H3CData 网络流量分析一体机

网络流量分析一体机

产品介绍

产品简介

网络流量分析一体机是一款大容量存储的高性能数据包采集和分析平台，可以分布部署在网络的关键节点，实现了对网络通讯数据包级的高性能实时分析。

通过对数据存储，挖掘、分析，实现对关键业务中的网络异常、应用性能异常和网络行为异常实时发现、以及异常原因的回溯分析，提升对关键业务的运行保障和问题处置效率。

产品形态

H3C NaviData5200一体机硬件设备，通过交换机、路由器、分光器等镜像网络中的流量旁路部署在网络中。

核心功能

流量回溯分析：任意时间段的拖拽回溯历史MAC、IP、应用、会话、数据报文，一级级深度钻取，WEB协议解码，多角度还原历史场景；

流量可视分析：数10万用户、2000+应用、上万服务器的流量、质量、行为进行全量展示、相互关联、多级钻取；

异常流量分析： 流量异常、质量异常、行为异常、协议异常进行告警展示、日志记录；

产品优势

高性能：10G-40Gbps实时处理能力；

高精度：多种精度实时统计分析（1秒~1天）；

大容量：强大数据存储 (内置最大 60TB)；

回溯：TB级原始流量数据秒级定位；

扩展性：提供Restful API接口，Syslog接口；

产品主要功能

网络流量采集

- ✓ 平台采用旁路部署方式，通过以太口、POS 端口镜像方式采集网络流量数据，不改变企业原有网络架构；
- ✓ 支持基于 VLAN、VXLAN、MPLS VLAN、QINQ、网段等方式配置虚链路接口，实现对云数据中心、SDN 网络、分流交换汇聚流量进行灵活采集；
- ✓ 可提供链路流量实时数据包抓取及历史数据回溯功能，并可自定义捕获条件与参数。

应用协议解析

- ✓ 平台采用 DPI（Deep Packet Inspection）深度包检测技术进行应用层协议解析，可准确高效识别 1800 余种预定义应用，500 种自定义应用，充分分析网络流量构成、性能、流速等；
- ✓ 支持离线报文远程解码分析，支持源端回溯系统存储报文通过 WEB 进行协议解码（不需要下载到本地）、时序图展示、HTTP 等内容还原；

流量回溯分析

- ✓ 能够分布式部署在各个监控的网络节点，实时分析捕获流量,实时保存捕获到的网络通讯数据包，进行长时间、大容量的数据存储能力；
- ✓ 能发现网络中存在的窃密行为，对捕获的原始数据包、数据流、网络会话、应用日志等各种统计数据；
- ✓ 具备快速的数据检索能力、随时分类查看及调用任意时间段的数据，具有回溯分析的能力；

流量全景呈现

- ✓ 平台对网络流量实现 OSI 7 层流量监控分析，可显示全双工接口的收、发和全部的流量、数据包信息；
- ✓ 提供对主机、协议、会话等维度的分析内容呈现，并支持关联分析、智能排序、模糊查询、多级钻取等功能；
- ✓ 针对用户、业务应用及服务器对象，即可呈现历史数据统计分析结果，也可提供实时流量、会话信息的呈现与条件检索，让用户对网络流量、业务状态一目了然。

网络质量呈现

- ✓ 针对网络流速、时延、异常等情况进行实时分析和趋势预测，对故障定位、链路升级、带宽规划、策略调整等进行数据支撑；
- ✓ 支持网络异常的监控与呈现，包括网络层、应用层的异常连接、异常会话的统计分析结果呈现；
- ✓ 支持网络响应时延和应用响应时延的监控与呈现，协助判断用户体验时延偏差是由于网络影响导致还是应用影响导致。

视频质量分析

- ✓ 视频监控网络质量进行分析，分析流量、流量突发、网络丢包、网络时延、网络抖动等业务指标，针对摄像头、业务服务器进行质量排名；
- ✓ 针对单个摄像头、区域内所有摄像头、摄像头—业务服务器进行统一质量呈现；

- ✓ 支持视频监控网络流量异常（流量中断、突发、时延抖动超标）告警；

应用行为分析

- ✓ 针对内部用户访问内部资源与外部资源以及外部用户访问内部资源的多种用户行为进行画像分析和数据关联分析，准确识别异常用户访问和用户异常访问；
- ✓ 针对用户各种访问资源和行为进行细粒度日志审计，并根据日志信息与用户正常访问基准进行比对，实现用户访问合规性分析与安全趋势分析。

异常流量分析

- ✓ 通过对流量数据异常检测，快速发现网络攻击、蠕虫、木马、异常连接、敏感数据外发、违规操作等危害网络安全的异常行为；
- ✓ 快速发现高级定向攻击行为，准确获取攻击痕迹与证据，及时阻止进一步扩散和渗透。

典型应用场景

网络出口流量分析

- ✓ 出口进出流量细粒度全景呈现
- ✓ 出口进出流量多维度呈现
- ✓ 流量回溯分析故障、责任界定
- ✓ 提升运维管理效率和响应速度

数据中心流量分析

- ✓ 虚拟链路网络流量与质量的监控
- ✓ 关键业务多维度呈现、分析
- ✓ 流量回溯分析故障、责任界定
- ✓ 异常流量监测与发现
- ✓ 提升运维管理效率和响应速度

产品规格

产品型号	硬件环境	产品性能	硬件规格
BD-ND5200-G2-12LFF-40Gb-B	H3C NaviData5200 一体机	40Gbps/20 万用户	双 Intel E5-2683 v4 CPU，内存 128GB，4 个千兆电口，4 个万兆光口，硬盘 64TB，双电源；
BD-ND5200-G2-12LFF-20Gb-B	H3C NaviData5200 一体机	20Gbps/10 万用户	双 Intel E5-2630 v4 CPU，内存 64GB，4 个千兆电口，2 个万兆光口，硬盘 44TB，双电源；
BD-ND5200-G2-12LFF-10Gb-B	H3C NaviData5200 一体机	10Gbps/5 万用户	双 Intel E5-2620 v4 CPU，内存 32GB，4 个千兆电口，2 个万兆光口，硬盘 12TB，双电源；

选配信息

项目	描述
BD-ND5200-G2-12LFF-40Gb-B	支持 40Gbps 流量采集，适配 H3C NaviData5200 一体机高端硬件；
BD-ND5200-G2-12LFF-20Gb-B	支持 20Gbps 流量采集，适配 H3C NaviData5200 一体机中端硬件；
BD-ND5200-G2-12LFF-10Gb-B	支持 10Gbps 流量采集，适配 H3C NaviData5200 一体机中低端硬件；
特征库升级服务（LIC-X-1Y）	提供网络流量采集软件 APP 应用一年升级功能，支持 BD-ND5200-G2-12LFF-40Gb-B\BD-ND5200-G2-12LFF-20Gb-B\BD-ND5200-G2-12LFF-10Gb-B 型号；

新华三大数据技术有限公司

郑州总部
郑州市高新区科学大道与黄帜栌总部大观 1 号
邮编：450000
电话：010-63108666
传真：010-63108666

http://www.h3c.com.cn

客户服务热线
400-810-0504