

# ASDM 6.4 : 有IKEv2配置示例的站点到站点VPN通道

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[在HQ-ASA的ASDM配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

## 简介

本文描述如何配置在两Cisco可适应安全工具(ASA)之间的一个站点到站点VPN通道使用Internet Key Exchange (IKE)版本2。使用可适应安全设备管理器(ASDM) GUI向导，它描述用于的步骤配置VPN通道。

## 先决条件

### 要求

确保思科ASA配置与[基本设置](#)。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本8.4的Cisco ASA 5500系列自适应安全设备及以后
- Cisco ASDM软件版本6.4及以后

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。

### 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 背景信息

IKEv2，是增强对包括这些好处的现有IKEv1协议：

- 在IKE对等体之间的少量消息交换
- 单向验证方法
- 对端死机检测(DPD)和NAT遍历的内置支持
- 使用验证的可扩展的认证协议(EAP)
- 使用防结渣的Cookie，排除简单DOS攻击风险

## 配置

本部分提供有关如何配置本文档所述功能的信息。

**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

本文档使用以下网络设置：



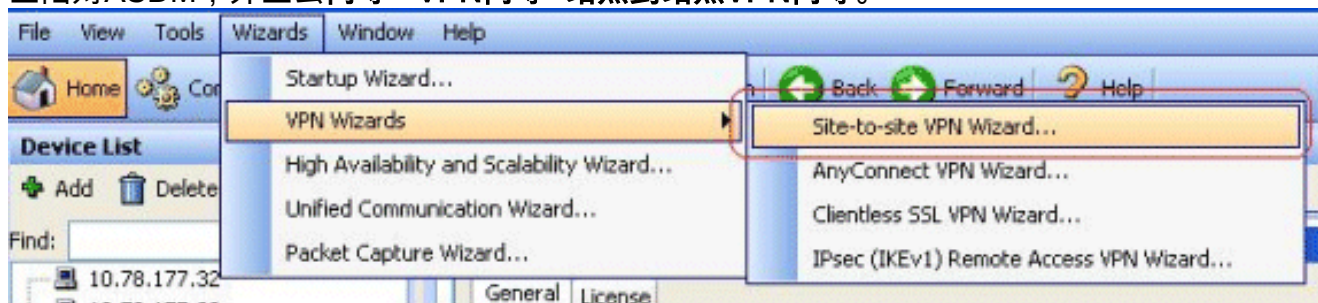
本文显示站点到站点VPN通道的配置在HQ-ASA的。同样能被跟随象在BQ-ASA的一镜像。

## 在HQ-ASA的ASDM配置

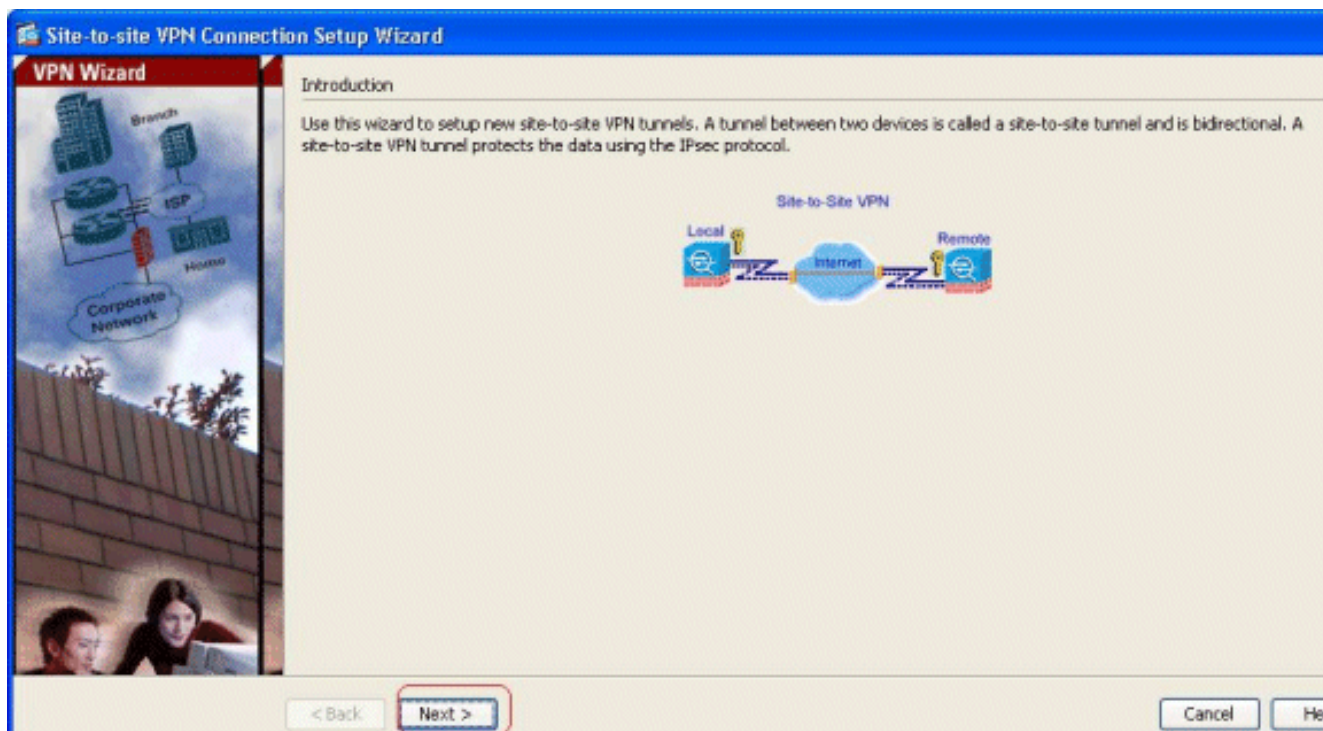
使用一个易用GUI向导，此VPN通道能配置。

完成这些步骤：

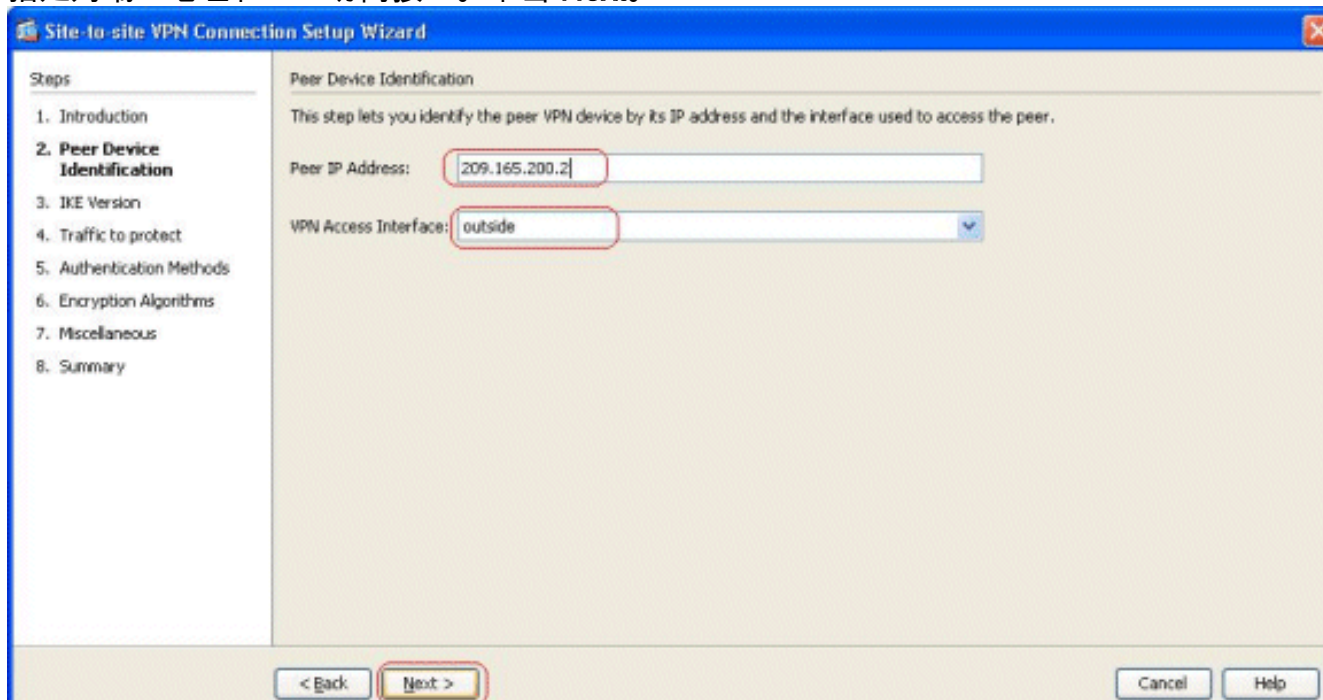
1. 登陆对ASDM，并且去向导>VPN向导>站点到站点VPN向导。



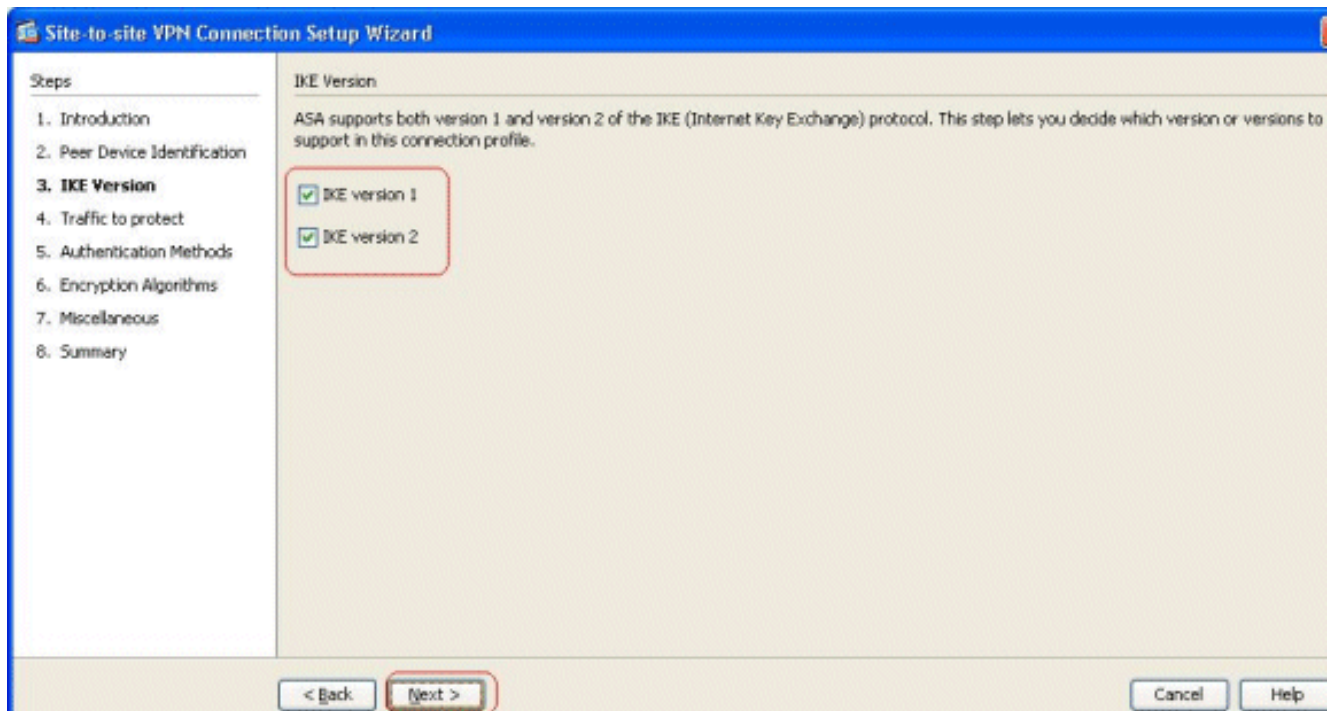
2. 站点到站点VPN连接设置窗口出现。单击 **Next**。



3. 指定对端IP地址和VPN访问接口。单击 **Next**。

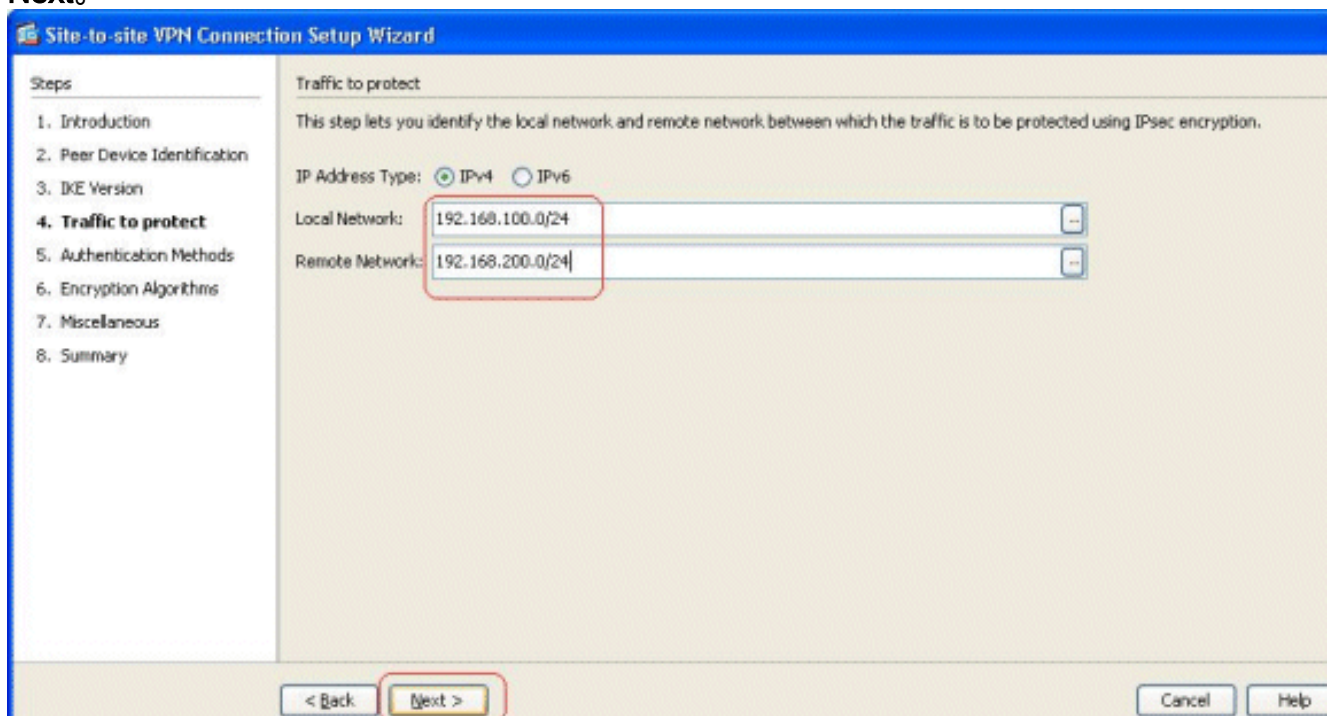


4. 选择两个IKE版本，并且其次单击。

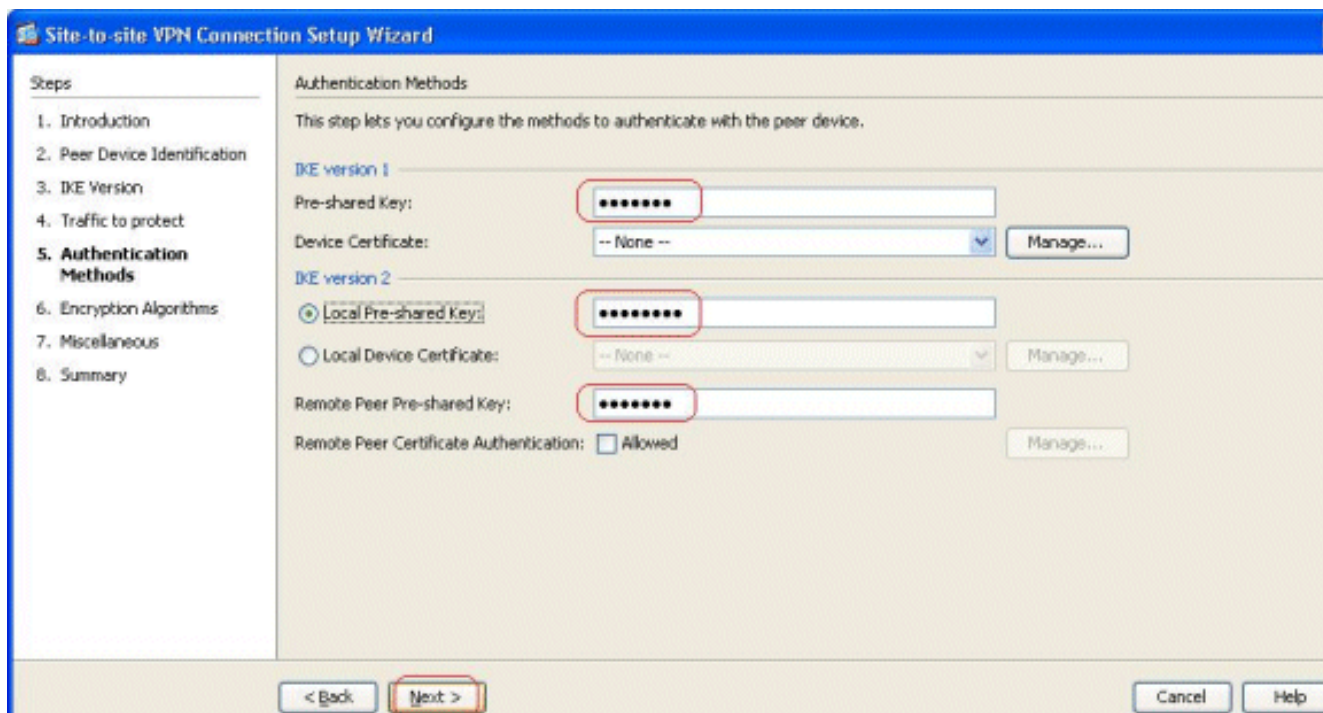


**注意：** IKE两个版本配置此处，因为发起者可能有一个备份从IKEv2到IKEv1，当IKEv2发生故障时。

5. 指定本地网络和远程网络，以便这些网络之间的流量通过VPN通道加密并且通过。单击**Next**。

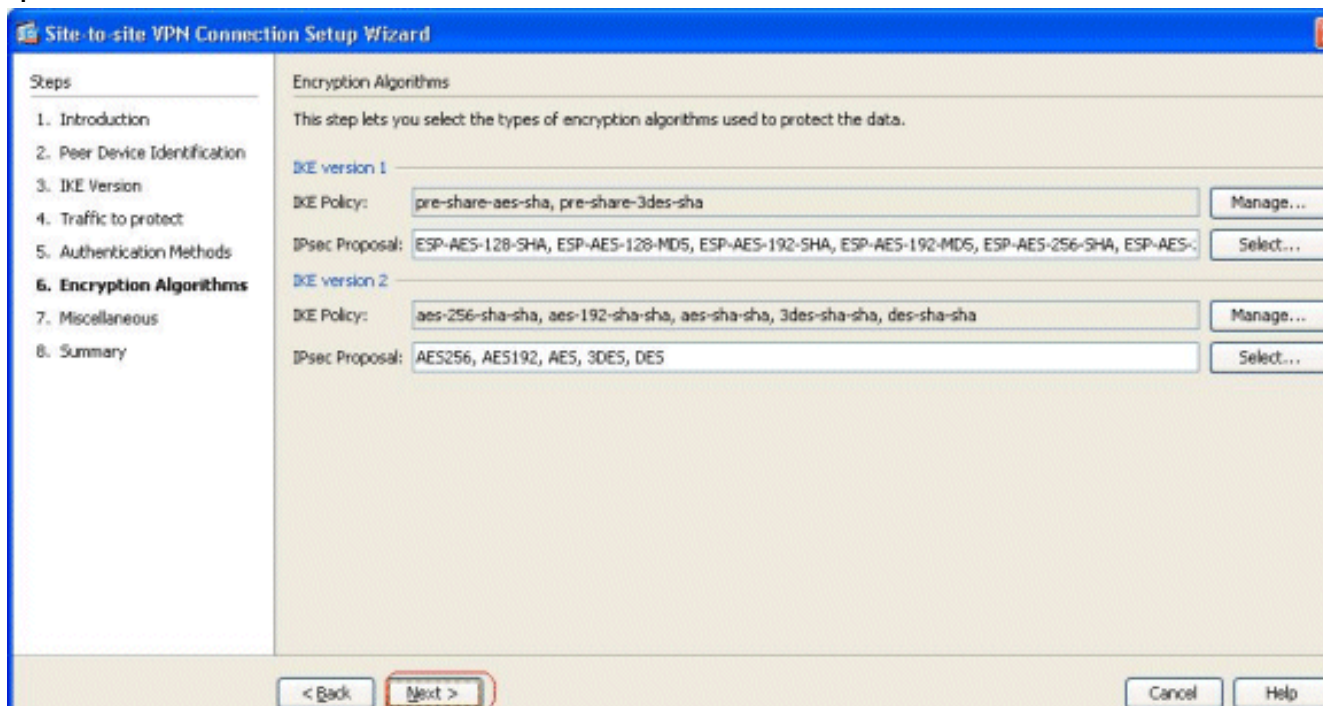


6. 指定IKE两个版本的预先共享密钥。

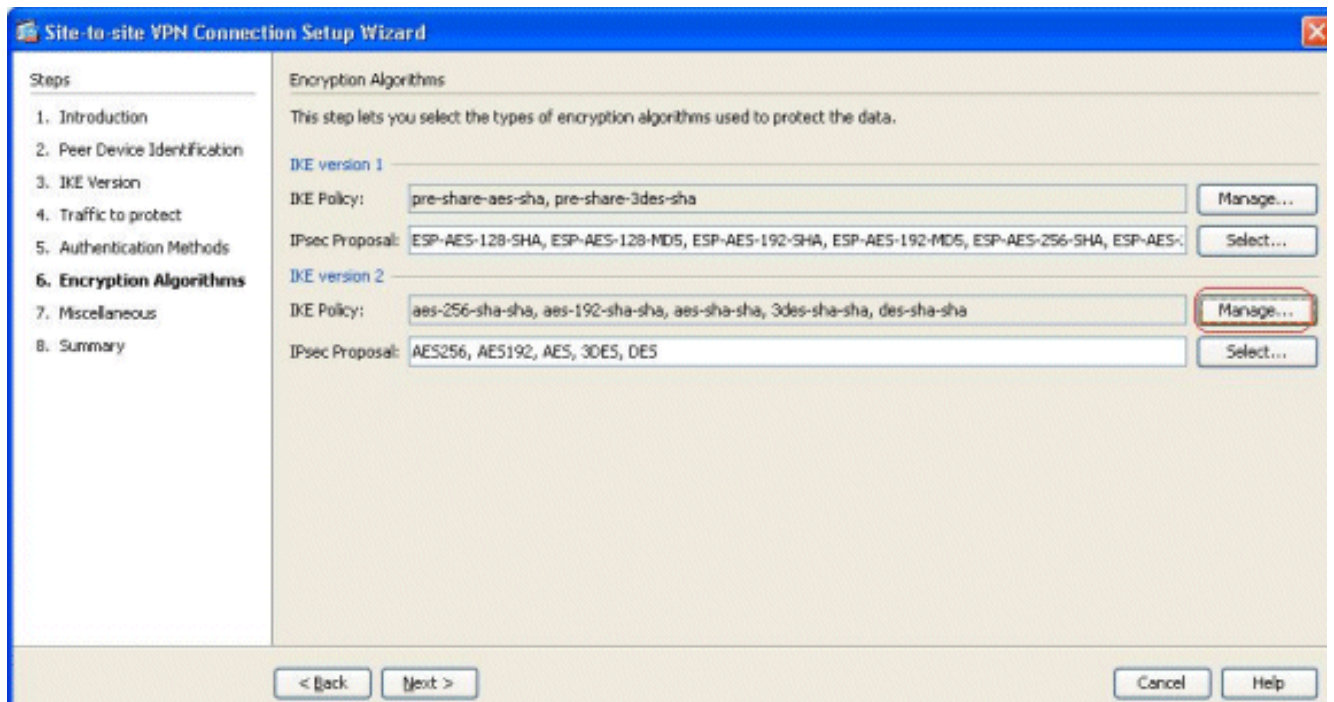


IKE版本1和2之间的主要区别位于根据他们允许的认证方法。IKEv1只允许验证的一种类型在两个VPN末端(即预先共享密钥或证书)。然而，IKEv2允许使用分开的本地和远程验证将配置的(即创建人的响应方的密钥验证，但是证书验证)不对称认证方法CLIs。进一步，您能有不同的预先共享密钥在两端。在HQ-ASA末端的本地预先共享密钥变为远程预先共享密钥在BQ-ASA末端。同样，在HQ-ASA末端的远程预先共享密钥变为本地预先共享密钥在BQ-ASA末端。

7. 指定两IKE版本1和2的加密算法。这里，默认值接受



8. 单击设法...为了修改IKE策略。



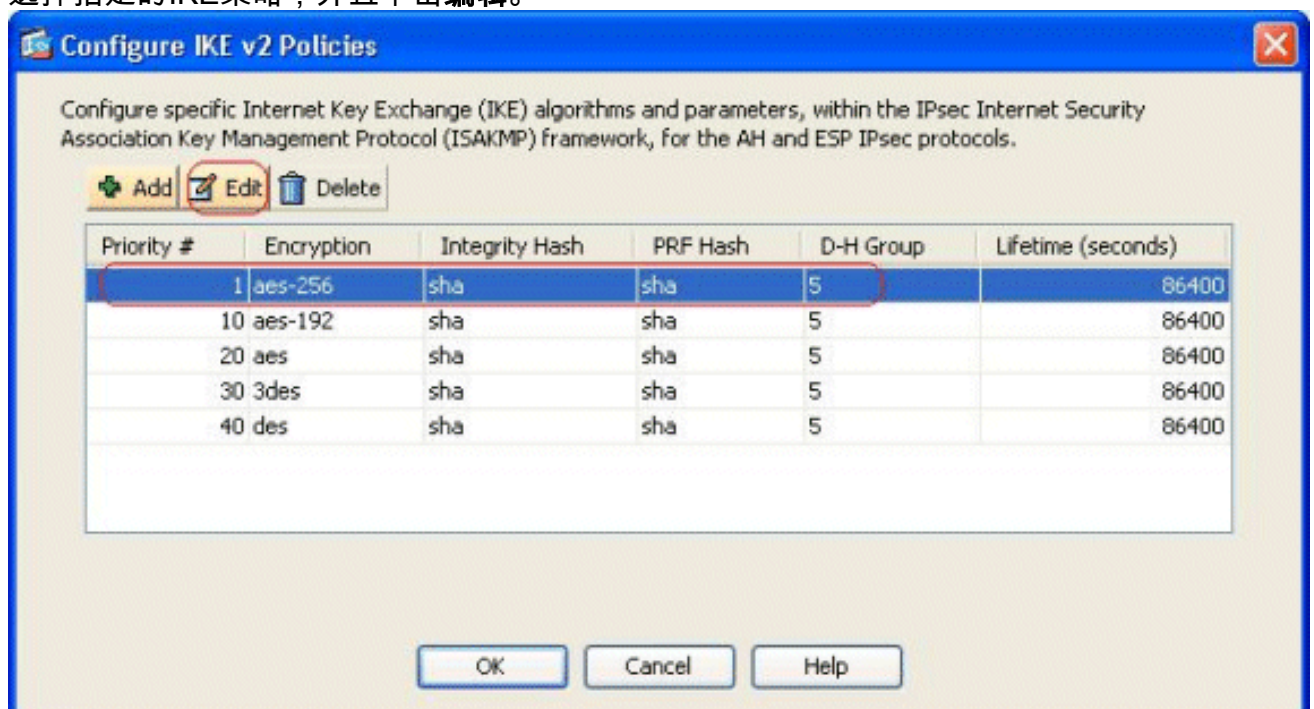
注意：在IKEv2的IKE策略是同义的对在IKEv1的ISAKMP策略。在IKEv2的IPsec建议是同义的对在IKEv1设置的转换。

9. 当您设法修改现有策略，此消息出现

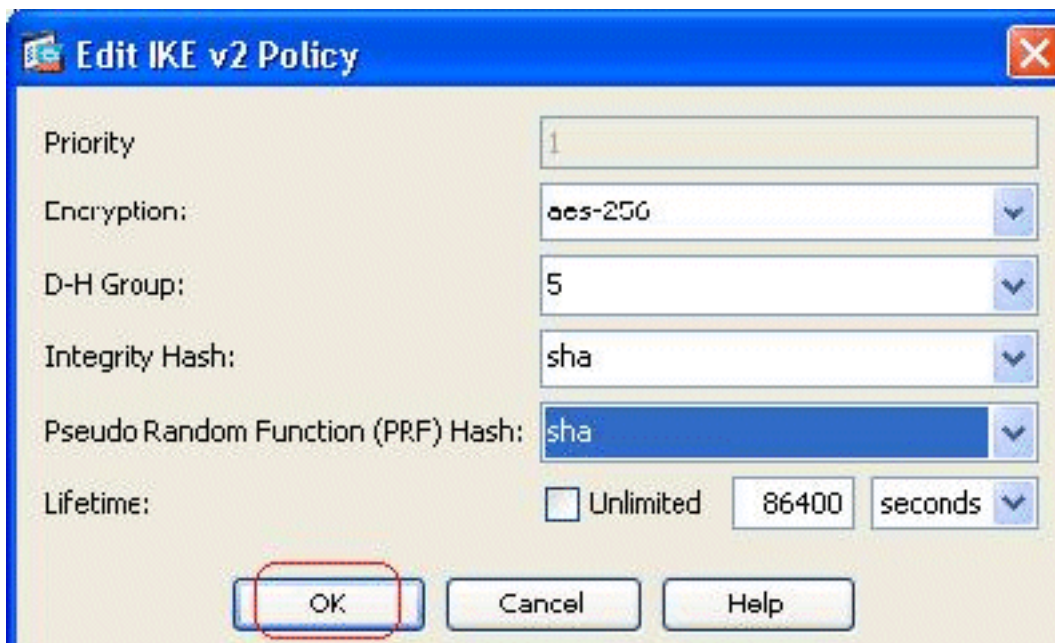


点击OK键为了继续

10. 选择指定的IKE策略，并且单击编辑。



11. 您能修改参数例如优先级、加密、D-H组、完整性哈希、PRF哈希和寿命值。完成后单击

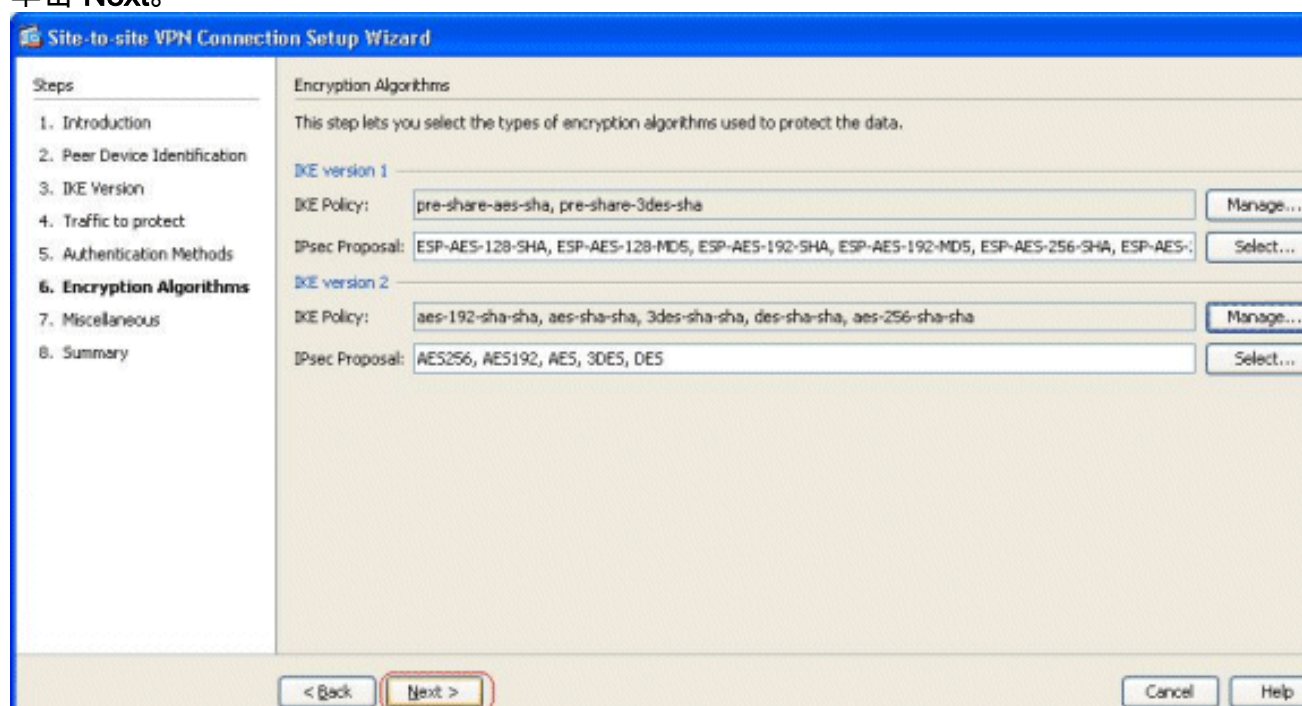


OK。

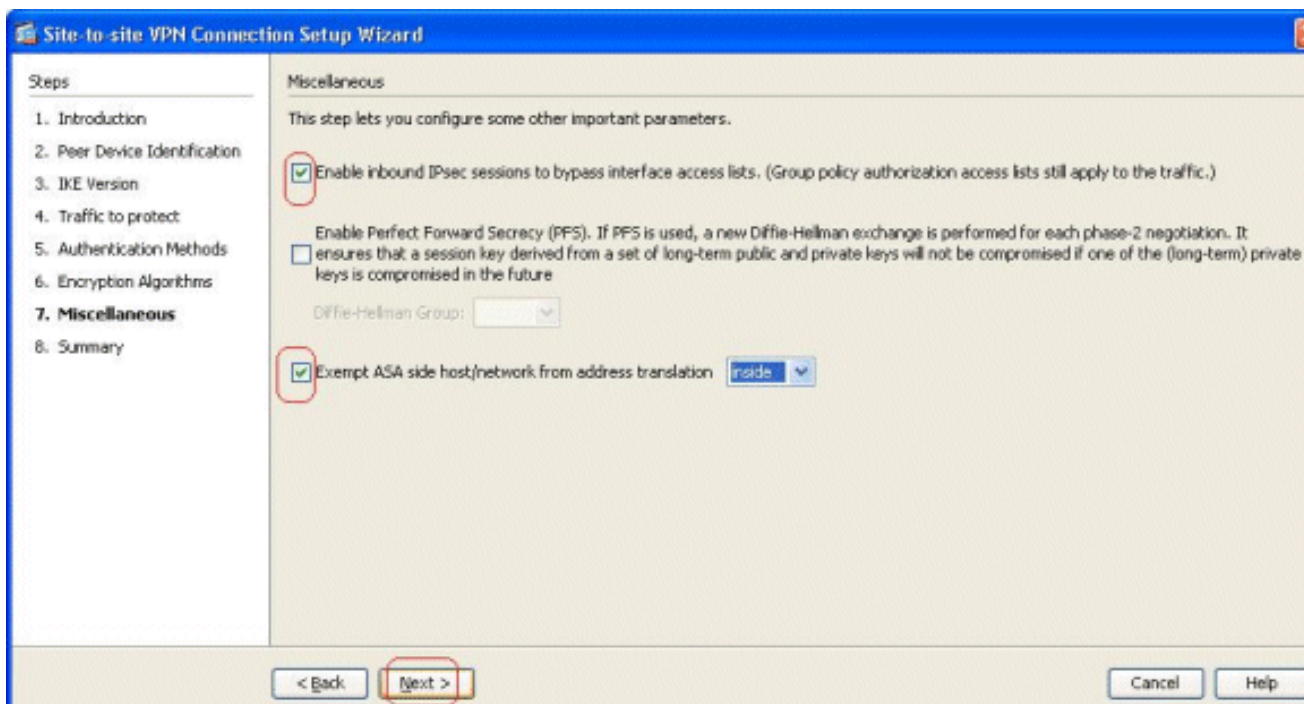
IKEv2允许

将分开协商的完整性算法与假随机的功能(PRF)算法。这在当前可用的选项的IKE策略能配置SHA-1或MD5。您不能修改默认情况下定义的IPsec建议参数。单击**精选**在IPsec建议字段旁边为了添加新建的参数。IKEv1和IKEv2之间的主要区别，根据IPsec建议，是IKEv1接受转换设置根据加密和认证算法的组合。IKEv2单个接受加密和完整性参数和终于做所有可能或组合这些。您可能查看这些在此向导结束时，概略的幻灯片的。

12. 单击 **Next**。

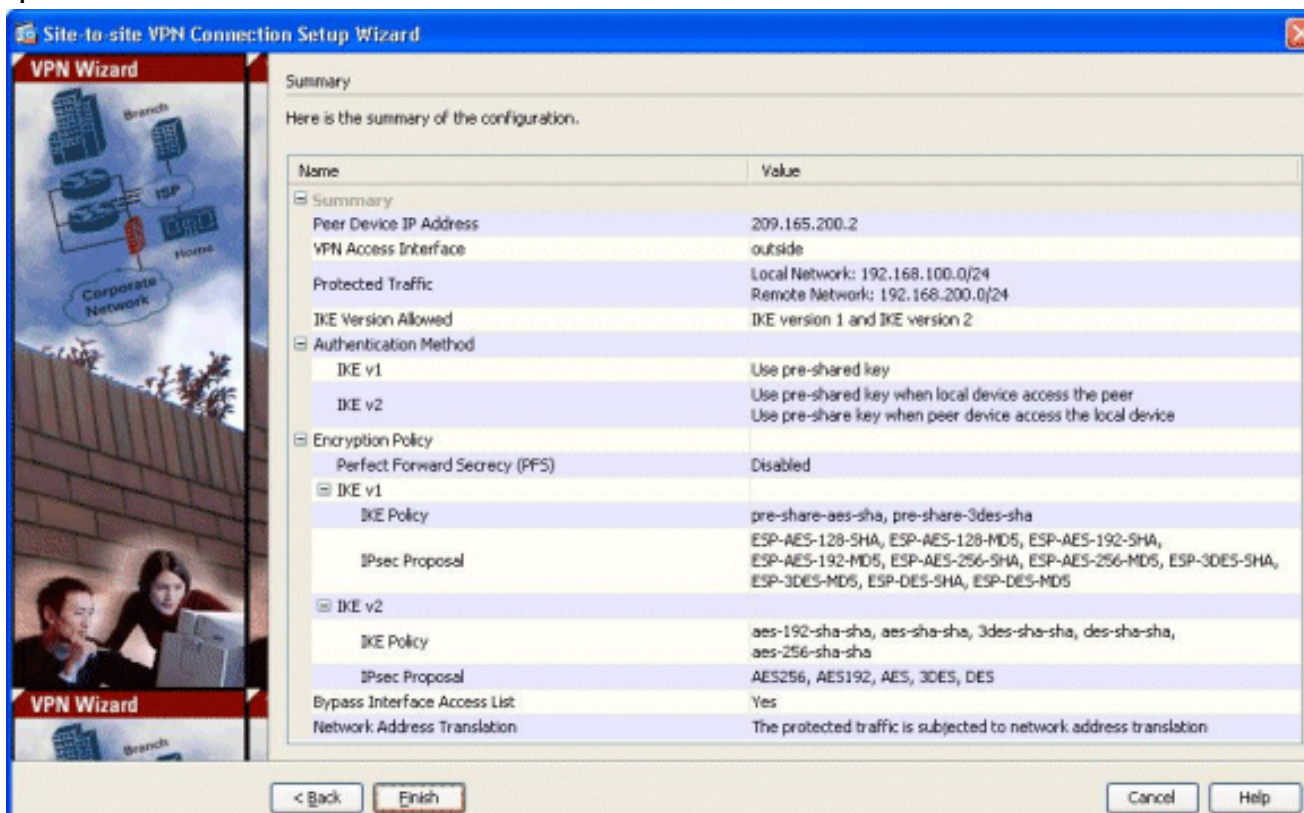


13. 指定详细信息，例如NAT免税、PFS和接口ACL绕过。**其次**选择。



14. 配置的摘要能被看到此处

:



点击芬通社为了完成站点到站点VPN通道向导。新连接配置文件创建与配置的参数。

## 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。

- [显示crypto ikev2 sa](#) -显示IKEv2运行时SA数据库。



- [显示vpn-sessiondb详细信息|2|](#) -显示关于站点到站点VPN会话的信息。

## [故障排除](#)

### [故障排除命令](#)

[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。

**注意：** 使用 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- [debug crypto ikev2](#) -表示IKEv2的调试消息。

## [相关信息](#)

- [Cisco ASA 5500系列设备技术支持](#)
- [技术支持和文档 - Cisco Systems](#)