تكوين واجهات النفق الظاهرية ASA في سيناريو ISP المزدوج

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاختلافات بين خريطة VTI و crypto
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تكوين VTI (واجهات النفق الظاهري) بين جهاز ASAs (أجهزة الأمان المعدلة) باستخدام بروتوكول IKEv2 (تبادل مفاتيح الإنترنت الإصدار 2) لتوفير اتصال آمن بين فرعين. ولكل من الفرعين إرتباطات ISP لأغراض التوفر الفائق وموازنة الأحمال. يتم إنشاء منطقة جوار لبروتوكول العبارة الحدودية (BGP) عبر الأنفاق من أجل تبادل معلومات التوجيه الداخلية.
يتم تقديم هذه الميزة في ASA، الإصدار 9.8(1). يتوافق تنفيذ ASA VTI مع تنفيذ VTI المتاح على موجهات IOS.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- بروتوكول BGP

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جدران حماية ASAv التي تشغل إصدار البرنامج 9.8(1)6.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاختلافات بين خريطة VTI و crypto

- خريطة التشفير هي ميزة إخراج للواجهة. لإرسال حركة المرور عبر النفق المستند إلى خريطة التشفير، يلزم توجيه حركة مرور البيانات إلى واجهة واجهة واجهة واجهة الإنترنت (التي تسمى بشكل تقليدي الواجهة الخارجية) ويجب مطابقتها مع قائمة التحكم في الوصول (ACL) للتشفير. ومن ناحية أخرى، فإن VTI واجهة منطقية. يتم تمثيل النفق إلى كل نظير من نظراء شبكات VPN بواسطة VTI مختلف. إن يشير التوجيه باتجاه VTI، الربط سيتم تشفيرها وإرسالها إلى النظير المتوافق.

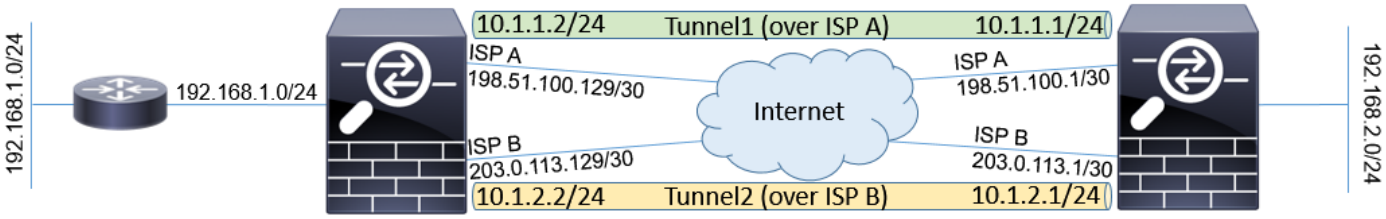
- VTI يزيل الحاجة إلى إستخدام قوائم الوصول إلى التشفير وقواعد إستثناء ترجمة عنوان الشبكة (NAT).

- لا تسمح قائمة التحكم في الوصول إلى خريطة التشفير (ACL) بإدخالات متداخلة. VTI هو شبكة VPN تستند إلى المسار وتنطبق قواعد التوجيه العادية لحركة مرور VPN، والتي تبسط التكوين والعمليات لاستكشاف الأخطاء وإصلاحها.

- تمنع خريطة التشفير حركة مرور البيانات بين المواقع المراد إرسالها بنص غير مشفر إذا كان النفق معطل. لا تحمي VTI تلقائيا من ذلك. يجب إضافة المسارات الفارغة لضمان تساوي الوظائف.

التكوين

الرسم التخطيطي للشبكة



التكوينات

ملاحظة: هذا المثال غير مناسب للسيناريو الذي يكون فيه ASA عضوا في نظام مستقل مستقل مستقل مستقل مستقل بذاته وله روابط BGP مع شبكات ISP. وهو يغطي الطبوولوجيا التي تحتوي فيها ASA على ربطتين مستقلتين موزدتي خدمات الإنترنت (ISP) مع العناوين العامة من أنظمة مستقلة مختلفة. في هذه الحالة، يمكن أن يقوم ISP بنشر حمايه من الانتحال تحقق مما إذا لم يتم الحصول على الحزم المستلمة من IP العام الذي ينتمي إلى ISP آخر. وفي هذا التكوين، يتم إتخاذ التدابير المناسبة لمنع هذا.

1. معلمات التشفير والمصادقة الشائعة. يمكن العثور على معلومات حول معلمات التشفير الموصى بها في:
   https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

   على كل من ASAs:

```
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. قم بتكوين ملف تعريف IPsec. يجب أن يكون أحد الجانبين هو البادئ ويجب أن يكون أحد الطرفين هو المستجيب لمفاوضات IKEv2:

ASA إلى اليسار:

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

ASA يمين:

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

3. قم بتمكين بروتوكول IKEv2 على كل واجهات ISP.

كل من ASA:

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

4. قم بتكوين المفتاح المشترك مسبقا للمصادقة المتبادلة على ASAs:

ASA إلى اليسار:

```
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 يمين:

```
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. تكوين واجهات ISP:

ASA إلى اليسار:
```
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 يمين:
```
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. الارتباط الأساسي هو واجهة ISP A. يعد ISP B ثانويا. يتم تعقب توفر الارتباط الأساسي باستخدام طلب إختبار اتصال ICMP لمضيف في الإنترنت، في هذا المثال، يستخدم ASAs بعضهم بعضا واجهة ISP A كوجهة إختبار اتصال:

ASA إلى اليسار:
```
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 يمين:
```
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. يتم إنشاء VTI الأساسي عبر ISP A. يتم إنشاء VTI الثانوي عبر ISP B. يلزم وجود طريق ثابت باتجاه وجهة النفق. وهذا يضمن أن الحزم المشفرة تترك من الواجهة المادية الصحيحة لتجنب حالات السقوط المضادة لانتحال ISP:

ASA إلى اليسار:
```
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 يمين:

```
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. تكوين VTI:

ASA إلى اليسار:

```
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 يمين:

```
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. تكوين BGP. يعد النفق المرتبط ب ISP A أساسي. تتميز البادئات المعلن عنها عبر النفق الذي تم تكوينه عبر ISP B ببادئة محلية أقل، مما يجعلها أقل تفضيلا بواسطة جدول التوجيه:

ASA إلى اليسار:

```
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 يمين:

```
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. (إختياري) للإعلان عن شبكة إضافية خلف ASA الأيسر غير المتصلة مباشرة به، يمكن تكوين إعادة توزيع المسار الثابت:

    ASA إلى اليسار:

```
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. (إختياري) يمكن موازنة حمل حركة المرور بين الأنفاق استنادا إلى وجهة الحزمة. في هذا المثال، يفضل التوجيه إلى شبكة 192.168.10.0/24 على نفق النسخ الاحتياطي (ISP B tunnel)

    ASA إلى اليسار:

```
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. لمنع إرسال حركة مرور البيانات بين المواقع بنص واضح إلى الإنترنت إذا كانت RFC1918 عناوين جميع إضافة تمت .فاشلة مسارات إضافة يلزم ،الأنفاق معظم للبساطة:

    ASA كل من:

```
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. (إختياري) بشكل افتراضي، ترسل عملية ASA BGP رسائل keepalives مرة واحدة لكل 60 ثانية. إذا لم يتم تلقي إستجابة keepalive من النظير لمدة 180 ثانية، يتم الإعلان عن

وفاتها. لزيادة سرعة فشل قاعدة الكشف، يمكنك تكوين وحدات توقيت BGP. في هذه المثال، يتم إرسال رسائل keepalives كل 10 ثوان ويتم الإعلان عن المجاور مع الطع بعد 30 ثانية.

```
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
```

التحقق من الصحة

التحقق من تشغيل نفق IKEv2:

```
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
```

التحقق من حالة جوار BGP:

```
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
```

التحقق من المسارات المستلمة من BGP. يتم تثبيت المسارات التي تحمل علامة ">" في جدول التوجيه:

```
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
```

استكشاف الأخطاء وإصلاحها

تصحيح الأخطاء المستخدمة لاستكشاف أخطاء بروتوكول IKEv2 وإصلاحها:

```
debug crypto ikev2 protocol 4
debug crypto ikev2 platform 4
```

للحصول على مزيد من المعلومات حول أستكشاف أخطاء بروتوكول IKEv2 وإصلاحها:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

للحصول على مزيد من المعلومات حول أستكشاف أخطاء بروتوكول BGP وإصلاحها:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

معلومات ذات صلة

- قواعد تحديد مسار BGP:
  https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- دليل تكوين ASA BGP:
  https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).