[2012-08-06]Comware V5平台防火墙的会话单向流检测是什么

金山 2012-08-06 发表

Q：Comware V5平台防火墙的会话单向流检测是什么?

A：在部分组网环境中，由于路由规划、不同厂商设备分担流量等原因，造成同一会话中只有单方向的报文在V5平台防火墙上处理，这种流量可以称为单向流。比如在某公司出口，H3C V5平台防火墙与友商防火墙形成分担关系，所有内网上行公网流量由V5防火墙处理，所有返回流量由友商防火墙处理，这便是一种典型的单向流场景。虽然单向流是一种不好的组网规划，但有时不可避免。如果来回数据流经过的是H3C V5防火墙的双机中不同的设备，比如防火墙A和B组成双机，从内到外数据流经过A，而返回的从外到内流量经过B，此场景不适宜开启单向流检测功能，而应该使用“非对称路径的双机热备”来解决。

对于防火墙而言，单向流即会话的来回路径不一致，会使得状态检测防火墙只能收到单向报文，从而无法根据协议状态机创建正常会话，进而无法转发数据。以TCP会话三次握手过程为例，SYN报文经过V5防火墙，但SYN+ACK报文从另外一台设备经过，当第三个ACK报文经过V5防火墙时，由于报文与当前会话状态不匹配，造成会话不能正常建立，业务不能正常交互。通过开启单向流检测功能，网管管理员可以使防火墙在一定范围内修改协议状态机，使得防火墙会话得以正常建立，解决这一问题。

当V5防火墙使能单向流状态功能后，为满足会话表项的正常建立，防火墙针对TCP/UDP/RAWIP等协议的状态机会有一些变化，主要内容包括：

针对TCP协议报文：

双向流状态机认为首报文是SYN_ACK是非法的，但在单向流检测模式下需要考虑SYN报文可能不经过设备，因此首报文就是SYN_ACK。在单向流检测模式下SYN_ACK报文将新建会话并切换到SYN_RECV状态。

双向流状态机认为SYN_SENT状态下收到正向ACK报文是非法的，但在单向流检测模式下需要考虑SYN_ACK报文可能不经过设备，因此第二个报文就是正向ACK。在单向流检测模式下将会话切换到TCP_ESTABLISHED状态。

对于UDP报文：

双向流状态机UDP会话在UDP_OPEN状态时，收到正向报文会维持UDP_OPEN状态不变。而在单向流检测下将会使会话切换到UDP_READY状态。也就是说两个正向报文就会使会话进入UDP_READY状态。

对于RAWIP报文：

双向流状态机在RAWIP_OPEN状态时，收到正向报文会维持RAWIP_OPEN状态不变。而在单向流检测下将会使会话切换到RAWIP_READY状态。也就是说两个正向报文就会使会话进入RAWIP_READY状态。