第 35 卷 第 4 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.4 Computer Engineering February 2009
·安全技术· 文章编号：1000—3428(2009)04—0154—03 文献标识码：A 中图分类号：TP393.08

基于防火墙钩子的 IPSec VPN 研究与实现

张 明，陈性元，杜学绘，钱雁斌
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：针对采用网络驱动接口规范(NDIS)实现 IPSec VPN 系统过程中存在的问题，提出一种基于防火墙钩子的 IPSec VPN 系统，研究了 Windows 网络层防火墙钩子数据包过滤技术，将 IPSec 封包处理提升到网络层中加以实现。该系统能有效解决由 NDIS 实现方式引起的 MTU 处理、路由和数据包分片、重组等问题，提高了系统处理效率，且具有较好的应用特性。

关键词：IPSec VPN 系统；防火墙钩子；网络驱动接口规范

Research and Implementation of IPSec VPN Based on Firewall Hook

ZHANG Ming, CHEN Xing-yuan, DU Xue-hui, QIAN Yan-bin
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Aiming at the problems existed in the process of using Network Driver Interface Specification(NDIS) to implement IPSec VPN system, a new IPSec VPN system based on firewall hook is presented, and the data packet filtering technology for firewall hook at Windows network layer is researched, which upgrades the IPSec encapsulation processing to network layer and implements it. This system can effectively solve the problems caused by NDIS such as MTU, routing and reassembly. It promotes the processing efficiency and has better performance of application.

【Key words】 IPSec VPN system; firewall hook; Network Driven Interface Specification(NDIS)

1 概述

飞速发展的 Internet 为人们提供了经济、便利、快速、可靠和灵活的 WAN 通信，但由于最初设计的缺陷，Internet 仍不能提供与专用网相匹配的安全性。VPN 技术就是在这一背景下产生并发展起来的，利用隧道技术，综合多种安全机制，将属于同一安全域的网络节点构建成安全、独占、自治的虚拟网络。它既能运行在 Internet 或公共 IP 网络上，又能提供足够的安全性。IPSec 协议是由因特网工程任务组(IETF)提出的 IP 安全标准，是 VPN 系统实现的主要技术之一。近年来 IPSec VPN 技术以其独具特色的优势赢得人们越来越多的青睐，并成为网络安全领域的热点。

作为最普及的操作系统，Windows 本身也支持 IPSec VPN 的构建，但出于对其代码不公开和安全性等因素考虑，目前，IPSec VPN 普遍是在 Windows2000/XP 环境下的网络驱动接口规范层(NDIS)中实现的[1-2]。这种采用 BITS 技术实现的 VPN 系统将 IPSec 实现于数据链路层，并存于 IP 协议和网卡驱动器之间。因此，它需要大量重复的网络层工作，如 MTU 处理、路由和分片、重组等，在增加开发难度的同时，系统性能也受到影响。同时，随着 VPN 系统的大规模应用，VPN 之间、VPN 与防火墙等基于 NDIS 技术的安全软件之间经常产生冲突。针对上述问题，有些文献也提出了不同的优化方法[2-3]，但这些 VPN 功能与运行效率的“折中”解决方案不能从根本上解决上述问题。

本文在研究 Windows 系统内核模式下防火墙钩子数据包过滤技术的基础上，将 IPSec 处理提升到网络层中加以实现，并与 Windows 下 TCP/IP 协议栈紧密结合，从根本上解决了因 NDIS 实现方式所引起的问题。

2 防火墙钩子数据包过滤技术

安全可靠地拦截网络数据包，然后对其加以控制和处理是实现 VPN 和防火墙等网络安全产品的基础。NDIS, TDI 等内核数据包过滤技术已被广泛应用于安全产品的开发。不少文献对这些公开的数据包过滤技术也进行了深入研究[4]，这里不再累述。结合 IPSec 协议主要针对 IP 数据进行处理的特点，本文着重研究 Windows 网络层防火墙钩子过滤接口以及基于该接口的数据包过滤技术。防火墙钩子过滤接口是 Windows 未文档化的数据包过滤接口之一。因此，本文提及的部分内容和结论是对通用的 Windows 2000/XP/2003 系统中防火墙钩子接口实验和测试结果的总结。

2.1 防火墙钩子概述

从 Windows 2000 开始，微软增加了对防火墙钩子接口的支持。防火墙钩子接口被设计用来管理流经 TCP/IP 协议栈内的数据包，阻止来自互联网的非授权用户访问本机。在 Windows XP 中，微软添加了一个全状态过滤功能的内置防火墙，它的内核驱动 IPNat.sys 就是个防火墙钩子过滤驱动程序，同时这个防火墙也具有处理网络地址转换的功能。防火墙钩子数据包过滤技术具备持续、稳定的阻拦、截取、修改网络数据包的功能。

防火墙钩子接口在 TCP/IP 协议栈中的位置如图 1 所示。防火墙过滤接口在路由、分片和组包模块之上。网络数据包流出/流入该接口时，相应的分片/组包操作由系统 TCP/IP 协议栈完成。因此，在该接口对数据包进行处理时不用考虑 MTU 处理、路由和数据包的分片、重组等由 NDIS 实现方式所产生的问题。

基金项目：公安部“金盾工程”基金资助项目(JIGAB23WD13)
作者简介：张 明(1982－)，男，硕士研究生，主研方向：网络安全；陈性元，教授、博士生导师；杜学绘，副教授；钱雁斌，博士研究生
收稿日期：2008-07-20 **E-mail：**zxyming@126.com

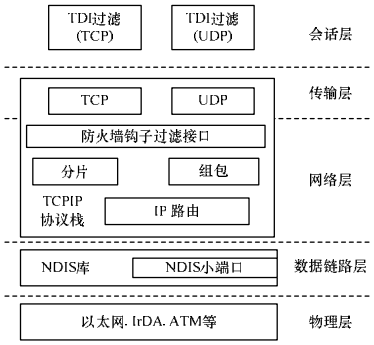


图 1　内核模式 Windows 网络体系结构

2.2　防火墙钩子数据缓冲区管理

防火墙钩子数据缓冲区管理采用缓冲区大小可调的链表方式，由 3 级结构组成，如图 2 所示。

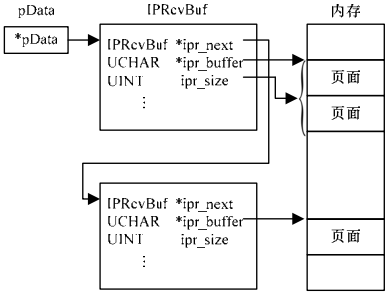


图 2　防火墙钩子缓冲区结构

在图 2 中，防火墙钩子回调函数之间传递的参数*pData 表示一个完整的数据包，指向第 1 个 IPRcvBuf 类型结构。发送和接收的数据包由一个或多个 IPRcvBuf 结构链接而成。在 IPRcvBuf 结构中，参数 ipr_buffer 指向缓冲区在内存中存储位置，参数 ipr_size 表示缓冲区的大小。参数 ipr_next 指向同一数据包的下一个 IPRcvBuf 结构。防火墙钩子接口支持对 IPRcvBuf 结构和其缓冲区的创建、释放和修改。

对于所有本机发出的 IP 数据包，都由 3 个 IPRcvBuf 结构组成，其中，每个结构的缓冲区包含一个协议信息。例如，对于一个发送的 UDP/TCP 包，会产生一个有 IPRcvBuf 结构的链表：第 1 个结构的缓冲区是 IP 协议头，下一个是 UDP/TCP 协议头，剩下的是 UDP/TCP 载荷。

对于所有本机收到的 IP 数据包，根据数据包长度不同，IPRcvBuf 结构的个数也有所不同。通常情况下，当 IP 数据包的总长度不超过 1 500 Byte 时，收包只有一个 IPRcvBuf 结构，所有的数据都在这个结构的缓冲区中。当 IP 数据包的总长度超过 1 500 Byte 时，收包将有至少 3 个结构：第 1 个结构的缓冲区长为 20 Byte，由 IP 协议头内容填充；从第 2 个结构开始，每 1 480 Byte 的 IP 载荷填充一个结构缓冲区；最后一个结构的缓冲区由剩余部分的 IP 载荷填充。

另外，通过对缓冲区中数据包 IP 协议头字段的分析发现：在发包中，IP 头校验和总为 0；在收包中，对 IP 头中校验和部分做修改不影响数据包的接收。因此，在应用该接口修改截获数据包时，如加解密和 NAT，可以不进行 IP 头校验和计算工作，在一定程度上提高了处理速度。

3　基于防火墙钩子的 IPSec VPN 设计与实现

3.1　总体设计

结合对防火墙钩子过滤技术的研究和 WDM 开发技术的掌握，本文设计并实现了 Windows2000/XP 下的 VPN 系统。如图 3 所示，系统大体上可分为 2 个部分：系统用户模式部分和系统内核模式部分。

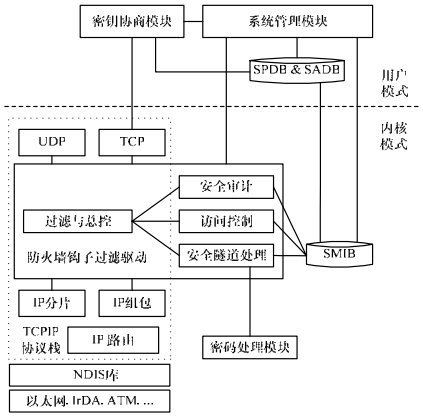


图 3　基于防火墙钩子的 VPN 系统组成结构

系统用户模式部分包括 VPN 系统管理模块、密钥交换模块、安全策略数据库(SPDB)和安全关联数据库(SADB)。密钥交换模块基于 Socket 通信实现 IPSec 协议族的 IKE 协议，完成 SA 的自动建立、协商、修改。系统管理模块实现对 SPDB 和 SADB 的管理，包括对安全策略(SP)和安全关联(SA)的增加、删除、查询等；保证密钥在生成、保存、交换以及使用时的安全；通过系统管理模块与内核模式的接口，将有效的 SP, SA 信息及系统控制信息传递给 VPN 系统内核模式部分。

系统内核模式部分主要是防火墙钩子驱动模块，对主机接收和发出的数据包执行访问控制、安全审计等功能。安全管理信息数据库(SMIB)包含系统用户模式部分传递的 SP, SA 等信息和审计信息。过滤与总控模块截获所有流经 TCP/IP 协议栈的 IP 数据包，同时调度和总控系统内核部分其他功能模块。安全审计模块按照审计策略，审计进出系统的数据包及其处理情况。访问控制模块具有基于安全策略 SP 的访问控制功能，可以根据安全策略决定数据包的处理方式。安全隧道处理模块根据访问控制策略结果，调用密码处理模块中相应加密函数，完成对数据包的动/静态隧道封装。

3.2　数据包的截取

在 DriverEntry 进程中，先初始化防火墙钩子的驱动列表。列表中包含将挂接在 IP 协议驱动上的防火墙钩子驱动。一个防火墙钩子驱动定义一个指针，指向一个 IPPacket FirewallPtr 类型的回调函数。每个流经 IP 驱动的数据包都要流经挂接在 IP 协议驱动上的防火墙钩子驱动。

注册防火墙钩子驱动时，先将回调函数填入 IP_SET_FIREWALL_HOOK_INFO 结构中。该结构由 3 个参数组成，另外 2 个参数分别用于设置该回调函数的优先级和驱动执行中该回调函数是否有效。系统按优先级调用有效的回调函数，这就避免了防火墙钩子驱动间的冲突，然后驱动创建一个输入输出请求包 IRP，它包含已建立的 IP_SET_FIREWALL_HOOK_INFO 和 IOCTLIOCTL_IP_SET_FIREWALL_ HOOK，最后将该 IRP 传给 IP 协议驱动的设备对象，完成注册。

将过滤与总控模块设计成一个 IPPacketFirewallPtr 类型的防火墙钩子回调函数。该模块截取网络数据包后传递访问控制模块，后者根据包含的策略信息决定如何处理数据包：(1)若策略拒绝该包发送，则回调函数返回“ DROP PACKET ”值，IP 驱动将该包丢弃；(2)若策略允许该包直接发送，则回调函数返回“ ALLOW PACKET ”值，该包通过防火墙钩子驱动，返回给 IP 驱动；(3)若策略要求对该包执行 VPN 处理，则调用安全隧道处理模块对该包进行封装。在封装完成后，

回调函数返回“ ALLOW PACKET ”值，该包返回给 IP 驱动。

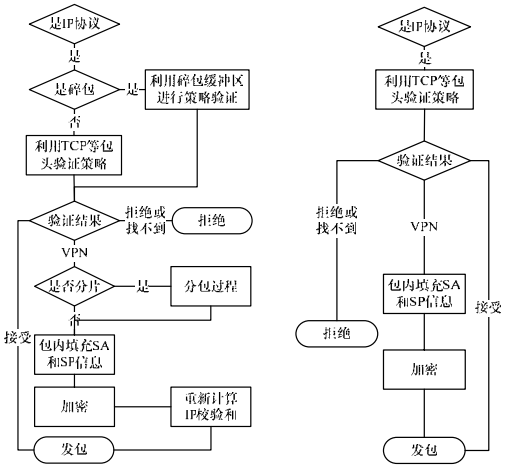
3.3 数据包的加解密

防火墙钩子回调函数运行在 IRQL＝DISPATCH_LEVEL 级别上，然而硬件加解密驱动函数通常运行在 IRQL＝PASSIVE_LEVEL 级别上。由于 DISPATCH_LEVEL 级别高于 PASSIVE_LEVEL，若回调函数直接调用硬件加密驱动会导致 Windows 蓝屏死机，因此解决在高 IRQL 级别上对低级别函数的调用是实现加解密模块调用的关键。

本系统采用工作队列 WorkItem 方式解决该问题，利用 WorkItem 排队加解密调用函数。当 DriverEntry 进程处于 DISPATCH_LEVEL 级别时，系统将加解密函数塞入 WorkItem 队列中，当进程降低到 PASSIVE_LEVEL 时，队列中的函数会被系统调用。防火墙钩子过滤回调函数与加解密函数间数据的交互是通过共享数据缓冲区间接完成的。

3.4 数据包的隧道处理流程

IPSec 隧道处理模块作用于防火墙钩子接口截取的数据包，用到许多 Windows 系统自身 IP 协议栈功能，如数据包分片重组、PMTU、路由转发、数据包校验等，如图 4 所示。



(a)采用 NDIS 的发包流程　(b)采用防火墙钩子的发包流程

图 4　2 种实现方式发包流程对比

从图 4 可以看出，与基于 NDIS 开发的 VPN 系统相比，该系统减少了诸多处理环节，从根本上提高了 IPSec 的处理效率。

3.5 功能特点

综上所述，基于防火墙钩子的实现方式主要有以下特点：

(1)处理性能

该方式直接对 IP 数据包进行处理，回避了 NDIS 方式存在的 MTU 处理、路由和数据包分片、重组等问题，提高了处理效率和网络适应性。

(2)开发和应用

NDIS 方式编程实现复杂且容易出错，在应用中经常与基于 NDIS 技术的安全软件发生冲突。本文方式基于优先级调用各个防火墙钩子驱动，避免了冲突的发生。

(3)安全性

2 种实现方式均位于 Windows 内核层，能截取所有流经系统 TCP/IP 协议栈的数据包，具有较高的安全性。

4 结束语

本文通过分析 TCP/IP 栈中的防火墙钩子数据包过滤技术，并基于这种技术在 Windows2000/XP 系统中实现了 IPSec VPN 系统。从开发和执行过程分析来看，新方式的作用较明显。考虑到更高的安全性，可采用增加 NDIS 安全辅助模块或与专业防火墙配合的方式提高 VPN 系统的安全性，这是下一步研究工作的重点。

参考文献

[1] 徐大为, 龚　玲, 杨宇航. NDIS 中间层驱动程序设计和虚拟专用网客户端的实现[J]. 计算机工程, 2002, 28(2): 174-176.

[2] 于　佳, 孔凡玉, 李大兴. VPN 在 Windows 2000 上的实现与性能优化方法[J]. 计算机应用, 2004, 24(5): 45-46, 49.

[3] 肖　凌, 李之棠, 梅　松. 一种基于虚拟网卡的 Windows VPN 体系结构研究[J]. 小型微型计算机系统, 2007, 28(9): 1586-1590.

[4] 朱雁辉. Windows 防火墙与网络封包截获技术[M]. 北京: 电子工业出版社, 2002.

(上接第 151 页)

[4] Liang Xiaohui, Cao Zhenfu, Lu Rongxing, et al. Efficient and Secure Protocol in Fair Document Exchange[J]. Computer Standards & Interfaces, 2008, 30(3): 167-176.

[5] Stadler M. Publicly Verifiable Secret Sharing[C]//Proc. of EUROCRYPT’96. Zaragoza, Spain: [s. n.], 1996: 190-199.

[6] Koblitz N, Menezes A, Vanstone S A. The State of Elliptic Curve Cryptography[J]. Design Codes Cryptography, 2000, 19(2): 173-193.

[7] Scott M. Computing the Tate Pairing[C]//Proc. of CT-RSA’05. San Francisco, USA: [s. n.], 2005: 293-304.

(上接第 153 页)

[3] Li Jiguo, Cao Zhenfu, Zhang Yichen. Nonrepudiable Proxy Multi-Signature Scheme[J]. Journal of Computer Science and Technology, 2003, 18(3): 399-402.

[4] Hwang Shin-Jia, Chen Chiu-Chin. Cryptanalysis of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers[J]. International Journal of Informatics, 2003, 14(2): 205-212.

[5] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]//Proc. of CRYPTO’84. Berlin, Germany: Springer-Verlag, 1984.

[6] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]//Proc. of CRYPTO’01. Berlin, Germany: Springer-Verlag, 2001.

[7] Chen Liqun, Lee M J. Improved Identity-based Signcryption[C]//Proc. of PKC’05. Berlin, Germany: Springer-Verlag, 2005: 362-379.

[8] Waters B. Efficient Identity-based Encryption Without Random Oracles[C]//Proceedings of EUROCRYPT’05. Berlin, Germany: Springer-Verlag, 2005: 114-127.

[9] Boyen X, Waters B. Compact Group Signatures Without Random Oracles[C]//Proceedings of EUROCRYPT’06. Berlin, Germany: Springer-Verlag, 2006: 427-445.

[10] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10): 1743-1756.