Cloud Delivered Firewall Tunnel wijzigen van RSA naar PSK-verificatie

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het opnieuw configureren van het verificatiemechanisme van de Cloud Delivered Firewall Tunnel van RSA naar PSK op Cisco ASA.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

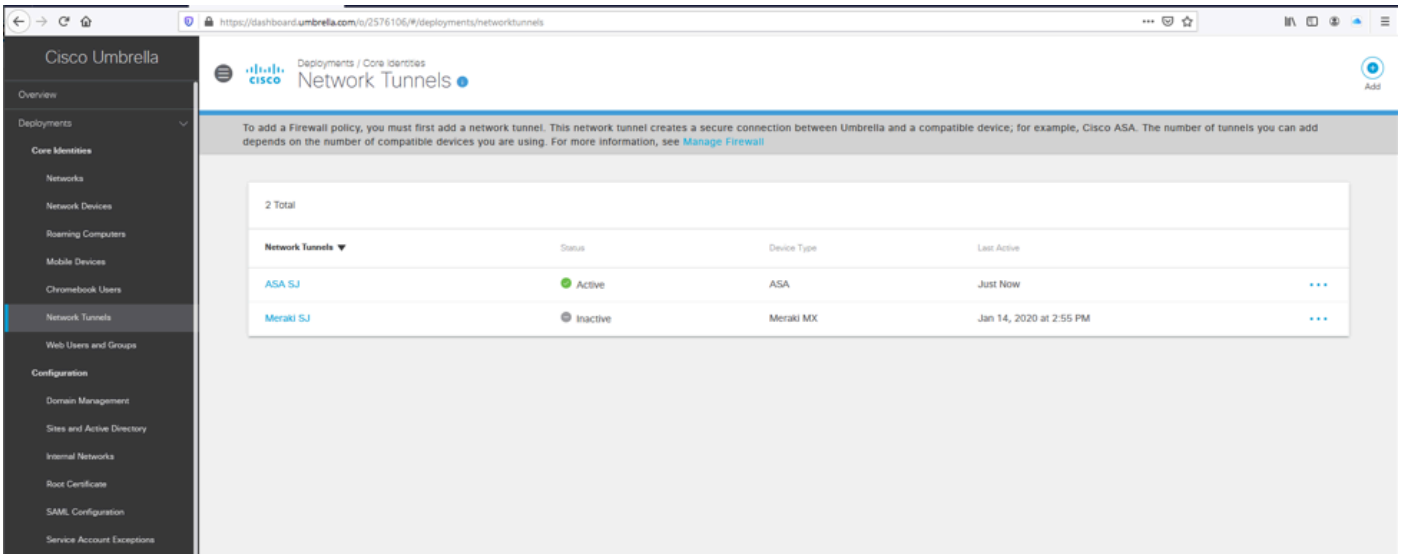
De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

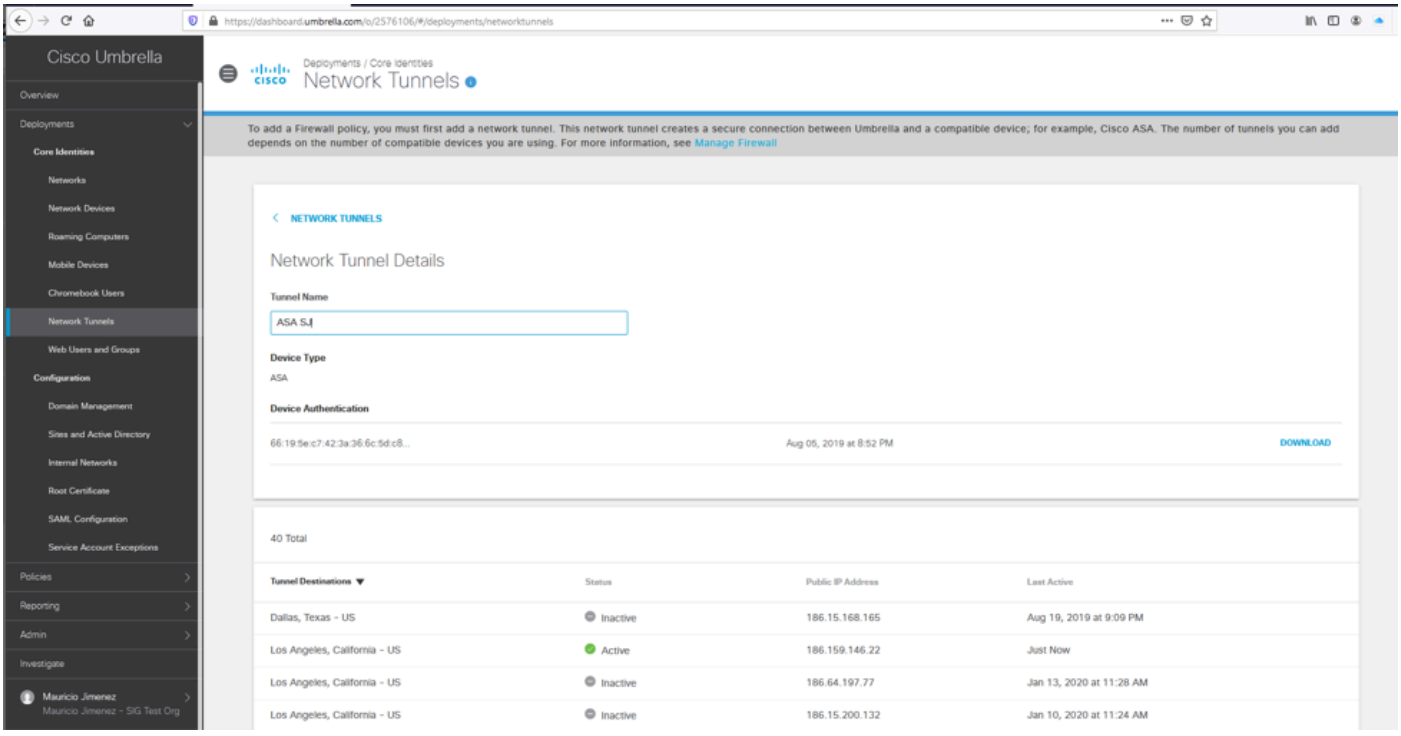
Stap 1: Verifieer een bestaande tunnel met behulp van RSA-verificatie

Controleer of u een bestaande tunnel hebt met RSA-verificatie en of de status van de tunnel in de ASA wordt weergegeven die is gekoppeld aan dit verificatietype.

1. Zoek in het dashboard van de paraplu de netwerktunnel met de ASA met een vingerafdruk voor verificatie van het apparaat.



Afbeelding 1.png



Afbeelding 2.png

2. In de Cisco ASA kunt u deze opdrachten uitvoeren om het verificatietype en het IP-adres van

de kop te controleren dat voor de tunnel wordt gebruikt.

```
show crypto ikev2 sa
```

en

```
show crypto ipsec sa
```

Afbeelding 3.png

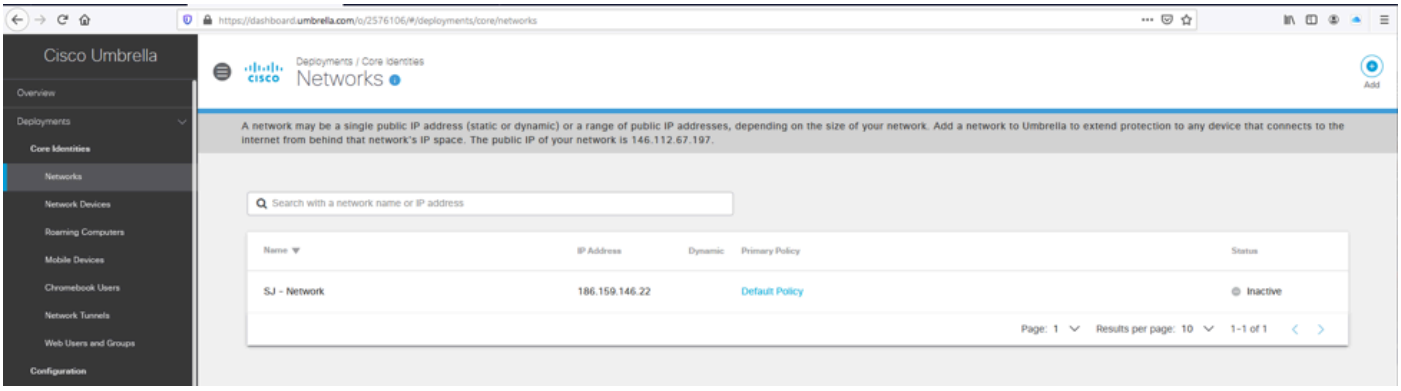
```
ASA-SJ# sh crypto ipsec sa
interface: vti
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: 186.159.
146.22

      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 --->
```

Afbeelding 4.png

Stap 2: Registreer het openbare IP van ASA

1. Zorg ervoor dat uw openbare IP-adres wordt gebruikt door de ASA-externe interface die is geregistreerd als een netwerk in het Umbrella-dashboard.

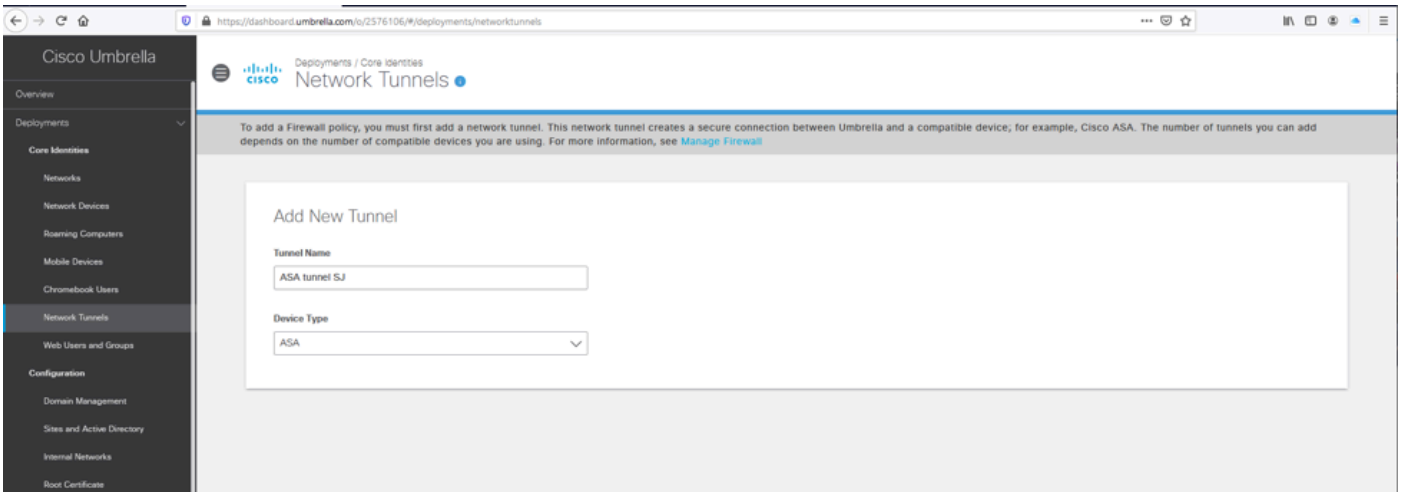
2. Als het netwerk niet bestaat, voegt u het netwerk toe en bevestigt u het openbare IP-adres dat door de ASA-interface wordt gebruikt. Het voor deze tunnel gebruikte Network object moet worden gedefinieerd met een /32 subnetmasker.



Afbeelding 5.png

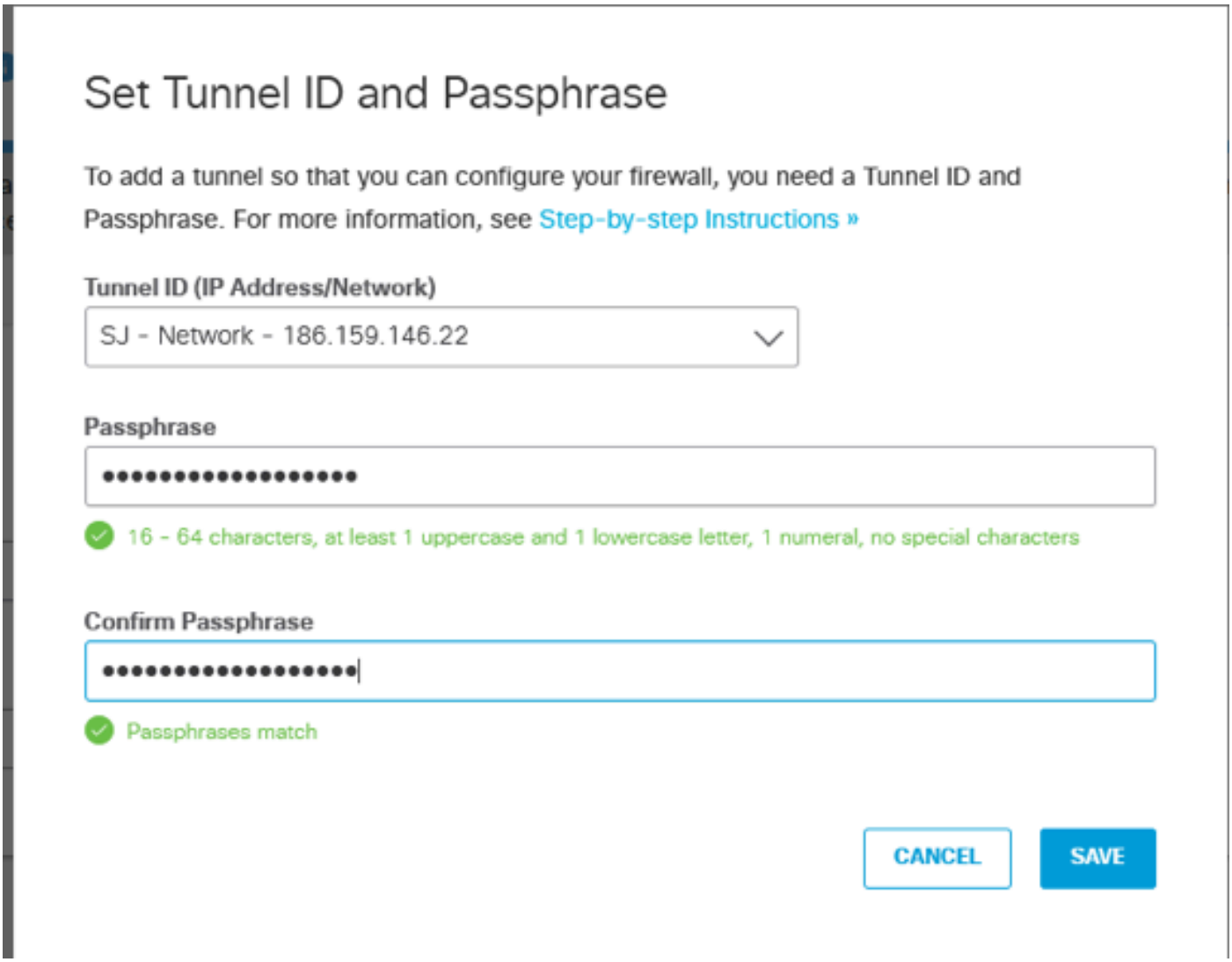
Stap 3: Nieuwe ASA-tunnel maken

1. Maak in het overkoepelende dashboard onder Implementaties/Netwerktunnels een nieuwe tunnel door de optie Toevoegen te selecteren.

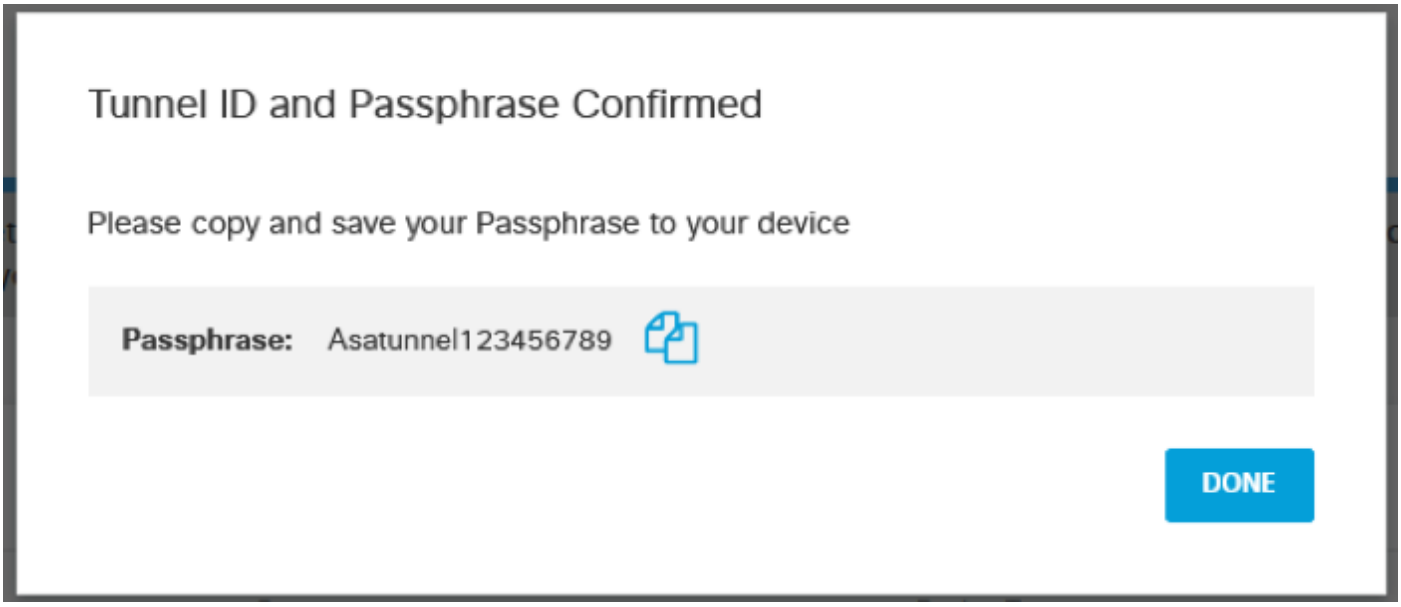


Afbeelding 6.png

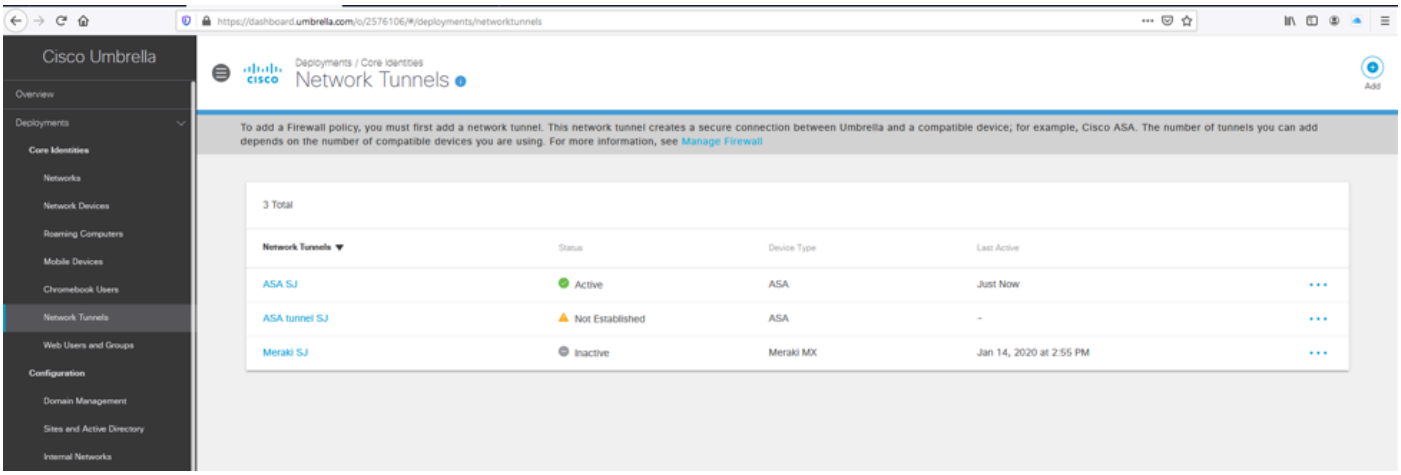
2. Selecteer de tunnel-ID op basis van het netwerk dat overeenkomt met het openbare IP-adres van uw ASA-externe interface en stel een wachtwoordzin in voor de PSK-verificatie.



Afbeelding 7.png



Afbeelding 8.png



Afbeelding 9.png

Stap 4: Nieuwe tunnelgroep maken

1. Maak in de ASA een nieuwe tunnelgroep aan met de nieuwe kop IP voor Umbrella en geef de wachtwoordzin op die in het Umbrella-dashboard is gedefinieerd voor de PSK-verificatie.

2. De bijgewerkte lijst van overkoepelende datacenters en IP's voor de headends is te vinden in de overkoepelende documentatie.

```
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 *****
```

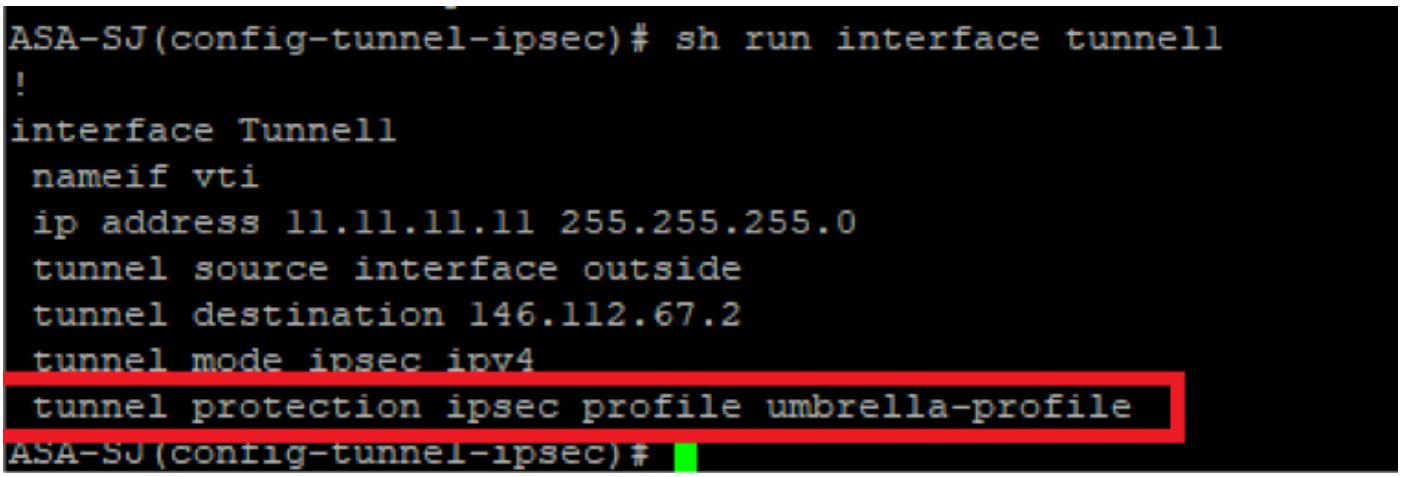
Afbeelding 10.png

Stap 5: Zoek het IPSec-profiel dat wordt gebruikt voor de tunnelinterface

1. Zoek naar het "crypto ipsec-profiel" dat wordt gebruikt in de tunnelinterface voor de

routegebaseerde configuratie naar de Umbrella-kop (# wordt vervangen door de ID die wordt gebruikt voor de tunnelinterface naar de Umbrella):

```
show run interface tunnel#
```



Afbeelding 11.png

2. Als u niet zeker bent van de tunnel-ID, kunt u deze opdracht gebruiken om bestaande tunnelinterfaces te verifiëren en te bepalen welke wordt gebruikt voor de op de paraplutunnel gebaseerde configuratie:

```
show run interface tunnel
```

Stap 6: Verwijder Old Trustpoint uit IPSec-profiel

1. Verwijder het vertrouwenspunt uit uw IPSec-profiel dat verwijst naar de RSA-verificatie voor de tunnel. U kunt de configuratie controleren met deze opdracht:

```
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
```

Afbeelding 12.png

2. Verwijder het vertrouwenspunt met de volgende opdrachten:

```
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
```

Afbeelding 13.png

3. Bevestig dat het trustpoint uit het crypto-ipsec-profiel is verwijderd:

```
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
```

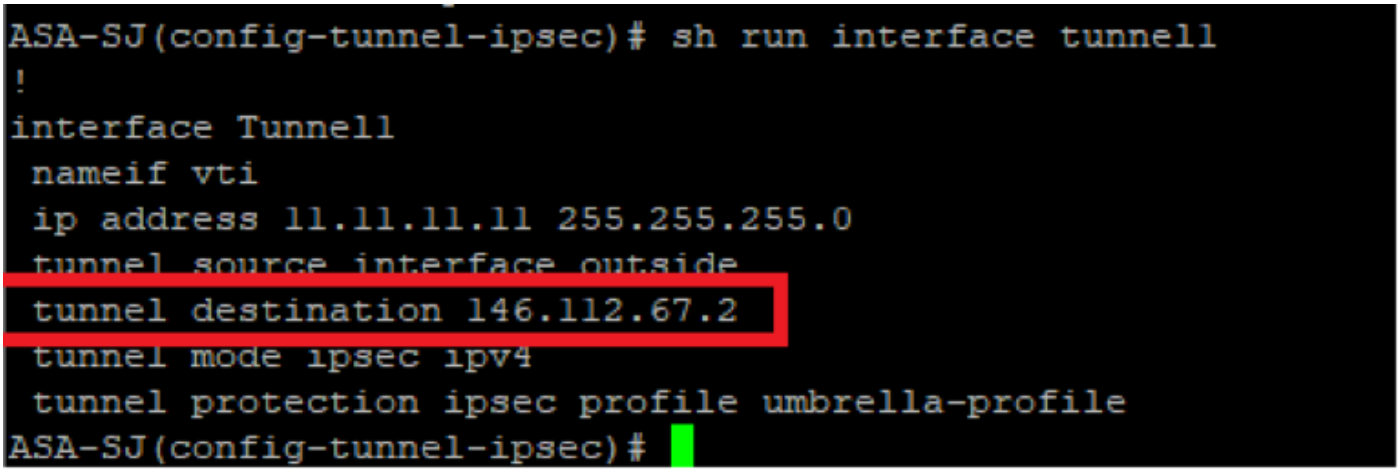
Afbeelding 14.png

Stap 7: Tunnel-interface bijwerken met nieuwe Umbrella Headend IP

1. Vervang de bestemming van de tunnelinterface door het nieuwe IP-adres van het kopstuk van de paraplu dat eindigt in .8.

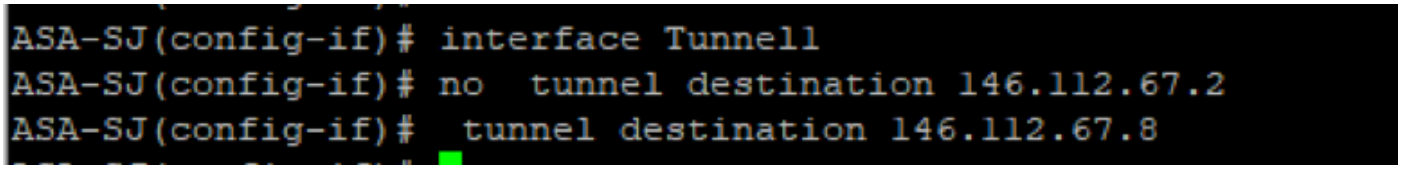
- U kunt deze opdracht gebruiken om de huidige bestemming te controleren, zodat deze wordt vervangen door het IP-adres uit de nieuwe IP-adresbereiken van het datacenter, die te vinden zijn in de overkoepelende documentatie:

```
show run interface tunnel
```



Afbeelding 15.png

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



Afbeelding 16.png

2. Bevestig de wijziging met de opdracht:

```
show run interface tunnel#
```

```
ASA-SJ(config-if)# show run interface tunnel1
!
interface Tunnel1
 nameif vti
 ip address 11.11.11.11 255.255.255.0
 tunnel source interface outside
 tunnel destination 146.112.67.8
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile umbrella-profile
```

Afbeelding 17.png

Stap 8: Bevestig dat de nieuwe tunnelconfiguratie is ingesteld

1. Bevestig dat de tunnelverbinding met Umbrella correct is hersteld met het bijgewerkte IP-adres van de koptelefoon en dat de PSK-verificatie met deze opdracht wordt gebruikt:

```
show crypto ikev2 sa
```

```
ASA-SJ(config-if)# sh crypto ikev2 sa

IKEv2 SAs:

Session-id:5, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                 Remote                                Status         Role
 89307167 186.159.146.22/4500                   146.112.67.8/4500                     READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:19, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/347 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: 0xc133a3b2/0xea076575
```

Afbeelding 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
```

Afbeelding 19.png

Stap 9 (optioneel): Verwijder de oude tunnelgroep

1. Verwijder de oude tunnelgroep die naar het vorige IP-bereik van de Umbrella-kop wees .2.

U kunt deze opdracht gebruiken om de juiste tunnel te identificeren voordat u de configuratie verwijdert:

```
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 *****
```

Afbeelding 20.png

2. Verwijder elke verwijzing van de oude tunnelgroep met behulp van deze opdracht:

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

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

Afbeelding 21.png

Stap 10 (optioneel): Verwijder Old Trustpoint

1. Verwijder elke verwijzing naar het eerder gebruikte vertrouwenspunt met de op de paraplutunnel gebaseerde configuratie met deze opdracht:

```
sh run crypto ipsec
```

De vriendelijke naam die voor het trustpoint wordt gebruikt, is te vinden wanneer u het "crypto ipsec-profiel" bekijkt:

```
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
```

Afbeelding 22.png

2. U kunt deze opdracht uitvoeren om de trustpoint-configuratie te bevestigen. Zorg ervoor dat de vriendelijke naam overeenkomt met de configuratie die wordt gebruikt in de crypto ipsec-profielopdracht:

```
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
```

Afbeelding 23.png

3. Gebruik de opdracht voor meer informatie over het certificaat:

```
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:
```

Afbeelding 24.png

4. Verwijder het vertrouwenspunt met de opdracht:

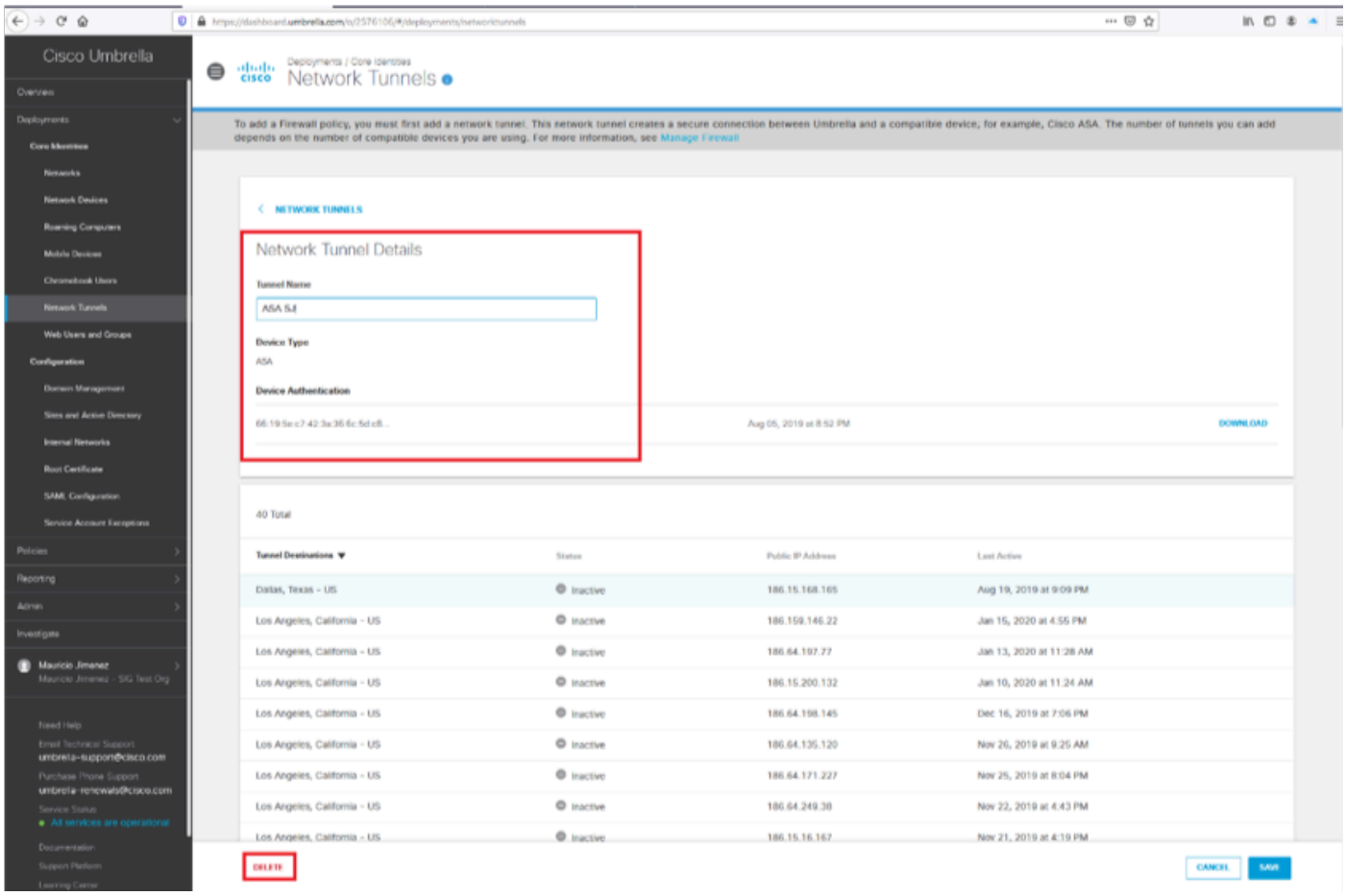
```
no crypto ca trustpoint <trustpoint-name>
```

```
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)#
```

Afbeelding 25.png

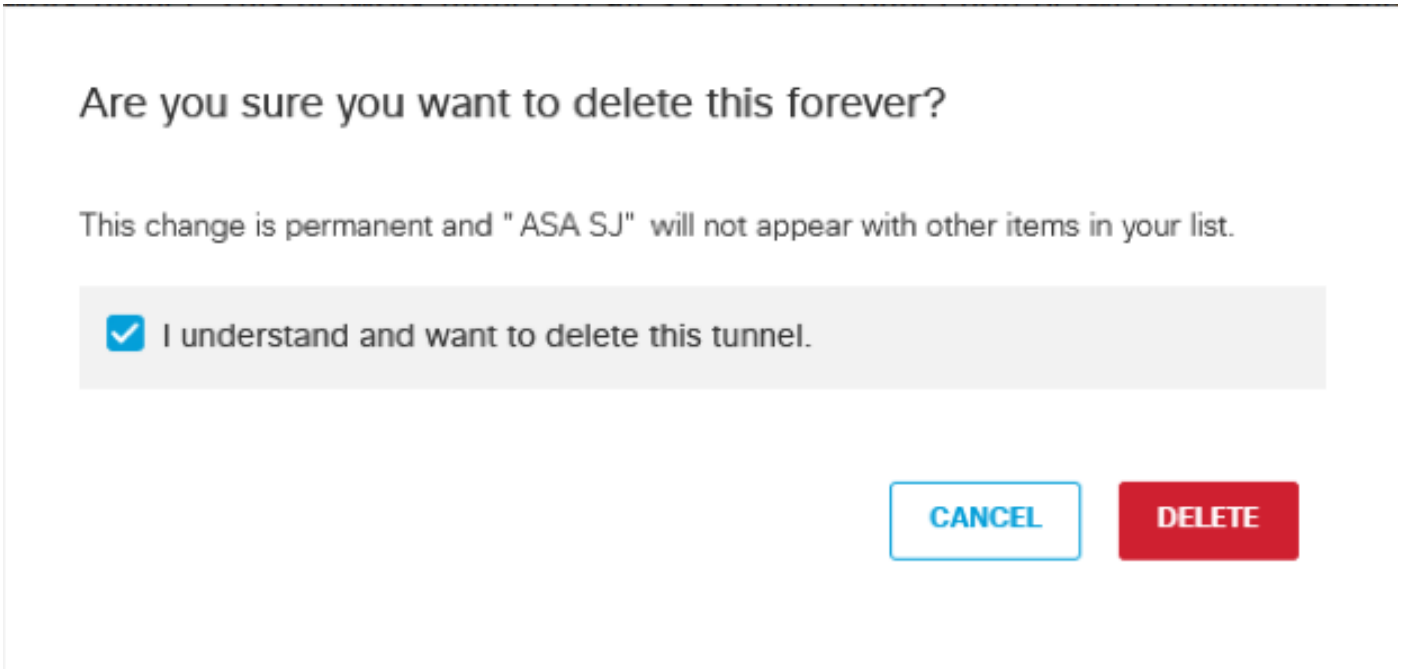
Stap 11 (optioneel): Oude netwerktunnel verwijderen

1. Verwijder de oude netwerktunnel uit het Umbrella-dashboard door naar Netwerktunneldetails te navigeren en Verwijderen te selecteren.



Afbeelding 26.png

2. Bevestig de verwijdering door de optie Ik begrijp en wil deze tunnel verwijderen in het pop-upvenster te selecteren en selecteer vervolgens Verwijderen.



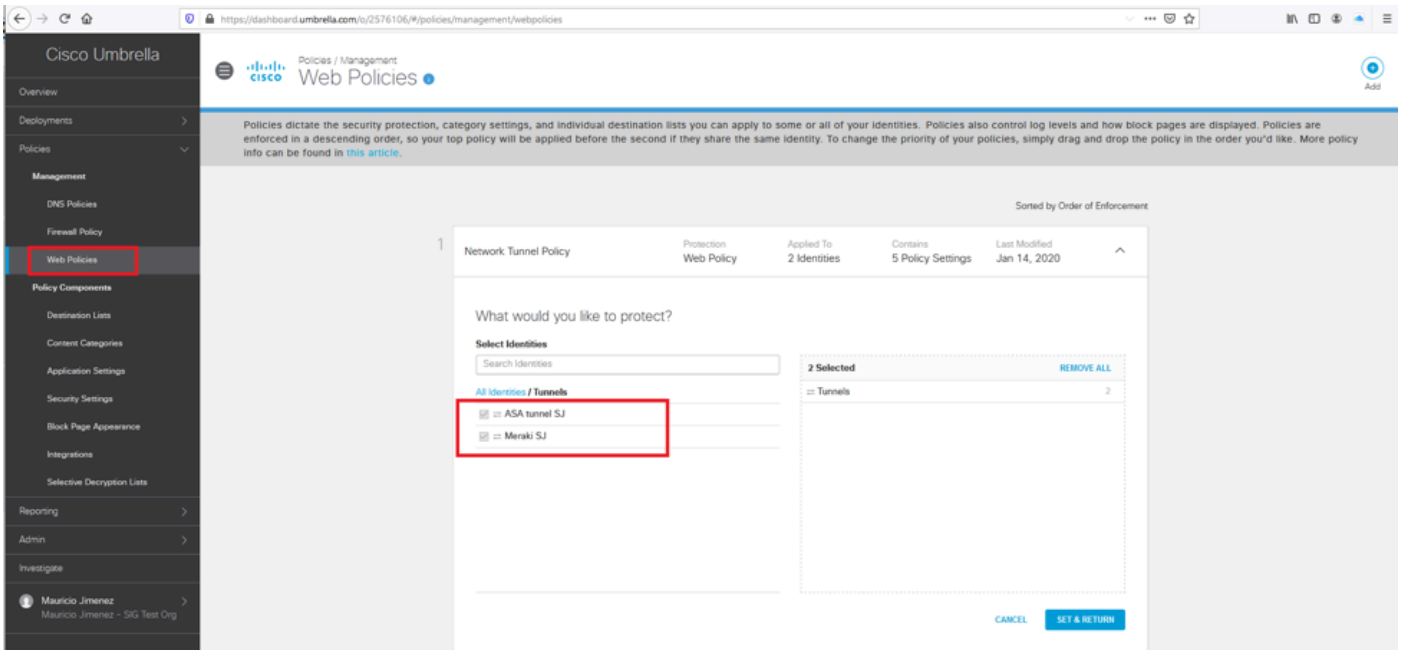
Afbeelding 27.png

Stap 12: Webbeleid bijwerken met nieuwe tunnelidentiteit

Bevestig dat uw webbeleid de bijgewerkte identiteit heeft met de nieuwe netwerktunnel:

1. Navigeer in het Umbrella-dashboard naar Beleid > Beheer > Webbeleid.

2. Controleer het gedeelte Tunnels en bevestig dat uw webbeleid de bijgewerkte identiteit heeft met de nieuwe netwerktunnel.



Afbeelding 28.png

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.