

Next-Generation Firewalls

NSG-3100/NSG-5100 security platforms deliver business reliability for large and medium-sized enterprises and data centers.



NSG-3100/NSG-5100 Next-Generation Firewalls

FS firewalls provide comprehensive and granular visibility and control of applications. They can identify and prevent potential threats associated with high-risk applications while providing policy-based control over applications, users, and user-groups. Policies can be defined that guarantee bandwidth to mission-critical applications while restricting or blocking unauthorized or malicious applications. They provide real-time protection for applications from network attacks including viruses, spyware, worms, botnets, ARP spoofing, DoS/DDoS, Trojans, buffer overflows, and SQL injections. They incorporate comprehensive network security and advanced firewall features for large and medium-sized enterprises and data centers.

Benefits

- IPS, Anti-Virus, Threat Prevention, Attack Defense, URL Filtering
- SSL Decryption, Application Control
- IPsec VPN, SSL VPN, L2TP VPN, PnPVPN
- NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- iQoS, Traffic Shaping, Bandwidth Allocation
- GUI, CLI (Console, SSH, Telnet), SNMP

Key Features

Granular Application Identification and Control

- Provide fine-grained control of web applications regardless of port, protocol, or evasive action.
- They can identify and prevent potential threats associated with high-risk applications while providing policy-based control over applications, users, and user-groups.
- Security policies can be defined that guarantee bandwidth to mission-critical applications while restricting or blocking unauthorized or malicious applications.

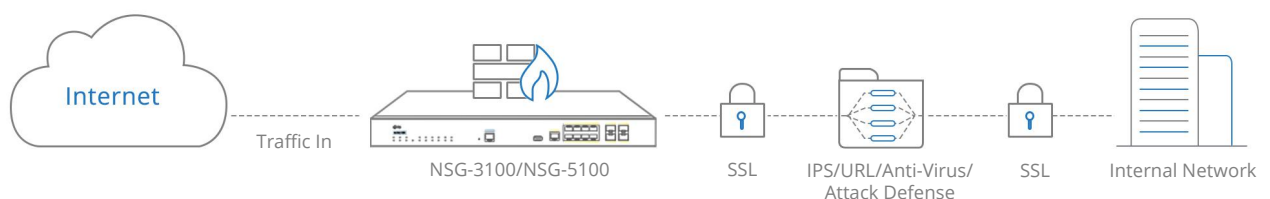
Comprehensive Threat Detection and Prevention

- Provide real-time protection for applications from network attacks including viruses, spyware, worms, botnets, ARP spoofing, DoS/DDoS, Trojans, buffer overflows, and SQL injections.
- They incorporate a unified threat detection engine that share packet details with multiple security engines (AD, IPS, URL filtering, Anti-Virus).

Superior Network Adaptability

- The intelligent link load balancing greatly promotes the link utilization and user experience for network access to meet the diverse requirements.
- With VPN acceleration chip, they can significantly improve IPSec/SSL VPN performance and support VPN deployment in large-scale network environments.
- Support virtual firewall technology and provide the private security protection service for tenants.

Deployment



NSG-3100/NSG-5100 incorporate a unified threat detection engine that share packet details with multiple security engines, including IPS, URL filtering, Anti-Virus, Attack Defense. They can support application identification and control, data security and load balancing.

They provide comprehensive network security and advanced firewall features for large and medium-sized enterprises and data centers.

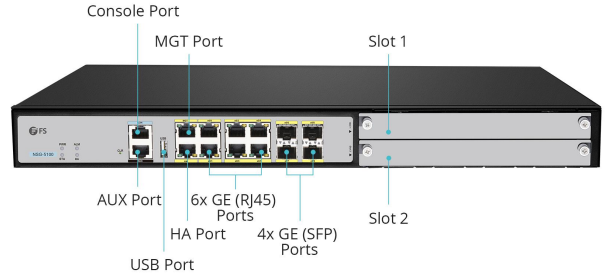
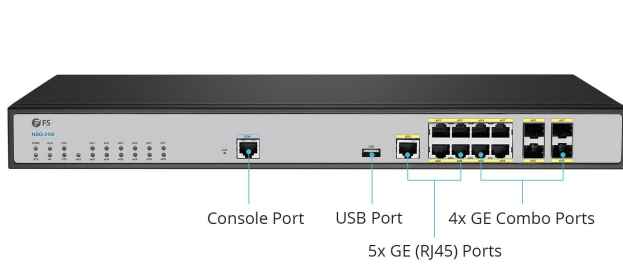
Panel Overview

NSG-3100

FS NSG-3100 Next-Generation Firewall combines the most comprehensive security protections to defend your mid-sized to large enterprises deployments.

NSG-5100

FS NSG-5100 Next-Generation Firewall provides the most advanced threat prevention security for enterprise and data centers networks



Specification

System Specification

Items	NSG-3100	NSG-5100
Ports	5x GE (RJ45), 4x Combo	6x GE (RJ45), 4x SFP
Firewall Throughput ⁽¹⁾	2.5 Gbps	6 Gbps
NGFW Throughput ⁽²⁾	650 Mbps	1 Gbps
Threat Protection Throughput ⁽³⁾	500 Mbps	800 Mbps
IPS Throughput ⁽⁴⁾	1 Gbps	1.8 Gbps
IMIX Throughput ⁽⁵⁾	800 Mbps	2 Gbps
AV Throughput ⁽⁶⁾	700 Mbps	1.2 Gbps
IPSec VPN Throughput ⁽⁷⁾	1 Gbps	3 Gbps

System Specification

Items	NSG-3100	NSG-5100
New Sessions/sec ⁽⁸⁾	50,000	80,000
Maximum Concurrent Sessions	1 Million	2 Million
IPSec Tunnel Number	2,000	4,000
SSL VPN Users	8/1,000	8/2,000
Intrusion Prevention	1-Year Subscription Included	1-Year Subscription Included
Anti-Virus	1-Year Subscription Included	1-Year Subscription Included
URL Filtering	1-Year Subscription Included	1-Year Subscription Included
QoS	1-Year Subscription Included	1-Year Subscription Included
Management Ports	1x Console Port, 1x USB port	1x Console Port, 1x AUX Port, 1x USB Port, 1x HA, 1x MGT
Expansion Slots	N/A	2x Slots
Maximum Power Consumption	1x 45W, Redundancy 1 + 1	1x 150W, Redundancy 1 + 1
Power Supply	Dual (one included)	Dual (one included)
AC Input Power	100-240V, 50/60Hz, 1A	100-240V, 50/60Hz, 1A
DC Input Power	N/A	-40 to -60V, 4A
Warranty	1 Year	1 Year
Dimension (HxWxD)	1.7"x17.4"x9.5" (44x442x241 mm)	1.7"x17.2"x14.4" (44x436x366 mm)
Weight	5.5 lb (2.5kg)	12.3 lb (5.6kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10-95% (no dew)

NOTES: ⁽¹⁾ Firewall throughput data is obtained under single-stack UDP traffic with 1518-byte packet size;

⁽²⁾ NGFW throughput data is obtained under 64 Kbytes HTTP traffic with application control and IPS enabled;

⁽³⁾ Threat protection throughput data is obtained under 64 Kbytes HTTP traffic with application control, IPS, AV and URL filtering enabled;

⁽⁴⁾ IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on;

⁽⁵⁾ IMIX throughput data is obtained under UDP traffic mix (64 byte : 512 byte : 1518 byte =5:7:1);

⁽⁶⁾ AV throughput data is obtained under HTTP traffic with file attachment;

⁽⁷⁾ IPSec VPN throughput data is obtained under Preshare Key AES256+SHA-1 configuration and 1400-byte packet size packet;

⁽⁸⁾ New Sessions/s is obtained under TCP traffic.

Software Features

Software Features and Protocols	
Network Services	<ul style="list-style-type: none"> • Dynamic routing (OSPF, BGP, RIPv2) • Static and policy routing • Route controlled by application • Built-in DHCP, NTP, DNS Server and DNS proxy • Tap mode – connects to SPAN port • Interface modes: sniffer, port aggregated, loopback, VLANS (802.1Q and Trunking) • L2/L3 switching & routing • Virtual wire (Layer 1) transparent inline deployment
Firewall	<ul style="list-style-type: none"> • Operating modes: NAT/route, transparent (bridge), and mixed mode • Policy objects: predefined, custom, and object grouping • Security policy based on application, role and geo-location • Application Level Gateways and session support: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, DCERPC, DNS-TCP, DNS-UDP, H.245 0, H.245 1, H.323 • NAT and ALG support: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN • NAT configuration: per policy and central NAT table • VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing • Global policy management view • Security policy redundancy inspection • Schedules: one-time and recurring
Intrusion Prevention	<ul style="list-style-type: none"> • Protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia • IPS Actions: default, monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time • Packet logging option • Filter based selection: severity, target, OS, application or protocol • IP exemption from specific IPS signatures • IDS sniffer mode • IPv4 and IPv6 rate based DoS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCIP/ICMP session flooding (source/destination) • Active bypass with bypass interfaces • Predefined prevention configuration
Anti-Virus	<ul style="list-style-type: none"> • Manual, automatic push or pull signature updates • Flow-based Antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP • Compressed file virus scanning

Software Features and Protocols

Attack Defense

- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN Flood, DNS Query Flood defense
- ARP attack defense

IP Reputation

- Botnet server IP blocking with global IP reputation database

URL Filtering

- Flow-based web filtering inspection
- Manually defined web filtering based on URL, web content and MIME header
- Dynamic web filtering with cloud-based real-time categorization database: over 140 million URLs with 64 categories (8 of which are security related)
- Additional web filtering features:
 - Filter Java Applet, ActiveX or cookie
 - Block HTTP Post
 - Log search keywords
 - Exempt scanning encrypted connections on certain categories for privacy
- Web filtering profile override: allows administrator to temporarily assign different profiles to user/group/IP
- Web filter local categories and category rating override

Botnet C&C Prevention

- Regularly update the botnet server addresses
- prevention for C&C IP and domain
- Support TCP, HTTP, and DNS traffic detection
- IP and domain whitelists

SSL Decryption

- Application identification for SSL encrypted traffic
- IPS enablement for SSL encrypted traffic
- AV enablement for SSL encrypted traffic
- URL filter for SSL encrypted traffic
- SSL Encrypted traffic whitelist
- SSL proxy offload mode

Endpoint Identification

- Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
- Support 10 operation systems
- Support query based on IP and endpoint quantity

Data Security

- File transfer control based on file type
- File protocol identification, including HTTP, FTP, SMTP and POP3
- File signature and suffix identification for over 100 file types
- Content filtering for HTTP-GET, HTTP-POST, FTP and SMTP protocols
- IM identification and network behavior audit

Software Features and Protocols

Application Control

- Over 3,000 applications that can be filtered by name, category, subcategory, technology and risk
- Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
- Actions: block, reset session, monitor, traffic shaping
- Identify and control cloud applications in the cloud
- Provide multi-dimensional monitoring and statistics for cloud applications, including risk category and characteristics

Quality of Service (QoS)

- Max/guaranteed bandwidth tunnels or IP/user basis
- Tunnel allocation based on security domain, interface, address, user/user group, server/server group, application/app group, TOS, VLAN
- Bandwidth allocated by time, priority, or equal bandwidth sharing
- Type of Service (TOS) and Differentiated Services (DiffServ) support
- Prioritized allocation of remaining bandwidth
- Maximum concurrent connections per IP
- Bandwidth allocation based on URL category

Server Load Balancing

- Weighted hashing, weighted least-connection, and weighted round-robin
- Session protection, session persistence and session status monitoring
- Server health check, session monitoring and session protection

Link Load Balancing

- Bi-directional link load balancing
- Outbound link load balancing includes policy based routing, ECMP and weighted, embedded ISP routing and dynamic detection
- Inbound link load balancing supports SmartDNS and dynamic detection
- Automatic link switching based on bandwidth, latency, jitter, connectivity, application
- Link health inspection with ARP, PING, and DNS

VPN

- IPSec VPN
 - IPSec Phase 1 mode: aggressive and main ID protection mode
 - Peer acceptance options: any ID, specific ID, ID in dialup user group
 - Supports IKEv1 and IKEv2 (RFC 4306)
 - Authentication method: certificate and pre-shared key
 - IKE mode configuration support (as server or client)
 - DHCP over IPSEC
 - Configurable IKE encryption key expiry, NAT traversal keep alive frequency
 - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
 - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
 - Phase 1/Phase 2 Diffie-Hellman support: 1,2,5
 - XAuth as server mode and for dialup users
 - Dead peer detection
 - Replay detection
 - Autokey keep-alive for Phase 2 SA

Software Features and Protocols

<p>VPN</p>	<ul style="list-style-type: none"> • IPSEC VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design) • IPSEC VPN configuration options: route-based or policy based • IPSEC VPN deployment modes: gateway-to-gateway, full mesh, hub-and-spoke, redundant tunnel, VPN termination in transparent mode • One time login prevents concurrent logins with the same username • SSL portal concurrent users limiting • SSL VPN port forwarding module encrypts client data and sends the data to the application server • Supports clients that run iOS, Android, and Windows XP/Vista including 64-bit Windows OS • Host integrity checking and OS checking prior to SSL tunnel connections • MAC host check per portal • Cache cleaning option prior to ending SSL VPN session • L2TP client and server mode, L2TP over IPSEC, and GRE over IPSEC • View and manage IPSEC and SSL VPN connections • PnPVPN
<p>VSYS</p>	<ul style="list-style-type: none"> • System resource allocation to each VSYS • CPU virtualization • Non-root VSYS support firewall, IPsec VPN, SSL VPN, IPS, URL filtering • VSYS monitoring and statistic
<p>IPv6</p>	<ul style="list-style-type: none"> • Management over IPv6, IPv6 logging and HA • IPv6 tunneling, DNS64/NAT64 etc • IPv6 routing protocols, static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+ • IPS, application identification, URL filtering, Anti-Virus, access control, ND attack defense
<p>High Availability</p>	<ul style="list-style-type: none"> • Redundant heartbeat interfaces • Active/Active and Active/Passive • Standalone session synchronization • HA reserved management interface • Failover: <ul style="list-style-type: none"> - Port, local & remote link monitoring - Stateful failover - Sub-second failover - Failure notification • Deployment options: <ul style="list-style-type: none"> - HA with link aggregation - Full mesh HA - Geographically dispersed HA

Software Features and Protocols

User and Device Identity

- Local user database
- Remote user authentication: TACACS+, LDAP, Radius, Active
- Single-sign-on: Windows AD
- 2-factor authentication: 3rd party support, integrated token server with physical and SMS
- User and device-based policies
- User group synchronization based on AD and LDAP
- Support for 802.1X, SSO Proxy
- WebAuth page customization
- Interface based authentication
- Agentless ADSSO (AD Polling)
- Use authentication synchronization based on SSO-monitor

Management

- Management access: HTTP/HTTPS, SSH, telnet, console
- Central Management: Web service APIs
- System Integration: SNMP, syslog, alliance partnerships
- Rapid deployment: USB auto-install, local and remote script execution
- Dynamic real-time dashboard status and drill-in monitoring widgets

Logs & Reporting

- Logging facilities: local memory and storage (if available), multiple syslog servers
- Reliable logging using TCP option (RFC 3195)
- Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets, URL etc.
- Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications, WiFi related events
- IP and service port name resolution option
- Brief traffic log format option
- Three predefined reports: security, flow and network reports
- User defined reporting
- Reports can be exported in PDF via Email and FTP

Ordering Information

NSG-3100

Default Configuration	NSG-3100 Next-Generation Firewall, includes 5x GE (RJ45), 4x combo ports, 1 AC power unit, IPS service, Anti-Virus, QoS, URL filtering service, hardware warranty and software upgrading service. (1 Year)
------------------------------	--

NSG-5100

Default Configuration	NSG-5100 Next-Generation Firewall, includes 6x GE (RJ45), 4x SFP ports, 1 AC power unit, IPS service, Anti-Virus, QoS, URL filtering service, hardware warranty and software upgrading service. (1 Year)
------------------------------	--

NSG-3100/NSG-5100 Customized Service

Hardware Options	AC power extension unit. Hardware warranty for 1, 2, 3 years. Quantity of Virtual System and SSL VPN Concurrent Users.
Software License	Maximum Performance and Sessions of AEL(Only supported on NSG-3100). Software Upgrading service for 1, 2, 3 years. IPS, Antivirus, QoS, URL Filtering, Botnet C&C Prevention, IP Reputation for 1, 2, 3 years.

Business Module Options

NSG-5100 INTERFACE CARDS

I/O Ports	8x GE (RJ45)	8x SFP	4x GE Bypass (2 pair bypass ports)	4x GE (RJ45) with PoE
Dimension	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)	1 U (Occupies 2 generic slots)
Weight	1.8 lb (0.8kg)	2.0 lb (0.9kg)	1.8 lb (0.8kg)	0.9 lb (0.4kg)

NOTE:

1. The optical transceiver module is not included.
2. The interface cards are unavailable online. You can contact with Sales@fs.com freely for your needs. Thanks.

Accessories



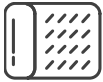
Power Supply (Installed)*1



Power Cord*1



Console Cable*1



Rubber Pads*4



Rack Mount Brackets*2



Screws M4/M6+
Nuts*20



Cat5e Cables*2



Grounding Cable*1



User Manual*1



 <https://www.fs.com>



The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.