Neusoft

- Intelligent Protection
- Network Interconnection
- Safe & Reliable

NISG 9000X

Intelligent NGFW for Medium & Large-Scale Enterprises

Intelligent NGFW for Medium & Large-Scale Enterprises

NISG 9000X Security Gateway is a high-performance, intelligent next-generation firewall (NGFW). Featuring a modular design, it integrates multiple cutting-edge security technologies—including firewall, VPN, DoS/DDoS protection, IPS, anti-virus, anti-spam, URL filtering, application protocol identification and control, and cloud-based threat detection. It also fully supports IPv6, delivering an industry-leading, all-in-one security solution.

NISG 9000X Key Features

Integrated Threat Defense & Uninterrupted Business

Powered by Neusoft's patented NEL engine, it provides end-to-end protection from the network to the application layer.

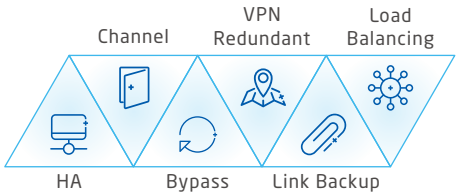
With 9,000+ signatures, it blocks XSS, SQL injection, and Dos/DDos attacks.
Real-time detection optimizes performance while integrating IPS and antivirus for complete security.

Robust Disaster Recovery

Software: Supports HA, VPN redundancy, and link failover to ensure business continuity.

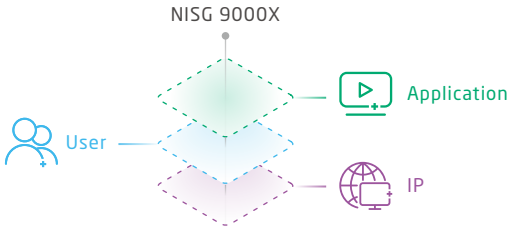
Hardware: Dual power supplies and hardware bypass ensure uninterrupted data services during failures.

Key Features: High Availability (HA) , VPN Redundancy , Load Balancing , Hardware Bypass , Link Failover.



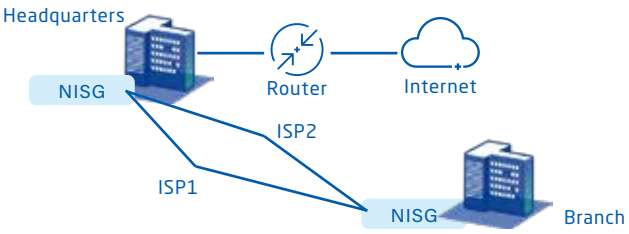
Comprehensive Intelligent Security Capability

- Role-based Intelligent Application Control.
- Multi-Layer Traffic Shaping for Critical Applications.
- Supports Local Database, RADIUS, Web, LDAP, and eDirectory authentication, enabling flexible identity verification and precise access control to ensure secure and compliant network access.



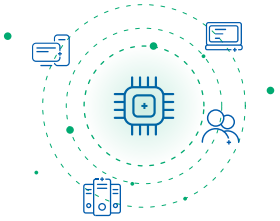
Secure SD-WAN

Intelligent link monitoring and automatic path switching, based on application recognition, minimize delays and packet loss, enhance user experience, and reduce TCO.



Powerful VPN Interconnection Capabilities

NISG 9000X offers high-performance, enterprise-grade VPN features, including IPSec VPN, SSL VPN, and GRE VPN. These features enable reliable and secure connections between data centers, branch offices, and remote users, ensuring safe data transmission during remote interconnections, ensuring safe data transmission during remote interconnections



Protection for Industrial Scenarios

Tailored for industrial environments, NISG 9000X accurately parses key protocols such as Modbus and S7.

It detects abnormal commands and attacks, blocks threats, and ensures industrial control network stability without disrupting production—delivering a solid security barrier.

Comprehensive Audit & Visualization

Provides real-time logging, monitoring, and customizable reports with visualized audit data, enabling administrators to gain clear insights into security posture, track threats, and support compliance requirements with ease.

NISG 9000X Feature Lists

Operating Modes
- Transparent Mode
- Routing/NAT Mode
- Hybrid Mode
- Bypass Mode
- Virtual Wire

Network
- Trunk
- Channel
- VLAN (Maximum 4096)
- STP/RSTP
- DHCP Snooping
- Security Zone
- Dynamic DNS (DDNS)
- BFD Detection

Application Layer Gateway
- Dynamic Ports: FTP, TFTP, SIP, H.323, RTSP, Oracle, Tuxedo, etc.
- DNS ALG

Routing
- Static Routing (with BFD Detection)
- Dynamic Routing (RIP/OSPF/BGP)
- Policy-Based Routing (PBR)
- Link Load Balancing
- Intelligent ISP Routing

Firewall
- Access Policy
- Multicast Policy
- Session Policy
- Auto Detection of IP/MAC Binding
- DHCP Association with IP/MAC Binding
- Session Timeout
- Policy Hit Analysis
- Policy Redundancy Analysis
- Policy Conflict Detection
- Intelligent Policy Self-Learning

Address Translation
- Destination Network Address Translation
- Source Network Address Translation
- Port Address Translation (PAT)
- Policy-Based NAT/PAT
- NAT-Based Server Load Balancing
- IP/Group IP Mapping

Application Security
- Intrusion Prevention System
- Antivirus
- Mail Security
- URL Filtering
- Malicious Code Protection
- Web Protection
- Data Leakage Prevention
- Content Filtering
- SSL Inspection

Secure SD-WAN

- Intelligent Path Selection
- Link Quality Monitoring
- Link Quality Optimization
- Intelligent Link Switching
- Flexible branch interconnection

QoS

- QoS by User,IP,Service , Application, and Time
- Bidirectional QoS and Reverse QoS

VPN

- IPSec VPN
- Routing-Based VPN
- Policy-Based VPN
- Resource-Based VPN
- IKEv2 Remote Access VPN
- L2TP over IPSec
- Gateway-to-Gateway VPN
- IPSec NAT Traversal (NAT-T)
- Dead Peer Detection (DPD)
- Perfect Forward Secrecy
- Anti-Replay Attack Protection
- Domain-Based VPN
- Multiple SAs
- Reverse Routing
- VPN Group
- IKEv1/v2
- SSL Tunnel VPN
- GRE Tunnel (Generic Routing Encapsulation Tunnel)
- Certificate, CA Center
- VPN Client
- Support for IPv6
- VPN Xauth Authentication
- Multi-System Support(Windows、Mac、Android、IOS)

Authentication

- Local Database Authentication
- User Limit of Built-in Database
- RADIUS Authentication
- Web Authentication
- LDAP Authentication
- eDirectory Authentication

Application Identification and Control

- Social Communication Applications
- Business Applications
- Multimedia Applications
- Network Construction Applications
- General Internet Applications
- Browser-Based Applications
- Client-Server Applications
- Peer-to-Peer (P2P) Applications
- Network Protocol Applications
- Custom Applications

Virtual System

- Maximum Virtual System
- Maximum Zone
- Logical Interface Allocation

High Availability

- Dual-Machine Hot Standby
- Active-Standby / Active-Active Mode
- Ethernet Channel / Redundant Interface
- Configuration Synchronization
- Firewall/VPN Session Synchronization
- Device Failure Detection
- Link Failure Detection
- HA Traffic Encryption
- New Member Authentication
- Hardware Bypass
- Redundant Power Supply
- Transparent Mode HA

Logging/Monitoring

- E-mail
- Syslog
- SNMP (v1/v2c/v3)
- SNMP Trap
- SNMP MIB Customization
- Route Tracing
- VPN Tunnel Monitoring
- Session Table Monitoring
- Resource Monitoring
- Network Status Monitoring

Multicast

- RPF (Reverse Path Forwarding)
- IGMP V1, V2 (Internet Group Management Protocol)
- IGMP Snooping
- DVMRP (Distance Vector Multicast Routing Protocol)
- MLDv2 (Multicast Listener Discovery Version 2)

Attack Defense

- ARP Attack Defense
- DoS/DDoS Attack Defense
- Network Attack Defense
- Probing Attack Defense
- Packet Fragmentation Attack Defense
- SYN Attack Defense
- Malformed Packet Attack Defense
- IP Spoofing Attack Defense
- DNS Flood Attack Defense

System Management

- Separation of Administrative , Security,and Audit Functions
- Two-Factor Authentication
- System Upgrade/UTM Libray Upgrade (Automatic/Manual)
- Logging & Auditing
- Automatic Configuration Backup
- USB Log Exporting
- Reporting
- Object/Object Group
- Diagnostic Tools
- One-Click Technical Support
- Web Management
- Webshell
- CLI (Telnet, SSH, Console)

Product Association

- Endpoint Monitoring
- Based Auto Access Control Based on Endpoint Health Status
- Auto Isolation of Unprotected Endpoints

NISG 9000X Specifications

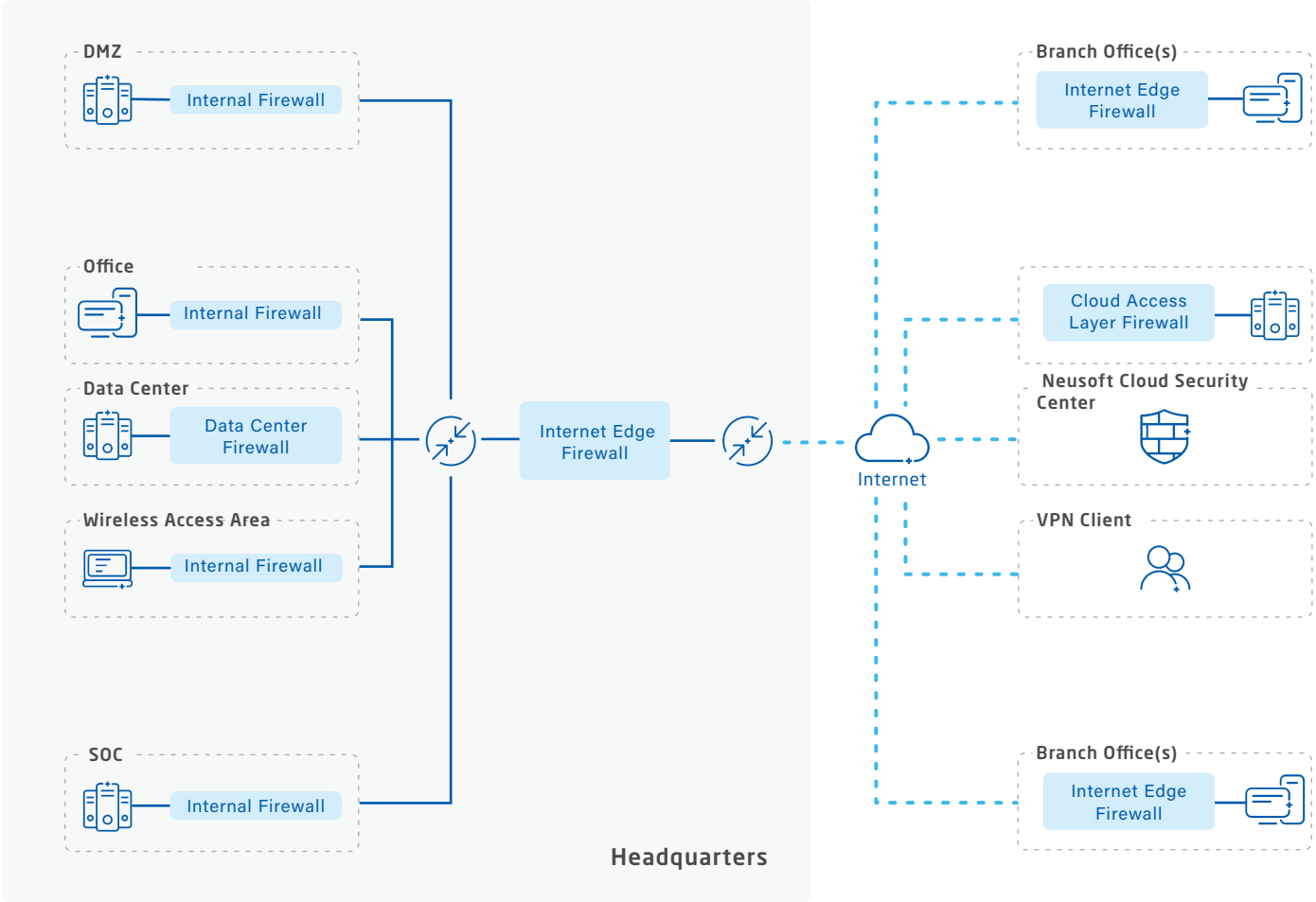
Parameter	Description					
Hardware						
Model	 9000X-S	 9000X-A	 9000X-H	 9000X-N	 9000X-C	 9000X-E
Interface	6 x GE RJ45	4 x GE RJ45, 2 x Combo	6 x GE RJ45	6 x GE RJ45, 2 x 1GE SFP, 2x10GESFP+	2 x GE RJ45	1 x GE RJ45
USB	2xUSB2.0	1xUSB2.0	2xUSB2.0	2xUSB2.0	2xUSB2.0	2xUSB2.0
Console	1x Console	1x Console	1 x Console	1 x Console	1 x Console	1 x Console
Slots	1 x Expansion slots	1 x Expansion slots	2 x Expansion slots	2 x Expansion slots	4 x Expansion slots	8 x Expansion slots
Bypass	1 x Bypass ports by default	1 x Bypass ports by default	3 x Bypass ports by default	2 x Bypass ports by default	N/A	N/A
HA	N/A	N/A	N/A	N/A	1 x HA ports by default	1 x HA ports by default
Screen	N/A	N/A	N/A	1x LCD interface screen	N/A	N/A
Power Supply	Single / Redundant Power Supply	Single / Redundant Power Supply	Single / Redundant Power Supply	Single / Redundant Power Supply	Single / Redundant Power Supply	Single / Redundant Power Supply
Strorage	1TB (surveillance-grade) /4TB (enterprise-grade) Storage media license (Mandatory)	1TB (surveillance-grade) /4TB (enterprise-grade) Storage media license (Mandatory)	1TB (surveillance-grade) /4TB (enterprise-grade) Storage media license (Mandatory)	1TB (surveillance-grade) /4TB (enterprise-grade) Storage media license (Mandatory)	1TB (surveillance-grade) /4TB (enterprise-grade) Storage media license (Mandatory)	1TB (surveillance-grade) /4TB (enterprise-grade) Storage media license (Mandatory)

Performance	
Firewall Throughput	4~180Gbps
Application Control Throughput (64 KHTTP)	3~60Gbps
IPS Throughput (64K HTTP)	600Mbps~10Gbps
NGFW Throughput (64K HTTP)	500Mbps~10Gbps
Threat Prevention Throughput (64K HTTP)	280Mbps~2Gbps
Anti-Virus Throughput (64K HTTP)	280Mbps~3Gbps
Concurrent Connections	5,000,000~25,000,000
New Connections	34,000~460,000
IPSec VPN Throughput	360Mbps~14Gbps
SSL VPN Throughput	115Mbps~1Gbps

Accessories	
NNCM-8-1000T-SGD	8-Port Gigabit Ethernet Expansion Card (Non-Bypass)
NNCM-8-1000TB-SGD	8-Port Gigabit Ethernet Expansion Card (4-Pair Bypass)
NNCL-4-1000T-SGD	4-Port Gigabit Ethernet Expansion Card (Non-Bypass)
NNCL-4-1000TB-SGD	4-Port Gigabit Ethernet Expansion Card (2-Pair Bypass)
NNCM-8-1000G-SGD	8-Port 1GE SFP Expansion Card
NNCL-4-1000G-SGD	4 Port 1GE SFP Expansion Card
NNCX-2-10G-SGD	2-Port 10GE SFP+ Expansion Card
NNCX-4-10G-SGD	4-Port 10GE SFP+ Expansion Card
SFP-PLUS-SM-10-SGD	10GE SFP+ Single-Mode (10km) Optical Transceiver
SFP-PLUS-MM-SGD	10GE SFP+ Multi-Mode Optical Transceiver

Comprehensive Intelligent Threat Protection

- Deployed at the Internet edge to block threats, enforce access control, and deliver robust perimeter security.
- Positioned at internal network boundaries to provide regional access control and safeguard endpoints and servers.
- Integrated at the data center access layer to secure connectivity and protect critical infrastructure.
- NISG 9000X establishes secure, encrypted tunnels between headquarters, branch offices, data centers, and remote users, ensuring safe and reliable data transmission.



Neusoft

Neusoft Corporation (Headquarters)
No.2 Xin Xiu Street, Hun Nan New District, Shenyang, Liaoning, PRC
Postal Code: 110179

Neusoft Malaysia Sdn Bhd
Units 07-03, Menara EcoWorld,Bukit Bintang City Centre, No. 2, Jalan Hang Tuah,55100 Kuala Lumpur.

Neusoft Japan Co.,Ltd
Tokyo Fashion Town BLDG. EAST 7F,
3-6-11, Ariake, Koutou-Ku, Tokyo 135-8071, Japan.

E-mail: security_info@neusoft.com
Neusoft Cybersecurity: neteye.neusoft.com/en
Neusoft Corporation: www.neusoft.com