تنفيذ DVTI على جدار الحماية الآمن و Cisco IOS

المحتويات

المقدمة

يوضح هذا المستند كيفية تنفيذ مخرج واجهة النفق الظاهري الديناميكي والحل الذي يتم التحدث به مع EIGRP على جهاز الأمان القابل للتكيف.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الفهم الأساسي لواجهات النفق الظاهرية على ASA

- إمكانية اتصال أساسية بين الموزع/الفورع/ISP
- الفهم الأساسي ل EIGRP

- جهاز الأمان القابل للتكيف، الإصدار 9.19(1) أو إصدار أعلى

المكونات المستخدمة

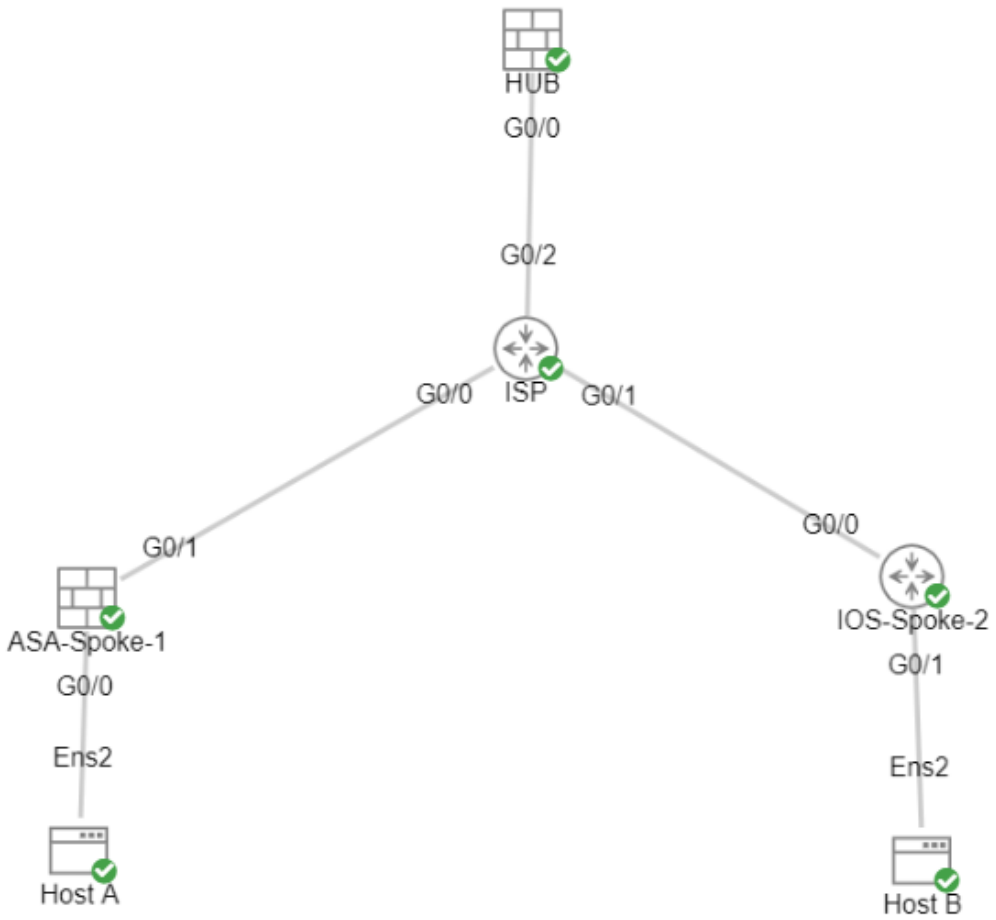
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهازان ASAv، كلاهما الإصدار 9.19(1). أستخدم ل TALK 1 و HUB
- جهازان Cisco IOS® v، الإصدار 15.9(3)M4. الأول لجهاز ISP، والثاني مستخدم ل Talk 2.
- مضيفان من Ubuntu لحركة المرور العامة المخصصة للأنفاق

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

الرسم التخطيطي للشبكة



التكوينات

تكوين واجهة WAN ومعلمات تشفير IKEv2 على Hub ASA

دخلت تشكيل أسلوب على الصرة.

```
interface g0/0
ip address 198.51.100.1 255.255.255.0
nameif OUTSIDE
```

تكوين معلمات IKEv2 على Hub ASA

قم بإنشاء نهج IKEv2 الذي يحدد معلمات المرحلة الأولى لاتصال IKE.

```
crypto ikev2 policy 1      (The number is locally significant on the device, this determine the order i
encryption aes-256         (Defines the encryption parameter used to encrypt the initial communication
integrity sha256           (Defines the integrity used to secure the initial communication between the
group 21                   (Defines the Diffie-Hellman group used to protect the key exchange between d
prf sha256                 (Pseudo Random Function, an optional value to define, automatically chooses
lifetime seconds 86400     (Controls the phase 1 rekey, specified in seconds. Optional value, as the de
```

إنشاء مقترح IKEv2 IPsec لتحديد معلمات المرحلة 2 المستخدمة لحماية حركة المرور.

```
crypto ipsec ikev2 ipsec-proposal NAME              (Name is locally signicant and is used as a refer
protocol esp encryption aes-256                     (specifies that Encapsulating Security Payload an
protocol esp integrity sha-256                      (specifies that Encapsulating Security Payload an
```

إنشاء ملف تعريف IPsec يحتوي على مقترح IPsec.

```
crypto ipsec profile NAME                  (This name is referenced on the Virtual-Template Interface
set ikev2 ipsec-proposal NAME              (This is the name previously used when creating the ipsec-
```

إنشاء واجهة إسترجاع وقالب ظاهري

```
interface loopback 1
ip address 172.16.50.254 255.255.255.255       (This IP address is used for all of the Virtual-Access
nameif LOOP1
```

```
interface Virtual-Template 1 type tunnel
ip unnumbered LOOP1                              (Borrows the IP address specified in Loopback1 for a
nameif DVTI
tunnel source Interface OUTSIDE                  (Specifies the Interface that the tunnel terminates
tunnel mode ipsec ipv4                           (Specifies that the mode uses ipsec, and uses ipv4)
tunnel protection ipsec profile NAME             (Reference the name of the previously created ipsec
```

إنشاء مجموعة نفق والإعلان عن عنواني IP لواجهة النفق عبر تبادل IKEv2

قم بإنشاء مجموعة نفق لتحديد نوع النفق وطريقة المصادقة.

```
tunnel-group DefaultL2LGroup ipsec-attributes          ('DefaultL2LGroup' is a default tunnel-group
virtual-template 1                                     (This command ties the Virtual-Template previ
ikev2 remote-authentication pre-shared-key cisco123    (This specifies the remote authentication as
ikev2 local-authentication pre-shared-key cisco123     (This specifies the local authentication as a
ikev2 route set Interface                              (Advertises the VTI Interface IP over IKEv2 e
```

تكوين توجيه EIGRP على Hub ASA

```
router eigrp 100
network 172.16.50.254 255.255.255.255        (Advertise the IP address of the Loopback used for the Vi
```

تكوين الواجهات على ASA المتصل

قم بتكوين واجهة WAN.

```
interface g0/1
ip address 203.0.113.1 255.255.255.0
nameif OUTSIDE-SPOKE-1
```

قم بتكوين واجهة LAN.

```
interface g0/0
ip address 10.45.0.4 255.255.255.0
nameif INSIDE-SPOKE-1
```

تكوين واجهة إسترجاع.

```
interface loopback1
ip address 172.16.50.1 255.255.255.255
nameif Loop1
```

تكوين معلمات تشفير IKEv2 على ASA التبليغي

قم بإنشاء نهج IKEv2 الذي يطابق المعلمات الموجودة على الصرة.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 21
prf sha256
lifetime 86400
```

قم بإنشاء مقترح IKEv2 IPsec يطابق المعلمات الموجودة على الصرة.

```
crypto ipsec ikev2 ipsec-proposal NAME           (Name is locally signicant, this does not need to matc
protocol esp encryption aes-256
protocol esp integrity sha-256
```

إنشاء ملف تعريف IPsec يحتوي على مقترح IPsec.

```
crypto ipsec profile NAME               (This name is locally significant and is referenced in the SVTI
set ikev2 ipsec-proposal NAME           (This is the name previously used when creating the ipsec-propo
```

تكوين واجهة النفق الظاهري الثابتة على ASA المتصل

قم بتكوين واجهة نفق ظاهري ثابتة تشير إلى الموزع. شكلت ال يتحدث أداة عادي ساكن إستاتيكي نفق قارن إلى الصرة، فقط الصرة يحتاج قالب ظاهري.

```
interface tunnel1
ip unnumbered loopback1
nameif ASA-SPOKE-SVTI
tunnel destination  198.51.100.254          (Tunnel destination references the Hub ASA tunnel source. C
tunnel mode ipsec ipv4
tunnel protection ipsec profile NAME
```

إنشاء مجموعة نفق والإعلان عن عناوين IP لواجهة النفق عبر تبادل IKEv2

```
tunnel-group 198.51.100.1 type ipsec-l2l                    (This specifies the connection type as ipsec
tunnel-group 198.51.100.1 ipsec-attributes                  (Ipsec attributes allows you to make changes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
ikev2 route set Interface
```

تكوين توجيه EIGRP على ASA المتصل

قم بإنشاء نظام مستقل EIGRP وطبق الشبكات المطلوبة التي سيتم الإعلان عنها.

```
router eigrp 100
network 10.45.0.0 255.255.255.0        (Advertises the Host-A network to the hub. This allows the hub t
network 172.16.50.1 255.255.255.255    (Advertises and utilizes the tunnel IP address to form an EIGRP
```

تكوين الواجهات على الموجه المتصل

```
interface g0/0
ip address 192.0.2.1 255.255.255.0
no shut
```

```
interface g0/1
ip address 10.12.0.2
no shut
```

```
interface loopback1
ip address 172.16.50.2 255.255.255.255
```

تكوين معلمات IKEv2 و AAA على الموجه الذي تم التحدث به

إنشاء مقترح IKEv2 لمطابقة معلمات المرحلة الأولى على ASA.

```
crypto ikev2 proposal NAME       (These parameters must match the ASA IKEv2 Policy.)
encryption aes-cbc-256           (aes-cbc-256 is the same as the ASA aes-256. However, AES-GCM of any v
                                  and is not a matching parameter with plain AES.)
integrity sha256
group 21
```

قم بإنشاء سياسة IKEv2 لإرفاق العرض (العروض).

```
crypto ikev2 policy NAME
proposal NAME               (This is the name of the IKEv2 proposal created in the step ikev2.)
```

إنشاء نهج تخويل IKEv2.

```
crypto ikev2 authorization policy NAME   (IKEv2 authorization policy serves as a container of IKEv2 loca
route set Interface
```

تمكين AAA على الجهاز.

```
aaa new-model
```

إنشاء شبكة تخويل AAA.

```
aaa authorization network NAME local    (Creates a name and method for aaa authorization that is refere
```

قم بإنشاء ملف تعريف IKEv2 يحتوي على مستودع للمعلمات غير القابلة للتداول الخاصة بوجهة مستخدم IKE SA، مثل الهويات المحلية أو البعيدة وأساليب المصادقة.

```
crypto ikev2 profile NAME
match identity remote address  198.51.100.1    (Used to match the address of the Hub VTI source Interfa
identity local address  192.0.2.1              (Defines the local IKE-ID of the router for this IKEv2 p
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
no config-exchange request                     (Applies to Cisco IOS, Cisco IOS-XE devices do this by d
                                                which is unsupported on the ASA.)
aaa authorization group psk list NAME NAME     (Specifies an AAA method list and username for group. Th
```

قم بإنشاء مجموعة تحويل لتحديد معلمات التشفير والتجزئة المستخدمة لحماية حركة المرور النفقي.

```
crypto ipsec transform-set NAME esp aes 256 esp-sha256-hmac
```

إنشاء ملف تعريف IPsec تشفير لتضمين مجموعة التحويل وملف تعريف IKEv2.

```
crypto ipsec profile NAME                  (Define the name of the ipsec-profile.)
set transform-set NAME                     (Reference the name of the created transform set.)
set ikev2-profile NAME                     (Reference the name of the created IKEv2 profile.)
```

تكوين واجهة النفق الظاهرية الثابتة على الموجه الذي تم التحدث عنه

قم بتكوين واجهة نفق ظاهري ثابتة تشير إلى الموزع.

```
interface tunnel1
ip unnumbered loopback1
tunnel source g0/0
tunnel mode ipsec ipv4
tunnel destination 198.51.100.1
tunnel protection ipsec profile NAME      (Reference the name of the created ipsec profile. This applies
                                           and transform set parameters to the tunnel Interface.)
```

تكوين توجيه EIGRP على الموجه المتصل

قم بإنشاء نظام مستقل EIGRP وطبق الشبكات المطلوبة التي سيتم الإعلان عنها.

```
router eigrp 100
network 172.16.50.2 0.0.0.0     (Routers advertise EIGRP networks with the wildcard mask.
                                 This advertises the tunnel IP address to allow the device to form an E
network 10.12.0.0 0.0.0.255      (Advertises the Host-B network to the hub. This allows the hub to noti
```

التحقق من الصحة

استخدم هذه القسم لتأكيد عمل التكوين بشكل صحيح.

توجيه ASA:

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

تشفير ASA:

```
show run crypto ikev2
show run crypto ipsec
show run tunnel-group [NAME]
show crypto ikev2 sa
show crypto ipsec sa peer X.X.X.X
```

القالب الظاهري والوصول الظاهري ل ASA:

```
show run interface virtual-template # type tunnel
show interface virtual-access #
```

توجيه IOS من Cisco:

```
show run | sec eigrp
show ip eigrp topology
show ip eigrp neighbors
show ip route
show ip route eigrp
```

تشفير IOS من Cisco:

```
show run | sec cry
show crypto ikev2 sa
show crypto ipsec sa peer X.X.X.X
```

واجهة نفق IOS من Cisco:

```
show run interface tunnel#
```

استكشاف الأخطاء وإصلاحها

يوفر هذه القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تصحيح أخطاء ASA:

```
debug crypto ikev2 platform 255

debug crypto ikev2 protocol 255

debug crypto ipsec 255

debug ip eigrp #

debug ip eigrp neighbor X.X.X.X
```

تصحيح أخطاء IOS من Cisco:

```
debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 packet

debug crypto ikev2 internal

debug crypto ipsec

debug crypto ipsec error

debug ip eigrp #

debug ip eigrp neighbor X.X.X.X
```

معلومات ذات صلة

- الدعم التقني والتنزيلات من Cisco

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).