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 and encryption mechanisms and other protocols.

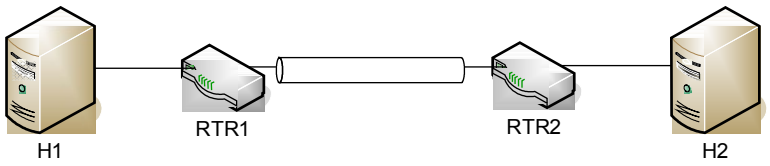

Figure 1: Tunnel scenario

Relevant IOS documentation

You will be working on IOS 12.3. The security portions of the configuration guides are at http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfencov.html Of interest here are the chapters on "Configuring IPSec Network Security" and "Configuring Internet Key Exchange Security Protocol".

The configuration language is similar to the PIX configuration language. One particular item to note is the difference in ACLs. The IOS ACLs can be named by number. Different number ranges have different semantics. For example low numbers are "standard" ACLs which only specify one network (the source or the destination depending on the usage). High numered ACLs and named ACLs are "extended" and have the same fields as the PIX ACLs.

Also when specifying a network in an IOS ACL, you specify a wildcard rather than a network mask. This is the inverse of the network mask. Specify a zero for bits that are fixed in the network address and a one for "don't care" bits. For example, 192.168.100.0 255.255.255.0 specifies the range 192.168.100.0-255 when used in a PIX ACL. You would specify 192.168.100.0 0.0.0.255 to get the same thing in an IOS ACL.

Lab Configuration

The lab is configured with three 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.

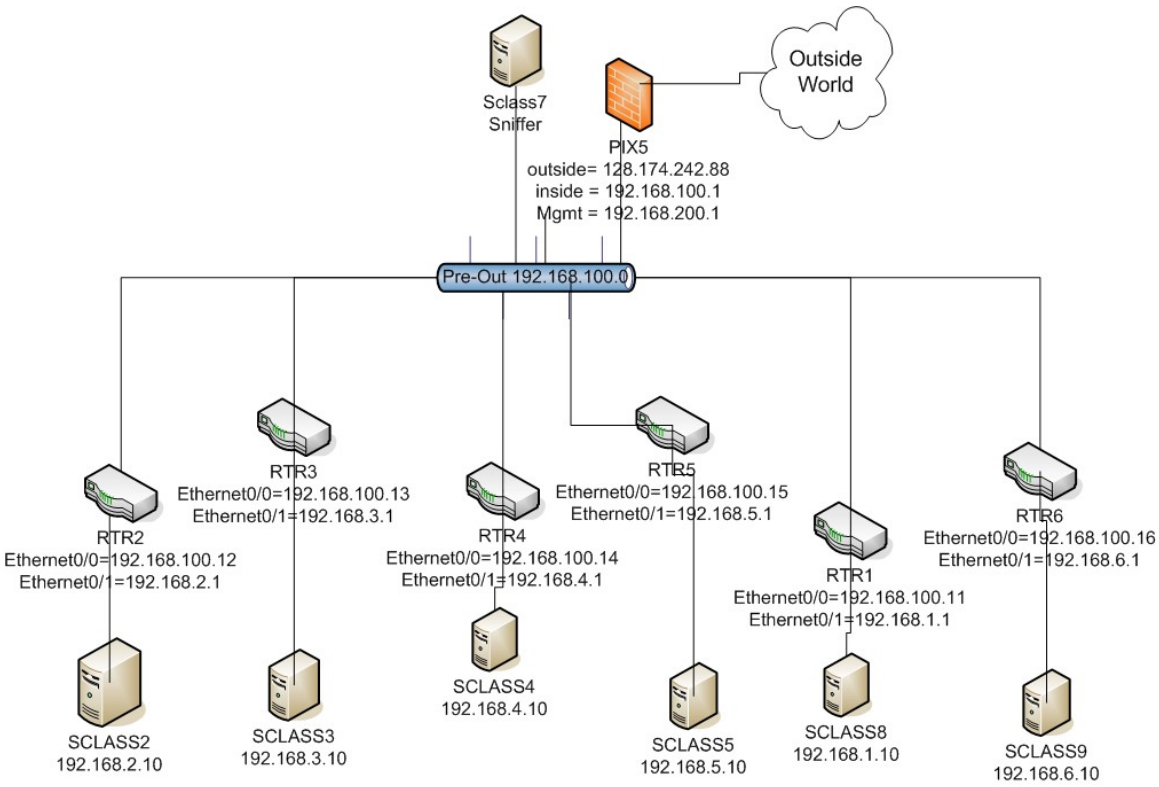

Figure 2: IPSec lab topology.

Testing Traffic and debugging

The machine **sclass7** is plugged in a span port for the pre-out vlan on the switch. So running wireshark on sclass7 will show all traffic passing over the Pre-Out vlan.

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

Free free to start the apache web server on the linux boxes sitting behind the routers. Feel free to add more content. The web site files are at /var/www/html.

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