



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.

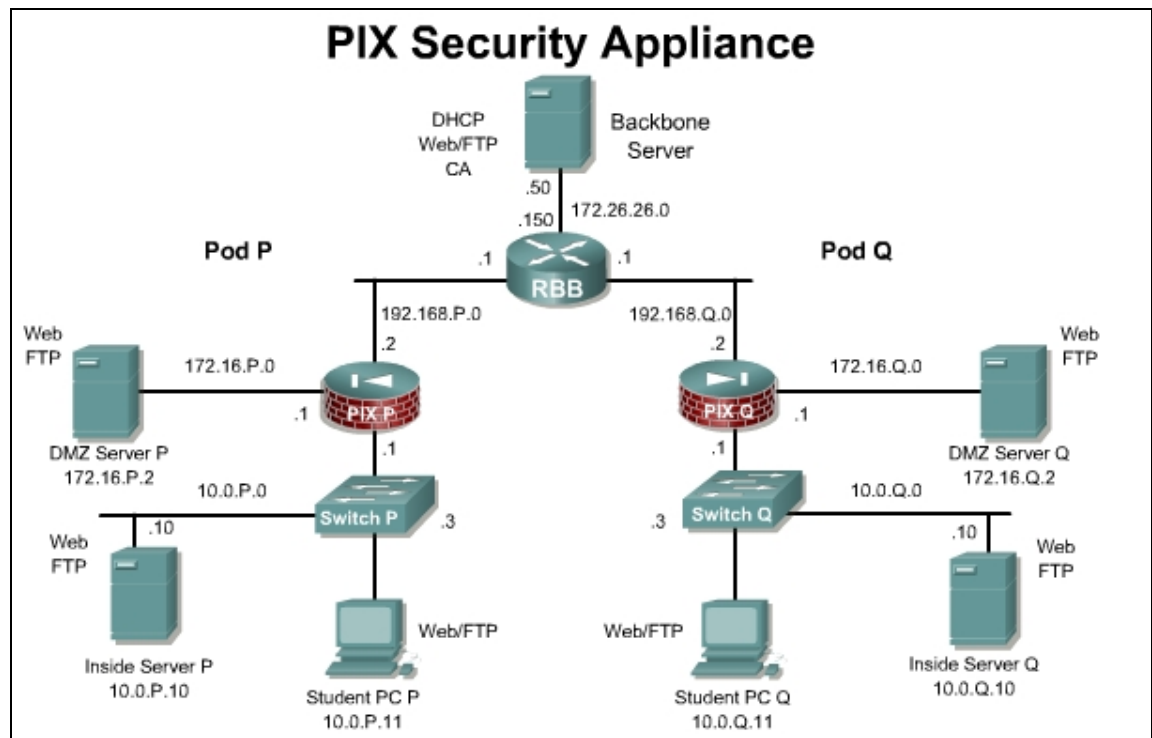
Host/Network and Service Types—ASDM uses Host/Network and service type objects. You can add, edit or delete network type object groups in **Configuration>Hosts/Networks>Group** and service type object groups in **Tools>Service Groups**, **Configuration>VPN**, and **Configuration>Access Rules**.

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.

CLI Command

☒ Single Line ☐ Multiple Line

Command:

Response:

Result of the command: "clear configure access-list"

The command has been sent to the device

- 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.

Configuration > Features > Security Policy > Access Rules

☒ Access Rules ☐ AAA Rules ☐ Filter Rules ☐ Service Policy Rules

Show Rules for Interface:

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	any	any		inside (outbound)	ip
-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	any	any		dmz (outbound)	ip

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:

- From the Access Rules page, click on the **Add New Rule** icon or the **Add** button.
- Create an Access Rule which permits ICMP echo traffic from the outside to the Bastionhost. Click the **OK** button when finished.

Add Access Rule

Action

Select an action: **permit**

Apply to Traffic: **incoming to src interface**

Source Host/Network

☒ IP Address ☐ Name ☐ Group

Interface: **outside**

IP address: **0.0.0.0**

Mask: **0.0.0.0**

Destination Host/Network

☒ IP Address ☐ Name ☐ Group

Interface: **dmz**

IP address: **172.16.1.2**

Mask: **255.255.255.255**

Time Range

Time Range: **-- Not Applied --**

Rule Flow Diagram

Rule applied to traffic incoming to source interface

any → outside → dmz → bastionhost 172.16.1.2

Allow traffic

Protocol and Service

☐ TCP ☐ UDP ☒ ICMP ☐ IP

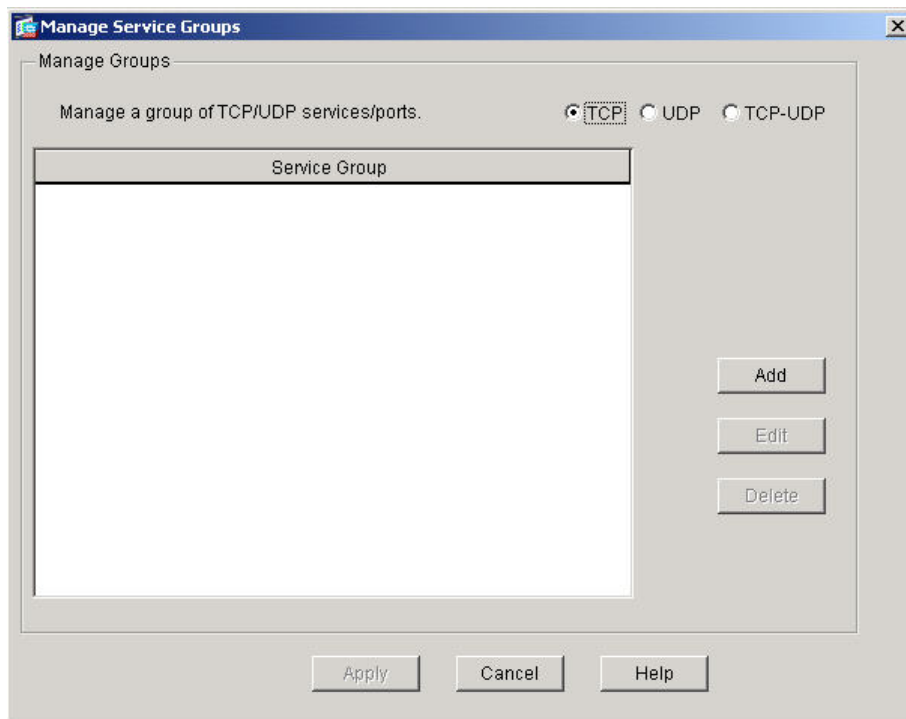
ICMP Type

ICMP type: **echo**

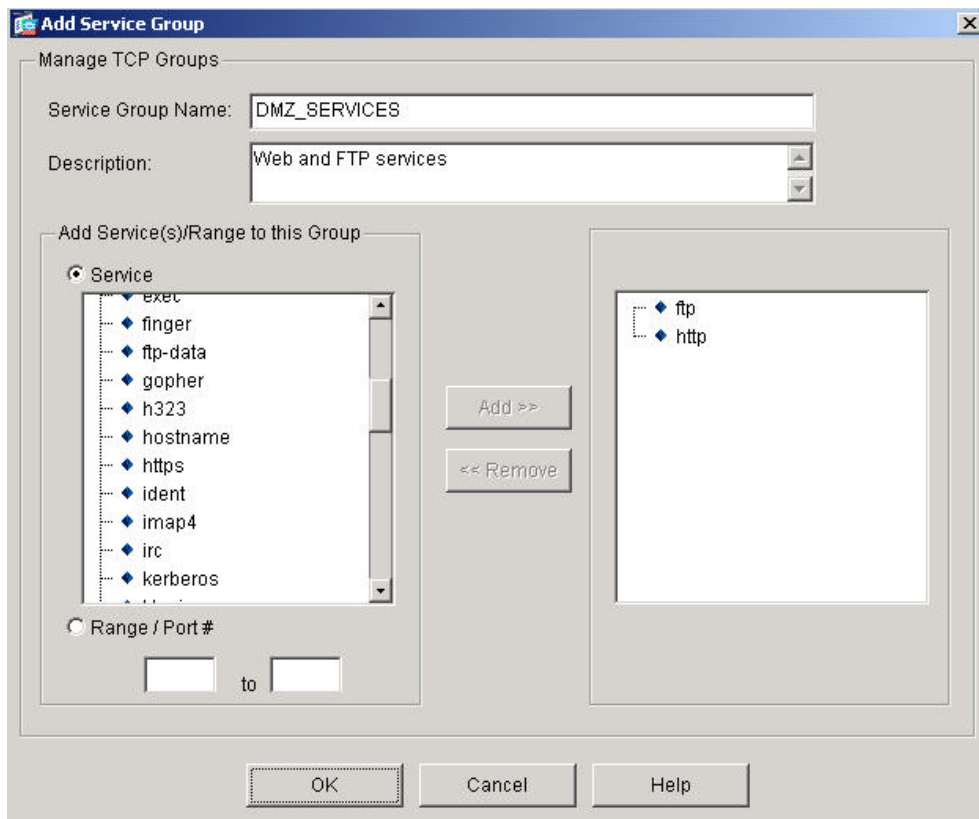
Please enter the description below (optional):

OK Cancel Help

- Click the **Add New Rule** icon.
- Create a permit statement to permit traffic with a source of outside (ANY) and the destination of DMZ (bastionhost)
- Click on the **Manage Service Groups** button. The Manage Service Groups window will appear.

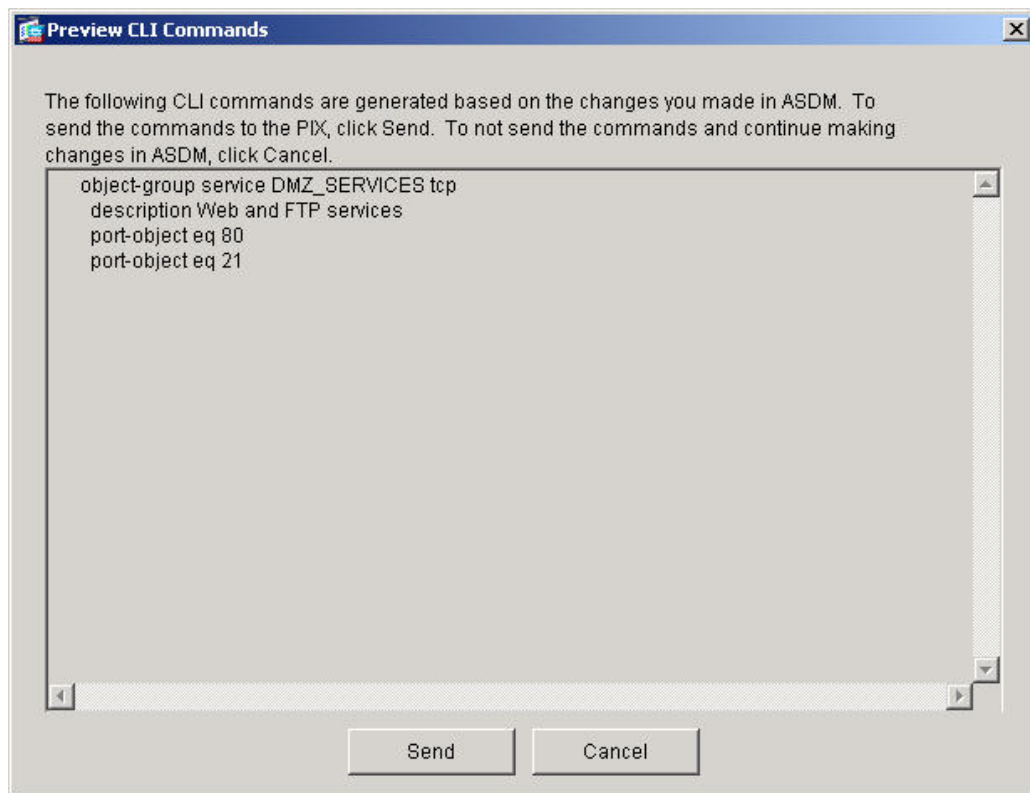


- f. Make sure the TCP radio button is checked.
- g. Click on the **Add** button. The **Add Service Group** window appears.
- h. Enter a Service group name of **DMZ_SERVICES** and a description of **Web and FTP services**.



- 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.

Command Line Interface

Command Line Interface

Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash.

CLI Command

☒ Single Line ☐ Multiple Line

Command:

Response:

Result of the command: "show access-list"

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list outside_access_in: 2 elements
access-list outside_access_in line 1 remark Web and FTP access to the Bastionhost
access-list outside_access_in line 2 extended permit tcp any host 192.168.1.11 object-group DMZ_SERVICES
access-list outside_access_in line 2 extended permit tcp any host 192.168.1.11 eq www (hitcnt=0)
access-list outside_access_in line 2 extended permit tcp any host 192.168.1.11 eq ftp (hitcnt=0)
```

- c. Click the **Close** button when finished.
- d. Exit ASDM.