[2012-5-7]H3C Comware V3平台防火墙维护类常见问题FAQ

金山 2012-05-07 发表

H3C Comware V3平台防火墙维护类常见问题FAQ

Q：H3C Comware V3平台防火墙CPU进程VSIF、SOCK占用率高，应如何处理?

A：V3平台防火墙基于单核心单线程硬件架构，当设备处理的业务流量较大时容易出现CPU占用率高的现象。VSIF进程与防火墙转发任务相关，可以反映出防火墙转发任务（如NAT业务）的负载情况；SOCK进程与防火墙本地收发报文任务相关，可以反映出防火墙本地任务（如L2TP、IPSec业务）的负载情况。以F1000S为例，这款型号防火墙吞吐量约为1Gbps，当防火墙处理的流量接近1Gbps时出现CPU利用率高是正常情况，此时可以考虑升级硬件设备或将业务分流，减轻单台设备的性能压力。在个别局点，即使业务流量压力很小也出现了CPU利用率高的问题，这通常与V3防火墙同时进行转发业务和本地业务时效率不高的问题有关。举例如下：故障现象发生时，防火墙CPU占用率很高，达到80%以上。在防火墙外网接口，既配置了NAT Outbound配置，又有IPSec配置，即防火墙既有转发任务，又有本地任务。如果取消两个配置其中之一，CPU利用率便马上下降，如果恢复配置，CPU利用率又会立即上升。该类问题目前没有特别有效的方法，建议增加一台设备将两种业务分开，比如使用另一台设备执行NAT业务，原防火墙只保留IPSec业务；或者将设备升级为一台Comware V5平台防火墙解决。

Q：H3C Comware V3平台防火墙运行过程中出现NAT Server功能失效应如何处理?

A：V3防火墙由于软件实现原因，在运行过程中可能会发生NAT Session表冲突，导致NAT Server功能失效。具体表现为当公网客户端通过NAT Server访问内网服务器时，报文从公网至内网转发时根据NAT Server执行目的IP地址转换，服务器返回数据却根据公网口配置的NAT Outbound命令执行源IP地址转换，造成客户端接收的返回数据包Socket错误而无法正常处理。该问题可以通过在配合NAT Outbound命令使用的ACL中，配置Deny规则，禁止服务器返回数据流匹配NAT Outbound命令相应的ACL规则缓解。