分布式防火墙环境的边界防御系统

钱伟中[1]，王蔚然[1]，袁宏春[2]

(1. 电子科技大学电子工程学院 成都 610054; 2. 电子科技大学计算机科学与工程学院 成都 610054)

【摘要】针对传统边界防火墙在动态防御方面的缺陷，对防火墙和入侵检测系统之间的三种联动技术进行分析比较，提出了一种基于分布式防火墙环境，具备防火墙和入侵检测功能，采用系统嵌入方式的边界防御系统模型。模型利用队列通信机制实现防火墙和入侵检测协同工作，共同检测和防范对系统的入侵行为，并通过安全通信模块与分布式防火墙连接。最后给出了在Linux下的实现。

关 键 词 分布式防火墙; 边界防火墙; 入侵检测系统; 联动协议

中图分类号 TP393.08 **文献标识码** A

Boundary Defense System Based on DFW

QIAN Wei-zhong[1]，WANG Wei-ran[1]，YUAN Hong-chun[2]

(1. School of Electronic Engineering, UEST of China Chengdu 610054;

2. School of Computer Science and Engineering，UEST of China Chengdu 610054)

Abstract Allusion to the limitation of the traditional boundary firewall in dynamic defense, the thesis analyses and compares three interactive technologies between firewall and intrusion-detection system and proposes a boundary defense system model which with the function of firewall and intrusion detection adopts system embedded mode based on the distributed firewall environment. It implements firewall cooperates with intrusion detection by queue communication. Firewall and intrusion detect and defend intrusion to system and connect to distributed firewall by secure communicating module. Finally the thesis expatiates on the realization in Linux.

Key words distributed firewall; boundary firewall; intrusion detection system; interaction protocol

分布式防火墙由网络安全管理平台[1]、边界防火墙、入侵检测系统(Intrusion Detection System，IDS)[2, 3]、内部防火墙和主机防火墙Agent共同组成。安全管理平台实现对所有安全组件的统一配置、管理和信息的收集与分析。防火墙和IDS是分布式防火墙的重要组成部分。边界防火墙将内部可信区域与外部危险区域有效隔离，为网络边界提供保护，是抵御入侵的重要手段。然而，防火墙提供的是静态防御，它的规则都必须事先设置，对于实时攻击或异常行为不能实时反应，无法自动调整策略设置以阻断正在进行的攻击。IDS具有发现入侵的功能，其重点更多地放在对入侵行为的识别上，网络整体的安全策略还需由防火墙完成，同时，传统边界防火墙是信息安全的孤岛，无法根据分布式环境安全需要调整安全策略。为了对入侵行为进行更有效的检测与防御，本文在讨论联动技术基础上，提出并实现了基于分布式防火墙环境，融合边界防火墙及入侵检测功能的边界防御系统。

收稿日期：2004 – 09 – 27
基金项目：信产部电子信息发展基金资助项目
作者简介：钱伟中(1976 –)，男，江苏无锡人，硕士，助教，主要从事网络安全方面的研究.

1 防火墙与入侵检测联动技术研究

1.1 IDS自身安全性问题

目前入侵检测技术已成为网络安全中一个重要的研究方向而受到越来越多的重视，入侵检测技术是对计算机网络或计算机系统中若干关键点的信息进行收集和分析，从中检测到网络或系统中可能存在的各种非法攻击、恶意破坏、错误操作等违反安全策略的行为或迹象，并对此做出有效的防范和防卫行为。

IDS在提高网络安全性的同时，自身也成为网络攻击的目标。针对IDS的缺陷，经验的攻击者会直接对IDS进行攻击。由于网络IDS是“失败开放”(Fail Open)的，一旦网络IDS停止工作，其保护的网络就会暴露在攻击者面前。因此，针对IDS的攻击给网络安全带来的危害比针对普通主机的攻击更为严重。对网络IDS的攻击通常有欺骗攻击、崩溃攻击及拒绝服务攻击(Denial of Service, DOS)等。欺骗攻击指攻击者用精心设计的报文来误导IDS，使它对所分析的报文做出错误的判断。崩溃攻击指攻击者利用某种IDS设计上的缺陷，发送针对性极强的报文致使系统崩溃。针对网络IDS的DOS攻击，是指攻击者伪造大量有攻击表现的信息包，使被攻击的IDS频繁告警，耗尽可用资源，陷入拒绝服务状态，同时使管理者无法分辨哪些告警是针对真正的攻击发出的，从而使IDS失去作用。

1.2 防火墙和IDS的联动

入侵防御系统(Intrusion Prevention System，IPS)是指不但能检测入侵的发生，而且能通过自动响应方式，实时地中止入侵行为的发生和发展，保护信息系统不受实质性攻击的一种智能化的安全产品。它是目前网络安全技术领域中正在兴起的一项研究。

联动技术指IDS发现入侵后，通过一定的联动协议将阻断要求传递到防火墙从而实现对入侵源数据通道的封堵，它是IPS实现的重要手段。开放式安全平台(Open Platform for SECurity，OPSEC)技术就是典型的联动技术。国内的天融信网络卫士防火墙实现的网络安全体系也是联动技术的应用[4]。联动技术使防火墙及时获取IDS提供的入侵信息，阻断攻击源的攻击，保护正常的数据通道，记录隐藏的渗透和破坏性攻击，对防止系统渗透、大规模拒绝服务攻击、非授权访问等有较好的效果，同时对IDS也可进行有效保护。

防火墙和IDS之间的联动包括三种方式：(1) 端口映像方式：防火墙将网络中指定的一部分流量镜像到IDS中，IDS再将处理后的结果通知防火墙，要求其相应的修改安全策略。它适用于通信量不大但在内网和非军事化区(DeMilitarized Zone，DMZ)都有需求的情况。(2) 专用响应方式：当IDS发现网络中的数据存在攻击企图时，通过一个开放接口实现与防火墙的通信，双方按照固定的协议进行网络安全事件的传输，更改防火墙安全策略，对攻击的源头进行封堵。(3) 系统嵌入方式：把IDS嵌入防火墙中，IDS不再将网卡设置成混杂模式进行输入数据包的接收，而是检测通过防火墙过滤后的数据包，运行机制如图1所示。

进入防火墙的数据报先经过防火墙预先设定的规则库进行过滤，防火墙将需要IDS进行进一步检测的数据报送交IDS。IDS通过检测发现需要阻断的入侵行为时，将检测结果反馈给防火墙，由防火墙对数据包进行封堵或进行相关规则的动态修改，以阻断后续入侵数据包，从而达到整体安全控制的目的。

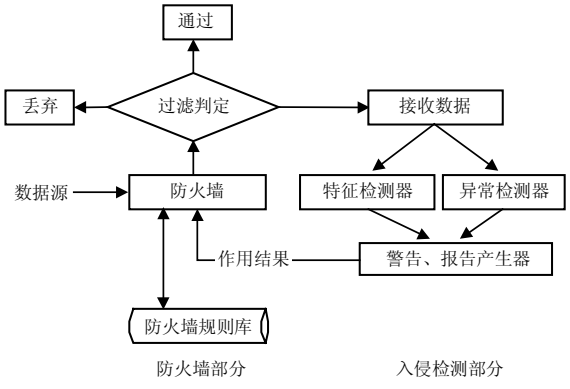

图1 采用系统嵌入方式的防火墙与IDS联动

三种方式中，(1)、(2)将防火墙和IDS分布在不同的设备上实现，两者之间的联动需要进行网络通信，当网络入侵频繁时，需要耗费较多的网络带宽。另外，联动通信的安全性需要考虑以下几个方面：地址欺骗攻击：如攻击者伪造内部可信服务器地址进行攻击，结果造成防火墙阻断该服务器发出的包，而使内部正常通信中断。信息传递安全。防火墙和IDS之间的通信应该防止网络窃听所造成的信息泄露。身份识别：攻击者可能冒充防火墙和IDS二者之一对另外一方进行攻击，因此需要建立完善的身份鉴别机制。与之相比，(3)即能实现(1)、(2)的安全防御功能，节约网络

带宽，同时由于安全模块都在同一台主机上实现，能够更加紧密结合彼此功能，防止地址欺骗，避免网络传输所带来的安全性问题。

2　边界防御系统结构模型

分布式防火墙将分布式通信技术和Agent技术引入到了传统防火墙体系结构当中，使用网络安全管理平台实现对位于子网边界的边界防火墙的远程管理。网络安全管理平台向远程边界防火墙分发安全策略和收集告警、审计信息。边界防火墙集防火墙和IDS功能于一体，并通过分布式通信技术将自身安全控制纳入到整个分布式防火墙环境中，形成边界防御系统。根据对三种联动技术的比较，采用系统嵌入的联动方式，系统体系结构如图2所示。

图2中，边界防御系统处于内外网络连接的边界，通过端口将网络安全域划分为内网、外网和DMZ，包括入侵检测和防火墙两个有机结合的功能模块。整体构成上，分为防火墙和入侵检测两个功能模块。防火墙工作在系统核心层，所有进入防御系统数据包先经过防火墙过滤。入侵检测功能模块在应用层实现，划分为主线程和入侵检测两个线程，通过队列通信机制实现数据在内核和用户态之间的传递。

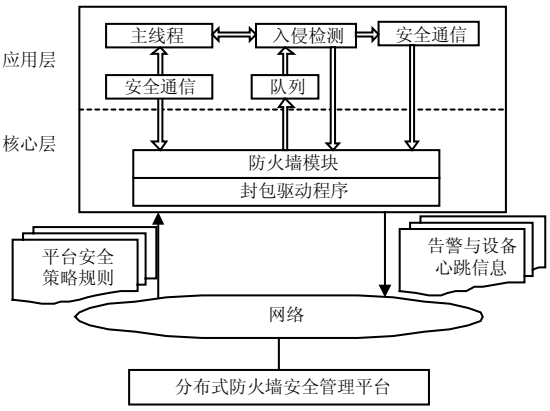

图2　边界防御系统体系结构

另外，由于在分布式防火墙环境下，各种安全组件在功能、地理位置、操作系统以及实现细节等方面存在多样性。因此如果要实现边界防御系统和分布式防火墙安全管理平台的无缝连接，必须采用统一的安全策略描述机制，同时必须保证网络安全管理平台和边界防御系统间的信息通讯的安全性、平台无关性和可扩展性[5]。为了避免硬件故障所导致的安全隐患，边界防御系统定期向网络安全管理平台发送心跳信息。

3　实　现

基于上述联动技术及边界防御系统结构模型，在Linux下实现了防火墙与IDS的联动。由于可扩展标记语言(eXtensible Markup Language，XML)具有结构简单、描述灵活和跨平台的特性，采用XML作为分布式防火墙的安全策略描述语言。采用基于公开密钥的加密技术的安全套接字协议层(Secure Socket Layer，SSL)证书加密通信实现边界防御系统和分布式防火墙各部件间安全通信。

3.1　主线程实现

应用层进程在系统启动后自动加载后作为系统守护进程。在Linux中，系统把线程作为处理器调度的对象，一个进程可由多个并发的线程构成。在进程创建时自动创建一个线程，称之为主线程。主线程采用TCP套接字，同时在SSL层进行加密通信，启动后处于Listen状态，等待接收指令。它实现了如下功能：(1) 接收网络安全管理平台发布的采用XML规范的策略描述语言，并根据策略对象定义分别转换为对应的本地描述语言，通过执行iptables脚本将规则应用于位于核心层的防火墙模块，或启动nids。(2) 接收入侵检测线程发送DOS或DDOS告警消息，产生自动策略下发到防火墙模块以阻止攻击的进行。(3) 负责向网络安全管理平台定时发送设备心跳信息。(4) 定时向网络安全平台发送升级请求，获取最新程序版本。(5) 定时证书更新。

3.2　联动模块实现

边界防御系统实现了防火墙和入侵检测的有机互动。处于系统核心层的防火墙模块采用iptables+netfilter架构，实现了对流出和流入子网的网络数据包进行截获和分析，提供ip_queue模块，在用户空间维护队列queue，同时提供netlink接口将网络层数据包从内核态读取到用户态供入侵检测线程nids处理。nids参考通用入侵检测框架结构，包括预处理器插件、规则处理模块和输出插件三个部分实现。预处理器插件实现对

HTTP、TELNET、远程过程调用等协议的协议数据规整处理。如将HTTP协议中url部分出现的16进制数据统一转换为ASCII码，以便后续规则处理模块处理。规则处理模块应用基于ip、端口、应用数据的模式匹配技术[6]，对数据内容进行分析，通过netlink接口向内核中的防火墙模块发送消息DROP、REPLACE、ACCEPT，决定该数据包的下一步处理。输出插件由预处理器插件和规则处理模块调用通过SSL安全通道向日志服务器发送告警信息，同时集成异常检测功能，基于如下偏差模型：

给定一随机变量X和若干个观测值X_1，X_2，…，X_n，对于X统计模型是确定第n+1个观测值与前面的n个观测值相比较是否有异常。假设一个新的观测值X_{n+1}处于“可信区间”，则其活动是正常的，否则认为是异常的。“可信区间”直接依赖于前面的观测值，“可信区间”范围在：[$avg-d\times stdev$，$avg+d\times stdev$]。avg为前n次观测的平均值，d为与系统有关的参数，$stdev$为前n次观测的标准方差：

$$avg=(X_1+X_2+\cdots+X_n)/n,\quad stdev=\sqrt{\sum_{i=1}^{n}(X_i-avg)^2/n}$$

根据计算值是否落在可信区间范围内判定异常入侵，向主线程发送告警消息，主线程根据消息体描述的入侵源地址、端口等信息，生成iptables防火墙规则并通过防火墙iptables管理模块应用规则，以阻断入侵数据通道，减少匹配次数，降低重复报警数量，以保护入侵检测资源，实现系统的主动防御。

3.3 安全通信实现

边界防御系统采用SSL证书加密通信实现通信安全，采用的数据结构如图3所示。

命令类型	运行方式	数据长度

图3 安全通信数据结构

当接收模块接收到指令数据后，根据指令数据中的命令类型号判别该命令的类型，根据运行方式字段进一步确定该命令的运行方式，根据数据长度字段确定需要读取的后继字节数。安全通信模块实现了对XML格式描述的策略的接收，同时实现了告警信息向网络安全管理平台的安全传送。

4 结 束 语

本文提出的边界防御系统模型在分布式防火墙系统环境下实现了防火墙与入侵检测联动，使防护体系由静态到动态，由平面到立体，提升了防火墙的机动性和实时反应能力，也增强了入侵检测的阻断能力，体现了网络安全深度防御的思想。与传统边界防火墙相比，系统能更有效防御网络入侵，并针对网络入侵的变化进行自动响应。

参 考 文 献

[1] Bellovin S M. Distributed Firewalls[EB/OL]. http://www. research. att. com/~smb/papers/distfw. html, 1999-10-20

[2] Denning D E. An intrusion-detection model[J]. IEEE Transaction on Software Engineering, 1987, 13(2): 222-232

[3] 蒋建春, 马恒太, 任党恩. 网络安全入侵检测: 研究综述[J]. 软件学报, 2000, 11(11): 1 460-1 466

[4] 满林松, 吴亚飚. TOPSEC 网络安全体系平台[EB/OL]. http: //www. yesky. com/20010611/183951. shtml, 2000-10-05

[5] 彭清岚, 李之棠. 分布式防火墙系统的安全机制设计[J]. 计算机工程与科学, 2003, 25(2): 11-15

[6] 韩东海, 王 超, 李 群. 入侵检测系统实例剖析[M]. 北京: 清华大学出版社, 2002

编 辑 漆 蓉