RPKI: What the Day One Book doesn't tell you

Niels Raijer, NLNOG Day, 6 September 2019

DAY ONE: DEPLOYING BGP ROUTING SECURITY IN JUNOS

This book is intended for network administrators running Junos OS routers in the BGP default-free zone. It provides field-tested device and protocol configurations for creating a secure and stable network, as well as brief background information needed to understand and deploy these solutions in your own environment. Any network administrator may find the contents of the book interesting, but the real value is for those running a BGP network without having a default route present in their network (or accepting such a route from their upstream provider): the default free zone. .

"xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx.."

Jane Doe, VP, Deer Networks

"xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx. xxxx xxx xxxxxxx xx xx x xxxxxxxxxxx.."

Joe Buck, VP, Deer Networks

IT'S DAY ONE AND YOU HAVE A JOB TO DO, SO LEARN HOW TO:

- Understand the relevance of filtering routes as you learn them from your customers, peers, and transits.
- Understand what portion of via BGP received routes should be rejected for securing your routing table.
- Implement routing policies that reject invalid routing information.
- Understand and implement redundant Resource Public Key Infrastructure (RPKI) validators.
- Verify your configuration and support your network using basic troubleshooting commands.
- How to use RIR tools to make sure your routes and prefixes are accepted by other Internet Service Providers who filter and/or have deployed RPKI

ISBN 978-1-941441-82-4
52000
9 781941 441824

JUNIPER NETWORKS

DAY ONE: DEPLOYING BGP ROUTING SECURITY IN JUNOS

Aelmans & Raijeri

JUNIPER NETWORKS | Engineering Simplicity

DAY ONE: DEPLOYING BGP ROUTING SECURITY IN JUNOS

By Melchior Aelmans & Niels Raijer

RPKI implementation

- Last year I was here telling y'all to work on RPKI
- Filtering your transits is easy
- Filtering your peers is easy
- Filtering your customers is not so easy, but we managed to filter all* our customers since a month or so
    - * All customers? No … a small village in the northwest of Gallia resists

The case of the private AS

- We have customers who use BGP (because of blackholing, graceful shutdown and outstanding redundancy) but with a private AS, announcing our own prefixes to us

- RPKI considers these invalid

- Solution: create static ROAs on the core routers for now (in future: automate this on our validators)

```
group CUST-65530 {
    type external;
    description "CUST: 09999 - Job Snijders Enterprises Inc.”;
    import [ TRANSIT-CUSTOMER IMPORT-65530 REJECT-ALL ];
    export EXPORT-DEFAULT-ROUTE;
    remove-private;
    peer-as 65530;
    neighbor 37.139.1xx.1xx {
```

```
routing-options {
    validation {
            record 37.139.1xx.xxx/28 {
                maximum-length 28 {
                    origin-autonomous-system 65530 {
                        validation-state valid;
                    }
                }
            }
```

The case of the blackhole

- Customers can send us the RFC 7999 blackhole community 65535:666

- They can install blackholes via our web portal

- Some of these will have the wrong origin AS and RPKI will consider them invalid

- So of course I’m not here to tell you to skip RPKI checks for blackhole routes!

```
niels@CR0.NIKHEF.NL> show configuration policy-options policy-statement TRANSIT-CUSTOMER
term BLACKHOLE {
    from community BLACKHOLE-GLOBAL;
    then next policy;
}
[…]
niels@CR0.NIKHEF.NL> show configuration policy-options policy-statement IMPORT-65530
term BLACKHOLE-GLOBAL {
    from {
        family inet;
        community BLACKHOLE-GLOBAL;
        prefix-list-filter AS65530 orlonger;
    }
    then {
        next-hop discard;
        accept;
    }
}
[…]
```

The case of the blackhole (2)

- Work is being done by NTT, Telia and pmacct, because this clearly needs to be addressed before The Big Guys can do RPKI checks on their customers

- http://iepg.org/2019-03-24-ietf104/blackholing_reconsidered_ietf104_snijders.pdf

Questions? Or, rather, suggestions?