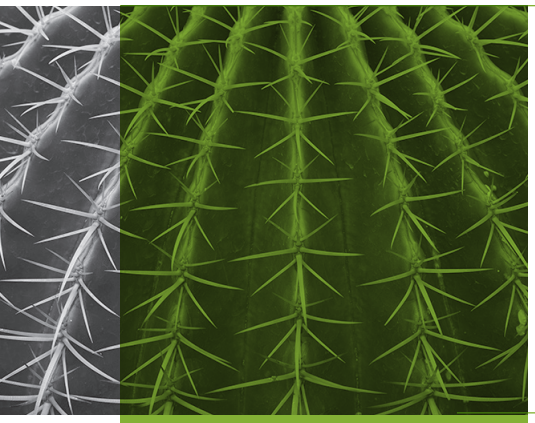

PROTECT YOUR BUSINESS WITH A NEXT-GENERATION FIREWALL

Next-generation firewalls deliver better protection through application-aware security and user role-based controls

Challenge

Organizations need more control over the applications and traffic on their networks to simultaneously protect their assets against attacks and manage bandwidth usage. The solution needs to be efficient while still delivering high levels of security assurance.

Solution

SRX Series Services Gateways deliver secure SD-WAN capabilities alongside next-generation firewall protection with integrated application awareness, intrusion prevention, role-based user controls, and best-in-class advanced security services.

Benefits

- *Protect against application-borne threats and manage bandwidth usage with application-based controls*
- *Minimize policy-management complexity with user- and role-based firewall controls*
- *Block network-based exploits, malware, and other threats with intrusion prevention and advanced security services*
- *Dynamically manage network traffic using secure SD-WAN and SD-LAN*
- *Streamline operations with a single, central management platform*

Organizations are looking for ways to protect their assets amidst an ever-increasing threat landscape. You only need to look at the latest headlines to see why security is more important than ever.

The latest generations of web-based applications, combined with the proliferation of mobile devices, have made it difficult to effectively manage traffic and provide access to data while delivering the right mix of security and network services. There might be hundreds or even thousands of applications running across a typical enterprise network—most sanctioned by central IT, others part of shadow IT efforts, and some even installed for personal use.

To support this environment, security teams must overcome a number of complex operational problems. How do you control which applications are allowed on your network? How do you restrict those that are not? How do you ensure that business-critical network traffic is prioritized? How do you bolster security without compromising operational efficiency?

Most importantly, how do you prevent security from negatively impacting your business, especially as the growing popularity of distributed working drives increasing demand for secure SD-WAN technologies? This is where a next-generation firewall can help.

The Challenge

As network infrastructure—and the threats targeting that infrastructure—continue to evolve, so too must the network security solutions tasked with protecting organizations. Today's network security solutions not only require the right architecture to deliver the appropriate mix of performance and scale in an evolving network environment, they must also give administrators visibility into and control over the applications traversing the network. This visibility must be available wherever those networks happen to be within an organization's multicloud fabric, whether they are wired, wireless, or WAN interconnects.

Many administrators have responded to today's business environment with layers of security solutions, deploying multiple security appliances to provide adequate protection. While these appliances do deliver considerable protection, they also increase network complexity, add management overhead, and reduce overall performance.

The Juniper Networks Next-Generation Firewall Solution

Juniper Networks® SRX Series Services Gateways deliver integrated next-generation firewall (NGFW) protection with application awareness, intrusion prevention system (IPS), user role-based controls, best-in-class advanced security services, and SDN capabilities. SRX Series firewalls also perform full-packet inspection, as well as applying application- and user-specific security policies.

With these powerful capabilities, you can create security policies based on the applications whose data is transiting the network and/or the user receiving or sending network traffic—all while simultaneously examining the content, regardless of source or destination. This protects your environment from threats, manages how network bandwidth is allocated, and maintains appropriate access controls.

The Juniper Networks AppSecure suite of application-aware security services for the SRX Series firewalls classifies traffic flows while providing greater visibility, enforcement, control, and protection. Using a sophisticated classification engine, AppSecure accurately identifies applications regardless of port or protocol—including those known for using evasive techniques to avoid detection.

AppSecure provides the context needed to regain control of network traffic, set and enforce policies based on accurate information, and deliver the performance and scale required to address your business needs. Services enabled by AppSecure include AppTrack for detailed visibility into application traffic; AppFW for granular enforcement of application traffic policies; and AppQoS for prioritizing and metering application traffic.

The SRX Series firewalls allow you to include additional content security through integrated advanced services and IPS, providing greater protection against malware, spam, phishing, and application exploits.

By combining security functionality with SDN capabilities, SRX Series firewalls let organizations of all sizes take advantage of software-defined wired and wireless LAN (SD-LAN), as well as software-defined WAN (SD-WAN) easily and securely. With Juniper, you can deploy agile, adaptable LAN and WAN fabrics across your entire organization, no matter your network's scale.

Juniper is known throughout the industry for meeting the needs of customers who require the largest and most resilient networks possible by delivering open, flexible solutions. In addition to the IPS and application signatures developed by Juniper's research teams, IT teams can add custom signatures to SRX Series security services, letting you tailor your solution to solve your specific business needs.

The SRX Series also provides user identity-based controls, allowing organizations to apply security policies to the users or groups operating on their networks through direct integration with a directory service. This, combined with AppSecure and the advanced policy-based routing (APBR) capabilities of the SRX Series Services Gateways, allows organizations to route individual data flows to specific networks, subnets, VLANs, or WAN interconnects based on various criteria.

This feature allows, for instance, split-tunnel WAN architectures. Branch, work-from-home, and temporary sites can route and protect Internet-bound traffic directly through a local Internet connection (or via a public cloud-based Internet hub), alleviating the load on the corporate WAN and/or VPN infrastructure. This reduces latency for Internet-bound data flows, increases performance, and lowers costs.

SRX Series Services Gateways come in a broad range of models. These range from distributed access-optimized all-in-one security and networking appliances to data center-optimized, scalable, high-performance chassis solutions. All SRX Series firewalls support next-generation capabilities, with most functionality supported on the Juniper Networks vSRX Virtual Firewall as well.

NGFW capabilities in the SRX Series platforms, as well as the Juniper Networks vSRX Virtual Firewall, can be centrally managed from a single management platform. Organizations have the option of choosing from an on-premises management solution, or one based in a public cloud.

IT teams can manage security services, perform logging and reporting, and segment management responsibilities through role-based access controls using either Junos Space® Security Director (on premises) or Contrail® Service Orchestration. Centralized management is based on the Junos® operating system, so it shares the same resiliency and massive scalability as Juniper's highly regarded network solutions preferred by the world's largest and most demanding networks. The combination of scalable and centralized management with SRX Series gateways delivers a powerful solution that brings context and clarity to the setting and enforcement of security policies. SRX Series firewalls block modern malware attacks while delivering the industry's highest performance—and while offering the capacity to grow with your business or traffic, from endpoint to edge, and every cloud in between.

Features and Benefits

- Identify data flows by application with AppSecure, and by user via network directory integration
- Manage, secure, and route individual data flows using advanced policy-based routing and SDN across wired, wireless, and WAN networks
- Secure your organization against network-based exploits targeting application vulnerabilities with an IPS that accommodates custom signatures

- Defend your business against malware, viruses, phishing attacks, intrusions, spam, and other threats through advanced security services with antivirus, antispam, and Web and content filtering
- Streamline operations by centrally managing all of your NGFWs from a single, highly scalable management platform, whether on-premises or in a public cloud

Solution Components

AppSecure

AppSecure is a suite of application security capabilities that identifies applications for greater network visibility, policy enforcement, control, and protection. AppSecure detects application behaviors and weaknesses to identify elusive and hard-to-stop application-borne security threats.

Intrusion Prevention System

Juniper's intrusion prevention system (IPS) defends organizations against network-based exploit attacks aimed at application vulnerabilities.

Advanced Security Services

The SRX Series can include comprehensive content security against malware, viruses, phishing attacks, intrusion attempts, spam, and other threats through advanced security services. Get a best-in-class security solution with antivirus, antispam, Web filtering, and content filtering at a great value by easily adding these services to your SRX Series Services Gateways or vSRX Virtual Firewall. Both cloud-based and on-box solutions are available.

User Role-Based Firewall

Juniper offers a range of user role-based firewall control solutions that support dynamic security policies. User role-based firewall capabilities are integrated with the SRX Series gateways for standard NGFW controls. More extensive, scalable, and granular access controls for creating dynamic policies are available by integrating SRX Series firewalls with the Juniper Identity Management Service (JIMS).

Scalable Centralized Management

Both Security Director and Contrail Service Orchestration provide extensive security scale, granular policy control, and policy breadth across an organization's entire network. Both management options help administrators quickly manage all phases of the security policy life cycle for stateful firewall, advanced security services, IPS, AppSecure, user role-based firewall, VPN, and Network Address Translation (NAT).

Control and Protect Your Network

Get more control over the applications and traffic on your network while protecting your business assets against attacks and managing bandwidth usage. With an NGFW, you can add security without adding operational complexity.

SRX Series Services Gateways deliver NGFW protection with application awareness, IPS, and user role-based control options plus best-in-class advanced security services. SRX Series firewalls come in a broad range of models from all-in-one security and networking appliances to highly scalable, high-performance chassis options. All solutions can be centrally managed, and other security services are easily added to existing SRX Series platforms for a cost-effective solution. Visit www.juniper.net/security or contact your Juniper representative for more information on the SRX Series Services Gateways and our NGFW solution.

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

JUNIPER NETWORKS | Engineering Simplicity

Copyright 2020 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, Junos, and other trademarks are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.