

知 ACG默认规则配置拒绝但不生效

ACG1000 李瑞 2021-07-02 发表

组网及说明

逻辑上串联的组网均涉及

问题描述

配置了默认规则为拒绝但是不生效，仍然能通，配置拒绝的策略后就能拒绝。

控制策略		策略分析																
		默认规则: <input type="radio"/> 允许 <input checked="" type="radio"/> 拒绝																
ID	状态	行为	策略	用户	源接口	目的接口	源地址	目的地址	应用	服务	协议	描述	匹配次数	应用安全	时间	日志	老化时	操作
1		拒绝	部门	SOE	...	any	any	any	即时通讯	any	any	微信	0	allow	-	0		
2		允许	default	any	any	any	any	any	全部	any	any		582	allow	-	0		
3		拒绝	default	any	any	any	any	any	办公软件	any	any	钉钉	0	allow	-	0		
4		允许	default	any	any	any	any	any	全部	any	any	测试: 允许	19	allow	-	0		
5		拒绝	default	any	any	any	any	any	全部	any	any	允许上网	0	allow	-	0		
6		允许	default	any	any	any	any	any	全部	any	any	测试: 网页	0	allow	-	0		
7		允许	default	any	any	any	any	any	全部	any	any	向日葵	15	allow	-	0		
8		拒绝	default	any	any	any	any	any	全部	any	any		273	allow	-	0		

过程分析

优先级：策略放通阻断>“域内接口间互访”>默认规则

解决方法

如下图所示，取消勾选安全策略配置中的“域内接口间互访”即可

安全域

名称 (1-31字符)

域内接口间互访

ge0
ge1
ge3
ge4
ge5

提交 取消

