

## Cyber Security Lab 5

### Due

April 6. For this lab you may work by yourself, or work with a partner and submit a single lab write up.

### Goal

Perform IPSec configuration on IOS routers.

### Requirements

Two IPSec tunnel scenarios need to be configured. Both scenarios will use IKE. You may select the authentication mechanism and other protocols.

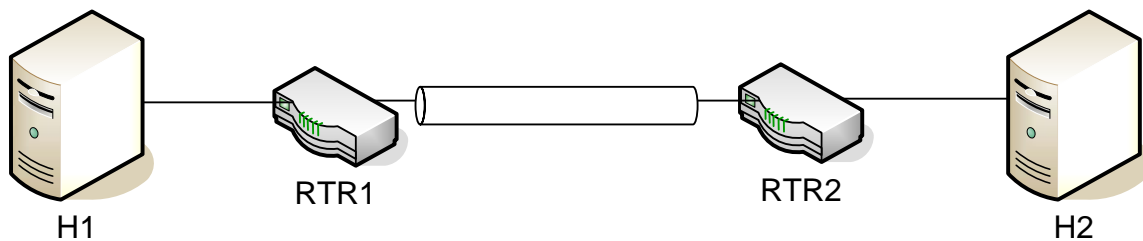


Figure 1: First scenario

The first is a symmetric scenario. Each peer's configuration is the inverse of the other. Logically there are two tunnels. The HTTP traffic to the peer's hosts should be authenticated but not encrypted, so it will go through the first tunnel. All other traffic should be authenticated and encrypted and will go through the second tunnel.

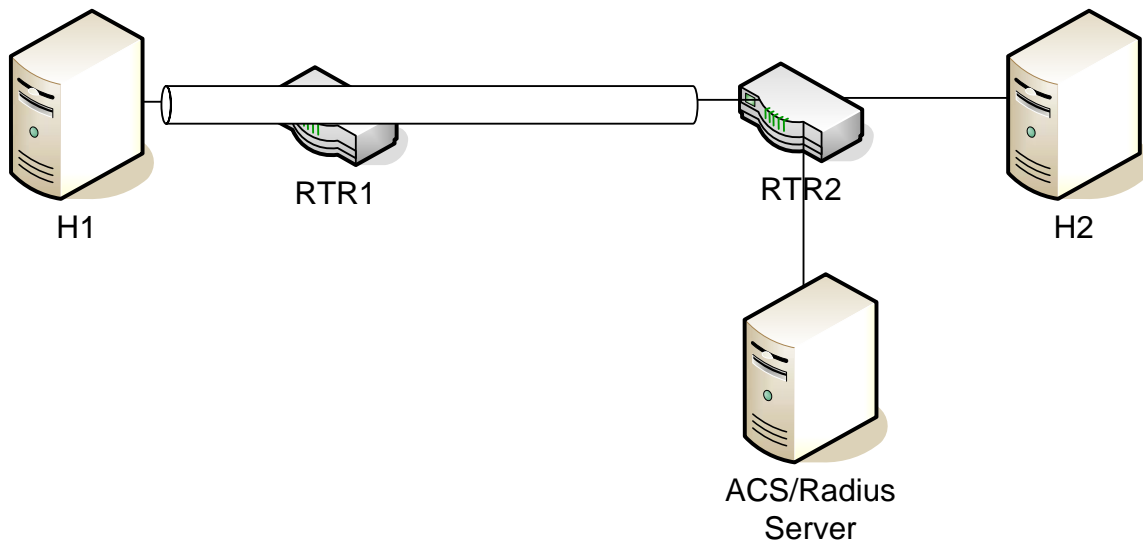


Figure 2: Second scenario.

The second is an asymmetric scenario. One router serves as the tunnel gateway. One host runs the VPN Client software to connect to the tunnel router, authenticate the user,

and dynamically negotiate its inside tunnel address. To configure the tunnel router, you will need to use the “mode configuration” and “xauth” commands described in the IKE handout.

The client running on the host will be prompted to authenticate himself. Assuming the authentication is successful, the resulting tunnel should get a tunnel address assigned by the tunnel gateway. This address should be on the subnet of the router’s local machines (e.g., on the same subnet as H2 in this case).

The ACS server will be configured with the fixed set of users from previous labs: alice, bob, carol, dave, ellen, and gus. Each user’s password is their user ID plus “-test”.

## **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](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”. We will walk through a simple static IPSec configuration during class on March 28 that uses the steps in these chapters.

### ***Lab Configuration***

The lab will be configured with two pairs of routers. As in the firewall lab, you can telnet to the router from the corresponding inside host. 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.

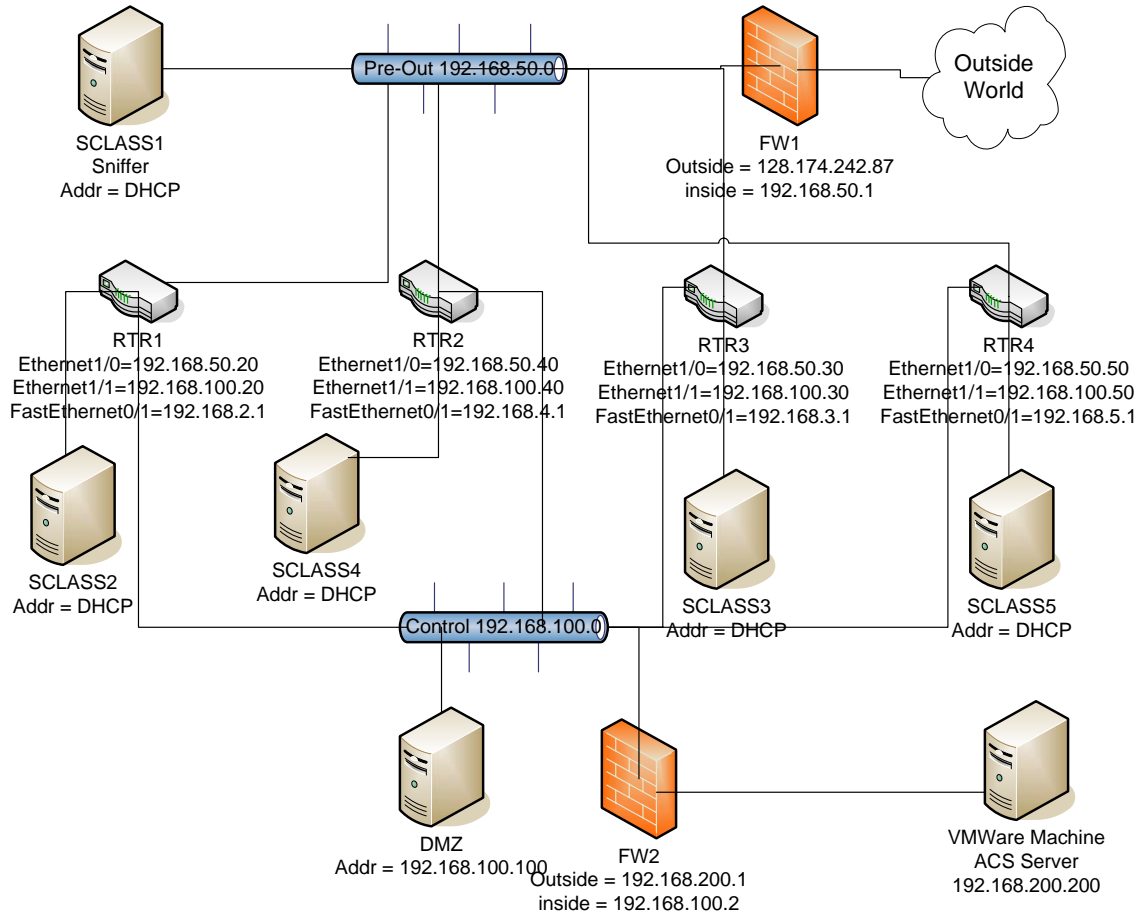


Figure 3: Final IPsec lab topology with two pairs of routers.

## Storing Configs

We will be using the tftp server at 192.168.100.100 to persistently store our configurations. Do not “write mem” and do not save changes to nvram when prompted on “reload”. “show run” shows the currently running config.

The “copy” command both stores configs to the tftp server and loads them back into memory. To store your current running config to the tftp server, first make sure the file exists and is world writeable. Then issue:

```
copy running-config tftp://192.168.100.100/ipsec/my-config
```

To bring your config back into member after rebooting issue

```
copy tftp://192.168.100.100/ipsec/my-config running-config
```

## Testing Traffic

Sclass5 is plugged in a span port for the pre-out vlan on the switch. So running ethereal on sclass5 will show all traffic passing over the Pre-Out vlan. Because ports can either monitor or be sources and sinks of communication in this model of switch, sclass5 cannot communicate with other machines. It can only monitor traffic.

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
```

## **ACS Server**

The second part of lab 5 requires configuring an IOS router to act as a IPSec tunnel endpoint for a VPN Client. The configuration example in [http://cisco.com/en/US/tech/tk583/tk372/technologies\\_configuration\\_example09186a00800946b7.shtml](http://cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a00800946b7.shtml) is very close to what we are aiming for.

You should not need to configure the ACS server directly. You can access the administrative interface through the URL <http://192.168.100.110:2002> if you want to look at the definitions or view the reports. Nor should you need to configure the VPN client connection profile. You should only need to configure the VPN gateway router.

User names and credentials are configured in the AAA server. These are our standard users, alice, bob, carol, dave, ellen, and gus with the corresponding passwords for <username>-test.

The router clients need to be configured with the key “class-test” to authenticate to the AAA server. The AAA server is configured to speak radius with the router clients.

## **VPN Client**

The VPN Client should be installed on the systems. It should have a single connection entry installed to test the connection with its peer router. There is not much one can configure on the VPN client connection.

- Authorizing as group “3000client” with shared secret “12345678”
- Host name with is the outside interface address of the corresponding router

You cannot configure the phase 1 or phase 2 transforms. The VPN Client submits most combinations as options. If you turn enable debugging on the router, the debug messages will show the details.

The only major caveat for proposal and transform selection is:

- Specify “group 2” for phase 1 or isakmp negotiation.
- Do not specify pfs for phase 2 or ipsec negotiation.

## **Router Configuration**

On the router you will need to configure the following elements. The router config in [http://cisco.com/en/US/tech/tk583/tk372/technologies\\_configuration\\_example09186a00800946b7.shtml](http://cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a00800946b7.shtml) is a good guideline to the specific commands.

- Connection to the AAA server
- Indication that users should authenticate against the AAA server
- Indication that groups (the VPN client machine itself) should authorize against a locally defined group policy.

- Definition of the local group policy named “3000client” with the key “12345678”.
- Define a local IP pool. The addresses in this pool will be assigned to the client traffic after it is decrypted. The addresses should \*not\* be in the target network, e.g., for router 1, the addresses should not be in the 192.168.1.0/24 network.
- Define the phase 1 isakmp policy.
- Define the phase 2 transform sets.
- Define the dynamic crypto map that specifies the transform set.
- Define the static crypto map that links to the dynamic crypto map.
- On the static crypto map specify the client authentication, group authorizations, and mode config.

Additional information about mode configuration and xauth can be found in the IKE configuration guide. Additional information about dynamic crypto maps can be found in the IPsec configuration guide.

## Logging and Debugging

To turn on and view logging:

- In global 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 global mode, “clear logging” to clear the buffers.
- Do your experiment
- “show logging” to step through your debug messages
- “show logging | redirect tftp://192.168.200.200/ipsec/skh-logging-output” will copy the buffered log messages for review on the tftp server.

## Hand-in Items

1. Description of the design of the first scenario, e.g., protocols used and basic design.
2. The pair of configuration files for the routers in the first scenario.
3. Description of the design of the second scenario, e.g., protocols used and basic design.
4. The configuration file for the router in the second scenario.
5. Ethereal capture of tunneled traffic.