配置在双重ISP方案的ASA虚拟隧道接口

目录

简介

本文描述如何配置VTI (虚拟通道Intrfaces)在两ASA (可适应安全工具)之间与使用IKEv2 (互联网密钥交换提供两个分组之间的安全连接的版本2)协议。两个分组有高availablility和负载均衡目的的两条ISP链路。边界网关协议(BGP)结邻在通道设立为了交换内部路由信息。
此功能在ASA版本9.8(1)介绍。ASA VTI实施是与VTI在IOS路由器的实施联机兼容。

先决条件

要求

Cisco 建议您了解以下主题：

- BGP协议

使用的组件

本文档中的信息根据运行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。如果您的网络实际，请保证您了解所有命令潜在影响。

在VTI和加密映射之间的区别

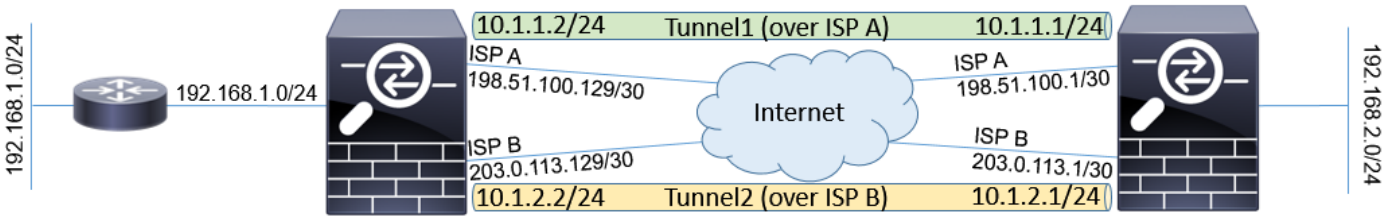
- 加密映射是接口的输出功能。为了发送流量通过加密映射根据通道，流量需要路由到面对接口的互联网(传统上呼叫外部接口)并且必须匹配加密ACL。另一方面， VTI是逻辑接口。对每VPN对等项的通道由一不同的VTI代表。如果往VTI的路由点，数据包将加密并且发送给对应的

对等体。

- VTI排除需要使用crypto访问列表和网络地址转换(NAT)免税规则。
- 加密映射访问控制表(ACL)不允许交迭的条目。VTI是路由基于VPN，并且正常路由规则为VPN流量适用，简单化配置并且处理排除故障。
- 如果通道发生故障，加密映射自动地防止在明文将发送的站点之间的流量。VTI不自动地防止受到它。无效路由需要被添加保证相等的功能。

配置

网络图



配置

Note: 此示例不适用于ASA是independed自治系统成员并且有与ISP网络的BGP对等互连的方案。它包括ASA有与公共地址的两条独立ISP链路从不同自治系统的拓扑。在这样案件中，ISP可能部署验证的反欺骗保护，如果收到的信息包从属于另一个ISP的公有IP没有被发出。在此配置中，适当的措施采取防止此。

1. 普通的加密和验证参数。关于推荐的密码参数的信息可以找到在：https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

   在两ASA ：

```
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简档。其中一侧必须是发起者，并且一个需要是IKEv2协商的响应方：

   被留下的ASA ：

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

ASA权利：

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

3. 在两个ISP接口的Enable (event) IKEv2协议。

两ASA ：

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

4. 配置预先共享密钥相互验证ASA ：

被留下的ASA ：

```
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权利：

```
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：

被留下的ASA ：

```
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权利：

```
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是附属的。主链路可用性跟踪与使用对一台主机的ICMP Ping请求在互联网里，在本例中ASA使用ISP A接口作为ping目的地：

   被留下的ASA ：

```
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权利：

```
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. 主要的VTI在ISP A. Secondary VTI总是设立在ISP B.往隧道目的地的静态路由是需要的Static设立。这保证从避免正确的物理接口的加密的信息包事假ISP反欺骗丢包：

   被留下的ASA ：

```
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权利：

```
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：

   被留下的ASA ：

```
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权利：

```
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。通道关联与ISP A主要的。在路由表做他们较少首选的通道通告的前缀形成在ISP B有更低本地prefernce ：

被留下的ASA ：

```
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权利：

```
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)为了通告没有直接地连接对它在左侧ASA后的另外的网络，静态路由再分配可以配置：

被留下的ASA ：

```
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)流量可以是负载被均衡在根据信息包目的地的通道之间。在本例中，往192.168.10.0/24网络的路由在备份通道(ISP B通道)被偏好

    被留下的ASA ：

```
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. 要防止站点之间的流量发送在明文对互联网，如果通道发生故障，无效路由需要被添加。所有RFC1918地址被添加的为了简化：

    两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进程发送Keepalive一次每60秒。如果Keepalive响应没有从对等体接收180秒，被宣称死。为了加速检测neigbor失败，您能配置BGP计时器。在本例中，Keepalive被发送每10秒，并且邻居在30秒之后被宣称下来。

```
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

如果IKEv2通道是UP，请验证：

```
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结邻状态：

```
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
```

验证从BGP接收的路由。路由标记用“>”在路由表里安装：

```
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

用于的调试排除故障IKEv2协议：

debug crypto ikev2协议4
debug crypto ikev2平台4

关于排除故障IKEv2协议的更多信息：
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

关于排除故障BGP协议的更多信息：
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