

White Paper

Optimizing the Data Center with Juniper Networks



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

Introduction	3
Trends Impacting the Data Center	3
Requirements for Optimizing the Data Center	4
Deliver LAN-like Performance	4
Scale Across Multiple Dimensions	5
Ensure High Availability	6
Provide Multi-layer Security	6
Enhance Visibility	7
Proven Enterprise Data Center Solutions from Juniper Networks	8
Routers	8
Security Platforms	8
WAN Application Acceleration and Optimization Platforms	9
Data Center Acceleration Platforms	10
Juniper Networks: Meeting the Data Center Requirements	10
Delivering LAN-like Performance	10
M-Series Routers:	10
Security Platforms:	11
WAN Acceleration:	11
Data Center Acceleration:	12
Scaling Across Multiple Dimensions	12
M-Series Routers:	12
Security Platforms:	13
WAN Acceleration:	13
Data Center Acceleration:	13
Ensuring High Availability	14
M-Series Routers:	14
Security Platforms:	14
WAN Acceleration:	15
Data Center Acceleration:	15
Providing Multi-layer Security	16
M-Series Routers:	16
Security Platforms:	16
WAN Acceleration:	17
Data Center Acceleration:	17
Unified Access Control (UAC):	17
Enhancing Visibility	18
M-Series Routers:	18
Security Platforms:	18
WAN Acceleration:	19
Data Center Acceleration:	19
Juniper Networks Data Center Solutions: Adapting to Business Needs	20

Introduction

Today, globalization and the move to virtualize business operations are among the trends placing new demands on the IT infrastructure and, in particular, the data center – the nerve center of the enterprise. IT is responding by looking for ways to optimize the data center and the supporting network infrastructure to deliver the performance, availability, and security the evolving business environment demands.

Juniper Networks understands these dynamics, and delivers proven solutions to meet the most challenging data center requirements – whether an enterprise is building new data centers or restructuring existing ones. The Juniper standards-based, best-in-class routing, security, and application acceleration solutions interoperate with existing standards-based hardware and software, enabling enterprises to leverage their existing infrastructure when optimizing their data center. With Juniper, enterprises can quickly and economically adapt their data center infrastructure to accommodate emerging business and technology trends.

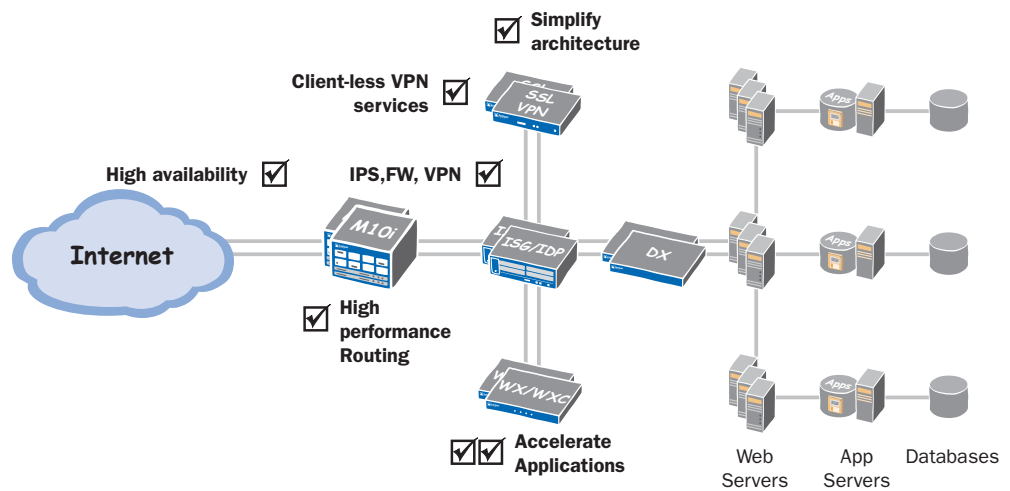


Figure 1: The data center is the nerve center of the enterprise, incorporating multiple technologies that are critical to ongoing business operations.

Trends Impacting the Data Center

Enterprises today are going global, extending geographically by opening offices and production facilities around the world. Likewise, enterprises have virtualized their operations, expanding their user populations beyond employees to include contractors, consultants, business partners, and customers who may be anywhere in the world. As a result, enterprises need to provide their end users with ubiquitous, secure connectivity while ensuring all corporate resources and applications are secure.

These trends are driving a number of IT initiatives that directly impact the data center, including the webification of applications, centralization of resources, and consolidation of data centers. In addition to supporting market conditions, these initiatives are designed to increase employee productivity and business agility while reigning in costs. For example, IT is making applications and data readily available to the enterprise’s far-flung user communities, regardless of where they are or how they connect to the data center.

The centralization of applications, file servers, and other resources within the data center reduces the cost of installing and maintaining equipment globally and eliminates the need for staff in remote offices. Centralization also provides greater control over resources, which is key to complying with government regulations and ensuring business continuity. Regulations such as the Health Insurance Portability & Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the

Gramm-Leach-Bliley Act (GLBA), Regulation NMS, and BASEL II require that companies protect their critical applications as well as customer (or patient) data, control access to that data, and prove how they have done so. Providing these protections is easier if applications, data, and resources are centralized in a small number of locations rather than highly distributed.

Consequently, enterprises are consolidating data centers and building new, centralized ones. For some time, the trend had been to distribute data centers around the world. While moving applications closer to users has benefits, it's proven costly in terms of hardware, software licenses, staffing, and services. Consolidating data centers enables enterprises to gain centralized control over critical resources and cut overhead expenses.

Centralization and consolidation must also ensure business continuity. Executives and IT are all too aware of the cost of system downtime and data loss, and IT is under greater pressure than ever to deliver non-stop operations. Many organizations are finding that it's easier to backup and recover data that's centralized and under direct IT control, adding impetus to server centralization and data center consolidation.

IT departments are also faced with extending ways to ensure business continuity for the global enterprise to sustain productivity and services. Pandemic events where social distancing may be required can cripple an organization if workers are forced to stay home and quarantines are enacted. In general, enterprise IT departments have had to balance two seemingly mutually exclusive mandates – providing open access to corporate applications and resources while offering increased performance, control and security.

Requirements for Optimizing the Data Center

Webification/open access, centralization, and consolidation all have business benefits. However, these initiatives place new demands on the data center which, if not addressed effectively, can undermine core business goals, such as growing revenue and productivity. For example, Web-enabling applications makes it possible to extend them to diverse users but raises performance and security concerns. Similarly, centralizing servers brings them conveniently together into a few sites but leaves branch offices and extended users such as partners vulnerable to performance degradation and availability snafus.

In particular, these strategic IT initiatives pose performance, scalability, availability, security, and visibility challenges for the data center infrastructure. By selecting the right solutions, IT can implement these initiatives without a major overhaul of existing data centers. Such a solution must address the following requirements.

Deliver LAN-like Performance

Centralizing application servers and other resources creates performance problems for remote users, who must now access these resources over a wide-area network (WAN). At the same time, the move to globalize and virtualize the enterprise is creating more remote users who need high-performance remote access to applications and resources.

Legacy applications, which are primarily client-server, were designed to operate over a high-speed local-area network (LAN). In contrast to the LAN, the WAN has capacity and latency constraints that can degrade application performance – in the worst case, making applications like file sharing, e-mail, and software development tools virtually unusable. Other types of transactional and real-time applications, such as voice over IP (VoIP) and video conferencing, are particularly sensitive to latency and jitter; if not properly addressed, the varying latency on WAN links can effectively kill these applications.

Web-enabling applications contributes to performance issues. These applications, with their content-rich interfaces, consume 10 times the WAN and server capacity as their client-server

counterparts. Application performance can suffer as applications contend for infrastructure resources. Another problem is that some application-level protocols and development environments require hundreds or even thousands of transaction exchanges between distributed users and centralized applications, making them highly inefficient on the WAN.

Server centralization and data center consolidation can also impact data backup and performance restoration, since the volume of data that needs to be backed up or restored at central sites increases. At the same time, increases in traffic volume between data centers and backup sites can strain the existing connectivity infrastructure, including routers and firewalls.

To effectively address performance issues related to globalization, virtualization, server centralization and data center consolidation, optimizing the data center solution must boost the performance of all application traffic, local and remote. It must provide WAN optimization, including data compression, TCP and application protocol acceleration, bandwidth allocation, and traffic prioritization. And it must accelerate data replication, backup, and restoration between data centers and remote sites, including disaster recovery sites.

Within the data center itself, a data center acceleration solution must boost the performance of both client-server and Web-based applications, and speed Web page downloads. In addition, it must offload CPU-intensive functions, such as TCP connection processing, and HTTP compression, from back-end application and Web servers.

In addition, a data center solution must ensure predictable performance for applications, supporting quality of service (QoS) technologies to allocate bandwidth for latency-sensitive applications such as VoIP. Beyond application acceleration, a data center solution must also ensure that critical infrastructure components, such as routers, firewalls, remote access platforms, and other security devices, have the performance characteristics necessary to handle the higher volumes of mixed traffic types associated with centralization and consolidation, as well as the needs of users operating around the globe.

Scale Across Multiple Dimensions

Centralizing servers and consolidating data centers can push the data center infrastructure to the limit, making it unstable. IT must be able to accommodate the rise in traffic without having to overbuild or rebuild the entire infrastructure. For example, security platforms must be able to scale in order to maintain security and high performance levels at all times or they hinder business activity and are more susceptible to attacks.

What's required are data center optimization solutions whose components scale, thus enabling IT to cost-effectively scale the existing infrastructure. For example, routers must be high capacity, both in terms of the volume of traffic they can handle and the number and speed of ports they support. They must also be able to apply forwarding filters and access control lists (ACLs) in a scalable and dynamic manner.

For their part, remote access devices must be capable of supporting a wide variety of endpoint devices and platforms for diverse remote employees, partners, and customers. They must also provide adequate security to ensure that managed and unmanaged endpoints, users, and networks are not compromised. Security gateways, firewalls, and intrusion prevention system (IPS) devices must have the aggregate throughput to handle the volumes of data going into and out of the data centers without missing a potential threat; maintain peak throughput under all conditions, including traffic spikes and attack scenarios; and rapidly ramp session rates.

Similarly, WAN acceleration platforms must scale to support higher-speed WAN links and increasing numbers of remote sites, as well as provide seamless expansion through stacking or clustering of multiple devices.

To support scalability, a data center acceleration platform must enable server farms to scale by offloading CPU-intensive tasks, such as TCP connection management and encryption, from back-end servers. Likewise, such a solution should perform server load-balancing as well as global load balancing, both to direct users to the nearest data center housing the applications and data they need and to protect against outages. For its part, the application acceleration platform must be seamlessly expandable through stacking or clustering of multiple devices.

Ensure High Availability

Enterprises must be prepared for any event that can impact business continuity, from a device failure or power outage to a major disaster, such as an earthquake or hurricane. In addition, enterprises must also consider the impact of a pandemic event, such as a major flu outbreak, where social distancing may be required. If quarantines are put in effect and workers are forced to stay at home, enterprises need to provide remote access to employees and business partners to sustain productivity and services.

Globalization and consolidation can magnify the challenge of maintaining high availability; any failure of the infrastructure can have serious consequences. For example, failure of a WAN link to a serverless office equals a total outage, while the failure of a data center can lead to significant downtime. Likewise, failure of a security device can result in much more data being at risk, or more rapid propagation of an attack.

The key components required to optimize the data center must be designed for high availability, including redundancy of critical subsystems and seamless failover. This requirement applies to routers, security products, and any other device along the user-to-data center path.

For example, gateway routers must support hot-swappable components and graceful restart, among other features. For their part, WAN acceleration platforms must support failover to secondary links, if available. Data center acceleration platforms must support application-specific health checking and load balancing across both local and distributed servers, while a data center optimization solution must support rapid data backup and restoration for disaster recovery and business continuity.

At the same time, organizations must be able to easily handle sudden peaks in demand for remote access in the event of a disaster where social distancing may be required. The remote access capabilities must be easy to deploy and enable anytime, anywhere connectivity to any device, and the deployment needs to be simple for the remote user to implement.

Provide Multi-layer Security

Extending applications to distant employees, as well as to customers, partners, and other users outside the company, raises security challenges. Employees and non-employees are being granted an ever widening range of network access, making the network increasingly vulnerable. IT must protect applications, data, and infrastructure by applying appropriate access controls without inhibiting user efficiency or negatively impacting application performance. IT must also mitigate risks from untrusted sources, such as non-employees, whose PCs and networks are not under IT control.

The move to globalize and virtualize the enterprise puts new demands on IT to secure remote access communications and protect site-to-site communications, including connections between data centers and from data centers to backup sites. IT must also fortify the network perimeter as increasing volumes of Web and other traffic types flow across it. In addition, enterprises must ensure that only authorized users have access to sensitive data – or risk penalties for regulatory non-compliance. And IT must continue to defend against malicious intruders, whose attacks are growing increasingly sophisticated.

A data center optimization solution must support a multi-layer security approach that protects the data center and internal network from the outside world, securely segments internal users and networks, and provides secure access for remote users. In particular, the security portion of a data center optimization solution must protect data center resources and defend against application-layer attacks. It must also securely segment the network internally to accommodate larger number of users accessing centralized applications and data sets and to meet regulatory requirements. And it must protect the network itself, defending against network layer assaults, such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

In addition, a data center optimization solution must provide user-based security, including secure access to applications and data by remote users. It must provide authentication, endpoint assessment, and policy enforcement for both remote and local users, and consistently apply security policies to both trusted and untrusted parties. Such a solution must operate inline to stop attacks before they inflict any damage, minimizing the time and costs associated with intrusions. For remote users, it must be able to detect and terminate malicious or infected users.

Enhance Visibility

As resources are centralized and applications made available to diverse users across the WAN, IT more than ever needs visibility into the WAN and data center infrastructure. Because the WAN is the lifeline delivering applications to remote users, enterprises can no longer rely solely on their service providers for all things management; they need direct insight into the performance, availability and policy-control characteristics of this expensive resource.

IT needs visibility into everything, including WAN and application utilization, who is accessing applications and data, who made changes to the system, and what security threats were stopped. Visibility through real-time and historical reporting empowers IT with the information needed to ensure maximum performance and availability across the entire data center infrastructure, meet regulatory requirements, and plan for future capabilities and capacity.

The optimized data center must give IT a clear picture of traffic going into and out of the data center. It must provide visibility into application, WAN, and resource utilization for the purposes of troubleshooting, fine-tuning, capacity planning, and reporting and accounting. It must provide IT with granular accountability data, including which resources and applications users have accessed; who made what changes to the system; and what security events occurred and how they were handled.

Such a solution must provide real-time and historical reports that range from high-level overviews geared to the CIO down to the detailed diagnostic data that a network engineer needs to troubleshoot a problem. It must provide a comprehensive set of predefined reports, as well as enable IT to generate custom reports and support trend analysis and forecasting.

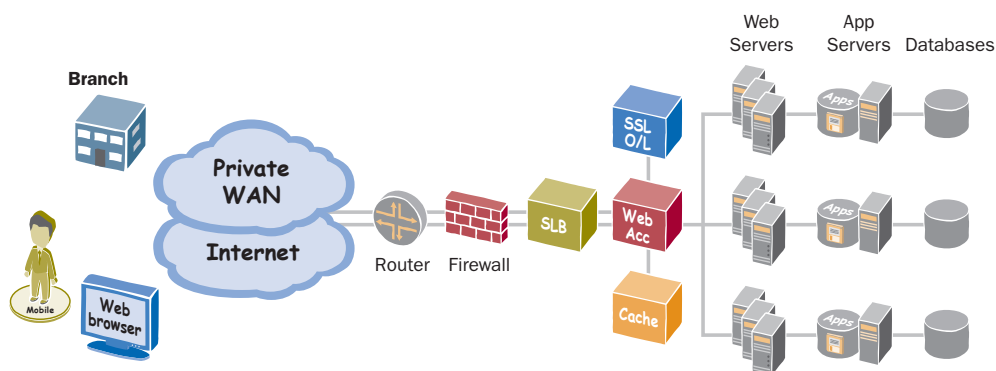


Figure 2: A complete data center solution must include all the components required to meet the needs of the evolving enterprise.

Proven Enterprise Data Center Solutions from Juniper Networks

Juniper Networks provides enterprises with a set of products that deliver the performance, scalability, resiliency, security, and visibility characteristics needed to meet the demands that strategic IT initiatives place on data centers. This product set encompasses high performance routers; robust products for layered security, including firewall, VPN, IPS, integrated security gateways, and secure remote access SSL VPN platforms; WAN acceleration platforms; and data center acceleration platforms.

Each product line in the Juniper data center solution set has a proven track record. In addition, Juniper carefully tracks emerging technologies and standards in the networking, security, operating system and applications arenas, ensuring enterprises have the right set of capabilities to address current and future IT initiatives. The Juniper data center solution includes:

Routers

Designed for optimal connectivity, Juniper routers combine a reliable hardware architecture with a modular operating system (JUNOS) to deliver multi-Gigabit-per-second (Gbps) performance. JUNOS executes many functions in parallel on assigned processing resources, enabling Juniper routers to support robust routing and advanced services, such as QoS, security, and policy-based controls, with predictable, stable performance. Available in a variety of form factors, the Juniper M-Series multiservice edge routers is particularly well suited to connect the enterprise data center to the corporate WAN and the Internet, and for interconnecting data centers.

The newest M-Series model, the M120, is a mid-range router with the characteristics of the higher end M320, but with a footprint and price that make it an ideal data center gateway. The M120 features 10 Gigabit Ethernet (GbE) support, full in-box redundancy, and advanced QoS capabilities. Like other M-Series routers, the M120 offers a set of Layer 2 and Layer 3 services, including MPLS, Layer 2.5 Internetworking VPNs, and a comprehensive Layer 3 VPN portfolio. It can be configured with 128 GbE ports and either two 10 GbE or OC-192 links.

Security Platforms

Juniper offers a complete line of gateway security and intrusion detection and prevention products, from standalone firewall/VPN IPS products and SSL VPN appliances to the Integrated Security Gateway (ISG) platform, which combines the Juniper firewall and VPN capabilities with the IDP product's inline protection features in a single chassis.

Juniper Intrusion Detection and Prevention (IDP) IPS devices stop network- and application-level attacks before they can inflict any damage, using stateful detection and prevention techniques to provide zero-day protection against worms, Trojans, spyware, keyloggers, and other malware. The Juniper IDP products, also provide information on rogue servers as well as types and versions of applications and operating systems that may have unknowingly been added to the network. IT can use the Juniper IDP to control access to specific applications, as well as ensure business-critical applications receive a predictable quality of service.

The Juniper firewall/VPN products provide stateful firewall and IPsec VPN capabilities with threat management, routing, and resiliency features. These Juniper devices include intrusion protection; antivirus (including anti-spyware, anti-adware, and anti-phishing) protection; anti-spam; and Web filtering. The Juniper firewall/VPN products support key routing protocols, including BGP, OSPF, RIPv1/2, and Equal Cost Multipath Control (ECMP) along with Network Address Translation (NAT).

Juniper Integrated Security Gateways (ISG) fully integrate the functionality of the Juniper firewall, VPN, and IDP products in a single chassis. The ISG provides strong network and access layer security, including policy-based rules using logical zones; virtualization through VLANs, virtual systems, and virtual routers; and mature networking capabilities, including dynamic routing and world-class IPsec VPN support.

The ISG platforms enable IT to easily segment security management by establishing virtual firewalls, VPNs, and IDPs, each with their own address book, policies, and management. By segmenting the network, these virtualization capabilities improve security while simplifying management and eliminating the need for additional hardware, thereby lowering the total cost of ownership.

Juniper Networks Secure Access SSL VPN appliances lead the SSL VPN market, with form factors and features for any size deployment. These SSL VPN appliances can secure LAN, intranet, and extranet access for employees, business partners, and customers. With SSL, users gain secure access from just a Web browser, eliminating the need for client software downloads, changes to internal servers, and costly ongoing maintenance and desktop support.

Using an SSL VPN allows enterprises to provide access to remote or mobile employees, partners, and customers while ensuring that these users see only what they are allowed to see, mitigating the risks of unmanaged devices or untrusted networks.

Best-in-class endpoint and host-checking security features provide access only to those users whose endpoints and networks meet certain preconditions. For example, a Secure Access appliance can be set to check the requesting PC's network and device settings, including scanning for malware and verifying operation of endpoint security packages such as personal firewalls and antivirus software. The requestor's IP address, browser type, and digital certificates can also be examined before login is allowed, and the results used to grant or deny access based on security policies.

WAN Application Acceleration and Optimization Platforms

The Juniper WAN application acceleration (WX and WXC) and optimization platforms cost-effectively accelerate, control, and prioritize application traffic over the WAN, improving application response times while maximizing WAN investments. The Juniper WAN acceleration platforms can significantly accelerate application response time while reducing bandwidth utilization. In addition, the WX and WXC platforms provide high availability for sites with multiple WAN links and give IT unprecedented visibility into WAN performance.

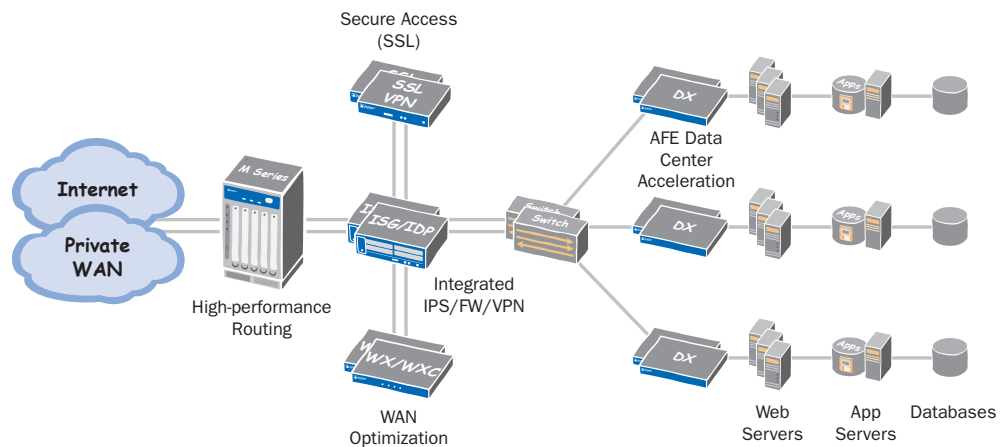


Figure 3: The complete Juniper Networks data center routing, security and acceleration solution set.

Data Center Acceleration Platforms

The Juniper data center acceleration (DX) and load-balancing platforms deliver best-of-breed application availability, acceleration, and intelligence for all web-enabled and IP-based business applications. Offering a set of application-fluent services in a single appliance, the DX provides server load balancing, global server load balancing, SSL encryption and termination, a fast, robust AppRules™ HTTP header body inspection and content rewriting engine, HTTP caching and compression, and application security.

The Juniper DX platforms boost application performance by accelerating page loads and transactions for Web-based applications while offloading network and security functions from servers. As a result, IT can provide LAN-like performance for users accessing centralized data and applications without having to overbuild the WAN and data center infrastructure. In addition, the DX platform's AppRules engine reduces application rewrite costs, while its load balancing capability ensures maximum high availability for local and global applications.

When used in combination, these Juniper products enable IT to create a robust data center infrastructure to realize Webification, centralization, and consolidation initiatives, enabling enterprises to lower their total cost of ownership, boost availability, and meet regulatory compliance obligations.

Juniper Networks: Meeting the Data Center Requirements

Juniper Networks offers enterprises the products and technologies they need to address the most demanding data center requirements. Whether deployed in a new data center or used to optimize existing data centers, the Juniper products deliver best-in-class performance, scalability, availability, security, and visibility.

Delivering LAN-like Performance

A range of Juniper products contribute to ensuring that application performance remains high, both within the data center and across the WAN, and that IT has the controls it needs to prioritize traffic and allocate bandwidth.

M-Series Routers:

The Juniper M-Series routers, including the M120, provide “performance without compromise” – forwarding high volumes of data across high-speed interfaces at line rate, even when services such as firewalling, NAT, IPsec, and Flow Accounting have been enabled. The M120 supports rich QoS capabilities that include enhanced classifiers, policers, shapers, schedulers and load balancers, while latency through the box is lower than 20_s, making it ideal for carrying transactional and real-time applications such as VoIP and video.

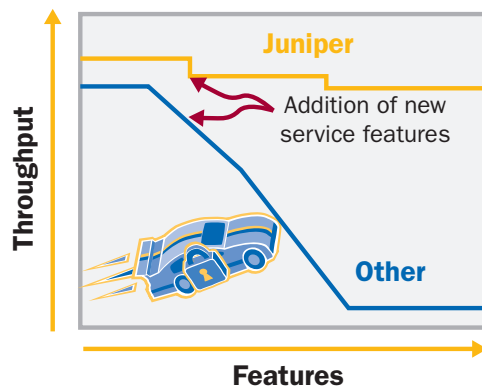


Figure 4: Minimal degradation of forwarding performance when complex services are turned on means uncompromised performance for M-Series routers.

Security Platforms:

The Juniper security products have been designed for high performance in terms of throughput, rapid ramp rate, and low latency, ensuring they have no negative impact on application performance. For example, the ISG with IDP platforms feature purpose-built hardware and software, with dedicated processing power for IDP, firewall, IPSec VPN, DoS, and management functions under the control of the security-hardened ScreenOS operating system. Similarly, the Secure Access SSL VPN features a state-of-the-art SSL acceleration chipset with support for RC4, 3DES, and AES encryption, and built-in compression for all remote access traffic.

WAN Acceleration:

The Juniper WX/WXC platforms ensure LAN-like performance for applications over the WAN by integrating compression and caching, protocol acceleration, bandwidth management, path optimization, and visibility and reporting techniques. The WX and WXC platforms increase WAN capacity by eliminating redundant transmissions; accelerate TCP and application-specific protocols, including CIFS, MAPI and HTTP; prioritize and allocate bandwidth access; and optimize application flows across multiple paths. The WXC platforms also have onboard hard drives that store larger data patterns over longer periods of time for more dramatic traffic reductions.

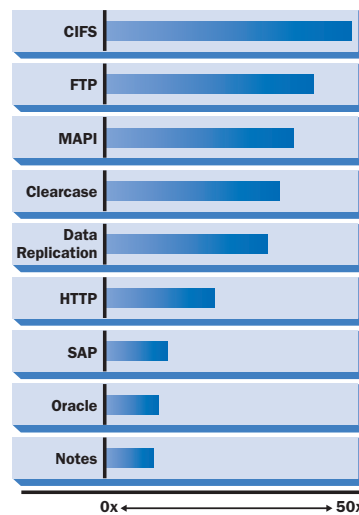


Figure 5: Juniper application acceleration solutions can improve application performance up to 50 times.

These techniques enable the WX and WXC platforms to significantly boost response times across WAN links, from 5x for TCP-based traffic to 100x for applications such as Microsoft Exchange and Windows file sharing. In addition, the WX/WXC platforms' Policy-based Multipath feature enables enterprises to deploy combined public/private WANs to connect data centers and branch offices. IT can define performance-related policies that specify which applications run over which WAN transport based on bandwidth, latency, and packet-loss characteristics.

In addition, the WC/WXC platforms have template-based QoS tools that allow IT to prioritize applications across WAN links and allocate bandwidth among applications. With these tools, IT can define minimum and maximum throughput levels for all applications, ensuring the best traffic mix and utilization on a given link and optimal performance for centralized applications. For example, IT can set bandwidth and priority constraints so that low-priority traffic such as e-mail doesn't interfere with mission-critical applications or delay-sensitive traffic such as VoIP.

Data Center Acceleration:

The DX platforms speed response times for Web-based applications by providing high-performance HTTP compression, caching, TCP/IP connection management, and SSL termination and encryption. With its optimized TCP/IP stack, the DX platform eliminates protocol inefficiencies, boosting the performance of Web-based applications over the WAN.

Deployed in front of content servers in the data center, the DX platform performs traditional load balancing while acting as a bi-directional HTTP proxy, processing all incoming and outgoing requests and offloading servers from CPU-intensive tasks. By handling TCP/IP connection management, the DX platform can reduce thousands of incoming client connections down to a few connections on the server side.

In addition, the DX platform’s AppRules control environment provides a bi-directional header and body inspection/content rewriting capability that enables IT to modify application behavior on active traffic flows without altering the application code itself. For example, AppRules can be used to improve workflows and fix broken Web-based applications to improve page load times.

This combination of application intelligence and Layer 7 acceleration with traditional load balancing allows the DX platform to satisfy basic server load-distribution needs while providing the application intelligence capabilities required to ramp applications to the next level of performance and availability.

Scaling Across Multiple Dimensions

The Juniper products are designed to accommodate the most demanding environments while giving customers room to grow.

M-Series Routers:

The Juniper M120 router delivers scalable connectivity with 10 GbE or OC192 links in a compact, cost-effective platform. The M120 supports latest Juniper routing engine (2GHz, 4GB), allowing the router to easily handle simultaneous full-internet feeds from many Internet service providers. In addition, the M120 supports scalable firewall capabilities and can run 10,000+ access control lists (ACLs).

Security Platforms:

Scalability is built into all Juniper security products. The Juniper high-end firewall/VPN platforms provide modular architectures designed to accommodate future performance, capacity, and functionality trends. For example, the NetScreen 5400 can be configured to support multiple

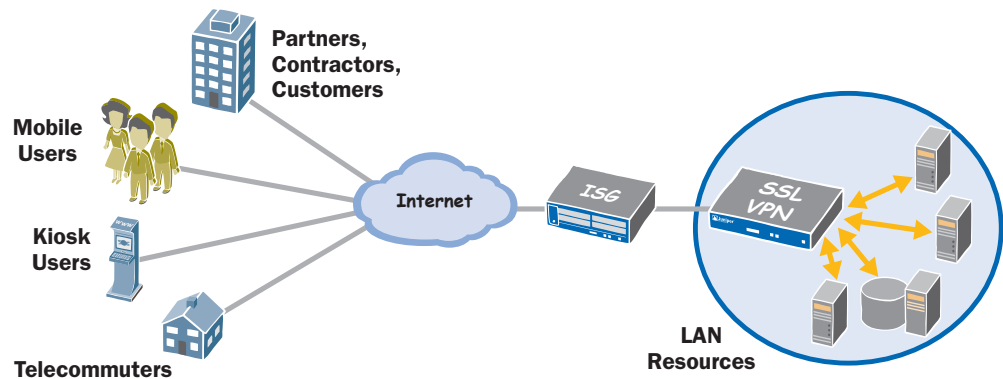


Figure 6: The Juniper SSL VPN platforms deliver a scalable solution for providing secure access to a wide range of distributed users.

Secure Port Modules to scale up to 30 Gbps firewall/VPN throughput, and additional, dedicated processing modules can be added to the ISG Series firewall/VPN platform to enable the integrated IDP.

The Secure Access platforms range from small units supporting from 10 to 25 concurrent users up to high-end units supporting 2,500 concurrent users. For greater scalability, Secure Access platforms can be clustered to support up to 12,500 concurrent users. In addition, Secure Access supports a large range of applications and platforms as well as a wide range of end-point devices, from PCs to mobile PDAs and phones.

WAN Acceleration:

Employing compression and caching techniques, the WX/WXC can scale WAN bandwidth by reducing traffic on existing links anywhere from 60 to 99 percent. These scalable platforms support link speeds from 64 Kbps up to 45 Mbps on a single device, and can be combined in a stack of up to three devices for 155 Mbps total throughput. Certain models can each support up to 2,000 remote sites and high numbers of tunnels. The WX 590, for example, supports up to 45 Mbps of traffic and 140 remote sites, while a WXC 590 stack can support up to 360 remote sites and link speeds up to 155 Mbps.

Data Center Acceleration:

The DX platform’s comprehensive Layer 4 and Layer 7 load balancing modes can scale server capacity two- to four-fold, depending on server and application metrics such as CPU and memory usage, server connection limits, application status, and network conditions. In addition, global load balancing directs users to the best data center based on server, application, and network conditions for scalability worldwide.

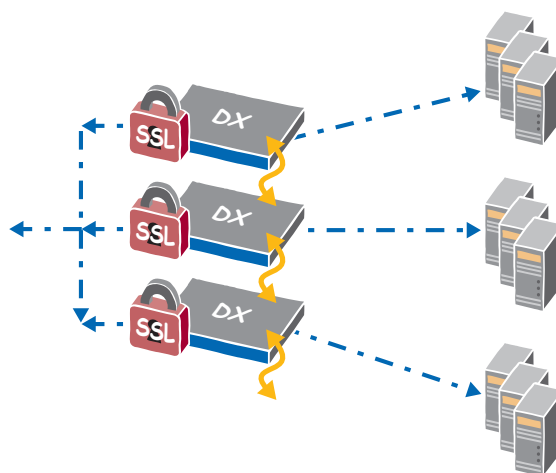


Figure 7: The DX platforms’ ActiveN feature delivers a scalable solution for incrementally adding acceleration and security to the data center.

ActiveN technology enables the DX platform’s performance to scale linearly, enabling up to 64 DX platforms to be clustered and act as a single device, delivering high performance to the busiest of sites.

Ensuring High Availability

All Juniper products are hardened, with robust redundancy and resiliency features designed to ensure and provide business continuity. With the Juniper data center solutions, enterprises can be assured of high availability.

M-Series Routers:

Designed to meet carrier requirements for resiliency and high availability, the Juniper routers feature three independent, protected system planes – a routing plane, a forwarding plane, and a services plane. The operating system is modular, so faults in one area don't affect another area and modules can be restarted independently.

The M120 goes a step further with a new architecture that decouples forwarding processes from the system I/O modules for higher reliability and performance. It also supports N:1 processor redundancy, whereby one processor card can be used as a backup for all the other processor cards in the system, as well as 1:1 redundancy. Other reliability features in the M120 include graceful restart and nonstop routing, whereby a router with redundant route control processors can store up-to-date copies of all state information, allowing the router to switch over from active to backup with no impact on other routers in the network.

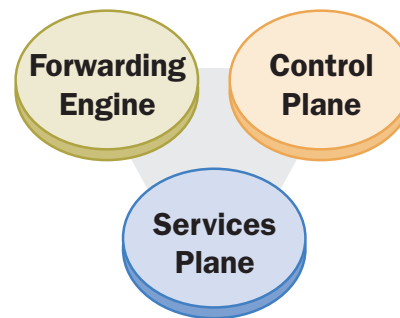


Figure 8: Three independent, protected system planes ensure high availability in the M-Series routers.

As with other M-Series routers, the M120 has hot-swappable physical interface and forwarding cards and fully redundant components, including power supplies and fan trays, routing engine, forwarding engine, and fabric. In addition, it can withstand DoS and other attacks.

Security Platforms:

The Juniper security platforms help enterprises cost-effectively deploy disaster recovery plans, enabling them to minimize risk and meet government mandates for continuity of operations (COOP) compliance. For starters, all Juniper security products feature redundant, hot-swappable components such as power supplies, fans, and hard drives. In addition, devices can be deployed in high-availability configurations such as active/passive and active/active high-availability modes offered on all Juniper firewall/VPN solutions.

The active/passive mode features one master and one backup device, with the secondary device mirroring the primary. In active/active mode, traffic is divided evenly between the two devices. Should one device fail, the other handles 100 percent of the traffic. With either mode, the Juniper firewall/VPN solutions provide stateful failover for firewall and VPN functions and maintain all active sessions, NAT, VPN tunnels, and security associations.

In terms of connectivity resiliency, the Juniper firewall/VPN products support dual-backup or dual Ethernet ports, along with route-based VPNs for redundancy; dual WAN ports can also be used to share traffic load. Similarly, the Secure Access SSL VPN appliances can be deployed in a fully redundant/meshed configuration with multiple load balancers and real-time data mirroring for optimized uptime and operational convenience. Enterprises can use cluster pairs for greater throughput and seamless failover.

The Juniper Networks Secure Access SSL VPN solutions help to ensure business continuity by connecting people even during the most unpredictable circumstances – be it a hurricane, fire, terrorist attack, transportation strike, or pandemic. The Juniper Secure Access SSL VPN appliances enable enterprises to maintain productivity by providing secure connectivity for all users. Employees can be assured access to applications and information from any device, anywhere, anytime, while customers receive uninterrupted service and partners can continue with online collaboration even in the event of a disaster. The product is easily deployed, and remote users can easily connect to enterprise applications and resources through the Internet without using any client downloads since the product uses SSL technology which is inherent in all Web browsers.

WAN Acceleration:

The WX/WXC platforms support redundant configurations and feature swappable, redundant power supplies and hard drives, and swappable fan trays. In the event of a failure, the platform converts to bypass mode, allowing traffic to pass through untouched. In addition, IT can use the WX/WXC platforms’ Policy-based Multipath capability to automatically divert application flows from one transport to another in the event the performance of a WAN link falls below a predefined threshold or one of the links fails outright. Since the WX and WXC platforms continually monitor WAN links, when link performance or the link itself is restored, application traffic is automatically reverted to the restored link.

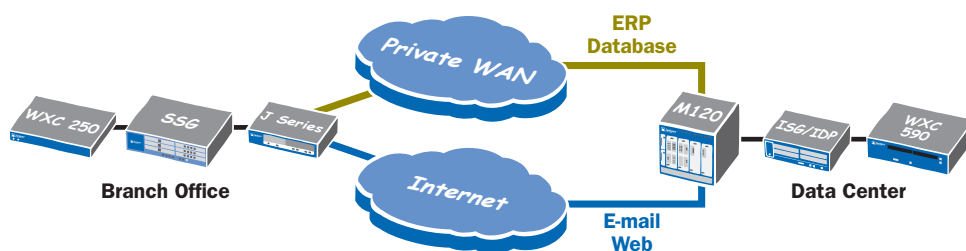


Figure 9: The Juniper Policy-based Multipath capability allows traffic to be assigned to a specific path to ensure availability of high-priority applications

Data Center Acceleration:

The DX platform has a number of features that ensure high availability of local and global applications, such as capturing and redirecting server errors, and routing users away from unavailable servers. For example, the DX platform performs server health checks, such as simple ICMP ping and Layer 7 HTTP content validation, and ensures that traffic is redirected away from unavailable or poorly performing servers. The DX platform also supports scriptable health checks for applications, which verify that the applications are not only up, but are delivering the right content as intended.

The DX platform also ensures disaster recovery for mission-critical applications by redirecting traffic to a secondary data center in the event the primary data center is unavailable due to an outage. In addition, the DX platform features robust server and connection management that allows IT to insert or deactivate servers and services on the fly. Likewise, ActiveN supports N + 1 redundancy so that the workload is redistributed automatically across a DX stack should one platform become unavailable.

Providing Multi-layer Security

The Juniper layered security solution provides protection at each critical juncture in the communications chain – from the user to the data center and back to the user. Consequently, each product within the Juniper data center solution has a security role to play.

M-Series Routers:

Juniper routers add to perimeter and interior defense. In addition to stateful firewall capabilities and the ability to run 10,000+ ACLs, M-Series devices are designed to continue operating even while under attack. A combination of control plane protection and the reservation of system resources enable Juniper routers to maintain control while under attack. For example, certain protocols can be rate-limited to reduce the effect of DoS and DDoS attacks on the control plane. In addition, IT can add security filters dynamically, even during an attack, ensuring new attacks are quickly contained. The filter provisioning is hitless (no packet loss), and make-before-break provisioning does not open any windows of security vulnerability. This type of robust DoS/DDoS prevention is crucial to protecting the data center.

Security Platforms:

Juniper security products address the full range of security needs and are among the most sophisticated in the industry. For an integrated security solution, the ISG series firewall/VPN/IDP solution protects the network perimeter as well as the internal network and server farms. The firewall defends against network-layer attacks such as DoS and DDoS, while the IDP defends against application-layer attacks. The ISG's IPSec VPN feature provides site-to-site tunneling, while the Secure Access SSL VPN appliances provide the most comprehensive security for remote access.

All Juniper IDP products, including the ISG with IDP, stop worms, Trojans, spyware, and other emerging attacks from penetrating the perimeter or network or from proliferating inside the network, providing zero-day protection against existing and emerging threats. Juniper IDP platforms protect more than 60 protocols against malware and recognize more than 3,600 attack objects, as well as user-customizable signatures. To stay current, Juniper also maintains a dedicated security team that develops responses to block newly discovered vulnerabilities and threats.

A key feature of the ISG line is virtualization, which enables IT to segment network traffic by setting up virtual security zones, virtual systems, virtual routers, and virtual VLANs. In this way, IT can logically divide the network into zones – for example a finance zone, wireless zone, etc. – so that security is no longer bound to physical interfaces.

On the user side, Juniper Secure Access SSL VPNs provide secure LAN, extranet, and intranet access to mobile employees, customers, and partners. In addition to authentication, authorization and auditing capabilities, Secure Access platforms also perform host posture checks, ensuring only authorized users operating compliant systems can access enterprise resources. For coordinated threat control, Juniper integrated Secure Access and IDP appliances tie the session identity of the SSL VPN with the threat detection capabilities of IDP to effectively identify, stop, and remediate both network- and application-level threats within remote access traffic.

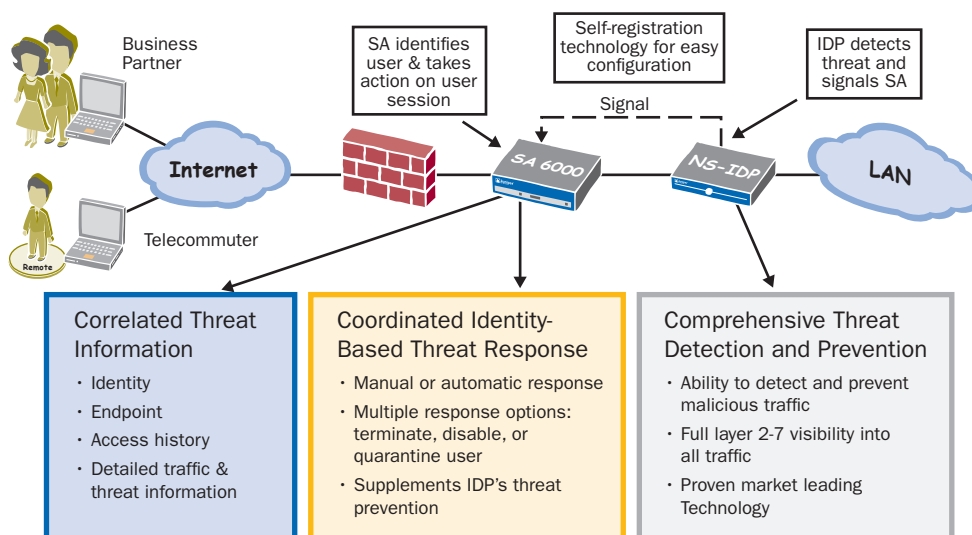


Figure 10: Juniper offers a complete, coordinated threat control solution.

WAN Acceleration:

The WX and WXC platforms provide IPsec encryption, if needed, for remote users. Because the WX/WXC platforms are deployed at both central and remote sites, Juniper designed them with an authentication capability; each WX/WXC platform is required to authenticate to a registration server before it can operate. In this way, IT has greater control over remote WX/WXC deployments. Authentication also ensures that WX/WXC devices from one enterprise won't autodiscover WX/WXC devices in a partner's network with which the enterprise shares an extranet connection. The failure of the WX/WXC platform acting as the registration server will automatically generate the election of a new registration server within the customer's domain.

Data Center Acceleration:

The Juniper DX platforms protect Web-based applications from popular Web attacks such as buffer overflow, cross-side scripting, and SQL injections. The DX platform also acts as an internal firewall, protecting the Web tier and content servers from malicious TCP and HTTP/Web-based attacks by authenticating all users and HTTP sessions before allowing access. HTTP protocol scrubbing ensures only well-formed, valid requests are passed through to servers, while TCP protocol scrubbing ensures that all TCP connections are terminated and sanitized at the DX device before being forwarded to the Web server.

Powerful URL filtering blocks requests for private, protected content, while the DX platform's server obfuscation feature masks Web server and operating system information from typical "fingerprinting" techniques. In addition, using the Auto SSL AppRule, the DX platform can automatically convert HTTP to HTTPS.

Unified Access Control (UAC):

This Juniper solution leverages a combination of identity-based policy and host posture checks to provide real-time access control throughout an enterprise network. UAC is composed of a policy manager, the Infranet Controller; policy enforcement devices, such as the ISG and Juniper firewall/VPN platforms; and the Infranet Agent. This lightweight software agent, provisioned by the Infranet Controller, assesses the end-point's compliance state and communicates it back to the Controller. UAC supports granular authorization rules, which can be based on group; URL, host, or port; client/destination; or end point/connection point.

UAC allows IT to deploy different end-point security solutions for different business needs, applications, and user groups. For example, employees with remote access can be checked for compliance with corporate images, antivirus software, and a personal firewall client on managed PCs. Non-employees, such as contractors, with unmanaged PCs can be checked for minimum security requirements. Even partner PCs can be checked through policy-based enforcement and optionally download integrated agents, such as malware scans.

Enhancing Visibility

Juniper provides unparalleled visibility into network traffic and security operations, giving IT a clear view of all activity for accounting, regulatory compliance, troubleshooting, and planning purposes. Granular visibility is crucial for understanding a wide range of operational information that can impact the data center or remote users – from WAN utilization and application performance to what security events occurred and how they were handled.

M-Series Routers:

Juniper routers track and display a variety of traffic data, both real-time and historical. The JUNOS Flow Accounting (J-Flow) feature, for example, provides a method for collecting IP traffic flow statistics, giving enterprises insight into their data flows for link utilization, fault isolation and capacity planning, offline security analysis, and internal billing. IT has the flexibility to enable J-Flow on an individual virtual router, interface or subinterface to collect statistics for specific locations.

With Real-time Performance Monitoring (RPM), enterprises can accurately monitor performance, including minimum delay, maximum delay, average delay and jitter; perform service level monitoring; monitor QoS and stateful firewall statistics; even monitor for and identify malicious employees.

Juniper routers ensure secure administration by employing authentication, Juniper-signed binaries, and user specific authorization profiles; and provide visibility into change management with a configuration audit trail, including a command history and completion information on each change.

JUNOS capabilities such as “Health Monitor” and “Event Policy” allow the Juniper routers to perform self monitoring and self diagnostics. In addition, Juniper routers support standards-based XML APIs that allow quick and easy interfacing with third-party network management applications, giving IT the ability to export records for further analysis or correlation.

Security Platforms:

Juniper security products feature detailed logging capabilities and robust reporting. All Juniper firewall/VPN products can record network activity, creating a log database of what the system saw and how it responded; for example, dropped “x” attacks or allowed “y” users to a Web site.

The ISG also provides visibility into IDP rules and policies so IT can see which policies have been hit and what impact they are having. A feature called Log Investigator helps IT drill down into any activity of interest to quickly understand and then take action on events. Investigative tools help IT with the forensics and auditing needed to quickly close out incidents. This level of visibility makes the Juniper IDP/IPS products crucial for regulatory compliance.

Beyond creating logs, the Juniper IDP solution gives IT a way to characterize a network based on the traffic and provides insight into the applications being used. For many organizations, knowing what type and version of operating system, web browser, and applications are in use is very important. For example, application-level detail is valuable for security, since a number of vulnerabilities are tied to specific versions of applications.

For remote access, the SSL VPN appliances provide granular auditing and logging. Everything a user does through the Secure Access SSL VPN appliances is logged, down to each time a user clicks his/her mouse. Logged data includes user sign-in and sign-out, session timeouts, user file requests, uploads, downloads, Web requests, every HTML request, Java Applet socket commands, and bytes transferred for client/server application requests.

All Juniper security platforms record changes to the system, including network, device, and policy information changes, and who made them. IT can quickly see who pushed an update or made a change to an object, for example, with the exact details of the change. Likewise, Juniper security products give IT the option to use predefined reports or to create custom reports, depending on needs (for example, top attacks, top sources, or top destinations) and to export reports into HTML or e-mail them for ease of information distribution.

WAN Acceleration:

The WX and WXC platforms provide extensive visibility into applications and their performance over the WAN, including real-time and historical views, with reports ranging from detailed diagnostic views up to CIO-level executive reports. WAN performance monitoring gives IT insight into link metrics such as throughput, availability, loss, and latency, as well as QoS metrics such as bandwidth allocation and application priority. Acceleration reports show the performance gains provided by TCP and protocol-specific acceleration, while compression reports detail the level of compression applied to applications. Data gathered by the WX and WXC platforms can also be exported to third-party tools for further analysis.

Data Center Acceleration:

Tracking more than 200 real-time statistics, DX platforms provide comprehensive visibility into all Web traffic inbound and outbound from the data center. By front-ending all servers, the DX platforms can consolidate traditional as well as Web logging data, easing management and freeing additional server resources. The DX offers both client- and server-side reporting, enabling IT to track statistics such as bytes in, bytes out, bytes saved; connections to clients vs. servers; SSL sessions; reused sessions; bytes and requests by content type; and system health status, including illegal response codes and errors. Historical data is easily time-sliced from seconds to years via online graphs, simplifying capacity planning, trending and troubleshooting of application and network issues.

Juniper Networks Data Center Solutions: Adapting to Business Needs

Juniper Networks makes it easy for enterprises to address market trends, such as globalization, and implement IT initiatives, such as server centralization, without having to overhaul their data centers. Juniper provides the comprehensive data center solutions enterprises need, whether they're looking to consolidate and simplify their existing data center architecture or cost-effectively deploy new data centers.

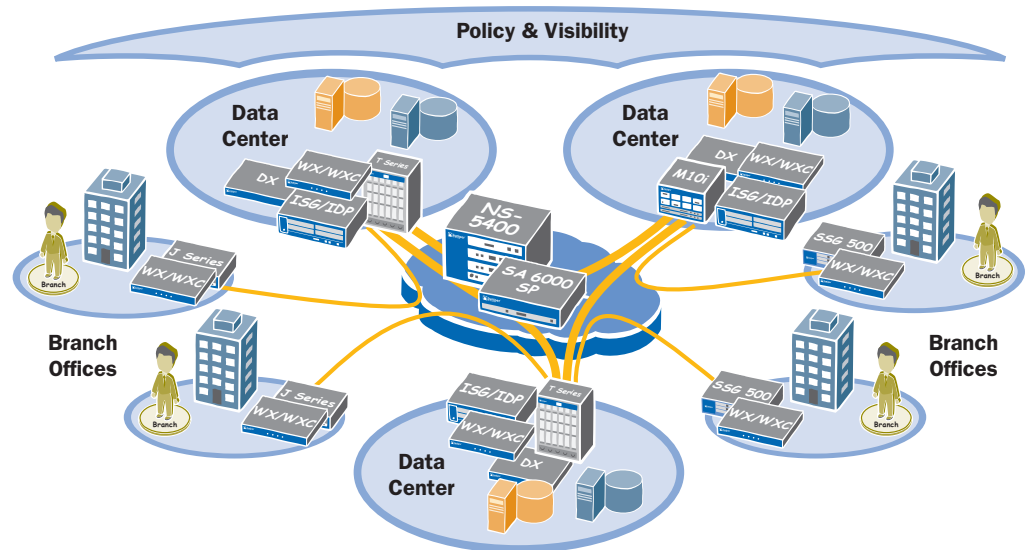


Figure 11: Juniper offers one of the industry's most complete portfolios for the distributed and extended enterprise.

Using the Juniper portfolio of routers, security and VPN appliances, and WAN and data center acceleration platforms, enterprises can maximize infrastructure and application performance, availability, and resiliency while gaining unprecedented security and visibility. With Juniper, enterprises can securely provide anytime, anywhere access to remote employees, partners and customers. The Juniper Networks data center solutions simplify regulatory compliance and streamline data backup and recovery, smoothing operations and ensuring business continuity.

The Juniper Networks data center solution enables enterprises to optimize their data centers to meet the business challenges of today and tomorrow.