Securing Enterprise Hybrid Clouds

High-performance, space-efficient, next-generation firewalls defend enterprise hybrid cloud infrastructure

Challenge

Traditional firewalls lack the agility to quickly react to emerging threats. An inability to scale, combined with limited connectivity capabilities, makes them easily overwhelmed by sophisticated attacks, creating disjointed silos that don't meet the most demanding security requirements.

Solution

The SRX4000 line of Services Gateways is ideally suited for enterprise hybrid clouds. Focusing on application visibility and control, intrusion prevention, advanced threat protection, and high availability, the SRX4000 line provides secure connectivity for small to medium-sized enterprise campuses and data centers.

Benefits

- High-performance next-generation firewalls provide advanced threat protection.
- Lower TCO results in significant CapEx and OpEx savings.
- Space-efficient 1 U form factor reduces power and space consumption.
- Highly secure VPN capabilities ensure secure connectivity to the public cloud.
- Centralized and intuitive security management simplifies policy enforcement and monitoring.

Juniper Networks hybrid cloud architecture enables enterprises to build secure, high-performance environments across 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, which are next-generation firewalls (NGFWs) with fully integrated, cloud-informed threat intelligence that offers outstanding performance, scalability, and integrated security services. Designed for high-performance security environments and seamless integration of networking, along with advanced malware detection with Juniper Sky™ Advanced Threat Prevention (ATP), application visibility and control, and intrusion prevention on a single platform, the SRX Series firewalls are best suited for enterprise hybrid cloud deployments.

The Challenge

With the growing reliance on cloud technologies, enterprise data centers have turned to hybrid cloud architectures to provide the flexibility and economic benefits of the public cloud alongside the high-performance NGFW features and capabilities deployed in the private cloud.

Migrating to a hybrid cloud model with traditional firewalls presents its own set of challenges, including low performance, limited security, and poor VPN performance. The poor suitability of traditional firewalls for hybrid cloud environments has created an immediate need for a high-performance, space-efficient NGFW solution that is easy to manage, provides complete visibility and comprehensive security, offers secure VPN capabilities across enterprise private and public cloud deployments, and allows enterprises to securely migrate to a hybrid cloud model.

The Juniper Networks Enterprise Hybrid Cloud Solution

The fully integrated NGFW and advanced networking features of Juniper's high-performance, space-efficient SRX Series Services Gateways allow enterprises to easily migrate to a hybrid cloud architecture. The midrange SRX4100 and SRX4200 Services Gateways set a new benchmark with their high-performance, highly secure VPN capabilities, while their one rack unit form factor makes them ideal for small to medium-sized enterprise campuses and data centers.

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

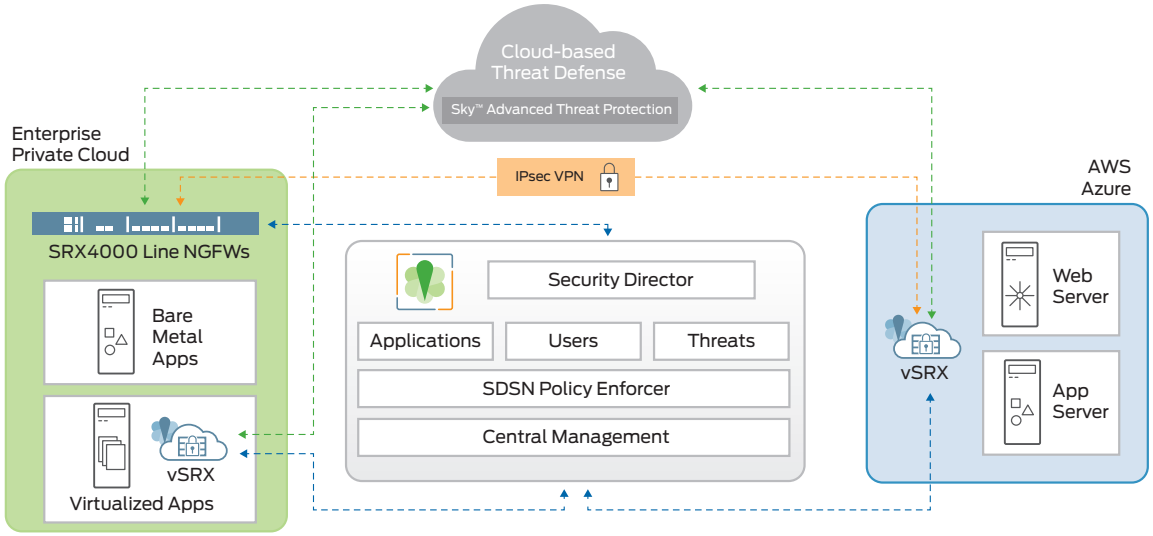

Figure 1: Hybrid cloud architecture overview

Migrating to a Secure Hybrid Cloud: Real-World Use Cases

Enterprises migrating to a secure hybrid cloud deployment are faced with a number of challenges. The following table describes two specific use cases, outlines the security requirements for each, and details the Juniper solutions that satisfy those requirements.

Use Cases	Enterprise Expansion Adding new private data center to a different geography	Leverage Public Cloud Benefits Distributing workloads across geographical locations
	A new e-commerce enterprise with a physical data center in New York wants to expand its global presence and decides to open offices globally.	A new video-streaming enterprise anticipates more viewers in Western Europe between 7 p.m. and 10 p.m. during November and December. Deploying a new physical data center or provisioning a virtual data center in a private cloud can be expensive to facilitate such intermittent usage.
Requirements	• The company needs to add a new private data center and deploy high-performance next-generation firewalls. • The company needs multiple public data centers with virtual firewalls deployed for remote and small offices. • Security requirements include application visibility and control, intrusion prevention, URL filtering, and advanced anti-malware protection. • Secure VPN connectivity is required between headquarters and private and public data centers. • Policies for the private data center need to be managed and enforced from headquarters in New York and be synced with other locations. • Other requirements include highly available hardware and software, 10GbE interface connectivity, and next business day replacement.	• The ability to provide a high-quality user experience in a cost-efficient manner without compromising customer privacy is critical. • Content and customer data need to be replicated. • The data center must be able to quickly scale up or down, based on user demand. • Loss of service due to failures of any kind is unacceptable. • Leaking copyrighted content or customer details is unacceptable. • Policies for this data center need to be managed and enforced from headquarters in New York.
Juniper Security Solutions		
Next-Generation Firewall (NGFW) and Secure Connectivity	• Physical SRX4100 and SRX4200 NGFWs are installed in the private data center. • All SRX Series NGFWs connect to the advanced threat defense system in the cloud (Juniper Sky ATP) and receive the latest threat information to detect zero-day attacks. • The SRX4100/SRX4200 firewalls in the private cloud connect to vSRX Virtual Firewalls in the public cloud via IPsec VPN for secure data transport.	• A vSRX Virtual Firewall is installed between the virtual private cloud (VPC) and Internet gateway of each Amazon Web Services (AWS) deployment to secure the instances and applications in the VPC. • The vSRX Virtual Firewalls in the public cloud connect to the physical SRX4100/SRX4200 NGFWs in the private cloud and headquarters via IPsec VPN for secure data transport. • The vSRX is also used for IPsec VPN termination, multisite VPN, and Network Address Translation (NAT) gateway functionality to facilitate and complement the AWS deployment.
Advanced Threat Protection	• All vSRX Virtual Firewalls connect to the advanced threat defense system in the cloud (Sky ATP) and receive the latest threat information to detect zero-day attacks.	
Central Management and Policy Enforcement	• The SRX4100/SRX4200 physical firewalls deployed in the private data center, and vSRX Virtual Firewalls deployed in AWS public data centers, register with Juniper Networks Junos Space™ Security Director, which centrally manages all security policies across the hybrid cloud infrastructure. • New security policies are centrally added to or updated from Security Director and enforced across all SRX Series physical and vSRX Virtual Firewalls.	

Key Features and Benefits

Capabilities	Benefits	Features
High-performance NGFW	· Application, user, and content visibility and control · Enables secure migration into hybrid cloud	· High-performance NGFW secures workloads on premise. · Highly secure VPN capabilities for secure connectivity to public cloud work seamlessly with the vSRX on AWS. · Key component of the Software-Defined Secure Network (SDSN) framework.
Advanced threat protection	· Intrusion prevention system (IPS), antivirus, antispam, Juniper Networks Spotlight Secure, Sky ATP	· Real-time updates to IPS signatures protect against exploits. · Includes industry-leading antivirus and URL filtering. · Open threat intelligence platform integrates with third-party feeds. · Provides zero-day attack protection.
Centralized management and policy enforcement	· Greater visibility with intuitive management · Faster detection and remediation · Enhanced operational efficiency · Massive scalability	· Simplified single-pane management. · End-to-end policy enforcement across network. · Actionable intelligence. · Superior automation. · Manage thousands of firewalls.
Compact footprint	· Space efficient · Quick installation · Lower total cost of ownership	· Industry-leading price and performance. · 1 U form factor is ideal for campuses and data centers. · Lowers power consumption.
High availability	· Prevents single points of failure	· Control link recovery. · Intelligent fabric monitoring mechanism and auto fabric link recovery. · High availability fault detection enhancements.
Highly secure IPsec VPN	· Highly secure connectivity	· High-performance IPsec VPN with dedicated crypto engine. · Diverse VPN options for various network designs include remote access and dynamic site-to-site communications. · Simple large VPN deployments with auto VPN. · Hardware-based crypto acceleration.
Easily expandable to public cloud	· Seamlessly extend security across public clouds without compromising flexibility and manageability	· vSRX in public cloud data centers include AWS and Microsoft Azure, enabling secure connectivity to the public cloud using highly secure VPN capabilities.

Solution Components

High-Performance, Space-Efficient, Next-Generation Firewalls in Private Cloud Enterprise Data Centers

SRX Series Services Gateways, designed for high-performance security services architectures, seamlessly integrate networking and security in a single platform. While a variety of SRX Series firewalls are available, the SRX4100 and SRX4200 are best suited for hybrid cloud architectures within private enterprise data centers, campuses, and regional headquarters.

Focusing on application visibility and control, intrusion prevention, advanced threat protection, and integrated cloud-based security, the SRX4100 and SRX4200 combine integrated unified threat management (UTM) with outstanding protection, performance, scalability, availability, and security services.

The SRX4100 and SRX4200 firewalls provide cost-effective, high-performance security in a small 1 U form factor, making them ideal for hybrid clouds. Purpose-built to protect up to 80 Gbps Internet Mix (IMIX) throughput environments, the SRX4100 and SRX4200 incorporate multiple security services and networking functions on top of the Juniper Networks Junos® operating system, the industry-leading OS that lowers OpEx with its automation capabilities.

	SRX4100	SRX4200
Firewall throughput	40 Gbps	80 Gbps
Firewall throughput—IMIX	20 Gbps	40 Gbps
Firewall throughput with application security	18 Gbps	35 Gbps
IPsec VPN throughput—IMIX	5 Gbps	9.6 Gbps
Intrusion prevention	10 Gbps	20 Gbps
NGFW* throughput	7 Gbps	15 Gbps
Connections per second	175,000	350,000
Maximum session	5 million	10 million

Performance, capacity, and features listed are based on systems running Junos OS 15.1x49 and are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployments.

*NGFW is a combination of advanced features such as application security, IPS, and URL filtering in addition to the foundational services such as logging and stateful firewall.

vSRX in Enterprise Public Cloud Data Centers

A vSRX Virtual Firewall installed between the VPC and Internet gateway of each AWS deployment in the public cloud secures the instances and applications in the virtual private cloud. The vSRX Virtual Firewall connects to Sky ATP, the advanced threat defense system in the cloud, and receives the latest threat information to help detect zero-day attacks.

The vSRX is also used for IPsec VPN termination, multisite VPN, and NAT gateway functionality to facilitate and complement the AWS deployment. vSRX Virtual Firewalls in remote data center locations connect to the SRX Series physical firewalls in the head office via IPsec VPN for secure data transport.

Junos Space Security Director centrally manages all security policies across the infrastructure. The vSRX Virtual Firewalls deployed in remote data centers register with Security Director.

SRX Series Firewalls Provide Highly Secure VPN Capability for Easy and Secure Migration to Hybrid Cloud

The highly secure VPN capabilities on SRX Series firewalls, with their dedicated crypto engines, allow you to build highly secure hybrid clouds. vSRX Virtual Firewalls in remote data centers connect to the physical SRX Series firewalls at headquarters via IPsec VPN for secure data transport.

More Use Cases for SRX Series Compact, High-Performance Next-Generation Firewalls

In addition to the hybrid cloud use case, the compact SRX Series high-performance, next-generation firewalls can also be deployed in different scenarios such as:

- Data center/campus deployments where rich NGFW capabilities are required
- Data center core deployments where low power consumption and compact physical firewalls are required
- Any environment where highly secure VPN capabilities and VPN tunnels are needed
- Small offices where space is at a premium and routing and security are needed in a single platform
- Networks where high-performance firewall and Sky ATP integration are required

To learn more about Juniper's SRX4000 line of Services Gateways and vSRX Virtual Firewall, please visit www.juniper.net/us/en/products-services/security/srx-series/srx4000 and www.juniper.net/us/en/products-services/security/srx-series/vsrx/.

Sky Advanced Threat Prevention: Advanced Malware Protection from the Cloud

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

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

Junos Space Security Director: Consistent Security Policy and Management Tools

With Juniper's scalable and intuitive Junos Space Security Director software, enterprises are able to make informed security decisions and achieve end-to-end visibility for applications, users, and threats in their physical and virtual cloud data centers. With a holistic view, rich security feature set, and easy-to-use actionable intelligence, Security Director allows enterprises 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.

Dynamic Policy Control, Detection, and Enforcement

Juniper's Software-Defined Secure Network (SDSN) platform 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 provides the ability to orchestrate policies created by the Sky ATP cloud-based malware detection solution and distribute them to Juniper Networks EX Series Ethernet Switches and Juniper Networks QFX Series switches, as well as to Juniper virtual and physical SRX Series firewalls deployed in your private and public cloud data centers.

To learn more about Security Director, please visit www.juniper.net/us/en/products-services/security/security-director. To learn more about Juniper's Software-Defined Secure Network, please visit www.juniper.net/us/en/solutions/software-defined-secure-networks.

Summary—Secure Your Hybrid Cloud Deployment with Juniper's High-Performance NGFWs

Juniper's security solutions seamlessly extend across private and public cloud architectures without compromising security, flexibility, and manageability. With midrange, 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 network, keep operational costs down, and easily migrate to a hybrid cloud architecture.

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 challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

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

3510612-001-EN Mar 2017