

Cambiare il tunnel del firewall fornito dal cloud da RSA all'autenticazione PSK

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Passaggio 1: Verifica di un tunnel esistente utilizzando l'autenticazione RSA](#)

[Passaggio 2: Registrazione dell'IP pubblico dell'ASA](#)

[Passaggio 3: Crea nuovo tunnel ASA](#)

[Passaggio 4: Crea nuovo gruppo di tunnel](#)

[Passaggio 5: Individuare il profilo IPsec utilizzato per l'interfaccia del tunnel](#)

[Passaggio 6: Rimuovi punto di trust precedente dal profilo IPsec](#)

[Passaggio 7: Aggiorna interfaccia tunnel con nuovo IP headend Umbrella](#)

[Passaggio 8: Conferma nuova configurazione tunnel stabilita](#)

[Passaggio 9 \(facoltativo\): Rimozione del gruppo di tunnel precedente](#)

[Passaggio 10 \(facoltativo\): Rimuovi punto di trust precedente](#)

[Passaggio 11 \(facoltativo\): Elimina tunnel di rete precedente](#)

[Passaggio 12: Aggiorna criteri Web con nuova identità tunnel](#)

Introduzione

In questo documento viene descritto come riconfigurare il meccanismo di autenticazione del tunnel Cloud Delivered Firewall da RSA a PSK su Cisco ASA.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

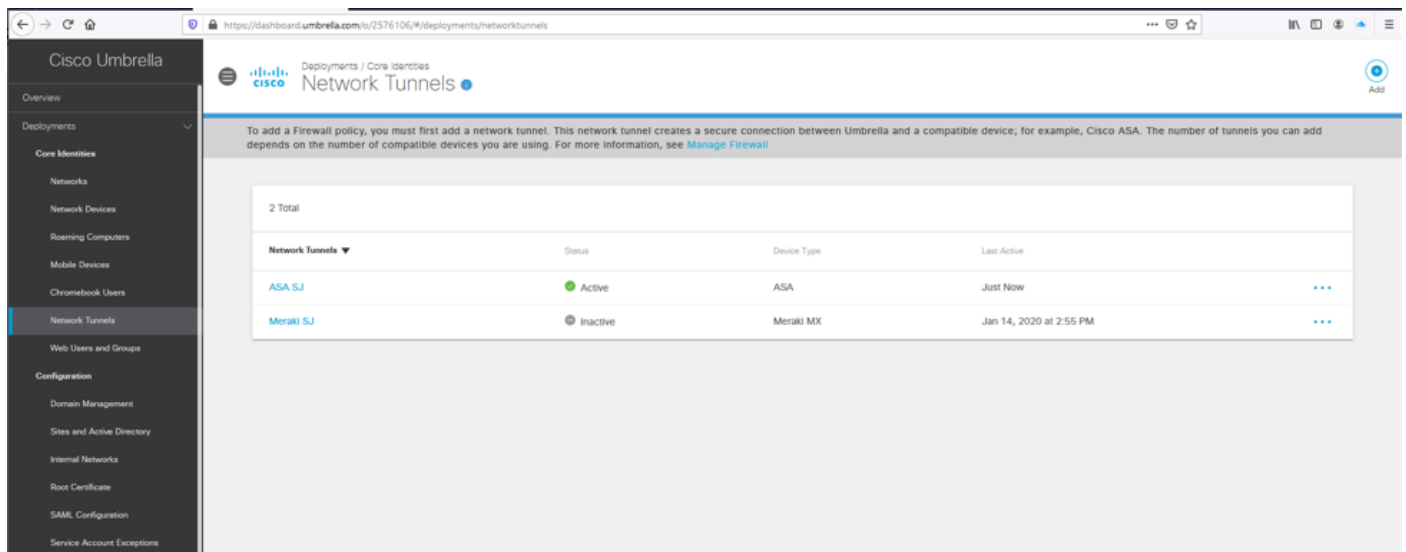
Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Passaggio 1: Verifica di un tunnel esistente utilizzando l'autenticazione RSA

Verificare di disporre di un tunnel esistente con autenticazione RSA e che lo stato del tunnel nell'ASA mostri la connessione con questo tipo di autenticazione.

1. Nel dashboard Umbrella, trovare il tunnel di rete con l'ASA che mostra un'impronta digitale di autenticazione del dispositivo.



Picture1.png

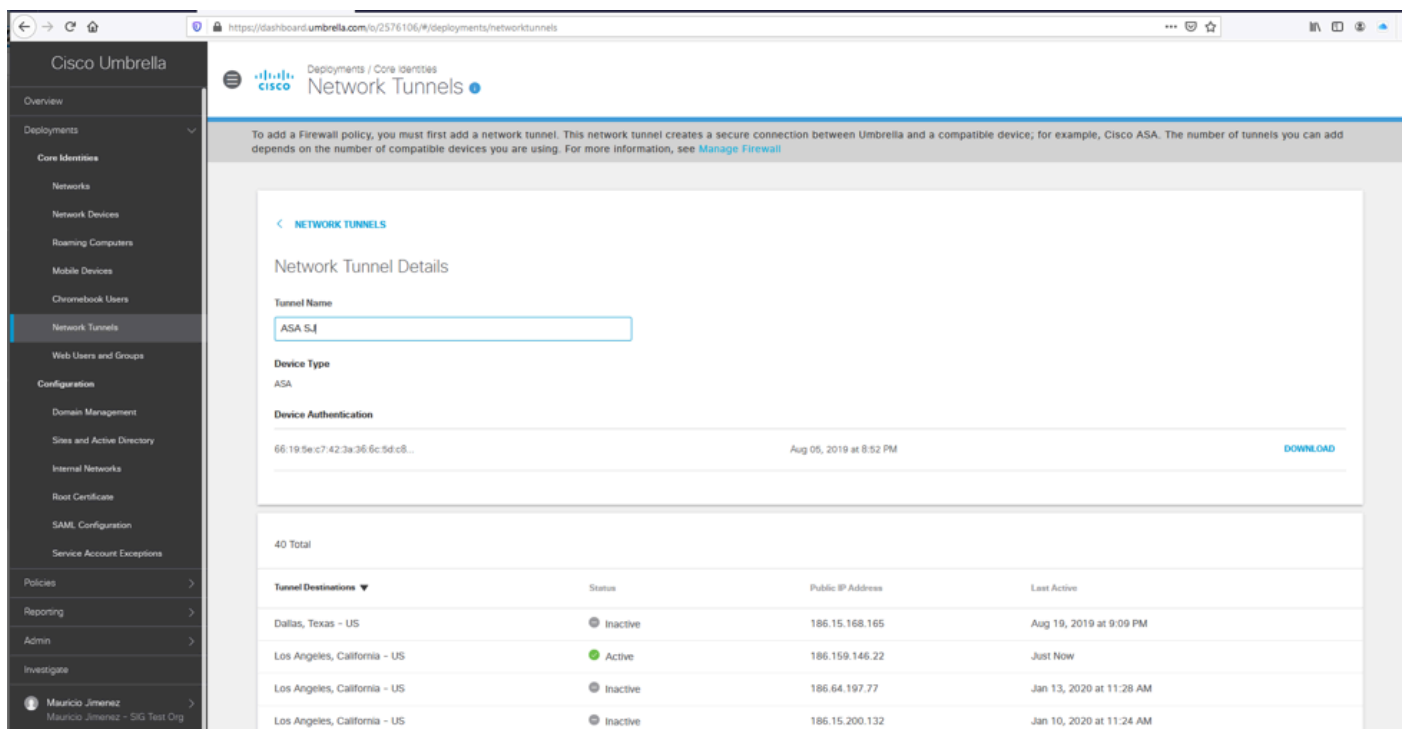


Immagine2.png

2. Nell'appliance Cisco ASA, è possibile eseguire questi comandi per verificare il tipo di

autenticazione e l'indirizzo IP dell'headend utilizzati per il tunnel.

```
show crypto ikev2 sa
```

e

```
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                               Status      Role      Remote
26325699 186.159.146.22/4500                      READY      INITIATOR 146.112.67.2/4500
          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/0xcceb02302
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 --->

```

Immagine4.png

Passaggio 2: Registrazione dell'IP pubblico dell'ASA

1. Verificare che l'IP pubblico utilizzato dall'interfaccia esterna ASA sia registrato come rete nel dashboard Umbrella.
2. Se la rete non esiste, aggiungerla e confermare l'indirizzo IP pubblico usato dall'interfaccia ASA. L'oggetto Network utilizzato per il tunnel deve essere definito con una subnet mask /32.

The screenshot shows the Cisco Umbrella Networks dashboard. The left sidebar contains navigation links: Overview, Deployments, Core Identities, Networks (selected), Network Devices, Roaming Computers, Mobile Devices, Chromebook Users, Network Tunnels, Web Users and Groups, and Configuration. The main content area displays a table of networks. The table has columns for Name, IP Address, Dynamic, Primary Policy, and Status. One network is listed: 'SJ - Network' with IP Address '186.159.146.22', Dynamic status, Primary Policy 'Default Policy', and Status 'Inactive'. Below the table, there are pagination controls: Page: 1, Results per page: 10, 1-1 of 1.

Name	IP Address	Dynamic	Primary Policy	Status
SJ - Network	186.159.146.22	Dynamic	Default Policy	Inactive

Immagine5.png

Passaggio 3: Crea nuovo tunnel ASA

1. Nel dashboard Umbrella in Distribuzioni/tunnel di rete, creare un nuovo tunnel selezionando l'opzione Aggiungi.

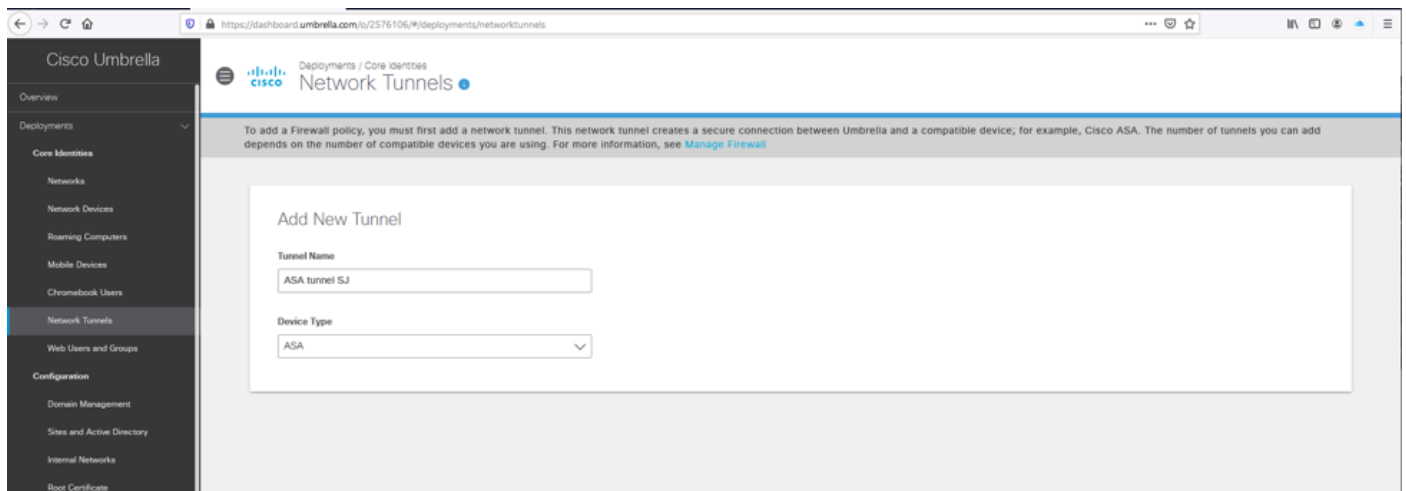


Immagine6.png

2. Selezionare l'ID tunnel in base alla rete che corrisponde all'IP pubblico dell'interfaccia esterna dell'ASA e impostare una passphrase per l'autenticazione PSK.

Set Tunnel ID and Passphrase

To add a tunnel so that you can configure your firewall, you need a Tunnel ID and Passphrase. For more information, see [Step-by-step Instructions »](#)

Tunnel ID (IP Address/Network)

SJ - Network - 186.159.146.22

Passphrase

●●●●●●●●●●●●●●●●

✓ 16 - 64 characters, at least 1 uppercase and 1 lowercase letter, 1 numeral, no special characters

Confirm Passphrase

●●●●●●●●●●●●●●●●

✓ Passphrases match

CANCEL

SAVE

Picture7.png

Tunnel ID and Passphrase Confirmed

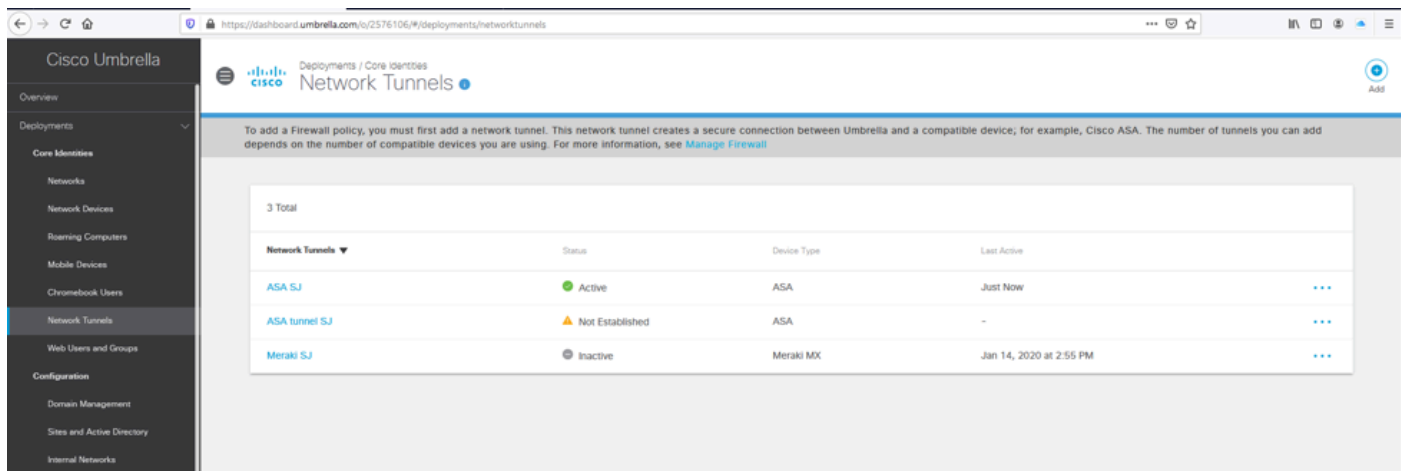
Please copy and save your Passphrase to your device

Passphrase: Asatunnel123456789



DONE

Immagine8.png

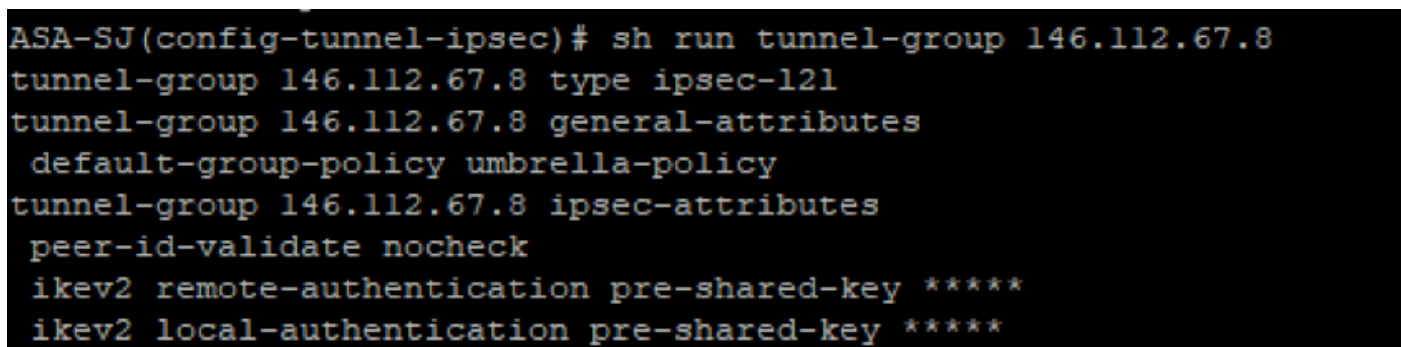


Picture9.png

Passaggio 4: Crea nuovo gruppo di tunnel

1. Sull'appliance ASA, creare un nuovo gruppo di tunnel utilizzando il nuovo headend IP per Umbrella e specificare la passphrase definita nel dashboard Umbrella per l'autenticazione PSK.
2. L'elenco aggiornato dei centri dati e degli indirizzi IP Umbrella per gli headend è disponibile nella [documentazione 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>
```



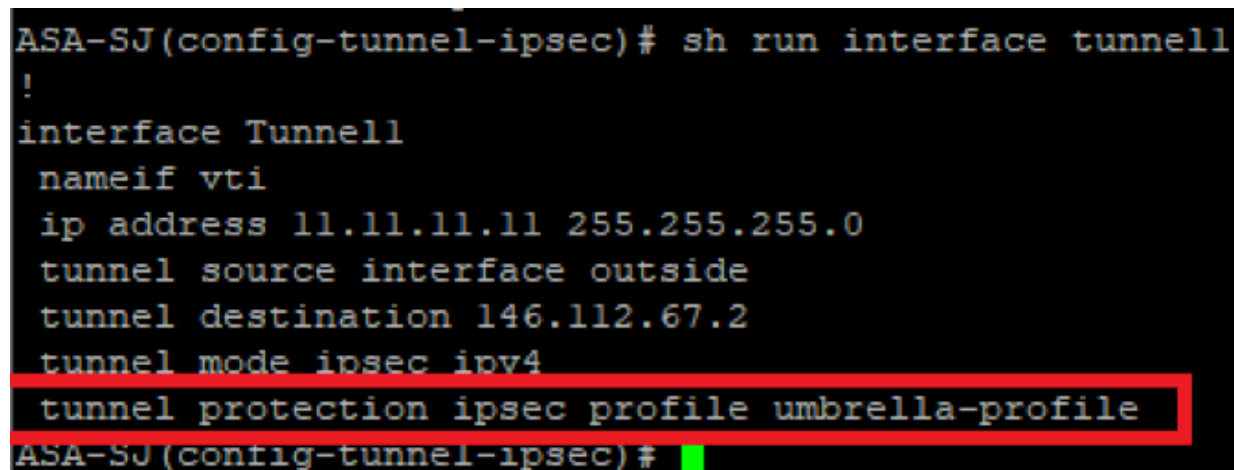
Picture10.png

Passaggio 5: Individuare il profilo IPsec utilizzato per l'interfaccia del tunnel

1. Cerca il "profilo IPsec crittografico" in uso nell'interfaccia del tunnel per la configurazione basata

sul percorso sull'headend Umbrella (il numero è sostituito dall'ID usato per l'interfaccia del tunnel con Umbrella):

```
show run interface tunnel#
```



```
ASA-SJ(config-tunnel-ipsec)# sh run interface tunnell
!
interface Tunnell
  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. Se non si è certi dell'ID del tunnel, è possibile usare questo comando per verificare le interfacce del tunnel esistenti e determinare quella usata per la configurazione basata sul tunnel Umbrella:

```
show run interface tunnel
```

Passaggio 6: Rimuovi punto di trust precedente dal profilo IPsec

1. Rimuovere il trust point dal profilo IPsec che fa riferimento all'autenticazione RSA per il tunnel. È possibile verificare la configurazione utilizzando questo 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 121-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. Continuare a rimuovere il trust point con questi comandi:

```
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. Confermare che il trust point è stato rimosso dal profilo IPsec di crittografia:

```
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 121-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
```

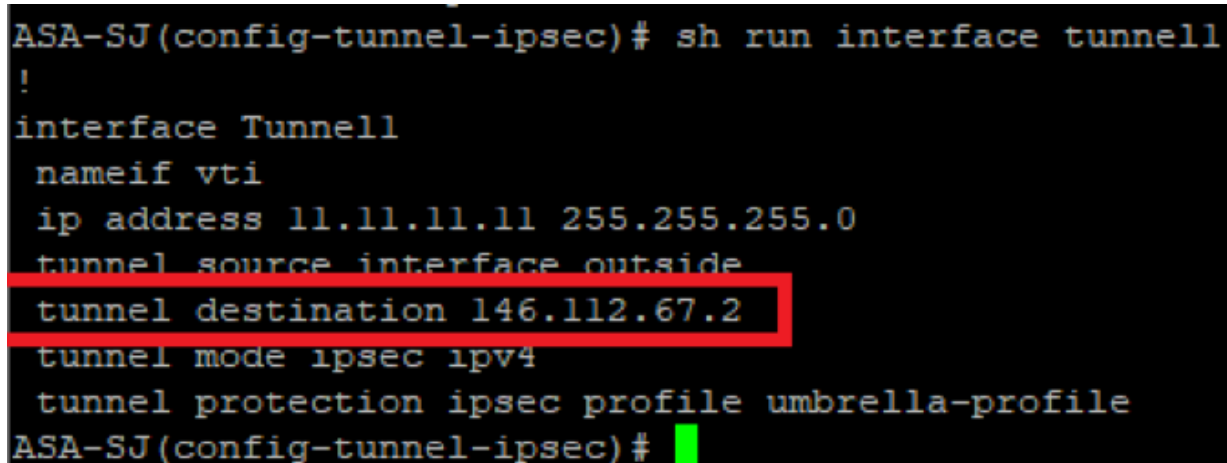
Picture14.png

Passaggio 7: Aggiorna interfaccia tunnel con nuovo IP headend Umbrella

1. Sostituire la destinazione dell'interfaccia del tunnel con il nuovo indirizzo IP dell'headend Umbrella che termina con .8.

- È possibile utilizzare questo comando per verificare la destinazione corrente in modo che venga sostituita con l'indirizzo IP dei nuovi intervalli di indirizzi IP del data center, disponibili nella [documentazione Umbrella](#):

```
show run interface tunnel
```



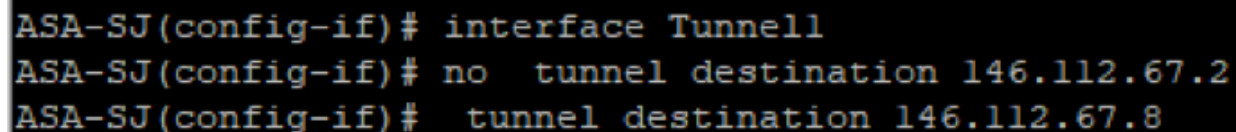
```
ASA-SJ(config-tunnel-ipsec)# sh run interface tunnell
!
interface Tunnell
  nameif vti
  ip address 11.11.11.11 255.255.255.0
  tunnel source interface outside
  tunnel destination 146.112.67.2
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile umbrella-profile
ASA-SJ(config-tunnel-ipsec)#
```

Picture15.png

```
Interface tunnel#
```

```
No tunnel destination <UMBRELLA DC IP address.2>
```

```
Tunnel destination <UMBRELLA DC IP address .8>
```



```
ASA-SJ(config-if)# interface Tunnell
ASA-SJ(config-if)# no tunnel destination 146.112.67.2
ASA-SJ(config-if)# tunnel destination 146.112.67.8
```

Picture16.png

2. Confermare la modifica con il comando:

```
show run interface tunnel#
```

```

ASA-SJ(config-if)# show run interface tunnelli
!
interface Tunnelli
 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

Passaggio 8: Conferma nuova configurazione tunnel stabilita

1. Confermare che la connessione del tunnel a Umbrella sia stata ristabilita correttamente con l'headend IP aggiornato e usare l'autenticazione PSK con questo 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

```

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

Passaggio 9 (facoltativo): Rimozione del gruppo di tunnel precedente

1. Rimuovere il vecchio gruppo di tunnel che indicava il precedente intervallo IP dell'headend Umbrella .2.

È possibile utilizzare questo comando per identificare il tunnel corretto prima di rimuovere la configurazione:

```
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. Rimuovere i riferimenti del vecchio gruppo di tunnel utilizzando questo comando:

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

```

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

```

Picture21.png

Passaggio 10 (facoltativo): Rimuovi punto di trust precedente

1. Rimuovere eventuali riferimenti al trust point utilizzato in precedenza con la configurazione basata sul tunnel Umbrella con questo comando:

```
sh run crypto ipsec
```

Il nome descrittivo utilizzato per il trust point è disponibile quando si controlla il "profilo IPsec di crittografia":

```
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 121-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. È possibile eseguire questo comando per confermare la configurazione del trust point. Verificare che il nome descrittivo corrisponda alla configurazione utilizzata nel 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
crl configure
crypto ca trustpoint asaconnector-trust
enrollment terminal
crl configure
```

Picture23.png

3. Per ottenere ulteriori dettagli sul certificato, utilizzare il 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:

```

Picture24.png

4. Rimuovere il trust point con il 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.

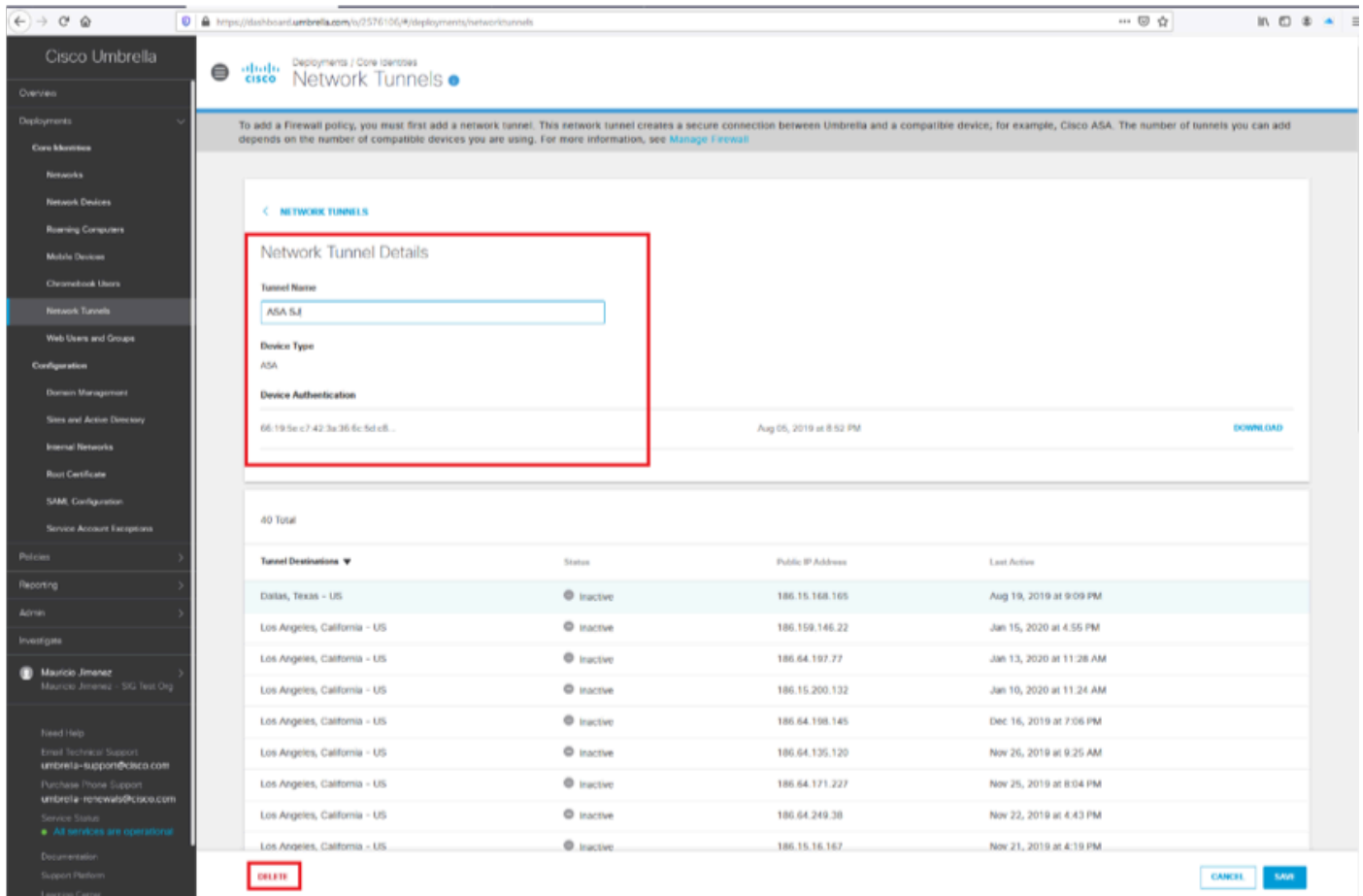
Are you sure you want to do this? [yes/no]: yes
INFO: Be sure to ask the CA administrator to revoke your certificates.
ASA-SJ(config)#

```

Picture25.png

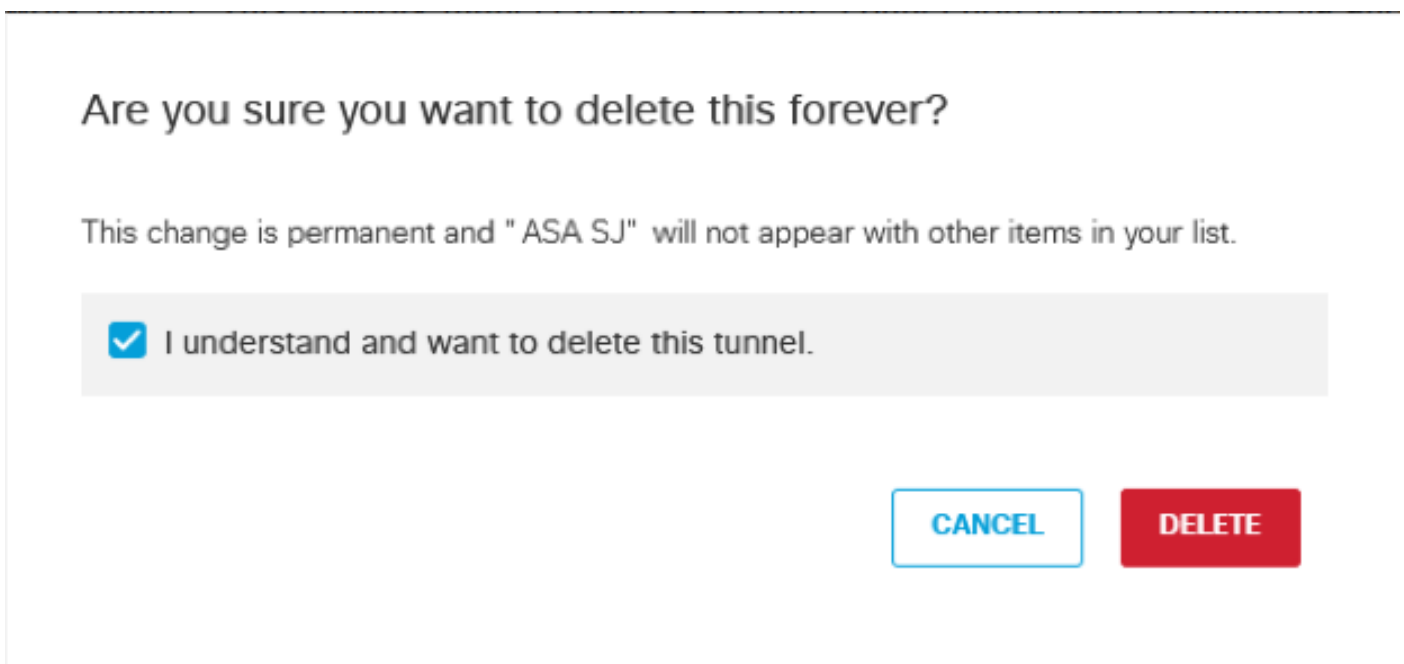
Passaggio 11 (facoltativo): Elimina tunnel di rete precedente

1. Eliminare il tunnel di rete precedente dal dashboard Umbrella passando a Dettagli tunnel di rete e selezionando Elimina.



Picture26.png

2. Confermare l'eliminazione selezionando l'opzione Comprendo e voglio eliminare questo tunnel nel popup, quindi selezionare Elimina.

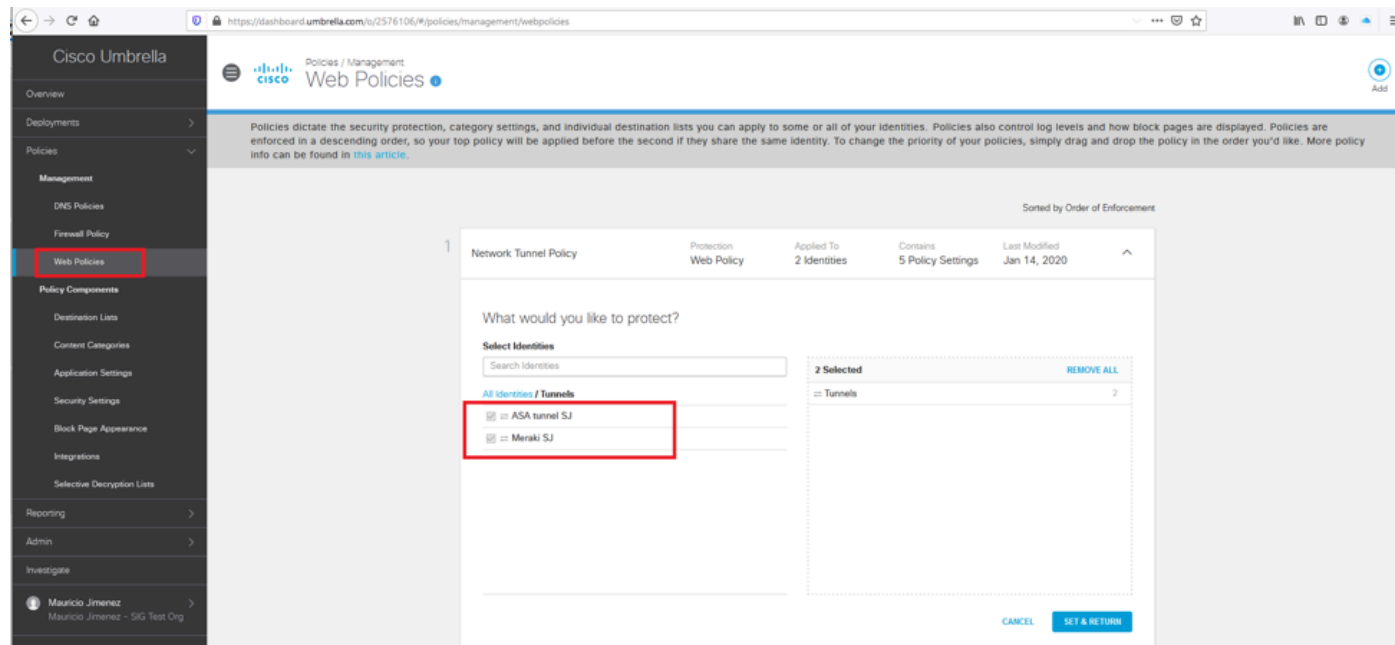


Picture27.png

Passaggio 12: Aggiorna criteri Web con nuova identità tunnel

Confermare che i criteri Web abbiano l'identità aggiornata con il nuovo tunnel di rete:

1. Nel pannello di controllo Ombrello, passare a Criteri > Gestione > Criteri Web.
2. Consulta la sezione Tunnel e conferma che i tuoi criteri Web hanno l'identità aggiornata con il nuovo tunnel di rete.



Picture28.png

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).