ASA到ASA动态到静态IKEv1/IPsec配置示例

目录

简介

本文档介绍如何使自适应安全设备(ASA)接受来自任何动态对等体（本例中为ASA）的动态IPsec站点到站点VPN连接。 如本文档中的网络图所示，当仅从Remote-ASA端启动隧道时，会建立IPsec隧道。由于动态IPsec配置，Central-ASA无法启动VPN隧道。Remote-ASA的IP地址未知。

配置Central-ASA以动态接受来自通配符IP地址(0.0.0.0/0)和通配符预共享密钥的连接。然后，将Remote-ASA配置为按照加密访问列表的指定，加密从本地到Central-ASA子网的流量。两端都执行网络地址转换(NAT)免除，以绕过IPsec流量的NAT。

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Cisco ASA（5510和5520）防火墙软件版本9.x及更高版本。

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。

配置

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

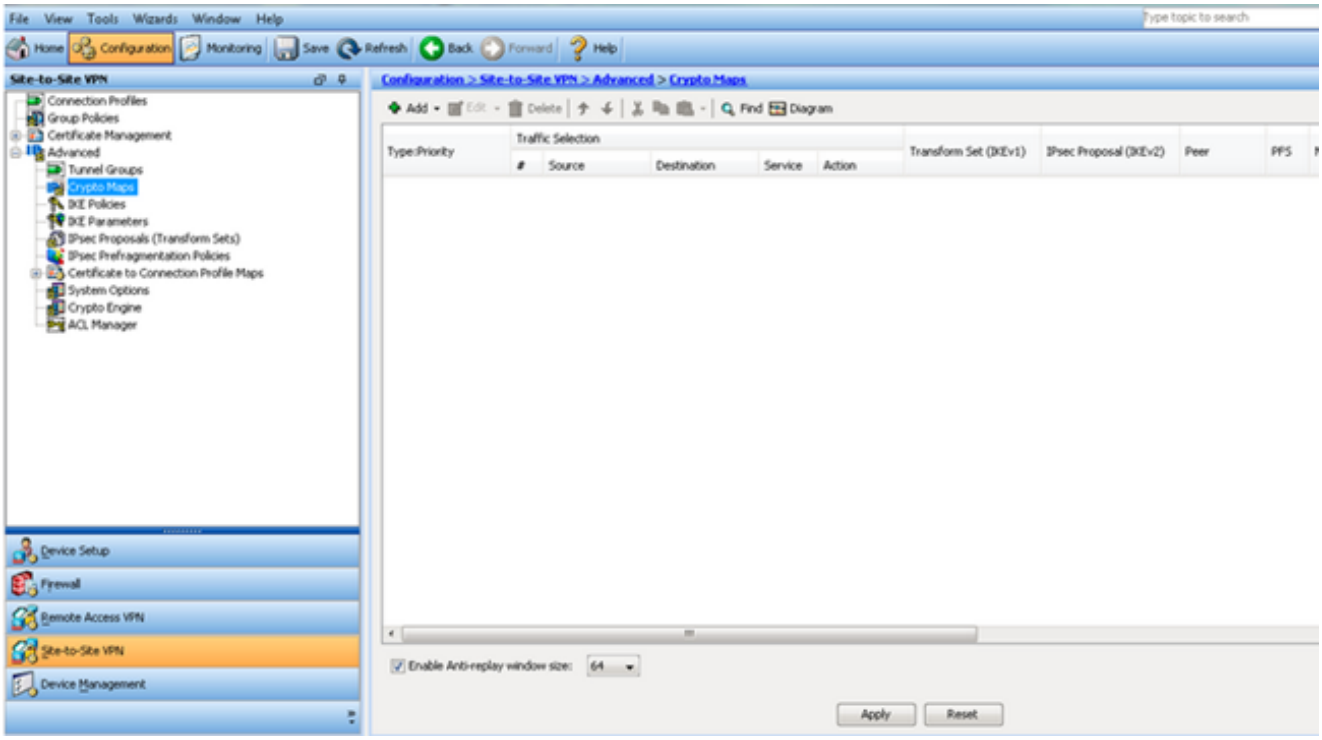
网络图

ASDM 配置

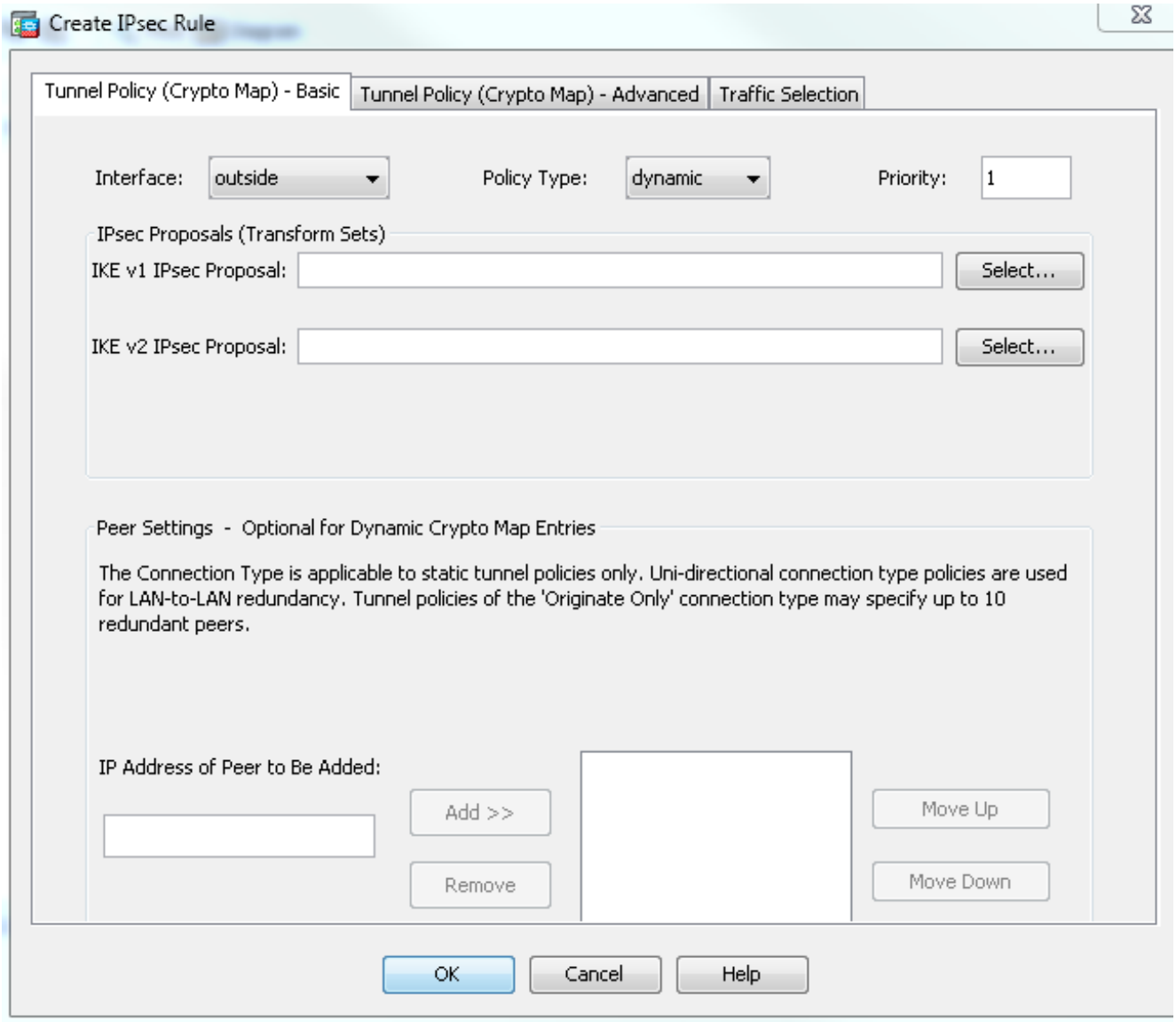
Central-ASA（静态对等体）

在具有静态IP地址的ASA上，设置VPN的方式是，它接受来自未知对等体的动态连接，同时仍使用IKEv1预共享密钥对对等体进行身份验证：

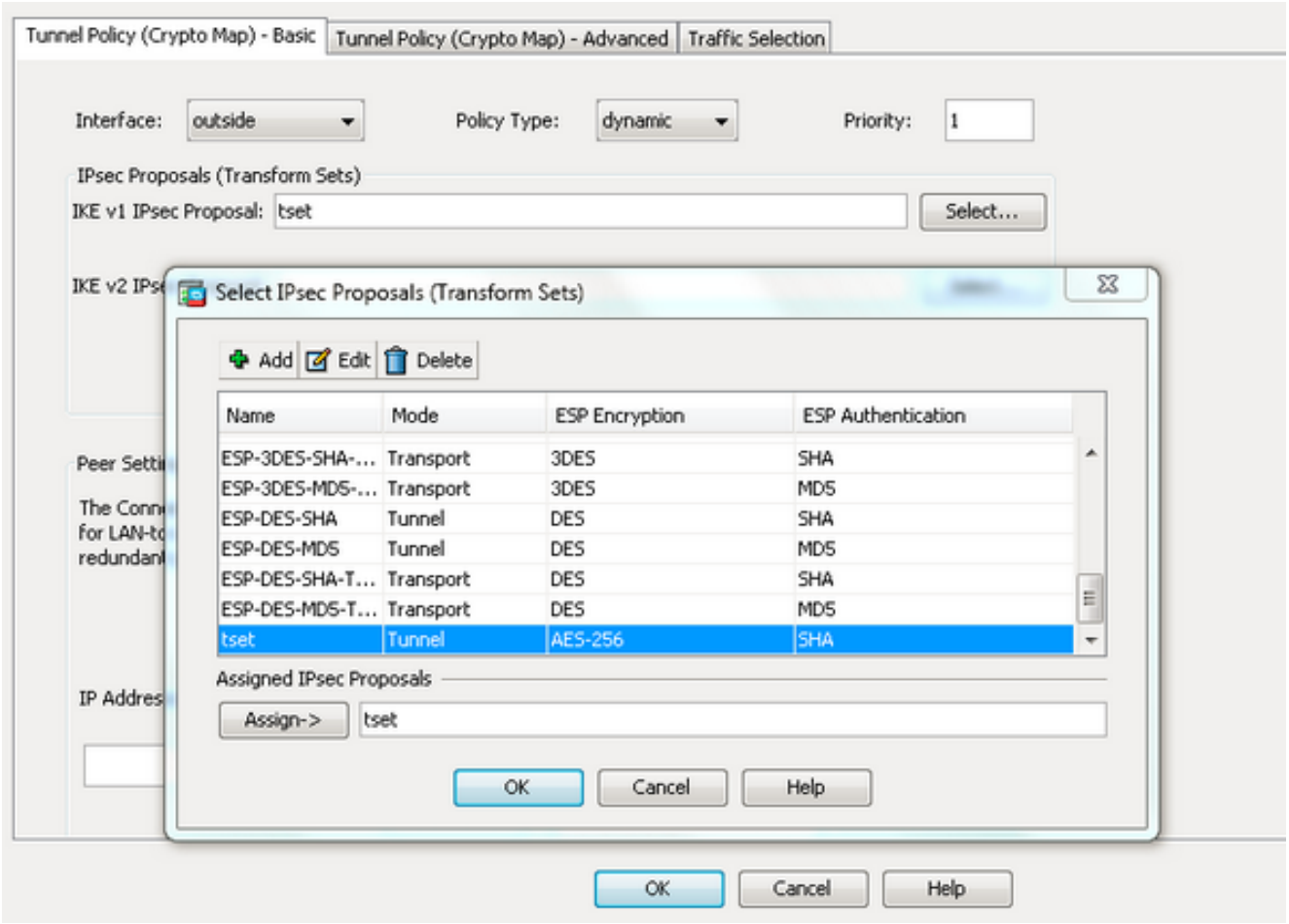
1. 选择**Configuration > Site-to-Site VPN > Advanced > Crypto Maps**。该窗口显示已有（如果有）的加密映射条目列表。 由于ASA不知道对等IP地址是什么，因此ASA要接受连接配置具有匹配转换集（IPsec建议）的**动态映**射。 单击 **Add**。



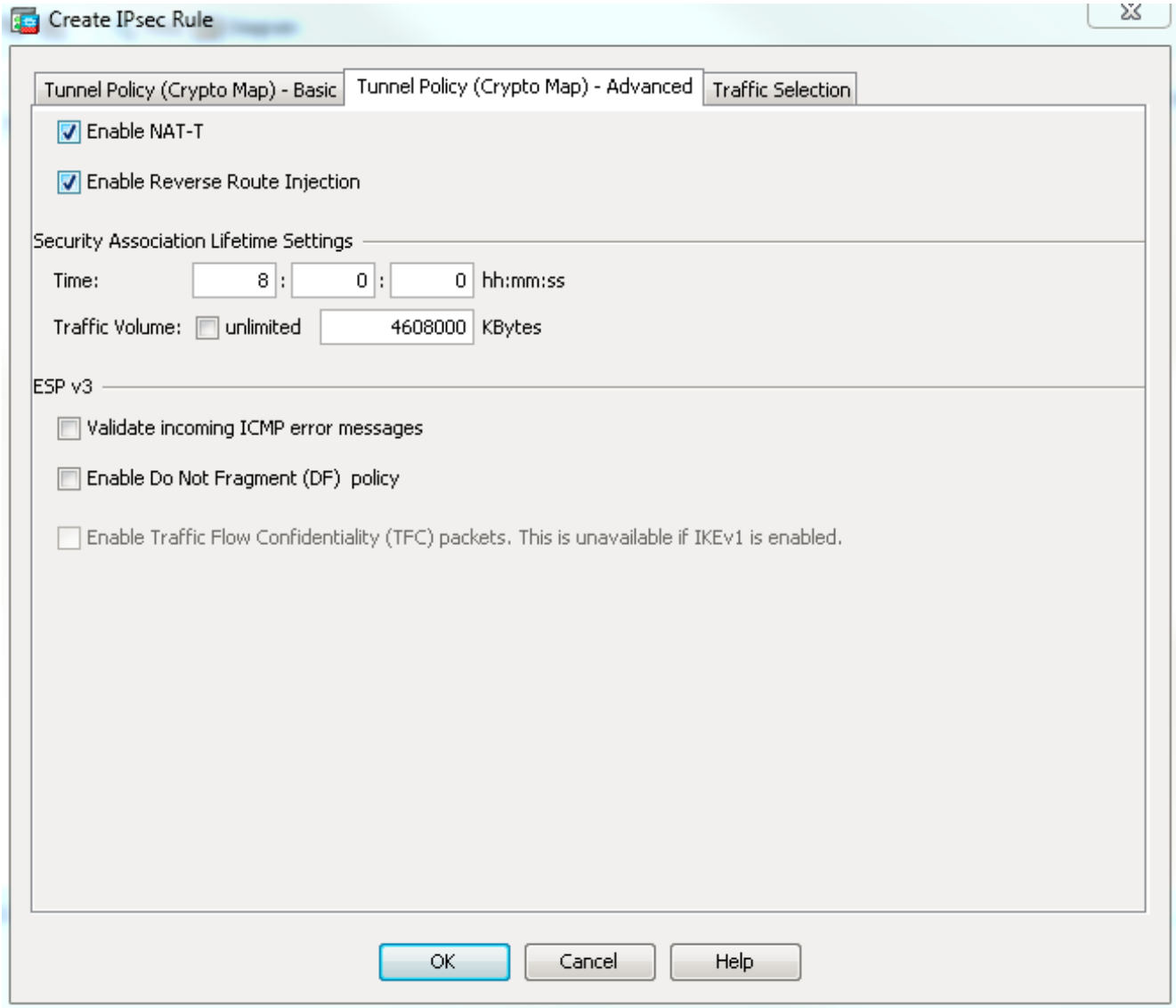
2. 在Create IPsec Rule窗口的Tunnel Policy(Crypto Map)- Basic选项卡中，从Interface下拉列表中选择**outside**，并从Policy Type下拉列表中选择**dynamic**。在Priority字段中，为此条目分配优先级，以防在Dynamic-Map下有多个条目。接下来，单击IKE v1 IPsec建议字段旁边的**选择**以选择IPsec建议。



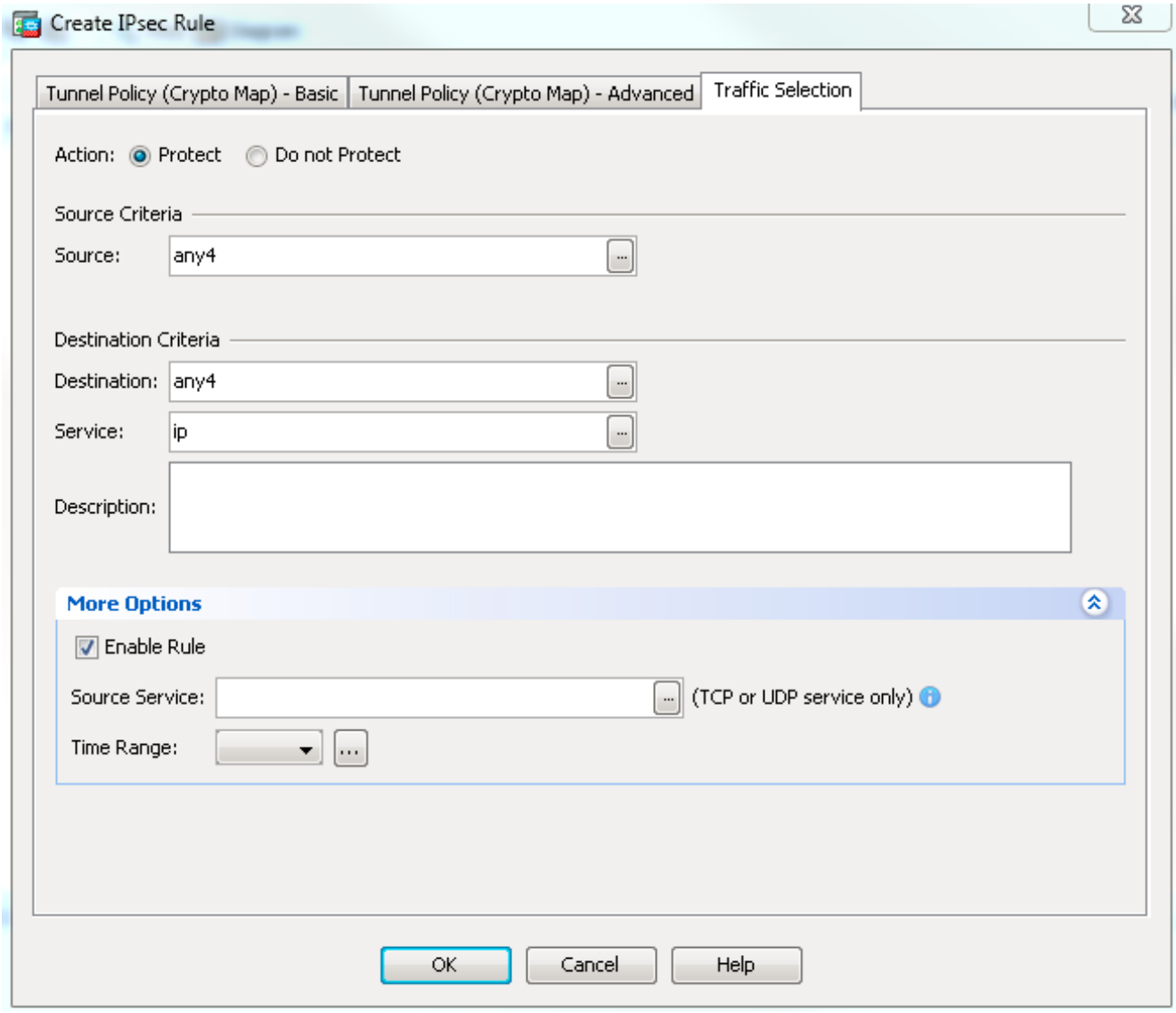
3. 当“选择IPsec建议（转换集）”对话框打开时，从当前IPsec建议中选择，或单击“添加”以创建新建议并使用相同建议。完成后单击 **OK。**

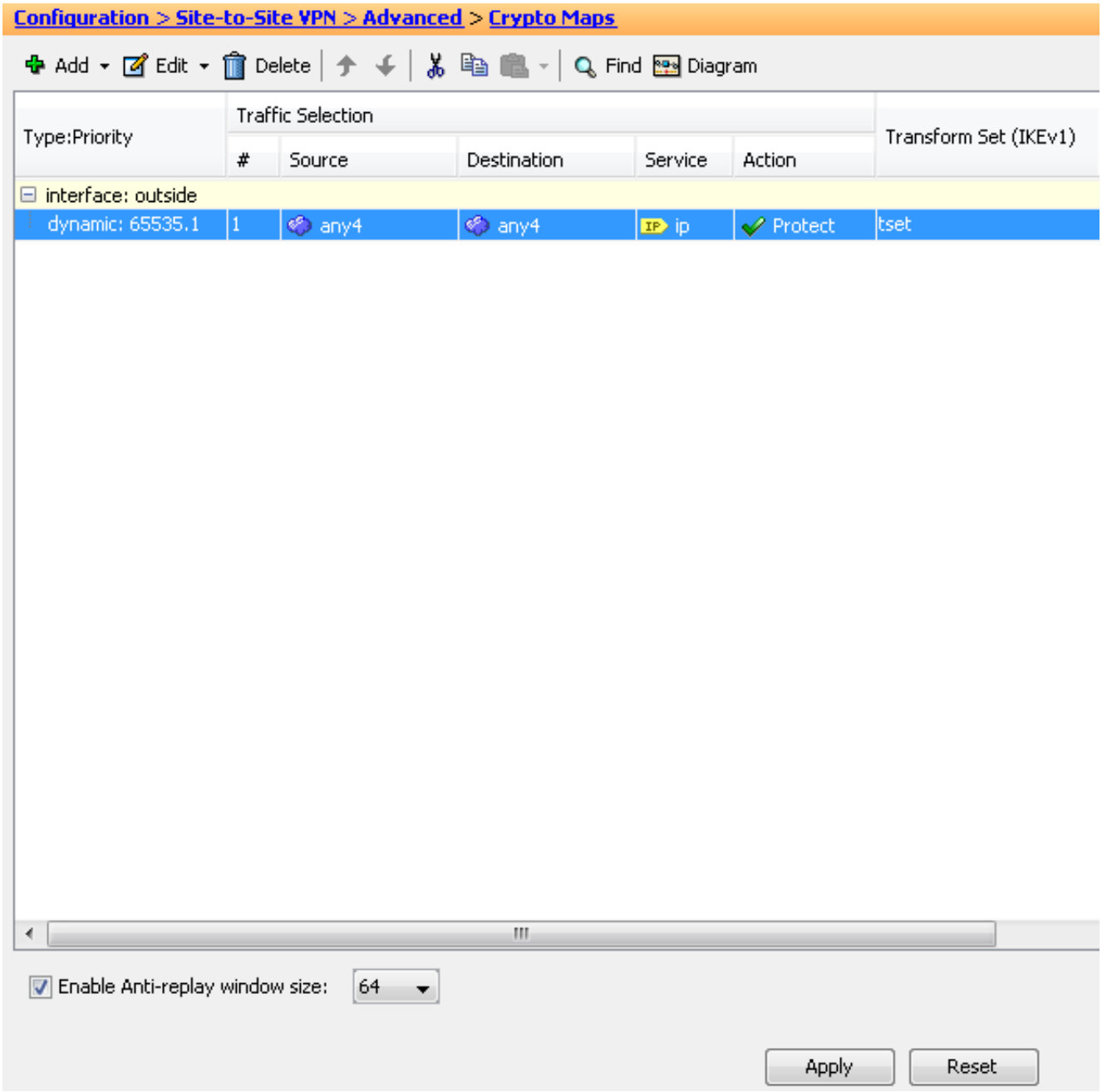


4. 在Tunnel Policy(Crypto Map)-Advanced选项卡中，选中**Enable NAT-T** 复选框（如果对等体位于NAT设备后，则为必选项）和**Enable Reverse Route Injection**复选框。当VPN隧道为动态对等体启用时，ASA为指向VPN接口的协商远程VPN网络安装动态路由。



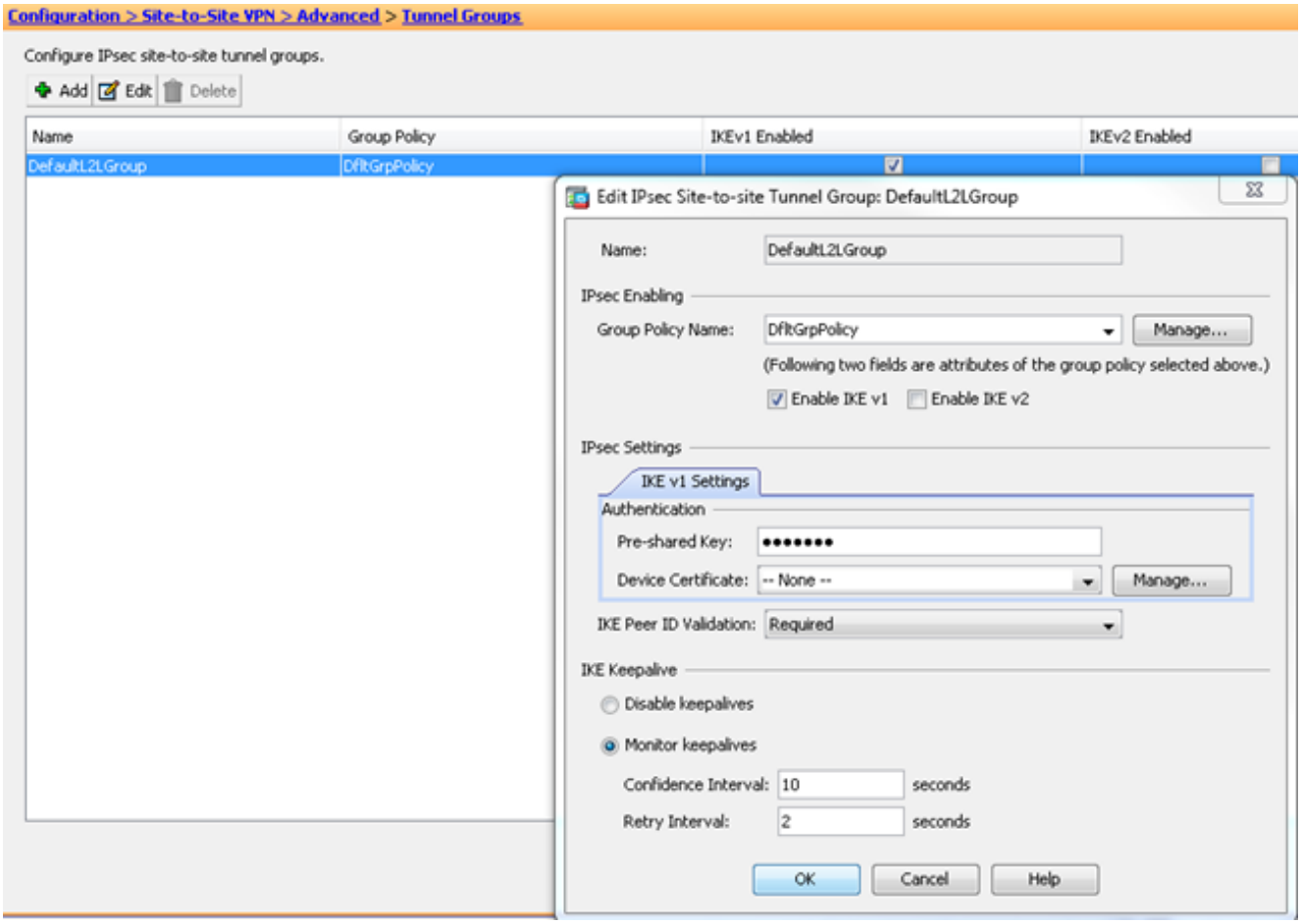
或者，从Traffic Selection（流量选择）选项卡中，您还可以定义动态对等体的相关VPN流量，然后单击**OK（确定）**。


Create IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
Action:
Protect
Do not Protect
Source Criteria
Source:
any4
Destination Criteria
Destination:
any4
Service:
ip
Description:
More Options
Enable Rule
Source Service:
(TCP or UDP service only)
Time Range:
OK
Cancel
Help



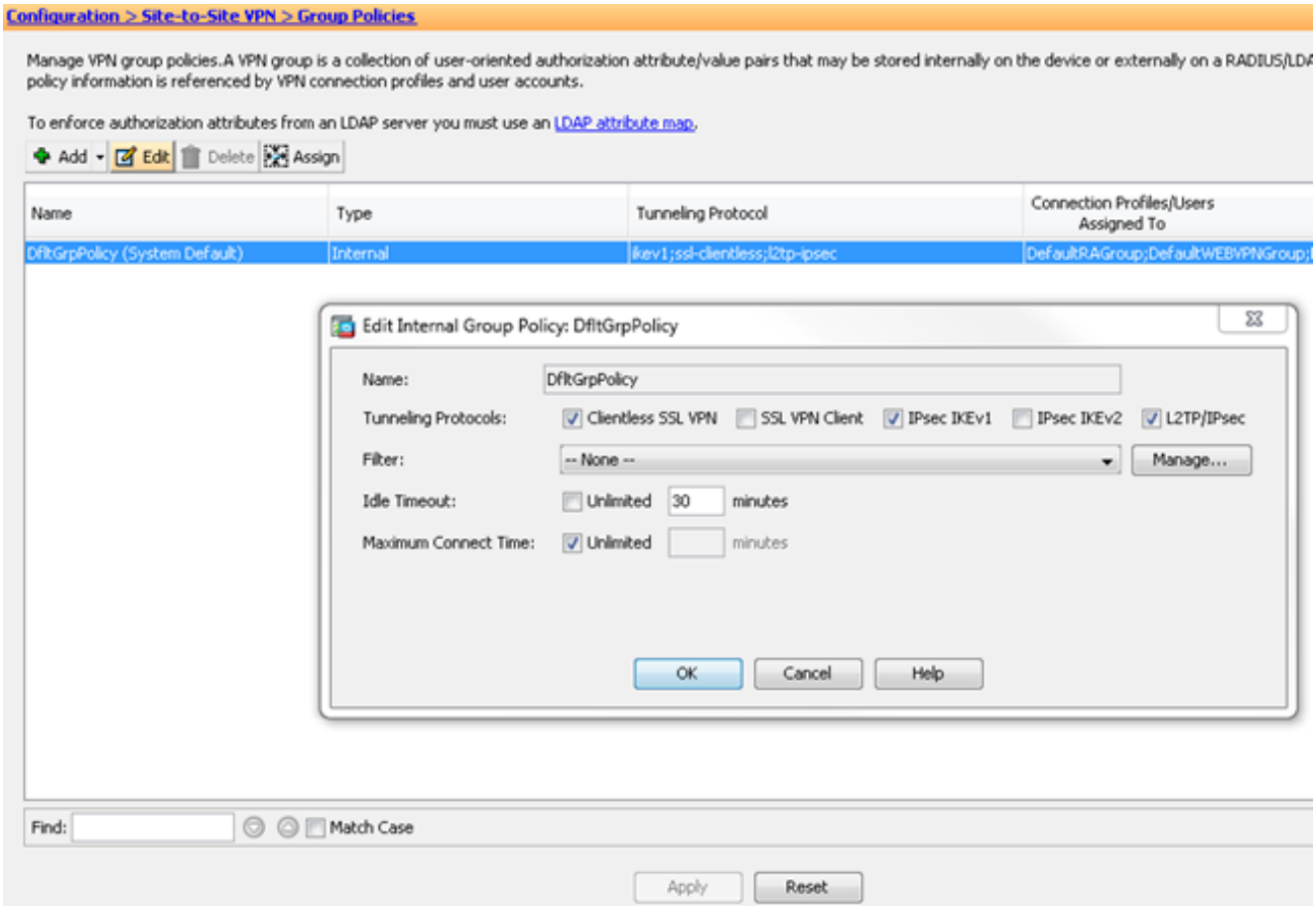
如前所述，由于ASA没有任何有关远程动态对等体IP地址的信息，因此未知连接请求将降级到DefaultL2LGroup下，默认情况下，ASA上存在该组。为了使身份验证成功，远程对等体上配置的预共享密钥（本例中为cisco123）需要与DefaultL2LGroup下的密钥匹配。

5. 选择**Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**，选择**DefaultL2LGroup**，单击**Edit**并配置所需的预共享密钥。完成后单击 **OK**。

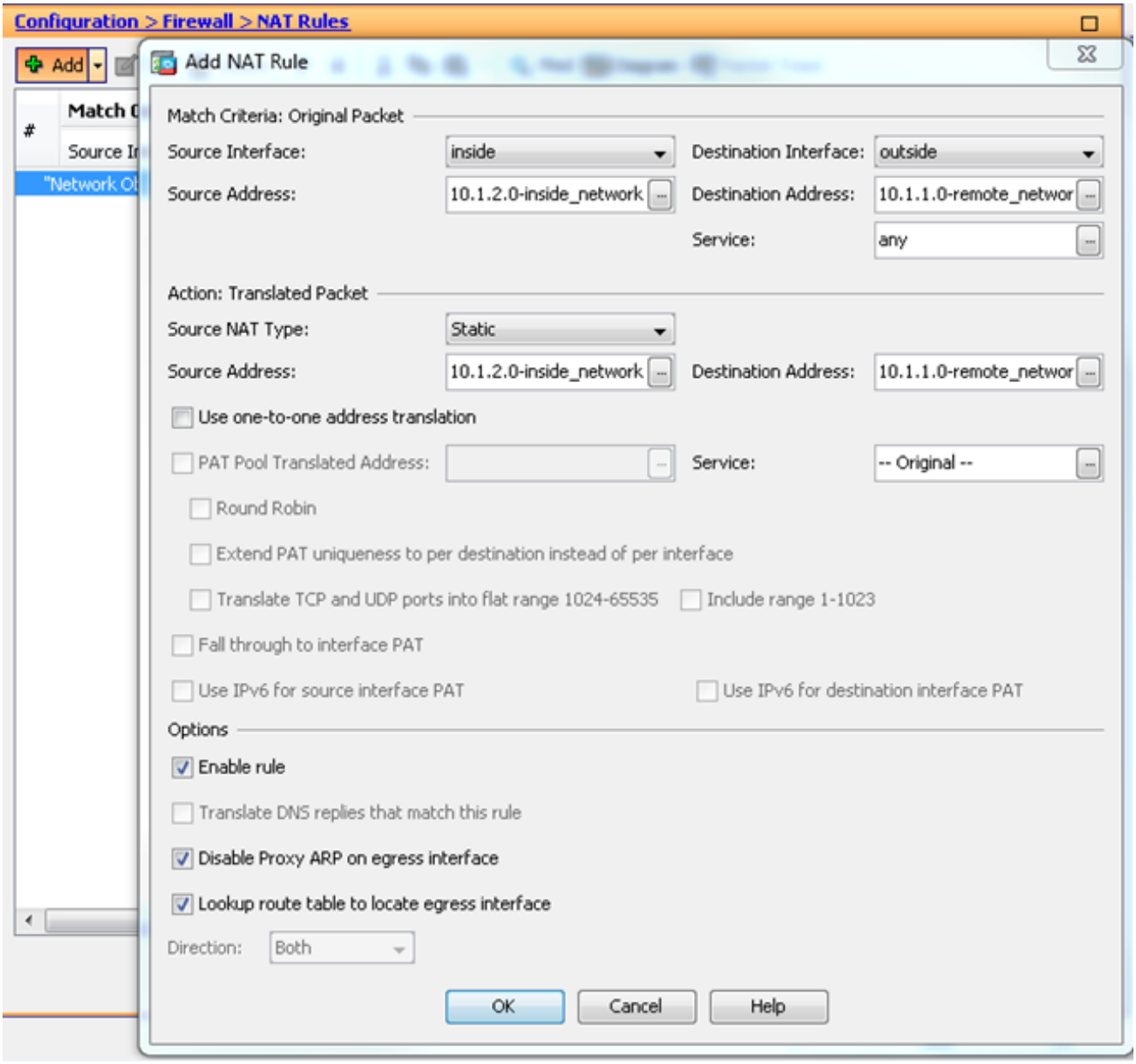


注意：这会在静态对等体(Central-ASA)上创建通配符预共享密钥。 任何知道此预共享密钥及其匹配建议的设备/对等体都可以成功建立VPN隧道并通过VPN访问资源。确保此预删密钥不与未知实体共享，且不易猜测。

6. 选择**Configuration > Site-to-Site VPN > Group Policies**，然后选择您选择的组策略（本例中为默认组策略）。单击**Edit**，然后在“Edit Internal Group Policy”对话框中编辑组策略。完成后单击 **OK。**

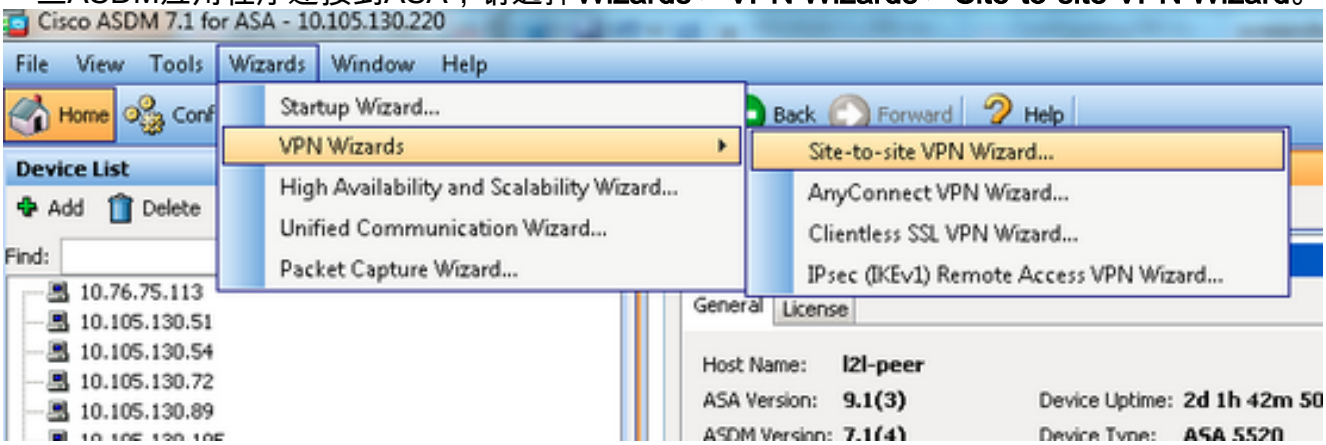


7. 选择**Configuration > Firewall > NAT Rules**，然后从Add Nat Rule窗口为VPN流量配置no nat(NAT-EXEMPT)规则。完成后单击 **OK。**

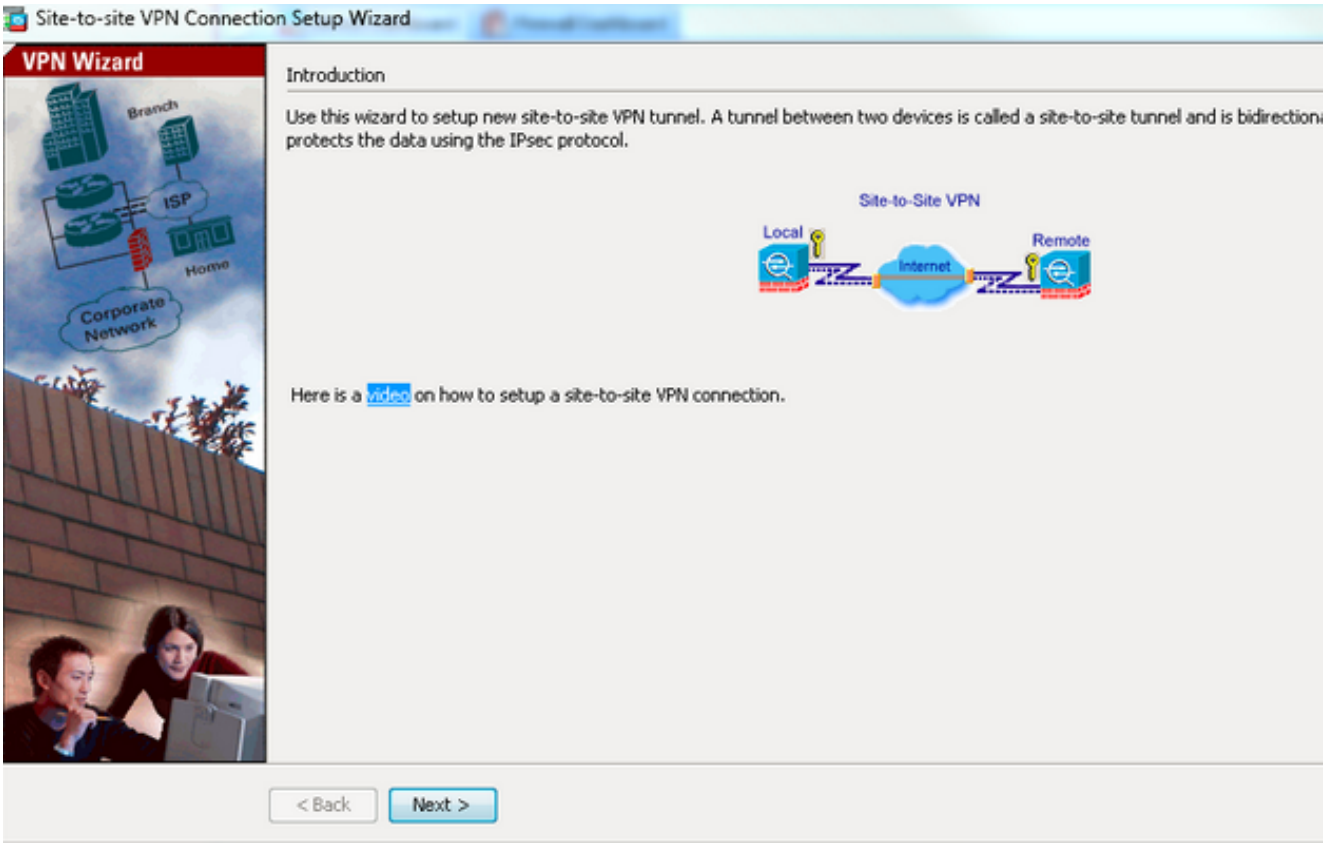


Remote-ASA（动态对等体）

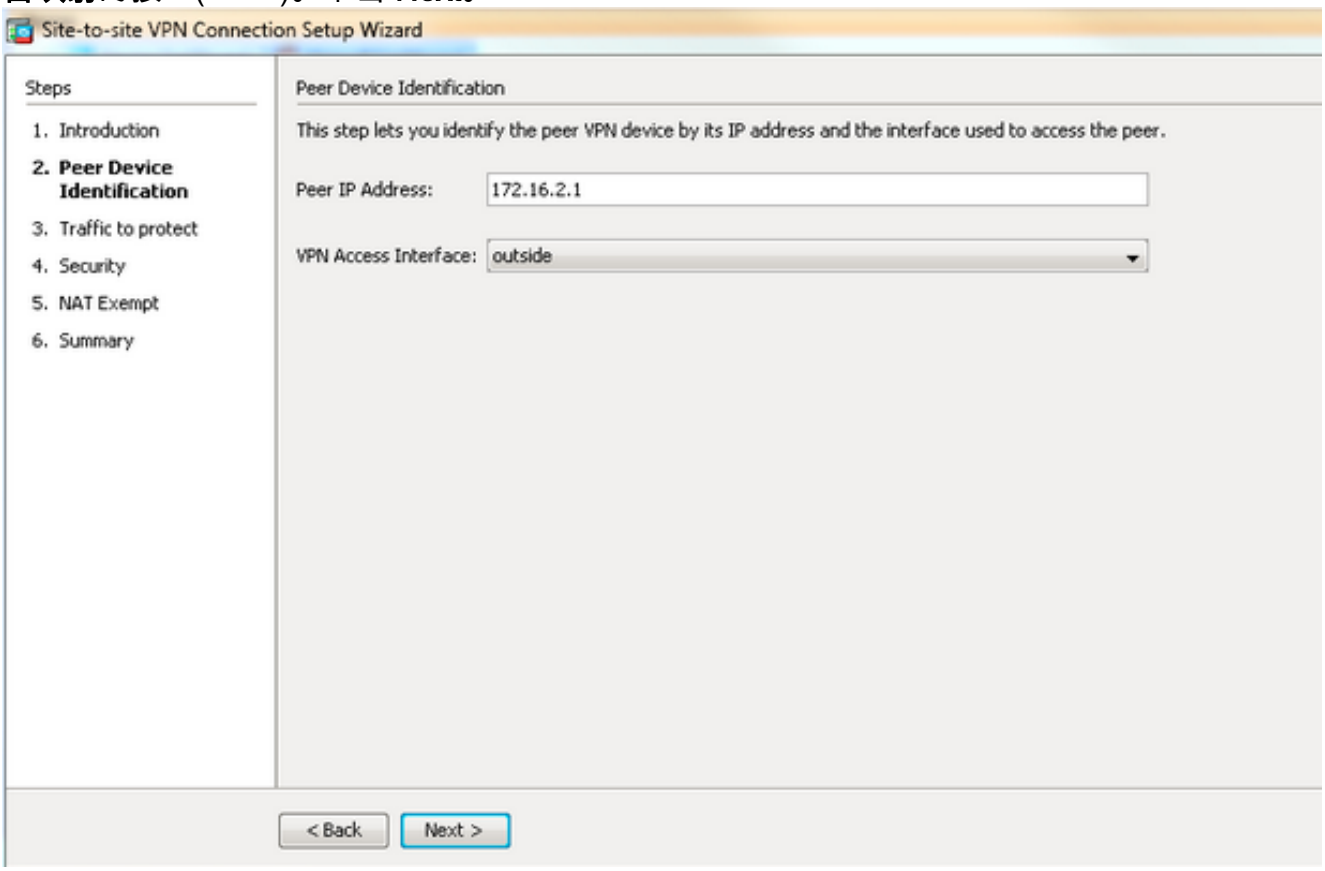
1. 一旦ASDM应用程序连接到ASA，请选择**Wizards > VPN Wizards > Site-to-site VPN Wizard**。



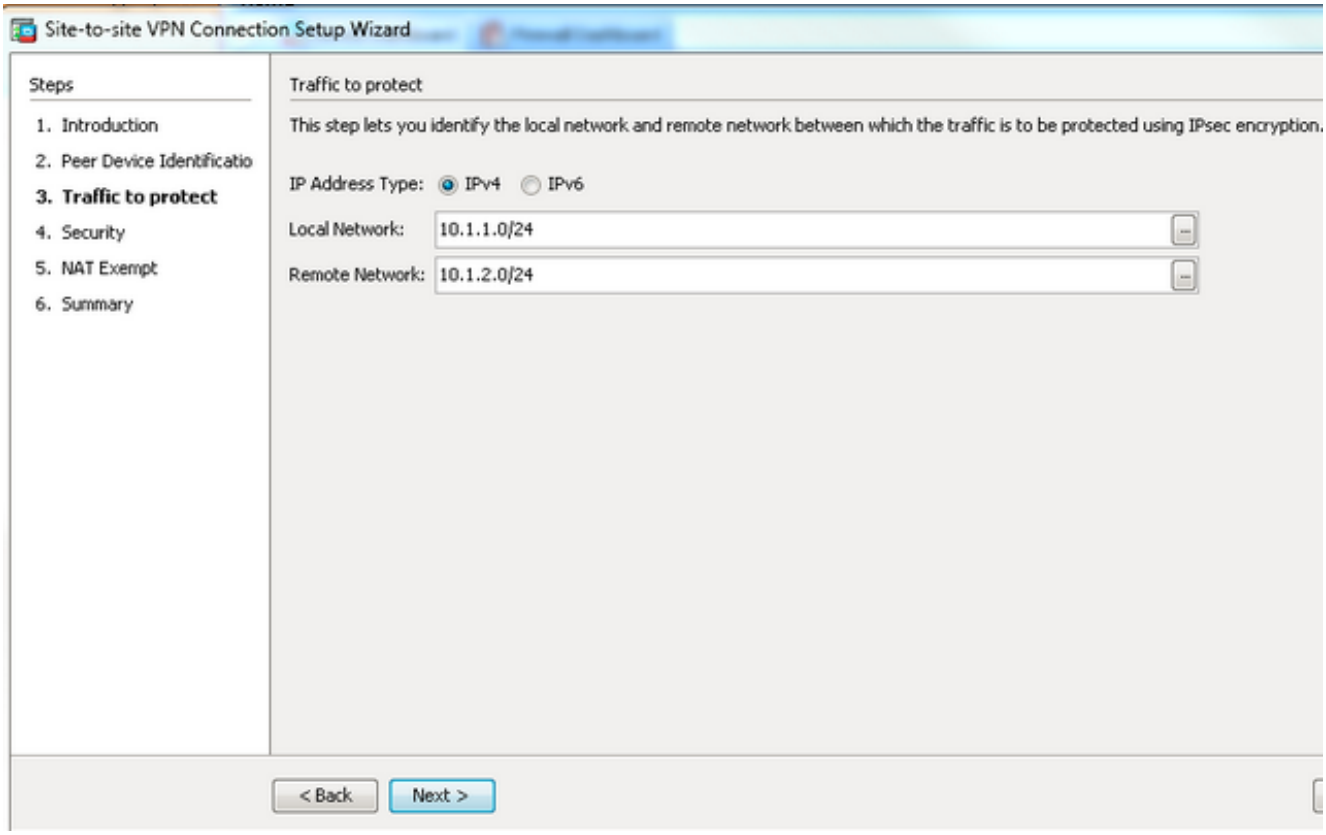
2. 单击 **Next**。



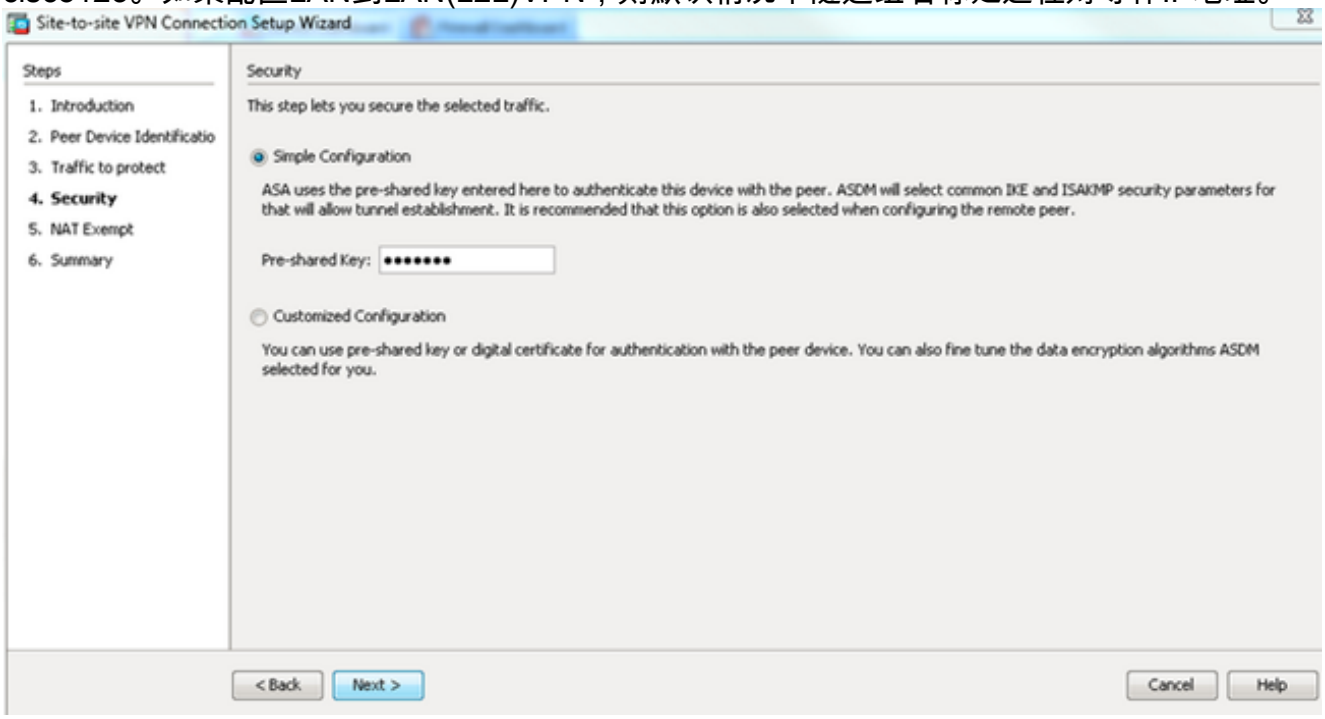
3. 从VPN Access Interface下拉列表中选择**outside**以指定远程对等体的外部IP地址。选择应用加**密映射**的接口(WAN)。单击 **Next**。



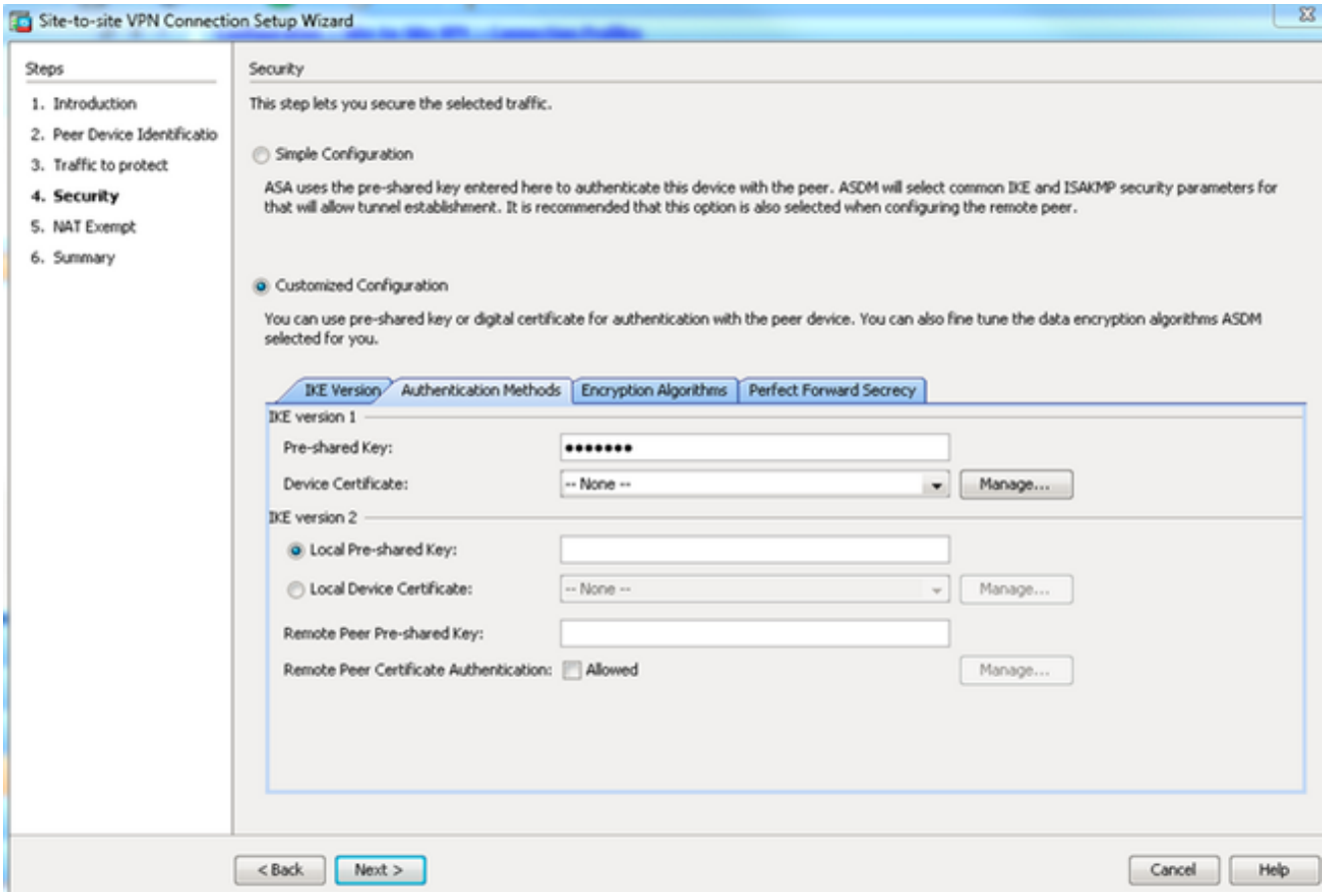
4. 指定应允许通过VPN隧道的主机/网络。在此步骤中，您需要为VPN隧道提供本地网络和远程网络。点击Local Network（本地网络）和Remote Network（远程网络）字段旁边的按钮，然后根据需要选择地址。完成后**单击**“下一步”。



5. 输入要使用的身份验证信息，在本例中为预共享密钥。本示例中使用的预共享密钥是cisco123。如果配置LAN到LAN(L2L)VPN，则默认情况下隧道组名称是远程对等体IP地址。

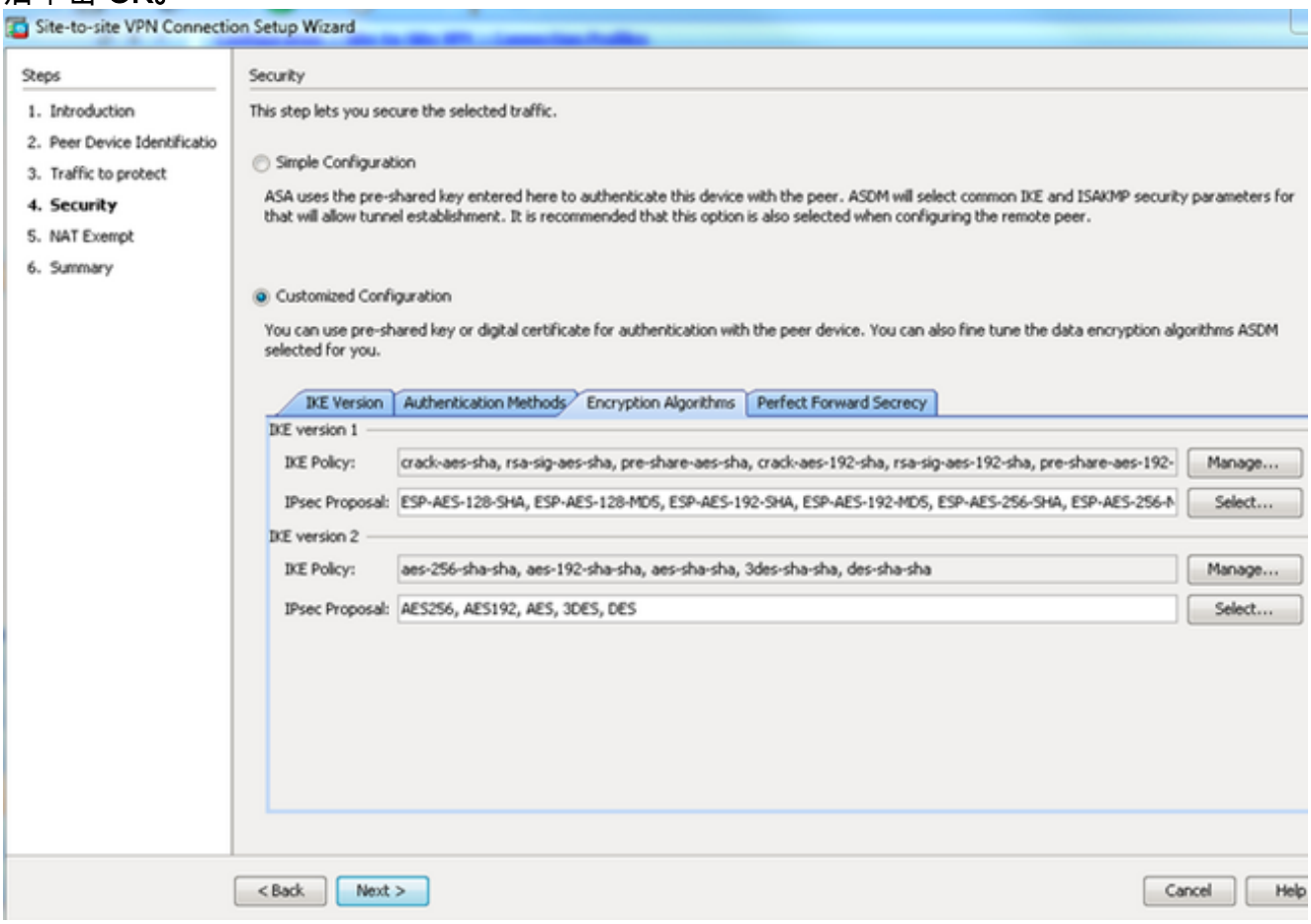


或者您可以自定义配置以包括您选择的IKE和IPsec策略。对等体之间至少需要一个匹配策略：在Authentication Methods选项卡的Pre-shared Key字段中，输入IKE version 1 pre-shared Key。在本例中，它是**cisco123**。

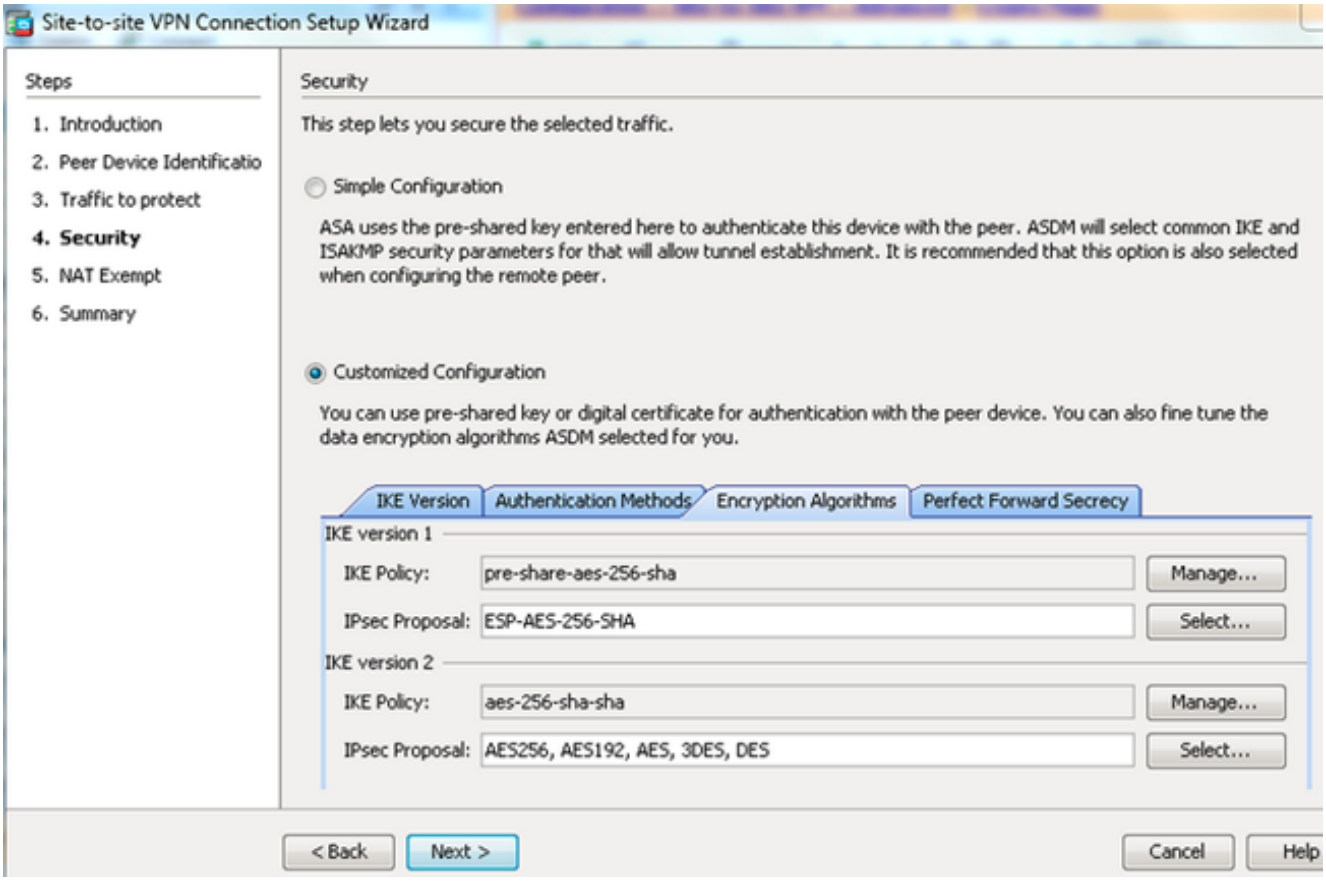


单击“Encryption Algorithms(加**密算法)”**选项卡。

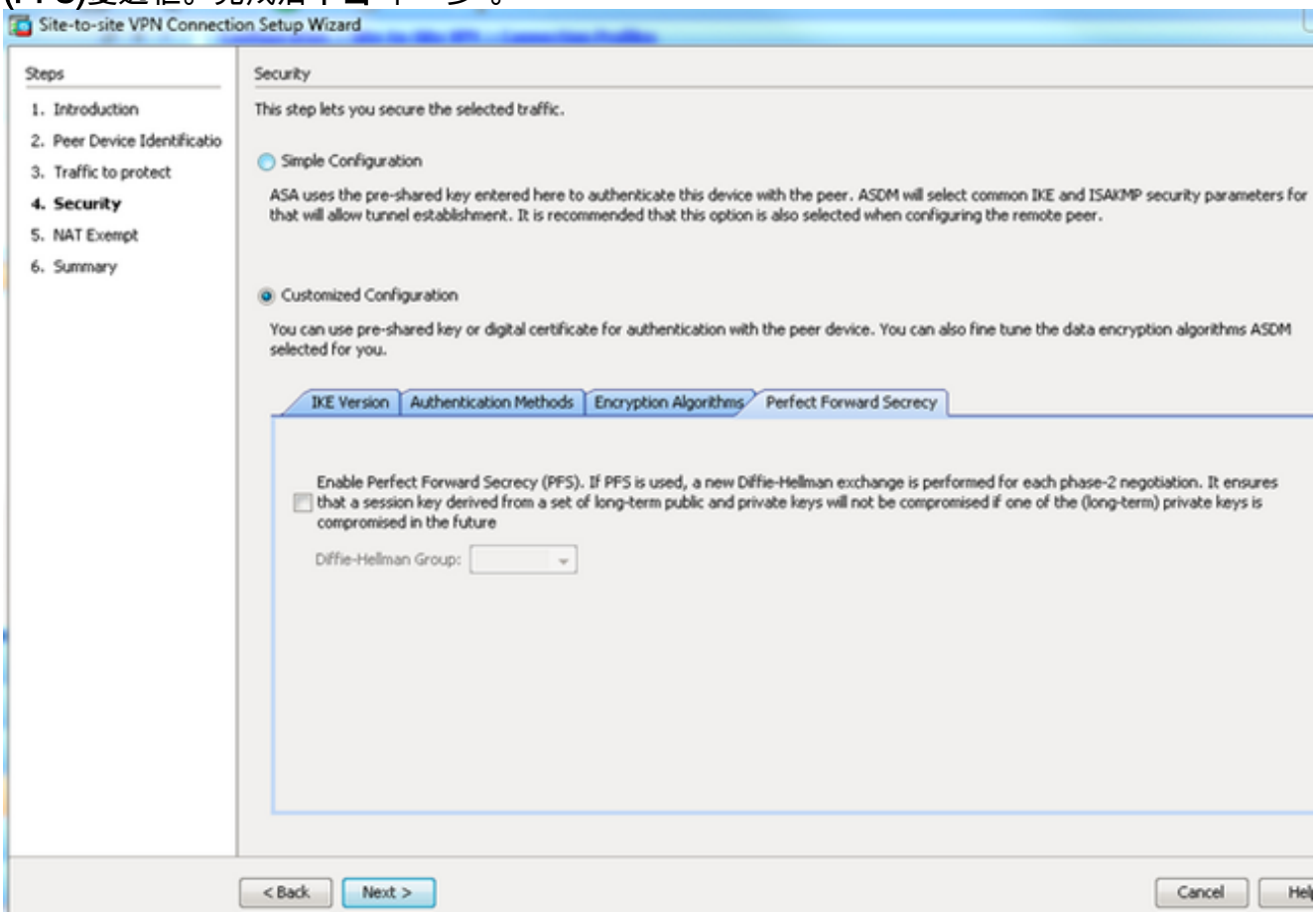
6. 单击**Manage**(IKE策略)字段旁边的，单击**Add（添加）并配置自定义IKE策略(第**1阶段)。 完成后单击 **OK。**



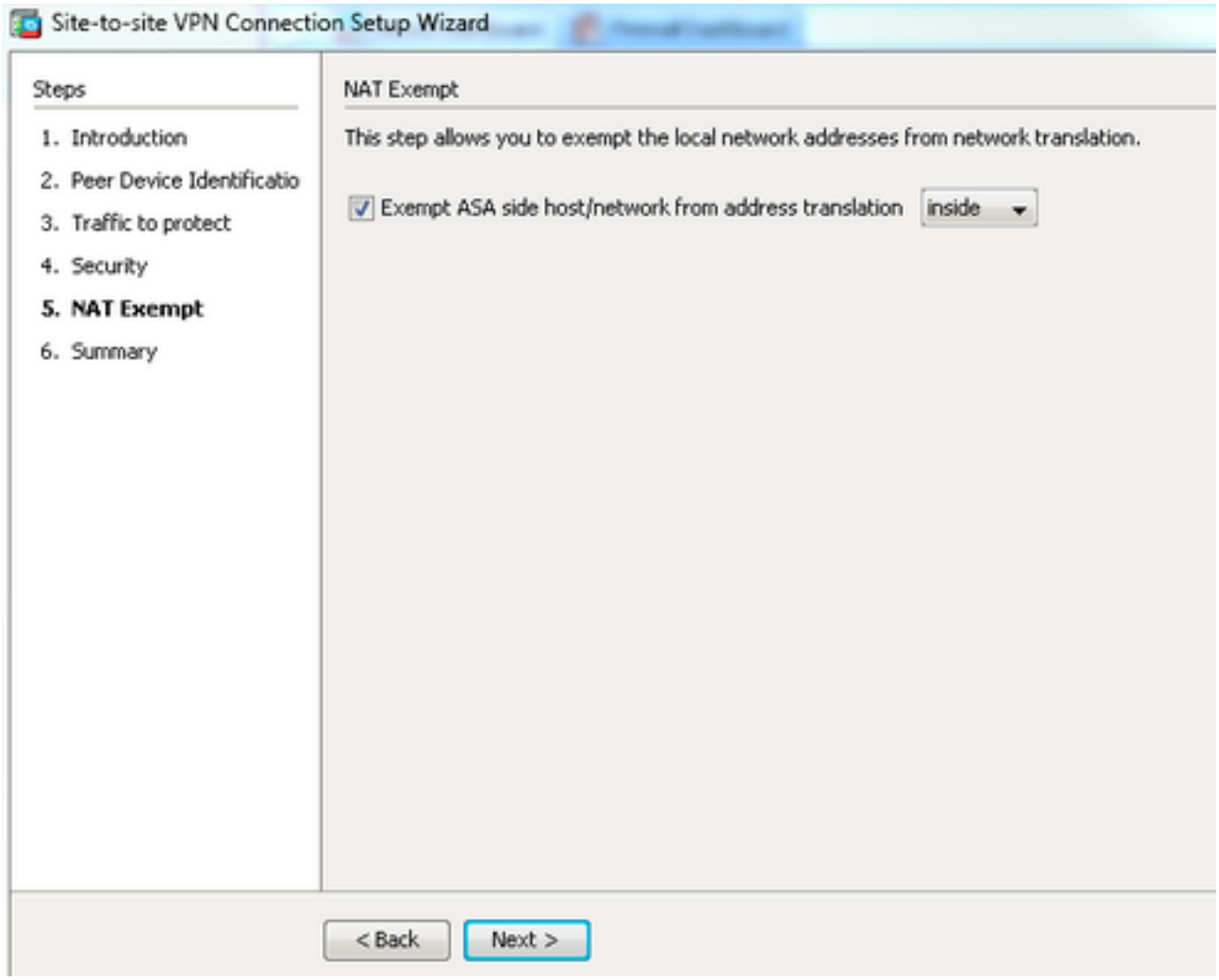
7. 单击IPsec Proposal字段旁的**Select**，然后选择所需的IPsec Proposal。完成后**单击**“下一步”。



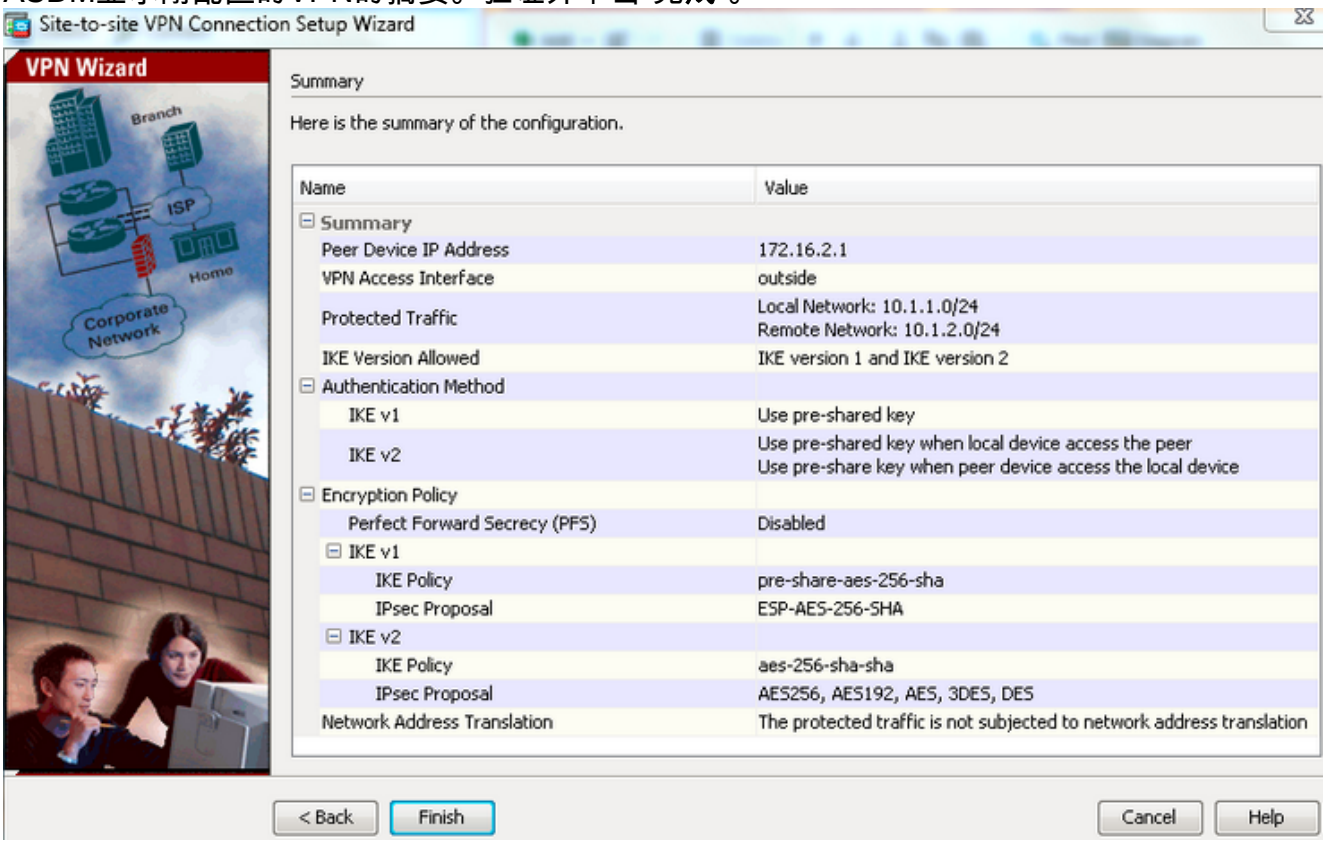
或者，您可以转到完全向前保密(Perfect Forward Secrecy)选项卡并选中**启用完全向前保密(PFS)**复选框。完成后**单击**“下一步”。



8. 选中**Exempt ASA side host/network from address translation**复选框以防止隧道流量从网络地址转换开始。从下拉列**表中选**择本地或内部，以设置可访问本地网络的接口。单击 **Next。**



9. ASDM显示刚配置的VPN的摘要。验证并单击“完**成**”。



CLI 配置

中央ASA（静态对等体）配置

1. 为VPN流量配置NO-NAT/NAT-EXEMPT规则，如以下示例所示：
```
object network 10.1.1.0-remote_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```
2. 在DefaultL2LGroup下配置预共享密钥，以验证任何远程Dynamic-L2L-peer:
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. 定义第2阶段/ISAKMP策略：
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. 定义第2阶段转换集/IPsec策略：
```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```
5. 使用以下参数配置动态映射： 所需的转换集启用反向路由注入(RRI)，允许安全设备学习连接客户端的路由信息（可选）
```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```
6. 将动态映射绑定到加密映射，应用加密映射并在外部接口上启用ISAKMP/IKEv1:
```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside
crypto ikev1 enable outside
```

Remote-ASA（动态对等体）

1. 为VPN流量配置NAT免除规则：
```
object network 10.1.1.0-inside_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-remote_network
subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup
```
2. 为静态VPN对等体和预共享密钥配置隧道组。
```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```
3. 定义PHASE-1/ISAKMP策略：
```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

4. 定义第2阶段转换集/IPsec策略：
   crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
5. 配置定义相关VPN流量/网络的访问列表：
   access-list outside_cryptomap extended permit ip object
   10.1.1.0-inside_network object 10.1.2.0-remote_network
6. 使用以下参数配置静态加密映射： 加密/VPN访问列表远程IPsec对等IP地址所需的转换集
   crypto map outside_map 1 match address outside_cryptomap
   crypto map outside_map 1 set peer 172.16.2.1
   crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
7. 在外部接口上应用加密映射并启用ISAKMP/IKEv1:
   crypto map outside_map interface outside
   crypto ikev1 enable outside

验证

使用此部分确认配置是否正常工作。

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。

- **show crypto isakmp sa** — 显示对等体上的所有当前IKE安全关联(SA)。
- **show crypto ipsec sa** — 显示所有当前IPsec SA。

本部分显示两个ASA的验证输出示例。

中央ASA

```
Central-ASA#show crypto isakmp sa

  IKEv1 SAs:

     Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

  1   IKE Peer: 172.16.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

    Central-ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

        local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1

        #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #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.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 30D071C0
      current inbound spi : 38DA6E51

      inbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

远程ASA

```
Remote-ASA#show crypto isakmp sa

  IKEv1 SAs:

     Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

  1   IKE Peer: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

  Remote-ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

        access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1

        #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #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.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
    path mtu 1500, ipsec overhead 74(44), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 38DA6E51
    current inbound spi : 30D071C0

    inbound esp sas:
    spi: 0x30D071C0 (818966976)
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, IKEv1, }
       slot: 0, conn_id: 8192, crypto-map: outside_map
       sa timing: remaining key lifetime (kB/sec): (4373999/28676)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x0000001F
  outbound esp sas:
    spi: 0x38DA6E51 (953839185)
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, IKEv1, }
       slot: 0, conn_id: 8192, crypto-map: outside_map
       sa timing: remaining key lifetime (kB/sec): (4373999/28676)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

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。

使用以下命令可以：

```
clear crypto ikev1 sa <peer IP address>
Clears the Phase 1 SA for a specific peer.
```

警告：clear crypto isakmp sa 命**令清除所有活动VPN隧道时，它是侵入式的。**

在PIX/ASA软件版本8.0(3)及更高版本中，可以使用clear crypto isakmp sa **<peer ip address>命令**清*除单个IKE SA*。在早于8.0(3)的软件版本中，请使用**vpn-sessiondb logoff tunnel-group *<tunnel-group-name>***命令以清除单个隧道的IKE和IPsec SA。

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1

clear crypto ipsec sa peer <peer IP address>
!!! Clears the required Phase 2 SA for specific peer.
```

```
debug crypto condition peer < Peer address>
!!! Set IPsec/ISAKMP debug filters.
debug crypto isakmp sa <debug level>
!!! Provides debug details of ISAKMP SA negotiation.
debug crypto ipsec sa <debug level>
!!! Provides debug details of IPsec SA negotiations
undebug all
!!! To stop the debugs
```

使用的调试：

```
debug cry condition peer <remote peer public IP>
debug cry ikev1 127
debug cry ipsec 127
```

Remote-ASA（启动器）

输入此packet-tracer命令以启动隧道：

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
```

```
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED


Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
 Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

Central-ASA（响应器）

```
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
```

.
Jan 20 12:42:35 **[IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group DefaultL2LGroup**
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]**Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED**
:
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, **IKE Responder starting QM**:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Received remote IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0**:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, **Received local IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0, Protocol 0, Port 0**Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 **[IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map check, map outside_dyn_map, seq = 1 is a successful match**
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) **Responder, Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0**:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Adding static route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0**

相关信息

- Cisco ASA系列命令参考
- IPsec 协商/IKE 协议支持页
- 请求注解 (RFC)
- 技术支持和文档 — 思科系统