一种集成的可伸缩的网络安全系统*

蒋 韬, 刘积仁, 秦 扬, 常桂然

(东北大学 计算机软件国家工程研究中心,辽宁 沈阳 110006)
E-mail: jiangtao@neusoft.com
http://www.neusoft.com

摘要: 常用的网络安全技术有防火墙、VPN(virtual private network)和 NAT(network address translation)等,它们的作用各异.但现有的一些网络安全系统未能将上述技术有机地加以结合,不能很好地兼顾系统执行效率,对系统内部缺乏细粒度的安全管理.针对上述问题,提出了一种集成的可伸缩的网络安全系统——NEUSec(NEUsoft security system),它在 Linux 环境下将包过滤防火墙、VPN 和 NAT 技术有机地融合在一起,结合 NAT 和代理服务技术组成了可伸缩的虚拟代理服务器,提出了基于改进型 Radix 树的安全策略查找机制,采用 RBAC(role-based access control)技术解决了系统内部安全管理的问题.与其他安全系统相比,NEUSec 是一个较为全面的、可伸缩的、兼顾效率的网络安全系统,在实际应用中取得了较好的效果.

关 键 词: 防火墙;VPN(virtual private network);NAT(network address translation);Linux 环境;虚拟代理服务器;RBAC(role-based access control)

中图法分类号: TP393 文献标识码: A

随着 Internet 技术的迅速发展,网络安全问题却日益严重,成为其进一步应用的瓶颈之一.常用的网络安全技术有防火墙、VPN(virtual private network)和 NAT(network address translation)[1,2]等,但是它们各自只能解决某一方面的安全问题,然而安全系统必须遵循所谓的“木桶原理”,即整个系统的安全性取决于系统中安全性最弱的一环,并且目前形势对传统的网络安全产品提出了新的需求:① 必须是一种综合的网络安全解决方案,尽可能解决大部分网络安全问题;② 必须在系统的安全性和性能之间合理地折衷;③ 必须重视内部网的安全管理.因此将防火墙、VPN 和 NAT 等功能集成在一起不仅有利于提供完善的安全功能,而且有利于制订统一的安全策略,实现基于策略的网络安全管理.同时,由于政治、军事、经济上的原因,我国也应研制开发并采用自己的网络安全系统和数据加密软件,以满足用户和市场的巨大需求,这也是信息安全技术有别于其他技术的重要特征.为此,在我们承担的国家 863 高科技发展计划资助项目“Internet/Intranet 环境下的网络安全系统”中,实现了一个 Linux 环境下的集成的可伸缩的网络安全系统——NEUSec(NEUsoft security system),并利用 RBAC(role-based access control)技术实现了对内部网有效的安全管理.本文将着重介绍系统的总体结构和关键技术的实现.

1 NEUSec 系统的体系结构

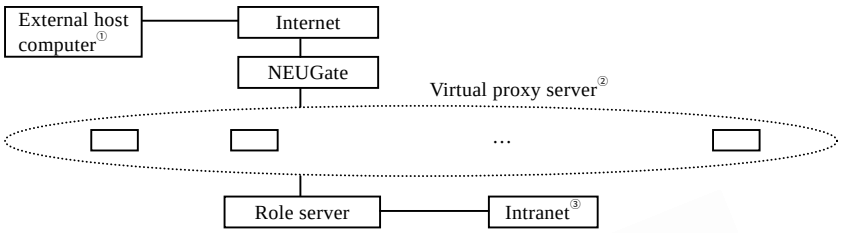
NEUSec 系统主要由 NEUGate、虚拟代理服务器和角色服务器几个部分组成(如图 1 所示),可以完成包过滤、代理、加密、认证、审计和日志等功能,以及对内网进行基于角色的访问控制,基本满足了目前绝大多数

* 收稿日期: 2000-04-18; 修改日期: 2000-09-19
基金项目: 国家 863 高科技发展计划资助项目(863-306-ZT05-05-5)

作者简介: 蒋韬(1970－),男,重庆人,博士,工程师,主要研究领域为网络安全技术,信息系统;刘积仁(1955－),男,辽宁丹东人,博士,教授,博士生导师,主要研究领域为信息安全系统,分布式多媒体技术;秦扬(1972－),女,河南沁阳人,工程师,主要研究领域为网络管理技术;常桂然(1946－),男,河北邯郸人,博士,教授,主要研究领域为计算机网络.

单位对网络安全的需求,在兼顾效率的同时,还考虑了安全系统的可伸缩性.

其中,NEUGate 是一个具有路由功能的智能网关,具有包过滤、VPN 和 NAT 功能.同时,为了克服传统包过滤防火墙在性能等方面的弱点,我们采用了基于 Stateful-Inspection[3] 架构的动态包过滤技术.传统的包过滤不考虑 TCP 包的连接状态,而动态包过滤技术的核心则在于从接收到的数据包中提取与安全策略相关的状态信息,将这些信息保存在一个动态状态表中,其目的是为了验证后续的连接请求,一旦一个连接建立起来,就可以不再对这个连接做更多工作,系统可以去处理别的连接,因此执行效率明显提高了.同时,采用动态包过滤技术还可以显著地提高系统的安全性,这是因为通过对连接状态的有效监控,从而杜绝了"中间人"攻击和序列号攻击等安全隐患.此外,动态包过滤还可以将动态状态信息组合起来,通过逻辑或数学运算,动态地产生一些规则,从而实现安全功能的可伸缩性,而不必像代理服务器型防火墙那样,每增加一项应用就必须开发相应的服务程序.对于无连接的 UDP 和 RPC 服务,我们通过在 UDP 通信上保持一个虚拟连接来实现 UDP 应用安全;由于对于 RPC 服务来说其端口号是不定的,我们通过动态端口映射图记录端口号、连接状态、程序号来实现此类应用的安全.同时,我们还采用一个专门的、基于内核的包转发引擎,能够加快包的转发速度.此外,缓存技术(cache)和基于 Radix 的策略查找和执行机制也能有效地提高防火墙的效率.



①外部主机,②虚拟代理服务器,③内部网.

Fig.1 The framework of NEUSec system

图 1 NEUSec 安全系统的体系结构

虚拟代理服务器是由一台或几台具有代理 HTTP,FTP,Smtp,Telnet 等协议功能的代理服务器组成,它们对用户是透明的.

角色服务器的主要作用是根据用户扮演的角色而不是用户的身份对内部网的资源进行访问控制,这样做的主要目的是简化内部网的安全管理,从而降低管理开销.

2 NEUSec 系统中关键技术的实现

2.1 NEUGate的实现

NEUGate 具有包过滤、VPN 和 NAT 的功能.由于 Linux 操作系统具有稳定、可靠、内核较小等优点,同时它又提供了源代码,可以保证系统底层的安全性.因此,我们在 Linux 系统中实现了上述功能,并对 Linux 的内核进行了裁减.NEUGate 在 Linux 系统上的实现分为核心态和用户态程序,其中核心态程序作为虚拟网络驱动程序加载,它与用户态程序之间的交互通过相应的接口来实现.整个系统采用模块化设计,可以根据需要调入相应模块.下面以 VPN 模块为例来介绍实现方法.VPN 模块的体系结构如图 2 所示.

从功能上讲,VPN 可分为 3 类:内部网 VPN、远程访问 VPN 和外部网 VPN.用来实现 VPN 的协议有多种,例如,工作在数据链路层的协议 PPTP,L2F 和 L2TP,工作在 IP 层的协议 GRE 和 IPSec,以及工作在会话层的 SOCK v5 协议.其中 IPSec[4]协议与其他协议相比具有功能全面、应用范围广、独立于具体的加密与认证算法的优点,并且支持 IPv6,并得到了绝大多数厂商的支持,具有广阔的应用前景,因此我们选择 IPSec 协议来实现 VPN 系统.

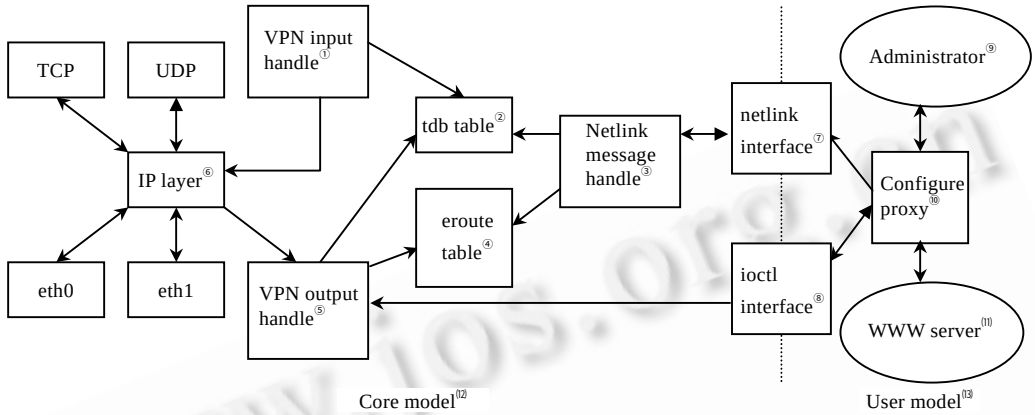
在 IPSec 的实现过程中,核心态模块实现对 IP 包的处理功能,即隧道封装、认证处理和加密处理.用户态模块向用户提供 VPN 系统的配置功能.核心态模块和用户态模块的通信,根据传递内容的不同,分别使用 netlink 接口和 ioctl 接口.

2.2 统一的安全策略管理

包过滤、VPN 和 NAT 等技术的融合,不仅可以满足功能上的互补,而且有利于制订统一的安全策略,保证系统安全策略实施的一致性和有效性.安全策略管理需要解决的一个关键问题是策略冲突问题.冲突的消解有多

种办法,其中最简单的办法是修改冲突策略的条件,以达到消解冲突的目的.如果仍然不能消解冲突,则可按照下面的方法来处理:

· “匹配优先”原则,即满足匹配的第 1 条策略.
· “优先权”原则,即满足优先权高的策略.
· “仲裁”原则,即增加附加条件以确定使用哪一条规则.



①VPN 输入处理,②tdb 表,③Netlink 消息处理,④eroute 表,⑤VPN 输出处理,⑥IP 层,⑦netlink 接口,⑧ioctl 接口,⑨管理员,⑩配置代理,⑪WWW 服务器,⑫核心态,⑬用户态.

Fig.2 The framework of VPN model

图 2 VPN 模块的体系结构

同时,安全策略服务的设计的好坏是影响系统性能的一个重要方面,需要考虑到下面一些因素:① 安全策略的配置在用户态,存储与执行在核心态,因此存在用户的易用性与系统的执行效率的平衡的问题;② 安全策略库的查找速度;③ 安全策略的执行速度.为了解决上述问题,我们设计的安全策略服务子系统包括用户态的配置代理、WWW 服务器、控制台,系统接口,核心态的安全策略引擎和安全策略库.一方面,为了方便用户表达策略,系统提供了两种策略配置接口,一种是本地配置接口,采用命令行方式;一种是远程配置接口,采用 WWW 界面方式,在这种方式下,后端使用 Java Servelet,前端使用浏览器,而数据的远程传递使用 SSL 协议.另一方面,安全策略需要以高效的数据结构保留在核心态,以利于 IPSec 处理模块调用.安全策略引擎对安全策略在用户态和核心态的转换起到了重要的作用,能够将用户在用户态描述的较为抽象的安全策略转化为具体的安全策略数据,有效地解决了易用性与系统效率的问题.同时,为了便于在核心态中快速地查找和执行安全策略,我们采取了两方面措施:① 采用缓存技术:在内存中专门开辟出一段缓冲区用于存放最近使用的安全策略,从而避免了频繁的安全策略库的查找过程.对于缓存的管理,采用缓存大小的动态自适应改变技术和最近最少使用(LRU)缓存更新以及缓存的一致性维护策略;② 设计了高效的 eroute 查找树.eroute 树是一种特殊类型的 radix 树,选择使用 radix 树主要基于有两点考虑:首先,radix 树可以支持非连续掩码(掩码中有“1”出现时,都从最左断开始并且连续出现),能够满足同时使用源地址和目的地址进行安全策略匹配的需要(将源地址和目的地址连在一起作为查找 radix 树的关键字,不可避免的要使用非连续掩码);其次,radix 树对不同长度协议地址的支持,能够适应增添新“选择子”的需求.使用 eroute 树的查询算法如下:

算法 **1.** eroute 树的查询算法

```
rn_search(v,head)
    struct eroute *head;
     register caddr_t v;
    {
        register struct eroute *x;
         for (x = head; x->rn_b >= 0;) {
            if (x->rn_bmask & v[x->rn_off])
```

```
                x = x->rn_r;
            else
                x = x->rn_l;
        }
    return x;
}
```

2.3 虚拟代理服务器的实现

虚拟代理服务器是通过 NAT 技术和基于权值的轮转调度算法实现的.NAT 分为多对多的动态映射和一对一的静态映射,其工作原理的算法描述如下(多对一情况下“IP+Port”的二级映射模式原理与此相同):

算法 **2.** 向外发送过程

```
BEGIN
Receive_a_Packet_from_Inside_interface(Packet);
If   (存在映射表中表项 X.Inside_IP_address==Packet.Sour_IP_address)
     {
      Replace_IP_address(Packet.Sour_IP_address,X.Outside_IP_address);
      Send_Packet_to_Outside_interface(Packet);
      }
else  {
       Create_a_Item_in_Table(映射表,Y);
       Y.Inside_IP_address=Packet_Sour_IP_address;
       Y.Outside_IP_address=从 Outside IP Pool 中取一个未用 IP;
       Replace_IP_address(Packet.Sour_IP_address,Y.Outsode_IP_address);
       Send_Packet_to_Outside_interface(Packet);
       }
END
```

算法 **3.** 向内发送过程(略)

通过 NAT 技术可以实现虚拟代理服务器的透明性,各代理服务器共享 Cache 和认证数据库,使用户觉得只是在与一个代理服务器打交道,而系统可根据性能需求对代理服务器的个数进行增删,从而满足安全系统在性能方面的可伸缩性要求,并且这种方案与单服务器方案相比具有较高的性能价格比和可靠性.同时,NEUGate 需要根据一定的规则将 IP 包发送到各个真实的代理服务器进行处理.通过分析,我们采用了基于权值的轮转调度算法.该算法的优点是实现时与代理服务器无关,同时又能兼顾各服务器之间的性能差异(例如,若 3 台服务器 A,B,C 的权值之比是 3:2:1,则相应的调度序列为 ABCABA).此外,NEUGate 上的监控进程会每隔一定时间对每个代理服务器发出 ARP 请求,若服务器超过一定时间没有响应,则说明该服务器发生故障,监控进程会立即通知调度进程将该服务器标记为不可用,并在调度表中删除其服务进程调度,从而满足系统在健壮性方面的可伸缩性要求.

2.4 RBAC策略的实现

有效的访问控制策略对系统的安全性起着重要的作用.传统的访问控制技术如访问控制列表、访问控制距阵、能力表等在大型系统管理时会带来查询速度慢、管理复杂和管理开销大的问题,而基于角色的访问控制(role based access control,简称 RBAC)技术可以有效地解决上述问题.在对由 Sandhu 等人提出的 RBAC96[5]模型以及 EnCommerce 公司提出的基于安全 Cookies 的 getAccess[6]系统和 Siemens Nixdorf 公司提出的基于 Kerberos 协议的 TrustedWeb[7]系统的分析基础上,我们采用了基于 CGI 程序的 RBAC 模型在 WWW 上的实现框架.其显著的优点是简单易用,无须对现有的服务器和客户端进行修改.

由图 3 可以看出,该框架主要包括下列部件:

· Role Server:用于说明并管理用户和角色的关系、角色等级、用户/角色的关系约束、现在活跃的角色、角色与权限之间的映射关系.

· CGI:它可以使用户在不修改 Web 服务器的前提下,完成对角色的权限分配和角色约束等功能.

·管理工具:它是一个特权程序,提供给服务器管理员.可以让服务器管理员创建角色以及用户、角色可以执行的操作;分配角色给用户,分配操作给角色;设定用户/角色关系,维护 RBAC 数据库.管理员可以通过浏览器来调用执行 RBAC/Web 管理工具.

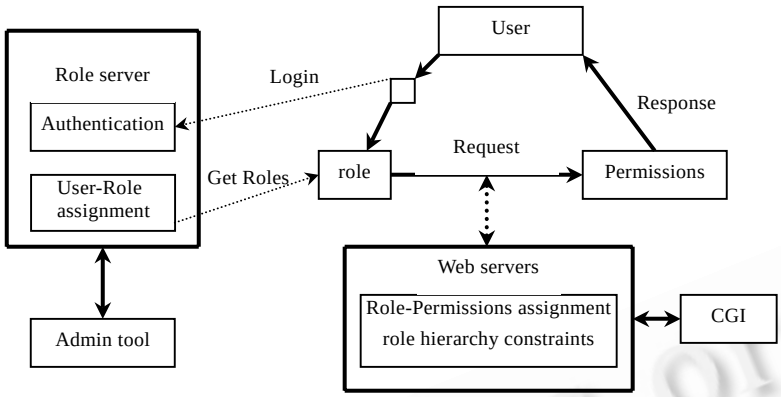


Fig.3 The framework of RBAC model on WWW

图 3 RBAC 模型在 WWW 上的实现框架

下面,我们以东方软件有限公司的内部网建设为例来说明 RBAC 模型的实现过程.

① 建立用户信息安全模型,根据用户的具体情况划分出若干角色和与之对应的权限.这个阶段要注意遵守最小权限和责权分离等安全原则.根据公司的具体情况,我们把角色分为总裁、副总裁、部长、职员 4 类角色,角色间具有偏序关系,其权限满足自反、传递和反对称等性质.

② 建立用户信息安全模型与 Web 服务器资源之间的映射,建立各自角色的访问控制矩阵.

③ 通过 get_user_id(*pw*,*u_id*),get_user_role(*u_id*,*u_role*),get_rules(*u_role*,*p_set*)等函数来实现用户认证、角色分配和权限分配等相应的访问控制功能.

通过实际运用,基于 RBAC 的访问控制方法具有以下特点:① 由于在用户和权限之间设立了角色这个中介,可以避免由于用户或权限的改动而引起存取矩阵的大幅度改动,简化了管理;② 建立的用户-角色、角色-权限之间的二级映射可以减小存取矩阵的规模,节省存储空间,改善响应速度.

3 性能分析

影响系统性能的因素有多个,如 IP 包的大小、主机 CPU 的性能、底层操作系统本身的性能以及网卡的性能等,对这些因素的把握主要是对性能价格比进行综合评估.但是从软件的角度来讲,动态包过滤技术和基于改进型 Radix 树安全策略查找机制以及采用何种加密和认证算法,都能够对系统性能产生一定的影响.为了验证系统的功能和性能,我们在东软集团的科学园和软件园这样的实际环境中对系统进行了测试,实验环境如下:分别以 PII 550(128M RAM)/Linux(2.2.36)平台作为两个 NEUGate 网关,采用 3COM 100M 自适应网卡,利用 SUN Ultra1,IBM RS6000 等中低档服务器作为代理服务器,以 SUN Ultra2 工作站作为角色服务器.通过对防火墙 VPN,NAT,代理服务器和角色服务器各功能的测试,结果表明系统工作正常,性能稳定,据测算在包过滤规则条数为 50、认证算法均采用 MD5 的情况下,加密算法采用 DES 算法时,其吞吐率峰值为 53.2M/s,均值为 30.2M/s;加密算法采用 3DES 算法时,其吞吐率峰值为 32.1M/s,均值为 19.7M/s.

4 结 论

目前,尽管国内外已研究和开发出一些类似产品,但大都各有侧重,缺乏一个完整的解决方案,例如,Checkpoint 公司开发的 Firewall-1 防火墙侧重于包过滤和 VPN 技术,没有应用虚拟代理服务器技术和基于角色的访问控制技术;Cisco 公司开发的 PIX 防火墙则缺乏方便的管理工具.而本文提出的一种集成的可伸缩的网络安全系统——NEUSec 具有以下显著特点:① 集成性,它在 Linux 环境下将包过滤防火墙,VPN,NAT 等技术

有机地融合在一起,提出了一个较为全面的网络安全解决方案;② 可伸缩性,本系统实现了在性能和健壮性方面的可伸缩性,特别是基于策略的安全管理技术能够满足安全管理的可伸缩性,企业规模的扩张不会影响到安全管理;③ 具有较高的性能价格比和底层安全性,特别适合国内中小企业的应用.总之,NEUSec 是一种较为全面的,兼顾效率的网络安全系统,具有较好的可伸缩性,能够满足绝大多数情况下的网络安全需求,目前在东软集团总部及其分支机构的实际应用中取得了较好的效果,其主要技术现已转移到东大阿尔派进行产品化工作.

References:

[1] Lin, Xiao-dong, Yang, Yi-xian, Ma, Yan. Design and implementation of Internet firewall. Journal of China Institute of Communication, 1998,19(1):66~69 (in Chinese).

[2] Jiang, Tao, Liu, Ji-ren. Design and implementation of a kind of virtual private network. Journal of Northeastern University, 2000, 21(2):136~139 (in Chinese).

[3] CheckPoint Corporation. Stateful Inspection Technology. White Paper, 2000. http://www.checkpoint.com/products/technology/stateful.html.

[4] Kent, S., Atkinson, R. Security Architecture for the Internet Protocol. RFC 2401, 1995. http://www.ietf.org/html.charters/ipsec-charter.html.

[5] Sandhu, R., Coyne, E.J. Role-Based access control models. IEEE Computer, 1996,29(2):38~47.

[6] EnCommerce. GetAccess. White Paper. 1998. http://www.encommerence.com/products.

[7] Siemens Nixdorf. TrustedWeb. White Paper. 1998. http://www.sse.ie/TrustedWeb.

附中文参考文献:

[1] 林晓东,杨义先,马严.Internet 防火墙系统的设计与实现.通信学报,1998,19(1):66~69.

[2] 蒋韬,刘积仁.一种虚拟私有网络模型的设计与实现.东北大学学报,2000,21(2):136~139.

An Integrated and Scalable Network Security System*

JIANG Tao, LIU Ji-ren, QIN Yang, CHANG Gui-ran

(*National Engineering Research Center for Computer Software*, *Northeastern University*, *Shenyang* 110006, *China*)

E-mail: jiangtao@neusoft.com

http://www.neusoft.com

Abstract: Firewall, VPN (virtual private network) and NAT (network address translation) are traditional network security technologies and each has different function. But some network security systems cannot combine these technologies, cannot give attention to efficiency of system, and scarce of fine-granularity inner security management. In order to solve these problems, an integrated and scalable network security system, NEUSec (NEUsoft security system), is presented in this paper, which integrates packet-filter, VPN and NAT technologies under Linux environment, combines NAT and proxy technologies to construct scalable virtual proxy server, the radix-based security policy search mechanism is presented, and the RBAC (role-based access control) technology is introduced to solve inner security management. Compared with other security systems, NEUSec is an all-around and scalable security system and gives an attention to efficiency. It has achieved a satisfactory result in practice.

Key words: firewall; VPN (virtual private network); NAT (network address translation); Linux environment; virtual proxy server; RBAC (role-based access control)

* Received April 18, 2000; accepted September 19, 2000
Supported by the National High Technology Development 863 Program of China under Grant No.863-306-ZT05-05-5