Ejemplo de Configuración de Túnel VPN IKEv2 de Sitio a Sitio Dinámico entre Dos ASA

Contenido

Introducción

Este documento describe cómo configurar un túnel VPN de intercambio de claves de Internet de sitio a sitio versión 2 (IKEv2) entre dos dispositivos de seguridad adaptables (ASA) donde un ASA tiene una dirección IP dinámica y el otro tiene una dirección IP estática.

Prerequisites

Requirements

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.

- ASA versión 5505
- ASA versión 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.

Antecedentes

Hay dos maneras de configurar esta configuración:

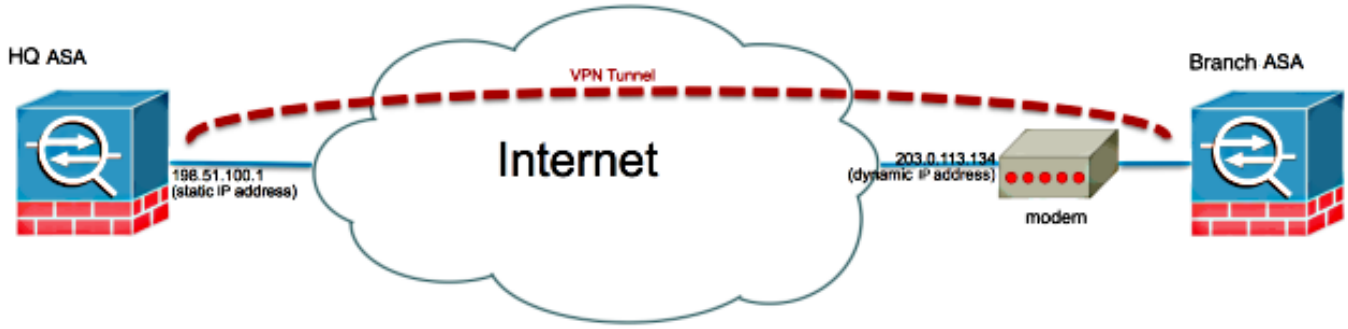
- Con el grupo de túnel DefaultL2LGroup
- Con un grupo de túnel con nombre

La mayor diferencia de configuración entre los dos escenarios es la ID de protocolo de administración de claves (ISAKMP) y de asociación de seguridad de Internet utilizada por el ASA remoto. Cuando se utiliza DefaultL2LGroup en el ASA estático, el ID ISAKMP del peer debe ser la dirección. Sin embargo, si se utiliza un grupo de túnel con nombre, el ID ISAKMP del par debe ser el mismo que el nombre del grupo de túnel con este comando:

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

La ventaja de utilizar grupos de túnel con nombre en el ASA estático es que cuando se utiliza el DefaultL2LGroup, la configuración en los ASA dinámicos remotos, que incluye las claves previamente compartidas, debe ser idéntica y no permite mucha granularidad con la configuración de las políticas.

Diagrama de la red



Configurar

En esta sección se describe la configuración de cada ASA en función de la solución que decida utilizar.

Solución 1 - Uso del DefaultL2LGroup

Esta es la forma más sencilla de configurar un túnel de LAN a LAN (L2L) entre dos ASA cuando un ASA obtiene su dirección dinámicamente. El grupo DefaultL2L es un grupo de túnel preconfigurado en el ASA y todas las conexiones que no coinciden explícitamente con ningún grupo de túnel determinado caen en esta conexión. Dado que el ASA dinámico no tiene una dirección IP predeterminada constante, significa que el administrador no puede configurar el ASA estático para permitir la conexión en un grupo de túnel específico. En esta situación, se puede utilizar el grupo DefaultL2L para permitir las conexiones dinámicas.

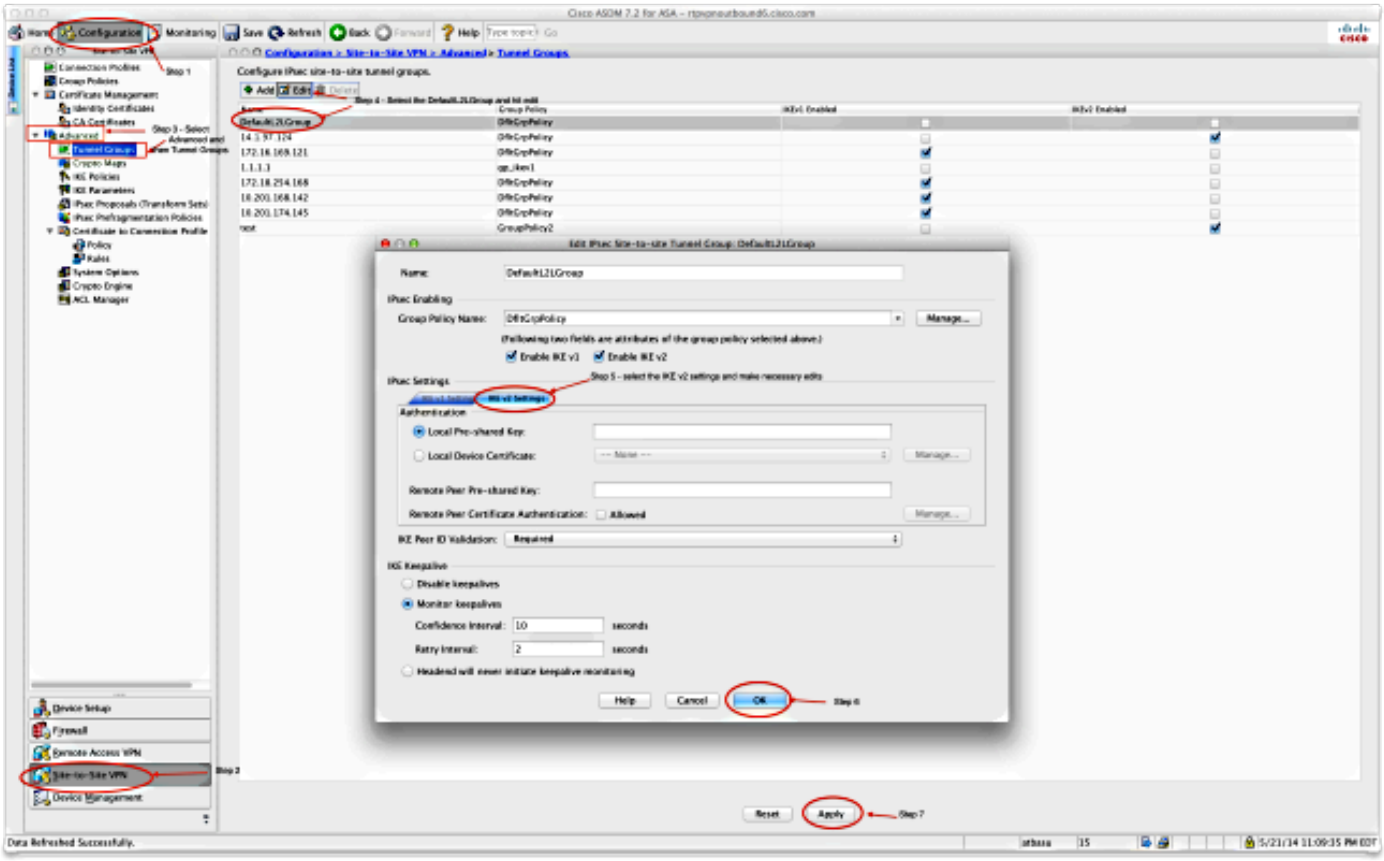
> **Sugerencia**: con este método, el inconveniente es que todos los peers tendrán la misma clave previamente compartida, ya que sólo se puede definir una clave previamente compartida por grupo de túnel y todos los peers se conectarán al mismo grupo de túnel DefaultL2LGroup.

Configuración de ASA Estático

```
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 Adaptive Security Device Manager (ASDM), 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, puede utilizar el asistente estándar para configurar el perfil de conexión adecuado o simplemente puede agregar una nueva conexión y seguir el procedimiento estándar.

Solución 2: Creación de un grupo de túnel definido por el usuario

Este método requiere un poco más de configuración, pero permite una mayor granularidad. Cada par puede tener su propia política independiente y clave previamente compartida. Sin embargo, aquí es importante cambiar el ID ISAKMP en el par dinámico para que utilice un nombre en lugar de una dirección IP. Esto permite que el ASA estático coincida con la solicitud de inicialización ISAKMP entrante al grupo de túnel correcto y utilice las políticas correctas.

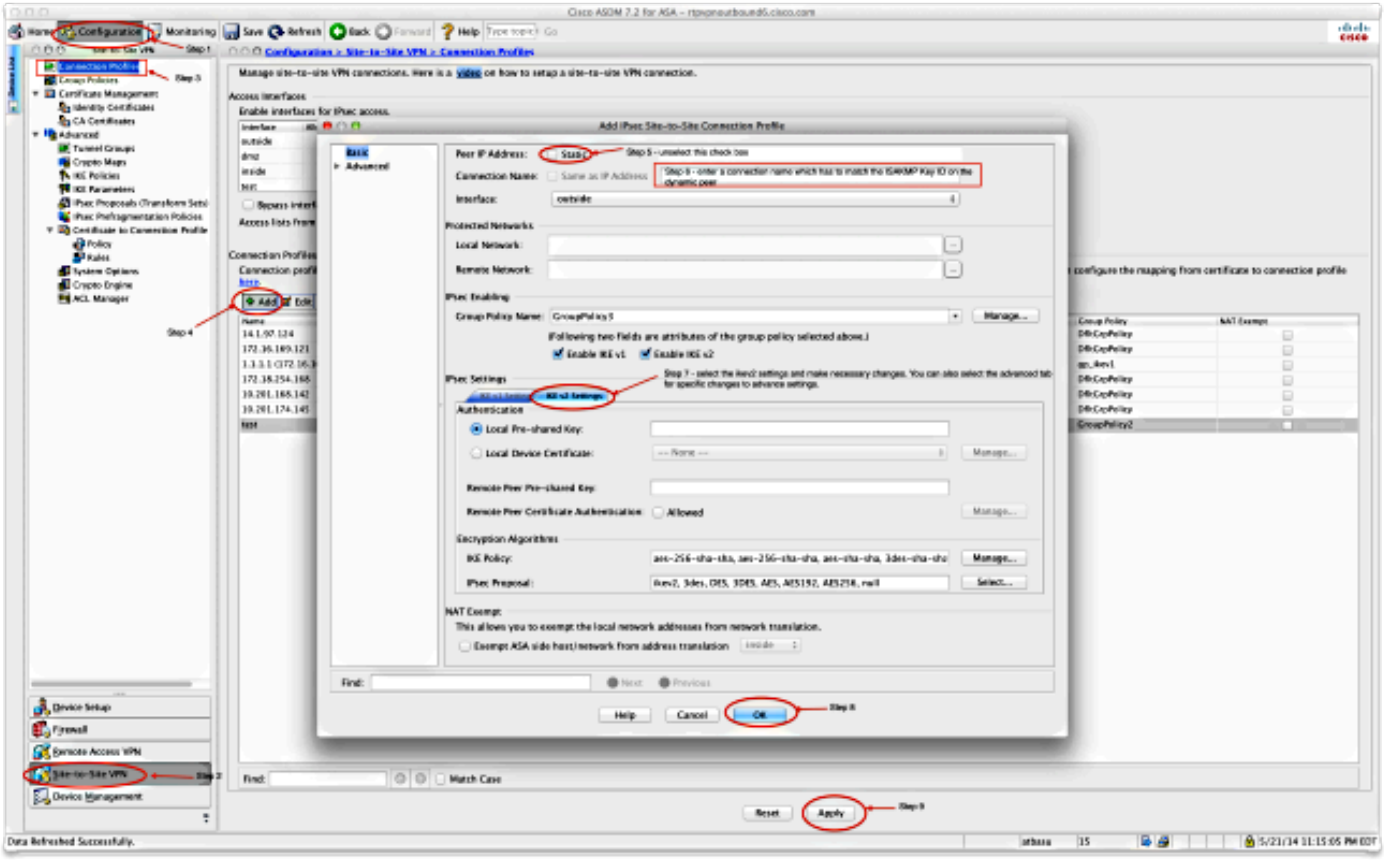
Configuración de ASA Estático

```
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 conexión es una dirección IP de forma predeterminada. Por lo tanto, cuando lo cree, debe cambiarlo para darle un nombre como se muestra en la captura de pantalla aquí:



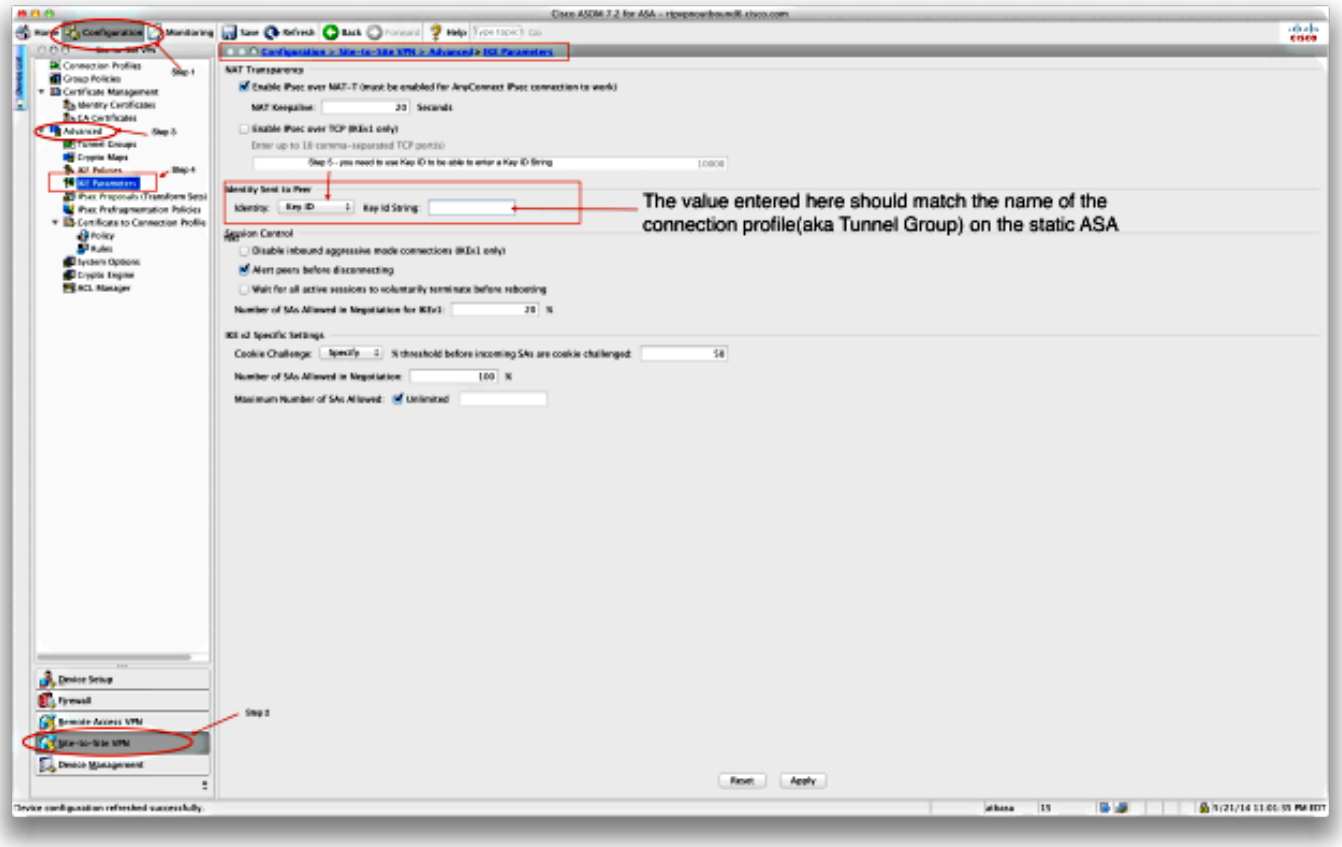
Configuración de ASA Dinámico

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

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

Como se ha descrito anteriormente, de forma predeterminada el ASA utiliza la dirección IP de la interfaz a la que se asigna el túnel VPN como ID de clave ISAKMP. Sin embargo, en este caso, el ID de clave en el ASA dinámico es el mismo que el nombre del grupo de túnel en el ASA estático. Por lo tanto, en cada par dinámico, el id de clave será diferente y se debe crear un grupo de túnel correspondiente en el ASA estático con el nombre correcto.

En el ASDM, esto se puede configurar como se muestra en esta captura de pantalla:



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

En el ASA estático

Aquí está el resultado del comando show crypto IKEv2 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: 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 show crypto IKEv2 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
```

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 de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

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

- paquete deb crypto IKEv2
- deb crypto IKEv2 internal