

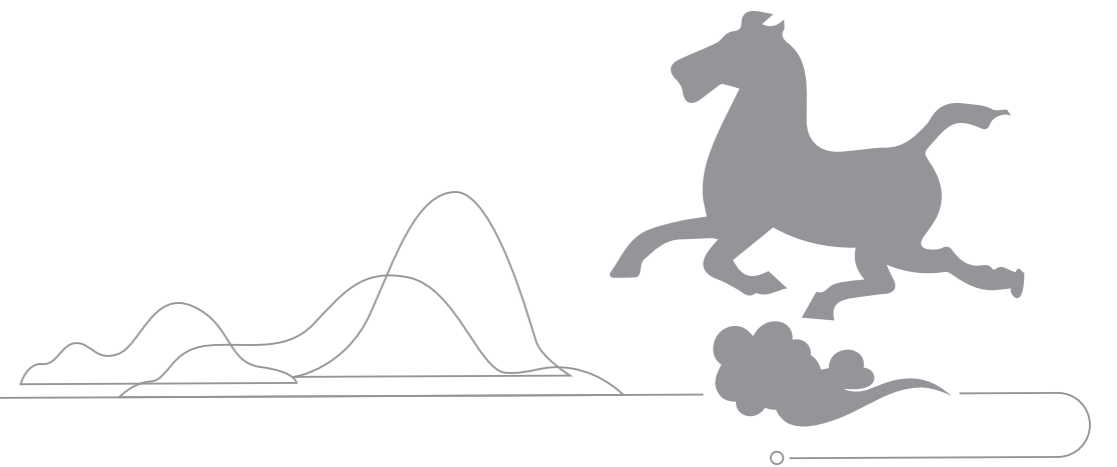
股票代码：002439



启明星辰 天清汉马T系列防火墙



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 电话：010-82779088

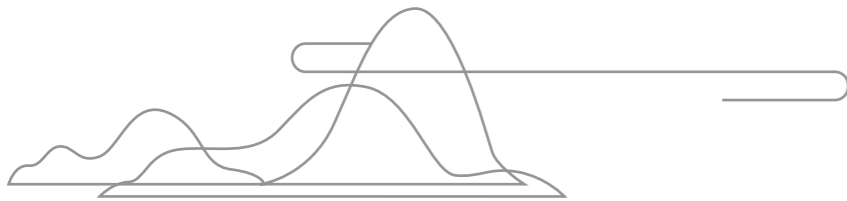


01 概 述 02

02 关键技术 03

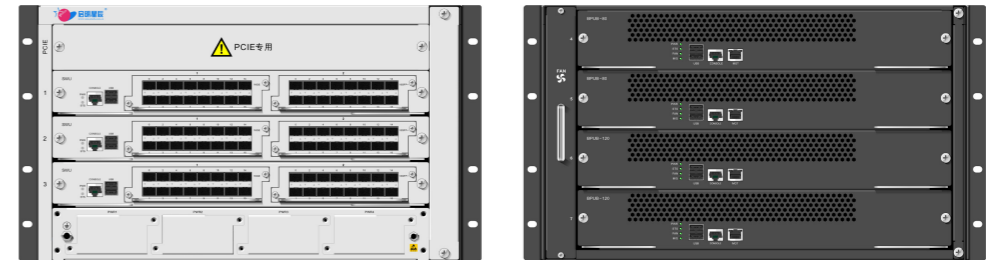
03 产品特点 05

04 产品规格 09



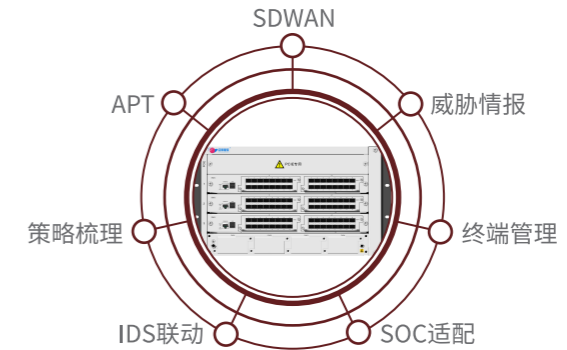
◎ 概述

天清汉马T系列防火墙是启明星辰推出的新一代T比特级高性能防火墙产品。创新性的采用SDN硬件交换和多核CPU业务模块相结合的架构设计,提供最高1.2T的无阻塞数据处理能力。



通过高安全等级的VSOS安全操作系统和高性能应用层流量处理引擎,从业务、用户、应用和行为等多维度出发,重构了安全控制、流量分类、攻击防护、VPN、应用识别、防病毒、入侵防火、行为管理、Web防护、多层嵌套QoS、用户认证等功能。提供用户策略、应用策略和行为策略等智能控制手段真正实现了L4-L7层业务的深度融合,为用户提供高性能、高可靠性的一体化安全防护。

支持与天阗高级持续性威胁检测与管理系统 (APT)、天阗入侵检测与管理系统 (IDS)、Venus Eye威胁情报、Flow Eye安全域流监控系统、天珣内网安全风险管理与审计系统、泰合信息安全运营中心系统 (SOC) 联动,实现更高层次的协同防护。



天清汉马T系列下一代防火墙系统还具备软件定义广域网 (SD-WAN) 功能,实时动态路径选择, WAN优化、动态VPN隧道,数据压缩,端到端QoS的SD-WAN解决方案。满足多种途径,灵活,低成本的广域网连接需求,实现分支机构和移动用户的快速安全接入,可以提供业务所需的可靠性和高效率。

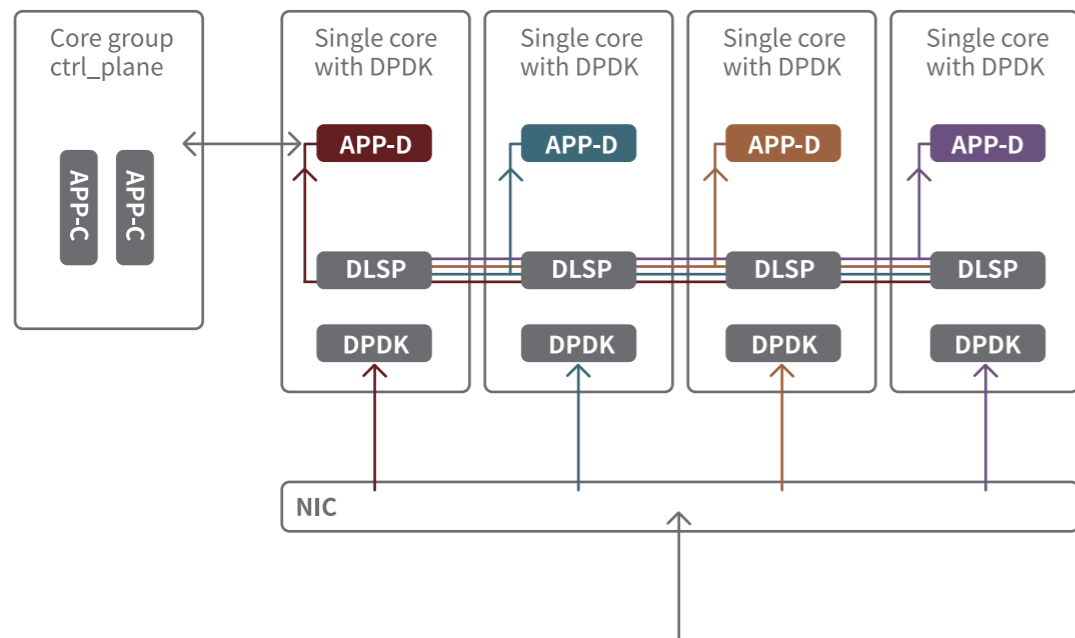
◎ 关键技术

多平面系统架构

启明星辰T系列防火墙在软件架构上采用了控制与业务分离的设计,根据业务类型分为控制面(Control Plane,简称CP)和数据面(Data Plane,简称DP)两部分,CP主要处理鉴权、配置、路由、日志和高可用性等管理业务,并提供WebUI、命令行、云管理平台和SDN API等管理接口。DP则处理网络层、应用层解析和防火墙各项策略的执行。每个CP或DP都与一个逻辑处理器进行绑定,避免由于系统调度对性能产生负面影响。

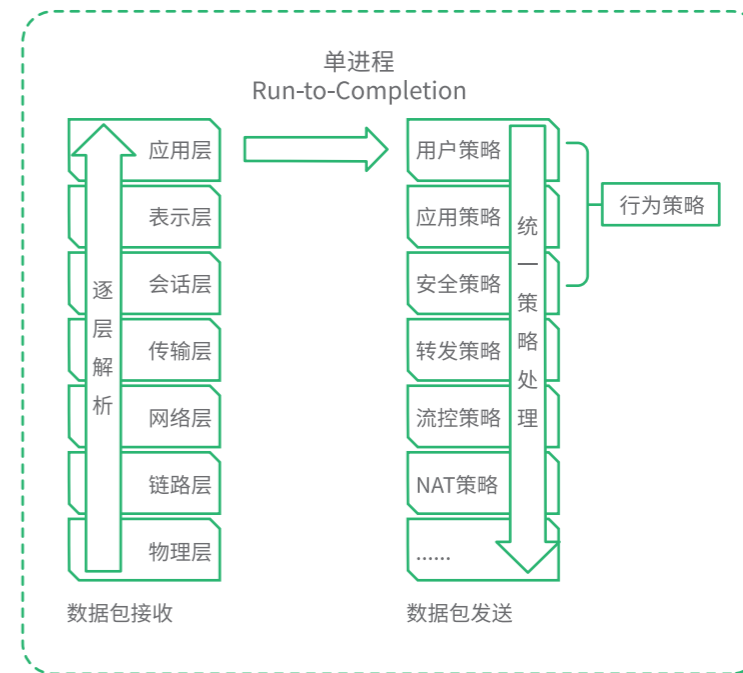
多核并行处理技术

启明星辰采用了独创的双平面动态分流架构对流量进行分配。当数据包到达启明星辰T系列防火墙时,首先由智能分流器对数据包进行初步分类。智能分流器根据当前启用的上层功能以及数据包的网络层、应用层信息,决定将该数据包投递到哪个处理核。智能分流器保证了数据包能在单个处理核上完成所有所需的处理(出于对某些特殊情况的处理,系统仍提供核间报文互操作机制),避免了跨节点访问内存的高昂开销,是保证多核并发性能的关键技术。



一体化报文处理引擎

启明星辰采用了一体化报文处理引擎完成报文的统一解析。引擎首先分析用户配置的各项功能,决定进行哪些分析,随后一次性对二至七层所有需要进行解析的内容进行统一处理,并将结果一并送至策略控制模块。策略控制模块依据这些解析结果,匹配用户配置的策略进行报文的后续处理。



一体化报文处理引擎配合智能分流器,在单个处理核的处理进程上完成从报文接收、报文解析、策略控制、报文发送的所有工作。一次解析,统一处理,避免了多模块、多进程之间的重复工作和报文拷贝。在策略统一处理时,还可基于用户策略、应用策略、安全策略等,进行更高层次的抽象,制定基于基础策略的高级策略。

◎ 产品特色

天清汉马T系列防火墙具备业界最强大的安全控制能力

启明星辰T系列防火墙在软件架构上采用了控制与业务分离的设计,根据业务类型分为控制面(Control Plane,简称CP)和数据面(Data Plane,简称DP)两部分,CP主要处理鉴权、配置、路由、日志和高可用性等管理业务,并提供WebUI、命令行、云管理平台和SDN API等管理接口。DP则处理网络层、应用层解析和防火墙各项策略的执行。每个CP或DP都与一个逻辑处理器进行绑定,避免由于系统调度对性能产生负面影响。

七元组访问控制:

以源地址、目的地址、源端口(源安全域)、目的端口(目的安全域)、服务类型、APP类型及用户为参数的访问许可控制;

七元组会话控制:

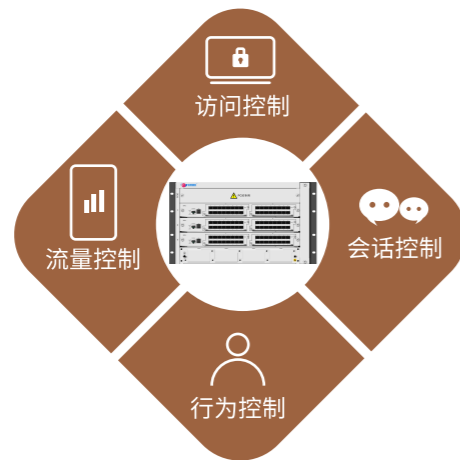
以源地址、目的地址、源端口(源安全域)、服务类型、APP类型及用户为参数的会话许可控制:总新建连接速率/总连接数、每源IP新建连接速率/每源IP总连接数、每目的IP新建连接速率/每目的IP总连接数;

应用行为控制:

深入APP或各类网络协议的细节参数,实现精细的网络行为管理和日志记录;

流量控制:

以源地址、目的地址、服务类型、APP类型及用户为参数的多层管道嵌套式流量及QoS控制。



基于多维度的强安全控制,可以为用户实现强有力的安全控制能力,从而有效提升整体安全防护水平,保障核心业务稳定可靠运行。

同时,天清汉马T系列下一代防火墙支持在各类网络环境中部署,从而在新一代业务环境下实现了防火墙核心价值的有效落地。

入侵防御和病毒过滤

支持领先的入侵防御技术和病毒过滤功能。产品采用了多种专利技术和创新技术,为客户提供最高可达数百G流量的入侵防御及防病毒性能。

超高的性能得益于采用标签的融合式综合匹配技术,在结构上最大限度地融合了存在冗余功能的模块,从而避免了重复的数据还原、分析过程。

应用行为管控

智能应用识别采用基于深度包检测(DPI)、深度流检测(DFI)和网络行为分析(NBA)技术,实现对主流应用的准确识别。

应用控制基于智能应用识别,提供领先的应用行为控制功能,可基于应用的深度信息和内容实现精细化控制。

高级持续威胁(APT)防护

支持与启明星辰天阗高级持续性威胁检测与管理系统(APT)联动

APT采用沙箱检测技术,对未知木马、病毒、恶意代码具有精确的检测效果,实现对未知威胁、高级持续威胁和0DAY攻击的有效防护。

威胁情报云动态防护

支持与启明星辰VenusEYE威胁情报云联动,基于实时更新的威胁情报提供动态安全防护功能。

全面支持IPv6环境下的安全防护

全面支持IPV6/V4双栈环境同时工作,且所有安全防护功能入侵防护、防病毒、应用控制、QoS流控、APT防护、威胁情报防护等均支持双栈环境下使用。

虚拟化防火墙

支持基于Hypervisor技术的底层硬件虚拟化。各虚拟防火墙完全隔离运行,相互无影响,可针对虚拟防火墙独立升级软件版、独立重启,并可实现虚拟防火墙之间的HA部署。

每个虚拟防火墙均提供完整的安全功能,包括防火墙、入侵防御、防病毒、应用行为管理、流控、VPN、IPv4/IPv6双栈等功能。

云防火墙

提供丰富的软件定义接口,可以通过vCenter-PlugIn或者LBaaS-Driver、FWaaS-Driver的方式跟云管理平台进行交互管理,并可适配VMware、KVM等环境,同时支持多种云平台的部署,为南北向流量、东西向流量提供高性能、高可靠、灵活弹性的四七层安全防护。

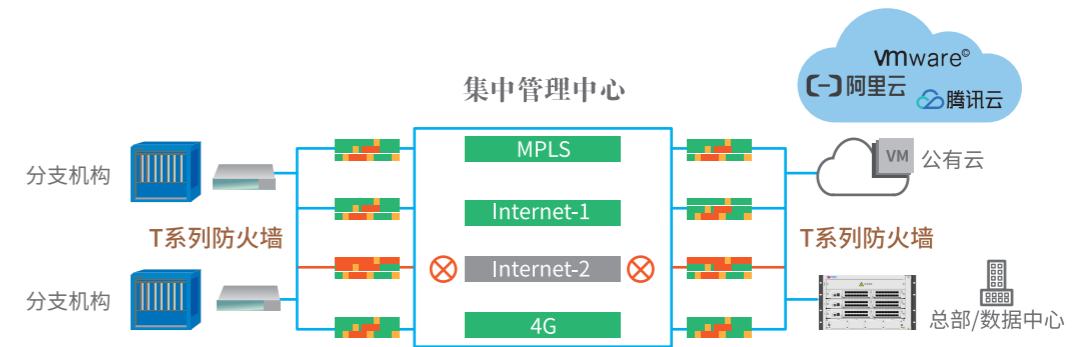
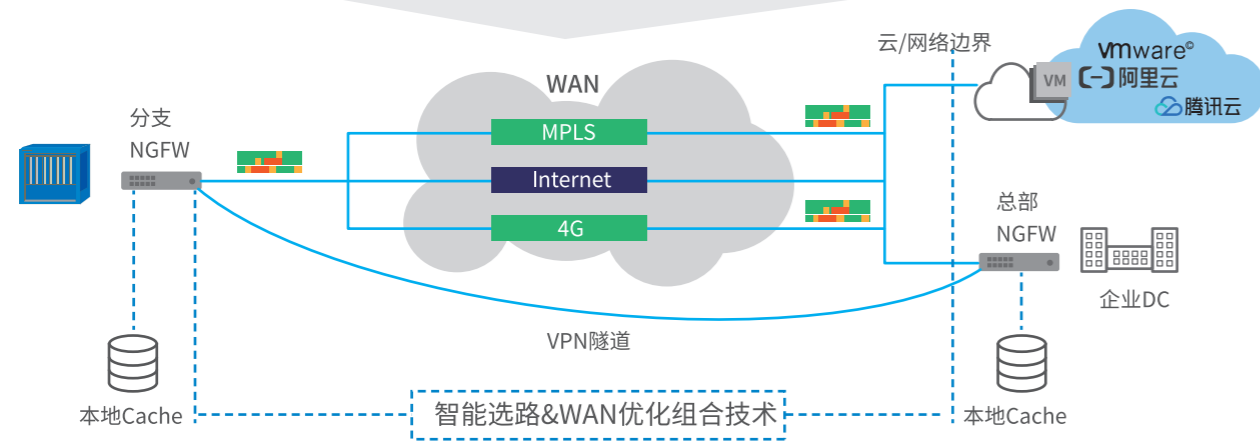
Vcloud云日志

提供防火墙日志云端存储与分析服务,可将防火墙、NAT、系统和安全等日志一键上报至云端,支持微信推送告警,微信报表推送,任意时间地点的日志查询。

软件定义广域网SDWAN

集成了软件定义广域网技术(SDWAN),可实现关键业务的可靠保障、业务加速、应用流量管理、业务一体化安全防护以及简化网络管理。

| 可靠性保障 | 业务加速 | 应用流量管理 | 业务安全防护 | 简化网络管理 |
|--|---|---|---|---|
| <ul style="list-style-type: none"> 智能路径选择 业务无丢包切换 关键业务流量复制 链路质量实时监控,丢包/延迟/抖动 | <ul style="list-style-type: none"> 双边业务加速 本地数据缓存 WAN数据压缩 视频传输优化 | <ul style="list-style-type: none"> 应用协议可视化 应用流量限速 动态带宽保障 应用行为管理 | <ul style="list-style-type: none"> 业务动态发布 应用控制 APT攻击联动 WEB安全防护 SSL VPN | <ul style="list-style-type: none"> 集中认证授权下发 集中配置自动下发 动态VPN组网 设备状态监控 |



国内独有的SDWAN+NGFW一体化融合解决方案,面向总部/省级/地市/县乡等政府部门纵向内网和大型企业内部生产环境

SDWAN特性包括:

多链路负载/基于链路质量的自动选路/关键业务多链路复制/数据压缩/TCP双边加速等。常见业务加速2倍-20倍。

专线组网用户:

大幅提升业务使用体验、提升业务可靠性、完整安全特性,如视频会议

互联网组网用户:

媲美专线效果大幅节省经费/VPN加密/完整安全特性

