网康科技
NETENTSEC

下一代防火墙NGFW

——全面应对新兴威胁的高性能应用层防火墙

下一代防火墙（NGFW）是网康科技推出的一款可全面应对新兴威胁的高性能应用层防火墙。凭借超强的应用识别能力，NGFW可深入洞察网络流量中的用户、应用和内容，借助全新的高性能单路径异构并行处理引擎，为用户提供高效的应用层一体化安全防护，帮助用户安全地开展业务并降低安全成本。

功能特性

完备的
基本防火墙特性

- 支持基于五元组（源地址、目的地址、源端口、目的端口、协议类型）的访问控制。
- 可全面防护扫描探查、Flood、DDoS及异常数据包等网络攻击。
- 支持源、目的地址转换，静态路由、动态路由协议、虚拟专用网（VPN）、高可靠性（HA）、应用层网关（ALG）等。
- 支持多链路负载均衡、运营商路由优选及应用引流功能，可有效优化链路负载，提升用户访问体验。

全方位
应用洞察与控制

- 精确识别流行的网络应用、移动应用，支持丰富的用户识别及认证技术，可对URL进行分类控制。
- 实现用户+应用+内容+时间的多维精细化访问控制，增强安全策略有效性。
- 基于用户+应用+时间保障核心业务的基础带宽，限制非关键业务最大带宽，避免网络拥塞，大幅提升网络可用性。

一体化
应用层威胁防护

- 基于应用协议识别的入侵防御功能，提供针对漏洞、后门进行的木马、蠕虫、缓冲区溢出、扫描、SQL注入及恶意软件等入侵行为的检测和防御。
- 基于云、本地双引擎查杀的病毒防护，支持对常用协议流量和压缩文件中的病毒进行查杀。
- 基于应用的一体化安全策略，给用户带来了全面的安全防护和简单、灵活的安全策略配置。

智能化
主动防御

- 根据应用的漏洞存在、技术特点和被威胁利用的可能性，对应用进行安全风险赋值和分类。
- 支持根据国家和地区提供网络流量和威胁统计的分布图，实现对去往和来源于不同国家和地区的流量和威胁的可视化。
- 支持用户、应用、威胁等维度的数据对比，以基线形式对比前一天、前一周或前一个月相同时段的应用和威胁情况。
- 支持安全事件集成关联分析，为用户提供相关数据的广泛关联、深度挖掘和直观呈现，进而协助用户快速溯源安全事件并及时预警潜在威胁。
- 可根据常见的行为特征，判别网络中可疑的僵尸主机并进行告警，同时根据行为特征符合度提供“置信值”帮助管理者及时发现僵尸网络。

咨询热线：400-678-3600　网康官网：www.netentsec.com　网康科技　地址：北京市海淀区中关村东路66号世纪科贸大厦A座3层（100190）

网关级 数据防泄漏

- 用户可通过正则表达式灵活定义文件内容特征，并及时阻断匹配特征的文件传输流量。
- 用户可对指定类型的文件传输进行阻断，基于内容识别文件类型，有效规避修改扩展名逃逸检查的风险。

低衰减、高性能

- 采用单路径处理引擎，数据包仅需一次拆解即可实现应用类型、木马、病毒、间谍软件、恶意网址等威胁特征的一次性匹配，大幅提升威胁检测效率，降低性能衰减。
- 基于Intel高性能硬件平台和DPDK软件技术，通过异构并行架构，提供高性能网络转发及应用、内容的并行处理，保证全功能开启后的高性能。

全网集中管理

- 可通过安全管理中心（Security Management Center，简称SMC），实现最多2000台下一代防火墙设备的集中管理。
- 可实现全网设备的配置下发，监控全网状态并及时预警风险。

技术规格

功能规格	
组网功能	ARP绑定、ARP代理、DNS、DDNS、PPPoE、DHCP、静态路由、RIP、OSPF、网口联动、多链路负载均衡、链路备份
VPN	IPSec VPN、SSL VPN、L2tp VPN
应用控制	中国最大应用识别库，识别3000余种网络应用，700余种移动应用及主流移动终端系统
攻击防护	IP Sweep、Port Scan、SYN Flood、ICMP Flood、UDP Flood、TearDrop、LAND、WinNuke、Smurf、Fraggle及Ping Of Death等
入侵防御	5600余种漏洞攻击防护及4000余种间谍软件防护
病毒防护	云端、本地双引擎可选，支持对HTTP、FTP、SMTP、POP3和IMAP协议流量，及gzip，zip，rar等压缩文件进行病毒查杀
URL过滤	全球最大中文网页分类库，收录3000余万条URL分类信息，可对URL进行分类控制
数据防泄漏	300余种文件传输应用的文件类型（共支持66类文件）及内容（共支持11类文件）过滤
主动防御	基于行为分析技术定位僵尸主机，利用应用威胁可视、安全基线对比和集成关联分析技术预警网络中的潜在风险
带宽管理	支持多级通道、虚拟线路、基于用户、应用类型、时间段的流量控制和保障
用户管理	支持30余种身份识别技术，可通过IP、MAC、用户名、密码等方式透明识别用户，并且与RADIUS、AD、LDAP、POP3、SMTP、城市热点、深澜身份认证等系统进行联动
	支持触发式Web认证、LDAP、Radius、POP3、IP/MAC绑定认证
	支持AD、CAMS、SAM、PPPoE单点登录，多点登录、用户有效期、页面跳转等
管理方式	Web界面（支持主流浏览器、Https加密传输）/命令行界面（SSH/Console）
部署方式	透明模式/网关模式/旁路镜像/混合模式（透明+网关）

产品订购

为保障用户安全投资的合理性，帮助更多用户的网络迅速处于NGFW的保护之下，网康科技为用户提供了“服务”、“设备”两种订购模式，用户可根据自身特点灵活选择其一订购。

	服务模式	设备模式
型　号	NF-S320/S360/S380系列	NF-1000/3000/5000系列
订购项目	用户按年（一年、二年、三年可选）订购安全服务 网康免费提供NGFW硬件平台	用户订购NGFW硬件平台，并按年订购（一年、二年、三年可选） 安全特征库升级服务
用户权益	**功能激活（服务期内）** 病毒防护、入侵防御、URL过滤 **更新升级** 软件版本、病毒特征库、漏洞特征库、恶意软件特征库、URL分类库、应用识别库升级 **原厂支持** 5*8远程支持、设备硬件质保	**功能激活（永久激活）** 病毒防护、入侵防御、URL过滤 **更新升级** 软件版本、病毒特征库、漏洞特征库、恶意软件特征库、URL分类库、应用识别库升级 **原厂支持** 5*8远程支持、设备硬件质保
服务终止	NGFW硬件平台不回收，病毒防护、入侵防御、URL过滤、SSL VPN功能失效，仅保留基本功能 软件版本、病毒特征库、漏洞特征库、恶意软件特征库、URL分类库、应用识别库停止升级 原厂技术支持服务终止	NGFW所有功能可继续使用 软件版本、病毒特征库、漏洞特征库、恶意软件特征库、URL分类库、应用识别库停止升级 原厂技术支持服务终止