

# FIVE REASONS TO MIGRATE TO NEXT-GENERATION SRX300 FIREWALLS

*Extending security across all points of the network to safeguard users, applications, and infrastructure*

## Challenge

Customers using outdated, end-of-life firewalls are putting themselves at tremendous risk for falling prey to a potential cyber attack, threatening the entire organization.

## Solution

By migrating to the latest SRX300 line of Services Gateways from Juniper, organizations can effectively position themselves to protect their business from the most sophisticated attacks.

## Benefits

- Identify and block threats in real time with advanced security
- Consolidate security and networking into a single platform
- Simplify security operations to respond faster to detected breaches
- Minimize disruptions to security operations

*The never-ending reports about security breaches make cybersecurity impossible to ignore. The World Economic Forum calls cyber attacks a risk of our increasing cyber dependency and considers the threat of a massive data breach or theft to be among the top five challenges facing us today.<sup>1</sup> Organizations must prepare themselves to detect, isolate, and respond to these cyber threats before costly data breaches and compliance violations threaten their business.*

## The Challenge

In an era of mobile, cloud, and the Internet of Things (IoT), the old tried-and-true perimeter security model is simply not sufficient to protect your business. Not only are cyber threats growing increasingly sophisticated and evolving quickly, the attack surface has expanded significantly. Legacy security infrastructure can't handle the network speeds and evasive threats that are becoming commonplace today. Aging solutions such as outdated firewalls not only compound the problem, but their complexity and time-consuming maintenance requirements can drain the security team's operational efficiency by distracting valuable talent, creating gaps that criminals, nation-states, and other attackers can exploit.

## The Juniper Networks Migration Path for Legacy Firewalls

Organizations employing legacy firewalls can easily migrate to Juniper Networks® SRX300 line of Services Gateways to gain comprehensive, simplified security. Customers can choose from a variety of models—including the SRX300, SRX320, SRX340, and SRX345—for advanced security, networking, SD-WAN, and LTE backup, all in a single platform. Ideal for branch and distributed enterprise locations, SRX Series Services Gateways bundles simplify the migration path, allowing you to quickly and easily upgrade your network and deploy the most comprehensive firewalls with advanced threat capabilities while investing in Juniper's expertise and security processes.

## Five Reasons to Migrate to SRX300 Next-Generation Firewalls

Obsolete and outdated firewalls increase security risk. Upgrading to the latest SRX300 Services Gateway improves an organization's security posture. Here are five reasons to migrate to the latest SRX300 to enjoy the benefits of powerful protection for your distributed enterprise.

<sup>1</sup>The Global Risks Report: 2018, World Economic Forum, [http://www3.weforum.org/docs/WEF\\_GRR18\\_Report.pdf](http://www3.weforum.org/docs/WEF_GRR18_Report.pdf)

1. **Advanced cybersecurity, simplified.** The SRX300 acts as a key enforcement point for Juniper's connected security platform, which simplifies operations while protecting users, applications, and infrastructure. Working with Juniper Sky™ Advanced Threat Prevention, the SRX300 provides advanced detection of hard-to-catch malware, such as ransomware, ensuring that your cyber defenses continually adapt to evolving risk conditions. Automated policy management and enforcement use network and threat data to update policies and deploy unified enforcement across your infrastructure.
2. **Real-time threat prevention.** Integrating the SRX300 Services Gateway with Juniper Sky ATP gives your organization another layer of protection, extending defenses by detecting and stopping never-before-seen malware before it hits its target. Using machine learning, Juniper Sky ATP employs real-time information from the cloud to continuously analyze Web and e-mail files for ransomware and other evasive threats. Integration with Juniper Sky ATP enables the SRX300 firewalls to deliver deep inspection, inline blocking, and actionable alerts.
3. **Enhanced security performance while preserving operational expertise.** The SRX300 line provides the most powerful security for distributed enterprises in the market today. By migrating to the latest next-generation platforms, your organization can preserve your existing Juniper security operational expertise while taking advantage of the higher performance and more powerful capabilities of the latest version of Juniper Networks Junos® operating system. Network and security teams don't have to learn how to configure and manage a new network OS, increasing IT operational efficiency and freeing up valuable time and resources for business innovation.
4. **Distributed enterprise deployments.** Organizations need a single platform that includes both security and SD-WAN capabilities for distributed and branch locations, along with features such as Zero Touch Provisioning (ZTP), application-based routing, and quality of experience (QoE).
5. **Secure Routing.** To support the widest variety of WAN connectivity, the SRX300 line of Services Gateways supports on-board fiber optic ports, Media Access Control Security (MACsec) ports, and LTE wireless backup, ensuring you can meet the needs of the different connection options for distributed enterprise and branch locations.

## Choosing the Right SRX300 Firewall

The SRX300 line of Services Gateways has been designed to meet any organization's varying needs in distributed enterprises. Current customers employing legacy Juniper firewalls can deploy the following SRX300 line models and upgrade to the latest next-generation firewall technology. For instance:

- If you currently use the SSG-5 or SRX100, you might consider migrating to the SRX300.
- If you currently use the SSG-20 or SRX210/SRX220, you might consider migrating to the SRX320.
- If you currently use the SSG-140 or SRX240, you might consider migrating to the SRX340 or SRX345.

Ideal for securing small branch or retail offices, the SRX300 line consolidates security, routing, SD-WAN, and WAN connectivity in a small desktop device. The SRX320 provides secure connectivity for small distributed enterprise branch offices, offering security, routing, SD-WAN, and WAN connectivity in a small desktop device that includes optional Power over Ethernet Plus (PoE+) ports. To securely connect midsize distributed enterprise branch offices, the SRX340 consolidates security, routing, SD-WAN, and WAN connectivity in a 1 U form factor. Supporting optional unified threat management (UTM) security capabilities and LTE wireless backup, the SRX340 provides the advanced security and WAN connectivity backup for any distributed location. Best suited for midsize to large distributed enterprise branch offices, the SRX345 Services Gateway consolidates security, routing, SD-WAN, and WAN connectivity in a 1 U form factor and support up to 5 Gbps firewall and 800 Mbps IPsec VPN.



SRX300



SRX320



SRX340



SRX345

## Summary—Simplify and Strengthen Cybersecurity

Cybersecurity is growing more complex by the day. No organization can trust old, outdated firewalls to defend against breaches and data theft. With Juniper's connected security platform and the SRX300 line of Services Gateways, you can dramatically improve and simplify your security posture, streamlining the integration of best-fit protections into your ecosystem to protect your organization efficiently and effectively.

### Next Steps

Learn more about SRX300 line of next-generation firewalls by visiting [www.juniper.net/us/en/products-services/security/srx-series/srx300/](http://www.juniper.net/us/en/products-services/security/srx-series/srx300/).

For more information on SRX300 migration bundles, please 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](http://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**

**JUNIPER** | Engineering  
NETWORKS | Simplicity

