站点IKEv2 VPN通道的动态站点在两ASA配置示例之间

目录

简介
先决条件
要求
使用的组件
背景信息
网络图
配置
解决方案1 -使用DefaultL2LGroup
静态ASA配置
动态ASA
解决方案2 -创建一用户定义的隧道群
静态ASA配置
动态ASA配置
验证
在静态ASA
在动态ASA
故障排除

简介

本文描述如何配置在两可适应安全工具(ASA)之间的一个站点到站点互联网密钥交换版本2 (IKEv2) VPN通道一个ASA有一个动态IP地址的地方，并且其他有一个静态IP地址。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA版本5505

- ASA版本9.1(5)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

有两种方式此配置可以设置：

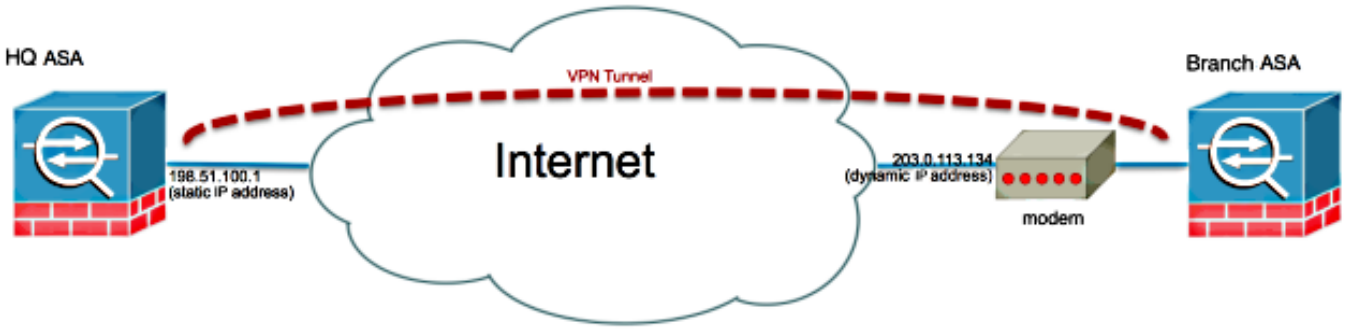
- 使用DefaultL2LGroup隧道组
- 使用一个已命名隧道组

两个方案之间的最大的配置差别是远程ASA使用的互联网安全协会和密钥管理协议(ISAKMP) ID。当DefaultL2LGroup在静态ASA时使用，对等体的ISAKMP ID必须是地址。然而，如果使用一个已命名隧道组使用此命令，对等体的ISAKMP ID必须是相同的隧道组组名：

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

使用静态ASA的已命名隧道组优点是，当使用时DefaultL2LGroup，在远程动态ASA的配置，包括预先共享密钥，必须是相同的，并且不允许与策略设置的粒度。

网络图



配置

此部分根据哪解决方案描述在每个ASA的配置您决定使用。

解决方案1 -使用DefaultL2LGroup

这是简单方法配置在两ASA之间的LAN对LAN (L2L)通道，当一个ASA动态地时得到其地址。DefaultL2L组是ASA的一个预先配置的隧道组，并且不明确地匹配任何特定的隧道组的所有连接在此连接落。因为动态ASA没有常数预先了确定IP地址，它含义admin不能配置Statis ASA为了允许在一个特定隧道组的连接。在这种情况下， DefaultL2L组可以使用为了允许动态连接。

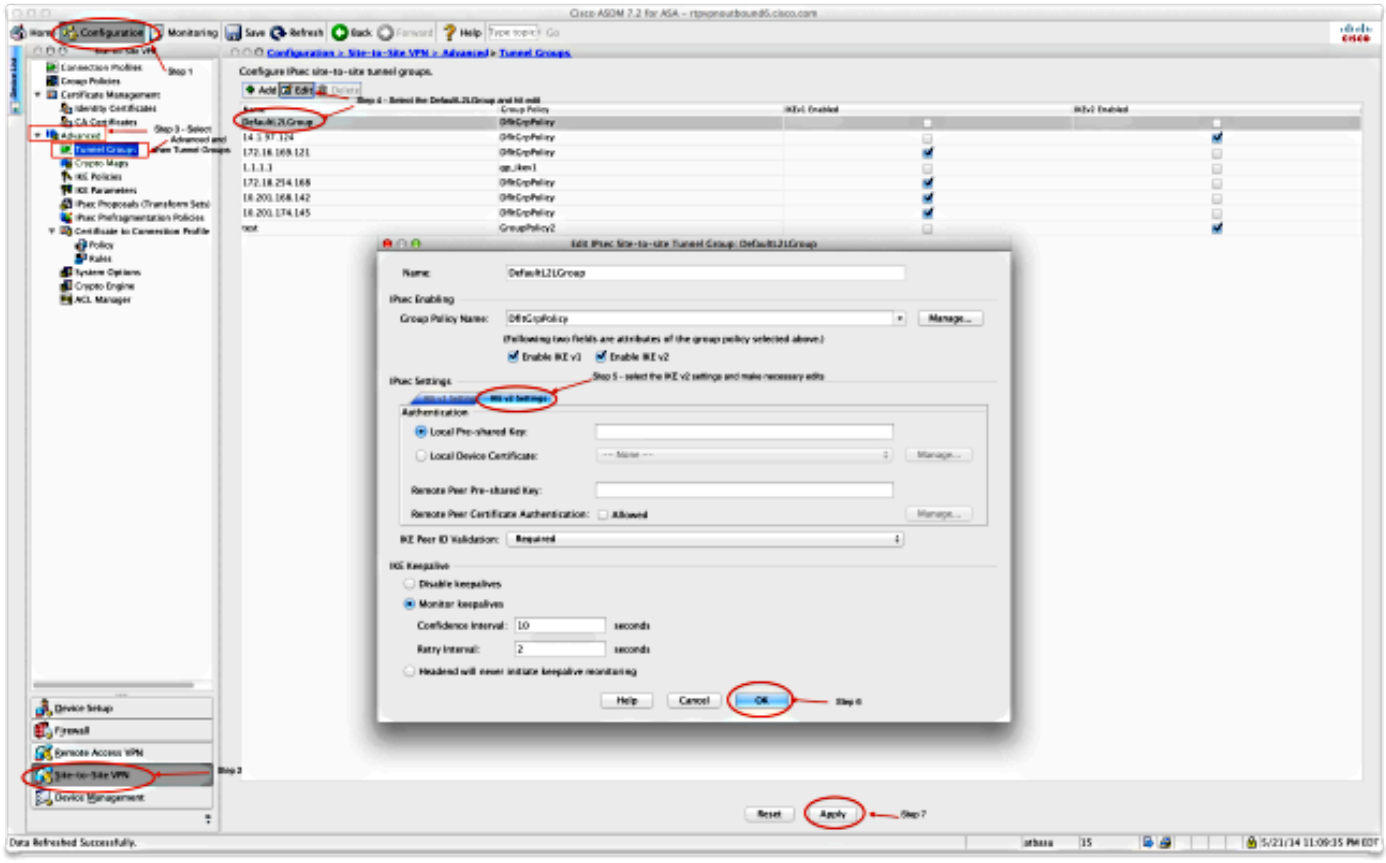
> **提示**： 使用此方法，下侧是所有对等体将有同一预先共享密钥，因为仅一预先共享密钥可以每隧道群定义，并且所有对等体将联络对同一DefaultL2LGroup隧道群。

静态ASA配置

```
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 *****
```

在可适应安全设备管理器(ASDM)，您能配置DefaultL2LGroup如显示此处：



动态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 *****
```

在ASDM，您能使用标准的向导为了设置适当的连接配置文件或您能添加新连接和遵从标准程序。

解决方案2 -创建用户定义的隧道群

此方法要求slighly更多配置，但是允许更多粒度。每对等体能有其自己的独立的政策和预先共享密钥。在这里更改在动态对等体的ISAKMP ID重要的，以便它使用一名称而不是IP地址。这允许静态ASA匹配流入ISAKMP初始化请求对正确的隧道组和使用正确的策略。

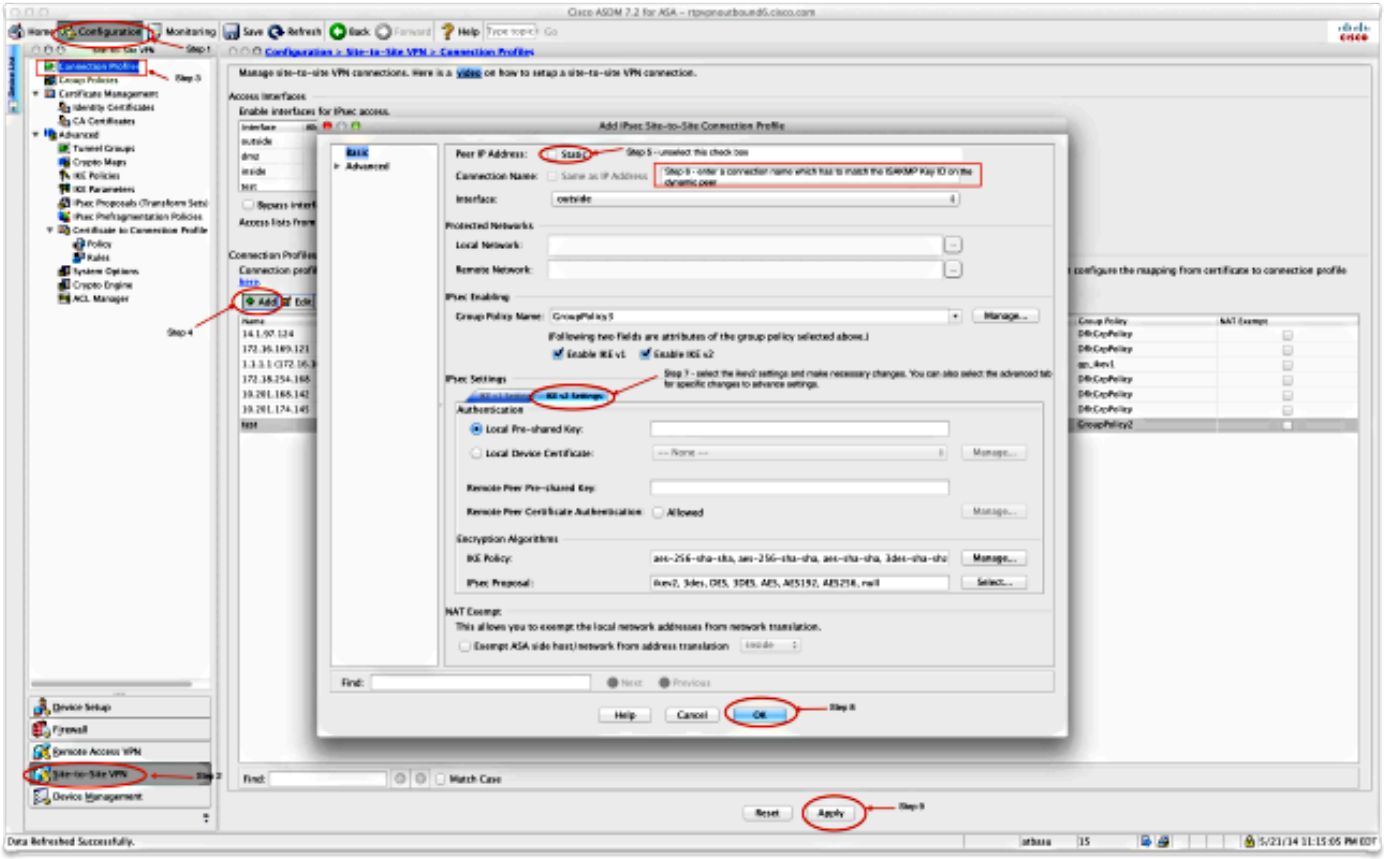
静态ASA配置

```
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 *****
```

默认情况下在ASDM，连接配置文件名称是IP地址。因此，当您创建它时，您必须更改它为了给予它名称如屏幕画面所显示此处：

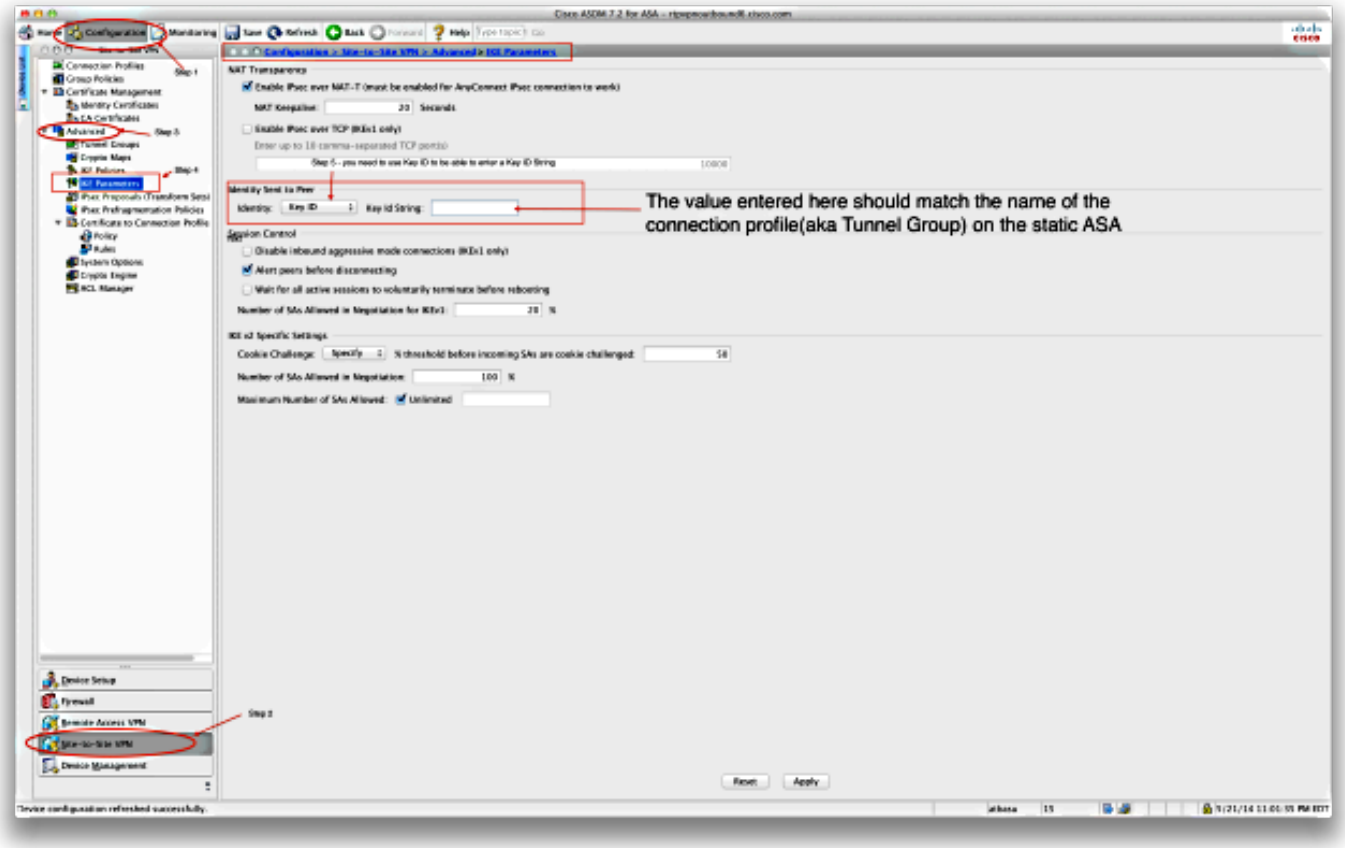


动态ASA配置

动态ASA是几乎配置在两解决方案的同一个方式增加一命令如显示此处：

crypto isakmp identity key-id DynamicSite2Site1
默认情况下如描述以前， ASA使用VPN通道被映射对作为ISAKMP key-id接口的IP地址。在此种情况，在动态ASA的key-id是相同的象隧道群的名称静态ASA的。因此在每动态对等体， key-id不同的，并且一对应的隧道群在与正确的名称的静态ASA必须创建。

如此屏幕画面所显示，在ASDM，这可以配置：



验证

使用本部分可确认配置能否正常运行。

在静态ASA

这是**显示crypto sa IKEv2 det**命令的结果：

```
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
```

这是结果**show crypto ipsec sa命令**：

```
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
```

在动态ASA

这是detail命令显示crypto的IKEv2 sa的结果：

```
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
```

这是结果show crypto ipsec sa命令：

```
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
```

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

> **注意**：使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **deb crypto IKEv2数据包**
- **内部的deb crypto IKEv2**