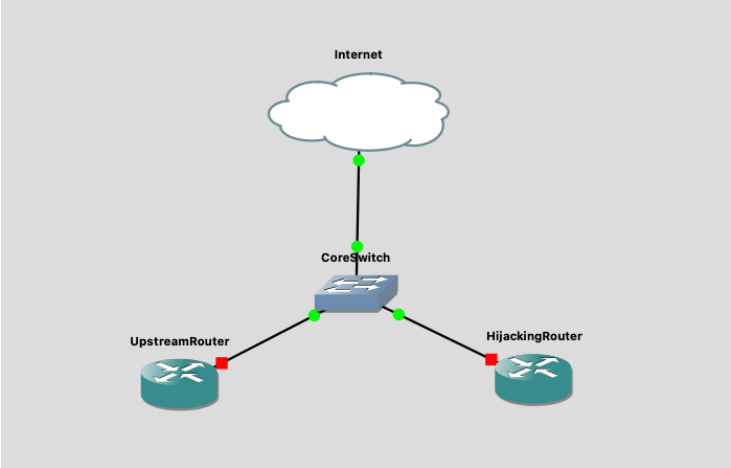
IDNIC RPKI Hands On Lab v5

Updated 23 August 2020

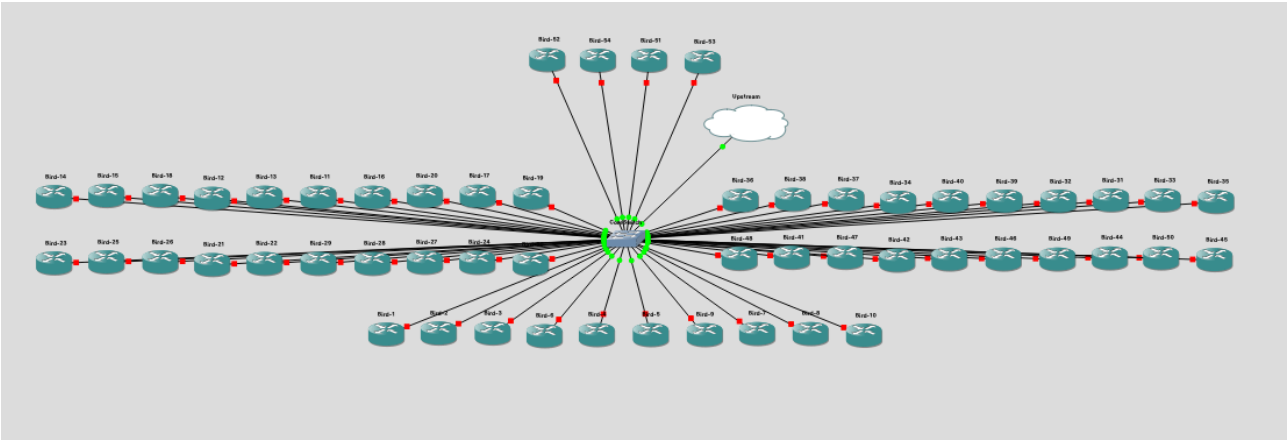
By: David Aditya Yoga Pratama
IDNIC Trainer

Topologi

Upstream



Peserta



Peer IP

Upstream Router 172.31.11.1 AS63880
Hijacking Router 172.31.11.2 AS63381

Konfigurasi Routinator

Cara masuk ke routinator

ssh -p <Port Routinator Anda> webinar@vlab.idnic.net
password : rpki2020

contoh
ssh -p 10301 webinar@vlab.idnic.net

Instance routinator pada lab ini sudah terinstall software routinator untuk menjalankan service routinator bisa dilakukan dengan perintah berikut:

```
routinator init  --accept-arin-rpa
routinator --verbose server --rtr <IP Server>:3323 --http <IP Server>:9556
```

Cara instalasi routinator bagi anda yang ingin mencobanya kembali di server anda setelah training ini adalah sebagai berikut:

Step 1
Install library-library pendukung

```
apt update
apt install ca-certificates rsync build-essential
```

Step 2
Install Rust & Routinator

```
curl --proto '=https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
source ~/.cargo/env
cargo install --locked routinator
```

Step 3
Start Routinator

```
routinator init  --accept-arin-rpa
routinator --verbose server --rtr <IP Server>:3323 --http <IP Server>:9556
```

Konfigurasi Mikrotik

Cara masuk ke routinator

ssh -p <Port Mikrotik Anda> admin@vlab.idnic.net
tanpa password

contoh
ssh -p 10301 admin@vlab.idnic.net

Sejak versi v7beta1 MikroTik sudah mengimplementasikan support untuk melakukan filtering route dengan RPKI. Berikut ini adalah dasar konfigurasinya.

Konfigurasi ROS v7 berbeda dengan v6. Beberapa perbedaan utamanya pada menu routing bgp adalah tidak adanya menu instance & peer. Menu-menu tersebut digantikan dengan menu berikut

1. Template
2. Connection
3. Peer Cache

A. Konfigurasi BGP di Mikrotik

1. Konfigurasi Template (BGP Instance di mikrotik v6)

/routing/bgp/template/set 0 as=<ASN Anda>

2. Konfigurasi Connection (BGP Peer di mikrotik v6)

Peer ke Router Upstream

/routing/bgp/connection/add remote.address=172.31.11.1 .as=63880 .role=ebgp connect=yes

Peer ke Router Upstream

/routing/bgp/connection/add remote.address=172.31.11.2 .as=63881 .role=ebgp connect=yes

B. Implementasi RPKI di Mikrotik

1. Mengkoneksikan MikroTik ke RPKI Validator
Step pertama adalah menghubungkan MikroTik dengan RPKI validator

```
/routing/bgp/rpki
add group=<Nama Validator> address=<IP
Validator> port=<Port Validator> refresh-interval=20
```

<Nama Validator> diisi dengan nama RPKI validator format pengisiannya berupa abjad & angka contoh VALIDATOR
<IP Validator> adalah IP routinator sesuai pembagian dari trainer

<Port Validator> adalah port yang digunakan saat melakukan inisialisasi routinator, default nya 3323

2. Melakukan pengecekan status ROA di MikroTik

```
/routing/rpki-check
group=<Nama Validator> prfx=<IP> origin-as=<ASN>
```

<Nama Validator> diisi dengan nama RPKI validator format pengisiannya berupa abjad & angka contoh VALIDATOR
<IP> adalah prefix yang akan dicek
<ASN> adalah ASN yang akan dicek

3. Drop RPKI Invalid MikroTik

```
/routing/filter/rule
add chain=bgp_in rpki-verify=<Nama Validator>
add chain=bgp_in match-rpki=invalid action=reject
add action=accept
```

<Nama Validator> diisi dengan nama RPKI validator format pengisiannya berupa abjad & angka contoh VALIDATOR

Konfigurasi Router Bird

Router bird sudah mendukung RPKI. Untuk menggunakan protokol RPKI, kita harus menginstall libssh terlebih dahulu sebelum melakukan compile router Bird.

ssh -p <Port Bird Anda> webinar@vlab.idnic.net
password: rpki2020

contoh
ssh -p 10301 webinar@vlab.idnic.net

Step 1
Install library-library pendukung

```
apt-get update
apt-get install make gcc g++ flex bison libssh-dev musl libncurses-dev libreadline-dev
```

Step 2
Install Bird Routing Daemon

```
wget ftp://bird.network.cz/pub/bird/bird-2.0.6.tar.gz
tar zxf  bird-2.0.6.tar.gz
cd bird-2.0.6/
./configure --prefix=/usr --sysconfdir=/etc
make -j2
make install
cat /dev/nul  > /etc/bird.conf
```

Konfigurasi Bird

```
log "/var/log/bird.log" { debug, trace, info, remote, warning, error, auth, fatal, bug };
router id <IP Server>;

roa4 table ROA4;
roa6 table ROA6;

protocol kernel {
    learn;
    persist;
    ipv4 {
        import all;
        export filter {
            if proto = "direct1" then reject;
            accept;
        };
    };
}


protocol device {
        scan time 60;
}

protocol direct {
        ipv4;
        interface "eth0";
}

protocol rpki VALIDATOR {
        roa4 { table ROA4; };
        roa6 { table ROA6; };
        remote <IP RPKI Validator>;
        port 3323;
        refresh keep 30;
        retry keep 30;
        expire keep 3600;
        transport tcp;
}

filter peer_in_v4 {
        if (roa_check(ROA4, net, bgp_path.last) = ROA_INVALID) then
        {
                print "Ignore invalid ROA ", net, " for ASN ", bgp_path.last;
                reject;
        }
        accept;
}
```

```
filter accept_all {
	accept;
}

protocol bgp REAL{
	debug all;
	local <IP Router> as <AS Anda>;
	multihop;
	neighbor 172.31.11.1 as 63880;
	ipv4 {
		import keep filtered;
		import filter peer_in_v4;
		export filter accept_all;

	};
}


protocol bgp HIJACKER{
	debug all;
	local <IP Router> as <AS Anda>;
	multihop;
	neighbor 172.31.11.2 as 63881;
	ipv4 {
		import keep filtered;
		import filter peer_in_v4;
		export filter accept_all;

	};
}
```

Konfigurasi Cisco

Berikut ini adalah konfigurasi cisco untuk melakukan filtering berdasarkan status ROV.

Cisco-GROUP_A1#sh running-config

```
router bgp <ASN>
 bgp router-id <IP Router>
 bgp log-neighbor-changes
 bgp rpki server tcp <IP Validator> port 3323 refresh 60
 bgp bestpath prefix-validate allow-invalid
 neighbor 172.31.11.1 remote-as 63880
 neighbor 172.31.11.1 description To.Router.Valid
 neighbor 172.31.11.1 soft-reconfiguration inbound
 neighbor 172.31.11.1 route-map RPKI-PESERTA-<No Urut> in
 neighbor 172.31.11.2 remote-as 63881
 neighbor 172.31.11.2 description To.Router.Hijacking
 neighbor 172.31.11.2 soft-reconfiguration inbound
 neighbor 172.31.11.2 route-map RPKI-PESERTA-<No Urut> in
!
!
!
route-map RPKI-PESERTA-<No Urut> permit 10
 match rpki invalid
 set local-preference 50
!
route-map RPKI-PESERTA-<No Urut> permit 20
 match rpki not-found
 set local-preference 100
!
route-map RPKI-PESERTA-<No Urut> permit 30
 match rpki valid
 set local-preference 200
!
```