

# APPSECURE FOR SRX SERIES SERVICES GATEWAYS

## Product Overview

AppSecure is a suite of next-generation security capabilities for Juniper Networks SRX Series Services Gateways that utilize advanced application identification and classification to deliver greater visibility, enforcement, control, and protection over the network.

Working in conjunction with the other security services of the SRX Series, AppSecure provides a deep understanding of application behaviors and weaknesses to prevent application borne threats that are difficult to detect and stop.

As an integrated service on the world's fastest services gateways, AppSecure provides the scalability to meet the requirements of the most demanding environments.

## AppSecure Description

As network infrastructure and the threats targeting that infrastructure continue to evolve, so too must the network security solutions adopted to protect organizations. At the same time, the latest generation of web-based applications and the proliferation of mobile devices provide an increasingly challenging task for network administrators to effectively manage traffic flows and access to data while delivering the right mix of security and network services. In the past, network administrators would simply buy a new appliance to overcome a security or network issue. However, that approach leads to greater network complexity, excessive management overhead, and poor overall performance.

Today's network security solutions must not only have the right architecture to deliver the appropriate mix of performance and scale in this evolving network environment, but must also deliver the right security services to give administrators visibility and control over the types of applications now traversing their networks. Juniper Networks® AppSecure is a suite of application-aware security services for the Juniper Networks SRX Series Services Gateways that classify traffic flows, bringing greater visibility, enforcement, control, and protection to network security. AppSecure uses a sophisticated classification engine to accurately identify applications regardless of port or protocol, including nested applications that reside within trusted network services.

The result is a powerful tool that helps bring context and clarity to the setting and enforcement of security policies, provides protection against common evasion techniques, and helps stop modern malware attacks, all while delivering the industry's highest performance and scale. AppSecure gives security administrators the context to regain control of their network traffic, set and enforce policies based on accurate information, and deliver the performance and scale required to address business needs. The services that are enabled by AppSecure include: AppTrack for detailed visibility of application traffic; AppFW for granular policy enforcement of application traffic; AppQoS to prioritize and meter application traffic; and AppDoS for greater control over the latest breed of botnet attacks targeting applications. AppSecure also works with the SRX Series' integrated intrusion prevention system (IPS) solution to deliver deeper protection against zero-day attacks.

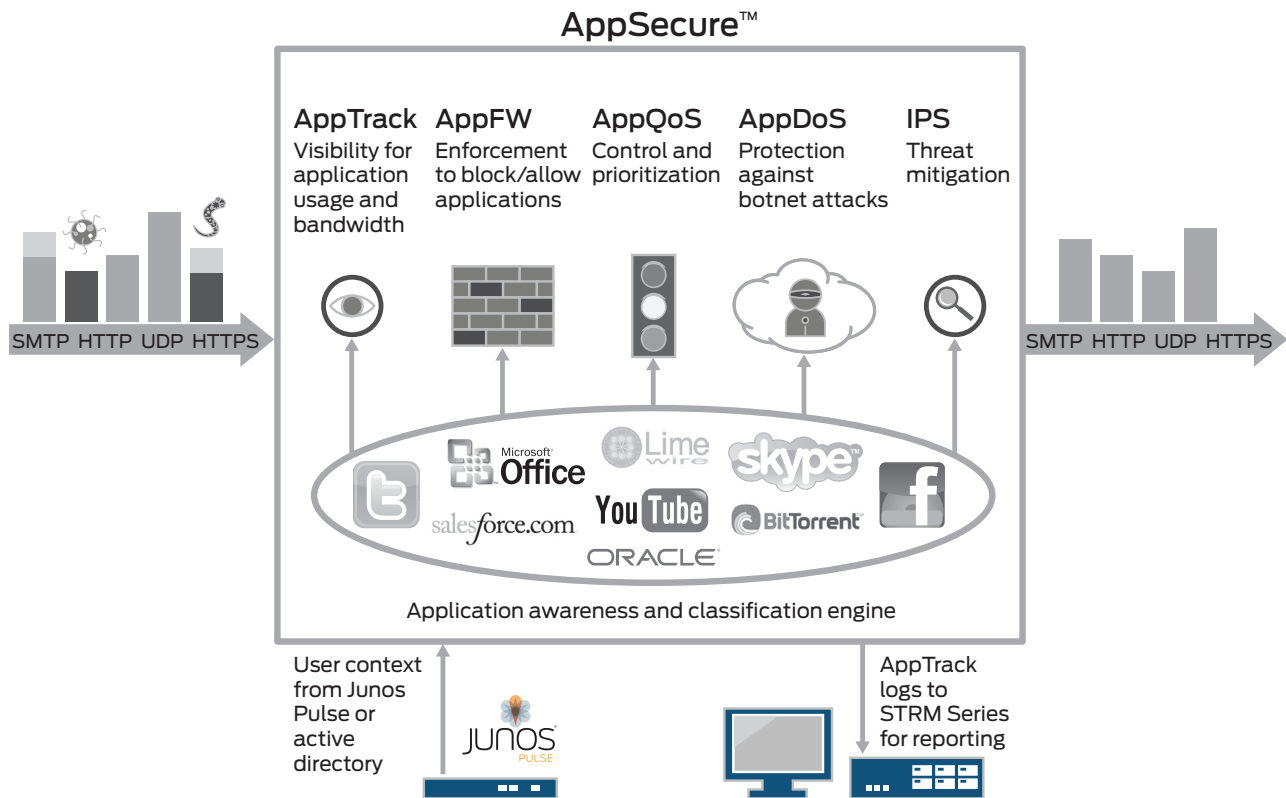


Figure 1: The application awareness and classification engine improves efficiency by inspecting network traffic and publishing the results for use by all of the AppSecure services.

### AppSecure Features and Benefits

Feature	Feature Description	Benefit
Application awareness and classification	Context, protocol information, and signatures used to identify applications on any TCP or UDP port.	Enables all AppSecure capabilities by exposing application information to advanced, next-generation security services for increased visibility, control and protection.
Nested application support	Accurate identification of applications running on top of, or embedded into approved/trusted services and protocols.	Provides enhanced protection against modern evasion techniques that utilize trusted services.
User-role based policies	Fine-grained policies, including application security, based on user role and identity for all endpoints including mobile devices.	Superior protection and easier policy management as user and user groups reduce the number of policies and rules needed to account for other elements such as location, device, and IP address.
SSL inspection	Inspection of HTTP traffic encrypted in SSL on any TCP/UDP port.	Combined with AppSecure, provides visibility and protection against threats embedded in SSL encrypted traffic.
Purpose built platform	Built from the ground up on dedicated hardware.	Delivers unrivaled performance and flexibility to protect service provider, enterprise and data center environments.
Junos® OS service integration on SRX Series	Rich set of native network and security services including: firewall, AppSecure, IPS, IPsec VPN, NAT, QoS, routing, and switching.	Provides consolidation and optimization of application-aware security services for maximum scale.

## Application Visibility with AppTrack

AppTrack collects byte, packet, session, and time statistics while accurately identifying hundreds of applications, giving network administrators detailed analysis of application data. AppTrack quickly and easily provides visibility into the types of applications traversing through the SRX Series gateway and allows classification based on risk level, users, groups, zones, source, and destination addresses, as well as volumes. This information can be used to assess adherence to usage policies, help address bandwidth management, or simply report on the most active users and applications. Juniper's centralized logging and reporting system, STRM Series Security Threat Response Managers, provides a flexible and extensible way to analyze data from a centralized location and take action. Using a variety of pre-defined report formats, STRM Series can generate reports based on AppTrack application log data.

## Application Enforcement with AppFW

AppFW enables administrators to create fine grained application control policies to allow or deny traffic based on dynamic application name or group names rather than static IP/port information. It is designed to simplify security policies by using application white lists and black lists, as well as to define what actions to perform on matched traffic while taking default action against all other traffic.

## Application Control with AppQoS<sup>1</sup>

With the increased use of web-based customer relationship management (CRM), enterprise resource planning (ERP), and other business tools, network administrators need a way to

prioritize business critical traffic over the network. AppQoS provides the ability to meter and mark traffic based on the application policies set by the administrator. These policies enable lower priority Web traffic to continue when network bandwidth allows, but ensures that mission critical traffic is delivered when usage levels surge.

## Application Protection with AppDoS

AppDoS identifies attacking botnet traffic and legitimate client traffic based on application-layer metrics and remediates these botnet attacks. Employing a multi-stage approach that includes server connection monitoring, deep protocol analysis, and bot-client classification, AppDoS delivers the ability to detect subtle changes in traffic patterns and client behaviors that could indicate an application-level denial-of-service (DoS) attack. Once suspicious activity is detected, AppDoS can then issue an alert, block offending IP addresses, or completely drop irregular sessions and packets. AppDoS is typically deployed with the SRX Series' integrated IPS service to increase protection against malicious attacks.

## Application Protection with IPS

IPS tightly integrates Juniper's latest and most advanced security features with the network infrastructure for threat mitigation and protection from a wide range of attacks and vulnerabilities. IPS subscribes to the results of application identification/contextualization. These results help determine the appropriate protocol decoding and attack objects to use for the permitted incoming traffic that will be processed by the IPS software services module.

## Specifications - Branch SRX Series Services Gateways

	SRX100/ SRX110 Services Gateway	SRX210 Services Gateway	SRX220 Services Gateway	SRX240 Services Gateway	SRX550 Services Gateway	SRX650 Services Gateway
Maximum AppSecure throughput <sup>2</sup>	90 Mbps	250 Mbps	300 Mbps	750 Mbps	1.5 Gbps	1.9 Gbps
Application identification	>900 applications	>900 applications	>900 applications	>900 applications	>900 applications	>900 applications
Maximum IPS throughput	75 Mbps	65 Mbps	80 Mbps	230 Mbps	800 Mbps	1 Gbps
Maximum connections per second	1,500	1,500	1,800	7,400	27,000	35,000
Maximum sessions	12,000	24,000	32,000	48,000	375,000	512,000

## Specifications - Data Center SRX Series Services Gateways

	SRX1400 Services Gateway	SRX3400 Services Gateway	SRX3600 Services Gateway	SRX5600 Services Gateway	SRX5800 Services Gateway
Maximum AppSecure throughput <sup>2</sup>	4 Gbps	16 Gbps	25 Gbps	50 Gbps	100 Gbps
Application identification	>900 applications	>900 applications	>900 applications	>900 applications	>900 applications
AppDoS protocols	>60 protocols + 600 contexts	>60 protocols + 600 contexts	>60 protocols + 600 contexts	>60 protocols + 600 contexts	>60 protocols + 600 contexts
Maximum IPS throughput	2 Gbps	6 Gbps	10 Gbps	15 Gbps	30 Gbps
Maximum connections per second	40,000	180,000	180,000/300,000 <sup>3</sup>	380,000	380,000
Maximum sessions	0.5 million	2.25 million/ 3 million <sup>3</sup>	2.25 million/ 6 million <sup>3</sup>	9 million	12.5/20 million <sup>4</sup>
SSL inspection	Yes	Yes	Yes	Yes	Yes

<sup>1</sup>AppQoS is currently supported on SRX Series Services Gateways for the data center. AppQoS support on SRX Series Services Gateways for the branch forthcoming in the near future.

<sup>2</sup>Throughput numbers based on HTTP traffic with 44 kilobyte transaction size.

<sup>3</sup>Additional Extreme License required for 3 million and 6 million sessions.

<sup>4</sup>To achieve more than 12.5M CP sessions on SRX5800, use software knob available from 10.4 or 11.4 and 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](http://www.juniper.net/us/en/products-services).

## Ordering Information

Model Number	Description
<b>AppSecure Subscription</b>	
SRX1XX-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX100 and SRX110
SRX210-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX210
SRX220-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX220
SRX240-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX240
SRX550-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX550
SRX650-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX650
SRX1400-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX1400
SRX3400-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX3400
SRX3600-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX3600
SRX5600-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX5600
SRX5800-APPSEC-A-1	1-year subscription for AppSecure and IPS updates for SRX5800
SRX1XX-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX100 and SRX110
SRX210-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX210
SRX220-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX220
SRX240-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX240
SRX550-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX550

Model Number	Description
SRX650-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX650
SRX1400-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX1400
SRX3400-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX3400
SRX3600-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX3600
SRX5600-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX5600
SRX5800-APPSEC-A-3	3-year subscription for AppSecure and IPS updates for SRX5800
SRX1XX-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX100 and SRX110
SRX210-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX210
SRX220-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX220
SRX240-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX240
SRX550-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX550
SRX650-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX650
SRX1400-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX1400
SRX3400-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX3400
SRX3600-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX3600
SRX5600-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX5600
SRX5800-APPSEC-A-5	5-year subscription for AppSecure and IPS updates for SRX5800

## About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at [www.juniper.net](http://www.juniper.net).

### 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  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

Juniper Networks (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 Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2012 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property 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.