Protecting Traditional and Cloud Data Centers with Security Intelligence

Improve security efficacy through dynamic intelligence

Challenge

Increasingly sophisticated threats can bring down clouds, interrupt data center operations, and lead to theft of critical data. Although a multitude of security intelligence feeds provides visibility into real-time threats, turning that data into actionable intelligence that executes through firewall policies simply has been too difficult.

Solution

SRX Series Services Gateways offer adaptive security intelligence services that help you optimize security policies and thwart cyber attacks. These firewalls help ensure that your security posture is calibrated for the threats actively working against you.

Benefits

- Attain effective threat intelligence that delivers timely protection against the latest threats
- Easily apply a variety of threat intelligence feeds for flexibility and highly customized firewall policies
- Reduce operational burden by dynamically incorporating security intelligence into firewall policy
- Maintain high performance, scalable data center protection with intelligent service chaining

Securing your data centers, edge, and cloud environments is an ongoing challenge. Your adversaries—cyber criminals, nation state attackers, hacktivists—continue to develop sophisticated, invasive techniques, resulting in a continually evolving threat landscape. Traditional firewalls focused on layer 3 and 4 inspection are not sufficient in today's threat environment. Next-gen firewalls are powerful, yet not designed to protect from the velocity and variety of new attacks. In today's world, your firewall must be able to take immediate action based on known or emerging intelligence. It must identify attacks accurately and act quickly.

With the shift to cloud architectures, traditional firewall administration becomes burdensome and fraught with human error due to the sheer complexity of distributed security. What's needed is a firewall that can adapt to emerging threats in near real time, in an automated and dynamic way.

The Challenge

As you build and manage a traditional or cloud data center, security is a fundamental element. Balancing the need for users to access applications with the need to protect your digital assets is no easy task. Consider some of the follow challenges:

- **Proprietary and Inflexible Security Platforms**—While some firewall solutions leverage cloud-based threat intelligence[1], the data involved is often proprietary, preconfigured on the firewall, and inflexible, not allowing you to select nor exert any control over the information provided.
- **Security Inefficacy**—The market is saturated with sources claiming to offer threat intelligence, though most of the available data feeds are not immediately actionable. Your firewall, therefore, is unable to use those data feeds directly within policy, providing less than optimal protection.
- **Static Address Groups**—Administrators typically rely on static address lists to apply inspection or blocking and must manually update the firewall policy every time any of these lists change. This is cumbersome and difficult to maintain.
- **Firewall Performance**—Firewall services, such as IPS and application inspection, tend to lead to dramatic performance reductions. In particular, intelligence data feed entries can quickly add up to the thousands (if not more) on a single firewall device, causing performance issues that can lead to unnecessary upgrades. And, your firewall may not be utilizing threat intelligence in a way that maximizes the firewall's resources.
- **Decentralized Policy Management**—As the number of firewalls increase across your network and you need consistent policies across the firewall estate, a reliable, centralized web-based management solution is critical.

[1] In this paper, we consider "threat intelligence" to be interchangeable with "security intelligence," except when referring to GeoIP (refers to address group).

The Juniper Networks SRX Series Firewall with Security Intelligence

Juniper offers a complete portfolio of scalable security solutions that protect customers from the most serious threats, based on the Juniper SRX Series Services Gateways. The SRX series provides a foundation that allows enterprise and service providers to implement a wide array of services, including UTM services, next-gen firewall services, and dynamic intelligence services.

These dynamic intelligence services allow multiple intelligence feeds—whether raw or curated—to be aggregated, normalized, analyzed, and dynamically distributed to security policies which execute at the firewall enforcement point. These services are enabled by an open, scalable framework integral to the SRX environment. This open framework is design with the assumption that threats will continue to grow, intelligence feeds will evolve, and security administrators will want to leverage big data in the quest to maintain a solid security posture.

Juniper SRX with Security Intelligence solution: a three-phased approach

1. **Security intelligence data is shared with Spotlight Secure Connector.**
   a. Spotlight Secure collects, optimizes, and sends up-to-date intelligence data feeds to Spotlight Secure Connector. Currently, the following feeds are offered: command and control (C&C) and GeoIP address feeds.
   b. Local intelligence data (customer-provided or third-party feeds) is sent to Spotlight Secure Connector.
2. **Spotlight Secure Connector dynamically aggregates security intelligence, ensuring that only the most up-to-date data is distributed to SRX Series gateways.** By aggregating threat intelligence on premises, you can obtain intelligence from a variety of sources, including Spotlight Secure, your own local feeds, and even third-party feeds. All of this data is then made available for policy enforcement on the SRX Series devices. This is unlike other offerings in the market where the burden falls on the firewall itself to reach out to a cloud service for data feeds, as well as on the firewall administrator who must manage the configuration of each firewall consuming security intelligence. Furthermore, Junos Space Security Director and Log Director centrally manage threat intelligence policies and provide security event logging for SRX Series devices.
3. **SRX Series gateways utilize security intelligence as part of security policy.** The SRX Series can enforce policies using the data feeds for specific use cases, such as stopping compromised systems from reaching out to C&C servers. Significant operational efficiency and rapid protection comes from the fact that SRX Series will act on address groups that are dynamically updated using custom feeds provided by either the administrator or GeoIP data from Spotlight Secure. Each dynamic address group is updated dynamically—it does not require any commit or configuration change, so that you can change the addresses used to apply security policies on the SRX Series without requiring a maintenance window.

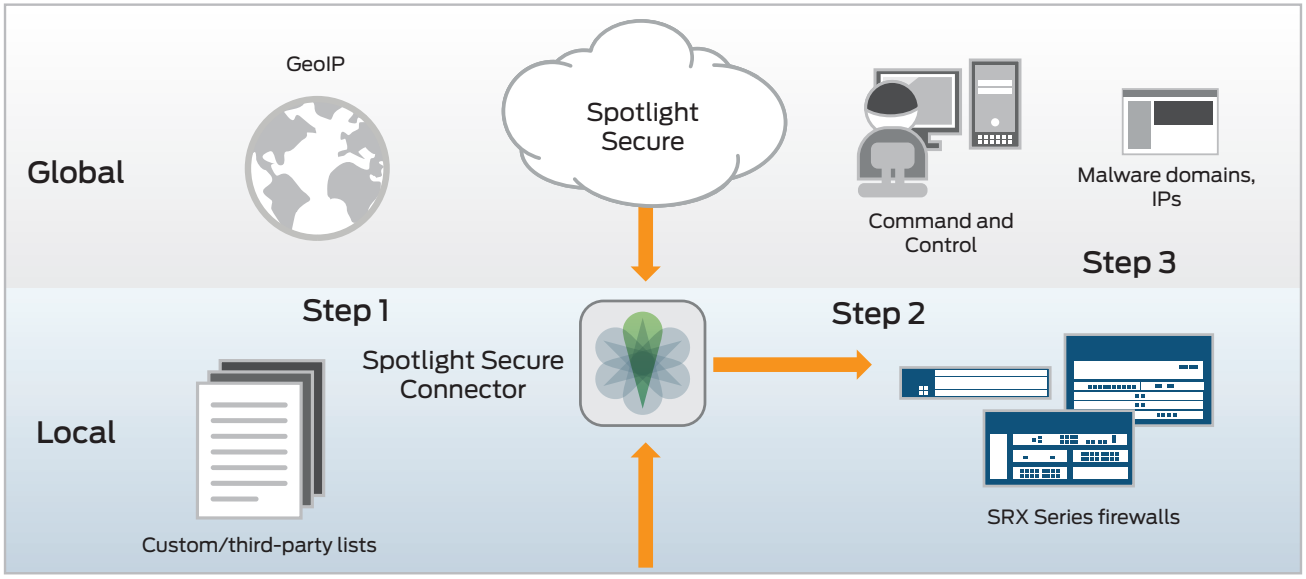

Figure 1: SRX Series with security intelligence based on integration with Spotlight Secure and Spotlight Secure Connector

Juniper Solution Features and Benefits

Juniper Security Intelligence Solution Feature	Description	Benefit
Scalable and open security intelligence framework	• On-premises aggregation and control of threat intelligence. • Extensible framework for adding new threat intelligence feeds, including custom feeds and other types of data for increased protection against new threats. • Customer control over data feed refresh rates. • Future-proof design to "plug in" new technologies.	• Adapts to your needs and custom use case scenarios to deliver added security and added operational flexibility • Allows you to easily and flexibly apply data feeds for more tailored policies
Actionable security intelligence that can be dynamically incorporated into SRX Series firewall policy	• Threat intelligence feeds which are readily usable by SRX Series appliances because threat intelligence data is aggregated. • More reliable compared to other solutions in the market due to reduced false positives. • Actionable due to threat severity scores. • Optimized for use within SRX Series firewall devices.	• Eliminates the need for customers to manually aggregate and clean up threat intelligence before it is available for enforcement • Enables effective and timely protection against newest threats, in support of your unique needs and network environment
Dynamically updated address groups	• No reliance on static address lists to apply inspection or blocking. • SRX Series will act on address groups that are dynamically updated using custom feeds provided by the administrator or GeoIP data made available through Spotlight Secure.	• Reduces operational burden for security administrator • Increases operational efficiency
Optimized implementation that maximizes resources and delivers real customer value	• SRX Series can support a very high volume of data feed entries (up to 1 million data feed entries on a single firewall). • Customers can prioritize threats to maximize firewall resources with the help of Spotlight Secure Connector.	• Enables performance needed for modern threat protection
Flexible centralized policy configuration and management of firewall policies	• Juniper firewall, IPsec VPN, IPS, UTM, NAT and security intelligence policies can easily be managed centrally through Junos Space Security Director.	• Allows support and management of large-scale deployments • Enables consistent policies across all SRX Series firewalls

Effective Security Is Key to the Cloud and Data Center

To help you keep up with new threats, Juniper adds important continuous value to the distributed threat intelligence feeds. In particular, the Juniper threat feed has the following characteristics:

- Highly focused on Command and Control (C&C) traffic related to malware and botnets, and includes threat intelligence in the form of IP addresses, domains, and URLs
- Based on a compilation of multiple third-party data sources plus original intelligence from Juniper's own malware research team
- Spotlight Secure refreshed hourly to ensure it is current and blocking only the latest threats
- Includes a threat severity rating for each feed entry, so you can write policy based on threat severity to fine-tune the solution for your own deployments in order to reduce false positives and increase efficacy

Our integrated solution enables each SRX Series device, based on available memory and resources, to determine how much data it can consume. The most active and dangerous threats are prioritized by Spotlight Secure Connector, thus ensuring maximum utility of the firewall's resources, which results in the best threat coverage possible.

Solution Components

SRX Series Services Gateways: Juniper firewalls that enforce firewall, IPsec VPN, IPS, AppSecure, UTM, NAT, and threat intelligence policies based on Spotlight Secure sourced (e.g., C&C, GeoIP) and/or Spotlight Secure Connector (e.g., customer or third-party) feeds. Most importantly, these features work in conjunction with each other, allowing you to select the security services important for your business needs and apply them as part of a layered security approach.

Junos Space Security Director: Centralized management platform from which to manage SRX Series policies.

Note: You must deploy the Junos Space Network Management Platform to use Security Director for security policy management.

Juniper Spotlight Secure: To keep up with the ever-changing threat landscape, dynamic security intelligence is imperative. Currently, through the Spotlight Secure cloud-based intelligence service and related threat intelligence system, Juniper supports a set of threat intelligence feeds to protect against a variety of threats:

- Command and control (C&C) feeds—to protect network from botnets
- GeoIP data (a set of IP addresses pertinent to a geographic location)—to limit/not send traffic to specific locations for business reasons

- Custom threat data feeds (customer or third-party sourced)—to protect against specific threats important to the customer/use case scenario; e.g., a list of IPs/URLs may be used as part of the SRX Series firewall policy in the form of a blacklist/whitelist

Dynamic address groups: List of IPs that can be used as either "source" or "destination" objects in an SRX Series rule. Dynamic address group is updated dynamically—it does not require any commit or configuration change, so that you can change the addresses used to apply security policies without requiring a maintenance window. The following feeds are supported for dynamic address groups:

- Custom IP list feeds
- GeoIP feed (from Spotlight Secure)

Spotlight Secure Connector: An extension of Spotlight Secure to your premise, Spotlight Secure Connector provides control and intelligence to the solution by consuming feeds from both Spotlight Secure and local sources that are, subsequently, shared with SRX Series gateways. The security intelligence feeds that are available through Spotlight Secure include:

- Known IPs, domains, and URLs for malicious C&C activity or botnet activity; for example, if an infected device tries to connect to a C&C server on the Internet, the SRX Series can block the traffic based on a real-time feed of C&C destinations that is delivered through Spotlight Secure. The feed data is updated often, dynamically loaded, and does not require any commit or configuration changes.
- GeoIP (country-to-IP mapping) data

The security intelligence obtained locally through the Spotlight Secure Connector includes:

- Custom IP list feeds from either customer provided data or from third parties (e.g., consortiums)—can take the form of a custom file that you manually upload or you can configure periodic updates via a Web server

Summary—Effective Network Protection Equals a Better Customer Experience

Every organization would agree that customer experience is a key business imperative and that security needs to "just work," even as new threats surface and as traffic grows.

Juniper's security intelligence for SRX Series Services Gateways has been built from the ground up to respond to a rapidly changing threat landscape. And, Juniper helps you save time and minimize complexity by centrally managing all SRX Series policies with the Junos Space Network Management Platform.

Lastly, we have provided an open security intelligence solution for you to build on and extend based on business needs. Spotlight Secure delivers actionable security intelligence that can be used in policy immediately, but you can choose to add your own sources of threat intelligence as needs change.

Next Steps

Visit www.juniper.net/security or contact your Juniper representative for more information on SRX Series Service Gateways and integrated security intelligence.

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

3510517-002-EN Aug 2015