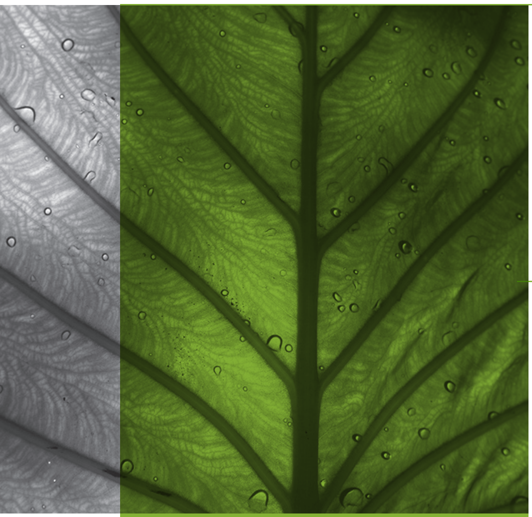

NEXT-GENERATION FIREWALL SERVICES

Product Overview

Juniper Networks delivers a variety of high-performance next-generation firewalls that combine application visibility, user identification, and deep content inspection to provide unparalleled granular control over the security infrastructure.

Product Description

Constant shifts in application use, user behavior, and network infrastructure have created a threat landscape that continues to expose organizations to a wide attack surface. Users are contributing to the problem by demanding access to a growing number of applications that operate across different devices without regard to business security.

A new security paradigm is needed to combat these threats while maintaining user access to new applications on different devices. Juniper Networks® SRX Series Services Gateways deliver integrated next-generation firewall (NGFW) protection services with application awareness, user identity, and content inspection. In addition to NGFW capabilities, the SRX Series devices also offer intrusion prevention, SSL inspection, URL filtering, and unknown threat detection, providing a single security platform that addresses a wide range of security requirements from a common architecture.

Architecture and Key Components

The SRX Series NGFW services architecture includes several key components that provide a powerful platform to protect enterprises from constant cyber attacks.

Application Identification and Control: AppSecure

Modern applications are no longer tied to traditional port-based communications. New applications are designed from the outset to circumvent traditional firewalls by dynamically changing ports and protocols, or by tunneling through commonly used services such as Web traffic. For the user, this means applications can be used from anywhere, at any time. For the enterprise, it means defending against a constantly changing threat landscape that directly targets applications and passes through traditional network-layer protections.

Juniper's NGFW services offer a powerful security platform that is well equipped to meet this challenge. At the core lies AppSecure, which offers robust visibility into and control over applications that run over the network. AppSecure provides a powerful mechanism that instantly recognizes even new applications by using identification techniques that pinpoint the exact identity of applications traversing the network, regardless of port, protocol, or encryption method.

Offering deep application visibility and control, AppSecure provides the context that links application use to a user, regardless of location and device. Furthermore, AppSecure is designed to understand application behaviors and identify vulnerabilities, blocking application-borne security threats before they can do any damage.

Once network traffic is fully classified, the threat footprint can be reduced by granularly defining security policy on an application, content, and user basis. User-centric applications designed primarily for personal communications, such as instant messaging, peer-to-peer file sharing, Webmail, social networking, and IP voice/video collaboration can now be classified as unique applications and granted specific access as sanctioned by the enterprise.

User Identification: UserFirewall

User identity is a core requirement of next-generation firewalls that enables administrators to create security policies that reflect business needs rather than network requirements. This creates a powerful mechanism for defining, managing, and refining security policies by defining firewall rules based on user identity rather than IP address. Through Juniper's UserFirewall feature, an SRX Series device can associate network traffic with a specific user through integration with directory services such as Active Directory. Policies can be defined to allow application use based on users or groups, enabling more powerful but much simpler security controls. Through UserFirewall, security policies can be expressed in terms of groups, allowing security policies to continue functioning as users are added or deleted from groups. In addition, UserFirewall provides visibility into application usage at the user level rather than IP address, providing powerful insights into application traffic traversing the network. Security administrators can reduce the threat footprint by adjusting security policies to align application usage with security and business practices.

Attack Mitigation: Intrusion Prevention System

Juniper's intrusion prevention system (IPS) is tightly integrated with Juniper's NGFWs to mitigate threats and protect against a wide range of attacks and vulnerabilities. Working in conjunction with Juniper Sky™ Advanced Threat Prevention (Sky ATP), IPS provides comprehensive defense against known and unknown threats, protecting against zero-day attacks before they hit the network. The solution constantly monitors for new exploits against recently discovered vulnerabilities, keeping network protection up to date against new cyber attack methods. Network-borne attacks against vulnerabilities on client and server systems are immediately blocked inline before any damage can be done.

Unknown Malware: Juniper Sky ATP

Juniper Sky ATP is a cloud-based service that provides complete advanced malware protection. Integrated with SRX Series firewalls, Juniper Sky ATP delivers a dynamic anti-malware solution that adapts to an ever-changing threat landscape, providing a cloud-based service that dynamically analyzes Web and e-mail files using powerful machine-learning algorithms to quickly identify new and unknown malware. Once a verdict is reached, the decision is sent to the SRX Series NGFW for enforcement. All major file types are supported by Juniper Sky ATP, including Microsoft (.docx, .xls, and .ppt), pdf, and Android Application (APK).

Block Known Threats: Anti-Malware Protection

Malicious activities continue to proliferate from multiple attack vectors, making the enterprise perimeter the first line of defense to block threats before they enter the network. Anti-malware protection combines cloud-based reputation intelligence with the SRX Series NGFW on-box horsepower to deliver lightweight and fast security. The result is a highly effective perimeter defense against a multitude of known threats, which doesn't slow down your users or your business.

Browsing Defense: Malicious URL Filtering

Spear phishing is a popular attack method that often leads to serious breaches within an enterprise. Unsuspecting users click on malicious URLs that install an exploit root-kit that is a precursor to an advanced persistent attack, setting the stage for valuable corporate data to be stolen. Attackers commonly compromise popular websites, tricking users to unintentionally provide their user passwords. Juniper's URL filtering module is constantly updated in real time, providing an up-to-date database of malicious URLs that are constantly being discovered around the world, preventing users from being compromised.

Encrypted Protection: SSL Proxy

SSL has become the universal method for authenticating websites and encrypting traffic between Web clients and Web servers. However, because SSL content is encrypted, users can directly download malware on to their end clients. Since organizations have no visibility into SSL connections, they are blind to any threats that are transmitted over HTTPS into their corporate enterprise.

Juniper offers a powerful application-level SSL proxy that sits between client and server, intercepting encrypted traffic, terminating the session, and re-initiating the connection towards the end destination. It can be used as an SSL "forward" proxy that sits between users on the corporate LAN and their access to the Internet, protecting the end client. It also intercepts HTTPS traffic by acting as a gateway at the enterprise perimeter, where it terminates encrypted traffic before it enters the enterprise. At that point, unencrypted traffic is immediately inspected to determine compliance with security policy, as set by the security team. Traffic is then handled by proactive malware engines that will immediately block malware, thwarting any security breach.

Features and Benefits

Deliverable	Deliverable Description	Benefits
AppSecure	Provides a sophisticated classification engine that accurately identifies applications regardless of port or protocol, including applications known for using evasive techniques to avoid identification.	Provides more granular control by identifying unique applications rather than IP addresses to enforce corporate security policies to match your specific business requirements.
User-Firewall	Integrates with directory services such as Active Directory to create firewall policies that are associated with specific users or groups to enforce security protection.	Enables more accurate and granular security policies through powerful but simplified security controls.
Intrusion Prevention System (IPS)	Offers comprehensive protection against a broad range of known security exploits in applications, databases, and operating systems.	Constantly monitors for new exploits against newly discovered vulnerabilities to ensure that network protection is up-to-date against the latest attack cyber methods.
Juniper Sky ATP	Cloud-based sandbox service that provides sophisticated advanced malware detection through powerful machine learning algorithms to identify previously unseen security threats.	Accurately identifies unknown and never-before-seen malware that eludes conventional methods, ensuring complete protection.
Anti-Malware Filtering	Protects against malware, viruses, phishing attacks, intrusions, spam, and other threats through antivirus, antispam, and Web and content filtering.	Implements real-time security defense that ensures businesses have up-to-date signatures that provide visibility into threats from all over the world.
Junos Space Security Director	Streamlines operations by centrally managing all NGFWs from a single pane of glass.	Simplifies complex security policy management and implementation through easy-to-use GUI, saving time and increasing productivity.

SRX Series Platform Support

Table 2 details the SRX Series platforms that support NGFW services and shows the minimum Junos release required.

Table 2: Next-Generation Firewall Services Support

Platform	Supported Junos Release
SRX300 line	15.1X49-D100 or later
SRX550	15.1X49-D100 or later
SRX1500	15.1X49-D100 or later
SRX4000 line	15.1X49-D100 or later
SRX5000 line	15.1X49-D100 or later
vSRX	15.1X49-D100 or later

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

To order Juniper Networks SRX Series Services Gateways, and to access software licensing information, please visit the How to Buy page on www.juniper.net.

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
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

JUNIPER NETWORKS | Engineering Simplicity