ترحيل نفق التشفير المستند إلى السياسة إلى نفق التشفير المستند إلى المسار على ASA

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

خطوات الترحيل:

التكوينات

النفق القائم على السياسة الحالية:

ترحيل النفق المستند إلى السياسة إلى النفق المستند إلى المسار:

التحقق من الصحة

استكشاف الأخطاء وإصلاحها

المقدمة

يوضح هذا المستند ترحيل الأنفاق المستندة إلى السياسات إلى أنفاق تستند إلى التوجيه على ASA.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن أنت تعرف هذا موضوع:

- الفهم الأساسي لمفاهيم IKEv2-IPSec VPN.
- معرفة شبكة VPN من IPSec على ASA وتكوينها.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco ASA: رمز ASA الإصدار 9.8(1) أو إصدار أحدث.

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.

التكوين

خطوات الترحيل:

1. إزالة تكوين VPN الحالي المستند إلى السياسة
2. تكوين ملف تعريف IPSec
3. تكوين واجهة النفق الظاهرية (VTI)
4. تكوين بروتوكول التوجيه الثابت أو بروتوكول التوجيه الديناميكي

التكوينات

النفق القائم على السياسة الحالية:

1. تكوين الواجهة:

واجهة الخروج حيث تكون خريطة التشفير مرتبطة.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
```

2. سياسة IKEv2:

وهو يحدد معلمات المرحلة الأولى من عملية تفاوض IPsec.

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

3. مجموعة الأنفاق:

وهو يحدد معلمات اتصالات VPN. تعتبر مجموعات النفق أساسية لتكوين شبكات VPN من موقع إلى موقع، نظرا لأنها تحتوي على معلومات حول النظير وأساليب المصادقة والمعلمات المختلفة للاتصال.

```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

4. قائمة التحكم في الوصول (ACL) المشفرة:

إنه يحدد حركة المرور التي يجب تشفيرها وإرسالها عبر النفق.

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0

access-list asa-vpn extended permit ip object-group local-network object-group remote-network
```

5. مقترح التشفير IPSec:

وهو يحدد اقتراح IPsec، الذي يحدد خوارزميات التشفير والتكامل للمرحلة 2 من تفاوض IPsec.

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

6. تكوين خريطة التشفير:

وهو يحدد سياسة إتصالات VPN ل IPsec، بما في ذلك حركة المرور التي سيتم تشفيرها وألقارنان ومقترح IPSec الذي تم تكوينه مسبقا. وهو مرتبط أيضا بالقارن الذي يعالج حركة مرور VPN.

```
crypto map outside_map 10 match address asa-vpn
crypto map outside_map 10 set peer 10.20.20.20
crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET

crypto map outside_map interface outside
```

ترحيل النفق المستند إلى السياسة إلى النفق المستند إلى المسار:

1. إزالة تكوين VPN الحالي المستند إلى السياسة:
   أولا، قم بإزالة تكوين VPN الحالي المستند إلى السياسة. ويتضمن ذلك إدخالات خريطة التشفير ذلك النظير، وقوائم التحكم في الوصول (ACL)، أو أي إعدادات ذات صلة.

```
no crypto map outside_map 10 match address asa-vpn
no crypto map outside_map 10 set peer 10.20.20.20
no crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET
```

2. تكوين ملف تعريف IPSec:
   قم بتعريف ملف تعريف IPsec باستخدام مقترح تحويل أو مقترح IKEv2 الموجود.

```
crypto ipsec profile PROPOSAL_IKEV2_TSET
 set ikev2 ipsec-proposal IKEV2_TSET
```

3. تكوين واجهة النفق الظاهرية (VTI):
   قم بإنشاء واجهة نفق ظاهري (VTI) وطبق ملف تعريف IPsec عليها.

```
interface Tunnel1
 nameif VPN-BRANCH
 ip address 10.1.1.2 255.255.255.252
 tunnel source interface outside
 tunnel destination 10.20.20.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROPOSAL_IKEV2_TSET
```

4. شكلت تحشد ساكن إستاتيكي أو حركي تحشد بروتوكول:
   قم بإضافة مسارات ثابتة أو تكوين بروتوكول توجيه ديناميكي لتوجيه حركة المرور من خلال واجهة النفق. في هذا السيناريو، نستخدم التوجيه الثابت.

   التوجيه الثابت:

```
route VPN-BRANCH 172.16.10.0 255.255.255.0 10.1.1.10
```

التحقق من الصحة

بعد الترحيل من شبكة VPN المستندة إلى السياسة إلى شبكة VPN المستندة إلى المسار باستخدام واجهات النفق الظاهرية (VTIs) على Cisco ASA، فمن المهم التحقق من تشغيل النفق وتشغيله بشكل صحيح. هنا عدة خطوات وأوامر يمكنك إستخدامها للتحقق

من الحالة واستكشاف الأخطاء وإصلاحها إذا لزم الأمر.

1. التحقق من واجهة النفق
تحقق من حالة واجهة النفق للتأكد من أنها قيد التشغيل.

<#root>

```
ciscoasa# show interface Tunnel1
```

Interface Tunnel1 "VPN-BRANCH", is up, line protocol is up

```
Hardware is Virtual Tunnel Interface
Description: IPsec VPN Tunnel to Remote Site
Internet address is
```

10.1.1.2/24

```
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 500000 usec
65535 packets input, 4553623 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
65535 packets output, 4553623 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
```

Tunnel source 10.10.10.10, destination 10.20.20.20

```
Tunnel protocol/transport IPSEC/IP
Tunnel protection
```

IPsec profile PROPOSAL_IKEV2_TSET

يوفر هذا الأمر تفاصيل حول واجهة النفق، بما في ذلك حالة التشغيل وعنوان IP ومصدر/وجهة النفق. ابحث عن هذه المؤشرات:
· حالة الواجهة قيد التشغيل.
· حالة بروتوكول البند قيد التشغيل.

2. التحقق من ارتباطات أمان IPsec (SAs)

تحقق من حالة معرفات فئات IPsec لضمان نجاح التفاوض على النفق.

<#root>

```
ciscoasa# show crypto ipsec sa
```

```
interface: Tunnel1
```

Crypto map tag: Tunnel1-head-0, seq num: 1, local addr:

10.10.10.10

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer:

10.20.20.20

#pkts encaps: 1000, #pkts encrypt: 1000, #pkts digest: 1000

#pkts decaps: 1000, #pkts decrypt: 1000, #pkts verify: 1000

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1000, #pkts compr. failed: 0, #pkts decompress failed: 0

local crypto endpt.:

10.10.10.10

/500, remote crypto endpt.:

10.20.20.20

/500
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 0xC0A80101(3232235777)
current inbound spi : 0xC0A80102(3232235778)

inbound esp sas:

spi: 0xC0A80102(3232235778)

transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: CSR:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y

Status: ACTIVE

outbound esp sas:

spi: 0xC0A80101(3232235777)

transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: CSR:2, crypto map: Tunnel1-head-0

```
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y
```

Status: ACTIVE

يعرض هذا الأمر حالة شبكات IPsec، بما في ذلك العدادات للحزم المغلفة والمقصة. تأكد من:
· توجد وحدات خدمة مدمجة (SA) نشطة للنفق.
· تتزايد عدادات التضمين والعزل، مما يشير إلى تدفق حركة المرور.

للحصول على معلومات أكثر تفصيلا، يمكنك إستخدام:

<#root>

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:
```

Session-id:2, Status:UP-ACTIVE

```
, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
3363898555
```

10.10.10.10/500 10.20.20.20/500 READY INITIATOR

```
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/259 sec
```

يعرض هذا الأمر حالة شبكات IKEv2، والتي تكون في حالة "الاستعداد".

3. التحقق من التوجيه
تحقق من جدول التوجيه لضمان الإشارة الصحيحة للمسارات من خلال واجهة النفق.

<#root>

```
ciscoasa# show route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF Intra, IA - OSPF Inter, E1 - OSPF External Type 1
E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
i - IS-IS, su - IS-IS summary null, 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, H - NHRP, l - LISP
+ - replicated route, % - next hop override
```

```
S 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

C 10.1.1.0 255.255.255.0 is directly connected, Tunnel1

S 172.16.10.0 255.255.255.0 [1/0] via 10.1.1.10, Tunnel1

ابحث عن المسارات التي يتم توجيهها عبر واجهة النفق.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. التحقق من تكوين النفق المستند إلى المسار لـ ASA.

2. لاستكشاف أخطاء نفق IKEv2 وإصلاحها، يمكنك إستخدام عمليات تصحيح الأخطاء التالية:

```
debug crypto condition peer <peer IP address>
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

3. لاستكشاف أخطاء حركة المرور وإصلاحها على ASA، يمكنك التقاط الحزمة والتحقق من 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).