两个ASA之间的动态站点到站点IKEv2 VPN隧道配置示例

目录

简介

本文档介绍如何在两个自适应安全设备(ASA)之间配置站点到站点互联网密钥交换版本2(IKEv2)VPN隧道，其中一个ASA具有动态IP地址，另一个具有静态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 9.1(5) 版

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。
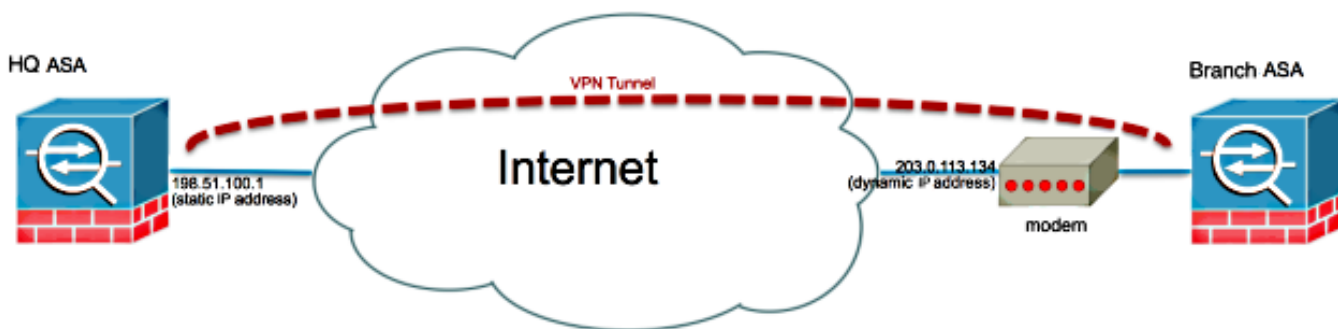
背景信息

设置此配置的方法有两种：

- 使用DefaultL2LGroup隧道组
- 具有命名隧道组

这两种方案之间的最大配置差异是远程ASA使用的互联网安全关联和密钥管理协议(ISAKMP)ID。当静态ASA上使用DefaultL2LGroup时，对等体的ISAKMP ID必须是地址。但是，如果使用命名隧道组，则对等体的ISAKMP ID必须与使用以下命令的隧道组名称相同：

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

在静态ASA上使用命名隧道组的优点是，当使用DefaultL2LGroup时，远程动态ASA（包括预共享密钥）上的配置必须相同，并且不允许在策略设置方面进行更精细的配置。

网络图

配置

本节根据您决定使用的解决方案介绍每个ASA上的配置。

解决方案1 — 使用DefaultL2LGroup

当一个ASA动态获取其地址时，这是在两个ASA之间配置LAN到LAN(L2L)隧道的最简单方法。DefaultL2L组是ASA上预配置的隧道组，并且此连接上所有未明确匹配任何特定隧道组的连接都属于此连接。由于动态ASA没有恒定的预定IP地址，这意味着管理员无法配置Statis ASA以允许在特
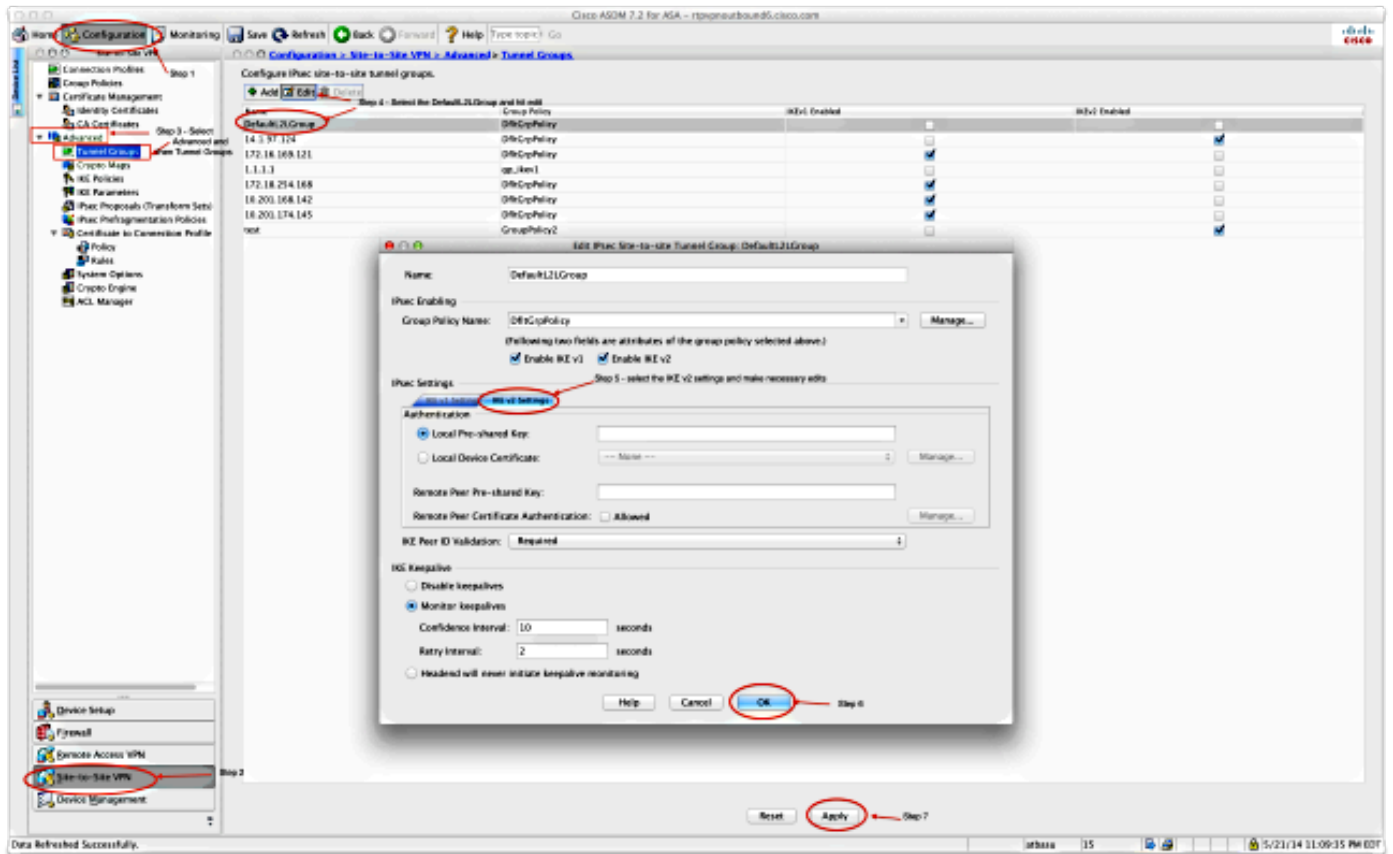
定隧道组上进行连接。在这种情况下，可以使用DefaultL2L组以允许动态连接。

> **提示**：使用此方法，缺点是所有对等体将具有相同的预共享密钥，因为每个隧道组只能定义一个预共享密钥，并且所有对等体将连接到同一DefaultL2LGroup隧道组。

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 *****
```

在自适应安全设备管理器(ASDM)上，可以配置DefaultL2LGroup，如下所示：

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上，您可以使用标准向导设置适当的连接配置文件，或者只需添加新连接并遵循标准步骤。

解决方案2 — 创建用户定义的隧道组

此方法需要稍多配置，但允许更精细的配置。每个对等体可以有其自己的单独策略和预共享密钥。但是，在此必须更改动态对等体上的ISAKMP ID，以便它使用名称而不是IP地址。这允许静态ASA将传入的ISAKMP初始化请求与正确的隧道组匹配并使用正确的策略。

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
```
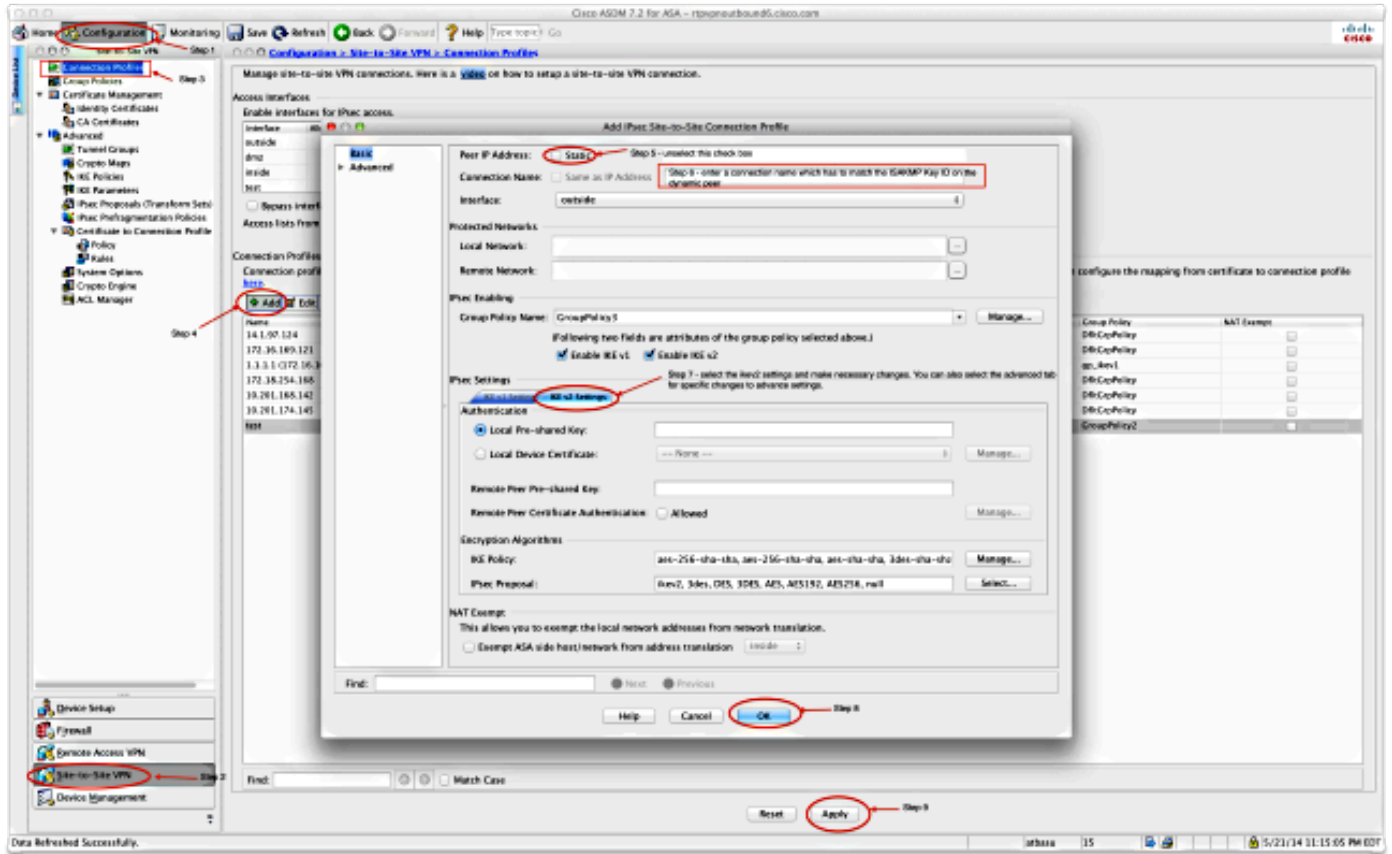
```
tunnel-group DynamicSite2Site1 general-attributes
 default-group-policy GroupPolicy4
tunnel-group DynamicSite2Site1 ipsec-attributes
 IKEv2 remote-authentication pre-shared-key *****
 IKEv2 local-authentication pre-shared-key *****
```

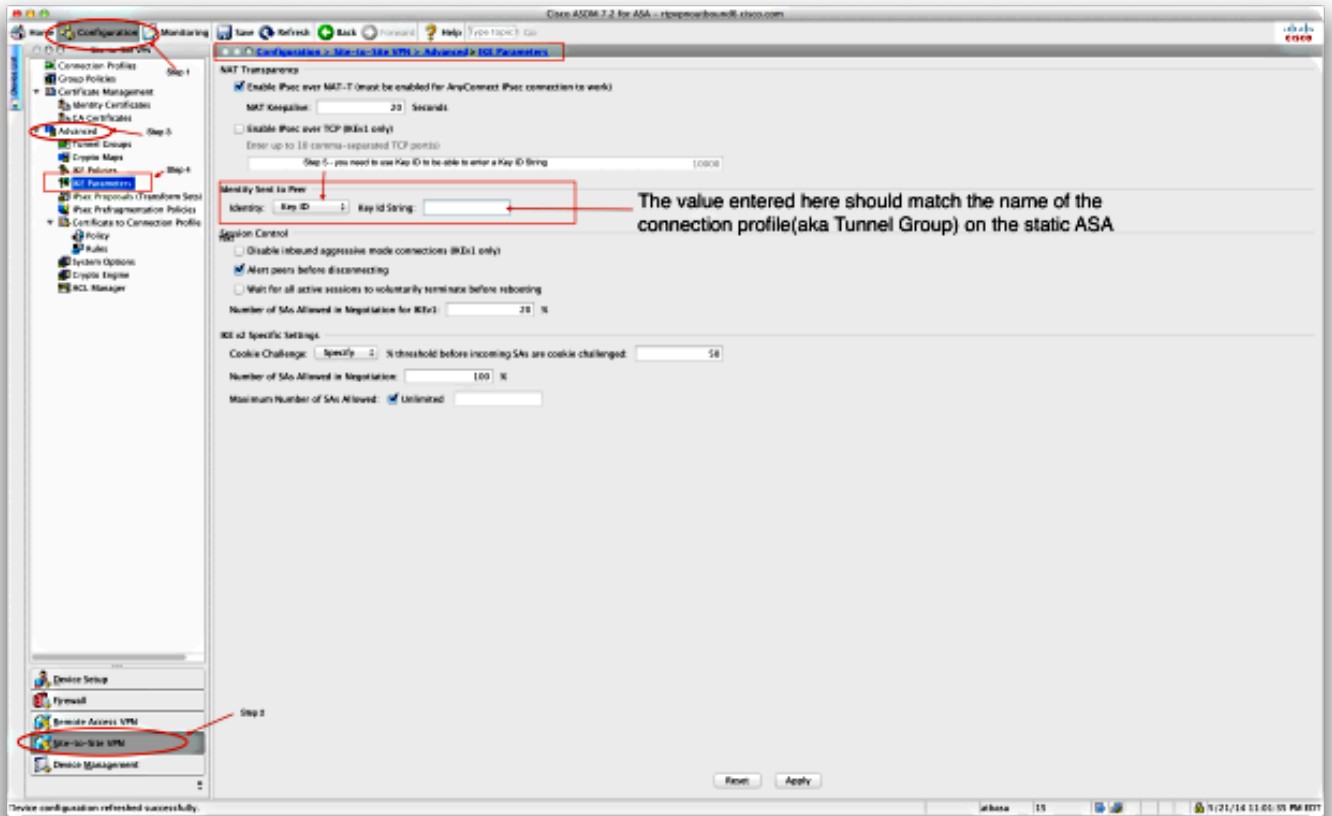在ASDM上，连接配置文件名称默认为IP地址。因此，创建时，必须对其进行更改，以便为其提供如下屏幕截图所示的名称：

动态 ASA 配置

在两个解决方案中，动态ASA的配置方式几乎相同，添加了一个命令，如下所示：

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

如前所述，默认情况下，ASA使用VPN隧道映射到的接口的IP地址作为ISAKMP密钥ID。但是，在这种情况下，动态ASA上的key-ID与静态ASA上隧道组的名称相同。因此，在每个动态对等体上，key-id将不同，并且必须在具有正确名称的静态ASA上创建相应的隧道组。

在ASDM上，可以按照以下屏幕截图所示配置：

The value entered here should match the name of the connection profile(aka Tunnel Group) on the static ASA

验证

使用本部分可确认配置能否正常运行。

在静态ASA上

以下是 show crypto IKEv2 sa 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
```

以下是 show crypto ipsec sa 命令的结果：

```
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上

以下是 show crypto IKEv2 sa detail 命令的结果：

```
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
```

以下是 show crypto ipsec sa 命令的结果：

```
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。使用输出解释器工具来查看 show 命令输出的分析。

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。使用输出解释器工具来查看 show 命令输出的分析。

> **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
- deb crypto IKEv2 internal