Being a better Netizen: MANRS @ DO

Tim Raphael

Senior Network Engineer,
Internet Edge and Backbone

NANOG 86 - Hollywood, CA
October 17-19, 2022
Contents

Who is DigitalOcean? 03
What is MANRS? 04
Why become MANRS compliant? 05
Requirements 06-07
What we did 08-31
What’s next 32-34
14 data centers in 8 global markets
An intro to MANRS

 Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

 MANRS operates four key programs that target Network Operators, Internet Exchange Points, Cloud and CDN Providers and Equipment Vendors to help improve their routing security posture.

 MANRS also offers Fellowship and Ambassador programs to engage motivated individuals of the Internet community. By participating you’ll talk about routing security issues and provide valuable input to drive the state of the art among existing and new member organizations.
Why become MANRS Compliant?

Our community is bigger than us.

- A Core Value at DigitalOcean
MANRS Cloud & CDN Program

Action 1:
Prevent propagation of incorrect routing information.

“... Whenever feasible, participants should check that the announcements originate from legitimate holders.”

Action 2:
Prevent traffic with illegitimate source IP addresses

“Implement anti-spoofing controls to prevent packets with illegitimate source IP address from leaving the network.”

Action 3:
Facilitate global operational communication and coordination

“Maintain globally accessible up-to-date contact information in PeeringDB and relevant RIR databases.”

Ref: https://www.manrs.org/cdn-cloud-providers/
MANRS Cloud & CDN Program

Action 4:
Facilitate validation of routing information on a global scale

"... routing information needs to be properly registered in public routing repositories... The two main types of repositories are IRRs and RPKI."

Action 5:
Encourage MANRS adoption

"A publicly available policy, a peering form or an email template with a recommendation to implement MANRS."

Ref: https://www.manrs.org/cdn-cloud-providers/
Action 1: Filtering

*Prevent propagation of incorrect routing information.*
Challenges

DigitalOcean runs a medium-large global network that peers with hundreds of ASNs on many of the biggest peering fabrics in the world.

Analysis and automation is required to find a workable solution that provides appropriate knobs to control for our scale.
Action 1: Filtering

Analysis

By collating IRR data related to our peers, I was able to look at the configuration impact of per-peer prefix filtering.

What is the sweet spot for making a meaningful improvement in routing security without compromising our current platform?

Generate prefix list length for each IRR object.

Aim to make a meaningful improvement to Routing Security.

Don’t compromise the network of today.
Action 1: Filtering

Analysis
Analysis

A cumulative graph provides a clearer perspective for determining where to draw the line to meet our needs today.

Limit the number of config lines to suite today’s platform but pick a limit that can be increased in the future easily.

100% coverage would result in ~6.5M LoC on some routers.

2M LoC ~ 95 sec apply times.

Picked a sensible point to maximise coverage within limitations.
Action 1: Filtering

Analysis
Action 1: Filtering

The heavy lift...

- **IRRd, Netbox and Peering Manager** for Source-of-Truth
- **SaltStack** to build prefix-lists and templates.
- Continual, automatic updates pushed to the network every 6 hours.
Action 1: Filtering

The outcome...

neighbor 192.0.2.1 {
    description "Example Network Name";
    import [ SCRUB-IMPORT-IPv4
    IX-IMPORT
    ABCIX-BILAT-IMPORT-IPv4
    AS65535-IX-IMPORT-IPv4 ];
    family inet {
        unicast {
            prefix-limit {...}
        }
    }
    export ABC-PEER-EXPORT;
    peer-as 65535;
}
The outcome...

> show policy-options policy-statement \n  AS65535-IX-IMPORT-IPv4

term ALLOW-RPKI-VALID {...}
term AS65535 {
  from {
    protocol bgp;
    prefix-list AS65535v4; ←
  }
  then {
    community add DO-IRR-VALID;
    accept;
  }
}
term DEFAULT-REJECT {...}

Filter on RPKI first
Filter by IRR second
Tag with useful communities as you go.
The outcome...

route-policy RP-AS65535-IMPORT-IPv4
apply RP-SCRUB-IN-IPV4
apply RP-IX-IMPORT
apply RP-ABCIX-BILAT-IMPORT-IPv4
if validation-state is valid then
  pass
else if destination in AS65535v4 then
  pass
else
  drop
end-policy
A quick shout out:

Mircea Ulinic

- Network Development Lead @ DigitalOcean
- Core maintainer for NAPALM
- Contributor to SaltStack (2017 Contributor of the year)
Action 2: Anti-Spoofing

Prevent traffic with illegitimate source IP addresses
Action 2: Anti-Spoofing

We already prevent spoofing!

Given DigitalOcean runs such a huge number of workloads, bad actors and spoofed traffic isn’t a new challenge. We already have several layers of protection to ensure that all traffic originating from DO is from legitimate sources.

Control from the hypervisor.

Internal detection tooling.

uRPF deployed on the edge of the network.
To be sure?

It’s best practice to ensure that our mechanisms to prevent spoofing are actually working. When they aren’t, we want to have a clear signal when they no longer are.

The CAIDA Spoofer project to the rescue! We run spoofer nodes in each of our DCs that attempt to send spoofed traffic to the public CAIDA endpoint. A Prometheus exporter regularly queries the public CAIDA API and will alert us if spoofed traffic is received.

Ref: https://www.caida.org/projects/spoofer/
To be sure?

alerts:
- alert: CAIDA Session Received
  expr: caida_spoofer_session == 1
  labels:
    service: CAIDA
    severity: warning
    instance: "caida-spoofer::${labels.session}" 
  annotations:
    playbook: <a href="https://doplaybooksite.tld/CAIDA+Spoofers+Servers" target="_blank">CAIDA Spoofers</a>
Action 3: Coordination

Facilitate global operational communication and coordination
How to find us...

We keep our WHOIS data up-to-date as we on-board new IP space through a regularly used playbook. This ensures all the same data is present on all our prefixes:

```bash
➜ ~ whois `host me.timraphael.com` 
    | awk '{print $4}' | grep Email
OrgTechEmail:  noc@digitalocean.com
OrgNOCEmail:  noc@digitalocean.com
OrgAbuseEmail:  abuse@digitalocean.com
```
## Action 3: Coordination

### How to find us...

Because we rely on our peering partners to keep their PeeringDB record up-to-date for automation reasons, we should set the best example and do so as well.

<table>
<thead>
<tr>
<th>DigitalOcean</th>
<th>Peering Policy Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>DigitalOcean</td>
</tr>
<tr>
<td>Also Known As</td>
<td>Digital Ocean</td>
</tr>
<tr>
<td>Long Name</td>
<td></td>
</tr>
<tr>
<td>Company Website</td>
<td><a href="https://www.digitalocean.com">https://www.digitalocean.com</a></td>
</tr>
<tr>
<td>ASN</td>
<td>14061</td>
</tr>
<tr>
<td>IRR as-set/route-set</td>
<td>AS-14061</td>
</tr>
</tbody>
</table>

**Contact Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Phone</th>
<th>E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abuse</td>
<td>Abuse</td>
<td></td>
<td><a href="mailto:abuse@digitalocean.com">abuse@digitalocean.com</a></td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations</td>
<td></td>
<td><a href="mailto:noc@digitalocean.com">noc@digitalocean.com</a></td>
</tr>
<tr>
<td>Policy</td>
<td>Peering</td>
<td></td>
<td><a href="mailto:peering@digitalocean.com">peering@digitalocean.com</a></td>
</tr>
</tbody>
</table>
Action 4: Global Validation

Facilitate validation of routing information on a global scale
We publish our routing data!

Given we allocate prefixes on a per-region basis, we need to ensure that the correct prefix lengths are kept up-to-date in our IRR objects. We use a scheduled “cron” job deployed to our internal application stack to ensure our IRR objects are accurate.
Action 4: Global Validation

We publish our routing data!

We use covering ROAs with max-prefix-length populated to ensure we have valid ROAs for the prefixes we intend to advertise.

<table>
<thead>
<tr>
<th>Routing completeness (IRR)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unregistered</td>
<td>0</td>
</tr>
<tr>
<td>Registered</td>
<td>735</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Routing completeness (RPKI)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>724</td>
</tr>
<tr>
<td>Unknown</td>
<td>11</td>
</tr>
<tr>
<td>Invalid</td>
<td>0</td>
</tr>
</tbody>
</table>

Automated IRR updates.

RPKI ROA coverage.

Automated alerting for non-compliance using Netbox reports.
We publish our routing data!

Netbox reports are used to check for compliance and give us strong alerting signals when things aren't correct.

<table>
<thead>
<tr>
<th>Report Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td><strong>test_announce_roa</strong></td>
</tr>
<tr>
<td>2022-02-20T14:42:19.708340+00:00</td>
</tr>
<tr>
<td><strong>test_aggregates_radb</strong></td>
</tr>
<tr>
<td>2022-02-20T14:42:00.073470+00:00</td>
</tr>
<tr>
<td>2022-02-20T14:42:00.155129+00:00</td>
</tr>
</tbody>
</table>
Action 5: Encourage Adoption

Encourage MANRS adoption
Action 5: Encourage Adoption

Simple as...

"...Peers are encouraged to implement Mutually Agreed Norms for Routing Security (MANRS) - [https://www.manrs.org](https://www.manrs.org)."

[https://as14061.net/](https://as14061.net/)
Compliance
DigitalOcean Joins MANRS Initiative to Combat Routing Security Threats

By Tim Rachael

Today we are pleased to announce that DigitalOcean has joined the Mutualy Agreed Norms for Routing Security (MANRS) initiative for CDN and Cloud Providers to reduce common routing security threats. The initiative, supported by the Internet Society, outlines actions network operators should take to improve the resilience and security of routing infrastructure.

https://www.digitalocean.com/blog/digitalocean-joins-manrs
What next?
Visibility is everything...

To help our peers we intend to launch an externally-facing looking glass that can help debug routing issues. To fit in with our other MANRS obligations we should ensure that RPKI status, route filtering status and various other aspects of routing policy are made clear with this tool.
Improvement never ends...

While most of our processes are automated, there is always those few that aren’t - we're continually aiming to improve automation coverage where it makes sense.

With the onset of a global network overhaul, new equipment gives us new capability to improve our filtering coverage.

Lastly, alerting and subsequent actions can always be improved as we experience new challenges and failure modes to learn from.
Thank you