利用VPN技术确保电子政务的安全

文／尚隽·吉林市电视台

一、电子政务对安全的需求

电子政务作为信息网络的一个特殊应用领域，运行着大量敏感的、需要保护的数据和信息。如果系统的安全性被破坏，造成敏感信息暴露或丢失，或网络被攻击等安全事件，那么产生的后果必然波及地区和整个国家。缺乏安全保障的电子政务信息系统，不可能实现真正意义上的电子政务。

为提高网络的安全性，各级政府部门采用建立政府专网、内外网隔离等手段。但是政府专网的覆盖范围小，成本高，不能满足电子政务的需要，尤其网上办事、网上申报这类需大面积覆盖到各个企业或个人的应用，因此电子政务必须要依靠互联网(Internet)。鉴于互联网是以开放和自由为基础，从协议规划、服务模式、网络管理等方面均缺乏安全性设计，所以它存在安全隐患。那么如何才能在互联网上进行安全的应用呢？答案是采用VPN技术。

二、VPN的分类

VPN（虚拟专用网络）指的是通过利用对两个专用终端之间的通讯进行加密的方式在公用的国际互联网上模拟出专用网络。它在连通性、服务质量和保密性等方面与现存的典型专用网络具有相同的性能。目前，电信业务和接入技术的发展，使用户可以选择多种技术来建立自己的广域网络。VPN的实现方式有多种，可以根据不同的着重点来区分VPN。

1．按VPN的部署模式分类

VPN的部署模式从本质上描述了VPN的通道是如何建立和终止的，一般有3种VPN部署模式：

（1）端到端(End—to—End)模式；

（2）供应商—企业(Provider—Enterprise)模式；

（3）内部供应商（Intra—Provider）模式。

2．按VPN的服务类型分类

根据服务类型，VPN业务大致可分为3类：Internet VPN、Access VPN与Extranet VPN。

（1）Internet VPN：即总部与分支机构间通过公共互联网构筑的虚拟网；

（2）Access VPN：又称为拨号VPN（即VPDN），是单个用户或小分支机构通过公共互联网远程拨号到总部的方式构筑的虚拟网；

（3）Extranet VPN：即不同企业或组织的网络通过公共互联网来构筑的虚拟网。

3．按VPN的技术分类

（1）传统的虚拟专用网络（VPN）

● 帧中继虚拟专用网络（VPN）（第二协议层）；

● ATM虚拟专用网络（VPN）（第二协议层）。

（2）基于用户地设备的虚拟专用网络(VPN)

● L2TP和PPTP虚拟专用网络(VPN)（第二协议层）；

● IPsec虚拟专用网络（VPN）（第三协议层）。

（3）提供者指配的虚拟专用网(PP—VPNs)

● BGP/MPLS 虚拟专用网(第二和第三协议层)。

（4）基于会话的虚拟专用网

● SSL虚拟专用网（第四及以下的协议层）；

● SOCKS虚拟专用网（第四及以下的协议层）。

三、各种VPN的实现原理简介

传统的虚拟专用网技术被服务供应商和企业广泛采用。然而由于它们的成本较高且功能较少，因而使得新的虚拟专用网技术，如IPsec VPN，SSL VPN和MPLS VPN正得到越来越多的应用。这些新的VPN技术与TCP/IP协议完全兼容，而TCP/IP可用于全球范围内的数据传输和路由选择。

公共网络传输信息的安全构成了VPN的关键技术。这种安全有三种，即身份验证、加密和封装，它们是各种虚拟专用网络的基础。然而，利用许多不同的技术，都可以实现身份验证、加密和封装。此外，这三种技术可以采用多种方式组合在一起。

在VPN中进行数据封装的过程中，产生了多种隧道技术，如第二协议层的隧道协议（L2TP），第二协议层的传送协议（L2F）和点对点隧道协议（PPTP）。PPTP使得远端用户以一种加密的、多协议的方式通过国际互联网访问某公司的网络。PPTP将诸如

IPX和NetBEUI之类的网络层协议封装起来并经过国际互联网进行传输。然而PPTP不支持单用户多隧道同时传输。它的后续协议L2TP（PPTP和L2F协议的组合）解决了上述的难题，能够支持单用户多隧道同时传输。PPTP和L2TP是第二层的协议，它们构成了VPN技术中从用户地设备（CPE）到用户地设备（CPE）进行连接的部分。

Internet安全协议（IPSec），是被采用得最广泛的VPN技术，是由Internet工程任务组（IETF）开发的一组身份验证和加密的协议，可用于IP网络中的数据保密、完整性检查、身份验证和密钥管理等诸多方面。一般说来，Internet安全协议（IPSec）主要用于安全阈的一个部分，它通过在一个数据包上面再围上另外一个数据包的办法来封装该数据包。这样，它就对整个数据包进行了加密。这种经过加密的信息流在没有其它安全措施的IP网络中形成了一个安全的信息隧道。IPsec是主要的第三协议层的VPN技术，在用户地设备（CPE）和用户地设备（CPE）之间提供了信息隧道。

SSL/TLS是一种常用于网络安全通讯（HTTPS）的技术，也可用于VPN。SSL VPN使用广为使用且极其成熟的SSL/TLS协议来处理建立VPN所必需的信息隧道的创建和密码元素。SSL/TLS比起IPSec来，更易于采用，并能提供简便且经过全面测试的平台。RSA握手（或DH）在使用上和IPSec中的IKE相同，而SSL密码库用于确保对称隧道的安全，那些受保护的IPSec隧道将使用类似的加密技术；而对称隧道，就像IPSec VPN一样，可传输专用通信。

流行于服务供应商之中的VPN技术是边界网关协议／多协议标签交换（BGP／MPLS）VPN。BGP/MPLS VPN被用来解决传统ATM和帧中继VPN网络中的不可拓展的难题。此外，MPLS VPN是一种无连接的VPN，它完全兼容于TCP/IP技术以及国际互联网世界，而采用TCP/IP技术及国际互联网所需的成本明显较为低廉。BGP/MPLS VPN标准在IETF的RFC2547中进行了定义，提供了第三协议层中的VPN解决方案，即利用BGP通过MPLS核心来传送路由信息。这种第三协议层中的MPLS VPN解决方案具备了第二协议层中方案的全部安全因素；并采用第三协议层的路由技术，增加了更强的可扩展性能。

SOCKS 5是一个电路级的代理协议，可促进经过鉴定的信息顺利地通过防火墙。SOCK 5支持绝大部分的验证、加密、隧道以及密钥管理等方面的计划；同时还支持一些使用诸如IPSec、PPTP或其它VPN技术所不能得到的功能。当SOCKS与其它的VPN技术配合起来使用的时候，就可以得到一个更为完备的安全解决方案，而这种解决方案是使用任何单项技术都不能得到的。例如，用户可以将IPSec和SOCKS组合在一起。IPSec可用于确保底层的网络传输的安全，而SOCKS可用于加强用户级及应用级的访问控制。

四、利用外包VPN实现电子政务安全是一条捷径

对于电子政务应用来说，VPN提供了点对点的连接、保密性、QoS和可管理性，不同的应用可以选用不同的VPN技术与服务。VPN可以使分支机构、出差人员以及网上办事的企业个人能够安全、方便、快捷地连接到政府网中，同时还能够节省时间和成本，保证连接的安全性。而用户把VPN交给专业的服务提供商管理，可以更加降低管理成本并节约费用，从而把更多的精力投入到核心业务中。对于实现VPN所必需的设备如VPN网关设备、大型主干网路由器和交换机等，均由服务提供商拥有并管理，这样又可节省资本开支。用户可以通过低成本的租用选项，从服务提供商或增值销售商处获得客户端设备(CEP)，从而实现了更大的升级灵活性。同时，服务商对服务水平协议（SLA）的改进和服务质量（QoS）保证，为政府外包VPN方式提供了进一步的保证。这种利用外包VPN实现电子政务安全的做法，有效地整合了社会资源，实现资源共享，共同构建节约型的和谐社会。

作者简介：

尚隽，女，1977年出生，吉林省吉林市人，工作单位：吉林市电视台，邮编：32000，理学士学位，现攻读东北大学信息学院研究生。

参考文献：

1 王达.虚拟专用网（VPN）精解[M].清华大学出版社，2004

2 高海英，薛元星，辛阳等. VPN技术[M].机械工业出版社，2004

3 戴宗坤等.VPN与网络安全[M]. 电子工业出版社，2002