天阗入侵检测与管理系统 V7.0

(NT16000-CS-L-JZ03)

天阗入侵检测与管理系统 V7.0（产品型号：NT16000-CS-L-JZ03）是一款集双向特征检测、机器学习模型、综合分析模型、威胁情报、挖矿分析等多场景、多种能力于一身的下一代检测探针。双向检测能力确保了上报事件的准确性，检测日志和攻击链等分析场景结合，能够协助运维人员快速的发现网络安全威胁。将数十种协议采集元数据与安全威胁日志加密后外发，为上层统一展示平台提供丰富基础的数据。

一、产品特点

- **全面精确的威胁发现**

入侵检测系统结合特征库针对已知攻击进行检测，实时告警各种网络攻击，如 SQL 注入、XSS 攻击、CSRF 攻击、缓冲区溢出、拒绝服务、扫描探测、非授权访问、蠕虫病毒、僵尸网络、木马后门、APT 事件、挖矿事件、勒索软件等攻击，同时针对已知攻击结合双向检测功能进行进一步优化，提高事件精准性，减少误报，减轻运维人员负担，有效帮助企业降低 IT 成本。

- **丰富多样的 DOS 攻击检测能力**

入侵检测系统能够全面检测 TCP_stream Flood、Tcp_synrst Flood、Tcp_synonly Flood、UDP Flood、ICMP Flood、DNS Flood、HTTP Flood，等常见的 DOS 攻击，发现网络异常宽带消耗，减轻 DOS 攻击对客户网络带来的危害。。

- **高度灵活规则自定义能力**

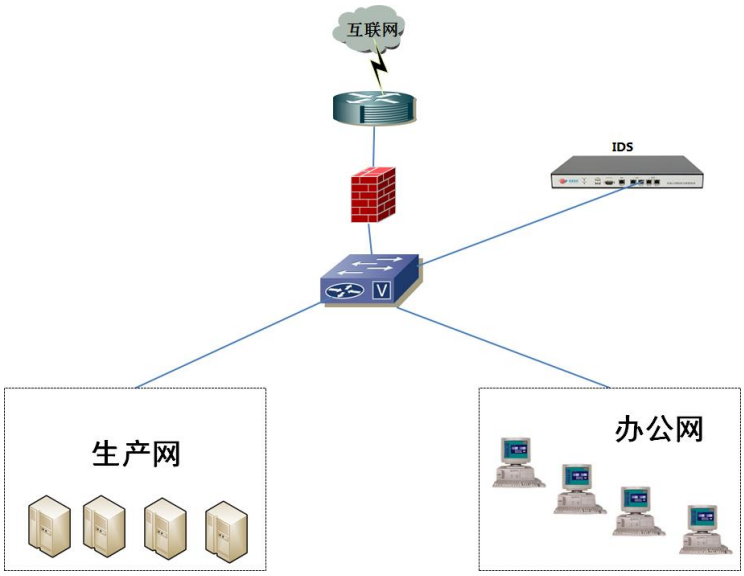
入侵检测系统具备全新规则系统，保持原有规则引擎同时完美兼容 snort 规则，支

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

持自写、开源、商用 snort 规则导入使用，同时兼容 LUA 脚本，通过脚本高级分析功能可用来检测规则集语法中无法检测的内容。

二、产品部署

从简化管理的角度来讲，适合采用简单的扁平化部署与管理方案。这种环境下，往往只需部署一台设备，采用单机管理的模式，整个部署环境如下图所示：



三、产品规格表

产品名称	**天阗入侵检测与管理系统 V7.0**
产品型号	**NT16000-CS-L-JZ03**
硬件规格	标准 2U 设备，配置 4 个千兆电口，4 个千兆光口，2 个万兆光接口，冗余电源；配置 6 个扩展槽位，硬盘容量为 4T；产品在《安防设备产品》名录中，符合该项目性能要求的产品。
产品名录情况	产品为《安防设备产品》名录中选取符合该项目性能要求的产品；
产品性能	整机吞吐率为 10Gbps，最大并发连接数为 600 万，每秒新建连接数 6 万
产品功能	1.系统具备庞大的攻击特征库，攻击特征库数量超过 9300 种；
	2.支持针对不同类别告警信息进行配置功能，并可以进行告警测试；

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

	3.具备 IPv4/IPv6 双栈解析能力；
	4.支持自定义规则功能，可以结合用户业务进行深度检测，自定义内容包括源 IP、目的 IP、源端口、目的端口、协议、事件威胁等级、事件类型；
	5.支持对常见的拒绝服务攻击（DOS）的检测能力，针对 TCP FLOOD、UDP FLOOD、ICMP FLOOD、DNS FLOOD 攻击行为进行检测；
	6.支持 DoS 攻击检测功能、僵尸检测功能及爬虫检测功能；
	7.支持在告警详情中自动对命中的 payload 进行高亮显示处理，提升安全研究人员对告警信息的分析效率与准确性，具体高亮内容涵盖基于特征规则触发的告警详情及通过算法分析识别的告警信息；
	8.支持通过多种方式识别网络中的资产信息,识别方式包括：主动探测、被动发现。；
	9.支持发现资产的类型，包括终端、视频设备、办公设备、网络设备、服务器、安全设备、工控设备等；
	10.支持全局白名单配置，白名单覆盖范围包括：告警、威胁情报、病毒检测等，可根据流量源目的 IP、端口以及协议、协议内容等维度进行灵活的全局过滤策略配置。

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦 邮政编码：100193
集团总机：010-82779088 集团传真：010-82779000 售后热线：400-624-3900
售后邮箱：support@venustech.com.cn 启明星辰微信公众号：venustech_weixin
官方微信 官方微博