تكوين تصغير حركة المرور بين نفقين من موقع إلى موقع

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يرسل VPN حركة مرور بين إثنان VPN نفق على قارن وحيد.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:
· فهم أساسي للموقع المستند إلى السياسة إلى شبكة VPN للموقع
· تجربة مع سطر أوامر ASA

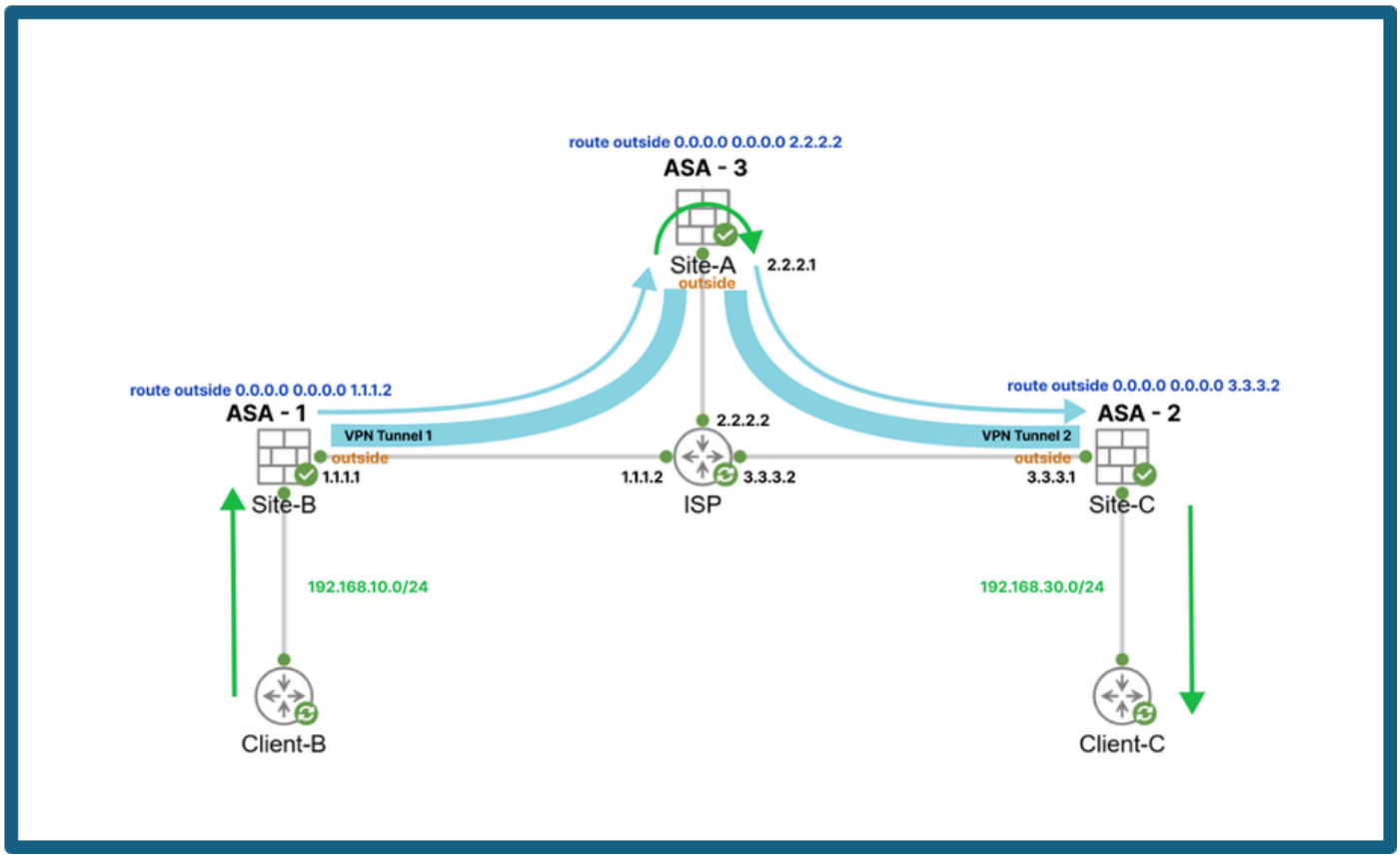
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:
· جهاز الأمان القابل للتكيف (ASA)، الإصدار 9.20
· IKEv1

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.

المخطط



المخطط

معلومات أساسية

يوضح هذا التكوين كيفية إعادة توجيه حركة المرور من نفق من موقع إلى موقع إلى آخر على الجهاز نفسه. لتوضيح هذا الإعداد، إستخدمنا ثلاث وحدات ASA تمثل الموقع A والموقع B والموقع C.

التكوين

يوضح هذا القسم التكوين المطلوب للسماح بحركة المرور من ASA-1 (الموقع ب) إلى ASA-2 (الموقع C) عبر ASA-3 (الموقع A).

لدينا نفقين لشبكة VPN تم تكوينهما:

- نفق VPN 1 : نفق VPN بين الموقع B والموقع A
- نفق VPN رقم 2 : نفق VPN بين الموقع C والموقع A

للحصول على إرشادات تفصيلية حول كيفية إنشاء نفق VPN مستند إلى السياسة

عل ASA، ارجع إل قسم تكوين ASA ف وثائق Cisco: تكوين نفق IPSec IKEv1 بين ASA وموجه XE من Cisco IOS

ASA (الموقع ب) تشكيل

نحتاج إل السماح بحركة المرور من شبكة الموقع-B إل شبكة الموقع-C ف قائمة الوصول الخاصة بالشفرة لنفق VPN 1 عل الواجهة الخارجية ل ASA 1.
ف هذا السيناريو، من 192.168.10.0/24 إل 192.168.30.0/24

قائمة الوصول إل التشفير:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

إستثناء nat:

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.1
```

خريطة التشفير ل VPN Tunnel 1:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA (الموقع C) تكوين التشفير

السماح بحركة المرور من شبكة SITE-C إل شبكة SITE-B ف قائمة الوصول الخاصة بتشفير VPN Tunnel 2 عل الواجهة الخارجية ل ASA 2.

في هذا السيناريو، من 192.168.30.0/24 إلى 192.168.10.0/24

قائمة الوصول إلى التشفير:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

إستثناء nat:

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 1
```

خريطة التشفير ل VPN Tunnel 2:

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

تكوين التشفير (الموقع A) ASA

السماح بحركة المرور من شبكة Site-C إلى شبكة Site-B في قائمة وصول التشفير
الخاصة بنفق VPN 1 وحركة المرور من شبكة Site-B إلى شبكة C في قائمة وصول
التشفير الخاصة بنفق VPN 2 على الواجهة الخارجية ل ASA في Site-A التي تكون في
الإتجاه العكسي لما قمنا بتكوينه على ASAs _.

في هذا السيناريو، من 192.168.30.0/24 إلى 192.168.10.0/24 ل VPN Tunnel 1 ومن
192.168.10.0/24 إلى 192.168.30.0/24 ل VPN Tunnel 2

قائمة الوصول إلى التشفير:

```
object network 192.168.30.0_24
```

```
subnet 192.168.30.0 255.255.255.0

object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

تكوين خريطة التشفير ل VPN Tunnel 1 و 2:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

بالإضافة إلى هذا ألأننا نحتاج إلى توجيه حركة مرور البيانات من الخارج إلى الخارج والتي تكون هي نفس الواجهة مع مستوى الأمان نفسه، فإننا بحاجة إلى تكوين الأمر:

```
same-security-traffic permit intra-interface
```

تدفق حركة المرور من الموقع (ب) إلى الموقع (ج)

لنأخذ بعين الاعتبار حركة المرور التي تم بدء تشغيلها من الموقع B إلى الموقع C من 192.168.30.0/24 إلى 192.168.10.0/24.

الموقع باء (المصدر)

1. يتم توجيه حركة المرور التي بدأت من الإصدار 192.168.10.0/24 network (site-b) والموجهة ل 192.168.30.0/24 network (site-C) إلى الواجهة الخارجية ل ASA-1 استنادا إلى جدول التوجيه الذي تم تكوينه.

2. بمجرد وصول حركة المرور إلى ASA-1، فإنها تطابق قائمة الوصول للتشفير 110 التي تم تكوينها على ASA-1. يؤدي هذا إلى تشغيل تشفير حركة المرور باستخدام نفق VPN 1، الذي يرسل البيانات بشكل آمن نحو الموقع A.

موقع-A (متوسط)

1. حركة المرور المشفرة من 192.168.10.0/24 to 192.168.30.0/24 arrives على الواجهة الخارجية لـ ASA في الموقع أ.
2. في الموقع A، يتم فك تشفير حركة مرور البيانات بواسطة نفق VPN 1 الاستعادة الحمولة الأصلية.
3. وبعد ذلك، تتم إعادة تشفير حركة مرور البيانات التي تم فك تشفيرها باستخدام نفق VPN 2 في الواجهة الخارجية لـ ASA في الموقع A.

موقع-C (الوجهة)

1. حركة المرور المشفرة من 192.168.10.0/24 to 192.168.30.0/24 reaches الواجهة الخارجية لـ ASA-2 في site-C.
2. يقوم ASA-2 بفك تشفير حركة المرور باستخدام نفق VPN 2 وإعادة توجيه الحزم إلى الوجهة المقصودة من 192.168.30.0/24 network، وتسليمها إلى LAN من Site-C.

عكس تدفق حركة المرور من الموقع C إلى الموقع B

ينتج عن تدفق حركة المرور العكسية، التي تنشأ من الموقع-C (192.168.30.0/24) and الخاص بالموقع B (192.168.10.0/24)، نفس العملية ولكن في الإتجاه العكسي:
1. في الموقع C، يتم تشفير حركة مرور البيانات بواسطة نفق VPN 2 قبل إرسالها إلى الموقع A.
2. في الموقع A، يتم فك تشفير حركة مرور البيانات بواسطة نفق VPN 2، ثم يتم إعادة تشفيرها باستخدام نفق VPN 1 قبل إعادة توجيهها إلى الموقع B.
3. في الموقع-B، يتم فك تشفير حركة مرور البيانات بواسطة نفق VPN 1 وتسليمها إلى الإصدار 192.168.10.0/24 network.

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).