Neusoft

NISG 3000 Series

N3 / N5 / N7

Small and Midsize Business Security

Security Bolstered for Evolving Threats

NISG 3000 Series

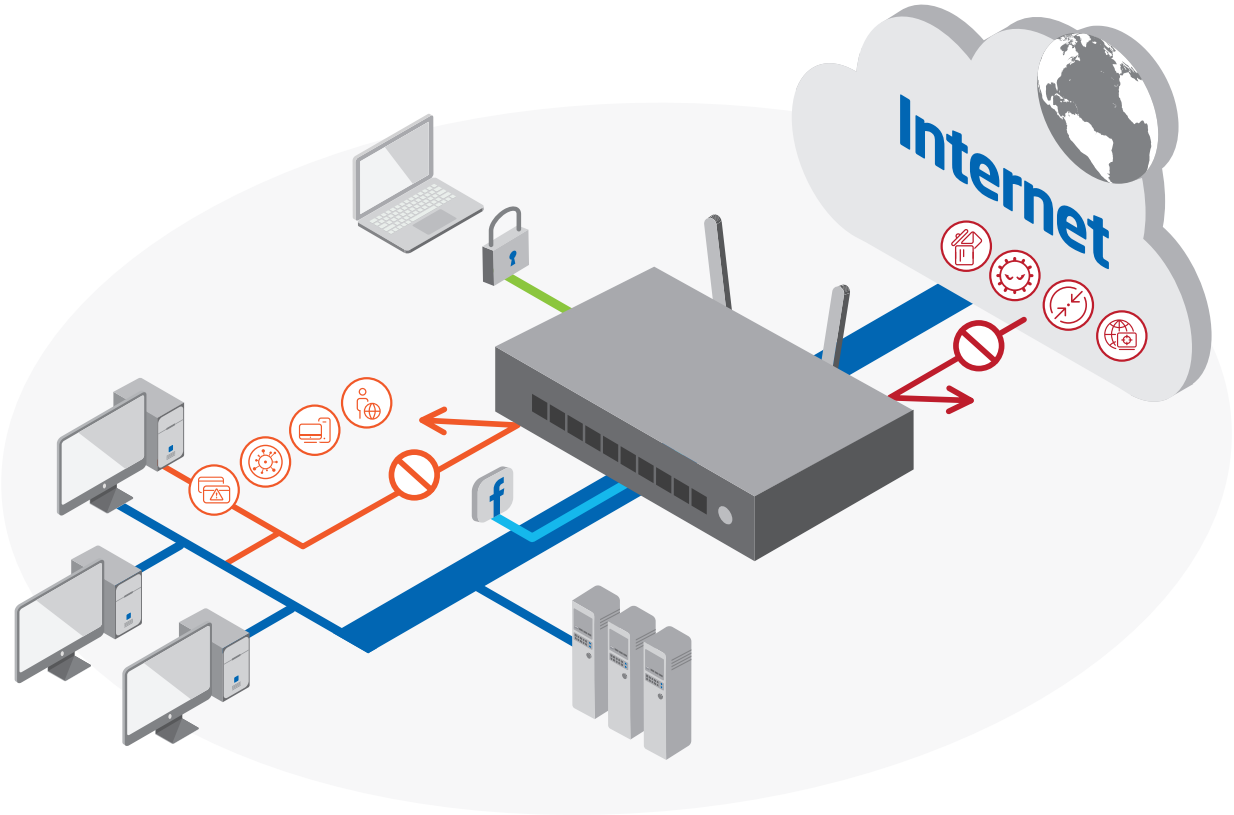
Enterprise-Grade Firewall for Mid-Size and Small Businesses

Small and midsize businesses (SMBs) are more susceptible to attacks because they lack resources such as money and dedicated staff to secure their IT infrastructure and combat threats, and they often end up paying a high price for the attacks. Therefore, cyber security is now a top priority for SMBs.

Neusoft Integrated Security Gateway (NISG) 3000 series is launched to provide industry-leading security solutions for SMBs and protect enterprise networks against increasingly sophisticated attacks. It is a multi-function firewall that integrates multiple security features including VPN, IPS, anti-virus, anti-spam, URL filtering and application control, and enables SMBs to carry out security deployment in an easy and affordable way.

Features & Benefits

- Expedites security deployment with an intuitive configuration wizard.
- iShield cloud platform makes device configuration and management simple and available anywhere and anytime; iAlert service makes device health status visible in an easy way.
- Able to support multiple industry-leading UTM engines ,which provides great flexibility and convenience for partners in different regions.
- Up to 4 Gbps application control performance ensures optimal user experience. Able to identify and control over 3000 types of applications to minimize network security risks.



Internal threats & External threats

Non-Compliant Network Behavior

The URL filtering function can restrict employees' Internet use and prevent employees from accessing violence, gambling, sex, and crime websites, and so on.

Virus Spread

The anti-virus function can detect emails and files sent by employees to prevent viruses from spreading.

Illegal Web Page Access

The page filtering function can filter sensitive words in web pages to prohibit internal employees from accessing some specific web pages.

Invisible Users and Network Activities

Application control function can accurately identifies users' identities and applications, therefore, it can monitor and understand user's network activities.

Virus Attack

Anti-virus function provides comprehensive protection for users when downloading files and receiving emails, keeping users safe from malware, ransomware, and other threats.

Spam Attack

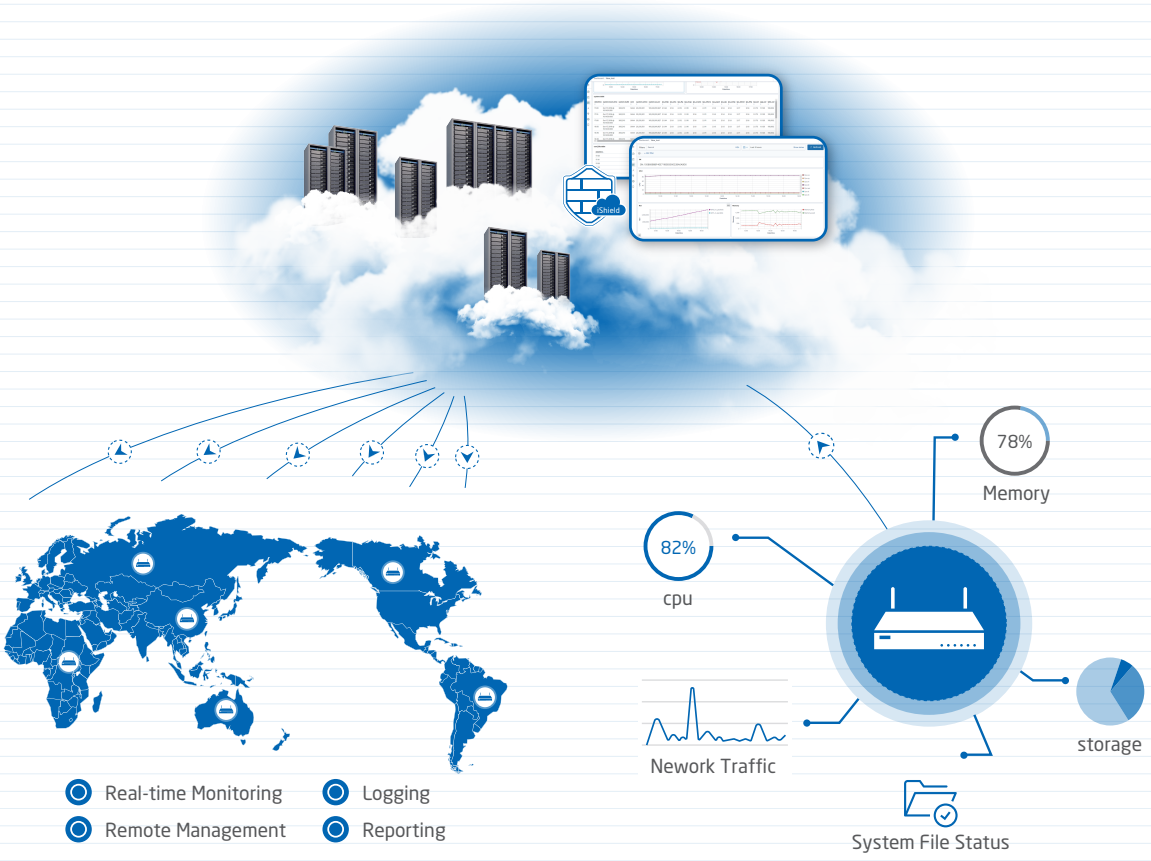
Anti-spam function can effectively prevent phishing emails, spam emails, fraud emails and so on.

Network Attack

The attack defense funciton can prevent external attacks, like DoS, DDoS, flood attacks, botnet attacks, and so on.

External Malicious Invasion

The Intrusion Prevention System (IPS) can identify attacks prompty and prevent hackers from employing system vulnerabilities to attack corporate servers, stealing user information, mining, constructing botnets, and implant Trojans.



Neusoft iShield Enables Easy Management and Maintenance

Neusoft iShield is a cloud management platform that offers centralized management of NISG devices and monitoring of NISG health status. It can effectively improve response speed, improve service quality, and reduce operation and maintenance costs.

Centralized Management

- Neusoft iShield cloud platform provides a very intuitive management portal to easily manage and configure a few or dozens of NISG devices. Users can remotely log in to manage devices distributed in different regions anytime and anywhere, greatly reducing time and labor costs.
- iShield can also provide services for storing logs, generating reports, and real-time monitoring for NISG devices without using other hardware and software, making management a lot easier.

Visible Device Health

- Neusoft iShield cloud management platform provides iAlert services, which helps administrators deeply understand the health of NISG devices, foresee security risks, and make remediation immediately to ensure the critical business continuity and enhance corporate network security.
- The iAlert service can perform statistics and analysis on the collected running status information of NISG devices, and present all in the central dashboard, which makes it a lot easier to locate security risks and prevent problems before they occur.
- Monitoring the health of NISG devices include system information, CPU, memory, disks, processes, network traffic, and so on, so that administrators can comprehensively understand and visualize the health status of NISG devices.

Features

Working Modes

Bridging Mode

Routing/NAT Mode

Hybrid Mode

Port Address Translation (PAT)

Policy-Based NAT/PAT

NAT-Based Load Balancing

IP Mapping

Group IP Mapping

Max Number of VLANs (4,094)

Max Number of Users (unlimited)

Network Modes

PPPoE

DHCP

Firewall

IP packet Filtering

IP-MAC Binding

Session Timeout

Application Security

Intrusion Prevention System (IPS)

Anti-Virus (AV)

Anti-Spam (AS)

URL Filtering

Application Identification

3,000+ Applications Identification

- Communication
- Business
- Networking
- General-Internet
- Browser-Based
- Client-Server
- Peer-to-Peer
- Network-Protocol
- Custom Applications

Dynamic Port Support

FTP

TFTP

SIP

H.323

RTSP

Oracle

Tuxedo

Wireless

802.11 a/b/g/n

2.4GHz, 5 GHz

AP/Client/Bridge/Repeater/Router

AES, TKIP

WEP, WPA/WPA2-PSK

WIDS

- Asleep Attack
- Association Frame Flooding
- Spoofed and Broadcasting
- De-Authentication
- Authentication Frame Flooding
- EAPOL Packet Flooding
- Long Duration Attack
- Null SSID Probe Response
- Spoofed and Broadcasting
- De-Association
- Wireless Bridge Detection

Features (Continued)

VPN

- IPSec VPN
- VPN in Transparent Mode
- VPN in Routing Mode
- Site-to-Site/ Remote Access VPN
- IPSec NAT traversal
- VPN Tunnel
- 3DES/AES encryption
- MD-5 and SHA-1 Authentication
- Auto IKE, PKI (X.509)
- L2TP over IPSec
- Dead Peer Detection (DPD)
- Perfect Forward Secrecy (DH group) : 1,2,5
- Anti-Replay
- DNS-Based VPN
- Pre-Shared Key
- Certificates

Route

- Static Route
- Policy-Based Route

Attack Defense

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

Authentication

- Local Authentication Database
- Max Number of Local Users (50,000)
- VPN Xauth/L2TP Authentication
- Web Authentication
- RADIUS Authentication
- LDAP Authentication

Logging/Monitor

- Syslog
- E-mail
- SNMP (v1/v2c)
- SNMP Trap
- Route Tracing
- Monitor on VPN Tunnels
- Monitor on Session Tables
- Monitor on Resources
- Monitor on Network Status

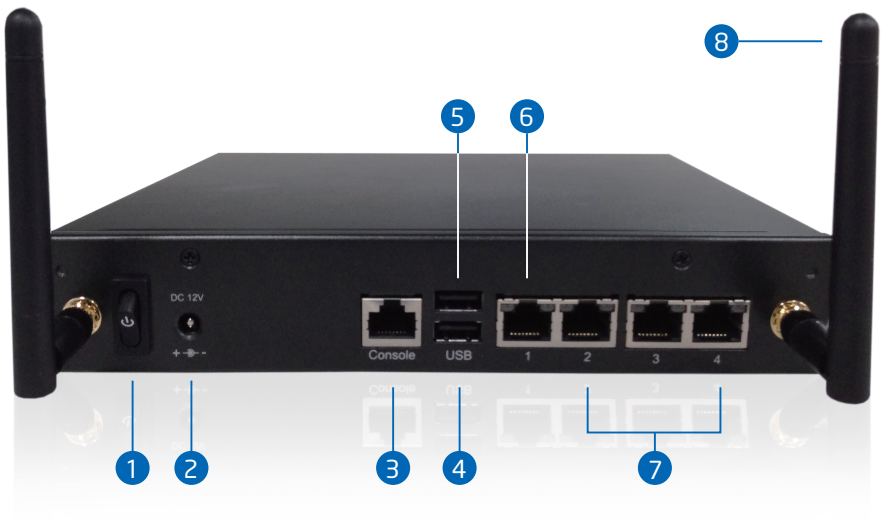
System Management

- WebUI
- CLI (Telnet, SSH, and Console)
- Assignment of Administrative Roles and Permissions
- Simplified Configuration Wizard
- Manual/Auto Software Update
- Log Maintenance
- Zone Division
- Object (IP addresses and services) Object Group
- Log Storage by USB
- iShield Centralized Management

Specifications

Performance	NISG 3000-N3	NISG 3000-N5	NISG 3000-N7
Firewall throughput	2.7 Gbps	2.7 Gbps	2.7 Gbps
Application control throughput	4 Gbps	4 Gbps	4 Gbps
VPN throughput	110 Mbps	110 Mbps	110 Mbps
IPS throughput	200 Mbps	200 Mbps	200 Mbps
AV throughput	205 Mbps	205 Mbps	205 Mbps
Maximum concurrent connections	200,000	200,000	200,000
New connections per second	12,000	12,000	12,000
Users	15	30	100
WIFI	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n

1. Power Switch
   Turn on/off power supply
2. DC 12V Input
3. Dedicated Management Port
4. USB 3.0 Port
   Connect USB devices
5. USB 2.0 Port
   Connect USB devices
6. WAN Port
   Connect to the Internet
7. LAN Port
   Connect to the local network
8. Wireless Antenna



Neusoft

Neusoft Corporation (Headquarters)

No.2 Xin Xiu Street, Hun Nan New District,

Shenyang, Liaoning, PRC

Zip Code: 110179

Email: securitybz@neusoft.com

Neusoft America Inc.

Morrisville

3000 RDU Center Drive, Suite 119,

Morrisville, NC 27560, United States