# Modification du tunnel pare-feu fourni dans le cloud de RSA en authentification PSK

## Table des matières



## Introduction

Ce document décrit les étapes pour reconfigurer le mécanisme d'authentification de Cloud Delivered Firewall Tunnel de RSA à PSK sur Cisco ASA.

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

### Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Étape 1 : Vérification d’un tunnel existant avec l’authentification RSA

Vérifiez que vous disposez d'un tunnel existant utilisant l'authentification RSA et que l'état du tunnel dans l'ASA indique connecté avec ce type d'authentification.

1. Dans le tableau de bord Umbrella, recherchez le tunnel réseau avec l'ASA montrant une empreinte digitale d'authentification de périphérique.

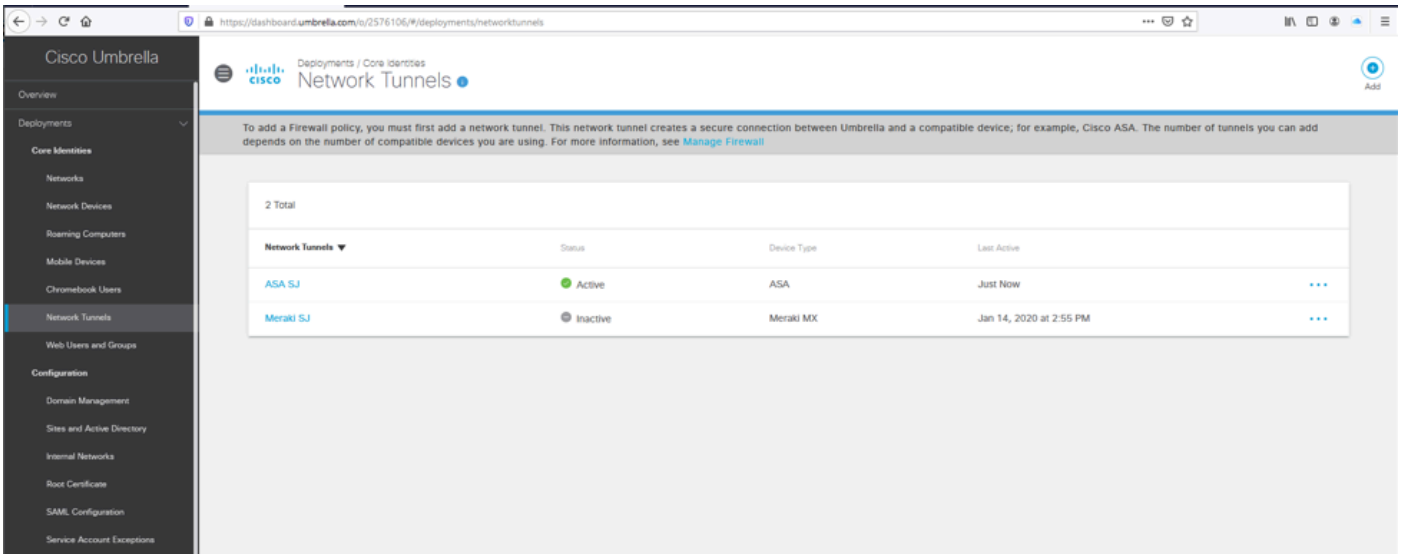


Image1.png

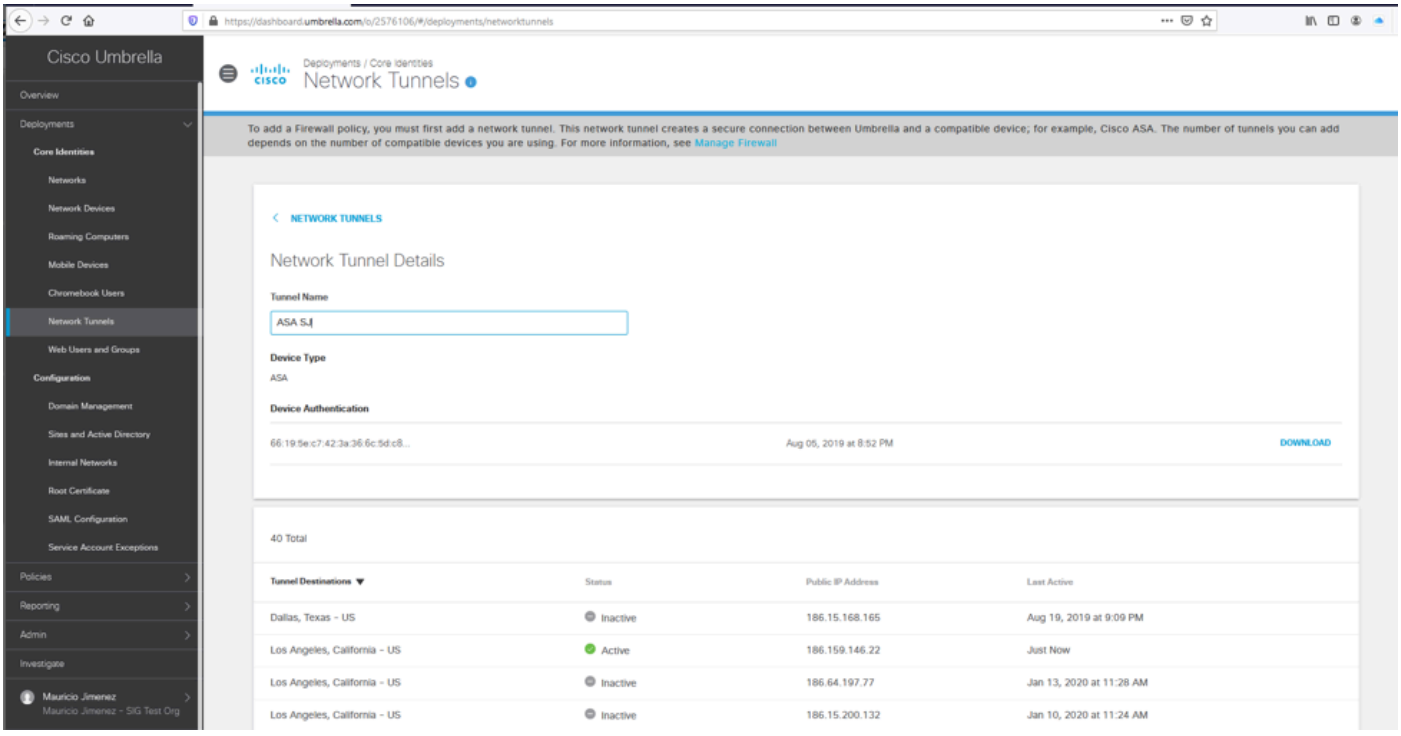


Image2.png

2. Dans Cisco ASA, vous pouvez exécuter ces commandes pour vérifier le type d'authentification

et l'adresse IP de tête de réseau utilisés pour le tunnel.

```
show crypto ikev2 sa
```

et

```
show crypto ipsec sa
```


Image3.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 --->
```

Image4.png

# Étape 2 : Enregistrement de l'adresse IP publique d'ASA

1. Assurez-vous que votre adresse IP publique est utilisée par l'interface externe ASA enregistrée en tant que réseau dans le tableau de bord Umbrella.

2. Si le réseau n'existe pas, continuez à l'ajouter et confirmez l'adresse IP publique utilisée par l'interface ASA. L'objet Network utilisé pour ce tunnel doit être défini avec un masque de sous-réseau /32.

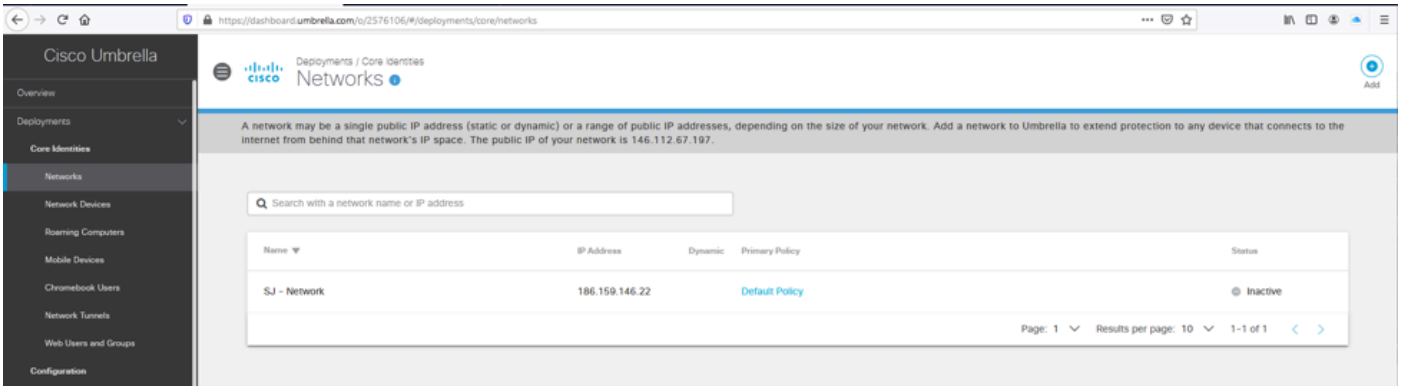


Image5.png

# Étape 3 : Créer un nouveau tunnel ASA

1. Dans le tableau de bord Umbrella sous Déploiements/Tunnels réseau, créez un nouveau tunnel en sélectionnant l'option Add.

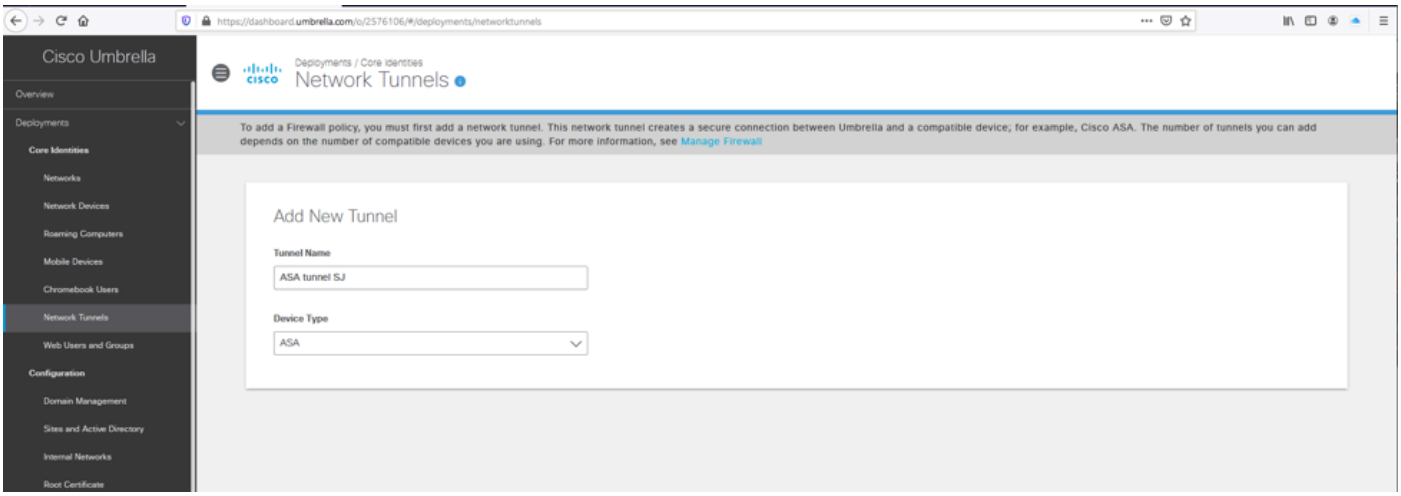


Image6.png

2. Sélectionnez l'ID de tunnel basé sur le réseau qui correspond à l'IP publique de votre interface externe ASA et configurez une phrase de passe pour l'authentification PSK.

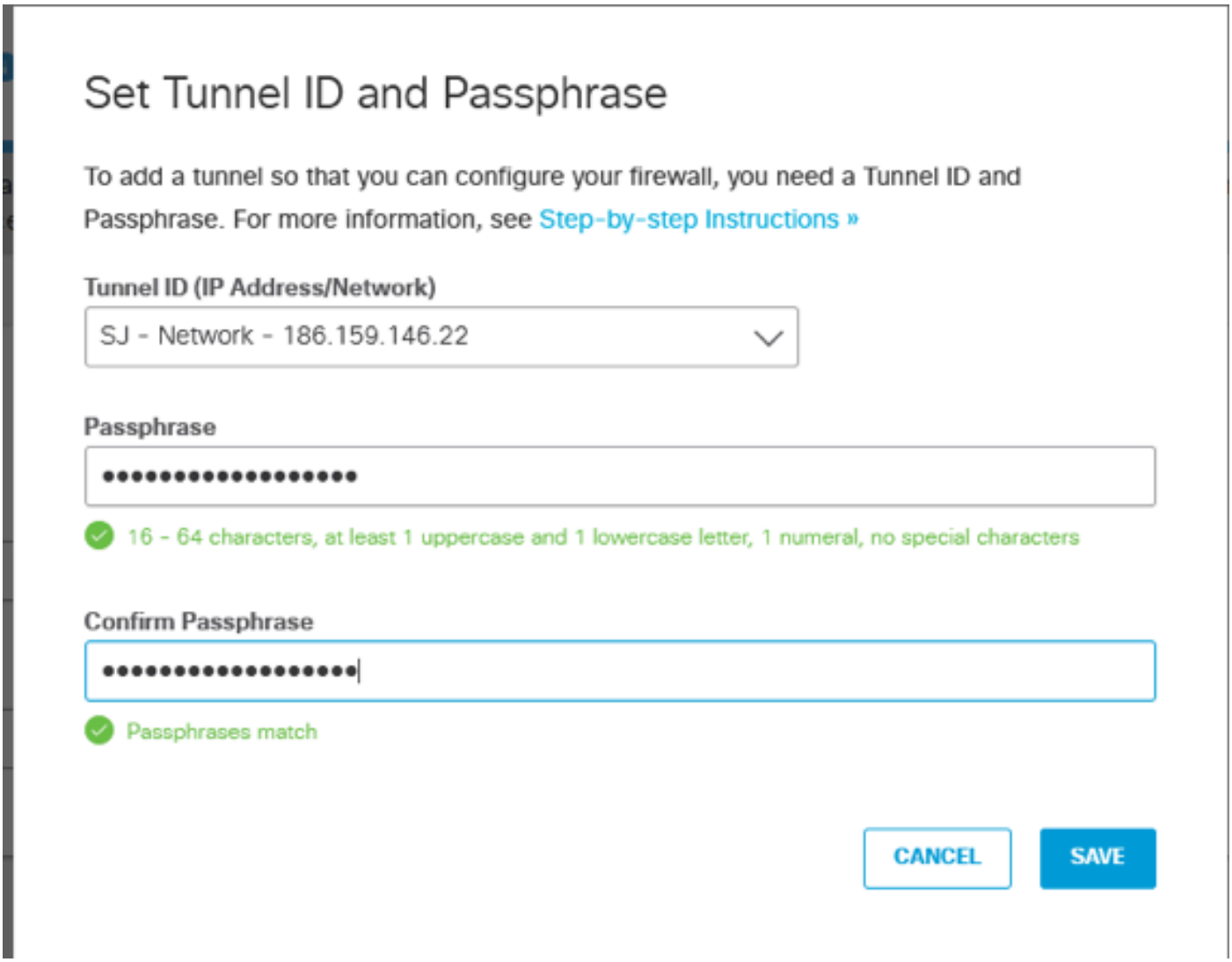


Image7.png

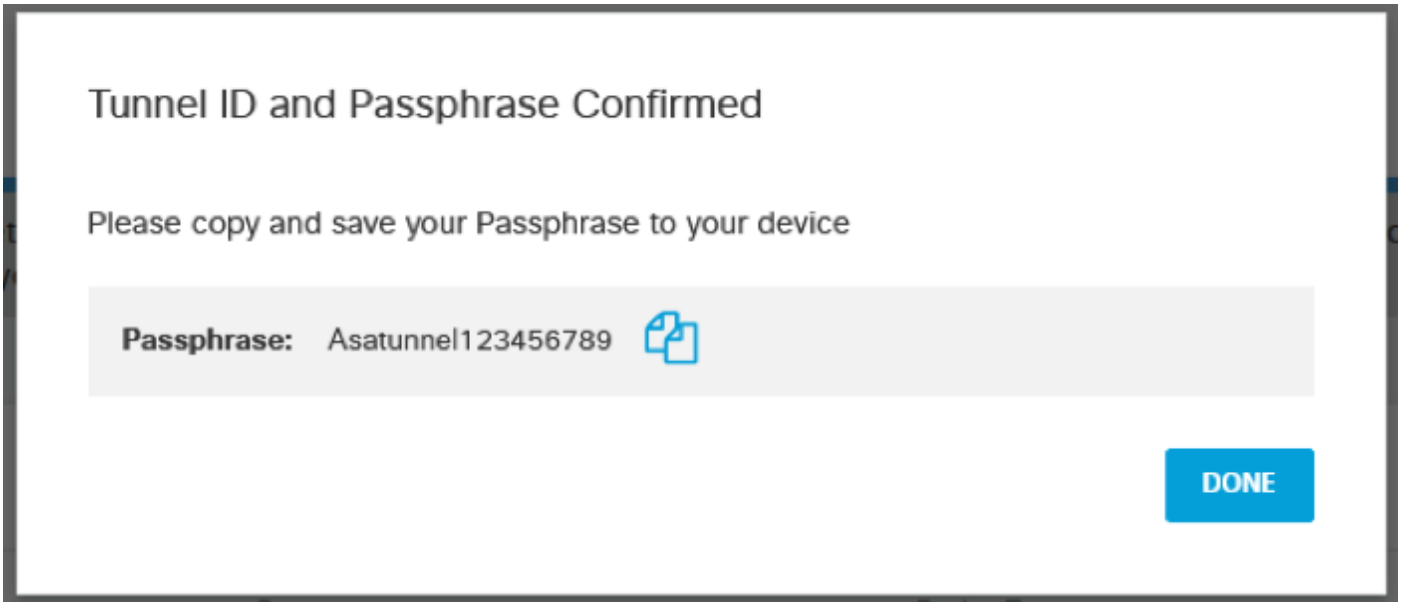


Image8.png

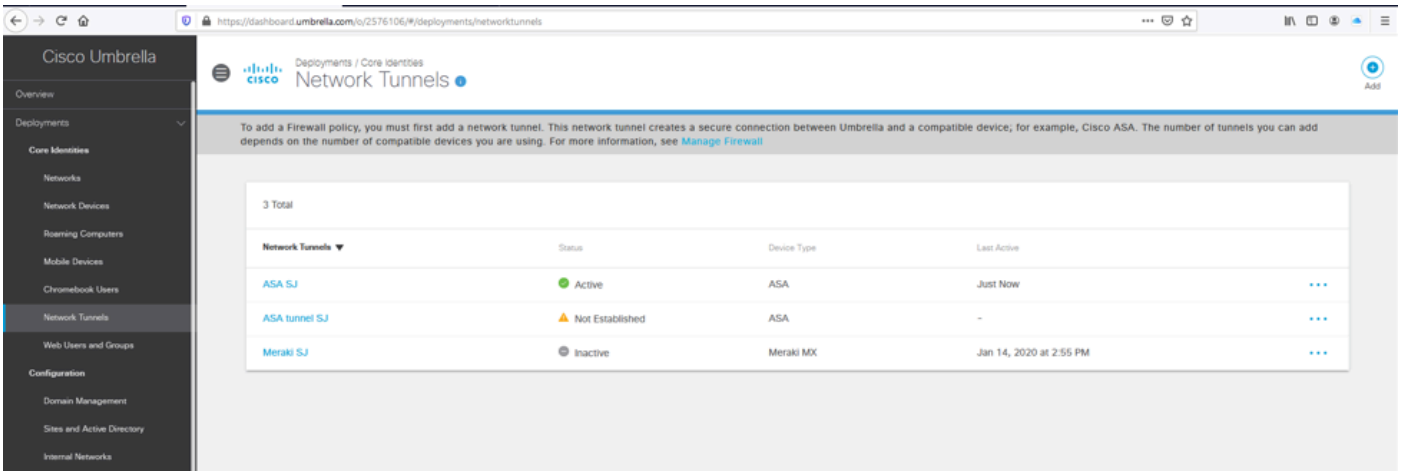


Image9.png

# Étape 4 : Créer un groupe de tunnels

1. Sur l'ASA, créez un nouveau groupe de tunnels à l'aide de la nouvelle adresse IP de tête de réseau pour Umbrella et spécifiez la phrase de passe définie dans le tableau de bord Umbrella pour l'authentification PSK.

2. La liste mise à jour des centres de données et IP Umbrella pour les têtes de réseau est disponible dans la documentation 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 *****
```

Image10.png

# Étape 5 : Localisez le profil IPSec utilisé pour l'interface de tunnel

1. Recherchez le «crypto ipsec profile» qui est utilisé dans l'interface de tunnel pour la configuration basée sur la route vers la tête de réseau Umbrella (# est remplacé par l'ID utilisé

pour l'interface de tunnel vers 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)#
```

Image11.png

2. Si vous n'êtes pas sûr de l'ID de tunnel, vous pouvez utiliser cette commande pour vérifier les interfaces de tunnel existantes et déterminer celle qui est utilisée pour la configuration basée sur le tunnel Umbrella :

```
show run interface tunnel
```

## Étape 6 : Supprimer l'ancien point de confiance du profil IPSec

1. Supprimez le trustpoint de votre profil IPSec qui fait référence à l'authentification RSA pour le tunnel. Vous pouvez vérifier la configuration à l'aide de cette commande :

```
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
```

Image12.png

2. Procédez à la suppression du point de confiance avec les commandes suivantes :

```
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
```

Image13.png

3. Confirmez que le point de confiance a été supprimé du profil ipsec de chiffrement :

```
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
```

Image14.png

## Étape 7 : Mettre à jour l'interface du tunnel avec la nouvelle adresse IP Umbrella Headend

1. Remplacez la destination de l'interface de tunnel par la nouvelle adresse IP de tête de réseau Umbrella se terminant par .8.

- Vous pouvez utiliser cette commande pour vérifier la destination actuelle afin qu'elle soit remplacée par l'adresse IP des nouvelles plages d'adresses IP du centre de données, qui se trouvent dans la [documentation 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)#
```

Image15.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
```

Image16.png

2. Confirmez la modification à l'aide de la commande :

```
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
```

Image17.png

## Étape 8 : Confirmer que la nouvelle configuration du tunnel a été correctement établie

1. Confirmez que la connexion du tunnel à Umbrella a été rétablie correctement avec l'adresse IP de tête de réseau mise à jour et en utilisant l'authentification PSK avec cette commande :

```
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
```

Image18.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
```

Image19.png

# Étape 9 (facultative): Supprimer l'ancien groupe de tunnels

1. Supprimez l'ancien groupe de tunnels qui pointait vers la plage IP de tête de réseau Umbrella précédente .2.

Vous pouvez utiliser cette commande pour identifier le tunnel correct avant de supprimer la configuration :

```
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 *****
```

Image20.png

2. Supprimez toute référence de l'ancien groupe de tunnels à l'aide de cette commande :

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

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

Image21.png

# Étape 10 (facultative): Supprimer l'ancien point de confiance

1. Supprimez toute référence du point de confiance précédemment utilisé avec la configuration Umbrella basée sur le tunnel avec cette commande :

```
sh run crypto ipsec
```

Le nom convivial utilisé pour le point de confiance se trouve lorsque vous consultez le « profil 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
```

Image22.png

2. Vous pouvez exécuter cette commande pour confirmer la configuration du point de confiance. Assurez-vous que le nom convivial correspond à la configuration utilisée dans la commande crypto ipsec profile :

```
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
```

Image23.png

3. Pour obtenir plus de détails sur le certificat, utilisez la commande suivante :

```
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:
```

Image24.png

4. Supprimez le point de confiance avec la commande :

```
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)#
```

Image25.png

# Étape 11 (facultative): Supprimer l'ancien tunnel réseau

1. Supprimez l'ancien tunnel réseau du tableau de bord Umbrella en naviguant jusqu'à Network Tunnel Details et en sélectionnant Delete.

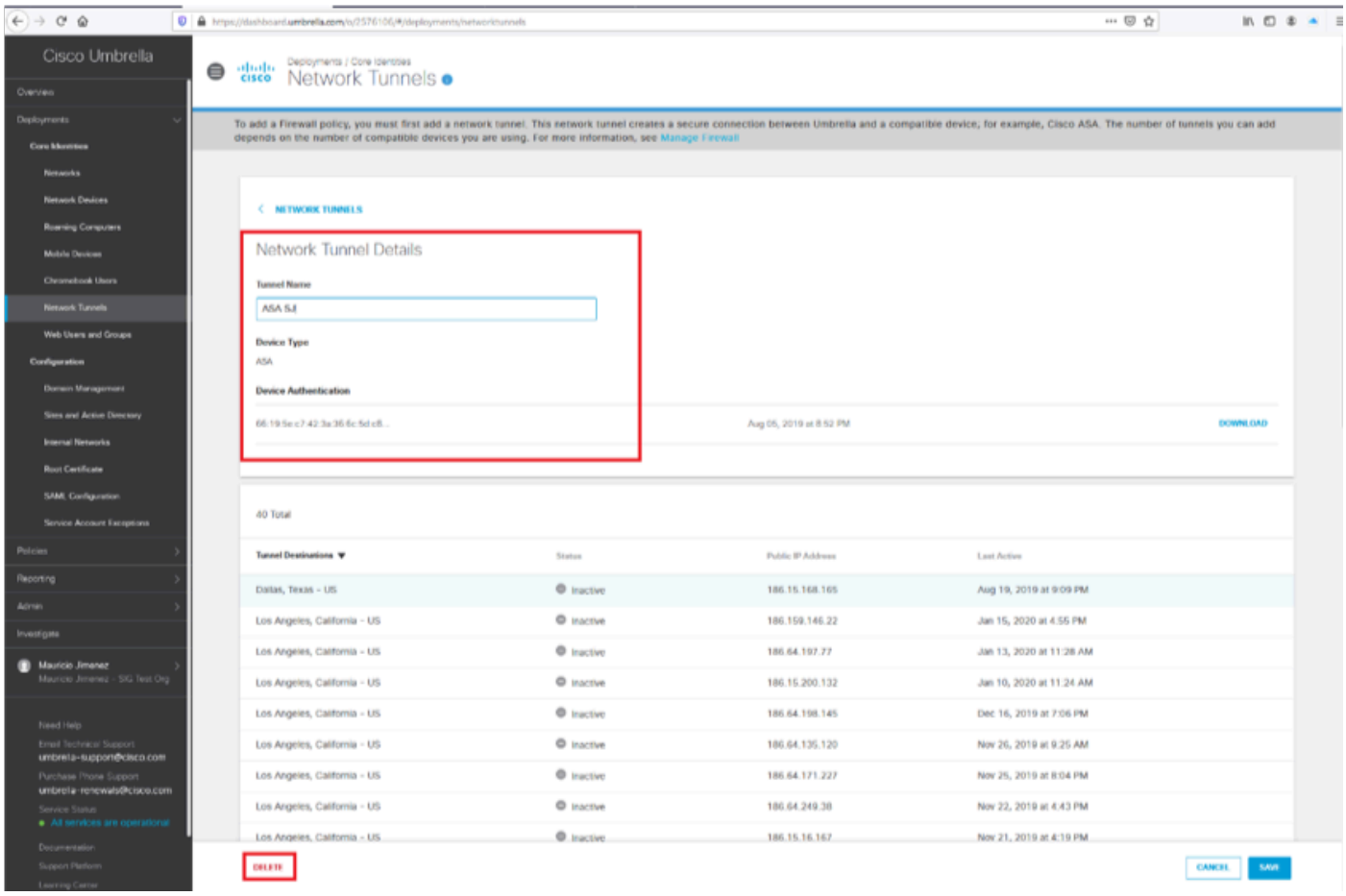


Image26.png

2. Confirmez votre suppression en sélectionnant l'option Je comprends et je veux supprimer ce tunnel dans la fenêtre contextuelle, puis sélectionnez Supprimer.

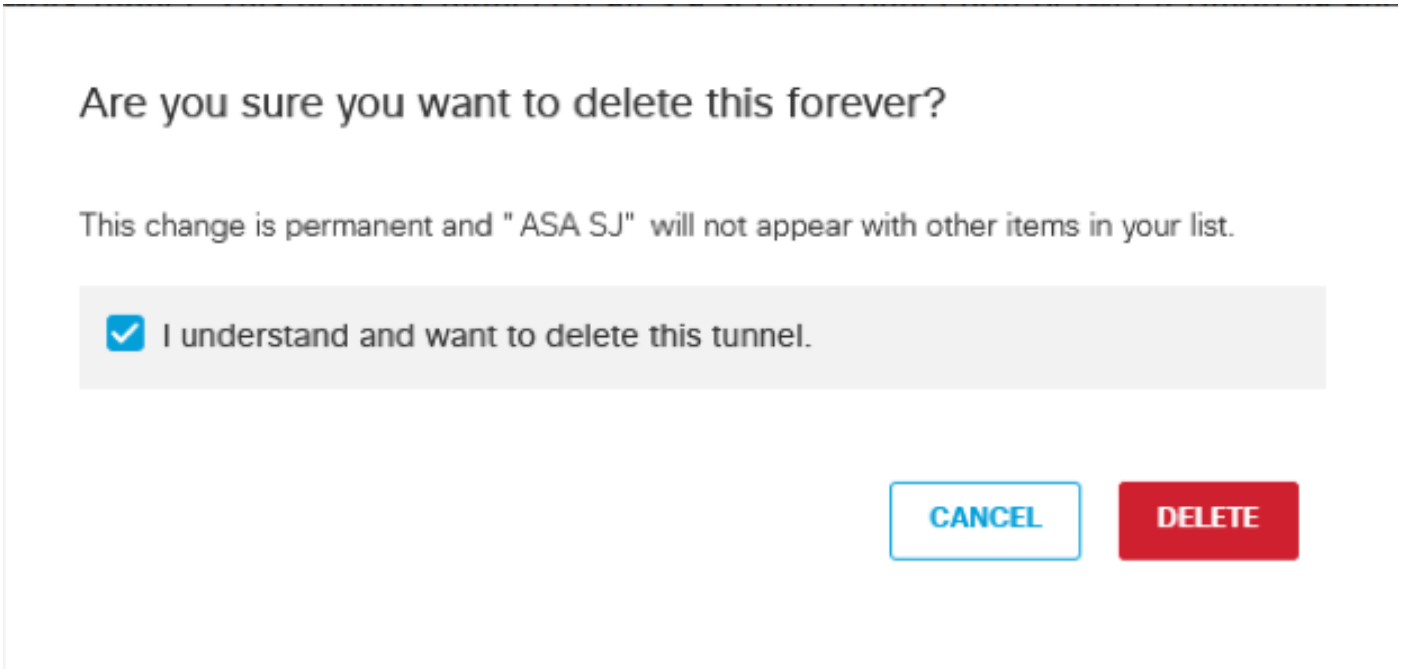


Image27.png

## Étape 12: Mettre à jour les stratégies Web avec une nouvelle

# identité de tunnel

Vérifiez que vos stratégies Web ont l'identité mise à jour avec le nouveau tunnel réseau :

1. Dans le tableau de bord Umbrella, accédez à Politiques > Gestion > Politiques Web.

2. Consultez la section Tunnels et vérifiez que vos stratégies Web ont l'identité mise à jour avec le nouveau tunnel réseau.

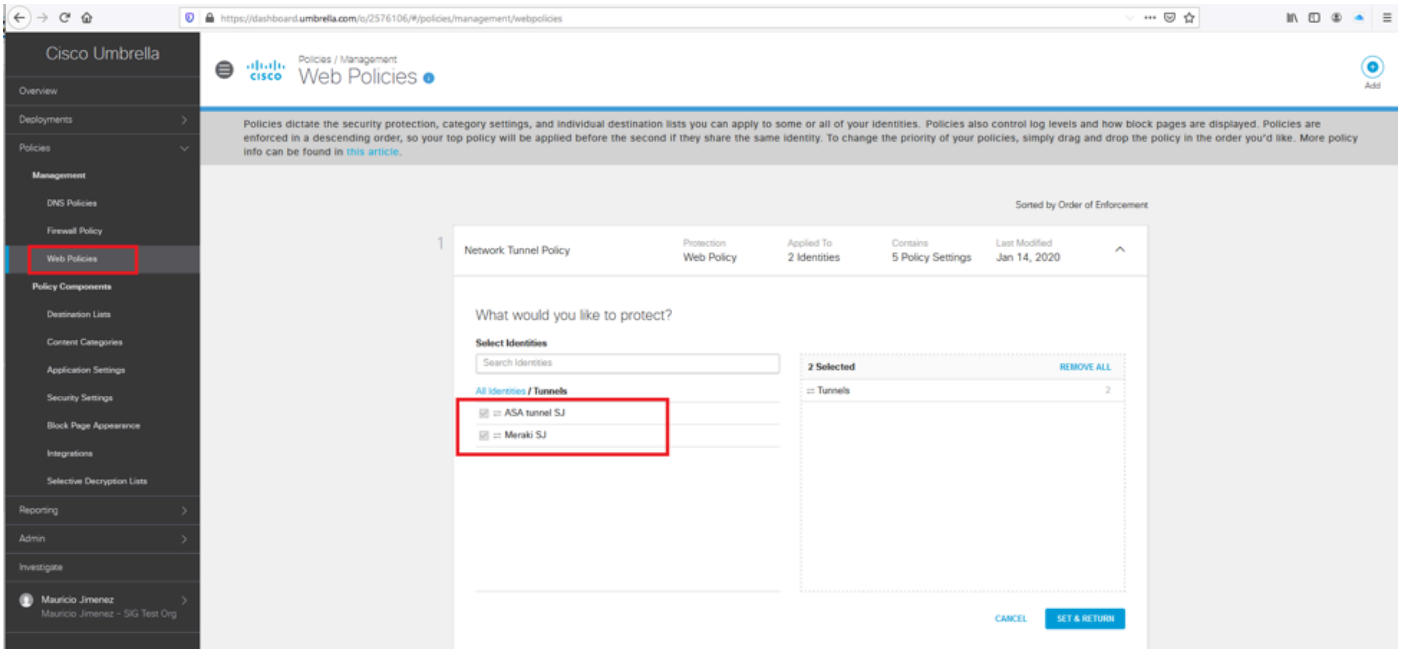


Image28.png

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.