The FENIX project

The walled Garden of Eden?

Ondřej Caletka

9th September 2016

Disclaimer: The speaker is not directly assiciated with the NIX.CZ nor the FENIX project.

About CESNET

- association of legal entities, est. 1996
  - public and state universities
  - Academy of Sciences
- non-profit organisation
  - development and operation of **NREN** (CESNET2)
  - advanced network technologies and applications R&D
  - international cooperation – GNx, GN3+, GLIF, EGI, GÉANT shareholder, EGI member, Internet2 affiliate member,...
- founding member – **CZ.NIC, NIX.CZ, FENIX**

About NIX.CZ

- association of legal entities, est. 1996
- non-profit organisation
  - community driven
  - members and customers
- operator of public neutral **IXPs**
  - NIX.CZ – Prague
    - 5 PoPs
    - 140 networks
    - 2.4 Tb capacity
  - NIX.SK – Bratislava – since 2015
    - 2 PoPs
    - 36 networks
    - 208 Gb capacity

1996–2016 CESNET

(D)DoS attacks in 2013

- between March 4th and 7th
- two waves each day: 9am – 11am, 2pm – 4pm
- targeting major Czech web sites

  Monday news portals
  Tuesday search engine `www.seznam.cz`
  Wednesday bank websites
  Thursday 2 out of 3 mobile carriers
- attractive for mass media

1996–2016 CESNET

DoS technical aspects

- sourced from transit operator RETN **via NIX.CZ**
- methods: SYN-Flood, DNS-reflection
- no harm for ISP
  - low volume (< 1 Gbps)
  - moderate packet rate (1 – 1.5 million pps)
- harmful for end sites
  - aggregation in one point
  - no SYN-cookies enabled
  - firewalls and loadbalancers up in smoke
- used solutions
  - controlled shutdown and waiting for the end of attack
  - moving service to another IP address (short DNS TTL)
  - filtration, scrubbers
  - **restricting traffic just for Czech ISPs**

Lessons learned

- NIX.CZ peering ≠ national peering
- NIX.CZ can transit spoofed traffic
- some victims misinterpreted attack transited via NIX.CZ as attack sourced from Czechia

Idea of secure peering VLAN inside NIX.CZ

- as a last resort in case of some massive attack
- for those that **trust each other**
- so **Czech users can access Czech services**

So the FENIX was born...

- club of **trustworthy operators** inside NIX.CZ which
  - avoid IP spoofing
  - take care of security incidents
- self-governed, semi-independent of NIX.CZ
  - NIX.CZ act as an arbiter
  - new members need recommendations
  - any member can veto
- self-regulation instead of goverment regulation
- high entry threshold

Connected to trusted network

1996–2016 CESNET

FENIX foundation

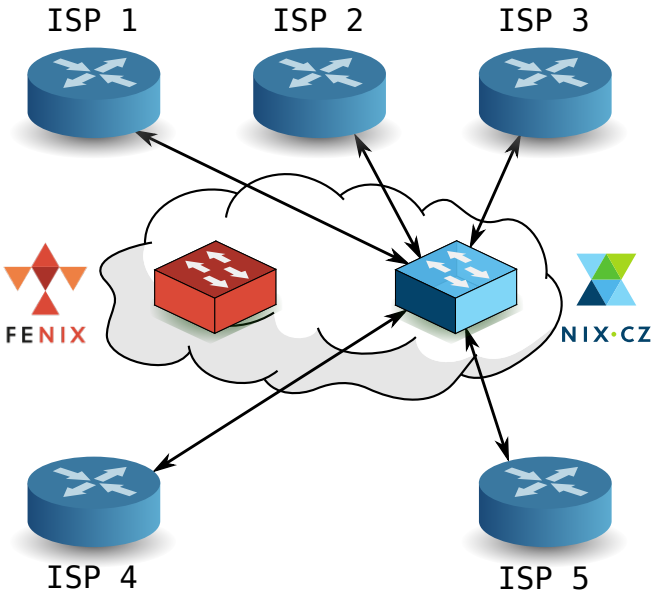
- founded by 6 operators in January 2014
  - **Active 24** (hosting)
  - **CESNET** (NREN)
  - **CZ.NIC** (TLD operator)
  - **Dial Telecom** (ISP)
  - **O2 CZ** (ISP, incumbent)
  - **Seznam.cz** (Czech Google)
- 13 members today
  - 9 % of members
  - 34 % of capacity
- similar ideas abroad
  - Trusted Networks Initiative
  - goverment network in Austria
  - ...

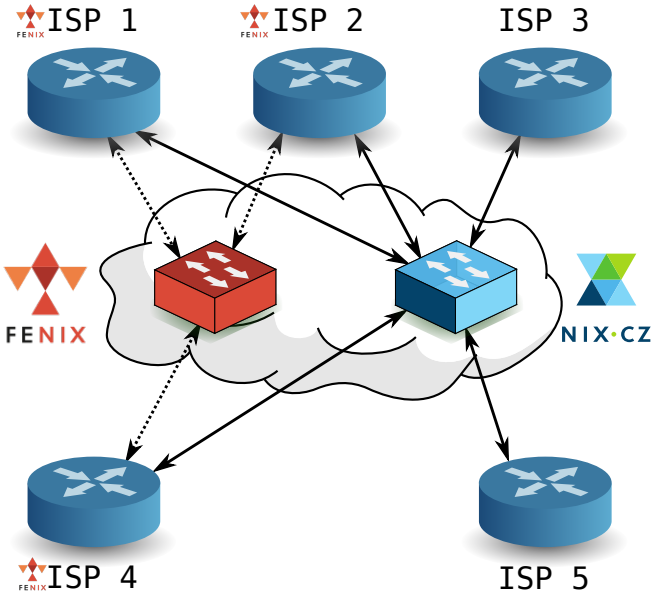
FENIX organisational criteria

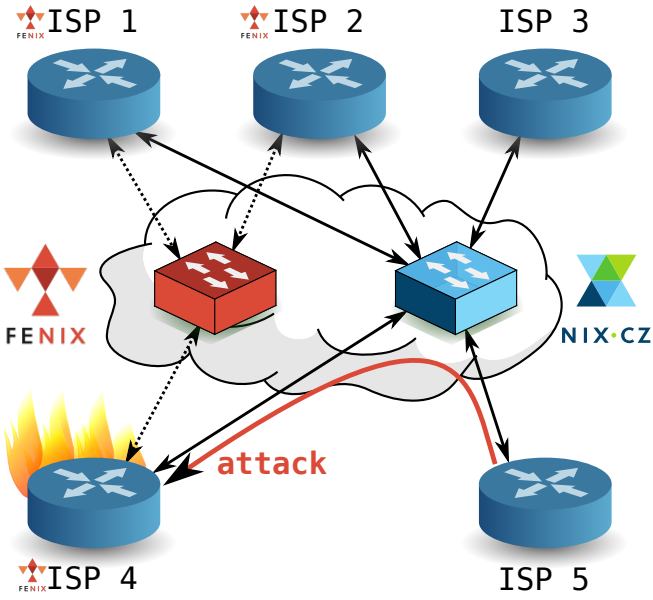
- Terms and Conditions allowing to disconnect customer originating malicious traffic
- 24×7 NOC, no Interactive Voice Response phone line
- Trusted Introducer listed CSIRT team
- NIX.CZ member for more than 6 months
- active participation
- recommendation from 2 FENIX members, no veto

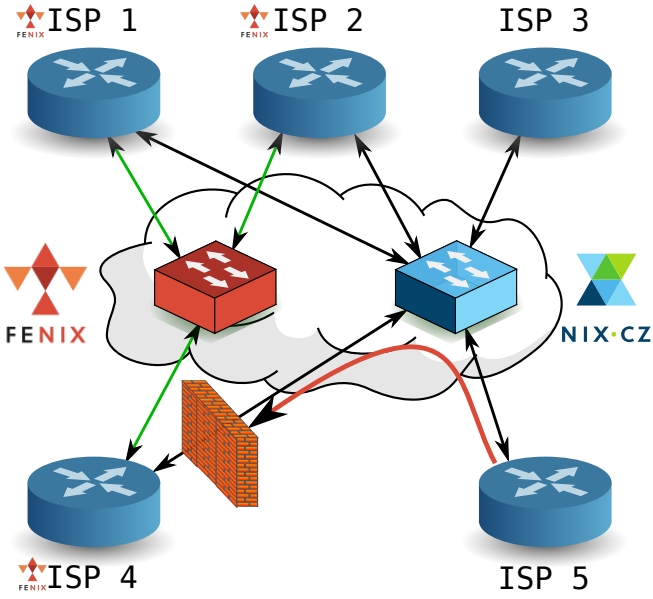
Secure peering VLAN

- former work title for the FENIX
- separate peering VLAN of last resort
- accessible by FENIX members only
- prepared for island-mode of operation
- each member decides on their own when to use it
- no data during *peace time*
  - BGP sessions up and running
  - data flow starts automatically when the regular peering VLAN is disconnected


ISP 1
ISP 2
ISP 3
FENIX
NIX·CZ
ISP 4
ISP 5


ISP 1
ISP 2
ISP 3
FENIX
NIX·CZ
ISP 4
ISP 5


ISP 1
ISP 2
ISP 3
FENIX
NIX·CZ
attack
ISP 4
ISP 5


ISP 1
ISP 2
ISP 3
FENIX
NIX·CZ
ISP 4
ISP 5

CESNET mission in FENIX

- we believe in FENIX principles
  - which should be **the default**
- we are pushing our clients to adopt similar rules
  - IP spoofing protection – do not rely on upstream to do the filtering
  - amplification attack protection
  - incident handling
- we do our best **not to source** or support any attack
- we offer tools for monitoring clients' networks – **Security Tools as a Service**

Why only few operators deploy BCP 38?

- the closer to the edge the simpler to deploy
- simple automatic `urpf-checks` don’t work well with multihoming
- network equipment vendors still don’t offer an easy to deploy solution for multihomed clients (Feasible Reverse Path Forwarding – BCP 84)
- loose RPF has no use against most spoofing attacks
- our solution: ACLs on customer ports
  - managed manually
  - prone to operator errors
  - probably too resource demanding for many ISPs

The walled Garden of Eden?

- the island mode is not *the Internet* as we know it
- a lot of stuff will break
  - well-known public DNS services like **8.8.8.8**
  - connectivity/captive portal detections in various OSes
  - **CRL and OCSP responders** – yes, somebody even validates them
- on the other hand, at least **something** should work
  - local DNS resolving (there are root and `.cz` TLD DNS servers inside the FENIX)
  - local services (Seznam.cz)
  - e-goverment (online POS records collection)
  - e-commerce (payment card acceptance)

Conclusion

- one does not simply deploy **separate and independent** internet network
  - but some sort of backup may be handy
  - especially for services affecting the off-line life
- FENIX-like communities very useful
  - consensual view
  - mutual help and assistence
  - sharing best practices
  - **personal trust**
- higher standards make networks **more reliable**
  - avoids possible goverment regulation
  - making the whole industry a better place

1996–2016 CESNET

Thank You!

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz

LinuxDays 2016
8th and 9th October
Prague

https://www.linuxdays.cz/2016/en/

1996–2016 CESNET