

# Juniper Networks IDP 50/200/600/1100



The Juniper Networks Intrusion Detection and Prevention products (Juniper Networks IDP) provide comprehensive and easy to use inline protection to stop network and application-level attacks before they inflict any damage, minimizing the time and costs associated with intrusions. Using industry recognized stateful detection and prevention techniques, Juniper Networks IDP provides day-zero protection against worms, Trojans, spyware, keyloggers, and other malware from penetrating the network and spreading from already infected users to others.

Juniper Networks IDP also provides information on rogue servers as well as types and versions of applications and operating systems that may have unknowingly been added to the network. Armed with the knowledge that unauthorized applications such as peer-to-peer or instant messaging have been added to the network, administrators can easily enforce compliance to security corporate application use policies. Not only can administrators control the access of specific applications, but with the support for Diffserv markings, they can now ensure business critical applications receive a predictable quality of service. Juniper Networks IDP products are managed by NetScreen Securix Manager (NSM), a centralized, rule-based management solution offering granular control over all Juniper FW, VPN and IDP products with easy access to extensive logging and fully customizable reporting, all from a single user interface. With the combination of highest security coverage, granular network control and visibility, and centralized management, Juniper Networks IDP is the best solution to keep critical information assets safe.

## Juniper Networks IDP 50/200/600/1100

**Management Capabilities** (Based on IDP 4.0 with NSM 2006.1 )

3 Tier System	
GUI Client Platforms	Windows NT, 2000, XP Red Hat Enterprise 3.0, 4.0
Management Server Platforms	Red Hat Enterprise 3.0, 4.0 Solaris 8, 9
User Interface Mechanisms	Java Application Command Line Interface
Number of Users	Unlimited
Centralized Management	Policy Management Log Viewing
Incident Management	
Role Based Administration	6 custom roles, 100 + activities
Complete Investigative Toolkit	Profiler Security Explorer
Logging	Over 50,000 logs per second
Log Exporting	PostgreSQL Database XMLFile CSVFile
Signature Updates	Signature updates provided daily, as well as in emergency Auto/Scheduled Signature Updates Auto/Scheduled Policy Update on Sensor
Reporting	Quick reports Fully customizable reports Exportable (HTML)
System Status Monitoring	Please see Juniper Networks NSM datasheet for more details on management specifications

### Sensor Software

Detection Methods (8 methods)	Stateful Signature Detection Protocol Anomaly Detection Backdoor Detection Traffic Anomaly Detection IP Spoofing Detection DoS Detection Layer 2 Detection Network Honeypot
Worm Protection	
Trojan Protection	
Spyware/Adware/Keylogger Protection	
Other Malware Protection	
Protection against attack proliferation from infected systems	
Reconnaissance Protection	
Request and Response Side Attack Protection	
VoIP Protection	
SYN Cookie	
Database Software Protection	

## Juniper Networks IDP 50/200/600/1100

Signatures	Stateful More than 500 number of contexts supported Compound (Stateful and Protocol Anomaly) Open signature format Custom, user definable Recommended Signatures from Juniper Security Team (for easy IDP policy configuration and hassle-free updates) Boolean Expressions Parallel signature matching
Protocols supported	More than 60
Traffic Interpretation	Reassembly Scrubbing Normalization
Active Responses	Drop Packet Drop Connection Diffserv (DSCP) marking 1-63
Passive Responses	TCP Resets Close Client Close Server Close Connection IP Action
Application Awareness	Application (L7) information/awareness Network (L2-L4) information/awareness Incident correlation Detailed Threat Descriptions and Remediation/Patch Info Enterprise Security Profiler (ESP) Create and enforce appropriate application usage policies Attacker and Target Audit Trail and Reporting
Notification Methods (Per-rule basis)	Built-in Log Viewer SMTP (Email) Custom Script SNMP trap SYSLOG XML CSV
Packet Management	User-specified logging Built-in packet viewer 3rd party compatibility
Operational Modes	Bridge Router Proxy-ARP Transparent Sniffer (Passive)
Enterprise Networking	802.1Q VLAN Support SNMP MIB-II Support

Sensor Hardware	Juniper Networks IDP 50	Juniper Networks IDP 200	Juniper Networks IDP 600C/600F	Juniper Networks IDP 1100C/1100F
<b>Interfaces</b>				
Traffic Ports	2 10/100/1000	8 10/100/1000	10 10/100/1000 or 8 FiberSX Gigabit <sup>(1)</sup> + 2 10/100/1000	10 10/100/1000 or 8 FiberSX Gigabit <sup>(1)</sup> + 2 10/100/1000
Management Ports	1 10/100/1000	1 10/100/1000	1 10/100/1000	1 10/100/1000
HA Ports	N/A	1 10/100/1000	1 10/100/1000	1 10/100/1000
<b>Memory (RAM)</b>				
	1 GB	1 GB	4 GB	4 GB
<b>Maximum Session Throughput</b>				
	10,000 Up to 50 Mbps	70,000 Up to 250 Mbps	220,000 Up to 500 Mbps	500,000 Up to 1 Gbps
<b>High Availability</b>				
Standalone Failover	No	Yes	Yes	Yes
HA Clustering	No	Yes	Yes	Yes
Load Sharing	No	Yes	Yes	Yes
3rd Party Failover	No	Yes	Yes	Yes
Fail-Open	Yes <sup>(2)</sup>	Yes <sup>(2)</sup>	Yes <sup>(2)</sup>	Yes <sup>(2)</sup>
<b>Physical Redundancy</b>				
Redundant Power	No	Optional	Yes	Yes
RAID	No	No	Yes	Yes
<b>Physical</b>				
AC Power Wattage	260 Watts	500 Watts	500 Watts	500 Watts
AC Power Voltage	100-240VAC, 60-50Hz, 5A Max	100-240VAC, 60-50Hz, 10A Max	100-240VAC, 60-50Hz, 10A Max	100-240VAC, 60-50Hz, 10A Max
System Battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell	3V coin cell
Operating Temp	50° to 95°F	50° to 95°F	50° to 95°F	50° to 95°F
Storage Temp	-40° to 158°F	-40° to 158°F	-40° to 158°F	-40° to 158°F
Relative Humidity (Operating)	8% to 90% noncondensing	8% to 90% noncondensing	8% to 90% noncondensing	8% to 90% noncondensing
Relative Humidity (Storage)	5% to 95% noncondensing	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	-50 to 10,000 ft
Altitude (Storage)	-50 to 35,000 ft	-50 to 35,000 ft	-50 to 35,000 ft	-50 to 35,000 ft
<b>Weight</b>				
	14.5 lbs	29.5 lbs	33.5 lbs	36.5 lbs
<b>Height</b>				
	1.69 in. 1U	3.4 in. 2U	3.4 in. 2U	3.4 in. 2U
<b>Width</b>				
	17 in.	17 in.	17 in.	17 in.
<b>Depth</b>				
	15 in.	19 in.	19 in.	19 in.
<b>MTBF (Bellcore model)</b>				
	66,000 hrs	45,000 hrs (56,000 hrs w/optional redundant power implemented)	48,000 hrs/45,000 hrs	48,000 hrs/45,000 hrs

(1) Each Fiber Gigabit interface is multimode (Base-SX) LC connectors only. If single mode is needed the user will need an external converter.

(2) Integrated Bypass for all 10/100/1000 traffic ports - link and power loss detection; the Fiber gigabit interfaces require third-party Bypass unit, which is purchased separately

### GUI Client Platform Requirements (Based on NSM 2006.1)

The client application is a Java-based application that runs on Windows 2000, NT, XP, Red Hat Enterprise 3.0 or 4.0. JRE version 1.4.2 is included.

Recommended capacities (min):

- CPU 400 MHz Pentium II or equivalent
- RAM 1 GB
- Available Disk Space 100MB
- Connectivity to Server 384 kbps (DSL) or LAN

### NSM Device Server Platform Requirements (Based on NSM 2006.1)

NSM Device Server software runs on Red Hat Enterprise 3.0 or 4.0, Solaris 8, or Solaris 9.

Recommended capacities (min):

- CPU: 1 GHz
- RAM: 1 GB for 1-2 sensors running Profiler; 2 GB for 3-8 sensors; 8 GB for 9-20 sensors
- Hard Disk 18 GB
- NIC 100 Mbps

An NSM Device Server will support up to 100 IDP sensors, of which 20 can be running Profiler, along with up to 2000 Juniper FW/VPN systems. A separate GUI Server option is available for deployments where log generation rates exceed 1000 logs per second for all devices or over 200 devices are being managed

### Product

Product	Part Number
IDP 50 Intrusion Detection and Prevention Appliance	NS-IDP-50
IDP 200 Intrusion Detection and Prevention Appliance	NS-IDP-200
IDP 600C Intrusion Detection and Prevention Appliance	NS-IDP600C
IDP 600F Intrusion Detection and Prevention Appliance	NS-IDP-600F
IDP 1100C Intrusion Detection and Prevention Appliance	NS-IDP-1100C
IDP 1100F Intrusion Detection and Prevention Appliance	NS-IDP-1100F
NetScreen-Security Manager, 5 devices (included with IDP purchase)	NS-SM-5
NetScreen-Security Manager, 10 devices	NS-SM-10
NetScreen-Security Manager, 25 devices	NS-SM-25
NetScreen-Security Manager, 50 devices	NS-SM-50
NetScreen-Security Manager, 100 devices	NS-SM-100
Other NSM options also available	

### Accessories/Spares

IDP AC Power Supply (IDP 200, 600 and 1100 only)	NS-IDP-PWR-AC-003
IDP Rail Kit	NS-IDP-RCK-03
IDP SCSI Hard Drive (IDP 600 and 1100 only)	NS-IDP-HD-003



CORPORATE HEADQUARTERS  
AND SALES HEADQUARTERS  
FOR NORTH AND SOUTH AMERICA  
Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888-JUNIPER (888-586-4737)  
or 408-745-2000  
Fax: 408-745-2100  
www.juniper.net

EAST COAST OFFICE  
Juniper Networks, Inc.  
10 Technology Park Drive  
Westford, MA 01886-3146 USA  
Phone: 978-589-5800  
Fax: 978-589-0800

ASIA PACIFIC REGIONAL  
SALES HEADQUARTERS  
Juniper Networks (Hong Kong) Ltd.  
Suite 2507-11, Asia Pacific Finance Tower  
Citibank Plaza, 3 Garden Road  
Central, Hong Kong  
Phone: 852-2332-3636  
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA  
REGIONAL SALES HEADQUARTERS  
Juniper Networks (UK) Limited  
Juniper House  
Guildford Road  
Leatherhead  
Surrey, KT22 9JH, U. K.  
Phone: 44(0)-1372-385500  
Fax: 44(0)-1372-385501

Copyright 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.