实验十：防火墙实现用户上网认证

一、实验简介

本实验在实验九的基础上，增加园区网用户主机的上网认证。认证功能基于防火墙 FW-1 配置，采用本地认证方式。园区网内部的用户主机必须通过防火墙认证，才能访问园区网资源（例如服务器网段或互联网）），否则无法访问。

二、实验目的

1、掌握基于华为防火墙进行上网认证的方法；

三、实验学时

2 学时

四、实验类型

综合型

五、实验拓扑

本实验的网络拓扑如图 10-1 所示。其中“Internet” 代表互联网

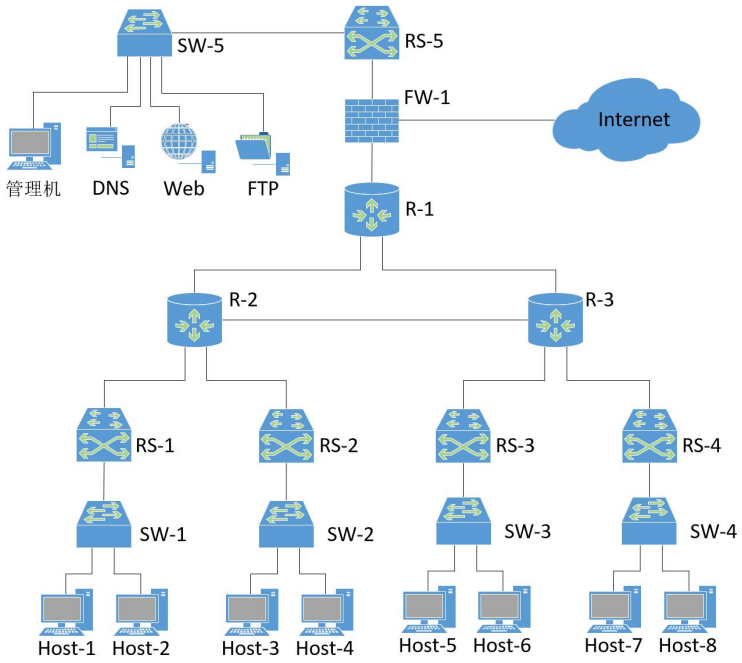

图 10-1 网络拓扑

六、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

七、实验步骤

【提醒】本实验各步骤具体操作，由学生自主查阅相关资料完成，或见本课程参考书《网络运维管理从基础到实战》项目九任务一。

步骤 01：设置本地实体机为管理机并能够 Web 登录 FW-1

本实验以 Web 方式配置防火墙 FW-1，为了模拟实际工作环境，在数据中心区域（即服务器区域）的交换机上接入一台管理机。该管理机将以 web 方式登录 FW-1 并进行相关配置，所以该管理机需要具备浏览器。由于 eNSP 中的仿真 PC 不具有浏览器功能，所以此处的管理机可用一台虚拟机（例如 Widows 虚拟机）代替，或者直接用本地实体主机（即学生的笔记本电脑）来代替。

为了简化操作，建议此处使用实体主机（即学生的笔记本电脑）来模拟管理机的操作。注意，管理机与 FW-1 之间要路由可达。

【提醒】本地实体主机在接入 eNSP 中时，为了能够访问 FW-1，可能需要在笔记本电脑上的命令提示符界面中，以管理员身份添加本机路由（使用 route add 命令）。

步骤 02：设置防火墙（FW-1）的 Web 方式登录

本实验中，通过管理机以 Web 方式登录防火墙并进行认证配置。所以，首先要对防火墙自身进行配置，使其允许 Web 登录，主要包括给防火墙配置管理 IP、使能 http（https）服务、添加 Web 登录的用户和密码等。

【注意】管理机以 Web 方式登录防火墙时，所需要的用户名和密码可由管理员自行设置，并自己记住，不要忘记

步骤 03：设置防火墙 FW-1 的认证方式并添加认证用户

（1）管理机 Web 登录防火墙 FW-1

在本地实体主机（即学生的笔记本电脑）的浏览器中，输入防火墙 FW-1 的管理 IP 地址，即可看到防火墙的 Web 登录界面。输入前面所创建的管理员用户名和密码，登录防火墙。

（2）设置认证方式

将 FW-1 的认证方式设置为“本地认证”

（2）添加用户组和认证用户

【要求】此处设置用户在防火墙处进行认证时，所需要用到的用户名和密码。为了以示区别，此处的用户名必须是学生本人的学号，登录密码由学生自定。

本实验提交检查时，将检查本要求。

注意：此处创建的用户名是供上网用户进行身份认证时使用的。步骤 02 中创建的用户是供管理员以 Web 方式登录防火墙使用的，两者不要搞混了！

步骤 04：在防火墙 FW-1 上添加认证策略

在防火墙 FW-1 上添加新的认证策略，使得指定的用户主机的通信在到达防火墙 FW-1 时，必须满足该认证策略的要求，才能登录防火墙 FW-1，进而执行后续操作。

【要求】新的认证策略中，采用对报文的来源 IP 地址进行认证，学生指定的网段内的主机发出的报文，经过 FW-1 时，需要进行认证。

注意：本实验提交检查时，将检查本要求。

完成认证有关的配置后，需要点击防火墙窗口上方导航栏右侧的【保存】按钮，保存相关配置。

步骤 05：在防火墙 FW-1 的下连接口上配置 Web 登录服务

由于园区网用户主机要通过 FW-1 的下连接口以 Web 方式登录防火墙的认证界面，所以此处需要配置该接口允许 Web 服务，参考命令如下。

```
[FW-1]interface GigabitEthernet 1/0/0
[FW-1-GigabitEthernet1/0/0]service-manage http permit
[FW-1-GigabitEthernet1/0/0]service-manage https permit
[FW-1-GigabitEthernet1/0/0]quit
```

步骤 06：设置本地实体机为园区网用户主机并接入 eNSP

由于园区网用户主机在进行认证时，需要通过浏览器以 Web 方式登录防火墙的认证界面，并且输入用户名和密码，eNSP 中的仿真终端没有浏览器，无法实现这一功能。所以此

处直接将本地实体机通过虚拟网卡接入 eNSP 中的用户区域网络，然后利用浏览器 Web 登录 FW-1，从而进行认证操作。

【提醒】本地实体主机在接入 eNSP 中时，为了能够访问 FW-1，可能需要在笔记本电脑上的命令提示符界面中，以管理员身份添加本机路由（使用 route add 命令）。本步骤添加的路由与步骤 01 中添加的路由不要冲突。

步骤 07：认证测试

在本地实体主机的浏览器中输入防火墙 FW-1 的认证地址 https://10.0.1.1:8887（10.0.1.1 是防火墙下连接口的 IP 地址，8887 是华为防火墙的认证端口），可以看到防火墙的认证界面，输入在不在 03 中设置的认证用户名和密码，并点击“登录”按钮，可以看到登录成功界面，表示认证成功。

测试认证成功前后，用户主机访问服务器的情况。

八、思考与讨论

1. 本地认证和服务器认证有什么区别？
2. 在本实验对应的教学课件中，讲到本地认证的四个组成部分：用户、接入设备、Portal 服务器、认证服务器，结合本实验内容，谈谈这四个部分分别在哪里？各起着什么作用？
3. 本实验中，分别在步骤 03 和步骤 07，以 Web 方式登录防火墙，结合实验内容结果，谈谈这两次登录防火墙有什么不同之处？
4. 自行设计实验操作，验证一下 FTP、HTTP、DHCP、DNS 的报文流量，是否受认证的限制，例如，假设 Host5 是 DHCP 客户端，是否必须认证通过后，其发出的 DHCP 报文，才能通过防火墙？

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。