ACG1000旁路部署设备上及ACGM上均看不到审计日志

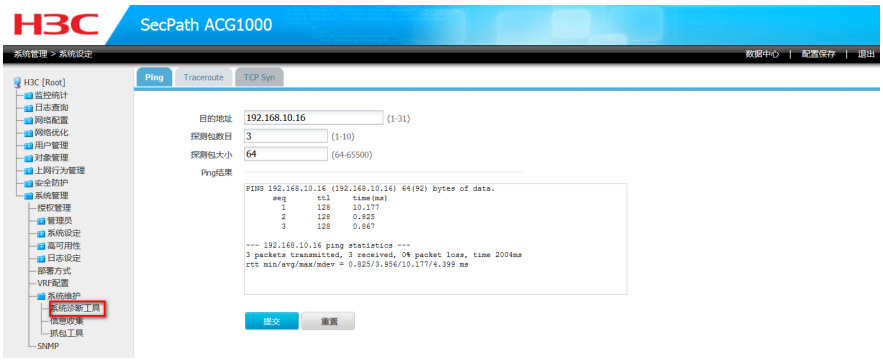
ACG1000 旁路 孙兆强 2016-09-18 发表

现场ACG1000旁路部署，在设备上和日志分析管理平台上都看不到审计日志。现场确认有流量，交换机流量镜像正确，并且策略也已经配置。

1.检查接口模式，已经修改为旁路部署。
2.查看客户配置的策略，发现选择的策略的源和目的接口都是镜像口。这样配置是有问题的。因为镜像过来的流量对ACG1000而言只收不发，所以出接口匹配不上策略，无法审计不出日志。将源和目的接口都改为any之后设备上日志都正常了。
3.设备上审计到日志之后，日志分析管理平台上仍然看不到流量。检查日志分析管理平台上设备上的状态是未上线状态。

名称	设备型号	设备IP	状态	CPU	MEM	磁盘	描述	WEB管理	详情	操作
acg1000-2		192.168.13.161		0%	0%	0%	---	WEB管理	查看	

对照官网配置，设备上配置日志服务器正确，日志分析管理平台添加设备正确。测试与日志分析管理平台的联通性。用设备自带测试工具测试结果如下。



测试结果，ACG1000与日志分析管理平台通信正常。怀疑与接口配置有关。查看相关资料发现，接口下缺少命令allow access center-monitor。在接口下配置此命令后点击操作栏尝试重新连接之后ACG1000与日志分析管理平台对接状态正常，日志接收正常。

名称	设备型号	设备IP	状态	CPU	MEM	磁盘	描述	WEB管理	详情	操作
acg1000-2		192.168.13.161		14%	34%	0%	---	WEB管理	查看	

这条命令的意思是允许集中网管来管理设备，这条命令只能通过命令行来进行配置。在web界面无法进行配置。

1.将策略中的接口源和目的都改为any，旁路审计时没有特殊要求策略中接口都配置成any
2.进入命令行，在接口下添加如下命令：
H3C> en
H3C# system-view
H3C(config)# interface ge0
H3C(config-ge0)#allow access center-monitor
3.

1.接口要改为旁路部署方式，请确认接口配置
2.旁路部署策略中源和目的接口改为any
3.注意ACG1000和日志分析管理平台的版本有对应关系，请查看ACG1000或者ACGM版本说明书。