RPKI validator na straży BGP

Ihor Hreskiv — 04.2023 — MBUM #7 — Kraków

Ihor Hreskiv

MIKROTIK
CERTIFIED TRAINER

Jestem miłośnikiem urządzeń MikroTik od kilku lat

Potrafię wyjść z VIM :)

eve-ng fan

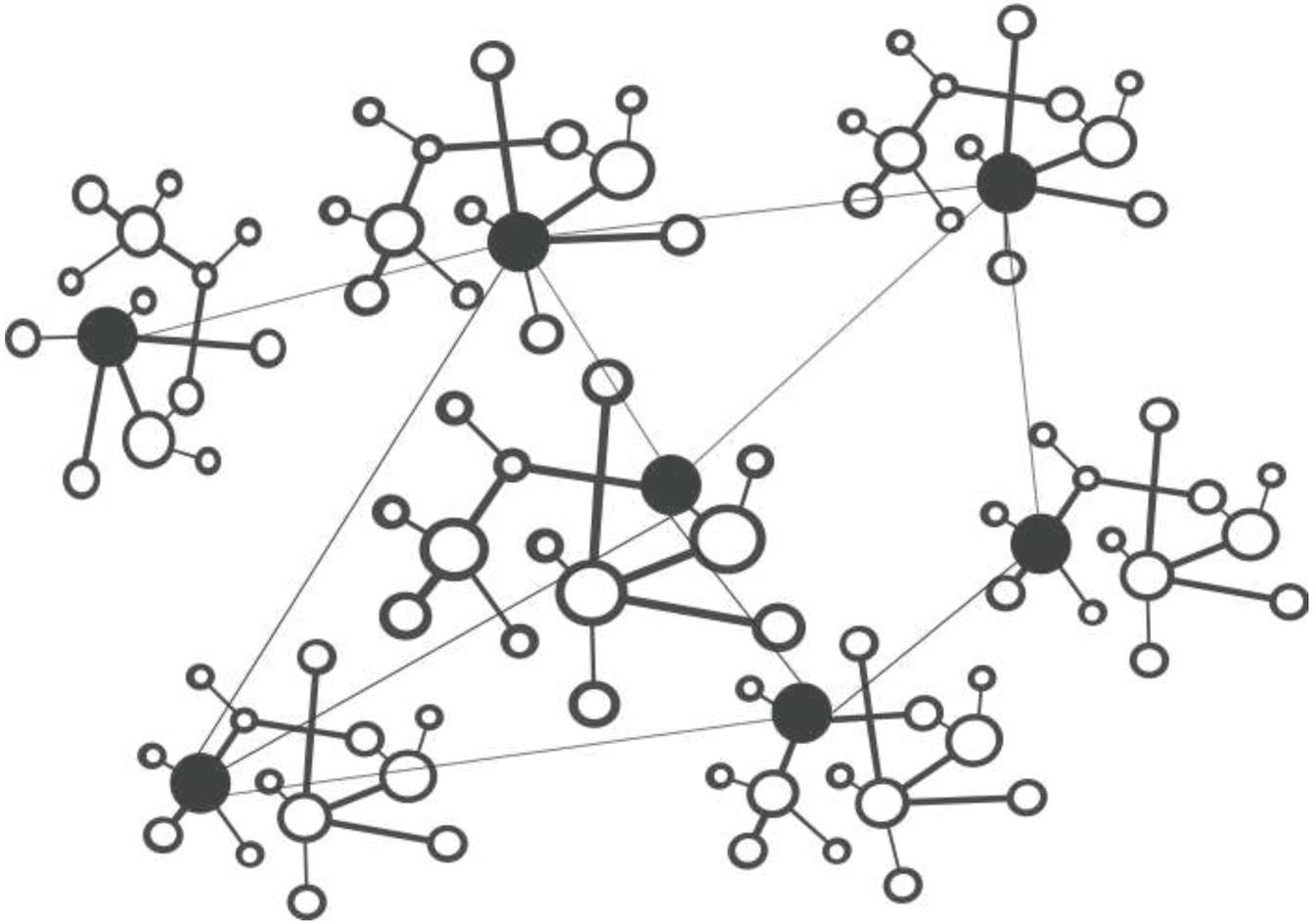
Najczęściej używam CHR

MTC(all)E

BGP w skrócie

BGP (ang. *Border Gateway Protocol*) — zewnętrzny protokół routingu.
BGP jest podstawą działania współczesnego Internetu.

The Internet
Sieć która składa się z sieci



BGP a bezpieczeństwo

BGP hijacking (*przejęcie/porwanie protokołu BGP*), czasami określane jako *przejęcie prefiksu*, *przejęcie trasy* — to nielegalne przejęcie grup adresów IP poprzez uszkodzenie tablic routingu, utrzymywanych przy użyciu protokołu Border Gateway Protocol (BGP).

BGP hijacking

BGP hijacking może nastąpić celowo lub przypadkowo na jeden z kilku sposobów:

- AS ogłasza, że jest *origin* dla prefiksu, dla którego w rzeczywistości nie jest.
- AS ogłasza bardziej szczegółowy prefix niż taki, który może ogłosić prawdziwy źródłowy AS.
- AS ogłasza, że może skierować ruch do porwanego AS krótszą trasą niż jest już dostępna, niezależnie od tego, czy trasa faktycznie istnieje.

BGP hijacking

Niektóry ze znanych atak BGP hijacking:

1. Luty 2008 - Pakistan telekom AS17557 - nieautoryzowane ogłoszenie prefiksu 208.65.153.0/24 który jest częścią 208.65.152.0/22 należący do YouTube. *https://cnet.co/41sp06G*

2. Kwiecień 2020 - Rostelekom AS12389 - ogłoszenie się *origin* dla około 50 prefiksów *https://bit.ly/3N2dfj4*


RPKI
IP
ASN

Resource Public Key Infrastructure

RPKI (*Resource Public Key Infrastructure*) — system używany do sprawdzania poprawności i zabezpieczania informacji o routingu w Internecie.

Jest to hierarchiczny system certyfikatów cyfrowych, który weryfikuje własność bloków adresów IP (prefiksów) oraz numerów systemów autonomicznych (ASN).

IETF RFC pokrewny z RPKI

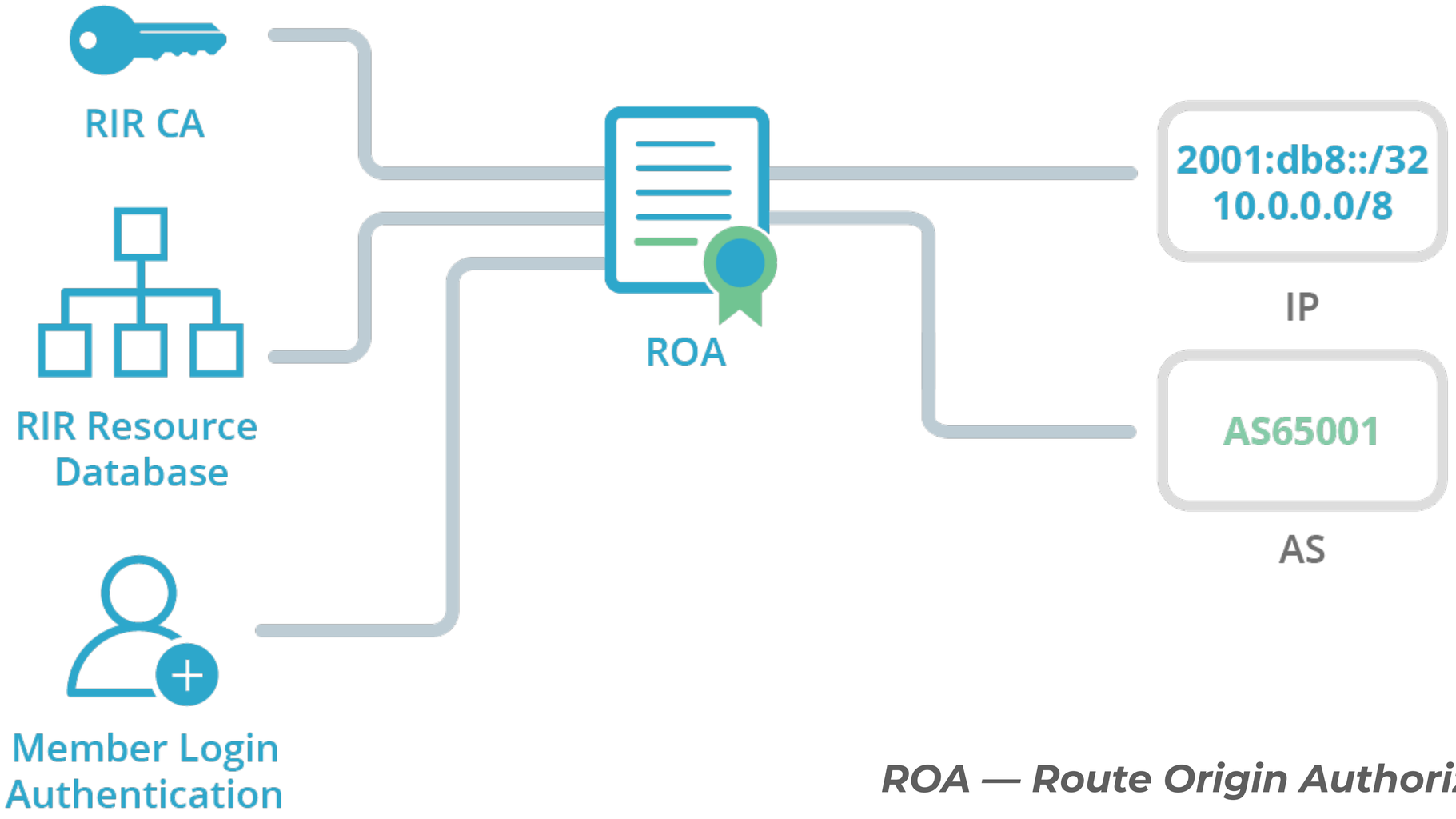
https://tools.ietf.org/html/rfc6480
An Infrastructure to Support Secure Internet Routing

https://tools.ietf.org/html/rfc6482
A Profile for Route Origin Authorizations (ROAs)

https://tools.ietf.org/html/rfc6483
Validation of Route Origin using PKI and ROAs

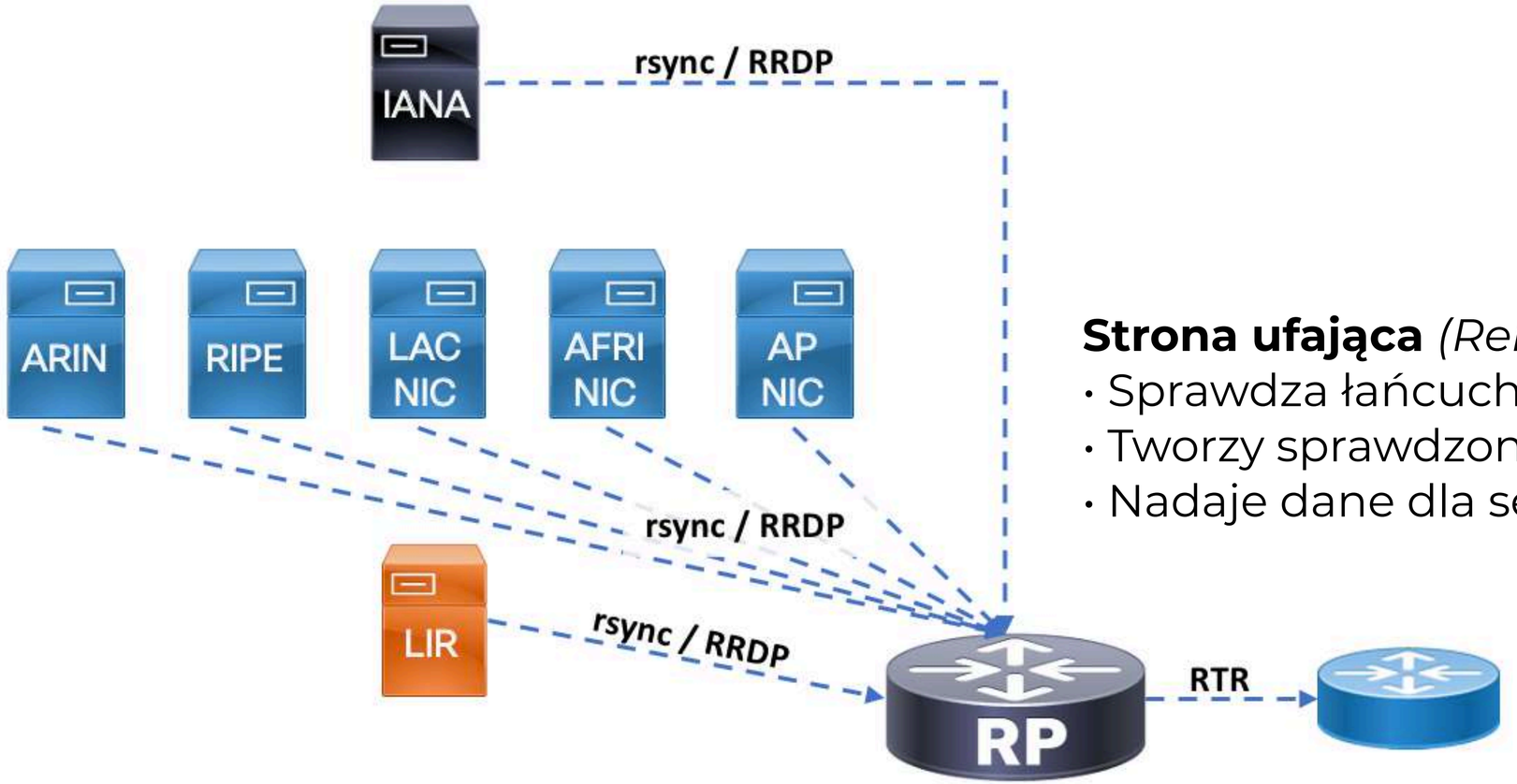
https://tools.ietf.org/html/rfc6810
The RPKI to Router Protocol (RTR)

Resource Public Key Infrastructure



ROA — Route Origin Authorization

RPKI proces walidacji



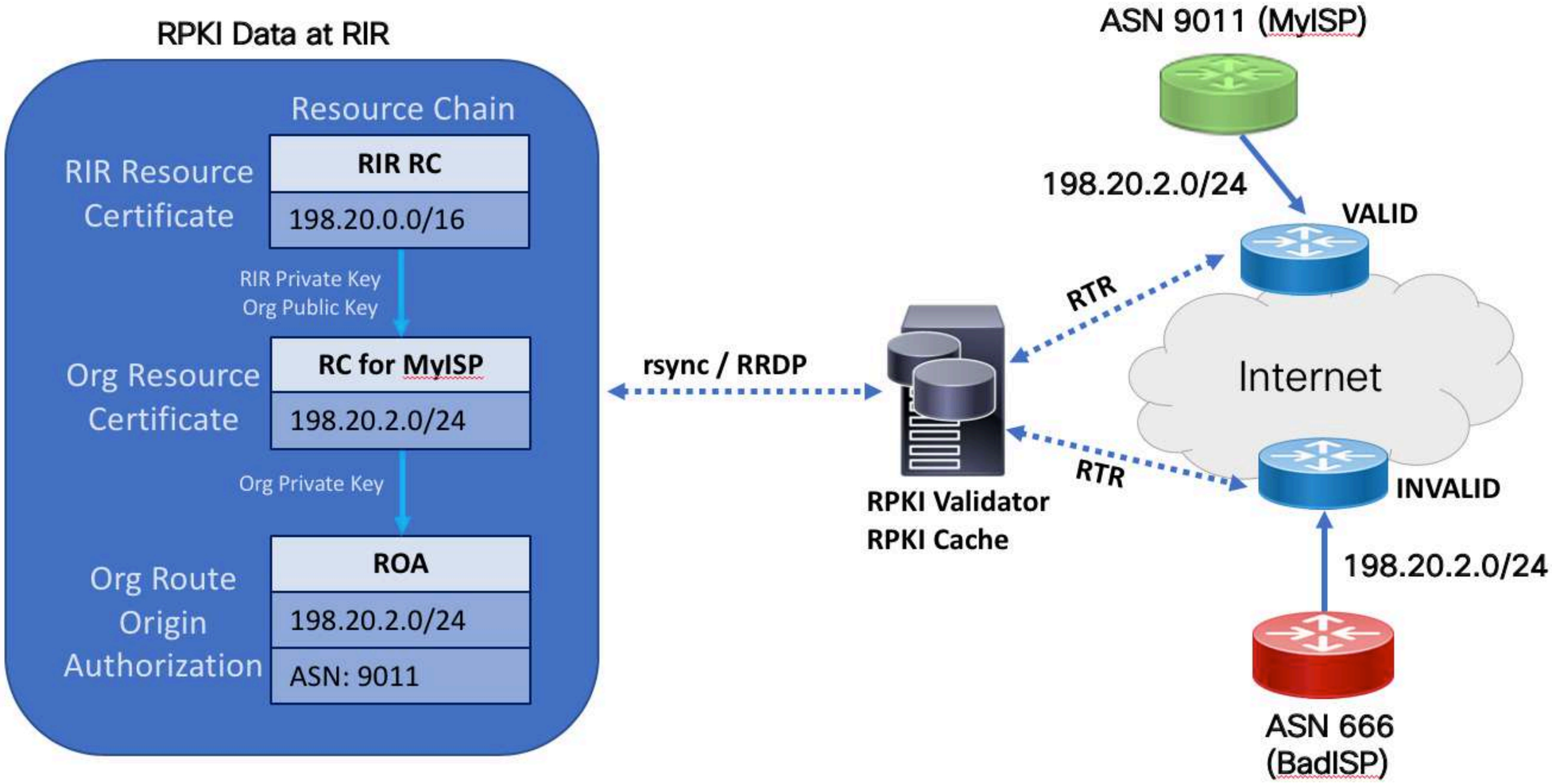
Strona ufająca *(Relying Party)*

- Sprawdza łańcuch
- Tworzy sprawdzony cache
- Nadaje dane dla serwera RTR

RTR — RPKI-to-Router (RTR) protocol

RRDP — RPKI Repository Delta Protocol (RRDP)

RPKI proces walidacji



Resource Public Key Infrastructure

RouterOS w nowej wersji ROS7 ma zaimplementowane wsparcie dla RPKI do protokołu BGP, zdefiniowanego w *RFC8210*.

RTR to bardzo lekki protokół o niskim zużyciu pamięci, aby niezawodnie uzyskiwać dane walidacji prefiksów z walidatorów RPKI.


ROUTINATOR

Czym jest Routinator?

Routinator — narzędzie open-source służące do weryfikacji i pobierania informacji z infrastruktury RPKI.

Routinator może być używany do pobierania i przechowywania certyfikatów RPKI, weryfikacji prawidłowości podpisów cyfrowych i uwierzytelniania właścicieli adresów IP i numerów ASN w protokole BGP.

https://github.com/NLnetLabs/routinator

Instalacja i konfiguracja Routinator

Obrazy Docker zbudowane w oparciu o Alpine Linux i dostępne dla architektur:

- amd64
- arm/v6
- arm/v7
- arm64

Minimalne wymagania dla Routinator: RAM — 1 GB, HDD — 4GB.

Instalacja i konfiguracja Routinator

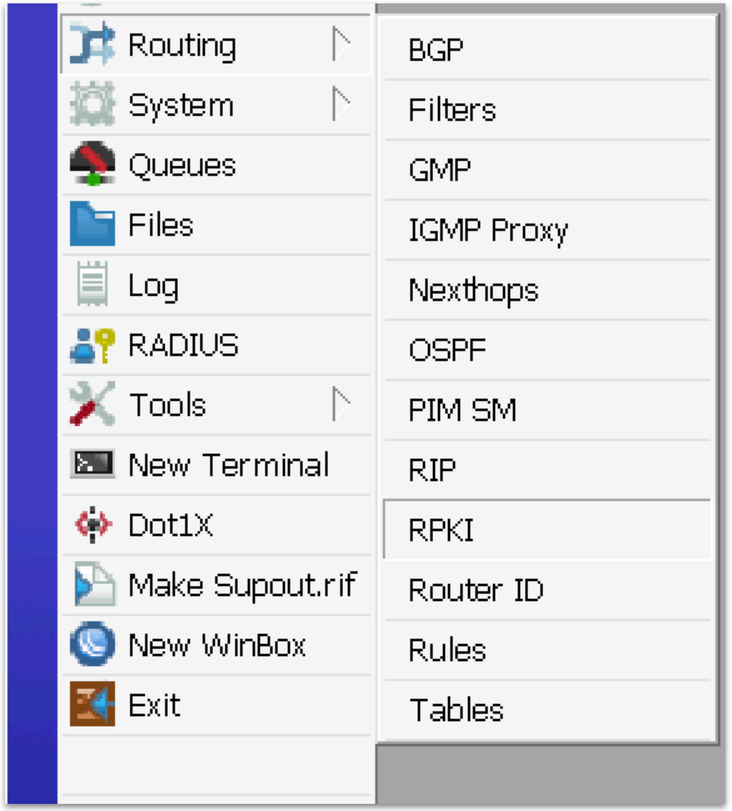
Uruchomienie kontenera (może się różnić od systemu operacyjnego):

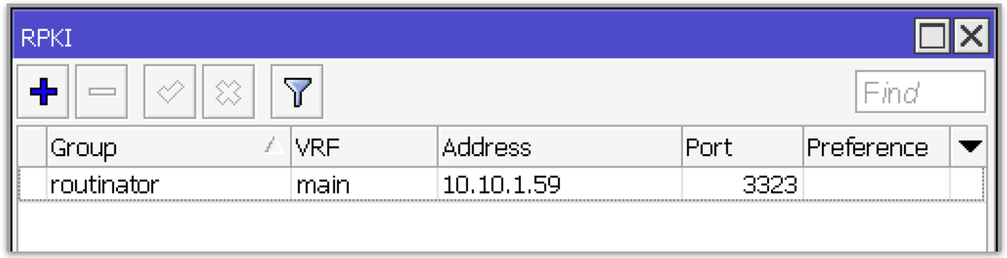
```
sudo docker run -d --restart=unless-stopped --name routinator \
    -p 3323:3323 \
    -p 8323:8323 \
    nlnetlabs/routinator
```

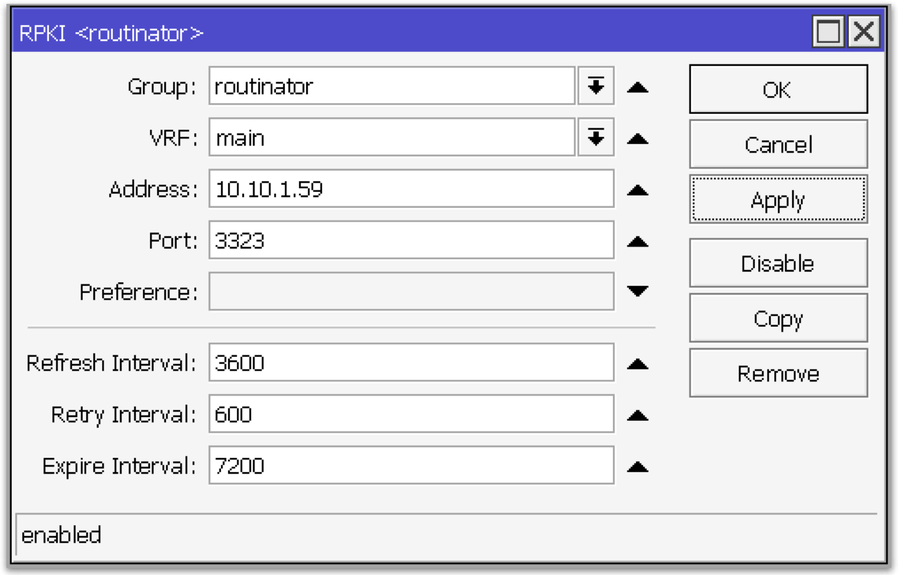
Porty używane kontenerem:
tcp/3323 — *rtr*
tcp/8323 — *http*
tcp/9556 — *prometheus exporter*

https://routinator.docs.nlnetlabs.nl/en/stable/installation.html#binary-packages

Routinator I ROS7








```
/routing rpki
add address=10.10.1.59 disabled=no group=routinator port=3323
```

https://help.mikrotik.com/docs/display/ROS/RPKI

Routinator I ROS7

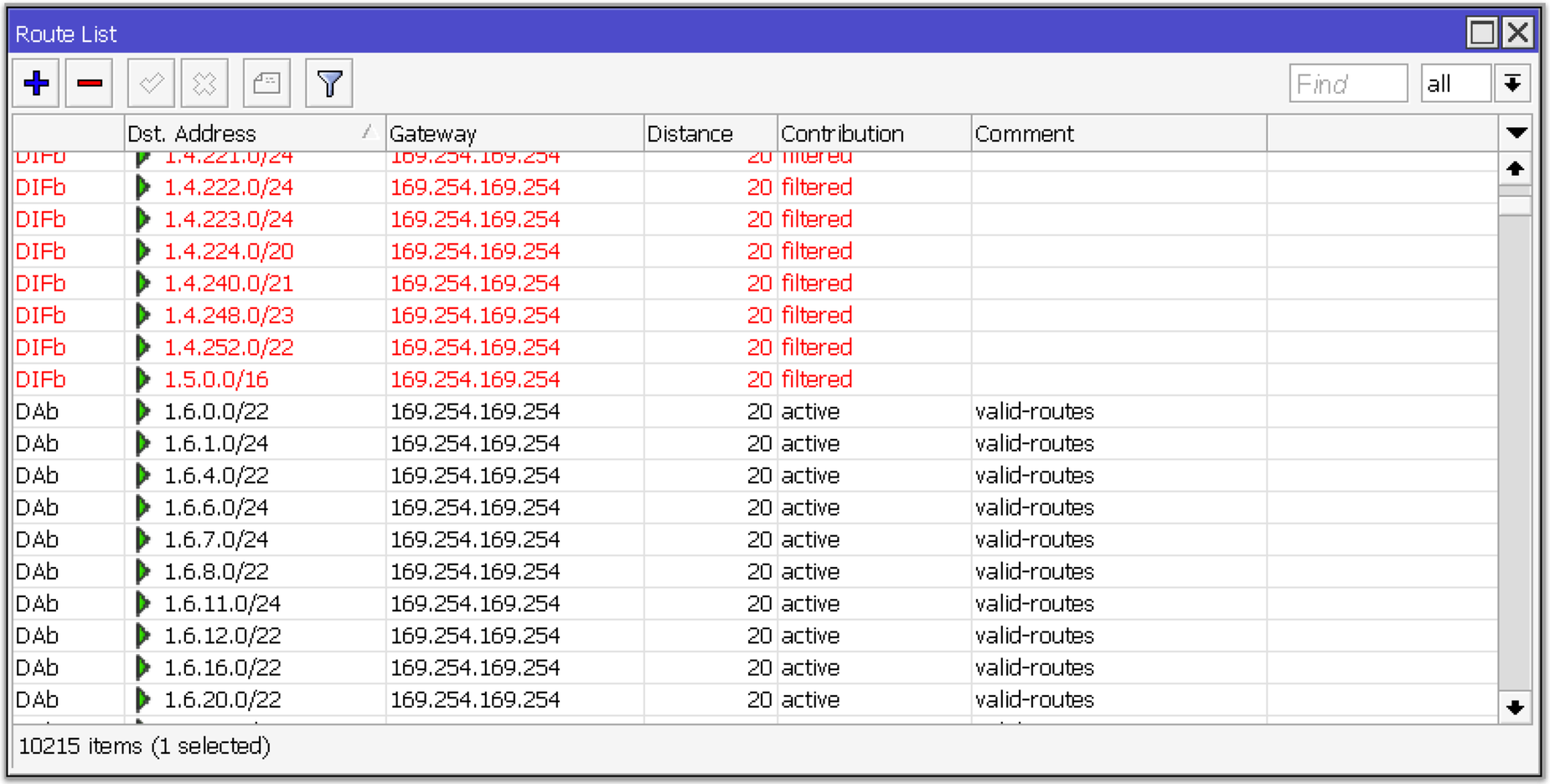
Dla sprawdzania prefiksów należy dodać reguły do filtra w routing-u.

```
/routing filter rule
add chain=vultr-bgp-in disabled=no rule="rpki-verify routinator"
add chain=vultr-bgp-in disabled=no rule="if (dst in 0.0.0.0/0 && gw == \
    169.254.169.254 && rpki valid) {set comment valid-routes; accept;}"
```

169.254.169.254 adres bramy od operatora, który należy zamienić na swój

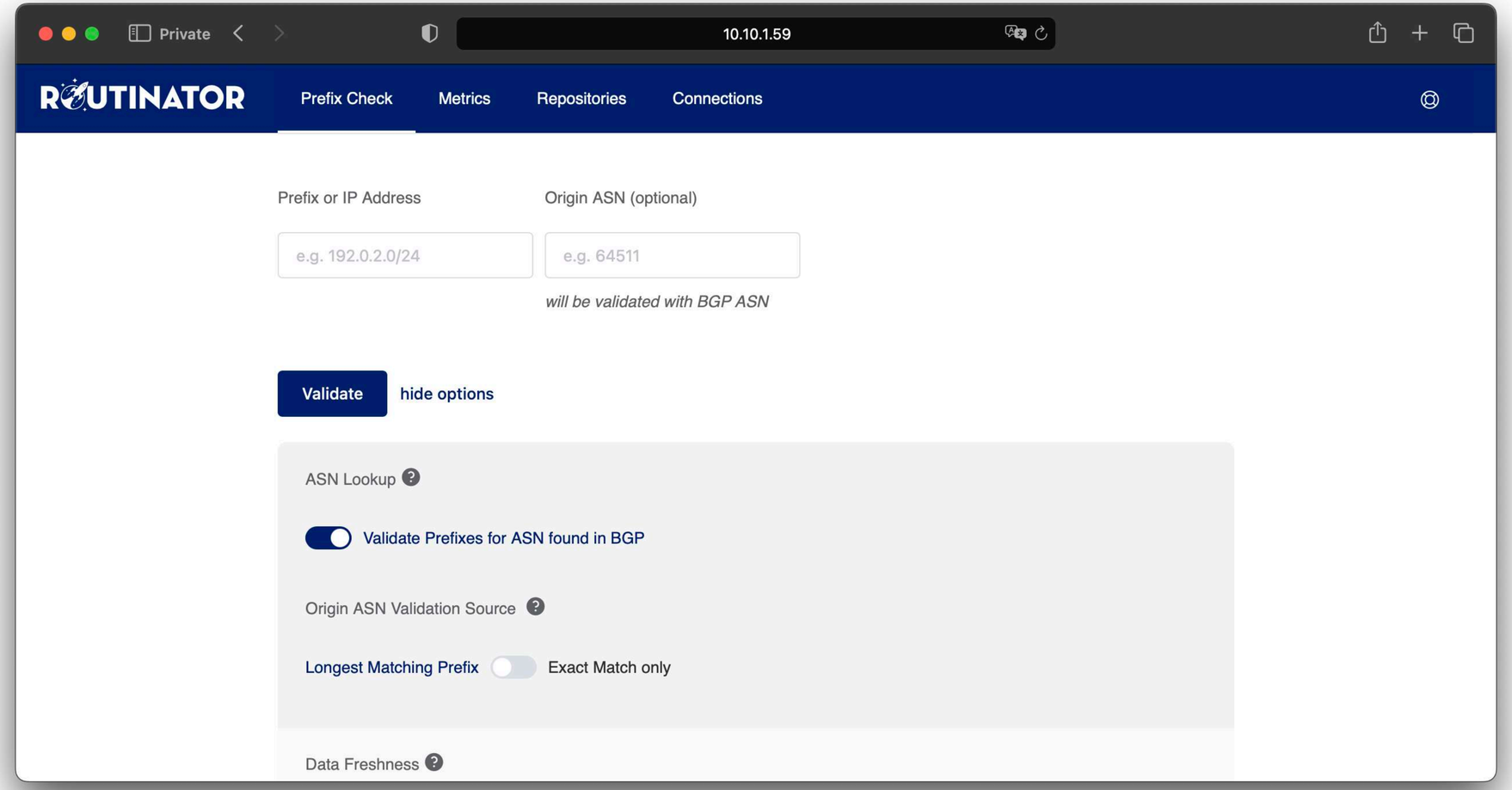
Routinator I ROS7

Wynik działania



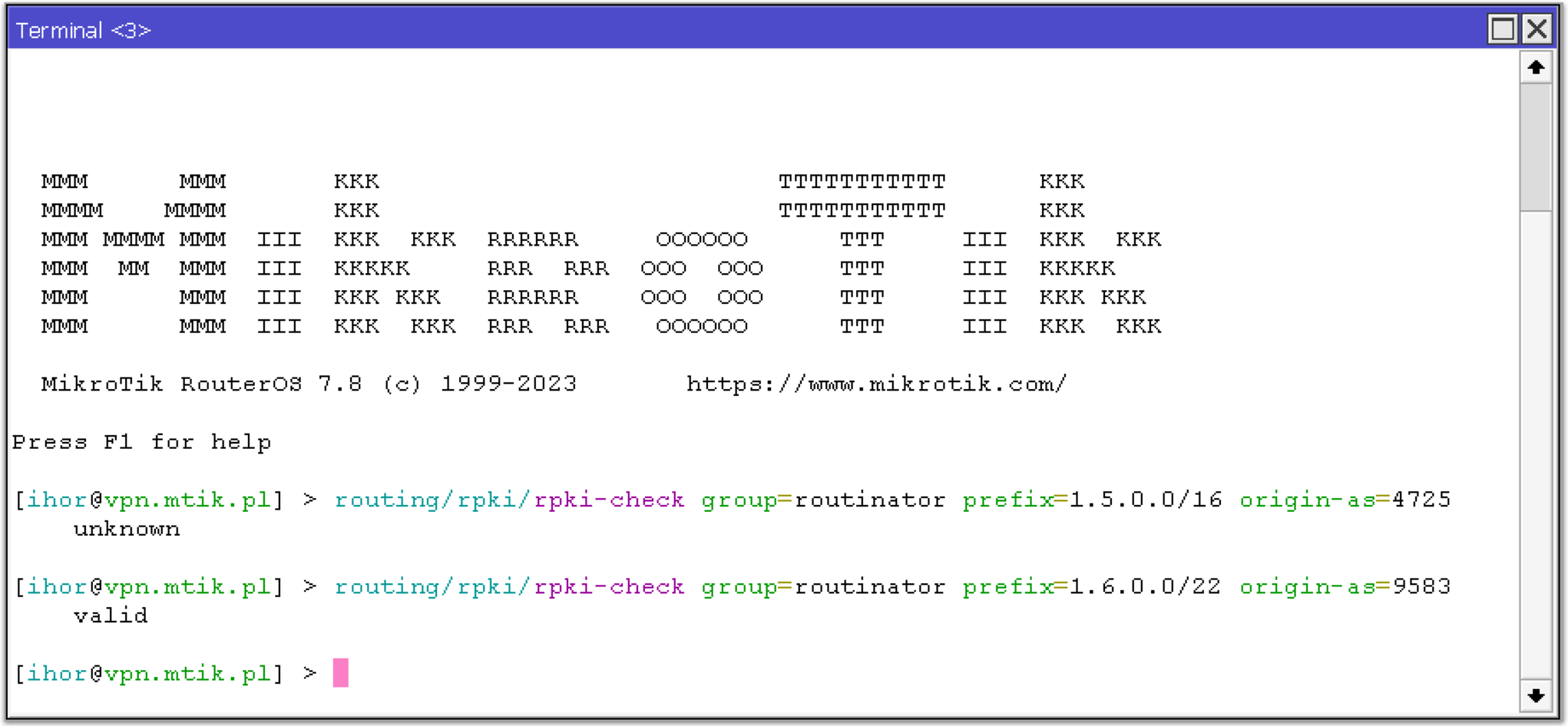
Routinator

Sprawdzanie prefiksów za pomocą strony WWW



Routinator

Sprawdzanie prefiksów za pomocą ROS CLI



Przyszłość rozwoju

Obecnie jest opublikowany *draft* protokołu RTR
https://datatracker.ietf.org/doc/html/draft-ymbk-8210bis-00

Także dla sprawdzanie *AS_PATH* parametru za pomocą protokołu ASPA, *draft* jest opublikowany
https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-05

Dziękuję

e-mail: ihor@hreskiv.pl