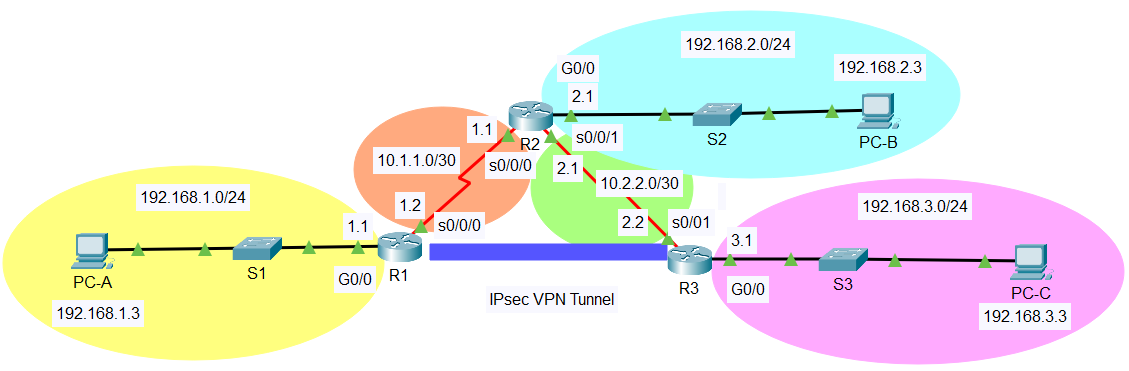


**Configure y verifique una VPN IPsec de sitio a sitio**

**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 |
| R1 | 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 |
| R2 | S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| R2 | 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 |
| R3 | 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 |

# Objectivos

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

# Background / Scenario

La topología de la red muestra tres ruteadores. Su tarea es configurar R1 y R3 para admitir una VPN IPsec de sitio a sitio cuando el tráfico fluye entre sus respectivas LAN. El túnel IPsec VPN es de R1 a R3 a través de R2. R2 actúa como un paso y no tiene conocimiento de la VPN. IPsec proporciona una transmisión segura de información confidencial a través de redes desprotegidas, como Internet. IPsec opera en la capa de red y protege y autentica los paquetes IP entre los dispositivos IPsec participantes (pares), como los ruteadores Cisco.

Parámetros de políticas de la fase 1 de ISAKMP

| Parámetros | Opciones de parámetros y valores predeterminados | R1 | R3 |
| --- | --- | --- | --- |
| **Método de distribución de claves (keys)** | Manual o **ISAKMP** | **ISAKMP** | **ISAKMP** |
| **Algoritmo de encriptación o cifrado** | **DES**, 3DES, o AES | AES 256 | AES 256 |
| **Algoritmo Hash** | MD5 o **SHA-1** | **SHA-1** | **SHA-1** |
| **Método de autenticación** | Claves previamente compartidas (Pre-shared keys) o **RSA** | pre-share | pre-share |
| **Intercambio de claves (keys)** | DH Group 1, 2, o 5 | DH 5 | DH 5 |
| **Tiempo de vida IKE SA** | 86400 segundos o menos | **86400** | **86400** |
| **Clave ISAKMP** | Proporcionado por el usuario. | vpnpa55 | vpnpa55 |

**Nota:** Los parámetros en negrita son los predeterminados. Solo los parámetros sin negrita deben configurarse explícitamente

Una **algoritmo hash** es un algoritmo matemático que transforma cualquier bloque de datos en una nueva serie de caracteres con una longitud fija.

Parámetros de políticas de la fase 2 de IPsec

| Parámetros | R1 | R3 |
| --- | --- | --- |
| **Nombre del conjunto de transformación** | VPN-SET | VPN-SET |
| **Cifrado de transformación ESP** | esp-aes | esp-aes |
| **Autenticación de transformación ESP** | esp-sha-hmac | esp-sha-hmac |
| **Dirección IP de pares (peer IP Address)** | 10.2.2.2 | 10.1.1.2 |
| **Tráfico a encriptar o cifrar** | 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) |
| **Nombre del mapa criptográfico** | VPN-MAP | VPN-MAP |
| **Establecimiento SA** | ipsec-isakmp | ipsec-isakmp |

Los ruteadores han sido pre-configurados con lo siguiente:

* Password de consola: **ciscoconpa55**
* Password de líneas vty: **ciscovtypa55**
* Password de modo privilegiado: **ciscoenpa55**
* Nombre de usuario SSH y password: **SSHadmin** / **ciscosshpa55**
* OSPF 101

## Parte 1: Configura los parámetros de IPsec en R1

### Paso 1: Verifica la conectividad.

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

### Paso 2: Habilitar el paquete de tecnología de seguridad

* + - 1. Habilite el paquete de tecnología de seguridad mediante el siguiente comando:

R1(config)# **license boot module c1900 technology-package securityk9**

* + - 1. Acepte el contrato de licencia de usuario final : **yes**
      2. Guarde la configuración en ejecución y vuelva a cargar el ruteador para habilitar la licencia de seguridad.
      3. Verifique que el paquete de tecnología de seguridad se haya habilitado mediante el comando **show version**.

### Paso 3: Identifique el tráfico interesante en R1.

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

R1(config)# **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**

### Paso 4: Configure la política ISAKMP de la fase 1 en R1.

Configure las propiedades de la política criptográfica **ISAKMP 10** en el **R1**. Consulte la tabla **Fase 1 de ISAKMP** para conocer los parámetros específicos a 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.

R1(config)# **crypto isakmp policy 10**

R1(config-isakmp)# **encryption aes 256**

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

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

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

### Paso 5: Configure la clave criptográfica compartida y la dirección del par remoto

Configure la clave criptográfica compartida **vpnpa55** y la dirección del par remoto.

R1(config)# **crypto isakmp key vpnpa55 address 10.2.2.2**

### Paso 6: Configure la política IPsec de la fase 2 de IKE en R1

* + - 1. 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**

* + - 1. Cree el mapa criptográfico **VPN-MAP** que une todos los parámetros de la Fase 2. Utilice el número de secuencia 10 e identifíquelo como un mapa **ipsec-isakmp**.

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 7: Configure el mapa criptográfico en la interfaz de salida.

Enlace el mapa criptográfico VPN-MAP a la interfaz Serial 0/0/0 de salida.

R1(config)# **interface s0/0/0**

R1(config-if)# **crypto map VPN-MAP**

## Parte 2: Configurar los parámetros de IPsec en R3

### Paso 1: Habilitar el paquete de tecnología de seguridad

* + - 1. En **R3**, emita el comando **show version** para verificar que la información de la licencia del paquete de tecnología de seguridad se haya habilitado.
      2. Si el paquete de tecnología de seguridad no se ha habilitado, habilite el paquete y vuelva a cargar **R3**

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

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

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

### Paso 3: Configurar las propiedades ISAKMP de la fase 1 de IKE en R3.

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

R3(config)# **crypto isakmp policy 10**

R3(config-isakmp)# **encryption aes 256**

R3(config-isakmp)# **authentication pre-share**

R3(config-isakmp)# **group 5**

R3(config-isakmp)# **exit**

R3(config)# **crypto isakmp key vpnpa55 address 10.1.1.2**

### Paso 4: Configure la política IPsec de fase 2 de IKE en el R3

* + - 1. Cree el conjunto de transformación **VPN-SET** para usar **esp-aes** y **esp-sha-hma**

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

* + - 1. Cree el mapa criptográfico **VPN-MAP** para unir todos los parámetros de la Fase 2. Utilice el número de secuencia 10 e identifíquelo como un mapa **ipsec-isakmp**.

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**

### Pago 5: Configure el mapa criptográfico en la interfaz de salida

Enlace el mapa criptográfico VPN-MAP a la interfaz **Serial 0/0/1** de salida.

R3(config)# **interface s0/0/1**

R3(config-if)# **crypto map VPN-MAP**

## Parte 3: Verifique la VPN IPsec

### Paso 1: Verifique el túnel antes del tráfico interesante

Emita el comando **show crypto ipsec sa** en **R1**. Tenga en cuenta que la cantidad de paquetes encapsulados, encriptados, desencapsulados y desencriptados se establece en 0.

### Paso 2: Crea tráfico interesante

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

### Paso 3: Verifique el túnel después del tráfico interesante.

En el **R1**, vuelva a ejecutar el comando **show crypto ipsec sa**. Observe que la cantidad de paquetes es mayor que 0, lo que indica que el túnel VPN IPsec está funcionando.

### Paso 4: Crea tráfico no interesante

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

### Paso 5: Verifique el túnel

En **R1**, vuelva a ejecutar el comando **show crypto ipsec sa**. Observe que la cantidad de paquetes no ha cambiado, lo que verifica que el tráfico no interesante no está encriptado