

# 兩個ASA之間的動態站點到站點IKEv2 VPN隧道配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[解決方案1 — 使用DefaultL2LGroup](#)

[靜態ASA配置](#)

[動態ASA](#)

[解決方案2 — 建立使用者定義的隧道組](#)

[靜態ASA配置](#)

[動態ASA配置](#)

[驗證](#)

[在靜態ASA上](#)

[在動態ASA上](#)

[疑難排解](#)

## 簡介

本文檔介紹如何在兩個自適應安全裝置(ASA)之間配置站點到站點Internet金鑰交換版本2(IKEv2)VPN隧道，其中一個具有動態IP地址，另一個具有靜態IP地址。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA版本5505

- ASA版本9.1(5)

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

此配置的設定方法有兩種：

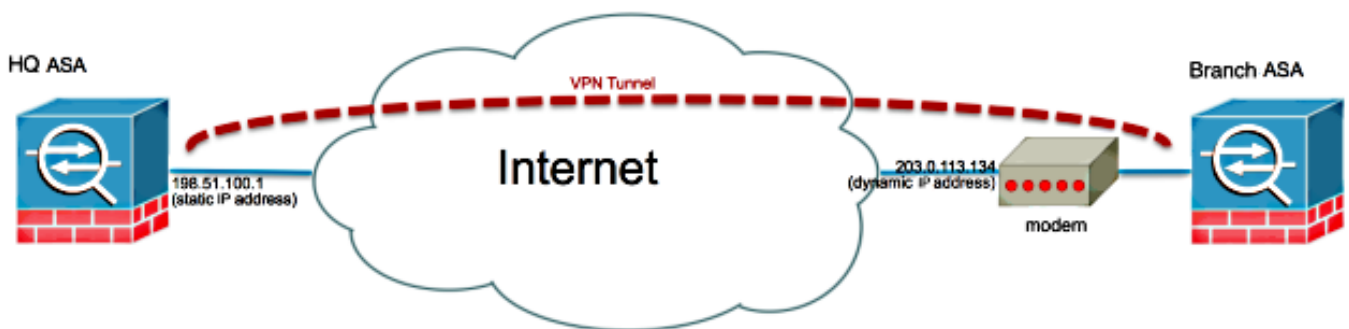
- 使用DefaultL2LGroup隧道組
- 具有命名隧道組

這兩種方案之間最大的配置差異是遠端ASA使用的網際網路安全關聯和金鑰管理協定(ISAKMP)ID。在靜態ASA上使用DefaultL2LGroup時，對等體的ISAKMP ID必須是地址。但是，如果使用命名隧道組，則對等體的ISAKMP ID必須與使用以下命令的隧道組名稱相同：

```
crypto isakmp identity key-id
```

在靜態ASA上使用命名隧道組的優勢在於，在使用DefaultL2LGroup時，遠端動態ASA上的配置（包括預共用金鑰）必須相同，並且不允許在策略設定中有太多粒度。

## 網路圖表



## 設定

本節介紹每個ASA上的配置，具體取決於您決定使用的解決方案。

### 解決方案1 — 使用DefaultL2LGroup

當一個ASA動態獲取其地址時，這是配置兩個ASA之間的LAN到LAN(L2L)隧道的最簡單方法。DefaultL2L組是ASA上預配置的隧道組，所有未明確匹配任何特定隧道組的連線都位於此連線上。由於動態ASA沒有固定的預定IP地址，這意味著管理員無法配置靜態ASA以允許特定隧道組上的連

線。在這種情況下，可使用DefaultL2L組來允許動態連線。

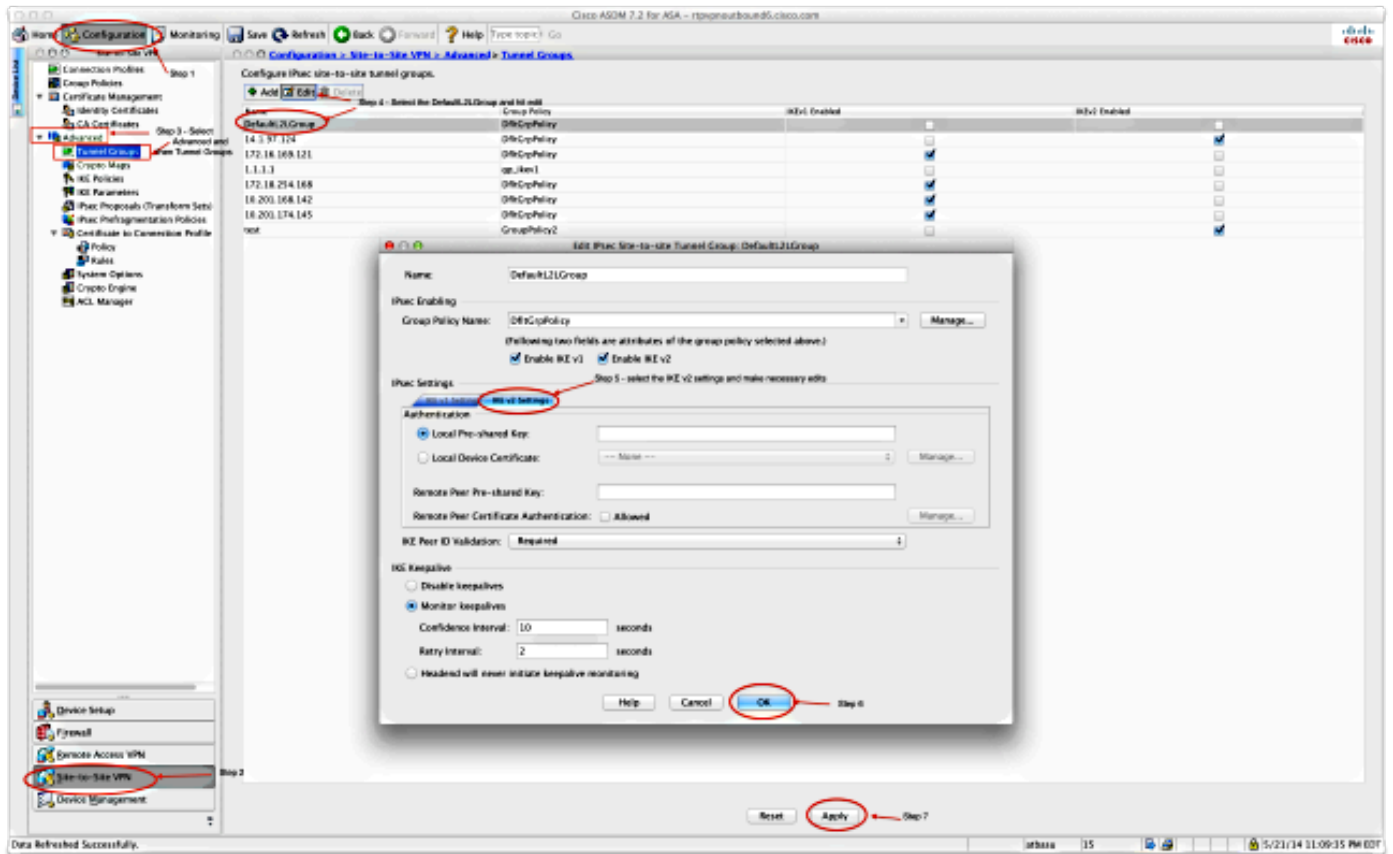
**提示：**使用此方法，缺點是所有對等體將具有相同的預共用金鑰，因為每個隧道組只能定義一個預共用金鑰，並且所有對等體將連線到同一個DefaultL2LGroup隧道組。

## 靜態ASA配置

```
interface Ethernet0/0
 nameif inside
 security-level 100
 IP address 172.30.2.6 255.255.255.0
!
interface Ethernet0/3
 nameif Outside
 security-level 0
 IP address 207.30.43.15 255.255.255.128
!
boot system disk0:/asa915-k8.bin
crypto ipsec IKEv2 ipsec-proposal Site2Site
 protocol esp encryption aes-256
 protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto engine large-mod-accel
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 10 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev1 transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-
256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map Outside_map interface Outside
crypto IKEv2 policy 2
 encryption aes-256
 integrity sha512
 group 24
 prf sha512
 lifetime seconds 86400
crypto IKEv2 policy 3
 encryption aes-256
 integrity sha group 5 2
 prf sha
 lifetime seconds 86400
```

```
crypto IKEv2 policy 10
  encryption aes-192
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 20
  encryption aes
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 30
  encryption 3des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 40
  encryption des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 enable inside client-services port 443
crypto IKEv2 enable Outside client-services port 443
group-policy Site2Site internal
group-policy Site2Site attributes
  vpn-idle-timeout none
  vpn-session-timeout none
  vpn-filter none
  vpn-tunnel-protocol IKEv2
tunnel-group DefaultL2LGroup general-attributes
  default-group-policy Site2Site
tunnel-group DefaultL2LGroup ipsec-attributes
  IKEv2 remote-authentication pre-shared-key *****
  IKEv2 local-authentication pre-shared-key *****
```

在自適應安全裝置管理器(ASDM)上，可以配置DefaultL2LGroup，如下所示：



## 動態ASA

```

interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 IP address 172.16.1.1 255.255.255.224
!
interface Vlan2
 nameif outside
 security-level 0
 IP address dhcp setroute
!
ftp mode passive
object network NETWORK_OBJ_172.16.1.0_24
 subnet 172.16.1.0 255.255.255.0

```

```
object-group network DM_INLINE_NETWORK_1
  network-object object 10.0.0.0
  network-object object 172.0.0.0
access-list outside_cryptomap extended permit IP 172.16.1.0 255.255.255.0
object-group DM_INLINE_NETWORK_1
nat (inside,outside) source static NETWORK_OBJ_172.16.1.0_24 NETWORK_OBJ_
172.16.1.0_24 destination static DM_INLINE_NETWORK_1 DM_INLINE_NETWORK_1
nat (inside,outside) source dynamic any interface
crypto ipsec IKEv2 ipsec-proposal Site2Site
  protocol esp encryption aes-256
  protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal DES
  protocol esp encryption des
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
  protocol esp encryption 3des
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
  protocol esp encryption aes
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set pfs group5
crypto map outside_map 1 set peer 198.51.100.1
crypto map outside_map 1 set ikev1 phase1-mode aggressive group5
crypto map outside_map 1 set IKEv2 ipsec-proposal Site2Site
crypto map outside_map interface outside
crypto IKEv2 policy 2
  encryption aes-256
  integrity sha512
  group 24
  prf sha512
  lifetime seconds 86400
crypto IKEv2 policy 3
  encryption aes-256
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 10
  encryption aes-192
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 20
  encryption aes
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 30
  encryption 3des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 40
```

```

encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 enable outside
management-access inside
group-policy GroupPolicy_198.51.100.1 internal
group-policy GroupPolicy_198.51.100.1 attributes
  vpn-tunnel-protocol IKEv2
tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 general-attributes
  default-group-policy GroupPolicy_198.51.100.1
tunnel-group 198.51.100.1 ipsec-attributes
  ikev1 pre-shared-key *****
  IKEv2 remote-authentication pre-shared-key *****
  IKEv2 local-authentication pre-shared-key *****

```

在ASDM上，您可以使用標準嚮導來設定適當的連線配置檔案，也可以簡單地新增新連線並遵循標準過程。

## 解決方案2 — 建立使用者定義的隧道組

此方法需要稍多的配置，但允許更精細的配置。每個對等體可以有自己的單獨策略和預共用金鑰。但是，在此必須更改動態對等體上的ISAKMP ID，以便它使用名稱而不是IP地址。這允許靜態ASA將傳入的ISAKMP初始化請求與正確的隧道組匹配，並使用正確的策略。

### 靜態ASA配置

```

interface Ethernet0/0
  nameif inside
  security-level 100
  IP address 172.16.0.1 255.255.255.0
!
interface Ethernet0/3
  nameif Outside
  security-level 0
  IP address 198.51.100.1 255.255.255.128
!
boot system disk0:/asa915-k8.bin
object-group network DM_INLINE_NETWORK_1
  network-object object 10.0.0.0
  network-object object 172.0.0.0

access-list Outside_cryptomap_1 extended permit IP object-group DM_INLINE_NETWORK_
1 172.16.1.0 255.255.255.0

crypto ipsec IKEv2 ipsec-proposal Site2Site
  protocol esp encryption aes-256
  protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
  protocol esp encryption aes

```

```
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
protocol esp encryption 3des
protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto engine large-mod-accel
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev1 transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-
SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set IKEv2 ipsec-proposal
AES256 AES192 AES 3DES DES
crypto dynamic-map DynamicSite2Site1 4 match address Outside_cryptomap_1
crypto dynamic-map DynamicSite2Site1 4 set IKEv2 ipsec-proposal Site2Site
crypto map Outside_map 65534 ipsec-isakmp dynamic DynamicSite2Site1
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map Outside_map interface Outside

crypto IKEv2 policy 2
encryption aes-256
integrity sha512
group 24
prf sha512
lifetime seconds 86400
crypto IKEv2 policy 3
encryption aes-256
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 policy 10
encryption aes-192
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 policy 20
encryption aes
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 policy 30
encryption 3des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 policy 40
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 enable Outside client-services port 443
management-access inside

group-policy GroupPolicy4 internal
group-policy GroupPolicy4 attributes
vpn-tunnel-protocol IKEv2

tunnel-group DynamicSite2Site1 type ipsec-l2l
```

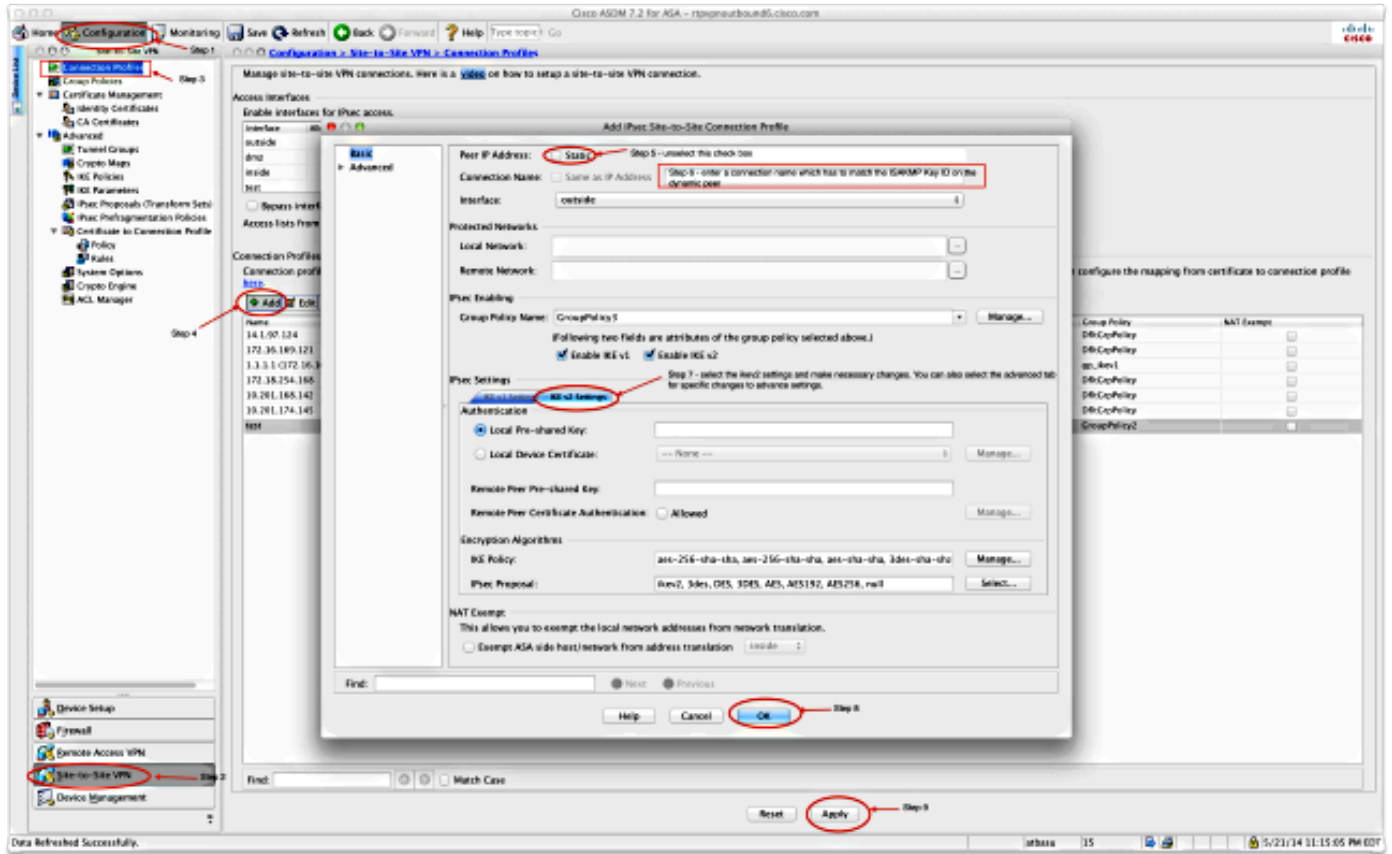


```

tunnel-group DynamicSite2Site1 general-attributes
 default-group-policy GroupPolicy4
tunnel-group DynamicSite2Site1 ipsec-attributes
 IKEv2 remote-authentication pre-shared-key *****
 IKEv2 local-authentication pre-shared-key *****

```

在ASDM上，連線配置檔名稱預設為IP地址。因此，建立它時，必須對其進行更改，以便為其指定一個名稱，如下面的螢幕截圖所示：



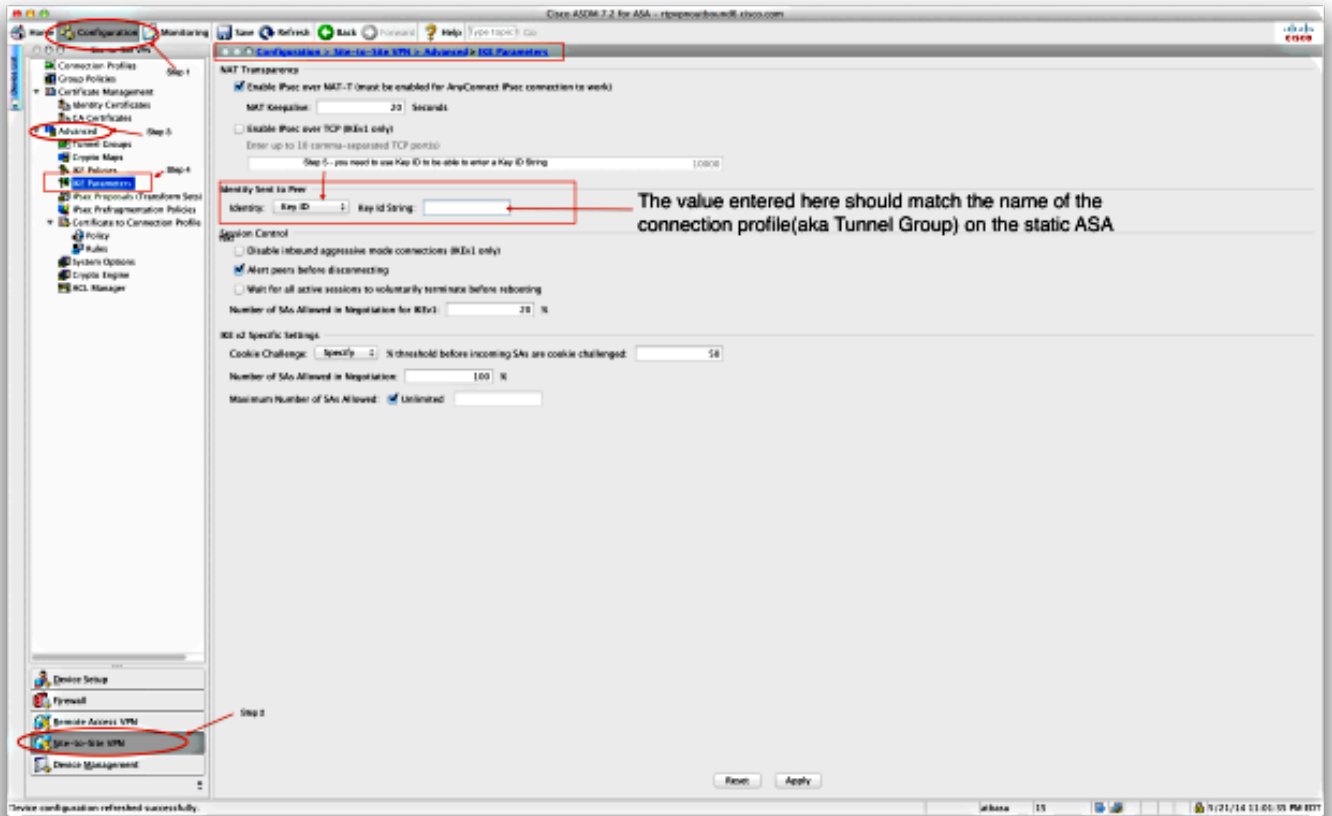
## 動態ASA配置

動態ASA的配置方式幾乎相同，新增了一個命令，如下所示：

```
crypto isakmp identity key-id DynamicSite2Site1
```

如前所述，預設情況下，ASA使用VPN隧道對映到的介面的IP地址作為ISAKMP金鑰ID。但是在這種情況下，動態ASA上的金鑰ID與靜態ASA上的隧道組的名稱相同。因此，在每個動態對等體上，金鑰ID將不同，並且必須在靜態ASA上使用正確的名稱建立相應的隧道組。

在ASDM上，可按如下螢幕截圖所示進行配置：



## 驗證

使用本節內容，確認您的組態是否正常運作。

## 在靜態ASA上

以下是show crypto IKEv2 sa det命令的結果：

IKEv2 SAs:

Session-id:132, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id          Local              Remote            Status            Role
1574208993        198.51.100.1/4500 203.0.113.134/4500  READY            RESPONDER
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:24, Auth sign: PSK,
Auth verify: PSK
Life/Active Time: 86400/352 sec
Session-id: 132
Status Description: Negotiation done
Local spi: 4FDF215BDEC73EC      Remote spi: 2414BEA1E10E3F70
Local id: 198.51.100.1
Remote id: DynamicSite2Site1
Local req mess id: 13           Remote req mess id: 17
Local next mess id: 13         Remote next mess id: 17
Local req queued: 13           Remote req queued: 17
Local window: 1                Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is detected outside
```

```
Child sa: local selector 172.0.0.0/0 - 172.255.255.255/65535
remote selector 172.16.1.0/0 - 172.16.1.255/65535
ESP spi in/out: 0x9fd5c736/0x6c5b3cc9
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

以下是show crypto ipsec sa命令的結果：

```
interface: Outside
Crypto map tag: DynamicSite2Site1, seq num: 4, local addr: 198.51.100.1

access-list Outside_cryptomap_1 extended permit IP 172.0.0.0 255.0.0.0
172.16.1.0 255.255.255.0
local ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 203.0.113.134

#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 12, #pkts decrypt: 12, #pkts verify: 12
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1, #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.: 198.51.100.1/4500, remote crypto endpt.:
203.0.113.134/4500
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: 6C5B3CC9
current inbound spi : 9FD5C736

inbound esp sas:
spi: 0x9FD5C736 (2681587510)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
slot: 0, conn_id: 1081344, crypto-map: DynamicSite2Site1
sa timing: remaining key lifetime (kB/sec): (4193279/28441)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00001FFF

outbound esp sas:
spi: 0x6C5B3CC9 (1817918665)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
slot: 0, conn_id: 1081344, crypto-map: DynamicSite2Site1
sa timing: remaining key lifetime (kB/sec): (3962879/28441)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

## 在動態ASA上

以下是show crypto IKEv2 sa detail命令的結果：

IKEv2 SAs:

Session-id:11, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id          Local              Remote            Status            Role
1132933595        192.168.50.155/4500  198.51.100.1/4500  READY            INITIATOR
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:24, Auth sign: PSK,
Auth verify: PSK
  Life/Active Time: 86400/267 sec
  Session-id: 11
  Status Description: Negotiation done
  Local spi: 2414BEA1E10E3F70      Remote spi: 4FDFF215BDEC73EC
  Local id: DynamicSite2Site1
  Remote id: 198.51.100.1
  Local req mess id: 13             Remote req mess id: 9
  Local next mess id: 13           Remote next mess id: 9
  Local req queued: 13             Remote req queued: 9
  Local window: 1                  Remote window: 1
  DPD configured for 10 seconds, retry 2
  NAT-T is detected inside
Child sa: local selector 172.16.1.0/0 - 172.16.1.255/65535
  remote selector 172.0.0.0/0 - 172.255.255.255/65535
  ESP spi in/out: 0x6c5b3cc9/0x9fd5c736
  AH spi in/out: 0x0/0x0
  CPI in/out: 0x0/0x0
  Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
  ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

以下是show crypto ipsec sa命令的結果：

```
interface: outside
  Crypto map tag: outside_map, seq num: 1, local addr: 192.168.50.155

  access-list outside_cryptomap extended permit IP 172.16.1.0 255.255.255.0
172.0.0.0 255.0.0.0
  local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
  current_peer: 198.51.100.1

  #pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
  #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 12, #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.: 192.168.50.155/4500, remote crypto endpt.:
198.51.100.1/4500
  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: 9FD5C736
  current inbound spi : 6C5B3CC9

inbound esp sas:
  spi: 0x6C5B3CC9 (1817918665)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, NAT-T-Encaps, PFS Group 5, IKEv2, }
  slot: 0, conn_id: 77824, crypto-map: outside_map
```

```
sa timing: remaining key lifetime (kB/sec): (4008959/28527)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
  0x00000000 0x00000003
outbound esp sas:
spi: 0x9FD5C736 (2681587510)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, PFS Group 5, IKEv2, }
slot: 0, conn_id: 77824, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4147199/28527)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
  0x00000000 0x00000001
```

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

**附註：** 使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

- deb crypto IKEv2 packet
- deb crypto IKEv2 internal