

配置 Cisco VPN 3000 集中器与网络关联 PGP 客户端

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置网络关联PGP客户端连接到Cisco VPN 3000集中器](#)

[配置Cisco VPN 3000集中器接受从网络关联PGP客户端的连接](#)

[相关信息](#)

简介

本文描述如何配置Cisco VPN 3000集中器和网络关联相当完善的保密性(PGP)客户端运行版本6.5.1接受从彼此的连接。

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：

- Cisco VPN 3000集中器版本4.7
- 网络关联PGP客户端版本6.5.1

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。

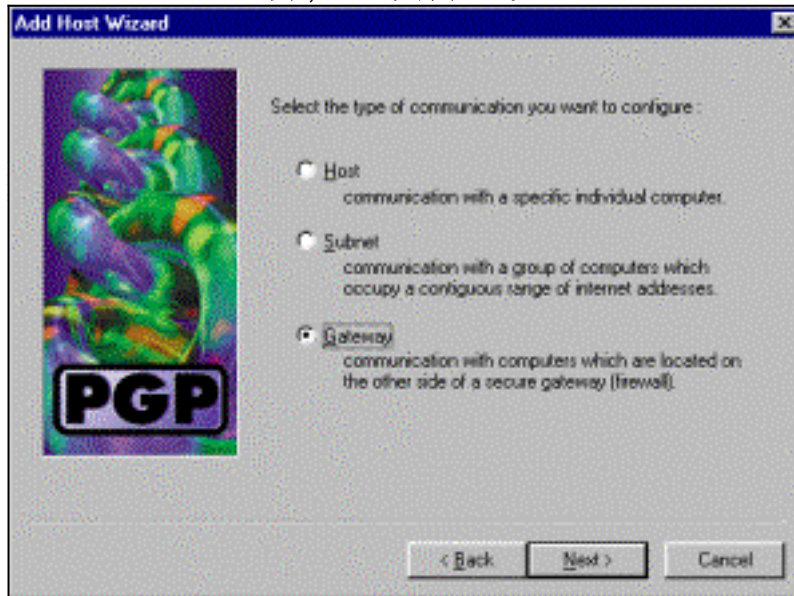
规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置网络关联PGP客户端连接到Cisco VPN 3000集中器

使用此步骤配置网络关联PGP客户端连接到VPN 3000集中器。

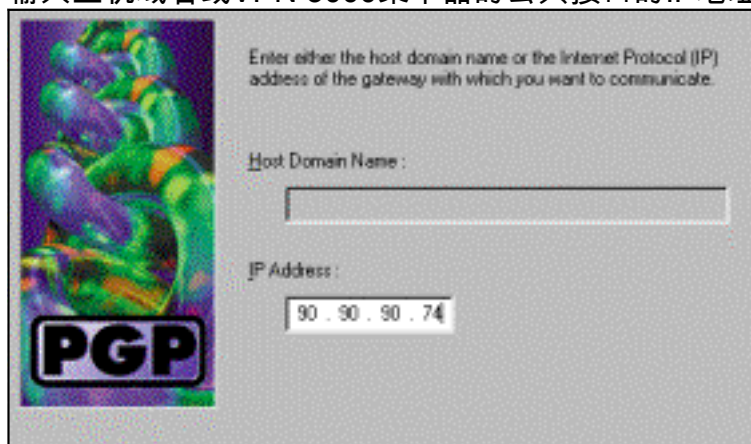
1. 启动PGPNet >主机。
2. 单击其次添加然后单击。
3. 选择GATEWAY选项，并且其次单击。



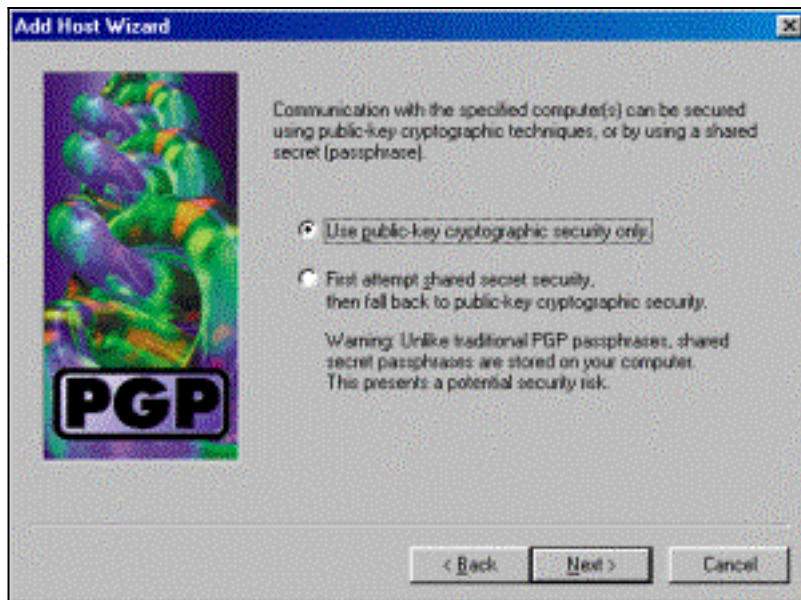
4. 进入连接的一描述性名称并且其次单击。



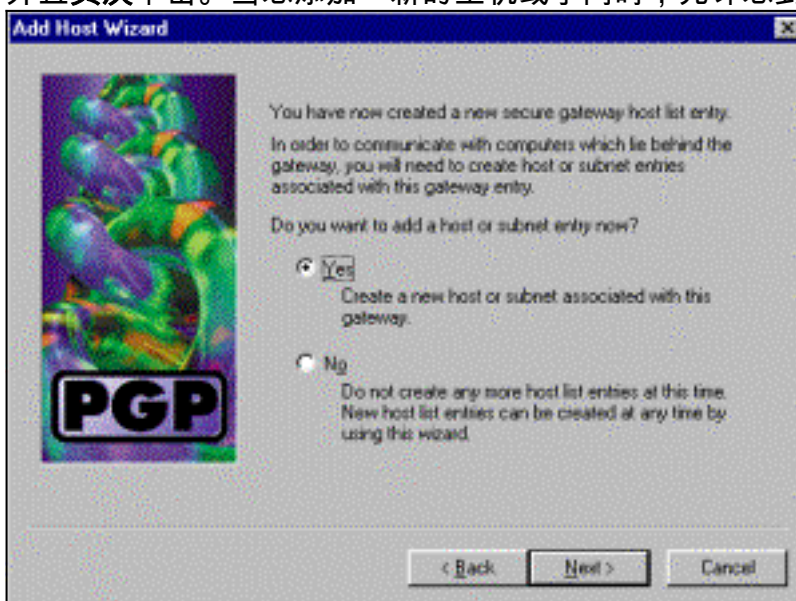
5. 输入主机域名或VPN 3000集中器的公共接口的IP地址并且其次单击。



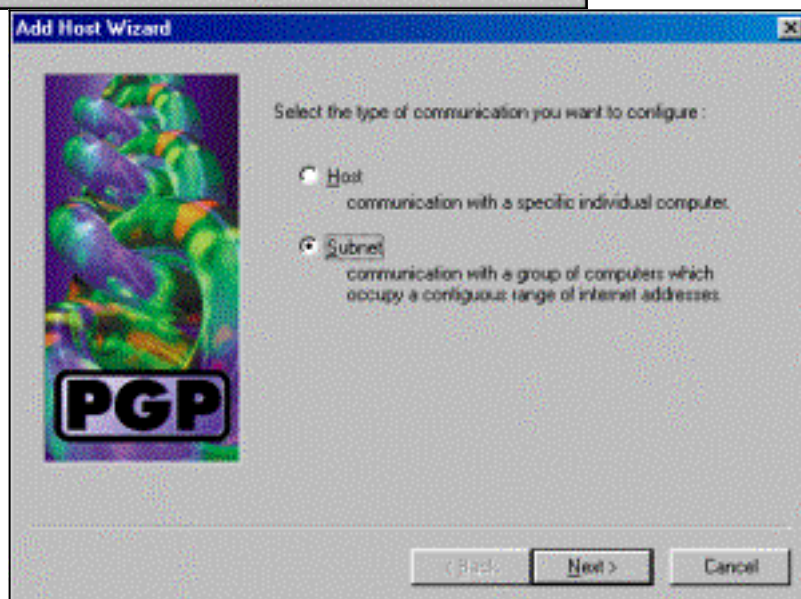
6. 选择仅使用公钥口令安全并且其次单击。



7. 选择是，并且其次单击。当您添加一新的主机或子网时，允许您到达私有网络，在您的连接被

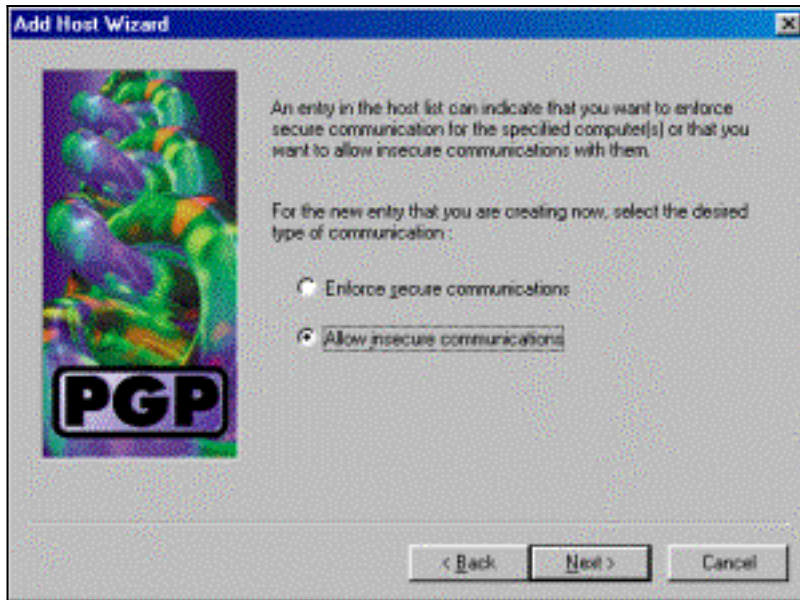


巩固后。

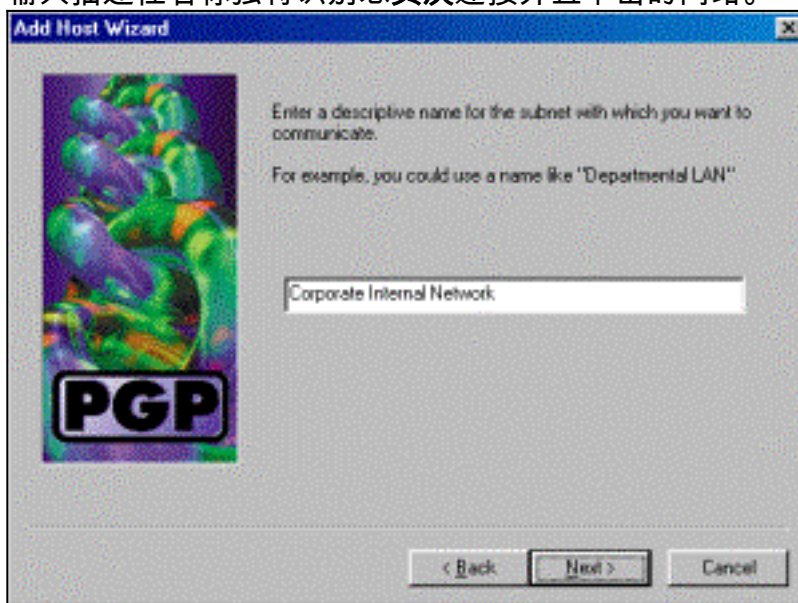


8. 选择子网并且其次单击。

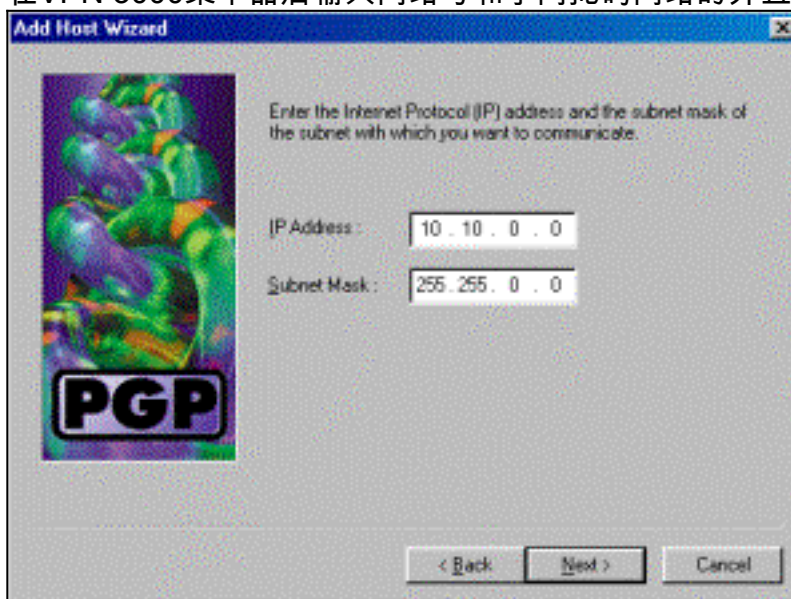
9. 选择允许不安全通信并且其次单击。VPN 3000集中器处理连接的安全，不是PGP客户端软件



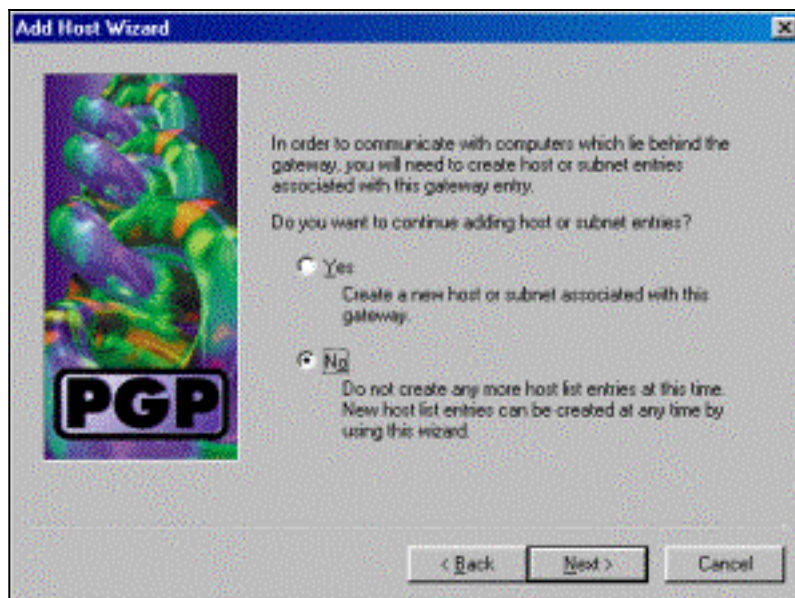
10. 输入描述性名称独特识别您其次连接并且单击的网络。



11. 在VPN 3000集中器后输入网络号和子网掩码网络的并且其次单击。



12. 如果有更多内部网络，请选择是。否则，请选择没有并且其次单击。



配置Cisco VPN 3000集中器接受从网络关联PGP客户端的连接

使用此步骤配置Cisco VPN 3000集中器接受从网络关联PGP客户端的连接：

1. 选择**Configuration > 建立隧道和安全 > IPSec > IKE Proposals**。
2. 通过选择它激活IKE-3DES-SHA-DSA建议在非激活建议列。其次，请点击**激活按钮**然后单击**保存必要的按钮**。
3. 选择**Configuration > Policy Management > Traffic Management > SAS**。
4. 单击 **Add**。
5. 留下所有除了这些字段在他们的默认设置：**SA名称**：创建唯一的名称识别此。**数字证书**：选择已安装服务器识别证书。**IKE建议**：挑选IKE-3DES-SHA-DSA。
6. 单击 **Add**。
7. 选择**Configuration > User Management > Groups**，单击**添加组**，并且配置这些字段：**注意**：如果所有您的用户是PGP客户端，您能使用基本组(**Configuration > User Management > Base Group**)而不是创建新建的组。如果那样，请跳到Identity选项的步骤并且完成仅IPSec选项的步骤1和2。在Identity选项下，请输入此信息：**组名称**:输入一个唯一的名称。(此组名一定是相等的与PGP客户端的数字证书的OU字段。)**密码**：输入组的密码。在IPSec选项下，请输入此信息：**验证**：设置此对无。**模式配置**:不选定此。
8. 单击 **Add**。
9. 保存始终当必要时。

相关信息

- [Cisco VPN 3000 系列集中器支持页](#)
- [IPSec 支持页面](#)
- [VPN软件下载\(仅限注册用户\)](#)
- [技术支持 - Cisco Systems](#)