

天融信NGFW®下一代防火墙

www.topsec.com.cn

产品概述

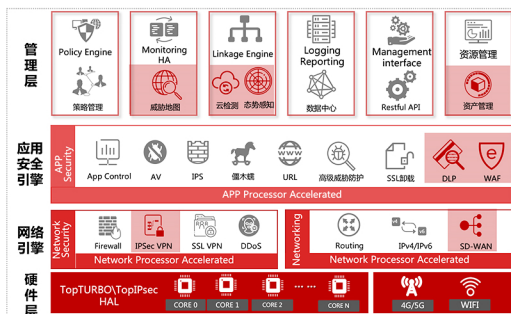
在以“云、大、物、移、智”等新兴技术为代表的变革时代，网络安全不断面临新的威胁与挑战。天融信作为国内网络安全行业的领军企业，凭借20多年的安全研发积累与安全服务经验，从客户所面临的实际需求出发，针对新的应用模式和安全威胁，适时推出基于NGTOS系统的天融信NGFW®下一代防火墙系列产品。



产品特点

高性能处理架构

天融信NGFW®下一代防火墙采用自主研发的64位多核多平台并行安全操作系统NGTOS，拥有优秀的模块化架构设计，在系统上层引擎的设计中，采用了特有的用户态协议栈，能够充分利用多核CPU的计算资源，完美支持多路多核的全功能并行业务处理。同时，NGTOS系统通过采用基于多元组的一体化流检测机制，保证天融信NGFW®下一代防火墙在处理复杂网络流量和安全业务时能够具备快速高效的处理能力。

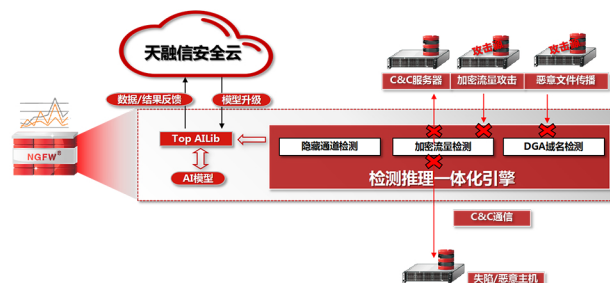


深度识别管控

天融信NGFW®下一代防火墙的应用识别引擎综合运用单包特征识别、多包特征识别、统计特征识别等多种识别方式进行细粒度、深层次应用和协议识别，同时采用多层匹配模式与多级过滤架构及基于专利的加密流量识别方法，实现对应用层协议和应用程序的精准识别。

高级威胁深度防御

高级威胁攻击通常使用先进的攻击手段对特定目标进行长期持续性的网络攻击，具有长期经营与策划、高度隐蔽等特性。天融信NGFW®下一代防火墙内置多种高级威胁攻击防御解决手段，包括基于AI的高级威胁检测、基于行为分析的异常威胁检测和基于联动的未知威胁检测，打破高级威胁攻击隐蔽性和持续性这两个特性，斩断其“攻击链条”，多方位对高级威胁进行深度检测防御，有效阻止高级威胁攻击。



IPv4/IPv6双栈

天融信NGFW®下一代防火墙支持完整的IPv4/IPv6协议栈，通过对IPv4/IPv6全面的协议特性的支持并且融合下一代安全防护能力，为各种IPv4/IPv6应用提供支撑，帮助客户轻松应对IPv4及IPv6环境下的多种威胁。同时，可提供全面的业务安全防护，包括基于IPv6的应用层检测(FTP/TFTP)、病毒过滤、URL过滤、ADS、IPS、WAF等功能。

安全可视化

天融信NGFW®下一代防火墙具有专门的监控和数据中心功能模块，管理员通过监控面板可以快速地查看设备的流量统计信息以及了解设备的运行情况。管理员可以查看设备、接口、应用、用户、服务器等网络对象的运行状态、流量统计信息、安全威胁信息等。

全域感知协同防护

当前任何单一的网络安全产品都不可能解决所有安全问题。网络安全防护的有效性需要多种安全产品进行联动，融合各自的安全能力，补足单体的不足。天融信NGFW®下一代防火墙通过协同机制，联动终端和网端，调动网内IDS、APT、EDR、DLP等安全产品的检测能力，实现全局预警、协同防护、自动处置，为客户构建由单点向全域，由静态到动态的主动化纵深防御体系。

智能管理安全运维

为了便于客户掌握网络中安全情况以及降低运维管理工作量，天融信NGFW®下一代防火墙提供了智能运维管理的一系列工具，包括安全监控、数据中心、安全中心、安全策略管理、集中管理、第三方管理接口等，便于管理员梳理IT资产对网络整体运行情况统计分析，同时降低安全运维工作量，维护安全策略一致性。



威胁地图与攻击溯源

天融信NGFW®下一代防火墙能根据IP地址数据库，展示各个地理位置威胁地图，也可以根据地理位置设置不同的访问控制策略。天融信NGFW®下一代防火墙提供对威胁的全方位可视化，其中包括攻击者维度，受害者维度，事件维度等多维度多视角的展示：通过对攻击者从地理信息、IP地址、攻击统计信息对攻击者进行肖像刻画；通过对受害者资产属性分析对受害者进行画像；通过对攻击类型及过程和时间等元素分析，对攻击过程进行全视角的分析和刻画，让攻击威胁无处遁形，全方位可视。天融信NGFW®下一代防火墙支持攻击溯源，持续性威胁感知，并可针对攻击源头进行有效阻断，能大幅降低安全事件对用户资产的影响。快速推送告警事件，协助用户第一时间响应处置，助安全一臂之力。

典型应用

企业网边界

- 为用户提供整网安全的第一道防线，在网络关键位置建立安全控制点。
- 通过多维的访问控制和安全防护能力，对各安全域之间通信流量执行深度威胁检测，实时阻断病毒、蠕虫、木马等众多已知威胁，提供边界综合安全防护能力，阻止威胁蔓延。
- 利用AI技术检测DGA域名、隐蔽通道、恶意加密流量等威胁，阻断高级威胁攻击。
- 通过与用户网络内的IDS、APT、EDR等多种产品联动，实现安全设备间协同防护，构建全域安全防护体系基础，提升整网安全有效性。

