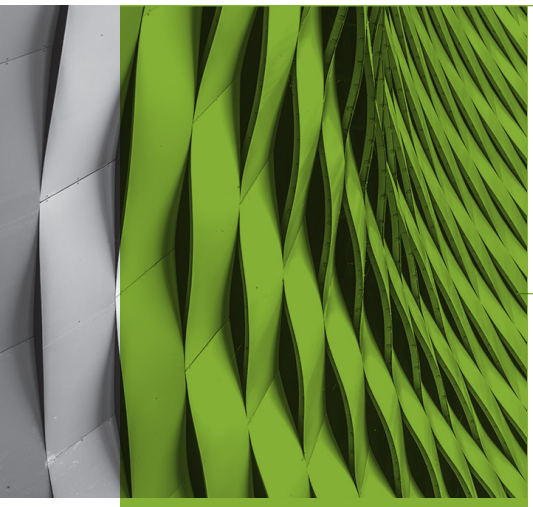

SECURITY DIRECTOR

Product Overview

Juniper Networks® Security Director is the central manager for all SRX Series Services Gateways. It provides security policy management for all physical, logical, and virtual firewalls through an innovative, intuitive, and centralized web-based interface that offers enforcement across emerging and traditional threat vectors. It provides detailed visibility into application performance, reduces risk while enabling users to diagnose, and it resolves problems quickly.

Providing extensive scale, granular policy control, and policy breadth across the network, Security Director helps administrators manage all phases of the security policy lifecycle for stateful firewall and next-generation firewall (NGFW) services, managing security both on-premises and in the cloud through a centralized web-based interface.

Product Description

Network security management is how administrators operationalize their firewall architecture and provide visibility across individual deployments, policies, and traffic, and gain insight from threat analytics across the entire network traffic.

It can be a curse if management solutions are slow or restricted in their level of granularity and visibility; or a blessing with intuitive wizards, time-saving orchestration tools, and insightful dashboards. Security Director provides security policy management for all physical, virtual, and containerized firewalls (SRX Series Services Gateways). Through an intuitive, centralized, web-based interface, Security Director reduces management costs and errors by providing visibility, intelligence, automation, and effective security across SRX deployments in both public and private clouds concurrently.

Security Director is your portal to Secure Access Service Edge (SASE), bridging your current security deployments with your future SASE rollout. Security Director enables organizations to manage security anywhere and everywhere, on-premises and in the cloud with unified policy management that follows users, devices, and applications wherever they go. Policies can be created once and applied everywhere. Customers can use both Security Director Cloud and on-premises instances simultaneously to securely transition to a SASE architecture.

With Security Director, organizations can transition to a SASE architecture seamlessly, securely, and at a pace that's best for each individual business. The bi-directional sync between Security Director and on-premise and individual firewalls, provides a cohesive management experience that supports a seamless transition to the cloud. Its unified policy management provides easy-to-use, consistent security policy that follows the user, device, and application—without needing to copy over or recreate rule sets.

Figure 1: Security Director Cloud Architecture

The Security Director dashboard provides customizable, information-rich widgets offering visually intuitive displays that report security device status at a glance. A pallet allows you to easily navigate between firewall, threat, intrusion prevention system (IPS), application, throughput, and device-related information to create a customized view of the Juniper Networks SRX Series Services Gateways firewall environment.

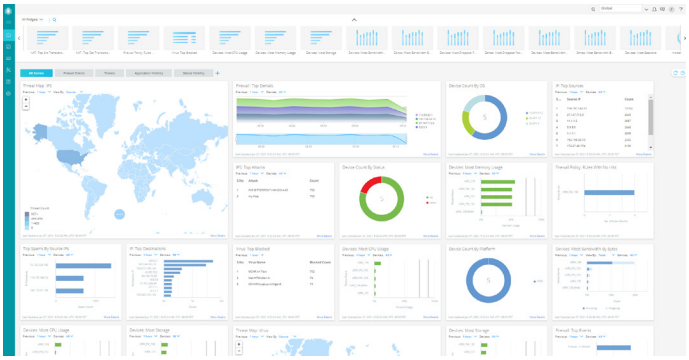

Figure 2: Security Director Dashboard

You can quickly determine which SRX Series devices have generated the most alarms or consume the most CPU cycles or RAM for a specific time period through the dashboard.

By drilling down on widgets, administrators can sort and search various events to effortlessly obtain detailed information such as top viruses blocked, top destinations, top sources, and other details to ensure that the network is safe.

Security Director is an innovative solution for managing the application, user, and IP environments. Network administrators can choose between three different views to see how applications and users affect the network, observe bandwidth utilization levels, or determine the number of sessions created. Granular usage details, such as which applications are the riskiest, can be viewed. Top talkers are easy to identify and remediate. You can also compare different time frames and determine when utilization is typically at its peak.

With most security management solutions, administrators must run a report or open several tabs to find the applications or users they want to manage. Then they must manually create the required firewall rules, determine where to place those rules, and hope they don't conflict with any existing rules, thereby creating a host of new problems. This task is an exceptionally tedious, time-consuming, and error-prone process.

Security Director is extremely user-friendly and does not require users to run multiple reports or open multiple tabs and manually analyze the data to find answers. Instead, Security Director provides administrators with the ability to quickly find crucial answers, at a glance, without digging through reports.

Using the actionable intelligence that Security Director provides, administrators can select one or more applications or user/user groups from the Application Visibility or User Visibility charts, then simply select "Block." Security Director automatically creates the requested rule or rules and deploys them in the optimal location within the rules base, avoiding any anomalies and taking the guesswork out of managing the application and user environment.

Security Director also provides actionable intelligence when it comes to threat mitigation. For example, the Threat Map widget shows the number of IPS events detected per geographic location, giving you immediate awareness of threat activity and providing the means to remediate with one click.

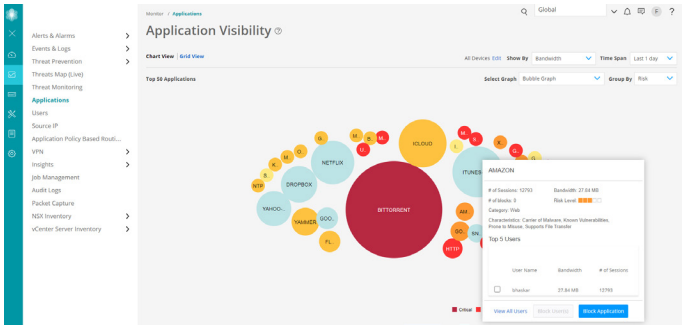

Figure 3: Application Visibility Dashboard

Security Director Insights

Security Director Insights unifies visibility across the network by correlating threat detection information, including detections from other vendor products, and enables one-touch mitigation to quickly address gaps in defense.

Figure 4: Security Director Insights Dashboard

Security Director Insights collects and automatically correlates data across multiple security layers—email, endpoint, server, cloud workloads, and network—so threats are detected faster, and security teams can improve investigation and response times. It also uses mitigation rules to prevent future attacks.

With Security Director Insights, customers can:

- Understand when and where an attack is happening by using it to correlate and prioritize security events from multiple security solutions across various parts of the network.
- Use custom threat and incident scoring so that security teams respond to and can mitigate attacks that have the potential to do the most harm to the business.

- Mitigate active threats across the network—on Juniper SRX Series firewalls, EX and QFX Series switches, wired and wireless access points driven by Mist AI, along with third-party solutions—with one click.

Customers can use Security Director Insights to track attack indicators across their networks, from client to cloud, regardless of which vendor product in their environment made the detection.

Policy Enforcer

Policy Enforcer provides a simplified user intent-based threat management policy modification and distribution tool. It allows updated policies to deploy on Juniper Networks EX Series Ethernet Switches, MX routers, QFX Series switches, and Juniper virtual and physical SRX Series Services Gateways.

Security Director provides automated enforcement and policy orchestration that allows updated security policies to deploy across Juniper SRX firewalls, EX Series switches, QFX series switches, MX series routers, and third-party network devices. The software helps automate threat remediation and microsegmentation policies across your entire network.

An intuitive user interface within Security Director gives administrators the flexibility to control and modify network elements, enforcement groups, threat management services, and profile definitions.

Using Policy Enforcer, Security Director automatically updates policies based on threats identified by Juniper Advanced Threat Prevention (ATP). Through Policy Enforcer, updated policies are then distributed to enforcement points such as firewalls, switches, and wireless solutions, ensuring real-time network protection.

Firewall Policy Analysis

With Firewall Policy Analysis, you can gain visibility into anomalies in your network by scheduling reports that show shadow or redundant firewall rules. Firewall Policy Analysis makes recommendations to fix all reported issues and uses automation to optimize your rule-base.

Firewall Policy Analysis eliminates the need to run a monthly or quarterly anomaly report, and having to manually fix all of the issues. You run the report once and Security Director will adapt.

Table 1. Security Director Features and Benefits

Features	Description	Benefits
Security Director Insights	Collects and automatically correlates data across multiple security layers—email, endpoint, server, cloud workloads and network—so threats are detected faster, and security teams can improve investigation and response times. Prevents future attacks with mitigation rules.	• Understand when and where an attack is happening by using it to correlate and prioritize security events from multiple security solutions across various parts of the network. • Use custom threat and incident scoring so that security teams respond to and can mitigate attacks that have the potential to do the most harm to the business. • Mitigate active threats across the network—on SRX Series firewalls, EX and QFX Series Switches, wired and wireless access points driven by Mist AI, along with third-party solutions—with one click.
Policy Enforcer	Creates and centrally manages security policies through a user intent-based system, evaluating threat intelligence from multiple sources while dynamically enforcing policies in near real-time across the network. Enforces threat management policies at firewalls and access switches, aggregating threat feeds from Advanced Threat Prevention Cloud, SecIntel, and on-premises custom threat intelligence solutions with allow list and blocklist support.	• Reduces the risk of compromise by eliminating stale rules and automatically updating enforcement based on network threat conditions. • Improves protective posture by quarantining and tracking infected hosts. • Allows security practitioners to focus on maximizing security rather than writing tedious policy rules.
Firewall policy analysis	Provides the ability to schedule reports that show shadow or redundant firewall rules are and recommends actions to fix all reported issues.	Allows administrators to maintain an efficient firewall rule base by quickly identifying ineffective and unnecessary rules.
Firewall rule placement guidance	Upon creation of a new rule, analyzes existing firewall rule base to recommend optimal position and application.	Significantly reduces shadowing rules.
Metadata-based policies	Enables administrators to create object metadata-based user-intent firewall policies.	Simplifies policy creation and maintenance workflows. In addition to making policies more readable from a user intent perspective, this feature streamlines firewall troubleshooting.
Dynamic policy actions	Enables security administrators to initiate different actions, including firewall, logging, IPS, URL filtering, and Antivirus, among others, under different conditions.	Reduces the time required to adjust the organization's security posture under different conditions and streamlines threat remediation workflows.
Firewall policy hit count	Shows hit counts for each firewall via meters and filters that display which rules are hit the least. Security Director also can keep a lifetime hit count.	Allows administrators to assess each firewall rule's effectiveness and quickly identify unused rules, resulting in a better-managed firewall environment.
Live threat map	Displays where threats are originating in near real-time and allows you to take action to stop them.	Provides near-real-time insight into network-related threats. Allows you to block traffic going to or coming from a specific country with a single click.

Features	Description	Benefits
Innovative application visibility and management	Provides an easy and intuitive way to see which applications use the most bandwidth, have the most sessions, or are most at risk. Know which users are accessing non-productive applications and by how much. Top talkers are displayed in an easy-to-understand manner. Block applications, IP address, and users with a simple mouse click.	Delivers greater visibility, enforcement, control, and protection over the network.
Simplified threat management	Reports where threats are originating and where they are going via a global map. Blocking a country is easy; simply mouse over the country to take action.	Provides insight needed to manage network-related threats effectively. Allows you to block traffic going to or coming from a specific country with a single click.
Snapshot support	Allows users to snapshot, compare, and roll back configuration versions.	Simplifies configuration changes and allows recovery from configuration errors.
Policy lifecycle management	Provides the ability to manage all phases of security policy lifecycles, including creating, deploying, monitoring, remediation, and maintenance.	• Enables central control over stateful firewall, AppFW, URL filtering, anti-virus, IPS, VPN, and NAT in one Security Director management console. • Eases administration by unifying common policy tasks within a single interface. • Reduces errors by enabling the reuse of policies across multiple devices.
Drag-and-drop	Allows firewall, IPS, and NAT rules to be reordered by simply dragging them to a new location.	Enables firewall, IPS, and NAT objects to be added or copied by dragging them from one cell to another or from a pallet located at the bottom of the policy table.
VPN auto-provisioning and import	Simply tell Security Director which VPN topology to use and which devices you want to participate in the topology, and Security Director will auto-provision the tunnels. If you have an existing Juniper VPN environment, Security Director can import the VPNs to provide an easy and effective way to manage them.	Makes pre-existing SRX Series firewall VPNs easier to manage.
Role-based access for policies and objects	Allows devices, policies, and objects to be placed within domains and assigns read/write permissions to a user.	Provides customers a way to segment administrative responsibility for policies and objects.
REST APIs for automation	Provides RESTful APIs used in conjunction with automation tools.	Automates configuration and management of physical, logical, or virtual SRX Series firewalls.
Logging and reporting through Junos Space Log Director application	Enables integrated logging and reporting.	Tight coupling with Security Director: • Displays rules and events in the same window • Allows administrator to easily shift views from logs to corresponding rules and vice versa Direct access to Security Director policies and objects: • Role-based access control (RBAC) • Event viewer for events aggregation and filtering • Dashboard with customizable graphs • Reports generated and automatically sent via email • Email alerts automatically generated based on threshold SRX Series health monitoring: - CPU utilization - Memory utilization - VPN monitoring System log forwarding to security information and event management (SIEM)

To order Juniper Security Director and access software licensing information, please visit the How to Buy page at www.juniper.net/us/en/how-to-buy/.

Files uploaded to the cloud for processing are destroyed afterward to ensure privacy. The Juniper Networks privacy policy can be found on the product Web portal at www.juniper.net/us/en/privacy-policy/.

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.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

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
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700

Driven by Experience™