cesnet

Nástroje pro FlowSpec a RTBH

Jiří Vraný, Petr Adamec a Josef Verich
CESNET

30. leden 2019
Praha

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…

Dashboard

Exafs v 0.2.1 | Add IPv4 | Add IPv6 | Add RTBH | API Key | Admin | Logged in as , role: admin, org: Cesnet, Celý svět

Default dashboard

Rules IPv4/v6

Source adress	Source port(s)	Destination adress	Dest. port(s)	Protocol(s)	Expires	Action	Flags	Action
203.0.113.0 / 24			22	tcp	2019-02-08 12:30:00	QoS 0.1 Mbps		
Comment:	RFC 5737 ...			**Created by:**	Petr Adamec			
192.0.2.100 / 32			25	tcp	2019-02-08 12:30:00	Redirect to DDoS Protector		
Comment:	RFC 5737 ...			**Created by:**	Petr Adamec			
2001:db8:1::1 / 128				udp	2019-02-08 12:30:00	Discard		
Comment:	RFC 3849 ...			**Created by:**	Petr Adamec			

Rules RTBH

IP adress (v4 or v6)	Community	Expires	Action
198.51.100.0 / 24	2852:666	2019-02-08 12:30:00	

Seznam organizací

Exafs v 0.2.1 | Add IPv4 | Add IPv6 | Add RTBH | API Key | Admin | Logged in as , role: admin, org: Cesnet, Celý svět

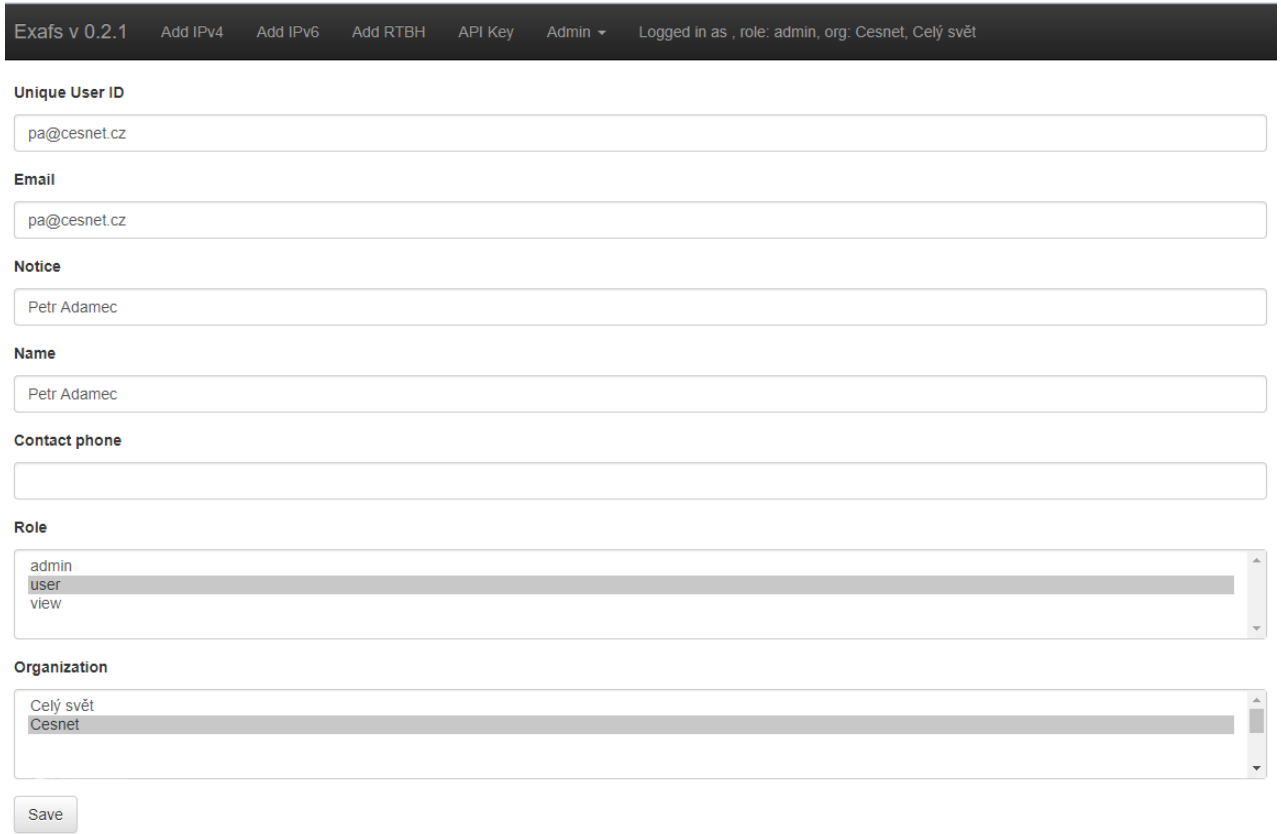
Name	Adress Range	action
TU Liberec	147.[redacted].0/16 2001:[redacted]::/48	
Cesnet	147.[redacted].0.0/15 147.[redacted].0.0/14 160.[redacted].0.0/15 146.[redacted].0.0/16 147.[redacted].0.0/16 158.[redacted].0.0/16 158.[redacted].0.0/16 193.[redacted]2.0/20 193.[redacted]60.0/20 193.[redacted]92.0/19 195.[redacted].0.0/16 195.[redacted].64.0/19 78.[redacted].128.0/17 2001:[redacted]::/29	

Seznam akcí

Exafs v 0.2.1 | 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 65535:1001	Presmerovani na cisticku (RT 65535:1001)	user	
24	Redirect to analyzator	redirect 65535:1101	Presmerovani na analyzator (RT 65535:1101)	admin	
25	QoS 0.05 Mbps	rate-limit 6400	QoS	user	

Přidání uživatele



Přidání IPv6 pravidla

Exafs v 0.2.1 | Add IPv4 | Add IPv6 | Add RTBH | API Key | Admin | Logged in as , role: admin, org: Cesnet, Celý svět

New IPv6 rule

Source address
2001:db8:1::

Source prefix length (bytes)
64

Next Header
UDP

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

Destination address

Destination prefix length (bytes)

Source port(s) - ; separated

Destination port(s) - ; separated
25;487

Packet length

Action
QoS 1 Mbps

Expiration date
02/08/2019 12:30

Comments
RFC 3849 - IPv6 Address Prefix Reserved for Documentation

Save

Zobrazení přidaného pravidla ALU/Nokia 1/2

```
===============================================================================
IPv6 Filter
===============================================================================
Filter Id           : 11001                       Applied        : Yes
Scope               : Template                    Def. Action    : Forward
System filter       : Unchained
…
Description         : FlowSpec - globalni
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry               : 2500
Origin              : Inserted by embedded filter fSpec-0 entry 2500
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_189_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 1024 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

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

Zobrazení přidaného pravidla ALU/Nokia 2/2

```
===============================================================================
==
Filter Match Port Lists
===============================================================================
==
Port list "_tmnx_fSpec_ipv6_189_dst"
    25    487
    NUM ports/ranges: 2

    References:
        IPv6-filter 2002 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 1/2

```
AFI: IPv6
  Flow           :Source:2001:db8:1::/0-64,NH:=17,DPort:=25|=487
    Actions      :Traffic-rate: 1048576 bps  (bgp.1)
    Statistics                               (packets/bytes)
      Matched                :                      0/0
      Transmitted            :                      0/0
      Dropped                :                      0/0
```

Zobrazení přidaného pravidla CISCO 2/2

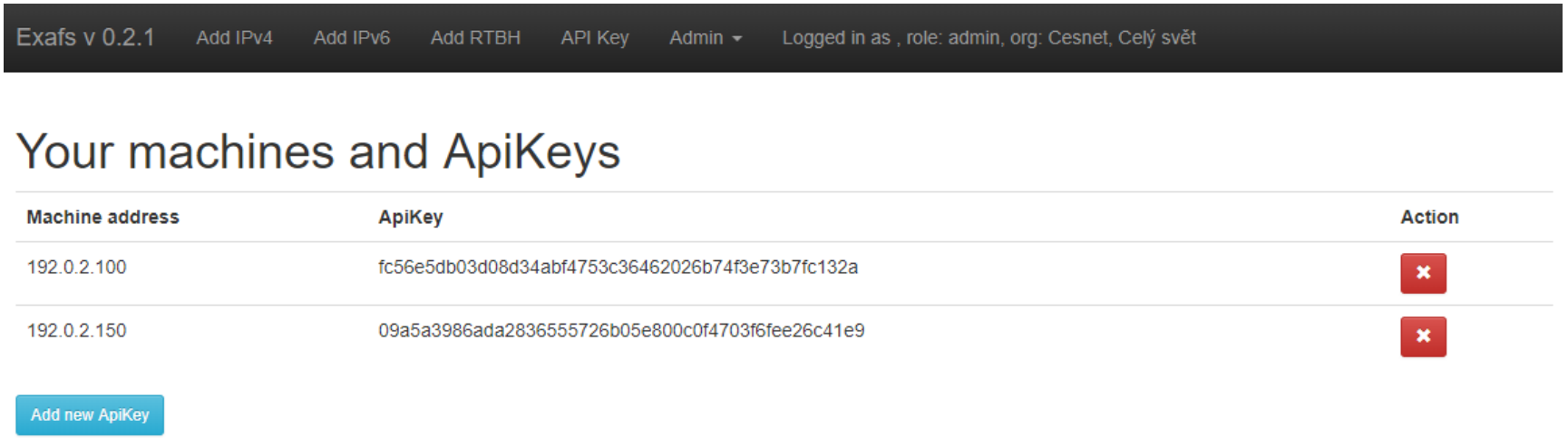
```
policy-map type pbr __bgpfs_default_IPv6
 handle:0x36000003
 table description: L3 IPv4 and IPv6
 class handle:0x760003c5  sequence 1024
   match source-address ipv6 2001:db8:1::/64
   match protocol udp
   match destination-port 25 487
  police rate 1048576 bps
   conform-action transmit
   exceed-action drop
  !
 !
 class handle:0xf6000003  sequence 4294967295 (class-default)
 !
 end-policy-map
```

cesnet

a to dlouho slibovaná…

Novinka!

API – vytvoření klíče



API – získání tokenu

```
[pa@pa ~]$ 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":
 ohTeiXiegiel1siong9yoe1sa3beweebahquohsu1DeiFohG0ia6Keeth2miiluun9po4kaiquieTaigaeY5hohT5qua9uf
6oBa7ewuaH3jope6lahbeyo8eiga9yiNeeH2Iopoo2Ieyiic2chaibeeLe1wongiac7uu1eeth7Yikoi1aeci3Thaesh2aip
a5ohquee4Ewe6aiph7roo5deiGhei2elootuo4no7OoJu6dae6ahfiekuBei2pei3
}
```

API – přidání pravidla

```
[pa@pa ~]$ curl --include  --request POST --header "Content-Type: application/json"  --header "x-access-
token: token" --data-binary "{ \"action\": 2,  \"protocol\": \"tcp \", \"source\": \"198.51.100.1\",
\"source_mask\": 32, \"source_port\": \"\", \"expires\": \"02/08/2019 12:30\" }"
'https://localhost/api/v1/rules/ipv4'
```

Odpověď serveru (bez hlaviček):


```
{
  "message": "IPv4 Rule saved",
  "rule": {
    "action": "QoS 1 Mbps",
    "comment": "",
    "created": "Wed, 30 Jan 2019 10:30:00 GMT",
    "dest": "",
    "dest_mask": null,
    "dest_port": "",
    "expires": "Fri, 08 Feb 2019 12:30:00 GMT",
    "flags": "",
    "id": 18,
    "packet_len": "",
    "protocol": "tcp",
    "rstate": "active rule",
    "source": "198.51.100.1",
    "source_mask": 32,
    "source_port": "",
    "user": "pa@cesnet.cz"
  }
}
```

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