使用IPsec VTI配置安全eBGP會話

目錄

簡介

本文說明如何使用IPsec虛擬通道介面(VTI)和資料平面流量的實體介面（非通道）來保護外部邊界閘道通訊協定(eBGP)鄰居關係。此配置的優點包括：

- 具有資料機密性、反重放、真實性和完整性的BGP鄰居會話的完全保密性。
- 資料平面流量不受隧道介面的最大傳輸單元(MTU)開銷的限制。客戶可以傳送標準MTU封包（1500位元組），而不會影響效能或進行分段。
- 由於安全原則索引(SPI)加密/解密限於BGP控制平面流量，因此減少了終端路由器上的額外負荷。

此配置的優點是資料平面不受隧道介面的限制。根據設計，資料平面流量不受IPsec保護。

必要條件

需求

思科建議您瞭解以下主題：

- eBGP設定和驗證基礎
- 使用路由對映的BGP策略記帳(PA)操作
- 基本網際網路安全關聯和金鑰管理協定(ISAKMP)和IPsec策略功能

採用元件

本檔案中的資訊是根據Cisco IOS®軟體版本15.3(1.3)T，但其他支援的版本能運作。因為IPsec組態是一種加密功能，所以請確保您版本的程式碼包含此功能集。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

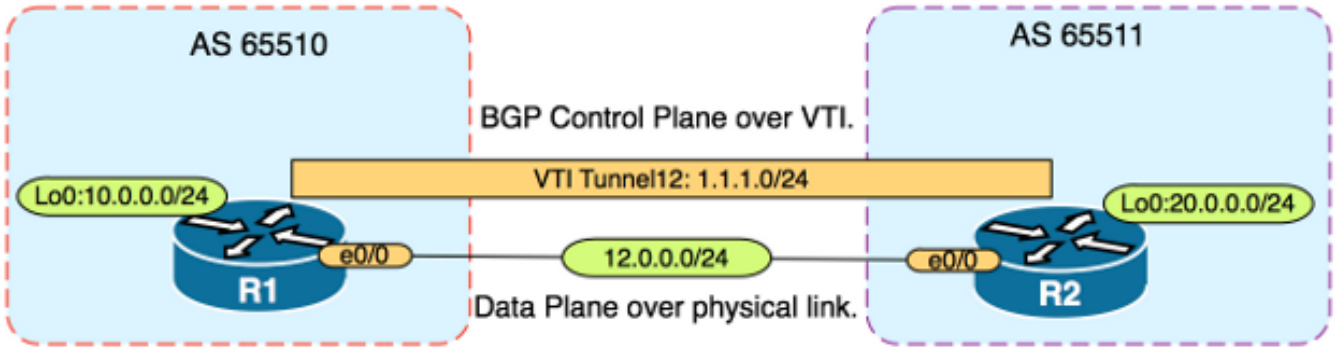
注意：本文中的組態範例使用溫和的密碼演演算法，這些演演算法可能適合也可能不適合您的

環境。有關各種密碼套件和金鑰大小的相對安全性的討論，請參閱下一代加密白皮書。

設定

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



組態

請完成以下步驟：

1. 在R1和R2上使用R1上的預共用金鑰配置Internet金鑰交換(IKE)第1階段引數： **附註**：不要使用DH組編號1、2或5，因為它們被視為下級。如有可能，請使用具有橢圓曲線加密(ECC)的DH組，例如組19、20或24。高級加密標準(AES)和安全雜湊演算法256(SHA256)應被視為分別優於資料加密標準(DES)/3DES和消息摘要5(MD5)/SHA1。切勿在生產環境中使用密碼「cisco」。**R1配置**

```
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配置

```
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. 為R1和R2上的NVRAM中的預共用金鑰配置6級密碼加密。這樣可以降低在路由器受到威脅時讀取以明文儲存的預共用金鑰的可能性：

```
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
```

附註：啟用6級密碼加密後，活動配置將不再顯示預共用金鑰的純文字檔案版本：

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

!
```

3. 在R1和R2上配置IKE階段2引數： **R1配置**

```
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配置

```
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
```

附註：設定完全轉發保密(PFS)是可選的，但會提高VPN強度，因為它會強制在IKE第2階段SA建立中生成新的對稱金鑰。

4. 在R1和R2上配置隧道介面，並使用IPsec配置檔案進行安全保護： **R1配置**

```
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配置

```
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. 在R1和R2上配置BGP，並將loopback0網路通告到BGP: **R1配置**

```
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配置

```
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. 在R1和R2上配置路由對映，以手動更改下一跳IP地址，使其指向物理介面而不是隧道。您必須將此路由對映應用於入站方向。 **R1配置**

```
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配置

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

驗證IKE第1階段和IKE第2階段均已完成。 在IKE第2階段完成之前，虛擬通道介面(VTI)上的線路通訊協定不會變更為「up」：

```
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
```

請注意，在應用路由對映之前，下一跳IP地址指向BGP鄰居IP地址，該地址是隧道介面：

```
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
```

流量使用通道時，MTU會限製為通道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
```

應用路由對映後，IP地址將更改為R2的物理介面，而不是隧道：

```
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
```

變更資料平面，以使用實體下一個躍點，而不是允許標準大小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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。