JUNIPER NETWORKS

Junos® OS

IDP Series Appliance to SRX Series Services Gateway Migration Guide

Release
15.1X49-D670

Modified: 2016-11-23

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS IDP Series Appliance to SRX Series Services Gateway Migration Guide
15.1X49-D670

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and 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/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- vSRX
- SRX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software 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 Partner Support Service 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: http://kb.juniper.net/InfoCenter/
- 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.

PART 1

Overview

CHAPTER 1

Introduction to the Intrusion Prevention System

IDP Series Appliances to SRX Series Devices Migration Overview

This topic provides a brief overview of some basic considerations when moving from standalone Juniper Networks IDP Series Intrusion Detection and Protection Appliances or Juniper Networks ISG Series Integrated Security Gateways with IDP security module to the Juniper Networks SRX Series Services Gateways.

Introduction

SRX Series devices are equipped with full security and networking capabilities and represents the highest performing firewalls with natively integrated full intrusion prevention system (IPS) technology from Juniper Networks IDP Series Intrusion Detection and Prevention Appliances, providing inline protection against current and emerging threats throughout the network.

Although an SRX Series IDP policy can be configured entirely from within Juniper Networks J-Web software, this document focuses primarily on the CLI, Juniper Networks Network and Security Manager (NSM) and Junos Space Security Director configuration steps, with the intention of providing an easy transition and learning path for both system engineers new to the IDP Series and those already familiar with managing standalone IDP Series and ISG Series with IDP solutions.

NSM is the sole means for configuring and managing the IDP security policy on Juniper Networks ISG Series Integrated Security Gateways with IDP security module and standalone IDP Series sensors running IDP 4.x and above.

Because standalone IDP Series devices are typically deployed in either sniffer or transparent mode, additional considerations regarding network design must be addressed. These involve:

- Network interfaces configuration
- Security zones configuration

In addition, there are considerations regarding the following security features:

- Denial of service (DoS) and flood protection.
- Traffic anomaly detection or screens (as well as some of the detection methods applicable for SRX Series devices).
- Configured settings and actions must be closely analyzed because adding a new device can potentially impact network traffic—particularly in regard to Layer 3 processing.

SRX Series Services Gateways can be deployed in inline mode and sniffer mode (only high-end SRX Series devices). The sniffer mode is not supported on branch SRX Series devices.

Multimethod Detection

SRX Series devices deploy two rulebases—a main IDP rulebase and an exempt rulebase.

In addition, SRX Series devices use security zones that are based on technology available with ScreenOS-based security devices, and provide detailed screen protection as an alternative for some basic standalone detection methods or rulebases.

Logging

Logging on an SRX Series device must be configured to send records in response to security events through system logging to a preconfigured syslog server, such as the Juniper Networks Juniper Secure Analytics (JSA).

Sensor Configuration Settings

On both standalone IDP Series and SRX Series devices, a number of sensor configuration settings can be configured to fine-tune IDP Series behavior and can be accessed from the CLI, Juniper Networks Network and Security Manager (NSM) and Junos Space Security Director (SD). If any of the settings have been changed from the default value or need to be further modified, you must manually modify them. There are no automated processes to export or import modified settings.

Key Points to Consider

Note the following key points when you migrate from IDP Series Appliances to SRX Series devices:

- In comparison with deep inspection on ScreenOS, the fundamental IPS detection capabilities on the SRX Series devices do not differ from that available on IDP Series Appliances or ISG Series with IDP security modules.
- Not all IPS features are available on SRX Series IDP. We recommend that you familiarize yourself with documentation that details those differences.
- SRX Series devices are inline devices, and only SRX Series high-end devices can be configured in sniffer mode (transparent mode).
- IPS does not need a separate license to run as a service on the SRX Series device; however, a license is required for IPS updates.
- A base firewall policy is required and needs to include an IPS application-service statement to enable IPS inspection.
- Enabling all attacks is not supported. If the policy does not load, check the service log files for policy size and load results.
- NSM 2008.2 requires 2 gigabytes of RAM.
- To push the policy from NSM successfully, both NSM and the SRX Series device have to be at the same detector version level, and any device mismatch information has to be reconciled.
- A system log (syslog) server is required to collect security event-related messages when the messages are identified on the SRX Series data plane.
- It is s important to understand that compiling and applying an IPS policy can take some time, depending on the number of attack objects and the size of the policy. Starting with Junos OS Release 12.1, SRX Series devices are leveraged for smarter compilation engine along with caching compiled information so that the compilation process takes much less time. The compilation process is conducted asynchronously, which means that the SRX Series device starts the process but will not hold up CLI, NSM, or SD session, but instead will allow you to check back later on the status.

Related Documentation

- Understanding Intrusion Prevention System for SRX Series Devices on page 5
- Installing the IPS License (CLI) on page 13

Understanding Intrusion Prevention System for SRX Series Devices

Overview

The Juniper Networks intrusion prevention system (IPS) feature detects and prevents attacks in network traffic.

SRX Series devices provide the IPS functionality integrated within the Junos OS software; no special hardware is needed. IPS administrators have the option of deploying and administering IPS using the CLI, Juniper Networks Network and Security Manager (NSM), or the Junos Space Security Director.

IPS Architecture

The IPS architecture is composed of the following:

- SRX Series device with IPS—IPS functionality is integrated as part of Junos OS and no special hardware is required.
- Management—SRX Series devices can be fully managed using the CLI commands. However, if there are multiple SRX Series devices involved in the IPS deployment, we recommend using the JJuniper Networks Network and Security Manager (NSM) or Junos Space Security Director application.
- Logging—Juniper Secure Analytics (JSA) is Juniper Networks' security information and event management (SIEM) solution. JSA has predefined dashboards and reports for the SRX Series devices IPS solution. In addition to logging, JSA provides event correlation, incident management, and flow monitoring. SRX Series logs are in syslog (structured data syslog) format, and these can be sent to JSA or to any other syslog servers that users might already have in place.

IPS with Chassis Clustering Limitations

IPS is supported in both active/passive and active/active chassis cluster modes on both branch and high-end SRX Series devices with the following limitations:

- No inspection is performed on sessions that fail over or fail back. Only new sessions after a failover are inspected by IPS, and older sessions become firewall sessions.
- The IP action table is not synchronized across nodes. If an IP action is taken for a session, and the source IP, destination IP or both is added to the IP action table, this information is not synchronized to the secondary node. Therefore, the sessions from the source IP, destination IP or both will be forwarded until a new attack is detected.
- The SSL session ID cache is not synchronized across nodes. If an SSL session reuses a session ID and it happens to be processed on a node other than the one on which the session ID is cached, the SSL session cannot be decrypted and will be bypassed for IPS inspection.

Related Documentation

- IDP Series Appliances to SRX Series Devices Migration Overview on page 3
- *Intrusion Detection and Prevention Feature Guide for Security Devices*

Understanding the Intrusion Prevention System Deployment Modes for SRX Series Devices

This topic provide you an overview of the different types of IPS deployment modes for SRX Series devices.

IPS provides three different modes of deployment:

- Integrated mode
- Inline-tap mode
- Sniffer mode

Integrated Mode

Integrated mode is supported on both branch and high-end SRX Series devices. Integrated mode is the default mode in which IPS operates on the SRX Series devices (There are no specific indications that show that the device is in integrated mode.)

NOTE: We recommend deploying IPS in integrated mode.

Inline-Tap Mode

Junos OS Release 10.2 and later supports Inline-tap mode only on high-end SRX Series devices.

The main purpose of inline-tap mode is to provide best-case deep inspection analysis of traffic while maintaining overall performance and stability of the device. When a device is in inline-tap mode, the firewall process (flowd) processes the firewall traffic as normal, but makes a copy of the packet and puts it in a queue for the independent IPS module (idpd) to inspect. In the meantime, flowd forwards the original packet without waiting for idpd to perform the inspection.

Because inline tap mode puts IPS in a passive mode for inspection, preventative actions such as close, drop, and mark diffserv are deferred. The drop packet action is ignored.

NOTE: In inline-tap mode, the SRX Series device with IPS provides minimum protection. Upon detecting an attack, idpd can reset a session, but by the time the reset occurs, flowd would have allowed malicious packets through the network.

Sniffer Mode

Sniffer mode is supported only on high-end SRX Series devices. You can use the sniffer mode of IPS deployment by configuring the interfaces in promiscuous mode and manipulating the traffic and flow setup with routing.

On all high-end SRX Series devices, in sniffer mode, ingress and egress interfaces work with flow showing both source and destination interface as egress interface.

As a workaround, in sniffer mode, use the tagged interfaces. Hence, the same interface names are displayed in the logs. For example, ge-0/0/2.0 as ingress (sniffer) interface and ge-0/0/2.100 as egress interface are displayed in the logs to show the source interface as ge-0/0/2.100.

```
set interfaces ge-0/0/2 promiscuous-mode
set interfaces ge-0/0/2 vlan-tagging
set interfaces ge-0/0/2 unit 0 vlan-id 0
set interfaces ge-0/0/2 unit 100 vlan-id 100
```

Related Documentation

- IDP Series Appliances to SRX Series Devices Migration Overview on page 3
- Understanding Intrusion Prevention System for SRX Series Devices on page 5
- Installing the IPS License (CLI) on page 13

Getting Started with IPS on SRX Series Devices

Before configuring the SRX Series device for IPS functionality, perform the following tasks:

1. **Install the License**—You must install an IDP license before you can download any attack objects. If you are using only custom attack objects, you do not need to install a license, but if you want to download Juniper Networks predefined attack objects, you must have this license. Juniper provides you with the ability to download a 30-day trial license to permit this functionality for a brief period of time to evaluate the functionality. All you need is run the **request system license add** command either specifying a file storage location or copy and paste it into the terminal.
2. **Configure Network Access**—Before you can download the attack objects, you must have network connectivity to either the Juniper download server or a local server from which the signatures can be downloaded. This typically requires network configuration (IP/Netmask, routing, and DNS) and permitted access to reach the server. At the time of this writing, HTTP proxies are not supported, but you can configure a local webserver from which to serve the files.
3. **Download Attack Objects**—Before deploying the IPS, you must first download the attack objects from which the policy will be compiled. Triggering a manual download does not configure the SRX Series device to download them in the future, so you must configure automatic updates to download them.
4. **Install Attack Objects**—Once the download has been completed, you must install the attack updates before they are actually used in a policy. If you already have a policy configured, you do not need to recommit the policy—installing the updates adds them to the policy. The installation process compiles the attack objects that have been downloaded to a stage directory into the configured policy.
5. **Download Policy Templates (optional)**—You can optionally download and install predefined IPS policies known as policy templates provided by Juniper to get started.

After finishing this chapter, you should be able to configure your own policy, so you probably will not need policy templates.

NOTE: Starting with Junos OS Release 12.1, the SRX Series devices automatically push the signature package to the secondary member of the chassis cluster. Prior to Junos OS Release 12.1, you had to use the fxp0 on both members of the cluster because both members had to download their own instance. With 12.1 and beyond, there is no explicit configuration. SRX Series device will download the signature package and push it to the secondary member during the download process.

Related Documentation

- IDP Series Appliances to SRX Series Devices Migration Overview on page 3
- Understanding Intrusion Prevention System for SRX Series Devices on page 5
- Understanding the Intrusion Prevention System Deployment Modes for SRX Series Devices on page 7

PART 2

Configuration

CHAPTER 2

IPS Configuration

Installing the IPS License (CLI)

You can either download an IPS license from the license server, or manually install IPS if you received a license from Juniper Networks.

Access the SRX Series device console through the serial cable plugged into the console port on the device or by using a terminal session such as SSH.

To apply your IPS subscription license to the device, use the following CLI command:

```
user@host> request system license update
```

If you received a license for manual installation, perform the following tasks:

1. Access the SRX Series Services Gateway console either by plugging the serial cable into the console port on the device or by using a terminal session such as SSH.
2. Check for an IPS license (required for all IPS updates):

   ```
   user@host> show system license
   ```

   ```
   License usage:
                                  Licenses     Licenses    Licenses    Expiry
     Feature name                        used    installed      needed
     logical-system                         0          0           0    permanent
   ```

3. If there are no licenses installed, obtain the chassis serial number by using the following CLI command:

   ```
   user@host> show chassis hardware
   ```

4. A serial number is needed to generate the IPS license. You can add a license key from a file or URL or from the terminal.

   - From a file or URL:

     ```
     user@host> request system license add <file name>
     ```

- From the terminal:

  user@host> request system license add terminal

5. When prompted, enter the license key, separating multiple license keys with a blank line. If the license key you enter is invalid, an error is generated when you press Ctrl-D to exit license entry mode.
6. Verify the system license by entering the **show system license** command.

   user@host> show system license

```
License usage:
                    Licenses     Licenses    Licenses   Expiry
  Feature name         used    installed      needed
  idp-sig               4            1           0  permanent


Licenses installed:
  License identifier: JUNOS208639
  License version: 2
  Valid for device: AA4508AD0005
  Features:
    idp-sig   - IDP Signature
     date-based, 2009-0406 08:00:00 GMT-8 - 2010-04-06 08:00:00 GMT-8
```

Related Documentation

- IDP Series Appliances to SRX Series Devices Migration Overview on page 3
- Understanding Intrusion Prevention System for SRX Series Devices on page 5

Initial Configuration Overview

Enabling a fully functional IPS service on SRX Series Services Gateways includes the following basic configuration steps:

Basic Configurations

1. Configure basic networking, security, and access components (in most cases this will already be configured).
2. Configure and activate IPS policy.
3. Configure firewall policy to associate specific rules with IPS.
4. Download attack objects including sensor updates.
5. Configure logging.
6. Update security-package.
7. Verify configuration and test functionality.

Initial Configuration Assumptions

Before starting the IPS policy configuration, this document assumes that an initial networking configuration exists and that an admin user has full access to the SRX Series. Initial device configuration on our sample system is as follows:

```
user@ost > show configuration | display set
set system root-authentication encrypted-password “$ABC123”
set system name-server 1.2.3.4
set system login user mxb uid 2000
set system login user mxb class super-user
set system login user mxb authentication encrypted-password “$123ABC”
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set interfaces fxp0 unit 0 family inet address 192.168.1.221/24
set routing-options static route 0.0.0.0/0 next-hop 192.168.1.1
set security idp security-package url https://services.netscreen.com/cgi-bin/index.cgi
```

NOTE: Throughout this document we provide commands required to configure specific features; however, in order to activate associated functionality, configuration changes need to be successfully committed (using the commit command).

Related Documentation

- IDP Series Appliances to SRX Series Devices Migration Overview on page 3
- Understanding Intrusion Prevention System for SRX Series Devices on page 5
- Understanding the Intrusion Prevention System Deployment Modes for SRX Series Devices on page 7

IPS Configuration (CLI)

Configuring Interfaces

1. Display current interfaces (assumption is interfaces have been properly cabled)

```
user@host# configure
fxp0 {
   unit 0 {
      family inet {
         address 192.168.1.221/24;
      }
   }
}

[edit]
user@host# run show interfaces | match ge-0/0
Physical interface: ge-0/0/0, Enabled, Physical link is Down
```

```
Physical interface: ge-0/0/1, Enabled, Physical link is Down
Physical interface: ge-0/0/2, Enabled, Physical link is Up
Physical interface: ge-0/0/3, Enabled, Physical link is Up
Physical interface: ge-0/0/4, Enabled, Physical link is Down
Physical interface: ge-0/0/5, Enabled, Physical link is Down
Physical interface: ge-0/0/6, Enabled, Physical link is Down
Physical interface: ge-0/0/7, Enabled, Physical link is Up
Physical interface: ge-0/0/8, Enabled, Physical link is Down
Physical interface: ge-0/0/9, Enabled, Physical link is Down
Physical interface: ge-0/0/10, Enabled, Physical link is Down
Physical interface: ge-0/0/11, Enabled, Physical link is Down
```

2. Configure forwarding interfaces as shown in "Configuring the IPS Policy on SRX Series Devices Using NSM" on page 21.

```
user@host# set interfaces ge-0/0/2 unit 0 family inet address 33.3.3.1/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 44.4.4.1/24
```

3. Verify the configuration.

```
user@host# run show interfaces terse | match /24
```

```
ge-0/0/2.0  up up inet 33.3.3.1/24
    ge-0/0/3.0 up up inet 44.4.4.1/24
     ge-0/0/7.0 up up inet 192.168.2.222/24
    fxp0.0     up up inet 192.168.1.221/24
```

Configuring Security Zones

1. Configure security zones.

   a. Display existing zones:

```
user@host> show security zones
```

```
Security zone: junos-global
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 0
Interfaces:
```

   b. Configure zones abc-trust and abc-untrust and assign interfaces accordingly.

```
user@host# set security zones security-zone abc-trust interfaces ge-0/0/2
user@host# set security zones security-zone abc-untrust interfaces ge-0/0/3
```

2. Verify the configuration.

```
user@host# run show security zones
```

```
Security zone: abc-trust
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
ge-0/0/2.0

Security zone: abc-untrust
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
ge-0/0/3.0
```

```
Security zone: junos-global
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 0
Interfaces:
```

Configuring IPS Security Policy

1. Configure IPS policy abc-idp-policy.

   The simple configuration in this section involves setting up one rule looking for all critical attacks and, in case a match is found, dropping the associated connection, setting that event as critical and logging it with an alert. The second rule is configured to look for major attacks and to perform a recommended action upon detecting a severe attack, as well as logging the event.

   NOTE: Logging means sending a system log (syslog) message to an appropriate, preconfigured syslog server. Logging configuration steps are provided in subsequent sections.

   ```
   user@host> set security idp idp-policy abc-idp-policy rulebase-ips rule 1
     match from-zone any to-zone any source-address any destination-address
     any application any attacks predefined-attack-groups Critical
   user@host> set security idp idp-policy abc-idp-policy rulebase-ips rule 1
     then severity critical notification log-attacks alert
   user@host> set security idp idp-policy abc-idp-policy rulebase-ips rule 1
     then severity critical notification log-attacks alert
   user@host> set security idp idp-policy abc-idp-policy rulebase-ips rule 2
     match from-zone any to-zone any source-address any destination-address
     any application any attacks predefined-attack-groups Major
   user@host> set security idp idp-policy abc-idp-policy rulebase-ips rule 2
     then action recommended
   user@host> set security idp idp-policy abc-idp-policy rulebase-ips rule 2
     then severity major notification log-attacks
   ```

2. Verify IPS policy abc-idp-policy.

   ```
   user@host> show security idp idp-policy abc-idp-policy
   rulebase-ips {
     rule 1 {
       match {
         from-zone any;
         source-address any;
         to-zone any;
         destination-address any;
         attacks {
           predefined-attack-groups Critical;
         }
       }
       then {
         action {
           drop-connection;
         }
         notification {
   ```

```
            log-attacks {
              alert;
            }
          }
          severity critical;
        }
      }
      rule 2 {
        match {
          from-zone any;
          source-address any;
          to-zone any;
          destination-address any;
          attacks {
            predefined-attack-groups Major;
          }
        }
        then {
          action {
            recommended;
          }
          notification {
            log-attacks;
          }
          severity major;
        }
      }
    }
```

3. Set trace options.

   a. To provide detailed IPS process event information (policy compilation result, policy loading results, dfa matches, and so on) which allows for further system analysis, tuning, and easier troubleshooting, it is highly recommended to enable trace options. The following is an example setting that configures trace to write all security events encompassing all debug levels (error, info, notice, verbose, and warning). The trace filename is not specified trace if it is not written into the file named after the process being traced, which is the case with IDP/var/log/idpd:

      ```
      user@host> set security idp traceoptions flag all
      user@host> set security idp traceoptions level all
      ```

   b. For this example, we limit the file size to 100 MB. This means that the process will write this file and once it reaches 100 MB, it will rename it to idpd.0 and continue with a new idpd. The default number of files is 3 and if file numbers are exhausted, the oldest file (idpd.2) gets overwritten.

      ```
      user@host> set security idp traceoptions file size 100M
      ```

4. Verify trace options settings.

   ```
   user@host> show security idp traceoptions
   ```

   ```
   file size 100m;
   flag all;
   level all;
   ```

5. Activate IPS Series policy.

   user@host> set security idp active-policy abc-idp-policy

6. Verify active IPS policy.

   user@host> show security idp active-policy

```
active-policy abc-idp-policy;
```

NOTE: To deploy IPS policy on the SRX Series devices, one more step is required—configuring firewall security policy to identify which traffic is to be processed by the IPS service. This is described in the following section.

Configuring Firewall Security Policy

For traffic entering the SRX Series device to be processed by IPS security policy firewall, the security policy needs to be configured accordingly.

Following are steps required to configure firewall security policy and finalize Intrusion Prevention System configuration on the SRX Series gateway. This will result in traffic between security zones abc-untrust and abc-trust being inspected by IPS security policy abc-idp-policy.

1. Ensure that the system is configured with the default policy denying all traffic. This basically means traffic will 1. be denied throughout the gateway unless specifically allowed to by firewall security policy.

   user@host> show security policies

```
Default policy: deny-all
```

2. Configure policy.

   user@host> set security policies from-zone abc-untrust to-zone abc-trust policy abc match source-address any destination-address any application any
   user@host> security policies from-zone abc-untrust to-zone abc-trust policy abc then permit application-services idp
   user@host> set security policies from-zone abc-trust to-zone abc-untrust policy abc match source-address any destination-address any application any
   user@host> set security policies from-zone abc-trust to-zone abc-untrust policy abc then permit application-services idp

3. Verify configuration.

```
user@host> show security policies
from-zone abc-untrust to-zone abc-trust {
  policy abc {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
```

```
                idp;
              }
            }
          }
        }
      }
      from-zone abc-trust to-zone abc-untrust {
        policy abc {
          match {
            source-address any;
            destination-address any;
            application any;
          }
          then {
            permit {
              application-services {
                idp;
              }
            }
          }
        }
      }
```

IPS Logging

IPS generates event logs when an event matches an IPS policy rule in which logging is enabled. When you configure a rule for logging, the device creates a log entry for each event that matches that rule.

When configured to do so, an IPS service will send events that match policy entry to the logging server directly from the data plane via emulated IP address, encapsulated in 514/udp.

Configure logging:

1. Configure interface data plane to send syslog messages from:

   user@host# set interfaces ge-0/0/7 unit 0 family inet address 192.168.2.1/24

2. Choose the format (standard or structured format).

   user@host# set security log format syslog

3. Set the emulated source IP address (interface cannot be fxp0).

   user@host# set security log source-address 192.168.2.211

4. Set severity.

   user@host# set security log stream jet severity debug

5. Indicate the syslog server IP address (to which logs are sent via 514/udp).

   user@host# set security log stream jet host 192.168.2.212

6. Verify log configuration.

   user@host# show security log

```
format syslog;
source-address 192.168.2.211;
stream jet {
severity debug;
host {
192.168.2.212;
}
```

Related Documentation

- IDP Series Appliances to SRX Series Devices Migration Overview on page 3
- Installing the IPS License (CLI) on page 13
- Initial Configuration Overview on page 14
- Configuring the IPS Policy on SRX Series Devices Using NSM on page 21

Configuring the IPS Policy on SRX Series Devices Using NSM

This topic covers a basic SRX Series device IPS security policy configuration using NSM.

NOTE: This example uses the same network setup, same IPS, and same firewall security policies as described in "IPS Configuration (CLI)" on page 15.

Before you configure an IPS deployment, make sure you have:

- Identified the recommended release.
- Selected the management platform. IPS on SRX Series devices can be fully managed through the CLI, Junos Space Security Director, NSM, or J-Web. This example focuses on configuring IPS using NSM.
- Before starting the IPS policy configuration, ensure that an initial networking configuration exists and that an administrator has full access to the SRX Series device.

There are two possible approaches for configuring an SRX Series device IPS security policy with NSM.

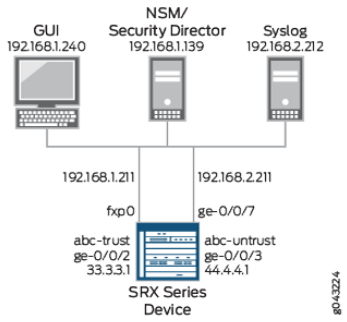
- Configure basic setup through the CLI and import the device with the policy into NSM.
- Configure both the firewall and the IPS security policy from NSM entirely from within one of the following device policy management modes:
  - Central Policy Mode (Policy at NSM level applicable to any selected device. This is the default mode.)
  - In-Device Policy Mode (Policy at device level and applicable to the actual device that is accessed and edited through the configuration details.)

NOTE: When you update the SRX Series device in Central Policy Mode, the security policy from the Policy Manager is pushed.

When you update the SRX Series device in In-Device Policy Mode, the security policy as configured under the hierarchy **security->idp->idp policy** is pushed.

The SRX Series device is imported into NSM with a CLI-based configuration.

Figure 1: SRX Series Device Deployment



- Configuring the IPS Policy by Importing the SRX Series Device into NSM on page 22
- Configuring the IPS Policy from Central Policy Mode on page 24
- Configuring the IPS Policy from In-Device Policy Mode on page 24

Configuring the IPS Policy by Importing the SRX Series Device into NSM

The following steps show how to configure an IPS policy using the CLI to set up a basic policy and import the SRX Series device with the policy into NSM:

1. Add the new device. Select **Existing** and **Not Reachable** for the device.
2. Select device specifications such as:
   - **Device Name**
   - **Color**
   - **OS Name**
   - **JUNOS OS Type**
   - **Platform**
   - **Managed OS Version**
3. Configure the SRX Series device to connect to NSM.
4. From the console, configure the SRX Series device by entering the following commands:

   ```
   user@host# set system services outbound-ssh client nsm device-id EEC4B8
   user@host# set system services outbound-ssh client nsm secret <one-time-password>
   user@host# set system services outbound-ssh client nsm 192.168.1.139 port 7804
   user@host# set system services outbound-ssh client nsm services netconf
   ```

5. Import the device.

NOTE: Importing the device by default imports it in the Central Policy Mode and, as a part of the process, imports the currently configured security policy on that device into the NSM policy tree.

If a security policy with the same name already exists in the NSM database (from a previous import), a new, incrementally numbered policy will be created at each import (SRX-host-abc-idp-policy_1, SRX-host-abc-idp-policy_2, and so on).

If there is no security policy configured on the SRX Series device, no policy will be imported and the administrator will have to configure a security policy either using the CLI or will need to configure it from NSM.

6. Configure the security policy.

   After successfully importing the device, the administrator can create a new security policy, tune or change the existing policy and then deploy changes, updates, or both by using the following standard Update Device procedure.

   This procedure describes security policy configuration and deployment through Central Policy Mode. Policy SRX-Recommended will be created (based on the Recommended security policy template) and applied to the SRX Series device.

   NOTE: If the device being imported does not match the Detector Engine information in the NSM database, the security policy update will fail.

   a. Reconcile the inventory.

      When importing a new device or performing any changes to configuration that result in a hardware or software mismatch between information stored in NSM and in the device itself, you will have to reconcile inventory. Updating the policy on the device that is out of sync will result in inventory reconcile failure.

      To bring a device in sync from the NSM:

      - Right-click the device and select **View/Reconcile Inventory**.
      - Select **Refresh**, which opens a new window and displays any mismatched items (highlighted).
      - Select **Reconcile** to update the database information. Once successful, selecting **Reconcile** again will show the inventory without any highlighted items.

   b. Update the IDP Protocol Detector Engine.

      If the IDP Protocol Detector Engine on the SRX Series device does not match the Detector Engine on the NSM prior to pushing the policy, you will need to correct this situation as follows:

      - To check the Detector Engine version installed on NSM, select **Attack Update Manager** and select **IDP-SRX Detector Engine version**.

- If the Detector Engine version does not match, a failure message is displayed when attempting to update the device.

  To fix this situation, you need to bring both NSM and the SRX Series device into sync. Although it is possible to roll back a couple of versions on the NSM, we recommend that you download and install the most recent security package from the SRX Series CLI. For more details on how to update security packages, see "Managing the IPS Signature Database (CLI)" on page 30.

Configuring the IPS Policy from Central Policy Mode

To configure the IPS policy from the Central Management Policy Mode, follow these steps:

1. Select **Firewall/VPN Devices with IDP** as the device model.
2. Select **Recommended (predefined)** policy as the template.
3. Assign the policy to the SRX Series device. A security policy with firewall and IPS rule bases is automatically created and gets associated with the SRX Series device.
4. Configure firewall zones. You can configure the policy for traffic between existing zones on the device.

   Once you are satisfied with the configuration, push your policy by right-clicking the device and selecting **Update Device**.

Configuring the IPS Policy from In-Device Policy Mode

When the device is in In-Device Policy mode, an administrator is able to configure a device-level configuration as described in the "IPS Configuration (CLI)" on page 15.

Security policy and other configuration setting changes performed through the Device Manager apply to that device only and are applied only when the device is in In-Device Policy Mode. If the device is in Central Policy Mode, these changes are not applied.

Switching from one mode to another imports the device configuration from the device into the NSM. The following steps provide an overview of how to set the security policy through the Device Manager in In-Device Policy Mode.

1. Access configuration details.
2. Configure interfaces.
3. Configure security zones.
4. Assign interfaces to security zones.
5. Create a firewall policy and associate the IPS services.
6. Select a default firewall policy.
7. Configure the IPS policy.
8. Set traceoptions.

9. Set logging.
10. Update the device.

Related Documentation

- Initial Configuration Overview on page 14
- Installing the IPS License (CLI) on page 13

PART 3

Updating the IPS Signature Database

CHAPTER 3

Downloading and Updating the IPS Signature Database

Understanding the IPS Signature Database

The signature database is one of the major components of the intrusion prevention system (IPS). It contains definitions of different objects, such as attack objects, application signature objects, and service objects, that are used in defining IDP policy rules. As a response to new vulnerabilities, Juniper Networks periodically provides a file containing attack database updates on the Juniper Networks website. You can download this file to protect your network from new threats.

NOTE: **IPS does not need a separate license to run as a service on the SRX Series device; however, a license is required for IPS updates. Custom attacks and custom attack groups in IDP policies can also be configured and installed even when a valid license and signature database are not installed on the device.**

The IPS signature database is stored on the IPS-enabled device and contains definitions of predefined attack objects and groups. These attack objects and groups are designed to detect known attack patterns and protocol anomalies within the network traffic. The IPS signature database includes more than 5000 signatures and more than 1200 protocol anomalies.

IPS updates and application signature package updates are a separately licensed subscription service. You must install the IPS signature-database-license key on your device for downloading and installing daily signature database updates from the Juniper Networks website. The IPS signature license key does not provide grace period support.

NOTE: If you require both AppSecure and IPS features, you must install the application signature license in addition to the IPS signature-database-update license key.

The signature database comprises the following components:

- Detector engine—The IDP detector engine is a dynamic protocol decoder that includes support for decoding more than 60 protocols and more than 500 service contexts. You can download the protocol detector engine updates along with the signature database updates.
- Attack database—The attack signature database stores data definitions for attack objects and attack object groups. Attack objects comprise stateful signatures and traffic anomalies. You specify attack objects in IDP rulebase rules. New attacks are discovered daily, so it is important to keep your signature database up to date. You can download the attack database updates from the Juniper Networks website.
- Application signature database—The application signature database stores data definitions for application objects. Application objects are patterns that are used to identify applications that are running on standard or nonstandard ports.

NOTE: We recommend using the latest version of the signature database to ensure an up-to-date attack database.

Related Documentation

- IDP Series Appliances to SRX Series Devices Migration Overview on page 3
- Understanding Intrusion Prevention System for SRX Series Devices on page 5
- Installing the IPS License (CLI) on page 13

Managing the IPS Signature Database (CLI)

This example shows how to install and schedule the signature database updates using the CLI.

Requirements

Before you install the signature database updates, ensure that you have installed an IPS license key.

Overview

IPS signature database management comprises the following tasks:

- Update the signature database—Download the attack database updates available on the Juniper Networks website. New attacks are discovered daily, so it is important to keep your signature database up to date.
- Verify the signature database version—Each signature database has a different version number with the latest database having the highest number. You can use the CLI to display the signature database version.
- Update the protocol detector engine—You can download the protocol detector engine updates along with the signature database. The IPS protocol detector contains Application Layer protocol decoders. The detector is coupled with the IDP policy and is updated together. It is always needed at policy update time, even if there is no change in the detector.
- Schedule signature database updates—You can configure the IPS-enabled device to automatically update the signature database after a set interval.

Configuration

Downloading and Installing the IPS Signature Package

Step-by-Step Procedure

New attacks are discovered daily, so it is important to keep your signature database up to date. In this example, you download and then install the latest signature package from the signature database server:

1. Download the attack database updates available on the Juniper Networks website:

   user@host>**request security idp security-package download**

   By default, when you download the security package, you download the following components into a Staging folder in your device: the latest version of the complete attack object groups table, the application objects table, and the updates to the IPS Detector Engine. Because the attack objects table is typically very large, by default the system only downloads updates to the attack objects table. However, you can download the complete attack objects table by using the **full-update** configuration option.

2. Check the security package download status:

   user@host>**request security idp security-package download status**

   On a successful download, the following message is displayed:

   ```
   Done;Successfully downloaded from
   (http://services.netscreen.com/cgi-bin/index.cgi).
   Version info:1884(Thu Mar 17 12:06:35 2011, Detector=11.4.140110223)
   ```

3. After downloading the security package, you must install the package to update the security database with the newly downloaded updates from the Staging folder in your device. Install the security package:

   user@host>**request security idp security-package install**

4. Check the status of the install:

   user@host>**request security idp security-package install status**

   On a successful install, the following message is displayed:

```
Done;Attack DB update: successful - [UpdateNumber=1884,ExportDate=Thu Mar
17 12:06:35 2011,Detector=11.4.140110223]
 Updating control-plane with new detector: successful
 Updating data-plane with new attack or detector: successful
```

Verifying the Signature Database Version

Step-by-Step Procedure

Each signature database has a different version number with the latest database having the highest number.

- Use the CLI to verify the signature database version installed:

  user@host>**show security idp security-package version**

  The following sample output shows the version number for the signature package:

```
user@host> show security idp security-package-version
Attack database version:1883(Wed Mar 16 12:10:26 2011)
Detector version :12.6.140121210
Policy template version :N/A
```

Scheduling the Signature Database Updates

Step-by-Step Procedure

You can configure an IPS-enabled device to automatically update the signature database after a set interval. After the initial manual setup, we recommend that you schedule the signature updates so you always have protection against new vulnerabilities.

- To schedule the signature package download, from configuration mode, specify the start time and the interval for the download:

  user@host>**set security idp security-package automatic interval *interval* start-time <YYYY-MM-DD.HH:MM:SS>**

  For example, to set a schedule for the signature download every 72 hours, you use the following configuration:

  user@host>**set security idp security-package automatic interval 72 start-time**

Verification

To confirm that the configuration is working properly, perform this task:

- Verifying the IPS Signature Database on page 32

Verifying the IPS Signature Database

Purpose Display the IPS signature database.

Action From operational mode, enter the **show security idp** command.

Related Documentation

- Understanding Intrusion Prevention System for SRX Series Devices on page 5
- Understanding the IPS Signature Database on page 29
- Managing the IPS Signature Database (Security Director) on page 33

Managing the IPS Signature Database (Security Director)

This example shows how to install and schedule the signature database updates using Junos Space Security Director.

Requirements

This example uses the following hardware and software components:

- SRX Series device

Before you install the signature database updates, ensure that you have:

- Installed an IPS license key

Overview

The IPS signature database can be updated using either the CLI or Junos Space Security Director. SRX Series devices can be fully managed from the CLI; however, for large deployment scenarios that use multiple SRX Series devices, it is easier to manage the security package using a management platform.

Configuration

Downloading and Installing the IPS Signature Package

Step-by-Step Procedure

In this example, you download and then install the latest signature package from the signature database server:

1. Navigate to **Security Director->Downloads->Signature Database**.

   Choose the signature package listed as the latest and select **Action>Download** to download the signature package to Security Director.

   ```
   user@host>request security idp security-package download
   ```

By default, when you download the security package, you download the following components into a Staging folder in your device: the latest version of the complete attack object groups table, the application objects table, and the updates to the IPS Detector Engine. Because the attack objects table is typically very large, by default the system only downloads updates to the attack objects table. However, you can download the complete attack objects table by using the **full-update** configuration option.

2. Check the security package download status:

   user@host>**request security idp security-package download status**

   On a successful download, the following message is displayed:

   ```
   Done;Successfully downloaded from
   (http://services.netscreen.com/cgi-bin/index.cgi).
   Version info:1884(Thu Mar 17 12:06:35 2011, Detector=11.4.140110223)
   ```

3. After downloading the security package, you must install the package to update the security database with the newly downloaded updates from the Staging folder in your device. Install the security package:

   user@host>**request security idp security-package install**

4. Check the status of the install:

   user@host>**request security idp security-package install status**

   On a successful install, the following message is displayed:

   ```
   Done;Attack DB update: successful - [UpdateNumber=1884,ExportDate=Thu Mar
   17 12:06:35 2011,Detector=11.4.140110223]
    Updating control-plane with new detector: successful
    Updating data-plane with new attack or detector: successful
   ```

Verifying the Signature Database Version

Step-by-Step Procedure

Each signature database has a different version number with the latest database having the highest number.

- Use the CLI to verify the signature database version installed:

  user@host>**show security idp security-package version**

  The following sample output shows the version number for the signature package:

  ```
  user@host> show security idp security-package-version
  Attack database version:1883(Wed Mar 16 12:10:26 2011)
  Detector version :12.6.140121210
  Policy template version :N/A
  ```

Scheduling the Signature Database Updates

Step-by-Step Procedure

You can configure IPS-enabled device to automatically update the signature database after a set interval. After the initial manual setup, we recommend that you schedule the signature updates so you always have protection against new vulnerabilities.

- To schedule the signature package download, from configuration mode, specify the start time and the interval for the download:

```
user@host>set security idp security-package automatic interval interval start-time
  <YYYY-MM-DD.HH:MM:SS>
```

For example, to set a schedule for the signature download every 72 hours, you use the following configuration:

```
user@host>set security idp security-package automatic interval 72 start-time
```

Verification

To confirm that the configuration is working properly, perform this task:

- Verifying the IPS Signature Database on page 35

Verifying the IPS Signature Database

Purpose Display the IPS signature database.

Action From operational mode, enter the **show security idp** command.

Related Documentation

- Understanding Intrusion Prevention System for SRX Series Devices on page 5
- Understanding the IPS Signature Database on page 29
- Managing the IPS Signature Database (CLI) on page 30

Example: Updating the IPS Signature Database Manually

This example shows how to update the IPS signature database manually.

Requirements

Before you begin, configure network interfaces.

Overview

Juniper Networks regularly updates the predefined attack database and makes it available as a security package on the Juniper Networks website. This database includes attack object and attack object groups that you can use in IDP policies to match traffic against known attacks.

In this example, you download the security package with the complete table of attack objects and attack object groups. Once the installation is completed, the attack objects and attack object groups are available in the CLI under the **predefined-attack-groups** and **predefined-attacks** configuration statements at the **[edit security idp idp-policy]** hierarchy level. You create a policy and specify the new policy as the active policy. You only

download the updates that Juniper Networks has recently uploaded and then update the attack database, the running policy, and the IPS protocol detector with these new updates.

Configuration

CLI Quick Configuration

CLI quick configuration is not available for this example, because manual intervention is required during the configuration.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To manually download and update the signature database:

1. Specify the URL for the security package.

   ```
   [edit]
   user@host#set security idp security-package url
     https://services.netscreen.com/cgi-bin/index.cgi
   ```

   NOTE: By default it will take URL as https://services.netscreen.com/cgi-bin/index.cgi.

2. Commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

3. Switch to operational mode.

   ```
   [edit]
   user@host# exit
   ```

4. Download the security package.

   ```
   user@host>request security idp security-package download full-update
   ```

5. Check the security package download status.

   ```
   user@host>request security idp security-package download status
   ```

6. Update the attack database using the **install** command.

   ```
   user@host>request security idp security-package install
   ```

7. Check the attack database update status using the following command. The command output displays information about the downloaded and installed versions of attack database versions.

   ```
   user@host>request security idp security-package install status
   ```

8. Switch to configuration mode.

   ```
   user@host>configure
   ```

9. Create an IDP policy.

```
[edit ]
user@host#edit security idp idp-policy policy1
```

10. Associate attack objects or attack object groups with the policy.

```
[edit security idp idp-policy policy1]
user@host#set rulebase-ips rule rule1 match attacks predefined-attack-groups
  “Response_Critical”
```

11. Set action.

```
[edit security idp idp-policy policy1]
user@host#set rulebase-ips rule rule1 then action no-action
```

12. Activate the policy.

```
[edit]
user@host#set security idp active-policy policy1
```

13. Commit the configuration.

```
[edit]
user@host# commit
```

14. In the future if you want to download the signature package, download only the updates that Juniper Networks has recently uploaded.

```
user@host>request security idp security-package download
```

15. Check the security package download status.

```
user@host>request security idp security-package download status
```

16. Update the attack database, the active policy, and the detector with the new changes.

```
user@host>request security idp security-package install
```

17. Check the attack database, the active policy, and the detector.

```
user@host>request security idp security-package install status
```

NOTE: It is possible that an attack has been removed from the new version of an attack database. If this attack is used in an existing policy on your device, the installation of the new database will fail. An installation status message identifies the attack that is no longer valid. To update the database successfully, remove all references to the deleted attack from your existing policies and groups, and rerun the install command.

Results From configuration mode, confirm your configuration by entering the **show security idp** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
  user@host# show security idp
  idp-policy policy1 {
```

```
    rulebase-ips {
      rule rule1 {
    match {
    attacks {
      predefined-attack-groups Response_Critical;
    }
    }
      then {
    action {
    no-action;
    }
  }
  }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform this task:

- Verifying the IDP Signature Database Manually on page 38

Verifying the IDP Signature Database Manually

Purpose Display the IDP signature database manually.

Action From operational mode, enter the **show security idp** command.

Related Documentation

- *Intrusion Detection and Prevention Feature Guide for Security Devices*
- *Updating the IDP Signature Database Manually Overview*
- *Example: Updating the Signature Database Automatically*
- *Understanding the IDP Signature Database*

Example: Downloading and Installing the IPS Signature Package in Chassis Cluster Mode

This example shows how to download and install the IPS signature database to a device operating in chassis cluster mode.

- Requirements on page 38
- Overview on page 39
- Downloading and Installing the IPS Signature Database on page 39

Requirements

Before you begin, set the chassis cluster node ID and cluster ID. See *Example: Setting the Chassis Cluster Node ID and Cluster ID for Branch SRX Series Devices*.

Overview

The security package for intrusion detection and prevention (IDP) contains a database of predefined IDP attack objects and IDP attack object groups that you can use in IDP policies to match traffic against known and unknown attacks. Juniper Networks regularly updates the predefined attack objects and groups with newly discovered attack patterns.

To update the signature database, you must download a security package from the Juniper Networks website. After downloading the security package, you must install the package to update the security database with the newly downloaded updates from the Staging folder in your device.

NOTE: On branch SRX Series devices, if your device memory utilization is high on the control plane, loading a large IDP policy might cause the device to run out of memory. This can trigger a system reboot during the IPS security package update.

When you download the IPS security package on a device operating in chassis cluster mode, the security package is downloaded to the primary node and then synchronized to the secondary node. This synchronization helps maintain the same version of the security package on both the primary node and the secondary node.

Downloading and Installing the IPS Signature Database

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

1. Specify the URL for the security package.

   ```
   [edit]
   user@host# set security idp security-package url
     https://services.netscreen.com/cgi-bin/index.cgi
   ```

2. Switch to operational mode.

   ```
   [edit]
   user@host# exit
   ```

3. Download the IPS security package to the primary node (downloads in the **var/db/idpd/sec-download** folder).

   ```
   {primary:node0}[edit]
   user@host> request security idp security-package download
   ```

   The following message is displayed:

   ```
   node0:
   --------------------------------------------------------------------------
   Will be processed in async mode. Check the status using the status checking
    CLI
   ```

4. Check the security package download status.

   ```
   {primary:node0}[edit]
   ```

```
user@host> request security idp security-package download status
```

On a successful download, the following message is displayed.

```
node0:
--------------------------------------------------------------------------
Done;Successfully downloaded from
(https://services.netscreen.com/cgi-bin/index.cgi)
and synchronized to backup.
Version info:1871(Mon Mar  7 09:05:30 2011, Detector=11.4.140110223)
```

5. Update the attack database using the **install** command.

```
user@host> request security idp security-package install
```

6. Check the attack database update status. The command output displays information about the downloaded and installed versions of the attack database.

```
{primary:node0}[edit]
user@host> request security idp security-package install status
```

```
node0:
--------------------------------------------------------------------------
Done;Attack DB update : successful - [UpdateNumber=2011,ExportDate=Mon Oct
17 15:13:06 2011,Detector=11.6.140110920]
     Updating control-plane with new detector : successful
     Updating data-plane with new attack or detector : not performed
      due to no existing running policy found.

node1:
--------------------------------------------------------------------------
Done;Attack DB update : successful - [UpdateNumber=2011,ExportDate=Mon Oct
17 15:13:06 2011,Detector=11.6.140110920]
     Updating control-plane with new detector : successful
     Updating data-plane with new attack or detector : not performed
      due to no existing running policy found.
```

NOTE: You must download the IPS signature package to the primary node. This way, the security package is synchronized on the secondary node. Attempts to download the signature package to the secondary node will fail.

If you have configured a scheduled download for the security packages, the signature package files are automatically synchronized from the primary node to the backup node.

Related Documentation

- Understanding Intrusion Prevention System for SRX Series Devices on page 5
- Understanding the IPS Signature Database on page 29
- Managing the IPS Signature Database (CLI) on page 30
- Managing the IPS Signature Database (Security Director) on page 33