

## 一种安全隧道网关的设计与实现

陈建华<sup>1,2</sup>, 何彬彬<sup>1</sup>, 崔莹<sup>1</sup>

(1 电子科技大学 地表空间信息技术研究所, 四川 成都 610054; 2 成都理工大学 信息工程学院, 四川 成都 610059)

**摘 要:** 针对应用层客户/服务器系统安全性欠缺的情况, 设计、实现了一套基于 SSL/TLS 协议的安全隧道网关, 以提供无缝的安全集成. 客户端隧道网关与服务器端隧道网关之间基于 X. 509 证书进行身份认证, 并建立 SSL/TLS 安全链接转发客户端请求与服务器端响应. 隧道网关与客户端、服务器之间采用普通 TCP/IP 链接进行数据传输. 隧道网关使已有客户/服务器系统无需任何修改即可享有机密性、完整性和可认证的数据传输. 最后给出了网关测试结果与应用实例.

**关键词:** SSL/TLS; 隧道网关; 客户/服务器系统; 安全集成

**中图分类号:** TP393. 08

**文献标识码:** A

**文章编号:** 1000-7180(2011)04-0005-04

## Design and Implementation of a Kind of Secure Tunnel Gateway System

CHEN Jian-hua<sup>1,2</sup>, HE Bin-bin<sup>1</sup>, CUI Ying<sup>1</sup>

(1 Institute of Geo-Spatial Information Science and Technology,

University of Electronic Science and Technology of China, Chengdu 610054, China;

2 College of Information Engineering, Chengdu University of Technology, Chengdu 610059, China)

**Abstract:** Facing with the lack of security in current running client/server systems, this paper designs and implements a kind of secure tunnel gateway system based on SSL/TLS protocol in order to provide seamless security integration to them. Client tunnel gateway and server tunnel gateway authenticate each other based on X. 509 certificate, and create SSL/TLS connections to transmit the clients' requests and servers' responses. The gateway system uses normal TCP/IP connections to transport data with the clients and servers. It provides confidentiality, integrity and authentication for clients/servers data transmission, which needs no modification to them. Then, this paper presents its test result and application instances.

**Key words:** SSL/TLS; tunnel gateway; client/server system; security integration

### 1 引言

SSL/TLS<sup>[1-2]</sup> (Secure Socket Layer/Transport Layer Security, 即安全套接字层/传输层安全协议) 是工作于网络传输层与应用层之间的一种安全协议. 它基于对称密码算法、非对称密码算法、散列算法提供了传输层之上端到端数据传输的机密性、完整性和认证性. SSL/TLS 是独立于传输层的协议, 它采用基于公钥算法的 X. 509 数字证书在 TCP 链接建立之后, 安全链接建立之前协商双方数据传输

时采用的对称加密密钥、完整性校验散列算法等安全要素, 同时基于证书进行服务器端身份认证和可选的客户端身份认证; 之后安全链接建立, 客户端与服务器即可进行安全数据传输. SSL/TLS 设计用于 WEB 客户端与 WEB 服务器之间进行 HTTPS 安全数据传输, 并已成为互联网安全标准和 WEB 领域事实上的工业标准.

TP 隧道网关设计用于为: HTTP、FTP、TELNET 和普通 Socket 通信提供透明的安全数据传输. 上述通信皆为端到端, 为提供便捷、灵活、高效、

一致的安全性,并对比 IPSec 协议点到点所有数据加解密、校验的低效性和非灵活性,TP 隧道网关基于 SSL/TLS 协议进行了设计、实现,既保证了已有客户/服务器业务系统数据安全传输的透明切入,同时也灵活保留了客户/服务器计算机上其他数据的普通传输。TP 隧道网关不仅扩展了 SSL/TLS 的应用领域,而且为现有应用层客户/服务器系统安全性的透明集成提供了新的思路。

## 2 SSL/TLS 隧道网关整体结构

基于 SSL/TLS 的 TP 隧道网关是一套应用层安全解决方案,由部署于业务客户端的隧道网关和部署于业务服务器端的隧道网关构成<sup>[3]</sup>。整体结构见图 1。业务客户端隧道网关设计运行于 Windows 平台下,并与各业务客户端部署于同一台 PC 机上。因为各客户端通常是分散部署的,将网关与它们部署在一起,既方便客户端操作人员的操作,又方便对其身份进行认证,同时基本不影响各自的性能。各客户端与隧道网关在本机上采用 TCP/IP 进行普通数据传输,客户端隧道网关与远程服务器端隧道网关采用 SSL/TLS 进行安全数据传输。业务服务器端隧道网关设计运行于 Linux 平台下,通常与各业务服务器部署于同一局域网中不同的服务器计算机上,以保证业务服务器和隧道网关都能发挥最大性能,同时也可最小化对它们的认证和维护(同一局域网中的服务器,仅需在隧道网关处统一认证即可,每一局域网中的服务器都将分别设置服务器端隧道网关)。业务服务器与隧道网关之间采用 TCP/IP 进行普通数据传输。

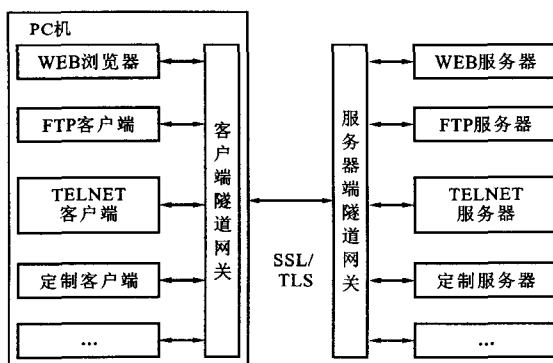


图 1 TP 隧道网关整体结构

隧道网关操作流程如下:

(1) 由 TP CA 认证中心颁发客户端和服务器端隧道网关 X.509 数字证书和 RSA 公私钥对,并写入 USB IC 卡中(私钥不出卡,并采用使用者口令

加密;证书及公私钥对也可由其他认证中心颁发)。

(2) 服务器端隧道网关设置自己的 IP 地址及监听端口。插入 USB IC 卡并输入密钥保护口令,接下进入监听状态。

(3) 客户端隧道网关设置业务客户端建连 IP 地址及监听端口、远程业务服务器 IP 地址及端口、WEB 服务器安全传输信任列表(IP 地址/域名及端口)、远程服务器端隧道网关 IP 地址及端口等信息。插入 USB IC 卡并输入密钥保护口令,接下等待进入链接状态。

(4) 业务客户端设置服务器端 IP 地址和端口为客户端隧道网关指定值(IP 通常为环回地址)。

(5) 业务客户端连接远程服务器。数据到达客户端隧道网关,该网关与远程服务器端隧道网关建立 SSL/TLS 安全链接;之后数据加密并到达服务器端隧道网关,解密后发送给对应业务服务器。之后客户、服务器间数据在隧道网关间加解密传输。

## 3 业务客户端隧道网关设计与实现

### 3.1 体系结构设计

业务客户端隧道网关体系结构见图 2。配置模块设置业务客户端建连 IP 地址及监听端口、远程业务服务器 IP 地址及端口、WEB 服务器安全传输信任列表(IP 地址/域名及端口)、远程服务器端隧道网关 IP 地址及端口等信息。上述设置中,同一类型业务服务器可以设置多个;服务器端隧道网关也可设置多个,只是针对不同网关,上述信息将分组设置(以实现网关间多对多的链接)。设置完毕触发业务监听模块做监听设置更新。业务监听模块初始化各业务监听端口,进入循环监听状态。当检测到客户端建连请求后,根据监听端口触发相应业务数据安全转发模块,随后检测监听端口更新设置,复又进入监听状态。针对 WEB 浏览器建连请求,如果目标 WEB 服务器处于安全传输信任列表中,则触发 HTTP 数据安全转发模块,否则触发 HTTP 数据普通转发模块。HTTP 数据普通转发模块直接将来自 WEB 客户端的请求数据转发至目标 WEB 服务器,同时将 WEB 服务器响应数据转发给浏览器。HTTP 数据安全转发模块与服务器端隧道网关建立 SSL/TLS 链接后,将请求加密发送给它,由其解密后发送给目标 WEB 服务器。同时将来自服务器端隧道网关转发的 WEB 服务器响应解密后直接发送给 WEB 浏览器。FTP、TELNET、定制客户端数据安全转发模块等工作模式与 HTTP 数据安全转

发模块类似。SSL/TLS 模块分别为各数据安全转发模块提供 SSL/TLS 安全通信接口,包括 X.509 证书认证接口。

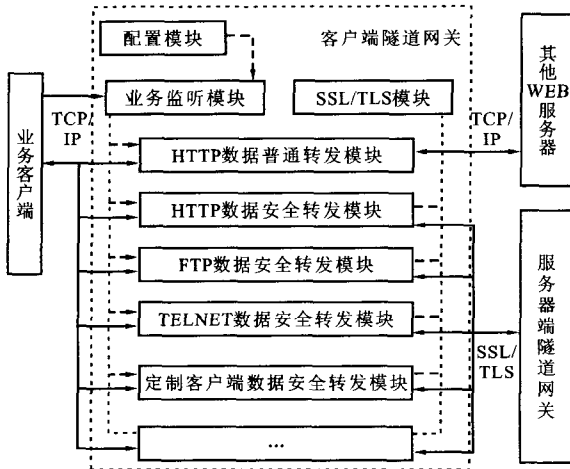


图2 业务客户端隧道网关体系结构

### 3.2 关键技术实现

客户端隧道网关采用线程池以多线程方式实现,以提升性能。业务监听线程负责接收客户端建连请求,并提取线程池中数据转发线程以执行数据转发功能。为保证并发性与及时响应,每一链接对应一个线程。各数据安全转发线程运行时,首先通过 SSL/TLS 模块提供的通信接口建立到服务器端隧道网关的安全链接,随后发送 T-L-V 格式的自定义控制报文通知服务器端隧道网关新建链接对应的远程业务服务器 IP 地址(WEB 服务器可为域名)和监听端口(皆在配置模块中设置),以便服务器端隧道网关建立到业务服务器的 TCP/IP 链接。之后接收业务客户端请求并加密转发给服务器端隧道网关,同时解密服务器端隧道网关加密并转发的业务服务器响应,并发送给客户端;数据转发循环进行,直到链接终止。在 HTTP、FTP 各数据安全转发线程中,都需要对请求、响应消息做适当的解析、修改和补充,方能进行正常通信,这是由协议决定的,并可应用于各 WEB、FTP 客户—服务器间。而 TELNET、定制客户端转发线程透明转发请求、响应,无需对传输消息做处理。对于 HTTP 数据普通转发线程也必须解析、修改、补充 HTTP 报文方能实现 WEB 客户端与服务器之间的正确通信。SSL/TLS 通信接口基于 OpenSSL<sup>[4-5]</sup> 开源项目封装,以动态链接库形式提供。对服务器端隧道网关证书的认证在首次与其建连时完成,此后各转发线程仅需调用接口进行 SSL/TLS 建连和通信。OpenSSL 接口函数有: SSLInitiate、SSLConnect、SSLAccept、

SSLCertificateVerify、SSLRead、SSLWrite、SSLClose 等。

## 4 业务服务器端隧道网关设计与实现

### 4.1 体系结构设计

业务服务器端隧道网关体系结构与客户端隧道网关有一定的相似性,见图3。配置模块主要设置自身 IP 地址及监听端口等信息,为业务监听模块服务。业务监听模块初始化之后进入循环监听状态。如果检测到客户端隧道网关 SSL/TLS 建连请求,依据客户端隧道网关发送的控制报文,触发对应业务数据安全转发模块,自身重又进入监听状态。HTTP 数据安全转发模块建立与指定 WEB 服务器的 TCP/IP 链接,随后读取客户端隧道网关通过 SSL/TLS 链接发送的请求数据,将其解密发送给目标 WEB 服务器。同时将来自 WEB 服务器的响应数据加密后转发给客户端隧道网关。FTP、TELNET、定制服务器数据安全转发模块等工作模式与 HTTP 数据安全转发模块类似。SSL/TLS 模块分别为各数据安全转发模块提供 SSL/TLS 安全通信接口<sup>[6]</sup>,包括 X.509 证书认证接口。

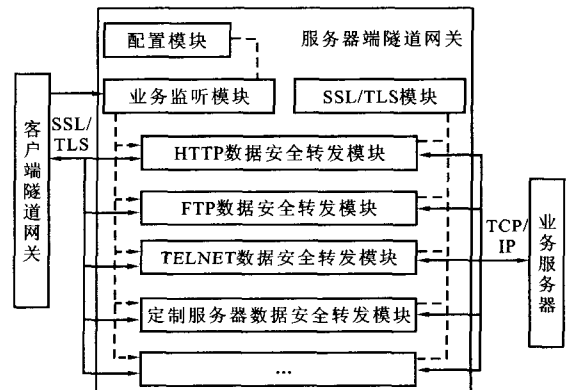


图3 业务服务器端隧道网关体系结构

### 4.2 关键技术实现

为提升性能,服务器端隧道网关在 Linux 平台下同样采用线程池以多线程方式实现。业务监听线程负责接收客户端隧道网关 SSL/TLS 建连请求,建连后读取客户端隧道网关发送的 T-L-V 格式的自定义控制报文以确定业务类型及目标服务器 IP 地址与端口,并提取线程池中数据转发线程以执行数据转发功能。考虑并发性与响应性,每一链接对应一个线程。各数据安全转发线程运行时,首先建立与指定业务服务器的 TCP/IP 链接,之后通过 SSL/TLS 模块提供的通信接口函数接收客户端隧道网关请求数据,将其解密并转发给目标服务器,同时加

密目标服务器发来的响应数据并转发至客户端隧道网关;数据转发循环进行,直至链接终止.与客户端隧道网关不同,在 HTTP、FTP、TELNET、定制服务器各数据安全转发线程中无需对请求、响应消息做任何解析、修改和补充,直接透明转发即可.之所以将 HTTP、FTP 客户——服务器间请求、响应消息的修改、补充等工作放在客户端隧道网关,原因在于:服务器端隧道网关链接处理负载要远远大于客户端隧道网关,此举意在减轻服务器端隧道网关负担. SSL/TLS 通信接口基于 OpenSSL 开源项目封装,以动态链接库形式载入.客户端隧道网关的证书认证工作在首次建连时完成,之后其他新建安全链接无需认证证书,而数据转发线程只需直接调用 SSL/TLS 通信接口收、发数据.

## 5 测试与应用

TP 隧道网关经编码实现,并进行了严格的  $\alpha$ 、 $\beta$  测试.测试表明:在 100M 以太网环境下,业务客户端与业务服务器间部署隧道网关后,数据传输速率为无隧道网关时的 35%~40%,这主要是 SSL/TLS 协议加解密、完整性校验耗时造成的;而隧道网关两次对数据的明文转发对速率的影响仅为 4%~6%(与直接传输对比).服务器端隧道网关在处理器—Intel Pentium4 1.6 GHz、内存—512 MB、操作系统—RedHat Linux9.0 环境下,最大 SSL/TLS 链接数可达 1 000.如果硬件配置提高,链接数随之提高;不过链接数越趋近极值,各业务客户端数据传输速率越低.广域网环境未经测试,但由于广域网延时高,客户、服务器间经隧道网关的数据传输速率与直接传输速率的比值理应比以太网环境高.

TP 隧道网关目前已运行于国内某电信公司部

分分公司和一数据通信公司中.前者为 HTTP、FTP 及数据库访问定制系统等业务提供安全通信;后者为各分公司与总部以 WEB 形式下载、上传计划书、财务报表等提供安全通信.初步运营反馈表明:隧道网关运行良好、稳定.

## 6 结束语

基于 SSL/TLS 的隧道网关为应用层客户/服务器系统安全性的无缝集成提供了一种崭新的思路,并具有方便、灵活、透明的特点,具有良好的应用前景.

## 参考文献:

- [1] Freier Alan O, Philip Karlton, Kocher Paul C. The SSL protocol version 3.0[EB/OL]. [2010-06-30]. <http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt>.
- [2] Dierks T, Certicom, Allen C, et al. The TLS protocol version 1.0[EB/OL]. [2010-06-30]. <http://www.ietf.org/rfc/rfc2246.txt>.
- [3] 安庆,陶宏才. C/S 模式下文件迁移服务器结构的设计[J]. 微电子学与计算机, 2009, 26(4): 129-132.
- [4] OpenSSL[EB/OL]. [2010-06-30]. <http://www.openssl.org>.
- [5] Viega J, Messier M, Chandra P. Network security with OpenSSL[M]. Sebastopd, California: O'Reilly Media, 2002.
- [6] 陈英杰,王海欣,白国强,等. 一种能够实现多种散列函数的 VLSI—IP 模块设计[J]. 微电子学与计算机, 2010, 27(4): 89-94.

## 作者简介:

陈建华 男,(1976—),博士.研究方向为空间数据提取与分析、计算机应用技术.

(上接第 4 页)

- [6] 张继军,吴哲辉. 上下文无关 Petri 网语言的 Pumping 引理[J]. 小型微型计算机系统, 2008, 29(4): 698-702.
- [7] 张继军,费玉奎,耿霞. 有界 Petri 网等价性的判定算法[J]. 微电子学与计算机, 2008, 25(12): 5-8.
- [8] 张继军,吴哲辉,董卫. Petri 网的状态转换图[J]. 小型微型计算机系统, 2008, 29(9): 1714-1718.
- [9] 蒋昌俊. 矢量文法与 PN 机[J]. 中国科学 A 辑, 1995, 25(12): 1315-1322.
- [10] 张继军,费玉奎,董卫. 二元文法[J]. 计算机工程与科

学, 2008, 30(11): 95-98.

## 作者简介:

张继军 男,(1965—),教授,CCF 高级会员.研究方向为自动机理论及应用、Petri 网理论及应用.

董卫 男,(1979—),讲师.研究方向为 Petri 网理论及应用.

范昊 男,(1977—),博士.研究方向为 Petri 网理论及应用.