Konfigurieren einer sicheren eBGP-Sitzung mit einem IPsec-VTI

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine externe Border Gateway Protocol (eBGP)-Nachbarbeziehung mit der Verwendung einer IPsec Virtual Tunnel Interface (VTI) sowie der physischen Schnittstellen (Non-Tunnel) für den Datenverkehr auf der Datenebene gesichert wird. Vorteile dieser Konfiguration:

- Vollständiger Datenschutz der BGP-Nachbarsitzung mit Datensicherheit, Anti-Wiedergabe, Authentizität und Integrität.
- Der Datenverkehr auf der Datenebene ist nicht auf den Overhead der Maximum Transmission Unit (MTU) der Tunnelschnittstelle beschränkt. Kunden können Standard-MTU-Pakete (1.500 Byte) ohne Leistungsauswirkungen oder Fragmentierung senden.
- Weniger Overhead auf die Endpunkt-Router, da die Verschlüsselung/Entschlüsselung mit dem Security Policy Index (SPI) auf den BGP-Kontrollebenen-Datenverkehr beschränkt ist.

Der Vorteil dieser Konfiguration besteht darin, dass die Datenebene nicht auf die Beschränkung der getunnelten Schnittstelle beschränkt ist. Der Datenverkehr auf Datenebene ist standardmäßig nicht durch IPsec gesichert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- eBGP-Konfigurations- und Verifizierungsgrundlagen
- Manipulation von BGP Policy Accounting (PA) mithilfe einer Route Map
- Grundlegende Funktionen der Internet Security Association und des Key Management Protocol (ISAKMP) und der IPsec-Richtlinie

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco IOS® Softwareversion 15.3(1.3)T, andere unterstützte Versionen funktionieren jedoch. Da die IPsec-Konfiguration eine kryptografische Funktion ist, stellen Sie sicher, dass Ihre Codeversion diesen Funktionssatz enthält.

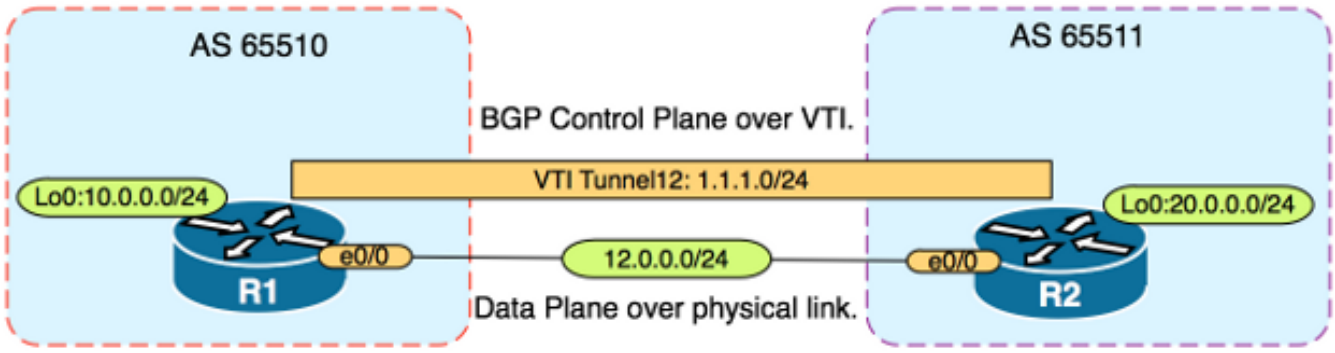
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

> **Vorsicht:** Im Konfigurationsbeispiel dieses Dokuments werden bescheidene Verschlüsselungsalgorithmen verwendet, die möglicherweise nicht für Ihre Umgebung geeignet sind. Im Next Generation Encryption White Paper wird die relative Sicherheit verschiedener Verschlüsselungssuiten und Schlüsselgrößen erläutert.

Konfiguration

> **Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



Konfigurationen

Führen Sie diese Schritte aus:

1. Konfigurieren Sie die Parameter für Phase 1 des Internet Key Exchange (IKE) auf R1 und R2 mit dem vorinstallierten Schlüssel auf R1: **Hinweis:** Verwenden Sie niemals die DH-Gruppennummern 1, 2 oder 5, da sie als unterlegen gelten. Verwenden Sie möglichst eine DH-Gruppe mit Elliptic Curve Cryptopgraphy (ECC), z. B. Gruppen 19, 20 oder 24. Advanced Encryption Standard (AES) und Secure Hash Algorithm 256 (SHA256) sollten als besser als Data Encryption Standard (DES)/3DES bzw. Message Digest 5 (MD5)/SHA1 angesehen werden. Verwenden Sie niemals das Kennwort "cisco" in einer Produktionsumgebung.**R1-Konfiguration**

```
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-Konfiguration

```
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. Konfigurieren Sie die Kennwortverschlüsselung der Stufe 6 für den vorinstallierten Schlüssel im NVRAM auf R1 und R2. Dadurch wird die Wahrscheinlichkeit verringert, dass der im Klartext gespeicherte vorinstallierte Schlüssel bei einem Router-Ausfall gelesen wird:

```
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
```

Hinweis: Sobald die Level-6-Kennwortverschlüsselung aktiviert ist, wird in der aktiven Konfiguration nicht mehr die Textversion des vorinstallierten Schlüssels angezeigt:

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

!
```

3. Konfigurieren der IKE Phase 2-Parameter für R1 und R2: R1-Konfiguration

```
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-Konfiguration

```
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
```

Hinweis: PFS (Perfect Forward Secrecy) ist optional, erhöht jedoch die VPN-Stärke, da es eine neue symmetrische Schlüsselgenerierung in der IKE Phase 2 SA-Einrichtung erzwingt.

4. Konfigurieren Sie die Tunnelschnittstellen auf R1 und R2, und sichern Sie sie mit dem IPsec-Profil: R1-Konfiguration

```
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-Konfiguration

```
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. Konfigurieren Sie BGP auf R1 und R2, und kündigen Sie die Loopback0-Netzwerke dem BGP an: **R1-Konfiguration**

```
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-Konfiguration

```
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. Konfigurieren Sie eine Routenübersicht auf R1 und R2, um die nächste Hop-IP-Adresse manuell so zu ändern, dass sie auf die physische Schnittstelle und nicht auf den Tunnel zeigt. Sie müssen diese route-map auf die eingehende Richtung anwenden. **R1-Konfiguration**

```
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-Konfiguration

```
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
```

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Überprüfen Sie, ob die IKE-Phase 1 und die IKE-Phase 2 abgeschlossen sind. Das Leitungsprotokoll auf der Virtual Tunnel Interface (VTI) ändert sich nicht in "up" (aktiv), bis IKE Phase 2 abgeschlossen ist:

```
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
```

Beachten Sie, dass vor der Anwendung der route-map die Next-Hop-IP-Adresse auf die BGP-Nachbarn-IP-Adresse verweist, die die Tunnelschnittstelle ist:

```
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
```

Wenn der Datenverkehr den Tunnel verwendet, ist die MTU auf die Tunnel-MTU beschränkt:

```
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
```

Nach Anwenden der Route Map wird die IP-Adresse in die physische Schnittstelle von R2 und nicht in den Tunnel geändert:

```
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
```

Ändern Sie die Datenebene, um den physischen nächsten Hop anstelle des Tunnels zu verwenden, sodass die MTU der Standardgröße zulässig ist:

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.