实验四：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

综合型

四、实验拓扑设计

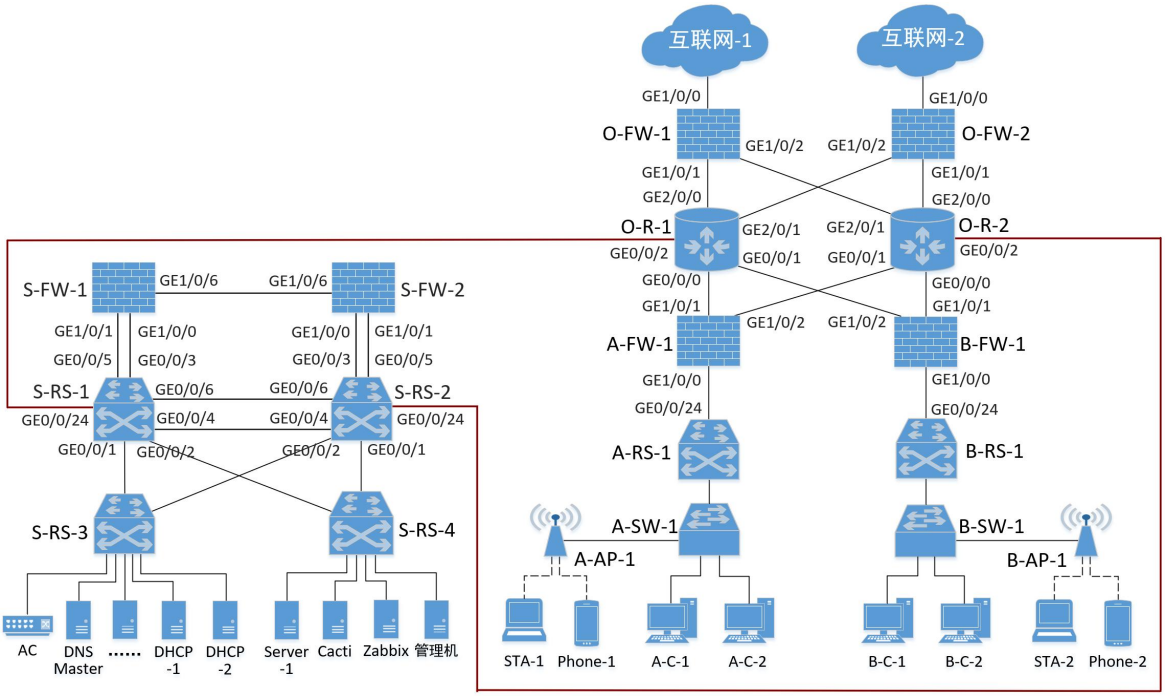

图 1 加入防火墙后的拓扑设计

本实验在前面实验 3 的基础上，在网络中增加防火墙以提升网络安全，并且通过防火墙进行认证，使用拓扑见图 1 所示。

1、实验拓扑说明

（1）在园区网边界的接入网络中增加两台防火墙，通过配置双链路 NAT 及配置安全策略，实现出口访问控制与设备灾备，当外部网络需要访问内部网络资源时将受到控制，例如必须以 VPN 方式进行访问。

（2）数据中心的边界区域增加两台防火墙，旁挂部署，进出数据中心网络的流量必须先引流到防火墙，经过防火墙安全策略过滤后，再进一步转发。

（3）为了实现数据中心防火墙的设备灾备，将两台防火墙设置为双机热备，当一台出现故障时，可通过另一台进行工作。此外，两台防火墙的工作方式为负载分担，即正常情况两台防火墙分担通信流量，若一台出现故障，则另一台承担全部流量。

（4）每个用户区域通过一台防火墙连接到核心路由器，控制园区网用户对网络资源的访问。

2、防火墙安全策略设计

2.1 用户区域边界防火墙的安全策略

自行设置用户区域边界防火墙的安全域和安全策略，并根据自行设置的安全策略填写表 1

2.2 数据中心区域防火墙的安全策略

表 1 用户区域边界防火墙安全策略

序号	策略名称	来源	目的地	协议	动作	策略含义
…	……					

设计要求：

1. 此处所设置的安全策略，必须和教材中“【项目八】-【任务三】-【安全策略设计】-1、用户区域边界防火墙的安全策略”中的策略**不一样**！
2. 实验考核时，需向教师汇报本表的内容。

自行设置用户区域边界防火墙的安全域和安全策略，并根据自行设置的安全策略填写表 2

表 2 数据中心区域边界防火墙安全策略

序号	策略名称	来源	目的地	协议	动作	策略含义
…	……					

设计要求：

1. 此处所设置的安全策略，必须和教材中“【项目八】-【任务三】-【安全策略设计】-2、**数据中心区域**防火墙的安全策略”中的策略**不一样**！
2. 实验考核时，需向教师汇报本表的内容。

2.3 园区网边界防火墙的安全策略

自行设置用户区域边界防火墙的安全域和安全策略，并根据自行设置的安全策略填写表 3

表 3 园区网边界防火墙的安全策略

序号	策略名称	来源	目的地	协议	动作	策略含义
…	……					

设计要求：

1. 此处所设置的安全策略，必须和教材中“【项目八】-【任务三】-【安全策略设计】-3、园区网边界防火墙的安全策略”中的策略**不一样**！
2. 实验考核时，需向教师汇报本表的内容。

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。

任务一：实现园区网通信（含防火墙部署）（30 分）

【任务说明】根据图 1 所示的网络拓扑，完成园区网的部署以及防火墙安全策略的实现。

【提示】本任务的具体操作，可参考教材项目八或课程网站

具体步骤如下：

步骤 01：实现用户区域边界防火墙的部署及访问控制

根据图 1 网络拓扑规划及防火墙安全策略说明，实现用户区域防火墙 A-FW-1 和 B-FW-1 的部署及通信控制。

步骤 02：实现数据中心区域防火墙的部署及访问控制

根据图 1 网络拓扑规划及防火墙安全策略说明，实现用户区域防火墙 S-FW-1 和 S-FW-1 的部署及通信控制

步骤 03：实现园区网边界防火墙的部署及访问控制

根据图 1 网络拓扑规划及防火墙安全策略说明，实现用户区域防火墙 O-FW-1 和 O-FW-1 的部署及通信控制

步骤 04：测试防火墙策略效果

自行设计操作，验证防火墙策略的实施效果。

任务二：在防火墙 A-FW-1 上实现本地认证（20 分）

【任务说明】在任务一的基础上，在防火墙 A-FW-1 防火墙上配置本地认证，使得用户区域 A 中的用户主机（例如 A-C-1），必须在防火墙 A-FW-1 处经过认证，才能访问网络（例如访问数据中心或互联网）。也就是说，A-C-1 必须经过防火墙认证，所发出的报文才能通过防火墙 A-FW-1。

【提示】本任务的具体操作，可参考教材项目九的任务一或课程网站相关视频

步骤 01：设置防火墙（A-FW-1）的 Web 方式登录

本任务中，计划通过管理机，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）、添加登录的用户名和密码等。自行查阅相关资料，配置防火墙的 Web 登录。

此处的管理机部署在数据中心区域，可用本地实体主机代替。注意，管理机与 A-FW-1 之间要路由可达。

【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 02：设置防火墙 A-FW-1 的认证方式并添加认证用户

（1）管理机 Web 登录防火墙 A-FW-1

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。输入前面所创建的管理员用户名和密码，登录防火墙。

（2）设置认证方式

将 A-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姓名全拼，例如张三，则其认证用户名为 zhangsan。 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 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！

步骤 03：在防火墙 A-FW-1 上添加认证策略

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】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。

步骤 04：防火墙 A-FW-1 开启认证后进行通信测试

此时，防火墙 A-FW-1 开启了本地认证，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，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。

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。

任务三：在防火墙 B-FW-1 上实现 Radius 服务器统一认证（20 分）

【任务说明】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。

本任务在上一任务的基础上，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（B-FW-1）的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。

【提示】本任务的具体操作，可参考教材项目九的任务二或课程网站相关视频

步骤 01：创建并部署 RADIUS 服务器

主要内容包括：

（1）创建 RADIUS 虚拟机

（2）在线安装 FreeRADIUS

（2）在 Radius 服务器中增加 B-FW-1 客户端

指明 RADIUS 服务器能够接收哪些客户端（即防火墙）发来的认证请求

（3）添加认证用户信息

由于各个防火墙收到认证请求以后，会将认证请求转发至 RADIUS 服务器，因此需要在 RADIUS 服务器中添加所有上网用户的认证信息（用户名和密码），从而形成集中的用户管理，最终实现全网统一认证。

【要求】 为了汇报检查时以示区别，此处要求添加两个用户信息，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；

（4）部署 RADIUS 服务器

将配置好的 RADIUS 服务器部署到 eNSP 中的园区网，使得 Radius 服务器防火墙 B-FW-1 之间路由可达。

步骤 02：登录防火墙 B-FW-1 并进行配置

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

步骤 03：防火墙 B-FW-1 开启认证后进行通信测试

结合任务二的本地认证，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。

六、实验考核

实验考核从【完成维度】和【时间维度】两个维度进行评分。

1、【完成维度】考核

本维度主要考核学生完成实验的程度以及对实验内容的理解程度，包括【任务完成度】和【回答问题】两个部分。具体如下：

（1）任务完成度（70 分）

学生在完成实验后，要当面提交教师检查实验结果。教师检查每个实验任务的完成情况，并根据实验指导书中每个任务的分值，给出任务完成度的分数。本项目满分 70 分。

（2）回答问题（30 分）

学生在完成实验后，要当面提交教师检查实验结果，并回答教师提问。教师根据学生回答情况评分。本项目满分 30 分。

【注意】：教师提问时，可参考“七、思考与讨论”中的问题，从中随机选取 2-3 个问题进行提问。

2、【时间维度】考核

本维度主要考核学生完成实验的时间，具体如下：

（1）当堂提交（100 分起评）

本实验的实验课当堂提交并通过【完成维度】考核的，从 100 分起评。

（2）一周内提交（90 分起评）

本实验的实验课结束一周内提交并通过【完成维度】考核的，从 90 分起评，即本次实验考核最高 90 分。

（3）一周后提交（80 分起评）

本实验的实验课结束一周后提交并通过【完成维度】考核的，从 80 分起评，即本次实验考核最高 80 分。

（4）未提交（0 分）

本学期教学工作结束时，仍未提交的，本次实验考核 0 分。

七、思考与讨论

学生在做实验时，要结合实验内容和过程，讨论分析以下问题，以备教师提问

1. 根据自己在【四、实验拓扑设计】-【2、防火墙安全策略设计】中的设计，结合表 1、表 2、表 3 内容，向老师汇报自己在各区域防火墙上所配置的安全策略内容。

2. 什么是防火墙安全域？基础的安全域有哪些？这些安全域的安全级别的值分别是多少？根据自己的实际配置，谈谈本实验中各防火墙的安全域是如何设计的？例如防火墙 A-FW-1 中，定义哪些安全域？这些安全域分别表示什么区域？每个安全域包含哪些防火墙接口？

3. 结合本实验和实验一的实际操作，对比分析防火墙上配置 NAT 和路由器上配置 NAT 的异同点。（注意，不要从网上随便复制背诵）

4. 以用户区域边界防火墙 A-FW-1 为例，自主设计实验并验证：

   （1）华为防火墙在默认配置下，是允许报文通过，还是不允许通过？

   （2）当防火墙只配置了接口 IP，并启用 OSPF，但没有配置安全策略，其他保持默认配置，此时是允许报文通过，还是不允许通过？

   （3）当防火墙只配置了接口 IP，并启用 OSPF，其他保持默认配置下，当从用户主机 ping 防火墙的接口时（假设此时用户主机到防火墙之间路由可达），此时是能 ping 通，还是不能？说明原因。

5. 数据中心区域的防火墙采用旁挂部署方式，如果此处 S-RS-1 不采用 VRF 配置方式，而是在 S-RS-1 和 S-FW-1 之间配置静态路由，能否实现数据包的引流（即到达 S-RS-1 的数据包会先被引流到 S-RS-1，然后再被发回 S-RS-1，然后再继续传输）？举例具体分析。

6. 数据中心区域的防火墙采用旁挂部署方式，为了旁挂引流，S-RS-1 采用 VRF 配置方式。VRF 是什么意思？结合实际操作，举例说明 VRF 的工作原理。

7. 数据中心区域的防火墙采用旁挂部署方式，并且实现双机热备。结合实际配置，举例分析此处防火墙实现双机热备的原理。

8. 数据中心区域的防火墙采用旁挂部署方式，并且在实现双机热备时，使用了 VRRP 技术。问：什么是 VRRP？其工作原理是什么？试举例说明本实验任务一中对 VRRP 的应用。

9. 结合任务二和任务三的实际操作，谈谈本地认证和 Radius 统一认证的区别，并举例说明。

10. 对本实验任务三 Radius 统一认证的实现过程进行总结，举例说明在园区网内实现 Radius 统一认证

所需要进行的操作。

11. 以抓包分析的方式，分别验证本实验中：

（1）A-FW-1 实现了本地认证而不是 Radius 服务器认证

（2）B-FW-1 实现了 Radius 服务器统一认证，而不是本地认证

12. 本实验任务二中，步骤 01 和步骤 02 中都在防火墙上设置了用户和密码。问：这两个步骤中所设置的用户和密码在作用上有什么不同？

13. 本实验任务二步骤 01 中，在通过管理机配置防火墙 A-FW-1 时，为什么用本地实体主机作为管理机？

14.