IDP SERIES INTRUSION DETECTION AND PREVENTION APPLIANCES

(IDP75, IDP250, IDP800, IDP8200)

Product Overview

With the growing number of applications allowed in from the Internet and the increased exposure to sophisticated network attacks, it's ever more important for companies to safeguard their networks. Evasive methods of delivering exploits continue to increase and 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 IDP Series Intrusion Detection and Prevention Appliances offer the latest capabilities in in-line network intrusion prevention system (IPS) functionality to manage the use of unwanted applications and protect the network from a wide range of attacks delivered by those allowed applications. IDP Series appliances deliver comprehensive threat coverage and industry-leading response time for maximum protection of network resources.

Product Description

Juniper Networks® IDP Series Intrusion Detection and Prevention Appliances provide comprehensive management of unwanted applications and easy-to-use in-line protection that stops network- and application-level attacks before they inflict any damage, minimizing the time and costs associated with maintaining a secure network. Using industry-recognized stateful detection and prevention techniques, the IDP Series provides zero-day protection against worms, trojans, spyware, key loggers, and other malware from penetrating the network or spreading from already infected users.

IDP Series Intrusion Detection and Prevention Appliances not only help protect networks against attacks, they provide 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 IDP Series, go a step further by enabling accurate detection and reporting of volume used by applications such as social networking, peer-to-peer, or instant messaging. Armed with the knowledge of specific applications running in the network, administrators can use application policy enforcement rules to easily manage these applications by limiting bandwidth, restricting their use, or prioritizing them lower with DiffServ marking. Not only can administrators control the access of specific applications, they can ensure that business-critical applications receive a predictable quality of service (QoS) while enforcing security policies to maintain compliance with corporate application usage policies.

Collaborative projects are commonplace in today's workplace. Making sure that security policies are easily enforced requires knowledge of how those collaborative user groups are formed. The IDP Series works in harmony with Juniper Networks Unified Access Control infrastructure to enforce application and security policies based on user-role information learned from the IC Series Unified Access Control Appliances. The IC Series interacts with companies' Active Directory (AD) or LDAP servers to assign users to roles and provides host information upon which the IDP Series can act. This extends the application policy enforcement (APE) and IPS rules for management of applications and more control over threats.

Juniper Networks IDP8200 Intrusion Detection and Prevention Appliance offers market-leading performance with 10 Gbps of real-world throughput suited for large enterprises and service providers. The large throughput also enables the deployment of IPS appliances at the network core in addition to the network perimeter to secure and enforce QoS within the corporate network. The built-in bypass features as well as separation of control and data plane make the IDP8200 an ideal solution for networks requiring the highest throughput and reliability.

Juniper Networks IDP250 and IDP800 Intrusion Detection and Prevention Appliances offer market-leading IPS capabilities for mid-size and large enterprises as well as service providers. Supporting various high availability (HA) options, the IDP250 and IDP800 offer continual security coverage for enterprise and service provider networks.

The Juniper Networks IDP75 Intrusion Detection and Prevention Appliance brings full IPS capabilities 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.

IDP Series Intrusion Detection and Prevention Appliances are managed by Juniper Networks Network and Security Manager, 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 Series appliances from a single user interface. With the combination of highest security coverage, granular network control, and visibility and centralized management, the IDP Series is the best solution to keep critical information assets safe.

Features and Benefits

IDP Series Capabilities

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances offer several unique features that assure the highest level of network security.

FEATURE	FEATURE DESCRIPTION	BENEFIT
Application awareness/ identification	This 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.
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.
Predefined and custom signatures[1]	More than 6,200 predefined signatures are included for identifying anomalies, attacks, spyware, and applications. Customization of signatures to personalize the attack database is allowed.	Attacks are accurately identified and attempts at exploiting a known vulnerability are detected. Customers fine-tune the attack database specific to their environment to avoid false-positives.
Traffic interpretation	Reassembly, normalization, and protocol decoding are provided.	Overcome attempts to bypass other IDP Series detections by using obfuscation methods.
Application Volume Tracking (AVT)	This tracks and collects volumetric application usage information.	This aids in proper creation of application policies based on observed network bandwidth consumption by application.
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]As of June 2009, there are 6,200 signatures available with daily updates provided.

Traffic Detection Methods

The IDP Series offers 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 is provided.	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	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.

Granular Traffic Control

To support a wide range of business requirements, the IDP Series offers granular visibility and control over the flow of traffic in the network. Customers can interact with the IDP Series appliances using an application focus, threat prevention focus, or both by utilizing the application enforcement policy rules and IPS policy rules, respectively.

FEATURE	FEATURE DESCRIPTION	BENEFIT
Application policy enforcement	A rule base is dedicated to managing unwanted applications using any number of actions.	Easily mange the applications allowed into the network while maintaining threats at bay.
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.
Application rate limiting	This defines the amount of bandwidth allowed for an individual or group of applications by direction (client-to-server and server-to-client).	Preserve network resources by controlling the amount of bandwidth consumed by applications allowed into the network.
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.
Recommended actions	Juniper Networks Security Team provides recommendations on appropriate action for each attack object.	Ease of maintenance is provided. 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.
VLAN-aware rules	Unique policies are applied to different VLANs.	Apply unique policies based on department, customer, and compliance requirements.
MPLS traffic inspection	Network traffic encapsulated in MPLS labels is inspected.	The number of IDP Series sensors is reduced.

Centralized Management

Centralized management of IDP Series appliances and firewall products is enabled through Network and Security Manager. NSM has tight integration across multiple platforms that 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.
Scheduled security update	Automatically update IDP Series 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 Series appliances.

Logging, Reporting and Notification

The combination of IDP Series appliances and NSM offers extensive logging and reporting capabilities.

FEATURE	FEATURE DESCRIPTION	BENEFIT
IDP reporter	Preconfigured real-time reporting capability is available in each IDP Series appliance.	Provides detailed real-time reports from each IDP Series appliance installed in the network without taxing the central IT organization.
Profiler	Captures accurate and granular detail of the traffic pattern over a specific span of time.	Provides details on what threats are encountered by the network, as well as the mix of various application traffic.
Security explorer	Interactive and dynamic touch graph provides comprehensive network and application-layer views.	Greatly simplify the understanding of the network traffic as well as details of attacks.
Application profiler	Works with application volume tracking feature to display application usage and create application policy enforcement rules.	Quickly identify and control which applications are running on the network by simple log-to-rule creation step.

IDP75

IDP250

IDP800

IDP8200

Specifications

	IDP75	IDP250	IDP800	IDP8200
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 lb	16.5 lb	27 lb	41 lb
A/C power supply	100 - 240 VAC, 50 - 60 Hz 4.0 - 2.0 A Max 200 W	100 - 240 VAC, 50 - 60 Hz 5.0 - 1.5 A Cold swappable, max 300 W	100 - 240 VAC, 50 - 60 Hz 6.0 - 2.0 A Hot swappable, dual redundant, max 400 W	100 - 240 VAC, 50 - 60 Hz 10.0 - 4.0 A Hot swappable, dual redundant, max 700 W
D/C power supply	N/A	N/A	(Optional) 36 - 75 VDC, 24 - 11 A Hot swappable, dual Redundant, 710 W max	(Optional) 36 - 75 VDC, 24 - 11 A Hot swappable, dual redundant, 710 W max
Mean Time Between Failures (MTBF)	75,000 hrs	73,000 hrs	108,000 hrs	73,000 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	Two RJ-45 Ethernet 10/100/1000 with bypass	N/A
Modular I/O slots	0	0	2	4
Modular I/O cards	N/A	N/A	• 4-port Gigabit Ethernet copper with bypass • 4-port Gigabit Ethernet fiber SFP • 4-port Gigabit Ethernet SX-bypass	• 4-port Gigabit Ethernet copper with bypass • 4-port Gigabit Ethernet fiber SFP • 4-port Gigabit Ethernet SX-byPass • 2-port 10 Gigabit Ethernet w/o bypass 2-port 10 Gigabit Ethernet 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	100,000	300,000	1 Million	5 Million
Throughput	150 Mbps	300 Mbps	1 Gbps	10 Gbps
Redundancy				
Redundant power	No	No	Yes	Yes
DC	No	No	Yes	Yes
RAID	No	No	Yes	Yes
Built-in bypass	Yes	Yes	Yes	Yes
Environment				
Operating temperature	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)
Storage temperature	-40º to 158º F (-40º to 70º C)	-40º to 158º F (-40º to 70º C)	-40º to 158º F (-40º to 70º C)	-40º to 158º F (-40º to 70º C)
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)	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)
Altitude (storage)	40,000 ft (12,192 m)	40,000 ft (12,192 m)	40,000 ft (12,192 m)	40,000 ft (12,192 m)

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services/.**

Ordering Information

MODEL NUMBER	DESCRIPTION
IDP Series Appliances	
IDP75	IDP75 Intrusion Detection and Prevention Appliance
IDP250	IDP250 Intrusion Detection and Prevention Appliance
IDP800	IDP800 Intrusion Detection and Prevention Appliance
IDP8200	IDP8200 Intrusion Detection and Prevention Appliance
I/O Modules for IDP800 and IDP8200	
IDP-10GE-2SR-BYP	IDP 2-port 10GbE with bypass (SR) (For IDP8200 only)
IDP-10GE-2XFP	IDP 2-port 10GbE (SR/LR) (For IDP8200 only)
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)
UNIV-SFP-COP	IDP copper SFP
UNIV-SFP-FLX	IDP fiber SFP LX
UNIV-SFP-FSX	IDP fiber SFP SX
UNIV-SFP-FSR	XFP short range fiber transceiver
UNIV-SFP-FLR	XFP long range fiber transceiver
Management*	
NS-SM-S-BSE	Network and Security Manager software with 25-Device License
NS-SM-ADD-50D	Additional 50-Device License
NS-SM-ADD-100D	Additional 100-Device License
	Additional NSM license options available

MODEL NUMBER	DESCRIPTION
Accessories	
UNIV-74G-HDD	Replacement HDD for IDP800 and IDP8200
UNIV-PS-710W-DC	DC power supply for IDP800 and IDP8200
UNIV-PS-400W-AC	AC power supply for IDP800
UNIV-PS-700W-AC	AC power supply for IDP8200
UNIV-PS-300W-AC	AC power supply for IDP250
IDP-FLASH	Installation media for IDP75, IDP250, IDP800
IDP-FLASH-8200	Installation media for IDP8200
UNIV-MR2U-FAN	Replacement fan for IDP800
UNIV-HE2U-FAN	Replacement fan for IDP8200
UNIV-HE2U-RAILKIT	Rack mounting kit for IDP8200 (includes rails)
UNIV-MR2U-RAILKIT	Rack mounting kit for IDP800 (includes rails)
UNIV-MR1U-RAILKIT	Rack mounting kit for IDP250 and IDP75 (includes rails)

*5-Device License included with every IDP Series appliance.

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**.

Corporate and Sales Headquarters
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

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

1000221-004-EN Dec 2009

Printed on recycled paper