Tomáš Čejka
cejkat@cesnet.cz

Monitorování sítě pomocí flow

case studies

LinuxDays 2017

Úvod

Přehled použitých „pojmů“ I

- **Flow record** / „záznam o toku“
  Agregovaná informace o jednosměrně přenesených datech, tok je identifikován adresami, porty, protokolem, časem
- **Flow exporter** / Monitoring probe / „exportér toků“
  HW/SW zařízení, parsuje pakety, počítá a exportuje flow data
- **Flow collector** / „kolektor“
  přijímá flow data z exportérů, která ukládá a zpracovává (např. IDS)
- Intrusion Detection System (**IDS**)
  systém pro detekci škodlivého provozu / „anomálií“
- **Warden**
  systém pro sdílení informací o detekovaných bezpečnostních událostech mezi členy komunity

Přehled použitých „pojmů“ II

- Network Entity Reputation Database (**NERD**)
  systém pro analýzu detekovaných událostí, sbírání informací o entitách a výpočet „reputačního skóre“

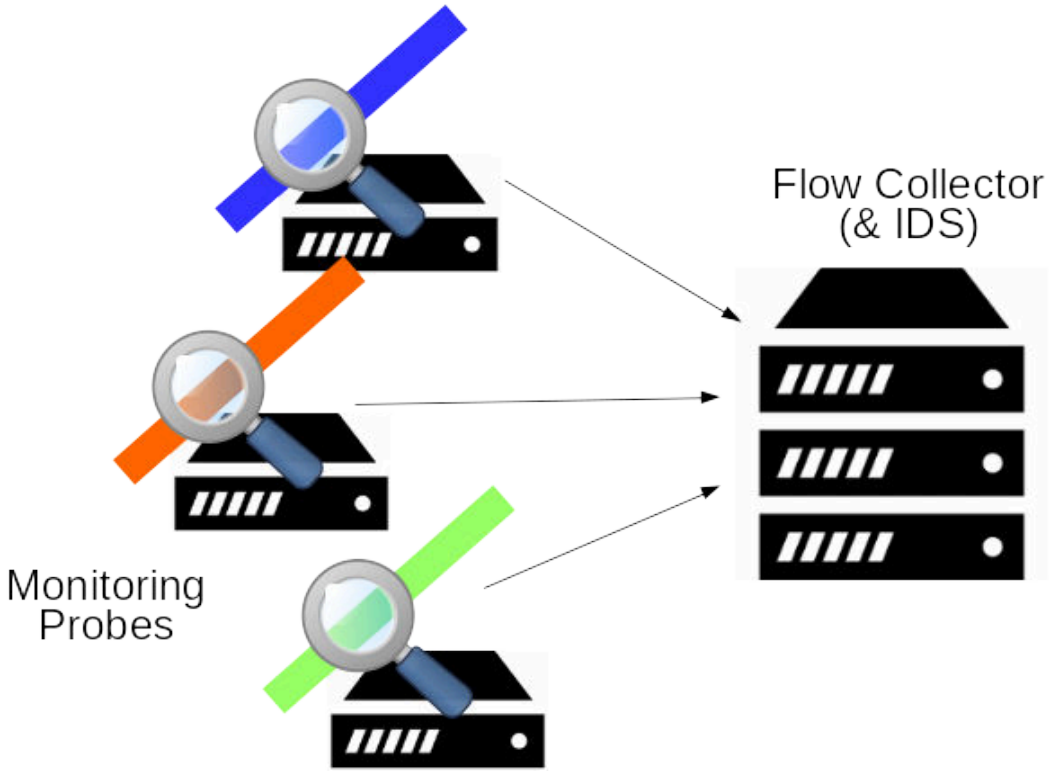
All-in-One: STaaS

Security Tools as a Service (STaaS)

- https://github.com/CESNET/STaaS
- Virtuální stroj / možnost instalace na fyzický stroj
- **Sada nástrojů:**
  - Flow exporter (flow_meter, po instalaci vypnutý)
  - Flow collector (IPFIXcol, primární zdroj dat, ukládání flow dat)
  - „stream-wise“ IDS (NEMEA)
  - Warden klient
  - Nagios (NRPE pluginy)
  - Munin
  - GUI pro zobrazení/vyhledávání flow dat (SCGui)
  - GUI pro zobrazení lokálně detekovaných událostí

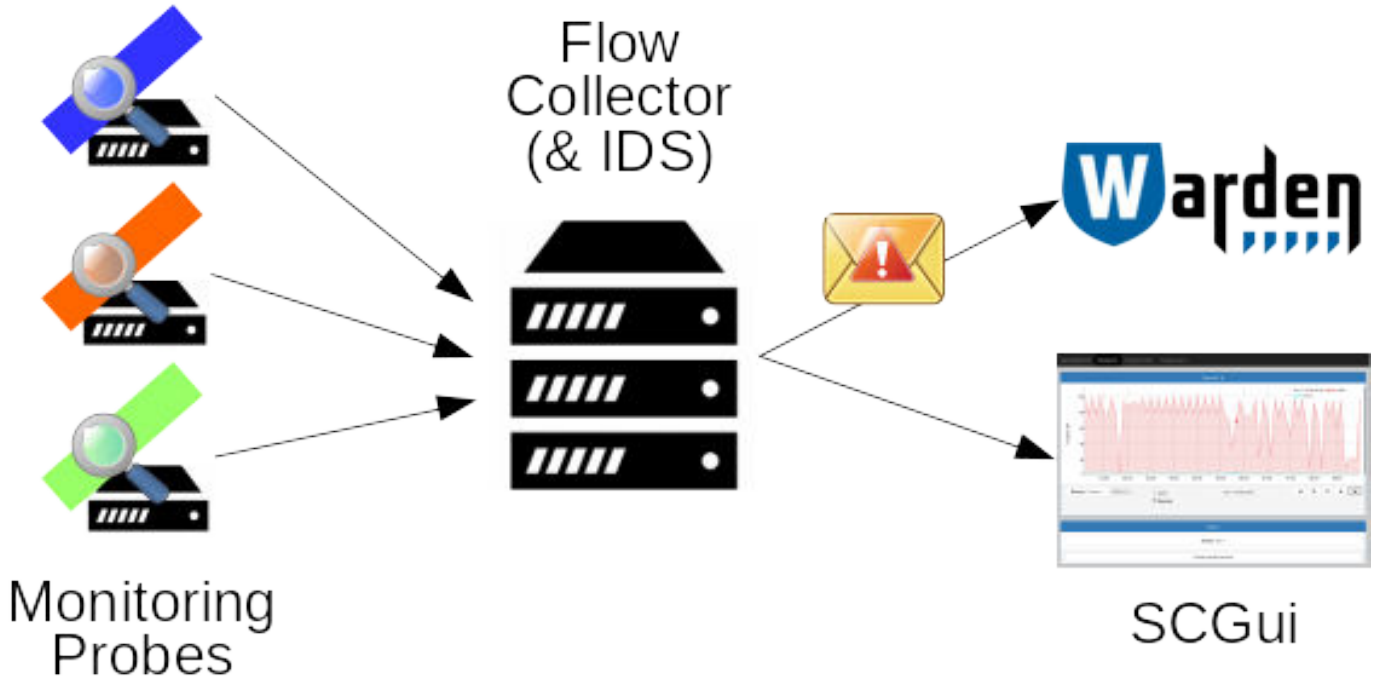
Základní použití

Jeden či více exportérů, kolektor

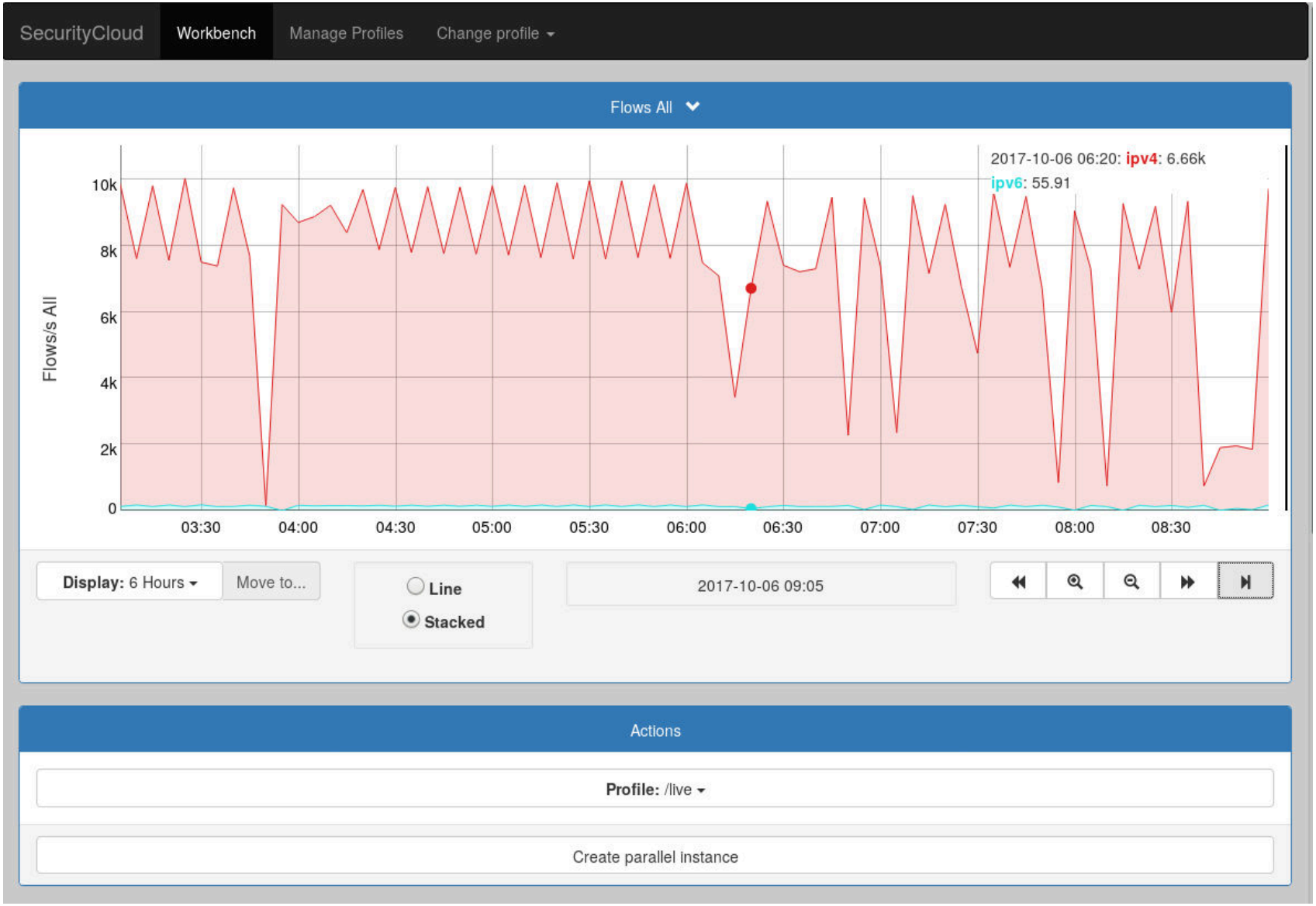


Ukládání flow dat + odesílání alertů

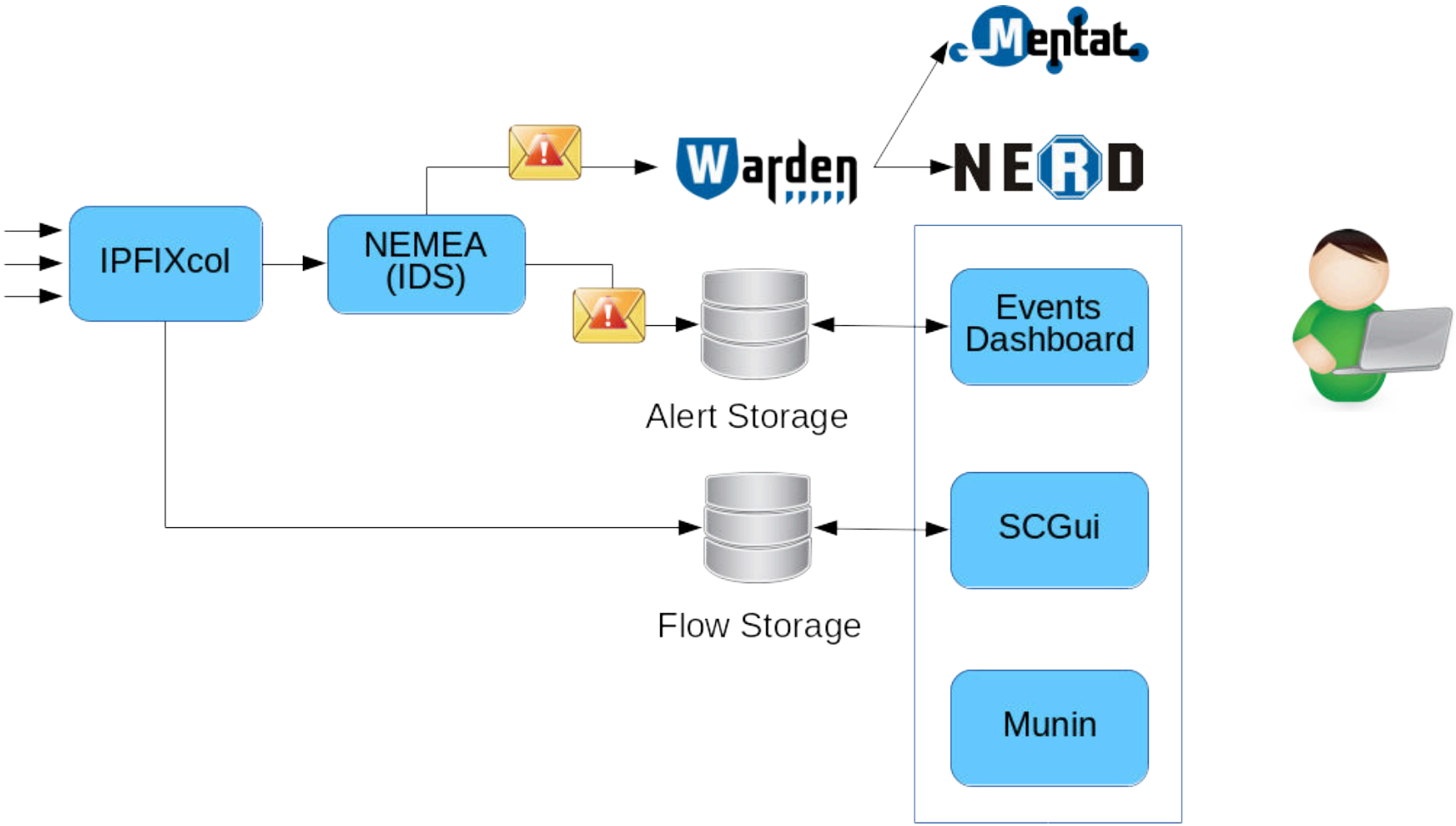
- Prohlížení a vyhledávání flow dat pomocí SCGui místo dříve používaného `nfsen`
- Detekované události je možné odesílat do Wardenu



SecurityCloud GUI (SCGui)

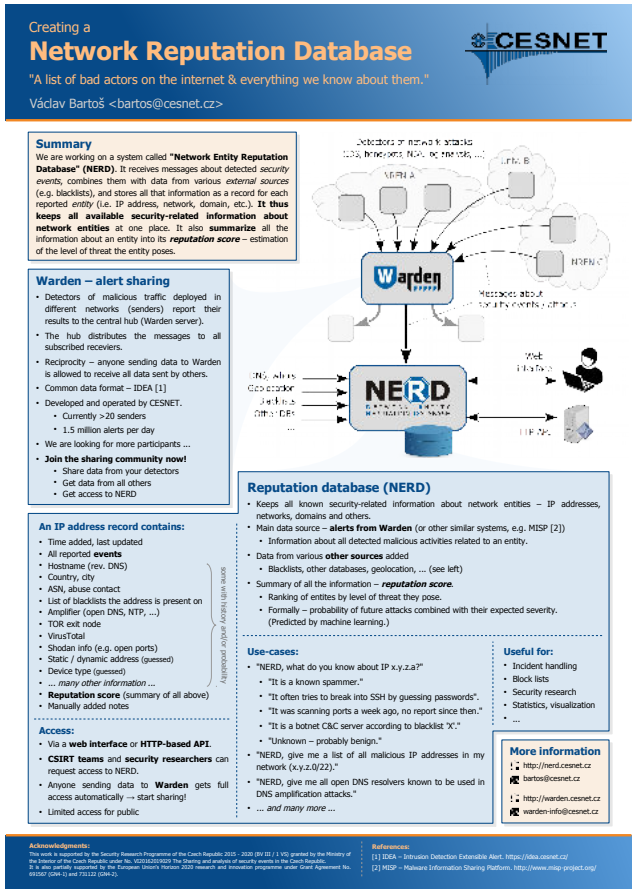


Kolektor trochu podrobněji



Network Entity Reputation Database (NERD)

- http://nerd.cesnet.cz/
- http://nerd.cesnet.cz/tnc16-poster.pdf



Jak to rozjet — evoluce

1. Sestavení ze zdrojových kódů
2. RPM balíky
3. Vagrant / Packer
4. Ansible

Ansible: Jak nainstalovat stroje

- Základní použití je popsáno v README.md
- Ansible playbook: https://github.com/CESNET/STaaS

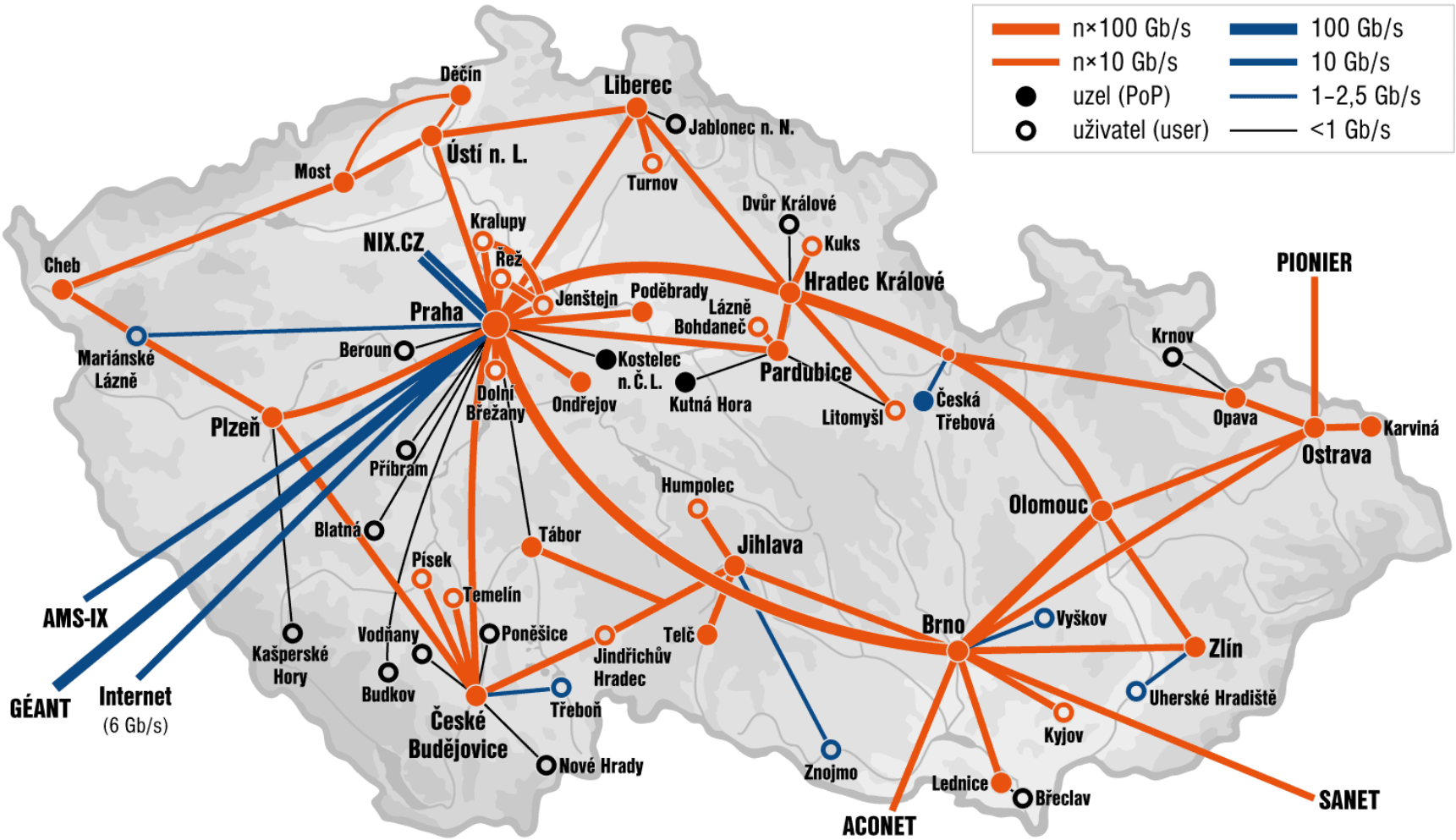
```
ansible-playbook -i inventory/hosts  site.yml \
   --tags install
```

Jak vytvořit svou upravenou instanci stroje

- Lze vyjít z ukázky *staas-vagrant*
- Je potřeba připravit nastavení proměnných pro stroj (`host_vars`)
- Možnost upravit inventář — (konfigurační) soubory, které se kopírují na stroj

CESNET2

Infrastruktura CESNET2



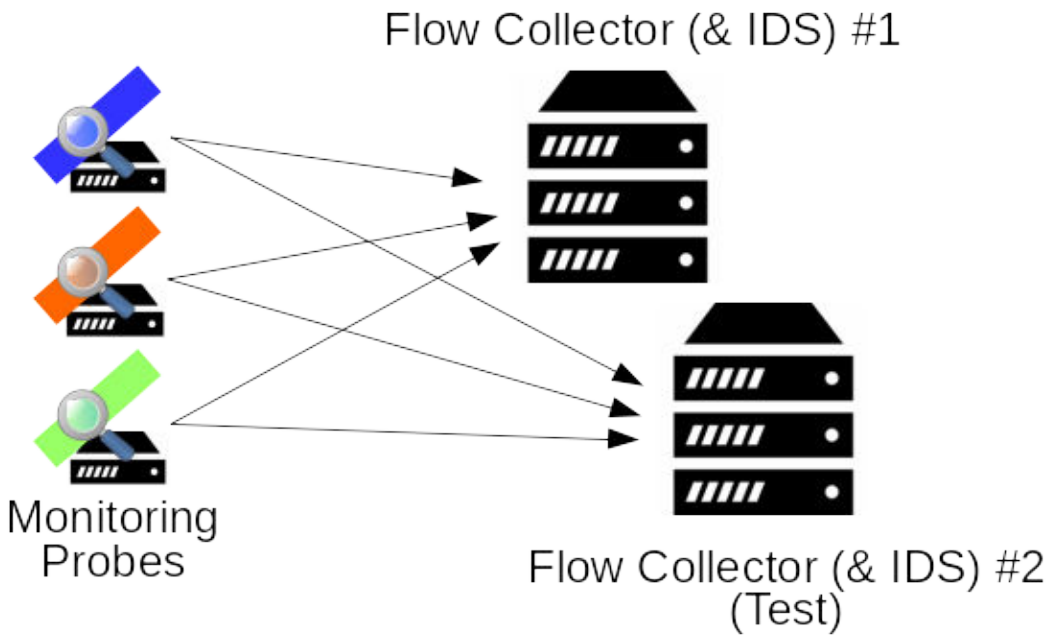
Infrastruktura CESNET2 — hraniční linky

- 13 hraničních linek, do 7 sítí/peeringu (duplikované linky)
- 10 Gb/s a 100 Gb/s linky
- 6 měřících bodů, většina v režimu 10x 10 Gb/s
- 7 COMBO karet (linka GÉANT: 2 karty v serveru)
- cca 12 testovacích měřících bodů

http://netreport.cesnet.cz/netreport/

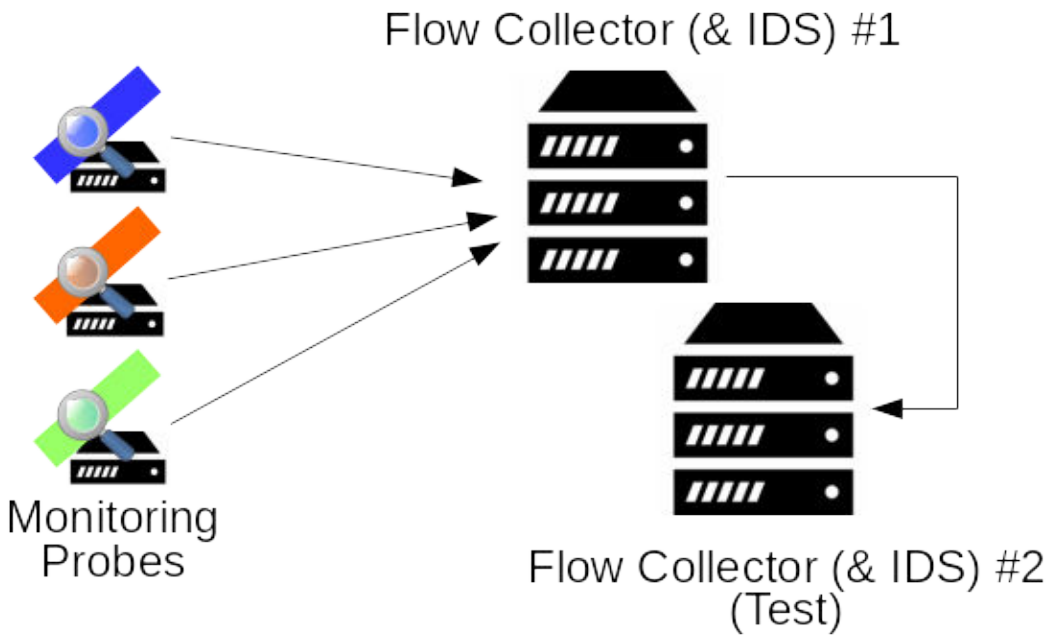
Přeposílání dat na exportérech (CESNET)

- Přeposílání na testovací kolektor



Přeposílání dat na kolektoru (CESNET)

- Přeposílání na testovací kolektor pomocí IPFIXcol

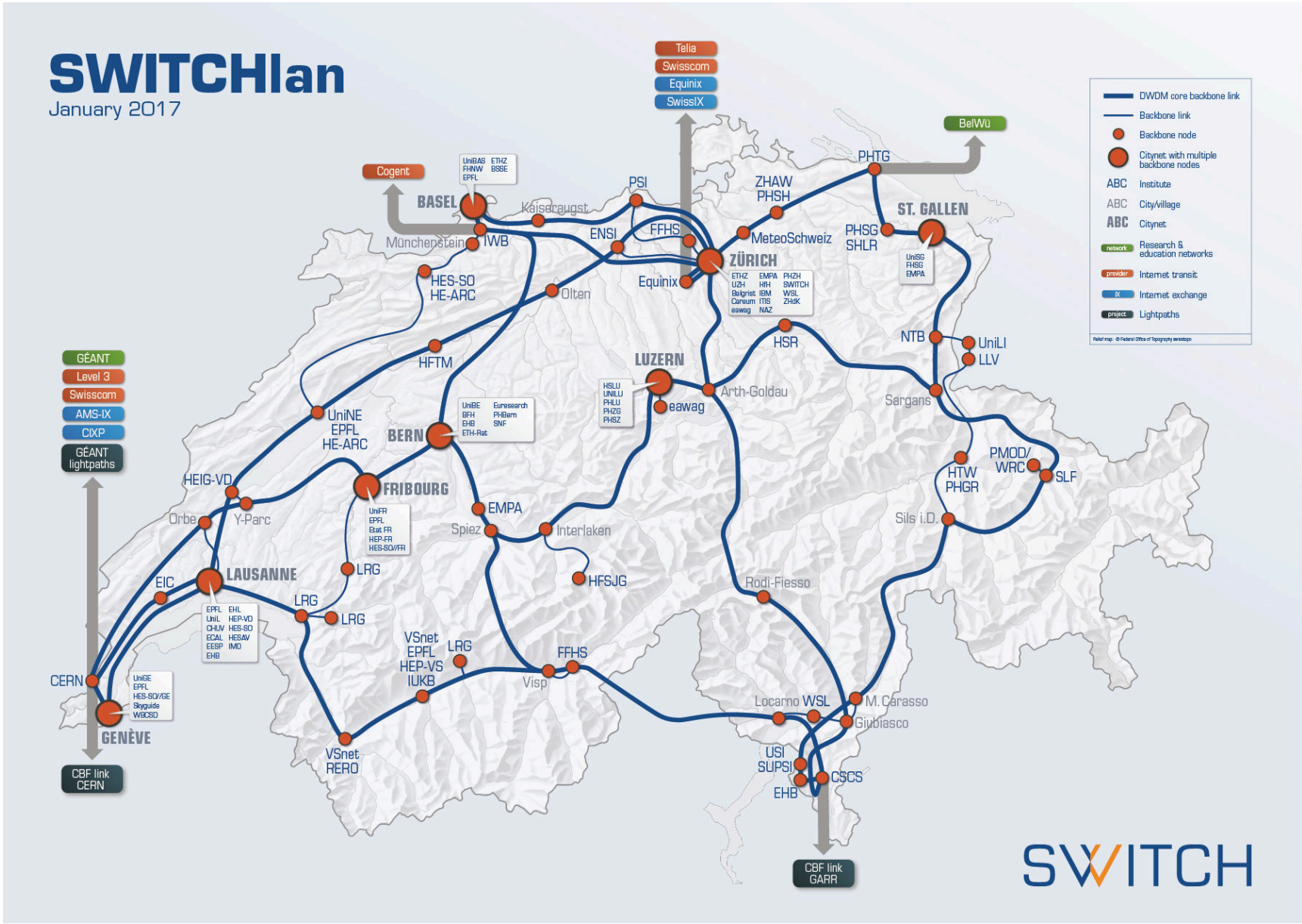


CESNET: jaké stroje používáme (mj.)

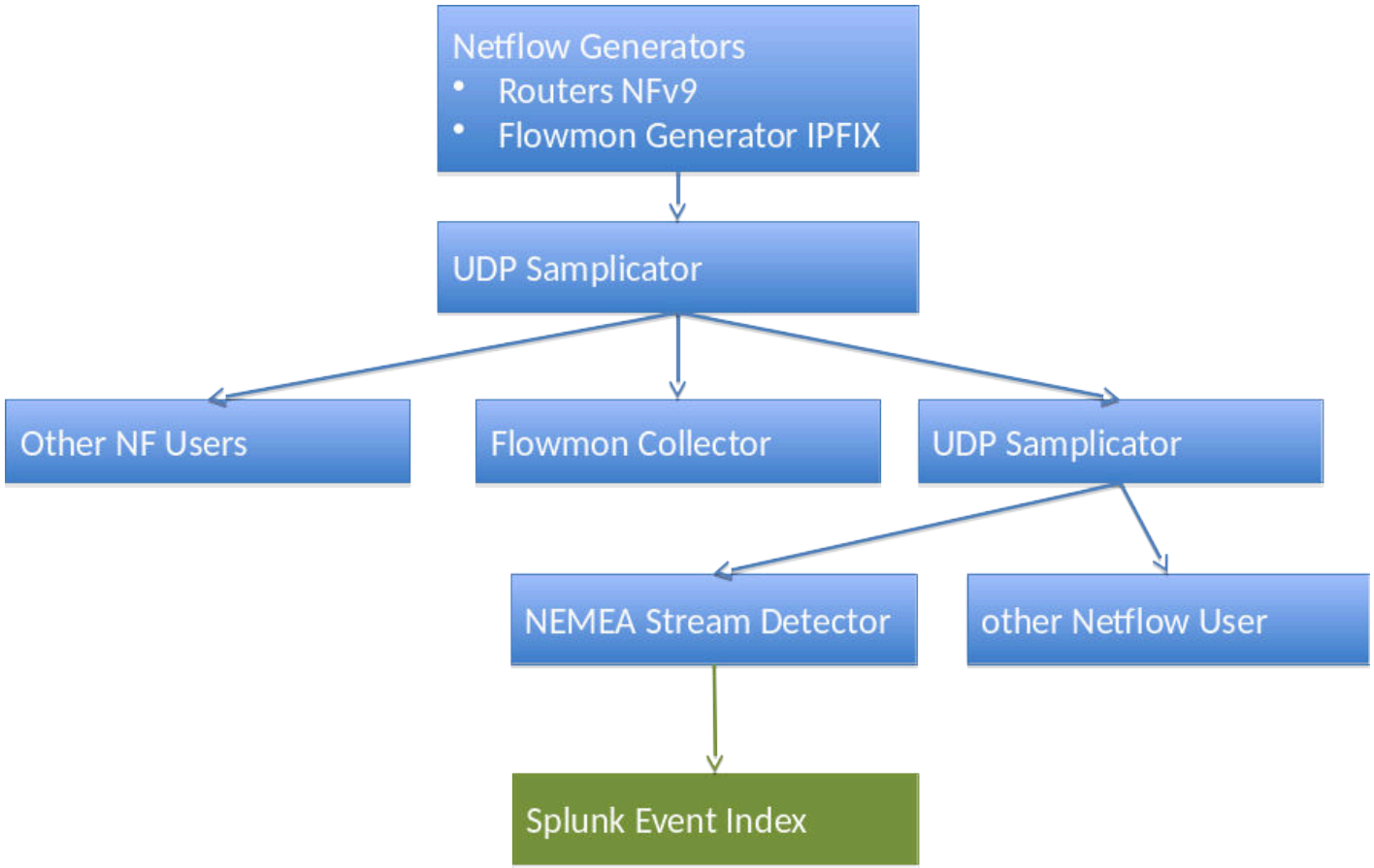
- staas-demo
- collector
- collector-test
- staas-monitor (dohled, nagios)

SWITCH

Infrastruktura SWITCH (akademická síť ve Švýcarsku)



SWITCH

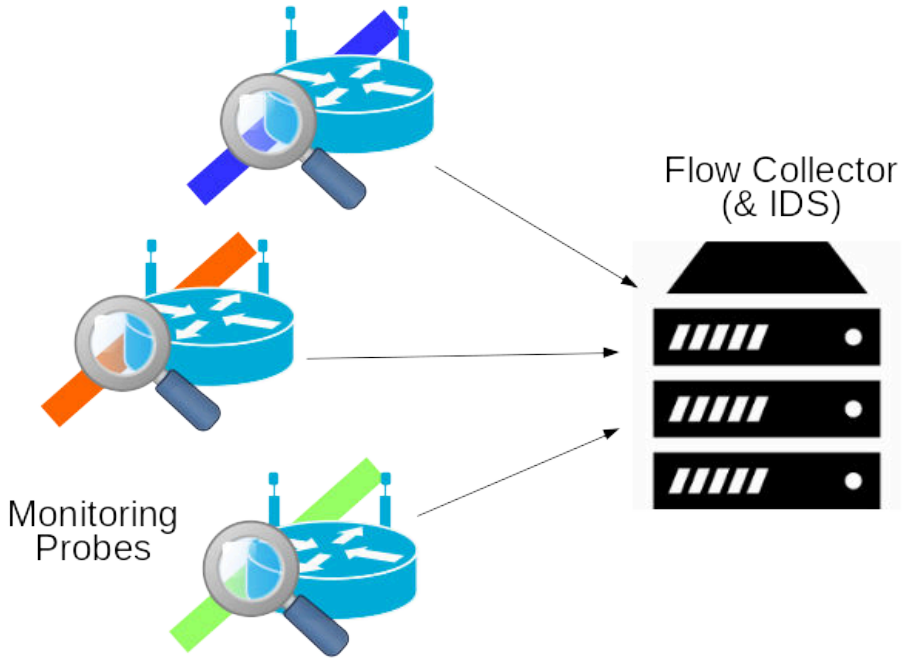


- Provoz zároveň vedle Flowmon kolektoru
- IPFIXcol + NEMEA
- Události se ukládají do Splunk

Moje kancelář

flow_meter: Export z PC nebo OpenWrt směrovače

- flow_meter (zmíněný na LD2016)
- Flow export ze SOHO routerů v IPFIX formátu (https://github.com/CESNET/NEMEA-OpenWrt)
- Nasazeno u mě v kanceláři :-)
- Testováno na:
  - TP-Link WRT1043ND, TP-Link Archer C7, NEXX, CZ.NIC Turris, CZ.NIC Turris Omnia



Další použití flow_meter exportéru

- samostatná sonda + analyzátor, možnost ukládání/zpracovávání provozu přímo na sondě
- možný zdroj informací pro PassiveDNS
- export flow včetně MAC
- export flow včetně L7 rozšíření

Téměř konec prezentace

Pozvánky

1. Stánek CESNET — dema:
   - *L0 SDN a železniční doprava*
   - *Flexibilní zpracování paketů rychlostí 100 Gb/s*
2. Stánek Bastlíři SH
   - *Indoor LoRaWAN gateway* (s podporou CESNET)
3. Měsíc kybernetické bezpečnosti (`http://mkb.cesnet.cz`)
   - Hacking soutěž „The Catch“ (8. 10. – 5. 11. 2017)
   - Seminář Security Fest (31. 10. 2017, Masarykova kolej ČVUT)

Kontakty

E-Mail: cejkat@cesnet.cz
Mailinglist: nemea@cesnet.cz
Přihlášení:
https://random.cesnet.cz/mailman/listinfo/nemea
Web: http://nemea.liberouter.org
Git: https://github.com/CESNET/NEMEA
Twitter: @tomcejka, @NEMEA_System