クラウド配信ファイアウォールトンネルをRSA認証からPSK認証に変更

内容

はじめに

このドキュメントでは、Cisco ASAでCloud Delivered Firewall Tunnelの認証メカニズムをRSAからPSKに再設定する手順について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

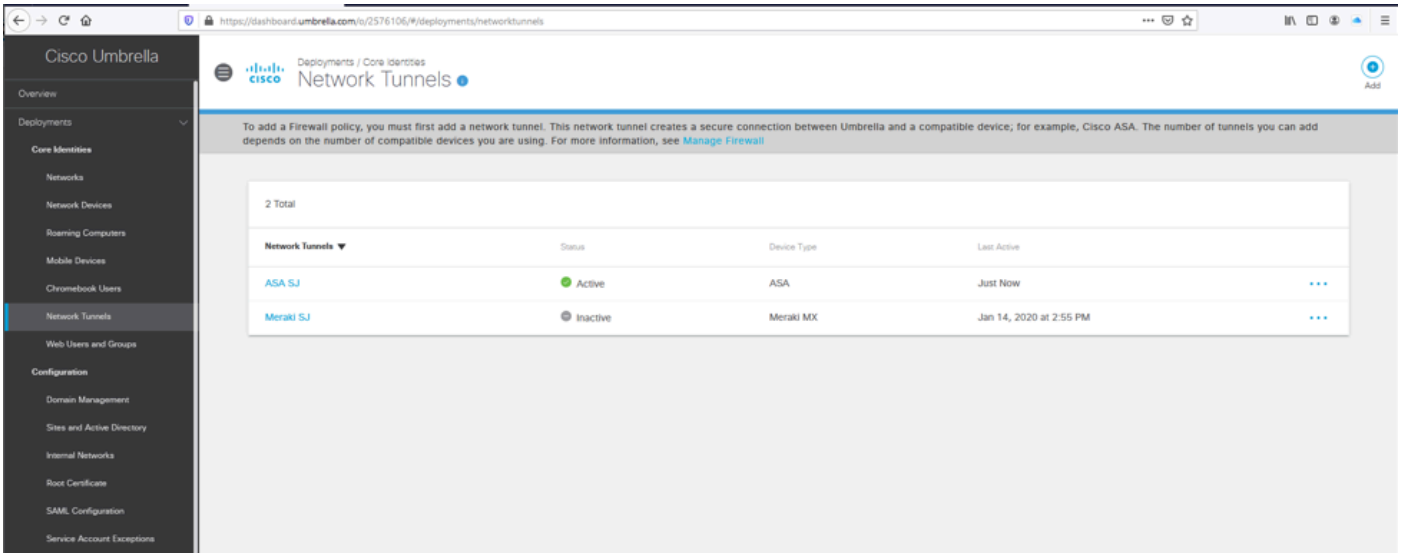
このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

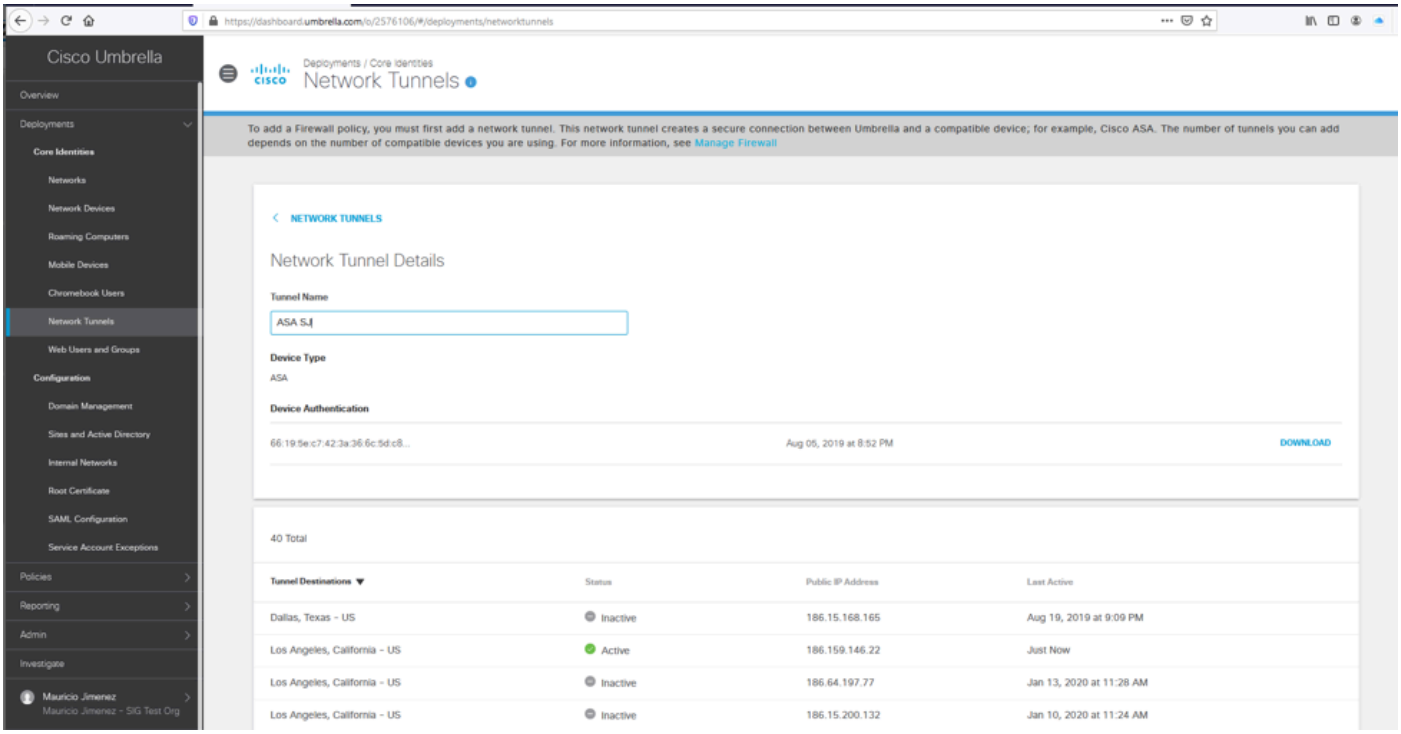
ステップ1:RSA認証を使用した既存のトンネルの確認

RSA認証を使用する既存のトンネルがあること、およびASAのトンネルのステータスがこの認証タイプで接続されていることを確認します。

1. Umbrellaダッシュボードで、デバイス認証フィンガープリントを示すASAを含むネットワークトンネルを見つけます。



画像1.png



画像2.png

2. Cisco ASAでは、次のコマンドを実行して、トンネルに使用されている認証タイプとヘッドエンドIPを確認できます。

show crypto ikev2 sa

と

show crypto ipsec sa

画像3.png

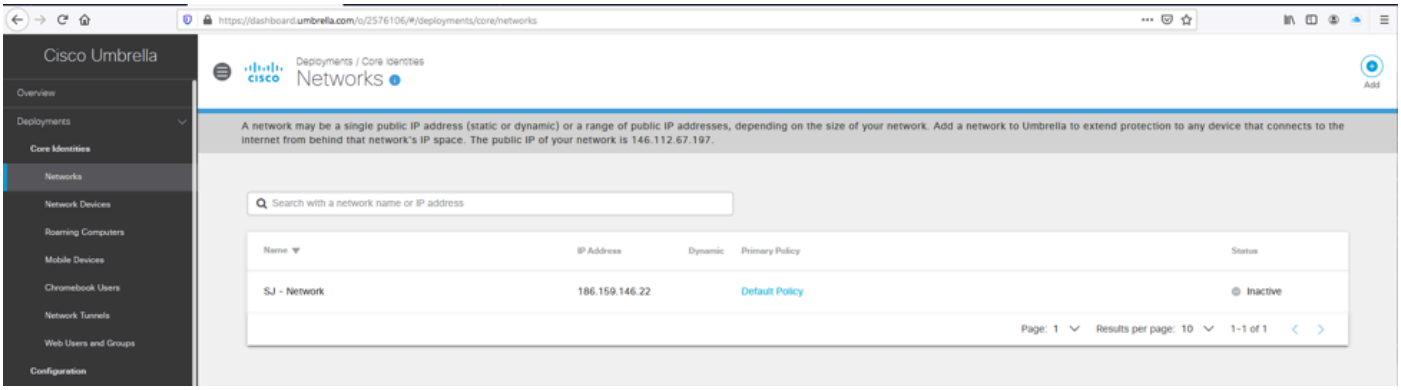
```
ASA-SJ# sh crypto ipsec sa
interface: vti
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: 186.159.
146.22

      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 --->
```

画像4.png

ステップ2:ASAのパブリックIPの登録

1. ASA外部インターフェイスで使用されているパブリックIPが、Umbrellaダッシュボードにネットワークとして登録されていることを確認します。

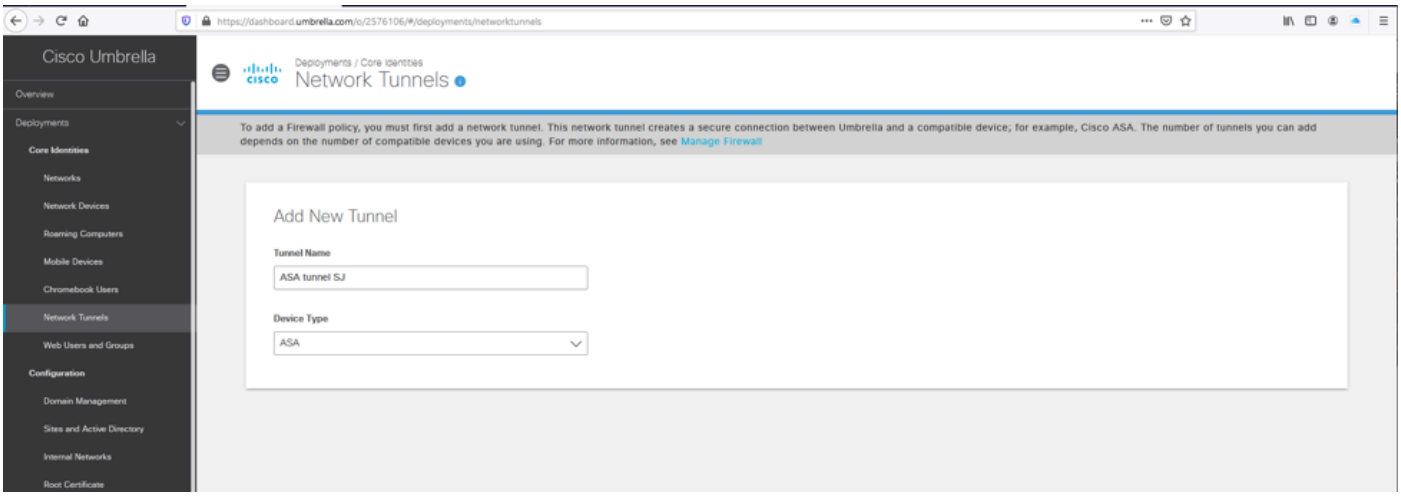
2. ネットワークが存在しない場合は、ネットワークの追加に進み、ASAインターフェイスによって使用されるパブリックIPを確認します。このトンネルに使用するNetworkオブジェクトは、/32サブネットマスクで定義する必要があります。



画像5.png

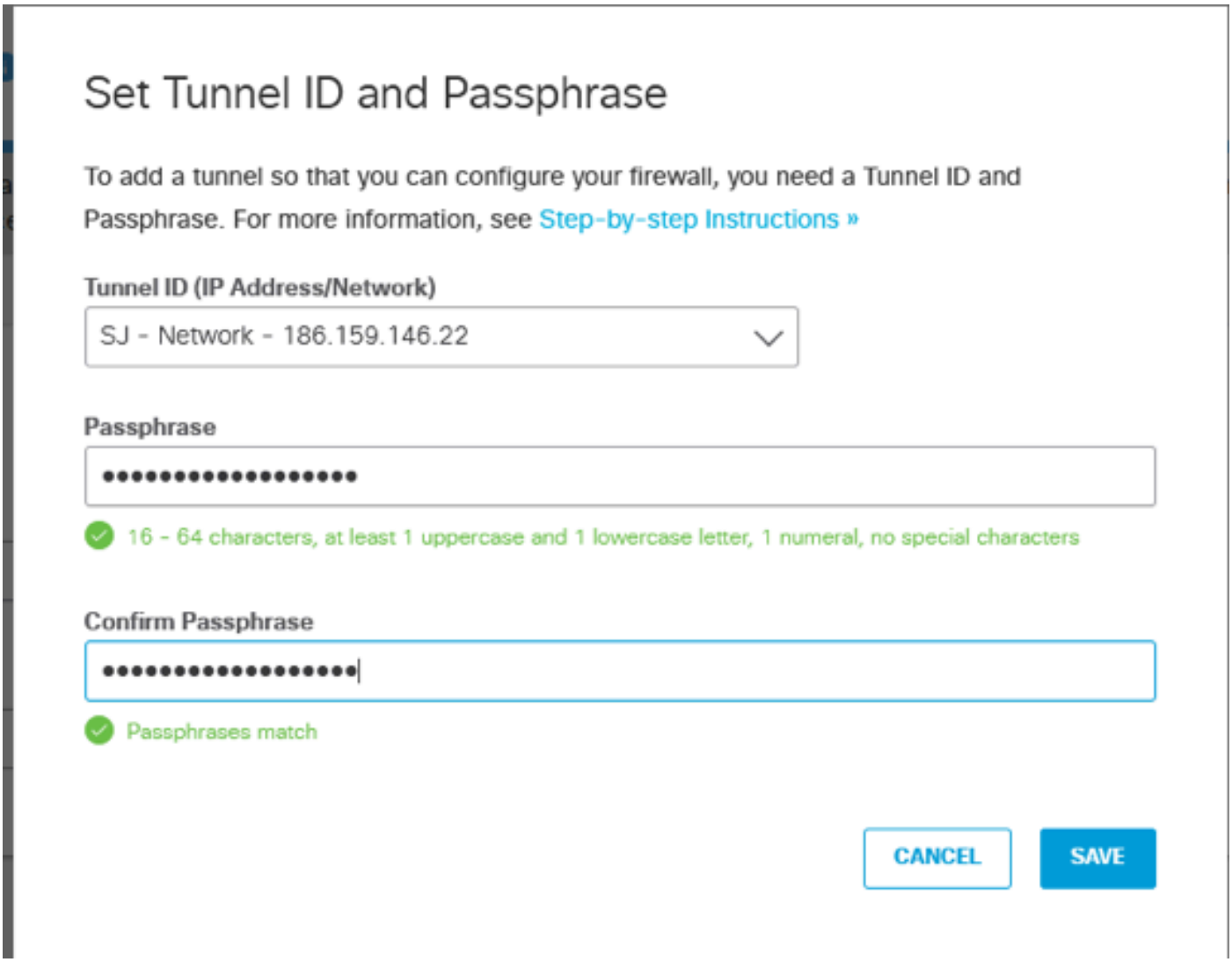
ステップ3：新しいASAトンネルの作成

1. UmbrellaダッシュボードのDeployments/Network Tunnelsで、Addオプションを選択して、新しいトンネルを作成します。

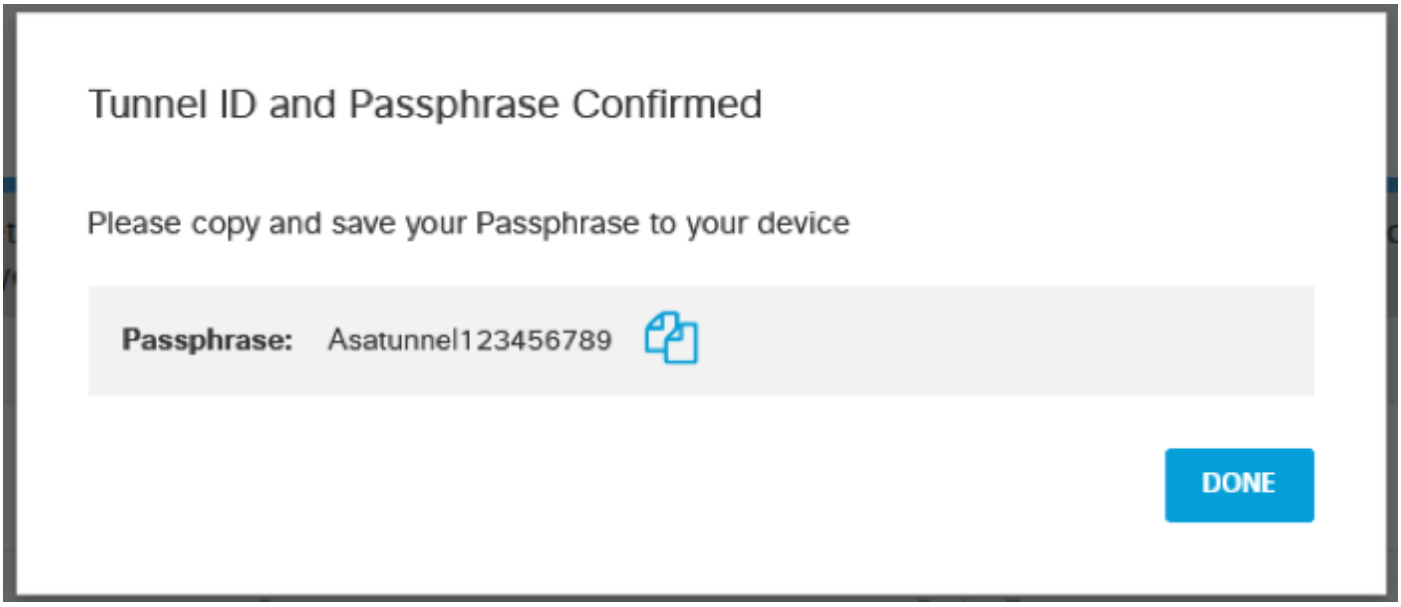


画像6.png

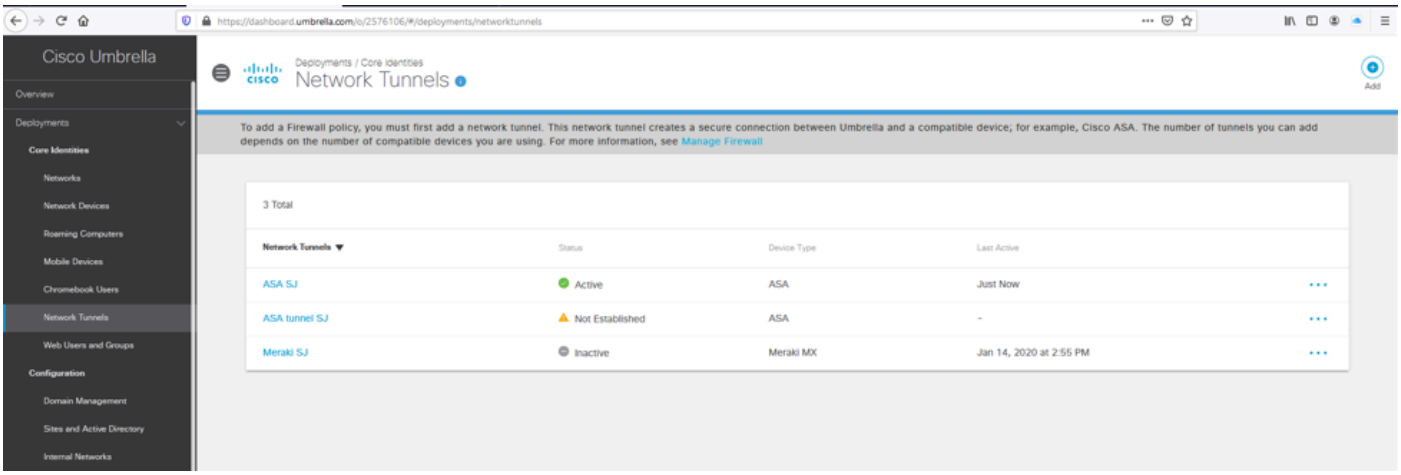
2. ASA外部インターフェイスのパブリックIPと一致するネットワークに基づいてトンネルIDを選択し、PSK認証用のパスフレーズをセットアップします。



画像7.png



画像8.png



画像9.png

ステップ4：新しいトンネルグループの作成

1. ASAで、Umbrellaの新しいヘッドエンドIPを使用して新しいトンネルグループを作成し、UmbrellaダッシュボードでPSK認証用に定義されているパスフレーズを指定します。

2. Umbrellaのデータセンターおよびヘッドエンド用IPの更新されたリストについては、Umbrellaのドキュメントを参照してください。

```
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 *****
```

画像10.png

ステップ5：トンネルインターフェイスに使用されるIPSecプロファイルを見つける

1. トンネルインターフェイスで、Umbrellaヘッドエンドへのルートベース設定に使用されている

「crypto ipsec profile」を検索します（#は、Umbrellaへのトンネルインターフェイスに使用されるIDに置き換えます）。

```
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)#
```

画像11.png

2. トンネルIDが不明な場合は、次のコマンドを使用して、既存のトンネルインターフェイスを確認し、Umbrellaトンネルベースの設定に使用されているインターフェイスを判別できます。

```
show run interface tunnel
```

ステップ6:IPSecプロファイルから古いトラストポイントを削除する

1. トンネルのRSA認証を参照しているIPSecプロファイルからトラストポイントを削除します。この設定を検証するには、次のコマンドを使用します。

```
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
```

画像12.png

2. 次のコマンドを使用して、トラストポイントの削除に進みます。

```
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
```

画像13.png

3.トラストポイントがcrypto ipsec profileから削除されたことを確認します。

```
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
```

画像14.png

ステップ7：トンネルインターフェイスを新しい包括ヘッドエンドIPで更新する

1. トンネルインターフェイスの宛先を、.8で終端する新しいUmbrellaヘッドエンドIPアドレスに置き換えます。

- このコマンドを使用して、現在の宛先を確認し、新しいデータセンターのIPアドレス範囲のIPに置き換えることができます。このアドレス範囲については、Umbrellaのドキュメントを参照してください。

```
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)#
```

画像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
```

画像16.png

2. 次のコマンドで変更を確認します。

```
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
```

画像17.png

ステップ8：新しいトンネル設定が正常に確立されたことを確認します

1. 次のコマンドを使用して、更新されたヘッドエンドIPを使用し、PSK認証を使用して、Umbrellaへのトンネル接続が正しく再確立されたことを確認します。

```
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
```

画像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
```

画像19.png

ステップ9（オプション）：古いトンネルグループを削除します。

1. 以前のUmbrellaヘッドエンドIP範囲.2を指していた古いトンネルグループを削除します。

設定を削除する前に、次のコマンドを使用して正しいトンネルを特定できます。

```
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 *****
```

画像20.png

2. 次のコマンドを使用して、古いトンネルグループの参照を削除します。

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

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

画像21.png

ステップ10（オプション）：古いトラストポイントを削除する

1. 次のコマンドを使用して、以前にUmbrellaトンネルベースの設定で使用したトラストポイントの参照をすべて削除します。

```
sh run crypto ipsec
```

トラストポイントに使用するフレンドリ名は、「crypto ipsec profile」を確認すると表示できます。

```
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
```

画像22.png

2. このコマンドを実行すると、トラストポイントの設定を確認できます。フレンドリ名が、crypto ipsec profileコマンドで使用されている設定と一致していることを確認します。

```
sh run crypto ca trustpoint
```

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

画像23.png

3. 証明書の詳細を取得するには、次のコマンドを使用します。

```
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:
```

画像24.png

4. 次のコマンドを使用して、トラストポイントを削除します。

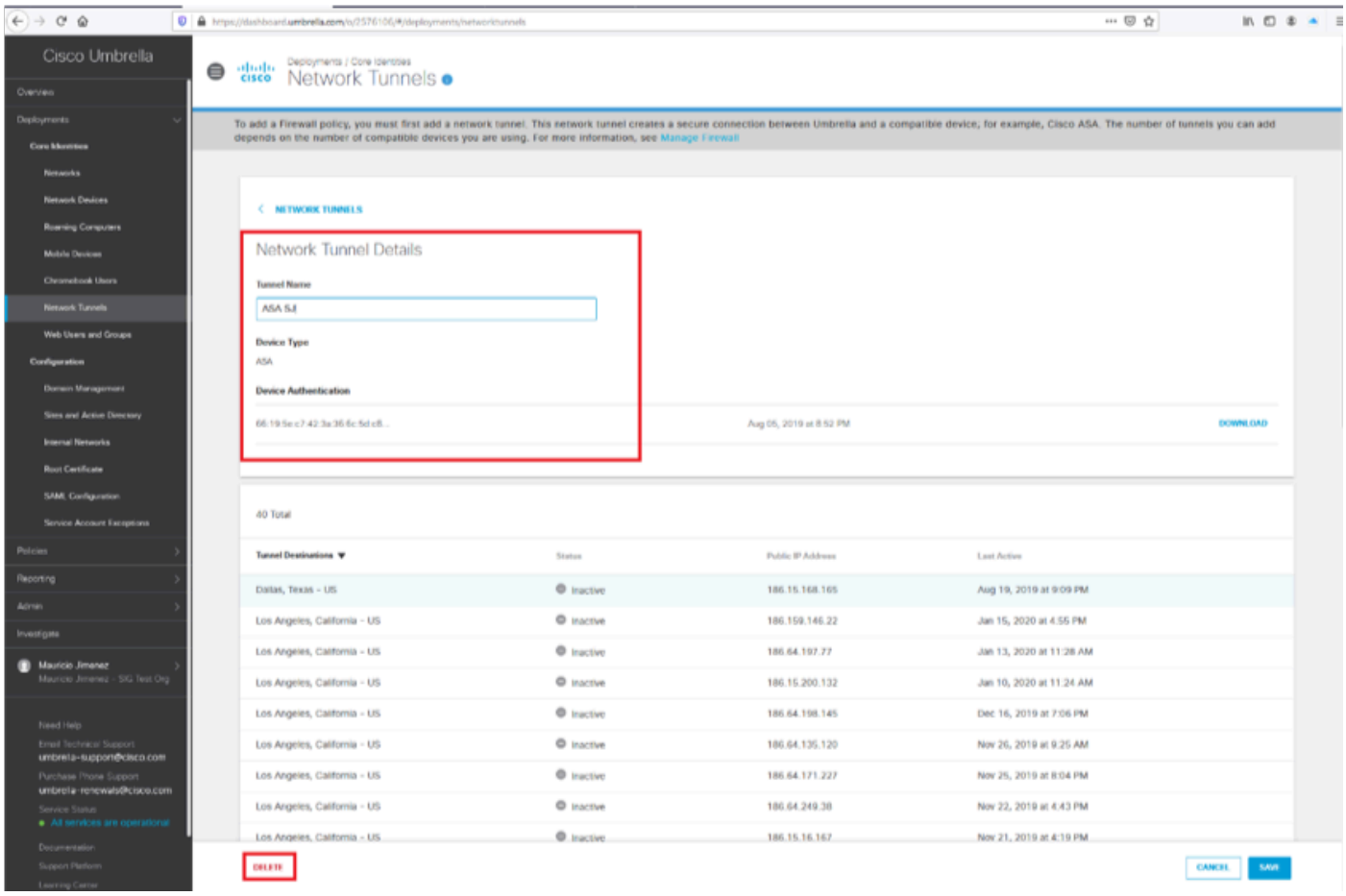
```
no crypto ca trustpoint <trustpoint-name>
```

```
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)#
```

画像25.png

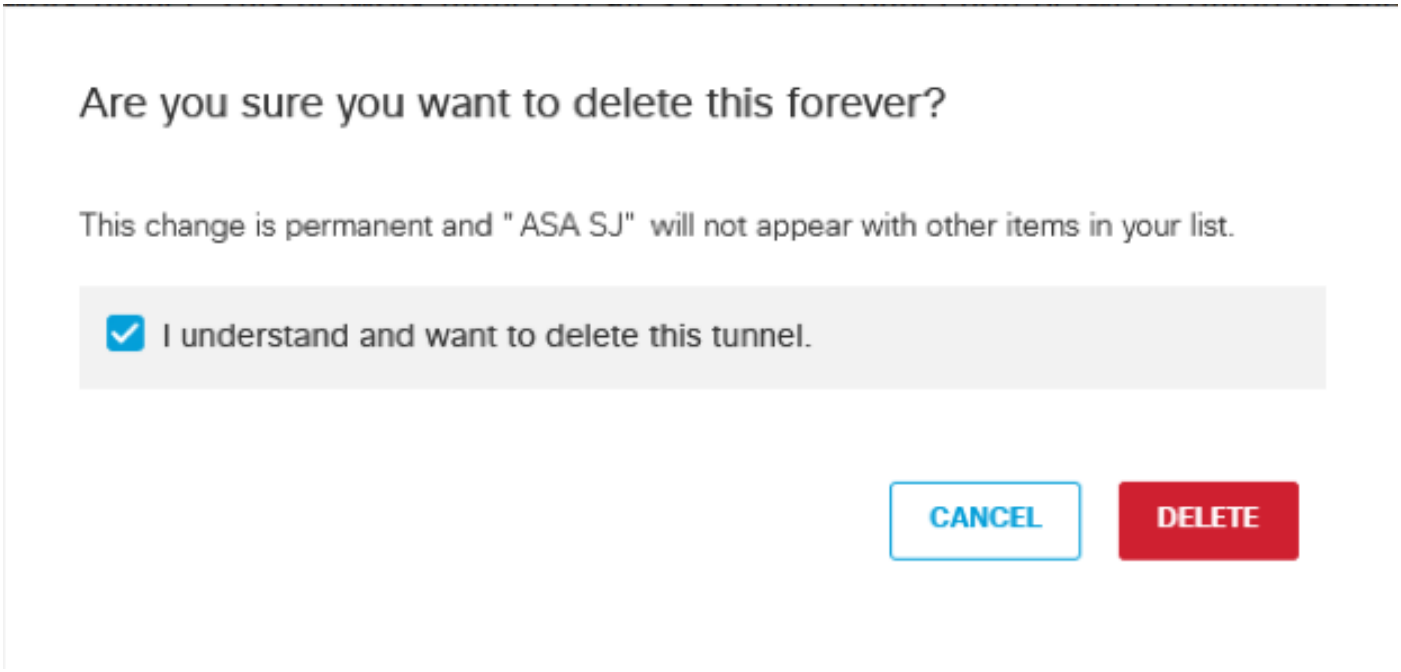
ステップ11（オプション）：古いネットワークトンネルの削除

1. Umbrellaダッシュボードから古いネットワークトンネルを削除します。Network Tunnel Detailsに移動してDeleteを選択します。



画像26.png

2. ポップアップでI understand and want to delete this tunnelオプションを選択して削除を確認し、Deleteを選択します。



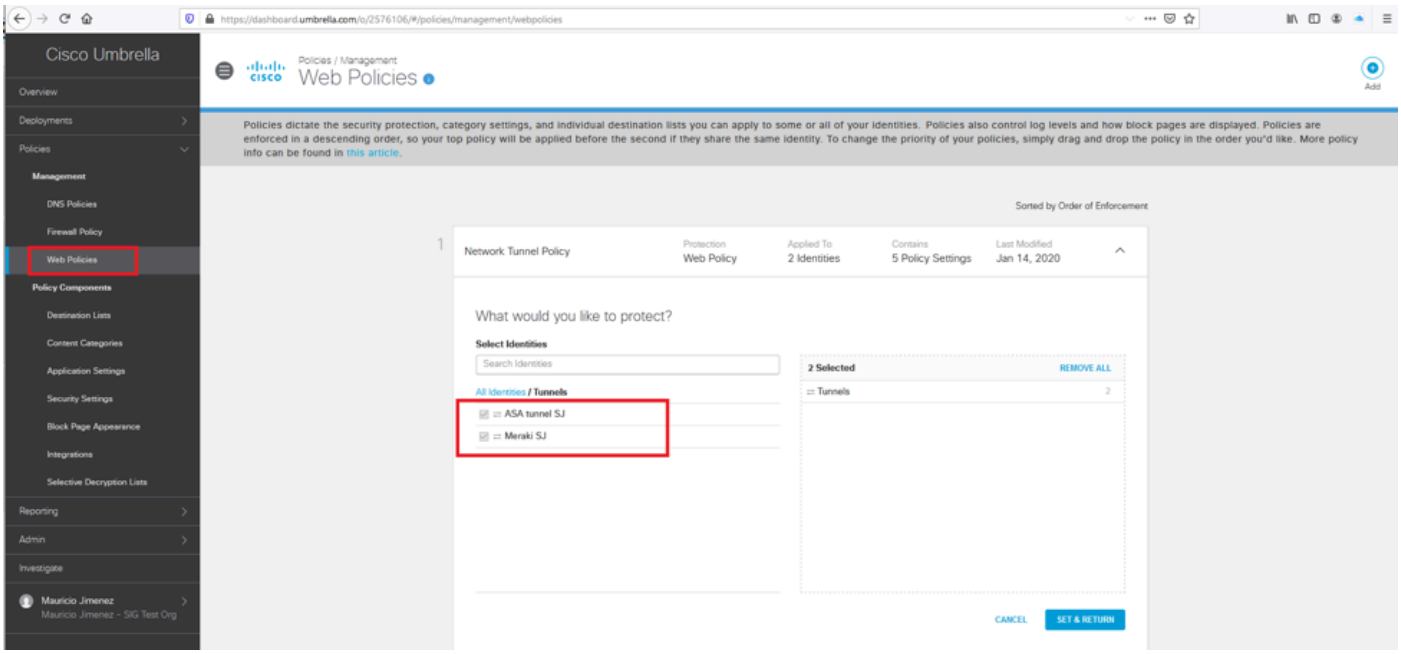
画像27.png

手順12：新しいトンネルIDを使用してWebポリシーを更新する

新しいネットワークトンネルを使用して、WebポリシーのIDが更新されていることを確認します。

1. Umbrellaダッシュボードで、Policies > Management > Web Policiesの順に移動します。

2. 「トンネル」セクションを確認し、Webポリシーが新しいネットワークトンネルで更新されたIDを持っていることを確認します。



画像28.png

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。