

实验五：防火墙旁挂部署

一、实验简介

根据实验拓扑部署网络，在数据中心区域的路由交换机 RS-2 一侧，旁挂一台防火墙（FW-2）。这种部署并不改变原有网络的拓扑结构，并且通过在 RS-2 和 FW-2 上配置静态路由，使得通过数据中心交换机（RS-2）的流量都会被首先引流到旁挂的防火墙（FW-2）上进行安全策略检测，而不是直接转发至核心路由器（R-1）或者 Server-1。只有安全策略允许通过的流量才会被防火墙发送回交换机 RS-2，并被 RS-2 进一步转发至目的地（即转发至 R-1 或 Server-1），从而保证数据中心网络安全。

二、实验目的

- 1、完成防火墙的旁路部署；
- 2、完成交换机 VRF（虚拟路由转发）配置，并实现防火墙旁路引流；
- 3、通过旁路防火墙的安全策略，实现对数据中心网络的安全防护。

三、实验理论

- 1、防火墙
- 2、VRF（虚拟路由转发）

四、实验规划



1、网络拓扑规划

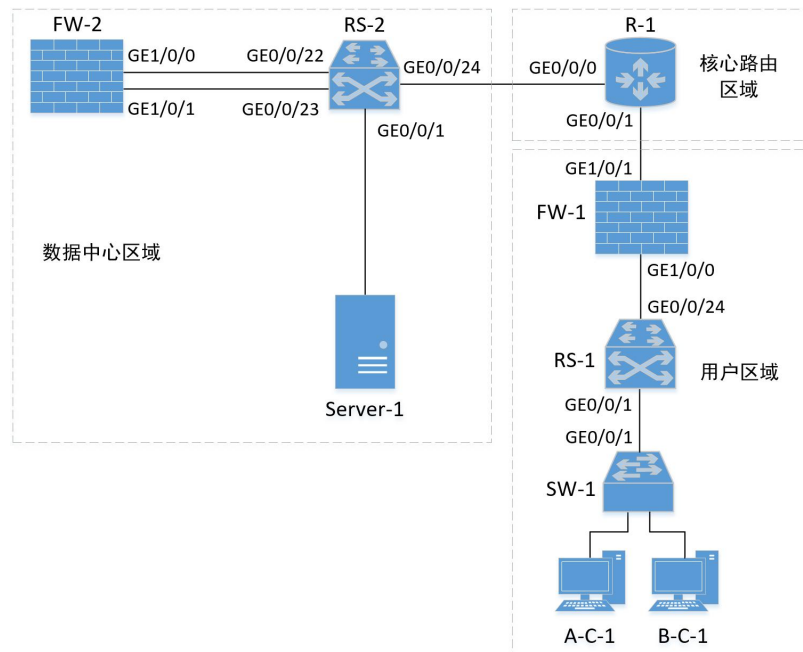


图 1 实验五的网络拓扑规划

2、交换机 VLAN 设计

学生自定

3、IP 地址设计

学生自定

4、路由设计

学生自定

5、防火墙安全策略

学生自定

五、实验内容及打分

教师根据各任务的完成情况与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、步骤一：在 eNSP 中部署网络（10 分）

根据网络拓扑规划，在 eNSP 中部署硬件设备：

2、步骤二：配置用户区域网络（10 分）

本任务中，用户区域网络中各设备（包括交换机 SW-1、三层交换机 RS-1 和防火墙 FW-1）的配置与任务一相同，用户可参考任务一进行相关配置。

3、步骤三：配置防火墙 FW-2（20 分）

包括更改防火墙登录密码、配置防火墙接口地址、将接口加入安全区域、配置静态路由、配置安全策略等。

4、步骤四：配置三层交换机 RS-2（20 分）

这是本实验的重点，包括配置 VRF、配置 VRF 相关接口、配置 OSPF 路由、配置静态路由等。

5、步骤五：配置路由器 R-1（10 分）

包括配置接口地址、配置目的网络是服务器网段的静态路由，实现报文可转发至 RS-2；配置 OSPF，并将静态路由引入到 OSPF，使得外部网络中的其他路由设备可以通过 OSPF 获取到该静态路由的信息，从而知道目的网络是服务器网段的报文该如何转发。

6、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

通过抓取报文，验证报文是否被引流到防火墙 FW-2。

