تغيير نفق جدار الحماية الذي تم تسليمه للسحابة من مصادقة RSA إلى مصادقة PSK

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لإعادة تكوين آلية مصادقة نفق جدار الحماية الذي تم تسليمه للسحابة من RSA إلى PSK على Cisco ASA.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

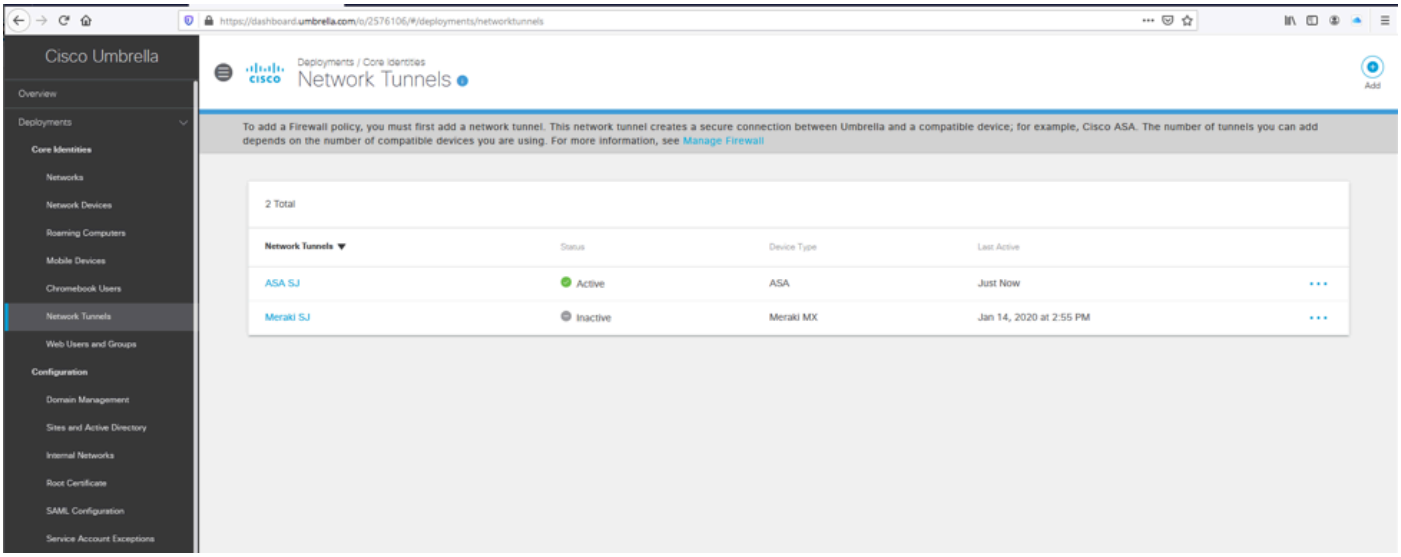
تستند المعلومات الواردة في هذا المستند إلى Cisco Umbrella.

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.

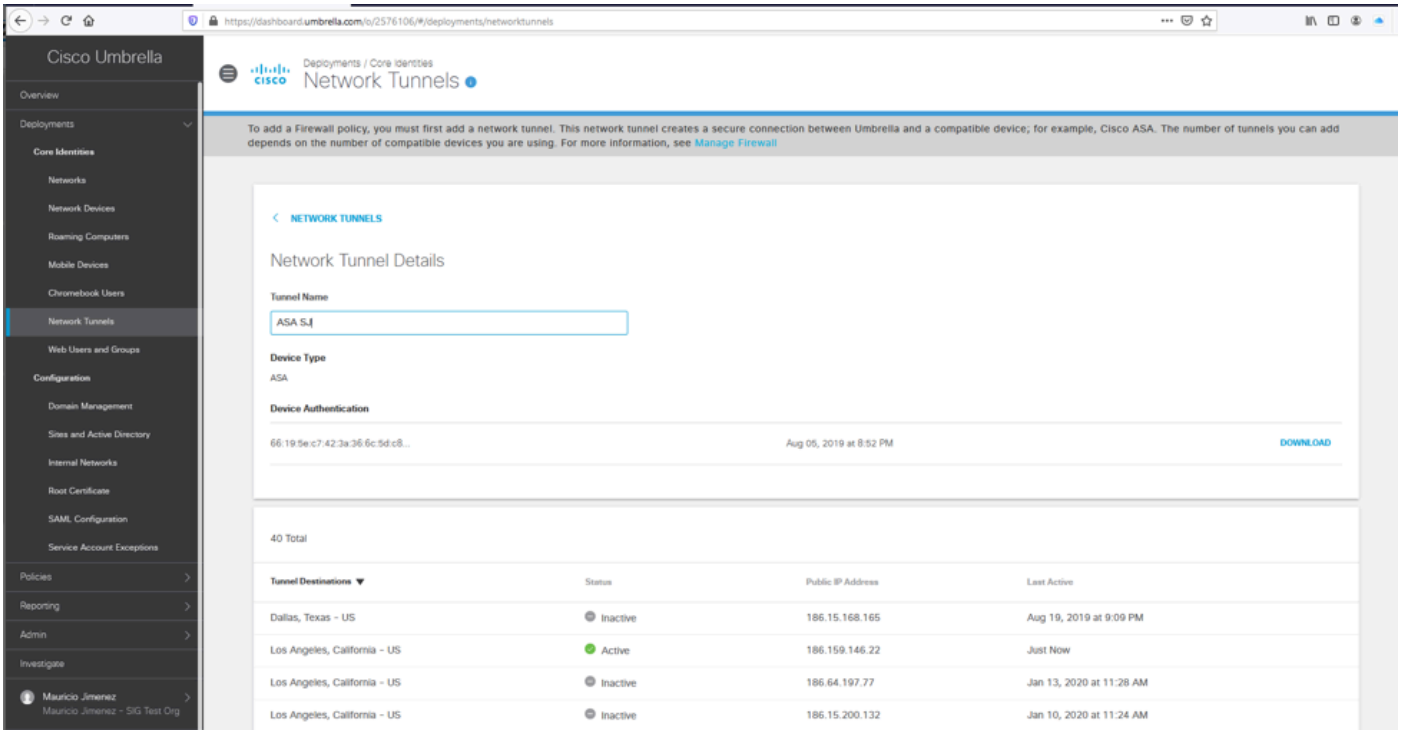
الخطوة 1: التحقق من نفق موجود باستخدام مصادقة RSA

تحقق من وجود نفق باستخدام مصادقة RSA ومن إظهار حالة النفق في ASA متصل بنوع المصادقة هذا.

1. في لوحة معلومات Umbrella، ابحث عن نفق الشبكة باستخدام ASA الذي يظهر بصمة إصبع مصادقة الجهاز.



صورة 1.png



صورة 2.png

2. في Cisco ASA، يمكنك تشغيل هذه الأوامر للتحقق من نوع المصادقة و IP لوحدة الاستقبال والبث المستخدمة للنفق.

show crypto ikev2 sa

و

show crypto ipsec sa

```
ASA-SJ# sh crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                         Remote
                                    Status          Role
 26325699 186.159.146.22/4500                           146.112.67.2/4500
                                     READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:19, Auth sign: RSA, Auth
verify: RSA
      Life/Active Time: 86400/4542 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: 0xeccfd18d/0xccb02302
ASA-SJ#
```

ةروص 3.png

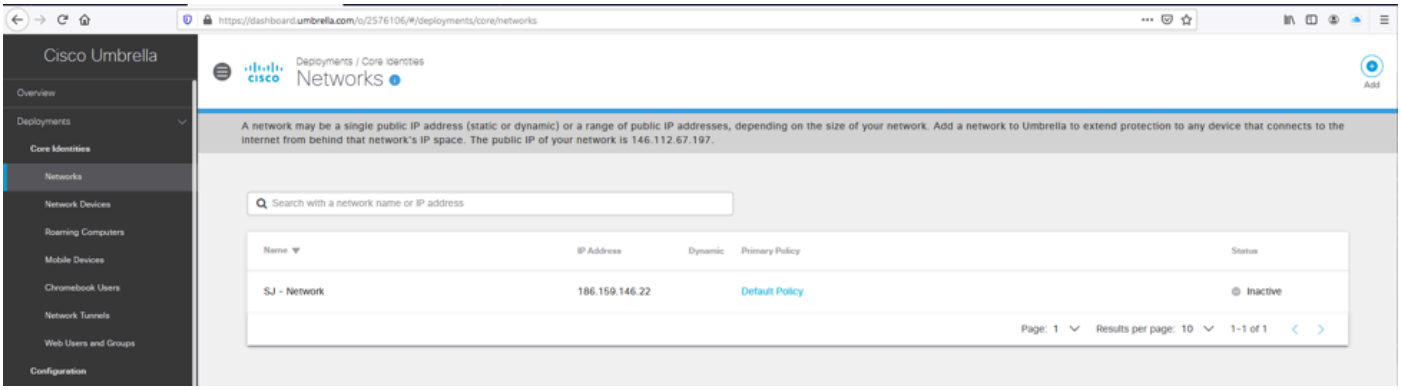
```
ASA-SJ# sh crypto ipsec sa
interface: vti
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: 186.159.
146.22

      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: 146.112.67.2


      #pkts encaps: 1734481, #pkts encrypt: 1734481, #pkts digest: 1734481
      #pkts decaps: 3553655, #pkts decrypt: 3553655, #pkts verify: 3553655
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 1734482, #pkts comp failed: 0, #pkts decomp failed:
0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 186.159.146.22/4500, remote crypto endpt.: 146.112.67
.2/4500
      path mtu 1500, ipsec overhead 82(52), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CCB02302
      current inbound spi : ECCFD18D

<--- More --->
```

صورة 4.png

الخطوة 2: تسجيل عنوان IP العام الخاص ب ASA

1. تأكد من وجود عنوان IP العام لديك الذي تستخدمه واجهة ASA الخارجية ومسجل كشبكة في لوحة معلومات Umbrella.

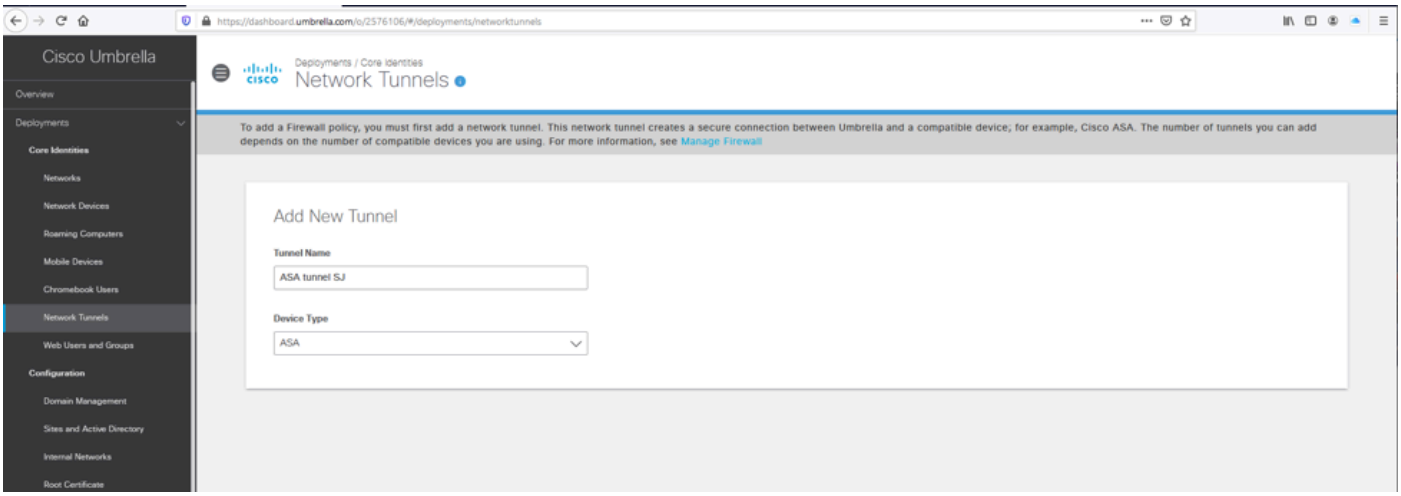
2. إذا لم تكن الشبكة موجودة، فقم بالمتابعة لإضافتها وتأكيد IP العام المستخدم من قبل واجهة ASA. يجب تعريف كائن الشبكة المستخدم لهذا النفق باستخدام قناع الشبكة الفرعية /32.



صورة 5.png

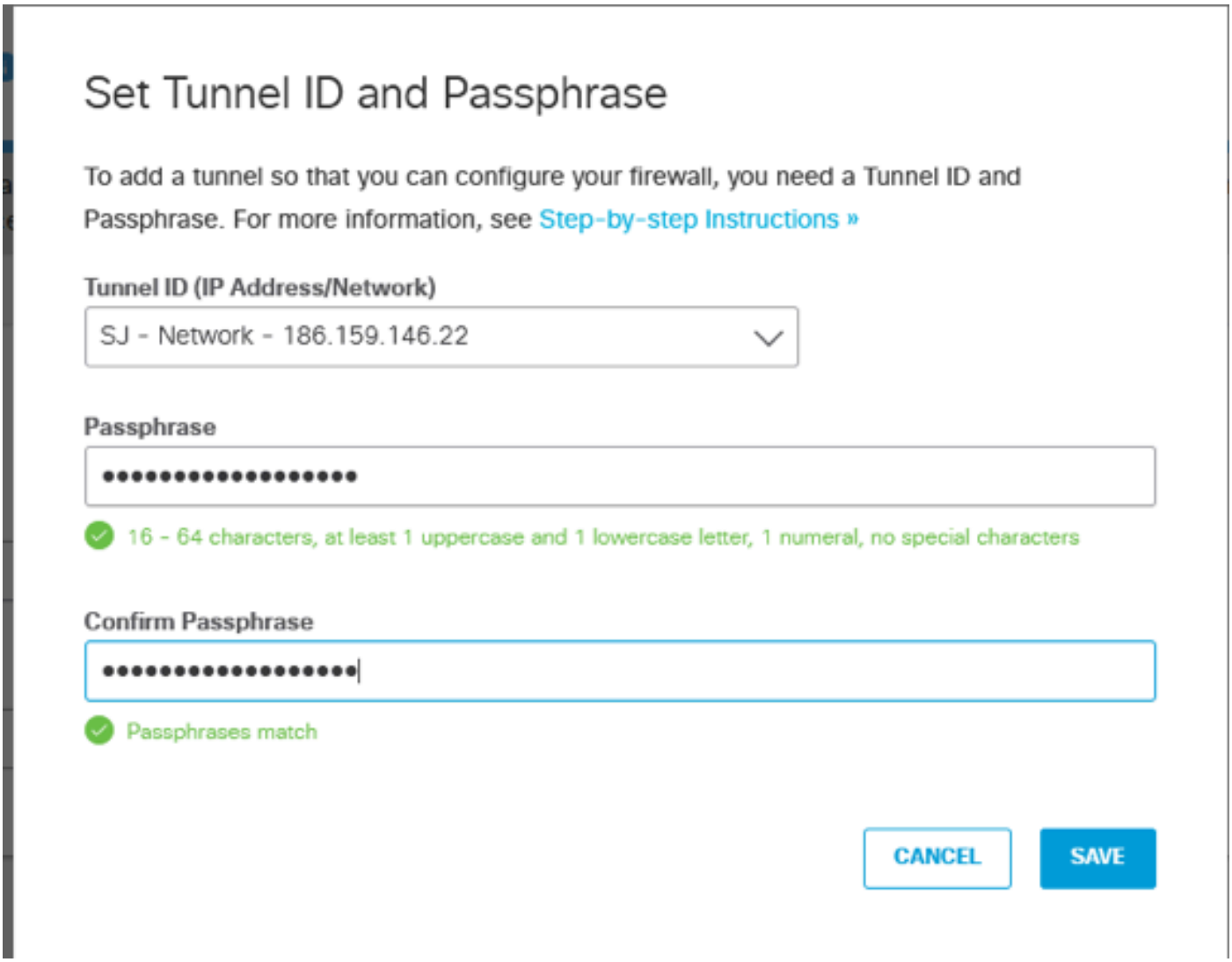
الخطوة 3: إنشاء نفق ASA جديد

1. في لوحة المعلومات Umbrella ضمن عمليات النشر/أنفاق الشبكة، قم بإنشاء نفق جديد من خلال تحديد خيار الإضافة.

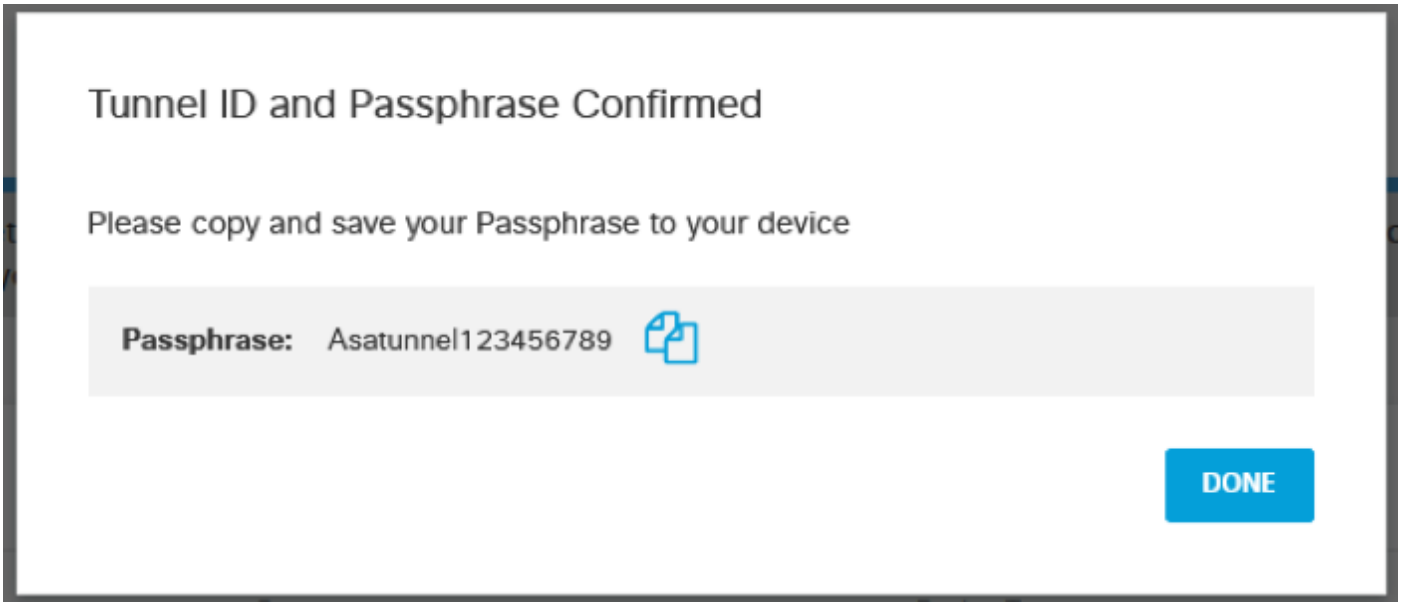


صورة 6.png

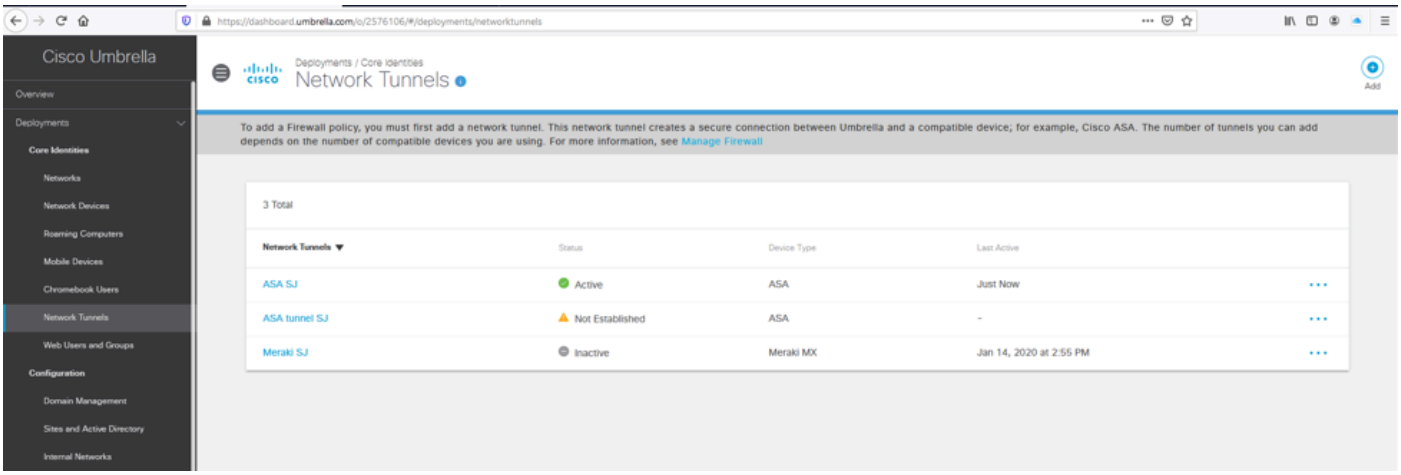
2. حدد معرف النفق استنادا إلى الشبكة التي تطابق IP العام الخاص بواجهة ASA الخارجية وأدخل عبارة مرور لمصادقة PSK.



ةروص 7.png



ةروص 8.png



صورة 9.png

الخطوة 4: إنشاء مجموعة نفق جديدة

1. على ASA، قم بإنشاء مجموعة نفق جديدة باستخدام وحدة الاستقبال والبث الجديدة IP لـ Umbrella وحدد عبارة المرور المعرفة في لوحة معلومات Umbrella لمصادقة PSK.

2. يمكن الاطلاع على القائمة المحدثة لمراكز بيانات Umbrella و IPs الخاصة بالنهايات الرئيسية في وثائق Umbrella.

```
tunnel-group <UMB DC IP address .8> type ipsec-l2l
tunnel-group <UMB DC IP address .8> general-attributes
 default-group-policy umbrella-policy
tunnel-group <UMB DC IP address .8> ipsec-attributes
 peer-id-validate nocheck
ikev2 local-authentication pre-shared-key 0 <passphrase>
ikev2 remote-authentication pre-shared-key 0 <passphrase>
```

```
ASA-SJ(config-tunnel-ipsec)# sh run tunnel-group 146.112.67.8
tunnel-group 146.112.67.8 type ipsec-l2l
tunnel-group 146.112.67.8 general-attributes
 default-group-policy umbrella-policy
tunnel-group 146.112.67.8 ipsec-attributes
 peer-id-validate nocheck
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

صورة 10.png

الخطوة 5: تحديد موقع ملف تعريف IPSec المستخدم لواجهة النفق

1. البحث عن ملف تعريف IPsec crypto ips" الذي يتم إستخدامه في واجهة النفق الخاصة

بالتكوين المستند إلى المسار إلى وحدة الاستقبال والبث Umbrella (# يتم إستبداله بالمعرف المستخدم لواجهة النفق إلى Umbrella):

```
show run interface tunnel#
```

```
ASA-SJ(config-tunnel-ipsec)# sh run interface tunnel1
!
interface Tunnel1
 nameif vti
 ip address 11.11.11.11 255.255.255.0
 tunnel source interface outside
 tunnel destination 146.112.67.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile umbrella-profile
ASA-SJ(config-tunnel-ipsec)#
```

Picture11.png

2. إذا لم تكن متأكدا من معرف النفق، فيمكنك إستخدام هذا الأمر للتحقق من واجهات النفق الموجودة وتحديد النوع المستخدم للتكوين المستند إلى نفق Umbrella:

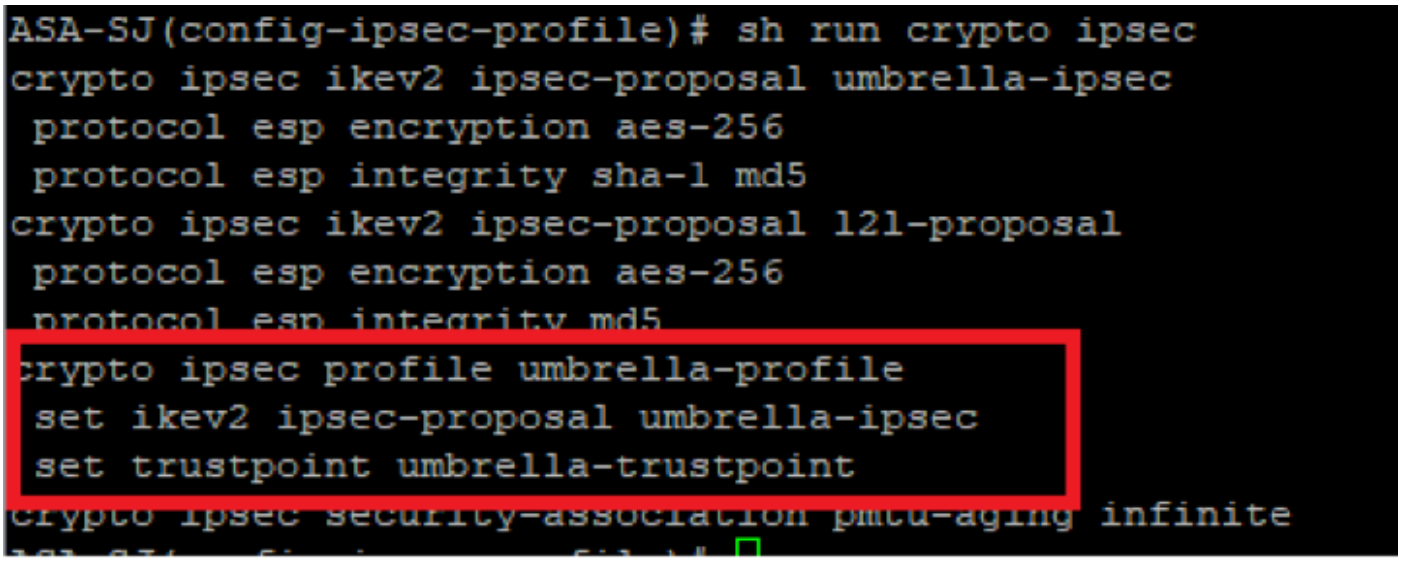
```
show run interface tunnel
```

الخطوة 6: إزالة TrustPoint القديم من ملف تعريف IPSec

1. قم بإزالة TrustPoint من ملف تعريف IPSec الذي يشير إلى مصادقة RSA للنفق. يمكنك التحقق من التكوين باستخدام هذا الأمر:

```
show crypto ipsec
```

```
ASA-SJ(config-ipsec-profile)# sh run crypto ipsec
crypto ipsec ikev2 ipsec-proposal umbrella-ipsec
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal l2l-proposal
 protocol esp encryption aes-256
 protocol esp integrity md5
crypto ipsec profile umbrella-profile
 set ikev2 ipsec-proposal umbrella-ipsec
 set trustpoint umbrella-trustpoint
crypto ipsec security-association pmtu-aging infinite
```

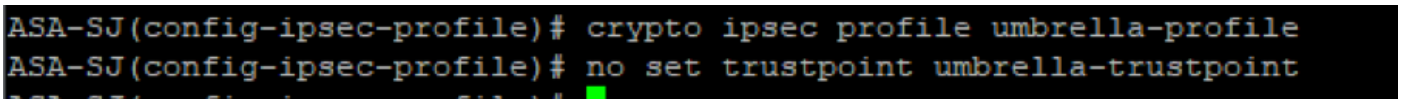


صورة 12.png

2. انتقل إلى إزالة TrustPoint باستخدام الأوامر التالية:

```
crypto ipsec profile <profile name>
no set trustpoint umbrella-trustpoint
```

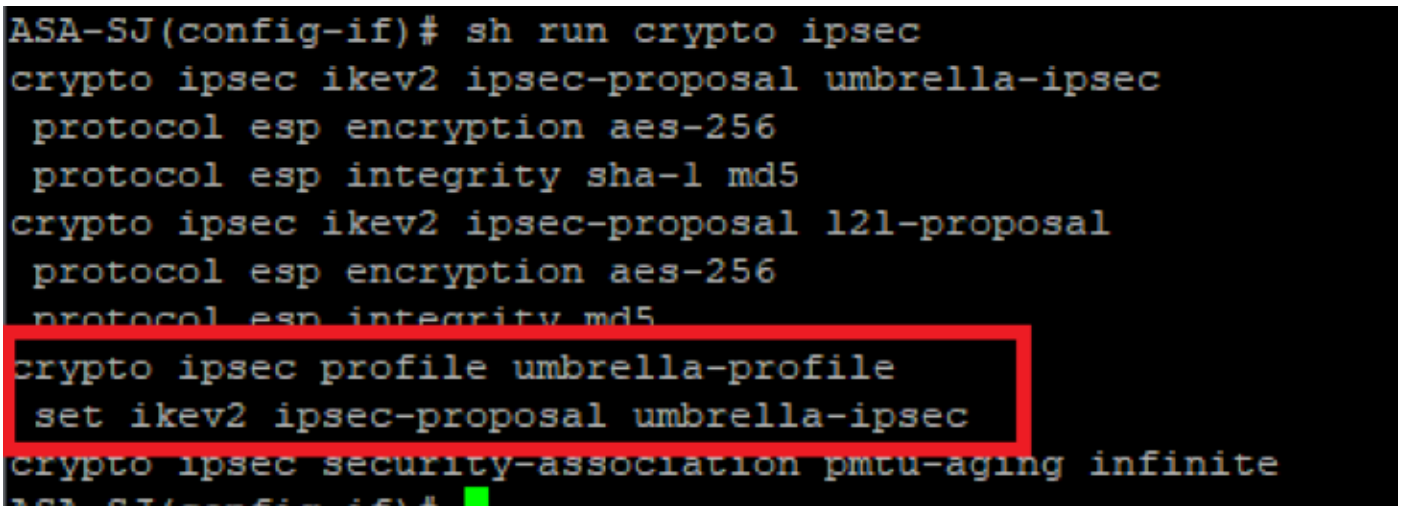
```
ASA-SJ(config-ipsec-profile)# crypto ipsec profile umbrella-profile
ASA-SJ(config-ipsec-profile)# no set trustpoint umbrella-trustpoint
```



صورة 13.png

3. تأكد من إزالة TrustPoint من ملف تعريف IPsec للتشفير:

```
ASA-SJ(config-if)# sh run crypto ipsec
crypto ipsec ikev2 ipsec-proposal umbrella-ipsec
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal l2l-proposal
 protocol esp encryption aes-256
 protocol esp integrity md5
crypto ipsec profile umbrella-profile
 set ikev2 ipsec-proposal umbrella-ipsec
crypto ipsec security-association pmtu-aging infinite
```



صورة 14.png

الخطوة 7: تحديث واجهة النفق باستخدام عنوان IP جديد لوحدة الاستقبال والبث Umbrella

1. إستبدال وجهة واجهة النفق بعنوان IP لنقطة الاستقبال والبث الجديدة Umbrella التي تنتهي في .8.

- يمكنك إستخدام هذا الأمر للتحقق من الوجهة الحالية حتى يتم إستبداله ب IP من نطاقات عناوين IP لمركز البيانات الجديد، والتي يمكن العثور عليها في وثائق Umbrella:

```
show run interface tunnel
```

```
ASA-SJ(config-tunnel-ipsec)# sh run interface tunnel1
!
interface Tunnel1
 nameif vti
 ip address 11.11.11.11 255.255.255.0
 tunnel source interface outside
 tunnel destination 146.112.67.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile umbrella-profile
ASA-SJ(config-tunnel-ipsec)#
```

صورة 15.png

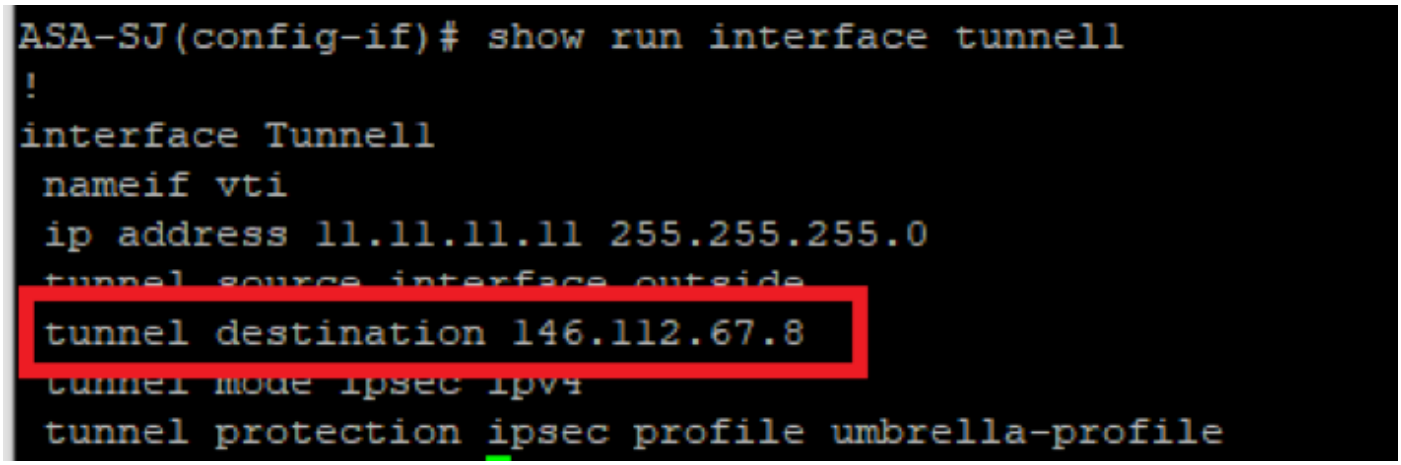
```
Interface tunnel#
No tunnel destination <UMBRELLA DC IP address.2>
Tunnel destination <UMBRELLA DC IP address .8>
```

```
ASA-SJ(config-if)# interface Tunnel1
ASA-SJ(config-if)# no  tunnel destination 146.112.67.2
ASA-SJ(config-if)#  tunnel destination 146.112.67.8
```

صورة 16.png

2. تأكد من التغيير باستخدام الأمر:

```
show run interface tunnel#
```

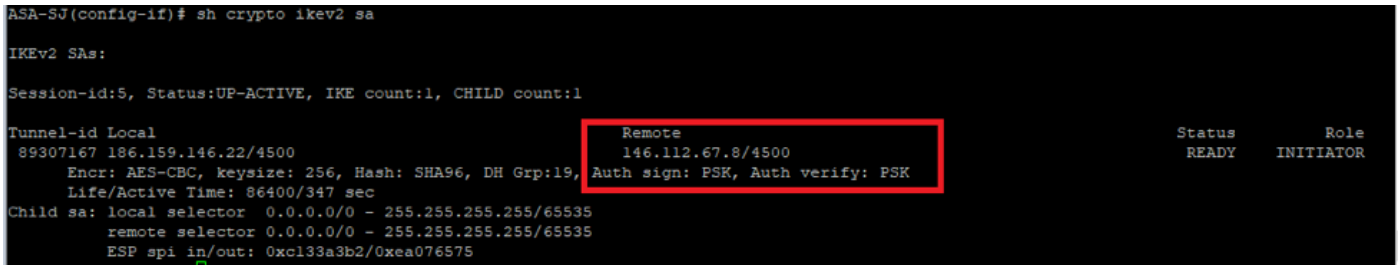


صورة 17.png

الخطوة 8: تأكيد تكوين النفق الجديد بنجاح

1. تأكد من إعادة إنشاء اتصال النفق ب Umbrella بشكل صحيح باستخدام IP محدث لوحدة الاستقبال والبث باستخدام مصادقة PSK باستخدام هذا الأمر:

```
show crypto ikev2 sa
```



صورة 18.png

```
show crypto ipsec sa
```

```
ASA-SJ(config-if)# show crypto ipsec sa
interface: vti
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: 186.159.146.22

      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: 146.112.67.8


      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 186.159.146.22/4500, remote crypto endpt.: 146.112.67.8/4500
      path mtu 1500, ipsec overhead 82(52), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: EA076575
      current inbound spi : C133A3B2
```

صورة 19.png

الخطوة 9 (اختيارية): إزالة مجموعة النفق القديمة

1. قم بإزالة مجموعة النفق القديمة التي كانت تشير إلى نطاق IP لنقطة الاستقبال والبث السابقة Umbrella .2.

يمكنك إستخدام هذا الأمر لتعريف النفق الصحيح قبل إزالة التكوين:

```
show run tunnel-group
```

```
ASA-SJ(config)# sh run tunnel-group
tunnel-group DefaultL2LGroup general-attributes
 default-group-policy l2lpolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
tunnel-group 146.112.67.2 type ipsec-l2l
tunnel-group 146.112.67.2 general-attributes
 default-group-policy umbrella-policy
tunnel-group 146.112.67.2 ipsec-attributes
 peer-id-validate nocheck
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate umbrella-trustpoint
tunnel-group 146.112.67.8 type ipsec-l2l
tunnel-group 146.112.67.8 general-attributes
 default-group-policy umbrella-policy
tunnel-group 146.112.67.8 ipsec-attributes
 peer-id-validate nocheck
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

صورة 20.png

2. قم بإزالة أي مرجع لمجموعة النفق القديمة باستخدام هذا الأمر:

```
clear config tunnel-group <UMB DC IP address .2>
```

```
ASA-SJ(config)# clear config tunnel-group 146.112.67.2
```

صورة 21.png

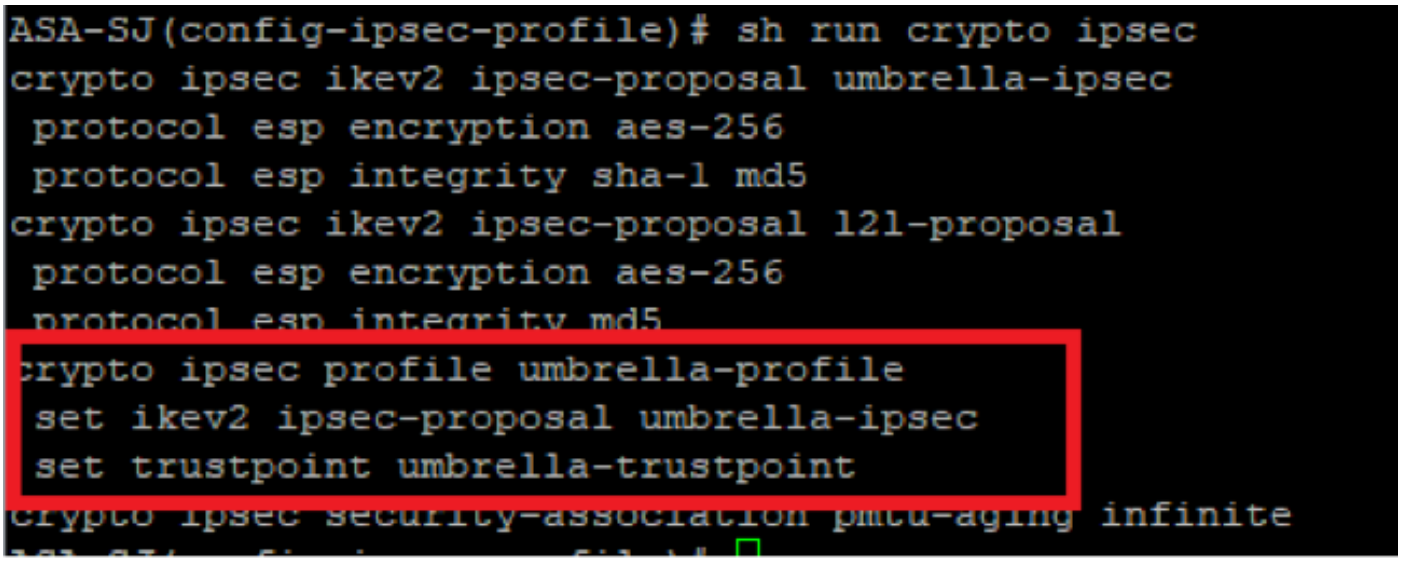
الخطوة 10 (اختيارية): إزالة TrustPoint القديمة

1. قم بإزالة أي مرجع لنقطة الثقة المستخدمة سابقا مع التكوين المستند إلى نفق Umbrella باستخدام هذا الأمر:

```
sh run crypto ipsec
```

يمكن العثور على الاسم المألوف المستخدم ل TrustPoint عند مراجعة ملف تعريف "crypto ipSec":

```
ASA-SJ(config-ipsec-profile)# sh run crypto ipsec
crypto ipsec ikev2 ipsec-proposal umbrella-ipsec
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal l2l-proposal
 protocol esp encryption aes-256
 protocol esp integrity md5
crypto ipsec profile umbrella-profile
 set ikev2 ipsec-proposal umbrella-ipsec
 set trustpoint umbrella-trustpoint
crypto ipsec security-association pmtu-aging infinite
```

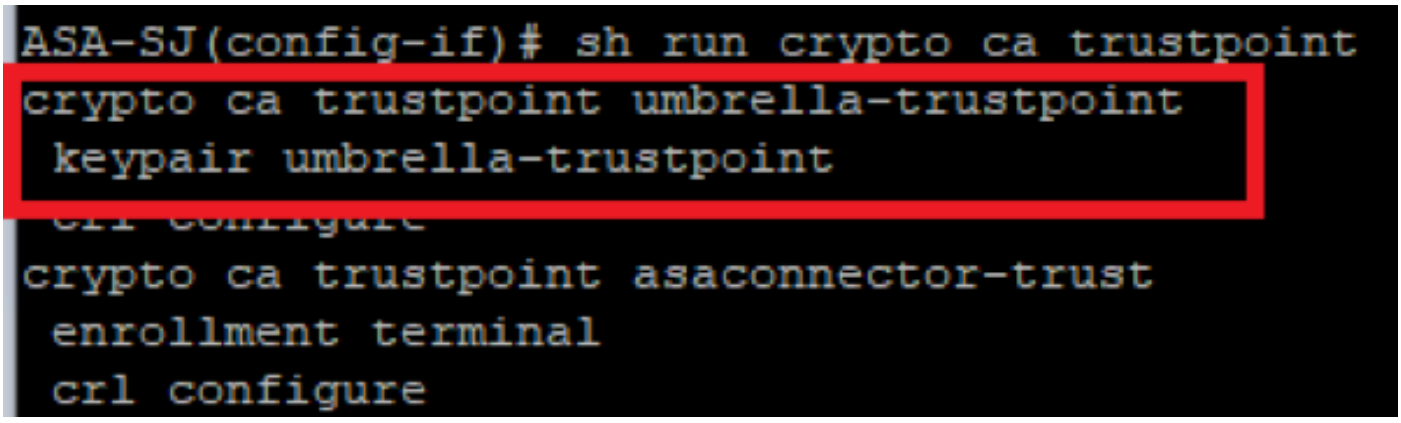


صورة 22.png

2. يمكنك تشغيل هذا الأمر لتأكيد تكوين TrustPoint. تأكد من تطابق الاسم المألوف مع التكوين المستخدم في أمر ملف تعريف crypto IpSec:

```
sh run crypto ca trustpoint
```

```
ASA-SJ(config-if)# sh run crypto ca trustpoint
crypto ca trustpoint umbrella-trustpoint
 keypair umbrella-trustpoint
crypto ca trustpoint asaconnector-trust
 enrollment terminal
 crl configure
```



صورة 23.png

3. للحصول على مزيد من التفاصيل حول الشهادة، أستخدم الأمر:

```
show crypto ca certificate <trustpoint-name>
```

```
ASA-SJ(config-if)# show crypto ca certificates umbrella-trustpoint
Certificate
  Status: Available
  Certificate Serial Number: 365510264a580b66b1f5a2b6b8a618ec
  Certificate Usage: Signature
  Public Key Type: RSA (3072 bits)
  Signature Algorithm: SHA384 with RSA Encryption
  Issuer Name:
    cn=Cisco Umbrella CA
    o=Cisco Umbrella
    c=US
  Subject Name:
    cn=cdfw-2576106-293960662-umbrella.com
  Validity Date:
    start date: 20:52:11 CST Aug 5 2019
    end   date: 20:52:11 CST Aug 5 2021
  Storage: config
  Associated Trustpoints: umbrella-trustpoint

CA Certificate
  Status: Available
  Certificate Serial Number: 60fa7229af4c481e
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
```

صورة 24.png

4. إزالة نقطة الثقة باستخدام الأمر:

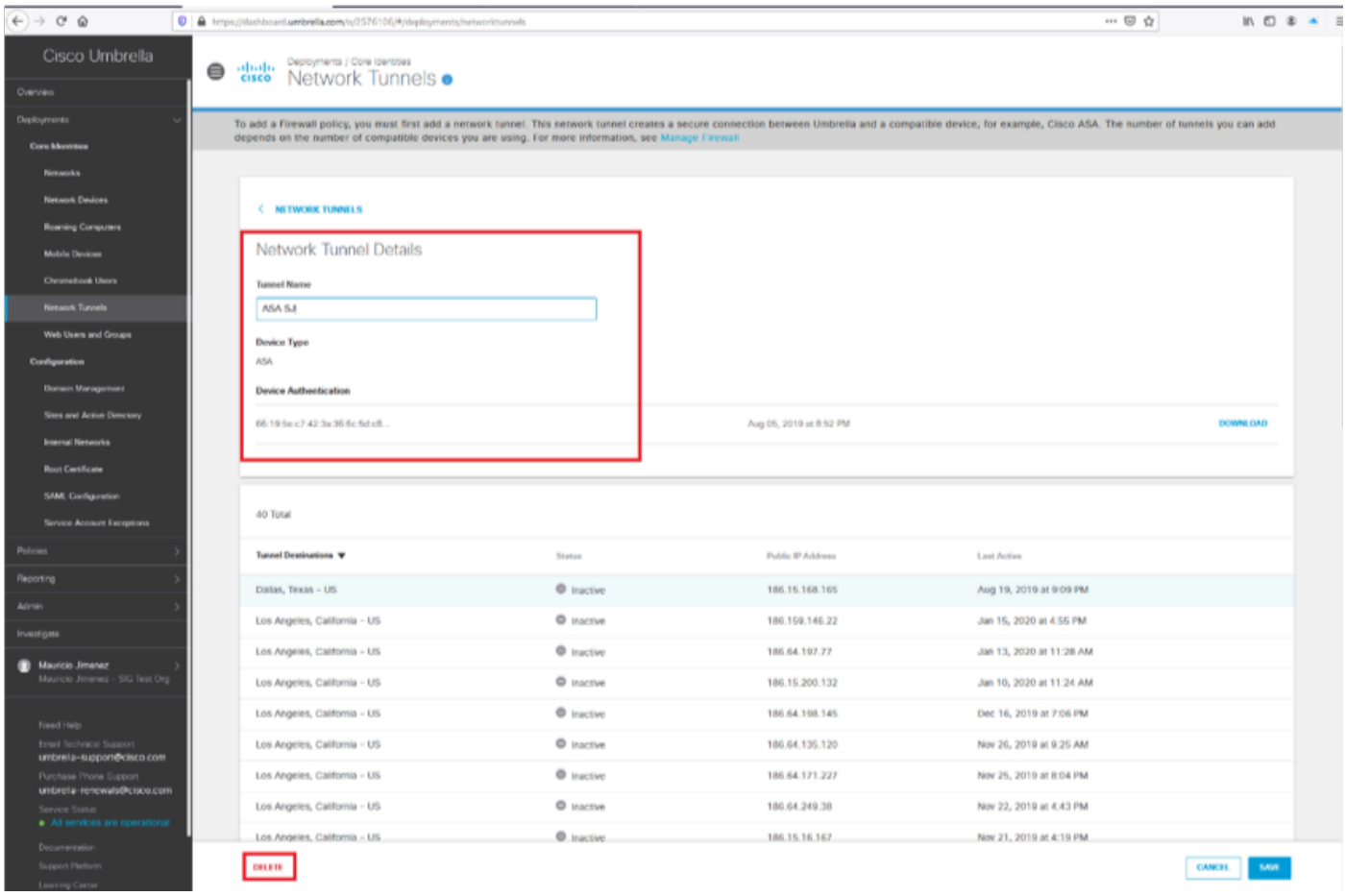
```
no crypto ca trustpoint <trustpoint-name>
```

```
ASA-SJ(config)# no crypto ca trustpoint umbrella-trustpoint
WARNING: Removing an enrolled trustpoint will destroy all
certificates received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]: yes
INFO: Be sure to ask the CA administrator to revoke your certificates.
ASA-SJ(config)#
```

صورة 25.png

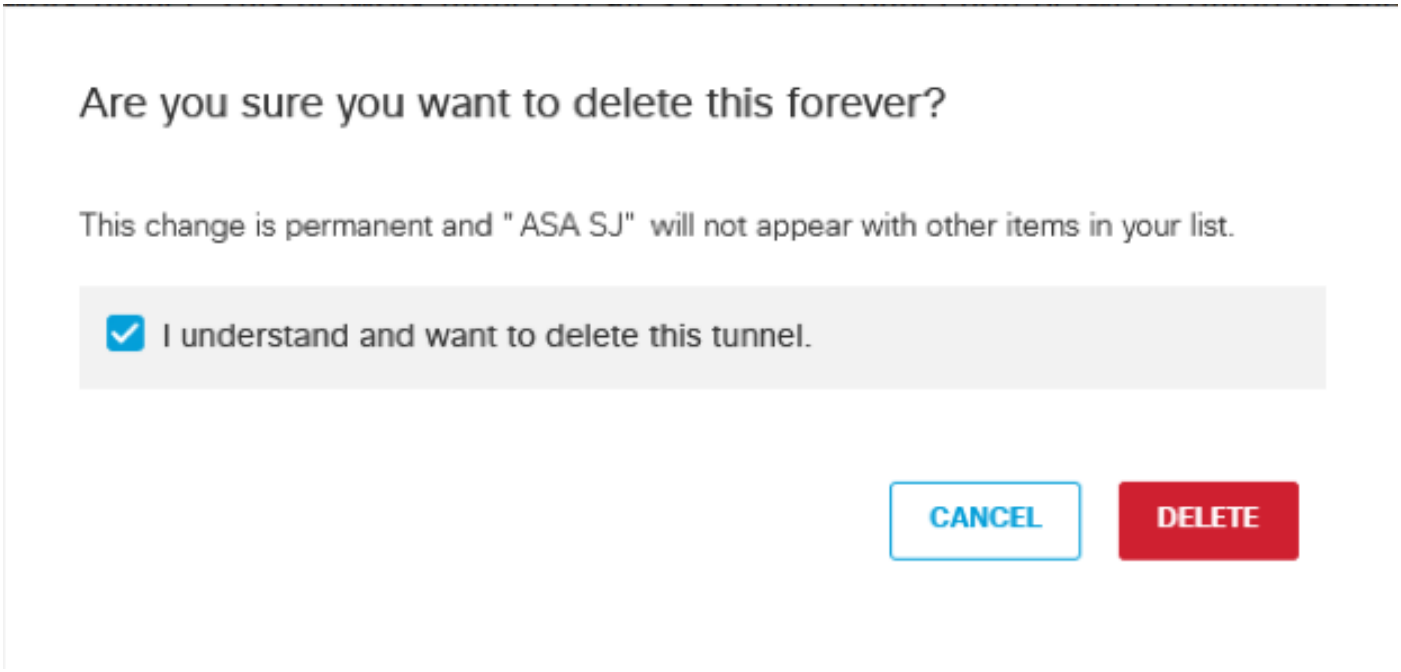
الخطوة 11 (اختيارية): حذف نفق الشبكة القديم

1. احذف نفق الشبكة القديم من لوحة معلومات Umbrella من خلال الانتقال إلى تفاصيل نفق الشبكة وتحديد Delete.



صورة 26.png

2. تأكد من الحذف بتحديد خيار أنا أفهم وأريد حذف هذا النفق في القائمة المنبثقة، ثم حدد حذف.



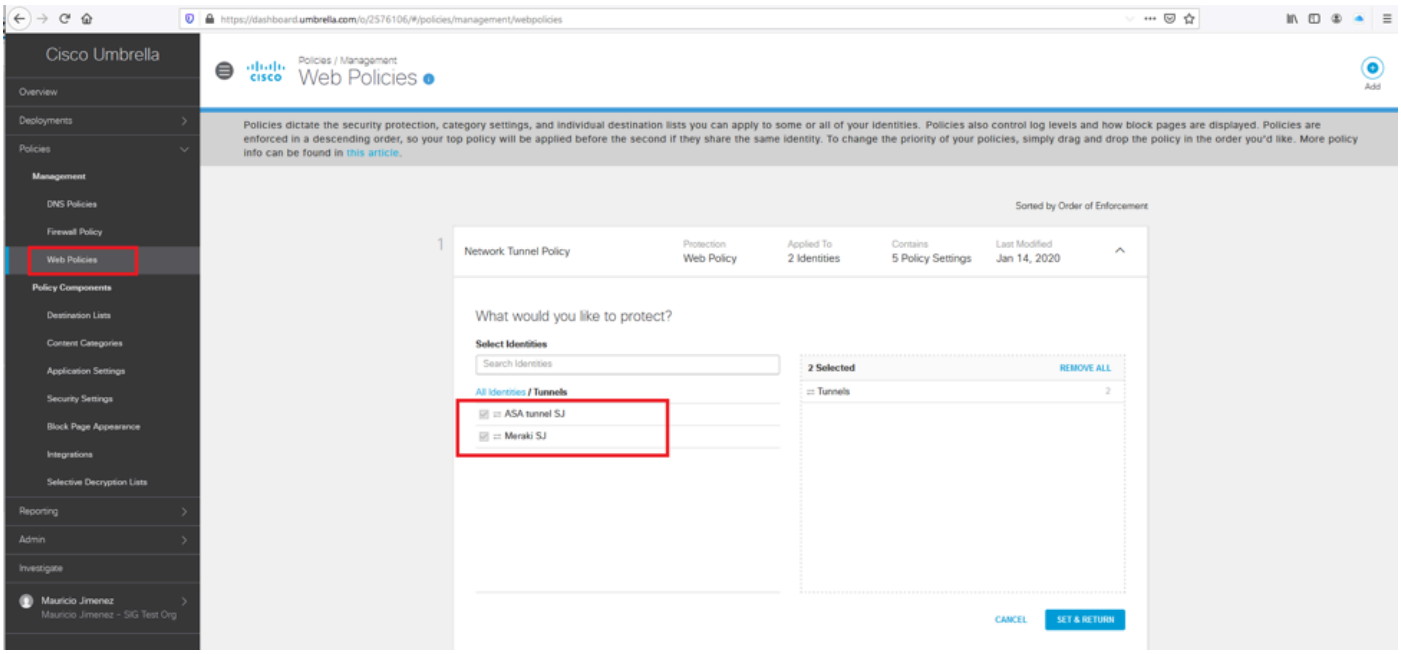
صورة 27.png

الخطوة 12: تحديث سياسات ويب بهوية نفق جديدة

تأكيد أن نهج الويب لديك تحتوي على الهوية المحدثة باستخدام نفق الشبكة الجديد:

1. في لوحة المعلومات Umbrella، انتقل إلى السياسات > الإدارة > سياسات الويب.

2. راجع قسم الأنفاق وتأكد من أن سياسات الويب لديك تحتوي على الهوية المحدثة باستخدام نفق الشبكة الجديد.



صورة 28.png

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).