Validating MANRS of a network

Andrei Robachevsky

robachevsky@isoc.org

Mutually Agreed Norms for Routing Security

MANRS provides baseline recommendations in the form of Actions

- Distilled from common behaviors – BCPs, optimized for low cost and low risk of deployment
- With high potential of becoming norms

MANRS builds a visible community of security minded operators

- Social acceptance and peer pressure

MANRS

MANRS for Network operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

Commitment, transparency and credibility

Inform and improve MANRS participants about their degree of commitment

- Establish measurable indicators of MANRS readiness
- Publish through the MANRS Observatory (https://observatory.manrs.org/)

MANRS Observatory provides a view from the outside (with its limitations), but how does the network really looks for the inside? Create a local auditing tool. It will automate parsing router configurations to detect a wide range of common configuration issues

- Help network engineers secure their eBGP speaking routers, implement MANRS actions to prevent spoofed traffic, secure BGP route policy and help validate global routesWhile
- Potentially use this as a complementary indicator for MANRS readiness when evaluating an application

Project vision

A locally run tool for auditing BGP and anti-spoofing configurations on various platforms

Tool will take in a configuration file and output a report showing how well the router did against the pre-defined rules

- MANRS is a first candidate, but there may be other sets
- Audit configs from different vendors/OSes

What kind of checks?

Action 1 – Filtering

- Are inbound routing advertisements from customers and peers secured by applying prefix-level filters?
- Is the router configured to connect to a RPKI-to-Router interface for ROA validation? Is the router configured to drop RPKI invalids?

Action 2 – Anti-spoofing

- Is uRPF strict mode enabled on interfaces connected to customers?
- Are there ACLs applied to stub customers to prevent them from sending spoofed traffic?

More difficult kind of checks

Action 1 – Filtering

- Are prefix-level filters dynamically applied from IRR entries?
- Do prefix filters match the customer cone?

Action 2 – Anti-spoofing

- Are the ACLs correctly match customer’s network blocks?

Prototype Implementation

Developed as part of a hackathon at Charter Communications

Robot Framework based automatic router configuration analyzer

Use of a single, high level, cross-platform tool makes it more accessible to a broad range of users

Produces graphical/web based reports to make it easier to understand and act on the results

Extensible w/Python for more complex analysis if needed

Sample output

```
------------------------------------------------------------------------------
ACLs being applied to single homed stub customers to prevent them ... | FAIL |
'set interfaces et-0/0/0 description "CWDM4 testing"set interfaces et-0/0/0 unit 0 family inet address 192.168.1.2/24
' does not contain 'inet6 filter input'
------------------------------------------------------------------------------
Are inbound routing advertisements from customers and peers secure... | PASS |
------------------------------------------------------------------------------
Are inbound routing advertisements restricted to only /24 and shor... | PASS |
------------------------------------------------------------------------------
Are inbound routing advertisements restricted to only /48 and shor... | PASS |
------------------------------------------------------------------------------
Are inbound routing advertisements secured by applying AS-path fil... | PASS |
------------------------------------------------------------------------------
Are outbound routing advertisements to peers and transit secured b... | PASS |
------------------------------------------------------------------------------
Is the router configured to connect to a RPKI-to-Router interface ... | PASS |
------------------------------------------------------------------------------
Is the router configured to drop RPKI invalids?                       | PASS |
------------------------------------------------------------------------------
Are communities applied to routes recieved from customers? Are out... | PASS |
------------------------------------------------------------------------------
Is BGP TTL security (GTSM) applied to all BGP sessions?               | FAIL |
```

Screenshot courtesy Rich Compton and Pratik Lotia

Reports

Check Cfg. Is there control plane policing enabled on TCP port 179 - IPv6?			yes	FAIL	ignore_case=True: 'admin@ENWECORZB0J-BCR04> show configuration | display set set version 17.4R1-S4.2 set groups re0 interfaces em0 unit 0 family inet address 10.240.32.27/23 set groups re0 interfaces em0 unit 0 family inet6 address 2605:1c00:50f3:67::32:27/64 set groups re0 routing-options static route 0.0.0.0/0 next-hop 10.240.32.1 deactivate groups re0 routing-options static route 0.0.0.0/0 set groups re0 routing-options static route 172.30.104.0/24 next-hop 10.240.32.1 set groups re0 routing-options static route 172.30.105.0/24 next-hop 10.240.32.1 set groups re1 interfaces em0 unit 0 family
Check Cfg. uRPF check on all interfaces - IPv4			yes	FAIL	'set interfaces et-0/0/0 description "CWDM4 testing"set interfaces et-0/0/0 unit 0 family inet address 192.168.1.2/24 ' does not contain 'inet rpf-check'
Check Cfg. uRPF check on all interfaces - IPv6			yes	FAIL	'set interfaces et-0/0/0 description "CWDM4 testing"set interfaces et-0/0/0 unit 0 family inet address 192.168.1.2/24 ' does not contain 'inet6 rpf-check'
Check Cfg. Are communities applied to routes recieved from customers? Are outbound filters applied to match only routes carrying the correct commmunity attribute?			yes	PASS	
Check Cfg. Are inbound routing advertisements from customers and peers secured by applying prefix-level filters?			yes	PASS	
Check Cfg. Are inbound routing advertisements restricted to only /24 and shorter for IPv4?			yes	PASS	
Check Cfg. Are inbound routing advertisements restricted to only /48 and shorter?			yes	PASS	

Screenshot courtesy Rich Compton and Pratik Lotia

From a prototype to a tool

Beta-test the prototype.

- Verify that the results that the tool is outputting are results that people can actually use and will help them
- Verify that people would actually use this tool. If not, then it's not worth putting in time to work on it. I'm not sure how we can verify this. Maybe a survey?

Increase the platforms supported by the tool.

- Populate a “library” of configurations: what is the priority – MikroTik, Cisco IOS, Huawei?

Share the tool with others to encourage them to use it.

Could this be useful?

Would like to contribute?

manrs@isoc.org