cesnet

HSOC – technická skupina

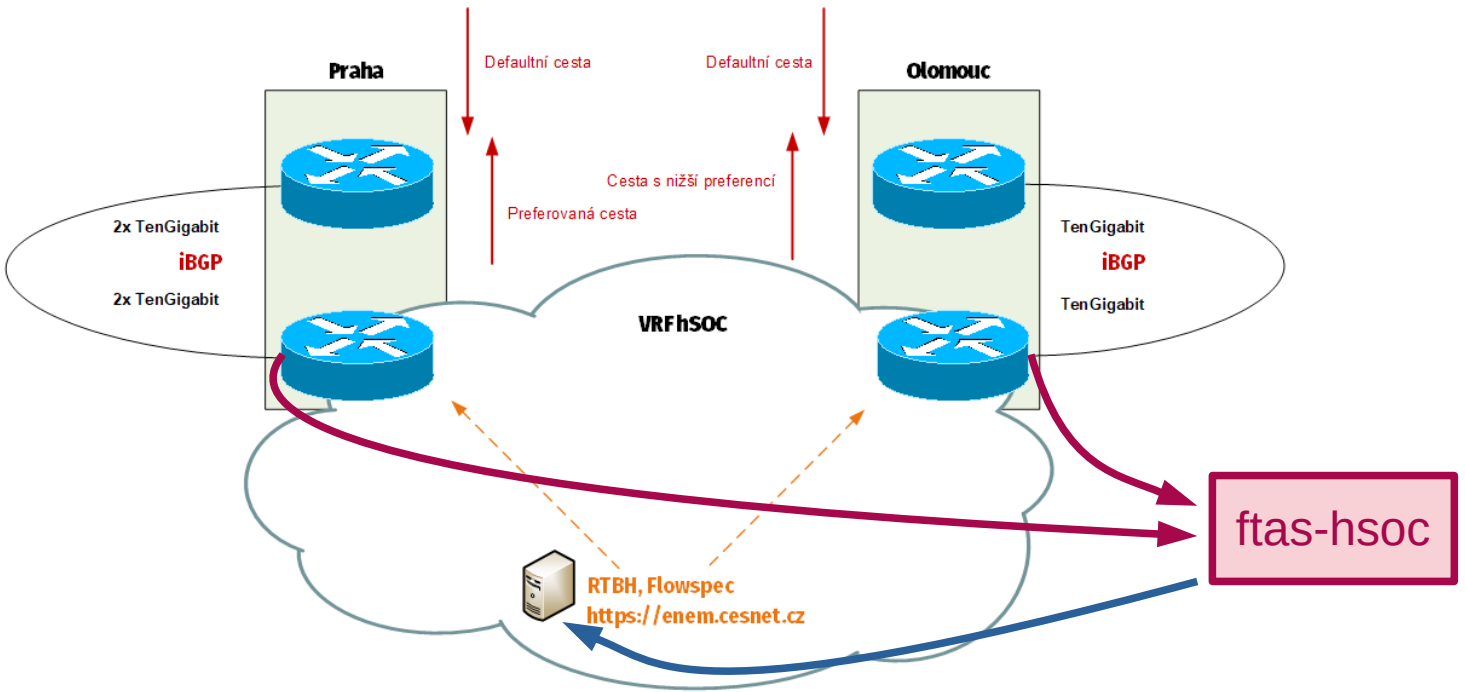
- flow-based monitoring, VRF, připojené sítě

Tomáš Košňar
CESNET

2020/11/27
VC, hsoc-tech

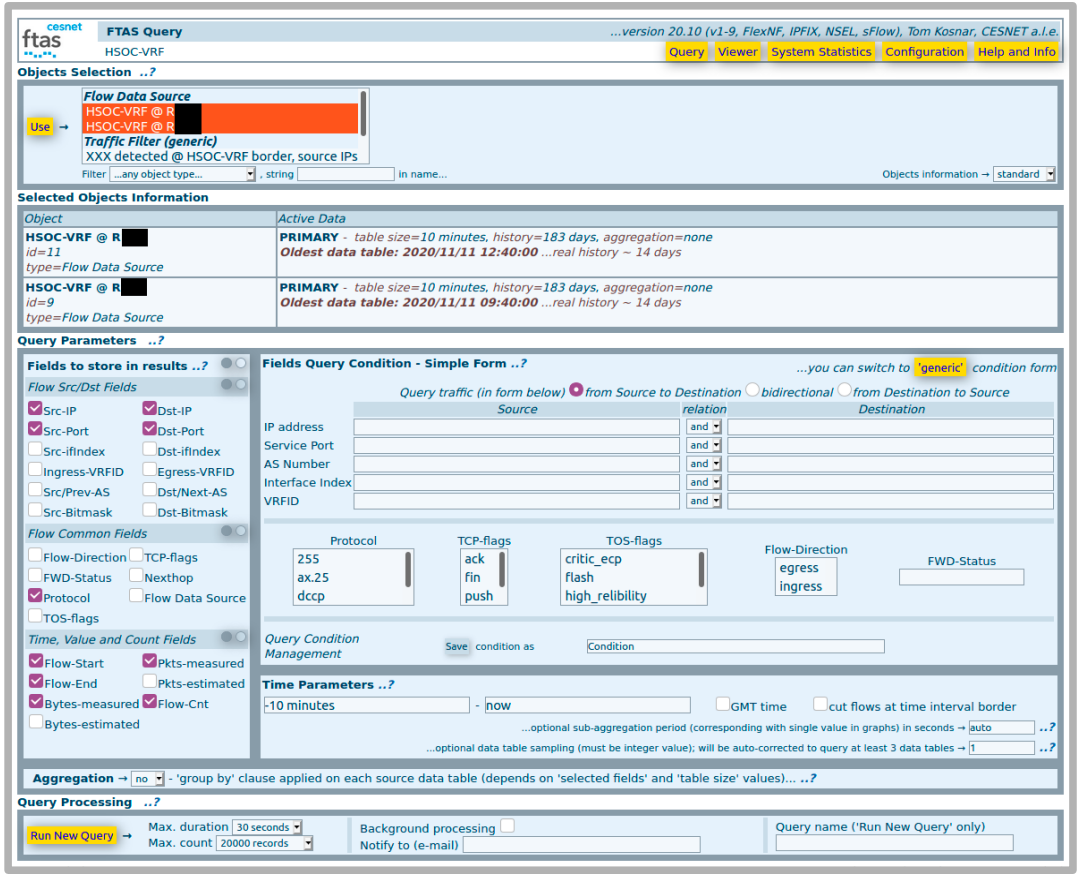
ftas-soc – flow-based monitoring VRF

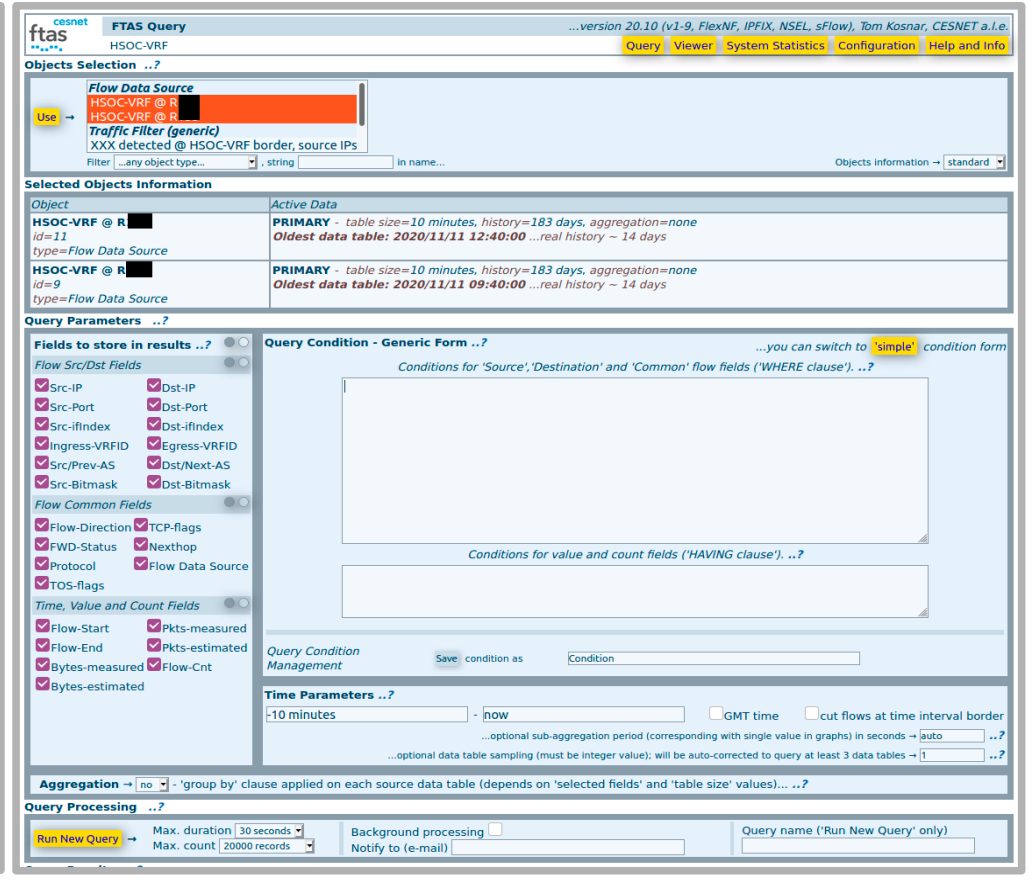
- dedikovaný L3 flow-based monitoring pro VRF
- pro IH, detektory anomálií mezi VRF a vnějším světem



ftas-soc – flow-based monitoring VRF

- ex-post analýza provozu, UI (provoz přes perimetr hsoc-vrf)





ftas-soc – flow-based monitoring VRF

- ex-post analýza provozu, UI

Query Condition - Generic Form ..? ...you can switch to 'simple' co

Conditions for 'Source','Destination' and 'Common' flow fields ('WHERE clause'). ..?

```
proto=6 and tcp_flags=2 and tcp_flags<>16 and pktlen<128
and src_ip=0.0.0.0-255.255.255.255,::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
and src_ip<>www.cesnet.cz,195.113.0.0/24 and dst_ip<>www.seznam.cz
or
proto=17 and src_port=0,19,53,161,389,11211 and pktlen>1000
```

o	>	Direction	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	ifIndex	TOS-flags	TCP-flags	Bytes-estimated	Pkts-estimated	Flow-Data-Sou
1.		ingress	Forwarded	36.68.8.x	195.113.x.x	tcp (6)	63551	http (80)	384	156	00000000	syn(2)	180.000 B	3.000 p	HSOC-VRF @ R
2.		ingress	Forwarded	103.249.95.x	185.8.x.x	tcp (6)	60902	ssh (22)	384	156	00000000	syn(2)	180.000 B	3.000 p	HSOC-VRF @ R
3.		ingress	Forwarded	24.0.34.x	185.8.x.x	tcp (6)	50248	ssh (22)	384	156	00000000	syn(2)	180.000 B	3.000 p	HSOC-VRF @ R
4.		ingress	Forwarded	125.42.98.x	185.8.x.x	tcp (6)	59121	http (80)	384	156	00000000	syn(2)	180.000 B	3.000 p	HSOC-VRF @ R
5.		ingress	Forwarded	185.8.14.x	185.8.x.x	tcp (6)	57593	microsoft-ds (445)	384	156	00000000	syn(2)	152.000 B	3.000 p	HSOC-VRF @ R
6.		ingress	Forwarded	125.163.161.x	185.8.x.x	tcp (6)	51541	microsoft-ds (445)	384	156	00000000	syn(2)	152.000 B	3.000 p	HSOC-VRF @ R
7.		ingress	Forwarded	180.245.53.x	185.8.x.x	tcp (6)	65323	microsoft-ds (445)	384	156	00000000	syn(2)	152.000 B	3.000 p	HSOC-VRF @ R
8.		ingress	Forwarded	49.36.135.x	185.8.x.x	tcp (6)	63412	microsoft-ds (445)	384	156	00101000	syn(2)	152.000 B	3.000 p	HSOC-VRF @ R
9.		ingress	Forwarded	180.245.53.x	185.8.x.x	tcp (6)	60455	microsoft-ds (445)	384	156	00000000	syn(2)	152.000 B	3.000 p	HSOC-VRF @ R
10.		ingress	Forwarded	159.192.164.x	185.8.x.x	tcp (6)	53999	microsoft-ds (445)	384	156	00000000	syn(2)	152.000 B	3.000 p	HSOC-VRF @ R
11.		ingress	Forwarde												R
12.		ingress	Forwarde												R
13.		ingress	Forwarde												R
14.		ingress	Forwarde												R
15.		ingress	Forwarde												R
16.		ingress	Forwarde												R
17.		ingress	Forwarde												R

o	Dst-IP	Protocol	TOS-flags	TCP-flags	Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Src-Port-Cnt	Dst-Port-Cnt
1.	185.8.x.x	tcp (6)	10100100	syn(2)	254.132 KB	5.776 Kp	19	29	1006
2.	185.8.x.x	tcp (6)	10110100	syn(2)	1.936 KB	37.000 p	19	27	18
3.	185.8.x.x	tcp (6)	10101100	syn(2), rst(4)	1.900 KB	42.000 p	25	28	15
4.	185.8.x.x	tcp (6)	10101100	syn(2), rst(4)	1.672 KB	35.000 p	18	20	11

ftas-soc – flow-based monitoring VRF

- **detekce anomálií, automat** (provoz přes perimetr hsoc-vr)
  - **pouze "síťová vrstva"** ~ L3-L5 – **co lze z principu odvodit z obsahu provozních informací**

Anomaly & security detections
flow_count_filter=src_ip
flow_count_filter_ipv4_bitmask=30
flow_count_filter_limit1=((matching_pkts_portion>90% or matching_octets_portion>90%) and matching_pktrate>=2) or matching_pktrate>100
flow_count_filter_limit2=matching_pktrate>=2 or (matching_pktrate>=2 and (dst_ip_cnt>1 or dst_port_cnt>1 or src_port_cnt>1))
flow_count_filter_evaluation_delay=60
flow_count_filter_evaluation_delay_max=300
flow_count_filter_use_statist_values=1
flow_count_filter_fragment_flows=1
Anomaly & security notifications (email)
flow_count_filter_notify=1
security_or_flow_count_notify_required_duration=20/0.7
security_or_flow_count_notify_to=[redacted]cesnet.cz
security_or_flow_count_notify_ttl=60
security_or_flow_count_notify_end_of_anomaly=1
X-FTAS-Report-Handling=[redacted]
security_or_flow_count_notify_record_count=100

use_fields_aggregate_time=2

Filtering conditions
filter_condition=[proto=6 and tcp_flags=[redacted] and tcp_flags<>[redacted] and flow_direction=0]
flow_source=[HSOC-VRF @ R[redacted] HSOC-VRF @ R[redacted]

ftas-soc – flow-based monitoring VRF

- notifikace detekovaných anomálií
  - overview

Subject: 195.178.[redacted]/30 (Src-IP) - '[redacted] detected @ HSOC-VRF border, source IPs' - 140. CONT.
Date: Thu, 26 Nov 2020 13:23:33 +0100 (CET)

```
Notification      : 195.178.[redacted]/30 (Src-IP) - '[redacted] detected @ HSOC-VRF border, source IPs'
Handling          : none
Events            : 5535 events detected (42x since last notification)

Summary, overview
  Duration        : 11124.653 seconds within 2020/11/26 10:16:43 - 2020/11/26 13:22:07
  Data sources    : HSOC-VRF @ R[redacted]
  Flows           : 2194.568 Kflows, 0.197 Kflows/s, no drops
  Pkts            : 2195.163 Kp, 0.197 Kp/s, no drops
  Bytes           : 96.585 MB, 0.069 Mb/s, 43.999 Bpp, no drops

Current event
  Duration        : 19.920 seconds within 2020/11/26 13:21:48 - 2020/11/26 13:22:07
  Data source     : HSOC-VRF @ R[redacted]
  Flows           : 390 flows, 19.578 flows/s, no drops
  Pkts            : 391 p, 19.629 p/s, no drops
  Bytes           : 17.2 KB, 6.908 Kb/s, 43.99 Bpp, no drops
  Src-IP/2        : 195.178.[redacted], 195.178.[redacted]
  Dst-IP/1        : 185.8.161.138
  Protocol/1      : tcp
  Src-Port/8      : 46196, 46197, 47983, 48239, 48240, 50565, 50566, 50567
  Dst-Port/64+    : 4, 26, 32, 212, 497, 1027, 1037, 1040, 1044, 1074, 1082, 1086, 1089, 1151,
1244, 1259, 1272, 1594, 1687, 1721, 1875, 2005, 2020, 2100, 2105, 2126, 2492, 2525, 3005, 303
3493, 3659,...
```

ftas-soc – flow-based monitoring VRF

- **notifikace detekovaných anomálií**
  - odkazy pro vyhledání v UI, vzorek provozu

```
Link to FTAS UI -> 'detector data only' query (valid 10 days, no guarantee that you have access there):
https://ftas-hsoc.cesnet.cz/ftas/stat.pl?go2=88a0056eae5e3b5b98483165a174308950acab906927bc2532227ecb6ee38849
Link to FTAS UI -> 'Flow Source data' query (valid 10 days, no guarantee that you have access there):
https://ftas-hsoc.cesnet.cz/ftas/stat.pl?go2=88a0056eae5e3b5b98483165a17430892468fe1a6610606bf53a5db9484113b7

Sample of corresponding traffic information (100 records max.):
Forwarded, ingress: 195.178.[redacted]  tcp(6)/50565 --> 185.8.[redacted]  tcp(6)/32 : 44/44 B, 1/1 p, 44 Bpp, 12:21:48[GMT], 13:21:48[CET +0100], +0.000000 s, tos=00000000, tcp_flags=
Forwarded, ingress: 195.178.[redacted]  tcp(6)/46197 --> 185.8.[redacted]  tcp(6)/1687: 44/44 B, 1/1 p, 44 Bpp, 12:21:48[GMT], 13:21:48[CET +0100], +0.000000 s, tos=00000000, tcp_flags
Forwarded, ingress: 195.178.[redacted]  tcp(6)/50566 --> 185.8.[redacted]  tcp(6)/eklogin(2105): 44/44 B, 1/1 p, 44 Bpp, 12:21:48[GMT], 13:21:48[CET +0100], +0.000000 s, tos=00000000,
Forwarded, ingress: 195.178.[redacted]  tcp(6)/50566 --> 185.8.[redacted]  tcp(6)/32 : 44/44 B, 1/1 p, 44 Bpp, 12:21:48[GMT], 13:21:48[CET +0100], +0.000000 s, tos=00000000, tcp_flags=
Forwarded, ingress: 195.178.[redacted]  tcp(6)/46196 --> 185.8.[redacted]  tcp(6)/41511: 44/44 B, 1/1 p, 44 Bpp, 12:21:48[GMT], 13:21:48[CET +0100], +0.000000 s, tos=00000000, tcp_flag
Forwarded, ingress: 195.178.[redacted]  tcp(6)/50567 --> 185.8.[redacted]  tcp(6)/32 : 44/44 B, 1/1 p, 44 Bpp, 12:21:48[GMT], 13:21:48[CET +0100], +0.000000 s, tos=00000000, tcp_flags=
Forwarded, ingress: 195.178.[redacted]  tcp(6)/50565 --> 185.8.[redacted]  tcp(6)/1154: 44/44 B, 1/1 p, 44 Bpp, 12:21:48[GMT], 13:21:48[CET +0100], +0.000000 s, tos=00000000, tcp_flags
Forwarded, ingress: 195.178.[redacted]  tcp(6)/50565 --> 185.8.[redacted]  tcp(6)/5800: 44/44 B, 1/1 p, 44 Bpp, 12:21:48[GMT], 13:21:48[CET +0100], +0.000000 s, tos=00000000, tcp_flags
```

ftas-soc – flow-based monitoring VRF

- regulace provozu, +notifikace

```
################################################################################
# EXAFS traffic control for this detector: ACTIVE mode                         #
# will add 1 'rtbh' rules to community 'RTBH vrf Nemocnice' (id=4) - configured=0, limit=2   #
# RTBH rule added                                                              #
# ipv4       : 195.178.[redacted]                                              #
# ipv4_mask  : 30                                                              #
# expires    : 2020/11/26 14:10                                                #
# comment    : FTAS - src_ip=195.178.[redacted] detected @ HSOC-VRF border, source IPs      #
#  (detector_id=7)                                                             #
# community  : 4                                                               #
################################################################################
```

All RTBH rules that you can modify

IP adress (v4 or v6)	Community	Expires	User	Edit	
195.178.[redacted] / 30	RTBH vrf Nemocnice	2020/11/26 14:10	FTAS		

aktuální stav, k řešení do budoucnosti

- přístup k UI – *komunitní CSIRT ?*
- provozní údaje celé VRF
  - nestrukturované (jinak to nedává smysl) ...*GDPR*
- řešení flow-based monitoringu pro konkrétní organizace ?
  - mimo tuto instanci systému

ftas-soc – flow-based monitoring VRF

- **L3 flow-based monitoring provozu organizace pro zájemce**

- pokud nemáte svůj vlastní monitoring
- informace o provozu organizace (zpravidla na perimetru, lze detailněji)
- bez ohledu na to, kde a ke komu jsou připojeni
- možnost zpracování, uchování a zpřístupnění provozních informací systémem FTAS
  - ve vhodné instanci systému
    - v e-infrastruktuře
    - někde jsou k dispozici krajské instance (po dohodě s IT kraje)
    - samostatná instalace na vlastním HW uživatele

cesnet

Děkuji za pozornost.