SRX4600 SERVICES GATEWAY SECURES MISSION-CRITICAL, CLOUD-GRADE DATA CENTERS AND CAMPUS NETWORKS

Juniper offers enterprises and service providers a high-performance multicloud security solution

Challenge

An inability to scale, low performance, and limited connectivity capabilities mean that traditional firewalls are easily overwhelmed by sophisticated attacks. This leaves them unable to quickly react to threats and creates disjointed silos that don't meet the most demanding security requirements.

Solution

The SRX4600 Services Gateway leverages advanced threat protection, high availability, strong automation features, and actionable intelligence to protect mission-critical data centers and campus networks, acting as a central enforcement point in the Juniper Connected Security framework.

Benefits

- *Delivers high-performance, next-generation firewall for advanced threat protection*
- *Features space-efficient 1 U design, reducing power and space consumption*
- *Enables logical partitioning of the firewall via high-scale multitenancy, reducing CapEx and OpEx*
- *Secures multicloud connectivity with safe, high-performance IPsec VPN capabilities*
- *Simplifies auto-provisioning and policy enforcement via centralized, intuitive security management for lateral threat prevention*

Juniper Networks data center security solutions enable enterprises, cloud security providers, and service providers to build highly secure, high-performance networks across mission-critical private and public cloud data centers. The easy-to-manage, scalable architecture keeps operational costs down, allowing users to do more with fewer resources. Security is optimized by the space-efficient Juniper Networks® SRX Series Services Gateways— enterprise network firewalls with fully integrated, cloud-informed threat intelligence offering outstanding performance, scalability, and integrated security services.

The SRX4600 Services Gateway is designed specifically for high-performance security environments, providing comprehensive security for mission-critical enterprise and service provider data center deployments. Offering seamless integration of networking and security in a single platform, combined with multiple high-speed interfaces and advanced malware and ransomware detection working with Advanced Threat Prevention Cloud, the SRX4600 delivers the application visibility, control, "zero-day" protection, and intrusion prevention your business desperately needs.

The Challenge

As the demand for modern data centers increases, enterprises and service providers alike are planning to expand existing or build new, more efficient data centers to avoid downtime and latency issues, improve their IT efficiency, and increase their power usage effectiveness (PUE). Traditional firewalls are poorly suited for protecting mission-critical data center architectures, creating a demand for more space-efficient, higher performing enterprise network firewall solutions that are easy to manage, provide complete visibility and comprehensive security, offer secure VPN capabilities across private and public clouds, and enable the transformation to modern data centers.

The Juniper Networks Data Center Security Solution

Juniper's data center security solution addresses the needs of today's most demanding enterprise and service provider customers. The fully integrated enterprise network firewall capabilities and advanced networking features of Juniper's high-performance, space-efficient SRX Series Services Gateways allow organizations to easily build or expand their existing infrastructure into modern, highly secure, and highly efficient data centers.
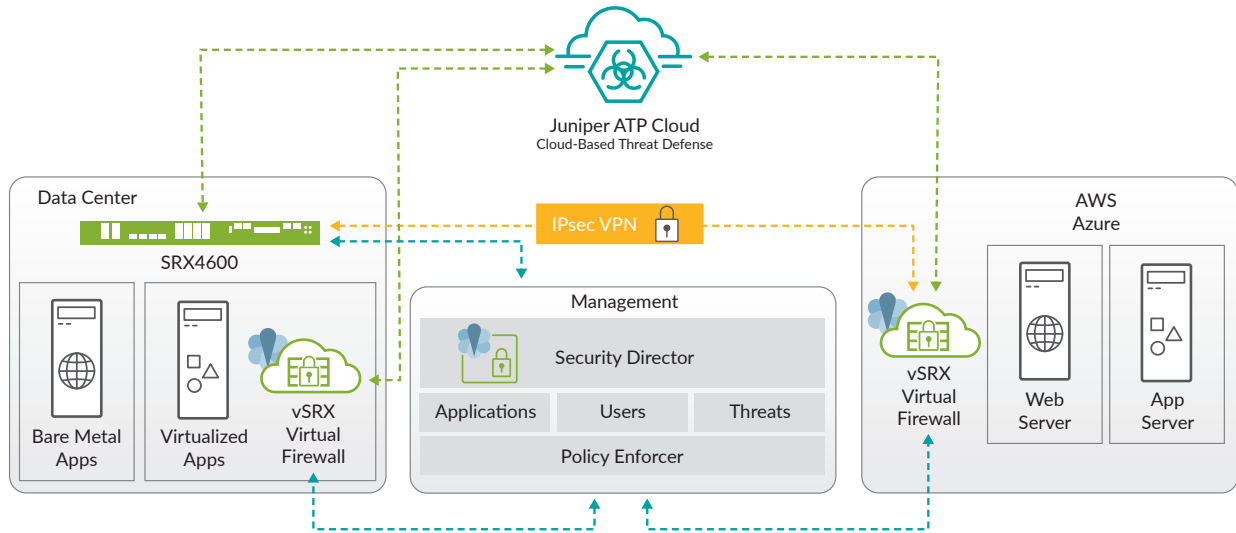
Figure 1: Data center architecture overview

The midrange SRX4600 Services Gateway sets the benchmark with its high-performance, highly secure VPN capabilities, while its 1 U form factor makes the SRX4600 ideal for space-constrained enterprise and service provider data centers.

Intuitive centralized management and policy orchestration capabilities deliver powerful, actionable security intelligence, while automated workflows enable administrators to effectively manage physical and virtual SRX Series firewalls deployed across different architectures. By providing detailed insight into and control over all applications, users, and devices, the SRX Series firewalls help stop threats quickly.

Use Cases

Securing Mission-Critical Data Center and Campus Networks

Whether enterprises or service providers, organizations building new data centers, or expanding or modernizing their global footprint, are faced with a number of challenges. The following table describes specific use cases for the SRX4600 Services Gateway, outlines the requirements for each, and details the Juniper features that satisfy those requirements.

Use Case	Deployment	Customer Requirements	Juniper Solution
Data Center Edge	• Private cloud	• Protect data center edge • Protect data center core • Intrusion prevention system (IPS) • Automation	Space-efficient, diverse I/O, high performance: • Compact form factor: 1 U • Diverse high-speed interfaces: 10GbE, 40GbE, 100GbE • Stateful firewall sessions: 60 million • 65 Gbps (server side) IPS • 60 Gbps next-generation firewall
	• Multicloud	• High-performance secure connectivity for multiclouds	High scale and high performance: • IPsec performance: 20 Gbps • IPsec tunnels: 5000
	• Cloud Security as a Service (SaaS)	• Scaled multitenancy, per-tenant advanced security and management	Scalable and multitenant solutions: • Up to 300 tenants • Per-tenant L7 services • Strong automation and management
Campus and Secure Router	• Enterprise network firewall/advanced threat prevention • Secure router/hub	• Secure application • Protection against advanced threats	Feature-rich services: • Juniper Connected Security: Intent-based policy, Juniper ATP Cloud, and E2E policy • SSL proxy: 2 Gbps • IPsec performance: 20 Gbps • IPsec tunnels: 5000
Service Provider Edge	• Gi firewall • Security gateway • Roaming firewall	• Distributed service model for security gateway and Gi firewall	Multiservices gateways: • Integrated security • IPsec: 20 Gbps • IPsec tunnels: 5000

Key Features and Benefits

To meet the requirements of users modernizing or building data centers, Juniper's data center security solution delivers the following features and capabilities.

Business Requirement	Features	Capabilities
High Performance	Up to 95 Gbps of large packet firewall throughput and up to 75 Gbps of IMIX firewall throughput	• Best suited for enterprise campus and data center edge deployments • Ideal for secure router deployments at the head office • Addresses future needs for scale and feature capacity
High-Quality End-User Experience	Application visibility and control	• Detects 3500+ L3-L7 applications, including Web 2.0 • Controls and prioritizes traffic based on application and use role • Inspects and detects applications inside SSL-encrypted traffic
Advanced Threat Protection	Intrusion prevention system (IPS), antivirus, antispam, Juniper Networks SecIntel, Juniper ATP Cloud	• Provides real-time updates to IPS signatures and protects against exploits • Implements industry-leading antivirus and URL filtering • Delivers open threat intelligence platform that integrates with third-party feeds • Protects against zero-day attacks
Professional-Grade Networking Services	Routing, secure wire	• Supports carrier-class advanced routing and quality of service (QoS)
Highly Secure	IPsec VPN	• Provides high-performance IPsec VPN with dedicated crypto engine • Offers diverse VPN options for various network designs, including remote access and dynamic site-to-site communications • Simplifies large VPN deployments with auto VPN • Includes hardware-based crypto acceleration
Highly Reliable	Chassis cluster, redundant power supplies	• Dual (redundant) dedicated MACsec-enabled 10GbE HA control and HA fabric link ports with seamless high availability • Stateful configuration and session synchronization • Active/active and active/backup deployment scenarios • Highly available hardware with dual power supply unit (PSU)
Easy to Manage and Scale	On-box GUI, Juniper Networks Junos Space® Security Director	• Centralized management for auto-provisioning, firewall policy management, Network Address Translation (NAT), and IPsec VPN deployments • Simple, easy-to-use, on-box GUI for local management
Low TCO	Junos OS	• Routing and security integrated in a single device • Lower OpEx with Junos OS automation capabilities

Solution Components

The SRX4600 Services Gateway provides cost-effective security in a small 1 U form factor. Purpose-built to protect Internet Mix (IMIX) firewall throughput network environments up to 80 Gbps, the SRX4600 incorporates multiple security services and networking functions on top of the industry-leading Juniper Networks Junos® operating system. The SRX4600 best-in-class security and advanced threat mitigation capabilities are offered as 60 Gbps of next-generation firewall, 65 Gbps of IPS, and up to 20 Gbps of IPsec VPN in data center, enterprise campus, and regional headquarter deployments with IMIX traffic patterns.

The SRX4600 recognizes more than 3500 applications and nested applications in plain text or SSL-encrypted transactions. The firewalls also integrate with Microsoft Active Directory and combine user information with application data to provide network-wide application and user visibility and control.

To learn more about the SRX4600 Services Gateway, please visit **www.juniper.net/us/en/products-services/security/srx-series/srx4600/**.

Table 1: SRX4600 performance statistics[1]

Performance/Specification	SRX4600
Firewall throughput	95 Gbps
Firewall throughput—IMIX	75 Gbps
IPsec VPN throughput—IMIX/1400 B	16/55 Gbps
Application security performance[2]	80 Gbps
Intrusion Prevention System[3]	65 Gbps
Next-generation firewall[3]	60 Gbps
Connections per second (CPS)	600,000
Maximum security policies	80,000
Maximum concurrent sessions (IPv4 or IPv6)	60 million
Route table size (RIB/FIB) (IPv4 or IPv6)	4 million/1.2 million

1. Performance, capacity, and features listed are based on systems running Junos OS 17.4R1-S1 and are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployments.

2. Throughput numbers based on UDP packets and RFC2544 test methodology

3. Throughput numbers based on HTTP traffic with 44 KB transaction size and up to the numbers captured here

Hybrid/Multicloud Data Centers

The highly secure VPN capabilities on SRX Series Services Gateways, with their dedicated crypto engines, allow you to build highly secure hybrid multiclouds. Physical SRX Series devices like the SRX4600 can securely connect to vSRX Virtual Firewalls deployed in different public clouds to ensure origin authentication, data confidentiality, and integrity.

The vSRX Virtual Firewall connects to Juniper ATP Cloud, the advanced threat defense system in the cloud, receiving the latest threat information to help prevent zero-day attacks. The vSRX is also used for IPsec VPN termination, multisite VPN, and NAT gateway functionality to facilitate and complement different public cloud deployments. vSRX Virtual Firewalls deployed in remote data center locations connect to the SRX4600 located in the head office or in the private data center via IPsec VPN for secure data transport between private and public clouds.

Junos Space Security Director centrally manages and enforces all security policies across the infrastructure irrespective of their deployment location.

To learn more about the Juniper Networks vSRX Virtual Firewall, please visit www.juniper.net/us/en/products-services/security/srx-series/vsrx

Juniper ATP Cloud: Advanced Malware Protection from the Cloud

A cloud-based service that's integrated with Junos Space Security Director and SRX Series firewalls, Juniper ATP Cloud delivers a dynamic anti-malware solution that adapts to an ever-changing threat landscape. Juniper ATP is a cloud-based advanced anti-malware service that uses dynamic analysis (sandboxing) to defend against sophisticated zero-day attacks for your data centers and provides built-in machine learning to improve verdict accuracy.

To learn more about Juniper ATP Cloud, please visit www.juniper.net/us/en/products-services/security/advanced-threat-prevention/.

Junos Space Security Director: Consistent and Unified Security Policy and Management Tools

With Juniper's scalable and intuitive Junos Space Security Director software, you can make informed security decisions and gain end-to-end visibility into applications, users, and threats in your physical and virtual cloud data centers. With a holistic view, rich security feature set, and easy-to-use actionable intelligence, Security Director allows you to immediately take remedial actions and block high-risk applications and threats with a single click. User visibility and user-level application and threat visibility features allow administrators to create policies to improve user productivity, bandwidth usage, and session consumption for one or more data centers. By offering single-pane-of-glass management and an easy-to-use intelligent security rule creation wizard and auto-rule placement, Security Director lets you create less complex security policies faster for assets that are deployed in private or public clouds.

To learn more about Security Director, please visit www.juniper.net/us/en/products-services/security/security-director.

Juniper Connected Security: Dynamic Policy Control, Detection, and Enforcement

Juniper Connected Security leverages the entire network, not just perimeter firewalls, as a threat detection and security enforcement domain. The Policy Enforcer component of Junos Space Security Director orchestrates policies created by Juniper ATP Cloud, distributing them to Juniper Networks EX Series Ethernet Switches, Juniper Networks QFX Series switches, and third-party switches, as well as to Juniper virtual and physical SRX Series firewalls deployed in private and public cloud data centers. Juniper Connected Security user intent policies facilitate the use of a single metadata-based policy model across physical and cloud deployments, taking alternative action across a large set of policies in an automated manner based on network status.

To learn more about Juniper Connected Security, please visit www.juniper.net/us/en/solutions/security/.

Summary—Secure Your Mission-Critical Data Centers with Juniper's High-Performance Firewalls

Juniper's security solutions empower you to seamlessly migrate to modern, high-performance data center architectures without compromising security, flexibility, and manageability. With high-performance, space-efficient, next-generation firewalls, smarter and faster centralized management, and highly evolved security intelligence and automation tools, Juniper Networks allows you to secure your mission-critical, cloud-grade data centers and campus networks while keeping your operational costs down.

Next Steps

For more information about Juniper's security solutions, please visit us at www.juniper.net/us/en/products-services/security and contact your Juniper Networks representative.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

Fax: +1.408.745.2100

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

JUNIPGR NETWORKS | Engineering Simplicity

EXPLORE JUNIPER
Get the App.

JUNIPER 1ON1

Available on the App Store

ANDROID APP ON Google Play