在 RV34x 系列路由器上配置 AnyConnect 虚拟专用网络 (VPN) 连接

目标

本文档旨在展示如何在 RV34x 系列路由器上配置 AnyConnect VPN 连接。

使用AnyConnect安全移动客户端的优势：

1. 安全且持续的连接
2. 持久的安全性和策略实施
3. 可从自适应安全设备(ASA)或企业软件部署系统部署
4. 可定制和可翻译的
5. 易于配置
6. 支持互联网协议安全(IPSec)和安全套接字层(SSL)
7. 支持Internet密钥交换版本2.0(IKEv2.0)协议

简介

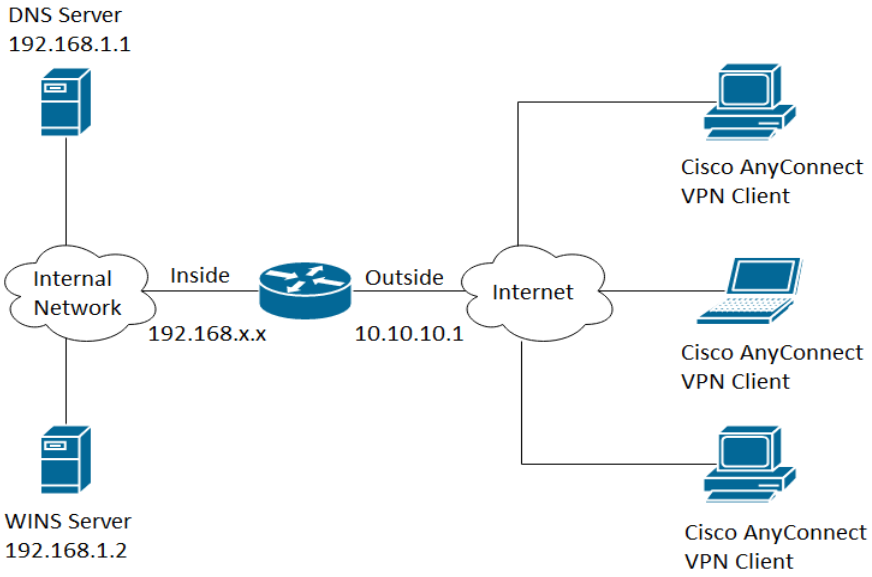
虚拟专用网络(VPN)连接允许用户通过公共或共享网络（例如Internet）访问、发送和接收来自专用网络的数据，但仍能确保安全连接到底层网络基础设施，以保护专用网络及其资源。

VPN客户端是在要连接到远程网络的计算机上安装并运行的软件。此客户端软件的设置配置必须与VPN服务器的配置相同，例如IP地址和身份验证信息。此身份验证信息包括用于加密数据的用户名和预共享密钥。根据要连接的网络的物理位置，VPN客户端也可以是硬件设备。如果使用VPN连接连接位于不同位置的两个网络，通常会发生这种情况。

Cisco AnyConnect安全移动客户端是一种软件应用程序，用于连接到在各种操作系统和硬件配置下工作的VPN。此软件应用程序使用户可以安全访问另一个网络的远程资源，就像直接连接到其网络一样。Cisco AnyConnect安全移动客户端提供了一种创新的新方法，可在基于计算机或智能手机平台上保护移动用户，为最终用户提供更加无缝、始终受保护的体验，并为IT管理员提供全面的策略实施。

在RV34x路由器上，从固件版本1.0.3.15开始并不断向前发展，不需要AnyConnect许可。仅对客户端许可证收费。

有关RV340系列路由器上的AnyConnect许可的详细信息，请参阅有关RV340系列路由器的AnyConnect许可的文章。



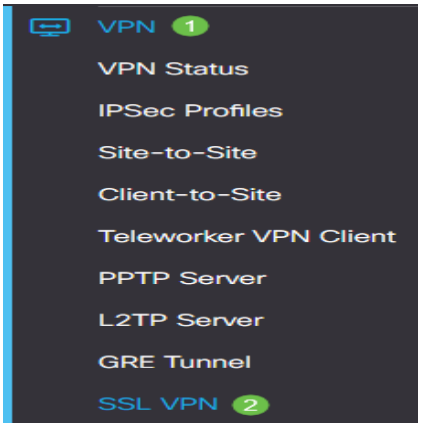
适用设备 |固件版本

- Cisco AnyConnect 安全移动客户端 | 4.4(下载最新版)
- RV34x系列 | 1.0.03.15(下载最新版本)

在RV34x上配置AnyConnect VPN连接

在RV34x上配置SSL VPN

步骤1:访问路由器基于Web的实用程序并选择**VPN > SSL VPN**。



第二步：单击**On**单选按钮以启用Cisco SSL VPN服务器。

强制网关设置

以下配置设置是必需的：

第三步：从下拉列表中选择网关接口。此端口将用于通过SSL VPN隧道传递流量。选项有：

- WAN1

- WAN2
- USB1
- USB2

注意：在本例中，选择了WAN1。

第四步：在*Gateway Port*字段中输入用于SSL VPN网关的端口号，范围为1至65535。

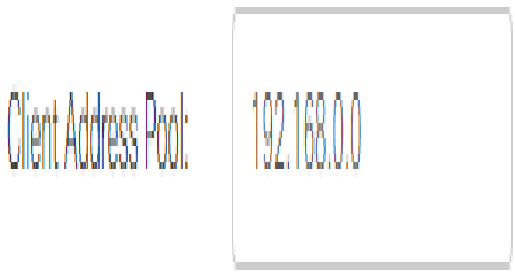
注意：在本示例中，8443用作端口号。

第五步：从下拉列表中选择证书文件(Certificate File)。此证书对尝试通过SSL VPN隧道访问网络资源的用户进行身份验证。下拉列表包含默认证书和导入的证书。

注意：在本示例中，选择Default。

第六步：在*客户端地址池*字段中输入客户端地址池的IP地址。此池将是分配给远程VPN客户端的IP地址范围。

注意：确保IP地址范围不会与本地网络中的任何IP地址重叠。



注意：在本示例中，使用192.168.0.0。

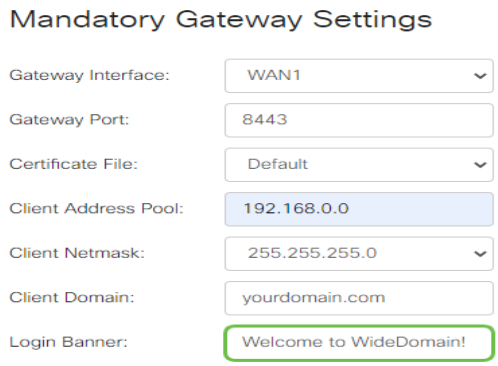
步骤 7.从下拉列表中选择Client Netmask。

注意：在本示例中，选择了255.255.255.128。

步骤 8在*Client Domain*字段中输入客户端域名。这是应推送到SSL VPN客户端的域名。

注意：在本示例中，WideDomain.com用作客户端域名。

步骤 9在*Login Banner*字段中输入显示为登录标语的文本。这是客户端每次登录时显示的标语。

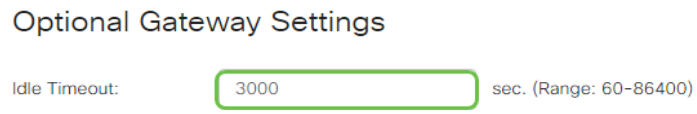


注意：在本示例中，欢迎使用Widedomain！用作登录标语。

可选网关设置

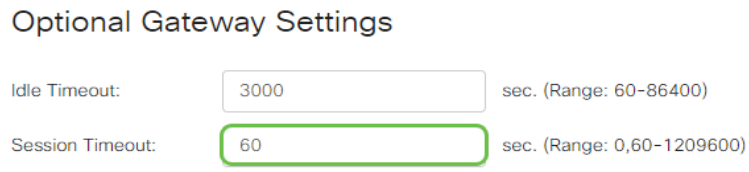
以下配置设置是可选的：

步骤1:输入介于60到86400之间的空闲超时值（以秒为单位）。这是SSL VPN会话可以保持空闲的持续时间。



注：在本示例中，使用3000。

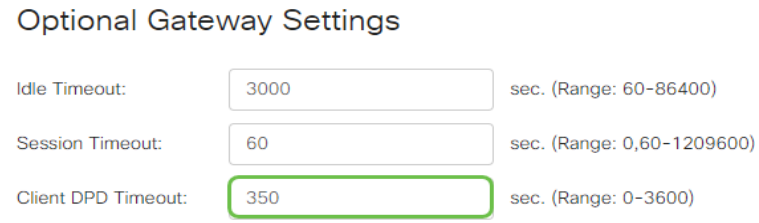
第二步：在*Session Timeout*（会话超时）字段中，输入一个*以秒为*单位的值。这是传输控制协议(TCP)或用户数据报协议(UDP)会话在指定的空闲时间之后超时的时间。范围从 60 至 1209600。



注：在本示例中，使用60。

第三步：在*ClientDPD Timeout*字段中输入介于0到3600之间的值（以秒为单位）。此值指定定期发送HELLO/ACK消息以检查VPN隧道的状态。

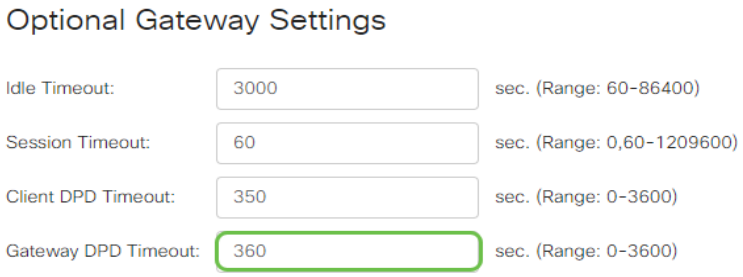
注意：必须在VPN隧道的两端启用此功能。



注意：在本示例中，使用350。

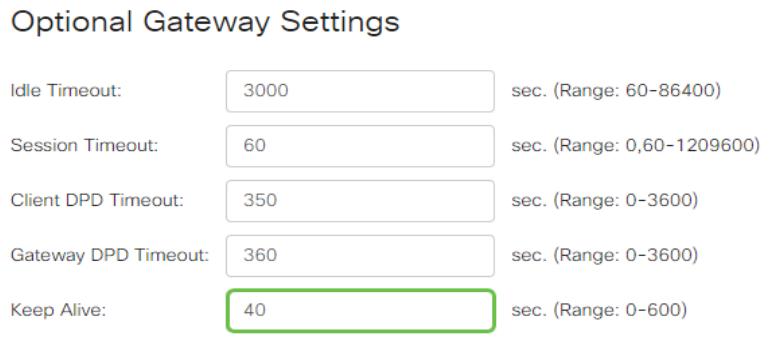
第四步：在*GatewayDPD Timeout*字段中输入介于0到3600之间的值（以秒为单位）。此值指定定期发送HELLO/ACK消息以检查VPN隧道的状态。

注意：必须在VPN隧道的两端启用此功能。



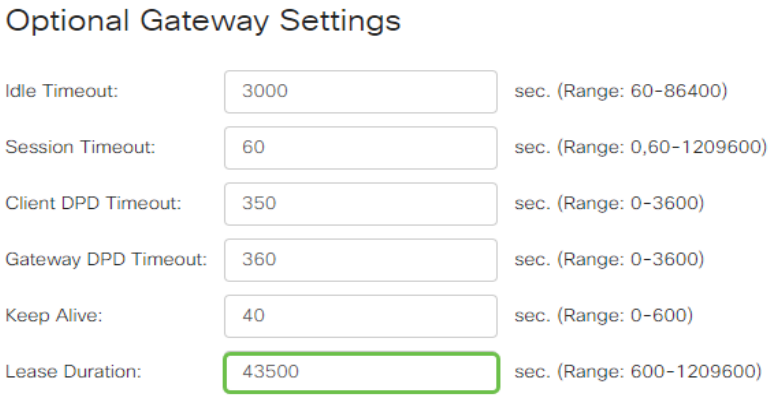
注意：在本示例中，使用360。

第五步：在*Keep Alive*字段中输入一个介于0到600之间的值（以秒为单位）。此功能可确保您的路由器始终连接到Internet。如果它被丢弃，它将尝试重新建立VPN连接。



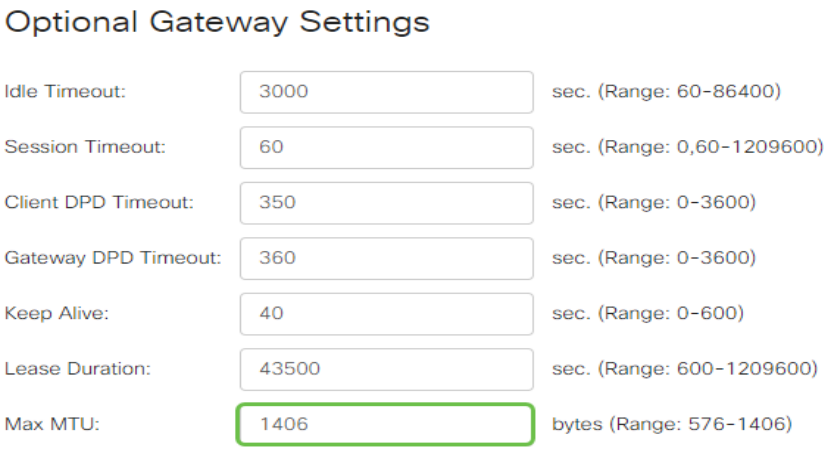
注意：在本示例中，使用40。

第六步：在*Lease Duration*字段中输入要连接的隧道的持续时间值（以秒为单位）。范围从 600 至 1209600。



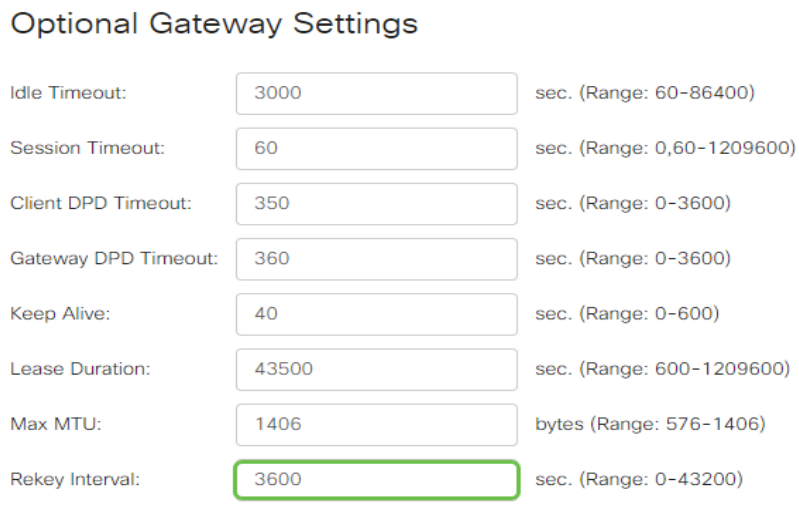
注意：在本示例中，使用43500。

步骤 7.输入可通过网络发送的数据包大小（以字节为单位）。范围从 576 至 1406。



注意：在本示例中，使用1406。

步骤 8在*Rekey Interval*字段中输入中继间隔时间。Rekey功能允许SSL密钥在会话建立后重新协商。范围从 0 至 43200。

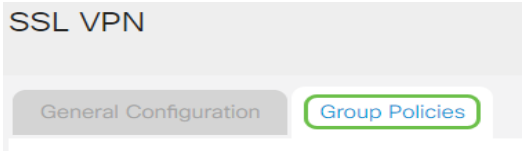


注意：在本示例中，使用3600。

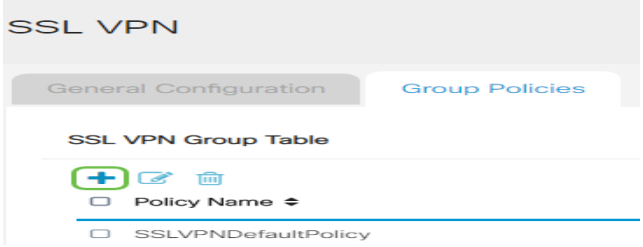
步骤 9单击 **Apply**。

配置组策略

步骤1:点击**Group Policies选项**卡。



第二步：点击SSL VPN Group Table下的**Add**按钮以添加组策略。



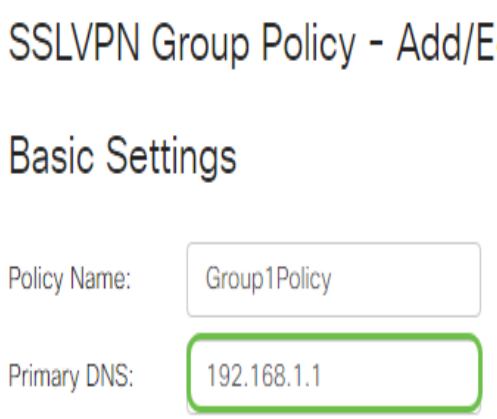
注：SSL VPN组表将显示设备上的组策略列表。您还可以编辑列表中的第一个组策略，名为

SSLVPNDefaultPolicy。这是设备提供的默认策略。

第三步：在*Policy Name*字段中输入您的首选策略名称。

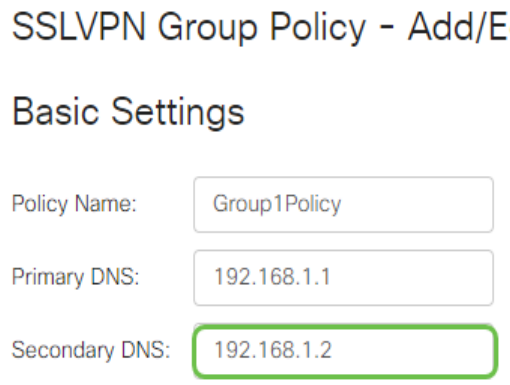
注意：在本示例中，使用组1策略。

第四步：在提供的字段中输入主要DNS的IP地址。默认情况下，已提供此IP地址。



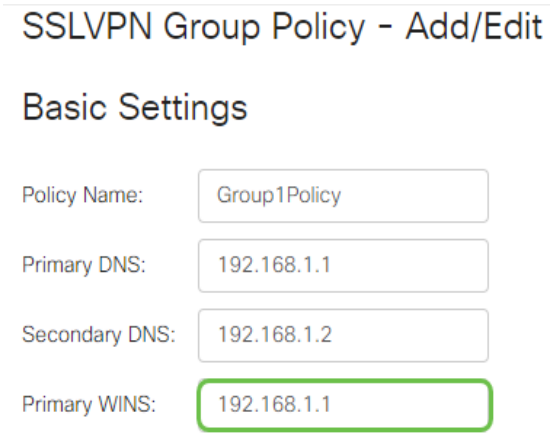
注意：在本示例中，使用192.168.1.1。

步骤5.（可选）在提供的字段中输入辅助DNS的IP地址。这将在主DNS发生故障时用作备份。



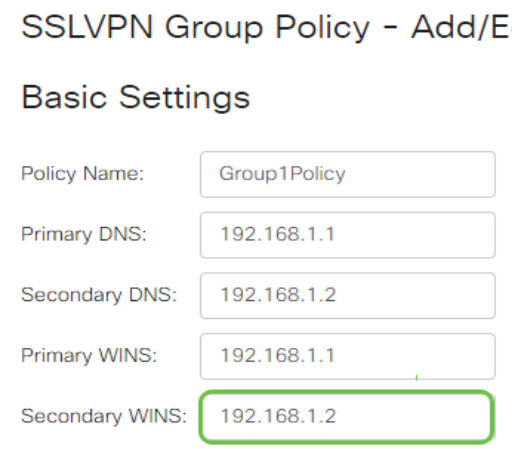
注意：在本示例中，使用192.168.1.2。

步骤6.（可选）在提供的字段中输入主WINS的IP地址。



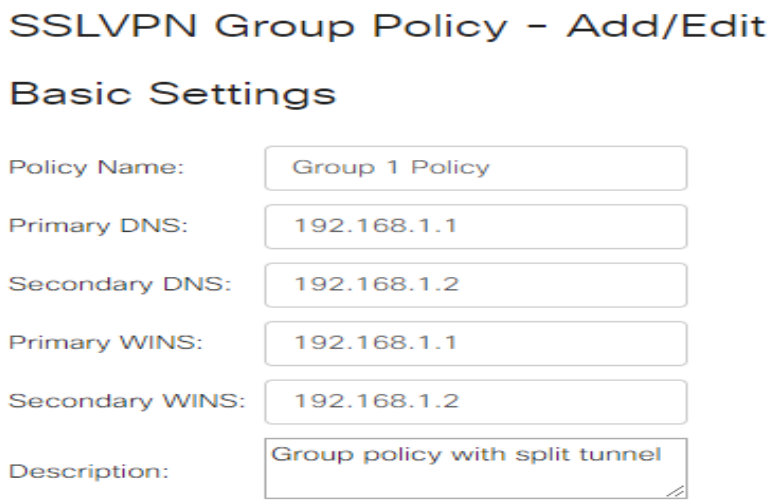
注意：在本示例中，使用192.168.1.1。

步骤7.（可选）在提供的字段中输入辅助WINS的IP地址。



注意：在本示例中，使用192.168.1.2。

步骤8.（可选）在*说明*字段中输入策略的说明。

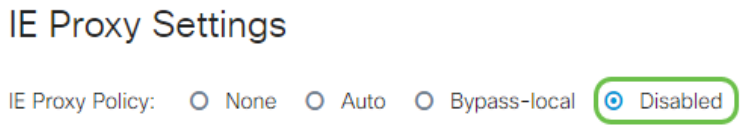


注意：在本示例中，使用具有拆分隧道的组策略。

第9步（可选）点击单选按钮选择IE代理策略以启用Microsoft Internet Explorer(MSIE)代理设置以建立VPN隧道。选项有：

- 无 — 允许浏览器不使用代理设置。

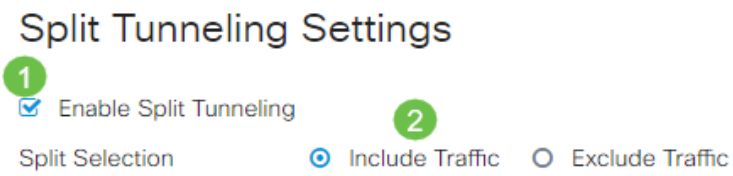
- 自动 — 允许浏览器自动检测代理设置。
- Bypass-local — 允许浏览器绕过在远程用户上配置的代理设置。
- 已禁用 — 禁用MSIE代理设置。



注意：在本示例中，选择Disabled。这是默认设置。

第10步。（可选）在Split Tunneling Settings区域中，选中**Enable Split Tunneling**复选框以允许以未加密方式将发往Internet的流量直接发送到Internet。完全隧道会将所有流量发送到终端设备，然后将其路由到目标资源，从而消除企业网络的Web访问路径。

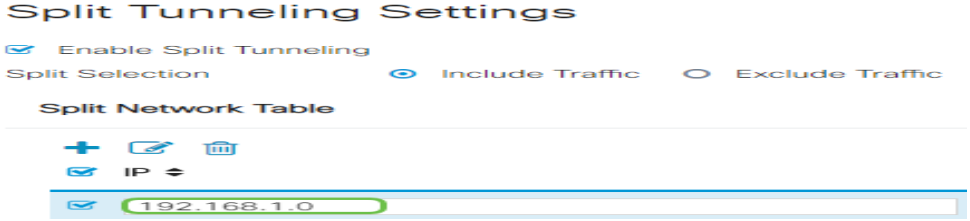
步骤11.（可选）点击单选按钮，选择应用分割隧道时是包括还是排除流量。



注意：在本示例中，选择Include Traffic。

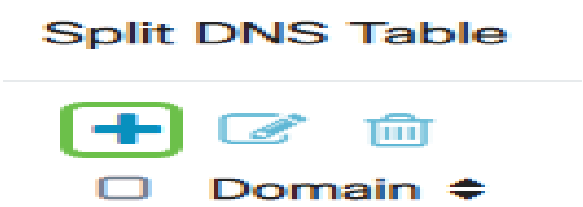
步骤 12在Split Network Table中，单击**Add**按钮添加拆分网络例外。

步骤 13在提供的字段中输入网络的IP地址。



注意：在本示例中，使用192.168.1.0。

步骤 14在拆分DNS表中，单击**Add**按钮以添加拆分DNS异常。



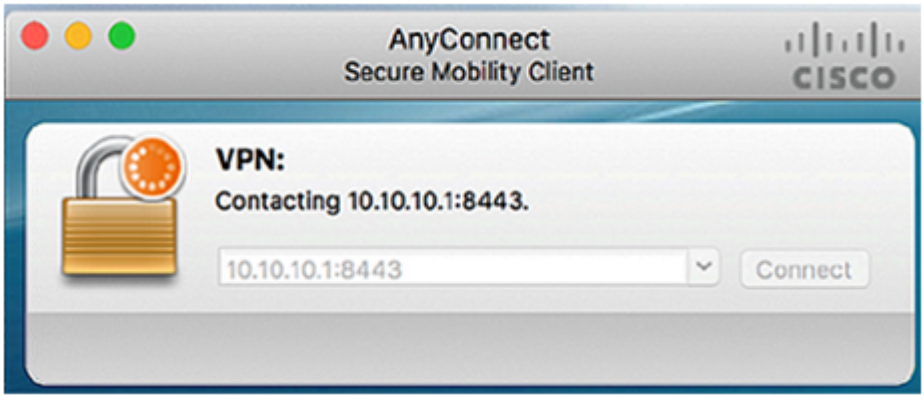
步骤 15在提供的字段中输入域名，然后单击**Apply**。

检验AnyConnect VPN连接

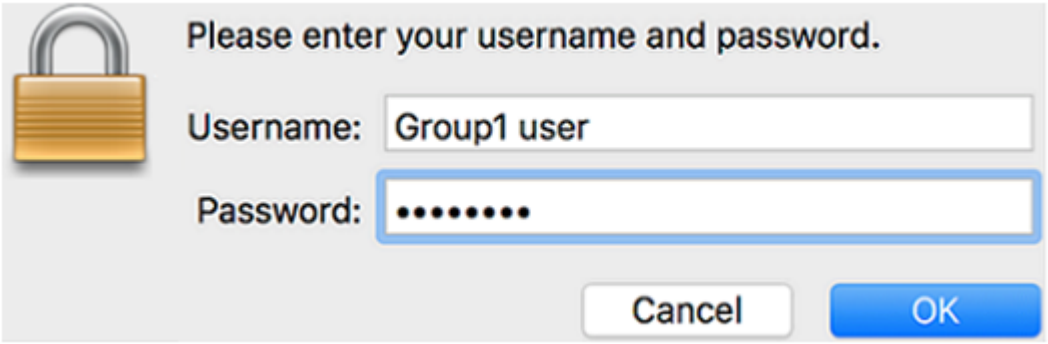
步骤1:点击**AnyConnect Secure Mobility Client**图标。

第二步：在AnyConnect Secure Mobility Client窗口中，输入网关IP地址和网关端口号，用冒号(:)分隔，然后单击**Connect**。

注意：在本示例中，使用10.10.10.1:8443。软件现在将显示它正在联系远程网络。

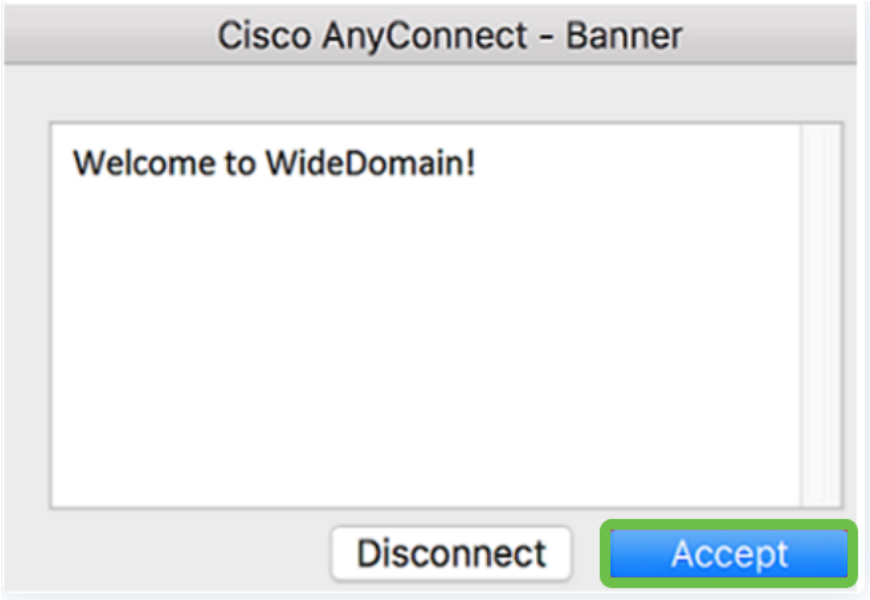


第三步：在各自的字段中输入您的服务器用户名和密码，然后单击**OK**。

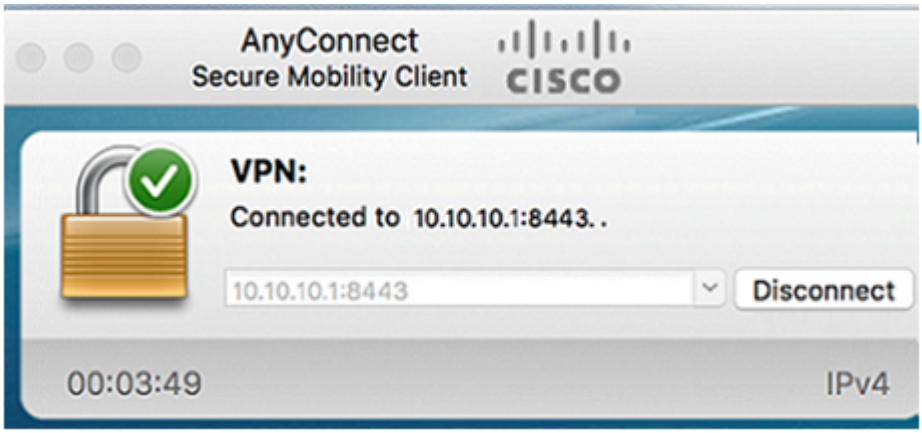


注意：在本示例中，Group1用户用作用户名。

第四步：一旦建立连接，系统就会显示登录横幅。单击 **Accept**。



AnyConnect窗口现在应指示与网络的VPN连接是否成功。



步骤5.（可选）要断开网络连接，请单击**Disconnect**。

您现在应该已经使用RV34x系列路由器成功配置了AnyConnect VPN连接。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。