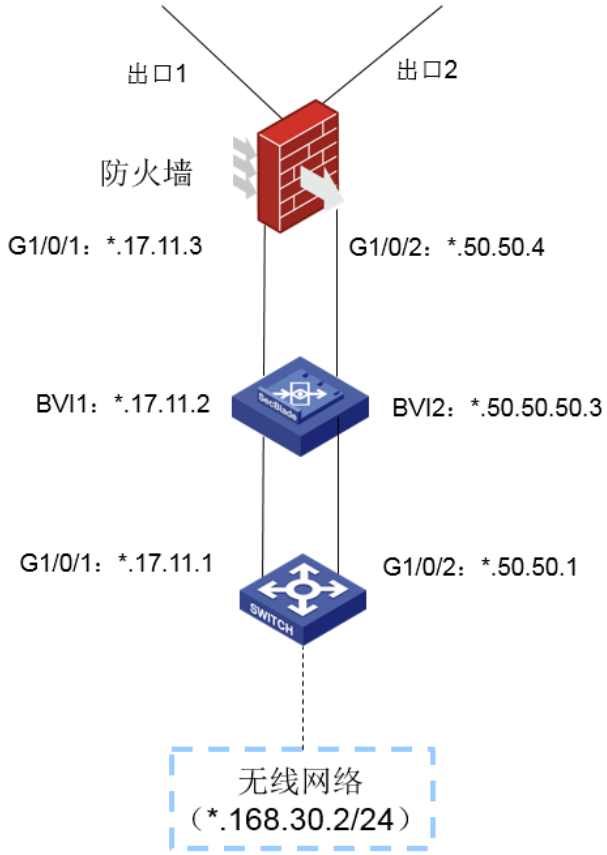
某局点ACG设备做短信认证，能重定向出认证页面URL，但是认证页面内容无法显示的处理经验案例

AAA Portal 徐猛 2021-06-06 发表

组网及说明

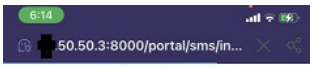
现场拓扑大致如下，组网说明：

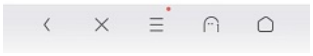
无线网络的网关在核心交换机上，核心交换机上行双链路到ACG，ACG双链路到防火墙，ACG在核心交换机和防火墙之间使能了两个透明网桥，进行透明部署。同时在交换机和防火墙上配置了主备路由，主走ACG的BVI1的网桥口。经过NQA探测如果异常，切换到BVI2口进行转发。



问题描述

现场需要对无线终端进行短信认证，在配置完短信认证后，发现终端能弹出认证页面，且能显示出重定向的页面URL信息，但是认证页面是空白的。





过程分析

一、首先对现场的配置进行了核查：

（1）短信认证基本配置：

（3）地址对象配置无误：

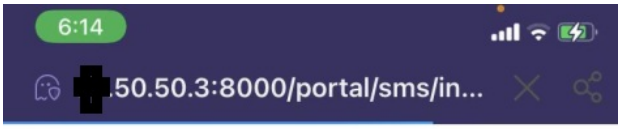
	名称	内容(网络，范围，主机)	排除地址	描述	引用	操作
1	any	0.0.0.0/0		任何地址	6	
2	private	10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,		私有地址	1	
3	ChinaUnicom	1.2.2.0/24,1.4.4.0/24,1.8.0.0/16,...		中国联通	0	
4	ChinaTelecom	1.0.1.0/24,1.0.2.0/23,1.0.8.0/21,...		中国电信	0	
5	ChinaEducation	1.51.0.0/20,1.51.16.0/20,1.51.32.0/19,...		教育网	0	
6	ChinaMobile	36.128.0.0/12,36.144.0.0/14,36.148.0.0/16,...		中国移动	0	
7	fuwuqi	192.168.50.248/29		服务器	0	
8	banggongshi	192.168.66.0/24		办公室	1	
9	zizhizhongduan	192.168.62.0/24		自助终端	1	
10	xibangong	192.168.63.0/24		西办公	1	
11	dongbangong	192.168.65.0/24		东办公	1	
12	wuxian	192.168.30.0/24		无线	2	

（5）网桥接口配置：

	接口名称	描述	包含接口	IP地址	IPv6地址	连接状态	启用状态	操作
1	bvi1		ge13, ge1	[redacted]17.1.2/29		up		
2	bvi2		ge2, ge4	[redacted]50.50.3/24		up		
3	bvi3		ge2.300, ge4.300			up		

经上述检查配置，发现配置无误。

二、由于重定向出的URL地址是*.50.50.3的地址。于是我们在终端上直接telnet该地址的80端口测试，发现不通：



保证ACG回包给终端的流量和终端访问外网时，经过ACG的流量，经过的接口和链路是同一组接口和链路即可。现场添加了一条静态路由，将回给终端192.168.30.0/24网段的路由，走BVI1口回给核心交换机后正常。

三、在ACG上执行debug看下报文丢弃原因

H3C> en

H3C# debug dp drop

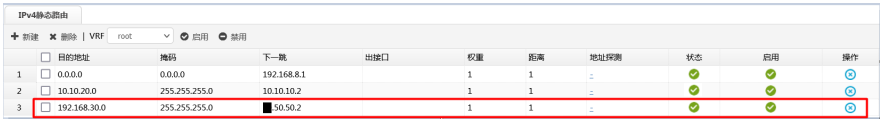
H3C# debug dp filter src-ip +源IP地址

H3C# dis log debug

发现会回显web-auth类型的web认证阻断记录。

由于重定向的URL的地址为*.50.50.3的地址，怀疑是否由于ACG的报文响应是从BVI2口响应回去的，从而后续终端再次发起的访问*.50.50.3的流量从BVI1口进来的时候认为未做认证而阻断丢弃了。

后续检查路由发现果然如此，存在一条去往私网业务段的路由，走BVI2口回包的：



现场添加了一条静态路由，将回给终端192.168.30.0/24网段的路由，走BVI1口回给核心交换机的*.17.11.1地址后正常。