Route Origin Validation Lab

Part-1: Installing RPKI Validator (Fort)

Login Details

- Username `apnic` and password `training`.

Lab Setup

For this lab, we will use FORT from NIC México as the RPKI validator.

1. Login to your server (SSH from the jumphost to your container using the `username` and `password` given above), where `X` is your VM number:

   ```
   ssh apnic@192.168.30.X
   ```

2. Update the repository

   ```
   sudo apt update && sudo apt upgrade
   ```

   - ***NOTE:*** Please note that FORT has the following dependencies:

     - jansson
     - libcrypto (LibreSSL or OpenSSL >=1.1)
     - rsync

   - Install the dependencies:

     ```
     sudo apt install autoconf automake build-essential libjansson-dev libssl-dev pkg-config rsync libcurl4-openssl-dev libxml2-dev
     ```

3. Fetch the source file from the repo

```
wget https://github.com/NICMx/FORT-validator/releases/download/v1.4.2/fort-1.4
.2.tar.gz
```

- Unarchive and install Fort:

```
tar zxvf fort-1.4.2.tar.gz
cd fort-1.4.2
./configure
make
sudo make install
```

- We will use the setup script to fetch and install the 5 RIR TALs (make sure you are still in the `fort-1.4.2` directory when you execute the following commands):

  - *NOTE: the setup script only expects one argument: the directory path for the RIR TALs*

```
wget https://raw.githubusercontent.com/NICMx/FORT-validator/v1.4.2/fort
_setup.sh
chmod 755 ./fort_setup.sh
mkdir tal
./fort_setup.sh ./tal
```

  - You need to agree/accept ARIN's Relying Party Agreement (type `yes` as shown below):

```
apnic@group04:~/fort-1.4.2$ ./fort_setup.sh ./tal

Please download and read ARIN Relying Party Agreement (RPA) from https://www.arin.net/resources/manage/rpki/rpa.pdf

Once you've read and if you agree ARIN RPA, type "yes" to proceed with ARIN's TAL download: yes
```

  - The five RIR TALs get fetched, the local repo directory is created, and `fort-config/json` file is created with directory path to the TALs and the local repo:

```
-------------------------------------------------------
-------------------  Success!  --------------------
-------------------------------------------------------

- The five RIRs TAL's were downloaded to '/home/apnic/fort-1.4.2/tal'.
- The directory /tmp/fort/repository was created, so it can be used as the local repository.
- The configuration file '/home/apnic/fort-1.4.2/fort-config.json' was created with the following content:
{
  "local-repository": "/tmp/fort/repository",
  "tal": "/home/apnic/fort-1.4.2/tal"
}

- This configuration file can be utilized with FORT validator, e.g.:
  $ fort -f "/home/apnic/fort-1.4.2/fort-config.json"
- Or its members can be utilized as FORT validator arguments, e.g.:
  $ fort --tal "/home/apnic/fort-1.4.2/tal" --local-repository "/tmp/fort/repository"
```

4. Start the validator (RTR server):

```
fort -f ./fort-config.json --server.address="192.168.30.X#8323" --output.roa="
/tmp/fort/roas.csv" &
```

   - the RTR server (192.168.30.X, where `X` is your container IP) is listening on port `8323` and we are printing the VRP to an output file (`/tmp/fort/roas.csv`).

   - Confirm Fort is running:

     ```
     ps aux | grep fort
     ```

   - Have a look at the validated ROA payload (*Origin ASN, Prefix, Max prefix length*):

     ```
     more /tmp/fort/roas.csv
     ```

     ```
     apnic@group04:~/fort-1.4.2$ more /tmp/fort/roas.csv
     ASN,Prefix,Max prefix length
     AS141462,103.159.186.0/24,24
     AS141462,103.159.187.0/24,24
     AS141462,2001:df5:8b80::/48,48
     AS63920,43.225.48.0/22,24
     AS63920,103.44.32.0/22,24
     AS63920,103.65.252.0/22,24
     AS63920,103.208.164.0/22,24
     AS63920,137.59.168.0/22,24
     AS63920,2401:cd80::/31,48
     AS63920,2404:4180::/32,48
     AS132238,103.96.76.0/22,24
     AS135419,103.120.112.0/22,22
     AS135419,103.120.112.0/24,24
     AS135419,103.120.113.0/24,24
     AS135419,103.120.114.0/24,24
     AS135419,103.120.115.0/24,24
     AS38719,103.52.62.0/24,24
     AS38719,103.67.234.0/23,24
     AS38719,103.67.248.0/24,24
     AS38719,2405:df80::/32,32
     ```

     - If there is no output yet, it means Fort is still working through the initial process of fetching ROAs from the repos and validating, which generally takes a while.

   - Check the local cache (of the repository)

     ```
     ls /tmp/fort/repository
     ```

5. **[Optional]** If you have two separate Validators installed (for redundancy), compare the validated ROA payload outputs for consistency:
    - But before you compare the VRPs, you need to sort the output. Example belowing using `sort` to sort alphanumerically:

      ```
      sort /tmp/fort/roas.csv > fort_sorted.csv
      ```

      - Now you can compare the validated ROA outputs, for example Routinator and Fort:

        ```
        diff -u rout_sorted.csv fort_sorted.csv
        ```

      - Discuss any differences with your group mates and instructor.

Now your validator is ready to feed the validated cache to BGP speaking routers through the RTR (RPKI-to-Router) protocol.

Part-2: RTR session

Validator side

Fort can act as an RTR server, to allow RPKI enabled routers to connect to it and fetch the validated cache (ROA cache).

- Based on the above, the RTR server is listening on `192.168.30.X` (where X is your VM number) and port `8323`
- The timers can be tweaked to suit your need (RFC8210 has recommendations).