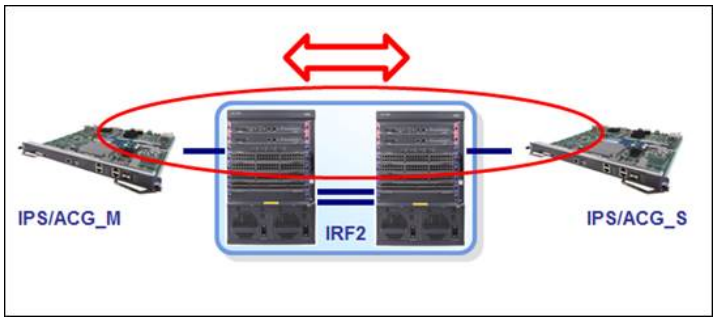
[2013-04-01]关于H3C SecBlade IPS&ACG插卡MQC引流部署可能导致广播风暴的公告

金山 2013-04-01 发表

关于H3C SecBlade IPS&ACG插卡
MQC引流部署可能导致广播风暴的公告

【产品型号】
SecBlade IPS、SecBlade ACG
【涉及版本】
所有版本
【问题描述】
2块以上（含2块）SecBlade IPS、SecBlade ACG单板配合H3C交换机部署MQC引流方案。设备割接入网后，在交换机与安全板卡内联接口出现报文风暴现象，引发业务丢包、网络中断等严重故障。
【原因分析】
常见组网如下图所示：



两台S7500E交换机各安装一块IPS、ACG类安全板卡，交换机部署IRF2。
由于SecBlade IPS、SecBlade ACG两类安全板卡属二层透明设备，交换机通过MQC引流方式将业务报文利用内联接口重定向至安全板卡后，通过安全策略检查的业务报文仍然会从该内联接口返回交换机继续转发。这个特殊机制对于交换机而言相当于在其与IPS、ACG内联口上形成了一个自环接口，而2个这样的内联口则形成了一个二层环路。例如，上图中部署2块IPS、ACG类安全板卡，内联接口均允许VLAN 10通过。当交换机在VLAN 10内接收到一个广播报文后，会通过内联接口广播至2块安全板卡，安全板卡接收并处理完成后分别回送给交换机，而交换机又会将接收到的报文再次广播至安全板卡，周而复始，沿上图中红圈所示形成严重的报文风暴现象，最终影响交换机正常业务转发处理。
在单台或多台未部署IRF2的交换机上配置2块或2块以上IPS、ACG类安全板卡，采用MQC引流方式，内联接口允许通过相同VLAN，一旦在该VLAN中出现二层广播、组播、未知单播报文，也会引起报文风暴现象，原理与前述相同。
【规避措施 / 解决方案】
在交换机配合SecBlade IPS、SecBlade ACG安全板卡部署MQC引流方案中，应注意在方案设计、部署实施等方面，参考以下方法，避免上述问题的发生。
1、若根据报文二层头信息配置交换机MQC引流策略，可配置为根据报文目的MAC地址是否为交换机三层虚接口MAC地址来决定是否执行重定向动作；同时在交换机与安全板卡内联接口配置QoS策略，仅允许目的MAC地址为交换机三层虚接口MAC地址的报文通过，阻断其它二层报文。配置案例详见附件一。
2、若根据报文三层头信息配置交换机MQC引流策略，可配置为仅重定向IP单播报文至安全板卡，同时在交换机与安全板卡内联接口部署QoS策略阻断二层组播、广播报文；并通过合理规划组网、配置二层内全部三层设备主动发送免费ARP报文等方式，避免在交换机与安全板卡内联接口允许通过的VLAN中内出现二层未知单播报文。配置案例详见附件二。
3、采用OAA引流方案（除S5800系列交换机外需取消IRF2部署）。