



Lab 9.1.7c Configure Multiple Interfaces using CLI – Challenge Lab

Objective

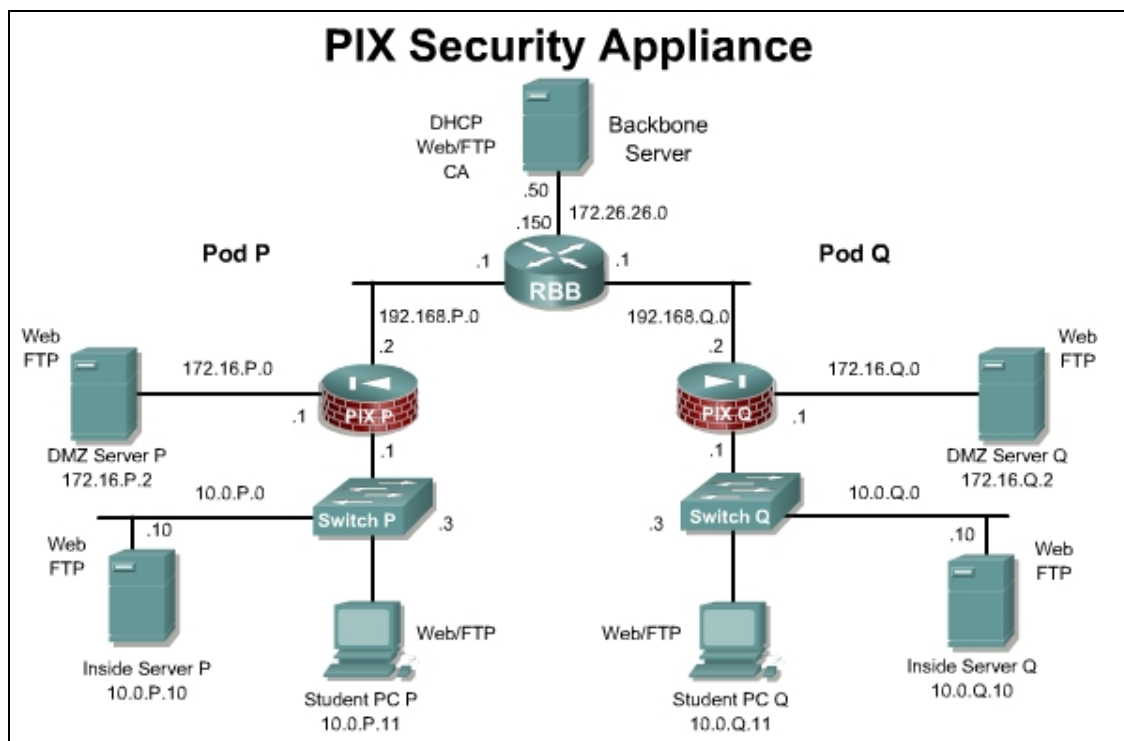
In this lab, the students will complete the tasks of configuring three PIX interfaces and configure access through the PIX Security Appliance.

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:

- Erase the existing configuration and reload the PIX Security Appliance.
- Name the PIX Security Appliance **PixP**.
(where P = pod number)
- Name the appropriate interfaces as inside, outside, and DMZ and assign security levels.
- Give each interface the appropriate IP address and subnet mask.
- Enable the Ethernet 0, Ethernet 1, and Ethernet 2 interfaces as 100-Mbps full duplex.
- 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.
- Set a default route for all internal hosts to exit the outside interface.
- 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.
- Allow internal FTP and WWW traffic to reach the DMZ bastion host.
- 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.
- 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.
- 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.
- Use the **show** commands to verify operation:

What **show** commands are useful to verify configuration and operation?
