网络安全 VPN 关键技术的应用研究

陈红忠
（云南磷化集团有限公司，云南 昆明 650607）

摘 要：在过去的网络配置过程中，要想实现远程访问，需借助 DDN 专线，该方法费用很高。对移动用户和远程个人用户，可通过拨号线路和企业局域网互联，但这会给网络带来安全风险。基于此，提出远程访问技术——VPN，在介绍其功能和优缺点的基础上，对其网络安全关键技术与具体应用进行深入分析，旨在为这项技术的应用发挥预期作用效果提供可靠参考依据。

关键词：VPN；网络安全；关键技术
中图分类号：TP3 **文献标识码**：A **文章编号**：1004-7344(2021)15-0270-02

0 引言

VPN 主要功能在于公用网络基础上进行专用网络的建立，实现加密通讯，目前在企业网络领域得到了广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。

1 VPN 概述

为了使外地员工正常访问企业的内网，基于 VPN 的实现方案为在内网当中架设专门的 VPN 服务器。员工在联网以后与该服务器相连，通过服务器即可进入到内网。为提高数据安全性，通讯数据均实现了加密处理。在加密处理支持下，数据如同在一条专门链路上实施安全传输，相当于架设了专用网络，然而，VPN 只是一条公用链路，可将其称作虚拟专用网络，它的本质是借助加密技术通过封装形成数据通讯隧道。在 VPN 技术支持下，不论用户在家中或外地，均可通过互联网对内网资源进行访问，使其在企业当中得到了越来越广泛的应用。

VPN 处理流程为：①保护主机将明文信息传输至其他的 VPN；②VPN 以网络规则为依据，确定数据处理方式，如直接传输或加密；③对于需进行加密处理的数据，VPN 对其所有数据包实施加密，同时附上签名，添加新报头实施重新封装；④封装完成后，使数据包在隧道中进行传输；⑤在数据包传输至 VPN 后，开始解封，经核对确定数字签名正确后，方可对数据包实施解密。

VPN 常用实现方式为：对于大型局域网，可采用服务器搭建的方式来实现；采用专门软件或硬件来实现；很多硬件设备均具备 VPN 功能，如防火墙和路由器等，然而这些设备与不具备该功能的设备相比价格都比较昂贵。VPN 接入方式如图 1 所示。

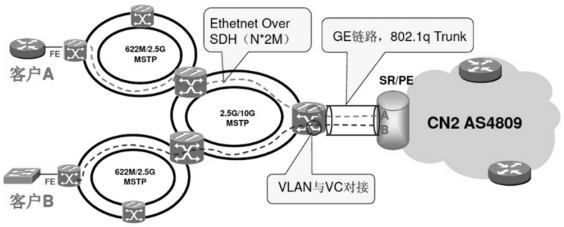

图 1 VPN 接入方式

2 VPN 优缺点

2.1 优点

(1)VPN 的应用能让所有员工及合伙人只利用本地宽带网即可实现对企业网络的连接，使宽带网成为一种高效且低成本的办公工具。

(2)VPN 具有模块化特征且可进行升级。采用 VPN 能使用户使用设置难度很低的基础设施，帮助新用户简单且快速的添加至该网络。因此，企业能在增加基础设施的情况下提供更多的应用及容量。

(3)基于虚拟专用网，用户能实现对 ISP 服务及设施的引用，并能掌握网络绝对控制权。充分利用 ISP 各项网络资源，无论是网路管理变化与安全设置都能由自己完成管理。另外，在企业的内部也可实现虚拟专用网的建立。

2.2 缺点

(1)企业无法对以互联网为基础的 VPN 性能及可靠性进行直接控制。机构需通过提供 VPN 的互联网服务确保服务得以正常运行。该因素决定了签署服务级协议是十分重要，即签署能确

保各项性能指标均符合要求的协议。

（2）企业创建并部署相应的线路是一项难度很大的工作。VPN 的应用要以深入理解网络及安全方面的问题为前提，做好规划与配置工作。基于此，由提供商对 VPN 实际运行负责在大多数情况下是一个很好的选择[1]。

（3）不同厂商所提供的 VPN 解决方案并不兼容，由于很多厂商都不愿意或未能严格遵守相关技术标准，所以若对不同厂商提供的产品进行混合使用将带来很多技术问题。如果只使用一个厂商提供的设备，其成本往往很高。

3 关键技术与应用

对于 VPN，一般采用以下技术来有效保证安全：

（1）隧道技术，该技术能在使网络标准保持不变的情况下，通过公共网络实现应用，使网络与用户实现连接及通信，利用 IP 协议等可路由协议通过网络将数据报传输至目标网络。就目前来看，主要采用对组播数据报进行封装的方式，使组播数据包被转换为 IP 数据报。对于 IP 数据报，其报头结构有所不同，可容纳所有组播数据报，封装过程中，IP 地址与最终目标都会插入至报头当中。之后通过协议算法传输数据报，由路由器进行发送，由目标路由器负责接收。在数据报被目标路由器接收后，开始解包，IP 地址将被组播地址完全代替，最后将数据报提供给主机。

（2）加密技术，VPN 的应用能有效提高安全水平，通过加密与身份识别可以保护数据防止窥探，防止数据窃贼与其他所有未经授权的用户获得数据。鉴于此，对 VPN 而言，主要采用公钥与对称两种加密体制充分结合的方式。其中，对于对称加密，其通信双方能对一个密钥予以共享，发送方通过这一密钥的应用能使明文变为密文，而接受方通过对相同密钥的应用能使密文变为到明文。对于公钥加密，亦可成为非对称加密。在实际通信时，发送方借助接受方公开密钥对信息进行加密，也能用发送方密钥对信息进行加密，并完成数字签名。在接收方获得消息之后，能用自己有用的密钥来解密，同时用发送方对应的密钥对数字签名予以解密，实现对发送方身份的有效验证。然按照不同形式，可将数据加密分成不同种类，数据加密贯穿在全过程当中，包括信息的存储、传输、鉴别及管理[2]。然而，在使用无线设备的情况下，VPN 均存在一定安全风险。接入点间的漫游很容易产生各类问题。比如用户在不同接入点之间进行漫游时，无论采用何种加密技术都会被攻破，进而威胁到网络安全。

（3）密钥管理技术，该关键技术主要任务在于保证公用数据网中密钥传递安全性。对于对称密钥，发送方可针对所有信息均声称唯一的对称密钥，同时利用公开密钥实施加密，再将完成加密的密钥与加密信息同时发送至接收方；对于公开密钥，电子商务领域主要采用的是数字证书，发送方与接受方均可以借助数字证书对公开密钥进行交换。

（4）身份认证技术，这是一项网络安全领域最为常用且直接的技术，能对合法和非法的用户进行识别，在使用网络前，先在身份认证系统中表明身份，经系统识别确认以后，以用户身份及权限级别为依据，确定能否对资源进行访问或能否执行某些操作，在对授权操作予以监督的同时避免非法操作的产生，这是避免黑客入侵与病毒破坏最为直接且有效的方式，在当前的信息安全领域占据重要地位。如今，身份认证技术快速发展得到了人员的高度重视，如按照层次与出现先后顺序，可将其分成以下几种：静态口令、一次性口令、数字证书与生物特征技术[3]。

在当前这个网络时代中，企业规模越来越大，各分支机构实际覆盖范围日益广泛，其内部与合作伙伴通信必将越来越频繁。因公网采用非加密明文实施传输，无论是安全性还是保密性都很差，而且入侵检测、防火墙与加密传输的方式有很高的成本，同时大多以被动式防御为主，无法满足现代企业发展提出的要求。VPN 凭借其加密传输与公网连接等优势，得到了更多企业的认可和信赖。企业信息大多存储于总部，总部的主机数量很多且数据流量巨大，对数据实时性与安全性都提出了很高要求。而在分支机构当中通常建有很多局域网，并在 ISP 的支持下和 Internet 网相连，VPN 网关主要部署于内网和 Internet 网之间的接口部位。人员能在访问内网的过程中，无须借助网关设备，在实际上安装并启动安全包方可完成访问。

如今，互联网正快速发展，电子商务不断成为人类商务活动主要模式。在很多企业中，都采用 Internet 实施商务活动，然而，其安全问题限制了其发展，如何建成一个便捷且安全的环境，保护信息，用户与商家都极其关心。对此，采用 VPN 可以为用户建立一个隧道，提供和令用网络相同的保障功能，并通过对组网的应用，还能减少通讯与组网方面的费用，提高灵活性，为开展电子商务活动的企业提供一个畅通其安全的网络，有效解决基础网络安全方面的问题。

4 结语

综上所述，网络的出现和应用在很大程度上改变了很多行业的具体运作方式，信息运营在完成了互联及资源共享。同时，网络安全也陆续得到更多人的关注和重视。在这种发展局势下，VPN 的出现和应用可以提供一种安全稳定且简洁高效的解决方法，目前正得到越来越广泛的应用。

参考文献

[1] 王景灏. 移动互联网络安全认证及安全应用中若干关键技术研究[J]. 黑龙江科技信息，2016，11(30)：188.

[2] 张莹.移动互联网络安全认证及安全应用中若干关键技术研究[J].无线互联科技，2016，12(8)：45-46.

[3] 冯常青. 移动互联网络安全认证及安全应用中若干关键技术研究分析[J].硅谷，2014，7(21)：35-36.

收稿日期：2021-03-06

作者简介：陈红忠（1968— ），男，汉族，云南昆明人，本科，工程师，主要从事计算机网络运维、办公室 OA 软件开发、服务器数据库管理、计算机系统维护、工业 PLC 程序开发、工业控制网络设计与配置工作。