CISCO SYSTEMS

CISCO NETWORKING ACADEMY PROGRAM

Network Security 1 v2.0

Instructor Lab Manual

Lab 1.1.1 Student Lab Orientation

Objective

In this lab, the students will complete the following tasks:

- Review the lab bundle equipment
- Understand the security pod topology
- Understand the pod naming and addressing scheme
- Load an IOS Firewall image
- Load the default lab configurations
- Cable the standard lab topology
- Test connectivity

Scenario

This lab describes the basics of cabling and configuring the standard lab topology for this course... Students will become familiar with the physical and logical topology that will be used throughout the course. To avoid problems with the lab exercises, proper lab setup and connectivity is required before configuring security. In real world scenarios, it is important to check the network for basic connectivity before proceeding with more advanced configurations.

Topology

Figure 1 illustrates the lab network environment used in the IOS Firewall router to IOS Firewall router lab activities. This topology will also be used in the labs that require configuration of the pod switches:

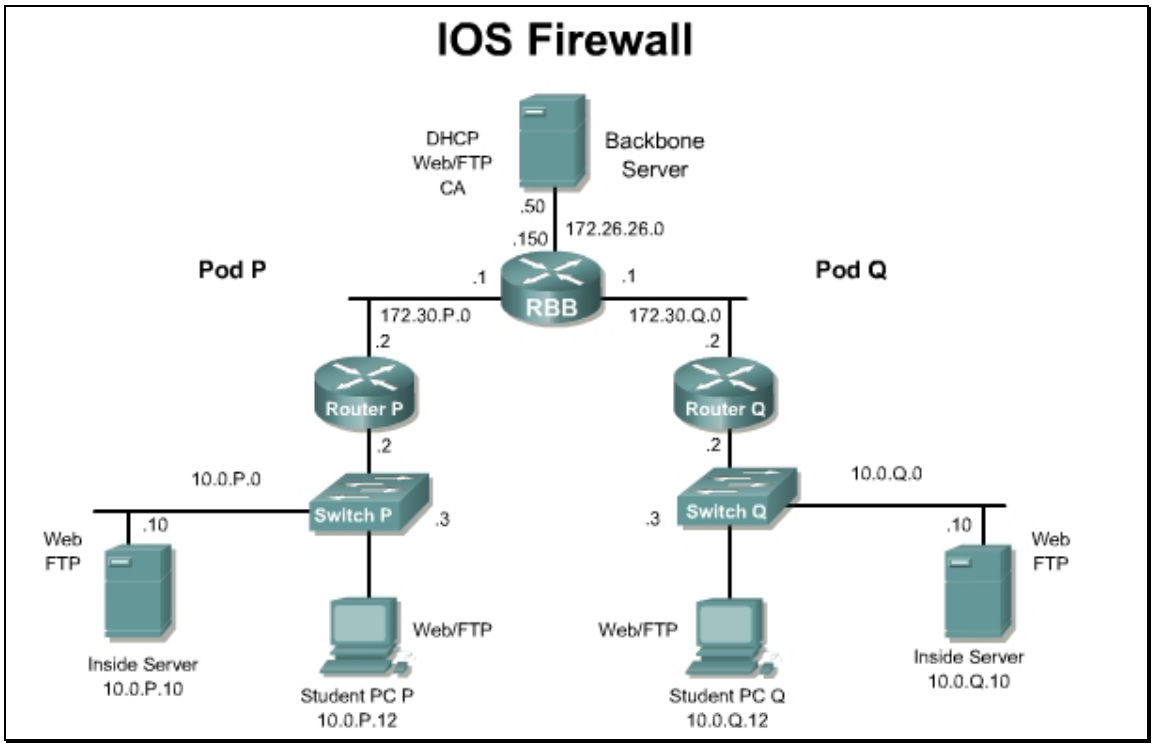


Figure 1

Figure 2 illustrates the lab network environment used in the VPN Client to IOS Firewall router lab activities:

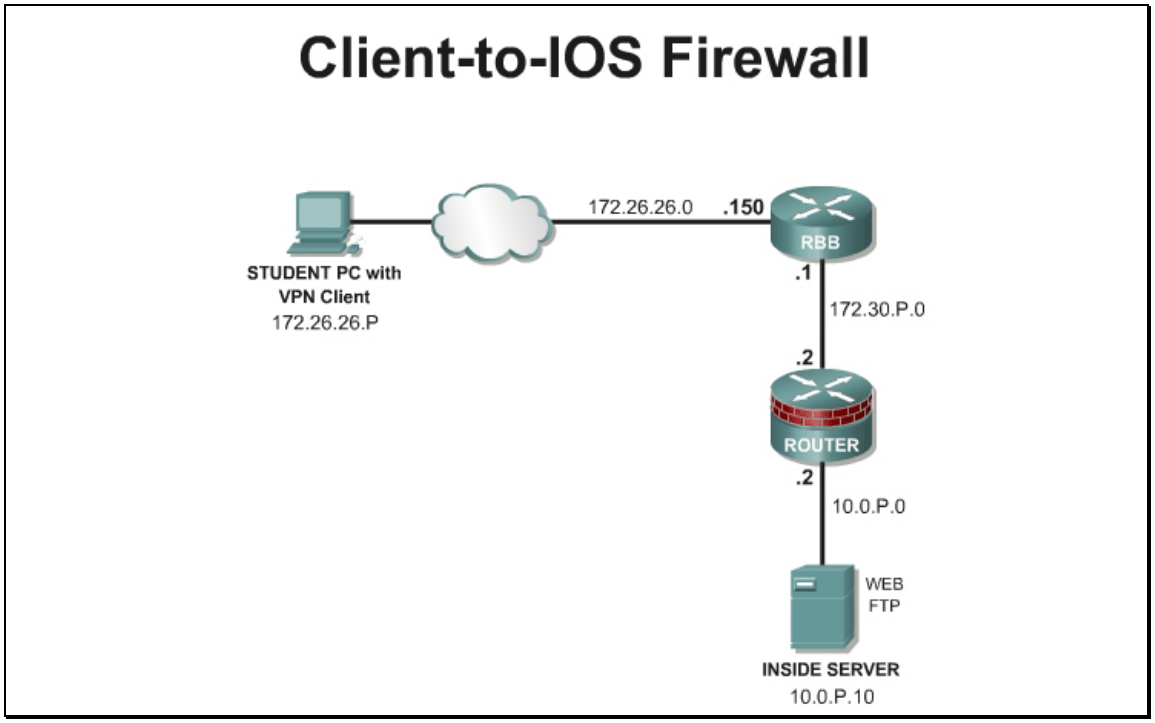


Figure 2

Figure 3 illustrates the lab network environment used in the PIX Security Appliance to PIX Security Appliance lab activities:

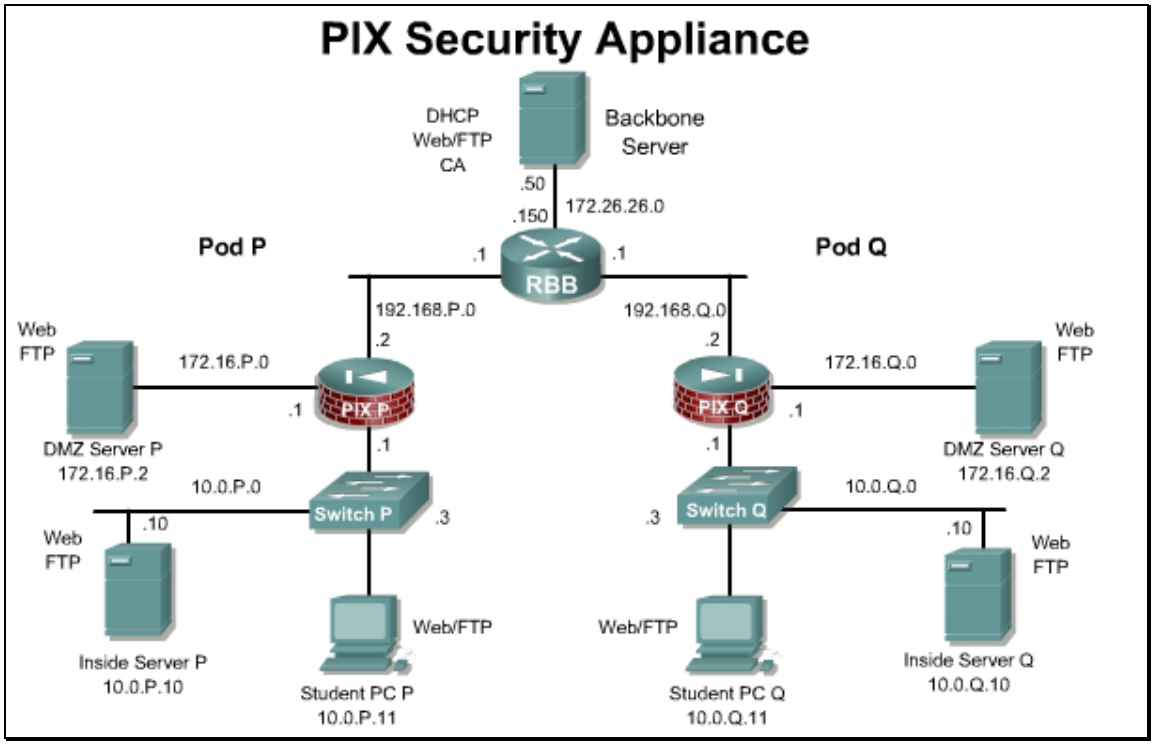


Figure 3

Figure 4 illustrates the lab network environment used in the VPN Client to PIX Security Appliance lab activities:

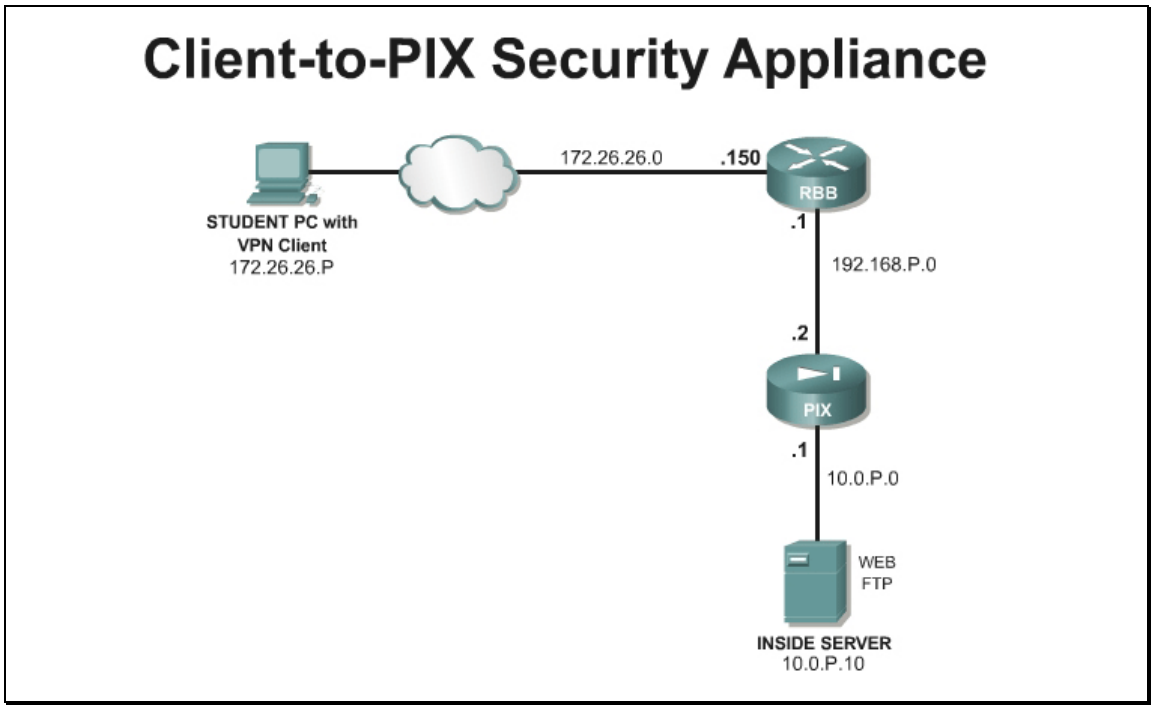


Figure 4

Figure 5 illustrates the logical topology with all of the devices connected.

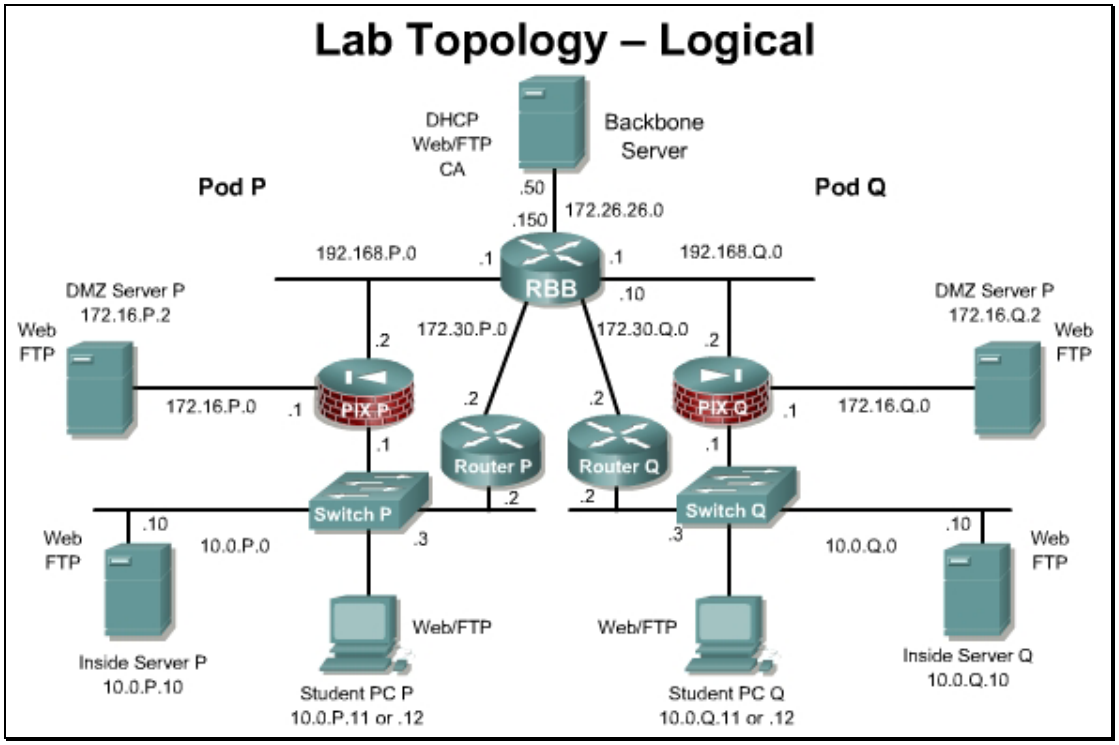


Figure 5

Preparation

There are two basic segments for the router topology:

Name	Trust Level	Common	Network	Physical Port
Inside	Trusted	Private-LAN	10.0.P.0/24	0/0
Outside	Untrusted	Public-WAN	172.30.P.0/24	0/1

There are three basic segments for the PIX Security Appliance topology:

Name	Trust Level	Common	Network	Physical Port
Inside	Trusted	Private - LAN	10.0.P.0/24	Ethernet0
Outside	Untrusted	Public-WAN	172.30.P.0/24	Ethernet1
Demilitarized Zone (DMZ)	Protected	Public Web Services	172.16.P.0/24	Ethernet2

In most of the labs, the physical interface will not be specific as Ethernet0, Fa0/0, E0/0 and so on. Instead, a lab will instruct students to configure the outside interface, the inside interface or the DMZ interface. Students will have to configure the interfaces based on the router or PIX Security Appliance model and interface characteristics.

Note that each topology figure indicates a specific numbering, naming and addressing scheme. The basic lab topology includes two pods. Each pod consists of a router, a PIX Security Appliance, a switch, a student PC, and an inside server. Some academies may have up to 10 pods. Therefore, the labs use **P** and **Q** values The **P** value in the addressing and naming scheme refers to the assigned Pod router that will be assigned to a team consisting of one to four students. The **Q** value in the naming and addressing scheme is used when testing the security or connectivity with the peer team. For example, the team on Pod 1 router is asked to Ping the neighbor router at 172.30.**Q**.2. In this case the **Q** will be substituted with a 2.

The basic tasks in most labs are:

- Configure security on the pod device, such as router or PIX Security Appliance.
- Test the security and services through the pod device and through the peer device.

When testing connectivity and security configurations, be careful to observe the prompt. Below are some possible prompts:

- **C:**
- **Router**>
- **http**://10.0.P.12
- **ftp**://172.26.26.50

This is important since testing will be performed from the DOS prompt, a device prompt, or a Web browser.

Tools and Resources:

In order to complete this lab, the following is required:

- Two pod IOS Firewall routers (ROUTER)
- Two pod PIX Security Appliances (PIX)
- Two pod switches (SW)
- Two student PCs (PC) located at 10.0.P.12
- Servers
    - Setup Option 1-Dedicated Devices
        - One Backbone_Internet (BB) Server
        - Two Inside Servers (IS) located at 10.0.P.10
        - Two DMZ Servers (DMZ) located at 172.16.P.2 (Routers can be substituted)
    - Setup Option 2-SuperServer
        - One SuperServer (SS) with Intel Pro Server NIC with VLAN support. The VLAN NIC is only needed if using the SuperServer model.
- One Backbone switch
- One Backbone router
- Two console cables
- HyperTerminal
- Assorted Cat5 patch cables
- One Label machine (Optional)

Additional Materials

None

Command List

In this lab, the following commands will be used to configure the pod routers:

Command	Description
copy run start	Stores the current configuration in RAM into NVRAM.
copy tftp flash	Downloads a new image from the TFTP server to Flash memory.
copy tftp start	Downloads a configuration from the TFTP server into the

Command	Description
	NVRAM
enable	Turns on privileged commands.
show interface	Displays statistics for all interfaces configured on the router.
show ip interface	Displays the status and global parameters associated with an interface.
show ip route	Displays the contents of the IP routing table.
show running-config	Displays the current configuration in RAM
show startup-config	Displays the saved configuration that is stored in NVRAM
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

Step 1 Examine the Devices

a. Physically examine each device. Notice the interfaces available on the IOS Router and PIX Security Appliance that are present in the lab environment.

b. Notice the devices are labeled with an adhesive label. Below is a sample list of devices that should be labeled:

Router	**PIX**	**Switch**	**Student PCs**
Router1	Pix1	Switch1	Student PC 1
Router2	Pix2	Switch2	Student PC 2

Device	**IP Address**	**Description**
RBB	172.26.26.150	backbone router
SW0	172.26.26.200	backbone switch
BB	172.26.26.50	Backbone/Internet server
Inside Server 1	10.0.1.10	Inside Server – Pod 1
Inside Server 2	10.0.2.10	Inside Server – Pod 2
DMZ Server 1	172.16.1.2	DMZ Server – Pod 1
DMZ Server 2	172.16.2.2	DMZ Server – Pod 2

The standard FNS lab bundle equipment will create two standard pods. Each pod can accommodate one team consisting of one to four students. Two students per pod is recommended.

Step 2 Configure Student PCs (PC1, PC2)

a. On the Student PCs, log in as administrator. Verify that the following list of installed software packages is located on the PC as directed by the instructor:

- Cisco Secure ACS v3.3 – It is recommended that the student PCs must be running Windows 2000 Server to install ACS. If the students PCs are not running Windows 2000 Server, ACS can be installed and run on the Inside servers or the Backbone server. This will require adjustments to the labs using ACS, when defining the AAA server address.
- Syslog Server – Kiwi or equivalent
- SSH Client – Putty.exe or equivalent
- Reconnaissance Tools – such as NMapWin and SNMPWalk
- VPN Client – Cisco VPN Client 4.6
- TFTP Server – SolarWinds TFTP Server or equivalent
- Other applications provided by the instructor

b. Verify the i386 folder is located on the root drive C:\. This folder is used when adding any Windows components without the Windows Installation CD.

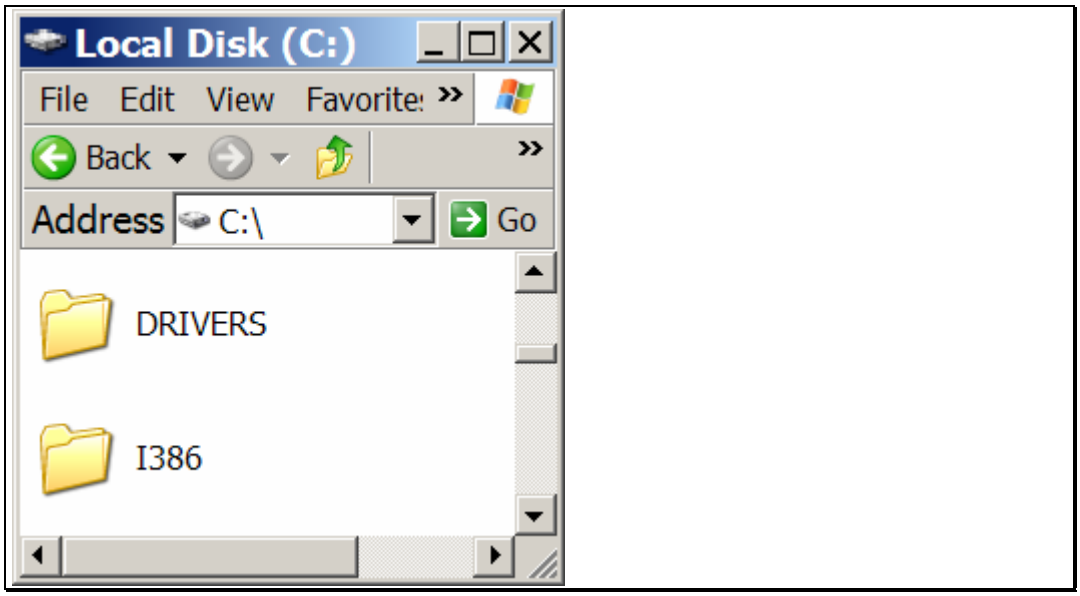


Figure 6

c. Verify that HyperTerminal or equivalent terminal emulation software is installed.

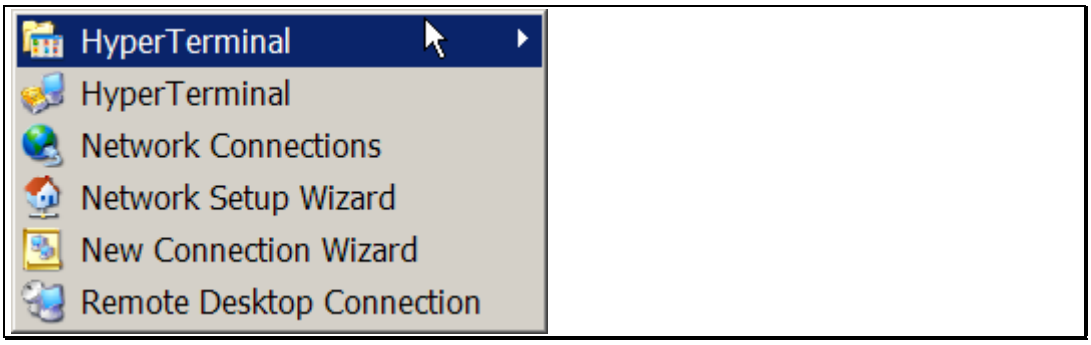


Figure 7

d. Configure the Student PCs TCP/IP settings and services. For this lab activity, use the router to router settings shown below.

These settings will be used for the router to router labs:

Label	Computer Name	Address	Gateway
Student PC1	PC1	10.0.1.12/24	10.0.1.2
Student PC2	PC2	10.0.2.12/24	10.0.2.2

These settings will be used for the PIX Security Appliance to PIX Security Appliance labs:

Label	Computer Name	Address	Gateway
Student PC1	PC1	10.0.1.11/24	10.0.1.1
Student PC2	PC2	10.0.2.11/24	10.0.2.1

e. Configure web and FTP services on the Student PCs. The instructor will provide default web pages to install in the wwwroot directory. Place the default configuration of all pod devices in the ftproot directory. The wwwroot and ftproot directories are located in C:\Inetpub by default.

f. Verify the web and FTP sites have been properly configured by opening Internet Services Manager (IIS) or equivalent web services if using another operating system or web server application. To verify that IIS is running, right click the My Computer icon and select **Manage** from the pop-up menu. Click the **+** icon next to **Services and Applications** to expand the menu and locate IIS.

Step 3 Verify the Lab Topology Cabling

Figure 8 illustrates a port mapping of SW0 in order to cable or verify the physical connections for the dedicated server setup option. Labeling the switch helps facilitate quick recabling when necessary.

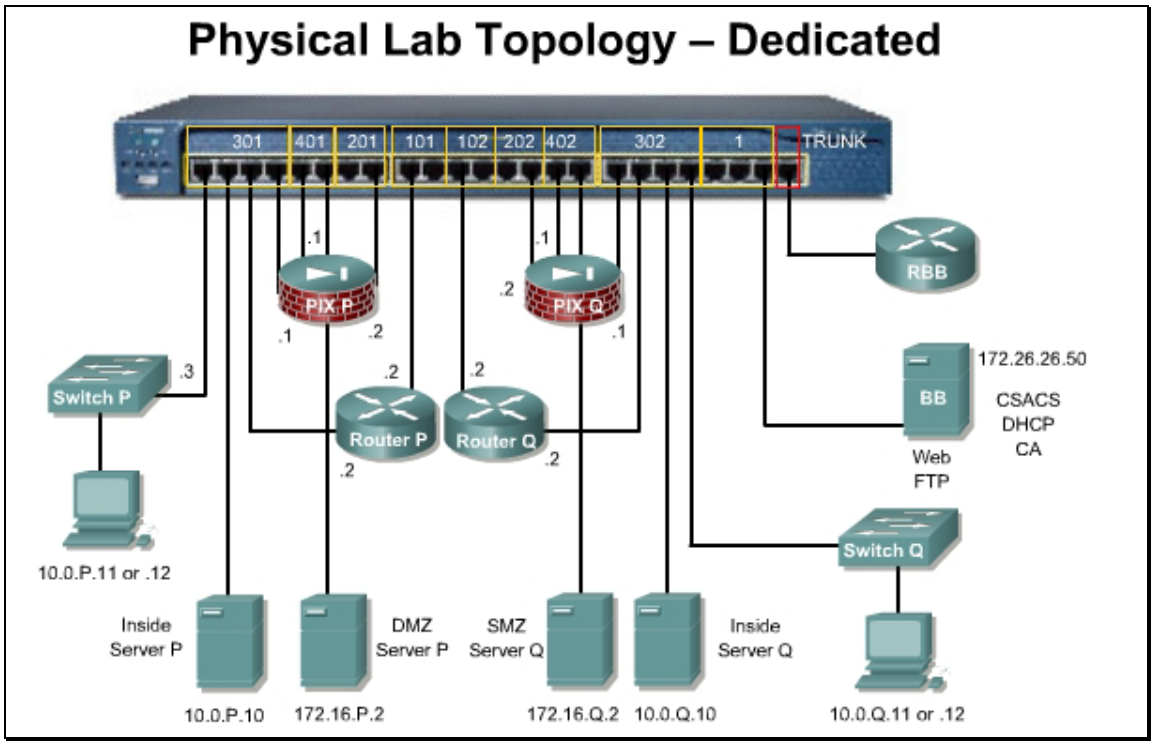


Figure 8

Figure 9 illustrates a sample port mapping of SW0 in order to cable or verify the physical connections for the SuperServer setup option. Labeling the switch helps facilitate quick recabling when necessary.

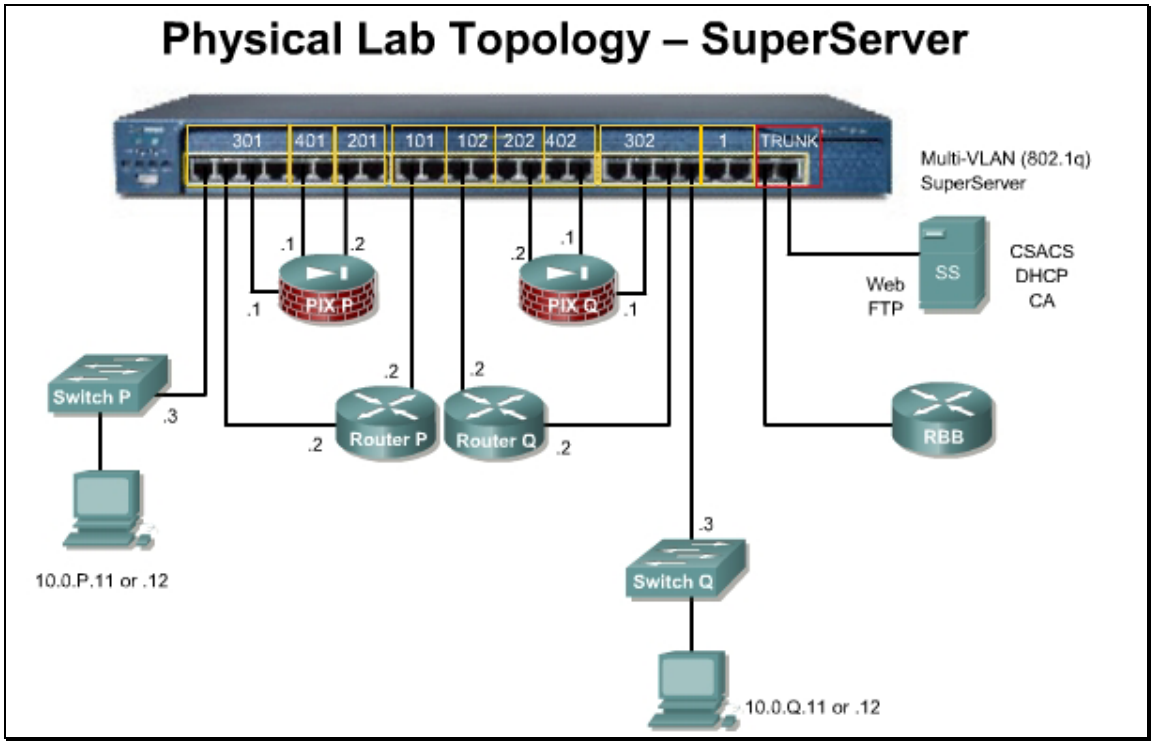


Figure 9

Step 4 Verify the Software Images on the Pod Devices

a. Power and test the pod devices. If needed, refer to the appendices to upgrade the IOS image.

Platform	Release	Images
2610XM-2611XM	12.3(14)T Advanced Security	c2600-advsecurityk9-mz.123-14.T1.bin
PIX 515E	7.0(1)	pix701.bin
Catalyst 2950, 2950T	12.1(22)	c2950-i6k2l2q4-mz.121-22.EA4.bin

The router image must be 12.3(8)T or above, as the IOS Intrusion Detection commands are significantly different in earlier IOS versions. If the router has an image that is earlier than 12.3(8)T, the image must be upgraded.

Security Device Manager (SDM) version 2.0 or later will be required for some of the labs. The PIX pod devices should have version 7.0 or higher with Adaptive Security Device Manger (ASDM) version 5.0.

Step 5 Load Default Configurations on Pod Routers

a. Reload, configure and verify Pod routers.

b. On the respective router, load the following configuration. These text files are available from the instructor.

Pod Router 1	Pod Router 2
hostname Router1 ! logging console enable password cisco ! username sdm privilege 15 password 0 sdm ! no ip domain-lookup ! ip dhcp excluded-address 10.0.1.1 10.0.1.12 ! ip dhcp pool POD1_INSIDE network 10.0.1.0 255.255.255.0 default-router 10.0.1.2 ! interface FastEthernet0/0 description inside ip address 10.0.1.2 255.255.255.0 no shutdown ! interface FastEthernet 0/1 description outside ip address 172.30.1.2 255.255.255.0 no shutdown ! router eigrp 1 network 10.0.0.0 network 172.30.0.0 no auto-summary ! ip classless ip http server ip http authentication local ! line vty 0 4 password cisco privilege level 15 transport input telnet ssh login local ! end	hostname Router2 ! logging console enable password cisco ! username sdm privilege 15 password 0 sdm ! no ip domain-lookup ! ip dhcp excluded-address 10.0.2.1 10.0.2.12 ! ip dhcp pool POD2_INSIDE network 10.0.2.0 255.255.255.0 default-router 10.0.2.2 ! interface FastEthernet 0/0 description inside ip address 10.0.2.2 255.255.255.0 no shutdown ! interface FastEthernet0/1 description outside ip address 172.30.2.2 255.255.255.0 no shutdown ! router eigrp 1 network 10.0.0.0 network 172.30.0.0 no auto-summary ! ip classless ip http server ip http authentication local ! line vty 0 4 password cisco privilege level 15 transport input telnet ssh login local ! end

c. Verify the router configuration and save it to flash.

```
RouterP#show run
RouterP#copy run start
```

The instructor will configure and verify RBB, SW0, and the basic configuration of the pod switches unless directed otherwise by the instructor.

Step 6 Test Connectivity

a. Verify that the router interfaces are up.

```
RouterP> show ip interface brief
```

b. Verify the routes.

```
RouterP> show ip route
```

c. From the router, ping the outside interface of the peer router.

```
RouterP> ping 172.30.Q.2
```

d. From the PC, ping RBB and the Backbone Server.

```
C:\ ping 172.26.26.150
```
and
```
C:\ ping 172.26.26.50
```

e. From the Student PC, ping the Inside Server.

```
C:\ ping 10.0.P.10
```

f. From a browser on the Student PC, access the ftp/web page of the Inside Server

```
http://10.0.P.10
```
and
```
ftp://10.0.P.10
```

g. From the Student PC, ping the inside PC of the peer.

```
C:\ ping 10.0.Q.12
```

h. From a browser on the Student PC, access the web/ftp page of the Backbone Server

```
http://172.26.26.50
```
and
```
ftp://172.26.26.50
```

i. From a browser on the Student PC, access the ftp page of the peer PC

```
http://10.0.Q.12
```
and
```
ftp://10.0.Q.12
```


Lab 1.3.4 Vulnerabilities and Exploits

Objective

In this lab, the students will complete the following tasks:

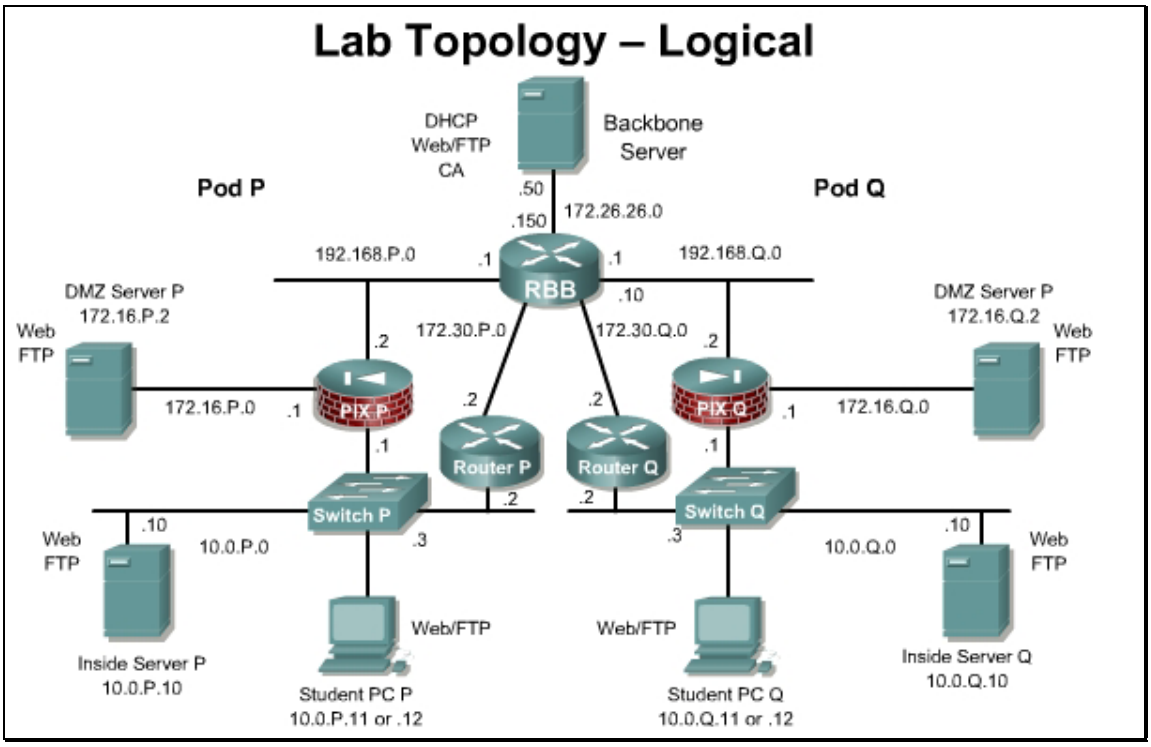
- The use of common network mapping tools, hacking programs, and scripts on a LAN and across a WAN.
- Where vulnerabilities are discovered, propose a fix or solution to the problem.

Scenario

A small company is using the topology discussed in the following topic. Assume that minimal security measures have been implemented. Discover vulnerability in any of the devices or software used in the network. This includes routers, switches, workstations, printers, servers, hubs, and wiring. The students will demonstrate this solution in the lab environment for observation by peers and the instructor.

Topology

This figure illustrates the network environment that will be used in this lab.



Preparation

Use the standard lab topology and startup router configuration for the Pod router. Configure the additional devices with the appropriate network address, gateway, and subnet mask if required.

Part I: Students or small groups will be stepped through the process of using a bootable Linux Security CD on the Student PC. Programs such as Nessus and Ethereal will be used to scan for vulnerabilities on the Pod router, Inside server, or other select targets on the lab topology. This lab is written to use the Local Area Security Linux CD.(200MB)

Part II: Students or small groups will conduct a search for one known vulnerability or exploit, or utilize one of the many tools on the Linux security CD. This lab can be repeated to allow students to experience each type of tool. Some of the common tools used are listed in the following:

- Reconnaissance
  - Network/packet sniffers or port scanners
  - Key loggers
  - Simple Network Management Protocol (SNMP) or other network management/configuration tools
- Access
  - Java, ActiveX or cgi scripts
  - Self executing software
  - Robots and control daemons
  - SNMP or other network management/configuration tools
  - Password tools such as brute force, dictionary, and so on
- Denial of service
  - Ping of death
  - SYN flood, User Datagram Protocol (UDP) bomb, and so on

Commands

Command	Description
ifconfig	Display the IP address settings for a Linux device
ping	Verify Layer 3 connectivity to another device.
sudo bash	Change to the root user in linux
telnet	Initiate a telnet connection with a remote device.

For this lab students can use any host PC or server for demonstration or implementation.

Tools and resources

To complete this lab, students should have access to the following equipment:

- Standard lab topology setup
- Bootable Linux security CD (Local Area Security Linux or equivalent)
  - There are numerous bootable Linux CDs available such as Local Area Security Linux, Knoppix STD, F.I.R.E., Auditor security collection, and many others. They range in size from 50MB to 750MB.
  - A bootable Linux Security CD allows a student to access many tools without the installation issues on Windows platforms.
  - The images run in RAM and typically do not affect the operating system on the PC.

Additional materials

The curriculum lists several excellent Web links that will help the student understand the material presented in these labs.

Other resources include these websites:

- http://www.2600.com/
- http://www.cert.org
- *Hacking Exposed: Network Security Secrets & Solutions*, Fourth Edition by Stuart McClure, Joel Scambray, George Kurty
- http://www.localareasecurity.com/
- http://www.moser-informatik.ch
- http://www.nessus.org
- http://www.ethereal.com/

Safety

Students and instructors must be careful not to violate any local, state, or federal laws as well as school or university network security policies. Using a bootable Linux security CD provides the tools with minimal risk and configuration requirements. However, it may be necessary to re-image or reload a workstation, device, or server operating system (OS) in order to completely eliminate any malicious code, virus, Trojan horse, or control daemon encountered in this lab.

Part I:

Step 1 Boot the Student PC (laptop) with the Linux CD

The Student PC will receive an address from the pod router DCHP server. Make sure the starting configuration is loaded on the Pod device, which has the DHCP server running.

a. On the powered down Student PC or laptop, insert the LAN Security CD into the CD ROM drive.
b. Power the Student PC or laptop
c. Assure the laptop boots into the Linux environment. This procedure will vary depending on the PC and laptop brand and current BIOS configuration. The Linux distribution may not support all hardware properly. If some of the PC hardware components are not detected, load the Linux distribution on another PC or laptop.
d. Open a Linux shell. **Apps>Shells>Bash** and verify the PC has an IP address in the 10.0.P.0/24 network range.

```
root@0[root]$ ifconfig
```

Step 2 Execute Nessus via GUI or CLI

GUI menu steps

a. Right click on the desktop, and navigate to **Apps>I.a.s>nessus**
b. Left click on the **nessus** application

CLI menu steps

a. Open a Linux shell. **Apps>Shells>Bash** Become root in your terminal if not already root.

```
root@0[root]$ sudo bash
root@0[root]#
```

b. First, start the nessus daemon and put the process in the background.

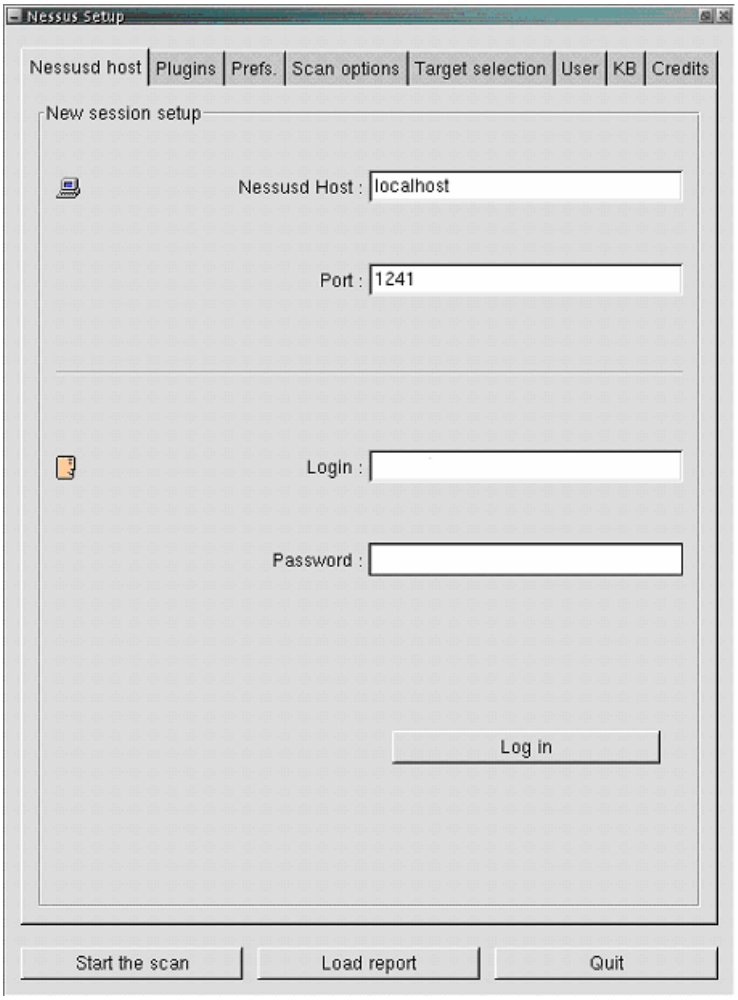
```
root@0[root]# nessusd&
```

c. Launch the nessus client.


```
root@0[root]# nessus&
```

Step 3 Log into the Nessus client

a. Login with the username **root** and password **root**
b. Click the **Log in** button



c. Click the **OK** button after reading the Warning message.

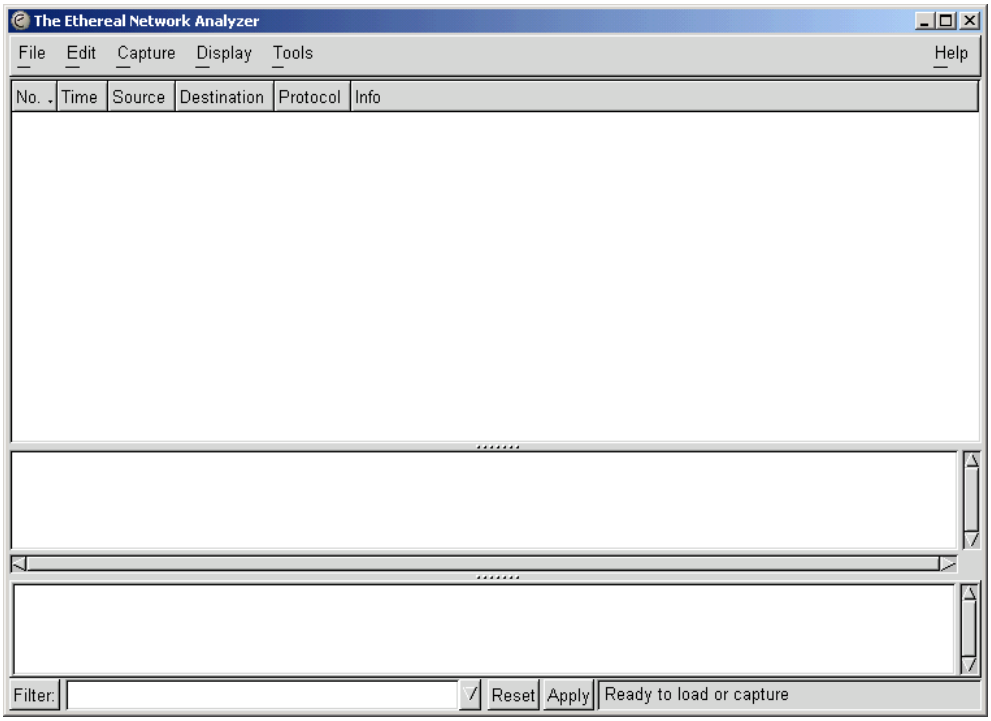
Step 4 Modify the Nessus Scan Options

a. Select the **Plugins** tab. Include all attacks, by clicking on the **Enable All** button. This should enable the dangerous plugins as well.
b. Select the **Prefs** tab. This tab displays the scanning options. Some of these options are options, such as scanning speed and scan type, are meant to be used with Nmap, and other options are passed to different Nessus modules. A few of the options on this page can be changed to speed up the scans.
    i. Change the ping type from TCP to ICMP.
    ii. Next, change the port selections to choose the **Fast scan (nmap-services)** instead of user specified ports.
c. Select the **Scan Options** tab. Some of these options are passed to NMAP, and other options affect the amount of information that is gathered. Make the following changes:
    i. Change the number of hosts to test to 5
    ii. Disable the LaBrea tarpit scan, if it is not already disabled.

d. Now choose the **Target Selection** tab. In the targets field, enter the network address of 10.0.P.2, 10.0.P.10, or another select host. The following options can be used to define the targets:
   i. A single IP address: For example, the IP address of the Pod device's inside interface.
   ii. A range of IP addresses: 10.0.1.1-254
   iii. Another range of IP addresses: 10.0.1.1-10.0.1.254
   iv. Again a range of IP addresses in CIDR notation: 10.0.1.1/24
   v. A hostname in Full Qualified Domain Name notation: Router1.cisco.com
   vi. A hostname (as long as it is resolvable on the server). Router1
   vii. Any combination of the aforementioned forms separated by a comma: 10.0.1.2, 10.0.1.10, 10.0.1.1

Step 5 Start the Scan and Monitor the packets using Ethereal

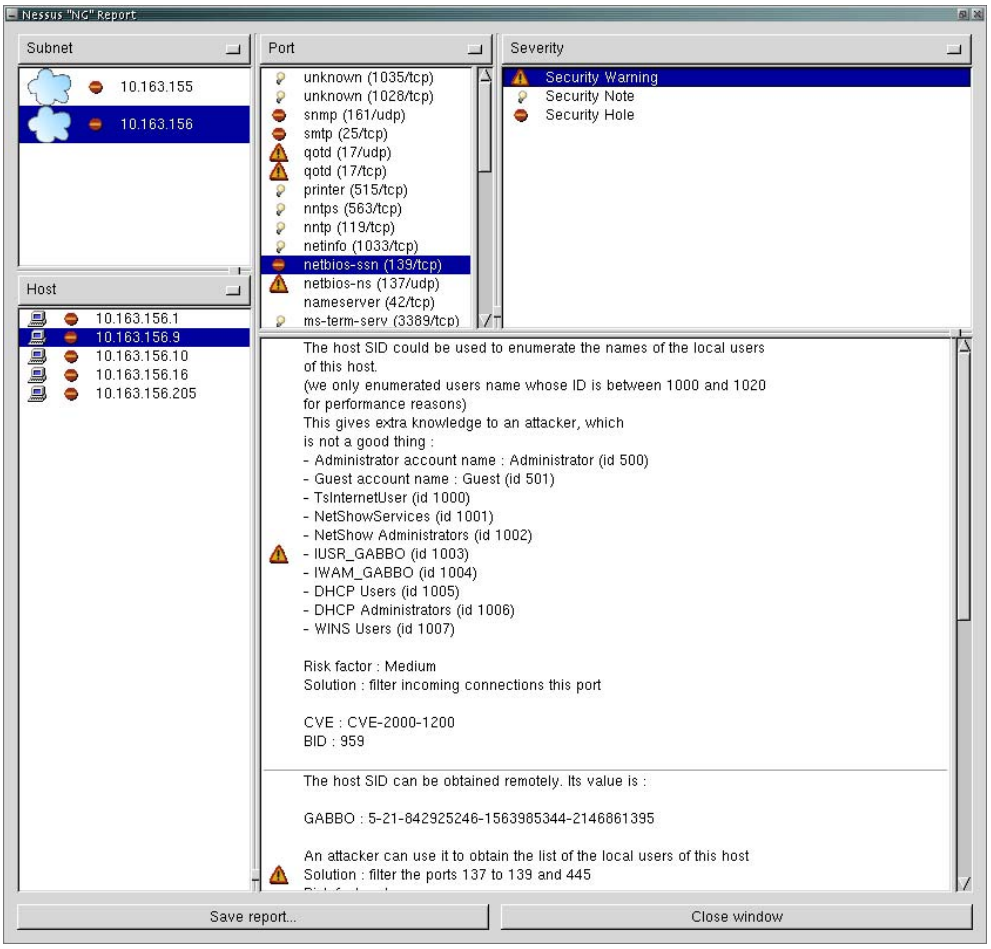
a. Click **Start the Scan**.
b. While the Scan is running, go to **Apps>I.a.s>Ethereal**



c. Start a capture. **Capture>Start.**
d. Click the **OK** button.
e. Allow Ethereal to capture about 100 packets, then stop the capture.
f. View the packets and notice the various types of IP traffic (TCP, ICMP, HTTP) which is part of the scan.

Step 6 View the vulnerabilities

a. Let the scans complete, and then check the results displayed in the Nessus window.



b. Four boxes of results will be displayed after the scan. Check through the results and see what vulnerabilities were identified.

c. If you have a question about the vulnerabilities you identified, you can perform a quick Internet search using Google or another search engine.

d. When you are finished using Linux on your PC or laptop, enter the **`halt`** command at the Bash prompt to exit Linux and then restart your computer after removing the Linux CD.

Part II:

Step 1 Research an exploit or vulnerability

a. Research on the Internet one known exploit, script, or software tool of your choice. Or, use another tool available on the Linux security CD.

1. What is the filename, program name, and exploit name?

Answer: Answers will vary.

b. Obtain instructor approval, and then install the file. Make sure that instructor approval has been obtained before downloading or executing.

1. What is the filename of the executable that has been downloaded?

Answer: Answers will vary.

2. How long did it take to find the desired exploit, script, and software tool?

Answer: Answers will vary.

3. What was the source of the file, exploit, or vulnerability?

Answer: Answers will vary.

4. Describe the target device in terms of its name, model, OS, and function in the network.

Answer: Answers will vary.

5. What source device or operating system is required to implement this exploit or vulnerability?

Answer: Answers will vary.

6. Is this a known exploit? Who posted the advisory? Did the vendor acknowledge the problem? What are the recommended countermeasures?

Answer: Answers will vary.

7. Are there any additional tools or knowledge required to implement this exploit or vulnerability?

Answer: Answers will vary.

8. What is the projected cost to implement this exploit or vulnerability?

Answer: Answers will vary.

9. How difficult is it to implement this exploit or vulnerability?

Answer: Answers will vary.

10. What is the projected damage or cost to a victim's network if this exploit is used against it? Which devices are most impacted?

Answer: Answers will vary.

Step 2 Install, configure, and execute software tool

a. Install, configure, and execute one of the software tools.

1. How long did it take to install and configure this tool?

Answer: Answers will vary.

2. What were the results? Did the tool perform as anticipated? Why or why not?

Answer: Answers will vary.

3. If the target device was unaffected, what measures were taken to prevent the exploit?

Answer: Answers will vary.

Step 3 Fix the problem caused by the exploit

a. Fix the problem or damage caused by the exploit.

1. Is the damage easily reversed or remedied?

Answer: Answers will vary.

2. What is the time required to perform the repair or fix?

Answer: Answers will vary.

Step 4 Find a solution to the exploit

a. Find or propose a solution to this exploit or vulnerability.

1. Describe the proposed permanent solution or prevention.

Answer: Answers will vary.

2. With the approval of the instructor, implement the solution. How long did it take to implement the solution?

Answer: Answers will vary.

3. How difficult was it to implement or apply the solution or patch? What obstacles were encountered?

Answer: Answers will vary.

4. If a corporation has hundreds or thousands of the same target devices that are subject to the same exploit, how could a solution be implemented?

Answer: Answers will vary.

Step 5 Verify that the fix solved the problem

a. It is easy to go through the motions of installing a patch or fix without verifying that it actually solved the problem. Return to Step 2 and repeat the steps.

1. Did the solution prevent the exploit or vulnerability?

Answer: Answers will vary.

Step 6 Demonstrate the exploit

a. Demonstrate the exploit or vulnerability to other students and the instructor.

1. Did it function as planned?

Answer: Answers will vary.

Step 7 Reset all lab devices

a. Reset all lab devices and re-image the computers or devices if necessary or directed by the instructor.

Lab 2.1.2 Designing a Security Plan

Objective

In this lab, students will analyze, offer recommendations, and help improve the security infrastructure of a fictitious business. Students will complete the following tasks:

- Analyze business application requirements.
- Analyze security risks.
- Identify network assets.
- Analyze security requirements and tradeoffs.

Scenario

Widget Warehouse is a medium sized e-commerce company that supports 200 customers daily. The student has been hired to assist in the development of a new security policy. An assignment has been received to analyze the current network of Widget Warehouse. The Widget Warehouse network is comprised of an intranet with 200 users, and a public Web server that processes the company e-commerce traffic. The internal network is logically divided into an information technology (IT) department branch, an accounting branch, a customer service branch, a sales branch, and an inventory branch.

Preparation

To complete this lab, the students should have a firm understanding of the various security exploits that pose a risk to companies.

Tools and resources

The curriculum lists a number of excellent Web links that will help the student understand the material presented in these labs:

- Carnegie Mellon Software Engineering Institute or CERT http://www.cert.org
- National Institute of Standards and Technology Security Division or NIST http://csrc.nist.gov/

Step 1 Create a list of various attack intruders

a. The IT department for Widget Warehouse has a general understanding of security but they are very inexperienced with the various attacks an intruder can use to exploit their network resources. Create a list of various attacks intruders can use maliciously against the Widget Warehouse network. Also, provide a brief description of possible attacks, including their purpose.

Attack Name	Attack Description

Answers:

Attack Name	Attack Description
Masquerade	An attack where the intruder assumes the identity of a valid users. For example, an intruder can spoof a trusted IP address and gain access to confidential information.
Session Replay	This is when a trusted communication session is recorded by an intruder and later played back to impersonate the trusted sessions.
Denial of Service	This is when an intruder floods network resources with numerous requests. This attack can result in a crash of network devices or slower performance.
Data Manipulation	With data manipulation, the network intruder can capture, manipulate, and replay data sent over a communication channel.
Port Redirection	Attacks where intruders use a compromised host to pass traffic through a firewall that would otherwise be dropped.
Social Engineering	This is when an intruder manipulates people, usually by claiming to be the person in charge of the network, to gain access to network resources.
Backdoors	Paths into systems that can be created during an intrusion or with specifically designed Trojan horse code.
Trojan horse	A generic term used to describe a malicious program that masquerades a useful or harmless utility.
E-mail bombs	Usually a free program that will send bulk e-mails to individuals, lists, or domains, monopolizing e-mail services.

Step 2 Make a List of Security Requirements

a. One of the first steps in creating a security policy is gathering the requirements for the company. Create a list of questions to ask the Widget Warehouse executives, in order to better understand their security requirements and business goals.

1. Widget Warehouse requirements.

_____

_____

_____

_____

_____

Answer: (answers will vary)

1. What resources are mission-critical?
2. What information is considered sensitive?
3. If compromised, what could be the potential cost to your business?
4. What is the available budget for securing your network?
5. What is the cost of downtime of mission-critical services or resources?
6. If your e-commerce site is unavailable to the customer, how much business will be lost?
7. How much interaction is there amongst internal departments?

Step 3 Identify Security Implementation Options

a. Based on the questions, it is discovered that mission-critical information is passed between remote departments in the company over the LAN and the Internet. What security implementation could be used to keep this information out of unauthorized hands? Provide a brief explanation with each answer.

_____

_____

_____

_____

_____

_____

_____

Answer: (answers will vary)

Authentication gives access to authorized users only. For example, using one-time passwords as a means to authenticate users.

Firewalls allow the network administrator to filter network traffic to allow only valid traffic and services.

Virtual Private Networks (VPNs) hide traffic contents to prevent unwanted disclosure to unauthorized or malicious individuals.

Step 4 Create a Description of the Security Wheel

a. The Widget Warehouse executives do not completely understand the continual process of security. They appear to be under the impression that once a security policy is implemented it will be sufficient for an extended period of time. Create a description of the security wheel and discuss the benefits of such a model.

The security wheel is comprised of four steps:

Step Name	Step Description

Answer:

Step Name	Step Description
Secure	Implementing security devices with the intent to prevent unauthorized access to network systems
Monitor	Monitor the network for violations and attacks against the corporate security policy
Test	Test the effectiveness of the security safeguards in place by using various tools to identify the vulnerabilities of the network
Improve	Make security improvements after collecting and analyzing information from the monitoring and testing phases.

Step 5 Passive Monitoring

a. The management of Widget Warehouse wishes to see some of the available options in security monitoring. As the consultant, suggest that a passive monitoring scheme may be an option they should pursue. Write a description of passive monitoring that is to be presented to Widget Warehouse management.

_____

_____

_____

_____

_____

_____

Answer: (answers will vary)

Passive methods include using intrusion detection or IDS devices to automatically detect intrusion. This method requires only a small number of network security administrators for monitoring. These systems can detect security violations in real time and can be configured to automatically respond before an intruder does any damage.

Step 6 Explain Using a Security Policy

a. Explain to the IT Department how using a security policy can provide advantages to the company as a way to secure sensitive information.

1. Developing a security policy.

_____

_____

_____

_____

_____

_____

Answer: (answers will vary)

Developing a security policy:

- Provides a process to audit existing network security.
- Provides a general security framework for implementing network security.
- Defines which behavior is and is not allowed.
- Helps determine which tools and procedures are needed for the organization.
- Helps communicate consensus among a group of key decision makers and defines responsibilities of users and administrators.
- Defines a process for handling network security incidents.
- Enables global security implementation and enforcement. Computer security is now an enterprise-wide issue and computing sites are expected to conform to the network security policy.
- Creates a basis for legal action if necessary.

Comments

Lab 2.5.2a Configure SSH

Objective

In this lab, the students will complete the following tasks:

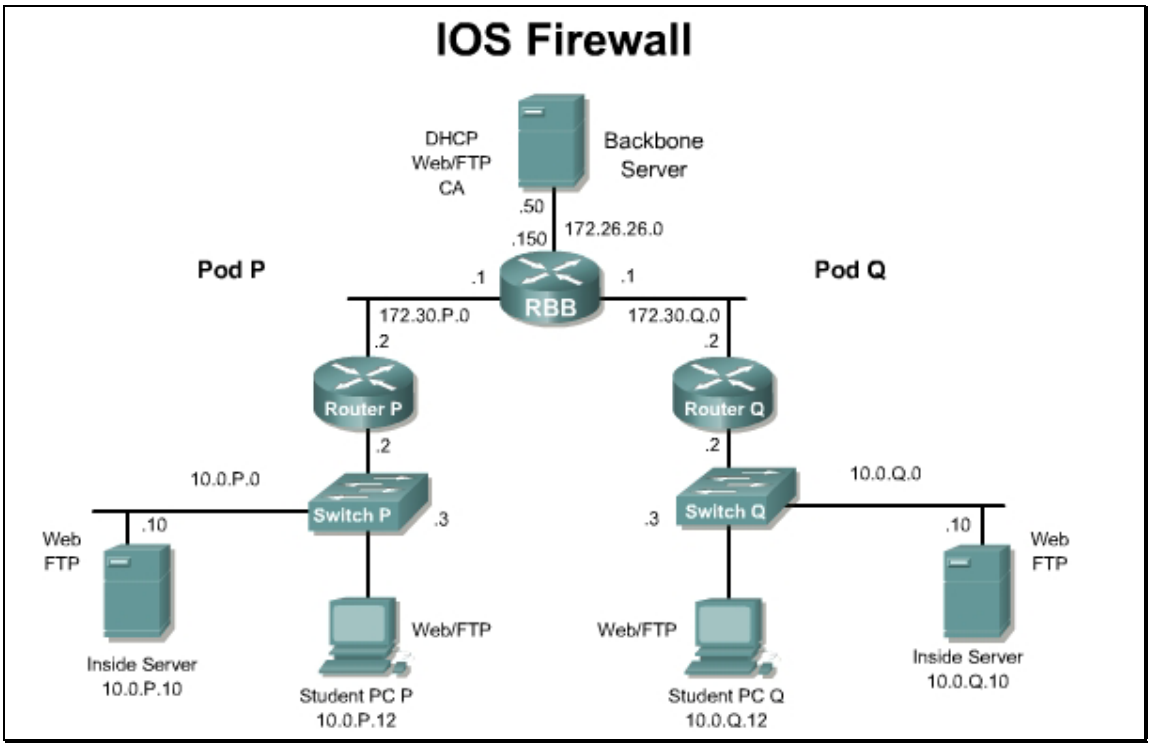
- Configuring a router as a Secure Shell (SSH) server Version 1.
- Install and configure a SSH client on the Student PC.
- Using show and debug commands to troubleshoot SSH
- Strengthen SSH by configuring SSHv2.

Scenario

An IT administrator is concerned about using Telnet for remote administration. Therefore, the security policy has been updated and now requires the use of encrypted sessions for remote management sessions. The IT administrator must now configure SSH on the perimeter router.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal

emulator on the student PC. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Prior to starting the lab, ensure that each host PC is loaded with a SSH client. There are numerous SSH clients available for free on the Internet. The lab was developed using the PuTTY SSH client.

http://www.chiark.greenend.org.uk/~sgtatham/putty/

Tools and resources:

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- SSH client

Further information about the objectives covered in this lab can be found at the following websites:

- http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html
- http://www.chiark.greenend.org.uk/~sgtatham/putty/

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
crypto key generate rsa	Generates Rivest, Shamir, and Adleman (RSA) key pairs.
hostname	This command changes the hostname of the router.
ip domain-name	Defines a default domain name that the Cisco IOS software uses to complete unqualified host names.
ip ssh	Use the **ip ssh** command to configure Secure Shell (SSH) control parameters on the router. Use the **version** option to specify the SSH version.
transport input	Defines which protocols to use to connect to a specific line of the router.

Step 1 Configuring SSH on a Router

To enable SSH on the router, the following parameters should be configured:

- Hostname
- Domain-name
- Asymmetrical keys
- SSH timeouts
- Local authentication
- Version

a. Set router parameters

Begin by configuring the router hostname and domain-name using the following commands:

- To configure the router hostname, use the **hostname** *hostname* command in configuration mode. In this lab, the hostname has been configured to RouterP, where P is the pod number. For example, if the team has been assigned to Pod 5 then the hostname would be Router5.

  ```
  RouterP(config)#hostname RouterP
  ```

  After the hostname is set, the active CLI will dynamically change.

- To configure the router IP domain-name, use the **ip domain-name** *domain name* command in Configuration Mode.

  ```
  RouterP(config)#ip domain-name cisco.com
  ```

What command can be used to view both the hostname and IP domain name?

Answer: `show running-config`

Use the **ip ssh version 1** command to configure the router to use SSH version 1.

Step 2 Generate Asymmetric Keys

a. Generate RSA keys

Enter the following command in the configuration mode:

```
RouterP(config)#crypto key generate rsa ?
```

What are the available help options for this command?

Answer: `General-keys, Usage-keys`

b. Generate RSA keys (continued)

- To enable SSH for local and remote authentication on the router enter the command **crypto key generate rsa** and press **Enter**. The router will respond with a message showing the naming convention for the keys.

What is the default size, in bits, of the key modulus?

Answer: 512 bits

Press **Enter** to accept the default key size and continue.

Step 3 Configure SSH Timeouts

a. Configuring SSH timeouts and authentication retries is a way of providing additional security for the connection. Use the command **ip ssh {[time-out** *seconds*]**} {authentication-retries integer}** to enable timeouts and authentication retries. Set the SSH timeout to 15 seconds and the amount of retries to 2 by entering the following commands:

```
RouterP(config)#ip ssh time-out 15
RouterP(config)#ip ssh authentication-retries 2
```

1. What is the maximum timeout value allowed? What is the maximum amount of authentication retries allowed?

Answer: 120 seconds in the maximum timeout value and 5 is the maximum amount of retries available.

Step 4 Configure Local Authentication and vty

a. Use the following commands to define a local user and assign SSH communication to the vty lines:

```
RouterP(config)# username student password cisco
RouterP(config)# line vty 0 4
RouterP(config-line)# transport input ssh
RouterP(config-line)# login local
```

1. What are the available parameters for the **transport input** command?

Answer:

```
all     All protocols
mop        DEC MOP Remote Console Protocol
none    No protocols
pad     X.3 PAD
rlogin  Unix rlogin protocol
ssh     TCP/IP SSH protocol
telnet  TCP/IP Telnet protocol
udptn   UDPTN async via UDP protocol
v120     Asyc over ISDN
```

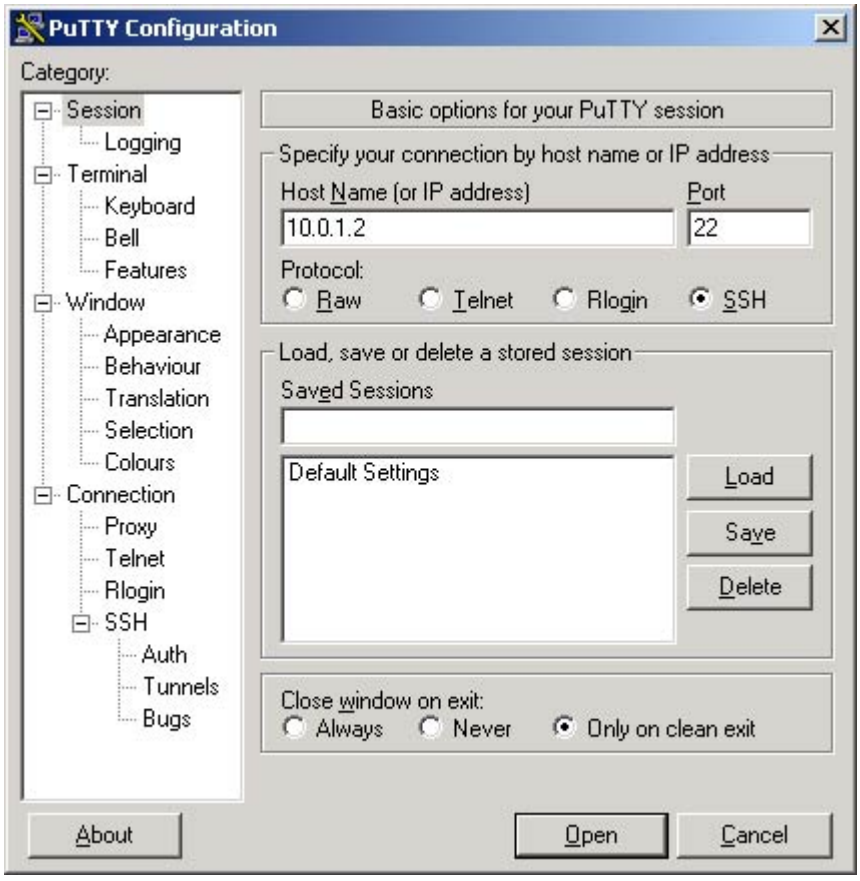
2. Why would you limit this only to SSH?

Answer: SSH is the only one of these options that uses encryption.

Step 5 Communicating Between a SSH PC (Client) to Router (Server)

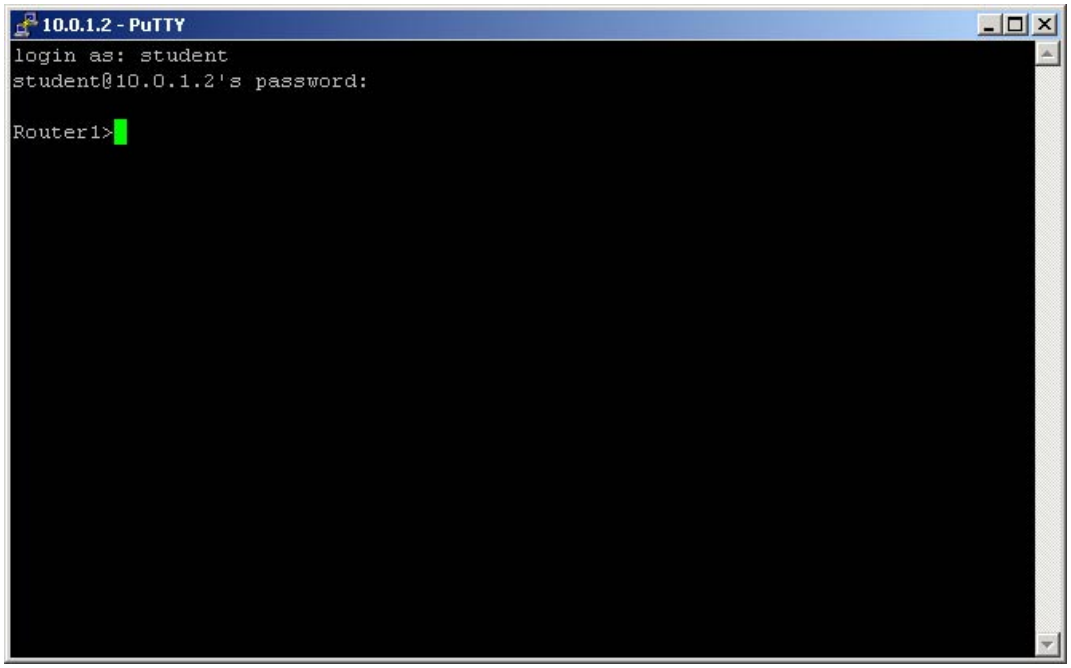
The basic settings to allow a PC and a router to establish a SSH session are now configured. In order to establish a SSH session, launch the SSH client from the student PC.

a. The configurations will vary between the different SSH clients. If PuTTY is being used as the SSH client, following these instructions. Launch the PuTTY.exe file and a pane with various configuration options will open.



b. In the “Host Name (or IP address)” input box enter the IP address of the pod router. Next, make sure that radio button next to “SSH” is selected under “Protocol:”. These two values must be sent to establish the SSH connection. To test the connection, press the **Open** command button at the bottom of the window.

c. The SSH client will prompt for the local username and password that was previously set on the Pod router. Enter the “**student**” for the username and “**cisco**” for the password.



1. Was the SSH connection successful? If so, how is the prompt displayed?

Answer: Yes. The prompt is displayed as `RouterP>`.

Step 6 Debug and Verify SSH

a. Enable debugging

i. Enable debugging of SSH by entering the following commands:

```
RouterP(config)#logging on
RouterP(config)#logging console
RouterP#debug ip ssh
```

b. SSH debug output

i. Next, open another instance of the SSH client and connect to the router. Use the correct username and password to log in to the router. The debug output should be similar to the output below.

```
03:45:37: SSH1: starting SSH control process
03:45:37: SSH1: sent protocol version id SSH-1.5-Cisco-1.25
03:45:37: SSH1: protocol version id is - SSH-1.5-PuTTY-Release-0.53b
03:45:37: SSH1: SSH_SMSG_PUBLIC_KEY msg
03:45:38: SSH1: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
03:45:38: SSH: RSA decrypt started
03:45:39: SSH: RSA decrypt finished
03:45:39: SSH: RSA decrypt started
03:45:39: SSH: RSA decrypt finished
03:45:39: SSH1: sending encryption confirmation
03:45:39: SSH1: keys exchanged and encryption on
03:45:41: SSH1: SSH_CMSG_USER message received
03:45:41: SSH1: authentication request for userid student
03:45:41: SSH1: SSH_SMSG_FAILURE message sent
03:45:44: SSH1: SSH_CMSG_AUTH_PASSWORD message received
03:45:44: SSH1: authentication successful for student
03:45:44: SSH1: requesting TTY
03:45:44: SSH1: setting TTY - requested: length 24, width 80; set:
length 24, width 80
03:45:44: SSH1: SSH_CMSG_EXEC_SHELL message received
03:45:44: SSH1: starting shell for vty03:45:37: SSH1: starting SSH
control process
```

ii. To get an idea of the debugging process and the debugging message, open another instance of the SSH client and intentionally enter the wrong username or password. View the debugging output for failed authentication. When you are done viewing the debugging output, use the **`no debug ip ssh`** command to stop debugging.

c. Viewing SSH sessions

i. Use the **show ssh** command to view the active SSH sessions.

ii. Fill in the appropriate values of the table below, based on the output of the **show ssh** command.

Connection	Version	Encryption	State	Username

1. Is the SSHv2 server running?

Answer: No.

d. Viewing SSH parameters

i. To display the version information and SSH parameters, use the **show ip ssh** command.

1. Is the output displayed exactly as the output below? If not, what are the differences?

```
RouterP#show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 15 secs; Authentication retries: 3
```

Answer: Answers will vary.

e. End the SSH connection. From the router console, terminate the SSHv1 session.

```
RouterP#disconnect ssh 0
```

`0` is the connection # which can be found in the output from the **show ssh** command.

Step 7 Configure SSH Version 2

a. SSH version 1 is more secure than telnet, however there are some cryptopgraphic weaknesses to SSHv1. Many devices now support SSHv2. Configuring SSHv2 is a way of providing additional security for the connection. Use the command **ip ssh version** to enable SSHv2.

Note: If the IOS version in use does not support SSHv2, proceed to Step 7 to communicate between two routers using SSHv1.

```
RouterP(config)#ip ssh version 2
RouterP(config)#exit
RouterP#
```

b. Next, open another instance of the SSH client and connect to the router. Use the correct username and password to log in to the router. Use the **show ssh** command to view the active SSH sessions.

Fill in the appropriate values of the table below, based on the output of the **show ssh** command.

Connection	Version	Encryption	Hmac	State	Username

1. Is the SSHv2 server running?

Answer: Yes

c. End the SSH connection. From the router console, terminate the SSHv1 session.

```
RouterP#disconnect ssh 0
```

0 is the connection **#** which can be found in the output from the **show ssh** command.

Step 8 Router to Router SSH Connection

a. Confirm peer SSH configurations

i. Verbally communicate with the peer team to ensure the peer router Q has been configured to accept a SSH connection. Also, confirm the version of SSH. The settings configured in Steps 1 through 7 will be applicable to enable a SSH connection between two routers. Only this time, instead of using a SSH client running on a host computer, the router will be the SSH client and will establish a connection to the peer router. By default, the Cisco IOS will act as both a SSH server and SSH client.

b. Testing Telnet

i. When the peer group is ready, enter the **telnet** command and establish connectivity with the peer router.

```
RouterP#telnet 172.30.Q.2  (where Q is the peer team router)
```

1. Was the Telnet connection successful? Why or why not?

Answer: If the router has been configured as described in Steps 1 though 7, the Telnet connection will fail. This is because the router has been configured to accept incoming SSH connection on TCP/IP port 22 and not Telnet TCP/IP port 23. Telnet and SSH are two separate entities and should not be considered the same

c. SSH parameters

i. Enter the following commands to establish a SSH connection to the peer router:

```
RouterP(config)#ssh ?
```

1. What are the additional arguments of the **ssh** command?

Answer:

```
RouterP>ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  WORD  IP address or hostname of a remote system
```

2. What encryption algorithms are available?

_____

Answer: 128, 192, or 256 bit AES

d. Router to router SSH connection

i. Enter the following command to establish a SSH connection to the peer router:

```
RouterP>ssh –c aes128-cbc –l student 172.30.Q.2
```

This command makes a SSH connection to a peer router with an address of 172.30.Q.2, 128 bit AES as the encryption, and "student" as the login username. The password is "cisco".

1. Was the SSH connection successful?

_____

Answer: Yes

e. Verify SSH

i. Enter the following command to verify the SSH connection:

```
RouterP#show ip ssh
RouterP#show ssh
```

1. What other commands could be useful to verify and troubleshoot SSH connections?

_____

_____

_____

Answers: `show running-config, debug ip ssh`

Lab 2.5.2b Controlling TCP/IP Services

Objective

In this lab, the students will complete the following tasks:

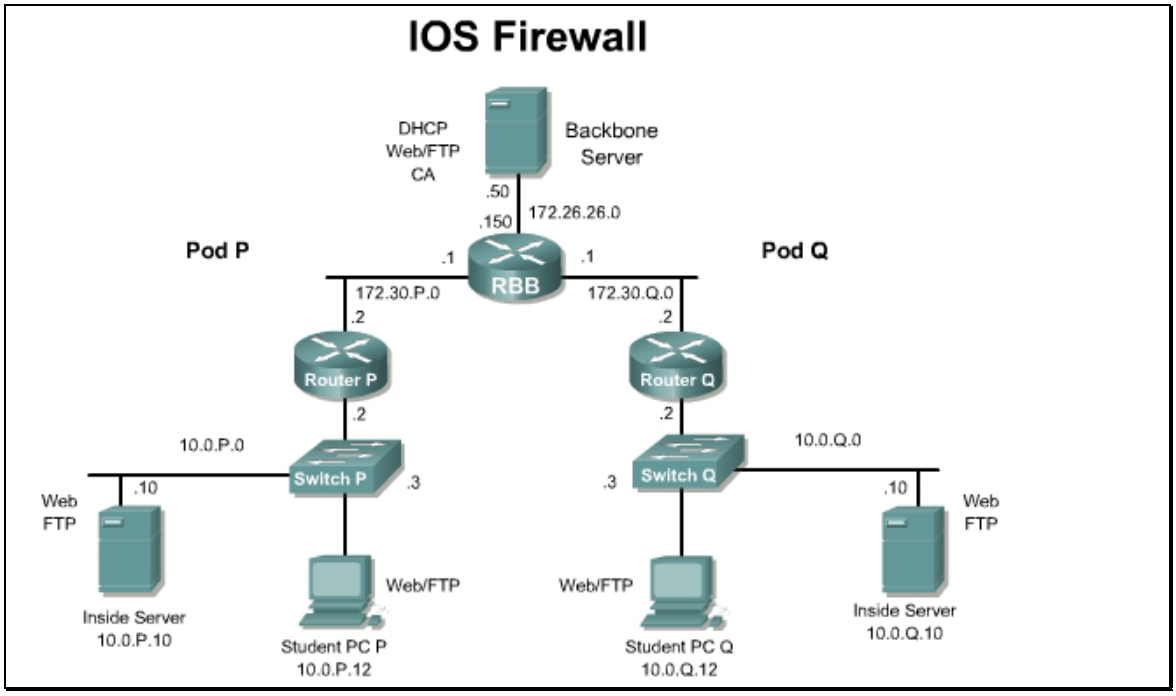
- Begin the process of implementing a secure perimeter router
- Explicitly deny common TCP/IP services
- Verify TCP/IP services have been disabled

Scenario

The XYZ Company is in the process of installing a perimeter router to defend their network against various security attacks, including access and DoS attacks. It is the responsibility of the network security administrator to implement a secure perimeter router based on the security policy. The first configuration task is to disable common TCP/IP services that can pose a risk to the internal network. Second, CDP, SNMP, and HTTP access to the router should be secured or disabled. Finally, the small services, such as echo, discard, and character generation, also known as chargen, should be disabled if not in use.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at, http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800b3dda.html.

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
no cdp enable	Disables Cisco Discovery Protocol on an interface
no cdp run	Disables Cisco Discovery Protocol globally
no ip mask-reply	Disables the Cisco IOS software response to the Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages.
no mroute-cache	Disables multicast route caching on the outside interface.
no ip proxy-arp	Use the **no ip proxy-arp** interface configuration command to disable proxy ARP on an interface.
no ip redirects	Use the **no ip redirects** interface configuration command to disable the sending of redirect messages if the router is forced to resend a packet through the same interface on which it was received.
no ip route-cache	Use the **no ip route-cache** interface configuration command to disable the use of a high-speed switching cache for IP routing as well as the use of autonomous switching.
no ip source-route	Use the **no ip source-route** command to cause the system to discard any IP datagram containing a source-route option.
no ip unreachables	Use the **ip unreachables** interface configuration command to enable the generation of ICMP unreachable

Command	Description
	messages on a specified interface.
no service finger	To disallow finger protocol requests, defined in RFC 742, to be made of the network server, use the **no service finger** global configuration command. This service is equivalent to issuing a remote **show users** command.
no ntp	Turns off the Network Time Protocol. Protocol used for the synchronization of clocks on devices in a network. Defined in RFC-1305.
no service tcp-small-servers	To deny access to minor TCP/IP services available from hosts on the network.
no service udp-small-servers	To deny access to minor UDP services available from hosts on the network.

Step 1 Disabling ICMP Messages on Fast Ethernet 0/1

a. Enter the Interface Configuration Mode for Fast Ethernet 0/1 or the outside interface on the perimeter router. In many production environments this will be a serial port such as Serial0/0 or Serial0/1. In this lab, enter the command **interface fa 0/1** at the Global Configuration Mode. This may vary depending on the router model.

1. How is the prompt displayed after entering the Interface Configuration Mode?

Answer: `RouterP(config-if)#`

b. Disable the automatic generation of ICMP, or ping, messages to untrusted or public networks. By default, ICMP automatically generates Redirect, Host Unreachable, and Mask Reply message. Intruders can intercept these messages and expose the network topology. Enter the following commands to disable these ICMP messages:

- To disable ICMP Redirect messages on the interface, enter the command **no ip redirects**.
- To disable ICMP Unreachable messages on the interface, enter the command **no ip unreachables**.
- To disable ICMP Mask Reply messages on the interface, enter the command **no ip mask-reply**.

1. ICMP messages are sent in response to certain IP packets. What information could an intruder gather if this information is not blocked?

Answer: If ICMP messages are sent to untrusted networks, intruders might use information to create a network map of the internal network.

Refer to the *Command Table* for help configuring this security policy.

Step 2 Disable Multicast Route Caching

a. Disable multicast route caching on the outside interface by entering the following command:

```
no ip mroute-cache
```

Refer to the *Command Table* and *Port Table* for help configuring this security policy.

Step 3 Disable Cisco Discovery Protocol

a. Use the **`show cdp neighbors fa0/1`** command to view CDP information learned from the outside interface.

b. Disable the Cisco Discovery Protocol (CDP) on the outside interface. Enter the following command to disable Cisco Discovery Protocol on an interface:

```
no cdp enable
```

1. What command disables Cisco Discover Protocol globally?

_____

Answer: **`no cdp run`**

Refer to the *Command Table* and *Port Table* for help configuring this security policy.

2. Enter the **`show`** command again. What information is displayed now? Was it expected? Why?

_____

_____

Answer: No neighbors are shown for fa0/1. This is the expected result, because CDP has been disabled on interface fa0/1. If CDP neighbors are still shown for fa0/1, this is because the router does not remove the entry for the neighbor on CDP disabled interfaces unless the hold time expires. The **`clear cdp table`** command can be used to clear the entries before the timer expires.

Step 4 Controlling HTTP and SNMP Access

a. Control the hosts that are allowed to create HTTP connections to the router. In this lab, accept HTTP connections from the inside host but not from the peer inside host. Enable HTTP services on the pod router using the **`ip http server`** command.

b. Create a standard access list to permit traffic from only the inside host. Write this access list on the line below.

_____

Answer: **`access-list 2 permit host 10.0.P.12`**

c. Apply this new ACL to HTTP connections using the **`ip http access-class`** *<acl>* command. Remember to use the newly defined ACL number.

d. Use the **`username student privilege 15 password cisco`** command to create a new username and password to use for HTTP access.

e. Enter the IP address of the pod router in a web browser on the inside host to test HTTP access. When prompted for a username and password, enter the username and password pair that was just created.

1. Was the connection successful?

_____

Answer: Yes

2. Try to connect to the HTTP server of the peer router. Was the connection successful? What was the error message?

_____

_____

Answer: No, “unable to open page.”

- To disable HTTP access, use the **no ip http server** command. Test this connection from the inside host.

3. Was the connection successful?

_____

Answer: No, “unable to open page.”

- To disable SNMP access, use the **no snmp-server** command.

4. Use the **show snmp** and **show run** command to verify the service is shutdown. Was there a response? Notice that a **show run** will not display the SNMP service as disabled.

_____

Answer: No, “%SNMP agent not enabled”

Step 5 Disabling Small Services

Most routers support a multitude of small services that may or may not be needed or used by an organization. These small services should be disabled, unless specifically needed.

a. Disable each of these services, using the **no** form of the commands:

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no ntp
no cdp run
```

1. Show the running configuration. Do these services show up?

_____

Answer: No

Step 6 Verify Configurations

a. Exit out of the Interface Configuration Mode and return to the privileged EXEC mode (RouterP#). Verify the configuration by entering the **show running-configuration** command.

1. Verify the configurations are displayed under “interface FastEthernet0/1” or the outside interface. Document the configuration below:

_____

_____

Answer: Configuration might vary

```
Interface FastEthernet0/1
       ip address 172.30.1.2 255.255.255.0
       no ip redirects
       no ip unreachables
       no ip mroute-cache
```


b. Verify the Cisco Discovery Protocol information. Enter the command **show cdp**.

1. What information is displayed?

_____

_____

_____

Answer: "% CDP is not enabled".

c. Verify Cisco Discovery Protocol has been disabled on outside interface. Enter the command **show cdp interface** to display CDP information specific to the interfaces.

1. Does the output display CDP information for the outside port? Why or why not?

_____

_____

_____

Answer: The output shows global CDP information. Earlier, CDP was disabled on a specific interface, FastEthernet0/1. However, CDP has been disabled globally and so the global status is shown instead of the status of the individual interfaces.

Sample perimeter router configuration

The sample configuration for the Pod 1 perimeter router is one possible outcome of this lab. Other configurations may vary according to available router features and interfaces.

```
Current configuration:
!version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname Router1
!
logging buffered 4096 debugging
no logging console
!
username student privilege 15 password 0 cisco
clock timezone PST -8
clock summer-time zone recurring
ip subnet-zero
no ip source-route
no ip finger
ip tcp selective-ack
ip tcp path-mtu-discovery
no ip domain-lookup
no ip bootp server
```



```
!
interface FastEthernet0/0
description inside
ip address 10.0.1.2 255.255.255.0
ip access-group 102 in
!
interface FastEthernet 0/1
description outside
ip address 172.30.1.2 255.255.255.0
no ip directed-broadcast
no ip redirects
no ip unreachables
no ip proxy-arp
no ip route-cache
no ip mroute-cache
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.2
no ip http server
!
no cdp run
!
line con 0
exec-timeout 0 0
logging synchronous
login local
transport input none
line aux 0
no exec
login local
line vty 0 4
access-class 1 in
login local
end
```


Lab 2.5.7 Configure Routing Authentication and Filtering

Objective

In this lab, the students will complete the following tasks:

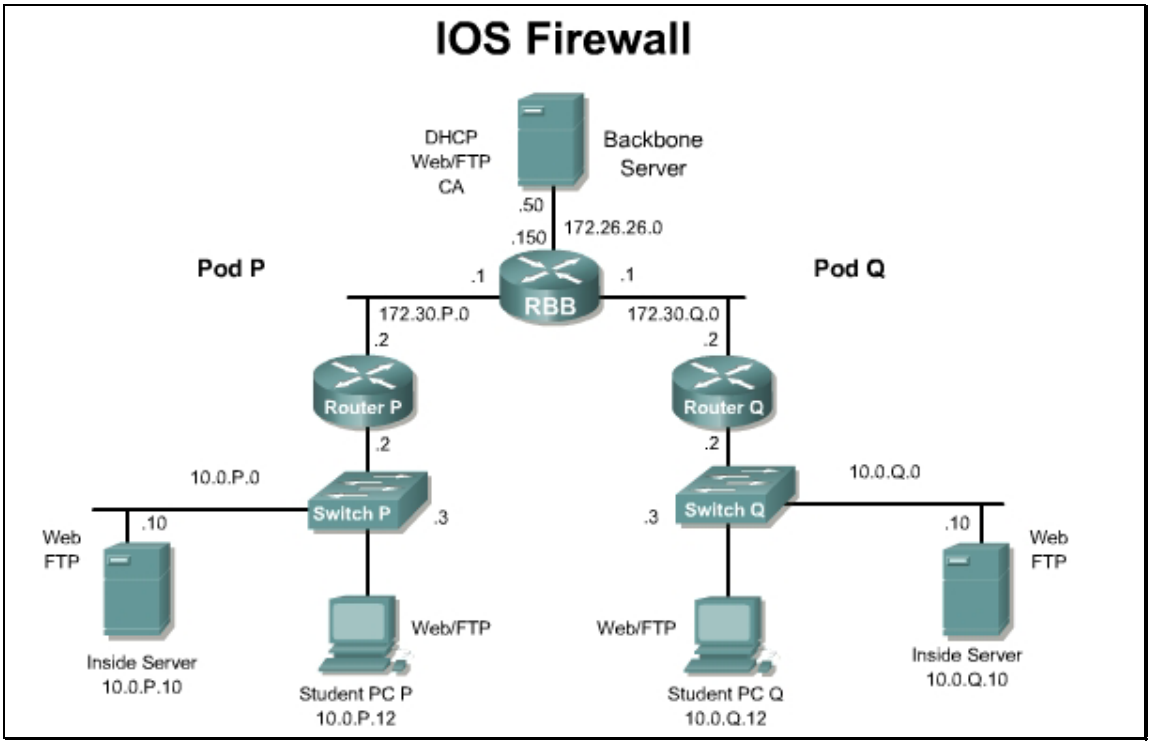
- Configure routing protocol authentication
- Configure route filters to control route updates from peer routers.

Scenario

Routing protocols are vulnerable to eavesdropping and spoofing of routing updates. To ensure secure routing, authentication of routing protocol updates to prevent the introduction of unauthorized or false routing messages from unknown sources must be implemented. Secondly, filtering networks in routing updates sent from the private network to external routers helps secure networks by hiding the details of networks that should not be accessed by external users. Finally, incoming routing updates should be filtered to provide protection against receiving false information in routing updates due to improper configuration or intentional activity that could cause routing problems.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Access the perimeter router console port using the terminal emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at, http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca762.html

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
distribute-list (in)	To filter networks received in updates.
distribute-list (out)	To suppress networks from being advertised in updates.
ip rip authentication key-chain *key-chain*	Enable authentication of IP Enhanced IGRP packets.
ip rip authentication mode md5	Enable MD5 authentication in IP Enhanced IGRP packets.
key	Use the key command to identify an authentication key on a key chain.
key chain	Use the key chain command to enable authentication for routing protocols, identifies a group of authentication keys.
key-string	Use the key-string command to specify the authentication string for a key.
passive-interface	Use the passive-interface command to prevent other routers on the network from learning about routes dynamically.

Step 1 Remove EIGRP

RIP version 2 is configured on RBB with the corresponding key chain. No changes are required on RBB.

a. Remove EIGRP from the running configuration or load the starting configuration. Remember that connectivity may not be available while there is no routing protocol configured

```
no router eigrp 1
```

b. Now configure RIP version 2.

```
router rip
 version 2
 network 10.0.0.0
 network 172.30.0.0
 no auto-summary
```

1. What routing protocols support route authentication using MD5?

_____

Answer: RIPv2, EIGRP, BGP, OSPF

Step 2 Enable MD5 Authentication

a. On the outside interface, enable Message Digest 5 (MD5) authentication for RIP.

ip rip authentication mode md5.

1. What authentication modes are available?

_____

Answer: MD5 and Text

b. Now configure the key chain **RTRAUTH** to be used in this authentication scheme. Remember that the syntax for this command is

```
ip rip authentication key-chain RTRAUTH
```

Step 3 Configure Key Chain

a. Set the router clock to the current time with the **clock set** command.

b. Next, configure the parameters of this key chain identified in the previous task. The key number and key string characteristics of the key chain must be configured.

c. From global configuration mode, configure the RTRAUTH key chain by using the **key chain** *nameofchain* command. For key 1, configure key string text of ***123456789***. Remember that the command syntax is **key-string** *text*.

```
key chain RTRAUTH
key 1
key-string 123456789
```

1. Did the prompt change? If so, how does the prompt appear?

_____

Answer: Yes,

```
RouterP(config-keychain)#
RouterP(config-keychain-key)#
```


d. Clear the existing route entries in the routing table.

```
clear ip route *
```

e. To see authentication occurring, use the **debug ip rip events** command. Notice that if the peer router is not authenticating, updates are ignored and the (invalid authentication) message will appear. When the peer router begins to authenticate, updates are processed.

f. From the student PC, ping the backbone router.

g. Turn the debugging off.

Step 4 Controlling Route Advertisements

It is often necessary to control what advertisements a routing protocol sends to its neighbors. The **passive-interface** command is used in a routing protocol configuration to block all advertisements send by that protocol out a particular interface. However, in certain cases, it might be more appropriate to only send advertisements of certain networks and not others in a routing protocol update. This is called route filtering.

To control which networks a router will accept routing updates from, a combination of an access list and a distribute list applied in the inbound direction is used.

a. Create a standard access list #10 to permit only networks in 172.30.0.0 to be learned from RBB and to block all other networks, such as 10.0.Q.0, from been learned by RouterP.

```
access-list 10 permit 172.30.0.0 0.0.255.255
```

b. The route filter is now applied to a specific routing protocol. Use the **distribute-list** command to tie the access list to the interface in the correct direction.

```
router rip
distribute-list 10 in fa0/1
```

c. Use the passive-interface command to stop routing updates from being sent by the inside interface.

```
passive-interface fa0/0
```

d. Clear the routing table of the router using the **clear ip route *** command.

Now examine the routing table.

1. Comment on the output as seen in the new routing table.

_____

Answer: Answers will vary. The peer inside network 10.0.Q.0 should not be in the routing table.

Similarly, the **distribute-list** command can be used to filter routes advertised out a particular interface by using the **out** keyword instead of **in**.

2. How could an outbound route filter be used to help secure the internal network from the outside?

_____

Answer: Answers will vary. Information about internal networks could be useful to an attacker, and should not be sent out in the routing advertisements.

Sample configuration

A sample configuration is shown below:

```
hostname Router1
!
key chain RTRAUTH
 key 1
  key-string 1234546789
!
interface FastEthernet0/0
 description inside
 ip address 10.0.1.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/1
 description outside
 ip address 172.30.1.1 255.255.0.0
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain RTRAUTH
 no ip mroute-cache
!
!
router rip
 version 2
 passive-interface FastEthernet0/0
 network 10.0.0.0
 network 172.30.0.0
 distribute-list 10 in FastEthernet0/1

no auto-summary
!

access-list 10 permit 172.30.0.0 0.0.255.255
```


Lab 3.2.3 Configure Basic Security using Security Device Manager (SDM)

Objective

In this lab, the students will complete the following tasks:

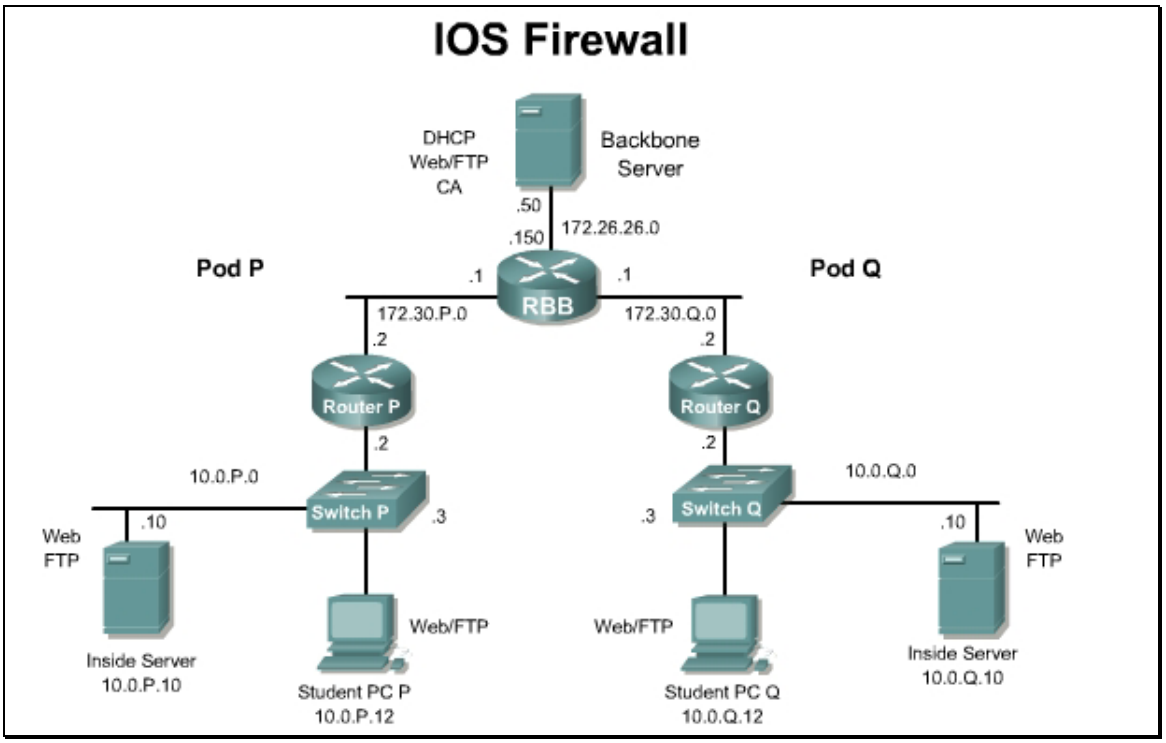
- Copy the SDM files to router Flash memory.
- Configure the router to support SDM.
- Configure a basic firewall.
- Reset a router interface.
- Configure PAT
- Create a banner.
- Configure secure management access

Scenario

Many SOHO and Small Business network administrators are not familiar or comfortable with the Cisco CLI. In this case, it is easier to use a GUI based tool to configure and monitor the router. Also, many experienced administrators are not familiar will security mechanisms and procedures which should be implemented on routers. SDM also uses an SSL encrypted session to secure the management traffic and prevent eavesdropping attacks.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the "*Student Lab Orientation*" if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- Java Virtual Machine. This is available for free from http://www.java.sun.com/.

Additional materials

Further information regarding the objectives covered in this lab can be found at the following websites:

- http://www.cisco.com/go/sdm
- http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_installation_guide09186a00803e4727.html
- http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a00803f5bdf.html

Command list

In this lab exercise, the following key commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
ip http server	Enable the Cisco Web browser user interface
ip http secure-server	Enable the Cisco Web secure browser user interface
ip http authentication local	Enable local authentication for Cisco Web browser user interface connections

Step 1 Copy the SDM Files to Router Flash Memory if needed

Complete the following steps to copy the SDM files from the TFTP server to the Pod router flash memory (where **P** = pod number).

a. Console into the pod router.

b. Enter enable mode using a password of **cisco**.

```
RouterP> enable
Password: cisco
RouterP#
```

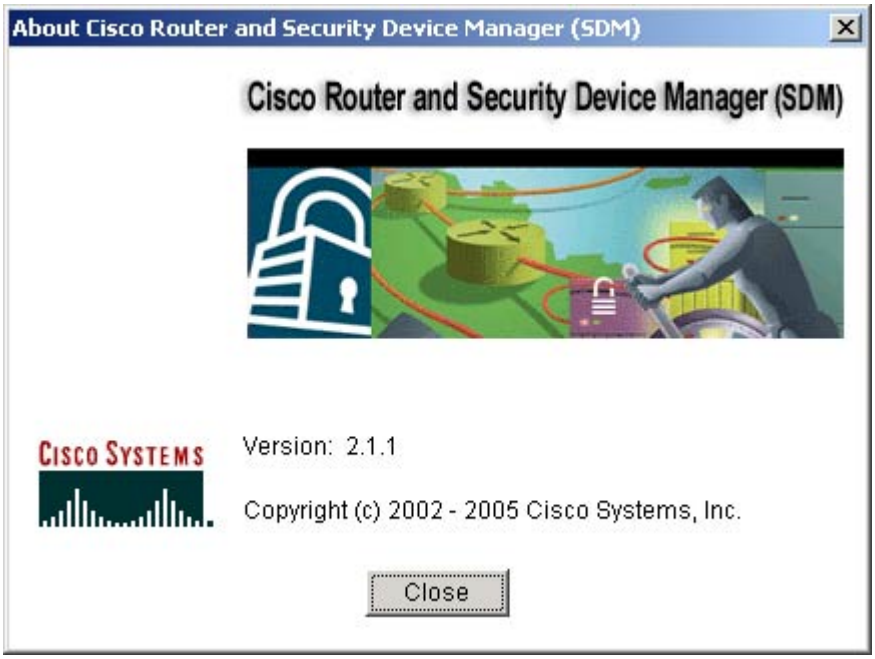
c. Check the contents of flash memory.

```
RouterP # show flash
System flash directory:
File  Length   Name/status
  1   16077820  c2600-advsecurityk9-mz.123-14.T1.bin
  2   1038     home.shtml
  3   1654     sdmconfig-26xx.cfg
  4   113152   home.tar
  5   820224   common.tar
  6   3085312  sdm.tar
[20099588 bytes used, 12930552 available, 33030140 total]
32768K bytes of processor board System flash (Read/Write)
```

There are 2 options at this point:

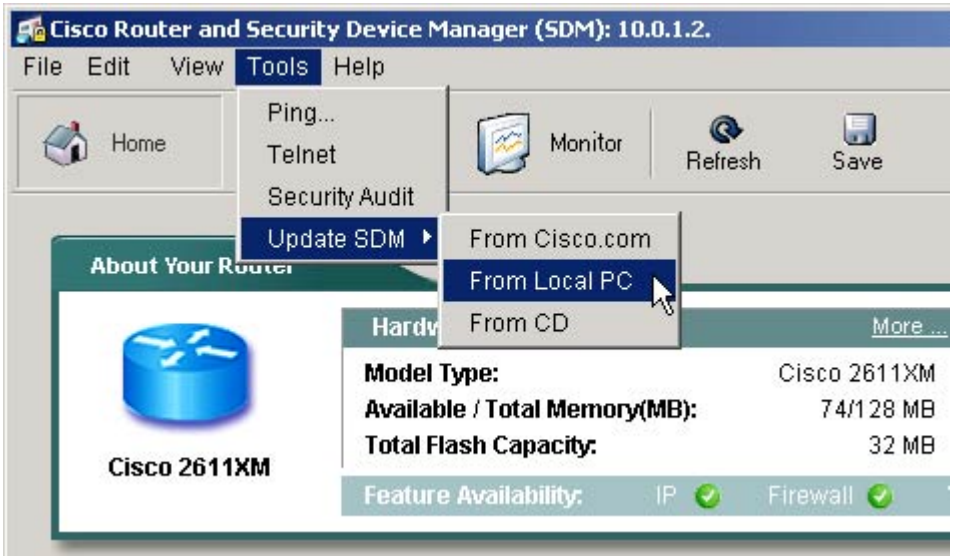
Option 1: If the files are not present, proceed to step d.

Option 2: If the files are present, proceed to Step 2 through Step 3. After step 3, go to **Help>About** to verify the version.



This course uses SDM version 2.1. Upgrade or downgrade as needed. The IOS image should also be a 12.3.(14) security image. The routers that are part of the standard course bundle ship with SDM installed by default.

d. Check with the instructor before installing or upgrading SDM or follow the directions located at http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_installation_guide09186a00803e4727.html to install, upgrade or downgrade SDM. A CCO login is required to obtain the needed SDM files. SDM can also be update from the SDM GUI interface.



Make sure all popup blockers have been disabled.

Step 2 Configure the Router to Support SDM

Complete the following steps to configure the pod router to support SDM (where **P** = pod number).

a. Enter global configuration mode using the **configure terminal** command.

```
RouterP# conf t
```

b. Enable the Cisco Web browser user interface using the **ip http server** command.

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


c. Enable the Cisco Web secure browser user interface using the **ip http secure-server** command. RSA keys are generated and SSH is enabled when this command is entered.

```
RouterP(config)# ip http secure-server
```

d. Enable local authentication for Cisco Web browser user interface connections using the **ip http authentication local** command.

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

e. Create a local privilege level 15 user account for SDM Cisco Web browser user interface login authentication.

```
RouterP(config)# username sdm privilege 15 password 0 sdm
```

Note: Enter the command exactly as shown for this lab exercise only. Do not use a username/password combination of sdm/sdm on any production routers. Always use unique username/password combinations in production environments.

f. Enter VTY line configuration mode using the **line vty** command.

```
RouterP(config)# line vty 0 4
RouterP(config-line)#
```

g. Configure the VTY privilege level for level 15 using the privilege level command.

```
RouterP(config-line)# privilege level 15
```

h. Configure VTY login for local authentication using the **login local** command.

```
RouterP(config-line)# login local
```

i. Configure VTY to allow both Telnet and SSH connections using the **transport input** command.

```
RouterP(config-line)# transport input telnet ssh
RouterP(config-line)# end
```

j. Copy the router running configuration to the startup configuration.

```
RouterP# copy run start
RouterP#
```

Step 3 Launch SDM

SDM is stored in the Flash memory of the router. It is launched by executing an HTML file, which then loads a signed SDM Java file. Complete the following steps to launch SDM.

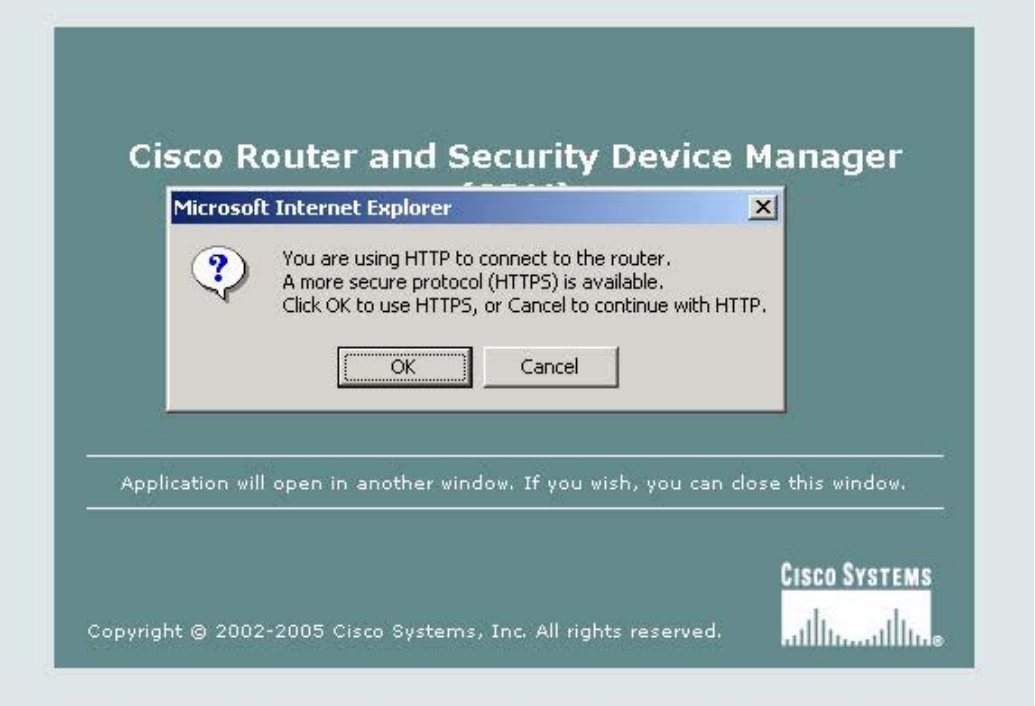
a. Open Internet Explorer on the student PC.

b. Enter the following URL in the browser address field (where **P** = pod number).

```
http://10.0.P.2
```

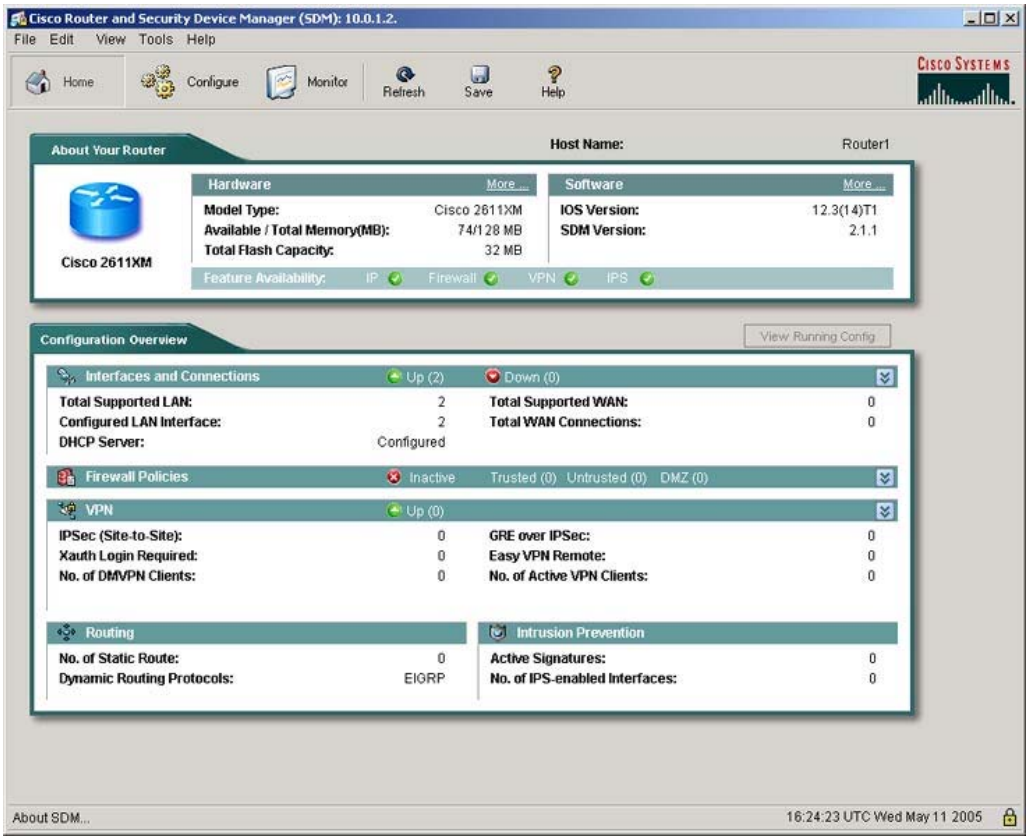
c. Enter the correct username "**sdm**" and password "**sdm**" in the Enter Network Password window.

d. Notice that this is an insecure management session. Click on the **OK** button to enter into a HTTPS connection.



Note: Multiple security alert windows may appear when launching SDM. If a security alert window appears, review the message contained in the window, and click **Yes** to continue. A username and password prompt may also appear multiple times. Enter the correct username "**sdm**" and password "**sdm**" in the Enter Network Password window.

e. Click **Yes** at the Security Warning window. The SDM window appears and the SDM loads the current configuration from the router.



f. Notice the information provided in the **About Your Router** and **Configuration Overview** tabs.

1. What two categories are covered in the About Your Router section?

Answer: Hardware and Software

2. What version of IOS and SDM are installed?

Answer: Answers will vary

3. What five categories are covered in the Configuration Overview section?

Answer: Interfaces and Connections, Firewall Policies, VPN, Routing and Intrusion Prevention

4. Is the Firewall Policies feature available? Active?

Answer: The Firewall Policies feature is available and the status is inactive

Step 4 Configure a Basic Firewall

Complete the following steps to configure a basic firewall on the Pod router.

a. Click the **Configure** button along the top of the SDM interface to configure the router settings.

b. Select **Firewall and ACL** from the category bar.

c. Select **Basic Firewall**.

When should the Advanced firewall be used?

Answer: The advanced mode can be used to configure pre-defined or custom firewall parameters with SDM, and to configure DMZ services.

d. Click **Launch the selected task**.

e. The Firewall Wizard screen appears. Click the **Next** button to begin the configuration.

f. For the outside (untrusted) interface, select the **FastEthernet0/1** Ethernet interface.

g. For the inside (trusted) interface, select the **FastEthernet0/0** interface.

h. Make sure the **Access rule log option** is checked.

i. A warning appears indicating that SDM cannot be launched from the FastEthernet0/1 interface after the Firewall Wizard is completed. Click the **OK** button to continue.

j. The Internet Firewall Configuration Summary screen appears. View the access rules that will be applied.

k. After viewing the configuration summary, click **Finish** to deliver the configuration to the router.

l. The Routing traffic configuration window appears. Make sure that **Allow EIGRP updates to come through the firewall** is checked, and then click **OK**.

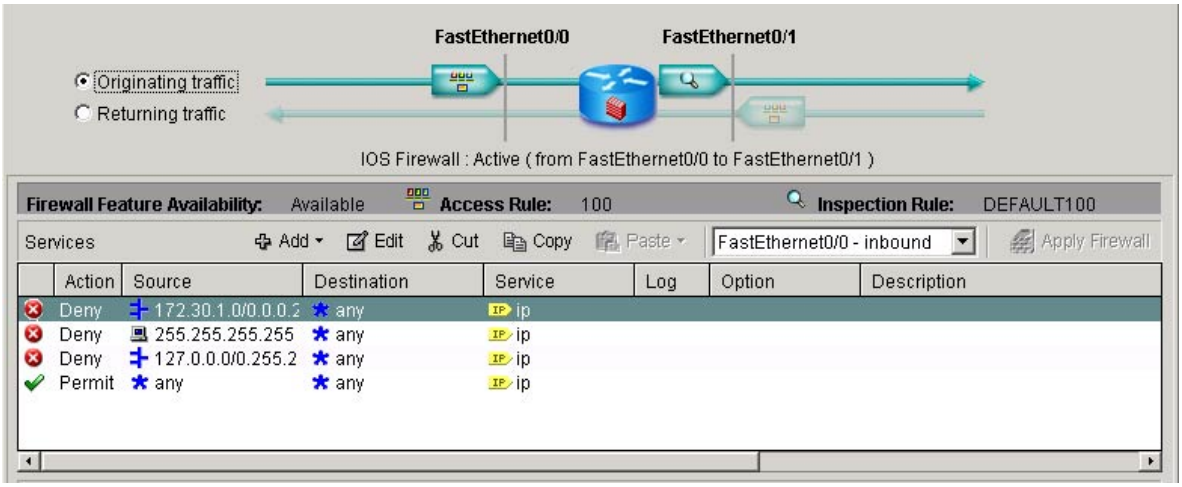
1. Why are RIP and OSPF unavailable?

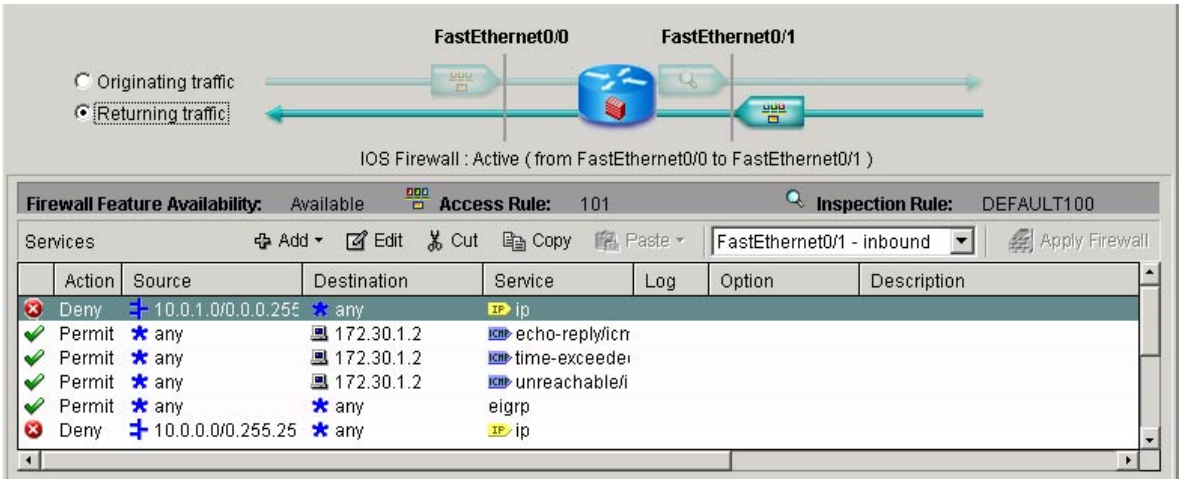
Answer: Only EIGRP is running on the network. RIP and OSPF are not used.

The Command Delivery status window appears. Verify the Configuration Delivery Status and click the **OK** button.

An Information widow appears. Click **OK** to proceed to the Firewall and ACL page.

Once complete, the new firewall appears in the Edit Firewall Policy / ACL tab in the Firewall and ACL page. Note the ACL rules that have been configured for both originating traffic and returning traffic.





m. Resume a console connection with the router and verify that the configuration generated from the SDM tool is in the running configuration.

Step 5 Reset a Router Interface

Complete the following steps to reset a router interface.

a. Select **Interfaces and Connections** from the Tasks bar on the Configure page.

b. Select the **Edit Interface/Connection** tab.

c. Select the **172.30.P.2** interface (where **P** = pod number). The interface status should be up.

d. Click **Disable**. Note how the status changes from up to down.

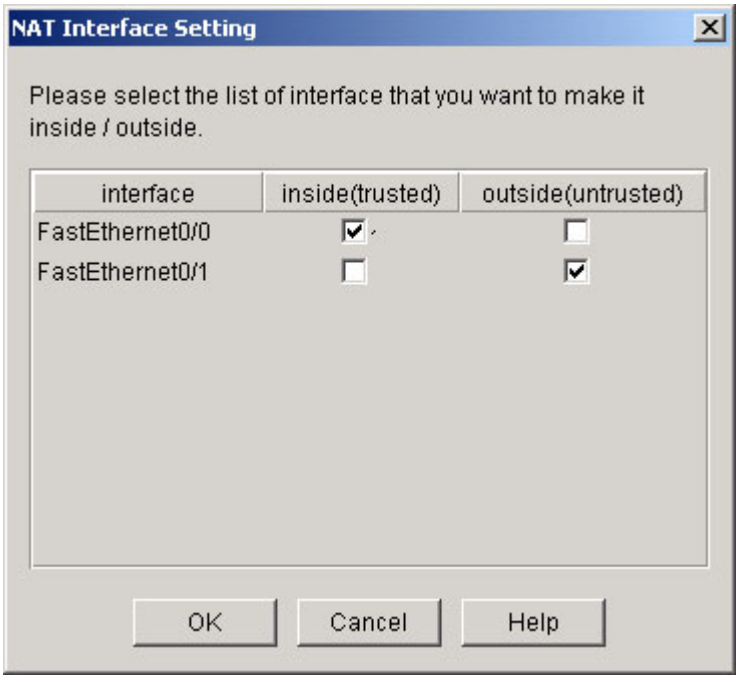
e. Click **Enable**. The interface should come back up.

Step 6 Configure PAT

Complete the following steps to configure NAT

a. Select **NAT** from the Tasks bar on the Configure page.

b. Click on the **Designate NAT Interfaces** button.

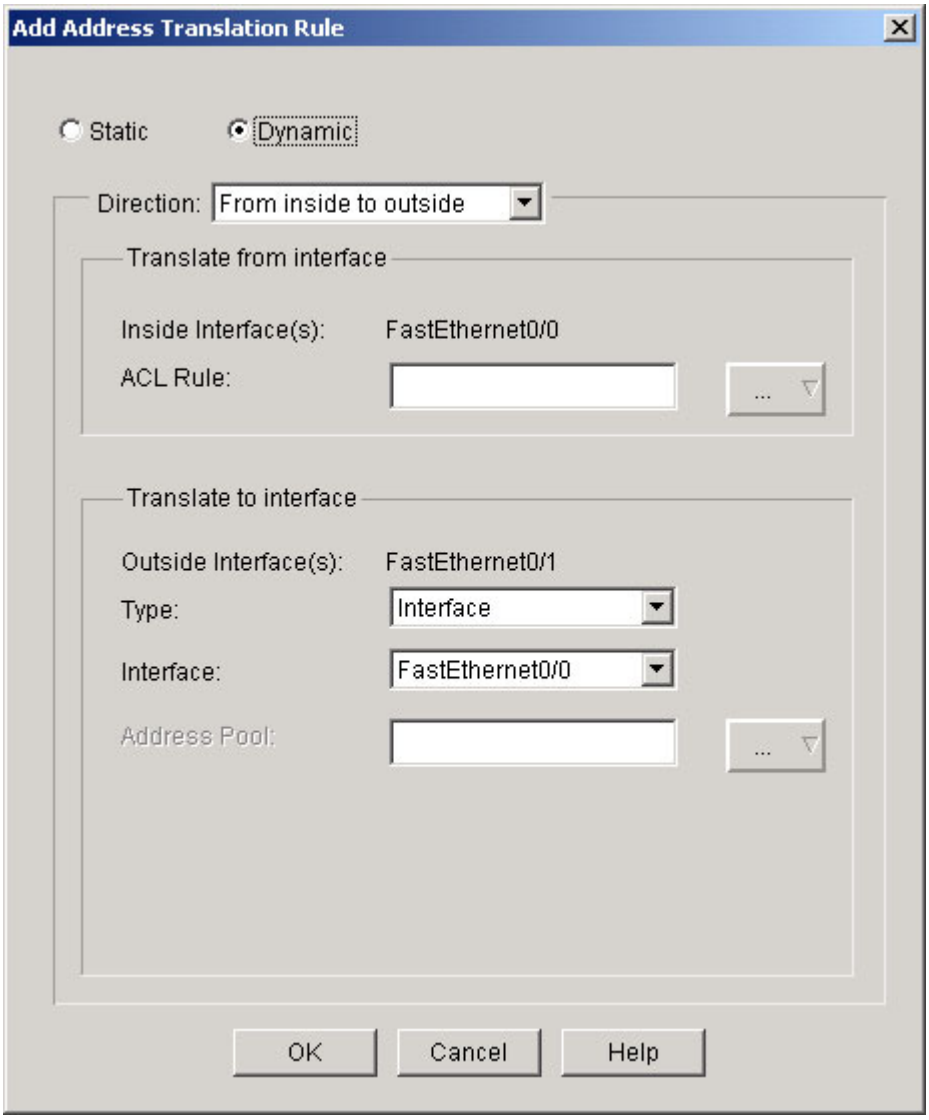


c. Check the appropriate inside and outside interfaces

d. Click the **OK** button. If the Command Delivery Status window appears, click the **OK** button on the window.

e. Click on the **Add** button.

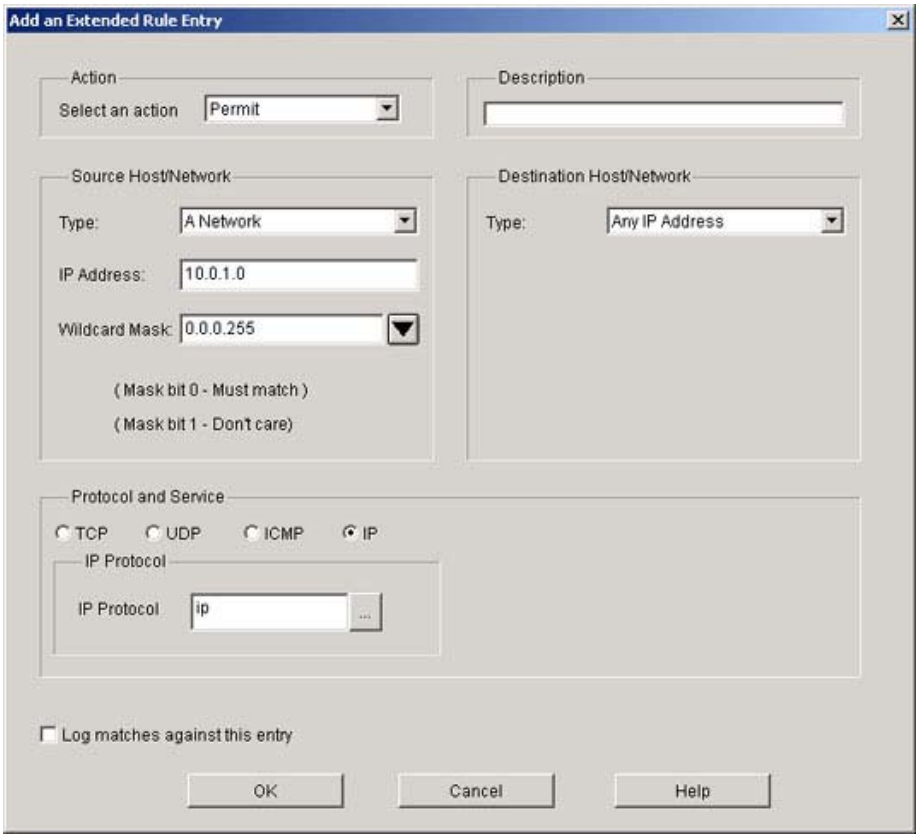
f. Click on **Dynamic**. The direction should be **From inside to outside**.



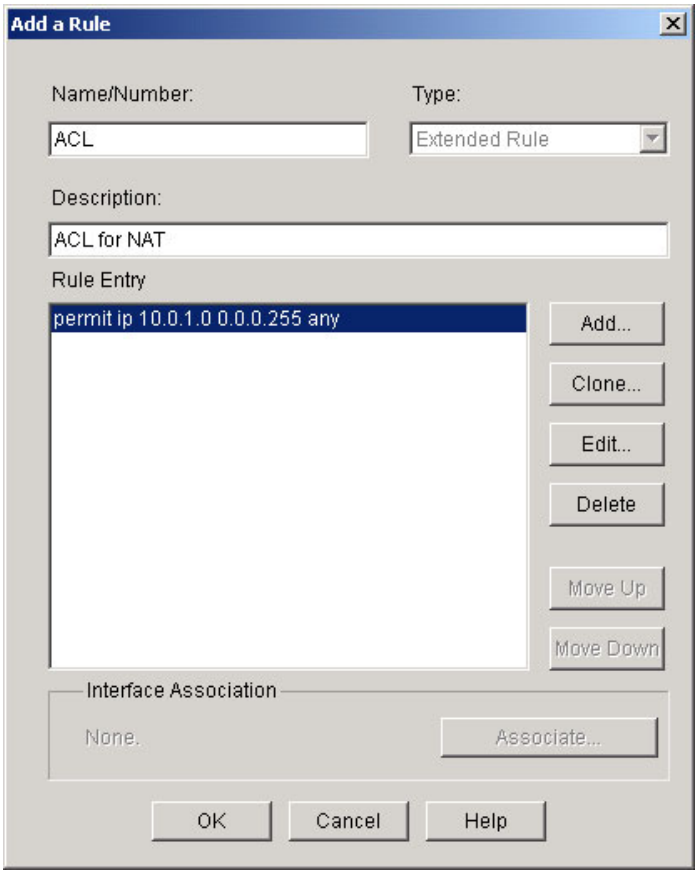
g. Click on the ACL rule button next to the **ACL Rule:** text field and click on **Create a new rule(ACL) and select…**

h. Create and Extended ACL named ACL with a description of ACL for NAT.

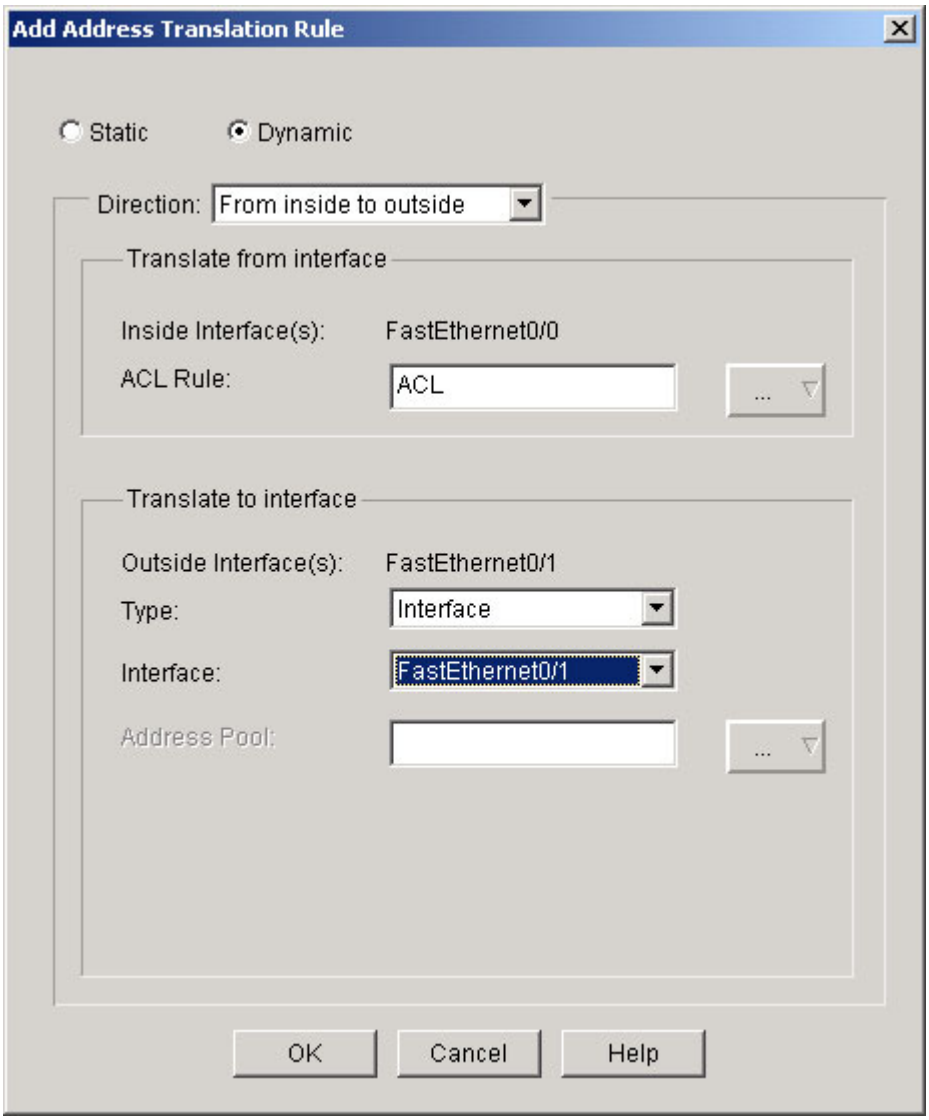
i. Click on the **Add** button and permit all IP traffic from the 10.0.P.0 network to any destination to be translated.



j. Click **OK** to return to the Add a Rule window.



k. Click **OK** to return to the Add Address Translation Rule window.



l. Select **Interface** as the type of translation.

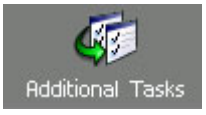
m. Choose the outside interface of **FastEthernet0/1**

n. Click the **OK** button. If the Command Delivery Status window appears, click the **OK** button on the window.

Step 7 Create a Banner

Complete the following steps to create a banner to discourage unauthorized access.

a. Select **Additional Tasks** from the Tasks bar on the Configure page.



b. Select **Banner** under **Device Properties**.

c. Click **Edit**.

d. Enter a banner to discourage unauthorized access, and then click the **OK** button to apply the configuration. If the Command Delivery Status window appears, click the **OK** button on the window.

Step 8 Management Access

Complete the following steps to rsstrict management access to the router.

a. Select **Additional Tasks** from the Tasks bar on the Configure page

b. Expand the **Router Access** menu and select **Management Access**.

c. Click the **Add** button.

d. Add the pod Host IP Address, 10.0.P.12.

e. Allow access from the FastEthernet0/0 interface

f. Check **Allow SDM**.

g. Check **Allow secure protocols only**.

What protocols are removed?

Answer: Telnet, HTTP, and SNMP are removed. SSH, HTTPS, and RCP are allowed.

h. Click **OK**.

i. A warning appears indicating that a Firewall is applied to the selected management interface. Click the **Yes** button to continue.

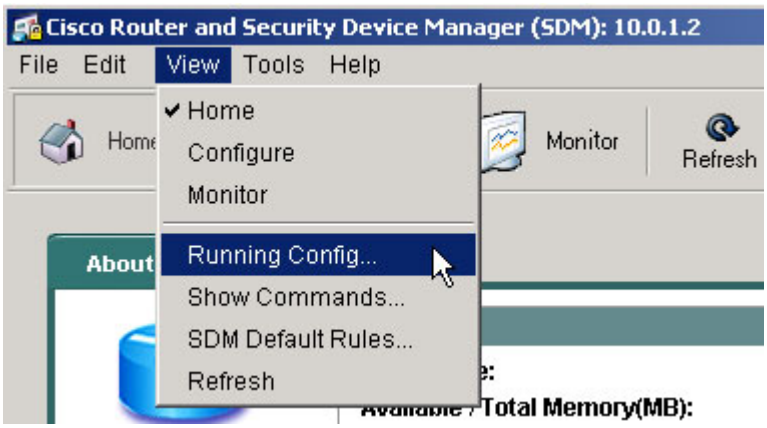
j. Click **Apply Changes**. If the Command Delivery Status window appears, click the **OK** button on the window.

k. Close the web browser and SDM. If prompted, click the Yes button to exit SDM. Open a new browser and enter **https://10.0.P.2** and reconnect to SDM. The browser refresh button may have to be used to reconnect as new keys are generated.

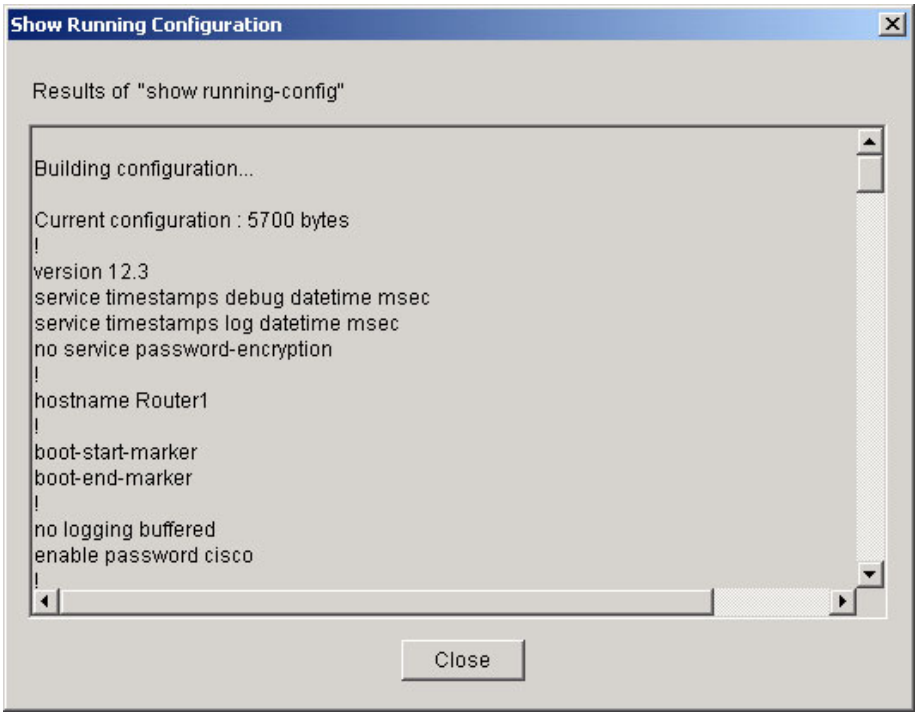
Step 10 Verify the IOS Firewall configuration

Complete the following steps to verify the running configuration.

a. In SDM, click on **View>Running Config…** from the top menu.

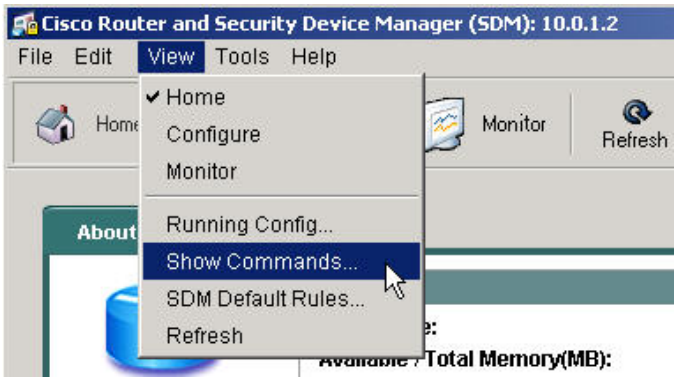


b. The running configuration window will appear.

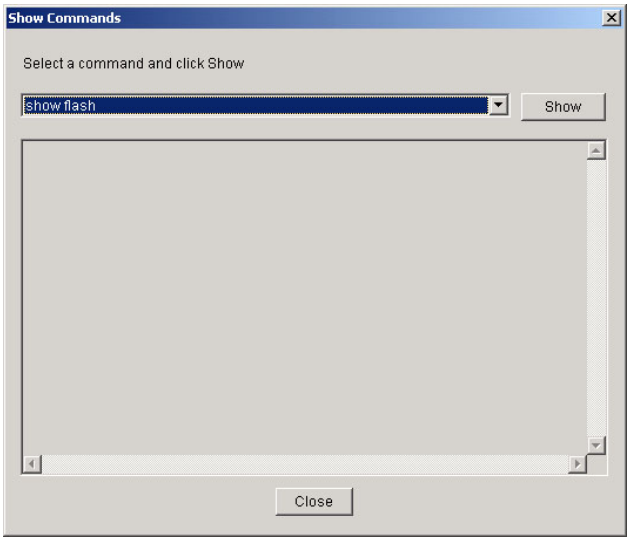


c. Scroll through and verify the configuration. Click the **Close** button when finished.

d. Next, click on **View>Show Commands…** from the top menu.



e. The Show Commands window will appear.



What commands are available?

_____

_____

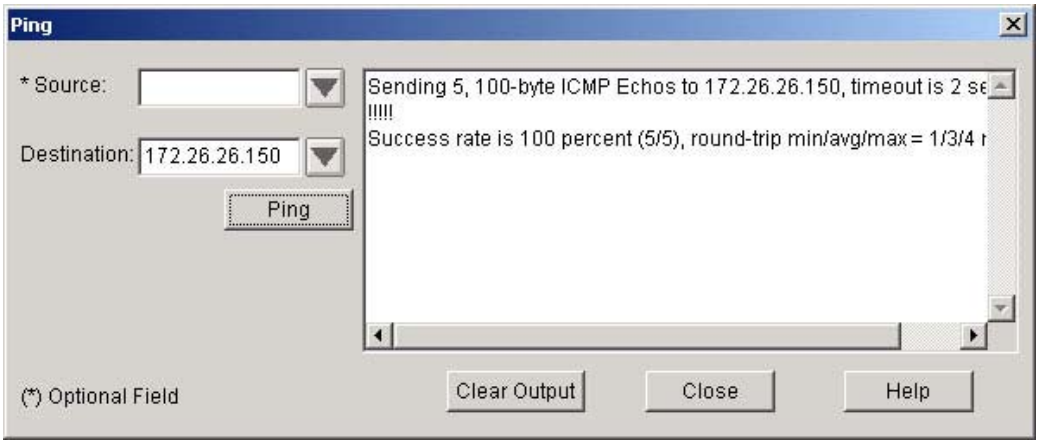
Answer: show flash, show startup-config, show access-lists, show diag, show interfaces, show protocols, and show version

f. Verify the Startup configuration using SDM. Click the **Close** button when finished.

Step 11 Verify connectivity

Complete the following steps to verify connectivity.

a. From the Student PC using SDM, ping RBB at 172.26.26.150. Click on **Tools>Ping** to access the ping window.



b. Click on the **Clear Output** button.

c. Ping the SW0 at 172.26.26.200. Click the **Close** button when finished.

d. Open a web browser and connect to RBB.

e. Next, try to access the pod router using https from an unauthorized address, such as the peer pod inside host.

f. From the Student PC, try to access the pod router via telnet or http.

```
C:\ >telnet 10.0.P.2
C:\ >telnet 10.0.1.2

Connecting To 10.0.1.2...Could not open connection to the host, on
port 23: Connect failed
```

Why is the connection refused?

_____

Answer: Because of the configuration changes made with SDM, telnet and http connections to the router cannot be made from the Student PC.

g. From the student PC, telnet to RBB. Enter the password **cisco** when prompted. Use the **who** command in user mode to verify NAT operation and view the translated source address.


```
RBB>who
    Line       User       Host(s)              Idle       Location
* 66 vty 0                 idle                 00:00:00 172.30.1.2

Interface      User        Mode                    Idle     Peer
Address
```

Notice that the 10.0.P.12 address is translated into a 172.30.P.2 address.

Lab 3.4.6a Configure the PIX Security Appliance using Setup Mode and ASDM Startup Wizard

Objective

In this lab exercise, the students will complete the following tasks:

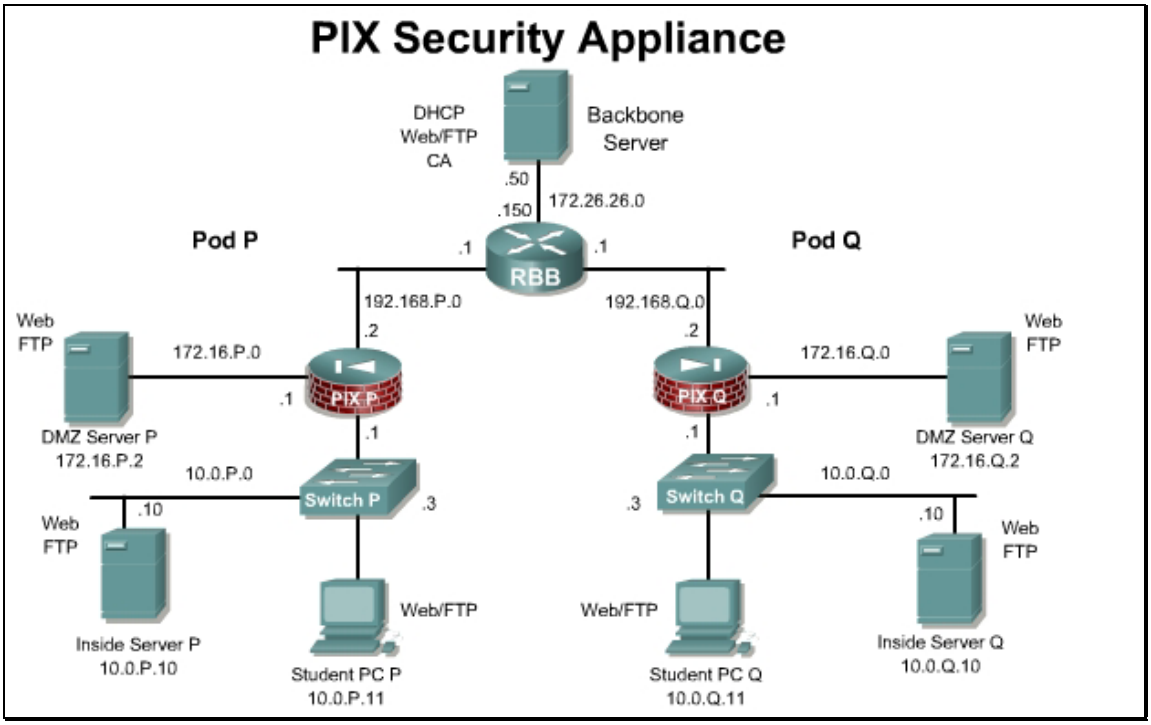
- Verify that the PIX Security Appliance and Student PC are properly cabled and installed
- Erase the current configuration.
- Configure basic settings using the Interactive Setup mode.
- Configure basic settings using the ASDM Startup Wizard.

Scenario

Company XYZ is increasing the security of their current internal network. Plans are also being made to install a publicly accessible web server. A new Cisco PIX Security Appliance has just arrived and has been installed, but requires configuration.

Topology

This figure illustrates the lab network environment:



Preparation

Begin with the standard lab topology. Access the PIX Security Appliance console port using the terminal emulator on the Student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Review the PIX Security Appliance 515E Quick Start Guide. The Quick Start guide, which ships with the PIX, is also located at the following URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_quick_start09186a00803e01f0.html

Tools and Resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional Materials

Student can use the following link for more information on the objectives covered in this lab:

http://www.cisco.com/go/pix

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
enable	Enter into privileged mode
copy tftp[:[[**//***location*] [**/***tftp_pathname*]]] **flash**[:[**image** | **asdm**]]	Change software images without requiring access to the TFTP monitor mode.
reload	Reload the PIX Security Appliance
setup	Enter into Interactive setup mode
show version	View the current PIX operating system and Adaptive Security Device Manager version
write erase	Erase the startup configuration.

Step 1 Erase the Configuration

Complete the following steps to erase the current PIX Security Appliance configuration and access the PDM wizard:

a. In the terminal window, erase the current PIX Security Appliance configuration. When prompted to confirm, press **Enter**.

```
PixP# write erase
Erase configuration in flash memory? [confirm] <Enter>
```


b. Reload the PIX Security Appliance. When prompted to confirm, press **Enter**.

```
PixP# reload
Proceed with reload? [confirm] <Enter>
```

Step 2 Configure the PIX using Setup Mode

a. When prompted to pre-configure the PIX Security Appliance through interactive prompts, press **Enter**.

b. Accept the default Firewall mode, routed, by pressing **Enter**

```
Firewall Mode [Routed]: <Enter>
```

c. Agree to use the current password by pressing **Enter**:

Note	The default password is blank.

```
Enable password [<use current password>]: <Enter>
```

d. Allow password recovery by pressing **Enter**.

```
Allow password recovery [yes]? <Enter>
```

e. Accept the default year by pressing **Enter**:

```
Clock (UTC):
Year [2005]: <Enter>
```

f. Accept the default month by pressing **Enter**:

```
Month [May]: <Enter>
```

g. Accept the default day by pressing **Enter**:

```
Day [12]: <Enter>
```

h. Accept the default time stored in the host computer by pressing **Enter**:

```
Time [11:21:25]: <Enter>
```

i. Enter the inside interface IP address of the PIX Security Appliance:

```
Inside IP address: 10.0.P.1
```

(where P = pod number)

j. Enter the network mask that applies to inside IP address:

```
Inside network mask: 255.255.255.0
```

k. Enter the hostname:

```
Host name: PixP
```

(where P = pod number)

l. Enter the DNS domain name of the network on which the PIX Security Appliance runs:

```
Domain name: cisco.com
```

m. Enter the IP address of the host running ASDM:

```
IP address of host running Device Manager: 10.0.P.11
```

(where P = pod number)

n. Enter **y** at the prompt to use the configuration and write it to the Flash memory of the PIX Security Appliance.

Step 3 Verify PIX Version 7.0(1) and PDM 5.0(0) images

Complete the following steps to install the correct image versions:

a. Enter into enable mode. Press **Enter** when prompted for a password.

```
PixP> en
```

b. Verify the correct OS image version is running.

```
PixP# show version
Cisco PIX Security Appliance Software Version 7.0(1)
Device Manager Version 5.0(0)67
```

c. If the correct OS image version and ASDM version are running, proceed to Step 4.

d. If needed, load the PIX operating system file into the PIX Security Appliance:

```
PixP# copy tftp://10.0.P.11/ pix701.bin flash
```

Note	The instructor will provide the correct location of the binary image file

e. Reload the PIX.

f. Configure the PIX using the interactive setup mode as detailed in Step 2.

g. If needed, load the ASDM files into the PIX Security Appliance:

```
PixP# copy tftp://10.0.P.11/asdm-501.bin flash:asdm
```

(where P = pod number)

Note	The instructor will provide the correct location of the binary ASDM file

Step 4 Configure the Student PC and Access PDM

a. On the Student PC, open the network control panel.

b. Configure the Student PC address as 10.0.P.11 /24 with a Gateway address of 10.0.P.1.

(where P = pod number)

c. Access the ASDM console by completing the following sub-steps:

d. On the Student PC, open a web browser. In the browser, enter **https://10.0.P.1**.

e. In the Security Alert window, click **Yes**.

f. When prompted for a username and password, leave the text fields blank and click the **OK** button.

g. The initial Cisco ASDM 5.0 window opens. Click **Run ASDM as a Java Applet**.

h. In the Warning – Security window, click **Yes**.

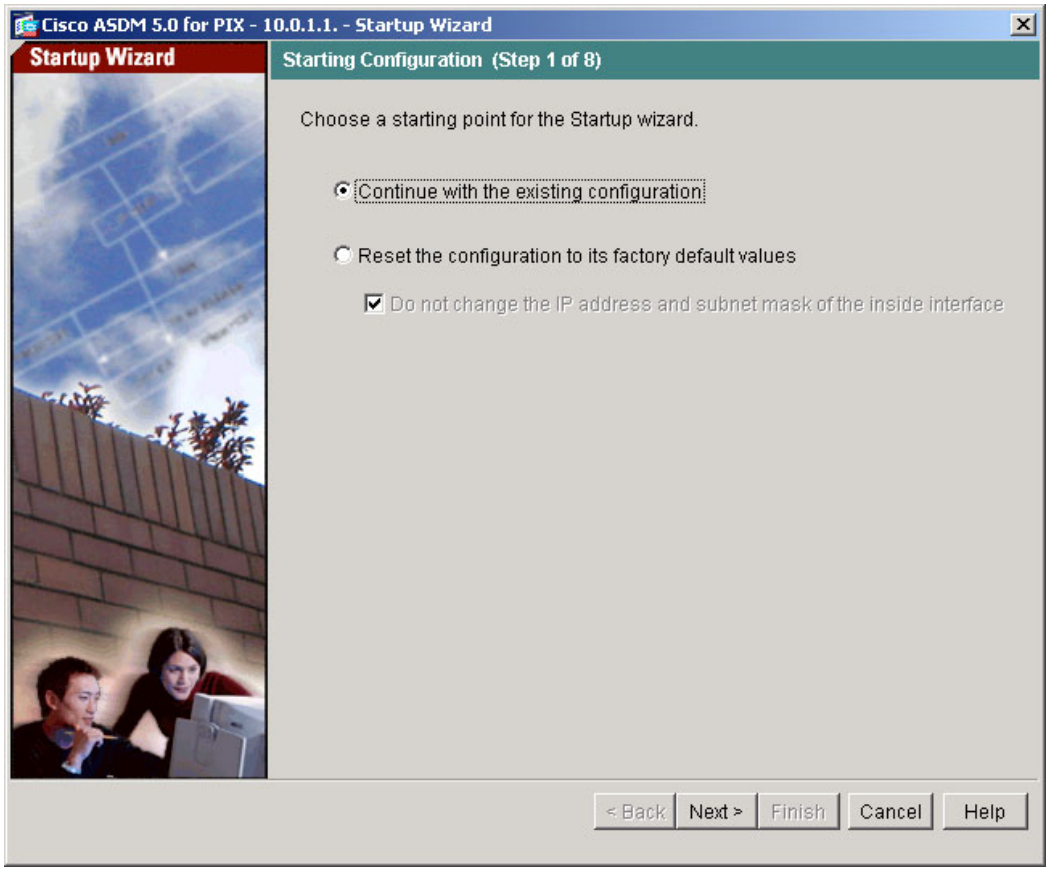
Note	Multiple security alert windows may appear when launching ASDM. If a security alert window appears, review the message contained in the window, and click **Yes** to continue

i. When prompted for the username and password, do not enter a username or password. Click **OK** to launch ASDM.

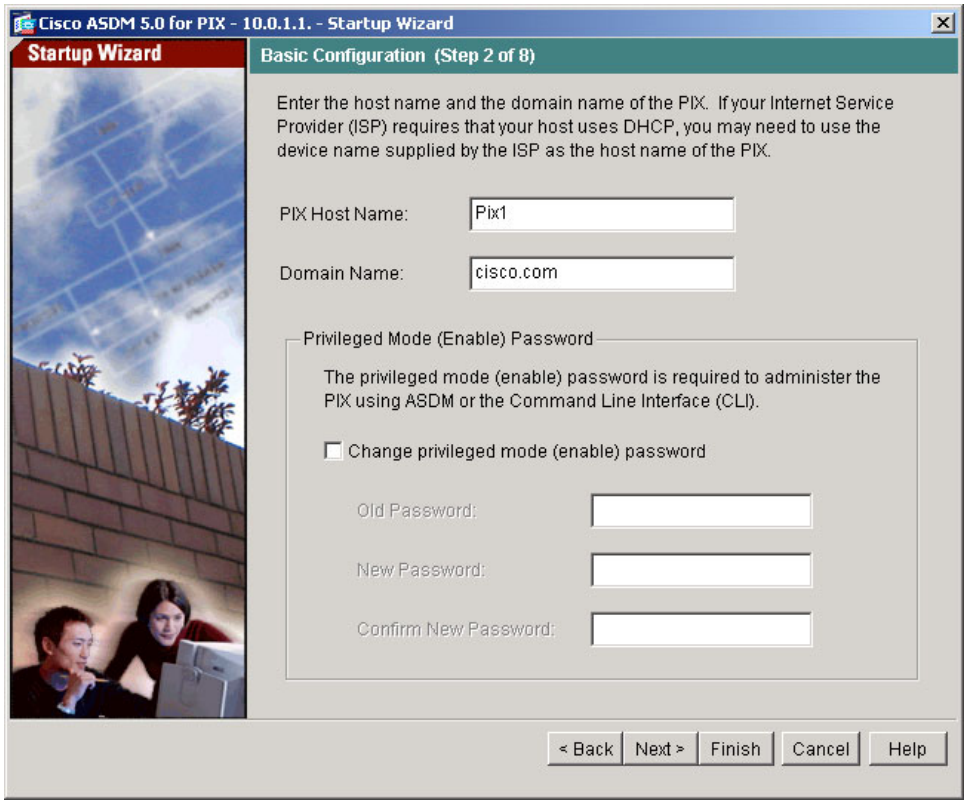
Step 5 Configure the PIX using the Startup Wizard

a. Open the Startup Wizard by navigating to **Wizards>Startup Wizard**. Click on Startup Wizard.

b. The Startup Wizard window appears. Make sure that **Continue with the Current Configuration** is selected and click the **Next** button to continue.

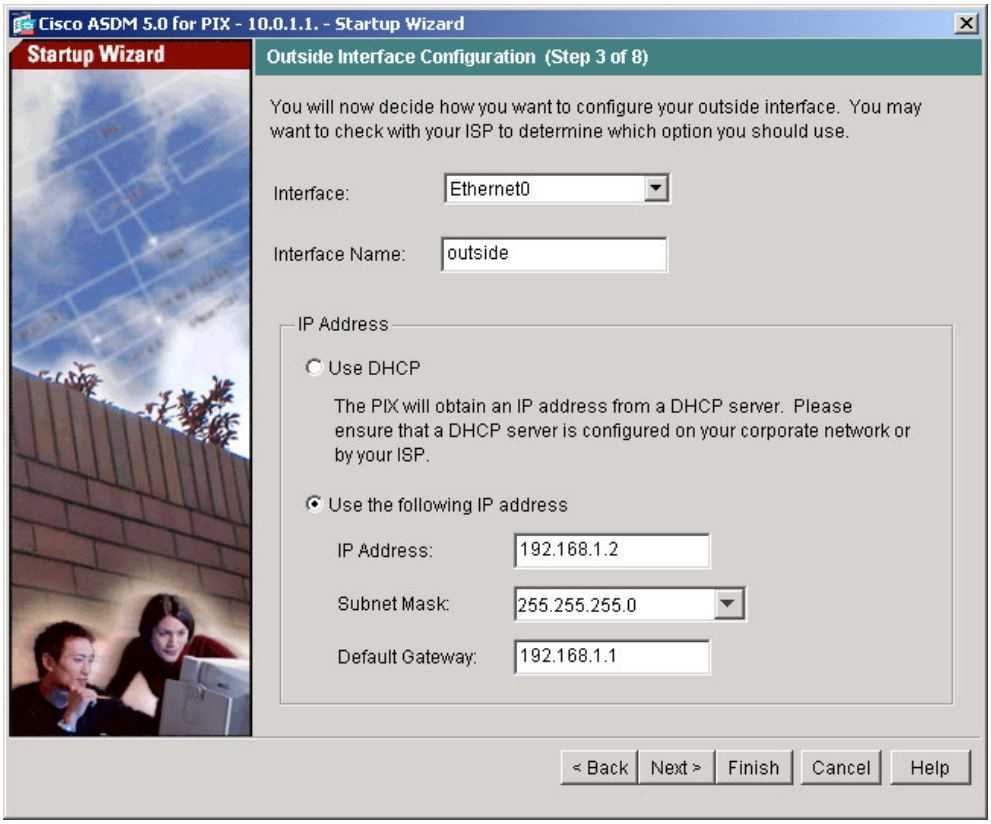


c. In the **Basic Configuration** window, use the PIX hostname, **PixP** along with the Domain Name of **cisco.com**.



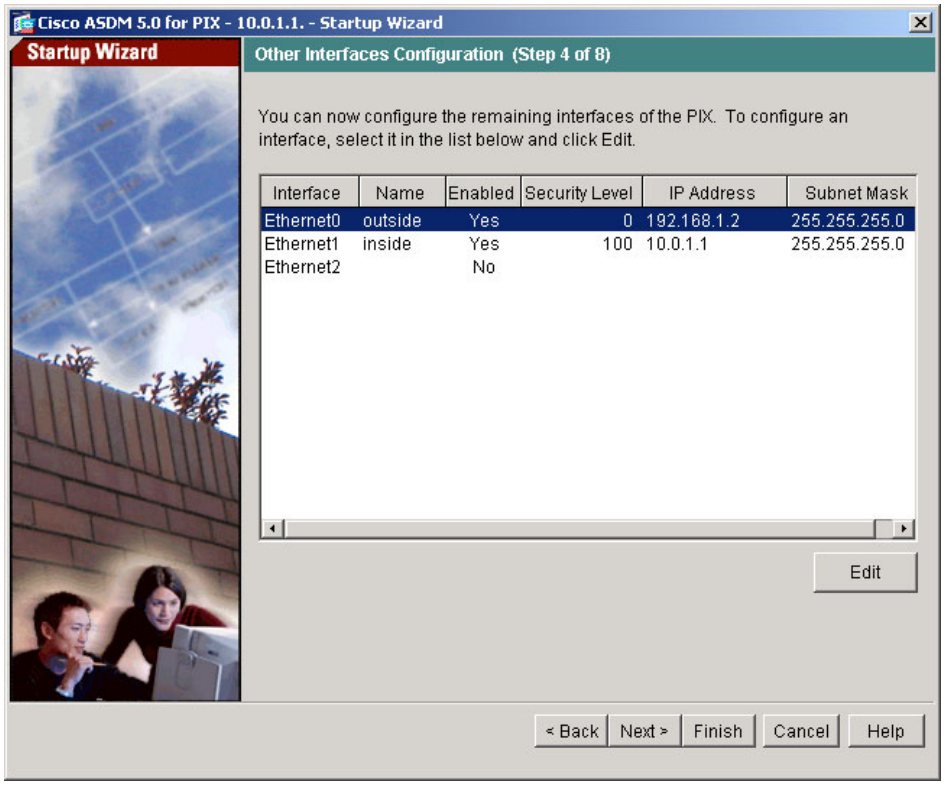
d. Click the **Next** button.

e. In the **Outside Interface Configuration** window, set an IP address of 192.168.P.2 / 24 with a default gateway of 192.168.P.1 on Ethernet 0. Name the interface **outside**.

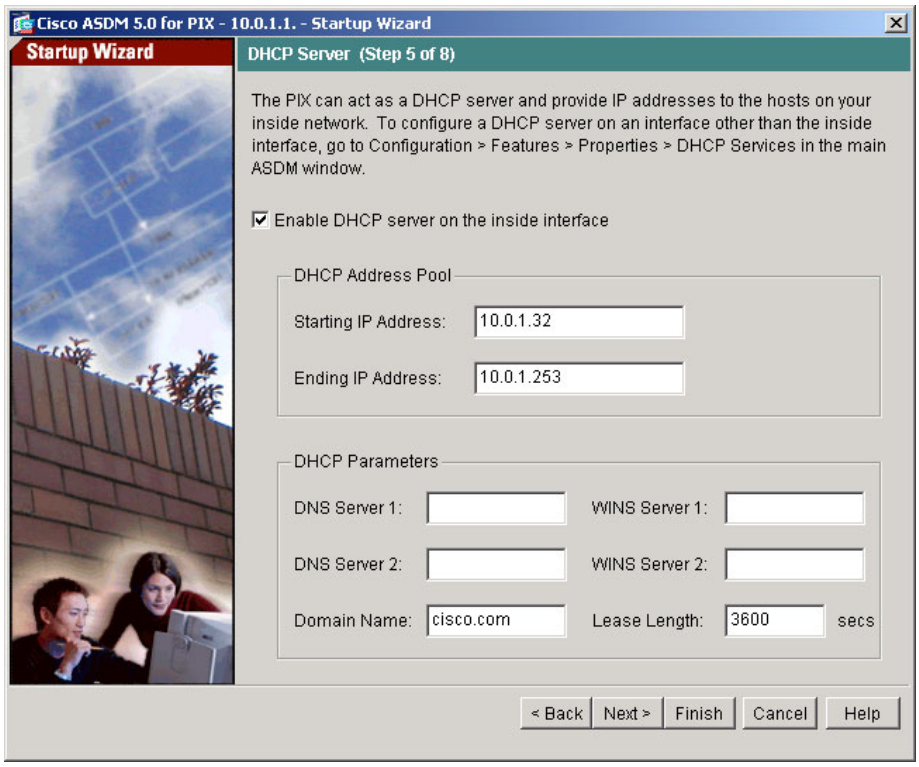


f. Click the **Next** button.

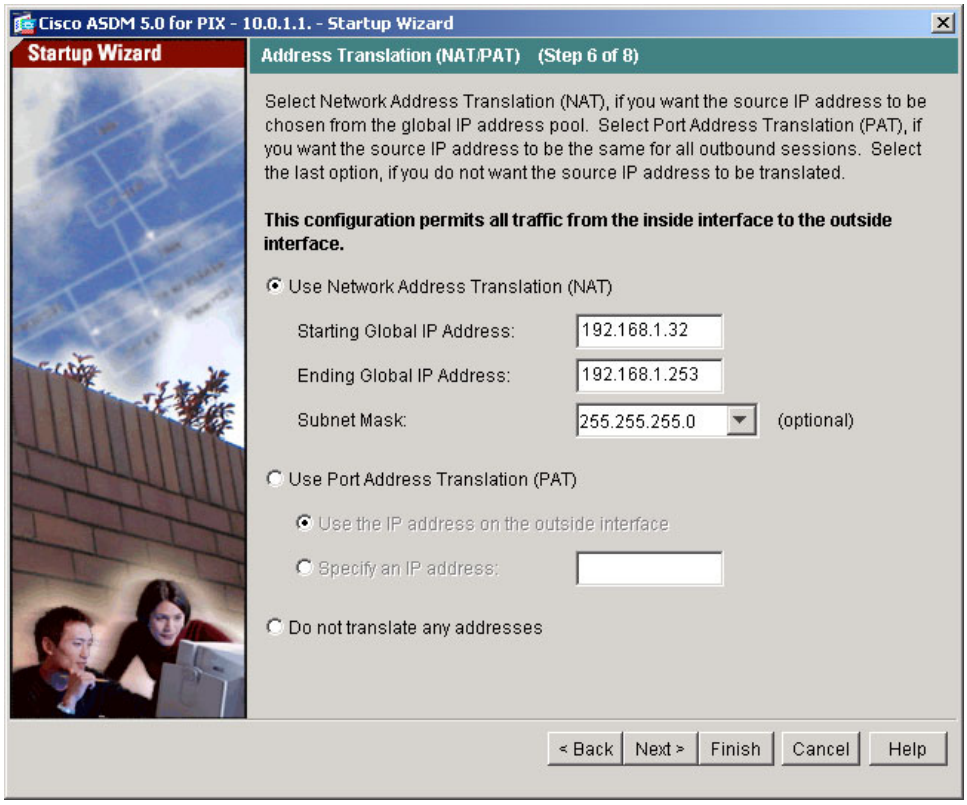
g. In the **Other Interfaces Configuration** window, verify the configuration of the inside and outside interfaces. If the configuration is incorrect, click on the **Edit** button to modify. Click the **Next** button.



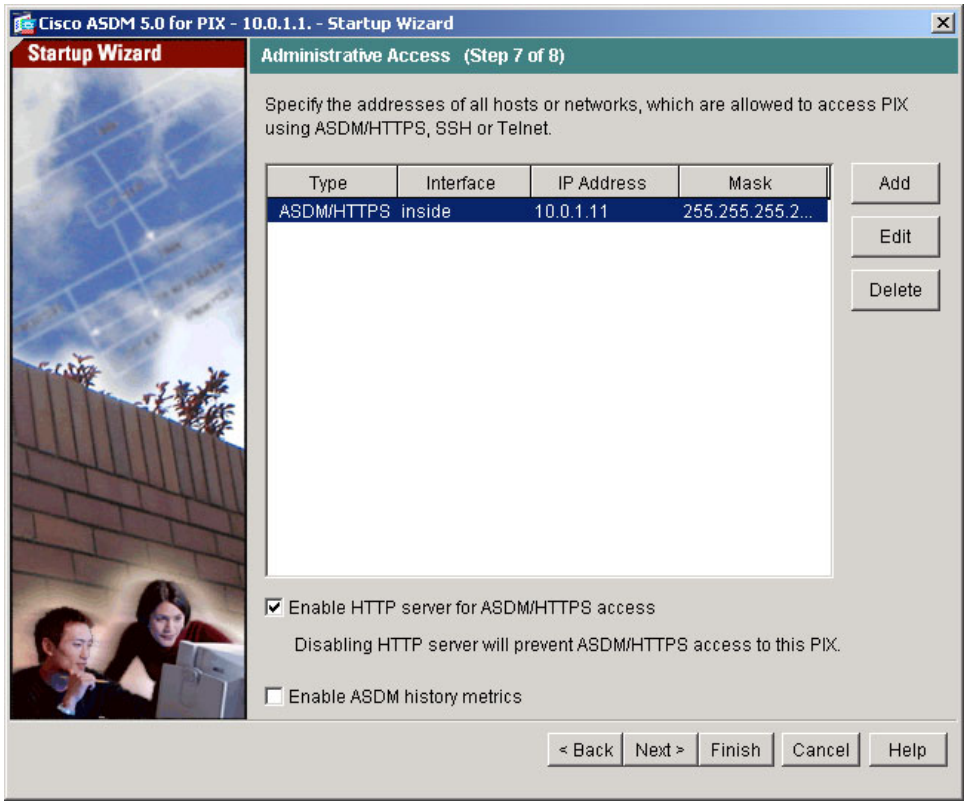
h. In the **DHCP Server** window, enable DHCP server on the inside interface. Use an address pool of 10.0.P.32 to 10.0.P.253. Enter a Domain Name of cisco.com. Use the default lease length of 3600 seconds. Click the **Next** button



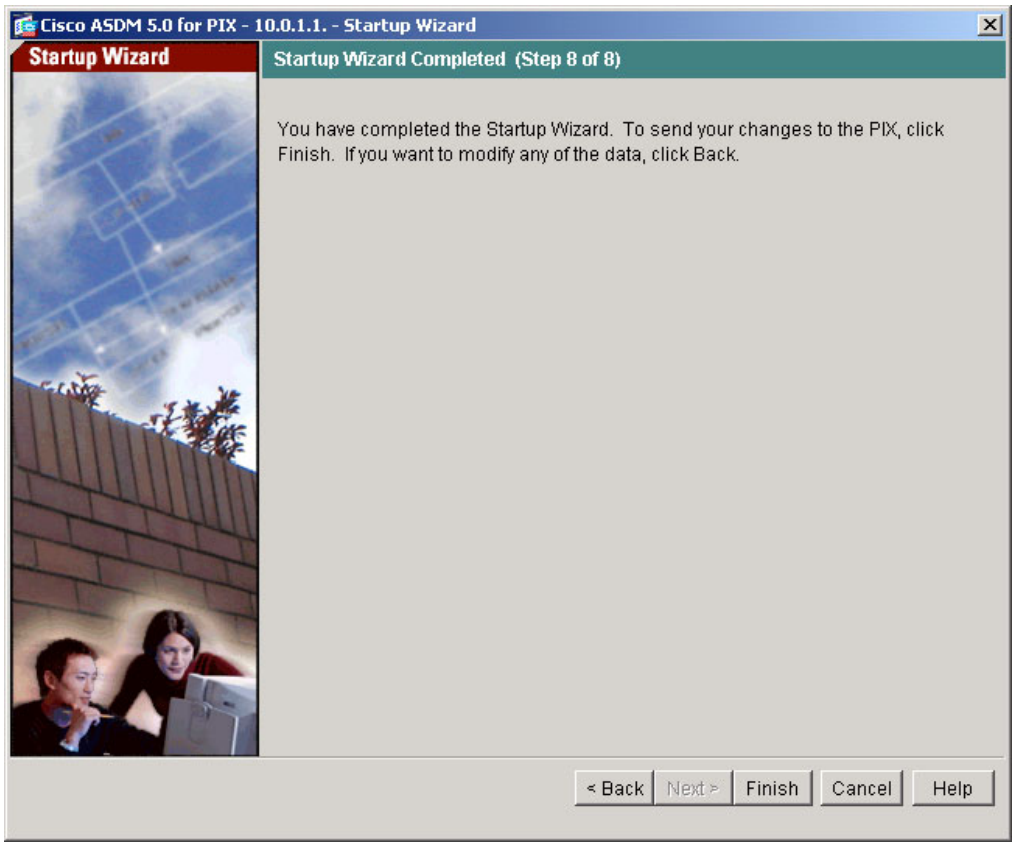
i. In the **Address Translation (NAT/PAT)** window, configure a NAT address pool of 192.168.P.32 through 192.168.P.253 with a subnet mask of 255.255.255.0. Click the **Next** button.



j. In the **Administrative Access** window, click the **Next** button.



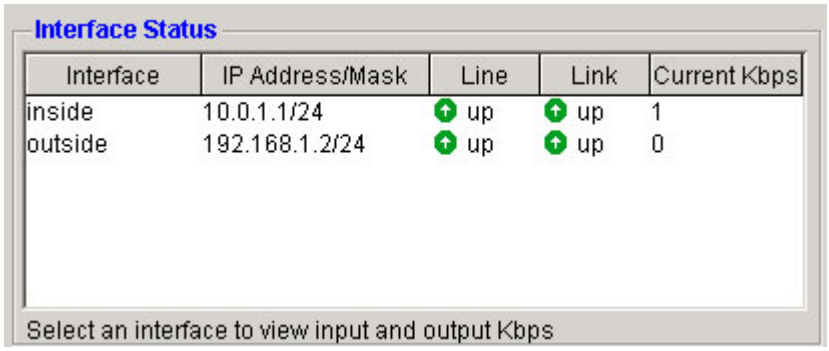
k. Click **Finish** on the **Startup Wizard Completed** window.



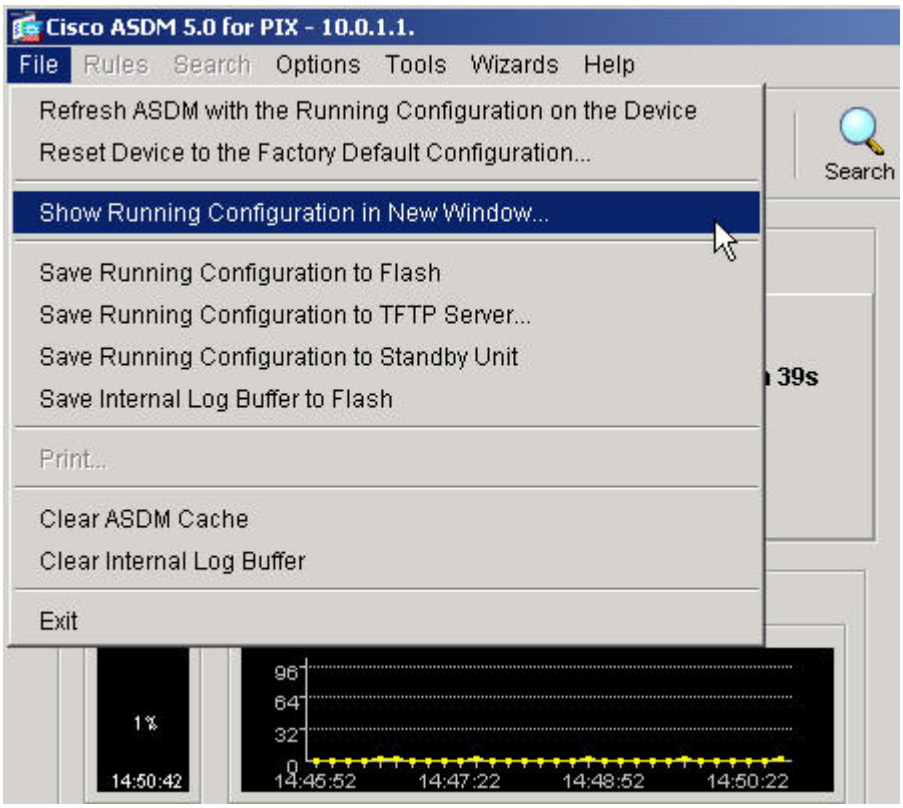
l. If the Preview CLI Commands window appears, click the **Send** button to continue.

m. Click the **Refresh** button to bring the current PIX Security Appliance configuration into ASDM.

n. Verify the status of the newly configured outside interface on the ASDM home page.



o. Navigate to **File>Show Running Configuration in New Window**.



p. Click the **Save** button to save the running configuration to Flash memory. Click the **Yes** button in the confirmation dialog box to continue.

q. If the Preview CLI Commands window appears, click the **Send** button to continue.

r. Exit PDM.

Lab 3.4.6b Configure the PIX Security Appliance using CLI

Objective

In this lab exercise, the students will complete the following tasks:

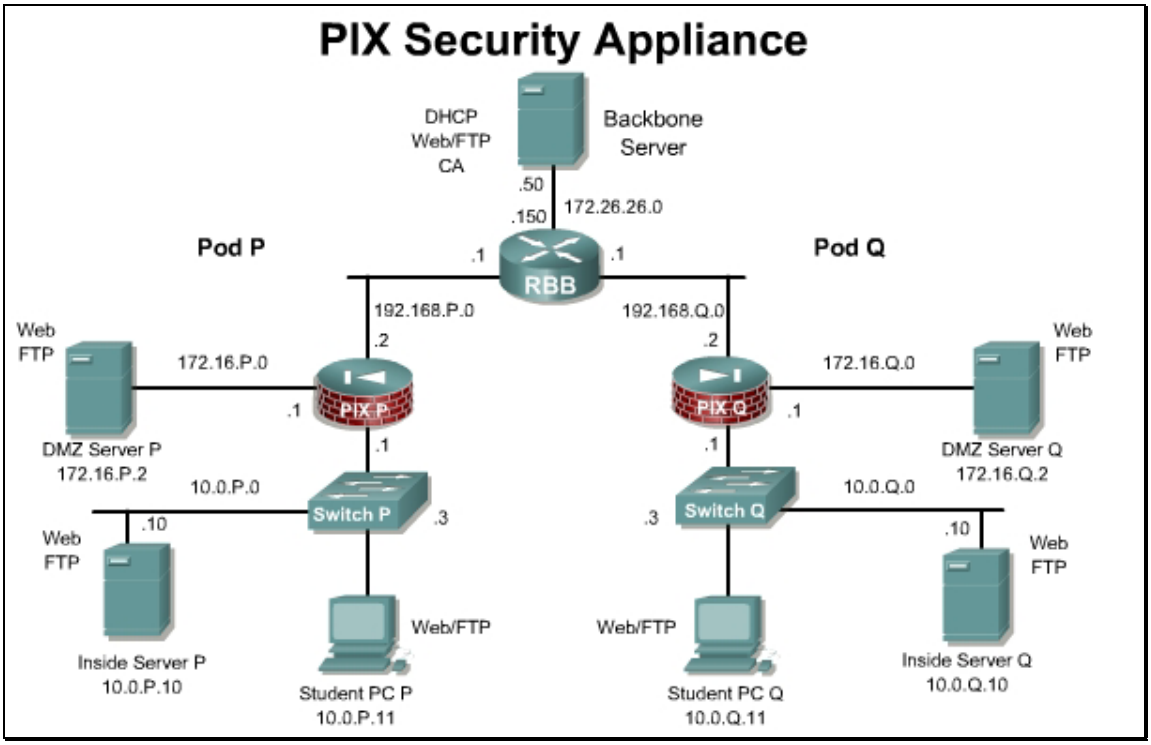
- Execute general maintenance commands.
- Configure the PIX Security Appliance inside and outside interfaces.
- Test and verify basic PIX Security Appliance operation.

Scenario

ASDM is very useful for the most common configurations; however advanced configuration and modification of existing PIX configuration are usually best completed through the CLI. Afterwards, the configuration can be pasted in PIX configuration mode. Students familiar with IOS should be able to quickly adapt to the PIX IOS-like command structure.

Topology:

This figure illustrates the lab network environment.



Preparation

Verify the devices are cabled according to the standard lab topology. Access the PIX console port using the terminal emulator on the Student PC. If desired, save the configuration to a text file for later analysis. Refer back to the “Student Lab Orientation” if more help is needed.

Tools and Resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional Materials

Further information about the objectives covered in this lab can be found at, http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080423230.html

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
interface	To configure an interface and enter interface configuration mode, use the **interface** command in global configuration mode.
ip address *ip_address* [*netmask*]	The **ip address** command defines the IP address of each interface.
nameif *if_name*	The **nameif** command defines a name of an interface. This command is used to assign interface names on the PIX Security Appliance.
security-level	To set the security level of an interface, use the **security-level** command in interface configuration mode. The interface named as inside has a default security level of 100, and the interface named as outside has a default security level of 0.
reload	The **reload** command reboots the PIX Security Appliance and reloads the configuration from a bootable floppy disk or, if a diskette is not present, from Flash memory.
route *if_name ip_address netmask gateway_ip* [metric]	Use the **route** command to enter a default or static route for an interface.
show history	The **show history** command displays previously entered commands.

Command	Description
show memory	The **show memory** command displays a summary of the maximum physical memory and current free memory available to the PIX Security Appliance operating system. Memory in the PIX Security Appliance is allocated as needed.
show running-config	The **show run** command displays the current configuration on the terminal.
show version	The **show version** command displays the following details of the PIX Security Appliance unit such as software version, operating time since last reboot, processor type, flash memory type, interface boards, serial number (BIOS ID), activation key value , timestamp for when the configuration was last modified
write erase	The **write erase** command clears the Flash memory configuration.
write memory	The **write memory** command stores the current configuration in Flash memory, along with the activation key value and timestamp for when the configuration was last modified.
write terminal	The **write terminal** command displays the current configuration on the terminal.

Step 1 Practice General Commands

The instructor will provide the procedures for access to the PIX Security Appliance console port, as this will vary according to the lab connectivity. After connecting to the PIX Security Appliance console port, the PIX Security Appliance prompt appears. If the prompt that appears is not the configuration mode prompt, enter configuration mode. The password should be null. Ask the instructor for assistance if necessary.

```
PixP>enable
Password: <Enter>
PixP#configure terminal
PixP(config)#
```

a. Erase the PIX Security Appliance default configuration. When prompted to confirm, press **Enter**.

```
PixP(config)# write erase

Erase PIX configuration in flash memory? [confirm] <Enter>
```

b. Reboot the PIX Security Appliance. When prompted to confirm, press **Enter**.

```
PixP(config)# reload

Proceed with reload? [confirm} <Enter>
```

c. The PIX Security Appliance prompts to load through interactive prompts. Press **Ctrl + Z** to escape, or type **no** at the prompt and press **Enter**. The unprivileged mode prompt appears.

```
Pre-configure PIX Firewall through interactive prompts [yes]?
Ctrl + Z

pixfirewall>
```


d. Display the list of help commands:

```
pixfirewall> ?
```

e. Enter the privileged mode of the PIX Security Appliance. When prompted for a password, press **Enter**.

```
pixfirewall> enable
Password: <Enter>
pixfirewall#
```

f. Display the list of help commands:

```
pixfirewall# ?
```

g. Use the **write terminal** or **show run** command to display the PIX Security Appliance configuration on the terminal screen.

Note Press the **Q** key to escape the PIX Security Appliance output. Press the **Enter** key to go line by line. Press the **Spacebar** to go page by page. Also, the **write terminal** and **show run** commands can be used in Privileged EXEC [pixfirewall#] and Global Configuration [pixfirewall(config)#] modes on a PIX Security Appliance. This is different from the operations of a Cisco IOS Router.

```
pixfirewall# write terminal
: Saved
:
PIX Version 7.0(1)
names
!
interface Ethernet0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
```



```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
pager lines 24
no failover
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
```



```
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
[OK]
pixfirewall#
```

h. Enter the **show memory** command:

```
pixfirewall# show memory
```

1. How many total bytes does the PIX Security Appliance have? How many bytes are free?

_____

_____

Answer: (may vary) 67108864 bytes total, 43094016 bytes free

h. Enter the **show version** command:

```
pixfirewall# show version
Cisco PIX Security Appliance Software Version 7.0(1)
Device Manager Version 5.0(1)
Compiled on Thu 31-Mar-05 14:37 by builders
System image file is "flash:/pix701.bin"
Config file at boot was "startup-config"
pixfirewall up 3 mins 37 secs
Hardware:   PIX-515E, 64 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xfff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB
 0: Ext: Ethernet0           : media index  0: irq 10
 1: Ext: Ethernet1           : media index  1: irq 11
 2: Ext: Ethernet2           : media index  2: irq 11
Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
```



```
GTP/GPRS                        : Disabled
VPN Peers                       : Unlimited
This platform has an Unrestricted (UR) license.
Serial Number: 807043526
Running Activation Key: 0xc335d572 0xa882e04f 0x24f21c7c 0xbbe45090
0x420cf18a
Configuration has not been modified since last system restart.
```

i. Enter the **show history** command:

```
pixfirewall# show history
```

1. What commands are displayed with the show history command?

_____

_____

Answer: (may vary)

enable

write terminal

show memory

show version

show history

Note: The up and down cursor keys on the keyboard can be used to recall commands. The IOS shortcuts **Ctrl + P** and **Ctrl + N** can also be used in the same way.

j. Enter the configuration mode and change the hostname to **PixP** using the **hostname** command:

```
pixfirewall# configure terminal
pixfirewall(config)# hostname PixP
```

(where P = pod number)

k. Enable the use of names rather than IP addresses:

```
PixP(config)# names
```

l. Assign the name ‘bastionhost’ to the server on the DMZ:

```
PixP(config)# name 172.16.P.2 bastionhost
```

(where P = pod number)

m. Assign the name ‘insidehost’ to the student PC:

```
PixP(config)# name 10.0.P.11 insidehost
```

(where P = pod number)

n. Save the configuration to Flash memory:

```
PixP(config)# write memory
Building configuration...
Cryptochecksum: e901c202 27a9db19 7e3c2878 0fc0966b
[OK]
```


Step 3 Configure PIX Security Appliance Interfaces

To configure PIX Security Appliance Ethernet interfaces, complete the following steps:

a. Configure the PIX Security Appliance interfaces as follows:

```
PixP(config)# interface ethernet0
Pix1(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
Pix1(config-if)# ip address 192.168.P.2 255.255.255.0
Pix1(config-if)# speed auto
Pix1(config-if)# duplex full
Pix1(config-if)# no shutdown
Pix1(config-if)# interface ethernet2
Pix1(config-if)# nameif dmz
Pix1(config-if)# security-level 50
Pix1(config-if)# ip address 172.16.P.1 255.255.255.0
Pix1(config-if)# speed auto
Pix1(config-if)# duplex full
Pix1(config-if)# no shutdown
Pix1(config-if)# interface ethernet1
Pix1(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
Pix1(config-if)# ip address 10.0.P.1 255.255.255.0
Pix1(config-if)# speed auto
Pix1(config-if)# duplex full
Pix1(config-if)# no shutdown
PixP(config)# show nameif
Interface                Name                     Security
Ethernet0                outside                    0
Ethernet1                inside                   100
Ethernet2                dmz                       50
```

Note By default the interfaces are disabled.

Note Make sure to check the switch or hub device, which connects to the PIX. A different hardware speed and duplex setting may be required.

b. Verify the interface configuration with the **show interface** command:

```
PixP(config)# show interface
Interface Ethernet0 "outside", is up, line protocol is up
Hardware is i82559, BW 100 Mbps
     Full-Duplex(Full-duplex), Auto-Speed(100 Mbps)
     MAC address 000b.fd81.e81d, MTU 1500
     IP address 192.168.1.2, subnet mask 255.255.255.0
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collisions, 0 deferred
     0 lost carrier, 0 no carrier
      input queue (curr/max blocks): hardware (128/128) software
      (0/0)
     output queue (curr/max blocks): hardware (0/0) software (0/0)
     Received 0 VLAN untagged packets, 0 bytes
     Transmitted 0 VLAN untagged packets, 0 bytes
     Dropped 0 VLAN untagged packets
Interface Ethernet1 "inside", is up, line protocol is up
Hardware is i82559, BW 100 Mbps
     Full-Duplex(Full-duplex), Auto-Speed(100 Mbps)
     MAC address 000b.fd81.e81e, MTU 1500
     IP address 10.0.1.1, subnet mask 255.255.255.0
     57 packets input, 11088 bytes, 0 no buffer
     Received 57 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collisions, 0 deferred
     0 lost carrier, 0 no carrier
      input queue (curr/max blocks): hardware (128/128) software
      (0/0)
     output queue (curr/max blocks): hardware (0/0) software (0/0)
     Received 0 VLAN untagged packets, 0 bytes
     Transmitted 0 VLAN untagged packets, 0 bytes
     Dropped 0 VLAN untagged packets
      Interface Ethernet2 "dmz", is up, line protocol is up
```



```
Hardware is i82559, BW 100 Mbps
      Full-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      MAC address 0002.b3bb.d61f, MTU 1500
      IP address 172.16.1.1, subnet mask 255.255.255.0
      54 packets input, 10812 bytes, 0 no buffer
      Received 54 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      1 packets output, 64 bytes, 0 underruns
      0 output errors, 0 collisions, 0 interface resets
      0 babbles, 0 late collisions, 0 deferred
      0 lost carrier, 0 no carrier
       input queue (curr/max blocks): hardware (128/128) software
       (0/1)
      output queue (curr/max blocks): hardware (0/1) software (0/1)
      Received 15 VLAN untagged packets, 3113 bytes
      Transmitted 1 VLAN untagged packets, 28 bytes
      Dropped 15 VLAN untagged packets
```

c. Ensure that the IP addresses are correctly configured and are associated with the proper network interface:

```
PixP(config)# show ip address
System IP Addresses:
Interface                Name      IP address      Subnet mask
Method
Ethernet0                outside   192.168.P.2     255.255.255.0
manual
Ethernet1                inside    10.0.P.1        255.255.255.0
manual
Ethernet2                dmz       172.16.P.1      255.255.255.0
manual
Current IP Addresses:
Interface                Name      IP address      Subnet mask
Method
Ethernet0                outside   192.168.P.2     255.255.255.0
manual
Ethernet1                inside    10.0.P.1        255.255.255.0
manual
Ethernet2                dmz       172.16.P.1      255.255.255.0
manual
where P = pod number)
```


d. Write the configuration to the Flash memory:

```
PixP(config)# write memory
```

e. Use the **show config** command to verify the saved configuration

```
PixP(config)# show config
```

Step 4 Configure global addresses, NAT, and routing for inside and outside interfaces

Complete the following steps to configure a global address pool, Network Address Translation (NAT), and routing:

a. Enable nat configuration requirement

```
PixP(config)# nat-control
```

b. Assign one pool of registered IP addresses for use by outbound connections:

```
PixP(config)# global (outside) 1 192.168.P.20-192.168.P.254 netmask
255.255.255.0
PixP(config)# show run global
global (outside) 1 192.168.P.20-192.168.P.254 netmask 255.255.255.0
```

(where P = pod number)

c. Configure the PIX Security Appliance to allow inside hosts to use NAT for outbound access:

```
PixP(config)# nat (inside) 1 10.0.P.0 255.255.255.0
```

(where P = pod number)

d. Display the currently configured NAT:

```
PixP(config)# show run nat
nat (inside) 1 10.0.P.0 255.255.255.0 0 0
```

(where P = pod number)

e. Assign a default route:

```
PixP(config)# route outside 0 0 192.168.P.1
```

(where P = pod number)

f. Display the currently configured routes:

```
PixP(config)# show route
S    0.0.0.0 0.0.0.0 [1/0] via 192.168.P.1, outside
C    10.0.P.0 255.255.255.0 is directly connected, inside
C    172.16.P.0 255.255.255.0 is directly connected, dmz
C    192.168.P.0 255.255.255.0 is directly connected, outside
(where P = pod number)
```

1. Is newly created default route shown in the output? What is the difference between the newly created route and the other routes displayed?

_____

_____

_____

Answer: Yes. The new route is indicated as static and the others are indicated as connected. The other routes are created from the directly connected networks, which is based on the interface configuration.

g. Copy the current configuration to Flash memory:

```
PixP(config)# write memory
```

h. Write the current configuration to the terminal and verify that the previous commands have been entered correctly:

```
PixP(config)# write terminal
: Saved
:
PIX Version 7.0(1)
names
name 172.16.1.2 bastionhost
name 10.0.1.11 insidehost
!
interface Ethernet0
 duplex full
 nameif outside
 security-level 0
 ip address 192.168.P.2 255.255.255.0
!
interface Ethernet1
 duplex full
 nameif inside
 security-level 100
 ip address 10.0.P.1 255.255.255.0
!
interface Ethernet2
 duplex full
 nameif dmz
 security-level 50
 ip address 172.16.P.1 255.255.255.0
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PixP
ftp mode passive
pager lines 24
mtu dmz 1500
mtu outside 1500
mtu inside 1500
no failover
```



```
monitor-interface dmz
monitor-interface outside
monitor-interface inside
asdm image flash:/asdm
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 192.168.P.20-192.168.P.254 netmask 255.255.255.0
nat (inside) 1 10.0.P.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.P.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
```



```
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:186cbc95531d29b184276f9e35b1579d
: end
[OK]
[OK]
```

(where P = pod number)

i. Test the operation of the global and NAT statements configured by originating connections through the PIX Security Appliance by completing the following substeps:

j. Open a web browser on the student PC.

k. From the Student PC, use a web browser to access the Backbone server at IP address 172.26.26.50 by entering **http://172.26.26.50**.

l. Observe the translation table:

```
PixP(config)# show xlate
```

The display should appear similar in the following:

```
1 in use, 1 most used
Global 192.168.P.20 Local insidehost
```

(where P = pod number)

A global address chosen from the low end of the global range has been mapped to the student PC.

Step 5 Test the Inside, Outside, and DMZ Interface Connectivity

To test and troubleshoot interface connectivity using the PIX Security Appliance **ping** command, complete the following steps:

a. Ping the inside interface:

```
PixP(config)# ping 10.0.P.1
Sending 5, 100-byte ICMP Echos to 10.0.P.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

b. Ping the inside host:

```
PixP(config)# ping insidehost
Sending 5, 100-byte ICMP Echos to insidehost, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

c. Ping the outside interface:

```
PixP(config)# ping 192.168.P.2
Sending 5, 100-byte ICMP Echos to 192.168.P.2, timeout is 2 seconds:
!!!!!
```



```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(where P = pod number)

d. Ping the backbone router:

```
PixP(config)# ping 192.168.P.1
Sending 5, 100-byte ICMP Echos to 192.168.P.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(where P = pod number)

e. Ping the DMZ interface:

```
PixP(config)# ping 172.16.P.1
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(where P = pod number)

f. Ping the bastion host:

```
PixP(config)# ping bastionhost
Sending 5, 100-byte ICMP Echos to bastionhost, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10
ms
```


Lab 3.6.3 Configuring the PIX Security Appliance with ASDM

Objective

In this lab exercise, the students will complete the following tasks:

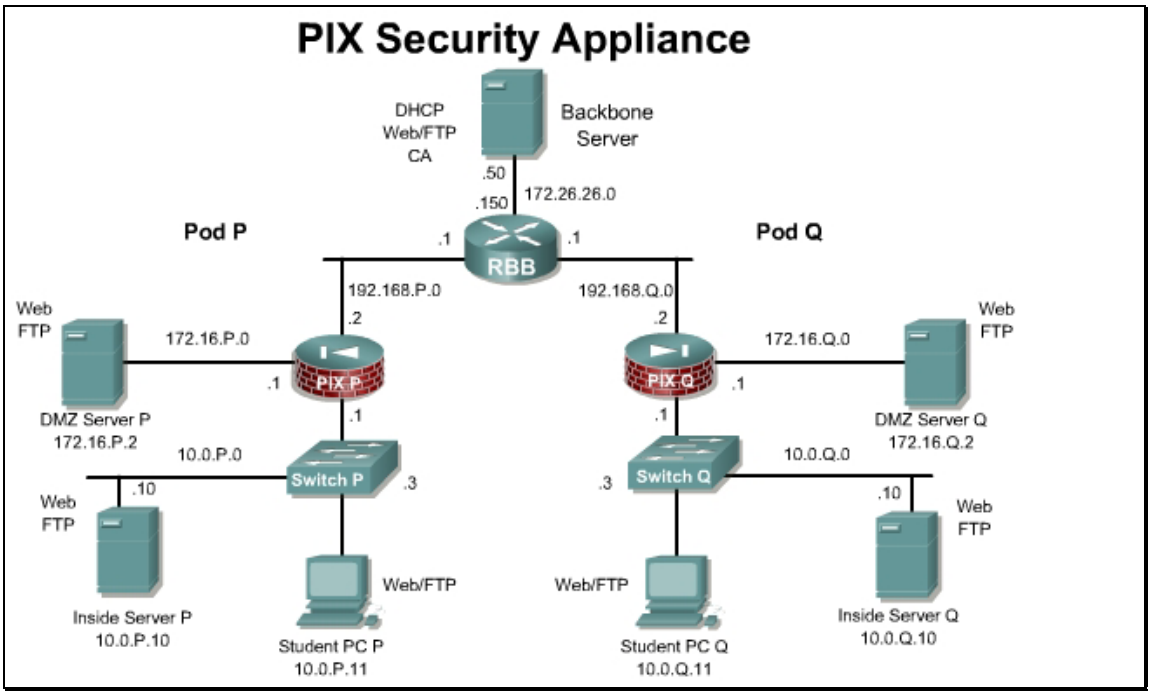
- Configure basic settings using ASDM
- Configure outbound access with NAT.
- Test connectivity through the PIX Security Appliance.
- Configure Banners
- Configure Telnet and SSH for remote access

Scenario

The Cisco Adaptive Security Device Manager is a browser-based configuration tool that enables administrators to set up, configure, and monitor the PIX Security Appliance graphically, without requiring an extensive knowledge of the PIX Security Appliance command-line interface (CLI).

Topology

This figure illustrates the lab network environment:



Preparation

Begin with the standard lab topology. Access the PIX Security Appliance console port using the terminal emulator on the Student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and Resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional Materials

Student can use the following link for more information on ASDM:

http://www.cisco.com/go/asdm

If needed, a TFTP server can be found at http://www.weird-solutions.com/

If needed, a SSH client can be found at http://www.chiark.greenend.org.uk/~sgtatham/putty/

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
reload	Reload the PIX Security Appliance
write erase	Erase the startup configuration.

Step 1 Erase the Current PIX Security Appliance Configuration

Complete the following steps to erase the current PIX Security Appliance configuration and allow access the PIX using ASDM:

a. In the Terminal window, erase the current PIX Security Appliance configuration. When prompted to confirm, press **Enter**.

```
PixP# write erase
Erase PIX configuration in flash memory? [confirm] <Enter>
```

b. In the Terminal window, reload the PIX Security Appliance. When prompted to confirm, press **Enter**.

```
PixP# reload
Proceed with reload? [confirm] <Enter>
```

c. When prompted to pre-configure the PIX Security Appliance through interactive prompts, press **Enter**.

d. Accept the default Firewall mode, routed, by pressing **Enter**

```
Firewall Mode [Routed]: <Enter>
```

e. Agree to use the current password by pressing **Enter**:

```
Enable password [<use current password>]: <Enter>
```


f. Allow password recovery by pressing **Enter**.

```
Allow password recovery [yes]? <Enter>
```

g. Accept the default year by pressing **Enter**:

```
Clock (UTC):
Year [2002]: <Enter>
```

h. Accept the default month by pressing **Enter**:

```
Month [Nov]: <Enter>
```

i. Accept the default day by pressing **Enter**:

```
Day [14]: <Enter>
```

j. Accept the default time stored in the host computer by pressing **Enter**:

```
Time [11:21:25]: <Enter>
```

k. Enter the inside interface IP address of the PIX Security Appliance:

```
Inside IP address: 10.0.P.1
```

(where P = pod number)

l. Enter the network mask that applies to inside IP address:

```
Inside network mask: 255.255.255.0
```

m. Enter the hostname:

```
Host name: PixP
```

(where P = pod number)

n. Enter the DNS domain name of the network on which the PIX Security Appliance runs:

```
Domain name: cisco.com
```

o. Enter the IP address of the host running ASDM:

```
IP address of host running Device Manager: 10.0.P.11
```

(where P = pod number)

p. Enter **y** at the prompt to save the information to the Flash memory of the PIX Security Appliance.

Step 2 Verify the Student PC Configuration

a. Open the network control panel.

b. Verify that the Student PC address is 10.0.P.11 /24 with a Gateway address of 10.0.P.1.

(where P = pod number)

c. Access the ASDM console by completing the following sub-steps:

d. Open a web browser and enter **https://10.0.P.1**. to access ASDM.

e. In the Security Alert window, click **Yes**.

f. The initial Cisco ASDM 5.0 window opens. Click **Run ASDM as a Java Applet**.

g. In the Warning – Security window, click **Yes**.

Note: Multiple security alert windows may appear when launching ASDM. If a security alert window appears, review the message contained in the window, and click **Yes** to continue

h. When prompted for a username and password, do not enter a username or password. Click **OK** to launch ASDM.

Step 3 Configure the Inside and Outside Interfaces of the PIX Security Appliance

Complete the following steps to configure the inside and outside interfaces of the PIX Security Appliance, establish a default route, enable NAT for the internal network, and create a global pool of addresses for address translation:

a. Click the **Configuration** button to navigation to the Configuration screen..

b. Select **Interfaces** from the Features panel.

c. Configure the inside interface by completing the following sub-steps:

   i. Double-click in the row for **ethernet1** in the Interfaces table. Click the **OK** button when a warning about loss of connectivity appears. The Edit Interface window opens.

   ii. Verify that the Enable Interface check box is selected.

   iii. Verify that inside appears in the Interface Name field.

   iv. Verify that 10.0.P.1 appears in the IP Address field.

   (where P = pod number)

   v. Verify that 255.255.255.0 appears in the Subnet Mask drop-down menu.

   vii. Verify that 100 appears in the Security Level field.

   viii. Click **OK** to close the Edit Interface window.

d. Configure the outside interface by completing the following sub-steps:

   i. Double-click in the row for **ethernet0** in the Interfaces table. Click the **OK** button when a warning about loss of connectivity appears. The Edit Interface window opens.

   ii. Select the **Enable Interface** check box.

   iii. Enter the interface name **outside** in the Interface Name field.

   iv. Select the **Use Static IP** radio button within the IP Address group box.

   v. Enter **192.168.P.2** in the IP Address field.

   (where P = pod number)

   vi. Choose **255.255.255.0** from the Subnet Mask drop-down menu.

   viii. Enter **0** in the Security Level field.

   ix. Click **OK**. Click the **OK** button in the Security Level Change window.

   x. Click the **Apply** button**.**

   xi If the Preview CLI Commands window appears, click the **Send** button to continue.

e. To establish a default route, complete the following sub-steps:

   i. Select **Routing** from the Features panel.

   ii. Expand the **Routing** branch in the Categories tree.

   iii. Choose **Static Route** from the Routing list.

   iv. Select **Add** from the Static Route group box. The Add Static Route window opens.

   v. Choose **outside** from the Interface Name drop-down menu.

   vi. Enter **0.0.0.0** in the IP Address field.

   vii. Enter **0.0.0.0** in the Mask drop-down menu.

   vii. Enter **192.168.P.1** in the Gateway IP field.

   (where P = pod number)

   viii. Verify that 1 appears in the Metric field.

ix. Click **OK**. The static route appears in the Static Route table.

x. Click the **Apply** button.

xi. If the Preview CLI Commands window appears, click the **Send** button to continue.

f. Configure a global pool of addresses to be used for address translation by completing the following sub-steps:

i. Select **NAT** from the Features panel.

ii. Click the **Manage Pools** button. The **Manage Global Address Pools** window opens.

iii. Click **Add**. The **Add Global Pool** Item window opens.

iv. Choose **outside** from the Interface drop-down menu.

v. Enter **1** in the Pool ID field.

vi. Verify that the Range radio button is selected.

vii. Enter 192.168.P.32 in the first IP address field.

(where P = pod number)

viii. Enter 192.168.P.254 in the second IP address field.

(where P = pod number)

ix. Enter 255.255.255.0 in the Network Mask field.

x. Click **OK** to return to the **Mange Global Address Pools** window.

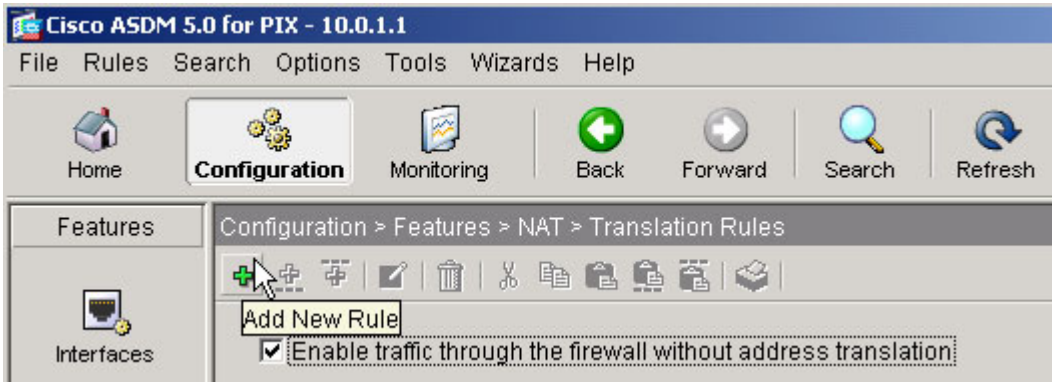
xi. Click **OK** to close the **Manage Global Address Pools** window.

xii. Click the **Apply** button. If the Preview CLI Commands window appears, click the **Send** button to continue.

g. Configure NAT by completing the following sub-steps:

i. Verify that the **Translation Rules** panel is still active.

ii. Verify that the **Translation Rules** radio button is selected.



iii. Choose **Rules>Add** from the main menu or click on the **Add New Rule** icon. The **Add Address Translation Rule** window opens.

iv. Verify that the inside interface is chosen in the **Interface** drop-down menu.

v. Click **Browse**. The **Select host/network** window opens.

vi. Verify that the inside interface is chosen in the drop-down menu.

vii. Select the inside network by doing the following:

viii. Click **10.0.P.0** in the directory structure list.

(where P = pod number)

ix. Click **OK**. This will return to the Add **Address Translation Rule** window.

x. Verify that outside is chosen in the **Translate address on Interface** drop-down menu.

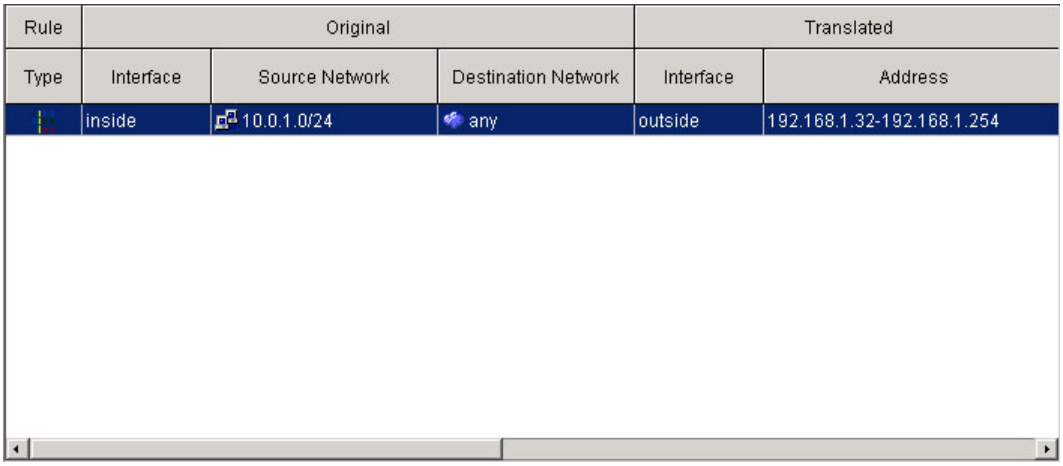
xi. Verify that **Dynamic** is selected in the **Translate Address To** group box.

xii. Choose **1** from the **Address Pool** drop-down menu.

xiii. Verify that the global pool configured earlier, 192.168.P.32–192.168.P.254, appears under **Address**.

(where P = pod number)

xiv. Click **OK** in the **Add Address Translation Rule** window. The new rule appears in the rules table.



Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	10.0.1.0/24	any	outside	192.168.1.32-192.168.1.254

xv. Click **Apply**. If the Preview CLI Commands window appears, click the **Send** button to continue.

Step 4 Test Interface Connectivity and NAT

Complete the following steps to test interface connectivity and NAT:

a. Test interface connectivity by completing the following sub-steps:

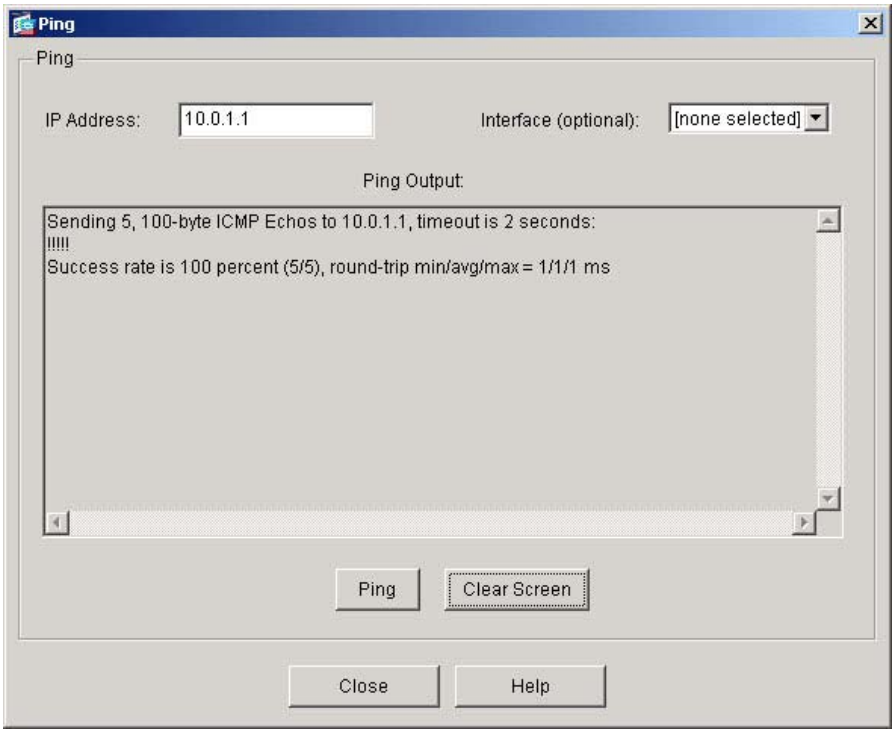
i. Choose **Tools> Ping**.

ii. In the IP Address field, enter **10.0.P.1**.

(where P = pod number)

iii. Click **Ping**.

iv. Observe the following output in the Ping Output window. The output should appear similar to the following:



v. Click Clear Screen.

b. Repeat the ping for the following IP addresses. A response for all pings should be received:

- The inside host:

  10.0.P.11

  (where P = pod number)

- The outside interface:

  192.168.P.2

  (where P = pod number)

- The backbone router:

  192.168.P.1

  (where P = pod number)

c. Exit the Ping window by clicking **Close**.

d. Test the operation of the global and NAT configured by originating connections through the PIX Security Appliance. To do this, complete the following sub-steps:

i. Open a web browser on the student PC.

ii. Use the web browser to access the SuperServer web page at IP address 172.26.26.50 by entering **http://172.26.26.50**.

Note	An HTTP connection is used as a test here because ICMP pings are not allowed through the PIX by default.

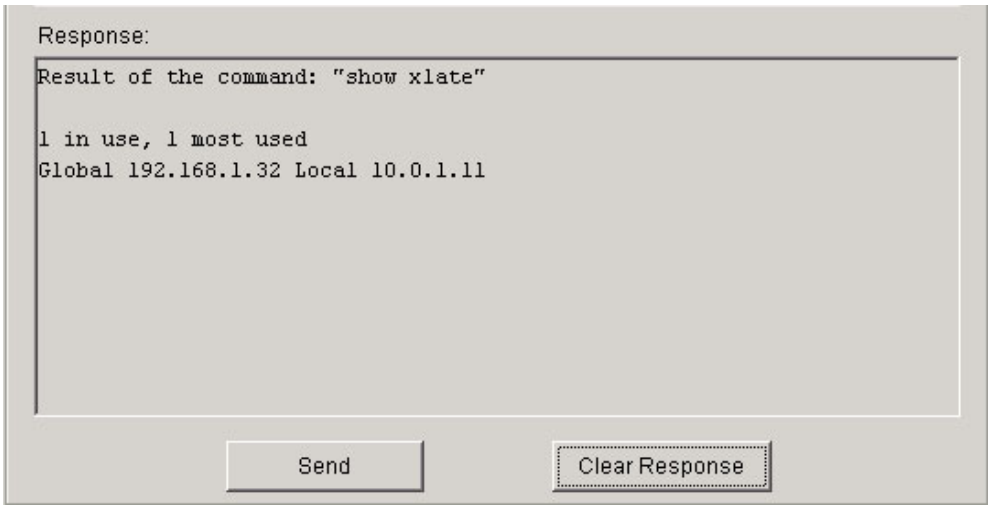
e. Observe the translation table by completing the following sub-steps:

i. Choose **Tools> Command Line Interface**. The Command Line Interface window opens.

ii. In the Command field, enter **`show xlate`**.

iii. Click **Send**.

iv. Observe the output in the Response field. It should appear similar to the following:



Note that a global address chosen from the low end of the global range has been mapped to the student PC.

f. Exit the Command Line Interface window by clicking **Close**.

Step 5 Configure remote access to the PIX Security Appliance

Complete the following steps to configure remote access to the PIX for remote configuration.

a. Select **Device Administration** from the Features panel.

b. Select **Administration>Telnet** from the tree menu.

c. Click the **Add** button in the Telnet window.

d. Configure the following values:

1. Interface Name: inside
2. IP Address: 10.0.P.11
3. Mask: 255.255.255.255

e. Click the **OK** button.

f. Set the timeout to 10 minutes.

g. Click the **Apply** button.

h. If the Preview CLI Commands window appears, click the **Send** button to continue.

i. From the Student PC, telnet to the PIX

```
C:\>telnet 10.0.P.1
```

j. Login with the default password **cisco**.

k. Exit the telnet session.

l. Navigate to **Administration>Password** in the tree menu.

m. Change the Telnet password to **cisco123**.

n. Click the **Apply** button.

o. If the Preview CLI Commands window appears, click the **Send** button to continue.

p. From the Student PC, telnet to the PIX.

```
C:\>telnet 10.0.P.1
```


q. Login with the password **cisco123**.

r. Exit the telnet session.

Note	Telnet is not recommended for remote access since the username and password are sent in clear text. SSH or SSL is recommended.

Step 6 Configure Banners

Complete the following steps to configure the PIX banners.

a. Navigate to **Administration>Banner** in the tree menu.

b. Configure the following banners.

1. Session: Session Banner - Authorized users only
2. Login: Login Warning - Authorized users only
3. Message of the Day: MOTD - Authorized users only

c. Click the **Apply** button.

d. If the Preview CLI Commands window appears, click the **Send** button to continue.

e. From the Student PC, telnet to the PIX

```
C:\>telnet 10.0.P.1
```

f. Login with the password **cisco123.** Note the appearance of the session banner.

g. Return to the ASDM interface and click on the **Monitoring** button on the main menu bar.

h. Click on **Administration** in the Features panel and **Telnet Sessions** in the tree menu. Note the **Currently Connected Telnet Sessions**.

i. On the Student PC, exit the Telnet session.

j. Return the Telnet monitoring window and click the **Refresh** button. The session entry should disappear.

Step 7 Configure Secure remote access to the PIX Security Appliance

Complete the following steps to configure secure remote access to the PIX for remote configuration.

a. Click on the **Configuration** button.

b. Click on **Device Administration** in the Features panel..

c. Click on **Key Pair** in the tree menu.

d. Click the **Add** button. The **Add Key Pair** window appears.

e. Verify that **Use default RSA key** is selected, and that the modulus size is 1024. Click **Generate Now** to create a new RSA key pair to be used when establishing an SSH connection to the PIX.

f. To configure the hosts that are permitted to make SSH connections to the PIX Security Appliance, click on **Secure Shell** in the tree menu.

g. Click the **Add** button and then configure the following values:

a. Interface Name: inside

b. IP Address: 10.0.P.11

c. Mask: 255.255.255.255

h. Click the **OK** button.

i. Set the timeout to 10 minutes

j. Click the **Apply** button.

k. If the Preview CLI Commands window appears, click the **Send** button to continue.

l. From the student PC, open a SSH client (PuTTY or equivalent) and login into the PIX at 10.0.P.1.

m. Login with credentials

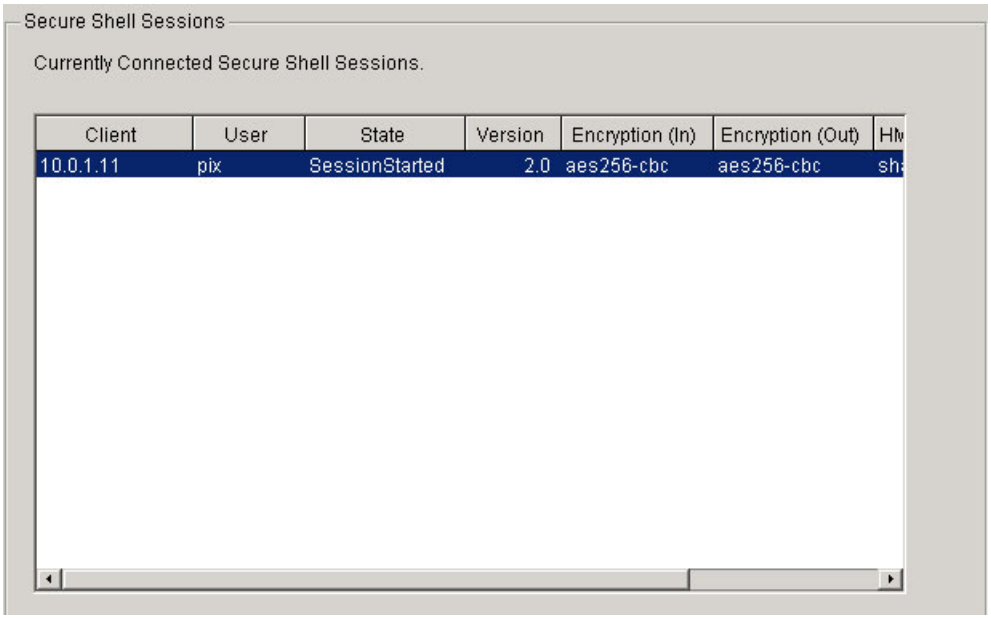
   a. Username: pix

   b. Password: cisco123

n. Note the banners configured previously.

o. Return to the ASDM interface and click on the **Monitoring** button on the main menu bar.

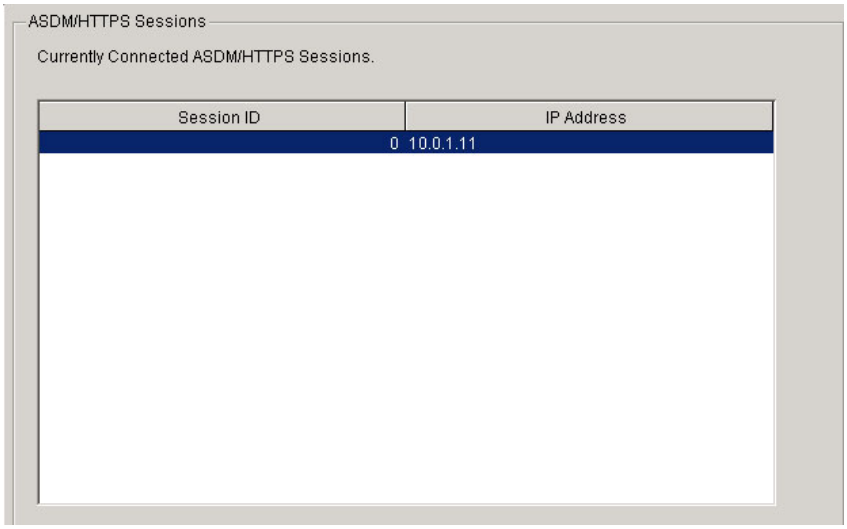
p. Click on **Secure Shell Sessions** in the tree menu. Note the **Currently Connected Secure Shell Sessions**.



q. On the Student PC, exit the SSH session.

r. Return the Secure Shell monitoring window and click the **Refresh** button. The Session entry should disappear.

s. Click on **ASDM/HTTPS Sessions** in the tree menu. Note the **Currently Connected ASDM/HTTPS Sessions.**



t. The current ASDM session will be displayed. Note that this session can be disconnected by selecting the session in the widow and then clicking the **Disconnect** button.

u. Exit PDM. When prompted to save the configuration, click the **Don't Save** button.

Lab 5.2.1 Install and Configure CSACS 3.3 for Windows

Objective

In this lab, the students will complete the following tasks:

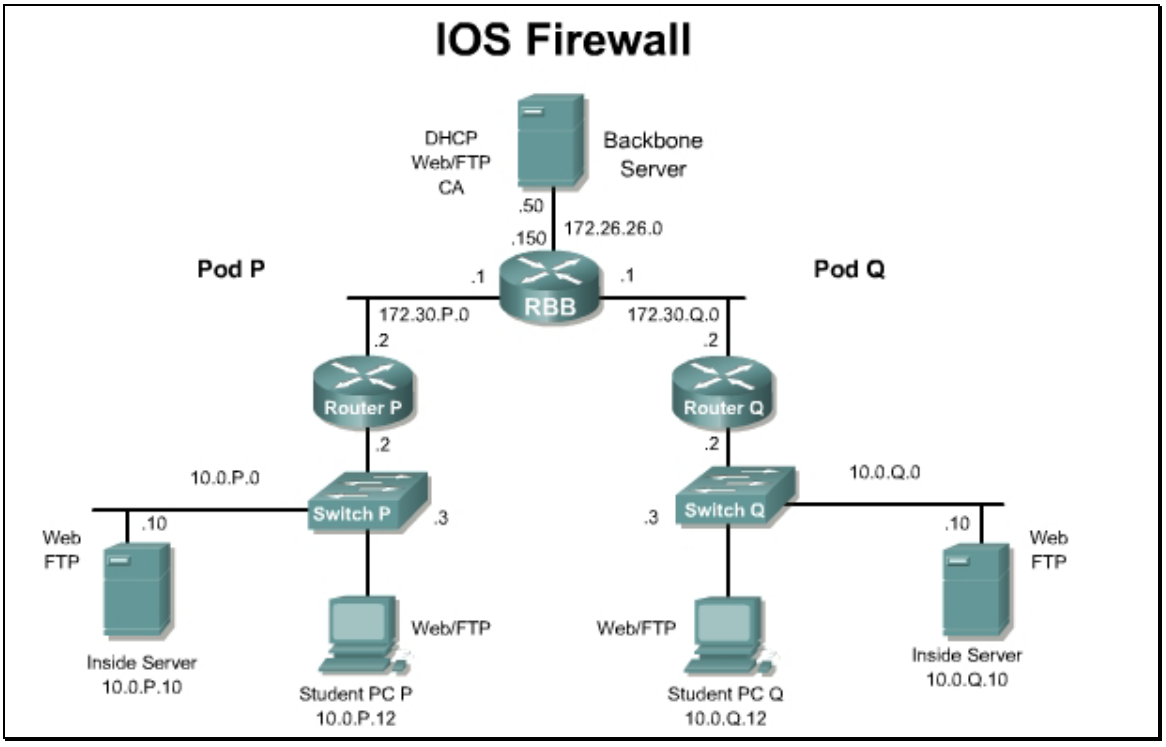
- Install Cisco Secure Access Control Server (CSACS) for Windows 2000
- Take a tour of CSACS for Windows

Scenario

Cisco Secure Access Control Server for Windows 2000/NT Servers (Cisco Secure ACS) network security software helps administrators authenticate users by controlling dial-in access to a network access server (NAS) device, an access server, Cisco PIX Security Appliance, switch, wireless access point, or router. Cisco Secure ACS operates as a Windows NT or Windows 2000 service and controls the authentication, authorization, and accounting (AAA) of users accessing networks.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the student PC. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- Cisco Secure Access Control Server (CSACS) version 3.3 or later for Windows 2000

Additional materials

The following websites provide additional information on CSACS:

- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_qanda_item09186a0080094bac.shtml
- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a0080115464.shtml
- http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_configuration_examples_list.html

Step 1 Install CSACS 3.3 for Windows 2000

Complete the following steps to install CSACS on the Windows 2000 server. This procedure assumes that the Windows 2000 server is operational.

a. Log in to Windows 2000 server using the administrator account. The instructor will provide the correct username and password combination for the administrator account.

b. Open the CSACS folder on the PC. Begin the CSACS installation by double-clicking the **Setup.exe** file. The CSACS for Windows NT/2000 installation wizard starts. Ignore any warning messages concerning memory requirements.

c. Click **Accept** to acknowledge the terms of the CAACS license agreement. Click **Next** to close the 'Welcome' window. Check all items listed in the 'Before You Begin' window and click **Next**. Click **Next** to accept the default settings in the 'Choose Destination Location' window.

d. Complete the following substeps within the Authentication Database Configuration window:

   i. Check the **Also Check the Windows User Database** option.

   ii. Check the **Yes refer to "Grant dialin permission to user" setting** check box.

   iii. Click **Next**.

e. Check all of the check boxes within the Advanced Options window and click **Next**. It is important to check all of the check boxes as this will determine the ACS options that will be available for configuration later.

f. Accept the default settings within the Active Service Monitoring window by clicking **Next**.

g. Accept default settings within the CiscoSecure ACS Service Initiation window by clicking **Next**. Setup then starts the CiscoSecure service.

h. Click **Finish**. A web browser will start with the Cisco Secure ACS v3.3 homepage.

i. Click on the **Interface Configuration** button, Click the **Advanced Options** text link.

Check the **Network Device Groups** box and click the **Submit** button.

j. Click on the **Network Configuration** button.

k. Click on the **(Not Assigned)** text link in the Network Device Groups window.

l. Click on the top **Add Entry** button in the AAA Clients section. Complete the following sub steps within the Add AAA Server window:

   i. Select **TACACS+ (Cisco IOS)** from the Authenticate Users Using scroll box.

   ii. Enter the name of the pod router to be used as the NAS in the AAA Client Hostname box. For example, Router1, Router2, and so on.

   iii. Enter the IP address (10.0.P.2) of the pod router inside interface in the Access Server IP Address box.

   iv Enter ***secretkey*** (one word and all lowercase) in the TACACS+ or RADIUS key box.

   v. Finish adding the pod router as the AAA client by clicking the **Submit+Restart** button.

m. Click on the Network Configuration button.

n. Click on the (Not Assigned) text link under Network device Group.

o. Click the Add Entry button in the AAA Servers section. Complete the following sub steps within the Cisco Secure ACS Add AAA Server window:

   i. Enter a name for the sudent PC, for example **studentP**, in the AAA Server Name box (where P = pod number).

   ii. Enter the IP Address of the student PC (**10.0.P.12**) in the AAA Server IP Address box (where P = pod number).

   iii. Enter **secretkey** (one word and all lowercase) in the Key field.

   iv. Make sure that **Cisco Secure ACS** is selected for the AAA Server Type.

   v. Make sure that **inbound/outbound** is selected for Traffic Type.

p. Finish adding the PC as the AAA Server by clicking the **Submit+Restart** button.

q. Close the Internet Explorer window containing the Cisco Secure ACS main window.

r. Close any open windows.

s. Using Windows Task Manager (**Ctrl**+**Alt**+**Delete** > **Task Manager**) check to see if the following services are now running on the Windows 2000 server PC:

   - CSAdmin.exe
   - CSAuth.exe
   - CSDBSync.exe
   - CSLog.exe
   - CSMon.exe
   - CSRadius.exe
   - CSTacacs.exe

   If these services are not listed as running, restart the Windows 2000 server PC and repeat this step.

   If all of the tasks are running, CSACS 3.3 for Windows 2000 has been successfully installed.

Step 2 Take a Grand Tour of CSACS for Windows

Complete the following steps to become familiar with the CSACS for Windows administration interface, and to change some global settings.

a. Start the ACS configuration manager by double-clicking the **ACS Admin** desktop icon.

b. Select the **Cisco Systems** icon at the top of the left frame.

1. What is displayed in the right frame? What is the release version?

_____

Answer: The CSACS home page; Version 3.3 or later.

c. Examine the user setup functions by completing the following substeps:

i. Select **User Setup** in the left frame.

ii. Enter **aaauser** in the User text box. Then click on the **Add/Edit** button.

iii. Enter the password **aaapass** in the **Password** and **Confirm Password** fields of the **User Setup** section.

iv. Press the **Submit** button.

v. Select the **List All Users** button.

1. How many users are configured?

_____

Answer: 1, aaauser.

d. Examine the group setup functions by completing the following substeps:

i. Select **Group Setup** in the left frame.

1. What group is shown in the Group window?

_____

Answer: The Default group.

ii. Select the **Users in Group** button in the center frame.

1. How many users are in the group?

_____

Answer: 1 user.

e. Select **Network Configuration** in the left frame:

1. How many AAA Clients are configured?

_____

Answer: One

f. Examine the system configuration functions by completing the following substeps:

i. Select **System Configuration** in the left frame.

ii. Select the **Service Control** text link in the System Configuration window and answer the following question.

1. What is the status of the Cisco Secure service, level of detail for logging, and frequency of the new file generation?

_____

Answer: Cisco Secure is currently running, the level is low, new file every day.

iii. Select **Cancel** to return to the select list.

iv. Select the **Logging** text link in the System Configuration window and answer the following question.

1. What log targets are enabled?

_____

Answer: Failed Attempts, RADIUS Accounting, TACACS+ Accounting, TACACS+ Administration.

v. Select **Cancel** to return to the select list.

vi. In the System Configuration window, select **Local Password Management** and then review the Password Validation Options, answer the following, and then select Cancel to return to the select list.

1. What is the purpose of the password validation options?

_____

Answer: Enables control of password length when users change their password.

vii. Select the **Cisco Secure Database Replication** text link in the System Configuration window, answer the following, and then select **Cancel** to return to the select list.
If this option does not appear, click Interface Configuration > Advanced Options and then check the CiscoSecure Database Replication checkbox and the Distributed System Settings checkbox.

1. What is the purpose of **Cisco Secure** Replication Setup?

_____

Answer: Enables control of database replication components, scheduling, and partners.

viii. Select the **ACS Backup** text link in the System Configuration window, answer the following, and then select **Cancel** to return to the select list.

1. Where can the ACS user and group databases be backed up?

_____

Answer: A local or networked directory; however the default is **C:\Program Files\CiscoSecureACSv3.3\CSAuth\System Backups**.

ix. Select the **ACS Restore** text link in the System Configuration window, answer the following, and then select **Cancel** to return to the select list.

1. What components can be backed up and restored?

_____

Answer: User and group database and the Cisco Secure ACS System Configuration.

x. Select the **ACS Service Management** text link in the System Configuration window, answer the following, and then select **Cancel** to return to the select list.

1. How can a system administrator be notified of events that are logged?

_____

Answer: Events can be logged to the NT/2000 event log, or an e-mail notification of the event can be sent to the system administrator.

g. Examine the interface configuration functions by completing the following substeps:

i. Select **Interface Configuration** in the left frame.

ii. Select the **User Data Configuration** text link in the Interface Configuration window, answer the following, and then select **Cancel** to return to the select list.

1. How are user-defined fields useful?

_____

Answer: Unique information that will be displayed for each specific user, such as location or department and can have the information reflected in the accounting logs if desired.

iii. Select the **Advanced Option** text link in the Interface Configuration window, perform the following task, and answer the following question.

iv. Ensure that all of the options are checked.

1. What is the purpose of selecting advanced options?

_____

_____

_____

_____

Answer: Advanced features can be configured that will appear in the user interface. Select only applicable features, reducing the complexity of the CSACS windows displayed.

v. Select **Submit** to return to the select list.

vi. Select the **TACACS+ (Cisco IOS)** text link in the Interface Configuration window, perform the following tasks, and answer the following questions.

If this option is not present, a AAA client needs to be added. This is done on the Network Configuration page. Click the **Add Entry** Button and enter the AAA Client Hostname, AAA Client IP Address, and the Key **secretkey**. Click the **Submit+Restart** button to finish adding the client.

vii. In the TACACS+ Services window, ensure PPP IP, PPP LCP, PPP Multilink, and Shell (exec) are selected.. These services will be available when clicking the Edit Settings button on the Group Setup page.

viii. In the Advanced Configuration Options window, ensure that all four of the boxes are checked. When the Advanced TACACS+ Features option is checked, TACACS+ options can be enabled for individual users on the User Setup page.

ix. Select **Submit** to return to the select list.

1. Where are the TACACS+ services and advanced configuration objects applied in this window?

_____

_____

Answer: TACACS+ Services and Advanced Configuration Objects configured in the TACACS+ (Cisco) window are applied and appear as selectable options in the User and Group setup windows for each user and group.

h. Click on the **Administration Control** button in the left frame.

1. What administrator accounts are configured?

_____

Answer: No administrator accounts are configured at this time.

2. What is the purpose of administrator control?

_____

_____

Answer: Administrator accounts can be added, deleted, and controlled from a web browser. Administrator passwords, privileges, system configuration, reports, and activities can be controlled.

i. Examine the external user database functions by completing the following substeps:

   i. Select **External User Databases** in the left frame.

   ii. Select the **Unknown User Policy** text link in the External User Databases window and answer the following questions

      1. What two options are available if a user is not found in the Cisco Secure database?

         _____

         _____

         Answer: Answers will vary. It depends on what configuration was created during the installation.

      2. Which one is the default?

         _____

         Answer: Answers will vary It depends on what configuration was created during the installation.

      3. What external databases can be checked for the unknown user?

         _____

         _____

         Answer: The Windows NT or Windows 2000 user database, or any configured, supported external database. For example, CRYPTOCard, ODBC, and so forth.

j. Select **Cancel** to return to the select list.

   i. Select the **Database Group Mappings** text link in the External User Databases window. Select **Cancel** to return back to the select list.

   ii. Select the **Database Configuration** text link in the External User Databases window, answer the following, and then select **Cancel** to return to the select list.

      1. What can be configured in the External User Database Configuration window?

         _____

         Answer: The external user database used for authentication

k. Examine the reports and activity functions by completing the following substeps:

   i. Select Reports and Activity in the left frame.

   ii. Select the **Administration Audit** text link in the Reports and Activity window, and answer the following question.

      1. What appears in the Administration Audit.csv file?

         _____

         Answer: A record of all administration actions.

l. Select **Online Documentation** in the left frame.

   i. Take a moment to browse the new features, software requirements, and troubleshooting sections of the online documentation.

Lab 6.1.3 Configure Local AAA on Cisco Router

Objective

In this lab, the students will complete the following tasks:

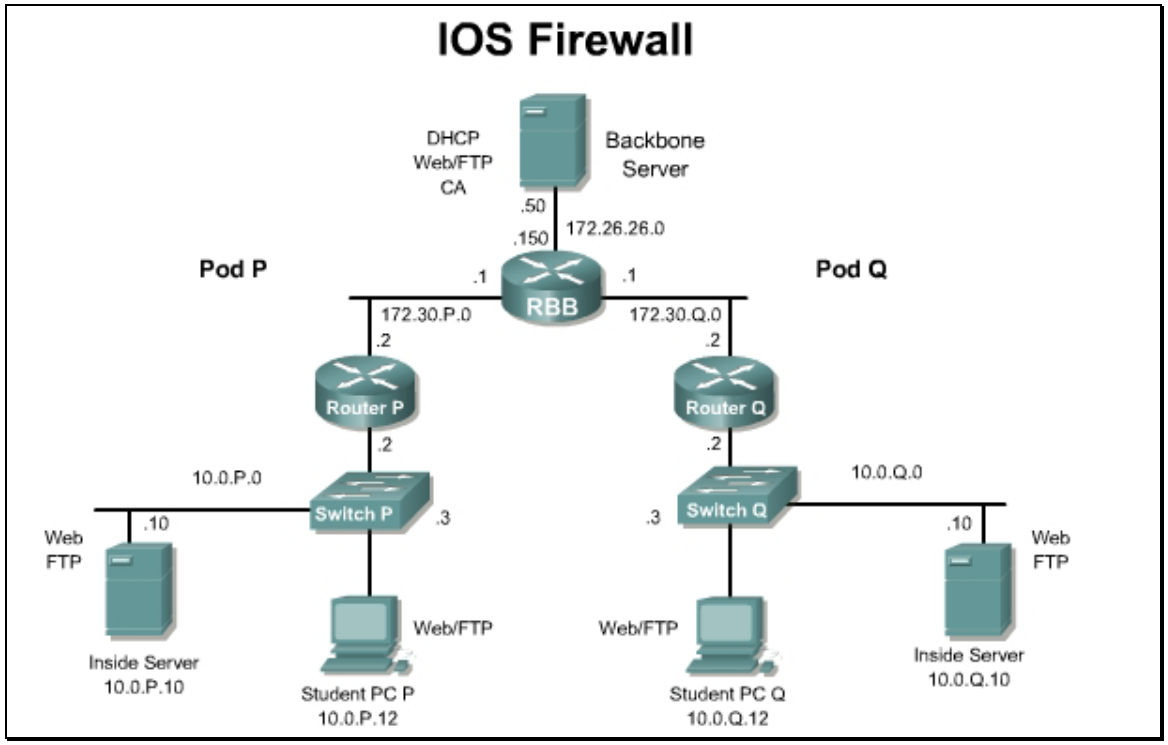
- Securing and testing access to the privileged EXEC, VTY, and console
- Configuring local database authentication using AAA
- Verify and test the AAA configuration

Scenario

Access control is a means network administrators can use to control who is allowed access key network devices and what services they are allowed to use once they have access. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which network administrators can set up access control.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the student PC. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

Additional Materials

The following websites provide additional information on AAA:

- http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d980f.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d9811.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d9810.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d9813.html

Command list

In this lab exercise the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
aaa authentication	Defines authentication parameters.
aaa new-model	Enables AAA.
debug aaa authentication	Enables AAA authentication debugging.
enable	Enters privileged EXEC mode.
enable password *password*	Sets a local password to control access to various privilege levels.
enable secret *password*	Specifies an additional layer of security over the **enable password** command.
enable secret level *level password*	Sets a password for the privilege level.

Command	Description
privilege level *level*	Configures a new privilege level for users and associate commands with that privilege level. *level* - Privilege level associated with the specified line.
privilege *mode* {**level** *level* | **reset**} *command-string*	*mode* - Configuration mode for the specified command. **level** *level* - Specifies the privilege level configured for the specified command or commands. The level argument must be a number from 0 to 15. **reset -** Resets the privilege level of the specified command or commands to the default and removes the privilege level configuration from the running-config file. **Note** If the **no** form of this command is used to reset the privilege level to the default, the default form of this command will still appear in the configuration file. To completely remove a privilege configuration, use the **reset** keyword. *command-string* - Command associated with the specified privilege level. If the **all** keyword is used, specifies the command and subcommands associated with the privilege level.
service password-encryption	Encrypts all passwords in the configuration files.
show privilege	Displays the current level of privilege.
username *username* **password** *password*	Defines a local user and password combination.

Step 1 Secure and Test Access to Privileged EXEC, Line, VTY, AUX, and Console

Configure the current password protection by protecting access points into the router with passwords. Complete the following steps on the pod router:

a. Set the security of the privileged EXEC mode by configuring an enable secret password of **rouge7fox.**

b. Configure the VTY password of all VTYs to **echo9**.

c. Configure a console password of **front door**. Yes, there is a space in the password.

d. Look at the running configuration. Note that all passwords except “enable secret” are clear text. Use the **service password-encryption** command to correct this.

e. Show the running configuration again to ensure all passwords are now encrypted.

1. What happens to the passwords when the **no service password-encryption** command is used?

_____

_____

Answer: The passwords are displayed in plain text in the configuration.

Step 2 Configure the Local Database Authentication Using AAA

In this section, configure the local database authentication using AAA for the enable, line, and local methods.

Now that the NAS access points are protected, use the AAA commands to prepare for migration to a Cisco Secure Access Control Server (CSACS) environment. The goal of this task is to illustrate that each router access point can be secured using unique methods.

In this lab, there are two access points or lines to protect: VTY and console.

Complete the following steps to configure login authentication.

a. Turn on AAA features. Note that on command examples, spaces are added at times for readability only:

```
RouterP(config)# aaa new-model
```

b. Configure the login authentication to use the enable password using the default list:

```
RouterP(config)# aaa authentication login default enable
```

This protects all logins access instantly.

c. Test the model. Exit from the privilege mode and then exit from user mode. Then try to access the router on the console port. A password prompt will appear.

1. Which password will be valid, **front door** or **rouge7fox**? Why?

_____

_____

Answer: The students should use **rouge7fox**. This is the enable password.

d. Protect the console specifically. Enter the following commands so the IS group can access the console. Be aware that some passwords contain spaces.

```
RouterP(config)# username admin password back door
RouterP(config)# aaa authentication login console-in local
RouterP(config)# line con 0
RouterP(config-line)# login authentication console-in
```

e. Using the local database, students have just given the console a different login method from all the others. Cisco recommends never using **admin** as a username because it is too easy to guess.

f. Exit the configuration, enable, and user modes, and test the method.

g. Secure the VTY access for the IS personnel by using the following commands:

```
RouterP(config)# username isgroup password other door
RouterP(config)# aaa authentication login is-in local
RouterP(config)# line vty 0 4
RouterP(config-line)# login authentication is-in
```

h. This is the same idea as the console protection, but on the Telnet access via the vty ports. Test by telneting into the NAS from the student PC.
Do not use any of the Telnet icons on the desktop. They may mapped to a specific server. Use the Telnet applet from MS-DOS instead.

1. What is prompted for at the beginning of the Telnet session?

_____

Answer: Username and password.

Step 3 Test the Connection with Debug

In this task, use debug to look at the indicators for successful and unsuccessful authentication attempts. Before beginning this section, ensure that all Telnet sessions are disconnected, except for the console session. It is important in debugging to ensure the proper time is set to reference messages, especially if logging multiple devices to a central logging system.

Check the NAS clock by logging in to user mode and typing **show clock**. If the time and date are incorrect, enter the following command: **clock set HH:MM:SS DD month YYYY**. For example, **clock set 17:00:00 21 March 2005**.

To look at the indicators for successful and unsuccessful authentication attempts, complete the following steps:

a. Log in to privileged mode and use the following command to verify the correct timestamp information for the debug output. Enable console logging of debug messages:

```
RouterP(config)# service timestamps debug datetime msec

RouterP(config)# logging on

RouterP(config)# logging console debugging
```

b. Turn on debugging for AAA authentication:

```
RouterP# debug aaa authentication
```

c. Trigger an AAA authentication event by exiting the console connection and then logging in using **admin** and **back door** as the username and password.

d. After logging in and being presented the user mode prompt, continue with privileged mode. The debug information should be similar to the following:

```
Username:

Mar 21 17:05:00.461: AAA/AUTHEN/LOGIN (00000053): Pick method list
'console-in'

Username: admin

Password:

RouterP>enable

Password:

Mar 21 17:05:11.656: AAA: parse name=tty0 idb type=-1 tty=-1

Mar 21 17:05:11.656: AAA: name=tty0 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=0 channel=0

Mar 21 17:05:11.656: AAA/MEMORY: create_user (0x82B2138C)
user='admin' ruser='NU

LL' ds0=0 port='tty0' rem_addr='async' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0'

Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): port='tty0'
list='' action=LOGIN service=ENABLE

Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): console enable -
default to enable password (if any)

Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): Method=ENABLE

Mar 21 17:05:11.660: AAA/AUTHEN(3254755694): Status=GETPASS

RouterP#

Mar 21 17:05:18.671: AAA/AUTHEN/CONT (3254755694): continue_login
(user='(undef)')
```



```
Mar 21 17:05:18.671: AAA/AUTHEN(3254755694): Status=GETPASS

Mar 21 17:05:18.671: AAA/AUTHEN/CONT (3254755694): Method=ENABLE

Mar 21 17:05:18.755: AAA/AUTHEN(3254755694): Status=PASS

Mar 21 17:05:18.755: AAA/MEMORY: free_user (0x82B2138C) user='NULL'
ruser='NULL'

port='tty0' rem_addr='async' authen_type=ASCII service=ENABLE
priv=15

RouterP#
```

e. Log out of the router before continuing.

f. Log in to the router and enter an invalid enable password:

```
Username:

Mar 21 17:07:40.612: AAA/AUTHEN/LOGIN (00000054): Pick method list
'console-in'

Username: admin

Password:

RouterP>enable

Password:

Mar 21 17:07:52.103: AAA: parse name=tty0 idb type=-1 tty=-1

Mar 21 17:07:52.103: AAA: name=tty0 flags=0x11 type=4 shelf=0 slot=0
adapter=0 p ort=0 channel=0

Mar 21 17:07:52.107: AAA/MEMORY: create_user (0x82CE62E0)
user='admin' ruser='NULL' ds0=0 port='tty0' rem_addr='async'
authen_type=ASCII service=ENABLE priv=15 initial_task_id='0'

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): port='tty0'
list='' action=LOGIN service=ENABLE

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): console enable -
default to enable password (if any)

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): Method=ENABLE

Mar 21 17:07:52.107: AAA/AUTHEN(2358711356): Status=GETPASS

% Access denied

RouterP>

Mar 21 17:07:55.180: AAA/AUTHEN/CONT (2358711356): continue_login
(user='(undef)')

Mar 21 17:07:55.180: AAA/AUTHEN(2358711356): Status=GETPASS

Mar 21 17:07:55.180: AAA/AUTHEN/CONT (2358711356): Method=ENABLE

Mar 21 17:07:55.260: AAA/AUTHEN(2358711356): password incorrect

Mar 21 17:07:55.260: AAA/AUTHEN(2358711356): Status=FAIL

Mar 21 17:07:55.260: AAA/MEMORY: free_user (0x82CE62E0) user='NULL'
ruser='NULL'

port='tty0' rem_addr='async' authen_type=ASCII service=ENABLE
priv=15

RouterP>
```


Step 4 Telnet from the Student PC to the NAS

a. Telnet from the student PC to the NAS and enter a username and password. After a successful Telnet authentication, enter the privileged EXEC mode. The students should use the following passwords:

- Telnet username **isgroup**
- Telnet password **other door**
- Enable password **rouge7fox**

The **debug aaa authentication** and **debug aaa authorization** output should be similar to the output below:

```
RouterP#

Mar 21 17Mar 21 17:42:18.065: AAA/AUTHEN/LOGIN (00000011): Pick
method list 'is-in'

Mar 21 17Mar 21 17:42:25.890: AAA/AUTHOR (00000011): Method list
id=0 not configured. Sk ip author

Mar 21 17Mar 21 17:42:29.817: AAA: parse name=tty67 idb type=-1
tty=-1

Mar 21 17:42:29.817: AAA: name=tty67 flags=0x11 type=5 shelf=0
slot=0 adapter=0  port=67 channel=0

Mar 21 17:42:29.817: AAA/MEMORY: create_user (0x82D1B690)
user='isgroup' ruser=

'NULL' ds0=0 port='tty67' rem_addr='10.0.1.12' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0'

Mar 21 17:42:29.817: AAA/AUTHEN/START (3905120739): port='tty67'
list='' action=LOGIN service=ENABLE

Mar 21 17:42:29.821: AAA/AUTHEN/START (3905120739): non-console
enable - default to enable password

Mar 21 17:42:29.821: AAA/AUTHEN/START (3905120739): Method=ENABLE

Mar 21 17:42:29.821: AAA/AUTHEN(3905120739): Status=GETPASS

Mar 21 17:42:34.064: AAA/AUTHEN/CONT (3905120739): continue_login
(user='(undef)')

Mar 21 17:42:34.068: AAA/AUTHEN(3905120739): Status=GETPASS

Mar 21 17:42:34.068: AAA/AUTHEN/CONT (3905120739): Method=ENABLE

Mar 21 17:42:34.152: AAA/AUTHEN(3905120739): Status=PASS

Mar 21 17:42:34.152: AAA/MEMORY: free_user (0x82D1B690) user='NULL'
ruser='NULL

' port='tty67' rem_addr='10.0.1.12' authen_type=ASCII service=ENABLE
priv=15
```

b. Next, Telnet from the student PC to the pod router but enter a wrong enable password. The **debug aaa authentication** and **debug aaa authorization** output should be similar to the output below:

```
RouterP#

Mar 21 17:43:56.639: AAA/AUTHEN/LOGIN (00000012): Pick method list
'is-in'

Mar 21 17:44:05.129: AAA/AUTHOR (00000012): Method list id=0 not
configured. Sk ip author
```



```
Mar 21 17:44:08.090: AAA: parse name=tty67 idb type=-1 tty=-1

Mar 21 17:44:08.090: AAA: name=tty67 flags=0x11 type=5 shelf=0
slot=0 adapter=0  port=67 channel=0

Mar 21 17:44:08.090: AAA/MEMORY: create_user (0x82D1BE74)
user='isgroup' ruser=

'NULL' ds0=0 port='tty67' rem_addr='10.0.1.12' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0'

Mar 21 17:44:08.090: AAA/AUTHEN/START (3951678639): port='tty67'
list='' action=LOGIN service=ENABLE

Mar 21 17:44:08.094: AAA/AUTHEN/START (3951678639): non-console
enable - default to enable password

Mar 21 17:44:08.094: AAA/AUTHEN/START (3951678639): Method=ENABLE

Mar 21 17:44:08.094: AAA/AUTHEN(3951678639): Status=GETPASS

Mar 21 17:44:12.886: AAA/AUTHEN/CONT (3951678639): continue_login
(user='(undef)')

Mar 21 17:44:12.890: AAA/AUTHEN(3951678639): Status=GETPASS

Mar 21 17:44:12.890: AAA/AUTHEN/CONT (3951678639): Method=ENABLE

Mar 21 17:44:12.974: AAA/AUTHEN(3951678639): password incorrect

Mar 21 17:44:12.974: AAA/AUTHEN(3951678639): Status=FAIL

Mar 21 17:44:12.974: AAA/MEMORY: free_user (0x82D1BE74) user='NULL'
ruser='NULL

' port='tty67' rem_addr='10.0.1.12' authen_type=ASCII service=ENABLE
priv=15
```

1. What syntax indicates the authentication was unsuccessful?

_____

_____

Answer: Status=FAIL

Step 5 View a Sample Configuration for the NAS

At this point, the NAS configuration should look like the one shown in this task.

a. To view the configuration, log in to privileged mode and enter **`show running config`**:

```
version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Router1

!

boot-start-marker

boot system flash

boot-end-marker
```



```
!
enable secret 5 $1$0G/5$Q0NZw3aKe7IawIE/LpS9A1
enable password 7 0822455D0A16
!
aaa new-model
!
!
aaa authentication login default enable
aaa authentication login console-in local
aaa authentication login is-in local
!
aaa session-id common
!
resource policy
!
memory-size iomem 15
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.0.1.1 10.0.1.12
!
ip dhcp pool POD1_INSIDE
   network 10.0.1.0 255.255.255.0
   default-router 10.0.1.2
!
!
no ip ips deny-action ips-interface
no ip domain lookup
!
no ftp-server write-enable
!
!
!
username admin password 0 back door
username isgroup password 0 other door
```



```
!
!
!
!
!
interface FastEthernet0/0
 description inside
 ip address 10.0.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description outside
 ip address 172.30.1.2 255.255.255.0
 duplex auto
 speed auto
!
router eigrp 1
 network 10.0.0.0
 network 172.30.0.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
!
ip http server
ip http authentication local
no ip http secure-server
!
!
!
control-plane
!
!
!
!
line con 0
 password 7 08275E41070D45131D041E
 login authentication console-in
```



```
line aux 0
line vty 0 4
 privilege level 15
 password 7 0001100E0B02
 login authentication is-in
 transport input telnet
!
!
end
```


Lab 6.1.4 Configure Authentication Proxy

Objective

In this lab exercise, the students will complete the following tasks:

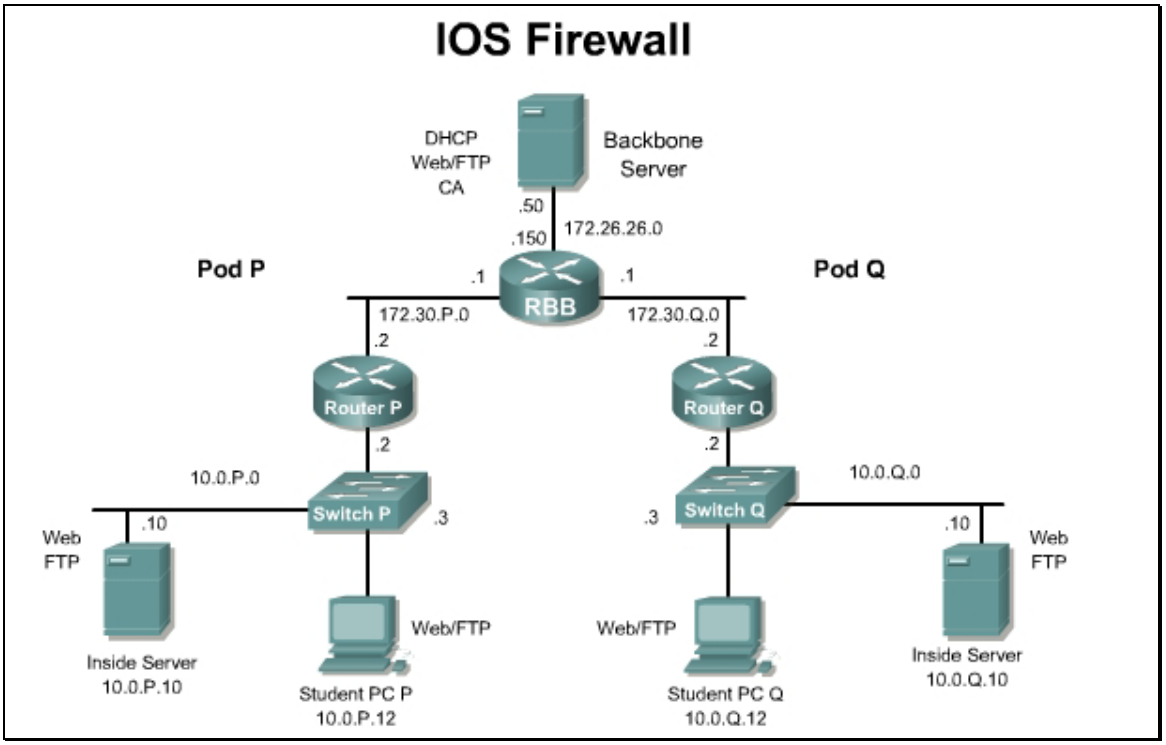
- Configure Cisco Secure Access Control Server (CSACS) for Windows 2000.
- Configure authentication, authorization, and accounting (AAA).
- Configure an authentication proxy.
- Test and verify an authentication proxy.

Scenario

A company wants to require users to authenticate internally before accessing external web and ftp resources on the Internet. The security policy has been updated accordingly. As an IT administrator, configure the perimeter router to act as an authentication proxy in order to meet the security policy requirements.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod routers. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

In preparation for this lab, CSACS should be configured with a user in the Default Group with a username of aaauser and aaapass as the password.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- Cisco Secure Access Control Server (CSACS) 3.3 or later for Windows 2000

Additional materials

Further information about the objectives covered in this lab can be found at the following websites:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d981d.html

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a008017cf42.html

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
aaa authentication	Defines AAA authentication parameters.
aaa authorization	Defines AAA authorization parameters.
aaa new-model	Enables AAA.
debug aaa authentication	Enables AAA authentication debugging.
ip auth-proxy	Defines authentication proxy rules.
ip http	Defines HTTP settings.
tacacs-server	Defines TACACS Server settings.

Step 1 Configure CS ACS for Windows 2000

a. On the workstation, open Cisco Secure ACS from the desktop.

b. Click **Interface Configuration** on the far left column of CSACS to go to the Interface Configuration window.

c. Click **TACACS+ (Cisco IOS)** to configure this option. Scroll down to the New Services frame.

d. Select the first line under New Services and enter **auth-proxy** under Services. Select the checkbox next to the field where **auth-proxy** has been entered. Make sure to check the check box directly to the left of the Service field.

e. Under **Advanced Configuration** Options, choose **Advanced TACACS+ Features** if it is not already selected.

f. Click **Submit** to submit the changes.

g. Click **Group Setup** to open the Group Setup window. Select **0: Default Group (1 user)** in the Group drop-down menu. Click the **Edit Settings** button to go to the Group Setup for this group.

h. Scroll down to the **auth-proxy** check box and the **Custom attributes** check box near the bottom of the Group Settings frame. Check both the **auth-proxy** check box and the **Custom attributes** check box.

i. Enter the following in the **Custom attributes** box.

```
proxyacl#1=permit tcp any any
priv-lvl=15
```

j. Click the **Submit + Restart** button to submit the changes and restart CSACS. Wait for the interface to return to the Group Setup main window.

1. Did CSACS restart successfully?

_____

Answer: Yes

Step 2 Configure AAA

To configure AAA, complete the following steps:

a. On the router, enter global configuration mode.

```
RouterP# configure terminal
```

b. Enable AAA.

```
RouterP(config)# aaa new-model
```

1. The **aaa ?** command provides what options?

_____

_____

_____

Answer: accounting, attribute, authentication, authorization, cache, configuration, dnis, group, local, max-sessions, nas, new-model, pod, route, session-id, session-mib, traceback, user

c. Specify the authentication protocol.

```
RouterP(config)# aaa authentication login default group tacacs+
```

d. Specify the authorization protocol.

```
RouterP(config)# aaa authorization auth-proxy default group tacacs+
```


e. Define the TACACS+ server and its key.

```
RouterP(config)# tacacs-server host 10.0.P.12
```

Note	If ACS is running on a computer other than the student PC, this IP address will be different.

(P=pod number.)

```
RouterP(config)# tacacs-server key secretkey
```

Step 3 Define the ACLs to Allow TACACS+ Traffic

a. Define the ACLs to allow TACACS+ traffic to the inside interface from the AAA server. Also allow outbound Internet Control Message Protocol (ICMP) traffic as well as FTP and WWW traffic. Block all other inside initiated traffic.

```
RouterP(config)# access-list 101 permit tcp host 10.0.P.12 eq tacacs
host 10.0.P.2
RouterP(config)# access-list 101 permit icmp any any
RouterP(config)# access-list 101 permit tcp 10.0.P.0 0.0.0.255 any
eq ftp
RouterP(config)# access-list 101 permit tcp 10.0.P.0 0.0.0.255 any
eq www
RouterP(config)# access-list 101 deny ip any any
```

(where P = pod number)

b. Define the ACLs to allow inbound ICMP traffic as well as FTP and WWW traffic to the inside web or FTP server. Block all other outside initiated traffic.

```
RouterP(config)# access-list 102 permit eigrp any any
RouterP(config)# access-list 102 permit icmp any any
RouterP(config)# access-list 102 permit tcp any host 10.0.P.10 eq
ftp
RouterP(config)# access-list 102 permit tcp any host 10.0.P.10 eq
www
RouterP(config)# access-list 102 deny ip any any
```

c. Enable the router HTTP server for AAA.

```
RouterP(config)# ip http server
RouterP(config)# ip http authentication aaa
```

1. What options are available with the **ip http ?** help command?

_____

_____

_____

_____

Answer: access-class, active-session-modules, authentication, client, max-connections, path, port, secure-active-session-modules, secure-ciphersuite, secure-client-auth, secure-port, secure-server, secure-trustpoint, trustpoint, server, session-module-list, timeout-policy

Step 4 Configure an Authentication Proxy

Complete the following steps to configure authentication proxy:

a. Define an authentication proxy rule.

```
RouterP(config)# ip auth-proxy name APRULE http auth-cache-time 5
```

1. What other protocols can use AAA as an authentication proxy?

   _____

   Answer: TACACS+, RADIUS

b. Apply the authentication proxy rule to the inside interface.

```
RouterP(config)# interface fastethernet 0/0
RouterP(config-if)# ip auth-proxy APRULE
RouterP(config-if)# ip access-group 101 in
RouterP(config-if)# exit
```

c. Apply the ACL to the outside interface.

```
RouterP(config-if)# interface fastethernet 0/1
RouterP(config-if)# ip access-group 102 in
```

Step 5 Test and Verify an Authentication Proxy

Complete the following steps to test and verify authentication proxy:

a. On the router, use the **show access-list** command to check the access lists. Fill in the blanks below using the output from this command.

```
RouterP# show access-list
```

1. Extended IP access list 101

   _____

   _____

   _____

   _____

   Answer:
   ```
   permit tcp host 10.0.P.12 eq tacacs host 10.0.P.2
   permit icmp any any
   permit tcp 10.0.P.0 0.0.0.255 any eq ftp
   permit tcp 10.0.P.0 0.0.0.255 any eq www
   deny ip any any
   ```

2. Extended IP access list 102

   _____

   _____

   _____

   _____

   Answer:
   ```
   permit eigrp any any
   permit icmp any any
   permit tcp any host 10.0.P.10 eq ftp
   ```



```
permit tcp any host 10.0.2.10 eq www
deny ip any any
```

b. Use the **show ip auth-proxy configuration** command to verify the authorization proxy configuration. Fill in the blanks below using the output from this command.

```
RouterP# show ip auth-proxy configuration
```

1. Authentication global cache time is _____ minutes
2. Auth-proxy name _____
3. http list not specified auth-cache-time_____ minutes

Answer:

```
RouterP# show ip auth-proxy configuration
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name APRULE
    http list not specified inactivity-timer 5 minutes
```

c. Use the **show ip auth-proxy cache** command to verify the authorization proxy configuration.

```
RouterP# show ip auth-proxy cache
```

1. Why is the cache empty?

_____

Answer: No user sessions have been created.

d. From the workstation command prompt, ping the backbone server.

```
C:\> ping 172.26.26.50
Pinging 172.26.26.50 with 32 bytes of data:
Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
Reply from 172.26.26.50: bytes=32 time=36ms TTL=125
```

e. Use the web browser to connect to the backbone web server.

f. In the URL field enter **http://172.26.26.50.**

g. Enter the following when the web browser prompts for a username and password.

```
Username: aaauser
Password: aaapass
```


h. Use the **show access-list** command to check the ACLs. Fill in the blanks below using the output from this command.

```
RouterP# show access-list
```

1. Extended IP access list 101

_____

_____

_____

_____

Answer: Answers will vary

2. Extended IP access list 102

_____

_____

_____

_____

_____

_____

Answer: Answers will vary

i. On the router, use the **show ip inspect all** command to see the CBAC parameters:

```
RouterP# show ip inspect all
```

_____

_____

_____

_____

_____

_____

Answer:

```
RouterP#sh ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500]
connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0
minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
```


j. Use the **show ip auth-proxy cache** command to verify the authorization proxy configuration. Fill in the blank below using the output from this command.

```
RouterP#show ip auth-proxy cache
```

_____

Answer:
```
RouterP#show ip auth-proxy cache
Authentication Proxy Cache
Client IP 10.0.2.12 Port 2448, timeout 5, state HTTP_ESTAB
```

Step 6 Test and Verify Authentication Proxy

Complete the following steps to test and verify authentication proxy a second time:

a. Use the web browser to connect to the backbone web server.

b. In the URL field enter **http://172.26.26.50**.

Note Use a "." at the end of the IP address to download a new copy of the web page. Otherwise, the browser may display a cached copy.

1. Was it necessary to authenticate again? Why?

_____

_____

_____

Answer: No. The session is still authenticated

c. Use the **clear ip auth-proxy cache *** command to clear the authorization proxy cache.

```
RouterP# clear ip auth-proxy cache *
```

1. Why is it necessary to clear the cache?

_____

_____

Answer: The session will be cached and the user will not be required to authenticate.

d. Use the **show ip auth-proxy cache** command to verify the cache has been cleared.

```
RouterP# show ip auth-proxy cache
```

1. Has the cache been cleared?

_____

Answer: Yes

Lab 6.3.9 Configure Local AAA on the PIX Security Appliance

Objective

In this lab exercise, the students will complete the following tasks:

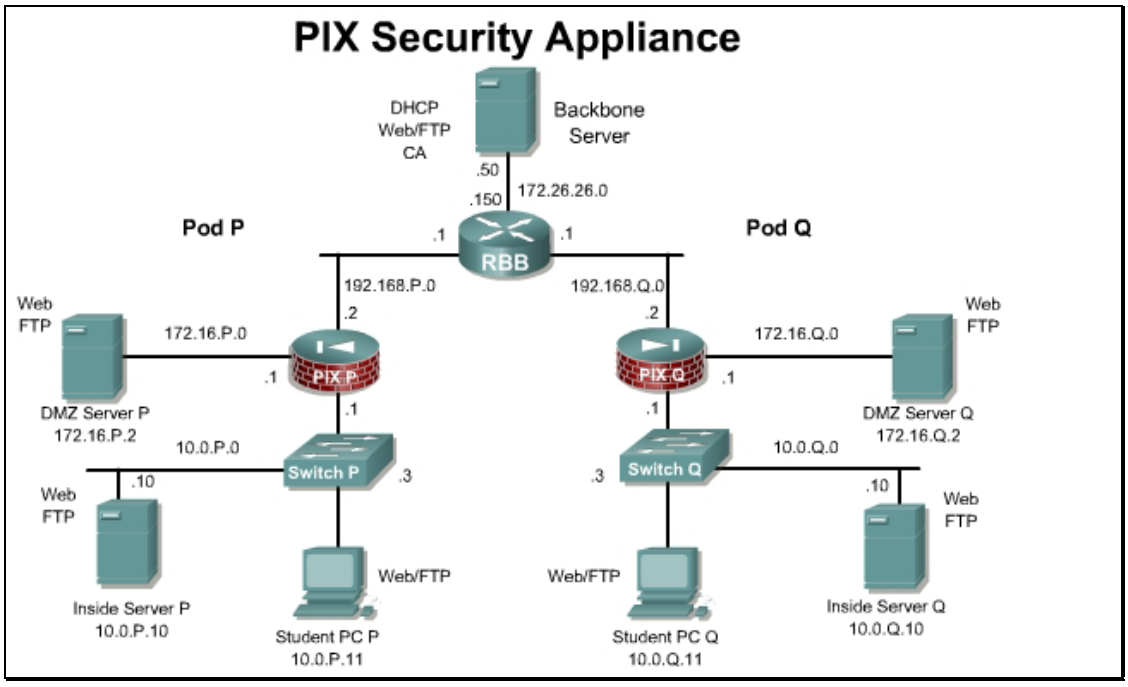
- Configure a local user.
- Configure and test inbound and outbound authentication.
- Configure and test telnet and http console access
- Configure and test Virtual Telnet authentication.
- Change and test authentication timeouts and prompts.

Scenario

A small company only has 10 users, but would like to implement stronger user authentication through the PIX Security Appliance. Currently, the budget cannot accommodate a AAA Server. Within the next year, the company plans to expand to 50 users and will need to implement server-based AAA with local AAA backup. Configure the Local AAA features on the PIX.

Topology

This figure illustrates the lab network environment:



Preparation

Begin with the standard lab topology and verify the starting configuration on pod PIX Security Appliance. Access the PIX Security Appliance console port using the terminal emulator on the Student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and Resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional Materials

Student can use the following links for more information on the objectives covered in this lab:

- http://www.cisco.com/go/pix

Command List:

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
aaa authentication secure-http-client	Enable encrypted authentication session.
aaa authentication { include | exclude } *authentication-service interface-name local-ip local-mask [foreign-ip foreign-mask] server-tag*	Configure AAA authentication
aaa authentication {serial | enable | telnet | ssh | http} console *server-tag* **[LOCAL]**	Configure AAA to authenticate serial, telnet, http, or ssh remote administration sessions
aaa { authentication | authorization | accounting } match *acl-name interface-name server-tag*	Bind an ACL to a AAA configuration.
auth-prompt [**accept** | **reject** | **prompt**] *string*	Change the AAA challenge text. (Configuration mode.)
clear configure aaa	Removes all AAA command statements from the configuration.
clear uauth	Removes an auth-prompt command statement from the configuration.
show running-config aaa	Displays the AAA authentication configuration.
show running-config auth-prompt	Displays authentication challenge, reject or acceptance prompt.

Command	Description
show uauth	Displays one or all currently authenticated users, the host IP to which they are bound, and, if applicable, any cached IP and port authorization information.
timeout [xlate | conn | udp | icmp | rpc | h225 | h323 | mgcp | mgcp-pat | sip | sip_media | uauth *hh*:*mm*:*ss*]	Sets the maximum idle time duration. This command is used in global configuration mode.
username {*name***} {nopassword | password** *password* **[encrypted]} [privilege** *priv_level***]}**	Configure a local username and password

Step 1 Add a User in the Local Database

Complete the following steps to configure local users

a. Configure a local user.

```
PixP(config)# username aaalocal password aaapass privilege 15
```

b. Verify the user:

```
PixP(config)# show running-config username
username aaalocal password VaA5TNJEpa8lcyOT encrypted privilege 15
```

Step 2 Enable the Use of Inbound Authentication

Complete the following steps to enable the use of inbound authentication on the PIX Security Appliance:

a. Configure the PIX Security Appliance to require authentication using the local user database for all inbound traffic:

```
PixP(config)# aaa authentication include any outside 0 0 0 0 LOCAL
Warning: The keyword 'any' will be converted to 'tcp/0' in config.
```

(Where P = pod number)

b. Verify the configuration:

```
PixP(config)# show running-config aaa
aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 LOCAL
```

c. Enable console logging of all messages:

```
PixP(config)# logging on
PixP(config)# logging console debug
```

Note If the web browser is open, close it. Choose **File > Close** from the web browser menu.

d. Test the configuration by initiating an HTTP session with the peer bastion host at 192.168.Q.11 or from an Internet PC located on the 172.26.26.0 network, test the configuration by initiating an HTTP session with the pod bastion host.

http://192.168.P.11

(where P = pod number)

e. When the web browser prompts, enter **aaalocal** for the username and **aaapass** for the password. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-609001: Built local-host outside:192.168.Q.10

%PIX-6-609001: Built local-host dmz:bastionhost

%PIX-6-302013: Built inbound TCP connection 1645 for
outside:192.168.2.10/4178 (

192.168.2.10/4178) to dmz:bastionhost/80 (192.168.P.11/80)

%PIX-6-109001: Auth start for user '???' from 192.168.Q.10/4178 to
bastionhost/80

%PIX-2-109011: Authen Session Start: user 'aaalocal', sid 1

%PIX-6-109005: Authentication succeeded for user 'aaalocal' from
192.168.2.10/4178 to bastionhost/80 on interface outside.
```

f. After a peer successfully authenticates to the PIX Security Appliance, display the PIX Security Appliance authentication statistics:

```
PixP(config)# show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'aaalocal' at 192.168.Q.10, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

1. What does the value in absolute timeout mean?

_____

_____

Answer: After 5 minutes, the user must reauthenticate when initiating a new connection. The absolute timer runs continuously, but waits to re-prompt the user when the user starts a new connection. The new connection can be started by doing something such as clicking a link after the absolute timer has elapsed. The user is then prompted to reauthenticate.

Step 3 Enable the Use of Outbound Authentication

Complete the following steps to enable the use of outbound authentication on the PIX Security Appliance:

a. Configure the PIX Security Appliance to require authentication for all outbound traffic:

```
PixP(config)# aaa authentication include any inside 10.0.P.0
255.255.255.0 0 0 LOCAL

Warning: The keyword 'any' will be converted to 'tcp/0' in config.

Verify the configuration:

PixP(config)# show runnig-config aaa

aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 LOCAL

aaa authentication include tcp/0 inside 10.0.1.0 255.255.255.0
0.0.0.0 0.0.0.0 LOCAL
```


b. Test HTTP outbound authentication from the Student PC. Ping RBB first to test connectivity.

```
C:\> ping 172.26.26.150
Pinging 172.26.26.150 with 32 bytes of data:
Reply from 172.26.26.150: bytes=32 time=1ms TTL=254
Reply from 172.26.26.150: bytes=32 time=1ms TTL=254
Reply from 172.26.26.150: bytes=32 time=1ms TTL=254
Reply from 172.26.26.150: bytes=32 time=1ms TTL=254
Ping statistics for 172.26.26.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

c. Open a web browser on the Student PC and connect to RBB. When the web browser prompts for HTTP Authentication, enter **aaalocal** for the username and **aaapass** for the password.

http://172.26.26.150

After the HTTP session is authenticated, a password is still required to access RBB. When prompted, leave the username blank and use '**cisco**' for the password.

1. Why did the ping work without authentication?

_____

Answer: The PIX is configured to require authentication for tcp traffic only. icmp traffic will not require authentication.

d. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-609001: Built local-host outside:172.26.26.150
%PIX-6-302013: Built outbound TCP connection 1699 for
outside:172.26.26.150/80 (172.26.26.150/80) to
inside:insidehost/4285 (192.168.1.10/4285)
%PIX-6-109001: Auth start for user '???' from insidehost/4285 to
172.26.26.150/80
%PIX-2-109011: Authen Session Start: user 'aaalocal', sid 3
```



```
%PIX-6-109005: Authentication succeeded for user 'aaalocal' from
insidehost/4285 to 172.26.26.150/80 on interface inside
```

e. Display authentication statistics on the PIX Security Appliance:

```
PixP(config)# show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'aaalocal' at insidehost, authenticated (idle for 0:00:05)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

f. Clear any existing uauth sessions.

```
PixP(config)# clear uauth
PixP(config)# show uauth
Current Most Seen
Authenticated Users     0     1
Authen In Progress      0     1
```

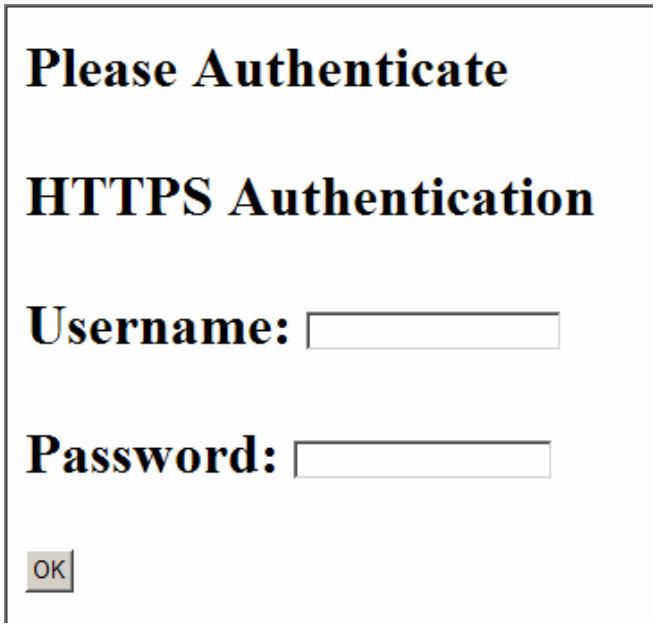
Note If the web browser is open, close it. Choose **File-Exit** from the web browser menu

g. This form of authentication passes the username and password in clear text. To increase security it is best to use an SSL encrypted session.

```
PixP(config)# aaa authentication secure-http-client
```

h. Open a web browser on the Student PC and connect to RBB. When the web browser prompts, enter **aaalocal** for the username and **aaapass** for the password

```
http://172.26.26.150
```



i. Accept the certificate.

j. The following will be displayed on the PIX.

```
%PIX-6-109001: Auth start for user '???' from insidehost/4315 to
172.26.26.150/443

%PIX-2-109011: Authen Session Start: user 'aaalocal', sid 5

%PIX-6-109005: Authentication succeeded for user 'aaalocal' from
insidehost/4315 to 172.26.26.150/443 on interface inside
```

After the HTTP session is authenticated, a password is still required to access RBB. When prompted, leave the username blank and use '**cisco**' for the password.

Step 4 Enable Authentication for CLI Access

Complete the following steps to enable authentication of Telnet and ASDM access to the PIX Security Appliance:

a. Configure the PIX Security Appliance to require authentication for Telnet and ASDM connections:

```
PixP(config)# aaa authentication telnet console LOCAL

PixP(config)# aaa authentication http console LOCAL
```

b. Verify the configuration:

```
PixP(config)# show running-config aaa

aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 LOCAL

aaa authentication include tcp/0 inside 10.0.P.0 255.255.255.0
0.0.0.0 0.0.0.0 LOCAL

aaa authentication telnet console LOCAL

aaa authentication http console LOCAL

aaa authentication secure-http-client
```

c. Configure the PIX Security Appliance to allow console Telnet logins from the inside host:

```
PixP(config)# telnet insidehost 255.255.255.255 inside
```

d. Verify the configuration:

```
PixP(config)# show running-config telnet

insidehost 255.255.255.255 inside
```

e. Clear any existing uauth sessions:

```
PixP(config)# clear uauth

PixP(config)# show uauth

Current Most Seen

Authenticated Users 0 2

Authen In Progress 0 1
```

g. Telnet to the PIX Security Appliance console:

```
C:\> telnet 10.0.P.1

Username: aaalocal

Password: aaapass

Type help or '?' for a list of available commands.

PixP>
```


(where P = pod number)

h. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1

%PIX-6-302013: Built inbound TCP connection 1847 for
   inside:insidehost/4346 (insidehost/4346) to NP Identity
   Ifc:10.0.P.1/23 (10.0.1.1/23)

%PIX-7-710001: TCP access requested from insidehost/4346 to
   inside:10.0.P.1/telnet

%PIX-7-710002: TCP access permitted from insidehost/4346 to
   inside:10.0.P.1/telnet

%PIX-6-611101: User authentication succeeded: Uname: aaalocal

%PIX-6-605005: Login permitted from insidehost/4346 to
   inside:10.0.P.1/telnet for user "aaalocal"
```

i. Close the Telnet session:

```
PixP>quit
```

(where P = pod number)

Step 5 Enable the Use of Authentication with Virtual Telnet

Complete the following steps to enable the use of authentication with virtual Telnet on the PIX Security Appliance:

a. Configure the PIX Security Appliance to accept authentication to a virtual Telnet service:

```
PixP(config)# virtual telnet 192.168.P.5
```

(where P = pod number)

b. Verify the virtual Telnet configuration:

```
PixP(config)# show running-config virtual
virtual telnet 192.168.P.5
```

(where P = pod number)

c. Clear any existing uauth sessions

```
PixP(config)# clear uauth
PixP(config)# show uauth
                    Current Most Seen
Authenticated Users     0     1
Authen In Progress      0     1
```

d. Telnet to the virtual Telnet IP address to authenticate from the Student PC:

```
C:\> telnet 192.168.P.5
LOGIN Authentication
Username: aaalocal
Password: aaapass
Authentication Successful
Connection to host lost.
```

(where P = pod number)

1. Why would a virtual Telnet IP address be created on the PIX Security Appliance?

Answer: The virtual Telnet option provides a way to authenticate users that require connections through the PIX Security Appliance using services or protocols that do not support authentication. The virtual Telnet IP address is used both to authenticate in and authenticate out of the PIX Security Appliance.

```
%PIX-6-609001: Built local-host outside:192.168.P.5

%PIX-6-302013: Built outbound TCP connection 1909 for
outside:192.168.P.5/23 (192.168.P.5/23) to inside:insidehost/4364
(192.168.P.10/4364)

%PIX-6-109001: Auth start for user '???' from insidehost/4364 to
192.168.P.5/23

%PIX-2-109011: Authen Session Start: user 'aaalocal', sid 7

%PIX-6-109005: Authentication succeeded for user 'aaalocal' from
insidehost/4364 to 192.168.P.5/23 on interface inside
```

Note: If the web browser is open, close it. Choose **File-Close** from the web browser menu.

e. Test the authentication. Open the web browser and enter the following in the URL field:

http://172.26.26.150

Since the user has already been authenticated using virtual telnet,there should be no authentication prompt for the HTTP session. Although the HTTP session is already authenticated, a password is still required to access RBB. When prompted, leave the username blank and use '**cisco**' for the password.

f. Clear the uauth timer:

```
PixP(config)# clear uauth

PixP(config)# show uauth

                Current Most Seen

Authenticated Users     0     1

Authen In Progress      0     1
```

Note	If the web browser is open, close it. Choose **File>Close** from the web browser menu.

g. Test that the user is no longer authenticated and that there is a need to re-authenticate. On the Student PC, open the web browser and enter the following in the URL field:

http://172.26.26.150

h. When prompted, enter **aaalocal** for the username and **aaapass** for the password.

1. Why is authentication needed this time?

Answer: The AAA authentication cache has been cleared with the **clear uauth** command.

Step 6 Change the Authentication Timeouts and Prompts

Complete the following steps to change the authentication timeouts and prompts:

a. View the current uauth timeout settings:

```
PixP(config)# show running-config timeout uauth
timeout uauth 0:05:00 absolute
```

b. Set the uauth absolute timeout to 3 hours:

```
PixP(config)# timeout uauth 3:00:00 absolute
```

c. Set the uauth inactivity timeout to 30 minutes:

```
PixP(config)# timeout uauth 0:30:00 inactivity
```

d. Verify the new uauth timeout settings:

```
PixP(config)# show runnig config timeout uauth
timeout uauth 3:00:00 absolute uauth 0:30:00 inactivity
```

e. View the current authentication prompt settings:

```
PixP(config)# show running-config auth-prompt
```

Nothing should be displayed.

f. Set the prompt that users get when authenticating:

```
PixP(config)# auth-prompt prompt Please Authenticate
```

g. Set the message that users get when successfully authenticating:

```
PixP(config)# auth-prompt accept You've been Authenticated
```

h. Set the message that users get when their authentication is rejected:

```
PixP(config)# auth-prompt reject Authentication Failed, Try Again
```

i. Verify the new prompt settings:

```
PixP(config)# show runnig-config auth-prompt
auth-prompt prompt Please Authenticate
auth-prompt accept You've been Authenticated
auth-prompt reject Authentication Failed, Try Again
```

j. Clear any existing uauth sessions:

```
PixP(config)# clear uauth
PixP(config)# show uauth
                  Current Most Seen
Authenticated Users     0     1
Authen In Progress      0     1
```

k. Initiate an HTTP connection to RBB to test the new authentication prompts.
From the Student PC, enter the following URL in a web browser:

http://172.26.26.150

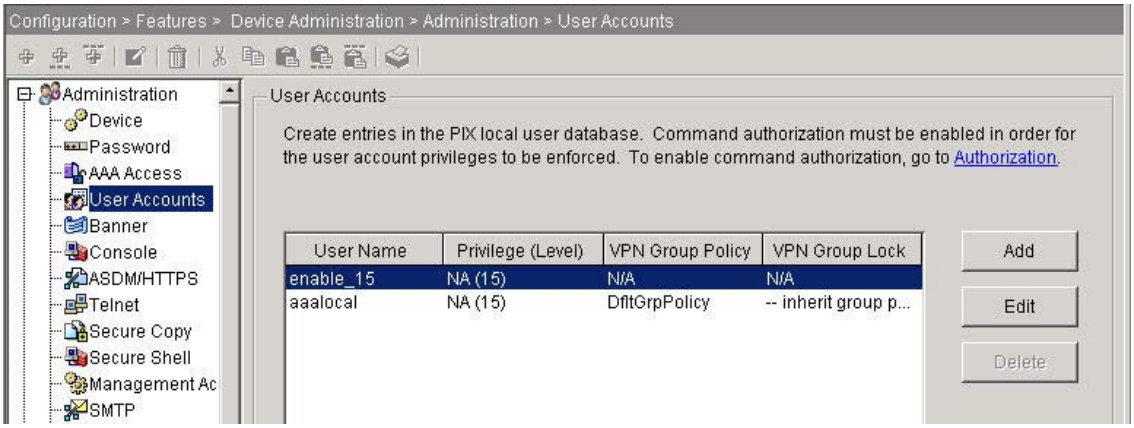
l. Verify the running configuration of the PIX Security Appliance against the ending configuration provided for this lab activity.

Step 7 Verify and Monitor Local AAA using ASDM

Complete the following steps to verify and monitor Local AAA using ASDM.

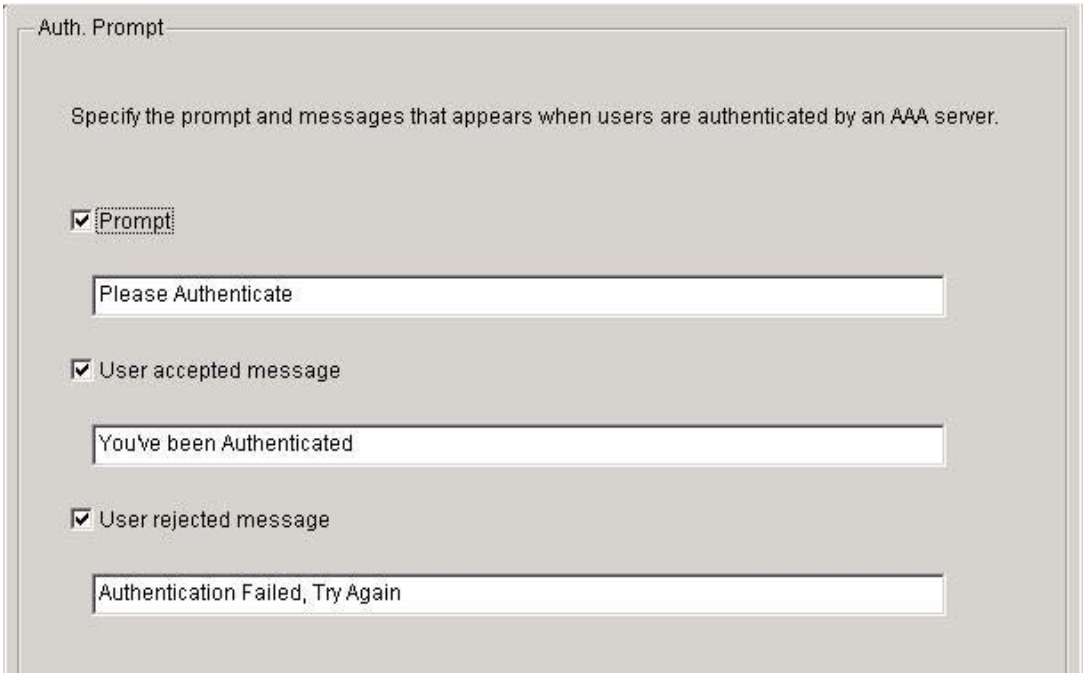
a. Log into ASDM using the **aaalocal** and **aaapass** credentials.

b. Navigate to **Configuration>Features>Device Administration>Administration>User Accounts**



c. Add a new user **aaalocal2/aaapass2** with a privilege level of **15**. Click **Apply**

Navigate to **Configuration>>Features>Properties> AAA Setup>Auth. Promt**. Notice the 3 authentication prompts that were configured previously

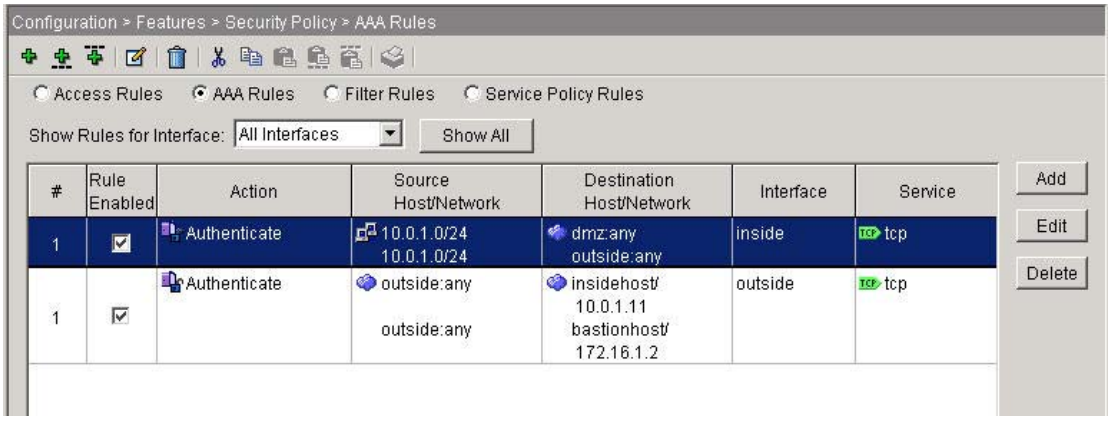


d. Edit these as desired. Click **Apply** when done.

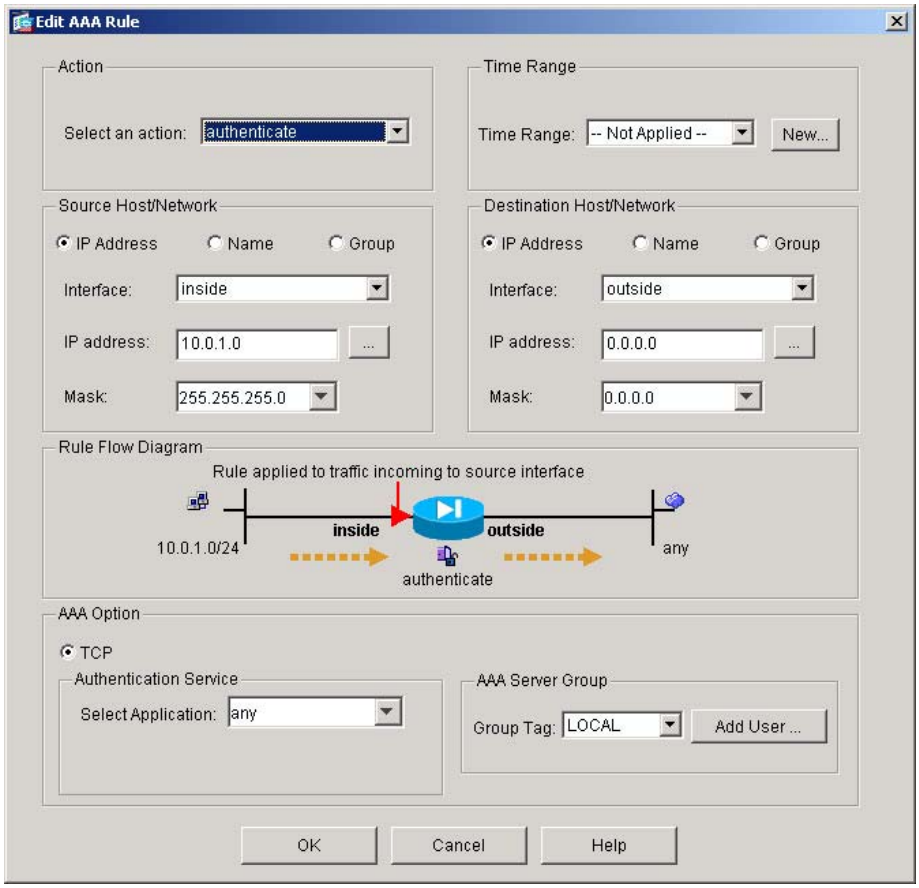
e. Navigate to **Configuration>Features>Security Policy**

f. Click on the **AAA Rules** radio button. Notice the 2 authentication rules that were configured previously.

g. Click on the **Show Detail** radio button to view more details about the AAA rules.



h. Double click on the top rule. The Edit Rule window will open.



i. Review the actions that are available in the drop down menu.

Change the Destination to the DMZ network of 172.16.P.0/24. Click **OK**.

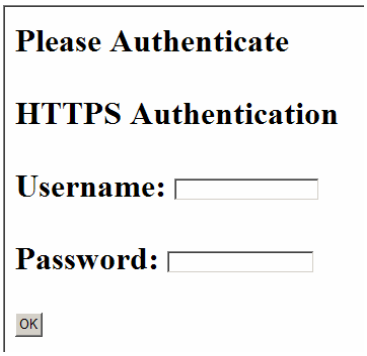
j. Click **Apply** to change the rule. Click the **Send** button if prompted.

k. If prompted with a warning that the keyword 'any' will be changed 'to tcp/'0' in the configuration, click the **OK** button to continue.

l. From the Menu, go to **Tools>Command Line Interface**

Clear any existing authentication by entering the **`clear uauth`** command. Click the **Send** Button. Click the **Close** button after the command is sent.

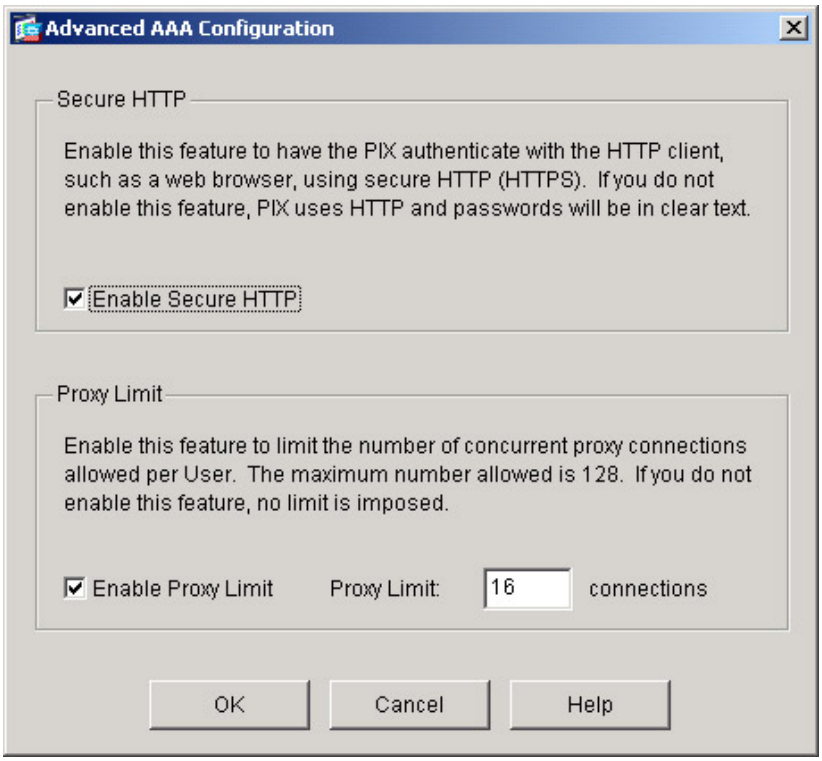
m. From the Student PC web browser, initiate an HTTP connection to the DMZ web server. A PIX authentication window will appear.



n. Authenticate to the PIX with the username **aaalocal2** and the password **aaapass2**.. The DMZ web page should appear.

o. Return to PDM. Navigate to **Monitoring Features >Administration > Authenticated users** to verify that the user is logged in.

p. Navigate to **Configuration > Features > Security Policy**. Click on the **AAA Rules** radio button. At the bottom of the Access Rule window, click on the **Advanced** button. This is where the Secure HTTP can be enabled or disabled.



q. Click on the **Cancel** button in the Advanced AAA Configuration window.

Lab 6.3.10 Configure AAA on the PIX Security Appliance Using Cisco Secure ACS for Windows 2000

Objective

In this lab exercise, the students will complete the following tasks:

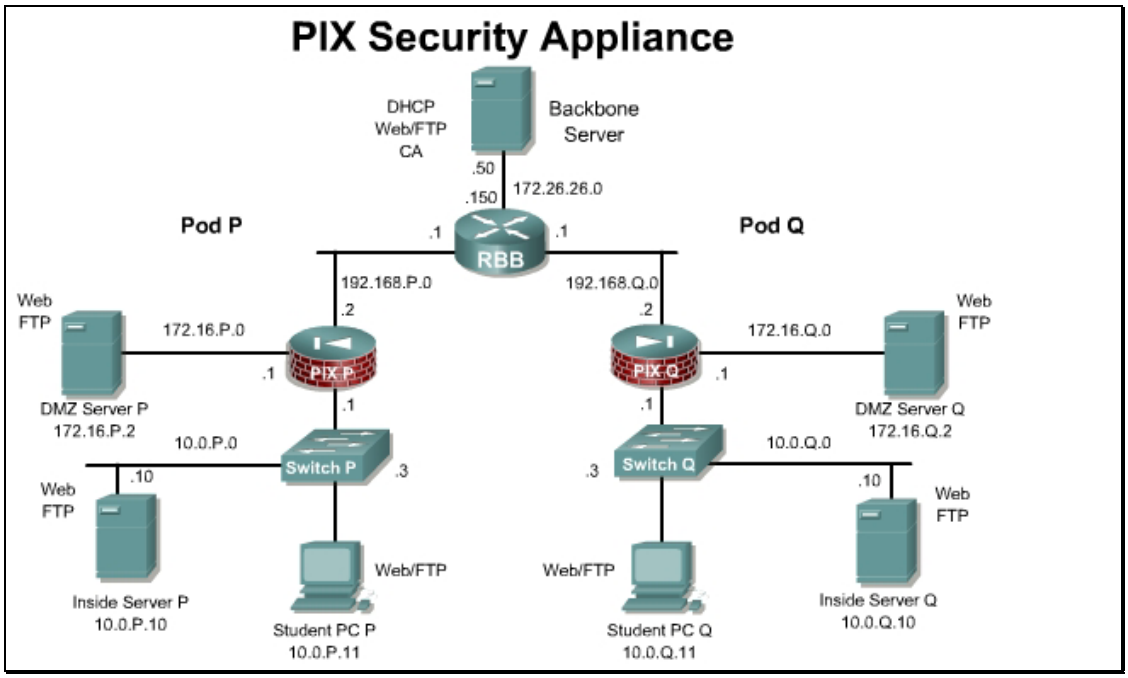
- Add a user to the Cisco Secure ACS database.
- Identify the AAA server and protocol.
- Configure and test inbound and outbound authentication.
- Configure and test console access and Virtual Telnet authentication.
- Change and test authentication timeouts and prompts.
- Configure and test authorization and accounting

Scenario

A small company has grown from 10 users to over 50. A Windows 2000 Server has just been installed and configured with Cisco Secure ACS software. All of the appropriate patches and updates have been completed. At this point, the PIX Security Appliance must be configured to use server based AAA.

Topology

This figure illustrates the lab network environment:



Preparation

Begin with the standard lab topology and verify the starting configuration on pod PIX Security Appliances. Access the PIX Security Appliance console port using the terminal emulator on the Student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

On the Backbone Server, ensure that FTP is configured with the following account:

User: **ftpuser** Password: **ftppass**

To download a trial version of ACS for educational purposes only go to http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-eval or contact the instructor for instructions. A CCO login is required to access this page.

Tools and Resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- Cisco Secure ACS version 3.3 or later.

Additional Materials

Student can use the following links for more information on the objectives covered in this lab:

http://www.cisco.com/go/acs

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
aaa authentication secure-http-client	Enable encrypted authentication session.
aaa authentication { include | exclude } *authentication-service interface-name local-ip local-mask [foreign-ip foreign-mask] server-tag*	Configure AAA authentication
aaa authorization { include | exclude } *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*	Configure AAA authorization
aaa accounting {include | exclude} *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*	Configure AAA accounting
aaa authentication {serial | enable | telnet | ssh | http} console *server-tag* **[LOCAL]**	Configure AAA to authenticate serial, telnet, http, or ssh remote administration sessions
aaa-server *server-tag* [(*interface-name*)] **host** *server-ip* [*key*] [**timeout** *seconds*]	Specify an AAA server. (Configuration mode.)

Command	Description
auth-prompt [**accept** | **reject** | **prompt**] *string*	Change the AAA challenge text. (Configuration mode.)
clear configure aaa	Removes aaa command statements from the configuration.
clear configure aaa-server	Removes aaa-server command statements from the configuration.
clear uauth	Removes an auth-prompt command statement from the configuration.
show running-config aaa	Displays the AAA authentication configuration.
show running-config aaa-server	Displays AAA server configuration.
show running config auth-prompt	Displays authentication challenge, reject or acceptance prompt.
show uauth	Displays one or all currently authenticated users, the host IP to which they are bound, and, if applicable, any cached IP and port authorization information.
timeout [xlate | conn | udp | icmp | rpc | h225 | h323 | mgcp | mgcp-pat | sip | sip_media | uauth *hh*:*mm*:*ss*]	Set the maximum idle time duration. (Configuration mode.)

Step 2 Verify the Users in the Cisco Secure ACS Database

Complete the following steps to verify users in the Cisco Secure ACS database:

a. Double click the ACS Admin icon on the desktop to launch the Cisco Secure ACS.

b. The Cisco Secure ACS interface should now be displayed in the web browser. Click **User Setup** to open the User Setup interface.

c. To view the list of current users, press **Find**. The User List will appear on the right hand side of the interface.

   1. Is there an entry for **aaauser**?

      _____

      Answer: Answers will vary.

d. If there is an entry for **aaauser**, proceed to Step 3. If there is no entry for **aaauser**, complete the remaining substeps to add a user in the Cisco Secure ACS database.

e. Add a user by entering **aaauser** in the user field.

f. Click **Add/Edit** to go into the user information edit window.

g. Give the user a password by entering **aaapass** in both the Password and Confirm Password fields.

h. Click **Submit** to add the new user to the Cisco Secure ACS database. Wait for the interface to return to the User Setup main window.

Step 3 Verify the Existing AAA Clients

Complete the following steps to verify the existing AAA clients:

a. The Cisco Secure ACS interface should be displayed in the web browser. Click **Network Configuration** to open the Network Configuration Setup interface. The Network Configuration Setup interface provides the ability to search, add, and delete AAA Clients, AAA Servers, and Proxy Distribution Tables.

b. Click the **(Not Assigned)** link to view the AAA Clients and Servers. The table at the top of the window displays all AAA Clients that have been configured.

1. Is there an AAA client entry for PixP?

_____

Answer: Answers will vary.

c. If there is an entry for PixP in the AAA Client table, proceed to Step 4. If there is no entry for PixP, continue to Step3d below to configure PixP as an AAA client.

d. To add PixP as an AAA client, click **Add Entry**. Enter the following information in the text boxes:

AAA Client Hostname: **PixP**

AAA Client IP Address: **10.0.P.1**

Key: **secretkey**

e. Verify the authentication is **TACACS+ (Cisco IOS)**. If any of check boxes are selected, uncheck them and press **Submit + Restart**.

After a few moments, the Network Configuration Setup interface will refresh.

1. Is the PixP AAA client displayed?

_____

Answer: Yes.

Step 4 Identify the AAA Server and the AAA Protocol on the PIX Security Appliance

Complete the following steps to identify the AAA server and the AAA protocol on the PIX Security Appliance:

a. Create a group tag called MYTACACS and assign the TACACS+ protocol to it:

```
PixP(config)# aaa-server MYTACACS protocol tacacs+
```

b. Return to configuration mode.

```
PixP(config-aaa-server-group)# exit
PixP(config)#
```

c. Define the AAA server:

```
PixP(config)# aaa-server MYTACACS (inside) host 10.0.P.11
```

Note If the Cisco Secure ACS is running on a computer other than the student PC, this IP address will be different.

d. Define the key used to authenticate to the AAA server:

```
PixP(config-aaa-server-host)# key secretkey
```

e. Return to configuration mode.

```
PixP(config-aaa-server-host)# exit
PixP(config)#
```


f. Verify the configuration:

```
PixP(config)# show running-config aaa-server
aaa-server MYTACACS protocol tacacs+
aaa-server MYTACACS host 10.0.P.11
key secretkey
```

Step 5 Enable the Use of Inbound Authentication

Complete the following steps to enable the use of inbound authentication on the PIX Security Appliance:

a. Configure the PIX Security Appliance to require authentication for all inbound traffic:

```
PixP(config)# aaa authentication include any outside 0 0 0 0
MYTACACS
Warning: The keyword 'any' will be converted to 'tcp/0' in config.
```

b. Verify the configuration:

```
PixP(config)# show running-config aaa
aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS
```

c. Enable console logging of all messages:

```
PixP(config)# logging on
PixP(config)# logging console debug
```

Note If the web browser is open, close it. Choose **File-Close** from the web browser menu.

d. Now test a peer pod inbound web authentication. Open the web browser, and initiate an HTTP connection with the DMZ web server of the peer pod:

http://192.168.Q.11

(where Q = peer pod number)

Or, from an internet PC, test your configuration.

http://192.168.P.11

(where P = pod number)

e. When the web browser prompts, enter **aaauser** for the username and **aaapass** for the password. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-302013: Built inbound TCP connection 277 for
outside:192.168.Q.10/3408 (192.168.Q.10/3408) to dmz:bastionhost/80
(192.168.1.11/80)
%PIX-6-109001: Auth start for user '???' from 192.168.Q.10/3408 to
bastionhost/80
%PIX-6-302014: Teardown TCP connection 277 for
outside:192.168.Q.10/3408 to dmz:bastionhost/80 duration 0:00:09
bytes 111 TCP FINs
%PIX-6-302013: Built inbound TCP connection 278 for
outside:192.168.2.10/3409 (192.168.Q.10/3409) to dmz:bastionhost/80
(192.168.P.11/80)
```



```
%PIX-6-109001: Auth start for user '???' from 192.168.Q.10/3409 to
bastionhost/80

%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1

%PIX-6-609001: Built local-host inside:10.0.P.10

%PIX-6-302013: Built outbound TCP connection 279 for
inside:10.0.P.10/49 (10.0.P.10/49) to NP Identity Ifc:10.0.P.1/1042
(10.0.P.1/1042)

%PIX-2-109011: Authen Session Start: user 'aaauser', sid 1

%PIX-6-109005: Authentication succeeded for user 'aaauser' from
192.168.Q.10/3409 to bastionhost/80 on interface outside
```

(where P = pod number, and Q = peer pod number)

If the authentication does not occur, the PIX Security Apliance will display an error message similar to the following example:

```
aaa server host machine not responding
```

If this happens, there could be a configuration problem in the ACS software. Make sure the ACS server is reachable using the ping command. Verify that the secret keys match.

f. After a peer successfully authenticates to the PIX Security Appliance, display the PIX Security Appliance authentication statistics:

```
PixP(config)# show uauth
                     Current Most Seen
Authenticated Users        1        1
Authen In Progress         0        1
user 'aaauser' at 192.168.Q.10, authenticated
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

(where Q = peer pod number)

1. What does the value in absolute timeout mean?

_____

_____

Answer: After 5 minutes, the user must reauthenticate when initiating a new connection. The absolute timer runs continuously, but waits to re-prompt the user when the user starts a new connection. The new connection can be started by doing something such as clicking a link after the absolute timer has elapsed. The user is then prompted to reauthenticate.

Step 6 Enable the Use of Outbound Authentication

Complete the following steps to enable the use of outbound authentication on the PIX Security Appliance:

a. Configure the PIX Security Appliance to require authentication for all outbound traffic:

```
PixP(config)# aaa authentication include any inside 0 0 0 0 MYTACACS
Warning: The keyword 'any' will be converted to 'tcp/0' in config.
```

b. Verify the configuration:

```
PixP(config)# show running-config aaa
```



```
aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS

aaa authentication include tcp/0 inside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS

Test HTTP outbound authentication from the Student PC.  Ping RBB
first.

C:\> ping 172.26.26.150

Pinging 172.26.26.150 with 32 bytes of data:

Reply from 172.26.26.150: bytes=32 time=1ms TTL=254

Reply from 172.26.26.150: bytes=32 time=1ms TTL=254

Reply from 172.26.26.150: bytes=32 time=1ms TTL=254

Reply from 172.26.26.150: bytes=32 time=1ms TTL=254

Ping statistics for 172.26.26.150:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

c. Open a web browser on the Student PC and connect to RBB. When the web browser prompts, enter **aaauser** for the username and **aaapass** for the password.

http://172.26.26.150

After the HTTP session is authenticated, a password is still required to access RBB. When prompted, leave the username blank and use '**cisco'** for the password.

1. Why did the ping work without authentication?

_____

Answer: The PIX is configured to require authentication for TCP traffic only. ICMP traffic will not require authentication.

d. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-109001: Auth start for user '???' from insidehost/3454 to
172.26.26.150/80

%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1
```



```
%PIX-6-609001: Built local-host inside:10.0.P.10

%PIX-6-302013: Built outbound TCP connection 315 for
inside:10.0.P.10/49 (10.0.P.10/49) to NP Identity Ifc:10.0.P.1/1043
(10.0.P.1/1043)

%PIX-2-109011: Authen Session Start: user 'aaauser', sid 2

%PIX-6-109005: Authentication succeeded for user 'aaauser' from
insidehost/3454to 172.26.26.150/80 on interface inside
```

(where P = pod number)

e. Display authentication statistics on the PIX Security Appliance:

```
PixP(config)# show uauth
                    Current Most Seen
Authenticated Users        2        2
Authen In Progress         0        1
user 'aaauser' at insidehost, authenticated
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
user 'aaauser' at 192.168.Q.10, authenticated
absolute timeout: 0:05:00
inactivit   y timeout: 0:00:00
```

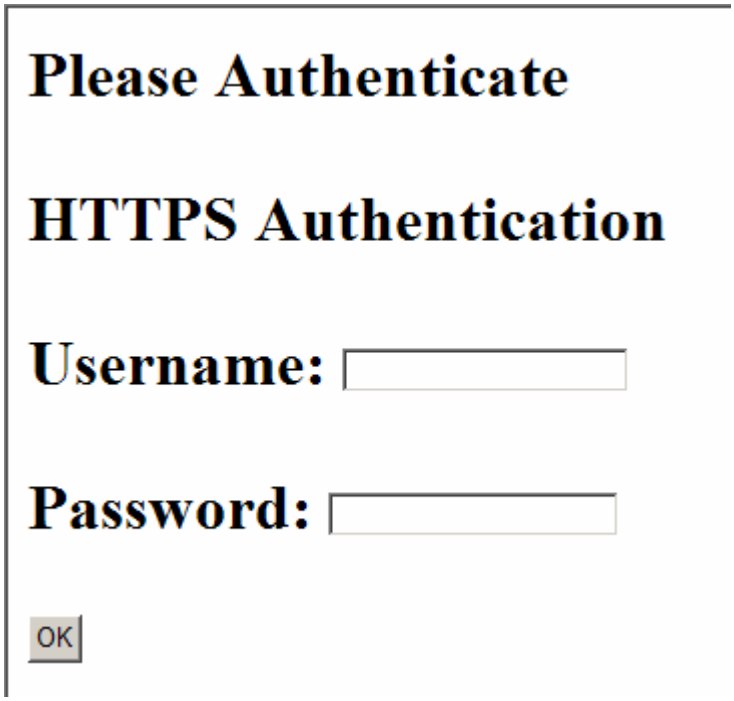
Note If the web browser is open, close it. Choose **File-Exit** from the web browser menu

f. By default the username and password are sent in clear text during HTTP authentication. To increase security it is best to use an SSL encrypted session. First, clear the authenticated sessions. Then configure the PIX Security Appliance to secure HTTP client authentication traffic using SSL.

```
PixP(config)# clear uauth
PixP(config)# aaa authentication secure-http-client
```

g. Open a web browser on the Student PC and connect to RBB. When the web browser prompts, enter **aaauser** for the username and **aaapass** for the password

http://172.26.26.150



h. Accept the certificate.

After the HTTP session is authenticated, a password is still required to access RBB. When prompted, leave the username blank and use '**cisco'** for the password.

Step 7 Enable Console Telnet Authentication

Complete the following steps to enable console Telnet authentication at the PIX Security Appliance:

a. Configure the PIX Security Appliance to require authentication for Telnet console connections:

```
PixP(config)# aaa authentication telnet console MYTACACS
```

b. Verify the configuration:

```
PixP(config)# show running-config aaa
aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS
aaa authentication include tcp/0 inside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS
aaa authentication telnet console MYTACACS
aaa authentication secure-http-client
```

c. Configure the PIX Security Appliance to allow console Telnet logins from the inside host:

```
PixP(config)# telnet insidehost 255.255.255.255 inside
```

d. Verify the configuration:

```
PixP(config)# show telnet
insidehost 255.255.255.255 inside
```

e. Clear the uauth sessions:

```
PixP(config)# clear uauth
PixP(config)# show uauth
Current Most Seen
```



```
Authenticated Users 0 2
Authen In Progress 0 1
```

g. Telnet to the PIX Security Appliance console:

```
C:\> telnet 10.0.P.1
Username: aaauser
Password: aaapass
Type help or '?' for a list of available commands.
PixP>
```

(where P = pod number)

h. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-605005: Login permitted from insidehost/3507 to
inside:10.0.1.1/telnet for user "aaauser"
```

i. Close the Telnet session:

```
PixP>quit
```

(where P = pod number)

Step 8 Enable the Use of Authentication with Virtual Telnet

Complete the following steps to enable the use of authentication with virtual Telnet on the PIX Security Appliance:

a. Configure the PIX Security Appliance to accept authentication to a virtual Telnet service:

```
PixP(config)# virtual telnet 192.168.P.5
```

(where P = pod number)

b. Verify the virtual Telnet configuration:

```
PixP(config)# show running-config virtual
virtual telnet 192.168.P.5
```

(where P = pod number)

c. Clear the uauth sessions:

```
PixP(config)# clear uauth
PixP(config)# show uauth
                    Current Most Seen
Authenticated Users     0     2
Authen In Progress      0     1
```

d. Telnet to the virtual Telnet IP address to authenticate from the Student PC:

```
C:\> telnet 192.168.P.5
LOGIN Authentication
Username: aaauser
Password: aaapass
Authentication Successful
Connection to host lost.
C:\>
```


(where P = pod number)

1. Why would a virtual Telnet IP address be created on the PIX Security Appliance?

_____

_____

Answer: The virtual Telnet option provides a way to authenticate users who require connections through the PIX Security Appliance using services or protocols that do not support authentication. The virtual Telnet IP address is used both to authenticate in and authenticate out of the PIX Security Appliance.

Note	If the web browser is open, close it. Choose **File-Close** from the web browser menu.

e. Test the authentication. Open the web browser and enter the following in the URL field:

http://172.26.26.150

There should be no authentication prompt.

f. Clear the uauth timer:

```
PixP(config)# clear uauth
PixP(config)# show uauth
                  Current Most Seen
Authenticated Users     0     2
Authen In Progress      0     1
```

Note: If the web browser is open, close it. Choose **File-Close** from the web browser menu.

g. Test that there is no authentication and need to re-authenticate. On the Student PC, open the web browser and enter the following in the URL field:

http://172.26.26.150

h. When prompted, enter **aaauser** for the username and **aaapass** for the password.

1. Why is authentication needed this time?

_____

_____

Answer: The AAA authorization cache has been cleared with the clear uauth command.

Step 9 Change the Authentication Timeouts and Prompts

Complete the following steps to change the authentication timeouts and prompts:

a. View the current uauth timeout settings:

```
PixP(config)# show running-config timeout uauth
timeout uauth 0:05:00 absolute
```

b. Set the uauth absolute timeout to 3 hours:

```
PixP(config)# timeout uauth 3:00:00 absolute
```

c. Set the uauth inactivity timeout to 30 minutes:

```
PixP(config)# timeout uauth 0:30:00 inactivity
```

d. Verify the new uauth timeout settings:

```
PixP(config)# show running-config timeout uauth
```



```
timeout uauth 3:00:00 absolute uauth 0:30:00 inactivity
```

e. View the current authentication prompt settings:

```
PixP(config)# show running-config auth-prompt
```

Nothing should be displayed.

f. Set the prompt that users get when authenticating:

```
PixP(config)# auth-prompt prompt Please Authenticate
```

g. Set the message that users get when successfully authenticating:

```
PixP(config)# auth-prompt accept You've been Authenticated
```

h. Set the message that users get when their authentication is rejected:

```
PixP(config)# auth-prompt reject Authentication Failed, Try Again
```

i. Verify the new prompt settings:

```
PixP(config)# show running-config auth-prompt
auth-prompt prompt Please Authenticate
auth-prompt accept You've been Authenticated
auth-prompt reject Authentication Failed, Try Again
```

j. Clear the uauth timer:

```
PixP(config)# clear uauth
PixP(config)# show uauth
                  Current Most Seen
Authenticated Users     0     2
Authen In Progress      0     1
```

k. Telnet to the Virtual Telnet IP address to test the new authentication prompts. From the Student PC, enter the following:

```
C:\> telnet 192.168.P.5
LOGIN Authentication
Please Authenticate
Username: wronguser
Password: Authentication Failed, Try Again
LOGIN Authentication
Please Authenticate
Username: aaauser
Password: aaapass
You've been Authenticated
Authentication Successful
```

(where P = pod number)

Step 10 Enable the Use of Authorization

Complete the following steps to enable the use of authorization on the PIX Security Appliance:

a. Configure the PIX Security Appliance to require authorization for all outbound FTP and HTTP traffic:

```
PixP(config)# aaa authorization include ftp inside 0 0 0 0 MYTACACS
PixP(config)# aaa authorization include http inside 0 0 0 0 MYTACACS
```

1. What are some of the benefits of implementing authorization? Drawbacks?

_____

_____

_____

Answer: Answers will vary. Benefits may include statements discussing increased security. Drawbacks may include statements concerning increased complexity for the user.

c. Verify the configuration:

```
PixP(config)# show running-config aaa
aaa aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS
aaa authentication include tcp/0 inside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS
aaa authentication telnet console MYTACACS
aaa authorization include ftp inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
MYTACACS
aaa authorization include http inside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS
aaa authentication secure-http-client
```

d. Test FTP authorization failure from the Student PC:

```
C:\> ftp 172.26.26.50
Connected to 172.26.26.50
220-FTP Server : (user 'aaaserver')
220
User (172.26.26.50:(none)): aaauser@ftpuser
331-Password:
331
Password: aaapass@ftppass
530
Login failed
```

e. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-109001: Auth start for user 'aaauser' from insidehost/3707 to
172.26.26.50/21
%PIX-6-302015: Built outbound UDP connection 1086 for
outside:171.70.157.213/1029 (171.70.157.213/1029) to
inside:insidehost/3708 (192.168.P.10/3708) (aaauser)
```



```
%PIX-6-302015: Built outbound UDP connection 1087 for
outside:171.68.222.151/1029 (171.68.222.151/1029) to
inside:insidehost/3708 (192.168.P.10/3708) (aaauser)

%PIX-6-302015: Built outbound UDP connection 1088 for
outside:171.68.10.142/1029 (171.68.10.142/1029) to
inside:insidehost/3708 (192.168.P.10/3708) (aaauser)

%PIX-6-302016: Teardown UDP connection 1069 for
outside:171.70.157.213/1029 to inside:insidehost/3703 duration
0:02:02 bytes 0 (aaauser)

%PIX-6-302016: Teardown UDP connection 1070 for
outside:171.68.222.151/1029 to inside:insidehost/3703 duration
0:02:02 bytes 0 (aaauser)

%PIX-6-302016: Teardown UDP connection 1071 for
outside:171.68.10.142/1029 to inside:insidehost/3703 duration
0:02:02 bytes 0 (aaauser)

%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1

%PIX-6-609001: Built local-host inside:10.0.P.10

%PIX-6-302013: Built outbound TCP connection 1090 for
inside:10.0.P.10/49 (10.0.P.10/49) to NP Identity Ifc:10.0.P.1/1049
(10.0.P.1/1049)

%PIX-6-109008: Authorization denied for user 'aaauser' from
insidehost/3707 to 1
```

(where P = pod number)

f. Test web authorization failure. Open the web browser and go to the following URL:

http://172.26.26.150

g. When prompted for a username and password, enter **aaauser** as the username and **aaapass** as the password:

```
User Name: aaauser

Password: aaapass
```

h. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-109001: Auth start for user 'aaauser' from insidehost/3748 to
172.26.26.150/80

%PIX-6-609001: Built local-host NP Identity Ifc:10.0.P.1

%PIX-6-609001: Built local-host inside:10.0.P.10

%PIX-6-302013: Built outbound TCP connection 1148 for
inside:10.0.P.10/49 (10.0.P.10/49) to NP Identity Ifc:10.0.P.1/1052
(10.0.P.1/1052)

%PIX-6-609001: Built local-host NP Identity Ifc:172.26.26.150

%PIX-6-106015: Deny TCP (no connection) from 172.26.26.150/80 to
insidehost/3748 flags RST ACK  on interface NP Identity Ifc

%PIX-6-609002: Teardown local-host NP Identity Ifc:172.26.26.150
duration 0:00:00

%PIX-6-109008: Authorization denied for user 'aaauser' from
insidehost/3748 to 172.26.26.150/80 on interface inside
```

(where P = pod number)

i. On Cisco ACS, click **Group Setup** to open the Group Setup interface.

j. Choose **0: Default Group (1 user)** from the Group drop-down menu.

k. Click **Users in Group** to display the users in the Default Group. The following information should be shown for the user:

- User: **aaauser**
- Status: **Enabled**
- Group: **Default Group (1 user)**

l. Click **Edit Settings** to go to the Group Settings interface for the group.

m. Scroll down in Group Settings until Shell Command Authorization Set is displayed, and select the **Per Group Command Authorization** button.

n. Select the **Permit** radio button.

n. Select the **Command** check box.

o. Enter **ftp** in the Command field.

p. Enter **permit 172.26.26.50** in the Arguments field.

q. Click **Submit + Restart** to save the changes and restart Cisco Secure ACS. Wait for the interface to return to the Group Setup main window.

r. Test FTP authorization success from the Windows 2000 server:

```
C:\> ftp 172.26.26.50
Connected to 172.26.26.50
220-FTP Server (user 'aaauser')
220
User (172.26.26.50:(none)): aaauser@ftpuser
331-Password:
331
Password: aaapass@ftppass
230-220 172.26.26.50 FTP server ready.
331-Password required for ftpuser
230-User ftpuser logged in.
230
ftp>
```

s. On the PIX Security Appliance console, the following should be displayed:

```
%PIX-6-109001: Auth start for user 'aaauser' from insidehost/3869 to
172.26.26.50/21
%PIX-6-609001: Built local-host NP Identity Ifc:10.0.1.1
%PIX-6-609001: Built local-host inside:10.0.1.10
%PIX-6-302013: Built outbound TCP connection 1502 for
inside:10.0.1.10/49 (10.0.1.10/49) to NP Identity Ifc:10.0.1.1/1102
(10.0.1.1/1102)
%PIX-6-109007: Authorization permitted for user 'aaauser' from
insidehost/3869 to 172.26.26.50/21 on interface inside
```

(where P = pod number)

Step 11 Enable the Use of Accounting

Complete the following steps to enable the use of accounting on the PIX Security Appliance:

a. Configure the PIX Security Appliance to perform accounting for all outbound traffic:

```
PixP(config)# aaa accounting include tcp/0 inside 0 0 0 0 MYTACACS
```

b. Verify the configuration:

```
PixP(config)# show running-config aaa accounting
aaa accounting include tcp/0 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
MYTACACS
aaa authentication secure-http-client
```

c. Clear the uauth sessions:

```
PixP(config)# clear uauth
PixP(config)# show uauth
                    Current Most Seen
Authenticated Users        0        2
Authen In Progress         0        1
```

d. Test FTP outbound accounting from the Student PC:

```
C:\> ftp 172.26.26.50
Connected to 172.26.26.50
220-Please Authenticate :
220
User (172.26.26.50:(none)): aaauser@ftpuser
331-Password:
331
Password: aaapass@ftppass
230-220 172.26.26.50 FTP server ready.
331-Password required for ftpuser
230-User ftpuser logged in.
230
ftp>
```

e. View the accounting records. On Cisco Secure ACS, click **Reports and Activity** to open the Reports and Activity interface.

f. Click the **TACACS+ Accounting** link.

g. Click the **TACACS+ Accounting active.csv** link to open the accounting records.

The following should be displayed:

Date	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	**	NAS Portname	NAS IP Address	cmd
5/24/2005	11:14:45	aaauser	Default Group	10.0.P.11	start	**	28	10.0.P.1	ftp

(where P = pod number)

h. Verify the PIX running configuration with the ending configuration.

j. Turn off logging on the PIX Security Appliance:

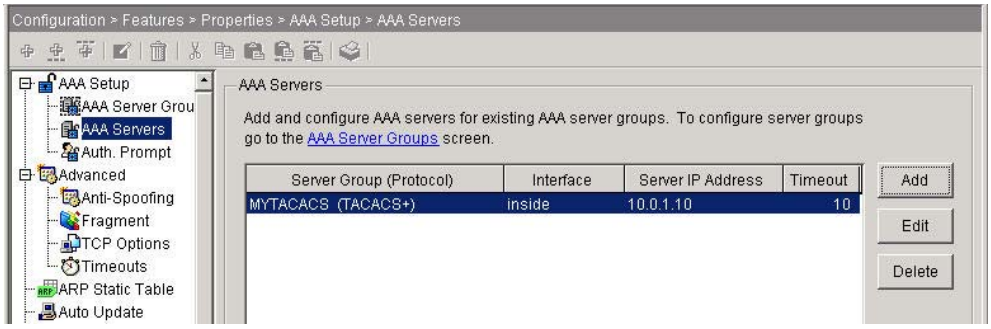
```
PixP(config)# no logging on
```

Step 7 Verify and Monitor Local AAA using ASDM

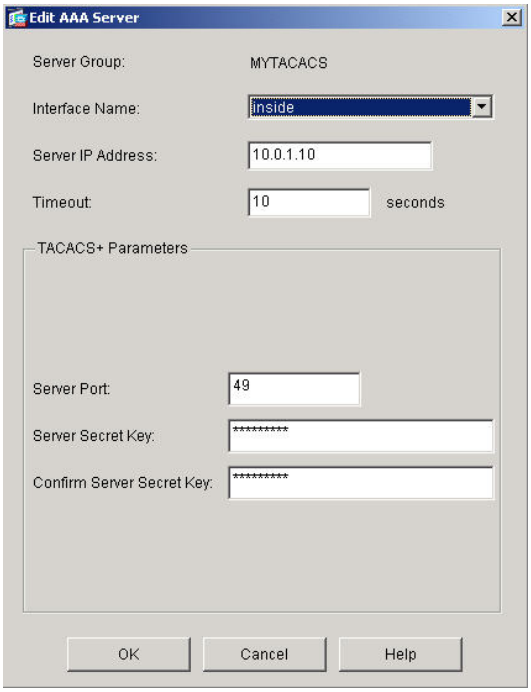
Complete the following steps to verify and monitor Local AAA using ASDM.

a. Log into ASDM.

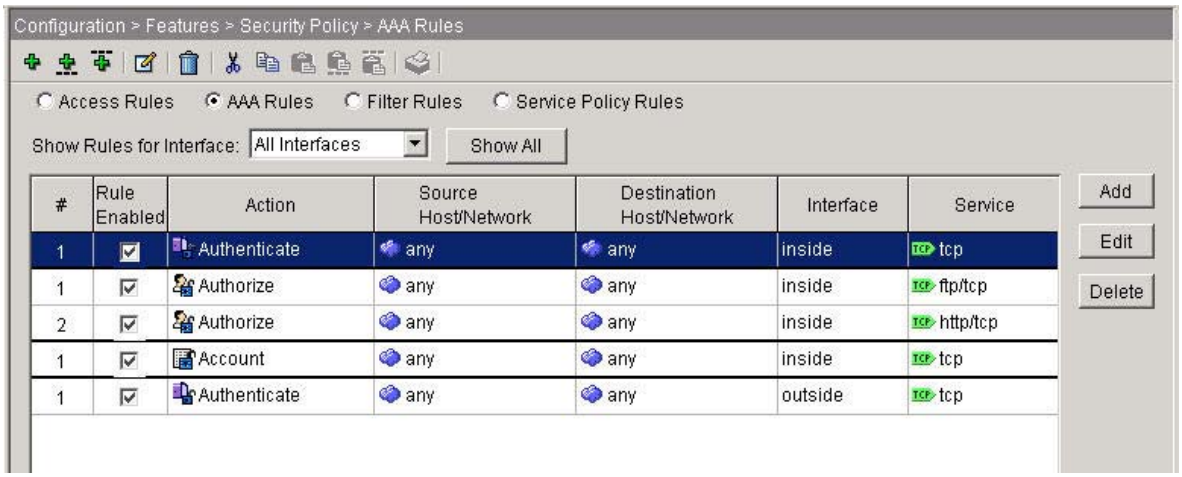
b. Navigate to **Configuration>Features> Properties>AAA Setup>AAA Servers**



c. Double click on the Server in the list to verify the AAA Server configuration. After reviewing the properties, click the **OK** button to close the window.



d. Navigate to **Configuration>Features>Security Policy>AAA Rules**.



e. Double click on any of the rules to edit.

Lab 7.1.9 Configure EAP on Cisco ACS for Windows

Objective

In this lab, the students will complete the following tasks:

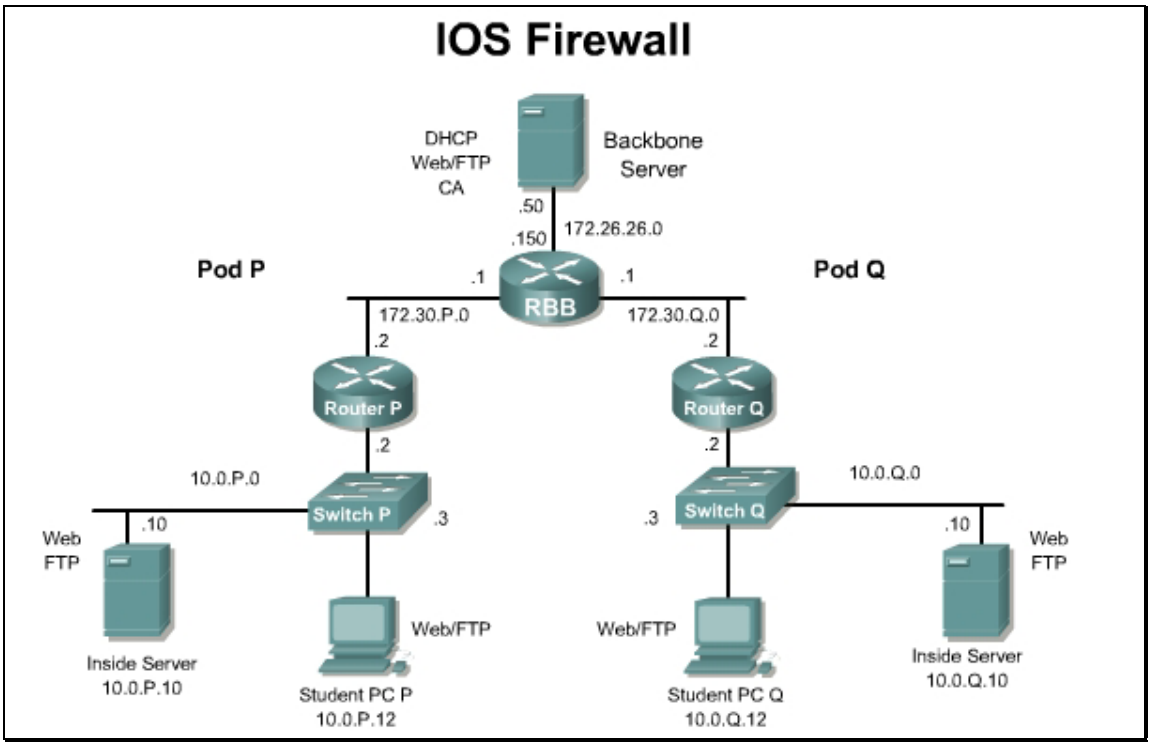
- Obtain a certificate for the ACS server.
- Configure ACS to use a certificate from storage.
- Specify additional certificate authorities that the ACS should trust.
- Restart the service and configure EAP settings on the ACS.
- Specify and configure the access point as an AAA client.
- Configure the external user databases.
- Restart the service.

Scenario

The XYZ company would like to implement 802.1x authentication on the corporate network. Before the 2950 switches can be configured to support 802.1x authentication of network clients, a RADIUS authentication server must be put in place. In this activity, students will configure Extensible Authentication Protocol (EAP) with Cisco Secure ACS for Windows so that it can be used as an authentication server in the 802.1x implementation.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod switch. Access the pod switch console port using the terminal emulator on the Windows 2000 server. If desired, save the switch configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

A server certificate must be available for the Cisco Secure ACS before you can install it. With Cisco Secure ACS, certificate files must be in Base64-encoded X.509. If a server certificate is not already in storage, the procedure in Step 1 can be used to create a certificate for installation. The Cisco Secure ACS can be used to generate a self-signed digital certificate to be used for PEAP authentication protocol or for HTTPS support of Cisco Secure ACS administration. This capability supports TLS/SSL protocols and technologies without the requirement of interacting with a CA.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

Step 1 Generate a Self-signed Certificate

a. Create a directory for use with certificate.

```
c:>md c:\acs_server_cert
```

b. In the navigation bar, click **System Configuration**.

c. Click **ACS Certificate Setup**.

d. Click **Generate Self-Signed Certificate**.

e. type in **cn=securacs** in **Certificate Subject**

f. type in **c:\acs_server_cert\acs_server_cert.cer** in **Certificate File**

g. type in **c:\acs_server_cert\acs_server_cert.pvk"** in **Private Key File**

h. type in **secur** for the private key password.

i. In the Retype private key password box, retype the private key password.

j. In the Key length box, select the default key length of **2048 bits**.

k. In the Digest to sign with box, select the **SHA1** hash digest to be used to encrypt the key.

l. To install the self-signed certificate when you submit the page, select the **Install generated certificate** option.

Note	If the Install generated certificate option is used, the Cisco Secure ACS services must be restarted after submitting this form to adopt the new settings.

Note	If the Install generated certificate option is not selected, the certificate file and private key file are generated and saved when Submit is clicked in the next step, but they are not installed into the local machine storage.

m. Click **Submit**. The specified certificate and private key files are generated and stored, as specified. The certificate becomes operational, if the Install generated certificate option was selected, only after the Cisco Secure ACS is restarted.

n. To restart the Cisco Secure ACS services, Click on **System Configuration** then **Service Control**, and then click on the **Restart** button.

Step 2 Configure EAP Settings

In this step, select and configure how Cisco Secure ACS handles options for authentication. In particular, use this procedure to specify and configure the varieties of EAP that are allowed, and to specify whether to allow either MS-CHAP Version 1 or MS-CHAP Version 2, or both.

a. In the navigation bar, click **System Configuration**.

b. Click **Global Authentication Setup**.

c. Make sure **Allow EAP-MD5** is checked.

d. Click **Submit**.

Note	To save any changes to the settings that have been made but are to be implemented later, click **Submit**. The Cisco Secure ACS services can be restarted at any time by using the Service Control page in the System Configuration section.

Step 3 Specify the Switch as a AAA Client

a. Click on Network Configuration button.

b. Click on **(Not Assigned)** under Device Groups.

c. Click on **Add Entry** in the AAA client window**.**

d. Input the following:

   i. IP address of the pod switch, **10.0.P.3**

      (Where P = pod number)

   ii. key = **secretkey**

   iii. authenticate using **RADIUS (IETF)**

e. Click **Submit.** The hostname now appears in the AAA Clients window.

Step 4 Restart the Cisco Secure ACS Service

a. Click on **System Configuration** then **Service Control**.

b. Click on **Restart**.

Lab 7.2.8 Configure 802.1x Port-Based Authentication

Objective

In this lab, the students will complete the following tasks:

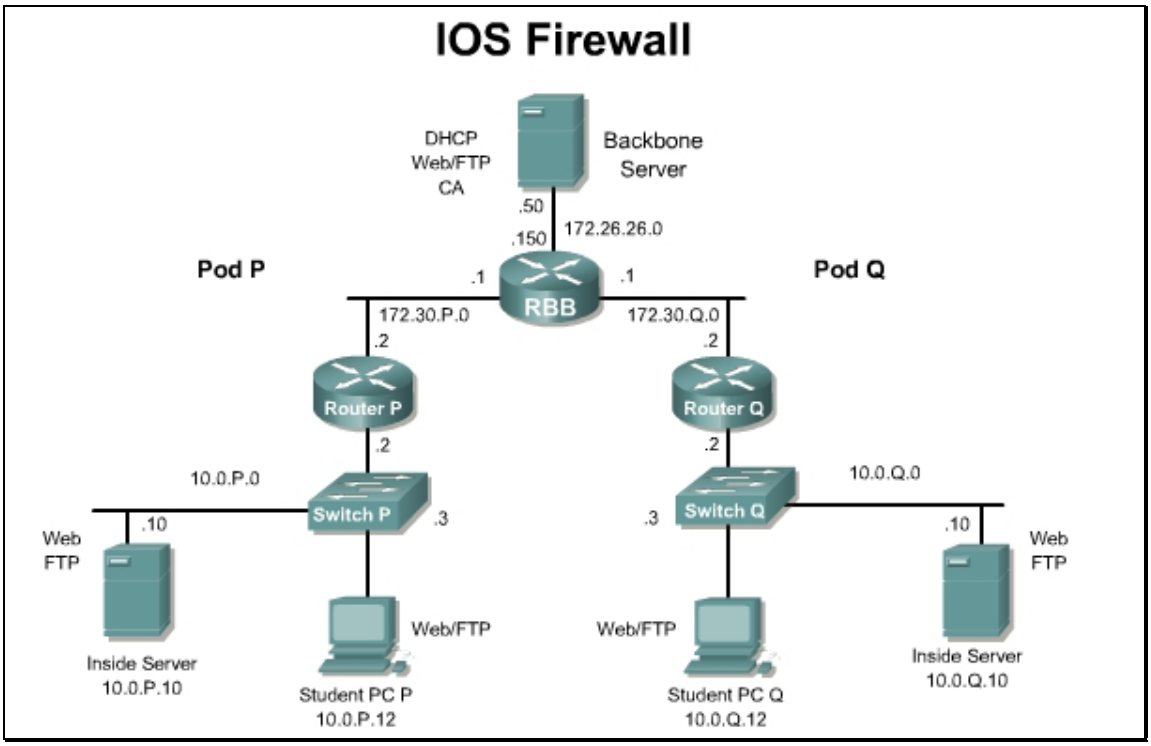
- Enable 802.1x authentication.
- Configure the switch-to-RADIUS server communication.
- Enable periodic re-authentication.
- Manually re-authenticate a client connected to a port.
- Change the quiet period.
- Change the switch-to-client retransmission time.
- Set the switch-to-client frame-retransmission number.
- Enable multiple hosts.
- Reset the 802.1x configuration to the default values.
- Display 802.1x statistics and status.

Scenario

Now that the Cisco Secure ACS has been configured with the parameters that enable it to perform as an 802.1x authentication server, the XYZ company network is ready for 802.1x switch configuration. The PCs that are permitted to be on the network will also need to be configured to act as 802.1x clients. In this activity, students will configure 802.1x port-based authentication on a Catalyst 2950 switch.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod switch. Access the pod switch console port using the terminal emulator on the Windows 2000 server. If desired, save the switch configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- A second PC to be used as an 802.1x client

Additional materials

Further information about the objectives covered in this lab can be found at,
http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00800d84b9.html

http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp

Command List

In this lab exercise, the following switch commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

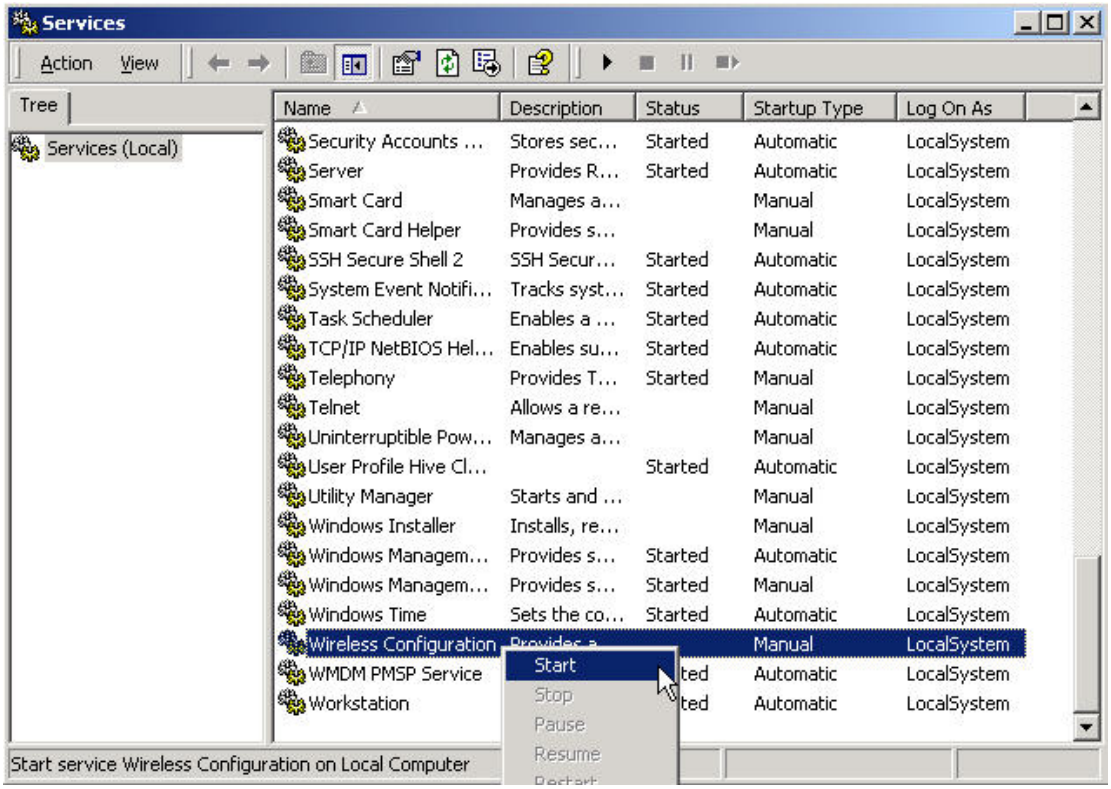
Switch Commands

Command	Description
aaa authentication dot1x ***{*****default	listname*****}*** *method1* ***[****method2...****]***	To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command
aaa new-model	To enable the AAA access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.
dot1x default	To reset the global 802.1x parameters to their default values, use the **dot1x default** command in global configuration mode.
dot1x max-req *number-of-retries*	To set the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the **dot1x max-req** command in interface configuration or global configuration mode. To disable the number of times that were set, use the **no** form of this command.
dot1x multiple-hosts	To allow multiple hosts (clients) on an 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**, use the **dot1x multiple-hosts** command in interface configuration mode. To return to the default setting, use the **no** form of this command.
**dot1x port-control {auto	force-authorized	force-unauthorized}**	To set an 802.1x port control value, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.
dot1x re-authenticate *interface-type interface-number*	To enable periodic reauthentication of the client PCs on the 802.1x interface, use the **dot1x reauthentication** command in interface configuration mode. To disable periodic reauthentication, use the **no** form of this command.
dot1x timeout {auth-period *seconds* **| held-period** *seconds* **| quiet-period** *seconds* **| ratelimit-period** *seconds* **| reauth-period** *seconds* **| server-timeout** *seconds* **| start-period** *seconds* **| tx-period** *seconds***}**	To set retry timeouts, use the **dot1x timeout** command in interface configuration mode. To remove the retry timeouts, use the **no** form of this command.
radius-server host {*hostname* **|** *ip-address***} [auth-port** *port-number***] [acct-port** *port-number***] [timeout** *seconds***] [retransmit** *retries***] [key** ***string*****] [alias{***hostname* **|** *ip-address***}]**	To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.
show dot1x [interface *interface-name* **[details]]**	To show details for an identity profile, use the **show dot1x** command in privileged EXEC mode.
show dot1x [interface *interface-name* **[details]]**	To show details for an identity profile, use the **show dot1x** command in privileged EXEC mode.

Step 1 Prepare a PC for 802.1x Authentication

a. This lab requires an additional PC that must be capable of using 802.1x authentication. If the PC already has this capability, proceed to substep d.

b. To enable the 802.1x client choose **Start > Settings > Control Panel > Administrative Tools >Services**. Right click on the **Wireless Configuration** icon and select **Start** from the menu.

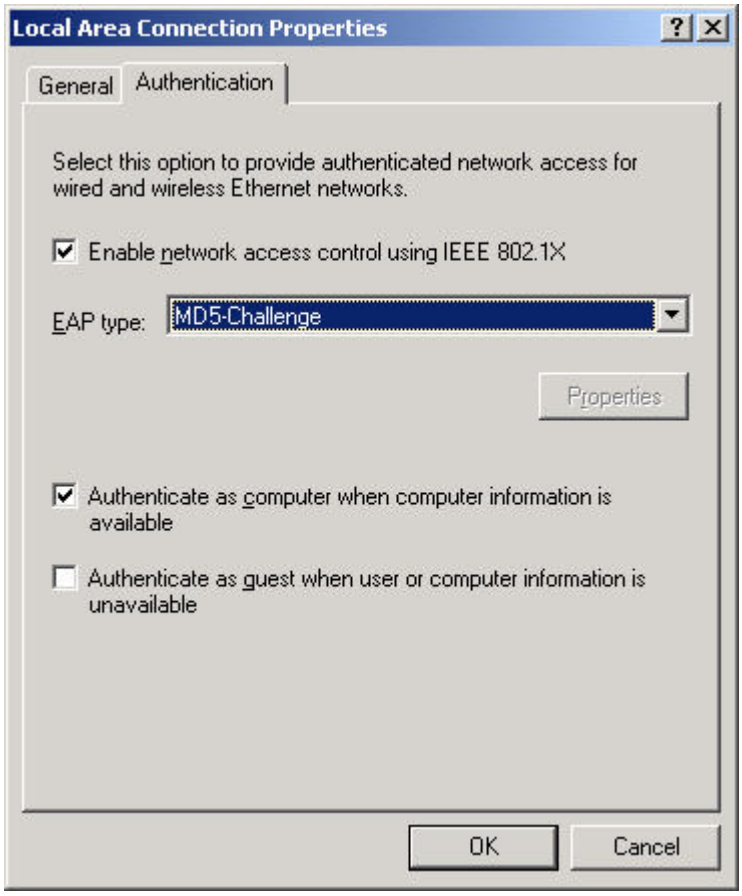


c. If necessary, an 802.1x client for Microsoft Windows can be downloaded from the following URL:

http://support.microsoft.com/default.aspx?scid=kb;en-us;313664

d. On the PC, under the **Authentication** tab of **Local Area Network Connection Properties** check the following:

- Enable network access control using IEEE 802.1X box is checked.
- EAP type = MD5-Challenge



Step 2 Enable 802.1x Authentication on the Switch

a. Enable AAA on the pod switch.

```
SwitchP(config)# aaa new-model
```

Create an 802.1x authentication method list. To create a default list that is used when a named list is not specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. The **group radius** keyword is used to indicate the list of all RADIUS servers that is configured on the switch will be used for authentication.

```
SwitchP(config)# aaa authentication dot1x default group radius local
```

b. Configure AAA accounting.

```
SwitchP(config)# aaa accounting network default start-stop group
radius

SwitchP(config)# aaa accounting connection default start-stop group
radius
```

c. Enable dot1x system-auth-control.

```
SwitchP(config)# dot1x system-auth-control
```

d. Enter interface configuration mode, and specify the interface to be enabled for 802.1x authentication.

```
SwitchP(config)# interface fa0/12
```


e. Enable 802.1x authentication on the interface.

```
SwitchP(config-if)# dot1x port-control auto
```

f. Return to privileged EXEC mode.

```
Switch(config-if)# end
```

g. Verify the entries. Check the Status column in the 802.1x Port Summary section of the display. An `enabled` status means the port-control value is set either to **`auto`** or to **`force-unauthorized`**.

```
SwitchP# show dot1x
Sysauthcontrol                  = Enabled
Supplicant Allowed In Guest Vlan  = Disabled
Dot1x Protocol Version          = 1
Dot1x Oper Controlled Directions  = Both
Dot1x Admin Controlled Directions = Both
```

1. What command enables system-authorization?

_____

Answer: `dot1x system-auth-control`

Step 3 Configure the Switch-to-RADIUS Server Communication

a. Configure the RADIUS server parameters on the switch.

```
SwitchP(config)# radius-server host 10.0.P.12 auth-port 1812 key
secretkey
```

Note	If CSACS is not installed on the student PC, use the host address of the PC where CSACS is installed.

Note	Port 1812 is the default UDP destination port for RADIUS authentication requests.

b. Return to privileged EXEC mode.

```
SwitchP(config)# end
```

c. Verify the entries in the configuration.

```
SwitchP# show running-config
```

The following lines should appear in the configuration:

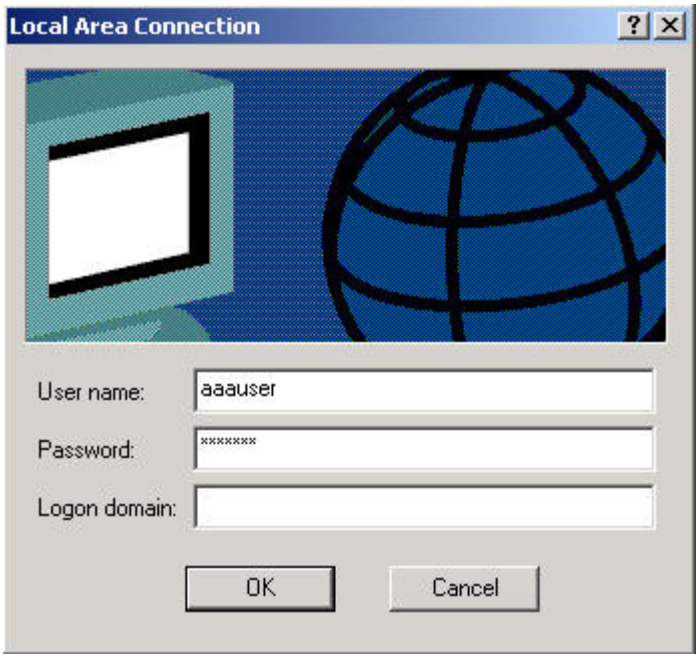
```
!
radius-server host 10.0.2.12 auth-port 1812 acct-port 1813 key
secretkey
radius-server retransmit 3
!
```


d. View the current status of the port that has been configured for 802.1x authentication with the **`show dot1x all`** command.

```
Dot1x Info for interface FastEthernet0/12
--------------------------------------------------
Supplicant MAC <Not Applicable>
   AuthSM State      = CONNECTING
   BendSM State      = IDLE
PortStatus         = UNAUTHORIZED
MaxReq             = 3
HostMode           = Multi
Port Control       = Auto
QuietPeriod        = 90 Seconds
Re-authentication  = Enabled
ReAuthPeriod       = 4000 Seconds
ServerTimeout      = 30 Seconds
SuppTimeout        = 30 Seconds
TxPeriod           = 45 Seconds
Guest-Vlan         = 0
```

e. Connect the second PC to port FastEthernet 12 on the pod switch.

f. When prompted for authentication, enter the username **aaauser** and the password **aaapass**. Leave the Login Domain blank.



g. The PC is now authenticated as an 802.1x client. Verify that the port has been authenticated with the **show dot1x interface** command.

```
SwitchP# show dot1x interface fa0/12
Supplicant MAC 0002.557a.4ab8
   AuthSM State      = AUTHENTICATED
   BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

Step 4 Enable Periodic Re-authentication

a. Change to interface configuration mode.

```
SwitchP(config)#int fa0/12
```

b. Enable periodic re-authentication of the client, which is disabled by default.

```
SwitchP(config-if)# dot1x reauthentication
```

c. Set the number of seconds between re-authentication attempts. The default is 3600 seconds.

```
SwitchP(config-if)# dot1x timeout reauth-period 4000
```

d. Return to privileged EXEC mode.

```
SwitchP(config)# end
```

e. Verify the entries in the configuration.

```
SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
--------------------------------------------------
Supplicant MAC 0002.557a.4ab8
   AuthSM State      = AUTHENTICATED
   BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Enabled
```



```
ReAuthPeriod      = 4000 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

Step 5 Manually Re-Authenticate a Client Connected to a Port

a. Manually re-authenticate the client connected to a port.

```
SwitchP# dot1x re-authenticate interface fa0/12
```

b. Use the **show dot1x all** command to verify that the client has been re-authenticated.

```
SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
--------------------------------------------------
Supplicant MAC <Not Applicable>
   AuthSM State      = CONNECTING
   BendSM State      = IDLE
PortStatus        = UNAUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Enabled
ReAuthPeriod      = 4000 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

Step 6 Change the Quiet Period

a. Set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 0 to 65535 seconds; the default is 60.

```
SwitchP(config-if)# dot1x timeout quiet-period 90
```

b. Issue a **show dot1x all** command to verify that the quiet period has been changed.

```
SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
Supplicant MAC 0002.557a.4ab8
   AuthSM State      = AUTHENTICATED
   BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
```



```
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod      = 4000 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

Step 7 Change the Switch-to-Client Retransmission Time

a. Set the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65535 seconds; the default is 30.

```
SwitchP(config-if)# dot1x timeout tx-period 45
```

b. Issue a **show dot1x all** command to verify the change in the configuration.

```
SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
--------------------------------------------------
Supplicant MAC 0002.557a.4ab8
   AuthSM State      = AUTHENTICATED
   BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod      = 4000 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 45 Seconds
Guest-Vlan        = 0
```

Step 8 Set the Switch-to-Client Frame-Retransmission Number

a. Set the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10 and the default is 2.

```
SwitchP(config-if)# dot1x max-req 3
```

b. Issue a **show dot1x all** command to verify the change in the configuration.

```
SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
```



```
---------------------------------------------------
Supplicant MAC 0002.557a.4ab8
   AuthSM State      = AUTHENTICATED
   BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 3
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod      = 4000 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 45 Seconds
Guest-Vlan        = 0
```

Step 9 Enable Multiple Hosts

a. Enter interface configuration mode, and specify the interface to which multiple hosts are indirectly attached.

```
SwitchP(config)# interface fa0/12
```

b. Allow multiple hosts (clients) on an 802.1x-authorized port.

```
SwitchP(config-if)# dot1x host-mode multi-host
```

Note	The **dot1x port-control** interface configuration command must be set to **auto** for the specified interface.

c. Issue a **show dot1x all** command to verify the change to the configuration.

```
SwitchP# show dot1x all
Dot1x Info for interface FastEthernet0/12
---------------------------------------------------
Supplicant MAC 0002.557a.4ab8
   AuthSM State      = AUTHENTICATED
   BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 3
HostMode          = Multi
Port Control      = Auto
QuietPeriod       = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod      = 4000 Seconds
ServerTimeout     = 30 Seconds
```



```
SuppTimeout       = 30 Seconds
TxPeriod          = 45 Seconds
Guest-Vlan        = 0
```

Step 10 Display 802.1x Statistics and Status

a. Use the **show dot1x statistics interface** command to display 802.1x statistics for a specific interface.

```
SwitchP# show dot1x statistics interface Fa0/12
PortStatistics Parameters for Dot1x
---------------------------------------
TxReqId = 8     TxReq = 10      TxTotal = 15
RxStart = 0     RxLogoff = 0    RxRespId = 2    RxResp = 4
RxInvalid = 0   RxLenErr = 0    RxTotal= 6
RxVersion = 1   LastRxSrcMac 0002.557a.4ab8
```

Sample configuration

A sample configuration is shown below:

```
Switch1#show run
Building configuration...

Current configuration : 2404 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch1
!
aaa new-model
aaa authentication dot1x default group radius local
aaa accounting connection default start-stop group radius
enable secret 5 $1$4vWf$S3sXATwAalDNo1solkYQA0
!
ip subnet-zero
!
no ip domain-lookup
ip ssh time-out 120
ip ssh authentication-retries 3
!
```



```
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
dot1x system-auth-control
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 301
!
interface FastEthernet0/2
 switchport access vlan 301
!
interface FastEthernet0/3
 switchport mode access
!
interface FastEthernet0/4
 switchport mode access
!
interface FastEthernet0/5
 switchport mode access
!
interface FastEthernet0/6
 switchport mode access
!
interface FastEthernet0/7
 switchport mode access
!
interface FastEthernet0/8
 switchport mode access
!
interface FastEthernet0/9
 switchport mode access
!
interface FastEthernet0/10
 switchport mode access
!
interface FastEthernet0/11
```



```
 switchport mode access
!
interface FastEthernet0/12
 switchport mode access
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x timeout quiet-period 90
 dot1x timeout tx-period 45
 dot1x timeout reauth-period 4000
 dot1x max-req 3
 dot1x reauthentication
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport mode access
!
interface FastEthernet0/14
 switchport mode access
!
interface FastEthernet0/15
 switchport mode access
!
interface FastEthernet0/16
 switchport mode access
!
interface FastEthernet0/17
 switchport mode access
!
interface FastEthernet0/18
 switchport mode access
!
interface FastEthernet0/19
 switchport mode access
!
interface FastEthernet0/20
 switchport mode access
!
interface FastEthernet0/21
 switchport mode access
```



```
!
interface FastEthernet0/22
 switchport mode access
!
interface FastEthernet0/23
 switchport mode access
!
interface FastEthernet0/24
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan301
 ip address 10.0.1.3 255.255.255.0
 no ip route-cache
!
ip http server
radius-server host 10.0.1.12 auth-port 1812 acct-port 1813 key
secretkey
radius-server retransmit 3
!
line con 0
line vty 0 4
 password cisco
line vty 5 15
!
!
end
```


Lab 8.3.13 Configure Cisco IOS Firewall CBAC

Objective

In this lab, the students will complete the following tasks:

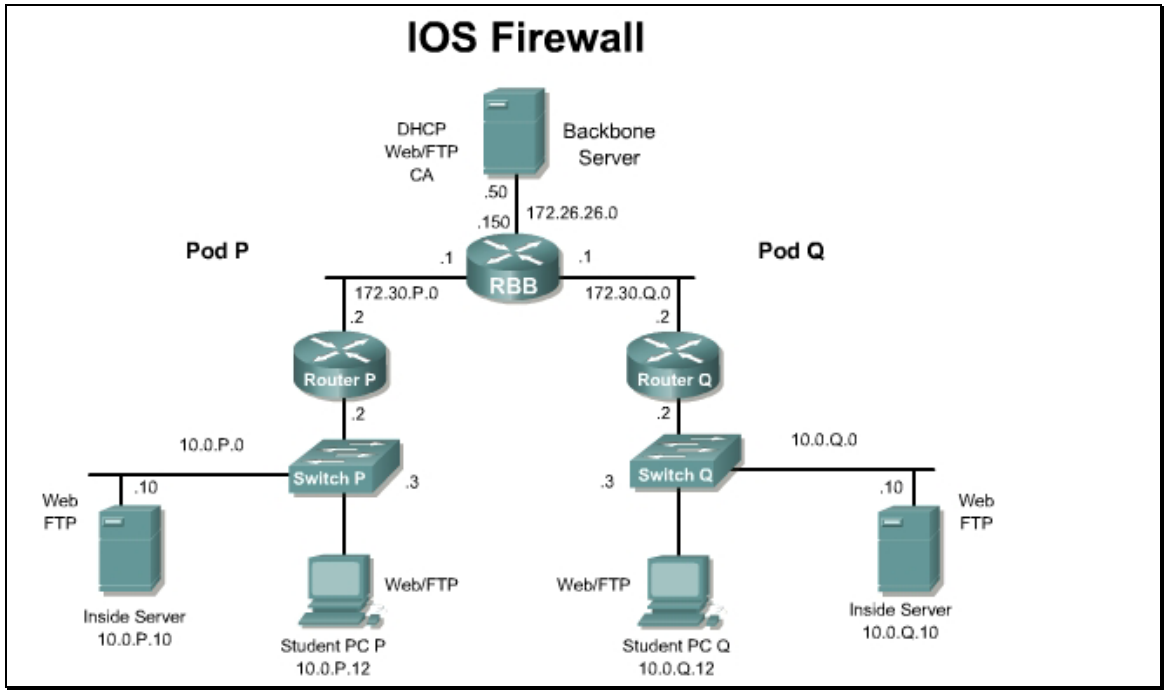
- Configure a simple firewall including CBAC using the Security Device Manager (SDM).
- Understand how CBAC enables a router-based firewall.
- Configure a simple firewall including CBAC and RFC Filtering using the IOS CLI
- Test and verify CBAC operation

Scenario

In a secure network, it is important that internal network remain protected form the outside network. Context-Based Access Control (CBAC) uses special format access control lists to protect internal network segments. This provides much greater protection than a standard perimeter router. CBAC is a component of the Cisco IOS Firewall feature set.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod routers. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the student PC. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at,

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c5.html

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
logging on	Enable logging to the console
logging 10.0.P.12	Enable logging to the syslog server
ip inspect audit-trail	Enable the audit trail
show access-lists	Check ACLs
show ip inspect name	View the CBAC configuration and session information.
show ip inspect config	Displays the complete CBAC inspection configuration
show ip inspect interfaces	Displays interface configuration with respect to applied inspection rules and access lists.
show ip inspect sessions detail	Displays existing sessions that are currently being tracked and inspected by CBAC. The optional detail keyword causes additional details about these sessions to be shown.
show ip inspect all	Displays all CBAC configurations and existing sessions that are currently being tracked and inspected by CBAC.

Part I: Configure CBAC using the Security Device Manager

Step 1 Using the SDM Firewall Wizard

Complete the following steps to configure a basic firewall using SDM:

a. Establish an SDM connection to the router using the username **sdm** and password **sdm**.

b. Click on the **Configure** button located in the main tool bar.

c. Click the **Firewall and ACL** button in the **Tasks** panel.

d. Click the **Basic Firewall** radio button and click the **Launch the selected task** button. The Basic Firewall Configuration Wizard pop up appears. Click the **Next** button. The Basic Firewall Interface Configuration page appears.

e. Select the Outside (untrusted) interface using the pull down tool. Select **FastEthernet0/1** or the appropriate interface which is connected to the “outside”.

f. Select the Inside (trusted) interface using the check boxes. Checkboxes allow users to select more than one inside interface at a time. Check the **FastEthernet0/0** box, leaving any others blank. Select the **Access Rule Log Option** to enable logging of denied access rule entries. Click **Next**

g. A warning may appear indicating that SDM may not be available to launch on a given interface (the outside interface, FA0/1) once the Firewall Wizard completes. Acknowledge the warning by clicking **OK**. The Internet Firewall Configuration Summary appears.

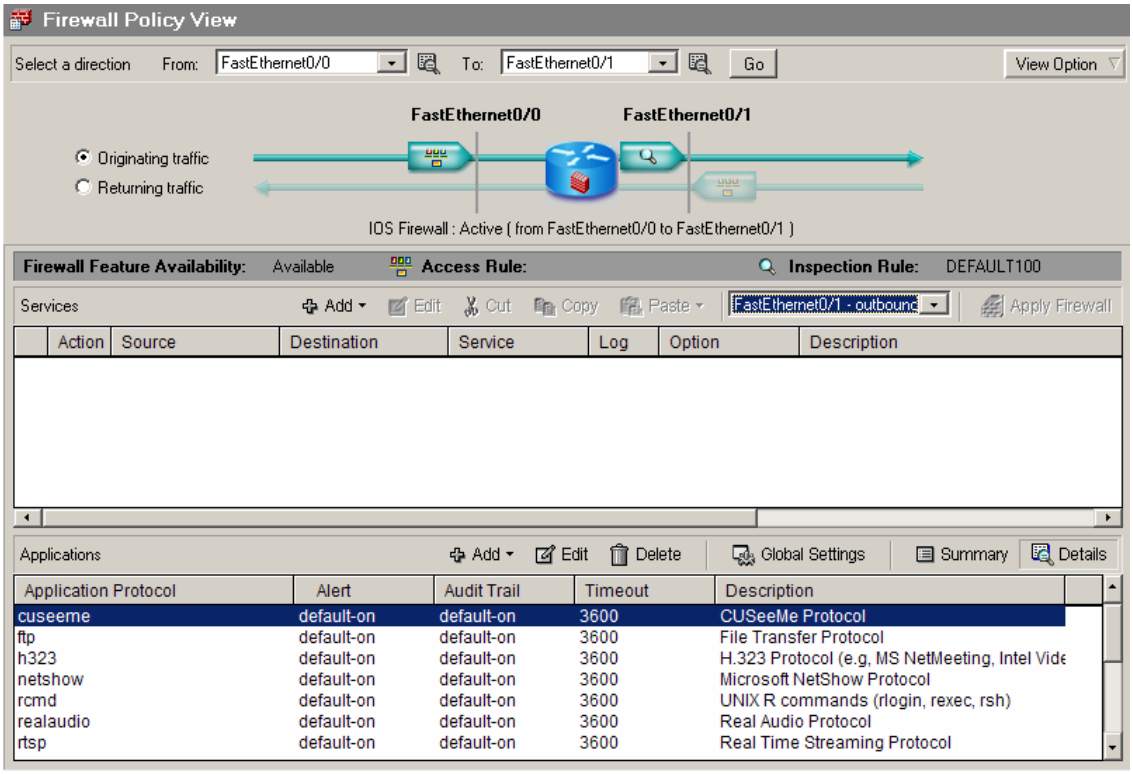
h. Click **Finish**. A popup to select which routing protocol traffic to allow will appear. Veirfy that EIGRP is selected and click **OK**.

1. Complete the SDM generated configuration. Depending on what configurations may be present, prompts and pop ups may vary. The SDM generated configuration is now delivered to the running configuration of the router. Test the configuration delivery by clicking the View item in the toolbar, and then selecting **Running Config** from the resulting pull-down menu.

Step 2 Verify the basic firewall configuration created by SDM

Complete the following steps to verify the CBAC configuration:

Click the **Configuration** button in the top menu, then the **Firewall and ACL** button in the **Tasks** panel. Select the **Edit Firewall Policy/ACL** tab.

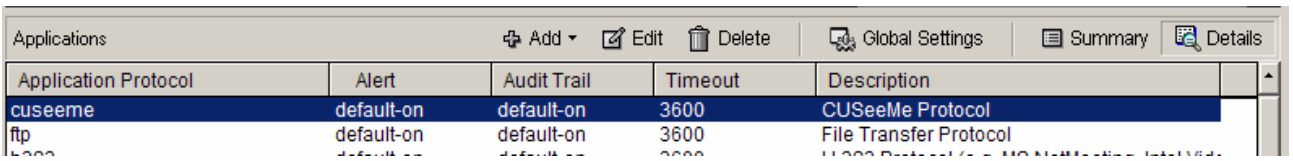


a. Notice the firewall icon, which is a brick wall, within the router icon. This indicated CBAC is running on the router.

1. What is the Inspection Rule name?

Answer: DEFAULT100

b. To see more information about the inspected protocols, click on the Details button in the Applications box.



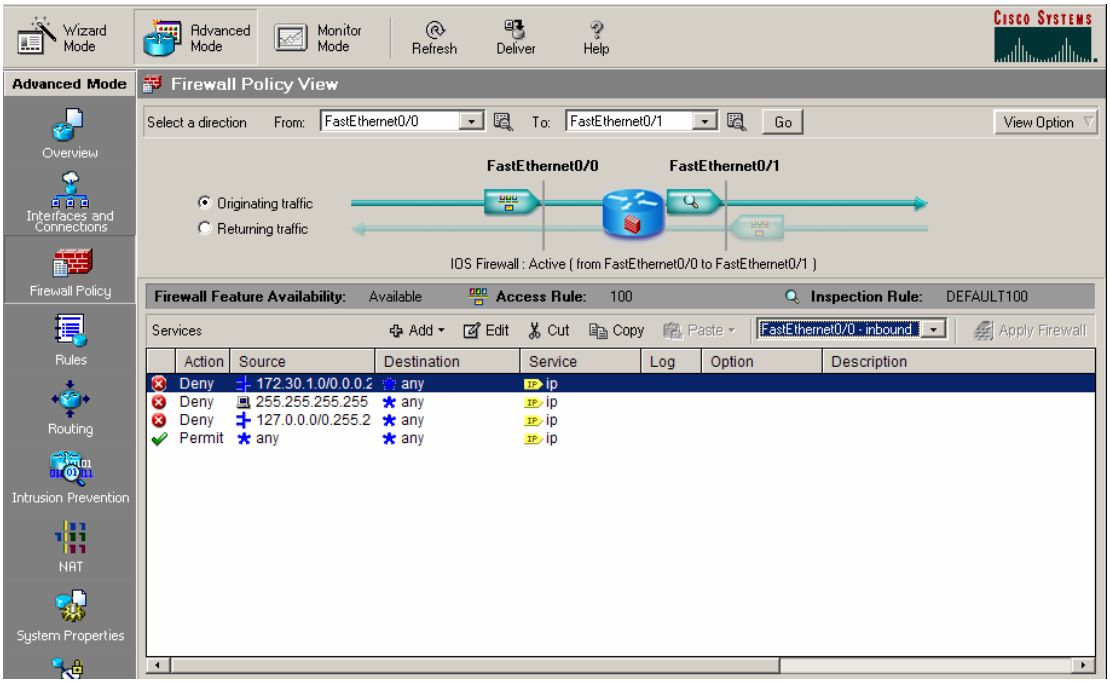
2. What applications are inspected?

Answer: cuseeme, ftp, h223, icmp, netshow, rcmd, realaudio, rtsp, smtp, sqlnet, streamworks, tftp, tcp, udp, vdolive

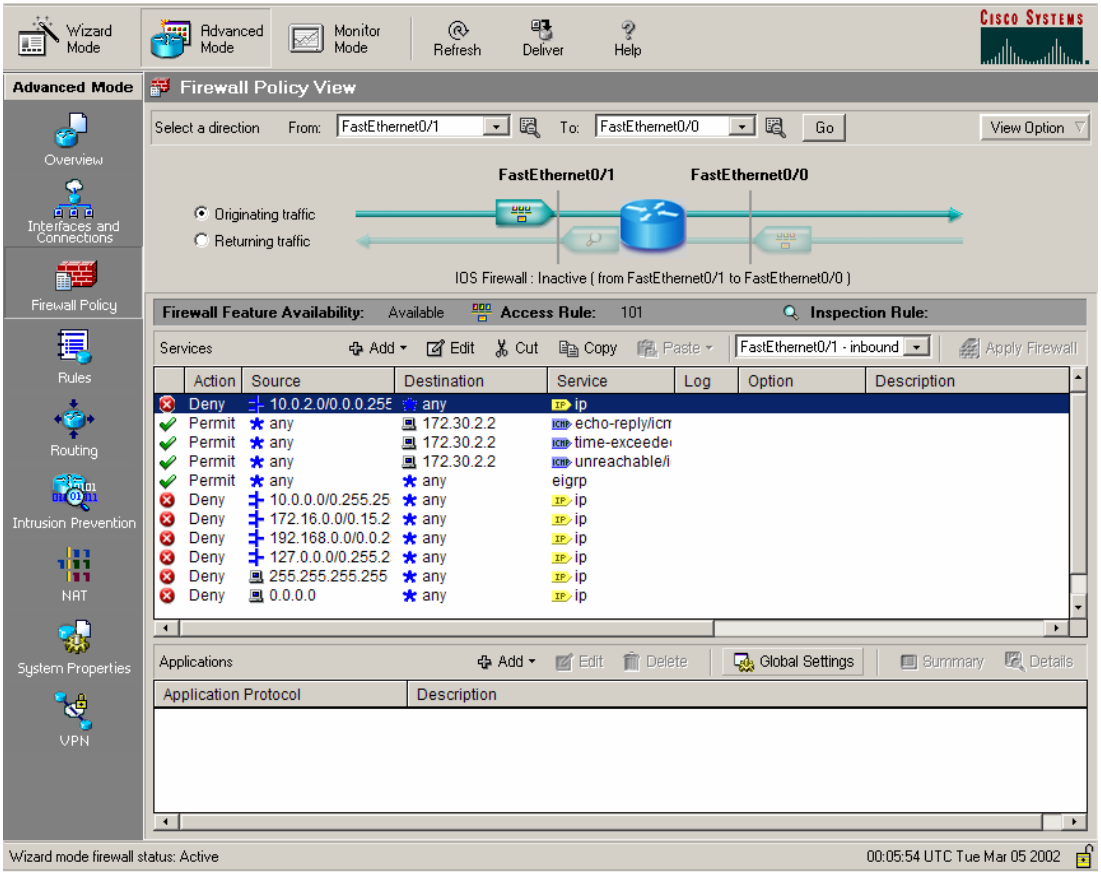
3. Can new applications be added or deleted?

Answer: Yes, applications can be added or deleted.

c. Verify the inbound ACLs on the inside interface.



d. Click on the **View Option** button within the Edit Firewall Policy/ACL window. Select **Swap From and To Interface**.



e. Notice that the firewall icon within the router is no longer present, and there is no Inspection Rule listed.

f. Click on the **View Option** button within the Edit Firewall Policy/ACL window. Select **Swap From and To Interfaces** again to return the interfaces to the correct configuration.

g. Carefully look at the overall CBAC configuration. Note how the ACLs and Inspection policy are applied to the router.

1. Which interface is the Inspection policy applied? Which direction? In or Out

_____

Answer: The inspection policy is applied on Fa0/0, the inside interface. The inspection policy is applied inbound.

2. Will traffic from the loop back or broadcast address be denied or passed? Which RFCs define these settings? What will happen to all other traffic?

_____

Answer: Traffic originating from loopback and broadcast addresses will be denied. This is defined by RFC 1918. Other traffic initiated from the inside address space will be allowed and will be inspected by CBAC.

3. What security has been applied to the outside interface?

_____

Answer: The SDM Firewall Wizard has created and applied an access list for the outside interface.

Step 3 Configure Logging and Audit Trails

Complete the following steps to configure logging and auditing trails:

a. On the router, enable logging to the console and the Syslog server.

```
RouterP(config)# logging on
RouterP(config)# logging console
RouterP(config)# logging 10.0.P.12
(where P = pod number)
```

b. Enable the audit trail:

```
RouterP(config)# ip inspect audit-trail
RouterP(config)# end
```

c. Start the Kiwi Sylog software on the Student PC.

d. Observe the output created via the router console or within the Kiwi log window as traffic is generated in the next step.

Step 4 Verify and test the basic firewall configuration created by SDM

Complete the following steps to verify and test the firewall configuration.

a. On the router, use the following commands to verify the CBAC configuration:

```
RouterP# show ip inspect name DEFAULT100
RouterP# show ip inspect config
RouterP# show ip inspect interfaces
RouterP# show ip inspect all
```

b. View the current inspection sessions.

```
RouterP#show ip inspect sessions
```



```
RouterP#
```

(There should not be any active sessions)

c. Ping RBB from the Student PC command prompt:

```
C:\> ping 172.26.26.150
Pinging 172.26.26.150 with 32 bytes of data:
Reply from 172.26.26.150: bytes=32 time=34ms TTL=125
Reply from 172.26.26.150: bytes=32 time=34ms TTL=125
Reply from 172.26.26.150: bytes=32 time=34ms TTL=125
Reply from 172.26.26.150: bytes=32 time=36ms TTL=125
```

d. On the router, use the following command to view the new dynamic ACL.

```
RouterP# show ip inspect sessions
Established Sessions
 Session 8447EF40 (10.0.P.12:0)=>(0.0.0.0:0) icmp SIS_OPEN
```

e. Use the following command to view the session detail. This command must be used within 10 seconds of the ping to achieve the results shown below.

```
RouterP# show ip inspect sessions detail
Established Sessions
 Session 833B7378 (10.0.1.12:8)=>(172.26.26.150:0) icmp SIS_OPEN
  Created 00:00:02, Last heard 00:00:00
   ECHO request
  Bytes sent (initiator:responder) [96:96]
   In  SID 172.26.26.150[0:0]=>10.0.P.12[0:0] on ACL 101  (4
   matches)
  In  SID 0.0.0.0[0:0]=>10.0.P.12[14:14] on ACL 101
  In  SID 0.0.0.0[0:0]=>10.0.P.12[3:3] on ACL 101
  In  SID 0.0.0.0[0:0]=>10.0.P.12[11:11] on ACL 101
```

f. Wait 10 seconds and reissue the command.

```
RouterP# show ip inspect sessions detail
```

1. There should not be any active sessions. Why?

_____

Answer: The session has timed out.

g. From the Student PC, telnet to RBB.

```
C:\> telnet 172.26.26.150
```

h. Use the following command to view the new dynamic ACL.

```
RouterP# show ip inspect sessions
Session 84521F20 (10.0.P.12:4525)=>(172.26.26.150:23) tcp
SIS_OPEN
```

1. How can this session be identified as a telnet session?

_____

Answer: This session can be identified as a telnet session because it uses port 23.

i. Use the following commands to view the session detail.

```
RouterP# show ip inspect sessions detail

Established Sessions

 Session 84521F20 (10.0.P.12:4597)=>(172.26.26.150:23) tcp
SIS_OPEN

  Created 00:00:07, Last heard 00:00:05

  Bytes sent (initiator:responder) [37:66]

  In  SID 172.26.26.150[23:23]=>10.0.P.12[4597:4597] on ACL 101
(9 matches)
```

j. Close the telnet session.

k. From the Student PC, use the web browser to connect to RBB.

Enter **http://172.26.26.150** in the URL field. Do not enter the password.

l. Use the following command to view the new dynamic ACL.

```
RouterP# show ip inspect sessions

Session 844B5980 (10.0.P.12:4675)=>(172.26.26.150:80) tcp
SIS_OPEN
```

1. How can this session be identified as a web session?

_____

Answer: This session can be identified as a web session because it uses port 80.

m. Use the following commands to view the session detail.

```
RouterP# show ip inspect sessions detail

Established Sessions

 Session 844B5980 (10.0.P.12:4675)=>(172.26.26.150:80) tcp
SIS_OPEN

  Created 00:01:51, Last heard 00:01:51

  Bytes sent (initiator:responder) [358:338]

  In  SID 172.26.26.150[80:80]=>10.0.P.12[4675:4675] on ACL 101
(3 matches)
```

n. Return to web browser to enter the password to RBB

o. Observe the console or Kiwi Syslog window as the dynamic ACLs entries are removed.

```
00:40:06: %FW-6-SESS_AUDIT_TRAIL: Stop tcp session: initiator
(10.0.P.12:4675) sent 440 bytes -- responder (172.26.26.150:80) sent
823 bytes
```

1. How long does a typical TCP session remain open to a device?

_____

Answer: The default connection timeout is 30 seconds. The default FIN wait timeout is 4 seconds. The default idle timeout is 3600 seconds (one hour).

Part II: Configure CBAC using CLI

Step 1 Define and Apply Inspection Rules and ACLs using IOS CLI

Complete the following steps to define and apply inspection rules and Access Control Lists (ACLs):

a. Reload the startup configuration for this lab or remove the existing ACLs and CBAC configuration applied by SDM.

b. Enter global configuration mode on the perimeter router.

c. On the router, define a CBAC rule to inspect all TCP and FTP traffic.

```
RouterP(config)# ip inspect name FWRULE tcp timeout 300
RouterP(config)# ip inspect name FWRULE ftp timeout 300
RouterP(config)# ip inspect name FWRULE icmp
```

d. Define the ACLs to allow outbound ICMP traffic and CBAC traffic (FTP and WWW). Block all other inside-initiated traffic.

(RFC 2827 filtering)

```
RouterP(config)# access-list 100 deny ip 172.30.P.0 0.0.0.255 any
(where P = pod number)
```

(RFC 1918 filtering)

```
RouterP(config)# access-list 100 deny ip host 255.255.255.255 any
RouterP(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255
any
RouterP(config)# access-list 100 permit ip any any
```

e. Define ACLs to allow inbound ICMP traffic and CBAC traffic (FTP and WWW) to the inside web or FTP server. Block all other outside-initiated traffic.

(RFC 2827 filtering)

```
   RouterP(config)# access-list 101 deny ip 10.0.P.0 0.0.0.255
any
```

(permit ping and routing updates)

```
RouterP(config)# access-list 101 permit icmp any host 172.30.P.2
echo-reply
RouterP(config)# access-list 101 permit icmp any host 172.30.P.2
time-exceeded
RouterP(config)# access-list 101 permit icmp any host 172.30.P.2
unreachable
RouterP(config)# access-list 101 permit eigrp any any
RouterP(config)# access-list 101 deny ip 10.0.0.0 0.255.255.255
any
```

(RFC 1918 filtering)

```
RouterP(config)# access-list 101 deny ip 172.16.0.0 0.15.255.255
any
RouterP(config)# access-list 101 deny ip 192.168.0.0 0.0.255.255
any
RouterP(config)# access-list 101 deny ip 127.0.0.0 0.255.255.255
any
RouterP(config)# access-list 101 deny ip host 255.255.255.255 any
```



```
RouterP(config)# access-list 101 deny ip host 0.0.0.0 any
RouterP(config)# access-list 101 deny ip any any log
!
```

(where P = pod number)

f. Apply the inspection rule and ACL to the inside interface:

```
RouterP(config)# interface fa0/0
RouterP(config-if)# ip access-group 100 in
```

g. Apply the ACL to the outside interface:

```
RouterP(config-if)# interface fa0/1
RouterP(config-if)# ip inspect FWRULE out
RouterP(config-if)# ip access-group 101 in
RouterP(config-if)# exit
```

Step 2 Configure Logging and Audit Trails

Complete the following steps to configure logging and auditing trails:

a. Log into the perimeter router and access global configuration mode.

b. On the router, enable logging to the console and the Syslog server.

```
RouterP(config)# logging on
RouterP(config)# logging console
RouterP(config)# logging 10.0.P.12
```

(where P = pod number)

c. Enable the audit trail:

```
RouterP(config)# ip inspect audit-trail
RouterP(config)# end
RouterP#
```

d. Start the Kiwi Sylog software on the Student PC.

Step 3 Test and Verify CBAC

Complete the following steps to verify and test the firewall configuration.

a. On the router, use the following commands to verify the CBAC configuration:

```
RouterP# show ip inspect name FWRULE
RouterP# show ip inspect config
RouterP# show ip inspect interfaces
RouterP# show ip inspect all
```

b. View the current inspection sessions.

```
RouterP#show ip inspect sessions
RouterP#
```

(There should not be any active sessions)

c. Ping RBB from the Student PC command prompt:

```
C:\> ping 172.26.26.150
Pinging 172.26.26.150 with 32 bytes of data:
Reply from 172.26.26.150: bytes=32 time=34ms TTL=125
Reply from 172.26.26.150: bytes=32 time=34ms TTL=125
Reply from 172.26.26.150: bytes=32 time=34ms TTL=125
Reply from 172.26.26.150: bytes=32 time=36ms TTL=125
```

d. On the router, use the following command to view the new dynamic ACL.

```
RouterP# show ip inspect sessions
Established Sessions
Session 8447EF40 (10.0.P.12:0)=>(172.26.26.150:0) icmp SIS_OPEN
```

e. Use the following commands to view the session detail. This command must be used within 10 seconds of the ping to achieve the results shown below. Repeat the ping if needed.

```
RouterP# show ip inspect sessions detail
Established Sessions
 Session 84521F20 (10.0.P.12:0)=>(0.0.0.0:0) icmp SIS_OPEN
  Created 00:00:04, Last heard 00:00:01
   Destinations: 1
       Dest addr [172.26.26.150]
  Bytes sent (initiator:responder) [128:128]
   In  SID 172.26.26.150[0:0]=>10.0.P.12[0:0] on ACL 101  (4
   matches)
  In  SID 0.0.0.0[0:0]=>10.0.P.12[14:14] on ACL 101
  In  SID 0.0.0.0[0:0]=>10.0.P.12[3:3] on ACL 101
  In  SID 0.0.0.0[0:0]=>10.0.P.12[11:11] on ACL 101
```

f. Wait 10 seconds and reissue the command.

```
RouterP# show ip inspect sessions
```

1. There should not be any active sessions. Why?

_____

Answer: The session has timed out.

g. From the Student PC, telnet to RBB.

```
C:\> telnet 172.26.26.150
```

h. Use the following command to view the new dynamic ACL.

```
RouterP# show ip inspect sessions
Session 84521F20 (10.0.P.12:4525)=>(172.26.26.150:23) tcp
SIS_OPEN
```

1. How can this session be identified as a telnet session?

_____

Answer: This session can be identified as a telnet session because it uses port 23.

i. Use the following commands to view the session detail.

```
RouterP# show ip inspect sessions detail

Established Sessions

 Session 84521F20 (10.0.P.12:4597)=>(172.26.26.150:23) tcp
SIS_OPEN

  Created 00:00:07, Last heard 00:00:05

  Bytes sent (initiator:responder) [37:66]

  In  SID 172.26.26.150[23:23]=>10.0.P.12[4597:4597] on ACL 101
(9 matches)
```

j. Close the telnet session.

k. From the Student PC, use the web browser to connect to RBB.

Enter **http://172.26.26.150** in the URL field. Do not enter the password.

l. Use the following command to view the new dynamic ACL.

```
RouterP# show ip inspect sessions

Session 844B5980 (10.0.P.12:4695)=>(172.26.26.150:80) tcp
SIS_OPEN
```

1. How can this session be identified as a web session?

_____

Answer: This session can be identified as a web session because it uses port 80.

m. Use the following commands to view the session detail.

```
RouterP# show ip inspect sessions detail

Established Sessions

 Session 844B5980 (10.0.P.12:4695)=>(172.26.26.150:80) tcp
SIS_OPEN

  Created 00:01:51, Last heard 00:01:51

  Bytes sent (initiator:responder) [358:338]

  In  SID 172.26.26.150[80:80]=>10.0.P.12[4675:4695] on ACL 101
(3 matches)
```

n. Return to web browser to enter the password to RBB

o. Observe the console or Kiwi Sylog window as the dynamic ACLs entries are removed.

```
00:40:06: %FW-6-SESS_AUDIT_TRAIL: Stop tcp session: initiator
(10.0.P.12:4695) sent 440 bytes -- responder (172.26.26.150:80)
sent 823 bytes
```

1. How long does a typical TCP session remain open to a device?

_____

Answer: The tcp timeout has been set to 300 seconds (five minutes)

Lab 9.1.7a Configure Access Through the PIX Security Appliance using ASDM

Objective

In this lab exercise, the students will complete the following tasks:

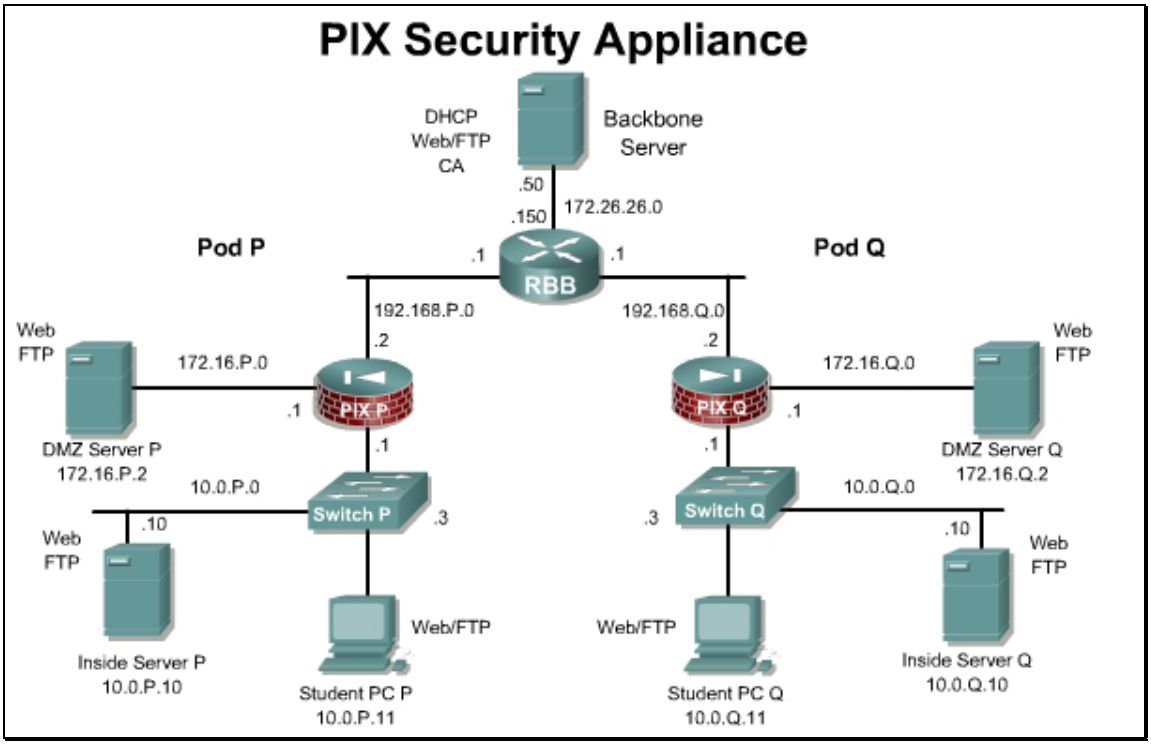
- Use ASDM to verify the starting configuration.
- Configure the PIX Security Appliance to allow inbound traffic to the bastion host using ASDM
- Configure the PIX Security Appliance to allow inbound traffic to the inside host using ASDM
- Test and verify correct PIX Security Appliance operation using ASDM

Scenario

In this exercise, the task is to configure the PIX Security Appliance using ASDM to protect Company XYZ internal network and public web services from intruders.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod PIX Security Appliances. Access the PIX Security Appliance console port using the terminal emulator on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at, http://www.cisco.com/application/pdf/en/us/guest/products/ps6121/c1225/ccmigration_09186a008045786c.pdf

Step 1 Verify the starting configuration.

The starting configuration should be loaded for this lab. Verify the configuration.

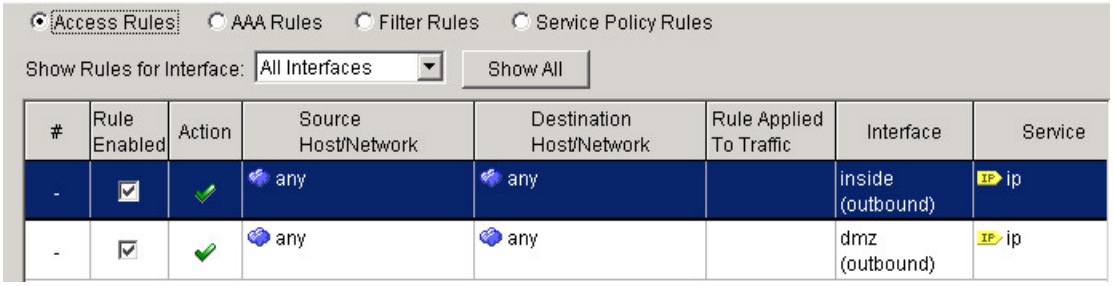
a. From the student PC web browser, log into ASDM

https://10.0.P.1

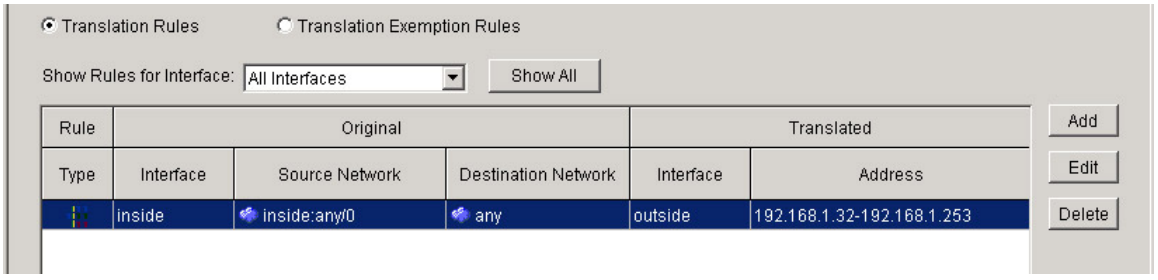
(Where P= pod number)

b. Click on the **Configuration** button.

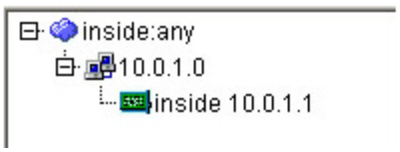
c. Click on **Security Policy** in the **Features** tab, and verify that there are rules to allow traffic from inside (outbound) and dmz (outbound).



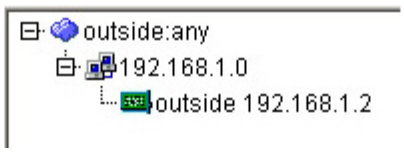
d. Click on the **NAT** in the **Features** panel, and verify the NAT configuration.



e. Click on the **Building Blocks** in the **Features** panel, and then select **Hosts/Networks** from the tree menu. Verify the inside, outside, and DMZ address configuration. A sample from Pix1 is shown below.



Inside



Outside

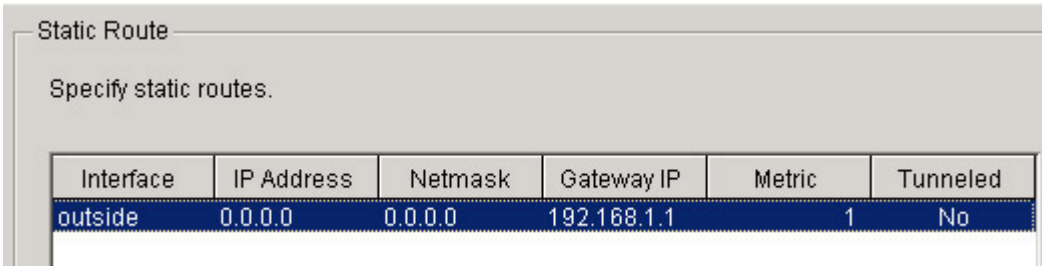
DMZ

f. Click on the **Interfaces** in the **Features** panel.

g. Verify the inside, outside, and DMZ address configuration. A sample from Pix1 is shown below.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet1	inside	Yes	100	10.0.1.1	255.255.255.0	No	1500
Ethernet2	dmz	Yes	50	172.16.1.1	255.255.255.0	No	1500
Ethernet0	outside	Yes	0	192.168.1.2	255.255.255.0	No	1500

h. Click on **Routing** in the **Features** panel, and select **Static Route** from the tree menu. Verify the default outbound route.



i. Navigate to **Tools>Ping…** and ping the following addresses.

   a. RBB: 192.168.P.1 and 172.26.26.150

   b. SuperServer 172.26.26.50

   c. DMZ: 172.16.1.2

j. Using a web browser, test connectivity from the Student PC to the RBB web interface:

http://172.26.26.150

k. Using a web browser, test connectivity from the Student PC to the SuperServer web interface:

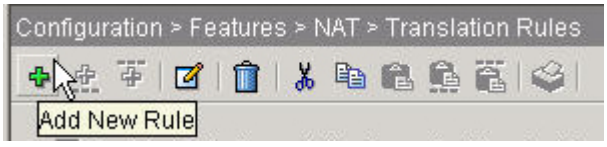
http://172.26.26.50

Step 2 Configure the PIX Security Appliance to Allow Users on the Inside Interface to Access the Bastion Host

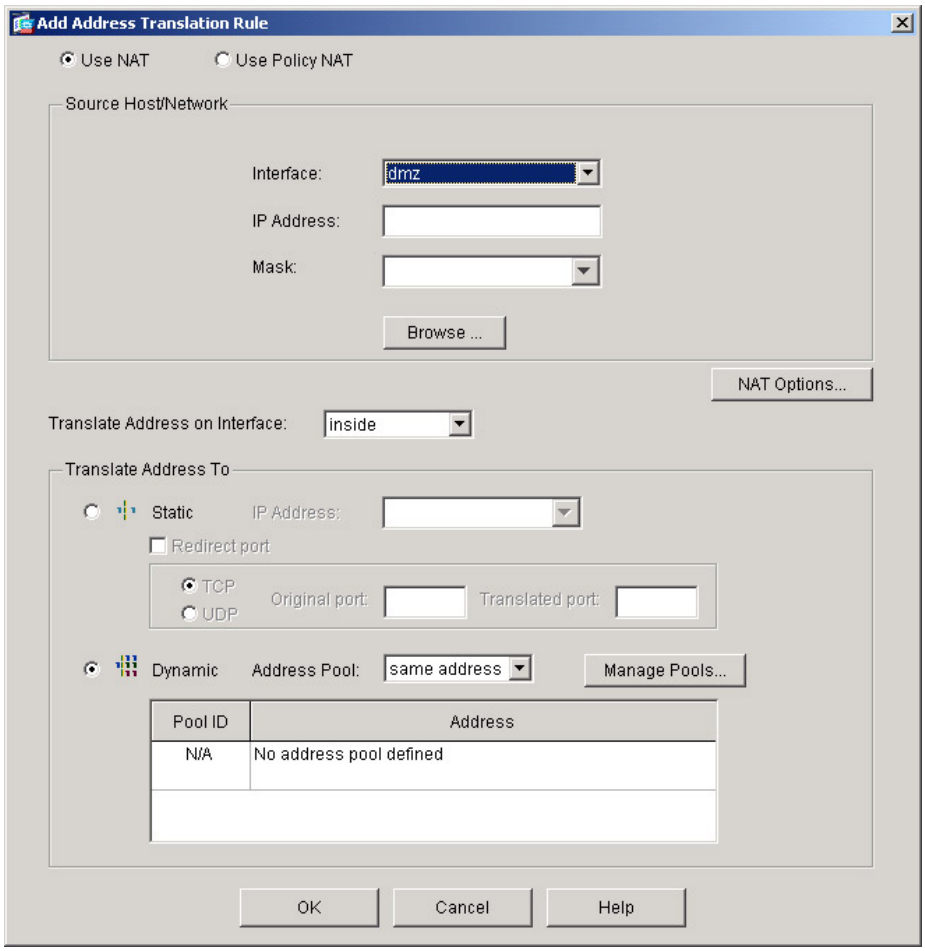
In this step, access will be configured to allow traffic from the inside network to access the DMZ network.

a. Click on the **NAT** in the Features panel.

b. Click on the **Add New Rule** icon or click on **Rules>Add** from the menu.



c. The **Add Address Translation Rule** window appears



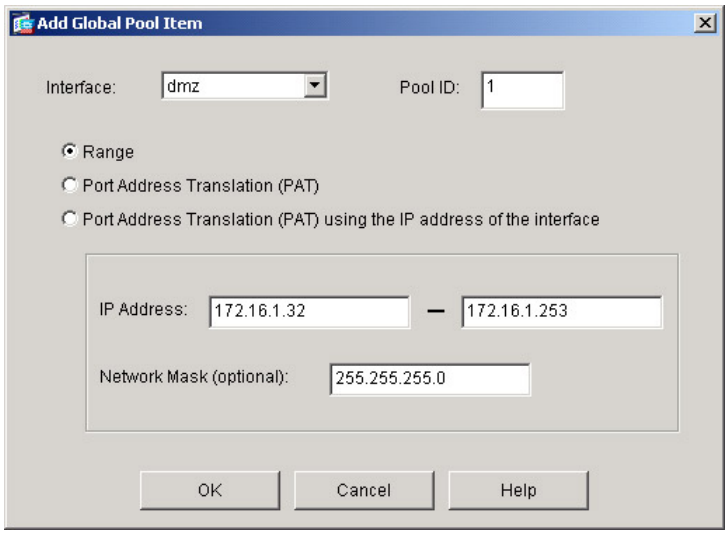
d. Click on the **Browse** button and select the **inside:any/0** network

e. In the **Translate address on interface** drop down menu, verify that **dmz** is selected.

f. Click on the **Manage Pools** Button. The **Manage Global Address Pools** window appears.

g. Click on the **Add** button. The **Add Global Pool Item** window appears.

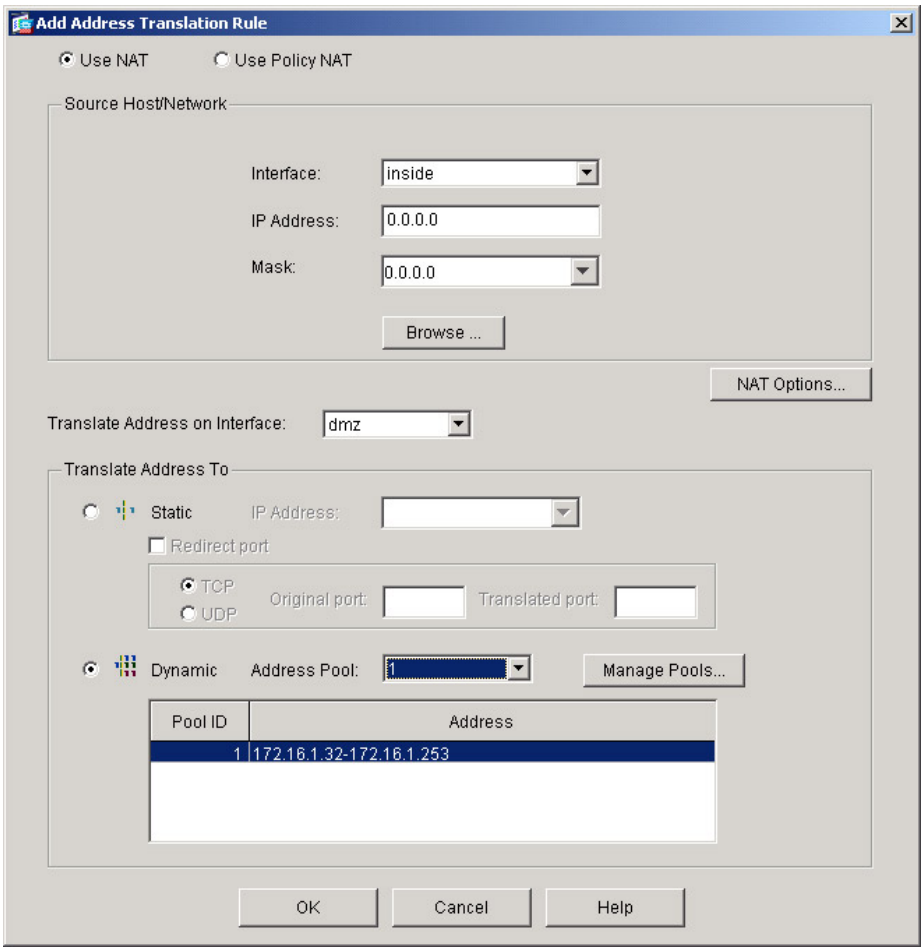
h. Choose **dmz** for the interface and enter a Pool ID: of **1**. Enter a Range of **172.16.P.32 – 172.16.P.253** with a mask of **255.255.255.0**



i. Click the **OK** button to return to the **Manage Global Address Pools** window.

j. Click **OK** to return to the **Add Address Translation Rule** window.

k. In the Dynamic Address pool drop down menu, Select **1**



l. Click **OK** to return to the main **Translation Rules** window.

m. Click on the **Apply** button. If the **Preview CLI Commands** window appears, click the **Send** button to continue.

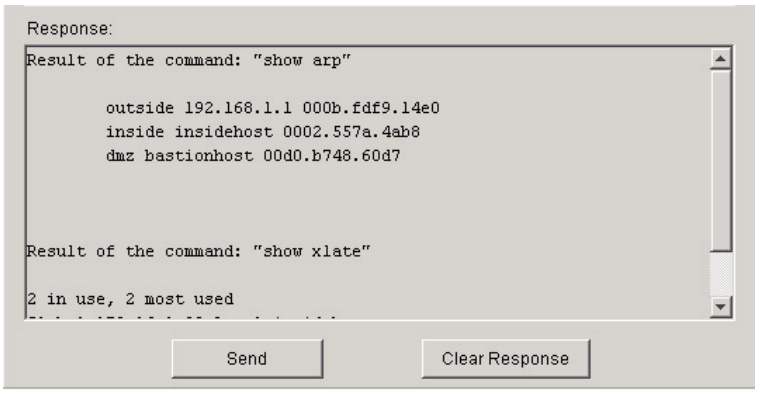
Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	inside:any/0	any	dmz	172.16.1.32-172.16.1.253
	inside	inside:any/0	any	outside	192.168.1.32-192.168.1.25

n. Go to **Tools>Command Line Interface…** and issue a **`clear xlate`** command.

o. Close the **Command Line Interface** window. If a **Confirm Configuration Refresh** dialog box appears, click the **Yes** button to continue.

p. Test web access to the pod bastion host from the pod PC using the web browser to access the pod bastion host by entering **http://172.16.P.2**. The home page of the bastion host should appear on the web browser.

q. Return to **Tools>Command Line Interface…** Use the **`show arp`**, **`show conn`**, and **`show xlate`** commands to observe the transaction:



r. Click on the **Close** button.

s. Test the FTP access to the bastion host from the PC. Verify that there is an FTP server running on the DMZ server.

t. Establish an FTP session using a command prompt, web browser, or ftp client. If a web browser or ftp client is used, the Passive FTP option must be available and enabled in the FTP client application.

u. For a command prompt, choose **Start** > **Run** > **ftp 172.16.P.2**. If the following message appears, this indicates the bastion host has been reached:

`"Connected to 172.16.P.2."`

(where P = pod number)

v. Log into the FTP session:

`User (172.16.P.2(none)): anonymous`

`331 Anonymous access allowed, send identity (e-mail name) as password.`

`Password: cisco`

(where P = pod number)

w. In ASDM, click on the **Monitoring** button.

x. Click on **the Interface Graphs>DMZ** in the tree menu.

y. Add the following to the graph list and Click the **Graph It!** button.

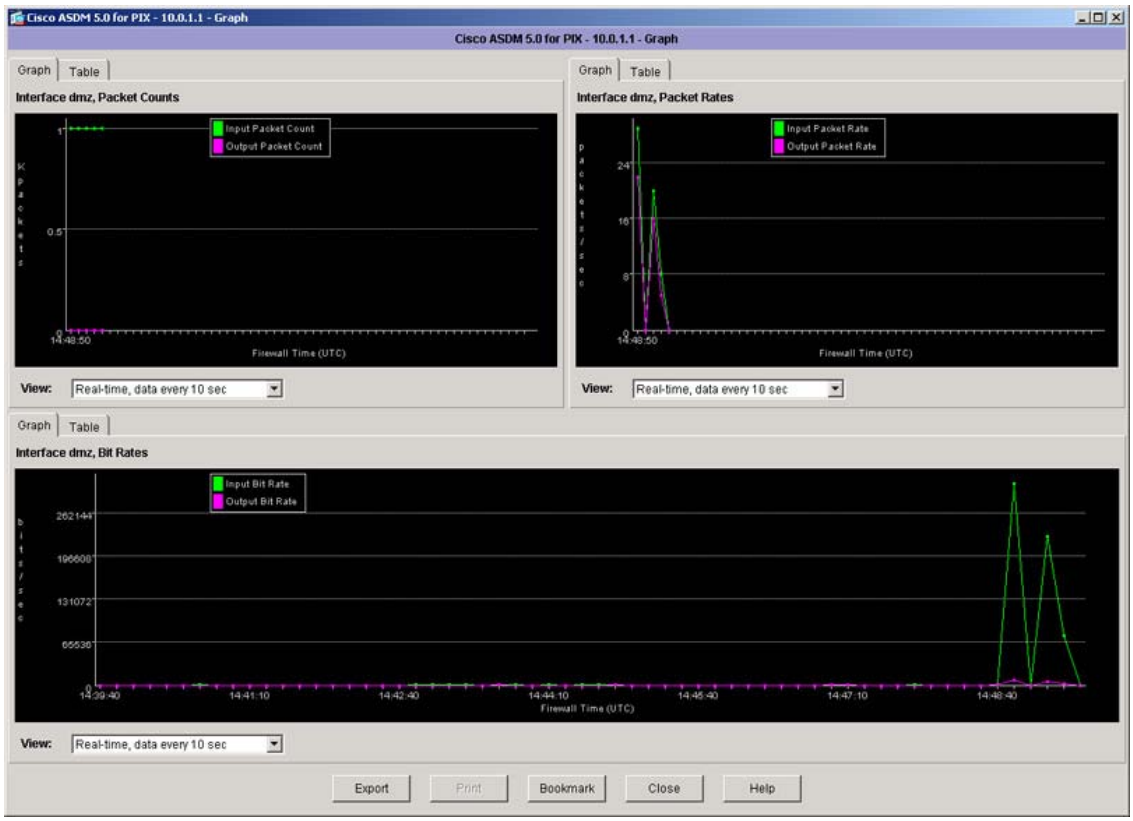
   a. Packet Counts

   b. Packet Rates

   c. Bit Rates

z. Download a large file to the Student PC.

aa. Observe the traffic graph in real time.



bb. Log out of the FTP session and close the traffic graph window.

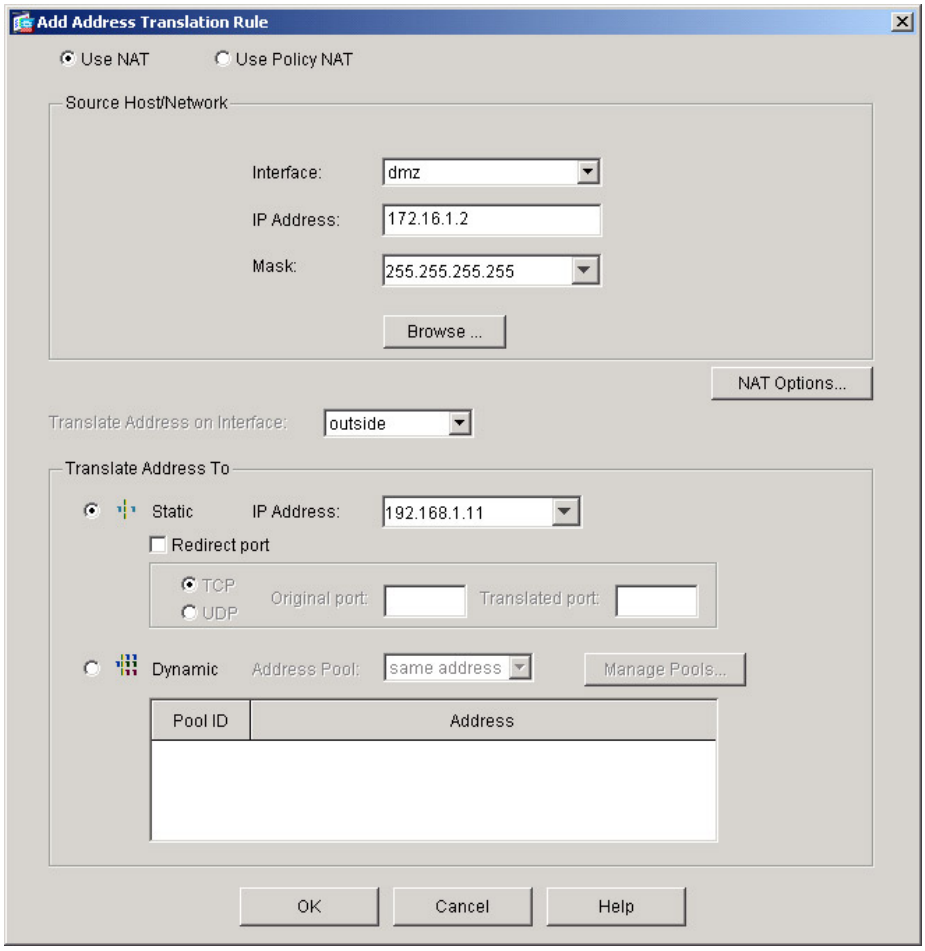
Step 3 Configure Access from the Outside to the Bastion Host

Configure a static translation so that traffic originating from the bastion host always has the same source address on the outside interface of the PIX Security Appliance. Then configure an ACL to allow users on the outside interface to access the bastion host.

a. On the Configuration page, click on the **NAT** in the **Features** panel.

b. Click on the **Add New Rule** icon or click on **Rules>Add** from the menu. The **Add Address Translation Rule** window appears.

c. Create a static translation for the pod bastion host. Use the IP address 172.16.P.2 /32 for the bastion host. Translate this address to the static outside address 192.168.P.11. A sample screenshot of Pix1 is shown below.



d. Click the **OK** button to return to the main translation tab window.

e. Click the **Apply** button. Notice the new static translation is added to the existing list of 2 dynamic translation entries.

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	dmz	bastionhost 172.16.1.2	any	outside	192.168.1.11
	inside	inside:any/0	any	dmz	172.16.1.32-172.16.1.253
	inside	inside:any/0	any	outside	192.168.1.32-192.168.1.25

f. After the static entry is complete, the next step is to define an ACL to permit web and ftp traffic associated with the static entry.

g. Click on **Security Policy** in the **Features** panel.

h. Click on the **Add New Rule** icon. The **Add Access Rule** window appears.

i. Configure the ACL as follows

1. Action: Permit
2. Source: Outside (0.0.0.0/0.0.0.0)
3. Destination: dmz –bastionhost 172.16.1.2

j. Verify that **TCP** is selected in the Protocol and Service group box.

k. Verify that = is chosen in the Service drop-down menu within the Source Port group box.

l. Verify that **any** appears in the Service field within the Source Port group box.

m. Verify that = is chosen in the Service drop-down menu within the Destination Port group box.

n. Click the **…** button within the Destination Port group box. The Service window opens.

o. Choose **http** from the Service list.

p. Click **OK**. This will return to open the **Add Access Rule** window.

q. Click **OK** to return to the main **Access Rules** window.

r. Repeat the same steps to Add an Access Rule for ftp.

s. Click the **OK** button

t. Click the **Apply** button.

u. Click **Send** if the preview CLI Commands window appears. The following Access rules should be displayed in the main Access Rules window.

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
-	☑	✔	any	any		inside (outbound)	ip
-	☑	✔	any	any		dmz (outbound)	ip
1	☑	✔	any	bastionhost/ 172.16.1.2	incoming	outside	http/tcp
2	☑	✔	any	bastionhost/ 172.16.1.2	incoming	outside	ftp/tcp

v. From a console session on the PIX, clear the translations and turn on packet debugging for the DMZ interface.

```
PixP# clear xlate
PixP# debug packet dmz
```

w. Test web access to the bastion host. Observe the debug output while the connections occur.

Option 1: Peer pod groups complete the testing.

i. Open a web browser on the Student PC.

ii. Use the web browser to access the bastion host of the peer pod group:

http://192.168.Q.11 (where Q = peer pod number)

iii. Use the web browser or ftp client to access the bastion host of the peer pod group:

ftp://192.168.Q.11 (where Q = peer pod number)

iv. Have a peer pod group test the configuration in the same way.

Option 2: Independent testing – From an Internet PC located on the outside (172.26.26.0/24) network, test access to the DMZ server. The internet PC can be configured to receive IP settings from the DHCP server function of RBB.

i. Open a web browser on the Internet PC.

ii. Use the web browser to access the bastion host:

http://192.168.P.11 (where P = pod number)

iii. Use the web browser or ftp client to access the bastion host:

ftp://192.168.P.11 (where P = pod number)

iv. Have a peer pod group test the configuration in the same way.

v. If you are using a Windows 2K Superserver, you may need to enter a static route statement using a command prompt on the Superserver:

```
C:\> route add 172.26.26.220 mask 255.255.255.255 172.16.P.1
```

(where 172.26.26.220 is the Internet PC address)

x. From a console session on the PIX, disable the debugging.

```
PixP# no debug packet dmz
PACKET trace off
```

y. In ASDM, navigate to **File>Show Running Configuration in New Window**. Note the configuration statements that have been added from this Step.

```
access-list outside_access_in permit tcp any host 192.168.1.11 eq
www
access-list outside_access_in permit tcp any host 192.168.1.11 eq
ftp
static (dmz,outside) 192.168.1.11 bastionhost netmask
255.255.255.255
access-group outside_access_in in interface outside
```

Step 4 Configure Inbound Access to the Student PC

Complete the following steps to configure the PIX Security Appliance to permit inbound access to the Student PC on the inside interface:

a. Create a static translation for the inside host by completing the following sub-steps:

i. Select **NAT** from the **Features** panel.

ii. Select the **Add New Rule** icon in the toolbar. The **Add Address Translation Rule** window opens.

iii. Verify that the **inside** interface is chosen in the Interface drop-down menu for the **Source/Host Network** group box.

iv. Enter the IP address **10.0.P.11** and subnet mask **255.255.255.255** for the inside host.

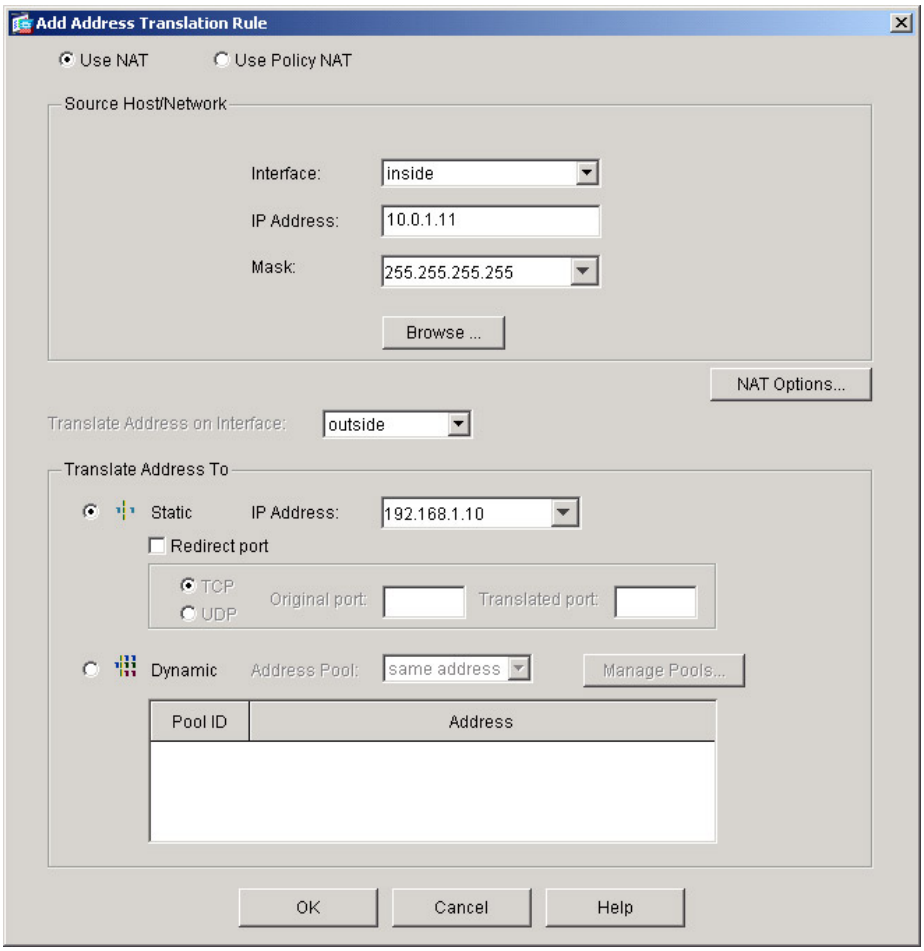
(where P = pod number)

v. Verify that **outside** is chosen in the **Translate Address on Interface** drop-down menu.

vi. Select **Static** in the **Translate address To** group box.

vii. Enter **192.168.P.10** in the IP Address field.

(where P = pod number)



viii. Click **OK**. The new rule appears on the Translation Rules tab.

ix. Click **Apply**. The Preview CLI Commands window opens.

x. Click **Send**.

b. Configure an ACL to allow pinging through the PIX Security Appliance by completing the following sub-steps:

i. Select **Security Policy** from the **Features** panel.

ii. Click on the **Add New Rule** icon. The **Add Access Rule** window appears.

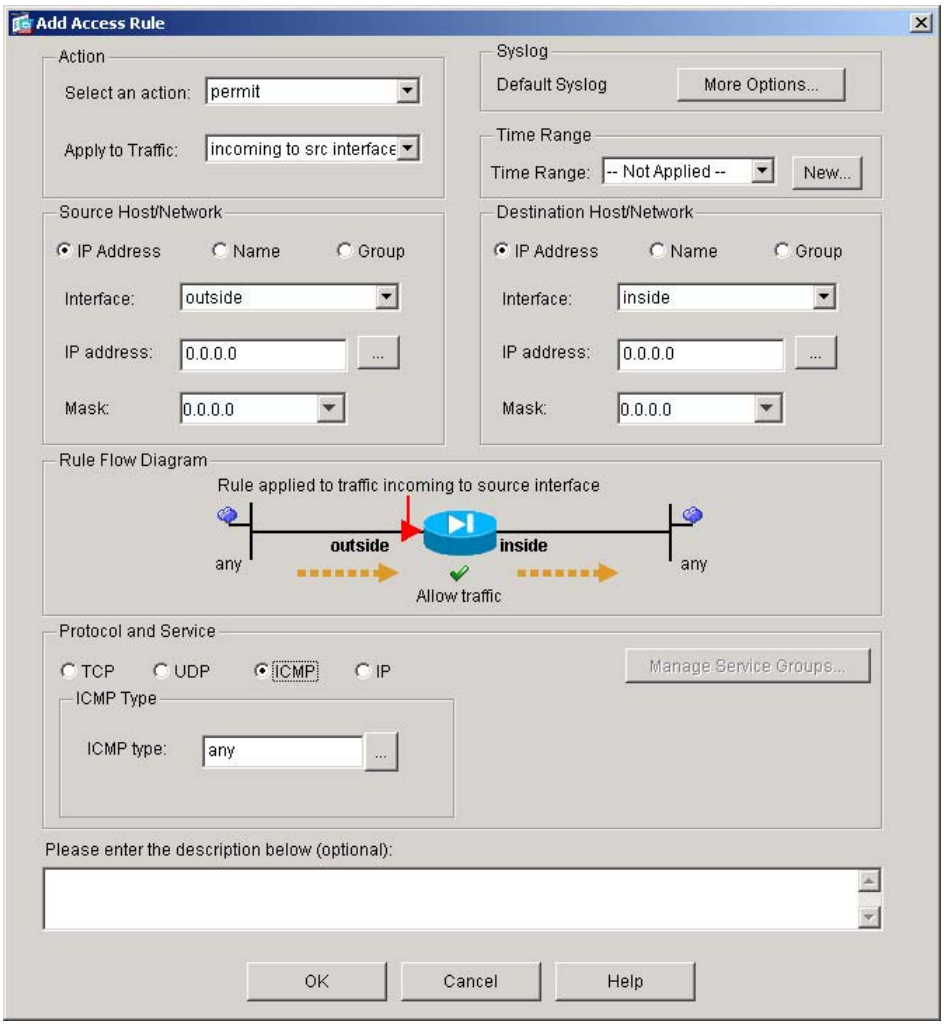
iii. Verify that **permit** is chosen in the **Select an action** drop-down menu.

iv. Choose **outside** from the **Interface** drop-down menu in the **Source Host/Network** group box.

v. Choose **inside** from the **Interface** drop-down menu in the **Destination Host/Network** group box.

vi. Select **ICMP** in the **Protocol and Service** group box.

vii Verify that **any** is selected in the **ICMP type** group box.



viii. Click **OK**. The new rule appears in the **Access Rules** window.

ix. Click **Apply**. The Preview CLI Commands window opens.

x. Observe the ACLs to be sent to the PIX Security Appliance.

xi. Click **Send**.

c. Ping the inside host of the peer pod from the internal host. Be sure to coordinate with the peer pod:

```
C:\> ping 192.168.Q.10
Pinging 192.168.Q.10 with 32 bytes of data:
Reply from 192.168.Q.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.Q.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.Q.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.Q.10: bytes=32 time<10ms TTL=125>
```

(where Q = peer pod number)

d. Configure an ACL to allow Web access to the inside host from the outside by completing the following sub-steps:

i. Select **Security Policy** from the **Features** panel.

ii. Click on the **Add New Rule** icon. The **Add Access Rule** window appears..

iii. Verify that **permit** is chosen in the **Select an action** drop-down menu.

iv. Choose **outside** from the **Interface** drop-down menu within the **Source Host/Network** group box.

v. Choose **inside** from the **Interface** drop-down menu within the **Destination Host/Network** group box.

vi. Click the **…** button in the **Destination Host/Network** group box. The **Select host/network** window opens.

vii. Verify that **inside** is chosen in the interface drop-down menu.

viii. Select the IP address of the inside host:

10.0.P.11

(where P = pod number)

ix. Click **OK**. The **Add Access Rule** window becomes active.

x. Select **TCP** in the **Protocol and Service** group box.

xi. Verify that **=** is chosen in the **Service** drop-down menu within the **Source Port** group box.

xii. Verify that **any** appears in the **Service** field within the **Source Port** group box.

xiii. Verify that **=** is chosen in the **Service** drop-down menu within **the Destination Port** group box.

xiv. Click the **…** button within the **Destination Port** group box. The Service window opens.

xv. Choose **http** from the **Service** list.

xvi. Click **OK** to return to the **Add Access Rule** window.

xvii. Click **OK**.

xviii. Click **Apply**. The **Preview CLI Commands** window opens.

xix. Note the ACLs to be sent to the PIX Security Appliance.

xx. Click **Send**.

e. Clear current translations by completing the following sub-steps:

i. Choose **Tools>Command Line Interface**. The **Command Line Interface** window opens.

ii. Enter **clear xlate** in the **Command** field.

iii. Click **Send**.

iv. Verify that the output in the Response field is similar to the following:

```
Result of the command: "clear xlate"
The command has been sent to the device
```

f. View current translations by completing the following sub-steps:

i. Click **Clear Response** in the **Command Line Interface** window.

ii. Enter **show xlate** in the **Command** field.

iii. Click **Send**.

iv. Verify that the output in the Response field is similar to the following:

```
Result of the command: "show xlate"
2 in use, 4 most used
Global 192.168.1.11 Local bastionhost
```



```
Global 192.168.1.10 Local insidehost
```

v. Click **Close** in the **Command Line Interface** window.

g. Test web access to the Student PC.

Option 1: Peer pod groups complete the testing.

i. Open a web browser on the Student PC.

ii. Use the web browser to access the Student PC of the peer pod group:

http://192.168.Q.10 (where Q = peer pod number)

iii. Have a peer pod group test the configuration in the same way.

Option 2: Independent testing – From an Internet PC located on the outside (172.26.26.0/24) network, test access to the Student PC.

i. Open a web browser on the Internet PC.

ii. Use the web browser to access the Student PC:

http://192.168.P.10 (where P = pod number)

iii. If you are using a Windows 2K Superserver, you may need to enter a static route statement using a command prompt on the Superserver:

`C:\> route add 172.26.26.220 mask 255.255.255.255 172.16.P.1`

(where 172.26.26.220 is the Internet PC address)

Lab 9.1.7b Configure Access Through the PIX Security Appliance using CLI

Objective

In this lab exercise, the students will complete the following tasks:

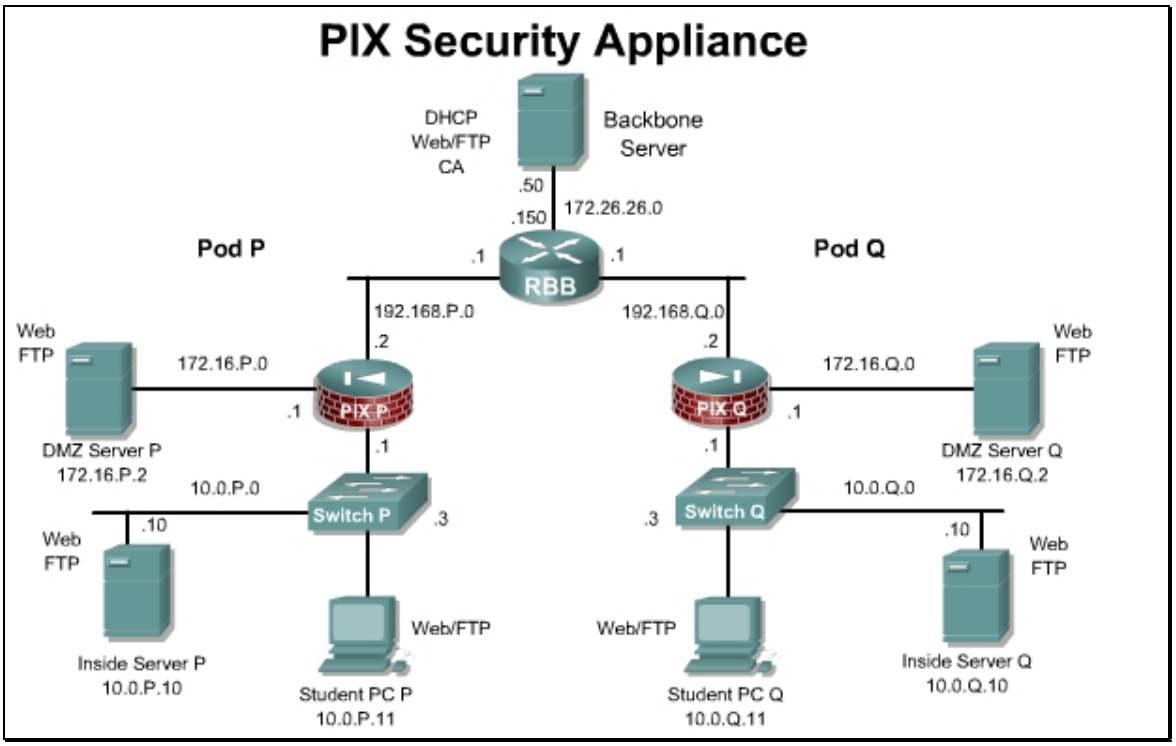
- Configure the PIX Security Appliance to allow inbound traffic to the inside host.
- Configure the PIX Security Appliance to allow inbound traffic to the bastion host.
- Test and verify correct PIX Security Appliance operation.

Scenario

In this exercise, the task is to configure the PIX Security Appliance to protect the internal campus network from outside intruders, while allowing web/ftp access to a DMZ server and web access to one host on the inside.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod PIX Security Appliance. Access the PIX Security Appliance console port using the terminal emulator on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at,

http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_configuration_guides_list.html

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
clear xlate	Clears the contents of the translation slots.
debug icmp trace	Displays information about Internet Control Message Protocol (ICMP) traffic.
global (*mapped_interface*) *nat_id* {*mapped_ip_address* [-*mapped_ip_address*] [**netmask** *mapped_mask*]} | **interface**	Create or delete entries from a pool of global addresses.
show arp	Change or view the arp table, and set the arp timeout value.
show conn	Display connection information.
show xlate	Display current translation and connection slot information.
static (*real_interface*,*mapped_interface*) {*mapped_ip_address*| **interface**} {*real_ip_address* [**netmask** *mask*]} | {**access-list** *access_list_name*} [**dns**] [**norandomseq** [**nailed**]] [[**tcp**] [max_conns [*emb_lim*]] [**udp** *udp_max_conns*]	Configure a persistent one-to-one address translation rule by mapping a local IP address to a global IP address. This is also known as Static port address translation (Static PAT). Configuration mode.

Step 1 Verify the starting configuration

Load the startup configuration or configure the following via CLI.

a. Configure the hostname and domain name.

b. Configure name to address mappings for:

- bastionhost at 172.16.P.2
- insidehost at 10.0.P.11

(Where P = pod number)

c. Configure the inside, outside, and DMZ interface(s).

ii. Give each interface the appropriate IP address and name.

iii. Enable the Ethernet 0, Ethernet 1, and Ethernet 2 interfaces as 100-Mbps full duplex.

iv. Assign all hosts on the inside network to a Network Address Translation (NAT) pool.

v. Define a global pool of IP addresses for inside hosts to use on the outside interface. Use IP addresses 192.168.P.32–192.168.P.253.

vi. Set a default route for all internal hosts to exit the outside interface.

d. Enable ASDM access for the inside host.

e. Test connectivity from the inside to outside using HTTP or FTP.

Step 2 Configure the PIX Security Appliance to Allow Users on the Inside Interface to Access the Bastion Host

Configure the PIX Security Appliance to allow access to the DMZ from the inside network.

a. Assign one pool of IP addresses for hosts on the public DMZ:

```
PixP(config)# global (dmz) 1 172.16.P.32-172.16.P.253 netmask
255.255.255.0
```

(where P = pod number)

c. Clear the translation table so that the global IP address will be updated in the table:

```
PixP(config)# clear xlate
```

d. Write the current configuration to Flash memory:

```
PixP(config)# write memory
```

e. Test connectivity to the bastion host from the PIX.

```
PixP(config)# ping 172.16.P.2
```

(where P = pod number)

f. Test web access to the pod bastion host from the pod PC by completing the following substeps:

i. Open a web browser on the Student PC.

ii. Use the web browser to access the pod bastion host by entering **http://172.16.P.2**.

(where P = pod number)

The home page of the bastion host should appear on the web browser.

g. Use the **show arp**, **show conn**, and **show xlate** commands to observe the transaction:

```
PixP(config)# show arp
outside 192.168.P.1 00e0.1e41.8762
inside insidehost 00e0.b05a.d509
```



```
dmz bastionhost 00e0.1eb1.78df


PixP(config)# show xlate
1 in use, 2 most used
Global 172.16.P.33 Local insidehost
PixP(config)# show conn
2 in use, 2 most used
TCP out bastionhost:80 in insidehost:1076 idle 0:00:07 Bytes 461
flags UIO
TCP out bastionhost:80 in insidehost:1075 idle 0:00:07 Bytes 1441
flags UIO
```

(where P = pod number)

h. Test the FTP access to the bastion host from the PC by completing the following substeps:

i. Establish an FTP session to the bastion host by choosing **Start** > **Run** > **ftp 172.16.P.2**. If the following message appears, this indicates the bastion host has been reached:

```
"Connected to 172.16.P.2."
```

(where P = pod number)

j. Log into the FTP session:

```
User (172.16.P.2(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as
password.
Password: cisco
```

(where P = pod number)

k. Quit the FTP session after connecting and authenticating:

```
ftp> quit
```

Step 3 Configure the PIX Security Appliance to Allow Users on the Outside Interface to Access the Bastion Host

Configure a static translation so that traffic originating from the bastion host always has the same source address on the outside interface of the PIX Security Appliance. Then configure an ACL to allow users on the outside interface to access the bastion host.

a. Create a static translation for the pod bastion host. Use the hostname configured in a previous lab step for the bastion host at 172.16.P.2.

```
PixP(config)# static (dmz,outside) 192.168.P.11 bastionhost
(where P = pod number)
```

b. Configure an ACL to allow users on the outside interface to ping the bastion host.

```
PixP(config)# access-list OUTSIDE_ACCESS_IN permit icmp any any echo
PixP(config)# access-group OUTSIDE_ACCESS_IN in interface outside
```

c. Ping a peer bastion host from the internal host as allowed by the ACL through the static:

```
C:\> ping 192.168.Q.11
```

(where Q = peer pod number)

d. View current static translations:

```
PixP(config)# show xlate
2 in use, 2 most used
Global 172.16.P.34 Local insidehost
Global 192.168.P.11 Local bastionhost
```

(where P = pod number)

e. Test the web access to the bastion hosts of peer pod groups by completing the following substeps. The tests should fail.

i. Open a web browser on the client PC.

ii. Use the web browser to access the bastion host of the peer pod group by entering **http://192.168.Q.11**.

(where Q = peer pod number)

iii. Have a peer pod attempt to access their peer bastion host in the same way.

1. Why did the connection fail?

_____

Answer: There is no access list to allow traffic through the PIX Security Appliance yet.

f. Test the FTP access to the bastion hosts of other pod groups by completing the following substeps. The FTP connection to the peer bastion host should fail.

i. On the FTP client, attempt to get into the bastion host of another pod group by choosing **Start** > **Run** > **ftp 192.168.Q.11**.

(where Q = peer pod number)

ii. Have a peer pod group use FTP to attempt to access their peer bastion host.

g. Configure ACLs to allow web and FTP access to the bastion host from the outside and then test the access. Configure the ACLs to allow TCP traffic from clients on the outside network to access the DMZ bastion host using the previously configured static:

```
PixP(config)# access-list OUTSIDE_ACCESS_IN permit tcp any host
192.168.P.11 eq www
PixP(config)# access-list OUTISDE_ACCESS_IN permit tcp any host
192.168.P.11 eq ftp
```

h. Test web access to the bastion hosts of peer pod groups by completing the following substeps. The test to access the peer pod bastion host should be successful.

i. Open a web browser on the client PC.

ii. Use the web browser to access the bastion host of the peer pod group:

http://192.168.Q.11.

(where Q = peer pod number)

iii. Have a peer pod group test the static and ACL configuration in the same way.

iv. Use the **show arp**, **show conn**, and **show xlate** commands to observe the transaction.

i. Test the FTP access to the bastion hosts of other pod groups by completing the following substeps:

i. On the student PC, use FTP to get into the bastion host of another pod group by choosing **Start** > **Run** > **ftp 192.168.Q.11**.

(where Q = peer pod number)

ii. Have a peer pod group use FTP to get into the bastion host to test the static and ACL configuration.

iii. Use the **show arp**, **show conn**, and **show xlate** commands to observe the transaction.

Step 4 Configure the PIX Security Appliance to Allow Users on the Outside Interface to Access the Inside Host

a. Configure a static translation so that traffic originating from the student PC always has the same source address on the outside interface of the PIX Security Appliance. Then configure an ACL to allow users on the outside interface to access the student PC.

b. Create a static translation from the outside PIX Security Appliance interface to the internal host, and create an ACL to allow web connections from the outside to the PC on the inside:

```
PixP(config)# static (inside,outside) 192.168.P.10 insidehost
```

```
PixP(config)# access-list OUTSIDE_ACCESS_IN permit tcp any host
192.168.P.10 eq www
```

(where P = the pod number)

c. Turn on Internet Control Message Protocol (ICMP) monitoring at the PIX Security Appliance:

```
PixP(config)# debug icmp trace
```

```
debug icmp trace enabled at level 1
```

d. Clear the translation table:

```
PixP(config)# clear xlate
```

e. Ping the static outside address of the peer inside host to test the translation. Observe the source and destination of the packets at the console of the PIX Security Appliance:

```
C:\> ping 192.168.P.1
```

(where Q = peer pod number)

Note the example display for PixP:

```
ICMP echo request (len 72 id 5 seq 0) 10.0.Q.11 > 192.168.P.10
ICMP echo reply (len 72 id 5 seq 0) insidehost > 10.0.Q.11
ICMP echo request (len 72 id 5 seq 1) 10.0.Q.11 > 192.168.P.10
ICMP echo reply (len 72 id 5 seq 1) insidehost > 10.0.Q.11
ICMP echo request (len 72 id 5 seq 2) 10.0.Q.11 > 192.168.P.10
ICMP echo reply (len 72 id 5 seq 2) insidehost > 10.0.Q.11
ICMP echo request (len 72 id 5 seq 3) 10.0.Q.11 > 192.168.P.10
ICMP echo reply (len 72 id 5 seq 3) insidehost > 10.0.Q.11
ICMP echo request (len 72 id 5 seq 4) 10.0.Q.11 > 192.168.P.10
ICMP echo reply (len 72 id 5 seq 4) insidehost > 10.0.Q.11
```

f. Observe the source, destination, and translated addresses on the PIX Security Appliance console.

g. Test web access to a peer pod inside host as allowed by the static and ACL configured in this task by completing the following substeps:

i. Open a web browser on the Student PC.

ii. Use the web browser to access the inside host of the peer pod by entering

http://192.168.Q.10.

(where Q = peer pod number)

h. Turn off the ICMP debugging:

```
PixP(config)#no debug icmp trace
```

i. Write the current configuration to the terminal and verify the previously entered commands are correct. After verifying the configuration, use the **write memory** to save the configuration to Flash memory. The configuration should appear similar to the following:

```
PixP(config)# write terminal
: Saved
:
PIX Version 7.0(1)
names
name 172.16.P.2 bastionhost
name 10.0.P.11 insidehost
!
interface Ethernet0
 speed 100
 nameif outside
 security-level 0
 ip address 192.168.P.2 255.255.255.0
!
interface Ethernet1
 speed 100
 nameif inside
 security-level 100
 ip address 10.0.P.1 255.255.255.0
!
interface Ethernet2
 speed 100
 nameif dmz
 security-level 50
 ip address 172.16.P.1 255.255.255.0
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PixP
domain-name cisco.com
ftp mode passive
access-list OUTSIDE_ACCESS_IN extended permit icmp any any echo
access-list OUTSIDE_ACCESS_IN extended permit tcp any host
192.168.P.11 eq www
```



```
access-list OUTSIDE_ACCESS_IN extended permit tcp any host
192.168.P.11 eq ftp
access-list OUTSIDE_ACCESS_IN extended permit tcp any host
192.168.P.10 eq www
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
monitor-interface outside
monitor-interface inside
monitor-interface dmz
asdm image flash:/asdm
no asdm history enable
arp timeout 14400
global (outside) 1 192.168.P.32-192.168.P.253 netmask 255.255.255.0
global (dmz) 1 172.16.P.32-172.16.P.253 netmask 255.255.255.0
nat (inside) 1 0.0.0.0 0.0.0.0
static (dmz,outside) 192.168.P.11 bastionhost netmask
255.255.255.255
static (inside,outside) 192.168.P.10 insidehost netmask
255.255.255.255
access-group OUTSIDE_ACCESS_IN in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.P.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http insidehost 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 10.0.P.32-10.0.P.253 inside
dhcpd lease 3600
dhcpd ping_timeout 50
dhcpd domain cisco.com
```



```
dhcpd enable inside
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:599d3ee100d62cfb3db8fe1790a77fcb
: end
Pix1(config)#
```


Lab 9.1.7c Configure Multiple Interfaces using CLI – Challenge Lab

Objective

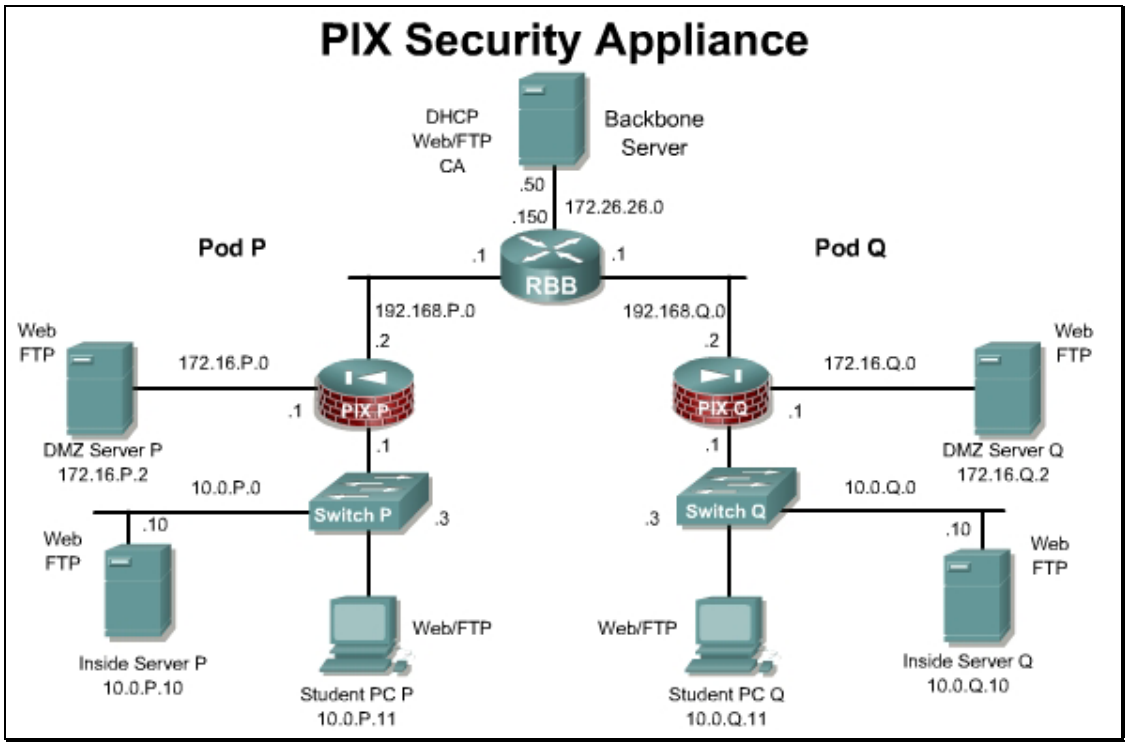
In this lab, the student will complete the following tasks of configuring three PIX interfaces and configure access through the PIX Security Appliance.

Scenario

In this lab, configure the PIX Security Appliance to allow inside and outside hosts to access the services of a web server on the DMZ interface. Review the topology carefully before beginning. In this activity, try to configure the PIX without any configuration notes or command references.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology. Access the PIX Security Appliance console port using the terminal emulator on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_installation_and_configuration_guides_list.html.

Step 1 Configure the PIX Security Appliance

Perform the following steps to configure the PIX Security Appliance:

a. Erase the existing configuration and reload the PIX Security Appliance.

b. Name the PIX Security Appliance **PixP**.

(where P = pod number)

c. Name the appropriate interfaces as inside, outside, and DMZ and assign security levels.

d. Give each interface the appropriate IP address and subnet mask.

e. Enable the Ethernet 0, Ethernet 1, and Ethernet 2 interfaces as 100-Mbps full duplex.

f. Assign all hosts on the inside network to a Network Address Translation (NAT) pool. Define a global pool of IP addresses for inside hosts to use on the outside interface. Use IP addresses 192.168.P.32–192.168.P.253.

g. Set a default route for all internal hosts to exit the outside interface.

h. Assign a name to a single host on the DMZ network. Since this host provides public services that protect the inside network from external connections, call this host 'bastionhost'. This host has an IP address of 172.16.P.2.

i. Allow internal FTP and WWW traffic to reach the DMZ bastion host.

j. Create a static mapping for the DMZ bastion host at 172.16.P.2 to the global IP address 192.168.P.11. Configure an ACL to permit HTTP, ICMP, and FTP traffic to the global IP address.

k. Define a global pool of IP addresses for inside hosts to access the DMZ interface. Here the interface name will be dmz and the range of IP addresses will be 172.16.P.32-172.16.P.253.

l. Test the configuration. FTP and WWW traffic should be able to reach the DMZ bastion host from the peer pod and from the inside host.

m. Use the **show** commands to verify operation:

What **show** commands are useful to verify configuration and operation?

_____

_____

_____

Answer: Answers will very. Examples: **show access-list, show run** (produces the same output as write terminal), **show conn, show xlate**

Lab 9.1.9 Configure ACLs in the PIX Security Appliance using CLI

Objective

In this lab exercise, the students will complete the following tasks:

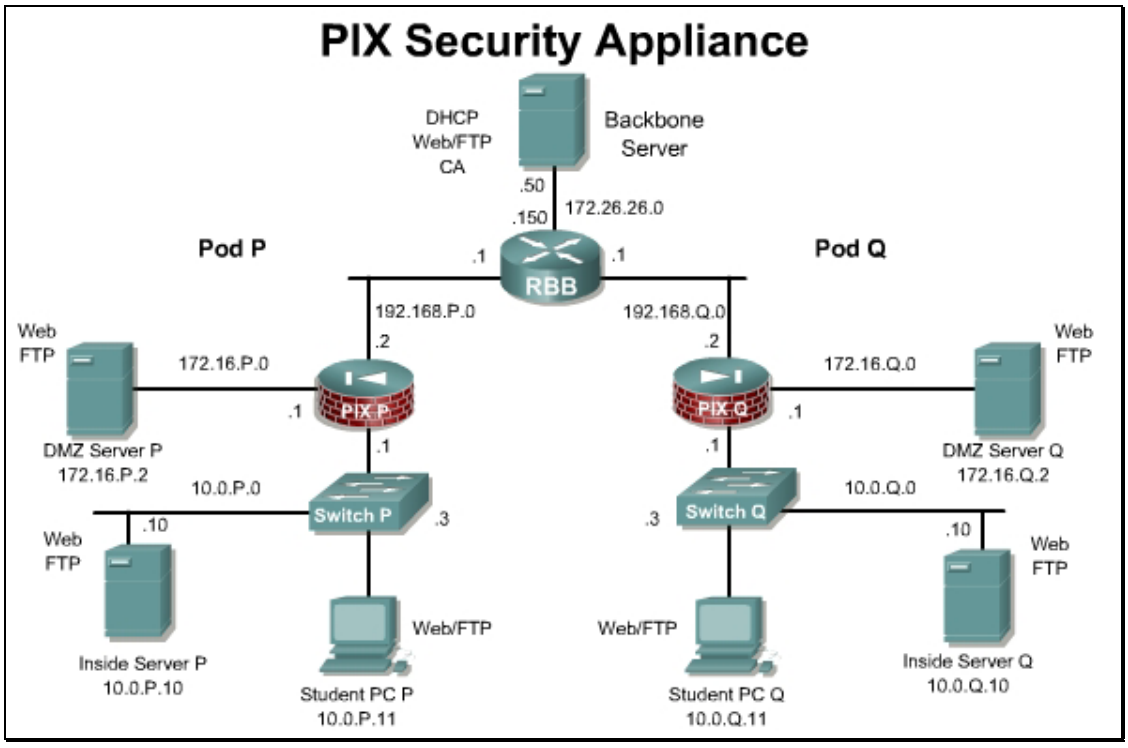
- Disable pinging to an interface.
- Configure inbound and outbound access control lists (ACLs).
- Configure malicious active code filtering.

Scenario

Company XYZ has purchase and installed a PIX Security Appliance on the network. By default, the PIX does not allow any traffic from a lower security interface to a higher security interface. In order for hosts on a higher security interface to be accessed from a lower security interface, access control lists must be configured on the PIX.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod PIX Security Appliance. Access the PIX Security Appliance console port using the terminal emulator on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_installation_and_configuration_guides_list.html.

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {**host** *source-ip* | *source-ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id* | **any**} {**host** *destination-ip* | *destination-ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]	Command used to configure an access list.
clear configure icmp	Removes **icmp** command statements from the configuration.
filter activex {[*port***[-***port***] | except }** *local_ip local_mask foreign_ip foreign_mask***]**	Block outbound ActiveX, Java applets, and other HTML <object> tags from outbound packets.
filter java {[*port***[-***port***] | except }** *local_ip local_mask foreign_ip foreign_mask***]**	Specifies to filter out Java applets returning from an outbound connection.
icmp {permit | deny} *ip_address net_mask* **[***icmp_type***]** *if_name*	Enables or disables the ability to ping a PIX Security Appliance interface.
show running-config access-list	Displays the configured access lists.
show running-config filter	Displays URL, Java, and ActiveX filtering configurations.

Command	Description
url-server [**(***if_name***)**] **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]	Command used to define Websense filtering.

Step 1 Disable Pinging to an Interface

Perform the following lab steps to configure an ICMP ACL to prevent pinging to the PIX Security Appliance interfaces:

a. Ping the inside interface of the PIX Security Appliance from the inside host:

```
C:\>ping 10.0.P.1
Pinging 10.0.P.1 with 32 bytes of data:
Reply from 10.0.P.1: bytes=32 time<10ms TTL=128
Reply from 10.0.P.1: bytes=32 time<10ms TTL=128
Reply from 10.0.P.1: bytes=32 time<10ms TTL=128
Reply from 10.0.P.1: bytes=32 time<10ms TTL=128
```

(where P = pod number)

b. Ping the outside interface from the inside host. By default, pinging through the PIX Security Appliance to a PIX Security Appliance interface is not allowed:

```
C:\>ping 192.168.P.2
Pinging 192.168.P.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

(where P = pod number)

c. Use the **icmp** command to prevent pinging the inside interface:

```
PixP(config)# icmp deny any echo inside
```

1. Why would this command be used in a production network?

_____

Answer: To prevent inside users from pinging the firewall, limiting the amount of information that can be gathered by a potential attacker.

d. View the ICMP ACL:

```
PixP(config)# show running-config icmp
icmp deny any echo inside
```

e. Ping the inside PIX Security Appliance interface from the inside host. The ICMP ACL causes the ping to fail:

```
C:\>ping 10.0.P.1
Pinging 10.0.P.1 with 32 bytes of data:
Request timed out.
```



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

(where P = pod number)

f. Enable pinging to the PIX Security Appliance inside interface:

```
PixP(config)# clear configure icmp
```

g. Verify that the ICMP ACL is removed by pinging the inside interface of the PIX Security Appliance:

```
C:\>ping 10.0.P.1
Pinging 10.0.P.1 with 32 bytes of data:
Reply from 10.0.P.1: bytes=32 time<10ms TTL=128
Reply from 10.0.P.1: bytes=32 time<10ms TTL=128
Reply from 10.0.P.1: bytes=32 time<10ms TTL=128
Reply from 10.0.P.1: bytes=32 time<10ms TTL=128
```

(where P = pod number)

Step 2 Configure Inbound ACLs

Perform the following steps to configure ACLs:

a. Configure the following statics for the pod bastion host and the pod inside host:

```
pixP(config)# static (dmz,outside) 192.168.P.11 bastionhost netmask
255.255.255.255
pixP(config)# static (inside,outside) 192.168.P.10 insidehost
netmask 255.255.255.255
```

(where P = pod number)

b. Test web access to the bastion host of the peer pod. The peer bastion host should not be accessible by HTTP at this point.

i. Open a web browser on the student PC.

ii. Use the web browser to access the bastion host of the peer pod by entering:

http://192.168.Q.11.

(where Q = peer pod number)

c. Test FTP access to the bastion host of peer pod. The peer bastion host should not be accessible by FTP at this point. Attempt to access the bastion host of another pod group using FTP:

Start > Run > ftp 192.168.Q.11

(where Q = peer pod number)

d. Create an ACL to permit inbound HTTTP and FTP access to the bastion host from the peer outside network:

```
pixP(config)# access-list ACLIN permit tcp 192.168.Q.0 255.255.255.0
host 192.168.P.11 eq www
pixP(config)# access-list ACLIN permit tcp host 192.168.Q.10 host
192.168.P.11 eq ftp
```

(where P = pod number, Q = peer pod number)

1. What command would be used to allow access to a mail server running on the bastion host?

   _____

   Answer: **access-list ACLIN permit tcp 192.168.Q.0 255.255.255.0 host 192.168.P.11 eq smtp**

e. Add commands to permit inbound web traffic to the inside host, permit inbound pings, permit icmp echo replies to the inside host, and deny all other traffic from the Internet:

```
pixP(config)# access-list ACLIN permit tcp any host 192.168.P.10 eq www
pixP(config)# access-list ACLIN permit icmp any any echo
pixP(config)# access-list ACLIN permit icmp any host 192.168.P.10 echo-reply
pixP(config)# access-list ACLIN deny ip any any
```

   (where P = pod number)

f. Bind the ACL to the outside interface:

```
pixP(config)# access-group ACLIN in interface outside
```

g. Create an access-list to allow icmp echo-replies from the bastion host:

```
pixP(config)# access-list ICMPDMZ permit icmp host bastionhost any echo-reply
```

h. Bind the new ACL to the dmz interface:

```
pixP(config)# access-group ICMPDMZ in interface dmz
```

i. Display the access-list configuration. Use the **show running-config access-list** command to display the configuration only, with no line numbers or hit counts

```
pixP(config)# show running-config access-list
access-list ACLIN extended permit tcp 192.168.Q.0 255.255.255.0 host 192.168.P.11 eq www
access-list ACLIN extended permit tcp host 192.168.Q.10 host 192.168.P.11 eq ftp
access-list ACLIN extended permit tcp any host 192.168.P.10 eq www
access-list ACLIN extended permit icmp any any echo
access-list ACLIN extended permit icmp any host 192.168.P.10 echo-reply
access-list ACLIN extended deny ip any any
access-list icmpdmz extended permit icmp host bastionhost any echo-reply
```

   (where P = pod number, Q = peer pod number)

j. Use the **show access-list** command to display the access list and observe the hit counts and line numbers:

```
pixP(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (denyflow- max 4096)       alert-interval 300
access-list ACLIN; 6 elements
access-list ACLIN line 1 extended permit tcp 192.168.Q.0 255.255.255.0 host 192.168.P.11 eq www (hitcnt=0)
```



```
access-list ACLIN line 2 extended permit tcp host 192.168.Q.10 host
192.168.P.11 eq ftp

(hitcnt=0)

access-list ACLIN line 3 extended permit tcp any host 192.168.P.10
eq www (hitcnt=0)

access-list ACLIN line 4 extended permit icmp any any echo
(hitcnt=0)

access-list ACLIN line 5 extended permit icmp any host

192.168.6.10 echo-reply (hitcnt=0)

access-list ACLIN line 6 extended deny ip any any (hitcnt=0)

access-list icmpdmz; 1 elements

access-list icmpdmz line 1 extended permit icmp host bastionhost any
echo-reply (hitcnt=0)
```

(where P = pod number, Q = peer pod number)

Step 3 Test and Verify the Inbound ACLs

Perform the following steps to test the inbound ACL:

a. Have a peer inside host ping the inside host:

```
C:\>ping 192.168.Q.10

Pinging 192.168.Q.10 with 32 bytes of data:

Reply from 192.168.Q.10: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.10: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.10: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.10: bytes=32 time<10ms TTL=128
```

(where Q = peer pod number)

b. Have a peer inside host ping the bastion host:

```
C:\>ping 192.168.Q.11

Pinging 192.168.Q.11 with 32 bytes of data:

Reply from 192.168.Q.11: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.11: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.11: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.11: bytes=32 time<10ms TTL=128
```

(where Q = peer pod number)

c. Ping the bastion host from the student PC:

```
C:\>ping 172.16.P.2

Pinging 172.16.P.2 with 32 bytes of data:

Reply from 172.16.P.2: bytes=32 time<10ms TTL=128

Reply from 172.16.P.2: bytes=32 time<10ms TTL=128

Reply from 172.16.P.2: bytes=32 time<10ms TTL=128

Reply from 172.16.P.2: bytes=32 time<10ms TTL=128
```

(where P = pod number)

d. Ping the Backbone server from the student PC:

```
C:\>ping 172.26.26.50

Pinging 172.26.26.50 with 32 bytes of data:

Reply from 172.26.26.50: bytes=32 time<10ms TTL=128

Reply from 172.26.26.50: bytes=32 time<10ms TTL=128

Reply from 172.26.26.50: bytes=32 time<10ms TTL=128

Reply from 172.26.26.50: bytes=32 time<10ms TTL=128
```

e. Test web access to the bastion hosts of peer pod groups by completing the following substeps. The web request should be successful when accessing the peer bastion host via its static mapping:

   i. Open a web browser on the student PC.

   ii. Use the web browser to access the bastion host of the peer pod group by entering: **http://192.168.Q.11**.

   (where Q = peer pod number)

   iii. Have a peer pod group attempt to access the bastion host in the same way.

f. Test web access to the inside hosts of peer pod groups by completing the following substeps. Access to the IP address of the static mapped to the inside host of the opposite pod group should be successful:

   i. Open a web browser on the client PC.

   ii. Use the web browser to access the inside host of the peer pod group by entering: **http://192.168.Q.10**.

   (where Q = peer pod number)

   iii. Have a peer pod group attempt to access the inside host in the same way.

g. Test FTP access to the bastion hosts of peer pod groups by completing the following substeps. Access to the peer bastion host via FTP should be successful:

   i. Using FTP, attempt to access the bastion host of a peer pod group:

   Start > **Run** > **ftp 192.168.Q.11**.

   (where Q = peer pod number)

   ii. Have a peer pod group use FTP to attempt to access their peer bastion host.

   1. Were any of the above steps unsuccessful? Why?

   _____

   _____

   Answer: The attempts should be successful, because they are permitted by the ACL statements.

h. Display the access lists again and observe the hit counts:

```
PixP(config)# show access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max
4096)       alert-interval 300

access-list ACLIN; 6 elements

access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.P.11 eq www(hitcnt=2)

access-list ACLIN line 2 extended permit tcp host 192.168.Q.10 host
192.168.P.11 eq ftp (hitcnt=0)
```



```
access-list ACLIN line 3 extended permit tcp any host 192.168.P.10
eq www (hitcnt=2)

access-list ACLIN line 4 extended permit icmp any any echo
(hitcnt=20)

access-list ACLIN line 5 extended permit icmp any host 192.168.P.10
echo-reply (hitcnt=12)

access-list ACLIN line 6 extended deny ip any any (hitcnt=0)

access-list ICMPDMZ; 1 elements

access-list ICMPDMZ line 1 extended permit icmp host bastionhost any
echo-reply (hitcnt=12)
```

(where P = pod number, Q = peer pod number)

Step 4 Configure an Outbound ACL

Perform the following lab steps to configure ACLs:

- Deny outbound web traffic.
- Allow outbound FTP traffic from the internal network to 172.26.26.50.

a. Test web access to the Internet by completing the following substeps. The test to access 172.26.26.50 should be successful:

   i. Open a web browser on the student PC.

   ii. Use the web browser to access Internet host 172.26.26.50 by entering:

   http://172.26.26.50.

b. Test FTP access to Internet host 172.26.26.50. Access to the host 172.26.26.50 via FTP should be successful:

   On the FTP client, attempt to access host 172.26.26.50:

   Start>Run>ftp 172.26.26.50

c. Create an ACL that prevents users on the internal network from making outbound HTTP connections:

```
PixP(config)# access-list ACLOUT deny tcp any any eq www
```

   This access list prevents all outbound connections.

d. Enter the **access-group** command to create an access group that will bind the ACL to an interface:

```
PixP(config)# access-group ACLOUT in interface inside
```

e. Display the configured access lists, and observe the hit count:

```
PixP(config)# show access-list

access-list ACLIN; 6 elements

access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.P.11 eq www(hitcnt=4)

access-list ACLIN line 2 extended permit tcp host 192.168.Q.10 host
192.168.P.11 eq ftp (hitcnt=1)

access-list ACLIN line 3 extended permit tcp any host 192.168.P.10
eq www (hitcnt=4)

access-list ACLIN line 3 extended permit icmp any any echo
(hitcnt=20)
```



```
access-list ACLIN line 5 extended permit icmp any host 192.168.P.10
echo-reply (hitcnt=12)

access-list ACLIN line 6 extended deny ip any any (hitcnt=0)

access-list ICMPDMZ; 1 elements

access-list ICMPDMZ line 1 extended permit icmp host bastionhost any
echo-reply (hitcnt=12)

access-list ACLOUT; 1 elements

access-list ACLOUT line 1 extended deny tcp any any eq www
(hitcnt=0)
```

(where P = pod number, Q = peer pod number)

f. Test web access to the Internet by completing the following substeps. The test via HTTP should fail.

   i. Open a web browser on the student PC.

   ii. Use the web browser to access the Internet by entering:

   http://172.26.26.50.

g. Test FTP access to an Internet host. The FTP connection should fail as well due to the implicit deny any:

   On the FTP client, attempt to access host 172.26.26.50:

   Start>Run>ftp 172.26.26.50

h. Display the access list again and note that the hit count has incremented:

```
PixP(config)# show access-list

access-list ACLIN; 6 elements

access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.P.11 eq www (hitcnt=4)

access-list ACLIN line 2 extended permit tcp host 192.168.Q.10 host
192.168.P.11 eq ftp (hitcnt=1)

access-list ACLIN line 3 extended permit tcp any host 192.168.P.10
eq www (hitcnt=4)

access-list ACLIN line 4 extended permit icmp any any echo
(hitcnt=20)

access-list ACLIN line 5 extended permit icmp any host 192.168.P.10
echo-reply (hitcnt=12)

access-list ACLIN line 6 extended deny ip any any (hitcnt=0)

access-list ICMPDMZ; 1 elements

access-list ICMPDMZ line 1 extended permit icmp host bastionhost any
echo-reply (hitcnt=12)

access-list ACLOUT; 1 elements

access-list ACLOUT line 1 extended deny tcp any any eq www
(hitcnt=3)
```

   (where P = pod number, Q = peer pod number)

i. Add an additional command to the ACL to permit outbound FTP access to host 172.26.26.50:

```
PixP(config)# access-list ACLOUT permit tcp 10.0.P.0 255.255.255.0
host 172.26.26.50 eq ftp
```

   (where P = pod number)

j. Add another access list command statement to deny other outbound IP traffic:

```
PixP(config)# access-list ACLOUT deny ip any any
```

This access list statement is only needed to enable viewing of the hit counts.

k. View the access list again:

```
PixP(config)# show access-list ACLOUT
access-list ACLOUT; 3 elements
access-list ACLOUT line 1 extended deny tcp any any eq www
(hitcnt=3)
access-list ACLOUT line 2 extended permit tcp 10.0.P.0 255.255.255.0
host 172.26.26.50 eq ftp (hitcnt=0)
access-list ACLOUT line 3 extended deny ip any any (hitcnt=0)
```

(where P = pod number)

Step 5 Test and Verify the Outbound ACL

Perform the following steps to test the outbound ACL:

a. Test web access to the Internet by completing the following substeps. Access to the Internet host will fail due to the deny ACL:

i. Open a web browser on the student PC.

ii. Use the web browser to attempt to access the Internet by entering:

http://172.26.26.50.

b. Test FTP access to an Internet host by performing the following on the FTP client. At this point, a connection using FTP will work:

Start>Run>ftp 172.26.26.50

c. Test the FTP access to a peer pod bastion host by attempting to access the peer pod bastion host on the FTP client. The connection using FTP should fail:

Start>Run>ftp 192.168.Q.11

(where Q = peer pod number)

d. View the outbound access list again and observe the hit counts:

```
PixP(config)# show access-list ACLOUT
access-list ACLOUT line 1 extended deny tcp any any eq www
(hitcnt=2)
access-list ACLOUT line 2 extended permit tcp 10.0.P.0 255.255.255.0
host 172.26.26.50 eq ftp (hitcnt=1)
access-list ACLOUT line 3 extended deny ip any any (hitcnt=3)
```

(where P = pod number)

Be sure to enter the following command exactly as shown. If the ACL name is omitted all access list statements are removed.

e. Remove the outbound ACL:

```
PixP(config)# clear configure access-list ACLOUT
```

f. Verify that the outbound ACL has been removed:

```
PixP(config)# show access-list
access-list ACLIN; 6 elements
```



```
access-list ACLIN permit tcp 192.168.Q.0 255.255.255.0 host
192.168.P.11 eq www(hitcnt=4)

access-list ACLIN permit tcp host 192.168.Q.10 host 192.168.P.11 eq
ftp (hitcnt= 1)

access-list ACLIN permit tcp any host 192.168.P.10 eq www (hitcnt=4)

access-list ACLIN permit icmp any any echo (hitcnt=20)

access-list ACLIN permit icmp any host 192.168.P.10 echo-reply
(hitcnt=12)

access-list ACLIN deny ip any any (hitcnt=0)

access-list ICMPDMZ; 1 elements

access-list ICMPDMZ permit icmp host bastionhost any echo-reply
(hitcnt=12)
```

(where P = pod number, Q = peer pod number)

g. View the access groups:

```
PixP(config)# show running-config access-group

access-group ACLIN in interface outside

access-group ICMPDMZ in interface dmz

pixP(config)#
```

Save the configuration:

```
PixP(config)# write memory
```

Step 6 Filter Malicious Active Code

Perform the following lab steps to configure ActiveX and filter Java.

Note If the ActiveX and Java applets are not working properly, the security settings in the web browser may need to be adjusted to allow these applets to run. The Java Virtual Machine must be running for the Java Applet to run. Also, any popup blockers that are running on the student PCs must be disabled, as the links for the applets on the pod homepage will launch the applets in a new window.

---

a. Enter **http://192.168.Q.10** in the web browser. After the peer pods homepage appears, click on the **ActiveX Control** link. The ActiveX Control should open successfully.

Did the ActiveX Control open successfully?

_____

Answer: Yes.

b. On the PIX Security Appliance, enter the **filter activex** command to block ActiveX from any local host and for connections to any foreign host on port 80:

```
PixP(config)# filter activex 80 0 0 0 0
```

a. What is the significance of 0 0 0 0?

_____

Answer: It is a shortcut representing 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0.

c. Open a new web browser and enter **http:192.168.Q.10**. After the webpage opens, click on the **ActiveX Control** link. The ActiveX Control should not open successfully.
Note: It might be necessary to clear the web browser cache. In Internet Explorer, go to **Tools > Internet Options….** and click the **Delete Files** button in the **Temporary Internet files** area.

Did the ActiveX Control open successfully?

_____

Answer: No.

d. Enter **http://192.168.Q.10** in the web browser. After the peer pods homepage appears, click on the **Java Applet** link. The Java Applet should open successfully.

Did the Java Applet open successfully?

_____

Answer: Yes.

e. Enter the **filter java** command to block Java applets:

```
PixP(config)# filter java 80 0 0 0 0
```

f. Open a new web browser and enter **http:192.168.Q.10**. After the webpage opens, click on the **Java Applet** link. The Java Applet should not open successfully.
Note: It might be necessary to clear the web browser cache.

Did the Java Applet open successfully?

_____

Answer: No.

g. Use the following command to show the filters:

```
PixP(config)# show running-config filter
filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

Step 7 Configure the PIX Security Appliance to Work with a URL Filtering Server

Perform the following steps to configure the PIX Security Appliance to work with a URL-filtering server:

a. Enter the **url-server** command to designate the URL-filtering server:

```
PixP(config)# url-server (inside) host 10.0.P.11 timeout 30 protocol
TCP version 4
```

b. Show the designated url-server by entering the following command:

```
PixP(config)# show running-config url-server
url-server (inside) vendor websense host insidehost timeout 30
protocol TCP version 4 connections 5
```

c. Enter the **filter url http** command to prevent outbound users from accessing WWW URLs that are designated with the filtering application:

```
PixP(config)# filter url http 0 0 0 0 allow
```

d. Display the **filter url http** command by using the following command:

```
PixP(config)# show running-config filter
filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 allow
```

e. Remove the **filter** commands from the configuration:

```
PixP(config)# clear configure filter
```


f. Remove the **url-server** command:

```
PixP(config)# no url-server (inside) host insidehost
```

(where P = the pod number)

g. Save the configuration:

```
PixP(config)# write memory
```

Step 8 Download, Install, and Configure a URL Filtering Server (OPTIONAL)

If time permits, download, install, and configure a web filtering server. A Cisco IOS Firewall is also able to interoperate with Websense and N2H2 servers to provide web filtering.

Websense

http://www.websense.com/downloads/

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a00801e4197.shtml

N2H2

http://www.n2h2.com/products/bess.php?device=pix

Lab 9.2.3 Configure Service Object Groups using ASDM

Objective

In this lab, the students will complete the following tasks:

- Configure an inbound access control list (ACL) with object groups.
- Configure a service object group.
- Configure web and ICMP access to the inside host.
- Test and verify the inbound ACL.

Scenario

The XYZ Company has a PIX Security Appliance installed and operating on the network. The existing configuration on the PIX uses ACL statements for each individual service, such as HTTP or FTP. Using ASDM, configure a service object group to make the access rules more modular and scalable.

PIX Firewall Version 6.2 and higher support four types of named object groups:

- host/network (network)
- protocol
- icmp-type
- service

When configuring object groups with ASDM, use the following guidelines:

Object Group Names—The Name of any object group must be unique to all four types. For example, a service group and a network group may not share the same name.

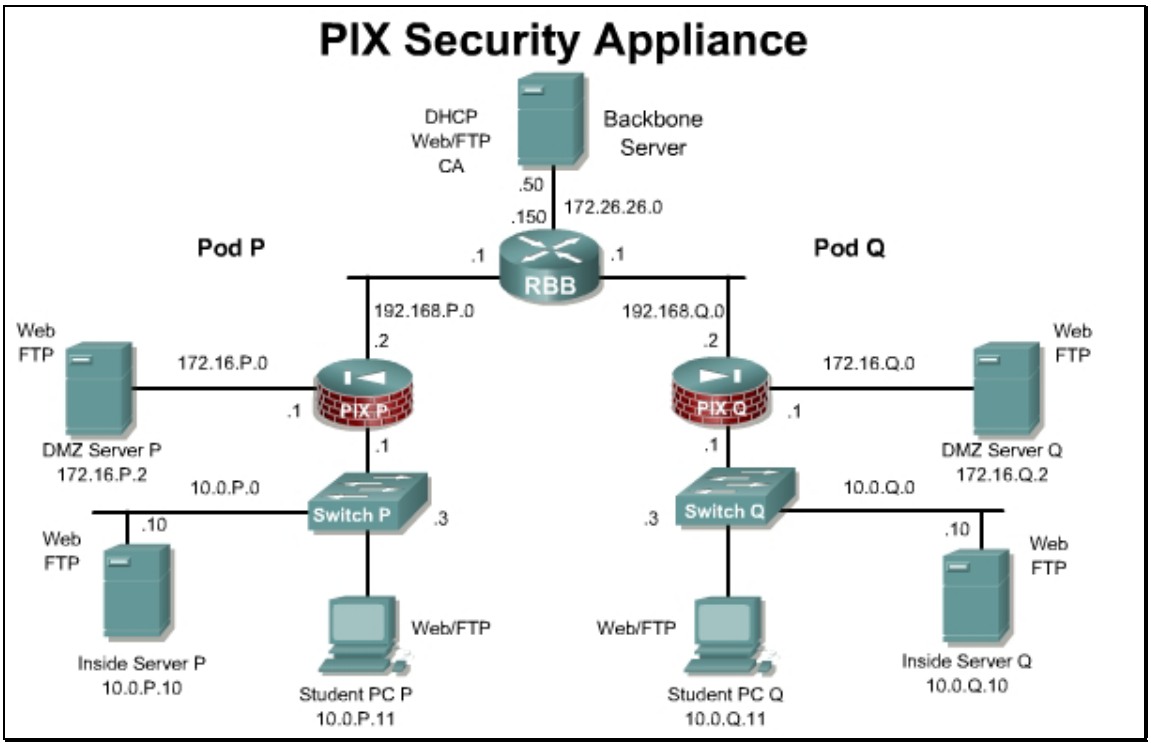
Host/Network and Service Types—ASDM uses Host/Network and service type objects. You can add, edit or delete network type object groups in **Configuration>Hosts/Networks>Group** and service type object groups in **Tools>Service Groups**, **Configuration>VPN**, and **Configuration>Access Rules**.

ICMP and Protocol Types—The object group types icmp-type and protocol cannot be created in ASDM and, therefore, cannot be renamed in ASDM. However, ASDM does support editing and deleting object groups using **Tools>Command Line Interface**.

Hierarchical/Nested Service Groups—Manage Service Groups lets you associate multiple TCP or UDP services (ports) in a named group. You can also add service object groups to a service object group. You might find this useful when the use of groups is hierarchical or to reuse existing service groups. You can then use the nested service group like any other group in an access rule, a conduit, or for IPSec rules. Nested network groups are not supported by ASDM.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod PIX Security Appliance. Access the PIX Security Appliance console port using the terminal emulator on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at:

http://www.cisco.com/go/ASDM

Step 1 Remove the Existing ACLs and using ASDM

In this step, verify and then remove the existing ACLs.

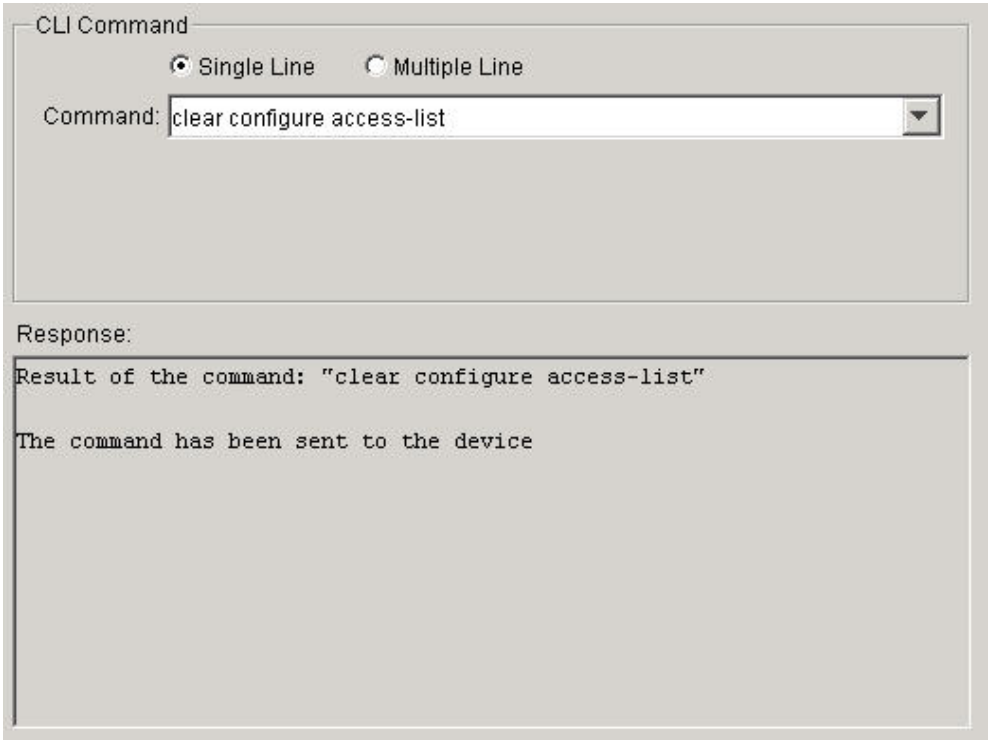
a. Log into ASDM.

b. Click on the **Configuration** button

c. Click on **Security Policy** in the Features panel. Verify that the **Access Rules** radio button is checked.

d. From the Menu, go to **Tools>Command Line Interface**.

e. Delete any existing ACL entries by entering the **`clear configure access-list`** command.

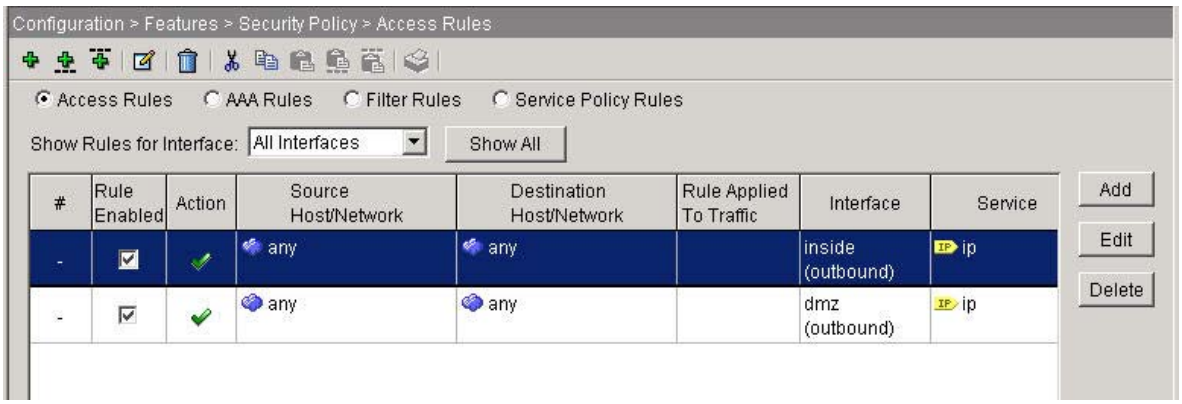


f. Click the **Send** Button.

g. Click the **Close** button to return to the **Access Rules** page in the Configuration.

h. If the **Confirm Configuration Refresh** window appears, click the **Yes** button to refresh the configuration shown in the ASDM interface.

i. There should only be 2 implicit rules remaining on the **Access Rules** page.

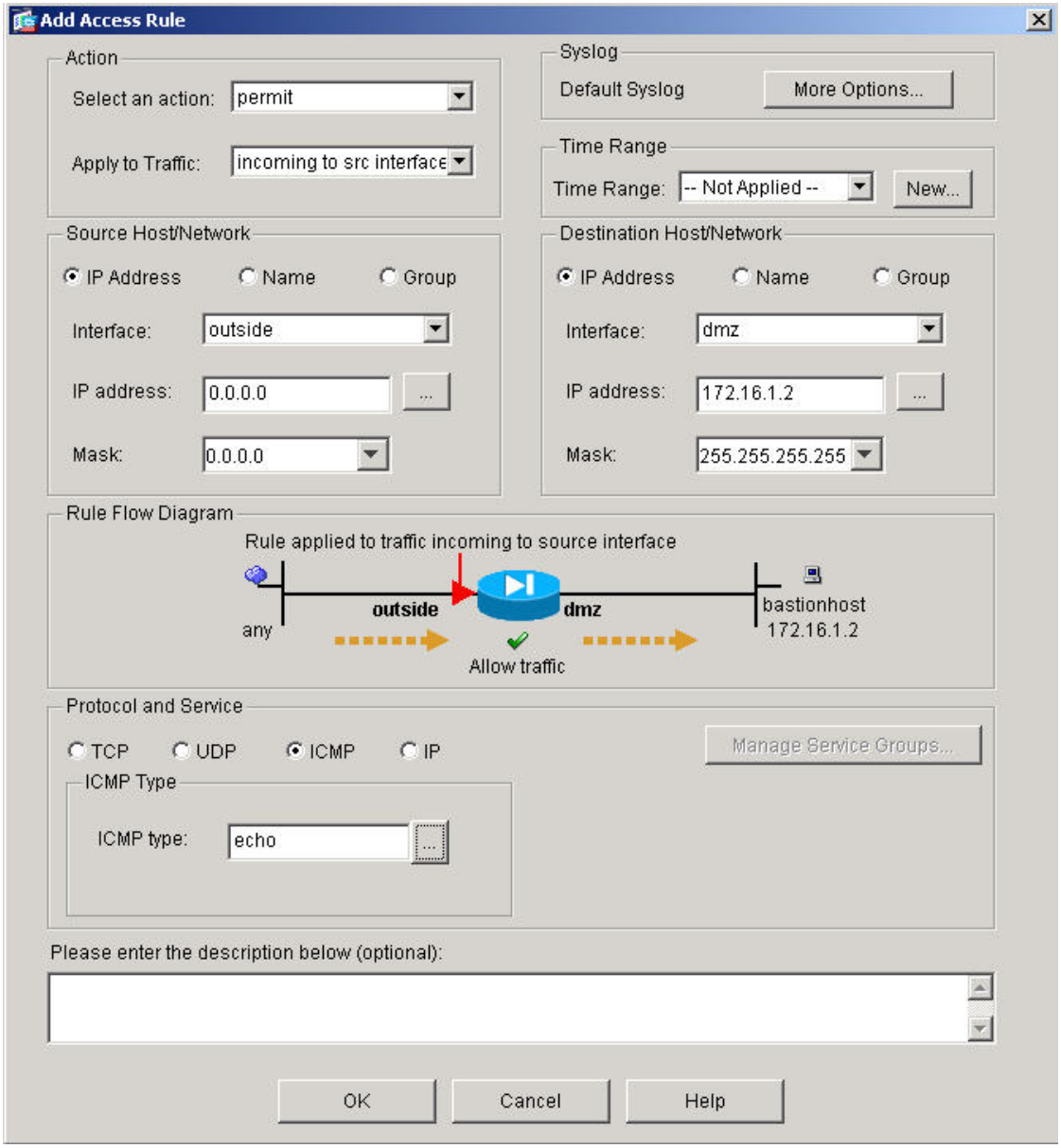


Step 2 Allow ICMP, HTTP and FTP from the Outside to the DMZ

Complete the following steps to permit inbound web and ICMP traffic to the bastion host:

a. From the Access Rules page, click on the **Add New Rule** icon or the **Add** button.

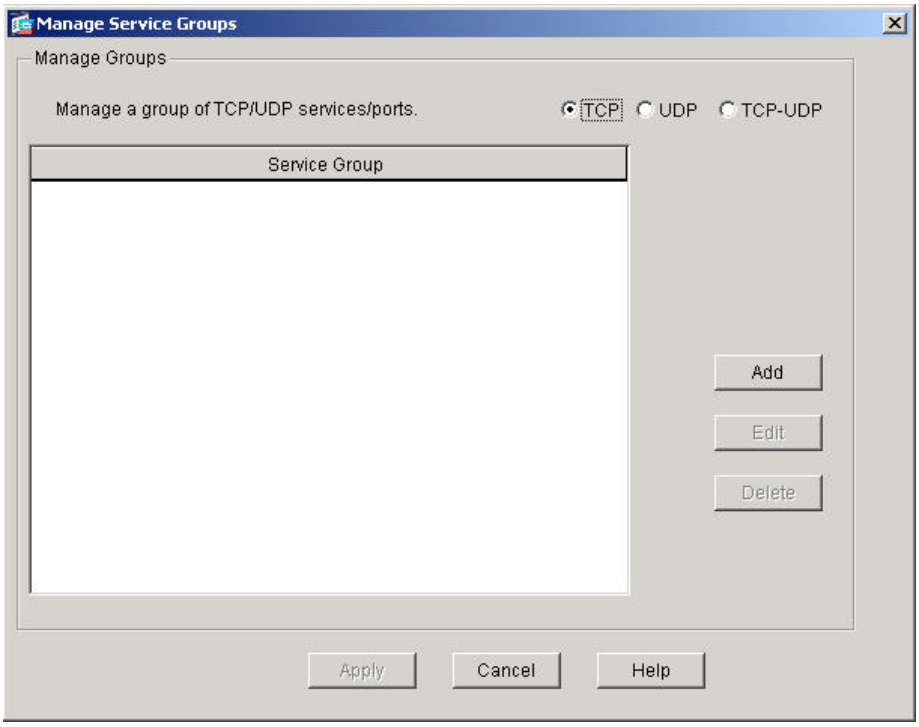
b. Create an Access Rule which permits ICMP echo traffic from the outside to the Bastionhost. Click the **OK** button when finished.



c. Click the **Add New Rule** icon.

d. Create a permit statement to permit traffic with a source of outside (ANY) and the destination of DMZ (bastionhost)

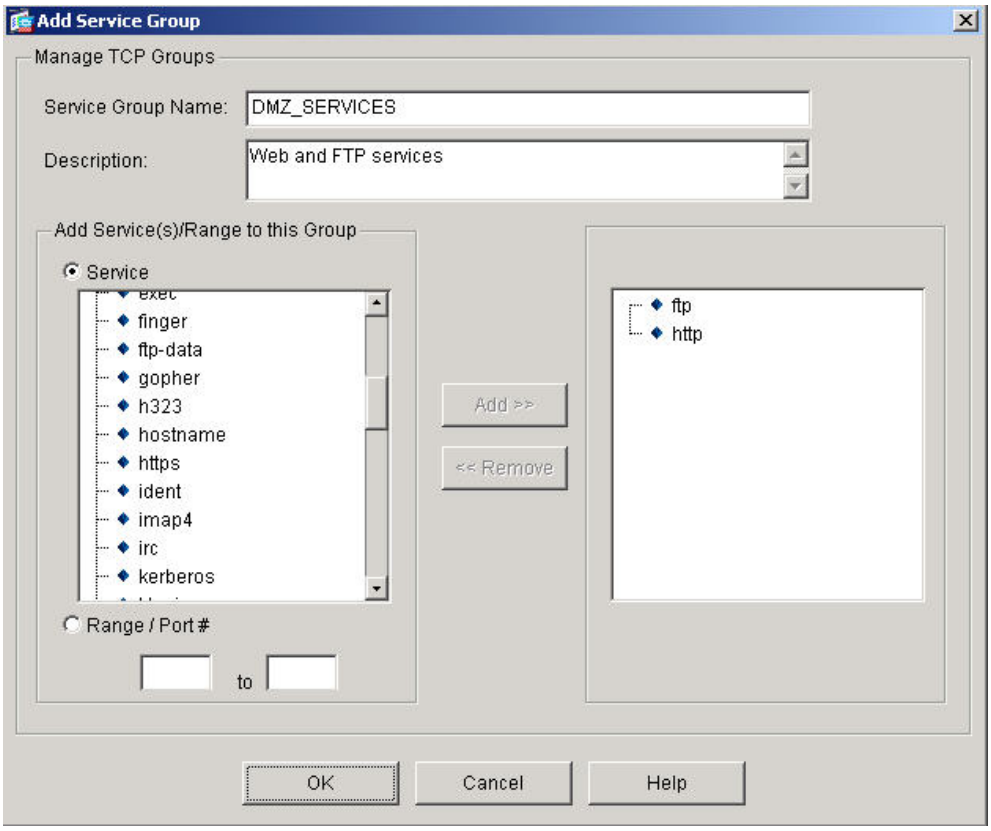
e. Click on the **Manage Service Groups** button. The Manage Service Groups window will appear.



f. Make sure the TCP radio button is checked.

g. Click on the **Add** button. The **Add Service Group** window appears.

h. Enter a Service group name of **DMZ_SERVICES** and a description of **Web and FTP services**.

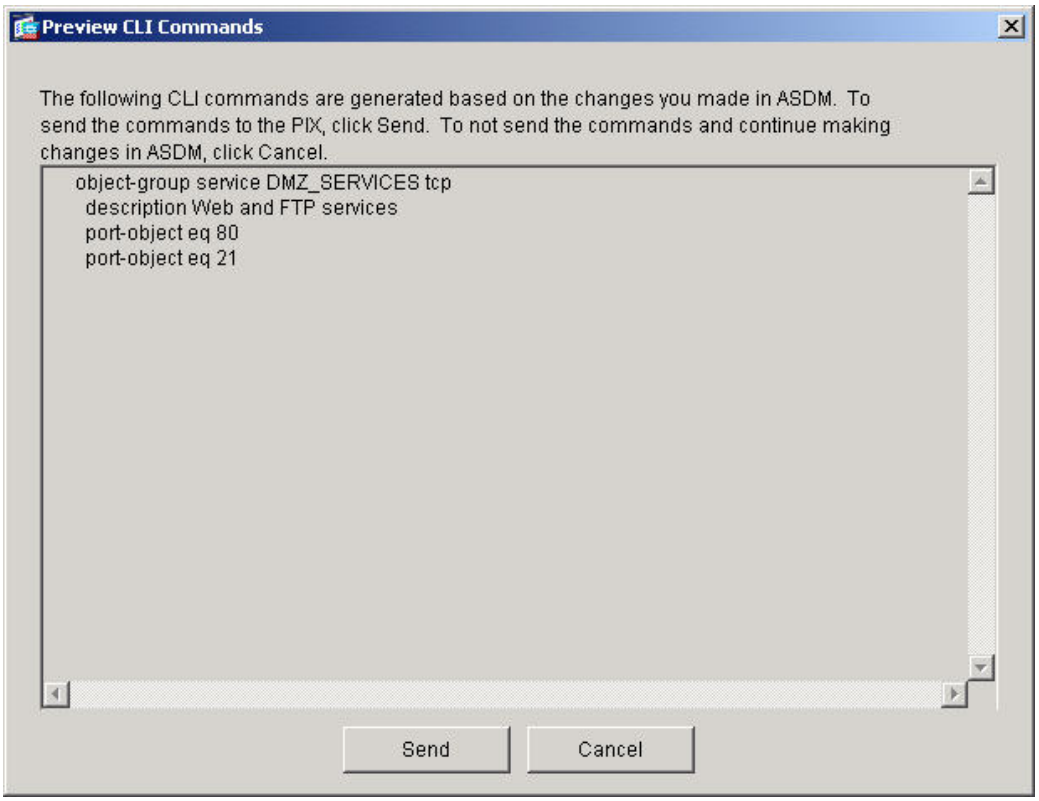


i. Add ftp and http to the Services list on the right by clicking on each Service and click on the **Add** button.

j. Click the **OK** button, returning to the **Manage Service Groups** window

k. Click on the **Apply** button.

l. If prompted by the Preview CLI Commands window, click on the **Send** button.



m. The **Add Access Rule** window will become active.

n. In the Destination Port field, click on the **Service Group** radio button.

o. Choose **DMZ_SERVICES** in the drop down list.

p. Enter a description at the bottom. **Web and FTP access to the Bastionhost**

q. Click **OK**, returning to the Access Rules window.

r. Click on the **Apply** button.

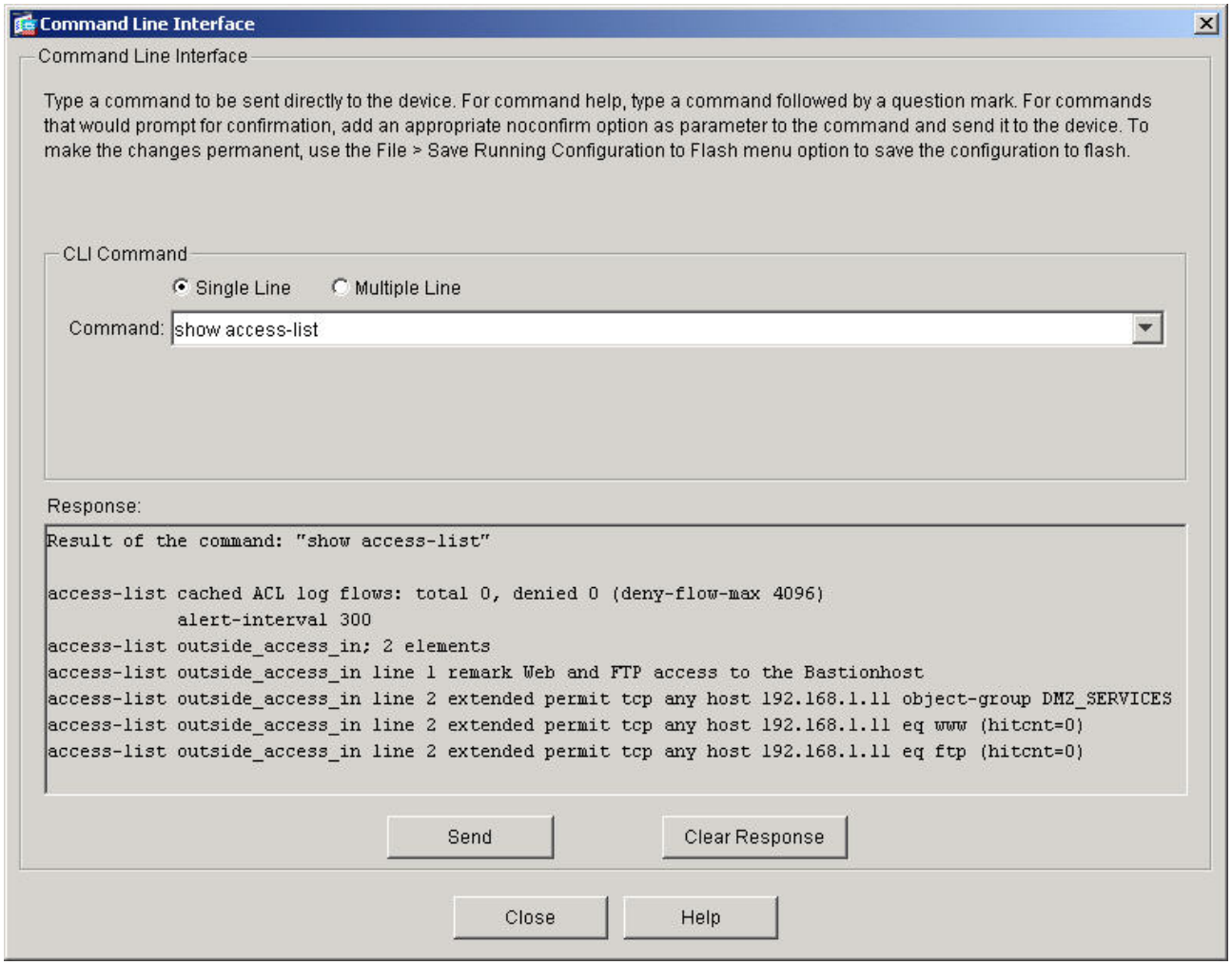
s. If prompted by the Preview CLI Commands window, click on the **Send** button.

Step 3 Verify the ACLs

Verify the configuration:

a. From the Menu, go to **Tools>Command Line Interface**

b. View the ACL entries by entering the **`show access-list`** command. Click the **Send** Button.



c. Click the **Close** button when finished.

d. Exit ASDM.

Lab 9.2.5 Configure Object Groups and Nested Object Groups using CLI

Objective

In this lab, the students will complete the following tasks:

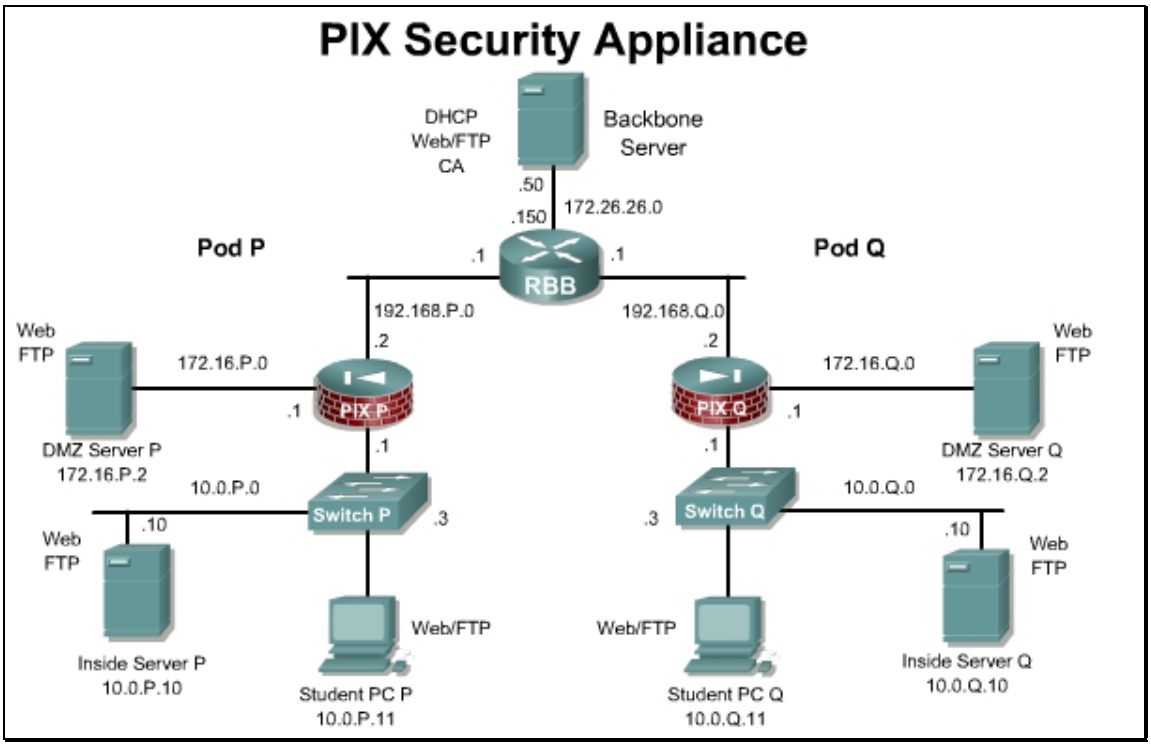
- Configure a service, ICMP-Type, and nested server object group.
- Configure an inbound access control list (ACL) with object groups.
- Configure web and ICMP access to the inside host.
- Test and verify the inbound ACL.

Scenario

In the previous lab, ASDM was used to configure a service object group. ASDM has some limitations when adding, editing, and deleting some object group types. CLI is the preferred method to handle object groups and nested object groups.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod PIX Security Appliances. Access the PIX Security Appliance console port using the terminal emulator on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080423271.html#wp1053224

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
access-group *access-list* {**in | out**} **interface** *interface_name* [*per-user-override*]	Binds the access list to an interface. Configuration mode.
access-list *id* [**line** *line-number*] [**extended**] {**deny | permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {**host** *source-ip* | *source-ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id* | **any**} {**host** *destination-ip* | *destination-ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]	Create an access list.
object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*	The **object-group** command isused to define a protocol, network, or icmp-type object group.
object-group service *obj_grp_id* {**tcp** | **udp** | **tcp-udp**}	Defines a group of TCP/UDP port specifications such as **eq smtp** and **range 2000 2010**.
show running-config object-group [**id** *grp_id* | *grp_type*]	Displays the current object groups in the configuration.

Step 1 Configure a Service Group Containing HTTP and FTP

To configure a service group containing HTTP and FTP, complete the following steps:

a. Delete the ACL configured in the previous lab.

```
PixP(config)# clear configure access-list outside_access_in
```

b. Verify that the ACL has been removed:

```
PixP(config)# show running-config access-list
```

c. Delete the service group configured in the previous lab.

```
PixP(config)# no object-group service DMZ_SERVICES tcp
```

d. Create a TCP service group named **MYSERVICES**. This step assigns a name to the group and enables the service object subcommand mode:

```
PixP(config)# object-group service MYSERVICES tcp
```

b. Add HTTP and FTP to the service object group:

```
PixP(config-service)# port-object eq http
PixP(config-service)# port-object eq ftp
```

1. What is the command to group consecutive services?

_____

Answer: `port-object range` *`begin_service end_service`*

c. Return to configuration mode:

```
PixP(config-service)# exit
```

d. Verify that the object group has been configured successfully:

```
PixP(config)#show running-config object-group
object-group service MYSERVICES tcp
port-object eq www
port-object eq ftp
```

Step 2 Configure an ICMP-Type Group

To configure an ICMP-Type group, complete the following steps:

a. To assign a name to the group and enable the ICMP-Type subcommand mode, create an ICMP-Type object group named PING:

```
PixP(config)# object-group icmp-type PING
```

b. Add ICMP echo to the ICMP-Type object group:

```
PixP(config-icmp-type)# icmp-object echo
```

c. Add ICMP echo-reply to the ICMP-Type object group:

```
PixP(config-icmp-type)# icmp-object echo-reply
```

d. Add ICMP unreachable messages to the ICMP-Type object group:

```
PixP(config-icmp-type)# icmp-object unreachable
```

e. Return to configuration mode:

```
PixP(config-icmp-type)# exit
```


f. Verify that the object group has been configured successfully:

```
PixP(config)# show running-config object-group
object-group service MYSERVICES tcp
port-object eq www
port-object eq ftp
object-group icmp-type PING
icmp-object echo
icmp-object echo-reply
icmp-object unreachable
```

Step 3 Nest an Object Group Within Another Object Group

To nest an object group within another object group, complete the following steps:

a. Create a network object group named FTPSERVERS:

```
PixP(config)# object-group network FTPSERVERS
```

b. Add the bastion host to the object group:

```
PixP(config-network)# network-object host 192.168.P.11
```

(where P = pod number)

c. Return to configuration mode:

```
PixP(config-network)# exit
```

d. Create a network object group named ALLSERVERS:

```
PixP(config)# object-group network ALLSERVERS
```

e. Nest the FTPSERVERS group within the ALLSERVERS group:

```
PixP(config-network)# group-object FTPSERVERS
```

f. Add the following servers to the ALLSERVERS group:

- 192.168.P.10
- 192.168.P.6
- 192.168.P.7

```
PixP(config-network)# network-object host 192.168.P.10
PixP(config-network)# network-object host 192.168.P.6
PixP(config-network)# network-object host 192.168.P.7
```

(where P = pod number)

g. Verify that the object group has been configured successfully:

```
PixP(config-network)# show running-config object-group
object-group service MYSERVICES tcp
   port-object eq www
   port-object eq ftp
object-group icmp-type PING
   icmp-object echo
   icmp-object echo-reply
```



```
   icmp-object unreachable
object-group network FTPSERVERS
   network-object host 192.168.P.11
object-group network ALLSERVERS
   group-object FTPSERVERS
   network-object host 192.168.P.10
   network-object host 192.168.P.6
   network-object host 192.168.P.7
```

(where P = pod number)

f. Return to configuration mode:

```
PixP(config-network)# exit
```

(where P = pod number)

Step 4 Configure an Inbound ACL With Object Groups

Complete the following steps to configure an inbound ACL to perform the following:

- Allow inbound web traffic from a peer pod network to the bastion host.
- Allow inbound FTP traffic from a peer pod internal host to the bastion host.

a. Test web access to the peer pod bastion host by completing the following substeps. The test to the peer bastion host should fail.

   i. Open a web browser on the student PC.

   ii. Use the web browser to access the bastion host of the peer pod group by entering **http://192.168.Q.11**.

   (where Q = peer pod number)

b. Test web access to the inside host of the peer pod by completing the following substeps. The test to the peer inside host should fail.

   i. Open a web browser on the student PC.

   ii. Use the web browser to access the inside host of the peer pod group by entering **http://192.168.Q.10**.

   (where Q = peer pod number)

   Why have these connection attempts failed?

   _____

   _____

   _____

   Answer: The default configuration is for no access. After clearing the access lists, there was no permitted path.

c. From the FTP client, test FTP access to the peer pod bastion host. Access to the peer bastion host using FTP should fail.

   Start>Run>ftp 192.168.Q.11

   (where Q = peer pod number)

d. Use the MYSERVICES group to create an ACL permitting inbound web and FTP access to the bastion host from the peer outside network:


```
PixP(config)# access-list ACLIN permit tcp 192.168.Q.0 255.255.255.0
object-group FTPSERVERS object-group MYSERVICES
```

(where Q = peer pod number)

e. Bind the ACL to the outside interface:

```
PixP(config)# access-group ACLIN in interface outside
```

f. View the ACLs:

```
PixP(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max
4096)       alert-interval 300
access-list ACLIN; 2 elements
access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 object-group FTPSERVERS object-group MYSERVICES
access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.P.11 eq www (hitcnt=0)
access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.P.11 eq ftp (hitcnt=0)
PixP(config)#
```

g. Ping the peer pod inside host. The ping should fail.

```
C:\>ping 192.168.Q.10
Pinging 192.168.Q.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

(where Q = peer pod number)

h. Ping the peer pod bastion host. The ping should fail.

```
C:\>ping 192.168.Q.11
Pinging 192.168.Q.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

(where Q = peer pod number)

i. Test web access to the peer pod bastion host by completing the following substeps. Access to the peer bastion host should be successful.

   i. Open a web browser on the student PC.

   ii. Use the web browser to access the bastion host of the peer pod group by entering **http://192.168.Q.11**.

   (where Q = peer pod number)

j. Test web access to the peer pod inside host by completing the following substeps. Access to the peer pod inside host should fail.

   i. Open a web browser on the client PC.

ii. Use the web browser to access the inside host of the peer pod group by entering **http://192.168.Q.10**.

(where Q = peer pod number)

k. From the FTP client, test FTP access to the peer pod bastion host. Access to the peer bastion host via FTP should be successful.

```
Start>Run>ftp 192.168.Q.11
```

(where Q = peer pod number)

l. From the FTP client, test FTP access to the peer pod inside hosts. Access to the peer inside host via FTP should fail.

```
Start>Run>ftp 192.168.Q.10
```

(where Q = peer pod number)

1. Why does the connection attempt to the peer pod inside host fail?

_____

_____

_____

Answer: There is no permitted access to the inside hosts with the current access list.

Step 5 Configure ACLIN

Complete the following steps to configure ACLIN to perform the following:

- Permit inbound web and ICMP traffic to all hosts behind the PIX Security Appliance
- Deny all other traffic from the Internet

a. Use a network hosts group to add an ACL entry permitting web traffic to all hosts behind the PIX Security Appliance:

```
PixP(config)# access-list ACLIN permit tcp any object-group
ALLSERVERS eq www
```

b. Permit ICMP traffic to all hosts behind the PIX Security Appliance:

```
PixP(config)# access-list ACLIN permit icmp any any object-group
PING
```

c. Deny all other traffic from the Internet:

```
PixP(config)# access-list ACLIN deny ip any any
```

d. Bind the ACL to the outside interface:

```
PixP(config)# access-group ACLIN in interface outside
```

e. Create an ACL to permit echo replies to the inside host from the bastion host:

```
PixP(config)# access-list ACLDMZ permit icmp any any object-group
PING
```

f. Bind the ACL to the demilitarized zone (DMZ) interface:

```
PixP(config)# access-group ACLDMZ in interface dmz
```

g. Display the ACLs and observe the hit counts:

```
PixP(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max
4096)       alert-interval 300
access-list ACLIN; 10 elements
```



```
access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 object-group FTPSERVERS object-group MYSERVICES

access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.1.11 eq www (hitcnt=0)

access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.1.11 eq ftp (hitcnt=0)

access-list ACLIN line 2 extended permit tcp any object-group
ALLSERVERS eq www

access-list ACLIN line 2 extended permit tcp any host 192.168.P.11
eq www (hitcnt=0)

access-list ACLIN line 2 extended permit tcp any host 192.168.P.10
eq www (hitcnt=0)

access-list ACLIN line 2 extended permit tcp any host 192.168.P.6 eq
www (hitcnt=0)

access-list ACLIN line 2 extended permit tcp any host 192.168.P.7 eq
www (hitcnt=0)

access-list ACLIN line 3 extended permit icmp any any object-group
PING

access-list ACLIN line 3 extended permit icmp any any echo
(hitcnt=0)

access-list ACLIN line 3 extended permit icmp any any echo-reply
(hitcnt=0)

access-list ACLIN line 3 extended permit icmp any any unreachable
(hitcnt=0)

access-list ACLIN line 4 extended deny ip any any (hitcnt=0)

access-list ACLDMZ; 3 elements

access-list ACLDMZ line 1 extended permit icmp any any object-group
PING

access-list ACLDMZ line 1 extended permit icmp any any echo
(hitcnt=0)

access-list ACLDMZ line 1 extended permit icmp any any echo-reply
(hitcnt=0)

access-list ACLDMZ line 1 extended permit icmp any any unreachable
(hitcnt=0)
```

(where P=pod number, and Q = peer pod number)

Step 6 Test and Verify the Inbound ACL

Complete the following steps to test the inbound ACL:

a. Ping the inside host of the peer pod:

```
C:\>ping 192.168.Q.10

Pinging 192.168.Q.10 with 32 bytes of data:

Reply from 192.168.Q.10: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.10: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.10: bytes=32 time<10ms TTL=128

Reply from 192.168.Q.10: bytes=32 time<10ms TTL=128
```


(where Q = peer pod number)

b. Ping the bastion host of the peer pod:

```
C:\>ping 192.168.Q.11
Pinging 192.168.Q.11 with 32 bytes of data:
Reply from 192.168.Q.11: bytes=32 time<10ms TTL=128
Reply from 192.168.Q.11: bytes=32 time<10ms TTL=128
Reply from 192.168.Q.11: bytes=32 time<10ms TTL=128
Reply from 192.168.Q.11: bytes=32 time<10ms TTL=128
```

(where Q = peer pod number)

c. From the student PC, ping the bastion host:

```
C:\>ping 172.16.P.2
Pinging 172.16.P.2 with 32 bytes of data:
Reply from 172.16.P.2: bytes=32 time<10ms TTL=128
Reply from 172.16.P.2: bytes=32 time<10ms TTL=128
Reply from 172.16.P.2: bytes=32 time<10ms TTL=128
Reply from 172.16.P.2: bytes=32 time<10ms TTL=128
```

(where P = pod number)

d. From the student PC, ping the Backbone server:

```
C:\>ping 172.26.26.50
Pinging 172.26.26.50 with 32 bytes of data:
Reply from 172.26.26.50: bytes=32 time<10ms TTL=128
Reply from 172.26.26.50: bytes=32 time<10ms TTL=128
Reply from 172.26.26.50: bytes=32 time<10ms TTL=128
Reply from 172.26.26.50: bytes=32 time<10ms TTL=128
```

e. Test web access to the peer pod bastion host by completing the following substeps. Access to the peer bastion host should be successful.

   i. Open a web browser on the student PC.

   ii. Use the web browser to access the bastion host of the peer pod group by entering **http://192.168.Q.11**.

   (where Q = peer pod number)

f. Test web access to the peer pod inside host by completing the following substeps. Access to the peer pod inside host should now be successful.

   i. Open a web browser on the client PC.

   ii. Use the web browser to access the inside host of the peer pod group by entering **http://192.168.Q.10**

   (where Q = peer pod number)

g. From the FTP client, test FTP access to the peer pod bastion host. Access to the peer bastion host via FTP should be successful.

   Start>Run>ftp 192.168.Q.11

   (where Q = peer pod number)

h. From the FTP client, test FTP access to the peer pod inside host. Access to the peer inside host via FTP should fail.

Start>Run>ftp 192.168.Q.10

(where Q = peer pod number)

i. Display the ACLs again and observe the hit counts:

```
PixP(config)# show access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max
4096)       alert-interval 300

access-list ACLIN; 10 elements

access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 object-group FTPSERVERS object-group MYSERVICES

access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.1.11 eq www (hitcnt=0)

access-list ACLIN line 1 extended permit tcp 192.168.Q.0
255.255.255.0 host 192.168.1.11 eq ftp (hitcnt=0)

access-list ACLIN line 2 extended permit tcp any object-group
ALLSERVERS eq www

access-list ACLIN line 2 extended permit tcp any host 192.168.P.11
eq www (hitcnt=0)

access-list ACLIN line 2 extended permit tcp any host 192.168.P.10
eq www (hitcnt=2)

access-list ACLIN line 2 extended permit tcp any host 192.168.P.6 eq
www (hitcnt=0)

access-list ACLIN line 2 extended permit tcp any host 192.168.P.7 eq
www (hitcnt=0)

access-list ACLIN line 3 extended permit icmp any any object-group
PING

access-list ACLIN line 3 extended permit icmp any any echo
(hitcnt=0)

access-list ACLIN line 3 extended permit icmp any any echo-reply
(hitcnt=4)

access-list ACLIN line 3 extended permit icmp any any unreachable
(hitcnt=0)

access-list ACLIN line 4 extended deny ip any any (hitcnt=0)

access-list ACLDMZ; 3 elements

access-list ACLDMZ line 1 extended permit icmp any any object-group
PING

access-list ACLDMZ line 1 extended permit icmp any any echo
(hitcnt=0)

access-list ACLDMZ line 1 extended permit icmp any any echo-reply
(hitcnt=8)

access-list ACLDMZ line 1 extended permit icmp any any unreachable
(hitcnt=0)
```


Lab 9.4.10 Configure and Test Advanced Protocol Handling on the Cisco PIX Security Appliance

Objective

In this lab exercise, the students will complete the following tasks:

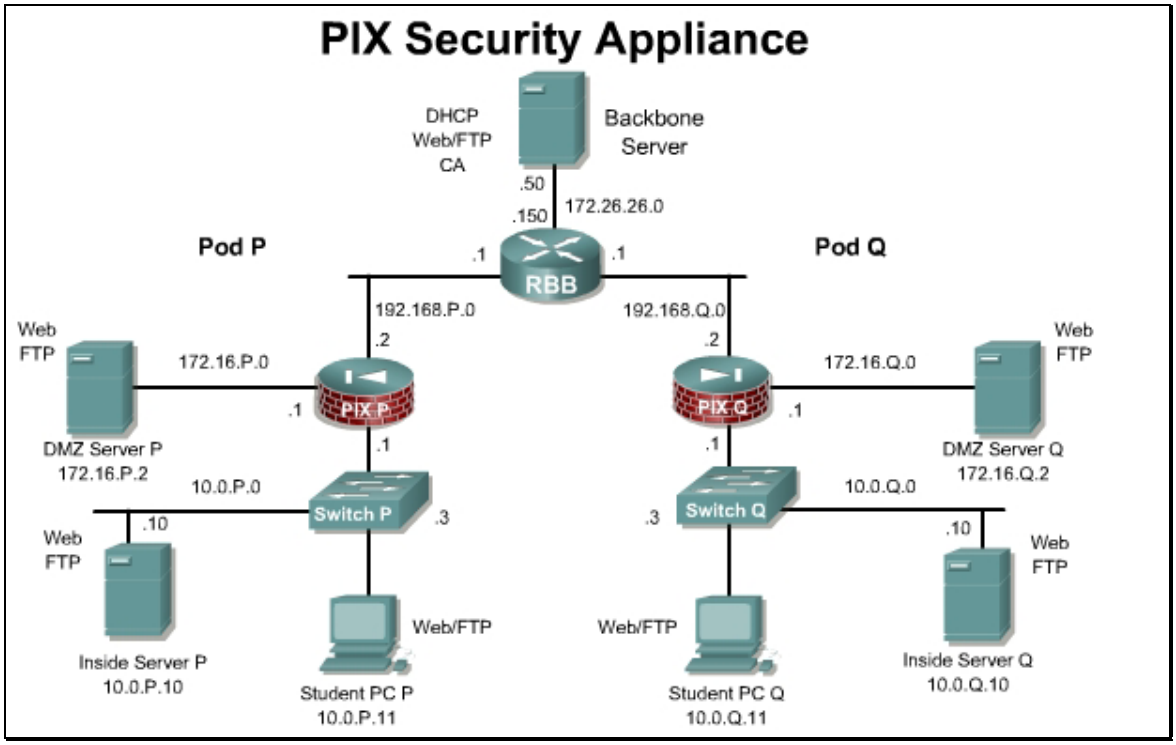
- Display the Inspection protocol configurations
- Change the Inspection protocol configurations
- Test the outbound FTP Inspection protocol
- Perform FTP deep packet inspection

Scenario

Some applications embed addressing information into the application data stream and negotiate randomly picked Transport Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers or IP addresses. In these cases application aware inspection must be performed.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod PIX Security Appliance. Access the PIX Security Appliance console port using the terminal emulator on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
clear configure fixup	To clear the fixup configuration, use the **clear configure fixup** command in global configuration mode.
ftp-map *map_name*	To identify a specific map for defining the parameters for strict FTP inspection, use the **ftp-map** command in global configuration mode.
policy-map *name*	To configure a policy, use the **policy-map** command in global configuration mode.
show running-config policy-map	To display all the policy-map configurations or the default policy-map configuration, use the **show running-config policy-map** command in privileged EXEC mode.
show running-config service-policy	To display all currently running service policy configurations, use the **show runnig-config service-policy** command in global configuration mode.

Step 1 List the Fixup Protocols

Complete the following steps and enter the commands as directed to view the current configurations of the PIX Security Appliance:

a. Show the default modular policy class-map running on the PIX security appliance:

```
pixP# show run class-map
class-map inspection_default
match default-inspection-traffic
```

1. What is the default class-map name?

Answer: `inspection_default`

b. Show the default modular policy-map running on the PIX security appliance:

```
pixP# show running-config policy-map
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

1. What is the default policy-map name?

_____

Answer: `global_policy`

2. What is the class for this policy?

_____

Answer: `inspection_default`

3. By default, which protocols are inspected by the PIX Security Appliance? Check each protocol that applies:

dns		**netbios**	
ftp		**mgcp**	
h323 ras		**tftp**	
rsh		**snmp**	
sip		**rtsp**	
skinny		**icmp**	
sunrpc		**h323 h225**	
xdmcp		**esmtp**	

sqlnet	
http	
dns	X
ftp	X
h323 ras	X
rsh	X
sip	X
skinny	X
sunrpc	X
xdmcp	X

netbios	X
mgcp	
tftp	X
snmp	
rtsp	X
icmp	
h323 h225	X
esmtp	X
sqlnet	X
http	

c. List the default modular policy service-policy running on the PIX Security Appliance:

```
PixP# show running-config service-policy
service-policy global_policy global
```

1. What is the default service-policy name?

_____

Answer: global_policy

2. Where is the default service-policy applied?

_____

Answer: The policy is applied globally.

Step 2 Change the Protocol Inspection Configuration

Complete the following steps and enter the commands as directed to change some of the current configurations of the PIX security appliance:

a. Disable the following Inspection protocols in the default policy-map:

```
PixP# configure terminal
PixP(config)# policy-map global_policy
PixP(config-pmap)# class inspection_default
PixP(config-pmap-c)# no inspect sunrpc
PixP(config-pmap-c)# no inspect h323 ras
PixP(config-pmap-c)# no inspect sqlnet
PixP(config-pmap-c)# exit
PixP(config-pmap)# exit
PixP(config)#
```

(where P = pod number)

b. Show the changes to the default modular policy-map running on the PIX Security Appliance:

```
PixP# show running-config policy-map
```

1. After the policy-map change, which protocols are inspected by the PIX Security Appliance?

dns	
ftp	
h323 ras	
rsh	
sip	
skinny	
sunrpc	
xdmcp	
netbios	
mgcp	
tftp	
snmp	
rtsp	
icmp	
h323 h225	
esmtp	
sqlnet	
http	

dns	**X**
ftp	**X**
h323 ras	
rsh	**X**
sip	**X**
skinny	**X**
sunrpc	
xdmcp	**X**
netbios	**X**
mgcp	
tftp	**X**
snmp	
rtsp	**X**
icmp	
h323 h225	**X**
esmtp	**X**
sqlnet	
http	

Step 3 Test Outbound FTP Protocol Inspection

Complete the following steps and enter the commands as directed to test the outbound FTP Protocol Inspection:

a. FTP to the backbone server from the student PC using the Windows FTP client:

```
C:\> ftp 172.26.26.50
User (172.26.26.50:(none)): ftpuser
331 Password required for ftpuser.
Password: ftppass
```

1. Was it possible to log into the server? Why or why not?

_____

Answer: Yes. The FTP session is allowed through and inspected by the PIX Security Appliance.

b. Do a directory listing at the FTP prompt:

```
ftp> dir
```

1. Was it possible to see a file listing? Why or why not?

_____

Answer: Yes. The FTP session is allowed through and inspected by the PIX Security Appliance.

c. Quit the FTP session:

```
ftp> quit
```

d. Turn off the FTP Inspection protocol on the PIX Security Appliance:

```
PixP(config)# policy-map global_policy
PixP(config-pmap)# class inspection_default
PixP(config-pmap-c)# no inspect ftp
PixP(config-pmap-c)# exit
PixP(config-pmap)# exit
PixP(config)#
```

(where P = pod number)

e. Again, ftp to the backbone server from the student PC using the Windows FTP client:

```
C:\> ftp 172.26.26.50
User (172.26.26.50:(none)): ftpuser
331 Password required for ftpuser.
Password: ftppass
```

1. Was it possible to log into the server? Why or why not?

_____

Answer: Yes. The FTP connection is allowed through the PIX Security Appliance.

2. Do a directory listing at the FTP prompt:

```
ftp> dir
```

3. Was it possible to see a file listing? Why or why not?

_____

Answer: No. The **dir** command is invalid when the PIX Security Appliance FTP inspection in turned off.

f. Quit the FTP session:

```
ftp> quit
```

Note If the FTP client is hung, press Ctrl+C until the C:\ prompt returns, or close the command prompt window.

g. Open a browser. Set the browser for passive FTP. In Internet Explorer, this can be done through navigation to **Tools > Internet Options > Advanced** and select **Use Passive FTP**. It should be possible to make an FTP connection to the backbone server from the student PC.

h. Enter the following in the URL field:

ftp://172.26.26.50

1. Was the connection successful? Why or why not?

_____

Answer: Yes. The passive FTP session is allowed through the PIX Security Appliance.

2. Was it possible to see a file listing? Why or why not?

_____

Answer: Yes. The passive FTP session is allowed through the PIX Security Appliance.

i. Disable passive FTP on the browser. Close the web browser.

Step 4 Perform FTP Deep Packet Inspection

Complete the following steps to perform FTP deep packet inspection:

a. Set all protocol inspection to the factory defaults:

```
PixP(config)# clear configure fixup
```

(where P = pod number)

b. Define an FTP-map to disallow the FTP **get** command:

```
PixP(config)# ftp-map no_get
PixP(config-ftp-map)# deny-request-cmd retr
PixP(config-ftp-map)# exit
PixP(config)#
```

c. FTP to the backbone server from the student PC using a web browser. It should be possible to open a file because the restrictions that were configured in the previous step have not been applied. To test default FTP inspection, enter the following in the URL field:

ftp://172.26.26.50

1. Was the connection successful? Why or why not?

_____

Answer: Yes. The FTP session is allowed through the PIX Security Appliance.

2. Was it possible to see a file listing? Why or why not?

_____

Answer: Yes. The FTP session is allowed through the PIX Security Appliance.

3. Was it possible to open one of the listed files? Why or why not?

_____

Answer: Yes. The FTP session is allowed through the PIX Security Appliance.

d. Close the browser

e. Apply the FTP-map restriction to the default policy-map:

```
PixP(config)# policy-map global_policy
PixP(config-pmap)# class inspection_default
PixP(config-pmap-c)# inspect ftp strict no_get
PixP(config-pmap-c)# exit
PixP(config-pmap)# exit
```



```
PixP(config)#
```

f. FTP to the backbone server from the student PC using a web browser. It should not be possible to open, or retrieve, a file. To do this, enter the following in the URL field:

ftp://172.26.26.50

1. Was the connection successful? Why or why not?

_____

Answer: Yes. The FTP session is allowed through the PIX Security Appliance.

2. Was it possible to see a file listing? Why or why not?

_____

Answer: Yes. The FTP session is allowed through the PIX Security Appliance.

3. Was it possible to open one of the listed files? Why or why not?

_____

Answer: No. The PIX Security Appliance has been configured to not allow the FTP **get** command.

g. Close the browser.

h. Verify the change to the default policy-map settings:

```
PixP(config)# show run policy-map
policy-map global_policy
class inspection_default
inspect dns
inspect netbios
inspect rtsp
inspect tftp
inspect xdmcp
inspect sunrpc
inspect ftp strict no_get
inspect h323 h225
inspect h323 ras
inspect rsh
inspect sqlnet
inspect sip
inspect skinny
```

(where P = pod number)

i. View the Service-Policy statistics. Examine the inspect ftp packet, drop, and reset-drop count.

```
pix1(config)# show service-policy
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: dns, packet 0, drop 0, reset-drop 0
```



```
Inspect: netbios, packet 0, drop 0, reset-drop 0
Inspect: rtsp, packet 0, drop 0, reset-drop 0
Inspect: tftp, packet 0, drop 0, reset-drop 0
Inspect: xdmcp, packet 0, drop 0, reset-drop 0
Inspect: ftp strict no_get, packet 236, drop 0, reset-drop 8
Inspect: h323 ras, packet 0, drop 0, reset-drop 0
Inspect: rsh, packet 0, drop 0, reset-drop 0
Inspect: esmtp, packet 0, drop 0, reset-drop 0
Inspect: sqlnet, packet 0, drop 0, reset-drop 0
Inspect: sip, packet 0, drop 0, reset-drop 0
Inspect: skinny, packet 0, drop 0, reset-drop 0
Inspect: sunrpc, packet 0, drop 0, reset-drop 0
```

j. Set all protocol inspection to the factory defaults:

```
pixP(config)# clear configure fixup
```

(where P = pod number)

k. Verify the protocol inspection settings:

```
pixP(config)# show run policy-map
policy-map global_policy
class inspection_default
inspect dns
inspect netbios
inspect rtsp
inspect tftp
inspect xdmcp
inspect sunrpc
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect sqlnet
inspect sip
inspect skinny
```

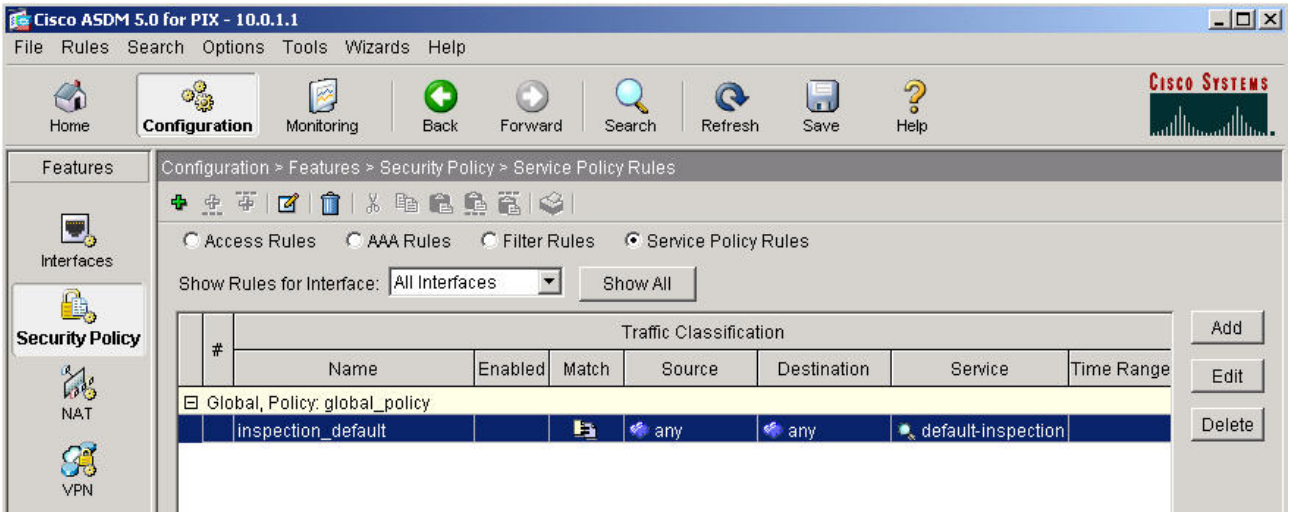
(where P = pod number)

Step 5 View the Fixup Protocols using ASDM

Complete the following steps:

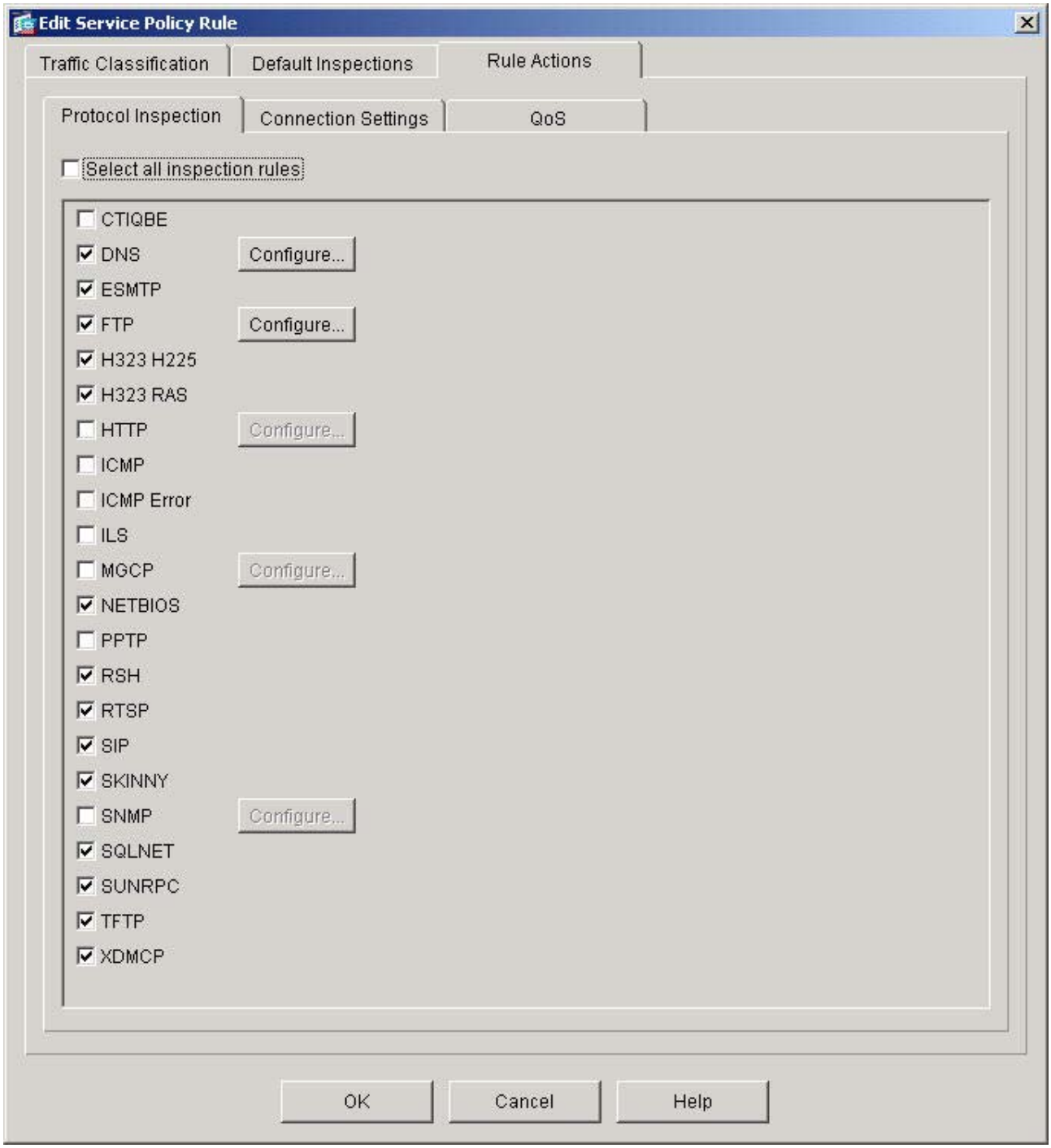
a. Log into ASDM

b. Navigate to **Configuration>Features>Security Policy>Service Policy Rules**.



c. Double click on the **inspection_default** rule. The **Edit Service Policy** window appears.

d. Click the **Rule Actions** tab, then click the **Protocol Inspection** tab. This tab allows the administrator to enable or disable the different types of application inspection that are available.



e. After reviewing the protocol inspection information, exit ADSM.

Lab 10.2.4 Mitigate Layer 2 Attacks

Objective

In this lab, the students will complete the following tasks:

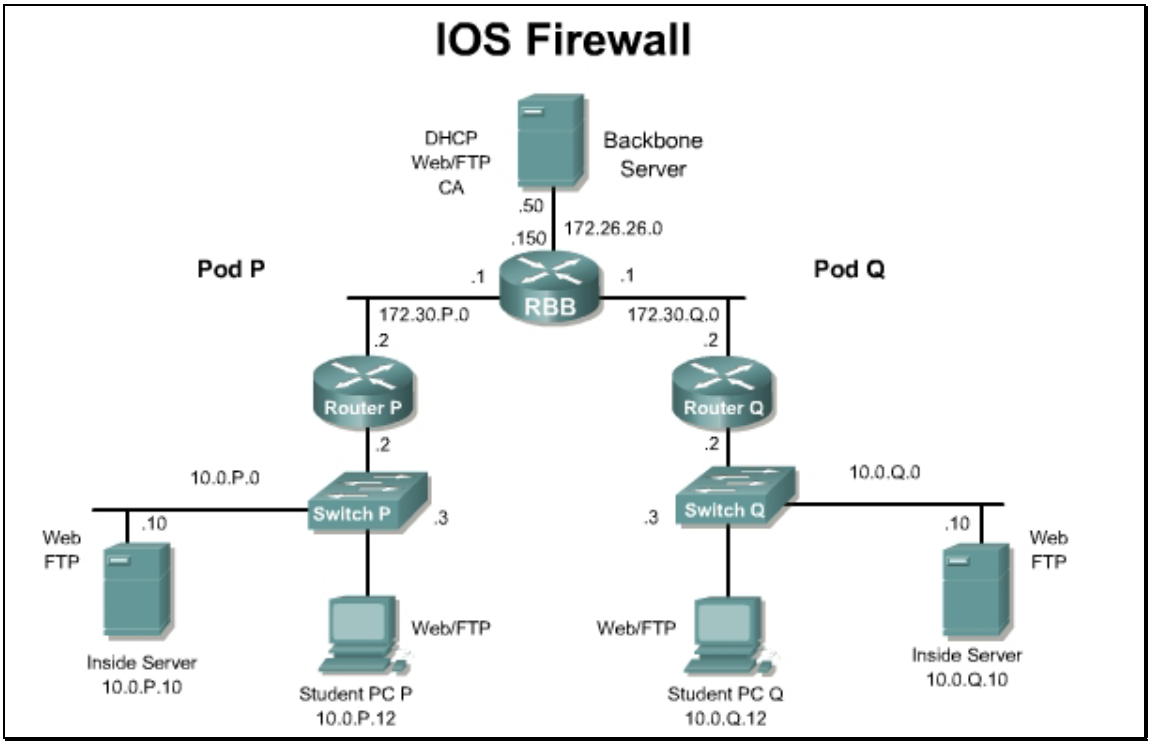
- Mitigate against CAM table overflow attack with appropriate Cisco IOS commands.
- Mitigate against MAC spoofing attacks with appropriate Cisco IOS commands.
- Mitigate against DHCP starvation attacks with appropriate Cisco IOS commands.

Scenario

The XYZ Company has a number of 2950 switches that are deployed throughout the building in order to provide network access for the employees. Attacks that use Layer 2 of the OSI model are quickly gaining sophistication and popularity. The network administrator must mitigate the effects of these attacks as much as possible.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod switch. Access the pod switch console port using the terminal emulator on the Windows 2000 server. If desired, save the switch configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- A second PC to be used to test the configuration

Command List

In this lab exercise, the following switch commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Switch Commands

Command	Description
arp timeout *seconds*	To configure how long an entry remains in the Address Resolution Protocol (ARP) cache, use the **arp timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.
show port-security [address] [interface *interface-id*]	To display the port security settings for an interface or for the switch, use the **show port-security** command.
switchport port-security	Enables port security on the interface.
switchport port-security mac-address *mac-addr*	To set the maximum number of secure MAC addresses on an interface, use the **switchport-port-security mac-address** command. Use the **no** form of this command to remove a MAC address from the list of secure MAC addresses.
switchport port-security maximum *max-addr*	Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 128; the default is 128.
switchport port-security violation {*shutdown* | *restrict* | *protect*}	Set the security violation mode for the interface.
ip dhcp snooping	Enables DHCP snooping globally.
ip dhcp snooping vlan *vlan_id {,vlan_id}*	Enable DHCP snooping on a VLAN or range of VLANs. A single VLAN can be identified by VLAN ID number, or start and end VLAN IDs can be used to specify a range of VLANs. The range is 1 to 4094.
ip dhcp snooping trust	Configure the interface as trusted or untrusted. The default is untrusted.
ip dhcp snooping limit rate *rate*	Configure the number of DHCP packets per second than an interface can receive. The range is 1 to 4294967294. The default is no rate limit configured.

Step 1 Mitigate the CAM Table Overflow Attack

Complete the following steps to mitigate against CAM table overflow attack with appropriate Cisco IOS commands:

Note The enable secret password for the pod switch is **cisco**.

a. Enter the interface configuration mode for port FastEthernet 0/12

```
SwitchP(config)#interface fastEthernet 0/12
SwitchP(config-if)#
```

(Where P = pod number)

b. Set the port mode to access.

```
SwitchP(config-if)# switchport mode access
```

c. Enable port security on the selected interface.

```
SwitchP(config-if)# switchport port-security
```

d. Configure the maximum number of MAC addresses that can be configured or learned on this port. The default is 1.

```
SwitchP(config-if)# switchport port-security maximum 1
```

e. Configure an action to be taken when a violation occurs. The default is shutdown.

```
SwitchP(config-if)# switchport port-security violation shutdown
```

1. What other options are available for actions to be taken when a violation to occur?

_____

Answer: `restrict` and `shutdown`

f. Record the MAC address of the student PC for use in the next step. For example, **0000.ffff.1111**

g. Configure a static MAC address entry for the device that will be attached to the port.

```
SwitchP(config-if)# switchport port-security mac-address
0000.ffff.1111
```

h. Plug the student PC into the port Fa0/12 and try to ping the gateway.

C:\WINNT\system32>**ping 10.0.P.2**

1. Was the ping successful?

_____

Answer: Yes

i. Return to privileged EXEC mode.

```
SwitchP(config-if)# end
SwitchP#
```

j. Verify the port security settings for port Fa0/12.

```
SwitchP# show port-security interface fastEthernet 0/12
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
```



```
Last Source Address        : 0000.0000.0000
Security Violation Count   : 0
```

k. Verify that the MAC address of the student PC is configured as a secure address.

```
SwitchP# show port-security address
       Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                          (mins)
----    -----------       ----                -----   -------------
 30P    0000.ffff.1111    SecureConfigured    Fa0/12       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

1. What address type is shown for the MAC address of the student PC?

_____

Answer: SecureConfigured

Step 2 Mitigate MAC Spoofing Attacks

Complete the following steps to mitigate against CAM table overflow attack with appropriate Cisco IOS commands.

a. Enter the interface configuration mode for port FastEthernet 0/12

```
SwitchP(config)#interface fastEthernet 0/12
SwitchP(config-if)#
```

(Where P = pod number)

b. Configure the maximum number of MAC addresses that can be configured or learned on this port.

```
SwitchP(config-if)# switchport port-security maximum 1
```

c. Configure an action to be taken when a violation occurs.

```
SwitchP(config-if)# switchport port-security violation shutdown
```

d. Specify an ARP timeout of ten seconds. The default is four minutes.

```
SwitchP(config-if)# arp timeout 10
```

e. Unplug the student PC from port Fa 0/12. Plug another PC that does not have the correct MAC address into port Fa 0/12.

f. Return to privileged EXEC mode.

```
SwitchP(config-if)# end
SwitchP#
```

g. Use the following commands to verify that the interface Fa 0/12 is shut down due to a security violation.

```
SwitchP# show port-security
```



```
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
     Fa0/12             1            1                  1         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
SwitchP# show port-security interface fastEthernet 0/12
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address        : 0000.ffff.2222
Security Violation Count   : 1
```

2. What state is the port in after the security violation occurs?

_____

Answer: err-disabled

```
SwitchP# show interfaces status err-disabled
Port      Name               Status       Reason
Fa0/12                       err-disabled psecure-violation
```

Step 3 Mitigate DHCP Starvation Attacks

Complete the following steps to mitigate against DHCP starvation attacks with appropriate Cisco IOS commands.

a. Enable DHCP snooping globally.

```
SwitchP(config)# ip dhcp snooping
```

b. Enable DHCP snooping on VLAN 301.

```
SwitchP(config)# ip dhcp snooping vlan 301
```

c. Switch to interface configuration mode for interface Fa 0/12.

```
SwitchP(config)# interface fastEthernet 0/12
```

d. Configure the interface as trusted. The **no** keyword can be used to configure an interface to receive messages from an untrusted client. The default is untrusted.

```
SwitchP(config-if)# ip dhcp snooping trust
```


e. Configure the number of DHCP packets per second than an interface can receive to be 100. The default is no rate limit configured.

```
SwitchP(config-if)# ip dhcp snooping limit rate 100
```

1. What is the range of DHCP packets per second that can be configured on the interface?

_____

Answer: The range is 1 to 4294967294

h. Return to privileged EXEC mode.

```
SwitchP(config-if)# end
SwitchP#
```

f. Verify the DHCP snooping configuration.

```
SwitchP# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
301
Insertion of option 82 is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/12             yes         100
```

