Packet Tracer: Configuración de GRE por IPsec (optativo)

Topología

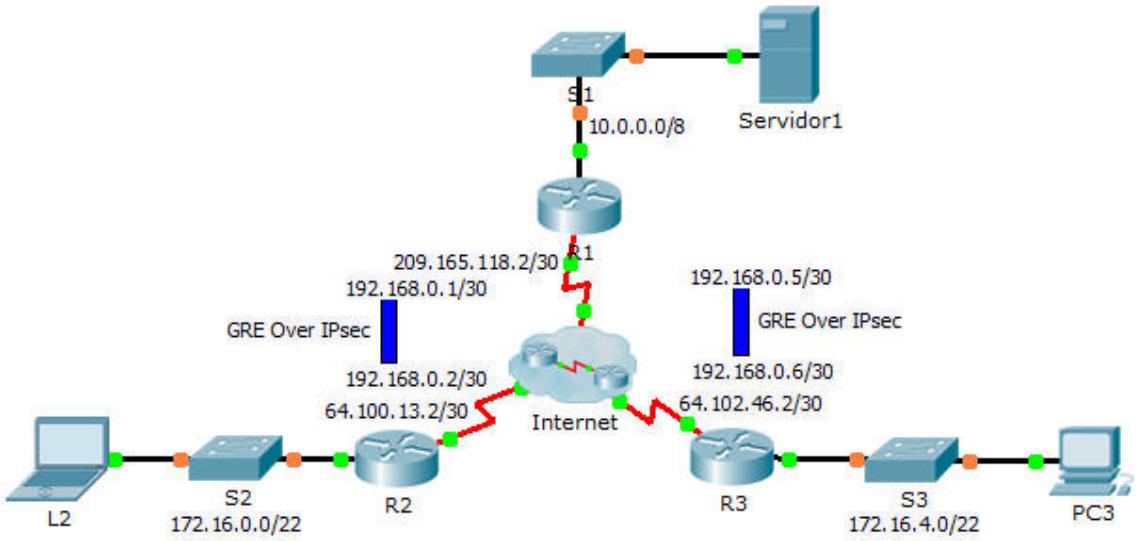

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
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

Objetivos

Parte 1: Verificar la conectividad de los routers

Parte 2: Habilitar las características de seguridad

Parte 3: Configurar los parámetros de IPsec

Parte 4: Configurar los túneles GRE por IPsec

Parte 5: verificar conectividad

Situación

Usted es el administrador de red de una empresa que desea configurar un túnel GRE por IPsec a una oficina remota. Todas las redes están configuradas localmente y solo necesitan que se configure el túnel y el cifrado.

Parte 1: Verificar la conectividad de los routers

Paso 1: Hacer ping del R1 al R2 y el R3.

a. Desde el **R1**, haga ping a la dirección IP de S0/0/0 en el **R2**.

b. Desde el **R1**, haga ping a la dirección IP de S0/0/0 en el **R3**.

Paso 2: Hacer ping de la L2 y la PC3 al Server1.

Intente hacer ping de la **L2** a la dirección IP del **Server1**. Se debe repetir esta prueba después de configurar el túnel GRE por IPsec. ¿Cuáles fueron los resultados de los pings? ¿Por qué?

Paso 3: Hacer ping de la L2 a la PC3.

Intente hacer ping de la **L2** a la dirección IP de la **PC3**. Se debe repetir esta prueba después de configurar el túnel GRE por IPsec. ¿Cuáles fueron los resultados de los pings? ¿Por qué?

Parte 2: Habilitar las características de seguridad

Paso 1: Activar el módulo securityk9.

Se debe activar la licencia del paquete de tecnología de seguridad para completar esta actividad.

a. Emita el comando **show version** en el modo EXEC del usuario o EXEC privilegiado para verificar si se activó la licencia del paquete de tecnología de seguridad.

```
-----------------------------------------------------------------
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. De lo contrario, active el módulo **securityk9** para el siguiente arranque del router, acepte la licencia, guarde la configuración y reinicie.

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

c. Una vez finalizada la recarga, vuelva a emitir el comando **show version** para verificar si se activó la licencia del paquete de tecnología de seguridad.

```
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. Repita los pasos 1a a 1c con el **R2** y el **R3**.

Parte 3: Configurar los parámetros de IPsec

Paso 1: Identificar el tráfico interesante en el R1.

a. Configure la ACL 102 para identificar como interesante el tráfico proveniente de la LAN en el **R1** a la LAN en el **R2**. Este tráfico interesante activa la VPN con IPsec para que se implemente cada vez que haya tráfico entre las LAN del **R1** y el **R2**. El resto del tráfico que se origina en las LAN no se cifra. Recuerde que debido a la instrucción implícita deny any, no hay necesidad de agregar dicha instrucción a la lista.

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

b. Repita el paso 1a para configurar la ACL 103 a fin de identificar como interesante el tráfico en la LAN del R3.

Paso 2: Configurar las propiedades de la fase 1 de ISAKMP en el R1.

a. Configure las propiedades de la política criptográfica ISAKMP **102** en el **R1** junto con la clave criptográfica compartida **cisco**. No es necesario que se configuren los valores predeterminados, por lo que solo se deben configurar el cifrado, el método de intercambio de claves y el método DH.

```
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. Repita el paso 2a para configurar la política 103. Cambie el direccionamiento IP según corresponda.

Paso 3: Configurar las propiedades de la fase 2 de ISAKMP en el R1.

a. Cree el conjunto de transformaciones **VPN-SET** para usar **esp-aes** y **esp-sha-hmac**. A continuación, cree la asignación criptográfica **VPN-MAP** que vincula todos los parámetros de la fase 2. Use el número de secuencia **10** e identifíquelo como una asignación **ipsec-isakmp**.

```
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. Repita el paso 3a para configurar R1_R3_Set y R1_R3_Map. Cambie el direccionamiento según corresponda.

Paso 4: Configurar la asignación criptográfica en la interfaz de salida.

Por último, vincule las asignaciones criptográficas **R1_R2_Map** y **R1_R3_Map** a la interfaz de salida Serial 0/0/0. **Nota:** esta actividad no se califica.

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

Paso 5: Configurar los parámetros de IPsec en el R2 y el R3.

Repita los pasos 1 a 5 en el **R2** y el **R3**. Use los mismos nombres de ACL, conjunto y asignación que en el **R1**. Tenga en cuenta que cada router solo necesita una conexión cifrada al **R1**. No hay ninguna conexión cifrada entre el **R2** y el **R3**.

Parte 4: Configurar los túneles GRE por IPsec

Paso 1: Configurar las interfaces de túnel del R1.

a. Ingrese al modo de configuración del túnel 0 del **R1**.

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

b. Establezca la dirección IP como se indica en la tabla de direccionamiento.

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

c. Establezca el origen y el destino para las terminales del túnel 0.

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

d. Configure el túnel 0 para trasmitir el tráfico IP por GRE.

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

e. La interfaz de túnel 0 ya debe estar activa. En caso de que no sea así, trátela como a cualquier otra interfaz.

f. Repita los pasos 1a a 1f para crear la interfaz de túnel 1 al R3. Cambie el direccionamiento según corresponda.

Paso 2: Configurar la interfaz Tunnel 0 del R2 y el R3.

a. Repita los pasos 1a a 1e con el **R2**. Asegúrese de cambiar el direccionamiento IP según corresponda.

b. Repita los pasos 1a a 1e con el **R3**. Asegúrese de cambiar el direccionamiento IP según corresponda.

Paso 3: Configurar una ruta para el tráfico IP privado.

a. Defina una ruta del **R1** a las redes 172.16.0.0 y 172.16.4.0 con la dirección de siguiente salto de la interfaz de túnel.

b. Defina una ruta del **R2** y el **R3** a la red 10.0.0.0 con la dirección de siguiente salto de la interfaz de túnel.

Parte 5: Verificar la conectividad

Paso 1: Hacer ping de la L2 y la PC3 al Server1.

a. Intente hacer ping de la **L2** y la **PC3** a la dirección IP del **Server1**. El ping debería realizarse correctamente.

b. Intente hacer ping de la **PC3** a la dirección IP de la **L2**. El ping debe fallar, porque no hay ningún túnel entre las dos redes.