文章编号:1005－0523(2002)02－0005－04

# 基于规则的网络安全管理系统研究

李 蕙

(华东交通大学 现代教育技术中心,江西 南昌 330013)

**摘要**:首先系统地研究了网络安全技术,提出了网络管理安全参考模型,然后阐述了基于规则的网络安全管理技术,并给出了系统结构设计方案.该方案能提供更加简单而有效的途径,对动态环境下的安全进行管理.

**关 键 词**:基于规则;网络安全管理;网络设计

**中图分类号**:TP393.06 **文献标识码**:A

## 1 引 言

随着网络规模的扩大,网络安全技术要求更加复杂,当然也更加重要.随着安全技术的快速发展,IT组织对安全技术、工具的选择范围越来越大,如何合理地选择不同的安全技术组合,使之充分、有效地保护部门的IT资产,就成为我们必须面对,必须加以解决的问题.另外,由于网络规模的扩大,IT组织对安全技术、安全管理人员的需求越来越大,如何提高安全管理效率、降低安全管理成本,又成为IT组织必须解决的另一个问题.基于规则的网络安全管理系统,就是为解决上述问题而提出的.基于规则的安全管理是一种使用高层规则来管理安全技术的方法.使用这种方法,将促使IT部门把安全措施提炼成一组安全规则;其最大优点是许多功能可以自动而快速的执行.

## 2 网络安全概念与技术

要了解网络安全,有两个方面的内容:一是网络系统存在什么样的安全风险,包括风险的类型和风险的程度,以及评估可能的潜在攻击;二是如何运用安全管理技术,有效的防范这些安全问题.

### 2.1 安全风险

概括的讲,安全风险可能是来自部门内部的威胁,也可能是来自部门外部的威胁.

#### 2.1.1 内部威胁

顾名思义,内部威胁是来自部门内部的隐藏的威胁.CSI(Computer Security Institute)最近的Computer Crime and Security Survey显示:643例非授权访问中,有71%是来自内部的.内部威胁和外部威胁一样严重威胁着IT资源,甚至过之而尤不及.

#### 2.1.2 外部威胁

随着Internet的联通,来自外部的威胁呈指数增长.E-mail是外部威胁的最主要载体,其次是WWW和FTP服务.

来自外部的入侵者可以采取许多不同的攻击技术.尤其是对于那些基于Internet的商业系统,他们的商务很大程度上依赖于他们提供的服务的可用度(Availability).例如,被拒服务型(denial－of－service)攻击击跨很多著名网站,就是很好的例子.其它攻击技术,包括这样一些程序,它们占用绝大部份设备资源,以致合法用户无法获得资源,导致无法进行工作.

### 2.2 攻击类型

#### 2.2.1 病毒、软件炸弹型攻击

软件病毒是一段能自附在其它程序上的代码,

**收稿日期**:2001－11－15

**作者简介**:李蕙(1962－),女,吉林长春人,华东交通大学工程师.

中国知网 https://www.cnki.net

它能够窃取数据、口令等，能够获取未经授权的访问，能够更改或删除数据，能够崩溃系统、破坏硬盘，能够伪装成其它用户，它还能象医学上的病毒一样能够自我繁殖和感染其它系统.

对于病毒型攻击的防范措施包括：实行访问控制防止病毒写入敏感数据，安装病毒检测软件，避免从未知源地下载软件，以及任何软件安装前的必要检查等.

### 2.2.2 被拒服务型攻击

顾名思义，被拒服务型攻击是攻击者恶意反复发出的被拒绝的服务请求，这些请求数据包消耗大量的网络带宽资源，严重的会导致系统崩溃.例如，TCP SYN 流攻击就是这样一种被拒服务型攻击.攻击者从一个假冒的，实际不存在的地址发出 TCP—SYN，受攻击者回发 TCP—SYN—ACK 给该假冒地址，并且等待回答，因此联接处于等待状态；实际上，回答是永远也收不到的，因为源地址根本不存在；该联接保持可达 75 秒.显然，如果攻击者不断的发送 SYN，受攻击者可能因此而没法通讯，甚至崩溃.

### 2.2.3 IP 盗用型攻击

IP 盗用是一种欺骗目标机器致使其相信信息是来自/发往合法机器的过程.这种欺骗可能出现在 IP 系统的所有层，如地址分析协议 ARP 欺骗，IP 源地址欺骗，EMAIL 欺骗等.

### 2.2.4 数据帧被截取

一个用户跨过 Internet 联接远程的系统，这就使得能监视网络数据流的攻击者有进行攻击的可能.比方电子邮件，Telnet 或 Ftp 会话的内容，要是被攻击者监视的话，攻击者就很可能由此获得有关网址、商业传递等方面的信息.

### 2.2.5 会话截取型攻击

只要找到一个网络插头、一台网络主机，攻击者就可以监视网段上的信息流，以获得经主机授权的会话(session)；他可以发送大量的无用数据，以致原有系统崩溃；进而攻击者可以用这些崩溃了的主机地址，发送数据帧给其它主机.

会话型攻击的防止办法包括，使用加密方法防止数据被盗和会话被截取；另外就是强化物理端口的安全管理，防止未使用的网络插头被攻击者利用.

### 2.2.6 路由攻击

攻击者可以通过注入假的路由信息到路由系统中，从而重定向信息流至黑洞，重定向信息流到慢的链路上，乃至重定向信息流至其它目的地以便截取和修改.解决这一攻击的办法是，加强授权管理，只接受那些来自已知路由器的路由更新.

## 2.3 网络系统安全技术

### 2.3.1 防火墙技术

防火墙技术是一种隔阻外来入侵者，从而保护内部网络资源的技术.防火墙就是这样一个处于内部网络和外部公共网络之间的一个或多个系统，它能够限制、控制两个方向的访问.当然，很显然防火墙不能完全把来自外部的访问拒之门外，也就是应该在允许要求的访问和保护网络资源有个折衷；防火墙也能用于内部网，以限制对某一网段的访问.

### 2.3.2 IP 过滤技术

流入或流出网络的信息流都是源自一个特定的 IP 地址.IP 过滤就是一种访问控制机制，它能根据 IP 地址和要求的服务过滤网络信息流.如图 1 所示

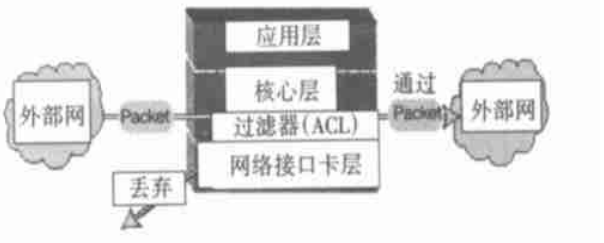


图 1 基于 IP 过滤技术的访问控制

访问控制表(ACLs—Access Control Lists)是 IP 过滤技术中的核心.访问控制表就象一个安全级别非常高的专门会议的来宾表一样，它包括：

•名单表：如什么人被邀请、允许参加
什么人不允许进入
可能还包括诸如餐饮服务人员、鲜花供应人员、演职人员等

•规则：如媒体人员禁止入内

所以，访问控制表(ACL) 就象来宾表的作用一样，除了描述能够和不能够通过防火墙或路由器的服务外，它还列出什么人能、什么人不能访问.

为了更有效地保证未经授权的访问和服务不被允许进入网络，必须审慎而全面地构造访问控制表.此外，访问控制表中规则的顺序也非常重要，因为防火墙是按顺序查找、匹配执行的.

对于大型复杂的网络系统来说，创建和维护访问控制表是一件乏味的事情.况且人工管理整个网络系统的访问控制表是相当困难的，有时只有极少的一部分访问控制表得到应用.

为此，为了充分利用 IP 过滤带来的益处，安全

中国知网 https://www.cnki.net

管理人员需要使用访问控制表管理工具,使得访问控制表的应用和管理更加方便.

### 2.3.3　应用代理技术

代理是防火墙中为用户通过防火墙申请服务起中介作用的一个应用程序.用户首先得建立至防火墙的联接,然后再是到防火墙中的应用代理的联接.代理应用再根据它收集到的信息和所要求的联接,决定是否允许这一请求.如果代理批准这一联接,它即建立一条单独的从防火墙到计划目的地的联接.代理接受来自用户的数据,然后传递到目的地.

代理技术的关键是不允许数据帧在网络系统之间直接流通,而是由代理在其中起中介作用.

### 2.3.4　虚拟专用网

虚拟专用网(VPN) 是一种利用公共 Internet 在不同地理位置之间建立一个安全网络联接的一种技术.虚拟网,简单的说,就是在两个兼容防火墙之间的经过加密的通讯联接.一个防火墙先把数据帧加密,再发送;另一个防火墙则对接受到的数据帧进行解密(当然要使用同一个密钥解密) .这种在传输前对数据帧进行加密,就避免了外部攻击者,当数据在网络上传输时,对数据进行截取.

## 3　网络管理安全参考模型

对网络系统来说可能存在各种攻击类型,相应的可以采取不同的解决办法.而对于大型的网络系统来说,它有不同的操作人员,有不同的系统,如网络管理系统、单元管理系统,和各种基本的网络基本单元所组成;它们互相之间存在不同的联接,因而联接的需求也不同.显然,有必要研究网络系统中的各个组成部件,它们之间的联系,这些联系类型可能存在的安全威胁及其解决方法.这就是网络管理安全模型问题.

网络管理安全参考模型是一个有用的工具.它可用于确定网络部件的安全需要,可用于考查部件之间的联接需要,可用于分析对于不同的联接存在不同的安全威胁,以及采取相应的解决办法.

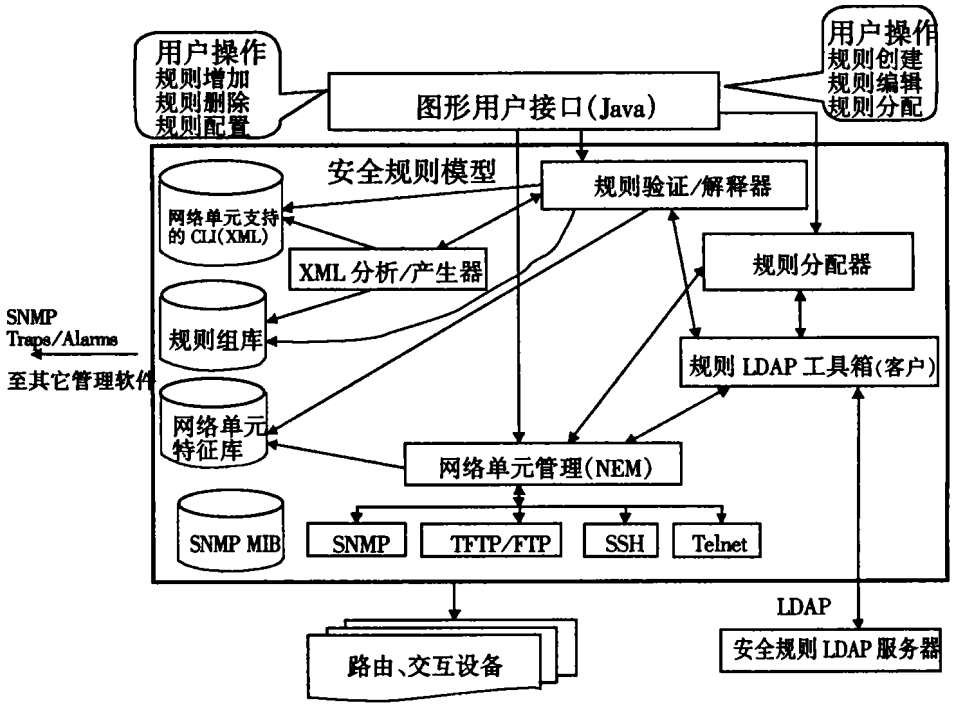


**图 2　基于规则的网络安全系统结构设计**

## 4　基于规则的安全管理系统设计

如图 2 所示,对于一个 IT 组织来说,它有广泛的安全技术、安全工具可供选择.然而,选择一套行之有效的安全工具组合实属不易,而要有效地管理这些安全工具,使 IT 组织的网络资源免受侵害,更是一种挑战.所以可以说,虽然所选择的技术是事关安全的重要方面,有效的管理这些安全技术却是最为关键的了.

基于规则的安全管理是一种利用高层规则,而非拘泥于技术细枝末节的管理安全技术的途径.例

中国知网　https://www.cnki.net

如,我们假定改变安全管理规则,使得指定的部门允许使用 FTP 服务.这种通过规则的管理,使得安全管理者只需输入一条规则,允许对某些部门的主机 FTP 服务.如果没有基于规则的管理,那么管理人员需要在所有的防火墙,或 IP 过滤设备上对每台所选定的主机,逐条的建立是否允许 FTP 访问的 ACL 列表.在大型网络中,当职员、服务器、防火墙、服务等发生变化时,安全管理之困难可想而知.

基于规则的安全管理,其优越性在于:(1)它能促使 IT 部门将安全管理途径归纳为安全规则.这将改善安全管理途径,使安全管理更加全面;(2) 多项管理功能自动而快速的实现成为可能.

### 4.1 基于规则的网络安全管理

基于规则的安全管理工具,为网络安全管理人员提供了定义和改变安全访问规则的能力.基于那些规则变化,安全管理工具自动的建立正确的访问控制表,并应用到相应的防火墙和路由器中.这可谓基于规则的管理工具能节省时间的非常经典之例子.网络/安全管理人员只需要定义或修改访问规则,而非逐条的编写访问控制表.当访问控制表达到 4,000 行时,这种时间的节省、复杂性的降低,效果是相当可观的.此外,对于大型网络系统来说,网络安全管理人员可能有成百上千的防火墙和 IP 过滤路由器要配置,而且每个设备可能有多个接口卡要配置;如果仍沿用手工办法对所有接口卡、所有设备建立和维护访问控制表,那么所需要的时间将是难以忍受的,而由于管理大量的访问控制表导致的复杂性的增加却更加严重.

### 4.2 基于规则的安全管理系统结构设计

## 4 结束语

网络系统安全的重要性和高级安全人员的缺乏从来就是一对矛盾.解决这一矛盾的途径是选择易于实施、易于使用而又高性能的安全工具.这些高性能包括提供易于使用的图形用户接口,自动的产生和实施访问控制表,以及方便的对这些访问控制表的维护.而基于规则的安全管理系统就是这样一种能够提供更简便却更有效的,在动态环境下的安全管理的工具.

目前,完全成熟的基于规则的安全管理系统市场上还很少见.可以预计,该系统的实现具有广泛的技术市场前景.

**参考文献:**

[1] Enterprise Management Associates, An Introduction to Network Security-Ensuring the Safety of Your Network, May 2000.

[2] White Paper, Policy-Based Networking Creating the Business-Driven Network, Lucent Technologies, Bell Labs Innovations.

[3] White Paper, IP Security, Ascend Communications, 1997.

[4] M. Condell, C. Lynn, J.Zhao, BBN, Security Policy Specification Language, Internet Draft, March 10, 2000.

[5] White Paper, Delivering End-to-End Security in Policy-Based Networks, Cicso Systems, 1998.

[6] M.F. Arnett, M. Coulombe, TCP/IP 实用技术指南[M]. 北京:清华大学出版社,西蒙与舒斯特国际出版公司, 1997.

[7] 胡道元 计算机网络[M].北京:清华大学出版社, 1998.

# Study on Policy-Based Network Security Management System's Design

**LI Yi**

(Modern Educational Technology Center, East China Jiaotong-University, Nanchang 330013, China)

**Abstract**: In this paper, the network security technology is discussed systematically, the network management reference model is presented, and then the technology of policy-based network security management is studied, finally the system design model of policy-based network security management is brought forward. This model can provide an easier and more efficient way to manage security in dynamic environments.

**Key words**: policy-based; network security management; network design

中国知网 https://www.cnki.net