在双ISP场景中配置ASA虚拟隧道接口

目录

简介

本文档介绍如何使用IKEv2（Internet密钥交换版本2）协议在两个分支机构之间提供安全连接，在两个ASA（自适应安全设备）之间配置VTI（虚拟隧道接口）。两个分支机构都有两个ISP链路，以实现高可用性和负载均衡。边界网关协议(BGP)邻居关系在隧道上建立，以便交换内部路由信息。此功能在ASA版本9.8(1)中引入。ASA VTI实施与IOS路由器上提供的VTI实施兼容。

先决条件

要求

Cisco 建议您了解以下主题：

- BGP协议

使用的组件

本文档中的信息基于运行9.8(1)6软件版本的ASAv防火墙。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

VTI与加密映射之间的差异

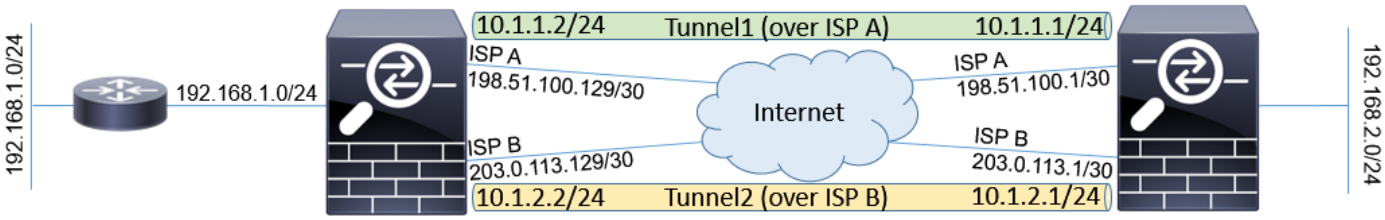
- 加密映射是接口的输出功能。为了通过基于加密映射的隧道发送流量，流量需要路由到面向互联网的接口（通常称为外部接口），并且必须与加密ACL匹配。另一方面，VTI是逻辑接口。到每个VPN对等体的隧道由不同的VTI表示。如果路由指向VTI，则数据包将被加密并发送到相应

的对等体。

- VTI无需使用加密访问列表和网络地址转换(NAT)免除规则。
- 加密映射访问控制列表(ACL)不允许重叠条目。VTI是基于路由的VPN，VPN流量应用常规路由规则，可简化配置和故障排除过程。
- 如果隧道关闭，加密映射会自动阻止以明文形式发送站点之间的流量。VTI不会自动防范它。需要添加空路由，以确保功能相同。

配置

网络图



配置

注意: **此示例不适用于ASA是独立自治系统成员且与ISP网络有BGP对等的场景。**它涵盖拓扑，其中ASA有两条独立的ISP链路，这些链路的公有地址来自不同的自治系统。在这种情况下，ISP可以部署反欺骗保护，以验证收到的数据包是否并非来自属于另一ISP的公有IP。在此配置中，会采取适当措施来防止这种情况。

1. 常见加密和身份验证参数。有关推荐加密参数的信息，请访问：https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

   在两个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配置文件。其中一端必须是发起方，另一端必须是IKEv2协商的响应方：

   ASA左侧：

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

ASA权限：

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

3. 在两个ISP接口上启用IKEv2协议。

两个ASA:

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

4. 配置预共享密钥以相互验证ASA:

ASA左侧：

```
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权限：

```
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接口：

ASA左侧：

```
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权限：

```
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. 主链路是ISP A接口。ISP B是辅助。主链路可用性通过使用ICMP ping请求跟踪到Internet中的主机，在本例中，ASA使用彼此的ISP A接口作为ping目的：

   ASA左侧：

```
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权限：

```
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VTI始终在ISP A上建立。辅助VTI在ISP B上建立。需要通向隧道目的地的静态路由。这可确保加密数据包从正确的物理接口离开，以避免ISP防欺骗丢弃：

   ASA左侧：

```
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权限：

```
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左侧：

```
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权限：

```
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。与ISP A关联的隧道是主隧道。通过ISP B形成的隧道通告的前缀具有较低的本地优先级，这使路由表更不优先：

ASA左侧：

```
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权限：

```
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. （可选）为了通告未直接连接到的ASA后面的其他网络，可以配置静态路由重分发：

ASA左侧：

```
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. （可选）可以根据数据包目的地在隧道之间负载均衡流量。在本示例中，通向192.168.10.0/24网络的路由优先于备用隧道（ISP B隧道）

    ASA左侧：

```
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. 为防止在隧道关闭时以明文形式将站点之间的流量发送到互联网，需要添加空路由。为简单起见，添加了所有RFC1918地址：

    两个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.（可选）默认情况下，ASA BGP进程每60秒发送一次keepalive。如果在180秒内未从对等设备收到keepalive响应，则会声明其为dead。为了加快检测邻居故障，您可以配置BGP计时器。在本例中，keepalive每10秒发送一次，邻居在30秒后声明关闭。

```
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
```

验证

验证IKEv2隧道是否已启用：

```
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
```

验证BGP邻居状态：

```
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
```

检验从BGP收到的路由。标有“>”的路由将安装在路由表中：

```
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
```

故障排除

用于排除IKEv2协议故障的调试：

debug crypto ikev2 protocol 4
debug crypto ikev2 platform 4

有关IKEv2协议故障排除的详细信息：
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

有关BGP协议故障排除的详细信息：
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

相关信息

- **BGP路由选择规则：**
  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
- 技术支持和文档 - Cisco Systems