



Tomáš Čejka

cejkat@cesnet.cz

Monitorování sítě pomocí flow

case studies

Úvod

Přehled použitých „pojmu“ I

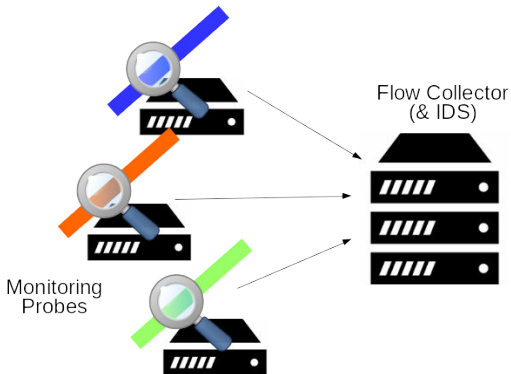
- **Flow record** / „záznam o toku“
Agregovaná informace o jednosměrně přenesených datech, tok je identifikován adresami, porty, protokolem, časem
- **Flow exporter** / Monitoring probe / „exportér toků“
HW/SW zařízení, parsuje pakety, počítá a exportuje flow data
- **Flow collector** / „kolektor“
přijímá 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

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

Security Tools as a Service (STaaS)

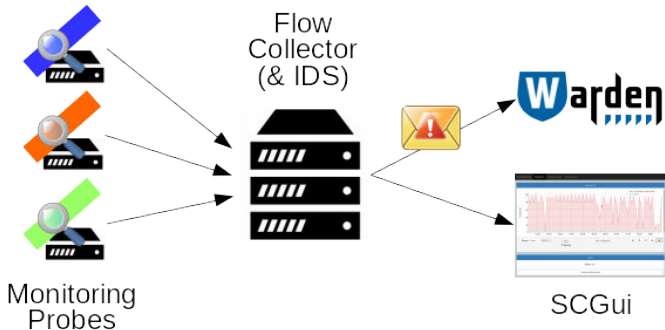
- <https://github.com/CESNET/STaaS>
- Virtuální stroj / možnost instalace na fyzický stroj
- **Sada nástrojů:**
 - Flow exporter ([flow_meter](#), po instalaci vypnutý)
 - Flow collector ([IPFIXcol](#), primární zdroj dat, ukládání flow dat)
 - „stream-wise“ IDS ([NEMEA](#))
 - Warden klient
 - Nagios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

Jeden či více exportérů, kolektor



Ukládání flow dat + odesílání alertů

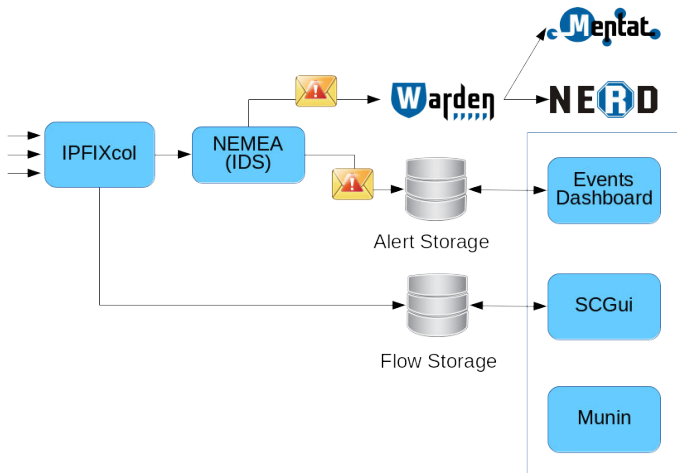
- Prohlížení a vyhledávání flow dat pomocí **SCGui** místo dříve používaného **nfsen**
- Detekované události je možné odesílat do Wardenu



SecurityCloud GUI (SCGui)



Kolektor trochu podrobněji



Network Entity Reputation Database (NERD)

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

Creating a
Network Reputation Database
"A list of bad actors on the internet & everything we know about them."
Václav Bartoň <barton@cesnet.cz>

Summary
We are working on a system called "Network Entity Reputation Database" (NERD). It receives messages about detected security events, correlates them with data from various external sources (e.g. blacklists), and stores all that information as a record for each reported entity (i.e. IP address, network, domain, etc.). **In this paper, all available security-related information about network entities of our choice. It also summarizes all the information about an entity into a reputation score** – indication of the level of threat the entity poses.

Warden – alert sharing
• Definition of network entity deployed in different networks (domains) report their results to the central hub (Warden server).
• The hub distributes the messages to all subscribed networks.
• Recipient – anyone sending data to Warden is allowed to receive all data sent by others.
• Common data format – JSON.
• Developed and operated by CESNET.
• Currently 100+ members.
• 1.5 million alerts per day.
• We are looking for more participants...
• Join the sharing community now!
• Share data from your detectors
• Get data from all others
• Get access to NERD

An IP address record contains:
• Time added, last updated
• All specific events
• Hashes (see DNS)
• Country, city
• ASN, abuse contact
• List of blacklists the address is present on
• Aspiration (open DNS, HTTP, ...)
• DNS mail results
• Whois data
• Warden info (e.g. open ports)
• WHOIS / dynamic, domain (parent)
• Domain type (parent)
• ... many other informations...
• Reputation score (summary of all above)
• Manually added notes

Access:
• Via a web interface or HTTP-based API.
• CERT teams and security researchers can request access to NERD.
• Anyone sending data to Warden gets full access automatically – alert sharing.
• Limited access for public.

Reputation database (NERD)
• Range of known security-related information about network entities – IP addresses, networks, domains and others.
• Main data source – alerts from Warden (or other similar systems, e.g. MISP [2]).
• Information about all detected malicious activities related to an entity.
• Data from various other sources added:
• Blacklists, other databases, geolocation, ... (see [4])
• Summary of all the information – reputation score.
• Ranking of entities by level of threat they pose.
• Normally – probability of future attacks combined with their expected severity.
(Predicted by machine learning).

Use-cases
• "NERD, what do you know about IP x.y.z?"
• "It is a known spammer."
• "It often tries to break into SSH by guessing passwords."
• "It sends scanning ports a week ago, no report since then."
• "It is a known DNS server according to blacklist X."
• "Telecom – probably benign."
• "NERD, give me a list of all malicious IP addresses in my network for a 24h?"
• "NERD, give me all open DNS resolvers known to be used as DNS amplification attacks."
• ... and many more...

Useful for:
• Incident handling
• Block lists
• Security research
• Forensics, visualization
• ...

More information
• Web interface
• REST API
• <http://nerd.cesnet.cz/>
• barton@cesnet.cz

Acknowledgements
• CESNET, Technical Services Department (TSD) (Data provided by TSD) (NERD infrastructure, Security Network, Web/Reporting platform)

- 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>

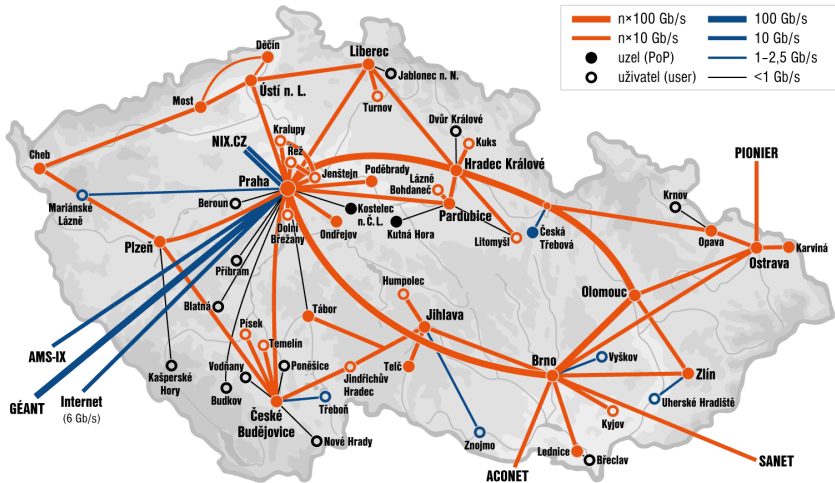
```
ansible-playbook -i inventory/hosts site.yml \
    --tags install
```

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

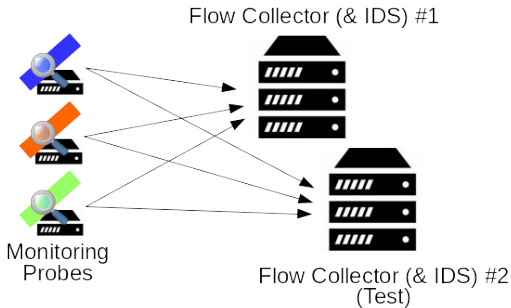


- 13 hraničních linek, do 7 sítí/peeringu (duplikované linky)
- 10 Gb/s a 100 Gb/s linky
- 6 měřících bodů, většina v režimu 10x 10 Gb/s
- 7 COMBO karet (linka GÉANT: 2 karty v serveru)
- cca 12 testovacích měřících bodů

<http://netreport.cesnet.cz/netreport/>

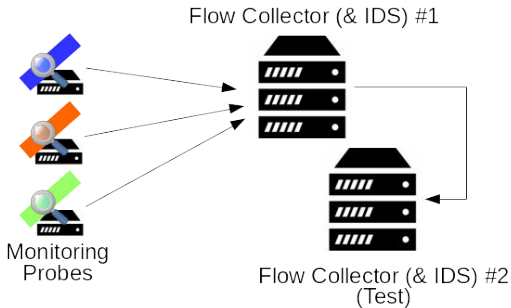
Přeposílání dat na exportérech (CESNET)

- Přeposílání na testovací kolektor



Přeposílání dat na kolektoru (CESNET)

- Přeposílání na testovací kolektor pomocí IPFIXcol



CESNET: jaké stroje používáme (mj.)

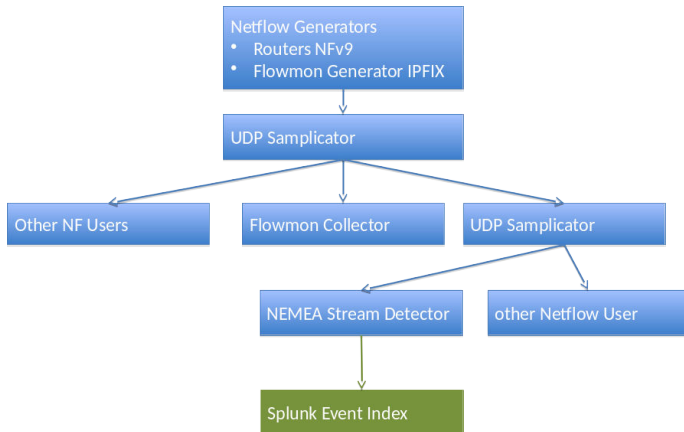
- [staas-demo](#)
- collector
- collector-test
- staas-monitor (dohled, nagios)

SWITCH

January 2017



SWITCH

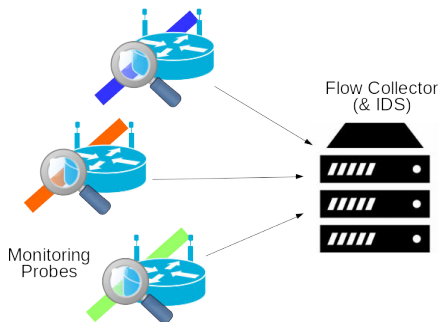


- Provoz zároveň vedle Flowmon kolektoru
- IPFIXcol + NEMEA
- Události se ukládají do Splunk

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

- ❶ Stánek CESNET — dema:
 - *L0 SDN a železniční doprava*
 - *Flexibilní zpracování paketů rychlostí 100 Gb/s*
- ❷ Stánek Bastlíři SH
 - *Indoor LoRaWAN gateway* (s podporou CESNET)
- ❸ 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](#)

