두 ASA 간의 동적 사이트 대 사이트 IKEv2 VPN 터널 컨피그레이션 예

목차

소개

이 문서에서는 한 ASA에 동적 IP 주소가 있고 다른 ASA에는 고정 IP 주소가 있는 두 ASA(Adaptive Security Appliance) 간에 사이트 간 IKEv2(Internet Key Exchange Version 2) VPN 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 버전 5505
- ASA 버전 9.1(5)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 컨피그레이션을 설정할 수 있는 두 가지 방법은 다음과 같습니다.

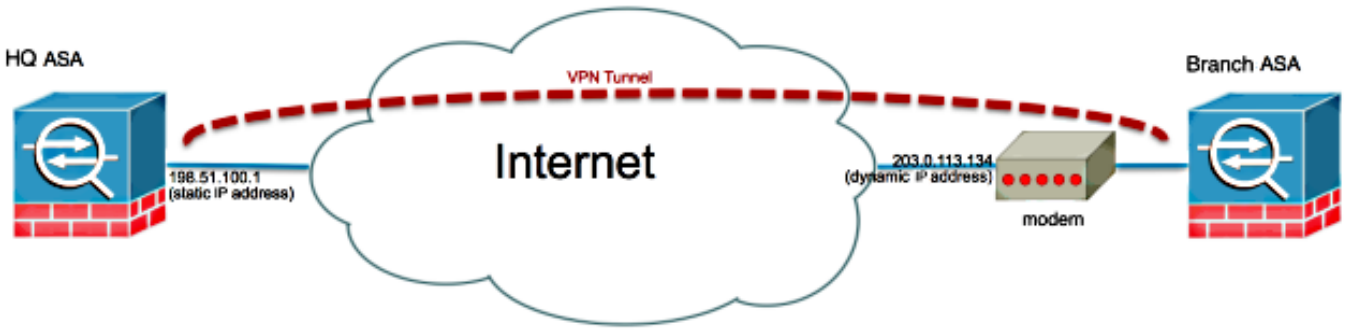
- DefaultL2LGroup 터널 그룹 사용
- 명명된 터널 그룹 사용

두 시나리오 간의 가장 큰 구성 차이는 원격 ASA에서 사용하는 ISAKMP(Internet Security Association and Key Management Protocol) ID입니다.고정 ASA에서 DefaultL2LGroup을 사용할 경우 피어의 ISAKMP ID가 주소여야 합니다.그러나 명명된 터널 그룹을 사용하는 경우 피어의 ISAKMP ID는 다음 명령을 사용하여 터널 그룹 이름과 같아야 합니다.

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

고정 ASA에서 명명된 터널 그룹을 사용할 때의 이점은 DefaultL2LGroup을 사용할 때 사전 공유 키를 포함하는 원격 동적 ASA의 컨피그레이션이 동일해야 하며 정책 설정을 훨씬 세부적으로 수행할 수 없다는 점입니다.

네트워크 다이어그램



구성

이 섹션에서는 사용하려는 솔루션에 따라 각 ASA의 컨피그레이션에 대해 설명합니다.

솔루션 1 - DefaultL2LGroup 사용

이는 한 ASA가 동적으로 주소를 가져올 때 두 ASA 간에 LAN-to-LAN(L2L) 터널을 구성하는 가장 간단한 방법입니다.DefaultL2L Group은 ASA의 사전 구성된 터널 그룹이며 특정 터널 그룹과 명시적으로 일치하지 않는 모든 연결은 이 연결에서 발생합니다.동적 ASA에는 일정한 미리 결정된 IP 주소가 없으므로 관리자가 특정 터널 그룹에서 연결을 허용하기 위해 Statis ASA를 구성할 수 없음을 의미합니다.이 경우 DefaultL2L 그룹을 사용하여 동적 연결을 허용할 수 있습니다.

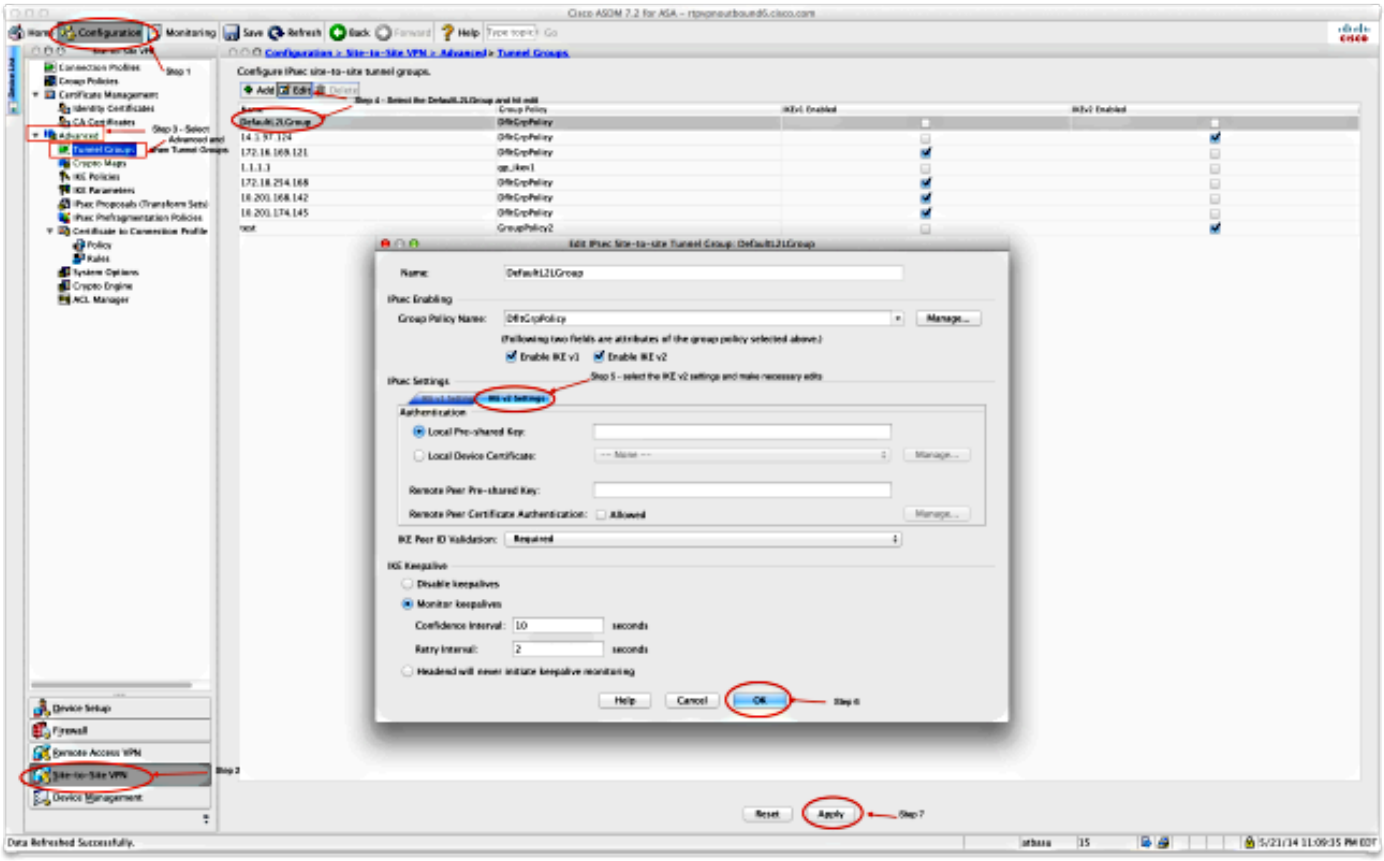
> **팁**: 이 방법을 사용하면 터널 그룹당 하나의 사전 공유 키만 정의할 수 있으며 모든 피어가 동일한 DefaultL2LGroup 터널 그룹에 연결되므로 모든 피어가 동일한 사전 공유 키를 갖게 됩니다.

고정 ASA 컨피그레이션

```
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 *****
```

ASDM(Adaptive Security Device Manager)에서 다음과 같이 DefaultL2LGroup을 구성할 수 있습니다.



동적 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 *****
```

ASDM에서 표준 마법사를 사용하여 적절한 연결 프로파일을 설정하거나 새 연결을 추가하고 표준 절차를 따르면 됩니다.

솔루션 2 - 사용자 정의 터널 그룹 생성

이 방법을 사용하려면 약간 더 많은 구성이 필요하지만 더 세분화할 수 있습니다.각 피어는 고유한 개별 정책 및 사전 공유 키를 가질 수 있습니다.그러나 여기서는 IP 주소 대신 이름을 사용하도록 동적 피어의 ISAKMP ID를 변경하는 것이 중요합니다.이렇게 하면 고정 ASA가 수신 ISAKMP 초기화 요청을 올바른 터널 그룹에 일치시키고 올바른 정책을 사용할 수 있습니다.

고정 ASA 컨피그레이션

```
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
```

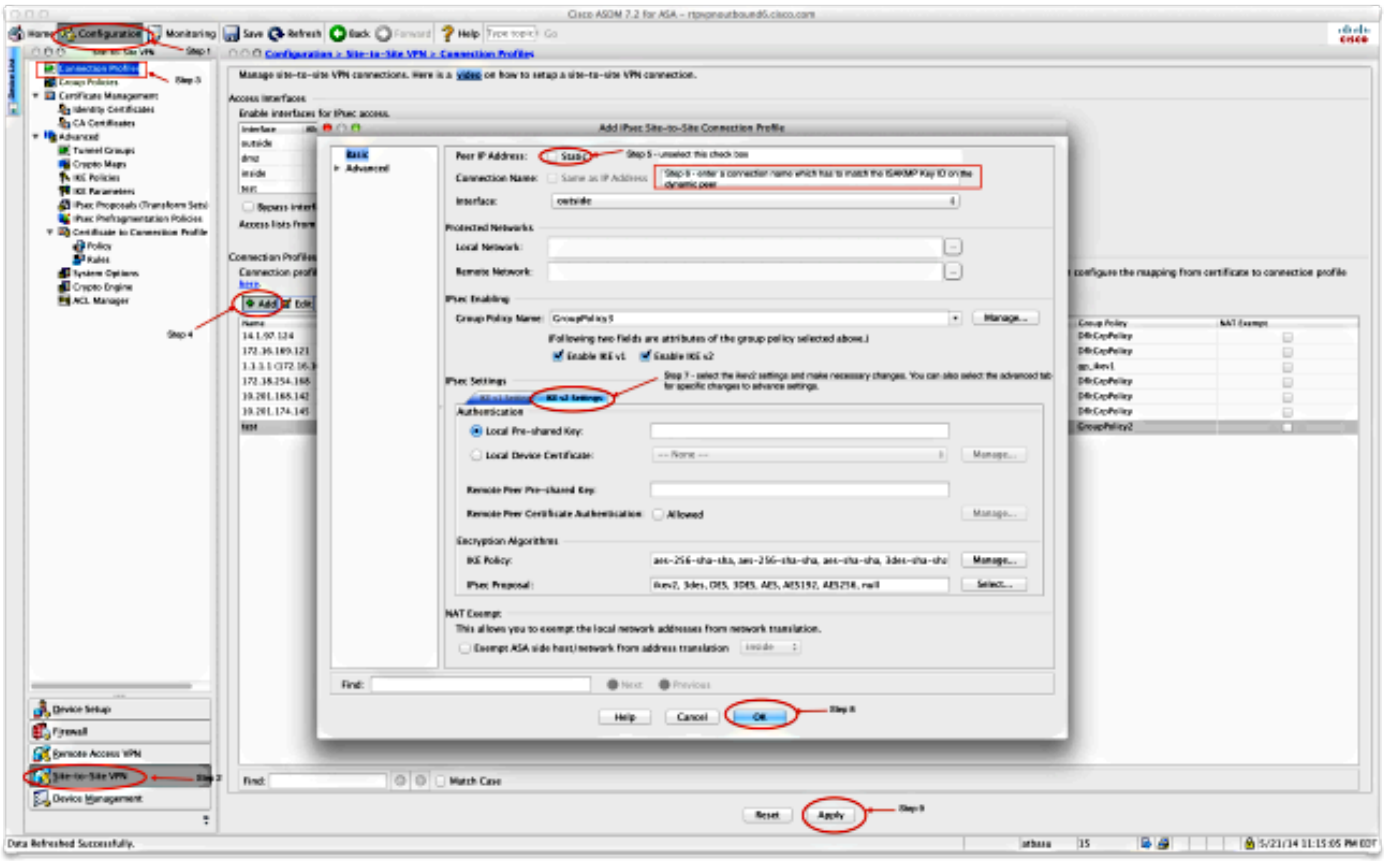
```
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto engine large-mod-accel
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 *****
```

ASDM에서 연결 프로파일 이름은 기본적으로 IP 주소입니다.따라서 이 파일을 만들 때 다음 스크린샷과 같이 이름을 지정하려면 변경해야 합니다.



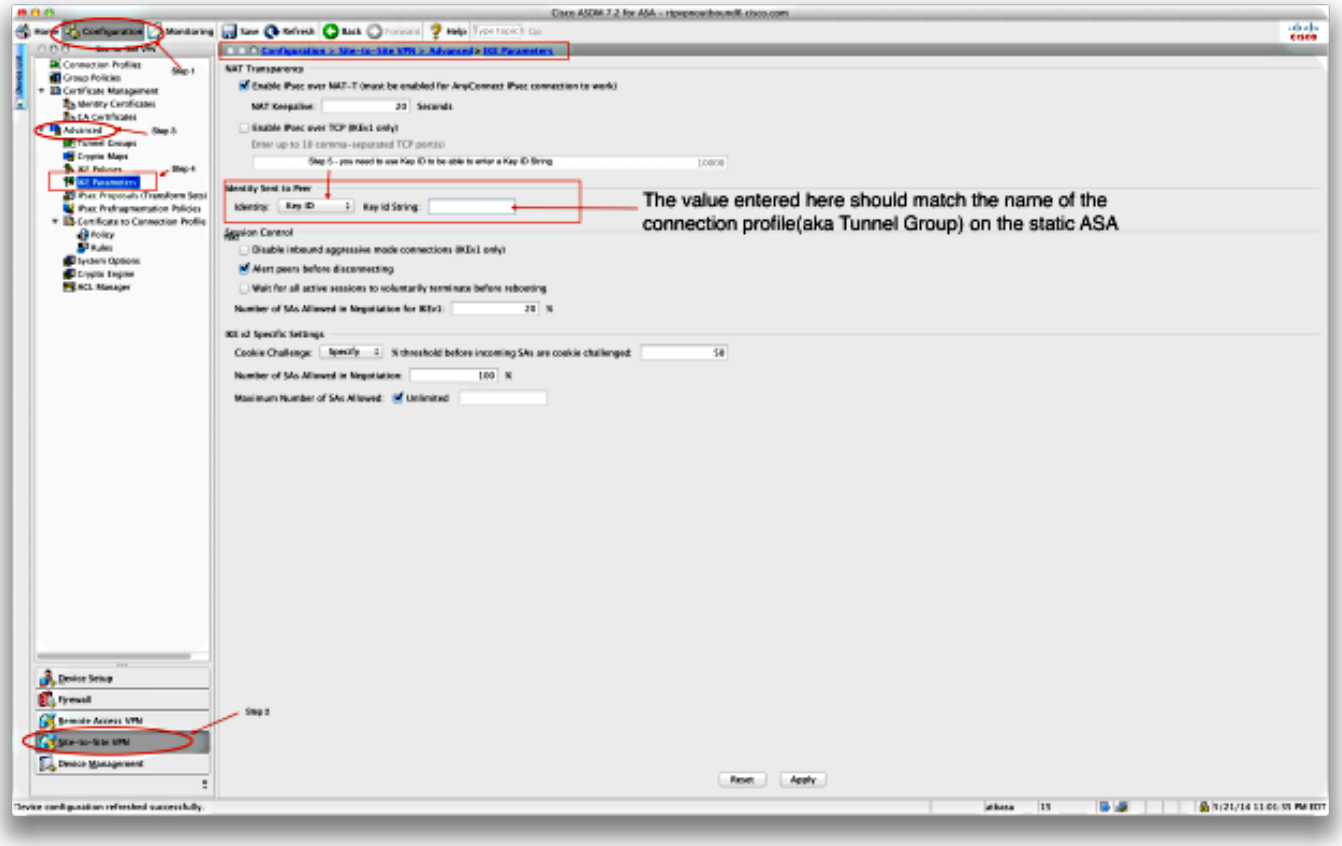
동적 ASA 컨피그레이션

Dynamic ASA는 두 솔루션 모두에서 거의 동일한 방식으로 구성되며 여기에 나와 있는 것처럼 하나의 명령이 추가됩니다.

`crypto isakmp identity key-id DynamicSite2Site1`

앞에서 설명한 대로 기본적으로 ASA는 VPN 터널이 매핑된 인터페이스의 IP 주소를 ISAKMP 키 ID로 사용합니다.그러나 이 경우 동적 ASA의 키 ID는 고정 ASA의 터널 그룹 이름과 동일합니다.따라서 모든 동적 피어에서 key-id는 다르며 적절한 이름을 가진 해당 터널 그룹을 Static ASA에 생성해야 합니다.

ASDM에서는 이 스크린샷과 같이 구성할 수 있습니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

정적 ASA에서

다음은 show crypto IKEv2 sa det 명령의 결과입니다.

```
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
```

다음은 show crypto ipsec sa 명령의 결과입니다.

```
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
```

동적 ASA에서

다음은 show crypto IKEv**2 sa detail** 명령의 결과입니다.

```
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
```

다음은 show crypto ipsec sa 명령의 결과입니다.

```
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
```

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

> **참고:debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **deb crypto IKEv2 패킷**
- **deb crypto IKEv2 내부**