Lab 2.5.7 Configure Routing Authentication and Filtering

Objective

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

Configure routing protocol authentication

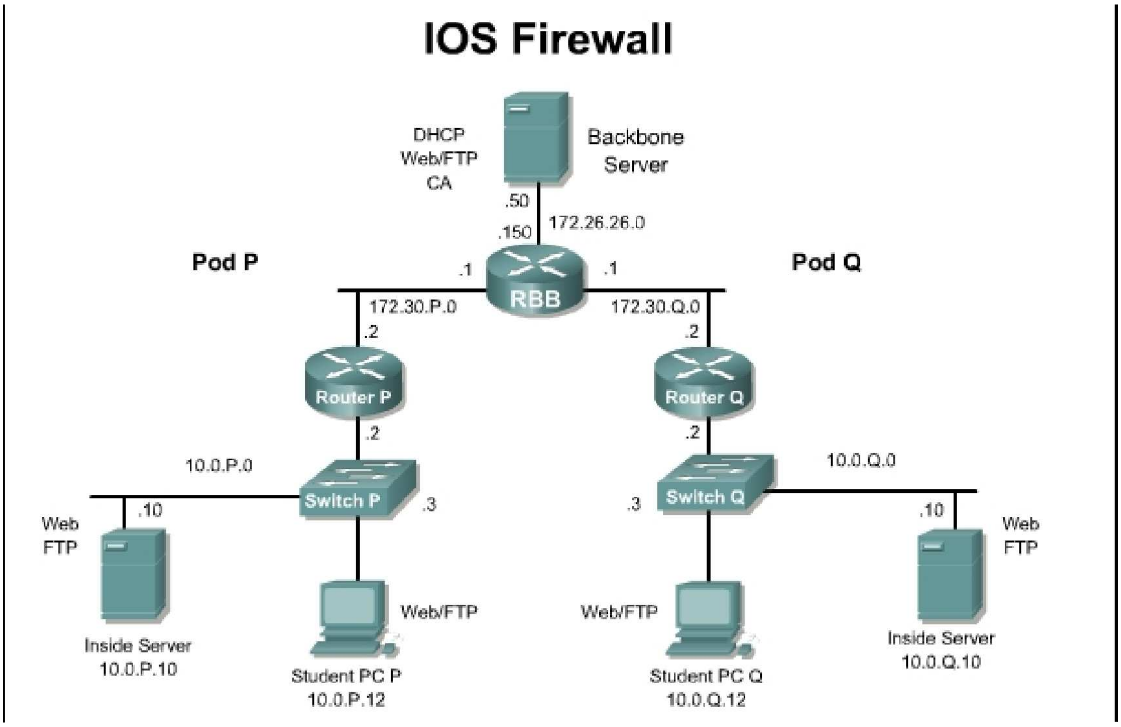
Configure route filters to control route updates from peer routers.

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?

____

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?

____

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?

____

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.

   ____

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?

   ____

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
```