FENIX member experience

-

CESNET e-Infrastructure

Tom Košňar

CESNET a. l. e.

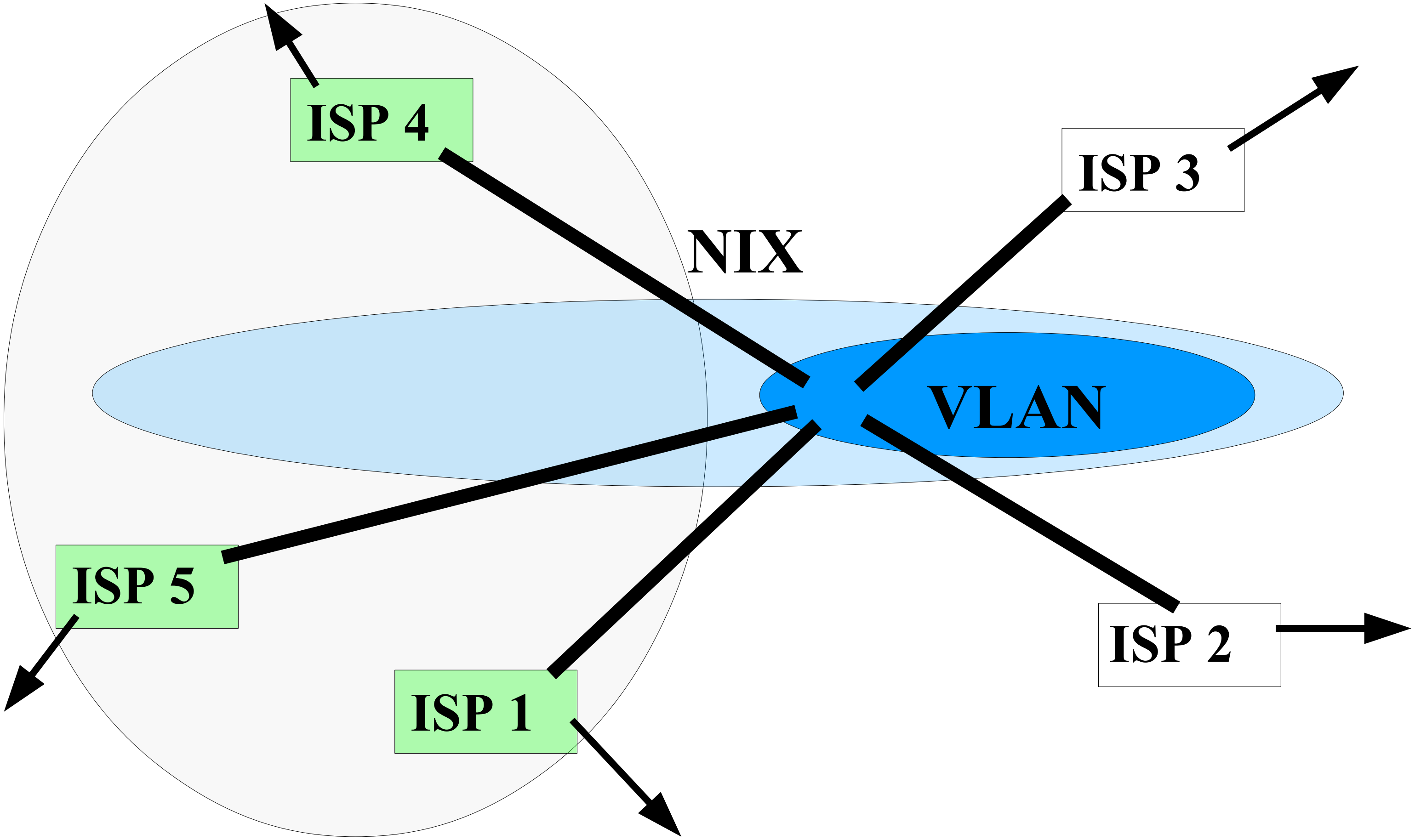
kosnar@cesnet.cz

CESNET a. l. e.

- **CESNET, Association of Legal Entities, established in 1996** (Czech public & state universities and Academy of Sciences)
- **Non-profit organisation**
  - *Development and operation of **NREN** (National Research and Education Network) in the Czech Republic – to support science & research & education (non-public operator)*
  - *Research and development of advanced network technologies and applications, broadening knowledge about the advanced networking topics*
  - *International cooperation – GNx, GN3+, GLIF, EGI, GÉANT shareholder, EGI member, Internet2 affiliate member,...*
  - *Founding member – **NIX.CZ**, **CZ.NIC**, FENIX*
- *More information on http://www.cesnet.cz (cz) or http://www.ces.net (en)*

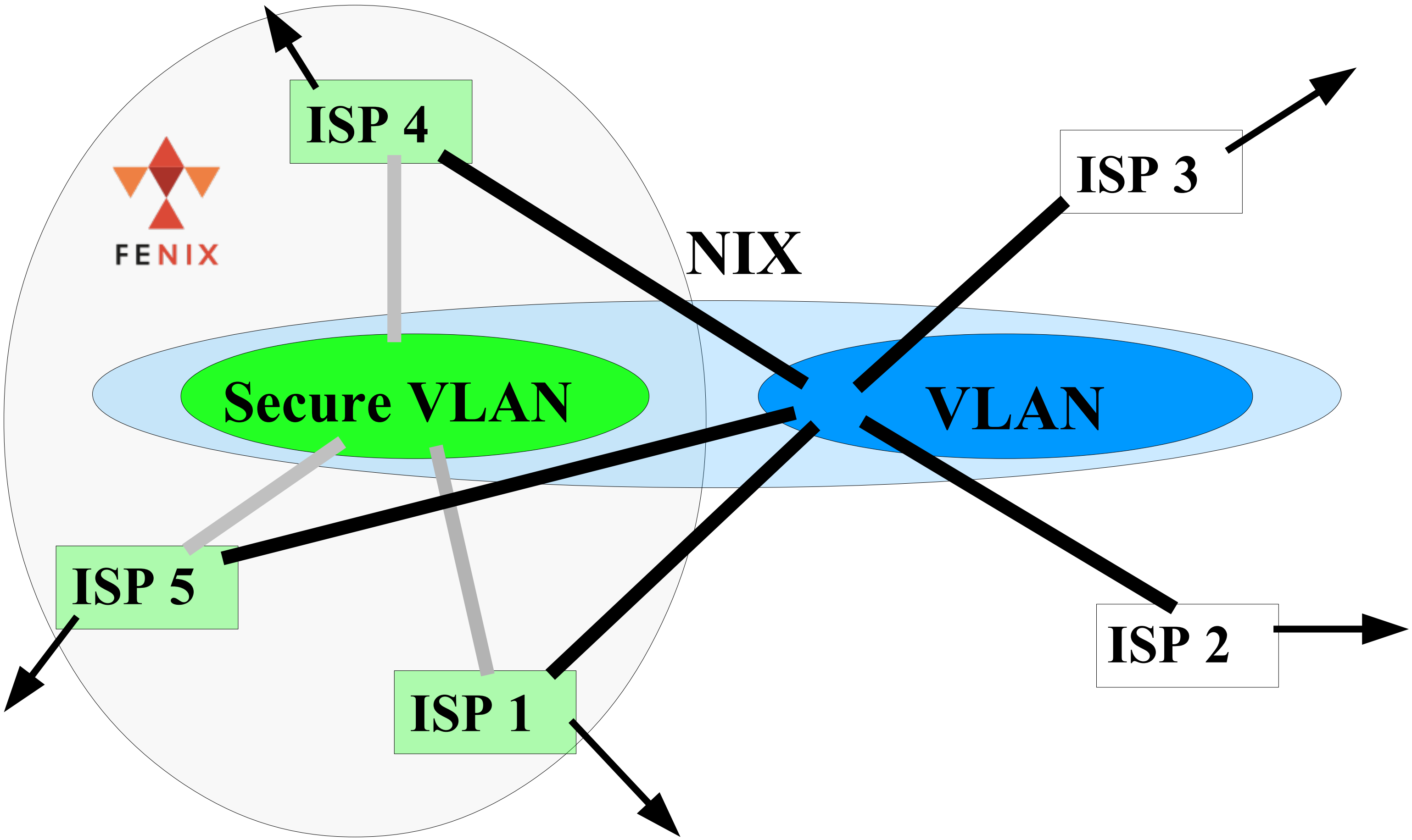
FENIX at NIX.CZ

- **Last-resort solution - “island based“ functionality of “CZ services“ for “CZ users“ under extreme attacks**
- **Technically** – standalone secure VLAN (+tools, setups) at NIX.CZ platform



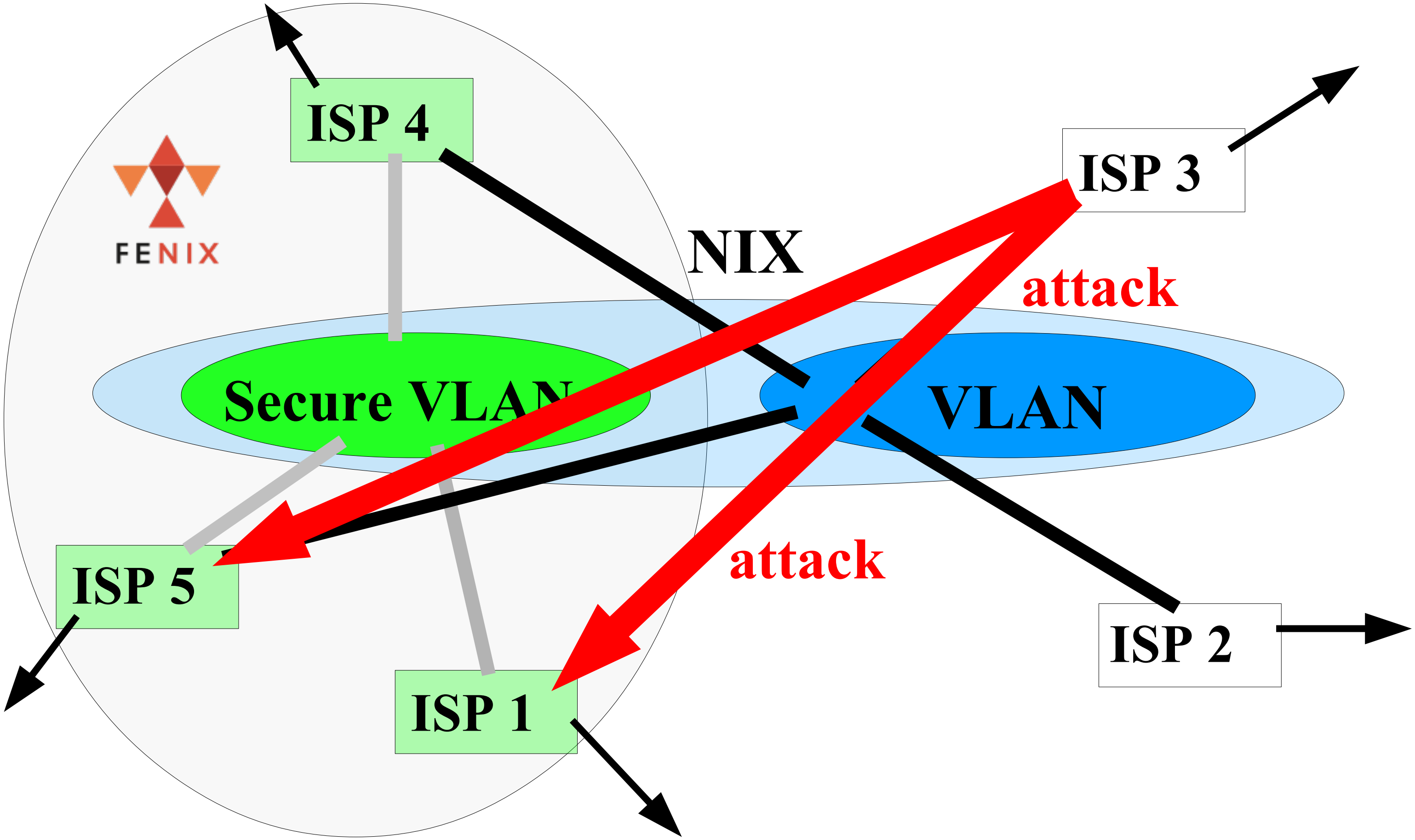
FENIX at NIX.CZ

- **Last-resort solution - “island based“ functionality of “CZ services“ for “CZ users“ under extreme attacks**
- **Technically** – standalone secure VLAN (+tools, setups) at NIX.CZ platform



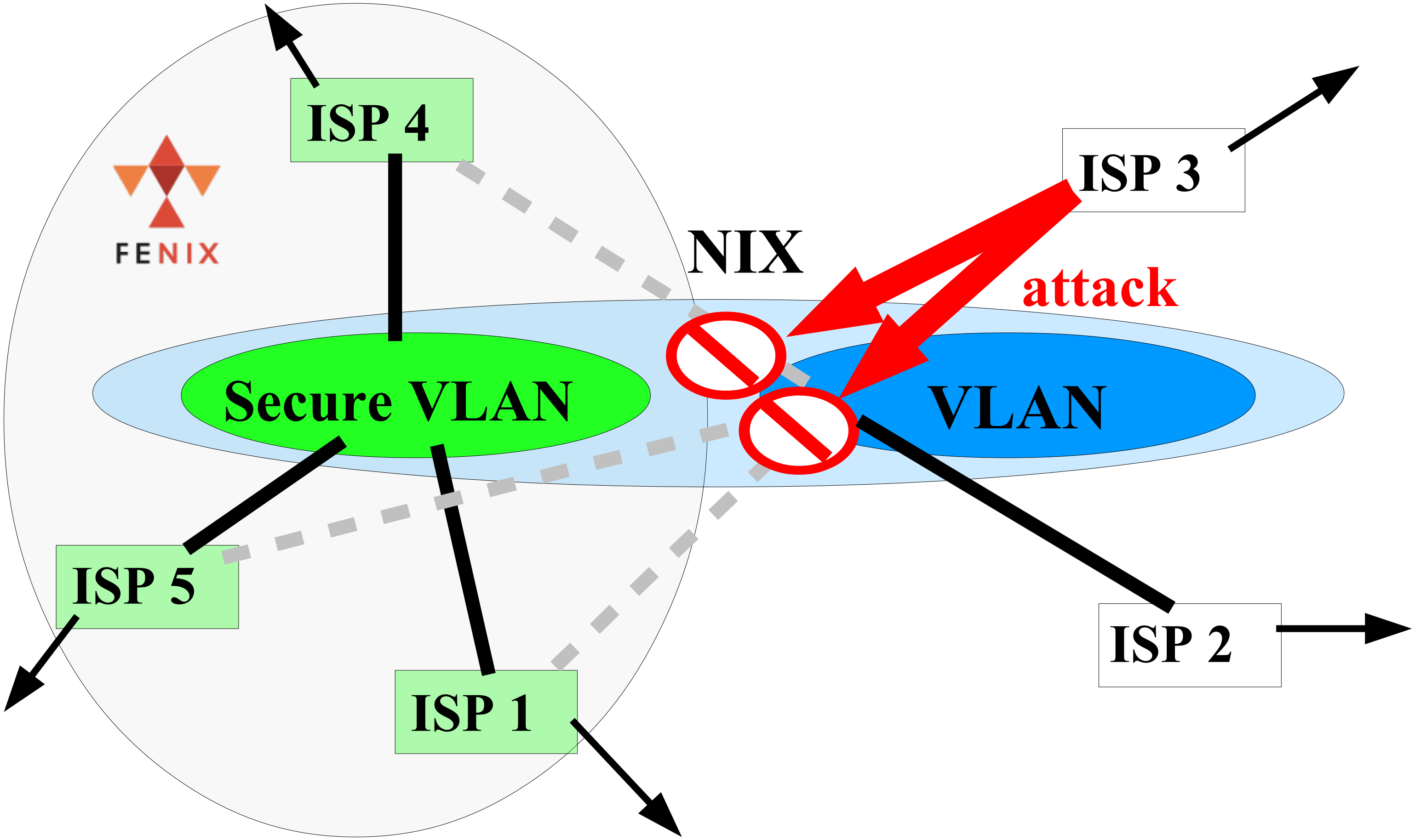
FENIX at NIX.CZ

- **Last-resort solution - “island based“ functionality of “CZ services“ for “CZ users“ under extreme attacks**
- **Technically** – standalone secure VLAN (+tools, setups) at NIX.CZ platform



FENIX at NIX.CZ

- **Last-resort solution - “island based“ functionality of “CZ services“ for “CZ users“ under extreme attacks**
- **Technically** – standalone secure VLAN (+tools, setups) at NIX.CZ platform



FENIX at NIX.CZ

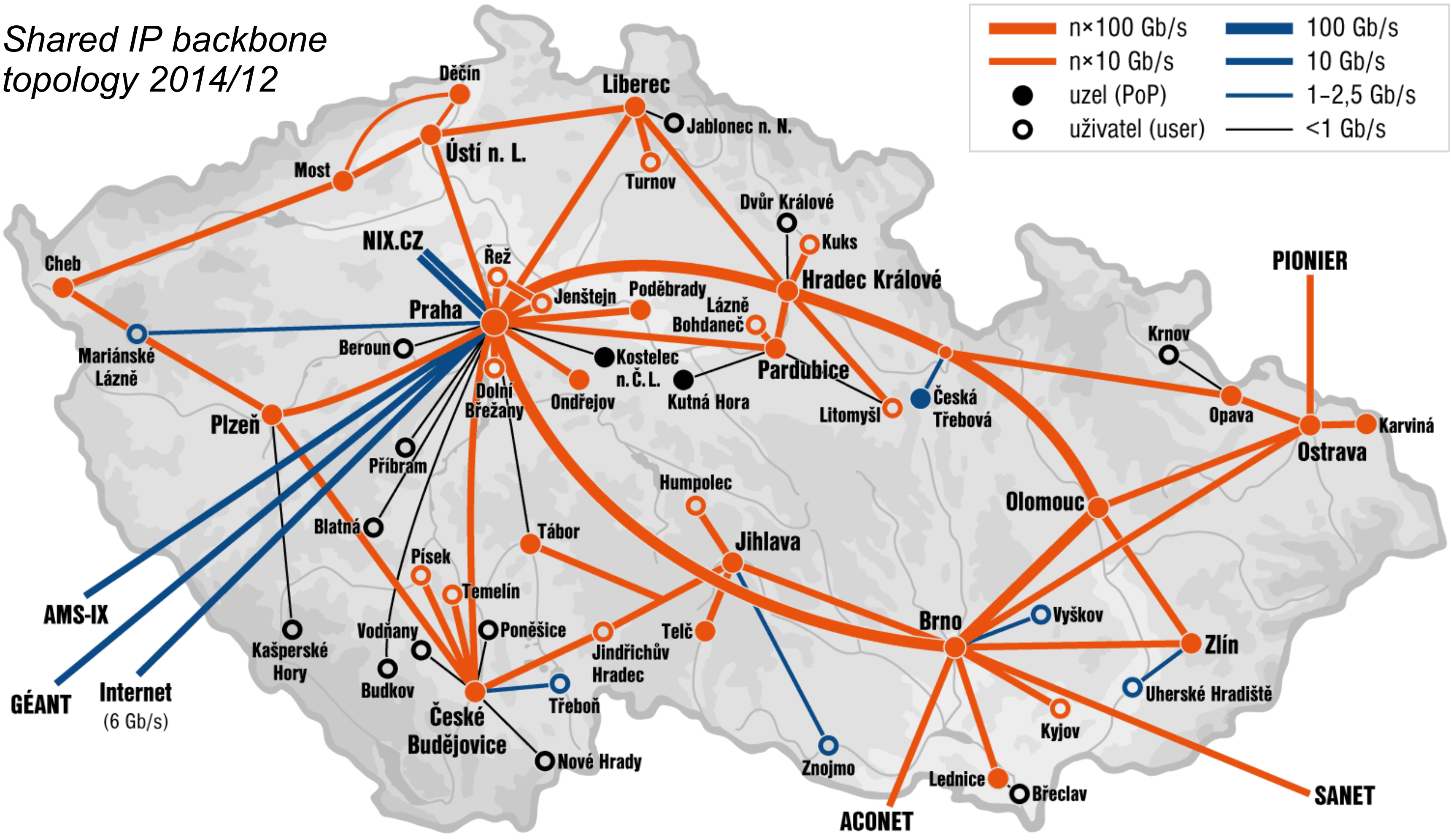
- **Last-resort solution - “island based“ functionality of “CZ services“ for “CZ users“ under extreme attacks**
- **Organisationally – “trust group“**
- **Based on agreed set of standards**
  - *CSIRT (at least listed @ Trusted Introducer – TERENA/GÉANT), 24x7 NOC (real), 6+ months and active @ NIX.CZ, at least 2 members support when entering*
  - *BCP-38/SAC004 (/24, /48), RS based RTBH, IPv6, DNSSEC (key domains), fully redundant NIX.CZ connection, network monitoring (both infrastructure & IP traffic), amplification protection (DNS, NTP, SNMP), CoPP RFC6192, BGP – MD5, incident reaction time better than 30 minutes*
- Founded January 2014 – 6 members + NIX.CZ, now 10

FENIX standards at CESNET

- *CESNET basically met FENIX standards (pioneering i some areas) at the beginning but we pushed a lot of things forward because of shared responsibility..*
- **NREN – specific environment** (community, comprehensive infrastructure)
  - High throughput **network**, **distributed storage** infrastructure, **HPC** (distributed - grid, cloud based), **collaborative environment** & **multimedia** infrastructure, **AAI** (federation of IdPs, federated access to network), etc..
- **NREN backbone network operation strategy**
  - Transparent behaviour
  - No traffic regulation unless necessary..
  - Offer tools and services to our users to regulate themselves

FENIX standards at CESNET

- **NREN – specific network environment**
  - High free capacity available up to end-nodes *(large networks Nx10 Gbps up-links)* & active user community (~400K)
  - ..are we potentially dangerous ??



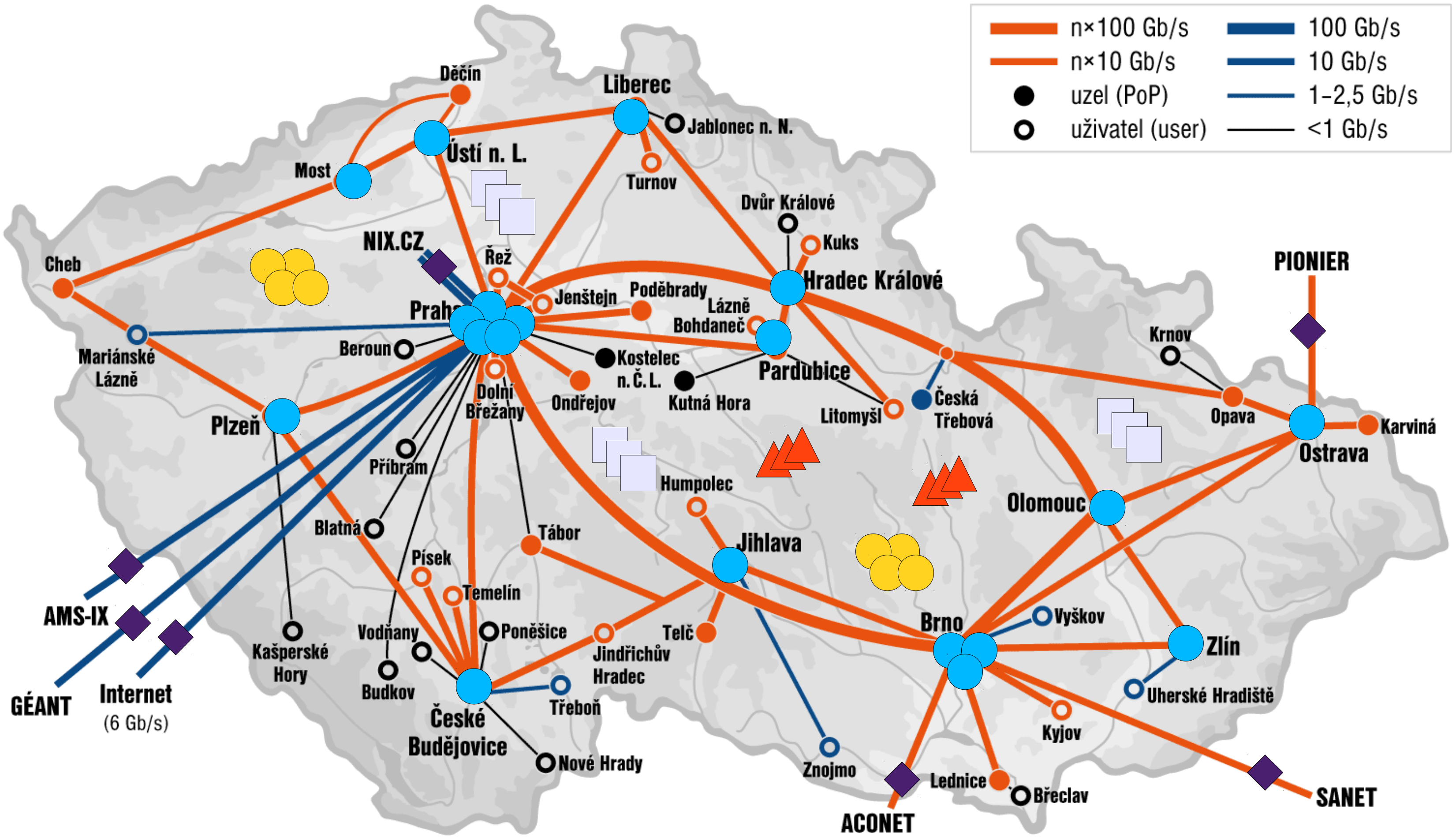
Shared IP backbone topology 2014/12

FENIX standards at CESNET

- **NREN – specific network environment**
- **BCP-38**
  - /16 v4 networks (single institutions) → have to rely on our users (and help them.. IP → MAC resolution)
  - Static filters (strict modes not possible everywhere)
- **SNMP** & **Flow based** monitoring
  - a) <u>in backbone</u>, b) <u>in user networks</u>, as service for users
  - *AS-wide anomaly detection set up by default → CSIRT, standard IH*
- **HW accelerated probes** at all external links
  - Anomalies, alternative NetFlow resources, DPI ready ~ e.g. *passive detection of heart bleeding servers*
- **IDS, Honey Pots**, systems for sharing information about detected attacks and anomalies etc.

FENIX standards at CESNET

- **Monitoring tools @ CESNET backbone**



◆ - HW accelerated probes

● - large scale (backbone-wide) flow based monitoring (NetFlow data sources)

● - Honey Pots

□ - IDS, IPS, tar pit based systems, etc..

▲ - SNMP based monitoring

1 year experience being a FENIX member

- **Shared FENIX responsibility**
  - Increases our motivation to take care consistently and to be precise & accurate while improving things – we did a lot of small technical improvements ~ solving “devil in detail“
  - Accelerates cooperation among subjects involved
    - technical staff
    - consensual views
    - mutual help and assistance
    - personal trust

1 year experience being a FENIX member

- **Shared FENIX responsibility**
  - Accelerates our internal communication esp. between “security“ and “network“ staff (strategy as well as operation)
  - We are forcing users *(+educate and support them with services and tools)* to be responsible for their network behaviour for a long time → communicating FENIX project (+ new Cyber Security Law in Czech Rep.) helps us with their motivation ;-)

1 year experience being a FENIX member

→ **it helps to increase endurance of our infrastructures** - technically & organisationally

→ **and thus pushes up the limits** beyond which we will have to switch to “island mode“..

It also pushes up the level of services and then whole market in general....

..and it makes sense..

Thank you..