

Cyber Security in Class IPSec Exercise

Goal

Set up IPSec tunnel between a pair of IOS routers.

Requirements

In class you will create a tunnel between a pair of IOS routers. All traffic from the hosts in network to the other network should pass through the tunnel. You must configure IKE to get the tunnel set up. You may select the authentication mechanism and other protocols.

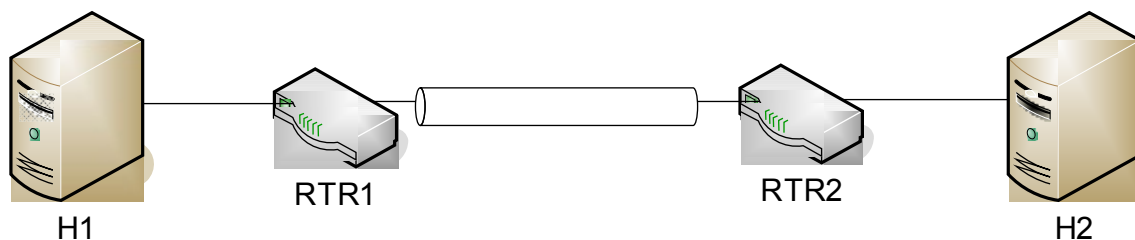


Figure 1: Tunnel scenarios

Things you will need to know

Relevant IOS documentation

You will be working on IOS 12.3. The security portions of the configuration guides are at

http://cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d583.html#wp999534. Of interest here are the chapters on “Configuring IPSec Network Security” and “Configuring Internet Key Exchange Security Protocol”.

Lab Configuration

The lab is configured with two pairs of routers. As in the firewall lab, you can telnet or ssh to the router from the corresponding inside hosts. The telnet and enable passwords are “class-test”. “config term” will take you to configuration mode. “show run” will show you the current running config. To ssh use “alice” and her standard password.

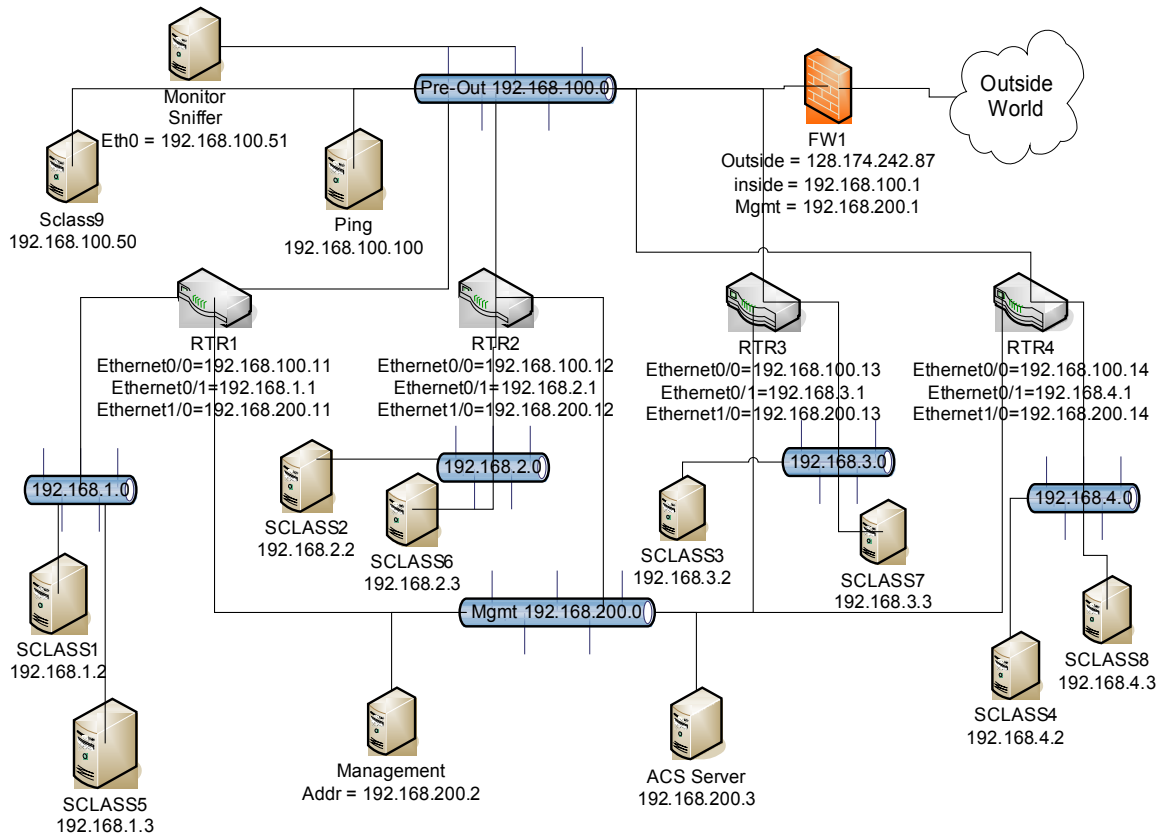


Figure 2: IPSec lab topology.

Storing Configs

The **management** machine is still at 192.168.200.2 and still running the ftp server. Unlike the firewall lab, the startup configs are stored in nvram on the router not on the ftp server. You can use the “copy” command as on the PIX to copy to and from the ftp server and the running-config. To store your current running config to the ftp server, issue:

```
copy running-config ftp://alice:alice-test@192.168.200.2/configs/skh-rtr.cfg
```

To bring your config back into member after rebooting issue

```
copy ftp://alice:alice-test@192.168.200.2/configs/skh-rtr.cfg running-config
```

Since we will be sharing hardware between groups, you should not store your changes to the NVRAM on the routers. **Do not “write mem” and do not save changes to nvram when prompted on “reload”**. “show run” shows the currently running config. When you are done working for the day, copy your config to the ftp server and reboot the router by issuing the reload command. When you come back to work on your lab some more

you can use the copy command to bring your config back into memory (after making sure the config is clean from the previous groups edits).

Testing Traffic

The machine **Monitor** (sitting where sclass9 used to be sitting) is plugged in a span port for the pre-out vlan on the switch. So running wireshark on Monitor will show all traffic passing over the Pre-Out vlan. Monitor has two ethernet cards, one dedicated to sniffing traffic (eth1) and another to act as a normal communicating interface for the machine (eth0).

On each of the tunnel routers you can issue the following command to look at the current state of the SA table:

```
show crypto engine connection active
```

The apache web server should be started on all of the linux boxes sitting behind the routers. Feel free to add more content. The web site files are at /var/www/html.

Logging and Debugging

To turn on and view logging:

- In exec mode, “debug crypto isakmp”, “debug radius”, “debug crypto ipsec”, “debug aaa authentication”
- In config mode, “logging on”, “logging buffer debug”, and “logging buffer 40000”
- In exec mode, “clear logging” to clear the buffers.
- Do your experiment
- “show logging” to step through your debug messages
- “show logging | redirect ftp://alice:alice-test@192.168.200.2/ipsec/skh-logging-output” will copy the buffered log messages for review on the ftp server.