V5平台防火墙“单向流检测”功能是怎样的？哪些场景需要使用？

其他 彭旭 2019-10-29 发表

问题描述

V5平台防火墙“单向流检测”功能是怎样的？哪些场景需要使用？

解决方法

通常情况下，Comware V5平台防火墙在处理网络流量时，严格按照协议及域间策略检查经过设备的报文，对于合法报文，可以正常建立防火墙会话表项并转发，对于异常报文及不符合域间策略的报文则丢弃处理。

以TCP协议为例，防火墙上默认存在Trust区域至Untrust区域允许的策略，Trust区域客户端首先发起连接，向处于Untrust区域的服务器建立TCP三次握手连接。防火墙从正向收到SYN，反向收到SYN+ACK，正向收到ACK报文后，创建一条TCP EST状态的会话表项。但如果因组网原因，例如V5防火墙和另一台路由器共同部署在网络出口，上行流量通过V5防火墙转发，下行流量通过路由器转发，那么在V5防火墙上，就仅能收到SYN报文和ACK报文，SYN+ACK报文不经过防火墙。如此在V5防火墙上是无法创建会话表项的，后续业务报文也不能正常转发处理。UDP、ICMP协议的情况与前述TCP协议类似。

当我们在V5平台防火墙上使能“单向流检测”后，在域间策略允许的前提下，以TCP协议为例，防火墙从正向接收到SYN报文和ACK报文，或者从反向接收到SYN+ACK报文，都可以直接创建一条EST状态的TCP会话表项。这样该条会话的后续报文就可以转发了。UDP、ICMP协议使能该特性后原理与TCP协议相似。

除防火墙和路由器组网且来回路径不一致的环境外，在H3C V5平台防火墙与其他友商防火墙或路由交换设备混合组网且来回路径不一致环境、或者其他的只有单向报文经过防火墙的特殊组网环境中，都可以通过开启“单向流检测”使防火墙可以正常创建会话表项并转发业务报文。由于“单向流检测”功能开启后，防火墙对会话表项创建条件的检查相对较弱，因此不建议在普通组网环境中开启此功能，避免削弱防火墙的安全性。