实验九：园区网中防火墙的综合部署

一、实验简介

在园区网的关键位置部署防火墙，实现全网通信的安全控制。

二、实验目的

1、实现园区网关键位置的安全防护。

三、实验类型

综合性

四、实验设计

1、园区网风险分析

园区网未加入安全设计时的网络拓扑，如图 9-1 所示。

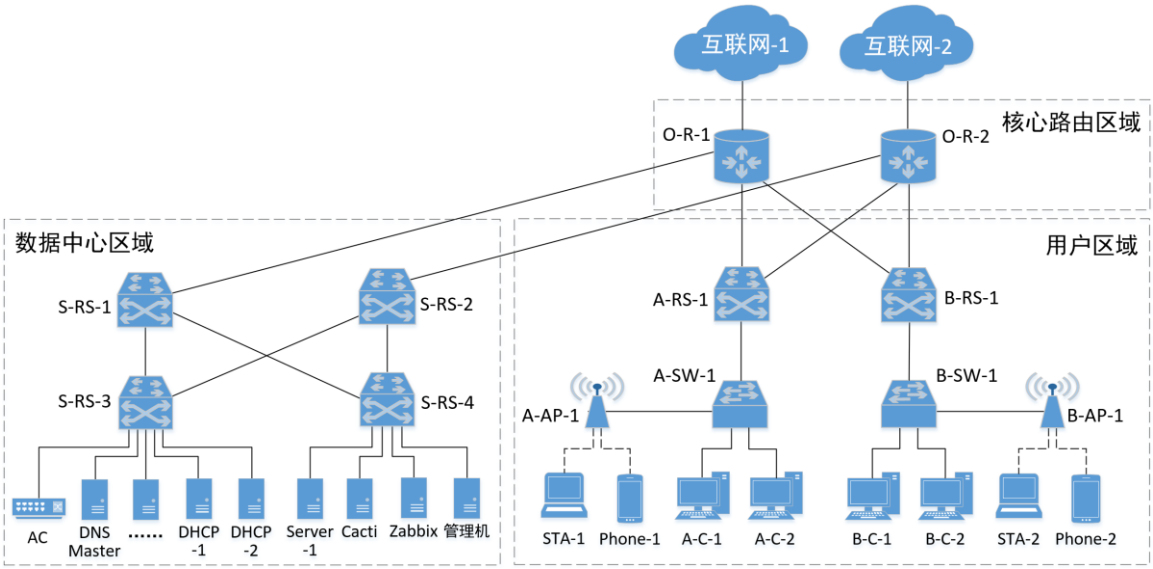

图 9-1 未加入安全设计的网络拓扑

对现有园区网网络安全现状进行分析，目前主要存在以下问题：

（1）园区网接入互联网区域无法实现边界网络的访问控制与安全防护，容易受到攻击；

（2）数据中心区域与核心网络之间缺少安全防护，无法有效实现服务器的访问控制；

（3）用户区域网络缺少访问控制措施，无法对网络用户行为以及访问内容进行控制；

2、设计安全方案

为了解决网络设计中的安全风险，在网络中增加防火墙以保证网络安全。

（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。

根据安全方案，添加防火墙以后的网拓扑结构如图 9-2 所示。

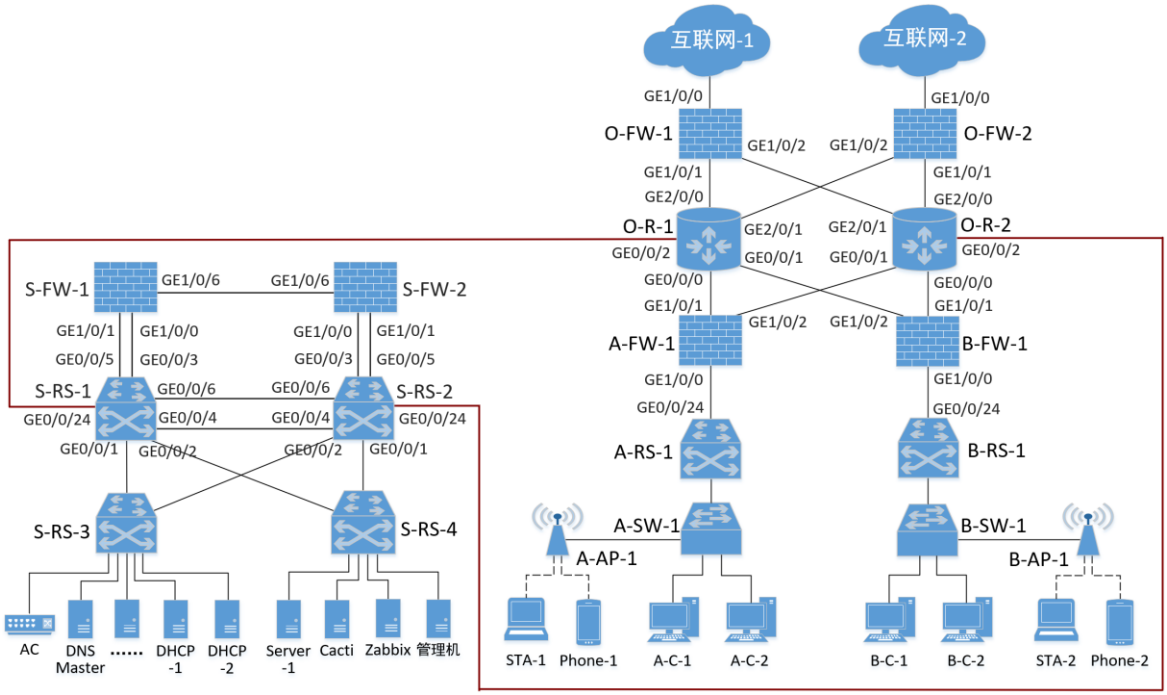

图 9-2 加入防火墙后的拓扑设计

3、安全策略设计

3.1 用户区域边界防火墙的安全策略

（1）数据中心的管理机，可以通过 SNMP 服务采集园区网内各网络设备的数据，可以通过 SSH 方式远程管理园区网的网络设备；

（2）从用户区域向外部网络（即用户区域之外的区域）的主动通信被允许；

（3）注意 AP 和 AC 之间的通信被允许。

（4）其他通信均禁止。

3.2 数据中心区域防火墙的安全策略

（1）允许园区网中的用户区域主机访问数据中心提供的 Web 服务（可用仿真代替）、DNS 服务、DHCP 服务和 NTP 服务；

（2）不允许外部网络对数据中心区域内部服务器的 Ping 操作。

（3）从数据中心网络向外部网络的所有通信被允许；
（4）注意 AP 和 AC 之间的通信被允许；
（5）其他通信均禁止。

3.3 园区网边界防火墙的安全策略

（1）允许数据中心的服务器网段访问互联网；
（2）允许用户区域 A 的主机访问互联网；
（3）其他通信均禁止。

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

1、任务一：在 eNSP 中实现图 9-1 所示网络通信（10 分）

（1）根据图 9-1 网络拓扑规划，在 eNSP 中部署硬件设备；
（2）实现全网互通；

2、任务二：实现用户区域边界防火墙的部署及访问控制（20 分）

根据图 9-2 网络拓扑规划，实现用户区域防火墙 A-FW-1 和 B-FW-1 的部署及通信控制

3、任务三：实现数据中心区域防火墙的部署及访问控制（20 分）

根据图 9-2 网络拓扑规划，实现用户区域防火墙 S-FW-1 和 S-FW-1 的部署及通信控制

4、任务四：实现园区网边界防火墙的部署及访问控制（20 分）

根据图 9-2 网络拓扑规划，实现用户区域防火墙 O-FW-1 和 O-FW-1 的部署及通信控制

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

六、实验拓展及分析

学生可自行设计防火墙安全策略，并验证。