Cisco RV路由器VPN概述和最佳实践

目标

本文档的目标是向任何新使用Cisco RV系列路由器的用户概述虚拟专用网络(VPN)最佳实践。

目录

简介

似乎很久以前，你唯一能工作的地方就是办公室。你可能记得，回到家里，你必须得在周末去办公室处理一件工作事情。除了在办公室外，没有其他方法可以从公司资源中获取数据。那些日子已经结束了。在当今时代，您可以在旅途中；在家、另一间办公室、一家咖啡店甚至另一个国家/地区开展业务。缺点是黑客总是想窃取您的敏感数据。仅使用公共互联网是不安全的。您如何才能获得灵活性和安全性？设置VPN!

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隧道可建立一个专用网络，该专用网络可以使用加密来编码数据，并使用身份验证来确保客户端的身份，从而安全地发送数据。公司办公室通常使用VPN连接，因为即使员工不在办公室，也有必要允许他们访问其专用网络。

通常，站点到站点VPN会将整个网络相互连接。它们扩展了网络，并允许来自一个位置的计算机资源在其他位置可用。通过使用支持VPN的路由器，公司可以通过公共网络（例如Internet）连接多个

固定站点。

VPN的客户端到站点设置允许远程主机或客户端像位于同一本地网络一样运行。在路由器配置用于Internet连接后，可以在路由器和终端之间建立VPN连接。VPN客户端除需要匹配设置以建立连接外，还取决于VPN路由器的设置。此外，某些VPN客户端应用是特定于平台的，它们也依赖于操作系统(OS)版本。设置必须完全相同，否则它们无法通信。

VPN可以设置为以下任意一项：

- 安全套接字层 (SSL)
- Internet协议安全(IPSec)
- 点对点隧道协议(PPTP) — 不如SSL或IPSec安全
- 通用路由封装 (GRE)
- 第 2 层隧道协议 (L2TP)

如果您以前从未设置过VPN，那么在本文中将会收到许多新信息。本指南不是分步指南，而是供参考的更多概述。因此，在继续操作并尝试在网络中设置VPN之前，最好阅读本文的全部内容。本文中提供了特定步骤的链接。

思科不支持第三方非思科产品，包括GreenBow、OpenVPN、Shrew Soft和EZ VPN。它们严格出于指导目的被包括在内。如果您在文章之外需要这些方面的支持，请与第三方联系以获得支持。

使用VPN连接的优点

- 使用VPN连接有助于保护机密的网络数据和资源。
- 它为远程工作人员或公司员工提供了便利性和可访问性，因为他们可以轻松访问总部资源，而不必亲自到场，同时还可以维护专用网络及其资源的安全性。
- 与其他远程通信方法相比，使用VPN连接的通信可提供更高级别的安全性。高级加密算法使这一点成为可能，从而保护私有网络免受未经授权的访问。
- 用户的实际地理位置受到保护，不会暴露于公共网络或共享网络（如Internet）。
- VPN允许添加新用户或用户组，而无需添加其他组件或进行复杂的配置。

使用VPN连接的风险

- 配置错误可能会带来安全风险。由于VPN的设计和实施可能很复杂，因此有必要将配置连接的任务委托给有丰富知识和经验的专业人员，以确保专用网络的安全不会受到损害。
- 它可能不太可靠。由于VPN连接需要Internet连接，因此，提供商必须拥有经过验证和测试的声誉，才能提供卓越的Internet服务，并保证最少的停机时间甚至不会停机。
- 如果出现需要添加新基础架构或新配置集的情况，技术问题可能因不兼容而产生，尤其是当它涉及不同的产品或供应商时，与您已经在使用的产品或供应商不同的情况。
- 连接速度可能会变慢。如果您使用的是提供免费的VPN服务的ISP连接，则连接速度可能也会

很慢，因为这些提供商并不优先选择连接速度。请注意，VPN吞吐量取决于路由器的硬件功能。

有关VPN工作方式的更多信息，请点击此处。

配置VPN时使用的提示

1. 配置不同站点之间的VPN时，两端使用不同的LAN IP子网。例如，如果所连接的站点使用192.168.x.x编址方案，则您需要使用10.x.x.x或172.16.x.x - 172.31.x.x子网。另一种方法是使用不同的子网掩码。当您更改路由器IP地址时，动态主机配置协议(DHCP)上的设备将自动获取该子网中的IP地址。
2. 使用路由器WAN接口上的静态公有IP实现稳定的VPN连接。
3. 确保所选的加密和身份验证级别与要为VPN建立VPN隧道的路由器相同。
4. 确保输入的PSK和密钥有效期与远程路由器相同。PSK可以是任何您想要的，只要在站点和客户端上设置为客户端时，它必须与客户端匹配。根据设备的不同，可能存在禁止使用的符号。Key Lifetime是系统更改密钥的频率。首选证书，因为它被认为更安全。
5. 对于大多数VPN，客户端不需要证书即可使用VPN，它仅用于通过路由器进行验证。例如，OpenVPN需要客户端和站点证书。
6. 在第I阶段设置您的SA生存时间比在第II阶段设置SA生存时间长。如果您使第I阶段短于第II阶段，那么您将不得不频繁地来回重新协商隧道，而不是数据隧道。数据隧道需要更高的安全性，因此最好将第II阶段的寿命短于第I阶段。
7. 将所有密码更改为更复杂的密码。

VPN类型

安全套接字层(SSL)

Cisco RV34x系列路由器使用AnyConnect支持SSL VPN。RV160和RV260可以选择使用OpenVPN，这是另一个SSL VPN。SSL VPN服务器允许远程用户使用Web浏览器建立安全VPN隧道。此功能允许使用本地超文本传输协议(HTTP)通过SSL超文本传输协议安全(HTTPS)浏览器支持轻松访问各种Web资源和支持Web的应用。

SSL VPN允许用户使用安全且经过身份验证的路径通过加密网络流量远程访问受限网络。

在SSL中设置访问有两种选项：

1. 自签名证书：由自己创建者签名的证书。不建议这样做，并且只应在测试环境中使用。
2. CA签名证书：此证书更安全，强烈推荐。第三方会付费验证网络是否合法，并创建CA证书，然后将其附加到站点。有关CA证书的详细信息，请参阅本文的证书部分。

本文档中提供了有关AnyConnect相关文章的链接。有关AnyConnect的概述，请单击此处。

IPSec 简档

Easy VPN(EZVPN)、GreenBow和Shrew Soft是互联网协议安全(IPSec)VPN。IPSec VPN在两个对等体之间或从客户端到站点提供安全隧道。被视为敏感的数据包应该通过这些安全隧道发送。必须

定义散列算法、加密算法、密钥生存期和模式等参数，以保护这些敏感数据包，这些参数应通过指定这些隧道的特性进行定义。然后，当IPsec对等体看到此类敏感数据包时，它会设置适当的安全隧道，并通过此隧道将数据包发送到远程对等体。

在防火墙或路由器中实施IPsec后，它可提供强大的安全性，可应用到所有跨越边界的流量。公司或工作组内的流量不会产生与安全相关的处理开销。

为了成功加密和建立VPN隧道的两端，双方需要就加密、解密和身份验证的方法达成一致。IPsec配置文件是IPsec中的中心配置，它定义了算法(例如加密、身份验证和Diffie-Hellman(DH)组)，用于自动模式以及手动密钥模式中的第I阶段和第II阶段协商。

IPsec的重要组件包括互联网密钥交换(IKE)第1阶段和第2阶段。

IKE第一阶段的基本用途是对IPSec对等体进行身份验证，并在对等体之间设置安全通道以启用IKE交换。IKE第一阶段执行以下功能：

- 验证并保护IPSec对等体的身份
- 在对等体之间协商匹配的IKE安全关联(SA)策略以保护IKE交换
- 执行经过身份验证的Diffie-Hellman交换，最终结果为具有匹配的共享密钥
- 设置安全隧道以协商IKE第二阶段参数
- 在主模式和主动模式下发生

IKE第二阶段的目的是协商IPSec SA以设置IPSec隧道。IKE第二阶段执行以下功能：

- 协商受现有IKE SA保护的IPSec SA参数
- 建立IPSec安全关联
- 定期重新协商IPSec SA以确保安全性
- 或者，执行额外的Diffie-Hellman交换
- 仅使用一种模式，快速模式

如果在IPSec策略中指定了完全向前保密(PFS)，则在每个快速模式中执行新的DH交换，提供具有更大的熵（密钥材料寿命）的密钥材料，从而更好地抵抗密码攻击。每个DH交换需要较大的指数值，从而增加CPU使用率并产生高性能成本。

- 在RV34x系列路由器上配置互联网协议安全(IPSec)配置文件
- 在RV160和RV260上配置IPSec配置文件（自动密钥模式）
- 在RV160和RV260路由器上配置IPsec配置文件手动密钥模式

点对点隧道协议 (PPTP)

PPTP是用于创建公共网络之间的VPN隧道的网络协议。PPTP服务器也称为虚拟专用拨号网络(VPDN)服务器。 PPTP有时用于其他协议，因为它速度更快且能够在移动设备上工作。但是，必须注意的是，它不如其他类型的VPN安全。有多种方法可以连接PPTP类型帐户。单击链接了解更多信息：

- 在Rv34x系列路由器上配置点对点隧道协议(PPTP)服务器
- 在RV320和Windows上的RV325 VPN路由器系列上配置点对点隧道协议(PPTP)服务器

通用路由封装

通用路由封装(GRE)是一种隧道协议，它通过封装方式提供了一种简单的通用方法，用于在另一个协议上传输一个协议的数据包。

GRE封装有效负载，即需要在外部IP数据包内传送到目的网络的内部数据包。GRE隧道充当虚拟点对点链路，它具有由隧道源和隧道目标地址标识的两个终端。

隧道终端通过中间IP网络路由封装数据包，通过GRE隧道发送负载。沿途的其他IP路由器不解析负载（内部数据包）；它们只解析外部IP数据包，将其转发到GRE隧道终端。到达隧道终点时，GRE封装被删除，负载被转发到数据包的最终目的地。

网络中的数据报封装有多种原因，例如源服务器想要影响数据包到达目的主机所采用的路由。源服务器也称为封装服务器。

IP-in-IP封装涉及在现有IP报头上插入外部IP报头。外部IP报头中的源地址和目的地址指向IP内隧道的端点。IP报头堆栈用于将数据包通过预定路径转发到目的地，前提是网络管理员知道传输数据包的路由器的环回地址。

此隧道机制可用于确定大多数网络架构的可用性和延迟。请注意，从源到目的地的整个路径不必包含在报头中，但可以选择网络的一个网段来引导数据包。

第 2 层隧道协议

L2TP不为其隧道流量提供加密机制。相反，它依赖其他安全协议（如IPSec）来加密数据。

在L2TP访问集中器(LAC)和L2TP网络服务器(LNS)之间建立L2TP隧道。IPSec 隧道也建立在这些设备之间，并使用 IPSec 对所有 L2TP 隧道流量进行加密。

L2TP的一些关键术语：

- CHAP — 质询握手身份验证协议。点对点身份验证协议(PPP)。
- L2TP接入集中器(LAC)- LAC可以是连接到公共交换电话网(PSTN)的思科网络接入服务器。LAC只需实施介质即可通过L2TP进行操作。LAC可以使用局域网或广域网（例如公共或专用帧中继）连接到LNS。LAC是传入呼叫的发起方和传出呼叫的接收方。
- L2TP网络服务器(LNS) — 几乎所有连接到局域网或广域网（如公共或专用帧中继）的Cisco路由器都可以充当LNS。它是L2TP协议的服务器端，必须在任何终止PPP会话的平台上运行。LNS是呼出呼叫的发起者和呼入呼叫的接收者。图1描述了LAC和LNS之间的呼叫例程。
- 虚拟专用拨号网络(VPDN)-一种使用PPP交付服务的访问VPN。

如果您想了解有关L2TP的详细信息，请点击以下链接：

- 在RV34x路由器上配置L2TP WAN设置
- 广域网配置指南：第2层服务，Cisco IOS XE版本3S

与Cisco RV系列VPN路由器兼容的VPN

	RV34X	RV32X	RV160X/RV260X
IPSec(IKEv1)			
ShrewSoft	Yes	Yes	Yes
格林博	Yes	Yes	Yes
Mac内置客户端	Yes	Yes	无
iPhone/iPad	Yes	Yes	无
安卓	Yes	Yes	Yes
L2TP/IPSec	是(PAP)	无	无
PPTP	是(PAP)	是*	是(PAP)
Other（其他）			
AnyConnect	Yes	无	无
Openvpn	无	Yes	Yes
IKEv2			
Windows 窗口版本	是*	无	是*
MAC	Yes	无	Yes
iPhone	Yes	无	Yes
安卓	Yes	无	Yes

VPN 技术	支持的设备	支持的客户端*	详情和注意事项
IPSec(IKEv1)	RV34X、RV32X、RV160X/RV260X	原生：Mac、iPhone、iPad、Android 其他：EasyVPN（Cisco VPN客户端）、ShrewSoft、Greenbow	最易于设置、故障排除和支持。它可在所有路由器上使用，设置简单（大多数情况下），具有最佳的日志记录进行故障排除。包括大多数设备。这就是为什么我们通常推荐ShrewSoft（免费而且有效）和Greenbow（不免费，但是有效）。 对于Windows，我们选择ShrewSoft和Greenbow客户端，因为Windows没有纯IPSec本地VPN客户端。对瑞软和绿宝来说，它参与度更高一些，但并不难做到。在首次设置后，可以导出客户端配置文件，然后在其他客户端上导入客户端配置文件。 对于RV160X/RV260X路由器，因为我们没有Easy VPN选项，因此必须使用第三方客户端选项，该选项不能与Mac、iPhone或iPad配合使用。不过，我们可以设置ShrewSoft、Greenbow和Android客户端进行连接。对于Mac、iPhone和iPad客户端，我推荐IKEv2（如下所示）。

AnyConnect	RV34X	Windows、Mac、iPhone、iPad、Android	有些客户要求完整的思科解决方案，仅此而已。它设置简单，具有日志记录，但难以理解日志。需要客户端许可要求，产生成本。它是一个完整的思科解决方案并经过更新。故障排除并不像IPSec那么简单，但比其他VPN选项更容易。
L2TP/IPSec	RV34X	原生：Windows	对于需要在Windows中使用内置VPN客户端的客户，我会建议这样做。以下是两个警告： 1.我们仅在使用本地身份验证时支持PAP身份验证。我们必须进入每个客户端，选择可选或不选择加密，禁用MS-CHAP选项并启用PAP。这意味着用户名/密码以明文形式发送。这不是一笔大生意，因为所有内容都使用IPSec加密，并且必须在每个客户端上进行设置。在Windows上，这是可配置的，但在Mac、iPhone、iPad或Android设备上不可配置，因此实际上只能由Windows客户端使用，除非它们具有外部身份验证服务器（如Radius或LDAP）。 2.如果路由器位于NAT设备之后，则Windows计算机上的连接将失败。解决方法是在每个客户端上创建注册表项，以便在客户端和路由器上均允许NAT。
IPSec(IKEv2)	RV34X、RV160X/RV260X	原生：Windows、Mac、iPhone、iPad、Android	用于IKEv2的Windows本地客户端需要证书身份验证，这需要PKI基础设施，因为路由器和所有客户端都需要具有来自同一CA（或其他受信任CA）的证书。 对于想要使用IKEv2的客户，我们会为其Mac、iPhone、iPad和Android设备设置该设置，并且我们通常为其Windows计算机（ShrewSoft、Greenbow或L2TP/IPSec）设置IKEv1。
开放式VPN	RV32X、RV160X/RV260X	Open VPN是客户端	设置更困难，故障排除和支持更困难。受RV160X/RV260X和RV320支持。设置比IPSec或AnyConnect更复杂，尤其是当它们使用证书时（大多数情况下使用证书）。故障排除比较困难，因为路由器上没

有任何有用的日志，并且依赖于客户端日志。此外，OpenVPN客户端版本更新已无警告地更改了他们接受的证书。此外，我们发现Chromebooks无法满足此要求，因此必须使用IPSec解决方案。

*我们测试尽可能多的组合，如果有具体的硬件/软件组合，请访问此处。否则，请参阅按设备列出的相关配置指南，了解所测试的最新版本。

证书

您是否曾访问过一个网站，并收到过有关其不安全的警告？它不会让您相信您的隐私信息是安全的，而且它不是安全的！如果站点安全，您将在站点名称前看到一个已关闭的锁图标。这是站点已验证安全的符号。您想确保看到锁图标已关闭。您的VPN也是如此。

设置VPN时，应从证书颁发机构(CA)获取证书。证书从第三方站点购买并用于身份验证。这是证明您的站点安全的官方方式。实质上，CA是可信来源，用于验证您是否为合法企业并且可以受到信任。对于VPN，您只需要较低级别的证书，且成本最低。您会由CA签出，他们验证您的信息后，会向您颁发证书。此证书可作为文件下载到您的计算机上。然后，您可以进入路由器（或VPN服务器）并将其上传到那里。

CA在颁发数字证书时使用公钥基础设施(PKI)，它使用公钥或私钥加密来确保安全性。CA负责管理证书请求和颁发数字证书。一些第三方CA包括IdenTrust、Comodo、GoDaddy、GlobalSign、GeoTrust和Verisign。

VPN中的所有网关都必须使用相同的算法，否则它们将无法通信。为简单起见，建议从同一受信任的第三方购买所有证书。这使多个证书更易于管理，因为它们必须手动续订。

注：客户端通常不需要证书即可使用VPN；它仅用于通过路由器进行验证。例外情况是OpenVPN，它需要客户端证书。

为简单起见，一些小型企业选择使用密码或预共享密钥来代替证书。这样做不太安全，但可以免费设置。

有关证书的详细信息，请参阅以下链接：

- RV160和RV260系列路由器上的证书（导入/导出/生成CSR）
- 在RV34x系列路由器上使用第三方SSL证书替换默认自签名证书

路由器上的站点到站点VPN

对于本地和远程路由器，必须确保用于VPN连接的预共享密钥(PSK)/密码/证书和安全设置全部匹配。如果一个或多个路由器使用网络地址转换(NAT)（大多数Cisco RV系列路由器都使用它），则需要在本地和远程路由器上对VPN连接执行防火墙免除。

有关详细信息，请查看以下站点到站点文章：

- 在RV34x上配置站点到站点VPN
- 在RV340或RV345路由器上配置站点到站点VPN
- Cisco Tech Talk：在RV340系列路由器上配置站点到站点VPN（视频）
- 在RV160和RV260路由器上配置站点到站点VPN（基本设置）
- RV160和RV260路由器上的站点到站点VPN（高级设置和故障转移）

路由器上的客户端到站点VPN

在客户端上设置VPN之前，管理员需要在路由器上配置它。

单击查看下列路由器配置文章：

- 在RV160和RV260路由器上配置VPN设置向导
- 使用RV160和RV260配置软件VPN客户端
- Cisco Tech Talk：在RV160和RV260上配置Shrew Soft VPN(视频)
- 设置并使用GreenBow IPsec VPN客户端与RV160和RV260路由器连接

创建客户端到站点配置文件

在客户端到站点VPN连接中，来自Internet的客户端可以连接到服务器，以访问服务器后面的公司网络或LAN，但仍保持网络及其资源的安全性。此功能非常有用，因为它创建了一个新的VPN隧道，允许远程工作人员和商务旅行者使用VPN客户端软件访问您的网络，而不会影响隐私和安全性。以下文章特定于RV34x系列路由器：

- 在RV34x系列路由器上配置客户端到站点的虚拟专用网络(VPN)连接
- 在 RV34x 系列路由器上配置 AnyConnect 虚拟专用网络 (VPN) 连接

如果为源 All Traffic和目标 All Traffic设置端口转发，则客户端到站点VPN将不起作用。

用户组

在路由器上为共享同一组服务的用户集合创建用户组。这些用户组包括组的选项，例如关于如何访问VPN的权限列表。根据设备，可以允许PPTP、站点到站点IPSec VPN和客户端到站点IPSec VPN。例如，RV260的选项包括OpenVPN，但不支持L2TP。RV340系列配备用于SSL VPN的AnyConnect，以及强制网络门户或EZ VPN。

这些设置使管理员能够进行控制和过滤，以便只有授权用户才能访问网络。Shrew Soft和TheGreenBow是两个最常见的可下载VPN客户端。它们需要根据路由器的VPN设置进行配置，才能成功建立VPN隧道。以下文章专门介绍了用户组的创建过程：

- 在RV34x路由器上创建用于VPN设置的用户组

为VPN设置用户组时，请确保将默认管理员帐户保留在管理员组中，并为VPN创建新的用户帐户和用户组。如果将管理员帐户移动到其他组，您将阻止自己登录路由器。因此，您必须执行出厂重置并再次配置该路由器，仅保留管理员组中的默认管理员帐户。

用户帐户

在路由器上创建用户帐户是为了允许使用本地数据库对本地用户进行身份验证，用于各种服务，如PPTP、VPN客户端、Web图形用户界面(GUI)登录和安全套接字层虚拟专用网络(SSLVPN)。这样，管理员就可以控制和过滤仅访问网络的授权用户。以下文章专门介绍用户帐户的创建：

- 为RV34x路由器上的VPN客户端设置创建用户帐户

客户端位置上的客户端到站点

在客户端到站点VPN连接中，来自Internet的客户端可以连接到服务器，以访问服务器后面的公司网络或LAN，但仍保持网络及其资源的安全性。此功能非常有用，因为它创建了一个新的VPN隧道，允许远程工作人员和商务旅行者使用VPN客户端软件访问您的网络，而不影响隐私和安全性。VPN设置为在发送和接收数据时对数据进行加密和解密。

AnyConnect应用可与SSL VPN配合使用，并且专门用于RV34x路由器。其他RV系列路由器不提供此功能。从1.0.3.15版开始，不再需要路由器许可证，但需要为VPN客户端购买许可证。有关Cisco AnyConnect安全移动客户端的详细信息，请点击此处。有关安装说明，请从以下文章中选择：

- 在 Mac 计算机上安装 Cisco AnyConnect Secure Mobility Client
- 在 Windows 计算机上安装 Cisco AnyConnect Secure Mobility Client

有一些第三方应用程序可用于所有RV系列路由器的客户端到站点VPN。如前所述，思科不支持这些应用；提供此信息是为了提供指导。

GreenBow VPN Client是第三方VPN客户端应用，使主机设备能够配置客户端到站点IPsec隧道或SSL的安全连接。这是包含支持的付费应用程序。

- 设置并使用GreenBow IPsec VPN客户端与RV160和RV260路由器连接

OpenVPN是一个免费的开源应用程序，可以设置并用于SSL VPN。它使用客户端 — 服务器连接，通过互联网在服务器和远程客户端位置之间提供安全通信。

- RV160和RV260路由器上的OpenVPN

Shrew Soft是一个免费的开源应用程序，可以设置并用于IPsec VPN。它使用客户端 — 服务器连接，通过互联网在服务器和远程客户端位置之间提供安全通信。

- 使用RV160和RV260配置软件VPN客户端

Easy VPN通常用于RV32x路由器。以下是一些可供参考的信息：

- 在RV320和RV325 VPN路由器系列上配置Easy Client to Gateway虚拟专用网络(VPN)
- Cisco Easy VPN 问答
- 基于Cisco IOS软件的路由器上的Easy VPN

设置向导

最新的Cisco RV系列路由器附带一个VPN设置向导，该向导将引导您完成设置步骤。通过VPN设置向导，可以配置基本LAN到LAN和远程访问VPN连接，并分配预共享密钥或数字证书进行身份验证。有关详细信息，请参阅以下文章：

- 在RV160和RV260上配置VPN设置向导
- 在RV34x系列路由器上使用设置向导配置虚拟专用网络(VPN)连接

结论

这篇文章让您对VPN有了更好的了解，并提供了一些提示，帮助您顺利完成任务。现在，您应准备好配置自己的设备！查看链路并确定在Cisco RV系列路由器上设置VPN的最佳方法。

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）。