

NetScreen-5000 Series



NETSCREEN®
Scalable Security Solutions



At a glance

- **Multi-function security system**

Integrated network security solution with stateful inspection firewall, robust Denial of Service (DoS) protections, high performance IPSec VPN, and traffic management capabilities

- **Modular, chassis-based systems**

Family of purpose-built, high performance, integrated security systems offering flexible and scalable solutions for large enterprises and carriers

- **Industry leading performance**

Firewall performance scales to 12 Gbps and VPN performance to 6 Gbps

- **Virtualization**

Logical partitioning of the system into separate entities for traffic, policy, and management segmentation enables multi-departmental or multi-customer security enforcement from a single system

Product overview

The NetScreen-5000 Series is a line of purpose built, high-performance security systems designed to deliver a new level of high-performance capabilities for large enterprise, carrier, and data center networks. The NetScreen-5000 Series consists of two products, the 2-slot NetScreen-5200 and the 4-slot NetScreen-5400. The NetScreen-5000 Series security systems integrate firewall, DoS and DDoS protection, VPN, and traffic management functionality in low-profile modular chassis.

Built around NetScreen's third generation security ASIC and distributed system architecture, the NetScreen-5000 Series offers excellent scalability and flexibility while providing high levels of security through NetScreen's custom operating system, NetScreen ScreenOS. The NetScreen-5000 Series employs a switch fabric for data exchange and separate multi-bus channel for control information, delivering scalable performance for the most demanding environments.

NetScreen's GigaScreen-II ASIC

NetScreen's third-generation security ASIC, the GigaScreen-II, is capable of independent operation and can provide advanced functionality at gigabit throughput rates as a full packet-processing engine, including packet parsing, classification, encryption, decryption, Network Address Translation (NAT) and session matching. Combined with its ability to directly connect internally to switch fabrics, the GigaScreen II delivers a truly scalable security solution in NetScreen-5000 systems.

Secure Port Modules (SPM)

The NetScreen-5000 Series offers two Secure Port Modules, the 8 GigE SPM and the 2 GigE 24FE SPM, providing highly flexible solutions for varying network requirements. Both modules are built around the GigaScreen-II ASIC to provide

accelerated stateful inspection firewall and IPSec VPN capabilities. Individual ports may also be combined into trunk groups using Link Aggregation to deliver multi-gigabit connections to adjacent network elements.

Management module

Each product in the NetScreen-5000 Series is equipped with a management module providing overall control and configuration of the system. Access to management functions is provided through two serial ports and one 10/100 Ethernet port dedicated to management functions. Comprehensive management options may also be accessed in-band through one or more interfaces on the secure port modules. The management module additionally provides external compact flash for general storage of logs, configurations, and firmware images, as well as two dedicated GigE ports for High Availability (HA) traffic when used in redundant network topologies.

NetScreen ScreenOS

NetScreen ScreenOS firmware powers the entire system. At its core is a custom-designed, real time operating system built from the outset to deliver a very high level of security and performance. ScreenOS provides an integrated, easy-to-use platform for its many functions, including:

- ICSA certified stateful inspection firewall
- ICSA certified IPSec VPN gateway
- Virtualization of security, network, and management functions
- High Availability to ensure maximum network reliability
- Rich set of management interfaces, including CLI, WebUI, and centralized management
- Transparent, Route, and NAT modes and VLAN support to ease integration of security into existing networks

Firewall

NetScreen's full-featured firewall uses stateful inspection-based technology to provide security against external and internal attacks. All interfaces – physical and virtual – support Denial of Service (DoS) and attack mitigation features. This provides added flexibility and security for today's networks through:

- Fully integrated solution with security-optimized hardware, operating system, and firewall providing a higher level of security and performance than loosely-coupled software-based solutions
- Extensive DoS and attack prevention capabilities including SYN attack, ICMP flood, Port Scan, and others; combined with hardware accelerated session initiation, provides protection even in high-stress network environments
- Route mode – standard Layer 3 mode of operation
- NAT, Port Address Translation (PAT) – which shield internal, non-routable IP addresses
- Transparent mode – where the device functions as a Layer 2 IP security bridge

Virtual Private Network (VPN)

In addition to a stateful inspection firewall, the NetScreen-5000 Series is a full-featured VPN solution. VPN tunnels can be initiated and/or terminated on any interface, allowing advanced VPN deployments, such as securing wireless LANs with IPSec for encryption and authentication. The integrated nature of the ScreenOS allows VPN traffic to be fully inspected after decryption and then encrypted again, if necessary, for final delivery. The NetScreen-5000 Series delivers robust VPN solutions, providing support for redundant, reliable IPSec VPN networks (in addition to High Availability between two devices), including:

- Redundant VPN gateways, allowing an administrator to configure multiple gateway definitions for a given VPN tunnel with automated fail-over of gateways when one becomes unreachable
- VPN tunnel interfaces allowing dynamic routing to choose the appropriate tunnel based on routing decisions
- Comprehensive remote access VPN support, including support for XAUTH for user authentication of dial-up users

Virtualization (Virtual Systems, VLANs, and Security Zones)

NetScreen's security systems provide several virtualization features allowing logical partitioning of the system into separate security domains for traffic, policy, and management separation. Traffic segmentation is achieved at the interface level, through 802.1Q VLANs, or with IP address subnets. Security Zones group interfaces (both virtual and/or physical) into an internal, logical network. Policies are then applied between zones or within each Security Zone between interfaces. Virtual Systems add an additional layer of segmentation, allowing the NetScreen-5000 Series to be partitioned into multiple security domains, each with a unique set of administrators, policies, VPNs, and address books. Together, these virtualization techniques allow multiple customers or enterprise departments to be secured by a single system for simplified deployment and management without sacrificing the security of separate devices.

High Availability

The NetScreen-5000 Series provides the most comprehensive integrated High Availability solution available for security solutions today. With the NetScreen Redundancy Protocol (NSRPv2), the NetScreen-5000 Series can be deployed in fully meshed network environments as well as in Active/Active (load sharing) redundancy groups with stateful firewall and VPN fail-over. Benefits include:

- Sub-second fail-over between interfaces or devices
- Active/Active provides for higher burst capacity than Active/Passive, and ensures both devices are working properly and passing traffic
- Full mesh configurations allow for redundant physical paths in the network
- Provides leaderless clustering to prevent a single point of failure

Note: Active/Active High Availability available with ScreenOS 4.0

Traffic Management

The NetScreen-5000 provides hardware rate limiting for each secure port module interface, allowing network administrators to ensure that bandwidth is properly shared at aggregation points in the network. The DiffServ stamp in IP headers can be set under policy control, allowing the classification engine to provide QoS information about individual packets to the remainder of the network.

Comprehensive management

NetScreen's security systems include robust management capabilities, allowing network administrators to securely and cost affectively manage up to 10,000 devices and thousands of remote VPN clients. Since VPN functionality is built-in, all management can be encrypted for truly secure remote management. Management capabilities and features include:

- Browser-based management with the built-in WebUI (HTTP and HTTPS)
- Command Line Interface (CLI) accessible via Secure Command Shell (SSH v1.5 compatible), Telnet, and console port
- E-mail alerts, SNMP alarms
- Integration with Syslog or WebTrends™ for external logging, monitoring, and analysis
- Up to 20 administrators with three levels of access: root admin, admin, and read-only, with more granular control available when used in conjunction with NetScreen's policy based management, NetScreen-Global PRO and NetScreen-Global PRO Express
- A unique administrative login per Virtual System, allowing a root administrator to partition management access to the WebUI or CLI
- Policy-based centralized management and monitoring using NetScreen-Global PRO or NetScreen-Global PRO Express*

**Supported with the NetScreen-5200 8G today; supported in the future with the NetScreen-5200 2G24FE and the NetScreen-5400*

NetScreen-5000 Series Performance

Feature	NetScreen-5200 8G ⁽¹⁾	NetScreen-5200 2G24FE ⁽²⁾	NetScreen-5400 ⁽²⁾
Concurrent sessions	1,000,000	1,000,000	1,000,000
New sessions/second	25,000	23,000	21,000
Firewall performance	Up to 4 Gbps	Up to 2 Gbps	Up to 12 Gbps
3DES (168 bit) performance	Up to 2 Gbps	Up to 1 Gbps	Up to 6 Gbps
Policies	40,000 ⁽⁴⁾	40,000 ⁽⁴⁾	40,000 ⁽⁴⁾
Number of slots	2	2	4
Traffic interfaces	8 mini-GBIC (SX or LX)	2 mini-GBIC (SX or LX) and 24 10/100	Up to 24 mini-GBIC (SX or LX) or 6 mini-GBIC (SX or LX) and 72 10/100

NetScreen-5000 Series Features ⁽³⁾

Virtualization

Maximum number of Virtual Systems	500
Maximum number of Security Zones	1,000
Maximum number of Virtual Routers	500
Number of VLANs supported (8G SPM)	4,000 max; 500 per port
Number of VLANs supported (2G24FE SPM)	1,254 max; 500 per GigE port/254 shared among 24 10/100 ports

Mode of Operation

Transparent mode	Yes
Route mode	Yes
NAT (Network Address Translation)	Per interface
Policy-based NAT	Yes
PAT (Port Address Translation)	Yes
Virtual IP	8 ⁽⁷⁾
Mapped IP	10,000 ⁽⁴⁾
Users per port	Unrestricted

Routing

Number of Virtual Routers	2 default, up to 500 (requires Virtual System license key)
OSPF/BGP	ScreenOS 4.0 and later, up to 8 up instances each ⁽⁴⁾
Routes	20,000 ⁽⁴⁾

Network Attack Protection⁽⁶⁾

Number of attacks detected	31 with ScreenOS 4.0 28 with ScreenOS 3.1
DoS and DDoS protections	Yes
Malformed packet protections	Yes
Malicious URL protections	Yes
Network attack protections configurable per zone	Yes

VPN

Dedicated VPN tunnels	25,000 ⁽⁴⁾
Manual Key, IKE, PKI (X.509)	Yes
AES, 3DES (168-bit) and DES (56-bit) encryption	Yes
Perfect forward secrecy (DH Groups)	1,2,5
Prevent replay attack	Yes
Remote access VPN	Yes
L2TP within IPSec	Yes
Site-to-site VPN	Yes
Star (hub and spoke) VPN network topology	Yes
IPSec NAT Traversal	Yes
Tunnel interfaces	1,024
Redundant VPN gateways	Yes

IPSec Authentication

SHA-1	Yes
MD5	Yes
PKI Certificate requests (PKCS 7 and PKCS 10)	Yes
Automated certificate enrollment (SCEP)	Yes
Online Certificate Status Protocol (OCSP)	Yes

Certificate Authorities supported

VeriSign CA	Yes
Entrust CA	Yes
Microsoft CA	Yes
RSA Keon CA	Yes
iPlanet (Netscape) CA	Yes
Baltimore CA	Yes
DOD PKI CA	Yes

Firewall and VPN User Authentication

Built-in (internal) database-user limit	25,000
RADIUS (external) database	Yes
RSA SecurID (external) database	Yes
LDAP (external) database	Yes
RADIUS authentication accounting	Yes
XAUTH VPN authentication	Yes
Web-based authentication	Yes

Traffic Management

Maximum bandwidth	Yes, per physical interface
DiffServ stamp	Yes, per policy

High Availability (HA)

Active/Active or Active/Passive High Availability with NSRPv2	Active/Active w/ScreenOS 4.0 Active/Passive w/ScreenOS 3.1
Redundant interfaces/full mesh	Yes, w/ScreenOS 4.0
Session protection for firewall and VPN	Yes
Device failure detection	Yes
Link failure detection	Yes
Path monitoring	Yes
Network notification on fail-over	Yes
Authentication for new HA Members	Yes
Encryption of HA Traffic	Yes

System Management

WebUI (HTTP and HTTPS)	Yes
Command Line Interface (console)	Yes
Command Line Interface (telnet)	Yes
Secure Command Shell (SSH v1.5 compatible)	Yes
NetScreen-Global PRO	Yes, w/ScreenOS 4.0
NetScreen-Global PRO Express	Yes, w/ScreenOS 4.0
All management via VPN tunnel on any interface	Yes
SNMP full custom MIB	Yes

Administration

Multiple administrators	Yes, up to 20
Remote administrator database	RADIUS/LDAP/SecurID
Administrative networks	6
Root admin, admin, and read only user levels	Yes
Software upgrades and configuration changes	TFTP/WebUI/Global
Schedules	256

Logging/Monitoring

Syslog	External
E-mail (2 addresses)	Yes
NetIQ WebTrends	External
SNMP	Yes
Traceroute	Yes
VPN tunnel monitor	Yes
Websense URL filtering	External

External Flash

CompactFlash™	128 or 512 MB Sandisk
Event logs and alarms	Yes
System config script	Yes
ScreenOS software	Yes

(1) Performance, capacity, and features provided with ScreenOS 4.0.0r2. May vary with other ScreenOS releases.

(2) Performance, capacity, and features provided with ScreenOS 3.1.0r1. May vary with other ScreenOS releases.

(3) Specifications and features apply to all versions of ScreenOS, except were noted.

(4) Shared among all Virtual Systems.

(5) Supported with the NetScreen-5200 8G today; supported in the future with the NetScreen-5200 2G24FE and the NetScreen-5400

(6) See NetScreen product documentation for a complete list of network attack protections.

(7) Not available with Virtual Systems.

Specifications and Ordering Information

Specifications:

NetScreen-5000 Standards Supported

ARP, TCP/IP, UDP, ICMP, HTTP, HTTPS, RADIUS, IPSec (IPESP, IPAH), MD5, SHA1, DES, 3DES, AES, IKE, OSPF, BGP, TFTP (client), SNMP, X.509v3, VLAN 802.1Q

NetScreen-5200 Physical and Environmental

3.4" x 19" by 20" (H x W x D) chassis

19", 2U rack mountable enclosure, front and rear or mid mount options

Rear access for power supply, all other access from front

Operating Temperature: 0 to 40 degrees C, 32 to 105 degrees F

Non-operating temperature: -20 to 70 degrees C, -4 to 158 degrees F

Humidity: 10 to 90%, non-condensing

Maximum heat dissipation: 511 BTU/hour (150 watts)

Average heat dissipation: 297 BTU/hour (87 watts)

Weight: 37 pounds

AC Power

Input Voltage: 90 to 264 VAC

Input Frequency: 47 to 63 HZ, auto-ranging

Maximum Input Current: 3A at 100 VAC

Maximum output: 150 watts DC

DC Power

Input Voltage: -36 to -60 VDC

Nominal Input Voltage: -48 VDC

Maximum Input Current: 6A at -36 VDC

Maximum output: 150 watts DC

NetScreen-5400 Physical and Environmental

8.6" x 19" by 14" (H x W x D) chassis

19", 5U rack mountable enclosure

Front mountable

All components front accessible

Operating Temperature: 0 to 45 degrees C, 32 to 113 degrees F

Non-operating temperature: -20 to 70 degrees C, -4 to 158 degrees F

Humidity: 10 to 90%, non-condensing

Maximum heat dissipation: 1,023 BTU/hour (300 watts)

Average heat dissipation: 713 BTU/hour (209 watts)

Weight: 45 pounds

NetScreen-5200 Certifications

GR-63-Core: NEBS, Environmental Testing Physical Protection

GR-1089-Core: EMC and Electrical Safety for Network

Telecommunications Equipment

Safety

UL, CUL, CSA, CB, Austel

Emissions

FCC class A, BSMI, CE class A, C-Tick, VCCI class A

NetScreen-5400 Certifications

GR-63-Core: NEBS, Environmental Testing Physical Protection

GR-1089-Core: EMC and Electrical Safety for Network

Telecommunications Equipment

Safety

UL, CUL, CSA, CB, Austel

Emissions

FCC class A, BSMI, CE class A, C-Tick, VCCI class A

Ordering information:

Product

Part Number

NetScreen-5200 Bundles

NetScreen-5200, 1 2G24FE SPM, 0 VSYS, AC

NS-5200-P00A-S00

NetScreen-5200, 1 2G24FE SPM, 0 VSYS, DC

NS-5200-P00D-S00

NetScreen-5200, 1 8G SPM, 0 VSYS, AC

NS-5200-P01A-S00

NetScreen-5200, 1 8G SPM, 0 VSYS, DC

NS-5200-P01D-S00

NetScreen-5200, 1 8G SPM, 100 VSYS, AC

NS-5200-P01A-S01

NetScreen-5200, 1 8G SPM, 100 VSYS, DC

NS-5200-P01D-S01

NetScreen-5200, 1 8G SPM, 500 VSYS, AC

NS-5200-P01A-S02

NetScreen-5200, 1 8G SPM, 500 VSYS, DC

NS-5200-P01D-S02

NetScreen-5400 Bundles

NetScreen-5400, 1 2G24FE SPM, 0 VSYS, AC

NS-5400-P00A-S00

NetScreen-5400, 1 2G24FE SPM, 0 VSYS, DC

NS-5400-P00D-S00

NetScreen-5400, 1 8G SPM, 0 VSYS, AC

NS-5400-P01A-S00

NetScreen-5400, 1 8G SPM, 0 VSYS, DC

NS-5400-P01D-S00

NetScreen-5400, 1 8G SPM, 100 VSYS, AC

NS-5400-P01A-S01

NetScreen-5400, 1 8G SPM, 100 VSYS, DC

NS-5400-P01D-S01

NetScreen-5400, 1 8G SPM, 500 VSYS, AC

NS-5400-P01A-S02

NetScreen-5400, 1 8G SPM, 500 VSYS, DC

NS-5400-P01D-S02

Virtual Systems

NetScreen-5000 VSYS Upgrade 0 to 5

NS-5000-VSYS-5

NetScreen-5000 VSYS Upgrade 5 to 25

NS-5000-VSYS-25

NetScreen-5000 VSYS Upgrade 25 to 50

NS-5000-VSYS-50

NetScreen-5000 VSYS Upgrade 50 to 100

NS-5000-VSYS-100

NetScreen-5000 VSYS Upgrade 100 to 250

NS-5000-VSYS-250

NetScreen-5000 VSYS Upgrade 250 to 500

NS-5000-VSYS-500

NetScreen-5000 VSYS Upgrade 0 to 500

NS-5000-VSYS

NetScreen-5000 Components

Management Module

NS-5000-MGT

8G (8 mini-GBIC) Secure Port Module (SPM)

NS-5000-8G

2G24FE (2 mini-GBIC 24 10/100) SPM

NS-5000-2G24FE

mini-GBIC transceiver - SX

NS-SYS-GBIC-MSX

mini-GBIC transceiver - LX

NS-SYS-GBIC-MLX

NetScreen-5200 Components

NetScreen-5200 Chassis

NS-5200-CHA

NetScreen-5200 AC Power Supply

NS-5200-PWR-AC

NetScreen-5200 DC Power Supply

NS-5200-PWR-DC

NetScreen-5200 Fan Assembly

NS-5200-FAN

NetScreen-5400 Components

NetScreen-5400 Chassis

NS-5400-CHA

NetScreen-5400 AC Power Supply

NS-5400-PWR-AC

NetScreen-5400 DC Power Supply

NS-5400-PWR-DC

NetScreen-5400 Fan Assembly

NS-5400-FAN

NetScreen-5400 Fan Assembly

NS-5400-FAN

NetScreen product warranty and services

NetScreen's standard warranty provides one year of hardware support, and 90 days of software support. A portfolio of annual maintenance offerings are available, and are recommended to ensure the system is kept updated with the latest software enhancements and to ensure high availability for end users. NetScreen also offers training and certifications programs as well as Professional Services for consulting, installation, and configuration support.

For more information about NetScreen services or products, please call toll-free 1-800-638-8296 in the US, +44 8700 750000 in Europe, 001-408-616-5973 in Latin America or 852-2519-3988 in Asia, or visit us at www.netscreen.com.

Copyright © 1998-2003 NetScreen Technologies, Inc.

NetScreen, NetScreen Technologies, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. IDP, MIMD, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote, GigaScreen ASIC, GigaScreen-II ASIC and NetScreen ScreenOS, and Stateful Signature are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Part Number: 2003.1.50.2.5000.web2



NETSCREEN®
Scalable Security Solutions

805 11th Avenue
Building 3
Sunnyvale, California 94089
Phone: 408.543.2100
Fax: 408.543.8200

www.netscreen.com

