

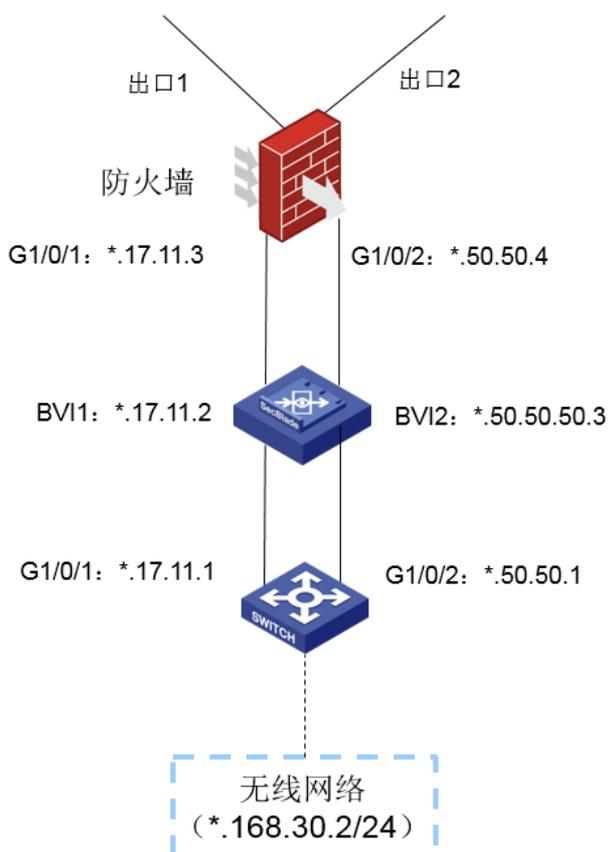
知 某局点ACG设备做短信认证，能重定向出认证页面URL，但是认证页面内容无法显示的处理经验案例

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：

短信认证配置

基础配置

启用

超时时间 120 (10-144000分钟)

无感知 (10-144000分钟)

页面跳转设置 之前访问的页面 重定向URL 认证结果页面

接口参数配置 建议配置DNS服务器，用于访问网关地址

厂商 一信通

短信内容前缀 衡水税务 (如：淘宝)

网关地址 https://api.ums86.com:9600 (请联系短信商销售人员获取)

企业编号 243902

用户名称 zqxdsj

用户密码 zgjz8559

短信内容 <identifying-code>, 这是专属于你的验证码, 登录后就可以免费上网啦!

(3) 地址对象配置无误：

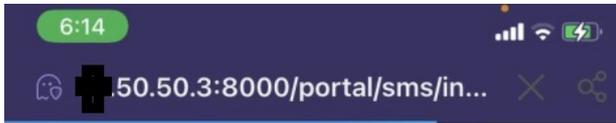
名称	内容(网络, 范围, 主机)	排除地址	描述	引用	操作
any	0.0.0.0/0		任何地址	6	
private	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16		私有地址	1	
ChinaUnicom	1.2.2.0/24, 1.4.4.0/24, 1.8.0.0/16...		中国联通	0	
ChinaTelecom	1.0.1.0/24, 1.0.2.0/23, 1.0.8.0/21...		中国电信	0	
ChinaEducation	1.51.0.0/20, 1.51.16.0/20, 1.51.32.0/19...		教育网	0	
ChinaMobile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

(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
bvi1		ge13, ge1	17.1.2/29		up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
bvi2		ge2, ge4	50.50.3/24		up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
bvi3		ge2_300, ge4_300			up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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。

```
无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::b04d:72d9:dcfd:a18d%16
IPv4 地址 . . . . . : 192.168.30.34
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.30.254

C:\Users\111111>telnet 50.50.3 8000
正在连接50.50.50.3...无法打开到主机的连接。 在端口 8000: 连接失败

C:\Users\111111>
```

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：

目的地址	掩码	下一跳	出接口	权重	距离	地址探测	状态	启用	操作
0.0.0.0	0.0.0.0	192.168.8.1		1	1	-	●	●	⊙
10.10.20.0	255.255.255.0	10.10.10.2		1	1	-	●	●	⊙
192.168.30.0	255.255.255.0	50.50.2		1	1	-	●	●	⊙

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。

