DOI:10.16104/j.issn.1673-1883.2004.04.041
第 16 卷第 4 期 西昌师范高等专科学校学报 Vol.16,No.4
2004 年 12 月 Journal of Xichang Teachers College Dec., 2004

分布式防火墙技术及应用

罗明英

（西昌学院 信息技术系，四川 西昌 615022）

【摘 要】 分布式防火墙是指那些驻留在网络中主机如服务器或桌面机并对主机系统自身提供安全防护的软件。本文在分析传统防火墙的特点和存在的问题的基础上，讨论了分布式防火墙这种新的防火墙体系结构及其技术特点，最后介绍一个应用实例。

【关键词】 防火墙；分布式防火墙；主机驻留；网络安全

【中图分类号】G202 【文献标识码】B 【文章编号】1008-6307(2004)04-0133-03

The Application of Distributed Firewalls Technology

LUO Ming-ying

(*Department of Information Technology, Xichang College, Xichang 615022, Sichuan*)

Abstract: Distributed firewalls are host-resident security software applications that protect the enterprise network's critical endpoints against unwanted intrusion-that is,its servers and end-user machines. This text is on the basis of analysing the characteristic and question of traditional firewalls, Have discussed such new system structure and technological characteristic of distributed firewalls, Introduce a application example at last.

Key words: Firewalls; Distributed firewalls; Host-resident; Network security

1 引言

随着计算机技术和Internet的发展，社会各个机构建立了内部网络(Intranet)，当机构将其Intranet与Internet连接之后，Intranet的内部数据和网络设施暴露给Internet上的黑客时，网络管理员越来越关心网络的安全。为了提供所需级别的保护，Intranet需要有安全策略来防止非法用户访问内部网络上的资源和非法向外传递内部信息。即使一个机构没有连接到Internet上，它也需要建立内部的安全策略来管理用户对部分网络的访问并对敏感或秘密数据提供保护。

Internet防火墙是这样的系统(或一组系统)，它能增强机构内部网络的安全性。防火墙系统决定了那些内部服务可以被外界访问；外界的那些人可以访问内部的那些可以访问的服务，以及那些外部服务可以被内部人员访问。要使一个防火墙有效，所有来自和去往Internet的信息都必须经过防火墙，接受防火墙的检查。防火墙必须只允许授权的数据通过，并且防火墙本身也必须能够免于渗透。

2 传统防火墙存在的问题

传统的防火墙设置在网络的边界，在内部企业网和外部互联网之间构成一个屏障，进行网络存取控制，我们可以称之为边界防火墙(Perimeter Firewall)。边界防火墙有如下固有缺欠：

(1)结构性限制 边界防火墙的工作机理依赖于网络的物理拓扑结构。但随着越来越多的企业利用互联网构架自己的跨地区网络，包括家庭移动办公和的服务器托管等越来越普遍，所谓内部企业网已经是一个逻辑的概念；另一方面，电子商务的应用要求商务伙伴之间在一定权限下进入到彼此的内部网络，所以说，企业网的边界已经是一个逻辑的边界，物理的边界日趋模糊，边界防火墙的应用受到了愈来愈多的结构性限制。

(2)内部安全 边界防火墙设置安全策略的一个

收稿日期：2004-11-06

作者简介：罗明英(1964-)，女，副教授，在读软件工程硕士。

基本假设是：网络的一边即外部的所有人是不可信任的，另一边即内部的所有人是可信任的。但在实际环境中，据统计，80%的攻击和越权访问来自与内部，也就是说，边界防火墙在对付网络安全的主要威胁内部威胁时束手无策。

(3)效率和故障 边界防火墙把检查机制集中在网络边界处的单点上，产生了网络的瓶颈问题，这也是目前防火墙用户在选择防火墙产品时不得不首先考察其检测效率而按前机制反在其次的原因。边界防火墙厂商也在不遗余力地提高防火墙单机处理能力甚至采用防火墙群集技术来解决这个边界防火墙固有的结构性瓶颈问题 ;另外，安全策略的复杂性也给效率问题雪上加霜，对边界防火墙来说，针对不同的应用和多样的系统要求，不得不经常在效率和可能冲突的安全策略之间权衡利害取得折中方案，产生了许多策略性的安全隐患 ;最后，边界防火墙本身也存在着单点故障危险，一旦出现问题或被攻克，整个内部网络完全暴露在外部攻击者面前。

3 分布式防火墙技术

3.1 分布式防火墙的概念

随着互联网的发展和人们对网络安全性认识的提高，防火墙作为一种网络隔离控制技术和网络安全措施，越来越受到广泛的重视。防火墙技术本身也伴随着互联网应用特别是电子商务应用的深入不断发展，分布式防火墙(Distributed Firewalls)技术就是当前防火墙技术领域中依次有深远意义的机构性变革。

针对传统边界防火墙的缺欠，“分布式防火墙”的概念被专家学者提出来。从狭义和与边界防火墙产品对应来讲，分布式防火墙产品是指那些驻留在网络中主机如服务器或桌面机并对主机系统自身提供安全防护的软件产品；从广义来讲，“分布式防火墙”是一种新的防火墙体系结构。

3.2 分布式防火墙产品

目前，分布式防火墙产品的种类和生产厂家都很多，但归纳起来，分布式防火墙主要有如下几类产品：

(1)、网络防火墙(Network Firewall)：用于内部网与外部网之间(即传统的边界防火墙)和内部网子网之间的防护产品，后者区别于前者的一个特征是需支持内部网可能有的IP和非IP协议。

(2)、主机防火墙(Host Firewall)：对于网络中的服务器和桌面机进行防护，这些主机的物理位置可能在内部网中，也可能在内部网外，如托管服务器或移动办公的便携机。

(3)中心管理(Central Management)：边界防火墙只是网络中一个单一设备，管理是局部的。对分布式防火墙来说，每个防火墙作为安全监测机制可以根据安全性的不同要求布置在网络中的任何需要的位置上，但总体安全策略又是统一策划和管理的，安全策略的分发及日志的汇总都是中心管理应具备的功能。中心管理是分布式防火墙系统的核心和重要特征之一。

3.3 分布式防火墙技术

分布式防火墙技术可以总结为如下几个方面：

主机驻留(Host-resident)：主机防火墙的重要特征是驻留在被保护的主机上，该主机以外的网络不管是处在内部网还是外部网都认为是不可信任的，因此可以针对该主机上运行的具体应用和对外提供的服务设定针对性很强的安全策略。主机防火墙对分布式防火墙体系结构的突出贡献是使安全策略不仅仅停留在网络与网络之间，而是把安全策略推广延伸到每个网络末端。

嵌入操作系统内核(Embedded in OS kermel0：众所周知，操作系统自身存在许多安全漏洞，运行在其上的应用软件无一不受到威胁。主机防火墙也运行在该主机上，所以起运行机制是主机防火墙的关键技术之一。为自身的安全和彻底堵住操作系统的漏洞，主机防火墙的安全监测核心引擎要以嵌入操作系统内核的形态运行直接接管网卡，在把所有数据包进行检查后再提交操作系统。为实现这样的运行机制，除为这需要一些自身的开发技术外，与操作系统厂商的技术合作也是必要的条件，因为这需要一些操作系统不公开的内部技术接口。不能实现这种嵌入式运行模式的主机防火墙受到操作系统安全性的制约，存在明显的安全隐患。

个人防火墙(Personal Firewall)：个人防火墙是在分布式防火墙之前业已出现一类防火墙产品。IDC将个人防火墙定义为成本在100美圆以下，以一般消费者和小企业为客户群，通过Cable或DSL调制解调器实现高速不间断来连接的独立产品。分布式针对桌面应用的主机防火墙与个人防火墙有相似之处如它们管理方式迥然不同，个人防火墙的安全策略有系统使用者自己设置，目标是防外部攻击，而针对桌面应用的主机防火墙的安全策略由整个系统的管理员统一安排和设置，除了对该桌面机起到保护作用外。也可以对该桌面机的对外访问加以控制，并

且这种安全机制是对桌面机的使用者是不可见和不可改动的。其次,不同于个人防火墙面向个人用户,针对桌面应用的主机防火墙是面向企业级客户的,它与分布式防火墙其它产品共同构成一个企业级应用方案,形成一个安全策略中心统一管理,安全检查机制分散布置的分布式防火墙体系结构。

托管服务器(Hosting) :互联网和电子商务的发展促进了互联网数据中心(Internet Data Center)的迅速崛起,起主要业务之一就是服务器托管服务。对服务器托管用户而言,该服务器逻辑上是其企业网的一部分,只不过物理上不在企业内部,对于这种应用,边界防火墙解决方案就显得比较牵强附会,而针对服务器的主机防火墙解决方案则是其一个典型应用。用户只需在改服务器上安装上主机防火墙软件,并根据该服务器的应用设置安全策略即可,并可以利用中心管理软件对该服务器进行远程监控,不需任何额外租用新的空间放置边界防火墙。对互联网数据中心而言,也需要提供包括防火墙安全服务在内的增值服务来提高竞争力,区别于用边界防火墙方案向托管用户提供防火墙安全增值服务,采用主机防火墙方案有其独到之处 :首先,可以向托管用户提供针对特定用户特定应用的安全服务,使服务更安全更贴切 ;其次,消除了边界防火墙的结构性瓶颈问题。

4　分布式防火墙在IDC中的应用

对互联网数据中心而言,在激烈的市场竞争环境中,需要提供包括防火墙安全服务在内的增值服务来提高竞争力。以世纪互联为例,该互联网数据中心向托管用户系统提出了管理防火墙系列服务,包括独享式防火墙、共享式防火墙和主机式防火墙三种服务,其中主机式防火墙服务是利用美国网屹安全公司CyberwallPLUS-SV主机防火墙,其应用模式如图2所示。图中的公司A、B、C都是托管用户,它们都有不同数量的服务器在数据中心托管,服务器上也有不同的应用。如果托管用户希望把这些服务器的安全问题委托给数据中心专业的安全服务部门来负责,就可以与数据中心签定相应的安全服务保障合同。数据中心的安全服务部门在需提供安全服务的服务器上安装一套CyberwallPLUS-SV主机防火墙,根据用户具体应用要求,设定相应策略。对于安装了CyberwallPLUS-CM中心管理系统的管理终端,数据中心安全服务部门的技术人员可以对所有在数据中心委托安全服务的服务器的安全状况进行监控和提供有关的安全日志记录。

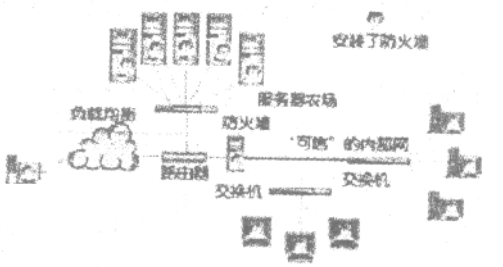

图1　分布式防火墙方案

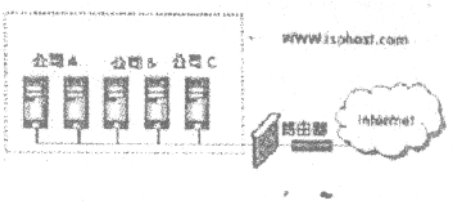

图2　在托管服务器上安装分布式防火墙

5　结束语

传统防火墙通常在网络边界站岗,如果说它对来自外部网的攻击算得上是个称职的卫士,那么对于80%的来自内部网的攻击它就显得心有余而力不足,而分布式防火墙,它的专长在于堵住内部网漏洞,充分利用好分布式防火墙技术,能大大提高网络的安全性。

注释及参考文献:

〔1〕William Stallings. Cryptography and Network Security : Principles and Practice. Second Edition. Prentice Hall, New Jersey,1998

〔2〕3Com Technical Papers, Internet Firewalls and Security. Available at http ://www.3com.com/tech-nology/tech_net/white_papers

〔3〕3Com Technical Papers, Private Use of Networks for Service Providers. Available at http ://www.3com.com/technology/tech_net/white_papers

〔4〕钟乐海.Intranet安全对策研究.四川师范学院学报(自然科学版),2002年第1期

〔5〕杨波.网络安全理论与应用.北京 :电子工业出版社,2002年1月

〔6〕代伟.维护网络安全.北京 :国防工业出版社,2002年1月