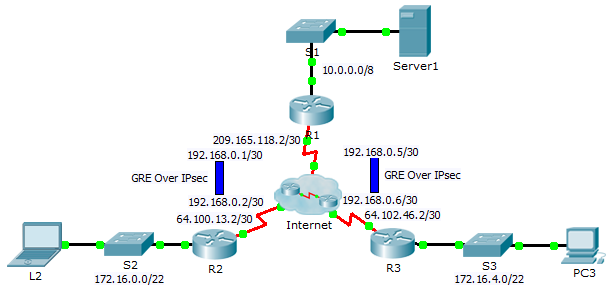
Packet Tracer –Configuring GRE over IPsec (Optional)(Instructor Version)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

1. Topology



1. 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 |

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

1. 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.

1. Verify Router Connectivity
   1. Ping R2 and R3 from R1.
      1. From **R1**, ping the IP address of S0/0/0 on **R2.**
      2. From **R1**, ping the IP address of S0/0/0 on **R3.**
   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? The pings failed because there is no route to the destination.

* 1. 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? The pings failed because there is no route to the destination.

1. Enable Security Features
   1. Activate securityk9 module.

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

* + 1. 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

* + 1. 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**

* + 1. 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

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

1. Configure IPsec Parameters
   1. Identify interesting traffic on R1.
      1. Configure ACL 101 to identify the traffic from the LAN on **R1** to the LAN on **R2** and **R3** as interesting. This interesting traffic will trigger the IPsec VPN to be implemented whenever there is traffic between the **R1** and **R2 -** **R3** 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 101 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.3.255**

* + 1. Repeat Step 1a to configure ACL 101 to identify the traffic on the LAN of R3 as interesting.

R1(config)# **access-list 101 permit ip 10.0.0.0 0.255.255.255 172.16.4.0 0.0.3.255**

* 1. Configure the ISAKMP Phase 1 properties on R1.
     1. Configure the crypto ISAKMP policy **101** 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 101**

R1(config-isakmp)# **encryption aes**

R1(config-isakmp)# **authentication pre-share**

R1(config-isakmp)# **group 5**

R1(config-isakmp)# **exit**

* + 1. Generate isakmp keys for each peer of **R1**.

R1(config)# crypto isakmp key cisco address 64.100.13.2

R1(config)# crypto isakmp key cisco address 64.102.46.2

* 1. Configure the ISAKMP Phase 2 properties on R1.
     1. 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 **101** and identify it as an **ipsec-isakmp** map.

R1(config)# **crypto ipsec transform-set R1\_Set esp-aes esp-sha-hmac**

R1(config)# **crypto map R1\_Map 101 ipsec-isakmp**

R1(config-crypto-map)# **set peer 64.100.13.2**

R1(config-crypto-map)# **set peer 64.102.46.2**

R1(config-crypto-map)# **set transform-set R1\_Set**

R1(config-crypto-map)# **match address 101**

R1(config-crypto-map)# **exit**

* 1. Configure the crypto map on the outgoing interface.

Finally, bind the **R1\_Map** crypto map 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\_Map**

* 1. Configure IPsec Parameters on R2 and R3

Repeat Steps 1-4 on **R2** and **R3**. Modify the set, and map names from **R1** to **R2** and **R3**. Use the same extended ACL number, 101. Note that each router only needs one encrypted connection to **R1**. There is no encrypted connection between **R2** and **R3**.

R2(config)#access-list 101 permit ip 172.16.0.0 0.0.3.255 10.0.0.0 0.255.255.255

R2(config)#crypto isakmp policy 101

R2(config-isakmp)# encryption aes

R2(config-isakmp)# authentication pre-share

R2(config-isakmp)# group 5

R2(config-isakmp)# exit

R2(config)#crypto isakmp key cisco address 209.165.118.2

R2(config)#crypto ipsec transform-set R2\_Set esp-aes esp-sha-hmac

R2(config)#crypto map R2\_Map 101 ipsec-isakmp

R2(config-crypto-map)# set peer 209.165.118.2

R2(config-crypto-map)# set transform-set R2\_Set

R2(config-crypto-map)# match address 101

R2(config-crypto-map)#interface Serial0/0/0

R2(config-if)# crypto map R2\_Map

R2(config-if)#interface Tunnel0

R2(config-if)# ip address 192.168.0.2 255.255.255.252

R2(config-if)# tunnel source Serial0/0/0

R2(config-if)# tunnel destination 209.165.118.2

R2(config-if)# tunnel mode gre ip

R2(config-if)#ip route 10.0.0.0 255.0.0.0 192.168.0.1

R2(config)#end

R3(config)#access-list 101 permit ip 172.16.4.0 0.0.3.255 10.0.0.0 0.255.255.255

R3(config)#crypto isakmp policy 101

R3(config-isakmp)# encryption aes

R3(config-isakmp)# authentication pre-share

R3(config-isakmp)# group 5

R3(config-isakmp)# exit

R3(config)#crypto isakmp key cisco address 209.165.118.2

R3(config)#crypto ipsec transform-set R3\_Set esp-aes esp-sha-hmac

R3(config)#crypto map R3\_Map 101 ipsec-isakmp

R3(config-crypto-map)# set peer 209.165.118.2

R3(config-crypto-map)# set transform-set R3\_Set

R3(config-crypto-map)# match address 101

R3(config-crypto-map)#interface S0/0/0

R3(config-if)# crypto map R3\_Map

R3(config-if)#interface Tunnel 0

R3(config-if)# ip address 192.168.0.6 255.255.255.252

R3(config-if)# tunnel source serial 0/0/0

R3(config-if)# tunnel destination 209.165.118.2

R3(config-if)# tunnel mode gre ip

R3(config-if)#ip route 10.0.0.0 255.0.0.0 192.168.0.5

R3(config)#end

1. Configure GRE Tunnels over IPSec
   1. Configure the Tunnel interfaces of R1.
      1. Enter into the configuration mode for **R1** Tunnel 0.

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

* + 1. Set the IP address as indicated in the Addressing Table.

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

* + 1. 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**

* + 1. Configure Tunnel 0 to convey IP traffic over GRE.

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

* + 1. The Tunnel 0 interface should already be active. In the event that it is not, treat it like any other interface.
    2. Repeat Steps 1a-f to create the Tunnel 1 interface to **R3**. Change the addressing where appropriate.

R1(config)# **interface tunnel 1**

R1(config-if)# **ip address 192.168.0.5 255.255.255.252**

R1(config-if)# **tunnel source s0/0/0**

R1(config-if)# **tunnel destination 64.102.46.2**

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

* 1. Configure the Tunnel 0 interface of R2 and R3.
     1. Repeat Steps 1a – e with **R2**. Be sure to change the IP addressing as appropriate.

R2(config)# **interface tunnel 0**

R2(config-if)# **ip address 192.168.0.2 255.255.255.252**

R2(config-if)# **tunnel source s0/0/0**

R2(config-if)# **tunnel destination 209.165.118.2**

R2(config-if)# **tunnel mode gre ip**

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

R3(config)# **interface tunnel 0**

R3(config-if)# **ip address 192.168.0.6 255.255.255.252**

R3(config-if)# **tunnel source s0/0/0**

R3(config-if)# **tunnel destination 209.165.118.2**

R3(config-if)# **tunnel mode gre ip**

* 1. Configure a route for private IP traffic.
     1. 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.

R1(config)# **ip route 172.16.0.0 255.255.252.0 192.168.0.2**

R1(config)# **ip route 172.16.4.0 255.255.252.0 192.168.0.6**

* + 1. Define a route from **R2** and **R3** to the 10.0.0.0 network using the next-hop address of the tunnel interface.

R2(config)# **ip route 10.0.0.0 255.0.0.0 192.168.0.1**

R3(config)# **ip route 10.0.0.0 255.0.0.0 192.168.0.5**

1. Verify Connectivity
   1. Ping Server1 from L2 and PC3.
      1. Attempt to ping the IP address of **Server1** from **L2** and **PC3**. The ping should be successful.
      2. Attempt to ping the IP address of **L2** from **PC3**. The ping should fail because there is no tunnel between the two networks.
2. Configuration Scripts
3. Router R1

license boot module c2900 technology-package securityk9

access-list 101 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.3.255

access-list 101 permit ip 10.0.0.0 0.255.255.255 172.16.4.0 0.0.3.255

crypto isakmp policy 101

encryption aes

authentication pre-share

group 5

exit

crypto isakmp key cisco address 64.100.13.2

crypto isakmp key cisco address 64.102.46.2

crypto ipsec transform-set R1\_Set esp-aes esp-sha-hmac

crypto map R1\_Map 101 ipsec-isakmp

set peer 64.100.13.2

set peer 64.102.46.2

set transform-set R1\_Set

match address 101

interface S0/0/0

crypto map R1\_Map

interface Tunnel 0

ip address 192.168.0.1 255.255.255.252

tunnel source serial 0/0/0

tunnel destination 64.100.13.2

tunnel mode gre ip

ip route 172.16.0.0 255.255.252.0 192.168.0.2

interface Tunnel 1

ip address 192.168.0.5 255.255.255.252

tunnel source serial 0/0/0

tunnel destination 64.102.46.2

tunnel mode gre ip

ip route 172.16.4.0 255.255.252.0 192.168.0.6

1. Router R2

license boot module c2900 technology-package securityk9

access-list 101 permit ip 172.16.0.0 0.0.3.255 10.0.0.0 0.255.255.255

crypto isakmp policy 101

encryption aes

authentication pre-share

group 5

exit

crypto isakmp key cisco address 209.165.118.2

crypto ipsec transform-set R2\_Set esp-aes esp-sha-hmac

crypto map R2\_Map 101 ipsec-isakmp

set peer 209.165.118.2

set transform-set R2\_Set

match address 101

interface Serial0/0/0

crypto map R2\_Map

interface Tunnel0

ip address 192.168.0.2 255.255.255.252

tunnel source Serial0/0/0

tunnel destination 209.165.118.2

tunnel mode gre ip

ip route 10.0.0.0 255.0.0.0 192.168.0.1

1. Router R3

license boot module c2900 technology-package securityk9

access-list 101 permit ip 172.16.4.0 0.0.3.255 10.0.0.0 0.255.255.255

crypto isakmp policy 101

encryption aes

authentication pre-share

group 5

exit

crypto isakmp key cisco address 209.165.118.2

crypto ipsec transform-set R3\_Set esp-aes esp-sha-hmac

crypto map R3\_Map 101 ipsec-isakmp

set peer 209.165.118.2

set transform-set R3\_Set

match address 101

interface S0/0/0

crypto map R3\_Map

interface Tunnel 0

ip address 192.168.0.6 255.255.255.252

tunnel source serial 0/0/0

tunnel destination 209.165.118.2

tunnel mode gre ip

ip route 10.0.0.0 255.0.0.0 192.168.0.5

1. Device Configs
2. Router R1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R1

crypto isakmp policy 101

encr aes

authentication pre-share

group 5

crypto isakmp key cisco address 64.100.13.2

crypto isakmp key cisco address 64.102.46.2

crypto ipsec transform-set R1\_Set esp-aes esp-sha-hmac

crypto map R1\_Map 101 ipsec-isakmp

set peer 64.100.13.2

set peer 64.102.46.2

set transform-set R1\_Set

match address 101

license udi pid CISCO2911/K9 sn FTX15241LLM

license boot module c2900 technology-package securityk9

spanning-tree mode pvst

interface Tunnel0

ip address 192.168.0.1 255.255.255.252

tunnel source Serial0/0/0

tunnel destination 64.100.13.2

tunnel mode gre ip

interface Tunnel1

ip address 192.168.0.5 255.255.255.252

tunnel source Serial0/0/0

tunnel destination 64.102.46.2

tunnel mode gre ip

interface GigabitEthernet0/0

ip address 10.0.0.1 255.0.0.0

duplex auto

speed auto

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 209.165.118.2 255.255.255.252

crypto map R1\_Map

interface Serial0/0/1

no ip address

shutdown

interface Vlan1

no ip address

shutdown

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

ip route 172.16.0.0 255.255.252.0 192.168.0.2

ip route 172.16.4.0 255.255.252.0 192.168.0.6

access-list 101 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.3.255

access-list 101 permit ip 10.0.0.0 0.255.255.255 172.16.4.0 0.0.3.255

line con 0

line aux 0

line vty 0 4

login

end

1. Router R2

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R2

crypto isakmp policy 102

encr aes

authentication pre-share

group 5

crypto isakmp key cisco address 209.165.118.2

crypto ipsec transform-set R1\_R2\_Set esp-aes esp-sha-hmac

crypto map R1\_R2\_Map 102 ipsec-isakmp

set peer 209.165.118.2

set transform-set R1\_R2\_Set

match address 102

license udi pid CISCO2911/K9 sn FTX15249J0B

license boot module c2900 technology-package securityk9

spanning-tree mode pvst

interface Tunnel0

ip address 192.168.0.2 255.255.255.252

tunnel source Serial0/0/0

tunnel destination 209.165.118.2

tunnel mode gre ip

interface GigabitEthernet0/0

ip address 172.16.0.1 255.255.252.0

duplex auto

speed auto

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 64.100.13.2 255.255.255.252

crypto map R1\_R2\_Map

interface Serial0/0/1

no ip address

shutdown

interface Vlan1

no ip address

shutdown

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

ip route 10.0.0.0 255.0.0.0 192.168.0.1

access-list 102 permit ip 172.16.0.0 0.0.3.255 10.0.0.0 0.255.255.255

line con 0

line aux 0

line vty 0 4

login

end

1. Router R3

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R3

crypto isakmp policy 103

encr aes

authentication pre-share

group 5

crypto isakmp key cisco address 209.165.118.2

crypto ipsec transform-set R1\_R3\_Set esp-aes esp-sha-hmac

crypto map R1\_R3\_Map 103 ipsec-isakmp

set peer 209.165.118.2

set transform-set R1\_R3\_Set

match address 103

license udi pid CISCO2911/K9 sn FTX1524446J

license boot module c2900 technology-package securityk9

spanning-tree mode pvst

interface Tunnel0

ip address 192.168.0.6 255.255.255.252

tunnel source Serial0/0/0

tunnel destination 209.165.118.2

tunnel mode gre ip

interface GigabitEthernet0/0

ip address 172.16.4.1 255.255.255.252

duplex auto

speed auto

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 64.102.46.2 255.255.255.252

crypto map R1\_R3\_Map

interface Serial0/0/1

no ip address

shutdown

interface Vlan1

no ip address

shutdown

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

ip route 10.0.0.0 255.0.0.0 192.168.0.5

access-list 103 permit ip 172.16.4.0 0.0.3.255 10.0.0.0 0.255.255.255

line con 0

line aux 0

line vty 0 4

login

end