Neusoft Corporation (Headquarters)
No.2 Xin Xiu Street, Hun Nan New District,
Shenyang, Liaoning, PRC
Zip Code: 110179
E-mail: securitybz@neusoft.com
Website: www.neusoft.com
Cybersecurity: neteye.neusoft.com/en/

Neusoft

- Integrated Security Features
- Easy Setup & Management
- Cloud Monitoring Platform

NISG 9000Std

Integrated NGFW Capabilities

Next-Gen UTM for SMEs

Enterprise-Grade UTM/Security Gateway for SMEs

NISG 9000Std is the ideal next-generation UTM solution for SMEs.
By consolidating multiple security functions into a single device, it delivers an all-in-one security solution featuring easy setup and management.

External Threat Prevention

Network Attack Defense

Block DoS, DDoS, flooding, and botnet attacks with our advanced attack defense capabilities.

Anti-Spam & Anti-Phishing

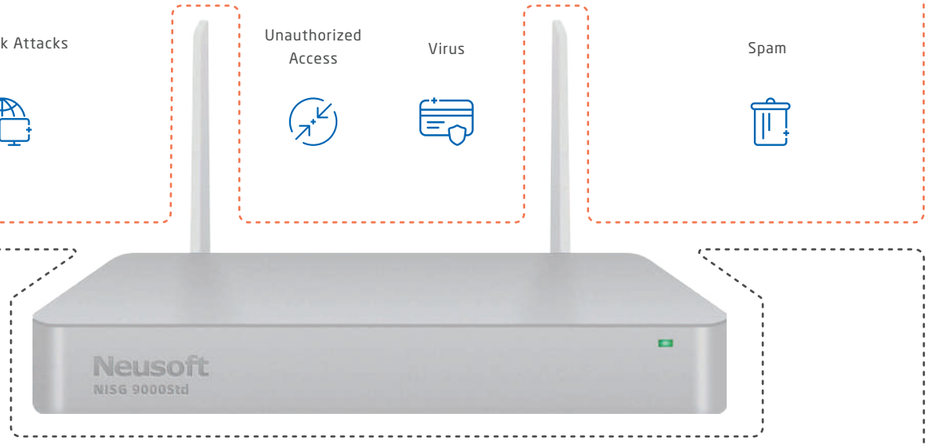
Stop phishing emails, spam, and fraudulent messages with powerful anti-spam filtering.

Anti-Virus & Anti-Malware

Real-time antivirus scanning for downloads and email attachments safeguards users from malware, ransomware, and other cyber threats.

Unauthorized Access Control

IPS detects and blocks incoming attacks, by preventing server exploits, data theft, cryptojacking, botnet propagation, and Trojan infections.



Unauthorized Access Control

User Auth & Management

Web Access Control

Virus Spread Prevention

Web Access Control

Web filtering with keyword detection blocks access to restricted websites.

Virus Spread Prevention

Antivirus scanning of outgoing emails and files prevents malware propagation.

Access Control Enforcement

URL filtering restricts access to non-business related sites including violence/gambling/adult content and criminal activity websites.

User Authentication & Management

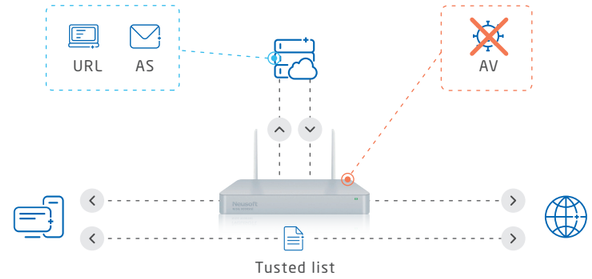
Centralized user account management with network access monitoring and application usage tracking.

Internal Threat Mitigation

Q1:

Does NISG 9000Std support both local detection and online inspection capabilities?

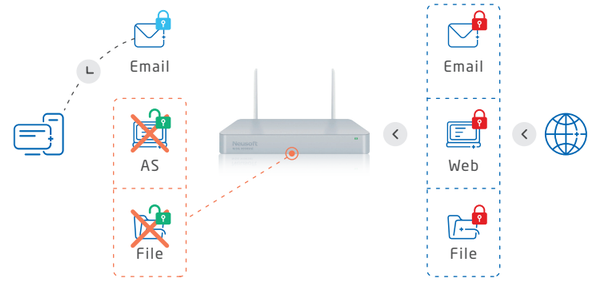
Yes. NISG 9000Std provides real-time local detection combined with scheduled cloud updates for anti-spam, URL filtering, and virus signature databases. This hybrid approach delivers multi-layered security against sophisticated network threats.



Q2:

Does NISG 9000Std protect against malware in encrypted communications?

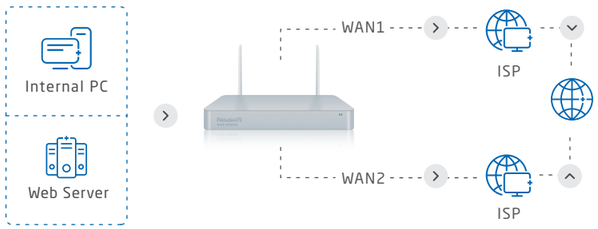
Yes. NISG 9000Std performs SSL-encrypted traffic scanning to detect and block malicious content within encrypted channels.



Q3:

Can I switch ISPs immediately during network failures?

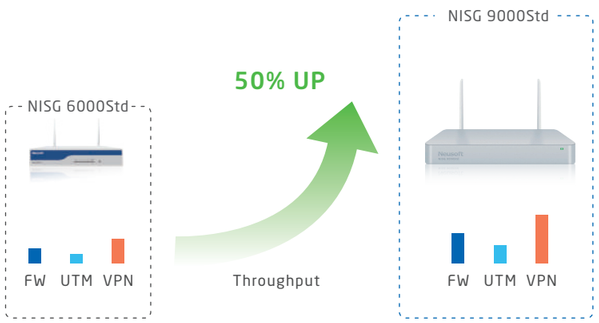
Yes. NISG 9000Std provides dual WAN ports. It enables simultaneous connections to different ISPs and supports automatic failover to prevent business disruption during outages.



Q4:

Does NISG 9000Std impact network throughput or latency?

No. NISG 9000Std delivers high performance and deploying NISG 9000Std will not impact existing network performance.



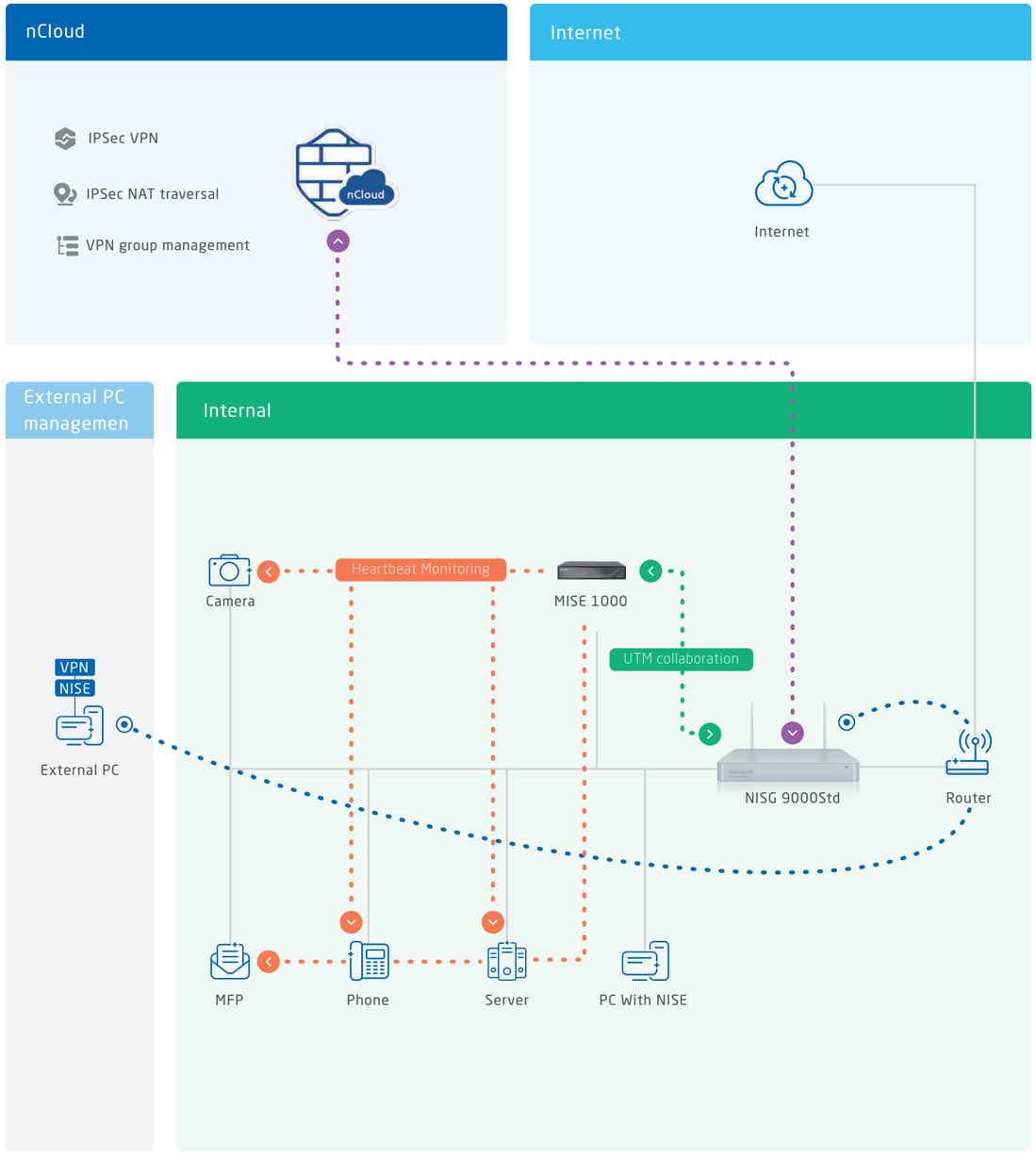
All-in-One Security Solution for SMEs

Communication between NISG and nCloud

VPN remote communication for external PCs

Collaborative communication between NISG and NISE

Communication for NISE monitoring



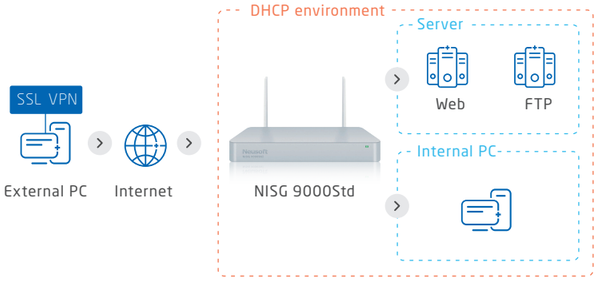
1.Enable Remote Management and Device Status Monitoring with nCloud

nCloud is a cloud management platform for NISG and NISE.
By monitoring security via the cloud, it enables rapid response, thereby reducing operational costs.

Remote Management | Real-Time Monitoring | Log Storage | Default/Customized Reports

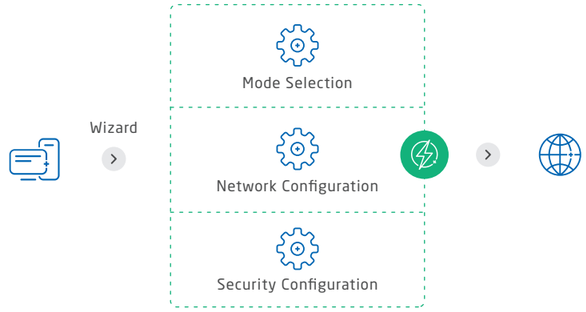
2.Secure Remote Access with UTM's VPN

A dedicated virtual network can be established within the corporate network, enabling secure communication between remote users and internal systems.

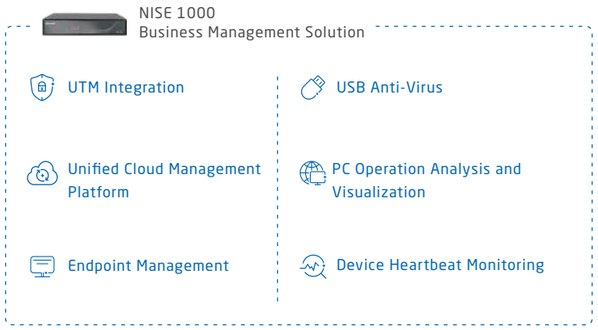


3.Quick and Easy Setup Reduces Maintenance Complexity

Device setup and deployment can be easily completed using a wizard, eliminating the need for lengthy procedures and reducing operational workload.



4.Enhanced Security Defense and Endpoint Visibility through Integration with Business Management Solution NISE 1000



Product Features

NISG 9000Std integrates the next-generation firewall, advanced security, and convenient features.

Firewall

NISG 9000Std provides user- and application-based control, combining traditional firewall protection with advanced application-layer security and identity-aware management for comprehensive network visibility and secure access. The traditional firewall protection includes access control, static routing, policy-based routing, DNS proxy, and DHCP services

IPS

NISG 9000Std integrates patented IPS engine which can detect and block thousands of attacks targeting OS, databases, web/mail servers, and applications. NISG 9000Std provides customizable IPS policies and attack signatures for enhanced network protection.

DoS/DDoS Defense

NISG 9000Std can defend against 60+ types of attacks including SYN/UDP/ICMP floods, IP option attacks, and port scans.

Anti-Virus

NISG 9000Std employs heuristic virus scanning technology to prevent virus propagation through corporate email systems, while scanning and filtering files downloaded via HTTP/FTP protocols and applications, effectively defending against viruses and malicious software.

Anti-Spam

NISG 9000Std can filter spam by senders, recipients, subject lines, and email content. NISG 9000Std can accurately identify and block spam by using intelligent algorithms, while maintaining real-time spammer databases for enhanced protection.

nCloud Management Platform

Neusoft's nCloud platform enables administrators to easily manage and configure NISG devices anytime, anywhere.

Reporting

NISG 9000Std can export monitoring data into customizable reports, which can be distributed via email. Delivery schedules can be configured to meet specific operational requirements.

Server Protection

NISG 9000Std can secure email and web servers against data leaks and cyberattacks, while providing interim protection during vulnerability remediation.

IPSec VPN

NISG 9000Std can establish multiple gateway-to-gateway IPSec VPN tunnels with policy-based routing and VPN capabilities, enabling secure encrypted data transfer between corporate offices and branches.

Remote Access VPN

NISG 9000Std enables secure remote connections to corporate networks via encrypted VPN tunnels with authentication, preventing data interception or tampering. It supports both IKEv1 and IKEv2 protocols for reliable, high-performance cross-platform security.

IPv6

With certified IPv6 Ready, NISG 9000Std ensures full compatibility with Japanese IPv6 networks.

URL & Content Filtering

NISG 9000Std can block access to websites by URL and content category, including violence, pornography, and non-business.

Application Control

NISG 9000Std can identify 3,000+ applications and perform control while securing enterprise software to reduce network risks.

DNS Protection

NISG 9000Std safeguards corporate networks against phishing and online fraud through DNS blacklist and cache poisoning protection.

Logging & Monitoring

NISG 9000Std provides comprehensive logs (management, session, IPS, anti-virus, anti-spam, URL filtering, application control, etc.) for rapid threat detection. Real-time monitoring displays network status, application usage, traffic statistics, and URL access.

Wireless

NISG 9000Std wireless module can work in dual-mode (AP/client) with full 802.11a/b/g/n/ac support across 2.4GHz/5GHz bands, featuring enterprise encryption (AES/TKIP) and multiple authentication modes including WEP/WPA2-PSK/RADIUS.

SSL Inspection

NISG 9000Std can decrypt and inspect most SSL traffic (including QUIC/HTTPS/IMAPS/POP3S/SMTPS), enabling full security scanning (anti-virus, anti-spam, URL filtering, IPS, application control) while minimizing data leakage risks.

NISG 9000Std Specifications

Hardware Specifications

Hardware	Description
Processor	Denverton
CPU	Intel Atom® Processor C3558
Memory	8 G
Storage	64 G
Interfaces	WAN/LAN GB Ethernet Port x6 Dual Band Wireless-PCI-E,2.4G/5G IEEE 802.11 a/b/g/n/ac USB ×2 Console x 1
Weight	1.25kg
Dimensions	277{W} x 174.5{D} x 38{H}(mm)
Power Consumption	ADS-65HI-12N-1,AC Max 48W
Operating Environment	0~40° C (Work) -40~70° C (Storage)
Power Consumption	CE emission, FCC Class A, RoHS, UL, VCCI

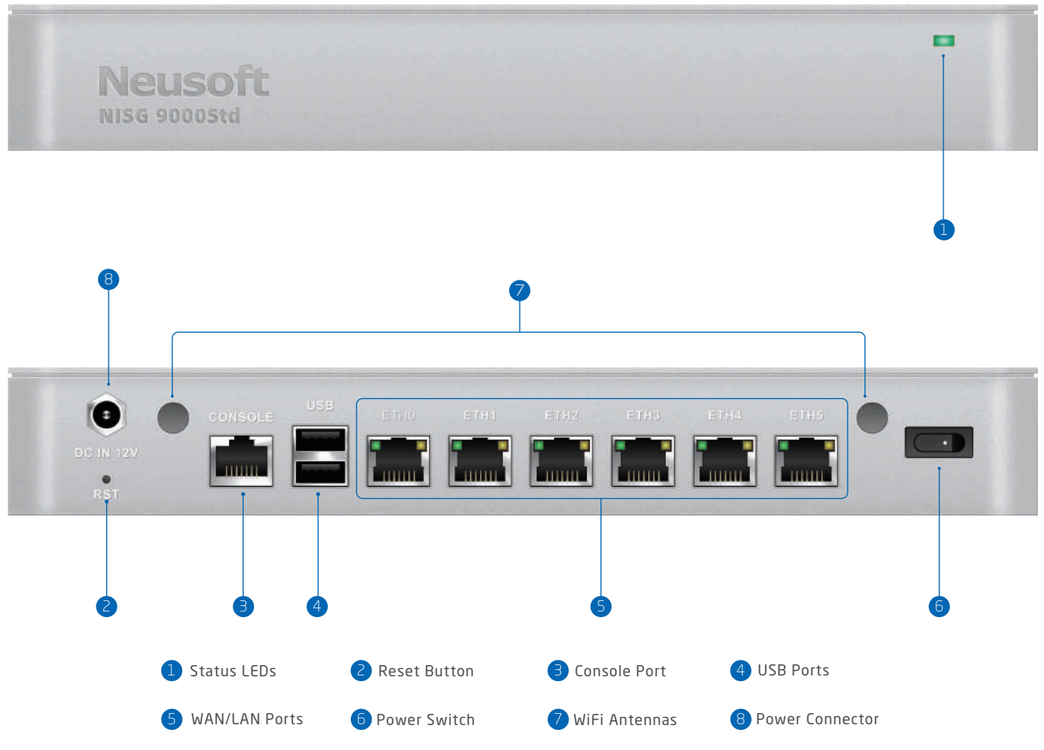
Performance

Performance	Description
Firewall Throughput	6,000 Mbps
VPN Throughput	1,900 Mbps
IPS Throughput	800 Mbps
Anti-Virus Throughput	850 Mbps
Max Concurrent Connections	500,000
New Connections/sec	57,000

Hardware Models

Model	Supported Users
NISG 9000Std-N3	15
NISG 9000Std-N5	30
NISG 9000Std-N7	100

Hardware



1 Status LEDs
2 Reset Button
3 Console Port
4 USB Ports
5 WAN/LAN Ports
6 Power Switch
7 WiFi Antennas
8 Power Connector