NetScreen-5000 Series

NETSCREEN®
Scalable Security Solutions

At a glance

- **Multi-function Security System**

  Integrated network security solution with stateful inspection firewall, robust 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

- **Virtual Systems**

  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 of purpose-built, high-performance security systems, including the 2-slot NetScreen-5200 and 4-slot NetScreen-5400, delivers a new level of high-performance capabilities for large enterprise, carrier, and data center networks. Built around NetScreen's third-generation security ASIC technology and distributed system architecture, the NetScreen-5000 Series offers excellent scalability and flexibility in network security systems.

The NetScreen-5000 system architecture includes multiple processing modules that work together to deliver a range of security gateway interface and performance configurations. Available modules include security processing modules in a variety of port configurations and a management module for overall system control. These modules may be combined in different ways, allowing customization of the system to the specific customer environment. 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.

All NetScreen-5000 Series systems contain fault tolerant components for high reliability. Hot-swappable, load-sharing power supplies provide N+1 redundancy. The fan assembly offers redundant fans in a hot-swappable module with replaceable air filter.

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, 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 module

Built around one or more GigaScreen-II ASICs, each secure port module provides the core stateful inspection and IPSec VPN capabilities for traffic through any of its network interfaces. Individual ports may also be combined into trunk groups using Link Aggregation to deliver multi-gigabit connections to adjacent network elements. A variety of configurations are available for various combinations of 10/100 Mbps and gigabit Ethernet (GigE) interfaces and security processing capacity. This capability enables scaled solutions through additional secure port modules, while freeing the management module to focus on overall system control functions.

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. Optimized to deliver the best performance on all NetScreen security appliances and systems, NetScreen 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, both internal and external

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-prevention 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
- Network Address Translation (NAT), Port Address Translation (PAT)—which shield internal, non-routable IP addresses—as well as 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 is a full-featured VPN solution. VPN tunnels can be initiated and/or terminated on any interface, allowing advanced VPN deployments. The integrated nature of the ScreenOS allows VPN traffic to be fully inspected after decryption and then encrypted again, if necessary, for final delivery. Large enterprises can, for example, secure several network segments with a single system, providing privacy through encryption, such as wireless LAN segments, while still inspecting traffic between segments.

The NetScreen-5000 functions equally well in a carrier environment as a gateway between networks, or to terminate secure mobile or wireless WAN connections on one side and VPN connections to customers' networks on the other. The solution also delivers:

- Comprehensive remote-access VPN support
- Extensive site-to-site VPN capabilities

Virtualization (Virtual Systems, VLANs, and Security Zones)

NetScreen's security systems provide several virtualization features allowing logical partitioning of the system into separate entities for traffic, policy, and management separation. Traffic separation is achieved at the interface level through 802.1Q VLANs for ease of integration into the switched network. Security zones group interfaces—both virtual and/or physical—into an internal, logical network. Policy is then applied between zones, allowing similar traffic from multiple interfaces to be easily controlled in a single policy specification. Finally, to fully segment traffic and administrative functions in the device so it functions like a set of independent devices, Virtual Systems may be created to represent multiple logical devices. Together, these virtualization features 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

A pair of NetScreen-5000 systems can synchronize all configuration information, active firewall session tables, and VPN connections for redundant, fault-tolerant network designs. When deploying Active/Passive configurations of two identical devices, even the failure of one device results in near-zero interruption to network operations. The NetScreen-5000 Series will support NetScreen's NSRPv2 High Availability solution in Q3, 2002. This enhanced solution delivers Active/Active capability for sub-second fail over and participation in full mesh network topologies. Unlike many other security products in the market, High Availability is a standard feature in NetScreen security systems.

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 support, allowing network administrators to securely manage the devices. Since VPN functionality is built-in, all management can be encrypted for truly secure remote management. Management features include:

- *Browser-based management with the built-in Web UI (HTTP and HTTPS)*

- *Command line interface (CLI) accessible via Secure Command Shell (SSH v.1 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 3 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*

- *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 (available in second half of 2002)*

NetScreen-5000 Series Performance [1]

Feature	NetScreen-5200	NetScreen-5400
Concurrent sessions	1,000,000 (2)	1,000,000 (2)
New sessions/second	25,000	25,000
Firewall performance	Up to 4 Gbps	Up to 12 Gbps
Triple-DES (168 bit) performance	Up to 2 Gbps	Up to 6 Gbps
Policies	40,000 (4)	40,000 (4)
Rules	200,000 (4)	200,000 (4)
Number of slots	2	4
Traffic interfaces	2 mini-GBIC (SX or LX) and 24 10/100 or 8 mini-GBIC (SX or LX)	Up to 6 mini-GBIC (SX or LX) and 72 10/100 or 24 mini-GBIC (SX or LX)

NetScreen-5000 Series Features [1]

Virtualization
Maximum number of Virtual Systems	500
Maximum number of Security Zones	1,000
Maximum number of Virtual Routers	500
Number of VLANs supported	4,000

Mode of Operation
Transparent mode (all interfaces)	Yes
Route mode (all interfaces)	Yes
NAT (Network Address Translation)	Per interface
Policy-based NAT	Yes
PAT (Port Address Translation)	Yes
Virtual IP	8 (6)
Mapped IP	4,000 (4)
IP routing—static routes	4,000 (4)
Users per port	Unrestricted

Firewall Attacks Detected (Per Interface)
SYN flood	Yes (3)
ICMP flood	Yes (3)
UDP flood	Yes (3)
Ping of death	Yes
IP spoofing	Yes
Port scan	Yes (3)
Land attack	Yes
Tear drop attack	Yes
Filter IP source route option	Yes
IP address sweep attack	Yes
WinNuke attack	Yes
Java/ActiveX/Zip/EXE	Yes
Default packet deny	Yes
User-defined Malicious URL	Yes, 64
Per-source session limiting	Yes
SYN fragments	Yes
SYN and FIN bit set	Yes
No flags in TCP	Yes
FIN with no ACK	Yes
ICMP fragment	Yes
Large ICMP	Yes
IP source route	Yes
IP record route	Yes
IP security options	Yes
IP timestamp	Yes
IP stream	Yes
IP bad options	Yes
Unknown protocols	Yes

Traffic Management
Guaranteed bandwidth	No
Maximum bandwidth	Yes
Priority-bandwidth utilization	No
DiffServ stamp	Yes

Firewall and VPN User Authentication
Built-in (internal) database - user limit	25,000
RADIUS (external) database	Yes
RSA SecureID (external) database	Yes
LDAP (external) database	Yes

External Flash
Compact Flash	128 or 512 MB Sandisk
Event logs and alarms	Yes
System config script	Yes
ScreenOS software	Yes

VPN
Dedicated VPN tunnels	25,000 (4)
Manual Key, IKE, PKI (X.509)	Yes
3DES (168-bit), AES (128-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

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

High Availability (HA)
Active/Active full mesh High Availability with NSRP v2	Future ScreenOS
Active/Passive full synchronization High Availability	Yes
Session protection for firewall and VPN	Yes
Device failure detection	Yes
Link failure detection	Yes
Network notification on failover	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 compatible)	Yes
NetScreen-Global PRO	Yes (5)
NetScreen-Global PRO Express	Yes (5)
All management via VPN tunnel on any interface	Yes
SNMP full custom MIB	Yes

Administration
Multiple administrators	20
Remote administrator database	RADIUS
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

---

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

(2) Minimum capacity with one secure port card, may vary with hardware configuration

(3) Physical interface only – virtual interfaces inherit physical interface properties

(4) Shared among all Virtual Systems

(5) NetScreen-5000 Series supported in NetScreen-Global PRO and NetScreen-Global PRO Express version 3.2

(6) Not available in Virtual Systems

Specifications:

NetScreen-5000 Standards Supported

ARP, TCP/IP, UDP, ICMP, HTTP, RADIUS, IPSec (IPESP, IPAH), MD5, SHA1, DES, 3DES, AES, IKE, 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: 510 BTU/hour (150 watts)

Average heat dissipation: 300 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

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

Ordering information:

Product	Part Number
NetScreen-5200 Bundles	
NetScreen-5200, 8 GigE SPM, 0 VSYS, AC	NS-5200-P01A-S00
NetScreen-5200, 8 GigE SPM, 0 VSYS, DC	NS-5200-P01D-S00
NetScreen-5200, 8 GigE SPM, 100 VSYS, AC	NS-5200-P01A-S01
NetScreen-5200, 8 GigE SPM, 100 VSYS, DC	NS-5200-P01D-S01
NetScreen-5200, 8 GigE SPM, 500 VSYS, AC	NS-5200-P01A-S02
NetScreen-5200, 8 GigE SPM, 500 VSYS, DC	NS-5200-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
8 GigE Secure Port Module (SPM)	NS-5000-8G
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

System packages and components including the NetScreen-5400 and/or the 24-port 10/100 secure port module will be available when those products are shipping.

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 products, call toll-free 1-800-638-8296 or visit us at www.netscreen.com

N E T S C R E E N ®

Scalable Security Solutions

350 Oakmead Parkway
Sunnyvale, CA 94085
Phone: 408.730.6000
Fax: 408.730.6200
www.netscreen.com

Part Number: 2002.4.50.1.5000