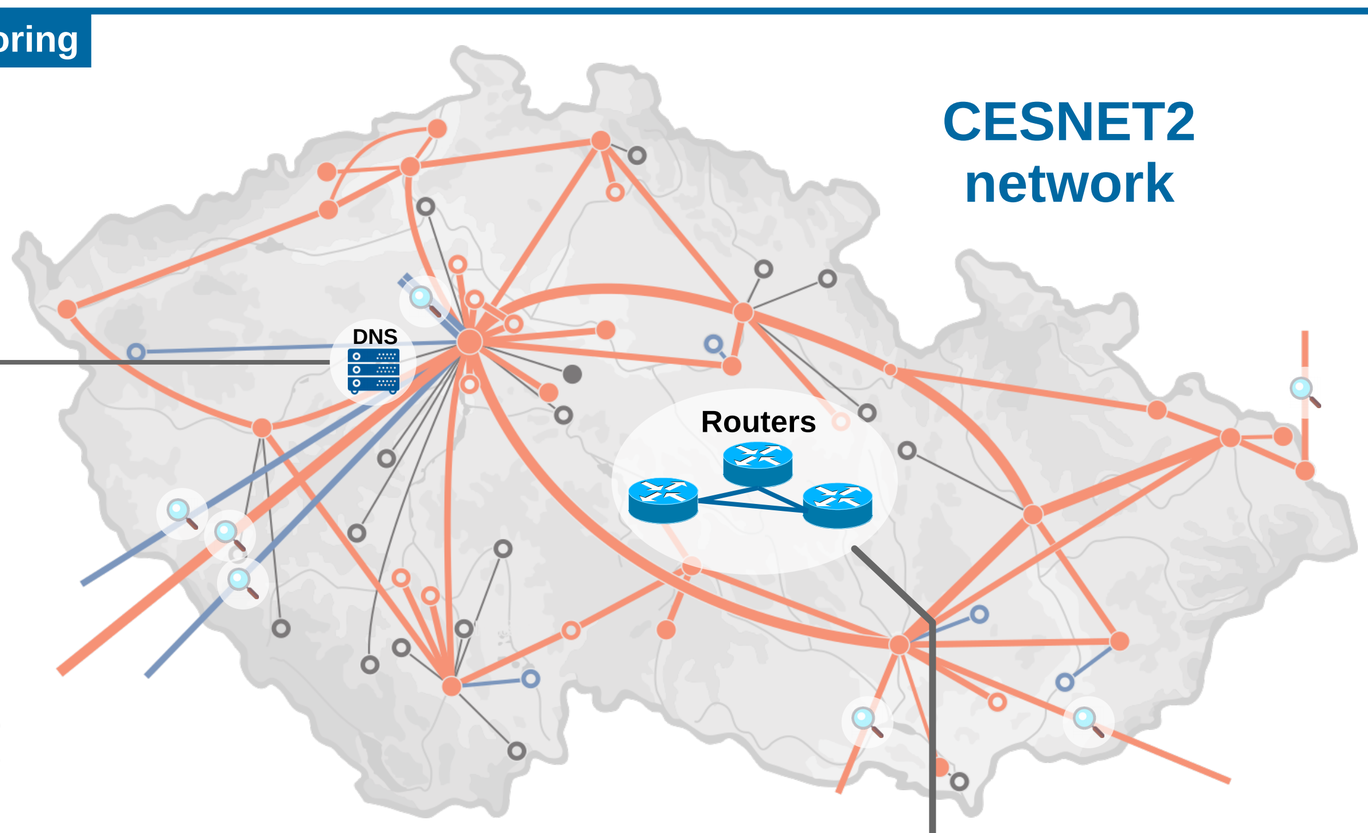
CESNET Monitoring & Security Infrastructure

Václav Bartoš, Tomáš Čejka *{bartos,cejka}@cesnet.cz*

Monitoring



CESNET2 network

DNS data

Monitoring probes

- Deployed on all perimeter links (complete visibility of in/out traffic)
- Based on our in-house developed 100GE network cards with FPGA for hardware acceleration.

L7-extended flow monitoring
- Full speed (up to 100Gbps) flow monitoring without sampling.
- Parsing of selected L7 protocols
- IPFIX output

Time Machine

On-demand full packet capture. Circular buffers allow to capture traffic transferred several minutes *before* the capture request was issued. Used to capture samples of suspicious traffic for further analysis.

IPFIX

Suricata IDS

Monitoring one of our links to the Internet

NetFlow

Honeypots

Various honeypots, e.g. **Cowrie, Dionaea, LaBrea**, in CESNET's own network as well as in university networks.

New project – **Honeypot as a Service** (HaaS)
- Preconfigured VMs with various honeypots
- Remote maintenance and updates
- Reports to Warden

https://haas.cesnet.cz/

Protection

Antispam gateway

Anti-spam and anti-virus solution deployed on our mail servers. Also provided as a service for end networks.

Reports spamming IP addresses to Warden.

Rate-limiting of some protocols

Permanent rate-limiting (traffic policing) configured on the edge routers to mitigate some common amplification attacks.
- NTP, SNMP, SSDP, CharGen, ...
- These protocols never generate large amounts of traffic normally; dropping some legitimate packets is not critical.
- Not possible for DNS

DDoS Protector

100Gbps DDoS scrubbing centre based on our FPGA-accelerated network card. Close HW/SW cooperation:
- HW computes traffic statistics
- SW decides what traffic to block (several algorithms for different attack types)
- HW performs filtering

In case of attack, all traffic to target is rerouted via this device, cleaned traffic is sent back to network.

RTBH

Unwanted traffic can be routed to the backbone. Filtering is triggered by end network admins via BGP or by calling to the service desk.

Data storage & analysis

NEMEA (IDS)

Modular IDS system for real-time analysis of flow data.
- Supports IPFIX data with L7 headers
- Real-time stream-wise processing
- Detection of various threats, e.g. port scans, bruteforce, DDoS, DNS anomalies, SIP attacks, …
- Ad-hoc traffic filtering

https://nemea.liberouter.org/

FTAS

NetFlow collector and analyzer.
- Designed specifically for large networks
- Multitenancy, knowledge of network and organizational hierarchy – accessible to local admins. at universities, they can see only their data.
- Anomaly detection, reporting.
- Processes data from core routers (visibility of both external and internal communication).

Passive DNS

Keeps history of DNS resolutions made by our main DNS servers.
Plan: also include DNS data observed by monitoring probes.

SecurityCloud

Scalable flow data collector. Fast queries thanks to distributed data storage. Allows data search via a modern GUI.

NOC

CERTS

Service desk

End-network admins

Alert processing

Alerts

Alerts

Warden

Simple alert sharing system
- Detectors deployed in different networks (senders) report their results to the central hub (Warden server).
- The hub distributes the messages to all subscribed receivers.
- Reciprocity – anyone sending data to Warden is allowed to receive all data sent by others.
- Common data format – IDEA (https://idea.cesnet.cz/)
- Open-source server and several clients

Main instance operated by CESNET, you can join our sharing community.

Note: alerts = low-level security events; results of detection from honeypots, flow analysis systems, IDS, log analyzers, etc.

https://warden.cesnet.cz/

Alerts

Mentat (SIEM)

Distributed modular SIEM.
- Stores and processes IDEA messages from Warden
- Allows to search alerts & reports
- Sends email report to a local admin if a malicious host in our constituency is found (or in other network who asked us to send reports)

https://mentat.cesnet.cz/

Alerts

NERD

Advanced IP reputation database
- A record for each known malicious IP address.
- Information about previous detections
- Information from external sources (DNS, whois, blacklists, geolocation, BGP ranking, …)
- Ranking by “reputation score”

https://nerd.cesnet.cz/

Sharing with other NRENs
(project PROTECTIVE, see another poster)

Other alert sources
(sensors at other networks, IntelMQ, shadowserver, ...)