Juniper and Attivo Networks Add Inside-the-Network Threat Detection as a Next Layer of Defense

Discover and Dynamically Block Infected Nodes Inside the Network

Challenge

Protecting networks against malicious attacks requires constant vigilance. Network traffic must be continuously monitored for threat activity. Once potential attacks are identified, the threat must be contained and malicious activity blocked.

Solution

Integration of the Attivo BOTsink solution with Juniper Networks Security Intelligence (SecIntel) gives SRX Series Services Gateways the ability to block infected nodes from gaining Internet access and exfiltrating valuable company data.

Benefits

Juniper and Attivo's joint solution mitigates the threat posed by bots and advanced persistent threats (APTs) by attracting, engaging, analyzing, and containing attacks on the network before they can do any harm.

Protecting networks against malicious attacks requires constant vigilance. Network traffic must be continuously monitored for threat activity, and once potential attacks are identified, the threat must be contained and malicious activity blocked.

Juniper Networks® SRX Series Services Gateways offer a portfolio of scalable security solutions that protect customers from the most serious threats. The SRX Series provides a foundation that allows enterprise and service providers to implement a wide array of services, including unified threat management (UTM), next-generation firewall, and threat intelligence. And the open and scalable Juniper Networks Security Intelligence (SecIntel) framework enables Juniper to seamlessly integrate leading industry security partners, such as Attivo Networks, and offer customers complementary solutions to combat the broadest spectrum of malevolent threats.

The Challenge

As the scale and sophistication of network threats continues to increase, businesses need greater insight into attackers, threats, and the devices used in attacks. Next-generation security has to be built on automated and actionable intelligence that can be quickly shared to meet the demands of modern and evolving networks. SRX Series Services Gateways offer high-performance network security with advanced integrated threat intelligence, delivered on the industry's most scalable and resilient platform.

The Juniper Networks-Attivo Networks Joint Security Intelligence Solution

Juniper Networks has teamed with Attivo to add inside-the-network threat detection as a next layer of defense in today's security infrastructure. The Attivo Networks® BOTsink solution adds a new layer of security by accelerating breach discovery and providing an additional line of defense designed to make it difficult for attackers to reach or compromise valuable assets.

The Attivo BOTsink solution seamlessly integrates with Juniper Networks Security Intelligence (SecIntel) framework to provide the SRX Series Services Gateways the needed intelligence to block infected nodes from gaining Internet access and exfiltrating valuable company data. Once the BOTsink platform identifies an infected node, its IP address is sent to the Spotlight Secure Connector, a key component in Juniper Networks Spotlight Secure threat intelligence platform. A premises-hosted application, Spotlight Secure Connector accepts and distributes threat intelligence information to enforcement points through its API for SRX Series enforcement—quarantining the device, stopping any communication with the Command and Control server (C&C), and preventing any data exfiltration.

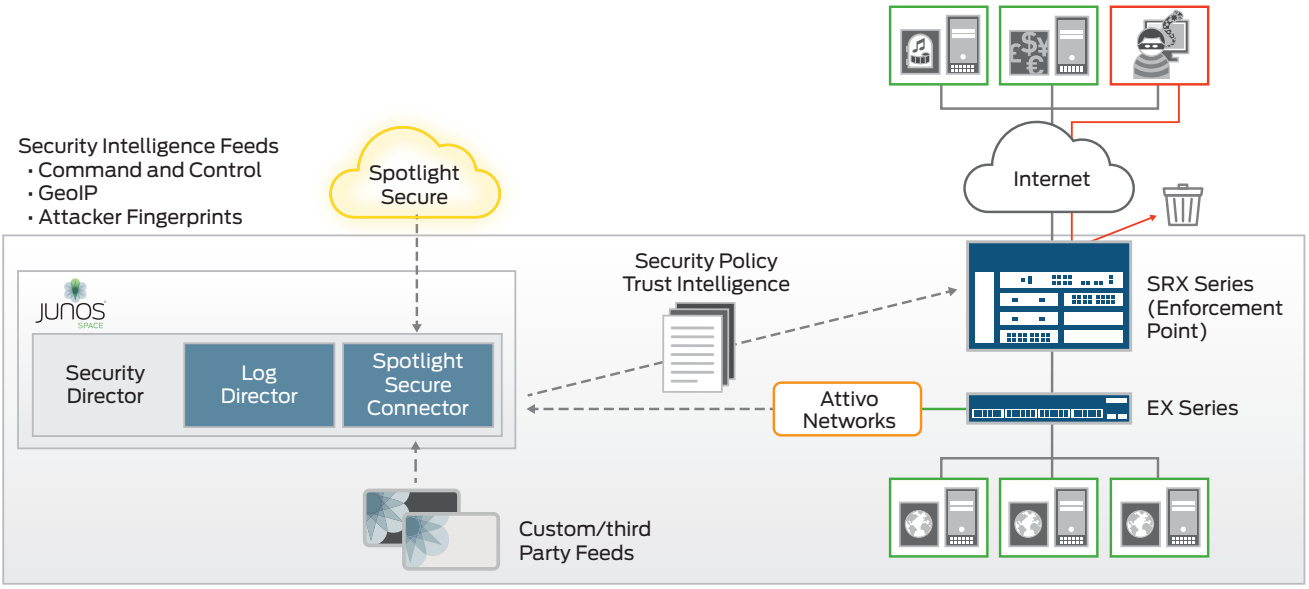

Figure 1: Security intelligence framework

There are two methods to bring feeds into the internal database of Juniper's SecIntel platform, where the SRX Series gateway can retrieve and apply the feed information to its firewall policies.

- The first is a list of IP addresses or ranges of addresses, without an associated threat score. These are typically used in blacklist or whitelist applications, where a threat level is inferred from the application. Blacklist entries are assumed to be "Bad," while whitelist entries are assumed to be "Good."
- The second data format, used by Attivo Networks, is an IP address with an associated threat level. This approach mimics the format used by Juniper's own threat feeds. The entries are typically used with SecIntel policies on the firewall. The threat levels allow a more granular application of the rules. Attivo seamlessly integrates with the Spotlight Secure Connector, giving SRX Series gateways the necessary intelligence to prevent infected nodes from gaining Internet access, moving laterally and exfiltrating valuable company data.

Spotlight Secure Connector provides an API that allows Attivo to push data directly into Spotlight Secure Connector. This enables the SRX Series gateway to quarantine the infected device, stop communication with a C&C server, and prevent data exfiltration.

Features and Benefits

- Seamless integration of Attivo BOTsink with Juniper SecIntel
- SRX Series devices equipped with the intelligence to block infected nodes from gaining Internet access and exfiltrating valuable company data

Solution Components

- Juniper Networks SRX Series Services Gateways
- Juniper Networks Spotlight Secure Connector
- Juniper Networks SecIntel Security Intelligence
- Attivo BOTsink

Summary—Inside-the-Network Threat Detection as a Next Layer of Defense

It takes constant vigilance and integrated security solutions to protect and mitigate against malicious attacks. Network traffic must be continuously monitored for threat activity, and once potential attacks are identified, the threat must be contained and malicious activity blocked. With this joint solution, Attivo Networks and Juniper Networks have created a very effective framework that combines Attivo BOTsink, SecIntel intelligence, and SRX Series gateways to do just that. This powerful combination mitigates the threat posed by bots and advanced persistent threats (APTs) by attracting, engaging, analyzing, and containing attacks on the network before they can do any harm.

Next Steps

To explore ways that your organization could benefit from the Juniper-Attivo joint security solution, please contact your Juniper Networks representative for more information.

About Attivo

Attivo Networks is the leader in dynamic deception technology, which in real-time detects intrusions inside the network, data center, and cloud before the data is breached. Leveraging high-interaction deception techniques, the Attivo BOTsink solution lures BOTs/APTs to reveal themselves, without generating false positives. Designed for efficiency, there are no dependencies on signatures, database lookup or heavy computation to detect and defend against cyber threats. Attivo solutions capture full forensics and provide the threat intelligence to shut down current and protect against future attacks.

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

3510562-001-EN Dec 2015