在雙ISP場景中配置ASA虛擬通道介面

目錄

簡介

本文檔介紹如何使用IKEv2（Internet金鑰交換版本2）協定在兩個自適應安全裝置(ASA)之間配置VTI（虛擬隧道介面）以提供兩個分支機構之間的安全連線。兩個分支機構都有兩個ISP鏈路，用於實現高可用性和負載均衡。邊界閘道通訊協定(BGP)鄰居關係是透過通道建立，以便交換內部路由資訊。
ASA 9.8(1)版引入了此功能。ASA VTI實施與IOS路由器上可用的VTI實施相容。

必要條件

需求

思科建議您瞭解以下主題：

- BGP通訊協定

採用元件

本文檔中的資訊基於運行9.8(1)6軟體版本的ASAv防火牆。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

VTI和密碼編譯對應之間的差異

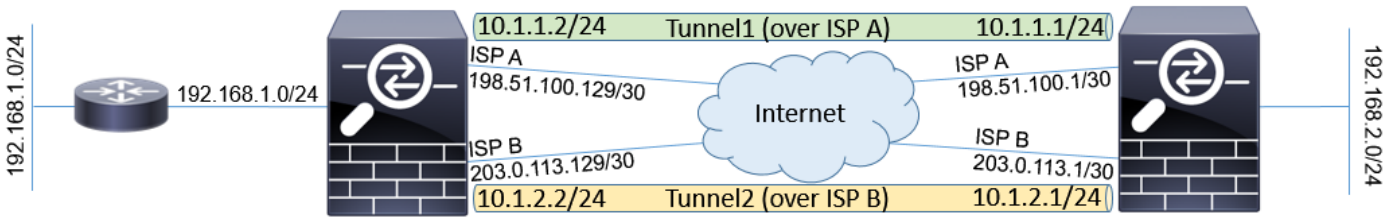
- 加密對映是介面的輸出功能。為了透過基於密碼編譯對應之通道傳送流量，流量需要路由到面對網際網路的介面（傳統上稱為外部介面），且必須針對密碼編譯ACL進行配對。另一方面

，VTI是一個邏輯介面。到每個VPN對等點的隧道由不同的VTI表示。如果路由指向VTI，則資料包將被加密並傳送到對應的對等裝置。

- VTI無需使用加密訪問清單和網路地址轉換(NAT)免除規則。
- 加密對映訪問控制清單(ACL)不允許重疊條目。VTI是基於路由的VPN，並且適用於VPN流量的常規路由規則可簡化配置和故障排除流程。
- 如果通道關閉，加密對映將自動阻止以明文形式傳送站點之間的流量。VTI不會自動對其進行保護。需要新增Null路由以確保功能相同。

設定

網路圖表



組態

注意:此示例不適用於ASA是獨立自治系統成員且與ISP網路具有BGP對等性的情況。它涵蓋的拓撲是ASA具有兩條獨立的ISP鏈路，這些鏈路具有來自不同自治系統的公有地址。在這種情況下，ISP可以部署反欺騙保護，以驗證收到的資料包是否來自屬於另一個ISP的公共IP。在此配置中，會採取適當措施以防止發生這種情況。

1. 常見的加密和身份驗證引數。有關推薦的加密引數的資訊，請訪問：https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

   在兩個ASA上：

```
crypto ikev2 policy 10
encryption aes-256
integrity sha256
group 24
prf sha256
lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal PROP
protocol esp encryption aes-256
protocol esp integrity sha-256
```

2. 配置IPsec配置檔案。一方必須是發起方，一方必須為IKEv2協商的響應方：

   ASA左側：

```
crypto ipsec profile PROF
set ikev2 ipsec-proposal PROP
set pfs group24
```

```
responder-only
```

ASA許可權：

```
crypto ipsec profile PROF
set ikev2 ipsec-proposal PROP
set pfs group24
```

3. 在兩個ISP介面上啟用IKEv2協定。

兩個ASA:

```
crypto ikev2 enable ispa
crypto ikev2 enable ispb
```

4. 配置預共用金鑰以對ASA進行相互身份驗證：

ASA左側：

```
tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
tunnel-group 203.0.113.1 type ipsec-l2l
tunnel-group 203.0.113.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

ASA許可權：

```
tunnel-group 198.51.100.129 type ipsec-l2l
tunnel-group 198.51.100.129 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
tunnel-group 203.0.113.129 type ipsec-l2l
tunnel-group 203.0.113.129 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

5. 配置ISP介面：

ASA左側：

```
interface GigabitEthernet0/1
nameif ispa
security-level 0
ip address 198.51.100.129 255.255.255.252
!
interface GigabitEthernet0/2
nameif ispb
security-level 0
ip address 203.0.113.129 255.255.255.252
!
```

ASA許可權：

```
interface GigabitEthernet0/1
```

```
nameif ispa
security-level 0
ip address 198.51.100.1 255.255.255.252
!
interface GigabitEthernet0/2
nameif ispb
security-level 0
ip address 203.0.113.1 255.255.255.252
!
```

6. 主要鏈路是ISP A介面。ISP B是輔助路由器。使用ICMP ping請求對網際網路中的主機跟蹤主鏈路的可用性，在本示例中，ASA使用彼此的ISP A介面作為ping目標：

ASA左側：

```
sla monitor 1
type echo protocol ipIcmpEcho 198.51.100.1 interface ispa
!
sla monitor schedule 1 life forever start-time now
!
track 1 rtr 1 reachability
!
route ispa 0.0.0.0 0.0.0.0 198.51.100.130 1 track 1
route ispb 0.0.0.0 0.0.0.0 203.0.113.130 10
```

ASA許可權：

```
sla monitor 1
type echo protocol ipIcmpEcho 198.51.100.129 interface ispa
!
sla monitor schedule 1 life forever start-time now
!
track 1 rtr 1 reachability
!
route ispa 0.0.0.0 0.0.0.0 198.51.100.2 1 track 1
route ispb 0.0.0.0 0.0.0.0 203.0.113.2 10
```

7. 主要VTI始終通過ISP A建立。輔助VTI通過ISP B建立。需要通往隧道目的地的靜態路由。這可確保加密資料包從正確的物理介面離開，以避免ISP反欺騙丟棄：

ASA左側：

```
route ispa 198.51.100.1 255.255.255.255 198.51.100.130 1
route ispb 203.0.113.1 255.255.255.255 203.0.113.130 1
```

ASA許可權：

```
route ispa 198.51.100.129 255.255.255.255 198.51.100.2 1
route ispb 203.0.113.129 255.255.255.255 203.0.113.2 1
```

8. VTI配置：

ASA左側：

```
interface Tunnel1
nameif tuna
ip address 10.1.1.2 255.255.255.0
tunnel source interface ispa
tunnel destination 198.51.100.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
!
interface Tunnel2
nameif tunb
ip address 10.1.2.2 255.255.255.0
tunnel source interface ispb
tunnel destination 203.0.113.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

ASA許可權：

```
interface Tunnel1
nameif tuna
ip address 10.1.1.1 255.255.255.0
tunnel source interface ispa
tunnel destination 198.51.100.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
!
interface Tunnel2
nameif tunb
ip address 10.1.2.1 255.255.255.0
tunnel source interface ispb
tunnel destination 203.0.113.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

9. BGP配置。與ISP A關聯的隧道是主隧道。在ISP B上形成的隧道上通告的字首具有較低的本地優先順序，這使得路由表不太優先使用它們：

ASA左側：

```
route-map BACKUP permit 10
set local-preference 80
!
router bgp 65000
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.1.1.1 remote-as 65000
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 next-hop-self
neighbor 10.1.2.1 remote-as 65000
neighbor 10.1.2.1 activate
neighbor 10.1.2.1 next-hop-self
neighbor 10.1.2.1 route-map BACKUP out
network 192.168.1.0
no auto-summary
no synchronization
exit-address-family
```

ASA許可權：

```
route-map BACKUP permit 10
set local-preference 80
!
router bgp 65000
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.1.1.2 remote-as 65000
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 next-hop-self
neighbor 10.1.2.2 remote-as 65000
neighbor 10.1.2.2 activate
neighbor 10.1.2.2 next-hop-self
neighbor 10.1.2.2 route-map BACKUP out
network 192.168.2.0
no auto-summary
no synchronization
exit-address-family
```

10. （可選）為了通告未直接連線到它的剩餘ASA後面的其他網路，可以配置靜態路由重分發：

ASA左側：

```
route inside 192.168.10.0 255.255.255.0 192.168.1.100 1
!
prefix-list REDISTRIBUTE_LOCAL seq 10 permit 192.168.10.0/24
!
route-map REDISTRIBUTE_LOCAL permit 10
match ip address prefix-list REDISTRIBUTE_LOCAL
!
router bgp 65000
address-family ipv4 unicast
redistribute static route-map REDISTRIBUTE_LOCAL
```

11. （可選）流量可根據封包目的地在通道之間進行負載平衡。在本示例中，通往192.168.10.0/24網路的路由優先於備用隧道（ISP B隧道）

    ASA左側：

```
route-map BACKUP permit 5
match ip address prefix-list REDISTRIBUTE_LOCAL
set local-preference 200
!
route-map BACKUP permit 10
set local-preference 80
```

12. 為了防止隧道關閉時站點之間的流量以明文形式傳送到網際網路，需要新增空路由。為了簡便起見，新增了所有RFC1918地址：

    兩個ASA:

```
route Null0 10.0.0.0 255.0.0.0 250
route Null0 172.16.0.0 255.240.0.0 250
route Null0 192.168.0.0 255.255.0.0 250
```

13.（可選）預設情況下，ASA BGP進程每60秒傳送一次keepalive。如果180秒內未從對等方收到keepalive響應，則宣告該響應已停止。為了加速檢測鄰居故障，您可以配置BGP計時器。在本範例中，keepalive每10秒傳送一次，而30秒後鄰居就會被宣佈關閉。

```
router bgp 65000
address-family ipv4 unicast
neighbor 10.1.1.2 timers 10 30
neighbor 10.1.2.2 timers 10 30
exit-address-family
```

驗證

驗證IKEv2通道是否啟動：

```
ASA-right(config)# show crypto ikev2 sa

IKEv2 SAs:

Session-id:32538, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
836052177 198.51.100.1/500 198.51.100.129/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:24, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/7 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
```

```
ESP spi in/out: 0xc6623962/0x5c4a3bce

IKEv2 SAs:

Session-id:1711, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
832833529 203.0.113.1/500 203.0.113.129/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:24, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/29 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x2e3715af/0xc20e22b4
```

驗證BGP鄰居關係狀態：

```
ASA-right(config)# show bgp summary
BGP router identifier 203.0.113.1, local AS number 65000
BGP table version is 29, main routing table version 29
3 network entries using 600 bytes of memory
5 path entries using 400 bytes of memory
5/3 BGP path/bestpath attribute entries using 1040 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2040 total bytes of memory
BGP activity 25/22 prefixes, 69/64 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.2 4 65000 6 5 29 0 0 00:00:51 2
10.1.2.2 4 65000 7 6 29 0 0 00:01:20 2
```

驗證從BGP收到的路由。標籤有「>」的路由將安裝在路由表中：

```
ASA-right(config)# show bgp

BGP table version is 29, local router ID is 203.0.113.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*>i192.168.1.0 10.1.1.2 0 100 0 i
* i 10.1.2.2 0 80 0 i
*> 192.168.2.0 0.0.0.0 0 32768 i
* i192.168.10.0 10.1.1.2 0 100 0 ?
*>i 10.1.2.2 0 200 0 ?

Verify routing table:

ASA-right(config)# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 198.51.100.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.2, ispa
S 10.0.0.0 255.0.0.0 is directly connected, Null0
C 10.1.1.0 255.255.255.0 is directly connected, tuna
L 10.1.1.1 255.255.255.255 is directly connected, tuna
C 10.1.2.0 255.255.255.0 is directly connected, tunb
L 10.1.2.1 255.255.255.255 is directly connected, tunb
S 172.16.0.0 255.240.0.0 is directly connected, Null0
S 192.168.0.0 255.255.0.0 is directly connected, Null0
B 192.168.1.0 255.255.255.0 [200/0] via 10.1.1.2, 00:02:06
C 192.168.2.0 255.255.255.0 is directly connected, inside
L 192.168.2.1 255.255.255.255 is directly connected, inside
B 192.168.10.0 255.255.255.0 [200/0] via 10.1.2.2, 00:02:35
C 198.51.100.0 255.255.255.252 is directly connected, ispa
L 198.51.100.1 255.255.255.255 is directly connected, ispa
S 198.51.100.129 255.255.255.255 [1/0] via 198.51.100.2, ispa
C 203.0.113.0 255.255.255.252 is directly connected, ispb
L 203.0.113.1 255.255.255.255 is directly connected, ispb
S 203.0.113.129 255.255.255.255 [1/0] via 203.0.113.2, ispb
```

疑難排解

用於對IKEv2協定進行故障排除的調試：

debug crypto ikev2 protocol 4
debug crypto ikev2 platform 4

有關IKEv2協定故障排除的詳細資訊：
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

有關疑難排解BGP通訊協定的詳細資訊：
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

相關資訊

- **BGP路由選擇規則：**
  https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- **ASA BGP配置指南：**
  https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- **技術支援與文件 - Cisco Systems**