**White Paper**

# SRX IDP

# Local Security Package Update

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089  USA
408 745 2000 or 888 JUNIPER
www.juniper.net

# Contents

## Overview

Juniper Networks regularly updates the predefined attack database and makes it available on the Juniper Networks website. This database includes attack object groups that you can use in IDP policies to match traffic against known attacks. Although you cannot create, edit, or delete predefined attack objects, you can use the CLI to update the list of attack objects that you can use in IDP policies.

Updating security package (which includes attack database updates) 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://services.netscreen.com/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.

Alternative approach exists where one could copy updates from the device with the Internet access to the device without it. This works just fine however, it hardly makes sense if corporate security policy prevents from having security devices connect to the Internet from their management port.
Another option is to request update files from Juniper TAC but again – this hardly scales.

The following section describes the solution to the problem described above and steps involved in updating SRX device locally.

## Download SignatureUpdate.xml.gz

Download the file **SignatureUpdate.xml.gz** from Juniper download server.

Depending on current status of the device attack database there are three possible download options of downloading **SignatureUpdate.xml.gz file**

1. when device does not have any attack database (from factory or after deleting DB).

   ```
   root@device> show security idp security-package-version
           Attack database version:N/A(N/A)
           Detector version :9.2.140081105
           Policy template version :N/A
   ```

   Use the following URL to get the **SignatureUpdate.xml.gz** file:

   https://services.netscreen.com/cgi-bin/index.cgi?device=srx5800&feature=idp&os=9.6&detector=9.2.140081105&from=&to=latest&type=update

   In the URL you can observe the following:
   - **device** = device type (e.g. srx5800 or srx3400 or srx210 etc)
   - **detector** = default detector (9.2.140081105)
   - **os** = Junos (9.6)

- **from** = current downloaded version (if there is no DB it will be null)
- **to** = latest (version to download. If not mentioned latest is downloaded)
- **feature** = idp (while other values above change - feature never changes)

2. when update involves updating the Attack Database from one version to another version. Please download **SignatureUpdate.xml.gz** file from the URL similar to the following with adjusted fields:

   https://services.netscreen.com/cgi-bin/index.cgi?device=srx5800&feature=idp&os=9.6&detector=10.2.140090602&from=1484&to=1479&type=update

   In the URL you can observe the following:
   - **device** = device type (e.g. srx5800 or srx3400 or srx210 etc)
   - **detector** = currently loaded detector (e.g. 10.2.140090602)
   - **os** = Junos (9.6)
   - **from** = currently loaded Attack DB version (e.g. 1484)
   - **to** = Attack DB version to download (e.g. 1479)
   - **feature** = idp (while other values above change - feature never changes)

3. when device update the the secdb from one version to latest version.
   Please download **SignatureUpdate.xml.gz** file from the URL similar to the following with adjusted fields:

   https://services.netscreen.com/cgi-bin/index.cgi?device=srx5800&feature=idp&os=9.6&detector=10.2.140090602&from=&to=latest&type=update

   In the URL you can observe the following:
   - **device** = device type (e.g. srx5800 or srx3400 or srx210 etc)
   - **detector** = currently loaded detector (e.g. 10.2.140090602)
   - **os** = Junos (9.6)
   - **from** = currently loaded Attack DB version
   - **to** = Attack DB version to download (latest)
   - **feature** = idp (while other values above change - feature never changes)

## Download other required files

Once you download the SignatureUpdate.xml.gz file, unzip it and open the file in order to locate the other URLs for downloading the rest of the Attack Database files.

Example of unzipped file – **SignatureUpdate.xml:**

```
<?xml version="1.0" encoding="UTF-8"?>

<Signature Update type="base"
xsi:noNamespaceSchemaLocation="http://services.netscreen.com/xmlupdate/SignatureUpdate.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://services.netscreen.com">
 <XMLVersion>1.0.0</XMLVersion>
 <UpdateNumber>1484</UpdateNumber>
 <ExportDate>Tue Aug 18 10:31:22 2009</ExportDate>
 <ApplicationGroups md5="6ee5d392ec033625292a689b1465b70a"
version="8">https://services.netscreen.com/xmlupdate/89/ApplicationGroups/8/application_groups.xml.gz
</ApplicationGroups>
 <Applications md5="6c7bae362af8fa5df969ca9cf26b5dd1"
version="19">https://services.netscreen.com/xmlupdate/89/Applications/19/applications.xml.gz</A
pplications>
 <Contexts md5="402ffe32a6c2c8d28291a458d4e8329a"
version="8">https://services.netscreen.com/xmlupdate/89/Contexts/8/contexts.xml.gz</Contexts>
 <Detector md5="8a3a7fa2fd214025f7e1b8f0f9f43b38" version="10.2.140090602"
family="srx">https://services.netscreen.com/xmlupdate/89/Detector/10.2.140090602/libidp-
detector.so.tgz.v</Detector>
 <Filters md5="cd85f6ab8c48ae087563aaf7d5844ded"
version="1">https://services.netscreen.com/xmlupdate/89/Filters/1/filters.xml.gz</Filters>
 <Groups md5="387deeff3e4713bf18f1632289c10beb"
version="2">https://services.netscreen.com/xmlupdate/89/Groups/2/groups.xml.gz</Groups>
 <Platforms md5="98f752b5af92c348e3d664ffd187b00a"
version="9">https://services.netscreen.com/xmlupdate/89/Platforms/9/platforms.xml.gz</Platforms>
 <Products md5="db6df3a3d22c280e84637d5faac81163"
version="2">https://services.netscreen.com/xmlupdate/89/Products/2/products.xml.gz</Products>
 <Services md5="cf106794e453acca87464aec38b29ee3"
version="7">https://services.netscreen.com/xmlupdate/89/Services/7/services.xml.gz</Services>
 <Templates md5="c4d5b4a11ac9eb363112eb60fb45315f"
version="1">https://services.netscreen.com/xmlupdate/89/Templates/1/templates.xml.gz</Templates>
 <Entries>
  <Entry>
   <InternalID>1</I
```

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

1. **applications.xml.gz**
   **https://services.netscreen.com/xmlupdate/89/Applications/19/applications.xml.gz**

2. **libidp-detector.so.tgz.v**
   **https://services.netscreen.com/xmlupdate/89/Detector/10.2.140090602/libidp-detector.so.tgz.v**

3. **groups.xml.gz**
   [https://services.netscreen.com/xmlupdate/89/Groups/2/groups.xml.gz](https://services.netscreen.com/xmlupdate/89/Groups/2/groups.xml.gz)

4. **platforms.xml.gz**
   [https://services.netscreen.com/xmlupdate/89/Platforms/9/platforms.xml.gz](https://services.netscreen.com/xmlupdate/89/Platforms/9/platforms.xml.gz)

Note – Firefox might complain so try IE.

## Update the device

Once you have download all the required files perform the following steps:

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

```
root@host% ls –al /var/db/idpd/sec-download
total 33396
drwxr-xr-x  3 root  wheel      512    Aug 22 00:59 .
drwxr-xr-x  7 root  wheel      512    Aug 22 00:53 ..
-rw-r--r--  1 root  wheel  11781025 Aug 22 00:19    SignatureUpdate.xml
-rw-r--r--  1 root  wheel    99518   Aug 22 00:16    applications.xml
-rw-r--r--  1 root  wheel   4112343  Aug 22 00:17    groups.xml
-rw-r--r--  1 root  wheel   1025961  Aug 22 00:57    libidp-detector.so.tgz.v
-rw-r--r--  1 root  wheel      613    Aug 22 00:17    platforms.xml
drwxr-xr-x  2 root  wheel      512    Aug 22 00:53    sub-download
```

2. on SRX run the following command:
   > **request security idp security package install source-path /var/db/idpd/sec-download**