

將雲交付的防火牆隧道從RSA更改為PSK身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[步驟 1:使用RSA身份驗證驗證現有隧道](#)

[步驟 2:註冊ASA的公共IP](#)

[步驟 3:建立新的ASA隧道](#)

[步驟 4:建立新隧道組](#)

[步驟 5:找到用於隧道介面的IPSec配置檔案](#)

[步驟 6:從IPSec簡檔中刪除舊信任點](#)

[步驟 7:使用新的Umbrella頭端IP更新通道介面](#)

[步驟 8:確認新隧道配置已成功建立](#)

[第9步 \(可選\) : 刪除舊隧道組](#)

[第10步 \(可選\) : 刪除舊信任點](#)

[第11步 \(可選\) : 刪除舊網路隧道](#)

[步驟 12:使用新隧道標識更新Web策略](#)

簡介

本文檔介紹在Cisco ASA上將雲交付防火牆隧道的身份驗證機制從RSA重新配置為PSK的步驟。

必要條件

需求

本文件沒有特定需求。

採用元件

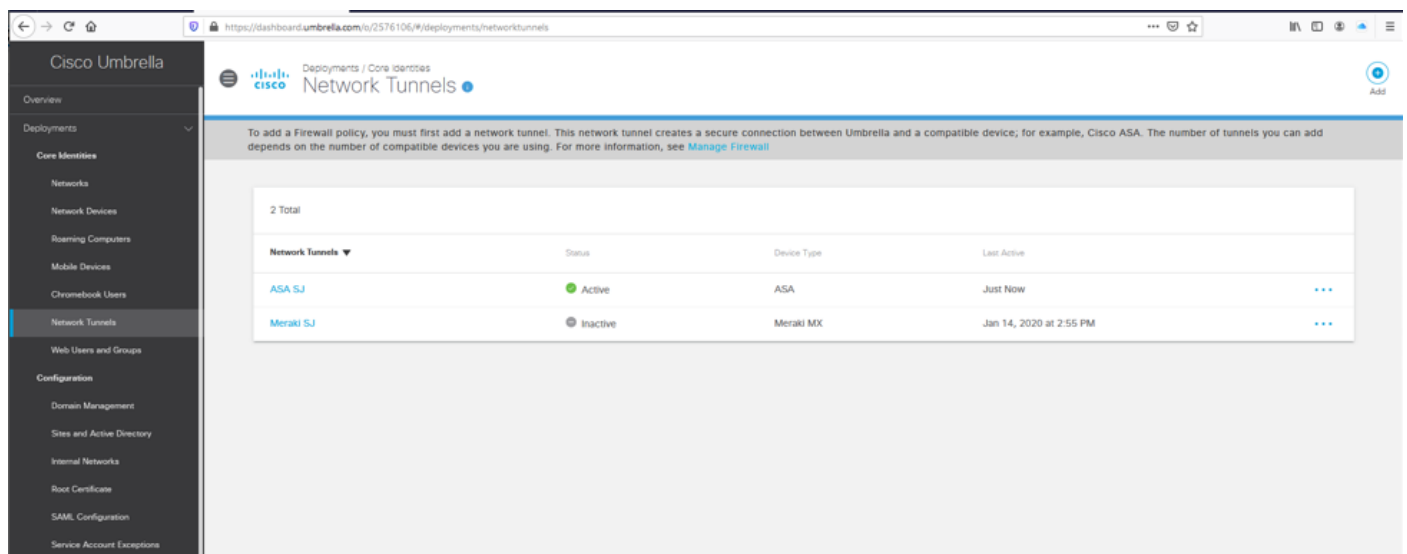
本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

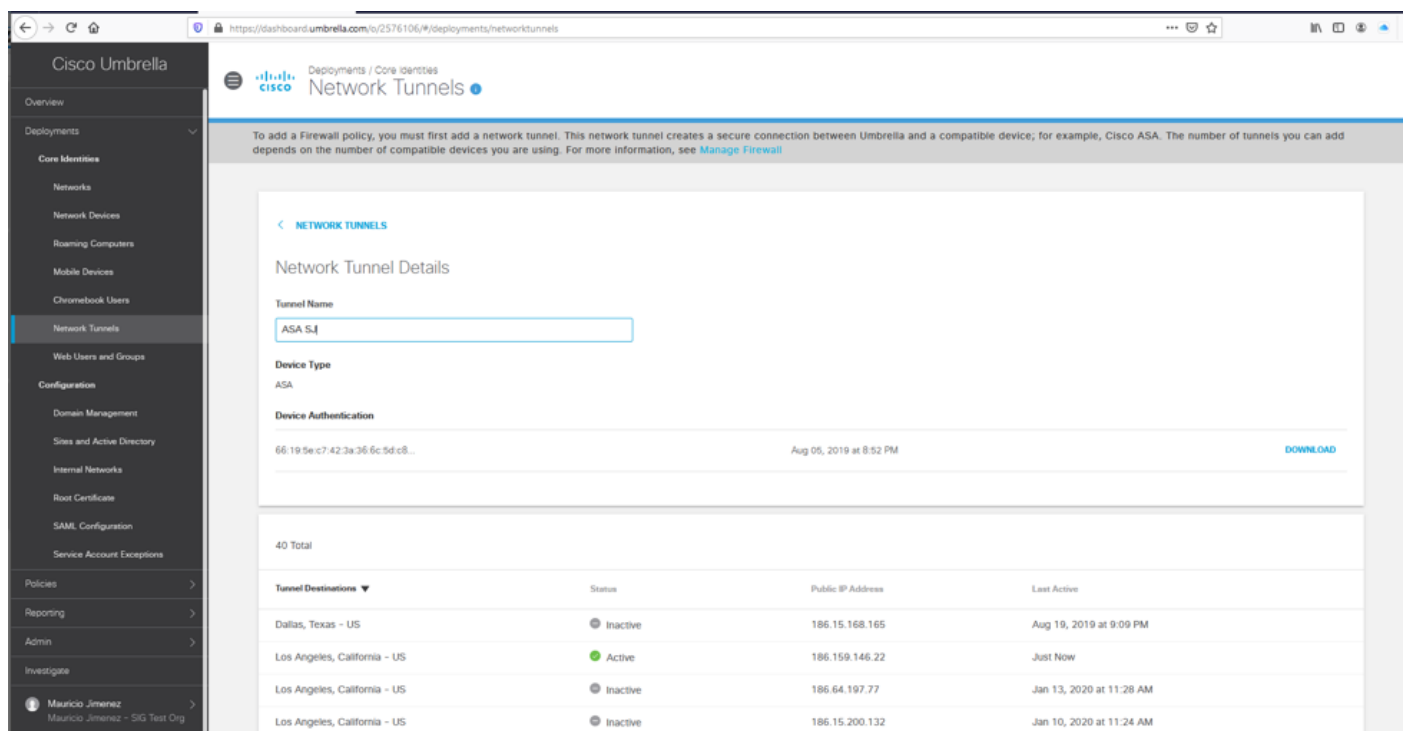
步驟 1:使用RSA身份驗證驗證現有隧道

驗證您已有一個使用RSA身份驗證的現有隧道，並且ASA中隧道的狀態顯示為已使用此身份驗證型別連線。

1.在Umbrella控制面板中，找到包含ASA顯示裝置身份驗證指紋的網路隧道。



圖片1.png



Picture2.png

2.在Cisco ASA中，您可以運行這些命令來驗證隧道所使用的身份驗證型別和頭端IP。

```
show crypto ikev2 sa
```

和

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#
```

圖片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

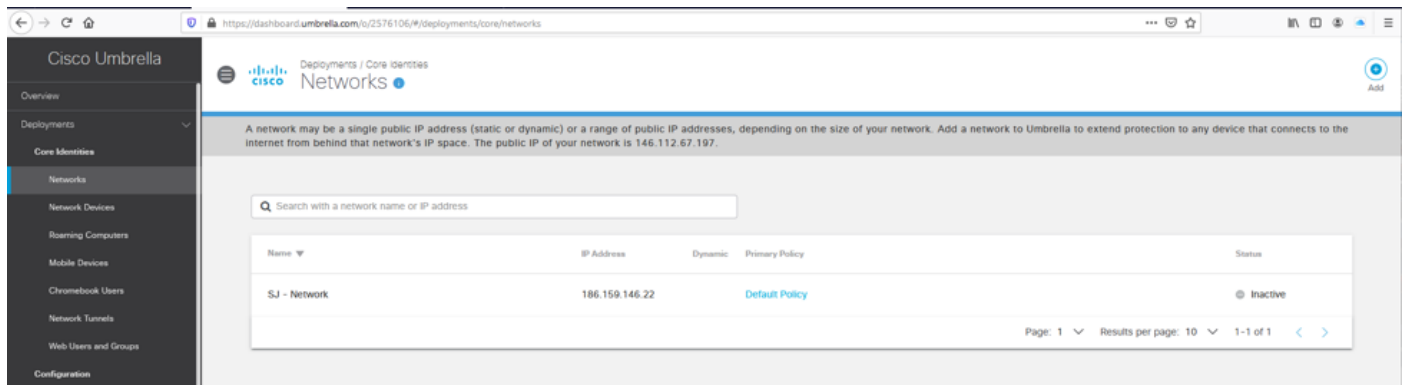
    local crypto endpt.: 186.159.146.22/4500, remote crypto endpt.: 146.112.67
.2/4500
    path mtu 1500, ipsec overhead 82(52), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: CCB02302
    current inbound spi : ECCFD18D

<--- More --->
```

圖片4.png

步驟 2:註冊ASA的公共IP

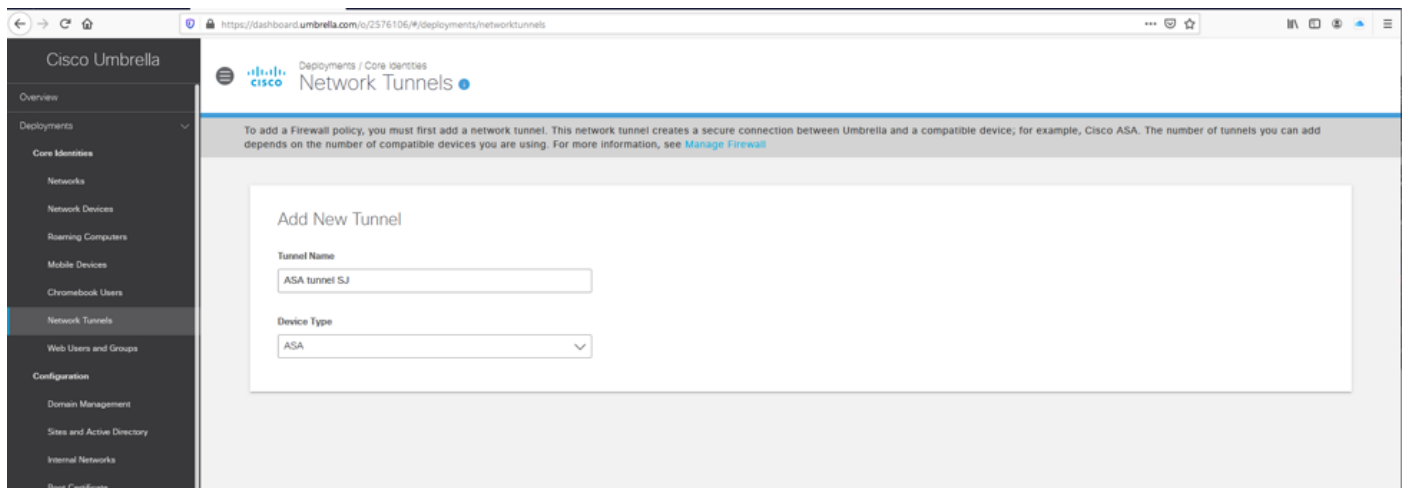
- 1.確保ASA外部介面使用的公共IP已在Umbrella控制面板中註冊為Network。
- 2.如果網路不存在，則繼續新增該網路並確認ASA介面使用的公共IP。必須使用/32子網掩碼定義用於此隧道的Network對象。



Picture5.png

步驟 3:建立新的ASA隧道

- 1.在部署/網路隧道下的Umbrella控制面板中，選擇Add選項建立一個新隧道。



Picture6.png

- 2.根據與ASA外部介面的公共IP匹配的網路，選擇隧道ID，並為PSK身份驗證設定密碼。

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

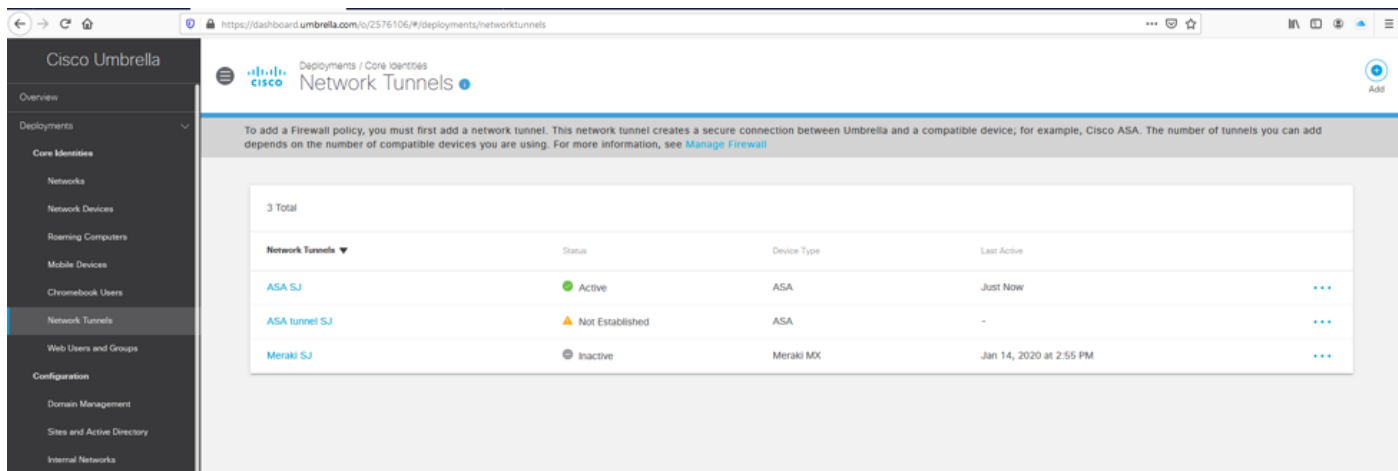
Please copy and save your Passphrase to your device

Passphrase: Asatunnel123456789



DONE

圖片8.png

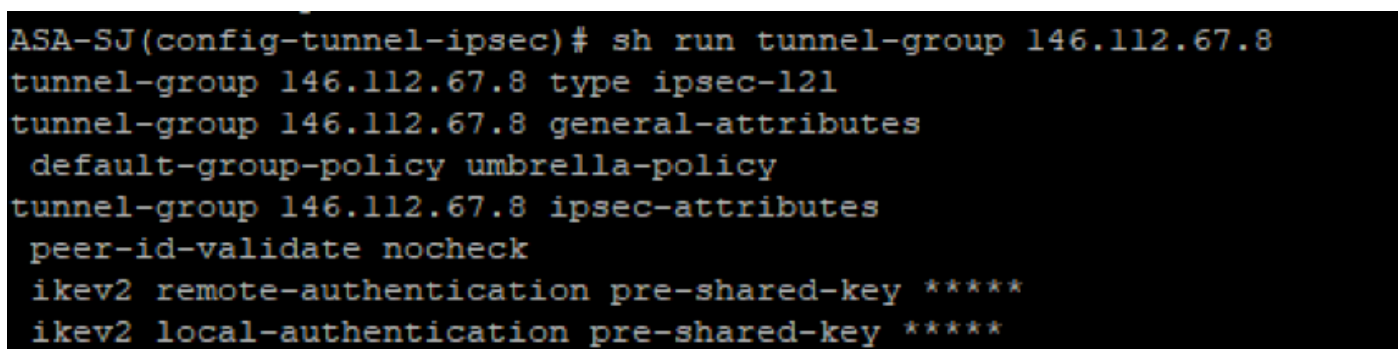


圖片9.png

步驟 4:建立新隧道組

- 1.在ASA上，使用用於Umbrella的新頭端IP建立新的隧道組，並在Umbrella控制面板中指定PSK身份驗證的密碼定義。
- 2.更新的頭端Umbrella資料中心和IP清單可在[Umbrella文檔中找到](#)。

```
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>
```

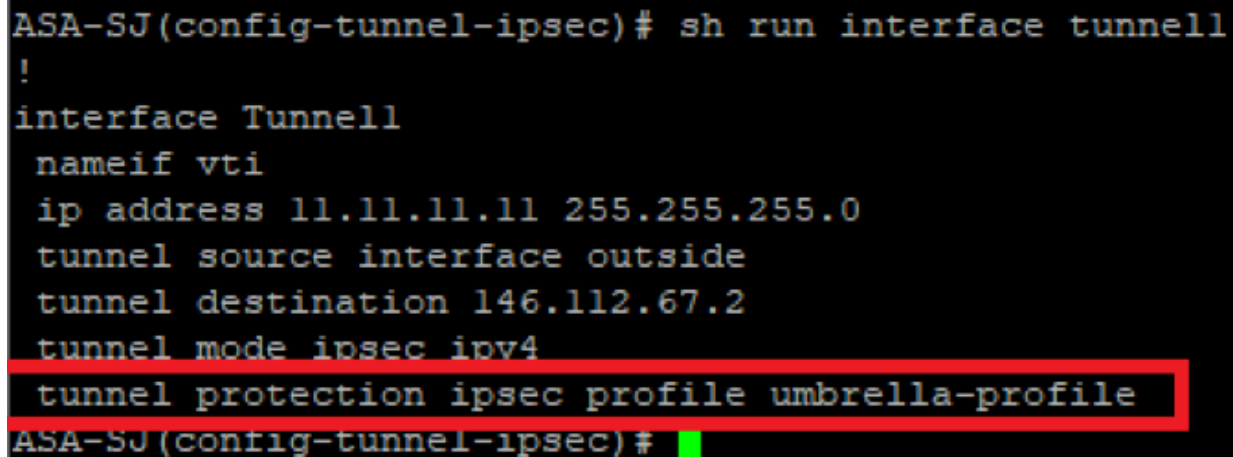


圖片10.png

步驟 5:找到用於隧道介面的IPSec配置檔案

- 1.搜尋隧道介面中正在使用的「crypto ipsec profile」，以便對Umbrella頭端進行基於路由的配置（#替換為對Umbrella的隧道介面使用的ID）：

```
show run interface tunnel#
```



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

圖片11.png

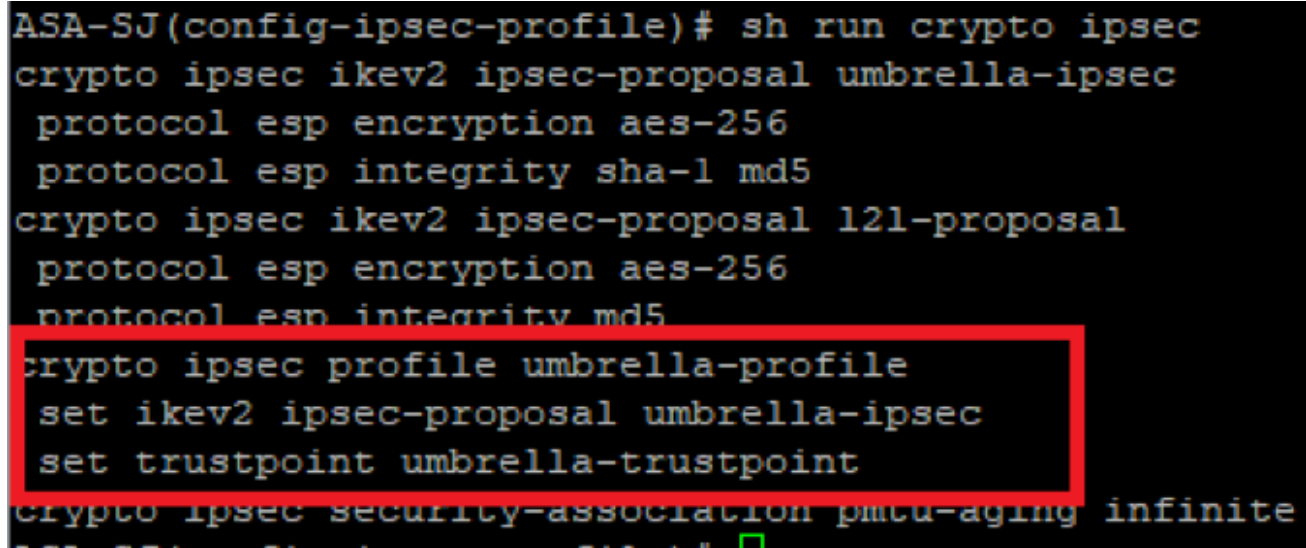
2.如果您不確定通道ID，則可以使用此命令驗證現有通道介面，並確定哪個介面用於基於Umbrella通道的配置：

```
show run interface tunnel
```

步驟 6:從IPSec簡檔中刪除舊信任點

1.從引用隧道的RSA身份驗證的IPSec配置檔案中刪除trustpoint。您可以使用以下命令驗證設定：

```
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.使用以下命令繼續刪除trustpoint:

```
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.確認已從crypto ipsec profile中刪除信任點：

```
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

步驟 7:使用新的Umbrella頭端IP更新通道介面

1.將通道介面的目的地替換為在.8中終止的新Umbrella頭端IP位址。

- 您可以使用此命令驗證當前目標，以便將其替換為新的資料中心IP地址範圍中的IP，該地址範圍可在[Umbrella文檔中找到](#)：

```
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)#
```

圖片15.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.使用命令確認更改：

```
show run interface tunnel#
```

```
ASA-SJ(config-if)# show run interface tunnell
!
interface Tunnell
 nameif vti
 ip address 11.11.11.11 255.255.255.0
 tunnel source interface outside
 tunnel destination 146.112.67.8
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile umbrella-profile
```

Picture17.png

步驟 8:確認新隧道配置已成功建立

1.確認已使用更新的頭端IP正確重新建立與Umbrella的隧道連線，並使用以下命令使用PSK身份驗證：

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

第9步（可選）：刪除舊隧道組

1.刪除指向上一個Umbrella頭端IP範圍。2.的舊通道組。

刪除組態之前，可以使用此命令識別正確的通道：

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 *****
ASA-SJ(config)#
```

Picture20.png

2.使用以下命令刪除舊隧道組的任何引用：

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

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

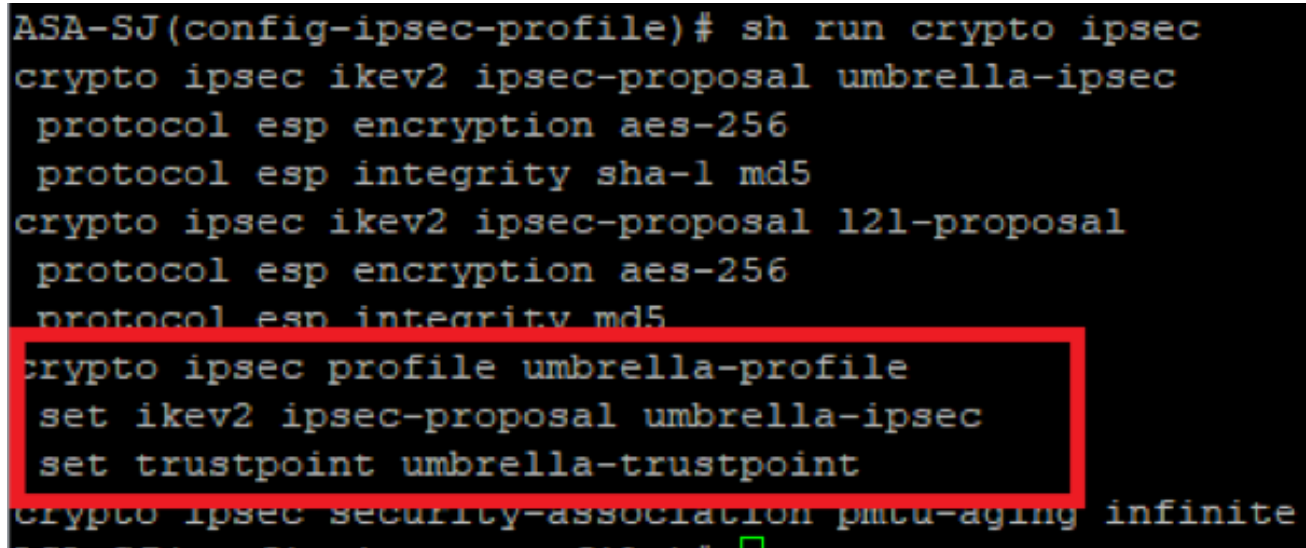
Picture21.png

第10步（可選）：刪除舊信任點

1.使用以下命令，刪除之前使用基於Umbrella隧道的配置所使用的信任點的任何引用：

sh run crypto ipsec

複查「crypto ipsec profile」時可以找到用於信任點的友好名稱：

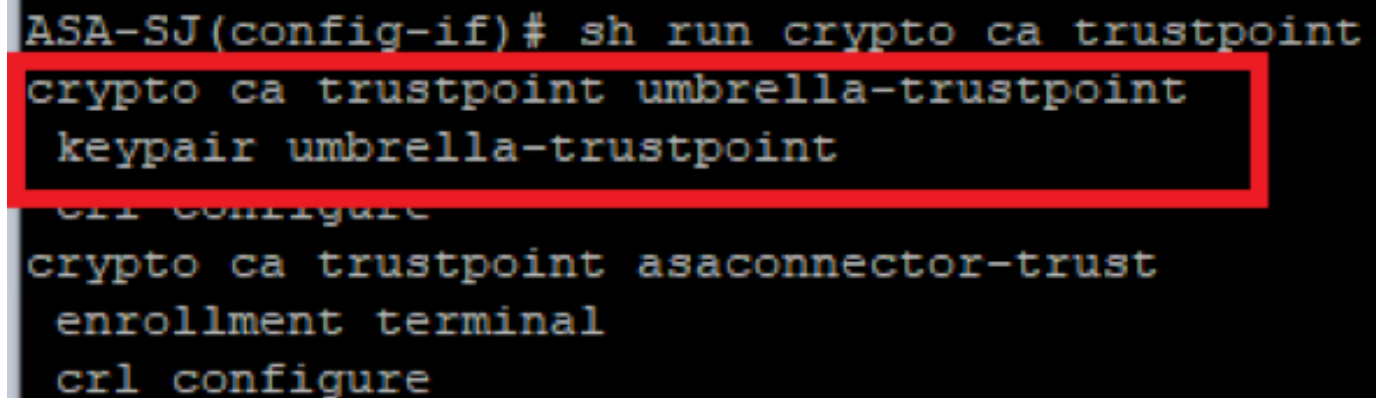


```
ASA-SJ(config-ipsec-profile)# sh run crypto ipsec
crypto ipsec ikev2 ipsec-proposal umbrella-ipsec
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal l2l-proposal
  protocol esp encryption aes-256
  protocol esp integrity md5
crypto ipsec profile umbrella-profile
  set ikev2 ipsec-proposal umbrella-ipsec
  set trustpoint umbrella-trustpoint
crypto ipsec security-association pmtu-aging infinite
```

Picture22.png

2.可以運行此命令來確認信任點配置。確保友好名稱與crypto ipsec profile命令中使用的配置匹配：

```
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.若要取得有關憑證的更多詳細資訊，請使用命令：

```
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.使用以下命令刪除trustpoint:

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

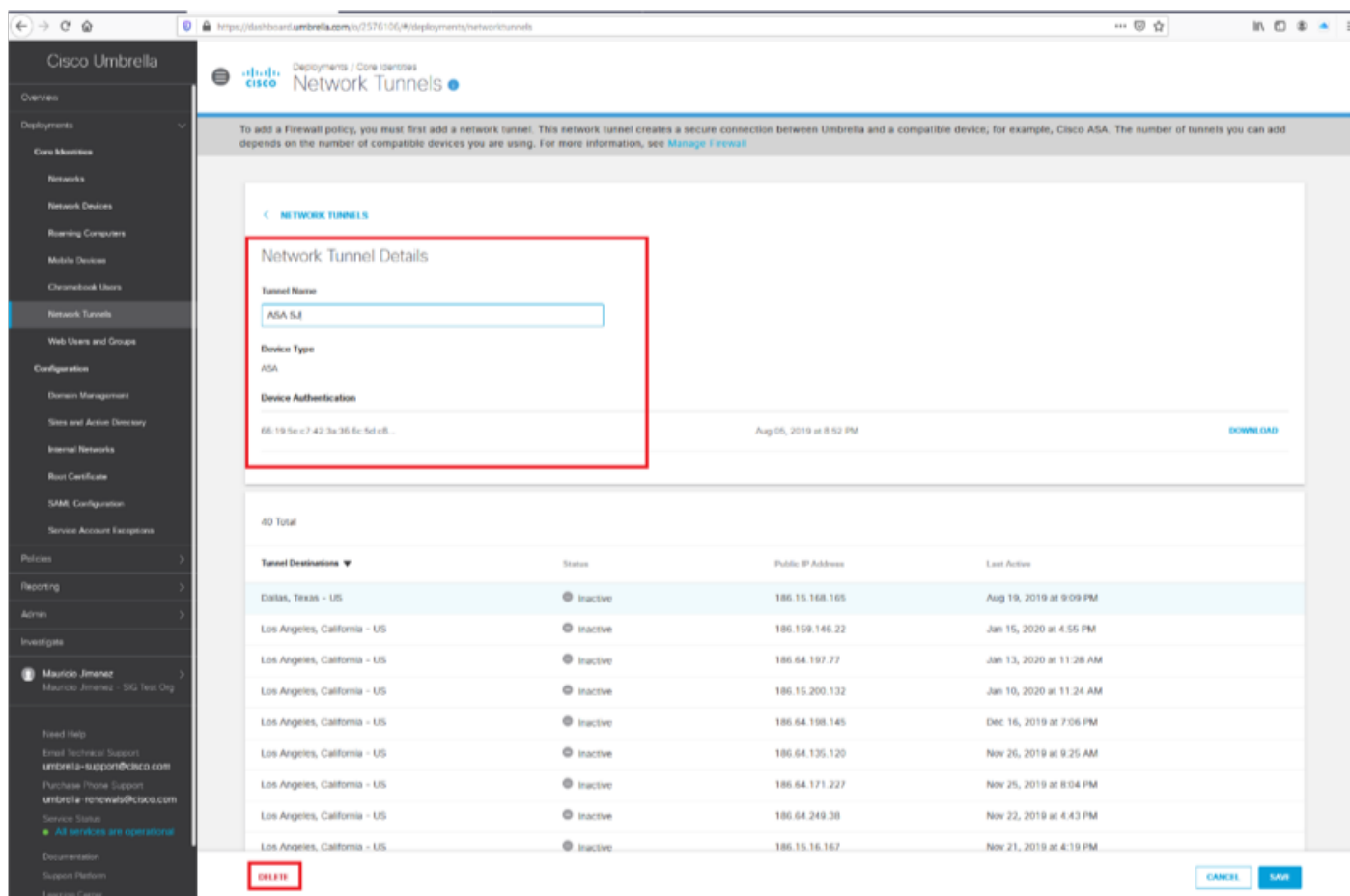
```
ASA-SJ(config)# no crypto ca trustpoint umbrella-trustpoint
WARNING: Removing an enrolled trustpoint will destroy all
certificates received from the related Certificate Authority.

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

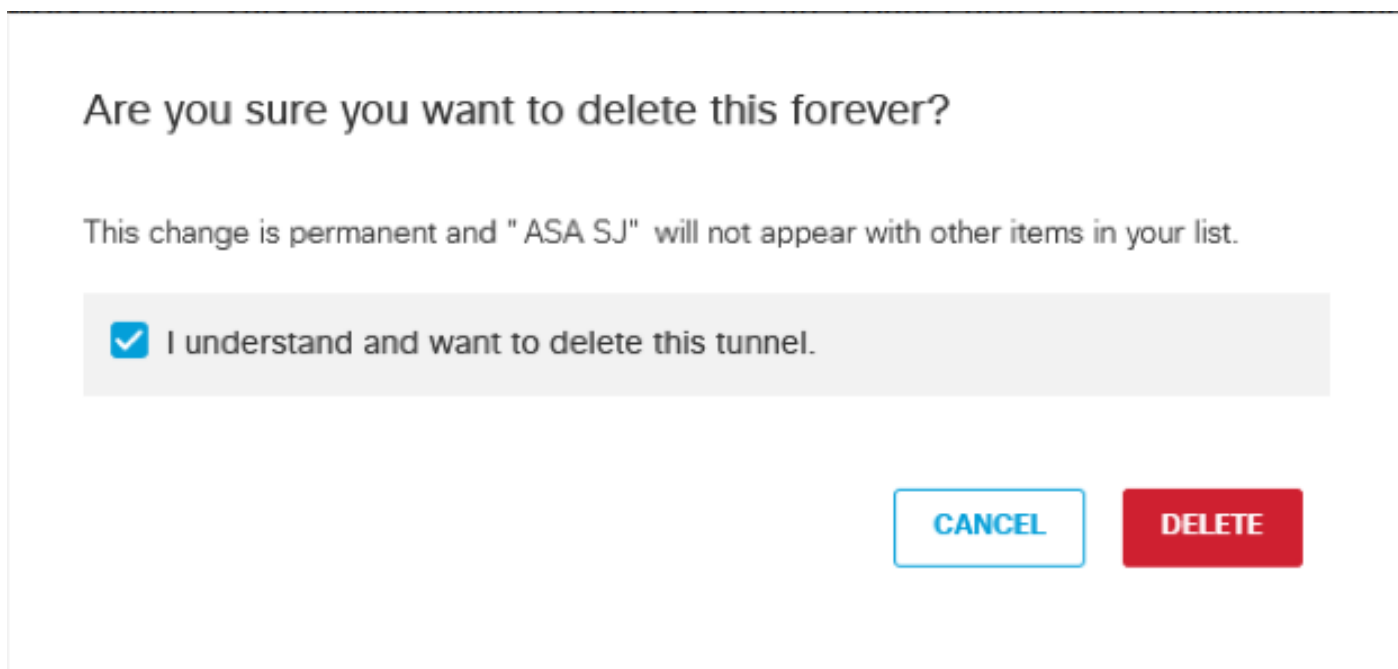
第11步（可選）：刪除舊網路隧道

1.導航到Network Tunnel Details 並選擇Delete，從Umbrella控制面板中刪除舊的網路隧道。



Picture26.png

2.在彈出視窗中選擇「我瞭解並希望刪除此隧道」選項，然後選擇「刪除」，以確認刪除。



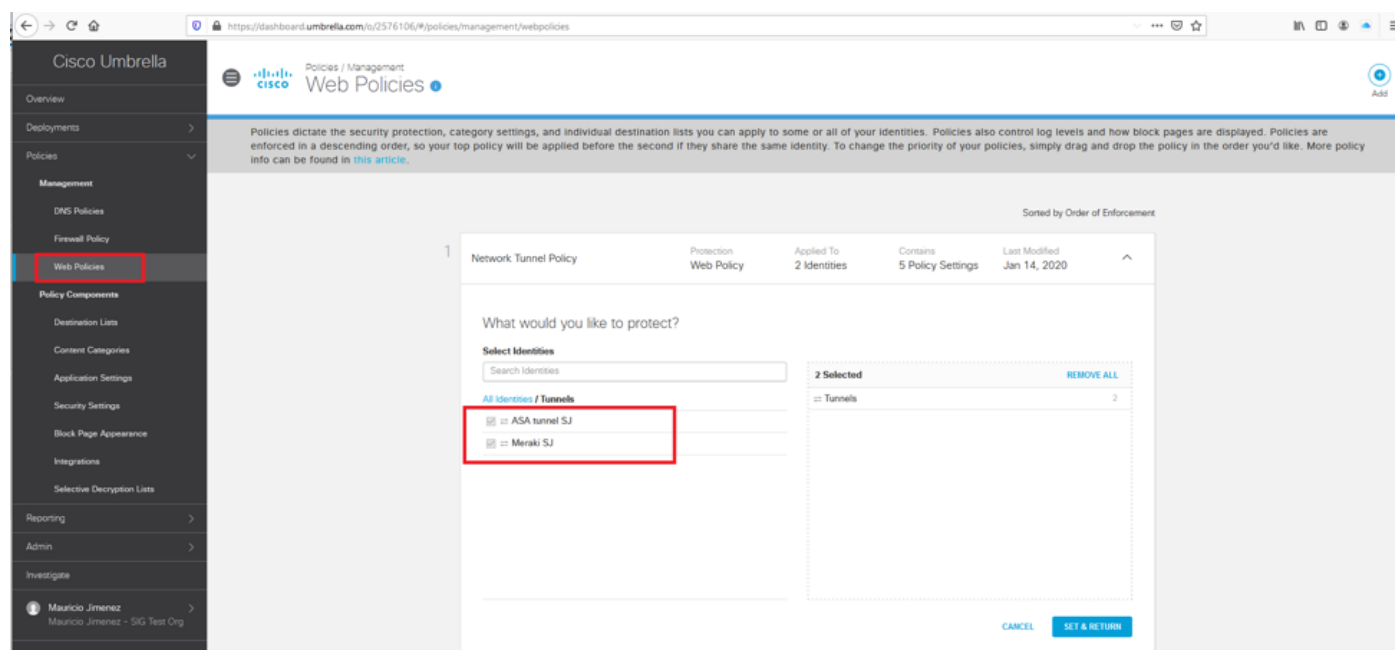
Picture27.png

步驟 12:使用新隧道標識更新Web策略

使用新的網路隧道確認您的Web策略具有更新的身份：

1.在Umbrella控制面板中，導航到Policies > Management > Web Policies。

2.檢視隧道部分，並確認您的Web策略具有使用新網路隧道的更新標識。



Picture28.png

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。