تكوين جلسة عمل eBGP آمنة باستخدام VTI ل IPsec

المحتويات

المقدمة

يوضح هذا المستند كيفية تأمين علاقة مجاورة لبروتوكول العبارة الحدودية الخارجية (eBGP) باستخدام واجهة النفق الظاهرية (VTI) ل IPsec مع الواجهات المادية (غير النفق) لحركة مرور مستوى البيانات. وتتضمن فوائد هذا التكوين ما يلي:

- الخصوصية الكاملة لجلسة عمل جوار BGP مع سرية البيانات ومقاومة إعادة التشغيل والأصالة والنزاهة.
- لا يتم تقييد حركة مرور مستوى البيانات بالنقل العلوي لوحدة الإرسال القصوى (MTU) لواجهة النفق. يمكن للعملاء إرسال حزم MTU قياسية (1500 بايت) دون أي تأثيرات على الأداء أو التجزئة.
- مصروفات عامة أقل على موجهات النقطة الطرفية نظرا لأن تشفير/فك تشفير فهرس سياسة الأمان (SPI) يقتصر على حركة مرور مستوى التحكم في BGP.

فائدة هذا التكوين هي أن مستوى البيانات غير مقيد بتقييد الواجهة النفقي. بالتصميم، لم يتم تأمين حركة مرور مستوى البيانات بواسطة IPsec.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أساسيات تكوين eBGP والتحقق منه
- التلاعب في محاسبة سياسة BGP (PA) باستخدام خريطة المسار
- ميزات سياسة بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت الأساسي (ISAKMP) و IPsec

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى برنامج Cisco IOS® الإصدار 15.3(1.3)T ولكن تعمل الإصدارات الأخرى المدعومة. نظرا لأن تكوين IPsec وميزة تشفير، تأكد من أن إصدار الرمز الخاص بك يحتوي على مجموعة الميزات هذه.

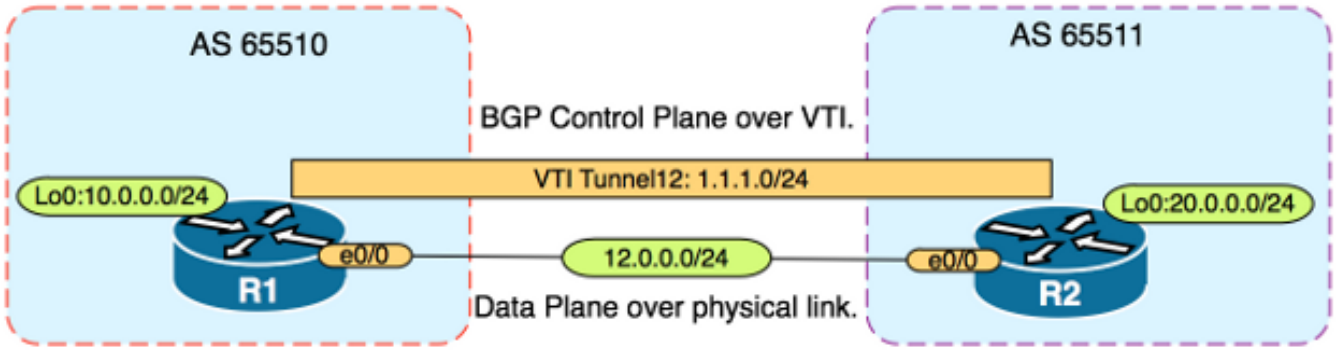
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

> **تحذير**: يستخدم مثال التكوين في هذا المستند خوارزميات تشفير متوافقة قد تكون غير مناسبة لبيئتك أو قد لا تكون مناسبة لها. راجع التقرير الرسمي للتشفير من الجيل التالي لمناقشة الأمان النسبي لمختلف مجموعات التشفير وأحجام المفاتيح.

التكوين

> **ملاحظة**: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة



التكوينات

أكمل الخطوات التالية:

1. قم بتكوين معلمات المرحلة 1 لـ Internet Key Exchange (IKE) على R1 و R2 باستخدام المفاتيح المشتركة مسبقا على R1: **ملاحظة**: استخدم أبدا أقوى مجموعة DH 1 أو 2 أو 5 المدعومة. إذا أمكن إستخدام مجموعة DH مع تشفير المنحنى البيضاوي أنها تعتبر أقل قيمة. يجب إعتبار معيار التشفير المتقدم (AES) 19 أو 20 أو 24. مثل المجموعات (ECC) 256 (SHA256) أفضل من معيار تشفير البيانات (DES)/3DES وخوارزمية التجزئة الآمنة و Message Digest 5 (MD5)/SHA1 على التوالي. استخدم كلمة المرور "cisco" أبدا في بيئة إنتاج.**تكوين R1**

```
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
```

تكوين R2

```
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. قم بتكوين تشفير كلمة المرور للمستوى 6 للمفاتيح المشتركة مسبقا في ذاكرة التخزين المؤقت لمفاتيح المشتركة مسبقا على R1 و R2. تحقق من هذه المفاتيح المشتركة مسبقا على NVRAM في النص العادي إذا تم أخذ لقطة للتكوين الحالي:

```
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
```

ملاحظة: بمجرد تمكين تشفير كلمة مرور المستوى 6، لن يعرض التكوين النشط إصدار النص العادي للمفاتيح المشتركة مسبقا:

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

!
```

3. تكوين معلمات المرحلة 2 من IKE على R1 و R2: **تكوين R1**

```
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
```

تكوين R2

```
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
```

ملاحظة: يعد تعيين السرية التامة لإعادة التوجيه (PFS) أمرا إختياريا ولكنه يحسن من إنشاء مفاتيح تم إختراقها في جديد إنشاء IKE المرحلة 2 SA.

4. قم بتكوين واجهات النفق في R1 و R2 وتأمينها باستخدام ملف تعريف IPsec: **تكوين R1**

```
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
```

تكوين R2

```
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. تكوين BGP على R1 و R2 والإعلان عن شبكات الاسترجاع0 في BGP: **تكوين R1**

```
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
```

تكوين R2

```
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. قم بتكوين خريطة مسار على R1 و R2 لتغيير عنوان IP للخطوة التالية يدويا حتى يشير إلى الواجهة المادية وليس إلى النفق. يجب تطبيق مخطط المسار هذا على الإتجاه الوارد. **تكوين R1**

```
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
```

تكوين R2

```
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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

[دعم أداة مترجم الإخراج (للعملاء المسجلين فقط) عرض أوامر show.](#) استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر show.

تحقق من اكتمال كل من المرحلة الأولى من IKE والمرحلة الثانية من IKE. يتغير الـ VTI إلى "up" حتى تكتمل المرحلة 2 من IKE:

```
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
```

لاحظ أنه قبل تطبيق خريطة المسار، يشير عنوان IP للخطوة التالية إلى عنوان IP المجاور والذي هو واجهة النفق BGP:

```
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
```

عند إستخدام حركة المرور للنفق، يتم تقييد وحدة الحد الأقصى للنقل (MTU) بـ النفق 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
```

بعد تطبيق خريطة المسار، يتم تغيير عنوان IP إلى الواجهة المادية ل R2، وليس النفق:

```
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
```

قم بتغيير مستوى البيانات لاستخدام الخطوة التالية الفعلية بالمقارنة مع النفق الذي يسمح بالحجم القياسي 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
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

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).