飞塔防火墙的SSL VPN技术在企业远程办公中的应用

张 玮
（中国石化华东油气分公司勘探开发研究院，江苏 南京 210036）

摘要：随着网络技术的高速发展，拥有多个异地分支机构的企业在其信息化建设中，必须具备良好的移动办公能力和需求，企业员工在基于Internet或4G网络下能随时异地访问企业内部网络，高效开展各类办公业务。SSL VPN是远程用户访问企业内部数据最快、最安全、最有效的技术。用户可以通过其快捷安全地实现远程办公，帮助企业提高生产力，增强网络安全。同时也可以降低企业的管理和运维成本。针对具有市场占有率较高的飞塔防火墙网络安全网关产品，讨论通过其SSL VPN虚拟专用网络技术构建适合企业应用需求的远程办公系统。

关键词：飞塔；SSL VPN；网络；远程办公
中图分类号：TP393 **文献标识码：**A

Effect of SSL VPN of Fortinet on telecommuting of enterprise

Zhang Wei
(Exploration and Development Research Institution, East China Company, Nanjing, Jiangsu 210036, China)

Abstract: With the rapid development of the network, during the information construction of the enterprises with multiple branches in different places, great mobile office capabilities are needed. The employees of the enterprises can access the Intranet of an enterprise at any time from another place under the Internet or 4G network to do the work efficiently. SSL VPN is the fastest, safest and most efficient technology for remote users to access the internal enterprise data. Through it, the quick and safe telecommuting for the users work remotely can help the enterprises to improve the productivity and enhance the network security. It can also reduce the management and operation cost of the enterprises. Aiming at the Fortinet, which has high market share, the telecommuting system suitable for the enterprise's needs is established by its SSL VPN virtual private network technology.

Key words: Fortinet, SSL VPN, network, telecommuting

1 前言

随着企业信息化建设工作的不断投入，各类应用系统如OA、ERP、合同等各类数据库系统的部署逐步实现了企业内部的无纸化网络办公，提高了生产、工作和学习的效率。但这些系统都是基于企业内网而建立的，而大中型企业员工跨区域工作和出差情况频繁，当其在其它区域工作时，将会离开公司内网，因此，需要从远程访问企业内部网络。此时，有必要通过安全快速的技术完成网络连接和资源共享，而VPN技术可以为企业提供更简单，更安全的远程网络技术，同时具备优异的网络性能和兼容性。

2 VPN原理概述及分类

2.1 VPN技术概述

VPN虚拟专用网是一种使用安全协议、身份验证，数据加密和其它技术在公共网络体系结构（通常是Internet）上建立的企业专用线路。它同时也是一个安全的网络隧道，可确保信息传输的安全性、完整性和真实性。VPN技术具备以下功能：加密数据以完成安全传输，确保公共网络上传输的数据不被其

收稿日期：2018-07-04。
作者简介：张玮（1984—），男，助理工程师，计算机信息技术研究。

他人拦截和破译;可以实现信息认证和身份认证,保证用户信息的安全性和合法性,并跟踪用户登录数据;实现访问控制,它可以对不同的用户级别划分权限,并控制其对资源的访问[1](图1)。

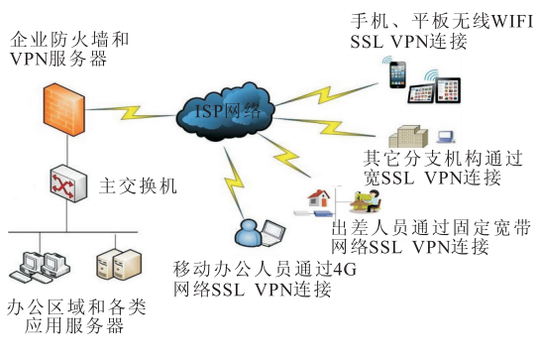

图1 SSL VPN连接到企业内部网络的示意图

Fig. 1 Connection of SSL VPN to the Intranet of the enterprise

VPN技术可根据其安全协议分为以下几类:①隧道协议(PPTP)是一种由多协议模式支持的虚拟网络技术,是微软联合相关的网络设备供应商共同开发的VPN技术;② L2 TP协议是一种将PPTP和第二层转发相互结合的协议,由IETF开发,目前是IETF第2层隧道协议的行业标准;③IPSec是基于IETF形成的开放标准框架,其目标是确保网络层面上的流量安全;④SSL协议即Secure Sockets Layer是一种高级安全协议,可分为两层:SSL记录协议,它建立在可靠的传输协议之上,并为更高层协议提供数据封装,压缩和加密等基本功能;另外一层是SSL握手协议,在实际数据传输开始之前,用于通信方的身份,加密算法的协商,加密密钥的交换等;⑤MPLS多协议标签转换协议基于分组交换技术,通过交换标签和ARIS服务扩展而形成。

2.2 SSL VPN协议的优势

SSL的英文全称是“Secure Sockets Layer”,中文名为“安全套接层协议层”。SSL协议指定了一种在应用程序协议和TCP / IP协议之间提供数据安全分层的机制。它为远程连接提供数据加密,服务器身份验证,消息完整性和可选的客户端身份验证。协议的三个特征是机密性、可识别性和完整性。与其它协议相比,它具有更强大的技术优势[2]。

1)传输过程安全。传输的进程加密强度确定网络的内部数据不被黑客拦截。传输过程中数据的加密强度越高,传输安全性就越高。在应用层建立的通道可以防止病毒、蠕虫和其它威胁。在SSL VPN协议下,所有客户端访问都由SSL VPN网关转发,并且不能直接访问应用服务器,因此,服务器不容易受到病毒、黑客等的攻击。IPSec VPN则是连接到公司的内部网络,内部网络的应用程序和系统可能会暴露给黑客。

2)用户身份验证。传统的用户名和密码验证相对简单,安全性不高。SSL协议利用PKI体系进行加密,效果比较好。

3)客户端设备的安全性。客户端计算机需要安装防病毒软件、防火墙等,以防止SSL VPN密码被木马窃取,因此SSL VPN需要检测客户端。

4)确保现有网络运行的稳定性,SSL VPN避免改变现有的网络拓扑,不受客户端和服务器NAT设备之间安装的防火墙的影响,穿透能力强。

5)IPSec VPN要求在远程访问客户端上正确安装和配置IPSec客户端软件和访问设备,其连接受网络地址转换或网关代理设备的影响。

6)SSL VPN具有更好的访问控制策略。SSL VPN侧重于保护特定的敏感数据,并且可以根据用户的不同身份赋予不同的访问权限。通过匹配某些身份认证,不仅可以控制访问人员的权限,而且可以对访问人员每次访问的关键信息进行数字签名,它为事后跟踪提供了基础。使用IPSec VPN网关时,用户可以任意访问Intranet中的资源,不能完全保护内部数据[3]。

7)SSL VPN具有更好的经济性。因为SSL VPN只需要在企业内部放置一台服务器,即可为所有用户实现远程安全访问。但是,对于IP Sec协议,每个附加访问分支都需要添加额外的硬件设备。

8)服务端的日志跟踪。SSL VPN服务器提供访问统计和跟踪功能。因此为服务器提供了更安全的方式。

2.3 SSL VPN面向的对象

首先,需要随时访问企业内部网络资源的移动办公用户,如信息系统管理员,出差人员和需要随时审批的人员。对于上述人员,远程SSL VPN可以通过Internet或4G网卡访问企业内部网络,随时随地访问内部数据,无需受限于当前设备的网络环境配置。

第二个是需要访问内部网络资源的合作伙伴或用户。网络管理员可以根据具体情况限制其对不同

应用权限的访问,用户只能访问受限制站点或站点中的某些页面和相关数据库[4]。

3 飞塔防火墙SSL VPN的优势与架设方案分析

3.1 飞塔防火墙的SSL VPN功能简介

作为行业领先的防火墙厂商,它结合了高性能VPN功能,代表了网络安全的新概念。突出了多功能实时网络防护的优势,完全适合各类系统网络的安全应用。客户端通过SSL VPN加密认证安全连接服务器后,员工可以根据不同的账号权限访问对应的企业网络资源。还可以扩展到访问无线网络设备,以实现资源调用和办公系统的共享。其SSL VPN具有以下几个特点:

1）提供有效数据加密:在飞塔中,SSL VPN系统在访问办公系统时需要加密,加密算法可以在公钥算法、私钥算法和消息认证中选择,从而实现更好的加密效果,保证了数据的安全性[5]。

2）底层数据安全性高:远程访问中,底层数据安全性是重中之重。飞塔产品具有相对独立的操作系统,大大减少了服务器的工作量,同时提高了应用服务器的响应能力。

3）飞塔产品具有硬件加速功能,SSL握手和加密传输都可以获得硬件加速,这为CPU提供了更多的资源空间来处理高级功能。

4）安全检测控制:飞塔客户端的安全保护模块可以自动检测安全管理中客户端的状态。并根据预设策略完成客户端登录管理,分配不同的访问策略。客户端安全模块还可以激活安全桌面功能,清除退出时的cookie,提高安全性能,并帮助企业确保关键应用和数据的安全性。

3.2 飞塔SSL VPN移动办公的整体解决方案

图2是企业的常见网络拓扑图。内部部署了网站和应用程序系统服务器,ERP,OA办公系统,即时消息系统和其它业务系统。以常见的飞塔Fortinet 200 B系统防火墙为例,解决移动用户,合作伙伴,分支机构等通过Internet访问企业内网的问题。通过SSL VPN协议技术建立安全的端到端访问。

企业移动办公首先考虑安全性和性能。飞塔

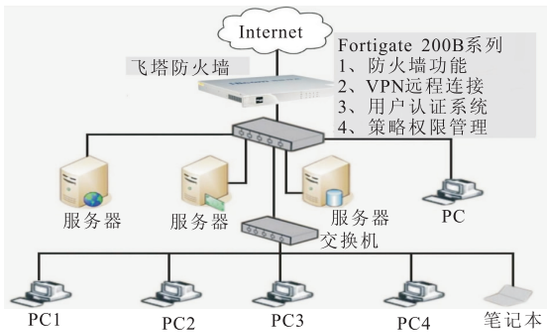

图2　使用飞塔防火墙的企业网络拓扑图

Fig. 2　Network topology of enterprise by Fortinet

200 B综合考虑该企业系统的功能与要求,VPN拓展为600人并发等级,可以对接入的用户进行精确的身份认证、权限划分,通过逻辑隔离服务器,具有不同身份的用户可以访问不同的应用程序服务器并使用不同的业务系统和资源。从而保证数据的安全传输。并且通过SSL VPN实现应用系统访问的集中管控,降低管理和维护成本,结合SSL VPN自动登录及应用系统单点登录技术,大大提高办公系统易用性。

3.2.1 服务端配置

以管理员身份登录飞塔200B防火墙SSL-VPN设置页面,点击启动SSL-VPN功能。在开通隧道模式后,系统将虚拟化出一个“ssl.root”接口,相关访问的流量都通过此接口进出。设置和创建通过VPN连接认证的用户和用户组(图3)。

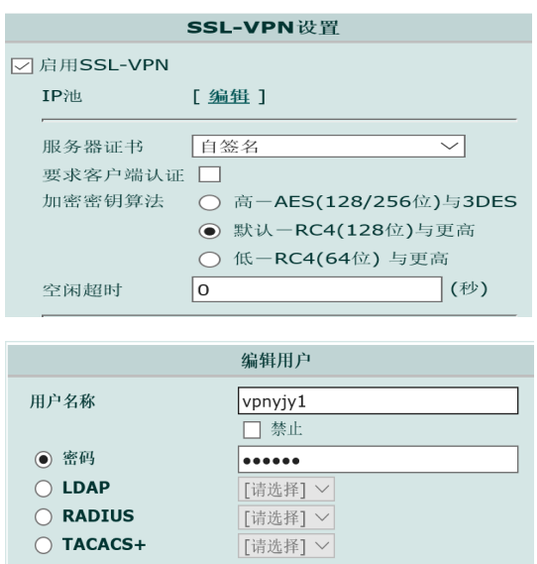

图3　设置SSL VPN功能及登录用户、用户组

Fig. 3　Function set of SSL VPN and users and user groups login

图4 设置防火墙出入口策略

Fig. 4 Set up of firewall

新建防火墙策略,设置从互联网到企业主干网、分支网络设备的访问权限(图4)。

将虚拟端口数据转发到用户VPN客户端,启动NAT内网地址转换。配置SSL VPN虚拟网关设备的静态路由,从而实现将IP地址DHCP分配到远程客户端(图5)

图5 设置SSL VPN路由及策略

Fig. 5 Set up of SSL VPN route and strategy

3.2.2 远程客户端的配置

下载Fortinet专属的SSL VPN客户端,安装后,打开软件界面,点击新建一个连接名称,输入服务器地址,用户名和密码,单击“连接”,连接成功,即可访问企业的内部资源。如果要访问企业内部域名应用

图6 客户端SSL VPN设置

Fig. 6 Set up of SSL VPN for client-side

系统,则找到虚拟拨号连接的DNS设置,改为企业专用的域名服务器,它可以实现私有域名解析和对各种业务系统的正常访问(图6)。

4 结束语

通过部署飞塔SSL VPN解决方案,有效解决了企业安全移动办公的问题。方便出差员工和分支机构访问企业内部的网络资源。同时,它确保了远程用户上传和下载数据的安全性。基于SSL VPN的远程办公可以有效降低企业成本,端到端的安全传输提高了数据的安全性和机密性。基于飞塔的SSL VPN技术易于维护和使用,推动了企业远程办公的快速发展。

参 考 文 献

[1] 张成,敬明旻,张强.应用SSL VPN实现国有企业移动办公的优势与方案[J].计算机光盘软件与应用,2012,15(15):147-148.

[2] 蔡加柳.应用SSL VPN实现安全移动办公[J].科技创新导报,2011,8(33):21.

[3] 丁锦武.基于SSL技术VPN在企业网络的应用[J].企业技术开发,2012,31(14):89-90.

[4] 潘华.基于SSL VPN的数字校园网络应用研究[J].电脑知识与技术,2013,9(28):6470-6472.

[5] 谢朝华.Fortinet:新运营时代需要专属安全[N].中国计算机报,2009-05-18(1-2).

(编辑 尹淑容)