信息安全产品技术丛书

防火墙产品原理与应用

丛书主编　顾健

主编　张艳　俞优　沈亮　陆臻

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息安全产品技术丛书

防火墙产品原理与应用

丛书主编　顾健
主编　张艳　俞优　沈亮　陆臻

阜阳师范学院图书馆
藏书

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书共 5 章，从防火墙产品的技术实现和标准介绍入手，对其产生需求、发展历程、实现原理、技术标准、应用场景和典型产品等内容进行了全面翔实的介绍。

本书适合防火墙产品的使用者（系统集成商、系统管理员）、产品研发人员及测试评价人员作为技术参考，也可供信息安全专业的大学生及其他科研人员参考。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

防火墙产品原理与应用/张艳等主编. —北京：电子工业出版社，2016.1
（信息安全产品技术丛书）
ISBN 978-7-121-27855-6

Ⅰ. ①防… Ⅱ. ①张… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 301392 号

策划编辑：李 洁
责任编辑：万子芬 特约编辑：徐 宏
印 刷：三河市双峰印刷装订有限公司
装 订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：720×1000 1/16 印张：16 字数：296 千字
版 次：2016 年 1 月第 1 版
印 次：2016 年 1 月第 1 次印刷
印 数：3 000 册 定价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着越来越多重要的信息应用以互联网作为运行基础，用户面临的威胁形形色色，各类网络安全问题日益突出，计算机病毒、协议缺陷、系统脆弱性、各类攻击等直接导致网络安全形势日趋严峻。如何有效地防御网络安全威胁，让网络连接更安全？

防火墙技术作为保护计算机网络安全的最常用技术之一，在不危及内部网络数据和其他资源的前提下，允许本地用户使用外部网络资源，并将外部未被授权的用户屏蔽在内部网络之外，从而解决因连接外部网络所带来的安全问题。

防火墙产品经历了怎样的发展历程？防火墙产品的各项防护功能是如何实现的？本书就是带着这些问题展开陈述的。

本书是信息安全产品技术丛书之一。本书在产品需求、发展历程、实现原理、技术标准、应用等几方面均有翔实的描述。与此同时，本书力求实用，收集了许多实际数据与案例，期望能够给读者在防火墙产品的安全防护技术和标准的了解方面予以一定的帮助。

本书的主要编写成员均来自公安部计算机信息系统安全产品质量监督检验中心，他们常年从事防火墙产品等信息安全产品的测评工作，对防火墙产品有深入的研究。部分作者全程参与了新型防火墙产品标准从规范、行标到国标的制定、修订工作，因此，本书在标准介绍和描述方面具有一定的权威性。

本书由顾健作为丛书主编，负责把握全书技术方向，第 1 章由张艳编写，第 2 章由俞优、沈亮编写，第 3 章由张艳编写，第 4、5 章由沈亮、陆臻编写。此外，顾建新、王志佳、冯婷婷、武滕等同志也参与了本书资料的收集和部分编写工作。由于编写人员水平有限和时间紧迫，本书不足之处在所难免，恳请各位专家和读者不吝批评指正。

本书的编写得到了北京天融信网络安全技术有限公司、华为技术服务有限公司和珠海经济特区伟思有限公司的大力协助，在此表示衷心的感谢！

编　者

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章 综 述

信息化时代的飞速发展为人们的生活带来了越来越多的便捷，但是，网络互联互通的开放性特性极大地方便了各种资源的联网，开创和拓宽了共享资源的途径，同时，随着人类在经济、工业、军事领域方面越来越多地依赖信息化管理和处理，由于信息网络在设计上对安全问题的忽视，以及爆发性应用背后存在的使用和管理上的脱节，使互联网中信息的安全性逐渐受到严重威胁，实用和安全矛盾逐渐显现。随着越来越多重要的信息应用以互联网作为运行基础，信息安全问题已经成为威胁民生、社会、甚至国家安全的重要问题。

1.1 为什么要防火墙产品

1.1.1 网络面临的安全威胁

随着计算机网络的普及，各类网络安全问题日益突出。自莫里斯蠕虫病毒出现以来，病毒的数量呈爆炸式增长，病毒传播的趋利性日益突出，病毒的破坏性及反查杀能力不断增强。安全漏洞数量增长较快，系统或软件的严重级别漏洞增多，各类安全漏洞并未引起足够的重视。

近年来计算机网络面临的威胁越来越多，人为的攻击事件数量呈剧烈上升趋势。然而，各种信息在公共通信网络上存储、传输，可能会被怀有各种目的的攻击者非法窃听、截取、篡改或毁坏，从而导致不可估量的损失。对于银行系统、商业系统、政府或军事领域而言，这些比较敏感的系统或部门对公共通信网络中存储与传输的数据安全问题尤为关注。

1. 网络协议和软件的安全缺陷

互联网的基石是 TCP/IP 协议簇，该协议簇在实现上力求效率，而没有考虑安全因素，因为那样无疑会增大代码量，从而降低 TCP/IP 的运行效率，所以说 TCP/IP 本身在设计上就是不安全的。

2. 计算机病毒

计算机病毒是专门用来破坏计算机正常工作，具有高级技巧的程序。它并不独立存在，而是寄生在其他程序之中，它具有隐蔽性、潜伏性、传染性和极大的破坏性。随着网络技术的不断发展、网络空间的广泛运用，病毒的种类急剧增加。目前全世界的计算机活体病毒达 14 万多种，其传播途径不仅通过软盘、硬盘传播，还可以通过网络的电子邮件和下载软件传播。只要带病毒的计算机在运行过程中满足设计者所预定的条件，计算机病毒便会发作，轻者造成速度减慢、显示异常、丢失文件，重者损坏硬件、造成系统瘫痪。

3. 身份信息窃取

任何人都可能成为身份信息窃取的受害者。在某些情况下，网络罪犯通过要求在电子邮件中或从该邮件链接到的网站上提供的信息，即可直接获得有关个人信息。在其他情况下，网络罪犯通过黑客入侵企业（如零售商或政府机构等）管理的大型数据库，同时窃取许多的个人信息。

4. 网络钓鱼诈骗

网络罪犯经常通过看似来自合法公司的电子邮件中的链接获取个人信息。这称为“网络钓鱼诈骗”。这些不法之徒使用来自合法公司或组织的邮件，蒙骗获取用户密码和其他信息，以便盗取用户的钱财或以用户的名义购物。

5. 分布式拒绝服务（DDoS）

分布式拒绝服务是利用多台计算机同时攻击一台服务器（如网站的服务器），

使服务器陷入瘫痪或停止正常运行。许多 DDoS 攻击可能利用多台 PC 发起攻击，这些 PC 由 BOT 控制者控制，将 PC 用作单个僵尸。

1.1.2　网络安全的实现

1. 访问控制

访问控制是网络安全防御和保护的主要策略。进行访问控制的目的是保证网络资源不被非法使用和非法访问。控制用户可以访问网络资源的范围，为网络访问提供限制，只允许具有访问权限的用户访问网络资源。

2. 数据加密技术

随着当前通信技术的快速发展，用户对信息的安全处理、安全存储、安全传输的需要也越来越迫切，并受到了广泛关注。信息在网络传输的安全威胁是由于 TCP/IP 协议所固有的，因此数据加密技术成为实现计算机网络安全技术的必然选择。

3. 病毒防护

病毒防护主要包括计算机病毒的预防、检测与清除。最理想的防止病毒攻击的方法就是预防，在第一时间内阻止病毒进入系统。

4. 攻击防御

攻击防御对网络及网络设备的传输行为进行实时监视，在恶意行为被发动时及时进行阻止，攻击防御可以针对特征分析及行为分析做出判断。

5. 完善安全管理制度

任何网络都没有 100%的安全，网络安全建设是“三分技术，七分管理”。因此，除了运用各种安全技术之外，还要建立一系列安全管理制度。制订严格的网络管理制度、安全设备的访问控制措施、机房管理制度、应急响应方案等，并

此为试读，需要完整PDF请访问：www.ertongbook.com

加强对软件及操作的管理。

1.1.3 采用防火墙系统的必要性

从计算机网络安全技术的角度来看，防火墙是指强加于两个网络之间边界处，以保护内部网络免遭外部网络威胁的系统或者系统组合。防火墙技术作为保护计算机网络安全的最常用技术之一，当前全球约有三分之一的计算机是处于防火墙的保护之下。防火墙在不危及内部网络数据和其他资源的前提下，允许本地用户使用外部网络资源，并将外部未被授权的用户屏蔽在内部网络之外，从而解决了因连接外部网络所带来的安全问题。

1.2 防火墙发展历程

1.2.1 防火墙技术的发展

防火墙技术经历了包过滤、应用代理网关、状态检测几个重要阶段，下面简要介绍一下其技术特点。

1. 包过滤技术

包过滤防火墙工作在网络层，对数据包的源及目的 IP 具有识别和控制作用，对于传输层，也只能识别数据包是 TCP 还是 UDP 及所用的端口信息。现在的路由器、带有路由功能的路由器以及通用操作系统基本都具有包过滤（Packet Filter）控制的能力。

包过滤防火墙具有的缺陷：

（1）不支持应用层协议。假如内网用户提出这样一个需求，只允许内网员工访问外网的网页（使用 HTTP 协议），不允许去外网下载电影（一般使用 P2P 协议），这时包过滤防火墙无能为力，因为它不认识数据包中的应用层协议，访

问控制粒度太粗糙。

（2）不能处理新的安全威胁。它不能跟踪 TCP 状态，所以对 TCP 层的控制有漏洞。如当它配置了仅允许从内到外的 TCP 访问时，一些以 TCP 应答包的形式从外部对内网进行的攻击仍可以穿透防火墙。

2. 应用代理网关技术

应用代理网关防火墙彻底隔断内网与外网的直接通信，内网用户对外网的访问变成防火墙对外网的访问，然后再由防火墙转发给内网用户。所有通信都必须经应用层代理软件转发，访问者任何时候都不能与服务器建立直接的 TCP 连接，应用层的协议会话过程必须符合代理的安全策略要求。

应用代理网关的优点是可以检查应用层、传输层和网络层的协议特征，对数据包的检测能力比较强。

缺点也非常明显，主要有：

（1）难以配置。由于每个应用都要求单独代理进程，这就要求网管能理解每项应用协议的弱点，并能合理配置安全策略，由于配置烦琐，难以理解，容易出现配置失误，最终影响内网的安全防范能力。

（2）处理速度非常慢。断掉所有的连接，由防火墙重新建立连接，理论上可以使应用代理防火墙具有极高的安全性，但是实际应用中并不可行，因为对于内网的每个 Web 访问请求，应用代理都需要开一个单独的代理进程，它要保护内网的 Web 服务器、数据库服务器、文件服务器、邮件服务器及业务程序等，就需要建立一个个的服务代理，以处理客户端的访问请求。这样，应用代理的处理延迟会很大，内网用户的正常 Web 访问不能及时得到响应。

3. 状态检测技术

我们知道，Internet 上传输的数据都必须遵循 TCP/IP 协议，根据 TCP 协议，

每个可靠连接的建立需要经过“客户端同步请求”、“服务器应答”、“客户端再应答”三个阶段，我们最常用到的 Web 浏览、文件下载、收发邮件等都要经过这三个阶段。这反映出数据包并不是独立的，而是前后之间有着密切的状态联系，基于这种状态变化，引出了状态检测技术。

状态检测防火墙摒弃了包过滤防火墙仅考查数据包的 IP 地址等几个参数，而不关心数据包连接状态变化的缺点，在防火墙的核心部分建立状态连接表，并将进出网络的数据当成一个个的会话，利用状态表跟踪每一个会话状态。状态监测对每一个包的检查不仅根据规则表，更考虑了数据包是否符合会话所处的状态，因此提供了完整的对传输层的控制能力。

网关防火墙的一个挑战就是能处理的流量，状态检测技术在大大提高安全防范能力的同时也改进了流量处理速度。状态检测技术采用了一系列优化技术，使防火墙性能大幅度提升，能应用在各类网络环境中，尤其是在一些规则复杂的大型网络上。

1.2.2 防火墙发展的新技术趋势

1. 高性能

随着运营商、金融、大型企业的数据中心等用户对安全的关注，对防火墙高吞吐量、高性能连接处理能力的要求越来越迫切。对动辄十吉字节，几十吉字节的流量来说，传统的硬件架构已无法满足用户的需求，因此多核处理，ASIC 加速芯片处理等技术纷纷登场。

2. 适用于 IPv4/6 环境

随着 IPv6 的推广与普及，一方面，现有的信息安全产品必须适应 IPv6 的网络环境；另一方面，随着 IPv6 使用时间的延伸，新的安全问题将逐渐暴露，新的安全防护技术也将逐渐产生。虽然在纯 IPv6 网络中，IPv6 端与端的 IPSec 以及最终摆脱 NAT 的发展构架对防火墙产品的冲击影响较大，但在 IPv4/6 共存阶

段，针对不同过渡协议混杂的背景，防火墙产品还是有着技术发展和实现的需求。

3. 应用层深度控制技术

随着网络大量新业务的推出，网络带宽被越来越多的业务流量占据。防火墙用户对其业务的关注度越来越高，在此环境下，基于深度控制技术的防火墙开始越来越多被提及。此类防火墙的特点是基于用户的策略配置，业务展现友好，具有强大的应用层控制能力和内容分析能力。

4. 虚拟化技术

随着云时代的到来，各类云服务逐渐进入普通大众的生活。伴随着云服务而来的也有新的风险及机遇。防火墙作为基础的网络安全产品，伴随着云技术的发展，作为云服务平台的虚拟化技术也在高端防火墙产品中出现。

1.2.3　其他新型防火墙

1. Web 应用防火墙

Web 应用防火墙是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。

Web 应用防火墙具有以下四大个方面的功能。

（1）审计设备：用来截获所有 HTTP 数据或者仅仅满足某些规则的会话。

（2）访问控制设备：用来控制对 Web 应用的访问，既包括主动安全模式也包括被动安全模式。

（3）架构/网络设计工具：当运行在反向代理模式，它们被用来分配职能、集中控制、虚拟基础结构等。

（4）Web 应用加固工具：这些功能增强被保护 Web 应用的安全性，它不仅

能够屏蔽 Web 应用固有弱点，而且能够保护 Web 应用编程错误导致的安全隐患。

2. 数据库防火墙

数据库防火墙技术是针对关系型数据库保护需求应运而生的一种数据库安全主动防御技术，数据库防火墙部署于应用服务器和数据库之间。用户必须通过该类防火墙才能对数据库进行访问或管理。

数据库防火墙的特点如下所述。

（1）屏蔽直接访问数据库的通道：数据库防火墙部署介于数据库服务器和应用服务器之间，屏蔽直接访问的通道，防止数据库隐通道对数据库的攻击。

（2）攻击保护：实时检测用户对数据库进行的 SQL 注入和缓冲区溢出攻击，并报警或者阻止攻击行为，同时详细审计攻击操作发生的时间、来源 IP、登录数据库的用户名、攻击代码等详细信息。

（3）细粒度权限控制：按照 SQL 操作类型包括 Select、Insert、Update、Delete，对象拥有者，以及基于表、视图对象、列进行权限控制。

（4）安全审计：系统能够审计对数据库服务器的访问情况，包括用户名、程序名、IP 地址、请求的数据库、连接建立的时间、连接断开的时间、通信量大小、执行结果等信息，并提供灵活的回放日志查询分析功能，可以生成报表。

3. 工业控制防火墙

随着信息技术的迅猛发展，信息化在企业中的应用取得了飞速发展，互联网技术的出现，使得工业控制网络中大量采用通用 TCP/IP 技术，ICS 网络和企业管理网的联系越来越紧密。另一方面，传统工业控制系统采用专用的硬件、软件和通信协议，设计上基本没有考虑互联互通所必须考虑的通信安全问题，工控系统的安全隐患问题日益严峻。

工业控制防火墙的特点所下所述。

（1）支持专用工业通信协议：与常规防火墙不同的是，工业防火墙是基于内置工业通信协议的防护模式，由于工业通信协议通常是基于常规 TCP/IP 在应用层的高级开发，所以该防火墙不仅是在端口上的防护，更重要的是基于应用层上数据包深度检查，为工业通信提供独特的、工业级的专业隔离防护。

（2）工业型设计：硬件安装设计、环境温度要求、功耗散热、体积接口等方面需要符合工业要求。

（3）实时报警识别：由于工业生产的特殊性，任何非法的（未被允许的）访问都需要产生明确的、有效的、实时的报警信息，从而故障问题会在原始发生区域被迅速发现和正确解决，防止故障对生产网络的扩散影响。

此为试读，需要完整PDF请访问：www.ertongbook.com