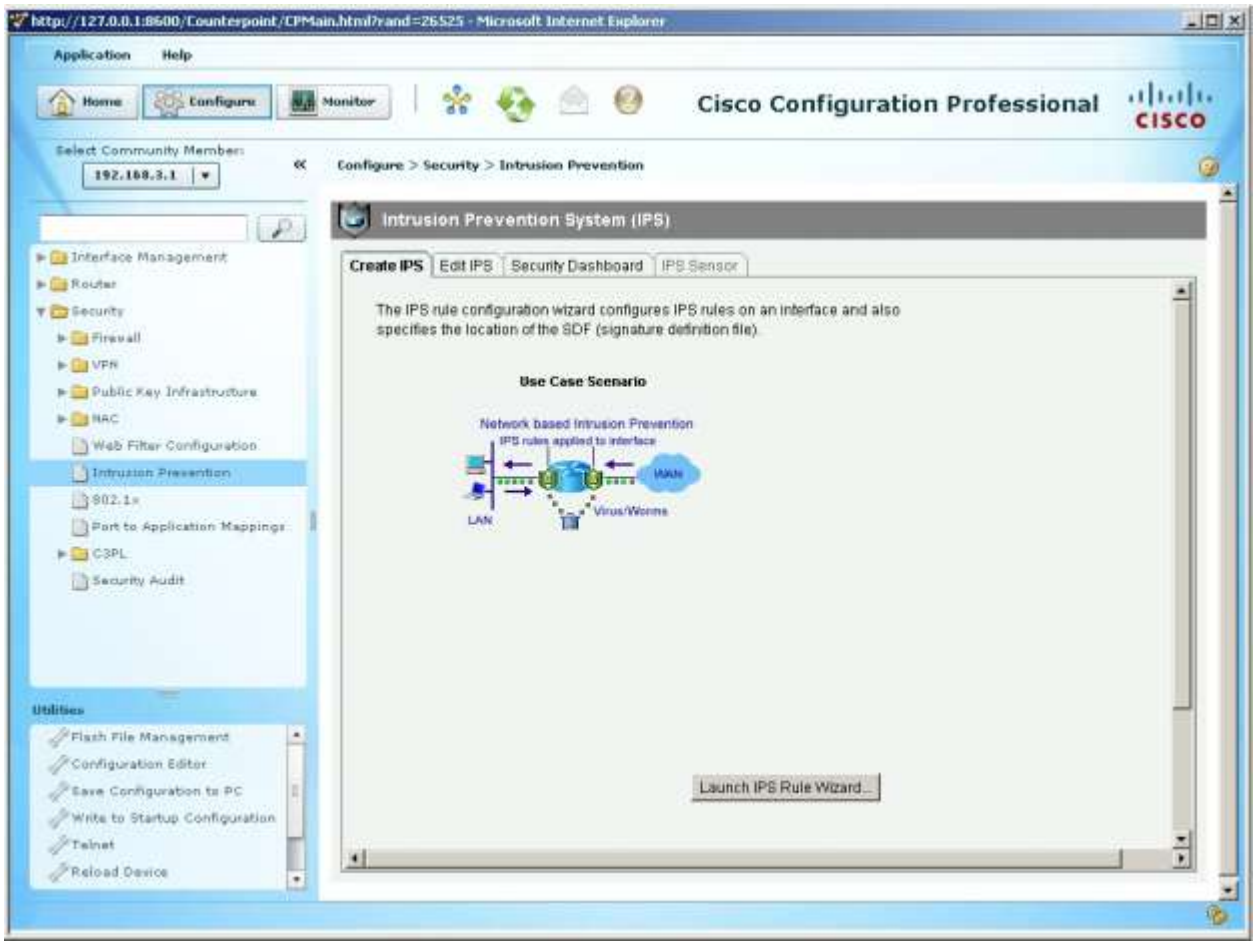
a. Start CCP on PC-C. In the Manage Devices window, add R3 IP address 192.168.3.1 in the first IP address field. Enter **admin** in the Username field, and **cisco12345** in the Password field.

b. At the CCP Dashboard, click the **Discover** button to discover and connect to R3. If discovery fails, click the **Discovery Details** button to determine the problem.

Note: If you are using Java version 1.6 or later, the Java console displays by default when CCP is run. If the Java console displays, you can close it. You can also start the Java plug-in application and choose **Advanced > Java Console > Do not start console**. The Java console will not appear again unless you change the setting.

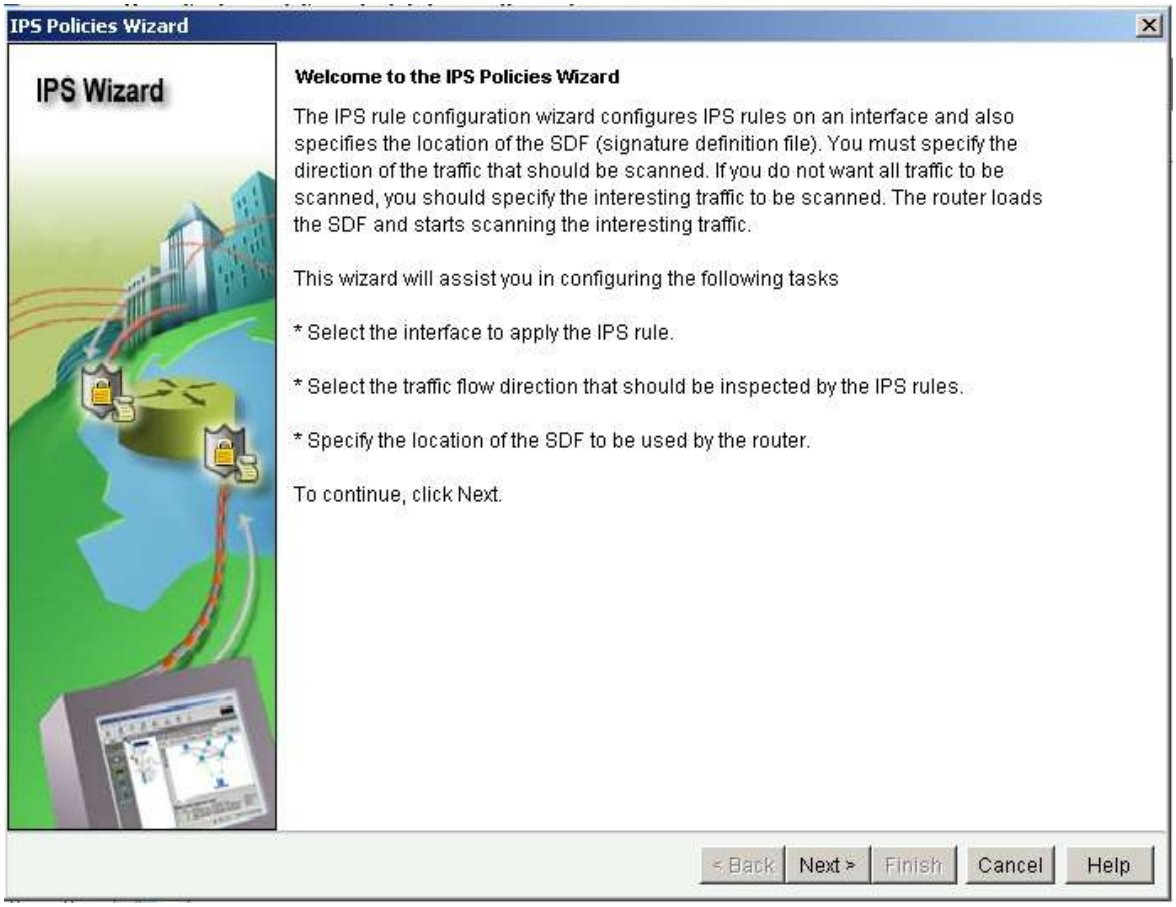
Step 2: Use the CCP IPS Wizard to configure Cisco IOS IPS.

a. Click the **Configure** button at the top of the CCP screen and then choose **Security** > **Intrusion Prevention > Create IPS**.



b. Click the **Launch IPS Rule Wizard** button to open the Welcome to the IPS Policies Wizard window.

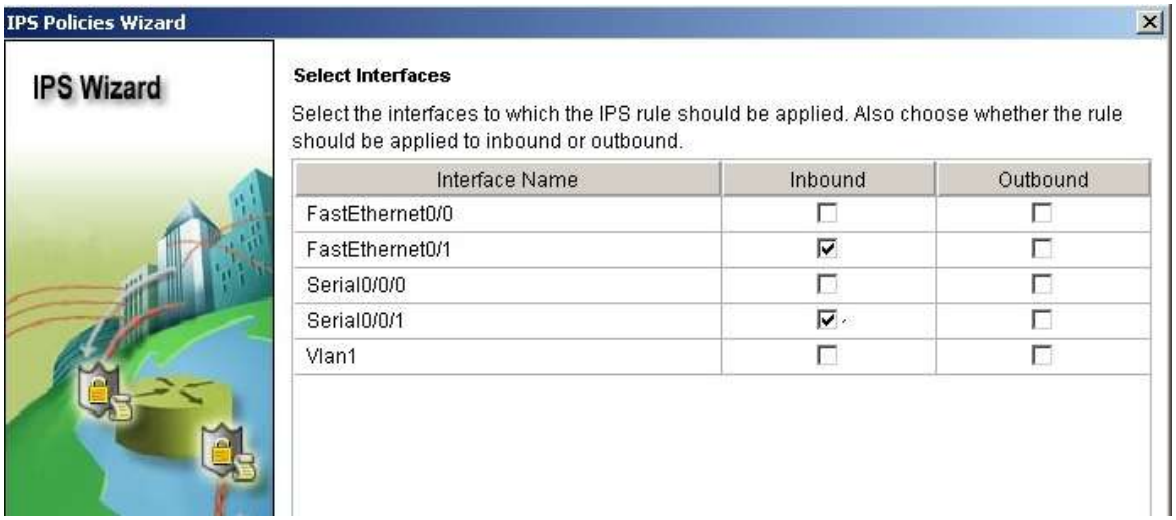
c. Read the information on the IPS Policies Wizard screen to become familiar with what the wizard does. Click **Next**.



Note: SDEE dialog boxes might appear. Read the information and click **OK** for each dialog box.

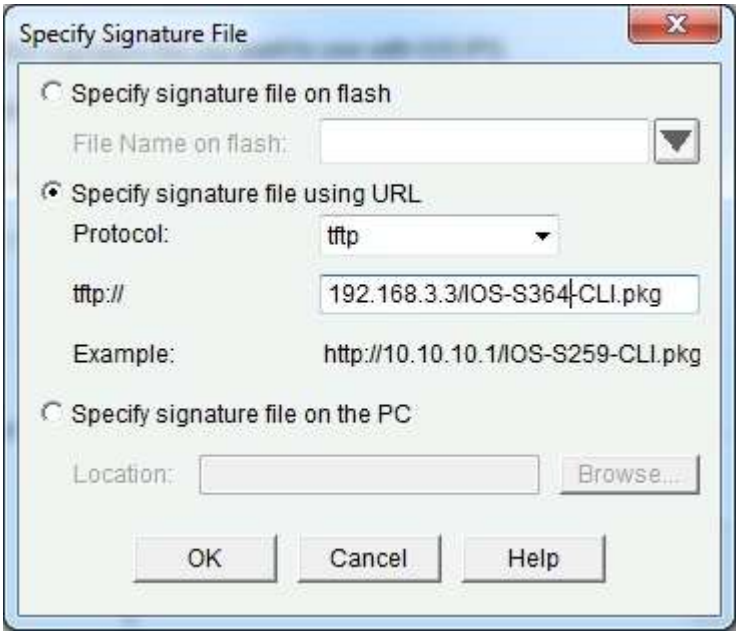
d. In the Select Interfaces window, check the **Inbound** check box for Fast Ethernet0/1 and Serial0/0/1. Click **Next**.

Note: Selecting inbound on both interfaces allows IPS to monitor attacks on the router from the internal and external network.



e. In the Signature File and Public Key window, click the ellipsis (**…**) button next to Specify the Signature File You Want to Use with IOS IPS to open the Specify Signature File window. Confirm that the **Specify signature file using URL** option is chosen.

f. For Protocol, select **tftp** from the drop-down menu. Enter the IP address of the PC-C TFTP server and the filename. For example, 192.168.3.3/IOS-S364-CLI.pkg.



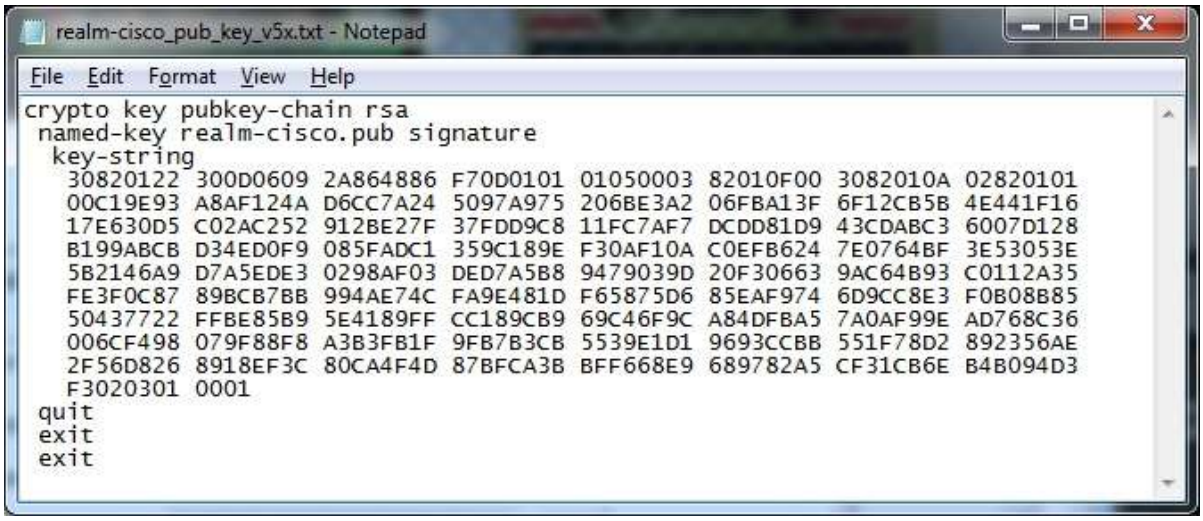
g. What other options can be specified as a source for the Signature File?

_____

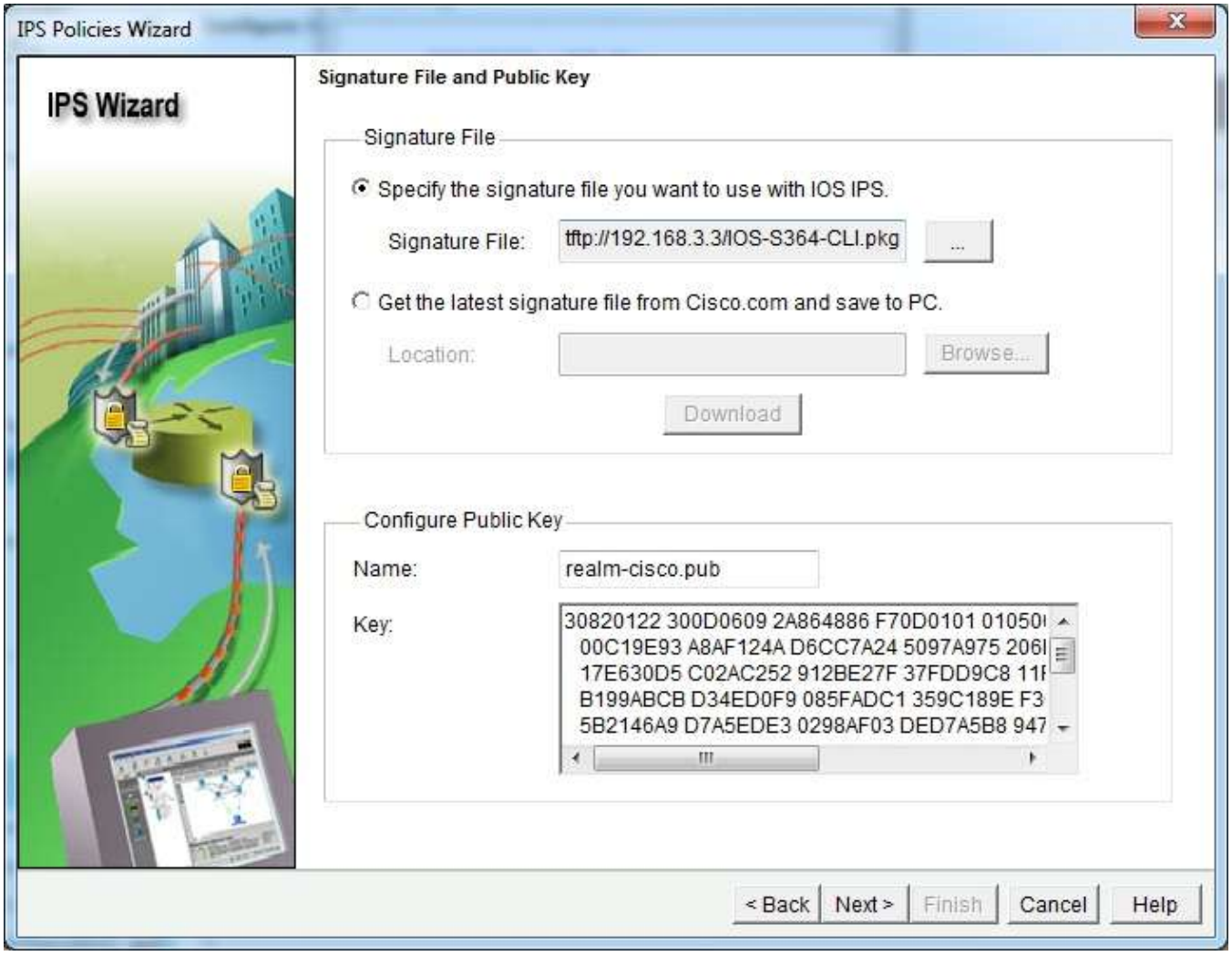
h. Click **OK** to return to the Signature File and Public Key window. In the Configure Public Key section of the Signature File and Public Key window, enter **realm-cisco.pub** in the Name field.

i. Each change to the signature configuration is saved in a delta file. This file must be digitally signed with a public key. You can obtain a key from Cisco.com and paste the information in the Name and Key fields. In this lab, you will copy and paste the key from a text file on PC-C.

j. Open the realm-cisco-pub-key.txt file located on the PC-C desktop. The following is an example from the realm-cisco-pub-key.txt file.



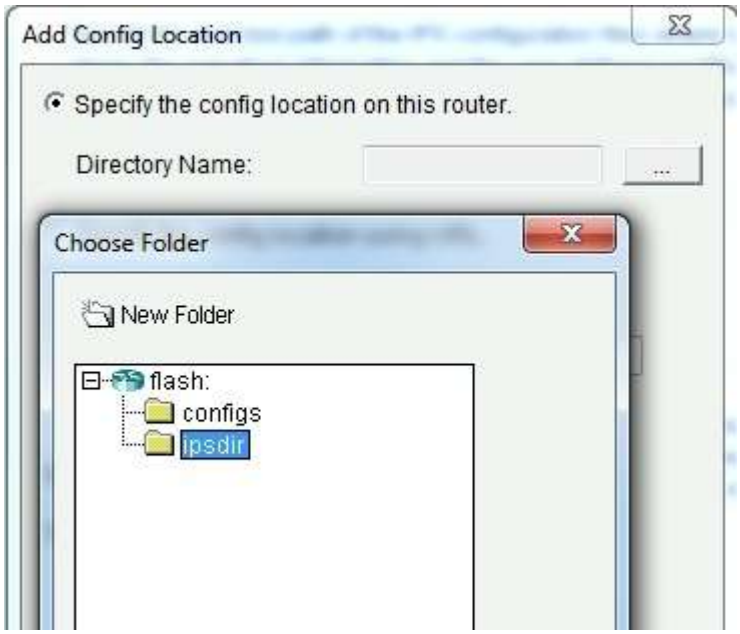
k. Copy the text between the phrase **key-string** and the word **quit** into the **Key** field in the Configure Public Key section. The Signature File and Public Key window should look similar to the following when the entries are completed.



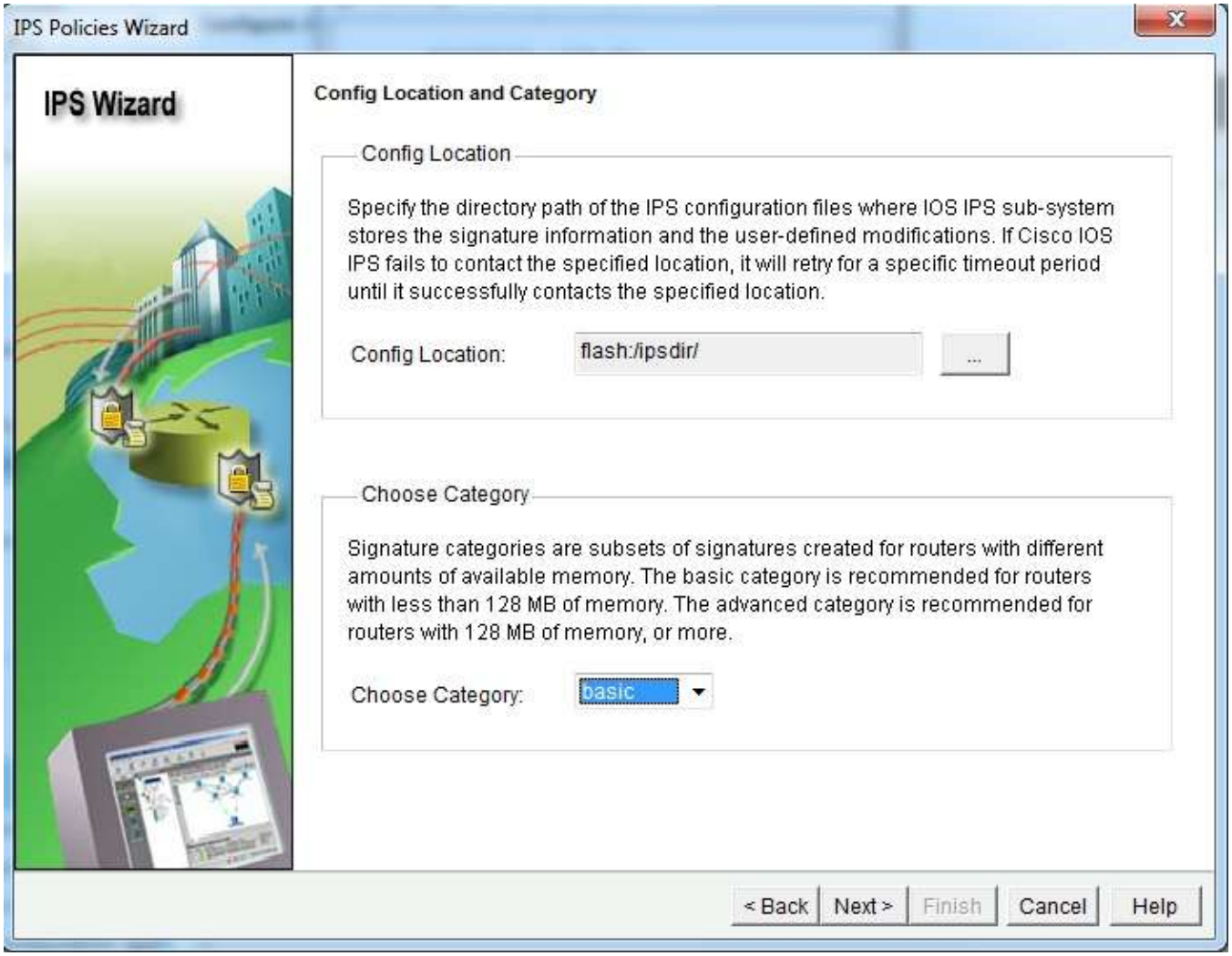
l. Click **Next** to display the Config Location and Category window. This is used to specify where to store the signature information. This file is used by the Cisco IOS IPS for detecting attacks from coming into the Fast Ethernet0/1 or Serial0/0/1 interfaces.

m. In the Config Location and Category window in the Config Location section, click the ellipsis (**...**) button next to **Config Location** to add the location.

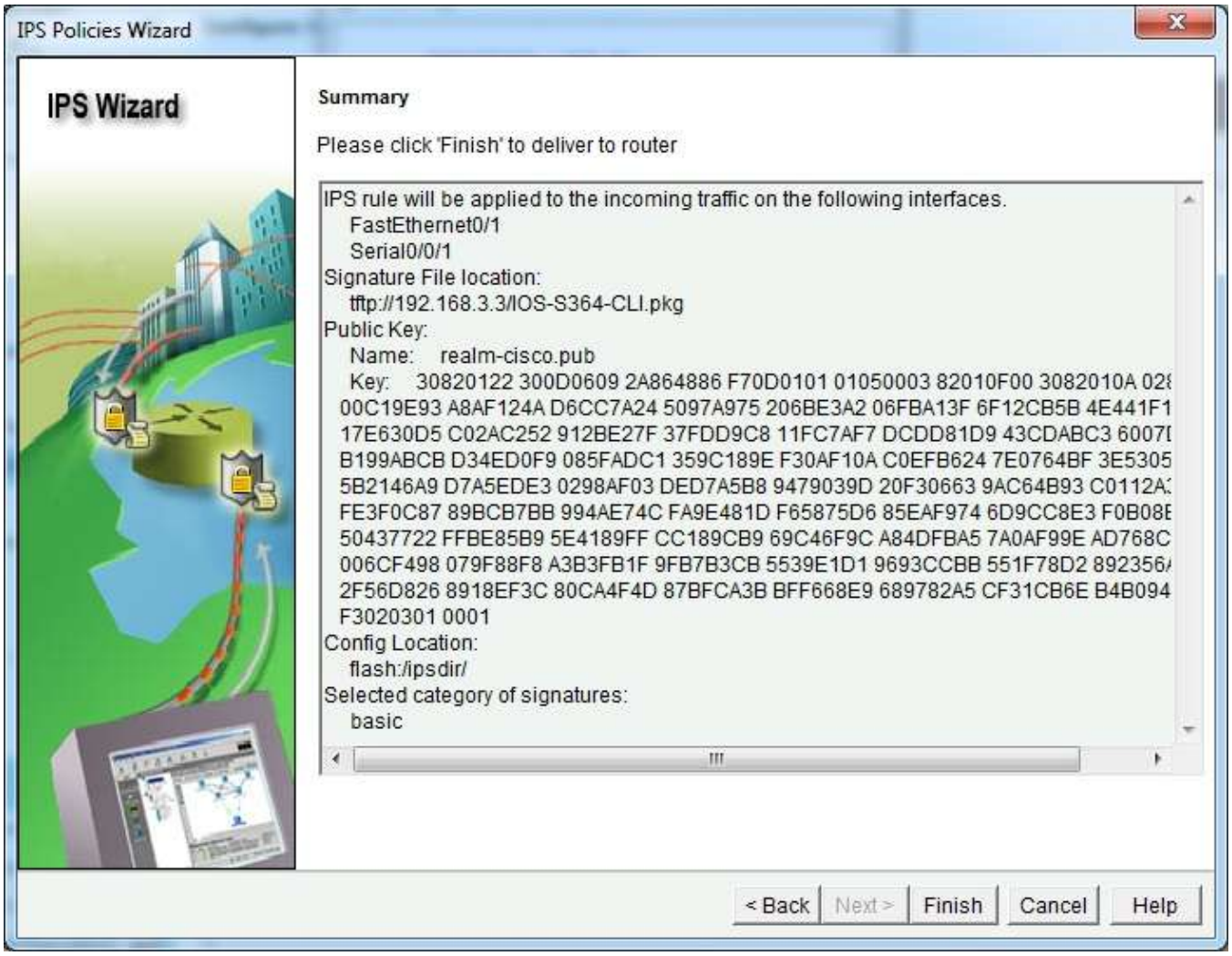
n. Verify that **Specify the config location on this router** is selected. Click the ellipsis (**...**) button. Click the plus sign (**+**) next to flash. Choose **ipsdir** and then click **OK**.



o. Because router memory and resource constraints might prevent using all the available signatures, there are two categories of signatures: basic and advanced. In the Choose Category field of the Config Location and Category window, choose **basic**. The Config Location and Category window should look similar to the following when the entries are completed.



p. Click **Next** in the Cisco CCP IPS Policies Wizard window. The Summary window appears. Examine the IPS configuration information shown.

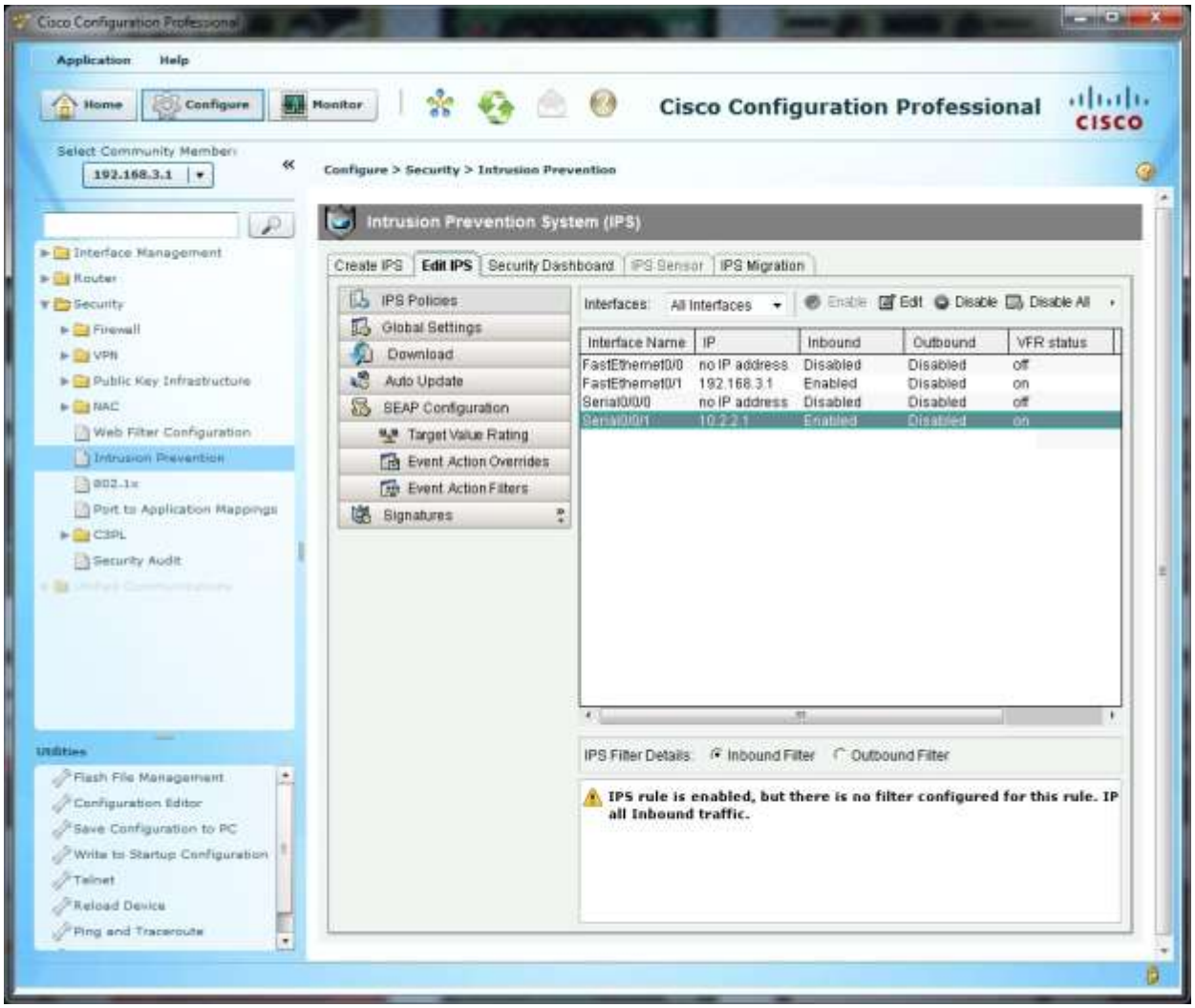


q. Click **Finish** in the IPS Policies Wizard window and review the commands that will be delivered to the router.

r. Click **Deliver**. How many commands were delivered to the router? _____

s. When the Commands Deliver Status window is ready, click **OK**. The IOS IPS Configuration Status window opens stating that it can take several minutes for the signatures to be configured.

t. When the signature configuration process has completed, you return to the IPS window with the Edit IPS tab selected. Your screen should look similar to the following.



u. Select interface Serial0/0/1 from the list. What information is displayed at the bottom of the screen?

_____

Task 5: Modify Signature Settings

Step 1: Verify connectivity.

From PC-C, ping R3. The pings should be successful.

Step 2: Configure the IPS application to drop ping (echo request) traffic.

a. From CCP, click **Configure** and choose **Security > Intrusion Prevention > Edit IPS > Signatures**. How many total signatures are there? _____

Are all of them enabled? _____

b. In the View By drop-down list, choose **Sig ID**.

c. In the **Sig ID** field, enter **2004**, and then click **Go**. What is Sig ID 2004?

_____

d. Do you know why the pings from PC-C in Step 1 were successful?

_____

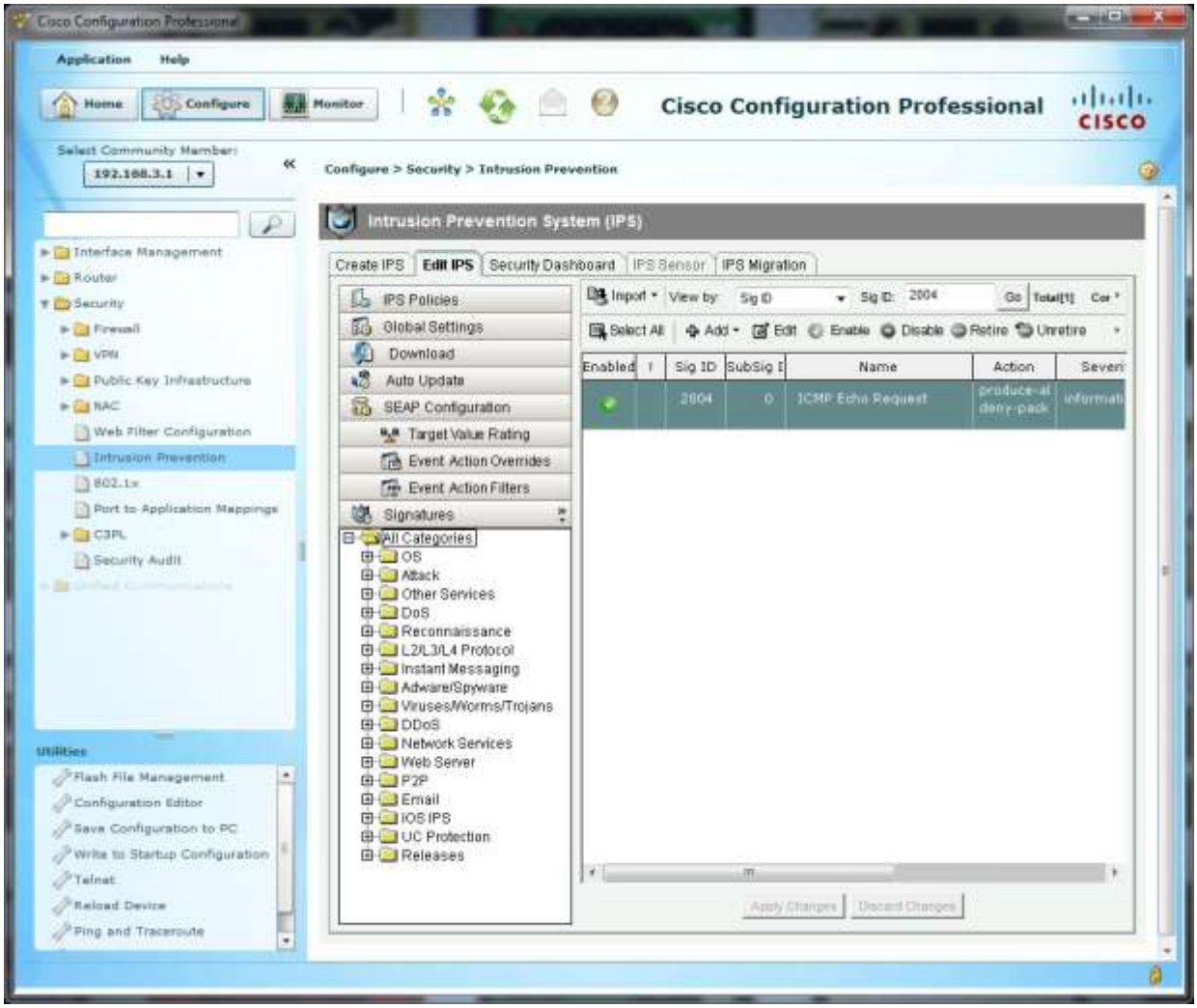
e. Select signature **2004**, click the **Unretire** button**,** and then click the **Enable** button.

f. Right-click the signature and choose **Actions** from the context menu.

g. Choose **Deny Packet Inline** and leave the **Produce Alert** check box checked. Click **OK**.

h. Click **Apply Changes**. It may take some time for the changes to take effect.

CCP 2.5 will list all the signatures again. Once again choose **Sig ID** in the View By drop-down list, enter **2004** in the **Sig ID** field and then click **Go**. Your screen should look similar to the following.



i. Return to PC-C and ping R3 again. Were the pings successful this time?

_____

Task 6: Configure IPS Global Settings Using CCP

In this task, you enable the syslog and SDEE global settings using the Cisco CCP GUI.

a. From CCP, click **Configure** and choose **Security > Intrusion Prevention > Edit IPS > Global Settings**.

b. Verify that the syslog and SDEE options are enabled.

Note: Even if the Syslog and SDEE options are already enabled, click the **Edit** button and explore the options available in the Edit Global Settings dialog box. Examine the options to learn whether Cisco IOS IPS has set the default to fail opened or to fail closed.

Task 7: Verify IPS Functionality with CCP Monitor and Ping

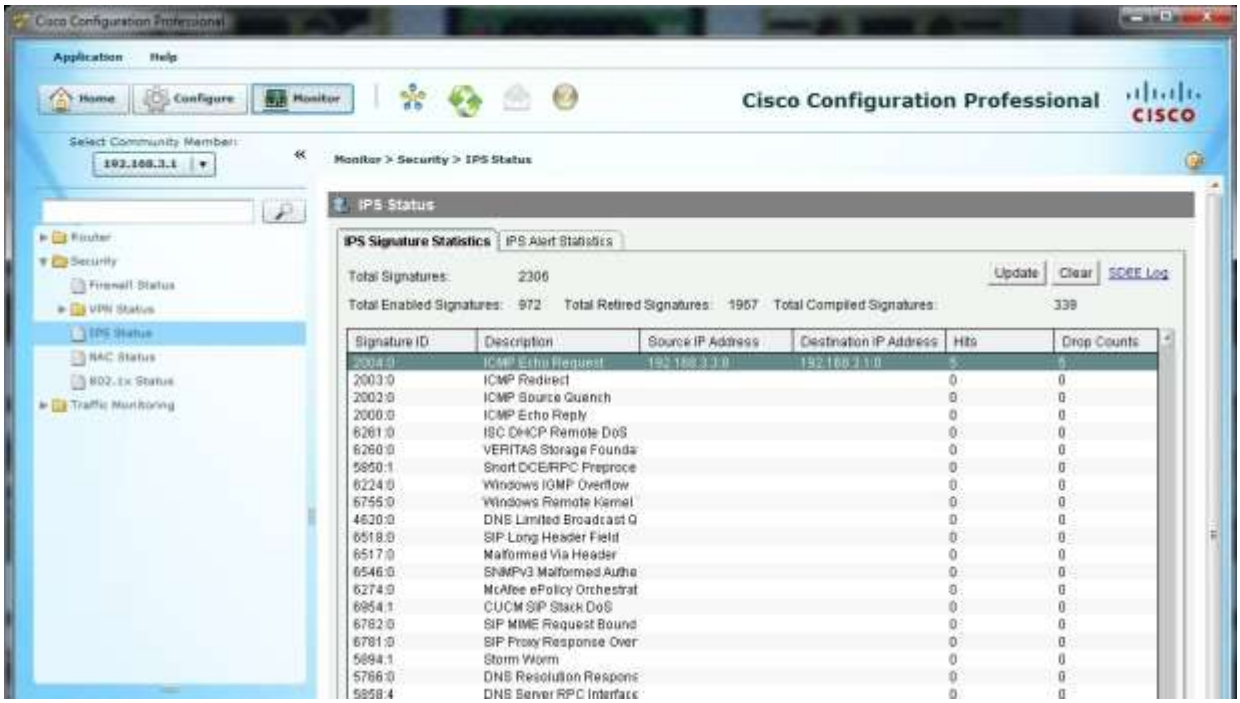
In this task, you demonstrate how the Cisco IOS IPS protects against an external attacker using ping.

a. From the R2 CLI, ping the R3 Fa0/1 interface at 192.168.3.1. Were the pings successful?

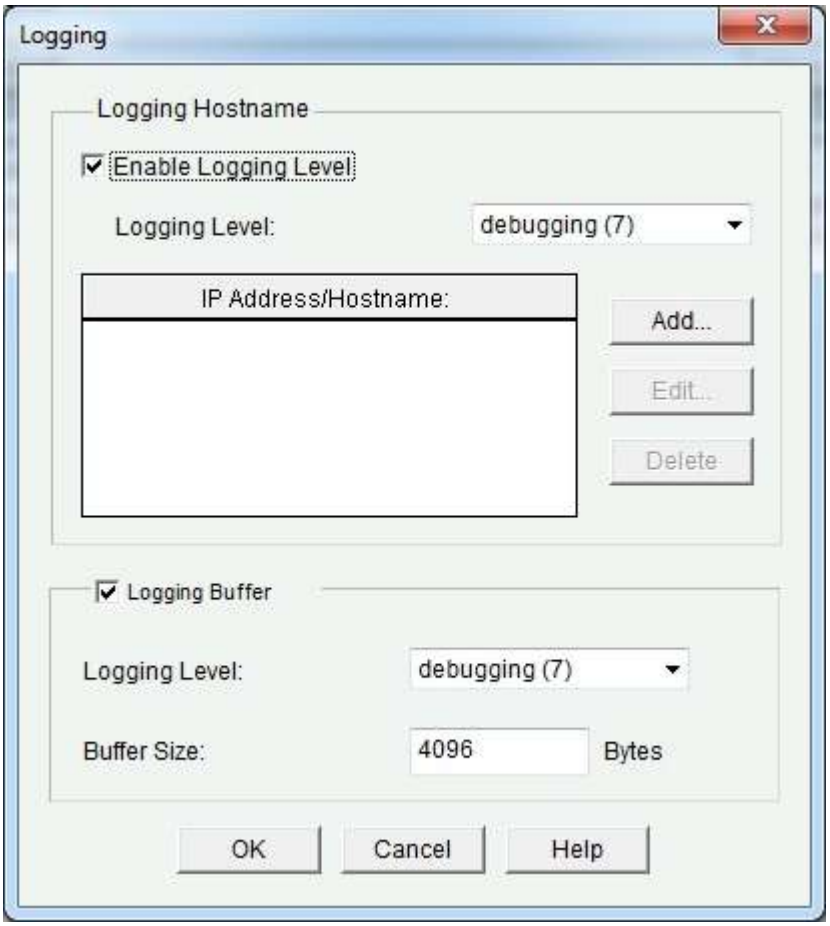
_____

b. From CCP, click the **Monitor** button and choose **Security > IPS Status**. The IPS Signature Statistics tab is selected by default. Wait for the screen to populate.

c. Scroll down to locate the signature ID 2004 ICMP echo request. You should see an entry similar to the one below indicating that IPS identified the ping attempt from R2. Notice that there are five hits and five drops for signature ID 2004, detected on Fa0/1 IP address 192.168.3.1.



d. From CCP, click the **Configure** button and choose **Router > Logging**. In the Additional Tasks window, ensure that Syslog is running on R3 by clicking on the **Edit** button. The window should be similar to this:

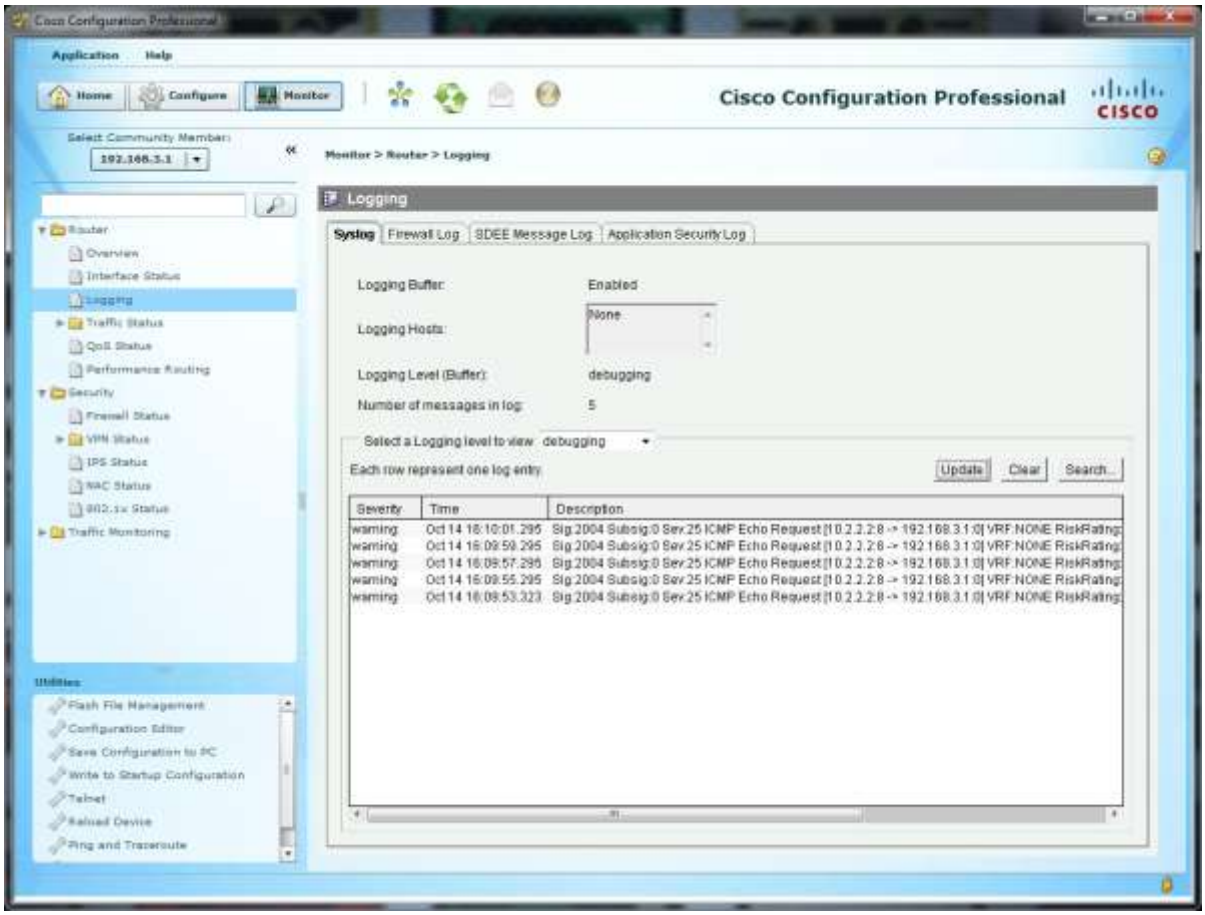


e. From CCP, click the **Monitor** button and choose **Router > Logging**.

f. A number of Syslog messages are displayed. Click the **Clear** button to clear the log.

g. From the R2 CLI, ping the R3 Fa0/1 interface at 192.168.3.1 again.

h. Click the **Update** button. You will see that the Cisco IOS IPS logged the ping attempts from R2.



Task 8: (Optional) Verify IPS Functionality with CCP Monitor and SuperScan

In this task, you will demonstrate how the Cisco IOS IPS protects against an internal attacker that is using SuperScan. SuperScan is a freeware scanning tool that runs with Windows XP that can detect open TCP and UDP ports on a target host. You can perform this task if the SuperScan program is available on PC-C or if it can be downloaded.

SuperScan will test the IPS capabilities on R3. You will run the scanning program from PC-C and attempt to scan open ports on router R2. The IPS rule iosips, which is set on R3 Fa0/1 inbound, should intercept the scanning attempts and send messages to the R3 console and CCP syslog.

Step 1: Download the SuperScan program.

a. If SuperScan is not on PC-C, download the SuperScan 4.0 tool from the Scanning Tools group at http://www.foundstone.com.

b. Unzip the file into a folder. The SuperScan4.exe file is executable and installation is not required.

Step 2: Run SuperScan and set scanning options.

a. Start SuperScan on PC-C. Click the **Host and Service Discovery** tab. Check the **Timestamp Request** check box, and uncheck the **Echo Request** check box. Scroll through the UDP and TCP port selection lists and notice the range of ports that will be scanned.

b. Click the **Scan** tab and enter the IP address of R2 S0/0/1 (10.2.2.2) in the **Hostname/IP** field.

Note: You can also specify an address range, such as 10.2.2.1 to 10.2.2.254, by entering an address in the Start IP and End IP fields. The program will scan all hosts with addresses in the range specified.

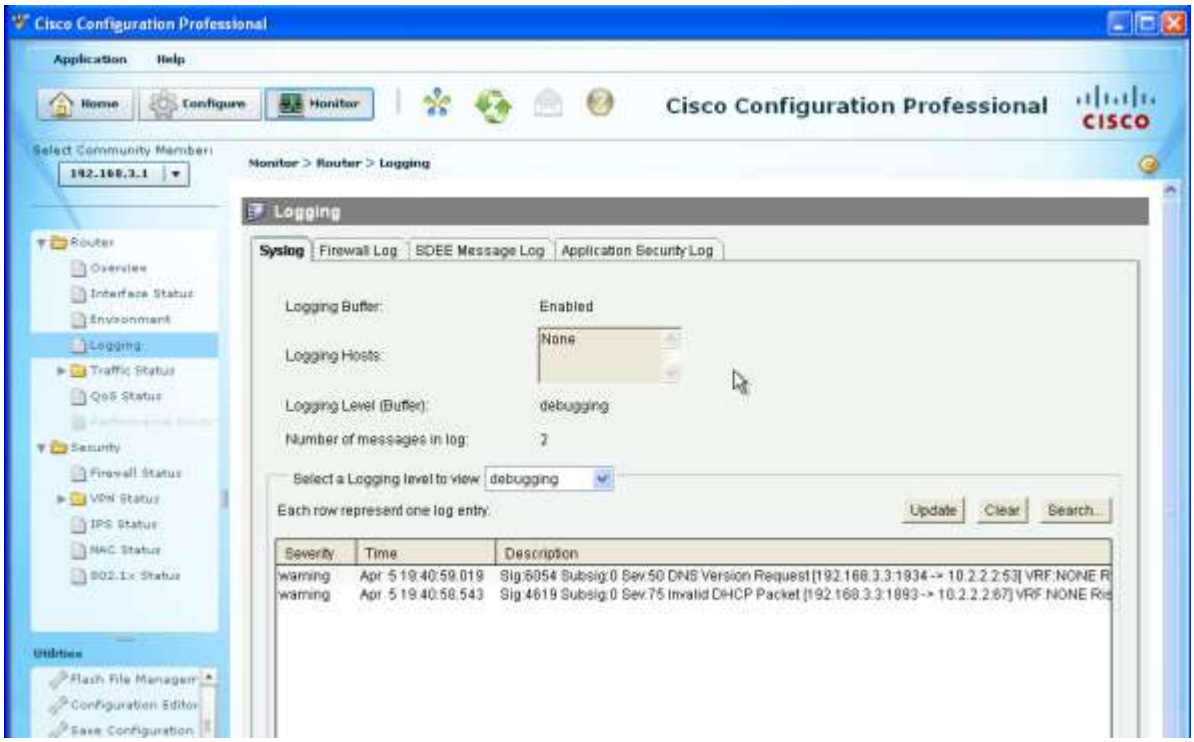
c. Click the button with the blue arrow in the lower left corner of the screen to start the scan.

Step 3: Check the results with CCP logging.

a. From Cisco CCP, choose **Monitor > Router > Logging**.

b. Click the **Update** button. You will see that the Cisco IOS IPS has been logging the port scans generated by SuperScan.

c. You should see syslog messages on R3 and entries in the CCP Monitor Log with descriptions that include one of these phrases: "`Invalid DHCP Packet`" or "`DNS Version Request`."



d. Close the SuperScan window.

Task 9: Compare the Results for Different IPS Configuration Methods.

a. On R1, display the running configuration after IPS was configured with IOS CLI commands. Note the commands related to IPS.

b. On R3, from the menu bar, choose **Utilities > View** > **Show Running Config** to display the running configuration after IPS was configured with the CCP GUI. Note the commands related to IPS.

c. What differences are there between the CLI-based running configuration and the CCP-based running configuration?

_____
_____
_____

Reflection

1. What are some advantages and disadvantages to using CLI or CCP to configure IPS?

_____
_____
_____
_____
_____

2. With version 5.x signature files, if changes are made to a signature, are they visible in the router running configuration?

_____
_____
_____
_____
_____

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				