RG-BDS-TSP系列
流量态势感知

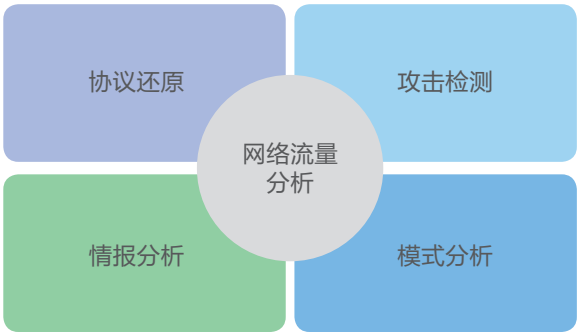
如有疑问
扫一扫在线咨询

Ruijie锐捷 Networks

产品概述

RG-BDS-TSP流量态势感知设备主要目的是进一步完善BDS在网络安全数据采集能力而开发的。其主要设计目的是能在高速网络环境下实现对主流网络数据包的解码、协议识别及会话重组/保存、重要原始网络数据包的保存、威胁情报检测、攻击检测等；对于相关重要的会话信息、攻击检测、威胁情报检测等生成的安全事件转发至BDS上层模块作为进一步分析的数据来源。

另外，RG-BDS-TSP利用一定的学习算法，提供了针对动态生成域名（DGA）的检测；以及对一些常见应用协议的元数据（Metadata）进行了抽取，用户可以对这些数据进行较为详细的查询。



RG-BDS-TSP分析维度和分析能力

RG-BDS-TSP具有独特而强大的网络流量审计和分析功能，结合攻击检测技术、异常流量检测技术、威胁情报技术、大数据安全分析技术、安全态势感知技术以及丰富的安全事件报告功能，可有效检测外部攻击、内部非法连接、网络会话模式异常等安全威胁，是对传统安全防御系统的完善和补充，成为企业提升安全防御水平的有力武器和必要工具。

产品特性

高速的网络抓包及模式匹配技术

RG-BDS-TSP采用零拷贝、全程无锁化技术处理网络流量数据包，而且充分利用CPU向量化指令对各类模式进行识别或匹配，故即使在超大流量情况下，系统整体处理也几乎感知不到延时。

协议的深度识别，更全面、更精确分析恶意行为

独有的智能协议识别技术，可高速、准确地识别千余种应用，检测各种协议伪装行为；同时支持HTTP、TLS（含HTTPS）、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet等协议的3-7层元数据提取、存储、搜索，分析，可二次挖掘可疑攻击行为。

高度智能化的分析能力

RG-BDS-TSP采用多种智能分析方法（包括支持向量机、马尔科夫转移概率分析、距离分析、参数及非参数假设检验分析等）对各类网络连接/流量进行深度分析，对可能隐藏的问题进行深层级挖掘，以提供更广范围、更深层次的安全检测能力。

多维度的纵深检测机制，提供最佳的检测率和最低的误判率

从已知签名检测、行为检测、网络会话异常检测、威胁情报检测及事件关联分析等多个维度对URL、邮件、网络通道、流量等威胁载体中各类安全威胁进行深度检测，并在高级持续威胁的漏洞利用、后门植入、后门网络通道，C&C回连、流量异常等多个阶段、多个攻击环节上形成纵深、完备的检测体系，从而提供最佳的检测率和最低的误判率。

情报为王，把握行动先机

整合包括最全的全球C&C黑名单库在内的多类的威胁情报库，可快速、准确发现已知的、可疑的高级持续威胁的攻击来源，使安全管理人员可以专注于实际风险及关键的威胁信息，把握先机，快速解决问题。

大数据安全分析，持续改进分析效能

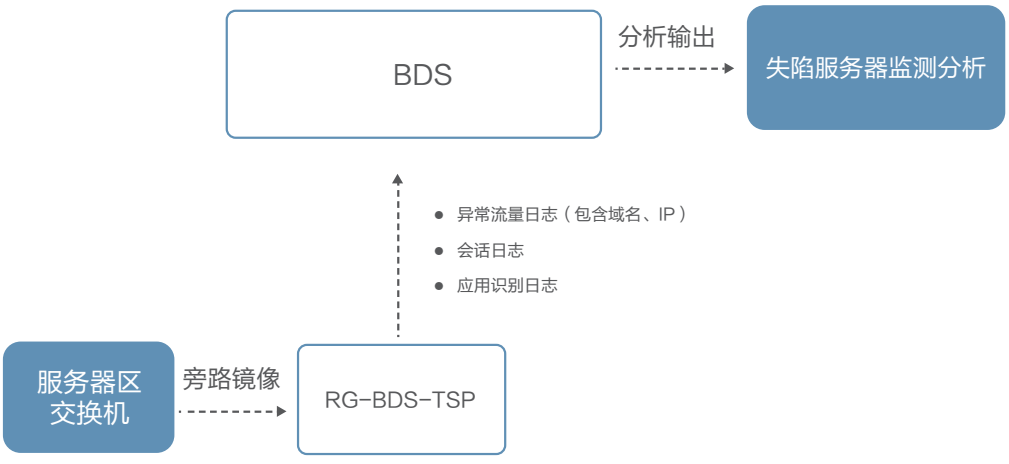
对于HTTP、TLS、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet等应用协议的元数据及会话数据，系统通过大数据技术全量存储、搜索分析，识别、挖掘其中可疑的攻击行为，促使安全分析效能持续改进。

增强的威胁态势可视化，掌控全局

根据威胁程度在客户所属国地图与世界地图上从多个维度来显示各类威胁攻击分布态势及会话分布态势，并可对威胁信息及会话进行深层次钻取、追踪分析，可快速把握全局，在攻击事件尚未形成破坏性影响前及时响应。

典型应用

RG-BDS-TSP可以配合RG-BDS-A共同使用；可将RG-BDS-TSP视为RG-BDS-A的组件进行部署。可采用旁路SPAN部署方式和TAP部署方式，两种部署方式均不会改变用户现有网络架构和网络配置，且不会对用户现有的生产业务或应用产生任何影响；设备部署的示意图如下：



RG-BDS-TSP联动部署示意图

RG-BDS-TSP也可以单独部署使用，直接部署在相应交换机旁边，采用旁路SPAN部署方式。用户只需要把要监控的流量从相应交换机镜像过来即可。设备部署的示意图如下：

RG-BDS-TSP独立部署示意图

订购信息

本产品订购信息		
型号	描述	备注
RG-BDS-TSP G	千兆流量安全态势感知探针，1U硬件，可独立使用作为流量安全态势感知，具备攻击检测、会话还原、流量深度分析能力，具备失陷分析和大屏展示，也可配合RG-BDS-A使用构成日志、流量综合态势感知，补充RG-BDS-A流量维度的采集分析能力。固化6个千兆电口，单电源，4TB硬盘、32G内存，默认支持1Gb吞吐，100万并发会话，提供2个扩展插槽，设备自带三年特征库升级服务授权。	硬件
RG-BDS-TSP X1	万兆流量态势感知硬件，标准2U机架设备，双电源，16T硬盘，2个千兆电口和2个万兆光口，3个扩展槽（每个扩展槽支持4千兆口/2万兆/4万兆扩展），最大支持14个万兆光口，提供高速、实时的网络会话还原、分析和存储功能；对各类主流网络协议进行深度识别，并配合大数据安全平台分析其中可能潜在的多种威胁，提供相关网络威胁数据包的取证功能。既可以配合大数据安全平台RG-BDS-A使用，也可以支持独立部署。	硬件
RG-BDS-TSP M600	低端流量态势感知硬件，标准1U机架设备，单电源，1T硬盘，6个千兆电口，4个千兆光口以及2个扩展槽；提供高速、实时的网络会话还原、分析和存储功能；对各类主流网络协议进行深度识别，并配合大数据安全平台分析其中可能潜在的多种威胁，提供相关网络威胁数据包的取证功能。既可以配合大数据安全平台RG-BDS-A使用，也可以支持独立部署。	硬件

锐捷网络股份有限公司

欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818