Internet 防火墙和服务质量

何刚　吴志美　（中国科学院软件研究所 100080）

摘要：如何防止用户私有数据被窃取，如何防止非法用户入侵，是 Internet 用户很关心的问题。本文简单介绍了 Internet 信息安全的一些概念，并介绍防火墙和服务质量的概念。最后阐述了一个 PC 机网关防火墙系统的实现。

关键词：Internet　Intranet　防火墙　服务质量

一、概述

1988 年，莫里斯病毒攻击了 6000 多台计算机，使整个网络处于瘫痪状态，造成了巨大的损失，计算机网络的安全问题引起人们广泛注意。随着 Internet 在全球的普及，计算机网络已经进入了人们的工作和生活，成为人们生活中的必不可少的东西。Internet 网络的安全问题，是 Internet 网络应用首先要解决的问题。

Internet 网络安全性主要有两个方面的内容：

1. 保证用户数据的私有性，防止非法窃取。

2. 限制用户（或应用程序）的访问权限，防止非法用户（或应用程序）的入侵。

目前，Internet 上的资源大多数都是可以共享的。随着 Internet 的发展，尤其是 Internet 在商业上的应用，用户私有数据逐渐增多，保护用户利益，防止非授权用户的非法窃取，防止非法用户入侵，是网络安全的主要功能。现在的计算机技术，例如端到端的加密、解密，密钥的管理算法等等，都已经能够保障用户端到端的安全传输。

可是由于用户的数量太大，使得为每一个用户都维持一个很好的安全保障系统比较困难，对于一个用户集团，希望用户子网内部的成员进入 Internet 网络时，受到某种约束，同时也能够保护资源不会流失，于是实现中提出了防火墙的概念，在用户子网中将所有用户安全控制交给一个独立的计算机来进行。

网络服务者所提供的服务多种多样，将服务分成各种类别，使用户能够访问到他们被允许访问的资源，同时能够防止用户接触到他们没有被授权访问的资源，实现特定的网络服务质量。

二、防火墙（Firewall）

防火墙在 Internet 的体系结构中可以用来隔离一个用户子网。用户子网中的所有节点都可以受到防火墙的约束和安全保证。

1. 防火墙的种类

防火墙可以在不同的网络层次上实现，通常有以下两种：

(1) 应用程序级防火墙。应用程序级防火墙可以用下图来说明。

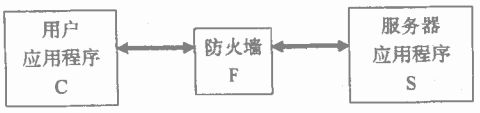

图 1　应用程序级防火墙

当用户应用程序 C 需要向服务器应用程序 S 提出请求时，C 不能够直接建立和 S 的直接传输层的联接，而是必须和防火墙 F 首先建立传输层的联接。当 F 认证了 C 的请求时，F 建立和 S 之间的传输层联接，然后 F 传递 C 提出的请求给 S，同时将 S 的应答传递给 C。

·优点

由于防火墙建立在应用程序级上，所有 IP 包都必须通过 F 的检查，伪造的 IP 包将不被用户应用程序接受，可以起到更好的防范作用。

·缺点

同样由于防火墙建立在应用程序上，防火墙就必须对每一种应用程序进行编程，使得这种防火墙在实际应用必须针对特定的应用背景，作特定的防火墙。

(2) IP 级防火墙。IP 级防火墙建立在 IP 包的基础上，通常设在子网的出口处，其结构如图 2 所示：

用户的应用程序 IP 层 C 向服务器应用程序 IP 层 S 发送一个 IP 包，要经过如下的过程：

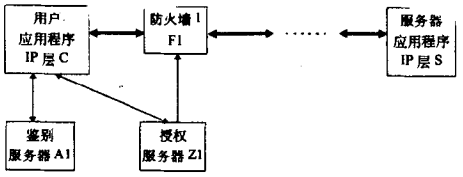

图 2　IP级防火墙

①C发向S的IP包到达防火墙F1；

②如果F1中没有有关C请求S的信息，则向C发出"需要认证"请求，否则将IP包传送下去；

③C收到"需要认证"请求时，首先向鉴别服务器A1认证自己；

④A1向C返回一个认证消息。A1可以鉴别出所有在"网络黑名单"上的非法用户，从而拒绝给此用户返回认证消息；

⑤C利用A1的认证消息，发送消息给授权服务器Z1，告诉Z1自己要发送IP包给S，请求Z1打开F1上通往S的通路；

⑥Z1检查C的请求，如果合理，就通知F1，允许C发往S的IP包通过F1，C重发IP包给S，此时F1允许C请求S，将IP包往后传递；

通过防火墙F1之后，IP包继续向前传送。每一级子网都可以有防火墙，IP包从C到达S要经过多次的安全控制，同样，S对C的请求的应答也要经过多次的安全控制才能够返回。

·优点

IP层的防火墙不用对每一种应用程序来进行编程，仅仅针对IP包来进行处理，因此应用中的防火墙大多数是IP层的防火墙。

·缺点

IP层的防火墙由于传递的是IP包，使得伪造IP包发送有可能通过防火墙，因此IP层的防火墙必须通过一定的手段来防止这种伪造的IP包。

2.防火墙在Internet中的位置

如图3所示，防火墙就象一个过滤器一样，过滤所有用户子网和Internet网络的信息交换，使得非法的入侵和信息窃取都被过滤掉。

对于防火墙来说，用户子网中的所有节点都是一样的，它向所有的节点通过相同的约束机制和安全保障措施。因此，用户子网中原来安全保障措施比较弱的节点就可以躲在防火墙后面，享有防火墙带来的安全保护，而对那些本来安全保障措施比较强的节点来说，防火墙可能根本提供不了新的安全保障，反而造成了许多的不便之处。同样，对于那些用户本来希望自由访问Internet的节点，也不得不受到防火墙的约束，对于这些节点来说，防火墙带来的不是好处，而是负担。

图 3　防火墙在Internet中的位置

防火墙是一个比较复杂的系统，防火墙本身也有许多问题要解决，如防火墙的效率，非对称寻径等等。市场上已有的防火墙大多都是防火墙的一个子集，我们所作的5wqos软件也是其中之一。

三、网络安全服务质量(Secure Qualities - Of - Services Forwarding)

当Internet支持一些特殊的服务质量要求时，会产生一些新的安全问题。用户提出一些特殊的服务要求，安全服务质量保证机制将安全检查设在网关上，把服务要求分成各种类别，然后查看用户的信息，确认该用户是否有权得到此类服务，如果有权，则把服务要求传递下去，如果没有权力，则将服务要求拒绝。

安全服务质量保证机制通常建立在IP层的基础之上。每一个IP包都携带安全认证信息显然是不合实际的，因此安全服务质量保证机制分成两个阶段：

1.设置阶段

设置的实现可以是动态的，应用程序可以通过网络进行修改；也可以是手动修改，用户通过修改网关的设置信息，完成安全服务质量保证的设置。通过设置，对每一个用户提出的各类要求，都形成一个确定的答案：允许或者拒绝。当用户的请求到达网关时，网关对要求进行分类，然后查看改用户的信息，将合法的请求传递下去。

2.分类阶段

分类阶段的主要功能就是将到达网关的IP进行分类。每一个IP包都携带着用于分类的信息，这部分信息通常被称为低层ID(Low - level ID, LLID)，分类阶段要完成LLID到各种要求的映射。这样通过LLID就可以

达到安全认证的目的。

目前，安全服务质量保证的分类通常是在现有的 IP 包中，对某些域进行的，如 IP 包的源地址、目的地址、端口号、高层协议类型等等。我们设计的软件 5WQOS 就是建立在这些域的基础上的安全服务质量保证。

四、Secure QOS 的实现－5WQOS 软件

我们研究室在最初使用 Internet 的时候，忽略了网络的安全功能，使得网络的运行出现了许多的隐患，这些隐患在网络计费时尤其明显。其中包括：

1.盗用其他用户的 IP 地址

由于计费是根据 IP 地址进行的，而子网 IP 地址的分配是协商进行的，以太网对于 IP 地址分配没有强制的措施，使得某些用户有可能在其他用户不在网络上的时候，冒用同子网中其他用户的 IP 地址登录入网，使用其他用户的 IP 地址来运行 Internet 软件。

2.非法使用空闲的 IP 地址

网络中有一些 IP 地址暂时没有分配，而子网中所有的计算机都可以以一个符合子网掩码的 IP 地址登录进入网络使用 Internet 网络，这样造成在空闲的 IP 地址上，有人使用 Internet 网络，却无人付帐。

3.大量传输服务没有限制

用户可以使用的软件有 Ftp、WWW 访问，电子邮件、BBS 等等。有些软件网络传输量少(如电子邮件)，而有些软件网络传输量很大(如 WWW 访问)。滥用网络传输量很大的软件，会造成网络的拥挤。

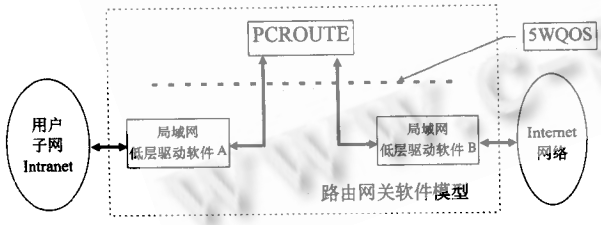

图 4　5WQOS 在网关软件中的位置

5WQOS 防火墙软件建立在已有的路由网关基础之上，省略了认证和授权的过程，采用静态的网关配置，将通过网关的 IP 包进行过滤分类，达到特定的网络服务质量，从而解决上述的问题。5WQOS 运行后所处的位置如图 4 所示。

在设置阶段，手动修改网关的设置，通过设置，5WQOS 可以将用户发往 Internet 网络的数据报进行分类。

有关 5wqos 软件的进一步信息请看：

http://isdn.iscas.ac.cn 之“科研成果”之“PC 机网关防火墙”

在分类阶段，5WQOS 对于数据报的分类采用如下过程：

(1)数据报由用户子网发到局域网低层驱动软件 A，A 将数据报交给 5WQOS。

(2)5WQOS 检测数据报的源 IP 地址和源以太网地址，如果与设置的 IP－以太网地址对相符合，则进行下一步，否则将此数据报扔掉。

(3)5WQOS 检测与源 IP 地址相对应的状态，如果该 IP 地址为合法地址，则进行下一步，否则该 IP 地址为非法 IP 地址(即该用户没有向网络管理员声明使用该 IP 地址)，5WQOS 将此数据报扔掉。

(4)5WQOS 检测与源 IP 地址相对应的权限 P，并检测目的 IP 地址，如果此数据报发往国外或者国内其他网络(即非中科院子网，目的 IP 地址不是 159.226.*.*)，当且仅当权限允许的情况下进行下一步，否则将此数据报扔掉。

(5)5WQOS 检测数据报的协议端口号，识别出应用程序类型(仅在有些情况下适用，因为协议端口号的分配有时是动态的)，将符合权限 P 的数据报传递给 PCROUTE，否则将此数据报扔掉。

对于从外部 Internet 网络发往用户子网的数据报，5WQOS 软件可以做类似的过滤，不过 Internet 上的软件大多采用面向联接的传输层协议，只要过滤一个方向的传输就已经足够了。

参考文献

[1] rfc1636, Security in the Internet Architecture, Feb., 1994

[2] 《新编 TCP/IP 协议与计算机网络互联技术》，海洋出版社，1991

[3] 《Novell 指南 NetWare 局域网分析》，电子工业出版社，1994

(来稿时间：1996 年 10 月)