教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

360企业安全集团组织编写

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥 编委会主任：封化民

防火墙技术及应用

杨东晓 张锋 熊瑛 任晓贤 雷敏 编著

Cyberspace Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

防火墙技术及应用

杨东晓 张锋 熊瑛 任晓贤 雷敏 编著

清华大学出版社
北京

内 容 简 介

本书全面介绍防火墙技术及应用知识。全书共5章，主要内容包括防火墙基本知识、防火墙技术、防火墙网络部署、防火墙安全功能应用和典型案例。每章最后提供了相应的思考题。

本书由360企业安全集团针对高校网络空间安全专业的教学规划组织编写，既适合作为网络空间安全、信息安全等专业的本科生相关专业基础课程的教材，也适合作为网络安全研究人员的入门基础读物。

图书在版编目(CIP)数据

防火墙技术及应用/杨东晓等编著. —北京：清华大学出版社，2019
(网络空间安全重点规划丛书)
ISBN 978-7-302-51961-4

Ⅰ. ①防… Ⅱ. ①杨… Ⅲ. ①防火墙技术 Ⅳ. ①TP393.082

中国版本图书馆CIP数据核字(2018)第291013号

责任编辑：张　民　战晓雷
封面设计：常雪影
责任校对：李建庄
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：10　　**字　　数**：227千字
版　　次：2019年1月第1版　　**印　　次**：2019年1月第1次印刷
定　　价：29.00元

产品编号：080620-01

网络空间安全重点规划丛书

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。系列教材的作者都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

该系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到系列教材中，以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会

暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006 年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007 年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时 5 年，制定出我国第一个信息安全专业指导性专业规范，于 2012 年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013 年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014 年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015 年 6 月，国务院学位委员会、教育部出台增设“网络空间安全”为一级学科的决定，将高校培养网络空间安全人才提到新的高度。2016 年 6 月，中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文〔2016〕4 号)。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》，进一步深化高等教育教学改革，促进网络安全学科专业建设和人才培养，促进网络空间安全相关核心课程和教材建设，在教育部高等学校信息安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下，启动了“网络空间安全重点规划丛书”的工作，由教育部高等学校信息安全专业教学指导委员会秘书长封化民校长担任编委会主任。本规划丛书基于“高等院校信息安全专业系列教材”坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍，目前已经有多本图书获得教育部和中央网信办等机构评选的“普通高等教育本科国家级规划教材”“普通高等教育精品教材”“中国大学出版社图书奖”和“国家网络安全优秀教材奖”等多个奖项。

“网络空间安全重点规划丛书”将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国网络空间安全学科的发展不断完善，力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn，联系人：张民。

“网络空间安全重点规划丛书”编审委员会

前言

没有网络安全，就没有国家安全；没有网络安全人才，就没有网络安全。

为了更多、更快、更好地培养网络安全人才，如今许多学校都在努力培养网络安全人才，都在下大功夫、花大本钱，聘请优秀老师，招收优秀学生，建设一流的网络空间安全专业。

网络空间安全专业建设需要体系化的培养方案、系统化的专业教材和专业化的师资队伍。优秀教材是网络空间安全专业人才培养的关键。但是，这是一项十分艰巨的任务。原因有二：其一，网络空间安全的涉及面非常广，至少包括密码学、数学、计算机、通信工程、信息工程等多门学科，因此，其知识体系庞杂，难以梳理；其二，网络空间安全的实践性很强，技术发展更新非常快，对环境和师资要求也很高。

“防火墙技术及应用”是网络空间安全和信息安全专业的基础课程，全面介绍防火墙技术及应用知识。全书共5章。第1章介绍防火墙基本知识，第2章介绍防火墙技术，第3章介绍防火墙网络部署，第4章介绍防火墙安全功能应用，第5章介绍典型案例。

本书既适合作为网络空间安全、信息安全等专业的本科生相关专业基础课程的教材，也适合作为网络安全研究人员的入门基础读物。本书将随着新技术的发展而更新。

由于作者水平有限，书中难免存在疏漏和不妥之处，欢迎读者批评指正。

作　者

2018年11月

目录

第1章 防火墙基本知识

本章主要介绍防火墙的基础知识。通过本章的学习，应理解防火墙产生的原因、防火墙的历史及发展趋势、安全域的基本概念和边界防御思想、防火墙产品标准、下一代防火墙的体系结构。

1.1 防火墙概述

1.1.1 防火墙产生的原因

网络的发展在为人们的工作和生活带来极大便利的同时也带来各种安全隐患。攻击者利用网络协议和软件安全漏洞对信息系统进行攻击；各种计算机病毒和木马程序在网络上传播，危害信息系统；攻击者盗取各种隐私信息，给公民的财产造成巨大损失；日益频发的网络安全问题给人们日常工作和生活带来极大威胁。

把不同安全级别的网络相连接，就产生了网络边界。例如，企业内部的网络和外部网络就是两种不同安全级别的网络，这两种不同安全级别的网络中间就是网络边界。从网络安全技术的角度来看，防火墙位于网络边界处，是保护内部网络免遭外部网络威胁的系统或者系统的组合，这些组合可以是硬件、软件或者是软硬件的组合。其中，软件形式的防火墙安装灵活，便于升级扩展，但其安全性受限于操作系统平台；硬件形式的防火墙基于特定用途的集成电路开发，性能优越，但其可扩展性差；软硬件结合的防火墙性能较高，也具有一定的可扩展性和灵活性。

网络边界是安全防护的重要阵地，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，从而解决了因内部网络用户连接外部网络所带来的安全问题和外部网络中恶意的攻击者恶意攻击内部网络各种资源的安全问题。防火墙技术是保护网络安全最常用的技术之一。

1.1.2 防火墙定义

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(security zone)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。防火墙结构示意图见图 1-1。

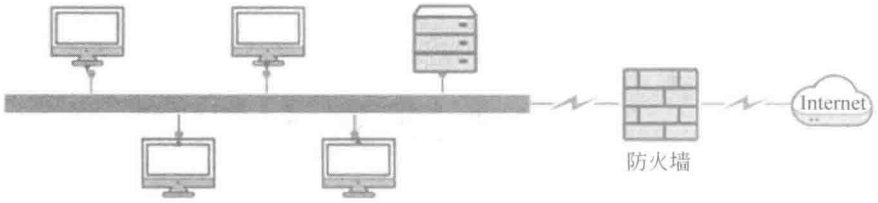

图 1-1　防火墙结构示意图

在 2015 年我国发布的编号为 GB/T 20281—2015 国家标准《信息安全技术　防火墙安全技术要求和测试评价方法》中对防火墙的定义为“部署于不同安全域之间，具备网络层访问控制及过滤功能，并具备应用层协议分析、控制及内容检测等功能，能够适用于 IPv4、IPv6 等不同的网络环境的安全网关产品”。

随着技术的不断进步，防火墙逐步发展到下一代防火墙，下一代防火墙可以全面应对应用层威胁，通过深入洞察网络流量中的用户、应用和内容，并借助全新的高性能单路径异构并行处理引擎，能够为用户提供有效的应用层一体化安全防护，帮助用户安全地开展业务并简化用户的网络安全架构。

1.1.3　防火墙的作用

随着防火墙的不断发展，其功能越来越丰富，但是防火墙最基础的两大功能仍然是隔离和访问控制。隔离功能就是在不同信任级别的网络之间砌“墙”，而访问控制就是在墙上开“门”并派驻守卫，按照安全策略来进行检查和放行。一个典型的企业网防火墙部署如图 1-2 所示。

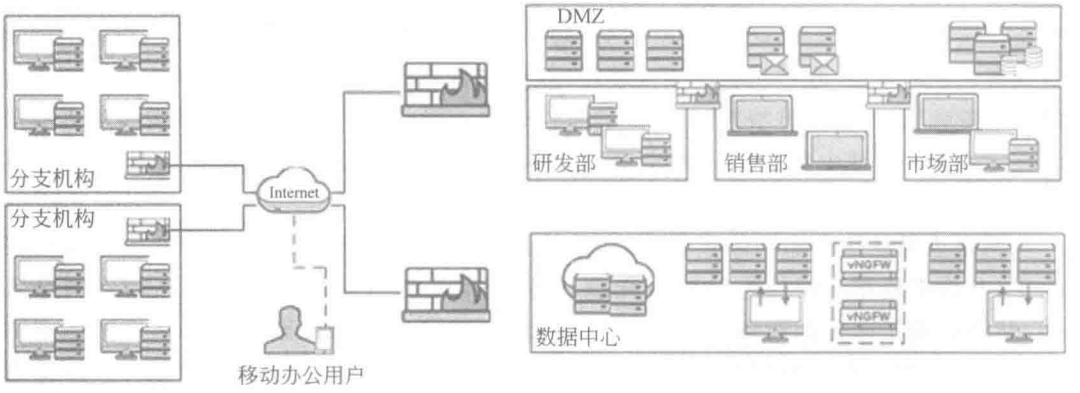

图 1-2　典型的企业网防火墙部署示例

防火墙的主要作用通常包括以下几点。

1. 提供基础组网和防护功能

防火墙能够满足企业环境的基础组网和基本的攻击防御需求。防火墙可以实现网络连通并限制非法用户发起的内外攻击，比如黑客、网络破坏者等，禁止存在安全脆弱性的服务和未授权的通信数据包进出网络，并对抗各种攻击。

2. 记录和监控网络存取与访问

作为单一的网络接入点，所有进出信息都必须通过防火墙，所以防火墙可以收集关于系统和网络使用和误用的信息并做出日志记录。通过防火墙可以很方便地监视网络的安全性，并在异常时给出报警提示。

3. 限定内部用户访问特殊站点

防火墙通过用户身份认证（如 IP 地址等）来确定合法用户，并通过事先确定的完全检查策略来决定内部用户可以使用的服务以及可以访问的网站。

4. 限制暴露用户点

利用防火墙对内部网络的划分，可实现网络中网段的隔离，防止影响一个网段的问题通过整个网络传播，从而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，同时保护一个网段不受来自网络内部其他网段的攻击，保障网络内部敏感数据的安全。

5. 网络地址转换

防火墙可以作为部署 NAT（Network Address Translation，网络地址转换）的逻辑地址来缓解地址空间短缺的问题，并消除在变换 ISP（Internet Service Provider，互联网服务提供商）时带来的重新编址的麻烦。

6. 虚拟专用网

防火墙还支持具有 Internet 服务特性的企业内部网络技术体系——虚拟专用网络（Virtual Private Network，VPN）。通过 VPN 将企事业单位在地域上分布在世界各地的局域网或专用子网有机联成一个整体。

1.2　防火墙的前世今生

1.2.1　防火墙发展历史及分类

防火墙的发展大致经历了第一代、第二代、第三代、第四代、第五代、统一威胁管理和下一代防火墙 7 个重要阶段。从第一代防火墙出现至今已有三十多年的历史，在发展过程中，不断发展的网络技术对防火墙也提出各种新需求，这些新需求推动着防火墙向前不断发展演进。下面简要介绍防火墙的发展历史。

1. 第一代防火墙

第一代防火墙采用静态包过滤（statics packet filter）技术，是依附于路由器的包过滤功能实现的防火墙，称为包过滤防火墙。随着网络安全的重要性和对防火墙性能要求的提高，防火墙逐渐发展成为一个独立结构的、有专门功能的设备。包过滤防火墙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相匹配。包过滤类型的防火墙遵循“最小特权原则”，即允许管理员通过设定策略决定数据包是否能通过防火墙。

2. 第二代防火墙

贝尔实验室在1989年推出第二代防火墙。第二代防火墙也称电路层防火墙，通过使用TCP连接将可信任网络中继到非信任网络来工作，但是客户端和服务器之间是不会直接连接的。电路层防火墙不能感知应用协议，必须由客户端提供连接信息。

3. 第三代防火墙

贝尔实验室在1989年同时提出了第三代防火墙，也就是应用层防火墙（也称代理防火墙）的初步结构。应用层防火墙通过代理服务实现防火墙内外计算机系统的隔离。

4. 第四代防火墙

1992年，美国南加利福尼亚大学信息科学院的Bob Braden开发了基于动态包过滤（dynamic packet filter）技术的第四代防火墙。这一类型的防火墙采用动态设置包过滤规则的方法，避免了静态包过滤技术的问题，依据设定好的过滤逻辑，检查数据流中的每个数据包，根据数据包的源地址、目标地址以及数据包所使用的端口确定是否允许该类型的数据包通过。1994年，市面上出现了第四代防火墙产品，即以色列CheckPoint公司推出的基于这种技术的商业化产品。

5. 第五代防火墙

1998年，NAI公司推出了一种自适应代理（adaptive proxy）技术，并在其产品Gauntlet Firewall for NT中得以实现，给代理类型的防火墙赋予了全新的意义，人们将其称为第五代防火墙。

6. 统一威胁管理

2004年，国际数据公司（IDC）提出统一威胁管理（United Threat Management，UTM）的概念，即将防病毒、入侵检测和防火墙安全设备划归统一威胁管理。从这个定义上来看，IDC既提出了UTM产品的具体形态，又涵盖了更加深远的逻辑范畴。从定义的前半部分来看，众多安全厂商提出的多功能安全网关、综合安全网关、一体化安全设备等产品都可被划归到UTM产品的范畴；而从定义的后半部分来看，UTM的概念还体现出信息产业经过多年发展之后对安全体系的整体认识和深刻理解。

2004年后，UTM市场得到了快速的发展，但也面临新的问题。首先是应用层信息的检测程度受到限制；其次是性能问题，因为UTM中多个功能同时运行，设备的处理性能将会严重下降。

7. 下一代防火墙

2008年，Palo Alto Networks公司发布了下一代防火墙，解决了多个功能同时运行时性能下降的问题，同时还可基于用户、应用和内容进行管控。

2009年，权威咨询机构Gartner提出了以应用感知和全栈可视化、深度集成IPS、适用于大企业环境并集成外部安全智能为主要技术特点的下一代防火墙产品定义雏形，这是“下一代防火墙”这一技术名词被首次提出。

Gartner在这份名为*Defining the Next-Generation Firewall*的报告中提出了以下

重要观点：

(1) 下一代防火墙应具备对网络应用的感知和识别能力，实现完全抛开协议端口的应用可视化和应用控制。

(2) 集成具有高质量的 IPS 引擎和特征码，是下一代防火墙的一个重要特征，IPS 应被深度集成到下一代防火墙中，和应用识别能力一样，成为下一代防火墙的一个基本能力，而并非将这些功能简单堆砌并独立管理、独立运行。

(3) 下一代防火墙包含基础防火墙的全部功能，并深度集成了 IPS 功能。随着传统防火墙、IPS 的自然更新，一部分用户可以考虑使用下一代防火墙替代传统防火墙或 IPS 设备。

(4) 下一代防火墙并不是以中小企业用户为主要目标市场的多功能防火墙或统一威胁管理设备。

阻断越权访问和恶意连接，并提供可预测的功能，是用户对安全网关设备最基本的功能预期。通过设置适当的安全策略，对企业的业务流量进行最小特权和白名单模式的放行，并实时检测存在于被允许流量中的威胁，是安全网关产品部署的最佳实践。下一代防火墙出现的原动力是为了在新的威胁环境下更好地满足上述要求。传统的防火墙、统一威胁管理产品在越来越多的场景下呈现出以下不足：

(1) 基于网络层操作的传统防火墙只能根据数据的 IP 地址、协议、端口信息来检测流量。随着网络应用的爆炸式发展，以及大量应用程序建立在 HTTP 或 HTTPS 等协议之上，传统防火墙已无法满足用户对业务流量可视和可控的需求。

(2) 漏洞利用、间谍软件、僵尸网络等应用层攻击已成为主流，此类攻击能够以业务流量为载体，传统防火墙依靠数据包头异常、连接频度等检测手段已无法识别此类威胁，利用 IPS 引擎对数据包的载荷部分进行深入检测已成为必要手段。

(3) 在下一代防火墙提出之前，市场上已存在集多种安全功能于一体的安全网关设备，但由于功能的简单堆砌，设备在开启较多安全功能之后性能衰减严重，并不能满足大企业环境对安全设备性能可预测性的需要。

从市场需求来看，下一代防火墙顺应安全局势而生，新产品品类的出现已是必然。

近些年，各个安全厂商也推出了各自的下一代防火墙产品，防火墙进入了一个新的时代。业界对下一代防火墙也有了更准确的定义：下一代防火墙是部署于两个或多个计算机网络间，以应用、用户和内容识别为基本能力，在对网络流量深度可视化的基础上，通过统一策略管理确保在网络间安全启用应用的安全设备。此外，下一代防火墙应提供多维的信息关联，具有风险感知、异常分析和事件回溯功能，并能与外部的智能系统联动。

1.2.2　防火墙的新技术趋势

未来几年，下一代防火墙的技术发展趋势将重点体现在以下方面。

1. 应用识别能力提升

在“互联网＋”时代，网络应用的发展空前繁盛，网络中的应用数量呈几何级数增长。下一代防火墙要向用户提供深度可视化和精细化控制的功能，必须建立在对网络应用和

应用内容全面、准确识别的基础之上。因此，下一代防火墙对网络流量的识别广度、深度和精度将随着应用数量、复杂程度的变化而持续提升。

2. 可视化能力提升

随着威胁环境的变化，安全能力正在由防范为主向快速检测和响应能力的构建转换。实现安全启用应用，首先应“看见”应用，其次是在此基础上持续监控和感知应用的风险、异常变化等，这些信息将为制定适合企业业务的安全策略提供基础的决策依据。下一代防火墙对于网络流量、应用风险和情境的可见性将直接决定其安全性和有效性。未来，下一代防火墙将持续提升其可视化能力，以满足用户要求越来越高的网络全局“能见度”的需求。

3. 智能化程度提升

安全防护正逐步从“个体或单个组织”的防护方式转变为“安全情报驱动”的信息共享和集体协作方式。依靠下一代防火墙单点的防护并不足以实现安全，下一代防火墙会融合更加丰富的安全功能，并与其他外部的安全智能系统实现无缝联动，如联动沙箱、威胁情报检测、基于云计算的安全信誉机制、基于大数据的异常行为分析技术等，以提高其对策略执行的判断力和事件响应的智能化程度。

4. 处理性能提升

下一代防火墙需要处理的安全事务将会越来越复杂。当前下一代防火墙的最大处理性能可适用于大型企业网、数据中心等场景。要满足大型数据中心、运营商网络环境的更高性能要求，必须优化软硬件架构，并持续提高应用层处理性能和安全检测性能。

5. 防火墙云端虚拟化

随着云计算技术的逐步成熟和应用，越来越多的应用和服务由云端提供。用户可以根据需求租用或者购买云端提供的虚拟化防火墙服务，而不是购买防火墙硬件设备部署在网络边界。云端虚拟化技术不仅是防火墙发展的趋势，也是各种应用和服务发展的趋势。目前，防火墙和 WAF(Web Application Firewall，Web 应用防火墙)等设备也趋向云端虚拟化，云端虚拟化的防火墙和 WAF 可以在云环境中实现无缝迁移、弹性调配资源等功能，达到为云中租户提供快速、有效的边界安全防护的目的。

1.3 安全域和边界防御思想

1.3.1 安全域

随着网络系统规模逐渐扩大，结构越来越复杂，组网方式随意性增强，缺乏统一规划，扩展性差；网络区域之间边界不清晰，互连互通没有统一控制规范；业务系统各自为政，与外网之间存在多个出口，无法统一管理；安全防护策略不统一，安全防护手段部署原则不明确；对访问关键业务的不可信终端接入网络的情况缺乏有效控制。针对上述问题，提出安全域这一概念。安全域是一种思路、方法，它通过把一个复杂巨系统的安全保护问题分