东软 FW5800-F1006

产品概述

东软 NetEye 集成安全网关（NISG）系列产品，是面向应用的智能化第二代防火墙。NISG 具备精细的应用识别与控制能力和智能化的带宽管控技术，能够有效管理上网行为，优化用户网络带宽资源，保障用户业务的安全。通过全方位一体化的多项尖端安全技术，NISG 可以抵御二层到七层的网络攻击，降低敏感信息泄露的风险，为用户网络排除“内忧外患”。

产品亮点

全方位、一体化安全防护，阻断更多威胁

• 一机多能，集传统防火墙功能与多种安全功能于一身，简化部署，减少投资。
• 全面抵御二至七层攻击威胁，保证关键业务安全。
• 特征库自动升级，防范最新漏洞、蠕虫和垃圾邮件等威胁。

精细的上网行为管控，大大提升工作效率

• 细粒度的应用识别与管控，严格控制与工作无关的应用流量，提高工作效率，防止信息泄露。
• 海量的 URL 识别与过滤，有效屏蔽风险网站，遵从法律法规。
• 多维度实施精准带宽控制，保障关键业务的可用带宽。

云安全中心智能联动，有效应对未知威胁

• 将可疑流量上传给云安全中心进行深度检测，可提高对未知威胁的检测能力。
• 将检测结果上传给云安全中心，云安全中心通过大数据和人工智能技术，快速形成信誉库和威胁特征库，统一下发给各安全网关，提升其安全检测能力。

高性能，提升用户访问体验

•高速数据处理性能，同时容纳大规模在线用户与应用连接；
•顶级安全检测防护能力，迅速识别阻断攻击威胁。

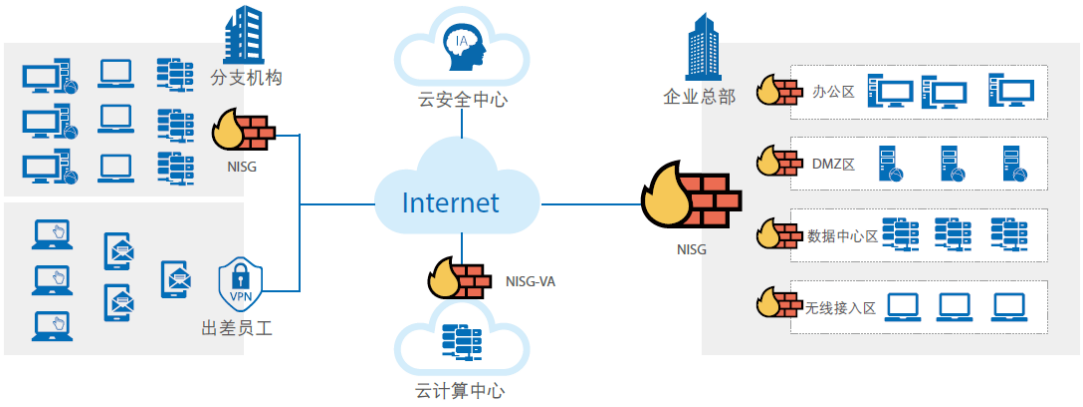
稳定可靠，保障业务持续性

• 软硬件结合的强大灾备处理能力，出现故障瞬间切换流量，提升网络健壮性，保障业务连续性。

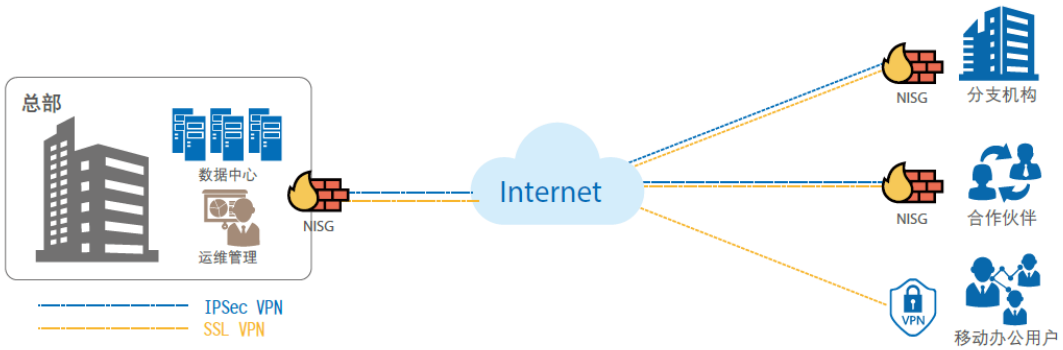
易用，提升安全管理效率

• 智能化的配置管理功能，直观的监控报表界面，配套方便易用的管理工具，大大提升管理效率。

应用场景 1



应用场景 2



主要功能特性

基本功能	接入模式	必须支持 NAT / 透明、路由、混合、三种工作模式
	多链路负载均衡	必须支持基于源、基于源和目的等多种负载均衡模式
	VPN 支持	必须支持 IPSec，IPSec VPN、SSL VPN、L2TP VPN
	路由协议	OSPF、BGP 和 RIPv1/v2（动态路由协议非透传）支持策略路由、支持 ISP 路由并内置多运营商路由表
		必须支持 IPv4 和 IPv6 的静态路由
		必须支持基于角色、用户、用户组的策略路由
	NAT 功能	要求必须支持多对多的 NAT，且公网地址池可选择逐一使用和同时使用两种模式
		支持对公开网络地址各区域（Public、Private、DMZ）的静态 NAT，基于端口的静态 NAT，基于安全策略的对源，目的与端口的 NAT 映射，基于用户身份认证的 NAT 策略；双向网络地址 NAT；可以支持 NAT/PAT
	IPv6	必须支持基于 IPv6 邻居发现协议（ND）的攻击防护，包括地址欺骗攻击、路由通告欺骗攻击及泛洪攻击等
		必须支持 IPv6 与 IPv4 的网络地址与协议转换技术:NAT64 和 DNS64

访问控制	抗 DDoS 攻击	必须支持抵御所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、Winnuke
	会话控制	必须支持会话控制功能，要求能够基于源、目的、应用协议三种条件做会话数限制
		必须支持会话控制功能，要求能够限制会话新建速率
	访问控制	支持按照应用、时间、用户帐号、IP 地址、服务端口、物理端口等方式对数据进行访问控制
	用户认证	支持本地数据库，并可通过 LDAP、Radius 和 Windows AD 域联动。
	双因素认证	可通过 Token 方式实现双因素认证。Token 需要同时支持硬件和软件形式，实现一次性口令认证，软件需支持安卓和 iOS 系统。
URL 过滤	网页过滤	可自定义某种过滤类别或某些 URL 允许访问的时间、字节数等配额限制，配额控制要求基于每源 IP 实现
	网页关键字定义	支持自定义 URL 地；支持 URL 地址/域名黑白名单址，域名过滤；支持基本于分值的网页关键词阻断规则；
AntiSpam 功能	反垃圾邮件功能	支持反垃圾邮件功能，能够识别并过滤垃圾邮件。支持 IMAP，POP3，SMTP 等协议的检测，并能够对垃圾邮件进行标记。且垃圾邮件相关的特征库可以实时在线更新。
IPS 功能	入侵防御系统	针对入侵攻击，支持在线（IPS）或旁路（IDS）方式部署。且 IPS 特征库不少于 10000 条。且支持 IPS 特征自定义功能，IPS 特征库支持实时在线更新。
AntiVirus 功能	反病毒功能	能够针对 HTTP、SMTP、POP3、IMAP、MAPI、FTP 等协议的文件进行病毒/恶意软件的检测及阻断。且病毒特征库能够实时在线更新。
网络应用识别	应用流量可视化	可按照应用分类进行流量监控并提供实时的图形化监控报表
	攻击防护	抗 DDOS 攻击：必须支持抵御下所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、WinNuke
IPSec VPN	互通性	严格遵循 RFC 国际标准，必须支持的算法有 DES、3DES、AES128、AES192、AES256，SHA-256、SHA-512 等
	快速部署	支持 IPSec 和 SSL VPN 的统一集成，还需支持 PPTP、L2TP 等 VPN 方式，以适应点对点、移动用户等多种接入场景
	User Peer	最少支持 50000 个 User peer
	VPN 高级功能	在 Hub-Spoke VPN 组网模式下支持 ADVPN(自动发现 VPN)功能
无线控制器	无线扩展	支持无线控制器功能，在需要时只需购买同品牌 AP 产品，即可实现无线覆盖。
交换机控制器	有线扩展	支持管理交换机功能，在需要时可以直接管理同品牌的交换机产品。

虚拟化功能	虚拟系统支持	支持虚拟系统功能，虚拟系统的主要功能和物理机一致，且支持的虚拟系统不少于 10 个。
系统监控	系统监控告警	支持监控设备系统资源的实时状况，必须包括 CPU、内存、接口带宽、日志容量等对象，支持 SNMP Traps 告警。
系统管理	系统管理接口	提供 Web 管理配置，通过 Web 管理不需要使用硬件密钥或软件的客户端。支持 Telnet/SSH 命令行管理。
	系统管理界面编排	支持防火墙管理界面自定义，比如隐藏不需要的功能项目，常用功能项目在页面自定义排序和组合方式
	系统分权管理	设备本身支持管理权限分级（大于 5 级：管理员、一般管理员、节点监控人员、远程协助、特殊应用保留）

指标参数 FW5800-F1006	
接口	2x GE SFP+ 16x GE SFP 18x GE RJ45
防火墙吞吐量	52Gbps
包转发率（64 字节）	49.5Mpps
最大并发会话数	1100 万
每秒新建会话数	36 万
IPSec VPN 吞吐量	27Gbps
IPSec VPN 隧道数	10 万
SSL VPN 吞吐量	6Gbps
VPN User peer	≥60000
SSL 并发用户数	10000
IPS 特征库	≥10000
Vdom 虚拟墙	≥10，最多可以扩展 250 个
NGFW（下一代防火墙）吞吐量	6Gbps
IPS 吞吐量	6.2Gbps
电源	100－240V AC，50－60Hz，标配冗余双电源
外观	2U
尺寸（H × W × L，mm）	89× 437 × 456