PRODUCT CATEGORY BROCHURE

IDP SERIES INTRUSION DETECTION AND PREVENTION APPLIANCES

Staying One Step Ahead

With the accelerating number of applications allowed in from the Internet and the higher frequency and sophistication of network attacks, it's increasingly important that you stay one step ahead. You can no longer just rely on solutions that merely react to new threats. Your solution must proactively manage application usage, protect your network based on newly found vulnerabilities and at times, even offer attack coverage before they run rampant.

To ensure a predictable quality of service for business-critical applications, your security policies must prioritize traffic by both application and user identity.

To secure your network from new viruses and attacks, your security solution must offer multiple attack detection methods and an efficient way to use the various capabilities.

To stay one step ahead of these attacks, you need a solution that can adapt to ever-changing security threats and allow you to do so with minimal effort.

Most Comprehensive Attack Coverage Available

IDP75

IDP250

IDP800

IDP8200

Juniper Networks® IDP Series Intrusion Detection and Prevention Appliances with Multi-Method Detection (MMD), offers comprehensive coverage by leveraging multiple detection mechanisms. For example, by utilizing signatures, as well as other detection methods including protocol anomaly traffic anomaly detection, the Juniper Networks IDP Series appliances can thwart known attacks as well as possible future variations of the attack.

Backed by Juniper Networks Security Lab, signatures for detection of new attacks are generated on a daily basis. Working very closely with many software vendors to assess new vulnerabilities, it's not uncommon for IDP Series to be equipped to thwart attacks which have not yet occurred. Such day-zero coverage ensures that you're not merely reacting to new attacks, but proactively securing your network from future attacks.

Minimizing False Positives, Increasing Peace of Mind

One of the top concerns in deployment of any IDP solution is false positives. Incorrectly identifying valid access and traffic as an attack could at times be just as damaging as a true attack. Critical business activities can be delayed and additional IT resources needed to investigate and determine the nature of the false positives.

Juniper Networks IDP Series with Stateful Signature Detection dramatically reduces false positives by examining the traffic in the context of the application. With full understanding of the application and its relevant traffic, the IDP Series can pinpoint the signature pattern-matching to the exact location where an attack can occur.

This application layer intelligence dramatically reduces the number of false positives compared to IDP platforms utilizing traditional non-stateful signature detection. In addition to the improved accuracy of the detection, the throughput of the solution is also optimized as the pattern detection is applied only to relevant network traffic.

Real-World Performance Without Sacrificing Security

Network throughput capacity of IDP platforms by itself often lends very little to the true performance of the appliance in a real-world environment. Many IDP platforms can exhibit very high throughput when only few attacks are being monitored. When more and more attack detections are enabled, the overall throughput can degrade. Also, while some appliances ship with default coverage settings optimized for performance, these settings often do not include the necessary attack coverage necessary in real-world deployments.

The throughput of Juniper Networks IDP Series appliances span wide range enterprise and service provider needs from 150 Mbps to 10 Gbps. All performance measurements are conducted in real-world deployment scenarios and are indicative of performance customers can expect when installing the IDP Series in their network.

JUNIPER NETWORKS SERVICE 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/.**

Streamline Your business With Better Understanding of Your Network

While an IDP solution is a critical component of every enterprise security infrastructure, it also offers the benefit of streamlining your business based on the applications used in the network. In addition to identifying viruses and attacks, the Juniper Networks IDP Series can identify the application associated with the particular traffic. Application intelligence enables accurate detection and reporting of volume used by applications such as social networking, peer-to-peer, or instant messaging. Armed with the knowledge of these applications running in the network, administrators can easily manage them by limiting bandwidth, restricting their use, or changing their prioritization for the best network optimization.

By accurately identifying and prioritizing application traffic, enterprises can ensure the necessary network bandwidth for business-critical applications without banning or blocking non-business applications. If necessary, specific application traffic can be blocked altogether to meet business or regulatory compliance.

Identity-Based Security That Delivers More Control

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 and which groups have application usage rights. The IDP Series works in harmony with Juniper Networks Unified Access Control infrastructure to obtain user role information gathered from the IC Series Unified Access Control Appliances thereby enabling enforcement of application and security policies based on user roles. The IC Series interacts with a company's Active Directory (AD) or LDAP servers to assign users to roles and provides host information upon which the IDP Series appliance can act. This allows for better management of applications and more control over threats by extending application policy enforcement and IPS rules with user role information.

Appliances and Integrated Solutions to Meet the Needs of Every Organization

Juniper Networks IDP Series appliances span a wide range of products offering network security solutions for small, mid-size and large enterprises, as well as data centers and service providers.

The appliances can be deployed in existing networks to thwart network attacks and interface with other Juniper Networks products such as the firewall and SSL VPN solutions to provide the highest level of network security available. The integrated IDP Series appliances offer the combination of IDP and firewall capabilities in a single footprint simplifying installation, network management and maintenance.

FEATURE	BENEFITS
Stateful signatures	• Intelligently track the state of the connection/traffic and scan for attack patterns matching the signature • Minimizes false-positives • Optimizes performance
Zero-day protection	• Protocol anomaly detection and same-day coverage for newly found vulnerabilities.
Traffic anomaly detection	• Identify attacks spanning multiple connections by comparing incoming traffic volume to baseline activities • Thwart attacks such as network probes and port scans
Application awareness/ identification	• Use of context, protocols and signatures to identify applications on any port. • Enable rules and policies based on applications.
Application policy enforcement	• Manage unwanted applications with various actions while maintaining threat coverage.
Application volume tracking	• Observe network bandwidth consumption per application.
Network honeypots	• Proactively identify potential attackers by impersonating network services that do not exist • Using the attacker's IP address, future attacks can easily be thwarted

Service and Support When and Where You Need It

To ensure your network is always secure, the Juniper Networks IDP Series Intrusion Detection and Prevention Appliances include the latest signatures and updates available from our Security Research Lab. Since new attacks can occur on a daily and sometimes hourly basis, your solution is not complete without the backing of Juniper Networks Security Research Lab.

Juniper Networks Professional Services consultants and authorized Juniper Networks partners are recognized as knowledgeable networking specialists throughout the industry. They are uniquely qualified to assist you in planning and implementing your IDP solution as well as other networking and security infrastructure solutions.

Juniper Networks Customer Support Center provides assistance, software upgrades, security updates and online knowledge tools to ensure highest reliability of your Juniper Network products. Juniper Networks Educational Services help customers keep pace with rapidly evolving technologies by sharing their expertise on how to operate and maintain secure networks.

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

♻ Printed on recycled paper

1500025-004-EN Oct 2009