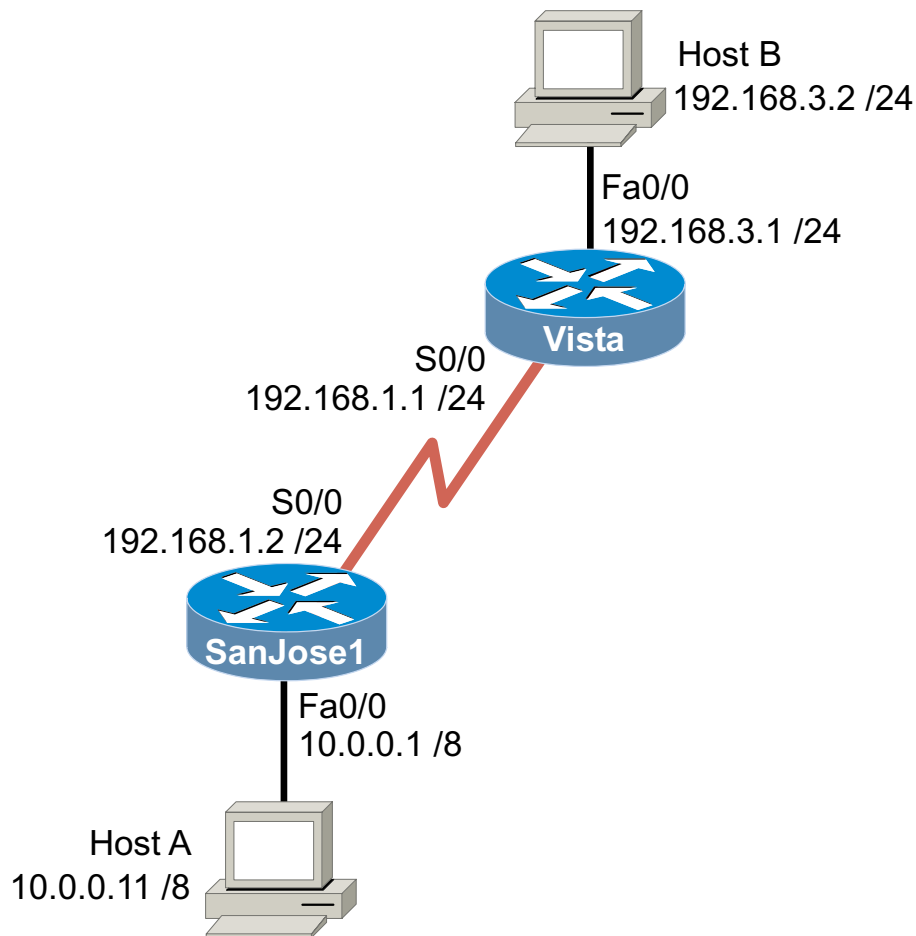


10.7.1 Lock-and-Key



Objective

In this lab, you configure a dynamic access list for lock-and-key security.

Scenario

International Travel Agency (ITA) maintains a secure network (10.0.0.0/8) behind SanJose1, which acts as a firewall. You have been transferred to a remote site in the company (192.168.3.0/24) that is not permitted through SanJose1's firewall. The company allows you to modify SanJose1's access list so that you, and you alone, can access the secured resources. Because you work at various stations at the remote site, you decide to configure lock-and-key so that you can get access from any IP address.

Step 1

Build and configure the network according to the diagram; use IGRP as the routing protocol. Be sure to enter the correct network statements.

Use ping and **show ip route** to test connectivity among all interfaces. Each router should have a complete routing table.

Step 2

Configure lock-and-key on SanJose1. You can assume that SanJose1 has a comprehensive access list set on Serial 0/0. But for the purposes of this lab, you need to configure only the portions of the list relevant to lock-and-key.

Because you expect to Telnet to SanJose1 to authenticate, you must permit Telnet access from your remote network. Also, SanJose1 will need to exchange routing updates with Vista, so you must be sure to permit IGRP. Enter the following commands on SanJose1:

```
SanJose1(config)#access-list 101 permit tcp 192.168.3.0 0.0.0.255
host 192.168.1.2 eq telnet
SanJose1(config)#access-list 101 permit igrp any any
SanJose1(config)#access-list 101 dynamic LETMEIN timeout 90 permit
ip 192.168.3.0 0.0.0.255 10.0.0.0 0.255.255.255
SanJose1(config)#username ernie password bert
SanJose1(config)#interface serial 0/0
SanJose1(config-if)#ip access-group 101 in
SanJose1(config-if)#line vty 0 4
SanJose1(config-line)#login local
SanJose1(config-line)#autocommand access-enable host timeout 2
```

Note that the dynamic access list statement contains the option **timeout 90**, which places an absolute limit on the amount of time that the temporary hole in the firewall can exist. After 90 minutes, you have to authenticate again, even if you've kept the connection busy with traffic.

The **autocommand** configuration is used to automate the process of creating a temporary access list entry. Upon authentication, SanJose1 executes the **access-enable** command and creates a temporary entry for your individual IP address. The **host** keyword prevents this temporary entry from including other members of your subnet. Finally, the **timeout 2** option configures the idle timeout to 2 minutes. If your connection is idle for more than two minutes, you have to authenticate again.

Step 3

Verify that the access list is working. From Host B, attempt to ping Host A, which is on the secure network. The ping to 10.0.0.11 should fail. If it doesn't, troubleshoot your access list.

When you have confirmed that the firewall on SanJose1 is preventing you from reaching 10.0.0.11, you can test the lock-and-key configuration.

From Host B, Telnet to SanJose1's Serial 0/0 (192.168.1.2). You are prompted to authenticate with a username and password. Enter the correct login information.

1. If SanJose1 is configured properly, you should be logged out of the Telnet session immediately. Why?

Again, from Host B, repeat your ping to 10.0.0.11. This ping should be successful.

2. If you don't send any more traffic, how much longer will this hole in the firewall exist?

3. Can other nodes on your subnet use this temporary hole? Why or why not?

Issue the **show ip access-lists** command on SanJose1.

4. What indications do you see that lock-and-key has been successfully configured?
-
