远程接入中的安全访问控制

刘晓宇

（天津市信息中心 应用开发处，天津 300000）

摘 要：以实际项目应用为例，利用 VPN、防火墙、策略交换机等几种典型设备，对解决企业的远程办公接入问题进行深入探究。

关键词：远程接入；VPN 技术；网络安全

中图分类号：TP302.1 **文献标识码**：A **文章编号**：1674-7720(2012)05-0052-02

Remote access of security access control

Liu Xiaoyu

(Department of Application Development, Tianjin Information Center, Tianjin 300000, China)

Abstract: This paper takes the application of actual project as an example, using VPN, firewalls, switches and other types of equipment, discusses the access problems of enterprise remote office.

Key words: remote access; VPN technology; network security

大型企业通常会有若干分驻全国各地的分支机构和为数不少的出差人员，为了解决这些员工的远程办公问题，使他们能够及时了解企业运转情况和参与生产、经营、管理工作的流程运转，远程接入成为一个现实的需求。

VPN 技术、防火墙的安全过滤技术、三层交换机的路由和控制技术共同实现了远程用户对企业不同应用域的安全访问控制。通过 VPN 接入，企业可以保证出差在外的员工访问公司里的信息，此外，通过笔记本电脑和一张基于 VPN 的 CDMA1X 卡，员工可以真正实现随时随地访问企业局域网的愿望。

1 远程访问的主要技术手段

某大型供电企业网络远程访问系统的拓扑图如图 1 所示，主要由 VPN 客户端软件、VPN 客户端 E-Key、VPN 网关、密钥管理中心、防火墙和策略路由交换机组成。该系统满足了企业员工通过多种网络环境，利用互联网通道访问企业内部网络资源的需求。通过身份认证系统确保了远程网络用户的真实性；通过对网络传递数据的加密确保了网络传输数据的机密性、真实性和完整性；通过对用户的分级管理和访问管理域的划分设定了不同类别的认证用户对 OA 办公区域、输变电生产管理区域、配网生产管理区域和市场营销管理区域等不同应用区域的访问权限，有效降低了企业信息资源的潜在风险。

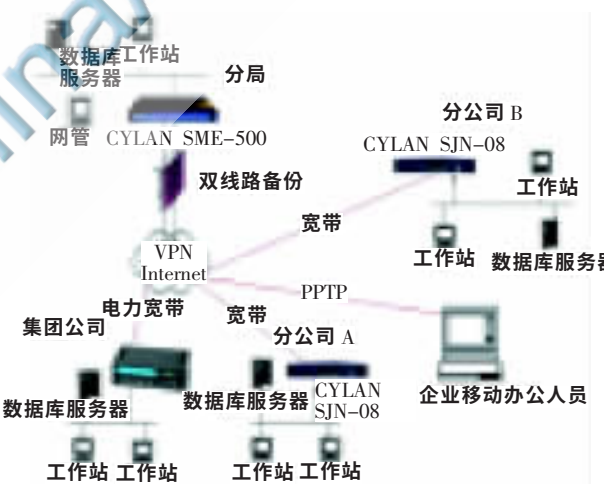

图 1 某大型供电企业网络远程访问系统的拓扑图

2 企业选择 IPSec 技术的主要原因

企业选择 IPSec 技术的主要原因有以下几个方面：

（1）经济。不用承担昂贵的固定线路的租费。DDN、帧中继和 SDH 的异地收费随着通信距离的增加而递增，分支越远，租费越高，而基于 Internet 则只承担本地的接入费用。

（2）灵活。连接 Internet 的方式可以是 10 Mb/s、100 Mb/s 端口，也可以是 2 Mb/s 或更低速的端口，还可以是便宜

的DSL连接，甚至可以是拨号连接。

（3）广泛。IPSecVPN的核心设备扩展性好，一个端口可以同时连接多个分支，包括分支部门和移动办公的用户。

（4）多业务。远程的IP话音业务和视频也可传送到远端分支和移动用户，连同数据业务一起，为现代化办公提供便利条件，节省大量长途话费。

（5）安全。IPSecVPN的显著特点是其安全性，这是它保证内部数据安全的根本。在VPN交换机上，通过支持所有领先的通道协议、数据加密、过滤/防火墙以及通过Radius、LDAP和SecurID实现授权等多种方式保证安全。同时，VPN设备提供内置防火墙功能，可以在VPN通道之外，从公网到私网接口传输流量。

3 系统的实现

该大型企业采用北电的PP8606路由交换机，以提供不同应用安全域的网段划分和策略控制。同时，部署带VPN功能的NetEye防火墙，它集VPN网关、密钥管理中心和防火墙于一体，提供密钥的生成、管理与分发，完成认证区域的划分、用户的接入和认证、用户IP地址的分配与访问控制功能。

3.1 通信密钥的生成与管理

VPN网络安全的关键是保证整个系统的密钥管理安全。NetEyeVPN采用基于PKI的密钥管理框架，实现安全可靠的密钥分发与管理。

密钥管理中心设立在网络中心。登录密钥管理中心后，在密钥加密卡内生成RSA公私钥对，通过使用专用的密钥加密卡作为密钥传递介质，并采用密钥加密密钥，保证了密钥颁发过程中的安全性。然后通过密钥管理中心添加VPN网关的IP地址和密钥交换端口信息，生成网关密钥和全局公钥文件。全局公钥文件使用管理中心的私钥签名，可以防止在传送过程中被替换或篡改。

3.2 VPN网关的密钥配置及用户E-Key的生成

上载合适的License许可后，就开启了NetEyeVPN防火墙的VPN功能，形成VPN网关。对VPN网关注入密钥管理中心生成的网关密钥对和全局公钥文件后，就可以在VPN网关上建立用户认证域。创建时可以选择本地认证或Radius认证，在认证域中创建用户，添加用户名和用户密码信息，生成用户E-Key。用户E-Key主要保存用户认证证书文件和用户名信息，以增强用户认证的安全性。

3.3 用户的登录认证与数据传输安全性的保证

当VPN用户通过VPN客户端软件和VPN客户端E-Key对VPN网关发送连接请求时，VPN网关对VPN用户进行鉴别与认证。其中，会话密钥按照IKE协议自动协商生成，并用协商好的密钥对数据进行加密。用户认证成功后，通过创建SA以及SA的组合（AH、ESP、IPIP）建立远程用户的访问隧道。NetEyeVPN遵循IPSec（IPSecurity）安全协议，采用隧道方式为用户数据提供加密、完整性验证，并通过集成的认证服务为信息传输提供安全保护。

3.4 应用区域的划分

在VPN网关的认证域中创建用户时，针对不同性质的用户创建了多个角色名称，分别对应于OA、生产、配网和营销等应用区域。设定VPN网关隧道虚拟设备IP地址池，将池中的IP地址分别分配到角色中，对应各应用域。在用户登录并经过认证后，用户将根据自己所属的角色分配IP地址，并自动加入到自己的应用域中。

4 系统的安全访问控制

VPN用户和VPN网关之间在公网上建立VPN网络通道之后，还需要通过安全策略和安全规则的制定，进一步把网络分成不同的安全访问区域，控制用户对不同安全区域的访问，使网络的安全性得到进一步提升。

防火墙一般位于企业网络的边缘控制点，如与Internet的连接处，还可以部署在企业网络内部的安全区域控制点上。安全区域防御的弱点是不能抵御来自区域内部的“合法”用户的攻击，如恶意或无意的内部用户，没有防火墙和安全保护较弱的远程移动工作者或SOHO被身份窃取者，以及安全区域存在的后门漏洞（无线网络、远程访问）等。

采用防火墙技术，通过制定安全策略可以实现对用户的访问进行控制和过滤。主要过滤内容为用户访问信息的源目的IP地址、目的端口号和连接协议等。经过防火墙安全控制策略过滤后的VPN用户将根据其所属角色及分配的IP地址范围访问经过授权的应用域，比如只能访问OA、生产管理、配网管理和营销应用域的其中之一或者几个域的组合。

本文采用北电的PP8606路由交换机，对不同的被访问应用安全域进行网段划分，建立网段连接路由信息和VPN客户IP返回路由。在路由交换机与VPN网关的互连端口上进行访问过滤控制策略，制定只允许合法的源IP地址、协议访问对应的应用域。本方法进一步加强了VPN用户对应用安全域的访问控制，从而在最大程度上减少了安全风险和不安全因素。

参考文献

[1] 李建福，唐建伟.远程接入VPN用户解决方案[J].通信世界，2006，（21B）：16-17.
[2] 翁玉良，王炳志.基于互联网技术的ERP远程接入问题研究[N].中国建材报，2008-02-18.
[3] JOHNSON J T.更好地连接远程工作人员[N].网络世界，2003-05-26.
[4] 李然.VPN带来改变[N].中国经营报，2003-02-10.
[5] 边歆.远程接入机会多多[N].网络世界，2007-07-16.
[6] 叶盛，高海锋，张根度.VPN的实现机制和系统评价[J].小型微型计算机系统，2002，23（9）：1053-1058.
[7] 刘丽，郭建.IPSec VPN远程接入MPLS VPN的几种方式[J].现代电信科技，2005，（9）：61-62.

（收稿日期：2011-11-02）

作者简介：
刘晓宇，男，1981年生，工程硕士，主要研究方向：.Net、Java程序开发、计算机网络。