

# NetScreen-IDP 10/100/500

## Intrusion Detection and Prevention



**NETSCREEN®**  
Scalable Security Solutions



Not all products shown

### At a glance

- **Attack prevention**

*First in-line device capable of dropping the malicious traffic as soon as the attack is detected, eliminating the impact of an intrusion*

- **Multi-Method Detection (MMD)™**

*Combines multiple detection methods in a single device to maximize the types of attacks accurately detected*

- **Centralized, rule-based management**

*Quick and easy to set up, manage and maintain, providing granular control over exactly how the system behaves with visibility into network threats that make it easy to thread through attack information and quickly make policy adjustments to ensure the network is effectively protected*

- **Enterprise network integration**

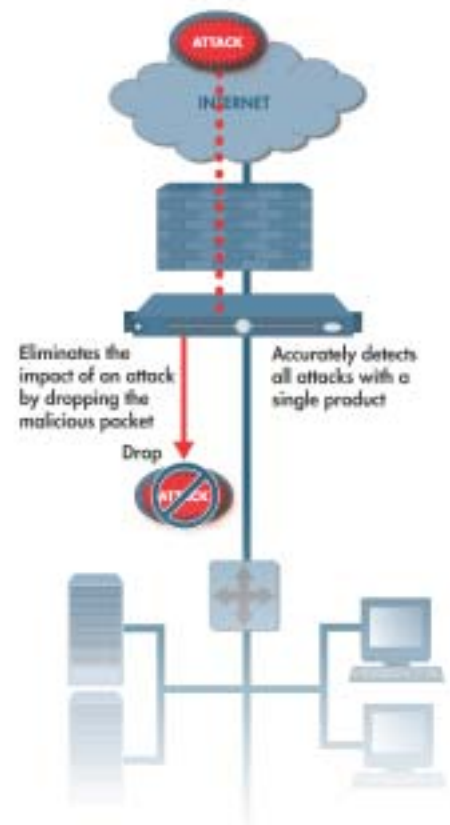
*Support for advanced networking features, such as VLANs for logical interfaces and SNMP for network monitoring systems, to integrate seamlessly into the network*

### How do you protect your network?

Most people think network intrusions happen to other people. The reality is they affect everyone. It is inevitable your network will be attacked, and the attackers will try all sorts of tricks to compromise your systems. Are you prepared?

### You need the NetScreen-IDP appliance for effective protection

The NetScreen Intrusion Detection and Prevention (NetScreen-IDP) system effectively identifies and stops attacks on your network, minimizing the time and costs associated with intrusions. It compliments your firewall, providing the next layer of security by looking deep into the network traffic to accurately identify intrusions and stop the attacks from ever reaching their destination. NetScreen-IDP implements a high-speed Multi-Method Detection (MMD) mechanism, combining eight different detection methods in a single product to provide the most comprehensive attack coverage available on the market. More importantly, it is the first device capable of operating in-line, so it can drop malicious traffic during the intrusion detection process, completely eliminating the impact of an attack. Combined with a centralized, rule-based management approach, which offers granular control over the system's behavior and easy access to its information, it is easy to see why NetScreen-IDP is the best way to keep your information assets safe.



# Accurate attack detection

## You need comprehensive and accurate detection

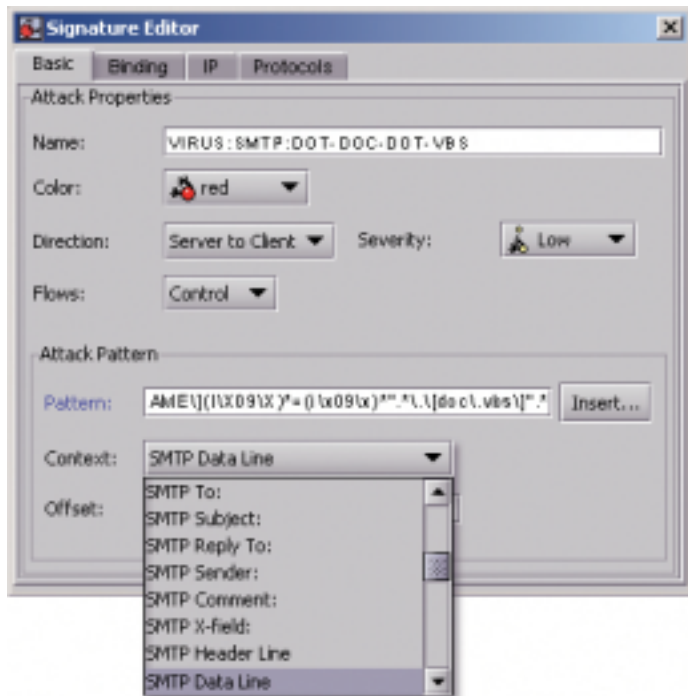
No single detection mechanism can detect all attacks. To eliminate the necessity of purchasing multiple intrusion detection products for comprehensive attack coverage, NetScreen-IDP was built from the ground up to combine multiple detection methods in a single solution. The NetScreen-IDP MMD mechanism integrates Stateful Signature, Protocol Anomaly, Backdoor, Traffic Anomaly, IP Spoofing, Layer 2 and SYN-Flood Detection, as well as a Network Honeypot, to provide the broadest attack detection coverage available. MMD leverages the strength of each method, using the most appropriate mechanism to accurately and efficiently detect intrusions.

## Stateful Signature Detection

The best-known detection mechanism is signature detection. Once network attacks are discovered and understood, security vendors will character-

ize them as an attack pattern, called a signature. These signatures are then compiled into a database and matched against the flow of traffic to identify attacks.

NetScreen developed an advanced signature form, called Stateful Signatures™, to produce the most accurate signature-based detection mechanism available. While other products typically use packet signatures, which blindly search for signature matches in all traffic, producing many false alarms, NetScreen-IDP uses Stateful Signatures, which intelligently look for attack patterns in only the relevant portions of traffic where the attack can be perpetrated. NetScreen-IDP does this by tracking the state of all communications to pinpoint exactly where to look for an attack. This reduces irrelevant pattern matching within benign traffic to significantly reduce false alarms. With NetScreen-IDP, you can trust the attacks being detected are real.



## Some of the protocols supported by NetScreen-IDP

Protocols	IP Protocol/Port	RFC
IP		791
TCP		793
ICMP		792
ARP		826
ECHO	TCP/7	347
ECHO	UDP/7	347
DISCARD	TCP/9	348
DISCARD	UDP/9	348
CHARGEN	TCP/19	364
FTP	TCP/21	959
SSH	TCP/22	Internet Drafts
TELNET	TCP/23	854
SMTP	TCP/25	821
DNS	TCP/53	1035, 1183, 2535, 1712, 1886, 1876, 2065, 2053, 2538, 2671
DNS	UDP/53	1035, 1183, 2535, 1712, 1886, 1876, 2065, 2053, 2538, 2671
DHCP	UDP/67	1497, 1533, 2131, 2132
TFTP	UDP/69	783, 1350
FINGER	TCP/79	742, 1288
HTTP	TCP/80	2616
POP3	TCP/110	1939, 1957
PORTMAKER	TCP/111(RPCBIND)	1833
PORTMAKER	UDP/111	1833
SMB/NETBIOS	TCP/139	1001, 1002, Internet Drafts
IMAP	TCP/143	2060
SNMP	UDP/161	1157
SNMP-TRAP	UDP/162	1157
REXEC	TCP/512	No RFC - Source Code Used
RLOGIN	TCP/513	1282
RSH	TCP/514	No RFC - Source Code Used
SYSLOG	UDP/514	3164
RTSP	TCP/554(Real-Audio)	2326
SSH	TCP/22	Internet Drafts
NNTP	TCP/119	0977
Gopher	TCP/70	1436
IDENT	TCP/113	1413
IDENT	UDP/113	1413
IRC	TCP/194	1459
MS-RPC	TCP/369	No RFC - Source code Used
RUSERS		No RFC - Source code Used
VNC		No RFC - Source code Used
Gnutella		No RFC - Source code Used
MSN-IM	Varies	No RFC - Source code Used
AOL-IM	Varies	No RFC - Source code Used
Yahoo-IM	Varies	No RFC - Source code Used

## Protocol Anomaly Detection

The second most used detection mechanism is Protocol Anomaly Detection. This method detects attacks that cannot be characterized, do not

have a pattern or have yet to be discovered. It works by comparing traffic to the published protocol specifications that "normal" traffic would follow. Any deviations from these protocols indicate that someone is trying to do something they probably shouldn't be doing, constituting an attack. There are cases where a product used in your company has implemented a protocol incorrectly. In this instance, you can selectively exclude the detection of specific protocol anomalies for specific systems.

NetScreen-IDP supports an extensive list of protocols and is the first to support SNMP (protecting you from tens of thousands of exploits) and NetBIOS (Windows-based vulnerabilities running on internal systems).

## Backdoor Detection

NetScreen developed a new detection mechanism designed to identify intrusions that give an attacker complete control over a network resource. These attacks, called backdoor attacks, enable the perpetrator to take control over a target system and often result in a significant financial impact and loss. For example, an

attacker can exploit a vulnerability to load a Worm onto a network resource and then interact with that system to take control of it. Once that system is compromised, the attacker continues to interact with it, trying different commands in an effort to launch attacks from that system or compromise other systems.

NetScreen is the first to offer a detection mechanism capable of identifying backdoors. This detection method enables NetScreen-IDP to identify the unique characteristics of interactive traffic and take appropriate action. Backdoor Detection can also identify some unknown attacks that don't deviate from protocol specifications and, therefore, would not be picked up by Protocol Anomaly Detection.

## Signature database and updates

NetScreen has a team of security experts dedicated to creating the signatures you need to combat the latest threats. In addition to the extensive signature database that is shipped with NetScreen-IDP, customers with a support contract will receive updates as frequently as once a week. Plus, NetScreen-IDP offers a Signature Editor to make it easy for you to write your own custom Stateful Signatures to quickly integrate your specific enterprise needs into your Security Policy. When uploading the NetScreen signature updates, NetScreen-IDP gives you the flexibility to either pick and choose the signatures you want or do a batch update. It can also reconcile signature updates with your custom signatures to make sure that they are not overridden or lost. The NetScreen-IDP centralized management approach allows you to easily download any Security Policy changes to the Sensors with the click of a button.

# Simple management

## Centralized management and monitoring

### Centralized, policy-based management

The entire NetScreen-IDP system can be controlled using a single, enterprise-wide Security Policy. With the push of a button, NetScreen-IDP will distribute the single, logical Security Policy to manage distributed Sensors, installing each rule on the appropriate Sensor(s). When you make changes to your Security Policy, all relevant configuration and signature information is automatically sent to the appropriate Sensors as an authenticated and encrypted communication. NetScreen-IDP tracks Security Policy revisions that have been installed, so you can always go back and see a history of the Policies you created. In addition to centralized control, NetScreen-IDP provides centralized log collection, storage and presentation, as well as centralized status monitoring of all components in your installation. These capabilities maximize the productivity of you and your team.

### Rulebase provides granular control

NetScreen-IDP enables you to dictate the system's behavior, without introducing complexity. The rule-based approach allows you to create individual rules that control what traffic NetScreen-IDP examines, the attacks it looks for, the action you want it to take when an attack is identified, and the Sensors to which you want that rule to apply. You decide how NetScreen-IDP responds to an attack, choosing from multiple options, ranging from sending an e-mail alarm to dropping the connection to protect your most sensitive resources. Advanced packet logging options allow you to specify how many packets to capture before and after the intrusion for forensic and investigative purposes.

### Advanced forensics

Investigating intrusions is an important and often time-consuming element of security. The NetScreen-IDP system simplifies the investigative process, providing closed loop investigation capabilities that enable you to link directly from summary information in the reports to the log record to the packet data and/or the Security Policy rule that triggered the alarm. This helps you follow the course of events related to any particular attack. NetScreen-IDP also provides advanced incident tracking capabilities, includ-

ing customizable annotation flags and user comment fields to ensure everyone knows what is happening with each incident.

### Reports

NetScreen-IDP provides several levels of reporting capabilities, including dashboard reports, investigative reports and management reports. This way, you can identify and present key security information at the appropriate level for everyone in your company—from the security administrator to the CIO. The dashboard aggregates information to give you a complete top-level picture of which hosts are being targeted, by whom and what attacks they are using against your network. By identifying these key trends in the network, you can ensure you stay on top of the most important events in your network. You can also visually correlate the host, attack source and attack type to quickly identify what is at risk in your network, so that you can set your priorities and respond quickly. This unique ability to drill into specific events significantly aids in forensic investigations. The management reports are designed to help you justify all of your security activities, providing easily understood graphs that offer a complete picture of your network security and the actions you have taken to protect your network.

### Customizable display

You control how you want to see and interact with the information captured by NetScreen-IDP to help you quickly extract the information most pertinent to you. For example, you can easily filter the logs and conduct searches for a specific attack. You can then save your customized views and preferences to ensure your interactions with NetScreen-IDP are consistent and intuitive. NetScreen-IDP facilitates data analysis for all members of your team and brings closure to each security incident.

### Quick deployment and configuration

NetScreen-IDP is delivered as a hardware appliance for quick installation, making it easy for you to start deriving value immediately. For example, there are templates to help you build your first Security Policy, and when you add a Sensor, NetScreen-IDP automatically authenticates and builds a secure communication channel between it and the Management Server.

## Simplified management

*NetScreen-IDP was designed to minimize the amount of time needed to manage the system, lowering your total cost of ownership and maximizing the effectiveness of your security team. By taking a centralized, rule-based management approach, NetScreen-IDP makes it simple for you to configure, maintain and manage your network security.*

*The NetScreen-IDP three-tier architecture allows multiple distributed administrative endpoints (User Interface) to access the centralized management server (Data Storage) and control geographically dispersed Sensors (Enforcement Points).*

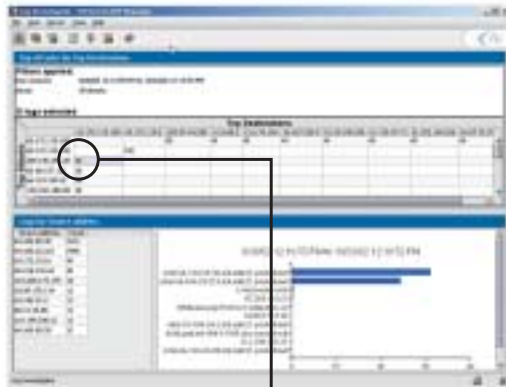
## Progressive drill into the data to identify key security events

### Dashboard



Stay on top of network activities and spot top level trends

### Log Investigator



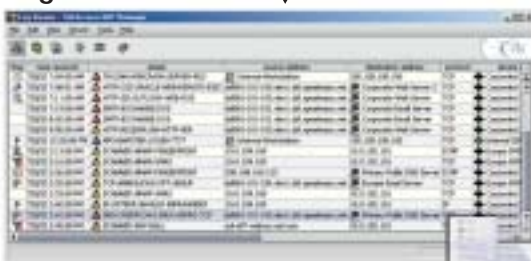
Investigate further by quickly correlating information to understand who is attacking which critical resources and with what attacks

### Security Policies



Jump to the policy to make any necessary changes, such as start dropping the attack to eliminate its impact on the network

### Log Viewer



Go directly to a set of logs to see the details of the attack in context

### Session Packet Data



View packets associated with alarm to see exactly what the attack did

# Prevention

## Passive responses don't protect

Passive IDSes can only alert the administrator or send a message to another device and hope that device can end the attack.

One option is to send a TCP reset message to the client (attacker) and/or server (victim) associated with the attack. Unfortunately, due to the nature of TCP transmissions, it is highly unreliable and doesn't work for non-TCP-based attacks. Even when successful, the reset terminates the connection after the attack reaches its "victim."

Another passive response option is to send a message to the firewall to block future communications from the IP address of the attack source. This also comes after the attack has reached the "victim." Plus, it can potentially form the basis for a Denial-of-Service (DoS) attack, which is a catastrophic side effect. An attacker using or spoofing the IP address of a business partner, customer or service provider for an attack can cause you to block that IP address and stop legitimate traffic from accessing your system.

Simply putting a firewall and a passive IDS on the same box doesn't change the reaction ability of the IDS. A passive IDS, whether implemented independently or on a platform with other devices, can only respond passively, which means the attack always reaches its victim.

## Only active responses eliminate the impact of the attack

The NetScreen-IDP system is the first in-line device capable of keeping your network safe by detecting and dropping the malicious traffic itself, so attacks never reach their victim.

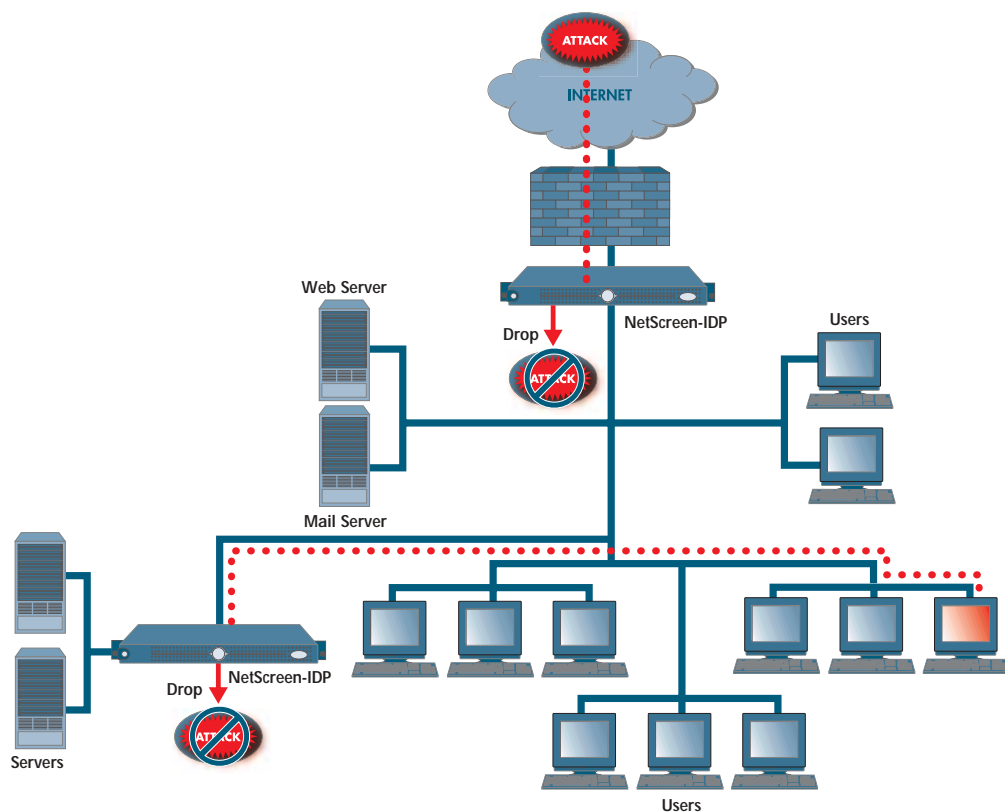
NetScreen-IDP uses a powerful rulebase that enables you to choose the exact conditions and attacks that warrant dropping the connection. Once you tell NetScreen-IDP to drop a specific connection, you no longer need to worry about that attack. You can also run NetScreen-IDP 100 and 500 in a High Availability configuration, giving you an extra measure of security when NetScreen-IDP operates as a gateway. If you prefer passive mode operation, you can run the NetScreen-IDP system as a sniffer and still derive the benefits of accurate detection and simple enterprise-wide management. However, NetScreen believes that once you have used NetScreen-IDP to prevent intrusions, you will never want to implement a passive mode IDS again. A firewall and an in-line NetScreen-IDP is a powerful combination, offering comprehensive protection for your most critical assets.

## Stop the attack during the detection process

*Not only do you need to know about the attacks in your network, but you also need to stop them. IDSes are passive and cannot directly stop an attack, so you need to spend a lot of time and money investigating the impact of an attack and recovering from the resulting damage.*

*The only way to secure your network is to stop an attack from ever impacting its destination, by dropping the offending traffic during the attack detection process. Any device that tries to stop the attack after it has been identified is too late.*

*Only an in-line device capable of detecting attacks and dropping the malicious packets itself, as soon as it is detected, can effectively stop an attack.*



## NetScreen-IDP Specifications

### Management Capabilities

3 Tier System		Yes
User Interface Platforms	Windows Linux	Yes Yes
Management Server Platforms	Linux RedHat 7.2 Solaris 8/9	Yes Yes
User Interface Mechanisms	Java Application Command Line Interface	Yes Yes
Number of Users		Unlimited
Centralized Management	Policy Management Log Viewing Incident Management	Yes Yes Yes
Logging		Over 50,000 logs per second
Log Exporting		Postgress SQL Database XML File CSV File
Signature Updates		Yes; signature updates provided weekly
Reports		Yes
System Status Monitoring		Yes

### Sensor Software

Detection Methods	8 Integrated Detection Methods	Yes
	Stateful Signature Detection	Yes
	Protocol Anomaly Detection	Yes
	Backdoor Detection	Yes
	Traffic Anomaly Detection	Yes
	IP Spoofing Detection	Yes
	DOS Detection	Yes
	Layer 2 Detection	Yes
	Network Honeygot	Yes

Signatures	Stateful Number of contexts supported Open signature format User definable Weekly updates provided Parallel signature matching	Yes 100+ Yes Yes Yes Yes
Traffic Interpretation	Reassembly Normalization Defragmentation	Yes Yes Yes
Active Responses	Drop Packet Drop Connection Resets	Yes Yes Yes
Passive Responses	TCP Resets Close Client Close Server Close Connection IP Actions	Yes Yes Yes Yes Yes
Notification Methods	Built-in Log Viewer SMTP (Email) Custom Script SNMP trap SYSLOG	Yes Yes Yes Yes Yes
Packet Management	User-specified logging Built-in packet viewer 3rd party compatibility	Yes Yes Yes
Operational Modes	Bridge Router Proxy-ARP Sniffer (Passive)	Yes Yes Yes Yes
Enterprise Networking	802.1Q VLAN Support SNMP MIB-II Support	Yes Yes

Sensor Hardware	NetScreen-IDP 10	NetScreen-IDP 100	NetScreen-IDP 500
Forwarding Interfaces			
10/100 Fast Ethernet:	2	2 (Expandable to 8)	None (Expandable to 8)
Gigabit Ethernet (Fiber):	None	None (Expandable to 2)	2
Copper Gigabit Ethernet		Optional	Optional
Management Interfaces			
10/100 Fast Ethernet	1	2	2
Memory (RAM):	512 MB	1 GB	4 GB
Maximum Session:	10,000	70,000	220,000
Throughput:	Up to 20 MB/Sec Nominal <sup>(1)</sup>	Up to 200 MB/Sec	Up to 500 MB/Sec
High Availability			
Standalone Failover:	No	Yes	Yes
HA Clustering:	No	Yes	Yes
Load Sharing:	No	Yes	Yes
3rd Party Failover:	No	Yes	Yes
Fail-Open:	Yes <sup>(2)</sup>	Yes <sup>(2)</sup>	No
Physical Redundancy			
Redundant Power:	No	Optional	Yes
RAID:	No	Optional	Yes
Physical			
AC Power Wattage:	275 Watts	275 Watts	275 Watts
AC Power Voltage:	100/240 VAC, 2.0-1.0 A, 50/60 Hz	100/240 VAC, 3.9-2.0 A, 50/60 Hz	100/240 VAC, 3.9-2.0 A, 50/60 Hz
System Battery:	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Operating Temp:	50° to 95°F	50° to 95°F	50° to 95°F
Storage Temp:	-40° to 149°F	-40° to 149°F	-40° to 149°F
Relative Humidity (Operating):	8% to 80% noncondensing	8% to 85% noncondensing	8% to 85% noncondensing
Relative Humidity (Storage):	5% to 95% noncondensing	5% to 95% noncondensing	5% to 95% noncondensing
Altitude (Operating):	-50 to 10,000 ft	-50 to 10,000 ft	-50 to 10,000 ft
Altitude (Storage):	-50 to 35,000 ft	-50 to 35,000 ft	-50 to 35,000 ft
Weight:	35.27 lbs.	35.27 lbs	35.27 lbs
Height:	1.69 in. 1U	1.69 in. 1U	1.69 in. 1U
Width:	19 in.	19 in.	19 in.
Depth:	26.9 in.	26.9 in.	26.9 in.

(1) The IDP-10 supports 20 MB/Sec of continuous throughput, however it can handle bursts at full line-speed.

(2) Requires NetScreen-IDP Bypass unit, which is purchased separately.

### Management server

Management software runs on either Solaris 7/8 or RedHat 7.2. Recommended RAM is 512 MB, Processor-1GHZ (Linux), 400 MHZ (Solaris), Hard Disk-18GB minimum

### Management GUI client application

The client application is a Java-based application that runs on Windows2000 and RedHat Linux version 7.2. JRE version 1.4.1 is included.

Disk Requirements: 64 MB

RAM Requirements: 256 MB

# Performance

## Performance

If a security device cannot keep up with traffic, information will be missed, enabling attackers to get by the system undetected. With NetScreen-IDP, you can be certain that all traffic is examined and intrusions are being handled on a real-time basis. It performs high-speed packet processing and alarm presentation to enable the immediate response to threats to your network. NetScreen-IDP runs in the kernel, eliminating the need to copy packets and perform multiple context switches. NetScreen-IDP is optimized to implement Multi-Method Detection at high data rates, using a proprietary algorithm that matches an unlimited number of signatures to traffic in parallel. As a result, NetScreen-IDP can maintain a fixed processing time; regardless of how many signatures it needs to match.

This approach provides efficiencies over all other products, which either match signatures one by one or match a few signatures at a time using parallel hardware or custom CPUs. Plus, NetScreen-IDP uses Stateful Signatures, eliminating the need to blindly compare attack patterns against all traffic.

Depending on your network requirements, there are currently three different NetScreen-IDP solutions to ensure you can effectively secure each network segment. NetScreen-IDP 10 is designed for branch-offices or low speed links. It provides Fast Ethernet connectivity and supports 20 MB/Sec of Nominal throughput; however, it can burst to full line-speed for sub-second bursts. For smaller central sites or large regional offices, NetScreen-IDP 100 is optimal, providing Fast Ethernet connectivity and the support of 200 MB/Sec maximum. Finally, NetScreen-IDP 500 is designed for large central sites, providing Gigabit Ethernet connectivity and support for upwards of 500 MB/Sec. For high traffic network segments, multiple NetScreen-IDP 100 or NetScreen-IDP 500 Sensors can be run in parallel, as a cluster, to increase performance capacity. NetScreen-IDP clusters automatically divide the network load, without the need to deploy third party load balancers, to provide multi-gigabit performance (2 gigabit maximum) to effectively protect your most trafficked network segments. NetScreen-IDP clustering enables stateful, stand-alone high availability, minimizing the risk of a single point of failure and maximizing your network protection.

## Ordering Information:

Product	Part Number
NetScreen IDP-10 Intrusion Detection and Protection Appliance	NS-IDP-10
NetScreen IDP-100 Intrusion Detection and Protection Appliance	NS-IDP-100
NetScreen IDP-500 Intrusion Detection and Protection Appliance	NS-IDP-500
<b>Accessories</b>	
NetScreen IDP-Bypass Fail Open Device (IDP-10 and IDP-100 only)	NS-IDP-BYP
NetScreen-IDP Fiber Gigabit NICs (set of 2 Cards)	NS-IDP-GB
NetScreen-IDP Quad 10/100 NIC	NS-IDP-QUAD-NIC
NetScreen-IDP Single 10/100 NIC	NS-IDP-NIC
NetScreen-IDP Redundant Hard Drive (IDP-100 and IDP-500 only)	NS-IDP-HD
NetScreen-IDP AC Power Supply (IDP-100 and IDP-500 only)	NS-IDP-PWR-AC
NetScreen-IDP Rapid Rail Kit	NS-IDP-RCK-01
NetScreen-IDP Chatsworth Rail Kit	NS-IDP-RCK-02

## 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, 001-408-616-5973 in Latin America or 852-2519-3988 in Asia, or visit us at [www.netscreen.com](http://www.netscreen.com).**

Copyright © 1998-2003 NetScreen Technologies, Inc.

NetScreen, NetScreen Technologies, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. IDP, MMD, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-1000, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, 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: 2003.4.60.2.idp

## Enterprise Networking capabilities

*The NetScreen-IDP solution supports advanced enterprise networking capabilities. These include 802.1Q VLAN Tagging on any interface, which allows the NetScreen-IDP Sensor to easily integrate with your existing switching and VLAN infrastructures. It also enables you to protect multiple logical network segments with a single device. Additionally, the NetScreen-IDP SNMP-based monitoring supports the MIB-II Standard, which allows you to use your existing SNMP-based network monitoring system (such as HP® OpenView™) to monitor IDP Sensors.*



**NETSCREEN®**  
Scalable Security Solutions

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

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