Configuración de una Sesión eBGP Segura con un VTI IPSec

Contenido

Introducción

Este documento describe cómo proteger una relación de vecino de protocolo de gateway fronterizo (eBGP) externa con el uso de una interfaz de túnel virtual (VTI) IPsec junto con las interfaces físicas (no túnel) para el tráfico del plano de datos. Entre las ventajas de esta configuración se incluyen las siguientes:

- Completa privacidad de la sesión de vecino BGP con confidencialidad de datos, anti-repetición, autenticidad e integridad.
- El tráfico del plano de datos no se limita a la sobrecarga de la unidad máxima de transmisión (MTU) de la interfaz de túnel. Los clientes pueden enviar paquetes MTU estándar (1500 bytes) sin implicaciones de rendimiento ni fragmentación.
- Menos sobrecarga en los routers de punto final, ya que el cifrado/descifrado de Security Policy Index (SPI) se limita al tráfico del plano de control BGP.

La ventaja de esta configuración es que el plano de datos no se limita a la limitación de la interfaz tunelizada. Por diseño, el tráfico del plano de datos no está protegido por IPSec.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Fundamentos de configuración y verificación de eBGP
- Manipulación de BGP Policy Accounting (PA) mediante un route-map
- Funciones básicas de políticas de IPsec y Asociación de seguridad de Internet y protocolo de administración de claves (ISAKMP)

Componentes Utilizados

La información en este documento se basa en Cisco IOS® Software Release 15.3(1.3)T, pero otras versiones soportadas funcionan. Puesto que la configuración de IPSec es una función criptográfica, asegúrese de que la versión del código contiene este conjunto de funciones.

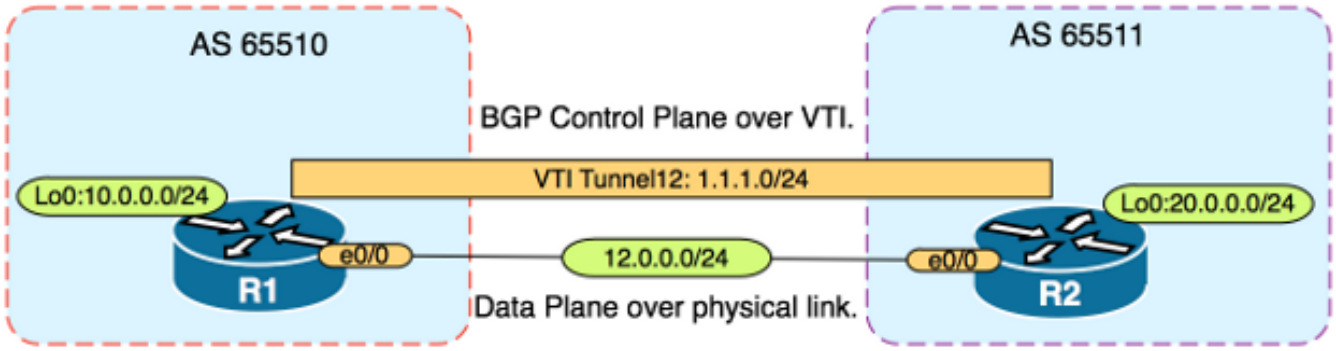
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Precaución:** El ejemplo de configuración de este documento utiliza algoritmos de cifrado modestos que pueden o no ser adecuados para su entorno. Consulte el informe técnico Encriptación de última generación para ver una explicación de la seguridad relativa de varios conjuntos de claves y tamaños de claves.

Configurar

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Configuraciones

Complete estos pasos:

1. Configure los parámetros de la fase 1 del Intercambio de claves de Internet (IKE) en R1 y R2 con la clave previamente compartida en R1: **Nota:** Nunca utilice los números de grupo DH 1, 2 ó 5, ya que se consideran inferiores. Si es posible, utilice un grupo DH con criptografía de curva elíptica (ECC) como los grupos 19, 20 o 24. El estándar de cifrado avanzado (AES) y el algoritmo hash seguro 256 (SHA256) deben considerarse superiores a los estándares de cifrado de datos (DES)/3DES y al resumen de mensaje 5 (MD5)/SHA1, respectivamente. Nunca utilice la contraseña "cisco" en un entorno de producción.**Configuración R1**

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 19
R1(config-isakmp)exit
```

```
R1(config)#crypto isakmp key CISCO address 12.0.0.2
```

Configuración R2

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash sha256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 19


R2(config-isakmp)exit

R2(config)#crypto isakmp key CISCO address 12.0.0.1
```

2. Configure el cifrado de contraseña de nivel 6 para la clave previamente compartida en NVRAM en R1 y R2. Esto reduce la probabilidad de que se lea la clave previamente compartida almacenada en texto sin formato si un router está comprometido:

```
R1(config)#key config-key password-encrypt CISCOCISCO

R1(config)#password encryption aes

R2(config)#key config-key password-encrypt CISCOCISCO

R2(config)#password encryption aes
```

Nota: Una vez que se habilita el cifrado de contraseña de nivel 6, la configuración activa ya no muestra la versión de texto sin formato de la clave previamente compartida:

```
!
R1#show run | include key
crypto isakmp key 6 \Nd`]dcCW\E`^WEObUKRGKIGadiAAB address 12.0.0.2

!
```

3. Configure los parámetros de la fase 2 IKE en R1 y R2: **Configuración R1**

```
R1(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R1(config)#crypto ipsec profile PROFILE

R1(ipsec-profile)#set transform-set TRANSFORM-SET
R1(ipsec-profile)#set pfs group19
```

Configuración R2

```
R2(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R2(config)#crypto ipsec profile PROFILE

R2(ipsec-profile)#set transform-set TRANSFORM-SET

R2(ipsec-profile)#set pfs group19
```

Nota: La configuración de Perfect Forward Secrecy (PFS) es opcional, pero mejora la resistencia de VPN, ya que fuerza una nueva generación de claves simétricas en el establecimiento de SA de la fase 2 de IKE.

4. Configure las interfaces de túnel en R1 y R2 y protéjelas con el perfil IPsec: **Configuración R1**

```
R1(config)#interface tunnel 12

R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#tunnel source Ethernet0/0

R1(config-if)#tunnel mode ipsec ipv4
```

```
R1(config-if)#tunnel destination 12.0.0.2

R1(config-if)#tunnel protection ipsec profile PROFILE
```

Configuración R2

```
R2(config)#interface tunnel 12

R2(config-if)#ip address 1.1.1.2 255.255.255.0

R2(config-if)#tunnel source Ethernet0/0

R2(config-if)#tunnel mode ipsec ipv4

R2(config-if)#tunnel destination 12.0.0.1

R2(config-if)#tunnel protection ipsec profile PROFILE
```

5. Configure BGP en R1 y R2 y anuncie las redes loopback0 en BGP: **Configuración R1**

```
R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 remote-as 65511

R1(config-router)#network 10.0.0.0 mask 255.255.255.0
```

Configuración R2

```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 remote-as 65510

R2(config-router)#network 20.0.0.0 mask 255.255.255.0
```

6. Configure un route-map en R1 y R2 para cambiar manualmente la dirección IP del siguiente salto de modo que apunte a la interfaz física y no al túnel. Debe aplicar este mapa de ruta en la dirección entrante. **Configuración R1**

```
R1(config)ip prefix-list R2-NETS seq 5 permit 20.0.0.0/24

R1(config)#route-map CHANGE-NEXT-HOP permit 10

R1(config-route-map)#match ip address prefix-list R2-NETS

R1(config-route-map)#set ip next-hop 12.0.0.2

R1(config-route-map)#end

R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 route-map CHANGE-NEXT-HOP in

R1(config-router)#do clear ip bgp *

R1(config-router)#end
```

Configuración R2

```
R2(config)#ip prefix-list R1-NETS seq 5 permit 10.0.0.0/24

R2(config)#route-map CHANGE-NEXT-HOP permit 10

R2(config-route-map)#match ip address prefix-list R1-NETS

R2(config-route-map)#set ip next-hop 12.0.0.1

R2(config-route-map)#end

R2(config)#router bgp 65511
```

```
R2(config-router)#neighbor 1.1.1.1 route-map CHANGE-NEXT-HOP in

R2(config-router)#do clear ip bgp *

R2(config-router)#end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Verifique que se hayan completado la fase IKE 1 y la fase IKE 2. El protocolo de línea de la interfaz de túnel virtual (VTI) no cambia a "activo" hasta que la fase IKE 2 haya finalizado:

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
12.0.0.1 12.0.0.2 QM_IDLE 1002 ACTIVE
12.0.0.2 12.0.0.1 QM_IDLE 1001 ACTIVE

R1#show crypto ipsec sa | inc encaps|decaps
#pkts encaps: 88, #pkts encrypt: 88, #pkts digest: 88
#pkts decaps: 90, #pkts decrypt: 90, #pkts verify: 90
```

Tenga en cuenta que antes de la aplicación del route-map, la dirección IP del siguiente salto apunta a la dirección IP del vecino BGP que es la interfaz de túnel:

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 1.1.1.2 0 0 65511 i
```

Cuando el tráfico utiliza el túnel, la MTU se limita a la MTU del túnel:

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set

*May 6 08:42:07.311: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:09.312: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:11.316: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:13.319: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:15.320: ICMP: dst (20.0.0.2): frag. needed and DF set.
Success rate is 0 percent (0/5)

R1#show interfaces tunnel 12 | inc transport|line
```

```
Tunnel12 is up, line protocol is up
Tunnel protocol/transport IPSEC/IP
Tunnel transport MTU 1406 bytes <---

R1#ping 20.0.0.2 size 1406 df-bit
Type escape sequence to abort.
Sending 5, 1406-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

Después de aplicar el route-map, la dirección IP se cambia a la interfaz física de R2, no al túnel:

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 12.0.0.2 0 0 65511 i
```

Cambie el plano de datos para utilizar el siguiente salto físico en lugar de que el túnel permita el tamaño estándar de MTU:

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.