Dynamische site naar site IKEv2 VPN-tunnel tussen twee ASA's Configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een site-to-site Internet Key Exchange, versie 2 (IKEv2) VPN-tunnel tussen twee adaptieve security applicaties (ASA's) kunt configureren, waarbij de ene ASA een dynamisch IP-adres heeft en de andere een statisch IP-adres heeft.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA versie 5505
- ASA versie 9.1(5)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Er zijn twee manieren waarop deze configuratie kan worden ingesteld:

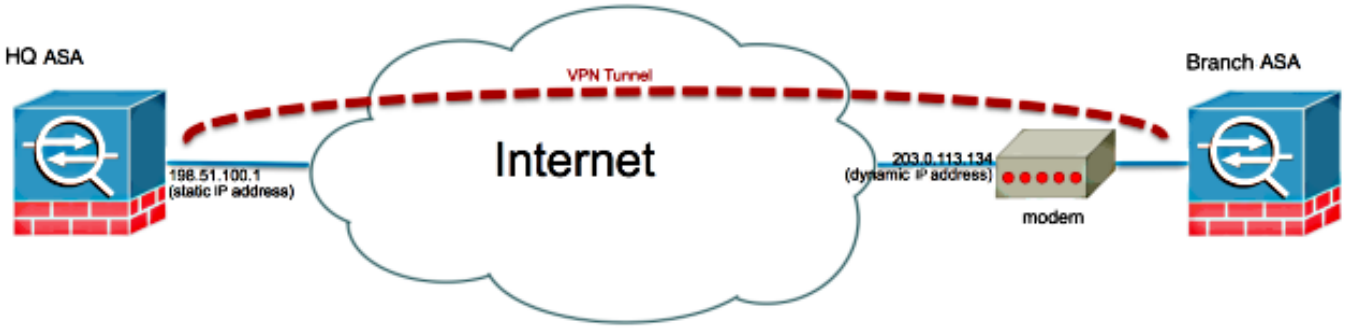
- Met de groep DefaultL2LG
- Met een naam van een tunnelgroep

Het grootste configuratieverschil tussen de twee scenario's is de ISAKMP-id (Internet Security Association and Key Management Protocol) die door de afgelegen ASA werd gebruikt. Wanneer de DefaultL2LGgroup op de statische ASA wordt gebruikt, moet de ISAKMP-ID van de peer het adres zijn. Als echter een genoemde tunnelgroep wordt gebruikt, moet ISAKMP-ID van de peer dezelfde naam hebben als de tunnelgroep die deze opdracht gebruikt:

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

Het voordeel van het gebruik van genoemde tunnelgroepen op de statische ASA is dat wanneer de DefaultL2LGgroup wordt gebruikt, de configuratie op de externe dynamische ASA's, die de vooraf gedeelde toetsen bevat, identiek moet zijn en niet veel granulariteit met de instelling van beleid toelaat.

Netwerkdiagram



Configureren

In dit gedeelte wordt de configuratie van elke ASA beschreven, afhankelijk van de oplossing die u

wilt gebruiken.

Oplossing 1 - Gebruik van de DefaultL2LG-groep

Dit is de eenvoudigste manier om een LAN-to-LAN (L2L) tunnel tussen twee ASA's te configureren wanneer één ASA-adres dynamisch wordt ontvangen. De DefaultL2L Group is een vooraf geconfigureerd tunnelgroep op de ASA en alle verbindingen die niet expliciet overeenkomen met een bepaalde tunnelgroep vallen op deze verbinding. Aangezien de Dynamische ASA geen constant vooraf bepaald IP adres heeft, betekent het dat de admin de Statis ASA niet kan configureren om de verbinding op een specifieke tunnelgroep toe te staan. In deze situatie kan de DefaultL2L Group gebruikt worden om de dynamische verbindingen mogelijk te maken.

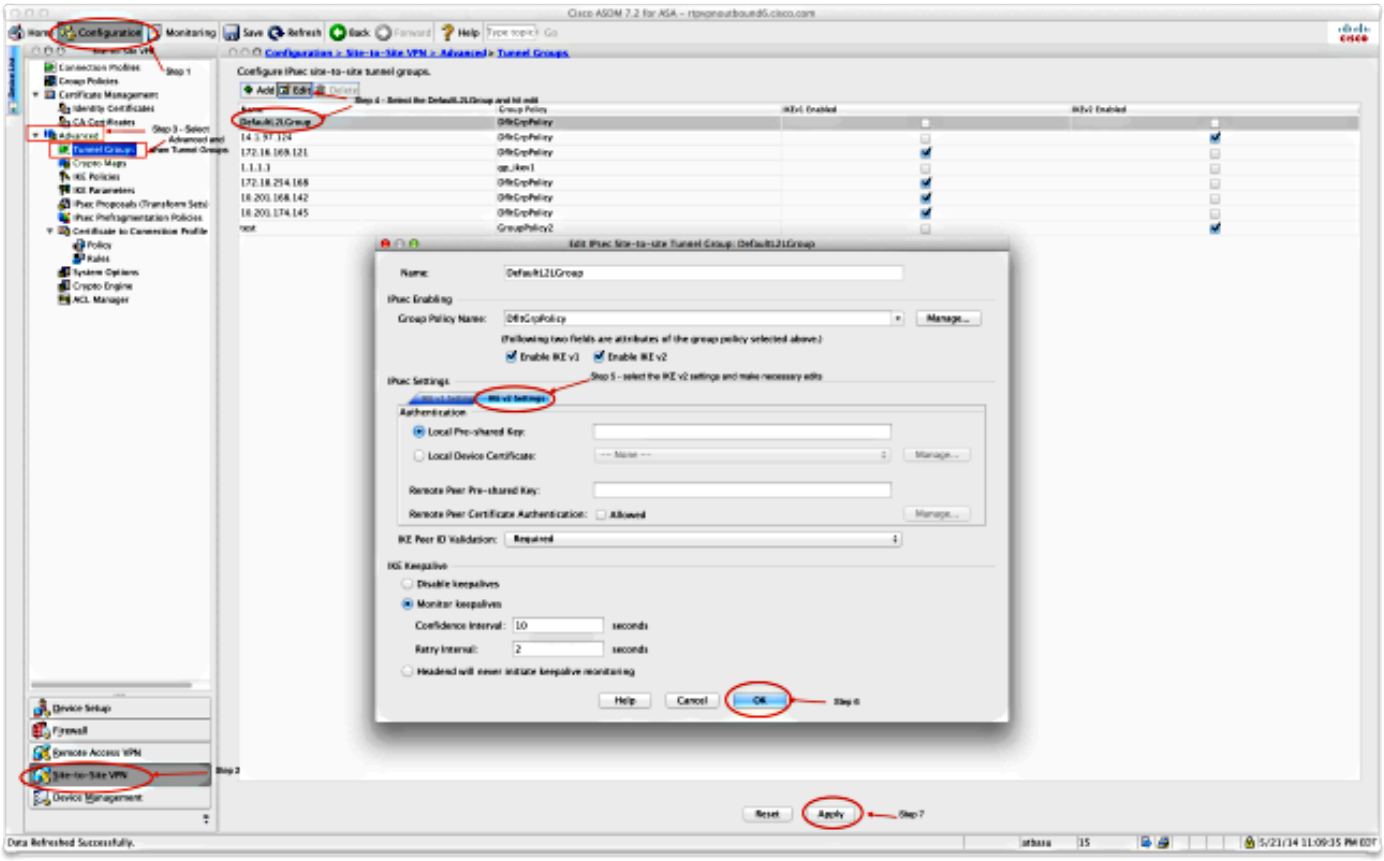
> **Tip**: Met deze methode is de negatieve kant dat alle peers dezelfde vooraf gedeelde sleutel hebben aangezien slechts één vooraf gedeelde sleutel kan worden gedefinieerd per tunnelgroep en alle peers verbinding zullen maken met dezelfde DefaultL2LGroup tunnelgroep.

Statische ASA-configuratie

```
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_CRYPTO_MAP 10 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 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_CRYPTO_MAP 65535 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
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 *****
```

Op het Adaptieve Security Devices Manager (ASDM) kunt u de DefaultL2LG groep configureren zoals hier wordt weergegeven:



Dynamisch 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 *****
```

In de ASDM-modus kunt u de standaardwizard gebruiken om het juiste verbindingsprofiel in te stellen. U kunt ook een nieuwe verbinding toevoegen en de standaardprocedure volgen.

Oplossing 2 - Maak een door de gebruiker gedefinieerde tunnelgroep

Deze methode vereist iets meer configuratie, maar het maakt meer granulariteit mogelijk. Elke peer kan zijn eigen eigen afzonderlijk beleid hebben en vooraf gedeelde sleutel. Hier is het echter belangrijk om de ISAKMP-ID op de dynamische peer te wijzigen, zodat deze in plaats van een IP-adres een naam gebruikt. Dit staat de statische ASA toe om het inkomende initialiseringsverzoek van ISAKMP aan de juiste tunnelgroep te passen en het juiste beleid te gebruiken.

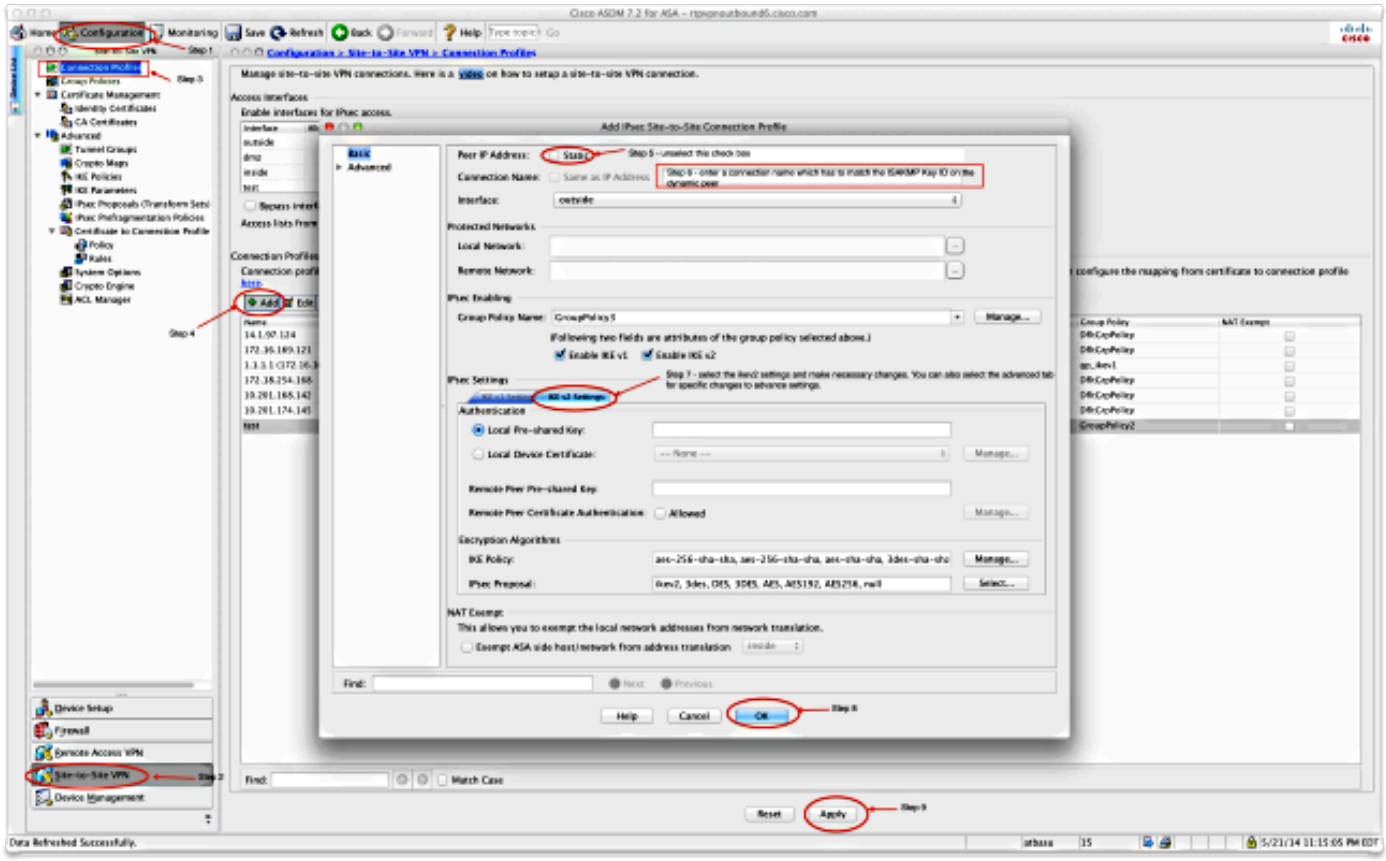
Statische ASA-configuratie

```
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_CRYPTO_MAP 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_CRYPTO_MAP 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_CRYPTO_MAP
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 *****
```

In de ASDM is de naam van het verbindingsprofiel standaard een IP-adres. Wanneer u het maakt, moet u het wijzigen om het een naam te geven zoals te zien is in de screenshot:



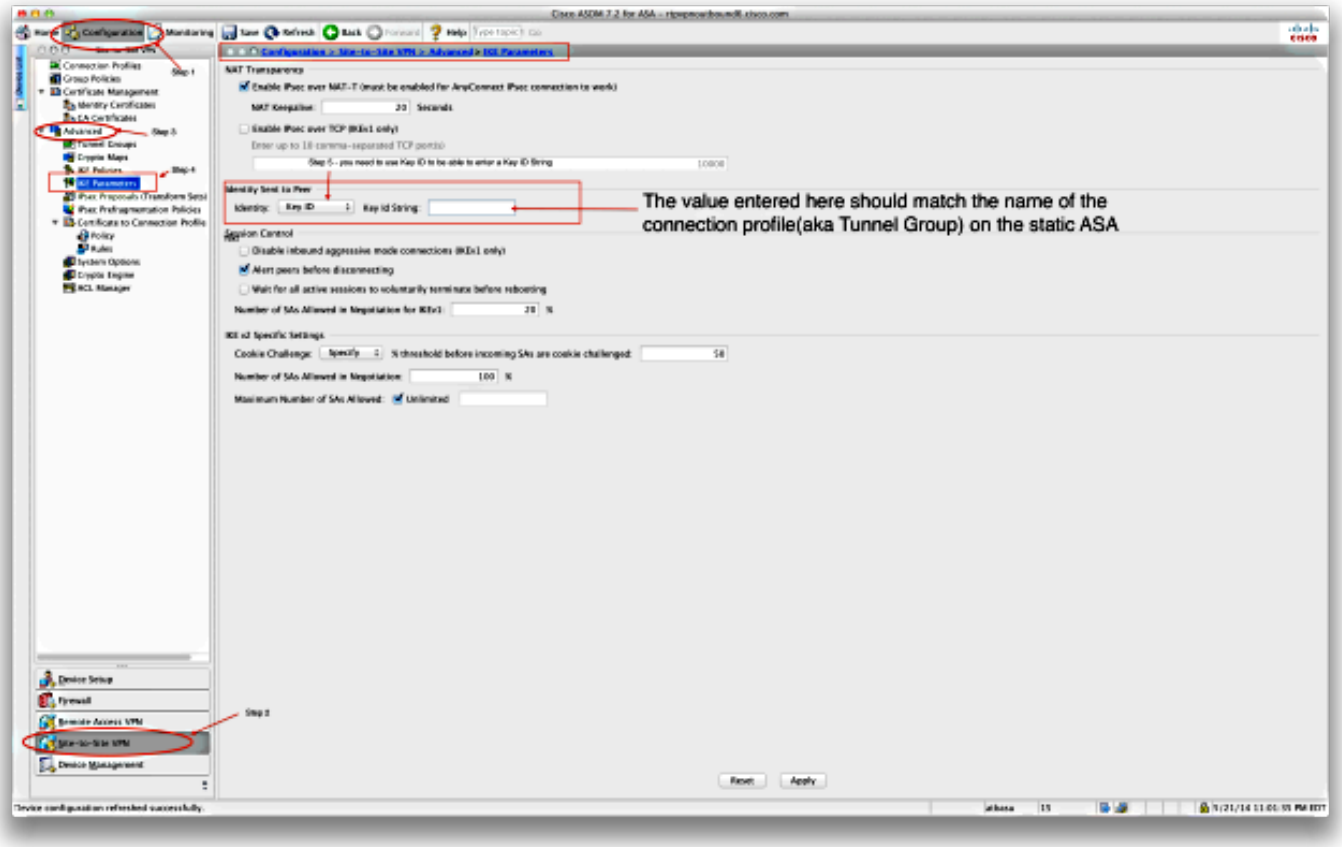
Dynamische ASA-configuratie

Dynamische ASA is in beide oplossingen bijna op dezelfde manier geconfigureerd met één opdracht zoals hier wordt getoond:

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

Zoals eerder beschreven, gebruikt de ASA standaard het IP adres van de interface waarop de VPN-tunnel in kaart is gebracht als de ISAKMP key-ID. In dit geval echter is de key-ID van de dynamische ASA dezelfde naam als de tunnelgroep op de Static ASA. Dus op elke dynamische peer, zal de key-id anders zijn en moet er een corresponderende tunnelgroep gecreëerd worden op de Static ASA met de juiste naam.

In de ASDM-modus kan dit worden ingesteld zoals in deze screenshot:



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Statische ASA

Dit is het resultaat van de **show crypto IKEv2 sa det** opdracht:

```
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: 4FDFF215BDEC73EC       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
```

Dit is het resultaat van de **show crypto ipsec** opdracht:

```
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
```

Dynamische ASA

Dit is het resultaat van de **show crypto IKEv2 als detail** opdracht:

```
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
```

Dit is het resultaat van de **show crypto ipsec** opdracht:

```
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
```

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht show.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht show.

> Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met debug opgeeft.

- deb-encryptie op IKEv2-pakket
- deb-crypto intern IKEv2