

Junos Space Security Director

Product Overview

In today's complex environment, network security management can become overly time-consuming and prone to error if management solutions are slow, unintuitive, or restricted in their level of granularity, control, and visibility. Junos Space Security Director provides security policy management for both physical and virtual firewalls (Juniper's Networks SRX Series Services Gateways and Firefly Perimeter) through an intuitive, centralized web-based interface that offers enforcement across emerging and traditional risk vectors.

Product Description

Juniper Networks® Junos® Space Security Director, an application on Junos Space Network Management Platform, provides extensive security scale, granular policy control, and policy breadth across the network. It helps administrators quickly manage all phases of the security policy life cycle for stateful firewall, unified threat management (UTM), intrusion prevention system (IPS), application firewall (AppFW), VPN, and Network Address Translation (NAT) through a centralized web-based interface. Junos Space Security Director reduces management costs and errors with efficient security policy, workflow tools, and a powerful “app” and platform architecture.

Because it runs on the Junos Space Network Management Platform, Junos Space Security Director enables administrators to extend their policy control capabilities both broadly and deeply. This includes managing security policy horizontally across multiple Juniper Networks SRX Series Services Gateways, and vertically to manage logical system (LSYS) instances or dense and varied security rule bases on individual SRX Series devices. This reach improves security policy consistency and compliance, even as networks scale. Security administrators can use Junos Space Security Director to speed and simplify security administration and reduce management costs and errors with efficient security policy and workflow tools.

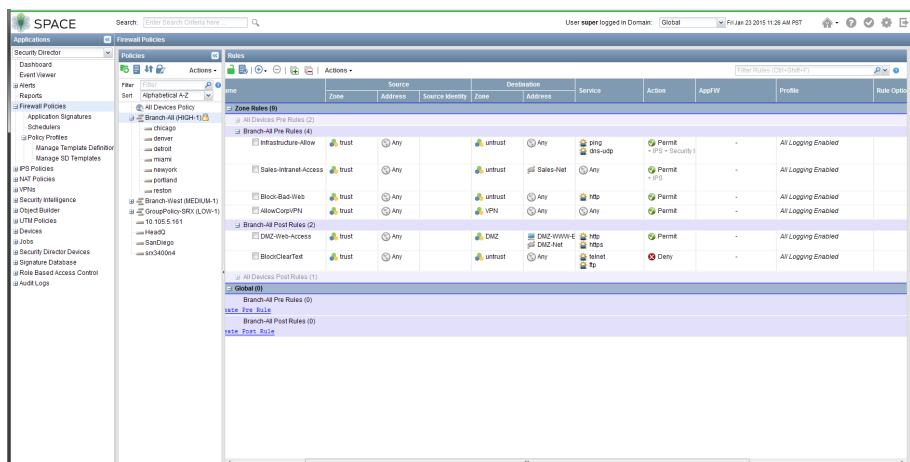


Figure 1: Firewall policy hierarchy allows for ease of management.

Security Director helps ease administration through a responsive Web interface with granular control over global, group, and device-level firewall policies. Administrators can intuitively manage the entire policy life cycle in one easy-to-use interface, from policy creation to remediation. Rapid search tools quickly locate policy terms or issues—even inside rules—for faster maintenance. They can also view event logs and generate reports from the same console, for managing network security incident investigation and response. Security Director reduces management costs and errors with efficient security policy,

workflow tools, and a powerful “app” and platform architecture. Specialized features such as Publish Workflow help delegate policy work by role and check policy/CLI before provisioning, to reduce the risk and costs of accidental errors. To improve policy accuracy and compliance, administrators can reuse Security Director policies across integrated firewalls, intrusion prevention, and NAT. Junos Space Security Director lays the groundwork for further management innovation across the network (i.e., domains) as part of the Junos Space Network Management Platform. For example, new apps can be added in a familiar interface, minimizing staff training time on new technologies and driving innovation as part of developer ecosystem contributions.

Junos Space

Junos Space Security Director is part of Junos Space, which is Juniper’s comprehensive network management solution that simplifies and automates management of Juniper’s switching, routing, and security devices. The Junos Space Network Management Platform provides deep element management for extensive fault, configuration, accounting, performance, and security (FCAPS) management capability, same-day support for new devices and Juniper Networks Junos operating system releases, a task-specific user interface, and northbound APIs to easily integrate

into existing network management system (NMS) or operations and business support system (OSS/BSS) deployments.

Extending the breadth of the Junos Space Network Management Platform are multiple Junos Space management applications that optimize network management for various domains. These applications, with their easy-to-use interfaces, enable you to provision new services across thousands of devices and optimize workflow tasks for specific domains such as core, edge, data center, campus, security, mobile, and more.

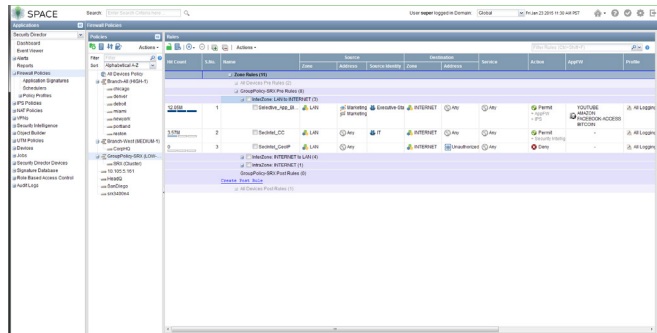


Figure 2: Use Junos Space Security Director to block Marketing’s access to multiple applications while allowing others access to the entire web.

Table 1: Junos Space Security Director Features and Benefits

Features	Description	Benefits
Firewall policy analysis	<ul style="list-style-type: none"> Provides ability to schedule reports that show which firewall rules are shadowed or redundant, and recommends actions to fix all reported issues 	<ul style="list-style-type: none"> Allows administrators to maintain an efficient firewall rule base by easily identifying ineffective and unnecessary rules
Firewall policy hit count	<ul style="list-style-type: none"> Shows hit counts for each firewall via meters, as well as filters that display which rules are hit the least. Security Director also has the ability to keep a lifetime hit count. 	<ul style="list-style-type: none"> Allows administrators to assess effectiveness of each firewall rule and quickly identify unused rules, resulting in better-managed firewall environment
VPN import	<ul style="list-style-type: none"> Enables SRX Series VPNs to be imported into Security Director 	<ul style="list-style-type: none"> Makes pre-existing SRX Series VPNs easier to manage via Security Director
Drag-and-drop	<ul style="list-style-type: none"> Allows firewall, IPS and NAT rules to be reordered by simply dragging them to a new location 	<ul style="list-style-type: none"> Enables firewall, IPS and NAT objects to also be added or copied by dragging them from one cell to another, or from a pallet located at the bottom of the policy table
UTM policy wizard	<ul style="list-style-type: none"> Makes UTM policy configuration easy by adding Juniper’s UTM Policy Wizard 	<ul style="list-style-type: none"> Provides an intuitive, step-by-step method for guiding administrators through the configuration and profile setting process
NAT policy and Event Viewer integration	<ul style="list-style-type: none"> Allows users to right-click on a NAT rule and be taken to events generated by that rule, enhancing and easing troubleshooting for NAT environments 	<ul style="list-style-type: none"> Eases troubleshooting of NAT policies through a simple mouse click, which allows administrators to see which events are associated with what NAT policy Takes administrators directly to the NAT policy associated with the events to take action
Web-based GUI	<ul style="list-style-type: none"> Graphical user interface that is responsive and portrays policy management capabilities in an intuitive view 	<ul style="list-style-type: none"> Allows administrators to drag and drop, easily switch between views, and quickly refresh data for an updated view
Policy locking	<ul style="list-style-type: none"> Prevents two users from editing the same policy at the same time 	<ul style="list-style-type: none"> Reduces configuration errors
Policy versioning	<ul style="list-style-type: none"> Allows users to snapshot, compare, and roll back configuration version 	<ul style="list-style-type: none"> Simplifies configuration changes and allows recovery from configuration errors

Features	Description	Benefits
Takes administrators directly to the NAT policy associated with the events to action	<ul style="list-style-type: none"> Provides ability to save and publish different services to be updated at a later time to appropriate firewalls 	<ul style="list-style-type: none"> Allows administrators to review their firewall, VPN, and NAT policies before updating the device Saves administrators troubleshooting time, avoids errors, and saves costs associated with errors
Policy life cycle management	<ul style="list-style-type: none"> Provides ability to manage all phases of security policy life cycles, including create, deploy, monitor, remediate, and maintain 	<ul style="list-style-type: none"> Enables central policy control over stateful firewall, AppFW, UTM, IPS, VPN, and NAT in one Junos Space Security Director management console Eases administration by unifying common policy tasks within a single interface Reduces errors by enabling reuse of policy across multiple devices
Application identification and classification policy management (using Juniper Networks AppSecure suite of security services)	<ul style="list-style-type: none"> Provides ability to control and protect against misuse of applications resulting in security risks or productivity impact on the enterprise, with applications like Facebook games or instant messaging 	<ul style="list-style-type: none"> Delivers greater visibility, enforcement, control, and protection over the network
IPS/AppFW signature management	<ul style="list-style-type: none"> Flexible, granular, and automatic signature management for IPS and AppFW 	<ul style="list-style-type: none"> Allows administrators to automatically download the latest signatures and view them instantly (with quick and dynamic filtering, users can preview and look at all signatures, then appropriately apply them) Provides better research, which can reduce false positives when applied to policy
UTM support	<ul style="list-style-type: none"> Configuration and policy creation for antivirus, Web filtering, and content filtering 	<ul style="list-style-type: none"> Allows administrators to centrally manage UTM across SRX Series deployments
Various VPN configuration support	<ul style="list-style-type: none"> Simple VPN: Predefined VPN profiles that provide the ability to easily configure site-to-site, hub-and-spoke, and fully meshed VPNs Extranet VPN: Ability to configure a secure connection between your Juniper device and a partner or supplier network 	<ul style="list-style-type: none"> Simple VPN: <ul style="list-style-type: none"> Allows administrators to leverage or customize existing VPN profiles, and in a few clicks configure thousands of VPN tunnels Saves time and reduces the risk of misconfiguration Extranet VPN: Supports agile and productive business by allowing quick and secure connections to partner or supplier networks
VPN dynamic routing management	<ul style="list-style-type: none"> Ability to leverage router and switch protocols such as OSPF and RIP to support VPN configuration 	<ul style="list-style-type: none"> Eases implementation of secure communication between SRX Series devices with Junos Space Security Director and other network devices
Logical system (LSYS) support	<ul style="list-style-type: none"> Ability to partition resources and run multiple instances of policies on an individual SRX Series gateway with LSYS support 	<ul style="list-style-type: none"> Scales security policy by enabling management of different security policies per LSYS instance on a single SRX Series services gateway Maximizes IT investments by reusing existing infrastructure for further functionality
All devices policy	<ul style="list-style-type: none"> Ability to group common policies and deploy them across all SRX Series Services Gateways/Firefly Perimeter virtual firewalls 	<ul style="list-style-type: none"> Allows administrators to maintain compliance by creating global policies that impact all SRX Series devices/Firefly Perimeter virtual firewalls
Role-based access for policies and objects	<ul style="list-style-type: none"> Ability to place devices, policies, and objects within domains and assign read/write permissions to a user 	<ul style="list-style-type: none"> Provides customers a way to segment administration responsibility for policies and objects
Read/write APIs for firewall policy, objects, and VPNs	<ul style="list-style-type: none"> Ability to develop applications related to firewall, objects, and VPNs for SRX Series gateway/Firefly Perimeter deployments 	<ul style="list-style-type: none"> Automates configuration of firewall policies and provisioning of VPNs
Logging and reporting through Junos Space Log Director application	<ul style="list-style-type: none"> Enables integrated logging and reporting for Junos Space Security Director 	<p>Tight coupling with Junos Space Security Director:</p> <ul style="list-style-type: none"> Displays rule and events in same window Allows administrator to easily shift views from logs to corresponding rules and vice versa <p>Direct access to Junos Space Security Director policies and objects:</p> <ul style="list-style-type: none"> Role-based access control (RBAC) Event viewer for events aggregation and filtering Dashboard with customizable graphs Reports generated and automatically sent via e-mail E-mail alerts automatically generated based on threshold <p>SRX Series health monitoring:</p> <ul style="list-style-type: none"> CPU utilization Memory utilization VPN monitoring <p>System log forwarding to security information and event management (SIEM)</p>

Specifications

Client Browser Support

Security Director is best viewed on the following browsers:

- Mozilla Firefox 26
- Chrome 26
- Internet Explorer 8.0 and 9.0

VMware Version

Junos Space works with VMware vSphere 4.0 and above.

Junos (Operating System) Software

The Juniper SRX Series Services Gateways devices run Junos Operating System (OS) software. Junos Space Security Director runs on Juniper Networks devices running Junos OS 10.3 and later releases.

Junos Space Network Management Platform

Junos Space Security Director 13.3 runs on Junos Space 13.3R1.9 and later releases.

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

Junos Space Appliance

Junos Space Appliance includes the complete Junos Space software package as well as the Junos OS operating system. The recommended specifications for a virtual machine installation are identical to the specifications of the physical appliance.

Model Number	Description
JA2500-A-BSE	Base Appliance

Junos Space Security Director

Junos Space Security Director software is licensed based on the number of security devices you will manage. For example, if you will be managing 100 SRX Series Services Gateways, then you would purchase a single license for JS-SECDIR-100. Note: You do not need to purchase a separate license for high availability (HA).

Model Number	Description
JS-SECDIR-5	Junos Space Security Director license for 5 devices
JS-SECDIR-10	Junos Space Security Director license for 10 devices
JS-SECDIR-100	Junos Space Security Director license for 100 devices

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

Copyright 2015 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos and QFabric are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

