

知 某局点F100没有应用排行以及上网行为监控无内容

应用审计 孔德飞 2023-07-17 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

现场流量日志与上网行为监控无内容

过程分析

流量日志需要打开会话统计功能

```
session statistics enable
```

流量排行需要打开会话top统计功能

```
session top-statistics enable
```

上网行为审计需要做如下配置

```
app-profile 1_ipv4
```

```
ips apply policy default mode protect
```

```
data-filter apply policy default
```

```
url-filter apply policy default
```

```
file-filter apply policy default
```

```
anti-virus apply policy default mode protect
```

```
apt apply policy default
```

并且在安全策略中调用 (profile 1_ipv4)

```
security-policy ip试图
```

```
rule 1 name GuideSecPolicy
```

```
action pass
```

```
profile 1_ipv4
```

```
source-zone Trust
```

```
destination-zone Untrust
```

```
destination-zone DMZ
```

调用之后, 安全策略试图下, 敲一下加速

```
[H3C-security-policy-ip]accelerate enhanced enable
```

全局系统试图下, 敲一下激活DPI的命令

```
[H3C]inspect activate
```

```
Rule's activity begin:100%
```

敲了之后, 通过如下命令查看DPI的开启状态, 为normal则正常

```
[H3C]display inspect status
```

```
Chassis 0 Slot 1:
```

```
Running status: Normal
```

以下命令需要配置

```
dac log-collect service dpi traffic enable
```

```
dac traffic-statistic user enable
```

时间问题, 如果应用排行没内容, 以下内容配一下

```
clock timezone UTC add 00:00:00
```

解决方法

配置关键点

- 1 流量日志需要打开会话统计功能
- 2 流量排行需要代开会话TOP统计功能
- 3 上网行为需要配置应用审计策略并且要在安全策略中调用

配置好效果如下



时间	用户名	IP地址	应用类型	应用名称
2023-07-17 22:13:50	192.168.6.9	192.168.6.9	访问网站	微信
2023-07-17 22:13:46	192.168.6.9	192.168.6.9	访问网站	http
2023-07-17 22:13:35	192.168.6.9	192.168.6.9	访问网站	微信
2023-07-17 22:13:25	192.168.6.9	192.168.6.9	访问网站	微信
2023-07-17 22:13:25	192.168.6.9	192.168.6.9	访问网站	微信
2023-07-17 22:13:22	192.168.6.9	192.168.6.9	访问网站	http



时间	源IP地址	源端口	目的IP地址	目的端口	应用	URL	流量	会话数	应用名称
2023-07-17 22:14:48	Untrust	Untrust	192.168.6.9	192.168.6.9	http	TCP	1.2KB	1	CyberPower15.02
2023-07-17 22:14:47	Trust	Untrust	192.168.6.9	192.168.6.9	http	TCP	1.7KB	1	CyberPower15.02
2023-07-17 22:14:47	Trust	Untrust	192.168.6.9	192.168.6.9	http	TCP	2.9KB	1	CyberPower15.02
2023-07-17 22:14:47	Trust	Untrust	192.168.6.9	192.168.6.9	http	TCP	3.1KB	1	CyberPower15.02
2023-07-17 22:14:47	Trust	Untrust	192.168.6.9	84.16.87.12	rtsp	UDP	152B	1	CyberPower15.02
2023-07-17 22:14:46	Trust	Untrust	192.168.6.9	84.16.87.12	HTTP流媒体	TCP	15.9KB	1	CyberPower15.02
2023-07-17 22:14:46	Trust	Untrust	192.168.6.9	84.16.87.12	HTTP流媒体	TCP	5.2KB	1	CyberPower15.02
2023-07-17 22:14:45	Trust	Untrust	192.168.6.9	42.91.145.194	HTTP流媒体	TCP	9.9KB	1	CyberPower15.02
2023-07-17 22:14:45	Trust	Untrust	192.168.6.9	42.91.145.194	HTTP流媒体	TCP	8.1KB	1	CyberPower15.02
2023-07-17 22:14:44	Trust	Untrust	192.168.6.9	202.89.203.96	HTTP流媒体	TCP	10.3KB	1	CyberPower15.02
2023-07-17 22:14:44	Trust	Untrust	192.168.6.9	202.89.203.96	HTTP流媒体	TCP	64.1KB	1	CyberPower15.02
2023-07-17 22:14:44	Trust	Untrust	192.168.6.9	202.89.203.96	HTTP流媒体	TCP	11.1KB	1	CyberPower15.02
2023-07-17 22:14:44	Trust	Untrust	192.168.6.9	192.168.6.9	rtsp	UDP	152B	1	CyberPower15.02



