Juniper Secure Analytics Risk Manager

Product Overview

Juniper Secure Analytics Risk Manager is an integral component of a complete security intelligence solution that can help security professionals stay ahead of advanced threats. The ability to proactively quantify risk from vulnerabilities, configuration errors, anomalous network activity, and threats can help organizations prevent exploits that target high-value assets and data.

Product Description

Log management and security information and event management (SIEM) have become trusted solutions for network and security operators, enabling them to quickly detect and isolate security incidents and meet specific compliance requirements, as well as a growing number of regulatory mandates. And while the information provided by SIEM is critical for network and compliance security management efforts, it primarily detects exploits as they occur, rather than prioritizing what actions can be taken to prevent them from happening in the first place.

Juniper Secure Analytics Risk Manager correlates network topology information with data from Juniper Networks® JSA Series Secure Analytics Appliances, including asset configurations, vulnerabilities, network events, and flow patterns. This provides valuable insights that reveal, for example, which assets and vulnerabilities are causing the most risk, so IT staff can prioritize their remediation tasks. The Juniper solution can also help identify firewall and intrusion prevention system (IPS) misconfigurations that may allow attackers into the network and create inefficiencies in devices.

Juniper Secure Analytics Risk Manager automates risk management functions in mission-critical areas, helping security professionals safeguard their organizations against an ever-growing spectrum of attacks, vulnerabilities, and compliance mandates. On today's smarter planet, organizations require better visibility into their security policies, postures, and practices than ever before, because instrumented, interconnected, and intelligent businesses collect and use more information.

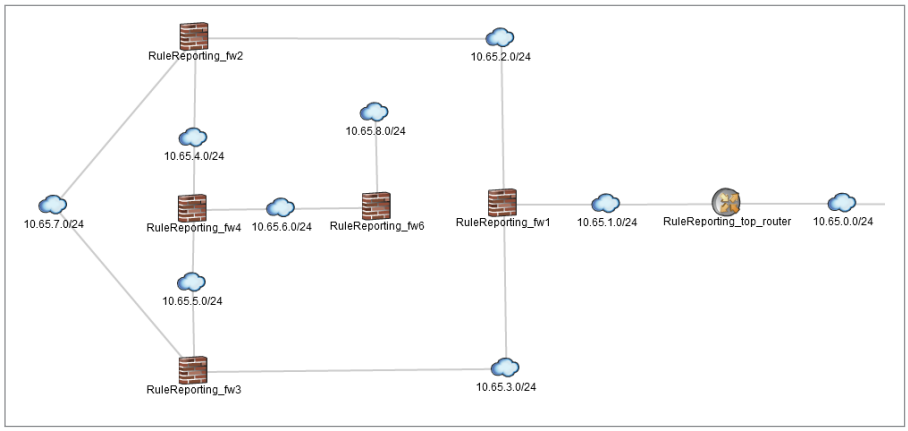

Figure 1. Juniper Secure Analytics Risk Manager topology viewer enables users to see network devices and relationships, including subnets and links.

Your ideas. Connected.™

Architecture and Key Components

Government regulations, industry guidelines, and corporate policies can all dictate specific network traffic and firewall policies that an organization must deploy, monitor, audit, and enforce. At a high level, the security objectives are normally pretty clear. These plans exist to achieve the desired security state, but the devil is—as usual—in the details.

Many network attacks succeed simply due to inconsistent network and security configuration practices, highlighting the need for automated network configuration monitoring and alerts for policy breaches. Other attacks succeed because unpatched vulnerabilities allow unfettered access to systems. Using traditional log management and SIEM solutions, where data typically exists in separate silos, organizations often lack the ability to easily correlate events and assess when network configurations are allowing traffic that is "out of policy."

Juniper Secure Analytics Risk Manager offers an integrated, policy-based approach that can greatly improve the organization's ability to asses information security risk through a single console shared with Juniper Secure Analytics and Juniper Secure Analytics Vulnerability Manager. Juniper Secure Analytics Risk Manager leverages a broad range of risk indicators, including asset, network, and security configuration data; network activity data; network and security events; and vulnerability scan results. It also provides other key capabilities as detailed below.

Vulnerability Risk Assessment

- **Quantification of risk:** Helps assess vulnerabilities and asset configurations based on industry standards and environmental factors, to help prioritize remediation
- **Correlation of known vulnerabilities with network topology:** Helps deliver a prioritized list of vulnerabilities to better assess which systems are most vulnerable to attack and should be remediated first
- **Advanced threat modeling, simulation, and visualization:** Simulates potential spread of threats through the network by leveraging vulnerability, network topology, and connection data

Network Security Configuration

- **Detailed configuration audit:** Helps improve consistency of firewall rules, including detection of shadowed rules, rule usage, and other configuration errors
- **Security focused network topology model:** Enables automated monitoring of configuration rules
- Configuration change comparison and auditing: Alerts users to risky or out-of-compliance configuration

Network Activity Monitoring

- **Advanced monitoring and analysis of network activity:** Quickly flags out-of-policy traffic based on security events and network flow data
- **Fast and efficient search of network activity:** Greatly reduces forensics efforts
- **Intuitive visualization tool:** Provides interactive analysis of current and historical network activity

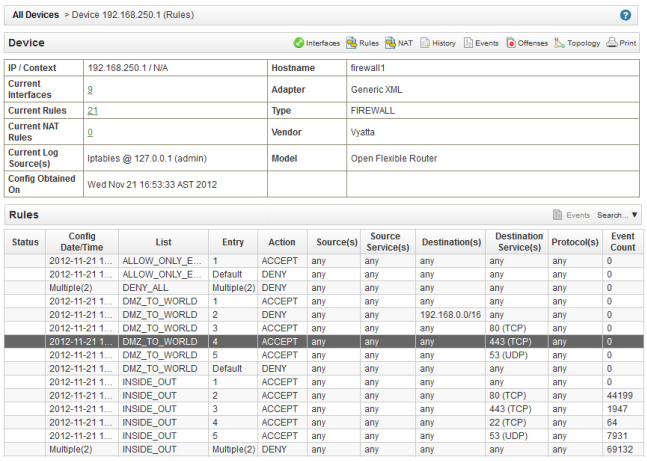

Figure 2. With the policy engine in Juniper Secure Analytics Risk Manager, risk scores can be dynamically adjusted based on environmental factors.

Network Security Event and Configuration Correlation

- **Correlation of firewall accept and deny events with rules:** Quantifies rule usage and effectiveness
- **Scheduled or on-demand collection of device configuration data:** Provides a historical configuration change record
- **Advanced asset database correlation:** Leverages information from a wide variety of network and security events and configuration sources, improving accuracy of results

Policy Monitoring to Improve Compliance

Juniper Secure Analytics Risk Manager features an automated policy engine that simplifies the assessment of a wide spectrum of information security and compliance policies. With an intuitive question-based interface, the policy engine integrates previously siloed risk indicators through regular monitoring of network assets for defined conditions. For example, the solution enables the correlation of asset vulnerability, configuration, and network activity, dynamically increasing or decreasing risk scores based on environmental factors, and enabling risk prioritized remediation.

The Policy Monitor feature allows active evaluation of multiple security policies. Juniper Secure Analytics Risk Manager provides out-of-the-box policy templates to assist with identifying risk

across regulatory mandates and information security best practices. These templates are easily extended to align with an organization's internal information security policies, and as exceptions are discovered, Juniper Secure Analytics Risk Manager can send e-mail, display notifications, generate a system logging event, or create an offense within JSA Series Secure Analytics Appliances. In addition, compliance reports include both policy exceptions and successes.

Device Configuration Management to Detect Changes and Profile Future Risks

Juniper Secure Analytics Risk Manager provides automated collection, monitoring, and auditing of device configurations across an organization's switches, routers, firewalls, and intrusion detection system/intrusion prevention system (IDS/IPS) devices. Through an ability to normalize cross-vendor device configuration data, Juniper Juniper Secure Analytics Risk Manager provides detailed comparisons across security devices—including firewall rules and policies—to quickly identify when network traffic is inconsistent with a regulation, corporate mandate, or industry best practice.

Juniper Secure Analytics Risk Manager maintains a history of configuration changes and enables users to audit this history across the network. This powerful capability allows users to compare normalized or raw device configurations, over time, across a single device or multiple devices through a single user interface.

The collection of device configuration data is also instrumental in building an enterprise-wide representation of a network's topology. Topology mapping can help an organization understand allowed and denied application activity across the network, resulting in improved consistency of device configuration.

Modeling and Simulation of Attacks and Network Configuration Changes

Juniper Secure Analytics Risk Manager helps organizations identify and prioritize their most significant risk areas. Simulations can help organizations understand the risk impact of proposed network configuration changes before they are implemented. For example, simulations can check network connectivity before and after a proposed network configuration change, such as adding a firewall rule to one or more devices.

Juniper Secure Analytics Risk Manager also offers threat modeling capabilities to simulate the potential spread of an exploit across the network by performing multistep correlations of at-risk systems with network traffic and topology data. Security teams can select a starting point for the attack, such as the Internet or an untrusted network, and then specify risk criteria, such as known system vulnerabilities or the protocol and port being used for the exploit. Juniper Secure Analytics Risk Manager then graphically displays the potential spread of the attack across multiple network tiers.

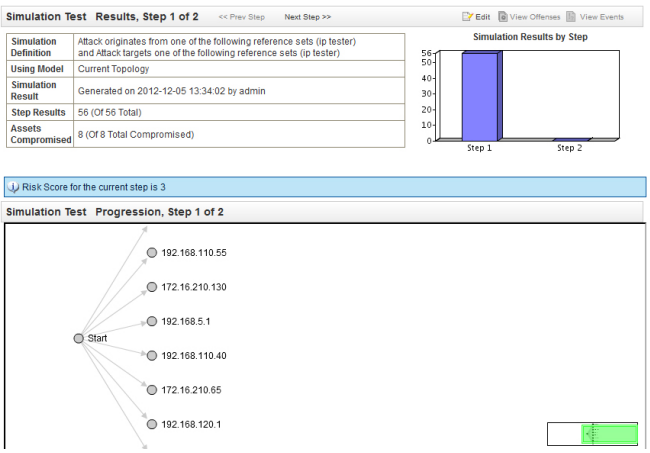

Figure 3. Juniper Secure Analytics Risk Manager attack simulation screen shows the potential spread of an exploit across the network.

Advanced Tools to Investigate Network Topologies, Traffic, and Forensics

Juniper Secure Analytics Risk Manager offers two network visualization security tools that provide unique, risk focused, graphical representations of the network. The end result of both of these visualizations offers network and security teams a revolutionary investigative capacity by providing vulnerability information before, during, and after an exploit. The first visualization tool, called the Topology Viewer, delivers detailed network topography views from both a routing and firewall configuration perspective. This insight comes from a unique combination of data sources, including device configuration, network activity data, and security events. IT teams can review the entire network or a portion of the network, and they can export views to image or Microsoft Visio formats.

The second visualization tool, called the Connection Monitor, quickly and efficiently analyzes historical network activity by automatically summarizing all firewall event and network flow data. Connection Monitor enables advanced traffic searches, including the ability to search on connections between hosts and networks using specific protocols and applications, as well as analyzing traffic to and from specific countries or geographical regions. These capabilities can significantly accelerate forensic and network traffic analyses.

Security Intelligence to Minimize Risk

Juniper Secure Analytics Risk Manager provides organizations with a comprehensive network security solution that not only enables them to access forensics during and after an attack, but also to proactively detect, prioritize, and remediate areas of high risk before they can be exploited.

The powerful security analytics, simulation, and visualization capabilities of Juniper Secure Analytics Risk Manager provide a unique opportunity for organizations to move away from day-to-day security "firefighting" and instead adopt a proactive, risk-based methodology that greatly strengthens network and security offenses while minimizing exploit risk.

Log management and SIEM are necessary for a good network defense. By adding Secure Analytics Risk Manager, organizations gain additional security intelligence that enables them to go on the offensive against those who wish to exploit their assets and networks.

Features and Benefits

- Visualize current and potential network traffic patterns with a network topology model, based on security device configurations
- Quantify and prioritize risk with a policy engine that correlates network topology, asset vulnerabilities, and actual network traffic, enabling risk-based remediation and facilitating compliance
- Centralize network security device management to help reduce configuration errors and simplify monitoring of firewall performance
- Model threat propagation and simulate network topology changes to help improve overall security

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

To learn more about how Juniper Secure Analytics Risk Manager can benefit your organization, please contact your Juniper Networks representative and visit www.juniper.net.

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

1000543-001-EN May 2016