How Virtual Private Networks Work（虚拟专用网如何工作）

目录

简介
先决条件
要求
使用的组件
规则
背景信息
VPN 由什么构成？
类比：每个 LAN 都是一座岛
VPN 技术
VPN 产品
相关信息

简介

本文包括VPN的基本原理，例如基本VPN组件、技术、隧道建立和VPN安全。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在过去的几十年里，世界已经发生了很大变化。许多企业现在必须考虑全球市场和物流管理系统，而不只是简单应付本地或本区域所关心的问题。许多公司在全国甚至是全球范围内建立了分支机构。但是所有公司都需要做一件事：无论他们的办公室建在哪里，他们都需要一种能维持快速、安全和可靠通信的手段。

直到最近，可靠的通信还是通过使用租赁线路维护广域网 (WAN) 来实现。从综合业务数字网络 (ISDN，在144 Kbps上运行)到光载波-3 (OC3，在155 Mbps上运行)光纤，专用线将公司的专用网扩展到邻近位置。广域网在可靠性、性能和安全性方面明显优于公共网络（如互联网）。然而维护 WAN，特别是使用租用线路时，成本可能会变得非常昂贵(成本通常会随着办公室之间的距离的增加而增加)。此外，专用线不是以下这种公司的可行的解决方案：公司部分工作人员的移动性很强（比如销售人员），并且他们可能需要频繁地远程连接公司网络和敏感数据。

当互联网的大众化增长，企业已经使用它作为扩大自己网络的方法。首先是 Intranet，它是为公司内部员工使用而设计的站点。现在，许多公司都构建了自己的虚拟私有网络 (VPN) 来适应远程员工和远端办公室的需求。

通常 VPN 可能在公司总部拥有一个主局域网 (LAN)，其他 LAN 则在远端办公室/设施和与现场连接的个人用户那里。

VPN 是一种使用公共网络（通常是互联网）的专用网络，用于将远程站点或用户连接到一起。与使用专用的真实世界连接（如专用线）不同，VPN 通过“虚拟”连接在公司专用网到远程站点或员工之间的互联网上进行路由。

VPN 由什么构成？

有两种常见的 VPN 类型。

- **远程访问** — 也称作虚拟专用拨号网络 (VPDN)，这是公司为需要从不同远程位置接入专用网的员工提供的用户到 LAN 连接。希望建立大型远程访问VPN的公司，一般会借助互联网服务提供商(ISP)向其用户提供某种形式的互联网拨号帐户。然后远程办公者能拨打 1-800 号码连接到互联网，并使用他们的 VPN 客户端软件访问公司网络。一个需要远程访问VPN的公司的好的实例是一家在拥有数百名在现场的销售人员的大型公司。远程访问VPN，允许通过第三方服务提供商，在公司的专用网络和远程用户之间建立安全加密连接。
- **站点到站点** - 通过专用设备和大规模加密，公司能通过公共网络连接多个固定站点（例如互联网）。每个站点仅需要一个与同一个公共网络连接的本地连接，从而可在长途专用专线上节约资金。站点到站点 VPN 可进一步分为 Intranet 和 Extranet。在同一公司的办公室之间构建的站点到站点VPN被称为intranet VPN，而将公司与合作伙伴或用户连接起来的网络则被称为 extranet VPN。

设计良好的 VPN 对公司非常有益。例如，它可以：

- 扩展地理连接
- 与传统的 WAN 相比，能降低运作成本
- 减少远程用户的中转时间和差旅费
- 提高生产力
- 简化网络拓扑
- 提供全球联网机会
- 支持远程办公
- 提供比传统 WAN 更加快速的投资回报 (ROI)

设计良好的 VPN 有哪些功能？它应当整合了以下各项：

- 安全
- 可靠性
- 可扩展性
- 网络管理

- 策略管理

类比：每个 LAN 都是一座岛

假设您生活在一座岛屿上，周围是一片汪洋。您的周围有成千上万个其他海岛，一些离您非常近，一些离您较远。旅行的正常方式是乘坐渡轮从您的海岛出发，到您想要参观的任意海岛。但乘渡船出行意味着您几乎毫无隐私可言，因为您的任何行动都被旁人看在眼里。

假定每座岛屿都表示一个私有 LAN，海洋则是 Internet。您乘渡船出行类似于通过 Internet 连接到某个 Web 服务器或另一台设备。您对组成互联网的线路和路由器没有控制权，正如您对轮渡的其他人没有控制权一样。如果您尝试利用公共资源连接两个私有网络，就容易受到安全问题的困扰。

您的岛屿于是决定架设一座通往另一座岛屿的桥梁，这样人们便可以更方便、安全、直接的方式往来于这两座岛屿。建立和维护网桥的费用非常昂贵，即使您连接的海岛非常近。但对于可靠、安全的路径的需要是很大的，以至于您无论如何都会这样做。您的岛屿想要连接到另一座远得多的岛屿，但您判定这样做的费用过高。

这种情况与拥有租用线路非常相似，桥(专线)与海(互联网)是分离的，但它们仍能与海岛(LAN)连接。许多公司之所以选择这一路由，就是因为在连接其远程办公室时有安全性和可靠性方面的需求。然而，如果办公室离得非常远，成本可能会特别高，正如跨越很远的距离建立网桥一样。

那么如何将 VPN 融入到这个比喻中呢？我们可以向各个岛屿的每位居民赠送一艘小潜水艇，这些潜水艇具有以下特点。

- 它速度很快。
- 无论您去哪里都能轻松携带。
- 它能使您完全避开所有其他的小船或潜水艇。
- 它是可靠的。
- 一旦购买了第一个，只要添加很少的成本就可以添加您的系列产品。

虽然我们两个海岛的生物可以与在海洋里与其他数据流一起移动，但这些生物可以在它们希望的任何时候进行往返，具有保密性和安全性。这本质上便是 VPN 的工作原理。您的网络的每个远程成员能以一种安全和可靠的方式沟通，他们使用互联网作为媒体连接到专用LAN。VPN不断适应更多用户和不同的位置，比一条专线容易得多。实际上，可扩展性是 VPN 相对于一般租用线路的一大优势。与成本随距离而增长的专线方法不同，创建VPN几乎与办公室的地理位置无关。

VPN 技术

设计良好的 VPN 有若干方法来确保您的网络连接和数据安全。

- **数据机密性** — 这可能是所有 VPN 实施提供的最重要服务。由于您的私有数据在公共网络中传播，因此数据机密性至关重要，它可以通过对数据进行加密来实现。该流程是将一台计算机发送的所有数据发送到另一个计算机，然后以另一台计算机才能解码的形式进行编码。多数 VPN 使用这些协议中的一种来提供加密。**Ipsec —** Internet 协议安全协议 (IPsec) 能够提供增强的安全功能，如更强大的加密算法和更全面的身份验证。IPsec 有两种加密模式：隧道模式和传输模式。当隧道模式只加密有效载荷时，传输模式加密报头和每个信息包的有效载荷。只有与 IPsec 兼容的系统才能利用此协议。并且，所有设备必须使用一个普通密钥或认证，并且必须设置非常相似的安全策略。对远程访问虚拟专用网用户来说，第三方软件程序包的某种表提供了用户PC的连接和加密。IPsec 支持 56 位（一重 DES）或 168 位（三重 DES）加密。**PPTP/MPPE** - PPTP 由 PPTP 论坛创建，该协会由 US Robotics、Microsoft、3COM、

Ascend 和 ECI Telematics 组成。PPTP 支持多协议 VPN，使用 Microsoft 点对点加密 (MPPE) 协议实现 40 位和 128 位加密。请务必注意，PPTP 自身不提供数据加密。**L2TP/IPsec** — 通常被称为 L2TP over IPsec，它在第二层隧道协议 (L2TP) 的隧道上提供 IPsec 协议安全的安全性。L2TP是PPTP论坛成员、Cisco和互联网工程任务组(IETF)合作开发的产品。主要用于 Windows 2000 操作系统上的远程访问 VPN，因为 Windows 2000 提供了一个本地 IPsec 和 L2TP 客户端。网络服务提供商还可以为拨号用户提供 L2TP 连接，然后使用 IPsec 对接入点和远端办公网络服务器之间的流量进行加密。

- **数据完整性** — 尽管在公共网中对数据加密很重要，但确保数据在传输过程中没有被修改也很重要。例如，IPsec 提供了一种机制，可以确保数据包的加密部分或数据包的整个报头及数据部分没有被篡改。如果检测到篡改，数据包会被丢弃。数据完整性也可以包括对远程对等体进行身份验证。
- **数据来源验证** — 验证发送数据的源的身份非常重要。这是必要防护装置，可以防御基于发送器身份伪装的大量攻击。
- **反重放** — 此项功能可以检测并拒绝被重放的数据包，以防止被欺骗。
- **数据隧道/数据流机密** - 建立隧道是在另一个信息包之内封装整个信息包，在网络上发送的过程。如果想隐藏产生数据流的设备身份，数据隧道是一种十分有用的方法。例如，使用 IPsec 的单个设备对属于多个主机（位于设备后面）的流量进行封装，并在现有数据包顶部添加自己的报头。通过对原始信息包和报头进行加密(并且根据处于顶部的第三层报头路由信息包)，隧道设备能有效地隐藏信息包的实际来源。只有受信任的对等体在剥离附加的报头并对原始报头进行解密后，才能确定真正的源。如RFC 2401所注释...通信的外部特性的描述在一些情况下也可以是需要关心的问题。 数据流机密性是一种服务，它隐藏了源地址和目的地址、消息长度或通信频率。在 IPsec 上下文中，在隧道模式特别是在安全网关中使用 ESP，能够提供一定级别的数据流机密性。此处所列出的所有加密协议也使用隧道在公共网络上传输加密数据。需要特别注意的是，隧道本身不提供数据安全保护。原始信息包只封装在另一个协议中，如果未加密，信息包捕获设备仍然可视。然而，它在这里提及是因为它是VPN如何起作用的不可缺少的一部分。建立隧道需要三种不同的协议。**乘客协议** — 传送的原始数据（IPX、Netbeui、IP）。**封装协议** — 用于包装原始数据的协议（GRE、IPsec、L2F、PPTP、L2TP）。**载体协议** — 网络用于传输信息的协议。原始信息包(乘客协议)在封装协议内部加密，然后放在载波协议报头内(通常为IP) 为在公共网络上进行传输。请注意，封装协议也经常对数据进行加密。像 IPX 和 NetBeui 这样一般不通过 Internet 传输的协议可以实现安全传输。对于站点到站点 VPN，封装协议通常为 IPsec 或通用路由封装 (GRE)。GRE包括关于您在封装什么类型的信息包的信息和在客户端和服务器之间连接的信息。对于远程访问 VPN，通常使用点对点协议 (PPP) 建立隧道。作为ICP/IP协议栈的一部分，PPP在主机计算机和远程系统之间进行网络通信时为其他IP 协议提供载体。PPP 建立隧道将使用 PPTP、L2TP 或 Cisco 的第二层转发 (L2F) 协议中的一种。
- **AAA** —认证、授权和记帐使用更多安全访问在远程访问VPN环境。无需用户身份验证，任何使用装有预配置 VPN 客户端软件的便携式计算机或 PC 的用户都可以与远程网络建立安全连接。但如果使用用户身份验证，还需要输入有效的用户名和口令才能完成连接。用户名和密码可以保存在VPN 自己的 终端设备上或外部AAA服务器上（该服务器为大量其他数据库，如Windows NT、Novell、LDAP等提供认证）。设立隧道的请求来自拨号客户端时，VPN设备将提示输入用户名和密码。这些信息随后在本地进行验证，或发送到外部 AAA 服务器，检查以下各项：您是谁（身份验证）您可以执行什么操作（授权）您实际执行了什么操作（记帐）记帐信息对于追踪客户端的安全审计、计费或报告目的特别有用。
- **不可否认性** - 在某些数据传输中，特别是那些与金融交易有关的传输，不可否认性是一个非常需要的特性。这有助于防止处理中一端拒绝的情况发生。与银行要求您在承兑支票前签字一样，验证操作是将数字签名附加到已发送的信息上，然后排除发送方拒绝参与交易的可能性。

有很多协议能够用于构建 VPN 解决方案。所有这些协议都能提供本文档中所列出的部分服务。协议的选择取决于所需的服务。例如，一个组织可能喜欢以明文形式传输的数据，但对保持数据的完整性十分关注；而另一个组织可能认为保持数据的机密性绝对重要。因此他们选择的协议会有所不

同。有关可以使用的协议，以及各个协议的相对优势的详细信息，请参阅哪种 VPN 解决方案适合您？

VPN 产品

根据 VPN 的类型（远程访问或站点到站点），您需要准备特定的组件来构建 VPN。其中可能包括：

- 每个远程用户的桌面软件客户端
- 专用硬件，如 Cisco VPN 集中器或 Cisco Secure PIX 防火墙
- 用于提供拨号服务的专用 VPN 服务器
- 服务提供商用于为远程用户提供 VPN 访问的网络接入服务器 (NAS)。
- 专用网络和策略管理中心

由于实施VPN没有广泛的接受标准，所以许多公司自己开发整合解决方案。例如，Cisco 提供的几个 VPN 解决方案包括：

- **VPN 集中器** — Cisco VPN 集中器结合了最先进的加密和身份验证技术，专用于建立远程访问或站点到站点 VPN，特别适合需要单个设备处理大量 VPN 隧道的应用环境。VPN集中器是为解决一个满足专用的远程访问虚拟专用网设备的需求而特别开发的。集中器提供高可用性、高性能的和高可扩展性，并且提供包括可扩展加密处理(SEP)模块在内的组件，这使用户能够轻松增加容量和吞吐量。"集中器提供适合10个0或更少远程访问用户的小型企业，也适合最多具有10,000个同步远程用户的大型企业。"
- **启用 VPN 的路由器/VPN 优化路由器** — 所有运行 Cisco IOS® 软件的 Cisco 路由器都支持 IPsec VPN。唯一的要求是，路由器必须运行具有适当功能集的 Cisco IOS 镜像。Cisco IOS VPN 解决方案完全支持远程访问、Intranet 和 Extranet VPN 需求。这意味着Cisco路由器在连接到运行VPN客户端软件的远程主机，或连接到另一个VPN设备（如路由器、PIX防火墙或者VPN集中器）时都能提供同样不错的操作。支持VPN的路由器适用于带有适度加密和隧道建立要求的VPN，能够通过Cisco IOS软件功能提供全部VPN服务。启用 VPN 的路由器包括 Cisco 1000、Cisco 1600、Cisco 2500、Cisco 4000、Cisco 4500 和 Cisco 4700 系列等等。Cisco 的 VPN 优化路由器可提供可扩展性、路由、安全保护和服务质量 (QoS)。路由器基于Cisco IOS软件，并能提供适合各种情况的设备，包括满足SOHO，中心站点VPN聚合接入的和大规模企业需要的各种设备。VPN优化的路由器设计能够满足严格的加密和隧道要求，并且经常使用其他硬件，如使用加密卡获得高性能。VPN 优化路由器包括 Cisco 800、Cisco 1700、Cisco 2600、Cisco 3600、Cisco 7200 和 Cisco 7500 系列等等。
- **Cisco 安全 PIX 防火墙** - 专用互联网交换 (PIX) 防火墙在单个硬件上结合了动态网络地址转换、代理服务器、信息包过滤、防火墙和 VPN 功能。该设备具有一个高度流线型的操作系统 ，而不使用Cisco IOS软件。该系统能够处理各种协议，提供集中于IP的强大稳健性的和性能。与 Cisco 路由器一样，所有型号的 PIX 防火墙均支持 IPsec VPN。所有需要的是必须符合启用 VPN功能的许可权要求。
- **Cisco VPN 客户端** — Cisco 同时提供硬件和软件 VPN 客户端。Cisco VPN 客户端（软件）是 Cisco VPN 3000 系列集中器附带的，不需要额外费用。此软件客户端可以在安装主机上，或者用来安全连接到中心站点集中器上(或其他VPN设备，如路由器或防火墙)。VPN 3002硬件客户端是在每台机器上部署VPN客户端软件，并为数个设备提供VPN连接的备选方案

您用来构建VPN解决方案的设备最终是要素数量设计的问题，包括期望的吞吐量和用户数量。例如，在某个拥有少量 PIX 501 用户的远程站点上，您可以考虑将现有 PIX 配置为 IPsec VPN 终点，前提是您能够接受大约 3 Mbps 的 PIX 501 3DES 吞吐量，以及最多 5 个 VPN 对等体的限制。另一方面，在充当VPN端点的中心站点（供大量VPN隧道使用）上请求VPN优化路由器或VPN集中器都是不错的想法。选择现在将取决于要建立的VPN隧道类型(LAN对LAN 或远程访问)和编号。支持

VPN的广泛Cisco设备，可以为网络设计者提供极大的灵活性和强大的解决方案，来满足每一种设计需求。

相关信息

- 了解 VPDN
- 虚拟专用网络 (VPN)
- Cisco VPN 3000 系列集中器支持页面
- Cisco VPN 3000 Client 支持页
- IPsec 协商/IKE 协议支持页
- PIX 500 系列防火墙支持页
- RFC 1661：点对点协议 (PPP)
- RFC 2661：第二层隧道协议“L2TP”
- 工作原理：虚拟私有网络如何工作
- VPN 概述
- Tom Dunigan 的 VPN 网页
- 虚拟私有网络协会
- 请求注解 (RFC)
- 技术支持 - Cisco Systems