cesnet

Potlačení nežádoucího provozu pomocí BGP Flowspec - ExaFS

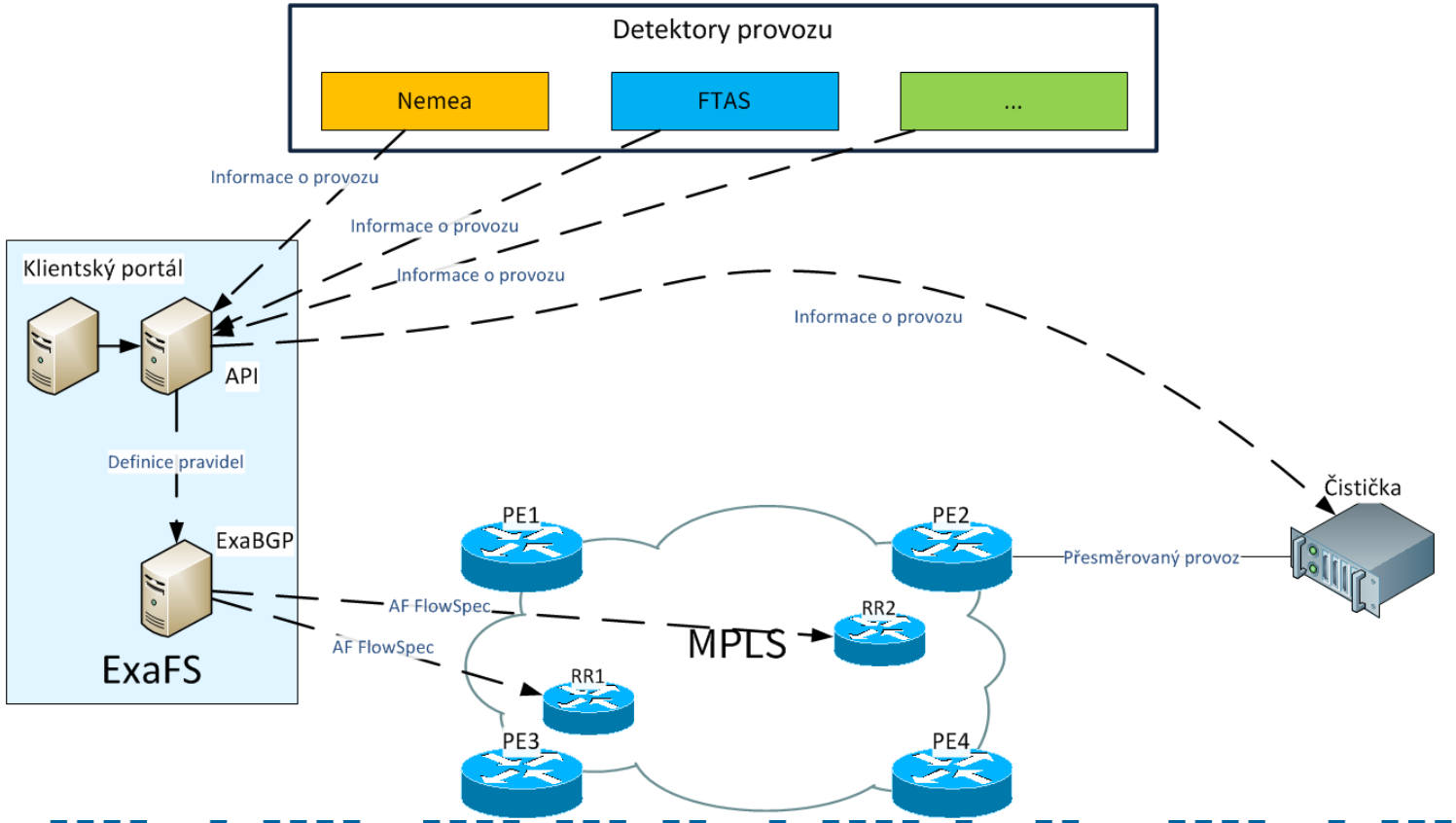
Josef Verich, Petr Adamec, Jiří Vraný a Tomáš Košňar
CESNET

29. května 2019
CSNOG

Motivace

- **Máme FlowSpec (konečně!) a co s ním?**
  - Nabídnout využití pro gramotné správce
  - Nabídnout využití pro řešení incidentů týmu CESNET-CERTS
  - Nabídnout využití pro připojené klienty
- **Jak to udělat? Využití již existujících programů (výsledek hledání - nula)**
  - Napíšeme si vlastní! (Fakt? A to jako kdo?)
- **A jdeme na to! Zadání:**
  - Hierarchická struktura, práva a vůbec všechno (+ několik popsaných papírů a pár desítek hodin diskuzí k tomu)
- **Je to tak jednoduché? Ne – máme už třetí zcela přepsanou verzi ;-)**
  - A vloženo pár měsíců práce…

Návaznost systémů



cesnet

Dashboard

Exafs v 0.2.5 | Add IPv4 | Add IPv6 | Add RTBH | API Key | Logged in as , role: user, org: TU Liberec

User dashboard

Rules IPv4/v6 that you can modify

Source adress	Source port(s)	Destination adress	Dest. port(s)	Protocol(s)	Expires	Action	Flags	User	Action
		[redacted].219 / 32	3702	udp	2019-06-01 10:00:00	Discard		[redacted]	
		[redacted]116 / 32	3702	udp	2019-06-01 10:00:00	Discard		[redacted]	
		[redacted].1 / 32	3702	udp	2019-06-01 10:00:00	Discard		[redacted]	

Rules RTBH

IP adress (v4 or v6)	Community	Expires	User	Action
[redacted]147 / 32	RTBH CESNET only	2019-05-12 13:00:00	[redacted]	

Rules IPv4/v6 that are read-only for you

Source adress	Source port(s)	Destination adress	Dest. port(s)	Protocol(s)	Expires	Action	Flags	User

Seznam organizací

Exafs v 0.2.5 | Add IPv4 | Add IPv6 | Add RTBH | API Key | Admin | Logged in as , role: admin, org: Cesnet, Celý svět

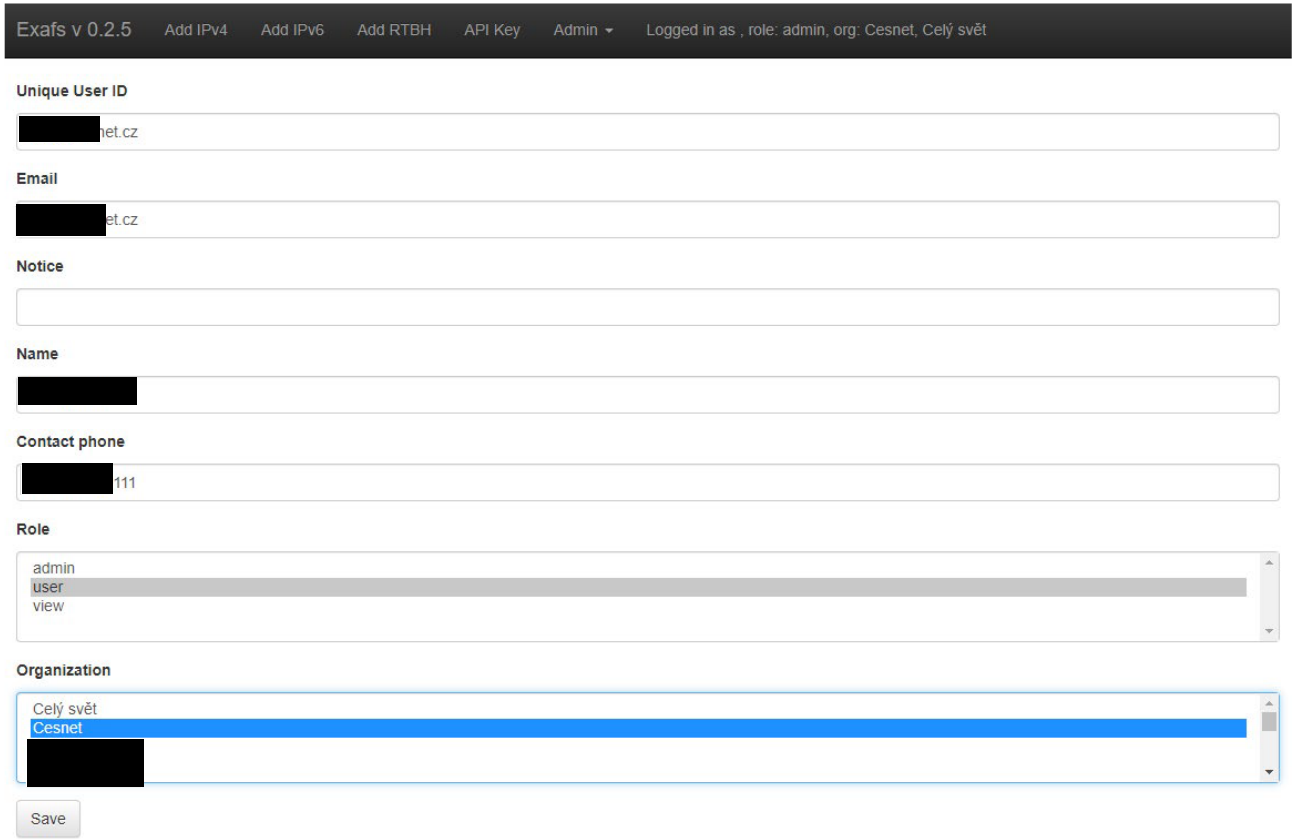
Name	Adress Range	action
TU Liberec	147.230.0.0/16 2001:718:1c01::/48	
Cesnet	147.32.0.0/15 147.228.0.0/14 160.216.0.0/15 146.102.0.0/16 147.251.0.0/16 158.194.0.0/16 158.196.0.0/16 193.84.32.0/20 193.84.160.0/20 193.84.192.0/19 195.113.0.0/16 195.178.64.0/19 78.128.128.0/17 2001:718::/29	

Seznam akcí

Exafs v 0.2.5 | Add IPv4 | Add IPv6 | Add RTBH | API Key | Admin | Logged in as , role: admin, org: Cesnet, Celý svět

Id	Name	Command	Description	Minimum level	action
1	QoS 0.1 Mbps	rate-limit 12800	QoS	user	
2	QoS 1 Mbps	rate-limit 131072	QoS	user	
3	QoS 10 Mbps	rate-limit 1310720	QoS	user	
5	QoS 100 Mbps	rate-limit 13107200	QoS	user	
6	QoS 500 Mbps	rate-limit 65536000	QoS	user	
7	Discard	discard	Discard	user	
8	Accept	accept	Accept	user	
9	Redirect to DDoS Protector	redirect 6[redacted]	Presmerovani na cisticku (RT 6[redacted])	user	
24	Redirect to analyzator	redirect 6[redacted]	Presmerovani na analyzator (RT 6[redacted])	admin	
25	QoS 0.05 Mbps	rate-limit 6400	QoS	user	

Přidání uživatele – správce



Přidání pravidlel

- **Routery NOKIA**
  - Na routerech Nokia - je (momentálně) možné použít pouze kombinaci délka paketu a discard!
- **Opatrně s fragmentovaným provozem!**
  - fragmenty mají zdrojový i cílový port „**0**“

Přidání IPv4 pravidla

Exafs v 0.2.5 | Add IPv4 | Add IPv6 | Add RTBH | API Key | Admin | Logged in as , role: admin, org: Cesnet, Celý svět

New IPv4 rule

Source address

Source mask (bits)

Protocol: UDP

TCP flag(s): SYN, ACK, FIN, URG, PSH, RST, ECE, CWR, NS

Destination address: 147[redacted]

Destination mask (bits): 24

Source port(s) - ; separated

Destination port(s) - ; separated: 3702

Packet length

Action: Discard

Expiration date: 05/15/2019 10:04

Comments: Web Services Dynamic Discovery (WS-Discovery)

Save

Přidání IPv6 pravidla

Exafs v 0.2.5 | Add IPv4 | Add IPv6 | Add RTBH | API Key | Admin | Logged in as , role: admin, org: Cesnet, Celý svět

New IPv6 rule

Source address

Source prefix length (bits)

Next Header: UDP

TCP flag(s): SYN, ACK, FIN, URG, PSH, RST, ECE, CWR, NS

Destination address: 2001:718[redacted]

Destination prefix length (bits): 64

Source port(s) - ; separated

Destination port(s) - ; separated: 3702

Packet length

Action: Discard

Expiration date: 05/15/2019 10:08

Comments: Web Services Dynamic Discovery (WS-Discovery)

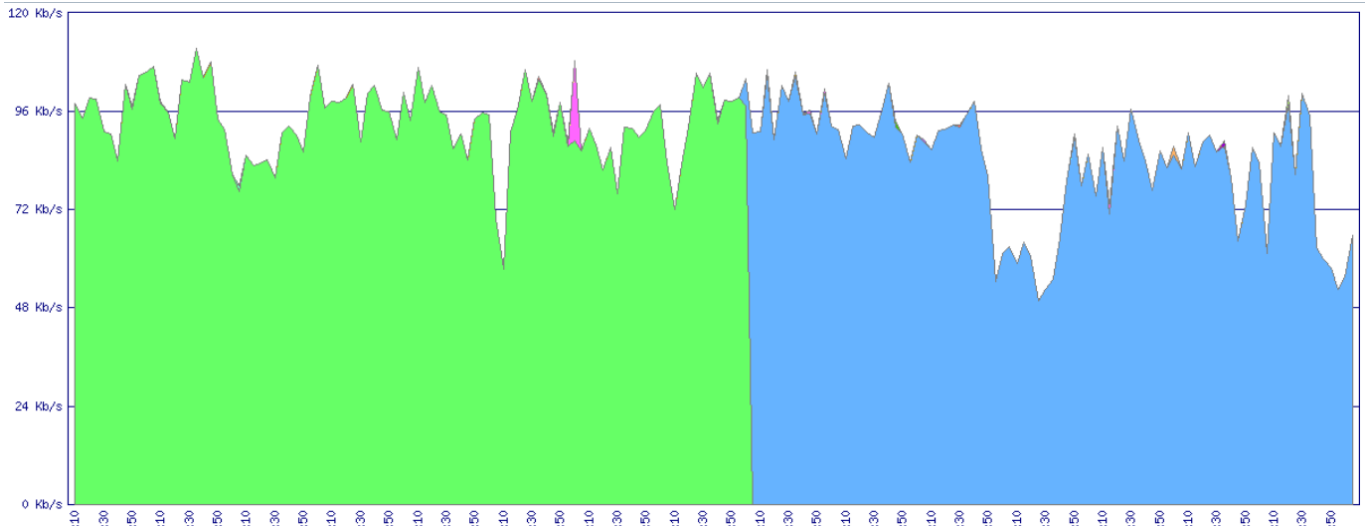
Save

Ověření přidání pravidla FTAS – 1/3

Results *(time values in **CEST**) ..?*

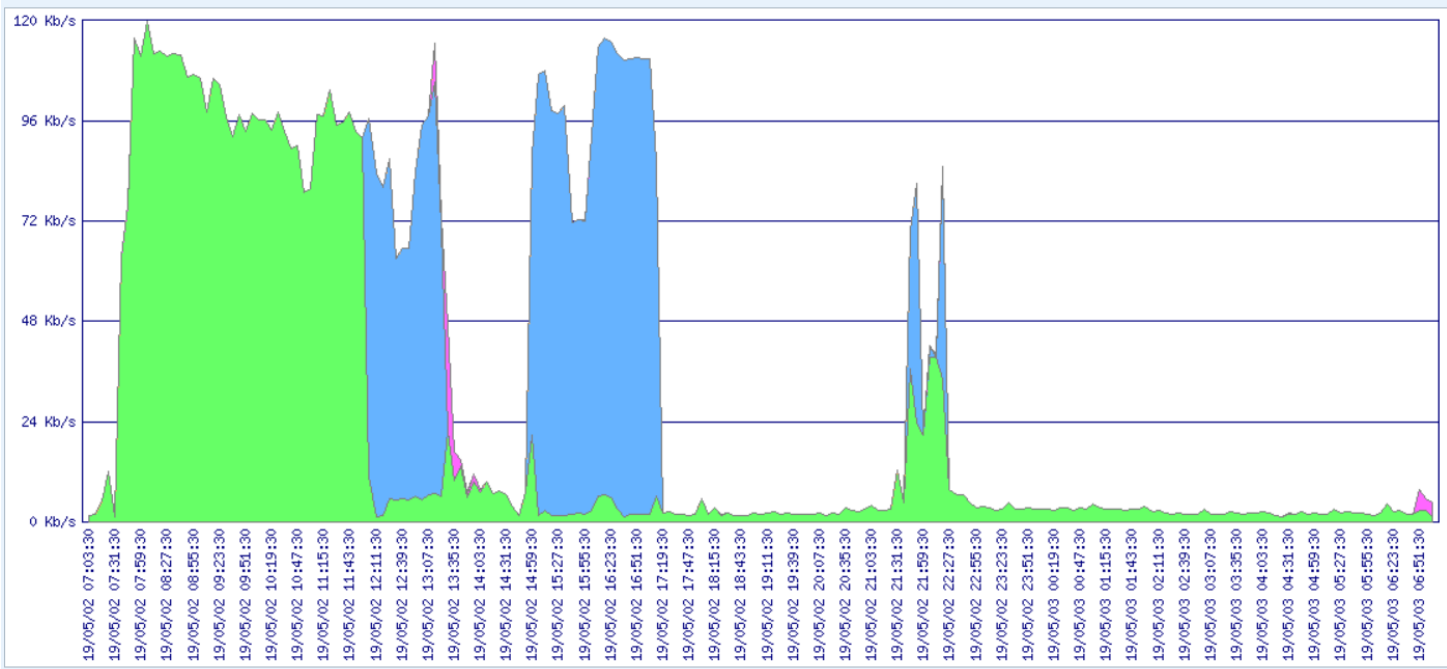
o	>	Flow-Direction	FWD-Status	Src-IP	Protocol	Dst-Port	Src-ifIndex	TCP-flags	Flow-Start [CEST]	Flow-End [CEST]	Bytes-measured	Pkts-measured	Dst-IP-Cnt	Flow-Cnt	Flow-Data-Source
1.		ingress	Forwarded	158.x.x.x	tcp (6)	3389	70	fin(1), syn(2), rst(4), ack(16)	19/05/02 11:30:00.000	19/05/02 12:01:38.777	22.247 MB	427.989 Kp	358993	427563	Olomouc: R133(65)
2.		ingress	Dropped	158.x.x.x	tcp (6)	3389	70	syn(2), ack(16)	19/05/02 12:01:38.783	19/05/02 12:29:59.474	17.621 MB	338.863 Kp	291899	338862	Olomouc: R133(65)
3.		ingress	Forwarded	158.x.x.x	tcp (6)	https (443)	70	fin(1), syn(2), push(8), ack(16)	19/05/02 11:38:21.992	19/05/02 12:18:22.776	60.396 KB	76.000 p	7	8	Olomouc: R133(65)
4.		ingress	Forwarded	158.x.x.x	tcp (6)	20888	70	syn(2), push(8), ack(16)	19/05/02 12:21:28.407	19/05/02 12:21:30.228	5.715 KB	12.000 p	1	2	Olomouc: R133(65)
5.		ingress	Forwarded	158.x.x.x	tcp (6)	20407	70	syn(2), push(8), ack(16)	19/05/02 12:26:50.738	19/05/02 12:26:52.323	5.675 KB	11.000 p	1	2	Olomouc: R133(65)
6.		ingress	Forwarded	158.x.x.x	tcp (6)	56171	70	syn(2), push(8), ack(16)	19/05/02 12:00:06.219	19/05/02 12:16:55.676	4.251 KB	15.000 p	2	2	Olomouc: R133(65)
7.		ingress	Forwarded	158.x.x.x	tcp (6)	63428	70	syn(2), push(8), ack(16)	19/05/02 11:32:49.153	19/05/02 12:09:59.268	3.854 KB	13.000 p	2	2	Olomouc: R133(65)
8.		ingress	Forwarded	158.x.x.x	tcp (6)	62253	70	syn(2), push(8), ack(16)	19/05/02 11:51:46.999	19/05/02 12:11:30.321	3.850 KB	13.000 p	2	3	Olomouc: R133(65)
9.		ingress	Forwarded	158.x.x.x	tcp (6)	63471	70	syn(2), push(8), ack(16)	19/05/02 11:33:58.370	19/05/02 11:53:10.954	3.850 KB	13.000 p	2	2	Olomouc: R133(65)
10.		ingress	Forwarded	158.x.x.x	tcp (6)	52623	70	syn(2), push(8), ack(16)	19/05/02 11:37:45.028	19/05/02 11:37:49.949	3.266 KB	9.000 p	1	1	Olomouc: R133(65)
11.		ingress	Forwarded	158.x.x.x	tcp (6)	63315	70	syn(2), push(8), ack(16)	19/05/02 12:02:34.301	19/05/02 12:02:39.017	3.266 KB	9.000 p	1	1	Olomouc: R133(65)
12.		ingress	Forwarded	158.x.x.x	tcp (6)	28494	70	syn(2), push(8), ack(16)	19/05/02 11:52:21.100	19/05/02 11:52:23.722	3.214 KB	8.000 p	1	1	Olomouc: R133(65)
13.		ingress	Forwarded	158.x.x.x	tcp (6)	61320	70	syn(2), push(8), ack(16)	19/05/02 12:23:45.235	19/05/02 12:23:47.448	3.214 KB	8.000 p	1	1	Olomouc: R133(65)
14.		ingress	Forwarded	158.x.x.x	tcp (6)	42261	70	syn(2), push(8), ack(16)	19/05/02 12:08:23.419	19/05/02 12:08:25.701	3.214 KB	8.000 p	1	1	Olomouc: R133(65)
15.		ingress	Forwarded	158.x.x.x	tcp (6)	55268	70	syn(2), push(8), ack(16)	19/05/02 12:03:55.746	19/05/02 12:04:00.942	3.214 KB	8.000 p	1	1	Olomouc: R133(65)
16.		ingress	Forwarded	158.x.x.x	tcp (6)	64167	70	syn(2), push(8), ack(16)	19/05/02 12:20:38.204	19/05/02 12:20:43.467	3.214 KB	8.000 p	1	1	Olomouc: R133(65)
17.		ingress	Forwarded	158.x.x.x	udp (17)	443	70		19/05/02 12:04:20.158	19/05/02 12:17:14.339	3.170 KB	8.000 p	2	2	Olomouc: R133(65)
18.		ingress	Forwarded	158.x.x.x	tcp (6)	18802	70	syn(2), push(8), ack(16)	19/05/02 12:29:37.032	19/05/02 12:29:38.515	2.715 KB	10.000 p	1	2	Olomouc: R133(65)
19.		ingress	Forwarded	158.x.x.x	tcp (6)	33076	70	syn(2), push(8), ack(16)	19/05/02 12:02:41.021	19/05/02 12:28:56.004	2.715 KB	10.000 p	2	3	Olomouc: R133(65)
20.		ingress	Forwarded	158.x.x.x	tcp (6)	50346	70	syn(2), push(8), ack(16)	19/05/02 12:27:19.168	19/05/02 12:27:20.576	2.715 KB	10.000 p	1	2	Olomouc: R133(65)
21.		ingress	Forwarded	158.x.x.x	tcp (6)	53840	70	syn(2), push(8), ack(16)	19/05/02 12:24:39.910	19/05/02 12:28:20.221	2.715 KB	10.000 p	1	2	Olomouc: R133(65)

Ověření přidání pravidla FTAS – 2/3



	Flow-Direction	FWD-Status	Src-IP	Protocol	Dst-Port	Src-ifIndex	TCP-flags	Flow-Start	Flow-End	Bytes-measured	Pkts-measured	Dst-IP-Cnt	Flow-Cnt	Flow-Data-Source
1.	ingress	Forwarded	158.x.x.x	tcp (6)	3389	70	fin(1), syn(2), rst(4), ack(16)	19/05/02 11:30:00.000	19/05/02 12:01:38.777	22.247 MB	427.989 Kp	358993	427563	Olomouc: R133(65)
2.	ingress	Dropped	158.x.x.x	tcp (6)	3389	70	syn(2), ack(16)	19/05/02 12:01:38.783	19/05/02 12:29:59.474	17.621 MB	338.863 Kp	291899	338862	Olomouc: R133(65)
3.	ingress	Forwarded	158.x.x.x	tcp (6)	https (443)	70	fin(1), syn(2), push(8), ack(16)	19/05/02 11:38:21.992	19/05/02 12:18:22.776	60.396 KB	76.000 p	7	8	Olomouc: R133(65)
4.	ingress	Forwarded	158.x.x.x	tcp (6)	20888	70	syn(2), push(8), ack(16)	19/05/02 12:21:28.407	19/05/02 12:21:30.228	5.715 KB	12.000 p	1	2	Olomouc: R133(65)
5.	ingress	Forwarded	158.x.x.x	tcp (6)	20407	70	syn(2), push(8), ack(16)	19/05/02 12:26:50.738	19/05/02 12:26:52.323	5.675 KB	11.000 p	1	2	Olomouc: R133(65)

Ověření přidání pravidla FTAS – 3/3



	Flow-Direction	FWD-Status	Src-IP	Protocol	Flow-Start	Flow-End	Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated	Dst-Port-Cnt	Flow-Cnt
1. >	ingress	Forwarded	158.x.x.x	tcp (6)	19/05/02 07:00:13.749	19/05/03 07:06:16.848	237.268 MB	711.805 MB	3.783 Mp	11.350 Mp	14824	3602493
2. >	ingress	Dropped	158.x.x.x	tcp (6)	19/05/02 12:01:38.783	19/05/03 03:34:27.471	157.504 MB	472.511 MB	3.029 Mp	9.087 Mp	1	3028914
3. >	ingress	Forwarded	158.x.x.x	udp (17)	19/05/02 07:23:14.314	19/05/03 07:05:02.642	3.298 MB	9.895 MB	5.833 Kp	17.499 Kp	6	232
4. >	ingress	Forwarded	158.x.x.x	icmp (1)	19/05/02 07:06:29.440	19/05/03 07:01:25.334	14.927 KB	44.781 KB	336.000 p	1.008 Kp	2	329

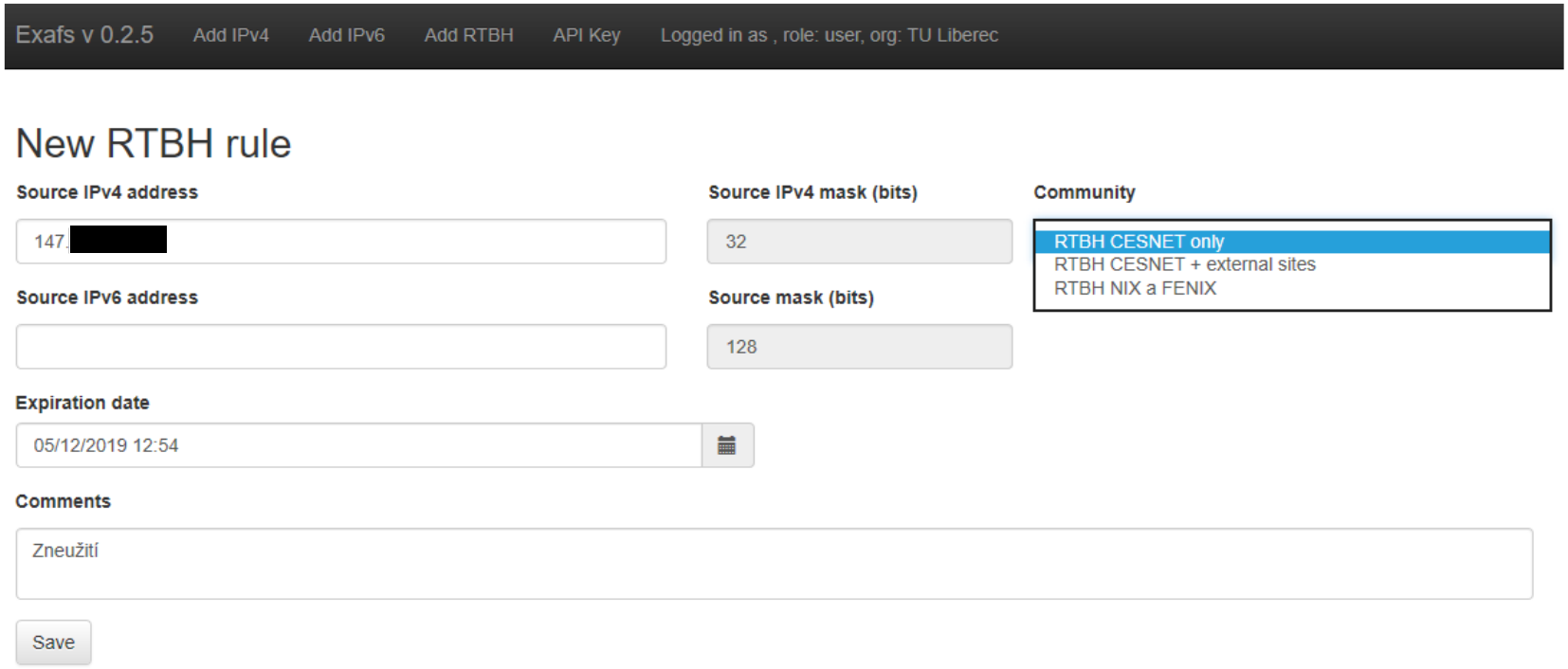
Konfigurace routeru – příkazy

```
router bgp <AS>
 neighbor 195.113.xxx.xxx
  use neighbor-group RR-ipv4
  password encrypted <password>
  description RR1
...
  !
  address-family ipv4 flowspec
   soft-reconfiguration inbound always
  !
  address-family ipv6 flowspec
   soft-reconfiguration inbound always
  !
  address-family vpnv4 flowspec
   soft-reconfiguration inbound always
  !
  address-family vpnv6 flowspec
   soft-reconfiguration inbound always
  !
 !
!

flowspec
 address-family ipv4
  local-install interface-all
 !
 address-family ipv6
  local-install interface-all
 !
!

interface Bundle-EtherX (vypnutí směrem k PE)
 description Rxxx
...
 ipv4 flowspec disable
 ipv6 flowspec disable
```

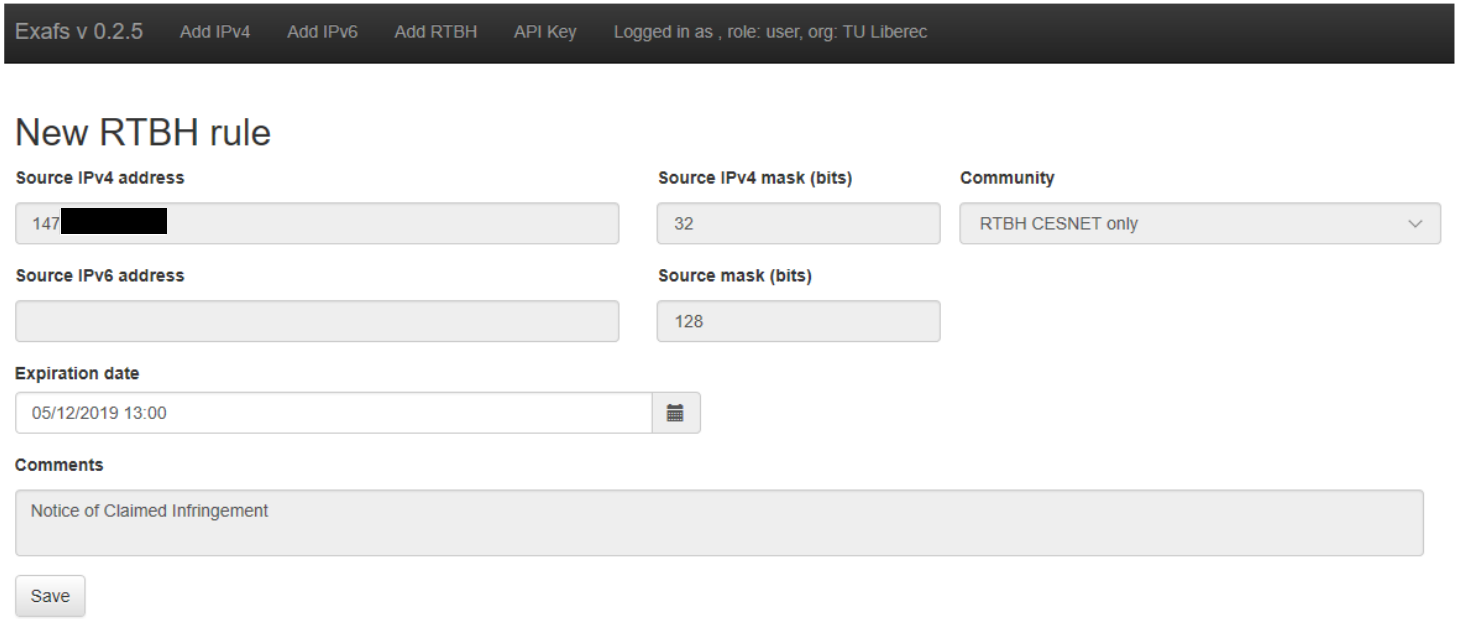
```
#--------------------------------------------------
echo "BGP Configuration"
#--------------------------------------------------
group "iBGP"
                peer-as <AS>
                path-mtu-discovery
                neighbor 195.113.xxx.xxx
                    description "Rxxx"
                    family ... flow-ipv4 mvpn-ipv6 flow-
ipv6 label-ipv6

                    authentication-key <hash> hash2
                    local-address 195.113.xxx.xxx
                    ...
                    exit


#--------------------------------------------------
echo "FLOWSPEC PARAMS Configuration"
#--------------------------------------------------
        flowspec
            ip-filter-max-size 5000
            ipv6-filter-max-size 5000
        exit
    exit


#--------------------------------------------------
echo "Filter Configuration"
#--------------------------------------------------
    filter
        ip-filter 11001 create/ip-filter 11001 create
            embed-filter flowspec router "Base"
        exit
    exit
```

```
        ipv6-filter 11001 create/ipv6-filter 11001 create
            filter-name "FS-global"
            default-action forward
            description "FlowSpec - globalni"
        exit


#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------

        sap 3/1/6 create
                    ingress
                        filter ip 11001
                        filter ipv6 11001
                    exit
```

Přidání RTBH pravidla

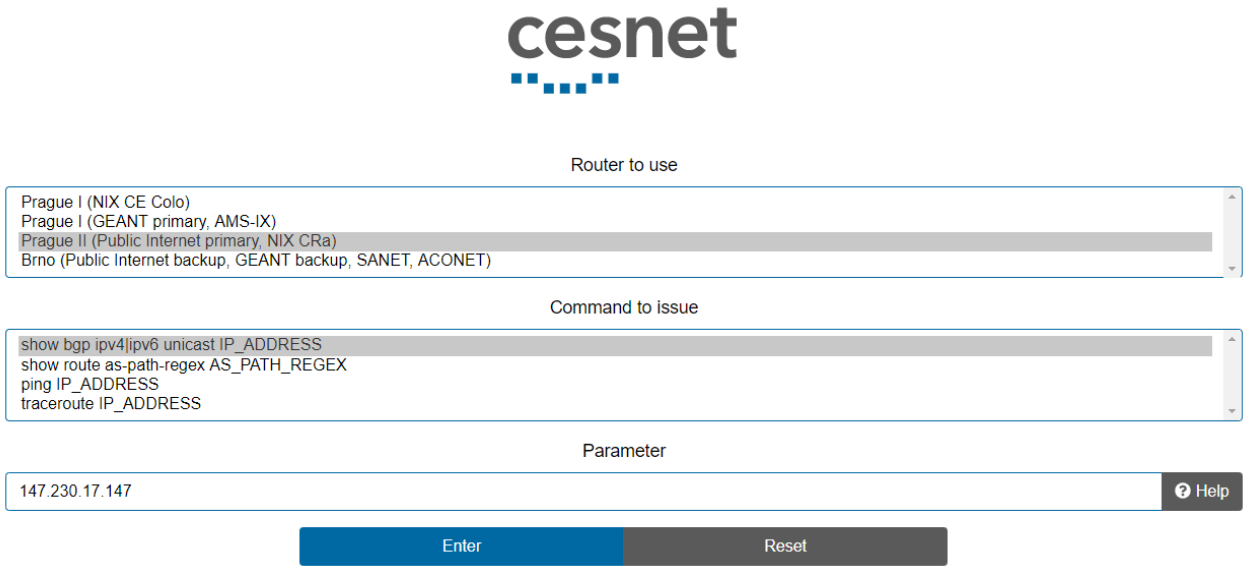


Editace RTBH pravidla

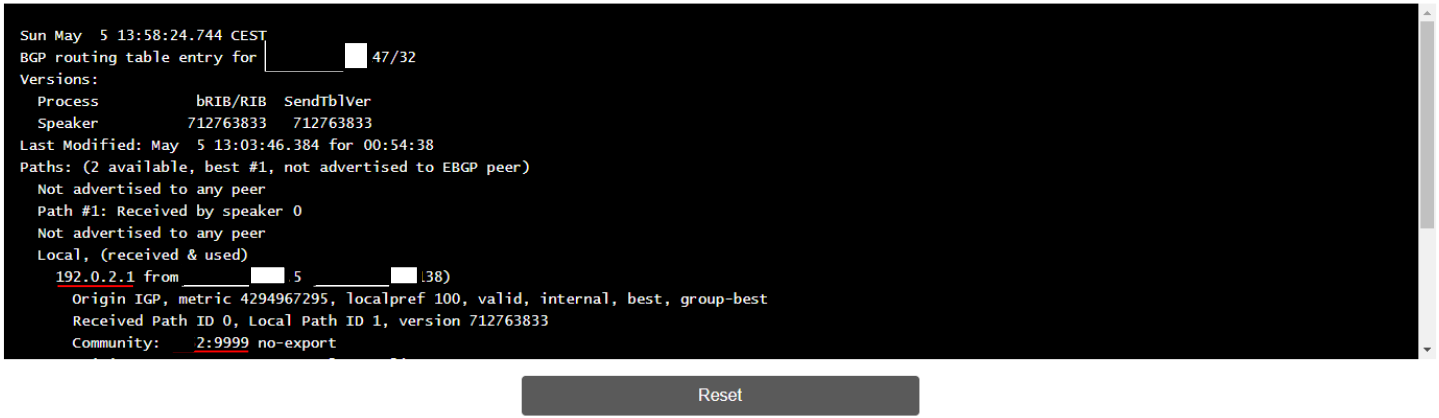


Ověření RTBH – 1/2

- Looking Glass https://lg.cesnet.cz



Ověření RTBH – 2/2



RFC 5635 – Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF) **– 192.0.2.1**

BGP Community -- Community: 2:9999 no-export

Ověření RTBH – správce

```
RP/0/RP0/CPU0:R1#sh ip route 192.168.1.1
Sun May  5 14:15:19.643 METDST

Routing entry for 192.168.1.1/32
  Known via "bgp 2", distance 200, metric 4294967294, type internal
  Installed May  5 13:03:46.460 for 01:11:33
  Routing Descriptor Blocks
    192.0.2.1, from 10.10.10.10
      Route metric is 4294967294
  No advertising protos.
RP/0/RP0/CPU0:R148#sh bgp ipv4 unicast 192.168.1.1
...
Paths: (2 available, best #1, not advertised to EBGP peer)
Advertisements of this net are suppressed by an aggregate.
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local, (received & used)
    192.0.2.1 from 10.10.10.10 (20.10.10.1)
      Origin IGP, metric 4294967295, localpref 100, valid, internal, best, group-best
      Received Path ID 0, Local Path ID 1, version 673909536
      Community: 2852:9999 no-export
      Originator: 20.10.10.1, Cluster list: 0.0.0.1
  ...
```

Zobrazení přidaného pravidla ALU/Nokia 1/3

```
A:R1# show filter ipv6 fSpec-0

===============================================================================
IPv6 Filter
===============================================================================
Filter Id           : fSpec-0
Scope               : Embedded
Entries             : 1 (insert By Bgp)
Sub-Entries         : 2 (insert By Bgp)
Description         : IPv6 BGP FlowSpec filter for the Base router
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry               : 2500
Origin              : Inserted by BGP FlowSpec
Description         : (Not Specified)
Log Id              : n/a
Src. IP             : 2001:db8:1::/64
Src. Port           : n/a
Dest. IP            : ::/0
Dest. Port          : port-list "_tmnx_fSpec_ipv6_131_dst"
Next Header         : 17                          Dscp           : Undefined
ICMP Type           : Undefined                   ICMP Code      : Undefined
Sampling            : Off                         Int. Sampling  : On
TCP-syn             : Off                         TCP-ack        : Off
Fragment            : Off
HopByHop Opt        : Off                         Routing Type0  : Off
Auth Hdr            : Off                         ESP header     : Off
Flow-label          : n/a                         Flow-label Mask: n/a
Egress PBR          : Disabled
Primary Action      : Rate-limit 100 kbps
Ing. Matches        : 0 pkts
Egr. Matches        : 0 pkts
Ing. Rate-limiter
  Offered           : 0 pkts
  Forwarded         : 0 pkts
  Dropped           : 0 pkts
Egr. Rate-limiter
  Offered           : 0 pkts
  Forwarded         : 0 pkts
  Dropped           : 0 pkts

===============================================================================

A:R1# show filter ipv6 "fSpec-0" entry 2500 % detail konkrétního pravidla
```

Zobrazení přidaného pravidla ALU/Nokia

```
A:R1# show filter match-list port-list "_tmnx_fSpec_ipv6_131_dst"

===============================================================================
Filter Match Port Lists
===============================================================================
Port list "_tmnx_fSpec_ipv6_131_dst"
    25    487
    NUM ports/ranges: 2

    References:
        IPv6-filter 2001 entry 2500 (Dst-Port)
        IPv6-filter 11001 entry 2500 (Dst-Port)
        IPv6-filter 16777217 entry 2500 (Dst-Port)
        NUM references: 3

===============================================================================
```

Zobrazení přidaného pravidla CISCO 1/5

```
RP/0/RP0/CPU0:R1#sh bgp ipv6 flowspec
Sun May  5 18:58:28.555 METDST
BGP router identifier 20.10.10.1, local AS number 2
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 7
BGP main routing table version 7
BGP NSR Initial initsync version 2 (Reached)
BGP NSR/ISSU Sync-Group versions 7/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network           Next Hop            Metric LocPrf Weight Path
*>iSource:2001:db8:1::/0-64,NH:=17,DPort:=25|=487/160
                     ::                  4294967295    100      0 i

Processed 1 prefixes, 1 paths
```

Zobrazení přidaného pravidla CISCO 2/5

```
RP/0/RP0/CPU0:R1#sh bgp ipv6 flowspec Source:2001:db8:1::/0-64,NH:=17,DPort:=25|=487/160 detail
Sun May  5 18:59:25.933 METDST
BGP routing table entry for Source:2001:db8:1::/0-64,NH:=17,DPort:=25|=487/160
NLRI in Hex: 02400020010db8000100000381110501199101e7/160
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 7           7
    Flags: 0x00001001+0x00000000;
Last Modified: May  5 18:30:48.700 for 00:28:37
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Flags: 0x4000000001068005, import: 0x20
  Not advertised to any peer
  Local, (received & used)
    :: from 10.10.10.10 (20.10.10.1)
      Origin IGP, metric 4294967295, localpref 100, valid, internal, best, group-best
      Received Path ID 0, Local Path ID 1, version 7
      Extended community: FLOWSPEC Traffic-rate:0,12800
      Originator: 20.10.10.1, Cluster list: 0.0.0.1
```

Zobrazení přidaného pravidla CISCO 3/5

```
RP/0/RP0/CPU0:R1#sh flowspec ipv6
Sun May  5 19:05:07.333 METDST

AFI: IPv6
  Flow           :Source:2001:db8:1::/0-64,NH:=17,DPort:=25|=487
    Actions      :Traffic-rate: 102400 bps  (bgp.1)
```

Zobrazení přidaného pravidla CISCO 4/5

```
RP/0/RP0/CPU0:R1#sh flowspec ipv6 Source:2001:db8:1::/0-64,NH:=17,DPort:=25|=487
Sun May  5 19:02:31.256 METDST

AFI: IPv6
  Flow           :Source:2001:db8:1::/0-64,NH:=17,DPort:=25|=487
    Actions      :Traffic-rate: 102400 bps  (bgp.1)
RP/0/RP0/CPU0:R1#sh flowspec ipv6 Source:2001:db8:1::/0-64,NH:=17,DPort:=25|=487 detail
Sun May  5 19:02:33.489 METDST

AFI: IPv6
  Flow           :Source:2001:db8:1::/0-64,NH:=17,DPort:=25|=487
    Actions      :Traffic-rate: 102400 bps  (bgp.1)
    Statistics                       (packets/bytes)
      Matched             :                0/0
      Dropped             :                0/0
```

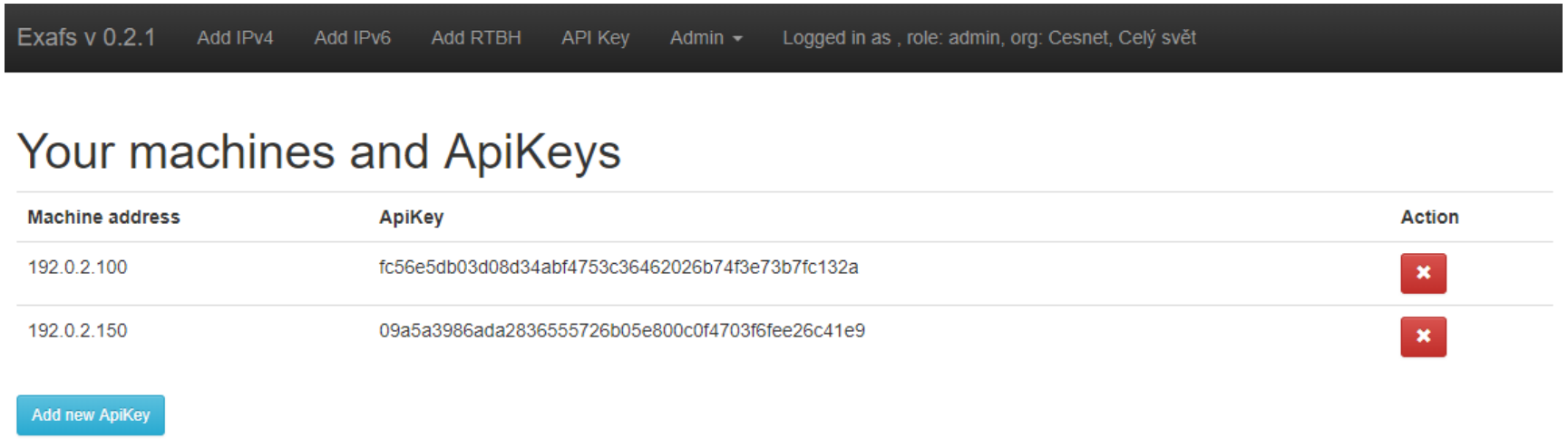
Zobrazení přidaného pravidla CISCO 5/5

```
RP/0/RP0/CPU0:R1#show policy-map transient type pbr pmap-name __bgpfs_default_IPv6
Sun May  5 19:14:22.894 METDST
policy-map type pbr __bgpfs_default_IPv6
 handle:0x36000003
 table description: L3 IPv4 and IPv6
 class handle:0x760002bc  sequence 1024
   match source-address ipv6 2001:db8:1::/64
   match protocol udp
   match destination-port 25 487
  police rate 102400 bps
   conform-action transmit
   exceed-action drop
  !
 !
 class handle:0xf6000003  sequence 4294967295 (class-default)
 !
 end-policy-map
!
```

cesnet

ExaFS API

API – vytvoření klíče



API – získání tokenu

```
[pa@oxx ~]$ curl -4 -include 'https://localhost/api/v1/auth/taiyahgach5AoD8Ohshoiphahch4kea5aafas'

HTTP/1.1 200 OK
Date: Wed, 30 Jan 2019 10:30:00 GMT
Server: Apache/2.4.38 (Red Hat Enterprise Linux) OpenSSL/1.0.2q-fips
Strict-Transport-Security: max-age=63072000; includeSubdomains;
Content-Type: application/json
Content-Length: 297

{
  "token":
 ohTeiXiegiel1siong9yoe1sa3beweebahquohsu1DeiFohG0ia6Keeth2miiluun9po4kaiquieTaigaeY5hohT5qua9uf6oBa7ewuaH
3jope6lahbeyo8eiga9yiNeeH2Iopoo2Ieyiic2chaibeeLe1wongiac7uu1eeth7Yikoi1aeci3Thaesh2aipa5ohquee4Ewe6aiph7ro
o5deiGhei2elootuo4no7OoJu6dae6ahfiekuBei2pei3
}
```

API – přidání pravidla

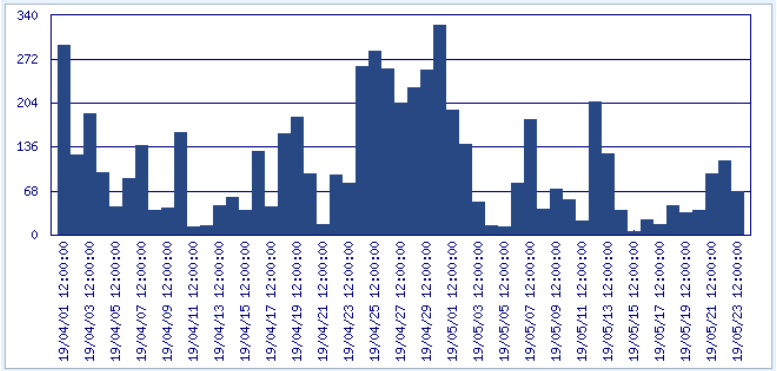
```
[pa@oxx ~]$ curl --include  --request POST --header "Content-Type: application/json"  --header "x-access-token: token" --data-binary "{ \"action\": 2,  \"protocol\": \"tcp \", \"source\": \"100.72.100.1\", \"source_mask\": 32, \"source_port\": \"\", \"expires\": \"03/05/2019 12:30\" }" 'https://localhost/api/v1/rules/ipv4'
```

Odpověď serveru (bez hlaviček):


```
{
  "message": "IPv4 Rule saved",
  "rule": {
    "action": "QoS 1 Mbps",
    "comment": "",
    "created": "Wed, 24 Apr 2019 10:30:00 GMT",
    "dest": "",
    "dest_mask": null,
    "dest_port": "",
    "expires": "Fri, 03 May 2019 12:30:00 GMT",
    "flags": "",
    "id": 18,
    "packet_len": "",
    "protocol": "tcp",
    "rstate": "active rule",
    "source": "100.72.100.1",
    "source_mask": 32,
    "source_port": "",
    "user": "pa@cesnet.cz"
  }
}
```

Testování API pro komunikaci s detekčními programy

- **FTAS**
  - knihovna pro spolupráci s ExaFS (ve vývoji/testování)
  - automatická regulace bude aplikovaná pouze při minimálním riziku výskytu “false positives“
    - aktuálně desítky až stovky událostí denně (viz. graf s denními agregáty od 1. dubna → dává smysl)
    - po nasazení pro tento účel přizpůsobíme detektory (lepší škálování, oddělení jasných případů apod.)
  - cílem je produkční nasazení do konce roku



	Bytes-estimated	Pkts-estimated	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt
1. >	176.669 GB	4.338 Gp	107467363	85645644	5661

cesnet

Co to pohnání

- exaBGP 3.4.26 (plánován přechod na verzi 4.0.x)

- Python 2.7 (kvůli RHEL, v aplikaci počítáno s přechodem na 3.7)
- 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

Plány 2019

- **Testování API pro komunikaci s detekčními programy**
- **Rozšiřování mezi další správce, klienty…**
- **A ladění a testy a ladění a opravy a testy a ladění**
- **Dlouhodobé plány**
  - Možnost konfigurace čističky z jednoho rozhraní

cesnet

A to je konec…

PŘIPRAVOVANÉ AKCE

Seminář IPv6

- 6. 6. 2019 na ČVUT v Praze
- jednodenní seminář věnovaný internetovému protokolu IPv6
- **Call for Lightning talk** seminar-ipv6@cesnet.cz
- **program a registrace:** https://www.cesnet.cz/akce/ipv6-2019/

NOVINKY SDRUŽENÍ CESNET

- Akce
  - https://www.cesnet.cz/akce/
- CESNET eNews
  - https://www.cesnet.cz/enews/
- Facebook
  - https://www.facebook.com/cesnet.cz/
- Twitter
  - https://twitter.com/CESNET_news