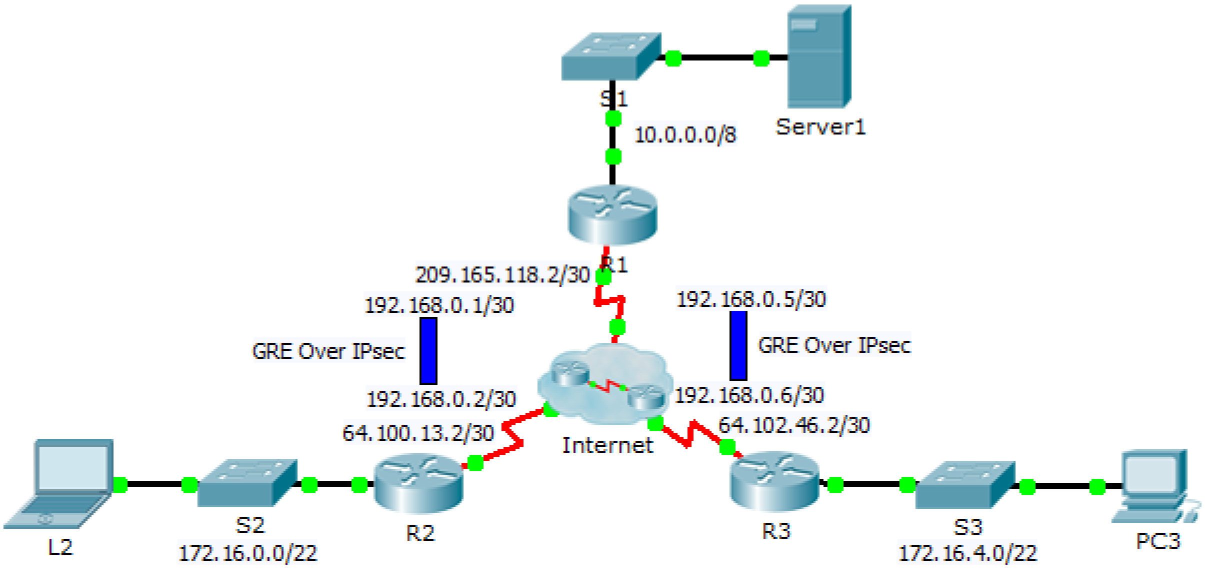
Packet Tracer – Configuring GRE over IPsec (Optional)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	10.0.0.1	255.0.0.0	N/A
	S0/0/0	209.165.118.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.1	255.255.255.252	N/A
	Tunnel 1	192.168.0.5	255.255.255.252	N/A
R2	G0/0	172.16.0.1	255.255.252.0	N/A
	S0/0/0	64.100.13.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.2	255.255.255.252	N/A
R3	G0/0	172.16.4.1	255.255.252.0	N/A
	S0/0/0	64.102.46.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.6	255.255.255.252	N/A
Server1	NIC	10.0.0.2	255.0.0.0	10.0.0.1
L2	NIC	172.16.0.2	255.255.252.0	172.16.0.1
PC3	NIC	172.16.4.2	255.255.252.0	172.16.4.1

Objectives

Part 1: Verify Router Connectivity

Part 2: Enable Security Features

Part 3: Configure IPsec Parameters

Part 4: Configure GRE Tunnels over IPsec

Part 5: Verify Connectivity

Scenario

You are the network administrator for a company which wants to set up a GRE tunnel over IPsec to remote offices. All networks are locally configured, and need only the tunnel and the encryption configured.

Part 1: Verify Router Connectivity

Step 1: Ping R2 and R3 from R1.

a. From **R1**, ping the IP address of S0/0/0 on **R2.**

b. From **R1**, ping the IP address of S0/0/0 on **R3.**

Step 2: Ping Server1 from L2 and PC3.

Attempt to ping the IP address of **Server1** from **L2**. We will repeat this test after configuring the GRE tunnel over IPsec. What were the ping results? Why?

Step 3: Ping PC3 from L2.

Attempt to ping the IP address of **PC3** from **L2**. We will repeat this test after configuring the GRE tunnel over IPsec. What were the ping results? Why?

Part 2: Enable Security Features

Step 1: Activate securityk9 module.

The Security Technology Package license must be enabled to complete this activity.

a. Issue the **show version** command in the user EXEC or privileged EXEC mode to verify that the Security Technology Package license is activated.

```
----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None

Configuration register is 0x2102
```

b. If not, activate the **securityk9** module for the next boot of the router, accept the license, save the configuration, and reboot.

```
R1(config)# license boot module c2900 technology-package securityk9
<Accept the License>
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

c. After the reloading is completed, issue the **show version** again to verify the Security Technology Package license activation.

```
Technology Package License Information for Module:'c2900'

----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

d. Repeat Steps 1a to 1c with **R2** and **R3**.

Part 3: Configure IPsec Parameters

Step 1: Identify interesting traffic on R1.

a. Configure ACL 102 to identify the traffic from the LAN on **R1** to the LAN on **R2** as interesting. This interesting traffic will trigger the IPsec VPN to be implemented whenever there is traffic between the **R1** and **R2** LANs. All other traffic sourced from the LANs will not be encrypted. Remember that because of the implicit deny any, there is no need to add the statement to the list.

```
R1(config)# access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0
0.0.3.255
```

b. Repeat Step 1a to configure ACL 103 to identify the traffic on the LAN of R3 as interesting.

Step 2: Configure the ISAKMP Phase 1 properties on R1.

a. Configure the crypto ISAKMP policy **102** properties on **R1** along with the shared crypto key **cisco**. Default values do not have to be configured therefore only the encryption, key exchange method, and DH method must be configured.

```
R1(config)# crypto isakmp policy 102
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 64.100.13.2
```

b. Repeat Step 2a to configure policy 103. Change the IP addressing where appropriate.

Step 3: Configure the ISAKMP Phase 2 properties on R1.

a. Create the transform-set **VPN-SET** to use **esp-aes** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map.

```
R1(config)# crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
R1(config)# crypto map R1_R2_Map 102 ipsec-isakmp
R1(config-crypto-map)# set peer 64.100.13.2
R1(config-crypto-map)# set transform-set R1_R2_Set
R1(config-crypto-map)# match address 102
R1(config-crypto-map)# exit
```

b. Repeat Step 3a to configure R1_R3_Set and R1_R3_Map. Change the addressing where appropriate.

Step 4: Configure the crypto map on the outgoing interface.

Finally, bind the **R1_R2_Map** and **R1_R3_Map** crypto maps to the outgoing Serial 0/0/0 interface. **Note**: This is not graded.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map R1_R2_Map
R1(config-if)# crypto map R1_R3_Map
```

Step 5: Configure IPsec Parameters on R2 and R3

Repeat Steps 1-5 on **R2** and **R3**. Use the same ACL, set, and map names as **R1**. Note that each router only needs one encrypted connection to **R1**. There is no encrypted connection between **R2** and **R3**.

Part 4: Configure GRE Tunnels over IPsec

Step 1: Configure the Tunnel interfaces of R1.

a. Enter into the configuration mode for **R1** Tunnel 0.

```
R1(config)# interface tunnel 0
```

b. Set the IP address as indicated in the Addressing Table.

```
R1(config-if)# ip address 192.168.0.1 255.255.255.252
```

c. Set the source and destination for the endpoints of Tunnel 0.

```
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 64.100.13.2
```

d. Configure Tunnel 0 to convey IP traffic over GRE.

```
R1(config-if)# tunnel mode gre ip
```

e. The Tunnel 0 interface should already be active. In the event that it is not, treat it like any other interface.

f. Repeat Steps 1a-f to create the Tunnel 1 interface to R3. Change the addressing where appropriate.

Step 2: Configure the Tunnel 0 interface of R2 and R3.

a. Repeat Steps 1a – e with **R2**. Be sure to change the IP addressing as appropriate.

b. Repeat Steps 1a – e with **R3**. Be sure to change the IP addressing as appropriate.

Step 3: Configure a route for private IP traffic.

a. Define a route from **R1** to the 172.16.0.0 and 172.16.4.0 networks using the next-hop address of the tunnel interface.

b. Define a route from **R2** and **R3** to the 10.0.0.0 network using the next-hop address of the tunnel interface.

Part 5: Verify Connectivity

Step 1: Ping Server1 from L2 and PC3.

a. Attempt to ping the IP address of **Server1** from **L2** and **PC3**. The ping should be successful.

b. Attempt to ping the IP address of **L2** from **PC3**. The ping should fail because there is no tunnel between the two networks.