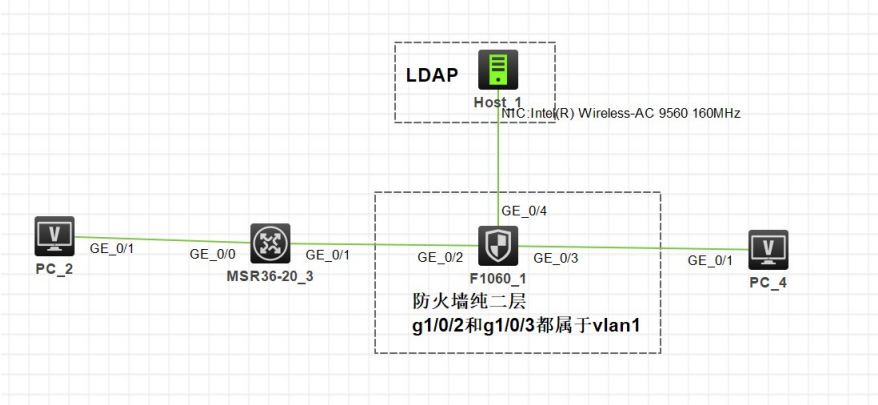
防火墙做portal认证结合ldap的案例

Portal认证 聂鹏 2021-10-15 发表

组网及说明

组网如下，防火墙纯二层，所有接口都属于vlan1



问题描述

防火墙纯二层，做portal结合ldap认证。发现认证后还是无法上网，用域名都无法触发PORTAL。

过程分析

抓包查看，发现回包被设备丢弃。//由于设备纯二层，无法debugging。
进一步分析发现，现场再vlaninterface1 下做的portal。
interface Vlan-interface1
 portal domain ldap
 portal apply web-server wxkwpt
现场在vlaninterface1上做的portal。会导致出去的流量设备认为是进入了vlaninterface1，而回来的流量也是进入了vlaninterface1 。
而portal没有会话关联来回流量，因此设备会要求外网的回包也做Portal，这个时候就会出现回程不通。

解决方法

配置免认证策略，将外网口的流量全都免认证。