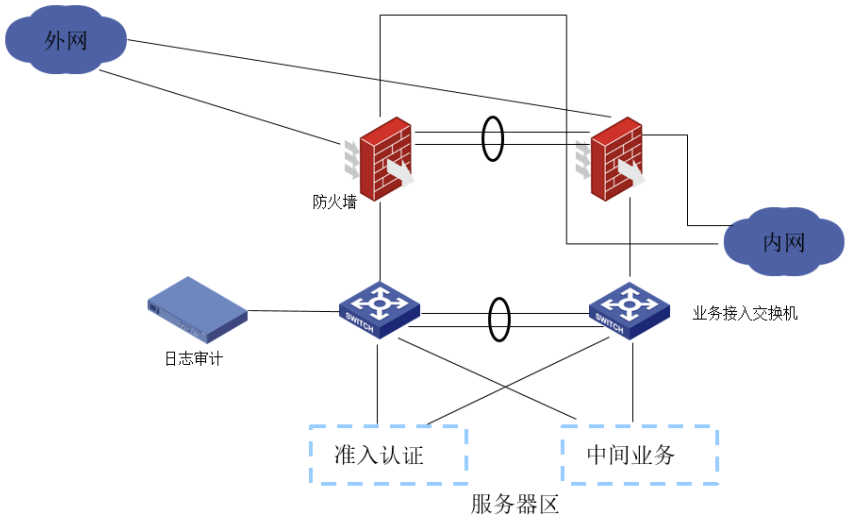
某局点F1090阻断代理服务器流量失败问题处理经验案例

数据过滤 特征库 **淡烟疏雨** 2022-02-28 发表

组网及说明

拓扑如下：



问题描述

要求是只对代理这个行为进行禁止，代理服务器上不止代理一个业务，还有其它应用，内网的用户需要访问这些

配置后发现阻断失败

过程分析

查看配置无误：

查看版本已知问题并未查询到该类说明

现场环境主要是http和socks，代理流量抓包分析

解决方法

http代理报文经分析，未被阻断的报文流量会识别成http代理和哔哩哔哩，按照优先级最终会识别成哔哩哔哩，能够通过修改特征库的方式解决http代理未识别问题，修改特征库预计3月10号上官网。可先用临时特征库。

Sock代理报文经分析，特征太弱，无法提取ac特征，建议使用自定义应用的方式进行识别。经分析回包，socks的端口都是10808。socks通过自定义应用，配置端口10808。