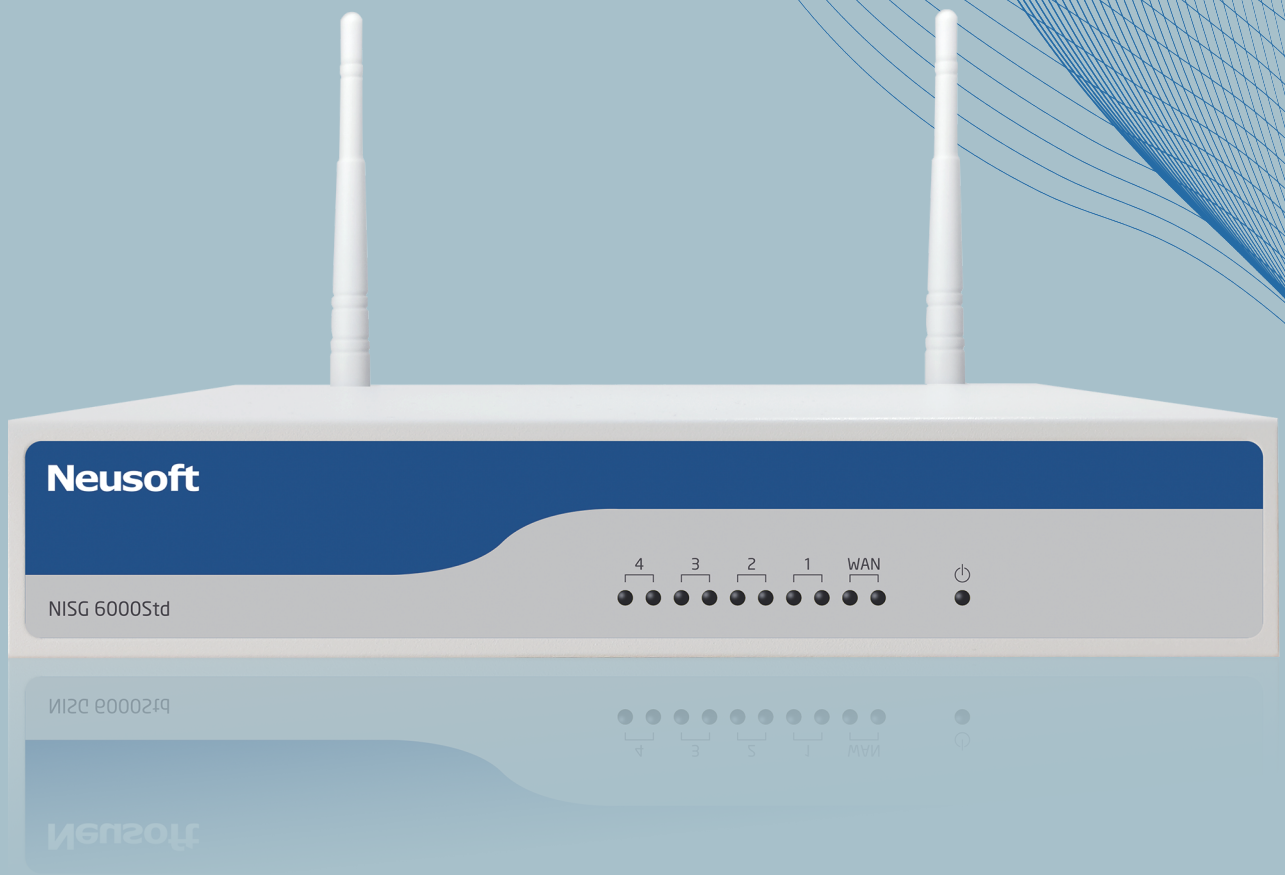
NISG 6000Std

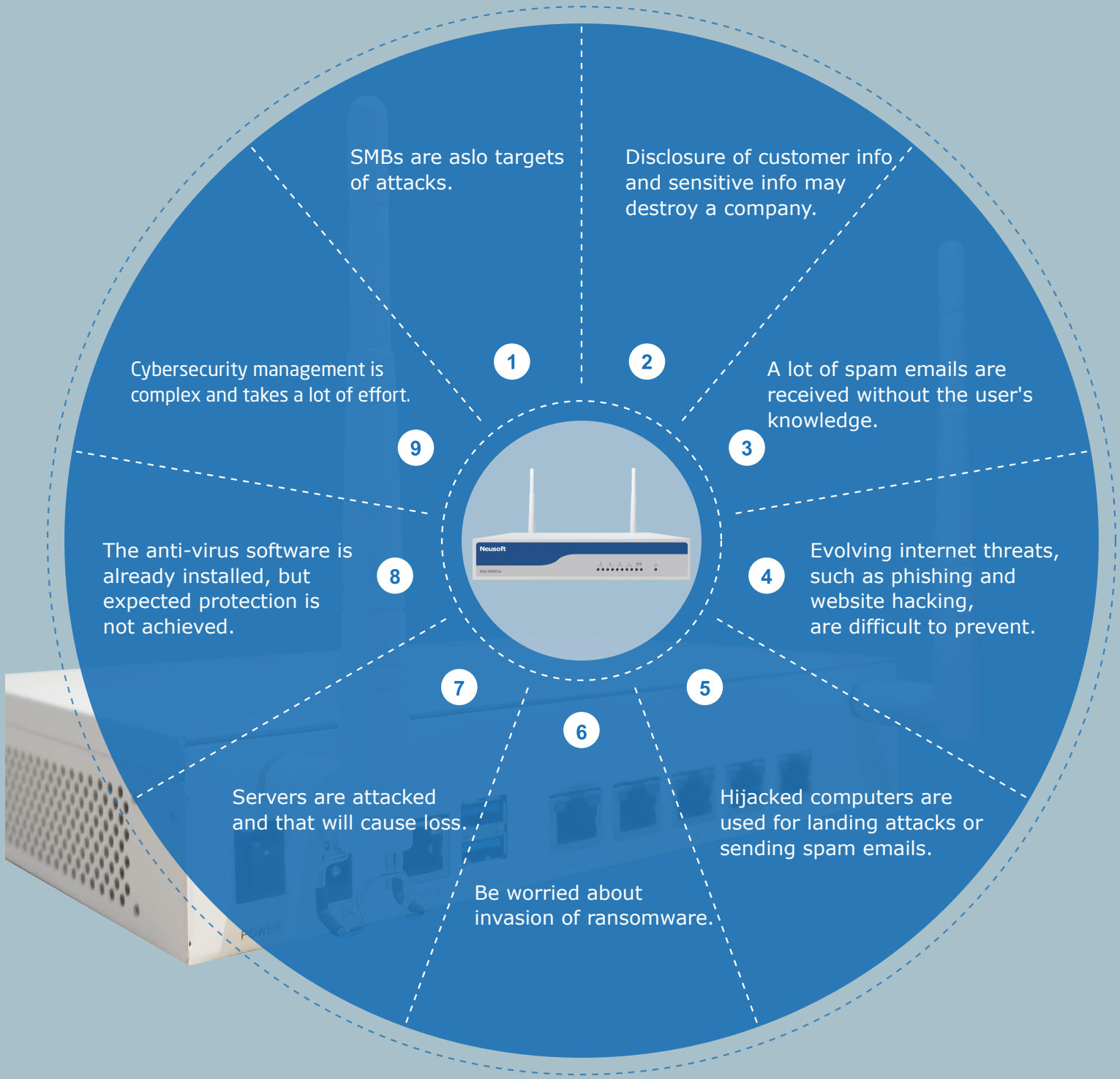
- Unified Security Features
- Easy-to-Use Configuration and Management
- Cloud-Based Monitoring Platform



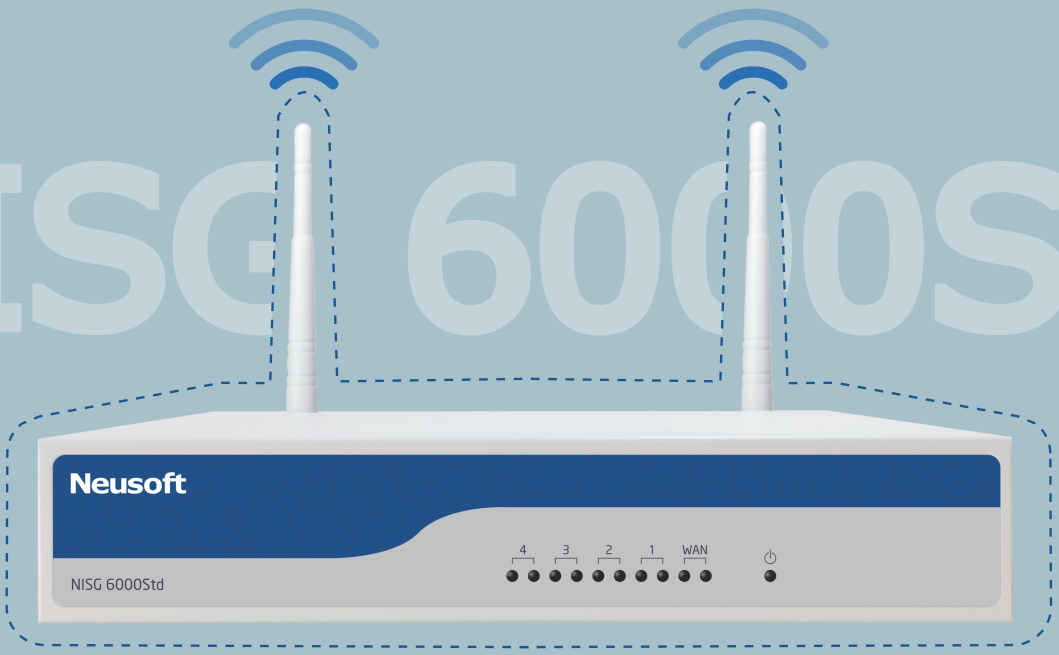
Next-Gen UTM for SMB
Unifying NGFW Features

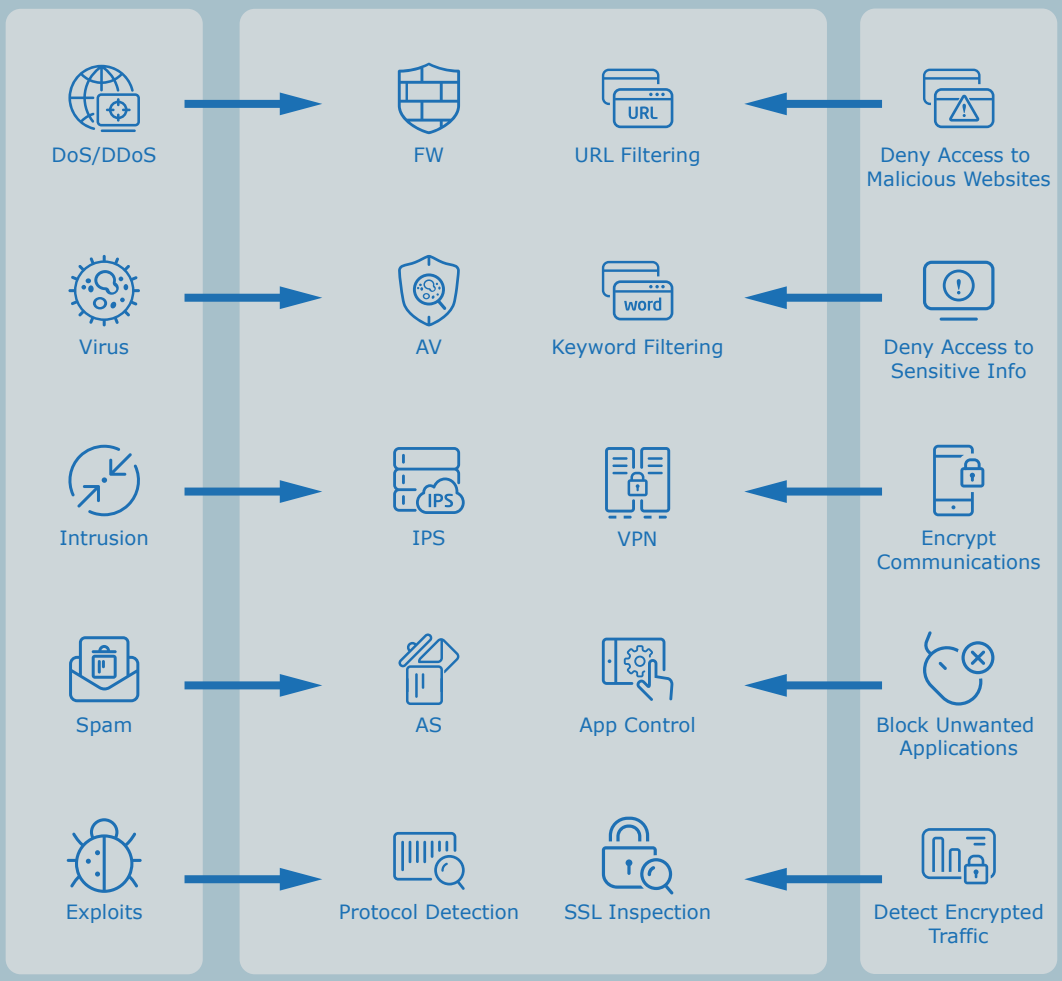
Neusoft

NISG 6000Std
helps to solve your pain points easily



NISG 6000Std





nCloud, a Cloud-Based Management Platform with Simplified Management and Easy Maintenance

Benefited Customers

- SMBs with distributed branches
- Requiring remote administration

- Real-Time Monitoring
- Logging
- Remote Management
- Reporting

[nCloud Benefits]

nCloud allows remote troubleshooting. Administrators can remotely log in and learn the UTM and network status.

nCloud allows remote authorization, initial config, and daily maintenance, saving time and cost.

nCloud is a cloud-based management platform improving service quality.
It can reduce maintenance costs by centralized monitoring of security status and acceleration of response.

[nCloud Features]

Remote Centralized Management

Through remote login, administrators can manage distributed networks anytime and anywhere.

Real-Time Monitoring

Administrators can check the stability of NISGs by monitoring their online status via nCloud. It can avoid impact on business from unexpected network failures.

Default/Customized Reporting

nCloud can generate reports based on statistics of system information, security information, and traffic information specified by the customer. Generated reports can be sent to specified recipients. Recipients can check the report content anytime.

Log Storage

NISG logs can be synchronized to and stored on nCloud. Logs stored on nCloud can provide necessary information for cause tracing and status reporting in case of security exceptions.

Features

NISG is a next-gen UTM appliance unifying FW, IPS, VPN and other security functions.

FW

User and application-based next-gen firewall. It integrates traditional firewall functions such as zone-based protection, access control, static routing, policy-based routing, DNS proxy, and DHCP service, as well as application-layer control and role-based control, thus enhancing access security.

IPS

IPS engine with international patented technology. It can analyze and identify thousands of attacks against common operating systems, databases, web servers, mail servers and application software, effectively block the attack traffic and alarm, and help enterprises resist intrusions.

DoS/DDoS

Defend against 54 common DoS/DDoS attacks such as SYN flood, UDP flood, ICMP flood, IP option attacks, and port scans.

Anti-Virus

It supports heuristic virus scanning technology to prevent viruses from spreading through the internal mail system. It also supports scanning and filtering files and software applications downloaded through HTTP and FTP, effectively helping enterprises defend against viruses and risky software.

Anti-Spam

The anti-spam engine supports filtering emails by the sender, subject and body. It analyzes whether an email is spam through intelligent algorithms. It can also filter well-known spam sending addresses through DNS check and other technologies to effectively block spam.

nCloud Management Platform

With Neusoft nCloud, administrators can easily manage and configure NISG devices anytime and anywhere.

Protocol Detection

It can analyze common network protocols and perform standard protocol detection, to effectively block potential malformed data packet attacks and protect office networks and servers.

Server Protection

It can protect the sensitive information of mail servers and web servers, thus to protect the internal mail and web servers from information leakage, effectively block server-oriented attacks, and make up for the risk of exposure due to the untimely upgrade of the server software version.

IPSec VPN

Compatible with all site-to-site VPN gateways that support standard IPSec VPN. Encryption and authentication can secure data transmitted between headquarters and branches from being eavesdropped and stolen. It can perform access control on encrypted data, and support route-based and policy-based VPN.

Remote Access VPN

Enterprise employees can connect to the office network through remote VPN. Encryption and authentication can secure the data from being stolen or tampered. Different access control policies can be performed on different employees to protect enterprise data.

IPv6

International IPv6Ready certified. It is fully compatible with IPv6 network, and supports comprehensive IPv6 security from Layer 3 to Layer 7.

URL Filtering & Content Filtering

URL filtering and web content filtering can effectively block office computers from accessing websites with violent and pornographic content.

Application Control

Fine-grained identification of common and high-traffic apps further helps enterprises manage common apps and thus reduce network risks. It can identify and control up to 3000 kinds of apps.

DNS Protection

Via DNS domain blacklist and DNS cache poisoning protection, NISG can effectively block phishing websites and network frauds, and thus protect enterprise networks from risks.

Logging & Monitoring

Management logs, traffic logs, IPS logs, anti-virus logs, anti-spam logs, and application control logs enable admins to learn the enterprise network risks. Real-time monitoring provides the network real-time status, and can display the top applications, top traffic, top URLs and other information for admins.

Wireless

The built-in wireless module can provide wireless access solutions, without need for additional APs. It supports wireless AP, wireless client and wireless relay functions to meet all wireless access and expansion needs. It supports 802.11a/b/g/n/ac, covering 2.4GHz and 5GHz. It provides three options for wireless data encryption: WEP, WPA/WPA2-PSK and WPA/WPA2-Radius, and support the AES and TKIP encryption algorithm.

SSL Inspection

NISG can inspect most SSL encrypted traffic, including AV, AS, URL filtering, IPS and application identification. Supported SSL protocols include HTTPS, IMAPS, POP3S, and SMTPS. This function can minimize the risk of enterprise data leakage and provide unified security for enterprises.

NISG 6000Std Specifications

Hardware Spec

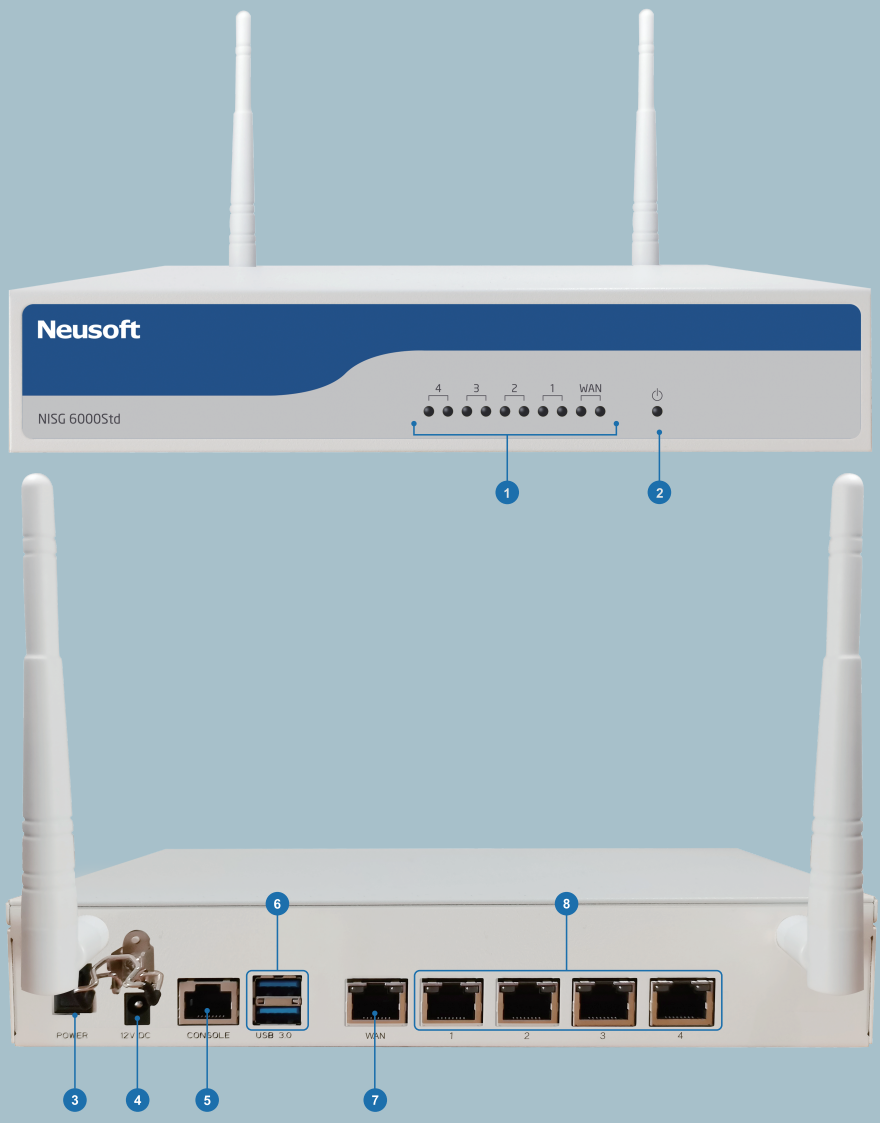
Series	NISG6000Std
Platform	Apollo Lake
CPU	Intel Celeron J3355, 2.00 GHz
Memory	4G
Storage	8G
Interfaces	WAN GB Ethernet Port×1 LAN GB Ethernet Port×4 Dual Band Wireless-PCI-E, 2.4G/5G IEEE 802.11 a/b/g/n/ac USB ×2 Console x 1
Dimensions & Weight	232{W} x 152{D} x 44{H}, 2.1 kg
Power	AC Max 60W
Operating Temperature	0~40º C(Work) -40~60º C(Storage)
Compliance	CE emission, FCC Class A, RoHS,VCCI

Performance Spec

Performance	NISG6000Std-W
FW Throughput	4 Gbps
VPN Throughput	190 Mbps
IPS Throughput	420 Mbps
AV Throughput	500 Mbps
Concurrent Sessions	200,000
New Sessions/Sec	22,000

Hardware Models

Model	Login Users
NISG 6000Std-W-N3	15
NISG 6000Std-W-N5	30
NISG 6000Std-W-N7	100

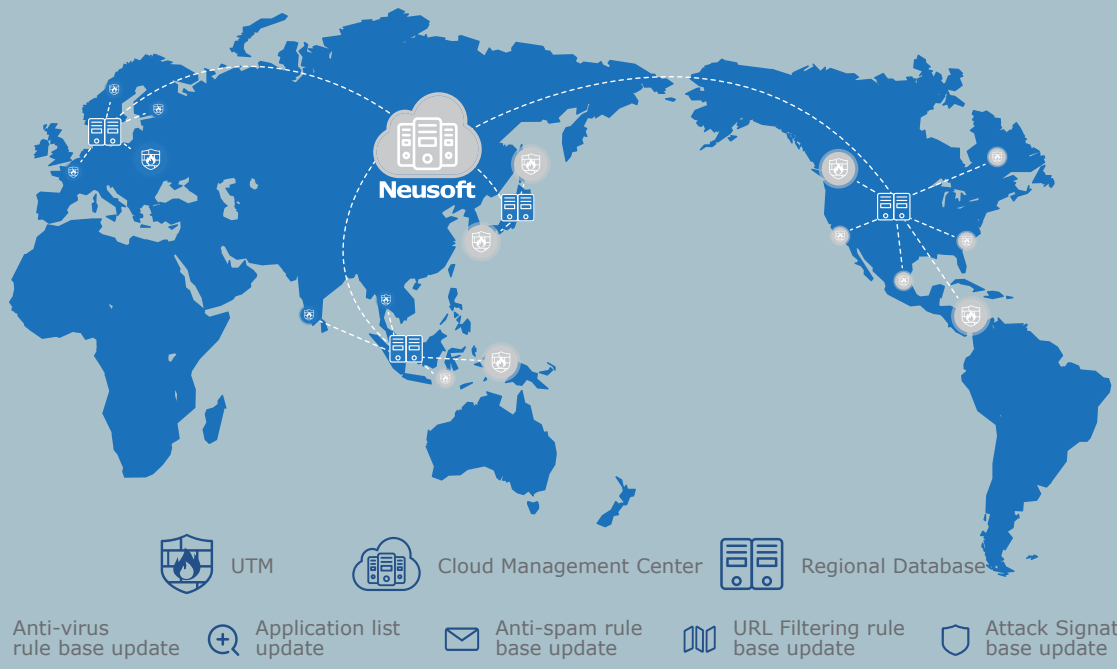


1 Port Status Led
2 Power Led
3 Power Switch
4 DC 12V
5 Console Port
6 USB 3.0 Port
7 WAN Port
8 LAN Port

Certifications

- VMware Ready
- Citrix Ready
- IPv6 Ready
- CVE Compatibility
- Microsoft MAPP Membership
- Patented IPS
- Telec (WiFi Certification for Japan)
- PSE (Power Certification for Japan)
- …

Public Cloud-Based Global Service System Providing Real-Time Service



Neusoft

Neusoft Corporation (Headquarters)
No.2 Xin Xiu Street, Hun Nan New District,
Shenyang, Liaoning, PRC
Zip Code: 110179
Email: securitybz@neusoft.com
Website: www.neusoft.com