教育部高等学校网络空间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

奇安信
新一代网络安全

奇安信集团组织编写

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

Web应用防火墙技术及应用实验指导

杨东晓 张锋 韩汶汐 王剑利 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

教育部高等学校网络空间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

Web应用防火墙技术及应用实验指导

杨东晓 张锋 韩汶汐 王剑利 编著

清华大学出版社
北京

内 容 简 介

本书为“Web应用防火墙技术及应用”课程的配套实验指导教材。全书分为4章，主要内容包括Web应用防火墙基本配置、Web应用防火墙安全防护应用、Web应用防火墙日志管理与分析、Web应用防火墙综合实验。

本书由奇安信集团联合高校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、信息安全等相关专业的本科生实验教材，也适合作为网络空间安全相关领域研究人员的基础读物。

图书在版编目(CIP)数据

Web应用防火墙技术及应用实验指导/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 978-7-302-52861-6

Ⅰ. ①W…　Ⅱ. ①杨…　Ⅲ. ①计算机网络－防火墙技术－教材　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2019)第082668号

责任编辑：张　民
封面设计：常雪影
责任校对：时翠兰
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**：19　　**字　　数**：439千字
版　　次：2019年9月第1版　　**印　　次**：2019年9月第1次印刷
定　　价：49.50元

产品编号：080617-01

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，进行了大量具有前瞻性的研究工作，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)。2019 年 6 月，教育部高等学校网络空间安全专业教学指导委员会召开成立大会。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，在教育部高等学校网络空间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，由教育部高等学校网络空间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，许多学校都在加大投入，聘请优秀教师，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，却也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，其知识体系庞大、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。

本书为“Web 应用防火墙技术及应用”课程的配套实验教材。通过实践教学，理解和掌握 Web 应用防火墙的基本配置、安全防护功能、日志管理与分析功能的使用，从而培养学生对 Web 应用防火墙设备的部署、应用和日常运维能力。

本书分为 4 章。第 1 章介绍 Web 应用防火墙基本配置，第 2 章介绍 Web 应用防火墙安全防护应用，第 3 章介绍 Web 应用防火墙日志管理与分析，第 4 章介绍课程设计，即 Web 应用防火墙综合实验。

本书适合作为网络空间安全、信息安全等相关专业的教材。随着新技术的不断发展，今后将不断更新图书内容。

本书编写过程中得到奇安信集团的王嘉、董少飞、白伟、段晓光、裴智勇、翟胜军，以及北京邮电大学雷敏等专家学者的鼎力支持，在此对他们的工作表示衷心的感谢！

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

2019 年 5 月

目录

第 1 章　Web 应用防火墙基本配置 …… 1

1.1　系统配置 …… 1

1.1.1　Web 应用防火墙登录管理实验 …… 1

1.1.2　Web 应用防火墙多网段登录管理实验 …… 5

1.1.3　Web 应用防火墙管理员设置实验 …… 14

1.1.4　Web 应用防火墙系统管理实验 …… 18

1.1.5　Web 应用防火墙配置管理实验 …… 21

1.2　对象管理 …… 30

1.2.1　Web 应用防火墙基础对象配置实验 …… 30

1.2.2　Web 应用防火墙服务器管理实验 …… 37

第 2 章　Web 应用防火墙安全防护应用 …… 55

2.1　Web 防护 …… 55

2.1.1　Web 应用防火墙 Web 防护实验 …… 55

2.1.2　Web 应用防火墙 HTTP 协议校验实验 …… 61

2.1.3　Web 应用防火墙 HTTP 访问控制实验 …… 72

2.1.4　Web 应用防火墙爬虫防护实验 …… 80

2.1.5　Web 应用防火墙盗链防护实验 …… 89

2.1.6　Web 应用防火墙 CSRF 防护实验 …… 97

2.1.7　Web 应用防火墙特征防护实验 …… 107

2.1.8　Web 应用防火墙文件上传检测实验 …… 114

2.1.9　Web 应用防火墙文件下载检测实验 …… 123

2.1.10　Web 应用防火墙敏感信息检测实验 …… 136

2.2　DDoS 防护 …… 148

2.2.1　Web 应用防火墙 DDoS 防护实验 …… 148

2.2.2　Web 应用防火墙 IP 防护实验 …… 154

2.2.3　Web 应用防火墙 TCP 防护实验 …… 167

2.2.4　Web 应用防火墙 UDP 防护实验 …… 174

2.2.5　Web 应用防火墙 HTTP 防护实验 …… 182

2.3 网页防篡改 …… 191
2.3.1 Web 应用防火墙主机网页防篡改防护服务器配置实验 …… 191
2.3.2 Web 应用防火墙网页防篡改实验 …… 201

第 3 章 Web 应用防火墙日志管理与分析 …… 218
3.1 Web 应用防火墙日志备份及恢复实验 …… 218
3.2 Web 应用防火墙审计日志管理实验 …… 225
3.3 Web 应用防火墙 Web 攻击溯源分析实验 …… 233

第 4 章 Web 应用防火墙综合实验 …… 250

第 1 章 Web 应用防火墙基本配置

Web 应用防火墙(Web Application Firewall,WAF)用以解决诸如防火墙等传统网络安全设备无法解决的 Web 应用安全问题。WAF 通过执行一系列针对 HTTP/HTTPS 的安全策略专门为 Web 应用提供防护。

其设计目标为:针对安全事件发生时序进行安全建模,分别针对安全漏洞、攻击手段及最终攻击结果进行扫描、防护及诊断,提供综合 Web 应用安全解决方案。

Web 应用防火墙是基于自主知识产权开发的新一代安全产品,作为网关设备,防护对象为 Web、Webmail 服务器。

任何一个单位购置 Web 应用防火墙设备后,需要先完成 Web 应用防火墙基本的系统配置,才能使 Web 应用防火墙的各种应用功能生效。本章主要完成 Web 应用防火墙的系统配置和对象管理实验。

Web 应用防火墙系统配置的第一步就是登录 Web 应用防火墙,Web 应用防火墙登录成功后可在 Web 应用防火墙中添加管理员角色,添加管理员后才可以开始进行 Web 应用防火墙的基本管理;Web 应用防火墙的系统配置完成后需要对 Web 应用防火墙进行对象管理,包括基础对象配置和服务器对象管理,配置好对象之后便可以在 Web 应用防火墙中实现对象所需的防护功能。

1.1 系统配置

1.1.1 Web 应用防火墙登录管理实验

【实验目的】

管理员可以熟练掌握 Web 应用防火墙的多种登录方式,并且能够根据实际的需求使用不同的登录方式管理 Web 应用防火墙。

【知识点】

HTTPS、SSH。

【场景描述】

A 公司部署了一台 Web 服务器对互联网上的用户提供服务,为了保障该 Web 服务

器不被外界攻击，公司采购了一台 Web 应用防火墙设备，交给安全运维工程师小王配置。小王现在想登录设备进行配置，请帮小王想想办法，如何通过 HTTPS、SSH 方式登录这台 Web 应用防火墙？

【实验原理】

Web 应用防火墙支持基于图形化界面（WebUI）和基于命令行（CLI）的管理方式，管理员可通过这两种方式对 Web 应用防火墙进行配置、维护和管理。

WebUI 登录方式为用户提供了更直观的人机交互方式，用户可通过 Web 页面对 Web 应用防火墙的网络进行配置，实现 HTTP 协议来访问设备。

另一种是基于 CLI 命令行的登录方式，管理员可以通过 SSH 或者 Telnet 终端访问设备，一般供工程师通过底层调试设备。

访问 Web 应用防火墙的设备需要与 Web 应用防火墙网络连通。

【实验设备】

- 安全设备：Web 应用防火墙设备 1 台。
- 主机终端：Windows XP 主机 1 台，Windows 7 主机 1 台。

【实验拓扑】

实验拓扑如图 1-1 所示。

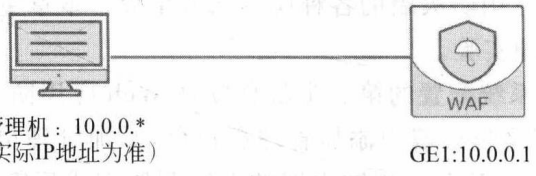

图 1-1　Web 应用防火墙登录管理实验拓扑

【实验思路】

（1）使用默认的 HTTPS 的方式登录设备。

（2）使用 SSH 的方式登录设备。

【实验步骤】

（1）在管理机中打开浏览器，在地址栏中输入 Web 应用防火墙产品的 IP 地址“https：//10.0.0.1”（以实际设备 IP 地址为准），进入 Web 应用防火墙的登录界面。输入管理员用户名 admin 和口令 admin，单击“登录”按钮，登录 Web 应用防火墙，如图 1-2 所示。

（2）登录 Web 应用防火墙设备后，会显示它的面板界面，如图 1-3 所示。

【实验预期】

使用管理员用户 admin 不仅可以通过 HTTPS 登录 Web 应用防火墙平台，也可以通过 SSH 的方式登录 Web 应用防火墙平台。

【实验结果】

（1）在管理机桌面双击 Xshell5。如弹出“会话”界面，关闭该界面。在 Xshell5 界面

图 1-2　Web 应用防火墙登录页面

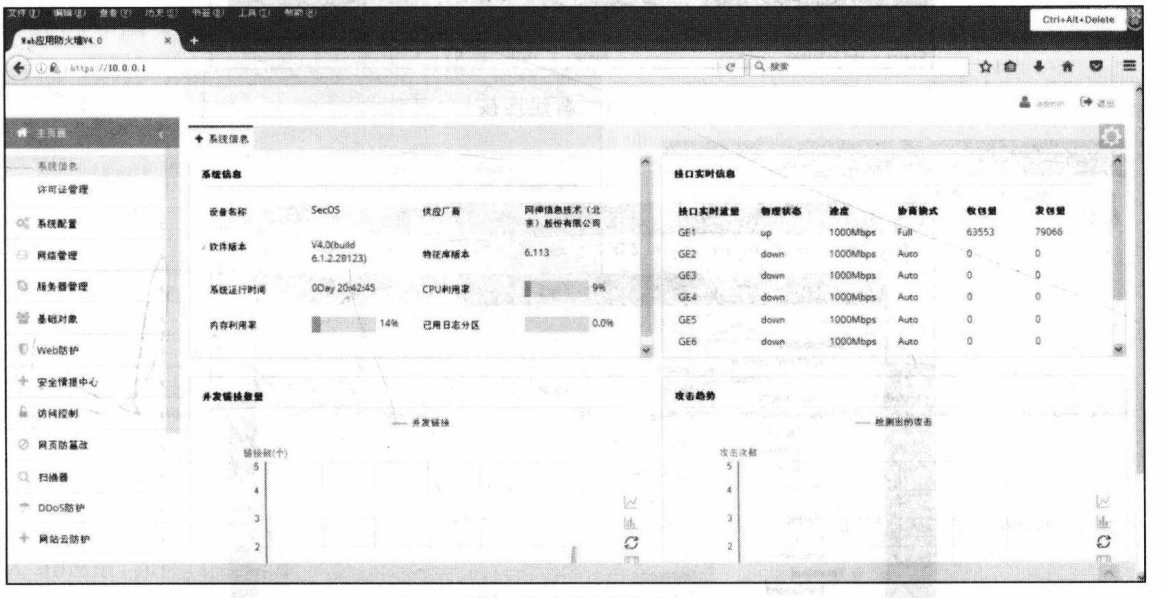

图 1-3　Web 应用防火墙面板界面

中单击 File→New，新建连接，如图 1-4 所示。

（2）在“New Session Properties”界面中，在 Name 中输入“SSH 登录 Web 应用防火墙”，将 Protocol 设置为 SSH，在 Host 中输入“10.0.0.1”。其他保持默认配置，如图 1-5 所示。

（3）单击 OK 按钮，关闭“New Session Properties”界面。在弹出的 Sessions 界面中，单击“SSH 登录 Web 应用防火墙”，单击 OK 按钮，返回 Sessions 界面，单击 Connect 按钮，如图 1-6 所示。

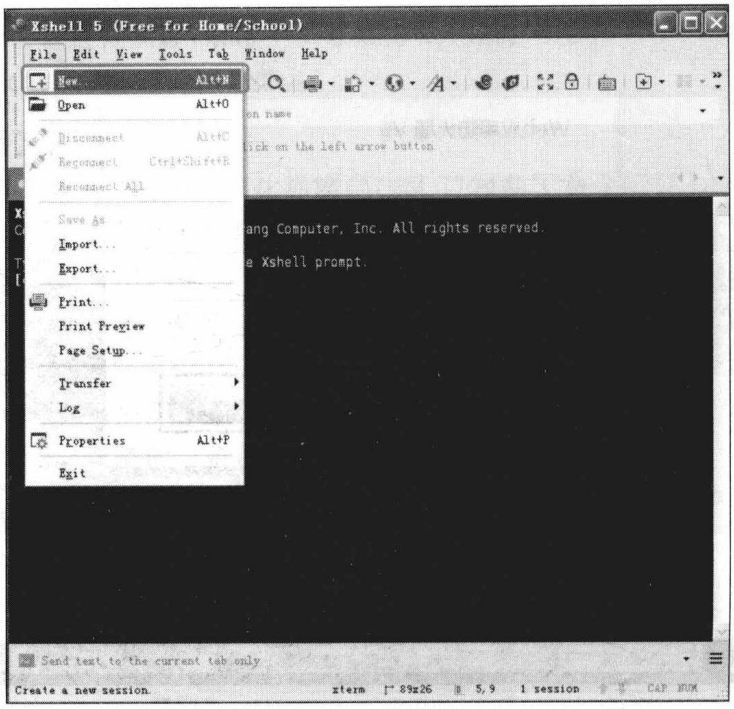

图 1-4　新建连接

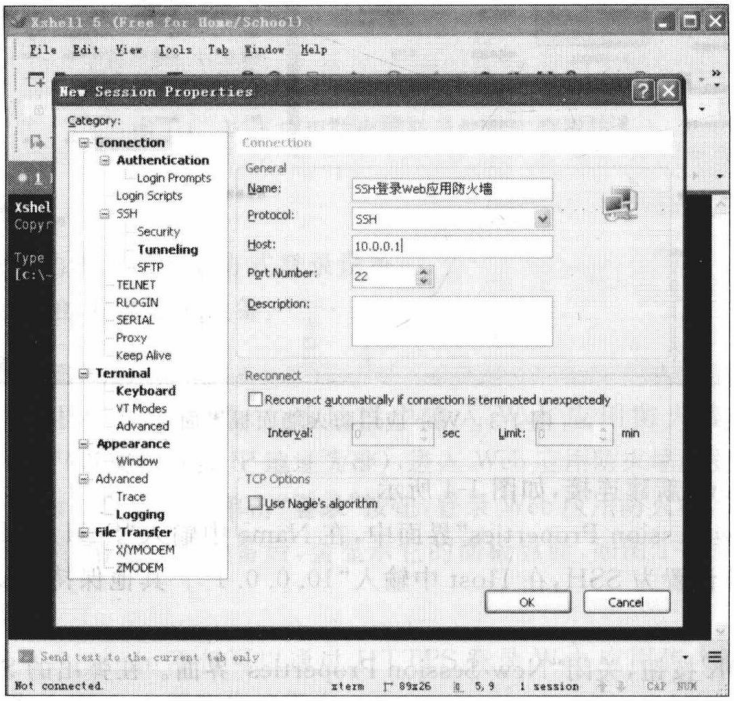

图 1-5　设置会话属性

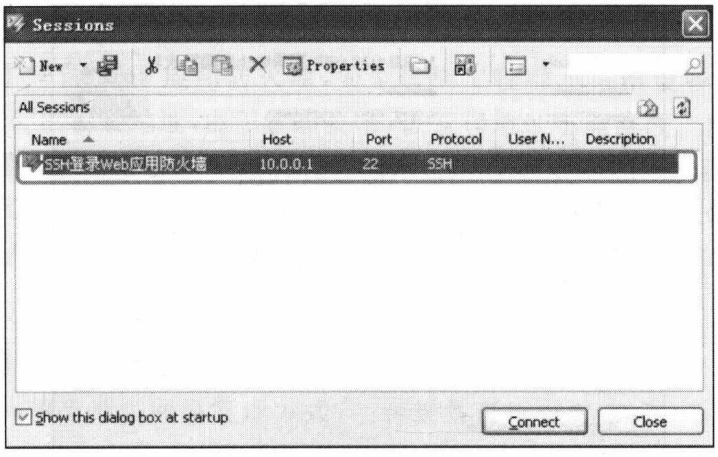

图 1-6　连接会话

(4) 在弹出的“SSH Security Warning”界面中，单击“Accept and Save”按钮，如图 1-7 所示。

(5) 在弹出的“SSH User Name”界面中，在“Enter a user name to login”中输入 admin，如图 1-8 所示。

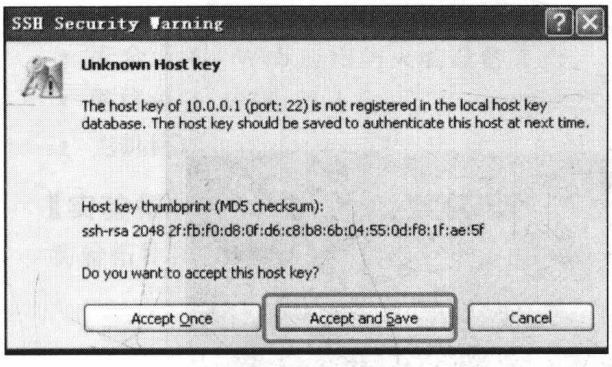

图 1-7　SSH 安全警告

图 1-8　输入用户名

(6) 单击 OK 按钮，在弹出的“SSH User Authentication”界面中，在 Password 中输入 admin，如图 1-9 所示。

(7) 单击 OK 按钮，连接 Web 应用防火墙，输入命令 help，按 Enter 键执行，返回正确结果，符合预期，如图 1-10 所示。

【实验思考】

Web 应用防火墙还有其他登录方式吗？

1.1.2　Web 应用防火墙多网段登录管理实验

【实验目的】

管理员通过添加 Web 应用防火墙管理系统的远程管理 IP 地址，实现多网段的主机对 Web 应用防火墙的管理。

图 1-9　输入口令

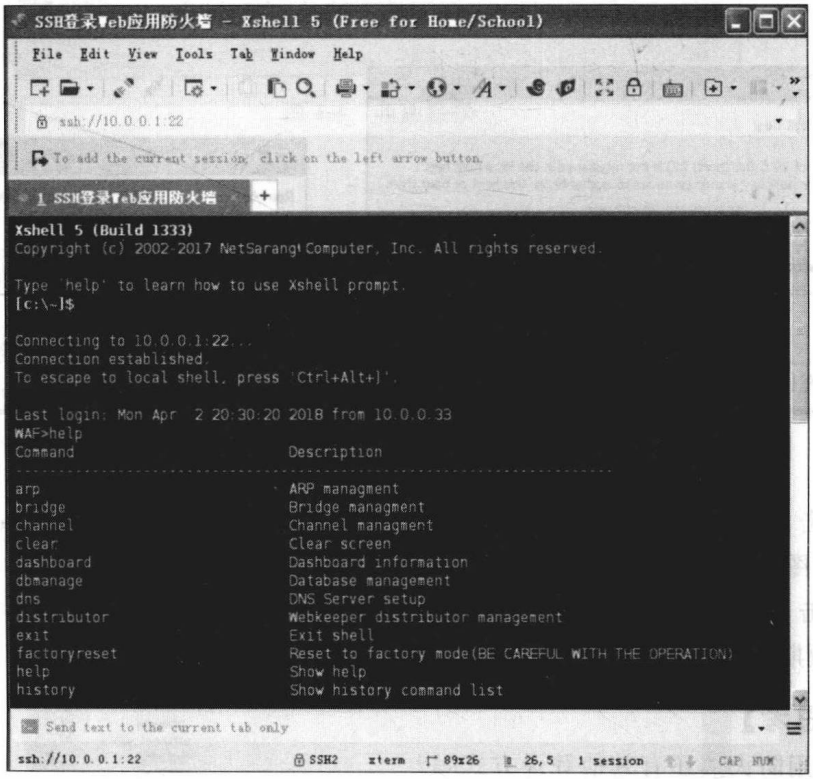

图 1-10　成功连接 Web 应用防火墙

【知识点】

管理端口、端口设置、远程管理。

【场景描述】

A 公司采购了一台 Web 应用防火墙，安全运维工程师小王给设备配置了 IP 地址“192.168.1.40/16”的管理地址，由于管理要求，该管理地址不能修改。网络管理员小张出于对网络统一管理的考虑，要求小王给这台 Web 应用防火墙配置的管理地址为“172.16.0.1/24”。小张还要求可以访问这台 Web 应用防火墙，小张所在的网段为“172.16.1.1/24”。请帮小王想想办法，如何通过配置 Web 应用防火墙实现小张访问这台 Web 应用防火墙的要求？

【实验原理】

Web 应用防火墙支持多网段管理方式，一台设备可以配置多个不同网段的管理 IP 地址。

Web 应用防火墙出于安全要求，默认出厂只允许“10.0.0.1/24”网段访问设备，其他网段的主机如需访问该设备，需要在远程管理模块中添加对应的 IP 地址和子网掩码，才能实现远程管理 Web 应用防火墙。

同时，Web 应用防火墙允许修改访问 WebUI 界面的端口，管理员可以根据实际的安全需求设置对应的端口。

【实验设备】

- 安全设备：Web 应用防火墙设备 1 台。
- 网络设备：路由器 1 台。
- 主机终端：Windows XP SP3 主机 1 台，Windows 7 主机 1 台。

【实验拓扑】

实验拓扑如图 1-11 所示。

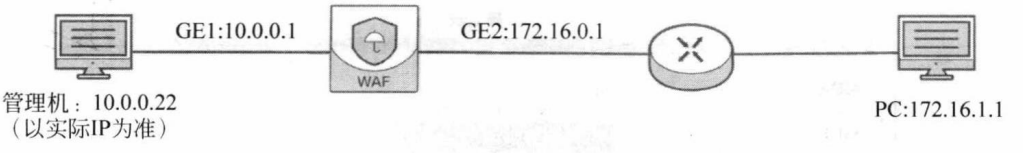

图 1-11　Web 应用防火墙多网段登录管理实验拓扑

【实验思路】

(1) 增加网桥接口。

(2) 增加远程管理 IP。

【实验步骤】

(1) 在管理机打开浏览器，在地址栏中输入 Web 应用防火墙产品的 IP 地址“https://10.0.0.1”(以实际设备 IP 地址为准)，进入 Web 应用防火墙的登录界面。输入管理员用户名 admin 和密码 admin，单击“登录”按钮，登录 Web 应用防火墙。

(2) 登录 Web 应用防火墙设备后，会显示它的面板界面。单击面板左侧导航栏中的“网络管理”→“网络接口”，单击“网桥接口”。在“网桥接口”界面中，单击“增加＋”按钮，

增加网桥接口，如图 1-12 所示。

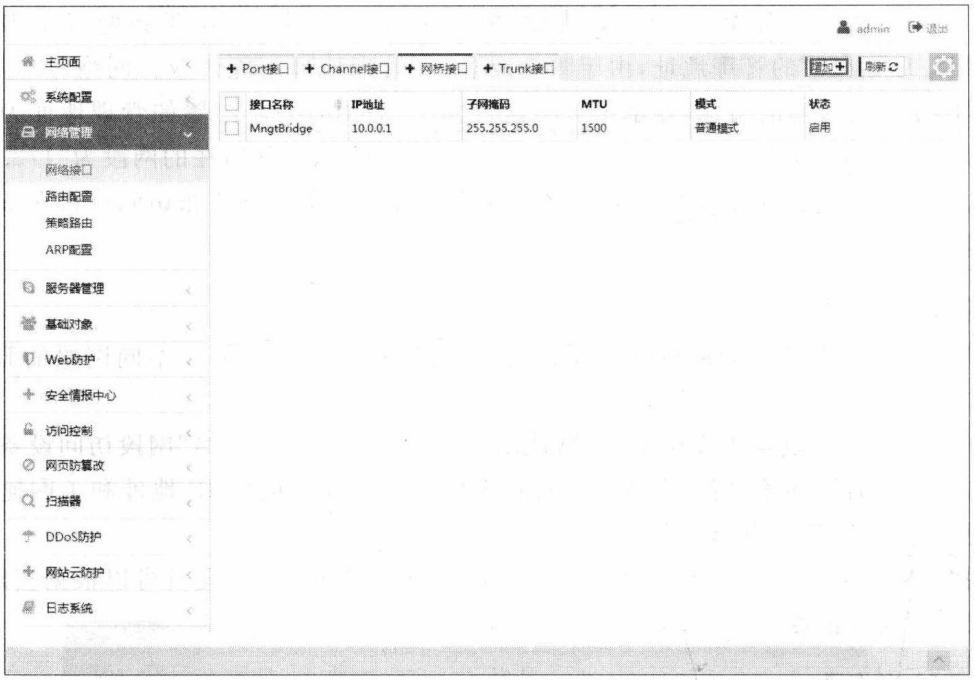

图 1-12　增加网桥接口

（3）在“增加网桥接口”界面中，除默认网桥号 1 保留作为管理网桥外，输入一个不重复的网桥号即可，本实验中输入“网桥号”为 12，其他保持默认配置，如图 1-13 所示。

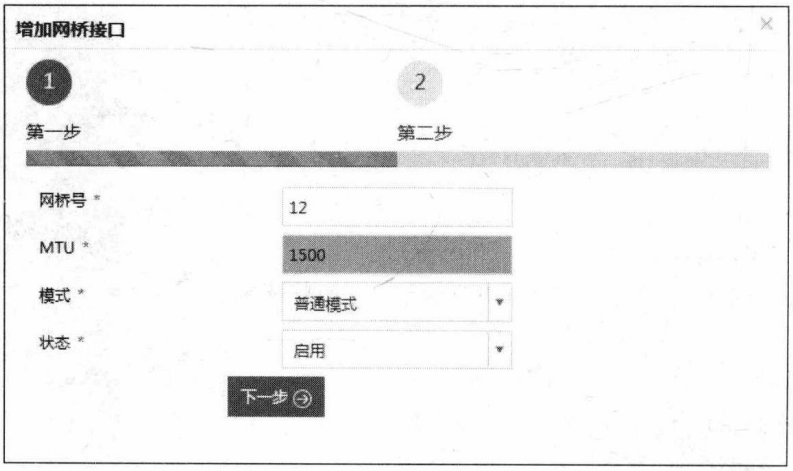

图 1-13　设置网桥接口

（4）单击“下一步”按钮，在弹出的增加网桥成功界面中单击“确定”按钮，再单击“增加＋”按钮，增加 IP，如图 1-14 所示。

（5）在“接口 IP 地址配置”界面中，输入“IP 地址”为“172.16.0.1”，“子网掩码”为“255.255.255.0”，勾选“管理 IP”右侧的复选框，其他保持默认配置，如图 1-15 所示。

（6）单击“保存”按钮，在弹出的操作成功界面中单击“确定”按钮，返回“编辑网桥接