

知 seccenter监控ACG流量分析中应用流量中应用识别为unknown问题的解决方法

Seccenter A1000 王树旺 2015-06-17 发表

seccenter监控ACG实现行为审计功能时，流量审计正常，流量分析中也有流量分类，但是业务分类中的名称只有unknown类型，但是会有多种颜色区分。如下图所示：



原因为seccenter上面的服务定义库本身不全，缺省的服务类型满足不了ACG上面的业务种类，导致页面显示为多种unknown的服务类型。

在seccenter上的设备列表中，找到对应的ACG设备，然后在右侧的操作列中选择“从设备导入服务定义库”功能，补充seccenter中服务类型不全的问题。执行完成后重启web服务。

运行状态	设备名称	区域	设备型号	IP地址	操作
严重	Unknown(10.6.168.187)	未知区域	IPS	10.6.168.187	[Icons]
严重	Unknown(10.6.168.188)	未知区域	IPS	10.6.168.188	[Icons]
严重	Unknown(10.6.168.189)	未知区域	IPS	10.6.168.189	[Icons]
严重	Unknown(10.153.89.106)	未知区域	H3C SecPath F1000-E	10.153.89.106	[Icons]
严重	Unknown(10.153.89.196)	网络中心	H3C SecPath ACG2000-M	10.153.89.196	[Icons]
严重	Unknown(10.153.89.197)	未知区域	H3C SecPath T1000-A	10.153.89.197	[Icons]
严重	Unknown(10.153.89.200)	网络中心	H3C SecPath ACG8000-S3	10.153.89.200	[Icons]
严重	Unknown(10.153.129.97)	未知区域	IPS	10.153.129.97	[Icons]
严重	Unknown(10.153.129.169)	未知区域	IPS	10.153.129.169	[Icons]

该问题的原因包含但不仅限如上原因，如果以上方法未能解决现场问题，请收集现场截图和版本信息找业务软件二线寻求帮助。