BGP Blackholing Project

Łukasz Bromirski
lukasz.bromirski@gmail.com
lbromirski@cisco.com

http://portal.null0.pl

BGP blackholing project

From 10000 meters

- Started in 2004, during last two years completely rebuilt & restarted during last PLNOG
- Using RTBH and/or uRPF and/or QPPB with a “twist”
- (currently) four redundant clusters of
  - Cisco IOS/IOS XE based routers (Cisco 7201/CSR 1000v)
  - FreeBSD "feed" VMs
  - Geographically dispersed in Poland, covering direct access to biggest core networks in the country (TelecityGroup, Thinx & SPs)
- Each of the Cisco boxes serves as a route reflector for customers – project members
- FreeBSD boxes digest and serve the prefixes with properly assigned communities

BGP blackholing project

From 3500 meters…

- Route servers announce prefixes for IPv4 and IPv6 AFs
- The “twist” – it can also pass (with verification) prefixes announced by member routes!
- Prefixes can be of a different kind, distinguished using known communities:

  bogons – not assigned, reserved, special
  64999:666

  evil – known C&C networks, spam sources, scanning, etc.
  64999:25, **64999:80**, **64999:135** and others

  members prefixes – to enable self-defense
  $MY_ASN:667, `my_own_ipv4/ipv6_prefix`

  other members prefixes – to enable remote self-defense
  $ATTACKING_ASN:667, `remote_ipv4/ipv6_prefix`

- BGP gives us a powerful policy tool, even for members with limited trust to other/smaller entities

BGP blackholing project

Other details

- We're experimenting with the QoS policy propagation with BGP

  ...and with BGP FlowSpec thanks to IOS-XR implementation (experimental RS you can connect to and pass/receive FlowSpec data)

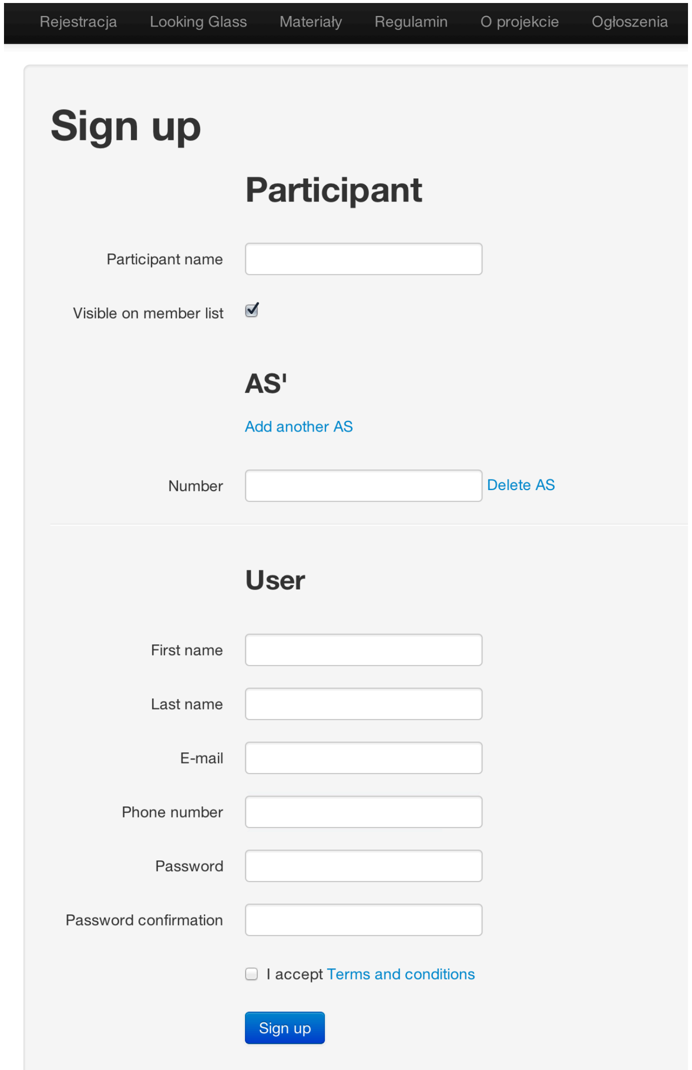
- …and with SIDR

  unfortunately, ROAs cover usual announced prefix length, not the ones we’re using (/28-/32 for IPv4 & /96-/128 for IPv6)

  ...alternative cache?

BGP blackholing project

Register at https://portal.null0.pl/register/



Sign up

Participant

Participant name

Visible on member list ☑

AS'

Add another AS

Number — Delete AS

User

First name

Last name

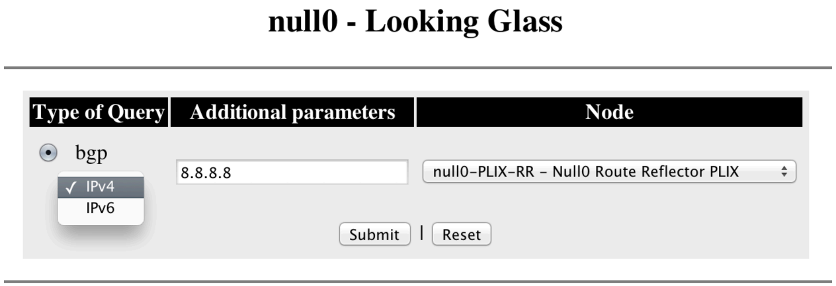
E-mail

Phone number

Password

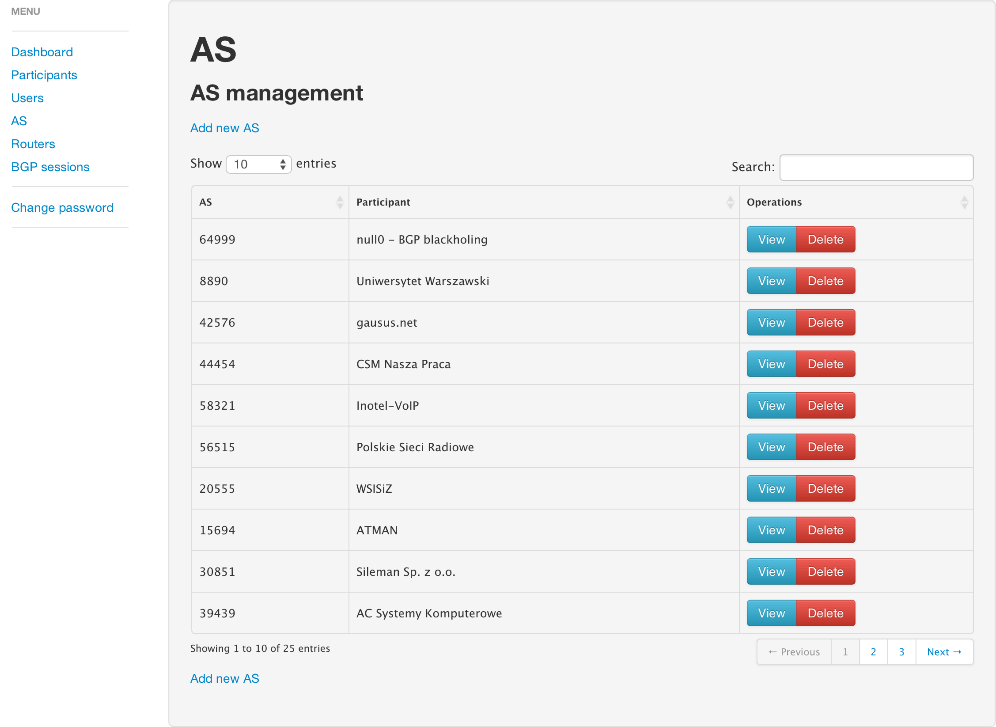
Password confirmation

□ I accept Terms and conditions



null0 - Looking Glass

Type of Query	Additional parameters	Node
● bgp ✓ IPv4 IPv6	8.8.8.8	null0-PLIX-RR – Null0 Route Reflector PLIX



AS

AS management

Add new AS

Show 10 entries Search:

AS	Participant	Operations
64999	null0 – BGP blackholing	View Delete
8890	Uniwersytet Warszawski	View Delete
42576	gausus.net	View Delete
44454	CSM Nasza Praca	View Delete
58321	Inotel-VoIP	View Delete
56515	Polskie Sieci Radiowe	View Delete
20555	WSISiZ	View Delete
15694	ATMAN	View Delete
30851	Sileman Sp. z o.o.	View Delete
39439	AC Systemy Komputerowe	View Delete

Showing 1 to 10 of 25 entries

Add new AS

It’s a wider idea, not one project

- We’re mainly about educating how to securely connect your network to the internet.. and internet to your network ☺
  - IPv4 and IPv6 typical edge scenarios
  - basic hardening, more advanced tweaks
  - establishing RR, going from iBGP full-mesh to RR for IPv4/IPv6
  - IPv4 and IPv6 SP scenarios, involving 6PE, 6VPE and other VRF/MPLS scenarios (many different deployment types)
  - uRPF and the value of it (spoofing!)
  - NetFlow v5, v9
  - value of trust between parties
  - SIDR – RPKI (yeah!)
- If you want to donate rack space/IP connectivity in secure & safe location – please contact me!

BGP Blackholing Project

Thank You!

Łukasz Bromirski
lukasz.bromirski@gmail.com
lbromirski@cisco.com

http://portal.null0.pl