Building Cheap, Transparent and Safe Firewall for Middle and Small Corporations Using Embedded Linux

用嵌入式Linux为中小型企业架设廉价、透明、安全的防火墙

申风兰　张会汀　方　山　(广州暨南大学电子工程系　510632)

摘要：首先本文介绍透明模式的巨大优越性，接着在对透明代理和透明模式这两上极易混淆概念作区分的基础上就透明模式的本质进行了深入分析，并找出实现它所必要的条件，充分利用Linux开放源代码资源，给出一种易行、廉价的解决方案，即基于嵌入式Linux工作于网桥模式的透明防火墙，以满足中小企业的资金有限而又需要安全、透明接入Internet以经济发展的需要。

关键词：透明模式　防火墙　网络安全　Linux

1　引言

目前国内大部分防火墙产品都实现了透明代理，而真正实现透明模式的很少，如东软的NetEye 2.0 "二合一模式"、联想网御2000 NG FW2000，价格昂贵，对于一般企业来讲难以承受；国外产品也贵得让中小企业不敢问津。

中小企业同样要安全的发展经济，如何实现透明、廉价、安全地接入Internet成为很多中小企业共同关心的话题和急需解决的问题。

2　透明模式的概念、本质以及和透明代理的异同点

透明模式关键在于透明，透明也就意味着防火墙对原有网络几近空无(网络中别的网络设备根本意识不到它的存在)，加入原有网络时，任何设置都无须改变，防火墙对用户、对原有网络设备完完全全是透明的。

透明模式其实质就是：防火墙无IP地址，即必须在没有IP的情况下工作，因而不能运行标准IP协议栈。

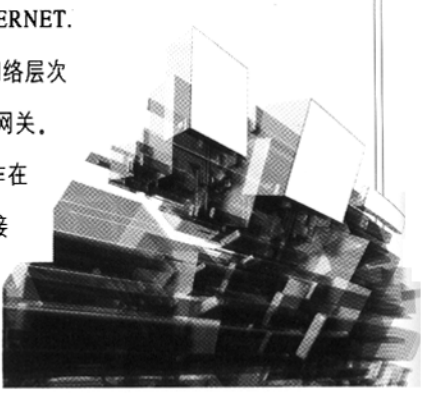
与透明模式在称呼上相似的透明代理则是代理服务对用户透明，当内部用户需要使用透明代理访问外部资源时，不需要进行设置，代理服务器会建立透明的通道让用户直接与外界通信，极大方便用户，减少配置使用过程中可能出现的问题。使用透明代理技术，可使防火墙的服务端口无法被探测到，大大提高了防火墙的安全性和抗攻击性。

二者都可以简化配置、提高系统安全性，但两只之间有着本质的区别。从功能上讲，透明代理仅仅是透明模式的一小部分，而且防火墙在非透明模式也可使用透明代理。从工作层次上讲，透明代理是在应用层起作用的，看不见IP的；透明模式则工作在IP层之下，对IP地址透明。二者易混淆，一些厂家也在此上做文章含糊其词。

3　从防火墙透明模式本质看其实现条件－方案理论基础

防火墙其实就是一个对所有过往内外网络的数据包接收，检查并合法转发、非法阻止的网络设备。

接收内外网络所有包，这就首先要求防火墙在物理上必须是一个网络互连设备，地理上成为连接两个网络的唯一通道，其次就是地址问题。我们知道Internet中数据包都是靠地址传送和接收的，而要实现透明模式，防火墙必须无IP地址，因此防火墙只有工作在数据链路层依靠物理MAC地址接收发送数据包，所以防火墙两边连接网络属于同一网段，其网络拓扑必然是最后经路由其出去连到INTERNET.



传统网络互边设备以工作的网络层次的不同分为中继器、网桥、路由器、网关。后两者工作在IP层以上；中继器工作在物理层，但有很多局限性(只能连接相同LAN，逐位复制放大传输，物理上延长LAN范围)；由前面条件限制，显然只能是选择工作在

图 1 系统模型图

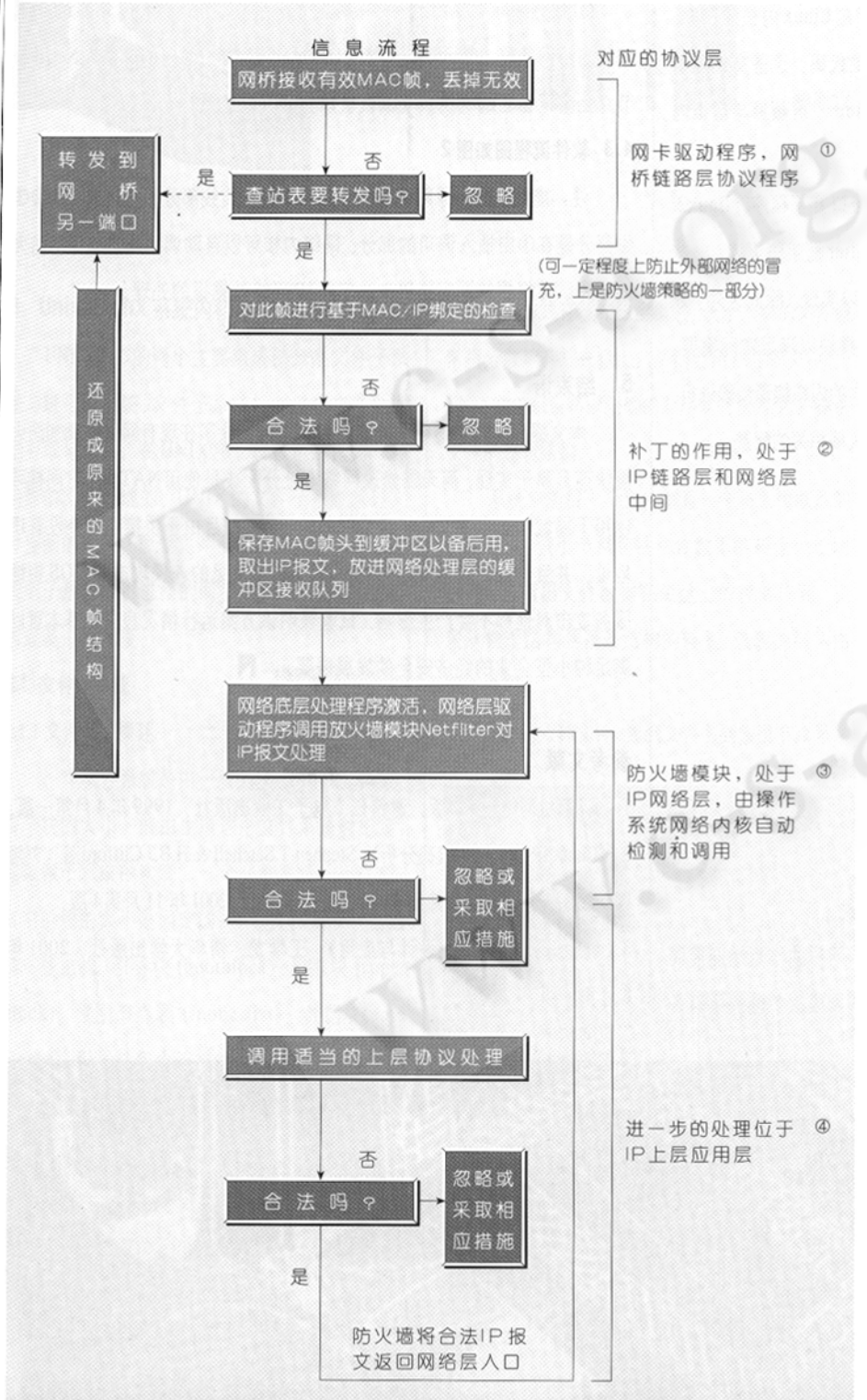


图 2 软件流程图

数据链路层的网桥模式。

还有一些非传统意义上的互连设备——堡垒主机，即两张网卡分别联接内外网络的主机。对于这些互连设备，要接收所有的包还需一定条件，或者网卡至于混杂模式或者网卡普通模式而用ARP透明代理。因为普通网卡都是只接收目的地址为本网卡地址、广播和组播地址的包。对于这些不仅原理较复杂，实现起来也麻烦，本文讲的是廉价、易行的方案，故在此只对网桥做论述。

因此最终方案就是架设基于网桥的透明防火墙，这样一来，网桥就可以接受通过的所有MAC数据帧。通过制造一个接口，使得上层能够截取由网桥转发的MAC数据帧，并对其进行解析处理，就能够达到安全目的。用Linux可以在主机上架设网桥，并且Linux还有防火墙工具netfilter，因此我们可以充分利用其源代码公开性找到一种简易、廉价的解决方案。

4 用嵌入式linux实现透明防火墙－方案具体实施

4.1 系统模型

如图1所示整个系统网络拓扑结构：

4.2 系统层次结构规划和实施步骤

(1) 从防火墙的构成层次上看，硬件平台 + 操作系统OS + Application layer 安全应用层 + Manager layer 管理层界面防火墙以实现方法分为：

硬件防火墙 专用"硬件平台 + 操作系统OS" 量身定制用专用芯片ASCII集成 价格昂贵，执行速度高

软件防火墙 通用"硬件平台 + 操作系统OS" + 纯软件实现防火功能 也很昂贵 如: CheckPoint 从降低成本出发，我们的做法：Bridge+ 补丁接口 + Netfilter

嵌入式Linux内核：引导程序、微内核、初始化进程、内存管理、文件系统、进程管理定制工业主板硬件平台

① 硬件平台：500M或更高的CPU、256M或

更高的内存、三块网卡(两块支持以太网桥，一块用于管理)、ROM用于固化嵌入式Linux,硬盘用于存储日志－－所有这些定制在工业主板上。测试的结果这样的配置可以满足一个10M以太网的速度要求，而不出现丢包现象，如果是100M或更高以太网则需要更高频率的处理器和更大的内存。

② 构造嵌入式Linux：嵌入式Linux由一个Linux内核和根据防火墙需要定制的模块组成。Linux内核的调度程序、文件系统和虚拟内存管理削弱了它的实时性，针对防火墙对此的要求，修改相应Linux内核源代码。针对虚拟内存修改Linux源代码中与体系结构无关的代码，这些文件集中在/driver/char,/ipc,/mm,/init,/kernel以及/include/Linux，屏蔽掉与虚拟内存机制有关的代码。

和防火墙相关模块有Bridge、Netfilter和二者接口补丁程序。linux2.2版本以上都支持网桥工作模式，2.4版本支持Netfilter框架防火墙。一些基本的防火墙功能都可以通过配置Iptable规则链得以实现。除此之外，还可以在Netfilter的hook节点上登记自己编写防火墙模块以满足实际需要。

③ 编译linux内核，使之工作在网桥模式。按照基本的内核编译步骤进行，只不过要关闭大多数开关，而仅仅打开一些必要于防火墙相关的配置。

CONFIG-FIREWALL=Y

CONFIG-FILTER=Y

CONFIG-IP-FIREWALL=Y

CONFIG-IP-FIREWALL-NETLINK=Y

CONFIG-IP-ROUTE-FWMARTK=Y

CONFIG-BRIDGE=Y

接下来DOWNLOAD一个叫BRCFG的UTILITY运行

Brcfg -enable 打开网桥

Ifconfig eh0 promise

Ifconfig eh1 promisc 使两块网卡都进入promisc模式

(2) 打补丁，使网桥模式和Netfilter无缝连接。网桥的作用是连接局域网，其网卡工作在混杂侦听模式，从端口接收到本网段上传输的所有各种帧，通过查看站表(路由目录)将收到的帧转发出到相应的端口去，具有学习缓冲区和生成树算法、路由判断，这些操作都由内部的端口管理软件和网桥协议实体实现。而补丁的作用就是截取网桥要转发的MAC数据帧，经预处理交给上面IP层的防火墙模块,实现在网桥化接口上使用IPTABLE进行数据过滤。整个软件流程以及补丁的作用见下面的软件流程图。

(3) 根据实际需要制定公共服务区对内部网络访问策略，外部internet访问内部网策略，来配置防火墙的Iptables规则链，必要的时候在Netfilter节点上登记自己编写防火墙的模块以完成其他必要功能。

4.3 软件流程图如图2

注：虚线部分为原网桥流程，被以下整个实线部分流程代替，即②③④部分是在①中插入调用的部分，网络内核可以自动调用用户编写的防火墙程序，并根据其返回结果来决定对IP网络数据报的处理。

5 结束语

本文提出了一种透明防火墙的解决方案，除了在现有网络中添加防火墙快速且易于实现，而无需修改网络地址分配或是使用NAT外，它同样可以用于局域网上创建受保护或受限制的子网，而且由于桥接口对外没有IP地址，并且不运行任何IP协议栈，因此很多常见的入侵攻击和DOS拒绝服务攻击对他都不会产生影响。试验表明该方案运行情况良好，基本可以满足种小型企业的经济安全的发展需要。

参考文献

1 《计算机网络》第2版，谢希仁，电子工业出版社，1999年4月第一版。

2 《Linux IP协议栈源代码分析》，Stephen T.Satchell & H.B.J Clifford著，刘隆国、翟刚、陆丽娜、辛炜 译，机械工业出版社，2001年11月第1版。

3 《嵌入式Linux系统设计与应用》，王学龙，清华大学出版社，2001年8月第一版。