教育部师资实践基地系列教材——信息与网络安全

神州数码校企合作技能训练系列

防火墙系统实训教程

FANGHUOQIANG XITONG SHIXUN JIAOCHENG

程庆梅　徐雪鹏　主编

全国职业技能大赛推荐参考书

神州数码校企合作技能训练指定教材

校企合作新课改教材

机械工业出版社
CHINA MACHINE PRESS

配电子课件

教育部师资实践基地系列教材——信息与网络安全

神州数码校企合作技能训练系列

防火墙系统实训教程

主　编　程庆梅　徐雪鹏

副主编　杜婉琛

参　编　李东方　王　岳　王　博

机械工业出版社

本书主要围绕神州数码多核防火墙系统的安装部署及各种典型应用展开。全书共设计4个单元，分别为搭建防火墙基本管理环境、配置防火墙基本功能、配置防火墙常见应用和配置防火墙高级功能，包括24个独立的任务。本书内容基本涵盖防火墙在现有项目中的典型应用案例。本书是典型的实训教程，以实际工作内容为依托，形成典型的任务工作设计，按照一般学习思维活动的特点进行系统化编排和整理。本书的主体内容均包含任务目标、任务设备与要求、任务实施、任务拓展思考和任务评价。这样安排既保证了任务的可操作性，又对任务实施后的理论提升创造了空间。同时，在每个单元的开始，均设有学习目标、重点及难点、知识补充和技能大赛赛点分析，主要为读者学习本单元的内容提供一定的指导。

本书可作为职业技术院校的教材，也可作为网络从业人员的参考用书。

本书配有授课用电子课件，可到机械工业出版社教材服务网 www.cmpedu.com 免费注册下载，或联系编辑（010-88379194）咨询。

图书在版编目（CIP）数据

防火墙系统实训教程/程庆梅，徐雪鹏主编．—北京：机械工业出版社，2012.3
教育部师资实践基地系列教材——信息与网络安全
ISBN 978-7-111-37826-6

Ⅰ．①防…　Ⅱ．①程…　②徐…　Ⅲ．①计算机网络—安全技术—教材
Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 052623 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策划编辑：梁　伟　　责任编辑：梁　伟　罗子超
封面设计：鞠　杨　　责任印制：杨　曦
北京四季青印刷厂印刷
2012 年 5 月第 1 版第 1 次印刷
184mm×260mm · 7 印张 · 161 千字
0 001—3 000 册
标准书号：ISBN 978-7-111-37826-6
定价：19.00 元
凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社服务中心：（010）88361066
销售一部：（010）68326294
销售二部：（010）88379649
读者购书热线：（010）88379203

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com
封面无防伪标均为盗版

前　言

21 世纪是科技的时代，各种新技术应用在社会生活的每个领域。伴随着网络技术的发展，除了使人们更加依赖网络之外，各种干扰人们正常使用网络的非主流技术也引起了人们越来越多的关注。公司、学校、公共热点区域……凡是可能使用到网络的地方都有可能存在网络安全的隐忧。

● 指导思想

作为整体网络的搭建者和管理者，神州数码网络公司集多年在网络搭建和管理项目中的经验，为广大网络管理员选取了实用的网络安全实训素材，并与机械工业出版社合作编写了本书。全书从网络安全的视角，针对管理员和工程师最关心的若干安全问题，使用直观、简洁的方式，以常见的网络安全隐患为主线，希望能为广大致力于从事网络安全相关工作的在校学生和其他技术人员提供快速有效的指导。

全书的项目全部来自真实的工程项目案例，经过资深安全工程师、研发人员以及课程规划师的提炼，最终形成了具有典型意义的指导性实训过程。

● 本书的特点

1）注重实践操作，知识点围绕操作过程按需介绍。

2）攻防结合，重点在防。

3）由浅入深，由简入繁，循序渐进。

4）侧重应用，抛开复杂的理论说教，学以致用。

● 编写思路

本书为神州数码网络大学安全系列教材，内容主要以多核防火墙在实践中的各种应用环境设置为主。全书从认识防火墙开始，第一部分主要围绕如何成为一名在客户使用环境中合格的安全设备管理员，主要内容为维护现有防火墙配置和升级版本；第二部分主要以网络工程师的调试项目为主，集成了若干项目的不同需求，主要内容为搭建网络安全环境和充分发挥防火墙的功能和特点；第三部分体现当代防火墙以应用为主，跟随应用灵活管理的特点，主要内容为如何应对大流量应用，如何控制非常规外网流量等应用层控制；第四部分选取 VPN 环境搭建过程最主要的两类作为范例，展示如何成功搭建不同需求下的 VPN 环境；第五部分围绕防火墙的日志等信息进行记录展开，示范如何搭建一个完整的，能够提供安全管理报告的网络管理环境。

● 读者对象

1）从事网络安全管理工作的网络管理人员。

2）为终端客户提供安全解决方案的网络安全工程师。

3）提供网络安全整体解决方案的售前、售后工程师。

4）有志于从事网络安全工程研究的网络从业者。

5）希望加固自身终端系统的网络使用者。

6）中等及高等职业技术院校 2、3 年级在校学生。

本书全体编者衷心感谢提供各类安全资料及项目素材的神州数码网络工程师、产品经理及技术部的同仁，同时也要感谢来自职业教育干线的合作教师们提供的大量需求建议，以及他们对部分内容的校对和整理。

由于编者的经验和水平有限，书中错漏之处难免，敬请广大读者批评指正。编者邮箱 duwc@digitalchina.com。

编　者

目　录

导　读

防火墙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。

防火墙有如下特性。

1）所有进出网络的通信流都应该通过防火墙。

2）所有穿过防火墙的通信流都必须有安全策略和计划的确认与授权。

3）防火墙自身具有较强的抗攻击能力。

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，有效地监控了内部网和 Internet 之间的活动，保证了内部网络的安全。防火墙可以是硬件型，所有数据首先都要通过硬件芯片监测；它也可以是软件型，软件在计算机上运行并监控。其实硬件型也就是在芯片里固化了软件，但是它不占用计算机 CPU 的处理时间，功能非常强大，处理速度很快。对于个人用户来说，软件型更加方便。

图 0-1 是一个典型的防火墙设备的前后面板，型号为 DCFW-1800 系列防火墙。

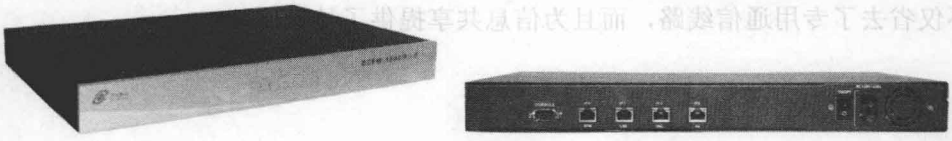

图 0-1　典型的防火墙设备前后面板

防火墙主要有如下几个功能。

1．防火墙是网络安全的屏障

防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以，网络环境变得更安全。例如，防火墙可以禁止诸如 NFS 等不安全的协议进出受保护网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上攻击类型的报文，并通知防火墙管理员。

2．防火墙可以强化网络安全策略

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经济。例如，在网络访问时，一次一密口令系统和其他的身份认证系统完全可以不

必分散在各个主机上，而只需集中在防火墙上。

3．对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，防火墙就能记录这些访问并做日志记录，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。另外，收集一个网络的使用和误用情况也是非常重要的。因为这样可以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。而统计网络使用对网络需求分析和威胁分析等而言也是非常重要的。

4．防止内部信息的外泄

通过防火墙对内部网络的划分，可实现内部网重点网段的隔离，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。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的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露内部细节（如Finger、DNS 等）的服务。Finger 显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，是否在被攻击时引起注意等。防火墙同样可以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。

除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN，将企事业单位在地域上分布在全世界的 LAN 或专用子网有机地连成一个整体。这样不仅省去了专用通信线路，而且为信息共享提供了技术保障。

单元 1

搭建防火墙基本管理环境

防火墙历经几代发展，现已成为非常成熟的硬件体系结构，具有专门的 Console 口，专门的区域接口，串行部署于 TCP/IP 网络中。网络一般划分为内、外、服务器区 3 个区域，对各区域实施安全策略以保护重要网络。本任务使用 DCFW-1800E-V2 防火墙，软件版本为 DCFOS-2.0R4。如果实训室的环境与此不同，请参照相关版本的用户手册进行设置。

就像路由器和交换机一样，在使用防火墙之前，需要经过基本的初始配置。防火墙的初始配置也是先通过 Console 口与计算机的串口连接，再通过超级终端程序进行选项配置。

学习目标

1．了解防火墙的基本配置方法，明确管理环境搭建要素和不同管理方法之间的差异

2．学会对防火墙配置文件的备份和替换，并了解防火墙系统的升级过程和关键步骤

重点及难点

1．防火墙管理环境搭建、SSH 及 WebUI 方式中的安全保障

防火墙是一种安全设备，其自身的安全直接影响到全网的安全，对防火墙的慎重管理将减少因为基于网络连通性的管理行为而带来的设备安全隐患。通常基于网络的连通可以采用安全性的链接，如使用 HTTPS 和 SSH 方式接入防火墙，都可以比以往仅仅使用 HTTP 和 telnet 的管理方式更安全，减少了由于开放管理端口而导致不必要的访问通过这些端口访问防火墙的内部资源。

2．管理用户的设置对防火墙的安全管理产生的影响

所谓管理用户，是指那些不拥有默认 admin 全部管理权限的自定义管理员，将管理员的权限细分，从而使管理员不会由于误操作或者账号保护不善而导致防火墙被不当的侵入和设置。

3．备份防火墙配置文件及操作系统文件的意义

对于安全设备而言，设备的配置文件被妥善地备份，将有助于在安全事件发生后以最快的速度恢复网络的可用性。通常设备的系统文件也需要同时进行备份，这样可以保障系统文

件丢失或者进行版本升级失败时，可以恢复系统。合格的网络管理和维护人员，一定要对所有关键网络设备中的重要文件备份，这样才可以在需要的时候及时、有效地恢复网络。

知识补充

防火墙在出厂时配置有默认的端口地址等，但一般的网络用户在第一次使用时会将这些端口地址及管理设置进行更改，这也是保证网络设备安全的一种有效手段。

可以使用随设备装箱的控制线缆将防火墙的 Console 口与计算机的串行接口连接，开启超级终端后进入设备的命令行配置模式对设备的初始信息进行配置。

1．关于设备的配置文件

一般设备的基本存储组件如下：

NVRAM——非易失性存储器，即掉电内容不丢失，这里通常存储设备的启动配置文件。

SDRAM——SDRAM，即 Synchronous Dynamic Random Access Memory，同步动态随机存储器，它是掉电丢失内容的，这里通常存放当前正在运行的配置文件和正在使用的策略表，以及其他缓存数据等。

BootROM——启动只读存储器，这里存放相当于设备自举程序的系统文件，其中的内容不可写，只可读，通常用于异常错误的恢复等操作。

Flash——闪式内存，它的内容也是掉电不丢失的，通常用来存放设备当前使用的软件版本。

在设备实现的过程中，一般会把 Flash 和 NVRAM 的功能进行整合，将启动配置文件和设备的当前启动软件版本均放在 Flash 中。

设备的启动过程如下。

1）系统硬件加电自检。运行 BootROM 中的硬件检测程序，检测各组件能否正常工作。完成硬件检测后，开始软件初始化工作。

2）软件初始化过程。运行 BootROM 中的引导程序，进行初步引导工作。

3）寻找并载入操作系统文件。操作系统文件可以存放在多处，至于采用哪一个操作系统，则是可以通过命令设置指定的。

4）操作系统装载完毕，系统在 NVRAM 中搜索保存的 Startup-Config 文件，进行系统的配置。如果 NVRAM 中存在 Startup-Config 文件，则将该文件调入 RAM 中并逐条执行。否则，系统默认无配置，直接进入用户操作模式进行路由器初始配置。

图 1-1 表示了这几个组件之间的关系和启动时的文件读取顺序。

图 1-1　设备启动时的文件读取顺序

2．关于设备的软件版本

设备系统文件包括 3 类：引导文件、系统映像文件和厂商设备配置文件。软件版本升级就是对这 3 类文件的更新，方法就是用新的文件覆盖旧的文件。

引导文件是指引导设备初始化等的文件，即通常说的 ROM 文件，在某些设备上通常为一份 boot.rom 文件，有时为 boot.rom 和 config.rom 文件。ROM 文件保存在 Flash 中，文件名固定为 boot.rom 和 config.rom。

系统映像文件是指设备硬件驱动和软件支持程序等的压缩文件，即通常说的 IMG 文件。系统映像文件保存在 Flash 中，文件名默认为 nos.img，或者*.bin。

厂商设备配置文件是保存厂商设备配置信息的基本配置文件，在系统映像文件启动时进行基本信息的动态显示与部分功能模块的动态加载。厂商设备配置信息一般包括厂商名称、厂商网址、Web 相关图片、Web 语言、设备类型等基本显示信息，以及 MIB OID、cluster MAC 地址、CLI 风格等功能控制信息。厂商设备配置文件保存在 Flash 中，文件名固定为 vendor.cfg。

提供给用户的文件名格式为<厂商缩写>-<交换机型号>-<版本号>-vendor.cfg。

有些文件在防火墙中不会呈现给用户，因此，目前在软件升级过程中只涉及其中的一种文件而已，具体情况根据厂商设置而定。

技能大赛赛点分析

本单元内容在历届大赛相关赛项中均占到比赛的 5%～10%，是考生必备的一项技能，务必做到熟练。本单元的内容基础性较强，命令也不是很复杂，但如果没有着重练习，在比赛过程中一旦在此环节出现故障将会影响整个比赛进度，因此，需要考生通过大量的练习达到熟练方可顺利应对技能大赛中的后续赛点。

虽然比赛赛点一般不会指明本单元所述技能，但这也是每次考试必考的一项，尤其是系统的升级与备份，其中使用的命令在每次考试中都要求使用，比如将配置文件保存到本地等。

任务 1　认识防火墙的外观与接口

1.1　任务目标

认识防火墙，了解各接口区域及其作用。

1.2　任务设备与要求

任务示意图如图 1-2 所示。

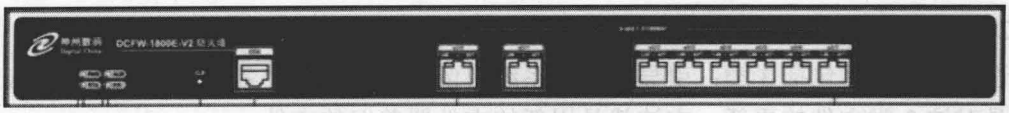

图 1-2　DCFW-1800E-V2 背板接口

1）熟悉防火墙各接口及其连接方法。

2）熟练使用各种线缆实现防火墙与主机和交换机的连通。

3）实现控制台连接防火墙进行初始配置。

1.3　任务实施

1.3.1　登录防火墙并熟悉各配置模式

1）打开防火墙包装箱，取出设备，从外观认识防火墙各接口，如图 1-3 所示。

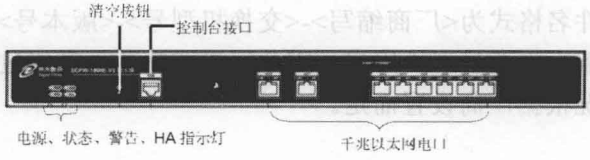

图 1-3　防火墙外观

2）使用设备自带的控制线缆将防火墙与计算机的串行接口连接，如图 1-4 所示。

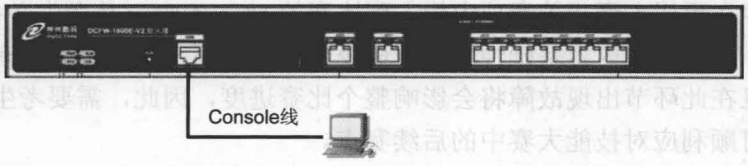

图 1-4　防火墙控制端口连接

3）配置计算机的超级终端属性，接入防火墙命令行模式。

计算机的超级终端属性与连接路由和交换机一致，不再赘述。

注意：防火墙中有两种默认的管理用户：超级管理用户（Super Admin）和普通管理用户（General Admin）。

默认的管理员用户口令和密码如下：

login：admin

password：admin

4）输入管理员用户口令和密码，可进入防火墙的执行模式，该模式的提示符如下所示，包含了一个数字符号（#）：

DCFW-1800#

5）在执行模式下，输入 configure 命令，可进入全局配置模式。提示符如下所示：

DCFW-1800（config）#

V2 系列防火墙的不同模块功能需要在其对应的命令行子模块模式下进行配置。在全局配置模式输入特定的命令，可以进入相应的子模块配置模式。

例如，运行 interface ethernet0/0 命令进入 ethernet0/0 接口配置模式，此时的提示符变更为

DCFW-1800（config-if-eth0/0）#

表 1-1 列出了常用的模式间的切换命令。

表 1-1　模式间的切换命令

模　式	命　令
执行模式到全局配置模式	Configure
全局配置模式到子模块配置模式	不同功能使用不同的命令进入各自的命令配置模式
退回到上一级命令模式	Exit
从任何模式退回到执行模式	End

1.3.2　通过计算机测试与防火墙的连通性

1）使用交叉双绞线连接防火墙和计算机，此时防火墙的 LAN-link 灯亮起，表明网络的物理连接已经建立。指示灯状态为闪烁，表明有数据在尝试传输。

2）此时打开计算机的连接状态，发现只有数据发送，没有接收到的数据，这是因为防火墙的端口在默认状态下都会禁止向未经验证和配置的设备发送数据，保证数据的安全。

1.4　任务拓展思考

1）防火墙的初始状态配置信息如何，怎样通过命令行查看初始配置信息？

2）本任务未配置防火墙的 IP 地址等信息，课后可从防火墙的前面板观察防火墙的状态，熟悉防火墙各种配置模式之间的切换和简化配置命令的书写模式。

1.5　任务评价

评价内容见表 1-2。

表 1-2　项目任务评价表

项目任务评价表					
	内　容		评　价		
	学习目标	评价项目	3	2	1
技术能力	快速准确地初步确定设备的物理接口类型等外在信息	能够从外观准确识别防火墙 Consol 接口和网络接口			
	熟悉防火墙设备的登录方式和模式	能够正确选取 Console 线缆并登录设备，熟练地在各配置模式之间进行切换			
通用能力	掌握测试设备间连通性的方法并灵活运用				
	理解防火墙作为安全设备的一些特殊设置，如默认状态端口不接收和发送任何数据				
综合评价					

任务2　搭建防火墙管理环境

V2 防火墙可以使用 Telnet、SSH、WebUI 方式进行管理。本任务使用 DCFW-1800E-V2 防火墙，软件版本为 DCFOS-2.0R4。如果实训室的环境与此不同，请参照相关版本的用户手册进行设置。

1）SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组所制定。通过使用 SSH，可以把所有传输的数据进行加密。它是目前较为可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效地防止远程管理过程中的信息泄露问题。SSH 由客户端和服务端的软件组成。

2）防火墙的 WebUI 图形化界面。防火墙是一个信息安全设备，保证自身的配置安全无误非常重要。由于配置安全策略是一个很复杂的过程，使用命令行可能出现一些不该出现的错误，所以，建议初学者使用图形化界面来配置防火墙。

2.1　任务目标

学会使用 Telnet、SSH、WebUI 方式登录防火墙。

2.2　任务设备与要求

任务示意图如图 1-5 所示。

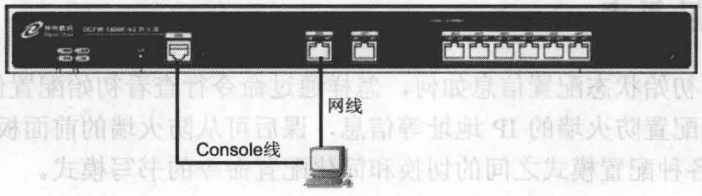

图 1-5　防火墙配置连接

掌握防火墙管理环境的搭建和配置方法，熟练使用各种管理方式管理防火墙。

2.3　任务实施

按照图 1-5 所示搭建任务环境。

2.3.1　搭建 Telnet 和 SSH 管理环境

1）运行 **manage telnet** 命令开启被连接接口的 Telnet 管理功能。

```
Hostname#configure
DCFW-1800（config）#interface Ethernet 0/0
DCFW-1800（config-if-eth0/0）#manage telnet
```

2）运行 manage ssh 开启 SSH 管理功能。

```
DCFW-1800（config-if-eth0/0）#manage ssh
```

3）配置计算机的 IP 地址为 192.168.1.*，从计算机尝试与防火墙的 telnet 连接。

注：用户口令和密码是默认的管理员用户口令和密码，即 admin，如图 1-6 所示。

图 1-6　计算机 telnet 登录过程

4）从计算机尝试与防火墙的 SSH 连接，如图 1-7 所示。

注：计算机中已经安装好 SSH 客户端软件。用户口令和密码是默认的管理员用户口令和密码，即 admin。

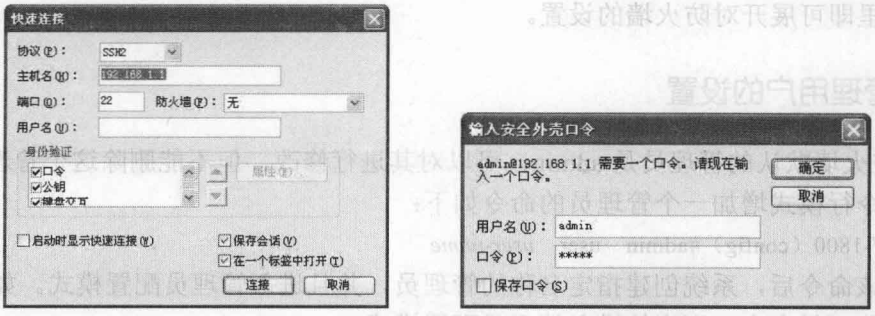

图 1-7　计算机建立 SSH 连接过程

2.3.2　搭建 WebUI 管理环境

初次使用防火墙时，用户可以通过该 E0/0 接口访问防火墙的 WebUI 页面。

在浏览器地址栏输入 http: //192.168.1.1 并按回车键，系统 WebUI 的登录界面如图 1-8 所示。

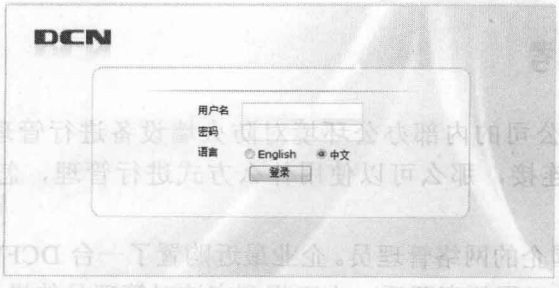

图 1-8　系统 WebUI 的登录界面

登录后的主界面如图 1-9 所示。

图 1-9　登录后的主界面

在这里即可展开对防火墙的设置。

2.3.3　管理用户的设置

V2 防火墙默认的管理员是 admin，可以对其进行修改，但不能删除这个管理员。

在命令行模式增加一个管理员的命令如下：

DCFW-1800（config）#admin　user　*user-name*

执行该命令后，系统创建指定名称的管理员，并且进入管理员配置模式。如果指定的管理员名称已经存在，则直接进入管理员配置模式。

DCFW-1800（config-admin）#

管理员特权为管理员登录设备后拥有的权限。DCFOS 允许的权限有 RX 和 RXW 两种。在管理员配置模式下，输入以下命令配置管理员的特权：

DCFW-1800（config-admin）#**privilege** {**RX** | **RXW**}

在管理员配置模式下，输入以下命令配置管理员的密码：

DCFW-1800（config-admin）#**password** *password*

2.4　任务拓展思考

1）如果需要在某公司的内部办公环境对防火墙设备进行管理，在这种情况下不可能使用 Console 直接连接，那么可以使用什么方式进行管理，怎样加强这种管理方式下的安全性？

2）小王是某大型国企的网络管理员。企业最近购置了一台 DCFW-1800S-L-V2 防火墙，在安装人员和售后技术工程师离开后，小王想到应该对管理员的操作加以限制，至少要设

置两个管理员的账号，一个用于全设备配置，另一个只能用于查看，以防止非管理员的非法操作，怎样做才能让小王的想法得到很好的实现呢？

2.5　任务评价

评价内容见表 1-3。

表 1-3　项目任务评价表

项目任务评价表					
	内　容		评　价		
	学习目标	评价项目	3	2	1
技术能力	使用网络方式对防火墙进行配置和管理	配置完成防火墙管理环境搭建，能够使用 3 种方式成功登录防火墙设备			
	学会通过增加管理用户的方式将防火墙的管理权限细化	成功增加一个只拥有部分管理权限的用户，并使用这个账户对设备进行相应的管理			
通用能力	了解 RX 和 RXW 权限的差异				
	能够使用 putty 或 secureCRT 等第三方超级终端软件以 SSH 方式登录防火墙				
综合评价					

任务 3　管理防火墙配置文件

DCFW-1800 系列防火墙的配置信息都被保存在系统的配置文件中。用户通过运行相应的命令或者访问相应的 WebUI 页面查看防火墙的各种配置信息，例如，防火墙的初始配置信息和当前配置信息等。配置文件以命令行的格式保存配置信息，并且也以这种格式显示配置信息。

3.1　任务目标

学会查看和保存防火墙的配置信息，同时了解如何导出和导入配置文件。

3.2　任务设备与要求

任务示意图如图 1-10 所示。

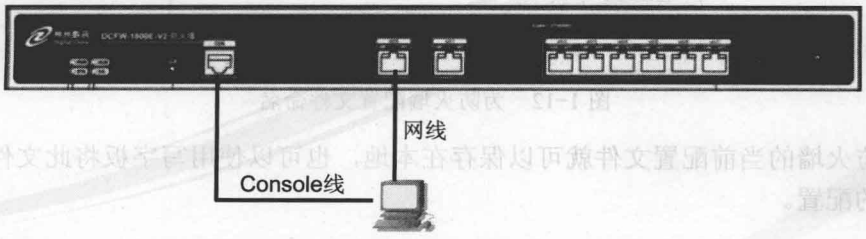

图 1-10　防火墙基本管理环境的搭建