PIX/ASA：VPN客户端用户的Kerberos认证和LDAP授权服务器组通过ASDM/CLI配置示例

目录

简介

本文描述如何使用Cisco Adaptive Security Device Manager (ASDM)配置Kerberos认证和LDAP授权服务器组Cisco PIX 500系列安全工具的。在本例中，服务器组由VPN隧道组的策略用于验证和认证流入的用户。

先决条件

要求

本文假设PIX是完全能操作和已配置的允许ASDM做配置更改。

注意： 要使 ASDM 可配置 PIX，请参阅允许 ASDM 进行 HTTPS 访问。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco PIX 安全设备软件 7.x 版及更高版本
- Cisco ASDM 5.x 版及更高版本

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。

相关产品

此配置可能也与Cisco可适应安全工具(ASA)版本7.x一起使用。

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

处理 VPN 用户时并不支持 PIX/ASA 7.x 软件中提供的所有可能的身份验证和授权方法。下表详细介绍对于 VPN 用户有哪些方法可用：

	本地	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
验证	是	是	是	是	是	是	否
授权	是	是	否	否	否	否	是

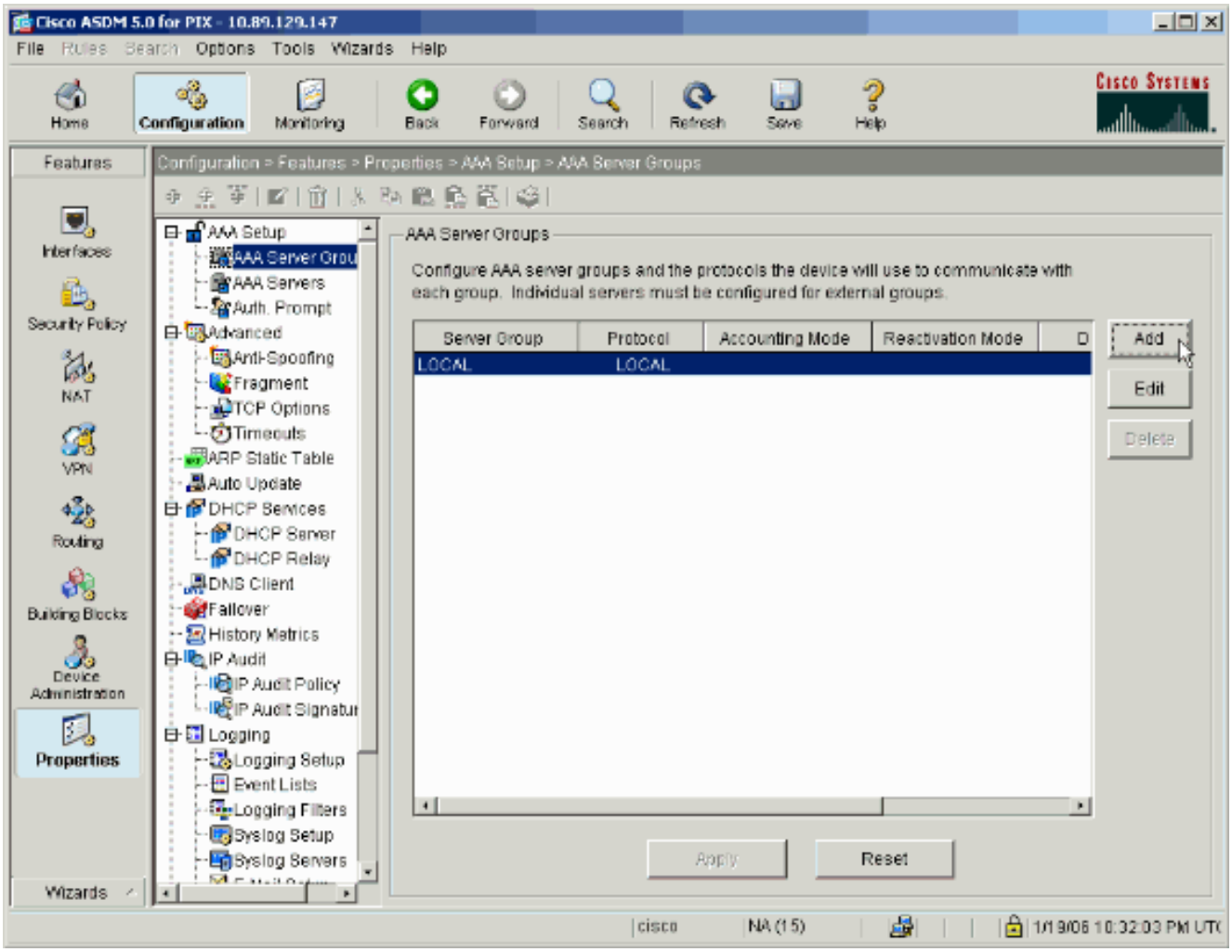
注意： 在本例中，Kerberos 和 LDAP 分别用于 VPN 用户的身份验证和授权。

使用 ASDM 配置 VPN 用户的身份验证和授权

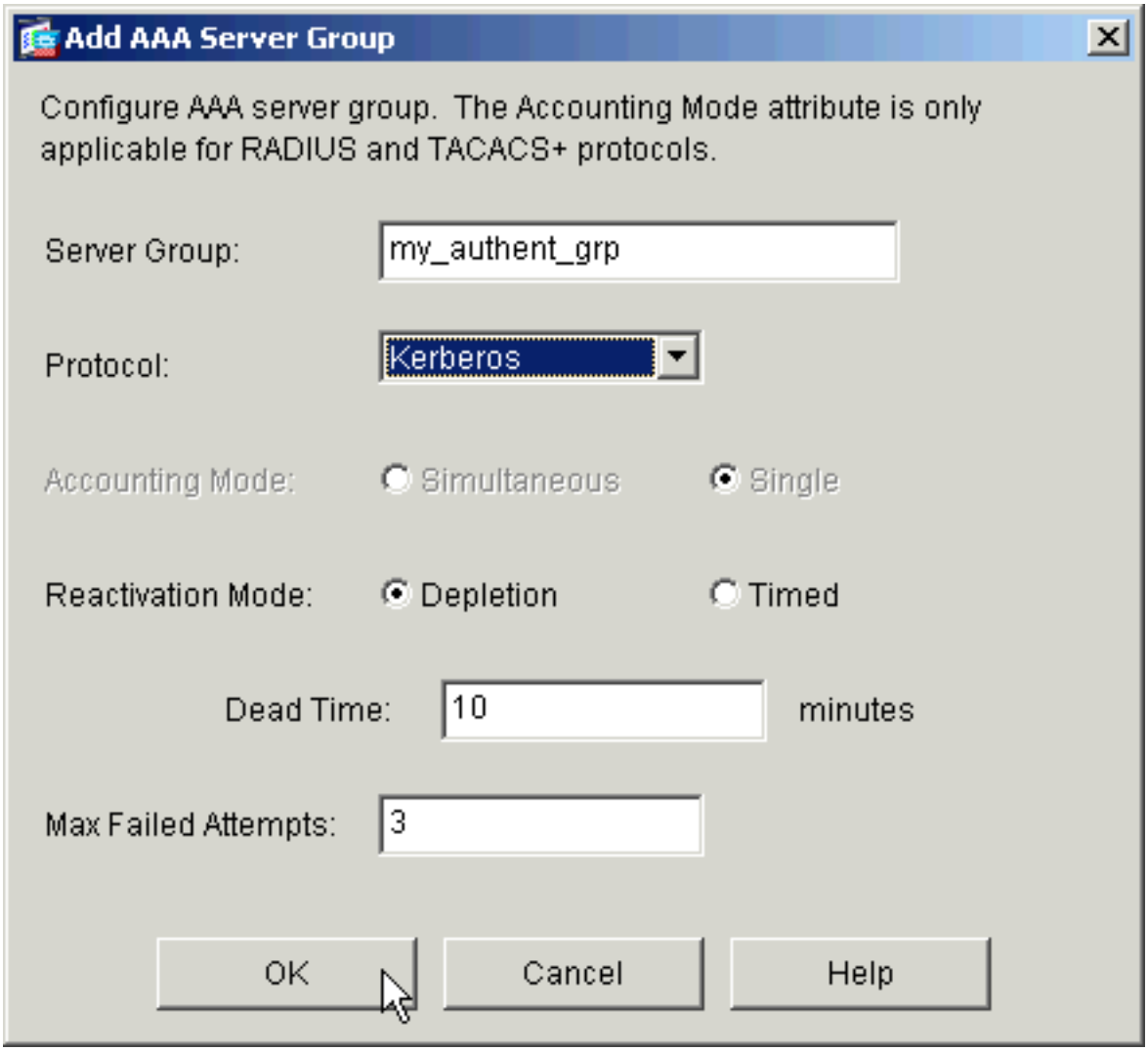
配置身份验证和授权服务器

完成这些步骤为了通过ASDM配置VPN用户的认证和授权服务器组。

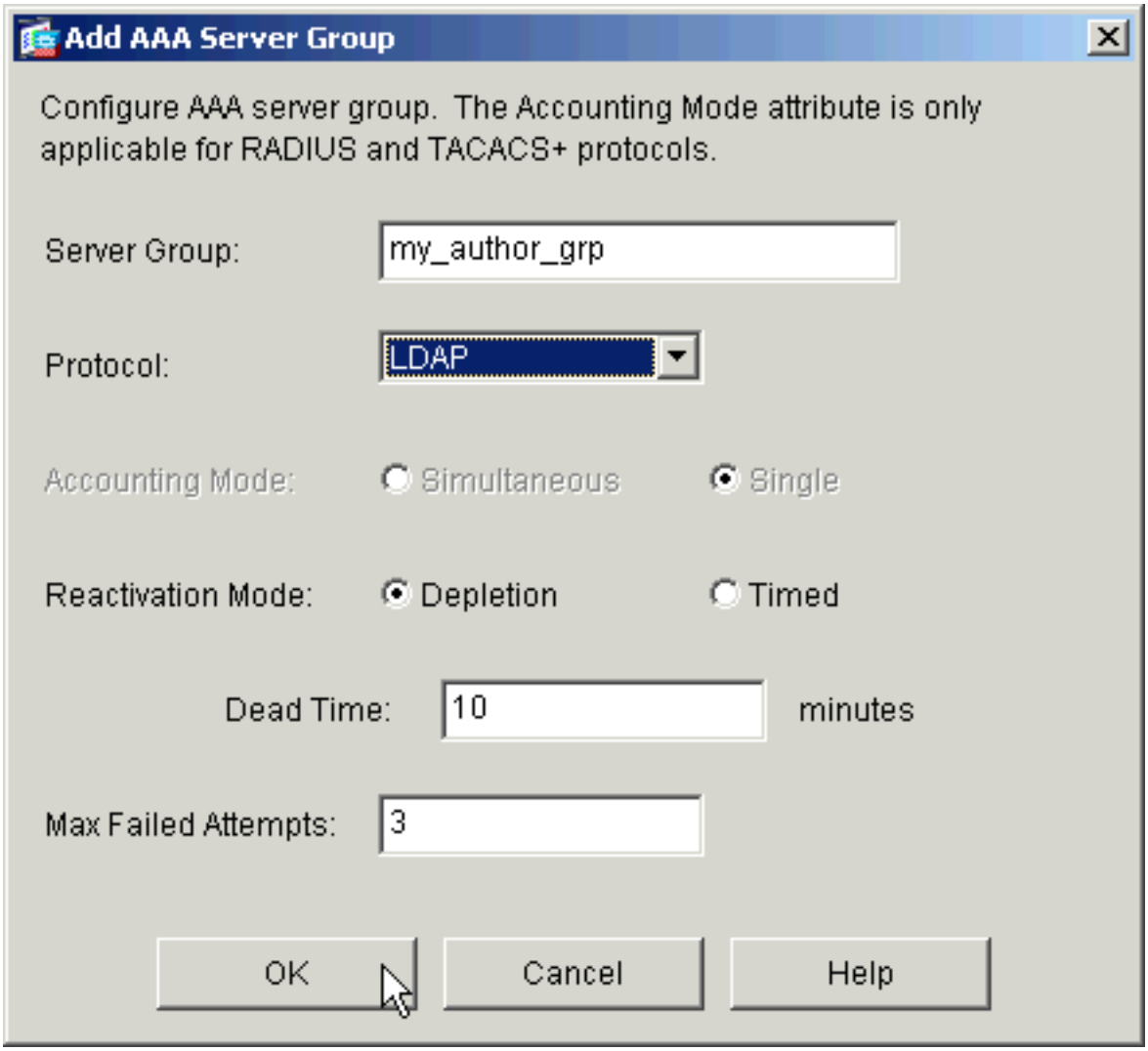
1. 选择**Configuration>属性>AAA设置>AAA服务器组**，并且单击**添加**。



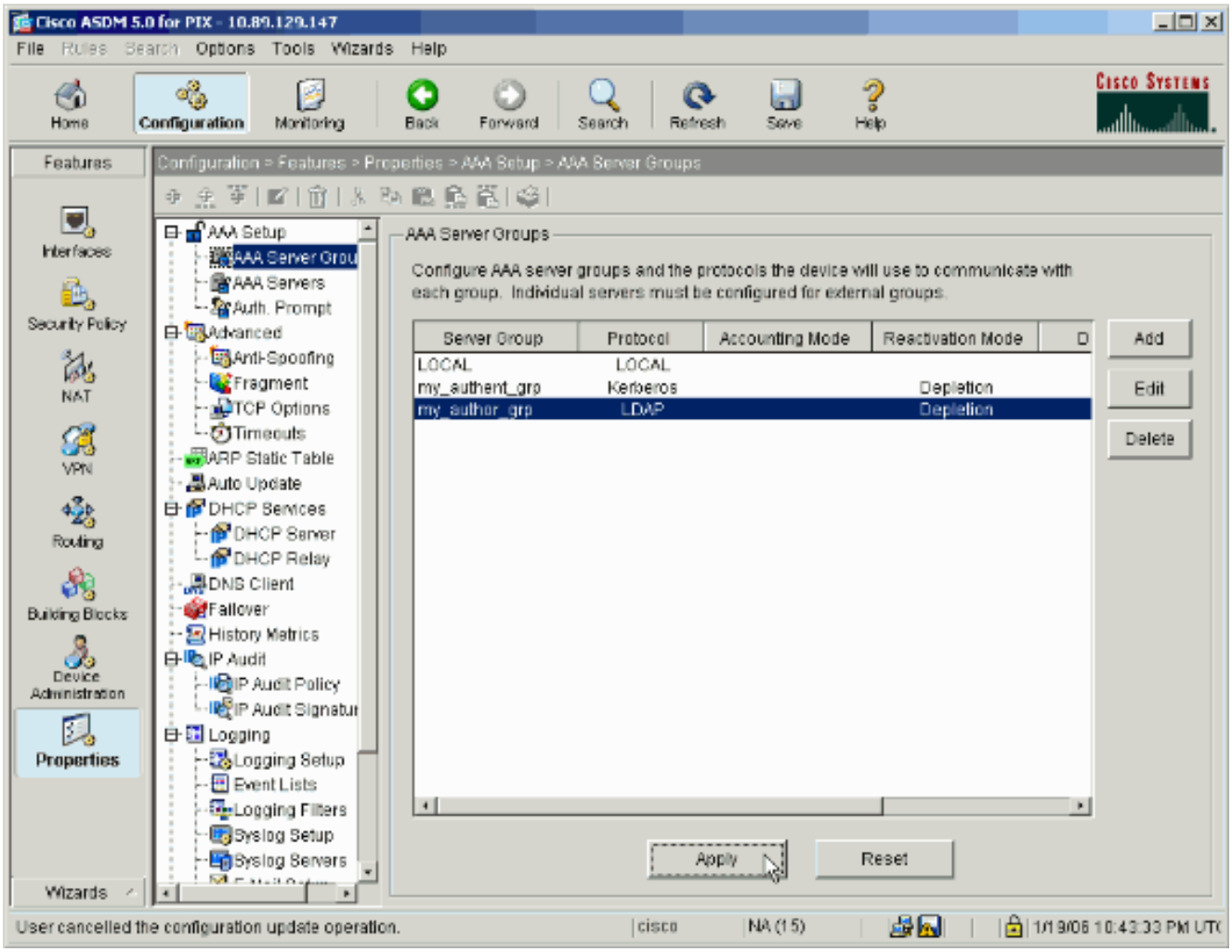
2. 定义一名称对于新证书服务器组，并且选择协议。Accounting Mode 选项仅用于 RADIUS 和 TACACS+。完成后单击 **OK**。



3. 重复步骤1和2为了创建一个新的授权服务器组。

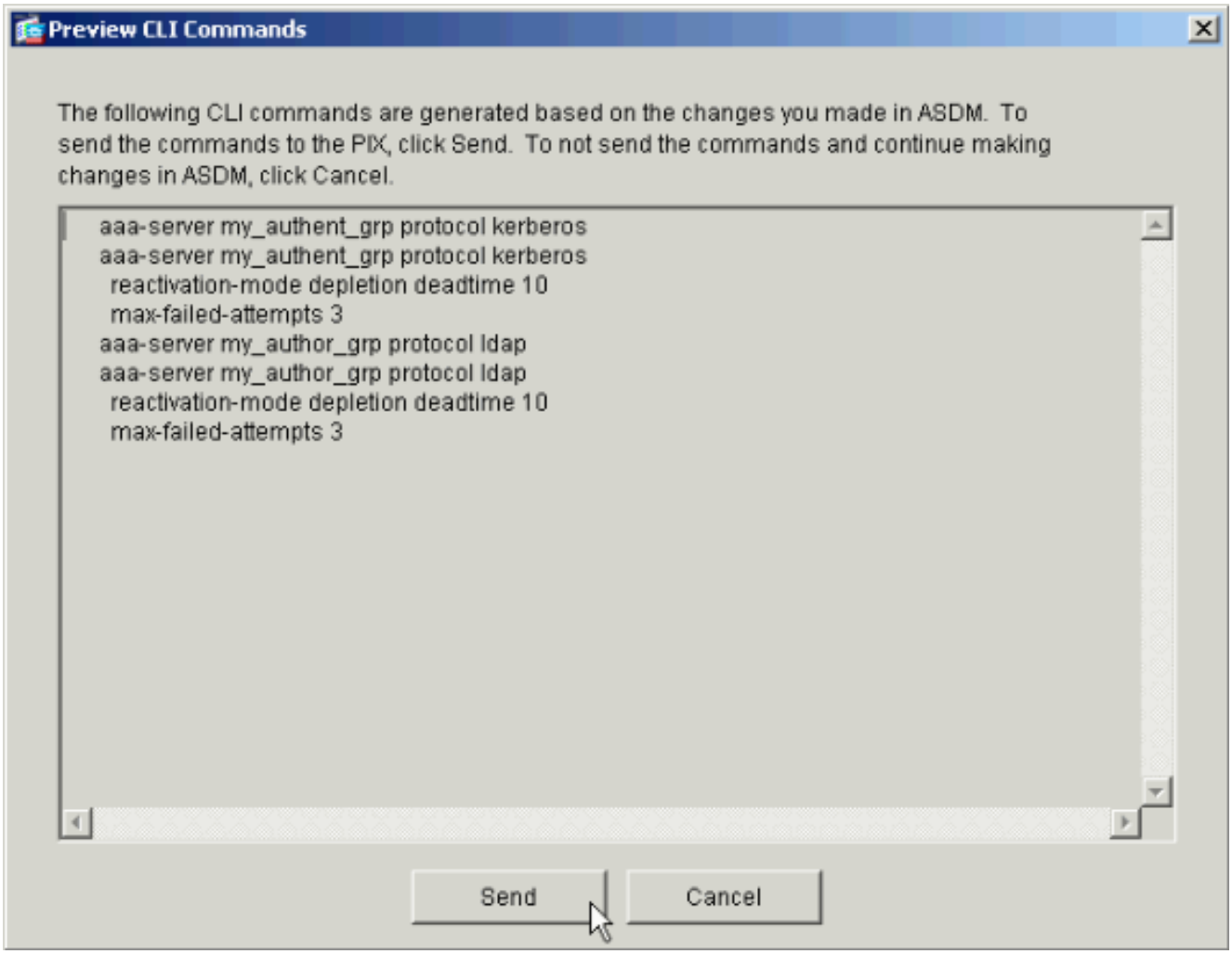


4. 单击**应用**为了发送对设备的更改。



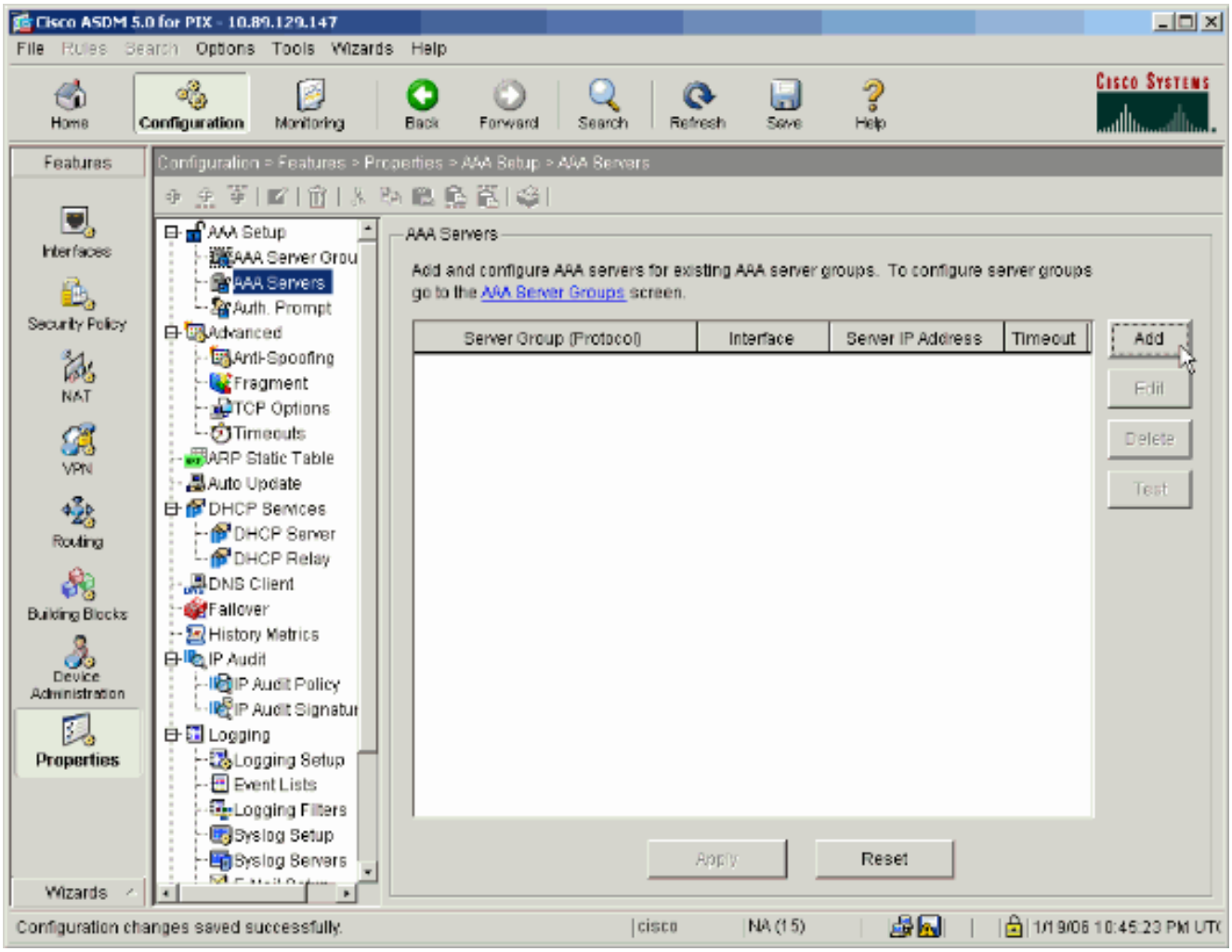
如果对其进行了相应配置，则设备当前将预览添加到运行配置的命令。

5. 点击**发送**为了发送命令到设备。

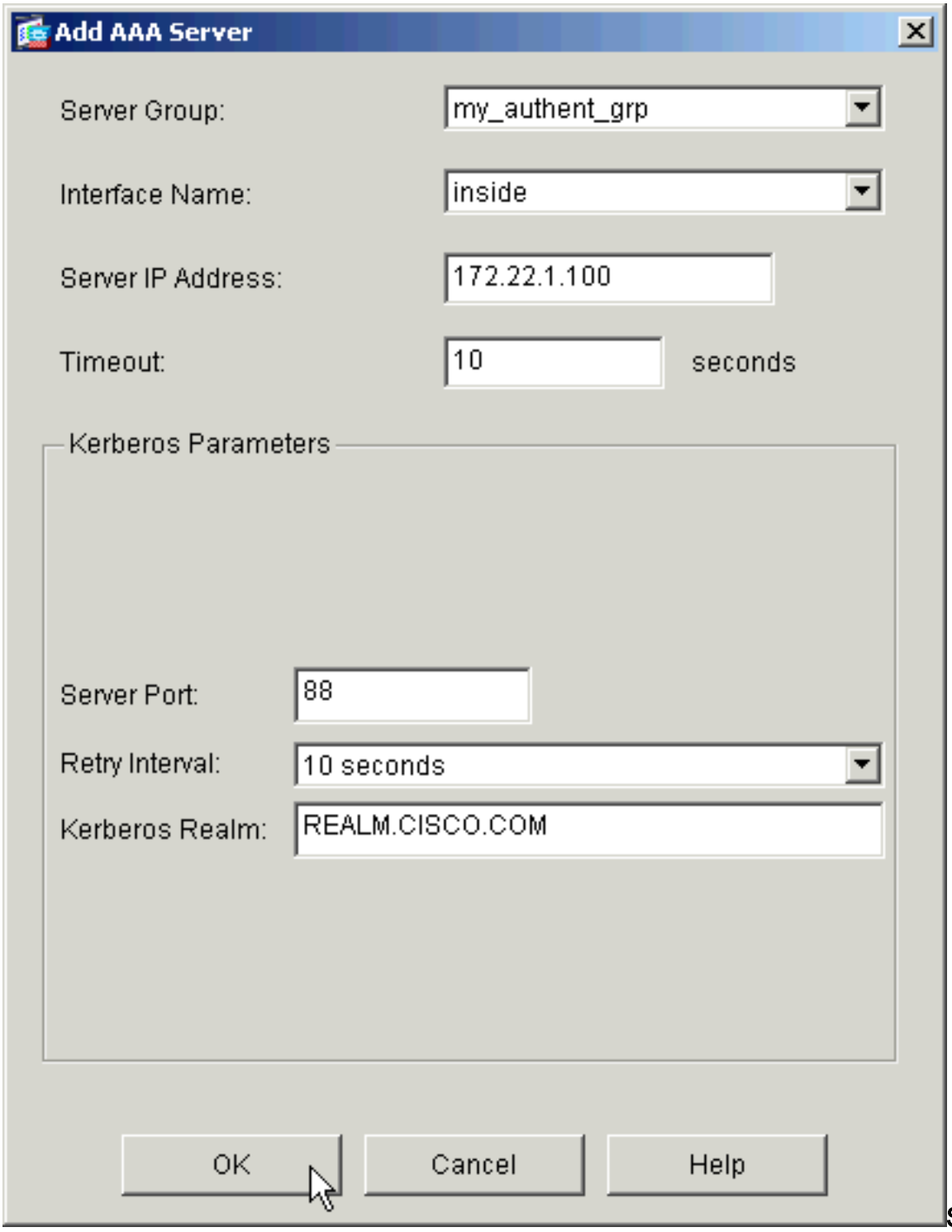


现在必须用身份验证和授权服务器填充新创建的服务器组。

6. 选择**Configuration>属性>AAA设置>AAA服务器**，并且单击**添加**。

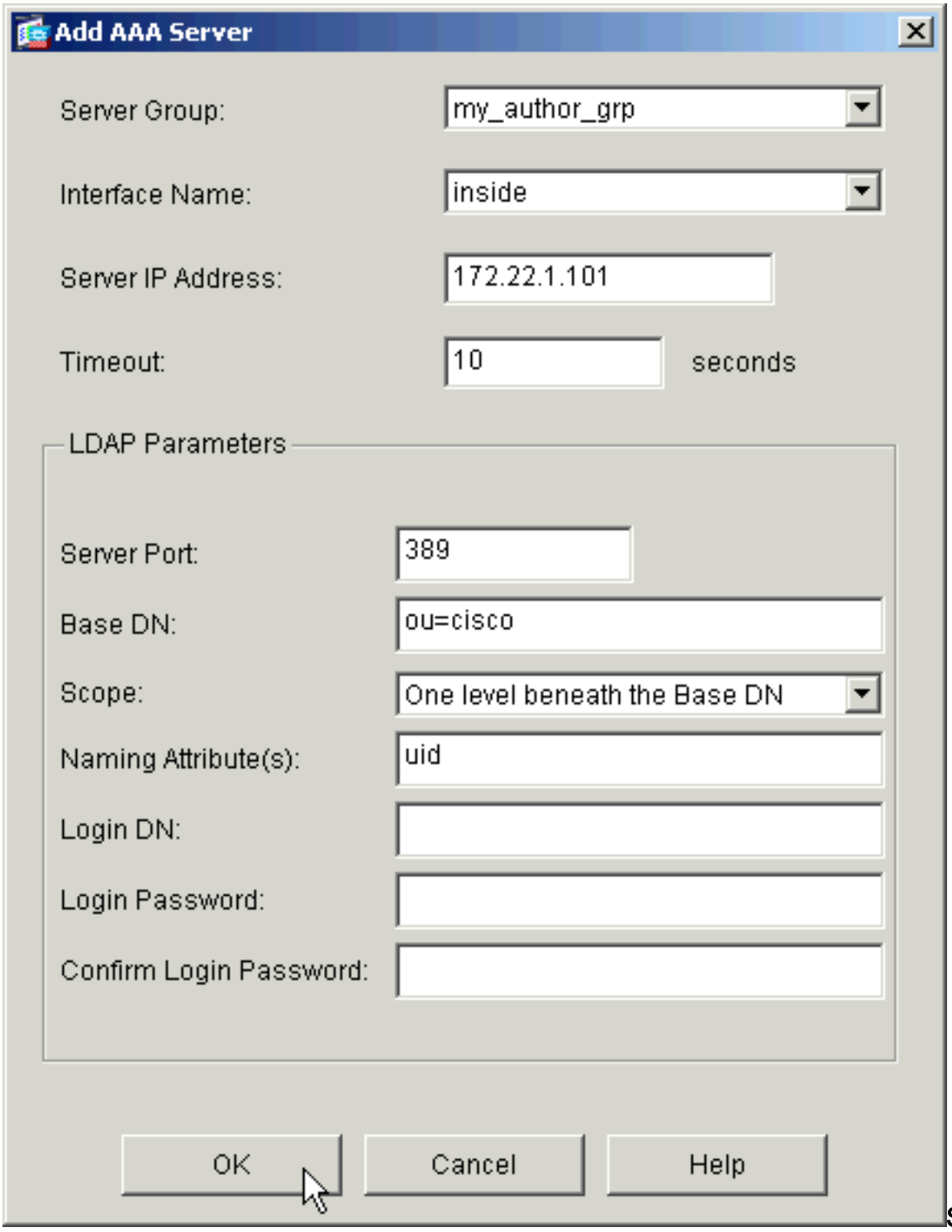


7. 配置身份验证服务器。完成后单击 OK。



Server Group — 选择步骤 2 中配置的身份验证服务器组。**Interface Name** — 选择服务器所在的接口。**Server IP Address** — 指定身份验证服务器的 IP 地址。**Timeout** — 指定等待服务器响应的最长时间（以秒计）。**Kerberos Parameters**：**Server Port** — 88 是 Kerberos 的标准端口。**Retry Interval** — 选择所需的重试间隔。**Kerberos Realm** — 输入 Kerberos 域的名称。通常这是全部为大写字母的 Windows 域名。

8. 配置授权服务器。完成后单击 **OK**。



Server Group — 选择步骤 3 中配置的授权服务器组。**Interface Name** — 选择服务器所在的接口。**Server IP Address** — 指定授权服务器的 IP 地址。**Timeout** — 指定等待服务器响应的最长时间（以秒计）。**LDAP Parameters**：**Server Port** — 389 是 LDAP 的默认端口。**Base DN** — 输入当服务器收到授权请求后在 LDAP 层次结构中应开始搜索的位置。**Scope** — 选择当服务器收到授权请求后对 LDAP 层次结构应搜索到的范围。**名字属性**—输入在LDAP服务器的条目独特定义的相对辨别名称属性。普通的名字属性是共同名称(CN)和用户ID (uid)。**Login DN** — 某些 LDAP 服务器（包括 Microsoft Active Directory 服务器）在其接受任何其他 LDAP 操作的请求之前，要求设备通过已经过身份验证的绑定建立握手。Login DN 字段定义设备的身份验证特征，这些特征应对应于具有管理权限的用户的那些特征。例如，cn=administrator。对于匿名访问，请将此字段留空。**Login Password** — 输入 Login DN 的密码。**Confirm Login Password** — 确认 Login DN 的密码。

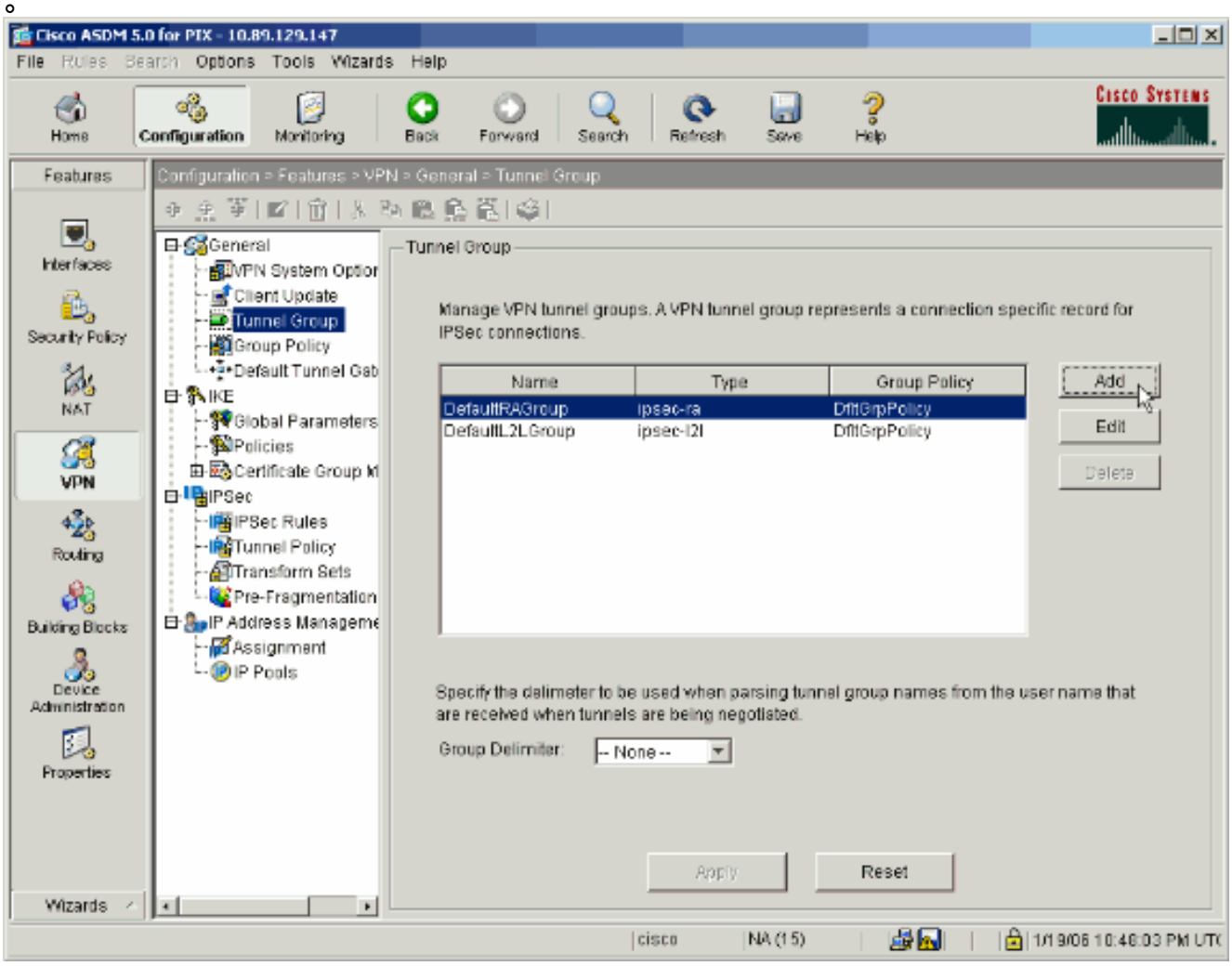
9. 在所有认证和授权服务器被添加后，请单击**应用**为了发送对设备的更改。如果对其进行了相应配置，则 PIX 当前将预览添加到运行配置的命令。

10. 点击**发送**为了发送命令到设备。

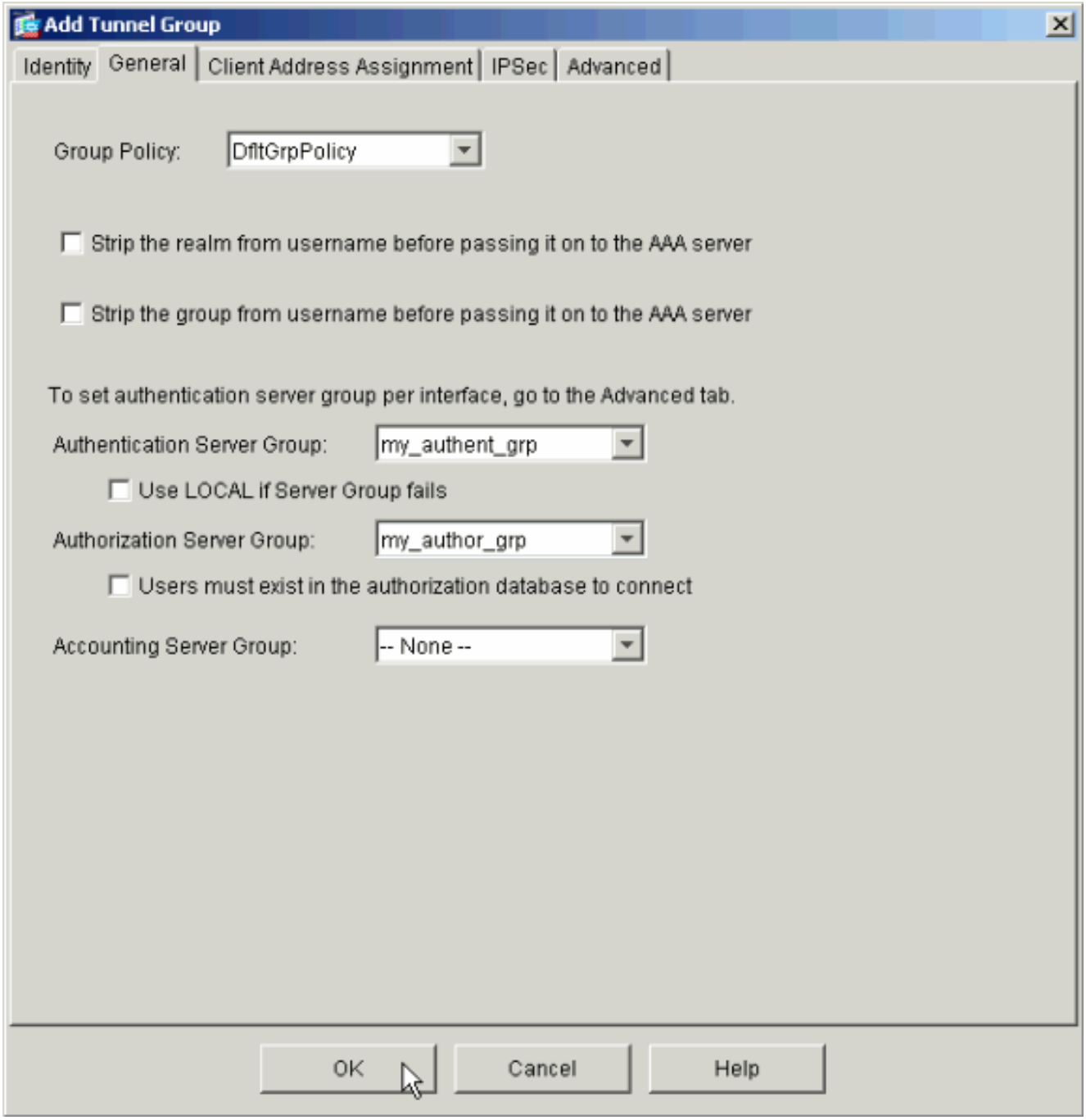
配置身份验证和授权的 VPN 隧道组

完成这些步骤为了添加您配置对VPN隧道组的服务器组。

1. 选择**Configuration> VPN >隧道组**，并且单击**添加**为了创建新通道组或者**编辑**为了修改现有组。



2. 在随后出现的窗口的 General 选项卡上，选择较早配置的服务器组。



3. ***可选：***如果添加了新的隧道组，则配置其他选项卡上的剩余参数。
4. 完成后单击 **OK**。
5. 在隧道组配置完成后，请单击**应用**为了发送对设备的更改。如果对其进行了相应配置，则 PIX 当前将预览添加到运行配置的命令。
6. 点击**发送**为了发送命令到设备。

使用 CLI 配置 VPN 用户的身份验证和授权

这是 VPN 用户的身份验证和授权服务器组的等效 CLI 配置。

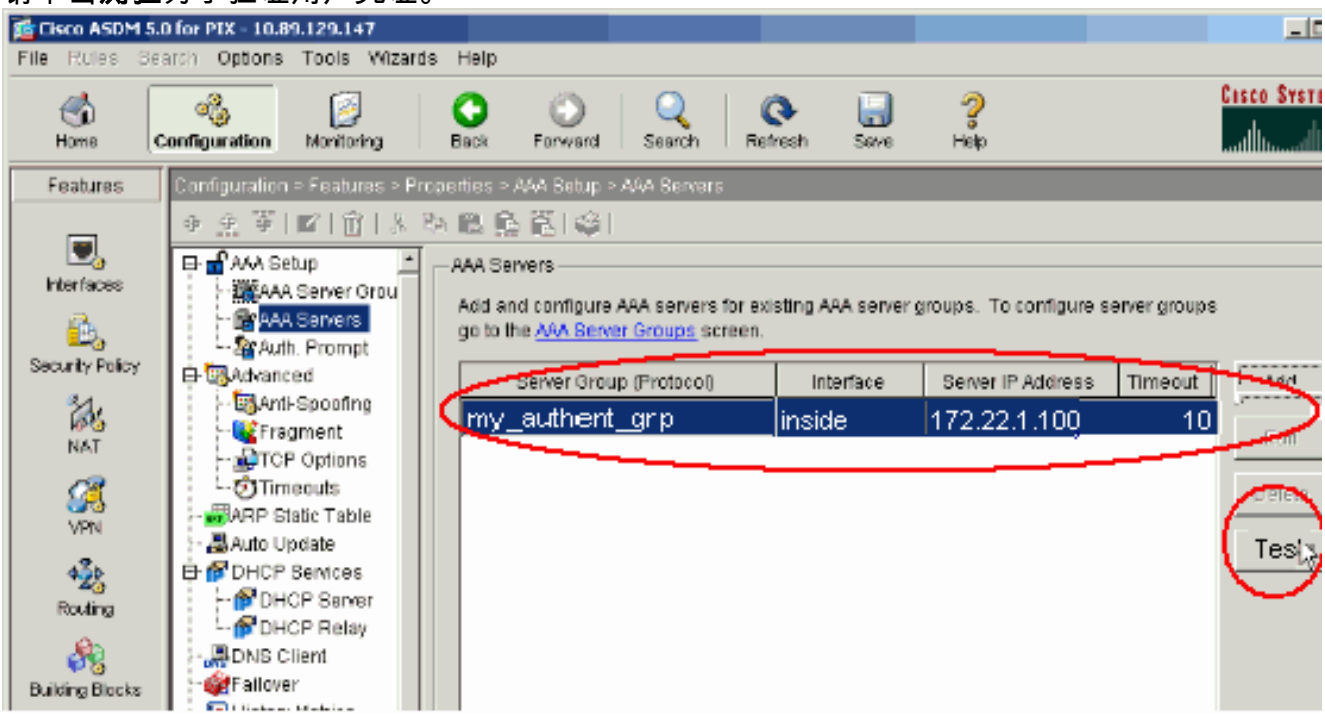
安全设备 CLI 配置
pixfirewall#**show run** : Saved : PIX Version 7.2(2) ! hostname pixfirewall domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0 shutdown no nameif no security-level no ip address ! interface Ethernet1 nameif inside security-level 100 ip address 172.22.1.105 255.255.255.0

```
! !--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid pager lines 24 mtu
inside 1500 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image flash:/asdm-522.bin !--- Output
is suppressed. aaa-server my_authent_grp protocol
kerberos aaa-server my_authent_grp host 172.22.1.100
kerberos-realm REALM.CISCO.COM aaa-server my_author_grp
protocol ldap aaa-server my_author_grp host 172.22.1.101
ldap-base-dn ou=cisco ldap-scope onelevel ldap-naming-
attribute uid http server enable http 0.0.0.0 0.0.0.0
inside no snmp-server location no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart tunnel-group DefaultRAGroup general-
attributes authentication-server-group my_authent_grp
authorization-server-group my_author_grp ! !--- Output
is suppressed.
```

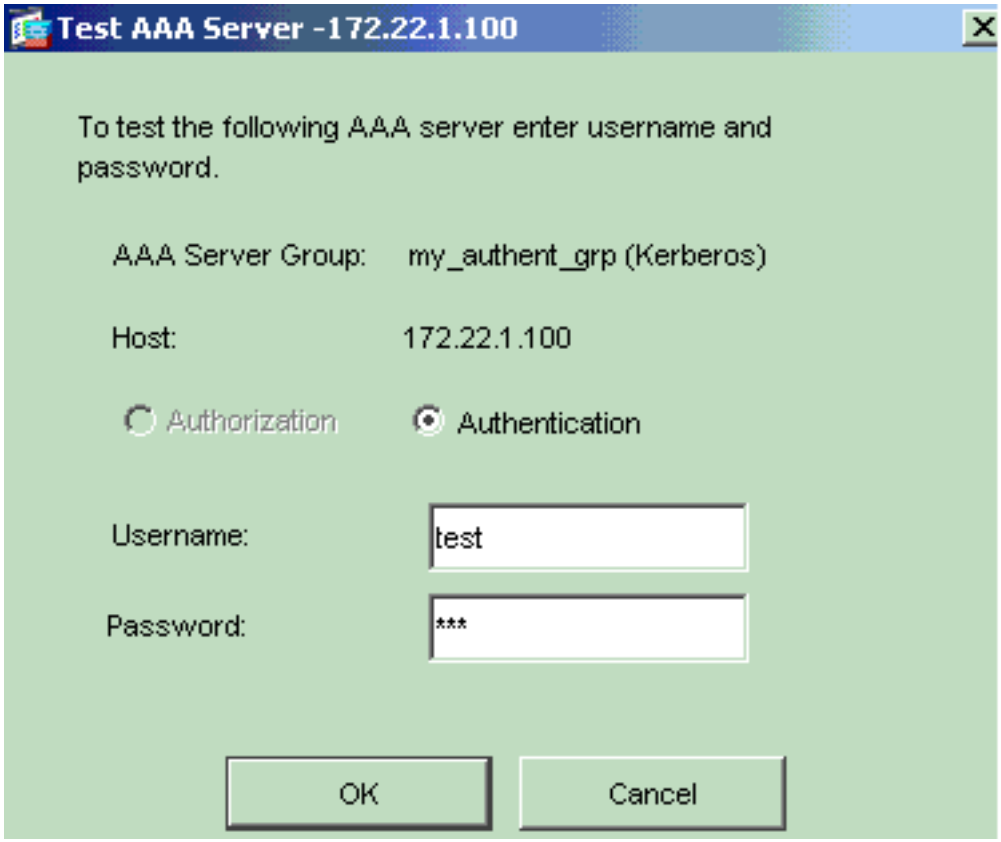
验证

完成以下这些步骤，验证 PIX/ASA 与 AAA 服务器之间的用户身份验证：

1. 选择**Configuration>属性>AAA设置>AAA服务器**，并且选择服务器组(my_authent_grp)。然后请单击**测验**为了验证用户凭证。

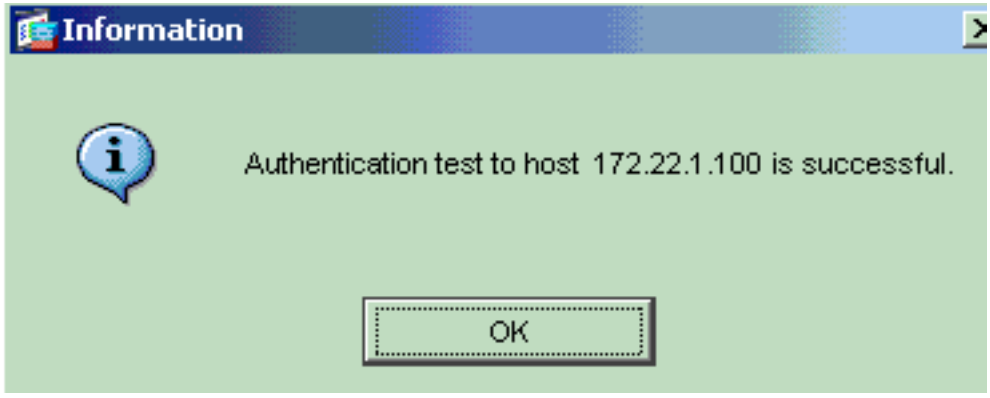


2. 提供 Username 和 Password（例如，username：test，而 password：测验)，和点击OK键为



了验证。

3. 您会看到身份验证成功。



故障排除

1. 身份验证失败的一个常见原因是时钟迟滞。请确保 PIX 或 ASA 上的时钟与身份验证服务器同步。当验证发生故障由于时滞时，您能收到此错误消息：`::- ERROR:Authentication Rejected:`Clock skew greater than 300 seconds..并且，此日志消息出现：`%PIX|ASA-3-113020 Kerberos error :Clock skew with server ip_address greater than 300 seconds`ip_address — Kerberos 服务器的 IP 地址。当由于安全设备和服务器上的时钟相差五分钟（300 秒），因此通过 Kerberos 服务器对 IPSec 或 WebVPN 用户进行身份验证失败时，将显示此消息。发生这种情况时，将拒绝连接尝试。为了解决此问题，请同步在安全工具和Kerberos服务器的时钟。
2. 必须禁用在激活目录(AD)的预验证，或者可能导致用户认证失败。
3. VPN客户端用户无法验证Microsoft Certificate服务器。显示以下错误消息：`"" (Error 14)`为了解决此问题，请不选定不**要求kerberose**在认证服务器的**预先身份验证**复选框。

相关信息

- 配置 AAA 服务器和本地数据库
- Cisco ASA 5500 系列自适应安全设备产品支持
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems