

在RV220W和RV120W设置的快速虚拟专用网络(VPN)

目标

虚拟专用网络(VPN)是使用一套公共电信设施和他们的技术例如互联网的网络，提供远程办公室或个人用户的安全访问对他们的组织网络。多数VPN实施使用互联网作为公共基础设施和各种各样的专门化的协议通过互联网支持专用通信。VPN跟随客户端和服务方法。VPN客户端验证用户，加密数据，并且管理会话用VPN服务器使用称为隧道的技术。

本文解释如何设置在RV220W和RV120W的快速VPN。

Note:从www.cisco.com下载最新的固件并且保存它在您的计算机。

可适用的设备

- RV120W
- RV220W

软件下载URL

<https://www.cisco.com/cisco/software/release.html?mdfid=283118607&flowid=24581&softw areid=282465795&release=1.4.2.1&relind=AVAILABLE&rellifecycle=&reltype=latest>

软件版本

- v1.0.4.17

建立快速虚拟专用网络的逐步程序

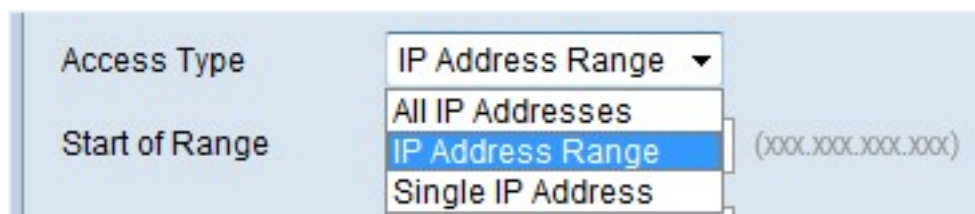
Enable (event)远程管理

远程管理允许您访问和控制设备，不用与实际单元的任何物理连接。启用远程管理允许您从一远程WAN网络访问设备。通过使用设备的LAN IP地址和HTTP，设备管理器从在LAN的一台计算机被获取。

步骤1. 登陆到Web配置工具并且选择**Administration > 远程管理**。远程管理页打开：

Step 2.检查**远程管理**复选框对enable (event)远程管理。

Note:如果此功能不是启用的， Cisco QuickVPN和SSL VPN访问不会作用。



步骤3.选择访问的种类授予在访问类型下拉菜单：

- 所有IP地址—允许所有IP地址访问设备。在您选择此选项前，用户将必须更改默认密码。
- IP地址范围—允许在被配置的范围的所有IP地址访问设备。输入允许的范围的开始的IP地址在范围字段开始。输入允许的范围的结束IP地址在范围字段末端。
- 单个IP地址—限制对一个设备的访问用单个IP地址(例如，您使用访问设备管理器)的计算机。在IP Address字段，请输入将产生的PC的IP地址远程管理权限。

步骤4.输入用于远程连接的端口号在Port Number字段。设置默认情况下端口号443。

Note: 如果配置除了443或60443的其他端口号， Cisco QuickVPN不会作用。

第 5 步：检查**远程SNMP**复选框对enable (event)简单网络管理协议(SNMP)和将远程使用管理设备。

步骤6.点击“**Save**”应用设置。

Note:当远程管理是启用的时，设备对认识其IP地址的人是可访问的。因为一个有恶意的广域网用户能重新配置设备和在许多方面误用它，请更改管理员和所有客户密码，在功能是启用的前。

互联网协议安全(IPsec)用户配置

互联网协议安全(IPsec)是获取的IP通信一个协议组由通信会话的每个IP信息包的认证和加密。

IPsec也包括协议为设立在会话期间将使用的加密密钥的代理程序在每次会话的开始和协商的之间相互验证。

步骤1.登陆到Web配置工具并且选择VPN > IPsec > VPN用户。VPN用户页打开：

VPN Users

PPTP Server Configuration

PPTP Server Enable

Starting IP Address (xxx.xxx.xxx.xxx)

Ending IP Address (xxx.xxx.xxx.xxx)

VPN Client Setting Table

<input type="checkbox"/>	No.	Enabled	Username	Password	Allow User to Change Password	Protocol
<input type="checkbox"/>	1	NA	cisco123	*****	Disabled	QuickVPN

步骤2.点击**添加**添加一个客户端在VPN客户端设置表里。

VPN Client Setting Table

<input type="checkbox"/>	No.	Enabled	Username	Password	Allow User to Change Password	Protocol
<input type="checkbox"/>	1	NA	cisco123	*****	Disabled	QuickVPN

Please click 'Save' button to take Add/Edit/Delete Operation into effect

步骤3.送进用户名或唯一标识符扩展登录用户的在用户名字段。

步骤4.输入密码在密码字段。

第 5 步：检查**允许用户更换密码**复选框允许QuickVPN用户更改此密码。

步骤6.从协议下拉菜单选择协议类型：

- QuickVPN —允许一个异地用户从认识设备的IP地址的其他LAN连接访问设备。
- PPTP —允许点到点隧道协议远程访问设备。
- XAUTH —允许用户的认证有方法的除在SA IKE参数提及的认证方法之外。XAUTH必须在一个被配置以下模式：
 - 无—此模式禁用XAUTH。
 - IPsec主机—路由器由有用户名和密码组合的一个远程网关验证。在此特定的模式下，路由器作为远程网关的VPN客户端。

-用户数据库— 在路由器创建的此模式用户帐户用于验证用户。