VPN与网络安全

四川大学信息安全研究所 戴宗坤 唐三平

摘 要 本文明确给出了VPN的定义、VPN和安全VPN的分类及其目标，最后列出了安全VPN需要满足的基本安全特征。

关键词 VPN、私有性、机密性、完整性、虚拟连接、IPSec、审计、基于策略，访问控制

1 引言

VPN(Virtual Private Network)，即“虚拟专用网络”，是通过对公共通信基础设施进行逻辑分割而构建的一种特殊通信环境。这种环境的特性是其私有性和隐秘性：私有性是虚拟的，即是通过对公共网络的逻辑分割方式，而非通过物理搭建私有的通信网络的方式来实现；其隐秘性表现在非该通信环境中的成员不能感觉到这种通信环境的存在。VPN也是一类组网技术，这类组网技术的目标是要在公网上按照某种共同利益的需要虚拟出私有的通信网络环境。VPN还是一种策略，实施该策略用以为用户提供定制的传输和安全服务。

VPN概念所隐含的私有性和隐秘性特性，使得VPN技术注定与安全通信技术有着千丝万缕的联系。但由此将VPN产品笼统界定为网络安全产品是不合适的。人们可能出于各种目的构建VPN，其中广为人知的Internet网络连接实际上就是一种广义的VPN实现。迄今为止，人们可以用来支持在公共网络上实现VPN的方法不下十种，其中路由过滤技术和隧道技术是目前两种主流的VPN实现机制，均可按网络管理者的意志加以选择。

目前有两大类VPN设施，一类是由NSP等建立基于公共通信设施的VPN体系，出售给各种商务和个人用户，主要解决网络资源共享以及服务质量控制等问题的面向社会服务的VPN网络，其VPN网关设备及其配置管理权不在用户自己手上；另一类则是基于自身特殊需求（例如行业系统信息的管理），在公共通信网络的IP层构成基于IPSec协议体系的内联网安全平台，这一类VPN网络只面向行业和系统内部，其VPN网关设备和设备配置管理权均是自主可控的。

我们介绍的是在IP网络层上的基于IPSec协议系列的安全VPN的实现。安全VPN是一种通过公共网络为实现一个利益共同体内网络连接安全、有序的数据传输安全而建立的安全通信平台。它强调的重点是通过公共网络组建“自己的”“内部”受控的网络环境的安全性。

2 安全VPN的目标

安全VPN的目标包括：连接和传输数据的机密性、完整性；数据源的真实性；环境内通信资源的可用性；对利益共同体内部和外部访问的可控性以及对访问的可审计性。

所谓连接和传输数据的机密性，即网络连接是不可见的、隐蔽的，连接传输的信息内容对未授权用户是毫无意义的乱码，或者根本就不可见。只有被授权用户才能通过密码变换或者其他手段得到可以理解的原数据。

完整性即连接自身以及所传输数据在整个传输过程中，没有受到未授权的生成、插入、增加和篡改。接收者得到的信息与发送者发送的信息完全一致，以及连接建立及维持过程的完整性。

数据源的真实性指数据事实上的发送者与声称的发送者是一致的。

通信资源的可用性是指利益共同体内的用户在希望得到服务（包括连接和信息内容）的时候，能够得到相应的服务。而可控性除了要求资源的可用性得到保障以外，还要求能够对利益共同体内的访问有合理的权限控制、确保利益体内通信环境的边界安全、以及对各个VPN节点的安全策略、规则和相应参数的集中统一的可管理性。

访问的可审计性是能对利益体内或外的访问行为作有效的日志记录，并能通过这些日志记录挖掘出安全相关信息。

3 实现安全VPN的基本要素

安全VPN概念应满足七个基本的安全要素，它们分别为：

作者简介：戴宗坤，1945年10月生，四川大学信息安全研究所常务副所长，高级工程师。唐三平，1973年2月生，博士研究生，主要研究方向为信息安全。

3.1 虚拟连接安全

虚拟连接指穿越公共基础设施形成VPN的那些安全隧道或采用路由过滤技术所形成的逻辑通道。它包括远程访问连接、内联网虚拟连接和外联网虚拟连接。安全的虚拟连接指对VPN连接或隧道的发起方和终止方身份的准确鉴别、连接两端实体被授予的适当的连接权限。虚拟连接的安全需要VPN的涉密节点能提供源鉴别服务。源鉴别服务可通过基于（非）对称密码技术的身份鉴别机制来提供；而访问授权则可通过访问控制方案来提供。

3.2 连接的边界安全

边界安全主要指如下三个基本目标的实现：一是连接授权；二是保护数据在边界不丢失或不被偷窃；三是防范某些禁止服务型攻击。

通过访问控制机制可实现连接授权服务；合理的网络规划和安全域管理，以及相应的访问授权控制则可以保护数据在边界不被偷窃或丢失；对某些禁止服务型攻击的防范一般通过基于策略的审计管理，以及实时的风险监控措施得到适当的防范。而使用密码技术也能一定程度防范禁止服务型攻击，其主要原理是运用处理量的差异，将需要大量处理时间的运算尽量延迟到身份鉴别或分组的有效性鉴别完成之后进行。

3.3 连接和传输的完整性

连接完整性保证网络的可用和可靠性，传输完整性保证传输数据不被非授权创建、修改、删除或重放。

为提供连接的完整性服务，在建立连接时，必须对实体身份进行鉴别，并在用户会话期间对连接的身份进行鉴别。可以使用专门的鉴别协议，或通过基于完整性等机制的分组级鉴别来实现对端实体的身份鉴别。数据传输的完整性主要通过完整性机制或基于非对称密码技术的数字签名机制来实现。

3.4 连接和传输的机密性

VPN网络的保密性包括连接保密、隧道传输和过渡保密以及数据内容保密。

连接保密指虚拟连接的发起与终止过程中的请求、质询、应答以及会话信息的隐密性。该服务一般通过机密性机制或位填充机制来实现。

隧道传输和过渡保密指连接或隧道建立后隧道本身的隐秘性，以及连接过渡的隐密性。隧道的隐秘性指不暴露隧道的存在性，可以通过机密性机制提供这一服务。连接过渡的保密性要求不能出现加密/鉴别的空白段，实施端端加密机制可以提供这一服务。

数据内容保密指通过隧道传输的数据内容不被未授权暴露或泄密。这需要提供机密性服务。该服务可通过加密和位填充等机制获得。

3.5 主动审计能力

主动审计指除系统对重要通信事件、操作事件以及违反ACL策略的通信进行日志记录和必要审查，特别包括对网络脆弱性漏洞的扫描以及对入侵的检测与对抗能力。主动审计服务主要使用审计与报警机制来实现。但在提供该服务的过程中，也可能使用完整性机制以提供审计过程的真实性和审计数据的可靠性，还可能使用机密性机制保护审计数据的传输和存储的机密性。

3.6 基于策略的集中式安全服务控制

集中式安全服务包括两个方面涵义，一是通过网络进行集中控制的安全管理；二是保证通过网络传输的管理信息本身的安全，这将涉及到管理信息的协议安全以及管理信息传输过程中的保密性和完整性。为了不给攻击者留下可乘之机，管理协议应具有严密的保护体系。而利用机密性机制、鉴别机制和完整性机制可为管理信息提供安全服务。

3.7 VPN设备的自我保护能力

VPN设备自身安全的指标有物理安全、操作平台安全、应用程序安全以及管理安全等。其中，物理安全涉及机械电子安全规范，达到物理坚固性、物理不可进入性以及电子辐射控制与防护要求；操作平台和应用程序安全涉及软件工程和安全级的内容，设备本身除接受管理工作站的配置管理命令外，对进出信息流必须运行于黑匣子状态；管理安全应坚持技术和法律法规手段结合，构建一个共同体内封闭的管理体系。

4 结束语

安全VPN是解决网络安全的有效技术，我们可以通过VPN构成内联网、外联网的安全平台。安全VPN在我国的党政机关和行业管理系统构建安全的跨地区内联网的过程中，将起到关键性的基础作用。但信息安全作为一个系统的概念，还要强调除了网络平台安全以外的与信息系统组件及其运行环境、信息主体和客体的整体安全。

(收稿日期：2001.1.3)