

Junos[®] Space Security Design 12.1 Release Notes

Release 12.1
31 May 2012

Junos Space Security Design application is a powerful and easy-to-use solution that allows you to create and publish firewall policies, IPSec VPNs, NAT policies, IPS policies and AppFirewall to provide appropriate security on the network. You would need to procure an IPS license to be able to push IPS signatures and App Firewall signatures to a device.

Contents

Security Design Release Notes	2
Technical Documentation	2
Installing Security Design	2
Supported Devices	2
Supported OS Versions	3
Supported Browsers	3
Management Scalability	3
New Features	3
Known Issues	6
Junos Space Documentation and Release Notes	8
Documentation Feedback	9
Requesting Technical Support	9
Self-Help Online Tools and Resources	10
Opening a Case with JTAC	10
Revision History	10

Security Design Release Notes

Junos Space Security Design application is a powerful and easy-to-use solution that lets you secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and application firewalls. (Note that, to push IPS and application firewall signatures to a device, you also need an IPS license.)

- [Technical Documentation](#)
- [Installing Security Design](#)
- [Supported Devices](#)
- [Supported OS Versions](#)
- [Supported Browsers](#)
- [Management Scalability](#)
- [New Features](#)
- [Known Issues](#)

Technical Documentation

Please refer to the following link for updated documentation for Junos Space Security Design 12.1:

http://www.juniper.net/techpubs/en_US/junos-space12.1/junos-space-security-design-sub-index.html

Installing Security Design

Security Design 12.1 can only be deployed on Network Application Platform 12.1 Release.

Supported Devices

Junos Space Security Design 12.1 is supported on the following SRX Series hardware devices:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX550
- SRX650
- SRX1400
- SRX 3400
- SRX 3600
- SRX 5600
- SRX 5800

Supported OS Versions

- Junos Space Security Design 12.1 supports Junos OS version 10.3 and above.
- The User or Role Policy feature is supported on Junos OS platform 12.1.
- SRX Series devices require Junos OS Release 12.1 to sync the Security Design description field to the device.
- Logical systems feature is supported on the device running Junos OS Release 11.2 and later (excluding VPN and IPS). Junos OS version 11.4 or later is required to manage VPN and IPS with logical systems.
- Junos OS Release 11.4 or later releases is required for AppFW feature support.

Supported Browsers

Junos Space Security Design 12.1 is best viewed on the following browsers:

- Mozilla Firefox 4.0 to 10.0
- Chrome 17 and 18
- Internet Explorer 8.0 and 9.0

Management Scalability

Junos Space Security Design 12.1 is designed to support management of large scale device management was tested to manage 6,000 devices with 100 rule policies. Large policy testing was performed with a 5,000 rule policy which included 10,000 address objects; and 5000 Custom Service objects. Object Builder scale testing was performed with 50,000 address objects.

New Features

The Junos Space Security Design 12.1 application includes the following new features:

- **Policy Import**—Security Design enables you to import firewall and NAT policies from a device. All objects supported by Security Design are imported during the policy import process. Rules that contain objects not supported by Security Design are imported with the disabled rule state.

You can migrate firewall and NAT policies from Network and Security Manager (NSM) for a set of devices. All objects supported by Security Design (addresses, services, address and service group) can be imported with the policy, with the exception of polymorphic objects. Rules referring to unsupported objects are disabled after the migration.

- **Logical Systems Support**—Security Design views a logical system like it does any other security device, and it takes ownership of the security configuration of the logical system. In Security Design, each logical system is managed as a unique security device.
- **Concurrent Policy Editing**—The concurrent edit detection feature prevents policy corruption or overwrite problems when multiple users edit the same policy. If a previous user has added new rules to the policy and saved the changes and when you attempt

to save your changes, you will be given the option to save the policy with a different name.

- **Inline Object Creation**—To optimize the creation of policies, Security Design allows you to create new objects for policies created within the policy editor. This option is available for firewall, NAT, VPN, and IPS policies.
- **SRX Global Policy Support**—Global policy rules are enforced regardless of ingress or egress zones; they are enforced on any device transit. Any objects defined in the global policy rules must be defined in the global address book.
- **Custom Column—User Defined Rule Comments for Firewall Policy**—The custom column feature is a more structured mechanism used for various purposes, such as tracking changes to firewall policies, and owners of a rule, by allowing you to define custom column views. Data in these columns can be captured and saved in the same way as with other columns. You can also search the custom column data.
- **Resource Validation**—Security Design policy publish operation now performs validation that the resources used in the policy do not exceed the capacity of the device or logical systems instance it is being applied to. The validated resources include address objects, services, and rules. For logical systems that have an assigned security profile, including the root logical system, Security Design validates the resource usage against the maximum and reserved quota configured in the respective profile.

If a particular capacity is exceeded, a warning message is provided to the user within the publish job.
- **Policy Based VPN**—Policy-based VPN feature provides support for creating a firewall policy that dynamically creates a VPN between two devices.
- **Extranet Devices**—This feature is used for creating a VPN tunnel between SRX Series devices and non-Junos extranet devices. This is supported for both policy-based and route-based VPNs.
- **VPN Dynamic Routing**—In Security Design, route-based VPNs support the dynamic routing protocols Open Shortest Path First (OSPF) and Routing Information Protocol (RIP), in addition to static routing. Security Design's support for these protocols simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN.
- **User or Role Policy**—For Junos OS release 12.1 and later releases, a user or role can be included as part of the source identity column in a firewall rule. This allows firewall and application policies to be applied to user identities rather than just network sources. This feature requires an Infranet Controller (IC) to manage users and roles, and Junos OS release 12.1 or later for policy enforcement.
- **Comments Sync to Device**—Also pushed to the device are the descriptions entered for the address, service, or NAT pool objects used in the firewall or NAT policies along with descriptions of NAT or firewall policy rules. This feature requires Junos OS version 12.1 or later.
- **Multiple Group Policy Membership**—The Multiple Group Policy Membership feature supports the placing of devices in more than one policy group, and assigning priorities

to the policy groups. This way, the policies, and the rules within them, are applied in the desired order.

- **Routing Instance Support**—In Security Design, the device running Junos OS supports NAT rules to be defined between routing instances in addition to zones and interfaces. This enables NAT rules to be defined with virtual routers created on a device and successful publish and update of such rules on the device. Also Security Design supports custom routing instance route-based VPN (static routing only).
- **Variables/Polymorphic Support for Zone**—Variable Zone objects can be used within a policy to allow the zone to be interpreted per-device, allowing a single group policy to be used across devices with differing zone configurations.

In Security Design 11.4, variables are supported only in addresses. Security Design 12.1 supports variables in zones also.

- **IPS Manual Mode**—A new configuration mode, Manual, is added to the existing IPS configuration modes allowing firewall and IPS policies to be managed completely independently. This mode will turn IPS on or off and give the user the ability to customize the IPS policy. An empty container for this IPS policy is created in the IPS Management workspace. You must manually add the IPS policy rules for these IPS policies. You can also add more IPS policy rules manually.
- **General IPS Update**—IPS policies can be published similar to firewall and NAT policies. During the firewall policies publish, you have an option to include IPS policies as well.
- **Duplicate Objects**—Security Design enables you to find duplicate address or service objects and take the following actions with the duplicate objects:
 - Merge the duplicate objects
 - Delete duplicate objects
 - Find the usage of duplicate objects
- **Show Object Value Information and Group Object Counts**—Tooltip view is available to show the object value information for the objects that you are using within the policies. Mouse over the source address or destination address to see in the tool tip. The tooltip contains address group name, values of the address such as IP, and subnet.
- **Filter Devices to Show Policy Presence**—To ease the process of identifying device exceptions to group policies, an option was added to the firewall policy workspace to allow policies which do not have any rules defined to be hidden. In the firewall policy workspace, you can hide the policies in the left pane that do not have any defined rule.
- **Rule Copy and Paste**—You can copy and paste rules in a firewall policy.
- **Promote Device Policy to Group**—In the firewall policy workspace, a device policy can be promoted to a group policy. A device policy is added to the existing group policy.

Known Issues

- When you upgrade Security Design from 11.4 to 12.1, the existing Advanced mode IPS policy configuration is converted to Express mode. 5 tuples will be reset to 'Any' and IPS rules added by you will be truncated.
- Junos 12.1 schema for SRX must be installed to support the User or Role Policy feature in a firewall policy.
- Removal of roles which are manually added into Security Design role table is not supported currently.
- In the firewall policy workspace, the preview configuration for a published policy that includes IPS does not show that IPS configuration. [PR 748307]
- A NAT address pool can contain only 8 addresses (references or IP). However, a device permits references to an address group, which can contain more than 8 members. If you import and update such a configuration, the update will fail because you will be attempting to publish a NAT pool with more than 8 addresses.
- If you click any workspace on the top platform taskbar (Policy, VPN, Object Builder, and so on) during a save, the save fails without displaying any warning message.
- You cannot edit the External Interface column in a VPN if the Protected Networks/Zone cell of the same row is expanded and more than one page. [PR 706402]

Workaround: Collapse the Protected Networks/Zone cell by clicking **Less** and then editing the External Interface column.

- In the NSM global domain pre and post rules, if install-on setting is configured for any other sub domains, those firewall policy rules will be migrated to Security Design as rules in the group policy for the NSM global policy.

Rules having the install-on settings for sub domains are not created within the respective migrated group policy, but instead, it is created within Security Design group policy representing the NSM global policy. [PR 773985]

- Domain rule migration of NAT is not supported. In NSM, domain rules are used only for firewall policies though NSM has the provision to create NAT policies.
- Rule set name is lost when the rule set is imported from a device or NSM and updated to the same device again.

Any NAT rule (source or destination or static) that is imported from a device to Security Design and updated to the same device again, Security Design deletes the existing rule set and recreates a new rule set name.

- NAT Policies imported from device which has proxy-ARP configured, and do republish update to same device would delete the proxy-ARP configuration from a device.
- When you uncheck the export default-route option and change the option to export static and OSPF or RIP routes for a hub device, update fails to delete the default route policy-option. [PR 771398]

Workaround: When unselecting export default option and selecting other export options (static, OSPF, or RIP), you must manually delete *term* from a device and paste the CLI

for other export options. The next update will pass because you have already deleted the export default option, and added new options under *term*.

- If VPN name is changed for a policy-based VPN, the changed name is not reflected in the policy rule-action. It still shows the old VPN name. However, publish takes the new name. [PR 780123]
- Security Design depends on the device change notification service to detect **out of band** CLI changes and Security Design updated changes, on a device. Because of a bug in differential calculation, Security Design does not receive these device change notifications, if and only if a scalar knob is changed in the device configuration either out of band or updated from Security Design. This causes the following issues in Security Design:
 - Security Design is not able to properly report device changes for **out of band** CLI changes of these nodes.
 - If device is in *device changed* mode, any update from Security Design which includes only such nodes, Security Design includes those changes also as a device change differential.

These issues do not occur if the changes include both scalar and non-scalar nodes. For example, scalar nodes such as permit|deny|reject action of firewall policy, destination-nat-translation/[off|interface] of destination NAT, and criteria. [PR 780709]

- The static route command is not complete for the route-based VPN having extranet device as an end point. The command is configured on SRX endpoint as “set routing-options static route”, and update will pass. But, you must manually add the routing options.
- If you upgrade Security Design from 11.4 to 12.1, all the migrated VPN from 11.4, must be republished.
- For the logical systems VPNs, host-inbound services of the external interface is not updated to permit IKE. You must manually configure it. [PR 776412]
- When you use routing instance in the destination pool, update is failing for a device running Junos OS Release 12.1. This behavior is inconsistent with different Junos OS Releases 10.3 and later. [PR 771449] [Device side PR 773264]
- Enabling auto Proxy ARP at policy level, and disabling any specific rule is not possible. [PR 753733]
- Security Design, NAT Pool Objects ILP may not load with IE9 browser when the pools count is about 8192 imported from device. [PR 754535]
- If an IP address is configured to any interface and then that interface is assigned to any logical systems, IP address is not shown in the **Manage Device** page. [PR 768883]
- If you import a device configuration where in some of the address objects are used in NAT and some in firewall policy, and try to publish and update the policy after importing both NAT and firewall policy, Security Design deletes the address objects that are not used in the firewall policy and finally update fails.

Workaround: After importing the device configuration, publish and update NAT first. Consecutively, publish and update the firewall policy. [PR 774904]

- When designing a Numbered Tunnel VPN in Security Design, there is a setting to specify the “Number of Peer devices per tunnel”. User can choose ‘All’ (in this case single tunnel is used for all peer devices, and it works fine) or specify a numeric value to indicate number of remote devices that will share one tunnel (this option does not work for static routing). Security Design configures IPs of same subnet for all tunnel interfaces, and this creates traffic flow issues, due to incorrect entries in SRX forwarding table. [PR 782000]

Workaround: if user intended to share one tunnel for specific number of peer devices, user can create multiple VPNs with the “Number of Peer devices per tunnel” setting configured as the default ‘All’ value.

- Rule order becomes incorrect when user selects one-by-one all rules in a group and ‘ungroup rule’. [PR 782531]

Workaround: Select rule group itself and ungroup would ensure the rules ungrouped in original order to ungroup all.

- Policy compare would not show correct differential when the policies have more than one duplicate zone-pair with same rule name either in disabled state or errors (imported rules). Policy Compare would consider zone-pair, rule name as key (from-zone, to-zone and rule name) to generate the differential results. [PR 782530]
- Create multiple rules in any firewall policy. Now change the from-zone or to-zone field by selecting a specific value (say ‘trust’) for first rule. This will work fine. Then try to change the zone field on the second rule to the same value (‘trust’) which was selected on the first rule, this selection does not work. But this issue would not occur if the user tries to change the zone field on the second rule to some other value other than the one used in the first rule. This behavior is seen in drop down menu of the columns – From Zone, To Zone, Profile in the firewall policy UI.



NOTE: This does not lead to any incorrect data storage in the Security Design database and also does not impact any service provisioning

Workaround: If user wants to select and apply the same zone used in the first rule for other rules also, then the user can temporarily click on some other zone in the drop down (other than the one selected in the first policy) and then select the same zone used in the first rule (here ‘trust’) to make it work.

Related Documentation

- Network Application Platform Release Notes

Junos Space Documentation and Release Notes

For a list of related Junos Space documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .

Revision History

—

Copyright © 2012, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.