



Lab 2.5.2b Controlling TCP/IP Services

Objective

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

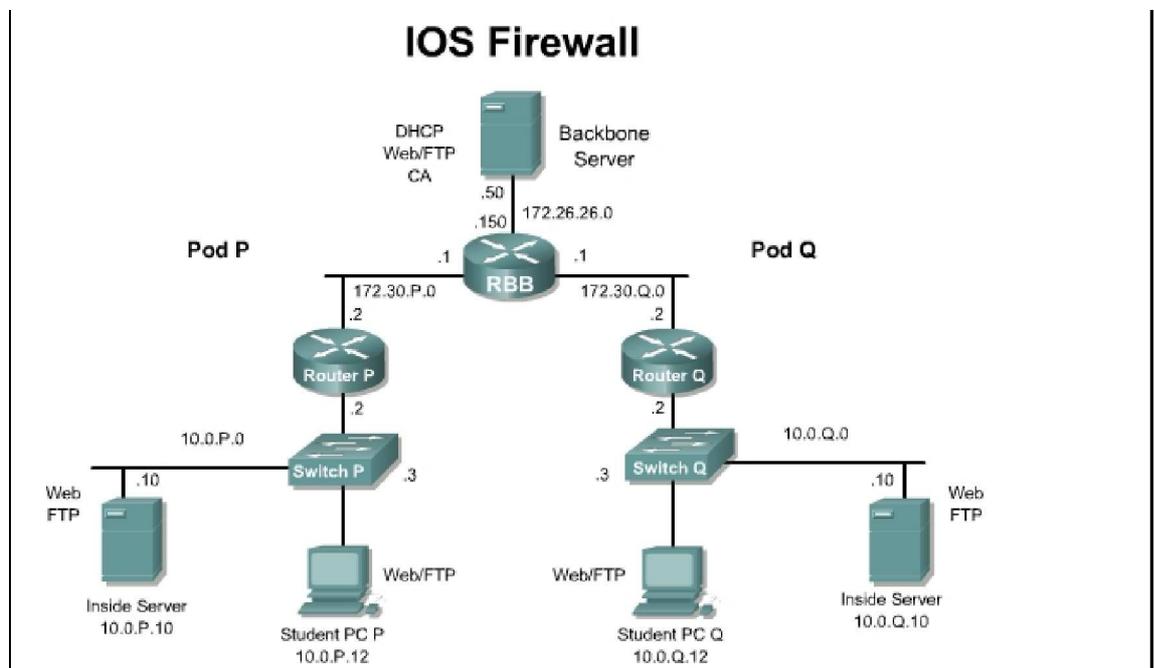
- Begin the process of implementing a secure perimeter router
- Explicitly deny common TCP/IP services
- Verify TCP/IP services have been disabled

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
<code>no cdp enable</code>	Disables Cisco Discovery Protocol on an interface
<code>no cdp run</code>	Disables Cisco Discovery Protocol globally
<code>no ip mask-reply</code>	Disables the Cisco IOS software response to the Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages.
<code>no mroute-cache</code>	Disables multicast route caching on the outside interface.
<code>no ip proxy-arp</code>	Use the <code>no ip proxy-arp</code> interface configuration command to disable proxy ARP on an interface.
<code>no ip redirects</code>	Use the <code>no ip redirects</code> 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.
<code>no ip route-cache</code>	Use the <code>no ip route-cache</code> interface configuration command to disable the use of a high-speed switching cache for IP routing as well as the use of autonomous switching.
<code>no ip source-route</code>	Use the <code>no ip source-route</code> command to cause the system to discard any IP datagram containing a source-route option.
<code>no ip unreachable</code>	Use the <code>ip unreachable</code> interface configuration command to enable the generation of ICMP unreachable messages on a specified interface.

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

- 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 unreachable`.

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?
-

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?
-

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?
-
-

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.
-

- 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?
-

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

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

3. Was the connection successful?
-

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.
-

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?
-

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:
-
-

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

1. What information is displayed?
-
-
-

- 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?
-
-
-

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 unreachable 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
```