Routing Security @ Claranet

David Freedman
Claranet Technology Group (CTG)

claranet Background

- Established 1996 as an ISP in the United Kingdom

- 2000+ person company, UK, FR, DE, NL, ES, PT, IT, BR

- Managed Services Provider (MSP) which are essentially ISP services that we manage for customers.

- Own our own Network Infrastructure in Europe

About me

- Network Engineer for 20+ years

- Infrastructure Manager at Claranet Technology Group

- Arbiter for the RIPE NCC

- Regular RIPE meeting + WG participant

- IETF contributor

Outbound Security

- We adhere to MANRS (http://www.manrs.org/), meaning that we:

    - Filter our outbound BGP announcements

    - Practise anti-spoofing in the data plane, doing source validation for outbound traffic

    - Maintain globally accessible, up-to-date contact information

    - Publish our routing data globally, allowing others to validate what we do

Publishing and maintaining contact data

https://as8426.peeringdb.com

If you take anything away from this talk, it's to make sure that if, you have an autonomous system, and you peer it with others, on the Internet, that you *should* register it on peeringdb.com

Publishing our routing data

- All valid announcements published in RIPEDB IRR

  - Policies published in AS8426 AUT-NUM

  - Route origins represented by AS-CLARANET macro.

- ROAs published for all prefixes we maintain

  - We use RIPE NCC managed RPKI (point and click)

AUT-NUM specifies your policy
We generate ours automatically from our records of customers and peers
(others use it to generate config, we use it to publish)
Doing this is not as important / relevant today.

```
$ whois -h whois.ripe.net -- -T aut-num -Br AS8426

aut-num:        AS8426
as-name:        CLARANET-AS
descr:          ClaraNET LTD
descr:          Global Autonomous System
remarks:
remarks:        *********************************************
remarks:        * The list below is generated automatically *
remarks:        *********************************************
remarks:
remarks:        AS5615 (PEER) - TISNL-BACKBONE Green ISP B.V.
mp-import:      afi ipv4.unicast from AS5615 80.249.208.115 at 80.249.208.82 accept AS5615
mp-export:      afi ipv4.unicast to AS5615 80.249.208.115 at 80.249.208.82 announce AS-CLARANET
mp-import:      afi ipv4.unicast from AS5615 80.249.208.78 at 80.249.208.82 accept AS5615
mp-export:      afi ipv4.unicast to AS5615 80.249.208.78 at 80.249.208.82 announce AS-CLARANET
mp-import:      afi ipv4.unicast from AS5615 80.249.208.78 at 80.249.209.228 accept AS5615
mp-export:      afi ipv4.unicast to AS5615 80.249.208.78 at 80.249.209.228 announce AS-CLARANET
mp-import:      afi ipv4.unicast from AS5615 80.249.208.115 at 80.249.209.228 accept AS5615
mp-export:      afi ipv4.unicast to AS5615 80.249.208.115 at 80.249.209.228 announce AS-CLARANET
mp-import:      afi ipv4.unicast from AS5615 195.69.144.78 at 195.69.144.82 accept AS5615
mp-export:      afi ipv4.unicast to AS5615 195.69.144.78 at 195.69.144.82 announce AS-CLARANET
mp-import:      afi ipv4.unicast from AS5615 195.69.144.115 at 195.69.144.82 accept AS5615
mp-export:      afi ipv4.unicast to AS5615 195.69.144.115 at 195.69.144.82 announce AS-CLARANET
remarks:        AS5631 (CUSTOMER) - VITAL-GROUP VITAL-GROUP UK Network
mp-import:      afi ipv4.unicast from AS5631 accept AS5631
mp-export:      afi ipv4.unicast to AS5631 announce ANY
remarks:        AS6067 (PEER) - ONYX Onyx Internet
mp-import:      afi ipv4.unicast from AS6067 195.66.224.35 at 195.66.224.66 accept AS-ONYX
mp-export:      afi ipv4.unicast to AS6067 195.66.224.35 at 195.66.224.66 announce AS-CLARANET
mp-import:      afi ipv4.unicast from AS6067 195.66.236.35 at 195.66.236.66 accept AS-ONYX
mp-export:      afi ipv4.unicast to AS6067 195.66.236.35 at 195.66.236.66 announce AS-CLARANET

<snip>
~
```
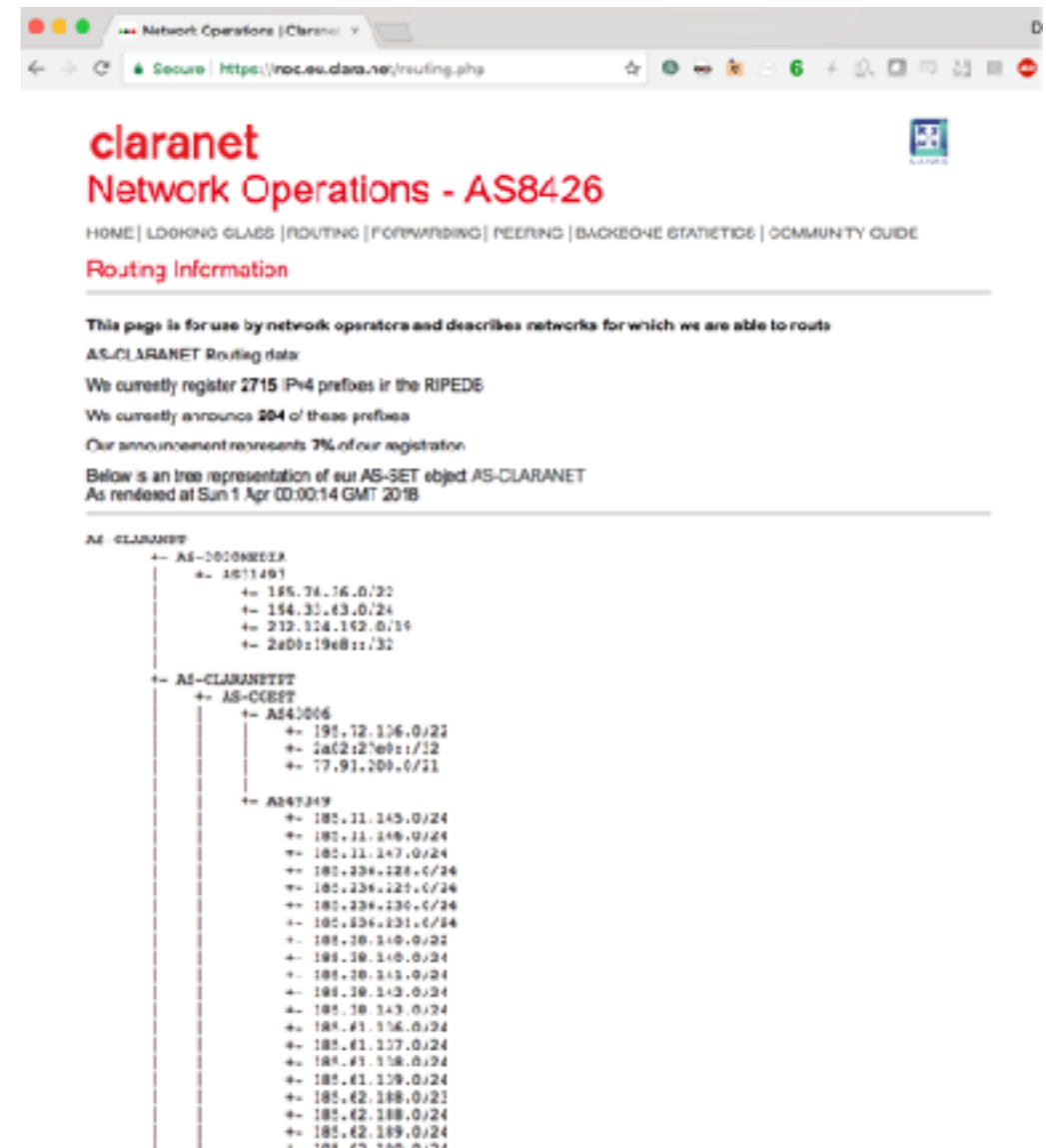
AS-SET (macro) more important
This we generate again automatically, from our customer database
You should keep this up to date at the top level

Keeping the levels below up to date is another challenge…

Publish ROAs for everything you originate
We are using RIPE NCC hosted RPKI
So ROAs exist for everything in the LIR

Automation of outbound prefix filters
Takes data from evaluation of our AS-MACRO

Plenty of open source tools to do this for you
(Example : bgpq3, https://github.com/snar/bgpq3)

```
$ bgpq3 -3 -4 -A -l AS-CLARANET -P -S RIPE AS-CLARANET
no ip prefix-list AS-CLARANET
ip prefix-list AS-CLARANET permit 5.159.40.0/21
ip prefix-list AS-CLARANET permit 5.206.224.0/21
ip prefix-list AS-CLARANET permit 5.206.224.0/21 ge 24 le 24
ip prefix-list AS-CLARANET permit 12.111.223.0/24
ip prefix-list AS-CLARANET permit 12.175.119.0/24
ip prefix-list AS-CLARANET permit 23.207.64.0/19 ge 20 le 20
ip prefix-list AS-CLARANET permit 31.3.136.0/21
ip prefix-list AS-CLARANET permit 31.3.137.0/24
ip prefix-list AS-CLARANET permit 31.3.139.0/24
ip prefix-list AS-CLARANET permit 31.172.240.0/20
ip prefix-list AS-CLARANET permit 37.44.8.0/21
ip prefix-list AS-CLARANET permit 37.220.96.0/21
ip prefix-list AS-CLARANET permit 41.222.104.0/21 ge 22 le 22
ip prefix-list AS-CLARANET permit 41.222.104.0/23 le 24
ip prefix-list AS-CLARANET permit 41.222.108.0/23 ge 24 le 24
ip prefix-list AS-CLARANET permit 41.222.110.0/23 le 24
ip prefix-list AS-CLARANET permit 43.228.128.0/22 ge 24 le 24
ip prefix-list AS-CLARANET permit 43.242.240.0/22 ge 24 le 24
ip prefix-list AS-CLARANET permit 45.60.0.0/16 ge 17 le 17
ip prefix-list AS-CLARANET permit 45.60.0.0/16 ge 24 le 24
ip prefix-list AS-CLARANET permit 45.64.64.0/22 ge 24 le 24
ip prefix-list AS-CLARANET permit 45.223.0.0/16
ip prefix-list AS-CLARANET permit 46.18.128.0/21
ip prefix-list AS-CLARANET permit 46.231.112.0/21
ip prefix-list AS-CLARANET permit 46.245.208.0/21
ip prefix-list AS-CLARANET permit 62.24.0.0/19
ip prefix-list AS-CLARANET permit 62.80.0.0/18
ip prefix-list AS-CLARANET permit 62.128.107.0/24
ip prefix-list AS-CLARANET permit 62.173.64.0/18
ip prefix-list AS-CLARANET permit 62.176.128.0/19
ip prefix-list AS-CLARANET permit 62.197.0.0/19
ip prefix-list AS-CLARANET permit 62.231.128.0/19
ip prefix-list AS-CLARANET permit 62.240.224.0/19
ip prefix-list AS-CLARANET permit 64.199.226.0/24
ip prefix-list AS-CLARANET permit 77.91.200.0/21
ip prefix-list AS-CLARANET permit 78.24.208.0/21
ip prefix-list AS-CLARANET permit 78.24.208.0/22 le 24
ip prefix-list AS-CLARANET permit 78.24.212.0/22
ip prefix-list AS-CLARANET permit 78.24.212.0/23 le 24
ip prefix-list AS-CLARANET permit 78.40.32.0/21

<snip>
```

Customer route filtering

- Customers speaking BGP should be filtered inbound

- We capture AUT-NUM or AS-SET at provision time

- Automatically build filters in the same way

```
ip prefix-list AS-CUSTOMER permit 212.22.254.0/23 ge 24 le 24
ip prefix-list AS-CUSTOMER permit 212.28.0.0/19 ge 20 le 20
ip prefix-list AS-CUSTOMER permit 212.43.192.0/18
ip prefix-list AS-CUSTOMER permit 212.49.192.0/18
ip prefix-list AS-CUSTOMER permit 212.54.140.0/24
ip prefix-list AS-CUSTOMER permit 212.57.64.0/19
ip prefix-list AS-CUSTOMER permit 212.61.0.0/16
ip prefix-list AS-CUSTOMER permit 212.66.0.0/19
ip prefix-list AS-CUSTOMER permit 212.82.224.0/19
ip prefix-list AS-CUSTOMER permit 212.124.192.0/19
ip prefix-list AS-CUSTOMER permit 212.125.64.0/19
ip prefix-list AS-CUSTOMER permit 212.126.128.0/19
ip prefix-list AS-CUSTOMER permit 212.169.0.0/18
ip prefix-list AS-CUSTOMER permit 212.188.128.0/17
ip prefix-list AS-CUSTOMER permit 213.2.0.0/16
```

Anti Spoofing (Customer packet filtering)

- BCP38 <u>strict</u> uRPF or ACL on all single homed customers.

```
!
interface GigabitEthernet0/0/0/0.101
 description Non-core: Some customer [London - 1000 Mbps - Primary]:Telco:1234567890:ZZZ001
 bandwidth 1024000
 ipv4 address 192.0.2.1 255.255.255.0
 ipv4 verify unicast source reachable-via rx
 ipv4 unreachables disable
 encapsulation dot1q 101
!
```

- Multi-homed customers are subject to ACL only.

- ACLs automatically generated by the same automation

- This can be done at customer or internetwork interface

Anti Spoofing

CAIDA Spoofer project
https://spoofer.caida.org

Go check your ASN now!

Peer inbound filtering

- Route filtering via IXP filtering route-server a quick win

  - But you need to find one (example, AMS-IX RS)

- If you have bilateral sessions, this is harder

  - You can generate per peer filters, presuming AS-SET is published

    - Argument against peering with somebody who doesn't do this

  - AS-SET also needs to be valid, and preferably clean and not excessive size

    - Scale issue on the peering edge with all of these filters.

- Also, if you rely on upstream providers, specific route filtering of these is likely impossible.

- General solution is usually to permit everything by default and deny BOGON (private and reserved) or known bad networks: - https://www.team-cymru.com/bogon-reference.html

  - You can do this for routes, and also for packets, even on shared media.

  - Don't forget to also deny your own prefixes / packets (unless you really need to accept them)

Policy Violations

- Policy violations occur usually when:

    - Multiple parties have genuine announcements

    - Traffic flows against policy

- Usually announcements cause forwarding conflict

- These can only be detected automatically by good telemetry (Netflow, sFlow) and analysis, this is what happens in our case.

- Can be resolved technically, politically or commercially

    - Partition of function at the edge helps here.
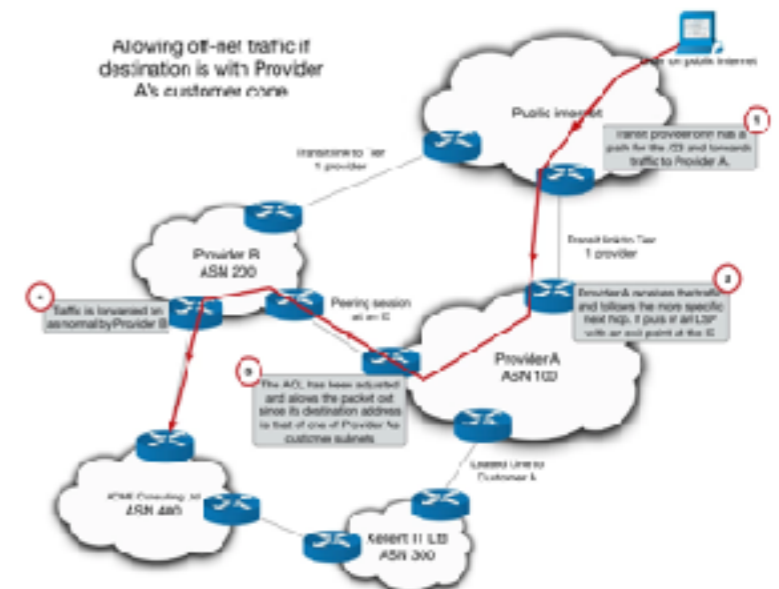
Questions?

david.freedman@uk.clara.net