

知 V7防火墙NAT会话日志输出到信息中心本机查看方式（D060之后较新版本上查看）

会话 Syslog日志 孔梦龙 2024-01-25 发表

问题描述

V7防火墙NAT会话日志输出到信息中心本机查看方式（D060之后较新版本上查看）

解决方法

(1) 开启NAT日志

nat log enable

nat log flow-begin

nat log flow-end

userlog flow syslog // 这个命令极其耗设备性能，开启后可能会引发CPU和内存异常



(2) 开启dac

dac log-collect service nat flow_log enable



%Jan 25 14:30:31:893 2024 F1090_P NAT/6/NAT_FLOW: Protocol(1001)=ICMP;Application(1002)=ICMP;Category(1174)=Other_Service;SrcIPAddr(1003)=61.2.2.1;SrcPort(1004)=31990;NatSrcIPAddr(1005)=6.6.6.16;NatSrcPort(1006)=0;DstIPAddr(1007)=55.66.1.1;DstPort(1008)=2048;NatDstIPAddr(1009)=55.66.1.1;NatDstPort(1010)=13;InitPktCount(1044)=1;InitByteCount(1046)=84;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=01252024143031;EndTime_e(1014)=;Event(1048)=(8)Session created;