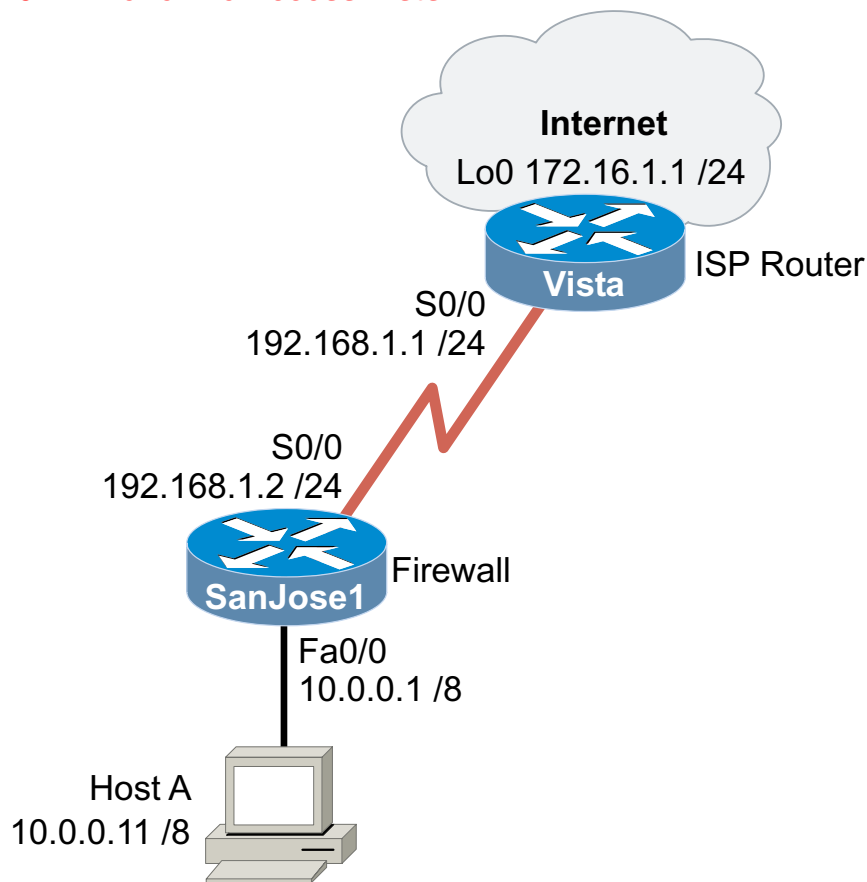


10.7.2 Reflexive Access Lists



Objective

In this lab, you configure a reflexive access list to implement IP session filtering.

Scenario

International Travel Agency (ITA) wants you to beef up security for its network 10.0.0.0/8. The company would like users on the 10.0.0.0/8 network to be able to establish sessions with remote hosts at will. At the same time, the company requires that you prevent outside sources from initiating a session. In other words, outside hosts should be able to talk to 10.0.0.0/8 hosts only if the 10.0.0.0/8 hosts started the conversation. You need to use a reflexive access list to implement this requirement.

Step 1

Build and configure the network according to the diagram; do not configure a routing protocol. The loopback interface on Vista will simulate an external network.

Use ping to test connectivity between directly connected neighbors. Note that Host A should not yet be able to ping Vista's loopback interface.

Step 2

Configure SanJose1 and Vista for static routing. ITA uses static routes to reach the outside world. Issue the following command:

```
SanJose1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

On the ISP's router (Vista), you must also configure a static route:

```
Vista(config)#ip route 10.0.0.0 255.0.0.0 192.168.1.2
```

When your static routes are configured, verify that Host A can ping Vista's loopback interface (172.16.1.1/24). Troubleshoot, as necessary.

Step 3

Configure SanJose1 to perform IP session filtering. Configure a reflexive access list, as shown:

```
SanJose1(config)#ip access-list extended FILTER-IN
SanJose1(config-ext-nacl)#permit ip any any reflect GOODGUYS
SanJose1(config-ext-nacl)#exit
SanJose1(config)#ip access-list extended FILTER-OUT
SanJose1(config-ext-nacl)#evaluate GOODGUYS
SanJose1(config-ext-nacl)#exit
SanJose1(config)#int e0
SanJose1(config-if)#ip access-group FILTER-IN in
SanJose1(config-if)#ip access-group FILTER-OUT out
```

These commands create two named access lists, FILTER-IN and FILTER-OUT. The FILTER-IN list monitors packet data as it is sent from a host into the E0 interface. The data is captured and put into a temporary list called GOODGUYS. The FILTER-OUT list looks at the data stored in GOODGUYS and monitors TCP/IP traffic being delivered out the E0 interface. Any TCP/IP traffic that originated from the 10.0.0.0 network is allowed to come back into the network.

Step 4

1. From Vista, ping the 10.0.0.11 host. At this point, Vista should not be able to ping 10.0.0.11. Why?

From Host A, ping Vista's loopback interface, 172.16.1.1. This ping should be successful.