

ASA 8.x/ASDM 6.x:使用ASDM在现有站点到站点VPN中添加新的VPN对等体信息

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[回退信息](#)

[ASDM 配置](#)

[创建新连接配置文件](#)

[编辑现有VPN配置](#)

[验证](#)

[故障排除](#)

[IKE Initiator unable to find policy:Intrf test_ext , 源 : 172.16.1.103 , 目的 : 10.1.4.251](#)

[相关信息](#)

简介

本文档提供有关使用自适应安全设备管理器(ASDM)将新VPN对等体添加到现有站点到站点VPN配置时要进行的配置更改的信息。在以下场景中，需要执行以下操作：

- Internet服务提供商(ISP)已更改，并使用了一组新的公共IP范围。
- 现场网络的完整重新设计。
- 站点上用作VPN网关的设备将迁移到具有不同公有IP地址的新设备。

本文档假设站点到站点VPN已正确配置且工作正常。本文档提供在L2L VPN配置中更改VPN对等体信息的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- [ASA站点到站点VPN配置示例](#)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科自适应安全设备5500系列，带软件版本8.2及更高版本
- 思科自适应安全设备管理器，软件版本6.3及更高版本

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

回退信息

站点到站点VPN在HQASA和BQASA之间工作正常。假设BQASA已完成网络重新设计，ISP级别的IP方案已修改，但所有内部子网详细信息保持不变。

此示例配置使用以下IP地址：

- 现有BQASA外部IP地址 — 200.200.200.200
- 新的BQASA外部IP地址 — 209.165.201.2

注意：此处仅修改对等体信息。由于内部子网没有其他更改，因此加密访问列表保持不变。

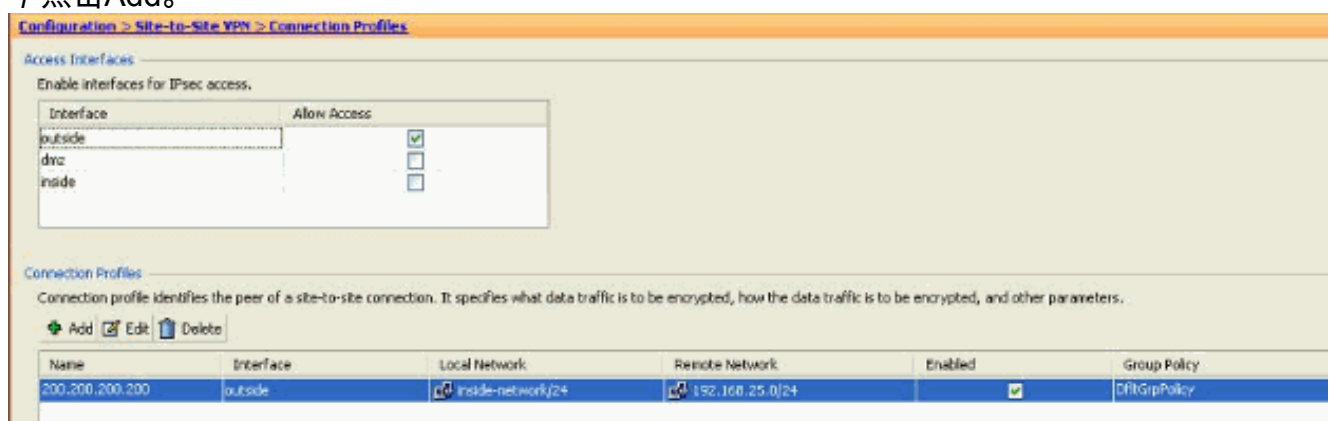
ASDM 配置

本节提供有关使用ASDM更改HQASA上VPN对等体信息的可能方法的信息。

创建新连接配置文件

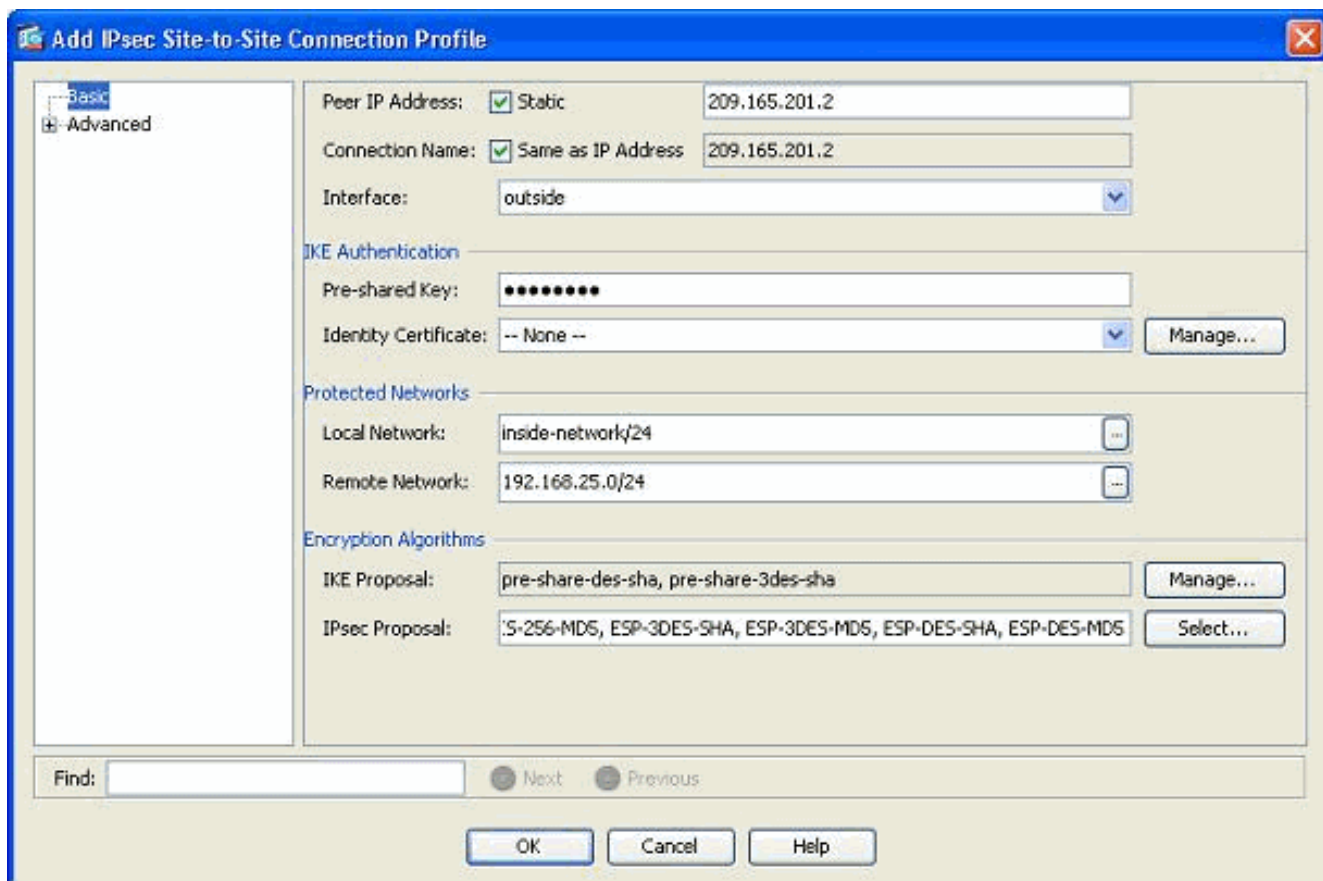
这可以是更简单的方法，因为它不会干扰现有VPN配置，并且可以使用新的VPN对等体相关信息创建新连接配置文件。

1. 转到 *Configuration > Site-to-Site VPN > Connection Profiles*，然后在Connection Profiles区域下点击Add。

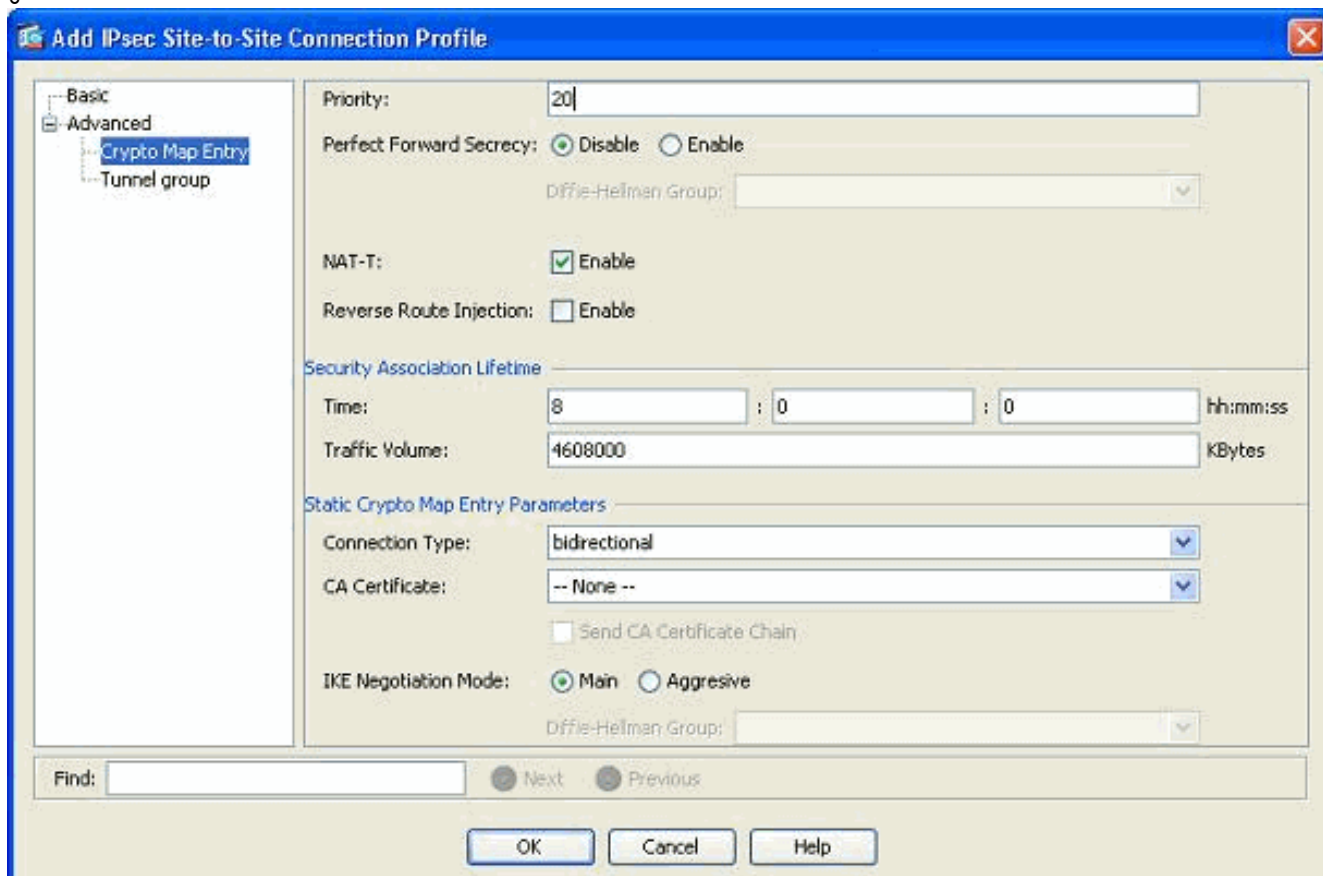


将打开“添加IPSec站点到站点连接配置文件”窗口。

2. 在“基本”选项卡下，提供对等IP地址、预共享密钥和受保护网络的详细信息。使用与现有VPN相同的所有参数，但对等体信息除外。Click OK.



3. 在“高级”菜单下，单击“加密映射条目”。请参阅“优先级”选项卡。此优先级等于其等效CLI配置中的序列号。如果分配的数字小于现有加密映射条目，则首先执行此新配置文件。优先级数值越高，值越小。这用于更改将执行特定加密映射的顺序。单击OK完成新连接配置文件的创建。



这会创建新隧道组以及关联的加密映射。在使用此新连接配置文件之前，请确保可以使用新IP地址到达BQASA。

编辑现有VPN配置

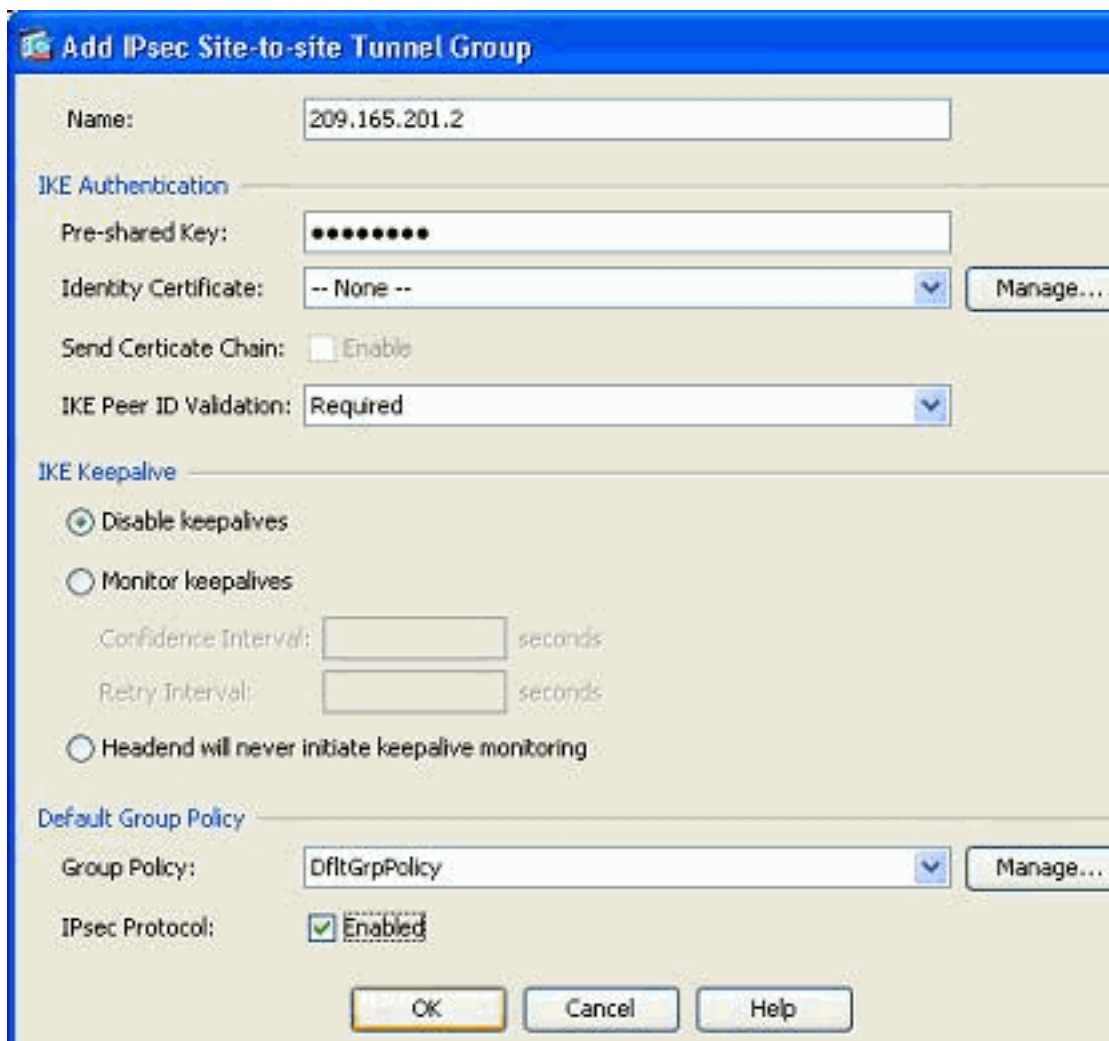
添加新对等体的另一种方法是修改现有配置。无法为新对等体信息编辑现有连接配置文件，因为它已绑定到特定对等体。要编辑现有配置，需要执行以下步骤：

1. 创建新隧道组
2. 编辑现有加密映射

创建新隧道组

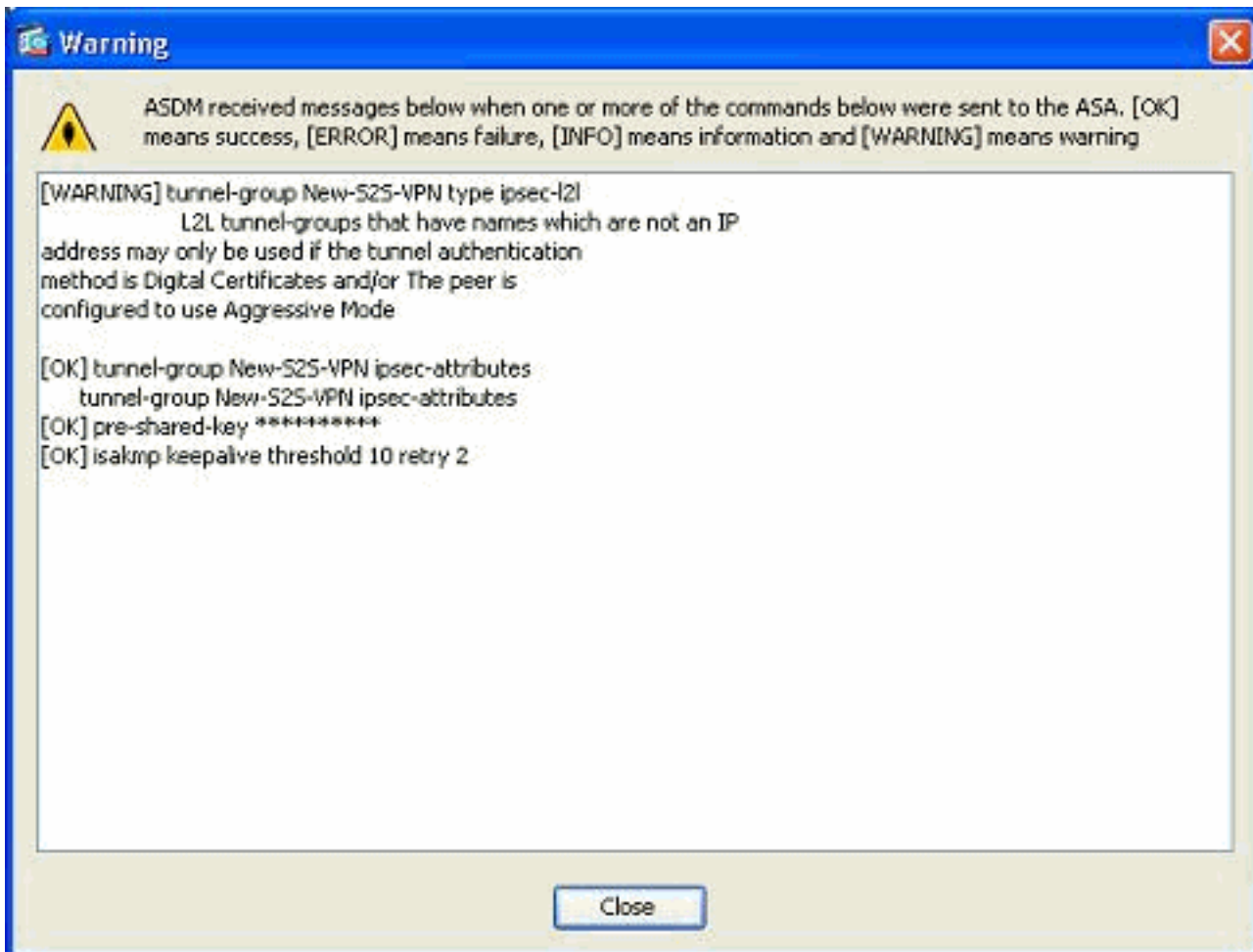
转到 *Configuration > Site-to-Site VPN > Advanced > Tunnel groups*，然后单击 *Add* 以创建包含新VPN对等体信息的新隧道组。指定“名称”和“预共享密钥”字段，然后单击 *OK*。

注意：确保预共享密钥与VPN的另一端匹配。



The screenshot shows the 'Add IPsec Site-to-site Tunnel Group' dialog box. The 'Name' field contains '209.165.201.2'. Under 'IKE Authentication', the 'Pre-shared Key' is masked with dots, 'Identity Certificate' is set to '-- None --', 'Send Certificate Chain' is disabled, and 'IKE Peer ID Validation' is set to 'Required'. Under 'IKE Keepalive', 'Disable keepalives' is selected. Under 'Default Group Policy', 'Group Policy' is set to 'DfltGrpPolicy' and 'IPsec Protocol' is checked and set to 'Enabled'. Buttons for 'OK', 'Cancel', and 'Help' are at the bottom.

注意：在“名称”字段中，当身份验证模式为预共享密钥时，应仅输入远程对等体的IP地址。只有身份验证方法通过证书时，才能使用任何名称。在名称字段中添加名称且预共享身份验证方法时，会出现此错误：

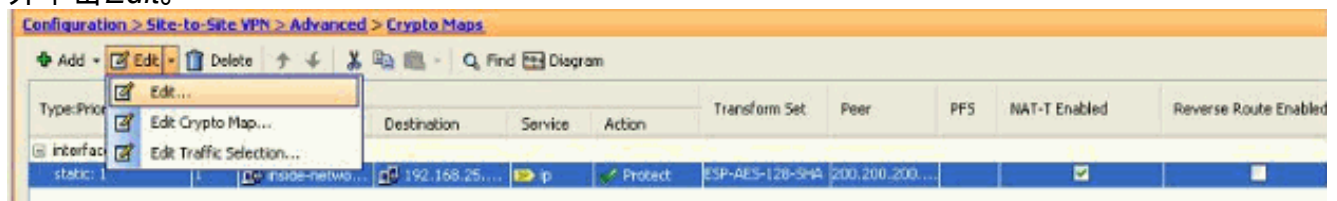


编辑现有加密映射

可以编辑现有加密映射以关联新的对等体信息。

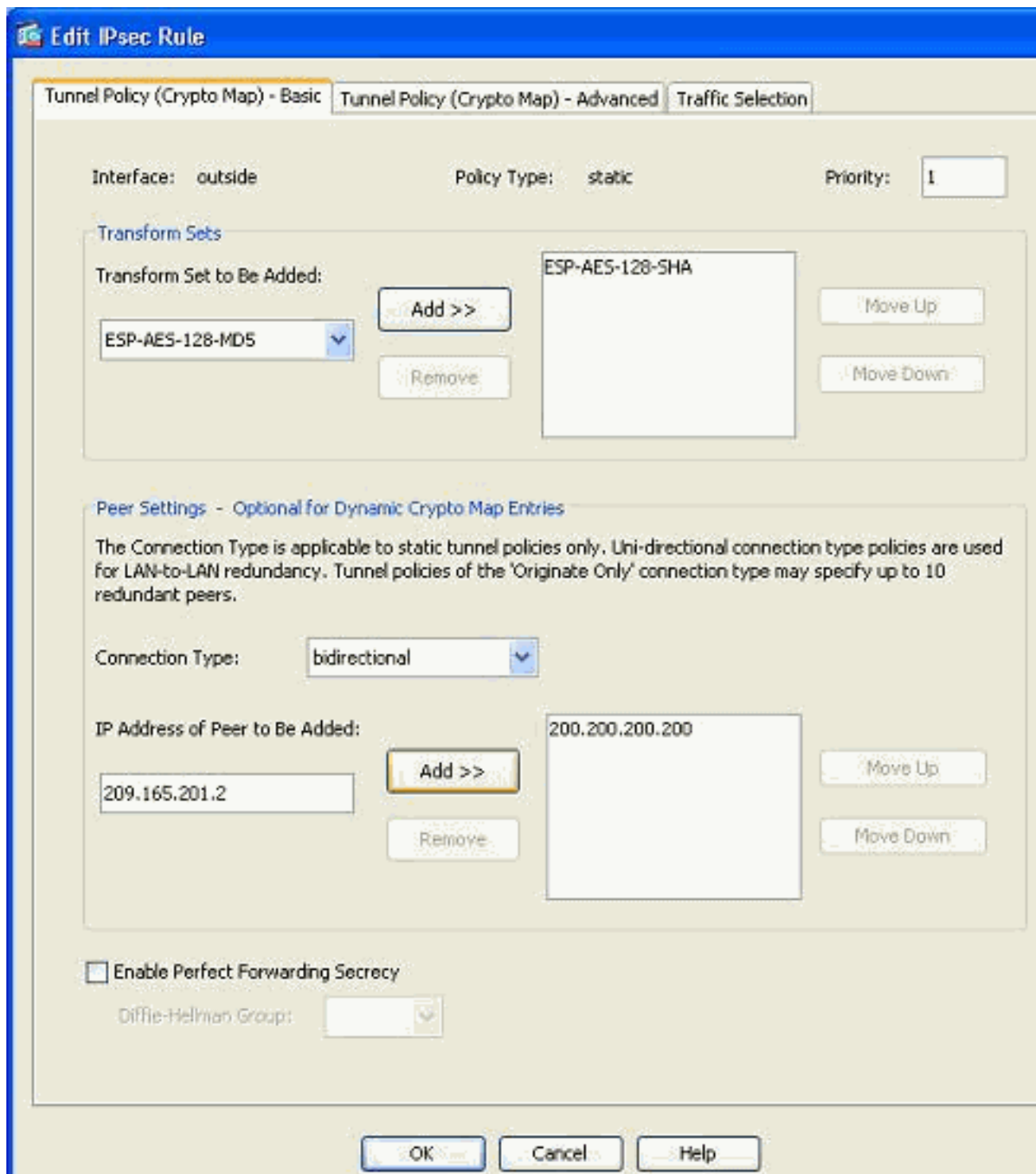
请完成以下步骤：

1. 转到 *Configuration > Site-to-Site VPN > Advanced > Crypto Maps*，然后选择所需的加密映射并单击 *Edit*。

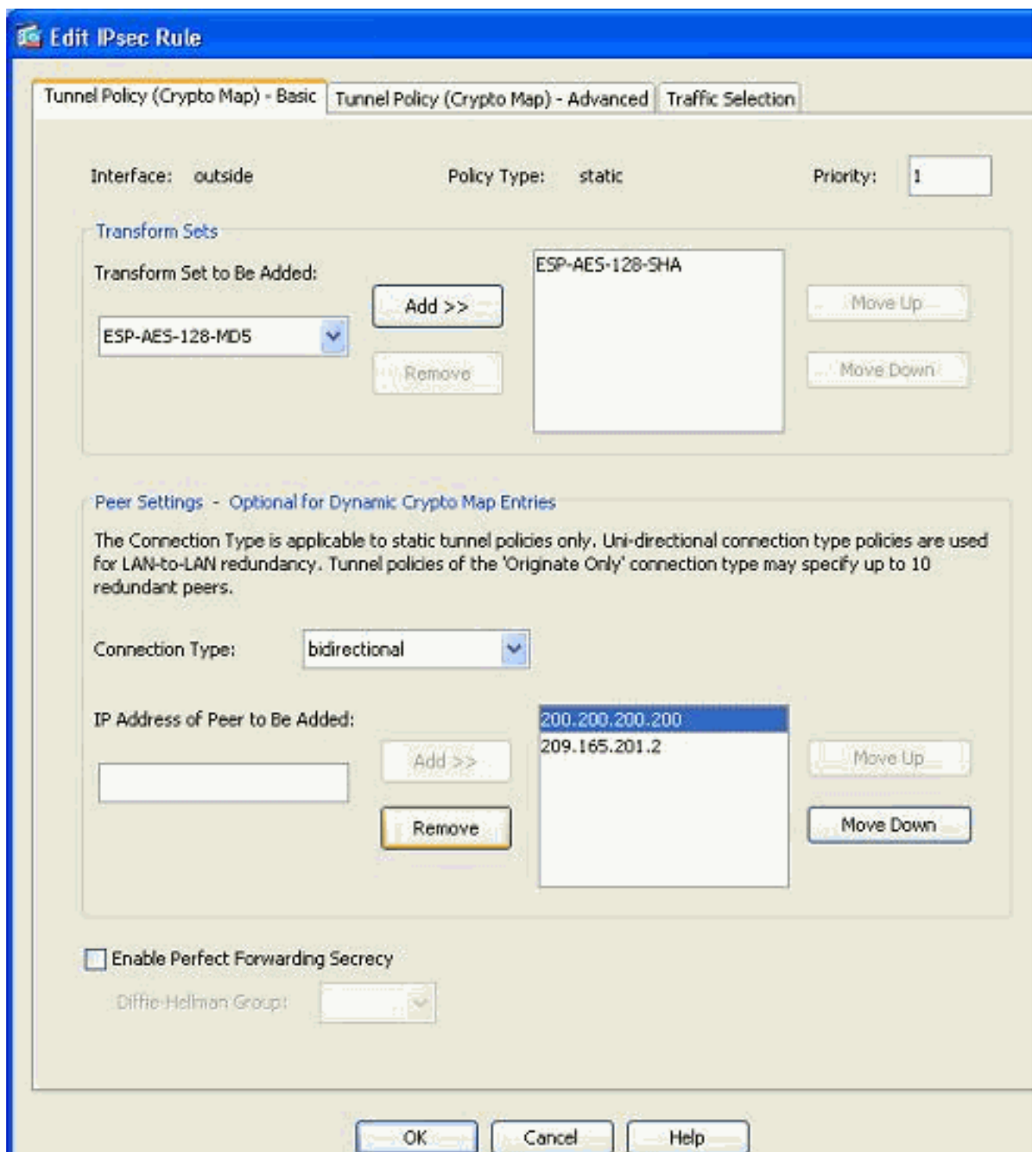


系统将显示 *Edit IPsec Rule* 窗口。

2. 在 Tunnel Policy (Basic) 选项卡的 Peer Settings (对等体设置) 区域中，在 Peer of Peer to Added (要添加的对等体的 IP 地址) 字段中指定新对等体。然后单击 *添加*。

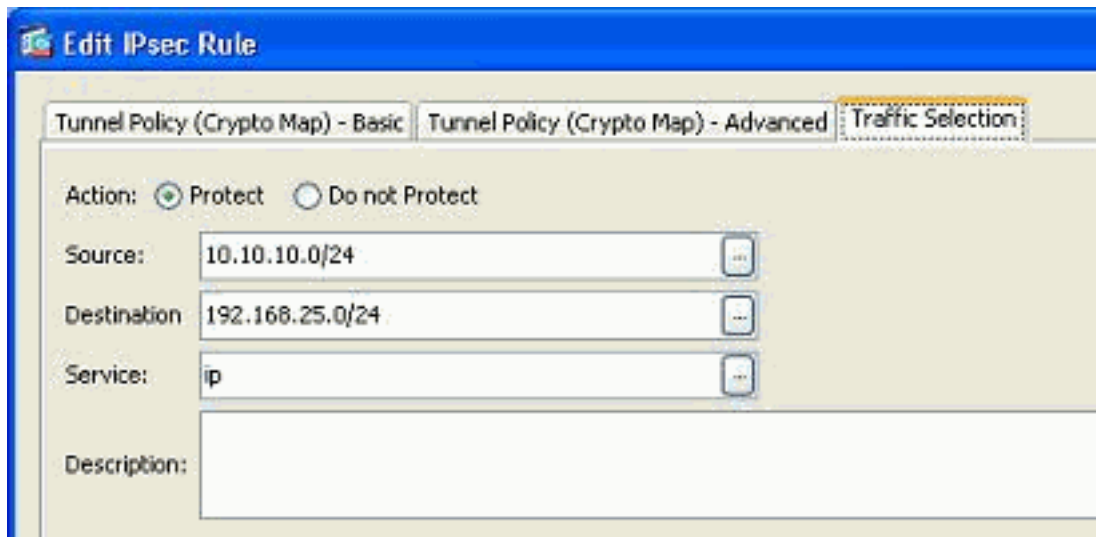


3. 选择现有对等IP地址，然后单击删除仅保留新的对等信息。Click **OK**.

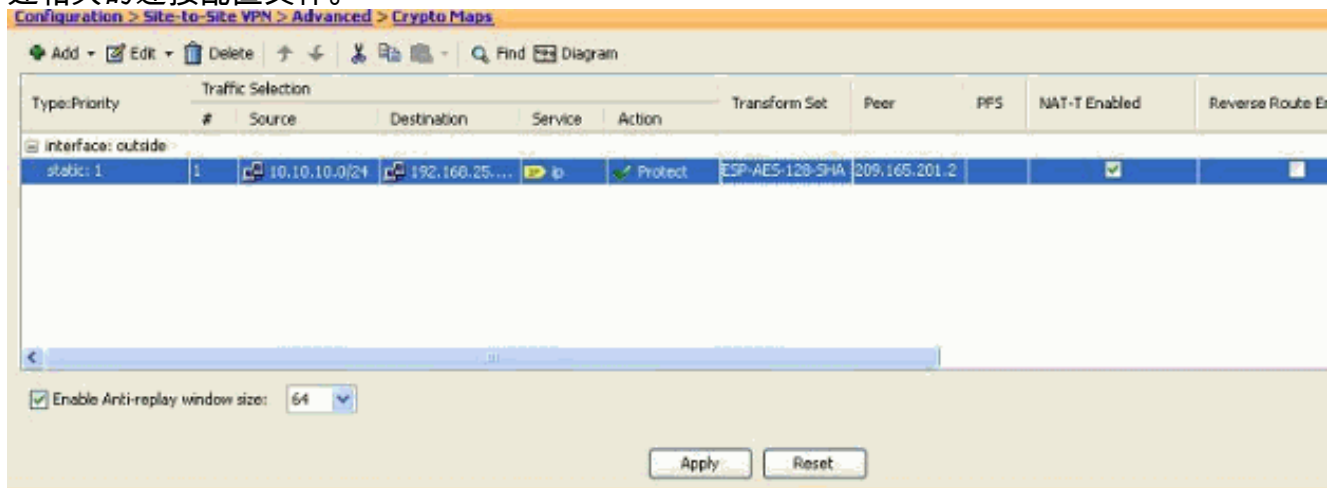


注意：修改当前加密映射中的对等体信息后，与此加密映射关联的连接配置文件会立即在 ASDM窗口中删除。

4. 加密网络的详细信息保持不变。如果需要修改这些，请转至“流量选择”选项卡。



5. 转到 *Configuration > Site-to-Site VPN > Advanced > Crypto Maps* 窗格以查看修改的加密映射。但是，在单击“应用”之前，这些更改不会发生。单击 *Apply* 后，转到 *Configuration > Site-to-Site VPN > Advanced > Tunnel groups* 菜单，以验证是否存在关联的隧道组。如果是，则将创建相关的连接配置文件。



验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

- 使用此命令可查看特定于单个对等体的安全关联参数：[show crypto ipsec sa peer <peer IP address>](#)

故障排除

使用本部分可排除配置故障。

[IKE Initiator unable to find policy:Intrf test_ext , 源 : 172.16.1.103 , 目的 : 10.1.4.251](#)

尝试将VPN对等体从VPN集中器更改为ASA时，日志消息中会显示此错误。

解决方案：

这可能是迁移期间执行的配置步骤不正确的结果。在添加新对等体之前，请确保删除接口的加密绑定。另外，请确保您使用隧道组中对等体的IP地址，而不是名称。

相关信息

- [采用ASA的站点到站点\(L2L\)VPN](#)
- [最常见的VPN问题](#)
- [ASA技术支持页](#)
- [技术支持和文档 - Cisco Systems](#)