WHITE PAPER

SRX AI & IDP

Offline Security Package Update

Version 4.0
Last modified 06/15/2015

Table of Contents

Overview

Juniper Networks regularly updates the predefined IPS and Application security database and makes it available on the Juniper Networks website. This database includes attack object groups that can be used in IDP policies to match traffic against known attacks. Although the predefined attack objects cannot edited, the attack objects can be updated through CLI to use in IDP policies.

Updating security package from CLI is rather simple process. However, for update to succeed, device is expected to have access to the Internet and Juniper download server (https://signatures.juniper.net/cgi-bin/index.cgi). Very often this requirement cannot be met due to security restrictions based around the corporate security policy which does not allow security devices management port to be connected directly to public networks such as Internet. In such case there is an option to upload the required security package manually onto the SRX.

AppID 2.0 and vSRX

Juniper Networks has introduced Application Identification version 2.0 from Junos 12.1X47 version of code which is better capable of detecting applications compared to prior version and it requires few extra files to be downloaded. The document goes through the relevant files. The document is also applicable for vSRX, note that the device name for vSRX is “firefly-perimeter” in the download URLs of manifest.xml and SignatureUpdate.xml.gz.

Before upgrading to 12.1X47 or above, it is recommended to upgrade to the latest signature package and remove any applications or application groups that are not present in latest signature package to avoid configuration failures. Please refer to the below release notes for more information.
http://www.juniper.net/techpubs/en_US/junos12.1x47/information-products/topic-collections/release-notes/12.1x47/index.html?topic-87506.html

Known Issue with Security Package download through web browsers

Some of the web browsers might show errors like “XML Parsing Error: not well-formed” for the security package urls, this is because the signature package hosting server cannot support full mime-types of the sigpack files.

In such cases the workaround is to right-click anywhere on the webpage and “save page as” xml. If it’s SignatureUpdate.xml.gz.xml, rename it to SignatureUpdate.xml.gz and extract.

Juniper recommendation is to download the IDP signature package files through tools like curl, wget etc. For example, on any linux based machine, below can be executed (as an example):

root@host:~/Desktop/idpdb$wget
https://services.netscreen.com/xmlupdate/194/SignatureUpdates/2511/SignatureUpdate.xml.gz

SRX AI only Offline Security Package Update

This section is applicable for scenarios where only AppSecure feature (AppTrack, AppFW or AppQoS) is used and not IPS feature. Follow the procedure below to download and install the application signatures.

1) Download manifest URL from the Juniper download server

AI Download URL for Junos 12.1X and 12.3X versions:

a) Download latest application package version

To download the latest security package for AI/appid, download the manifest.xml file from the URL
https://signatures.juniper.net/cgi-bin/index.cgi?type=manifest&device=jsrx650&feature=ai&detector=0.0.0&to=latest&os=12.1&build=44

For SRX highend device the device names are device=srx3400, srx3600 and so on
For SRX Branch devices the device names are device= jsrx210, jsrx240 and so on
For vSRX the device name is device=firefly-perimeter
“os=12.1” indicates the SRX JunOS version currently installed
“to = latest” indicates download the latest security package

b) Download a specific application package version

https://signatures.juniper.net/cgi-bin/index.cgi?type=manifest&device=jsrx650&feature=ai&detector=0.0.0&to=2497&os=12.1&build=44

Here version = 2098
The version can be any valid version < ‘latest’. This is useful to downgrade to a specific version once a latest AI package had been installed previously. The same rules for device, OS apply as in case a).

AI Download URL for versions prior to Junos 12.1X and 12.3X versions:

For Junos versions prior to 12.1X or 12.3X versions of code like 11.4 etc, the download url for manifest.xml is a little different, the OS context will be “os=”. Below is an example for Junos 11.4

https://signatures.juniper.net/cgi-bin/index.cgi?type=manifest&device=srx3600&feature=ai&detector=0.0.0&to=latest&os=11.4

2) Download application signature files

For Junos 12.1X47 and above or 12.3X48 and above versions:

Once the manifest.xml is downloaded, download the application_groups.xml.gz, applications.xml.gz, applications2.xml.gz and libqmprotocols.tgz using the urls listed in manifest.xml.

Example of manifest.xml file:

```
<manifest>
  <version>2497</version>
  <entry>
    <id>application_groups.xml.gz</id>
    <type>systable</type>
    <version>2497</version>
    <location>application_groups.xml</location>
    <checksum>84f13fc18350b4ff9bc6cd19d45f719c</checksum>
    <url>https://signatures.juniper.net/xmlupdate/226/ApplicationGroups/2497/application_groups.xml.gz</url>
  </entry>
```

```
...
 <entry>
  <id>applications.xml.gz</id>
  <type>systable</type>
  <version>2497</version>
  <location>applications.xml</location>
  <checksum>a97e05261ac284a4176636e754ece6ff</checksum>
  <url>https://signatures.juniper.net/xmlupdate/226/Applications/2497/applications.xml.gz</url>
 </entry>
...
```

Copy the downloaded files to the SRX at /var/db/appid/sec-download along with the manifest.xml.

For Junos versions prior to 12.1X47:

Once the manifest.xml is downloaded, download the application_groups.xml.gz and applications.xml.gz using the urls listed in manifest.xml.

Edit manifest.xml to change the <url> field in the manifest.xml file for application_groups.xml.gz and applications.xml.gz.
<url>file:/var/db/appid/sec-download/application_groups.xml.gz</url>
<url>file:/var/db/appid/sec-download/applications.xml.gz</url>

NOTE: Do not edit the manifest.xml file for 12.1X47 and 12.3X48 and above versions of Junos.

AI Install on HE-SRX for Junos 11.4 or later AND on Branch-SRX for Junos 11.2 or later

If the JunOS is 11.4 or later on DC-SRX or 11.2 and later release on Branch SRX, follow the steps below:

a. Unzip applications.xml.gz and application_groups.xml.gz

```
regress@router% cd /var/db/appid/sec-download
regress@router%gzip –d applications.xml.gz
regress@router%gzip –d application_groups.xml.gz
```

For Junos 12.1X47 and above:

```
regress@router% gzip -d applications2.xml.gz
```

b. Install the application signatures with command

```
regress@router>request services application-identification install
```

c. Check the version installed with command

```
regress@router >show services application-identification version
```

AI Install on HE-SRX for Junos 11.2 and previous releases

If the JunOS is 11.2 and earlier release on DC SRX, follow the steps below:

a. Set the download url path to point to the local directory in router configuration mode

```
regress@router# set services application-identification download url
file:/var/db/appid/sec-download/manifest.xml
regress@router# commit
```

b. Download / install application signatures from local directory

This will download from the local directory and install the application signatures in the configuration db.

```
regress@router >request services application-identification download
```

c. Check the version installed with command

```
regress@router >show services application-identification version
```

SRX AI & IPS Offline Security Package Update

1) Download SignatureUpdate.xml.gz

Depending on the status of the device there are three possible options for downloading SignatureUpdate.xml.gz

For Junos 12.1X and 12.3X versions:

For versions of code like 12.1X44, 12.1X47 or 12.3X48, the OS context will be “os=&build=”.

A. When device does not have any attack database (factory default or after deleting DB)

root@device > show security idp security-package version
Attack database version:N/A
Detector version : 12.6.160150609
Policy template version :N/A

In this case use the following URL to get the SignatureUpdate.xml.gz file if the Junos version is 12.1X47
https://signatures.juniper.net/cgi-bin/index.cgi?device=jsrx650&feature=idp&detector=12.6.160150609&to=latest&os=12.1&build=47&type=update

Note: In the above URL we can observe the following:
For SRX highend device the device names are device=srx3400, srx3600 and so on
For SRX Branch devices the device names are device= jsrx210, jsrx240 and so on
For vSRX the device name is device=firefly-perimeter
os= indicates the SRX JunOS version currently installed
from= current downloaded version (if there is no DB it will be null)
to = latest indicates download the latest security package. If not mentioned latest is downloaded
feature = idp (while other values above change - feature never changes)

Note : The detector version is different for different JunOS platforms. Refer to the detector release notes for more details on the detector versions. https://www.juniper.net/techpubs/software/management/idp/de/

B. When update involves updating the Attack Database from one version to another version

Download the SignatureUpdate.xml.gz file from the URL similar to the following with adjusted fields:
https://signatures.juniper.net/cgi-bin/index.cgi?device=jsrx650&feature=idp&detector=12.6.160150609&from=2516&to=2517&os=12.1&build=47&type=update

In the URL we can observe the following:
detector = currently loaded detector (e.g. 12.6.160150609)
from = currently loaded Attack DB version (e.g. 2516)
to = Attack DB version to download (e.g. 2517)

C. When update involves updating the signature database from one version to latest version

Download the SignatureUpdate.xml.gz file from the URL similar to the following with adjusted fields:
https://signatures.juniper.net/cgi-bin/index.cgi?device=jsrx650&feature=idp&detector=12.6.160150609&from=&to=latest&os=12.1&build=47&type=update

In the URL we can observe the following:
detector = currently loaded detector (e.g. 12.6.160150609)
os = Junos (12.1X47)
from = currently loaded Attack DB version. You can leave this value as null.
to = Attack DB version to download (latest)

For Junos versions prior to 12.1X and 12.3X:

The signature update URL is a bit different in versions prior to 12.1X and 12.3X. The OS context will be “os=”
https://signatures.juniper.net/cgi-bin/index.cgi?device=srx5800&feature=idp&os=10.2&detector=10.2.140090602&from=&to=latest&type=update

2) Download other required files

Once the SignatureUpdate.xml.gz file is downloaded, unzip it and open the file in order to locate the other URLs for downloading the rest of the Attack Database files. The files that need to be downloaded are highlighted.

Example of unzipped file or SignatureUpdate.xml:

<?xml version='1.0' encoding='UTF-8'?>
<SignatureUpdate type="base">
<XMLVersion>1.0.0</XMLVersion>
<UpdateNumber>2499</UpdateNumber>
<ExportDate>Wed May 27 18:27:41 2015 UTC</ExportDate>
<ApplicationGroups md5="1eb2e48a60e7ad44e9dceba70d26e0ab"
version="2499">https://signatures.juniper.net/xmlupdate/225/ApplicationGroups/2499/application_groups.xml.gz</
ApplicationGroups>
<ApplicationSchema md5="b309c781a484fcb3a03b8f1ad3c81a8e"
version="2499">https://signatures.juniper.net/xmlupdate/225/Applications/2499/applications.xsd</ApplicationSche
ma>
<Applications md5="3b46d8dab920eafbd6ad7e5d1e1ec8f9"
version="2499">https://signatures.juniper.net/xmlupdate/225/Applications/2499/applications.xml.gz</Applications>
<Detector md5="23576d12800c57c1938841d774d9c53c"
version="12.6.140140822"family="srx">https://signatures.juniper.net/xmlupdate/225/Detector/12.6.140140822/libi
dp-detector.so.tgz.v</Detector>
<Groups md5="2a0dd0163ba6b5b621e4790ccd682572"
version="2499">https://signatures.juniper.net/xmlupdate/225/Groups/2499/groups.xml.gz</Groups>
<Platforms md5="b39bdfc2ed512de44aeb39ceaaa9ff63"
version="2499">https://signatures.juniper.net/xmlupdate/225/Platforms/2499/platforms.xml.gz</Platforms>
<Templates md5="f8d508b3766c1e0d95a632a3ba93b851"
version="2499">https://signatures.juniper.net/xmlupdate/225/Templates/2499/templates.xml.gz</Templates>

From the file above we can identify URLs for downloading the following files:

a. Application_groups.xml.gz
https://signatures.juniper.net/xmlupdate/225/ApplicationGroups/2499/application_groups.xml.gz

b. Applications.xsd
https://signatures.juniper.net/xmlupdate/225/Applications/2499/applications.xsd

c. applications.xml.gz
https://signatures.juniper.net/xmlupdate/225/Applications/2499/applications.xml.gz

d. libidp-detector.so.tgz.v
https://signatures.juniper.net/xmlupdate/225/Detector/12.6.140140822/libidp-detector.so.tgz.v

e. groups.xml.gz
https://signatures.juniper.net/xmlupdate/225/Groups/2499/groups.xml.gz

f. platforms.xml.gz
https://signatures.juniper.net/xmlupdate/225/Platforms/2499/platforms.xml.gz

NOTE: For Junos 12.1X47 and above or 12.3X48 version and above:

In addition to above files, applications2.xml.gz and libqmprotocols.tgz should also be downloaded for the above mentioned versions.

<Applications2 md5="602a3d72c7d2699ff4b3594184a28d4f" version="2499">https://signatures.juniper.net/xmlupdate/225/Applications/2499/applications2.xml.gz</Applications2>
<Libqmprotocols md5="5632398c76d22a8809fde158ca078125" version="2499">https://signatures.juniper.net/xmlupdate/225/Libqmprotocols/2499/libqmprotocols.tgz</Libqmprotocols>

Note : When downloading the detector file from the browser it changes the extension to .tar. Pay close attention to the file extensions when downloading the file. Rename the file to .v if the browser changes the name.

3) Security package Installation

Once all the required files are downloaded perform the following steps:

For Junos 12.1X47 and above or 12.3X48 version and above:

Copy the applications2.xml.gz and libqmprotocols.tgz files as well along with below mentioned files and unzip applications2.xml.gz. Do not rename or change libqmprotocols.tgz.

For Junos versions prior to 12.1X47:

A. Copy applications.xml.gz, applications_groups.xml.gz, groups.xml.gz, platforms.xml.gz, SignatureUpdate.xml.gz and libidp-detector.so.tgz.v files to /var/db/idpd/sec-download directory on the SRX device.

B. Unzip all the files

```
root@host% gzip –d <filename> e.g “gzip –d Signatureupdate.xml.gz” or “gzip –d *.gz”
root@% ls -l
total 113028
-rw-r--r--  1 root  wheel  27371544 Jun  1 16:01 SignatureUpdate.xml
-rw-r--r--  1 root  wheel    315958 Jun  1 16:02 application_groups.xml
-rw-r--r--  1 root  wheel   2181526 Jun  1 16:03 applications.xml
-rw-r--r--  1 root  wheel     11885 Jun  1 16:02 applications.xsd
-rw-r--r--  1 root  wheel    721970 Jun  1 16:17 detector-capabilities.xml
-rw-r--r--  1 root  wheel   4225396 Jun  1 16:03 groups.xml
-rw-r--r--  1 root  wheel   5408004 Jun  1 16:22 libidp-detector.so.tgz.v
-rw-r--r--  1 root  wheel        83 Jun  1 16:25 manifest.xml
-rw-r--r--  1 root  wheel       463 Jun  1 16:03 platforms.xml
drwxr-xr-x  2 root  wheel       512 Jun  1 16:18 sub-download
```

C. Install the security package on SRX:

```
root@host>request security idp security-package install source-path /var/db/idpd/sec-download
```

D. Check the status of the install with command

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

E. Check the version installed with command

```
root@host > show security idp security-package-version
```

If an IDP policy was previously configured, the policy will be recompiled with the latest signature database. Upon successful compilation the policy will be loaded to the data plane.

SRX IDP Policy Templates offline update

1. Copy the SignatureUpdate.xml downloaded in the previous step to
/var/db/idpd/sec-download/sub-download folder

2. Open the SignatureUpdate.xml to find the url for templates.xml.gz and download it (example url below)
https://signatures.juniper.net/xmlupdate/225/Templates/2499/templates.xml.gz

3. Copy the templates.xml.gz to /var/db/idpd/sec-download/sub-download folder

4. Unzip templates.xml.gz
root@host%gzip –d templates.xml.gz

5. Install the policy templates
>request security idp security-package install policy-templates

6. Check the status of the install with the command
>request security idp security-package install status