谈防火墙系统的设计

姜力争 （中国建设银行山东省分行 250000）

一、防火墙系统设计

通常需要设置防火墙的地方就是 INTERNET 和 INTRANET 之间，当我们建立一个 INTERNET 防火墙时，首先必须确定它的基础结构。有两种类型的防火墙结构：即单层结构与多层结构。

在单层结构中，一台网络主机担负防火墙的所有功能并且连接到它所控制的每个网络。当只有两段网络需要互连，并且成本是主要的考虑因素时，通常选择单层结构的防火墙系统。它的优点是所有的防火墙功能都集中在一台主机上，在防火墙的功能相对简单并且仅有为数不多的网络需要互连时，对于操作和维护具有较高的性能价格比。单层结构的最大缺点是对于防火墙功能实现上的缺点和配置上发生错误的脆弱性，依靠这种类型的防火墙系统，某种设计上的的缺点或者错误可能导致网络被侵入。

在多层结构中，防火墙的功能被分布在几台主机上，通常把几台防火墙主机连续地连接起来，在它们中间是 DMZ 网络。这种结构较难设计与操作，但是通过变换设计防御策略能够提供更高的安全性。尽管成本较高，建议在不同的防火墙主机上采用不同的技术，以免同样的设计缺点和配置错误出现在各个主机上。利用这种结构的通常的设计是 INTERNET 上的防火墙：包括两台防火墙主机和一个 DMZ 网络。

二、防火墙系统功能选择

确定了基本结构后（主机数目、连接方法、每台主机上完成的任务），下一步是选择在这些主机上要实现的防火墙功能。通常的两类防火墙功能是包过滤和应用代理。这些功能可以分别使用或合并使用，可以在同一台或不同的主机上实现。在最近的产品中，包过滤防火墙产品已经具备了应用代理的某些功能，称为 stateful inspection 包过滤。

有很好的理由既使用包过滤功能又使用应用代理功能。一些服务，如 SMTP，HTTP，或 NNTP 通过包过滤控制通常就比较安全，而另外一些服务，如 DNS、FTP 则要求通常只有通过代理服务才能提供的更复杂的控制。包过滤运行得较快，而应用代理则一般运行较慢。为防止出现复杂的控制需要以至于使性能差到不能忍受程度的代理服务，可以选择 stateful inspection 包过滤。对于每一个防火墙系统的设计，应该尽可能多地选择这

些不同的功能(如包过滤、代理服务、stateful inspection),在合适的地方应用它们。

在今天的防火墙产品中,可用的功能包括:包过滤、应用代理、stateful inspection 包过滤。这些功能中的每一种都隐含着一类可供选择的运行平台。防火墙的运行平台指的是执行防火墙功能的特殊硬件平台及操作系统的组合。对于某些设计,平台的选择和功能的选择是相互独立的,而在其他场合,对其中的一项作出选择意味着另一种必须作出相应的选择。下面将要说明这些功能以及与之对应的可供选择的运行平台。

1.包过滤

因为在安全性需求和安全策略不同的网络中通常有路由器,因此,在路由器上实现包过滤功能使得只有经过许可的数据通过网络是可行的。通过在现存的路由设备中附加包过滤功能使路由器具有防火墙功能性能是一种性价比较好的作法。顾名思义,包过滤器指的是在路由的过程中对包进行过滤。过滤算法通常依据包头的内容(如源地址、目的地址、协议、端口号)。

总的来说,包过滤路由器提供了最高性能的防火墙机制。但由于它们是在较低层次上进行配置,配置起来比较难,要求了解协议的细节。

包过滤通常在两类平台上实现:

通用的计算机作为路由器使用。优点是功能扩展没有限制。缺点是中等性能,接口数量少,操作系统具有易损性。

专用目的的路由器。优点是性能高,接口数量多。缺点是功能不易扩展,可能需要更多的内存。

专用目的的路由器厂家已经在它们的路由器产品中增加包过滤器从而提供有限的访问控制以便用较少的设计改动满足用户需求。然而,他们毕竟只是路由器厂商而非安全产品厂商,所以,当他们的设计需要在路由功能和安全功能之间进行选择时,他们选择路由功能。在这个意义上,性能是路由性能而非防火墙性能,所以在进行路由器设计时,路由性能总是第一优先级。另外在路由器中增加包过滤功能,通常对路由功能具有负作用,进而影响网络的性能。另外可能需要更多的内存。

2.应用代理

一个应用代理是两段网络之间的防火墙系统上运行的应用程序。运行应用代理的主机不必是路由器。当一个客户程序通过代理建立一个到目的服务的连接时,它首先建立一个直接到代理服务器程序的连接。客户程序然后同代理服务器进行协商,使代理服务器以该客户的身份在代理服务器和目的服务之间建立连接。如果成功,就存在两条连接,一条从客户到代理之间,一条从代理到目的服务之间。一旦建立完成后,代理就在客户和目的服务之间双向接收并转发数据。代理决定所有的连接建立和数据转发;主机上所有的路由功能和代理无关。

与包过滤功能类似,应用代理可以运行在专用目的计算机上,也可运行在通用计算机上。总的来说,应用代理比包过滤路由器慢。但安全性却比包过滤路由器高。由于设计缺点或者它们所依赖的操作系统在实现路由功能时的疏忽,包过滤路由器始终受到限制。因为包过滤功能是后来加到路由功能上的,它们不能修正或弥补某些路由功能的缺点。为了作出更复杂的包过滤和访问控制的决策,应用代理要求较多的计算机资源和昂贵的计算机。例如一个运行在 UNIX 系统上的防火墙需要支持 200 个并发 HTTP 会话,主机必须能够以合理的运行性能支持 200 个 HTTP 代理进程。增加 100 个 FTP 会话,25 个 SMTP 会话,一些 LDAP 会话和一些 DNS 交易,这时的主机需要支持 500 到 1000 个代理进程。一些代理通过线程完成(可以显著地减少资源需求),但资源需求仍然很高。

3.stateful inspection 或动态包过滤

我们用 stateful inspection 或动态包过滤来指路由器上功能更强的包过滤。普通包过滤的过滤策略仅依据每个包的包头,而不考虑以前的包。stateful inspection 包过滤允许根据包数据内容的复杂组合和由前面的包建立起来的上下文关系计算过滤结果。同普通包过滤类似,stateful inspection 是对路由功能的附加,所以运行 stateful inspection 功能的主机必须是路由器。

采用 stateful inspection 的主要原因是基于性能和安全性的平衡比较。作为在路由上附加的 stateful inspection 比代理提供了更好的性能。它又比简单的包过滤提高了防火墙安全水平。象应用代理一样,它可以描述更复杂的访问控制条件,又类似于普通包过滤,stateful inspection 依靠高质量的底层路由系统。

三、选择防火墙的拓扑结构

以上描述了防火墙的功能,可以有多种方式组合使用这些功能。下面将论述经常采用的几种结构,合理选择不同的结构以便于提高防火墙系统的效率。

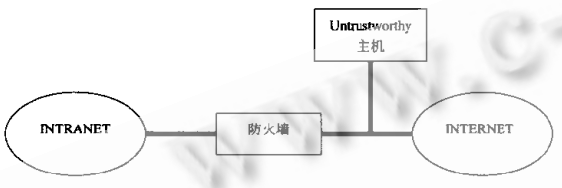
1.基础边界防火墙

这是所有防火墙系统的入门点。一个基础防火墙是单独的一台主机,连接企业内部网络与一些不可靠的网

络,通常是 INTERNET。在这种配置中,单台主机提供了所有防火墙功能。

2. Untrustworthy 主机

在基础边界防火墙中,增加一台主机位于防火墙不能保护的不可靠网络上。对这台主机进行尽可能安全的配置与管理。防火墙被配置成所有的进入和发出信息都通过这台主机。这台主机被称为 Untrustworthy 主机,因为它不被防火墙保护,所以可靠网络上的主机仅能够有限度地信任它。



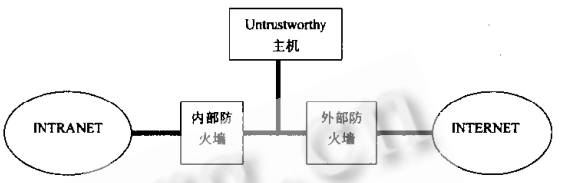
3. DMZ 网络

在 DMZ 网络中,不可靠主机被放到防火墙内部,但它自己确作为单独的一个网络(这时防火墙连接 3 段网络)。这种方法提高了安全性、可靠性和不可靠主机的可用性,但不能提高其他内部主机对它的信任程度。其他的 Untrustworty 主机为了完成诸如公共的 WEB 站点或 FTP 服务器任务,可以容易地放在 DMZ 区,建立一个公共服务网络。

4. 双防火墙

通过增加一台防火墙主机可以将企业的内部网络与不可靠网络彻底隔离。把不可靠网络连接到一台防火墙上,企业内部网络连接到另外一台防火墙上,DMZ 位居其中,内部网络与 INTERNET 之间的通信必须跨越两个防火墙和 DMZ。

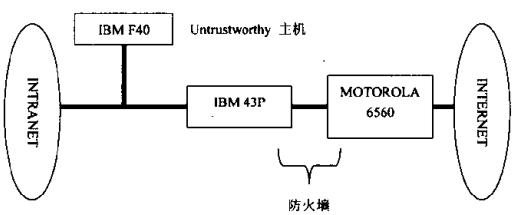
在每一种结构中,防火墙位于网络的边界用于访问控制,主要为了保护内部网络与不可靠网络的连接。完全位于网络内部的防火墙,也可以提供网络上不同子网间的相互保护。内部不同子网间的访问控制与内部网和 INTERNET 之间的访问控制没有区别,所以所有的上述结构也可以用于内部网络的防火墙。



在每一种结构中,防火墙位于网络的边界用于访问控制,主要为了保护内部网络与不可靠网络的连接。完全位于网络内部的防火墙也可以提供网络上不同子网间的相互保护。内部不同子网间的访问控制与内部网和 INTERNET 之间的访问控制没有区别,所以所有的上述结构也可以用于内部网络的防火墙。

四、应用实例

如图所示:在一个实际的企业内部网项目中,整个网络有 3 个安全区域:内部网部分,INTERNET 部分和 DMZ 区。其内部网部分覆盖全国范围,采用 IBM RISC/6000 系统以及 IBM NETFINITY PC 服务器作为整个企业网的硬件平台,LOTUS DOMINO/NOTES 群件作为软件平台。在总部设置 DMZ 区,一台 IBM RISC/6000 F40 作为外部的 WEB 服务器和外部的 DNS 域名服务系统。一台 IBM RISC/6000 43P 运行 IBM FIREWALL 软件作为防火墙,完成以下任务:通过对防火墙的设置实现外部用户对内部网访问的安全存取控制和内部用户对 INTERNET 访问的安全存取控制;通过对防火墙上相关代理服务的设置实现内部用户内 INTERNET 访问的管理。一部分包过滤功能在 Motorola 路由器上完成。



(来稿时间:1999 年 7 月)