Network security project of actual combat

网络安全项目实战

NETWORK SECURITY PROJECT OF ACTUAL COMBAT

主　编：李　敏　赵宇枫
副主编：胡方霞　罗惠琼
主　审：张　毅

重庆大学出版社
http://www.cqup.com.cn

网络安全项目实战

WANGLUO ANQUAN XIANGMU SHIZHAN

主　编　李　敏　赵宇枫
副主编　胡方霞　罗惠琼
主　审　张　毅

重庆大学出版社

内 容 简 介

本书分为四大部分，选择目前最主流的网络安全厂商的典型设备防火墙、IPS、VPN、UTM 为演练对象，共设计了 24 个教学项目。每个项目通过任务分解，图文并茂地按步骤详解了其应用配置和使用。另外，在防火墙、IPS、VPN 设备后选择了同时具有三者功能的 UTM 设备进行演练，既是顺应当前网络设备集成化的发展趋势，也是对前续项目的综合、强化演练。全书采用真实场景，与实际工作环境一致，既便于学生的职业技能培养，也便于学生岗位能力的塑造。

图书在版编目(CIP)数据

网络安全项目实战/李敏，赵宇枫主编. —重庆：重庆大学出版社，2013.7

ISBN 978-7-5624-7440-1

Ⅰ.①网… Ⅱ.①李…②赵… 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(2013)第 127550 号

网络安全项目实战

主　编　李　敏　赵宇枫

副主编　胡方霞　罗惠琼

主　审　张　毅

策划编辑：彭　宁　何　梅

责任编辑：文　鹏　　版式设计：彭　宁　何　梅

责任校对：贾　梅　　责任印制：赵　晟

*

重庆大学出版社出版发行

出版人：邓晓益

社址：重庆市沙坪坝区大学城西路 21 号

邮编：401331

电话：(023)88617190　88617185(中小学)

传真：(023)88617186　88617166

网址：http://www.cqup.com.cn

邮箱：fxk@cqup.com.cn（营销中心）

全国新华书店经销

重庆联谊印务有限公司印刷

*

开本：787×1092　1/16　印张：12.75　字数：318 千

2013 年 7 月第 1 版　2013 年 7 月第 1 次印刷

印数：1—3 000

ISBN 978-7-5624-7440-1　定价：25.00 元

前言

高等职业教育是针对职业岗位的实际需要而设置的职业岗位定向的教育。其教学体系的重中之重，就是对于职业技能的培养。本书就是这样一本针对学生技能培养的关于网络安全的教材。它选用了当前主流的网络安全厂商 H3C 的相应设备，按照“项目引导”“任务驱动”的指导思想编写，将网络安全设备的应用配置分解成不同的项目和任务，用图例展现。

本书的主要特色是搭建真实项目环境，进行真实项目演练。全书分为四大部分 24 个项目，每个项目分别演练了 FW、IPS、VPN、UTM 等网络安全设备的不同功能配置。本书层次清晰，递进合理。第四部分 UTM 由于是新型的网络安全设备，具有前三种设备的安全防护功能，因此可以看作是对前三种设备的综合强化演练。本书可以作为高职高专、成人高校网络相关专业“网络安全”课程的主要教材，在有前续课程概要地学习完主机安全和网络安全的基本原理后，本书针对相应网络设备进行项目演练和实训，深化学生技能培养。当然，在没有前续课程的前提下，也可以在本书每部分的基础知识提要和重点知识整理的框架下，用本书展开理论与实践一体化教学。同时，本书亦可以作为本科院校网络相关专业的技能实训教材和网络安全从业人员的工具参考书。

对于高职学生，本课程建议安排 80 学时进行理论与实践一体化学习。当然，由于网络设备更新换代较快，也可以在此基础上安排一定的辅助学时深化网络安全理论知识和新技术的学习。

序号	内　容	学时	辅助学时
1	防火墙(FW)	8	8
2	入侵防御系统(IPS)	8	8
3	虚拟专用网(VPN)	16	16
4	统一威胁管理(UTM)	48	24
合计		80	56

本书由李敏、赵宇枫担任主编，胡方霞、罗惠琼担任副主编，同时邀请两位企业高级工程师孙波和廖嘉林参与了编写。每个项目均为编者们亲自参与设计，同时也参考了大量的设备使用说明文档和相关资料。

本书由重庆大学张毅教授主审。

由于编者水平有限，时间仓促，书中不妥之处在所难免，恳请广大读者批评指正。

编　者

2013 年 3 月

目录

第 1 部分　防火墙(FW)

第 2 部分　入侵防御系统(IPS)

第 3 部分　虚拟专用网(VPN)

第 4 部分　统一威胁管理(UTM)

第 1 部分
防火墙(FW)

概　述

[基本知识提要]

• 什么是防火墙?

防火墙,又称 FW(Fire Wall),是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。它是一种获取安全性方法的形象说法,是一种计算机硬件和软件的结合。

• 防火墙主要分类

①包过滤防火墙:根据一组规则允许一些数据包通过,同时阻塞其他数据包,规则可以根据网络层协议(如 IP)信息或者传输层(如 TCP/UDP 头部)信息制定。

②应用代理防火墙:作为应用层代理服务器存在于信任与非信任网络之间,在应用层协议层面上提供高安全级别的保护。

③状态检测防火墙:比包过滤防火墙具有更高的智能和安全性。防火墙根据访问策略在数据流会话成功建立后记录状态信息并实时更新,所有后续数据报文都要与状态表信息相匹配,否则报文将被阻断。

现代防火墙基本为上述 3 种类型的综合体。

• 防火墙应该具有的安全特性

①网络隔离及访问控制;

②攻击防范;

③网络地址转换;

④应用层状态检测;

⑤内容过滤;

⑥安全管理。

[重点知识整理]

• **网络隔离及访问控制**

网络隔离及访问控制原理如图 1.1 所示。

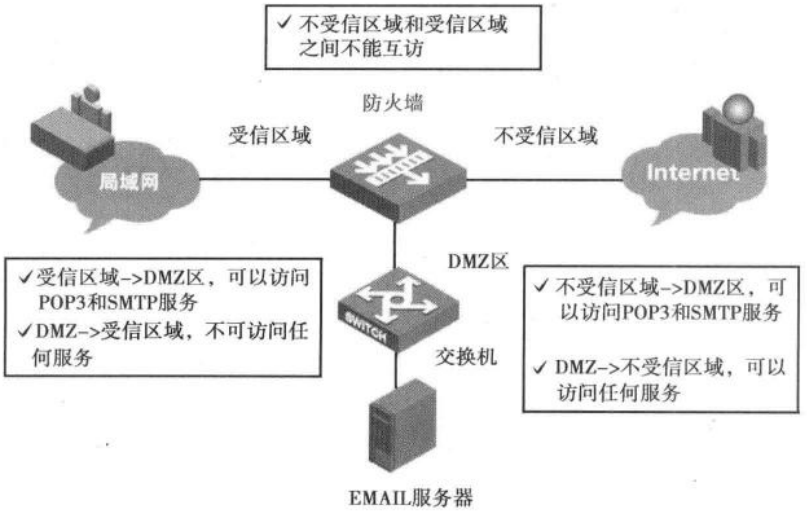

图 1.1　网络隔离及访问控制

• **攻击防范**

攻击防范原理如图 1.2 所示，防火墙在保证业务访问的同时阻止恶意攻击流量进入内部网络。

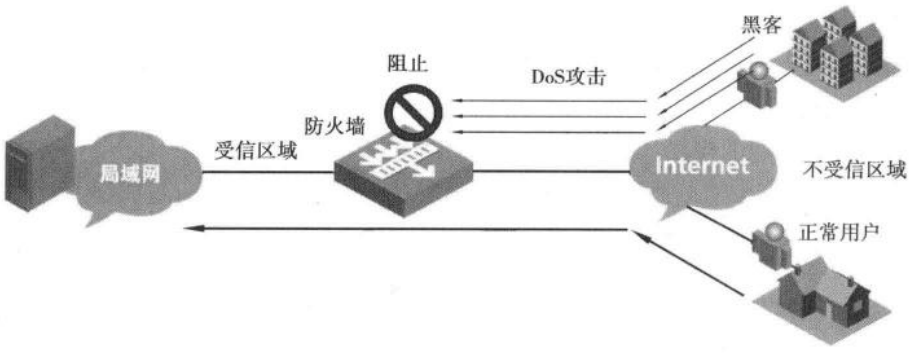

图 1.2　攻击防范原理

• **网络地址转换(NAT)**

网络地址转换原理如图 1.3 所示。网络地址转换有效解决了全球 IPv4 地址短缺的问题，并且对外隐藏了内部网络结构与设备，提供了一定的安全保障。

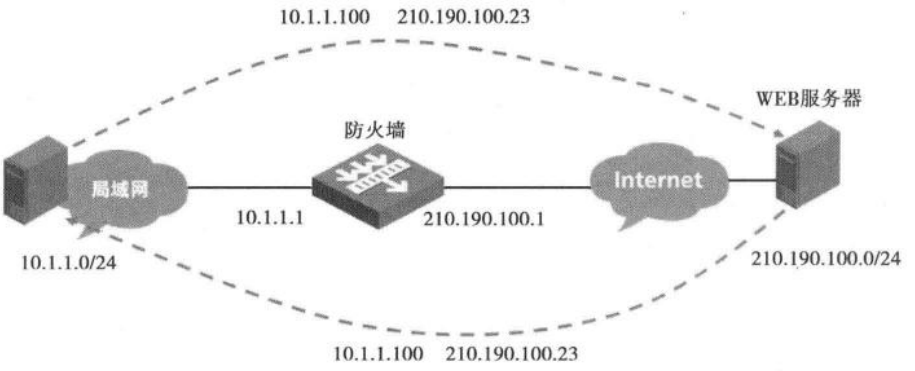

图 1.3　NAT 转换原理

• 应用层状态检测包过滤(ASPF)

与传统静态包过滤检测机制相比,ASPF 可以实时监测通信过程中交互的报文并动态建立数据包过滤机制,解决了简单包过滤防火墙无法处理动态协商通信端口协议和控制单向访问的问题,如图 1.4 所示。

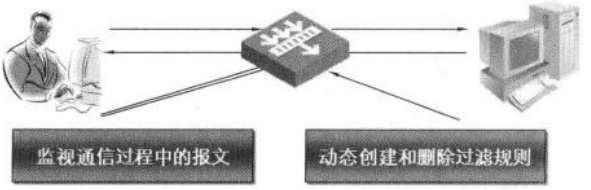

图 1.4　ASPF 原理

• 内容过滤

内容过滤功能可实现对访问与工作无关、非法网站等的阻止与审计,如图 1.5 所示。

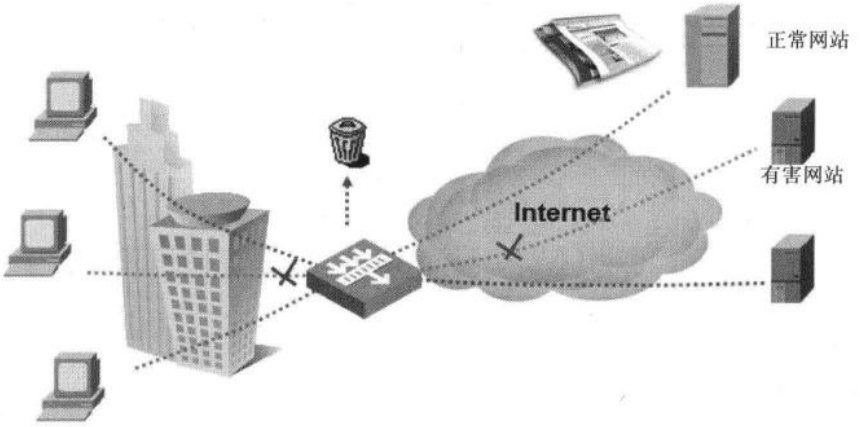

图 1.5　内容过滤示意图

• 防火墙与路由器

防火墙与路由器的安全特性差异见表 1.1。

表 1.1　防火墙与路由器的安全特性差异

常用安全特性	防火墙	路由器
基础设施及其安全(路由、链路冗余、QoS 等)	√	√
实现有效的访问控制(ACL、ASPF)	√	√
保证内部网络的隐蔽性(NAT)	√	√
重要的私有数据保护(VPN)	√	√
基于会话表的连接监控与状态热备	√	×
基于 3 层/4 层协议的攻击防护	√	×
针对网页、邮件等内容过滤	√	×
与 IDS 设备联动	√	×
安全日志信息(NAT 日志、ASPF 策略日志、流日志、攻击防范日志)	√	×

[学习目标]

①了解防火墙及防火墙技术分类与特性;

②了解防火墙体系结构与业务特性;

③掌握防火墙功能原理与配置方法;

④掌握防火墙典型组网应用;

⑤掌握防火墙常见问题处理方法。

[学时分配]

防火墙学时分配如表 1.2 所示。

表 1.2　防火墙学时分配表

项目名称	项目学时	辅助学时
项目 1　SecPath FW 安全区域与访问控制	2	2
项目 2　SecPath FW NAT 功能	2	2
项目 3　SecPath FW ASPF 功能	2	2
项目 4　SecPath FW 报文统计与攻击防范	2	2
合　计	8	8

项目 1

SecPath FW 安全区域与访问控制

[项目内容与目标]

- 掌握防火墙安全区域基本原理及配置方法；
- 掌握防火墙 ACL 相关命令及配置方法；
- 掌握防火墙包过滤技术基本原理及配置方法。

[项目组网图]

项目组网如图 1.6 所示：两台 PC 机模拟客户端，地址分别为 10.0.0.101 和 10.0.0.102，通过 S3600 交换机做二层转发；网关配置在防火墙 F100A 的 Eth0/0 口，地址为 10.0.0.1；服务器连接在防火墙 F100A 的 Eth1/0 口，防火墙接口地址为 172.31.0.1，服务器地址为 172.31.0.100。

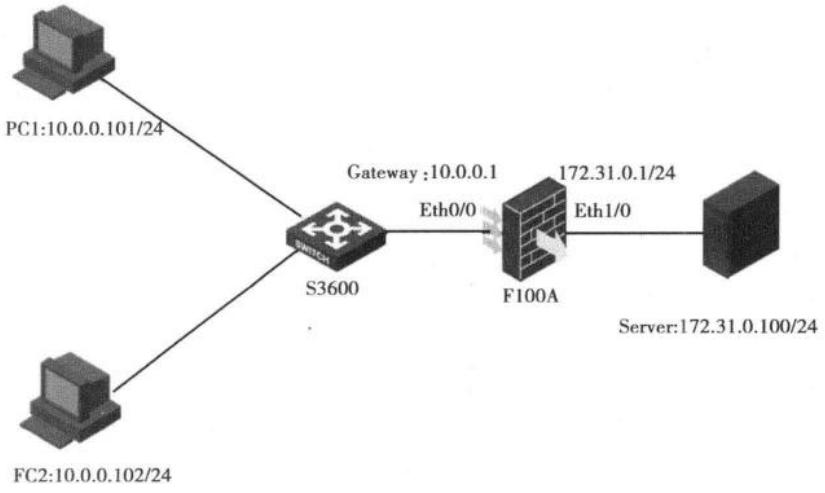

图 1.6　项目组网

[背景需求]

本项目背景是：通过 SecPath 防火墙对访问服务器的客户端进行控制，允许 PC1 访问服务器提供的服务，禁止 PC2 对服务器进行访问。

[所需设备和器材]

本项目所需之主要设备器材如表 1.3 所示。

表 1.3 所需设备和器材

名称和型号	版 本	数 量	描 述
F100A	CMW R1662P14	1	
S3600	CMW R1702P28	1	
服务器	—	1	可以用普通 PC 模拟
PC	Windows XP SP3	2	
第 5 类 UTP 以太网连接线	—	4	

[任务实施]

任务 1 防火墙接口及安全区域基本配置

步骤 1:F100A 防火墙接口地址配置

```
#
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
 ip address 172.31.0.100 255.255.255.0
#
interface Ethernet1/1
#
interface Ethernet1/2
#
```

步骤 2:F100A 防火墙安全区域配置

```
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet0/0
 set priority 85
```

```
#
firewall zone untrust
 add interface Ethernet1/0
 set priority 5
#
firewall zone DMZ
 set priority 50
#
```

步骤 3:F100A 防火墙缺省包过滤策略配置

```
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
```

步骤 4:S3600 交换机配置

在本项目中,S3600 作二层交换机,使用交换机默认的 VLAN1 即可满足 PC 间、PC 与防火墙间的二层通信。以 PC1、PC2、防火墙与 S3600 交换机的 1、2、3 号端口相连为例:

```
#
vlan 1
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
```

步骤 5:PC 及服务器地址及网关配置

请参考组网图 1.6 配置 PC 及服务器 IP 地址,具体配置过程略。配置示例如图 1.7 所示。

步骤 6:验证 PC 与服务器之间是否可以正常通信

可通过 ping 命令、HTTP 访问、FTP 访问等操作验证两台 PC 与服务器间是否可以正常通信,验证过程略。

任务 2　防火墙访问控制策略配置

以本项目任务 1 的配置结果为基础,在防火墙 F100A 上增加包过滤策略。

步骤 1:配置 ACL

```
#
acl number 2001
 rule 5 permit source 10.0.0.101 0
 rule 10 deny source 10.0.0.102 0
#
```

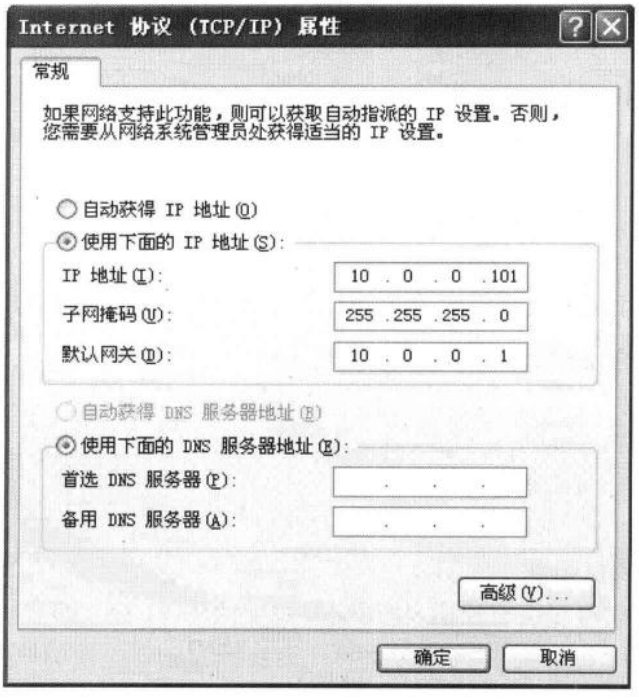

图 1.7　TCP/IP 属性配置

步骤 2:在防火墙接口配置包过滤策略

```
#
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
 firewall packet-filter 2001 inbound
#
```

步骤 3:验证设备配置结果是否满足需求

可通过 ping 命令、HTTP 访问、FTP 访问等操作验证 PC1 仍然可以正常访问服务,PC2 无法访问。

项目 2

SecPath FW NAT 功能

[项目内容与目标]

- 掌握防火墙 NAT 功能基本原理;
- 掌握防火墙 NAT Outbound、NAT Static、NAT Server 配置方法。

[项目组网图]

项目组网如图 1.8 所示:两台 PC 机模拟公司内网用户,地址分别为 10.0.0.101 和 10.0.0.102,通过 S3600 交换机做二层转发;网关配置在防火墙 F100A 的 Eth0/0 口,地址为 10.0.0.1;利用一台服务器模拟外网,连接在防火墙 F100A 的 Eth1/0 口,防火墙接口地址为 172.31.0.1,服务器地址为172.31.0.100。

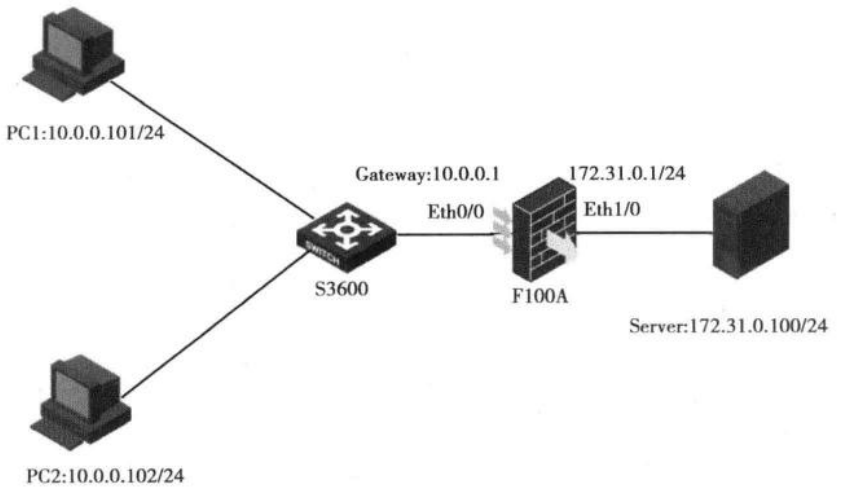

图 1.8 项目组网

[背景需求]

通过 SecPath 防火墙进行网络地址转换,实现当内网用户主动访问外网时,将源地址转换为地址池中的某个地址,以达到共享网络地址资源、对外屏蔽内部网络的目的;实现外网用户直接通过外部地址访问内网服务;实现一对一静态映射,使得某台内网主机固定使用某外网地址,并实现双向访问。