Cambio del túnel de firewall suministrado en la nube de RSA a autenticación PSK

Contenido

Introducción

Este documento describe los pasos para reconfigurar el mecanismo de autenticación del túnel de firewall entregado en la nube de RSA a PSK en Cisco ASA.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Paso 1: Verificación de un Túnel Existente Usando la Autenticación RSA

Verifique que tiene un túnel existente que utiliza la autenticación RSA y que el estado del túnel en el ASA se muestra conectado con este tipo de autenticación.

1. En el panel de Umbrella, busque el túnel Network con el ASA que muestra una huella digital de autenticación de dispositivo.

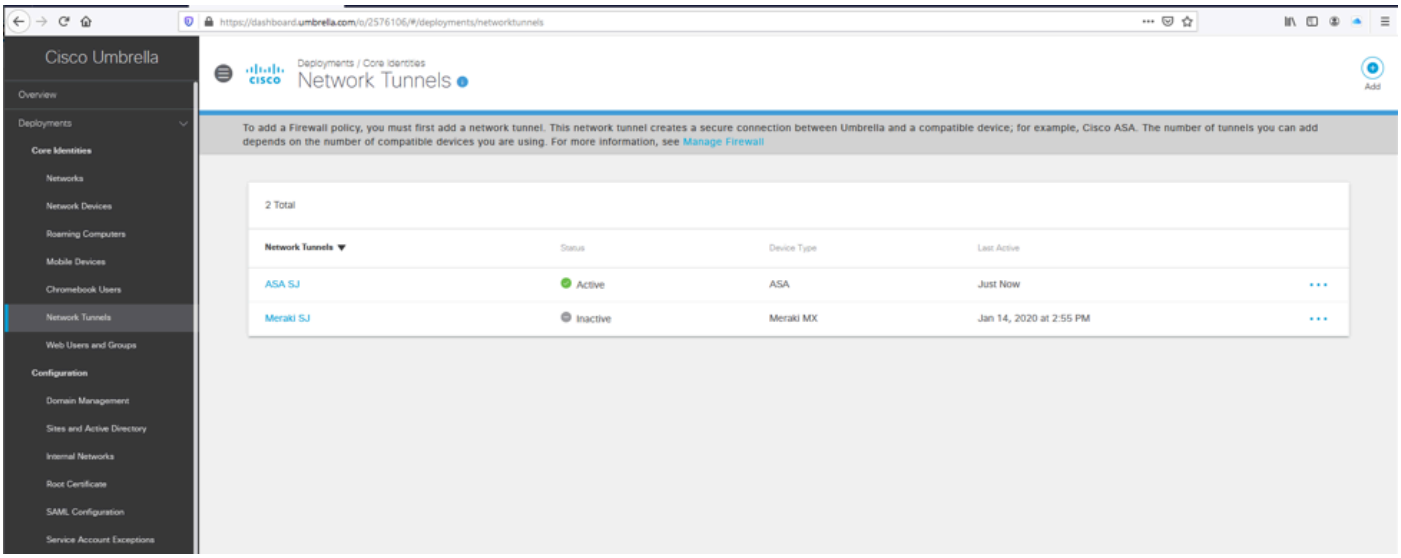

Imagen1.png

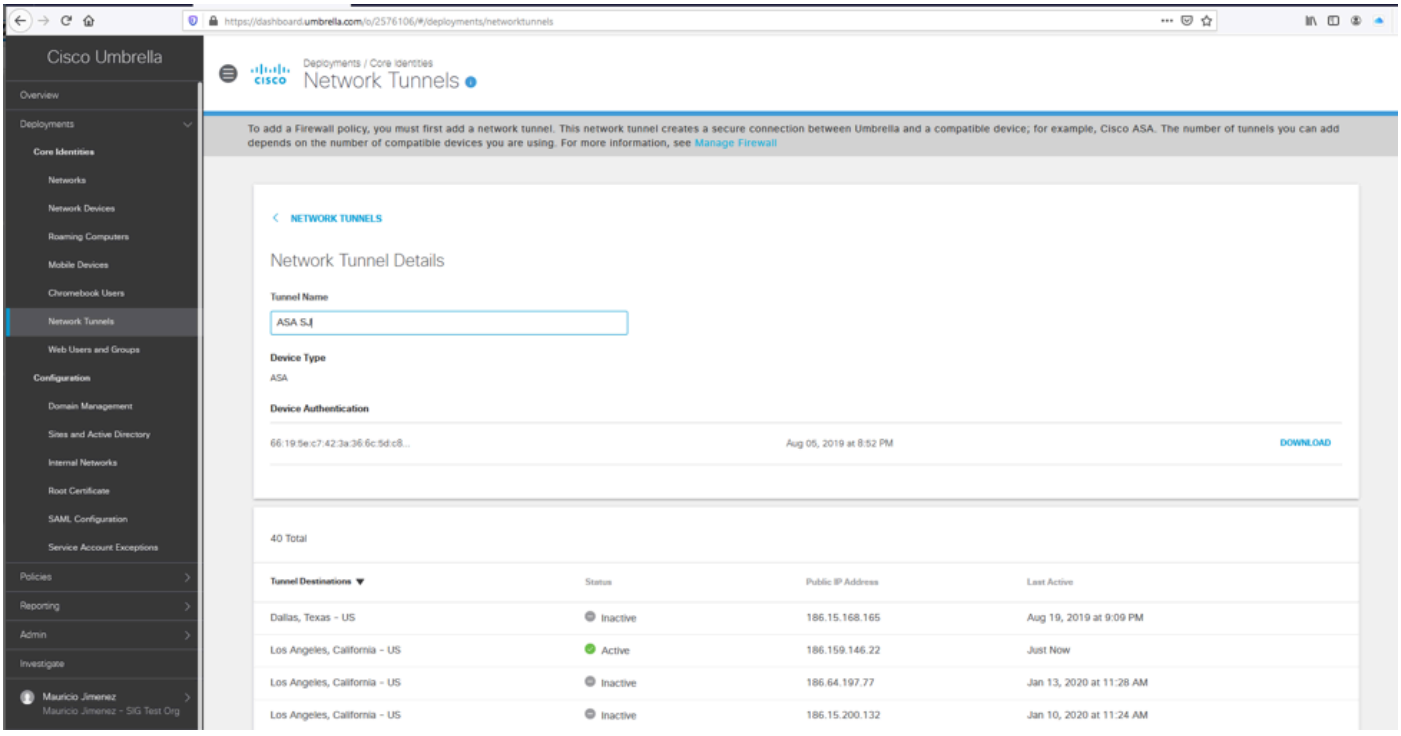

Imagen2.png

2. En Cisco ASA, puede ejecutar estos comandos para verificar el tipo de autenticación y la IP de

cabecera que se utiliza para el túnel.

```
show crypto ikev2 sa
```

y

```
show crypto ipsec sa
```

Imagen3.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 --->
```

Imagen4.png

Paso 2: Registrar IP pública de ASA

1. Asegúrese de que su IP pública utilizada por la interfaz exterior de ASA esté registrada como Red en el panel de Umbrella.

2. Si la Red no existe, entonces proceda a agregarla y confirme la IP pública utilizada por la interfaz ASA. El objeto Network utilizado para este túnel debe definirse con una máscara de subred /32.

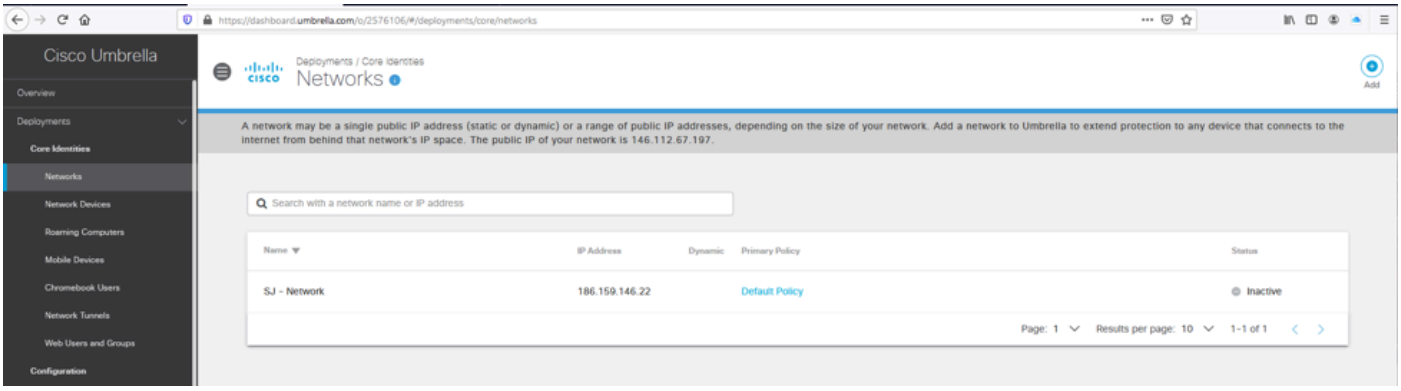

Imagen5.png

Paso 3: Crear nuevo túnel ASA

1. En el panel de control general, en Despliegues/Túneles de Red, cree un nuevo túnel seleccionando la opción Agregar.

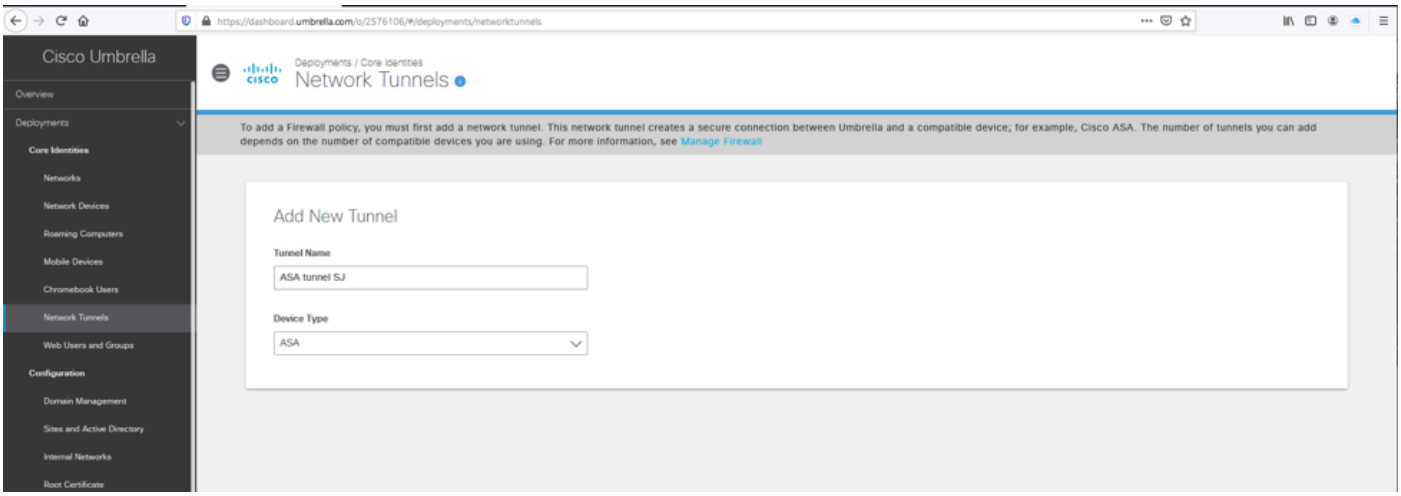

Imagen6.png

2. Seleccione el ID de túnel basado en la red que coincida con la IP pública de su interfaz exterior ASA y configure una frase de contraseña para la autenticación PSK.

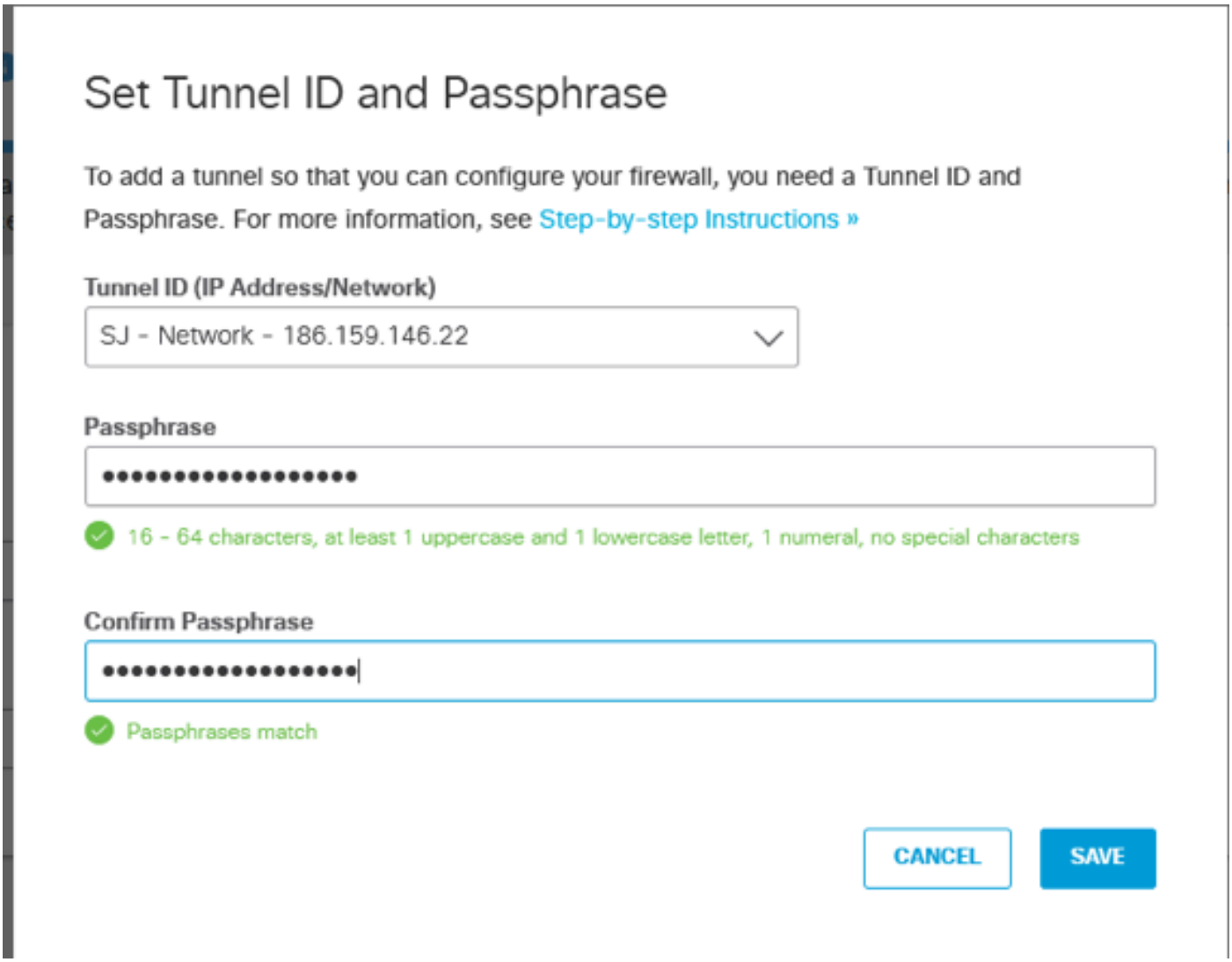

Imagen7.png

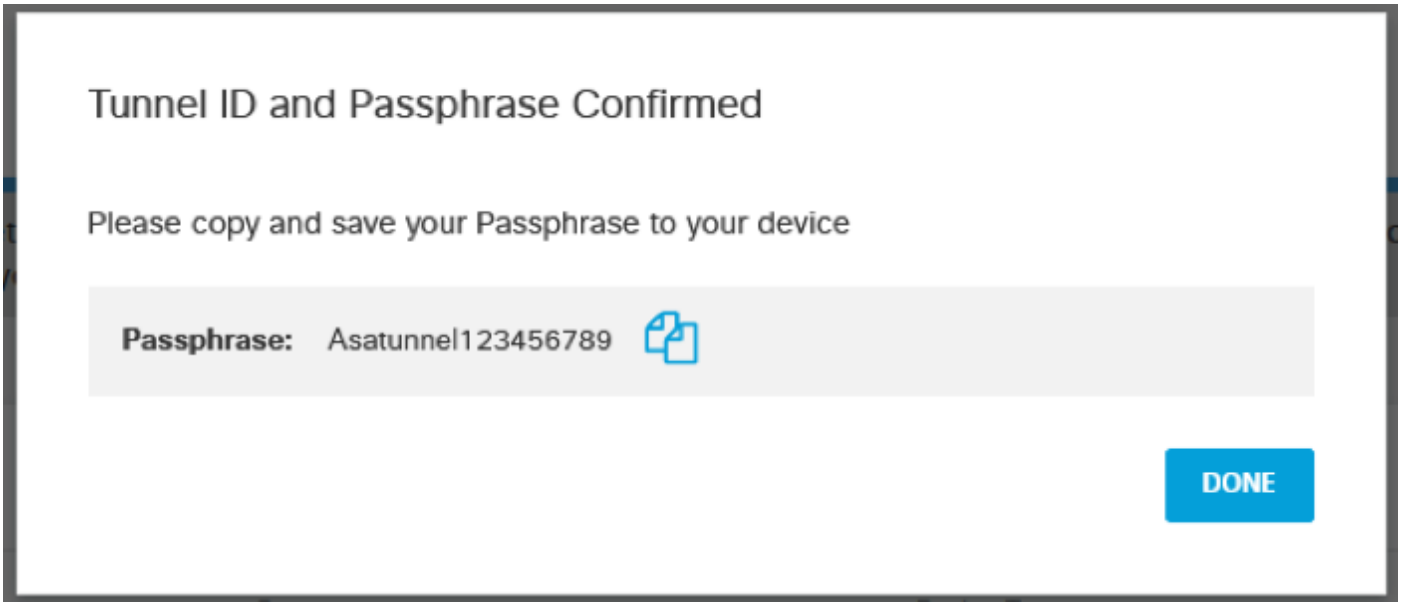

Imagen8.png

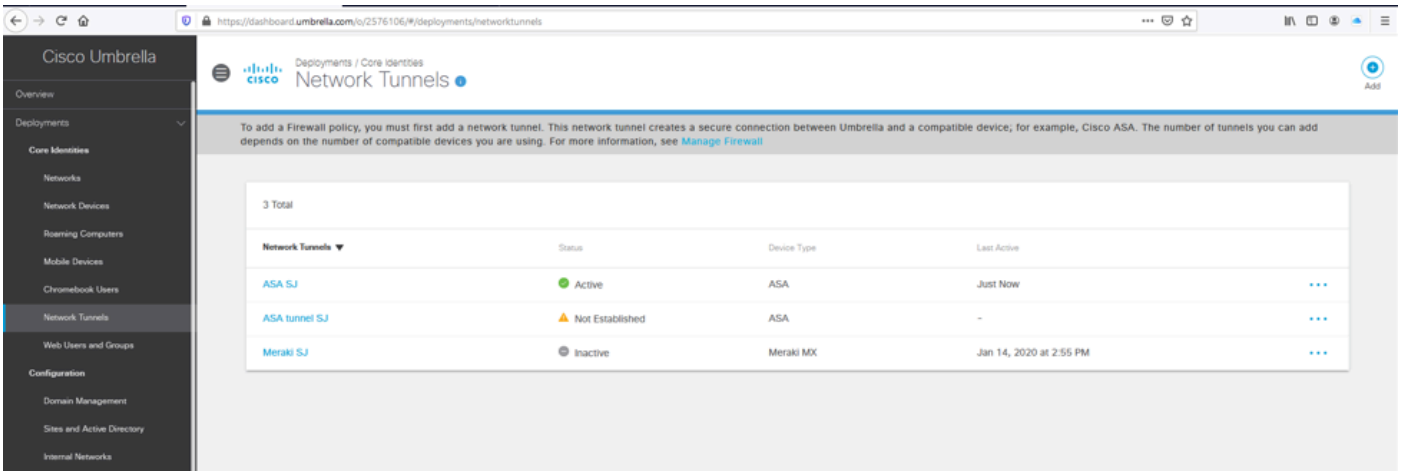

Imagen9.png

Paso 4: Crear nuevo grupo de túnel

1. En ASA, cree un nuevo grupo de túnel utilizando la nueva IP de cabecera para Umbrella y especifique la frase de contraseña definida en el panel de Umbrella para la autenticación PSK.

2. En la documentación de Umbrella puede encontrarse la lista actualizada de los centros de datos y direcciones IP de Umbrella para las cabeceras.

```
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 *****
```

Imagen10.png

Paso 5: Localice el perfil IPSec utilizado para la interfaz de túnel

1. Busque el "perfil crypto ipsec" que se está utilizando en la interfaz de túnel para la configuración basada en ruta a Umbrella headend (el nº se reemplaza con el ID utilizado para la interfaz de túnel a 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)#
```

Imagen11.png

2. Si no está seguro del ID de túnel, puede utilizar este comando para verificar las interfaces de túnel existentes y determinar cuál es la utilizada para la configuración basada en túnel de Umbrella:

```
show run interface tunnel
```

Paso 6: Eliminar punto de confianza antiguo del perfil IPSec

1. Quite el punto de confianza del perfil IPSec que hace referencia a la autenticación RSA para el túnel. Puede verificar la configuración mediante este comando:

```
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
```

Imagen12.png

2. Proceda a eliminar el trustpoint con estos comandos:

```
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
```

Imagen13.png

3. Confirme que el punto de confianza fue eliminado del perfil crypto ipsec:

```
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
```

Imagen14.png

Paso 7: Actualización de la interfaz de túnel con nueva IP de cabecera Umbrella

1. Sustituya el destino de la interfaz de túnel por la nueva dirección IP de cabecera de Umbrella que termine en .8.

- Puede utilizar este comando para verificar el destino actual para que se reemplace por la IP de los nuevos rangos de direcciones IP del Data Center, que se pueden encontrar en la documentación de Umbrella:

```
show run interface tunnel
```

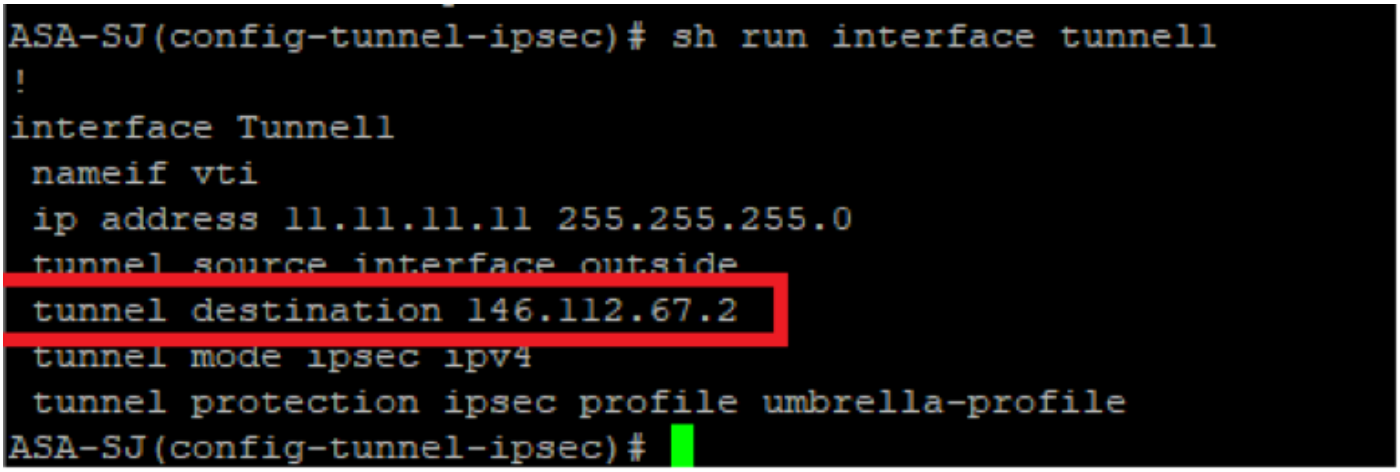

Imagen15.png

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

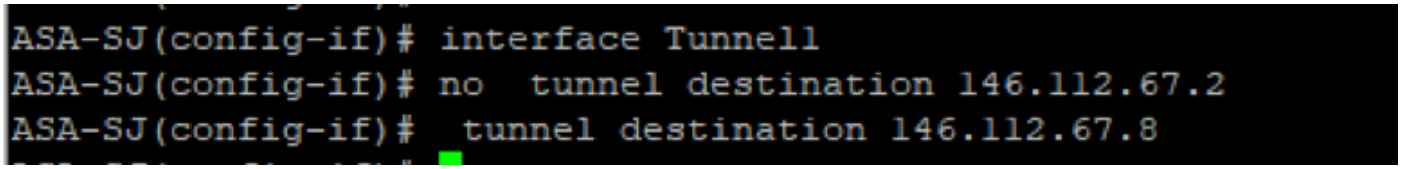

Imagen16.png

2. Confirme el cambio con el comando:

```
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
```

Imagen17.png

Paso 8: Confirmar establecimiento correcto de la nueva configuración del túnel

1. Confirme que la conexión de túnel a Umbrella se restableció correctamente con la IP de cabecera actualizada y utilizando la autenticación PSK con este comando:

```
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
```

Imagen18.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
```

Imagen19.png

Paso 9 (opcional): Elimine el grupo de túnel antiguo

1. Elimine el grupo de túnel antiguo que apuntaba al intervalo IP de cabecera Umbrella anterior .2.

Puede utilizar este comando para identificar el túnel correcto antes de eliminar la configuración:

```
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 *****
```

Imagen20.png

2. Elimine cualquier referencia del antiguo grupo de túnel mediante este comando:

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

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

Imagen21.png

Paso 10 (opcional): Eliminar punto de confianza antiguo

1. Elimine cualquier referencia del punto de confianza utilizado anteriormente con la configuración basada en el túnel Umbrella con este comando:

```
sh run crypto ipsec
```

El nombre descriptivo utilizado para el punto de confianza se puede encontrar al revisar el "perfil 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
```

Imagen22.png

2. Puede ejecutar este comando para confirmar la configuración del punto de confianza. Asegúrese de que el nombre descriptivo coincida con la configuración utilizada en el comando 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
```

Imagen23.png

3. Para obtener más detalles sobre el certificado, utilice el comando:

```
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:
```

Imagen24.png

4. Quite el punto de confianza con el comando:

```
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)#
```

Imagen25.png

Paso 11 (opcional): Eliminar túnel de red antiguo

1. Elimine el túnel de red antiguo del panel de control de Umbrella accediendo a Detalles del Túnel de Red y seleccionando Suprimir.

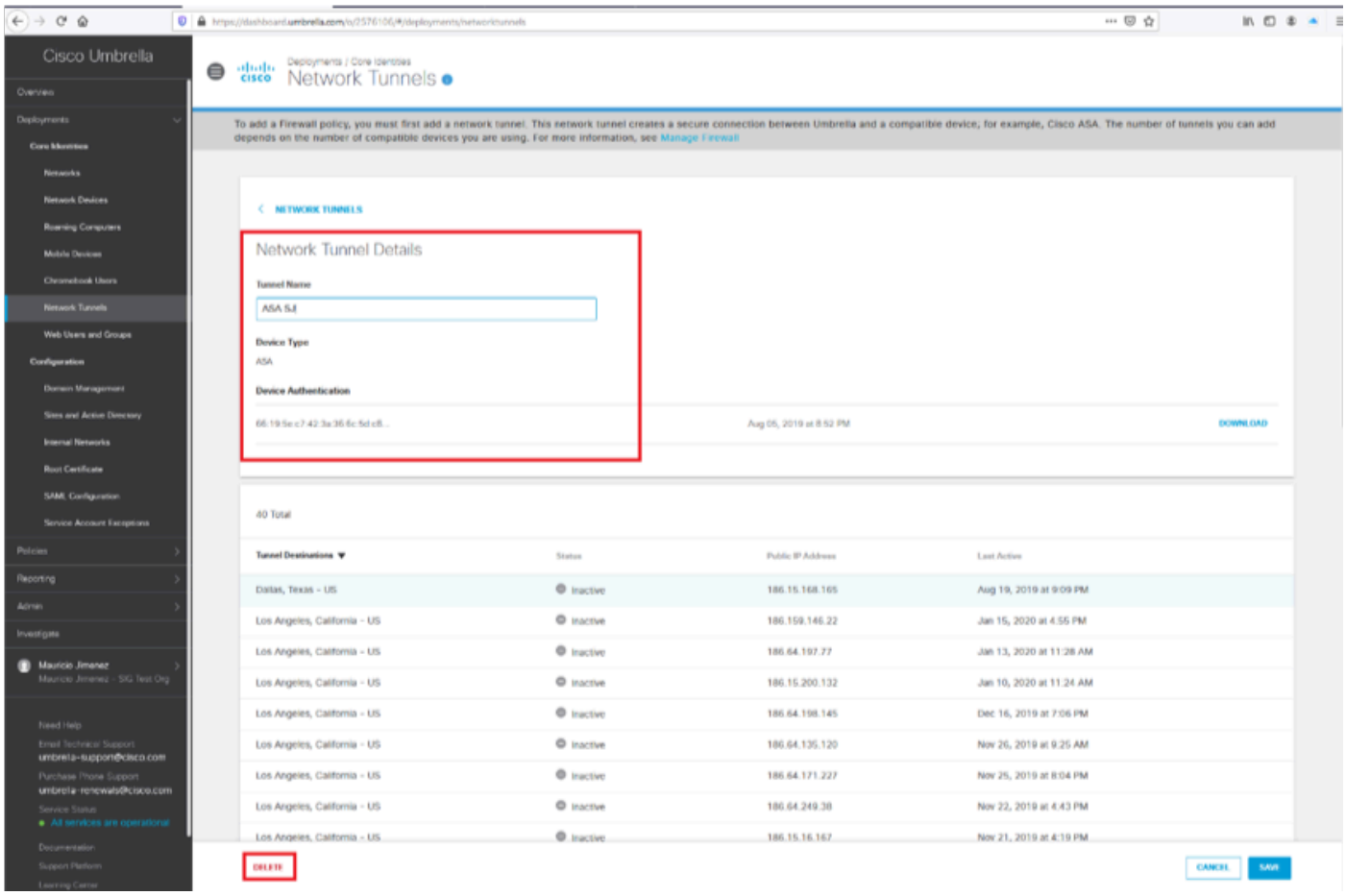

Imagen26.png

2. Confirme la supresión seleccionando la opción Comprendo y quiero suprimir este túnel en la ventana emergente y, a continuación, seleccione Suprimir.

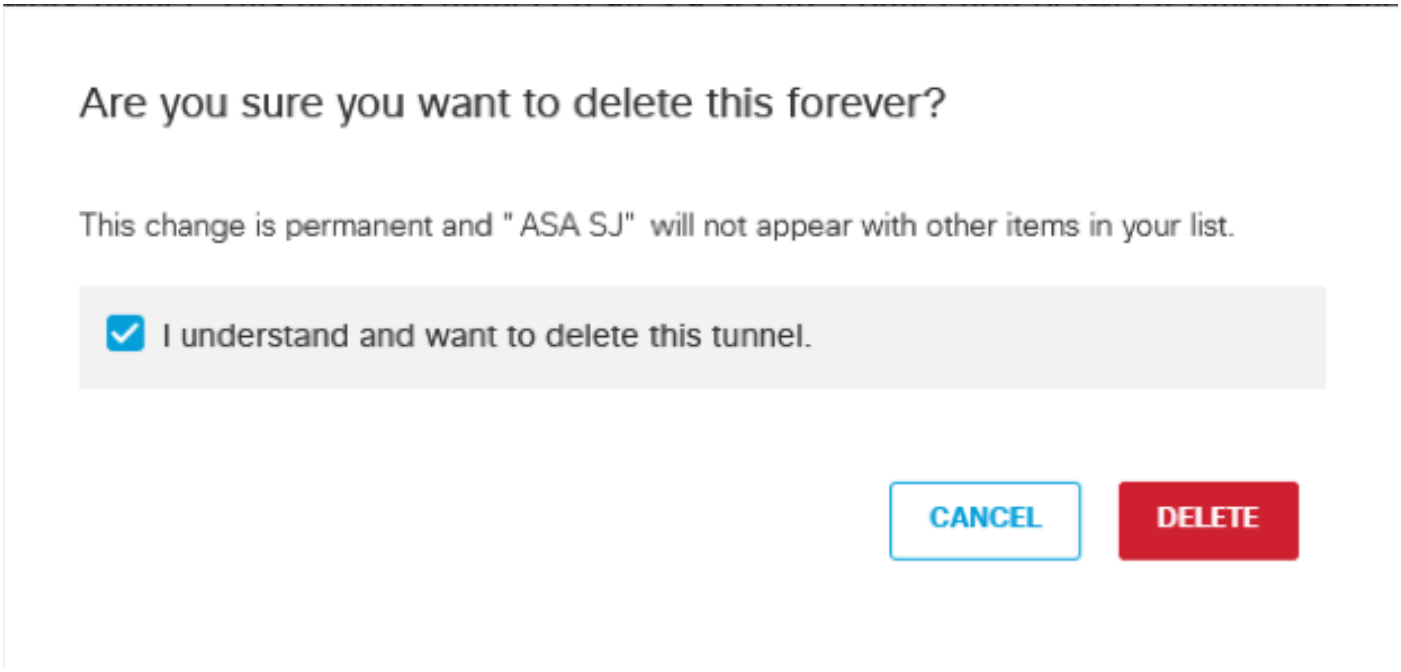

Imagen27.png

Paso 12: Actualización de políticas web con nueva identidad de

túnel

Confirme que las políticas web tienen la identidad actualizada con el nuevo túnel de red:

1. En el panel de Umbrella, navegue hasta Políticas > Gestión > Políticas web.

2. Revise la sección Túneles y confirme que las políticas web tienen la identidad actualizada con el nuevo túnel de red.

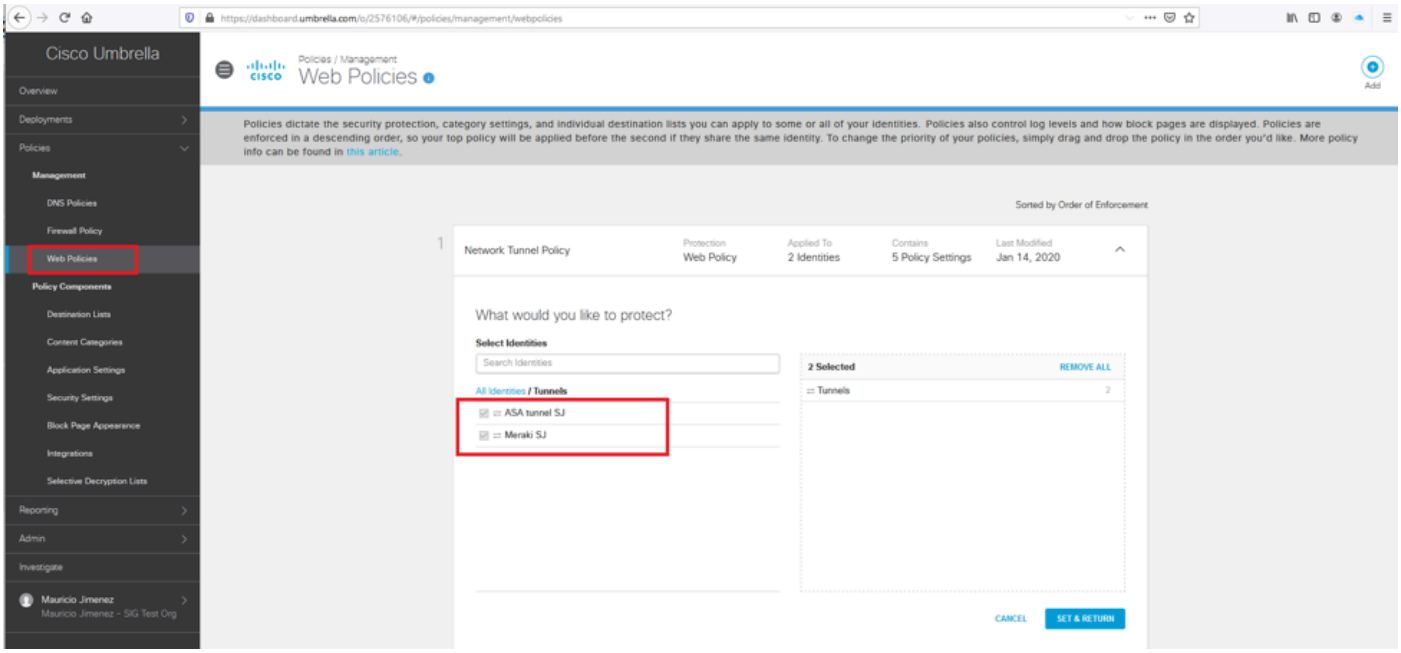

Imagen28.png

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).