

### **Tutorial: Running BGP in 2019**

and the contraction of the first and conditional and addition and additional and the construction and tradition in the

Eugene Bogomazov Qrator Labs



## Why we?

- Qrator Labs
  - DDoS mitigation
  - Own Anycast network

aanstaaaataa dhadan taadaankaadaalaan<u>nadilkanaatalilkaaaalkaaaanaaaaastaaaataaa</u>

- Radar
  - Where to place nodes?
  - BGP monitoring



#### What it's all about

aanataa aa dhadaa aa daan daadhadhadhadhadhadhaa aa daddhaa addhaa aa mataa aa baadhadhabata

- BGP BCP
- Analytics/Toolset
- Modern trends/security
- ROA party
  - But without booze :(



#### What it's not about

- Inner ISP structure
- Command examples
- Configuration automation
  - Templates
  - Validation
  - Deployment
- Must to follow recomendations



#### **Ideal** world

- Read the standards
- Get ASN and prefixes

aure Laure Lauri India de Lauri and anni and an India mai alaid Ingara I<u>l Ingara ann agus an aitead i an i</u> baile a

- Set a configuration
- And that's all...



### But...





### **Cruel world**

Implementation doesn't follow standards

emetacado albata da anticada de la la matellita castal libra ad libra anticada de la companya de la contradici

- Cheap/old hardware
- Incorrect/outdated configurations
- Curved arms
- Attackers



### We have a situation

aanataaaattaa dhadan taalaandaadhadhadhadhadhadhtaaataladhtaaaalhaaaannataaaattaadhadhta

- Nobody likes problems
  - At least their own
- Guiding stone
  - Prevention
  - Investigation
  - Mitigation



#### What it's all about

aanataaaattaa dhadan taalaandaadhadhadhadhadhadhtaaataladhtaaaalhaaaannataaaattaadhadhta

- **BGP BCP**
- Analytics/Toolset
- Modern trends/security
- ROA party



#### Where to start?

- We need an operational BGP BCP!
  - But we already have one (BCP194)
- Snijders presentations (here or here)
- Example of filters http://bgpfilterguide.nlnog.net/



### **TCP** security

- Basic ACL
- TCP MD5/TCP AO
- GTSM (aka TTL hack)
  - Even in case of multihop sessions

aanataa aa dhadaa aa daan daadhadhadhadhadhadhaa aa daddhaa addhaa aa mataa aa baadhadhabata



### Prefix filter. Denial

aanataa aa dhadaa aa daan daadhadhadhadhadhadhaa aa daddhaa addhaa aa mataa aa baadhadhabata

- Special use
- Too specific
- Default
- From unwanted directions
  - IXP prefixes
  - Local prefixes



### **Prefix filter. Permition**

- Static customer prefixes whitelist
  - Just no
- IANA allocated space
  - Only for v6
- Dynamic filter based on IRR information

aanataa aa kaasibaahii aa daa aa baadhaa badha badha badh baasa da baasa aa aa baasa baasa dha bata b

- It's having its own problems
- Later...



### **AS\_PATH** filter

aanataa....taadindintaalaanihaalaalaannitillitanatalailitaa...dilitaa...altiaa...altiaa...altiaa...

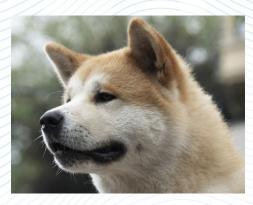
- Not covered by BCP
- Neighbor check
- Bogon ASN
- TIER\_1 filtering
- Other types?



### Leakage prevention

- Route Leak violation of policy
- Prevent with custom communities
- Prefix rate limiting
- Automation with BGP Roles

One problem:



a mata a alternativa taraka mita ariba di latini talih tama a latih tama alitina a ariba ara mata a ariba di m



### Community

- A way of marking routes
  - Carry information
  - Policy implementation
- Large Communities how to?
- Study your upstream capabilities
  - Geo/blacklist/"you name it" communities

energe en la company de la



# **Aggregation (rfd)**

Pretty often appeared (example)

- Decrease prefix max limit?
- BGPSec and ROA?
  - In case of updating routes
- Customers PI blocks?
  - In case of announcing own prefixes
- Do we really need it?



# **AS\_PATH length (rfd)**

- No limitation in RFC
- Someone was not ready (case, another)

aanataa aa kaasibaahaa malaandia adaallammadibbaa aa laidhaa adibaa aa mataa adaa dhadiidha

- Real distance is not so big
- Possible filtration can be applied
- But why?
  - And were is a border?



#### What it's all about

aanataaaattaa dhadan taalaandaadhadhadhadhadhadhtaaataladhtaaaalhaaaannataaaattaadhadhta

- BGP BCP
- Analytics/Toolset
- Modern trends/security
- ROA party



## Is something wrong?

and a continued and the description of the angle of the contribution of the contributi

- Business metrics
- Traffic drop
- Traffic raise
- Decreased number of users
- Increased number of tickets
- Or just intuition



### Yeah, investigation!

a mata a a la calibration da la mata ada al la fina del litera de la litera a al litera a mata a administrati

- Nature of a problem
  - Is it a BGP problem?
- What happened?
- Who is responsible?
- What to do next?



#### **Toolset**

- Ripe Atlas
- Ripe Widgets
- Public API
- Looking glasses
- Whois
- One possible example (not free)

aanalaassalaasiltostoi taalaanilaadissalaallannotallitanatalailitossaaltossaaninalaassalaasiltostoi t



### **Route analytics**

- BGP raw data
  - Ripe RIS, RV, PCH
- From MRT to human
  - bgpdump, bgpstream
- History player
  - BGPlay (but with 6 hour delay)

a mata a a la calinata da mata antica de alla matallita matala di bacca di bacca mata a a di badia di



#### In moment

- Ripe Atlas (framework)
  - But credits...
- Looking glasses
  - But pain (customized, without API, etc)

aanataa aa kaasibadan taadaan daasibadha maddibaasis dadbaasa dibaasa aa nataa aa baasibada ta

- Alternatives?
  - Ripe... API! (yeah, they have one)
  - Radar API (only paths)



### Why we need it?

- Find an attacker
- AS\_PATH manipulation?
  - Collect many routes
  - And neighbor check will save a day!

a mata a a la calinata da mata antica de alla matallita matala di bacca di bacca mata a a di badia di

- Except not always...
- In case of bad IP find an owner



#### Todo:

- Find abuse contact
  - Ripe method (or our)
- Write a letter
- Wait
- Or write a letter to special mailing list

aanataaaattaa dhadan taalaandaadhadhadhadhadhadhtaaataladhtaaaalhaaaannataaaattaadhadhta

And wait



#### Active?

- Create special filter
- Your address space under attack?
  - Hijack more specific announce
    - or delegate
  - Route leak AS\_PATH manipulation

and a continue of the feature of the administration and the continue of the co



#### What it's all about

aanataaaattaa dhadan taalaandaadhadhadhadhadhadhtaaataladhtaaaalhaaaannataaaattaadhadhta

- BGP BCP
- Analytics/Toolset
- Modern trends/security
- ROA party



#### **Main trends**

- Prevent accidental errors
  - Make explicit policies
  - Fail-safe strategy
  - Bring some automation in process

- Making life a little bit easier
  - Large Communities
  - Shutdown communication
  - Graceful shutdown



## uRPF (rfd)

Anti spoofing technique (BCP38, BCP84)

and a continue of the formation of a continue of the formation of the formation of the continue of the formation of the forma

- Based on BGP
  - Which is asymmetric
- Main enemy TE
- Modern draft is under development
  - Problem remains the same
- Someone use it?



### Security

Anything in route can be changed

aanstaaaataa dhabuttaalaankaadaalaallamatdikaa<u>atabbaaa dhaaaanstaaataaathabut</u>

- Anything
- Security by claiming
  - Route objects/IRR
  - ROA/RPKI
- Secure AS PATH



#### **IRR**

Create a Customer Cone with AS\_SET

aanataa aa dhadaa aa daan daadhadhadhadhadhadhaa aa daddhaa addhaa aa mataa aa baadhadhabata

- We all know problems
- Choose route objects
- Create a prefix filter



## IRR (rfd)

- Some IRR are not trusted
- No maxLength at all
  - Exact/covered filter type
- No any formal policy
  - Are we ready to define one?
  - What to do with delegated prefixes?

and the state of the late of the administration and the second transfer of the second transfer of the late of the



### Hello from the past

aanataa aa kaasibadan taadaan daasibadha maddibaasis dadbaasa dibaasa aa nataa aa baasibada ta

How to Sign It?

#### It's simple:

- 1. <a href="https://my.ripe.net/#/rpki">https://my.ripe.net/#/rpki</a>
- 2. Sign only aggregates;
- Set max\_length to 32 in IPv4 (128 in IPv6);

\* From last ROA signing party



#### O RLY?

How to Sign It?

#### It's simple:

- https://my.ripe.net/#/rpki
- Sign only aggregates
- 3. Set max\_length to 32 in IPv4 (128 in IPv6);

aure Laure Lauri India de Lauri and anni and an India mai alaid Ingara I<u>l Ingara ann agus an aitead i an i</u> baile a

\* From last ROA signing party



### ROA (rfd)

- Which maxLength to use?
  - Valid cases vs hijacks
  - Don't use at all?
  - Don't neet to be max for blackhole?

eanstacadoratholiciadamicadallamintillianadaillibraadhiaanatalaanataa.

- Less specific is «Not found»
  - Great with uRPF



# **AS\_PATH** manipulation

aanataa aa dhadaa aa daan daadhadhadhadhadhadhaa aa daddhaa addhaa aa mataa aa baadhadhabata

- Based on loop detection
- Route Leak prevention
- Link load balancing
- Link overloading
- Pilosov-Kapela (real example)



### **AS\_PATH** verification

	BGPSec	ASPA
Main goal	Stop crafted routes	Stop global propagation
AS_PATH + NLRI	Yes	Only AS_PATH
AS_PATH validation	Is real?	Is valid?
Cryptographic load	For each route in each direction	Only during filter creation
Partial deployment	For «connected islands»	For independent deployment
Prevent route leaks	With draft extension	As a side effect
Status	RFC; not spreaded	Draft; waiting



#### What it's all about

aanataaaattaa dhadan taalaandaadhadhadhadhadhadhtaaataladhtaaaalhaaaannataaaattaadhadhta

- BGP BCP
- Analytics/Toolset
- Modern trends/security
- **ROA** party



### **ROA** regional status

Around 21% of prefixes are signed

a mata a a la calibration da la mata ada al la fina del litera de la litera a al litera a mata a administrati

- Really good coverage
- More than 100 ISP are fully signed!
- Good big boys: AS198605, AS43451



#### How to check

#### Via any BGP prefix monitor

- https://bgp.he.net/AS197068#\_prefixes
- https://radar.grator.net/as197068/prefixes
- Via API
  - https://stat.ripe.net/docs/data\_api#rpki-validation
  - https://api.radar.qrator.net/#/Connectivity/prefixes

a mata a a dimensi a da mata a di a di la dina di di bana a la diba a a diba a a mata a a diba di di di di di

- Via dashbord
  - https://my.ripe.net/#/rpki



#### What to do next?

- Own repository great
  - But we are lazy
- Choose wisely your prefixes and maxLength
- Go to RPKI dashboard https://my.ripe.net/#/rpki

- Follow intuition
  - Or just read/watch



### **Questions?**

Contacts: eb@qrator.net



# PS: My questions (rfd)

- Do we need to aggregate routes?
- Do we need to standardize AS\_PATH max length

aanataa.....taaadhodootaalaandoaadaallannotallitanaaalaidhoa....dthaaa...nataa....taaadhodoot

- Does someone use uRPF? Not the loose one?
- What to sign in ROA?
- Is «Not Found» for less specific in ROA good?
- Do we need to create a standard policy for filtration based on IRR?