JUNIPER NETWORKS | Engineering Simplicity

Day One+

Intrusion Detection and Prevention

IN THIS GUIDE

Step 1: Begin

IN THIS SECTION

Meet Juniper Networks Intrusion Detection and Prevention System

Juniper Network's Intrusion Detection and Prevention (IDP) system, which is part of Junos OS, mitigates threats and protects against a wide range of attacks and vulnerabilities on your network. IDP constantly watches your network to identify and stop possible incidents, and then sends you a report of the actions it took.

The IDP signature database (also known as the attack database) is available as a security package on the Juniper Networks website. The attack database contains predefined IDP attack objects and IDP attack object groups that detect known attack patterns and protocol anomalies within network traffic. As new vulnerabilities are discovered, we periodically provide a file with updates to the attack database. With a valid license, you can download this file from the Juniper Networks website to protect your network from new threats.

The full IDP security package download includes policy templates that protect your network against the most common attacks. You can use the predefined IDP policy templates "as-is" or use them as a starting point to create new policies customized for your network.

In this guide, we walk you through how to install the IDP license, the IDP security package, and the IDP policy templates. Once you're up and running, you'll learn how to activate a policy template and enable an IDP action in a policy.

Let's get started!

Create Your User Account

You need a Juniper user account to install the IDP security package. With a Juniper user account, you can view your company's product information, participate in discussion forums with Juniper experts and networking peers, and open cases with our Customer Support team. If you don't already have one, see Account Setup.

Set Up Your Device

First and foremost, install your Juniper device and verify you have network access. The quickest and easiest way to do this is to follow the three-step instructions in the Day One+ guide for your device model: Day One +.

Juniper IDP runs on the following physical and virtual devices:

- Juniper Networks® SRX Series Services Gateways
- Juniper Networks® NFX150, NFX250, and NFX350 Network Services Gateways
- Juniper Networks® vSRX on Virtual Firewall on the Google Cloud platform

Download and Install IDP Licenses

IDP is enabled by default on all Juniper security devices. If you're using only custom attack signatures, you don't need an IDP license. However, if you want to install updates to the attack database, you'll need to subscribe to our separately licensed IDP subscription service and install the IDP license on your device. For details, see Install IDP License.

> **NOTE:** If your license key expires, you can continue to use the locally stored application security package content.

Check Your Connection to the Update Server

Let's make sure your device can access the update server on the Internet:

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

```
Successfully retrieved from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3222(Detector=12.6.180190722, Templates=3222)
```

In addition to verifying network connectivity, this command also shows the remote database version.

Download and Install the IDP Security Package

1. Login to your device via CLI as the admin user.
2. Download the IDP security package.

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

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

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

```
Done;Successfully downloaded from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3222(Tue Nov  5 14:09:35 2019 UTC, Detector=12.6.180190722)
```

3. Install the IDP security package.

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

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

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

```
Done;Attack DB update : successful - [UpdateNumber=3222,ExportDate=Tue Nov  5 14:09:35 2019
 UTC,Detector=12.6.180190722]
    Updating control-plane with new detector : successful
    Updating data-plane with new attack or detector : successful
```

Download and Install IDP Policy Templates

The IDP security package includes predefined IDP policy templates that you can activate as-is or use as a starting point to create new policies customized for your network. For more details, see Predefined IDP Policy Templates.

1. Download the predefined IDP policy templates.

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

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

2. Check the download status.

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

```
Done;Successfully downloaded from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3222
```

3. Install the IDP policy templates.

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

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

4. Verify that the templates are installed.

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

```
Done;policy-templates has been successfully updated into internal repository
     (=>/var/run/scripts/commit/templates.xsl)!
```

Activate the Policy Template Commit Script

The policy templates are included as a commit script in the IDP security package. Here's how to activate the commit script:

1. Enable the **templates.xsl** scripts file.

```
[edit]
user@host# set system scripts commit file templates.xsl
```

   This saves the policy templates to the Junos OS configuration database. You can access the policy templates through the CLI at the **[edit security idp idp-policy]** hierarchy level.

2. Commit the configuration to activate the commit script.

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

Deactivate the Commit Script File

Once you've saved the commit script to the Junos OS configuration database, we recommend that you delete or deactivate it to avoid the risk of overwriting the predefined policies with your modifications.

Here's how to delete or deactivate the commit script file:

```
user@host# delete system scripts commit file templates.xsl
```

```
user@host# deactivate system scripts commit file templates.xsl
```

Display the List of Predefined Policy Templates

The predefined policy templates in the attack database cover a wide range of network attack scenarios. You can view a list of the predefined policy templates using the **set security idp default-policy ?** command.

```
[edit]
user@host# set security idp default-policy ?
```

```
Possible completions:
 <default-policy>     Set active policy
  Client-And-Server-Protection
  Client-And-Server-Protection-1G
  Client-Protection
  Client-Protection-1G
  DMZ_Services
  DNS_Service
  File_Server
  Getting_Started
  IDP_Default
  IPS Policy
  Recommended
  Server-Protection
  Server-Protection-1G
  Web_Server
```

Step 2: Up and Running

IN THIS SECTION

Activate a Predefined Policy Template

Let's activate the predefined policy template named Recommended.

1. Set the default policy to Recommended.

```
[edit]
user@host# set security idp default-policy Recommended
```

2. Confirm the Recommended policy is enabled on your device.

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

```
default-policy Recommended;
```

Enable an IDP Action in a Policy

You can configure attack objects and groups as match conditions in IDP policy rules. In this example, we show you how to create a policy rule and enable the predefined attack group "HTTP-Critical" in a policy. The "HTTP-critical" attack group defines actions to take for HTTP traffic from the untrust zone to the trust zone. When this attack group is enabled, IDP tells the device to check for "HTTP-Critical" attacks and then take the action defined in the policy (which is probably to drop the traffic).

1. Create an IDP policy rule.

```
[edit]
user@host# set security idp idp-policy http rulebase-ips rule 1 match from-zone untrust
user@host# set security idp idp-policy http rulebase-ips rule 1 match to-zone trust
user@host# set security idp idp-policy http rulebase-ips rule 1 match application junos-http
user@host# set security idp idp-policy http rulebase-ips rule 1 match attacks predefined-attack-groups "HTTP - Critical"
user@host# set security idp idp-policy http rulebase-ips rule 1 then action recommended
user@host# set security idp idp-policy http rulebase-ips rule 1 then notification log-attacks
```

2. Commit the changes.

```
user@host#commit
```

3. Apply the IDP policy.

```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy policy-2 match source-address any
user@host# set security policies from-zone untrust to-zone trust policy policy-2 match destination-address any
user@host# set security policies from-zone untrust to-zone trust policy policy-2 match application junos-http
user@host# set security policies from-zone untrust to-zone trust policy policy-2 then permit application-services idp-policy
  http
```

4. Commit the changes.

```
user@host# commit
```

5. Verify that HTTP-Critical is enabled in the policy.

```
user@host#  show security policies policy-name policy-1 detail
```

```
user@host# show security idp idp-policy http
rulebase-ips {
    rule 1 {
        match {
            from-zone untrust;
            to-zone trust;
            application junos-http;
            attacks {
                predefined-attack-groups "HTTP - Critical";
            }
        }
        then {
            action {
                recommended;
            }
            notification {
                log-attacks;
            }
        }
    }
}

user@host# show security policies from-zone untrust to-zone trust policy policy-2
match {
    source-address any;
    destination-address any;
    application junos-http;
}
```

```
then {
    permit {
        application-services {
            idp-policy http;
        }
    }
}
```

The sample output confirms that the “HTTP-critical” attack group is enabled for the policy.

View Predefined Attacks and Attack Groups in an IDP Policy

The IDP attack database stores thousands of attack objects. To make them easier to manage, attack objects are organized into attack groups. An attack group contains two or more types of attack objects.

Use the **show security idp attack attack-list policy *policy-name*** command to view the attacks available in a IDP policy template or IDP policy. If an IDP policy contains an attack that belongs to several attack groups, the IDP policy command output will display the redundant attack names.

View a List of Detected Attacks

user@host> **show security idp attack table**

```
## Displays attack table (attack hits are aggregated across all SPUs)

user@host> show security idp attack table
IDP attack statistics:
Attack name                    #Hits
TROJAN:SUBSEVEN:SCAN            1303
APP:CA:ARCSRV:DISCOVERY-OF      1301
SCADA:DNP3:NON-DNP3             1301
TCP:C2S:AMBIG:C2S-SYN-DATA      1300
SCADA:MODBUS:NON-MODBUS         1299
OS:LINUXX86:NTPDX-OF             975
NETBIOS:WINS:REPLICATION-PTR     944
RPC:RPC.STATD:STATD-FMT-STR2     154
DOS:NETDEV:CISCO-PIM              16
DOS:NETDEV:CISCO-SUNND            16
SCADA:MODBUS:SLAVE-ID              7
SCADA:MODBUS:READ-ID               6
```

Step 3: Keep Going

Congratulations! You're up and running with IDP! Now you can proceed with managing IDP policies on your devices. Here are some excellent resources that will help you take your IDP knowledge to the next level:

If you want to	Then
Find in-depth product documentation for IDP	Check out the Intrusion Detection and Prevention User Guide in the Juniper TechLibrary
Understand the latest security advisories, and get a little extra help implementing your security solution	Take advantage of these awesome Juniper support resources: • Security Advisories • Security Services • JTAC and Customer Care Contact Information
Learn about training and certification opportunities	Explore these options: • Juniper Security (JSEC) On-Demand • Junos Networks Security Learning Path • Security Certification Track
Find out more about threat intelligence and understand the latest recommendations	Search IPS and application signature databases: • IPS Signatures • Application Signatures
See all documentation available for Junos OS	See the Junos OS Documentation
Stay up to date on new and changed features and known and resolved issues	See the Junos OS Release Notes
Ask your peers. Connect to labs. Find new learning opportunities	Visit the Intrusion Prevention Forum

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2021 Juniper Networks, Inc. All rights reserved. Rev. 01, May 2021.