

Juniper Networks® Secure Analytics (JSA) Risk Manager

The new addition to the JSA family helps to monitor device configurations by simulating changes to your network.

With JSA Risk Manager, you can:

- Monitor, discover, and prioritize vulnerabilities before sending alerts
- Visualize network traffic patterns with a network topology model
- Enable risk-based remediation, facilitating compliance
- Centralize network security device management
- Model threat propagation and simulate network topology changes

You can prioritize your remediation tasks with valuable insights into assets and vulnerabilities that are causing the most risk.



Configuration Monitor

JSA Risk Manager Configuration Monitor reviews and compares device configuration, allowing you to enforce security policies and monitor device modifications within your network.

Device IP	Context	Backup Status	Progress	Backup Log	Name	Adapter	Type	Vendor	Model	Log Source(s)	Config. Obtained On
10.219.16.196	N/A	SUCCESS	<div></div>	See Log	Test1	Juniper JUNOS	FIREWALL	Juniper	sr124002		Fri Feb 10 10:27:15 IST 2017
10.219.30.50	N/A	SUCCESS	<div></div>	See Log	Test1	Juniper JUNOS	FIREWALL	Juniper	sr1300		Fri Feb 10 10:19:45 IST 2017
10.206.32.183	N/A	SUCCESS	<div></div>	See Log	Test1	Juniper JUNOS	FIREWALL	Juniper	sr15000		Fri Feb 10 10:18:47 IST 2017

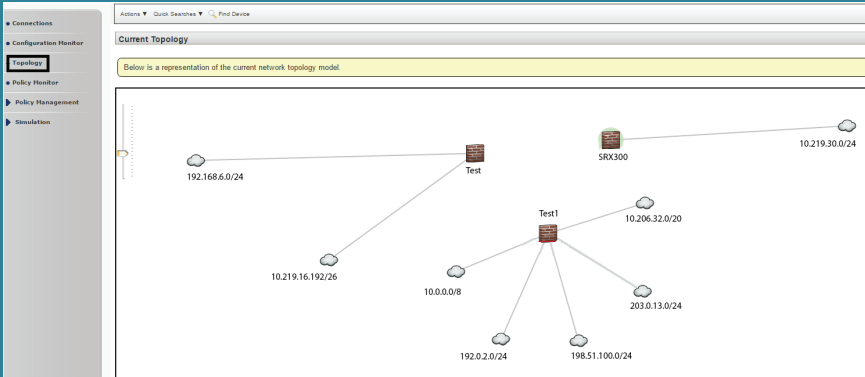
Network Topology Model

JSA Risk Manager visualizes current and potential network traffic patterns with a network topology model, based on security device configurations.

Intelligent Policy Manager

JSA Risk Manager Policy Management displays details about policy compliance and policy risk changes for assets, policies, and policy checks.

Status	Name	Group	Return Type	Imports	Monitor	Created By	Modified By	Policy Execution Time
Not secure	Assess any devices (i.e. firewalls) that allow banned protocols (i.e. Kazaa - port 1214 traffic) from the Internet to the DMZ	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess any inbound connections from the Internet to the DMZ	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets using unsecure protocols from the Internet to the DMZ	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets with client side vulnerabilities which have communicated with suspicious peers	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets with high risk vulnerabilities	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets with mail vulnerabilities (i.e. port 25) on a specific localities (i.e. mail network)	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets with new vulnerabilities reported after a specific date	Configuration	Devices/Rules	5	No	admin	admin	N/A



Network Simulator

Use simulations to define, schedule, and run exploit simulations on your network. You can create, view, edit, duplicate, and delete simulations.

Network Activity Monitor

JSA Risk Manager quickly flags out-of-policy traffic based on security events and network flow data, providing interactive analysis of current and historical network activity.

Status	Name	Group	Return Type	Imports	Monitor	Created By	Modified By	Policy Execution Time
Not secure	Assess any devices (i.e. firewalls) that allow banned protocols (i.e. Kazaa - port 1214 traffic) from the Internet to the DMZ	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess any inbound connections from the Internet to the DMZ	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets using unsecure protocols from the Internet to the DMZ	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets with client side vulnerabilities which have communicated with suspicious peers	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets with high risk vulnerabilities	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets with mail vulnerabilities (i.e. port 25) on a specific localities (i.e. mail network)	Configuration	Devices/Rules	5	No	admin	admin	N/A
Not secure	Assess assets with new vulnerabilities reported after a specific date	Configuration	Devices/Rules	5	No	admin	admin	N/A

Simulation Editor - Google Chrome

What do you want to name this simulation?
Assets susceptible to a client exploit simulation sourced from assets t

Which model do you want to run this simulation on?
Current Topology ☒ Use Connection Data

Importance Factor:
8

Where do you want the simulation to begin?
Attack originates from somebody that has visited one of the following geographic network locations over the last 1 days

Which simulations do you want to include in the attack?
☒ Attack targets one of the following IP addresses
☒ Attack targets one of the following networks
☒ Attack targets one of the following asset building blocks
☒ Attack targets one of the following reference sets
☒ Attack targets one of the following open ports using protocols
☒ Attack targets assets susceptible to one of the following vulnerabilities

Generate a simulation where...
 Attack originates from somebody that has visited one of the following geographic network locations (misc AnonymousProxy) over the last 3 days
☒ and Attack targets assets susceptible to vulnerabilities with one of the following classifications (Denial of Service)

Run this simulation for 3 steps Manual

Please select the groups you would like this simulation to be a member of:
☒ Templates

Save Simulation

For additional technical resources, please visit: www.juniper.net/documentation/



TechLibrary Landing Page — JSA:
https://www.juniper.net/documentation/en_US/release-independent/jsa/information-products/pathway-pages/jsa-series/product



JSA Product Page
(data sheets, specs, etc.):
<http://www.juniper.net/us/en/products-services/security/secure-analytics/>

DAY ONE POSTER

**Juniper Networks
Secure Analytics (JSA)
Risk Manager**

Juniper Networks
Information and
Learning Experience (iLX)