配置Cisco VPN 3000 系列集中器来支持带有RADIUS服务器的NT 密码到期功能

目录

简介

使用RADIUS服务器，本文包括关于如何的逐步指导配置Cisco VPN 3000系列集中器支持NT口令有效期功能。

参考的VPN3000 RADIUS with Expiry功能使用Microsoft互联网验证服务器为了学习与互联网认证服务器(IAS)的更加大致同样的案例。

先决条件

要求

- 如果您的RADIUS服务器和NT域验证服务器在两个独立的机器，请确保您设立了在两台机器之间的IP连通性。
- 确保您设立了从集中器的IP连通性到RADIUS服务器。如果RADIUS服务器是往公共接口，请勿忘记打开公共过滤器的RADIUS端口。
- 保证您能连接到从使用内部用户数据库的VPN客户端的集中器。如果这没有配置，请参考配置Ipsec- Cisco 3000 VPN客户端对VPN 3000集中器。

注意： 密码到期功能不可能与Web VPN或SSL VPN客户端一起使用。

使用的组件

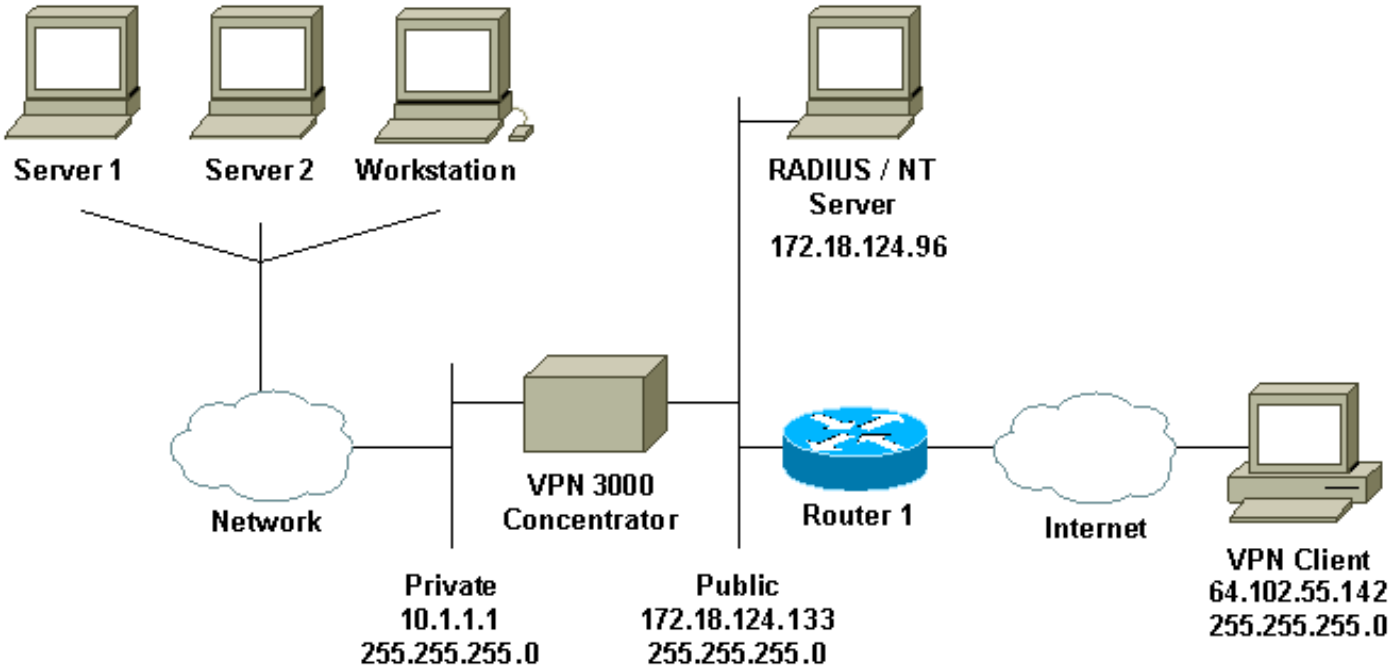
此配置使用下面软件和硬件版本开发并且被测试。

- VPN 3000集中器软件版本4.7
- VPN客户端版本3.5
- NT (CSNT)版本3.0 Microsoft Windows 2000激活目录服务器的Cisco Secure用户认证的

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。

网络图

本文档使用以下网络设置：



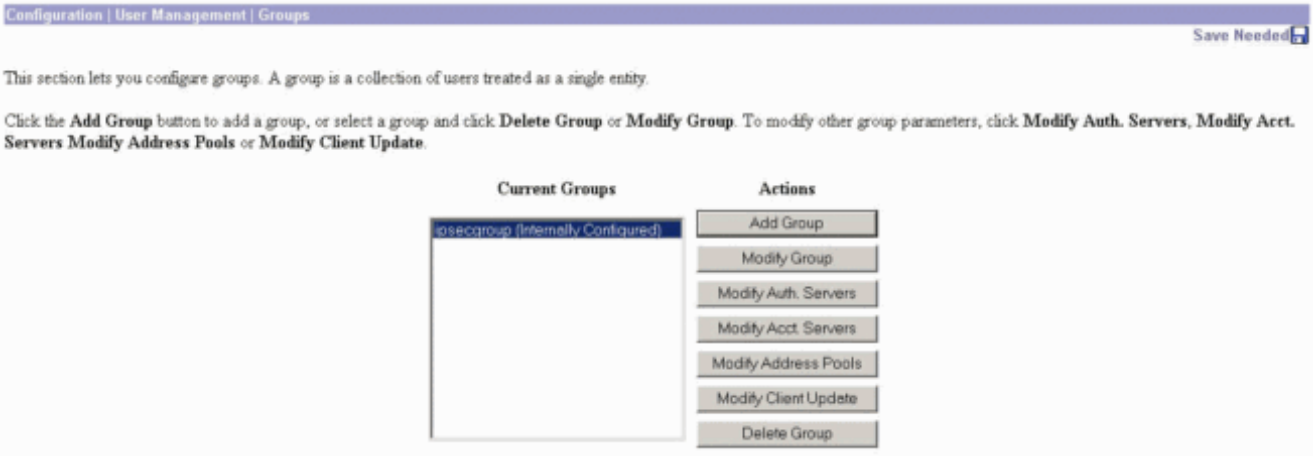
图表 注释

1. RADIUS服务器在此配置方面在公共接口。如果这是有您的特定设置的实际情形，请创建在您的公共过滤器的两个规则允许RADIUS流量输入和留下集中器。
2. 此配置显示运行在同样计算机的CSNT软件和NT域验证服务。这些元素在两个独立的机器可以如果必须由您的配置负责。

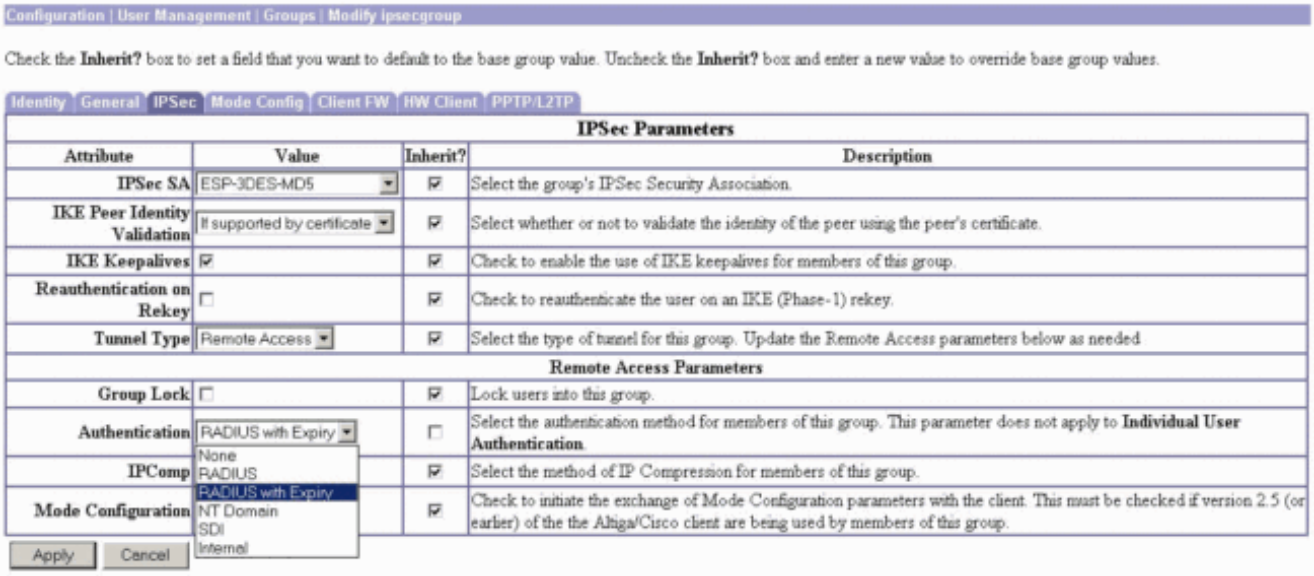
配置 VPN 3000 集中器

组配置

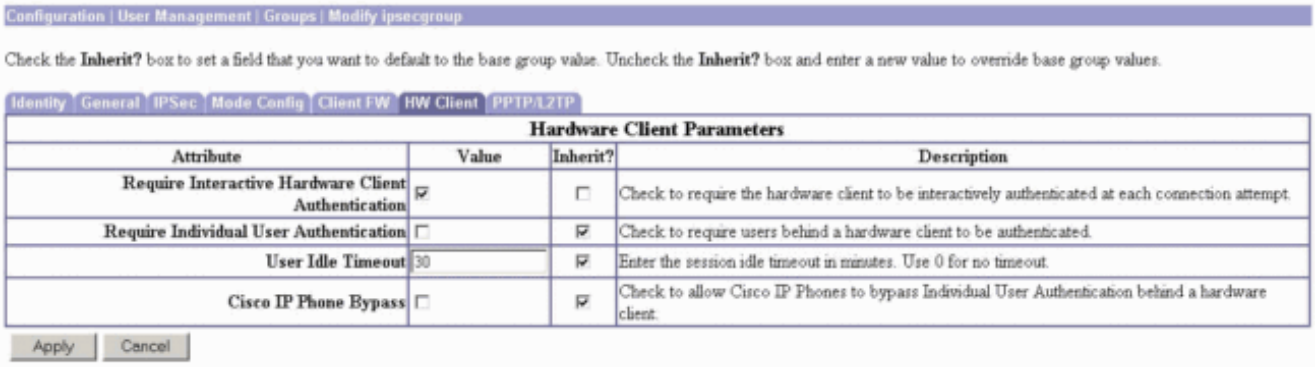
1. 要配置组接受从RADIUS服务器的NT口令有效期参数，去**Configuration > User Management > Groups**，选择您的从列表的组，和点击**修改组**。下面的示例显示如何修改名为“ipsecgroup的组”。



2. 去**IPSec选项**，确保， **RADIUS with Expiry**为**验证**属性选择。

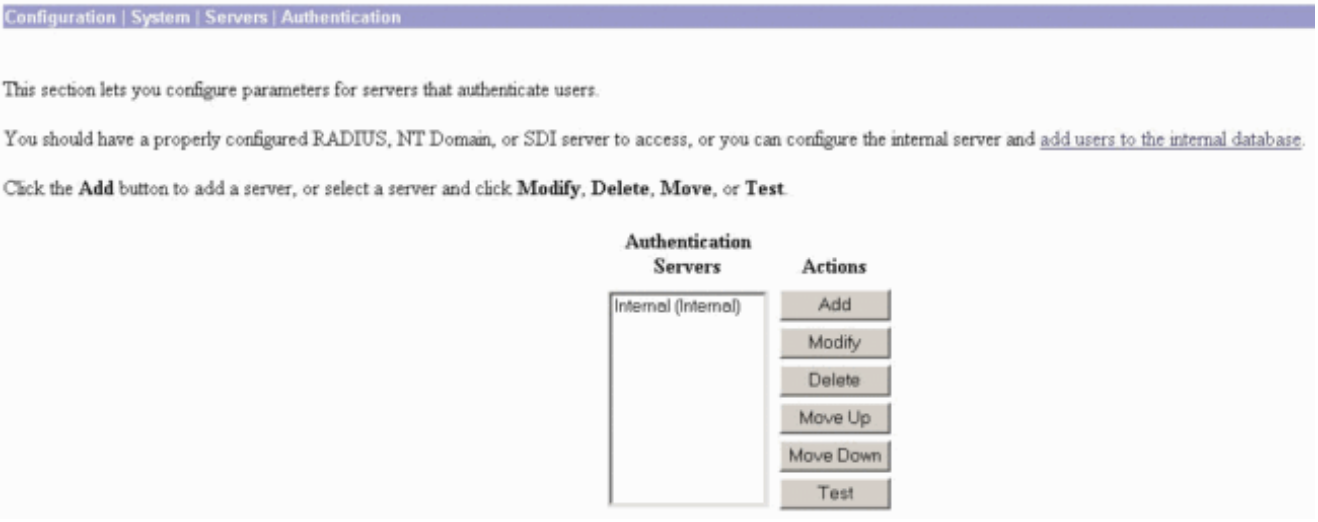


3. 如果在VPN 3002 Hardware Clients希望此功能启用，请去**HW Client选项**，确保， **Require Interactive Hardware Client Authentication**启用，则单击**应用**。

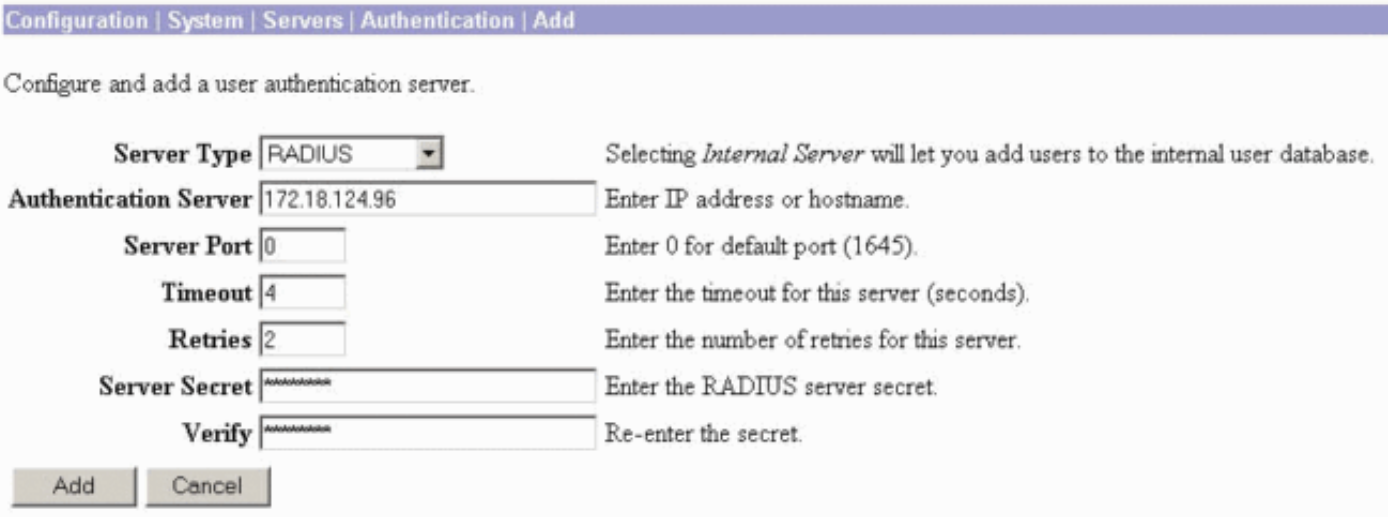


RADIUS 配置

1. 要配置在集中器的RADIUS服务器设置，请去**Configuration > System > Servers > Authentication** >Add。



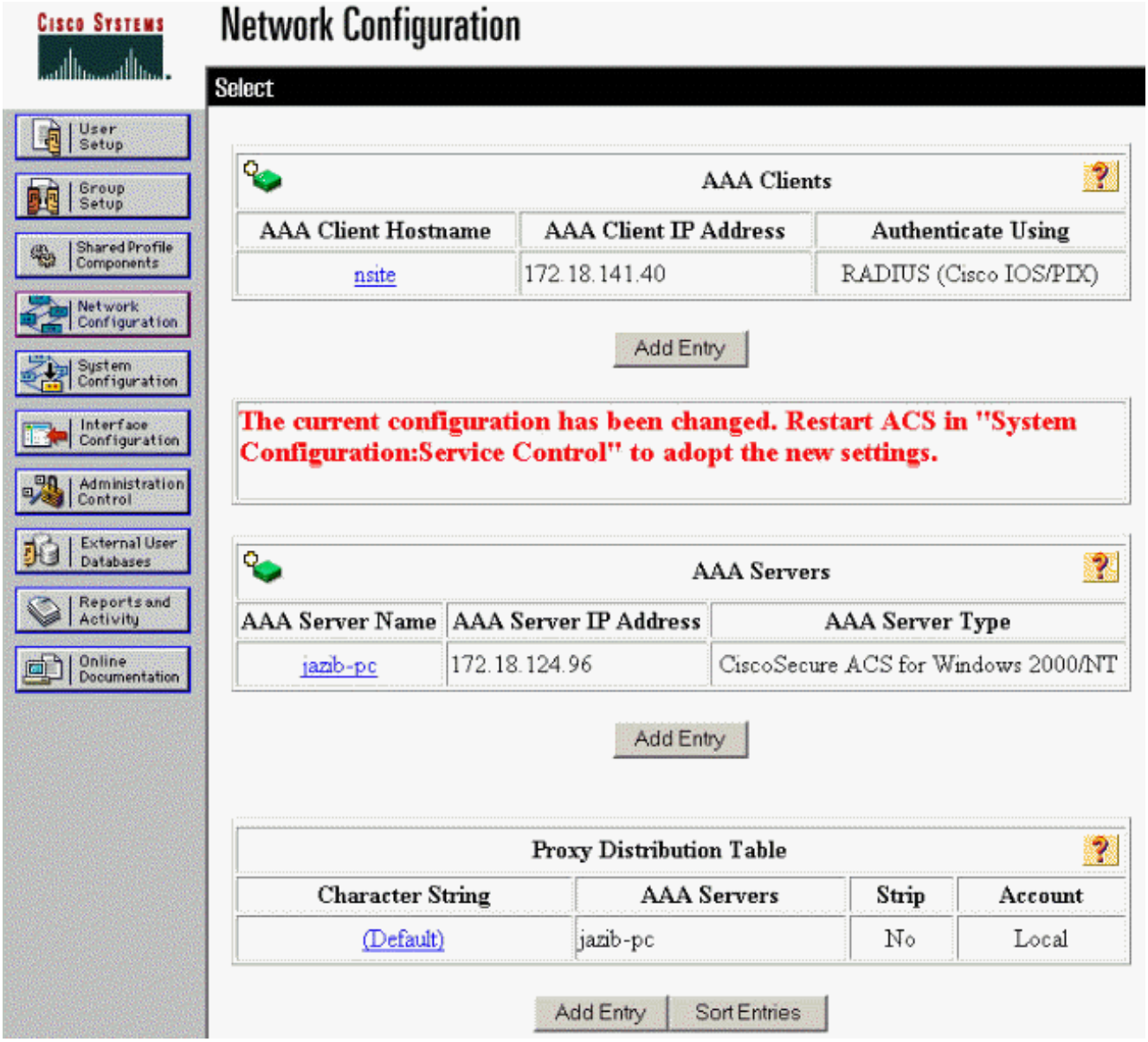
2. 在**Add屏幕上**，请键入对应于RADIUS服务器并且单击**添加的**值。下面的示例使用以下值。
   `Server Type: RADIUS Authentication Server: 172.18.124.96 Server Port = 0 (for default of 1645) Timeout = 4 Reties = 2 Server Secret = cisco123 Verify: cisco123`



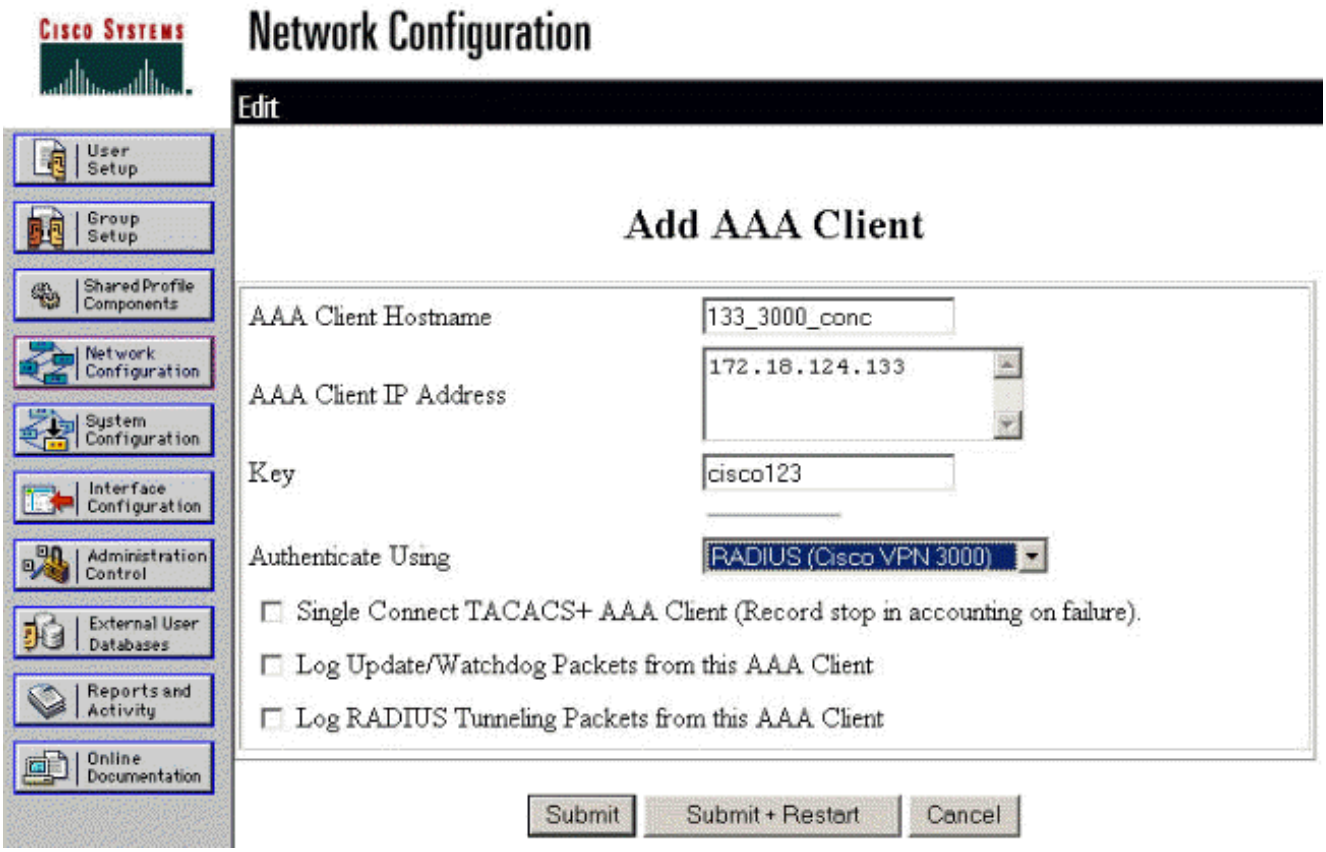
配置 Cisco Secure NT RADIUS 服务器

为 VPN 3000 集中器配置条目

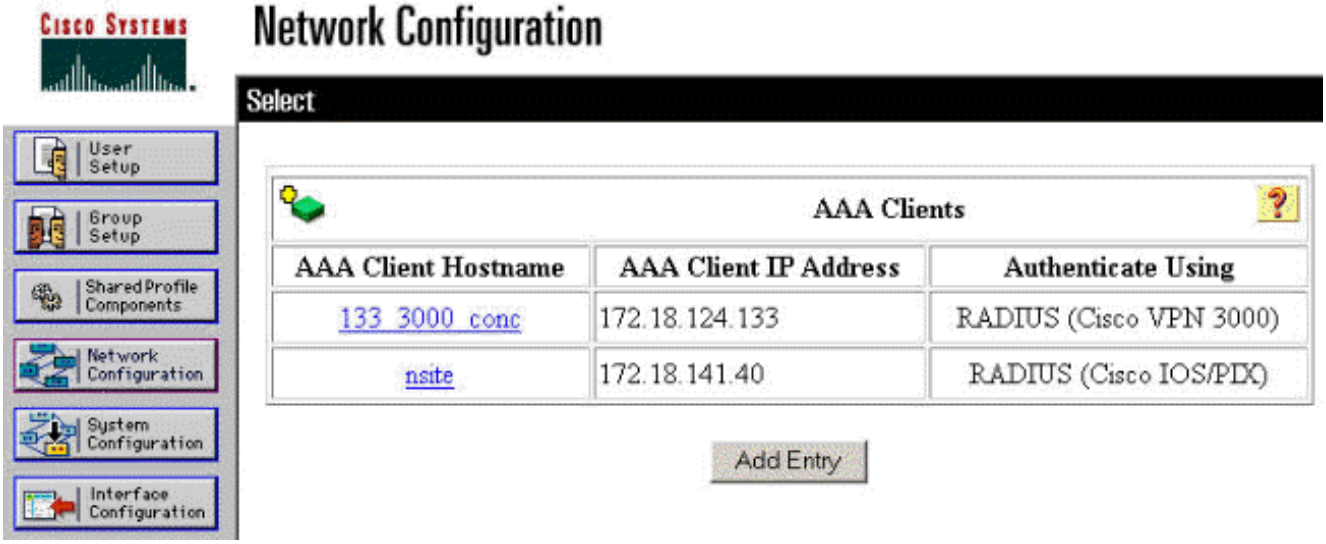
1. 登录CSNT并且点击**网络配置**在左面板中。在“AAA客户端下”，请点击**Add条目**。



2. 在“请添加AAA客户端”屏幕，输入适当的值添加集中器作为RADIUS客户端，然后点击 **Submit+Restart**。下面的示例使用以下值。`AAA Client Hostname = 133_3000_conc AAA Client IP Address = 172.18.124.133 Key = cisco123 Authenticate using = RADIUS (Cisco VPN 3000)`

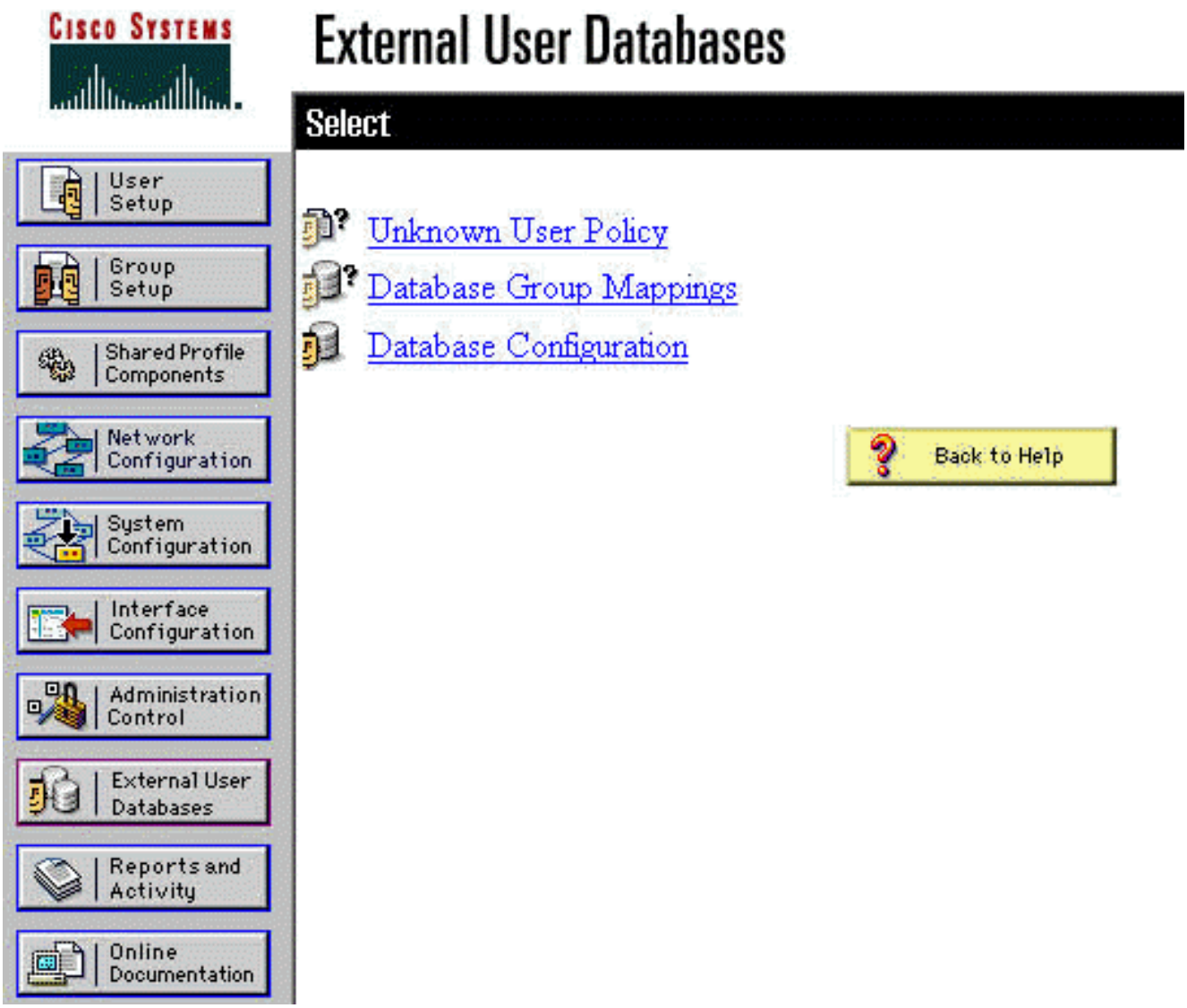


您的3000集中器的一个条目将出现在“**AAA客户端**”部分下。

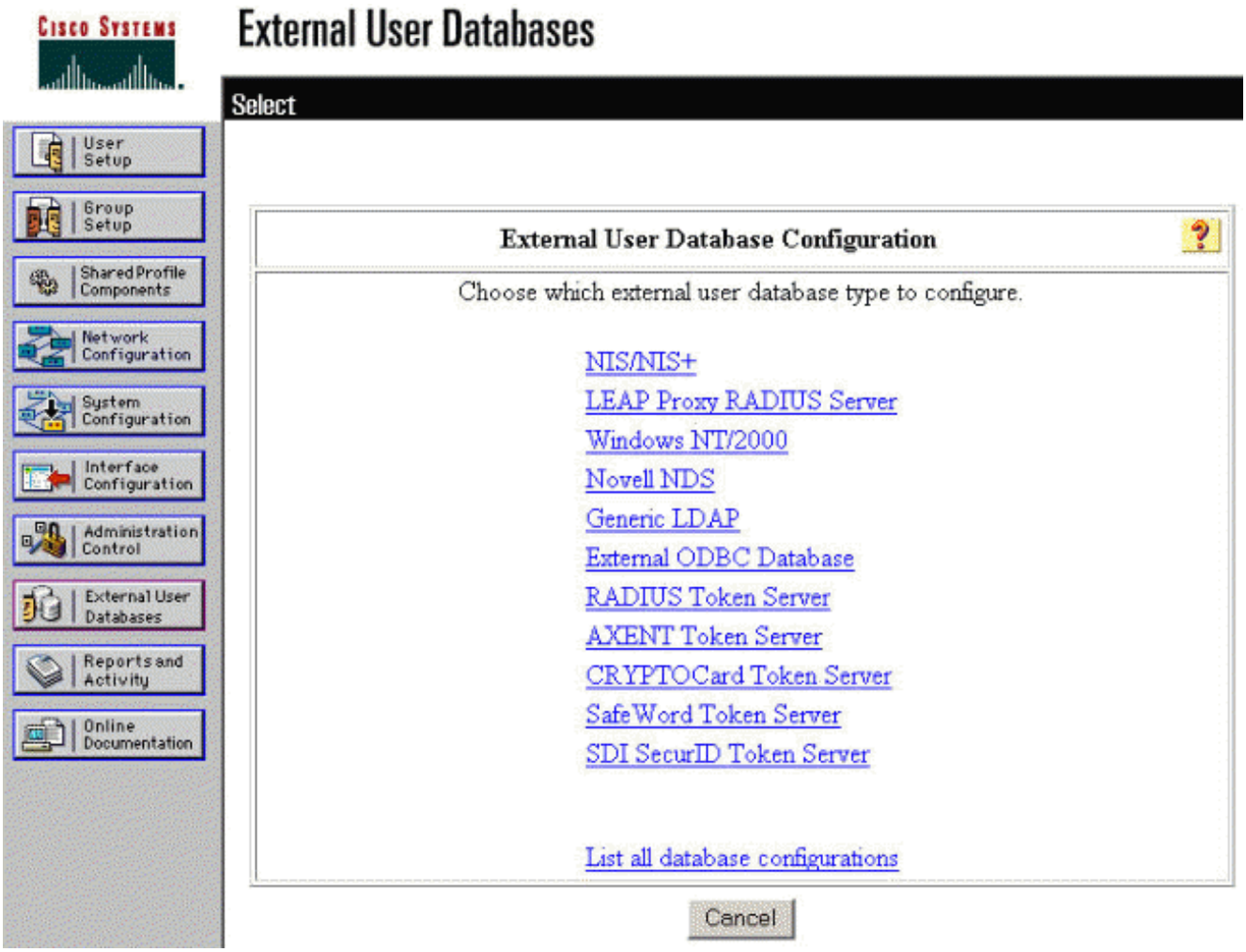


为 NT 域验证配置未知用户策略

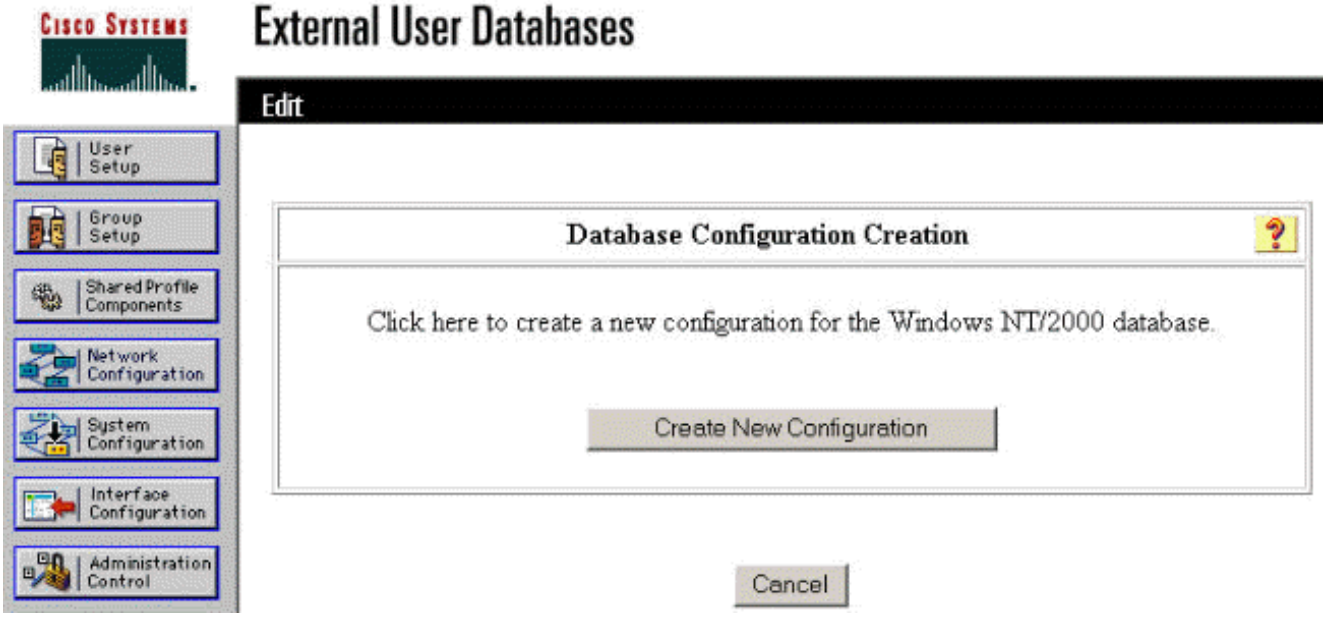
1. 要配置在RADIUS服务器的用户认证作为未知用户策略的部分，请点击**外部用户数据库**在左面板中，然后点击**数据库配置的**链路。



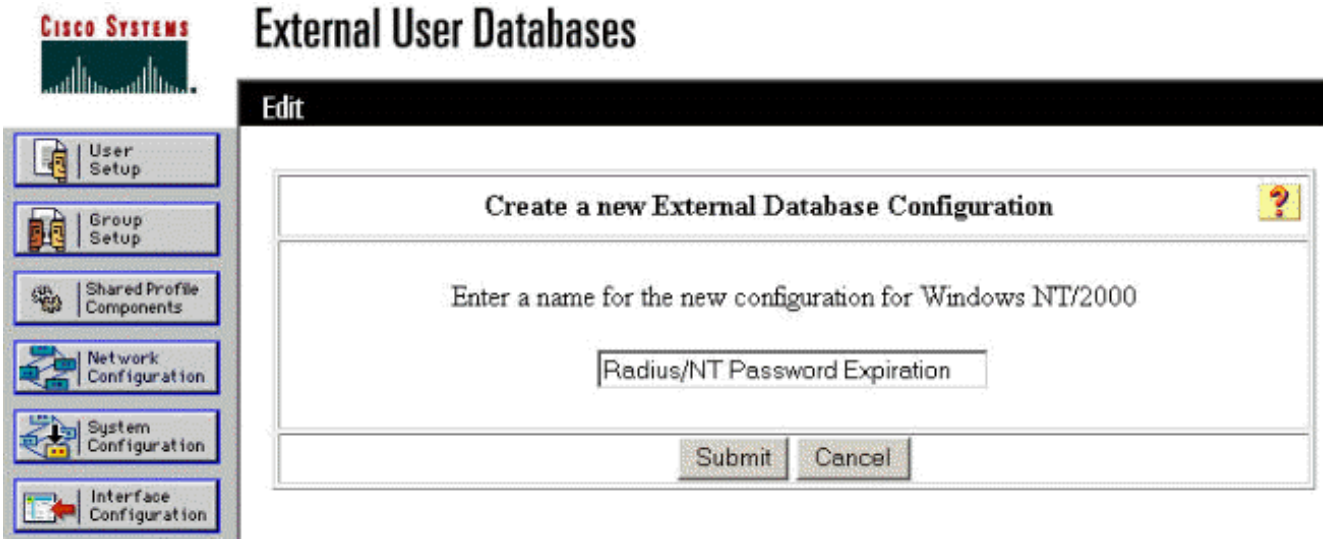
2. 在“外部用户数据库配置下”，请点击**Windows NT/2000**。



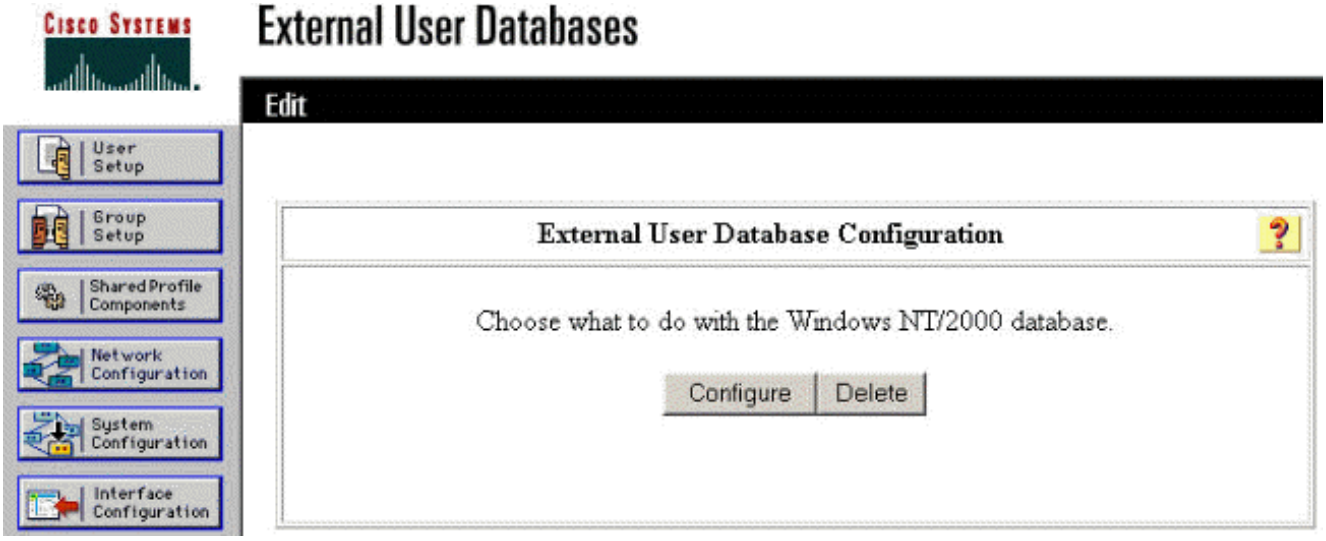
3. 在“数据库配置创建”屏幕，请单击**创建新的配置**。



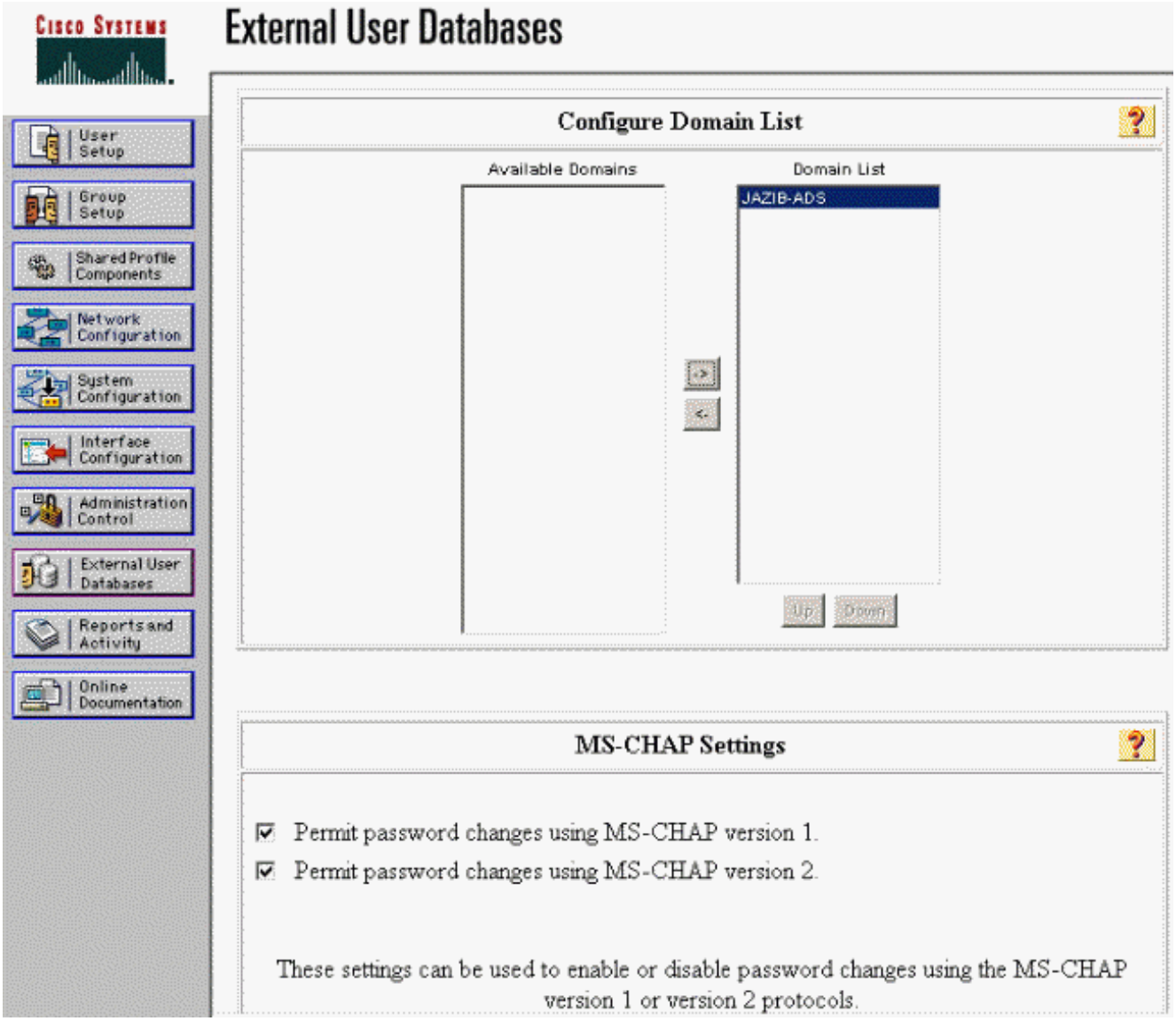
4. 当提示，请键入一名称对于NT/2000验证并且单击**提交**。下面的示例显示命名“Radius/NT密码到期”。



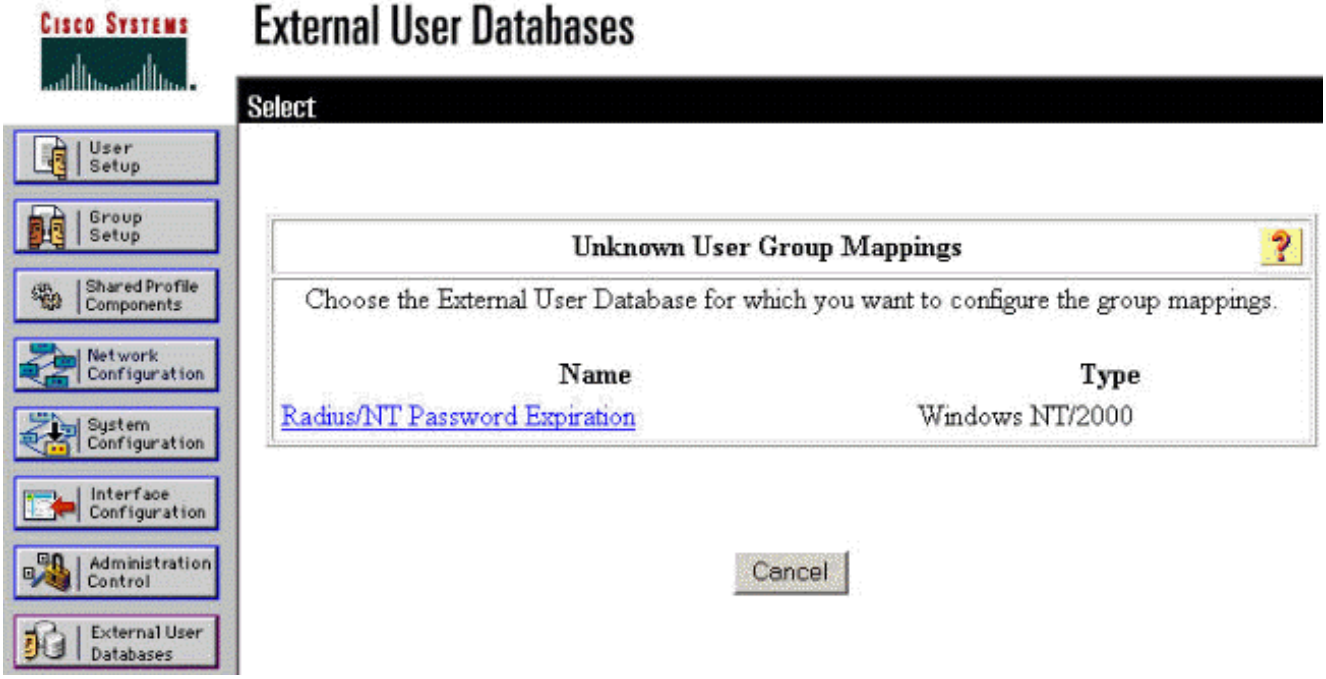
5. 单击**配置**配置用户认证的域名。



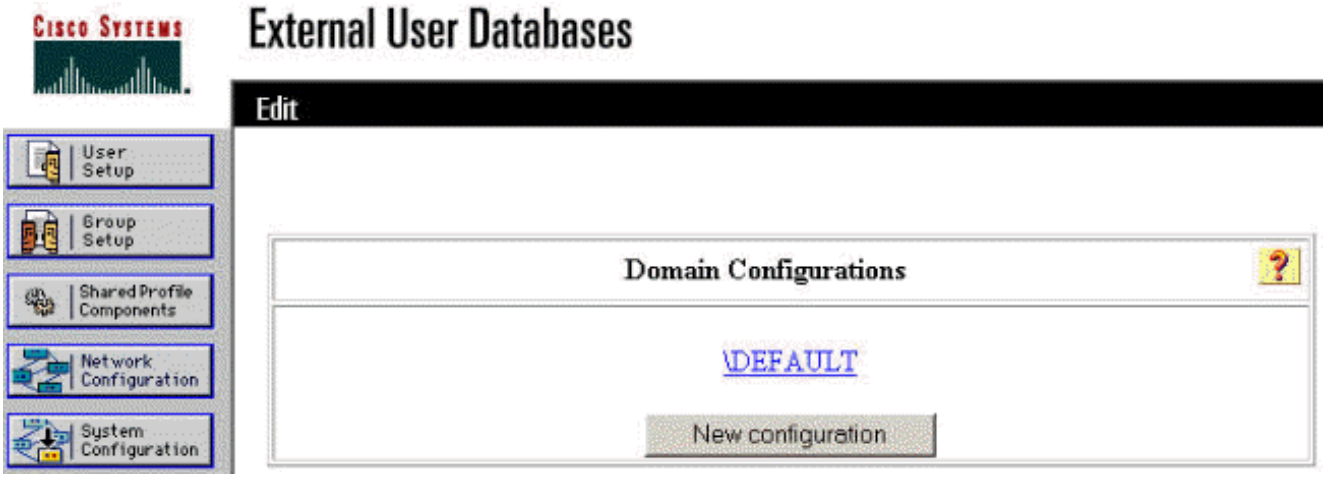
6. 选择您的从“可用的域的NT域”，然后单击右箭头按钮添加它对“域列表”。在“MS-CHAP设置下”，请保证**Permit密码更改使用MS-CHAP版本1和版本2的**选项选择。完成后，单击 **Submit**。



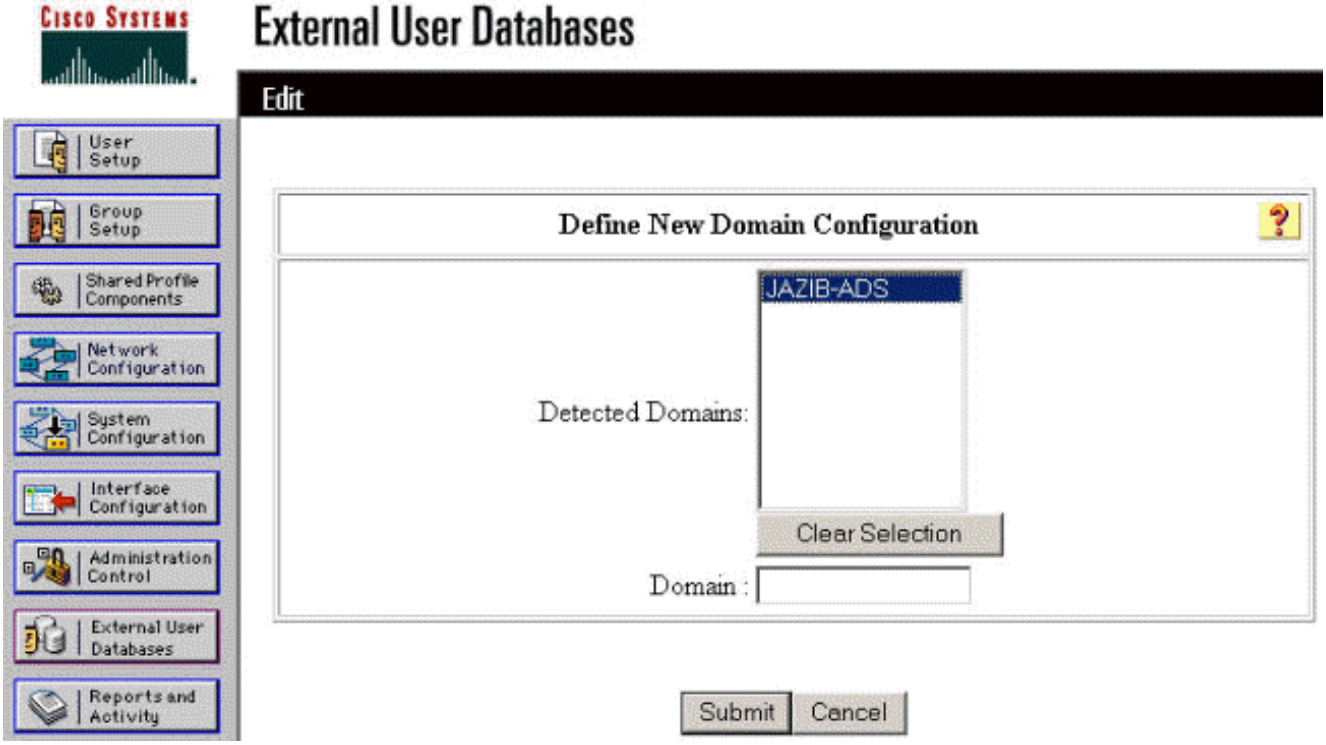
7. 点击**外部用户数据库**在左面板中，然后点击**数据库组映射的**链路(如在此示例中看到)。您应该为您的以前已配置的外部数据库看到条目。下面的示例显示“Radius/NT密码到期的一个条目”，该的数据库我们配置。



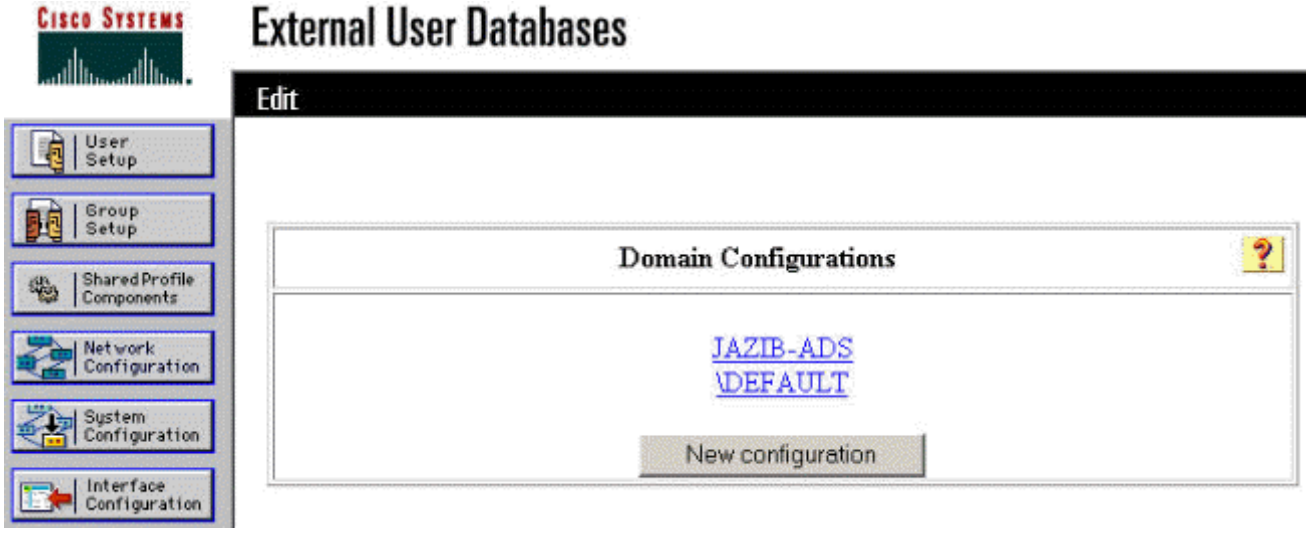
8. 在“域配置”请筛选，点击**新的配置**添加域配置。



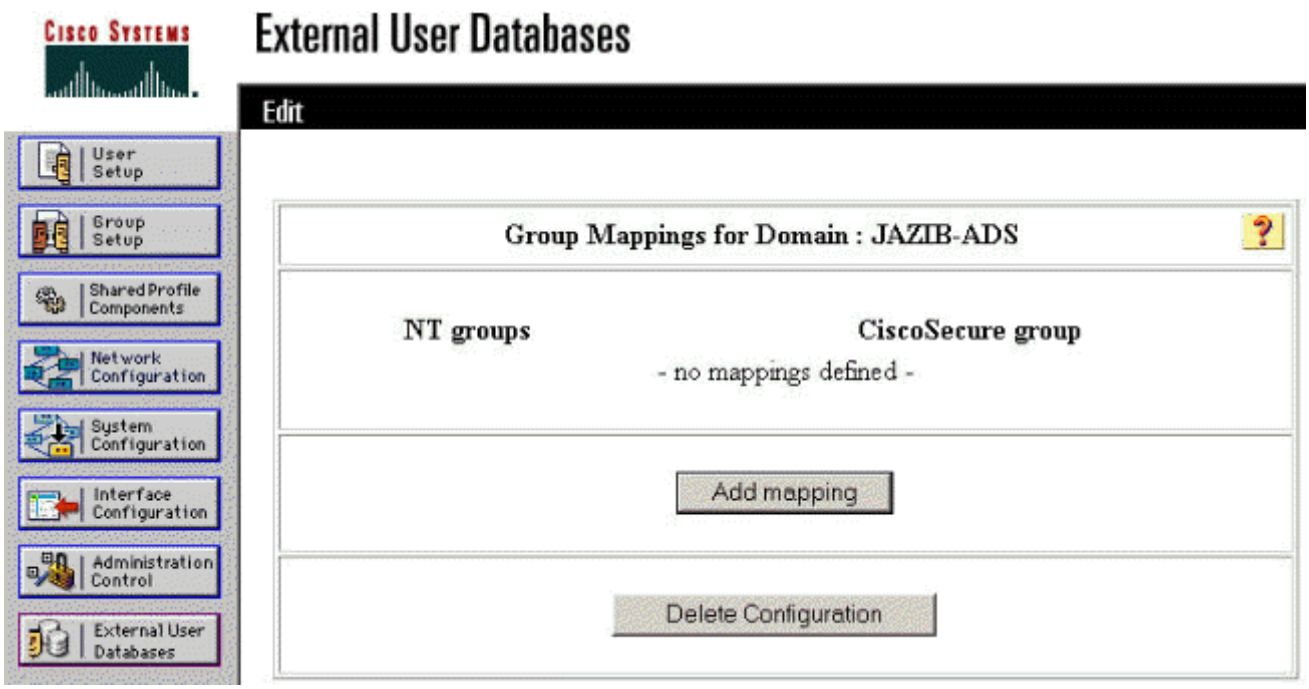
9. 选择您的从“检测的域”列表的域并且单击**提交**。下面的示例显示名为“JAZIB-ADS的域”。



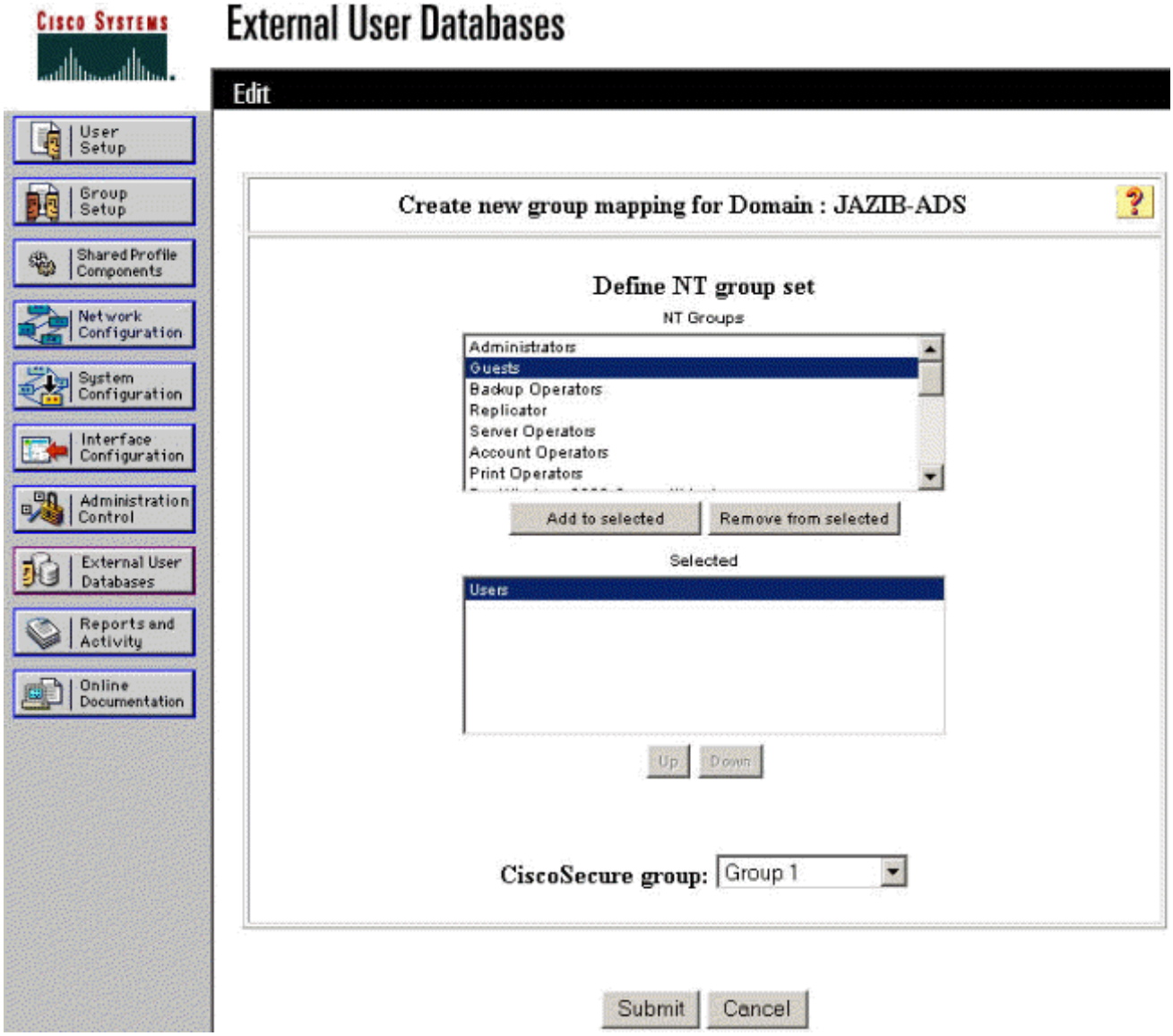
10. 点击您的域名配置组映射。此示例显示域“JAZIB-ADS”。



11. 单击**添加映射**定义组映射。

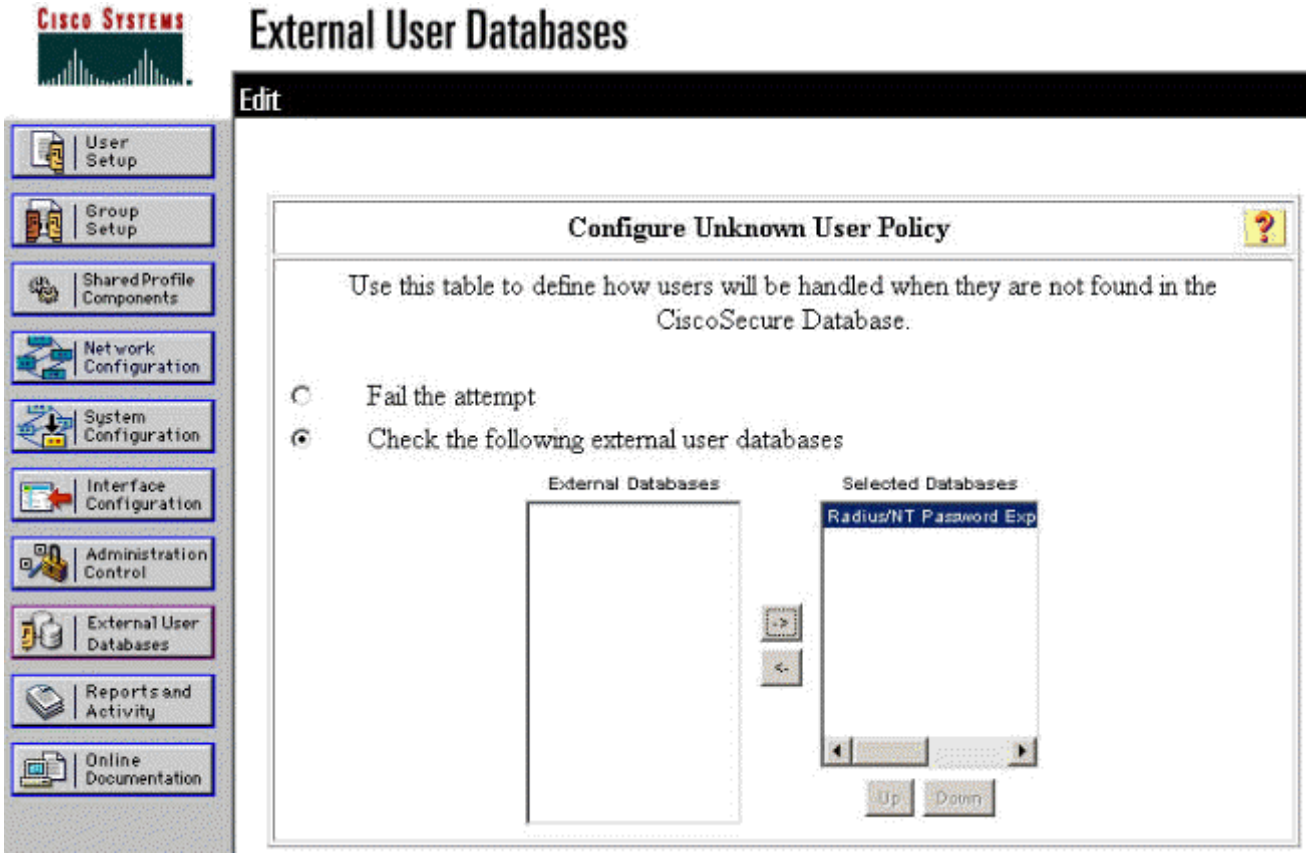


12. 在“创建新的组映射”屏幕，映射NT域的组给CSNT RADIUS服务器的一组，然后单击**提交**。示例下面的地图NT组“用户” RADIUS组的“组1."



13. 点击**外部用户数据库**在左面板中，然后点击**未知用户策略的**链路(如在此示例中看到)。确保**检查的**选项**以下外部用户数据库**选择。点击右箭头按钮移动从“外部数据库”列表的以前已配置的

外部数据库向“所选的数据库列表”。

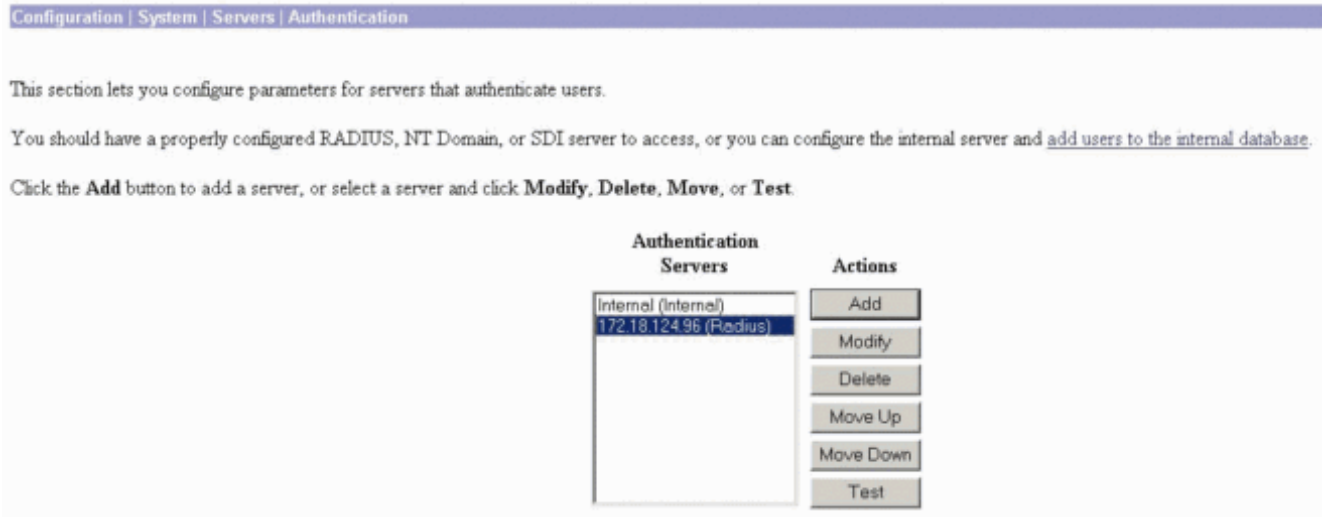


测试 NT/RADIUS密码到期功能

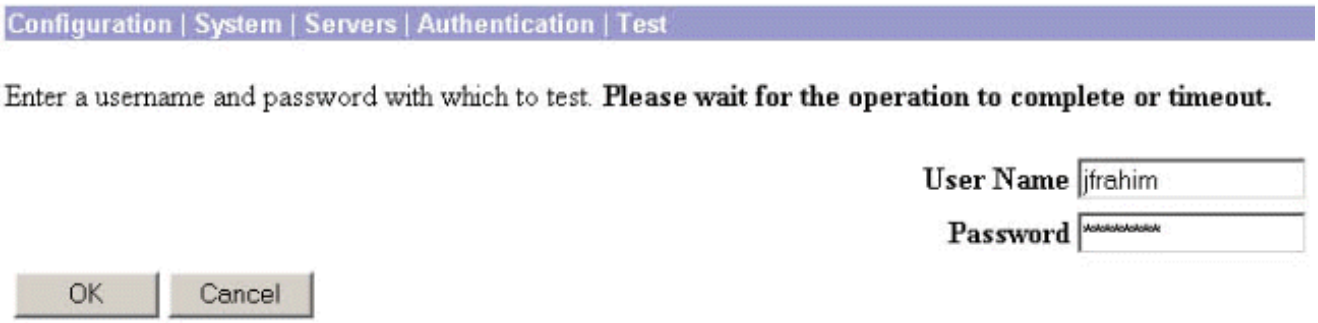
集中器提供功能测试RADIUS验证。要正确测试此功能，请确保您仔细遵从这些步骤。

测试 RADIUS 验证

1. 去**Configuration > System > Servers > Authentication**。选择您的RADIUS服务器并且点击**测验**。



2. 当提示，请键入您的NT域用户名和密码，然后点击OK键。下面的示例显示用户名“在有"cisco123"的NT域服务器”配置的jfrahim作为密码。

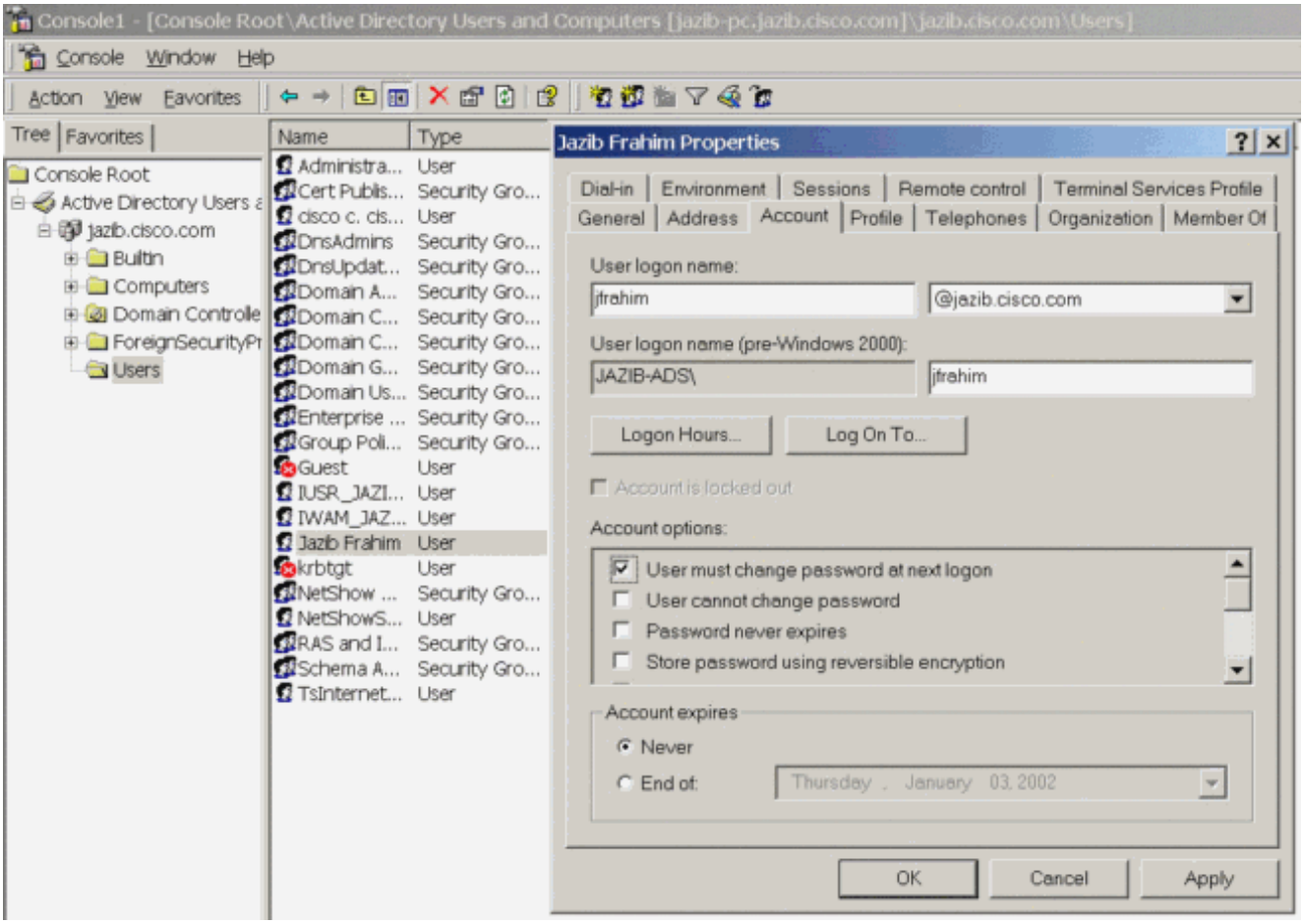


3. 如果您的验证适当地设置，您应该收到消息陈述“验证成功”。

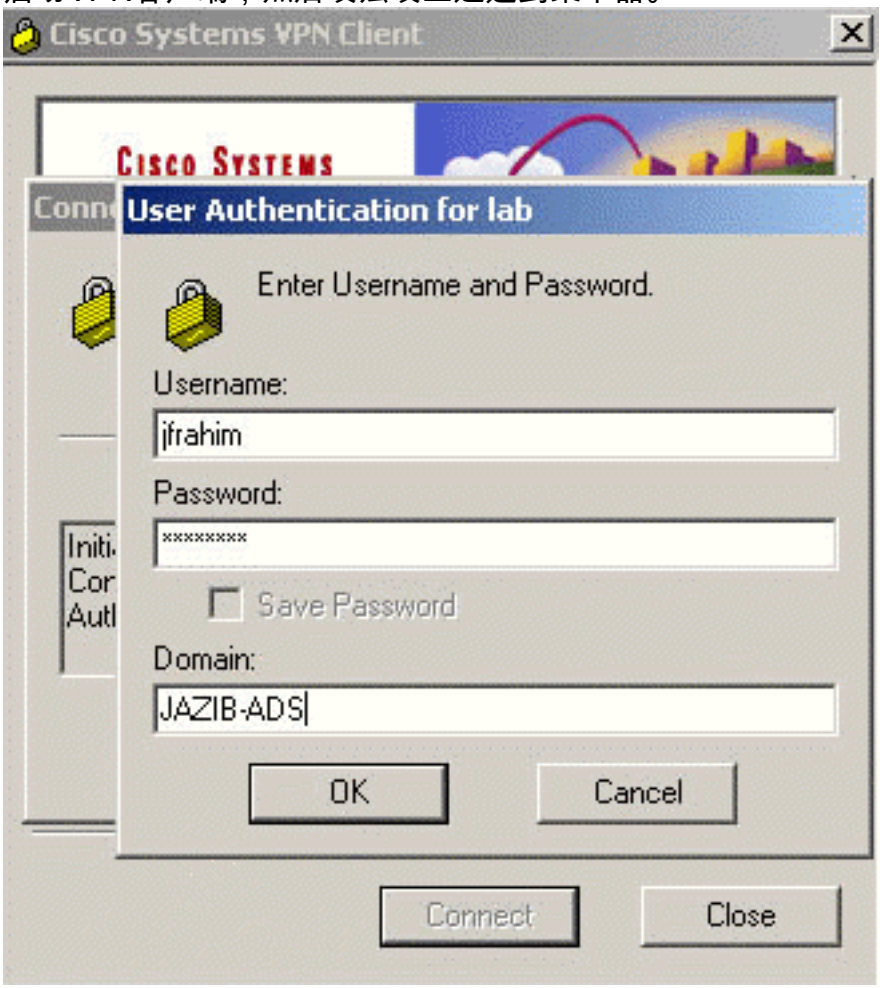
如果收到任何消息除显示的那个之外如上，有某个配置或连接问题。请重复在本文和测试的步骤略述的配置保证所有设置适当地做。并且请检查在您的设备之间的IP连通性。

使用 RADIUS 代理测试密码到期功能时的实际的 NT 域验证

1. 如果用户在域服务器已经定义，请修改属性，以便将提示用户更改密码在下登录。去用户的Properties对话框的“帐户”选项卡，选择**用户的**选项**必须更改密码在下登录**，然后点击OK键。



2. 启动VPN客户端，然后设法设立通道到集中器。



3. 在用户认证时，应该提示您更改密码。

相关信息

- Cisco VPN 3000 系列集中器
- IPsec
- 用于 Windows 的 Cisco 安全访问控制服务器
- RADIUS
- 请求注解 (RFC)