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 zero-day protection against worms, Trojans, spyware, keyloggers, and other malware from penetrating the network and spreading from already infected users to others. Juniper Networks IDP not only helps protect networks against attacks, it provides information on rogue servers and applications 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 allows administrators to more easily enforce security policies and maintain compliance with corporate application use policy. Combined with a centralized, rule-based management approach, which offers granular control over the system's behavior and easy access to extensive logging and fully customizable reporting, it is easy to see why Juniper Networks IDP is the best way to keep critical information assets safe.

		Juniper Networks IDP 50/200/600/1100
Management Capabilities (Based on IDP 3.1)		
3 Tier System		Yes
GUI Client Platforms	Windows 2000, XP	Yes
	Linux Red Hat 8, RHEL 3 AS, ES, WS	Yes
Management Server Platforms	Linux Red Hat 7.2 and 8 RHEL 3 AS, ES, WS	Yes
	Solaris 8 and 9	Yes
User Interface Mechanisms	Java Application	Yes
	Command Line Interface	Yes
Number of Users		Unlimited
Centralized Management	Policy Management	Yes
	Log Viewing	Yes
Incident Management		Yes
Logging		Over 50,000 logs per second
Log Exporting		PostgresSQL Database XMLFile CSVFile
Signature Updates		Yes; signature updates provided daily, as well as in emergency
Reporting		
Quick reports		Yes
Fully customizable reports		Yes
Exportable (HTML)		Yes
System Status Monitoring		Yes
Sensor Software		
Detection Methods (8 methods)	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 Honeypot	Yes
Worm Protection		Yes
Trojan Protection		Yes
Spyware/Adware/Keylogger Protection		Yes
Other Malware Protection		Yes
Protection against attack proliferation from infected systems		Yes
Reconnaissance Protection		Yes
Request and Response Side Attack Protection		Yes
VoIP Protection		Yes

		Juniper Networks IDP 50/200/600/1100
Signatures	Stateful	Yes
	Number of contexts supported	500 +
	Compound (Stateful and Protocol Anomaly)	Yes
	Open signature format	Yes
	Custom, user definable	Yes
	Parallel signature matching	Yes
Protocols supported		60 +
Traffic Interpretation	Reassembly	Yes
	Scrubbing	Yes
	Normalization	Yes
Active Responses	Drop Packet	Yes
	Drop Connection	Yes
Passive Responses	TCP Resets	Yes
	Close Client	Yes
	Close Server	Yes
	Close Connection	Yes
	IP Action	Yes
Application Awareness	Application (L7) information/awareness	Yes
	Network (L2-L4) information/awareness	Yes
	Incident correlation	Yes
	Detailed Threat Descriptions and Remediation/Patch Info	Yes
	Enterprise Security Profiler (ESP)	Yes
	Create and enforce appropriate application usage policies	Yes
	Attacker and Target Audit Trail and Reporting	Yes
Notification Methods	Built-in Log Viewer	Yes
	SMTP(Email)	Yes
	Custom Script	Yes
	SNMP trap	Yes
	SYSLOG	Yes
Packet Management	User-specified logging	Yes
	Built-in packet viewer	Yes
	3rd party compatibility	Yes
Operational Modes	Bridge	Yes
	Router	Yes
	Proxy-ARP	Yes
	Transparent	Yes
	Sniffer (Passive)	Yes
Enterprise Networking	802.1Q VLAN Support	Yes
	SNMP MIB-II Support	Yes

Sensor Hardware	Juniper Networks IDP 50	Juniper Networks IDP 200	Juniper Networks IDP 600C/600F	Juniper Networks IDP 1100C/1100F
Interfaces				
Traffic Ports	2 10/100/1000	8 10/100/1000	10 10/100/1000 or 8 FiberSX Gigabit(1) + 2 10/100/1000	10 10/100/1000 or 8 FiberSX Gigabit(1) + 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
Memory (RAM)	1 GB	1 GB	4 GB	4 GB
Maximum Session	10,000	70,000	220,000	500,000
Throughput	Up to 50 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps
High Availability				
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(2)	Yes(2)	Yes(2)	Yes(2)
Physical Redundancy				
Redundant Power	No	Optional	Yes	Yes
RAID	No	No	Yes	Yes
Physical				
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
Weight	14.5 lbs	29.5 lbs	33.5 lbs	36.5 lbs
Height	1.69 in. 1U	3.4 in. 2U	3.4 in. 2U	3.4 in. 2U
Width	17 in.	17 in.	17 in.	17 in.
Depth	15 in.	19 in.	19 in.	19 in.

(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 IDP 3.1)

The client application is a Java-based application that runs on Windows2000, NT, XP and Linux Red Hat 8 or RHEL 3 AS, ES, WS. JRE version 1.4.1 is included. Recommended capacities (min): 512 MB (IDP 3.1)

Management Server Platform Requirements

(Based on IDP 3.1)

IDP Management software runs on either Solaris 8 and 9 or Linux Red Hat 7.2/8 or RHEL 3 AS, ES, WS. Recommended processor (min): 1GHZ (Linux), 400 MHZ (Solaris). Recommended capacities (min): 1GB RAM and 18 GB hard disk.

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

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

Juniper NETWORKS

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