

实验八：防火墙实现访问控制

一、实验简介

在园区网中部署防火墙，实现访问控制。

二、实验目的

- 1、理解包过滤防火墙的工作原理；
- 2、掌握在 eNSP 中引入防火墙设备的方法；
- 3、掌握利用防火墙加强园区网安全管理的方法。。

三、实验学时

2 学时

四、实验类型

综合型

五、实验需求

- 1、硬件

每人一台计算机。

- 2、软件

计算机安装 Windows 10 操作系统、eNSP 网络仿真软件、VirtualBox 虚拟化软件

- 3、网络

实验本身内容不需要访问互联网。

- 4、工具

无

六、实验拓扑

本实验的网络拓扑如图 8-1 所示。其中，FW-1 是防火墙，R1~R3 是路由器，RS-1~RS-5 是路由交换机、SW-1~SW-5 是二层交换机，Host-1~Host-8 是用户主机，Service-DNS 表示 DNS 服务器（仿真），Service-Web 表示 Web 服务器（仿真），Service-FTP 表示 FTP 服务器（仿真）。



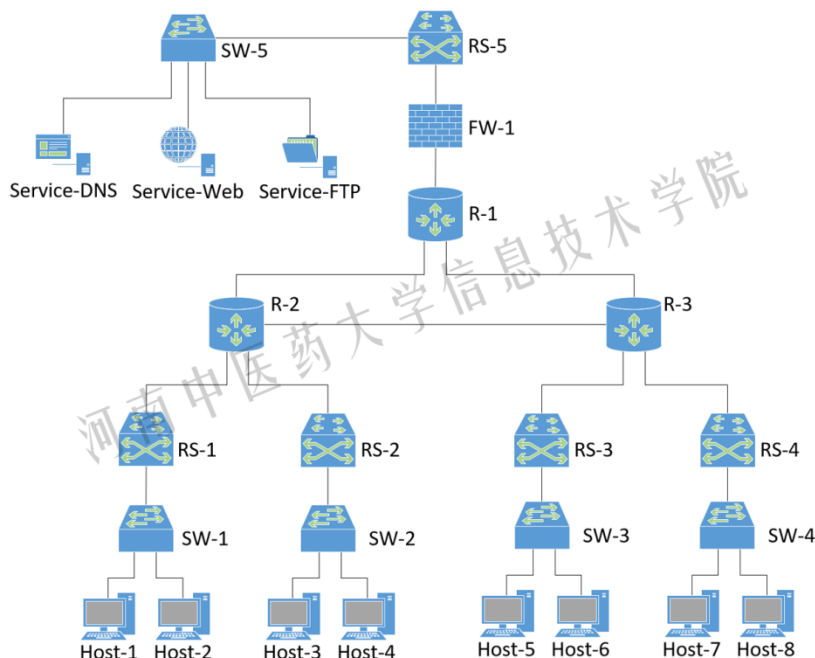


图 8-1 实验八的网络拓扑

七、实验任务及要求

1、任务 1：设计全网 IP 地址

(1) 所有用户主机的 IP 地址格式为 192.A.*.*，其中 A 为学生本人学号后 2 位，*表示该值由学生自定。各用户主机分属于不同 VLAN，其 IP 地址应属于不同的网段；

(注意：用户主机的 IP 地址通过 DHCP 自动获取)

(2) 各路由器互连接口的地址格式为 10.A.*.*，其中 A 为学生本人学号后 2 位，*表示该值由学生自定；

(3) 各个仿真服务器设置静态 IP 地址，格式为 172.16.A.*/24，其中 A 为学生本人学号后 2 位。

(4) 默认网关地址，由本网段最后一个可用单播地址表示。

2、任务 2：在 eNSP 中部署园区网

在 eNSP 中部署园区网，完成各网络设备的配置。

3、任务 3：设计防火墙安全策略

在网络连通正常的前提下，通过配置防火墙策略，实现以下安全目的：

- (1) Host-1~Host-8 主机不可以 Ping 通 Web 服务、FTP 服务、DNS 服务；
- (2) Host-1~Host-8 主机可以使用 DNS 解析服务；
- (3) 仅允许 Host-1-Host-4 主机可以以 Web 方式访问 Web 服务；



(4) 仅允许 Host-5~Host-8 主机可以访问 FTP 服务;

(5) 任何地址到任何地址的其他服务均禁止访问。

任务 4: 配置防火墙实现访问控制

配置防火墙实现用户主机对服务器的访问控制。

八、实验步骤

1、在 eNSP 中部署园区网 (5 分)

根据网络拓扑, 在 eNSP 中部署园区网并启动各设备。

由于本实验中要通过仿真的方式, 测试用户主机对各种网络服务的访问效果, 从而实现防火墙对 DNS、FTP、Web 访问的控制。原来使用的 PC 终端无法实现这些操作, 因此 Host-1~Host-8 采用 eNSP 中“终端”设备里的 Client。服务器(包括 DNS、DHCP、FTP)采用 eNSP 中“终端”设备里的 Server。

防火墙采用 USG6000V。其他设备型号同前面实验。

eNSP 中, 防火墙在第一次启动时, 需要载入设备文件, 扫描二维码 8-1 可转到本课程教材网站-【学习资源】, 在【软件资源】中下载“eNSP-plugin-vfw_usg.zip”解压缩即可得到设备文件。载入防火墙设备文件的操作可参考二维码 8-2 或教材项目十一任务 1。

注意: 华为防火墙初始用户名和密码分别为 admin, Admin@123。

2、配置用户主机地址 (5 分)

为了测试仿真服务器提供的服务, 此处的用户主机使用 Client 终端。配置各用户主机的 IP 地址。

具体操作参考二维码 8-3 或教材项目十一任务二

3、配置网络设备 (30 分)

配置除防火墙之外的其他网络设备

具体操作参考二维码 8-3 或教材项目十一任务二。



二维码 8-1 下载设备文件



二维码 8-2 防火墙基本配置



二维码 8-3 园区网中部署防火墙



4、配置仿真服务（10 分）

- (1) 创建测试 Web 服务所需要文件夹与文件
- (2) 创建测试 FTP 服务所需要文件夹与文件
- (3) 配置 DNS 仿真服务
- (4) 配置 Web 仿真服务
- (5) 配置 FTP 仿真服务

具体操作参考二维码 8-3 或教材项目十一任务二。

5、配置防火墙网络参数实现全网互通（20 分）

此处首先配置防火墙的基础网络参数，实现全网互通，用作与添加安全策略后通信进行对比。主要操作包括：

- (1) 配置防火墙接口；
- (2) 配置防火墙安全区域；
- (3) 配置防火墙路由信息（OSPF）
- (4) 测试全网通信

具体操作参考二维码 8-3 或教材项目十一任务二。

6、配置防火墙安全策略实现访问控制（30 分）

依据本实验指导书中“七、实验任务及要求”——“任务 3：设计防火墙安全策略”里所设计的安全策略，在防火墙上配置安全策略，然后测试相关通信效果。

具体操作参考二维码 8-3 或教材项目十一任务二。

九、实验考核（即形成性考核中的“实验实训”考核项目）

1. 学生在实验课上，当堂提交实验操作结果，并由教师现场检查完成情况；
2. 教师依据每个步骤的完成情况打分。

