虚拟专用网络工作原理

Contents

Introduction

本文档介绍有关 VPN 的基础知识，例如基本 VPN 组件、技术、隧道和 VPN 安全性。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

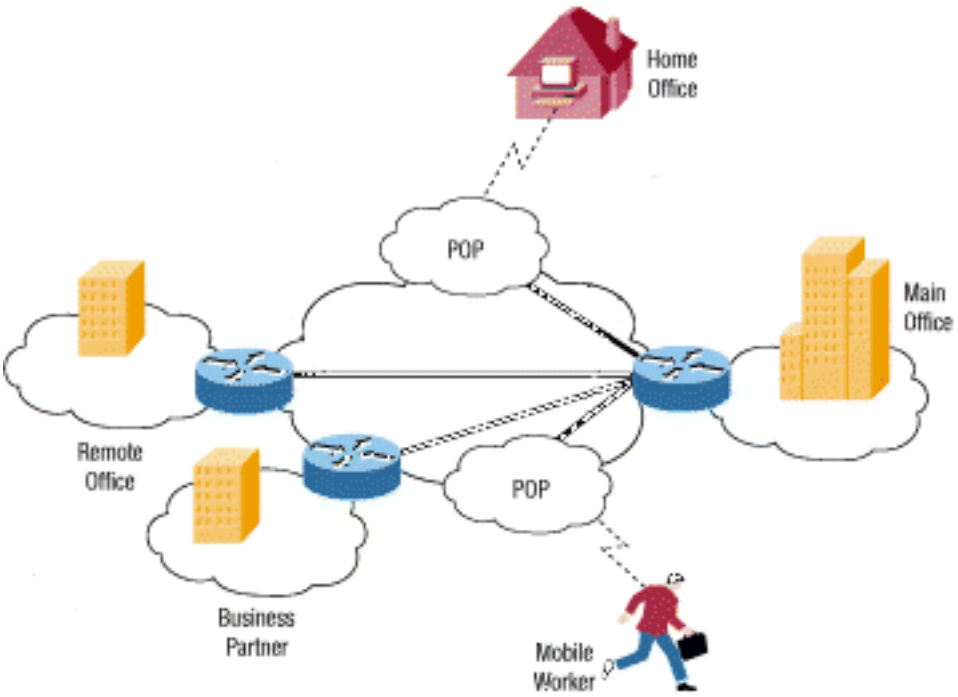
背景信息

世界在过去几十年里发生了很大变化。现在，许多企业不单单要应对本地或区域问题，还要考虑到全球市场和物流。许多公司的工厂遍布整个国家/地区，甚至遍布全球。但所有这些公司都有一个共同的需求，即：无论办公地点位于何处，都能通过某种途径，确保快速、安全和可靠地通信。

直到最近，实现可靠通信还意味着需要依靠租用线路来维持广域网 (WAN) 连接。从综合业务数字网（ISDN，运行速率为 144 Kbps）到光纤载波等级 3（OC3，运行速率为 155 Mbps）光纤等，租用

线路通过各种介质为公司提供一种将专用网络扩展到临近地理区域之外的途径。与互联网等公共网络相比，WAN 在可靠性、性能和安全性方面都具有明显的优势；但是要维持 WAN 连接（特别是在使用租用线路的情况下），成本可能会相当高昂，而且随着各办公地点之间距离的增加，成本往往也会增加此外，如果组织中存在一些高度仰赖移动办公的人员（例如营销人员），并且可能经常需要远程连接公司网络并访问敏感数据，那么租用线路并不是一个切实可行的解决方案。

随着互联网的兴起，企业开始寻求利用互联网来扩展他们的网络。首先是内联网，这是一种专供公司员工使用而设计的站点。现在，很多公司都搭建了自己的虚拟专用网网络 (VPN)，以满足远程员工和远程办公地点的需求。



一个典型的 VPN 可能包括公司总部的主局域网 (LAN)、远程办公地点或分支机构的其他 LAN，以及从公司网络外部连接进来的个人用户。

VPN 是一种使用公共网络（通常是互联网）将远程站点或用户连接起来的专用网络。VPN 不使用“真实”的专用连接（如租用线路），而是使用通过互联网实现的“虚拟”连接，将公司的专用网络与远程站点或员工连接到一起。

VPN 有哪些组成要素？

常见的 VPN 有两种。

- **远程访问 VPN** - 也称为虚拟专用拨号网络 (VPDN)。这是一种用户到 LAN 的连接，用于员工需要从各种远程位置连接到专用网络的公司。通常，如果公司希望搭建大型远程访问 VPN，都会借助于互联网服务提供商 (ISP) 来向用户提供某种形式的互联网拨号账户。然后，远程办公人员可以拨打 1-800 号码连接到互联网并使用 VPN 客户端软件访问公司网络。比如说，拥有数百名销售人员的大型公司就是需要使用远程访问 VPN 的典型示例。远程访问 VPN 能够通过第三方服务提供商在公司专用网络和远程用户之间实现加密的安全连接。
- **站点间 VPN** - 利用专用设备和大规模加密，公司可以通过公用网络（如互联网）连接多个固定站点。每个站点只需要在本地建立与相同公共网络的连接，从而避免因使用长距离专用线路而产生高昂费用。站点间 VPN 可进一步分为内联网或外联网。在同一家公司的办公地点之间构建的站点间 VPN 称为内联网 VPN，而用于将公司连接到其合作伙伴或客户的 VPN 称为外联网

VPN。

设计优良的 VPN 可使公司大大受益。例如，它可以：

- 扩展地理连接
- 降低运营成本（同传统 WAN 相比）
- 减少远程用户的交通时间和差旅费用
- 提高工作效率
- 简化网络拓扑
- 提供全球联网机会
- 提供远程办公支持
- 加快投资回报 (ROI) 速度（同传统 WAN 相比）

设计优良的 VPN 需要哪些功能？它应当集成：

- 安全
- 可靠性
- 可扩展性
- 网络管理
- 策略管理

打个比喻：每个 LAN 都是一座岛

假设您生活在广袤海洋中的一个岛上。您周围还有成千上万座其他岛屿，有一些离得非常近，有一些则离得很远。要去其他岛，通常的方式是从您所在的岛乘船前往要去的地方。当然，乘船也就意味着您几乎毫无隐私可言。无论您做什么别人都能看到。

现在我们把每一个岛看成一个专用局域网，而海洋就是互联网。乘船出行类似于通过互联网连接到某个 Web 服务器或另一台设备。您无法控制组成互联网的电缆和路由器，正如您无法控制船上的其他人。因此，如果您尝试利用公共资源连接两个私有网络，将很容易受到安全问题的困扰。

您所在的岛决定建造一座通往另一座岛的桥梁，以便两岛上的人可以更方便、更安全地直接往来。即使要连接的两座岛靠得很近，建造和维护桥梁的费用仍会非常高昂。但是，由于您特别需要找到一种能在岛间安全可靠往来的通道，所以您不顾一切地建了这座桥。您所在的岛可能还想同另外一个离得稍远的岛建立连接，但最终发现无法承担那么高的成本。

这同使用租用线路的情况非常类似。桥（租用线路）独立于海洋（互联网），但它让您能够连接各座岛屿 (LAN)。很多公司选择这种线路，是因为需要安全可靠地连接自己的远程办公地点。不过，如果办公地点离得非常远，那么成本会高得难以承受，这和建造大跨度桥的情况一样。

那么，VPN 在这个比喻中间又有什么作用呢？我们可以给两个岛上的每位居民一艘小型潜水艇，并且这些潜水艇具有以下特点：

- 速度快。
- 无论您去哪里，都很容易随身携带。
- 它可以让您完全隐身，其他任何船只或潜水艇都看不到您。
- 可靠。
- 只要买了第一艘潜水艇，以后再买其他潜水艇时只需很少的钱。

尽管这两个岛上的居民还是和其他人一样在海上航行，但他们却可以随时穿梭往返，而不会存在隐私和安全性的问题。这本质上便是 VPN 的工作原理。您网络中的每位远程成员都可以将互联网用作连接到专用局域网的媒介，从而以安全、可靠的方式进行通信。与租用线路相比，VPN 还可以更

方便地扩大范围，从而适应更多用户和不同地点的需求。实际上，可扩展性是 VPN 相对于一般租用线路的一大优势。与成本随着距离的增加而增加的租用线路不同，各办公地点地理位置的远近对搭建 VPN 的影响是微乎其微的。

VPN 技术

设计优良的 VPN 使用多种方法确保您的连接和数据安全。

- **数据保密性** -这可能是任何 VPN 实施所提供的最重要的服务。您的私有数据是通过公共网络传输的，因此为数据保密就显得至关重要。这可以通过对数据进行加密来实现。在加密过程中，需要提取一台计算机要发送给另一台计算机的所有数据，并将这些数据编码为只有另一台计算机才能解码的形式。大多数 VPN 使用以下一种协议来提供加密。**IPsec -** 互联网协议安全协议(IPsec) 提供增强的安全功能，例如更强的加密算法和更全面的身份验证。IPsec 有两种加密模式：隧道和传输。隧道模式加密每个数据包的报头和负载，而传输模式仅加密负载。只有符合 IPsec 标准的系统才能利用此协议。此外，所有设备必须使用公共密钥或证书，并且必须设置非常类似的安全策略。远程访问 VPN 用户可以使用一些形式的第三方软件包在用户 PC 上提供连接和加密。IPsec 支持 56 位（单 DES）或 168 位（三重 DES）加密。**PPTP/MPPE** - PPTP 由 PPTP 论坛（由 US Robotics、Microsoft、3COM、Ascend 和 ECI Telematics 组成的联盟）开发。PPTP 支持多协议 VPN，使用称为 Microsoft 点对点加密 (MPPE) 的协议进行 40 位和 128 位加密。必须注意的一点是，PPTP 本身不提供数据加密。**L2TP/IPsec** - 通常称为 L2TP over IPsec，它提供了 IPsec 协议在第 2 层隧道协议 (L2TP) 的隧道之上的安全性。L2TP 由 PPTP 论坛、思科和互联网工程任务组 (IETF) 合作开发。主要用于使用 Windows 2000 操作系统的远程访问 VPN，因为 Windows 2000 提供本地 IPsec 和 L2TP 客户端。互联网服务提供商还可以为拨入用户提供 L2TP 连接，然后在其接入点和远程办公地点网络服务器之间使用 IPsec 来加密流量。
- **数据完整性** - 除了公共网络中对数据进行加密，验证数据在传输过程中未被更改同样非常重要。例如，IPsec 中的一种机制能够确保数据包的加密部分或数据包的整个报头和数据部分未被篡改。如果检测到篡改，数据包会被丢弃。数据完整性还涉及对远程对等点进行验证。
- **数据源身份验证** - 对所发送数据的来源进行身份验证具有重要意义。这对防范许多依靠假冒发件人身份来发动的攻击非常必要。
- **防重放** - 检测和拒绝数据包重放来防止欺骗。
- **数据隧道/流量保密性** - 隧道传输过程是指将整个数据包封装在另一个数据包中并通过网络发送。如果需要隐藏流量发起设备的身份，数据隧道会很有用。例如，使用 IPsec 的设备会将属于多个主机的流量封装在一起，并在现有数据包的顶部添加自己的报头。通过加密原始数据包和报头（以及在路由数据包时使用在顶部额外添加的第 3 层报头），隧道设备能够有效隐藏数据包的实际来源。只有受信任的对等点在删除其他报头并解密原始报头后才能确定真正的来源。正如 RFC 2401 中所述，“...在某些情况下，还需要关注披露通信的外部特征。流量保密性是通过隐藏源地址和目标地址、消息长度或通信频率来解决后一种问题的服务。在 IPsec 上下文中，在隧道模式下使用 ESP（特别是在安全网关处）可以提供某种程度的流量保密性。”此处列出的所有加密协议也使用隧道作为在公共网络上传输加密数据的方法。需要注意，隧道本身并不能提供数据安全性。原始数据包仅封装在另一个协议中，如果未加密，仍然可能通过数据包捕获设备看到。我们之所以要在这里提及这一点，是因为它是 VPN 功能不可或缺的组成部分。隧道需要三种不同的协议。**乘客协议** - 传输的原始数据 (IPX、NetBeui、IP)。**封装协议** - 原始数据的封装协议 (GRE、IPsec、L2F、PPTP、L2TP)。**运载协议** - 传输信息的网络使用的协议。原始数据包（乘客协议）封装在封装协议中，然后放入运载协议的报头（通常是 IP）中，以便通过公共网络进行传输。注意，封装协议也经常执行数据加密。通常不会通过互联网传输的协议（IPX 和 NetBeui 等）可以保证安全、可靠地传输。对于站点间 VPN，封装协议通常是 IPsec 或通用路由封装 (GRE)。GRE 包括有关您要封装的数据包类型以及有关客户端和服务器

之间连接的信息。对于远程访问 VPN，隧道通常使用点对点协议 (PPP) 执行。作为 TCP/IP 堆栈的一部分，PPP 是在主机和远程系统之间通过网络进行通信时其他 IP 协议的载体。PPP 隧道将使用 PPTP、L2TP 或思科的第 2 层转发 (L2F) 其中的一种。

- **AAA** -身份验证，授权和记帐用于在远程访问 VPN 环境中进行更安全的访问。如果不进行用户身份验证，那么无论是谁，只要能接触到具有预配置 VPN 客户端软件的笔记本电脑/PC，都将可以建立到远程网络的安全连接。在进行用户身份验证后，仍然必须输入有效的用户名和密码，才能完成连接。用户名和密码可以存储在 VPN 终端设备本身或外部 AAA 服务器上，后者可以为许多其他数据库（如 Windows NT、Novell、LDAP 等）提供身份验证。当从拨号客户端发出建立隧道的请求时，VPN 设备会提示输入用户名和密码。然后可以在本地对其进行身份验证，或者将其发送到外部 AAA 服务器，由其进行检查：您是谁（身份验证）您被允许做什么（授权）您实际做了什么（记帐）记帐信息对于跟踪客户端用于安全审核、计费或报告目的特别有用。
- **不可否认性** - 在某些数据传输中，特别是与金融交易相关的数据传输中，不可否认性是非常理想的功能。这有助于防止一端否认参与了交易的情况。就像银行在兑现支票之前需要您的签名一样，不可否认性通过在发送的消息上附加数字签名来实现，从而排除发件人否认参与了交易的可能性。

存在许多可用于构建 VPN 解决方案的协议。所有这些协议都提供本文档中列出的某些服务子集。协议的选择取决于所需的服务集。例如，一个组织可能会对以明文形式传输的数据感到满意，但却非常关心维护其完整性，而另一个组织可能会发现维护数据保密性是绝对必要的。因此，他们对协议的选择可能不同。有关可用协议及其相对优势的更多信息，请参阅哪种 VPN 解决方案适合您？

VPN 产品

根据 VPN 的类型（远程访问或点到点），您需要安装某些组件来构建 VPN。这些组件可能包括：

- 每个远程用户的桌面软件客户端
- 专用硬件，如思科 VPN 集中器或思科安全 PIX 防火墙
- 用于拨号服务的专用 VPN 服务器
- 服务提供商用于远程用户 VPN 访问的网络访问服务器 (NAS)
- 专用网络和策略管理中心

由于没有广泛接受的 VPN 实施标准，许多公司自己开发了统包解决方案。例如，思科提供多种 VPN 解决方案，包括：

- **VPN 集中器** - 结合最先进的加密和身份验证技术，思科 VPN 集中器专门用于创建远程访问或站点间 VPN，非常适合部署在需要单个设备处理大量 VPN 隧道数据的环境中。VPN 集中器专门用于满足专用远程访问 VPN 设备的要求。集中器提供高可用性、高性能和可扩展性，并包含称为可扩展加密处理 (SEP) 模块的组件，使用户能够轻松提高容量和吞吐量。这些集中器适用于拥有 100 个或更少远程访问用户的小型企业，也适用于拥有多达 10,000 个并发远程用户的大型企业组织。

- **支持 VPN 的路由器/VPN 优化路由器** - 所有运行思科 IOS® 软件的思科路由器都支持 IPsec VPN。唯一的要求是，路由器必须运行具有相应功能集的思科 IOS 映像。思科 IOS VPN 解决方案完全支持远程访问、内联网和外联网 VPN 要求。这意味着，当连接到运行 VPN 客户端软件的远程主机或连接到其他 VPN 设备（如路由器、PIX 防火墙或 VPN 集中器）时，思科路由器可以同样正常工作。支持 VPN 的路由器适用于具有中等加密和隧道要求的 VPN，并完全通过思科 IOS 软件功能提供 VPN 服务。支持 VPN 的路由器的示例包括思科 1000、思科 1600、思科 2500、思科 4000、思科 4500 和思科 4700 系列。思科的 VPN 优化路由器提供可扩展性、路由、安全性和服务质量 (QoS)。这些路由器基于思科 IOS 软件，从小型办公室/家庭办公室 (SOHO) 访问到中央站点 VPN 聚合，再到大规模企业需求，这些路由器提供适用于各种情况的设备。VPN 优化路由器旨在满足高加密和隧道要求，并且通常使用其他硬件（如加密卡）来实现高性能。VPN 优化路由器的示例包括思科 800、思科 1700、思科 2600、思科 3600、思科

7200 和思科 7500 系列。
- **思科安全 PIX 防火墙** - 专用互联网交换 (PIX) 防火墙在单个硬件中结合了动态网络地址转换、代理服务器、数据包过滤、防火墙和 VPN 功能。该设备不再使用思科 IOS 软件，而是采用了高度精简的操作系统，通过专注于 IP，它能够处理各种协议，从而实现极高的稳定性和性能。与思科路由器一样，PIX 防火墙的所有型号都支持 IPsec VPN。所需要的只是必须满足启用

VPN 功能的许可要求。
- **思科 VPN 客户端** - 思科提供硬件和软件 VPN 客户端。思科 VPN 客户端（软件）与思科 VPN 3000 系列集中器捆绑在一起，无需额外费用。此软件客户端可以安装在主机上，用于安全连接到中央站点集中器（或任何其他 VPN 设备，如路由器或防火墙）。VPN 3002 硬件客户端是在每台计算机上部署 VPN 客户端软件，并为许多设备提供 VPN 连接的替代方案。

您用于构建 VPN 解决方案的设备选择最终是一个设计问题，取决于许多因素，包括所需的吞吐量和用户数量。例如，在 PIX 501 背后有少数用户的远程站点上，您可以考虑将现有 PIX 配置为 IPsec VPN 端点，前提是您接受 501 的 3DES 吞吐量约为 3 Mbps，并且最多只能有 5 个 VPN 对等点。另一方面，在充当大量 VPN 隧道的 VPN 端点的中心站点上，采用 VPN 优化路由器或 VPN 集中器可能是个不错的主意。现在的选择具体取决于类型（LAN 到 LAN 或远程访问）和正在建立的 VPN 隧道的数量。支持 VPN 的各种思科设备为网络设计人员提供了高度灵活性和强大的解决方案，可满足各种设计需求。

Related Information

- 了解 VPDN

- 虚拟专用网络 (VPN)
- 思科 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 系列防火墙支持页面
- RFC 1661：点对点协议 (PPP)
- RFC 2661：第 2 层隧道协议“L2TP”
- 工作原理：虚拟专用网络工作原理
- VPN 概述
- Tom Dunigan 的 VPN 页面
- 虚拟专用网络联盟
- 请求注解 (RFC)
- Technical Support - Cisco Systems