Juniper Networks
IDP 50/200/600/1100

Portfolio Description

The Juniper Networks Intrusion Detection and Prevention (IDP) products provide comprehensive and easy-to-use in-line protection to stop 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 to others.

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. Armed with the knowledge that applications such as peer-to-peer or instant messaging have been added to 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 upstream router to enforce bandwidth limitations on nonessential 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, easy access to extensive logging, fully customizable reporting and management of all Juniper FW/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 50 brings full Intrusion Prevention System (IPS) capability to small and mid-size businesses as well as remote offices. By offering the entire suite of IPS capabilities, businesses need not compromise on security when deploying cost-effective IPS products. Juniper Networks IDP 50 can be deployed with third-party bypass gear to ensure continued network connectivity in case of appliance failure.

Juniper Networks IDP 200, IDP 600 and IDP 1100 offer market-leading IPS capabilities to mid-size and large enterprises as well as service providers. Supporting various high-availability options, the Juniper IDP 200, IDP 600 and IDP 1100 offer continual security coverage for enterprise and service provider networks.

Juniper Networks Integrated Security Gateway (ISG) provides flexible solution for deploying integrated security product for large enterprise 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.

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 in 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) to protect the network from a wide range of attacks. Backed by the Juniper Networks Security Team, Juniper Networks IDP products also offer industry-leading response time to newfound vulnerabilities.

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. While 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	Protocols 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 DDOS attacks.
IP Spoofing Detection	The validity of allowed addresses inside and outside the network are checked.	Permit only authentic traffic while blocking disguised source.
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 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.

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 are improved through precise contexts of protocols.
Signatures[1]	There are more than 5000 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	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 typical enterprise to protect against.	Installation and maintenance are simplified while ensuring the highest network security.
Multi-Operational Modes	Various configuration modes are available including Sniffer, Transparent, Bridge and Router mode.	Provide flexibility to deploy an IDP in wide range of network scenarios.

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 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.	Provide visibility into current threats on the network, and 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.

[1]As of March 2007, there are 5,148 signatures with approximately 10 new signatures added every week.

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 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. The 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 to 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
Profiler	Capture accurate and granular detail of the traffic pattern over a specific span of time.	Provide details on what threats are encountered by the network as well as the mix of various application traffic.
Security Explorer	Interactive and dynamic touchgraph provide comprehensive network and application layer views.	Greatly simplify the understanding of the network traffic as well as details of attacks.

Specifications

	IDP 50	IDP 200	IDP 600C/600F	IDP 1100C/1100F
Dimensions and Power				
Dimensions	17"W x 1.69"H x 15"D	17"W x 3.4"H x 19"D	17"W x 3.4" H x 19"D	17"W x 3.4" H x 19"D
Weight	15lb	29.5lb	33.5lb	36.5lb
A/C Power Supply	100-240VAC, 50-60Hz, 5A Max, 260 Watts	100-240VAC, 50-60Hz, 10A Max, 500 Watts	100-240VAC, 50-60Hz, 10A Max, 500 Watts	10A100-240VAC, 50-60Hz, 10A Max, 500 Watts
System Battery	CR2032 3V Lithium coin cell	CR2032 3V Lithium coin cell	CR2032 3V Lithium coin cell	CR2032 3V Lithium coin cell
MTBF	66,000 hrs	45,000 hrs (56,000 hrs w/ redundant power)	48,000 hrs	48,000 hrs
Memory	1GB	1GB	4GB	4GB
Ports				
Traffic	2 RJ-45 Ethernet – 10/100/1000	8 RJ-45 Ethernet – 10/100/1000	RJ-45 Ethernet 10/100/1000 or Eight FiberSx Gigabit and Two RJ-45 Ethernet - 10/100/1000	RJ-45 Ethernet - 10/100/1000 or Eight FiberSx Gigabit and Two RJ-45 Ethernet - 10/100/1000
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
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	220,000	500,000
Throughput	Up to 50 Mbps	Up to 220 Mbps	Up to 500 Mbps	Up to 1Gbps

Specifications cont'd

	IDP 50	IDP 200	IDP 600C/600F	IDP 1100C/1100F
Redundancy				
Standalone Failover	No	Yes	Yes	Yes
HA Clustering	No	Yes	Yes	Yes
Load Sharing	No	Yes	Yes	Yes
Third-Party Failover	No	Yes	Yes	Yes
Fail-Open (via third- party bypass)	Yes	Yes	Yes	Yes
Redundant Power	No	Optional	Yes	Yes
RAID	No	No	Yes	Yes
Environment				
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% 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)	-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
Certifications				
Common Criteria EAL2	Yes	Yes	Yes	Yes

Ordering Information

Juniper Networks IDP Appliances

NS-IDP-50	IDP 50 Intrusion Detection and Prevention Appliance
NS-ISP-200	IDP 200 Intrusion Detection and Prevention Appliance
NS-IDP-600C	IDP 600C Intrusion Detection and Prevention Appliance
NS-IDP-600F	IDP 600F Intrusion Detection and Prevention Appliance
NS-IDP-1100C	IDP 1100C Intrusion Detection and Prevention Appliance
NS-IDP 1100F	IDP 1100F Intrusion Detection and Prevention Appliance

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	

Accessories

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

About Juniper

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support many different services and applications at scale. Service providers, enterprises, governments, and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security, and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at www.juniper.net.