网络专业校企合作开发项目式教学系列教材

防火墙与VPN技术实训教程

白树成◎主　编
杨宝强◎副主编

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

网络专业校企合作开发项目式教学系列教材

防火墙与VPN技术实训教程

主　编　白树成
副主编　杨宝强
参　编　邵长文　刘学普　孙景祥

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

内 容 简 介

本书基于“项目导向、任务驱动”的项目化教学方式编写而成，体现“基于工作过程”，“教、学、做”一体化的教学理念。

本书依托 H3C 网络学院和华网智通信集团相关项目，以 H3C 防火墙 F-100C 为实验平台对防火墙与 VPN 技术的应用进行了详细讲解。内容划分 18 个教学项目，具体内容包括：

项目一 安全区域配置、项目二 ACL 包过滤、项目三 网络地址转换、项目四 通过 NAT 对外提供 www 服务、项目五 IPSEC + IKE 功能的配置、项目六 IKE Keeplive 功能的配置、项目七 IPSec VPN 野蛮模式 NAT 穿越、项目八 IPSec 多网段独立保护功能的配置、项目九 路由器拨号接口上 IPSec 功能的配置、项目十 GRE 协议实训、项目十一 L2TP 协议实训、综合项目一 L2TP OVER IPSEC 功能配置、综合项目二 H3C SecPath GRE over IPSec 实训、综合项目三 H3C SecPath IPSec over GRE 实训、项目十二 L2TP 穿过 NAT 接入 LNS 功能配置、项目十三 L2TP 多域接入功能的配置、综合项目四 GRE Over IPSec + OSPF 功能的配置、综合项目五 IPSec Over GRE + OSPF 功能的配置。每个项目案例按照“项目提出”、“项目分析”、“项目实施”三部曲展开。读者能够通过项目案例完成相关知识的学习和技能的训练，每个项目案例来自企业工程实践，具有典型性、实用性、趣味性和可操作性。

本书既可以作为高职院校计算机应用专业和网络技术专业理论与实践一体化教材使用，也可供相关领域的工程技术人员学习、参考。

图书在版编目 (CIP) 数据

防火墙与 VPN 技术实训教程 / 白树成主编. 北京：电子工业出版社，2014.7

网络专业校企合作开发项目式教学系列教材

ISBN 978-7-121-23015-8

I. ①防… II. ①白… III. ①计算机网络－安全技术－高等学校－教材②虚拟网络－高等学校－教材 IV. ①TP393

中国版本图书馆 CIP 数据核字（2014）第 080458 号

策划编辑：王羽佳

责任编辑：郝黎明

印　　刷：三河市鑫金马印装有限公司

装　　订：三河市鑫金马印装有限公司

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：787×1 092　1/16　印张：6.5　字数：166.4 千字

版　　次：2014 年 7 月第 1 版

印　　次：2014 年 7 月第 1 次印刷

定　　价：25.00 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 Internet 迅猛发展和网络社会化的到来，网络已经无所不在地影响着社会的政治、经济、文化、军事、意识形态和社会生活等各个方面。同时在全球范围内 ，针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量仍在持续不断增加，网络攻击与入侵行为对国家安全、经济和社会生活造成了极大的威胁。因此，网络安全已成为世界各国当今共同关注的焦点。

防火墙技术与相关 VPN 技术对于一个企业的重要性也日益凸显，因此，本教材介绍了常见的防火墙应用技术和 VPN 技术，在一定程度上来保障企业信息安全。

该教材有如下特色。

1．体现“项目导向、任务驱动”的教学特点。

从实际应用出发，从工作过程出发，从项目出发，采用“项目导向、任务驱动”的方式，通过“项目提出”、“项目分析”、“项目实施”三部曲展开教学。在教学设计上，以工作过程为参照系来组织和讲解知识，培养学生的职业技能和职业素养。

2．体现“教、学、做”一体化的教学理念。

以学到实际技能、提高职业能力为出发点，以“做”为中心，教和学都围绕着做，在学中做，在做中学，从而完成知识学习，技能训练和提高职业素养的目标。

3．本书体例采用项目案例形式。

全书设有十八个项目案例（含五个综合项目），教学内容安排由易到难、由简单到复杂，循序渐进。学生能够通过项目学习，完成相关知识的学习和技能的训练。

4．项目案例的内容体现典型性、实用性、趣味性和可操作性。

本书力求体现教材的典型性、实用性、趣味性和可操作性。根据职业教育的特点，针对企业网络安全需求的实际应用，编写防火墙与 VPN 技术课程的实用型教材。减少枯燥难懂的理论，重点对网络服务的搭建、配置与管理进行全面细致的讲解，理论联系实际多一些，突出工程实践案例的实训。

5．符合高职学生认知规律，有助于实现有效教学。

本书打破传统的学科体系结构，将各知识点与操作技能恰当地融入各个项目中，突出现代职业教育的职业性和实践性，强化实践，培养学生实践动手能力，适应高职学生的学习特点，在教学过程中注意情感交流，因材施教，调动学生的学习积极性，提高教学效果。

本书是廊坊职业技术学院教师与企业工程师共同策划编写的一本工学结合教材。

本书项目一由杨宝强编写，项目二由邵长文编写，项目三、四由刘学普编写，项目五由孙景祥编写，项目六到十八由白树成编写。廊坊职业技术学院的张昕教授在百忙之中对全书进行了审阅。在本书的编写过程中，企业工程师杨宝强提出了许多宝贵意见，电子工业出版社的王羽佳编辑为本书的出版做了大量工作。在此一并表示感谢！

本书的编写过程中参阅了大量近年来出版的相关技术资料，吸取了许多专家和同仁的宝贵经验，在此向他们深表谢意。

由于计算机网络技术发展迅速，作者学识有限，书中误漏之处难免，望广大读者批评指正。

编　者

2014 年 7 月

目　录

项目一　安全区域配置

1.1　项目提出

某公司新购买了 H3C SecPath 防火墙，该防火墙是业界功能最全面、扩展性最好的防火墙/VPN 产品，集成防火墙、VPN 和丰富的网络特性，为用户提供安全防护、安全远程接入等功能。工程师小王为了更好地为公司服务，给其他技术人员讲解，首先要了解该公司防火墙的特征与基本配置方法。

1.2　项目分析

1．项目实训目的

掌握 H3C 防火墙 SecPath F100-C 的面板与接口；
掌握在 H3C 路由/防火墙上配置安全区域的方法。

2．项目实现功能

更改防火墙配置，把接口加入/删除 安全区域；PCA ping 通 PCB。

3．项目主要应用的技术介绍

防火墙安全域：安全域（zone）是防火墙产品所引入的一个安全概念，是防火墙产品区别于路由器的主要特征。一个安全区域包括一个或多个接口的组合，具有一个安全级别。在设备内部，安全级别通过 0～100 的数字来表示，数字越大表示安全级别越高。

一般来讲，安全域与各网络的关联遵循下面的原则：内部网络应安排在安全级别较高的区域、外部网络应安排在安全级别最低的区域。具体来说，Trust 所属接口用于连接用户要保护的网络；Untrust 所属接口连接外部网络；DMZ 区所属接口连接用户向外部提供服务的部分网络；从防火墙设备本身发起的连接即是从 Local 区域发起的连接。相应的所有对防火墙设备本身的访问都属于向 Local 区域发起访问连接。

1.3　项目实施

1．项目拓扑图

安全区域配置如图 1-1 所示。

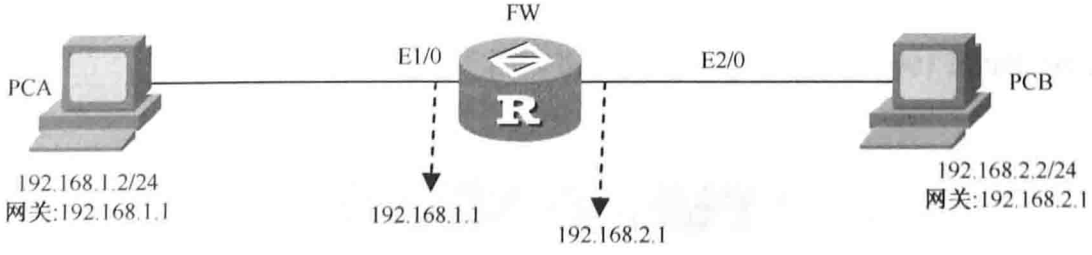


图 1-1　安全区域配置

2. 项目实训环境准备

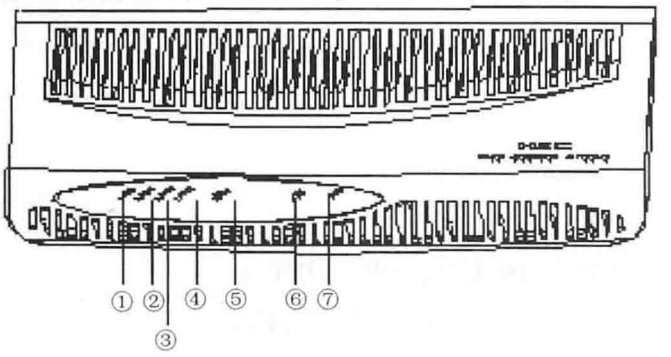
一台防火墙 SecPath F100-C，两台 PC。

为了不受原来的配置影响，在实训之前先将所有的配置数据擦除后重新启动，命令为：reboot。

3. 项目主要实训步骤

任务一　认识 H3C SecPath F100-C 防火墙前面板与接口，H3C SecPath SecPath F100-C 防火墙硬件特性

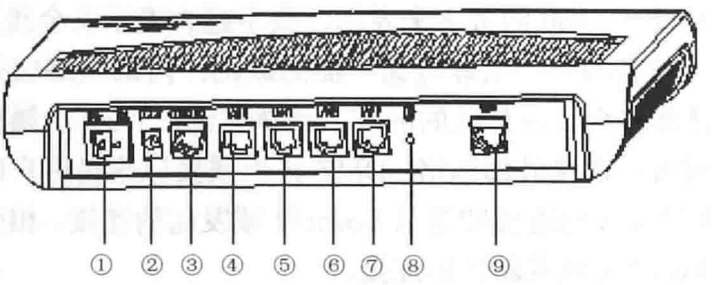
（1）H3C SecPath F100-C 防火墙前面板如图 1-2 所示。



① 以太网口指示灯 LAN3　② 以太网口指示灯 LAN2
③ 以太网口指示灯 LAN1　④ 以太网口指示灯 LAN0
⑤ 以太网口指示灯 WAN　⑥ 系统运行指示灯 SYS
⑦ 电源指示灯 PWR

图 1-2　H3C SecPath F100-C 防火墙前面板

（2）H3C SecPath F100-C 防火墙后面板如图 1-3 所示。



① 电源开关　② 电源输入插座
③ 配置口（CONSOLE）　④ 以太网口 0（LAN0）
⑤ 以太网口 1（LAN1）　⑥ 以太网口 2（LAN2）
⑦ 以太网口 3（LAN3）　⑧ 接地端子
⑨ 广域网口（WAN）

图 1-3　H3C SecPath F100-C 防火墙后面板

H3C SecPath F100-C 防火墙后面板实物图如图 1-4 所示。

图 1-4　H3C SecPath F100-C 防火墙后面板实物图

（3）指示灯含义和接口。

H3C SecPath F100-C 防火墙的指示灯共有 7 个，其含义如表 1-1 所示。

表 1-1　防火墙指示灯含义表

指示灯	含义
PWR 灯	灭：表示电源未接通； 亮：表示电源已接通
SYS 灯	闪烁：表示系统正常运行； 常亮或常灭：表示系统工作不正常
LAN0/LAN1/LAN2/LAN3/WAN 灯	灭：表示链路没有连通； 常亮：表示链路已经连通； 闪烁：表示接口有数据收发

如图 1-3 所示，H3C SecPath F100-C 防火墙主要接口包括 1 个配置口、1 个 10M 以太网口（WAN 口）和 4 个 10/100M 以太网口（LAN 口，LAN0 、LAN1 、LAN2 和 LAN3）。

任务二　配置防火墙使得两台主机互通

（1）按照图 1-1 要求，配置主机 IP 地址及网关，配置防火墙名称和两个接口 IP 地址。

```
<H3C>system
System View: return to User View with Ctrl+Z.
[H3C]sysname FW
[FW]int e1/0
[FW-Ethernet1/0]ip address 192.168.1.1 24
[FW-Ethernet2/0]ip address 192.168.2.1 24
```

（2）配置安全区域。

显示防火墙区域：

```
[FW]dis zone
local
  priority is 100
#
trust
  interface of the zone is :
  priority is 85
#
untrust
  interface of the zone is :
  priority is 5
#
DMZ
  interface of the zone is :
  priority is 50
#
```

内网（Lan）接口加入 trust 区域，外网（Wan）接口加入 untrust 区域：

```
[FW]firewall zone trust
```

```
[FW-zone-trust]add int e1/0
[FW-zone-trust]qu
[FW]firewall zone  untrust
[FW-zone-untrust]add int e2/0
```

（3）验证连通性：

```
PCB ping 网关 192.168.2.1 （e2/0 地址）
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out
Request timed out
PCA ping 网关 192.168.1.1 （e1/0 地址）
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out
Request timed out
主机 PCA ping 主机 PCB
Pinging 192.168.2.2 with 32 bytes of data:
Request timed out
Request timed out
```

为什么会不通呢？我们看一下当前配置会发现 firewall 默认规则没有配置为 permit。

（4）更改防火墙默认规则并再次验证连通性。

```
[FW]firewall packet-filter default permit
PCB ping 网关 192.168.2.1 （e2/0 地址）
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms ttl=255
Reply from 192.168.2.1: bytes=32 time=1ms ttl=255
PCA ping 网关 192.168.1.1 （e1/0 地址）
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms ttl=255
Reply from 192.168.1.1: bytes=32 time=1ms ttl=255
PCA ping PCB
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms ttl=255
Reply from 192.168.2.2: bytes=32 time=1ms ttl=255
```

1.4 项目总结与提高

（1）写出主要项目实施规划、步骤与实训所得的主要结论。

（2）登录 H3C 官网查看适合不同网络规模的防火墙产品，熟悉防火墙系列产品的特点及参数，可以为不同网络工程应用进行设备的选型。

项目二　ACL 包过滤

2.1　项目提出

网络工程师小王使用公司防火墙，为实现 ACL 包过滤功能，对内网地址 192.168.1.2/24 访问外网做限制，使其无法访问所有 WEB 界面。

2.2　项目分析

1．项目实训目的

掌握 H3C 防火墙配置 ACL 包过滤功能的配置。

2．项目实现功能

FW 内网地址为 192.168.1.1/24；公网地址为 192.168.2.1/24，配置 acl 包过滤，使 IP 地址 192.168.1.2 不能访问 Web 页面，但可以进行其他通信。

3．项目主要应用的技术介绍

ACL：访问控制列表（Access Control List，ACL）是路由器和防火墙接口的指令列表，用来控制端口进出的数据包。ACL 适用于所有的被路由协议，如 IP、IPX 等。这张表中包含了匹配关系、条件和查询语句，表只是一个框架结构，其目的是为了对某种访问进行控制。

ACL 主要包含以下几种。

基本 ACL：是只根据报文的源 IP 地址信息来制定规则的；

高级 ACL：根据报文的源 IP 地址，目的 IP 地址，IP 承载的协议类型，协议的特征等三、四层信息制定规则；

二层 ACL：根据报文的源 MAC 地址，目的 MAC 地址，VLAN 优先级，二层协议类型等信息制定规则；

用户自定义 ACL：可以以报文的头、IP 头等为基准，指定从第几个字节开始与掩码进行“与”操作，将报文提取出来的字符串和用户定义的字符串进行比较，找到匹配的报文。

2.3　项目实施

1．项目拓扑图

ACL 包过滤拓扑如图 2-1 所示。

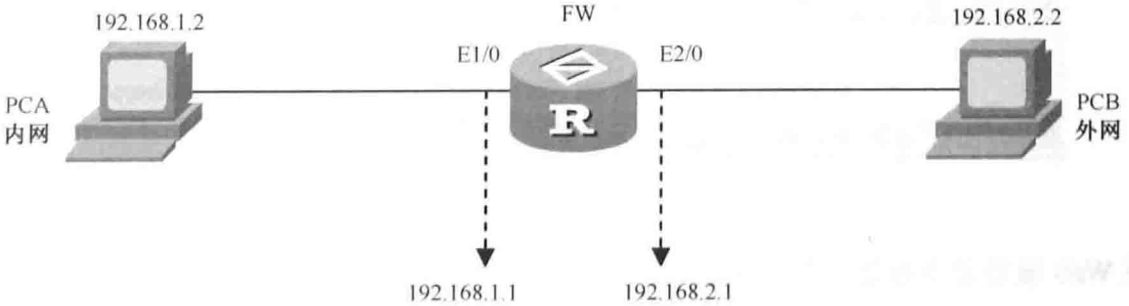


图 2-1　ACL 包过滤拓扑

2. 项目实训环境准备

一台防火墙 SecPath F100-C，两台 PC。为了不受原来的配置影响，在实训之前先将所有的配置数据擦除后重新启动，命令为：“reboot”。

3. 项目主要实训步骤

（1）PCA 和 PCB 按照要求配置 ip 地址。

（2）防火墙基本配置。

① 配置防火墙名称：

```
[H3C]sysname FW
```

② 把 E1/0 接口加入 trust 区域：

```
[FW]firewall zone trust
[FW-zone-trust]add int e1/0
```

③ 把 E2/0 接口加入 untrust 区域：

```
[FW]firewall zone untrust
[FW-zone-untrust]add int e2/0
```

④ 设置防火墙默认规则为 permit：

```
[FW]firewall packet-filter default permit
[FW]int e1/0
[FW-Ethernet1/0]ip addr 192.168.1.1 24
[FW]int e2/0
[FW-Ethernet2/0]ip addr 192.168.2.1 24
```

（3）PCB 主机模拟服务器，配置 webserver.exe。

打开 webserver.exe，初始界面自动关联上 PCB 的 IP 地址，如图 2-2 所示。

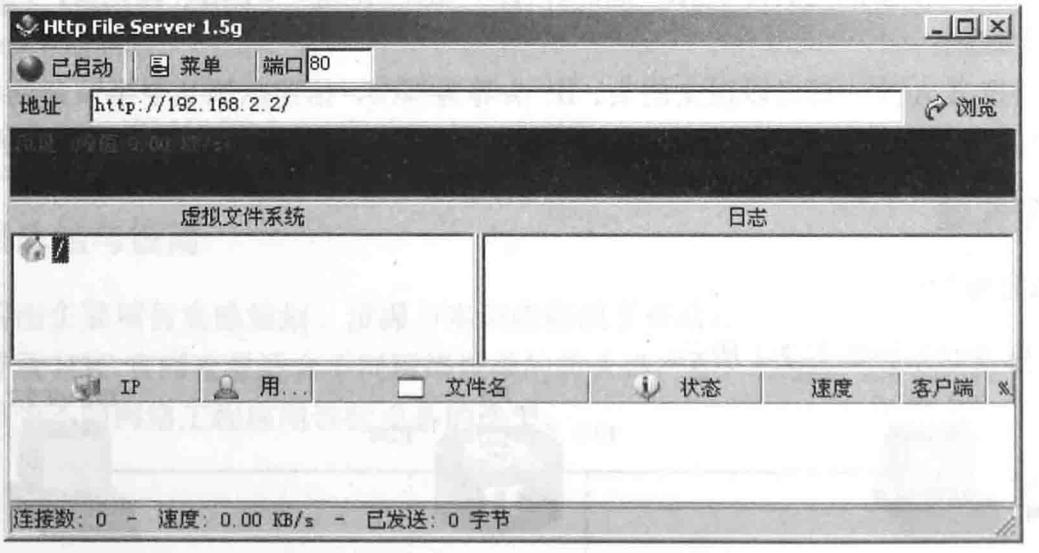


图 2-2 PCB webserver.exe 初始界面

在 Web 根目录下添加文件（index.htm），如图 2-3 所示。

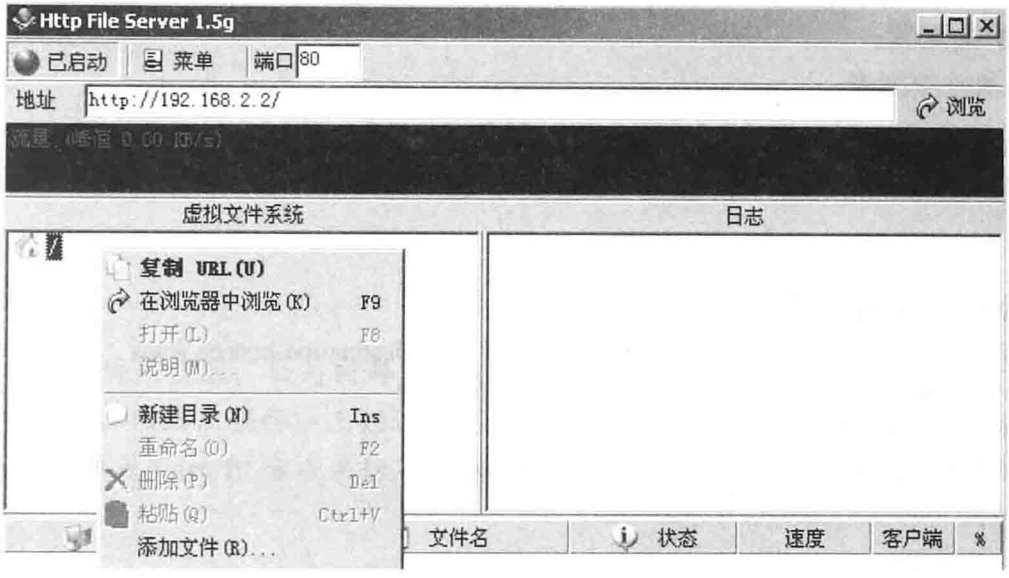


图 2-3　添加文件

添加成功并测试，发现访问记录和流量，如图 2-4 所示。

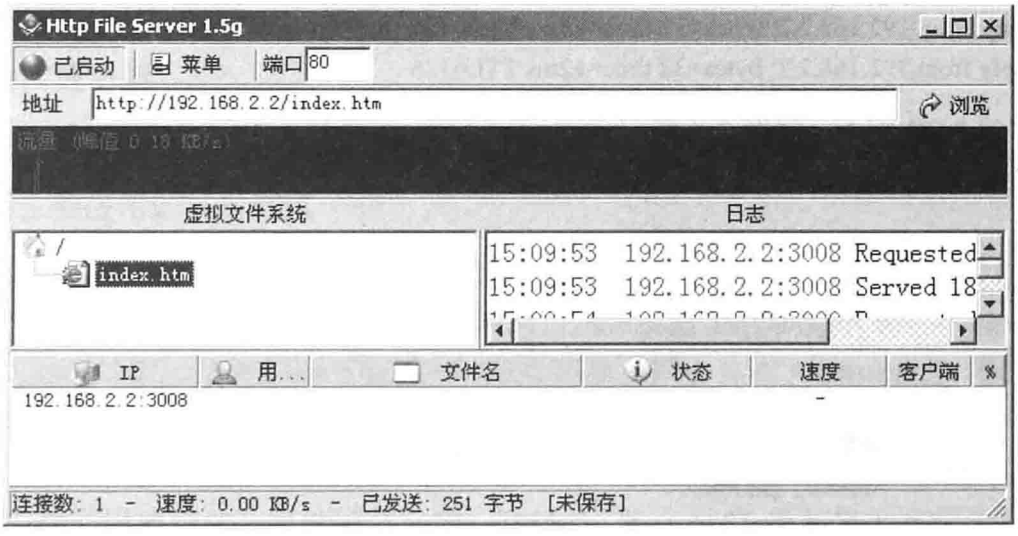


图 2-4　添加文件并测试

不配置 acl，PCA 可以访问 PCB Web 网页，如图 2-5 所示。

图 2-5　PCA 浏览 Web 服务

（4）FW 的配置。

定义基本控制列表：

```
[FW]acl number 2000
[FW-acl-basic-2000]rule 0 permit source 192.168.1.0 0.0.0.255
```

定义用于包过滤的访问控制的 ACL：

```
[FW]acl number 3005
[FW-acl-adv-3005]rule 0 deny tcp source 192.168.1.2 0 destination-port eq www
[FW-acl-adv-3005]rule 5 permit tcp source 192.168.1.2 0
[FW-Ethernet2/0]nat outbound 2000
[FW-Ethernet1/0]firewall packet-filter 3005 inbound
[FW]ip route-static 0.0.0.0 0.0.0.0 e 2/0
```

（5）验证连通性。

```
PCA ping PCB
D:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=15ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
```

PCA 访问 PCB Web，如图 2-6 所示。

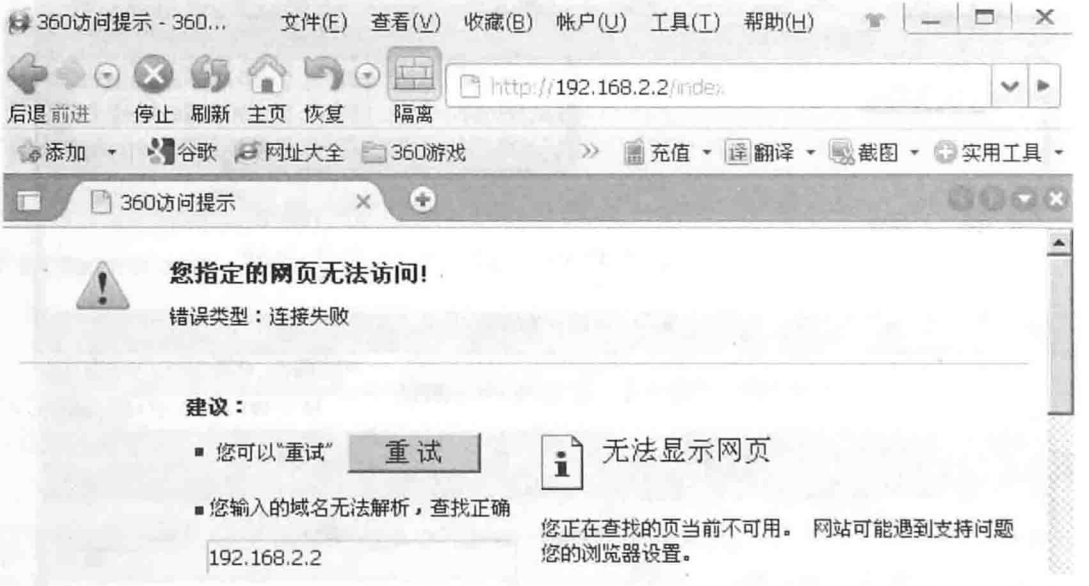


图 2-6 实施 acl 规则后 PCA 浏览 Web 服务

通过实训说明从 PCA ping PCB，可以 ping 通，但是访问 Web 却不可以实现。

2.4 项目总结与提高

（1）写出主要项目实施规划、步骤与实训所得的主要结论。

（2）思考如何禁止 PCA 主机 telnet 到 PCB 主机。

项目三　网络地址转换

3.1　项目提出

某公司搭建局域网络后，公司内部多个主机需要同时访问公网，以便充分利用互联网资源和提高工作效率，网络工程师小王经过考虑后决定配置防火墙 NAT 功能，使得内网用户通过 NAT 地址池转换或 Easy IP 方式来访问外网资源。

3.2　项目分析

1．项目实训目的

- 掌握 H3C 防火墙 NAT 地址池转换；
- 掌握 H3C 防火墙 Easy IP 方式的配置。

2．项目实现功能

内网用户通过路由器的 NAT 地址池（Easy IP 方式）转换来访问 Internet。

3．项目主要应用的技术介绍

NAT（Network Address Translation）的功能，就是指在一个网络内部，根据需要可以随意自定义的 IP 地址 ，而不需要经过申请。在网络内部，各计算机间通过内部的 IP 地址进行通信。而当内部的计算机要与外部 internet 网络进行通信时，具有 NAT 功能的设备（如路由器或者防火墙）负责将其内部的 IP 地址转换为合法的 IP 地址（即经过申请的 IP 地址）进行通信。

NAT 是一种私网地址与公网地址之间的一种转换，那么 NAT 设备就需要准备一定数量的公网地址，公网地址数的多少一方面取决于内网用户的多少，另一方面也取决于 NAT 设备的转换算法。NAT 可以最大化地利用 IPv4 地址资源，节约 IPv4 地址数量。除此之外防火墙还具备一定的安全功能，可以隐藏局域网的拓扑结构。

H3C 防火墙主要包含以下几种 NAT 方式。

Basic NAT：不涉及端口的转换，其 NAT 转换后防火墙记录的会话数可以无限多次，但是防火墙 NAT 模块工作的部分只是 IP 地址的转换，端口并不需要防火墙处理，所以防火墙 Basic NAT 能够转换的最大次数只根据地址池的大小而定，也是有限次的。同时它也不能节省 IP 地址。

NAPT：NAPT 方式属于多对一的地址转换，通过使用“IP 地址＋端口号”的形式进行转换，使多个私网用户可共用一个公网 IP 地址访问外网。因此是地址转换实现的主要形式。

Easy IP：NAT 设备直接使用出接口的 IP 地址作为转换后的源地址，工作原理与普通 NAPT 相同，是 NAPT 的一种特例，适用于拨号接入 Internet 或动态获得 IP 地址的场合。

3.3 项目实施

1. 项目拓扑图

网络地址转换拓扑如图 3-1 所示。

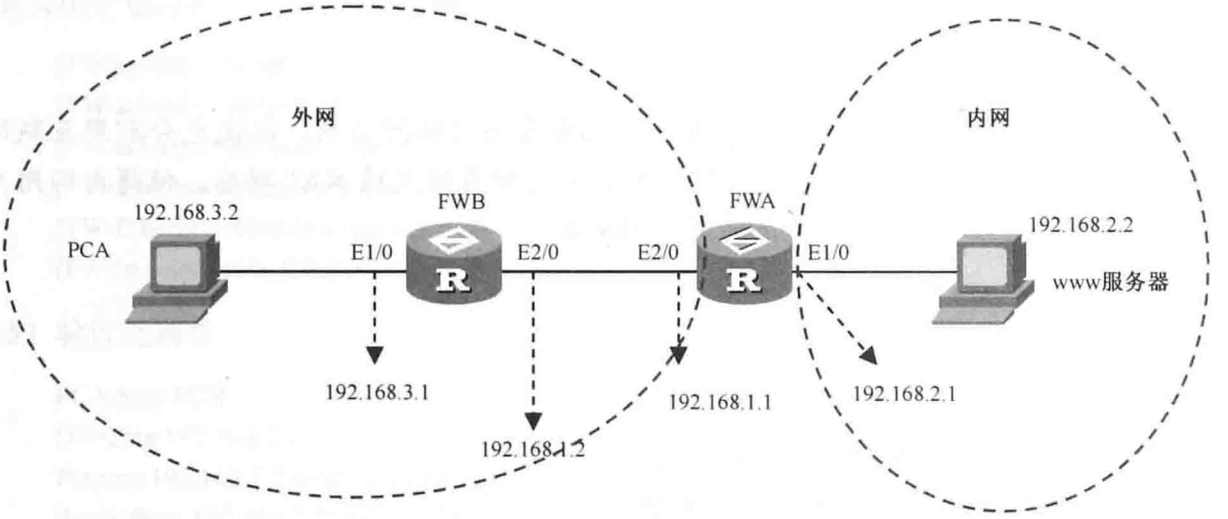


图 3-1 网络地址转换拓扑

2. 项目实训环境准备

两台防火墙 H3C SecPath F100-C，两台 PC。

3. 项目主要实训步骤

任务一 地址池方式做 NAT 的配置

（1）PCA 和 PCB 按照要求配置 IP 地址（并配置网关）。

（2）防火墙基本配置。

配置防火墙名称：

```
[H3C]sysname FWA
[H3C]sysname FWB
```

把 E1/0 接口加入 trust 区域：

```
[FWA]firewall zone trust
[FWA-zone-trust]add int e1/0
[FWB]firewall zone trust
[FWB-zone-trust]add int e1/0
```

把 E2/0 接口加入 untrust 区域：

```
[FWA]firewall zone untrust
[FWA-zone-untrust]add int e2/0
[FWB]firewall zone untrust
[FWB-zone-untrust]add int e2/0
```

设置防火墙默认规则为 permit，并在相关接口配置 IP 地址：

```
[FWA]firewall packet-filter default permit
[FWA-Ethernet1/0]ip addr 192.168.2.1 24
[FWA-Ethernet2/0]ip addr 192.168.1.1 24
[FWB]firewall packet-filter default permit
[FWB-Ethernet1/0]ip addr 192.168.3.1 24
[FWB-Ethernet2/0]ip addr 192.168.1.2 24
```

（3）FWA 和 FWB 的配置。

配置用户 NAT 的地址池：

```
[FWA]nat address-group 1 192.168.1.10 192.168.1.20
```

配置允许进行 NAT 转换的内网地址段：

```
[FWA]acl number 2000
[FWA-acl-basic-2000]rule 0 permit source 192.168.2.0 0.0.0.255
[FWA-acl-basic-2000]rule 1 deny
```

在出接口上进行 NAT 转换：

```
[FWA-Ethernet2/0]nat outbound 2000 address-group 1
```

配置静态路由：

```
[FWA]ip route-static 0.0.0.0 0.0.0.0 192.168.1.2
[FWB]ip route-static 192.168.2.0 24 192.168.1.1
```

（4）验证连通性。

内网主机 PCB ping 外网主机 PCA：

```
D:\>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=15ms TTL=126
Reply from 192.168.3.2: bytes=32 time=12ms TTL=126
Reply from 192.168.3.2: bytes=32 time=12ms TTL=126
```

结论：从 PCB　ping PCA，可以 ping 通。

任务二　Easy NAT 的配置

（1）PCA 和 PCB 按照要求配置 IP 地址（与任务一相同）。

（2）防火墙基本配置（与任务一相同）。

（3）FWA 和 FWB 的配置。

配置允许进行 NAT 转换的内网地址段：

```
[FWA]acl number 2000
[FWA-acl-basic-2000]rule 0 permit source 192.168.2.0 0.0.0.255
[FWA-acl-basic-2000]rule 1 deny
```

在接口 E2/0 上进行 NAT 转换：

```
[FWA-Ethernet2/0]nat outbound 2000
```

配置静态路由：