Juniper NETWORKS®

Datasheet

Juniper Networks IDP 75/250/800/8200

With the growing number and sophistication of network attacks, it's ever more important for companies to safeguard their networks. The problem is further compounded by the growing number of application and OS vulnerabilities, as well as the increasing speed with which new attacks are created to exploit these vulnerabilities. Juniper Networks Intrusion Detection and Prevention (IDP) products offer the latest capabilities in in-line network Intrusion Prevention System (IPS) functionality to protect the network from a wide range of attacks. Backed by the Juniper Networks Security Team, Juniper's IDP products also offer industry-leading response times to newly found vulnerabilities.

Product Description

Juniper Networks Intrusion Detection and Prevention (IDP) products provide comprehensive and easy-to-use in-line protection that stops network and application-level attacks before they inflict any damage to the network, minimizing the time and costs associated with maintaining a secure network. 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 or spreading from already infected users.

Juniper Networks IDP not only helps protect networks against attacks, it 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. Application signatures, available on the Juniper Networks IDP, goes a step further and enables accurate detection of specific applications such as peer-to-peer or instant messaging. Armed with the knowledge of specific applications running in the network, administrators can more easily enforce security policies and maintain compliance with corporate application use policy. Juniper Networks IDP also provides DiffServ markings to allow the routers to enforce bandwidth limitations on non-essential applications. Not only can administrators control the access of specific applications, but they can ensure that business-critical applications receive a predictable quality of service.

Juniper Networks IDP products are managed by Juniper Networks NetScreen-Security Manager (NSM), a centralized, rule-based management solution offering granular control over the system's behavior. NSM also provides easy access to extensive logging, fully customizable reporting, and management of all Juniper Networks firewall/VPN/IDP systems 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 75 brings full Intrusion Prevention System (IPS) capability to small and mid-size businesses as well as remote offices. The built-in ByPass functionality also provides a cost-effective method of ensuring continuous network availability. By offering the entire suite of IPS and high resiliency capabilities, businesses need not compromise on security when deploying cost-effective IPS products.

Juniper Networks IDP 250 and IDP 800 offer market-leading IPS capabilities to mid-size and large enterprises as well as service providers. Supporting various High Availability (HA) options, the Juniper IDP 250 and IDP 800 offer continual security coverage for enterprise and service provider networks.

Juniper Networks Integrated Security Gateway (ISG) offers a flexible solution for deploying integrated security products that support large enterprises and service providers. With the capability to add IDP security modules, the ISG product line offers market-leading integrated firewall, IPSec VPN and IPS capabilities in a single chassis.

Juniper Networks IDP 8200 offers market-leading performance with 10 Gbps of real-world throughput and is also suited for large enterprises and service providers. The large throughput also enables the deployment of IPS appliance at the network core in addition to the network perimeter to secure and enforce quality of service (QoS) within the corporate network. The built-in ByPass features as well as separation of control and data plane makes the IDP 8200 an ideal solution for networks requiring the highest throughput and reliability.

Features and Benefits

Traffic Detection Methods

Juniper Networks IDP products offer a combination of eight different detection methods to accurately identify the traffic flowing through the network. By providing the highest flexibility, the various detection methods also minimize false positives.

Feature	Feature Description	Benefit
Stateful Signature Detection	Signatures are applied only to relevant portions of the network traffic determined by the appropriate protocol context.	Minimize false positives.
Protocol Anomaly Detection	Protocol usage against published RFCs is verified to detect any violations or abuse.	Proactively protect network from undiscovered vulnerabilities.
Backdoor Detection	Heuristic-based anomalous traffic patterns and packet analysis detect Trojans and rootkits.	Prevent proliferation of malware in case other security measures have been compromised.
Traffic Anomaly Detection	Heuristic rules detect unexpected traffic patterns that may suggest reconnaissance or attacks.	Proactively prevent reconnaissance activities or block Distributed Denial of Service (DDoS) attacks.
IP Spoofing Detection	The validity of allowed addresses inside and outside the network is checked.	Permit only authentic traffic while blocking disguised source.
Denial of Service (DoS) Detection	SYN cookie-based protection from SYN flood attacks.	Protect your key network assets from being overwhelmed with SYN floods.
Layer 2 Detection	Layer 2 attacks are detected using implied rules for Address Resolution Protocol (ARP) table restrictions, fragment handling, connection timeouts and byte/length thresholds for packets.	Prevent compromised host from polluting an internal network using methods such as ARP cache poisoning.
Network Honeypot[1]	Open ports are impersonated with fake resources to track reconnaissance activities.	Gain insight into real-world network threats and proactively defend your network before a critical asset can be attacked.

IDP Capabilities

Juniper Networks IDP products offer several unique features that assure the highest level of network security.

Feature	Feature Description	Benefit
Protocol Decodes	More than 60 protocol decodes are supported along with more than 500 contexts to enforce proper usage of protocols.	Accuracy of signatures is improved through precise context of protocols.
Signatures[2]	Includes more than 5500 signatures for identifying anomalies, attacks, spyware and applications.	Attacks are accurately identified and attempts at exploiting a known vulnerability are detected.
Traffic Interpretation	Reassembly, normalization and protocol decoding are provided.	Overcome attempts to bypass other IDP detections by using obfuscation methods.
Application Awareness/ Identification	Includes use context, protocol information and signatures to identify applications on any port.	Enable rules and policies based on application traffic rather than ports—protect or police standard applications on non-standard ports.
Zero-Day Protection	Protocol anomaly detection and same-day coverage for newly found vulnerabilities are provided.	Your network is already protected against any new exploits.
Recommended Policy	Group of attack signatures are identified by Juniper Networks Security Team as critical for the typical enterprise to protect against.	Installation and maintenance are simplified while ensuring the highest network security.

[1] Network Honeypot features are not available on the IDP 8200.

[2] As of January 2008, there are 5,560 signatures available with approximately 10 new signatures added weekly.

Granular Traffic Control

To support a wide range of business requirements, Juniper Networks IDP products offer granular control over the flow of traffic in the network.

Feature	Feature Description	Benefit
Active Traffic Responses	Various response methods are supported including drop packet, drop connection, close client, close server and close client/server.	Provide appropriate level of response to attacks.
QoS/DiffServ Marking	Packets are marked using DiffServ code point (DSCP).	Optimize network and ensure necessary bandwidth for business-critical applications.
Passive Traffic Responses	Several passive responses such as logging and TCP reset are supported.	Gain visibility into current threats on the network with the ability to preempt possible attacks.
VLAN-Aware Rules	Unique policies are applied to different VLANs.	Apply unique policies based on department, customer and compliance requirements.
Recommended Actions	Juniper Security Team provides recommendations on appropriate action for each attack object.	Ease of maintenance. Administrators no longer need to research or be aware of appropriate response to each and every threat.
IPAction	Disable access at granular level is provided, ranging from specific host down to particular traffic flow for configurable duration of time.	Thwart attempts to launch DDoS attacks detected through traffic anomaly, DoS detection or network honeypot.

Centralized Management

Centralized management of Juniper Networks IDP and firewall products are enabled through NetScreen-Security Manager. NSM's tight integration across multiple platforms enables simple and intuitive network-wide security management.

Feature	Feature Description	Benefit
Role-Based Administration	More than 100 different activities can be assigned as unique permissions for different administrators.	Streamline business operations by logically separating and enforcing roles of various administrators.
Schedule Security Update	Automatically update IDP appliances with new attack objects/signatures.	Up-to-the-minute security coverage is provided without manual intervention.
Domains	Enable logical separation of devices, policies, reports and other management activities.	Conform to business operations by grouping of devices based on business practices.
Object Locking	Enable safe concurrent modification to the management settings.	Avoid incorrect configuration due to overwritten management settings.
Scheduled Database Backup	Automatic backup of NSM database is provided.	Provide configuration redundancy.
Job Manager	View pending and completed jobs.	Simplify update of multiple tasks and IDP devices.

Logging, Reporting and Notification

The combination of Juniper Networks IDP products and NSM offers extensive logging and reporting capabilities.

Feature	Feature Description	Benefit
IDP Reporter	Pre-configured real-time reporting capability available in each IDP appliance.	Provide detailed real-time reports from each IDP appliance installed in the network without taxing the central IT organization.
Profiler[3]	Capture accurate and granular detail of the traffic pattern over a specific span of time.	Up-to-the-minute security coverage is provided without manual intervention.
Security Explorer	Interactive and dynamic touchgraph provides comprehensive network and application layer views.	Greatly simplify the understanding of the network traffic as well as details of attacks.

[3] Profiler feature is not available with the IDP 8200.

Specifications

	IDP 75	IDP 250	IDP 800	IDP 8200
Dimensions and Power				
Dimensions (W x H x D)	17 x 1.69 x 15 in (43.2 x 4.3 x 38.1 cm)	17 x 1.69 x 15 in (43.2 x 4.3 x 38.1 cm)	17 x 3.4 x 19 in (43.2 x 8.6 x 48.3 cm)	17 x 3.4 x 19 in (43.2 x 8.6 x 48.3 cm)
Weight	15 lbs	16.5 lbs	27 lbs	41 lbs
A/C Power Supply	Auto Ranging 200 Watts	Auto Ranging 200 Watts	Auto Ranging 400 Watt Hot Swappable Dual Redundant	Auto Ranging 700 Watt Hot Swappable Dual Redundant
D/C Power Supply	N/A	N/A	N/A	710 Watt 48V DC Hot Swappable Dual Redundant
Mean Time Between Failures (MTBF)	66,000 hrs	45,000 hrs	48,000 hrs	48,000 hrs
Memory	1 GB	2 GB	4 GB	16 GB
Hard Drive	80 GB	80 GB	2 x 74 GB Redundant RAID 1 Array	2 x 74 GB Redundant RAID 1 Array
Ports				
Fixed I/O	Two RJ-45 Ethernet 10/100/1000 with bypass	Eight RJ-45 Ethernet 10/100/1000 with bypass	Ten RJ-45 Ethernet 10/100/1000 with bypass	N/A
Modular I/O Slots	0	0	0	4
Modular I/O Cards	N/A	N/A	N/A	4-port GE Copper with ByPass 4-port GE Fiber SFP 4-port GE SX-ByPass 2-port 10 GE SR-ByPass
Management	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000
High Availability (HA)	N/A	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000
Performance				
Max Session	10,000	70,000	500,000	5 Million
Throughput	150 Mbps	300 Mbps	1 Gbps	10 Gbps
Redundancy				
Redundant Power	No	No	Yes	Yes
RAID	No	No	Yes	Yes
Built-In Bypass	Yes	Yes	Yes	Yes
Environment				
Operating Temp	41 to 104° F (5 to 40° C)	41 to 104° F (5 to 40° C)	41 to 104° F (5 to 40° C)	41 to 104° F (5 to 40° C)
Storage Temp	-40 to 158° F (-40 to 70° C)	-40 to 158° F (-40 to 70° C)	-40 to 158° F (-40 to 70° C)	-40 to 158° F (-40 to 70° C)
Relative Humidity (operating)	8% to 90% condensing	8% to 90% condensing	8% to 90% condensing	8% to 90% condensing
Relative Humidity (storage)	5% to 95% noncondensing	5% to 95% noncondensing	5% to 95% noncondensing	5% to 95% noncondensing
Altitude (operating)	10,000 ft	10,000 ft	10,000 ft	10,000 ft
Altitude (storage)	40,000 ft	40,000 ft	40,000 ft	40,000 ft

Ordering Information

Model Number	Description
Juniper Networks IDP Appliances	
IDP75	IDP 75 Intrusion Detection and Prevention Appliance
IDP250	IDP 250 Intrusion Detection and Prevention Appliance
IDP800-BNDL	IDP 800 Intrusion Detection and Prevention Appliance
IDP8200	IDP 8200 Intrusion Detection and Prevention Appliance
I/O Modules for IDP 8200	
IDP-10GE-2SR-BYP	IDP 2 port 10GE with bypass (SR)
IDP-1GE-4COP-BYP	IDP 4 port copper with bypass
IDP-1GE-4SFP	IDP 4 port SFP (non-bypass)
IDP-1GE-4SX-BYP	IDP 4 port fiber with bypass (SX)
IDP-SFP-COP	IDP copper SFP
IDP-SFP-FLX	IDP fiber SFP LX
IDP-SFP-FSX	IDP fiber SFP SX
Management	
NS-SM-5	NetScreen-Security Manager, 5-Device License (included with IDP appliance)
NS-SM-10	NetScreen-Security Manager, 10-Device License
NS-SM-25	NetScreen-Security Manager, 25-Device License
NS-SM-50	NetScreen-Security Manager, 50-Device License
NS-SM-100	NetScreen-Security Manager, 100-Device License
	Additional NSM license options available

Model Number	Description
Accessories	
IDP-HDD	Replacement HDD for IDP 800 and IDP 8200
IDP-PS-DC	DC power supply for IDP 800 and IDP 8200
IDP800-PS-AC	AC power supply for IDP 800
IDP8200-PS-AC	AC power supply for IDP 8200
IDP-FLASH	Installation media for IDP75, IDP 250, IDP 800
IDP-FLASH-8200	Installation media for IDP 8200
IDP800-FAN	Replacement fan for IDP 800
IDP8200-FAN	Replacement fan for IDP 8200
IDP8200-ACC-RKMT-KIT-2U	Rack mounting kit for IDP 8200 (includes rails)
IDP800-ACC-RMKT-KIT-2U	Rack mounting kit for IDP 800 (includes rails)
IDP-ACC-RMKT-KIT-1U	Rack mounting kit for IDP 250 and IDP 75 (includes rails)

Performance-Enabling Services and Support

Juniper is the leader in Performance-Enabling Services and Support, which are designed around a time to value experience that accelerates, extends and optimizes the value of high performance networking. These services bring revenue-generating capabilities online faster for bigger productivity gains, faster rollouts of new business models and ventures, greater market reach, and higher levels of customer satisfaction. At the same time, Juniper helps build operational excellence—to maintain required levels of performance, reliability, and availability, scale and adapt to new business requirements, reduce operational costs, and cut exposure to IT risks.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

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

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44.(0).1372.385500
Fax: 44.(0).1372.385501

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.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803