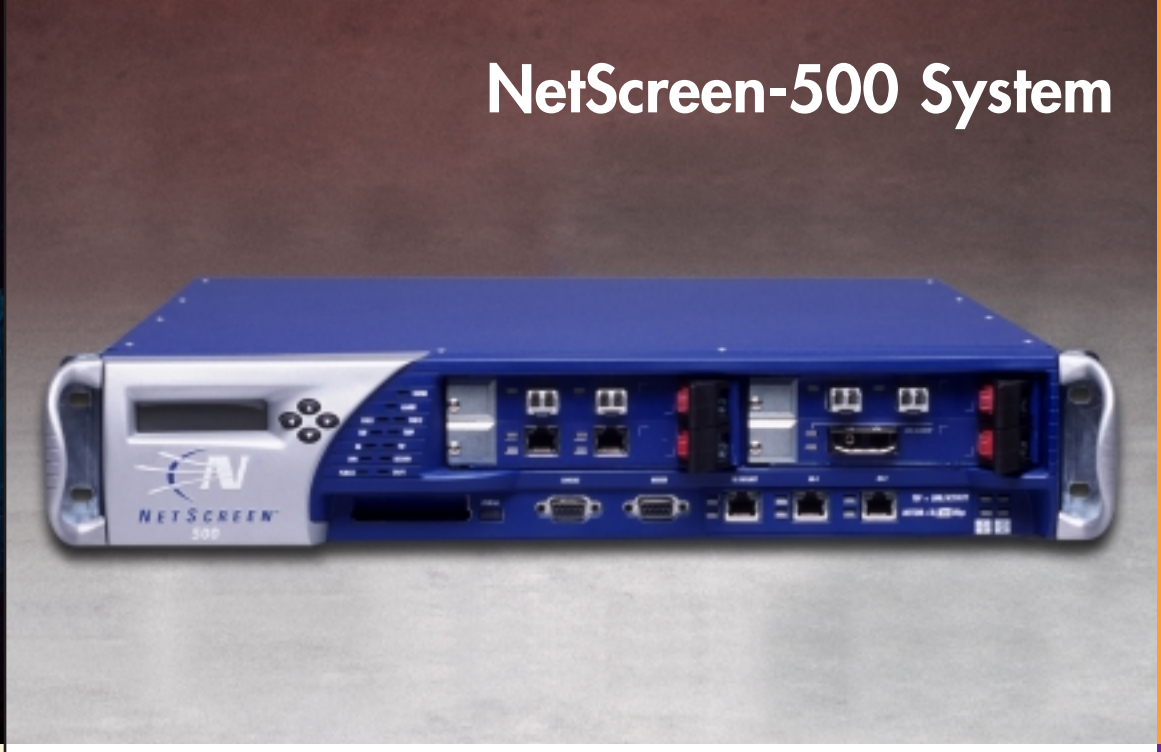
NetScreen-500 System



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, Flexible System**
  Purpose-built, high-performance, integrated security system offering flexible and scalable solutions for medium to large enterprises and carriers
- **Reliable Performance**
  Firewall performance scales to 700 Mbps and 3DES VPN performance to 250 Mbps, even under heavy traffic, large concurrent sessions, or a large number of VPN tunnels
- **Virtual Systems**
  Logical partitioning of the system into separate firewall and/or VPN domains for traffic, policy, and management segmentation enables multi-departmental or multi-customer security enforcement from a single system

Product overview

The NetScreen-500 is a purpose-built, high-performance security system designed to provide a flexible, high performance solution to medium and large enterprise central sites and service providers. The NetScreen-500 security system integrates firewall, VPN, and traffic management functionality in a low-profile, modular chassis.

The NetScreen-500 is built around NetScreen's custom, purpose-built GigaScreen ASIC, which provides accelerated encryption algorithms and policy look ups. In addition, there are two high speed busses to off-load management traffic from application traffic processing. This prevents High Availability and other management traffic from impacting throughput performance.

NetScreen's GigaScreen ASIC

NetScreen's GigaScreen security ASIC accelerates the firewall policy lookups and encryption and authentication algorithms in hardware, which is a significantly faster approach than in software and one that frees the CPU to manage data flow. This security-accelerating ASIC is tightly integrated with NetScreen's ScreenOS system software to eliminate unnecessary software layers and security holes found in security products built on general-purpose commercial operating systems.

Built-in management

The NetScreen-500 security system provides many built-in hardware features to enable extensive management of the device. Integral to the NetScreen-500 are two 10/100 Fast Ethernet High Availability (HA) interfaces, an out-of-band 10/100 Fast Ethernet management interface, a DB-9 console port, and a DB-9 modem port for an external modem. In addition, there is a built-in PCMCIA card for extra storage of additional configuration files and log files, and an LCD for device configuration and monitoring.

Interface modules

Three different interface modules are available on the NetScreen-500, designed to provide interface flexibility for varying network connectivity requirements and future growth requirements

- Dual port, 10/100 Fast Ethernet
- Single port, GBIC optical gigabit Ethernet
- Dual port, mini-GBIC optical gigabit Ethernet

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
- Traffic Management capabilities for maximizing limited bandwidth
- Virtualization of security, network, and management functions
- High Availability to ensure maximum network reliability
- Rich set of management interfaces, both internal and external
- Dynamic routing 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-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-500 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-500 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

Traffic management

The NetScreen-500 empowers a network administrator to monitor, analyze, and allocate bandwidth utilized by various types of network traffic in real-time, helping to ensure that business-critical traffic isn't impacted by web surfing or other non-critical applications. In service provider environments, this also allows an administrator to provide differentiated services when there is a shared connection.

Traffic Management is configurable on a per policy basis, based on IP address, user, application, or time of day. For each policy, guaranteed bandwidth, maximum bandwidth, and prioritization levels can be set. In addition, DiffServ packet marking is supported, allowing a NetScreen-500 to signal QoS to an MPLS network.

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 and Virtual Systems.

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-500 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-500 provides the most comprehensive integrated High Availability solution available for security solutions today. With the NetScreen Redundancy Protocol (NSRPv2), the NetScreen-500 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

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 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 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*

NetScreen-500 Features [1]

Performance	
Concurrent sessions	250,000
New sessions/second	17,000
Firewall performance	700 Mbps
3DES (168 bit) performance	250 Mbps
Policies	20,000 (2)
Traffic interfaces	Up to 8 10/100 or mini-GBIC (SX or LX), up to 4 GBIC (SX or LX)
Virtualization	
Maximum number of Virtual Systems	25
Maximum number of Security Zones	8 default, up to 50 custom
Maximum number of Virtual Routers	2 default, up to 25 custom
Number of VLANs supported	100
Mode of Operation	
Transparent mode (all interfaces)	Yes
Route mode (all interfaces)	Yes
NAT/PAT (all interfaces)	Yes
Policy-based NAT	Yes
Virtual IP	4 (4)
Mapped IP	4,000 – 256 per virtual system (2)
Users per port	Unrestricted
Routing	
OSPF/BGP	Yes, up to 8 instances each (2)
Static routes	Yes
Routes	8,192 (6)
Firewall Attacks Detected (per Security Zone)	
SYN attack	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	48
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	Yes
Maximum bandwidth	Yes
Priority-bandwidth utilization	Yes
DiffServ stamp	Yes
Firewall and VPN User Authentication	
Built-in (internal) database - user limit	15,000
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

VPN	
Dedicated VPN tunnels	10,000 (2)
Manual Key, IKE, PKI (X.509)	Yes
3DES (168-bit), AES (128, 192, 256-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
High Availability (HA)	
Active/Active or Active/Passive High Availability with NSRP v2	Yes
Redundant interfaces/full mesh	Yes
Session protection for firewall and VPN	Yes
Device failure detection	Yes
Link failure detection	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 (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/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	
PCMCIA (PC Card)	96 or 440MB, Type 2 & 3
Event logs and alarms	Yes
System config script	Yes
ScreenOS software	Yes

(1) Performance, capacity, and features as tested with NetScreen ScreenOS 4.0.0r1. May vary with other NetScreen ScreenOS releases.
(2) Shared among all Virtual Systems
(3) Physical interface only – virtual interfaces inherit these physical interface properties
(4) Not available with Virtual Systems
(5) NetScreen ScreenOS 4.0.0 supported in future release of NetScreen-Global PRO/PRO Express
(6) Share among all virtual routers

Specifications and Ordering Information

Specifications:

NetScreen-500 Standards Supported

ARP, TCP/IP, UDP, ICMP, HTTP, RADIUS, IPSec (IP-ESP, IP-AH), MD5, SHA1, DES, 3DES, AES, IKE, TFTP (client), SNMP, X.509v3, VLAN 802.1Q, OSPS, BGP

NetScreen-500 Physical and Environmental

3.5" x 17.5" by 17" (H x W x D) chassis

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

Rear access for power supply and fan module, all other access from front

Operating Temperature: 0 to 50 degrees C, 32 to 122 degrees F

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

Humidity: 10 to 90%, non-condensing

Maximum heat dissipation: 341 BTU/hour (100 watts)

Average heat dissipation: 300 BTU/hour (87 watts)

Weight: 27 pounds

MTBF: 6.5 years (Bellcore Model)

AC Power

Input Voltage: 90 to 264 VAC

Input Frequency: 47 to 63 HZ, auto-ranging

Maximum Output: 100 watts

DC Power

Input Voltage: -36 to -72 VDC

Nominal Input Voltage: -48 VDC

Maximum Output: 100 watts

NetScreen-500 Certifications

FIPS 140-1 Level 2

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-500SP Bundles	
NetScreen-500 system, SX GBIC, AC power	NS-500SP-GB1-AC
NetScreen-500 system, SX GBIC, DC power	NS-500SP-GB1-DC
NetScreen-500 system, SX dual-GBIC, AC power	NS-500SP-GB2-AC
NetScreen-500 system, SX dual-GBIC, DC power	NS-500SP-GB2-DC

SP Systems include 2 SX GBIC interface modules, 2 power supplies, fan module, and 25 Virtual Systems

NetScreen-500ES Bundles	
NetScreen-500 system, 2 SX GBIC modules, 2 AC power supplies	NS-500ES-GB1-AC
NetScreen-500 system, 2 SX GBIC modules, 2 DC power supplies	NS-500ES-GB1-DC
NetScreen-500 system, 2 SX dual-GBIC modules, 2 AC power supplies	NS-500ES-GB2-AC
NetScreen-500 system, 2 SX dual-GBIC modules, 2 DC power supplies	NS-500ES-GB2-DC
NetScreen-500 system, 3 dual-10/100 modules, 2 AC power supplies	NS-500ES-FE1-AC
NetScreen-500 system, 3 dual-10/100 modules, 2 DC power supplies	NS-500ES-FE1-DC
NetScreen-500 system, 2 dual-10/100 modules, 1 AC power supply	NS-500ES-FE2-AC
NetScreen-500 system, 2 dual-10/100 modules, 1 DC power supply	NS-500ES-FE2-DC

ES Systems include 2 or 3 interface modules, 1 or 2 power supplies, fan module, and 0 Virtual Systems

NetScreen-500 Virtual System Upgrades	
Upgrade to 5 Virtual Systems	NS-500-VSYS-5
Upgrade from 5 to 10 Virtual Systems	NS-500-VSYS-10
Upgrade from 10 to 25 Virtual Systems	NS-500-VSYS-25

Every Virtual System includes one virtual router and two security zones, usable in the virtual or root system

NetScreen-500 Spares	
GBIC interface module with SX transceiver	NS-500-HG1-SX
GBIC interface module with LX transceiver	NS-500-HG1-LX
Dual-port Mini GBIC interface module (SX)	NS-500-HG2-SX
Dual-port Mini GBIC interface module (LX)	NS-500-HG2-LX
Dual-port 10/100 interface module	NS-500-HF2
SX transceiver (GBIC)	NS-500-HSX
LX transceiver (GBIC)	NS-500-HLX
SX transceiver (Mini GBIC)	NS-SYS-GBIC-MSX
LX transceiver (Mini GBIC)	NS-SYS-GBIC-MLX
AC power supply	NS-500-PWR-AC
DC power supply	NS-500-PWR-DC
Fan module	NS-500-FAN

NetScreen product warranty and services

Every NetScreen product includes standard warranty features that assure the customer can deploy them confidently. E-mail based technical assistance is available on NetScreen appliances, systems and management products for one year. Hardware products come with a full year of standard RMA coverage in the unlikely event of failure. Both hardware and software products come with a short-term software service that provides any software feature releases or maintenance releases within 90 days of purchase.

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

NETSCREEN®

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

Part Number: 2002.6.50.1.500