防火墙技术分析与应用

张灵欣 方祁 (北方交通大学计算机系 100044)

摘要:计算机网络技术的发展促进了 Internet 的发展,但是 Internet 上的安全问题越来越受到人们的重视。本文深入介绍了网络安全技术——防火墙技术的概念和主要分类,为建设安全系统提供了理论依据。

关键词:网络安全 防火墙 堡垒主机

随着 Internet 以及网络技术的飞速发展,人们越来越体会到 Internet 的重要性和优越性,更多的组织和网络连入 Internet,使工作站能享受全球服务。但当人们通过 Internet/ Intranet 传递和获得经济、政治、军事等信息时,总是担心会不会有人窃取自己的信息资源,同时也在担心会不会有人在破坏自己的信息资源,网络安全技术逐渐成为研究的热点。

一、什么是"网络安全"?

在计算机安全性和计算机所能提供功能之间的平衡性是很重要的。在很多情况下,最安全的计算机往往功能是最简单的,能提供多种服务的则是最不安全的。

网络上的计算机由于开放性很强,它与外界的联系通道经常会被攻击。我们把这些攻击概括为两类:

1.被动攻击:窃听或跟踪网络上的相互通信,很难被发现。在被动攻击中,作案者想 方设法地去获取网络上的信息。这样的攻击可能是基于网络的(跟踪通路中的连接),或是基于系统的(用一个窃取数据的 Trojan Horse 来替代一个系统的组件)。

2.主动攻击:作案者一直想接管你的计算机,直接对你的计算机进行操作。尽管你可以确定自己的计算机没有被危害,但并不能保证另一端的计算机是否安全。在现实中,或者让一些计算机在你的信任范围内,或者你根本不去使用 Internet 网络。

主动攻击有几种:

(1) 系统访问权的获取,攻击者的目标是利用安全漏洞去获取对一个系统或客户端的访问权和控制权;

(2) 诱骗,攻击者假装是一个你所信任的系统或客户,骗取你的机密信息

(3) 对密码的攻击,攻击者努力地去获得密码来对数据进行解密

Internet 上的多点到多点的连接性会引起许多的问题。我们要保护自己的私有网络与 Internet 的接口,而且也要考虑传输通过 Internet 的数据的验证和加密,从而保护自己的私有数据,以及保护来自外部对自己私有网络的内部主机的任意访问。

限制私有网络与 Internet 的接口数量。如果你只有一个唯一的通道,你就会对私有网络的流出和流进有很好的控制,这是典型的防火墙连接方式。

二、防火墙的概念

防火墙是在两个网络之间实施访问控制策略的一个系统,通过在网络边界建立起来的相应网络监控系统来隔离内部和外部网络,阻挡外部网络的侵入。

它对两个或两个网络之间传输的数据或建立的连接按照一定的安全策略进行检查,来决定网络之间的通信是否被允许,被保护的网络成为安全网络,另一个网络被成为不安全网络。

一个好的防火墙应具有三个方面的特性:

(1) 在安全网络和不安全网络之间传输的数据一定要通过防火墙

(2) 只有被授权的合法数据即防火墙系统中安全策略允许的数据可以通过防火墙

(3) 防火墙本身不受各种攻击的影响

三、防火墙基本技术

在讨论各种防火墙技术之前,我们明确堡垒主机的概念。堡垒主机是对网络安全至关重要的防火墙主机,既一个机构中网络安全的中心主机,在这个机器上可以运行代理服务程序及其他应用程序,对来自安全网络和不安全网络的访问来说,必须要先访问到堡垒主机,进行安全验证。对堡垒主机必须进行完善的防御,对软件和系统应定期进行检查,查看系统日志文件,以便发现潜在的安全性问题。

1. IP 包过滤

如图 1 所示:

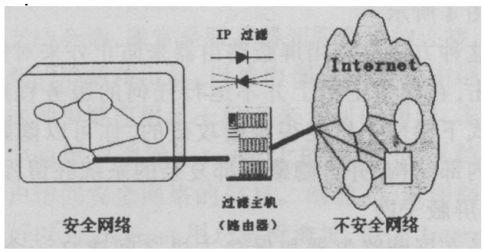

图 1　IP 包过滤结构示意图

一种最常用的策略是在私有网络与 Internet 之间插入一个路由器，如图 1 所示。这个路由器被称做屏蔽路由器，它检查通过路由器的所有的数据，筛除不符合要求的数据包。具体做法是检查所传输的数据包的源、目的 IP 地址、传送方向和 TCP/UDP 端口号等参数，并与用户预制的访问控制表进行比较，从而将符合条件的数据包转发到相应的目的地址端口，其余的数据包则被阻塞，从数据流中删除。这样你就可以阻止对网络内部主机和端口的访问，而且也可以防止内部的主机对 Internet 的访问。

另一种是在私有网络与 Internet 之间插入一个具有过滤功能的计算机，如图 1 所示。这台计算机上过滤功能与网关功能相结合，因此要求有两个或两个以上的接口，每个接口都在相应的网络上。其中之一是在安全网络内，另外的一个(或多个)在不安全网络内，过滤规则就是在安全接口和不安全接口之间起作用。设置的过滤规则存入相应的过滤文件中，当一个数据包到达过滤主机时，按顺序与过滤文件中的每一行相比较，直到有相匹配的某一行为止。如果你想指定某种服务可以通过，你应该在过滤主机上设定，但是在计算机上加的控制越多，你自己实际所有的控制权越少。

·包过滤只是将不合条件的数据包删除掉，而不具备登录、报告功能，因此不利于系统的审核管理，防火墙软件产品则可祢补这一缺陷。

·包过滤规则的设置不够灵活，而且一个包过滤规则是否完全严密及必要是很难判定的，因而在安全性要求较高的场合，通常还配合使用其他的技术来加强安全性。

2. **代理服务器和 SOCKS 服务器**

包过滤可以限制安全网络和不安全网络之间的一定数量的连接，但是利用某些被允许的连接，网络黑客就有机会来攻击安全网络。在防火墙处断开连接是一个好办法，这可以隐藏内部网络主机的地址和名字的信息；同时设置一个攻击者必须逾越的障碍，进行验证等安全措施。

与包过滤不同的是，使用这类防火墙时，外部网络和内部网络之间并不存在直接连接，即使防火墙发生了问题，外部网络也无法与内部网络进行连接。在防火墙上断开连接，有两种措施，分述如下：

(1)代理服务器：对客户端来说是一个服务器，而对服务器来说是客户端；

对于安全网络内部的用户，访问外部信息非常好的方法是使用代理服务器－－运行在安全网络内部提供对外服务的服务器。代理服务器上运行代理服务程序，接受来自代理客户的服务请求，对该用户的身份进行验证，如果是授权的用户，代理服务器与目标主机进行第二步连接，这样客户端与目的主机通过代理服务器建立了连接。如图 2 所示：

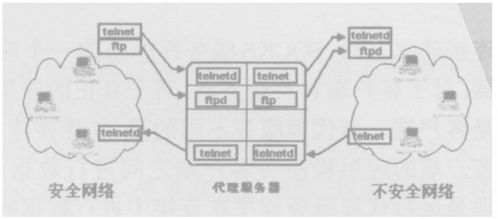

图 2　代理防火墙结构示意图

在防火墙上可以使用的代理服务是 Telnet 和 FTP，不安全网络使用 FTP 的方法是先从不安全网络 Telnet 进入安全网络，然后从安全网络内部使用 FTP。这就限制了外部用户从安全网络外直接获得信息。

代理服务器的主要优点是在客户端不必运行客户端程序，因此，建立了防火墙之后，在防火墙上注册的用户可以很方便地去访问另一个网络。当你通过代理服务器进行连接时，TCP/IP 的连接在防火墙被中断，减轻了网络的威胁；用 USER ID 及口令验证身份时，只要你的口令保证安全，防火墙也会很安全；日志的管理和审计功能，使网络更安全。

连接的建立有两个阶段，一个是从客户端到防火墙，另一个是从防火墙到目的端，这会耽误一些时间，影响系统的性能；同时代理有其专用性，提供的服务和应用是有限的。

(2) SOCKS：执行同代理服务器相同的功能，只是 SOCKS 在网络的会话层起作用，而不是在应用层。

SOCKS 是一个代理服务的标准，在防火墙上的执行服务程序。安全网络中想使用 SOCKS 的用户首先连接

到防火墙上一个特殊的端口，缺省为 1080，这个连接告诉 SOCKS 系统程序真正的 IP 地址和端口号，服务程序检查用户是否被授权，如果是的话，再进行连向真正地址和端口的第二步连接，然后把信息在这两个连接之间进行传送。如图 3 所示：

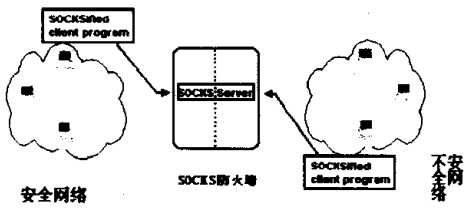

图 3　SOCKS 防火墙结构示意图

连接建立之后，SOCKS 服务程序扮演一个应用级的路由器，对于客户端它是服务器，对于真正的应用服务器来说是客户端。与代理服务不同的是，在连接建立之后，通过客户端的应用程序与客户端之间进行数据的传递，而代理是运行代理服务程序在连接中进行数据的传递。

对于向外的连接，SOCKS 与代理服务器有相同的目标，那就是中断会话，验证用户的身份，为用户提供一个安全的“出访门户“。在网关上有了 SOCKS 服务器，也需要对过滤规则进行必要的修改，端口 1080 需要在过滤规则中进行保护。

相比较而言，SOCKS 可能比代理服务器更为安全些。

3. 双宿网关

把屏蔽过滤和堡垒主机结合在一起是一个很好的方法，用这种方式，你可以利用过滤的功能保护双宿网关。同时，在安全网络之外的服务器与安全网络内部相联系时，可以用代理服务器来减少安全网络内部的暴露性。但是，这种配置会使防火墙的主机很复杂，因此如果一个攻击者进入网络，就会花费很长时间去检查出来。

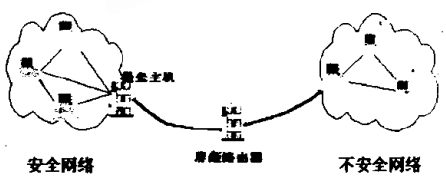

图 4　屏蔽路由器与堡垒主机结合方式

(1)屏蔽路由器结合堡垒主机

如图 4 所示：

在这种方法中利用屏蔽路由器来防止外来对堡垒主机的攻击，在堡垒主机上并不运行任何的服务程序。在这种方式下堡垒主机是很难被攻破的，你可以隐藏私有网络的内部结构，并且隐藏内部复杂的系统驻留程序 。

(2)屏蔽子网

这是在屏蔽路由器和堡垒主机之间建立一个子网，提供应用服务。如果在安全策略中要有一个能够提供广泛的服务的主机(例如 Web 服务器)，但仍然需要很强的保护，这种情况下经常采用这种方式。屏蔽路由器对服务提供适当的保护，这个网络也可以由两个屏蔽路由器和一个以上的堡垒主机构成(内部的堡垒主机可以结合对内部网络的屏蔽功能，实现代理和过滤两种防火墙功能)。

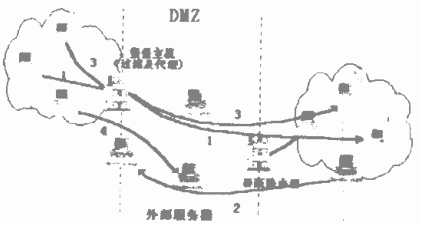

图 5　DMZ 结构示意图

屏蔽子网的典型方式是 DMZ(demilitarized zone)。其结构如图 5 所示：

外部的屏蔽路由器仅允许从不安全网络对子网中信息的访问，而不允许对安全网络内部的访问。内部的屏蔽路由器(或结合过滤功能的堡垒主机)仅允许安全网络对子网中信息的访问，而不允许子网中的服务器对安全网络内部的访问。图中的数字和箭头表示了几种不同类型的会话，这些功能是防火墙应当实现的：

①从安全网络中的客户端到 Internet 中的服务器的会话访问。这个会话在内部防火墙以代理(或 SOCKS)的方式被中断了，代理程序在外部屏蔽路由器的允许下建立会话的第二个连接。这种方式的优点是在代理服务器你可以控制用户对 Internet 的访问，与目标建立的会话连接是从防火墙开始的。这就是说网络黑客不能透析安全网络的内部结构。

②从 Internet 客户端对子网中信息服务器访问的会话连接，在外部屏蔽路由器得到允许，但被内部的防火墙

挡住。这就是说，外部的用户仅可以访问你所允许的、处于 DMZ 子网中的资源。

③支持会话，通常是服务器到服务器的连接，被允许通过外部的屏蔽路由器，但被内部防火墙的中继应用所中断。这种中继应用象一种有来无回的阀门，主要向安全网络中的用户透漏 Internet 上的信息，但阻挡不安全网络用户访问安全网络的信息。例如，安全网络中的一个用户可以为 Internet 用户解析地址，但为 Internet 用户提供的地址映射信息仅提供给 DMZ 中的服务器。

④理想的情况是内部的屏蔽路由器可以阻挡所有的会话连接，因此所有的连接被中断然后被代理程序或中继应用延续连接过程。在安全网络的主机和 DMZ 的服务器之间会有一些管理和商业信息的连接，内部防火墙的设计允许这些连接的通过。当你考虑这种方式时，资金是主要的考虑因素，因为由于完整性的原则，设计中的每一个构件都要求机器的配置很高。

4. 安全 IP 通道

如图 6 所示：

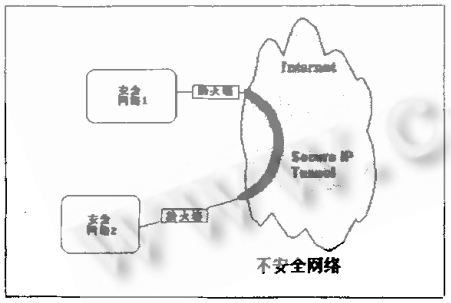

图 6　安全 IP 通道结构示意图

在两个私有网络之间建立一个私有 IP 通道，这个通道穿过一个公共网络(如 Internet)联系这两个私有网络。两个私有网络分别被防火墙保护，两个防火墙主机连在 IP 通道的两端，当数据通过 IP 通道从一个网络传向另一个网络时，通过第一个防火墙时数据被加密，到达另一端的防火墙时被解密，使数据能够安全地传输。这样在公共网络上建立一个虚拟的安全通道。

安全 IP 通道基于密码学来加强数据的安全性，即通道节点间有共同的密钥格式，利用密钥，IP 通道提供两种类型的安全性：

·授权，在从通道送出的数据包中附加信息授权码(MAC)，MAC 是根据数据内容 和加密密钥用单向 Hash 函数生成，接受方防火墙执行相同的操作，如果 MAC 匹配，则知道数据是经过加密的；

·加密，信息包中的数据由安全密钥加密，在传输中不可见。

授权和加密可以独立使用，可以根据对协议和数据安全性的高低，来决定使用情况。

外部攻击者能够窃听通过公共网络上的所有通信，安全 IP 通道允许你掩盖真实的数据，保证联系伙伴的身份，保证了数据的验证。

结束语

信息高速公路的巨大优势有目共睹，其优势在于其上的所有资源均可以共享，而这些也是其脆弱性之所在。本文介绍了网络安全技术 - - 防火墙技术，是解决 Internet 上的安全问题的有效措施，保护着网络上企业和个人利益的安全。铁路系统需要建设自己的 Intranet，建立一个完备的安全系统势在必行。

(来稿时间：1998 年 2 月)