

知 某局点ACG1060-X1 本地web认证不弹页面直接上网

ACG1000 Portal认证 应用审计 曾招维 2021-11-29 发表

组网及说明

ACG二层透明部署，网关在交换机，ACG在交换机和防火墙之间access口串联，ACG中间用的bvi透传报文，bvi口起了地址，终端可以ping通。

问题描述

设备运行正常，做了本地web认证，所有用户不做认证即可直接上网。查看web认证配置未见异常（未开无感知），相关网段的控制策略已取消，未开启全局白名单。

主要配置截图（ge13口、宿舍组用户做web认证）：

本地WEB认证

用户登录唯一性检查

单一帐号登录

允许重复登录

允许个数 无限制

允许登录数 (2-1000)

更多设置

客户端超时 心跳超时 (10-144000分钟)

强制重登录间隔 (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

重定向URL (1-127字符，请设置 http/https 设一条URL)

认证策略

启用

名称 (1-31 字符)

描述 (0-127 字符)

源接口

源地址

目的接口

目的地址

认证方式

时间

用户录入

用户有效时间 永久录入

有效期至

临时录入

ID	名称	源地址	目的地址	源接口	目的接口	认证方式	时间	用户录入	用户有效时间
7	neiwan	172.3.0.0/16	172.3.25.0/24						
8	宿舍	172.3.25.0/24							

全局白名单

启用 禁用

名称	地址	描述	状态	操作
----	----	----	----	----

策略配置

IPv4控制策略

ID	状态	ID	行为	策略	用户	源接口	目的接口	源地址	目的地址	应用	服务	终端	描述	匹配次数	应用时间	日志	老化时间	操作
1	禁用	2	允许	defi	宿舍组	any	any	any	any	全部	any	any		0	always		0	
2	启用	1	允许	defi	neiwan	ge13	ge12	neiwan	any	全部	any	any		0	always		0	

		物理接口	子接口	网桥接口	聚合接口	隧道接口	无线接口	安全域	虚拟网线
+ 新建 × 删除									
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	ge12, ge13	192.168.100.10		up	✔	✎ ⚙		

1、第一次远程查看测试终端上线的认证方式为静态绑定，但查看配置无IP-MAC绑定，全局配置搜索相关IP和MAC也无特殊配置：

用户									
刷新 选择 冻结 解除冻结 注销									
用户名	所属组	IP地址	认证方式	终端类型	登录时间	在线时长	状态	操作	
1	hjq	宿舍组	172.3.25	静态绑定	正在识别	2021/11/ 4 分钟	正常	🔒	

2、建议现场替换终端和升级版本观察一下，发现终端的认证方式变为了未认证，但还是可以正常上网。

在线用户									
用户组									
在线用户总数：946									
属性组									
认证用户 1									
移动用户 74									
匿名用户 945									
用户名	所属组	IP地址	认证方式	终端类型	登录时间	在线时长	状态	操作	
1	172.3.25.2	匿名用户	172.3.25.2	未认证	PC(Window 2021/11/16 2 分钟		正常	🔒	

3、开启mac敏感，识别模式地址对象组强制模式、开启https弹页面（user-policy https-portal enable），测试时一直有web流量访问（抓包可观察到）。

4、设备上portal页面正常，无定制化。

解决方法

后与现场多次沟通，发现是现场的接线有问题，认证策略中的ge12作为源接口后，认证正常。

