NetScreen Series Security Systems

Product Overview

The NetScreen Series is a line of purpose-built, high-performance security systems designed for large enterprise, carrier, and data center networks. Architected with both existing and future network design in mind, the NetScreen Series consists of two platforms: the 2-slot NetScreen-5200 and the 4-slot NetScreen-5400. Integrating firewall, VPN, traffic management functionality, Denial of Service (DoS) and Distributed Denial of Service (DDoS) protection in a low profile modular chassis, the NetScreen Series delivers scalable performance for the most demanding network environments.

Your ideas. Connected.™

Product Description

The Juniper Networks® NetScreen Series Security Systems are ideally suited for large enterprise network backbones, including:

- Departmental or campus segmentation
- Enterprise data centers for securing high-density server environments
- Carrier-based managed services or core infrastructure

Offering excellent scalability and flexibility while providing high levels of security, the NetScreen Series is differentiated by its chassis configuration for fans, power supplies, and number of slots for modules. Both the Juniper Networks NetScreen-5200 and Juniper Networks NetScreen-5400 support secure port modules that offer different throughput and interface options for deployment flexibility. All chassis are designed with hot-swappable, redundant fans and power supplies. This enables businesses to maximize device uptime and meet stringent government and industry certifications, such as the rigorous Network Equipment Building System criteria, the requirement for equipment used in the central office in the North American Public Switched Network.

Employing a switch fabric for data exchange and separate multi-bus channel for control information, the NetScreen Series can scale up to 30 Gbps firewall and 15 Gbps 3DES/AES VPN. It provides low-latency performance for all packet sizes and is ideal for multimedia, VoIP, and other streaming media applications.

Juniper Networks delivers all the components necessary to build and secure a highly available infrastructure. Redundant links for full-mesh topologies, sub-second stateful fail-over, path monitoring, and a secured control protocol all join to provide complete resilience for the security layer. The NetScreen Series also supports Juniper Networks virtual systems capability, with capacity up to 500 virtual systems. Virtual systems allow a single security device to be partitioned logically into multiple security domains, each with a unique virtual router, policy set, address book, and administrative login. Virtual systems can be used with physical interfaces, as well as VLAN tagged interfaces bound to any interface, with multiple security zones supported within each virtual system.

Whether the requirement is high-capacity session/tunnel aggregation, high-performance small-packet throughput, a high degree of system virtualization or a high degree of physical segmentation, the NetScreen Series is the ideal platform for large enterprise and carrier grade networks. The additional benefits associated with lower total cost of ownership and the ability to meet future service or application requirements make the NetScreen Series firewall/VPN the clear choice for network security operations.

Juniper Networks further expands overall system functionality and performance by introducing a new management module and three new secure port modules (SPMs) for the NetScreen Series. The new management module takes advantage of faster CPU speeds and larger CPU cache to enhance performance while the new SPMs take advantage of Juniper's fourth generation security ASIC to deliver advanced functionality at multi-gigabit rates. These new management and SPM modules deliver the Juniper heritage of high-performance security while expanding capabilities and capacities for NetScreen Series customers.

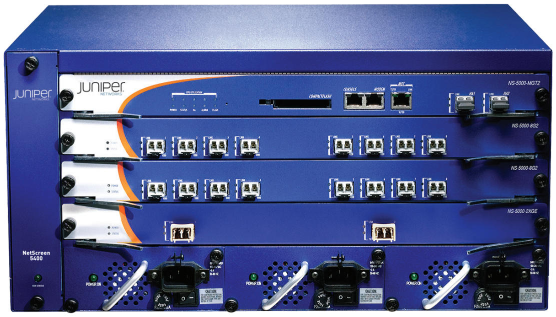
Features and Benefits

Feature	Feature Description	Benefit
Purpose-built platform	Modular, chassis-based security systems.	Delivers the high performance and configuration flexibility required to protect large enterprise and carrier environments.
High performance	ASIC based architecture employs a switch fabric for data exchange and a separate multi-bus channel for control information.	Ensures scalable performance and low latency in sensitive applications such as VoIP and streaming media.
Advanced network segmentation	Security zones, virtual LANs and virtual routers allow administrators to deploy security policies to isolate guests, regional servers, or databases.	Prevents unauthorized access, contains any attacks that may occur, and facilitates regulatory compliance.
System and network resiliency	Hardware component redundancy and full mesh configurations enable redundant physical paths in the network.	Provides the reliability required for high-speed network deployments.
High availability (HA)	Active/passive, active/active and active/active full mesh HA configurations using dedicated high availability interfaces.	Achieve maximum availability and ensure synchronization for sub-second failover between interfaces or devices.
Interface flexibility	Modular architecture enables deployment with a wide variety of interface options, including SFP (SX, LX, TX) and XFP 10 gigabit (SR or LR).	Simplifies network integration and helps reduce the cost of future network upgrades.
Robust routing engine	The NetScreen Series routing engine supports OSPF, BGP, RIP v1/2, transparent Layer 2 operation, NAT and Route mode.	Facilitates the deployment of the NetScreen Series as a combined security and LAN routing device, lowering operational and capital expenditures.
Virtual system support	Supports up to 500 virtual firewalls – each with a unique set of administrators, policies, VPNs, and address books.	Reduces the number of physical units and allows the partitioning of the network into separate administrative domains.
World-class professional services	From simple lab testing to major network implementations, Juniper Networks Professional Services will collaborate with your team to identify goals, define the deployment process, create or validate the network design, and manage the deployment.	Transforms the network infrastructure to ensure that it is secure, flexible, scalable, and reliable.

Product Options

Option	Option Description	Applicable Products
Integrated IPS (Deep Inspection)	Prevents application level attacks from flooding the network using a combination of stateful signatures and protocol anomaly detection mechanisms. IPS is annually licensed.	NetScreen-5200 and NetScreen-5400
Web filtering (redirect)	Block access to malicious Web sites using a Web filtering redirect solution such as SurfControl or Websense technology.	NetScreen-5200 and NetScreen-5400
Virtual systems	Supports up to 500 virtual firewalls—each with a unique set of administrators, policies, VPNs, and address books.	NetScreen-5200 and NetScreen-5400

NetScreen-5200



NetScreen-5400

Specifications

	NetScreen-5200	NetScreen-5400
Maximum Performance and Capacity[1]		
ScreenOS® Software version tested	ScreenOS 6.2	ScreenOS 6.2
Firewall performance (large packets)[2]	10/8 Gbps	30/24 Gbps
Firewall performance (small packets)	4 Gbps	12 Gbps
Firewall Packets Per Second (64 byte)	6 M PPS	18 M PPS
AES256+SHA-1 VPN performance[2]	5/4 Gbps	15/12 Gbps
3DES+SHA-1 VPN performance[2]	5/4 Gbps	15/12 Gbps
Maximum concurrent sessions[3]	1,000,000[9,10]	2,000,000[9,10]
New sessions/second[11]	26,500/22,000	26,500/22,000
Maximum security policies	40,000	40,000
Maximum users supported	Unrestricted	Unrestricted
Network Connectivity		
Fixed I/O	0	0
Interface expansion slots	2 (1 x Management, 1 x SPM)	4 (1 x Management, 3 x SPM)
LAN interface options	8 mini-GBIC (SX, LX or TX), or 2 XFP 10GB (SR or LR)	8 mini-GBIC (SX, LX or TX), or 2 XFP 10GB (SR or LR)
Firewall		
Network attack detection	Yes	Yes
Denial of Service (DoS) and Distributed Denial of Service (DDoS) protection	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes
Brute force attack mitigation	Yes	Yes
SYN cookie protection	Yes	Yes
Zone-based IP spoofing	Yes	Yes
Malformed packet protection	Yes	Yes
Unified Threat Management / Content Security[4]		
IPS (Deep Inspection firewall)	Yes	Yes
Protocol anomaly detection	Yes	Yes
Stateful protocol signatures	Yes	Yes
IPS/Deep Inspection attack pattern obfuscation	Yes	Yes
External URL filtering[5]	Yes	Yes
VoIP Security		
H.323 ALG	Yes	Yes
SIP ALG	Yes	Yes
MGCP ALG	Yes	Yes
SCCP ALG	Yes	Yes
NAT for VoIP protocols	Yes	Yes
IPsec VPN		
Concurrent VPN tunnels[3]	Up to 25,000	Up to 25,000
Tunnel interfaces[3]	Up to 8,191	Up to 8,191
DES (56-bit), 3DES (168-bit) and AES encryption	Yes	Yes
MD-5 and SHA-1 authentication	Yes	Yes
Manual key, IKE, PKI (X.509), IKEv2 with EAP	Yes	Yes
Perfect forward secrecy (DH Groups)	1,2,5	1,2,5
Prevent replay attack	Yes	Yes
Remote access VPN	Yes	Yes
L2TP within IPsec	Yes	Yes
IPsec NAT traversal	Yes	Yes
Redundant VPN gateways	Yes	Yes

	NetScreen-5200	NetScreen-5400
User Authentication and Access Control		
Built-in (internal) database - user limit[3]	Up to 50,000	Up to 50,000
Third-party user authentication	RADIUS, RSA SecurID, and LDAP	RADIUS, RSA SecurID, and LDAP
RADIUS Accounting	Yes – start/stop	Yes – start/stop
XAUTH VPN authentication	Yes	Yes
Web-based authentication	Yes	Yes
802.1X authentication	Yes	Yes
Unified access control enforcement point	Yes	Yes
PKI Support		
PKI Certificate requests (PKCS 7 and PKCS 10)	Yes	Yes
Automated certificate enrollment (SCEP)	Yes	Yes
Online Certificate Status Protocol (OCSP)	Yes	Yes
Certificate Authorities supported	VeriSign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape) Baltimore, DoD PKI	VeriSign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape) Baltimore, DoD PKI
Self-signed certificates	Yes	Yes
Virtualization[6]		
Maximum number of virtual systems	0 default, upgradeable to 500	0 default, upgradeable to 500
Maximum number of security zones	23 default, upgradeable to 1,023	23 default, upgradeable to 1,023
Maximum number of virtual routers	3 default, upgradeable to 503	3 default, upgradeable to 503
Maximum number of VLANs	4,093	4,093
Inter-VSYS Communication (shared-DMZ)	Yes	Yes
Routing		
BGP instances	128	128
BGP peers	256	256
BGP routes	30,000	30,000
OSPF instances	Up to 8	Up to 8
OSPF routes	30,000	30,000
RIP v1/v2 instances	Up to 512	Up to 512
RIP v2 routes	30,000	30,000
Dynamic routing	Yes	Yes
Static routes	30,000	30,000
Source-based routing	Yes	Yes
Policy-based routing	Yes	Yes
ECMP	Yes	Yes
Multicast	Yes	Yes
Reverse Path Forwarding (RPF)	Yes	Yes
IGMP (v1, v2)	Yes	Yes
IGMP Proxy	Yes	Yes
PIM SM	Yes	Yes
PIM SSM	Yes	Yes
Multicast inside IPsec tunnel	Yes	Yes

	NetScreen-5200	NetScreen-5400
IPv6		
Syn-Cookie and Syn-Proxy DoS Attack Detection	Yes	Yes
SIP, RTSP, Sun-RPC, and MS-RPC ALG's	Yes	Yes
Dual stack IPv4/IPv6 firewall and VPN	Yes	Yes
IPv4 to/from IPv6 translations and encapsulations	Yes	Yes
Virtualization (VSYS, Security Zones, VR, VLAN)	Yes	Yes
RIPng	Yes	Yes
BGP version 4	Yes	Yes
DHCPv6 Relay	Yes	Yes
NSRP (active/passive, active/active)	Yes	Yes
Transparent mode for IPv6	Yes	Yes
Mode of Operation		
Layer 2 (transparent) mode[7]	Yes	Yes
Layer 3 (route and/or NAT) mode	Yes	Yes
Address Translation		
Network Address Translation (NAT)	Yes	Yes
Port Address Translation (PAT)	Yes	Yes
Policy-based NAT/PAT	Yes	Yes
Mapped IP (MIP)[8]	20,000	20,000
Virtual IP (VIP)	64	64
MIP/VIP grouping	Yes	Yes
IP Address Assignment		
Static	Yes	Yes
DHCP, PPPoE client	No, No	No, No
Internal DHCP server	No	No
DHCP relay	Yes	Yes
Traffic Management Quality of Service (QoS)		
Guaranteed bandwidth	No	No
Maximum bandwidth	Yes – per physical interface only	Yes – per physical interface only
Ingress traffic policing	No	No
Priority-bandwidth utilization	No	No
DiffServ marking	Yes – per policy	Yes – per policy
Jumbo frames	Yes	Yes
Link aggregation up to 4 ports	8G2 SPM only	8G2 SPM only
High Availability (HA)		
Active/Active	Yes	Yes
Active/Passive	Yes	Yes
Redundant interfaces	8G2 SPM only	8G2 SPM only
Configuration synchronization	Yes	Yes
Session synchronization for firewall and VPN	Yes	Yes
Session failover for routing change	Yes	Yes
Device failure detection	Yes	Yes
Link failure detection	Yes	Yes
Authentication for new HA members	Yes	Yes
Encryption of HA traffic	Yes	Yes
LDAP and RADIUS server failover	Yes	Yes

	NetScreen-5200	NetScreen-5400
System Management		
WebUI (HTTP and HTTPS)	Yes	Yes
Command line interface (console)	Yes	Yes
Command line interface (telnet)	Yes	Yes
Command line interface (SSH)	Yes	Yes
Juniper Networks Network and Security Manager	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes
Rapid deployment	Yes	Yes
Administration		
Local administrator database size	8 MB	8 MB
External administrator database support	RADIUS/LDAP/SecurID	RADIUS/LDAP/SecurID
Restricted administrative networks	6	6
Root admin, admin and read only user levels	Yes	Yes
Software upgrades	Yes	Yes
Configuration rollback	Yes	Yes
Logging/Monitoring		
Syslog (multiple servers)	Yes	Yes
Email (two addresses)	Yes	Yes
NetIQ WebTrends	Yes	Yes
SNMP (v2)	Yes	Yes
SNMP full/custom MIB	Yes	Yes
Traceroute	Yes	Yes
VPN tunnel monitor	Yes	Yes
External Flash		
Additional log storage	Supports 1 GB or 2 GB industrial-grade SanDisk	Supports 1 GB or 2 GB industrial-grade SanDisk
Event logs and alarms	Yes	Yes
System configuration script	Yes	Yes
ScreenOS Software	Yes	Yes
Dimensions and Power		
Dimensions (W x H x D)	17.5 X 3.4 X 20 in (44.5 X 8.6 X 50.8 cm)	17.5 X 8.6 X 14 in (44.5 X 21.8 X 35.6 cm)
Weight	37 lb / 17 kg	45 lb / 20 kg
Rack mountable	Yes, 2U	Yes, 5U
Power supply (AC)	Yes, redundant, 100-240 VAC	Yes, redundant, 100-240 VAC
Power supply (DC)	Yes, redundant, -36 to -60 VDC	Yes, redundant, -36 to -60 VDC
Maximum thermal output	472 BTU/hour (W)	943 BTU/hour (W)
Certifications		
Safety certifications	UL, CUL, CSA, CB, Austel, NEBS Level 3	UL, CUL, CSA, CB, Austel, NEBS Level 3
EMC certifications	FCC class A, CE class A, C-Tick, VCCI class A	FCC class A, CE class A, C-Tick, VCCI class A
NEBS	Yes	Yes
MTBF (Bellcore model)	7.9 years	7.0 years

	NetScreen-5200	NetScreen-5400
Security Certifications		
Common Criteria: EAL4 and EAL4+	Yes, MGT2 / 8G2 / 2XGE	Yes, MGT2 / 8G2 / 2XGE
FIPS 140-2: Level 2	Yes, MGT2 / 8G2 / 2XGE	Yes, MGT2 / 8G2 / 2XGE
ICSA Firewall and VPN	Yes	Yes
Operating Environment		
Operating temperature	32° to 105° F (0° to 45° C)	32° to 105° F (0° to 45° C)
Non-operating temperature	- 4° to 158° F (-20° to 70° C)	- 4° to 158° F (-20° to 70° C)
Humidity	10% to 90% noncondensing	10% to 90% noncondensing

(1) Performance, capacity and features listed are based upon systems running ScreenOS 6.2 and are the measured maximums under ideal testing conditions unless otherwise noted. Actual results may vary based on ScreenOS release and by deployment. Please note the firewall/VPN performance data are identical for MGT2/SPM2 and MGT3/SPM3 configurations. For a complete list of supported ScreenOS versions for NetScreen Series Security Systems, please visit the Juniper Customer Support Center (**www.juniper.net/customers/support/**).

(2) Listed first, higher performance numbers are achieved with 2XGE, lower numbers with the 8G2 Secure Port Modules.

(3) Shared among all virtual systems.

(4) IPS/Deep Inspection is delivered by annual subscriptions purchased separately from Juniper Networks. Annual subscriptions provide signature updates and associated support.

(5) Redirect Web filtering sends traffic to a secondary server and therefore entails purchasing a separate Web filtering license from either Websense or SurfControl.

(6) Requires purchase of virtual system key. Every virtual system includes one virtual router and two security zones, usable in the virtual or root system.

(7) NAT, PAT, policy-based NAT, virtual IP, mapped IP, virtual systems, virtual routers, VLANs, OSPF, BGP, RIPv2, Active/Active HA, and IP address assignment are not available in layer 2 transparent mode.

(8) Not available with virtual systems.

(9) 512K or 1 million sessions per SPM can be achieved (2 ASICs per SPM), depending on inter-ASIC or intra-ASIC traffic flow respectively. 1 million sessions max on NetScreen-5200 and 2 million sessions max on NetScreen-5400.

(10) Two million sessions requires at least two Secure Port Modules (8G2 or 2XGE).

(11) The first numbers are performance achieved with the new MGT3/8G2-G4 modules, and the second numbers represent the performance achieved with the MGT2/8G2 modules.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

Model Number	Description
NetScreen-5200	
NS-5200	NS-5200 system, no SPM or MGT modules, includes fan tray, dual AC power supply, 19" rack mount, 0 VSYS
NS-5200-DC	NS-5200 system, no SPM or MGT modules, includes fan tray, dual DC power supply, 19" rack mount, 0 VSYS
Note: Add Management and SPM Modules to build complete systems	
NetScreen-5400	
NS-5400	NS-5400 system, no SPM or MGT modules, includes fan tray, 3 x AC power supply, 19" rack mount, 0 VSYS
NS-5400-DC	NS-5400 system, no SPM or MGT modules, includes fan tray, 3 x DC power supply, 19" rack mount, 0 VSYS
Note: Add Management and SPM Modules to build complete systems	

Model Number	Description
NetScreen Series – Components needed to build complete systems	
NS-5000-MGT2	Management Module 2
NS-5000-2XGE	2 x 10GbE Secure Port Module (SPM) – does NOT include transceivers
NS-5000-8G2	8 x GbE Secure Port Module 2 (SPM) – includes 8 x transceivers (SX)
NS-5000-8G2-TX[2]	8 x GbE Secure Port Module 2 TX (SPM) – includes 8 x Gig copper transceivers
NS-5000-MGT3[1]	Management Module 3
NS-5000-2XGE-G4[1]	2 x 10GbE Secure Port Module (SPM) – does NOT include transceivers
NS-5000-8G2-G4[1]	8 x GbE Secure Port Module (SPM) – includes 8 x transceivers (SX)
NS-5000-8G2-G4-TX[2]	8 x GbE Secure Port Module (SPM) – includes 8 x Gig copper transceivers

Model Number	Description
NetScreen Series – Virtual System Upgrades	
NS-5000-VSYS-5	VSYS upgrade 0 to 5
NS-5000-VSYS-25	VSYS upgrade 5 to 25
NS-5000-VSYS-50	VSYS upgrade 25 to 50
NS-5000-VSYS-100	VSYS upgrade 50 to 100
NS-5000-VSYS-250	VSYS upgrade 100 to 250
NS-5000-VSYS-500	VSYS upgrade 250 to 500
NS-5000-VSYS	VSYS upgrade 0 to 500
NetScreen Series – Accessories	
NS-SYS-GBIC-MSX	SX transceiver (mini-GBIC)
NS-SYS-GBIC-MLX	LX transceiver (mini-GBIC)
NS-SYS-GBIC-MXSR	XFP 10GbE transceiver Short Range (SR) (300 m)
NS-SYS-GBIC-MXLR	XFP 10GbE transceiver Long Range (LR) (10 km)
NetScreen-5200 – Components	
NS-5200-CHA	NetScreen-5200 chassis
NS-5200-PWR-AC	NetScreen-5200 AC power supply
NS-5200-PWR-DC	NetScreen-5200 DC power supply
NS-5200-FAN	NetScreen-5200 fan assembly
NetScreen-5400 – Components	
NS-5400-CHA	NetScreen-5400 chassis
NS-5400-PWR-AC	NetScreen-5400 AC power supply
NS-5400-PWR-DC	NetScreen-5400 DC power supply
NS-5400-FAN	NetScreen-5400 fan assembly

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPER NETWORKS