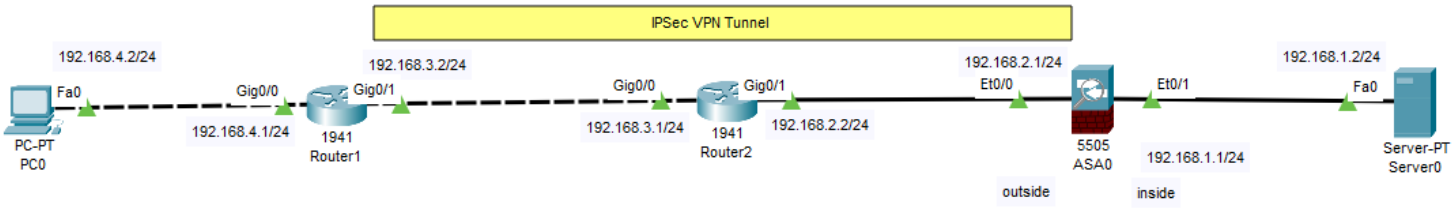
Cisco IPSec VPN Lab Assignment (version 1.1)

Using Cisco Packet Tracer, create a network comprising of two routers, one Cisco ASA 5505 firewall, one computer, and one web server as shown below. Make sure that port labels are shown (via Options > Preferences > Always Show Port Labels)



Configure the network interfaces of all devices with IP addresses and subnet masks shown. Make sure that the router interfaces are enabled via CLI "no shutdown" command. Router configurations can be saved via "write memory" CLI command.

On Router1, add a default static route so that traffic destined to unknown destinations will be forwarded to Router2.

On ASA 5505 firewall, add a default static route so that traffic destined to unknown destinations will be forwarded to Router2.

On Router2, add a static route so that traffic destined to network 192.168.4.0/24 will be forwarded to Router1.

From PC0, verify that you can ping IP address of Router1, Router2, and outside interface of ASA5505 firewall.

1. Submit a screenshot of your Packet Tracer network topology. Each network interface should be labelled with port number and IP address.

2. Submit a screenshot of output of a successful traceroute (tracert) from command prompt of PC0 to ASA5505 firewall's IP 192.168.2.1 (Note that you may need to configure an access list on firewall to permit icmp traffic from PCO to 192.168.2.1)

Configure a site-to-site IPSec VPN tunnel between Router1 and the ASA5505 firewall. The tunnel should permit all traffic between PC0 and Server0. Consult YouTube videos and other website for sample configurations.

On Router1, if "show version" shows that security license is disabled, you will need to run "license boot module c1900 technology-package securityk9" to activate security, "copy run start" to save configuration, and "reload" to reboot the router.

- Use "crypto isakmp key" command to define preshare key and IP address of other endpoint of tunnel.
- Use "crypto isakmp policy" command to define Phase1 security parameters (authentication, encryption, DH group#, hash algorithms)
- Use "crypto ipsec " command to specify transform set security parameters(encryption algorithm)
- Create ACL to permit all traffic between PC0 and Server0
- Define a crypto map to bind together phase1 and phase2 security parameters, ip address of peer, and ACL
- Apply crypto map to the interface on Router1 that corresponds to the VPN tunnel endpoint.

On ASA5505 firewall:

- Use "crypto ikev1" command to configure IKE phase1 policy (authentication, encryption, DH group#, and hash algorithms)
- Use "tunnel-group" command to create pre-share key for authentication of other tunnel end-point.
- Create ACL to define traffic that will be inserted into VPN tunnel
- Use "crypto ipsec" command to configure IPSec (IKE phase2) security parameters
- Use "crypto map" command to bind together IKE phase1 and IKE phase2 security parameters, ip address of peer, and ACL

- Apply crypto map to outside interface of ASA5505 interface

Generate some traffic between PC0 and Server0. Verify that IPSec VPN tunnel is up and the traffic between PC0 and Server0 is inserted into the tunnel. If IKE phase1 and IKE phase 2 security associations were not successfully created, you will need to troubleshoot your network configuration (try running "debug crypto isakmp" and "debug crypto ipsec" on Router1). Note that the authentication scheme, encryption algorithm, DH group number, and hash algorithm must match at the two tunnel endpoints (Router1 and ASA5505 firewall).

3. Submit a screenshot of a successful traceroute from PC0 to Server0 and another screenshot of PC0 browser successfully accessing web server http://192.168.1.2

4. Submit a screenshot of output of "show crypto isakmp sa" on Router1 CLI after IKE phase1 SA has formed.

5. Submit a screenshot of output of "show crypto ipsec sa" on Router1 CLI . Output should show information regarding VPN tunnel endpoints as well as the number of packets encapsulated and encrypted.

6. Submit a screenshot of output of "show crypto isakmp sa" on ASA5505 firewall CLI

7. Submit a screenshot of output of "show crypto ipsec sa" on ASA5505 firewall CLI

8. Submit a screenshot of output of a decoded ISAKMP packet traversing IPSec VPN tunnel (capture & decode packets in simulation mode). **Circle** the value of the transport layer protocol and port number that ISAKMP use.

9. Submit a screenshot of output of a decoded IPSec packet traversing IPSec VPN tunnel (capture & decode packets in simulation mode). **Circle** the value of the IP protocol number that IPSec uses.

10. Submit a copy of entire configuration file (output of "show run") of both the firewall and Router1