Configure a una sesión eBGP segura con un IPSec VTI

Contenido

Introducción

Este documento describe cómo asegurar una relación de vecino del Border Gateway Protocol externo (eBGP) con el uso de una interfaz del túnel virtual del IPSec (VTI) junto con las interfaces físicas (NON-túnel) para el tráfico del plano de los datos. Las ventajas de esta configuración incluyen:

- Aislamiento completa de la sesión del vecino BGP con la confidencialidad de los datos, la anti-respuesta, la autenticidad, y la integridad.
- El tráfico del plano de los datos no se obliga a los gastos indirectos de la Unidad máxima de transmisión (MTU) (MTU) de la interfaz del túnel. Los clientes pueden enviar los paquetes estándar MTU (1500 bytes) sin las implicaciones en el rendimiento o la fragmentación.
- Menos gastos indirectos en el Routers del punto extremo puesto que el cifrar/que desencripta del índice de la política de seguridad (SPI) se limita al tráfico del plano del control BGP.

La ventaja de esta configuración es que el avión de los datos no está obligado a la limitación de la interfaz tunneled. Por el diseño, el tráfico del plano de los datos no es IPSec asegurado.

Charles contribuido Stizza, ingeniero de Cisco TAC.

Prerequisites

Requisitos

Cisco recomienda tener conocimientos de estos temas:

- fundamentales de la configuración de eBGP y de la verificación
- Manipulación de las estadísticas de la política de BGP (PA) usando un route-map
- Funciones de políticas básicas del Internet Security Association and Key Management Protocol (ISAKMP) y del IPSec

Componentes Utilizados

¿La información en este documento se basa en el Cisco IOS? El Software Release 15.3(1.3)T pero el otro trabajo de las versiones admitidas. Puesto que la configuración IPSec es una característica criptográfica, asegúrese que su versión del código contenga a este conjunto de características.

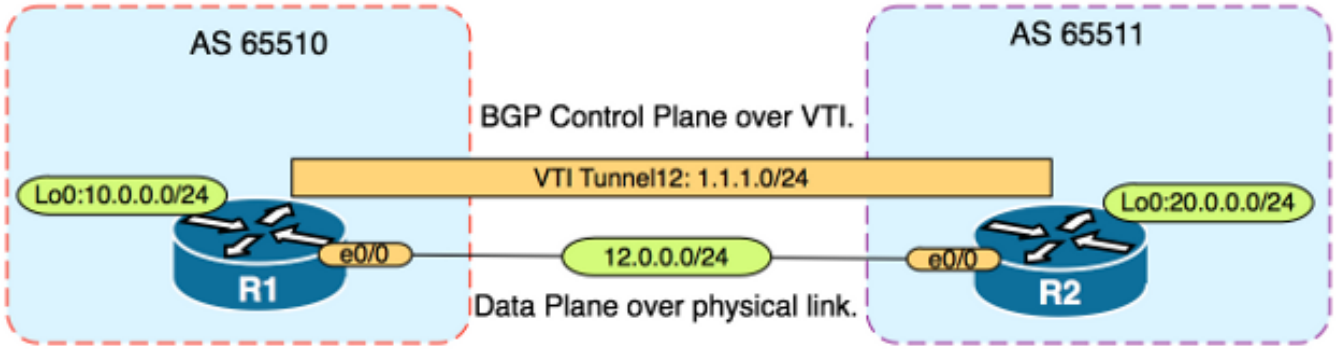
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

> **Caution**: El ejemplo de configuración en este documento utiliza los algoritmos modestos de la cifra que pudieron o no se pudieron adaptar para su entorno. Vea el White Paper del cifrado de la última generación para una discusión de la Seguridad relativa de las diversas habitaciones y de los tamaños de clave de la cifra.

Configurar

> **Note**: 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 de intercambio de claves de Internet (IKE) 1 en el r1 y el r2 con la clave previamente compartida en el r1:**Note**: Nunca utilice los números de grupo 1, 2 o 5 DH puesto que se consideran inferiores. Si es posible utilice a un grupo DH con la curva elíptica Cryptopgraphy (ECC) por ejemplo los grupos 19, 20 o 24. El Advanced Encryption Standard (AES) y el algoritmo de troceo seguro 256 (SHA256) se deben considerar superior a la Data Encryption Standard (DES)/3DES y la publicación de mensaje 5 (MD5)/SHA1 respectivamente. Nunca utilice la contraseña “Cisco” en un entorno de producción.**Configuración del 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 del 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 la encripción de contraseña del nivel 6 para la clave previamente compartida en el NVRAM en el r1 y el r2. Esto reduce la probabilidad de la clave previamente compartida salvada en el sólo texto de la lectura si comprometen a un router:

```
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
```

Note: Una vez que se habilita la encripción de contraseña del nivel 6, la configuración activa muestra no más la versión de sólo texto 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 el r1 y el r2:**Configuración del 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 del 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
```

Note: La determinación del Confidencialidad directa perfecta (PFS) es opcional pero mejora la fuerza VPN puesto que fuerza una nueva generación de clave simétrica en el establecimiento de la fase 2 SA IKE.

4. Configure las interfaces del túnel en el r1 y el r2 y asegúrelas con el perfil de ipsec:Configuración del 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 del 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. La configuración BGP en el r1 y el r2 y hacen publicidad de las redes del loopback0 en el BGP:Configuración del 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 del r2

```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.2 remote-as 65510

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

6. Configure un route-map en el r1 y el r2 para cambiar manualmente el IP Address de Next Hop de modo que señale a la interfaz física y no al túnel. Usted debe aplicar este route-map en la dirección entrante.Configuración del 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 del 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 del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Verifique que la fase 1 IKE y la fase 2 IKE hayan completado. El Line Protocol en la interfaz del túnel virtual (VTI) no cambia a “encima de” hasta que la fase 2 IKE haya completado:

```
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
```

Observe que antes de la aplicación del route-map, el IP Address de Next Hop señala a la dirección IP del vecino BGP que es la interfaz del 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, el MTU se obliga al túnel 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

*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 del r2, no el 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
```

Transborde avión de los datos para utilizar el salto siguiente físico en comparación con el tamaño estándar MTU de los permisos 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
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Troubleshooting

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