

天清入侵防御系统 V6.0

(NGIPS5000-FT)

一. 产品简介

天清 NGIPS 是启明星辰公司自行研制开发的入侵防御类安全产品, 基于“智能防御、运维无忧”的核心理念, 对常规的网络流量中的恶意威胁行为进行智能检测并阻止入侵行为, 提供研判分析和协同防护等多种场景化设计, 满足保障网络安全和高效运维的需求。

天清 NGIPS 融入了启明星辰公司在入侵攻击识别方面的积累和研究成果, 使其在攻击识别方面达到国际领先水平, 采用包括多模检测技术和 AI 检测等多种检测技术, 可以对网络蠕虫、间谍软件、木马软件、溢出攻击、数据库攻击、高级威胁攻击、暴力破解等多种深层攻击行为进行主动阻断、策略优化、日常运维、协同防护等特色模块, 可满足各种实施部署和安全运维的场景。

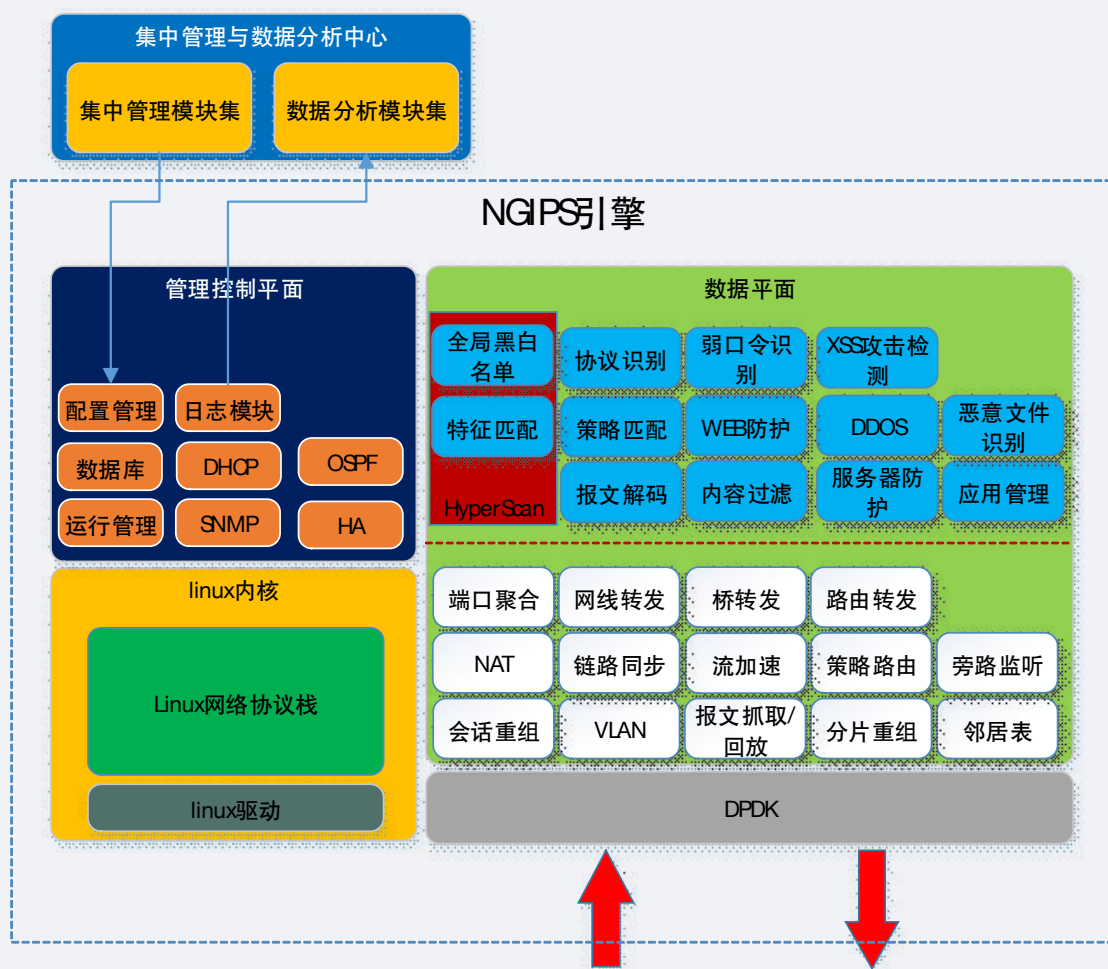
二、产品架构

天清 NGIPS 设备总体软件设计兼顾系统稳定性和运行效率, 采用“检测与控制相分离, 威胁特征相统一”的一体化设计思想, 天清 NGIPS 通过对管理控制平面和数据层面进行分离, 最终形成了以上的天清 NGIPS 软件结构。软件设计的解耦, 有利于提高软件的稳定性和可靠性。

为了实现高性能处理, 转发平面采用高性能报文处理, 利用轮询、零拷贝、核亲和性独占、大页内存、数据批量处理等技术实现了报文的快速转发, 检测平面采用多模匹配技术, 对报文内容的进行高效匹配, 提升检测效率。

集管中心主要包括集中管理和日志分析。集中管理实现对天清 NGIPS 设备的集中管理、升级管理、策略下发和设备监控。日志分析持续收集多台天清 NGIPS 设备发送的各种攻击日志和运维日志, 并进行日志存储、统计分析、研判分析和生产安全报表。





三、产品特点

► 强大的检测技术

天清 NGIPS 系列产品以全面的协议分析为基础，对其进行协议异常检测、流量异常检测、会话关联分析、跨包检测等多种技术，并提供编解码能力，提升抗逃逸检测能力，为客户网络提供全方位深层次多协议的防护。

► 完善的攻击特征库

天清 NGIPS 系列产品采用的攻击特征库，特征数量达到 1.8 万+，覆盖 60+攻击类型，涵盖系统破坏类、获取权限类事件、扫描探测类事件、系统漏洞类事件、信息收集事件等分类。特征库每周升级，并支持紧急响应及升级，实现对已知漏洞和零日攻击的检测和安全防护。





► WEB 防护

面对层出不穷变化多端的 WEB 系统攻击,天清 NGIPS 系列产品提供多种检测能力。攻击扫描阶段支持防爬虫、防漏扫、防 CGI 扫描,并内置 50 多种扫描器特征包括 Acunetix、Appscan、Nessus、Sqlmap、Webinspect、BurpSuite、绿盟极光等。在攻击实施阶段支持 SQL 注入、XSS 注入、系统命令注入、信息泄露、文件上传、系统漏洞、木马、等攻击行为进行检测防护。

► 账号安全

账号安全往往是系统的最薄弱的点,攻击者使用默认口令、密码字典进行穷举很容易获得正确的口令。天清 NGIPS 系统产品提供弱口令检测和暴力破解两种方式保障账号安全,弱口令检测内置自定义字典和多种密码复杂度算法,暴力破解内置了检测时间和阈值同时也支持根据业务情况进行自定义调节。天清 NGIPS 系列产品从流量测发现弱口令提高爆破难度,并支持检测和阻止持续爆破行为。

► 高效的病毒防护能力

天清 NGIPS 系列产品采用了高效的文件扫描技术,能够针对全球热点病毒进行实时检测。每周病毒库更新,实现新型病毒的检测和安全防护。

产品采用启发式防病毒检测技术,基于 3000 万级别的病毒库,对各类病毒(宏病毒、脚本病毒、蠕虫、木马、恶意软件、灰色软件等)实现全方位的检测和扫描,防范恶意软件给网络应用带来的病毒感染风险。

► 便捷的研判分析能力

为了方便安全运维团队进行定位,系统提供了对同一区域、同一源的重复日志的聚合能力,并辅助以流量取证、载荷标记、威胁情报、沙箱分析等上下文信息,为日志做标记、分析、汇总和研判。另外,关联多种日志中还原攻击者的攻击路径,进而通过情报云查技术对攻击者进行画像,方便安全运维人员对攻击进行研判分析。





四、产品规格

产品名称	天清入侵防御系统 V6.0
产品型号	NGIPS5000-FT
机架高度	1U 标准机架式设备
接口	6 个千兆电口, 4 个千兆光口
电源	冗余电源
产品功能	1. 产品使用银河麒麟高级服务器操作系统 V10 (内核版本 4.19)。 2. 系统提供覆盖广泛的攻击特征库, 可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断, 攻击特征库数量至少为 10000 种以上。 3. 系统提供 DoS/DDoS 攻击检测与防护能力, 支持 TCP/UDP/ICMP/ACK Flooding, 以及 UDP/ICMP Smurfing 等常见的 DoS/DDoS 的攻击, 支持设置阈值。 4. 支持基于 SCADA 等工控协议的相关漏洞攻击检测。 5. 系统具备攻击快照功能, 详细记录触发告警的数据特征, 以便做进一步的事件分析。

