TALLER 1

Configurar y verificar una VPN IPsec de sitio a sitio mediante CLI Respuestas

Packet Tracer: configurar y verificar una VPN IPsec de sitio a sitio mediante CLI

Topología

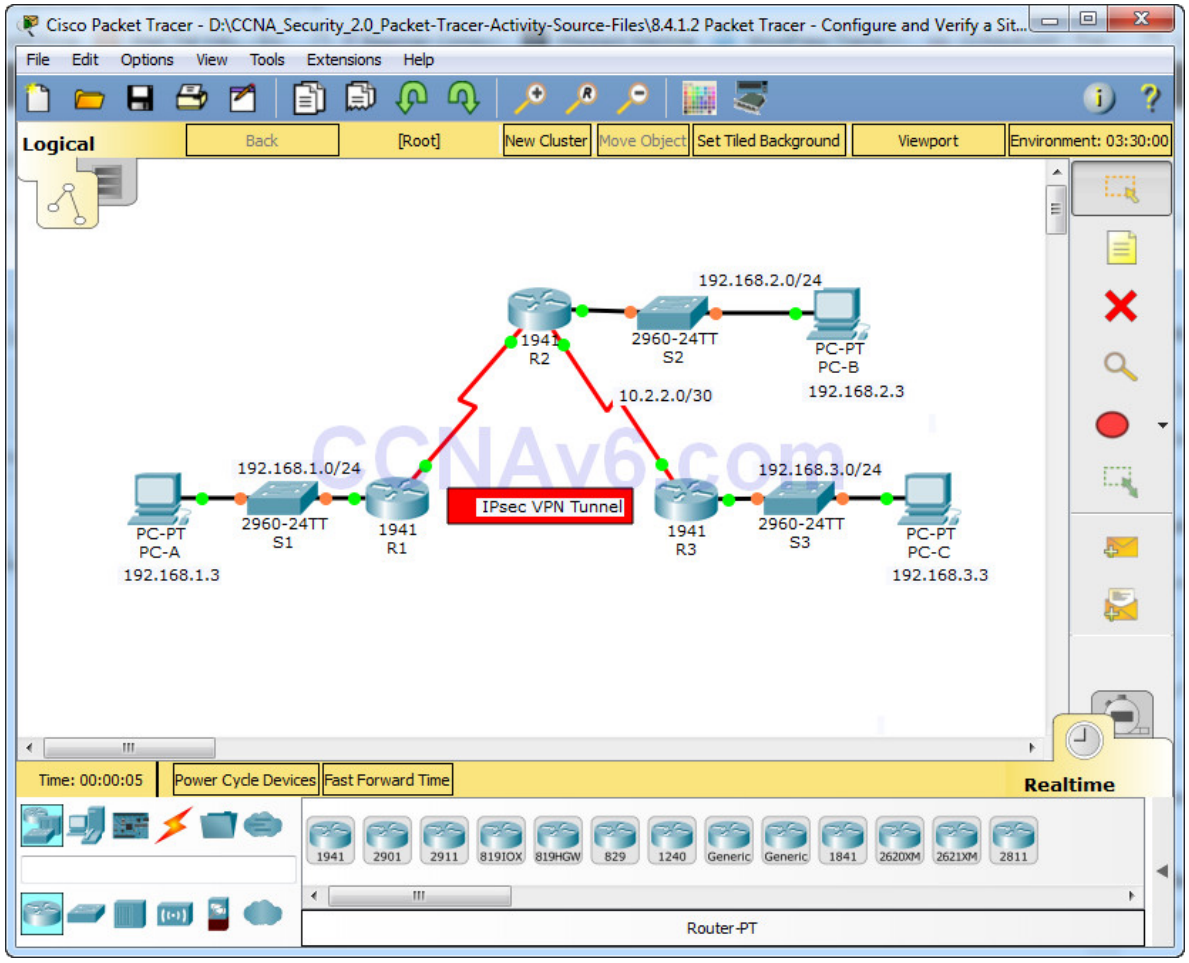

Tabla de direccionamiento

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objetivos

- Verificar la conectividad en toda la red.
- Configurar R1 para admitir una VPN IPsec de sitio a sitio con R3.

Antecedentes / Escenario

La topología de red muestra tres enrutadores. Su tarea consiste en configurar R1 y R3 para que admitan una VPN IPsec de sitio a sitio cuando el tráfico fluya entre sus respectivas redes LAN. El túnel VPN IPsec va de R1 a R3 a través de R2. R2 actúa como enlace de paso y no tiene conocimiento de la VPN. IPsec proporciona la transmisión segura de información confidencial a través de redes sin protección, como Internet. IPsec opera en la capa de red y protege y autentica los paquetes IP entre dispositivos IPsec participantes (pares), como los enrutadores Cisco.

Parámetros de política de la fase 1 de ISAKMP

Parameters		R1	R3
Key Distribution Method	Manual or **ISAKMP**	**ISAKMP**	**ISAKMP**
Encryption Algorithm	**DES**, 3DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or **SHA-1**	**SHA-1**	**SHA-1**
Authentication Method	Pre-shared keys or **RSA**	pre-share	pre-share
Key Exchange	DH Group 1, 2, or 5	DH 5	DH 5
IKE SA Lifetime	86400 seconds or less	**86400**	**86400**
ISAKMP Key		vpnpa55	vpnpa55

Nota : Los parámetros en negrita son predeterminados. Solo los que no están en negrita deben configurarse explícitamente.

Parámetros de política de IPsec Fase 2

Parameters	R1	R3
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.2.2.2	10.1.1.2
Traffic to be Encrypted	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Los enrutadores han sido preconfigurados con lo siguiente:

• Contraseña para la línea de consola: **ciscoconpa55**
• Contraseña para líneas vty: **ciscovtypa55**
• Contraseña de habilitación: **ciscoenpa55**
• Nombre de usuario y contraseña de SSH: **SSHadmin / ciscosshpa55**
• OSPF 101

Parte 1: Configurar los parámetros de IPsec en R1

Paso 1: Pruebe la conectividad.

Hacer ping desde PC-A a PC-C.

Paso 2: Habilite el paquete de tecnología de seguridad.

a. En R1, emita el comando **show version** para ver la información de licencia del paquete de tecnología de seguridad.
b. Si el paquete de Tecnología de Seguridad no se ha habilitado, utilice el siguiente comando para habilitar el paquete.

```
R1(config)# licencia módulo de arranque c1900 paquete de
tecnología securityk9
```

c. Acepte el acuerdo de licencia de usuario final.

d. Guarde la configuración en ejecución y vuelva a cargar el enrutador para habilitar la licencia de seguridad.

e. Verifique que el paquete de tecnología de seguridad se haya habilitado mediante el comando **show version .**

Paso 3: Identificar tráfico interesante en R1.

Configure la ACL 110 para identificar el tráfico de la LAN en R1 a la LAN en R3 como de interés. Este tráfico de interés activará la implementación de la VPN IPsec cuando haya tráfico entre las LAN de R1 a R3. El resto del tráfico proveniente de las LAN no se cifrará. Debido a la función implícita **"deny all"** , no es necesario configurar una sentencia **"deny ip any any"** .

```
R1(config)# lista de acceso 110 permitir ip 192.168.1.0
0.0.0.255 192.168.3.0 0.0.0.255
```

Paso 4: configurar la política ISAKMP de IKE Fase 1 en R1.

Configure las propiedades de la **política criptográfica ISAKMP 10** en el R1 junto con la clave criptográfica compartida **vpnpa55** . Consulte la tabla de la Fase 1 de ISAKMP para conocer los parámetros específicos que debe configurar. No es necesario configurar los valores predeterminados. Por lo tanto, solo se deben configurar el método de cifrado, el método de intercambio de claves y el método DH.

Nota : El grupo DH más alto compatible actualmente con Packet Tracer es el grupo 5. En una red de producción, deberá configurar al menos DH 14.

```
R1(config)# política criptográfica isakmp 10

R1(config-isakmp)# cifrado aes 256

R1(config-isakmp)# autenticación previa al uso compartido

R1(config-isakmp)# grupo 5

R1(config-isakmp)# exit

R1(config)# crypto isakmp clave vpnpa55 dirección 10.2.2.2
```

Paso 5: configurar la política IPsec de IKE Fase 2 en R1.

a. Cree el conjunto de transformación VPN-SET para usar **esp-aes** y **esp-sha-hmac.**

```
R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-
sha-hmac
```

b. Cree el mapa criptográfico VPN-MAP que vincula todos los parámetros de la Fase 2. Use el número de secuencia 10 e identifíquelo como un mapa ipsec-isakmp.

```
R1(config)# mapa criptográfico VPN-MAP 10 ipsec-isakmp

R1(config-crypto-map)# descripción Conexión VPN a R3
```

```
R1(config-crypto-map)# establecer par 10.2.2.2

R1(config-crypto-map)# establecer conjunto de transformación
VPN-SET

R1(config-crypto-map)# coincide con la dirección 110

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

Paso 6: Configure el mapa criptográfico en la interfaz saliente.

Vincula el mapa criptográfico VPN-MAP a la interfaz serial saliente 0/0/0.

```
R1(config)# interfaz s0/0/0

R1(config-if)# mapa criptográfico VPN-MAP
```

Parte 2: Configurar los parámetros de IPsec en R3

Paso 1: Habilite el paquete de tecnología de seguridad.

a. En R3, ejecute el comando show version para verificar que se haya habilitado la información de licencia del paquete de Tecnología de seguridad.

b. Si no se ha habilitado el paquete de Tecnología de seguridad, habilite el paquete y recargue R3.

Paso 2: Configure el enrutador R3 para admitir una VPN de sitio a sitio con R1.

Configure los parámetros reciprocantes en R3. Configure la ACL 110 para identificar el tráfico de la LAN en R3 a la LAN en R1 como interesante.

```
R3(config)# lista de acceso 110 permitir ip 192.168.3.0
0.0.0.255 192.168.1.0 0.0.0.255
```

Paso 3: configurar las propiedades ISAKMP de IKE Fase 1 en R3.

Configure las propiedades de la política criptográfica ISAKMP 10 en R3 junto con la clave criptográfica compartida vpnpa55.

```
R3(config)# política criptográfica isakmp 10

R3(config-isakmp)# cifrado aes 256

R3(config-isakmp)# autenticación previa al uso compartido

R3(config-isakmp)# grupo 5

R3(config-isakmp)# exit
```

```
R3(config)# crypto isakmp clave vpnpa55 dirección 10.1.1.2
```

Paso 4: configurar la política IPsec de IKE Fase 2 en R3.

a. Cree el conjunto de transformación VPN-SET para usar **esp-aes** y **esp-sha-hmac** .

```
R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-
sha-hmac
```

b. Cree el mapa criptográfico VPN-MAP que vincula todos los parámetros de la Fase 2. Use el número de secuencia 10 e identifíquelo como un mapa ipsec-isakmp.

```
R3(config)# mapa criptográfico VPN-MAP 10 ipsec-isakmp

R3(config-crypto-map)# descripción Conexión VPN a R1

R3(config-crypto-map)# establecer par 10.1.1.2

R3(config-crypto-map)# establecer conjunto de transformación
VPN-SET

R3(config-crypto-map)# coincide con la dirección 110

R3(config-crypto-map)# salir
```

Paso 5: Configure el mapa criptográfico en la interfaz de salida.

Vincula el mapa criptográfico VPN-MAP a la interfaz serial saliente 0/0/1. **Nota** : Esto no se califica.

```
R3(config)# interfaz s0/0/1

R3(config-if)# mapa criptográfico VPN-MAP
```

Parte 3: Verificar la VPN IPsec

Paso 1: Verificar el túnel antes de que entre tráfico de interés.

Ejecute el comando `**show crypto ipsec sa**` en R1. Observe que el número de paquetes encapsulados, cifrados, desencapsulados y descifrados es 0.

Paso 2: Crea tráfico interesante.

Hacer ping a PC-C desde PC-A.

Paso 3: Verificar el túnel después del tráfico interesante.

En R1, vuelva a ejecutar el comando **"show crypto ipsec sa"** . Observe que el número de paquetes es superior a 0, lo que indica que el túnel VPN IPsec funciona.

Paso 4: Crea tráfico poco interesante.

Haga ping a la PC-B desde la PC-A. **Nota** : Emitir un ping desde el enrutador R1 a la PC-C o desde el enrutador R3 a la PC-A no es tráfico de interés.

Paso 5: Verificar el túnel.

En R1, vuelva a ejecutar el comando **"show crypto ipsec sa"** . Observe que el número de paquetes no ha cambiado, lo que verifica que el tráfico no relevante no esté cifrado.

Paso 6: Verifique los resultados.

Tu porcentaje de finalización debe ser del 100%. Haz clic en **"Verificar resultados"** para ver los comentarios y la verificación de los componentes requeridos que se han completado.

SCRIPT R1

```
configuración t

Módulo de arranque de licencia c1900 paquete tecnológico
securityk9

Sí

fin

copiar configuración en ejecución configuración de
inicio



recargar



configuración t

lista de acceso 110 permiso ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255

Política de criptografía isakmp 10

cifrado aes 256
```

```
autenticación pre-compartir

grupo 5

salida

clave criptográfica isakmp vpnpa55 dirección 10.2.2.2

conjunto de transformaciones criptográficas ipsec
conjunto VPN esp-aes esp-sha-hmac

Mapa criptográfico VPN-MAP 10 ipsec-isakmp

Descripción Conexión VPN a R3

establecer par 10.2.2.2

conjunto de transformación VPN-SET

dirección del partido 110

salida

interfaz S0/0/0

mapa criptográfico VPN-MAP
```

SCRIPT R3

```
 configuración t

lista de acceso 110 permiso ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255

Política de criptografía isakmp 10

cifrado aes 256

autenticación pre-compartir

grupo 5

salida

clave criptográfica isakmp vpnpa55 dirección 10.1.1.2
```

```
conjunto de transformaciones criptográficas ipsec
conjunto VPN esp-aes esp-sha-hmac

Mapa criptográfico VPN-MAP 10 ipsec-isakmp

Descripción Conexión VPN a R1

establecer par 10.1.1.2

conjunto de transformación VPN-SET

dirección del partido 110

salida

interfaz S0/0/1

mapa criptográfico VPN-MAP
```