



**cesnet**  
"...."

**hSOC, enem (ExaFS)**

**Petr Adamec**  
**CESNET**

---

**26. listopadu 2020**



## ■ VRF

- Virtual routing and forwarding

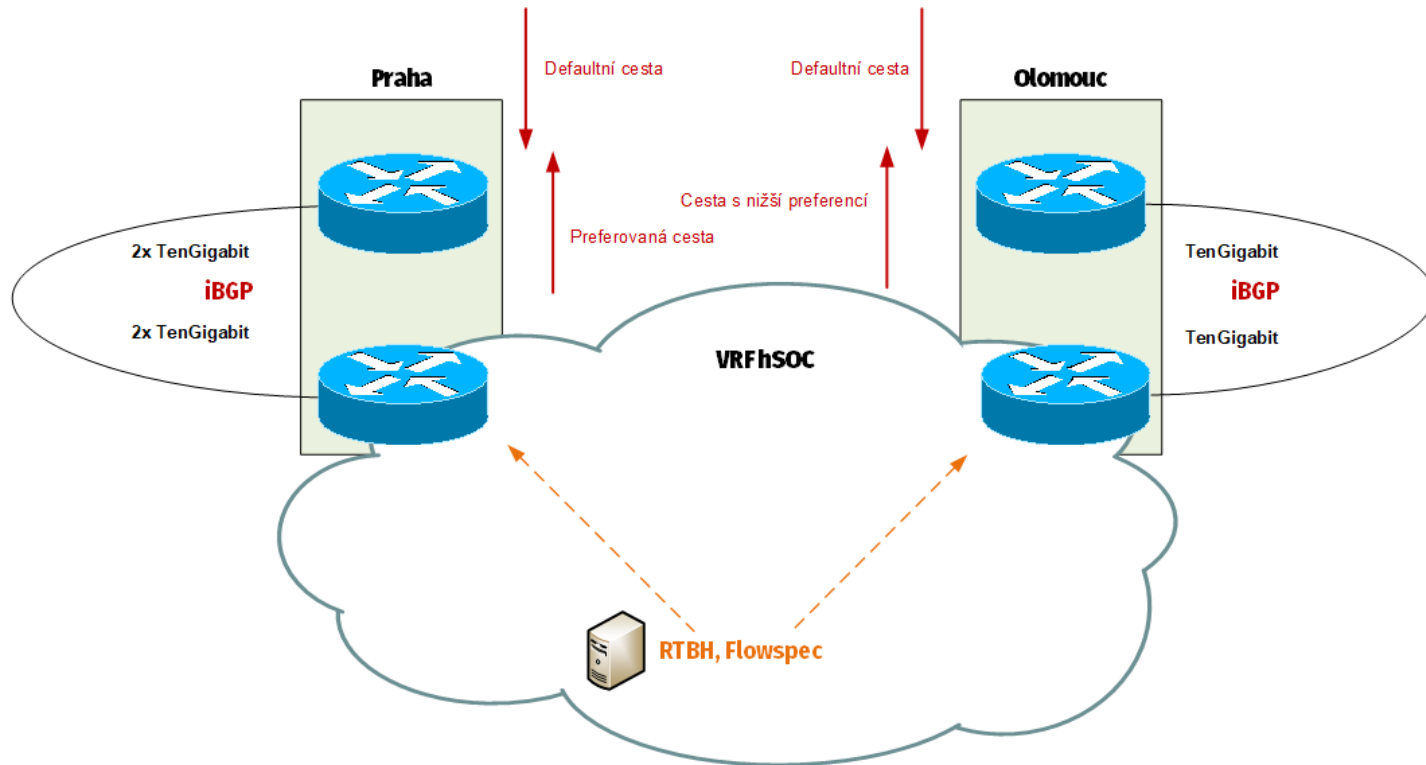
## ■ RTBH

- Remotely Triggered Black Hole (Remote Black Hole Triggering)

## ■ BGP Flowspec

## ■ BCP38 (RFC2827)

- Best Current Practice - Network Ingress Filtering



## ■ Co vlastně chráníme?

## ■ Existující ochrana na perimetru sítě CESNET

- **IN** – amplifikační útoky
- **OUT** – amplifikační útoky (omezený set)

## ■ Ochrana na perimetru klientů

- **BCP38**, filtrování prefixů aj.
- Klienti mají většinou vlastní vstupní ACL

## ■ Omezování útoků – klienti

- Nástroj exaFS – umožňuje používat RTBH a BGP Flowspec

IPv4 Rule saved ✕

## Active IPv4 rules

IPv4

IPv6

RTBH

Search...



Active

Expired

All

Source address ▾	Source port ▾	Dest. address ▾	Dest. port ▾	Protocol ▾	Expires ▾	Action ▾	Flags ▾	User ▾	Edit
192.168.1.1 / 32	25			tcp	2020/12/01 16:10	QoS 1 Mbps		[redacted]	<input type="checkbox"/> <span>⏸</span> <span>✕</span> <span>💬</span>



## New IPv4 rule

Source address

Source mask (bits)

Protocol

TCP flag(s)

- SYN
- ACK
- FIN
- URG
- PSH
- RST
- ECE
- CWR
- NS

Destination address

Destination mask (bits)

Source port(s) - ; separated

Destination port(s) - ; separated

Packet length

Action

- QoS 0.1 Mbps
- QoS 0.1 Mbps
- QoS 1 Mbps
- QoS 10 Mbps
- QoS 100 Mbps
- QoS 500 Mbps
- Discard
- Accept
- [redacted]
- QoS 0.05 Mbps
- Accept + community

Expiration date



## New RTBH rule

IPv4 address

IPv4 mask (bits)

Community

IPv6 address

IPv6 mask (bits)

Expiration date



Comments

Save



eNem (ExaFS 0.4.5) [Add IPv4](#) [Add IPv6](#) [Add RTBH](#) [API Key](#) [Admin](#) ▼ Logged in as [redacted], role: [redacted] org: Celý svět

NewKey saved ✕





## Your machines and ApiKeys

Machine address	ApiKey	Action
192.168.100.1	fedf42b4f95 [redacted]	<span>✕</span>

[Add new ApiKey](#)



eNem (ExaFS 0.4.5) Add IPv4 Add IPv6 Add RTBH API Key Admin ▾ Logged in as [redacted] role: [redacted] org: Celý svět

Name	Adress Range	action
Celý svět	0.0.0.0/0 ::/0	 
[redacted]	[redacted]	 



- **exaBGP 4.2.11**
- **Python 3.6.8 (default na RHEL3.7)**
- **MariaDB**
- **Flask + WTFORMS + SQLAlchemy**
- **Uvolněno pod licencí MIT**
- **Dostupné v repozitáři GITu <https://github.com/CESNET/exafs>**
- **Dokumentace API na <https://exafs.docs.apiary.io>**

**cesnet**  
"...."

**A to je konec...**

