

知 ACG1000策略中全局白名单针对mac地址不生效

应用审计 断桥残雪 2021-07-07 发表

问题描述

ACG1000策略中全局白名单针对mac地址不生效（依然受到策略限制），配置为此mac地址对应的ip地址就会生效（不受策略限制）

- 1、组网为跨三层组网，透明部署在核心交换与出口设备之间；
- 2、通过SNMP协议跨三层读取核心arp表获得终端的mac地址

解决方法

· 配置全局白名单的用户仅做会话识别，不做其它控制策略。

会话中三层访问的源mac为核心三层互联口mac，非终端mac，导致配置为mac地址不生效，ip生效

解决方法： 1、修改为二层组网，可通过mac白名单

2、保持现有组网，对该终端mac分配固定ip，通过ip白名单

