

# NetScreen Security Systems



**NETSCREEN®**  
Scalable Security Solutions



## At a glance

### • Purpose-built, integrated security systems

*High-performance security systems running NetScreen ScreenOS and the GigaScreen ASIC to deliver market-leading performance of up to 2 Gbps throughput, and up to 25,000 VPN tunnels*

### • Managed security domains

*Using NetScreen's unique Virtual Systems feature, up to 250 security domains can be provided for managed security services or enterprise partitioning*

### • System resiliency

*Solid-state design, redundant hot-swap power supplies and hot-swap fans deliver maximum uptime within each system. High Availability software enables NetScreen's systems to be deployed in fully meshed network environments and in Active/Active (load sharing) redundancy groups with stateful fail-over*

### • Expandable solutions with flexible configuration options

*Several configurations to meet the requirements of single enterprise deployments to large multi-customer Internet data centers*

### • Easy to deploy

*Intuitive user interface, and integrated functionality without complex recurring licensing fees*

## NetScreen security systems overview

NetScreen Technologies offers a line of purpose-built, high-performance security systems, integrating both stateful-inspection firewall and VPN functionality with industry-leading performance. NetScreen's integrated security systems are resilient platforms, offering expandable solutions for large enterprises and service providers.

### Firewall security

NetScreen's full-featured firewall uses technology based on stateful inspection, securing against intruders and denial-of-service attacks.

- NetScreen ScreenOS is an ICSA-certified stateful inspection firewall
- Fully integrated solution with security-optimized hardware, operating system and firewall provides higher level of security and performance than loosely coupled software-based solutions
- Robust Denial-of-Service (DoS) and attack prevention 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) – as well as transparent mode, where the device works as a Layer 2 IP security bridge

### Virtual Private Networking (VPN)

Integrated into all NetScreen Security Systems is a full-featured VPN solution. They support site-to-site and remote access VPN applications.

- Network designs can blend full mesh with hub-and-spoke topologies to simplify configuration and management of remote office VPNs, while delivering redundant, high performance links between major sites
- NetScreen ScreenOS is VPNC-certified for IPSec interoperability
- Leverages ICSA-certified NetScreen ScreenOS on the NetScreen-100 for IPSec interoperability
- 3DES, AES and DES encryption, IKE with digital certificates (PKI X.509) or pre-shared secrets or manual key negotiation
- SHA-1 and MD5 strong authentication
- Policy-based NAT enables extranet VPN applications

### Virtual Systems

NetScreen's Virtual Systems allow for the creation of multiple security domains, each with its own address book, policies, and management. Virtual Systems are combined with 802.1q VLAN tags to extend the Security Domain throughout a switched network. The NetScreen-1000 or NetScreen-500 and the corresponding VLAN switch network can appear as a combined security system with up to 500 ports or 100, respectively.

- Using Virtual Systems, a NetScreen Security System can function as up to 250 virtual firewall/VPN gateways
- Expand service offerings in the Internet data center to include managed VPN and firewall on shared hardware platform

# NetScreen-1000

## The NetScreen-1000

The NetScreen-1000 Multi-Gigabit Security System is an integrated security system for the most demanding enterprise and service provider environments. NetScreen integrates firewall and VPN security functionality with gigabit Ethernet throughput. By combining parallel processing with the hardware acceleration of NetScreen's GigaScreen ASIC, the NetScreen-1000 delivers the highest performance needed for broadband data applications. The NetScreen-1000's scalable architecture ensures that customers are able to meet escalating bandwidth requirements, ensuring years of continued protection. The NetScreen-1000 can easily integrate into the most demanding environments.

## NetScreen-1000SP Service Provider System:

The NetScreen-1000SP is optimized for the data center service provider and application infrastructure provider markets. The NetScreen-1000SP is a fully populated NetScreen-1000 system with NetScreen's multi-customer software support for up to one hundred Virtual Systems (upgradeable to 250) and 500 VLANs. It comes complete with the chassis, switch module, six processor modules, auxiliary module, two power supplies, and full software functionality.

## NetScreen-1000ES Enterprise System:

The NetScreen-1000ES is optimized for single enterprises and smaller data centers requiring gigabit firewall and 600 Mbps VPN support for e-business and corporate headquarters. The NetScreen-1000ES is a partially populated system with four processing modules and five Virtual Systems. It can be upgraded with additional processing modules (up to 6) and additional Virtual Systems (25, 50, 100 or 250).

## The NetScreen-1000 architecture

The main components of the NetScreen-1000 are the Processor Modules, the Switch II Module and the Auxiliary Module. These modules are linked together via a passive back plane in a 19-inch rack mountable chassis and powered by redundant power supplies with individual power feeds. Each Module performs dedicated functions; the Processor Modules, powered by a RISC processor and NetScreen's GigaScreen ASIC, performs the packet classification, policy lookup and firewall and VPN packet processing. A fully equipped system contains up to six processors, providing additional capacity. The Switch Module provides a 6 Gbps data path to distribute the traffic across the multiple Processor Modules and also links to the gigabit Ethernet connection of the trusted and untrusted networks. The Auxiliary Module provides both management system interface and backup for the system.

The NetScreen-1000 includes the following hardware components:

- Chassis: 8 slots, 19-inch rack mountable
- Switch II Module: Provides redundant gigabit Ethernet untrusted ports (LX or SX GBIC), redundant gigabit Ethernet trusted ports (MT-RJ) and two gigabit High Availability interfaces
- Processor Module: Session management, firewall security and VPN
- Auxiliary Module: Management interface contains a separate out-of-band management port, and a console port
- Power supplies: Redundant DC or AC power supplies
- Swappable fan module

## The Power of ASICs

*NetScreen's GigaScreen security ASIC processes the firewall access policies and encryption 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 operating system and system software to eliminate unnecessary software layers and security holes found in other security products built on general-purpose commercial operating systems. By bringing security functionality to the system level, NetScreen has removed the overhead of extra platform layers that currently degrade the performance of other security products, which are typically PC-based or workstation-based solutions.*

## High Availability

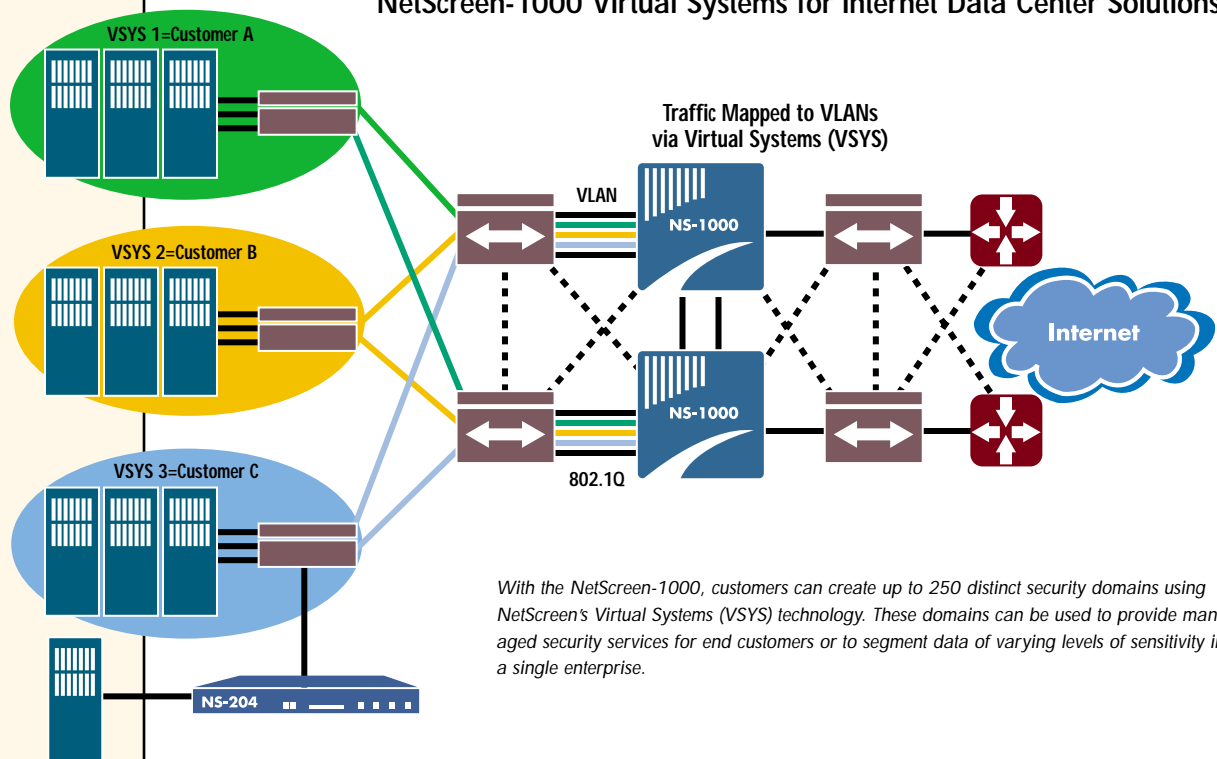
NetScreen Security Systems provide the most comprehensive High Availability solution available today. With the introduction of the NetScreen Redundancy Protocol (NSRP v2), NetScreen Systems can now be deployed in fully meshed network environments and in Active/Active (load sharing) redundancy groups with stateful fail-over.

When configured for High Availability, NetScreen Security Systems allow for the following capabilities and deployments:

- Stateful VPN and firewall fail-over
- Configurations are mirrored between HA group members to ensure proper behavior in case of a fail-over

- Redundant High Availability interfaces protecting against HA interface or link failures
- All active sessions and VPN tunnels are maintained across the HA group
- High Availability group status based on system health, link status with adjacent systems or path monitoring through adjacent systems to remote systems
- Failure detection and switching to the standby unit can be done in less than one second, independent of the number of active sessions and VPN tunnels
- Active/Active load sharing (in conjunction with stateful fail-over)
- Support for full mesh network topologies with monitored redundant Trust and Untrust connections

## NetScreen-1000 Virtual Systems for Internet Data Center Solutions



*With the NetScreen-1000, customers can create up to 250 distinct security domains using NetScreen's Virtual Systems (VSYS) technology. These domains can be used to provide managed security services for end customers or to segment data of varying levels of sensitivity in a single enterprise.*

# NetScreen-500

The NetScreen-500 Security System integrates firewall, VPN, and traffic management functionality in a low-profile, modular chassis. Using NetScreen's GigaScreen ASIC, the NetScreen-500 is capable of up to 700 Mbps firewall throughput, 250 Mbps 3DES VPN throughput, and supports 10,000 IPsec tunnels and up to 250,000 concurrent sessions. The NetScreen-500 is ideally suited for large enterprise environments with high bandwidth requirements or high capacity requirements, enterprise collocation facilities, and environments providing managed security services.

## NetScreen-500SP Service Provider System:

The NetScreen-500SP is optimized for environments providing managed security services. The NetScreen-500SP comes complete with two DC or AC power supplies, two GBIC or dual-GBIC interface modules, and software support for up to 25 Virtual Systems and 100 VLANs.

## NetScreen-500ES Enterprise System:

The NetScreen-500ES systems are optimized for large enterprise environments and collocation facilities requiring fast firewall and VPN performance, reliability, ease of management, and the potential to upgrade to 25 Virtual Systems. The NetScreen-500ES systems are offered with DC or AC power supplies and GBIC, dual-GBIC or dual-10/100 Fast Ethernet interface modules. All NetScreen-500ES systems can be upgraded to five, 10, or 25 Virtual Systems.

## The NetScreen-500 architecture

The NetScreen-500 is a high performance, reliable, and modular platform. To address high-performance requirements, the NetScreen-500 is designed around the custom, purpose-built GigaScreen ASIC, which provides accelerated encryption and policy look-ups. In addition, there are two processing busses to separate management traffic from traffic passing through the system. This prevents High Availability and other management traffic from impacting throughput performance. To address reliability, redundancy, and modularity requirements, the NetScreen-500 has minimal moving parts, unlike PC-based firewalls, and offers a hot-swappable fan module (made up of four fans), and redun-

dant power supplies. In addition, the NetScreen-500 can be set up in an Active/Active High-Availability topology in a full mesh with redundant links, with single links, or in an Active/Passive pair; all with fully synchronized firewall sessions and VPN tunnel information.

Summary of hardware components:

- Four interface module bays supporting GBIC, dual-Mini GBIC or dual-10/100 Fast Ethernet interface modules (up to 8 interfaces supported, mixes of interface types supported as well)
- Two DB9 serial ports, 1 for console and 1 for an external analog modem
- One 10/100 out-of-band management port
- Two redundant 10/100 High Availability ports
- Hot-swappable fan module
- Two redundant hot-swappable power supply trays accommodating AC or DC power
- LCD display for basic configuration and status alerts

All this, in a 2U, 19-inch rack mountable chassis.

## Programmable LCD eases deployment

The programmable LCD can be used to set basic system functionality, such as:

- Interface IP addresses, including the management interface
- Manageability options on those interfaces
- Alarm thresholds and status reports
- Can be disabled to prevent tampering with the device

## Traffic management

Traffic management allows a network administrator to monitor, analyze, and allocate bandwidth utilized by various types of network traffic in real time; ensuring business-critical traffic is never compromised for web surfing.

- Manage based on IP Address, user, application, or time of day
- Set guaranteed bandwidth and maximum bandwidth
- Prioritize traffic with eight prioritization levels
- Support for industry standard diffserv packet marking, allowing the NetScreen-500 to participate in an MPLS environment

## Robust, easy-to-use management

*NetScreen's security systems include robust management support, allowing a network administrator to securely manage the devices. Since VPN functionality is built in, all management can be encrypted for truly secure remote management.*

- Policy-based centralized management and monitoring using NetScreen-Global PRO or NetScreen-Global PRO Express
- 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
- Integrates with Syslog or NetIQ WebTrends™ for external logging, monitoring, and analysis
- Provides up to 20 administrators with 3 levels of access: root admin, admin, and read-only
- Virtual Systems provide a unique administrative login per Virtual System, allowing a root administrator to partition management access to the WebUI or CLI

**Firewall attack protections on every interface**

All interfaces support firewall denial-of-service and attack prevention features with NetScreen ScreenOS 3.1 and later, protecting against external and internal attacks. Each interface supports up to 28 attack preventions that are independently configurable per interface. This provides added flexibility and security for today's networks.

**VPN tunnels on any interface**

The NetScreen-500 with NetScreen ScreenOS 3.1 and later supports the ability to initiate and/or terminate IPSec VPN tunnels on any interface, allowing advanced VPN deployments. One critical application of this feature is in wireless LANs, where encryption can now be used to secure internal communications over wireless networks by terminating VPN tunnels on internal interfaces. Combined with firewall and user authentication services, networks can now be secured from unwanted access and wireless traffic can be encrypted to ensure privacy.

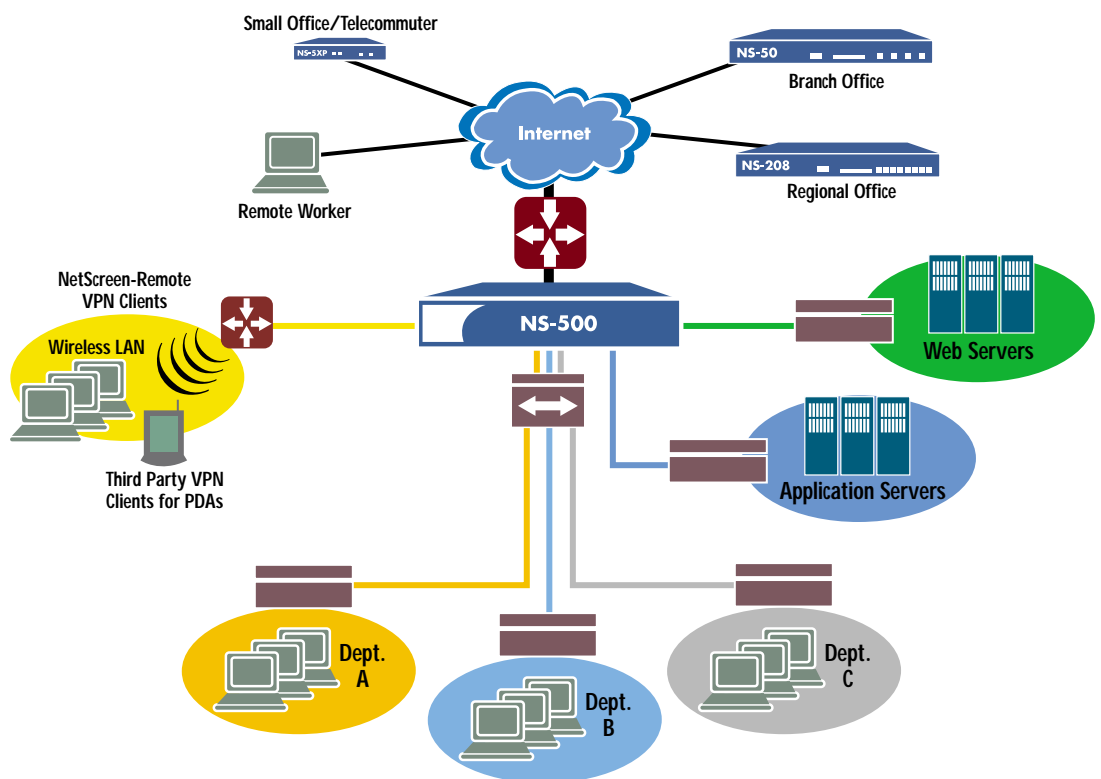
**Extranet VPN solutions**

NetScreen ScreenOS enables extranet VPN solutions by allowing content hosting companies and enterprises to easily establish security perimeters for customers and trading partners. Content hosts can now use what is known as Policy-based NAT to accept and differentiate individual customer's traffic. This enables traffic to access one or more servers even though the customer's private network addresses may be used by another customer. This is accomplished by applying security policies that translate each customer's address into distinct addresses that are recognizable by the central NetScreen device.

**Content filtering**

The NetScreen-500 can integrate with the NetIQ Websense™ content filtering solution to block inappropriate content and defer personal browsing to non-work hours.

**NetScreen-500, The Complete Enterprise Central Site Solution**



# Systems Features

Feature	NetScreen-1000SP (1)	NetScreen-1000ES (1)	NetScreen-500 (2)
<b>Performance</b>			
Concurrent sessions	500,000	300,000	250,000
New sessions/second	15,000	15,000	17,000
Firewall performance	2 Gbps	1 Gbps	700 Mbps
Triple-DES (168 bit)	1 Gbps	600 Mbps	250 Mbps
Policies	40,000 (3)	40,000 (3)	20,000 (3)
Schedules	256	256	256
Number of processing boards	6	4 (4)	N/A
Traffic interfaces	Untrust: 1 active GigE GBIC (SX or LX) and 1 redundant Trust: 1 active GigE MT-RJ and 1 redundant	Untrust: 1 active GigE GBIC (SX or LX) and 1 redundant Trust: 1 active GigE MT-RJ and 1 redundant	Up to 8 10/100 or mini-GBIC (SX or LX), up to 4 GBIC (SX or LX)
<b>Virtual Systems</b>			
Maximum number of Virtual Systems	250	250	25
Number of VLANs supported	500	500	100
<b>Mode of Operation</b>			
Transparent mode (all interfaces)	Yes	Yes	Yes
Route mode (all interfaces)	Yes	Yes	Yes
NAT (Network Address Translation)	Yes	Yes	Per interface
Policy-based NAT	Yes	Yes	Yes
PAT (Port Address Translation)	Yes	Yes	Yes
Virtual IP	4 (5)	4 (5)	4 (5)
Mapped IP	4096 (3)	4096 (3)	4096 (3)
IP routing—static routes	1,024 (3)	1,024 (3)	512 (3)
Users per port, Trusted	Unrestricted	Unrestricted	Unrestricted
<b>Firewall Attacks Detected</b>			
Syn attack	Yes	Yes	Yes
ICMP flood	Yes	Yes	Yes
UDP flood	Yes	Yes	Yes
Ping of death	Yes	Yes	Yes
IP spoofing	Yes	Yes	Yes
Port scan	Yes	Yes	Yes
Land attack	Yes	Yes	Yes
Tear drop attack	Yes	Yes	Yes
Filter IP source route option	Yes	Yes	Yes
IP address sweep attack	Yes	Yes	Yes
WinNuke attack	Yes	Yes	Yes
Java/ActiveX/Zip/EXE	Yes	Yes	Yes
Default packet deny	Yes	Yes	Yes
User-defined Malicious URL	48	48	48
Per-source session limiting	Yes	Yes	Yes
Syn fragments	Future ScreenOS	Future ScreenOS	Yes
Syn and FIN bit set	Future ScreenOS	Future ScreenOS	Yes
No flags in TCP	Future ScreenOS	Future ScreenOS	Yes
FIN with no ACK	Future ScreenOS	Future ScreenOS	Yes
ICMP fragment	Future ScreenOS	Future ScreenOS	Yes
Large ICMP	Future ScreenOS	Future ScreenOS	Yes
IP source route	Future ScreenOS	Future ScreenOS	Yes
IP record route	Future ScreenOS	Future ScreenOS	Yes
IP security options	Future ScreenOS	Future ScreenOS	Yes
IP timestamp	Future ScreenOS	Future ScreenOS	Yes
IP stream	Future ScreenOS	Future ScreenOS	Yes
IP bad options	Future ScreenOS	Future ScreenOS	Yes
Unknown protocols	Future ScreenOS	Future ScreenOS	Yes
<b>VPN</b>			
Dedicated VPN tunnels	25,000 (3)	15,000 (3)	10,000 (3)
Manual Key, IKE, PKI (X.509)	Yes	Yes	Yes
3DES (168-bit), AES (128-bit), & DES (56-bit) encryption	3DES and DES only, AES in future ScreenOS	3DES and DES only, AES in future ScreenOS	Yes
Perfect forward secrecy (DH Groups)	1,2,5	1,2,5	1,2,5
Prevent replay attack	Yes	Yes	Yes
Remote access VPN	Yes	Yes	Yes
L2TP within IPSec	Yes	Yes	Yes
Site-to-site VPN	Yes	Yes	Yes
Star (hub and spoke) VPN network topology	Yes	Yes	Yes
IPSec NAT Traversal	Yes	Yes	Yes
<b>IPSec Authentication</b>			
SHA-1	Yes	Yes	Yes
MD5	Yes	Yes	Yes
PKI Certificate requests (PKCS 7 & PKCS 10)	Yes	Yes	Yes
Automated certificate enrollment (SCEP)	No	No	Yes
Online Certificate Status Protocol (OCSP)	No	No	Yes
Certificate Authorities supported			
VeriSign CA	Yes	Yes	Yes
Entrust CA	Yes	Yes	Yes

# Systems Features

Feature	NetScreen-1000SP (1)	NetScreen-1000ES (1)	NetScreen-500 (2)
<b>IPSec Authentication (cont'd)</b>			
Microsoft CA	Yes	Yes	Yes
RSA Keon CA	Yes	Yes	Yes
iPlanet (Netscape) CA	Yes	Yes	Yes
Baltimore CA	Yes	Yes	Yes
DOD PKI CA	No	No	Yes
<b>Firewall &amp; VPN User Authentication</b>			
Built-in (internal) database - user limit	25,000	15,000	15,000
RADIUS (external) database	Yes	Yes	Yes
RSA SecureID (external) database	Yes	Yes	Yes
LDAP (external) database	Yes	Yes	Yes
<b>Traffic Management</b>			
Guaranteed bandwidth	N/A	N/A	Yes
Maximum bandwidth	N/A	N/A	Yes
Priority-bandwidth utilization	N/A	N/A	Yes
DiffServ stamp	N/A	N/A	Yes
<b>High Availability (HA)</b>			
Active/Active full mesh high availability with NSRP v2	Yes	Yes	ScreenOS 2.7.1 only
Active/Passive full synchronization High Availability	Yes	Yes	Yes
Session protection for firewall and VPN	Yes	Yes	Yes
Device failure detection	Yes	Yes	Yes
Link failure detection	Yes	Yes	Yes
Network notification on failover	Yes	Yes	Yes
Authentication for new HA members	Yes	Yes	Yes
Encryption of HA traffic	Yes	Yes	Yes
<b>System Management</b>			
WebUI (HTTP and HTTPS)	Yes	Yes	Yes
Command line interface (console)	Yes	Yes	Yes
Command line interface (telnet)	Yes	Yes	Yes
Secure Command Shell (SSH v1 compatible)	Yes	Yes	Yes
NetScreen-Global PRO	ScreenOS 2.6.0 (7)	ScreenOS 2.6.0 (7)	ScreenOS 3.0.0 (6)
NetScreen-Global PRO Express	ScreenOS 2.6.0 (7)	ScreenOS 2.6.0 (7)	ScreenOS 3.0.0 (6)
All management via VPN tunnel on any interface	Yes	Yes	Yes
SNMP full custom MIB	Yes	Yes	Yes
<b>Administration</b>			
Multiple administrators	20	20	20
Remote administrator database	RADIUS	RADIUS	RADIUS
Administrative networks	6	6	6
Root admin, admin, & read only user levels	Yes	Yes	Yes
Software upgrades & configuration changes	TFTP/WebUI/Global	TFTP/WebUI/Global	TFTP/WebUI/Global
<b>Logging/Monitoring</b>			
Syslog	External	External	External
E-mail (2 addresses)	Yes	Yes	Yes
NetIQ WebTrends	External	External	External
SNMP	Yes	Yes	Yes
Traceroute	Yes	Yes	Yes
VPN tunnel monitor	Yes	Yes	Yes
Websense URL filtering	No	No	External
<b>External Flash</b>			
PCMCIA (PC Card)	96MB, Type 1	96MB, Type 1	96 or 440MB, Type 2 & 3
Event logs & alarms	Yes	Yes	Yes
System config script	Yes	Yes	Yes
ScreenOS software	Yes	Yes	Yes
<b>Dimensions and Power</b>			
Height	22 inches	22 inches	3.5 inches
Width	17.5 inches	17.5 inches	17.5 inches
Length	20 inches	20 inches	17 inches
Weight	50 lbs.	50 lbs.	27 lbs.
Rack mountable	Yes	Yes	Yes
Power supply (AC)	95 to 240 variable (47 to 63 Hz)	95 to 240 variable (47 to 63 Hz)	90 to 264 VAC, (47 to 63 Hz)
Power supply (DC)	-36 to -72 VDC	-36 to -72 VDC	-36 to -72 VDC
Power consumption	350 Watts Maximum 180 Watts Average	350 Watts Maximum 180 Watts Average	100 Watts Maximum 60 Watts Average

(1) Performance, capacity, and features provided with NetScreen ScreenOS 2.8.0 r1 and the Switch II Module. May vary with other NetScreen ScreenOS releases.

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

(3) Shared among all Virtual Systems

(4) Upgradeable to 6 processing boards

(5) Not available with Virtual Systems

(6) ScreenOS 3.1.0 supported in future release of NetScreen-Global PRO/PRO Express

(7) ScreenOS 2.8.0 supported in future release of NetScreen-Global PRO/PRO Express

# Specifications and Ordering Information

## Specifications:

### 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

### Safety Certifications

#### NetScreen-1000:

Safety Certifications: CSA  
EMI: FCC Part 15 class A, CE, VCCI, C-Tick, BSMI

#### NetScreen-500:

Safety Certifications: CSA, UL  
EMI: FCC Part 15 class A, CE, VCCI, C-Tick, BSMI

#### NetScreen-1000 Environment

Temperature: 0 to 40 C (32 to 104 F)  
Relative Humidity: 10 to 90% non-condensing  
MTBF: 8.9 years

#### NetScreen-500 Environment

Temperature: 0 to 40 C (32 to 104 F)  
Relative Humidity: 10 to 90% non-condensing  
MTBF: 6.5 years

## NetScreen product warranty and services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that it will be free from material defects. Optional hardware maintenance and software subscription services are also available. These services are recommended to ensure the system is kept updated with the latest software enhancements and to ensure high availability for end users. Phone support services and training courses are also available from NetScreen.

## Ordering information:

### Product

#### NetScreen-1000SP Bundles

Product	Part Number
NetScreen-1000SP system, AC	NS-1KA-SYS-SW2
NetScreen-1000SP system, DC	NS-1KD-SYS-SW2

- Complete SP system includes chassis, Switch II Module, six Processor Module, Auxiliary Module, 2 power supplies, 100 VSYS and full software features

#### NetScreen-1000ES Bundles

Product	Part Number
NetScreen-1000ES system, AC, 5 Virtual Systems	NS-1KA-ES1-SW2
NetScreen-1000ES system, DC, 5 Virtual Systems	NS-1KD-ES1-SW2
NetScreen-1000ES system, AC, 25 Virtual Systems	NS-1KA-25-SW2
NetScreen-1000ES system, DC, 25 Virtual Systems	NS-1KD-25-SW2
NetScreen-1000ES system, AC, 50 Virtual Systems	NS-1KA-50-SW2
NetScreen-1000ES system, DC, 50 Virtual Systems	NS-1KD-50-SW2

- ES systems include chassis, Switch II Module, four Processor Modules, Auxiliary Module, 2 power supplies and software for firewall, VPN and High Availability

#### NetScreen-1000ES Starter Kit (No HA and 0 VSYS)

Product	Part Number
NetScreen-1000ES starter kit, AC	NS-1KA-ES2-SW2
NetScreen-1000ES starter kit, DC	NS-1KD-ES2-SW2

- ES Starter Kits include chassis, Switch II Module, four Processor Modules, Auxiliary Module, 2 power supplies and software for firewall and VPN

NetScreen-1000ES Starter Kit to ES system upgrade NS-1KS-SES

#### NetScreen-1000ES Virtual System Upgrades

NetScreen-1000ES 5 to 25 upgrade	NS-1KA-VSYS-25
NetScreen-1000ES 25 to 50 upgrade	NS-1KA-VSYS-50
NetScreen-1000ES 50 to 100 upgrade	NS-1KA-VSYS-100
NetScreen-1000ES 100 to 250 upgrade	NS-1KA-VSYS-250
NetScreen-1000ES 5 to 100 upgrade	NS-1KA-VSYS

#### NetScreen-1000 Spares

NetScreen-1000 Processor Board	NS-1K0-PRO
NetScreen-1000 Auxiliary Board	NS-1K0-AUX
NetScreen-1000 Switch II Board	NS-1K0-SW2
NetScreen-1000 Switch II Upgrade Kit	NS-1K0-SW2-KIT
NetScreen-1000 Power Supply AC	NS-1K0-PSA
NetScreen-1000 Power Supply DC	NS-1K0-PSD
NetScreen-1000 Chassis AC	NS-1K0-CHA
NetScreen-1000 Chassis DC	NS-1K0-CHD
NetScreen-1000 Fan	NS-1K0-FAN

### Part Number

### Product

#### NetScreen-500SP Bundles

Product	Part Number
NetScreen-500, SX dual-GBIC, AC	NS-500SP-GB2-AC
NetScreen-500, SX dual-GBIC, DC	NS-500SP-GB2-DC
NetScreen-500, SX GBIC, AC	NS-500SP-GB1-AC
NetScreen-500, SX GBIC, DC	NS-500SP-GB1-DC

- SP systems include 2 interface modules, 2 power supplies, fan module, and 25 Virtual Systems

#### NetScreen-500ES Bundles

Product	Part Number
NetScreen-500, 2 SX GBIC, 2 AC power	NS-500ES-GB1-AC
NetScreen-500, 2 SX GBIC, 2 DC power	NS-500ES-GB1-DC
NetScreen-500, 2 SX dual-GBIC, 2 AC power	NS-500ES-GB2-AC
NetScreen-500, 2 SX dual-GBIC, 2 DC power	NS-500ES-GB2-DC
NetScreen-500, 3 dual-10/100, 2 AC power	NS-500ES-FE1-AC
NetScreen-500, 3 dual-10/100, 2 DC power	NS-500ES-FE1-DC
NetScreen-500, 2 dual-10/100, 1 AC power	NS-500ES-FE2-AC
NetScreen-500, 2 dual-10/100, 1 DC power	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
Upgrade from 0 to 25 Virtual Systems	NS-500-VSYS

#### NetScreen-500 Spares

GBIC interface module (SX)	NS-500-HG1-SX
GBIC interface module (LX)	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-500-MSX
LX transceiver (mini-GBIC)	NS-500-MLX
AC power supply	NS-500-PWR-AC
DC power supply	NS-500-PWR-DC
Fan module	NS-500-FAN



350 Oakmead Parkway  
Sunnyvale, CA 94085  
Phone: 408.730.6000  
Fax: 408.730.6200

[www.netscreen.com](http://www.netscreen.com)

Copyright © 1998-2002 NetScreen Technologies, Inc.

NetScreen, NetScreen Technologies, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5, NetScreen-5XP, NetScreen-10, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-1000, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote, GigaScreen ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Part Number: 2002.3.10.1.sys

For more information about  
NetScreen products, call toll-free  
1-800-638-8296 or visit us at  
[www.netscreen.com](http://www.netscreen.com)