虚拟专用网络如何工作

目录

简介

本文包括VPN基本原理，例如基本的VPN组件、技术、隧道和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。

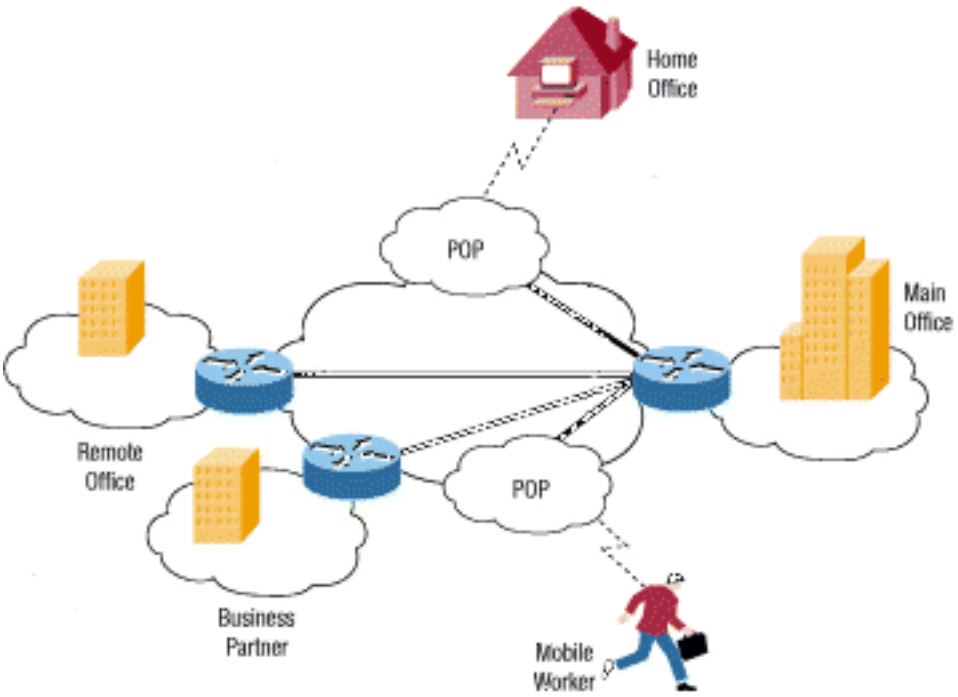
背景信息

世界很多在过去的二三十年里更改了。而不是处理本地或地域性关心，许多企业必须当前考虑全球市场和采购管理系统。许多公司安排设施传播全国各地，甚至环球。但是有所有公司需要的一件事：方式维护快速地，安全和可靠的通信，无论哪里找出他们的办公室。

近来，可靠的通信意味着使用租用线路维护一个广域网(广域网)。租用线路，范围自综合业务数字网络(ISDN，运行在144 Kbps)到光学载波-3 (OC3，运行在155 Mbps)光纤，提供一家公司方式扩展

他们的在他们的立即地理区域之外的专用网络。广域网有明显的优势超过一个公共网络类似互联网当谈到可靠性、性能和安全;但是维护广域网，特别当曾经租用线路时，可能变得相当消耗大(经常它费用提高，当办公室之间的距离增加)。另外，租用线路不是一部分的工作人员是高移动的组织的一个可行的解决方案(对销售人员通常就是这样)并且也许频繁地需要远程连接到公司网络和访问敏感数据。

当互联网的大众化增长，企业转向了它作为扩大他们自己的网络的方法。首先来内部网，是为使用仅设计的站点由公司员工。现在，许多公司创建他们自己的虚拟专用网络容纳异地的员工和远端办公室需要。



典型的VPN也许在公司的公司总部有一个主要局域网(LAN)，其他LAN在远程办公室或设施和从字段连接的个人用户。

VPN是使用一个公共网络的一个专用网络(通常互联网)一起连接远程站点或用户。而不是使用专用，真实世界的连接，例如租用线路， VPN使用“通过互联网路由的虚拟”连接从公司的专用网络与远程站点或员工。

什么做VPN ？

有VPN的两种常用类型。

- **远程访问**—并且呼叫虚拟专用拨号网络(VPDN)，这是有员工需要连接到从多种远端位置的专用网络的公司使用的用户到LAN连接。一般，希望设置一大远程访问VPN的公司提供互联网拨号帐户的某种表给他们的使用互联网服务提供商(ISP)的用户。远程办公者能然后拨打1-800号码到达互联网和使用他们的VPN客户端软件访问公司网络。需要远程访问VPN公司的一个好例子是与数百的一个大固定字段的销售员。远程访问VPN通过第三方服务服务供应商允许公司的专用网络和异地用户之间的安全，加密的连接。
- **站点到站点**—通过使用专用设备和大规模加密，公司能连接在一个公共网络的多个固定的站点例如互联网。每个站点需要与同一个公共网络的仅本地连接，从而存金钱在长的专用的专线。站点对站点VPN可以进一步分类到内部网或企业间网路。而被构件的VPN连接公司到其合作伙伴或用户指外联网VPN， Site to Site VPN被建立在同一家公司办公室之间被认为内部网VPN。

设计好的VPN能非常地有益于公司。例如，它能：

- 延伸地理连接
- 降低运作成本与传统广域网
- 降低转接时间和差旅费用异地用户的
- 改进生产率
- 简化网络拓扑
- 提供全球联网机会
- 提供远程办公者技术支持
- 比传统广域网提供更加快速的投资回报(ROI)

什么功能必要在设计好的VPN ？它应该合并这些项目：

- 安全
- 可靠性
- 可扩展性
- 网络管理
- 策略管理

类比：每个LAN是海岛

想象您在一个海岛上居住在巨大的海洋。有千位其他海岛所有在您，某非常接近和其他附近。正常方式移动将乘从您的海岛的一条轮渡到海岛您希望访问。移动在轮渡意味着您没有几乎保密性。您的任何能由别人看到。

假设，每个海岛表示专用LAN，并且海洋是互联网。当您乘轮渡时传播，类似于，当您连接到Web服务器或到另一个设备到互联网时。您不掌握金属丝，并且组成互联网的路由器，正如您不掌握轮渡的其他人民。使用一种公共资源，如果设法连接在两个专用网络之间这使您受影响安全问题。

您的海岛决定建立网桥到另一个海岛，以便有更加容易，人的更加安全和直接方式能移动在两个之间。是消耗大的建立和维护网桥，即使您与连接的海岛非常接近。但是需要对于可靠，安全的路径是很极大的您无论如何执行它。您的海岛希望连接到是去的第二个海岛，但是您决定是太消耗大的。

此情况是类似有一条租用线路。网桥(租用线路)是分别于海洋(互联网)，他们能连接海岛(LAN)。许多公司选择了此路由由于对安全的在连接他们的远程办公室的需要和可靠性。然而，如果办公室离得很远，费用可以是费用很高-正如设法建立跨过了不起的距离的网桥。

因此VPN是否如何适合对此类比？我们可能产生我们的海岛每个居民他们有这些属性的自己小的潜水艇。

- 它快速。
- 采取与您是容易的，无论哪里您去。
- 能完全地躲藏起来从您所有其他小船或潜水艇。
- 它是可靠的。
- 一旦第一被购买，开销一点添加另外的潜水艇到您的舰队。

虽然他们在海洋移动与其他数据流一起，我们的两个海岛居民可能反复传送，每当他们希望对与保密性和安全。那根本是VPN如何工作。您的网络的每名远程成员能以一种安全和可靠的方式沟通使用互联网作为媒体连接到专用LAN。VPN比一条租用线路能增长适应更多用户和不同的位置容易。实际上，可扩展性是VPN有在典型的租用线路的一个主要优点。不同于费用以介入的距离的比例增

加的租用线路，每个办公室问题的地理位置一点在VPN的创建。

VPN技术

设计好的VPN使用几个方法为了保持安全您的连接和的数据。

- **数据保密性**—或许这是所有VPN实施提供的主服务。因为您的私有数据在一个公共网络传播，数据保密性是重要的，并且可以通过加密数据获得。这是采取一台计算机发送到另一个并且编码它到表的所有数据的进程仅另一台计算机能解码。多数VPN使用这些协议之一提供加密。**Ipsec**-互联网协议安全协议(IPsec)提供改进的安全功能例如强加密算法和更多全面的验证。IPsec有两个加密模式：隧道和传输。当传输模式只加密有效载荷时，隧道模式加密报头和每个信息包有效载荷。IPSec兼容仅的系统能利用此协议。并且，所有设备必须使用一个普通的键或认证，并且必须有非常相似的安全策略设置。对于远程访问VPN用户，第三方软件软件包的某种表在用户PC提供连接和加密。IPSec技术支持56位(单个DES)或168-bit (三DES)加密。**PPTP/MPPE** — PPTP是由PPTP论坛创建的，包括US Robotics、Microsoft、3COM、Ascend和ECI远程信息处理的协会。PPTP支持多协议VPN，与40位和128-bit加密使用称为Microsoft点到点加密(MPPE)的协议。请注意PPTP单独不提供数据加密。**L2TP/IPsec** —通常被呼叫的IPSec上的L2TP，这提供IPSec协议的安全在隧道的第2层隧道协议。L2TP是一家合伙企业的产品在PPTP论坛的成员， Cisco和互联网工程任务组(IETF)之间的。主要使用远程访问VPN与Windows 2000操作系统，因为Windows 2000提供一个本地IPSec和L2TP客户端。互联网服务提供商能为拨入用户也提供L2TP连接，然后加密与IPsec的该数据流在他们访问点和远程办公室网络服务器之间。
- **数据完整性**—当重要的是时您的数据在一个公共网络被加密，验证是正重要的未更改在运送中。例如， IPsec有保证一个的机制信息包的加密的部分或者信息包的整个报头和数据部分，未被窜改。如果发现窜改，信息包被丢弃。数据完整性能也介入验证远端对等体。
- **数据来源验证**—验证数据的来源的身份发送是非常重要的。这是必要防护装置防御取决于伪装发送方的身份的一定数量的攻击。
- **反重播**—这是能力发现，并且拒绝被重赛的信息包和帮助请防止伪装。
- **数据隧道/数据流机密性**—隧道是封装在另一个信息包内的一整个数据包和发送它的进程在网络。在隐藏产生数据流处的设备的身份是理想的数据隧道是有用的。例如，使用IPsec的单个设备封装属于在它后的一定数量的主机并且添加其自己的报头在现有的信息包顶部的数据流。通过加密原始信息包和报头(和路由根据另外的第三层报头的信息包添加在上面)，隧道设备有效隐藏信息包的实际来源。在剥离另外的报头并且解码原始报头后，仅委托的对等体能确定真正的源。在RFC 2401中注明 ，“…通信的外部特性的描述可以在某些情况下也是关心。数据流机密性是通过隐瞒源地址和目的地址、信息长度或者频率表达此后关心通信的服务。在IPsec上下文，使用ESP在隧道模式下，特别是在安全网关，能提供数据流机密性的某个级别”。列出的所有加密协议这里也使用隧道作为方法传递在间公共网络的加密的数据。意识到是重要的建立隧道，单独，不提供数据安全。原始信息包仅仅被封装在另一个协议里面，并且也许仍然是可视的对信息包捕获设备，如果没加密。然而，被提及在这儿，因为它是一个总体部分的VPN如何作用。隧道要求三个不同的协议。**乘客协议**—被传送的原始数据(IPX、NetBeui， IP)。**封装协议**—在原始数据附近包裹的协议(GRE， IPsec， L2F， PPTP， L2TP)。**载波协议**—信息移动的网络使用的协议。原始信息包(乘客协议)是被封装的里面封装的协议，然后放置在载波协议报头(通常IP)里面在公共网络的发射的。注意封装的协议相当经常也执行数据的加密。协议例如IPX和NetBeui，不会在互联网间通常调用，可能实现安全传输。对于站点对站点VPN，封装的协议通常是IPsec或通用路由封装(GRE)。GRE包括关于什么类型的信息包的信息您关于连接的封装和信息客户端和服务器之间。使用点对点协议(PPP)，对于远程访问VPN，建立隧道通常发生。当沟通在主机计算机和远程系统之间时的网络一部分的TCP/IP协议栈， PPP是其他IP协

议的载波。PPP建立隧道将使用一PPTP、L2TP或者思科的第二层转发。

- **AAA** —认证、授权和记帐使用更多安全访问在远程访问VPN环境。没有用户认证，坐在与预先配置的VPN客户端软件的laptop/PC的人能建立安全连接到远程网络。然而使用用户认证，在连接完成前，有效用户名和密码必须也输入。用户名和密码可以存储在VPN终端设备，或者在一个外部AAA服务器，能提供认证给许多其他数据库例如Windows NT， Novell， LDAP，等等。当请求设立隧道自一个拨号客户端时进来， VPN设备提示输入用户名和密码。这可能本地然后验证或被发送到外部AAA服务器，检查：谁您是(认证)什么您允许执行(授权)什么您实际上(记帐)记帐信息为追查安全审计的客户端使用，计费或报告目的是特别有用的。
- **不可否认性**—在某些数据传输，特别是那些与金融交易关连，不可否认性是一个高度需要的功能。这是有用的在防止一端拒绝在处理参与的情况。很象内存段在尊敬您的承兑前要求您的签名，不可否认性工作通过附有一个数字签名传送的信息，因而阻止拒绝参与处理的发送方的可能性。

能使用拟订VPN解决方案的一定数量的协议存在。所有这些协议提供在本文列出的服务的某子集。协议的选择取决于期望服务集合。例如，而另一个组织也许发现维护的数据保密性必不可少，组织也许满意对数据调用在明文，但是极端挂虑关于维护其完整性。协议他们的选择也许因而是不同的。关于可用的协议和他们的相对力量的更多信息，请参见哪种VPN解决方案适合您?

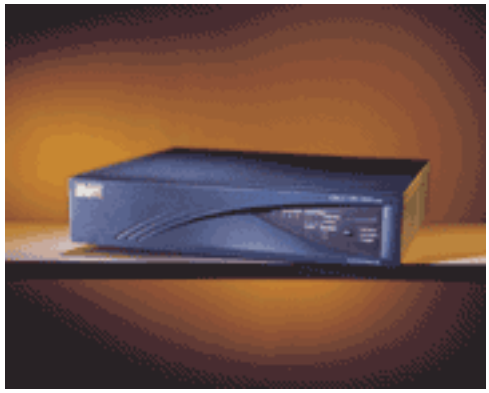
VPN产品

基于VPN的种类(远程访问或站点到站点)，您需要放在适当的位置某些组件构件您的VPN。这些也许包括：

- 每个异地用户的桌面软件客户端
- 专用硬件例如Cisco VPN集中器或Cisco Secure PIX防火墙
- 拨号服务的专用的VPN服务器
- 服务提供商(NAS)的网络接入服务器用于异地用户VPN访问
- 专用网络和策略管理中心

由于没有实现VPN宽被接受的标准，许多公司独自地提出了整合解决方案。例如， Cisco提供包括的几个VPN解决方案：

- **VPN集中器**—合并可用最先进的加密和验证技术， Cisco VPN集中器为创建远程访问或Site to Site VPN特别地被构件和理想地说配置需求是为了单个设备能处理一个非常大数目的VPN隧道的地方。VPN集中器特定开发解决为特定目的建造的需求，远程访问VPN设备。集中器提供高可用性、高性能和可扩展性并且包括组件，称为可扩展的加密处理(SEP)模块， enable (event)用户容易地增加容量和吞吐量。集中器在型号提供适用于与100个或少量远程访问用户



的小型企业对与10,000个同步远程用户的大型企业组织。
- **支持VPN的Router/VPN优化的路由器**—运行Cisco IOS软件支持IPsec VPN的所有Cisco路由器。唯一的要求是路由器必须运行Cisco IOS镜像以适当的功能集。Cisco IOS VPN解决方案支持远程访问、内部网和外联网VPN需求。这意味着Cisco路由器能同样好地工作，当连接到运行VPN客户端软件的一台远端主机或，当连接到另一个VPN设备例如路由器、PIX防火墙或者

VPN集中器。支持VPN的路由器为与适度加密和隧道需求的VPN是适当的并且通过Cisco IOS软件功能完全地提供VPN服务。支持VPN的路由器示例包括Cisco 1000、Cisco1600、Cisco2500、Cisco4000，Cisco4500和Cisco 4700系列。思科的VPN优化的路由器提供可扩展性、路由、安全和服务质量(QoS)。路由器根据Cisco IOS软件，并且有设备适用于每个情况，从small office/home office (SOHO)访问通过中心站点VPN聚合对大规模企业需要。VPN优化的路由器设计符合高加密和隧道要求和经常利用另外的硬件例如加密卡完成高性能。VPN优化的路由器示例包括Cisco 800、Cisco 1700、Cisco2600、Cisco3600，Cisco7200和

Cisco7500系列。

- **Cisco Secure PIX防火墙**—专用互联网交换(PIX)防火墙结合动态网络地址转换、代理服务器、信息包过滤、防火墙和VPN功能在硬件单件。而不是使用Cisco IOS软件，此设备有交换能力通过着重处理极其抗错性和性能的各种各样的协议IP的一最新型操作系统。如同Cisco路由器，所有PIX防火墙型号支持IPSec VPN。需要的所有是必须符合对enable (event)的许可权要求

VPN功能。

- **Cisco VPN Client** — Cisco提供硬件与软件VPN客户端。Cisco VPN Client (软件)来没有外加费用捆绑与Cisco VPN 3000 Series Concentrator。此软件客户端可以在主机上安装和使用安全地连接到中心站点集中器(或到其他VPN设备这样路由器或防火墙)。VPN 3002硬件客户端是选择对配置在每台机器的VPN客户端软件并且提供VPN连接给一定数量的设备。

您会使用拟订您的VPN解决方案设备的选择根本地是取决于一定数量的要素，包括期望吞吐量和用户的数量的设计问题。例如，在大致接受501's 3DES吞吐量3 Mbps和最多的限制5个VPN对等体条件下，在有少数用户的一个远程站点在PIX 501背后，您可能考虑配置现有的PIX作为IPSec VPN终端。另一方面，在中心站点作为很大数量的VPN隧道的一个VPN终端，参加为VPN优化的路由器或VPN集中器很可能是一个好想法。选择当前将取决于VPN隧道的类型(LAN对LAN或远程访问)和编号设置的。支持VPN的大范围Cisco设备提供网络设计员极大量的灵活性和一个稳健解决方案适应每设计需要。

相关信息

- 了解VPDN
- 虚拟专用网络
- Cisco VPN 3000 Series Concentrators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 ：Layer Two Tunneling Protocol "L2TP"
- 东西如何工作：虚拟专用网络如何工作
- VPN概述
- 汤姆Dunigan的VPN页
- 虚拟专用网络协会
- 请求注解 (RFC)
- 技术支持 - Cisco Systems