

# SPOTLIGHT ON INNOVATION



SRX3600



SRX3400

Juniper Networks SRX3600 Services Gateway and Juniper Networks SRX3400 Services Gateway are next-generation services gateways that deliver market-leading scalability and service integration in a midsize form factor.

## SRX Series Services Gateways

Juniper Networks SRX Series is the next-generation solution for securing ever-increasing network infrastructure and application demands. Based on Dynamic Services Architecture, the SRX Series is designed to provide unrivaled processing scalability, I/O flexibility, and high feature integration.

The SRX Series delivers unmatched performance and scalability to ensure future expansion and sustainable growth for your network infrastructure—no matter how large or small the location. From the top-of-the-line SRX5800, which offers 120 Gbps of firewall throughput and 350,000 new connections per second, the SRX offers the scalability that widely distributed enterprises require. Quite simply, it's the industry's highest-performing security solution.

Based on JUNOS® Software and leveraging the security heritage of ScreenOS, SRX Series Services Gateways integrate proven networking and security capabilities into a single solution. They feature many of the same benefits delivered by Juniper networking and security products—including full-featured firewall and IPS capabilities, DoS, NAT, and QoS. Management solutions include CLI and support for Network and Security Manager (NSM), which can manage all of Juniper's firewall, IDP, SSL, and UAC product lines.

### Key benefits of SRX Series Services Gateways include:

- Scalable and flexible processing capability via additional Service Processing Cards (SPC)
- Scalable interfaces via modular Input/Output Cards (IOC), enabling the ideal balance between processing and interface capabilities
- High integration of services, including firewall, IPS, routing, NAT, QoS, and other features

- Carrier-class reliability and streamlined feature integration on JUNOS Software for optimal traffic processing across various traffic processing features

### Juniper Networks SRX Series for service providers and enterprise data centers

#### New Juniper Networks SRX3600

With the midplane design of the SRX3000 line, the SRX3600 supports up to 30 Gbps firewall, 10 Gbps firewall and IPS, or 10 Gbps of IPsec VPN along with up to 175,000 new connections per second in a single, expandable midsize form factor. Based on the same high-speed switching fabric as the SRX5000 line, the SRX3600 is ideally suited for securing medium to large enterprise data centers, co-located data centers, or securing next-generation enterprise services/applications. It also can be deployed to secure service provider infrastructures as well as next-generation services.

#### New Juniper Networks SRX3400

The SRX3400 Services Gateway uses the same processing and I/O expansion modules as the SRX3600. Also supporting a midplane design, the SRX3400 can expand up to 20 Gbps firewall, 6 Gbps firewall and IPS, or 6 Gbps of IPsec VPN, along with up to 175,000 new connections per second in a single, expandable small form factor chassis. The SRX3400 is ideally suited for securing and segmenting enterprise data center network infrastructures as well as aggregating various security solutions.

## New Juniper Networks SRX Series for the branch

The SRX Series provides essential capabilities that connect, secure, and manage workforce centers that range in size from fewer than 10 users to hundreds of users. By consolidating fast, highly available switching, routing, security, and applications capabilities in a single box, enterprises can economically deliver new services, safe connectivity, and satisfying end-user experiences. The SRX Series for the branch provides perimeter security, content security, access control, and

network-wide threat visibility and control. Specifically:

- Best-in-class firewall and VPN capabilities secure the perimeter with minimal configuration and consistent performance. By using zones and policies, even new network administrators can configure and deploy an SRX Series Services Gateway quickly and securely.
- Policy-based VPNs support more-complex security architectures that require dynamic addressing and split tunneling.

- For content security, the SRX Series offers a complete suite of optimal unified threat management and IPS licenses to protect your network from the latest content-borne threats.
- The SRX Series for the branch interoperates with other Juniper Networks security products to deliver enterprise-wide universal access control and adaptive threat management.
- Multiple form factors allow you to make cost-effective choices for mission-critical deployments.

For more information, visit:

[www.juniper.net/us/en/products-services/security/srx-series/](http://www.juniper.net/us/en/products-services/security/srx-series/)



NSM Central Manager

Integral to Juniper Networks Adaptive Threat Management Solutions, Network and Security Manager (NSM) is a unified device management solution for Juniper's network infrastructure of routing, switching, and security devices.

## New Juniper Networks Adaptive Threat Management

Juniper Networks Adaptive Threat Management is the industry's first open solution set that provides real-time threat defense with unparalleled network-wide visibility and control—at scale—to reduce risk and increase productivity.

Based on a dynamic, open security infrastructure, Juniper's Adaptive Threat Management Solutions leverage new and enhanced technologies based on a best-

in-class networking product portfolio. The Adaptive Threat Management Solutions include:

- New Juniper Networks SRX3000 Series Services Gateways
- A new release of Juniper's network access control (NAC) solution, including Unified Access Control (UAC) 3.0 and Secure Access (SA) SSL VPN 6.4 technology with new standards-based interoperability functionality
- New releases of Juniper Networks Security Threat Response Manager (STRM) 2008.3 and Network and Security Manager (NSM) 2008.2 with advanced network management, threat response, and reporting

Juniper's UAC now supports the IF-MAP protocol from Trusted Computing Group's Trusted Network Connect (TNC). This protocol extends the TNC architecture to support standardized, dynamic data interchange among a wide variety of networking and security components, enabling customers to implement multi-vendor systems that provide coordinated defense-in-depth.

Enhanced Secure Access SSL VPN 6.4 and UAC 3.0 software releases deliver the industry's only coordinated, standards-based, enterprise-wide access control solution, working together to seamlessly orchestrate local and remote access and ensure consistently enforced global policies for any user or role—including employees, contractors, partners, and offshore users. Juniper offers broad support for mobile devices, as well as robust endpoint assessment. In addition, robust automatic remediation is available through collaboration with OPSWAT and participation in the OESISOK program. With new FIPS-compliant models of UAC and SA Series appliances, government

agencies now can provide secure remote network access that exceeds the needs of the most demanding and complex environments.

With the NSM 2008.2 and STRM 2008.3, enterprises can automate and correlate attack responses to increase IT productivity with universal network and security management that speeds deployment time and simplifies network correlation and reporting, enabling customers to effectively cut management costs by more than 50 percent.

For more information, visit:  
[www.juniper.net/us/en/solutions/enterprise/security-compliance/adaptive-threat-management/](http://www.juniper.net/us/en/solutions/enterprise/security-compliance/adaptive-threat-management/)

### New Juniper Networks Odyssey Access Client (OAC)

The latest versions of OAC seamlessly integrate with Unified Access Control (UAC), Juniper's standards-based, comprehensive, dynamic access control solution. The Juniper Networks Odyssey Access Client family is a complete set of secure, standards-based 802.1X access clients (suplicants) built explicitly for enterprises and government agencies. OAC provides strong wired and wireless security capable of fully protecting network data and user credentials, which can be easily and quickly deployed and managed enterprise-wide for a low total cost of ownership. OAC operates effortlessly with multiple authentication types, security profiles, networking environments, and complex authentication

schemes while supporting advanced security protocols. OAC secures user authentication and network connectivity, ensuring that users connect to the network in the appropriate manner, that login credentials are not compromised, and that user and network credentials and transmitted data remain secure and private.

The OAC FIPS Edition includes the Odyssey Security Component, a cryptographic module that is FIPS 140-2 Level 1 validated. OAC FIPS Edition also was accepted recently into evaluation for conformance to the Common Criteria (ISO/IEC 15408).

For more information, visit:  
[www.juniper.net/us/en/products-services/ipc/](http://www.juniper.net/us/en/products-services/ipc/)

Tell us what you think of Veer.

[Take a Short Survey ▶](#)



**CORPORATE AND  
SALES HEADQUARTERS  
JUNIPER NETWORKS, INC.**  
 1194 North Mathilda Avenue  
 Sunnyvale, CA 94089 USA  
 Phone: 888.JUNIPER (888.586.4737)  
 or 408.745.2000  
 Fax: 408.745.2100

**APAC HEADQUARTERS  
JUNIPER NETWORKS, INC. (HONG KONG)**  
 26/F, Cityplaza One  
 1111 King's Road  
 Taikoo Shing, Hong Kong  
 Phone: 852.2332.3636  
 Fax: 852.2574.7803

**EMEA HEADQUARTERS  
JUNIPER NETWORKS, INC. (IRELAND)**  
 Airside Business Park  
 Swords, County Dublin, Ireland  
 Phone: 35.31.8903.600  
 Fax: 35.31.8903.601