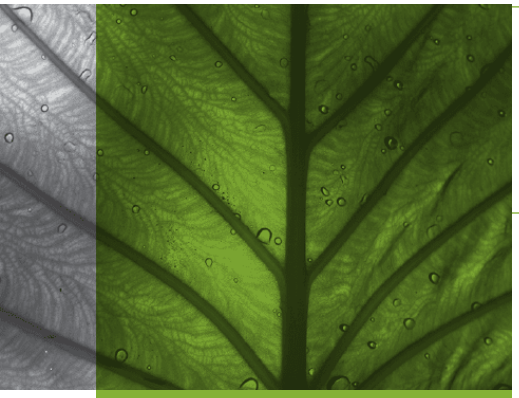

NEXT-GENERATION FIREWALL SERVICES DATASHEET

Product Overview

Juniper Networks delivers multiple high-performance next-generation firewalls that provide granular control and visibility from client to workload. Visibility, intelligence, and enforcement are fundamental pieces of a threat-aware network. Juniper offers additional security to combat known and unknown threats, including application identification, user identification, protection from network and application exploits, malware detection and prevention, Encrypted Traffic Insights, and URL filtering including blocking malicious websites.

Product Description

As distributed workforces become more prevalent, securing the network edge is more critical than ever to ensure users can access the data and applications they need when they need them.

In securing your distributed workforce, cloud-delivered security is not enough. You must start by putting employees first, allowing them to securely access the data and applications they need to do their jobs effectively, and helping you streamline yours. Unbroken visibility from client to workload, security assurance, and a single policy framework are essential tools to help secure your remote workforce.

Access should not increase the organization's risk. Additional security is needed to combat the increasing number of threats organizations face while maintaining user access to new applications on different devices. Juniper Networks® SRX Series Firewalls deliver integrated next-generation firewall (NGFW) protection services with application awareness, user identity, and content inspection for all deployments--physical, virtual, containerized, and as-a-service. In addition to NGFW capabilities, the SRX Series firewalls 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 and MSPs from constant cyberattacks.

User Identification and Access Control: User Firewall

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 flexibility creates a powerful mechanism for defining, managing, and refining security policies by creating firewall rules based on user identity rather than IP address. Through Juniper's User Firewall feature, an SRX can associate network traffic with a specific user by integrating with directory services such as Active Directory. Organizations can define policies to allow application use based on individual users or user groups, enabling more powerful but simpler security controls. Through User Firewall, 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, the User Firewall 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.

Application Identification and Control: AppSecure

The days of tying applications to traditional port-based communications are long gone. Today, new applications are designed to change ports and protocols dynamically. Some are designed to tunnel through services such as HTTP web traffic. This means applications can be used anywhere, at any time the user needs. Empowering users to access applications anywhere poses a challenge in defending against a constantly changing threat landscape that directly targets applications and passes through traditional network-layer protections to protect the enterprise.

Juniper NGFW Services offer a powerful security platform that is well equipped to meet this challenge. At the core lies AppSecure, which offers robust visibility and control over applications on the network.

AppSecure quickly recognizes applications and surfaces the application name, description of the service, and inherent level of risk, 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 understands application behaviors and identifies vulnerabilities, enabling administrators to block risky applications before they can do any damage. AppSecure helps reduce an application's threat footprint by allowing the definition of granular security policies, such as the level of deep packet inspection required and which users or groups are allowed access.

Exploit Protection: Intrusion Detection and Prevention (IDP/IPS)

Juniper's intrusion prevention system (IPS) is tightly integrated with Juniper SRX to mitigate network and application exploits and protect against a wide range of attacks. Juniper intrusion detection system (IDP) constantly monitors for new exploits against recently discovered vulnerabilities, keeping network protection up to date against the latest cyberattacks and stopping them at the exploit stage before they gain a foothold inside the network. IDP signatures can be enabled in detection-only mode or inline to block malicious traffic directly.

Real-Time Protection: SecIntel

SecIntel provides verified threat intelligence to all points of connection across the network to block malicious traffic, enabling a threat-aware network. To help reduce risk, SecIntel can be deployed on the SRX to block malicious traffic originating from malicious IP addresses and domains without the need for deep packet inspection. SecIntel's threat feeds are automated and constantly updated. Additionally, these feeds are scrubbed and verified by Juniper Threat Labs to maintain high detection efficacy and reduce false positives. SecIntel can help reduce the load on the network.

Block Known Threats: Network Anti-Malware

Malicious files, including ransomware and adware, are becoming more prevalent from multiple attack vectors. These threats compromise network endpoints and make them vulnerable to data theft, including credentials and personally identifiable information (PII). Detecting and blocking malware and unwanted files at the network level before making it onto an endpoint is critical to safeguarding users, applications, and infrastructure against attacks. Anti-malware protection combines cloud-based file reputation intelligence and malware signatures with the SRX Series NGFW to deliver lightweight and fast security. Gain a highly effective perimeter defense against known threats without slowing down your users or business. NGFW delivers lightweight and fast security. The result is a highly effective perimeter defense against many known threats, which doesn't slow down your users or business.

Browsing Defense: Enhanced Web Filtering (EWF)

Users spend more than half of their time browsing the Internet and using web-based tools. Web traffic must be both legitimate and safe. At the same time, specific web applications, such as online banking or healthcare, must remain private. EWF allows administrators to block unwanted URL categories, such as gambling and malware sites, and enables selective decryption to keep business traffic safe from threats. In contrast, users' personal traffic can remain private. To reduce attacks, EWF contains more than 180 URL categories that can be used within security policies on the SRX.

Encrypted Protection: SSL Proxy

SSL has become the universal method for authenticating websites and encrypting traffic between Web clients and Web servers.

Since SSL content is encrypted, users can download malware directly onto client endpoints. Since organizations have no visibility into SSL connections, they are blind to any threats transmitted over HTTPS to their corporate enterprise clients. Since organizations have no visibility into SSL connections, they are blind to any threats 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 and terminates encrypted traffic before impacting the organization. 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 instantly block malware, thwarting any security breach.

The SSL Proxy can be configured with exemptions that prevent traffic between certain URLs from being decrypted for user privacy protection. The exemptions can be set based on user groups, URL categories, or custom categories.

Unknown Threats: Juniper Advanced Threat Prevention (ATP)

Juniper Advanced Threat Prevention (ATP) is Juniper's threat intelligence hub and uses machine learning algorithms to provide complete advanced malware detection and prevention. ATP supports threat detection without breaking decryption and surfacing compromised devices. When integrated with SRX Series Firewalls, Juniper ATP leverages a global threat database to deliver threat intelligence, dynamic malware analysis, encrypted traffic insights, and adaptive threat profiling. Juniper ATP is offered as a cloud-based service or as an on-prem appliance.

Juniper ATP protects against trojans, worms, ransomware, botnets, and IoT threats.

Features and Benefits

Feature	Junos OS Version Required	Description	Benefits
Application identification	18.2.R1 or higher	Provides a sophisticated classification engine that identifies applications regardless of port or protocol, including those known for using evasive techniques to avoid identification. Delivers detailed analysis of application volume and usage based on bytes, packets, and sessions throughout the network. Enables tracking of application usage to identify high-risk applications and analyze traffic patterns to improve network management and control.	Gives ops teams more granular control by identifying unique applications rather than IP addresses to enforce corporate security policies to match your specific business requirements. Enables application usage tracking to identify high-risk applications and analyze traffic patterns to improve network management and control. Enhances security policy creation and enforcement based on applications and user roles rather than traditional port and protocol analysis.
AppQoS	18.2R1 or higher for use within Unified Policy	Leverages Juniper's rich QoS capabilities to prioritize applications based on customers' business and bandwidth needs.	Allows users to prioritize traffic and limit and shape bandwidth based on application information and contexts for improved application and overall network performance.
Advanced Policy-Based Routing (APBR)	18.2.R1 or higher	Classifies sessions based on applications and applies the configured rules to reroute the traffic.	Provides the ability to route traffic over different WAN links and assign higher priority to business-critical applications.
User Firewall	18.2.R1 or higher	Integrates with directory services such as Active Directory to create firewall policies associated with specific users or groups to enforce security protection.	Enables more accurate and granular security policies through powerful but simplified security controls.
SSL Proxy	18.2.R1 or higher	Sits between client and server, intercepting encrypted traffic, terminating the session, and re-initiating the connection towards the end destination, and can be used as an SSL "forward" proxy to protect the end client.	Prevents users from directly downloading malware hidden within encrypted traffic on their end clients.
Intrusion Detection System/ Intrusion Prevention System (IDS/IPS)	18.2.R1 or higher	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 Advanced Threat Prevention	18.2.R1 or higher	Provides cloud-based service that performs 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.
SecIntel	18.2.R1 or higher	Generates threat feeds that include attacker IPs, C&C, GeoIP, infected hosts, and dynamic address groups.	Reduces risk by enabling Juniper switches, routers, and firewalls to identify and block potential threats.

Feature	Junos OS Version Required	Description	Benefits
Encrypted Traffic Insights	20.2R1 or higher	Enables SRX Series Firewalls to collect relevant SSL/TLS connection data, including certificates used, cipher suites negotiated, and connection behavior. This information is processed by Juniper ATP, which uses network behavioral analysis and machine learning to determine whether the connection is benign or malicious. Policies on SRX Series Firewalls can be used to block encrypted traffic identified as malicious.	Restores visibility that was lost due to encryption without the heavy burden of full TLS/SSL decryption.
Adaptive Threat Profiling	20.2R1 or higher	Allows organizations to leverage their existing infrastructure to create security intelligence feeds based on real-time events occurring on their network. These feeds, unique to each organization, can be configured based on security policies and utilized by other enforcement points on the network to detect threats and update their infrastructure in real-time, blocking potential attacks.	Improves threat response times by taking real-time threat information and pushing it out to all points across the network.
Anti-Malware	18.2.R1 or higher (cloud-based) 18.2.R1 or higher (on- box)	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.
URL Filtering	15.1X49-D40 or higher	Provides web traffic categorizations that can be incorporated into application.	Prevents web-borne threats and unwanted browsing activity.
Security Director	15.1X49-D60 or higher	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.

Security Director

Juniper Networks® Security Director enables organizations to manage security anywhere and everywhere, on-premises and in the cloud, with unified policy management that follows users, devices, and applications wherever they go. Policies can be created once and applied everywhere. Use Security Director for network-wide visibility and policy management for deployments on-premises, in the cloud, and as a service.

Easily manage and deploy security policies from a single UI across all environments. It provides detailed visibility into application performance and reduces risk while enabling users to move quickly from "knowing" something is wrong to "doing" something to fix the problem.

Providing extensive scale, granular policy control, and policy breadth across the network, Security Director helps administrators manage all phases of the security policy lifecycle. Whether those security policies are delivered by physical, virtual, or containerized firewalls – or as a service – they are managed from a single management platform using a single policy framework that ensures a seamless and secure Zero Trust network.

Juniper Secure Edge

For as-a-Service deployments, Juniper® Secure Edge provides Firewall as a Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Data Loss Prevention (DLP) in a single-stack software architecture managed by Juniper Security Director Cloud. Juniper helps empower organizations to secure their workforce wherever they are. Users have fast, reliable, and secure access to the applications and resources they need, ensuring great user experiences. IT security teams gain seamless visibility across the entire network while leveraging their existing investments, helping them transition to a cloud-delivered architecture at the best pace for the business.

Juniper Secure Edge helps organizations provide consistent security policies that follow the user, device and application without copying or recreating rule sets. This makes it easy for organizations to deploy cloud-delivered application control, intrusion prevention, content and Web filtering, and effective threat prevention without breaking visibility or security enforcement.

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 https://www.juniper.net/us/en/products.html.

Ordering Information

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

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

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: +31.207.125.700

Juniper Networks | Driven by Experience™