ASA 8.x/ASDM 6.x ：使用ASDM，添加在一现有站点到站点VPN的新的VPN对等项信息

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[Backround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:Intf test_ext， Src ：172.16.1.103， Dst ：10.1.4.251](#)
[相关信息](#)

简介

本文提供关于与构形有关更改的信息做使用可适应安全设备管理器时(ASDM)，当一新的VPN对等项被添加到现有站点到站点VPN配置。这在这些情况下要求：

- 互联网服务提供商更改，并且使用新的一套公有IP范围。
- 网络的完整再设计在站点的。
- 作为VPN网关使用的设备在站点被移植到与一不同的公网IP地址的一新设备。

本文假设，站点到站点VPN适当地已经配置并且良好工作。本文在L2L VPN配置里提供步骤跟随为了更改一VPN对等项信息。

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：

- Cisco Adapative安全工具5500系列与软件版本8.2及以后
- 有软件版本的6.3 Cisco Adapative Security Device Manager及以后

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Backround信息

站点到站点VPN优良工作在HQASA和BQASA之间。假设， BQASA有完整网络再设计，并且IP模式被修改了在ISP级别，但是所有内部子网详细信息依然是同样。

此配置示例使用这些IP地址：

- 存在BQASA外部IP地址- 200.200.200.200
- 新的BQASA外部IP地址- 209.165.201.2

注意： 这里，将修改仅对等体信息。由于没有在内部子网上的其他变化， crypto访问列表保持同样。

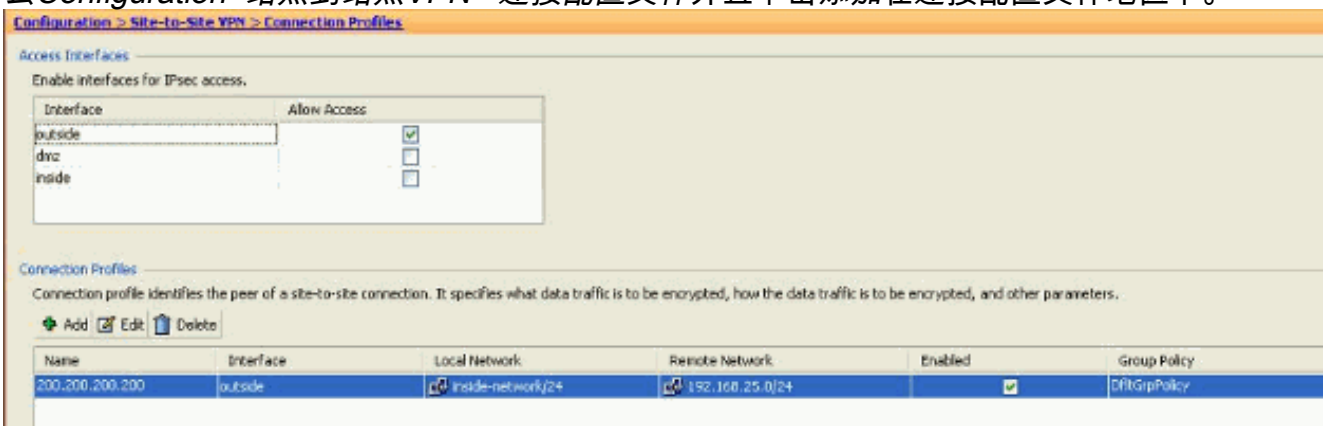
ASDM 配置

使用ASDM，此部分提供关于可能的使用的方法的信息更改关于HQASA的VPN对等项信息。

创建新连接配置文件

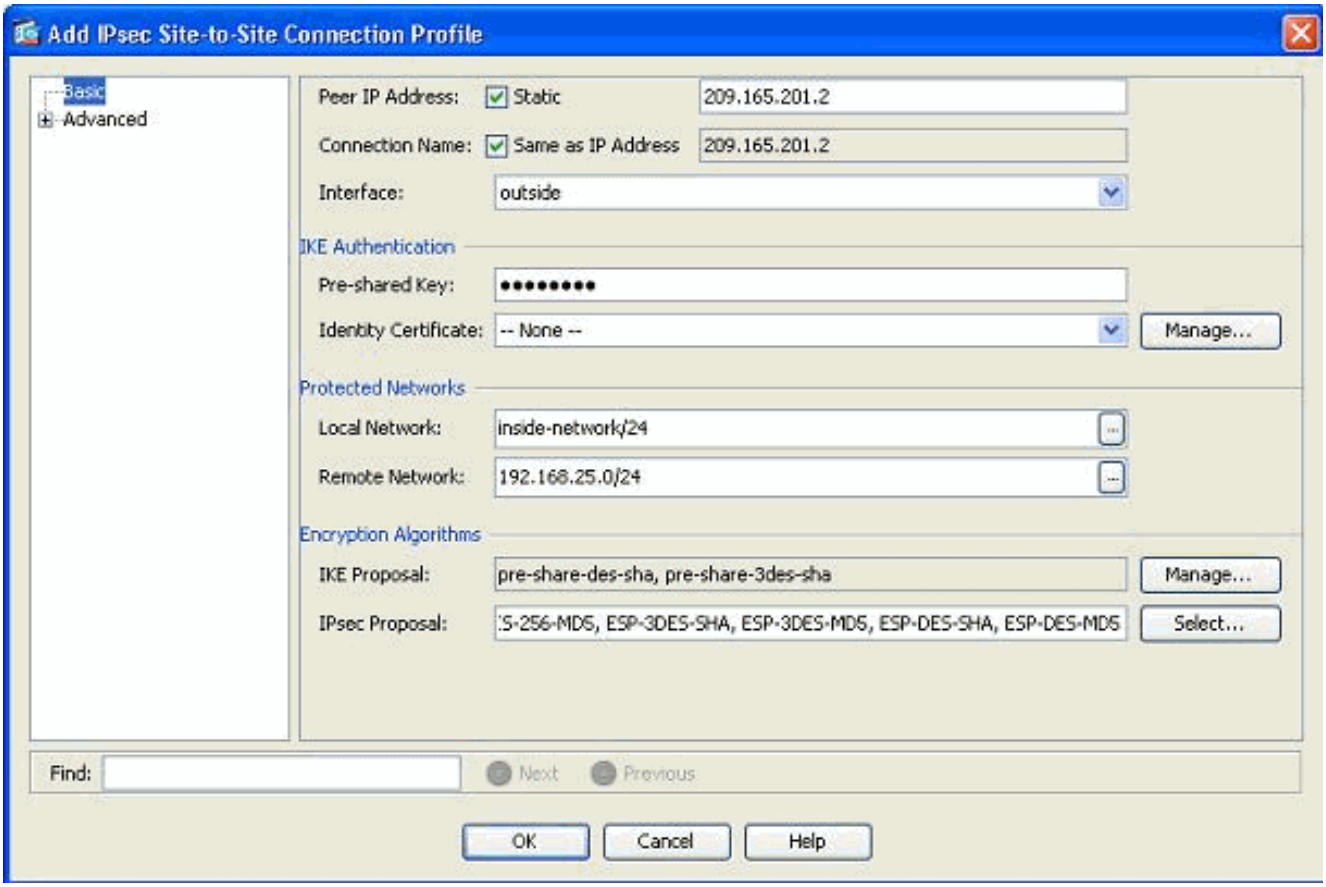
因为不干扰现有VPN配置，并且能创建与新的VPN对等项相关信息的一新连接配置文件这可以是更加容易的方法。

1. 去*Configuration>站点到站点VPN >连接配置文件*并且单击*添加*在连接配置文件地区下。

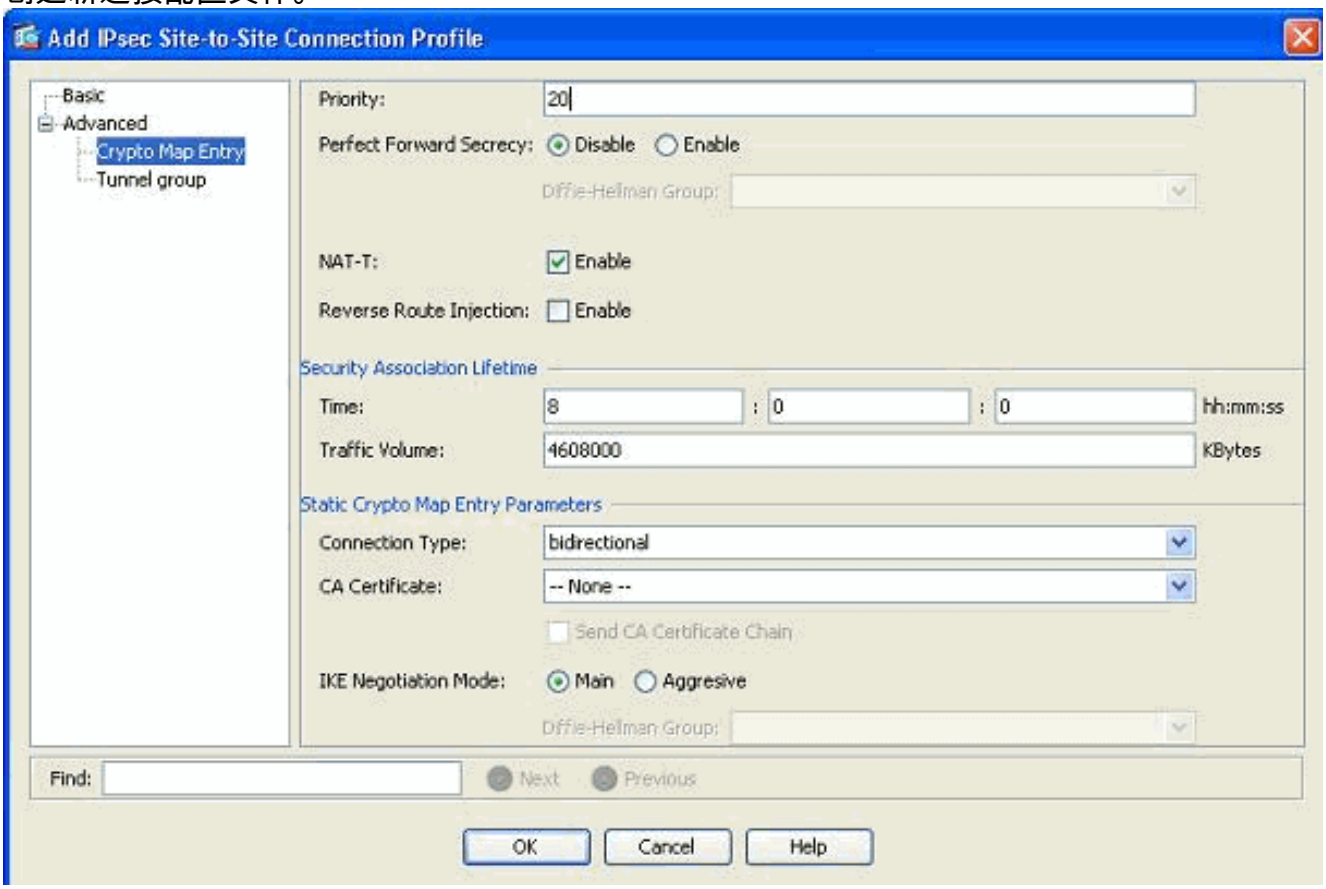


*添加IPSec站点到站点连接Profile窗口*打开。

2. 在基本选项下，为*对端IP地址*、*预先共享密钥*和*受保护的网络*请提供细节。请使用完会一样的参数作为现有VPN，除了对等体信息。单击**Ok**。



3. 在Advanced菜单下，请点击*加密映射项。参考优先级*选项卡。此优先级与序号是相等的在其等同CLI配置方面。当一点编号比现有加密映射项分配时，此新配置文件首先被执行。越高priority number，较少值。这用于更改一个特定加密映射将被执行顺序的命令。点击OK键完成创建新连接配置文件。



这与一个相关的加密映射一起自动地创建一新的隧道群。在您使用此新连接配置文件前，请确保您能到达BQASA用新的IP地址。

编辑现有VPN配置

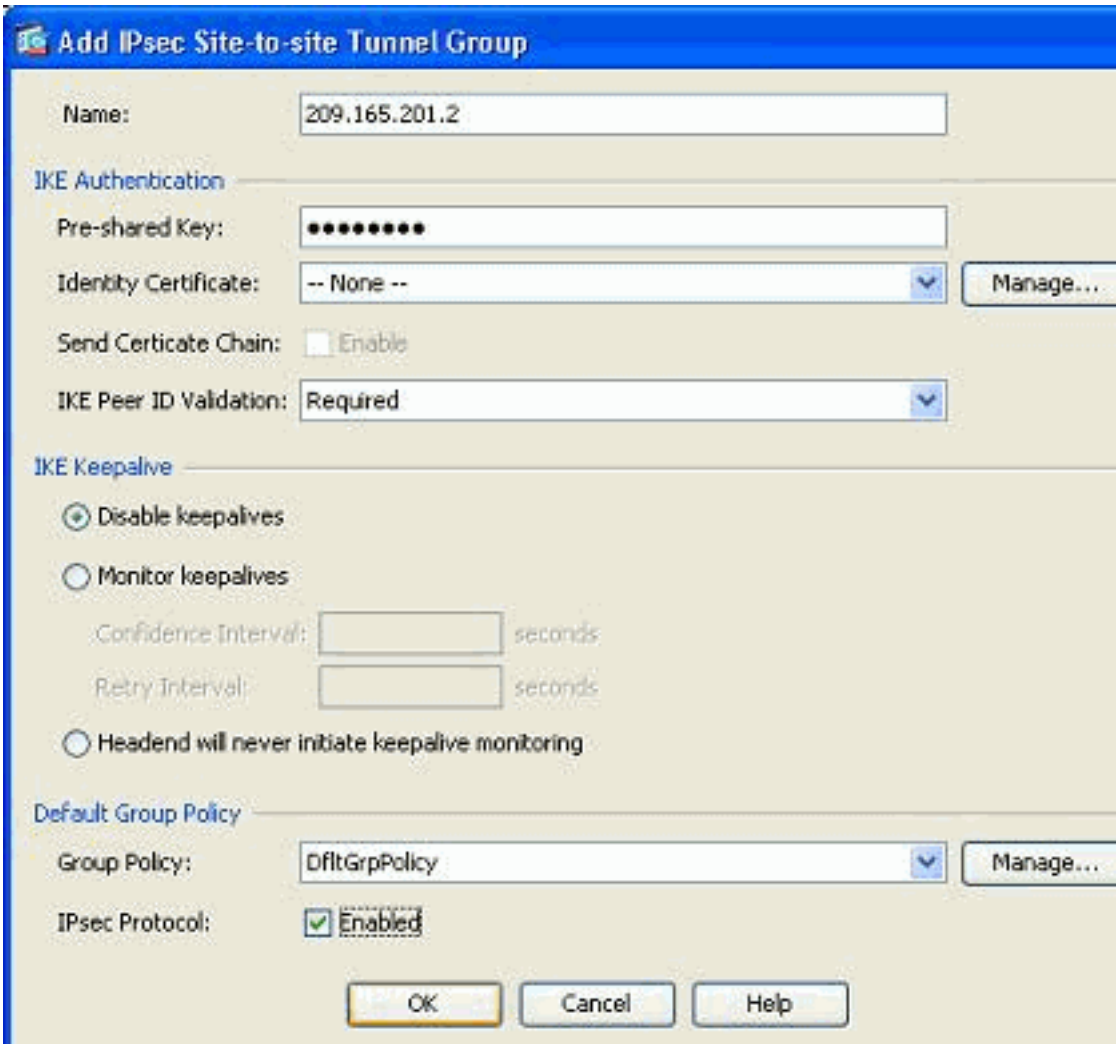
添加一新的对等体另一个方式将修改现有配置。因为一定给一特定对等体，现有连接配置文件不可能为新的对等体信息编辑。为了编辑现有配置，您需要执行这些步骤：

1. 创建新通道组
2. 编辑现有加密映射

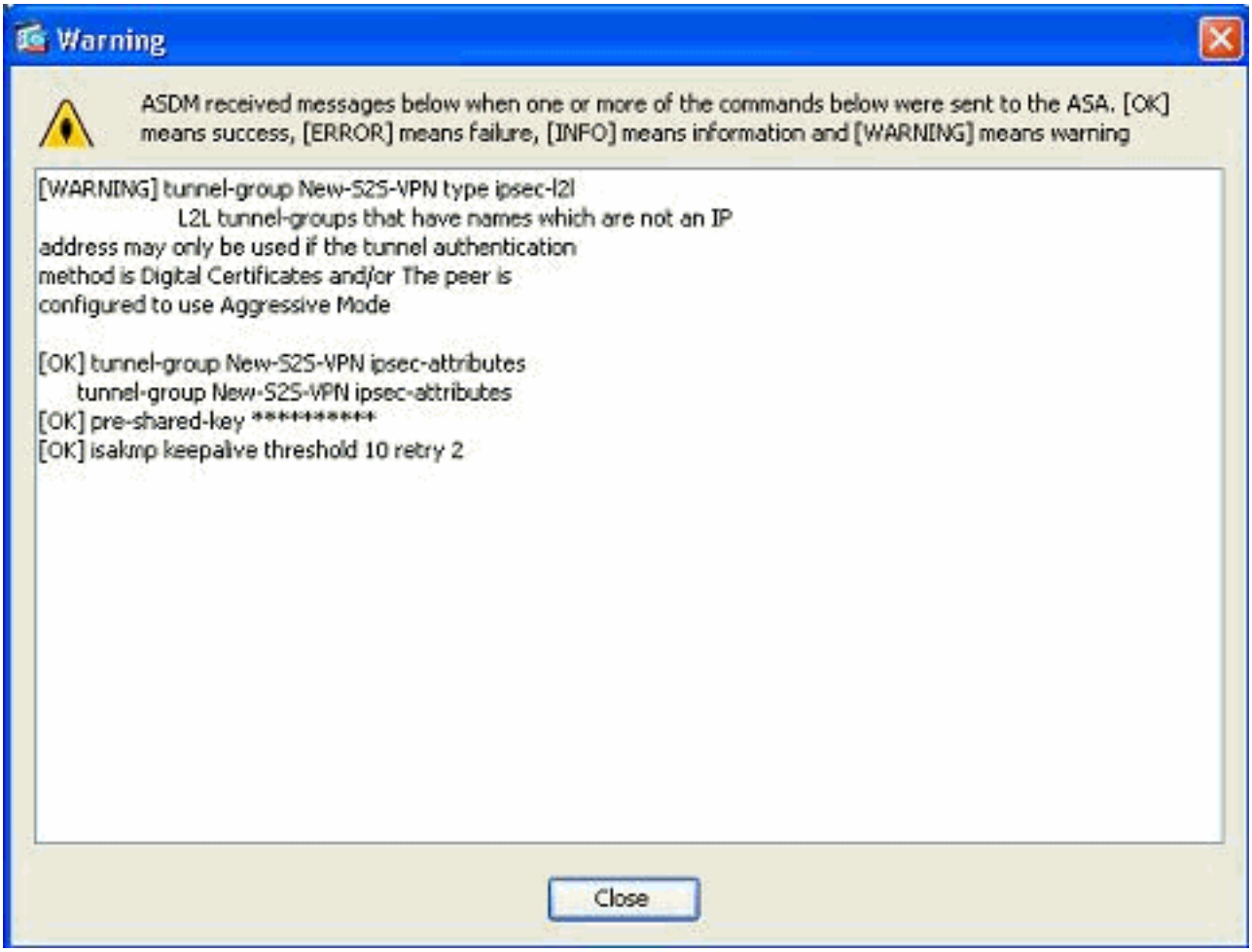
创建新通道组

去*Configuration>站点到站点VPN >Advanced >隧道组*并且单击*添加*创建包含新的VPN对等项信息的一新的隧道群。指定*名称*和*预先共享密钥*关键字域，然后点击OK键。

注意： 确保预先共享密钥匹配VPN的另一端。



注意： 在Name字段，远端对等体的仅IP地址，当认证模式是预先共享密钥时，应该输入。所有名称，只有当认证方法是通过证书时，可以使用。此错误出现，当名称在Name字段时被添加，并且认证方法预共享：

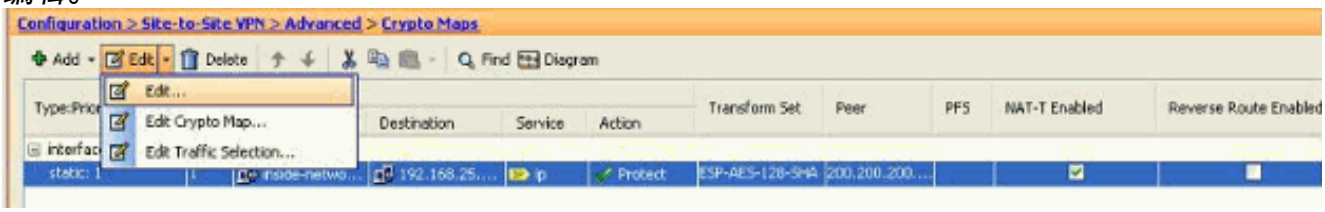


编辑现有加密映射

现有加密映射可以编辑为了关联新的对等体信息。

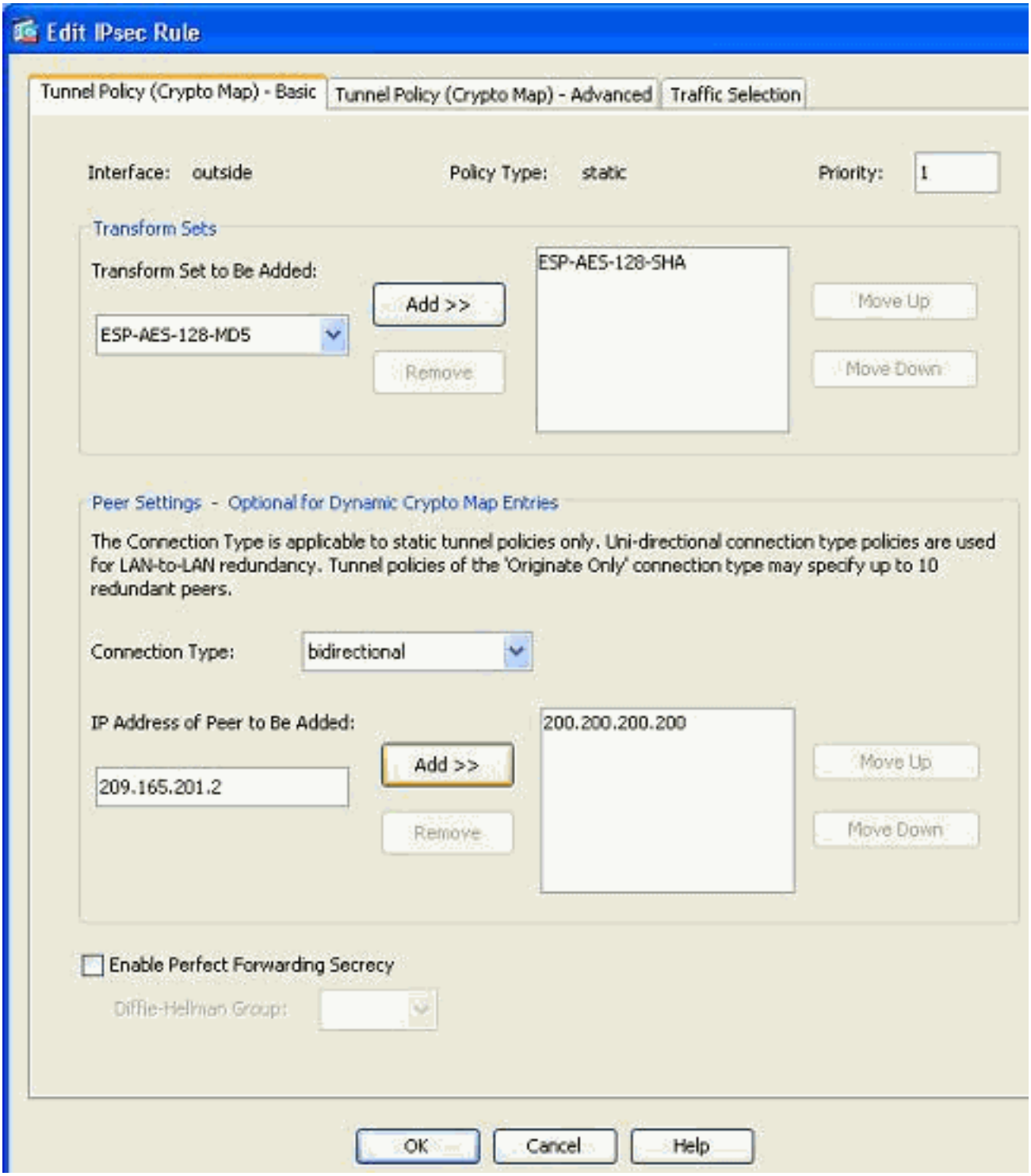
完成这些步骤：

1. 去*Configuration>站点到站点VPN >Advanced >加密映射*，然后选择需要的加密映射并且单击*编辑*。

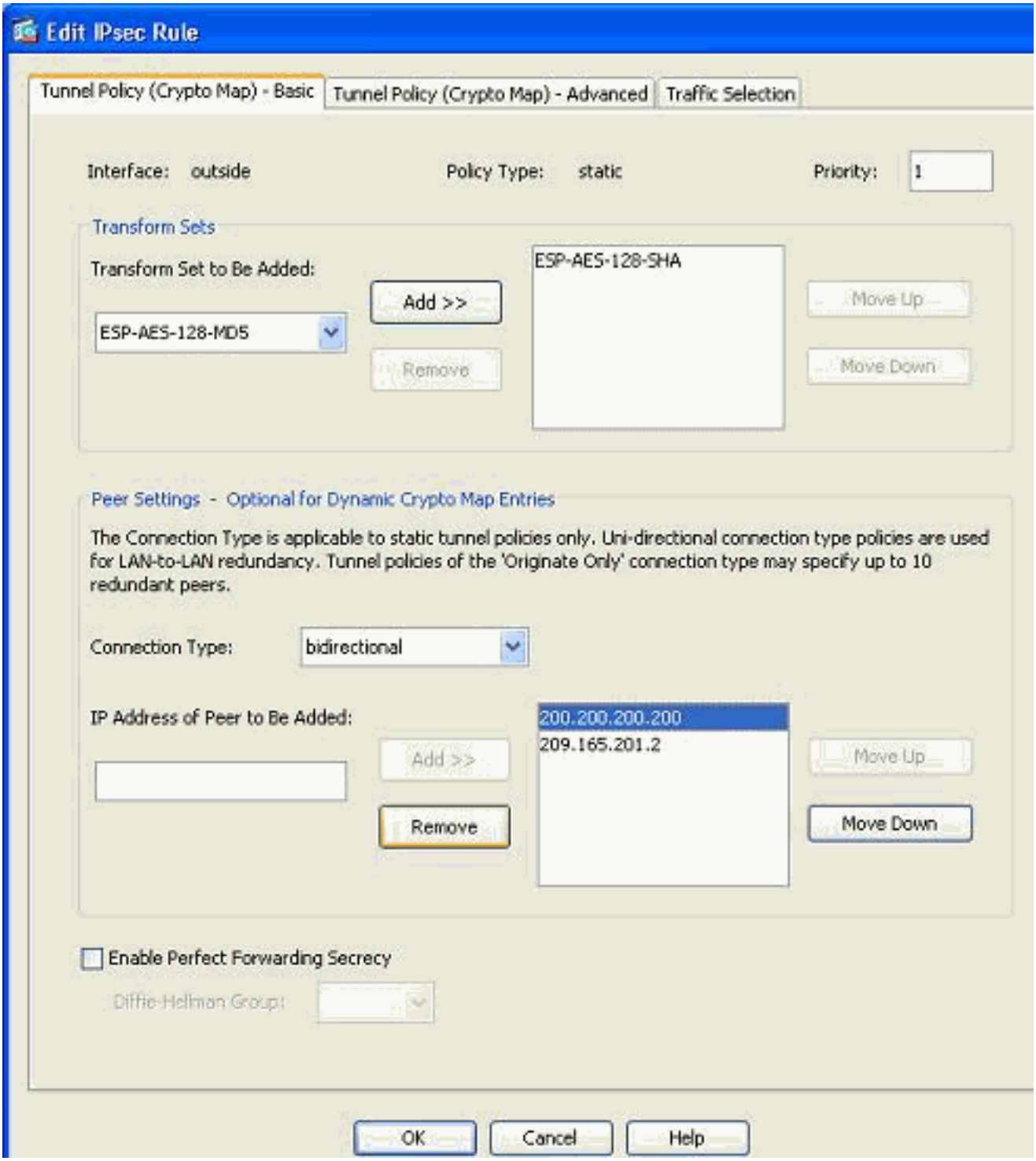


*编辑IPSec规则*窗口出现。

2. 在通道策略(基本)选项卡下，在对等体设置地区，请指定对等体的IP地址的新的对等体是被添加的字段。然后，请单击*添加*。

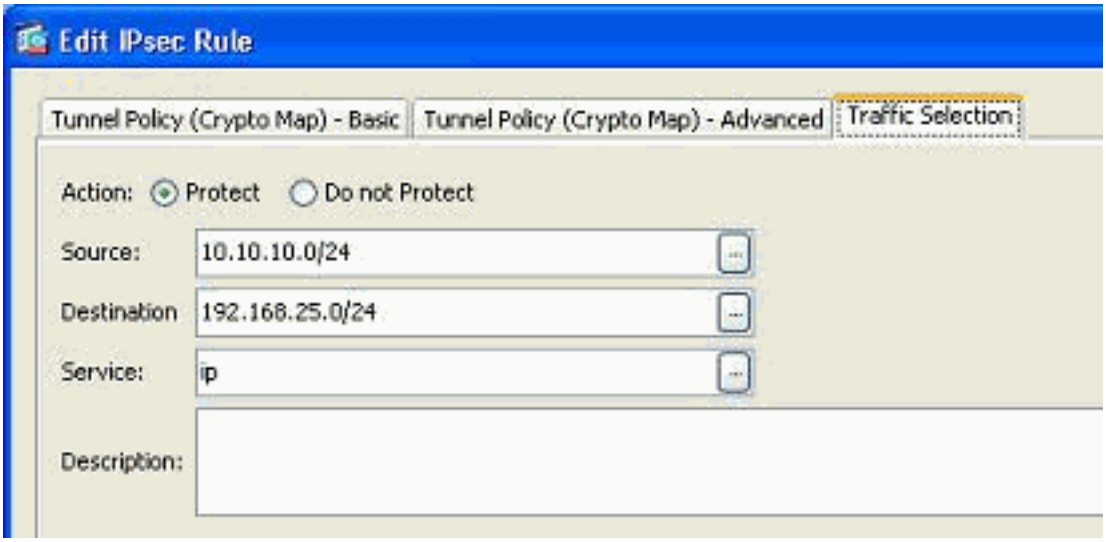


3. 选择现有对端IP地址并且点击*删除*保留仅新的对等体信息。单击**Ok**。

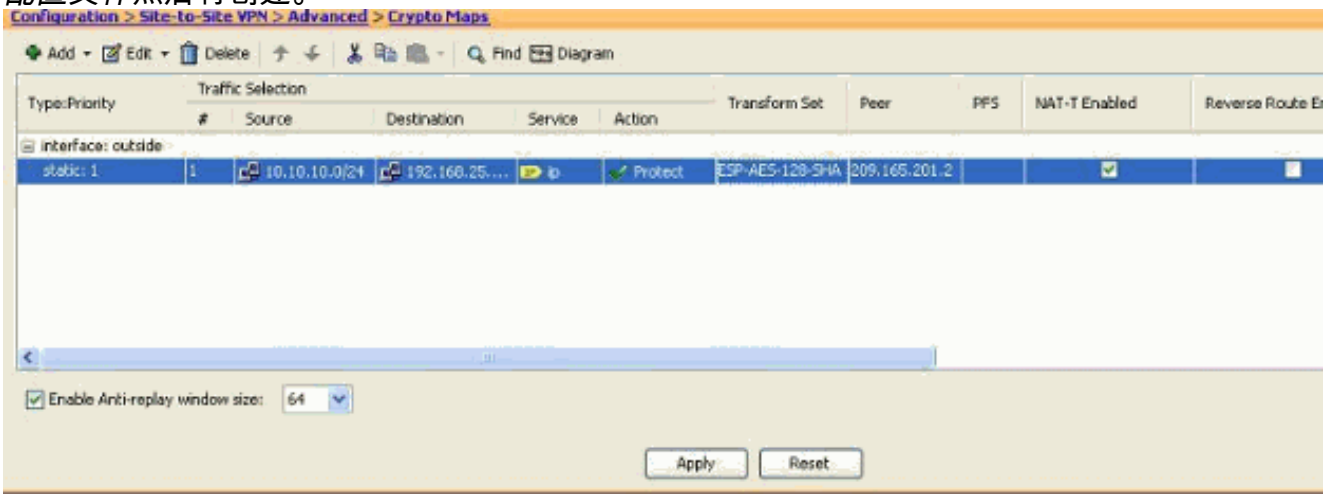


注意： 在您修改在当前加密映射后的对等体信息，连接配置文件关联与此加密映射立刻在ASDM窗口删除。

4. 已加密网络的详细信息依然是同样。如果需要修改这些，请去*流量选择*选项卡。



5. 去*Configuration>站点到站点VPN >Advanced >加密映射*窗格为了查看已修改加密映射。然而，这些更改不发生，直到您单击*应用*。在您单击后请*适用*，去于*Configuration>站点到站点VPN >Advanced >隧道组*菜单为了验证，如果一相关的隧道群存在。如果是，一个相关的*连接配置文件*然后将创建。



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。

- 请使用此命令查看安全关联参数特定对单个对等体：show crypto ipsec sa对等体<Peer IP地址>

故障排除

使用本部分可排除配置故障。

IKE Initiator unable to find policy:Intf test_ext， Src ：172.16.1.103， Dst ：10.1.4.251

当尝试更改从VPN集中器的VPN对等项到ASA时，此错误在日志消息显示。

解决方案：

这可以是不正确的配置步骤结果在迁移时跟随的。保证crypto约束对接口删除，在您添加一新的对等体前。并且，请确保您在隧道群中使用了对等体的IP地址，但是不是名称。

相关信息

- 站点的(L2L)与ASA的VPN站点
- 最普通的VPN问题
- ASA技术支持页
- 技术支持和文档 - Cisco Systems