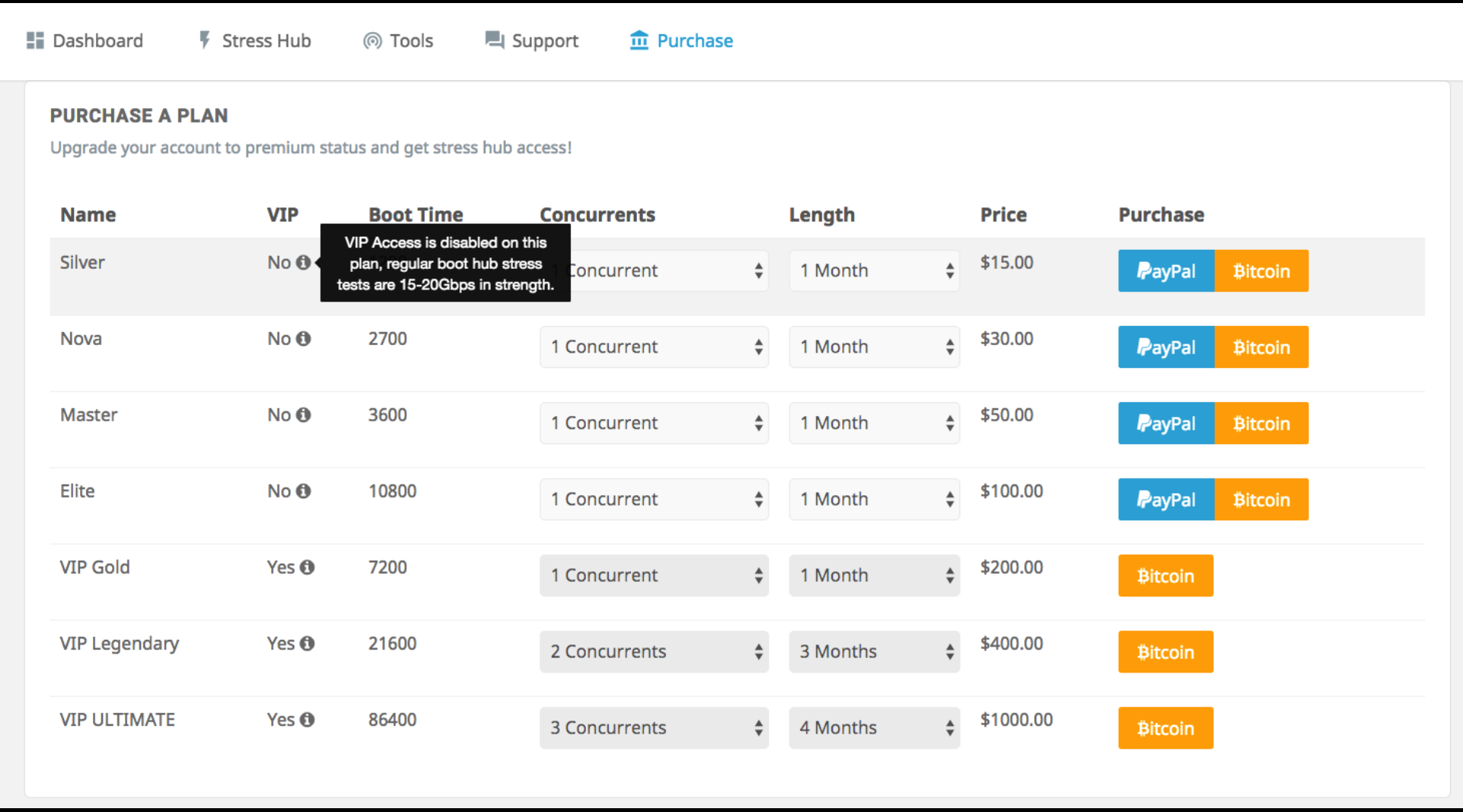
Analýza a mitigace DDoS útoků

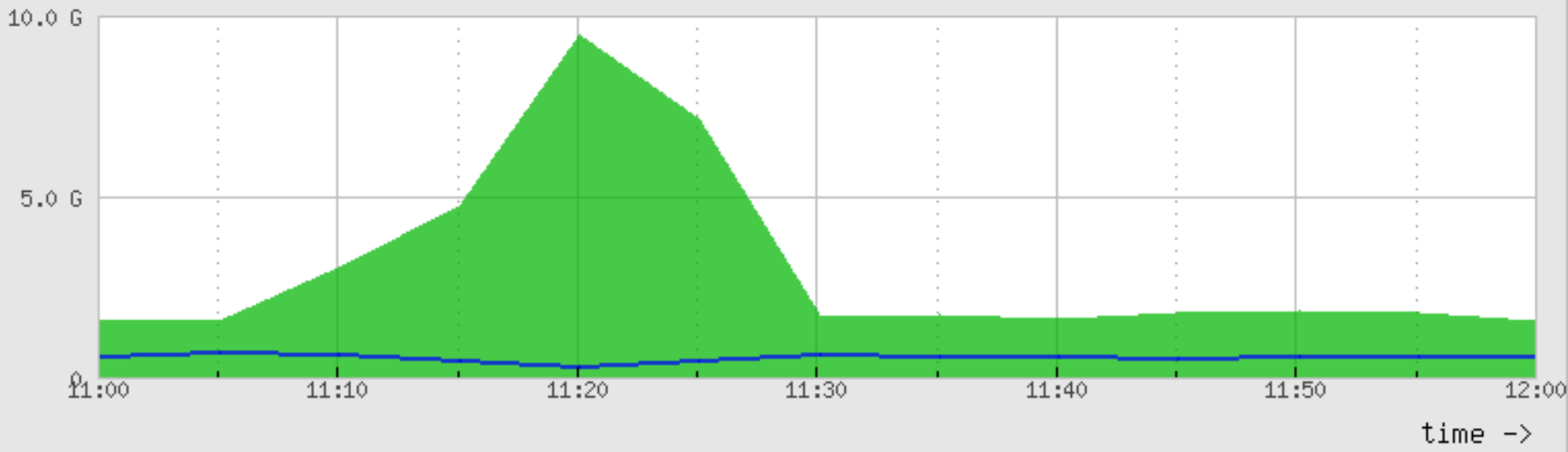
Tomáš Podermański
tpoder@vut.cz

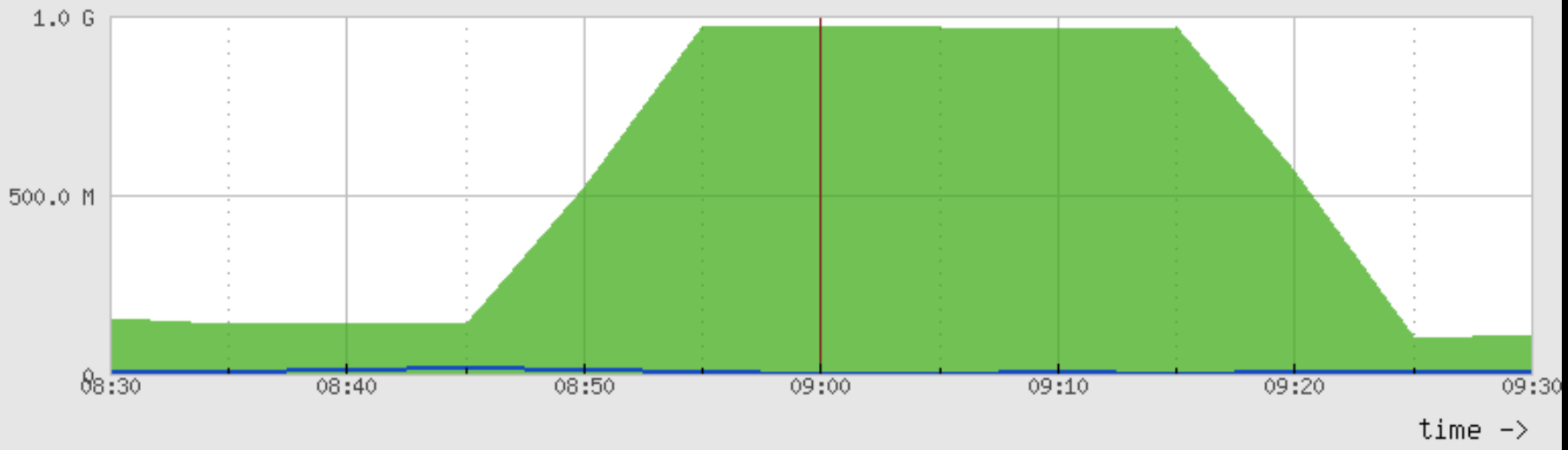
Náklady

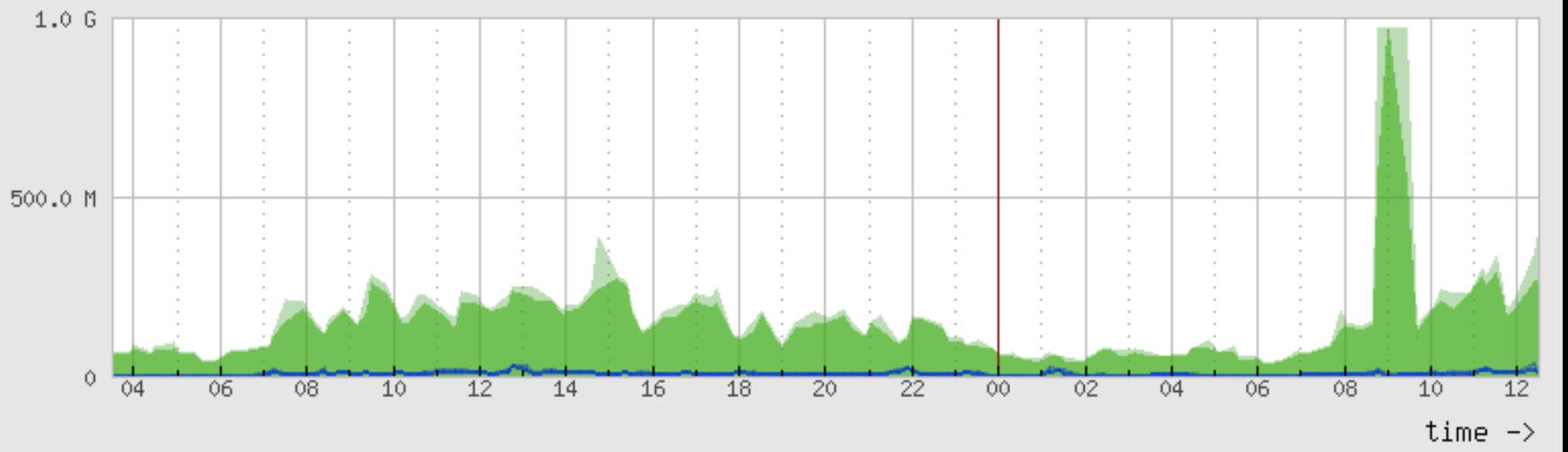
Škody

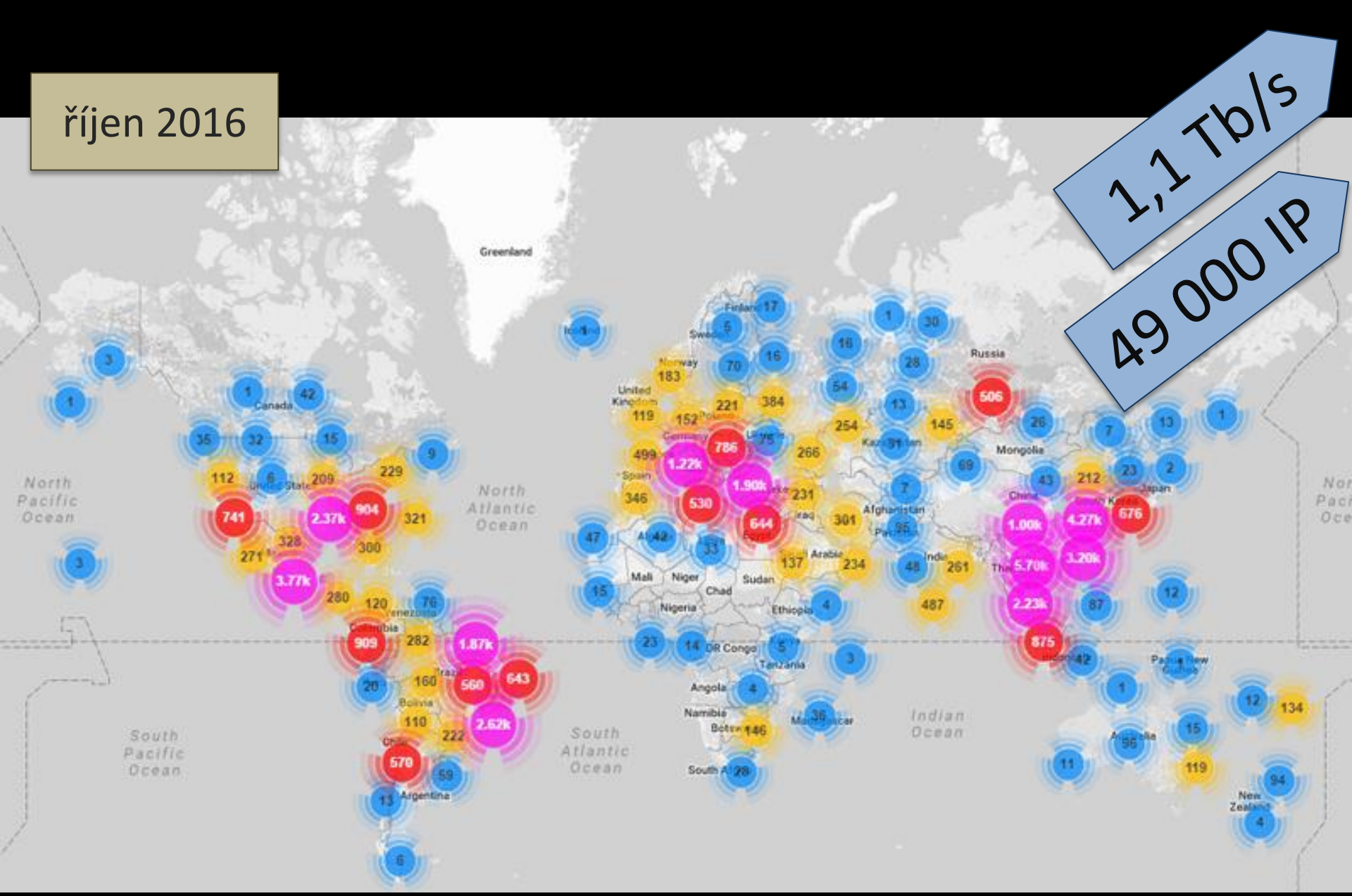

Dashboard
Stress Hub
Tools
Support
Purchase
PURCHASE A PLAN
Upgrade your account to premium status and get stress hub access!
Name
VIP
Boot Time
Concurrents
Length
Price
Purchase
Silver
No
VIP Access is disabled on this plan, regular boot hub stress tests are 15-20Gbps in strength.
Concurrent
1 Month
$15.00
PayPal
Bitcoin
Nova
No
2700
1 Concurrent
1 Month
$30.00
PayPal
Bitcoin
Master
No
3600
1 Concurrent
1 Month
$50.00
PayPal
Bitcoin
Elite
No
10800
1 Concurrent
1 Month
$100.00
PayPal
Bitcoin
VIP Gold
Yes
7200
1 Concurrent
1 Month
$200.00
Bitcoin
VIP Legendary
Yes
21600
2 Concurrents
3 Months
$400.00
Bitcoin
VIP ULTIMATE
Yes
86400
3 Concurrents
4 Months
$1000.00
Bitcoin

Date end : 2015-10-15T10:02:00
Data : pe-kou.mgmt.net.vutbr.cz/ten-gigabitethernet1:0:40
Info : 10G CESNET-VUT

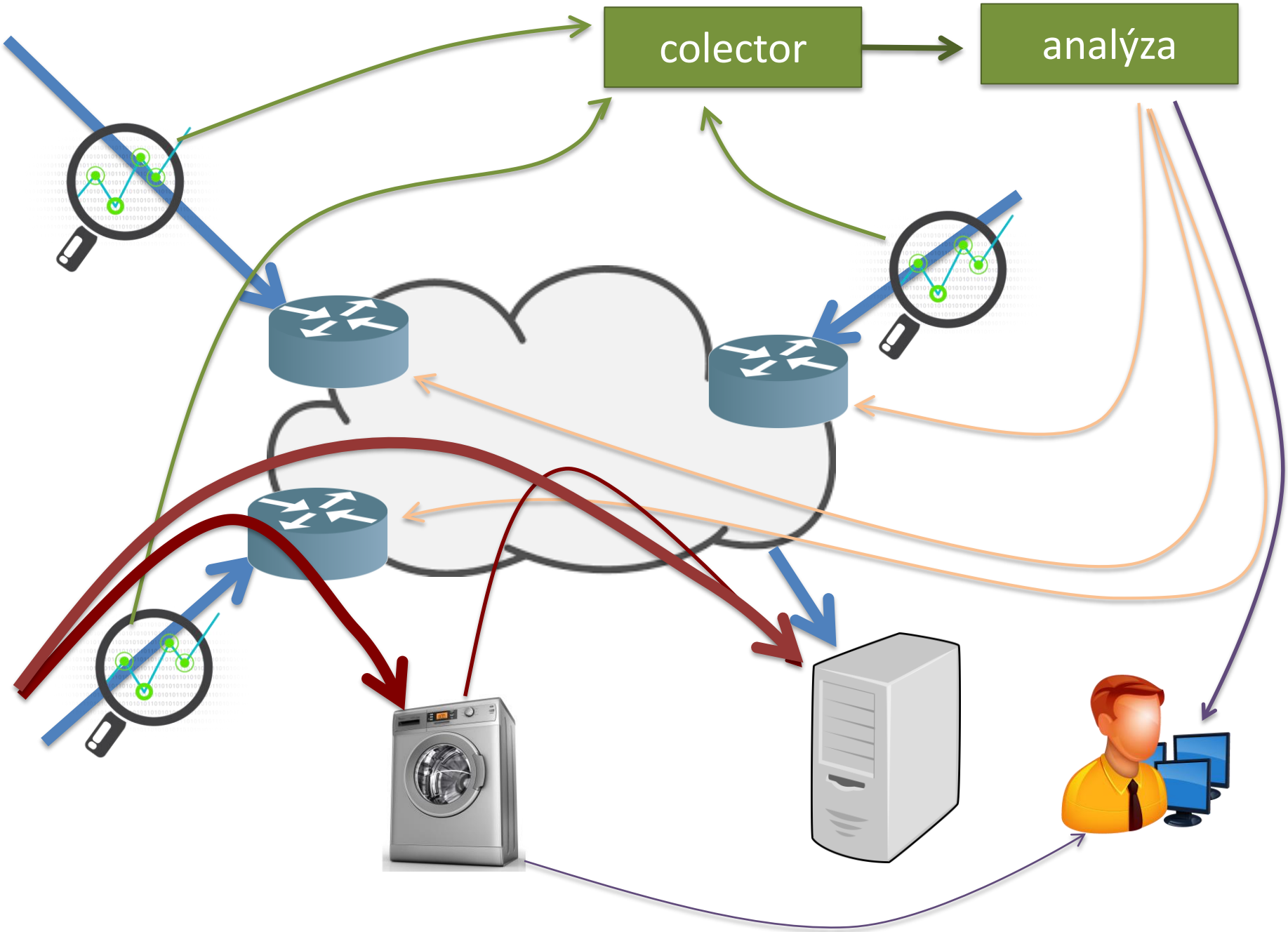



1.0 G
500.0 M
0
08:30
08:40
08:50
09:00
09:10
09:20
09:30
time ->
avg max last
In 518.23M 971.4M 112.34M
Out 6.7M 18.4M 7.89M


1.0 G
500.0 M
0
04
06
08
10
12
14
16
18
20
22
00
02
04
06
08
10
12
time ->
avg max last
In 167.02M 971.4M 272.6M
Out 8.01M 32.74M 11.61M


říjen 2016
1,1 Tb/s
49 000 IP
Greenland
North Pacific Ocean
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Canada
Russia
Mongolia
Japan
Norway
United Kingdom
Spain
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
DR Congo
Tanzania
Angola
Namibia
Afghanistan
Argentina
New Zealand

```
120     tcph->window = rand_next() & 0xffff;
121     tcph->syn = TRUE;
122
123     // Set up passwords
124     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                  // root     xc3511
125     add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                       // root     vizxv
126     add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                       // root     admin
127     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                   // admin    admin
128     add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                   // root     888888
129     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);               // root     xmhdipc
130     add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);               // root     default
131     add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);           // root     juantech
132     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                   // root     123456
133     add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                       // root     54321
134     add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);   // support  support
135     add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                           // root     (none)
136     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);       // admin    password
137     add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                           // root     root
138     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                       // root     12345
139     add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                           // user     user
140     add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                       // admin    (none)
141     add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                           // root     pass
142     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);   // admin    admin1234
143     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                           // root     1111
144     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);       // admin    smcadmin
145     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                       // admin    1111
146     add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                   // root     666666
147     add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);           // root     password
148     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                           // root     1234
149     add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);                   // root     klv123
150     add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x4F\x47\x4B\x4C\x51\x4F", 1); // Administrator admin
151     add_auth_entry("\x51\x47\x50\x54\x4B\x41\x47", "\x51\x47\x50\x54\x4B\x41\x47", 1);   // service  service
152     add_auth_entry("\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", "\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", 1); // supervisor supervisor
153     add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1);                   // guest    guest
154     add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);                   // guest    12345
```


colector
analýza

NetFlow/IPFIX

colector

analýza

BGP FlowSpec

Email,IDEA

1 – 5 min

0 – 5 min

< 10 sec

1 - 5 min

1 - 5 min

Několik poznámek

- Rostoucí rafinovanost DDoS útoků.
- DDoS útoky kombinované a proměnlivé v čase.
- Velmi dobrá znalost útočníků o zdrojovém a cílovém prostředí.
- Integrace detekčních a mitigačních nástrojů, rozumná reakční doba.
- Ohrožování okolí námi samotnými.
- Ekonomické aspekty DDoS.

Spolupráce – CESNET DDoS Protector

Analýza provozu

- Tvorba nástroju pro lepší orentaci v datech
  - Nástroj nfddos – analýza na základě netflow dat v reálném čase s odchycením provozu/paketů souvisejících s DDoS útokem.
  - Primární účel lepší porozumění charakteru útoku/útoků.

Mitigace DDoS

- Levná mitigace DDoS
  - Podkladem popis ddos útoku (např. DDoS Defender, jiný zdroj na bázi Flow Spec)
  - Filtrační jednotka - vysoké rychlosti/nízká cena
    - Síťový prvek s podporou FlowSpec
    - Autonomní zařízení – wire speed filtrace
- Testovací DDoS laboratoř