

# Exemple de configuration d'un tunnel VPN IKEv2 site à site dynamique entre deux ASA

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configuration](#)

[Solution 1 - Utilisation du groupe DefaultL2LG](#)

[Configuration statique ASA](#)

[ASA dynamique](#)

[Solution 2 - Créer un groupe de tunnels défini par l'utilisateur](#)

[Configuration statique ASA](#)

[Configuration dynamique ASA](#)

[Vérification](#)

[Sur l'ASA statique](#)

[Sur l'ASA dynamique](#)

[Dépannage](#)

## Introduction

Ce document décrit comment configurer un tunnel VPN IKEv2 (Internet Key Exchange version 2) site à site entre deux appliances de sécurité adaptatives (ASA) où un ASA a une adresse IP dynamique et l'autre une adresse IP statique.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA version 5505
- ASA version 9.1(5)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informations générales

Cette configuration peut être configurée de deux manières :

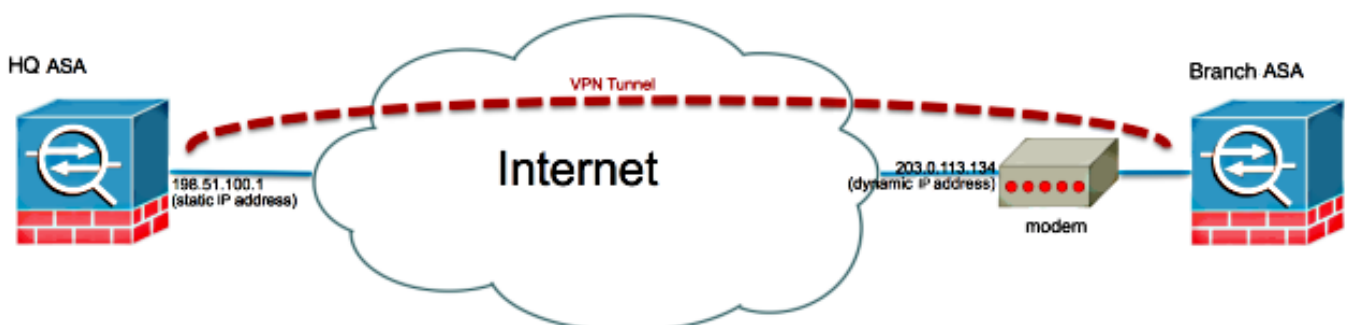
- Avec le groupe de tunnels DefaultL2LGroup
- Avec un groupe de tunnels nommé

La plus grande différence de configuration entre les deux scénarios est l'ID ISAKMP (Internet Security Association) et l'ID de protocole de gestion de clé utilisé par l'ASA distant. Lorsque DefaultL2LGroup est utilisé sur l'ASA statique, l'ID ISAKMP de l'homologue doit être l'adresse. Cependant, si un groupe de tunnels nommé est utilisé, l'ID ISAKMP de l'homologue doit être identique au nom du groupe de tunnels à l'aide de cette commande :

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

L'avantage de l'utilisation de groupes de tunnels nommés sur l'ASA statique est que lorsque le groupe DefaultL2LG est utilisé, la configuration sur les ASA dynamiques distants, qui inclut les clés pré-partagées, doit être identique et ne permet pas une grande granularité avec la configuration des stratégies.

## Diagramme du réseau



## Configuration

Cette section décrit la configuration de chaque ASA en fonction de la solution que vous décidez d'utiliser.

## Solution 1 - Utilisation du groupe DefaultL2LG

Il s'agit de la façon la plus simple de configurer un tunnel LAN à LAN (L2L) entre deux ASA lorsqu'un ASA obtient son adresse dynamiquement. Le groupe DefaultL2L est un groupe de tunnels préconfiguré sur l'ASA et toutes les connexions qui ne correspondent explicitement à aucun groupe de tunnels particulier tombent sur cette connexion. Puisque l'ASA dynamique ne possède pas d'adresse IP prédéfinie constante, cela signifie que l'administrateur ne peut pas configurer l'ASA statique afin d'autoriser la connexion sur un groupe de tunnels spécifique. Dans cette situation, le groupe DefaultL2L peut être utilisé afin d'autoriser les connexions dynamiques.

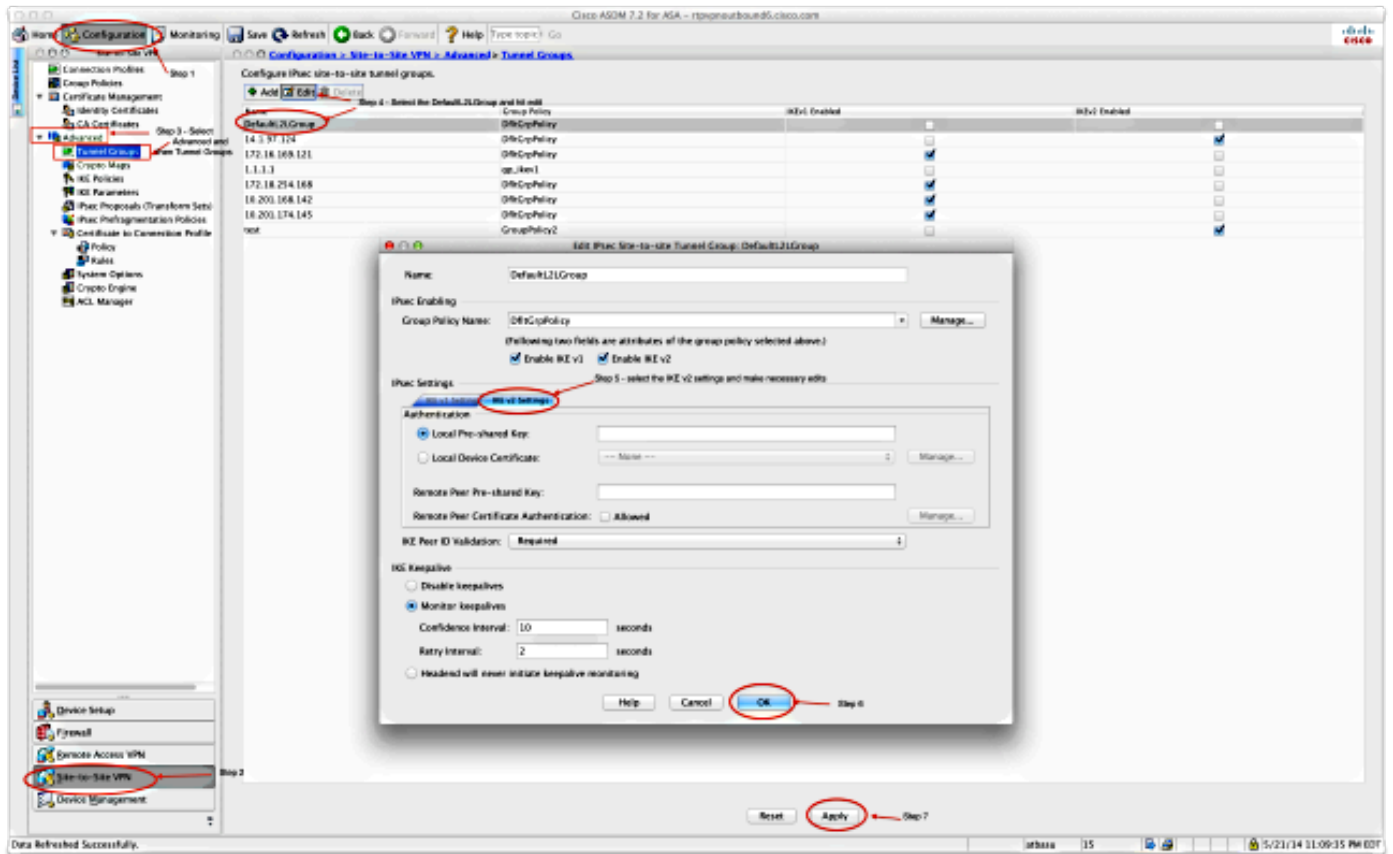
**Conseil :** avec cette méthode, l'inconvénient est que tous les homologues auront la même clé pré-partagée, car une seule clé pré-partagée peut être définie par groupe de tunnels et tous les homologues se connecteront au même groupe de tunnels DefaultL2LGroup.

### Configuration statique ASA

```
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 *****
```

Sur l'ASDM (Adaptive Security Device Manager), vous pouvez configurer le groupe L2LG par défaut comme indiqué ici :



## ASA dynamique

```

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 *****

```

Sur l'ASDM, vous pouvez utiliser l'assistant standard afin de configurer le profil de connexion approprié ou vous pouvez simplement ajouter une nouvelle connexion et suivre la procédure standard.

## Solution 2 - Créer un groupe de tunnels défini par l'utilisateur

Cette méthode nécessite un peu plus de configuration, mais elle permet une plus grande granularité. Chaque homologue peut avoir sa propre politique et sa clé pré-partagée. Cependant, il est important de modifier l'ID ISAKMP sur l'homologue dynamique afin qu'il utilise un nom au lieu d'une adresse IP. Cela permet à l'ASA statique de faire correspondre la demande d'initialisation ISAKMP entrante au groupe de tunnels de droite et d'utiliser les stratégies appropriées.

### Configuration statique ASA

```

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

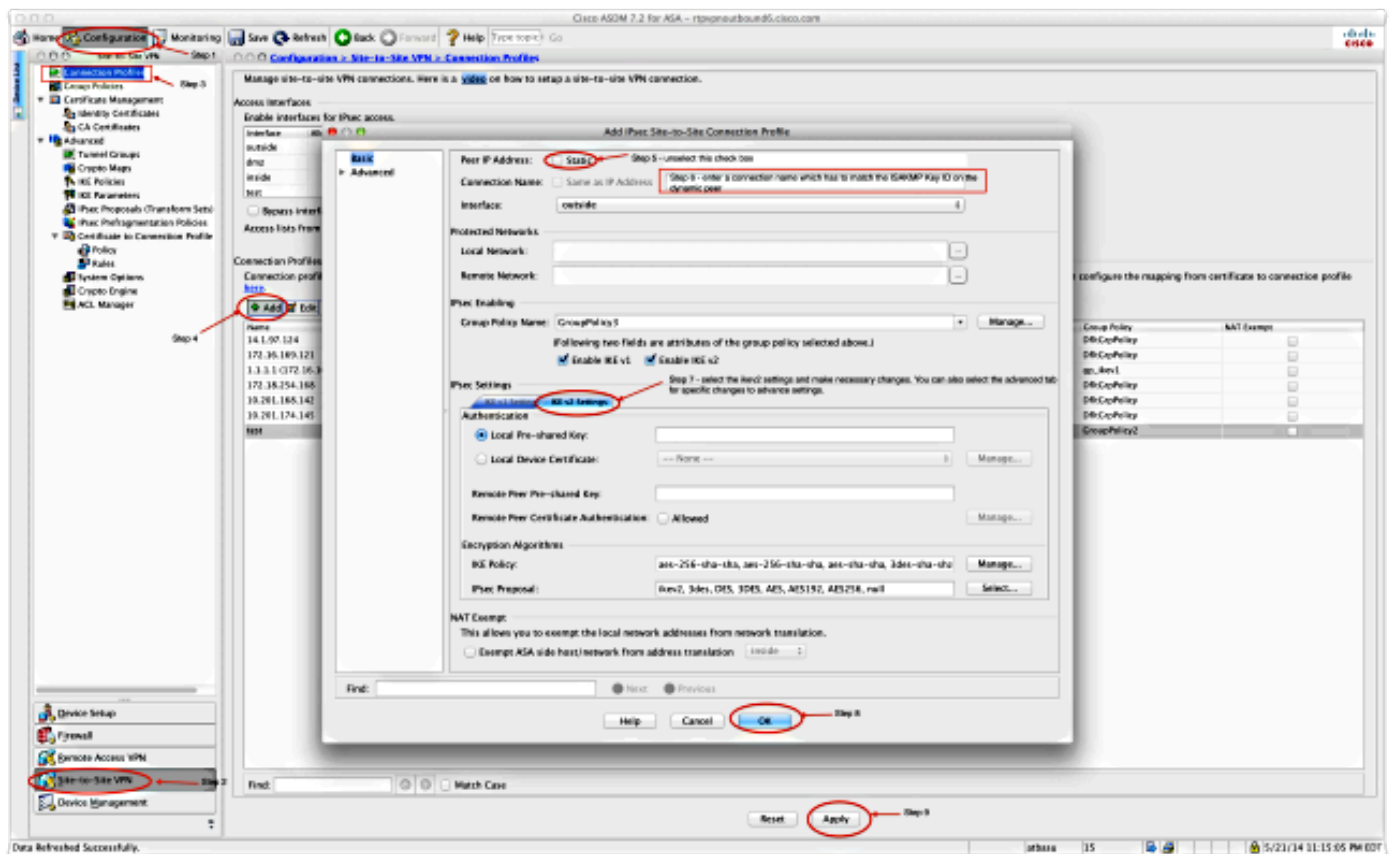
group-policy GroupPolicy4 internal
```



```
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 *****
```

Sur l'ASDM, le nom du profil de connexion est une adresse IP par défaut. Ainsi, lorsque vous le créez, vous devez le modifier afin de lui donner un nom comme indiqué dans la capture d'écran ici :



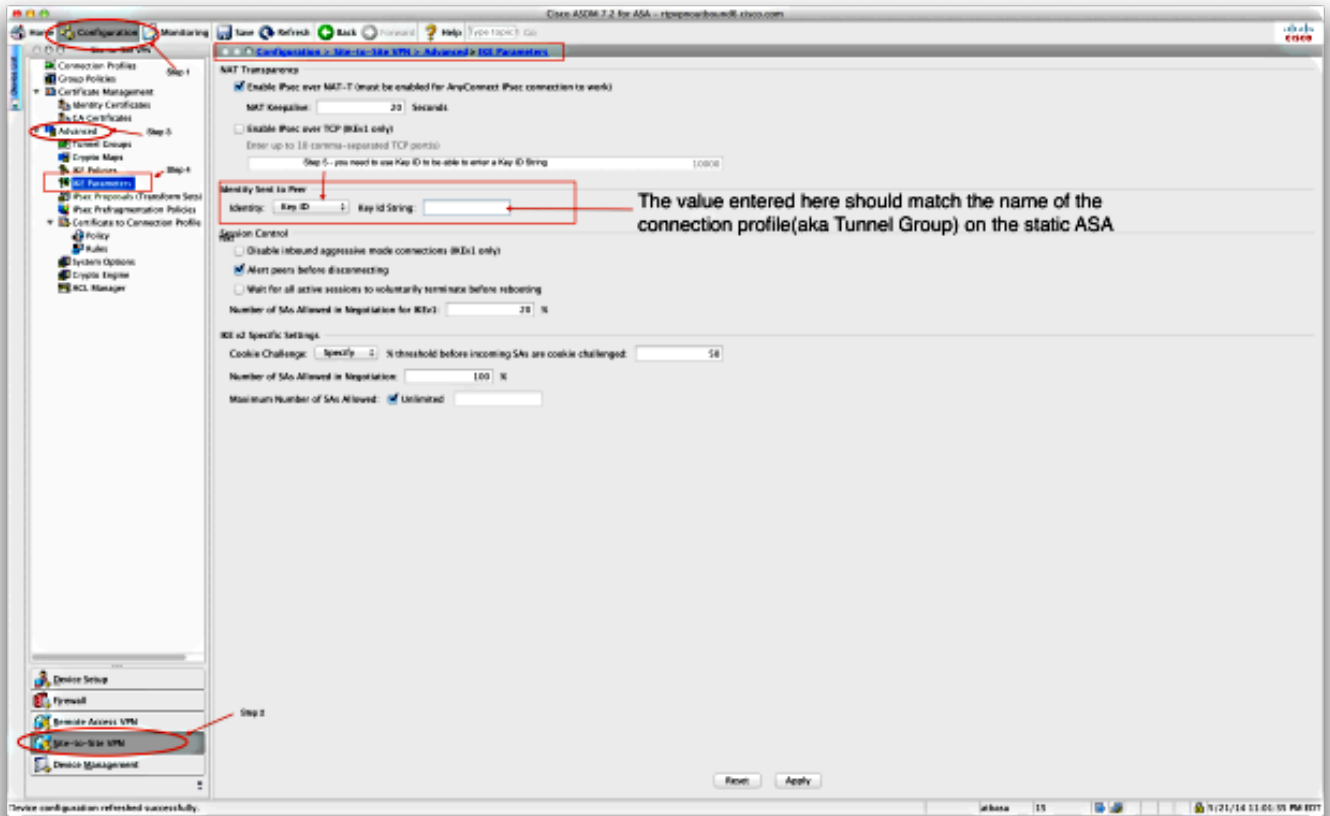
## Configuration dynamique ASA

La configuration de l'ASA dynamique est presque identique dans les deux solutions, avec l'ajout d'une commande, comme illustré ici :

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

Comme décrit précédemment, par défaut, l'ASA utilise l'adresse IP de l'interface à laquelle le tunnel VPN est mappé en tant qu'ID de clé ISAKMP. Cependant, dans ce cas, l'ID de clé sur l'ASA dynamique est identique au nom du groupe de tunnels sur l'ASA statique. Ainsi, sur chaque homologue dynamique, l'ID de clé sera différent et un groupe de tunnels correspondant doit être créé sur l'ASA statique avec le bon nom.

Sur l'ASDM, ceci peut être configuré comme indiqué dans cette capture d'écran :



## Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

## Sur l'ASA statique

Voici le résultat de la commande `show cryptoIKEv2 SA det` :

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
```

## Voici le résultat de la commande **show crypto ipsec sa** :

```
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
```

## Sur l'ASA dynamique

Voici le résultat de la commande **show crypto IKE v2 SA detail** :

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
```

**Voici le résultat de la commande show crypto ipsec sa :**

```
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
```

L'[Outil d'interprétation de sortie \(clients enregistrés seulement\) prend en charge certaines commandes d'affichage](#). Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

L'[Outil d'interprétation de sortie \(clients enregistrés seulement\) prend en charge certaines commandes d'affichage](#). Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

**Note:** Référez-vous aux [informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage](#).

- deb crypto paquet IKEv2
- deb crypto IKEv2 interne