

知 某局点M9K配置URL过滤黑名单不生效

URL过滤 小茗7ms 2022-03-29 发表

组网及说明

不涉及

问题描述

将指定ip加入URL过滤黑名单后，无法禁止访问

过程分析

1. 确认license是否有效

位置	特性名称	是否授权	类型	状态	有效期	安装时间
Chassis1	URLT	Y	Trial (date restricted)	In use	2022-02-17至2022-05-18	2022-02-17 08:37:05
	AV	Y	Date restricted	In use	2020-12-25至2025-12-29	
	IPS	Y	Date restricted	In use	2020-12-25至2025-12-29	
	ACG	N	-	-	-	
	IPRPT	N	-	-	-	
	SLB	N	-	-	-	
	SSL VPN	N	-	-	-	
	TT	N	-	-	-	
	WAF	N	-	-	-	

2. 确认URL过滤配置文件是否已调用及策略是否配置正确

编辑URL过滤配置文件

名称: 测试1 (1-31字符)

缺省动作: 允许 丢弃 重置 重定向 黑名单

开启云端查询功能: 开启HTTPS流量过滤功能:

白名单模式: 开启内嵌白名单功能:

记录日志:

白名单

HOST类型	HOST	URI类型	URI	编辑
--------	------	-------	-----	----

黑名单

HOST类型	HOST	URI类型	URI	编辑
文本	www.4399.com	--NONE--		

确定 取消

名称	源安全域	目的安全域	类型	ID	描述	源地址	目的地址	服务	用户	动作	内容...	命中...	流量	统计	应用	会话查看	编辑
<input checked="" type="checkbox"/>	MSK...	Any	Any	IPv4	0	Any	Any	Any	Any	允许	URL...				<input checked="" type="checkbox"/>	查看	
<input type="checkbox"/>	123	Any	Any	IPv4	1	Any	Any	Any	Any	允许					<input checked="" type="checkbox"/>	查看	
<input type="checkbox"/>	1	Any	Any	IPv6	1	Any	Any	Any	Any	允许					<input checked="" type="checkbox"/>	查看	

3. 确认DPI功能是否开启

```
=====  
display inspect status=====  
Chassis 1 Slot 0:  
Running status: normal  
Chassis 1 Slot 1:  
Running status: normal  
Chassis 1 Slot 4:  
Running status: bypass by configure  
Chassis 2 Slot 0:  
Running status: normal  
Chassis 2 Slot 1:  
Running status: normal  
Chassis 2 Slot 4:  
Running status: bypass by configure  
=====
```

bypass by configure: 代表因为配置原因引擎无法处理报文

```
#  
inspect optimization no-acsignature disable  
inspect optimization raw disable  
inspect optimization uncompress disable  
inspect optimization url-normalization disable  
inspect optimization chunk disable  
inspect bypass  
#
```

url过滤是属于dpi中的功能, inspect bypass将dpi功能全部关闭

inspect bypass命令用来关闭应用层检测引擎功能, 关闭应用层检测引擎功能后, 系统将不会对接收到的报文进行DPI深度安全处理。可能导致其他基于DPI功能的业务出现中断

url过滤是属于dpi中的功能, inspect bypass直接把dpi功能全部关闭, 由此找到了问题所在, 导致URL

过滤不生效

解决方法

开启DPI功能: `undo inspect bypass`

`undo inspect bypass`命令用来开启应用层检测引擎功能，此功能默认处于开启状态，但是开局一般建议关闭DPI功能，因为开启DPI功能比较消耗设备性能，导致CPU利用率高

