实验十一：通过 Radius 实现统一认证

一、实验简介

除了通过防火墙实现本地认证外，还可以针对入网用户进行统一认证。即在园区网中部署 RADIUS 认证服务器，所有上网用户的具体认证工作可全部从防火墙转发至 RADIUS 服务器中完成，这种认证方式也称为全网统一认证。

本实验在上一实验的基础上，VirtualBox 中创建 RADIUS 服务器并接入数据中心网络，将用户区域 B 的防火墙认证方式设置成服务器认证。防火墙 B-FW-1 收到认证请求后，会将认证请求转发至 RADIUS 服务器，并在 RADIUS 服务器中完成认证。

二、实验目的

1、实现 RADIUS 服务器的创建、认证配置与部署；

2、实现基于 RADIUS 服务器的全网统一认证。

三、实验类型

综合性

四、实验理论

1. RADIUS 简介

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统），协议定义了基于 UDP 的 RADIUS 报文格式及其传输机制，并规定 UDP 端口 1812、1813 分别作为认证、计费端口。

RADIUS 服务器通常需要维护三个数据库 Users、Clients、Dictionary。Users：用于存储用户信息，如用户名、口令以及使用的协议、IP 地址等配置信息；Clients：用于存储 RADIUS 客户端的信息，如接入设备的共享密钥、IP 地址等；Dictionary：用于存储 RADIUS 协议中的属性和属性值含义的信息。

RADIUS 协议最初由 Livingston 公司提出，目的是为拨号用户进行认证和计费。后来经过多次改进，形成了一项通用的认证计费协议。

2 RADIUS 报文结构

RADIUS 协议采用 UDP 报文来传输消息，RADIUS 报文结构如图 11-1 所示。

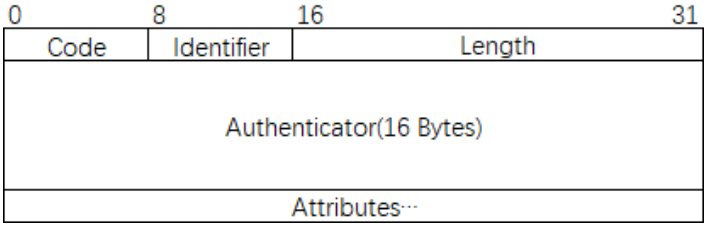

图 11-1 RADIUS 报文结构

RADIUS 各字段解释，如表 11-1 所示。

表 11-1 RADIUS 报文各字段含义

报文字段	报文说明
Code	长度为 1 个字节，说明 RADIUS 报文类型。
Identifier	长度为 1 个字节，用来匹配请求报文和响应报文。
Length	长度为 2 个字节，用来指定 RADIUS 报文的长度。
Authenticator	长度为 16 个字节，用来验证客户端与 RADIUS 服务器的消息
Attribute	不定长度，报文的内容主体，用来携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节。

3. RADIUS 认证报文

常见的 RADIUS 报文包括认证报文、计费报文、授权报文。其中认证报文详情如表 11-2 所示。

表 11-2 RADIUS 认证报文

报文名称	报文说明
Access-Request	认证请求报文，是 RADIUS 报文交互过程中的第一个报文，携带用户的认证信息（例如：用户名、密码等）。认证请求报文由 RADIUS 客户端发送给 RADIUS 服务器，RADIUS 服务器根据该报文中携带的认证信息判断是否允许接入。
Access-Accept	认证接受报文，是服务器对客户端发送的 Access-Request 报文的响应报文。如果 Access-Request 报文认证通过，则发送该类型报文。客户端收到此报文后，认证用户才能认证通过并被赋予相应的权限。
Access-Reject	认证拒绝报文，是服务器对客户端的 Access-Request 报文的拒绝响应报文。如果 Access-Request 报文即认证失败，则 RADIUS 服务器返回 Access-Reject 报文，用户认证失败。
Access-Challenge	认证挑战报文。EAP 认证时，RADIUS 服务器接收到 Access-Request 报文中携带的用户名信息后，会随机生成一个 MD5 挑战字，同时将此挑战字通过 Access-Challenge 报文发送给客户端。客户端使用该挑战字对用户密码进行加密处理后，将新的用户密码信息通过 Access-Request 报文发送给 RADIUS 服务器。RADIUS 服务器将收到的已加密的密码信息和本地经过加密运算后的密码信息进行对比，如果相同，则该用户为合法用户。

4. RADIUS 交互过程

RADIUS 认证过程包括用户、RADIUS 客户端和 RADIUS 服务器三者的交互过程，如图 11-2 所示。

图 11-2 RADIUS 工作交互流程

五、实验内容及打分

本实验共包含 3 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：创建并部署 RADIUS 服务器（30 分）

在 VirtualBox 中创建一台安装 CentOS 操作系统的虚拟机，并将其命名为 RADIUS。由于接下来要在线安装 FreeRADIUS 等软件，所以虚拟机创建好以后，暂不接入 eNSP 的仿真网络，其网卡连接方式保持默认设置“网络地址转换（NAT）”。

在线安装 FreeRADIUS，并对 RADIUS 服务器进行配置。配置完成后，将 RADIUS 服务器接入到 eNSP 中的园区网数据中心区域。

【要求 1】

1) 配置 RADIUS 服务器接收来自防火墙 B-FW-1 发来的认证请求；
2) 配置添加两个用户信息，用户名分别是学生本人的姓名全拼+01、本人的姓名全拼+02，例如有学生张三，则此处配置用户名为 zhangsan01 和 zhangsan02。 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：登录防火墙并配置（20 分）

以 Web 方式登录用户区域防火墙 B-FW-1（此处具体登录相关配置略），并进行认证相关配置。

主要包括

（1）在防火墙 B-FW-1 中添加 RADIUS 服务器信息

（2）设置防火墙 B-FW-1 的认证方式并添加认证用户

（3）在防火墙 B-FW-1 上添加认证策略

【要求 2】

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

任务三：防火墙 B-FW-1 开启认证后进行通信测试（20 分）

结合上一实验，此时，防火墙 A-FW-1 应开启了本地认证（仅认证用户主机发出的报文），B-FW-1 开启了服务器认证，分别从用户 A 区域和 B 区域访问数据中心进行通信测试。

验证此时用户区域中，不同网段内的用户主机访问数据中心区域网络的情况，体会本地认证和 RADIUS 统一认证的特点和不同。

【要求 3】

抓包验证本地认证和 RADIUS 统一认证的区别

抓包验证 RADIUS 统一认证过程中，防火墙 B-FW-1 和认证服务器之间的通信。

注意：本实验提交检查时，将检查本要求。

4、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。