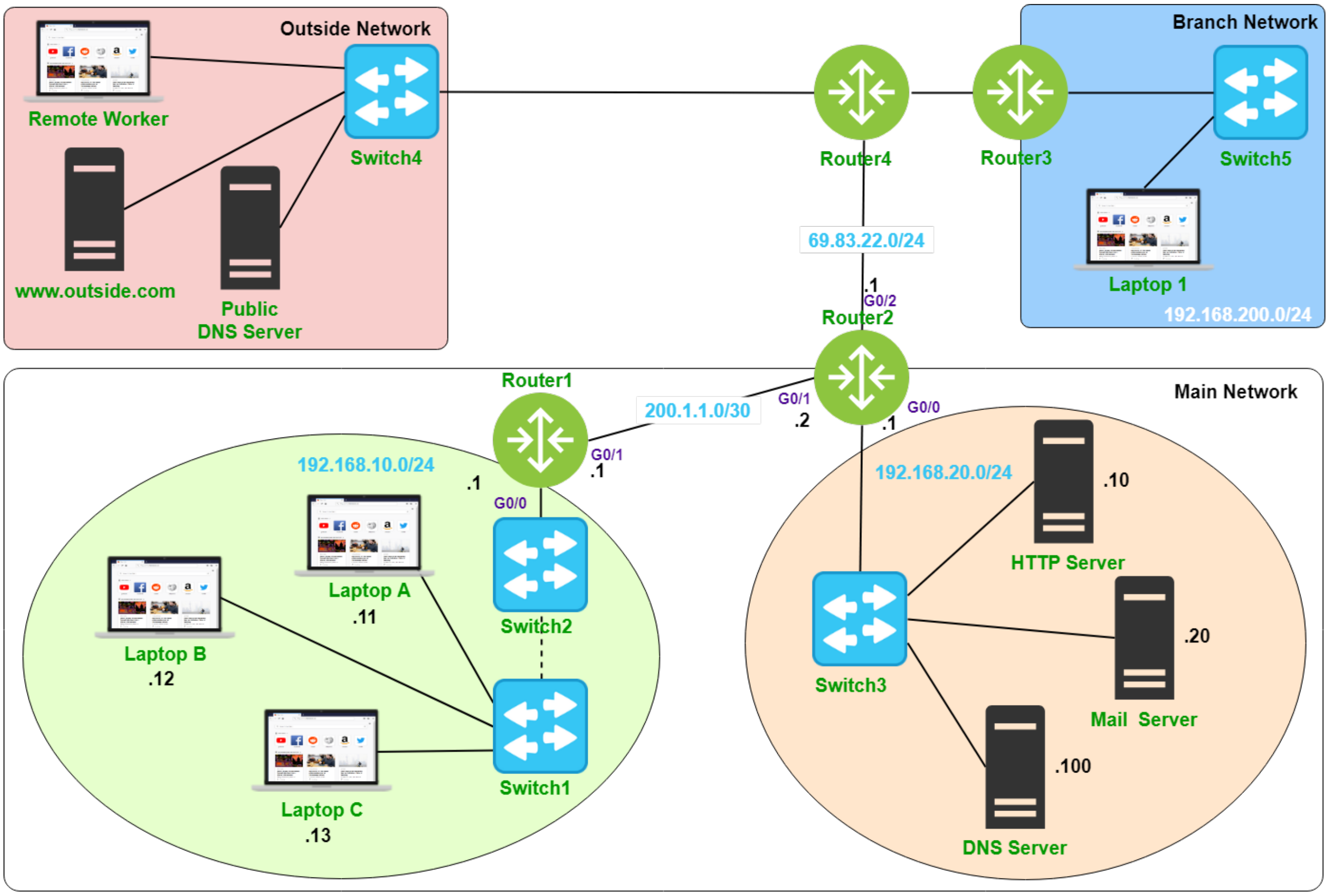
Lab 7 – IPsec VPN

Lab Topology and Learning Goals



VPNs are used to connect branch offices and remote workers to corporate resources. VPN tunnels use encryption and hashing to provide confidentiality, integrity and authentication to data transferred across the tunnel. In this lab, we create both a remote access and site-to-site IPsec VPN.

Lab Instructions and Required Resources

- Complete this lab in the Packer Tracer file: **INFO-6078 – Lab 7 – IPsec VPN.pkz**
- Take Lab Quiz: **Lab 7 - Requires Respondus LockDown Browser**

IPsec Remote Access VPN

A remote access VPN allows remote workers to access corporate resources over public networks such as the internet. Remote access VPNs generally require additional software and/or settings to be configured on the remote user's device.

Test Connection to the Data Centre from the Remote Locations

On the **Remote Worker** Laptop, open the **Command Prompt** and send a ping to the data centre IP address **192.168.20.1**. Does the ping succeed? Why is this so?

Modify the License on Router2

Activate the security technology package license to enable IPsec VPN support

```
Router2(config)# license boot module c2900 technology-package securityk9
```

Accept the EULA by typing yes

Save the configuration and reboot the router to load the features

```
Router2# copy run start
Router2# reload
```

Configure AAA Settings for Remote Access

```
Router2(config)# aaa new-model
Router2(config)# aaa authentication login RAVPN1 local
Router2(config)# aaa authorization network RAVPN2 local
Router2(config)# username remoteuser1 password cisco
```

Create an ISAKMP Policy for Phase 1 Negotiation

```
Router2(config)# crypto isakmp policy 10
```

View the available encryption, hashing, authentication and Diffie Hellman group types

```
Router2(config-isakmp)# encryption ?
Router2(config-isakmp)# hash ?
Router2(config-isakmp)# authentication ?
Router2(config-isakmp)# group ?
```

Configure the policy to use 3des for encryption, md5 for hashing and Diffie Hellman group 2

```
Router2(config-isakmp)# encryption 3des
Router2(config-isakmp)# hash md5
Router2(config-isakmp)# authentication pre-share
Router2(config-isakmp)# group 2
Router2(config-isakmp)# exit
```

Create a Pool of IP Addresses for VPN Users

```
Router2(config)# ip local pool IPsecPool 192.168.99.1 192.168.99.20
```

Configure Group Settings and Parameters that are Passed to Client Devices

```
Router2(config)# crypto isakmp client configuration group FanshaweVPN
Router2(config-isakmp-group)# key cisco123
Router2(config-isakmp-group)# pool IPsecPool
Router2(config-isakmp-group)# exit
```

Normally the group settings would configure DNS settings; however, Packet Tracer does not include this function

Configure the Phase 2 Policy with Settings for Authentication and Data Encryption

```
Router2(config)# crypto ipsec transform-set set1 esp-3des esp-md5-hmac
```

Configure a Dynamic Crypto Map and Specify the Allowed Transform Set

```
Router2(config)# crypto dynamic-map map1 10
Router2(config-crypto-map)# set transform-set set1
Router2(config-crypto-map)# reverse-route
Router2(config-crypto-map)# exit
```

Configure a Crypto Map to Bind Previously Configured Parameters Together

```
Router2(config)# crypto map map1 client configuration address respond
Router2(config)# crypto map map1 client authentication list RAVPN1
Router2(config)# crypto map map1 isakmp authorization list RAVPN2
Router2(config)# crypto map map1 10 ipsec-isakmp dynamic map1
```

Apply the Crypto Map to the Exterior Interface

```
Router2(config)# interface gigabitEthernet 0/2
Router2(config-if)# crypto map map1
```

Connect to the VPN from the Remote Worker Laptop

On the remote worker laptop, open the **VPN** settings an connect to the VPN with the following settings:

GroupName:	FanshaweVPN
Group Key:	cisco123
Host IP:	69.83.22.1
Username:	remoteuser1
Password:	cisco

If the VPN does not connect, troubleshoot as necessary

Test the VPN Connection

- Close the **VPN** settings and open the **Web Browser**
- Navigate to **www.fanshawe.ca**, does the page load?
- Navigate to **192.168.20.10**, does the page load now?

Close and reopen Packet Tracker before configuring site-to-site VPN

IPsec Site-to-Site VPN

Site-to-site VPNs are used to connect entire locations to one another over public networks. Site-to-site VPNs are implemented on infrastructure devices and are transparent to user's devices (no configuration is needed on the device).

Test Connection to the Data Centre from the Remote Locations

On **Laptop1** in the branch office, open the **Command Prompt** and send a ping to the data centre IP address **192.168.20.1**. Does the ping succeed? Why is this so?

Identify Interesting Traffic for IPsec on Router2

A site-to-site VPN tunnel will be created as needed when traffic deemed as interesting (traffic destined for the destination network) is encountered

On Router2, identify interesting traffic for the VPN

```
Router2(config)# access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
Router2(config)# access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.200.0 0.0.0.255
```

Create an ISAKMP Policy for Phase 1 Negotiation

```
Router2(config)# crypto isakmp policy 20
Router2(config-isakmp)# encryption 3des
Router2(config-isakmp)# hash md5
Router2(config-isakmp)# authentication pre-share
Router2(config-isakmp)# group 2
Router2(config-isakmp)# exit
Router2(config)# crypto isakmp key cisco123 address 194.56.44.2
```

Configure the Phase 2 Policy

Create a transform-set for IPsec

```
Router2(config)# crypto ipsec transform-set IPsec-StS esp-3des esp-md5-hmac
```

Configure a Crypto Map to Bind Previously Configured Parameters Together

```
Router2(config)# crypto map map2 20 ipsec-isakmp
Router2(config-crypto-map)# set peer 194.56.44.2
Router2(config-crypto-map)# set transform-set IPsec-StS
Router2(config-crypto-map)# match address 101
Router2(config-crypto-map)# exit
```

Apply the Crypto Map to the Exterior Interface

```
Router2(config)# interface gigabitEthernet 0/2
Router2(config-if)# crypto map map2
```

Modify the License on Router3

Activate the security technology package license to enable IPsec VPN support

```
Router3(config)# license boot module c2900 technology-package securityk9
```

Accept the EULA by typing yes

Reboot the router to load the features

```
Router3# copy run start
Router3# reload
```

Identify Interesting Traffic for IPsec on Router3

```
Router3(config)# access-list 101 permit ip 192.168.200.0 0.0.0.255 192.168.10.0 0.0.0.255
Router3(config)# access-list 101 permit ip 192.168.200.0 0.0.0.255 192.168.20.0 0.0.0.255
```

Create an ISAKMP Policy for Phase 1 Negotiation

```
Router3(config)# crypto isakmp policy 20
Router3(config-isakmp)# encryption 3des
Router3(config-isakmp)# hash md5
Router3(config-isakmp)# authentication pre-share
Router3(config-isakmp)# group 2
Router3(config-isakmp)# exit
Router3(config)# crypto isakmp key cisco123 address 69.83.22.1
```

Configure the Phase 2 Policy

Create a transform-set for IPsec

```
Router3(config)# crypto ipsec transform-set IPsec-StS esp-3des esp-md5-hmac
```

Configure a Crypto Map to Bind Previously Configured Parameters Together

```
Router3(config)# crypto map map2 20 ipsec-isakmp
Router3(config-crypto-map)# set peer 69.83.22.1
Router3(config-crypto-map)# set transform-set IPsec-StS
Router3(config-crypto-map)# match address 101
Router3(config-crypto-map)# exit
```

Apply the Crypto Map to the Exterior Interface

```
Router3(config)# interface gigabitEthernet 0/0
Router3(config-if)# crypto map map2
```

Test the VPN Connection

- On **Laptop 1**, open the **Command Prompt** and **ping 192.168.10.11**; is the ping successful?
- Again, on **Laptop 1**, open the **Web Browser** and navigate to **www.fanshawe.ca**, does the page load? Why is this so?