JUNIPER

Product Name: SRX

Main Website: http://www.juniper.net

Product Website: http://www.juniper.net/us/en/products-services/security/srx-series/

Product Integration Type

Firewall

Integration Objective

- Integrates with Juniper SRX to mitigate malicious IP addresses
- SmartCore compiles the list of malicious IP addresses from CNC IP addresses seen in infections. To avoid false-positives, SmartCore checks for the reputation of the CNC IP addresses
- As of version 3.5, SmartCore pushes the CNC IP addresses automatically to SRX, without any need for manual intervention

Customer Value Proposition

Integrates with existing third party infrastructure in the customer's environment to block calls to malicious CNC servers.

Tested Vendor Versions

SRX version 12.1 tested on the vSRX and SRX 650

ADF Integration Classification

Blocking: Firewall, Web Proxy

Integration Details

Enterprise. Can work in large environments with a variety of integration points.

Integration Method

Push: SmartCore pushes CNC IP addresses to SRX.

Integration Detail Summary (API, CLI)

- SmartCore uses SRX's netconf protocol to SSH into the SRX device
- SmartCore supports both zone attached and zone defined address book modes in SRX
- SmartCore pushes the CNC IP addresses to an address book defined in SRX
- An administrator can create policies on SRX that block connections going out to any address in the address book
- SmartCore can work with virtual and physical SRX devices
- CNC IP addresses can be added or removed from the SRX using Cyphort Manager UI
- User can also specify "expiry days" on the Cyphort Manager UI to automatically remove the CNC IP addresses from SRX after the specified number of days expire

Manager GUI Component

- Yes
- Cyphort Manager configuration: SRX settings can be configured under Settings -> Environmental Settings

GUI Operational Use Case

Under the Mitigation tab in the Cyphort Manager, the CNC IP addresses show up under Firewalls. The administrator can push or remove IP addresses from the SRX manually. From release 3.5 onwards, CNC IP addresses can be pushed automatically to the SRX device, without the need for manual intervention.

Threat Score Impact

No

Integration Documentation

N/A

Integration Demo

Yes

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com

Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com