课题	第 13 章　防火墙与 Squid 代理服务器搭建及应用
课时	4 课时（160 min）
教学目标	**知识技能目标：** （1）防火墙的基本概念、分类与作用 （2）Squid 代理服务器的分类及特点 （3）Linux 防火墙的架构及包过滤的匹配流程 （4）iptables 命令的格式和使用 （5）NAT 的配置方法 **素质目标：** （1）培养认真细致的工作态度和工作作风 （2）养成刻苦、勤奋、独立思考和细心检查的学习态度和学习习惯
教学重难点	**教学重点：**防火墙的基本概念、分类与作用，Squid 代理服务器的分类及特点 **教学难点：**Linux 防火墙的架构及包过滤的匹配流程，iptables 命令的格式和使用，NAT 的配置方法
教学方法	问答法、讨论法、讲授法、演示法、练习法
教学用具	电脑、投影仪、多媒体课件、教材
教学过程	**主要教学内容及步骤**
考勤	**【教师】清点上课人数，记录好考勤** **【学生】班干部报请假人员及原因**
第 1、2 节课	
问题导入	**【教师】提出以下问题：** 什么是防火墙？防火墙有哪些功能？ **【学生】聆听、思考、回答**
传授新知	**【教师】通过学生的回答，引入新知，讲解防火墙的基础知识，iptables 服务的安装，使用 iptables 实现 NAT 服务等知识** **14.1　防火墙** **14.1.1　认识防火墙（firewall）** 1．什么是防火墙 2．防火墙的功能 3．防火墙的类型 （1）按采用的技术划分。 ① 包过滤型防火墙 ② 代理服务器型防火墙 （2）按实现的环境划分。 ① 软件防火墙 ② 硬件（芯片级）防火墙

14.1.2 Linux 防火墙概述

1. Linux 防火墙的历史

2. Linux 防火墙的架构

Linux 防火墙系统由以下两个组件组成。

（1）netfilter。

（2）iptables。

14.1.3 iptables 规则的分层结构

1. 表（tables）

iptables 提供的这些表，专表专用，作用分别如下：

filter 表：nat 表

mangle 表

raw 表

2. 链（chains）

链用来处理不同流向的数据包。

INPUT 链 OUTPUT 链

FORWARD 链

PREROUTING 链

POSTROUTING 链

用户自定义链

3. 规则（rules）

14.1.4 数据包过滤匹配流程

表间的优先顺序，依次为：raw，mangle，nat，filter。

链间的匹配顺序：

入站数据出站数据

转发数据

14.1.5 代理服务器 Squid

1. Squid 代理服务器的作用

2. Squid 代理服务器的工作流程

3. Squid 代理服务器的分类及特点

Squid 代理服务器按照代理的设置方式可分为以下 3 种：

普通（标准）代理服务器

透明代理服务器

反向代理服务器

14.2 iptables 服务的安装

1. 安装 iptables 软件包

2．iptables 的常用管理命令

（1）添加、插入规则

（2）查看规则

【注意】

L 选项要放在 vn 后，否则会将 vn 当成链名。

（3）创建、删除用户自定义链

（4）删除、清空规则

（5）设置内置链的默认策略

（6）匹配条件的设置

（7）规则的保存与恢复

实例 1——管理 icmp

实例 2——设置远程登录限制

实例 3——作为专门 Web 服务器终端的配置

【注意】

其中：X 为物理机网卡 IP 地址的第 4 段。

14.3 使用 iptables 实现 NAT 服务

可使用的私网地址有：

A 类地址

B 类地址

C 类地址

1．NAT 服务的概念及分类

2．使用 SNAT 实现使用私网 IP 的多台主机共享上网

3．使用 DNAT 实现向公网发布私网的应用服务器

【注意】

内部网的计算机网关要设置为防火墙的内网卡的 ip 地址（10.10.1.254）。

4．设置默认策略

【注意】

默认全部链都是开启的，所以有些命令可不操作，另外，本文没用到 mangle 表，所以不做处理，mangle 表主要用在数据包的特殊变更处理上，比如修改 TOS 等特性。

5．设置回环地址

6．连接状态设置

7．设置 80 端口转发

	8．DNS 相关设置 9．允许管理员通过外网进行远程管理，开启 22 端口 10．允许内网主机登录 MSN 和 QQ 相关设置 11．允许内网主机收发邮件 12．NAT 端口映射设置 13．内网机器对外发布 Web 网站 14．禁止访问具体域名和 IP 地址 15．禁止 Internet 上的计算机通过 ICMP 协议 ping 到代理服务器的 eth0 接口 16．保存与恢复 iptables 配置 17．重启服务 **【学生】聆听、思考、记忆**
课堂实践	**【教师】组织学生以小组为单位完成以下任务：** 请在 Linux 操作系统下安装 iptables 服务，并使用 iptables 实现 NAT 服务，然后总结遇到的困难和解决方法。 **【学生】按要求进行操作，先完成的学生帮助本组其他学生完成操作，如遇问题可询问教师** **【教师】巡堂辅导，及时解决学生的问题**
课堂小结	**【教师】简要总结本节课的要点** 防火墙 iptables 服务的安装 使用 iptables 实现 NAT 服务 **【学生】总结回顾知识点**
作业布置	**【教师】布置课后作业** 请根据课堂上所学知识，完成教材课后练习。 **【学生】完成课后任务**
第 3、4 节课	
问题导入	**【教师】提出以下问题：** 你会 Squid 服务器的安装吗？ **【学生】聆听、思考、回答**
传授新知	**【教师】通过学生的回答，引入新知，讲解 Squid 服务器的安装、认识 Squid 配置参数与初始化、普通代理服务器的配置、透明代理服务器的配置及反向代理服务器的配置等知识** **14.4　Squid 服务器的安装** 1．检查是否安装了 Squid 服务器 2．安装 Squid 软件包 **14.5　认识 Squid 配置参数与初始化** 1．设置监听的端口

	2．设置内存缓冲大小 3．设置保存到缓存的最大文件的大小 4．设置用户下载的最大文件的大小 5．设置硬盘缓存的大小 6．设置 DNS 服务器的地址 7．设置运行 Squid 主机的名称 8．设置访问控制 9．设置日志文件 ①　用户访问 Internet 的日志——cache_access_log /var/log/squid/access.log。 ② 缓存日志文件——cache_log /var/log/squid/cache.log。 ③　缓存中网站传输情况的日志文件——cache_store_log /var/log/squid/store.log。 10．初始化 Squid 缓存目录 **14.6　普通代理服务器的配置** **14.7　透明代理服务器的配置** **14.8　反向代理服务器的配置** **【学生】聆听、思考、记忆**
课堂实践	**【教师】组织学生以小组为单位完成以下任务：** 请在 Linux 操作系统下安装 Squid 服务器，并进行各种配置，然后总结遇到的困难和解决方法。 **【学生】按要求进行操作，先完成的学生帮助本组其他学生完成操作，如遇问题可询问教师** **【教师】巡堂辅导，及时解决学生的问题**
课堂小结	**【教师】简要总结本节课的要点** Squid 服务器的安装 认识 Squid 配置参数与初始化 普通代理服务器的配置 透明代理服务器的配置 反向代理服务器的配置 **【学生】总结回顾知识点**
作业布置	**【教师】布置课后作业** 请根据课堂上所学知识，完成教材课后练习。 **【学生】完成课后任务**

教学反思	