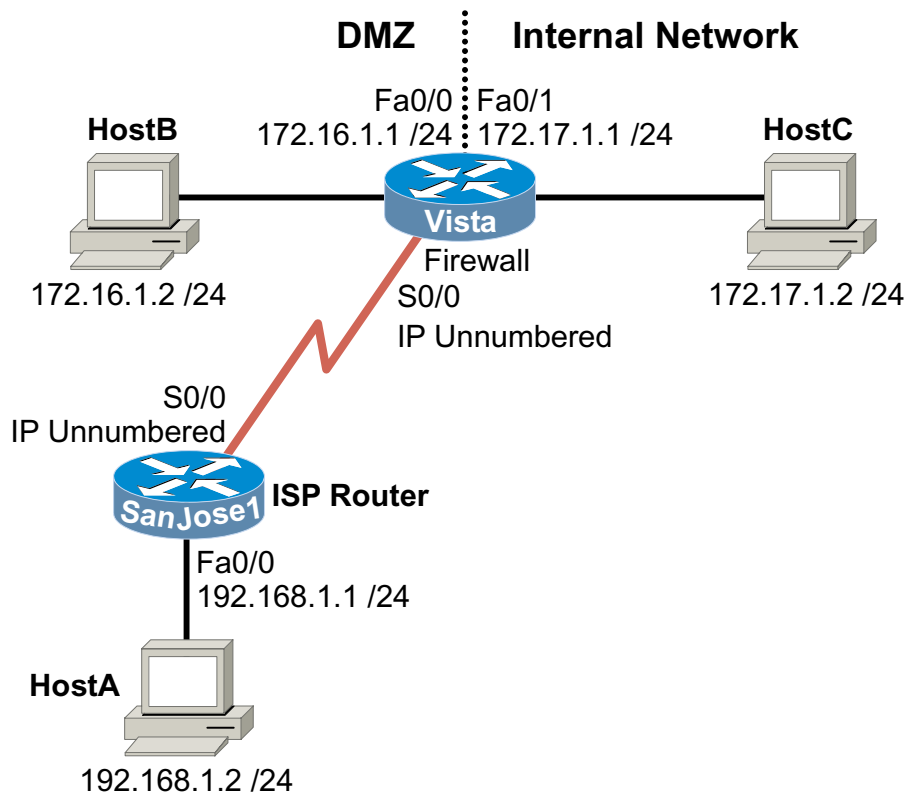


Lab 10.7.3 CBAC



Objective

In this lab, you configure content-based access control (CBAC) to secure an internal network and allow limited outside access to a DMZ.

Scenario

International Travel Agency (ITA) wants you to implement a rock-solid firewall on its border router, Vista. You are to secure its internal segment, 172.17.1.0/24, so that outside hosts cannot initiate a session with inside hosts. Furthermore, you are to secure the DMZ so that outside hosts can access the public services there, but only if outside hosts initiate the session. To prevent sophisticated attacks, no connections should be allowed to initiate from the DMZ.

Step 1

Build and configure the network according to the diagram; do not configure a routing protocol. Use IP unnumbered on both SanJose1 and Vista so that they use their FastEthernet 0/0 addresses for their serial connections.

Step 2

Configure SanJose1 and Vista for static routing. The ITA company uses a default route to reach the outside world. Issue the following command on Vista:

```
Vista(config)#ip route 0.0.0.0 0.0.0.0 s0
```

On the ISP's router (SanJose1), you must also configure static routes:

```
SanJose1(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0
SanJose1(config)#ip route 172.17.1.0 255.255.255.0 serial 0/0
```

Use **ping** to verify that SanJose1 can reach the hosts (172.16.1.2 and 172.17.1.2). Troubleshoot, as necessary.

Step 3

Configure access lists on Vista to protect the internal network. Issue the following commands on Vista:

```
Vista(config)#access-list 101 permit ip 172.17.1.0 0.0.0.255 any
Vista(config)#access-list 101 deny ip any any
Vista(config)#interface fastethernet 0/1
Vista(config-if)#ip access-group 101 in
```

Access list 101 might first appear unnecessary. But in a secure network that uses CBAC, it is important to explicitly specify what traffic an interface should accept. In this case, you expect FastEthernet 0/1 to accept traffic sourced from ITA's internal network (172.17.1.0/24). Although the **deny any any** is implicit, many administrators find it useful to include an explicit entry so that this statement will show up in the running configuration and **show ip access-lists** command output.

Next, you must configure an outbound access list on FastEthernet 0/1. Traffic leaving FastEthernet 0/1 will be traffic originating from either the DMZ or the Internet, so this list must protect your internal network.

Start configuring this list by allowing ICMP traffic, which internal hosts will require to make network management and troubleshooting easier. By permitting ICMP echo replies and other select traffic, you let your internal hosts receive important ICMP error messages from beyond their local network.

```
Vista(config)#access-list 102 permit icmp any any
administratively-prohibited
Vista(config)#access-list 102 permit icmp any any echo-reply
Vista(config)#access-list 102 permit icmp any any packet-too-big
Vista(config)#access-list 102 permit icmp any any time-exceeded
Vista(config)#access-list 102 permit icmp any any unreachable
Vista(config)#access-list 102 deny ip any any
Vista(config)#interface fastethernet 0/1
Vista(config-if)#ip access-group 102 out
```

Access list 102 effectively blocks all traffic from exiting FastEthernet 0/1 onto the internal network, except for the ICMP messages.

Verify that the access lists have taken effect. From SanJose1, ping Host C. These pings should not be successful.

1. Now ping SanJose1's FastEthernet 0/0 from Host C. These pings should be successful. Why?
-

Step 4

Configure the DMZ's inbound access list. On Vista, issue the following commands:

```
Vista(config)#access-list 111 permit ip 172.16.1.0 0.0.0.255 any
Vista(config)#access-list 111 deny ip any any
Vista(config)#interface fastethernet 0/0
Vista(config-if)#ip access-group 111 in
```

Again, you have used this simple list to specify the only permissible traffic that can enter Vista on FastEthernet 0/0.

Now configure the outbound access list for FastEthernet 0/0. This list will filter traffic originating from the internal network and the Internet. Assume for this lab that Host B is ITA's public DNS server. Use the following commands to allow hosts to use the server for lookup requests on UDP 53 and to allow DNS zone transfers on TCP 53:

```
Vista(config)#access-list 112 permit udp any host 172.16.1.2 eq
domain
Vista(config)#access-list 112 permit tcp any host 172.16.1.2 eq 53
```

Next, configure the access list to allow Web, FTP, and SMTP (mail) into the DMZ. Again, for the purposes of this lab, use Host B as the all-purpose server, but you can use the Vista's FastEthernet 0/0 as the Web server, as shown:

```
Vista(config)#access-list 112 permit tcp any host 172.16.1.2 eq ftp
Vista(config)#access-list 112 permit tcp any host 172.16.1.2 eq smtp
Vista(config)#access-list 112 permit tcp any host 172.16.1.1 eq www
```

Of course, the DMZ might also offer services that should be restricted to ITA users, such as POP3 and Telnet. You can accomplish that with the following commands:

```
Vista(config)#access-list 112 permit tcp 172.17.1.0 0.0.0.255 host
172.16.1.2 eq pop3
Vista(config)#access-list 112 permit tcp 172.17.1.0 0.0.0.255 any
eq telnet
```

It is safe to allow these services based on source address only if you configure the external interface, Serial 0/0, for antispoofing. You do this in Step 5.

Finally, allow the usual ICMP messages, explicitly deny all other IP protocols, and apply the access list with the following commands:

```
Vista(config)#access-list 112 permit icmp any any
administratively-prohibited
Vista(config)#access-list 112 permit icmp any any echo-reply
Vista(config)#access-list 112 permit icmp any any packet-too-big
Vista(config)#access-list 112 permit icmp any any time-exceeded
Vista(config)#access-list 112 permit icmp any any unreachable
Vista(config)#access-list 112 deny ip any any
Vista(config)#interface fastethernet 0/0
Vista(config-if)#ip access-group 112 out
```

Verify that the access lists have taken effect. From SanJose1, ping Host B. These pings should not be successful.

1. Now ping SanJose1's FastEthernet 0/0 from Host B. These pings should be successful. Why?

Step 5

After you configure the DMZ and internal access lists, you can now focus on the external interface (Serial 0/0), which represents the greatest security threat. First, configure an access list so that Internet hosts cannot easily spoof your internal network addresses:

```
Vista(config)#access-list 121 deny ip 172.17.1.0 0.0.0.255 any
Vista(config)#access-list 121 deny ip 127.0.0.0 0.255.255.255 any
Vista(config)#access-list 121 deny ip 224.0.0.0 31.255.255.255 any
Vista(config)#access-list 121 permit ip any any
Vista(config)#interface serial 0/0
Vista(config-if)#ip access-group 121 in
```

In addition to antispoofing, this list protects against packets using a loopback (127.0.0.0/8) or multicast address (224.0.0.0/3). Now configure the outbound list for Vista's Serial 0/0. Issue the following commands:

```
Vista(config)#access-list 122 permit icmp any any echo-reply
Vista(config)#access-list 122 permit icmp any any time-exceeded
Vista(config)#access-list 122 deny ip 172.16.1.0 0.0.0.255 any
Vista(config)#access-list 122 permit ip any any
Vista(config)#interface serial 0/0
Vista(config-if)#ip access-group 122 out
```

Access list 122 permits two important ICMP error messages from Internet hosts. It also prevents a DMZ host from leaving Vista via Serial 0/0. CBAC "pokes holes" in this denial entry so that outside users can connect to public services.

Don't be alarmed by the **permit ip any any** statement. If you check your configuration, you will see that both FastEthernet 0/0 and FastEthernet 0/1 are configured to **deny ip any any**, unless CBAC pokes holes in those entries, too.

Step 6

Configure CBAC on Vista:

```
Vista(config)#ip inspect name STANDARD ftp
Vista(config)#ip inspect name STANDARD http
Vista(config)#ip inspect name STANDARD smtp
Vista(config)#ip inspect name STANDARD sqlnet
Vista(config)#ip inspect name STANDARD tcp
Vista(config)#ip inspect name STANDARD tftp
Vista(config)#ip inspect name STANDARD udp
Vista(config)#ip inspect name STANDARD realaudio
Vista(config)#ip inspect dns-timeout 15
Vista(config)#ip inspect udp idle-time 1800
```

These commands create the CBAC inspect list called STANDARD. This list will match sessions for common application protocols. Also, you have to set the DNS timeout to 15 seconds because DNS connections should time out more quickly than other UDP connections. Otherwise, CBAC will have to maintain many useless connection state table entries for DNS requests that were completed a long time ago.

With the STANDARD list configured, you can apply it to the appropriate interfaces, as shown:

```
Vista(config)#interface fastethernet 0/1
Vista(config-if)#ip inspect STANDARD in
Vista(config)#interface serial 0/0
Vista(config-if)#ip inspect STANDARD in
```

No `ip inspect` command exists on the DMZ interface (FastEthernet 0/0), because outgoing conversations are never initiated from the DMZ. Note that this really means that no outgoing connections are permitted.

Verify your CBAC configuration by issuing the `show ip inspect all` command.

1. According to the output of this command, what is the DNS timeout value set to?

2. What is the inbound inspection rule?
