防火墙技术的研究与探讨

张晔 刘玉莎 (上海同济大学计算中心 200092)

摘要:本文在阐述各种防火墙技术的原理、优势及缺陷的基础上,对各种技术进行了综合比较,并对决定防火墙性能的主要因素进行了深入探讨。最后文章引出了防火墙技术的不足及发展方向。

关键词:网络安全 包过滤 应用网关 代理服务 状态检测

一、防火墙技术的研究和探讨

1. 种种防火墙技术的原理和比较

目前保护网络安全最主要的手段之一就是构筑防火墙,它是一道界于开放的、不安全的公共网与信息、资源汇集的内部网之间的屏障,这道屏障可由一个或一组系统组成,用以实施两个网络之间的访问控制和安全策略。狭义上防火墙指安装了防火墙软件的主机或路由器系统;广义上还包括整个网络的安全策略和安全行为。

防火墙技术一般可分为以下几种,包过滤(Packet Filtering)、应用网关(Application Layer Gateway)、代理服务(Proxy Service)、状态检测(Stateful Inspection)、电路层网关(Circuit Gateway)和自适应代理技术。以下列举了各种防火墙技术的原理及优缺点。

(1)包过滤技术。包过滤技术是在网络层对数据包进行选择和过滤,选择的依据是系统内设置的过滤逻辑,也被称为访问控制表(Access Control Table)。该技术通过检查数据流中的每个数据包的源地址、目标地址、源端口、目的端口及协议状态,或它们的组合来确定是否允许该数据包通过。

这种防火墙通常安装在路由器上,具有过滤效率高、成本低、易于安装和使用的特点。

其不足主要有以下几点:

①是一种基于 IP 的认证,因此不能识别相同 IP 地址的不同用户,不具备身份认证功能。与此同时,包过滤所判别的条件位于数据包的头部,由于 IPv4 的不安全性,导致各种条件极有可能被伪装。

②是一种基于网络层的安全技术,不具备检测通过高层协议(如应用层)而实施的攻击。

③过滤规则集具有相当的复杂性,但没有严格的测试工具来检验其正确性,难免仍会出现漏洞。

④对于采用动态或随机分配端口的服务,如 RPC(远程过程调用)服务,就很难进行有效地过滤。

(2)应用网关。应用网关是在应用层上实现协议过滤和转发功能,它针对特别的网络应用协议制定数据过滤逻辑。

由于该技术工作于应用层,因此具有高层应用数据或协议的理解能力。然而由于它与包过滤技术一样使用了过滤的机制,因此仍然保留了让防火墙外部网络直接了解内部网络结构和运行状态的可能。

(3)代理服务。代理服务向一些标准的服务应用提供代理。代理服务器接收客户请求后会检查并验证其合法性,若合法,它将作为一台客户机一样向真正的服务器发出请求并取回所需的信息,最后再转发给客户。它将内部系统与外界完全隔离开来,从外面只能看到代理服务器而看不到任何内部资源。而且代理服务器只允许被代理的服务通过,而其他所有服务都将完全被封锁住。

代理服务通常被认为是最安全的防火墙技术,因为只有那些被认为"可信赖的"并被代理的服务才允许通过防火墙,其他服务则被彻底封死。此外,由于代理服务与应用网关一样工作于应用层,因此还可以过滤协议,如可以过滤 FTP 连接,拒绝使用 PUT 放置命令,以保证用户不能将文件写到匿名服务器。

其不足主要有以下几点:

①由于该技术工作于网络的最高层,导致其不能完全透明地支持各种服务、应用,而必须为每种应用分别编写不同的代理程序。

②该技术将消耗大量的 CPU 资源,导致低性能。

(4)电路层网关。电路层网关在两个主机首次建立 TCP 连接时建立起一道屏障。它首先作为服务器接收外来请求,转发请求,与被保护的主机连接时则担当客户

机角色，起到一定的代理服务作用。它监视两主机建立连接时的握手信息，如 Syn、Ack 和序列数据等是否合乎逻辑，判定该会话请求是否合法。然而一旦会话连接有效后，该网关仅复制、传递数据，而不再进行任何过滤。

电路层网关在 IP 层代理各种高层会话，因此具有代理技术所特有的隐藏内部网络信息的能力，同时又可以看作是包过滤和应用网关的折衷。然而由于其仅仅关心是否允许或拒绝某一会话的建立，而对会话建立后所传输的具体内容不再作进一步分析，因此安全性仍不高。

(5)状态检测。状态检测技术将动态记录、维护各个连接的协议状态，并在网络层对通信的各个层次进行分析、检测，以决定是否允许通过防火墙。

由于该技术在网络层对上层协议数据进行分析、检测，因此可以把它看作是包过滤技术和应用网关技术的折衷和融合，兼备了较高的效率和安全性。与此同时，状态检测技术不但可以支持多种网络协议和应用，而且由于不需为不同的应用编写各自的代理程序，因此可以方便地扩展实现对各种非标准服务的支持。除此之外，因为状态监视技术将记录并动态维护每个连接的状态，实现了对 RPC 和 UDP(用户数据报)的支持。

(6)自适应代理技术。这是一种最新的防火墙技术，在某一程度上反映了目前防火墙技术的发展动态。该技术可以根据用户定义的安全策略，动态适应传送中的分组流量。如果安全要求较高，则最初的安全检查仍在应用层完成，以保证实现传统代理防火墙的最大安全性；而一旦代理明确了会话的所有细节，那么其后的数据包就可以直接经过速度快得多的网络层。这样一来，该技术就兼备了代理技术的安全性和状态检测技术的高效率。

为了更好地说明各种防火墙技术的实质和特点，以下对各种防火墙技术进行了综合比较：

表 1 各类防火墙技术对比

	包过滤	应用网关	代理服务	电路层网关	状态检测	自适应代理技术
工作层次	网络层	应用层	应用层	网络层	网络层	网络层或应用层
效率	最高	低	最低	高	高	自适应
安全性	最低	高	最高	低	高	自适应
根本机制	过滤	过滤	代理	代理	过滤	过滤或代理
内部信息隐藏	无	无	有	有	无	有
高层数据理解	无	有	有	无	有	有
支持应用	所有	标准应用（易扩展）	标准应用（不易扩展）	所有	标准应用（易扩展）	标准应用（不易扩展）
UDP支持	无	有	有	无	有	有

从上表中可以得出这样的结论——防火墙的性能及特点主要由以下两方面所决定，那就是其工作的层次及所采用的机制(过滤或是代理)。首先，工作层次是决定防火墙效率及安全性的主要因素。一般而言，工作层次越低，则效率越高，而安全性越低；反之，工作层次越高，则效率越低，而安全性越高。当然这里需要补充的是，安全性还与防火墙所采用的机制有着密切的关系，如果采用过滤机制，则防火墙具有内部信息隐藏的特点，安全性相对要高些；如果采用过滤机制，则安全性要低些。此外，从上表的分析中还可以得出各种隐藏的内在关系，例如，防火墙具有高层数据理解能力则必然不能透明支持各种应用，反之则可以。

按实现的硬件环境，可以分为基于路由器的防火墙和基于主机系统的防火墙。包过滤防火墙可基于路由器或基于主机系统来实现，而电路级网关和应用级网关只能由主机系统来实现。

按拓扑结构可以分为以下几种：

①双穴网关(Dual Homed Gateway)。该结构是由一台安装了两块网络接口卡的主机系统作为网关，分别连接外部网和被保护网络。在该双穴网关中，可以实现从包过滤到代理服务的所有技术来实现系统的安全策略。对双穴网关的最大威胁是直接登录到该主机后实施攻击，因此双穴网关对不可信任的外部主机的登录应进行严格的身份验证。

②屏蔽主机网关。屏蔽主机网关由一个运行代理服务的双穴网关和一个具有包过滤功能的路由器组成，一般情况下，双穴主机设置在被保护网络，路由器设置于双穴网关和外部网络之间。这样外部网络只能访问到双穴网关而不能直接访问被保护网络的其他资源，系统安全性大大提高了。

③屏蔽子网网关。一个独立的屏蔽子网位于外部网和被保护网络之间，起保护隔离作用。它由两台包过滤

路由器和一台代理服务主机构成。路由器过滤掉禁止或不能识别的信息，将合法的信息送到代理服务主机上，并让其检查，并向内或向外转发符合安全要求的信息。该方案安全性能很高，但管理也最复杂，成本也很高，应用于有高安全性需求的场合。

2.防火墙新技术

好的安全产品志在提供一整套解决网络安全问题的各种应用，为大量的网络用户及需保护的网络资源提供了一个可管理的、分布式的、安全的计算环境。显然，光靠纯粹的防火墙所提供的访问控制能力是远远不够的。除此之外，严格的认证技术、完善的授权机制、安全的数据传输、完备的审计报表、易于使用的集中式管理控制台也是必不可少的。近来，新型防火墙产品已越来越多地融合了各种安全技术，志在提供一套完整的企业级安全解决方案。

以下列举了防火墙所使用的一些新技术：

(1)实现内容安全，可自动进行病毒扫描，堵截非法 URL 和 Java 或 ActiveX 过滤。

(2)提供基于身份的认证，并可在各种认证机制中选择使用。

(3)网络地址翻译(NAT)，一方面缓解了 IP 地址不足的问题，同时又对外隐藏了内部信息。

(4)增加了防止基于协议攻击的手段，例如防止 IP 地址欺骗(IP Spoofing)，源路由攻击(Source Routing)，残片攻击(Tiny Fragment Attacks)，TCP SYN 攻击等。

(5)服务器负载平衡。

(6)流量分析，了解各种服务所占通信流量，或某一服务具体使用情况(如：最受欢迎的页面等)。

(7)提供加密通信隧道实现虚拟专用网。

(8)攻击检测用以实时检查各种网络攻击的痕迹，并采取相应的对策，如通知管理员或直接修改防火墙策略。

(9)详细的审计及完善的报表。

(10)企业级的管理，可以在管理控制台上统一制定一套安全策略，再由网络分发至各防火墙或其他安全设备。

(11)高可用性。此外，还有部分防火墙厂商还把 Web 页面超高速缓存和带宽管理等技术也结合进来。

表 2 各类防火墙产品对比

公 司	产 品	价 格	平 台	优 点	不 足
Microsoft	Proxy Server 2.0	$995	Windows NT 4.0	紧密集成在所有的Windows NT网络； 具有高级的HTTP代理功能	对非Windows客户端，有些功能不可用； 要求客户端在NT的用户数据库中注册，进行身份验证
Check Point Software	FireWall-1 3.0	$2995～18990	HP-UX，IBM AIX，Solaris，SunOS，WindowsNT	易于配置和重配置，支持平台多，多点管理最佳，功能面广	用户界面笨拙；监控工具和实时功能弱
Cisco System	PIX FireWall 4.1	$9000	专用硬件	安全模式简单，界面易于配置，熟悉Cisco路由器命令的人能很快掌握	代理功能有限，安全模式相当不灵活
Elron Software	Elron Firewall/Secure 320S	$4995	基于Intel CPU的微机，防火墙运行于自己的操作系统；管理界面运行在Windows NT/95	支持多协议，对简单网络可以快速配置	没有实际意义上的代理，身份验证要求额外的Windows应用程序
CyberGuard	CyberGuard Firewall 4 for Unix	$5995～14995	基于Intel CPU的微机，防火墙运行于固化在硬件里的操作系统之上	实时监测工具很好，内置域名系统，功能强大的代理	原始日志、配置界面不够平滑
Ukiah Software	NetRoad FireWall	高于$995	Windows NT	安装快速，包括IPX-to-IP网关，成本很低	文档资料较差，配置规则不灵活
Netguard	Guardian V3.0	$3980～8980	Windows NT(管理界面运行在Windows 95上)	优异的实时连接监控，较好的简单网络配置向导	文档资料不足，代理功能有限
Watchguard Technology	Watchguard Security System 3	高于$3995	专有硬件(管理界面运行于Linux或Windows平台)	采用吸引小型网络的"黑盒子"方法，配置灵活，很好的实时冲突避免功能	有限制的配置不能随需求增长，内部的Linux内核把支持操作系统的重担加在小厂商身上

3. 各种防火墙产品的比较

当前国外比较著名的防火墙产品有 Checkpoint 的 Firewall－1, Microsoft 的 Microsoft Proxy Server, Netscape 的 Netscape Proxy Server, Cisco 的 PIX Firewall, CyberSafe 的 Challenger 等。表 2 列举了各防火墙产品的主要性能及优缺点。

二、防火墙存在的问题及发展方向

以上是国外主流防火墙产品，尽管它们集成了各种安全技术，各有特色，然而在如何防止内部攻击这个问题上并没有拿出令人满意的方案。近年来，越来越多的企业倾向于根据安全等级，将内部网划分为多个子网，并在内部路由器上安装防火墙产品来保护内部敏感区域。然而，将彼此独立的防火墙简单地堆积在一起，永远不可能形成一套完整的、集成的、综合安全解决方案。简言之，传统解决方案有以下不足。

(1)高成本。无庸置疑，在内部网中有越多的主机或者资源需要保护，那么就有越多的安全检查点需要设置，这也就意味着更高的设备成本及系统维护开销。简言之，企业总拥有成本增加了。

(2)高管理负担。对于 IT 管理人员来说，他们将面临极大的挑战来管理、维护如此多的防火墙设备。

(3)存在盲点。传统防火墙将检查点设立于一个所谓"可信子网"的入口处。显然，发自于该子网内部任何主机的攻击都将成为该防火墙的盲点。除此之外，如果对 Modem(调制解调器)的使用不加以限制的话，攻击者完全可以通过"后门"，轻松地饶过防火墙，随心所欲地破坏窃取任何资源。

(4)降低网络的性能。由于有大量的安全检查点被安置于企业内部的各种路由设备上，内部网中所有的通信，无论是否需要进行安全检查，都将不可避免地经过若干个安全检查点，以至于造成相应的传输延迟。因此，整个网络的性能降低了。

(5)站点到站点的虚拟专用网。虽然目前有越来越多的防火墙产品集成了对 VPN 的支持，然而一般而言，这些 VPN 只是在介于两个站点网关之间的公共网络上建立了一条加密的数据通道，然而一旦通信越过目标站点网关，它将被解密并至于内部网中，可想而知，安全隐患出现了。

(6)复杂的状态同步机制。为了实现高可用性，两个或多个路由设备将被对等地放置于网络入口处。为了实现安全，防火墙被分别安装在这些路由设备上，同时，每个防火墙的状态必须在使用时保持完全一致，这是由于原本属于同一会话的 IP 包完全可能通过不同的传输路径。由此，一个复杂的状态同步机制必须引入安全系统。

从以上的分析可以看出，传统的防火墙结构在其技术原理上对来自内部的安全威胁不具备防范能力，为了实现其有限的防护能力，还必须要有一个相对封闭的网络拓扑结构来支持，因此只是一种短期内的解决方案。而只有运用先进认证技术，并在网络层上实施统一的用户端对端的数据流加密技术，再结合目前的防火墙技术以进行必要的内容检测、攻击检测及其他一些手段，才能解决内部网安全问题，并最终提供一套一体化的解决途径。这也是防火墙技术未来的发展方向。

参考文献

[1] Cheswick W. R. & Bellovin, S. R. (1994) Firewalls and Internet Security, Repelling the Wily Hacker, Addison－Wesley, Reading MA.

[2] Crane, E. (1996) Tomorrow' S Technology, Promising a Safe New World, Infosecurity News, MIS Institute Press, Inc., P. 20. URL: http://www. infosec-news. com

[3] 汪立东，钱丽萍。(1998－08) Internet 攻击和防火墙新技术，《计算机系统应用》，1998 年第 8 期，P20

[4] Scott Fuller, Kevin Pagan 著，Intranet Firewalls，董春，张红雨，刘英杰译：电子工业出版社，1997

(来稿时间：1999 年 4 月)