Spotlight Secure

Product Overview

Spotlight Secure is a highly open and scalable threat intelligence platform that aggregates threat feeds from multiple sources to deliver open, consolidated, actionable intelligence to SRX Series Services Gateways (firewalls) across the organization. These sources include Juniper threat feeds, third-party threat feeds, and threat detection technologies that the customer can deploy. Administrators can define enforcement policies from all feeds easily from a single management interface, Junos Space Security Director.

Your ideas. Connected.™

Product Description

Juniper Networks® Spotlight Secure threat intelligence platform aggregates threat feeds from multiple sources to deliver open, consolidated, actionable intelligence to Juniper Networks SRX Series Services Gateways (firewalls) across the organization. These sources include Juniper threat feeds from our own (Spotlight Secure) cloud-based service, third-party threat feeds, and threat detection technologies that the customer can deploy. Administrators are able to define enforcement policies from all feeds via, Juniper Networks Junos® Space Security Director, a centralized management point for the SRX Series.

Customers can utilize the advanced protection available using Juniper Spotlight Secure threat intelligence platform for a variety of use cases, including protection from advanced malware (related to Command and Control botnet activity) at an enterprise edge central HQ and/or remote locations, Web application protection for critical business applications in the data center and to enforce policies for monitoring and controlling traffic from specific countries. In addition, customers can integrate custom or third-party feeds, and other advanced protection technologies into Spotlight Secure for protection against threats specific to their industry or vertical. Financial and government verticals often have specific feeds that they need to use for compliance and security needs, and being able to use an open threat intelligence platform to use such feed data for policy enforcement can be highly beneficial.

Features and Benefits

As the threat landscape continues to accelerate and evolve, the security industry continues to respond with a variety of disparate new detection technologies. Unfortunately, this approach results in customers struggling to manage a patchwork of uncoordinated security tools, leaving a gap between detection and enforcement at the firewall. Many next-generation firewalls (NGFWs) include integrated capabilities, such as intrusion prevention system (IPS), antivirus signatures, and proprietary reputation feeds, but they are closed systems that are not capable of taking full advantage of the highly diverse third-party and custom feeds utilized by customers.

Protecting enterprise edge, traditional, and cloud data centers from advanced malware and other threats requires a new way of thinking about network defenses. Companies must focus on detecting attacks and attackers early on (rather than at the point of breach) and ensuring better integration of intelligence across security architectures (in contrast to point products without information sharing). The majority of security products on the market today attempt to detect a specific exploit at the instant that attack is launched. Regrettably, this only works against known attacks, where there is only a single opportunity to detect and stop the threat. Customers could benefit from being able to leverage data feed sources that have been optimized and can be easily used for policy enforcement quickly, before their network and subsequently critical data are compromised. For example, to effectively secure business- critical IT data centers, companies must have knowledge of the attacking devices—not just the IP address—and be able to disseminate that intelligence

quickly to all data center access control points by leveraging the firewall as an enforcement point.

With Spotlight Secure working in conjunction with SRX Series firewalls for policy enforcement at the perimeter, and optionally Juniper Networks WebApp Secure for local Web application attack detection, Juniper helps companies track and stop attackers early on, before they can do any harm.

SRX Series firewalls can easily consume threat intelligence from Spotlight Secure, a highly open and scalable platform. Spotlight Secure allows you to bring together diverse threat intelligence and detection capable of providing timely, actionable enforcement on the firewall. In terms of device scale, Spotlight Secure can push security intelligence to thousands of firewalls simultaneously via Junos Space Security Director. In terms of capacity, it allows over one million data feed entries to be utilized for policy enforcement by a single high-end SRX Series firewall (Juniper Networks SRX1400 Services Gateway and later versions). These entries can be related to Juniper sourced feeds, custom feeds, or a combination of both. The security administrator can manage the large number of feeds conveniently with a single point of management, Junos Space Security Director. Plus, Spotlight Secure enables comprehensive enforcement by the SRX Series firewall to stop the broadest spectrum of threats.

Spotlight Secure enables SRX Series firewalls to provide highly effective protection. With the platform, you can use and enforce the most effective technologies available provided by Juniper and other industry leaders, including feeds customized to your industry or organization. By providing real-time integration between threat feeds and the firewall, only the latest and most relevant intelligence is sent to firewalls, which reduces the need for manual transfer of new threat information to firewall enforcement, ensuring fast time to enforcement and low false positive rates with the latest intelligence. Threat severity ratings for each data feed entry allow security administrators to write policy based on ratings and to fine-tune solutions for their own deployments in order to reduce false positives and increase efficacy. Regular updates to Juniper threat feeds (via the cloud) ensure that feed data is current and help enforce policies on the SRX Series firewall based on only the latest threats, while maximizing firewall device resources.

Through Spotlight Secure, Juniper offers customers a wide breadth of options with regard to data feeds, enabling highly customizable protection.

- **Command and Control (C&C), anti-botnet threat feeds**—Malware is identified that is communicating with C&C servers, and botnets are stopped via the SRX Series firewall.
- **GeoIP feeds—**Mapped IP addresses to geographic region data are incorporated into the SRX Series firewall policy for monitoring/blocking traffic from/to specific locations in accordance with business policy.
- **Attacker device fingerprints**—Known attacker device information is utilized for monitoring/blocking traffic using either the SRX Series firewall or WebApp Secure. Specific features that go beyond IP address fingerprinting and offer companies protection from hackers who have already visited their websites include the following:
  - Attacker devices identified based on intrusion deception (through WebApp Secure) and policy enforcement via SRX Series firewall
  - Device-level tracking for definitive attacker identification with almost no false positives
  - Tracking of hundreds of identifying attributes, including browser version, browser add-on, IP address, time zone, and fonts
  - Identification rate of 99 percent
  - Device fingerprinting that overcomes use of proxy servers to identify and track the attacker's device, no matter which IP address the attacker is using to evade detection
  - Flexible counterresponses at both the application layer and network firewall
  - Continuous tracking of attackers, even if they shift proxies
  - Ability to direct counterresponses at a single offending device, so that legitimate customers who might be behind a shared IP address remain unaffected
  - Assignment of permanent aliases for attackers
  - Ability to direct counterresponses at a single offending device, so that legitimate customers who might be behind a shared IP address remain unaffected

Customers can also choose to use their own (custom/proprietary) or third-party feeds by building and applying custom whitelists, blacklists, or both and sharing them with Junos Space Security Director, which then shares the data with SRX Series firewalls for policy enforcement.

Spotlight Secure enables enterprises to achieve operational efficiency as they apply and manage security across the SRX Series firewall estate. First, with Spotlight Secure's simplified enforcement model, organizations can dramatically reduce administrative overhead. Integration between Junos Space Security Director and Spotlight Secure links cloud-based threat feeds to customer firewalls and provides a single aggregation point for multiple feeds into the firewall. Also, firewall policies, threat intelligence feeds, and reporting on enforcement and actions are all available in a single-pane view with Security Director. Furthermore, the latest aggregated threat intelligence can automatically syndicate across the entire firewall estate, with no need to update or commit firewall policy changes.

With Spotlight Secure, enterprises benefit from a security intelligence solution tightly integrated with the SRX Series firewall that helps them ensure the security of their sensitive and mission-critical data proactively, effectively, and with minimal operational overhead.

Architecture and Key Components

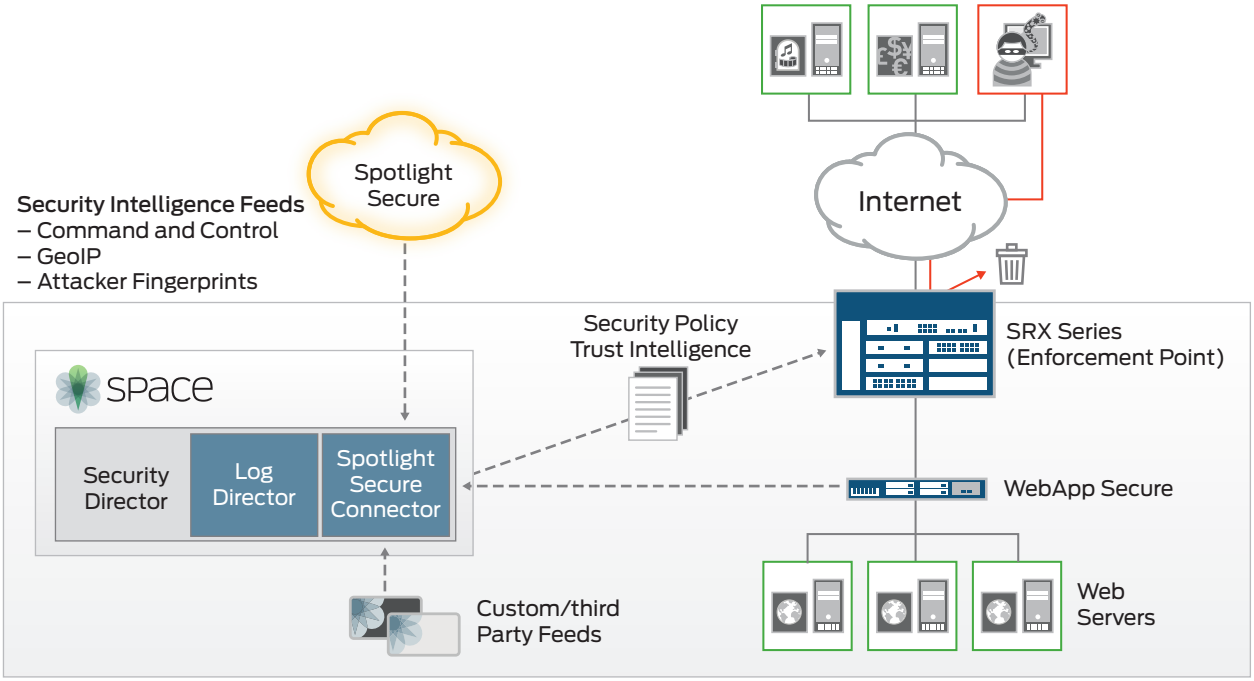

Figure 1: Linking security intelligence to policy enforcement by SRX Series (and optionally WebApp Secure) for rapid protection against advanced threats

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

What to Buy

To use security intelligence based on the Spotlight Secure threat intelligence platform for your SRX Series Services Gateways, you need to purchase, at a minimum, the following:

- Juniper Networks SRX550 Services Gateway or later model—This is for policy enforcement based on threat intelligence feeds.
- Juniper Networks Junos Space Network Management Platform—This product centrally aggregates threat intelligence before sharing with the policy enforcement point(s).
- Junos Space Security Director—This product centrally manages SRX Series firewall policies.
- Security Intelligence (SecIntel) Service software—This service applies threat intelligence to the firewall policy and adheres to the Juniper Software Advantage pricing model, which is a trust-based, no-enforcement model. The service license is sold as a subscription (fixed term) with the option to purchase for usage for 1, 3, or 5 years at a time. This subscription software license includes Juniper Care Software Advantage, entitling you to software updates and upgrades, 24x7 remote technical support, and online support.

You can optionally purchase these:

- Juniper threat feeds
- Command and Control (C&C), anti-bot—This is for policy enforcement based on known malicious IPs/URLs/domains tied to C&C source/botnet. The software adheres to the Juniper Software Advantage pricing model, as described previously under Security Intelligence (SecIntel) Service software.
- Web attacker fingerprints (global)—This software is for policy enforcement based on known malicious attacker devices and adheres to the Juniper Software Advantage pricing model.
- GeoIP—This software is for policy enforcement based on country-to-IP mapping information and adheres to the Juniper Software Advantage pricing model.
- WebApp Secure—This software or hardware appliance uses (local or global) attacker fingerprint data for policy enforcement either locally using WebApp Secure or at the network perimeter using SRX Series Services Gateways,

Juniper Networks products are sold directly as well as through Juniper partners and resellers. For more information on the Juniper Software Advantage business model, please visit www.juniper.net/us/en/products-services/security/.

For information on how to buy, please visit www.juniper.net/us/en/how-to-buy.

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.

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

1000427-003-EN Oct 2014