Sitio dinámico para localizar el túnel IKEv2 VPN entre el ejemplo de configuración dos ASA

Contenido

Introducción

Este documento describe cómo configurar un túnel del intercambio de claves de Internet versión 2 (IKEv2) VPN del sitio a localizar entre dos dispositivos de seguridad adaptantes (ASA) donde un ASA tiene un IP Address dinámico y el otro tiene un IP Address estático.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de ASA 5505
- Versión de ASA 9.1(5)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Hay dos maneras que esta configuración puede ser configurada:

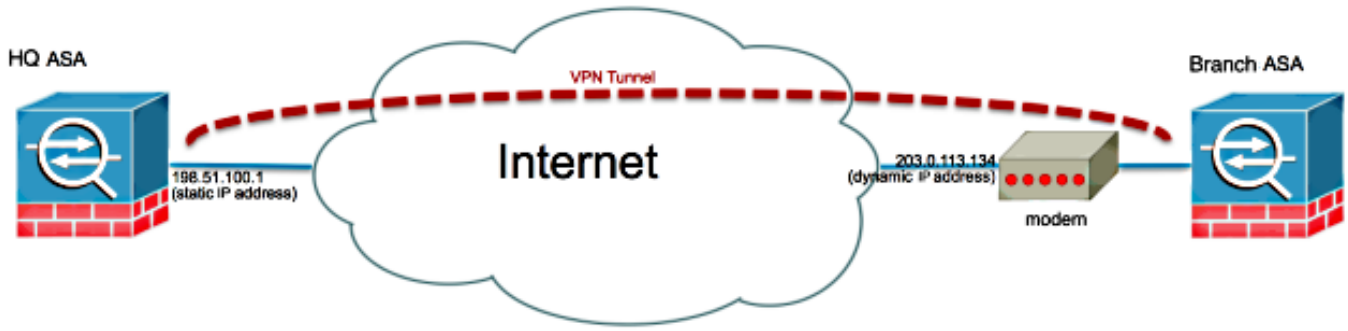
- Con el grupo de túnel DefaultL2LGroup
- Con un grupo de túnel Nombrado

La diferencia en la configuración más grande entre los dos escenarios es el Internet Security Association and Key Management Protocol (ISAKMP) ID usado por el telecontrol ASA. Cuando el DefaultL2LGroup se utiliza en el ASA estático, el ISAKMP ID del par tiene que ser el direccionamiento. Sin embargo si utilizan a un grupo de túnel Nombrado, el ISAKMP ID del par tiene que ser lo mismo el nombre de grupo de túnel usando este comando:

```
crypto isakmp identity key-id <tunnel-group_name>
```

La ventaja de usar a los grupos de túnel Nombrados en el ASA estático es que cuando se utiliza el DefaultL2LGroup, la configuración en los ASA dinámicos remotos, que incluye las claves previamente compartidas, tiene que ser idéntica y no permite mucho granularity con la configuración de las directivas.

Diagrama de la red



Configurar

Esta sección describe la configuración en cada ASA dependiendo de qué solución usted decide utilizar.

Solución 1 - Uso del DefaultL2LGroup

Ésta es la manera más simple de configurar un túnel del LAN a LAN (L2L) entre dos ASA cuando un ASA consigue su direccionamiento dinámicamente. El grupo DefaultL2L es un grupo de túnel preconfigurado en el ASA y todas las conexiones que no hacen juego explícitamente ninguna caída del grupo del túnel particular en esta conexión. Puesto que el ASA dinámico no tiene un constante predeterminó la dirección IP, él significa que el admin no puede configurar el Statis ASA para permitir la conexión en un grupo de túnel específico. En esta situación, el grupo DefaultL2L puede ser utilizado para permitir las conexiones dinámicas.

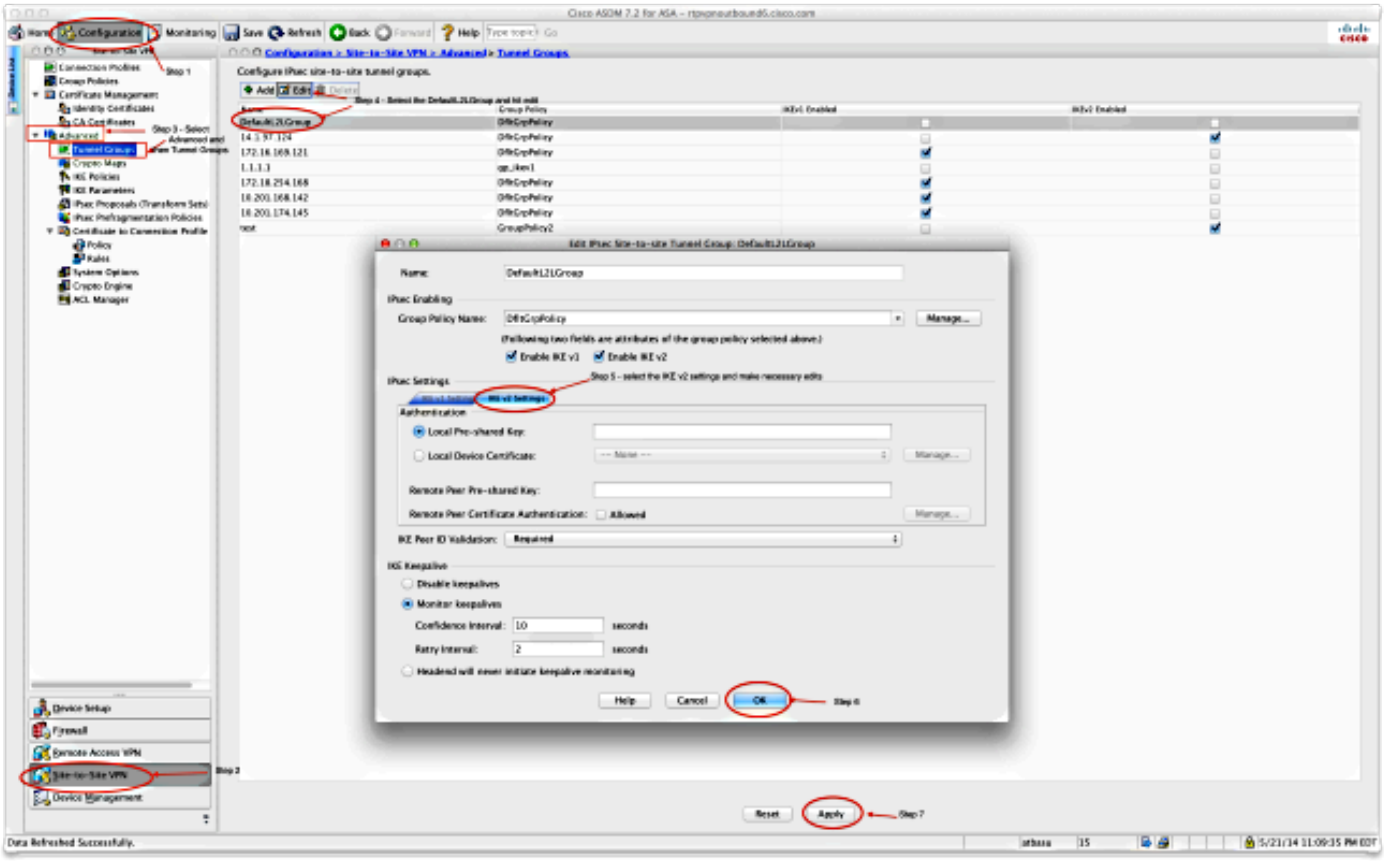
> Consejo: Con este método, la desventaja es que todos los pares tendrán la misma clave previamente compartida puesto que solamente una clave previamente compartida se puede definir por el grupo de túnel y todos los pares conectarán con el mismo grupo de túnel DefaultL2LGroup.

Configuración estática 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_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 *****
```

En el Administrador de dispositivos de seguridad adaptante (ASDM), usted puede configurar el DefaultL2LGroup como se muestra aquí:



ASA dinámico

```
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 *****
```

En el ASDM, usted puede utilizar al Asisitente estándar para configurar el perfil de la conexión apropiado o usted puede agregar simplemente una nueva conexión y seguir el procedimiento estándar.

Solución 2 - Cree a un grupo de túnel definido por el usario

Este método requiere slighly más configuración, pero permite más granularity. Cada par puede tener su propia política diferenciados y clave previamente compartida. Al menos aquí es importante cambiar el ISAKMP ID en el par dinámico de modo que utilice un nombre en vez de una dirección IP. Esto permite que el ASA estático haga juego la petición entrante de la inicialización ISAKMP al grupo de túnel adecuado y utilice las directivas correctas.

Configuración estática 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
```

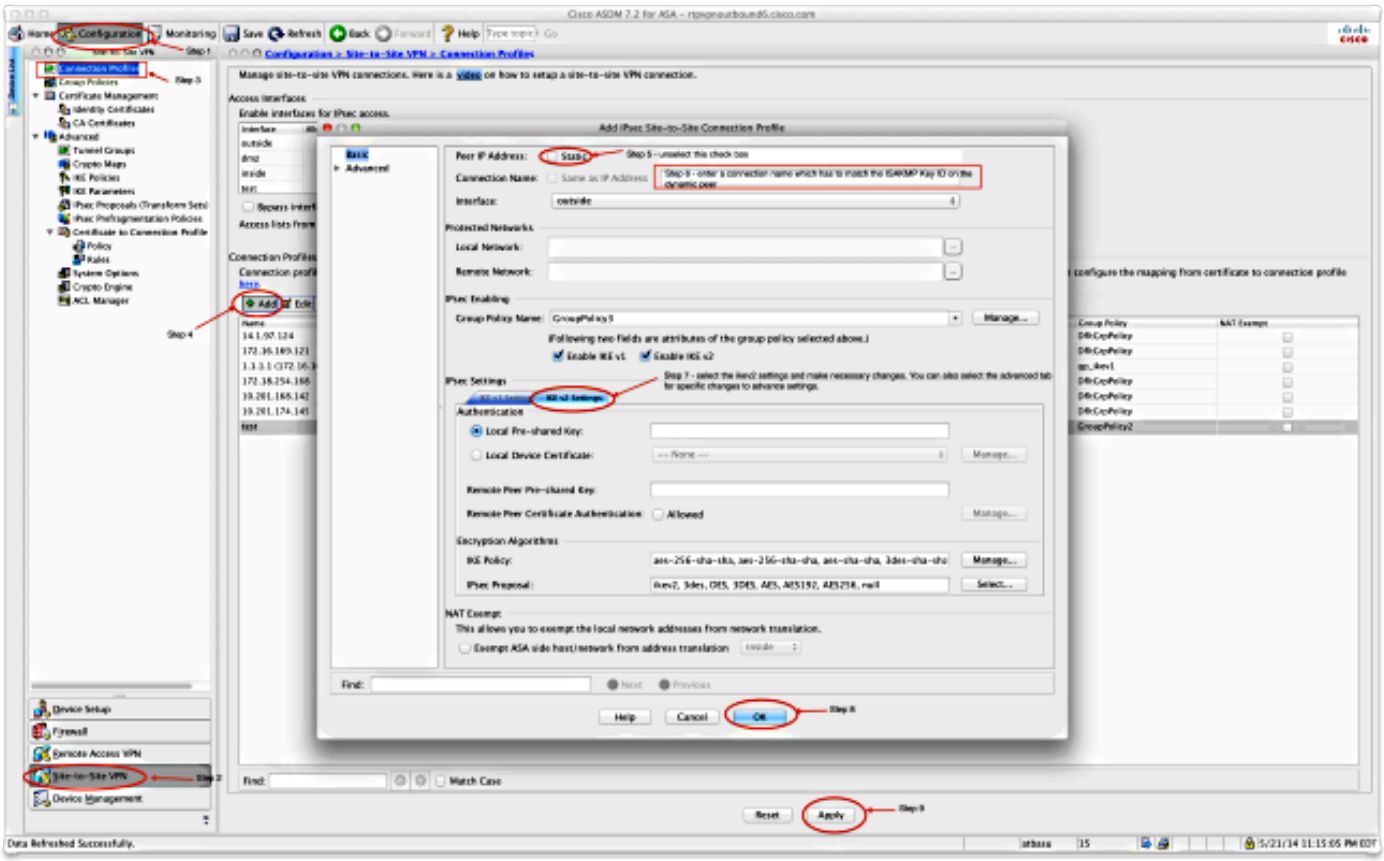
```
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto engine large-mod-accel
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_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 *****
```

En el ASDM, el nombre del perfil de la conexión es una dirección IP por abandono. Tan cuando usted lo crea, usted debe cambiarlo para darle un nombre tal y como se muestra en del tiro de pantalla aquí:



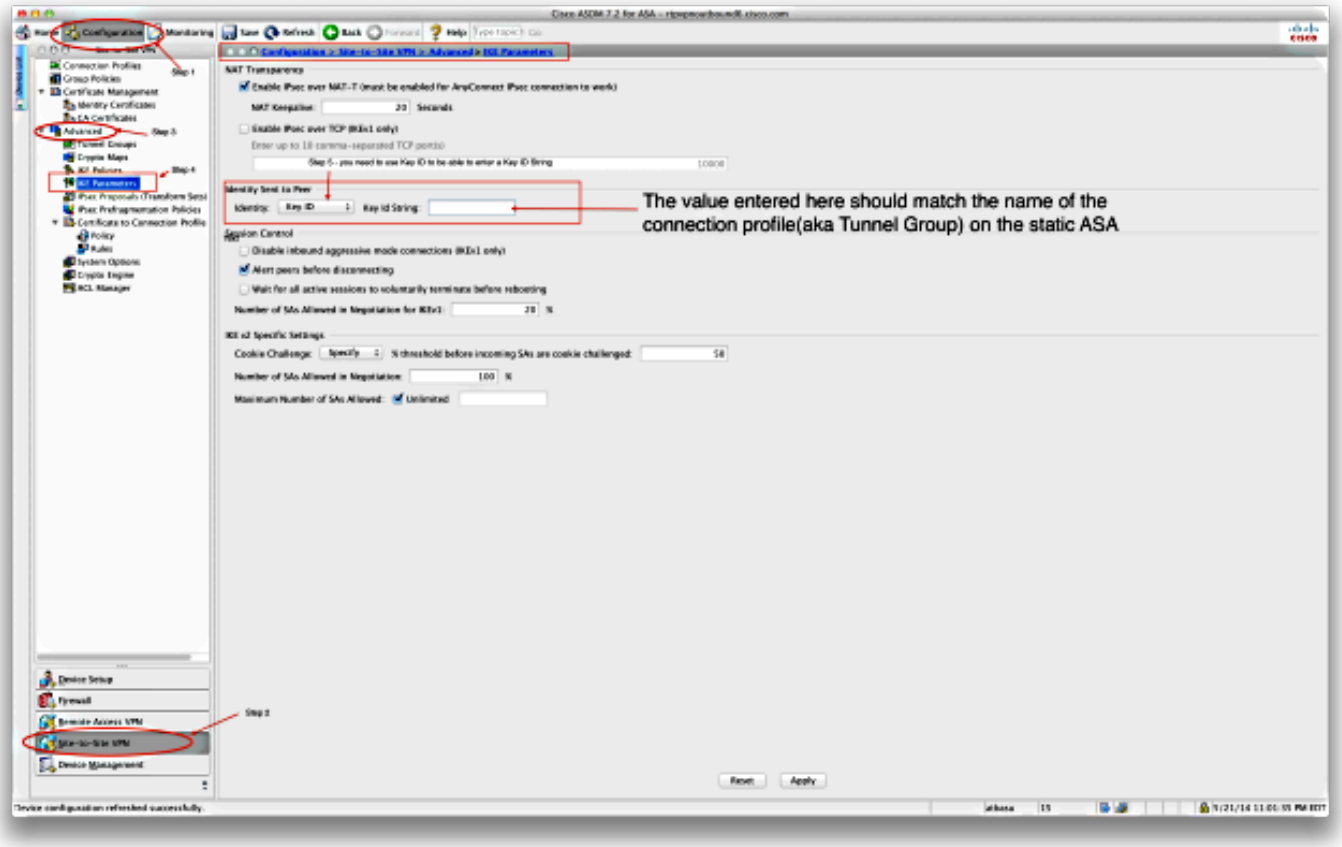
Configuración dinámica ASA

El ASA dinámico se configura casi la misma manera en ambas soluciones con la adición de un comando como se muestra aquí:

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

Según lo descrito previamente, por abandono el ASA utiliza la dirección IP de la interfaz que el túnel VPN está asociado como al ISAKMP CLAVE-ID. Al menos en este caso, el clave-ID en el ASA dinámico es lo mismo que el nombre del grupo de túnel en el ASA estático. Tan en cada par dinámico, la clave-identificación será diferente y un grupo de túnel correspondiente debe ser creado en el ASA estático con el nombre correcto.

En el ASDM, esto se puede configurar tal y como se muestra en de este tiro de pantalla:



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

En el ASA estático

Aquí está el resultado del comando **crypto del det IKEv2 sa de la demostración**:

```
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
```

Aquí está el resultado del **comando 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
```

En el ASA dinámico

Aquí está el resultado del **comando detail crypto IKEv2 sa de la demostración**:

```
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
```

Aquí está el resultado del comando 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
```

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

> Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **paquete crypto IKEv2 DEB**
- **DEB IKEv2 crypto interno**