目录

简介

通过无客户端 SSL VPN (WebVPN)，用户可以使用启用了 SSL 的 Web 浏览器从任意位置安全地访问公司 LAN 中的资源。用户首先使用 WebVPN 网关进行身份验证，然后通过该网关，用户可以访问预先配置的网络资源。Webvpn gateway在Cisco IOS路由器、思科可适应安全工具(ASA)，Cisco VPN 3000集中器和思科WebVPN服务模块可以配置Catalyst 6500及7600路由器的。

可以采用以下三种主要模式在 Cisco 设备上配置安全套接字层 (SSL) 虚拟专用网络 (VPN) 技术：无客户端 SSL VPN (WebVPN)、瘦客户端 SSL VPN（端口转发）和 SSL VPN 客户端 (SVC) 模式。本文档演示如何在 Cisco IOS 路由器上配置 WebVPN。

注意： 请勿更改路由器的 IP 域名或主机名，这将触发重新生成自签名证书，并且将覆盖已配置的信任点。如果已针对 WebVPN 对路由器进行了配置，重新生成自签名证书会导致连接问题。WebVPN 将 SSL 信任点名称与 WebVPN 网关配置绑定在一起。因此，如果颁发了新的自签名证书，则新的信任点名称将与 WebVPN 配置不匹配，从而使用户无法连接。

注意： 如果在使用永久性自签名证书的 WebVPN 路由器上运行 **ip https-secure server** 命令，将生成一个新的 RSA 密钥，并且证书将变为无效证书。系统将创建一个新的信任点，这会中断 SSL WebVPN。如果在运行 **ip https-secure server** 命令之后重新启动使用永久性自签名证书的路由器，将出现相同问题。

要了解有关瘦客户端 SSL VPN 的详细信息，请参阅使用 SDM 的瘦客户端 SSL VPN (WebVPN) IOS 配置示例。

要了解有关 SSL VPN 客户端的详细信息，请参阅在 IOS 上使用 SDM 配置 SSL VPN 客户端 (SVC) 的示例。

SSL VPN 在以下 Cisco 路由器平台上运行：

- Cisco 870、1811、1841、2801、2811、2821 和 2851 系列路由器
- Cisco 3725、3745、3825、3845、7200 和 7301 系列路由器

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- Cisco IOS 软件版本 12.4(6)T 或更高版本的高级映像
- 简介中列出的 Cisco 路由器平台之一

使用的组件

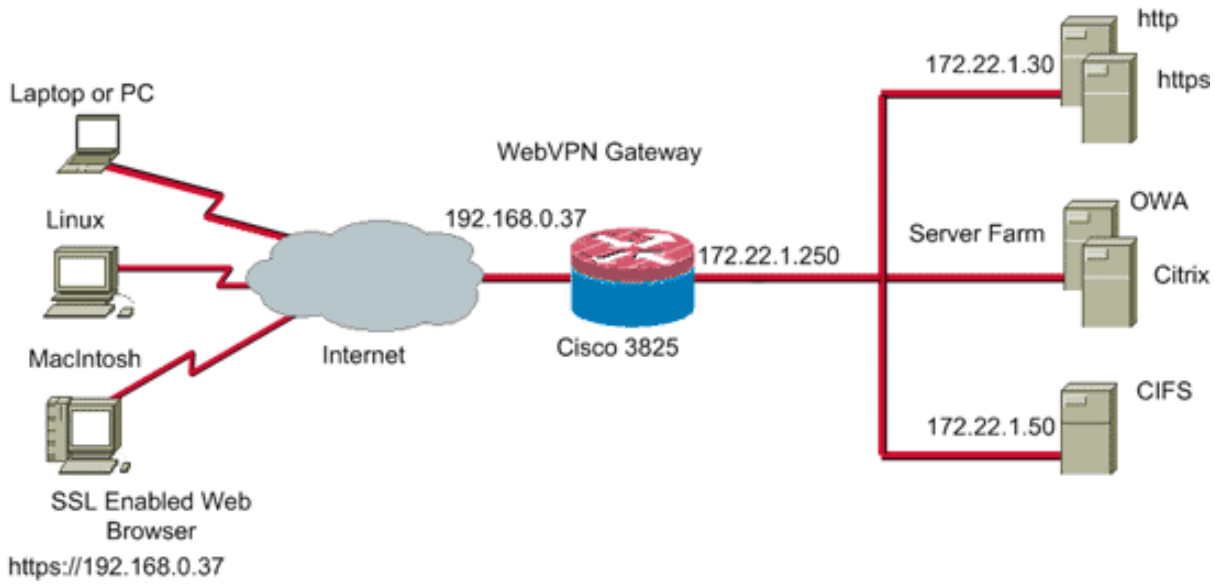
本文档中的信息基于以下软件和硬件版本：

- Cisco 3825 路由器
- 高级企业软件映像 - Cisco IOS 软件版本 12.4(9)T
- Cisco Router and Security Device Manager (SDM) - 版本 2.3.1

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。本示例中使用的 IP 地址摘自 RFC 1918 地址，这些地址是专用地址，不能在 Internet 上合法地使用。

网络图

本文档使用以下网络设置：



规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置前的任务

开始之前，请完成以下这些任务：

1. 配置主机名和域名。
2. 为路由器配置 SDM。Cisco 提供了一些带有 SDM 的预安装副本的路由器。如果尚未在路由器上加载 Cisco SDM，您可以从软件下载（仅限注册用户）获取该软件的免费副本。您必须拥有一个已签署服务合同的 CCO 帐户。有关安装和配置 SDM 的详细信息，请参阅 Cisco Router and Security Device Manager。
3. 为路由器配置正确的日期、时间和时区。

在 Cisco IOS 上配置 WebVPN

一个设备可以与多个 WebVPN 网关相关联。每个 WebVPN 网关只能与路由器上的一个 IP 相连。可以为特定 WebVPN 网关创建多个 WebVPN 上下文。要标识各上下文，请为每个上下文提供一个唯一的名称。一个策略组只能与一个 WebVPN 上下文相关联。策略组描述特定 WebVPN 上下文中的可用资源。

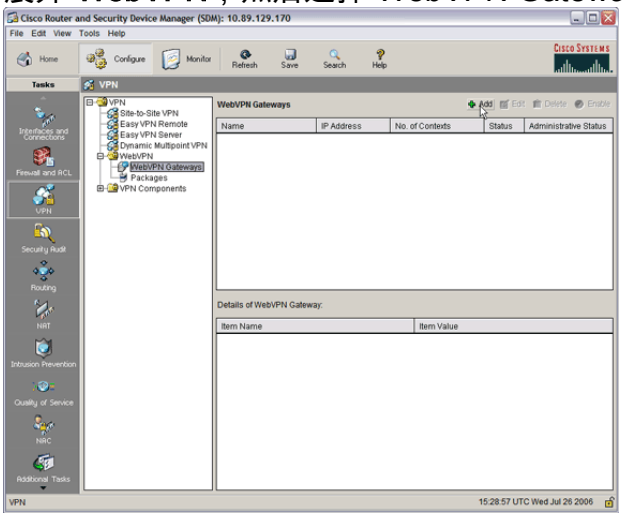
要在 Cisco IOS 上配置 WebVPN，请完成以下步骤：

1. 配置 WebVPN 网关
2. 配置策略组允许的资源
3. 配置 WebVPN 策略组并选择资源
4. 配置 WebVPN 上下文
5. 配置用户数据库和身份验证方法

步骤 1. 配置 WebVPN 网关

要配置 WebVPN 网关，请完成以下步骤：

1. 在 SDM 应用程序中，单击 **Configure**，然后单击 VPN。
2. 展开 **WebVPN**，然后选择 WebVPN Gateways。



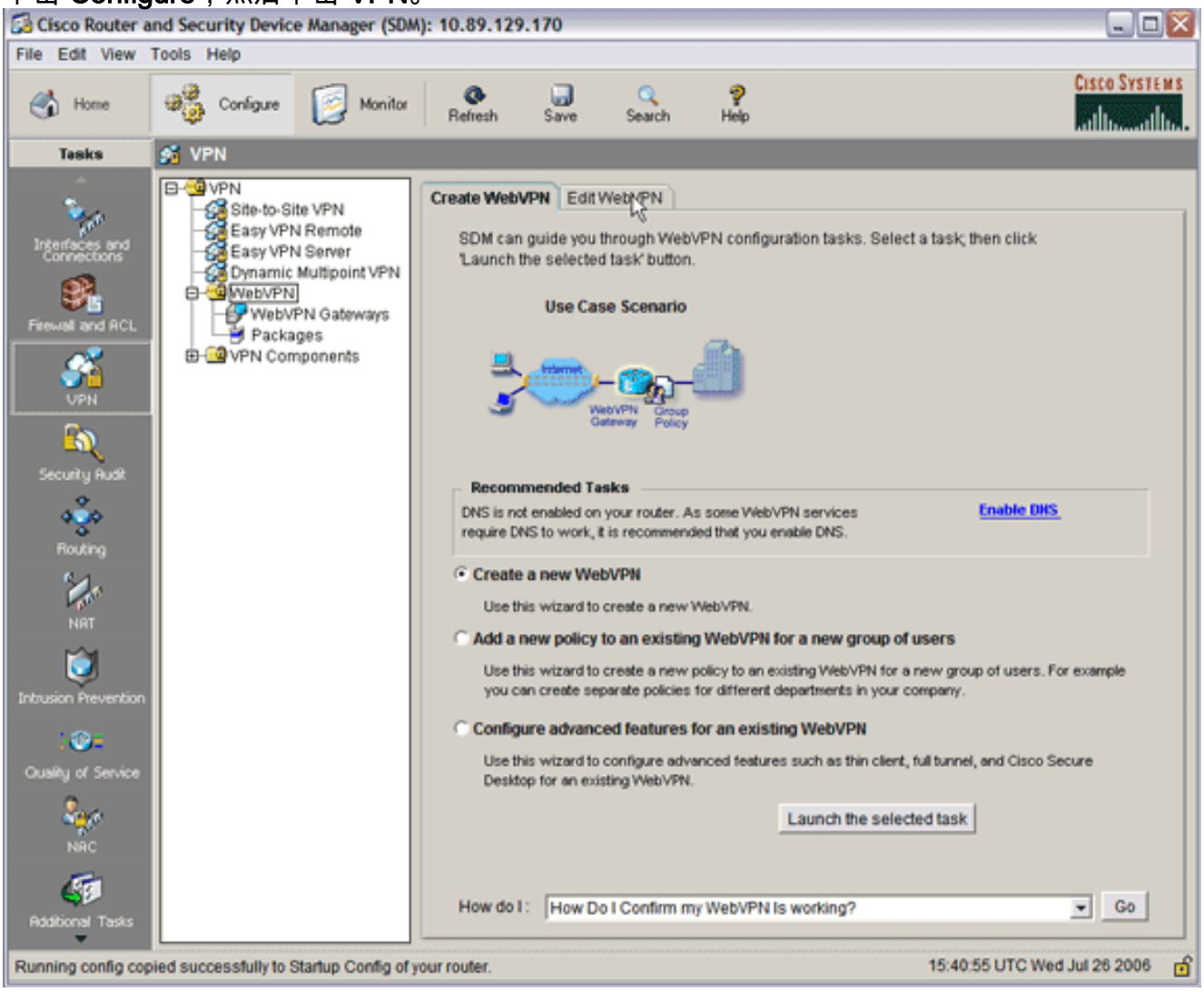
3. 单击 **Add**。此时将显示 Add WebVPN Gateway 对话框。
4. 在 Gateway Name 和 IP Address 字段中输入相应值，然后选中 **Enable Gateway** 复选框。
5. 选中 **Redirect HTTP Traffic** 复选框，然后单击 OK。
6. 单击 **Save**，然后单击 **Yes** 接受更改。

步骤 2. 配置策略组允许的资源

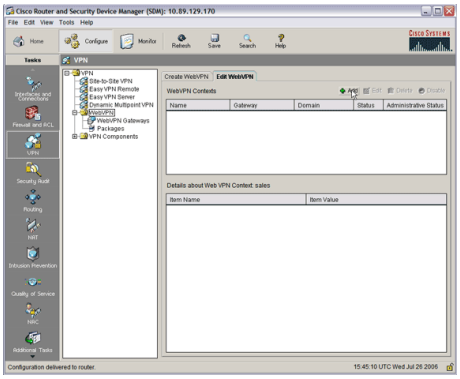
为了便于向策略组添加资源，可以在创建策略组之前先配置资源。

要配置策略组允许的资源，请完成以下步骤：

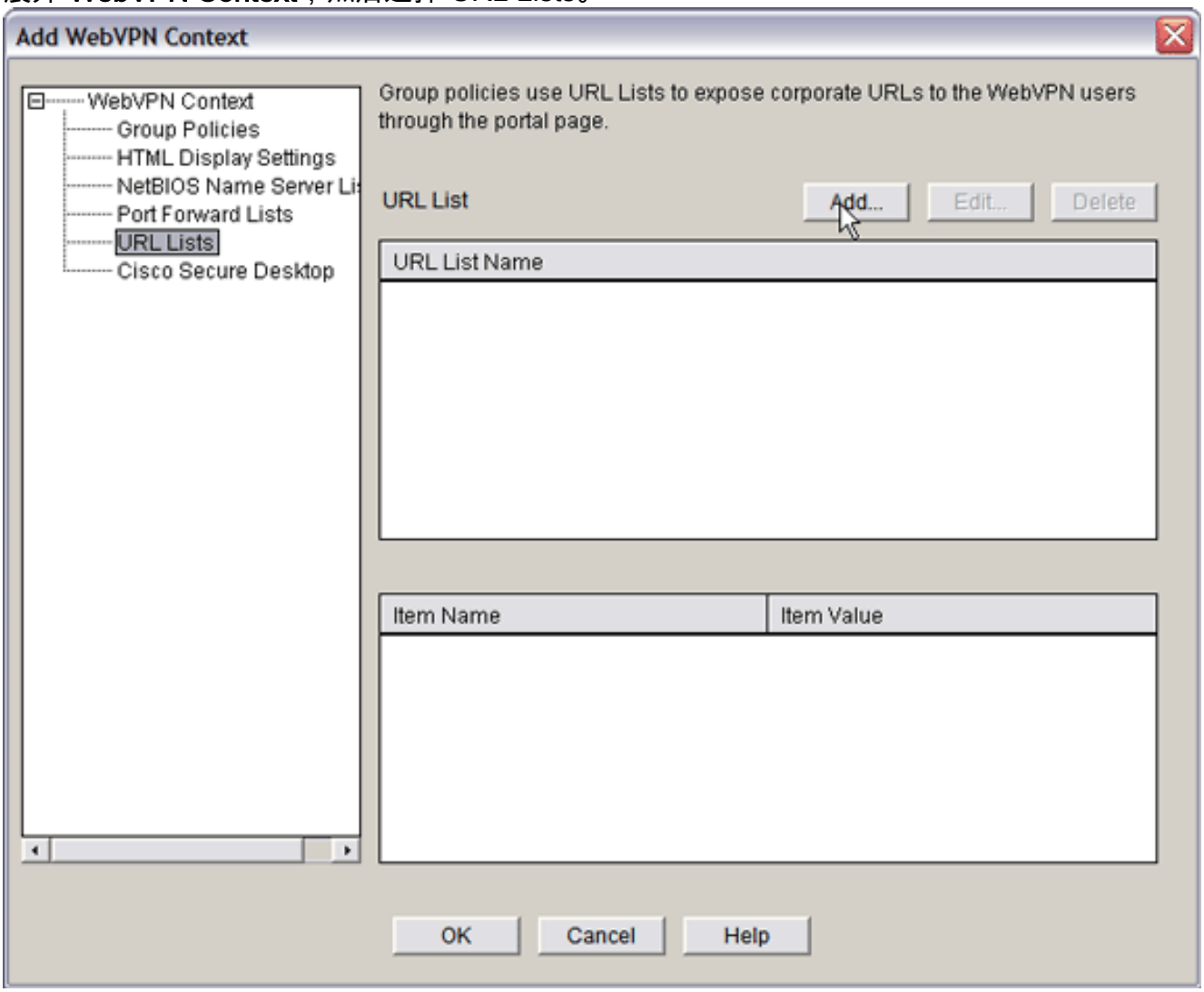
1. 单击 **Configure**，然后单击 **VPN**。



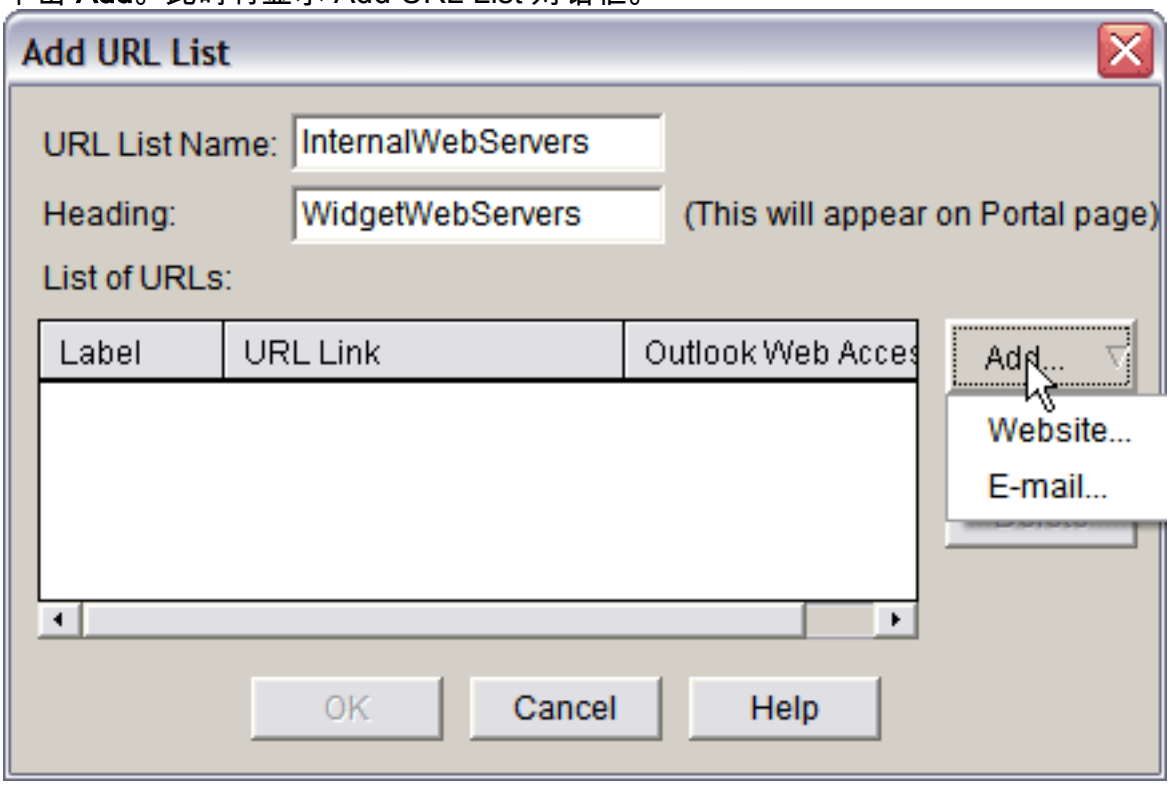
2. 选择 **WebVPN**，然后单击 Edit WebVPN 选项卡。**注意：** WebVPN 允许您配置对 HTTP、HTTPS、通过公用 Internet 文件系统 (CIFS) 协议浏览的 Windows 文件以及 Citrix 的访问。



3. 单击 **Add**。此时将显示 Add WebVPN Context 对话框。
4. 展开 **WebVPN Context**，然后选择 URL Lists。

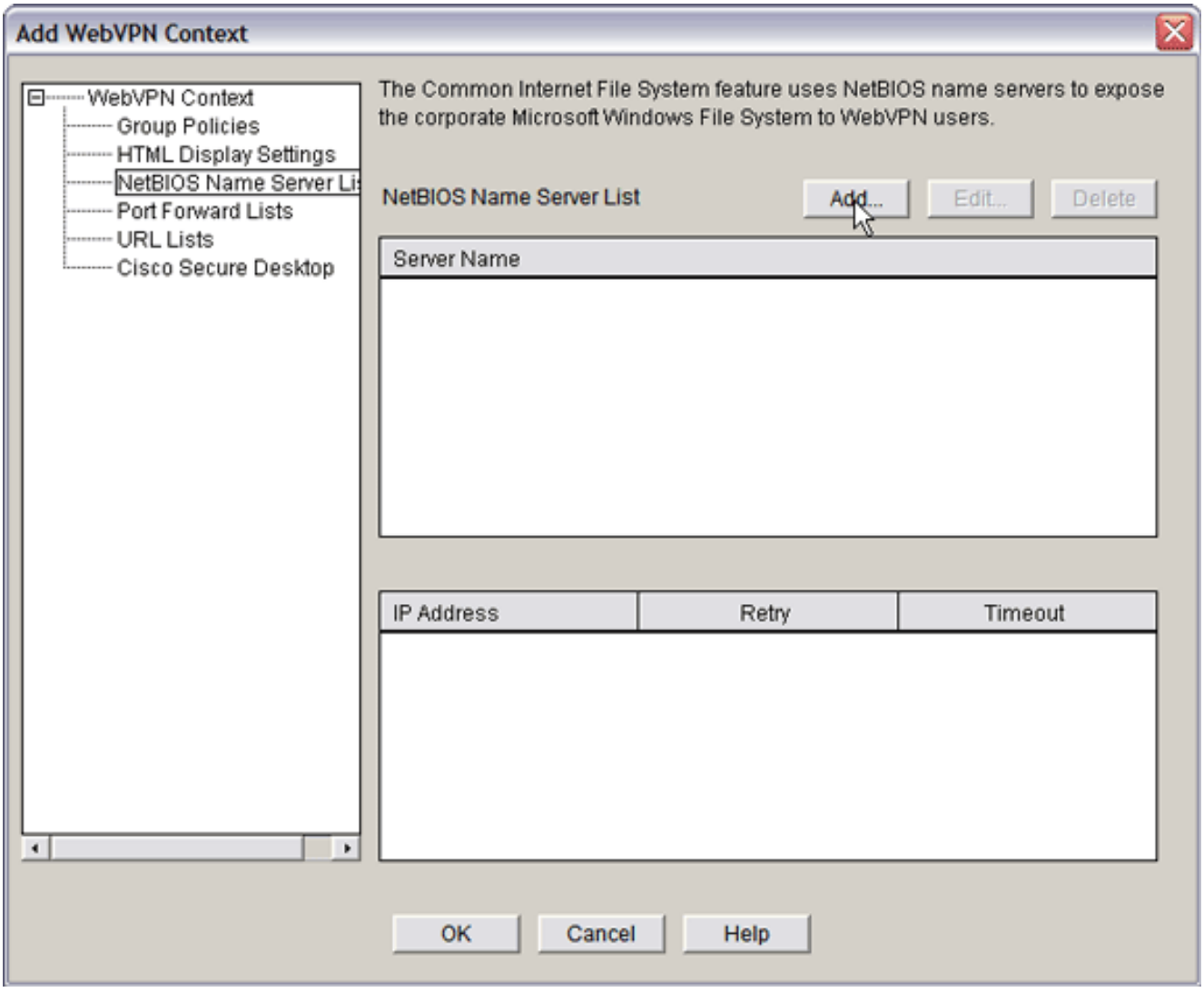


5. 单击 **Add**。此时将显示 Add URL List 对话框。

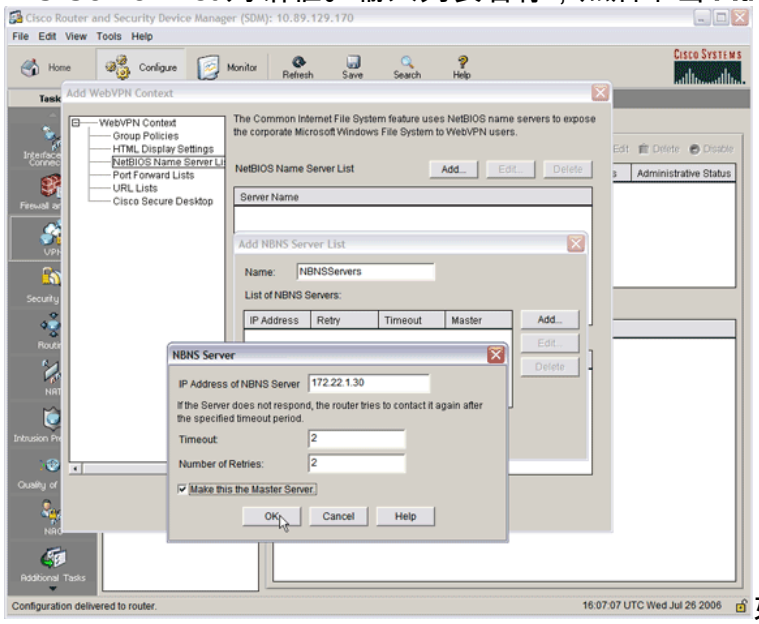


6. 在 URL List Name 和 Heading 字段中输入相应值。

7. 单击 **Add**，然后选择 Website。此列表包含要用于此 WebVPN 连接的所有 HTTP 和 HTTPS Web 服务器。
8. 要添加对 Outlook Web Access (OWA) 的访问，请单击 **Add**，选择 E-mail，然后在填写所有所需字段之后单击 OK。
9. 为了支持通过 CIFS 浏览的 Windows 文件，可以指定 NetBIOS 名称服务 (NBNS) 服务器，并在 Windows 域中按顺序配置相应共享。从 WebVPN Context 列表中，选择 **NetBIOS Name Server Lists**。



单击 **Add**。此时将显示 Add NBNS Server List 对话框。输入列表名称，然后单击 **Add**。此时将显示 NBNS Server 对话框。



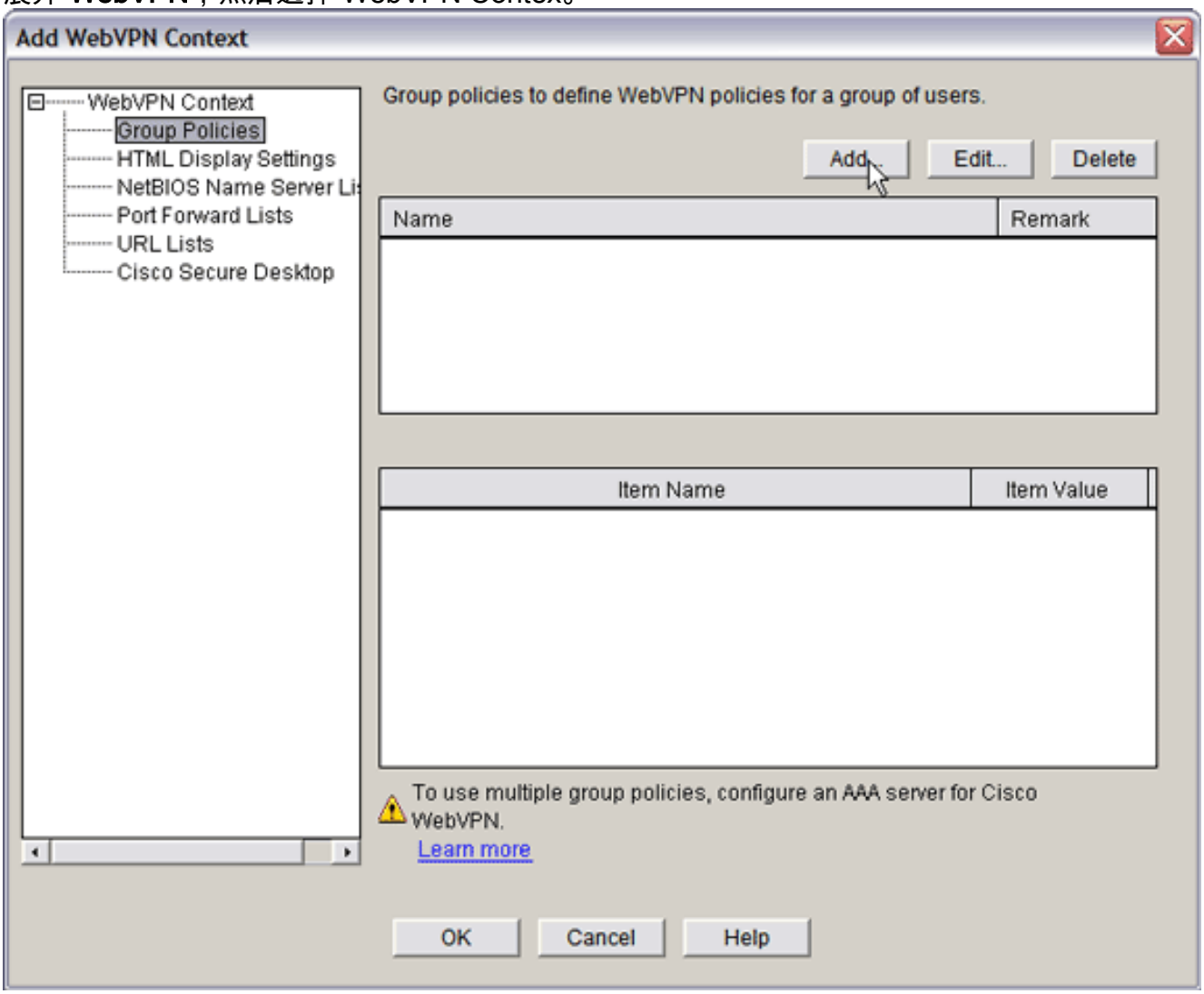
如果适用

，请选中 **Make This the Master Server** 复选框。单击 **OK**，再单击 **OK**。

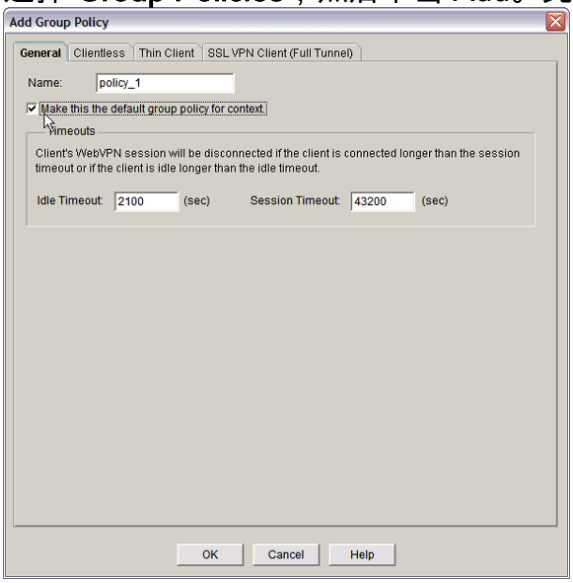
步骤 3. 配置 WebVPN 策略组并选择资源

要配置 WebVPN 策略组并选择资源，请完成以下步骤：

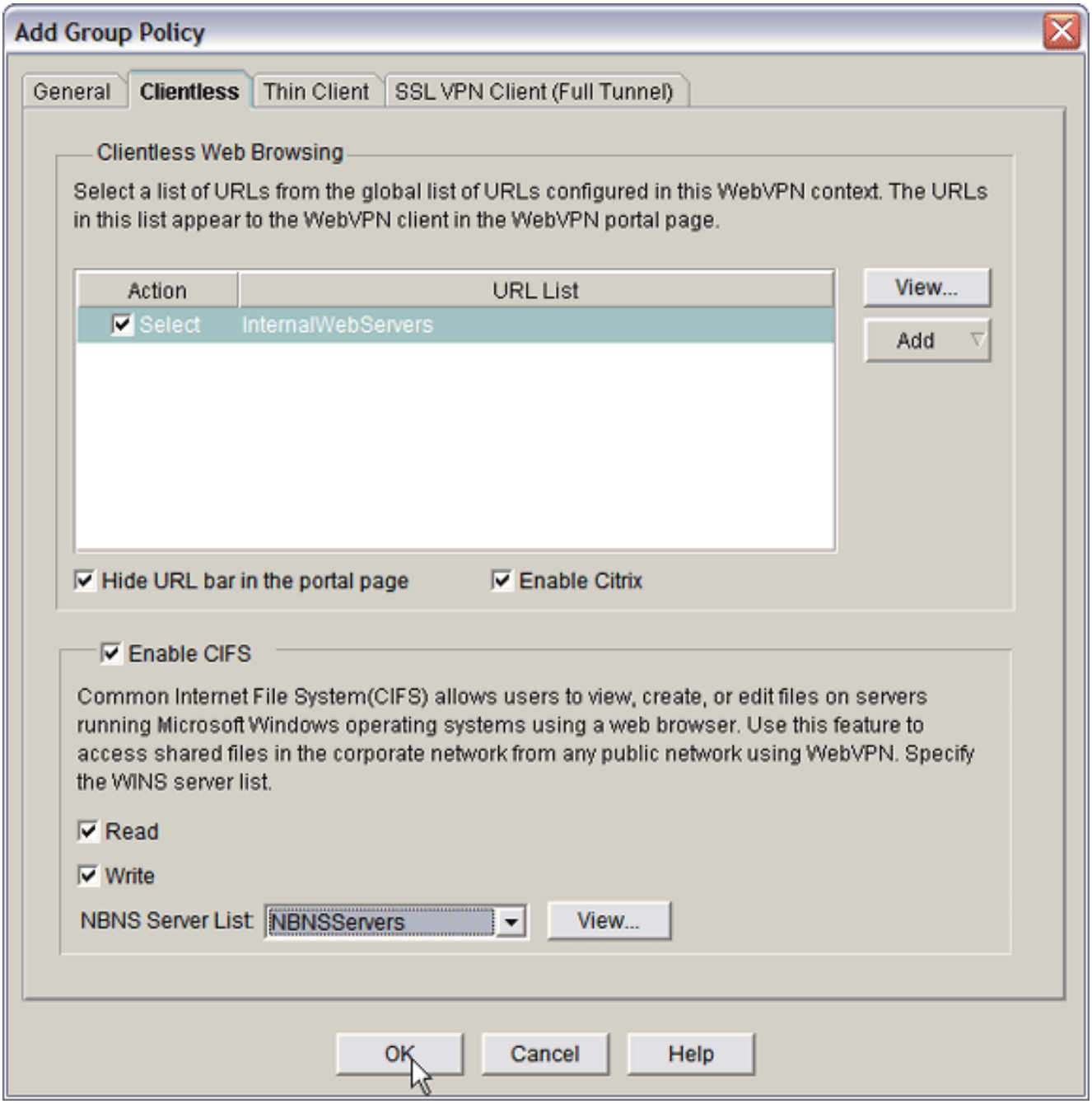
1. 单击 **Configure**，然后单击 **VPN**。
2. 展开 **WebVPN**，然后选择 WebVPN Contex。



3. 选择 **Group Policies**，然后单击 Add。此时将显示 Add Group Policy 对话框。



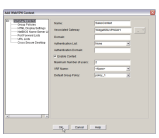
4. 输入新策略的名称，然后选中 **Make this the default group policy for context** 复选框。
5. 单击位于对话框顶部的 **Clientless** 选项卡。



6. 选中所需 URL List 对应的 **Select** 复选框。
7. 如果您的用户使用需要访问 Citrix 服务器的 Citrix 客户端，请选中 **Enable Citrix** 复选框。
8. 选中 **Enable CIFS**、Read 和 Write 复选框。
9. 单击 **NBNS Server List** 下拉箭头，并选择在步骤 2. 中为 Windows 文件浏览创建的 NBNS 服务器列表。
10. 单击 **Ok**。

步骤 4. 配置 WebVPN 上下文

要将 WebVPN 网关、组策略和资源链接在一起，必须配置 WebVPN 上下文。**要配置 WebVPN 上下文，请完成以下步骤：**

1. 选择 **WebVPN Context**，然后输入上下文的名称。 

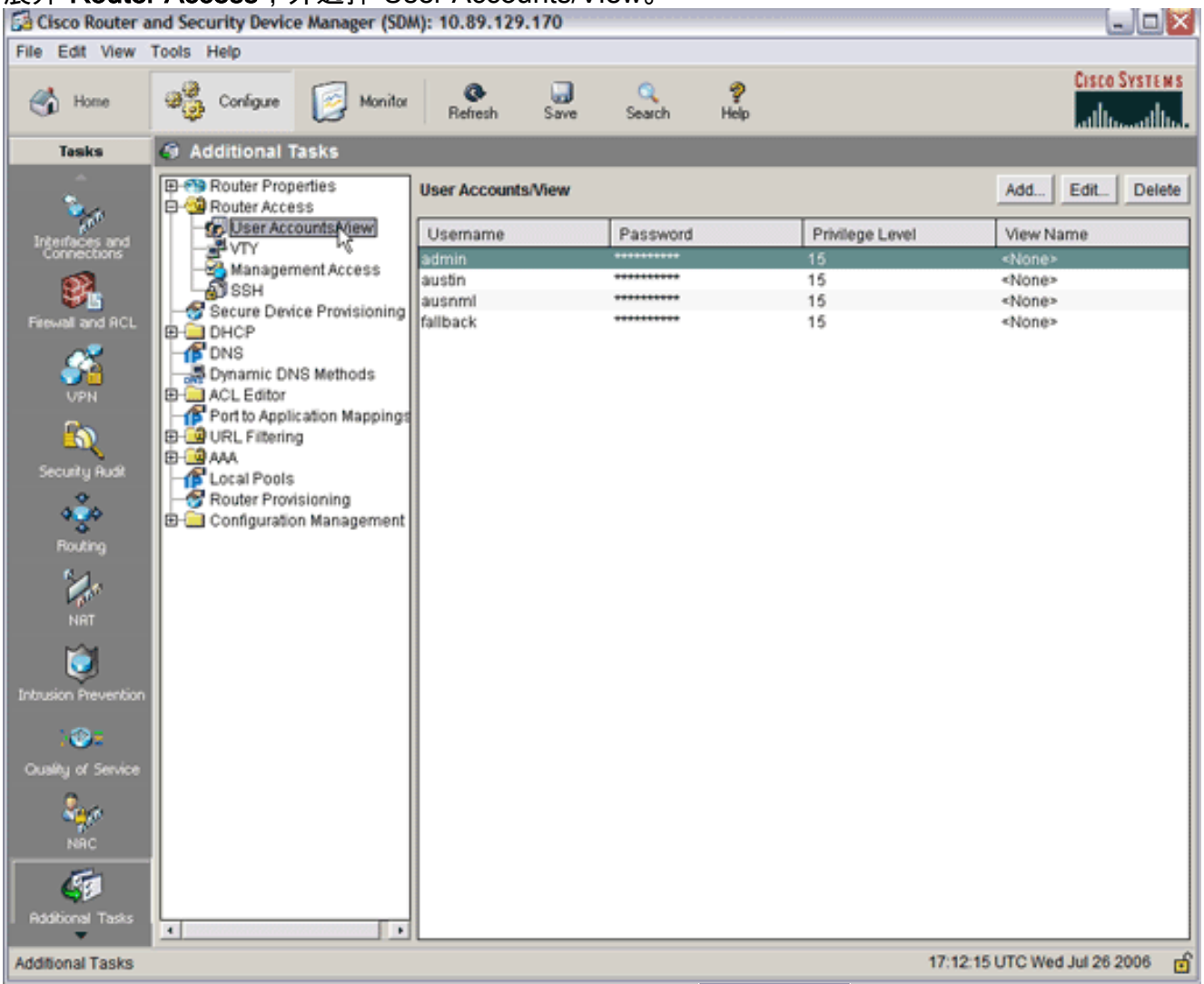
2. 单击 Associated Gateway 下拉箭头，并选择一个关联的网关。
3. 如果打算创建多个上下文，请在 Domain 字段中输入一个唯一的名称以标识此上下文。如果将 Domain 字段保留为空，用户必须使用 **https://IPAddress** 访问 WebVPN。如果输入了某个域名（如 *Sales*），用户必须使用 **https://IPAddress/Sales** 进行连接。
4. 选中 **Enable Context** 复选框。
5. 在 Maximum Number of Users 字段中，输入设备许可证允许的最大用户数。
6. 单击 **Default Group Policy** 下拉箭头，并选择与此上下文关联的组策略。
7. 单击 **OK**，再单击 **OK**。

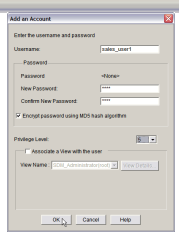
步骤 5. 配置用户数据库和身份验证方法

可以配置无客户端 SSL VPN (WebVPN) 会话，以便使用 Radius、Cisco AAA 服务器或本地数据库进行身份验证。本示例使用一个本地数据库。

要配置用户数据库和身份验证方法，请完成以下步骤：

1. 单击 **Configuration**，然后单击 Additional Tasks。
2. 展开 **Router Access**，并选择 User Accounts/View。



3. 单击 **Add** 按钮。此时将显示 Add an Account 对话框。 

4. 输入用户帐户和口令。
5. 单击 **OK**，再单击 **OK**。
6. 单击 **Save**，然后单击 **Yes** 接受更改。

结果

ASDM 创建了以下这些命令行配置：

```
ausnml-3825-01
```

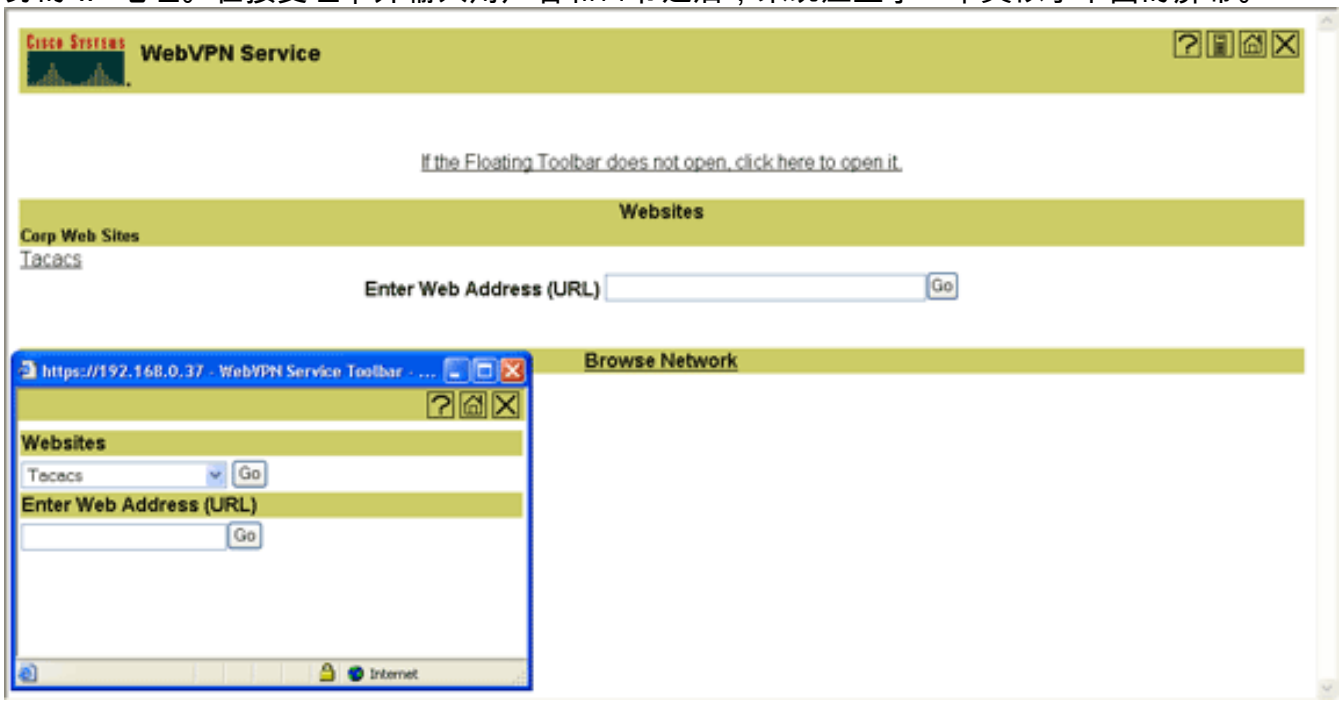
验证

使用本部分可确认配置能否正常运行。

步骤

要确认配置是否正常运行，请完成以下步骤：

- 以用户身份测试您的配置。在启用了 SSL 的 Web 浏览器中输入 **https://WebVPN_Gateway_IP_Address**；其中 *WebVPN_Gateway_IP_Address* 为 WebVPN 服务的 IP 地址。在接受证书并输入用户名和口令之后，系统应显示一个类似于下图的屏幕。



- 检查 SSL VPN 会话。在 SDM 应用程序中，单击 **Monitor** 按钮，然后单击 VPN Status。展开 **WebVPN (All Contexts)**，展开相应上下文，然后选择 Users。
- 检查错误消息。在 SDM 应用程序中，依次单击 **Monitor** 按钮、Logging 和 Syslog 选项卡。
- 查看服务的运行配置。在 SDM 应用程序中，单击 **Configure** 按钮，然后单击 Additional Tasks。展开 **Configuration Management**，并选择 Config Editor。

命令

有若干 **show** 命令与 WebVPN 关联。可以在命令行界面 (CLI) 上执行这些命令以显示统计信息和其他信息。有关 **show** 命令的详细信息，请参阅验证 WebVPN 配置。

注意： 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。

故障排除

使用本部分可排除配置故障。

注意： 请勿在复制期间中断 **Copy File to Server** 命令或导航到其他窗口。中断此操作可导致在服务器上保存的文件不完整。

注意： 用户可以使用 WebVPN 客户端上载和下载新的文件，但是不允许用户使用 **Copy File to Server** 命令在 WebVPN 上覆盖公用 Internet 文件系统中的文件。当用户尝试在服务器上替换某个文件时，用户将收到以下消息：

步骤

要排除配置故障，请完成以下步骤：

1. 确保客户端已禁用弹出窗口拦截器。
2. 确保客户端已启用 Cookie。
3. 确保客户端使用的是 Netscape、Internet Explorer、Firefox 或 Mozilla Web 浏览器。

命令

有若干 **debug** 命令与 WebVPN 关联。有关这些命令的详细信息，请参阅使用 WebVPN Debug 命令。

注意： 使用 **debug** 命令可能会对 Cisco 设备造成负面影响。使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- Cisco IOS SSLVPN
- Cisco IOS SSLVPN 问答
- 使用 SDM 的瘦客户端 SSL VPN (WebVPN) IOS 配置示例
- 在 IOS 上使用 SDM 配置 SSL VPN 客户端 (SVC) 的示例
- 技术支持和文档 - Cisco Systems