GENERATING NEW REVENUE STREAMS AND INCREASING NETWORK SECURITY

Dynamic Application Awareness and Intrusion Prevention System

Table of Contents

Executive Summary 3
Introduction 3
Evolving the Network to Increase Revenues 3
Pro-Actively Guarantee Quality of User Experience 4
Application Identification 4
Security 4
Policy and Identity Management for All-IP Networks 5
Junos OS Implementation: Dynamic Application Awareness and IPS 6
Inspecting Packets 7
Identifying Applications 7
Classifying Applications 8
Increasing Scalability 8
Enforcing Policies 8
Conclusion 9
Acronyms 9
About Juniper Networks 9

Table of Figures

Figure 1: Projected global mobile and data traffic vs. revenues for 2008-2013 3
Figure 2: Architecting network intelligence to enable new service models 5
Figure 3: Logical packet flow 6

List of Tables

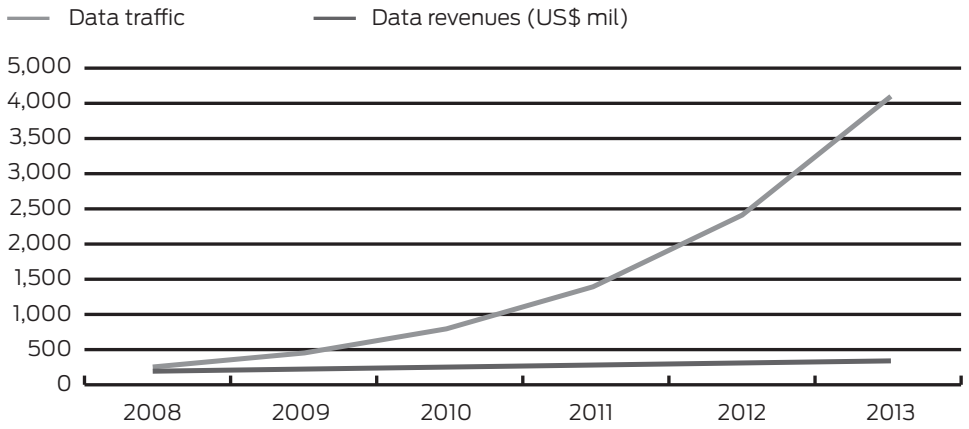
Table 1: Revenue-Generating Identity Use Cases 5
Table 2: Revenue-Generating Policy Use Cases 5

Executive Summary

This paper examines ways in which Juniper Networks® Dynamic Application Awareness and intrusion prevention system (IPS) software solutions enable service providers to increase revenue while expanding service flexibility, richness, and reach. The paper then describes the technologies behind these advanced solutions.

Introduction

In today's challenging economic environment, higher service revenues and profit margins are imperative. There is also a clear need to reduce CapEx and OpEx while deploying services with faster time to market. Yet, additional investments seem inevitable to accommodate traffic growth. In fact, the market trend indicates that revenues and traffic are decoupled. The 2008-2013 projection is for traffic to increase 1,587%, but for revenues to increase only 87% (Figure 1). Mobile, too, is slated to grow significantly faster than fixed traffic.[1]



Source: Informa Telecoms & Media

Figure 1: Projected global mobile and data traffic vs. revenues for 2008-2013

Juniper Networks M Series Multiservice Edge Routers Multiservices PIC (MS-PIC) and Juniper Networks MX Series 3D Universal Edge Routers Multiservices Dense Port Concentrator (MS-DPC) support two powerful software applications that address these growing traffic needs while overcoming economic hurdles. Moreover, these applications support the delivery of rich, value-added services, offering new means of revenue generation.

Dynamic Application Awareness—Supports advanced router-integrated application identification for the classification and policing of traffic associated with a particular application. The collection of statistics related to these activities also helps align infrastructure investments with application requirements, improve the operational environment, and create highly differentiated service offerings.

Intrusion prevention system—Tightly integrates Juniper's latest and most advanced security features with the network infrastructure to provide protection from a wide range of threats and attacks.

Evolving the Network to Increase Revenues

Innovative new service introduction is traditionally difficult, expensive, and time-consuming. Juniper Networks portfolio removes much of this cost and complexity, and permits the deployment of innovative new services based on a contextual combination of identity, location, device, application, and network state, all without compromising performance, scale, or reliability.

You no longer need to rely on equipment that offers only vanilla services. Moving towards increased service revenues means moving to an intelligent network where traffic is interrogated to determine its application type and to determine whether it represents a threat. This ability to recognize, characterize, and act upon specific traffic opens up opportunities in both on-net (walled garden) and off-net (open garden) environments.

[1] Source: Informa Telecoms & Media

In an on-net Junos® OS-based environment, you can deploy your own rich, multimedia services to a captive audience with full control over service delivery. By converging services over a common network, customer loyalty can be more readily gained and infrastructure upgrade costs reduced. Revenues are increased with more efficient traffic usage and bandwidth, and with wider flexibility in service deployment.

Using Junos OS-based solutions in an off-net environment, you can utilize third-party services and content to expedite time to market while charging both upstream and downstream. There is no heavy burden on application development, thus reducing costs and risks.

Pro-Actively Guarantee Quality of User Experience

Intelligent tools enable you to create tiered services and pro-actively enhance the user's experience while providing a choice of quality, price, and even security levels. The net result of this is higher ARPU, lower customer churn, and higher service uptake.

Application Identification

Consistently high service quality is required to avoid customer churn, and thus maintain revenue streams. Likewise, you must be able address the quality requirements of different applications and even create service tiers for several user groups that likely perceive quality of experience differently. The Dynamic Application Awareness solution achieves these goals, providing the processing power for both stateful and stateless detection and identification of L4-L7 applications. Residing on the MS-PIC in the M Series routers and on the MS-DPC in the MX Series routers, Dynamic Application Awareness uses deep inspection (DI) technology to examine the L4-L7 payload via port, address, and signature detection methods. Since this solution is integrated into the MS-PIC and MS-DPC, forklift upgrades are avoided along with the increased OpEx associated with qualifying, deploying, and maintaining standalone packet-inspection appliances.

Dynamic Application Awareness also improves the efficiency of the operations environment. For instance, you can collect and export data on application usage to enhance route and capacity planning activities, verify adherence to SLAs, and more precisely model the impact of specific applications on the network. Thus, with Dynamic Application Awareness, you can better align infrastructure investments with actual application requirements.

Full integration with Junos OS routing services, subscriber management functions, and policy management products provides dynamic policy-based application control that is tightly coupled with subscriber identity and network privileges. This coupling, in turn, enables the deployment of tiered services that include CoS and SLAs based on combinations of applications, subscriber-defined privileges, and provider-defined policies.

Security

Juniper's IPS protects the control plane and offers improved security for enhanced end-user experiences. We tightly integrate Junos OS IP technology with the most advanced security features, providing protection from a wide range of threats and attacks from both inside and outside the network, as well as supporting real-time policy assessment and enforcement.

Integrating IPS with M Series and MX Series routers reduces CapEx and OpEx by eliminating (or reducing) the need for standalone security appliances. By avoiding appliance proliferation, costs associated with inventory sparing, space, power, and cooling can be significantly reduced, as well as costs associated with qualifying, installing, managing, and maintaining security appliances.

CapEx and OpEx are similarly reduced due to the scalable, adaptive, future-proof nature of Junos OS. This will be critical in the future as the expected mobile traffic explosion from HSPA+/LTE will push current infrastructures to their limits. IPS offers a multilayered security matrix that secures and transports signaling and application layers with tight integration to identity and policy management functions.

Policy and Identity Management for All-IP Networks

Policy and identity management are the only mechanisms to date for guaranteeing real-time IP services without massive CapEx, and are absolute requirements for converged, service-oriented networks (Figure 2).

- Using a centralized policy engine and subscriber identity data enables you to interoperate between different networks, thus enabling cross-network, value-added service deployment.
- Junos OS identity and policy management technologies are independent of the transport network and maintain compatibility with future networks.
- With these technologies, you can cost-effectively allocate resources and avoid improper use by third parties.

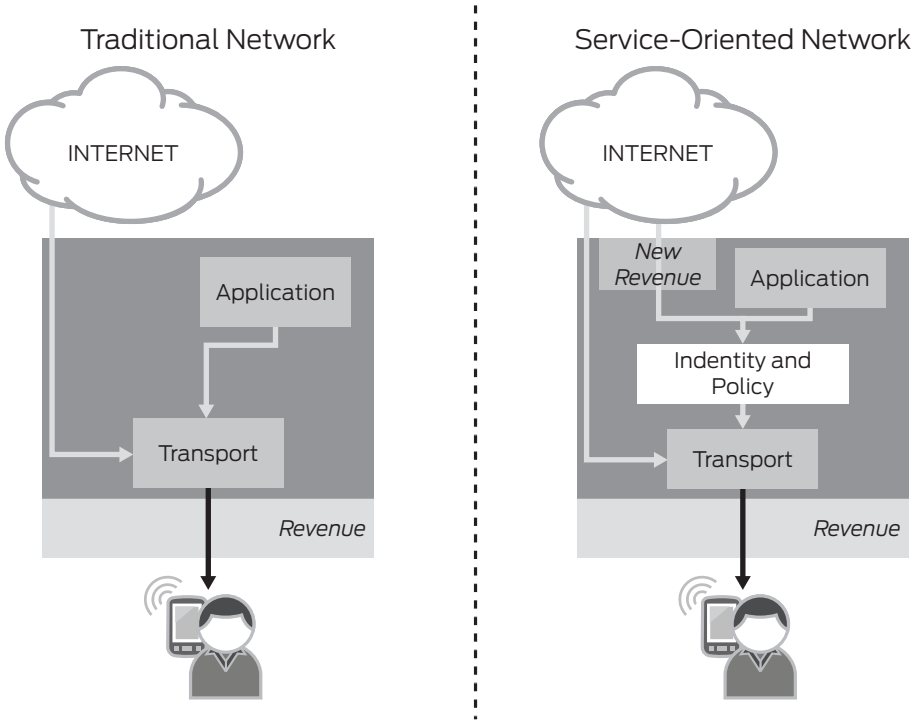


Figure 2: Architecting network intelligence to enable new service models

Tables 1 and 2 identify typical identity and policy use cases, respectively, for a wide variety of service deployments. Furthermore, transparent, flexible controls and billing enable you to apply granular charging mechanisms, such as per session, per subscriber, and per service, individually or in combination.

Table 1: Revenue-Generating Identity Use Cases

ON-NET SERVICES	VALUE-ADDED SERVICES
• Reduced sign-on	• Postpaid and prepaid billing
• Per-service billing	• Address management
• Network-aware services	• Concurrency management
• Mobility-aware services	• Wholesale
	• Lawful intercept
	• Roaming
	• Hot lining and redirect

Table 2: Revenue-Generating Policy Use Cases

NEW SUBSCRIPTION SERVICES	ON-NET SERVICES	OFF-NET SERVICES	OVER-THE-TOP SERVICES
• Tiered broadband plans	• Video on demand	• Content providers	• P2P mitigation
• Public WLAN	• IMS VoIP	• Gaming	• Enhanced P2P
• Turbo WLAN	• Video telephony	• Software as a service	• Congestion management
• Dynamic business services	• Video conferencing		• Threat mitigation

Junos OS Implementation: Dynamic Application Awareness and IPS

As opposed to most appliances that must examine every packet in every session, Dynamic Application Awareness and IPS enable you to identify applications by optionally configuring the software to examine just the first few packets of newly initiated sessions. Once the application is identified, a router-integrated policy manager provisions the forwarding plane (in real time) with the appropriate session handling instructions (such as, block, rate limit, apply CoS, etc). The forwarding plane resources then ensure that the session is treated and forwarded in accordance with the policy, and the service plane resources can be allocated to other sessions, permitting the solution to scale with high performance. Traffic flows through the Dynamic Application Awareness and the IPS processes as follows (Figure 3).

1. The subscriber initiates a session.
2. Dynamic Application Awareness: The session is forwarded to the Dynamic Application Awareness engine hosted on the MS-PIC/MS-DPC.

   IPS: The session is forwarded to the IPS engine hosted on the MS-PIC/MS-DPC.
3. Dynamic Application Awareness: The packet header is searched to identify the application based on its port, address, or signature.

   IPS: The packet is searched to identify threats and attacks using the following detection mechanisms.

   - Anomaly—check traffic against protocol standard.
   - Signature—protocol-aware context signature.
   - Backdoor—detect traffic bypassing normal authentication procedures.
4. The application policy request is forwarded to a local policy manager.
5. The local policy manager compares the identified application against a customer-defined list of application handling instructions.

   By default, all packets in the session are examined. One user-configurable option is that the session incurs no further analysis. In this case, Dynamic Application Awareness or IPS no longer analyzes this session, and its resources are available to analyze other sessions. Otherwise, the traffic is pushed to the forwarding plane (step 6).
6. The local policy manager provisions the appropriate enforcement functions on the forwarding plane in real time.

   - Rate limit traffic, packet drop
   - Classify traffic (DSCP mark for CoS handling)
   - Connection close, block traffic
   - Statistic gathering and logging

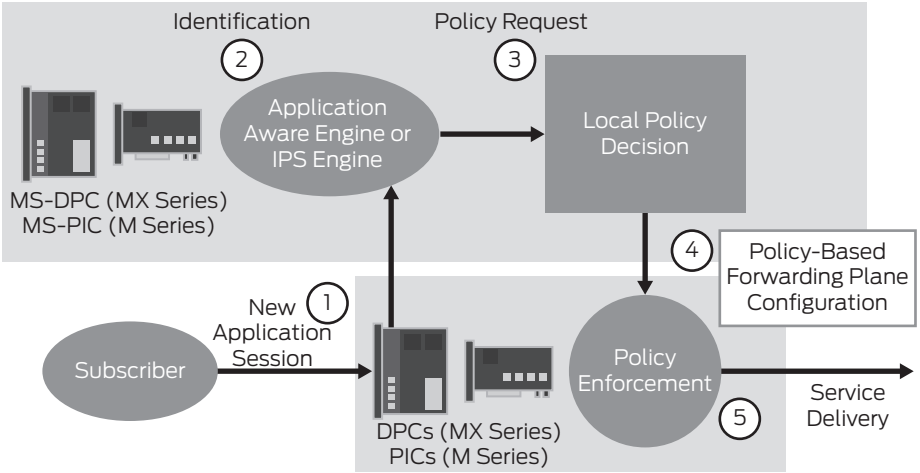


Figure 3: Logical packet flow

Inspecting Packets

For Dynamic Application Awareness, packets are inspected using DI technology. For IPS, packets are inspected using IPS technology.

- DI technology identifies applications, manages traffic, and monitors network utilization. Our DI technology examines only the L4-L7 payload and signatures without looking into the actual application content itself. It uses various means, including signatures, ports, and addresses, to investigate sessions directed through service cards to determine the application information within the session. Then it uses this information to identify applications.
- IPS technology is a very powerful security tool that eliminates threats and attacks. IPS looks beyond the TCP/UDP/IP header of the packet and into the actual data portion of the packet where the application data resides. This inspection checks traffic against protocol standards, checks traffic for signatures, and detects traffic that is bypassing normal authentication procedures.

Identifying Applications

Our DI technology identifies applications by detecting TCP/UDP applications that are running on standard and nonstandard ports and looking for specific patterns in the data packets of a session. The IPS functionality extends these mechanisms to identify and drop threats.

The Juniper detection mechanism examines the minimum number of packets that would not lead to reporting false attacks. With information about the actual application, DI technology applies the proper L7 decoders to both standard and nonstandard ports.

One method of identifying the application is based on predefined application signatures. These signatures are loaded using the CLI and are maintained by the Junos OS security team in partnership with the broader security industry community. Our signature-based method of application identification finds matching client/server and server/client regular expressions. Additionally, signatures can be updated without affecting the hardware or software; no reboot of the MS-PIC/MS-DPC is required.

Additional supported application identification methods are port-based, address-based, and protocol-based. All three use protocols to identify specific application control and data sessions.

- Port-based identification detects customized applications running on specific ports and is part of the application package download for predefined applications. It identifies ICMP code and type, IP protocol, and TCP/UDP port.
- Address-based identification provides a method of telling Junos OS that traffic identified between specified sources is for a particular application. Adding the source and destination addresses to the filter enables you to offer application-aware bandwidth guarantees and rate limiting between or to specific addresses.
- The signature method detects customized applications with specific signatures. These signatures are essential since most applications use evasive procedures to avoid being detected based on the port or address.

Classifying Applications

By combining a rules-based service with the identified applications, our DI and IPS technologies can apply policies to sessions based on application and application group membership, in addition to traditional packet matching rules. While DI is looking for the application hidden in a well-known port, IPS uses these applications to find actual threats (known attacks in the case of signatures) so that these packets and associated sessions can be dropped.

Packets are directed to the MS-PIC/MS-DPC that hosts the DI technology, which then classifies the application within the session. Once the application is identified, actions can be taken based on the configured policy. You can configure classifications and policies that can then be applied to each subscriber and/or interface. Following is a list of available policies and policy combinations.

- Accept
- Discard
- Rate Limit
- Accept and count
- Accept and set forwarding class
- Accept, count, and set forwarding class
- Rate limit and count
- Rate limit and set forwarding class
- Rate limit, count, and set forwarding class

Increasing Scalability

The current industry method for updating filters is to manually configure them, thus causing full recompilation before they are pushed down to the router. In contrast, Juniper enables you to dynamically configure filters to make incremental updates without the need for full recompilation. Each term is separate from the others so it can grow or prune independently of the other terms in the filter. With our approach, scalability can be increased by configuring the router to dynamically update the forwarding plane so that once a decision has been made about a particular session, the remaining traffic can bypass the MS-PIC/MS-DPC altogether.

Enforcing Policies

A policy manager, which is a set of policy-enforcing features, enables you to control resources, as well as process statistics and events, such as subscriber attachment or detachment.

On the Routing Engine, one policy-enforcing feature collects statistics and reports information on a per-subscriber, per-application basis. This technology creates and applies a service filter to the underlying logical interface, causing traffic bound for subscribers to be forwarded to the MS-PIC/MS-DPC associated with the service. Statistics are exported into a file.

There are two types of subscribers: static and dynamic.

- Static subscribers are manually assigned by the operator.
- Dynamic subscribers are assigned by DHCP.

On the MS-PIC/MS-DPC, another policy feature interfaces with the service layer, receives per-session directives from plug-ins, and enforces the configured actions. It also creates a subscriber database based on information provided by the Routing Engine and uses this information to collect and aggregate per-subscriber statistics, and then further aggregate them by application or by application group. The Policy Manager then sends these statistics to their destination point. The Policy Manager also uses this database to retrieve information for reporting statistics and for tracking sessions per subscriber.

Note that if you configure the traffic to bypass the MS-PIC/MS-DPC, these off-loaded sessions are still tracked for statistical purposes.

Conclusion

Dynamic Application Awareness and IPS enable you to align infrastructure investments with application requirements, improve the operational environment, create highly differentiated service offerings, and provide protection from a wide range of threats and attacks. They also help you make more informed network planning decisions and improve the end-user experience. With tighter control over network resources, improved security, and more efficient operations, you can now deploy new, differentiated services faster and at lower cost.

Acronyms

ARPU	average revenue per user
CapEx	capital expenditures
CoS	class of service
DHCP	Dynamic Host Configuration Protocol
DI	deep inspection
DPC	Dense Port Concentrator
DSCP	DiffServ code point
HSPA	High-Speed Packet Access
ICMP	Internet Control Message Protocol
IMS	IP Multimedia Subsystem
IPS	intrusion prevention system
LTE	Long Term Evolution
MS-DPC	Multiservices Dense Port Concentrator
MS-PIC	Multiservices Physical Interface Card
OpEx	operational expenditures
P2P	peer to per
SLA	service-level agreement
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WLAN	wireless LAN

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.

2000339-001-EN Dec 2009

Printed on recycled paper