

浅析 VPN 技术在企业网络建设中的应用

苑 宁

(沈阳有色金属研究院,辽宁 沈阳 110141)

摘 要:根据企业网络建设的需求,对目前应用广泛的 VPN 技术 IPsec VPN 和 SSL VPN 进行了分析比较,提出适合企业的 VPN 技术应用。

关键词:虚拟专用网络;IPsec VPN;SSL VPN;应用

中图分类号:TP393

随着国内企业重组和走出去步伐的加快,企业规模不断扩张,国内外子企业和分支机构越来越多,建设企业广域网实现企业内部信息沟通畅通,是在所有企业实行有效管理的共同需求。如何选择一种切实可行的解决方案,既能安全可靠地解决企业总部与分支企业和分支机构相互之间的安全通信及信息交换,又能最大限度保护原有投资,已经成为企业网络建设的迫切需求。应用 VPN (Virtual Private Network, 虚拟专用网络) 技术,为企业提供了解决方案。

1 VPN 技术

VPN 被定义为通过一个公用网络(通常是因特网)建立一个临时的、安全的连接,是一条穿过混乱的公用网络的安全、稳定的隧道。也可以说是虚拟出来的企业内部专线。VPN 技术能够提供可靠的数据加密、信息安全交换的能力,可采用的方案有点对点、用户对点、用户对用户的连接方式,它可以帮助远程用户、分支企业、分支机构、商业伙伴及供应商同企业内部网建立可信的安全连接,并保证数据的安全传输^[1-2]。VPN 具有以下优点:

1) 组网成本低廉。企业利用公用网组建的 Intranet,不再需要租用专线和使用大量的专业网管人员和设备,节省租用专线费用和人员开支。

2) 网络扩展性强。当增加新的用户或子网时,只需修改已有网络软件配置,在新增客户机或网关上安装相应软件并接入 Internet 后,新的 VPN 即可工作,其实现过程要比组建专用网简单。

3) 企业容易进行管理。用专线将企业的各个子网连接起来时,随着子网数量的增加,需要的专线数以几何级数增长。而使用 VPN 时只需要将各个子网接入 Internet 即可,不需要对各个线路进行管理。

4) 企业拥有控制权。VPN 应用中所有的设施和服务完全由企业掌握,企业可以把拨号访问交给网络服务提供商去做,而企业只负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。

5) 符合网络统一标准。VPN 通过采用“隧道”技术,并在 Internet 或国际互联网工程工作组(IETF)制定的 Ipsec 标准统一下,在公共网构建企业安全、机密、顺畅的虚拟专用链路。

2 VPN 的分类

VPN 既可以用于构建企业的 Intranet,也可以用于构建 Extranet。VPN 利用开放性的公用网络作为用户信息传输的媒体,通过附加的隧道封装、信息加密、用户认证和访问控制等技术实现对信息传输过程的安全保护,从而向用户提供类似专用网络的安全性能。VPN 技术按隧道协议分类,有 PPTP VPN、L2TPVPN、IPsec VPN、SSL VPN 和 MPLS VPN 等,目前有几种安全技术得到了较广泛的应用,每种技术都有自己的优点,同时也存在一定的不足。当前 VPN 领域内主流技术是 IPSEC VPN 与 SSL VPN,两者都应用于远程接入的加密和认证机制。

3 IPSEC VPN 与 SSL VPN 组网技术比较^[3]

3.1 IPSEC VPN 技术

IPSEC VPN 通过封装包的方法,通过 Internet 建立了一个通讯的隧道,通过这个通讯的隧道,就可以建立起网络的连接。IPSEC 是一套比较完整成为体系的 VPN 技术,它规定了一系列的协议标准。它为数据在通过公用网络在网络层进行传输时提供安全保障。

IPSec VPN 适用 Site to Site 组网。这是由于 IPSecVPN 采用隧道技术,部署时一般采用两端部署 VPN 网关方式。当企业总部和分支企业有很多 IT 设备时,采用 IPSec 组网方式比较灵活,支持应用广泛。组网时企业总部和分支机构分别采用 IPSEC VPN 网关设备,中心为每个节点分配一套密码,各个节点通过密码与中心交换机互相认证,建立 IP-SEC VPN 虚拟通路,这条通路的特性,如带宽、何时可以建立等通过中心统一管理,可以通过双密钥机制实现更加可靠的认证。

由于 IPSec VPN 部署在网络层,因此,内部网络对于通过 VPN 的使用者来说是透明的,一旦隧道建立外部用户能够直接访问企业全部的应用,由此会大大增加受到黑客攻击的风险,会严重威胁企业数据中心的安全。同时 IPSec VPN 部署管理复杂,最大的难点在于需要在隧道两端部署一对 VPN 网关,或是在客户端安装专用客户端软件,而且当用户的 VPN 策略稍微有所改变时,VPN 的管理难度将呈几何级数增长。尤其是对于大量的远端用户,除非已经在每一台客户使用的计算机上安装了管理软件,否则软件补丁的发布和远程电脑的配置升级将是一件十分繁琐的任务。

IPSec VPN 只能在部署 IPsec VPN 网关的地方适用,或者客户端安装专用软件后才能使用,这对于合作伙伴或商业客户来讲很难实现客户端专用软件安装,对于在网吧或出差等用户来讲就更不可能。

3.2 SSL VPN 技术

SSL(Secure Sockets Layer)“安全套接层协议层”,它是基于 WEB 应用的安全协议。SSL 协议指定了一种在应用程序协议(如 Http、Telnet、NMTTP 和 FTP 等)和 TCP/IP 协议之间提供数据安全性分层的机制,它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。SSL VPN 工作在 TCP 层,这个技术特性决定了它是一种基于应用的 VPN,可以更好的作为应用层的安全访问控制机制,并能够做到底层无关性,可以做到部署方式更灵活^[4]。

SSL VPN 一般的实现方式是在企业的防火墙后面放置一个 SSL 代理网关或接入服务器设备。如果用户希望安全地连接到公司网络上,那么当用户在浏览器上输入一个 URL 后,连接将被 SSL 代理服务器取得,并验证该用户的身份,然后 SSL 代理服务器将提供一个远程用户与各种不同的应用服务器之间连接。

SSL VPN 适用 Client to Site 组网。当客户端为 PC 终端设备时,采用此方式。当分支机构为少量终端或者 VPN 用户为分布在广泛地域的移动用户时更显优势。企业总部部署专用 SSL VPN 设备连接 Internet,分支企业和机构及移动用户通过 Internet 连接总部的 SSL VPN 服务器,经安全认证后即可使用各项应用,基本不用考虑计算机维护和相关网络安全。

SSL VPN 将远程安全接入延伸到 IPSec VPN 扩展不到的地方,使更多的员工在更多的地方,使用更多的设备安全访问企业网络资源。以前它只支持 WEB 方式的应用,为用户开发应用必须围绕着 WEB 来展开。现在新的 SSL VPN 能够实现各种基于 B/S、C/S 结构设计的应用程序,能够实现所有 IPSec VPN 支持的应用,支持 WINDOWS 网上邻居、FTP 等,SSL VPN 正在成为远程接入的事实标准。

由于 SSL VPN 是基于应用的 VPN,容易提供更细的访问控制,可以对用户、用户组的权限、资源、服务、文件进行更加细致的控制,重点在于保护具体的敏感数据。并可以与第三方认证系统、认证中心(CA)结合。就是说虽然都可以进入内部网络,但是不同人员可以访问的数据是不同的。不仅可以控制访问人员的权限,还可以对访问人员的每个访问、操作进行数字签名,为事后追踪提供了依据,达到更加安全的保护效果,充分保障企业数据中心的安全。

4 应用和结论

基于对 IPSEC VPN 与 SSL VPN 的分析比较适合现有分支企业的实际条件,在保护企业原有投资的基础上,企业总部采用两种技术相结合的方式通过网络接入。对于没有建设局域网或局域网环境较为简单的分支企业和机构,企业总部一般使用 SSL VPN 方式为企业用户建立 VPN 帐号,充分发挥企业现有网络的带宽资源。分支企业办公人员和出差人员可以随时随地以 SSL VPN 方式接入企业总部网络,满足各种办公环境下的网络通信需求,为了提高移动办公用户接入企业总部网络的安全性,针对 SSL VPN 用户可以在企业总部网络内搭建了 CA 认证服务器,对用户登录 VPN 时进行 CA 认证。对网络出口带宽足够大、边界部署了路由器或防火墙,基础网络建设比较好的分支企业,在它们的防火墙上配置 IPSEC VPN。这种局域网间的 VPN 方式提供直接、快速的加密通道,使分支企业的用户在使用总部网络资源时如同在总部一样安全快捷。(下转第 76 页)

.....
(上接第 30 页)

总之,通过 VPN 方式组建企业网络,能够经济、安全地实现企业内外部信息沟通,实现企业总部对分支企业运营状况及时了解和高效管理,掌握决策支持信息,从而达到提高企业信息化水平,提高企业竞争力和加快企业发展。

参考文献:

- [1] 王达. 虚拟专用网(VPN)精解[M]. 北京:清华大学出版社,2004.
- [2] 刘洋. IPSec VPN 和 SSL VPN 的分析比较[J]. 电脑知识与技术,2009(4):825-826.
- [3] 颜丙恒. 企业 VPN 多种技术方案比较研究[J]. 科技传播,2010(24):224.
- [4] 汪海航,谭成翔. VPN 技术的研究现状与发展趋势[J]. 计算程与应用,2001,23.