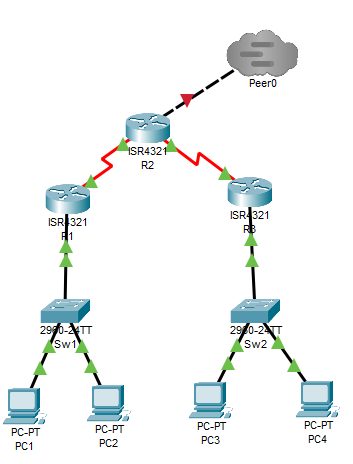
Performance Assessment 2– VPN tunneling protocols and IPsec

In this lab you will be using Packet Tracer. You will be using your network you configured in the previous lab.

Your network will a class B network based on a number assigned by your professor, which you will be using for the duration of the class. In the lab anytime you see an underline you should fill in this number.

**Student network: 10.\_\_\_\_.0.0/16**



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **System** | **Port** | **Connect To** | **IP address** | **Subnet Mask** | **Clock Rate** |
| R1 | G0/0/0.10 | Sw1 | 10.\_\_\_.1.1 | 255.255.255.192 | 60 users |
|  | G0/0/0.20 | Sw1 | 10.\_\_\_.1.65 | 255.255.255.224 | 30 users |
|  | Se0/1/0 | R2 | 10.\_\_\_.5.1 | 255.255.255.252 | 500000 |
| R2 | G0/0/0 | Tier1 | 11.0.0.\_\_\_ | 255.255.255.0 |  |
|  | Se0/1/0 | R3 | 10.\_\_\_.5.5 | 255.255.255.252 | 500000 |
|  | SE0/1/1 | R1 | 10.\_\_\_.5.2 | 255.255.255.252 |  |
| R3 | G0/1/0.10 | Sw2 | 10.\_\_\_.2.1 | 255.255.255.224 | 28 Users |
|  | G0/1/0.20 | Sw2 | 10.\_\_\_.2.33 | 255.255.255.240 | 12 Users |
|  | SE0/1/1 | R2 | 10.\_\_\_.5.6 | 255.255.255.252 |  |

**Task 1 – IPSec VPN Tunnel**

Site-to-Site IPSec VPN tunnels are used to allow secure transmission of data, voice and video between two sites. The VPN tunnel is created between two routers which encrypt and decrypt the data over the network. This makes the data inaccessible between the two routers and greatly reduces the chance of losing data over the network while it is being transmitted.

We will begin by configuring ISAKMP (Internet Security Association and Key Management Protocol) which allows us to setup and exchange keys between the two routers.

On R1 type the following

R1(config)# crypto isakmp policy 1

R1(config-isakmp)# encryption 3des

R1(config-isakmp)# hash md5

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# group 2

R1(config-isakmp)# lifetime 86400

R1(config)# crypto isakmp key firewallcx address 10.\_\_\_.5.6

R1(config)# ip access-list extended VPN-TRAFFIC

R1(config-ext-nacl)# permit ip 10.\_\_\_.1.0 0.0.0.63 10.\_\_\_.2.0 0.0.0.31

R1(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac

R1(config)# crypto map CMAP 10 ipsec-isakmp

R1(config-crypto-map)# set peer 10.\_\_\_.5.6

R1(config-crypto-map)# set transform-set TS

R1(config-crypto-map)# match address VPN-TRAFFIC

R1(config)# interface s0/1/0

R1(config-if)# crypto map CMAP

Take a screenshot of your show running-config for the R1 router.

Now configure R3

R3(config)# crypto isakmp policy 1

R3(config-isakmp)# encryption 3des

R3(config-isakmp)# hash md5

R3(config-isakmp)# authentication pre-share

R3(config-isakmp)# group 2

R3(config-isakmp)# lifetime 86400

R3(config)# crypto isakmp key firewallcx address 10.\_\_\_.5.1

R3(config)# ip access-list extended VPN-TRAFFIC

R3(config-ext-nacl)# permit ip 10.\_\_\_.2.0 0.0.0.31 10.\_\_\_.1.0 0.0.0.63

R3(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac

R3(config)# crypto map CMAP 10 ipsec-isakmp

R3(config-crypto-map)# set peer 10.\_\_\_.5.1

R3(config-crypto-map)# set transform-set TS

R3(config-crypto-map)# match address VPN-TRAFFIC

R3(config)# interface s0/1/1

R3(config- if)# crypto map CMAP

Take a screenshot of your show running-config for the R3 router.

Ping from PC1 to PC4 to verify you can reach across the encrypted channel. Take a screenshot.

Go back to R1 and configure NAT

R1(config)# ip nat inside source list 100 interface s0/1/0 overload

R1(config)# access-list 100 deny ip 10.\_\_\_.1.0 0.0.0.63 10.\_\_\_.2.0 0.0.0.31

R1(config)# access-list 100 permit ip 10.\_\_\_.1.0 0.0.0.63 any

Configure R3 for NAT

R3(config)# ip nat inside source list 100 interface s0/1/1 overload

R3(config)# access-list 100 deny ip 10.\_\_\_.2.0 0.0.0.31 10.\_\_\_.1.0 0.0.0.63

R3(config)# access-list 100 permit ip 10.\_\_\_.2.0 0.0.0.31 any

Ping from PC2 to PC3 to verify you can reach across the encrypted NAT channel. Take a screenshot.

**Deliverables**

* Screenshot of entire running-config for the R1 router
* Screenshot of entire running-config for the R3 router
* Screenshot of ping from PC1 to PC4
* Screenshot of ping from PC2 to PC3

PASTE SCREENSHOTS BELOW

**Task 2 – Set up an encrypted channel to your Tier1 provider**

Often Internet providers will set up secure tunnels for their clients.

On R2 type the following

R2(config)# crypto isakmp policy 1

R2(config-isakmp)# encryption 3des

R2(config-isakmp)# hash md5

R2(config-isakmp)# authentication pre-share

R2(config-isakmp)# group 2

R2(config-isakmp)# lifetime 86400

R2(config)# crypto isakmp key firewallcx address 11.0.0.1

R2(config)# ip access-list extended VPN-TRAFFIC

R2(config-ext-nacl)# permit ip 10.0.0.0 0.255.255.255 11.0.0.0 0.0.0.255

R2(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac

R2(config)# crypto map CMAP 10 ipsec-isakmp

R2(config-crypto-map)# set peer 11.0.0.1

R2(config-crypto-map)# set transform-set TS

R2(config-crypto-map)# match address VPN-TRAFFIC

R2(config)# interface g0/0/0

R2(config-if)# crypto map CMAP

On Tier1 router type the following

R1(config)# crypto isakmp policy 1

R1(config-isakmp)# encryption 3des

R1(config-isakmp)# hash md5

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# group 2

R1(config-isakmp)# lifetime 86400

R1(config)# crypto isakmp key firewallcx address 11.0.0.\_\_\_

R1(config)# ip access-list extended VPN-TRAFFIC

R1(config-ext-nacl)# permit ip 11.1.1.0 0.0.0.255 11.0.0.0 0.0.0.255

R1(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac

R1(config)# crypto map CMAP 10 ipsec-isakmp

R1(config-crypto-map)# set peer 11.0.0.\_\_\_

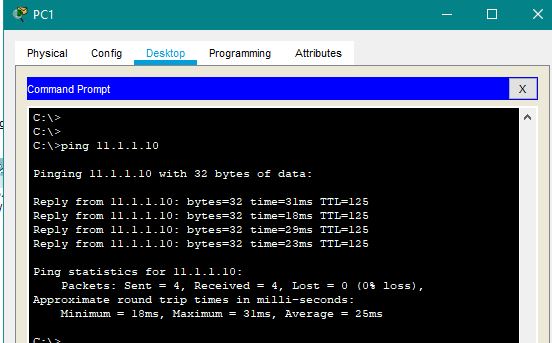
R1(config-crypto-map)# set transform-set TS

R1(config-crypto-map)# match address VPN-TRAFFIC

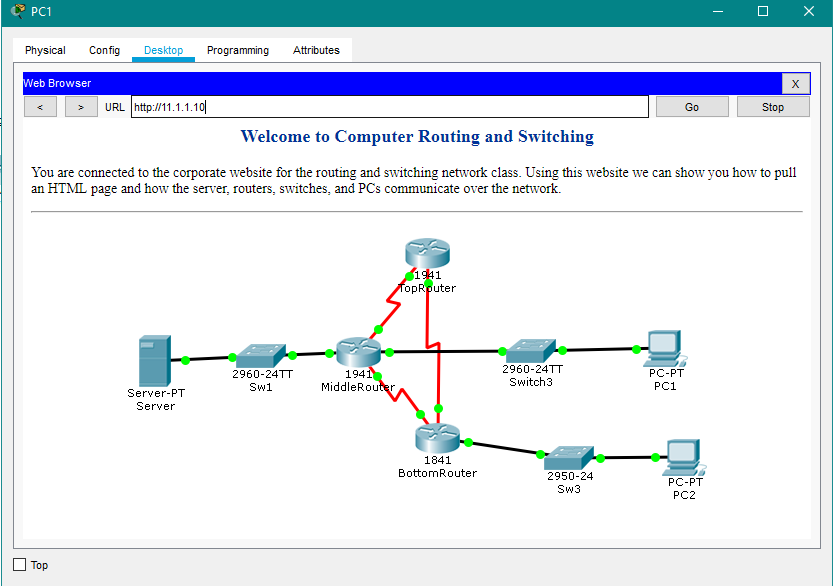
R1(config)# interface f0/0

R1(config-if)# crypto map CMAP

Ping from PC1 to the Tier1 Internet Server. Take a screenshot.



Pull a webpage from PC1 to the Tier1 Internet Server. Take a screenshot.



**Deliverables**

* Screenshot ping from PC1 to the Tier1 Internet Server
* Screenshot of webpage from the Tier1 Internet Server

PASTE SCREENSHOTS BELOW