哪种 VPN 解决方案适合您？

目录

简介

虚拟专用网络(VPN)正变得越来越普遍，是在广域范围内部署网络的一种更低成本，更加灵活的方式。随着技术的进步，研究人员不断引入各种选项来实现 VPN 解决方案。此技术说明解释其中一些选项并且描述使用它们的最好地方。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

使用的组件

本文档不限于特定的软件和硬件版本。

注意： Cisco还在非IOS平台提供加密支持，包括Cisco安全PIX防火墙、Cisco VPN 3000集中器和Cisco VPN 5000集中器。

NAT

互联网在短时间内得到了爆炸性的增长，这种增长比最初设计者预见的要快得多。在IP4.0版本中可用的有限数量的地址是此增长的证据，结果地址空间变得越来越少。此问题的一个解决方案是网络地址转换 (NAT)。

使用NAT将路由器配置在内部/外部边界上，这样当内部有任意个使用专用寻址机制的主机时，外部(通常是互联网)可以看见一个或几个注册地址。要保持地址转换方案的完整性，必须在内部(私有)网络和外部(公共)网络间的每个边界路由器上配置NAT。从安全立场看，NAT的一个优势是除非特别配置NAT网关来允许连接，否则专用网上的系统不能从外部网络接收流入的IP连接。此外，NAT 对源设备和目标设备是完全透明的。NAT 的建议操作涉及 RFC 1918 ，后者概述了适当的专用网络编址方案。 NAT 的标准在 RFC1631 中进行了描述。

下图使用内部转换网络地址池显示了 NAT 路由器边界定义。

NAT一般用于保存互联网上的可路由IP地址，它很昂贵，并且数量有限。NAT 还通过向互联网隐藏内部网络来确保安全性。

有关 NAT 工作原理的信息，请参阅 NAT 如何工作。

GRE 封装隧道

通用路由封装(GRE)隧道通过共享的WAN提供特定的路径，并采用新数据包报头封装数据流，以保证特定目的地的交付。网络是专用的，因为数据流只在终端进入隧道，并且在另一个终端离开。隧道不提供真正的机密性（机密性由加密提供）但是可以传送加密流量。隧道是在物理接口上配置的逻辑端点，可通过其传输流量。

正如图表显示的，GRE隧道还可以用来将非IP数据流封装到IP中，并且通过互联网或IP网络发送它。互联网分组交换 (IPX) 和 AppleTalk 协议是非 IP 数据流的示例。有关配置 GRE 的信息，请参阅配置 GRE 中的“配置 GRE 隧道接口”。

如果您已经有类似IPX或AppleTalk的多协议网络，并且必须通过互联网或IP网络发送数据流，那么GRE是VPN解决方案的理想之选。另外，GRE 封装通常与其他保护流量安全的方法（如 IPSec）结合使用。

有关 GRE 的更多技术详细资料，请参阅 RFC 1701 和 RFC 2784 。

IPSec 加密

在共享网络上发送数据的加密是通常与VPN相关的VPN技术。Cisco 支持 IP 安全 (IPSec) 数据加密方法。IPSec是一种开放标准的框架，在网络层参与的对端之间提供数据保密性、数据完整性和数据验证。

IPSec加密是互联网工程任务组(IETF)标准，在IPSec客户端软件中支持数据加密标准(DES) 的56位和三重DES (3DES) 168-bit对称密钥加密算法。使用 IPSec 时，GRE 配置是可选的。IPSec 还支持证书颁发机构和 Internet Key Exchange (IKE) 协商。IPSec加密可以配置在客户端、路由器和防火墙之间的独立环境里，或在接入VPN中与L2TP信道一起使用。多种操作系统平台均支持 IPSec。

如果您想为网络提供真正的数据保密性，那么IPSec加密法是适合的VPN解决方案。IPSec 也是开放标准，因此易于实现不同设备之间的互操作性。

PPTP 和 MPPE

点对点隧道协议 (PPTP) 是 Microsoft 开发的一项协议；该协议在 RFC2637 中进行了说明。PPTP在Windows 9x/ME，Windows NT和Windows 2000和Windows XP客户端软件中广泛配置，启用自愿VPN。

Microsoft点到点加密(MPPE)是使用基于RC4的40位或128位加密的Microsoft的信息IETF草案。MPPE是Microsoft PPTP客户端软件解决方案的一部分，并且在自动模式接入VPN体系结构中具有很大的作用。多数 Cisco 平台都支持 PPTP/MPPE。

在 Cisco 7100 和 7200 平台的 Cisco IOS 软件版本 12.0.5.XE5 中，增加了 PPTP 支持。在 Cisco IOS 12.1.5.T 中，增加了对更多平台的支持。Cisco 安全 PIX 防火墙和 Cisco VPN 3000 集中器也增加了对 PPTP 客户端连接的支持。

因为PPTP支持非IP网络，所以对远程用户必须拨入公司网络，访问异构公司网络非常有用。

有关配置 PPTP 的信息，请参阅配置 PPTP。

VPDN 和 L2TP

VPDN

虚拟专用拨号网络(VPDN)是一个Cisco标准，它允许针对远程接入服务器的专用网络拨入服务。在VPDN上下文中，拨入的接入服务器(例如AS5300)通常指网络接入服务器(NAS)。拨入用户的目标是指家庭网关 (HGW)。

基本情形是，先是点对点协议 (PPP) 客户端拨入本地 NAS。NAS确定PPP会话应该被发送到客户端的网关路由器。然后，HGW 将对用户进行身份验证并启动 PPP 协商。在完成PPP设置后，所有帧都是通过NAS 发送到客户端和家庭网关的。此方法集成了多个协议和概念。

有关配置 VPDN 的信息，请参阅配置安全功能中的*配置虚拟专用拨号网络*。

L2TP

第 2 层隧道协议 (L2TP) 是一项 IETF 标准，它融入了 PPTP 和 L2F 的最佳特性。L2TP 隧道主要在强制模式（即从 NAS 拨号到 HGW）下的访问 VPN 中使用，针对 IP 和非 IP 流量。Windows 2000 和 Windows XP 已增加此协议的本地支持，作为一种 VPN 客户端连接方式。

L2TP用于使用IP在一个公共网络（例如互联网）上建立隧道PPP。由于隧道出现在第 2 层，因此上层协议将不知道隧道的存在。与 GRE 一样，L2TP 也可封装任何第 3 层协议。UDP端口1701通过隧道发起人发送L2TP数据流。

注意： 1996年Cisco创建了第二层转发(L2F)协议，允许VPDN的连接。虽然 L2F 的其他功能仍受支持，但 L2F 已被 L2TP 替代。在 1996 年由 IETF 提出的互联网草案中，还创建了点对点隧道协议 (PPTP)。PPTP 提供了类似于 GRE 封装隧道协议的功能，适用于 PPP 连接。

有关 L2TP 的详细信息，请参阅第 2 层隧道协议。

PPPoE

以太网点对点协议 (PPPoE) 是主要在数字用户线 (DSL) 环境中部署的信息类 RFC。PPPoe在同一个LAN内利用现有的以太网结构允许用户起动多个PPP会话。此技术支持第3层服务选择，它是通过单个远程访问连接让用户同时连接到几个目的地的一个新兴应用。带有密码验证协议(PAP)或质询握手验证协议(CHAP)的PPPoE经常用于通知中心站点哪些远程路由器与它连接。

PPPoE 主要在服务提供商 DSL 部署和桥接以太网拓扑中使用。

欲知关于配置PPPoE的更多信息，请参阅在以太网和IEEE 802.1Q VLAN上配置PPPoE。

MPLS VPN

多协议标签交换(MPLS)基于Cisco标记交换的IETF新标准，该标准支持自动设置、快速滚动和提供商需要的可扩展性功能，以有效地提供访问、内联网和外联网路VPN服务。Cisco与服务提供商紧密合作，保证向支持MPLS的VPN服务的平稳转换。MPLS以基于标签的模式工作，当它们进入服务商网络并通过无连接的IP核心加快转发时，请标记信息包。MPLS在VPN属性范围内使用路由辨别器识别VPN会员和包含数据流。

MPLS还通过建立标签交换路径，增加通往IP路由示例的面向连接法的优势，这是根据拓扑信息而不是数据流创建的。MPLS VPN 广泛部署在服务提供商环境中。

有关配置 MPLS VPN 的信息，请参阅配置基本 MPLS VPN。

相关信息

- IPSec 支持页面
- 虚拟私有网络如何工作
- NAT 支持页
- GRE 支持页
- VPDN 支持页
- PPTP 支持页
- PPPoE 支持页
- 技术支持 - Cisco Systems