高速 SSL 协议芯片关键技术研究

桂祚勤,孟 涛,崔广财,林存花,陈浩涓
(江南计算技术研究所,江苏 无锡 214000)

摘 要:在信息安全领域快速发展的形势下,SSL VPN (secure socket layer virtual private network)作为主流安全访问及控制系统得到了广泛应用。随着千兆、万兆网络的发展,用户对于网络访问的速度要求更高,传统的软件实现 SSL VPN 已经无法满足网络高速发展的需求。在对 SSL 协议深入研究的基础上,提出基于 SSL 专用处理器和 TCP 硬核的 SSL 协议芯片设计模型,该设计采用 TCAM(ternary content access memory)+SRAM 的策略查找映射方式,有效降低系统开销,提升 SSL 的处理速度。针对 VPN 通信流的特点,将访问控制与 VPN 隧道、转发机制紧耦合,从而增强网络安全性。基于此模型设计的高速 SSL 协议芯片,可通过简单改变系统配置参数应对不同的网络环境,使其既可以工作在虚拟网络模式下,又可以工作在代理模式下,满足了多样化、快速化网络部署需求。

关键词:安全套接层;虚拟网络模式;代理模式;专用处理器;TCP 硬核
中图分类号:TN918 **文献标识码**:A **文章编号**:1673-629X(2020)06-0094-05
doi:10.3969/j.issn.1673-629X.2020.06.018

Research on Key Techniques of High Speed SSL Protocol Chip

GUI Zuo-qin,MENG Tao,CUI Guang-cai,LIN Cun-hua,CHEN Hao-juan
(Jiangnan Institute of Computing Technology,Wuxi 214000,China)

Abstract:In the context of rapid development in the field of information security,SSL VPN is widely used as the mainstream security and control system. With the development of 1 000Mbps and 10Gbps network,users have higher requirements on the speed of network access,and the traditional software implementation of SSL VPN has been unable to meet the needs of high-speed network development. Based on the deep research of SSL protocol,a SSL protocol chip design model is presented based on SSL ASIP and TCP hard core. The policy search mapping method of TCAM+SRAM is adopted to effectively reduce system overhead and improve the SSL processing speed. According to the characteristics of VPN communication stream,the access control is tightly coupled with VPN tunnel and transmission mechanism to enhance network security. The design of high speed SSL chip can response to different network environments by simply changing the configuration parameters of system,so it can work at virtual mode and agency mode which satisfy the need of diversity and rapid network deployment.

Key words:SSL;virtual work;agency work;ASIP;TCP core

0 引 言

SSL[1]安全套接层是网景公司提出的一种在客户端和服务器端之间提供安全通道的协议。经 SSL 安全协议处理后,客户与服务器之间传输的数据是加密的,客户端写入数据时自动被加密,到服务器端读出数据时又自动解密成明文[2],保证了信息的安全性和完整性。此外,SSL 安全协议还可以通过握手使通信双方相互交换数字证书信息,来确保对方身份的合法性。SSL 协议由握手协议层和记录协议层组成[3],主要包括记录协议以及建立在记录协议之上的握手协议、警告协议、更改密码说明协议和应用数据协议等子协议,位于 TCP/IP 协议模型的网络层和应用层之间,使用 TCP 协议来提供一种可靠的端到端的安全服务。SSL 协议在应用层通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作,在此之后,应用层协议所传送的数据都会被加密,这些密文数据被放入 TCP/IP 协议的发送队列中,并根据实时网络状况发送给对端,在传输过程中密文数据被分散到不同的 TCP/IP 报文中,在 TCP/IP 包的报头中并没有加密片段的概念,无形之中增加了解密的复杂度,TCP/IP 协议也间接地增加了 SSL 协议的安全性。

SSL 协议的实现对于服务器的计算资源开销很

收稿日期:2019-08-05 **修回日期**:2019-12-10
基金项目:国家自然科学基金(6732018)
作者简介:桂祚勤(1964-),男,硕士,高级工程师,研究方向为信息安全。

大[4],且并不是所有的应用都需要保密性、消息完整性和端认证服务,因此文中提出了一种高速 SSL 芯片设计模型,该设计模型采用 TCAM+SRAM 查找映射的方式进行区分服务,减小了系统不必要的开销;同时为了提升 SSL 安全协议的处理速度,自主设计了专用 SSL 安全协议处理器[5] 和 TCP[6] 硬核模块,提高了 SSL 流量和服务器的处理性能。

1　芯片框架模型

提出的高速 SSL 芯片设计模型既支持虚拟网络模式[7-10] 又支持 TCP 代理模式[11-13],可以在不关心内网具体应用形式下,满足一定的策略规则就可以映射到相应的安全策略[14]。

芯片框架结构如图 1 所示。

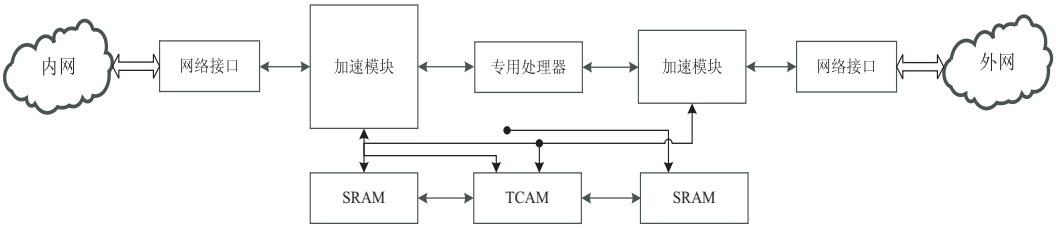

图 1　高速 SSL 芯片框图

网络接口模块主要负责网络包的接收与发送;加速模块又包含两部分:专用缓冲处理模块 BM 和硬件化的 TCP 协议处理模块,这两个模块辅助专用处理器完成不同应用模式下的 SSL 协议处理;专用处理器配备一套专用指令集和一套精简的通用指令集,主要负责通用网络包及 SSL 协议报文的处理;SRAM 中存储各个链接/隧道的具体处理策略;TCAM 中存储映射到各个链接/隧道的规则;SRAM+TCAM 模块的组合设计完成了链接/隧道的映射。

1.1　芯片工作模式

当芯片工作在虚拟网络模式下,根据配置,靠近内网的加速模块启用专用缓冲处理模块(BM),靠近外网的加速模块启用硬件化的 TCP 协议处理模块。从内网进入的网络包由 SRAM+TCAM 模块完成隧道映射后,分别进入 BM 缓冲区,当 BM 缓冲达到一定阈值或缓冲时间达到设定的超时时间后,以消息包的形式通知专用指令集处理器(ASIP),由 ASIP 根据 TCP 协议处理模块的实时处理情况决定是否提取数据到 TCP 的发送缓存中,若可以提取,则由 ASIP 完成 SSL 记录协议处理后以消息包的形式将数据打入 TCP 的发送缓存,TCP 加速模块根据 TCP 协议组装成 TCP/IP 报文后发送给外网;另外一个方向,从外网进入的网络包由 SRAM+TCAM 模块完成隧道映射后,进入 TCP 协议处理模块的接收缓存,TCP 协议处理模块内部的用户指令模块根据接收缓存的数据存储情况,自动提取数据递交给 ASIP,由 ASIP 完成后续 SSL 记录协议的处理工作,完成后将数据流发送给下行的 BM 处理模块,由其负责完成后续的 MAC 帧切割等处理工作,最终恢复成标准网络包后经由内网口发送到内部网络中。以上两个方向的处理流程是同时进行的,每个方向均可以达到千兆的处理带宽。

当芯片工作在 TCP 代理模式下,根据设计,两个加速模块均只启用 TCP 协议处理模块,与 ASIP 之间以消息包的形式进行通信。ASIP 给加速模块发送消息包申请链接建立,当加速模块完成链接建立后,发送消息包通知 ASIP 链接建立已经完成,ASIP 再将与其对应的策略绑定到该链接上,因此在处理 TCP 包时不需要处理策略等信息,只需将当前包所属的链接条目匹配出来,发送给 TCP 协议处理模块,TCP 协议处理模块根据链接条目读取该链接的状态信息和数据,轮询所有链接的接收和发送缓冲区,根据缓冲区数量确定是组装 TCP 报文还是发送消息包给 ASIP。当满足发包条件时,依据该链接对应的 SRAM 中相应字段策略进行组包并发送出去。

TCP 协议处理模块接收及发送缓冲以链表方式进行管理。首先需要解析出网络包的 TCP/IP/MAC 头,然后存储报文的 TCP 数据负载。TCP 协议处理模块以描述符的方式记录当前数据包所归属的 TCP 链接,以指针信息记录对应链接已接收的数据量,这些即为当前链接的状态信息,存储在 SRAM 中。

1.2　芯片安全性分析

根据芯片的具体工作模式及应用场景,与外部网络相连的均为 TCP 协议硬件加速模块,一般认为来自网络的威胁或攻击均出自外部网络,而 TCP 协议本身就有很好的抗攻击能力,这样承载在 TCP 协议之上的 SSL 协议就可以防止病毒、蠕虫等经由网络层传输的威胁。当芯片工作在 TCP 代理模式下,所有客户端的访问都是由芯片转发,而不能直接访问应用服务器,从而使服务器不易受到病毒、黑客等的攻击,而且芯片还可以提供细粒度的强访问控制和日志审计等功能,方便设备管理员及时应对突发状况。除此之外,芯片还具有防火墙功能,可以通过其将网络内部需要被授权外部访问的应用映射到防火墙的策略上,只有满足需求的链接才有权访问。

2 芯片实现的关键技术

2.1 专用 SSL 协议处理器设计技术

网络包复杂多样,采用处理器的方式可以灵活处理各种网络包,但针对网络协议处理这一单一功能,会浪费通用处理器的很多资源,同时指令集也不能有效适配网络协议处理。采用专用协议处理器(ASIP)不仅可以实现网络协议的灵活处理,还可以提高处理的效率。

图 2 为单个专用处理器核的微结构。该处理器核采用取码、译码、执行、访存、回写等五级流水线结构,同时配备一套专用指令集和一套精简的通用指令集,可以支持 4 条指令并发执行,具有性能高、面积小等优势。

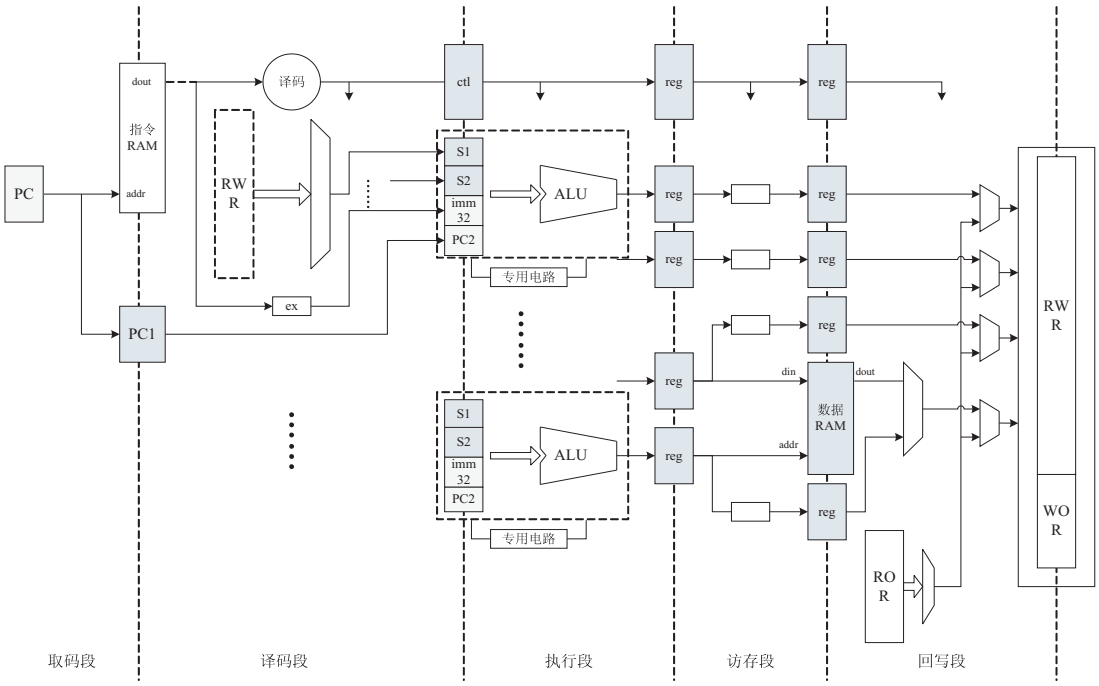

图 2 ASIP 微结构

高速 SSL 协议芯片中使用的专用处理器模块采用的是多核架构,在设计的过程中解决了以下技术难点:

(1)根据不同网络包的处理特点提炼出合理的指令集;

(2)处理器流水线级数的选取;

(3)硬件加速子模块的规划;

(4)多核资源调度。

经验证表明,该架构可以并发、灵活处理各种网络包。采用专用指令的流水线结构,提高了网络处理的带宽。

2.2 TCP 协议硬核加速模块设计技术

为了加速 TCP 协议处理和降低芯片设计代价,高速 SSL 协议芯片内部将整个 TCP 协议硬件化,总体框图如图 3 所示。使用专用 TCP 硬核替换通用的 CPU,可以降低芯片设计面积,提高内部处理带宽,但增加了设计的难度和风险。

TCP 硬核化设计是基于多个 RFC 协议的处理,设计中克服了协议的零散,无可整体参考等技术瓶颈。目前实现的 TCP 主要功能包括分片到达、用户指令、建链超时。其中分片到达设计最为复杂,主要根据标准 TCP 协议,融入了 SYN Flood、接收窗口糊涂算法、发送窗口糊涂算法、拥塞避免算法、TCP 重传超时、TCP 时间戳的处理。分片到达模块由链接建立,数据传输,链路关闭三个并行的模块组成。由于这五个主控模块是并行处理,因此当前的设计有很强的可扩展性,可根据需求将上述的模块进行复制以达到更高的处理带宽。

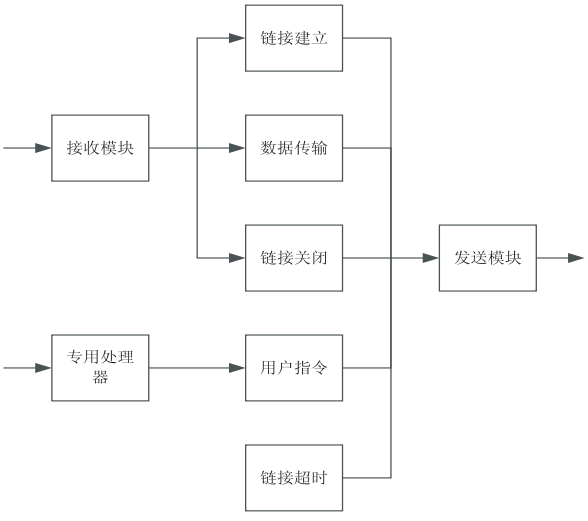

图 3 TCP 总体框图

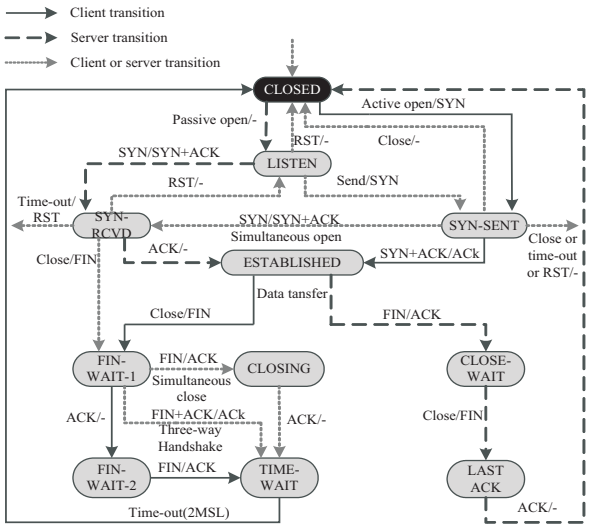

图 4　标准 TCP 状态跳转图

本芯片内部自主研发的 TCP 协议硬件加速模块,将图 4 所示的标准 TCP 状态跳转合理地分配到图 3 所示的 TCP 硬件设计总体框图的各个模块中,具体的硬件设计结合了 TCP 协议相关的 RFC 协议和 Linux 协议栈中 TCP 协议处理源码,下面详细描述各个 TCP 状态在各个模块中的划分。

链接建立模块包含 CLOSED,SYN_SENT,SYN_RECEIVED 三个状态的处理,该模块包含了建链之前、主动建链和被动建链三种情况的处理,模块的顶层根据输入状态来选择不同的状态跳转。如果输入 CLOSED 状态,就跳转到 CLOSED 处理流程,如果是 SYN_SENT 或 SYN_RECEIVED 状态,也跳转到相应的状态处理流程。为提高模块之间的并行处理效率,各状态处理模块对接收模块发来的数据先寄存、再处理,这样输入模块可以继续处理下一个 TCP 包,而不必等待各个状态处理结束。

数据传输模块主要包含 ESTABLISHED 状态的处理,整个 TCP 协议发送和接收数据相关的链表、状态位,以及与专用指令集处理器(ASIP)之间 SSL 握手协议、记录协议数据内容的递交等都是在该模块完成的,该模块也是整个 TCP 硬件处理的核心模块。

链接关闭模块主要包括如下状态的处理,链接关闭相关的状态为:FIN_WAIT_1,FIN_WAIT_2,TIME_WAIT,CLOSE_WAIT,LAST_ACK,CLOSING,在模块划分时根据其相关性将这些状态融合到一个处理模块当中。

用户指令模块主要负责与 ASIP 交互,处理 ASIP 下发的 open、send、close、abort、respond 等指令,是一个与软件交互的接口,它们之间通过消息包进行交互,用户指令模块在接收到 ASIP 的指令消息包后,按照 TCP 协议完成该命令的处理流程并给 ASIP 发送反馈消息包。

链接超时模块主要对计时器模块产生的超时信号进行处理,生成不同的超时响应包发给发送模块。超时处理的情况主要分为:超时关闭链接,超时发送 RST,超时保活探测,超时零窗口探测处理,超时发送重传队列,延迟确认。该模块会轮询读取并更新 SRAM 中的相关信息,当某条链接的超时信号有效时代表该链接超时情况发生,需要发送相应的 TCP 报文或关闭链接。

2.3　快速数据库查找设计技术

为了解决隧道/链接的映射问题[15],高速 SSL 协议芯片采用 TCAM+SRAM 的硬件查找方法。TCAM 存储映射规则,每条规则对应的执行动作作为查表结果存储在相应的 SRAM 中。由 TCAM 和 SRAM 配合完成网络报文的映射工作,一条规则对应一条 TCAM 条目,每个 TCAM 条目绑定一个 SRAM 存储空间,SRAM 存储空间可以有多个会话信息,但当前数据包只有一条适合的会话信息。该硬件实现方式能够满足高速查表的要求。

高速 SSL 协议芯片根据实际应用灵活地选择使用三元组(源 IP 地址、目的 IP 地址、协议)、四元组(源 IP 地址、目的 IP 地址、源端口和目的端口)还是五元组(源 IP 地址、目的 IP 地址、源端口、目的端口、协议)作为 TCAM 条目匹配的选择符,具体的处理流程如下:

(1)通过硬件协议头解析模块将报文选择符提取出来,发送给 TCAM 控制器进行匹配,支持飞行处理下一个报文;

(2)TCAM 返回的匹配结果直接发送给专用协议处理器;

(3)协议处理器直接将匹配结果作为 SRAM 读操作的地址输入,SRAM 中存储的内容即为该报文对应的安全策略;

(4)协议处理器根据安全策略内容处理相应报文。

通过芯片验证对该实现方法进行评估,表明用 TCAM+SRAM 的方法可以满足高速 SSL 协议芯片的性能,出网口速率可以达到满带宽传输。

3　仿真结果

SSL VPN 的性能主要从两个方面来分析:设备的数据吞吐量和并发链接的建立能力。文中以虚拟网络模式下的 SSL 为例,根据实际应用环境,在 FPGA 上搭建的测试环境如图 5 所示。

通过测试仪模拟局域网的用户组,半双工时(一边发送另一边接收),测试仪可以自动显示出芯片的处理能力,具体测试数据如表 1 所示。

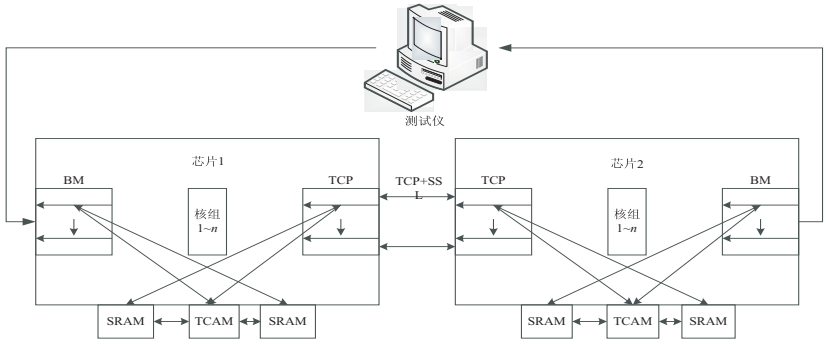

图 5 FPGA 测试环境简图

表 1 FPGA 测试数据

链接数	包长 /Byte	明文发送带宽/Mbps	明文接收带宽/Mbps
256	78	795.84	473.6
256	128	864.64	627.2
256	256	927.36	800
256	512	960	960
256	1 024	980.8	980.8
256	1 500	985.6	985.6
512	78	795.84	448
512	128	864	553.6
512	256	927.36	736
512	512	982.4	915.2
512	1 024	979.2	979.2
512	1 500	986.56	986.56
1 024	78	795.84	457.6
1 024	128	864.64	560
1 024	256	927.36	713.6
1 024	512	982.4	822.4
1 024	1 024	979.2	979.2
1 024	1 500	985.6	985.6

表中所有数据均为测试仪收发纯明文数据的带宽,加上链路层帧间隙(12B)及 SSL 密码报头后,处理速度达到千兆在线。分析可知,高速 SSL 协议芯片的数据吞吐量受链接数的影响相对较小,受本链接数据包大小影响比较大。高速 SSL 协议芯片全片仿真估算出 SSL 最大并发链接数可达 10 000 条;每秒 SSL 链接处理可达 2 000 条。

4 结束语

提出了一种高速 SSL 协议芯片的设计模型,并在 65 nm CMOS 工艺下流片成功,测试结果表明:SSL 安全协议处理芯片在 400 MHz 工作频率下,数据吞吐率能够满足 1 Gb/s 在线网络安全处理的要求。采用该设计模型的 SSL VPN 设备不仅很大程度上提升了网络处理性能,而且有力提高了 SSL VPN 设备的自主可控研发能力,符合信息安全设备自主可控发展要求,具有广阔的推广前景。

参考文献:

[1] DIERKS T, ALLEN C. The TLS protocol version 1.0[S]. [s.l.]:[s.n.],1999.

[2] 尹淑玲. SSL VPN 技术及应用研究[J]. 计算机技术与发展,2013,23(6):129-131.

[3] 单家凌,谢志成,赵崇劲. 基于 SSL 技术的 VPN 网关在无线网络中的应用[J]. 计算机系统应用,2014,23(2):60-64.

[4] 欧阳凯,周敬利,夏 涛,等. 基于 SSL VPN 接入机制的研究[J]. 计算机科学,2005,32(5):59-63.

[5] 石晶林,程 胜,孙江明. 网络处理器原理、设计与应用[M]. 北京:清华大学出版社,2003:1-12.

[6] POSTEL J. Transmission control protocol[S]. [s.l.]:[s.n.],1981.

[7] JAHAN S, RAHMAN M S, SAHA S. Application specific tunneling protocol selection for virtual private networks [C]//2017 international conference on networking, systems and security (NSysS). Dhaka:IEEE,2017:39-44.

[8] 张 仁,徐敬东,尹 乐,等. 基于 Web 浏览器的 SSL VPN 网关系统的设计和实现[J]. 计算机工程与设计,2007,28(4):835-838.

[9] KEN A. SSL VPN gateways:a new approach to secure remote access[J]. Database and Network Journal, 2003, 33(6):3-5.

[10] BHATT D V, SCHULZE S, HANCKE G P. Secure Internet access to gateway using secure socket layer[J]. IEEE Transactions on Instrumentation and Measurement, 2006, 55(3): 793-800.

[11] 夏 涛,周敬利,余胜生,等. 一种面向 SSL VPN 的新型应用层访问控制模型[J]. 计算机科学,2006,33(8):32-36.

[12] 李之棠,何桂丽,王美珍. 基于虚拟网卡的 SSL VPN 体系结构的研究[J]. 计算机应用研究,2007,24(12):327-329.

[13] 马淑文. SSL VPN 技术在校园网中的应用与研究[J]. 计算机工程与设计,2007,28(21):5137-5138.

[14] JASON J, RAFALOW L, VYNCKE E. IPSec configuration policy information model[S]. [s.l.]:[s.n.],2003.

[15] 徐家臻,陈萃萌. 基于 IPsec 与基于 SSL 的 VPN 的比较与分析[J]. 计算机工程与设计,2004,25(4):586-588.