文章编号:1001 - 9081(2003)12 - 0101 - 04

构建集成的 Linux 内核防火墙

郑小军,赵轶群
(同济大学 电子与信息工程学院,上海 200092)

摘 要:首先介绍了基于最新 Linux 内核的防火墙技术 netfilter 框架结构,包括包过滤防火墙、代理服务器、完全状态检测技术、NAT、DMZ 的概念、原理和用途,以及在 Linux 中具体实现的方法。着重探讨了一个用 Perl/ CGI 编写的集成的 WebAdmin 来构建一个集成的带有状态检测功能的防火墙系统,该系统可以通过 WebAdmin 管理界面来进行本地/ 远程配置管理整个防火墙的策略,并提供了包括对于 ADSL 服务获得的动态 IP 地址的支持,DNS 代理的集成,日志的记录,连接追踪,并特别集成了一个 PPTP VPN 的功能,使得该系统成为一个 all-in-one 的防火墙系统。

关键词:防火墙;Linux;netfilter;包过滤;NAT;DMZ;Perl/ CGI;VPN
中图分类号: TP393.08 **文献标识码**:A

Building an Integrated Firewall Based on Linux Kernel

ZHENG Xiao-jun, ZHAO Yi-qun
(School of Electronics and Information Engineering, Tongji University, Shanghai 200092, China)

Abstract: This article describes the netfilter framework of firewalls based on the newest Linux kernel, including the conceptions, principles, and usage of package filter firewalls, proxies, stateful-inspection technology, NAT and DMZ. It is mainly discussed the challenge of how to build an integrated firewall system with stateful-inspection by writing an interface of WebAdmin with Perl/ CGI language. The WebAdmin provides an unique management interface to maintain the whole strategies of the firewall, which is both available whether in short or long distance. Also it supports the dynamic IP address gained from ADSL service, an integrated DNS proxy server, and connection tracking, and it especially integrates a PPTP VPN server. With all these functions, it becomes a strong and all-in-one firewall system.

Key words: firewall; Linux; netfilter; package filter; NAT; DMZ; Perl/ CGI; VPN

防火墙是指设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口,能根据企业的安全政策(允许、拒绝、监测)控制出入网络的信息流,具有较强的抗攻击能力。随着人们对安全的日益重视和网络中各种不安全因素的涌现,防火墙已成为必不可少的安全工具。

由于 Linux 的低成本,健壮性以及对公开网络标准的支持,使其成为很多防火墙厂商最佳的选择,用以实现防火墙、IP 伪装、IP 网络地址转换和虚拟专用网络(VPN)。

Linux 防火墙经历了从 2.0 内核的 ipfwadm,到 2.2 内核的 ipchains,又到现在的 2.4 内核的 netfilter/ iptables,使得基于 Linux 内核的防火墙系统足够完善和强大以支持企业级的应用。

目前基于 Linux 的防火墙有很多,包括商业的和个人的。对于个人的 Linux 防火墙,一般都是通过输入一系列的命令或几个脚本来实施防火墙,这对策略的修改、实时监控和安全性都有很大的影响,缺少那些大型商用防火墙产品的管理工具。本文作者挑战性地探讨了用 Perl/ CGI 语言建立一个具有 Webadmin 管理工具的防火墙,提供了目前流行的 ADSL 的支持,使得在 IP 地址随时变化的情况下仍然能够保持防火墙的准确运行,并通过集成其它的一系列实用功能来实现一个 All-in-one 的防火墙系统。

1 防火墙用到的主要技术

1.1 包过滤

包过滤是防火墙最基本的功能之一。包过滤技术一般在网络层对数据包进行过滤,允许或拒绝特定的分组通过。过滤一般是基于一个 IP 分组的源地址、目的地址、协议和端口号等进行过滤。

1.1.1 Netfilter 框架

Netfilter 是 Linux2.4 实现的防火墙框架,它提供了一个抽象、通用化的框架,该框架定义的一个子系统实现的就是包过滤子系统。Netfilter 由一系列基于协议栈的钩子函数组成,为每种网络协议(IPv4、IPv6 等)定义一套钩子函数(IPv4 定义了 5 个钩子函数)。如图 1[1]。

数据包从左边进入系统,进行 IP 校验以后,数据包经过第一个钩子函数 NF-IP-PRE-ROUTING 进行处理;然后就进入路由代码,决定该数据包是需要转发还是发给本机的;若该数据包是发给本机的,则该数据经过钩子函数 NF-IP-LOCAL-IN 处理以后传递给上层协议;若该数据包应该被转发则它被 NF-IP-

收稿日期:2003 - 07 - 05;**修订日期**:2003 - 11 - 07
作者简介:郑小军(1978 -),男,江苏无锡人,硕士研究生,主要研究方向:网络信息安全、IDSS; 赵轶群(1943 -),男,江苏昆山人,教授,博士生导师,主要研究方向:决策支持系统、办公自动化.

FORWARD 处理;经过转发的数据包经过最后一个钩子函数 NF-IP-POST-ROUTING处理以后,再传输到网络上。

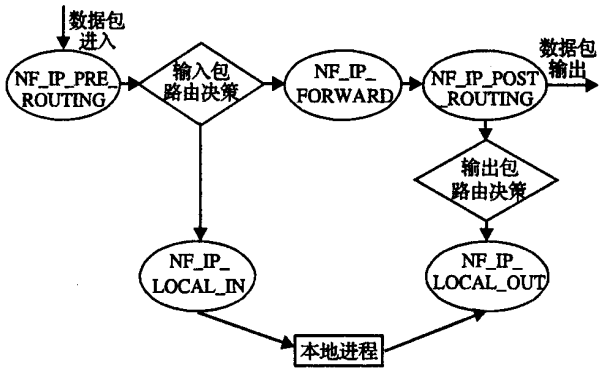

图 1 netfilter 框架示意图

本地产生的数据经过钩子函数 NF-IP-LOCAL-OUT 处理后,进行路由选择处理,然后经过 NF-IP-POST-ROUTING 处理以后发送到网络上[2]。

1.1.2 表、链规则

表提供特定的功能。缺省表是 filter,nat 和 mangle。

链是包传播的路径。不同的表包含了不同的内置链,用户自定义链能指向内置链。如果一个包通过用户链中没有匹配,它将返回调用的链。如果一个包通过内置链中没有匹配,那么将由此链的缺省方针来确定是丢弃或接受。

规则就是在链中用来实现某个特定匹配。图 2 表示数据包在 netfilter 表和链中的传播(与图 1 对应)。

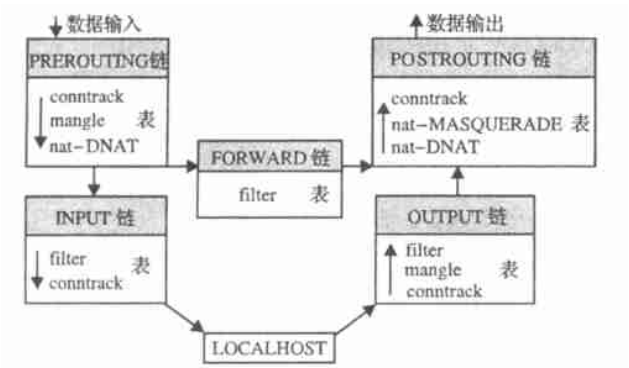

图 2 数据包在 netfilter 表和链中的传播

1.2 代理服务器

代理工作在应用层,主要是作为一个外部系统和内部系统的中继站,这样,数据包就不是直接传送,而是在中间作一些预处理后进行传送。每个代理只对已经精确定义协议应用的协议服务,可以对其它的协议封闭,并且可以采取一些安全策略。

代理服务器主要有以下两点优势:

1) 提高性能:代理服务器能够显著提高一组用户使用的性能,因为它可以在一定时间内缓存所有请求的结果。一个代理服务器可以支持成百上千的用户。主要的在线服务如 Compuserve 和美国在线都使用代理服务器阵列。

2) 过滤指令:代理服务器也可用于过滤指令,例如,一个公司可以通过代理服务器阻止公司的员工访问某些特殊的网站。

应用层网关的优点是允许受保护和未受保护网络的完全分离,确保没有包被允许从一个网络到另外一个网络直接传送。

1.3 完全状态包检测

状态检测技术(stateful-inspection),是在传统包过滤上的功能扩展,最早由 checkpoint 提出。

每个网络连接包括以下信息:源地址、目的地址、源端口和目的端口,叫作套接字对(socket pairs);协议类型、连接状态(TCP 协议)和超时时间等。防火墙把这些信息叫作状态(stateful)。传统的包过滤在遇到利用动态端口的协议时会发生困难,因为事先不知道需要打开哪些端口,如果将所有可能用的端口打开的话,则安全性得不到保障。

实现了状态检测的防火墙,能够检测每个连接状态,通过检查应用程序信息(如 ftp 的 PORT 和 PASS 命令),来判断此端口是否允许临时打开,而当传输结束时,端口又马上恢复为关闭状态。这样,它在自己的内存中维护一个跟踪连接状态的表,比简单包过滤防火墙具有更大的安全性。

在 Linux2.4 内核中,iptables 中的状态检测功能是由 state 选项来实现的。包括 INVALID、ESTABLISHED、NEW、RELATED 等状态选项。

1.4 网络地址转换(NAT)

网络地址转换(Network Address Translation)用于将一个地址(如私有局域网地址 LAN)映射到另一个地址(如 Internet 地址)。NAT 允许将一个组织私有地址的主机透明地连接到 Internet 中的主机,而无需内部主机拥有实际的 Internet 地址。

NAT 的这种将一个网络(如 LAN)隐藏在一个或几个 IP 地址下,对外部也隐藏了内部网络的拓扑结构,使得黑客很难知道内部网的结构,更好地保护了内部网。

Linux 有两种 NAT:SNAT(源端网络地址转换)和 DNAT(目的端网络地址转换),其中,SNAT 还包括 Masquerading(隐藏),是 SNAT 的简易设置。

Netfilter/iptables 的 NAT 表用两个链实现 NAT:PREROUTING(用于 DNAT)和 POSTROUTING(用于 SNAT)。

1.5 中立区(DMZ)

中立区(DMZ)也成为非军事区,其目的主要是为了管理配置的方便。通过将私网中需要向外界提供服务的服务器(如 HTTP 服务器、FTP 服务器和 Mail 服务器等)放到一个独立的网段上,再通过包过滤(如对于 HTTP 服务器只允许 HTTP 协议等)和 DNAT 将目的地为外部网接口地址转化到 DMZ 中的特定服务器上。配置有 DMZ 区的防火墙一般需配备至少三块网卡,采用三区隔离的概念[3]:内部网、Internet 和 DMZ。如图 3。

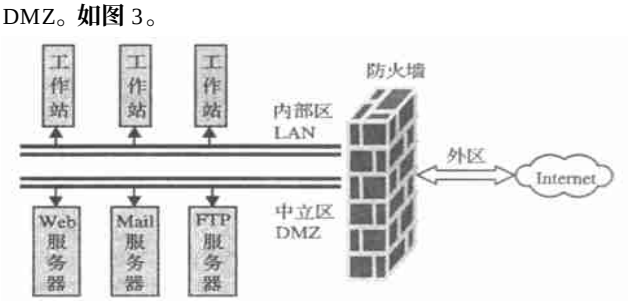

图 3 三区隔离的模型

中立区(DMZ)从本质上来讲和 LAN 没有区别,只是人为的规划和限制。因为如果把这么多 Internet 服务器都放置

在 IP 地址为同一个网段的 LAN 中,使得和 LAN 中其它的工作站共存,势必造成网络拥挤和 Internet 服务器的安全隐患。而通过设立与 LAN 分离的中立区后,可以只允许所需的服务通到中立区,大大减少了网络的冲突,增强了服务器的安全性,同时也提高了管理的方便性。

1.6　管理和日志

对于防火墙,一个很重要的功能是对各种行为进行记录和管理,包括系统自己的行为、内部网到外部网的行为,以及来自外界的各种攻击。

在这基础上,如果将日志的数据统计出来,用统计表格或统计图直观地表示出来,则可以增加管理的方便性和有效性。

1.7　连接追踪

防火墙一个很有用的作用就是能够实时地追踪当前的所有连接。通过检查当前进行的连接,可以知道当前防火墙的连接状态,这样就可以跟踪所需要监测的对象。

2　防火墙的主要模块实现

2.1　包过滤型防火墙的策略和实现

根据新的 iptables,对于不同网段的网络进行 FORWARD 转发,对于到主机的则使用 INPUT/OUTPUT 链。譬如,为了让 LAN 中的主机(192.168.0.x/24)访问 Internet(0.0.0.0/0),则使用 FORWARD 链转发;而为了让外界或内部访问到连接到 Internet 的那块网卡(假设为 eth1),这主要是在构建内部 HTTP 等服务器和使用 VPN 进行连接时使用到,则必须使用 INPUT 链允许外界访问该接口。如果使用静态公网地址,则可以比较简单地人为设定,但是如果使用 ADSL 拨号上网,就应该是允许连接通的虚拟接口(如 ppp0)上通过,但是由于地址是动态获得的,并且每次都不一样,则可以通过 perl 控制脚本每过一段时间来检查 ADSL 的连接,来动态配置由 ADSL 拨号获得的动态 IP 地址,使得在建立 ADSL 连接时就存储该 IP 地址,并且执行 $IPTABLES -A INPUT -s $UNIVERSE -d $EXTIP -j ACCEPT 来允许数据包的流通。

在所有的 FORWARD,INPUT/OUTPUT 链中都使用 -state 进行状态检测来提高安全性。

所有的配置参数都由 perl 命令保存在磁盘上,以便显示和恢复。并且一些基本的网络设置,如网络地址、网络服务、网卡的配置等都分为独立的管理界面进行管理,所得的数据可以供包过滤、网络地址转换等利用。

每增加/删除一个 package filter 规则,都是先保存配置参数,再执行 iptables 相应的命令,以保持磁盘上的记录和防火墙中过滤的策略同步。

2.2　网络地址转换的策略和实现

网络地址转换的功能非常多,可以对格式"源地址、服务、目的地址、服务"中的任何一项进行转换。SNAT 是对源地址进行转换,执行为 system "/sbin/iptables", "-t", "nat", "-A", "POSTROUTING", "-p", "$proto", "-s", "$rc-net", "--sport", "$port", "-d", "$les-net", "--dport", "$lport", "-j", "$at-type", "--to", "$hange-to";该命令解释为:对 nat 表中增加一条类型为 $at-type(SNAT)的规则,针对的协议为 $proto,源地址和端口为 $rc-net、$port,目的地址和端口为 $les-net、$lport,并将源地址转换为 $hange-to 的地址。应用举例为 LAN 内的所有主机共享上网,在其访问 Internet 时,对于外界,它们的地址为防火墙上对外的那块网卡上的地址,这样就隐藏了 LAN 内的拓扑结构,有效地保护了 LAN 的主机。

这里要特别说明的是 $les-net,如果使用静态 IP 地址的话则没有什么困难,但是如果是诸如 ADSL 动态获得地址的话,则有一定的困难。试想,如果 $les-net 用到了动态地址,则当 $les-net IP 地址改变了的话,非但原来的配置不能起作用,而且还会留下安全漏洞,因为这时候 IP 地址已经指到了别的主机上。为了解决这个问题,可以在/etc/host 文件中保存各个接口的地址和相应的主机名称,包括动态获得的地址,而在 $les-net 处则用主机名称代替。在每次更改 IP 的时候,动态更改 host 文件中的动态地址,而主机名没有改变。这样从理论上来讲好像就完全解决了。但事实是,Linux 系统在第一次配置 NAT 的时候,内核中 $les-net 处使用的确实是主机名,然而,当 IP 地址改变时,则系统利用缓存中的旧的 IP 地址替换掉了主机名,这样一来,原来的设想就不能实行了,只能在 IP 地址改变后重新刷新 NAT 链表。

对于 SNAT,还有一个简易的设置,那就是 masqurading 选项,它可以将一个 LAN 内的机器通过一个公网地址访问 Internet,允许的协议是所有的服务,而不能特定指定。执行的命令为 system "/sbin/iptables", "-t", "nat", "-A", "POSTROUTING", "-o", "$masq-if", "-s", "$masq-net", "-j", "$at-type"。

NAT 的另外一种就是 DNAT(目的地址转换)。一般来说,对于很多中型的组织和机构,都想将自己的 Web/FTP/Mail 服务器由自己保管,这样可以提供安全性、低费用性和无限的空间,这就需要用到 DNAT 技术。system "/sbin/iptables", "-t", "nat", "-A", "PREROUTING", "-p", "$proto", "-s", "$rc-net", "--sport", "$port", "-d", "$les-net", "--dport", "$lport", "-j", "$at-type", "--to", "$hange-to";其主要的作用是将来自外界的对于专门服务器的访问(如 Mail 服务器)定向到所指定的主机上,如将来自外界的 pop3/smtp 的请求,首先到达防火墙与 Internet 相连的网卡上,让后通过 DNAT 将所请求的服务 POP3/SMTP 定向到 DMZ 中的特定 Mail 服务器上。

2.3　VPN 的实现

目前用户对于 VPN 的要求越来越迫切,特别是一些企业的出差或旅游人员远离公司的时候,有时需要访问公司内部的服务器,这个时候需要一个安全的连接来提供这种服务。VPN 就可以很好地实现这个需求。这次集成在防火墙中的 VPN 采用的是 PPTP 的 VPN,现在还有一种流行的 VPN 是 IPSec VPN,IPSec VPN 可以提供更高的安全性,但是也需要特殊的客户端来提供支持,这无形中也增加了客户的开销。而 PPTP VPN 主要是 Microsoft 对 Windows 客户提供的 VPN 支持,可以在满足一定安全性的条件下,方便地进行 VPN 的连接。而且,移动用户的操作系统一般都是 Windows 系列的操作系统,使 PPTP VPN 非常实用而高效。

3 用 Perl 语言实现集成的 Linux 防火墙

3.1 集成总体概述

在构建集成的 Linux 防火墙的过程中,由于目前 ADSL 以低廉的价格提供了较高的带宽,所以获得了普遍的应用,本 Linux 防火墙集成了 ADSL 的功能(使用的 PPPoE 工具可以从 < http://www.roaringpenguin.com/pppoe 获得 >),同时也提供固定网关的支持,所以可以支持目前大部分 Internet 接入方式。对于一般的防火墙系统,普遍是不支持 ADSL 等服务的,因为这样的服务使得防火墙获得的 IP 地址是动态变化的,而对于防火墙来说,最重要的管理策略都是通过 IP 地址来进行管理的,所以如果连接外网的 IP 地址变化的话,那么原来配制的策略就会失效,同时也会产生安全漏洞。所以本防火墙要对动态变化的 IP 地址实施特殊的算法策略,使得防火墙在任何时候都能保持正确的配置而稳定地运行,包括 DNS 服务器、PPTP VPN 等支持,而且要在系统重起或者 Internet 连接断掉的情况下也能正常地恢复。

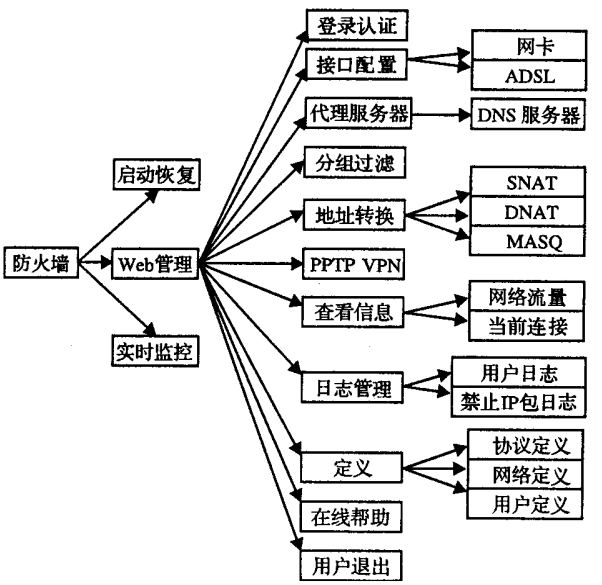

图 4 防火墙的结构

该系统采用 Perl CGI 语言构建了一个 WebAdmin 的管理界面,使得防火墙的所有管理和配置得以轻松进行本地、远程管理,这样就实现了一个完全整合的防火墙。

3.2 Apache 的配置、https 加密

由于需要用 perl 语言调用 Linux 系统命令,而这些命令只能在 root 的权限下执行,所以需要更改 Apache 的 httpd.conf 配置文件,将 User 改为 root。但是 Apache 一般并不允许这样修改,为了达到这个目的,需要下载 apache 源代码,在 Configuration 中设置 EXTRA-CFLAGS =-DBIG-SECURITY-HOLE,然后重新编译,安装。

为了在远程管理时增加安全性,可以通过 SSL 加密,使用 https 进行连接,端口是 443。当然,要实现 SSL 加密还要给 apache 加一个 SSL 补丁和 openssl 进行重新编译。

3.3 启动时规则(清空所有表、链)

当防火墙启动的时候,为了避免影响已存在的规则,应该予以清空,并且设置防火墙缺省的策略为拒绝所有的协议。一般来说,防火墙开始配置的时候有两种策略可供选择:一种是允许所有的策略,以后根据需要禁止特定的访问;另外一种就是先禁止所有的访问,然后根据需要打开特定的服务。对于防火墙来说,第一种策略存在着打开过多的服务的可能性,而管理员很难关闭一些不被注意的服务,但是这些服务却存在着给网上攻击留有后门的可能性。而第二种则很好地防止了这种危险,同时也符合"按需分配"的原则,在提高安全性的同时,也提高了系统的性能和带来了管理的方便。

Linux netfilter 中相应的命令为:刷新(flash)用户的所有策略为 IPTABLES-F INPUT/OUTPUT/FORWARD/-t NAT。其中,-F 表示刷新,INPUT/OUTPUT/FORWARD 分别为输入、输出和转发链,-t NAT 表示网络地址转换表。IPTABLES-P INPUT/OUTPUT/FORWARD DROP 中,-P 代表策略,DROP 表示禁止策略。防火墙策略一般为:ACCEPT(允许)、DENY(拒绝,并且返回拒绝信息给所请求的主机)和 DROP(拒绝,但不返回任何信息)。

所有这些都可以放到/etc/rc.d/rc.local 中,包括所有的 filter,snat/dnat/masqurading 和其它一些需要在启动的时候运行的脚本。

3.4 DNS 的规则

该集成防火墙在 Internet 上既保护 LAN,又是 LAN 的网关,为了可以使 LAN 内的客户端可以正确解析 Internet 域名,需要建立一个 DNS 服务器。但是对于一个集成的防火墙来说,如果把各种服务器软件都放在防火墙所在的机器上,那么无疑会带来防火墙的不稳定和低效,并且也影响 LAN 内访问的性能和服务器软件自身的整体性能,而且,把很多服务都放在一个有公网地址的服务器上,也会增加安全隐患。

我们在该防火墙上安装了一个简易的 DNS Server,有两个功能:转发来自 LAN 内客户端解析域名的请求到电信的 DNS 服务器上;缓存已经被解析过的域名,以便为 LAN 内的再次解析提供快速回答。

3.5 关机后重起的规则

防火墙在关机或重新启动前应该保存先前的配置,启动后恢复原来的配置。在碰到断电或其它突发事件时,如果在之前进行了防火墙策略的修改,但是没有保存,那么在系统启动后,先前的修改就消失了,这就需要在每次修改后自动保存防火墙的配置。

这里有两种策略。第一种:由于已经将防火墙的配置参数都用 perl 语言保存到了磁盘上,对于防火墙配置的每次修改都是实时的,所以无论是关机/重起,还是掉电式的突发关机,所有的参数都已保存在磁盘上,只要启动防火墙就可以根据配置文件由程序脚本自动重新配置防火墙;第二种和第一种差不多,netfilter 的配置工具 iptables 还有一个保存和恢复 iptables 配置策略的命令:iptales-save 和 iptables-restore,可以在防火墙重新启动的时候通过调用 iptables-restore 来自动载入原先由 iptables-save 保存的防火墙配置文件,和第一种方法不同的是,需要在每次修改防火墙策略后执行 iptables-save 命令保存和覆盖原来保存过的配置。

从表面上来看,使用 iptables-save/iptables-restore 应该比较简单,但事实是,用 iptables-save 保存的防火墙的策略在细节上和原来的命令有细微的差别,虽然在效果和功能上完全一致,但是正是这些细微差别却导致了使用 iptables-restore 后,无法对规则进行删除等的修改。所以,iptables-save/iptables-restore 命令应该说适合简单命令或脚本配置的防火墙,而不适合用于

(下转第 117 页)

乎是百分之百正确,表示数字水印对低通滤波有很好的强健性。

三种音乐经过标准化(Normalization)攻击后,数字水印取出的结果显示百分之百正确,表示我们的数字水印方法对标准化(Normalization)攻击有很好的强健性。

4.3　D/A 与 A/D 的攻击

针对可能的 D/A 与 A/D 攻击,我们模拟将藏有数字水印的音频信号从电脑的音效卡类比输出,利用传输线传输到另一台电脑的音效卡类比输入端。大提琴的音乐长度约 30s,双声道,取样频率为 44.1kHz,初始 d 值为 0.05,数字水印为 1010101……的连续数据,每个 Section 的长度 L 为 300 个 sample,经过 D/A 类比传输及 A/D 后,大提琴信号的振幅会改变,而且数据变得不同步,可能会增加一些前端信号。

我们发现在某些位移量的区域,数字水印有百分之百的正确率,表示经过 D/A 类比传输及 A/D 的大提琴音乐有数字水印的存在。由此实验结果得知,经过 A/D、D/A 及类比传输的攻击之后,本论文方法嵌入的数字水印仍可以百分之百地取出。

4.4　信号裁剪的攻击

嵌入数字水印的信号为大提琴的音乐,长度约 30s,双声道,取样频率为 44.1kHz,初始 d 值为 0.05,每个 Section 的长度 L 为 300 个 samples。大提琴的数字水印音乐分别经过不同大小的裁剪,使得 Section 位置变得不同步。利用同步码的搜寻法,找出位移的大小,则可以知道每个 Section 的正确位置,将数据完整地取出来。虽然利用同步码的搜寻法,找出位移的大小与实际有一些误差,但是这些位移的误差对实际的数字水印抽取没有很大的影响。

由实验结果得知,利用同步码的搜寻法可以将数字水印百分之百地取出。虽然数字水印可以完整地取回,但并不表示取回的二进位数据都没有错误,在数字水印的方法中,利用错误更正码中的回旋码来修正错误,并且利用重复隐藏多个数字水印来增加取出的正确性。

5　结论

在本论文中,数字水印音乐经过 MP3 压缩和一些数字信号处理的攻击测试,证明它们均有足够的强健性以对付非法人士的刻意攻击和破坏,能够发挥数字水印的功用,充分保护著作权及网络传输安全。但还有一些问题需要改善和解决:

1) 数字水印提取时,如果音频信号和原始音频不同步,将会花费相当的时间来搜寻数字水印,所以未来必须建立一套更快速的搜寻方法,提升数字水印提取的时间,使数字水印能更有效地应用。

2) 发展多数字水印(即多个数字水印可同时被 embedding,且不互相破坏)技术使数字水印更具实用性,但是目前还没解决多个数字水印之间互相影响的问题。

参考文献

[1] Boney L, Tewfik AH, Hanmdy KN. Digital watermarks for audio signals[A]. Proceedings of the Third IEEE International Conference on Multimedia Computing and Systems[C], 1997.

[2] Gruhl D, Lu A, Bender W. Echo hiding, Lecture Notes in Computer Science[A]. Proceeding of First International Workshop on Information Hiding[C]. Cambridge, UK,1996,295 - 315.

[3] Bassia P, Pitas I. Robust audio watermarking in the time domain [A]. EUSIPCO '98[C],1998.

[4] Lintian Q, Klara N. Non-invertible watermarking methods for MPEG encoded audio[A]. SPIE Conference on Security and Watermarking of Multimedia Contents[C], 2000,3657.

[5] Ikeda M, Takeda K, Itakura F. Audio data hiding by use of band-limited random sequences[A]. IEEE International Conference on Acoustics, Speech, and Signal Processing[C], 2001,4. 2315 - 2318.

(上接第 104 页)

集成的使用 WebAdmin 进行管理的防火墙。这种情况下,就只能使用第一种手工保存和恢复的方法。

4　防火墙的测试

防火墙在使用 WebAdmin 进行配置后,需要测试运行。对于网关固定 IP 地址的情况运行比较顺利,而对于 ADSL 连接的测试时间比较长。经过两周的稳定运行,期间包括人为地重起、ADSL 连接的断开、通过 NAT 配置网络服务器(Web 服务器和 Mail 服务器)等的测试,防火墙一直运行良好和稳定。现在已经完全代替了原先使用的德国 Astaro 防火墙来管理整个网络。

5　结束语

由于 Linux 源代码的开放性,使得许多组织和个人都按自己的兴趣和需要研究和开发基于 Linux 的操作系统,多年的研究已使得 Linux 成为一个高效、稳定和流行的操作系统。而对于建立专用的防火墙系统,则 Linux 平台是一个很好的研究和开发平台。

对于开发者来说,主要的问题有三个方面:一个是如何构建精简而浓缩、稳定而高效的集成防火墙;第二个在于如何集成和防火墙相关的服务,如 IPSec VPN 服务、动态域名解析服务(DDNS)、防病毒保护服务等,这些服务都是非常有用的网络安全应用,如果可以构建一个集成这些服务的(all-in-one)集成防火墙,而不是一个单一的防火墙,则更具有应用价值;还有一个就是对于 Linux 防火墙实现机制的内核分析,因为代码都是公开的,我们可以在此基础上实施自己的防火墙内核,以实现自己的知识产权。

参考文献

[1] Swith RW. Advanced Linux Networking[M]. Boston: Addison-Wesley,2002.

[2] 博嘉科技. Linux 防火墙技术探秘[M]. 北京:国防工业出版社,2002.

[3] Astaro AG User Manual for Astaro Security Linux 3.2[M/OL]. http://docs.astaro.org/older-versions/ASL-V3.2/asl-3.2-manual.pdf,2003 - 04 - 11.