RPKI

Overview

RouterOS implements the Resource Public Key Infrastructure (RPKI) to Router Protocol defined in RFC8210. RTR is a very lightweight low memory footprint protocol, to reliably get prefix validation data from RPKI validators.
More information on RPKI and how to set up validators can be found in the APNIC blog:

https://blog.apnic.net/2022/04/06/how-to-installing-an-rpki-validator-2/

Basic Example

Let's consider that we have our own RTR server on our network with IP address 192.168.1.1:

```
/routing/bgp/rpki
add group=myRpkiGroup address=192.168.1.1 port=8282 refresh-interval=20
```

If the connection is established and a database from the validator is received, we can check prefix validity:

```
[admin@rack1_b33_CCR1036] /routing> rpki-check group=myRpkiGroup prfx=70.132.18.0/24 origin-as=16509
    valid
```

Now the cached database can be used by routing filters to accept/reject prefixes based on RPKI validity. At first, we need to set up a filter rule which defines against which RPKI group performs the verification. After that filters are ready to match the status from the RPKI database. Status can have one of three values:

- **valid** - database has a record and origin AS is valid.
- **invalid** - the database has a record and origin AS is invalid.
- **unknown** - database does not have information of prefix and origin AS.
- **unverified** - set when none of the RPKI sessions of the RPKI group has synced database. This value can be used to handle the total failure of the RPKI.

```
/routing/filter/rule
add chain=bgp_in rule="rpki-verify myRpkiGroup"
add chain=bgp_in rule="if (rpki invalid) { reject } else { accept }"
```

Configuration Options

Sub-Menu: `/routing/rpki`

Property	Description
address (*IPv4/6*) mandatory	Address of the RTR server
disabled(*yes* | *no*; Default: **no**)	Whether the item is ignored.
expire-interval (*integer [600..172800]*; Default: 7200)	Time interval [s] polled data is considered valid in the absence of a valid subsequent update from the validator.
group (*string*) mandatory	Name of the group a database is assigned to.
port (*integer [0..65535]*; Default: 323)	Connection port number
preference (*integer [0..4294967295]*; Default: 0)	If there are multiple RTR sources, the preference number indicates a more preferred one. A lesser number is preferred.

refresh-interval (*integer [1..86400]*; Default: 3600)	Time interval [s] to poll the newest data from the validator.
retry-interval (*integer [1..7200]*; Default: 600)	Time Interval [s] to retry after the failed data poll from the validator.
vrf(*name*; Default: main)	Name of the VRF table used to bind the connection to.