Configurare una sessione eBGP sicura con una VTI IPsec

Sommario

Introduzione

In questo documento viene descritto come proteggere una relazione di adiacenza Border Gateway Protocol (eBGP) esterna con l'uso di una VTI (Virtual Tunnel Interface) IPsec insieme alle interfacce fisiche (non tunnel) per il traffico del data plane. I vantaggi di questa configurazione includono:

- Tutta la privacy della sessione BGP con riservatezza dei dati, anti-replay, autenticità e integrità.
- Il traffico del piano dati non è vincolato al sovraccarico dell'MTU (Maximum Transmission Unit) dell'interfaccia del tunnel. I clienti possono inviare pacchetti MTU standard (1500 byte) senza implicazioni sulle prestazioni o frammentazione.
- Riduzione del sovraccarico sui router del punto finale, in quanto la crittografia/decrittografia SPI (Security Policy Index) è limitata al traffico del control plane BGP.

Il vantaggio di questa configurazione è che il piano dati non è vincolato al limite dell'interfaccia tunneled. In base alla progettazione, il traffico del piano dati non è protetto da IPsec.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Fondamenti di configurazione e verifica di eBGP
- Manipolazione BGP Policy Accounting (PA) tramite route-map
- Funzionalità di base del protocollo ISAKMP (Internet Security Association and Key Management Protocol) e dei criteri IPSec

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco IOS® versione 15.3(1.3)T, ma sono supportate anche altre versioni. Poiché la configurazione IPsec è una funzionalità di crittografia, verificare che la versione del codice contenga questo set di funzionalità.

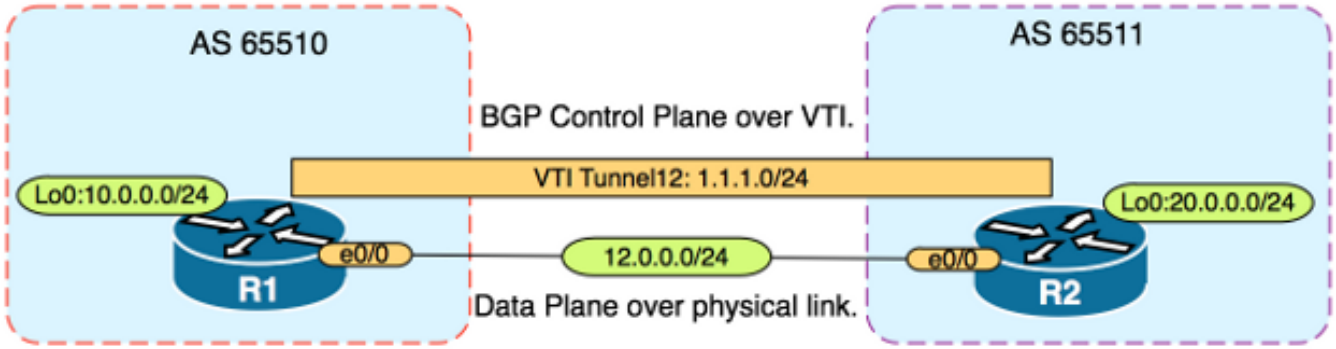
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Attenzione:** L'esempio di configurazione illustrato in questo documento utilizza algoritmi di cifratura di valore modesto che potrebbero essere adatti o meno al proprio ambiente. Per informazioni sulla sicurezza relativa di varie suite di cifratura e dimensioni delle chiavi, consultare il white paper sulla crittografia di nuova generazione.

Configurazione

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete



Configurazioni

Attenersi alla seguente procedura:

1. Configurare i parametri IKE (Internet Key Exchange) fase 1 su R1 e R2 con la chiave già condivisa su R1: **Nota:** Non utilizzare mai i numeri di gruppo DH 1, 2 o 5 poiché sono considerati inferiori. Se possibile, utilizzare un gruppo DH con ECC (Elliptic Curve Cryptopgraphy), ad esempio i gruppi 19, 20 o 24. AES (Advanced Encryption Standard) e SHA256 (Secure Hash Algorithm 256) devono essere considerati superiori rispettivamente a DES (Data Encryption Standard)/3DES e MD5 (Message Digest 5)/SHA1. Non usare mai la password "cisco" in un ambiente di produzione.**Configurazione 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
```

Configurazione 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. Configurare la crittografia della password di livello 6 per la chiave precondivisa nella NVRAM sui router R1 e R2. In questo modo si riduce la probabilità che la chiave precondivisa archiviata in testo normale venga letta se un router è compromesso:

```
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: Dopo aver abilitato la crittografia della password di livello 6, la configurazione attiva non visualizza più la versione in testo normale della chiave precondivisa:

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

!
```

3. Configurare i parametri IKE fase 2 su R1 e R2: **Configurazione 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
```

Configurazione 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: L'impostazione di PFS (Perfect Forward Secrecy) è facoltativa, ma migliora la forza della VPN poiché forza una nuova generazione di chiavi simmetriche nella definizione dell'associazione di sicurezza IKE fase 2.

4. Configurare le interfacce tunnel su R1 e R2 e proteggerle con il profilo IPsec: **Configurazione 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
```

Configurazione 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. Configurare BGP su R1 e R2 e annunciare le reti loopback0 in BGP: **Configurazione 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
```

Configurazione 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. Configurare una mappa dei percorsi su R1 e R2 in modo da modificare manualmente l'indirizzo IP dell'hop successivo in modo che punti all'interfaccia fisica e non al tunnel. È necessario applicare la route-map alla direzione in ingresso. **Configurazione 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
```

Configurazione 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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Verificare che sia la fase 1 che la fase 2 di IKE siano state completate. Il protocollo di linea sull'interfaccia del tunnel virtuale (VTI) non cambia in "attivo" finché non è stata completata la fase 2 di IKE:

```
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
```

Notare che prima dell'applicazione della route-map, l'indirizzo IP dell'hop successivo punta all'indirizzo IP del router adiacente BGP, ossia l'interfaccia del 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 1.1.1.2 0 0 65511 i
```

Quando il traffico usa il tunnel, l'MTU è limitata all'MTU del tunnel:

```
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
```

Dopo aver applicato la mappa dei percorsi, l'indirizzo IP viene modificato nell'interfaccia fisica di R2, non nel 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
```

Modificare il piano dati in modo da usare l'hop successivo fisico anziché il tunnel che permette l'MTU di dimensioni standard:

```
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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.