

클라우드 제공 방화벽 터널을 RSA에서 PSK 인증으로 변경

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[1단계: RSA 인증을 사용하여 기존 터널 확인](#)

[2단계: ASA의 공용 IP 등록](#)

[3단계: 새 ASA 터널 생성](#)

[4단계: 새 터널 그룹 생성](#)

[5단계: 터널 인터페이스에 사용되는 IPSec 프로파일을 찾습니다](#)

[6단계: IPSec 프로파일에서 이전 신뢰 지점 제거](#)

[7단계: 새 Umbrella Headend IP로 터널 인터페이스 업데이트](#)

[8단계: 새 터널 컨피그레이션이 성공적으로 설정되었는지 확인](#)

[9단계\(선택 사항\): 기존 터널 그룹 제거](#)

[10단계\(선택 사항\): 이전 신뢰 지점 제거](#)

[11단계\(선택 사항\): 이전 네트워크 터널 삭제](#)

[12단계: 새 터널 ID로 웹 정책 업데이트](#)

소개

이 문서에서는 Cisco ASA의 RSA에서 PSK로 클라우드 제공 방화벽 터널의 인증 메커니즘을 재구성하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

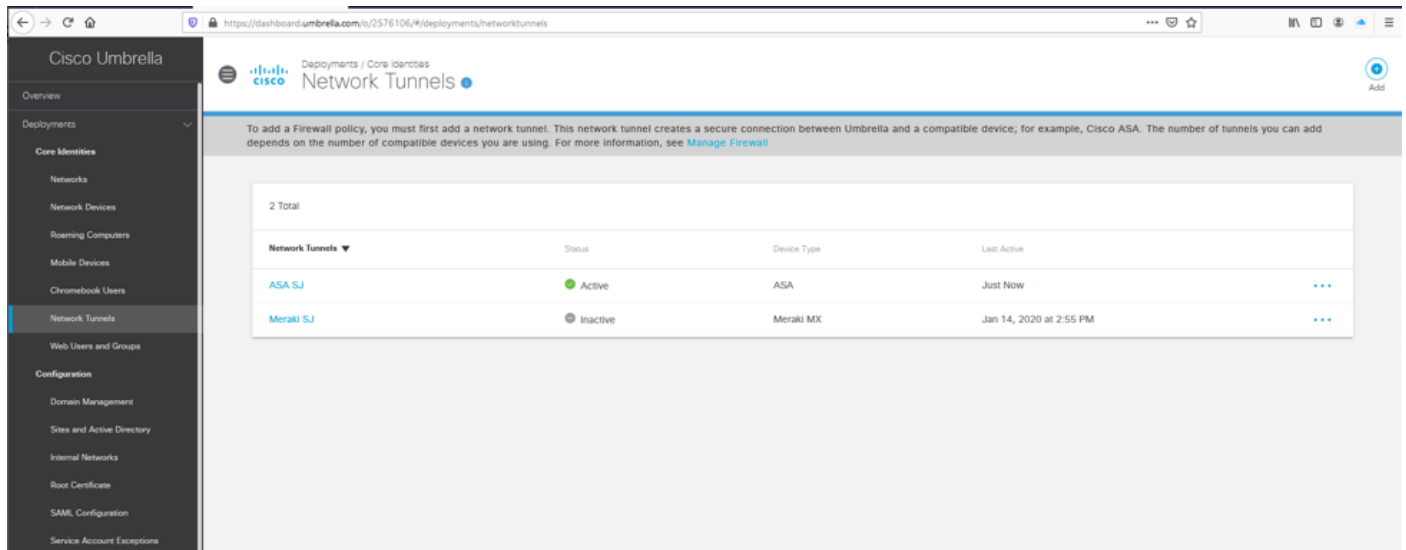
이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

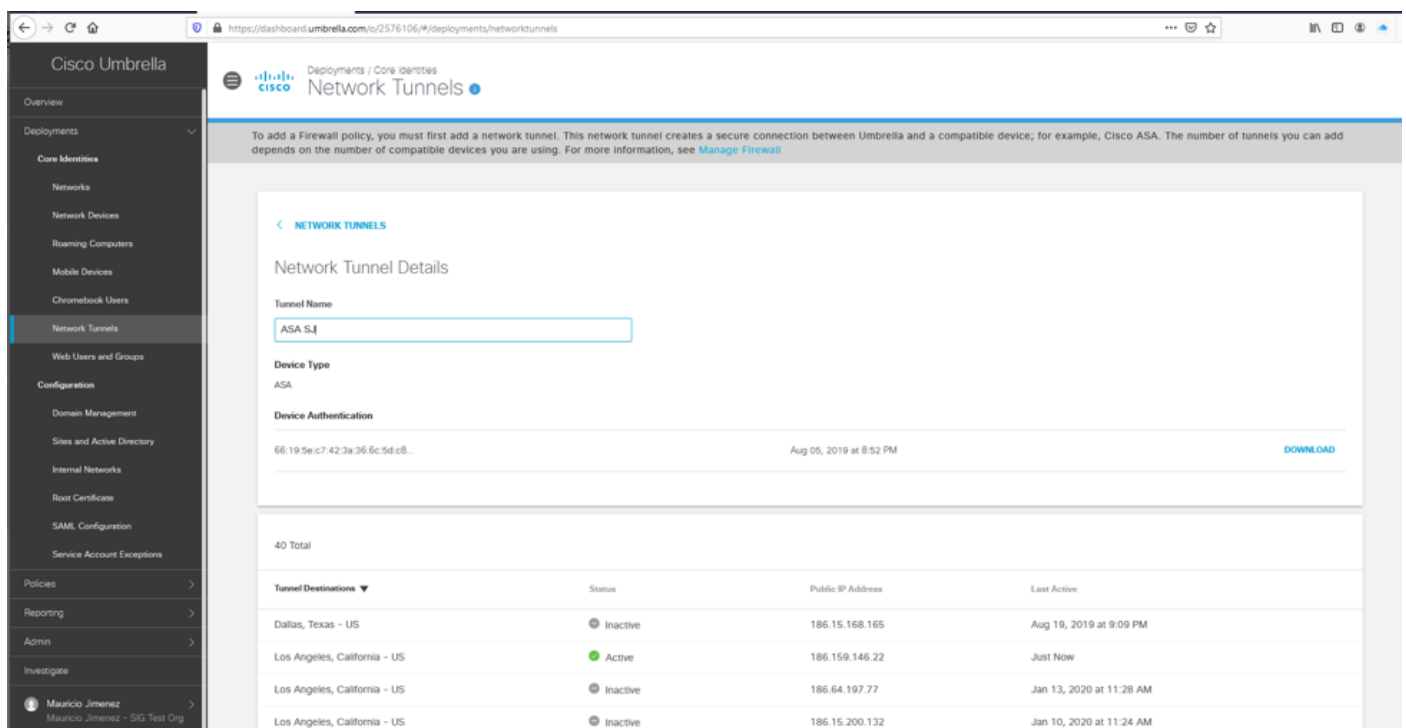
1단계: RSA 인증을 사용하여 기존 터널 확인

RSA 인증을 사용하는 기존 터널이 있고 ASA의 터널 상태가 이 인증 유형으로 연결됨으로 표시되는지 확인합니다.

1. Umbrella 대시보드에서 ASA에 디바이스 인증 핑거프린트가 표시된 네트워크 터널을 찾습니다.



Picture1.png



Picture2.png

2. Cisco ASA에서 이러한 명령을 실행하여 터널에 사용 중인 인증 유형 및 헤드엔드 IP를 확인할 수 있습니다.

show crypto ikev2 sa

및

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/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

2단계: ASA의 공용 IP 등록

1. Umbrella 대시보드에서 네트워크로 등록된 ASA 외부 인터페이스에서 사용하는 공용 IP가 있는지 확인합니다.

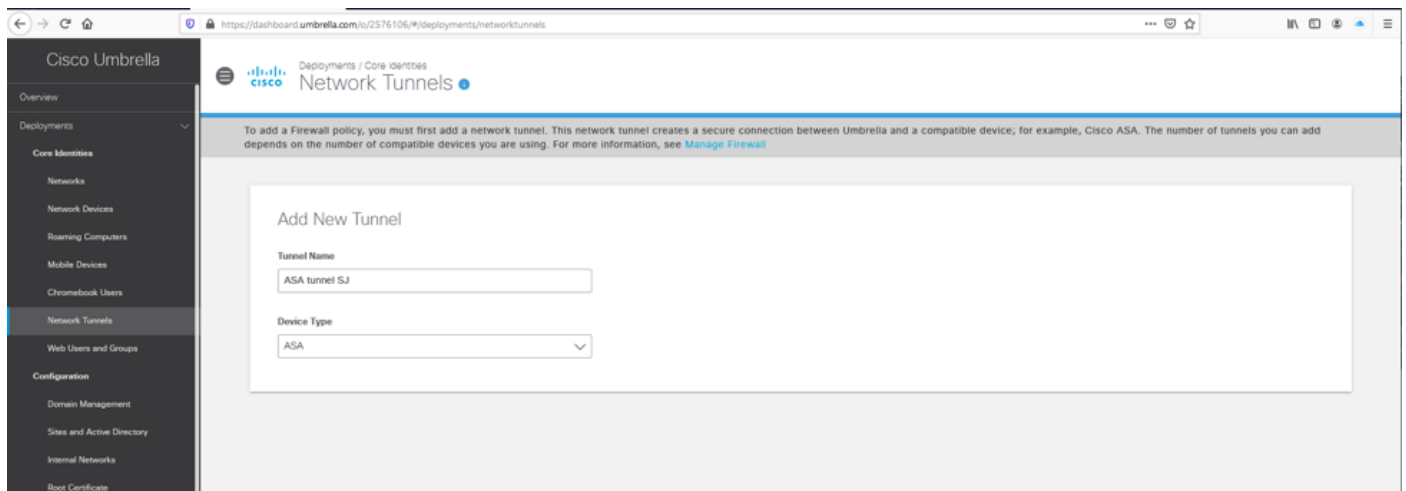
2. 네트워크가 없는 경우 계속해서 네트워크를 추가하고 ASA 인터페이스에서 사용하는 공용 IP를 확인합니다. 이 터널에 사용되는 네트워크 개체는 /32 서브넷 마스크로 정의되어야 합니다.

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 is a pagination bar showing 'Page: 1', 'Results per page: 10', and '1-1 of 1'.

Picture5.png

3단계: 새 ASA 터널 생성

1. Deployments/Network Tunnels(구축/네트워크 터널) 아래의 Umbrella 대시보드에서 Add(추가) 옵션을 선택하여 새 터널을 생성합니다.



Picture6.png

2. ASA 외부 인터페이스의 공용 IP와 일치하는 네트워크를 기반으로 터널 ID를 선택하고 PSK 인증을 위한 암호를 설정합니다.

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

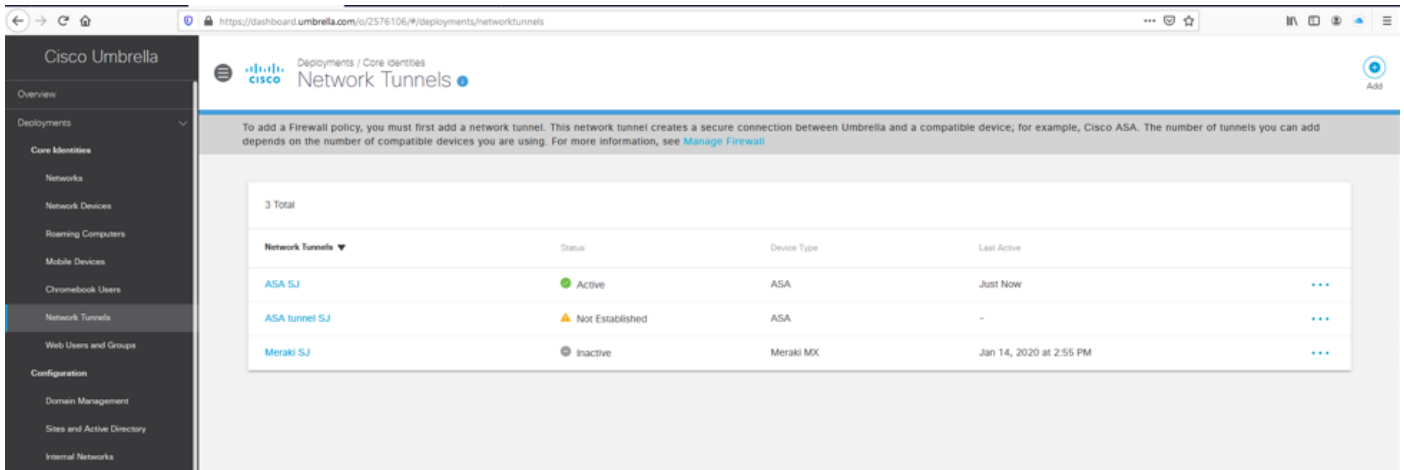
Please copy and save your Passphrase to your device

Passphrase: Asatunnel123456789



DONE

Picture8.png



Picture9.png

4단계: 새 터널 그룹 생성

1. ASA에서 Umbrella에 대한 새 헤드엔드 IP를 사용하여 새 터널 그룹을 만들고 Umbrella 대시보드에서 PSK 인증을 위해 정의한 암호를 지정합니다.
2. 업데이트된 Umbrella 데이터 센터 및 헤드엔드의 IP 목록은 [Umbrella](#) 문서에서 확인할 수 있습니다.

```
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>
```

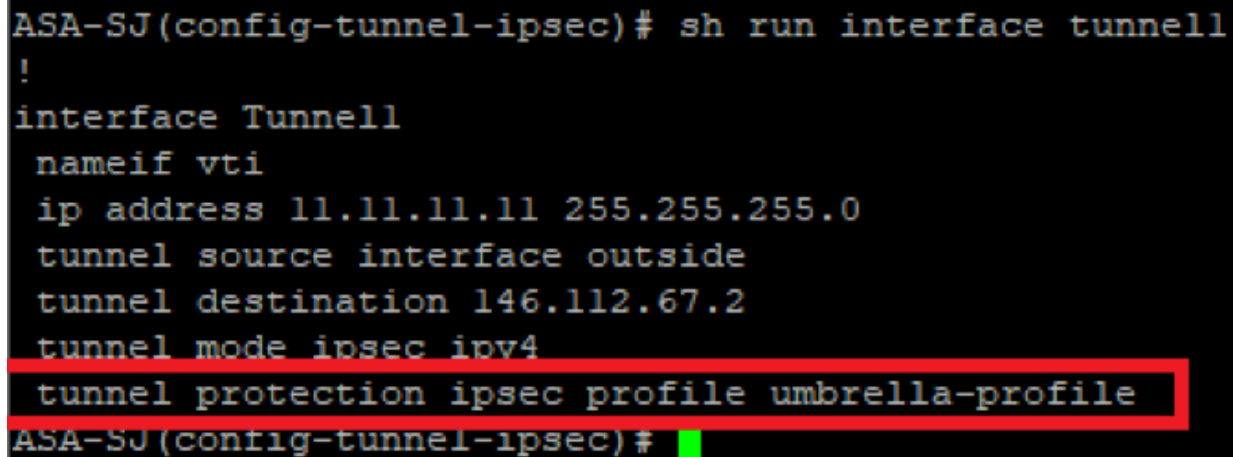
```
ASA-SJ(config-tunnel-ipsec)# sh run tunnel-group 146.112.67.8
tunnel-group 146.112.67.8 type ipsec-l2l
tunnel-group 146.112.67.8 general-attributes
default-group-policy umbrella-policy
tunnel-group 146.112.67.8 ipsec-attributes
peer-id-validate nocheck
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

그림10.png

5단계: 터널 인터페이스에 사용되는 IPSec 프로파일을 찾습니다

1. Umbrella 헤드엔드에 대한 경로 기반 컨피그레이션에 대해 터널 인터페이스에서 사용 중인 "crypto ipsec profile"을 검색합니다(#은 Umbrella에 대한 터널 인터페이스에 사용되는 ID로 교체됩니다).

```
show run interface tunnel#
```

A screenshot of a Cisco ASA command-line interface. The prompt is 'ASA-SJ(config-tunnel-ipsec)#'. The user enters 'sh run interface tunnel1'. The output shows the configuration for 'interface Tunnel1', including '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', and 'tunnel protection ipsec profile umbrella-profile'. The last line is highlighted with a red box. The prompt returns to 'ASA-SJ(config-tunnel-ipsec)#' with a green cursor.

```
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. 터널 ID에 대해 잘 모르는 경우 이 명령을 사용하여 기존 터널 인터페이스를 확인하고 Umbrella 터널 기반 컨피그레이션에 사용되는 인터페이스를 확인할 수 있습니다.

```
show run interface tunnel
```

6단계: IPSec 프로파일에서 이전 신뢰 지점 제거

1. 터널에 대한 RSA 인증을 참조하는 IPSec 프로파일에서 신뢰 지점을 제거합니다. 다음 명령을 사용하여 컨피그레이션을 확인할 수 있습니다.

```
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. 다음 명령으로 신뢰 지점을 제거합니다.

```

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. 신뢰 지점이 암호화 ipsec 프로파일에서 제거되었는지 확인합니다.

```

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

```

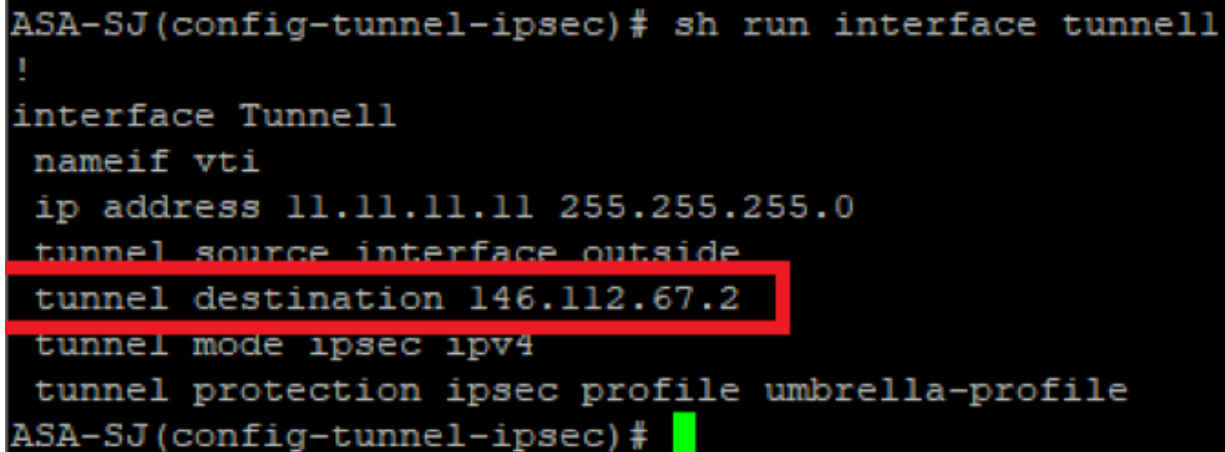
Picture14.png

7단계: 새 Umbrella Headend IP로 터널 인터페이스 업데이트

1. 터널 인터페이스의 목적지를 .8에서 종료되는 새 Umbrella 헤드엔드 IP 주소로 교체합니다.

- [Umbrella 설명서](#)에 있는 새 데이터 센터 IP 주소 범위의 IP로 교체되도록 이 명령을 사용하여 현재 대상을 확인할 수 [있습니다](#).

```
show run interface tunnel
```



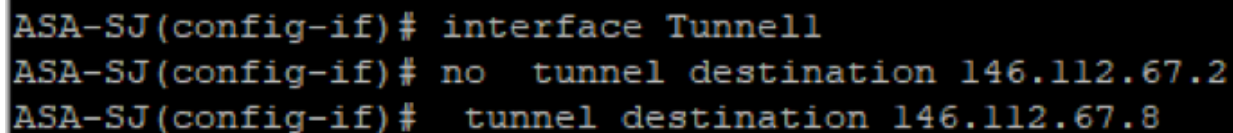
```
ASA-SJ(config-tunnel-ipsec)# sh run interface tunnell
!
interface Tunnell
  nameif vti
  ip address 11.11.11.11 255.255.255.0
  tunnel source interface outside
  tunnel destination 146.112.67.2
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile umbrella-profile
ASA-SJ(config-tunnel-ipsec)#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

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. 다음 명령을 사용하여 변경 사항을 확인합니다.

```
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

8단계: 새 터널 컨피그레이션이 성공적으로 설정되었는지 확인

1. Umbrella에 대한 터널 연결이 업데이트된 헤드엔드 IP를 사용하여 올바르게 다시 설정되었는지 확인하고 이 명령으로 PSK 인증을 사용합니다.

```
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

9단계(선택 사항): 기존 터널 그룹 제거

1. 이전 Umbrella 헤드엔드 IP 범위 .2를 가리키는 기존 터널 그룹을 제거합니다.

이 명령을 사용하여 컨피그레이션을 제거하기 전에 올바른 터널을 식별할 수 있습니다.

```
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. 다음 명령을 사용하여 이전 터널 그룹에 대한 참조를 제거합니다.

```
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

10단계(선택 사항): 이전 신뢰 지점 제거

1. 이 명령을 사용하여 Umbrella 터널 기반 컨피그레이션에서 이전에 사용된 신뢰 지점에 대한 참조를 제거합니다.

```
sh run crypto ipsec
```

신뢰 지점에 사용되는 친숙한 이름은 "crypto ipsec profile"을 검토할 때 찾을 수 있습니다.

```
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. 이 명령을 실행하여 신뢰 지점 컨피그레이션을 확인할 수 있습니다. 식별 이름이 crypto ipsec profile 명령에 사용된 컨피그레이션과 일치하는지 확인합니다.

```
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. 인증서에 대한 자세한 내용을 보려면 다음 명령을 사용하십시오.

```
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. 다음 명령을 사용하여 신뢰 지점을 제거합니다.

```
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.

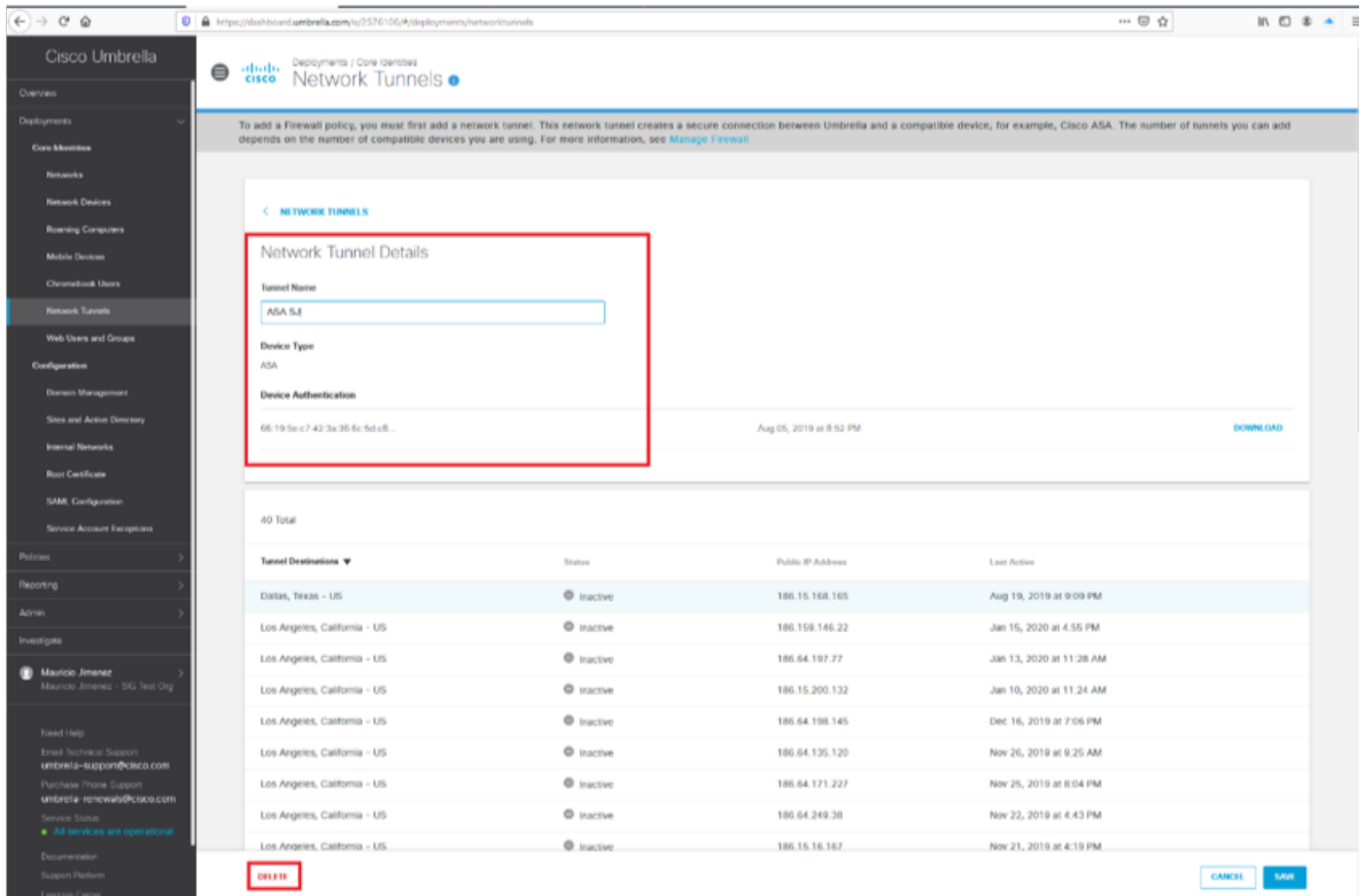
Are you sure you want to do this? [yes/no]: yes
INFO: Be sure to ask the CA administrator to revoke your certificates.
ASA-SJ(config)#

```

Picture25.png

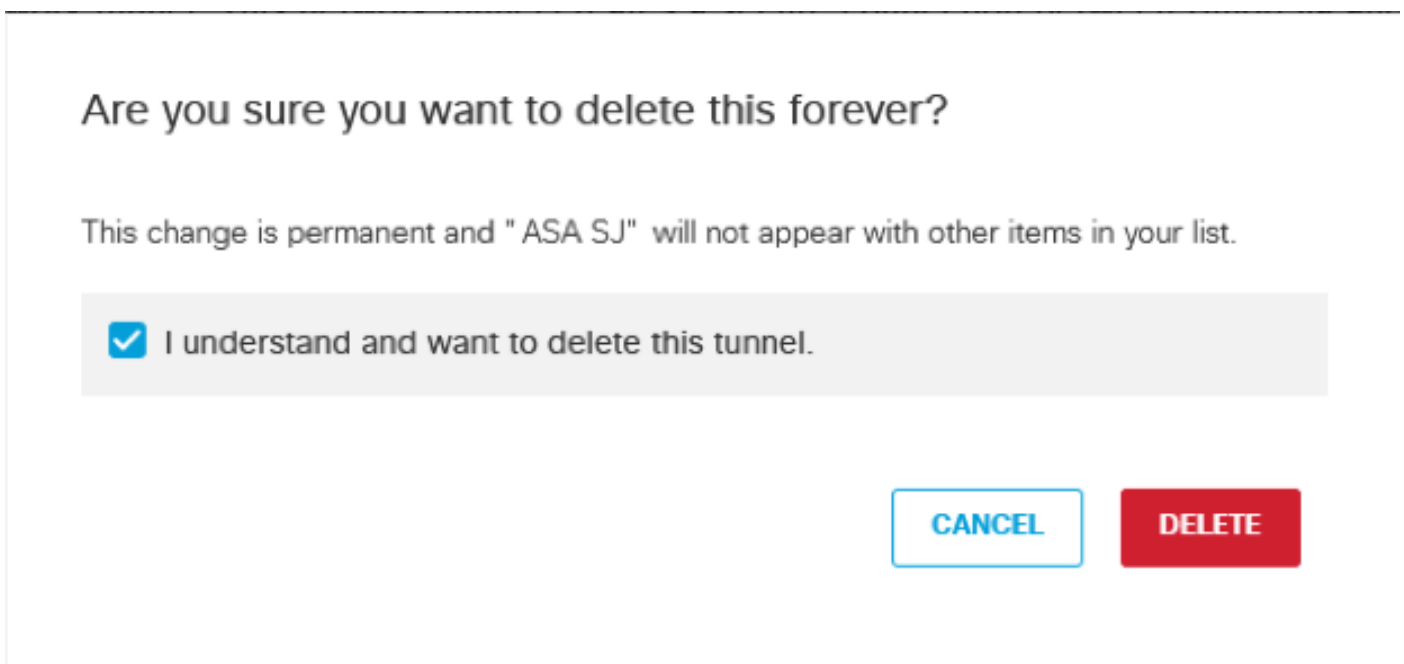
11단계(선택 사항): 이전 네트워크 터널 삭제

1. Umbrella 대시보드에서 Network Tunnel Details(네트워크 터널 세부사항)로 이동하고 Delete(삭제)를 선택하여 기존 네트워크 터널을 삭제합니다.



Picture26.png

2. 팝업에서 이 터널을 이해하고 삭제하려는 옵션을 선택하여 삭제를 확인한 다음 삭제를 선택합니다.



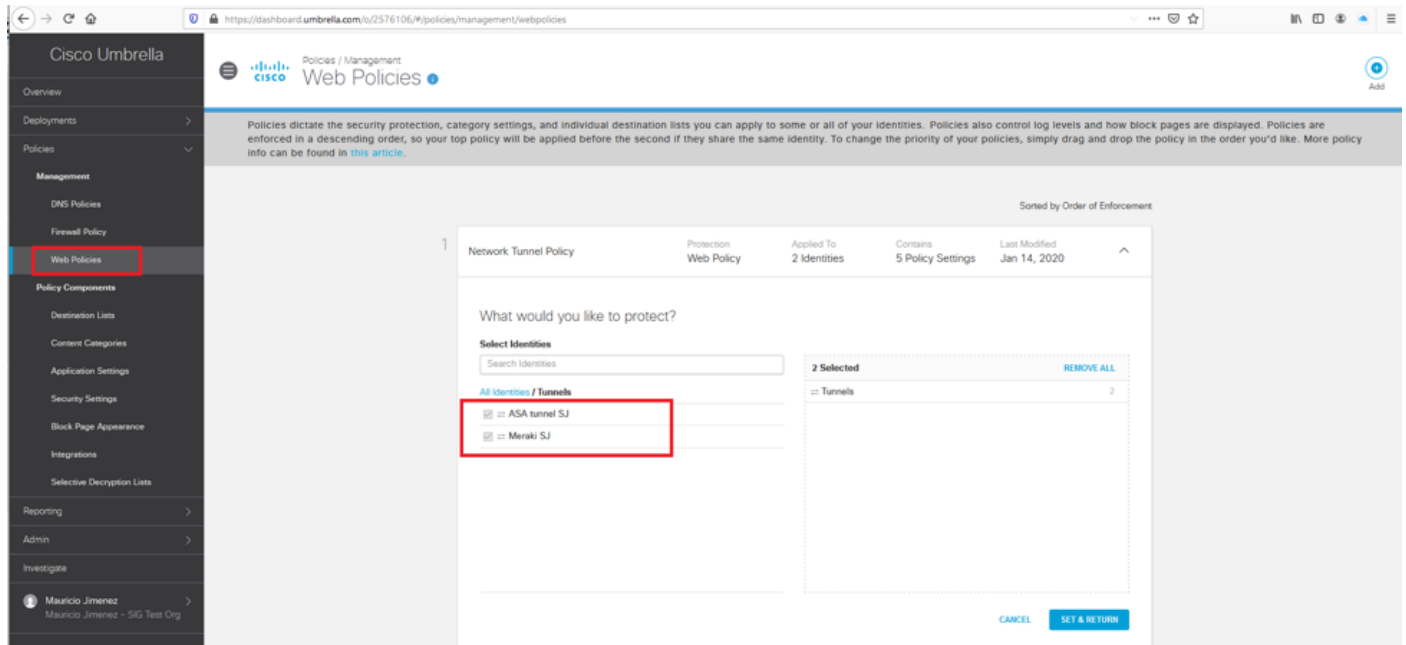
Picture27.png

12단계: 새 터널 ID로 웹 정책 업데이트

웹 정책에 새 네트워크 터널로 업데이트된 ID가 있는지 확인합니다.

1. Umbrella 대시보드에서 Policies(정책) > Management(관리) > Web Policies(웹 정책)로 이동합니다.

2. [터널] 섹션을 검토하고 웹 정책에 새 네트워크 터널과 업데이트된 ID가 있는지 확인합니다.



Picture28.png

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.