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

PeeringDB

Secure | https://www.peeringdb.com/asn/8426

PeeringDB

Search here for a network, IX, or facility

Advanced Search

claranet

Claranet

Edit

Organization	Claranet
Also Known As	
Company Website	http://www.clara.net
Primary ASN	8426
IRR Record	AS-CLARANET
Route Server URL	
Looking Glass URL	http://noc.eu.clara.net/lg.php
Network Type	Cable/DSL/ISP
IPv4 Prefixes	800
IPv6 Prefixes	40
Traffic Levels	20-50 Gbps
Traffic Ratios	Balanced
Geographic Scope	Regional
Protocols Supported	Unicast IPv4 Multicast IPv6
Last Updated	2016-03-14T21:37:50Z
Notes	

PeeringDB Configuration

Allow IXP Update	

Peering Policy Information

Peering Policy	http://noc.eu.clara.net/peering.php
General Policy	Selective
Multiple Locations	Preferred
Ratio Requirement	No
Contract Requirem...	Not Required

Contact Information

Role	Name	Phone / E-Mail
NOC	peerops	peerops@clara.net
Policy	peering	peering@clara.net

Public Peering Exchange Points

Filter

Exchange / ASN	IPv4 / IPv6	Speed / RS P...
AMS-IX 8426	80.249.208.82 2001:7f8:1::a500:8426:1	10G
AMS-IX 8426	80.249.209.228 2001:7f8:1::a500:8426:2	10G
CATNIX 8426	193.242.98.131 2001:7f8:2a:0:2:1:0:8426	1G
DE-CIX Frankfurt Main 8426	80.81.192.86 2001:7f8::20ea:0:1	10G
DE-CIX Frankfurt Main 8426	80.81.193.86 2001:7f8::20ea:0:2	10G
DE-CIX Madrid Main 8426	185.1.68.28 2001:7f8:a0::20ea:0:1	1G
Equinix Paris Equinix IX - PA Metro 8426	195.42.144.30 2001:7f8:43::8426:1	10G
France-IX Paris 8426	37.49.236.60 2001:7f8:54::60	10G
France-IX Paris 8426	37.49.236.61 2001:7f8:54::61	10G
GigaPIX LAN1 8426	193.136.250.50 2001:7f8:a:1::5	10G
GigaPIX LAN2 8426	193.136.251.5 2001:7f8:a:2::5	10G
IXManchester 8426	195.66.244.17 2001:7f8:4:2::20ea:1	1G
LINX LON1 Main 8426	195.66.224.66 2001:7f8:4::20ea:1	20G
LINX LON2 8426	195.66.236.66 2001:7f8:4:1::20ea:1	10G

Private Peering Facilities

Filter

Facility / ASN	Country / City
Digital Realty Amsterdam (Science Park) 8426	Netherlands Amsterdam
Digital Realty London (Sovereign House) 8426	United Kingdom London
Digital Realty London (West Drayton) 8426	United Kingdom West Drayton, Middlesex

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

```
$ whois -h whois.ripe.net -- -T as-set -Br AS-CLARANET

as-set:         AS-CLARANET
descr:          ASes routed by Claranet
members:        AS-CLARANETPT
members:        AS8426
members:        AS-2020MEDIA
members:        AS-CONTINENT8
members:        AS-DIADEMYS
members:        AS-DOMICILIUM
members:        AS-LUMINET
members:        AS-MOREA
members:        AS-NOMINET
members:        AS-NORTENET
members:        AS-OXYMIUM
members:        AS-RUNISO
members:        AS-TYPHON
members:        AS-WEL-TRANSIT
members:        AS12583
members:        AS12628
members:        AS12680
members:        AS15489
members:        AS15622
members:        AS15722
members:        AS15734

<snip>
```

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

RPKI Dashboard

41 CERTIFIED RESOURCES | ALERTS ARE SENT TO 1 ADDRESS

43 BGP Announcements
43 Valid | 0 Invalid | 0 Unknown

47 ROAs
47 OK | 0 Causing problems

BGP Announcements | Route Origin Authorisations (ROAs) | History | Search...

Create ROAs for selected BGP Announcements | Valid | Invalid | Unknown

Origin AS	Prefix	Current Status
AS8426	130.193.80.0/20	VALID
AS8426	176.52.208.0/21	VALID
AS8426	185.39.232.0/23	VALID
AS8426	185.77.172.0/22	VALID
AS8426	185.77.200.0/22	VALID
AS8426	185.77.64.0/22	VALID
AS8426	185.77.72.0/22	VALID
AS8426	185.77.72.0/23	VALID
AS8426	185.77.80.0/22	VALID
AS8426	194.112.32.0/19	VALID

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

Commits > 2b489e9e

Commit 2b489e9e authored a week ago

Browse files | Options

commited by [redacted].py on [redacted].clara.net

parent 2d447fa5 master

No related merge requests found

Showing 4 changed files with 8 additions and 8 deletions

Hide whitespace changes | Inline | Side-by-side

bogons-prefixes/bogons4-pfx-out-ios.txt

View file @ 2b489e9e

```
1   1
2   2   no ip prefix-list AS-CLARANET
3 - 3 + ! Created by [redacted]py on [redacted].clara.net at 15-03-2018 15:14:44 UTC
3 + 1:11:02 UTC
4   4   ip prefix-list AS-CLARANET permit 5.159.48.0/21
5   5   ip prefix-list AS-CLARANET permit 5.206.224.0/21
6   6   ip prefix-list AS-CLARANET permit 5.206.224.0/21 ge 24 le 24
...  ...  @@ -407,7 +407,7 @@ ip prefix-list AS-CLARANET permit 195.167.128.0/28 le 21
407 407 ip prefix-list AS-CLARANET permit 195.167.176.0/20 le 21
408 408 ip prefix-list AS-CLARANET permit 195.170.96.0/19
409 409 ip prefix-list AS-CLARANET permit 195.170.169.0/24
410 - 410 + ip prefix-list AS-CLARANET permit 195.191.216.0/24
410 + 410 + ip prefix-list AS-CLARANET permit 195.191.216.0/23 ge 24 le 24
411 411 ip prefix-list AS-CLARANET permit 195.208.252.0/23
412 412 ip prefix-list AS-CLARANET permit 195.211.164.0/23
413 413 ip prefix-list AS-CLARANET permit 195.216.0.0/19
...  ...
```

bogons-prefixes/bogons46-pfx-out-ios_xr.txt

View file @ 2b489e9e

```
1   1   prefix-set AS-CLARANET
2 - 2 + # Created by [redacted]py on [redacted].clara.net at 15-03-2018 15:14:44 UTC
2 + 1:11:02 UTC
3   3   5.159.48.0/21,
4   4   5.206.224.0/21,
5   5   5.206.224.0/21 ge 24 le 24,
...  ...  @@ -406,7 +406,7 @@ prefix-set AS-CLARANET
406 406 195.167.176.0/20 le 21,
407 407 195.170.96.0/19,
408 408 195.170.169.0/24,
409 - 409 + 195.191.216.0/24,
409 + 409 + 195.191.216.0/23 ge 24 le 24,
410 410 195.208.252.0/23,
411 411 195.211.164.0/23,
412 412 195.216.0.0/19,
...  ...
```

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 strict 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!

Recent tests

Secure | https://spoofer.caida.org/recent_tests.php?as_incl...

caida — Center for Applied Internet Data Analysis

Search CAIDA | Search | DONATE | CONTACT US

HOME | RESEARCH | DATA | TOOLS | INTERACTIVE | PUBLICATIONS | WORKSHOPS | PROJECTS | FUNDING

Recent tests

Spoofer Project Page Download FAQ
Data: Stats Summary Recent Tests Remediation Results by AS Results by Country Results by Provider Results by Traceroute

Result filters:

AS numbers or (partial) names: 8426 Country codes: Exclude NAT Only show non-remediated spoofing Change filters

Spoof status key	
received	Spoofed packet was received.
rewritten	Spoofed packet was received, but the source address was changed en route.
blocked	Spoofed packet was not received, but unspoofed packet was.
blocked	Spoofed packet was not received, but unspoofed packet was. Pattern of tests from this IP block indicates a switch from allowing spoofing to blocking it.
unknown	Neither spoofed nor unspoofed packet was received.

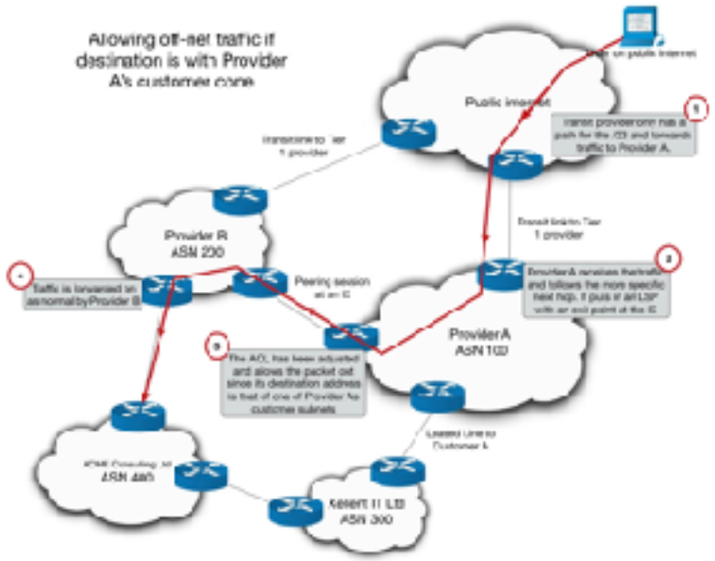
Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Spoof Private	Spoof Routable	Adjacency Spoofing	Results
438077	2018-04-02 07:33:57	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	blocked	blocked	none	Report
434314	2018-03-26 16:08:46	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	blocked	blocked	none	Report
434310	2018-03-26 16:04:23	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	blocked	blocked	none	Report
434005	2018-03-26 06:26:12	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	blocked	blocked	none	Report
431858	2018-03-22 07:25:40	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	blocked	blocked	none	Report
431363	2018-03-21 14:10:21	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	unknown	unknown	none	Report
431286	2018-03-21 11:50:33	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	blocked	blocked	none	Report
431256	2018-03-21 10:41:00	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	unknown	unknown	none	Report
429956	2018-03-19 11:38:07	212.61.12.x/24	8426 (CLARANET-AS)	nld (Netherlands)	yes	blocked	blocked	none	Report
353410	2017-11-14 11:18:24	212.188.254.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	blocked	blocked	none	Report
350177	2017-11-08 22:12:17	212.188.254.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes				Report
		2001:a88:d5xx::/40	8426 (CLARANET-AS)		no	blocked	blocked	/32	
345756	2017-11-01 20:13:36	212.188.254.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	blocked	blocked	none	Report
		2001:a88:d5xx::/40	8426 (CLARANET-AS)		no	blocked	blocked	/32	
298077	2017-08-16 18:08:45	80.168.113.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	rewritten	rewritten	none	Report
293830	2017-08-10 02:46:32	195.157.65.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	unknown	unknown	none	Report
292944	2017-08-09 02:57:58	195.157.65.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	unknown	unknown	none	Report
258824	2017-06-27 17:02:43	89.206.239.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	unknown	unknown	none	Report
248057	2017-06-14 22:43:09	213.165.152.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	unknown	unknown	none	Report
245200	2017-06-11 19:46:47	213.165.152.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	unknown	unknown	none	Report
234849	2017-05-30 16:44:34	213.165.152.x/24	8426 (CLARANET-AS)	gbr (United Kingdom)	yes	unknown	unknown	none	Report

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.



https://netquirks.co.uk/2018/01/23/the-friend-of-my-friend-is-my-enemy/

Questions?

david.freedman@uk.clara.net