Cisco路由器作为使用SDM的远程VPN服务器配置示例

目录

简介

本文档介绍如何使用 Cisco Security Device Manager (SDM) 来配置 Cisco 路由器，以使其充当 Easy VPN 服务器。通过 Cisco SDM，您可以使用基于 Web 的简单易用管理界面将路由器配置为适用于 Cisco VPN 客户端的 VPN 服务器。完成 Cisco 路由器配置后，可以使用 Cisco VPN 客户端对其进行验证。

先决条件

要求

本文档假设 Cisco 路由器处于完全运行状态，并配置为允许使用 Cisco SDM 进行配置更改。

注意： 为了允许使用 SDM 配置路由器，请参阅允许 SDM 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：

- 配备 Cisco IOS® 软件版本 12.3(14T) 的 Cisco 3640 路由器
- Security Device Manager 2.31 版
- Cisco VPN 客户端 4.8 版

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

在本部分中，您将了解有关配置 Easy VPN 服务器功能的信息，该功能允许远程终端用户使用 IPsec 与任何 Cisco IOS® 网关通信。

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：

配置过程

要使用 SDM 将 Cisco 路由器配置为远程 VPN 服务器，请完成以下步骤：

1. 在主窗口中选择 **Configure > VPN > Easy VPN Server**，然后单击 **Launch Easy VPN Server Wizard**。
2. 开始配置 Easy VPN 服务器之前，必须先在路由器上启用 AAA。单击 **Yes** 继续配置。窗口中将显示“AAA has been successfully enabled on the router”消息。单击 **OK** 启动 Easy VPN 服务器配置。
3. 单击 **Next** 启动 Easy VPN Server Wizard。
4. 选择客户连接终端所在的接口和认证类型。
5. 单击 **Next to** 配置 Internet 密钥交换 (IKE) 策略，再用 **Add** 按钮创建新策略。隧道两端的配置必须完全一致。但 Cisco VPN 客户端会自动为自己选择正确的配置。因此，无需在客户端 PC 上执行 IKE 配置。
6. 单击 **Next to** 选择默认转换集或添加新转换集，以指定加密和认证算法。这种情况下，使用默认转换集。
7. 单击 **Next to** 为组策略查找创建新的认证、授权和记帐 (AAA) 授权网络方法列表，或选择用于组授权的现有网络方法列表。
8. 在 Easy VPN 服务器上配置用户认证。可在外部服务器（如 RADIUS 服务器）和/或本地数据库中存储用户认证详细信息。AAA 登录验证方法列表被使用，用于决定搜索用户验证详细信息的顺序。
9. 在此窗口中，您可以对本地数据库中的用户组策略执行添加、编辑、复制或删除操作。
10. 为“Tunnel Group Name”输入名称。提供适用于认证信息的预先共享密钥。创建新池或选择一个现有池，用于将 IP 地址分配到 VPN 客户端。
11. 此窗口显示您已执行操作的汇总。如果对配置感到满意，请单击 **Finish**。
12. SDM 将配置信息发送到路由器，以更新运行配置。单击 **OK** 完成操作。
13. 完成操作后，可以在需要时编辑和修改配置方面的变化。

验证

尝试使用 Cisco VPN 客户端连接到 Cisco 路由器，以验证是否已成功配置 Cisco 路由器。

1. 选择 **Connection Entries > New**。
2. 填写新连接的详细信息。Host 字段应包含 Easy VPN 服务器（Cisco 路由器）隧道端点的 IP

地址或主机名。组认证信息应与步骤 9 中使用的组认证信息对应。完成后单击 **Save** 。
3. 选择新创建的连接，然后单击 **Connect**。
4. 输入扩展认证 (Xauth) 的用户名和口令。此信息取决于步骤 7 中的 Xauth 参数。
5. 成功建立连接后，从“Status”菜单中选择 **Statistics** 以验证隧道的详细信息。此窗口显示数据流和加密信息：若对此窗口进行了配置，则将显示分割隧道信息：
6. 选择 **Log > Log Settings**，在 Cisco VPN 客户端中启用日志级别。
7. 选择 **Log > Log Windows** 查看 Cisco VPN 客户端中的日志项。

相关信息

- 下载并安装 Cisco Router and Security Device Manager
- Cisco VPN 客户端支持页
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems