天融信NGFW®下一代防火墙

www.topsec.com.cn

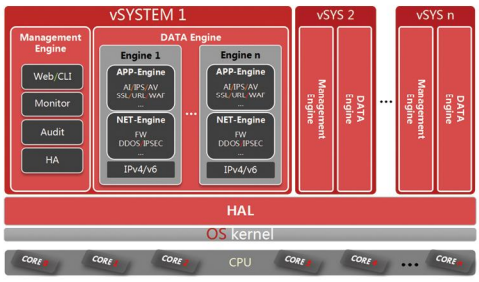
产品概述

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。



IPv4/IPv6双栈

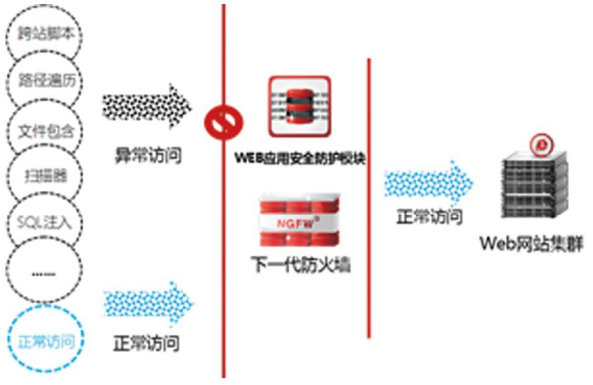
天融信NGFW®下一代防火墙支持完整的IPv4/IPv6协议栈，通过对IPv4/IPv6全面的协议特性的支持并且融合下一代安全防护能力，为各种IPv4/IPv6应用提供支撑，帮助客户轻松应对IPv4及IPv6环境下的多种威胁。同时，可提供全面的业务安全防护，包括基于IPv6的应用层检测（FTP\TFTP）、病毒过滤、URL过滤、ADS、IPS、WAF等功能

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。

WEB应用防护

天融信NGFW®下一代防火墙内置千余条Web应用安全规则库，可提供Web应用攻击防护、支持XSS注入、SQL注入、网站防扫描等功能，能够有效抵御针对Web应用的攻击而导致的网站敏感信息泄露、网站服务器被控制等事件的发生。

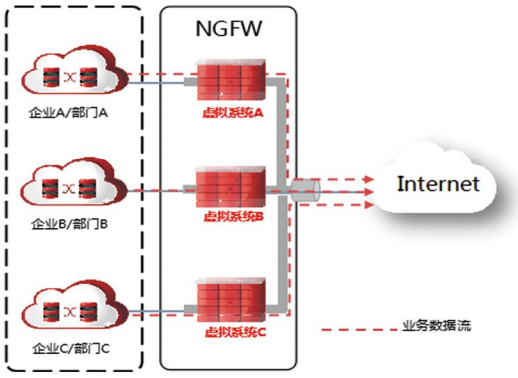


未知威胁防御

天融信NGFW®下一代防火墙支持通过异常行为分析和APT联动实现未知威胁防御。异常行为分析模块利用内置的智能统计学习算法，基于业务数据统计分析，构建一定周期内的正常业务基线，通过与实时数据比对分析，发现异常并及时告警。同时，通过与APT设备进行联动，发现隐匿的高级威胁并及时阻断。

安全资源虚拟化

天融信NGFW®下一代防火墙支持1：N虚拟化，具备网络虚拟化、安全虚拟化、系统虚拟化、管理虚拟化特性，可以为每个虚系统分配独立的安全资源，包括对象资源、安全策略、应用识别、病毒防御、入侵防御、URL分类过滤、内容过滤、审计报表等，从而确保客户组网更弹性、策略更清晰、管理更明确。

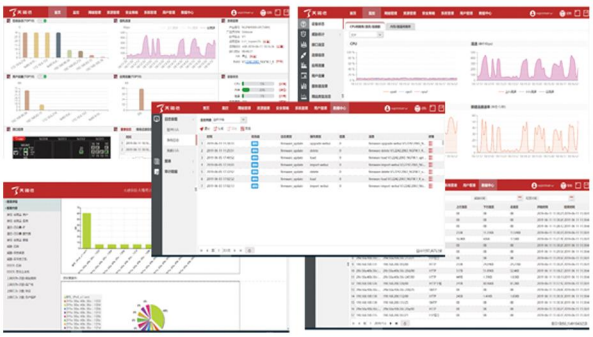


异常流量防护

天融信NGFW®下一代防火墙内置流量检测防御引擎，支持基于IP、ICMP、TCP、UDP、DNS、HTTP、NTP等众多协议类型的防护策略，能够检测与防御流量型DDoS攻击、应用型DDoS攻击、非法协议攻击等拒绝服务攻击。采用多种防御机制，通过流量业务预警、比例抽样分析、源认证、源限速、协议分析、模式过滤、业务应用防护、强制保护等多种技术手段，精准、快速地阻断攻击流量，保障客户业务网络通畅。

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。



典型应用

企业网边界

- 部署在企业互联网边界，配置防火墙访问控制功能，在网络关键位置建立安全控制点，对非法访问进行控制。
- 通过配置多维的访问控制和安全防护策略，对各安全域之间通信流量执行深度威胁检测，实时阻断众多安全威胁，提供边界综合安全防护能力，阻止威胁蔓延。
- 基于安全域、IP、用户、应用、时间建立Qos策略，保障关键核心业务优先处理。
- 通过数据过滤和文件过滤功能，保障企业关键信息不被泄露。