Packet Tracer: Configuración de VPN (optativo)

Topología

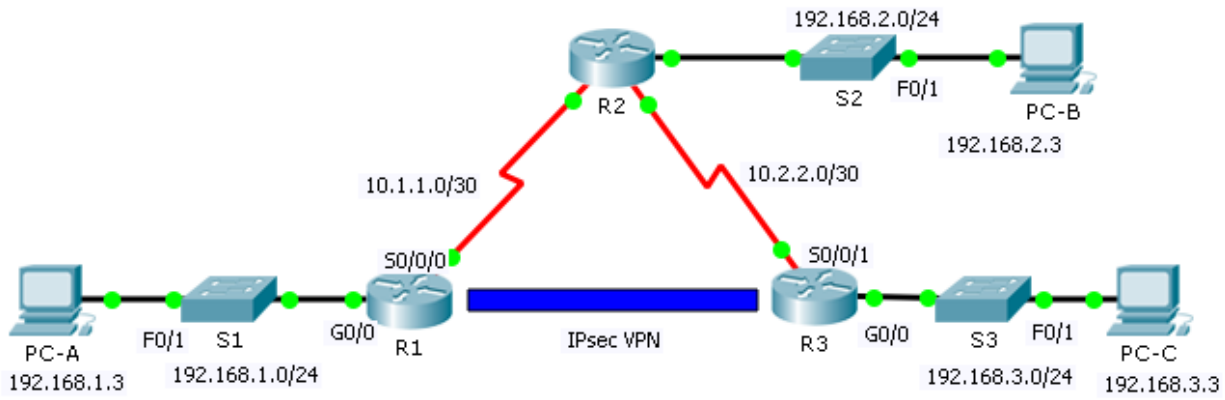

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Parámetros de política de fase 1 de ISAKMP

Parámetros		R1	R3
Método de distribución de claves	Manual o **ISAKMP**	ISAKMP	ISAKMP
Algoritmo de cifrado	**DES**, 3DES o AES	AES	AES
Algoritmo hash	MD5 o **SHA-1**	SHA-1	SHA-1
Método de autenticación	Claves previamente compartidas o **RSA**	Previamente compartidas	Previamente compartidas
Intercambio de claves	Grupo DH **1**, 2 o 5	DH 2	DH 2
Vida útil de SA IKE	86 400 segundos o menos	86400	86400
ISAKMP Key (Llave USB)		cisco	cisco

Los parámetros **en negrita** son valores predeterminados. Los demás parámetros se deben configurar explícitamente.

Parámetros de política de fase 2 de IPsec

Parámetros	R1	R3
Conjunto de transformaciones	VPN-SET	VPN-SET
Nombre de host del peer	R3	R1
Dirección IP del peer	10.2.2.2	10.1.1.2
Red para cifrar	192.168.1.0/24	192.168.3.0/24
Nombre de la asignación criptográfica	VPN-MAP	VPN-MAP
Establecimiento de SA	ipsec-isakmp	ipsec-isakmp

Objetivos

Parte 1: Habilitar las características de seguridad

Parte 2: Configurar los parámetros de IPsec en el R1

Parte 3: Configurar los parámetros de IPsec en el R3

Parte 4: Verificar la VPN con IPsec

Situación

En esta actividad, configurará dos routers para admitir una VPN con IPsec de sitio a sitio para el tráfico que fluye de sus respectivas LAN. El tráfico de la VPN con IPsec pasa a través de otro router que no tiene conocimiento de la VPN. IPsec proporciona una transmisión segura de la información confidencial a través de redes sin protección, como Internet. IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes (peers), como los routers Cisco.

Parte 1: 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.

Nota: la contraseña de los modos EXEC del usuario y EXEC privilegiado es **cisco**.

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
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 **R3**.

Parte 2: Configurar los parámetros de IPsec en el R1

Paso 1: Probar la conectividad.

Haga ping de la **PC-A** a la **PC-C**.

Paso 2: Identificar el tráfico interesante en el R1.

Configure la ACL 110 para identificar como interesante el tráfico proveniente de la LAN en el **R1** a la LAN en el **R3**. Este tráfico interesante activa la VPN con IPsec para que se implemente cada vez que haya tráfico entre las LAN de los routers **R1** y **R3**. 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 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Paso 3: Configurar las propiedades de la fase 1 de ISAKMP en el R1.

Configure las propiedades de la política criptográfica ISAKMP **10** en el **R1** junto con la clave criptográfica compartida **cisco**. Consulte la tabla de la fase 1 de ISAKMP para ver los parámetros específicos que se deben configurar. 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 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
```

Paso 4: Configurar las propiedades de la fase 2 de ISAKMP en el R1.

Cree el conjunto de transformaciones **VPN-SET** para usar **esp-3des** 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 VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Paso 5: Configurar la asignación criptográfica en la interfaz de salida.

Por último, vincule la asignación criptográfica **VPN-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 VPN-MAP
```

Parte 3: Configurar los parámetros de IPsec en el R3

Paso 1: Configurar el router R3 para admitir una VPN de sitio a sitio con el R1.

Ahora configure los parámetros recíprocos en el **R3**. Configure la ACL **110** para identificar como interesante el tráfico proveniente de la LAN en el **R3** a la LAN en el **R1**.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```


Paso 2: Configurar las propiedades de la fase 1 de ISAKMP en el R3.

Configure las propiedades de la política criptográfica ISAKMP **10** en el **R3** junto con la clave criptográfica compartida **cisco**.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
```

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

Como hizo en el **R1**, cree el conjunto de transformaciones **VPN-SET** para usar **esp-3des** 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**.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

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

Por último, vincule la asignación criptográfica **VPN-MAP** a la interfaz de salida Serial 0/0/1. **Nota:** esta actividad no se califica.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

Parte 4: Verificar la VPN con IPsec

Paso 1: Verificar el túnel antes del tráfico interesante.

Emita el comando **show crypto ipsec sa** en el **R1**. Observe que la cantidad de paquetes encapsulados, cifrados, desencapsulados y descifrados se establece en 0.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

```
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
<resultado omitido>
```

Paso 2: Crear el tráfico interesante.

Haga ping de la **PC-A** a la **PC-C**.

Paso 3: Verificar el túnel después del tráfico interesante.

En el **R1**, vuelva a emitir el comando **show crypto ipsec sa**. Ahora observe que la cantidad de paquetes es superior a 0, lo que indica que el túnel VPN con IPsec funciona.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0A496941(172583233)
<resultado omitido>
```

Paso 4: Crear el tráfico no interesante.

Haga ping de la **PC-A** a la **PC-B**.

Paso 5: Verificar el túnel.

En el **R1**, vuelva a emitir el comando **show crypto ipsec sa**. Por último, observe que la cantidad de paquetes no cambió, lo que verifica que el tráfico no interesante no está cifrado.