cesnet

Projekt FENIX

Tomáš Košňar
CESNET

26. 4. 2018

Seminář Proaktivní Bezpečnost

- **FENIX**
  - projekt vznikl na půdě NIX.CZ v roce 2013 (reakce na DoS útoky)
  - umožnit dostupnost internetových služeb v rámci zapojených subjektů i v případech extrémních útoků
  - autonomní řízení a rozhodování - členové projektu
  - podmínky pro vstup
    - **doporučení** alespoň dvou stávajících členů
    - **čestné prohlášení** o splnění organizačních a technických podmínek

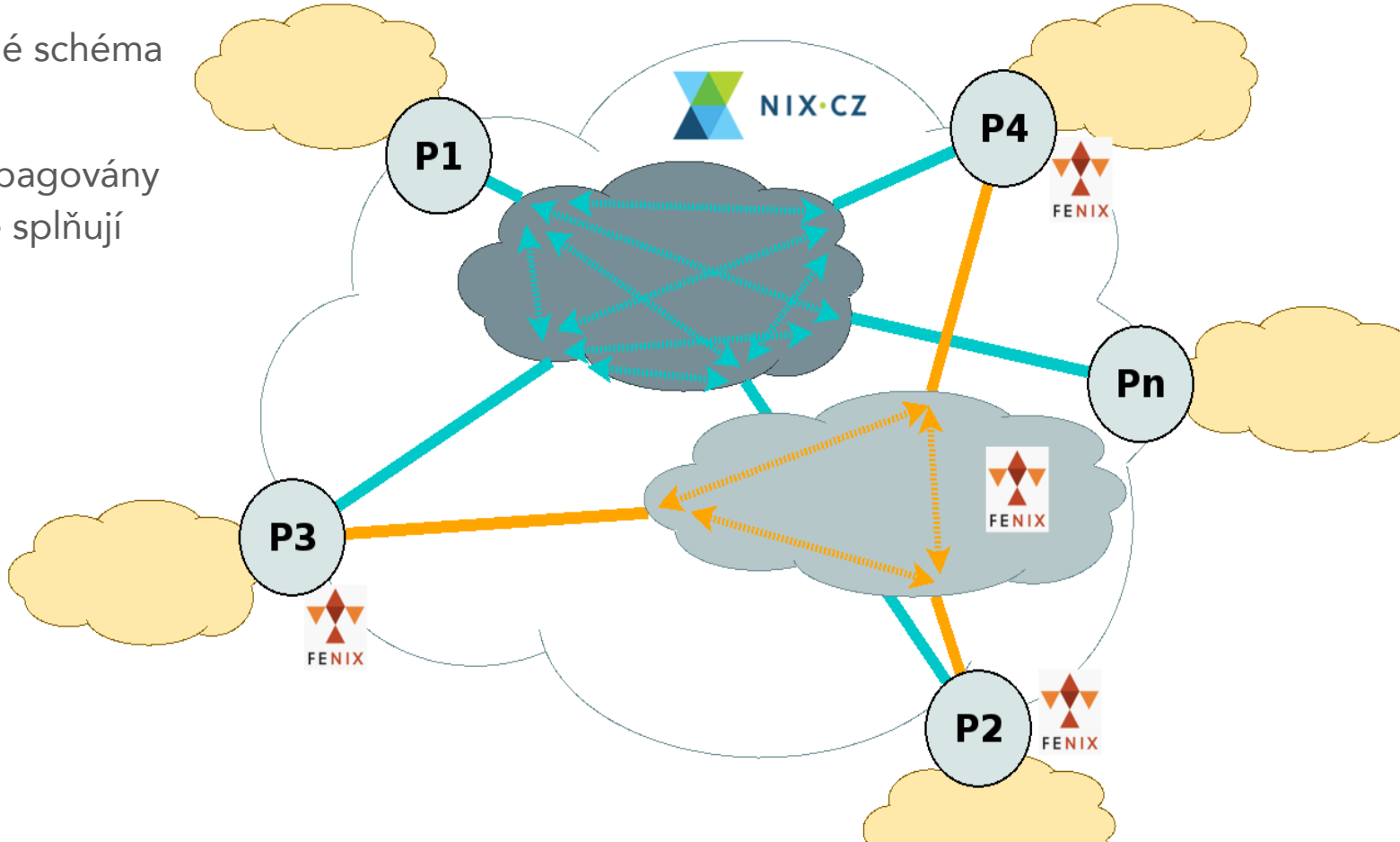
FENIX

- **FENIX**
  - **organizační podmínky**
    - připojen v NIXu alespoň 6 měsíců (podmínky připojení do NIXu)
    - aktivní účast na pracovních skupinách/hlasování v rámci projektu FENIX
    - 24/7 dohledové středisko
    - CERT/CSIRT tým s patřičným statusem
    - implementace vnitřních procesů pro řešení incidentů
    - reakční doba na bezpečnostní incident do 30 minut

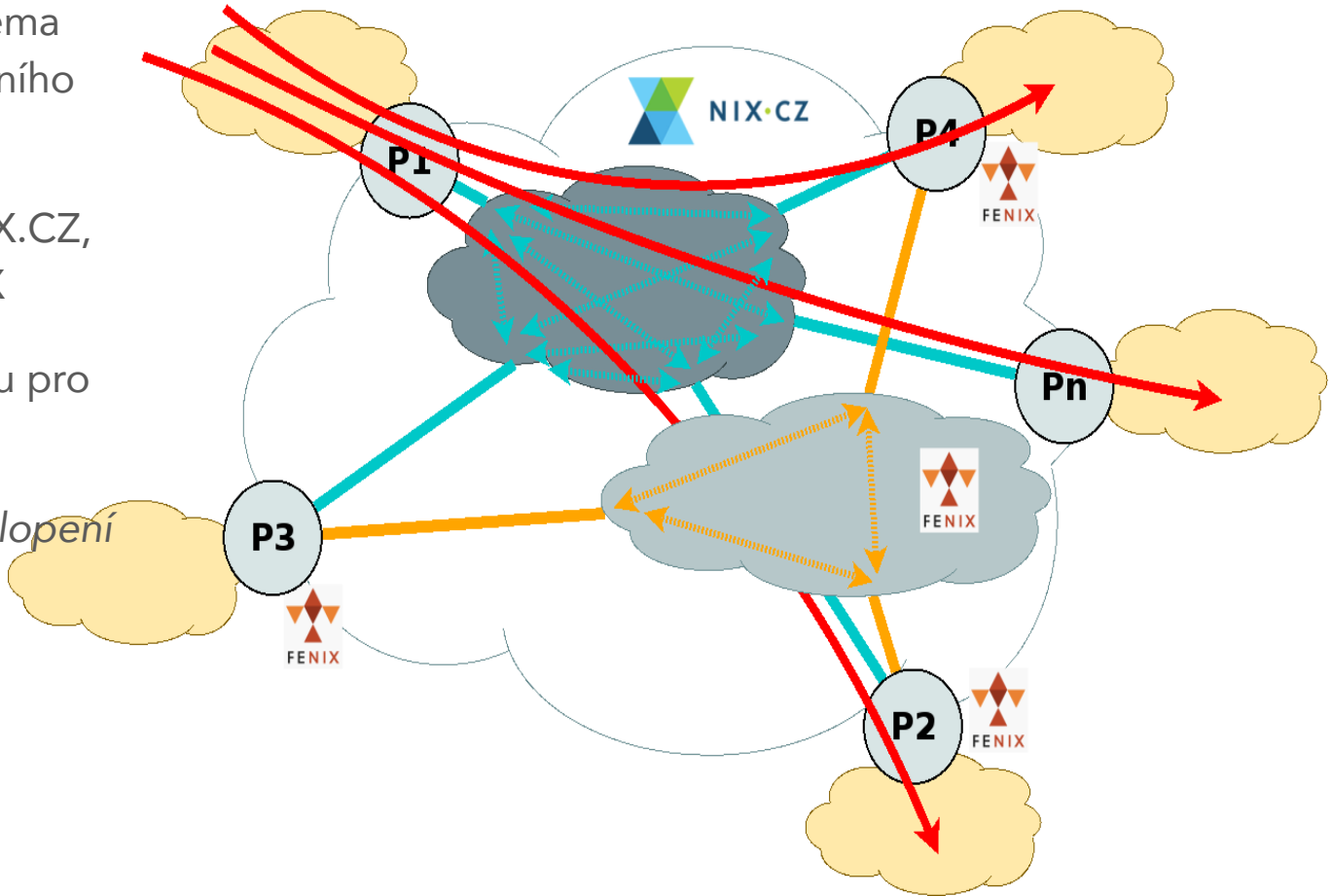
- **FENIX**
  - **technické podmínky**
    - plně redundantní přípojky do nejméně dvou uzlů NIX.CZ
    - aktivně využívá IPv4 a IPv6
    - DNSSEC podepsané domény
    - implementace control plane policy (RFC6192)
    - využívá route server v rámci FENIX
    - zapojen v systému RTBH filteringu NIX.CZ
    - kontrola zdrojových adres BCP38, SAC004 (/24,/48)
    - monitoring infrastruktury a uživatelských přípojek (SNMP, telemetrie)
    - monitoring provozu a IP toků (flow-based monitoring)
    - systém na detekci a eliminaci amplifikačních útoků

- **členové**
- zakládající
  - Active24
  - CESNET
  - CZ.NIC
  - Dial Telecom
  - NIX.CZ
  - Seznam.cz
  - O2 Czech republic
- aktuálně 20 členů

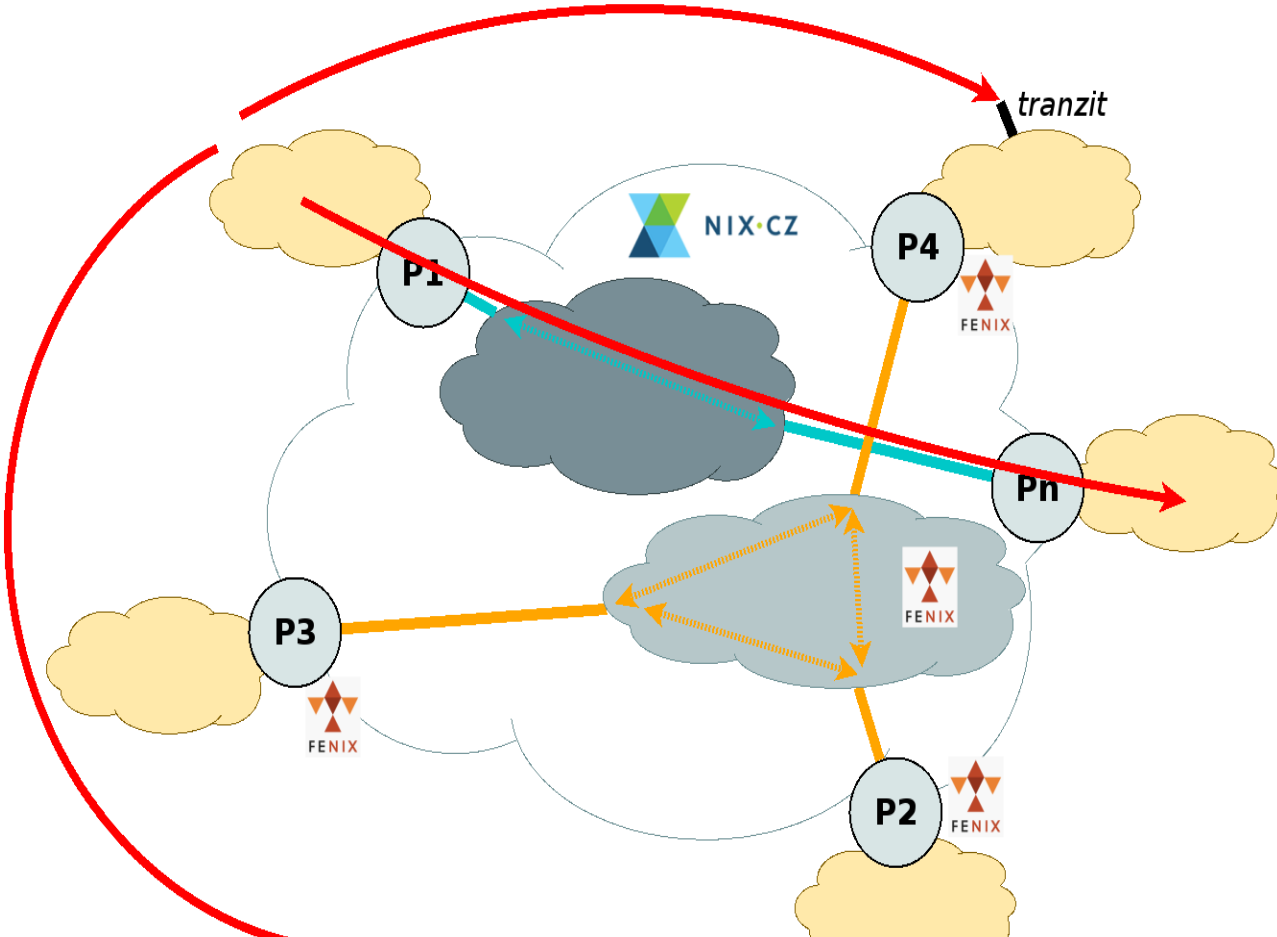
- **NIX.CZ** - zjednodušené schéma peeringu
- pozn.: do FENIXu propagovány pouze ty prefixy, které splňují podmínky



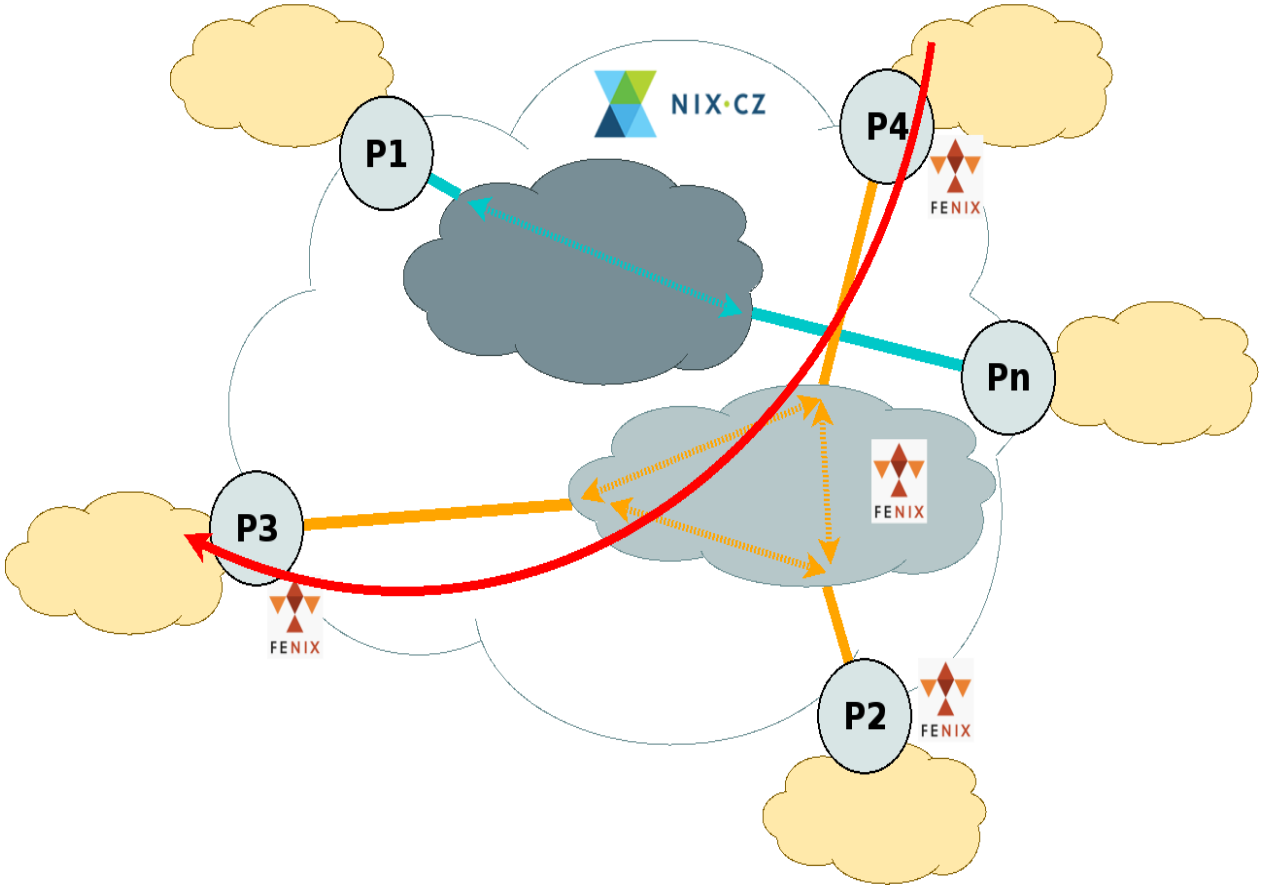
- **NIX.CZ** - zjednodušené schéma překlopení **FENIX** do ostrovního režimu
  - útok přes síť uživatele NIX.CZ, který není součástí FENIX
  - útok se šíří infrastrukturou pro „běžný“ peering
  - *..rozhodnutí členů o překlopení do ostrovního režimu*



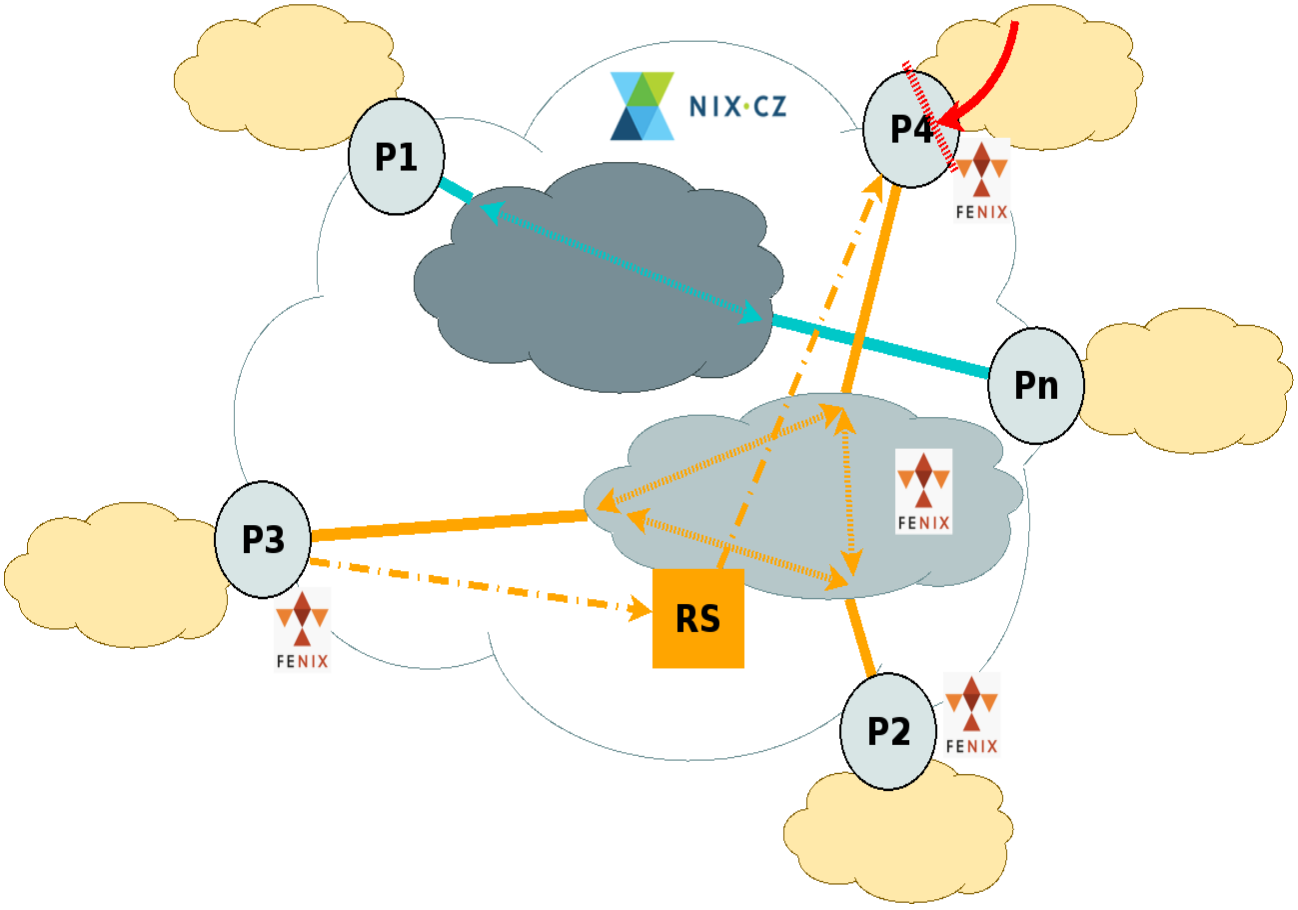
- **NIX.CZ** - zjednodušené schéma překlopení **FENIX** do ostrovního režimu
  - *..rozhodnutí členů o překlopení do ostrovního režimu*
  - „odpojení“ od infrastruktury pro „běžný“ peering
  - data útoku se přelijí do „tranzitního“ připojení
    - ..a ač se nezdá, je to pro operátory výhoda..



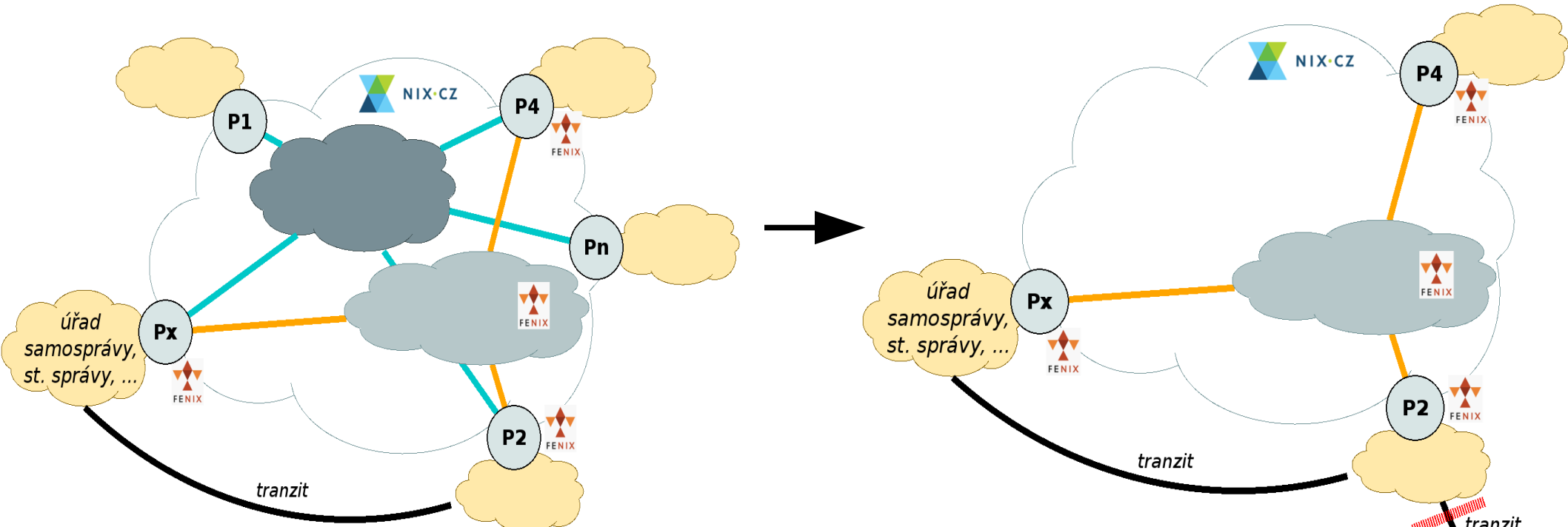
- **NIX.CZ** - zjednodušené schéma útoku v rámci **FENIX** ostrovního režimu
  - nižší pravděpodobnost
    - očekávané dodržení standardů
  - očekávaná „lepší“ reakce na útok
  - předpokládaná efektivní spolupráce



- **NIX.CZ** - zjednodušené schéma útoku v rámci **FENIX** ostrovního režimu
  - v případě, že nelze řešit jinak
    - RTBH



- **FENIX @ NIX.CZ - „**dostupnost českých služeb českým uživatelům i v extrémních situacích“
  - přiměřeně velké/významné síťové celky hostující důležité služby → do NIX ..FENIX ?
  - ..a jejich tranzitní operátor člen FENIX..



cesnet

Děkuji za pozornost...