网络检测与响应(NDR)

最佳实践

文档版本 01

发布日期 2025-09-04

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 NDR 最佳实践汇总

本文汇总了NDR常见应用场景的操作实践，为每个实践提供详细的方案描述和操作指导，帮助用户轻松使用NDR业务。

表 1-1 最佳实践一览表

实践	描述
使用NDR进行威胁溯源和分析	NDR实时对流经主机的流量进行威胁检测，过程中都检测到什么威胁，威胁进展到了什么阶段，需要用户对攻击的过程、进展和结果进行分析判断，然后做出相应的处理。
插件批量安装	介绍如何通过NDR为HSS主机批量安装插件。
使用NDR对主机流量进行检测	介绍如何通过NDR检测非加密流量和加密流量。
异常流量排查	基于流量统计数据，分析流量异常情况，定位业务问题或者网络威胁。

2 使用 NDR 进行威胁溯源和分析

应用场景

NDR实时对流经主机的流量进行威胁检测，过程中都检测到什么威胁，威胁进展到了什么阶段，需要用户对攻击的过程、进展和结果进行分析判断，然后做出相应的处理。

方案架构

*本节介绍解决方案架构，为了更直观，建议采用**图+文字**的形式，图中需要体现本方案的工作原理、涉及的资源、资源分布region、不同资源之间的关系、以及架构中的安全设计部分。*

方案优势

本节提供方案优势，基于前文介绍的方案架构，着重结合当前场景面临的技术痛点，从技术痛点逐条切入，分析我们提供的方案有哪些优势，可以为客户带来什么价值。

约束与限制

介绍整体方案层面的约束与限制。

资源和成本规划

需要用到的资源，例如：

资源	资源说明	数量	成本说明
云模式WAF（ELB接入）	用于接入网站，提供Web、CC攻击防护。	1	WAF的计费方式及标准请参考。
DDoS原生高级防护	用于防护接入WAF的网站类业务，提供DDoS攻击防护。	1	DDoS原生高级防护的计费方式及标准请参考。

步骤一：查看整体安全状态

步骤1 登录NDR服务控制台。

步骤2 在左侧导航树，选择“安全分析”。

步骤3 通过查看近1小时、近24小时和近7天的检测情况，了解NDR整体安全状态。

----结束

步骤二：分析攻击趋势

步骤1 在左侧导航树，选择“威胁检测 > 攻击趋势”。

步骤2 查看“外部访问”、“主动外联访问”、“内部访问”的攻击趋势，获取攻击集中的时间段、攻击类型分布和攻击次数等信息。

----结束

步骤三：分析攻击阶段

步骤1 在左侧导航树，选择“威胁检测 > ATT&CK矩阵”。

步骤2 查看网络攻击的技术类型，并展开分析该技术类型下的攻击日志。

----结束

步骤四：分析攻击者画像

步骤1 在左侧导航树，选择“威胁检测 > 攻击者画像”。

步骤2 展开分析攻击者IP相关信息，实现攻击溯源，并对攻击源IP进行处理。

----结束

3 插件批量安装

前提条件

ECS已经安装HSS，并且HSS开启了防护。

操作步骤

步骤1 进入主机插件管理界面，选择需要进行插件安装的主机，一次最多支持10台主机同时触发安装，选中后，单击触发安装。

步骤2 在弹出的窗口中选择要安装的插件规格以及版本，需要进行加密流量检测的主机需要安装专业版的插件。

步骤3 成功触发安装后，对应主机的状态会从“未安装”变为“安装中”。

步骤4 可以通过单击刷新按钮或单击“同步数据”获取插件安装的最新状态，状态从“安装中”变为“运行中”则说明插件已安装成功并正常运行。

----结束

4 使用 NDR 对主机流量进行检测

4.1 检测非加密流量

前提条件

主机已安装插件并且状态为运行中。

约束说明

非加密流量支持流量检测及全流量检测，开启流量检测只会检测高危流量，如需检测全部流量，请开启全流量检测。全流量检测开启的情况下，如果流量较大会导致服务器资源消耗增加，因此建议关闭全流量检测，仅开启流量检测。

检测非加密流量

步骤1 进入检测策略界面，选中需要开启流量检测的机器。

步骤2 单击开启流量检测按钮即可批量开启检测，一次最多支持10台主机同时触发开启检测。

----结束

4.2 检测 JAVA 进程的加密流量

前提条件

主机已安装专业版插件并且状态为运行中。

加密系统默认进程

步骤1 在左侧导航树中，选择“检测管理 > 检测策略”，进入“检测策略”页面。

步骤2 在目标服务器所在行，单击“加密进程配置”。

步骤3 在“系统内置”页签，打开“默认进程检测”的开关。在弹窗中，单击“确定”。

----结束

加密自定义进程

步骤1 在左侧导航树中，选择“检测管理 > 检测策略”，进入“检测策略”页面。

步骤2 在目标服务器所在行，单击“加密进程配置”。

步骤3 在“用户添加”页签，根据实际选择进程添加方式。

步骤4 添加系统运行中的进程：单击“添加进程”，勾选需要的进程后，单击“确认”。

步骤5 添加自定义进程：单击“创建自定义进程”，设置进程类型和进程名称后，单击“确认”。

表 4-1 参数说明

参数	说明
进程类型	当前支持二进制和Java，根据实际选择。
进程	输入进程的名称。

----结束

配置黑名单目录

步骤1 在左侧导航树中，选择“检测管理 > 检测策略”，进入“检测策略”页面。

步骤2 在目标服务器所在行，单击“加密进程配置”。

步骤3 在“黑名单目录”页签，单击“创建黑名单目录”，配置黑名单目录信息。

步骤4 配置完成后，单击“确认”。

表 4-2 参数说明

参数	说明
进程类型	当前支持二进制和Java，根据实际选择。
目录	设置无需检测加密流量的目录。 ● 所有绝对路径都以根目录“/”开始。 ● 路径中的每个目录和文件名之间用斜杠“/”分隔。 ● 控制拉黑范围，不允许直接填写“/”，至少是二级目录。 ● 仅支持“/文件夹/文件夹”，不支持“/abc/.. /abc/*/def”。
描述	输入进程的描述。

----结束

5 异常流量排查

应用场景

基于流量统计数据，分析流量异常情况，定位业务问题或者网络威胁。

前提条件

NDR检测插件已经安装到业务主机上，开启了防护功能。

步骤一：整体流量情况检视

- 通用场景

  通过单击“流量分析”，可查看近1小时、近24小时和近7天的流量统计情况统计，了解云业务的流量状态，进行业务分析和流量型攻击风险评估。统计方向支持外到内（外部访问云内主机），内到外（内部主机访问云外）和内到内（内部主机间访问）。

- 典型流量分析场景

  流量激增或跳变：可通过流量趋势折线图，了解特定时间段内存在流量突变情况。协助分析开展分析，研判是业务变化，或者网络攻击行为。

  如果是业务变化，反馈业务团队，是否要进行业务资源调整。

  如果是网络DoS攻击行为，要开展进一步的分析研判，确定是否要进行威胁处置。

步骤二：详细流量日志分析

步骤1 单击日志审计>日志分析功能菜单。

步骤2 然后单击流量日志选项卡，可查看一段时间内的流量统计数据。

一分钟会基于五元组维度，生成一条统计数据，统计数据中会记录时间、源/目的IP，端口，字节数和报文数等信息。支持按照多条件筛选，协助分析人员在第一步的统计报表基础上，进一步分析在特定时间段内的激增流量到底是哪些，然后开展业务应对或风险处置。

----结束

