计算机科学1999Vol. 26№. 8

包过滤防火墙的安全研究

On Security for Packet Filtering Firewalls

王家业 荆继武 朱森存

（中国科大研究生院信息安全国家重点实验室 北京 100039）

Abstract In this paper we will provide a general introduction to the principles of packet filtering firewalls, then identify and examine problems common to many current packet filtering implementations. Solutions to these problems are also proposed.

Keywords Firewall, Packet filtering, Network security

一、引言

包过滤和代理系统是目前互联网络防火墙中较为普遍使用的二种技术。其中包过滤防火墙由于可以与现有的路由器集成，也可以用独立的包过滤软件实现，十分灵活方便，所以应用最为广泛。但如果产品选择和使用不当，出现的问题也是最多的。

包过滤技术的主要依据是包含在IP包头中的各种信息，一般不涉及包体中的数据（当然根据包体中的关键词也可以过滤，本文不作讨论）。所以，包过滤技术可以过滤IP地址，而难以过滤具体用户；可以过滤服务，而一般难以过滤包含在服务中的具体操作。它是一种有效地保护内部网络的基本手段，但往往显得不够"精细"。

包过滤防火墙的安全性与厂商提供给用户的过滤功能及用户配置的过滤规则有密切关系。本文先简要介绍IP包过滤技术原理，然后重点分析包过滤防火墙的十类不安全因素及其解决方法。

二、包过滤技术原理

本文主要讨论IP包过滤，这是指对TCP/IP网络中的网络层和运输层的信息进行包过滤，因为在现实生活中提供非TCP/IP网络进行包过滤的防火墙极少，非IP包在广域网中也很少见，或者当它们在互连网中传输时，一般也被组装成另一个IP包；而且，TCP/IP网络中的IP以下层很难进行包过滤，而在应用层进行包过滤的情况也很少见。

包过滤防火墙主要根据IP包头和TCP/UDP/ICMP包头中的信息进行过滤。

（1）IP包头中可用的信息包括：

IP源地址：数据发送方的IP地址。利用该地址可以允许或禁止某些具有特定IP地址的机器发送的包通过防火墙。

IP目的地址：数据接收方的IP地址。利用该地址可以允许或禁止某些具有特定IP地址的机器通过防火墙接收到数据包。

IP协议类型：指IP包体中的数据的协议类型，可能是TCP，UDP，ICMP或其他的协议。利用它可以允许或禁止符合某种协议的包通过防火墙。

IP可选项：一般为空。如果包括的话，可以是可选项结束符，无操作，安全性与处理限制（军事应用），松散源路由选择，记录路由，数据流识别，严格源路由选择和互联网时间印迹等8项内容中某些项。其中对于包过滤来说，一定要禁止IP源路由选项。

（2）TCP包头中可用的信息包括：

TCP源端口号：代表数据源发送方发送该包的客户机或服务器程序，为一个16字节的正整数。客户机方的数字一般是随机分配的大于1023的数字，而服务器方一般是固定的小于1023的正整数，代表服务器提供的某种服务。利用该端口可以允许或禁止某种服务的包通过防火墙。

TCP目标端口号：代表数据接收方接收该包的客户机或服务器程序，为一个16字节的正整数。其作用同TCP源端口号。

TCP编码位：分为URG，ACK，PSH，RST，SYN，FIN共6位，用来确定报文段的目的和内容。其中的ACK位对过滤TCP协议包特别重要，它表明该包是用来建立一个TCP连接的第一包（ACK=

0)还是后续包(ACK=1),据此特征包过滤防火墙可以阻止经过防火墙的通信双方正确建立连接。

(3)UDP包头中的可用信息包括:

UDP源端口号:其含义与作用同TCP源端口号。

UDP目标端口号:其含义和作用同TCP目标端口号。

由于UDP采用无连接的方式提供高层协议间的事务处理,所以没有类似于ACK这样的标志信息。

另外,ICMP与TCP、UDP不同,它是在网络层中与IP一起使用的协议。ICMP应该说是IP的一部分,在它的上层没有任何其他协议,但它是通过IP来发送的。ICMP报文没有源端口号和目标端口号的信息,但它有消息类型编码。包过滤可以利用消息类型编码来对ICMP包进行过滤。其中的消息类型有:回送应答、无法到达目的地、抑制报源、重定向等。

三、包过滤防火墙的安全问题与分析

并非所有的包过滤防火墙都提供以上所有的过滤功能,也并非所有的用户都需要使用所有的过滤功能,所以,正确了解不同功能的包过滤防火墙的优点及其可能带来的安全问题,将有助于我们根据实际需要正确地选择防火墙产品并合理地进行配置。

1. 仅能根据源地址和目标地址过滤的防火墙

根据IP包收发双方的地址来过滤数据包,这是包过滤防火墙中最简单的方法。优点是配置简单,不用涉及通信双方具体的服务类型,而只允许指定的内部主机和外部主机之间进行通信。此外,该方法还能有效地防止外部主机伪装成内部主机。

但本方法不能防止黑客把自己的主机伪装成一个合法的外部主机;即黑客通过源地址伪装,可以用一个合法的源地址向内部主机发送报文,而包过滤防火墙毫无知觉。更进一步,黑客还可以在合法的外部主机与内部主机之间截获报文,和内部主机进行交互。其危险性可想而知。

另外,内部网中的某些不安全的服务,也会给黑客带来可乘之机。后面的分析会讨论到这种情况。

2. 仅能根据源端口号和目标端口号来过滤的防火墙

只允许外部网用户访问内部网中某些服务或只允许内部网的用户访问某些外部服务,这都是常见的情况。采用这种机制,可以禁止访问内部网中的某些不安全的服务,如基于RPC的服务等,从而能够有效地保护内部网资源。

很明显,这种情况必须保证提供服务的机器是可信的。对于内部网,由于我们可以对提供服务的机器进行详细检测,所以可以认为服务都是可信的;但对外部网的服务器所提供的服务而言,就不一定可信了。因为黑客很可能已经获得了外部网服务器的ROOT权限,从而完全控制了该机器。他可以把服务器提供的服务端口号改变,从而用其他危险的服务来代替防火墙认为是安全的服务,如此一来防火墙也就失去了应有的意义。

3. 没有ACK位检查的防火墙

对于TCP协议来说,如果包过滤防火墙没有提供ACK位检查禁止的手段,那就缺少了禁止外部用户与内部网络建立基于TCP的连接有效手段。

对于任何一个TCP连接来说,其第一包的ACK位与后续包是不同的:第一包的ACK为0,而后续包的ACK为1。利用这一特性,我们就可以方便地禁止外部用户访问内部服务器,而却允许内部用户访问外部网络。即禁止ACK=0的包进入内部网,从而无法建立连接。黑客把第一包数据的ACK位伪装为1也没有用,因为如此一来该包数据是可以通过防火墙,但就不能作为这个连接的第一包了。因此缺少ACK=0的第一包数据,也就不能建立连接。

4. 没有动态过滤能力的防火墙

由于UDP协议没有类似于ACK位的检查手段,如果内部网服务器中有基于UDP的服务,那就缺少了禁止外部用户访问内部网UDP服务的得力手段。

如果要求禁止外部用户访问内部网络基于UDP的服务,但同时允许内部网用户访问外部网基于UDP的服务,就应该使包过滤防火墙具有一定的记忆功能,即能够"动态"过滤UDP包。"动态"的意思是它能够记住内部网往外的UDP请求包,从而允许其相应的应答UDP包进入内部网。如果不是应答包,则一律拒绝。这种记忆功能只要防火墙记住内部网往外的UDP包的源端口号即可实现,它把该源端口号与欲进入内部网的UDP包的目的端口号进行比较,如果相同,证明为应答包,通过;否则丢弃该包。

5. 没有过滤基于RPC的服务的防火墙

基于RPC的服务都是比较危险的。例如黑客如果获得了内部网的NFS服务,他就可能获得该系统内的所有文件;而如果他获得了NIS/YP服务,就可

能获得口令文件。

然而，基于RPC的服务没有使用一个固定的服务端口，而且在系统每次重新启动后都不一样，这就给包过滤带来了很大困难。同时，拒绝外部网的黑客与端口映射器（固定端口号为111）的交互其作用也不大，因为黑客可以绕过端口映射器，用穷举法（共65536种可能性）查询该服务正在运行的端口号。

有些包过滤防火墙可以访问端口映射器，获得基于RPC的服务运行于那些端口，从而根据此端口信息来过滤。但是如此一来，防火墙每接收一个UDP包或每建立一条TCP连接，都要访问一次端口映射器，从而大大加重系统的负担。

所幸的是基于RPC的服务大都使用UDP协议，我们可以如下规定：除了指定的一些UDP服务（如DNS）外，其余全部拒绝。但需要防火墙本身支持这样的配置，并经过仔细测试。

6. 忽略源端口号过滤的防火墙

在防火墙没有源端口号过滤功能或者有但系统管理员没有在过滤规则中包含源端口号过滤信息时，将会出现意想不到的严重后果。

假如包过滤防火墙只想允许内部网用户接收和发送电子邮件，即允许往内和往外的SMTP连接通过防火墙，这时过滤规则中必然允许目标端口号大于1023的包通过。如果没有限制源端口号必须为25（SMTP的服务端口），那么该防火墙必然允许源端口号和目标端口号都大于1023的包通过。如果内部网中有服务器提供X11服务（服务端口号为6000），则黑客就可以名正言顺地访问该服务，包过滤就失去了作用。但如果在过滤规则中包含源端口号必须为25的话，这种情况就不会发生。

7. 只有单向过滤功能的防火墙

许多包过滤防火墙有这样一个致命的缺陷：只能对离开内部网的包采取过滤规则。这将导致如下问题：防火墙系统本身没有得到保护；对假冒内部IP地址的包无法过滤；对有2个以上接口的防火墙其配置十分复杂。

如果防火墙只能对进入内部网的包进行过滤，则以上3个问题的前2个可以解决，但第3个问题依然存在。很明显，假设某包过滤路由器有N个接口，则在防火墙内每个接口有N－1条路径和它相连，整个路由器内就有N＊（N－1）条通路。这就增加了防火墙配置的复杂度。

如果包过滤防火墙的每个接口都提供双向过滤功能，而且对每个接口都制定双向过滤规则，则以上问题就能很好解决。

8. 日志记录不全的防火墙

包过滤防火墙一般都有日志记录功能，但不同的产品其完善程度可能很不一样。没有日志记录功能的防火墙是不合格的，因为我们不能及时发现应该拒绝的包是否如愿被拒绝，而只能等待攻击发生后才能确定。

记录包是从哪个接口进入防火墙是非常重要的，因为它有助于伪包的鉴别。例如，发现与内部网相连的接口接收到有内部网源地址的包，这是正常的；但如果发现与外部网相连的接口接收到此类包，就说明出了问题，应该彻底检查。因为这可能说明内部网配置有误；或者黑客正攻击系统（是一个伪包）；也可能是内部网用户用类似于PPP拨号的方式建立了与外部网的直接相连，从而绕过了防火墙。

9. 没有禁止IP源路由选项的防火墙

从上节可以看到，在IP包头中包括有可选项，其内容可以为空，也可以设置，在8个可选项中，松散源路由和严格源路由选项对防火墙的配置影响最大。设置源路由的目的是让发送者指定IP包经过的网络路径，而不是由路由器决定如何转发该包。其中严格源路由给出的是IP分组到达其目的地必须经过的准确路径；松散源路由也是一样给出IP分组必须遵循的网络路径，但允许在列出的连续IP地址之间有多个网络跨度。

如果防火墙没有禁止IP包的源路由选项，那么防火墙就形同虚设，因为黑客可以通过设置IP源路由来绕过防火墙。如果防火墙没有禁止IP源路由的功能，那将非常危险。

10. 不能过滤IP分片的防火墙

IP协议的一个重要功能是根据底层对包大小的限制，从而把从上层接收到的包划分为较小的片。IP包划分后得到的所有片有这样的特点（以IP的上层协议是TCP为例）：每一片都包含完整的IP包头，但只有第一片同时还包含上层协议（如TCP）的包头。

如果包过滤防火墙只是根据IP包头信息过滤，IP分片就不会带来多大问题。但如果同时还要对上层协议的包头进行过滤的话，那就只有第一片被禁止，其余片都可以无障碍地通过，因为它们没有上层包头的信息。虽然这些片到达目的主机后不能正确组装成原来的IP包，但仍然能够泄露相当多的信息。如果防火墙内外用户联合作弊，危险性就更大。

（下转第42页）

对所建立工作流语义中的关键参数(如:人员、时间、费用、资源)反复多次地进行充分地配置及实时分析,在其正式运转之前验证其逻辑的正确性及完整性。经过仿真检验的语义信息被放入工作流数据库,作为工作流运行的依据。

⑤工作流应用对应具体的工作流,它涉及具体的业务处理过程,直接面向最终用户。在工作流应用运行过程中,工作组成员间依据一组已定义的规则及已制定的共同目标,交换文本文件、各种媒体信息及与任务相关的信息。通过工作流应用,用户可以改进和优化业务处理过程,有效地解决业务处理过程中的协调、通信和控制问题。在 NEUWork 中,工作流建立人员(Workflow Builder)利用工作流语义设计与仿真层提供的图形化描述工具,对整个业务处理过程及涉及的资源进行定义后,将其存入工作流数据库,经过 WFMSWORK 的解释,即完成一个工作流应用的开发。创建过程快速简洁,能够使工作流应用根据快速变化的环境动态地改变。工作流应用的运行由工作流管理支撑平台通过调用组件进行支持,在工作流应用中涉及到的资源及各业务步骤之间的依赖关系由工作流管理支撑平台统一进行管理。

结束语 本文提出了一个具有开放集成特征的工作流管理系统的体系结构,为实现该系统的开放性与集成性我们采用了分层策略、形式化描述及仿真技术、组件技术、基于事件驱动规则智能匹配的工作项目触发机制及基于知识的群体决策辅助机制。通过该系统的研究我们还提出了一个与传统的信息管理系统开发相比较更为有效,更灵活的方法,为来自不同应用领域的用户内部综合信息处理网(Intranet)提供了面向群体协作,具有开放集成结构特征并将用户需求分析、模型建立,仿真等功能结合为一体的开发环境。这一开发环境也适合各种动态变化的分布式应用环境的建立。

参考文献

1 Hollingsworth D. The Workflow Reference Model. Workflow Management Coalition, 1994

2 Shrivastava S K, Wheater S M. Architectural Support for Dynamic Reconfiguration of Large Scale Distributed Application. In: The 4th Intl. Conf. on Configurable Distributed Systems (CDS' 98) Annapolis, Maryland, USA, 1998. 4~6

3 Tang J, Veijalainen J. Transaction-oriented Workflow Concepts in Inter-organizational Environments. In: The Fourth Intl. Conf. on Information and Knowledge Management (CIKM' 95), Baltimore, Maryland, USA, 1995

4 Eder J, Liebhart W. Workflow Recovery. IEEE Computer Society Press, Brussels, Belgium, 1996. 124~134

5 Niu Junyu, et al. An Internet-Based Workflow Management System with Decision Support. In: Proc. of Second Intl. Workshop on CSCW in Design. 1997. 453~457

6 Ranno F, et al. A Language for Specifying the Composition of Reliable Distributed Applications. In: The 18th Intl. Conf. on Distributed Computing Systems (ICDCS' 98). Amsterdam, The Netherlands, 1998. 26~29

(上接第36页)

如果包过滤防火墙能够把第一片及其后续片都缓存下来,就能对后续的片实施与第一片相同的过滤规则。这就可以解决信息泄露的问题。

结束语 包过滤是目前应用最广泛的防火墙技术之一,但如果产品功能设计不全面,或用户配置不正确,就可能导致以上的种种问题。一旦包过滤防火墙厂商能够提供全面的包过滤手段,并且用户能够正确配置,就能使利用防火墙的风险减少到最低程度。

参考文献

1 David N, et al. Firewalls: don't get burned. Data Communication, 1997, 26(4)

2 Allen B L. Building network Firewalls with Routers and Bridges. Information Systems Security, winter 1994

3 Cheswich W R, Bellovin S M. Firewalls and Internet Security——Repelling the Wily Hacker. Addison-Wesley, 1994

4 Chapman D B. Network(In)Security Through IP Packet Filtering. In: USENIX Security Symoposium Proc. USENIX Association, September 1992 14~16

5 刘渊,等. 因特网防火墙技术. 机械工业出版社, 1998