Intrusion Detection and Prevention Portfolio

Juniper Networks IDP Appliances

Small/Mid Size Businesses

IDP 75

Regional Office

ISG 2000

Internet

IDP 800

IDP 8200

Admin

Server

Juniper Networks IDP 75

Juniper Networks IDP 250

Juniper Networks IDP 800

Juniper Networks IDP 8200

Juniper Networks ISG 1000

Juniper Networks ISG 2000
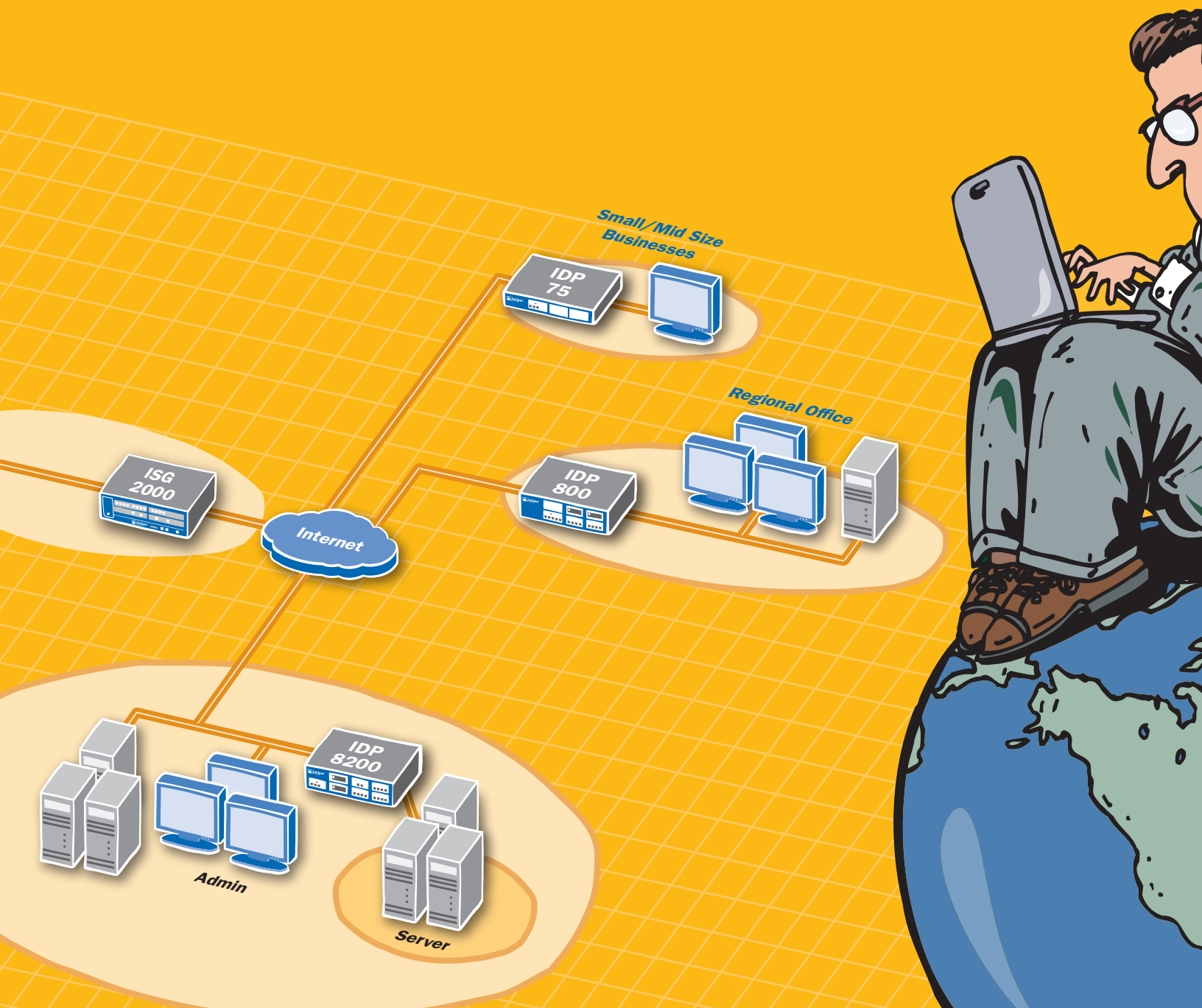
Staying one step ahead

As the frequency and sophistication of network attacks increases, 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 protect your network based on newly found vulnerabilities and at times, even offer attack coverage before they run rampant.

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

Juniper Networks® IDP 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 appliance 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 Juniper Networks IDP appliances 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 appliances 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 Juniper Networks IDP appliance 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 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 appliances in their network.

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 appliance can identify the application associated with the particular traffic. Based on this information, the relevant network traffic can be routed, blocked or prioritized to best optimize the network.

By accurately identifying and prioritizing application traffic, enterprise 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 all together to meet business or regulatory compliance.

Appliances and integrated solutions to meet the needs of every organization

Juniper Networks IDP 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 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
Protocol Anomaly Detection	• Identifies attacks using ambiguous traffic for particular network protocol such as SMB file sharing and SNMP as well as VoIP protocols such as SIP
Backdoor Detection	• Detect unauthorized interactive traffic due to worms or trojans inadvertently installed on trusted node • Detect attacks even if traffic is encrypted or utilized unknown protocol
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
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
Compound Signatures	• Combine stateful signatures to identify possible attacks even across multiple sessions

Service and support when and where you need it

To ensure your network is always secure, the Juniper Networks IDP family support offering includes 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.

Juniper
your
Net ™