NetScreen Security Systems

At a glance

• Purpose-built, integrated security systems

High-performance security systems running NetScreen-ScreenOS firewall and VPN software on ASIC-based hardware platforms 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 100 security domains can be provided for managed security services or enterprise partitioning

• High availability

Solid-state design, redundant hot-swap power supplies and hot-swap fans deliver maximum uptime within each system. High availability software enables failover to a redundant system with no loss of firewall sessions or VPN tunnels

• Scalable solutions with flexible configuration options

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

• User-friendly

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

NetScreen-1000

NetScreen-500

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 scalable solutions for large enterprises and service providers. All NetScreen Security Systems include support for Virtual Systems to secure multiple security domains.

Firewall

NetScreen's full-featured firewall uses technology based on stateful inspection, securing against intruders and denial-of-service attacks. NetScreen's custom-built GigaScreen ASIC processes the firewall access policies and encryption algorithms in hardware; providing significantly higher performance than software-only solutions.

- 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 than patched-together software-based solutions

- Robust attack prevention including SYN attack, ICMP flood, Port Scan, and others
- Network Address Translation (NAT), Port Address Translation (PAT)—which hide internal, non-routable IP addresses—as well as transparent mode
- Policy-based NAT allows inbound address translation

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.

- Comprehensive VPN support for both remote access and site-to-site 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 ICSA- and VPNC- certified for IPSec interoperability
- 3DES 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 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 the switch 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.

- Expand service offerings in the Internet data center to include managed VPN and firewall on shared hardware platform
- Segment the enterprise network for multiple DMZs or provide security between internal departments
- Map multiple VLANs to one Virtual System
- Separate WebUI, CLI, and administration access for each Virtual System

NetScreen Security Systems

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 failover.

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

- Stateful VPN & Firewall Failover
  – Configurations are mirrored between HA group members to ensure proper behavior in case of a failover
  – 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 failover)
- Support for full mesh network topologies with monitored redundant Trust and Untrust connections

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 (network address translation) 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.

Modularity

NetScreen systems are modular, allowing custom configuration and extra reliability. All systems offer redundant AC or DC power supplies

as well as removable fan modules. The NetScreen-1000 also comes equipped with multiple processing boards for increased redundancy and performance. The NetScreen-500 offers two types of interface modules and four interface module bays to allow increased system configuration.

Comprehensive 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.
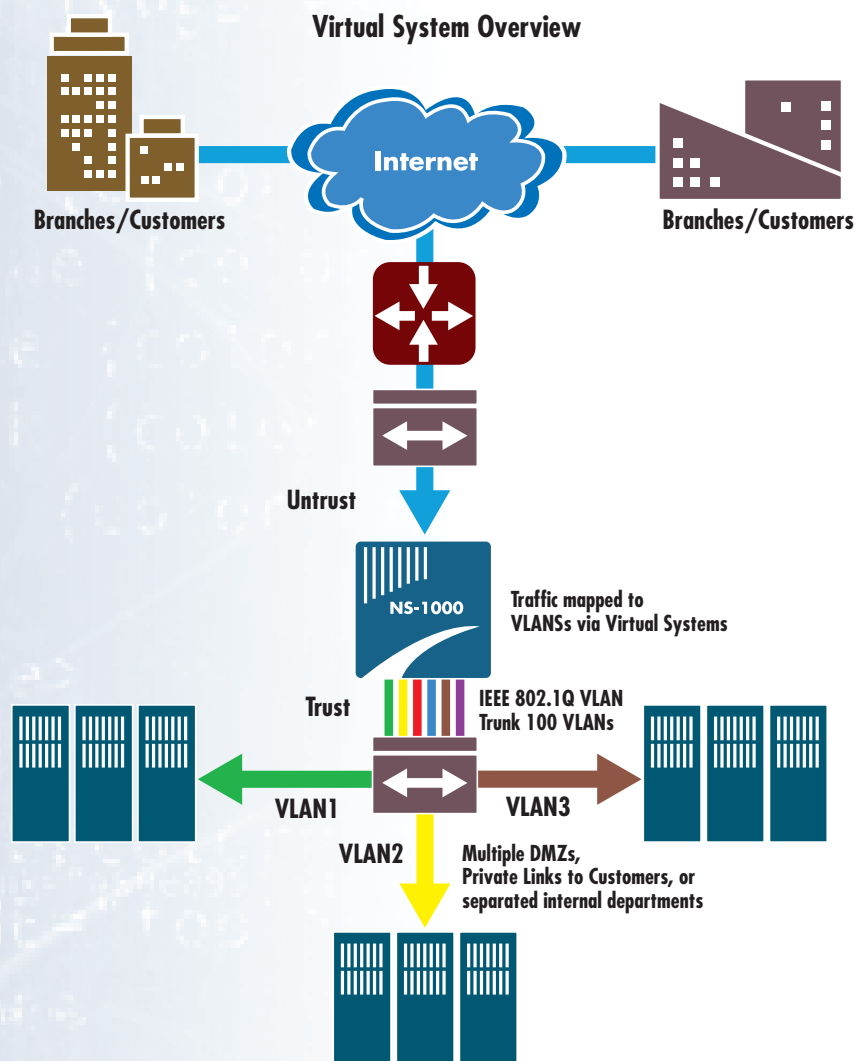
- Menu-driven central site management using NetScreen-Global Manager or NetScreen-Global PRO
- Browser-based management with the built in Web UI (HTTP and HTTPS)
- Command line interface (CLI) accessible via Secure Command Shell (SSH v.1 compatible), Telnet, and console port
- E-mail alerts, SNMP alarms
- Integrates with Syslog or WebTrends™ for external logging, monitoring, and analysis
- Provides up to 20 administrators with 3 levels of access: root admin, admin, and read-only

Collocation friendly

All NetScreen Systems are designed with collocation needs in mind. All rack mounting equipment is provided, and audible and visible alarms can be configured to help monitor device status by on-site technicians.

Virtual System Overview

Branches/Customers

Internet

Branches/Customers

Untrust

NS-1000

Traffic mapped to VLANSs via Virtual Systems

Trust

IEEE 802.1Q VLAN Trunk 100 VLANs

VLAN1

VLAN3

VLAN2

Multiple DMZs, Private Links to Customers, or separated internal departments

NetScreen-1000

NetScreen-1000

The NetScreen-1000 Multi-Gigabit Security System is an Internet 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 fastest firewall and encryption acceleration engine available, 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 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, or 100).
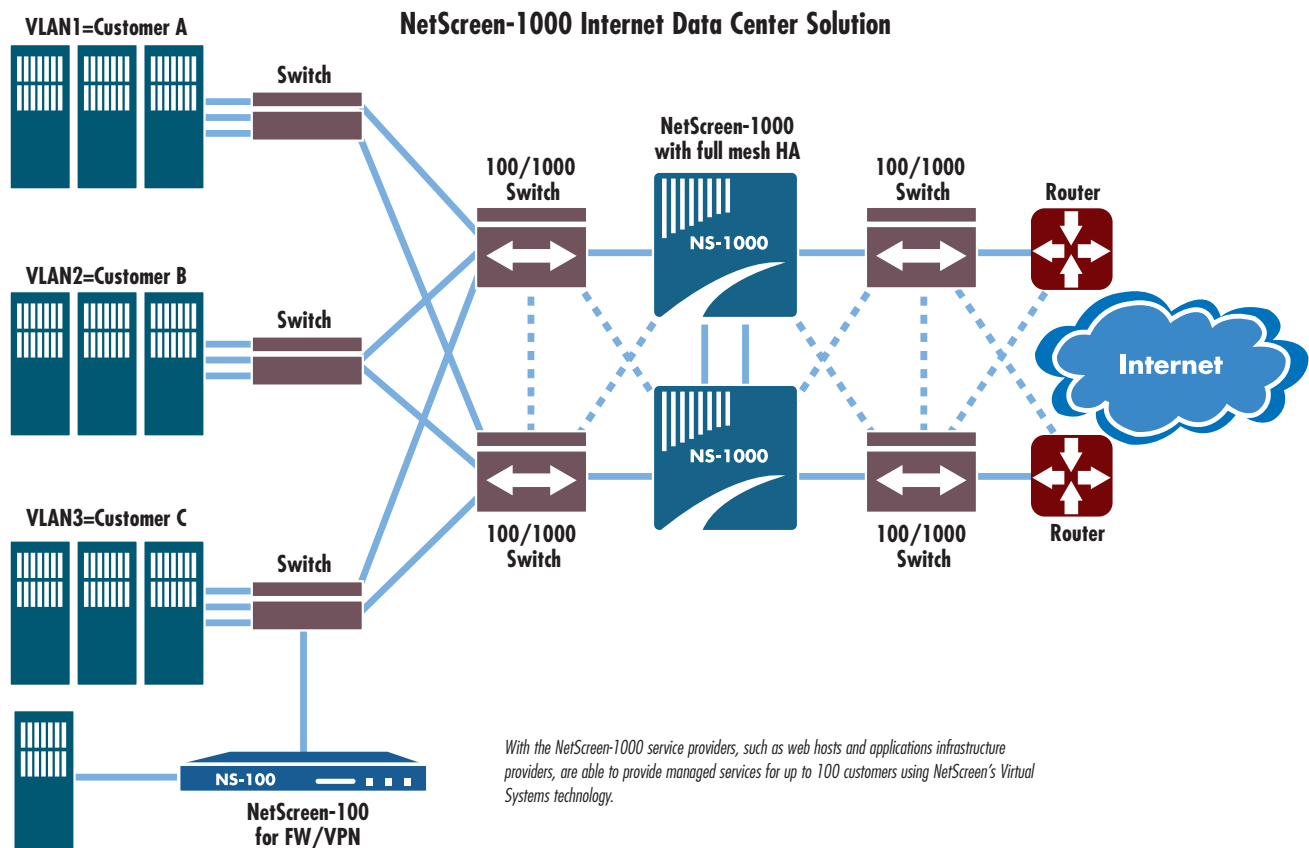
The NetScreen-1000 architecture

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 data packet interfaces with redundant gigabit Ethernet untrusted ports (LX or SX GBIC), redundant gigabit Ethernet trusted ports (MT-RJ) and two gigabit high availability interfaces. It also provides a 6 Gbps switch fabric
- 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

NetScreen-1000 Internet Data Center Solution

With the NetScreen-1000 service providers, such as web hosts and applications infrastructure providers, are able to provide managed services for up to 100 customers using NetScreen's Virtual Systems technology.

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. Leveraging features from both the NetScreen-100 and NetScreen-1000, the NetScreen-500 is ideally suited for large enterprise environments with high bandwidth 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 Systems:

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 security domains. 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 highly redundant platform. To address performance, 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 and redundancy concerns, the NetScreen-500 has minimal moving parts, and offers a hot-swappable fan module (made up of four fans), and redundant 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
- 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.

NetScreen-500 Enterprise Solution

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
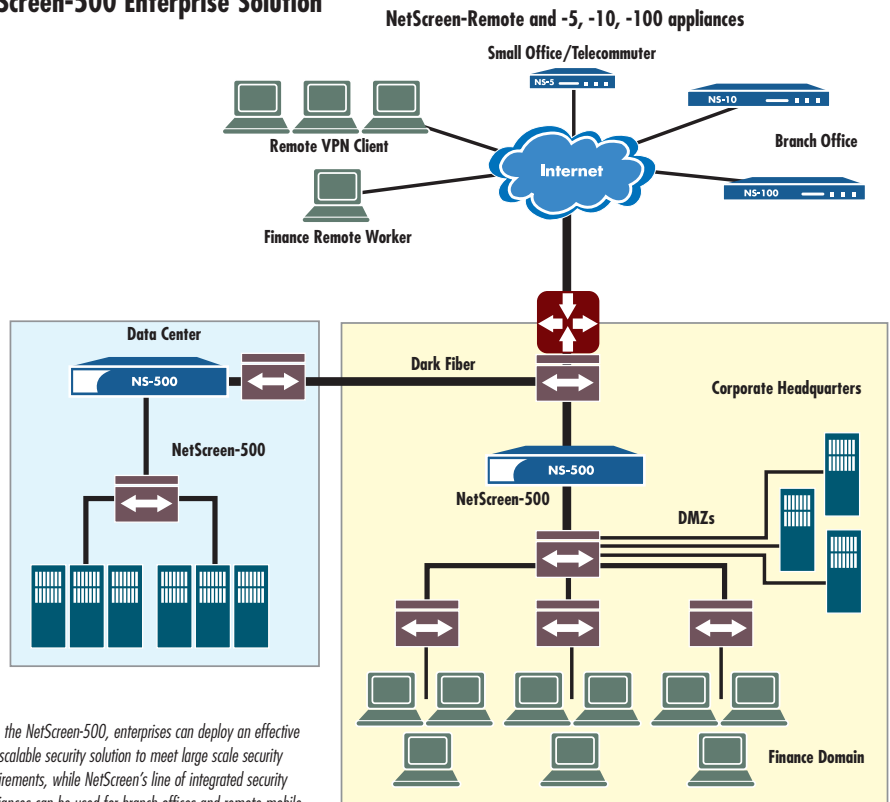
Traffic management

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

Content filtering

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

With the NetScreen-500, enterprises can deploy an effective and scalable security solution to meet large scale security requirements, while NetScreen's line of integrated security appliances can be used for branch offices and remote mobile workers.

System Features

Feature		NetScreen-1000	NetScreen-500
Performance	Concurrent sessions	500,000 (ES: 300,000)* (1)	250,000 (1)
	New sessions/second	15,000 (1)	22,000 (1)
	Firewall performance	2,000 Mbps wire speed (6)	700 Mbps
	Triple-DES (168 bit)	1,000 Mbps wire speed	250 Mbps
	Policies	40,000 (1)	20,000 (1)
	Schedules	256 (1)	256 (1)
Virtual Systems	Maximum number of Virtual Systems	100	25
	Number of VLANs supported	500	100
Mode of Operation	Transparent Mode (All Interfaces)	Yes (2)	Yes (2)
	Route Mode	Yes	Yes
	NAT (Network Address Translation)	Yes	Yes
	PAT (Port Address Translation)	Yes	Yes
	Virtual IP (VIP)	4 (2)	4 (2)
	Mapped IP	4096 (1)	4096 (1)
	IP routing — Static Routes	1024 (1)	512 (1)
	Policy-based NAT	Yes	Yes
	Users per port	Unrestricted	Unrestricted
Firewall Attack Detection	Syn Attack	Yes (3)	Yes (3)
	ICMP Flood detection, threshold selectable	Yes (3)	Yes (3)
	UDP Flood detection, threshold selectable	Yes (3)	Yes (3)
	Detect Ping of Death	Yes (3)	Yes (3)
	Detect IP Spoofing	Yes (3)	Yes (3)
	Detect Port Scan	Yes (3)	Yes (3)
	Detect Land Attack	Yes (3)	Yes (3)
	Detect Tear Drop Attack	Yes (3)	Yes (3)
	Filter IP source route option	Yes (3)	Yes (3)
	Detect IP address Sweep attack	Yes (3)	Yes (3)
	Detect WinNuke attack	Yes (3)	Yes (3)
	Java/ActiveX/Zip/EXE	Yes (3)	Yes (3)
	Default Packet deny	Yes (3)	Yes (3)
	DoS, DDoS Protection	Yes (3)	Yes (3)
VPN	Dedicated Tunnels	25,000 (ES:15,000)*(1)	10,000 (1)
	Manual Key, IKE, PKI (X.509)	Yes	Yes
	DES (56-bit) & 3DES (168-bit) Encryption	Yes	Yes
	Perfect Forward Secrecy (DH Groups)	1,2,5	1,2,5
	Prevent Replay Attack	Yes	Yes
	Remote Access VPN	Yes	Yes
	Site-to-site VPN	Yes	Yes
	Star (hub and spoke) VPN network topology	Yes	Yes
	L2TP	N/A	Yes
IPSec	Authentication		
	SHA-1	Yes	Yes
	MD5	Yes	Yes
	Certificate Requests (PKCS 7 & PKCS 10)	Yes	Yes
	Certificate Servers Supported		
	Verisign CA	Yes	Yes
	Entrust CA	Yes	Yes
	Microsoft CA	Yes	Yes
	RSA Keon CA	Yes	Yes
	IPlanet (Netscape) CA	Yes	Yes
	Baltimore CA	Yes	Yes
High Availability (HA)	High Availability (HA)	Yes	Yes
	Active/Active Support	Yes	Yes
	Full mesh deployments supported	Yes	Yes
	Redundant interfaces	Yes	Yes

Feature		NetScreen-1000	NetScreen-500
High Availability (HA)	Session protection for Firewall and VPN	Yes	Yes
	Device failure detection	Yes	Yes
	Link failure detection	Yes	Yes
	Network notification on failover	Yes	Yes
Firewall & VPN User Authentication	Built-In (internal) Database - user limit	25,000 (ES: 15,000)*	15,000
	RADIUS (external) database	Yes	Yes
	SA SecureID (external) database	Yes	Yes
	LDAP (external) database	Yes	Yes
Traffic Management	Guaranteed bandwidth	N/A	Yes (2)
	Maximum bandwidth	N/A	Yes (2)
	Priority-bandwidth utilization	N/A	Yes (2)
	DiffServ stamp	N/A	Yes (2)
System Management	WebUI (HTTP and HTTPS)	Yes	Yes
	Command Line Interface (console)	Yes	Yes
	Command Line Interface (telnet)	Yes	Yes
	Secure Command Shell (ssh v1 compatible)	Yes	Yes
	NetScreen-Global Manager	Yes	Yes
	NetScreen-Global PRO	Yes	Yes
	All management via VPN tunnel on any interface	Yes	Yes
Administration	Multiple administrators	20 (2)	20 (2)
	Remote administrator database	Radius	Radius
	Administrative networks	6	6
	Root Admin, Admin, & Read Only user levels	Yes	Yes
	Software Upgrades & Config Changes	TFTP/WebUI/Global	TFTP/WebUI
Logging/Monitoring	Syslog	External	External
	E-mail (2 addresses)	Yes	Yes
	WebTrends	External	External
	SNMP	Yes	Yes
	Traceroute	Yes	Yes
	VPN Tunnel Monitor	Yes	Yes
	Websense URL filtering	N/A	External (3)
PCMCIA	PCMCIA Card	96 MB, Type 1	440 MB, Type 2 & 3
	Event Logs & Alarms	Yes	Yes
	System Config Script	Ye	Yes
	ScreenOS Software	Yes	Yes
Dimensions and Power	Height	22 inches	3.5 inches
	Width	17.5 inches	17.5 inches
	Length	20 inches	17 inches
	Weight	50 lbs.	27 lbs.
	Rack Mountable	Yes	Yes
	Power input AC	95 - 240 variable (47 to 63 Hz)	95 - 240 variable (47 to 63 Hz)
	Power input DC	Option, -36 to -72VDC	Option, -36 to -72VDC
	Power consumption	350 Watts	100 Watts

*ES indicates NetScreen-1000ES where different from NetScreen-1000SP

(1) Shared among all Virtual Systems

(2) Not available with Virtual Systems

(3) Feature enabled or disabled for whole system, no individual Virtual System control

(4) Virtual Systems only

(5) Performance tested with GBIC cards, 10/100 cards support wire speed performance

(6) Performance with the Switch II Module–basic switch module achieves 1 Gbps firewall throughput

Specifications and Ordering

Specifications:

Standards supported

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

Certifications

NetScreen-1000:

Safety Certifications: CSA

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

NetScreen-500:

Safety Certifications: CSA

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

NetScreen-1000 Environment

Temperature: 0 to 55 C (32 to 131 F)

Relative Humidity: 10 to 90% non-condensing

NetScreen-500 Environment

Temperature: 0 to 50 C (32 to 122 F)

Relative Humidity: 10 to 90% non-condensing

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 meet published specifications. 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.

For more information about NetScreen products, call toll-free 1-800-638-8296

Ordering information:

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

- Complete System includes chassis, Switch II Module, six processor module, auxiliary module, 2 power supplies and full software features

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

- ES systems includes chassis, Switch II Module, four processor modules, auxiliary module, 2 power supplies and software for firewall, VPN and high availability

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

- ES systems includes chassis, Switch II Module, four processor modules, auxiliary module, 2 power supplies and software for firewall and VPN

Product	Part Number
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 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 Board	NS-1K0-SWI
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

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 interface modules, 2 power supplies, fan module, and 25 Virtual Systems

Product	Part Number
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

Product	Part Number
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
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-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

NETSCREEN™