# Change Cloud Delivered Firewall Tunnel from RSA to PSK Authentication

## Contents



## Introduction

This document describes the steps to reconfigure Cloud Delivered Firewall Tunnel's authentication mechanism from RSA to PSK on Cisco ASA.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on Cisco Umbrella.

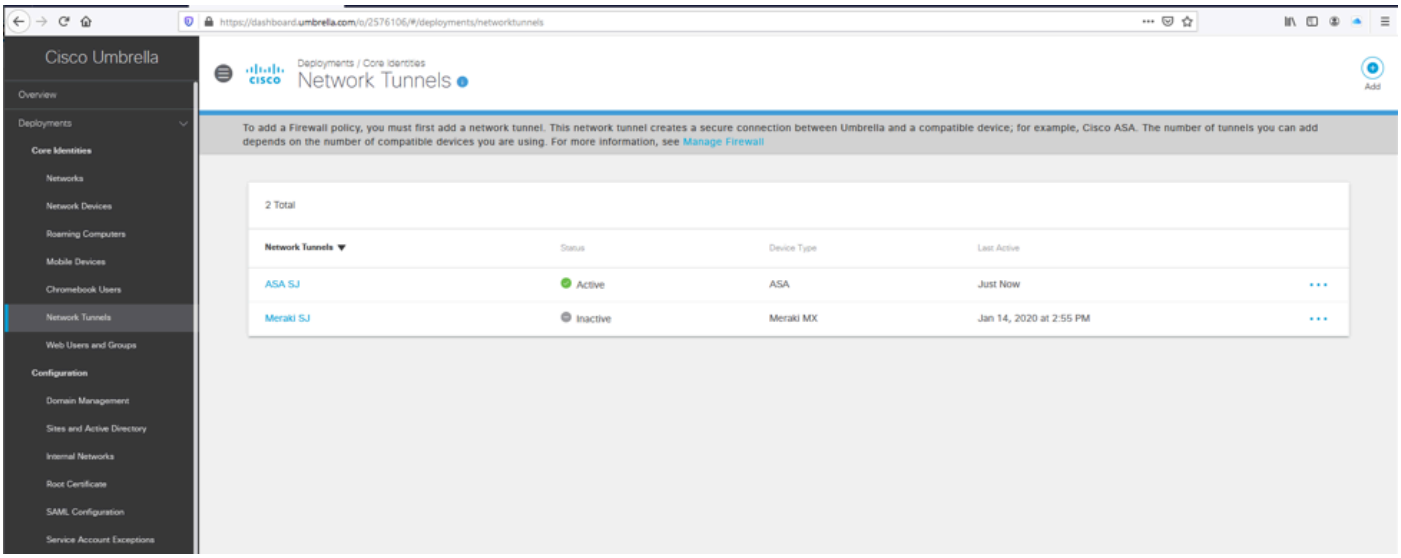
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Step 1: Verify An Existing Tunnel Using RSA authentication

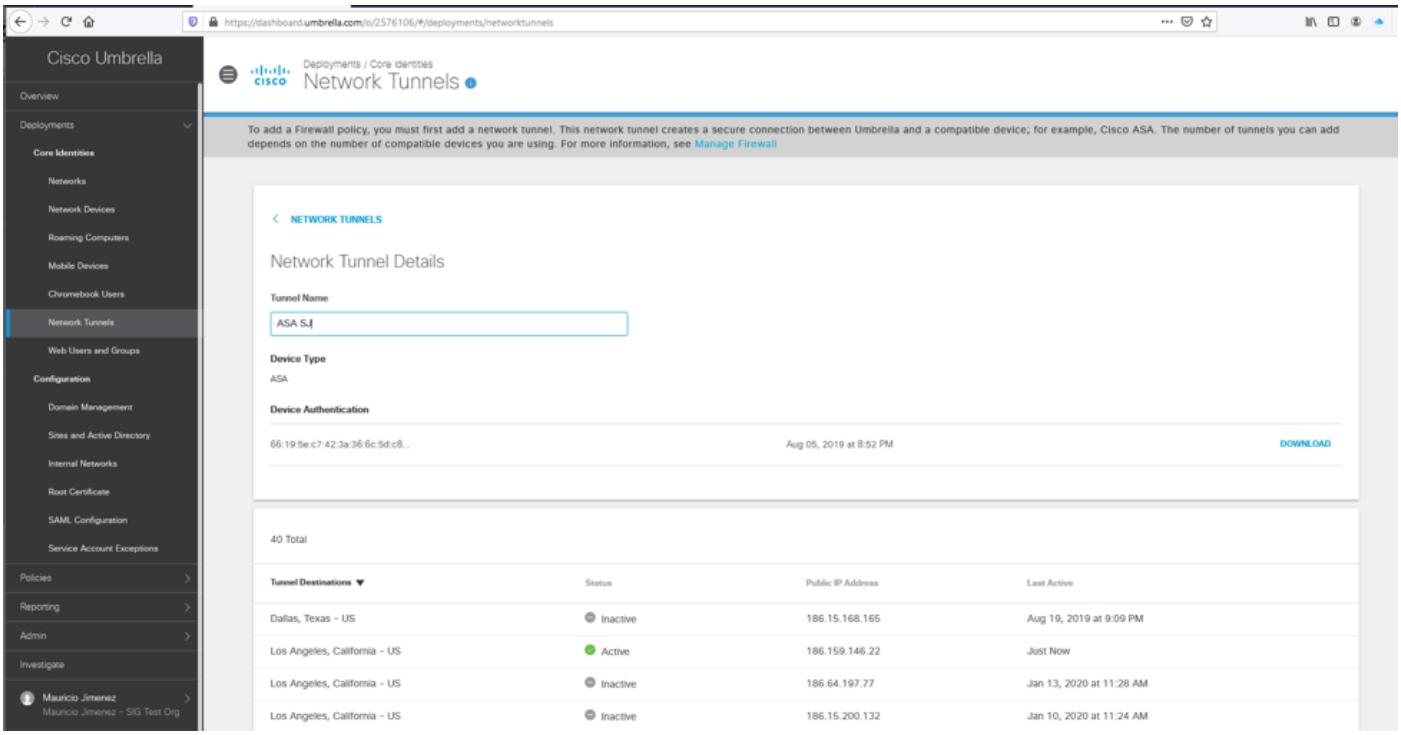
Verify that you have an existing tunnel using RSA authentication and that the status of the tunnel in the

ASA is showing connected with this authentication type.

1. In the Umbrella dashboard, find the Network tunnel with the ASA showing a Device authentication finger print.




*Picture1.png*




*Picture2.png*

2. In the Cisco ASA, you can run these commands to verify the authentication type and headend IP being used for the tunnel.

```
show crypto ikev2 sa
```

and

`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#
```

*Picture3.png*

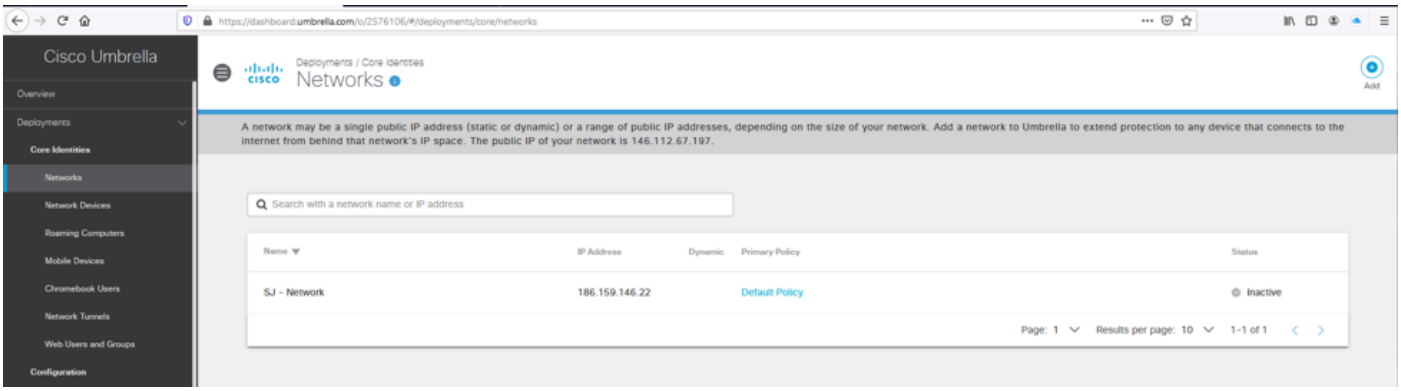
```
ASA-SJ# sh crypto ipsec sa
interface: vti
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: 186.159.
146.22

      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 --->
```

*Picture4.png*

# Step 2: Register ASA's Public IP

1. Make sure you have your public IP used by the ASA outside interface registered as a **Network** in the Umbrella dashboard.

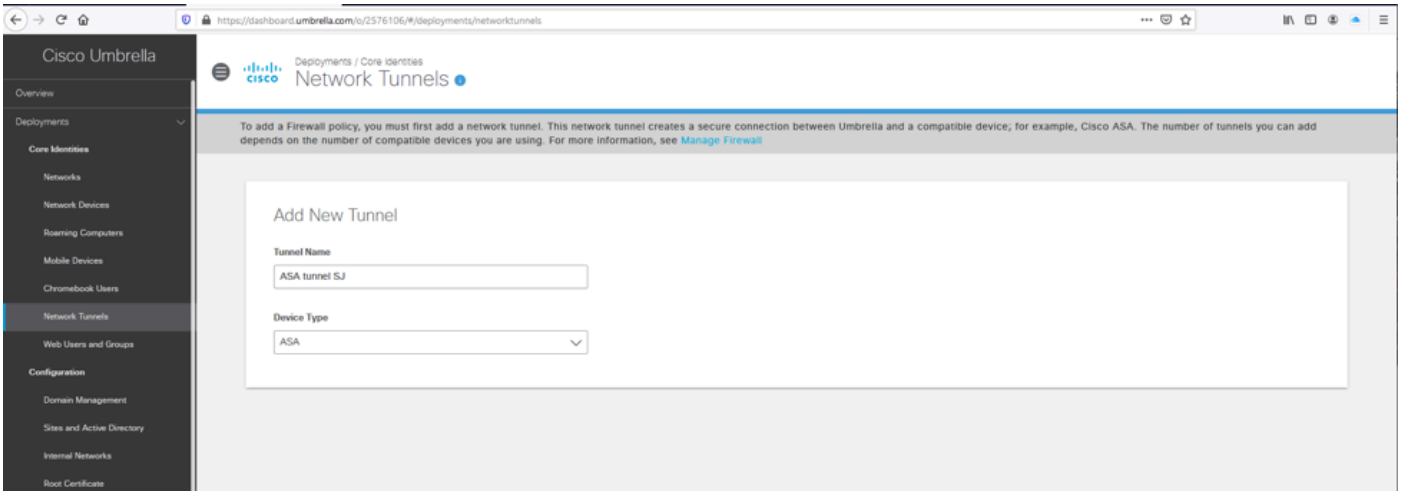
2. If the **Network** does not exist, then proceed to add it and confirm the public IP used by the ASA interface. The **Network** object used for this tunnel must be defined with a /32 subnet mask.




*Picture5.png*

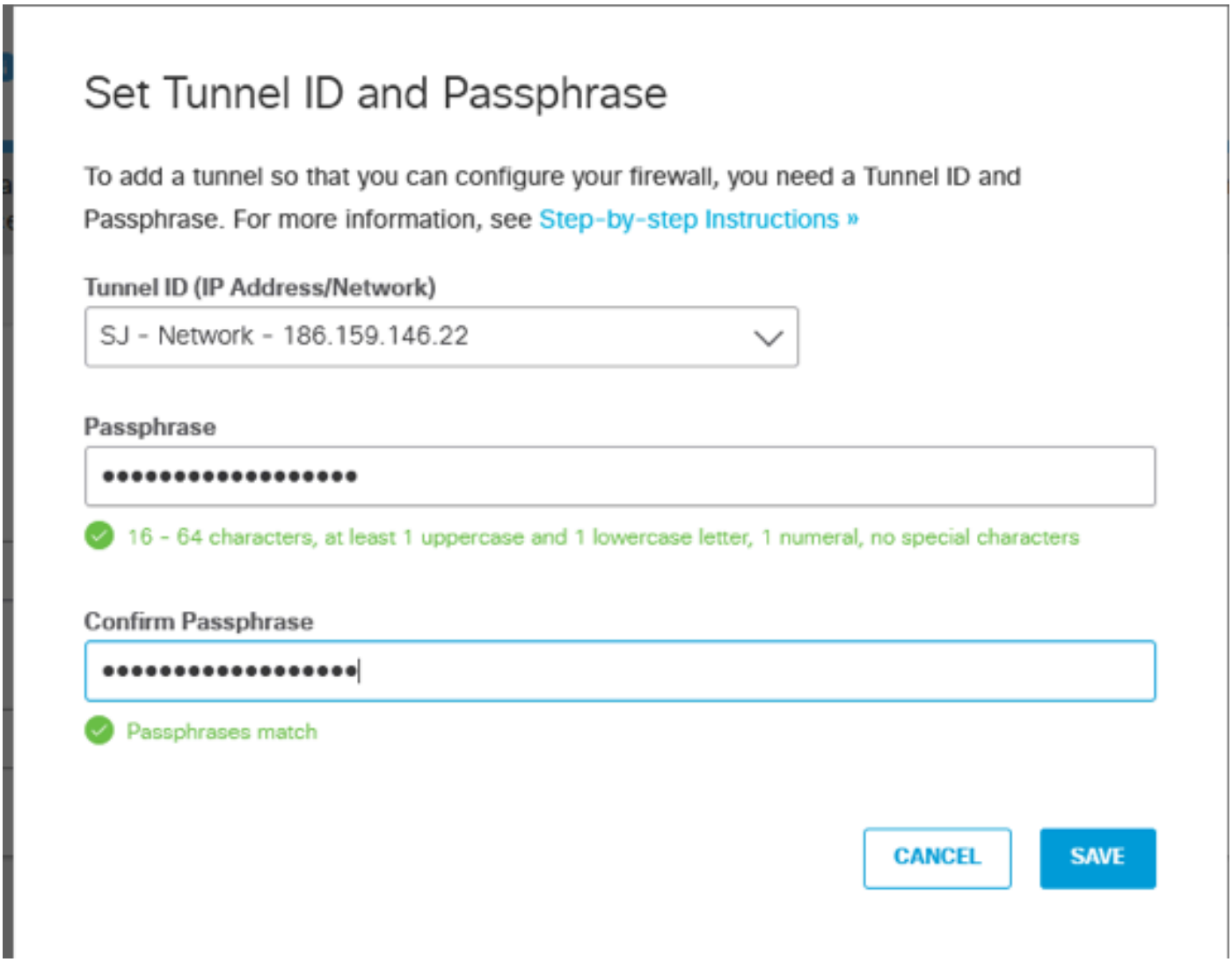
# Step 3: Create New ASA Tunnel

1. In the Umbrella dashboard under **Deployments/Network Tunnels**, create a new tunnel by selecting the **Add** option.

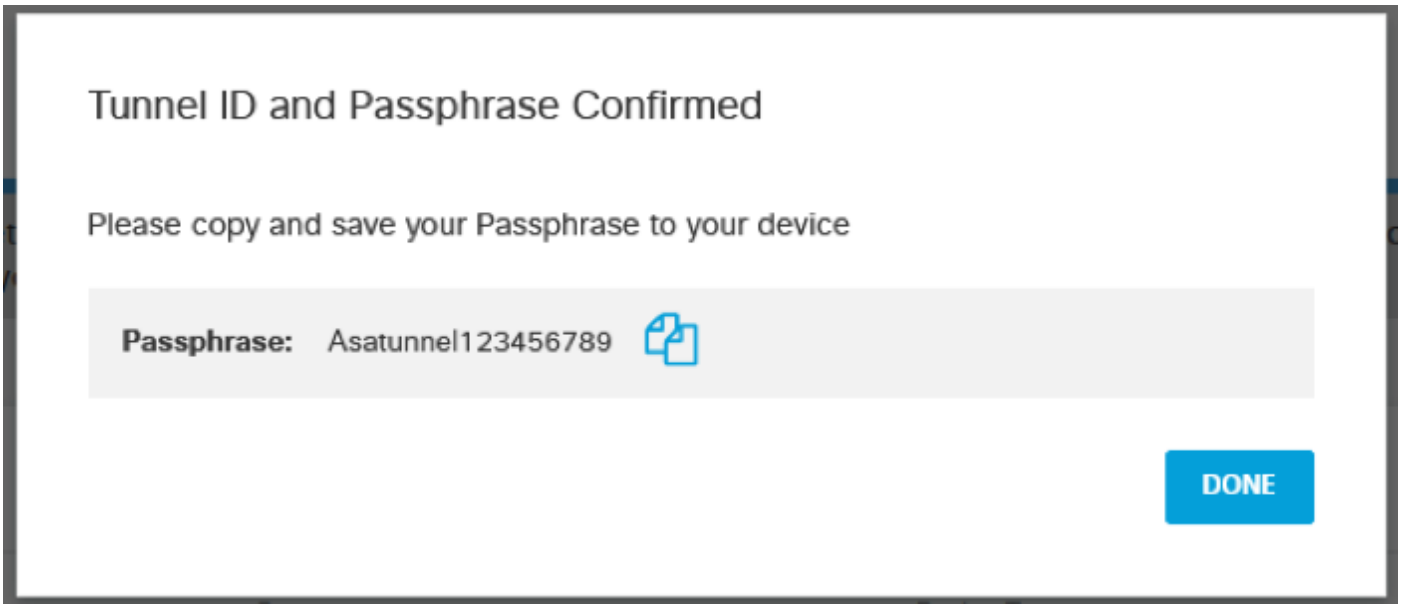



*Picture6.png*

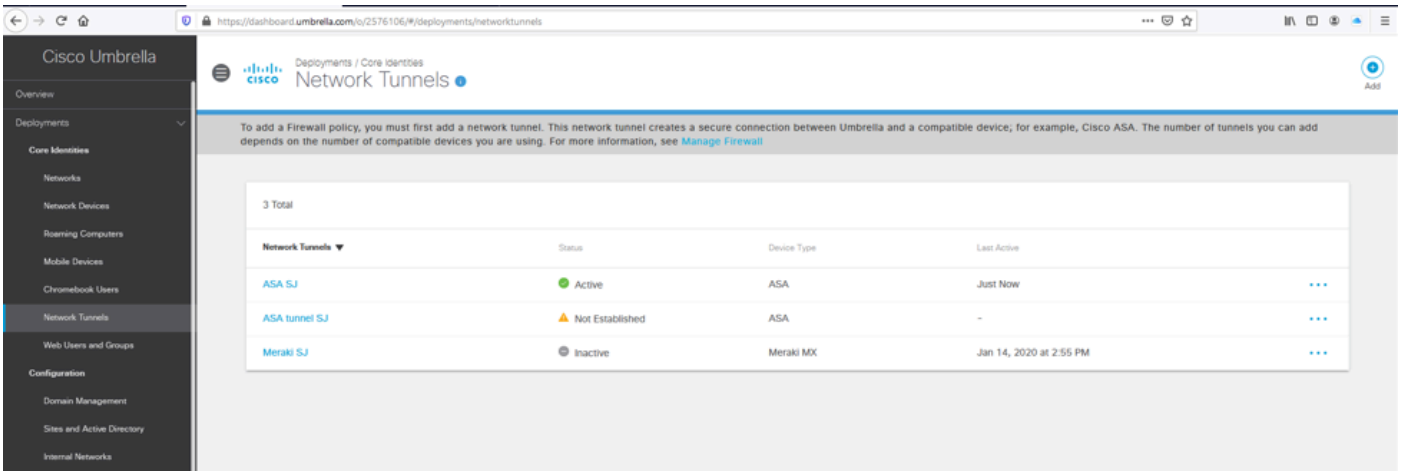
2. Select the **Tunnel ID** based on the Network that matches with the public IP of your ASA outside interface and setup a passphrase for the PSK authentication.




*Picture7.png*




*Picture8.png*




*Picture9.png*

# Step 4: Create New Tunnel-Group

1. On the ASA, create a new tunnel-group using the new headend IP for Umbrella and specify the **passphrase** define in the Umbrella dashboard for the PSK authentication.

2. The updated list of Umbrella data centers and IPs for the headends can be found in the Umbrella documentation.

```
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 *****
```

*Picture10.png*

# Step 5: Locate the IPSec Profile Used for the Tunnel Interface

1. Search for the "**crypto ipsec profile**" that is being used in the tunnel interface for the route-based configuration to Umbrella headend (# is replace with the ID used for the tunnel interface to 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. If you are not sure about the tunnel ID, then you can use this command to verify existing tunnel interfaces and determine which is the one used for the Umbrella tunnel-based configuration:

```
show run interface tunnel
```

## Step 6: Remove Old Trustpoint from IPSec Profile

1. Remove the **trustpoint** from your **IPSec profile** which reference the RSA authentication for the tunnel. You can verify the configuration by using this command:

```
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
```

*Picture12.png*

2. Proceed to remove the **trustpoint** with these commands:

```
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
```

*Picture13.png*

3. Confirm that the **trustpoint** was removed from the **crypto ipsec profile**:

```
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
```

*Picture14.png*

# Step 7: Update Tunnel Interface with New Umbrella Headend IP

1. Replace the destination of the tunnel interface to the new Umbrella headend IP address terminating in **.8**.

- You can use this  command to verify the current destination so it is replaced with the IP from the new Data Center IP address ranges, which can be found in the Umbrella documentation:

```
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)#
```

*Picture15.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
```

*Picture16.png*

2. Confirm the change with the command:

```
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
```

*Picture17.png*

# Step 8: Confirm New Tunnel Configuration Successfully Establishes

1. Confirm that the tunnel connection to Umbrella was reestablished correctly with the updated headend IP and using the PSK authentication with this command:

```
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
```

*Picture18.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
```

*Picture19.png*

# Step 9 (Optional): Remove the Old Tunnel-Group

1. Remove the old tunnel-group that was pointing to the previous Umbrella headend IP range **.2**.

You can use this command to identify the correct tunnel before removing the 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 *****
```

*Picture20.png*

2. Remove any reference of the old tunnel group using this command:

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

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

*Picture21.png*

# Step 10 (Optional): Remove Old Trustpoint

1. Remove any reference of the trustpoint used previously with the Umbrella tunnel-based configuration with this command:

```
sh run crypto ipsec
```

The friendly name used for the trustpoint can be found when you review the “crypto ipsec profile”:

```
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
```

*Picture22.png*

2. You can run this command to confirm the trustpoint configuration. Make sure the friendly name matches with the configuration used in the crypto ipsec profile command:

```
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
```

*Picture23.png*

3. To get more details about the certificate, use the command:

```
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:
```

*Picture24.png*

4. Remove the **trustpoint** with the command:

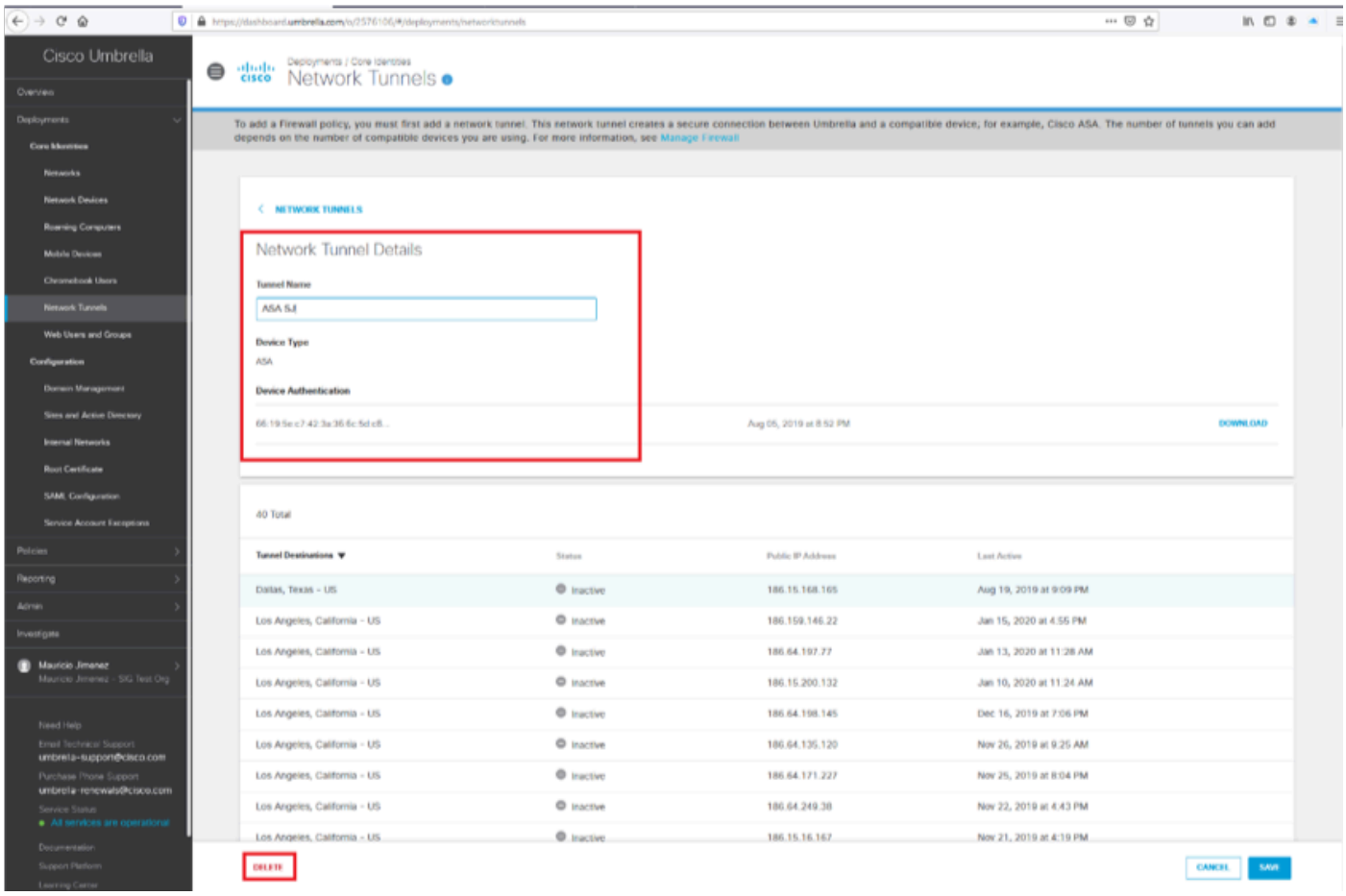
```
no crypto ca trustpoint <trustpoint-name>
```

```
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)#
```

*Picture25.png*

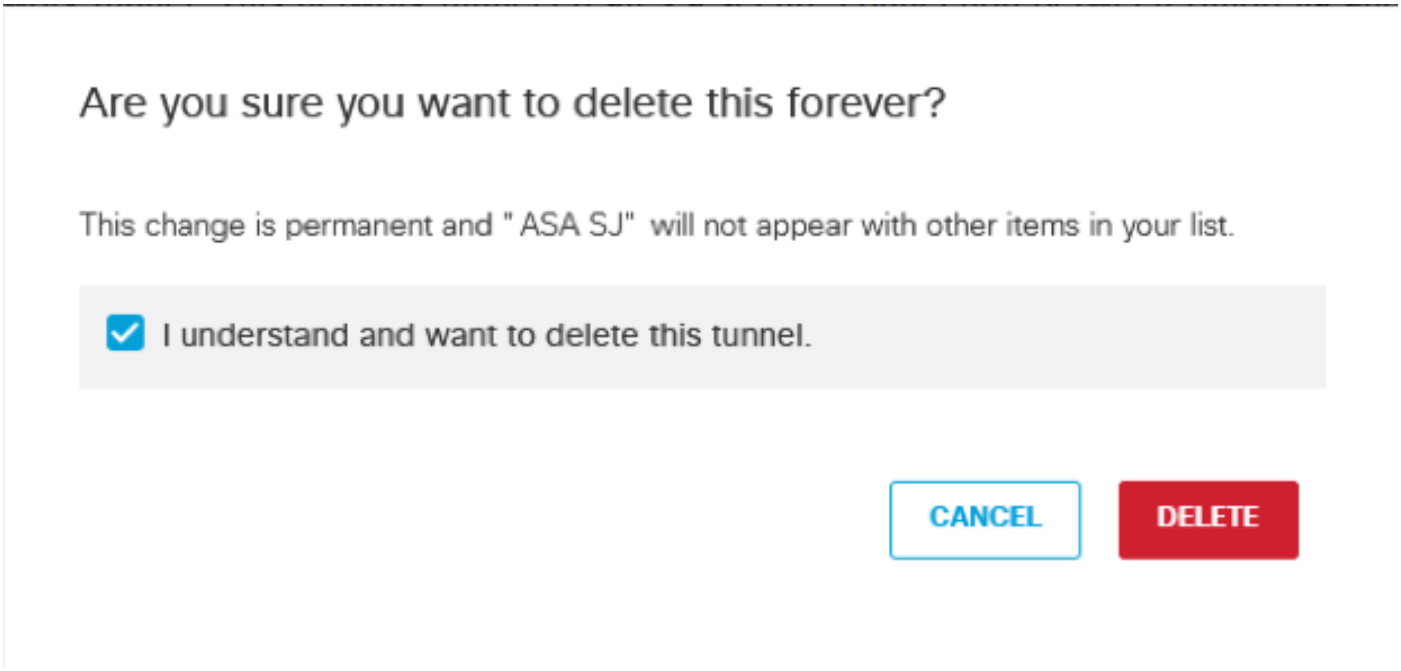
# Step 11 (Optional): Delete Old Network Tunnel

1. Delete the old network tunnel from the Umbrella dashboard by navigating to **Network Tunnel Details** and selecting **Delete**.




*Picture26.png*

2. Confirm you deletion by selecting the **I understand and want to delete this tunnel** option in the pop-up, then select **Delete**.



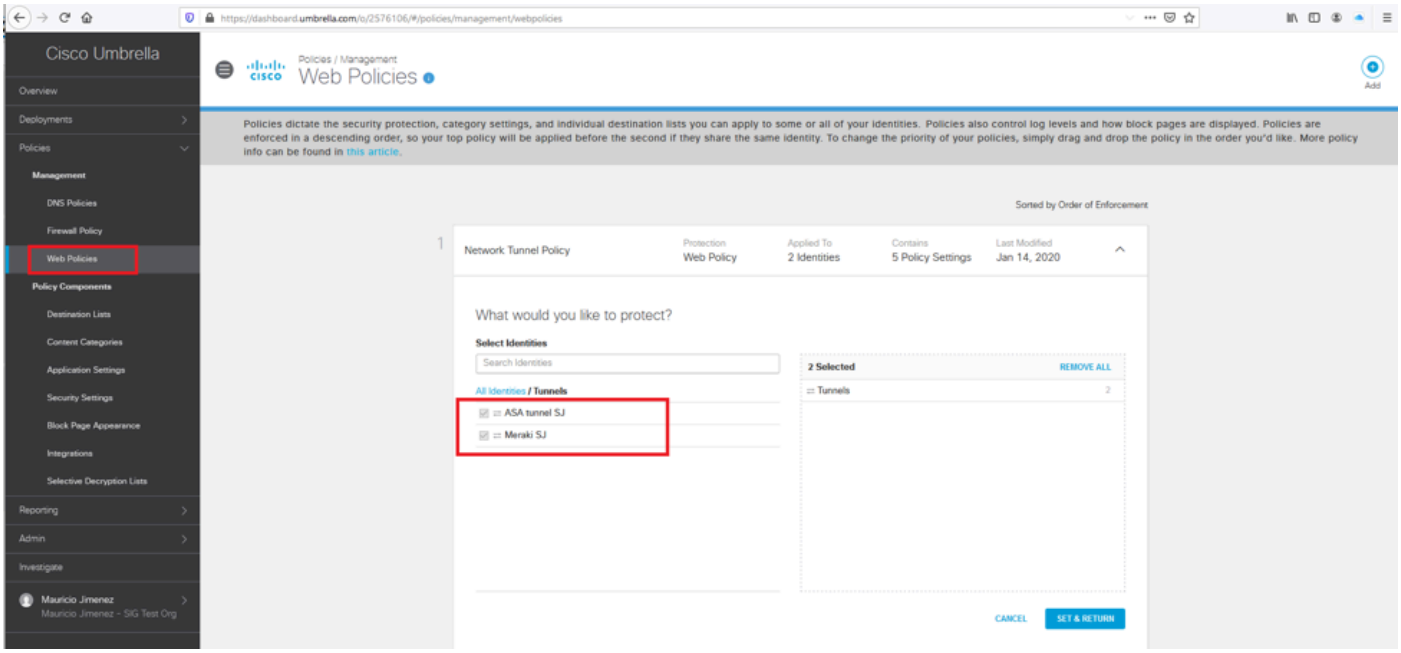

*Picture27.png*

# Step 12: Update Web Policies with New Tunnel Identity

Confirm your web policies have the updated identity with the new network tunnel:

1. In the Umbrella dashboard, navigate to **Policies > Management > Web Policies**.

2. Review the **Tunnels** section and confirm that your web policies have the updated identity with the new network tunnel.




*Picture28.png*