

Cyber Security IPSec Lab

Due

Thursday, February 21. For this lab you may work by yourself, or work with a partner and submit a single lab write up.

Goal

Configure IPSec tunnels between a PC and a router.

Requirements

In class you configured a symmetric router to router IPSec tunnel. For your lab assignment, you will configure a user authenticated IPSec tunnel between a PC and a router.

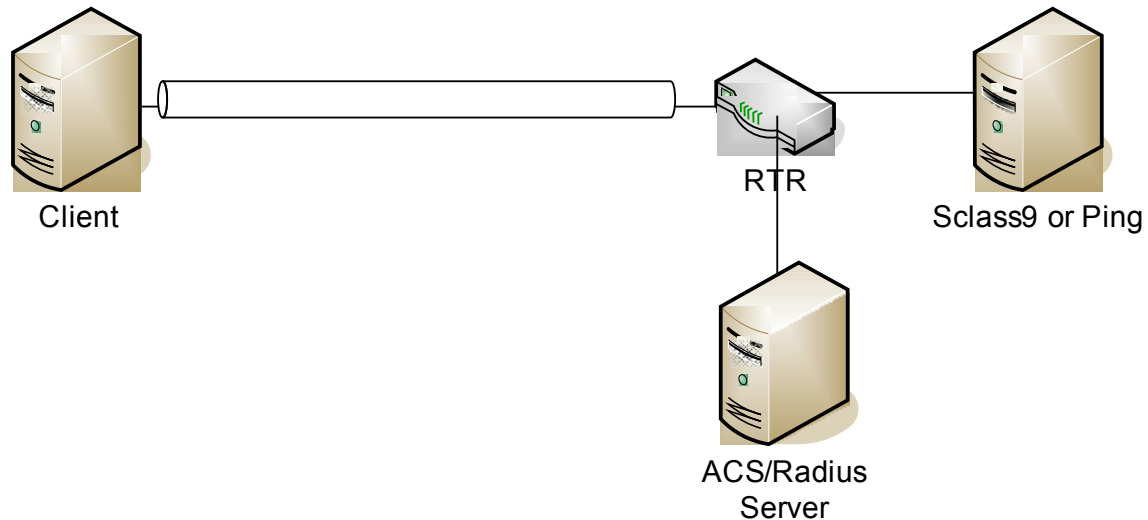


Figure 1: PC to router tunnel.

The 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 not be on the subnet of the router’s local machines (e.g., on the same subnet as Sclass9 or Ping 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. Of interest here are the chapters on “Configuring IPsec Network Security” and “Configuring Internet Key Exchange Security Protocol”. You used these writeups during the lab exercise on February 12.

ACS Server

The lab 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 is very close to what we are aiming for.

The Radius server, running the Cisco Access Control Server (ACS) software, is on 192.168.200.3. You should not need to configure the ACS server directly. You can access the administrative interface by accessing the ACS machine from the KVM switch and accessing the URL <http://localhost:2002>. From here you can look at the definitions or view the reports.

The ACS client definitions (the routers) show up under the network tab. There is also a reports tab. I have not looked at this with traffic. I would be interested to hear what is there. It could be that we are not enabled enough accounting/auditing to generate interesting reports, but it would be interesting to know.

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 PC's. 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 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. Something in the 192.168.10.0/24 network would work. *Extra points if you can explain why this is the case in your lab writeup.*
- 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.
- Once you enter the “aaa new-model” command, the router will expect to have a local administrative user defined. Enter “username root password 0 class-test” to define an administrative user root with password class-test. When telneting in, you will be prompted for both a user name and password.

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.

Hand-in Items

1. Description of the design of the client/gateway IPsec configuration, e.g., protocols used and basic design.
2. The configuration file for the router.
3. Wireshark capture of tunneled traffic.
4. What are the benefits and weaknesses of a client to gateway IPsec approach versus a client behind a pair of gateways?
5. What is the weak point of the client IPsec tunnel? If you were attacking this configuration, how would you start?