DOI:10.13274/j.cnki.hdzj.2001.06.019

一种 IP 访问控制技术的实现

李　蕾　　乔佩利　　陈训逊

【摘　要】 利用动态路由、IP 隧道、有限状态自动机和捕包等技术完成对有害网站 IP 的动态封堵，并可进行源 IP 地址的统计，系统具有可靠的生效验证和系统自检手段。

【关键词】 IP 访问控制　IP 隧道　OSPF　RIP　自动机

0　引言

随着 INTERNET 的发展，如何有效地控制网络使用者访问非法网站成为一个非常重大的课题。对于大的 ISP 来说，由于网络流量巨大，而且具有多个对外出口路由器，采用远程拨号到出口路由器的控制端口上进行手工配置以便对有害 IP 地址进行封堵。但由此会产生两个比较严重的问题：(1)对路由器的拨号配置要逐台通过控制口进行，由于配置条目多，而路由器控制口的速率低，因此，对路由器的一次配置和配置检查要耗时十几分钟，这样就造成了各个被控路由器的不同步，而且手工操作出错概率大，电话拨号线路不稳定，这些因素进一步延长了配置生效时间；(2)是通过对路由器控制口进行的配置必须保存到 NVRAM 中，而路由器的 NVRAM 的重写次数是有限的，频繁的重写 NVRAM 会造成系统硬件的损伤，产生的后果不堪设想。

1　系统主体功能的设计与实现

结合 IP 隧道、动态路由技术设计和实现了如下的 IP 访问控制系统，系统物理连接示意图如图 1 所示。

配置主机 H0 和配置路由器 R0 通过 100BASE－Tx 接口直接连接，R0 通过 100BASE－Tx 接口接入校园网骨干，并且分别和出口路由器 R1、R2 和 R3 建立 IP 隧道，在 H0 上配置静态路由和 RIP 路由协议，通过 RIP 路由协议将静态路由扩散到 R0 上，R0 和 R1、R2、R3 分别启动 OSPF 路由协议并且将各自的 IP 隧道虚拟端口加入 OSPF 骨干区(area 0)中，配置 R0 上的 OSPF 路由协议，使之能够学习到 RIP 中的路由信息并扩散到 R1、R2、R3。这样在逻辑上形成了基于 OSPF 协议的路由学习网络。由于 RIP 协

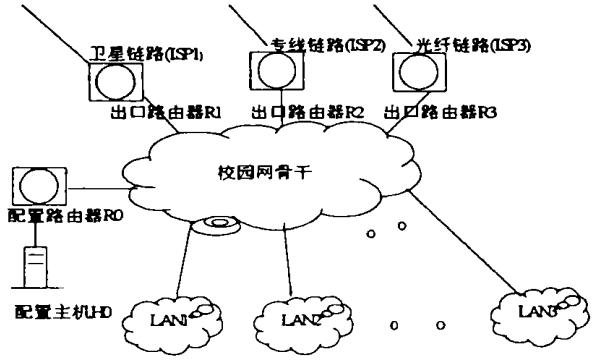

图 1　动态路由学习方式的 IP 封堵系统连接示意图

议简单并且多数的服务器操作系统中都支持，再加上 H0 和 R0 之间构成的自治系统中只有两个节点，所以采用 RIP 协议作为 H0 到 R0 的一级路由学习协议。而在 R0 和 R1、R2、R3 之间由于通过骨干网相连，RIP 协议的网络开销较大，且易产生广播风暴影响大网通讯，因此采用基于链路状态的动态路由协议 OSPF 作为 R0 到各出口路由器之间的路由学习协议。

以 204.177.92.196 为例，在主机 H0 上的网卡 fxp0 上绑定 IP 地址：ifconfig fxp0 204.177.92.196 netmask 255.255.255.255，然后在 LAN1 中的一台主机 H1 上对 204.177.92.196 进行路由跟踪，结果如下：

C:\>tracert －d 204.177.92.196

Tracing route to 204.177.92.196 over a maximum of 30 hops

1　＜10 ms　＜10 ms　＜10 ms　R1(省略实际 IP 地址)

2　＜10 ms　＜10 ms　10 ms　R0(省略实际 IP 地址)

2　＜10 ms　＜10 ms　10 ms　H0(省略实际

IP 地址)

Trace complete.

可以看到, 所有访问 204. 177. 92. 196 的包已经被路由到 H0 上去了, 这样就起到了对有害站点的封堵作用。采用该封堵技术的优点是:

高效: 由于 RIPv2 是采用触发更新的方式进行路由学习, 因此在 H0 上配置有害 IP 地址生效后, 该路由信息会立即广播给 R0, 而 R0 上的 OSPF 协议学习到该路由后会在几秒内发送给 R1、R2、R3, 所以效率非常高, 而且 R1、R2、R3 中的封堵路由信息同步时间数量级也是秒。

安全: 由于 H0 和 R0 之间是点到点连接, 所以不会存在 IP 欺骗问题, 而在 R0 和 R1、R2、R3 之间采用 IP 隧道进行虚拟内网连接并且采用隧道两端 IP 认证和口令认证, 所以安全可靠。

廉价: 只需增加一台配置路由器和一台 PC 机。

适用性广: 由于采用的协议都是 RFC 标准协议, 基本上所有的路由器都支持 OSPF 和 RIP。

使用方便: 对有害 IP 地址的所有封堵操作就是在 H0 的网卡上配置一个 IP。

2 系统辅助功能

除了上述主要功能, 系统还包括了下述辅助功能。(1)由于采用动态路由协议进行封堵路由学习, 因此, 在大型的互联网单位, 链路发生故障或出口路由器配置改变或出现协议故障时, 网管员难以及时发现其对封堵路由的影响, 所以在 H0 上设计了生效验证和协议自检程序。(2)为了对访问有害站点的 IP 进行分类统计和审计, 在 H0 上进行 IP 包捕捉, 对所有目的 IP 为有害地址的 TCP 请求连接包进行统计汇总。

这两部分程序包括生效验证和协议自检, 完成对出口路由器上封堵路由信息的检查和 OSPF 协议运行状态的检查。采用有限状态自动机技术编写 Telnet 客户端类, 完成对出口路由器的自动登录和读取路由表配置和 OSPF 协议状态, 采用多线程技术, 可以同时对多个出口路由器进行处理。

TELNET 单向数据流是一种典型的控制命令和数据混合在同一 TCP 流中的断续字符流式数据结构, 适于采用有限状态机的方式进行处理。本模块针对 TELNET 协议建立了状态机, 实现对 TELNET 数据流的过滤, 滤除数据流中的控制信息(包括 TELNET 命令串、ANSI 控制命令串等)。设置了如下 7 个状态:

STATE-TELNET-DATA	主状态, 数据状态
STATE-TELNET-CMD	TELNET 命令状态
STATE-TELNET-ANSI	ANSI 命令过滤前状态
STATE-TELNET-ANSI1	ANSI 命令过滤状态
STATE-TELNET-SUB1	子协商过滤状态
STATE-TELNET-SUB2	子协商过滤退出前状态
STATE-TELNET-WILLDO	OPTION 协商过滤状态

状态变迁图如图 2 所示: (箭头上的内容格式为"收到字符"/"所做处理")

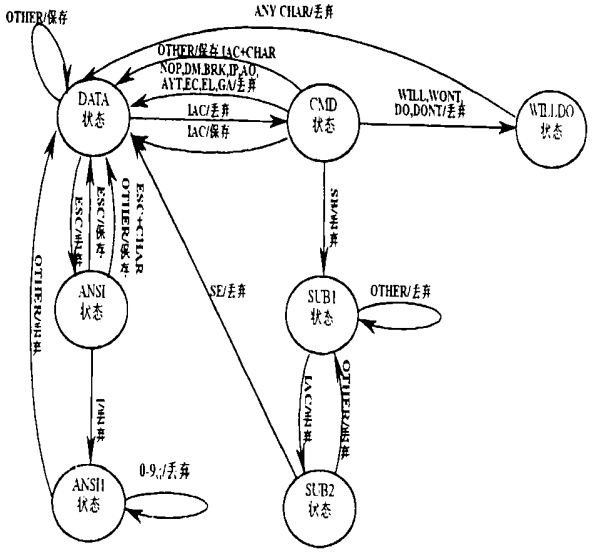

图 2 Telnet 过滤状态机

源 IP 分类统计: 本模块包括两部分程序, (1)是监听模块, 采用捕包技术监听 H0 的网卡上接收到的 IP 包, 对所有 TCP 包中, 目的 IP 地址为有害地址, 并且 TCP 头中 SYN 位置包的源目的 IP 地址记入日志数据库中。监听模块是实时联机工作的一个后台程序(daemon)。(2)是统计查询模块, 对监听模块产生的日志进行查询统计, 生成各种非类统计表格。

3 结论

动态路由、IP 隧道技术属于国际标准, 通用性强, 适于推广到全国各个互联网单位。采用的有限状态自动机和捕包技术, 技术先进, 效率高。通过几个月的实际运行, 证明采用 IP 访问控制技术能够高效、安全、方便地进行对有害网站的访问控制和审计, 实际效果良好。

作 者 简 介

李 蕾: 哈尔滨理工大学。邮编: 150080
乔佩利: 哈尔滨理工大学。邮编: 150080
陈训逊: 哈尔滨理工大学。邮编: 150080

[收稿日期: 2001—03—01 责任编辑: 李光辉]