

THE DYNAMIC SERVICES ARCHITECTURE: A NEW APPROACH TO NETWORK SOLUTION DESIGN

Providing Carrier-Class Reliability and Availability While Dramatically Increasing Throughput

Table of Contents

Executive Summary	1
Introduction	1
The Dynamic Services Architecture	2
The Traditional Network Appliance Architecture.	2
Not Just Another Chassis Design	2
Switch Fabric, Control Board and Route Engine	3
Service Processing Cards.	3
Input/Output Cards	3
Session Distribution/Load Balancing	3
Packet Flow	4
A Single, Modular Operating System	5
The Juniper Networks SRX Series Services Gateway.	5
Conclusion	6
About Juniper Networks.	6

Table of Figures

Figure 1: Basic session-based load balancing	4
Figure 2: An example of a fully integrated packet flow	5

Executive Summary

Today's network administrators are increasingly being asked to implement advanced applications and dynamic services to help support new business operations and centralize data. However, these investments also require deployment of more security, performance, and bandwidth as the network grows. Traditional approaches to scaling this expanding environment by adding appliances or blades are creating a new level of complexity and higher maintenance costs for IT organizations.

The new Dynamic Services Architecture uses a parallel computing model to replace the complicated collection of subsystems and firewalls with a single, powerful solution. This new approach to the provisioning of high-performance security and networking services provides the first dynamic services gateway, which simultaneously scales integrated security and networking capabilities with performance, and accelerates deployment of next-generation business and consumer services and applications.

Introduction

Just one year ago, the basic web browser was the basis for most networking activity. However, today's systems are rapidly changing. Applications such as peer-to-peer networking, conferencing, and mapping software are more complex and sophisticated, requiring better interaction based on faster availability. The increasing use of video conferencing alone strains the network with zero tolerance for latency. Demand for throughput is increasing exponentially as far more traffic traverses the network. Enter the Dynamic Services Architecture. A revolutionary new model that scales integrated security and network capabilities with performance to accelerate advanced service and application deployments, the Dynamic Services Architecture is based on an innovative new design that overcomes traditional approaches to networking.

Being unable to provide constant availability can literally make or break a service offering. An example is Comcast, which is trying to cope with increased traffic problems by placing highly unpopular restrictions on its heaviest users. Such a situation clearly demonstrates how basic traffic management can play a major role in the success or failure of a service.

At the same time, administrators must keep up with the broad range and increasing frequency of security threats, outages, and slow service. As they become more dependent on global networks, corporations grow increasingly vulnerable to problems that affect the accessibility of information for either employees or customers—and these problems are becoming more common. As just one example, as of August 2008 more data breaches had been reported than in all of 2007. According to the Identity Theft Resource Center of San Diego, malicious attacks are still the leading case of data breaches, with 13 percent due to intruders illegally hacking into files.

Another significant issue for many enterprises is the centralization of data centers. IT organizations not only face ongoing budget accountability, they also must provide new levels of remote access, security, compliance, and management. Many IT managers are addressing this challenge by consolidating multiple data centers to gain more centralized control, simplified maintenance, and reduced costs and carbon footprint. However, the side effect of this effort is that users must now access centralized applications (such as CRM, ERP, etc.) over the Internet or via far flung corporate networks. The result is often increased latency as applications compete for security resources, traffic prioritization, and storage space.

The fact is that traditional networking designs were not developed with carrier-class usage in mind. Today there is an evolving need for improved infrastructures for service providers, large enterprises, wireless carriers, and cable companies. These modern infrastructures require large capacity, highly scalable security systems that can meet continuously changing performance requirements.

One solution to these problems is an entirely new approach to developing network products: the Dynamic Services Architecture. This innovative concept radically departs from current architectural designs to provide an elegant new paradigm for meeting the needs of modern networking.

The Dynamic Services Architecture

First, to understand the need for this revolutionary approach, it is worth examining current architectural models and why they can not adequately support the networks of the very near future.

The Traditional Network Appliance Architecture

Despite dramatic advancements in speed, power, and functionality, today's networking and security architectures are designed in much the same way as the first IBM personal computer back in the 1970s. At the core of the PC is the CPU—and though processing speed and power has obviously increased exponentially, the premise that a PC is built around the CPU remains the same. Upgrades consist of replacing the existing chip with a faster one, rather than adding new capabilities; scalability is achieved by adding memory or expansion cards for modem, graphics, video, sound, etc. into existing slots. The number of slots is limited and, while the speed and density of cards has greatly improved, the fundamental characteristics of the design remain the same.

This architectural concept is also still used in most network security appliances today. Appliances are built around a fixed number of CPUs, with limited memory upgrade options and expansion slots that are usually strictly dedicated as I/O interfaces. Therefore, not surprisingly, many network appliances exhibit limitations similar to those of PCs, especially when deployed in very high traffic networks. CPUs are taxed to the limit, with little or no way to increase processing capacity, while I/O interface options do not offer enough expandability as the network grows. As a result, some deployments may exhibit traffic bottlenecks on the CPU, while plenty of I/O interfaces remain open; whereas other deployments may exhibit low CPU utilization but are running out of I/O.

Recently, the blade chassis has had some success in overcoming these limitations. It consists of an enclosure, designed on a fast backplane, with the ability to support blades, or cards, to provide a wide range of security capabilities. The idea is that when IT departments need more functionality, they simply install another blade.

However, this design suffers from many of the same limitations as network appliances. Most chassis are designed to simply provide a high-speed backplane, and little effort has been made to manage the blades as a single system, rather than as a collection of disparate cards. The result is a chassis shell that essentially houses multiple appliances in a blade form factor, with the same processing and I/O limitations that exist at the blade level. Of course, it is easier to install a blade than a new appliance. However, there are very few additional benefits to this approach.

Attempts have also been made to provide scalability on the software side. However, the success of these attempts has been limited by the fact that the hardware is not designed to support such functionality. Consequently, software updates may bog down the system and slow performance.

Confronted with these problems, the only solution left for IT departments has been to buy another appliance, with its own set of CPUs and ports, and then another, and another... creating a complex, constantly growing network environment that is time-consuming and costly to maintain.

It is clearly impossible for administrators to infinitely add appliances to secure networks. It has therefore become an imperative to break away from traditional designs and approach the architecture with a completely fresh eye, looking for new ways to deliver scalable dynamic services. A new Dynamic Services Architecture now allows network administrators to take advantage of a more flexible, scalable system that provides carrier-class reliability and availability while dramatically increasing throughput.

Not Just Another Chassis Design

The Dynamic Services Architecture is based on a chassis design; however, it is a complete departure from traditional chassis architecture. Rather than simply providing a fast backplane, the Dynamic Services Architecture includes the management and control necessary to incorporate individual blades into a powerful collective solution. Rather than housing disparate cards, the Dynamic Services Architecture adds each blade into a growing pool of resources. These resources can then be utilized as necessary for optimal processing of network traffic.

Switch Fabric, Control Board and Route Engine

At the heart of the Dynamic Services Architecture is the Switch fabric and Control Board (SCB). The SCB transforms the chassis from a simple blade enclosure into a highly effective mesh network. The purpose of the SCB is to allow all blades in the chassis to send traffic at extremely high bandwidth.

The Route Engine (RE) is tightly coupled with the functionality of the SCB and can be considered the central nervous system of the architecture. The RE is the control plane of the chassis and provides overall management and communications to and from system administrators, as well as calculating route tables for routing network traffic.

The operating system, which includes key chassis functionality, also runs on the RE. In the case of networking and security, functionalities such as advanced routing, switching, flow-base security, zone-based management, and screens are available on the OS.

Service Processing Cards

If the RE is the central nervous system of the chassis, the Service Processing Card (SPC), is the brain. SPCs are blades that provide the capacity to perform the heavy lifting of processing network packets. The chassis must have at least one SPC to operate.

The true elegance of this design is realized when more than one SPC is installed. Rather than the chassis now having two or more “brains,” as in traditional network architecture, the addition of a new SPC essentially results in a larger system that can perform many more tasks at a given time.

This important distinction is one of the key characteristics that sets the Dynamic Services Architecture apart from traditional designs. No longer do network administrators need to configure each blade to perform specific tasks. By increasing the processing capacity of the chassis while maintaining a single system, the architecture enables ongoing expansion of overall processing capacity without any management overhead.

To ensure the highest level of reliability, the SPCs and REs are physically and logically separated. This separation of the control and data planes ensures that a fault on any of the SPCs will not result in catastrophic failure of the entire chassis.

The importance of this concept can also be seen in a security situation such as a denial of service (DoS) attack. When the attack is launched, the administrator’s efforts to contact the system do not simply become part of network traffic, forced to compete with an exponentially growing amount of data during a situation in which immediate response is required. Because the control plane remains separate from traffic flow, IT managers can immediately respond to network-threatening situations to divert the attack, while all the SPCs continue to process network traffic.

Input/Output Cards

The chassis slots in the Dynamic Services Architecture are unique in that they are card-agnostic, allowing administrators to configure the architecture for their specific needs up to the limits of the chassis itself. For example, an organization that requires more processing capability, such as a military installation, may include more SPCs and fewer Input/Output cards (IOCs). An Internet service provider, on the other hand, may choose to provide a great deal of I/O for its customer traffic, while needing less raw processing power. As business requirements change, administrators may easily add IOCs and SPCs to reconfigure the architecture as needed.

Based on this agnostic slot design, the IOC can therefore scale independently—the chassis may be equipped with as many IOCs as there are available slots (with at least one slot for the SPC). The dynamic nature of the architecture then automatically maps each session to a SPC in real time as new sessions are received to be processed.

Session Distribution/Load Balancing

The Dynamic Services Architecture also supports automatic load balancing with advanced performance and capacity due to its session distribution design. This is enabled by the intelligent input/output and network processing subsystems, which balance sessions across the shared pool of SPCs (the “brain” discussed above). This is possible because all the SPCs in the system run the same services and have the same configuration. There is no specific mapping from one IOC to one SPC; rather, each flow is mapped dynamically upon session creation.

In fact, if only one SPC is installed, administrators can still run all services, such as firewall, VPN, Intrusion Prevention System (IPS), routing, quality of service (QoS), Network Address Translation (NAT), etc. Additional SPCs can be deployed to increase performance and capacity with no change to the system configuration.



Figure 1: Basic session-based load balancing

For example, as we see in Figure 1 in the first frame (One to One), a single IOC and a single SPC are processing packets. Packets flow from the IOC, to the SPC, and then back out the IOC.

In the second frame (Many to One), multiple IOCs are connected, still with only a single SPC. The system automatically directs all traffic from the IOCs to the SPC, and then routes that traffic back out a different port.

In the last frame (Many to Many), the system provides intelligent load balancing of sessions across a number of SPCs, four in this case. Any session coming in any port can be forwarded, on a session-by-session basis, to any SPC in the system.

This load balancing is performed automatically, with no configuration or oversight by the system administrator. This is dramatically opposed to traditional chassis-based solutions, where each processing blade is an independent firewall, with its own dedicated traffic, unique configuration, and routing support.

Packet Flow

In the same way, the packet flow within the Dynamic Services Architecture becomes fully integrated and far easier to manage. No longer is it necessary for administrators to provide separate instructions to each blade for traffic management. Each packet traversing the system now takes the same basic path:

1. The ingress packet enters Ethernet port on the IOC.
2. It is processed by the IOC and passed to the switch fabric.
3. One processing unit on the SPC receives and processes the packet for the firewall, IPsec VPN, and/or IPS. If the packet is to be dropped, the SPC does so and will typically log the event.
4. If the packet is to be passed, it is passed back through the switch fabric to the IOC, where it is processed by the IOC processor, where QoS is applied if necessary.
5. The packet is then passed out the Ethernet port to egress the system.

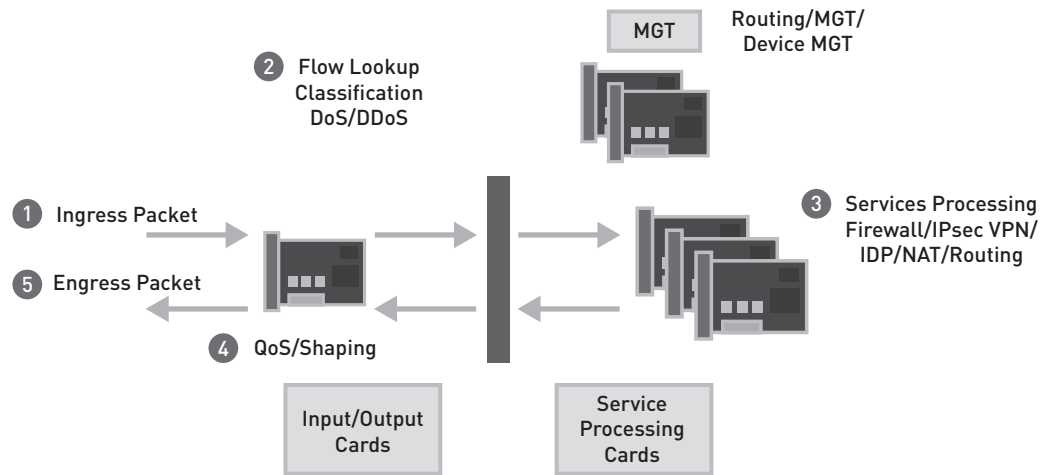


Figure 2: An example of a fully integrated packet flow (SRX5000 line)

The flexibility of the Dynamic Services Architecture is due to the fact that no fixed relationship is ever locked in between ports and data packets, allowing legitimate traffic to continuously pass through far more quickly. Perhaps even more importantly, as SPCs are added, traffic configurations need not change, enabling faster deployment, lessening the administration workload, and maintaining high traffic performance on the network.

A Single, Modular Operating System

The Dynamic Services Architecture relies upon a modular operating system that supports the integrated management of the network. This operating system includes:

- A cohesive operating system based on a single code source. This allows network administrators to configure and manage features from chassis to routing using the same tools across devices to monitor, administer, and update the entire network. It also simplifies new feature deployment, software upgrades, and other modifications, allowing IT organizations to function more efficiently with less training time and lower costs.
- A disciplined release train, or plan, for development that supports stable implementation of new features based on rigid quality metrics and testing. Each new version thus forms a complete superset of the prior release, guaranteeing that earlier features are still present and working. In addition, each new version should be released concurrently for all routers and switches. This helps to avoid the unpredictability, risk of disruption, expensive testing, and complexity of unplanned maintenance and upgrades.
- A modular architecture that enables flexible but stable innovation across functions, supporting streamlined development as well as enhanced fault-tolerance and failover. This supports high availability by isolating potential incidents for faster troubleshooting and resolution, ensuring uptime while restricting the spread of malicious code or messages.

This model simplifies new feature deployment and software upgrades, and reduces the likelihood of administrative error. It also includes tools that automate routine tasks, further limiting the chances of downtime and simplifying management.

The Juniper Networks SRX Series Services Gateway

An example of a product based on the Dynamic Services Architecture is the new Juniper Networks® SRX Series services gateway. The SRX5000 line provides an integrated infrastructure designed using parallel computing architectures that remove the traditional complexity of multiple subsystems. The result is a single, powerful system that allows IT administrators to take advantage of new and better network security management capabilities as well as dramatically improve performance.

The SRX Series runs on Juniper Networks JUNOS® Software, which is based on a modular design offering a single-source operating system for the network. Unlike any other product on the market, it provides one operating system, enhanced through one release, and developed based on a single modular architecture. The benefits of this streamlined approach was showcased in a recent survey by Lake Partners of more than 120 network operators, which found that many JUNOS Software users spend an average of 25 percent less time on common network operations tasks compared to competitive systems. Further, they reported an average time reduction of 54 percent in troubleshooting and unplanned events.

The SRX5000 line can:

- Achieve more than 100 Gbps firewall throughput and 30 Gbps IPS throughout in benchmarking tests, making it the highest-performing security solution in the industry
- Support high session counts and setup rates (8 million simultaneous sessions and 350,000 connections per second), which are essential for securing modern applications
- Natively integrate firewall, IPS, virtual VPN, DoS blocking services, NAT, and QoS
- Enable carrier-class reliability and availability

The SRX3000 line can:

- Achieve 30 Gbps firewall throughput and 10 Gbps IPS throughput in benchmarking tests
- Cover a wide range of price/performance points by separating I/O and network processing into separate cards
- Optimize rack space utilization by accepting processing cards in front and rear slots of the devices
- Support high session counts and setup rates (2 million simultaneous sessions and 175,000 connections per second), which are essential for securing modern applications.
- Natively integrate firewall, IPS, virtual VPN, DoS blocking services, NAT, and QoS
- Enable carrier-class reliability and availability

Benefits derived from the SRX Series design include:

- Greatly improved scalability and performance
- Flexibility based on modular architecture; improved ease of use and reduced workloads for IT organizations
- Improved application performance and user experience
- A lower total cost of ownership based on a single architecture running on a single network operating system

Conclusion

The Dynamic Services Architecture is a revolutionary new model that scales integrated security and network capabilities with performance to accelerate advanced service and application deployments. It is based on an innovative new design that overcomes traditional approaches to networking.

The SRX Series services gateway, with its flexible scalability, high integration, and performance, exemplifies the real-world benefit of the Dynamic Services Architecture. With this powerful technology, IT departments can provide constant scalability, high performance, simplified management, and comprehensive security to their users, while maintaining industry-leading performance, reducing operational costs, and maximizing their investment.

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

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
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. "Engineered for the network ahead" and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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

