# 防火墙包过滤技术发展研究*

翟 钰[1,3]，武舒凡[2]，胡建武[1]

(1. 西安建筑科技大学 信息与控制工程学院，陕西 西安 710071；2. 西安交通大学 电子与信息工程学院，陕西 西安 710071；3. 中国科学院 研究生院 国家计算机网络入侵防范中心，北京 100039)

**摘 要**：防火墙技术主要分为包过滤和应用代理两类。从数据包结构出发，分析包过滤技术，首先提出包过滤技术的核心问题；然后在分析传统包过滤技术缺陷的基础上，详细论述了包过滤技术的两种发展趋势；最后以技术实例说明了这两种趋势的融合。

**关键词**：防火墙；包过滤；动态包过滤；深度包检测

**中图法分类号**：TP393.08 **文献标识码**：A **文章编号**：1001-3695(2004)09-0144-03

# Research on Technology Development of Packet Filtering in Firewall

ZHAI Yu[1,3], WU Shu-fan[2], HU Jian-wu[1]

(1. *School of Information & Control Engineering, Xi'an University of Architecture & Technology, Xi'an Shanxi* 710071, *China*; 2. *School of Electronic & Information Engineering, Xi'an Jiaotong University, Xi'an Shanxi* 710071, *China*; 3. *National Computer Network Intrusion Protection Center, Graduate School, Chinese Academy of Science, Beijing* 100039, *China*)

**Abstract:** Firewall can be classified as packet filter and application agent. In this paper, the packet filter method was analyzed from the structure of data package. First the key problem of packet filter is proposed, then the two possible tendency of the packet filter method are thoroughly investigated. Finally, several cases are used to illustrate the combination of the two tendency.

**Key words:** Firewall; Packet Filter; Dynamic Packet Filter; Deep Packet Inspection

## 1 引言

随着 Internet 的迅速发展，网络应用涉及到越来越多的领域，网络中各类重要的、敏感的数据逐渐增多；同时由于黑客入侵以及网络病毒的问题，使得网络安全问题越来越突出。因此，保护网络资源不被非授权访问，阻止病毒的传播感染显得尤为重要。就目前而言，对于局部网络的保护，防火墙仍然不失为一种有效的手段。防火墙技术主要分为包过滤和应用代理两类。其中包过滤作为最早发展起来的一种技术，其应用非常广泛。

所谓包过滤，就是对流经网络防火墙的所有数据包逐个检查，并依据所制定的安全策略来决定数据包是通过还是不通过。包过滤最主要的优点在于其速度与透明性。也正是由于此，包过滤技术历经发展演变而未被淘汰。

由于其主要是对数据包的过滤操作，所以数据包结构是包过滤技术的基础。考虑包过滤技术的发展过程，可以认为包过滤的核心问题就是如何充分利用数据包中各个字段的信息，并结合安全策略来完成防火墙的功能。

本文从数据包结构的角度出发，分析包过滤技术，详细论述了包过滤技术的两种发展趋势。

收稿日期：2003-09-23；修返日期：2003-11-04

基金项目：国家“863”计划资助项目(2002AA142151)；中国科学院知识创新工程方向性项目(KGCX2-106)；北京市科技计划项目(H020120090530)

## 2 数据包结构

当应用程序用 TCP 传送数据时，数据被送入协议栈中，然后逐个通过每一层直到被当作一串比特流送入网络。其中每一层对接收到的数据都要增加一些首部信息。TCP 传给 IP 的数据单元称作 TCP 报文段(TCP Segment)；IP 传给网络接口层的数据单元称作 IP 数据报(IP Datagram)；通过以太网传输的比特流称作帧(Frame)。对于进入防火墙的数据包，顺序正好与此相反，头部信息逐层剥掉。IP，TCP 首部格式如图 1、图 2 所示。


图 1 IP 首部格式

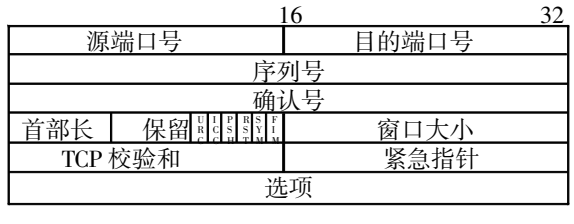


图 2 TCP 首部格式

对于帧的头部信息主要是源/目的主机的 MAC 地址；IP 数据报头部信息主要是源/目的主机的 IP 地址；TCP 头部的主要字段包括源/目的端口、发送及确认序号、状态标识等。

理论上讲, 数据包所有头部信息以及有效载荷都可以作为判断包通过与否的依据, 但是在实际情况中, 包过滤技术上的问题主要是选取哪些字段信息, 以及如何有效地利用这些字段信息并结合访问控制列表来执行包过滤操作, 并尽可能提高安全控制力度。

## 3　传统包过滤技术缺点

传统包过滤技术, 大多是在 IP 层实现, 它只是简单的对当前正在通过的单一数据包进行检测, 查看源/目的 IP 地址、端口号以及协议类型( UDP/TCP) 等, 结合访问控制规则对数据包实施有选择的通过。这种技术实现简单, 处理速度快, 对应用透明, 但是它存在的问题也很多, 主要表现有:

( 1) 所有可能会用到的端口都必须静态放开。若允许建立 HTTP 连接, 就需要开放 1024 以上所有端口, 这无疑增加了被攻击的可能性。

( 2) 不能对数据传输状态进行判断。如接收到一个 ACK 数据包, 就认为这是一个已建立的连接, 这就导致许多安全隐患, 一些恶意扫描和拒绝服务攻击就是利用了这个缺陷。

( 3) 无法过滤审核数据包上层的内容。即使通过防火墙的数据包有攻击性或包含病毒代码, 也无法进行控制和阻断。

综合上述问题, 传统包过滤技术的缺陷在于: ①缺乏状态检测能力; ②缺乏应用防御能力。而问题的根本原因在于: ①只对当前正在通过的单一数据包进行检测, 而没有考虑前后数据包之间的联系; ②只检查包头信息, 而没有深入检测数据包的有效载荷。

## 4　包过滤技术发展

传统包过滤技术必须发展进化, 在继承其优点的前提下, 采用新的技术手段, 克服其缺陷, 并进一步满足新的安全应用要求。从数据包结构出发考虑, 目前包过滤技术向两个方向发展: ①横向联系。即在包检测中考虑前后数据包之间的关系, 充分利用包头信息中能体现此关系的字段, 如 IP 首部的标识字段和片偏移字段、TCP 首部的发送及确认序号、滑动窗口的大小、状态标识等, 动态执行数据包过滤。②纵向发展。深入检测数据包有效载荷, 识别并阻止病毒代码和基于高层协议的攻击, 以此来提高应用防御能力。这两种技术的发展并不是独立的, 动态包过滤可以说是基于内容检测技术的基础。实际上, 在深度包检测技术中已经体现了两种技术的融合趋势。

### 4.1　动态包过滤

动态包过滤( Dynamic Packet Filter) 又称为基于状态的数据包过滤( Stateful Packet Filter) , 是在传统包过滤技术基础之上发展起来的一项过滤技术, 最早由 Checkpoint 提出。

与传统包过滤技术只检查单个、孤立的数据包不同, 动态包过滤试图将数据包的上下文联系起来, 建立一种基于状态的包过滤机制。对于新建的应用连接, 防火墙检查预先设置的安全规则, 允许符合规则的连接通过, 并在内存中记录下该连接的相关信息, 这些相关信息构成一个状态表。这样, 当一个新的数据包到达, 如果属于已经建立的连接, 则检查状态表, 参考数据流上下文决定当前数据包通过与否; 如果是新建连接, 则检查静态规则表。

动态包过滤通过在内存中动态地建立和维护一个状态表, 数据包到达时, 对该数据包的处理方式将综合静态安全规则和数据包所处的状态进行。这种方法的好处在于: 由于不需要对每个数据包进行规则检查, 而是一个连接的后续数据包( 通常是大量的数据包) 通过散列算法, 直接进行状态检查, 从而使性能得到了较大提高; 而且, 由于状态表是动态的, 因而可以有选择地、动态地开通 1024 号以上的端口, 使安全性得到进一步地提高。

动态包过滤技术克服了传统包过滤仅仅孤立的检查单个数据包和安全规则静态不可变的缺陷, 使得防火墙的安全控制力度更为细致。

### 4.2　深度包检测

目前许多造成大规模损害的网络攻击, 比如红色代码和尼姆达, 都是利用了应用的弱点。利用高层协议的攻击和网络病毒的频繁出现, 对防火墙提出了新的要求。防火墙必须深入检查数据包的内部来确认出恶意行为并阻止它们。

深度包检测( Deep Packet Inspection) 就是针对这种需求, 深入检测数据包有效载荷, 执行基于应用层的内容过滤, 以此提高系统应用防御能力。

应用防御的技术问题主要包括: ①需要对有效载荷知道得更清楚; ②也需要高速检查它的能力。

简单的数据包内容过滤对当前正在通过的单一数据包的有效载荷进行扫描检测, 但是对于应用防御的要求而言, 这是远远不够的。如一段攻击代码被分割到 10 个数据包中传输, 那么这种简单的对单一数据包的内容检测根本无法对攻击特征进行匹配。要清楚地知道有效载荷, 必须采取有效方法, 将单个数据包重新组合成完整的数据流。

应用层的内容过滤要求大量的计算资源, 很多情况下高达 100 倍甚至更高。因而要执行深度包检测, 带来的问题必然是性能的下降, 这就是所谓的内容处理障碍。为了突破内容处理障碍, 达到实时地分析网络内容和行为, 需要重点在加速上采取有效的办法。通过采用硬件芯片和更加优化的算法, 可以解决这个问题。一个深度包检测的流程框图如图 3 所示。

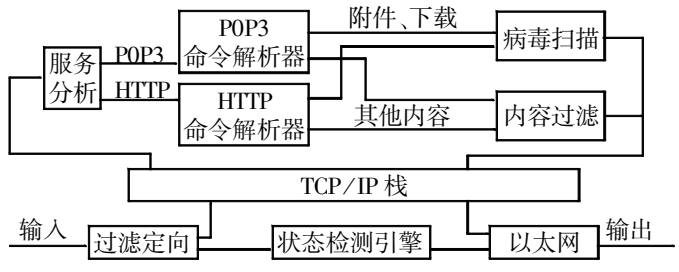


图 3　深度包检测框图

在接收到网络流量后, 将需要进行内容扫描的数据流定向到 TCP/IP 堆栈, 其他数据流直接定向到状态检测引擎, 按基本检测方式进行处理。定向到 TCP/IP 堆栈的数据流, 首先转换成内容数据流。服务分析器根据数据流服务类型分离内容数据流, 传送数据流到一个命令解析器中。命令解析器定制和分析每一个内容协议, 分析内容数据流, 检测病毒和蠕虫。如果检测到信息流是一个 HTTP 数据流, 则命令解析器检查上载和下载的文件; 如果数据是 Mail 类型, 则检查邮件的附件。如果数据流包含附件或上载/下载文件, 附件和文件将传输到病毒扫描引擎, 所有其他内容传输到内容过滤引擎。如果内容过滤启动, 数据流将根据过滤的设置进行匹配, 通过或拒绝数据。

## 5 流过滤技术

流过滤是东软集团提出的一种新型防火墙技术架构,它融基于状态的包过滤技术与基于内容的深度包检测技术为一体,提供了一个较好的应用防御解决方案。它以状态监测技术为基础,但在此基础上进行了改进。其基本的原理是:以状态包过滤的形态实现应用层的保护能力。通过内嵌的专门实现的 TCP/IP 协议栈,实现了透明的应用信息过滤机制。

流过滤技术的关键在于其架构中的专用 TCP/IP 协议栈。这个协议栈是一个标准的 TCP 协议的实现,依据 TCP 协议的定义对出入防火墙的数据包进行了完整的重组,重组后的数据流交给应用层过滤逻辑进行过滤,从而可以有效地识别并拦截应用层的攻击企图。

在这种机制下,从防火墙外部看,仍然是包过滤的形态,工作在链路层或 IP 层,在规则允许下,两端可以直接访问。但是,任何一个被规则允许的访问在防火墙内部都存在两个完全独立的 TCP 会话,数据以"流"的方式从一个会话流向另一个会话。由于防火墙的应用层策略位于流的中间,因此可以在任何时候代替服务器或客户端参与应用层的会话,从而起到了与应用代理防火墙相同的控制能力。如在对 SMTP 协议的处理中,系统可以在透明网桥的模式下实现完全的对邮件的存储转发,并实现丰富的对 SMTP 协议的各种攻击的防范功能。流过滤的示意图如图 4 所示。

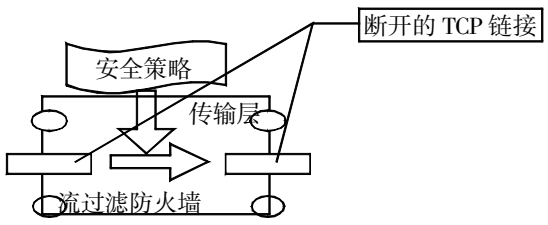


图 4 流过滤示意图

流过滤的结构继承了包过滤防火墙的应用透明的特点,非常容易部署,而且具有很好的应用防御能力。流过滤的另一个优势在于性能,完全为过滤和转发目的而重新实现的 TCP 协议栈相对于以自身服务为目的的操作系统中的 TCP 协议栈来说,消耗资源更少且更加高效,可以说流过滤采用专用的 TCP 协议栈解决了内容过滤障碍的问题,大大提高了防火墙处理速度。

## 6 结束语

本文从分析数据包结构出发,提出包过滤技术的核心问题是选取哪些字段信息,以及如何有效地利用这些字段信息并结合访问控制列表来执行包过滤操作,并尽可能地提高安全控制力度。在此基础上,分析了包过滤技术的两种发展趋势。我们看到,两种技术取长补短,相互融合,也是一种发展趋势。

**参考文献**:

[1] ouglas E Comer. 用 TCP/IP 进行网际互连[M]. 林瑶, 等. 北京: 电子工业出版社, 2001.

[2] Guido Van Rooij. Real Stateful TCP Packet Filtering in IP Filter[EB/OL]. http://citeseer.nj.nec.com/correct/491783.

[3] Richard Stiennon. Deep Packet Inspection: Next Phase of Firewall Evolution[EB/OL]. http://www.gartner.com/DisplayDocument?doc_cd=111579.

[4] 曹斌. 网络防火墙的体系结构[EB/OL]. http://neteye.neusoft.com/Docs/News/html/20010913112353854/htmlfile/20010913112353854.html.

[5] 费宗莲. 防火墙倾向内容过滤[EB/OL]. http://media.ccidnet.com/media/ciw/1169/c2301.html.

[6] 流过滤技术分析[EB/OL]. http://neteye.neusoft.com/Docs/News/html/20011212131209304/htmlfile/20011212131209304.html.

**作者简介**:

翟钰,硕士研究生,主要研究领域为网络信息安全;武舒凡,硕士研究生,主要研究领域为通信技术;胡建武,主要研究领域为自动控制。

(上接第 143 页) t-1 个签密者无法重构 t-1 次多项式 f(x),也就不能合谋得到签密者的私钥 $d_i$(i = 1, 2, …, t) 及组的私钥 $d_Q$。

(6) 在该方案中 t 个签密者用他们的子密钥对消息进行部分签密,然后把部分签密(而不是子密钥)发送给签密合成者。签密合成者把这些部分签密合成为签密消息,但他没有得到签密的子密钥,也无法合成组的私钥,这样就克服了签密合成者的欺骗。

## 4 结束语

本文首先提出一个基于椭圆曲线密码体制的签密方案,该方案是数字签名和公钥加密的有机集成,具有认证性、保密性、和计算量与通信量比较小等特点。然后基于所提出的签密方案和门限方案的思想,构造了一个新的基于椭圆密码体制的(t, n)门限签密方案。该方案除了具有保密性、认证性与鲁棒性外,还具有通信量小、执行效率高等优点。我们还可以利用文献[8, 9]中的密钥分配方法,把本文的方案进一步改进为没有可信中心的门限签密方案,限于篇幅我们将在另文中给出详细方案。

本文是在导师杨义先教授的精心指导下完成的,特此致谢。

**参考文献**:

[1] heng Y L. Signcryption and Its Application in Efficient Public Key Solutions[C]. Proceedings of Information Security Workshop (ISW'97). Springer-Verlag, 1997. 201-218.

[2] Lin C-C, Laih C-S. Cryptanalysis of Nyberg-rueppel's Message Recovery Scheme[J]. IEEE Communications Letters, 2000, 4(7): 231-232.

[3] Miyaji A. Another Countermeasure to Forgeries over Message Recovery Signature[J]. IEICE Trans Fundamentals, 1997, E80-A(11): 2191-2200.

[4] Boyd C. Digital Multisignatures[C]. Cryptography and Coding. Claredon Press, 1986. 241-246.

[5] Desmedt Y, Franlel Y, Threshold Cryptosystems[C]. Proc. CRYPTO'89, Springer-Verlag, 1990. 307-315.

[6] Shamir A. How to Share a Secret. Commun[J]. ACM, 1979, 24(11): 612-613.

[7] Desmedt Y, Frankel Y. Threshold Crytosystems[C]. Brassard Ged, Advances in Cryptology-CRYPT'89 Proceedings. Lecture Notes in Computer Science 435, Berlin: Springer-Verlag, 1990. 307-315.

[8] T P Pedersen. A Threshold Cryptosystem without a Trusted Party[C]. Proc. of Eurocrypt'91, Lecture Notes in Computer Science 547, Springer-Verlag, 1991. 221-238.

[9] C Park, K Kurosawa. New ElGamal Type Threshold Digital Signature Scheme[J]. IEICE Trans. Fundamentals, 1996, E79-A(1): 86-93.

**作者简介**:

戴元军(1974-),博士生,研究方向为密码学、电子支付、信息安全;杨成,博士生,研究方向为密码学、信息安全、信息隐藏。