计算机科学2002Vol. 29№. 4

Internet 防火墙透明代理技术的研究与实现

The Research and Implementation of the Technology of Transparent Proxy of the Internet Firewall

唐 寅 王蔚然

(电子科技大学计算机应用所 成都610054)

Abstract The technology of proxy applied in firewall can hide the structure of internal networks and protect internal networks of corporation from destruction of public networks. Meanwhile, it can also be used in solving the shortage of IP addresses and load balancing etc. It is allpied wildly in practice. Users can use proxy services easily by transparent proxy. Transparent proxy is usually used in current firewall production. This paper presents the technology of transparent proxy in detail and a mechanism to realize it.

Keywords Firewall, Proxy, Transparent, NAT, PAT

1 防火墙代理技术概述

代理型防火墙的基本思想仍是源于代理服务器,其目的主要是对外界屏蔽/保护内部网络的信息和结构,"切断"被保护网络与公共网络的直接联系。代理技术按照不同的标准可有多种分类方法,如按其实现机制在网络分层中所处的位置可分为链路级代理、网关级代理和应用级代理,按照用户使用的方式又可被分为应用代理和透明代理。包过滤防火墙的安全性是基于对包的 IP 地址的校验,它将所有通过的信息包中发送方 IP 地址、接收方 IP 地址、TCP/UDP 端口、TCP 链路状态等信息读出,并按照预先设定的过滤原则过滤信息包,以保证网络系统的安全。代理型防火墙则是将内部系统与外界隔离开来,从外面只能看到代理服务器而看不到任何内部资源,代理服务器接收客户请求后会检查验证其合法性,并像一台客户机一样取回所需的信息再转发给客户。

根据公安部最新安全产品检测规范(GB/T 17900-1999):网络代理服务器以各种代理服务为基础,通过它提供集中的应用服务,可以为不同的协议(Telnet、SMTP、FTP、HTTP 等)进行代理。代理服务器只允许有代理的服务通过,只有那些被认为"可信赖的"服务才允许通过防火墙,而其他所有服务都完全被封锁住。另外代理服务器不再局限于代理服务,它必须具有访问控制、应用层内容过滤、数据截获处理、安全审计等,以保证本地网络资源的安全和对外部网络访问的控制。如可以过滤 FTP 连接,拒绝使用 FTP put(放置)命令,以保证用户不能将文件写到匿名服务器;可以实施 URL 过滤,禁止对特定页面的请求等等。总之,代理型防火墙具有信息隐蔽、保证有效的认证和登录、简化过滤规则等优点。

2 透明代理技术

2.1 代理服务器

我们通常所说的代理服务实际上是指应用代理,它是通过代理服务器完成信息代理过程。代理服务器适用于 TCP/IP 网络环境,它由 HTTP、SMTP、FTP、Telnet、gopher 和 rlogin 等协议的代理服务所构成。传统的通信过程是这样的:客户端向服务器请求数据,服务器响应该请求,将数据传送给客户端。而引入代理服务器以后,这一过程变成了这样:客户端向服务器发起请求,该请求被送到代理服务器;代理服务器分析该请求,先查看自己缓存中是否有请求数据,如果有就直接传送给客户端,如果没有就代替客户端向该真实服务器发出请求,服务器响应以后,代理服务器将响应的数据传送给客户端,同时在自己的缓存中保留一份该数据的拷贝。这样,再有客户端请求相同的数据时,代理服务器就可以直接将数据传送给客户端,而不需要再向该服务器发起请求。其工作原理如图1所示。

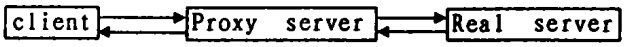

图1 代理系统工作原理

一般说来,代理服务器具有以下的功能:

1)通过缓存增加访问速度。缓存有主动缓存与被动缓存之分。所谓被动缓存,指的是代理服务器只在客户端请求数据时才将服务器返回的数据进行缓存,如果数据过期了,又有客户端请求相同数据时,代理服务器又必须重新发起新的数据请求,在将响应数据传送给客户端时又进行新的缓存。所谓主动缓存,就是代理服务器不断地检查缓存中的数据,一旦有数据过期,则代理服务器主动发起新的数据请求来更新数据。这样,当有客户端请求该数据时就会大大缩短响应时间。

2)节省 IP 地址资源。假如你只有有限的 IP 地址,但是需要提供整个组内的公网访问能力,那么你可以通过使用代理服务器提供用私有 IP 来实现访问公网。

3)隐藏内部网络结构。如果内部用户访问 Internet 都是通过代理服务器,那么代理服务器就成为进入 Internet 的唯一通道;如果你没有做反向代理,则对于 Internet 上的主机来说,整个内部网只有代理服务器是可见的,从而大大增强了网络的安全性。

4)身份认证。用来证实被认证对象是否名符其实或是否有效,防止入侵者主动攻击,如假冒、串改等。一般包括:用户—信息代理服务器的认证和代理服务器—代理服务器的认证。常见的认证方式有:加密口令、一次性口令系统、令牌认证和其他基于双因素的认证方式。

5)记录和审计。统计记录被代理服务的相关信息,提供为实施网络安全政策和审计工作所必需的系统管理接口,以方便地控制网络资源的使用,并对危害网络安全策略的网络活动给予报警。

常见的代理如 Apache、socks、squid、winGate 等,都基本具有上述的功能和特征。

2.2 透明代理原理与管理配置

透明代理应包含两方面含义:“透明”和“代理”。所谓“透明”是指用户意识不到防火墙的存在,便可完成内外网络的通讯。当内部用户需要使用透明代理访问外部资源时,用户不需要进行设置,代理服务器会建立透明的通道,让用户直接与外界通信;而“代理”则包含了前述代理服务的内容。透明技术与代理服务相结合即构成所谓“透明代理”。透明代理服务的实现可以有多种方式,CISCO 公司的 PIX-5xx 系列防火墙实现了所谓“直通式”(cut-Through)代理,它是通过对用户的代理认证后直接在网络核心层对用户数据的 TCP/UDP 包进行允许/拒绝;Linux 的透明代理是由网络核心层建立透明通道,所有需经由代理的服务先被定向到应用层对应的代理服务进程,再由该代理服务进程进行真正的代理服务;而一些公司的防火墙产品则采用将透明通道重定向到外接的应用代理服务器上来实现透明代理服务。

在实际使用中,传统代理和透明代理的配置方式有所不同。传统应用代理的配置工作一般如下:1)客户端浏览器被配置使用代理服务器的相应服务端口。2)客户端不需要配置 DNS。3)代理服务器上需要配置 DNS。4)客户端不需要配置缺省网关。

透明代理的配置工作一般如下:1)在代理服务器上启动透明代理服务。2)在客户端配置好 DNS。3)配置客户端的缺省网关为该透明代理服务器。4)客户端浏览器直接连接到 Internet。

由以上配置可以看出区别二者的一个关键是必须将透明代理服务器设为缺省网关。

3 透明代理的实现

透明代理的实现一般来说包括两部分,一是网络核心层提供 NAT/PAT (Network Address Translation/Port Address Translation),另一部分是应用层针对具体协议进行代理服务。NAT 可分为三类:静态 NAT、动态 NAT 和端口 NAT(即 PAT)。应用层的代理服务包括前面提到的 HTTP、FTP、TELNET、EMAIL 等各种网络代理服务。

从实现方式看,透明代理又可分为本地进程法和远地进程法。所谓本地进程法,即整个透明代理的实现均在一个主机上完成。下面以 HTTP 代理服务为例说明该透明代理的实现过程。如图2所示,私网用户的 IP 地址为10.0.0.10,发起连接的端口为 5080,外部 WWW 服务器的 IP 地址为 202.115.9.133,透明代理防火墙的私网接口 IP 地址为 10.0.0.1,公网接口 IP 地址为202.115.9.129。请求报文被路由到透明代理防火墙,在防火墙网络核心层 IP 分组被 NAT/PAT 截获,判断若该 IP 分组的目的端口是80,则将 IP 分组的目的地址转换为防火墙本机地址202.115.9.129,目的端口转换为8080,于是该 IP 分组被递交给在8080端口监听的 HTTP 代理进程,HTTP 代理进程与 NAT/PAT 模块通信,获取此次 HTTP 通信的真正目的地址:202.115.9.133:80,并与此真正的外部 Server 建立 TCP 连接,该请求代理过程随之实现。

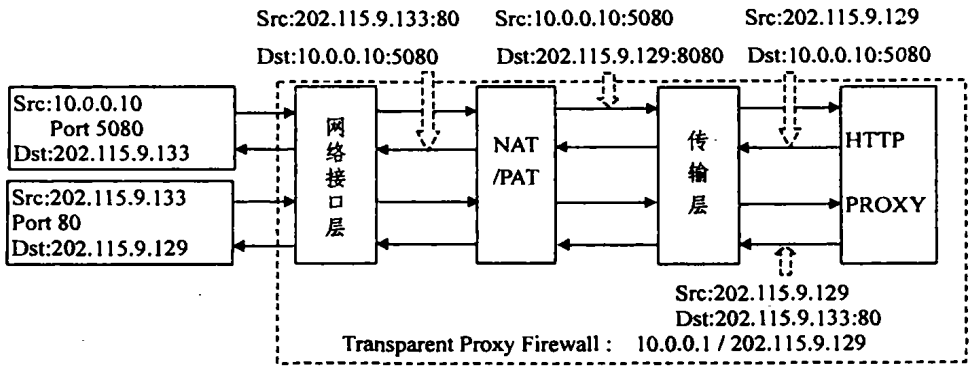

图2 透明代理防火墙工作过程

外部 Server 对私网用户的响应过程与上述过程类似。响应的 IP 分组首先被路由到 HTTP Proxy 202.115.17.129的8080端口,经 HTTP Proxy 处理后,Proxy 将响应分组转发至 10.0.0.10:5080,再由 NAT/PAT 模块将源地址改为 202.115.9.133:80,至此响应的代理过程随之实现。

所谓远地进程法,即“透明”与“代理”的实现分别在两台主机上实现。实现“透明”的主机负责建立透明通道,通向进行“代理”的主机,在“代理”主机上完成应用层的具体代理服务。其“透明”的实现与本地进程法基本一致,所不同的是应用代理的实现放在了另一台主机上。

由以上分析可以知道,无论采用何种透明代理方式,对被保护网络用户来说,他感觉到的是自己直接与真正的外部 Server 通信,整个代理过程由透明代理防火墙自动完成。

总结 代理技术的引入使企业内部网络与公网或 Internet 的通信能够被加以控制,犹如在内网与公网之间建立了一道屏障,因而又被称为代理型防火墙。它同时还可为 IP 地址紧缺以及负载均衡等问题提供解决的方法。透明代理使用户能方便地通过代理访问外部网络服务器。代理服务器发展到现在,功能得到了不断的扩充加强,除了前面我们论述到的基本功能外,又增添了应用层加密等新功能。虽然透明代理的引入为保护企业内部网络提供一个良好的解决方案。但同时我们也应看到,透明代理中的 NAT 功能如果在其实现时考虑不周全,将会影响到网络的管理和安全实施,例如若企业使用了 VPN(虚拟专用网),并用 Ipsec 进行安全认证和加密,那么如果 NAT 设计不当,将可能影响 VPN 功能正常运行。

参考文献

1 RFC 2607. Proxy Chaining and Policy Implementation in Roaming
2 Chapman D B, Zwicky E D. Building Internet Firewall
3 www.linuxforum.net/doc/file-wu.htm
4 www.cns911.com/docs/firewall/
5 squid.nlanr.net/
6 中华人民共和国国家标准. 网络代理服务器的安全技术要求 GB/T 17900--1999