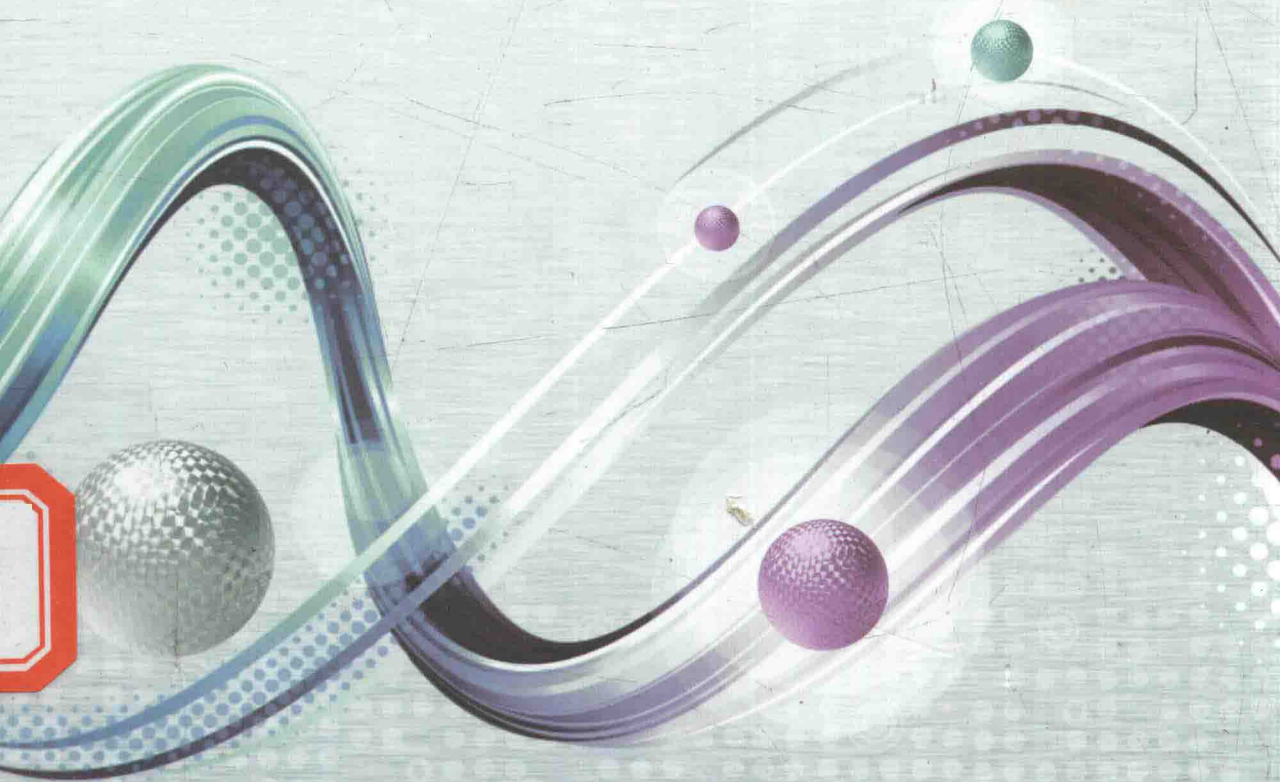
高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

新一代防火墙技术及应用

谢正兰　张　杰　编著
兰晓红　主审



西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

新一代防火墙技术及应用

谢正兰　张　杰　编著
兰晓红　　主审

西安电子科技大学出版社

内 容 简 介

本书共 12 章，主要内容包括：防火墙概述、防火墙常用技术、基本网络配置及常见网络环境部署、VPN 互联技术、服务器保护技术、网页防篡改技术、流量管理技术、高可用技术、风险发现及防护技术、常见攻击测试技术、NGAF 产品部署排错以及虚拟防火墙。

本书紧跟防火墙的发展前沿，既有理论深度，又有实用价值，理论与对应的项目实训紧密结合，突出重点难点，强化可操作性。本书可作为高校教材使用，也可作为云计算研发人员和云计算与网络安全技术爱好者的学习与参考资料。

图书在版编目(CIP)数据

新一代防火墙技术及应用 / 谢正兰，张杰编著. —西安：西安电子科技大学出版社，2018.4
ISBN 978-7-5606-4884-2

Ⅰ. ① 新… Ⅱ. ① 谢… ② 张… Ⅲ. ① 防火墙技术 Ⅳ. ① TP393.082

中国版本图书馆 CIP 数据核字(2018)第 054551 号

策　　划　李惠萍
责任编辑　李惠萍
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885882014 67　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱 xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西华沐印刷科技有限责任公司
版　　次　2018 年 4 月第 1 版　2018 年 4 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印　张　16.5
字　　数　389 千字
印　　数　1～3000 册
定　　价　36.00 元

ISBN 978-7-5606-4884-2 / TP

XDUP 5186001-1

前　言

目前，防火墙技术已经渗透到了各个行业当中，它已经成为新一代信息应用的重要基础设施，同时，掌握防火墙技术会使企业在市场中占据主动。当然，防火墙还存在着数据安全、行业标准、隐私权保护等诸多问题，然而随着技术的进步，防火墙技术将会逐渐完善。对于企业来说，对待防火墙更需要保持创新、务实和开放的态度并不断实践，所以本书引入了新一代防火墙的概念，使防火墙真正融入企业信息化应用管理中。

随着 Internet 宽带的发展与电子商务的盛行，网络安全问题变得日益重要。企业或个人越来越频繁地利用互联网进行各种交易，网络安全性已成为一个重要的议题。一般情况下，个人会用信用卡在网络上进行交易，公司之间会在网络上进行信息交换，因此一些重要资料就会在网络上流动，这时个人或公司传送的资料就有可能被拦截、修改或盗用。有些黑客为了获取他人技术而入侵别人的计算机，更严重的会导致企业的网站被破坏而无法工作并毁掉顾客资料，影响到公司的利益或顾客的隐私及权利。防火墙的目的就是保护网络不被未经授权的使用者经由外界网络不法侵入。

防火墙(Firewall)是指设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制(允许、拒绝、监测)出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的基础设施。

为了实现企业内部所需求的各项任务，防火墙需按照各类部门用户的需求制订安全策略，主要解决对于企业内网的分配和管理，便于统一管理各个部门的工作需求，改善以往比较混乱的情况，对所有关于网络的管理进行整合。

★ 本书主要内容

在编写本书之前，笔者花费了大量的心血和精力，对于全书的架构、各章知识点和章节中示例与案例循序渐进的引入做了明确的规划，避免了内容过多，

全而不精；着重章节内容的重点与难点的讲解，给出了大量应用实例、实验步骤等，强化了防火墙技术的可操作性。本书主要内容包括：防火墙概述、防火墙常用技术、基本网络配置及常见网络环境部署、VPN 互联技术、服务器保护技术、网页防篡改技术、流量管理技术、高可用技术、风险发现及防护技术、常见攻击测试技术、NGAF 产品部署排错以及虚拟防火墙。本书紧跟防火墙的发展前沿，既有理论深度，又突出实用价值，可作为高校相关专业的教材，也可作为云计算研发人员和云计算与网络安全技术爱好者的学习和参考资料。

★ 本书编写特点

• 本书采用理论与实践双线并行的架构设计，理论与对应的实战项目训练紧密结合。

• 内容精练，突出重点和难点，同时对重点难点的讲解运用了大量的示例来进行演示，便于学生理解与自学。

• 语言通俗，图文并茂；各章小结与练习题可供读者总结、提高。

★ 本书适用对象

无论是对于防火墙的初学者，还是有一定基础的 IT 运维人员，本书都是一本难得的学习和参考用书。本书非常适合高校计算机科学技术、网络工程、软件工程、网络技术、信息安全等专业高职生、本科生学习使用，也可供相关任课教师参考，还适合广大科研人员和工程技术人员研读。

由于作者水平有限，加之时间较紧，书中难免存在写作不到位的地方或疏漏之处，甚至存在错误之处，敬请读者批评指正。

编著者

2018 年 1 月

目　录

Chapter 1

第1章 防火墙概述

◆ 学习目标：

- 掌握防火墙的定义及功能；
- 掌握防火墙的基本结构；
- 了解防火墙的分类；
- 理解新一代防火墙的定义。

◆ 本章重点：

- 防火墙定义及功能；
- 防火墙基本结构；
- 新一代防火墙的定义。

◆ 本章难点：

- 无

◆ 建议学时数：4学时

本章从防火墙的标准定义出发，阐述了防火墙的功能、基本结构和分类，以及新一代防火墙技术的发展趋势。

1.1 防火墙的定义及功能

防火墙(Firewall)的本义是指古代在使用木制结构房屋时，为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围构筑起来的一道屏障，这种防护屏障就被称之为“防火墙”。其实与防火墙一起起作用的就是“门”。如果没有门，各房间的人如何沟通呢？这些房间的人又如何进去呢？当火灾发生时，这些人又如何逃离现场呢？这个门就相当于我们所讲的防火墙的“安全策略”，所以在此我们所说的防火墙实际并不是一堵实心墙，而是可以理解为带有一些小孔的墙。这些小孔就是用来留给那些允许进行的通信的通道，当然在这些小孔中安装了过滤机制，可以进行有效过滤，阻止非法通信。

现实生活中的防火墙就像是机场的安检部门，对进出机场的人和一切包裹进行检查，防止非法人员通过非法手段进入机场，同时保证合法包裹能够进入机场。而网络防火墙的产生正是基于以上的比喻。

1.1.1 防火墙的定义

国家标准 GB/T 20281—2006《信息安全技术 防火墙技术要求和测试评价方法》给出的防火墙定义是，设置在不同网络(如可信任的企业内部网络和不可信任的公共网络)或网络安全域之间的一系列部件的组合。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，能有效地监控流经防火墙的数据，保证内部网络和隔离区的安全。

防火墙可以是硬件也可以是软件，还可以是软硬件的组合。不管防火墙是何种形式，它本质上是一种访问控制机制。防火墙必须具备以下三个方面的基本特性：

- 内部网络和外部网络之间的所有数据流都必须经过防火墙；
- 能根据网络安全策略控制(允许、拒绝或监测)出入网络的信息流，且自身具有较强的网络抗攻击能力；
- 防火墙本身不会影响数据的流通。

1.1.2 防火墙的功能

一个典型的企业网络应用防火墙的拓扑结构如图 1.1 所示。在这样的拓扑结构中，网络被分为三个区域。

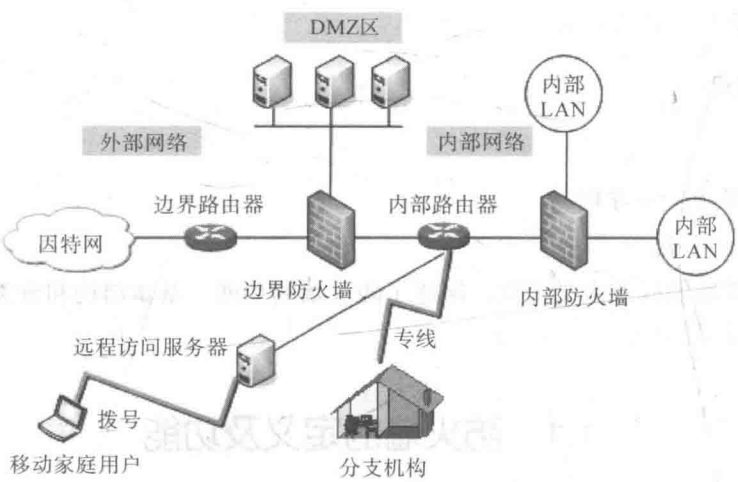


图 1.1　一个典型的企业网络应用防火墙的拓扑结构

1. 外部网络

外部网络部分包括互联网的主机和网络设备，此区域为防火墙的不可信公共网络部分。防火墙处于内部网络与外部网络的边界上，将对所有外部访问内部的通信按预先设置的规则进行监控、审核和过滤，不符合规则的通信将被拒绝通过，从而起到对内网的保护作用。

2. DMZ 区

DMZ(Demilitarized Zone，隔离区或非军事区)是指从内部网络中划分的一个小区域，专门用于放置既需被内部访问又需提供公众服务的服务器，如企业的 Web 服务器、E-mail 服务器、FTP 服务器、DNS 服务器等。此区域由于要提供对外服务，因而其被保护级别设置得较低。

3. 内部网络

内部网络是防火墙要保护的对象，包括内部网络中所有核心设备，如服务器、路由器、核心交换机及用户个人电脑。内部网络有可能包括不同的安全区域，具有不同等级的安全访问权限。虽然内部网络和 DMZ 区都属于内部网络的一部分，但它们的安全级别或策略是不同的。

以上网络拓扑结构中，部署了两种类型的防火墙，其中一类是边界防火墙，另一类是内部防火墙。

1) 边界防火墙

边界防火墙处于外部不可信网络(包括因特网、广域网和其他公司的专用网)与内部可信网络之间，控制来自外部不可信网络对内部可信网络的访问，防范来自外部网络的非法攻击。同时，边界防火墙保证了 DMZ 区服务器的相对安全性和使用的便利性。

目前所用的防火墙主要是边界防火墙。边界防火墙的主要功能有以下几个方面：

(1) 创建一个阻塞点。

防火墙在一个公司内部网络和外部网络间建立一个检查点。这种实现要求所有的流量都要通过这个检查点。一旦这些检查点清楚地建立，防火墙设备就可以监视网络，过滤和检查所有进出的流量。这样一个检查点，在网络安全行业中称之为“阻塞点”。通过强制所有进出流量都通过这些检查点，网络管理员可以集中在较少的地方来实现安全监测的目的。如果没有这样一个供监视和控制信息的点，系统或安全管理员则要在大量的地方来进行监测。

(2) 隔离不同网络，防止内部信息的外泄。

这是防火墙最基本的功能，它通过隔离内、外部网络来确保内部网络的安全，也限制了局部重点或敏感网络安全问题对全局网络造成的影响。企业秘密是大家普遍非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞，使用防火墙就可以隐蔽那些透漏内部细节信息的服务。例如，Finger 显示了主机的所有用户的注册名、真实名字，最后登录时间和使用 Shell 的类型等。但是 Finger 显示的信息非常容易被攻击者所截获，攻击者通过所获取的信息可以知道一个系统使用的频繁程度，以及这个系统是否有用户正在连线上网等信息。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解了。

(3) 强化网络安全策略。

通过以防火墙为中心的安全方案配置，能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更加经济，各种安全措施的有机结合，更能有效地对网络安全性能起到加强作用。

(4) 有效地审计和记录内、外部网络上的活动。

防火墙可以对内、外部网络存取和访问进行监控审计。如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并进行日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。这为网络管理人员提供了非常重要的安全管理信息，可以使管理员清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。

2) 内部防火墙

内部防火墙处于内部不同可信等级安全域之间，起隔离内部网络关键部门、子网或用户的作用。

内部防火墙的主要功能有以下几个方面：

- 可以精确制定每个用户的访问权限，保证内部网络用户只能访问必要的资源。
- 内部防火墙可以记录网段间的访问信息，及时发现误操作和来自内部网络其他网段的攻击行为。
- 通过集中的安全策略管理，使每个网段上的主机不必再单独设立安全策略，降低了因人为因素而导致的网络安全问题的可能性。

1.2　防火墙的基本结构

有的人认为防火墙的部署很简单，只要将防火墙的 LAN 口与企业内部网络连接，WAN 口与外部网络连接即可，其实这种看法是不正确的。由于用户的网络安全需求与防范目的不同，在实现具体的防火墙结构时，应进行不同的部署。一般防火墙有四种结构：屏蔽路由器防火墙、双宿主堡垒主机防火墙、屏蔽主机防火墙和屏蔽子网防火墙。

1.2.1　屏蔽路由器防火墙

屏蔽路由器防火墙结构是最初的防火墙结构方案，并不是采用专用的防火墙设备部署的，而是在原有的包过滤路由器上进行包过滤部署，因此又称之为包过滤路由器防火墙。这种防火墙应用结构如图 1.2 所示。

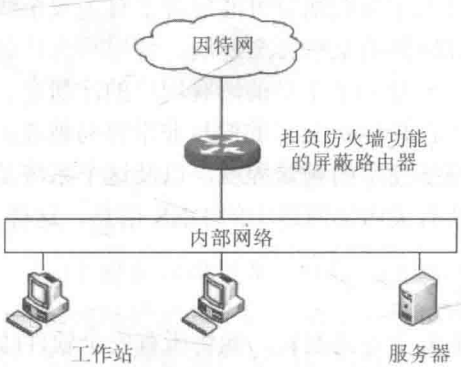


图 1.2　屏蔽路由器防火墙结构

在屏蔽路由器防火墙结构中，内部网络的所有出入都必须通过包过滤路由器，路由器审核每个数据包，依据过滤规则决定允许或拒绝数据包。

1.2.2　双宿主堡垒主机防火墙

双宿主堡垒主机防火墙结构用一台特殊主机来实现，这台主机也被称为堡垒主机。这台主机拥有两个不同的网络接口，一端接外部网络，另一端连接需要保护的内部网络，故称为双宿主机。此主机上运行着防火墙软件，可以转发应用程序、提供服务等，如图 1.3 所示。

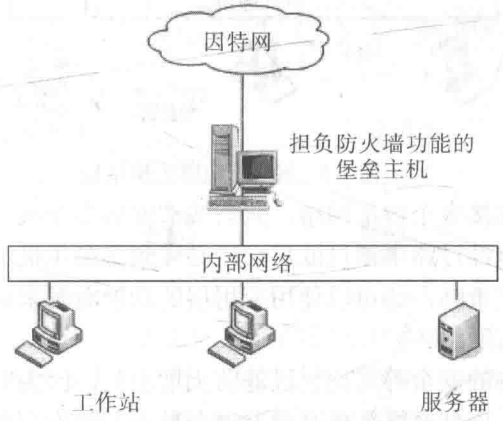


图 1.3　双宿主堡垒主机防火墙结构

双宿主堡垒主机防火墙结构优于屏蔽路由器防火墙结构，因为双宿主堡垒主机的系统软件可用于维护系统日志、硬件复制日志和远程日志，这对日后的检查很有用。但这不能帮助管理员确认哪些主机可能已被黑客入侵。

另外，双宿主堡垒主机防火墙的最大特点是 IP 层的通信是被阻止的，两个网络间的通信是靠应用层数据共享或应用层代理服务来实现的。该结构还应用于对多个内部网络或网段的安全防护，即一个堡垒主机可以同时连接着一个外网和多个内部网络，堡垒主机上需安装多个网卡。

双宿主堡垒主机是隔开内部和外部网络的唯一屏障，如果入侵者得到了双宿主机的访问权，就能迅速控制内部网络，因此双宿主机上只能安装小的服务，并设置较低的权限，以免被攻击者控制后对内部网络造成大的危害。

此外，双宿主机的角色决定了其性能非常重要，否则将影响外部用户对内部网络的访问。

1.2.3　屏蔽主机防火墙

屏蔽主机防火墙由屏蔽路由器和双宿主堡垒主机组成，是屏蔽路由器防火墙结构和双宿主堡垒主机防火墙结构的组合，如图 1.4 所示。

屏蔽主机防火墙使用一个屏蔽路由器，屏蔽路由器至少有一条路径，分别连接到非信任的网络和堡垒主机上。屏蔽路由器为堡垒主机提供基本的过滤服务，所有的 IP 数据包只有经过路由器过滤后才能到达堡垒主机。

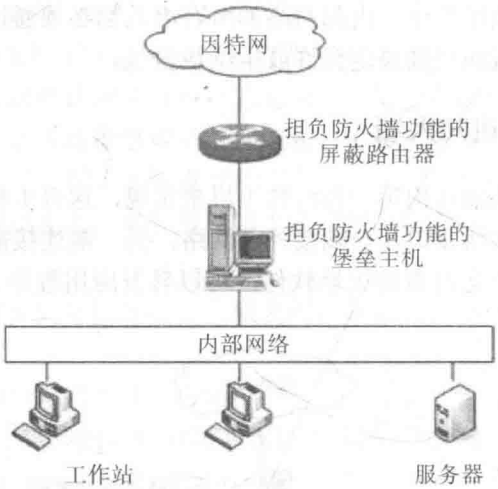


图 1.4　屏蔽主机防火墙结构

堡垒主机同样可以连接多个内部网络，只需按需安装多个网卡。

当外部网络的数据包经过路由器过滤后，还必须到堡垒主机上进行进一步检查。堡垒主机不仅可以使用网络层策略，还可以使用应用层的功能对发来的数据包进行检查，允许或者拒绝数据包进入内部网络。

屏蔽主机防火墙结构的安全等级比包过滤防火墙更高，因为它实现了网络层安全和应用层安全，入侵者在进入内部网络之前必须参透两种不同的安全系统。外部网络只能访问堡垒主机，去往内部网络的所有信息被阻断。

屏蔽主机防火墙存在一些问题，主要表现在如下三个方面：

(1) 屏蔽路由器成为安全关键点，也可能成为可信网络流量的瓶颈。

(2) 屏蔽路由器是否正确配置是防火墙安全与否的关键。屏蔽路由器的路由表必须正确防护，避免入侵者的修改。

(3) 禁止 ICMP 重新定向，以避免入侵者利用路由器对错误 ICMP 重定向消息的应答而攻击网络。

因此，在屏蔽主机防火墙结构中，堡垒主机有被绕过的可能，一旦堡垒主机被攻破，内部网络将完全暴露。

1.2.4　屏蔽子网防火墙

屏蔽子网防火墙使用一个或多个屏蔽路由器和堡垒主机，同时在内外网之间建立一个被隔离的子网，即 DMZ 区，这是当前应用最广泛的防火墙结构。屏蔽子网防火墙结构如图 1.5 所示。

屏蔽子网防火墙结构中存在三道防线，外部屏蔽路由器用于管理所有外部网络对 DMZ 区的访问，它只允许外部网络访问堡垒主机或 DMZ 区中对外开放的服务器，并防范来自外部网络的攻击。内部屏蔽路由器位于 DMZ 区与内部网络之间，提供第三层防御，它只接收来自堡垒主机的数据包，管理 DMZ 区到内部网络的访问，只允许内部网络访问 DMZ 区中的堡垒主机或服务器。

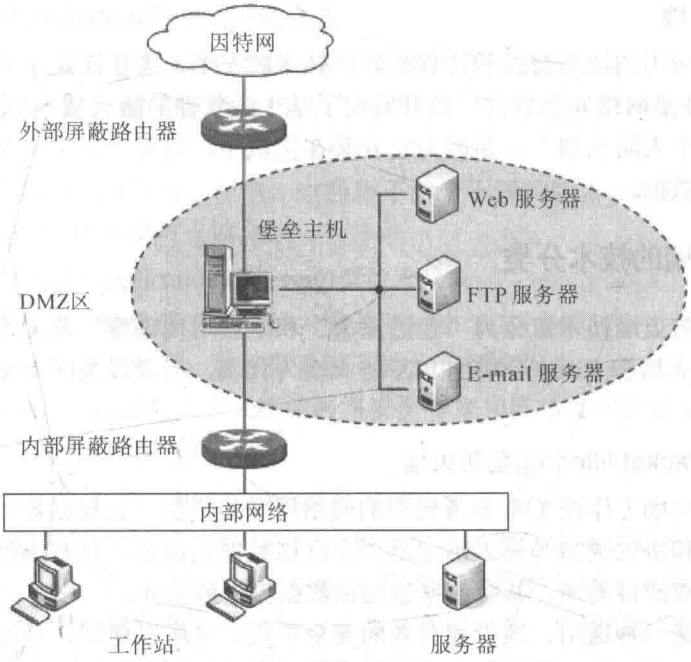


图 1.5　屏蔽子网防火墙结构

屏蔽子网防火墙系统的安全性很好，不管是外部网络访问内部网络的流量，还是内部网络访问外部网络的流量，都必须经过 DMZ 区子网并接受检查。

堡垒主机上可运行代理服务，是最容易受到入侵的，一旦堡垒主机被控制，可以屏蔽子网结构，在内部屏蔽路由器的保护下，保证内部可信网络的安全。当然，屏蔽子网防火墙结构也存在以下两点不足：

- 比其余结构所花的代价更高。
- 堡垒主机的配置更加复杂。

1.3　防火墙的分类

认识了防火墙的基本结构之后，我们就来对当前市场上的防火墙进行分类。目前市场上的防火墙产品非常之多，划分的标准也比较复杂，本节只对主流的分类标准进行介绍。

1.3.1　从防火墙的物理特性分类

很明显，如果从防火墙的物理特性来分，防火墙可以分为硬件防火墙和软件防火墙。

1. 硬件防火墙

最初的防火墙与我们平时所看到的集线器、交换机一样，都属于硬件产品。它在外观上与集线器和交换机类似，只有少数几个接口，分别用于连接内、外部网络，由防火墙的基本作用决定。

2. 软件防火墙

随着防火墙应用的逐步普及和计算机软件技术的发展，为了满足不同层次用户对防火墙技术的需求，许多网络安全软件厂商开发出了基于纯软件的防火墙，俗称“个人防火墙”。之所以说它是“个人防火墙”，是因为它安装在主机中，只对一台主机进行防护，而不是对整个网络进行防护。

1.3.2 从防火墙的技术分类

总体来讲，防火墙技术可分为“包过滤型”和“应用代理型”两大类。前者以以色列的 Checkpoint 防火墙和 Cisco 公司的 PIX 防火墙为代表，后者以美国 NAI 公司的 Gauntlet 防火墙为代表。

1. 包过滤(Packet filtering)型防火墙

包过滤型防火墙工作在 OS 参考模型的网络层和传输层，它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许该数据包通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则在数据流中被丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采取特殊的处理方式，它适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的；之所以有效，是因为它在很大程度上满足了绝大多数企业的安全要求。

在整个防火墙技术的发展过程中，包过滤技术出现了两种不同的版本，即第一代静态包过滤和第二代动态包过滤。

1) 第一代静态包过滤型防火墙

这类防火墙几乎是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制定。报头信息中包括 IP 源地址、IP 目标地址、传输协议(TCP、UDP、ICMP 等)、TCP/UDP 目标端口、ICMP 消息类型等。

2) 第二代动态包过滤型防火墙

这类防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为包状态监测(Stateful Inspection)技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目。

包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其弱点也是明显的：过滤判别的依据只是网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大的影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC 一类的协议；另外，大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常和应用网关配合使用，共同组成防火墙系统。

2. 应用代理(Application Proxy)型防火墙

应用代理型防火墙工作在 OSI 的最高层，即应用层。其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

在代理型防火墙技术的发展过程中，也经历了两个不同的版本，即第一代应用网关型防火墙和第二代自适应代理型防火墙。

1) 第一代应用网关(Application Gateway)型防火墙

这类防火墙是通过一种代理(Proxy)技术参与到一个 TCP 连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以达到隐藏内部网络结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术。

2) 第二代自适应代理(Adaptive Proxy)型防火墙

这类防火墙是近几年才得到广泛应用的一种新型防火墙。它可以结合代理型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高 10 倍以上。组成这种类型防火墙的基本要素有两个：自适应代理服务器(Adaptive Proxy Server)与动态包过滤器(Dynamic Packet Filter)。

在“自适应代理服务器”与“动态包过滤器”之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应 Proxy 的管理界面进行设置就可以了。然后，自适应代理会根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，以满足用户对速度和安全性的双重要求。

代理型防火墙的最突出的优点就是安全。由于它工作于最高层，所以它可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过滤。

另外，代理型防火墙采取的是一种代理机制，它可以为每一种应用服务建立一个专门的代理，所以内外部网络之间的通信不是直接的，而都需先经过代理服务器审核，通过后再由代理服务器代为连接，根本没有给内、外部网络计算机任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网络。包过滤型防火墙是很难彻底避免这一漏洞的。就像你要向一个陌生人递交一份声明一样，如果你先将这份声明交给你的律师，然后律师就会审查你的声明，确认没有什么负面的影响后才由他将此声明交给那个陌生人。在此期间，陌生人对你的存在一无所知，因为他仅与你的律师进行交接。如果他要对你进行侵犯，他直接面对的将是你的律师，而你的律师当然比你更加清楚该如何对付这种人。

1.3.3　从防火墙的应用部署分类

如果按防火墙的应用部署位置划分，防火墙可以分为边界防火墙、混合防火墙、个人防火墙三大类。