Een beveiligde eBGP-sessie configureren met een IPsec VTI

Inhoud

Inleiding

Dit document beschrijft hoe u een externe grensgateway Protocol (eBGP)-buurrelatie kunt beveiligen met het gebruik van een IPsec Virtual Tunnel Interface (VTI) samen met de fysieke interfaces (niet-tunnel) voor het gegevensverkeer. De voordelen van deze configuratie zijn:

- Volledige privacy van de BGP buursessie met gegevensvertrouwelijkheid, anti-replay, authenticiteit en integriteit.
- Het dataverkeer is niet beperkt tot de maximale transmissieeenheid (MTU) boven de tunnelinterface. Klanten kunnen standaard MTU-pakketten (1500 bytes) verzenden zonder implicaties of fragmentatie van prestaties.
- Minder overhead op de end-point routers sinds Security Policy Index (SPI) codering/decryptie is beperkt tot BGP-besturingsplane verkeer.

Het voordeel van deze configuratie is dat het gegevensvlak niet beperkt is tot de beperking van de tunnelinterface. Door ontwerp wordt het gegevensverkeer niet IPsec beveiligd.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

- eBGP-configuratie en -verificatiefundamentele onderdelen
- Manipulatie van BGP-beleidsaccounting (PA) op basis van een routekaart
- Basis Internet Security Association en Key Management Protocol (ISAKMP) en IPsec-beleidsfuncties

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS® softwarerelease 15.3(1.3)T maar andere ondersteunde versies werken. Aangezien de configuratie van IPsec een cryptografische functie is, dient u er zeker van te zijn dat uw versie van de code deze functieset bevat.

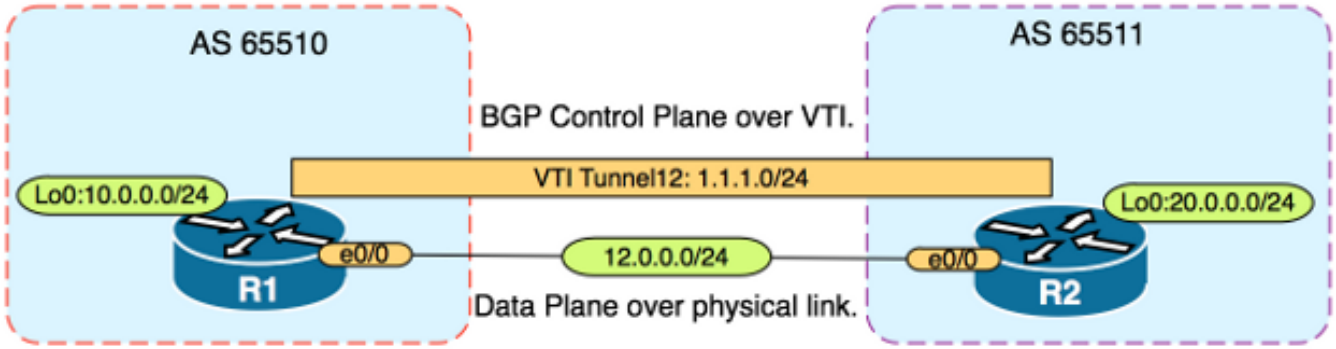
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

> **Voorzichtig:** Het configuratievoorbeeld in dit document maakt gebruik van bescheiden algoritmen van het algoritme van het algoritme die al dan niet geschikt voor uw omgeving zijn. Zie het Witboek Encryptie van de volgende generatie voor een discussie over de relatieve beveiliging van verschillende algoritme en hoofdformaten.

Configureren

> **Opmerking:** Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



Configuraties

Voer de volgende stappen uit:

1. Configuratie van de parameters van de Stap 1 van de Internet Key Exchange (IKE) op R1 en R2 met de vooraf gedeelde sleutel op R1: **Opmerking:** Gebruik de DH-groepen 1, 2 of 5 nooit, omdat ze inferieur worden geacht. Gebruik indien mogelijk een DH-groep met Elliptic Curve Cryptopgrafie (ECC) zoals groepen 19, 20 of 24. Advanced Encryption Standard (AES) en Secure Hash Algorithm 256 (SHA256) moeten worden beschouwd als beter dan Data Encryption Standard (DES)/3DES en Message Digest 5 (MD5)/SHA1. Gebruik het wachtwoord "cisco" nooit in een productieomgeving.**Configuratie 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
```

R2-configuratie

```
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. Configureer niveau 6 wachtwoordencryptie voor de vooraf gedeelde sleutel in NVRAM op R1 en R2. Dit vermindert de waarschijnlijkheid van de vooraf gedeelde sleutel die in gewone tekst is opgeslagen om te worden gelezen als een router gecompromitteerd is:

```
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
```

Opmerking: Zodra de wachtwoordencryptie van niveau 6 is ingeschakeld, toont de actieve configuratie niet langer de onbewerkte tekstversie van de vooraf gedeelde toets:

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

!
```

3. Configureer de parameters van IKE fase 2 op R1 en R2: **Configuratie 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
```

R2-configuratie

```
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
```

Opmerking: De instelling Perfect Forward SecRITY (PFS) is optioneel, maar verbetert de VPN-kracht omdat deze een nieuwe symmetrische sleutelgeneratie dwingt in de IKE fase 2 SA-instelling.

4. Configuratie van de tunnelinterfaces op R1 en R2 en veilig met het IPsec-profiel: **Configuratie 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
```

R2-configuratie

```
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. Configureer BGP op R1 en R2 en adverteer de loopback0-netwerken in BGP: **Configuratie 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
```

R2-configuratie

```
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. Configureer een route-map op R1 en R2 om het volgende hop-IP-adres handmatig te wijzigen, zodat het naar de fysieke interface wijst en niet naar de tunnel. Je moet deze routekaart op de binnenrichting toepassen. **Configuratie 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
```

R2-configuratie

```
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Controleer of zowel IKE fase 1 als IKE fase 2 voltooid zijn. Het lijnprotocol op de Virtual Tunnel Interface (VTI) verandert niet in "up" totdat IKE fase 2 is voltooid:

```
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
```

Merk op dat voorafgaand aan de toepassing van de route-kaart, het volgende IP-adres van de hop op het IP-adres van de buur dat de tunnelinterface is:

```
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
```

Wanneer het verkeer de tunnel gebruikt, is MTU beperkt tot de tunnel 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
```

Na het toepassen van de route-kaart, wordt het IP adres veranderd in de fysieke interface van R2, niet de tunnel:

```
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
```

Verander het gegevensvlak om de fysieke volgende hop te gebruiken in tegenstelling tot de tunnelvergunning MTU's van standaardgrootte:

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.