VPN 应用指南

VPN 应用指南

虚拟专用网络 VPN（Virtual Private Network ）能通过公用网络 Internet 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。VPN 是对企业内部网的扩展，它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。许多公司使用 VPN 向公司外部的员工提供企业网络接入。

VPN 的应用

VPN 虚拟专用网络我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样，但是它并不需要真正的去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。VPN 技术是路由器具有的重要技术之一，其核心就是在利用公共网络建立虚拟私有网。

- VPN和远程控制的区别是什么?
- 利用安全VPN远程访问　确保企业内部网络安全
- 使用VPN还是使用RPC/HTTPS?
- VPN安全：使用网络加密技术

Ipsec VPN 和 SSL VPN

SSL VPN 提供安全、可代理连接，只有经认证的用户才能对资源进行访问。SSL VPN 能对加密隧道进行细分，从而使得终端用户能够同时接入 Internet 和访问内

部企业网资源。IPSec VPN 通过在两站点间创建隧道提供直接（非代理方式）接入，实现对整个网络的透明访问；一旦隧道创建，用户 PC 就如同物理地处于企业 LAN 中。

- 连接处理金融事务的远程服务器必需Ipsec VPN吗？
- SSL VPN简化安全访问

VPN 的部署

VPN 能通过加密和安全过程维持安全性和私有性。VPN 的目的在于在分布式企业网络和企业合伙人之间，以及移动雇员和公司 IT 资源之间提供安全的通信。许多企业正在其服务器上使用 VPN 来准许其雇员从家里连接到公司服务器。VPN 的如此有价值，那么应当如何为企业部署 VPN 呢？

- 企业VPN部署指南
- VPN应该采用哪些防火墙控制？
- 解决Vista与VPN的兼容问题
- DMZ和VPN如何共存？
- 企业应该执行强制iPhone VPN吗？
- VPN是如何与即时通讯软件结合的?

支持分离通道的 VPN

分离通道技术允许 VPN 用户既可以通过 VPN 通道直接进行网络活动，同时又可以通过本地网络默认的网关进行另外的网络活动。如果你的目标是保护远程用户和工作场所之间的网络连接的安全，那么采用分离通道会比较好。

- 怎么在Vista操作系统中建立一个支持分离通道的VPN
- 分离通道功能会使VPN变得脆弱吗？

- 恶意软件能利用分离隧道的VPN入侵网络吗？

无线 VPN

早期的无线局域网经常使用远程访问虚拟专用网 （VPN）客户端，克服 WEP 和相关的安全装置的局限性。但是，假设 Wi-Fi 安全性已经得到了提高，VPN 在企业无线网中是否依然起到很大作用？在无线网中使用 VPN 的实际作用和局限性是什么呢？

- VPN在企业无线网中的作用
- 结合VPN与无线AP增强安全性

VPN和远程控制的区别是什么?

问：VPN 和远程控制的区别是什么？

答：虚拟专用网络（VPN）利用加密技术提供了一种通过因特网安全地连接到远程网络的方法。他们可以让你有效的“虚拟”访问办公室的物理网络，就像你在办公室一样。这种连接采用了加密技术，保护你的通信在通过因特网时不被窥探。许多企业利用 VPN 让出差和在家里工作的员工安全的访问公司的内部网络。

远程访问系统，例如微软远程桌面连接，虚拟网络计算（VNC）及类似产品，允许你用自己的鼠标和键盘来操纵通过网络连接的另一台电脑，就像你坐在那台电脑面前。如果你连接了一个远程系统，在你获取访问权之前将会被提示输入你的用户名和密码。

许多公司由于安全原因，协同采用这两种技术。想要进行远程控制公司网络中的电脑的用户必须首先连接到 VPN，然后建立远程访问连接。这种策略防止未知的因特网用户企图直接尝试未经授权的远程访问连接，提供了更多一层安全。

（作者：Mike Chapple 译者：Sean 来源：TechTarget中国）

利用安全VPN远程访问　确保企业内部网络安全

问：我们的企业在城市里有一主要的办事处，在距离主办事处约 150 英里远的地方有一个分支机构。我们需要非常安全的企业内部网络。传统的观点似乎是这样的：我们应该在主办事处配置一个单一的、带有防火墙的而且非常安全的因特网接入点。是否有不同的、更好一点的配置呢？如果考虑另一种配置，我应该注意哪些与安全有关的因素呢？

答：你所说的传统策略是一个常见的办法，它可以在一个接入点上小心的控制网络通信。然而，它也带来一些弊端：首先，它使得网络延迟了（用户感觉明显），因为它强制所有的网络流量都要经过主办事处的网络；其次，它有单点故障的风险，如果主办事处与网络失去了连接，那么分支机构办事处的网络也同样会失效。这不是一个好的拓扑结构，尤其是当你把分支机构办事处网站作为主办事处潜在的备份网站的时候。

我建议在两个办事处都配置因特网连接，并用 VPN 技术建立两个办公室之间沟通的安全通道。还有，你需要在两个地方都设置同样的防火墙和内容过滤机制，这样做可以充分保障两边的网络不会出现上面所提到的缺陷。

（作者：Mike Chapple　译者：Sean 来源：TechTarget中国）

使用VPN还是使用RPC/HTTPS?

人们如何从公司防火墙保护的环境外部安全地连接到微软的 Outlook?如果操作正确的话，通过 VPN(虚拟专用网)连接到 Outlook 是一种经过了试验和测试的安全方法。如果你的用户仅需要访问 Exchange，RPC over HTTPS 是一种安全的替代方法。

让我们快速看一下在互联网上把 Outlook 连接到 Exchange 的可能的方法。

·使用 SSL 的 Outlook Web Access(OWA over HTTPS)

·移动设备

·使用 MAPI/RPC 的完整的 Outlook(不要这样做!)

·使用 POP3 或者 IMAP4 的 Outlook

Outlook Web Access(OWA ,Outlook 网络接入):OWA 与每一个版本的 Exchange 一起进行了改进，是大多数用户使用的主要的远程连接方式。在 IIS(互联网信息服务器)的 /exchange 虚拟目录中启用“需要 SSL”和“需要 128 位加密”功能就很容易进行加密。

一个令人担心的 OWA 安全问题是，虽然信息是在磁盘上加密的，也许是在机场的售货亭加密的，但是，下载到硬盘的附件却没有加密。在 Exchange 2003 和 2000 软件中可能关闭这个功能。如果你需要一个允许这样加密文件的方法，Messageware 公司能够把文件在 Exchange 服务器上翻译成 HTTP 格式并且在安全的 OWA 窗口中显示出来。即将发布的 Exchange 2007 能够正确地处理这种情况。这个软件还允许安全访问内部文件和 SharePoint 站点，当然，这都是在管理控制下完成的。

移动设备:运行 Windows Mobile 操作系统的掌上设备正在日益流行。Exchange 包含让这些设备与 Exchange 服务器进行同步的功能。这个方式与 OWA 非常相似，你可以在 IIS 中的 Server-ActiveSync 虚拟服务器上部署 SSL(安全套接层)。此外，设备上必须有一份服务器的 SSL 证书。以前的版本可能会绕过这个功能，但是，现在不再能够绕过这个功能了。

完整的 Outlook:有些用户需要完整的 Outlook 客户端软件，这样，他们就能够有一个同步的邮箱。一般来说，这些用户群包括管理、销售、移动市场营销小组以及其它移动信息工人。

虽然使用本地的 MAPI/RPC 协议让 Outlook 实现在互联网上的连接是可能的，但是，我们无法打开我们防火墙上的端口实现这种连接。安全突破...、恶意软件...、职业限制措施等让我们无法实现这种连接。

POP3/IMAP4:使用 Outlook 连接到使用 POP3 或者 IMAP4E 的 Exchange 是可能的。它们都可以进行 SSL 加密，SMTP 也可以加密(POP3 和 IMAP4 使用 SMTP 作为他们的发送协议)。你可以在家里使用这些协议连接到一个 ISP 以便收发电子邮件。但是，大多数企业 Exchange 用户部门都在 Exchange 服务器上都关闭了这些功能，他们不打开他们的防火墙上的这些端口。

我们认为 VPN 是安全的，尽管 VPN 需要一个懂得如何管理它们的管理员。我的意思是你需要具体了解哪一些用户或者用户群能够访问哪些资源。安装一台 VPN 机器让所有的用户访问整个网络是很容易的。不过，我对使用 VPN 最担心的问题是有些用户把家里的计算机连接到企业网络。是的，有些用户整天都在玩计算机。SearchSecurity.com 网站有许多关于 VPN 的文章。Outlook 在这种环境下的工作是非常好的。Outlook 2003 的缓存功能允许移动邮件实现真正的后台处理。

如果你的一些旅行用户仅需要访问 Exchange，不需要访问你的内部网络，有一种替代的方法。RPC over HTTPS 接收 Outlook 数据包(MAPI/RPC)，然后让这些数据包通过隧道穿过加密的 HTTPS。回到你的环境内部，一个 RPC 代理服务可以解密这个数据包并且连接到 Exchange 服务器。。

应该指出的是，随着 2007 年的一批新产品的推出，RPC over HTTPS 将有一个新的名字:“Outlook Anywhere”。虽然老的名字说起来很容易，但是，新名字明确说出了它能做什么。

(作者：W. Lee Benjamin　来源：TechTarget中国)

VPN 安全：使用网络加密技术

作为一个分析师，我收到了越来越多的询问有关网络加密、加密的传输或者虚拟专用网安全的问题。也许那是因为担心遭到 TJ Maxx 的母公司 TJX、Marshalls 和 HomeGoods 商店等公司曾经历过的安全突破。当一个黑客利用明尼苏达州圣保罗附近的 Marshalls 服装商店的 Wi-Fi 网络的漏洞的时候(点击查看此事件)，数百万信用卡受到了损害。

遭遇安全突破的并不仅仅是 TJX 公司。还有一些引人注目的个人数据被突破的事件，包括美国政府内部 80%的现役军人的名字的个人数据被突破。这些事件促使美国政府下达一个行政命令，要求对传送和保存的个人身份识别数据采取加密措施。

我经常同网络工程师谈论有关加密传输中的数据的问题。在这里，我首先介绍加密传输的 VPN 的各种类型，然后再按照复杂性的顺序提出需要考虑的加密类型。加密传输中的信息的两种最常用的技术是 SSL(安全套接层)和 IPsec(IP 网络安全协议)。

网络加密的四种类型

1、无客户端 SSL：SSL 的原始应用。在这种应用中，一台主机计算机在加密的链路上直接连接到一个来源(如 Web 服务器、邮件服务器、目录等)。

2、配置 VPN 设备的无客户端 SSL：这种使用 SSL 的方法对于主机来说与第一种类似。但是，加密通讯的工作是由 VPN 设备完成的，而不是由在线资源完成的(如 Web 或者邮件服务器)。

3、主机至网络：在上述两个方案中，主机在一个加密的频道直接连接到一个资源。在这种方式中，主机运行客户端软件(SSL 或者 IPsec 客户端软件)连接到一台 VPN 设备并且成为包含这个主机目标资源的那个网络的一部分。

1. SSL：由于设置简单，SSL 已经成为这种类型的 VPN 的事实上的选择。客户端软件通常是很小的基于 Java 的程序。用户甚至可能都注意不到。
2. IPsec：在 SSL 成为创建主机至网络的流行方式之前，要使用 IPsec 客户端软件。IPsec 仍在使用，但是，它向用户提供了许多设置选择，容易造成混淆。

4、网络至网络：有许多方法能够创建这种类型加密的隧道 VPN。但是，要使用的技术几乎总是 IPsec。

在网络至网络的 VPN 的情况下，我们在讨论从一个网络设备到另一个网络设备的加密问题。由于我们期待目前的网络设备要做的事情，在这个讨论中会出现一些其它难题：

1. 与其它技术的相互作用：广域网经常使用服务质量、深度包检测或者广域网加速。如果在部署的时候没有考虑这些服务，加密就会使这些服务失效。网络地址解析是另一个需要克服的障碍，因为它首先会干扰建立一个加密的连接的能力。
2. 叠加网络：加密隧道 VPN 是通过在现有的网络上创建一个叠加的加密连接发挥作用的。加密的连接存在于这个网络上的两个具体接口之间。从源头上看，如果要加密的网络通讯被重新路由或者传送到不同的接口，它就不会被加密。如果这个通讯在加密之后被重新路由并且被发送到指定接口以外的其它接口，它就不能被解码或者被抛弃。
3. 在一个加密的 VPN 中，DNS、IP 地址和路由都需要特别注意。一些安全 VPN 技术与专用地址领域工作得非常好。有些安全 VPN 技术甚至在网络端点采用动态地址的情况下也能很好工作。在某些情况下，企业喜欢把所有的互联网通讯路由到一个中心的位置。在其它情况下，采用拆分隧道方法，分支地点有单独的互联网网关。
4. 带宽：网络工程师不停地解决带宽问题一边为其用户提供尽可能最好的体验。但是，在一个加密的 VPN 的情况下，他们必须要考虑加密带宽或者加密和解密大型数据流的能力。

无论是什么动机，探索这个技术正是时候。加密技术是比以前更便宜和产品更多的技术(这种技术嵌入在防火墙、路由器和广域网加速器)。但是，对于大多数网络工程师和设计师来说，这个技术需要不同的思路：按照复杂程度的顺序进行思考以便在这种技术中进行选择;努力地最大限度地减少网络和网络用户的负担;等等。通过遵守一些基本的原则，你可以确保加密技术成为保证你的网络安全的一种非常有用的、甚至是至关重要的工具。

(作者：Jeff Young 译者：东缘 来源：TechTarget中国)

连接处理金融事务的远程服务器必需Ipsec VPN吗？

问：我们使用两种方法通过互联网连接到远程服务器：Ipsec VPN 或者通过远程服务器的开放端口。这两台服务器主要用户金融事务。每一种方法有什么风险，你推荐使用哪一种？

答：首先，我要假设在连接两端的服务器上有网络防火墙和客户端防火墙。如果不是这样，干脆再次访问网络拓补结构，确定这种基本的互联网屏蔽是否可以安装。在你描述的情况中，保护服务器的防火墙的配置应该只允许远程服务器上的单一 IP 地址中的单一必须端口的流量。

其次，考虑一下适当的机密性控制。这两台服务器是如何互相联系的呢？ 他们使用 SSL 或其他安全、加密协议了吗？如果服务使用了安全协议，VPN 连接可能会增加不必要的通讯费用，因为每一条信息都需要加密解密两次。在这种情况下，跳过 VPN。另一方面，如果你不确定客户端/服务器协议使用的加密的安全性，使用强大加密的 IPsec VPN 就是安全而可靠的选择。

(作者：Mike Chapple　译者：Tina Guo　来源：TechTarget中国)

SSL VPN简化安全访问

许多公司使用 VPN 向公司外部的员工提供企业网络接入。目前，大多数远程接入 VPN 都使用 IP 安全扩展(IPsec)加密在公共 IP 网络上传输的专用 IP 数据包。然而，随着员工队伍的增长和多元化，IPsec VPN 客户对于最终用户来说是很麻烦的，对于网络管理员来说是成本是很高的。通过利用广泛应用的网络浏览器作为一个客户平台，SSL VPN 设备将是提供一种简单而安全的外点访问专用企业服务和数据的有希望的替代方法。

为什么使用 SSL VPN 设备?

市场研究公司 Gartner 预测，到 2008 年，SSL VPN 将成为主要的远程接入方式。三分之二以上的远程工作员工、四分之三的承包商和 90%以上的需要随机访问企业网络的雇员都将采用这种方式。作为一个基于浏览器的解决方案，SSL VPN 几乎能在任何系统上快速启动，不需要安装永久性的客户端软件。对于那些对管理旅行者和远程工作者的笔记本电脑感到厌烦以及那些需要不增加已经很沉重的 IT 工作量来扩大远程接入的企业来说，上述好处是有吸引力的。

用户通常可以使用一台 SSL VPN 设备从家里的或者公共的 PC 上加入网络，在任何可用的互联网连接上获得直接的访问。一旦用户通过身份识别，组或者单个规则便允许访问 SSL VPN 设备后面的代表系统、服务和数据的 URL。目标应用一般通过一个浏览器的窗口显示出来，由下载的 ActiveX 控件或者 Java 程序实施的。SSL 或者其 IETF(互联网工程任务组)的继任者 TLS(传输层安全)将用于数据压缩、散列、加密和在用户和 VPN 设备之间的传输全部信息。总之，SSL VPN 设备能够提供安全的访问，较少地依赖客户端软件。

应用 SSL VPN 设备

深入挖掘这个漂亮的外表，你将会发现 SSL 和 IPsec VPN 之间的巨大差别。例如，IPsec VPN 提供访问具体的子网或者整个企业网络。连接的主机必须分配一个这个专用网络地址空间中的 IP 地址。因为 SSL VPN 提供具体 URL 地址的访问，资源规则可以更详细并且能过更容易地隐藏内部网络的结构。从网络工程师的观点看，SSL VPN 整合更简单，因为这种设备能够在你防火墙的隔离区中使用，不用增加 IP 子网或者重新为 IP 子网编号。

另一方面，IPsec VPN 创建一个支持任何基于 IP 的应用程序的强大的、通用的应用程序。根据其设计，SSL VPN 设备可能需要逐步努力支持新的应用。例如，详细的设置可能需要把 URL 镜像为应用对象，并且重写 URL 以便隐藏内部信息。每一个 SSL VPN 设备都支持通用商务应用程序，如企业电子邮件和网络文件系统访问等。但是，专有的或者复杂的应用需要客户介入开发或者需要客户方面的端口转发代码。因此，许多公司最初都使用 SSL VPN 来增强其 IPsec VPN，把仅需要访问电子邮件的员工增加到 SSL VPN 网络，同时保留 IPsec VPN 以满足真正需要广泛的网络层访问的员工的需求。

在 SSL VPN 设备中寻求什么

当然，SSL VPN 设备必须有增强的平台的操作系统，并且通过安全界面进行管理。虽然早期的 SSL VPN 性能与 IPsec 相比还不是很好，但是，目前的企业设备能够使用硬件加速和高可用性等技术可靠地支持每一个大型的员工队伍。但是，除了对任何网络安全设备的这些基本的考虑之外，当你选择一台 SSL VPN 设备的时候，你应该考虑什么功能和因素呢?

VPN 架构——SSL VPN 设备是多种多样的：

·Web 代理设备仅支持 Web 应用程序。浏览器把普通的 HTTP 包在 SSL 中并且发送给这台设备。这台设备检查政策、镜像 URL 并且把 HTTP 请求转发给目标互联网服务器。

·应用解析设备让用户通过 ActiveX 或者 Java 接口与应用程序互动。这种 Java 接口模仿本地的应用程序图形用户界面，但是以 HTTP 格式发送请求。这台设备在把这个请求转发到目标服务器(非 Web 服务器)之前必须要把 HTTP 解析为每一个应用程序的本地协议。

·端口转发设备通过使用一个客户端代理在 SSL 隧道中转发本地应用协议来支持 TCP 客户机/服务器应用程序。这个代理与远程主机的应用端口连接在一起，同时，这台设备转发内部服务器(非 Web 服务器)发出和接收的信息。

·网络扩展设备通过使用一个客户端代理在一个 SSL 隧道中转发 IP 数据来支持任何 IP 应用程序。一个安装的代理拦截并且把出网的 IP 数据传送给这个设备。这台设备像一台网络层网关一样工作，在结构上与 IPsec 相似，但是没有标准 IPsec 的限制。

任何指定的设备可能都支持一个以上的结构。但是，从这里开始，将帮助你理解产品的客户和应用程序支持。

客户支持：每一个 SSL VPN 使用 Web 浏览器当作一个客户平台。但是，许多下载的客户端代码限制在公共 PC、非 Windows 主机、移动设备以及外部网合作伙伴的系统上使用。你能够满足客户的要求吗，例如客户对浏览器厂商/版本或者启用 ActiveX 的要求?这种设备能为现值的客户提供减少的功能，同时为使用 VPN 门户网页自己安装代理软件的雇员提供更多的功能吗?

应用程序支持：除了电子邮件和文件共享之外，考虑你的员工队伍需要的应用程序，这种设备是否/如何支持这些应用程序以及实现这些应用所需要的努力。例如，端口转发设备通常不需要客户化就能够支持许多客户机/服务器。但是，实时的应用(如 VoIP)可能需要网络扩展设备。确认你理解了在 URL 镜像和为你需要的应用程序进行协议解析都涉及到什么。

用户身份识别：SSL VPN 在提供授权服务之前必须要识别用户的身份。确认这种设备支持你需要的用户身份识别方式以及现有的身份识别服务器和用户数据库(如, RADIUS、主动目录和 LDAP)。此外，你要考虑这种设备是否能够从用户账户提取授权属性，并且考虑建立这种工作流所涉及的整合努力。

授权：SSL VPN 通常有能力强制执行控制用户(或者组)能够访问什么内容的详细规则。评估支持每一个需要的应用程序/资源的授权详细规则，苹果这种设备是否支持你定义的安全政策。例如，一些 SSL VPN 能够识别远程设备身份，让你限制那些在公共或者家庭 PC 上的用户的功能。

端点安全：在批准访问之前评估端点安全状况和一台设备的状况也是很有用的。SSL VPN 支持是为 NAC、NAP、TNC 和产品具体界面开发的，使它能够检查和/或者强制执行端点安全。采取的方法是要求在端点使用当前的安全补丁或者杀毒软件，或者限制不符合规定的端点能够访问的资源。考虑这种设备如何更好地适应你们公司的端点安全战略和实施。如果你计划支持没有管理的端点，你要评估对客户端安全措施的支持，如浏览器缓存、cookie 和历史记录的清除以及"沙盒处理"(sandboxing)。

审计与报告：最后，你要考虑这种设备如何跟踪和存档用户访问企业资源，并且考虑这种信息是否足以满足你的公司内部/外部报告的需求。

寻找 SSL VPN 设备

据市场研究公司 Synergy Research Group 称，2006 年全球 SSL VPN 年销售收入达到了 2.50 亿美元。这个市场领先的厂商是 Juniper、Citrix、F5、Aventail、北电网络、Whale 和 Array。在经历了快速增长和收购活动的市场中，跟上厂商和产品名称的变化以及新进入这个市场的厂商是很困难的。那些希望现在购买 SSL VPN 设备的人至少应该考虑下列竞争的产品：

Array Networks SPX Series

Aventail EX Series

Caymas Systems ID-Driven 网关

Check Point Connectra

思科 ASA 5500 系列产品

Citrix Systems 接入网关

F5 Networks FirePass

Juniper Networks Secure Access

诺基亚 SSL VPN

北电网络 VPN 网关

Blue Coat RA

SonicWALL SSL VPN

Whale 通讯公司(微软) 智能应用网关

要了解更多的有关虚拟专用网的技术和结构，请查看 SearchNetworking.com 网站的 VPN 网页。要阅读更多的有关 SSL VPN 设备和这些设备如何相互比较的资料，请阅读 David Strom 在 2006 年 9 月信息安全杂志上发表的文章《Not so simple》。

(作者：Lisa Phifer　来源：TechTarget中国)

企业VPN部署指南

问：我们公司现在正在做一个关于实现 VPN 以便于雇员进行远程工作的研究。VPN 的初步配置是不是往往比较昂贵，还有，我们应该避免哪些执行中易犯的错误呢？

答：幸运的是，一个 VPN 配置一般不贵。实际上，如果你的 VPN 用户只有几十个人，你可能在你的防火墙中已经拥有了你想要的技术。你可以详细查阅下防火墙供货商的文档。然而，如果你的 VPN 负荷很大，你可能需要买一个专门的为了有效处理而使用硬件加密技术的 VPN 产品。

我考虑了过去的 VPN 配置，建议请记住下面的两点要求以确保一个成功的 VPN 实现

预先为你的 VPN 定义验证方式。你需要什么类型的验证方式？使用用户名和密码进行验证这个方法简单而且用户都熟悉，但是可能不能提供足够的网络安全。很多企业会采用一个附加的技术，比如 keyfob 验证器，来增加对 VPN 用户身份验证的信任度。

创建书面的用户访问规定。VPN 用户可以使用哪些服务？可以允许他们使用坐在办公室的人员可以使用的同样的资源吗？或者在某种程度上缩小他们的访问权力呢？在你配置你的 VPN 之前，请坐下来然后制定出这些规定，否则你将一定会遇到麻烦。

事前稍微计划一下就可以实现一个成功的 VPN 配置。在开始阶段把策略和规定制定的很明确，以后你就可以更方便的让 VPN 融入你的公司运作。

(作者：Mike Chapple 译者：Sean 来源：TechTarget中国)

VPN应该采用哪些防火墙控制？

问：我们计划在企业中采用虚拟专用网（VPN），在 VPN 上应该采用哪些防火墙控制呢？

答：在 VPN 流量上采用的控制等级应该至少和在企业网上的类似用户流量上的控制等级相同。如果 VPN 只是员工使用的，在含有员工工作站的网络区域内终止 VPN 就是正常的合理选择。这种配置允许简单地把你在办公室中的防火墙控件采用到移动员工身上。

另一方面，如果 VPN 对第三方开放，例如厂商或者业务合作伙伴，你可能希望考虑把把这些用户放入专门的限制性区域内，可以限制他们对为了满足业务需要而必须访问的特殊资源的网络访问。这可以通过在防火墙区域内终止 VPN 实现，这个防火墙区域可以明确地控制从 VPN 到企业网络的流量类型。

我看到在很多企业中采用的一个解决方案是设置两到三个不同的 VPN，以用途不同设计。这通常可以使用单个的提供基于职责的访问的 VPN 工具完成。例如，可以在 VPN 上设置如下群组：

1. 员工
2. 系统管理员
3. 厂商
4. 点对点 VPN（Site-to-site VPNs）

然后可以根据他们的业务需求为每个职责群组设定不同的网络权限。例如，你可以让系统管理员有能力使用 SSL 协议创建和服务器之间的管理连接，而厂商和常规员工则不允许对它访问。

（作者：Mike Chapple　译者：Tina Guo 来源：TechTarget中国）

解决Vista与VPN的兼容问题

大多数 IT 部门正在缓慢地向 Windows Vista 过渡。他们担心整个公司范围内的应用将导致恶梦似的不兼容问题。但是，对于 Papa Gino's Inc. & D'Angelo Sandwich Shops 公司的网络管理员 Chris Cahalin 来说，微软最新的操作系统是必备的软件，因为这个软件大肆宣传其安全性能有了很大的改善。

Cahalin 申请参加了微软的 Vista 技术应用计划(TAP)。这个计划允许参加这在 Vista 仍在测试阶段时就选择一部分 Vista 软件使用并且直接参加微软的各个工程组。他的 IT 部门被允许参加了这个计划，从而使这家位于马萨诸塞州 Dedham 饭馆连锁店在应用最新版本的 Windows 方面走在了其它公司的前面。

这家公司目前正在从测试阶段向应用阶段发展。这个机构中的笔记本电脑将首先采用 Vista，随后是网络中剩余的 Windows 设备。

Cahalin 说，我们已经有一位地区经理在笔记本电脑中配置了 Vista 操作系统。通过 TAP 计划，我们与微软建立了直接联系以便发生故障时进行咨询。发现问题的最好方法就是使用它。这些资源确实为我们发生了一些事情。

同许多早期的应用者一样，Cahalin 的 IT 部门正在遇到一些不兼容的问题。当一种新技术在早期应用的时候通常会发生这个问题。在 Papa Gino 的案例中，这些问题不是 Vista 本身的瑕疵引起的。

Papa Gino 没用很长时间就找到了问题的原因：Vista 与该公司的虚拟专用网技术不兼容。Cahalin 认为，这是该公司安全计划中的一个重要问题。该公司使用一个虚拟专用网加密企业中的移动机器。这家公司的许多员工使用笔记本电脑在该公司在新英格兰地区的 400 多个地方旅行，他们经常在 IT 部门控制以外的无线热点和饭店房间里上网联系。

Cahalin 的大部分挫折是因为其虚拟专用网提供商思科系统公司没有为 Vista 的到来做好准备。由于虚拟专用网如此重要，他现在正在考虑使用其它厂商的产品。

Cahalin 说，对于我来说，思科的进展速度太慢了。每一个人都知道 Vista 即将推出。所有的第三方厂商都应该在 Vista 推出之前开始解决潜在的不兼容问题。

早期应用的推动因素

Cahalin 指出，Papa Gino 公司对信用卡处理的依赖以及不愿意遭遇 TJX 公司那样的数据突破的决心是促使该公司早期应用 Vista 而不是等待第一个服务包发布之后再使用的主要原因。

Cahalin 说，如果客户数据泄漏，任何一家公司的品牌都会遭到损失。信用卡对于我们的生意来说一直是很重要的。保护信用卡数据的安全是我们的责任。

HIPAA 法案、Sarbanes-Oxley 法和美国支付卡行业的数据安全标准等一些法规也对该公司有约束作用。所有这些法规都要求电子存储的数据都是准确的和安全的，没有在线掠夺者入侵的危险。

Cahalin 说，Vista 中的安全增强功能是值得他在虚拟专用网问题上耗费脑筋的。他说，使用 Vista，他能够更容易锁定个人的机器和为最终用户制定网络政策。他还很容易保证老式应用程序与 Vista 的连接和安全。人们喜欢的安全功能之一是用户账户控制。这是用户在启动某些应用程序时看到的那些弹出式警告的来源。

他说，这种弹出式对话框过一段时间就会被用户忽略。当人们设法使用老式的应用程序时，这些对话框肯定要经常出现。但是，我们通过设置正确的政策就可以绕过这些警告提示。通过这些政策，你可以告诉 Vista 哪些应用程序是合法的，哪些是不合法的。

同许多 Windows 管理员一样, Cahalin 一直不喜欢 Windows 为用户提供本地管理权限。这种做法很容易让攻击者控制有安全漏洞的计算机。Vista 通过封锁机器以外的本地管理访问权限改正了这个问题。至于界面布局，Cahalin 承认他还需要一些时间来适应。与早期版本的 Windows 不同，程序和选择不在同一个地方。但是，他说，考虑到 Vista 向 IT 管理员提供了这些程序的全部额外控制，这个代价是很小的。

他说，根据最终的分析，Vista 没有任何代价地提供了“令人震惊的安全水平”。

当然，并非每一个人都赞成这个观点。安全厂商 BeyondTrust 的首席执行官 John Moyer 说，他听许多用户说 Vista 把太多的决定权留给了最终用户，而不是公司的安全部门。

Moyer 说，微软喜欢说 Vista 是迄今为止最安全的操作系统。但是，现实是如果人们没有管理员权限就不能使用许多应用程序。企业不愿意用服务台处理用户每次遇到这个问题时打来的电话。当最终用户必须决定使用管理权限运行什么应用程序时，他们不喜欢这样做。对于用户来说还没有足够的透明度。

虚拟专用网僵局

虽然微软肯定要对人们部署 Vista 时遇到的挫折承担责任，无论设个挫折是由对话框引起的中断还是不兼容问题，但是，Cahalin 对于他遇到的挫折没有对微软表示一点不满。相反，他指责思科没有在虚拟专用网方面做好准备。

他说，这个问题是，当你使用思科产品的时候，你需要在思科的岛屿上生活。它是非常专用的产品。这种虚拟专用网连接很不稳定。这总是思科要适当地支持 Vista 的事情。

虚拟专用网问题的核心是 Papa Gino 公司喜欢使用一种安全套接层虚拟专用网，而思科还没有完成其安全套接层虚拟专用网与 Vista 兼容的问题。作为一项临时的绕过措施，Cahalin 正在转换到思科最近完成与 Vista 兼容的 IPSec 虚拟专用网。但是，许多 IT 专业人员认为，安全套接层虚拟专用网与基于 IPSec 虚拟专用网功能更全面。因此，目前这种状况是不理想的。

当获悉 Vista 的一些接口与安全套接层虚拟专用网有兼容性问题时，思科发言人证实思科已经在 IPsec 方面解决了这个问题并且正在努力使安全套接层兼容。思科不愿意让虚拟专用网团队的人出面详细说明这个问题。

Cahalin 目前正在探索放弃思科 5510 自适应性安全设备更换 Juniper 或者其它厂商的虚拟专用网产品。思科并不是 Cahalin 批评没有为 Vista 的到来做好准备的惟一一家厂商。Citrix 公司在兼容 Vista 方面也是行动迟缓。他说，Citrix 最近才发布 Citrix 演示服务器第 10 版客户端软件。这个软件旨在兼容 Vista。

Burton Group 高级分析师 Pete Lindstrom 说，实施重要的操作系统升级的公司都将遇到不兼容的问题。他说，思科虚拟专用网与 Vista 的兼容性问题可能存在许多原因。一种最有

可能的情况是思科正在花费时间研究这个问题，因为现在只有很少的思科用户正在积极地部署Vista。

他说，思科也许正在等待观察Vista的需求是什么。在某种程度上，并没有那样的多的公司像Papa Gino那样快地接受有风险的新事物。总的情况是采用的速度比较慢。思科也许看到了这种情况，认为他们有更多的时间解决虚拟专用网的问题。

保持第三方软件的安全

虽然Cahalin对Vista的安全功能感到很兴奋，但是，他认为采用多种来源的多层安全措施仍是有必要的。他指出，Papa Gino在2005年3月以后购买的全部台式电脑都配置了一个可信赖平台模块(TPM)。这种安装在主板上的芯片可用作硬件身份识别。TPM识别计算机，而不是识别用户。要实现这个功能，这个模块存储了专门发给主机系统的信息，如加密密钥、数字证书和口令等。

Cahalin说，虽然微软在把TPM管理建在Vista中取得了很大进步，但是，要真正有效地保证安全还需要安装第三方厂商的产品。他使用了Wave Systems公司的Embassy Trust安全套装软件进行加密并且正在考虑使用希捷技术公司的全面的硬盘加密选择。该公司还使用了配置指纹阅读器的戴尔笔记本电脑。

Cahalin说，长的和复杂的口令开始成为生产效率的一个障碍。因此，单一登录成为一种必要的东西。

Cahalin说，在他的第三方安全厂商和部署Vista之间，他更有信心地认为他的公司有足够的保护措施避免发生严重的数据突破事件。他说，如果思科研究出安全套接层虚拟专用网的兼容性方案，全世界都会感到很好。无论思科是否解决这个问题，或者Papa Gino是否选择其它的厂商，这个问题都将很快解决。

Moyer也赞成这个观点。他认为，为了纵深防御，第三方安全工具继续是必要的。他说，有一个标准的安全方法。这就是必须采取分层次的防御措施。如果你把全部安全都交给微软，那就好比让狐狸负责鸡窝的安全。

(作者：Bill Brenner　来源：TechTarget中国)

DMZ和VPN如何共存？

问：如果你有一个 VPN 防火墙路由器，它会受到 DMZ 服务器配置的影响吗？换句话说，DMZ 服务器和 VPN 可以共存吗？

答：DMZ 和 VPN 当然可以共存。实际上，它们是设计在一起工作的。

在典型的防火墙设置情形中，防火墙把网络分为明显的三个区：互联网，专用网和 DMZ。来自互联网的带内连接只允许连到 DMZ 中的服务器上；在互联网和专用网之间不允许直接的连接。提供公共服务的服务器（例如，Web 服务器和 SMTP 服务期）放置在 DMZ 内部，而为互联网用户提供服务的服务则存在于专用网上。

VPN 为远程用户提供了专用资源的访问权。用户经过 VPN 认证，然后就可以通过 VPN 连接访问专用网上的互联网资源。

(作者：Mike Chapple 译者：Tina Guo 来源：TechTarget中国)

企业应该执行强制iPhone VPN吗？

问：我听说有的厂商开始为 iPhone 提供 VPN 支持。我们公司有一些 iPhone 的用户。在什么情况下应该考虑使用强制 iPhone VPN 呢？

答：iPhone 实际上包括支持标准 PPTP 和 L2TP 的内置 VPN 客户机。除非你公司只支持 IPsec VPN 连接，你应该可以配置 iPhone，访问已有的企业 VPN。可以通过选择 General → Network → VPN 访问 iPhone 的 VPN 功能。

是否使用 VPN 的决定，要取决于你公司的安全需要。在下面的环境中，可以考虑使用强制 VPN：

1. 你在网络上使用内容过滤，希望限制 iPhone 用户的网络访问。
2. 你很关注用户对公共网络上不加密服务的访问，并且希望为你公司提供安全通道。

当要决定是否适用 VPN 时，iPhone 和其他计算机设备实际上没有太大的差别。如果所有的笔记本电脑都需要 VPN 连接，那么同时也使用 iPhone 就很有意义了。如果允许移动用户直接访问因特网，那么对于 iPhone 也可以执行相同的策略。

(作者：Mike Chapple 译者：Tina Guo 来源：TechTarget中国)

VPN是如何与即时通讯软件结合的?

问：我使用我家里的电脑（Windows XP Pro）通过 VPN 连接到公司的服务器。我下载了 AIM，在本地供我个人使用。是否 VPN 会对我的信息进行加密和保护?

答：VPN 允许一个公司的专用网络和它的远程用户之间能够通过第三方服务提供商进行可靠、加密的连接。它的目标是通过互联网扩展信任关系而不用牺牲安全性。当一个公司的服务器通过 VPN 访问时，用户 PC 和服务器之间的通信是通过 Internet 传输，使用加密隧道协议来提供保护和安全的。假如你公司的 VPN 配置是要求所有的 IP 通信都必须通过 VPN 通道，那么，所有的外部连接也必须经过公司的防火墙。这就确保你拥有和在办公室工作时同样等级的保护。

假如你使用一个即时通讯（IM）服务来和互联网上不属于你们公司的用户连接，一旦你的信息离开你的公司网络，就可能会成为明文。这一点非常重要，因为 IM 本身固有的不安全性，你的 IM 通信被允许通过你公司的防火墙是不太可能的。我猜想你们公司的 VPN 和防火墙被设置为只允许可以被接收的通信。如果是这种情况，你可以直接连接到 Internet 而不用通过你们公司的防火墙。因此，除非你有一个桌面防火墙在你的 PC 上用来防病毒和防间谍程序，否则你将把你自己带入被恶意代码攻击/感染的危险之中。

AIM（美国在线即时通讯软件）最新的版本允许你使用个人数字证书进行数字签名，并加密你的聊天记录和文件传输。不过，免费的 Internet 即时通讯软件一般都不会提供这样的功能。因此，你应该不要以为你的 IM 通讯是绝对安全的。最后为保险起见，我建议你和你们公司的网管确认一下，是否允许你在连接公司网络的 PC 上安装并运行像 AIM 这样的程序。

(作者：Michael Cobb 译者：王震 来源：TechTarget中国)

怎么在Vista操作系统中建立一个支持分离通道的VPN

问：我怎么在装有 vista 操作系统的计算机上设置一个支持分离通道和加密的 VPN 连接呢？

答：既然你问了有关分离通道的问题，那么让我们在考虑创建 VPN 连接的过程之前花点时间来解释下这个概念。默认的情况下，当你建立一个 VPN 连接后，Windows 会让所有的联系都通过 VPN 进行。所以，如果你在家登录了一个公司的 VPN，然后你查看你的电子邮件，或者在网上浏览网页，所有这些活动都是通过你的公司网络进行的。把这个作为默认状态是因为从公司的角度来看，这是最安全的方法，可以确保所有的连接都是安全的不管目的地是哪。

然而，由于某些原因你可能不想这样。首先，当你跟公司 VPN 连接的时候它允许你的公司检查所有你的个人网络活动。其次，你可能使你访问网络变的缓慢，因为所有的内容必须通过公司 VPN 进行发送。

另一方面，分离通道，对 VPN 连接进行设置以便于只有那些通向公司电脑的网络流量才通过 VPN 进行。其他的网络流量让你的电脑通过你本来的网络连接进行。

请按照下列步骤来设置在 Windows Vista 系统中分离通道的 VPN 连接：

1. 在控制面板中选择"Network & Internet."
2. 单击"View Network Status and Tasks."
3. 单击"Manage Network Connections."
4. 在你的 VPN 连接上右击，选择"Properties."
5. 选择"Networking"标签
6. 选中"Internet Protocol Version 4 (TCP/IP v4)."
7. 单击"Properties."
8. 单击"Advanced."
9. 取消"Use default gateway on remote network"选项的选择
10. 单击"OK"三次来关闭你刚才打开的窗口

这样设置以后，只有通向你公司网络的连接是通过 VPN 进行的。所有其他的网络连接都会用本地的网络进行连接。

(作者：Mike Chapple 译者：Sean来源：TechTarget中国)

分离通道功能会使VPN变得脆弱吗？

问：你会推荐配置一个带分离通道功能的 VPN 吗？这样的结构会让你的 VPN 变得有多脆弱？

答：分离通道技术允许 VPN 用户既可以通过 VPN 通道直接进行网络活动，同时又可以通过本地网络默认的网关进行另外的网络活动。

在最基本的 VPN 方案中，举个例子，一个家庭用户用一个 DSL 调制解调器可以建立一个 VPN 连接，强制他或她的所有系统流量都通过 VPN 通道连接到工作场所的网络。这些网络活动流量包括所有的内容，从电子邮件和其他的公司服务开始一直到简单的网页浏览。

当在这种 VPN 模式中引入分离通道功能时，只有一部分的网络流量通过 VPN 通道。管理员通过配置让 VPN 通道具有网络认知性，用户的 VPN 客户端程序就会根据每个包的目的地址进行智能路由。如果一个包是流向工作场所网络中的一个系统，那么它就会通过 VPN 通道发送。如果它的目的地是外面的网站，它就会通过用户的 DSL 网关直接流向目的地主机。

是否采用分离通道取决于你的业务需求。如果你的目标是保护远程用户和工作场所之间的网络连接的安全，那么采用分离通道会比较好。但是这样做的话，你需要培训你的用户，并确保他们知道哪些网络流量通过 VPN 通道、哪些不通过 VPN；你不会想让员工有虚假的安全感。

为什么我们不能完全的否定分离通道技术呢？因为当你不使用分离通道时，用户无法访问本地网络上的受限资源。我们可以再看一下家庭用户的情况。如果那个用户在家庭网络有一个私人设置的文件服务器，不使用分离通道技术就不能使用此服务器。还有，如果一个企业中有大量的用户采用这种没有分离通道功能的 VPN 模式，那么这个企业可能承担不起处理大量流向其他网络的流量负担。

(作者：Mike Chapple　译者：Sean来源：TechTarget中国)

恶意软件能利用分离隧道的VPN入侵网络吗？

问：隧道分离(split-tunnel)VPN 有多安全？木马、rootkit 或者其它恶意软件是否有可能通过分离隧道入侵企业网络，窃取敏感数据？遵从 PCI DSS 等法规不利于分离隧道的 VPN，这种说法是否正确？

答：分离隧道的 VPN 本身没有安全或不安全之说。然而，在决定集中流量还是实施分离隧道时，你需要平衡需求，控制所有用户的流量，抵御用户和企业在处理外部流量时可能会面临的危险。

隧道分离的美妙之处在于，你的公司不再需要为 VPN 用户提供一般的网络接入点。VPN 客户可以利用分离隧道，自动判断能否通过虚拟专用网获取网址，如果不能，用户可以通过网络连接直接传递网址。如果用户只能发送 10%的流量到企业网络，你可以让接入提供商处理剩下的 90%。

另外，分离隧道可能会给用户留下错误的安全感觉。如果他们遵循“从隧道接入 VPN”的原则，员工可能会觉得他们所有的流量，包括私人邮件和 Web 浏览数据，都被 VPN 加密了。他们可能不会意识到，本地网络的流量很容易被拦截。

从法规遵从的角度来讲，PCI DSS 并没有对分离隧道做出任何声明。我认为，在法规遵从的审计过程中，你应该合理地看待每种方法。分离隧道并没有真正降低企业网络受恶意软件感染的危险性。即使你制定了 VPN 隧道战略，如果恶意软件在计算机接入 VPN 之前已经存在，那么接入以后恶意软件依然会存在。如果你希望确保连接到 VPN 的系统不受恶意软件感染，我建议采用网络入控制（NAC）技术。

(作者：Michael Cobb　译者：周姝嫣　来源：TechTarget中国)

VPN在企业无线网中的作用

早期的无线局域网经常再次使用远程访问虚拟专用网 （VPN）客户端，克服 WEP 和相关的安全装置的局限性。但是，假设 Wi-Fi 安全性已经得到了提高，VPN 在企业无线网中是否依然起到很大作用？在无线网中使用 VPN 的实际作用和局限性是什么呢？本文中，TechTarget 中国的特约专家讨论了如何充分利用 VPN，以及如何消除无线局域网漫游和 VPN 信道之间的冲突。

VPN 如何起作用

VPN 信道一直都用于在诸如因特网之类的不受信任网络中提供数据的机密性和完整性。今天，许多公司使用信道来确保从远程工作者到公司网络边缘的 VPN 网关过程中信息流的安全。这个网关可以认证用户身份并控制可以达到的目的地。

今天，VPN 也正在强化终点安全的执行。在准许访问网络之前，会检查远程设备是否遵从法规。比如，可公共 PC 的工作者能仅允许检查电子邮件，而公司笔记本电脑的工作者则允许访问敏感的服务器。没有打补丁或者感染了特洛伊木马的笔记本电脑可能被导向到了检疫服务器，进行修补。

无线网用户可受惠于这些相同的安全措施。

1. 诸如有线等效保密（WEP）或者 Wi-Fi 网络安全存取（WPA）的版本 1 或者版本 2，VPN 信道可以隐藏通过无线电波发送的信息流。WEP/WPA 仅仅保护空中的连接，而 VPN 信道可以向任何干扰网络扩展。虽然这可能“在校内”并不重要，但是在使用住宅区无线局域网或者热点无线局域网时，这一点是很关键的。
2. 像 WEP-企业版本、VPN 网关都可以验证无线网用户，采用密码、双因素令牌、智能卡、或者证书。但是 802.1X 对局域网提供了要么全有要么全无的访问，而 Layer 3 VPN 和 Layer4 VPN 则可以限制可到达的目的地和应用程序。对拥有广泛不同的用户社区的大型无线局域网来说，更为精细的策略在是非常重要的。
3. 依赖这种产品，WPA-企业版本和 VPN 都可以强化终端的安全性。然而，VPN 使用一个代理器平台，跨越不同的网络（本地或者远程），可以更容易地实施一系列持久连续的规则。

4. 最后，这两种技术都需要客户端配置、用户身份管理、以及（某些情况下）软件安装。VPN 产品比 802.1X 产生的时间长一些，因此，许多 VPN 产品拥有更详尽的中央政策管理和更广泛的客户端操作系统/平台的支持。

VPN 如何阻止

有许多 VPN 信道标准，包括点对点信道协议（PPTP）、因特网协议安全（IPSec）和安全套接层协议（SSL）。VPN 产品和安全特性有很大的不同，并且直接影响到它们是否能满足你的无线需求以及满足的状况。

比如，虽然 PPTP 是最易攻破的共同 VPN 协议，但是，它也易于使用。PPTP 客户端内嵌在许多操作系统中：包括 Pocket PC 和 Mac OS，此外，基本不需要进行配置。在频谱的另一个终端，IPSec 提供了坚固的安全性，并由复杂的配置所支持，由 VPN 客户机安装。在 SSL VPN 层之间——要比 PPTP 更安全，配置起来要比配置 IPSec 更容易。

这种多样性使得很难相互比较 VPN，比 WPA 要简单得多。但是，关于 VPN 是如何阻止无线网，我们仍然可以做出全面的观测。

1. WEP 和 WPA 可以保护所有的链路层数据，包括局域网广播和多点传送。局域网使得更多的信息流暴露出来，这样在信道开启之前，很难防止信息“泄露”。这尤其符合用于受信任（校内）的无线局域网和不受信任（热点）的无线局域网中的设备，这里的局域网需要不同的 VPN 策略。
2. 虽然 VPN 可能与远程安全措施相吻合，但是对网络拓扑结构比较挑剔。比如，WPA-企业版本可以为无线工作站分配虚拟局域网标签，支持当地和独立子网中的局域网访问控制。VPN 通常使用虚拟的 IP 来达到这一目的，这就可以命令路由，并过滤网络中的变化。
3. 尽管当无线工作站漫游时，WPA-企业版本会带来延时，但是当工作站在 IP 子网间漫游，VPN 信道通常会破坏。虽然将所有无线用户集中在一个子网避免这一点的发生，但是这在大型无线局域网中是不可能的。
4. 需要特定的客户端软件 IPSec PN 在一些客户或者设备无法正常运行非定制客户端的无线局域网中是不切实际的（比如，无线扫描器、智能电话、VoWi-Fi 步话机）。然而，在需要特殊的 802.1X 请求的 WPA-企业版本安装中会面临类似的问题。

克服困难

大多数企业会采用 VPN 和 WPA2 的结合来结束对无线员工的保护。随着无线基础设施的成熟，许多人会将校内网升级成为 WPA2 企业版本。VPN 会坚持保护无线热点的移动工作者和家庭无线局域网的远程工作者。很少有公司可以控制远程网络，此外，安全状况也有所不同。用 VPN 托管所有校外无线网可能是在这些环境中执行公司制定的策略的唯一方法。

那么，在使用无线局域网的时候，你该如何面对 VPN 的挑战？

1. 将终端安全软件与你的虚拟专用网客户端相结合，终端安全软件可以进行核查以确保只要无线链路处于连接状态，VPN 就在运行，并且如果 VPN 信道关闭，就中断无线连接。配置个人防火墙以阻止非 VPN 信息流通过无线网进入或者离开。
2. 对于单一接入点的家庭无线局域网和因特网咖啡馆的用户而言，由于漫游导致的 VPN 中断可能并不是一个大问题。当在不同地点移动时，仍然需要保持连接的工作者就可能需要一个移动的 VPN。可以从 NetMotio、Columbitech,、Ecutel 和 AppGate 购买到移动 VPN 产品。当客户需要在网络之间移动时，这些移动式无线专用网产品可以提供持续的信道和会话。当某个设备暂时移出范围时，一些产品甚至可以排队等待接收的信息。虽然所支持的技术不同，但是移动 VPN 通常都需要客户端软件。
3. 当使用 VPN 来确保校内网工作者的安全时，应该使用提供“流动性”或者“子网漫游”的无线网关或者交换器。虽然这些特性是专有的，但是，当在子网间漫游时，通常会让 VPN 客户端保持相同的虚拟 IP。然而，当工作站离开无线网的覆盖范围时（比如，内部电梯、建筑物之间），仍然会发生应用中断。

最后，为了支持那些不能运行 VPN 客户端软件的客户和其它设备，应该使用一个 SSL VPN 或者受控的入口。受控入口虽然不对数据加密，但是可以用于控制并追踪网络的使用情况。SSL VPN 使用网络浏览器作为客户端平台，对数据进行加密，这样它甚至可以适用于客户端设备。

（作者：Lisa Phifer　译者：李娜娜 来源：TechTarget中国）

结合VPN与无线AP增强安全性

本文将介绍把虚拟专用网（VPN）与无线桥接器（access points，AP）结合起来以增强安全的两种方法。

询问任何熟悉安全的 IT 专业人员有关在企业环境中使用无线网络的问题，他们都会告诉你，普通的 AP 安全措施并不能真正解决问题。无线通信的广播性质、日益高级的无线监听工具和破解无线 AP 传输数据的手段，都表明不采用额外的措施，无线网络并不安全。大多数专家建议，把无线 AP 放在自己的网段中，并将这一网段用防火墙保护起来，防止内部网的其它部分与无线 AP 连接起来。

采取的下一个步骤是让你的所有的无线客户使用虚拟专用网软件，你的无线网络会更安全一些。同时，如果你的网络有一个 DMZ（半军事化区，内部网络与外部互联网之间的半安全区域），就使用这个 DMZ。如果没有 DMZ，就坚持使用老的方法， 使用单独的电缆隔离或者 AP 的虚拟网络，让数据在进入内部网之前通过一个防火墙，只让这个通信停留在网络的安全的一边。

有两种方法可以把虚拟专用网和无线 AP 结合起来。第一种方法是把 AP 放在 Windows 服务器的接口上，使用 Windows 内置的虚拟专用网软件增加无线通信的覆盖范围。这种方法允许你使用内置的 Windows 客户端软件以及 L2TP 和 IPSec 软件，为你的无线网路的通信进行加密。这种技术也适用于支持同样的内置或者免费的虚拟专用网客户端软件的其它操作系统。这个方法的好处是使用内置的软件，客户端软件的变化很小，非常容易设置和应用，不需要增加额外的服务器或者硬件成本。这种方法的不足是增加了现有的服务器的额外负荷（根据你提供服务的 AP 的数量和使用这些 AP 的客户数量的不同，负荷也有所不同）。服务器执行其它的任务也许会效果不好。如果同一服务器还提供防火墙功能，额外负荷可能会提示使用其它的服务器或者采用不同的方法。

第二种方法包括使用一个包含内置虚拟专用网网关服务的无线 AP。SonicWall、WatchGuard 和 Colubris 等公司目前提供一种单个机箱的解决方案。这种解决方案集成了 AP 和虚拟专用网功能，使应用无线安全网络更加容易。这种预先封装在一起的两种功能结合

在一起设备很容易安装、设置、配置和管理，而且很容易强制规定政策，让每一个无线连接都使用虚拟专用网完成连接。由于这种方法在使用的时候很容易选择，加密也更加合理了，避免了 802.1x 加密为虚拟专用网连接增加的费用。这种方法的弱点包括价格昂贵，购买新的机器只能满足新的无线局域网子网的需求，在不更换硬件的情况下很难从一种无线技术升级到另一种技术。

混合的方法也许包括与现有无线 AP 一起使用客户端软件，并且计划过渡到新的基于设备的产品。另一种方法是指定一台在 DMZ（或者在自己的网段）的服务器，专门处理无线连接、VPN 网关需求以及防火墙信息，开启或关闭无线网段。但是，在其中增加一个虚拟专用网，你可以提高安全性并且感到更有信心，有时日常网络通信在无线网络中像在有线网络中一样安全。

(作者：Ed Tittel　来源：TechTarget中国)