

Junos[®] Space Security Design 12.2 Release Notes

Release 12.2
November 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
Installing Security Design	2
Supported Devices	2
Supported OS Versions	3
Supported Browsers	3
Management Scalability	3
New Features	3
Known Issues	5
Junos Space Documentation and Release Notes	7
Documentation Feedback	7
Requesting Technical Support	8
Self-Help Online Tools and Resources	8
Opening a Case with JTAC	8
Revision History	9

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 and application firewall licenses.)

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

Installing Security Design

Security Design 12.2 can only be deployed on Network Application Platform Release 12.2 with patch 12.2P1.4. Install Junos Space Platform Release 12.2 and the patch 12.2P1.4 prior to installing Security Design.

For more information on the installation, refer to [Managing Junos Space Applications](#).

Supported Devices

Junos Space Security Design 12.2 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 12.2 supports Junos OS version 10.4 or 11.4 and above.
- 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 devices running Junos OS Release 11.4 and later.
- Junos OS Release 11.4 or later releases is required for AppFW feature support.



NOTE: Before you can manage an SRX Series using Security Design, ensure that the exact matching Junos schema is installed on the Junos Space Platform. If there is a mismatch, a warning message is displayed during the publish preview workflow.

Supported Browsers

Junos Space Security Design 12.2 is best viewed on the following browsers:

- Mozilla Firefox 4.0 to 10.0, and 14.0
- Chrome 17, 18, and 21
- Internet Explorer 8.0 and 9.0

Management Scalability

Junos Space Security Design was tested with a variety of customer configurations. A retail or branch configuration was tested with 10,000 devices and 100 firewall rules per device. Similarly, a datacenter scenario was tested with 10,000 rule policies, 20,000 address objects and 3,000 custom Service objects. Large rule deployment for a datacenter scenario supports 10,000 rule policy which includes 20,000 address objects; and 3000 custom service objects. Object Builder scale testing was performed with 50,000 address objects.

New Features

The Junos Space Security Design 12.2 application includes the following new features:

- **Policy and Object Locking**—Policy objects such as firewall and NAT policies support exclusive locking for editing. Objects used in the policies (Address, Service, NAT pools, and Variables) support *save as* functionality, if the objects are changed since it was open for edit.
- **Firewall Policy Versioning**—Policy versioning can be done by taking a snapshot of the policy. Snapshots for all types of policies can be created including All devices, Group, Device, and Device exceptions. This feature also supports rolling-back to a previous version, and comparing two arbitrary versions. A Snapshot is captured automatically when a policy is published.

- **Global Address Book Support for NAT Policy**—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.
- **IPS Mode Changes**—The IPS modes available in Security Design Release 12.1 (Basic, Express, Manual, and None) are simplified, and the IPS modes are now:
 - Basic—Select a signature set provided by the Juniper Networks, or a custom signature set per firewall policy, and then enable or disable IPS per rule.
 - Advanced—Configure a complete IPS policy for the corresponding firewall policy.
 - None—IPS is disabled for every rule in the firewall policy.
- **Usability Improvements**—Many usability improvements are made in object builder, policies, search, and publish and update.

The usability improvements in Object Builder are:

- Show unused addresses, and services
- Delete all unused addresses and services
- Replace addresses or services with another address or service
- Find address and service usage

The usability improvements in firewall and NAT policies are:

- Advanced search options to search for specific fields.
- Expand all and collapse all rule sets.
- Ignore inherited policies in compare policy.
- Rule group name change in import policy from device (firewall policy only).

The usability improvements in publish and update workflow is:

- Warning for out of band changes
- **Proxy ID in VPN**—Proxy ID is supported for both route-based and policy-based VPNs. Security Design supports only a single proxy ID.
- **NAT IPv6**—Similar to IPv4 NAT functionality, Security Design supports IPv6 NAT with source NAT, destination NAT, and static NAT functions. Also, IPv6 address is supported in persistent NAT.
- **NAT Ruleset**—Security Design automatically generates the ruleset names for source NAT, destination NAT, and static NAT rules. Automatically generated ruleset names consist of alphabets, numbers, underscore, and hyphen.
- **Selection of Externally Configured (not by SD) Policy-Based VPN in Firewall Rule**—In addition to the VPNs created and managed from Security Design, you can select a policy-based VPN on an SRX Series that was not created by Security Design.
- **Consolidated Configuration Device Update**—A consolidated configuration is a collection of pending configurations created for one or more devices by using Junos

Space applications or the Junos Space Network Application Platform. The main purpose of collecting them is to review them all in a device-centric view, and then potentially to deploy them to one or more devices in a single commit.

- **Import Enhancement**—Firewall rules are not disabled if IPS policy, policy-based VPN, or AppFW is configured during the device import.
- The following new permit actions are added for the policy:
 - Service offload
 - Destination address translation

Known Issues

- In the firewall policy workspace, the preview configuration for a published policy that includes IPS does not show that IPS configuration. [PR 748307]
- After the upgrade, the policy IDs are shown in the pending services column instead of the policy names, and for VPNs, no VPN name is displayed.

Workaround: To display the policy and VPN names in the pending services, you must republish the published policies and VPNs.

- 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.
- 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.

Workaround: Enable auto proxy-ARP when modifying the NAT policy.

- 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*.

- 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.

- 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 pool count is about 8192 imported from device. [PR 754535]
- 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 policy and NAT configurations from the device, you must publish both policy and NAT together. Then update works fine. [PR 774904]

- After upgrade from Security Design Release 12.1, group policy having IPS mode as None, with device exception having IPS mode as Basic or Advanced, is not shown on the left hand side tree of IPS policy.

Workaround: Modify the policy, change the IPS mode and save.

- During the device import or the NSM migration of large policies, job failure might happen because of transaction time out.

Workaround:

- In the Junos Space server console, go to /usr/local/jboss/server/all/conf/jboss-service.xml. In this file, navigate to the following snippet:

```
<!-- JBoss Transactions JTA -->
<mbean code="com.arjuna.ats.jbosstx.jta.TransactionManagerService"
  name="jboss:service=TransactionManager">
  <attribute name="TransactionTimeout">1800</attribute>
  <attribute
    name="ObjectStoreDir">${jboss.server.data.dir}/tx-object-store</attribute>
</mbean>
```

- Increase the transaction time out value to 3600 (depending upon the number or size of the imported or migrated policies).
- Restart the jboss by triggering **service jboss restart** command.
- If you unlock your own policy from Manage Policy Locks page, the page does not refresh automatically.

Workaround: Manually refresh the Manage Policy Locks page.

- When IPS installation fails with any of the following two errors, the Signature DB version does not get refreshed in the Install Configuration page.

- Upgrade IPS/Application Signature Succeeded version (21xx), But Loading IPS policy failed, Response from device:failed
- Install on device srx2-210h failed. Installation has exceeded the timeout of (max 30) mins, Please check your install status manually

Workaround: Click probe for the list to refresh.

- After IPS policy update, even if commit succeeds, policy compilation may fail. In Security Design Release 12.2, Security Design does not check the status of policy compilation.

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.