实验七：通过防火墙实现用户上网认证

一、实验简介

在前一个实验的基础上，以 Web 方式登录用户区域的边界防火墙 A-FW-1，在防火墙上开启本地认证功能。当用户区域 A 的用户访问网络资源时，若该访问需要通过防火墙（例如访问数据中心的 Web 服务器），则必须先在防火墙上进行认证，通过认证以后，才能进行后续访问。实现对用户上网行为的管理。

二、实验目的

1、掌握防火墙的本地认证配置；
2、实现对用户上网行为的管理。

三、实验类型

验证性

四、实验理论

1. 用户

用户指的是访问网络资源的主体，表示“谁”在进行访问，是网络访问行为的重要标识。在防火墙上，用户包括上网用户和接入用户。

（1）上网用户

内部网络中访问网络资源的主体。上网用户可以直接通过防火墙访问网络资源。

（2）接入用户

外部网络中访问网络资源的主体。接入用户需要先通过 SSL VPN、L2TP VPN 或 IPSec VPN 方式接入到防火墙，然后才能访问内部的网络资源。

2. 认证

防火墙通过认证来验证访问者的身份、确保身份合法有效。防火墙访问者进行认证的方式包括：本地认证、服务器认证、单点登录。

本地认证：接入用户将标识其身份的用户名和密码发送给防火墙，在防火墙上上存储了用户名和密码，验证过程在防火墙上进行。

服务器认证：接入用户将标识其身份的用户名和密码发送给防火墙，防火墙上没有存储用户名和密码，防火墙将用户名和密码发送至第三方认证服务器，验证过程在认证服务器上进行。

单点登录：访问者将标识其身份的用户名和密码发送给第三方认证服务器，认证通过后，第三方认证服务器将访问者的身份信息发送给防火墙，防火墙只记录访问者的身份信息不参与认证过程。

五、实验内容及打分

本实验共包含 4 个任务，由学生独立完成。教师在实验课上检查实验完成情况并提出相应问题，将根据各任务的完成情况及回答问题情况进行打分。

【提示】各任务的具体操作，可参考教材或课程网站

任务一：设置管理机以 Web 方式登录防火墙 A-FW-1（10 分）

本实验中，通过部署在数据中心区域的管理机（即本地实体主机，虚拟网卡地址 10.0.255.253/30）以 Web 方式登录防火墙 A-FW-1，然后进行认证配置。

自行查阅相关资料，配置防火墙的 Web 登录。

【提示】
在防火墙 A-FW-1 上配置防火墙管理 IP，并实现 A-FW-1 与管理机之间网络可达。
配置管理机访问防火墙时所通过的接口，使允许 http 和 https 操作；

【要求 1】
管理机以 Web 方式登录防火墙时，用户名必须是学生本人的姓名全拼+01，例如张三，则其用户名为 zhangsan01。 登录密码统一设置为 abcd@1234；
注意：本实验提交检查时，将检查本要求。

任务二：设置防火墙 A-FW-1 的认证方式并添加认证用户（20 分）

在本地实体主机的浏览器中，输入防火墙 A-FW-1 的管理 IP 地址，即可看到防火墙的 Web 登录界面。输入前面所创建的用户名和密码，登录防火墙。

（1）设置认证方式

【要求 2】
将认证方式设置为“本地认证”
注意：本实验提交检查时，将检查本要求。

（2）添加用户组和认证用户

【要求 3】
需要登录认证的用户名必须是学生本人的姓名全拼+02，例如张三，则其认证用户名为 zhangsan02。 登录密码统一设置为 abcd@1234；
注意：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 1 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！

任务三：在防火墙 A-FW-1 上添加认证策略（20 分）

在防火墙 A-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 A-FW-1 时，必须满足该认证策略的要求，才能登录防火墙 A-FW-1，进而执行后续操作。

【要求 4】
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 A-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。

任务四：防火墙 A-FW-1 开启认证后进行通信测试（20 分）

此时，防火墙 A-FW-1 开启认证（仅认证用户主机发出的报文），B-FW-1 未开启认证，分别从用户 A 区域和 B 区域访问数据中心进行通信测试。

【要求 5】

验证此时不同网段内的用户主机访问数据中心区域网络的情况，体会本地认证的作用和效果。

注意：本实验提交检查时，将检查本要求。

提示：

1. 由于用户区域主机在进行认证时，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。所以此处可将本地实体主机接入 eNSP 网络，进行验证。
2. 进行通信测试时，要留意园区网中各防火墙上原有的安全策略，例如数据中心的旁挂防火墙上是否配置了禁止外部网络主机 ping 数据中心的服务器；为了方便测试认证效果，也可以将所有防火墙的安全策略都设置成允许所有报文通过。

5、回答问题（30 分）

教师在实验课上检查实验完成情况并提出相应问题，将根据各任务的完成情况及回答问题情况进行打分。