Hillstone智能下一代防火墙技术白皮书之数据包路径检测篇

关键词： 数据包路径检测、在线检测、模拟检测、导入检测、可视化运维。

摘要： 本文介绍了Hillstone T系列智能下一代防火墙中具有专利的数据包路径检测技术，该技术通过在线检测、模拟检测、导入检测三种检测手段，自动对流经防火墙的数据包进行跟踪和信息收集，通过诊断及时发现故障点，给出诊断报告和修改建议，可以帮助用户提前发现防火墙内部安全处理过程故障点、自动快速定位问题，以及新业务上线前进行验证。

概述

当业务中断或防火墙设备发生故障时，运维人员比较关注如何能够方便、快速、准确地定位和解决问题。通常情况下，运维人员需要登录到防火墙设备上查阅相关配置、日志等信息定位故障，耗费大量的时间。Hillstone T系列智能下一代防火墙中独创的具有专利技术的数据包路径检测功能，通过对流经设备数据包的处理过程进行跟踪和信息收集，并以图形化方式动态展现防火墙内部数据处理的整个流程，自动进行故障诊断，并以报告形式给出故障原因及相应的处理建议，只需两三分钟时间，大大减少了手动进行故障诊断的时间。从而帮助网络运维人员更快更准的进行故障排查，提高解决故障的效率，减少因故障而导致业务中断的影响。

Hillstone 数据包路径检测技术

Hillstone数据包路径检测技术通过对流经防火墙的数据包进行跟踪，图形化展现数据包经过每个模块的处理过程，让用户明确知道数据包在防火墙上都经过哪些处理。数据包路径检测支持在线检测、模拟检测、导入检测三种诊断方式。

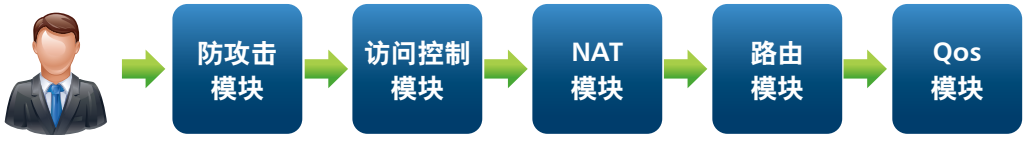

图1 数据包路径检测流程图

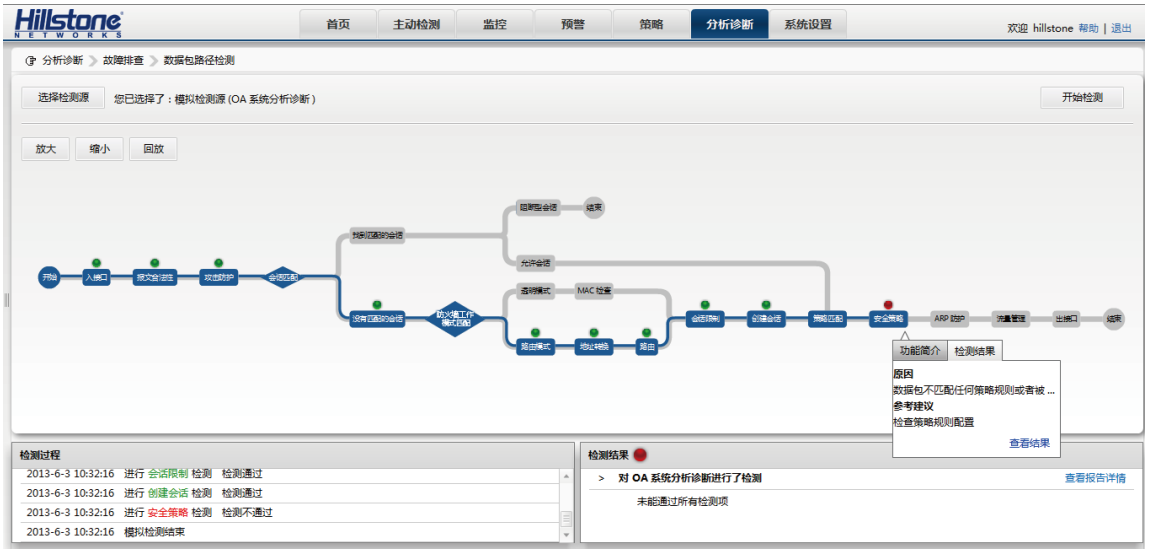

图2 数据包路径检测示例图

- 在线检测

在线检测，是针对用户实际的流量进行实时自动诊断，用户只需配置数据包的检测接口、源地址、用户名、URL、源端口、目的端口、协议、应用这些条件之一或组合。根据用户配置的条件，数据包路径检测模块会对流经防火墙的实际流量进行条件匹配，对匹配上的数据包进行路径检测，自动分析和呈现实际流量在防火墙中每一模块处理过程，诊断出故障所在，给出原因及修改建议。

图3 数据包路径在线检测流程图

- 导入检测

导入检测是导入用户抓包文件，配置诊断接口、源地址、目的地址、源端口、目的端口、应用、协议等过滤条件之一或组合，然后开始诊断。数据包路径检测模块会解析导入文件，根据抓包文件中数据包数据模拟其中数据包交互情况，并在防火墙中回放，系统会根据过滤条件进行诊断，帮助用户定位该抓包文件模拟真实流量中的问题，也可以帮用户在设备上线之前模拟真实流量交互情况。

图4 数据包路径导入检测流程图

- 模拟检测

模拟检测是根据用户设置的诊断接口、源地址、目的地址、协议、源端口、目的端口等相关条件，会自动生成一个数据包。通过诊断接口流入防火墙，模拟真实的流量来进行相关问题的诊断。同时，该诊断手段也可以帮助用户在设备未上线时来诊断防火墙配置以及对真实流量处理是否正确，保证设备上线时万无一失。

图5 数据包路径模拟检测流程图

上述三种诊断方式在进行数据包路径检测过程中会收集数据包及各模块处理信息，结合用户配置、设备资源信息、威胁信息等关联信息进行综合分析，诊断结束时以报告信息呈现出诊断结果，其中包含数据包路径流程图、检测源、检测时间、检测结果、检测报文、故障原因以及修改建议。

Hillstone 数据包路径检测技术用户价值

- **定期检测，提前发现故障点**

当运维人员进行网络日常维护时，可以利用Hillstone数据包路径检测技术进行防火墙的故障排查，定期通过在线检测、导入检测、模拟检测三种诊断方式进行数据包路径检测，来提早发现网络的故障点，减少故障造成的损失。

- **快速定位，及时解决故障**

当网络发生故障时，可以利用Hillstone数据包路径检测技术进行防火墙故障的排查，通过在线检测、导入检测、模拟检测三种诊断方式进行数据包路径检测，自动进行防火墙故障排查，运维人员可以根据诊断报告，快速定位和解决问题。

- **模拟流量，新业务上线验证**

当新业务上线时，运维人员会担心新上线业务会给原有网络带来影响或者新业务上线能否正常工作。用户可通过Hillstone数据包路径检测技术进行新业务上线前配置和功能验证，通过导入检测或模拟检测来模拟真实流量，进行配置和功能的验证，提前发现问题，保证新业务上线能正常运行。

文档编号：EX-09.01-SG0000-5.5R1-0215-Ch-02