实验八：防火墙实现访问控制

一、实验简介

在园区网中部署服务器子网，在用户区域网络和服务器子网之间部署防火墙（FW-1），通过设置防火墙安全策略，控制用户区域网络中的主机对服务器子网的访问，例如控制某用户主机网段只能访问 Web 服务器提供的 http 服务，而不能访问其他服务。

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、掌握利用防火墙实现园区网通信的访问控制。

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：

R1、R2 及其下联网络是用户区域网络（即用户子网），RS-1～RS-4 是用户区域网络中的路由交换机，起汇聚作用。SW-1～SW-4 是二层交换机，起接入作用。Host-1～Host-8 是用户主机，分别属于不同的 VLAN；

SW-5 连接的网络是服务器子网，其中 Service-DNS 表示 DNS 服务器（eNSP 仿真），Service-Web 表示 Web 服务器（eNSP 仿真），Service-FTP 表示 FTP 服务器（eNSP 仿真）。服务器子网接入在路由交换机 RS-5 上；

用户区域网络和服务器子网之间部署防火墙 FW-1。

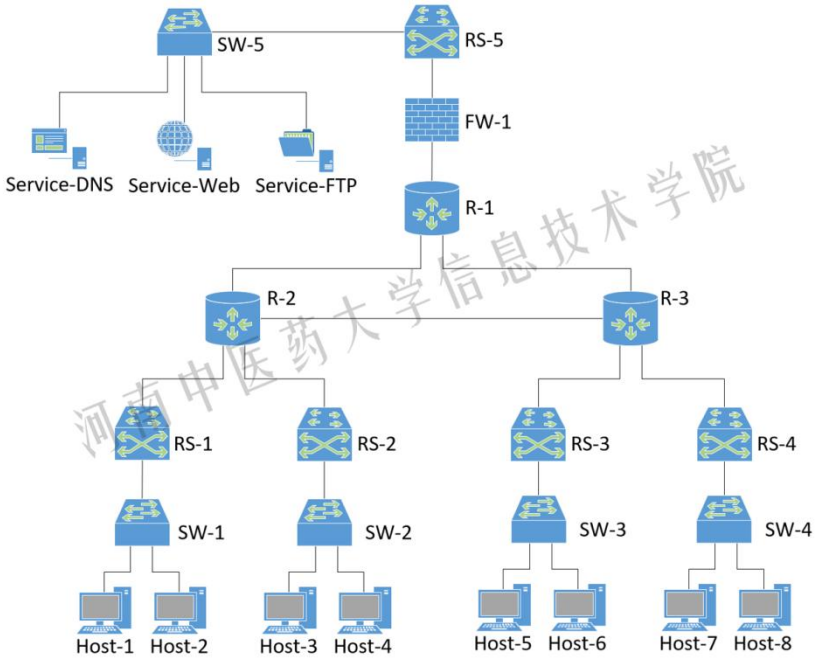

图 8-1 网络拓扑

七、实验步骤

1、设计全网 IP 地址

（1）所有用户主机的 IP 地址为静态 IP，其格式为 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；

（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）各个仿真服务器的 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、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，实现以下通信控制：

（1）Host-1～Host-4 主机不可以 Ping 通服务器子网中的服务器，Host-5～Host-8 可以；

（2）Host-1～Host-8 主机都可以使用 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；

3、在 eNSP 中部署园区网

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-plug-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。

注意：华为防火墙初始用户名和密码分别为 admin，Admin@123。

二维码 8-1 下载设备文件

二维码 8-2 防火墙基本配置

4、配置用户主机地址

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。

具体操作略。

5、配置网络设备

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。

6、配置仿真服务

（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

二维码 8-3 园区网中部署防火墙

（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。

7、配置防火墙网络参数实现全网互通

此处防火墙配置成路由模式。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。

8、配置防火墙安全策略实现访问控制

依据前面的规划，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。

八、思考与讨论

1. 本实验中，防火墙 FW-1 的安全区域是如何设置的？
2. 本实验中，防火墙的部署是路由模式还是透明模式？判断依据是什么？
3. 本实验中，防火墙 FW-1 是否配置了路由协议？配置了静态路由还是动态路由？具体是什么路由协议？
4. 假设本实验中，全网采用静态路由配置。则防火墙 FW-1 需要配置什么样的静态路由？
5. 本实验中，执行 Host-5 ping FTP 服务器，Host-5 发出的 ICMP 请求报文到达路由器 R-1 时，R-1 转发该报文的下一跳地址是什么？分析 R-1 的路由表，找到 R-1 转发该报文所依据的那条路由记录。
6. 针对题目中“*Host-1～Host-4 主机不可以 Ping 通服务器子网中的服务器*”的要求，你是如何配置防火墙策略的？谈谈具体配置。
7. 针对题目中“*Host-1～Host-8 主机都可以使用 DNS 解析服务*”的要求，你是如何配置防火墙策略的？谈谈具体配置。

8. 针对题目中“*仅允许 Host-1-Host-4 主机可以以 Web 方式访问 Web 服务*”的要求，你是如何配置防火墙策略的？谈谈具体配置。
9. 假设拓扑中的防火墙 FW-1 被配置成透明模式，执行 Host-5 ping FTP 服务器，Host-5 发出的 ICMP 请求报文到达路由器 R-1 时，R-1 转发该报文的下一跳地址是什么？

九、实验考核（即形成性考核中的“实验实训”考核项目）

1. 学生在老师指定的时间内完成实验，并且当面提交老师检查，回答教师提出的问题。
2. 教师根据学生完成实验情况以及回答问题情况，给本次实验打分。