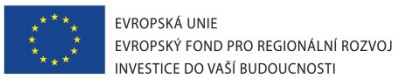
Služby e-Infrastruktury CESNET

Internet v Telči 2016

11. 8. 2016



Tomáš Košňar

CESNET z. s. p. o.

Sdružení CESNET

1996–2016 CESNET

- 1996 – založeno veřejnými VŠ a AV ČR
  - od ČVUT převzalo provoz sítě CESNET
  - začátky pan-evropského budování sítí pro výzkum, vývoj, vzdělávání → CESNET buduje oddělenou síť pro tento účel → provozuje 2 sítě (prodej komerční sítě 2000)
- několik generací sítí pro VVV, vždy v souvislosti s vývojem v evropském kontextu (TEN-34, Quantum, GÉANT..)
- 2011 – systematická podpora infrastruktur pro VV
  - cestovní mapa (vláda ČR) → Velká Infrastruktura CESNET
- 2016 → e-Infrastruktura CESNET

Sdružení CESNET

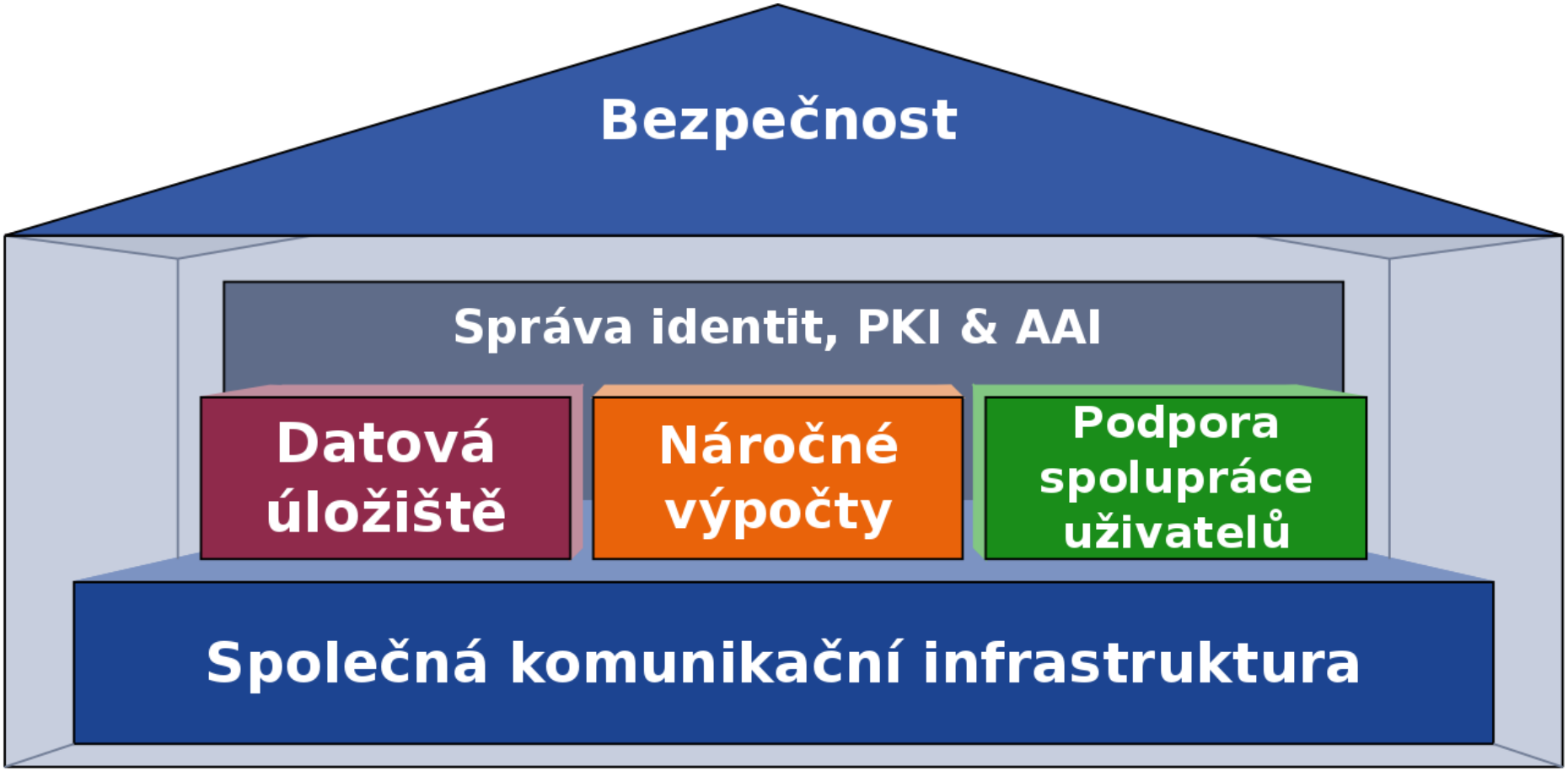
- Členství

e-Infrastruktura CESNET

- Budování komplexního prostředí pro potřeby VVV
- Uživatelé
  - Více než 300 organizací
  - Členové (Veřejné VŠ - 24, Státní VŠ – 2, AV ČR – 57 ústavů)
  - Veřejné a soukromé VŠ, nemocnice, výzkumné organizace, knihovny, muzea, galerie, ZŠ, SŠ, VOŠ, veřejná správa, samospráva, ..
  - *~ 450 tisíc individuálních uživatelů*
  - Přístup ke službám e-Infrastruktury vymezen „Access Policy“

e-Infrastruktura CESNET

- Symbolická architektura, základní komponenty



Společná komunikační infrastruktura

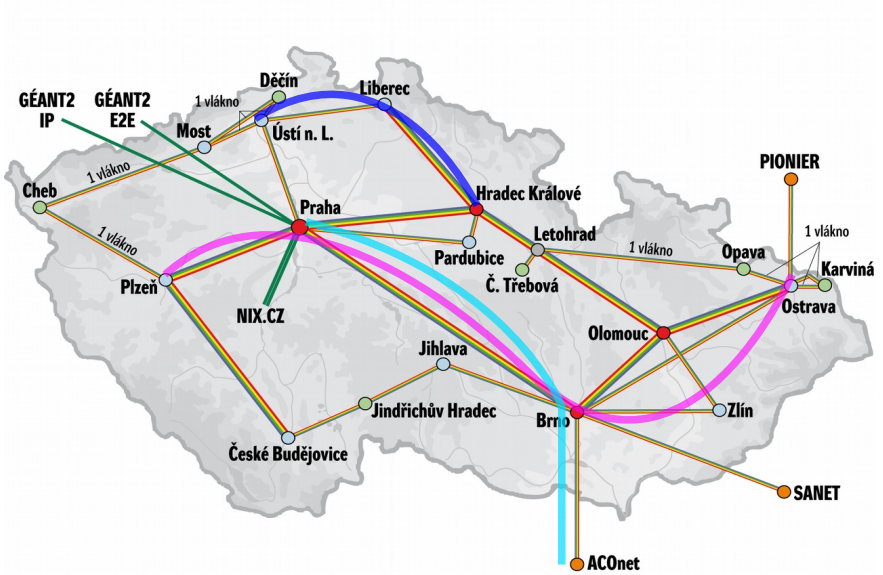
1996–2016 CESNET

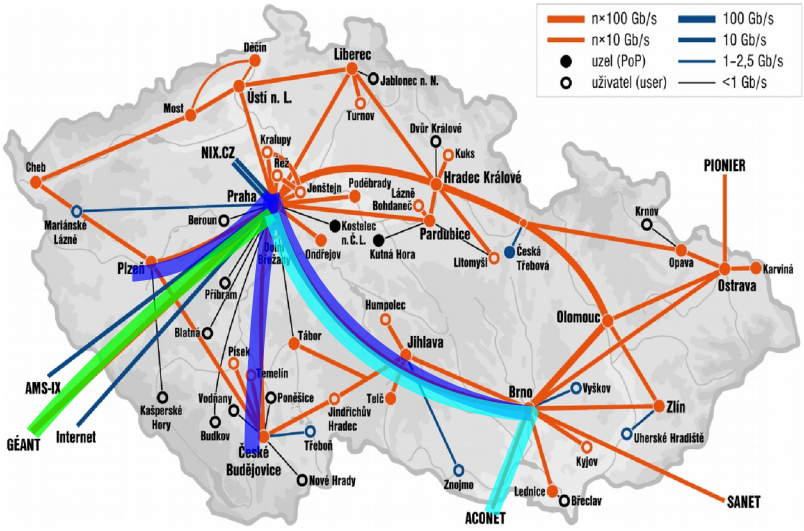
Podpůrná Infrastruktura	• Správa adresových zdrojů v4, v6, údajů v RIPE, asistence při zakládání LIR • **DNS** – primární, sekundární, záložní, DNSSEC • **Mail-relay** – záložní • **AntiSpam Gateway** • **Monitoring** infrastruktury, **IP provozu** • **24x7 dohled**
IP/MPLS páteřní infrastruktura	• Multi-Protocol Label Switching, IP, • Platforma pro vytváření **logických sítí** nebo **okruhů** pomocí služeb optické přenosové infrastruktury
Optická přenosová infrastruktura	• Vlnový multiplex – WDM technologie, 2 systémy – Cisco 15454, až 80 kanálů 1-100Gps – jádro – Open DWDM, 1-100Gps, připojování k páteři • Platforma pro vytváření **nezávislých propojů bod-bod**
Fyzická infrastruktura (temná vlákna)	• Optická vlákna, duální připojení páteřních uzlů • cca 6000 km (1800 jednovláknové)

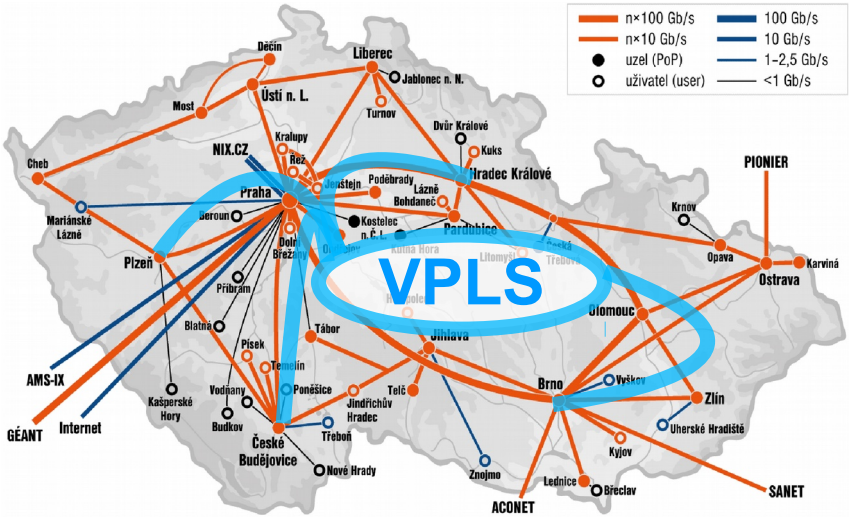
Služby komunikační infrastruktury

- **Vyhrazené okruhy a sítě**

- Fotonické služby – nezávislé „čistě“ optické propoje
  - Speciální náročné aplikace
- Lambda služby – optické propoje s OEO konverzí
- Vyhrazené okruhy a sítě
  - EoMPLS
  - VPLS







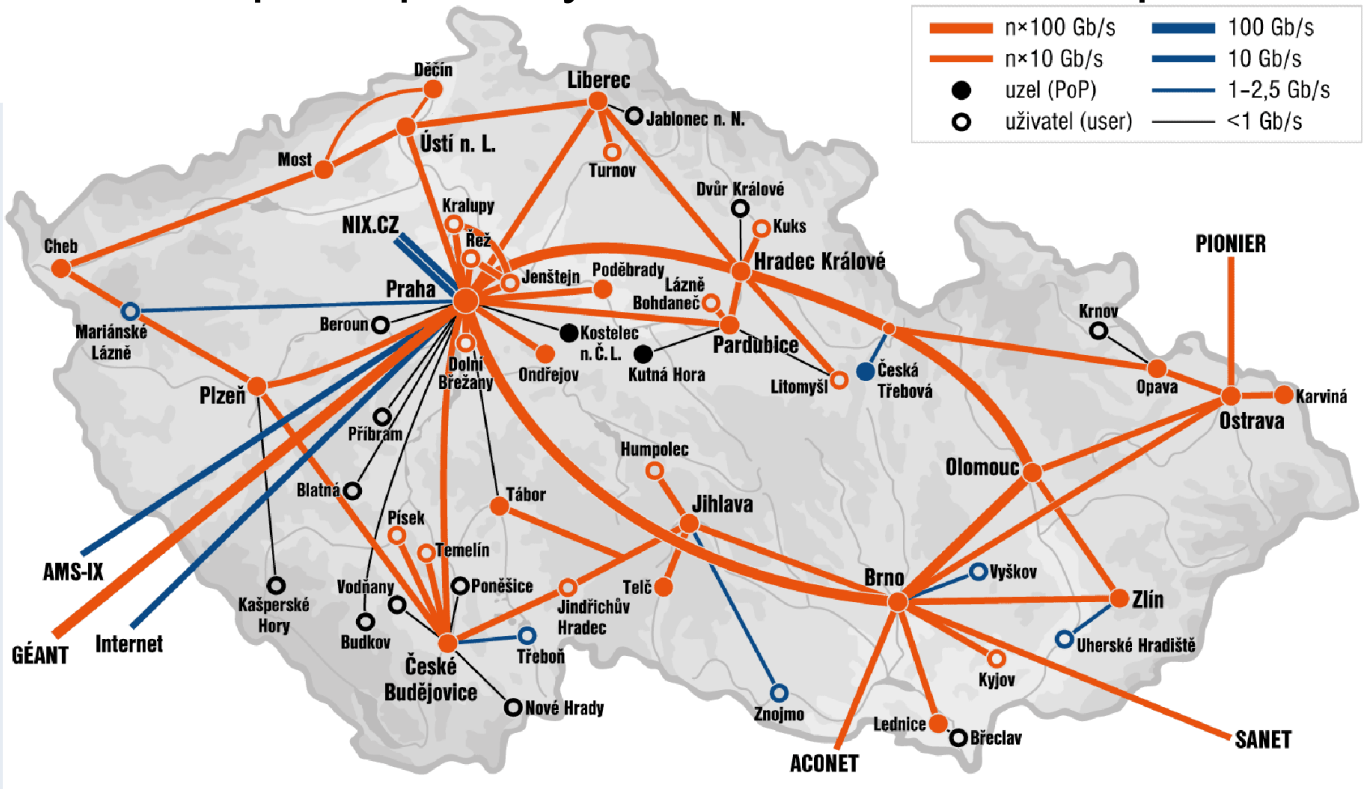
Služby komunikační infrastruktury

1996–2016 CESNET

- **Sdílená IP síť – připojení IP protokolem**
- **100 Gbps jádro; uzly Nx10 Gbps, 40-100 Gbps**
- Dostatečná kapacita, dostatečné přístupové rychlosti ~ Nx10, 40Gbps

- **Externí propojení**
- **220 Gbps**
- 100 Gbps GÉANT
- 120 Gbps IX, partneři
  - 40 Gbps NIX.CZ
  - 20 Gbps ACONET (VIX)
  - 20 Gbps SANET (SIX)
  - 10 Gbps PIONIER
  - 10 Gbps AMS-IX
  - 10 Gbps Google
  - 10 Gbps Tier-1

- **E2E**
  - 4x10 Gbps GÉANT
  - Nx10 CBF (AT, SK, PL)
  - 10 Gbps GLIF



- IPv4, IPv6 – dual stack, unicast, multicast
- Duální fyzické připojení uzlů
- Duální páteřní uzly
- Redundance, flexibilita

Služby komunikační infrastruktury

- **Sdílená IP síť – připojení IP protokolem**

- Symetrické připojení bez regulace provozu (legitimního), možnost redundantního připojení do dalšího uzlu
- Dohled a monitoring funkcí a bezpečnosti sítě 24/7/365
- Správa a přidělování adresových zdrojů IPv4, IPv6, správa údajů v RIPE, asistence při zakládání LIR
- DNS – primární, sekundární, záložní, DNSSEC
- Mail-relay – záložní
- AntiSpam Gateway

Služby komunikační infrastruktury

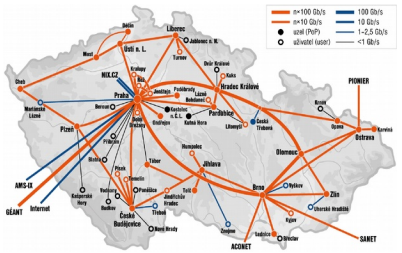
1996–2016 CESNET

- **Sdílená IP síť – připojení IP protokolem**

- BCP38, RPF check + další mechanismy eliminace podvržených zdrojových adres na vstupu do páteře
- Semi-automatická obrana páteře proti DDoS útokům na bázi amplifikace
- RTBH jako služba (BGP připojené sítě)
- Permanentní monitoring stavu a využití celé páteře
- Permanentní monitoring IP provozu (flow-based) na perimetru sítě a v celé páteři + detekce typických útoků
- *…perspektivy ~ BGP FlowSpec ?*
- CESNET - zakládající člen projektu FENIX v rámci NIX.CZ
- *...uživatelé a FENIX, podmínky projektů ?*

FENIX

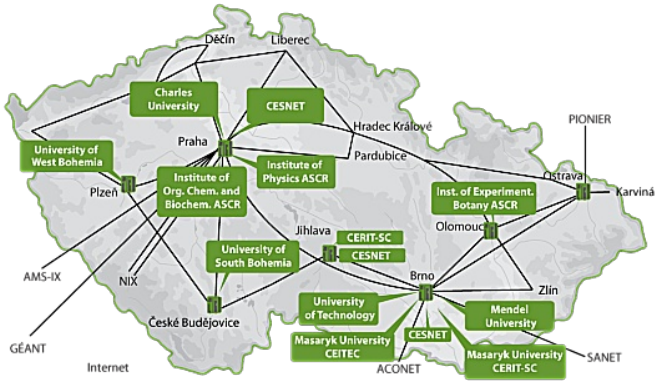
Důvěryhodný operátor



Náročné výpočty - MetaCentrum

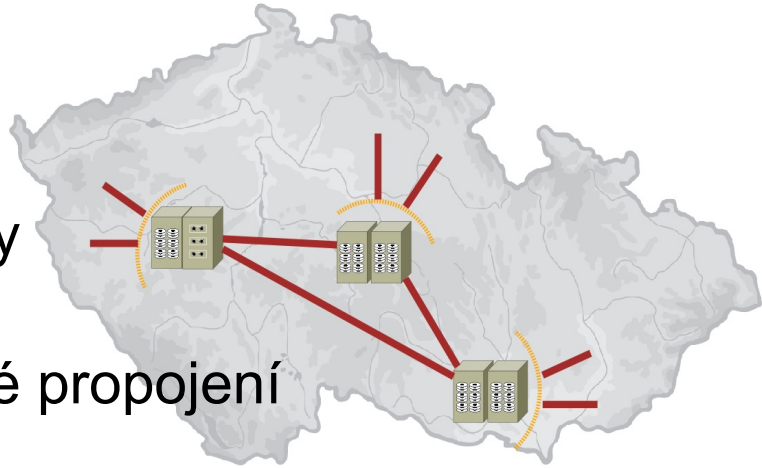
- **MetaCentrum** zajišťuje a koordinuje provoz **NGI** (Národní Gridové Infrastruktury) – národní součást **EGI** (Evropské GI)

„Sdružení výpočetních a datových zdrojů pro řešení velmi náročných úloh, které jsou za hranicemi výpočetních možností samostatného pracoviště“



- Aktuálně ~ 12k jader, 2PB storage (EGI 3.8PB)
- **Grid+Cloud+MapReduce výpočty**
  - Konvenční i specifický HW
- **Aplikační SW**
  - Koordinace pořizování a správy programového vybavení
  - https://wiki.metacentrum.cz/wiki/Kategorie:Aplikace
- **Uživatelská podpora**
  - Konkrétních problémy, optimalizace algoritmů, …
- **Integrace výpočetních kapacit do NGI**
- **Příprava specifického prostředí**
  - Úprava stávajícího nebo nové platformy (Galaxy, Chipster)
  - Specifické velké skupiny uživatelů (EGI, ELIXIR)

Datová úložiště



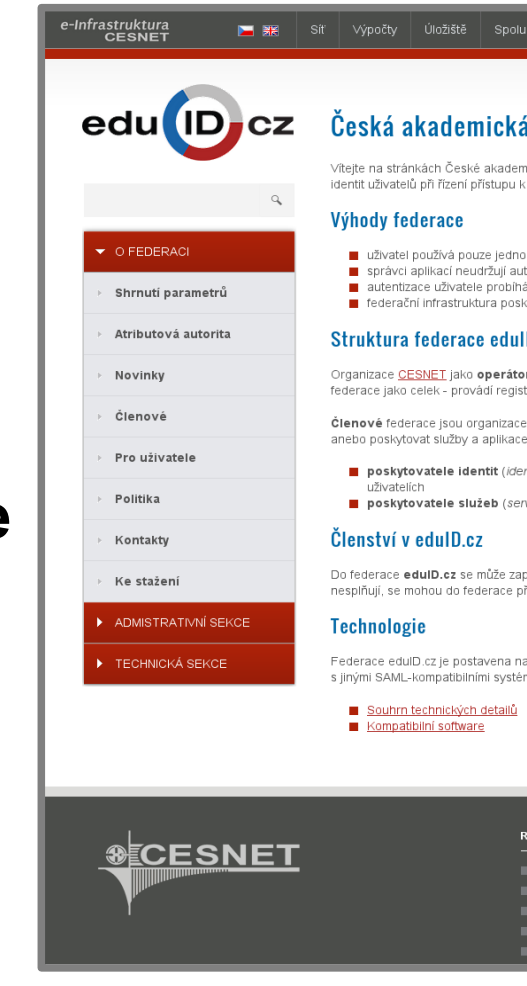
- Distibuovaná architektura HSM úložišť
- Plzeň, Jihlava, Brno → 21+PB fyzické kapacity
- Dedikovaná síťová infrastruktura pro vzájemné propojení
- Dedikovaná infrastruktura pro připojení do páteřní sítě
- Dlouhodobé ukládání primárně vědeckých dat (úroveň binárních dat)
- **Zálohy, archivace, sdílení dat, speciální aplikace**
  - Souborově orientovaný přístup - NFSv4, FTP, rsync, SCP, …
  - Speciální aplikace - Grid storage element, DCache
  - FileSender
  - ownCloud

Podpora spolupráce uživatelů

- **Webkonference** – základní kvalita obrazu
- **Videokonference** – H.323/SIP, MCU (Limit Full HD)
  - Začlenění zařízení uživatelů do VC infrastruktury, ClearSea, rezervační portál **meetings.cesnet.cz**
- **IP telefonie** – propojení IP-telefonních sítí v rámci e-infrastruktury a s partnery
- **Streaming** – distribuční platforma pro multimediální vysílání do Internetu (Windows Media, MPEG-4 Flash/HTML5)
- **Videoarchiv** – platforma pro uložení obsahu a jeho vystavení pomocí streamovacích serverů
- **Speciální obrazové přenosy a vizualizace**
  - Vysoké rozlišení, nízká latence, lékařské zákroky, vědecké vizualizace (SAGE, CAVE), vzdálená spolupráce pří zpracování obrazových dat HD+ (2K, 4K, 8K) apod.
  - Vlastní vyvíjené systémy (UltraGrid, 4K Gateway)

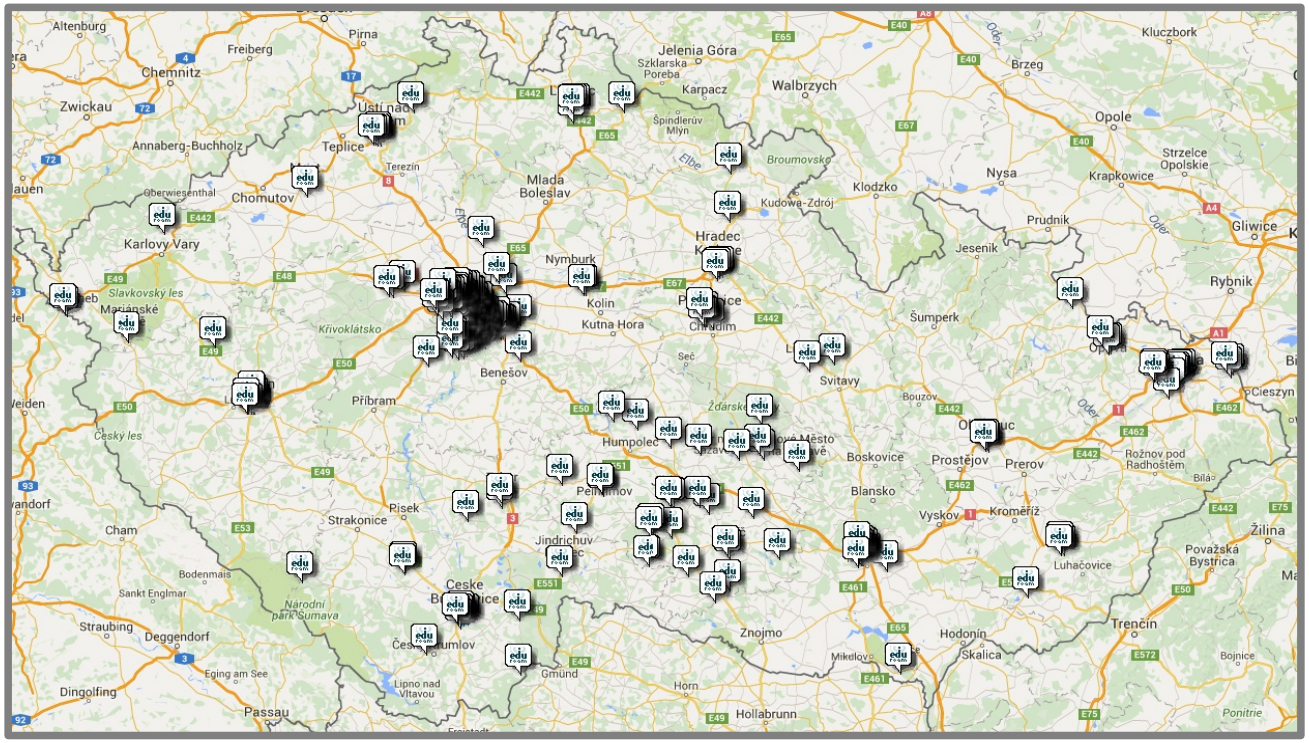
Správa identit PKI & AAI

- **eduID.cz - Česká akademická federace identit**
  - **Jedno uživatelské jméno a heslo pro přístup k řadě síťových služeb** *(v multi-institucionálním prostoru)*
  - Poskytovatelé služeb z národní komunity i mezinárodní
  - Součást mezinárodní interfederace eduGAIN
- **Certifikáty pro uživatele a servery**
  - Důvěryhodný server
  - Důvěryhodná identita uživatele
- **Jednotný systém správy účtů v e-Infrastruktuře**
  - Některé služby odebírané na individuální bázi
  - Strukturování uživatelské komunity
  - Řízený přístup ke zdrojům



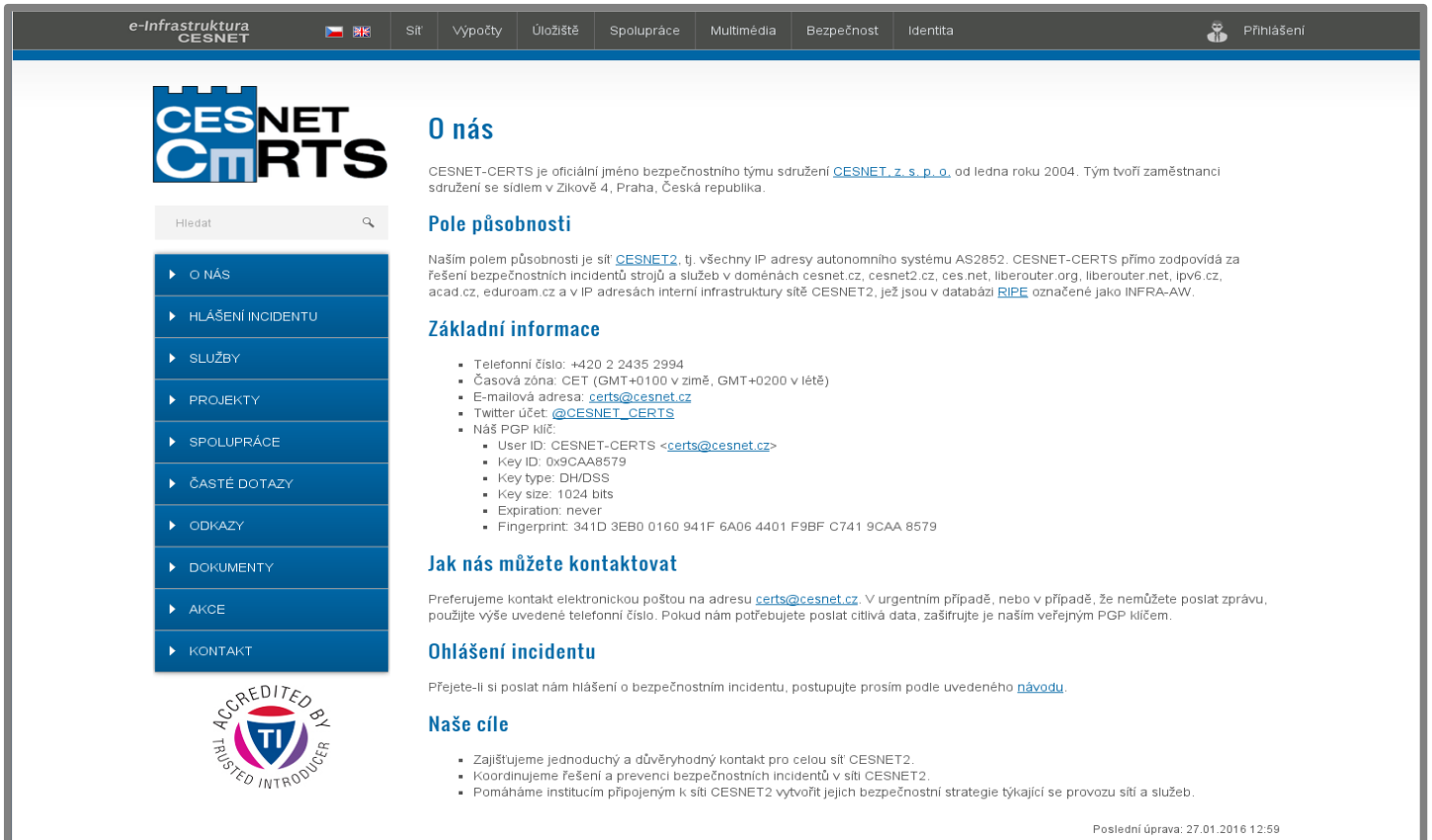
Správa identit PKI & AAI

- **eduroam -** „služba na pomezí“: služba z oblasti ověření uživatelů, z pohledu koncového uživatele síťová služba **- roaming uživatelů v hostitelské síti**
  - Síťovou infrastrukturu zajišťuje hostitelská síť; síťová infrastruktura je opřena o autentizační infrastrukturu (technicky RADIUS server hostitelské organizace zapojený do národní hierarchie)
  - *...podmínky projektů ?*



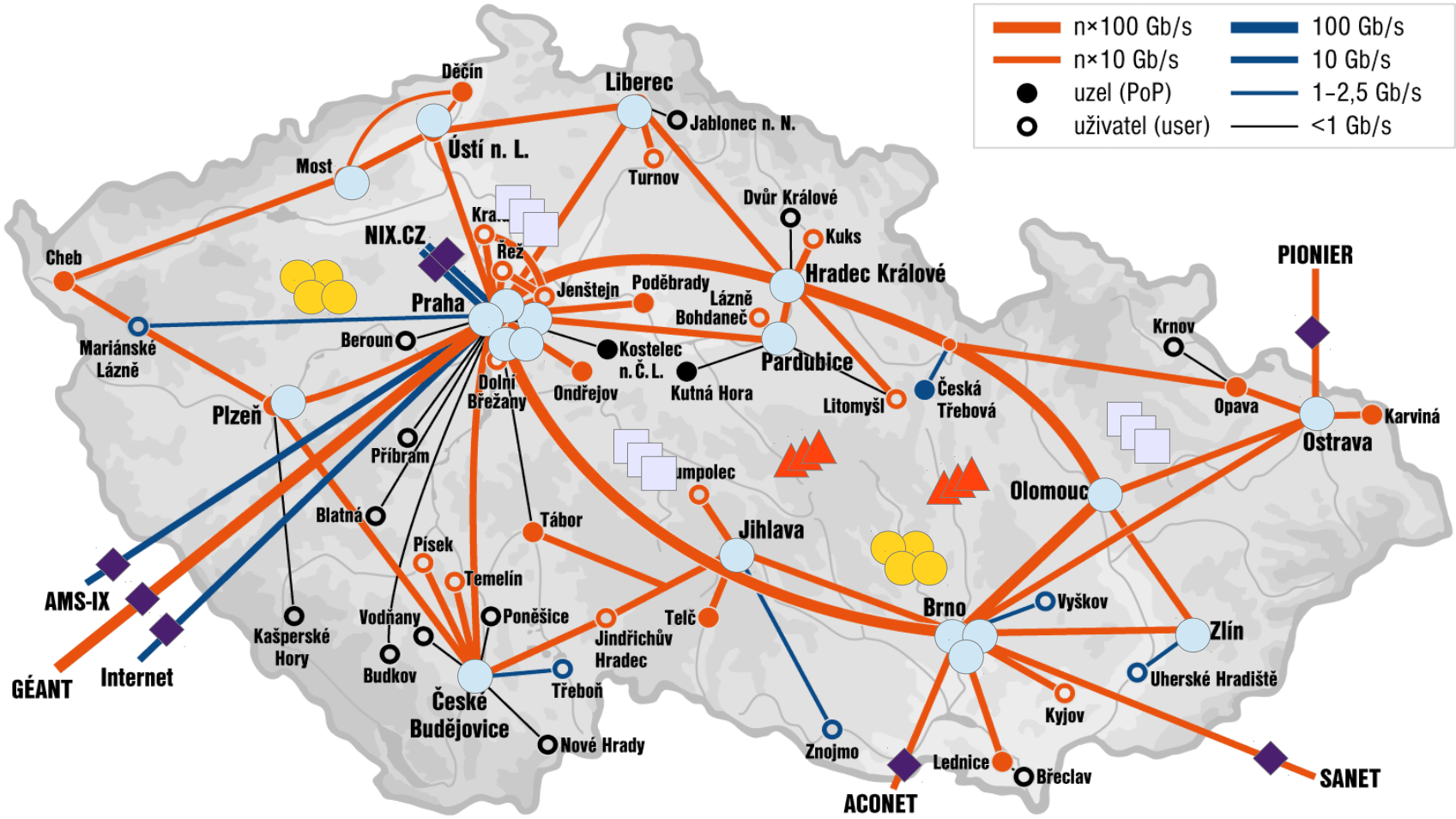
Bezpečnost

- **Řešení bezpečnostních incidentů (CSIRT)**
  - Bezpečnostní tým CESNET-CERTS
    - https://csirt.cesnet.cz/
  - Platforma (technická, organizační) pro řešení a asistenci při řešení bezpečnostních incidentů v e-infrastruktuře CESNET a administrativní doméně komunity



Bezpečnost

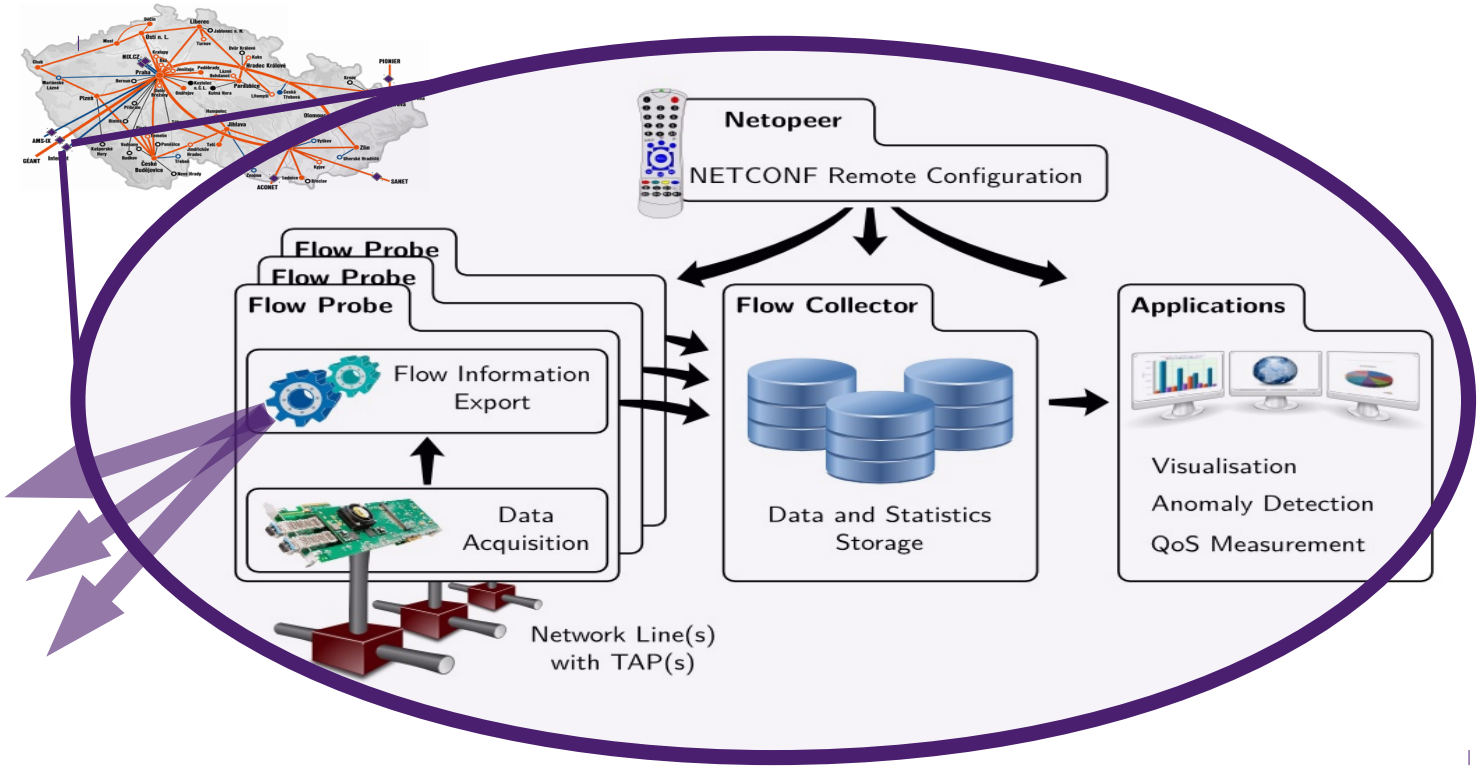
- **Infrastruktura a služby v oblasti bezpečnosti**



- ◆ - HW akcelerované sondy
- ● - plošný monitoring IP provozu na bázi toků (zdroje provozních informací)
- ● - Honey Pots
- ▢ - IDS a IPS systémy apod.
- ▲ - monitoring infrastruktury na bázi SNMP

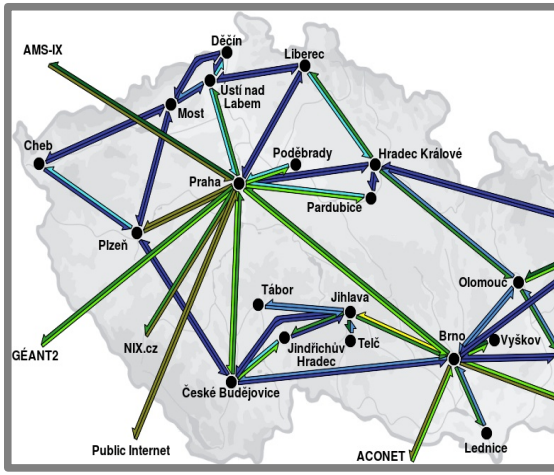
Bezpečnost

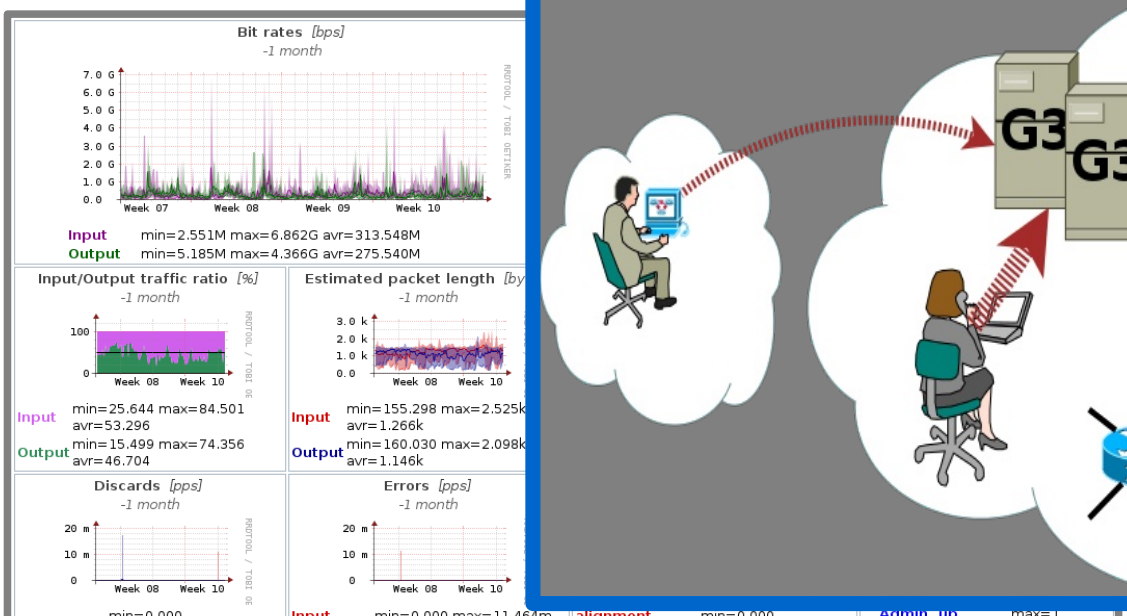
- **HW akcelerované sondy → kompletní provoz na lince**
  - Bezeztrátové a detailní měření síťových dat na volitelné úrovni detailu, tunelovaný provoz, detailně HTTP, DNS, SIP; užitečné pro ruční analýzu, možnost vyčlenit provoz; statistiky, zdroj dat a informací pro další výzkum
  - Detekce událostí a anomálií na paketové a IP úrovni
  - Perimetr e-Infrastruktury, STaaS

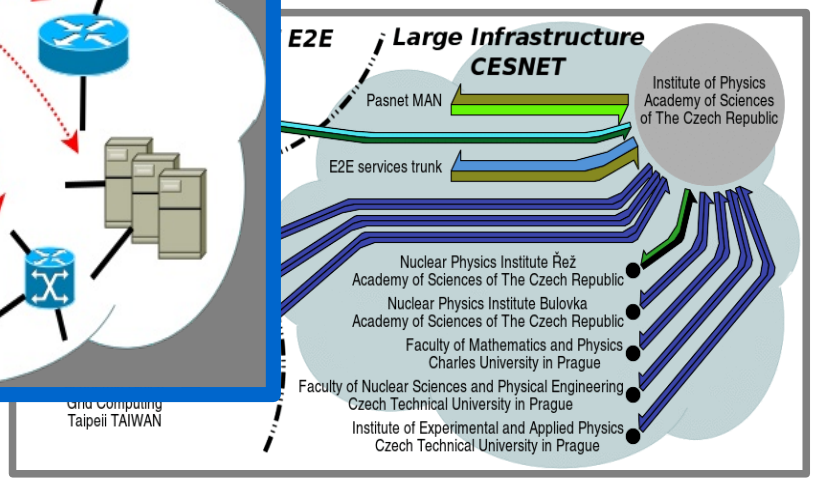


Bezpečnost

- **Systém G3 → prvky infrastruktury**
  - Sběr informací (SNMP a další metody) nejen ze síťových prvků
  - Interaktivní UI, periodický reporting
  - Detekce, vizualizace a notifikace anomálií
  - Síťová část e-Infrastruktury
  - **Služba pro uživatele – vlastní instance** *...kde ?*

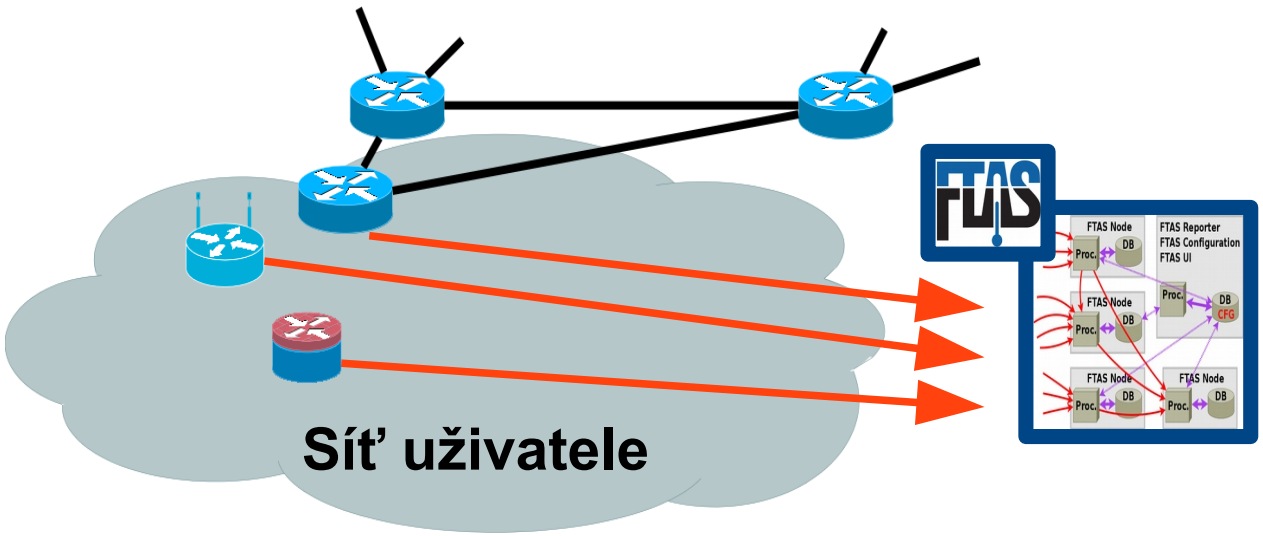


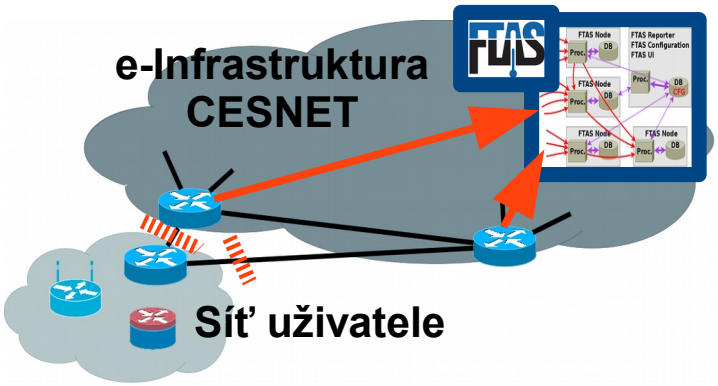


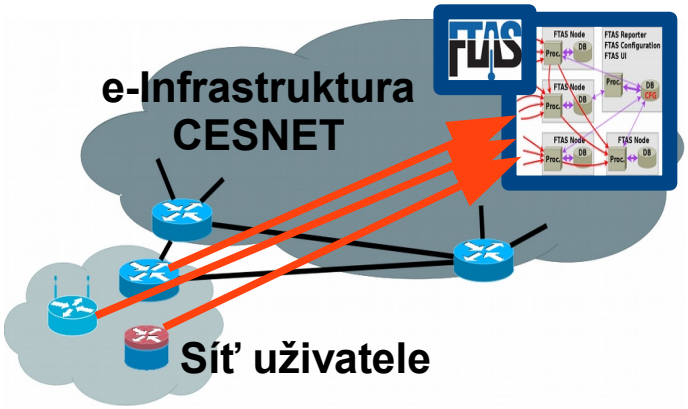


Bezpečnost

- **Systém FTAS → IP provoz na bázi toků**
  - Zpracování Informací o IP provozu na bázi toků (tzv. NetFlow)
  - Interaktivní UI, periodický reporting
  - Detekce a notifikace událostí/anomálií na úrovni IP toků
  - Síťová část e-Infrastruktury
  - **Služba pro uživatele** *...jak, kde ?*

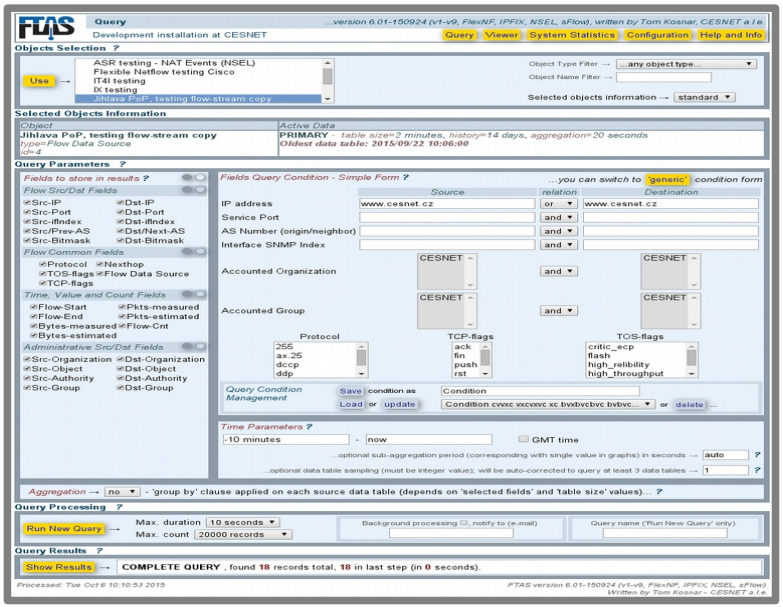


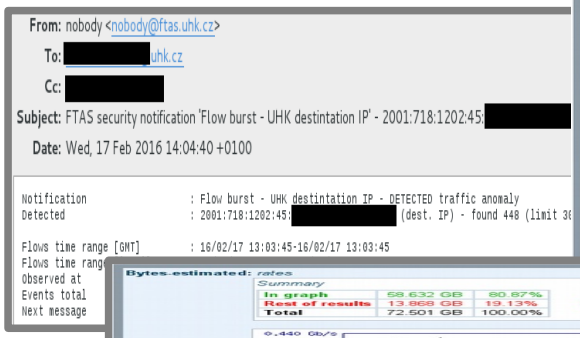


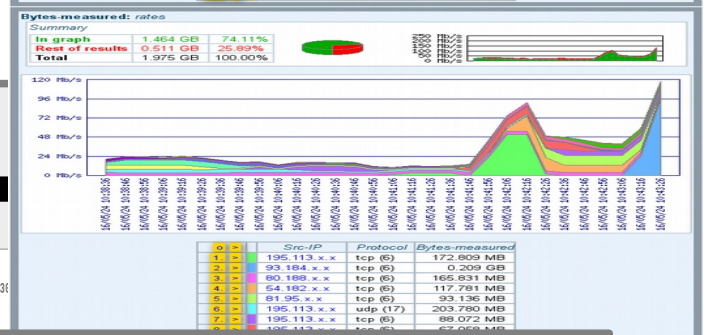


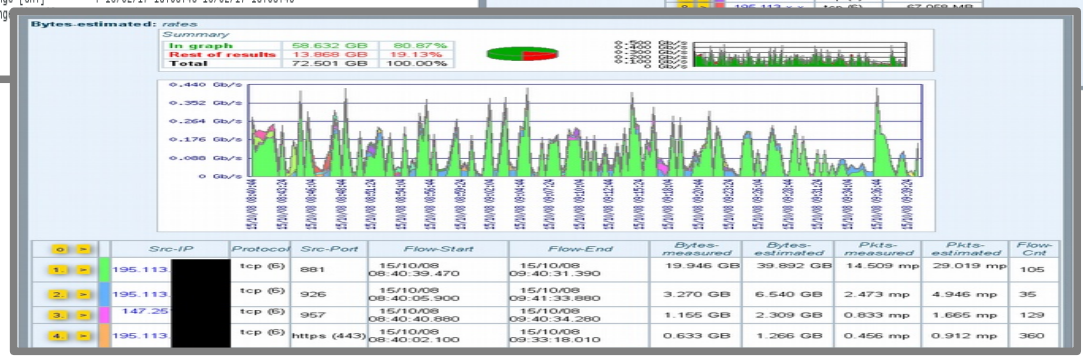
Bezpečnost

- **Systém FTAS → IP provoz na bázi toků**
- V závislosti na možnostech exportu zařízení
  - ~ běžné provozní záznamy (v1-v9, IPFIX, FNF, sflow)
  - Kompletní překladové provozní záznamy
  - Kompletní překladové logy (NSEL)
  - MAC adresy
- Plně konfigurovatelné detektory anomálií
- Fce UI → komplexní analýza provozu
- *...podmínky projektů ? ZKB ?*









Bezpečnost

- **IDS, IPS systémy Honeypoty**
- **Systémy pro sdílení informací, SIEM**
  - Sběr a „normalizace“ informací o anomáliích a detekovaných událostech

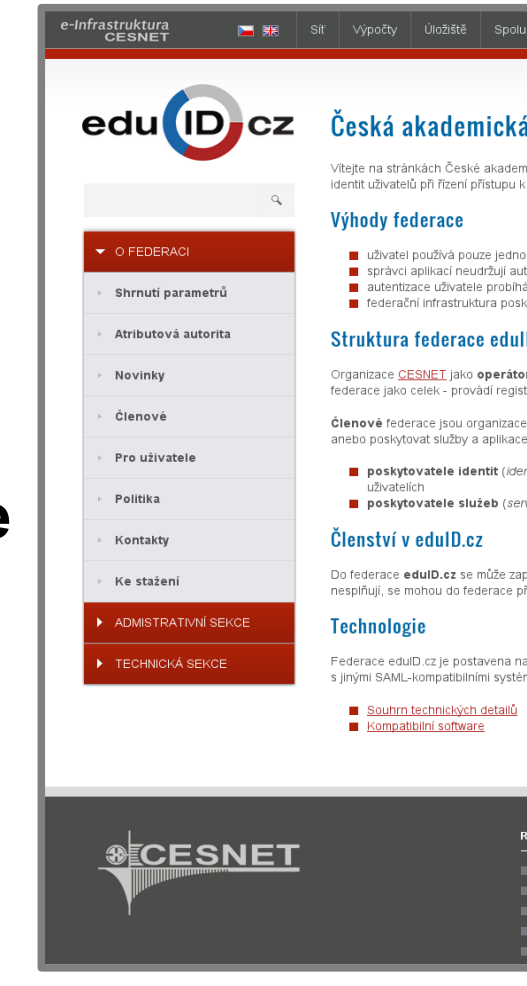
  - „Přispívám, přispíváš, přispíváme → odebírám“ (+ informace z více míst, agregace, korelace)
- **Forenzní laboratoř**
  - Penetrační testy
  - Zátěžové testy
  - Analýzy událostí
  - https://flab.cesnet.cz/

Bezpečnost

- **Bezpečnostní školení**
  - Na míru pro typové skupiny
    - Zaměstnanci
    - Studenti
  - Na míru tématicky
  - Technické a legislativní aspekty
  - Prevence, odpovědnost za svoje chování v síti, gramotné užívání výpočetní techniky
  - Diskuze o konkrétních problémech (v dané síti/místě/instituci)

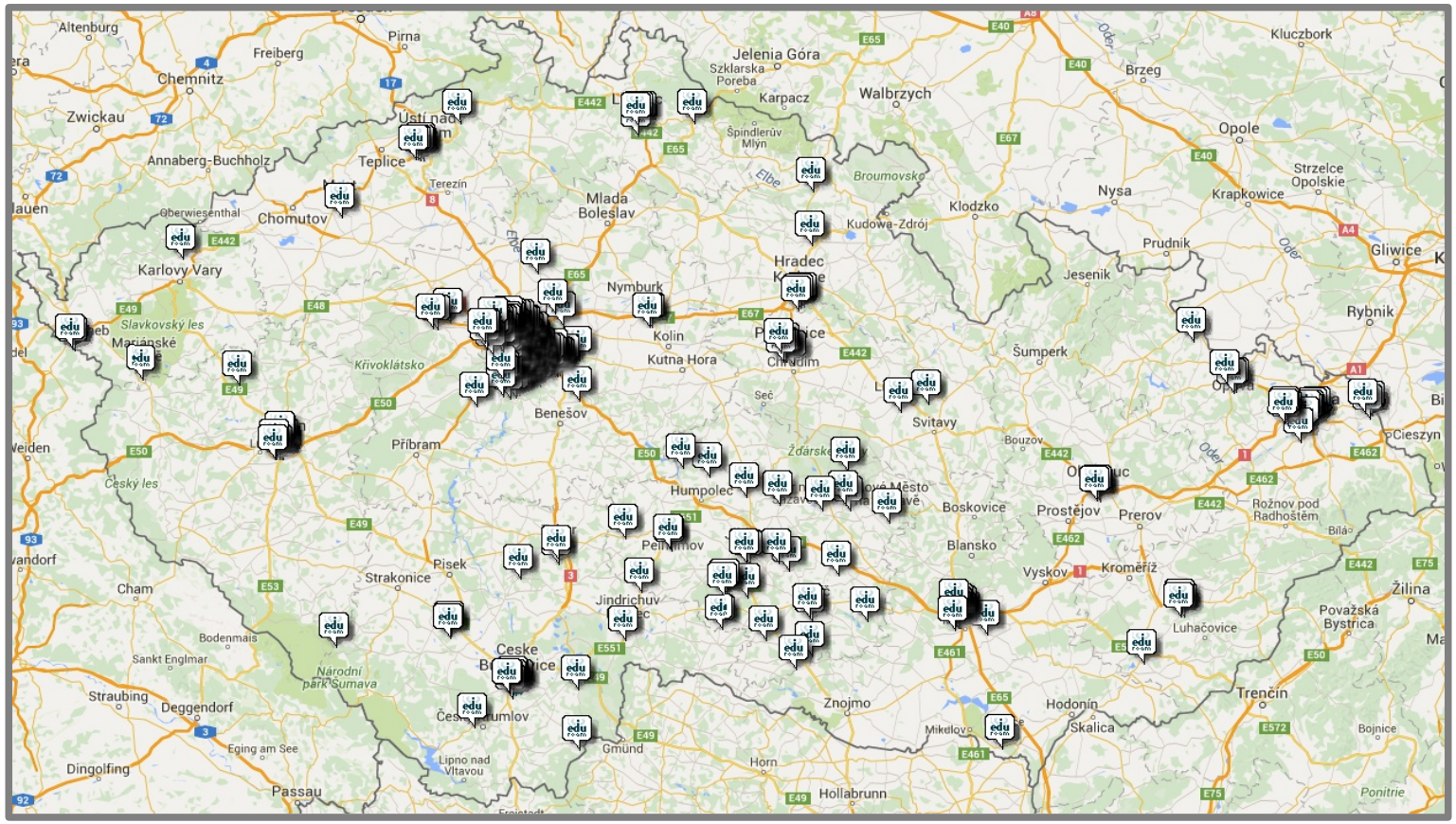
Správa identit PKI & AAI

- **eduID.cz - Česká akademická federace identit**
  - **Jedno uživatelské jméno a heslo pro přístup k řadě síťových služeb** *(v multi-institucionálním prostoru)*
  - Poskytovatelé služeb z národní komunity i mezinárodní
  - Součást mezinárodní interfederace eduGAIN
- **Certifikáty pro uživatele a servery**
  - Důvěryhodný server
  - Důvěryhodná identita uživatele
- **Jednotný systém správy účtů v e-Infrastruktuře**
  - Některé služby odebírané na individuální bázi
  - Strukturování uživatelské komunity
  - Řízený přístup ke zdrojům



Správa identit PKI & AAI

- **eduroam -** „služba na pomezí“: služba z oblasti ověření uživatelů, z pohledu koncového uživatele síťová služba **- roaming uživatelů v hostitelské síti**
  - Síťovou infrastrukturu zajišťuje hostitelská síť; síťová infrastruktura je opřena o autentizační infrastrukturu (technicky RADIUS server hostitelské organizace zapojený do národní hierarchie)



Další služby

- **Monitorování kvalitativních charakteristik sítě**
  - Propustnost, zpoždění, jitter, ztrátovost apod.
  - Pro uživatele náročných aplikací, správce sítí apod.
- **Časové služby**
  - Časová synchronizace (NTP servery – Stratum 1)
  - Časová razítka (Time-Stamp Authority)
- **Technické konzultace**
  - Ve všech odborných oblastech

Základní kontakt

1996–2016 CESNET

https://www.cesnet.cz/sluzby/

sluzby@cesnet.cz

Díky za trpělivost a pozornost...

???