# Mitigando Ataques DDoS Usando NFSEN e se defendendo.

Alexandre Giovaneli

GTS 29

Grupo de trabalho de Segurança

# Conteúdo:

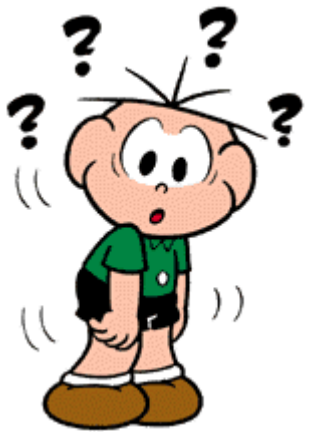
- A apresentação
- Vantagens e desvantagens de usar plataformas open source como o quagga.
- Orientando sobre qual o sistema operacional ideal para a função de quagga.
- Selecionando Hardware de baixo custo e Troughhput suportado
- Aplicações deste roteador.
- Instalando Sistema operacional FREEBSD
- Instalando o Quagga  e configurando.
  - Daemon
  - IPV4  E IPV6
  - Rota estática IPV4 E IPV6
  - OSPF e  OSPFV3
  - BGP IPV4 E IPV6
  - Filtros e comunidades como exemplo as do IX.SP
- Ajustes finos
- Sugestões e discussão

# Objetivo

- Conscientizar da extrema importância de se usar uma ferramenta de analise de trafego , e saber quais serviços estão realmente rodando em sua rede e  usando a favor do AS  estas ferramentas para  a detecção dos ataques volumétricos como o descrito nesta apresentação o DDoS e mitigando  também rapidamente e com eficiência.

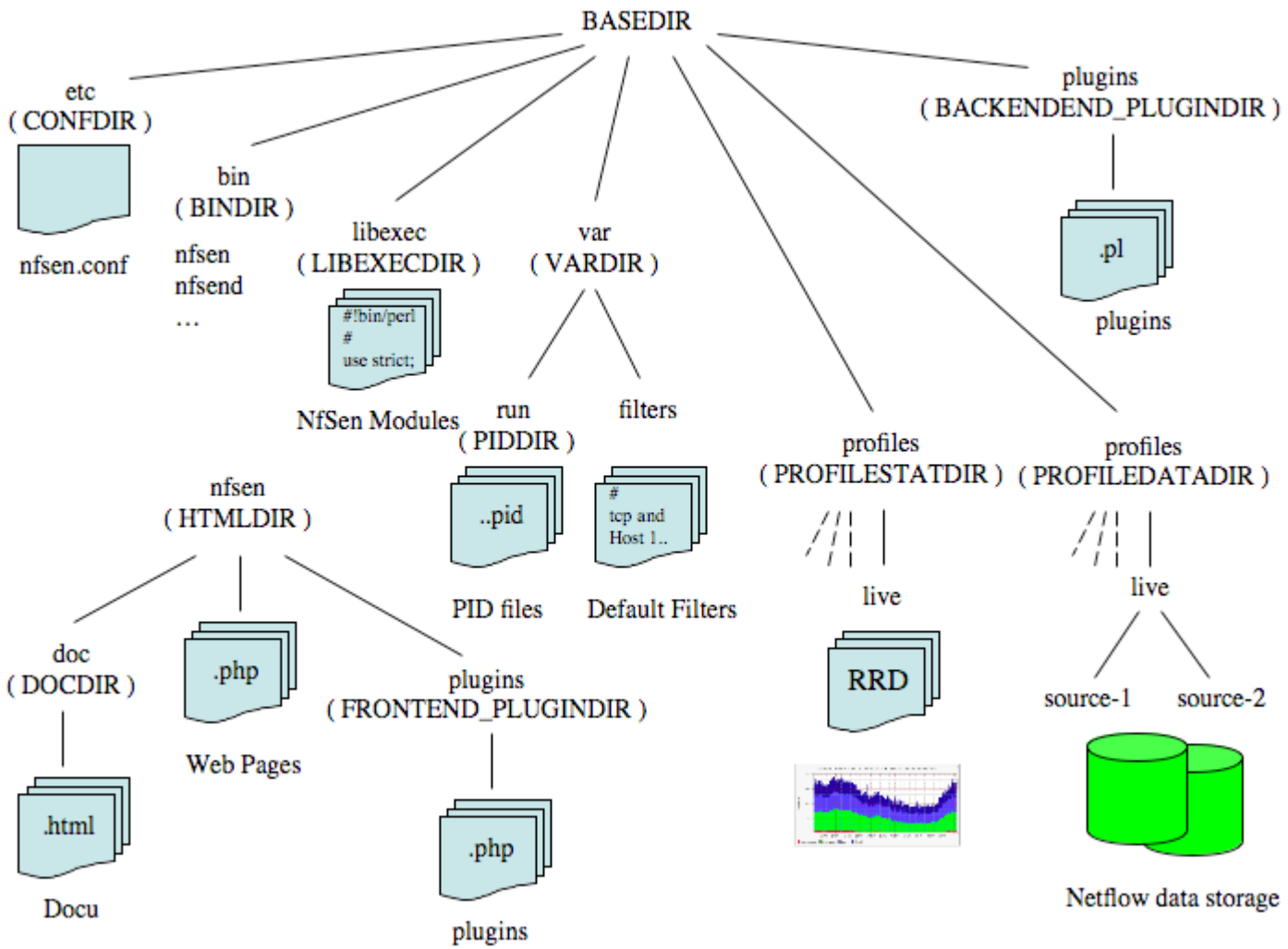
# O que é NfSen ?

- NfSen é um front-end gráfico baseado na web para as ferramentas nfdump netflow.
  - NfSen permite que você:
    - Exibir seus dados de fluxo de rede: fluxos, pacotes e bytes usando RRD (Round Robin Database).
      - Navegue facilmente pelos dados do netflow.
      - Processar os dados de fluxo de rede dentro do intervalo de tempo especificado.
      - Crie histórico, bem como perfis contínuos.
      - Defina alertas, com base em várias condições.
      - Escreva seus próprios plugins para processar dados do netflow em intervalos regulares.
      - Diferentes tarefas precisam de interfaces diferentes para seus dados de fluxo de dados. O NfSen permite que você mantenha todas as vantagens convenientes da linha de comando usando nfdump diretamente e dá-lhe também uma visão geral gráfica sobre seus dados de netflow.
        **NfSen está disponível em  sourceforge e distribuído sob a licença BSD .**



Fonte: http://nfsen.sourceforge.net/#mozTocId764303

# Estrutura NfSen



# Instalando o Nfsen no Debian

Alexandre Giovaneli

Gerente de Redes

# Observações:

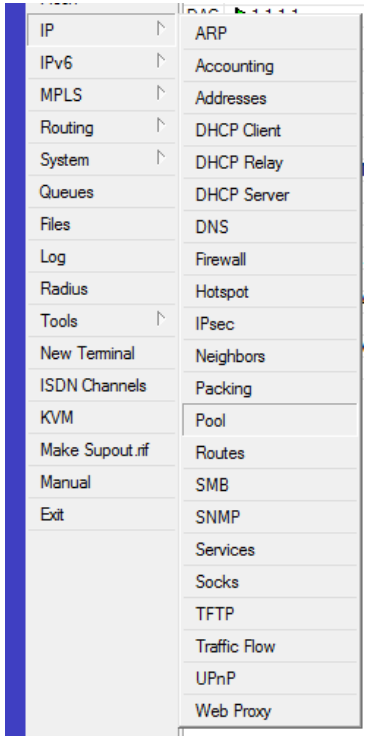
- Por ser fácil de instalar o debian, não colocamos o tutorial de instalação aqui, caso tenha necessidade segues os links
  - https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi39KSX2fTTAhXFTZAKHdXiD94QFggsMAE&url=https%3A%2F%2Fwww.debian.org%2Freleases%2Fjessie%2Fi386%2Findex.html.pt&usg=AFQjCNH4qEl316tyDev4HBdW2WMxR3sU1Q&sig2=oCQ2tzaedBDPYmIr18QioA
  - https://www.youtube.com/watch?v=pH1tkTYm9rg
  - www.google.com.br
- Na instalação do debian Selecione as opções abaixo para facilitar no trabalho:
  - SSH SERVER
  - SERVIDOR WEB

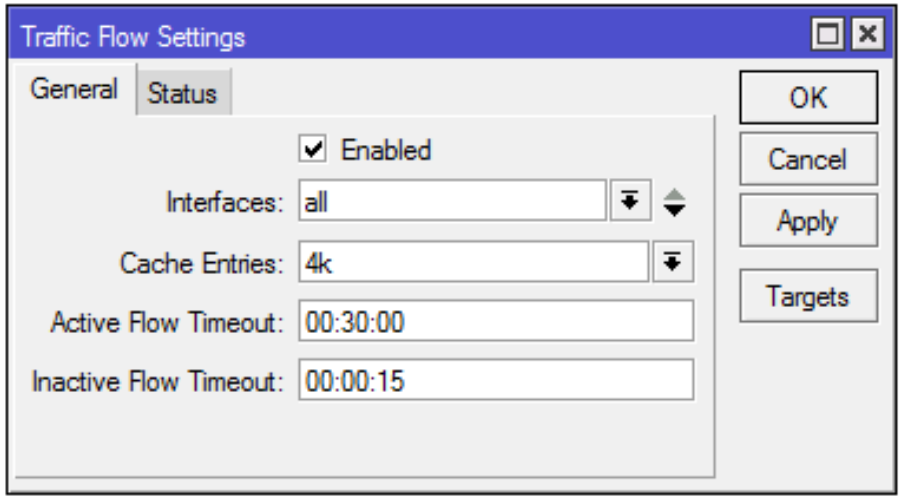
# Configuração do Coletor de dados NFDUMP

- O NFDUMP faz parte das ferramentas para acoletar os fluxos eviados pelos roteadores e swiches da rede.
- Em modo sudo  ( su )
  - apt-get install build-essential
  - apt-get install rrdtool mrtg librrds-perl librrdp-perl librrd-dev \
    libmailtools-perl php5 bison flex
  - cd
  - wget https://ufpr.dl.sourceforge.net/project/nfdump/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz
  - tar xvzf nfdump-1.6.13.tar.gz
  - cd nfdump-1.6.13
  - ./configure --enable-nfprofile --enable-nftrack
  - make
  - make install

# Para testar o NFDUMP

- Configurando o flow no seu roteador Mikrotik
  - Vá até IP>Traffic FLOW

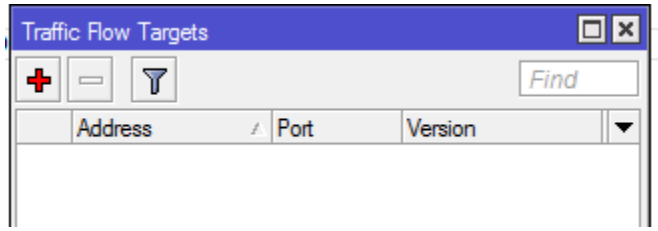


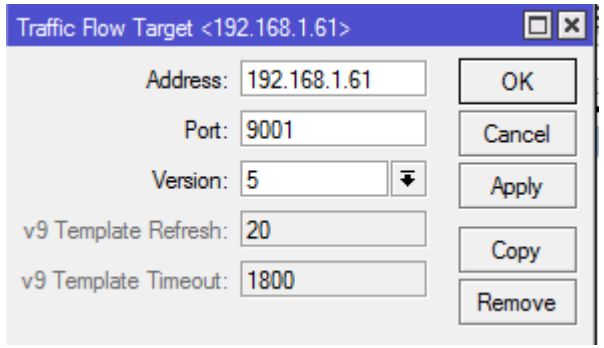

  - Clique em Targets

# Para testar o NFDUMP

- Clique em +




- Em  traffic flow target coloque o ip do servidor em configuração do FLOW e porta 9001 versio 5.



# Para testar o NFDUMP

- mkdir /tmp/nfcap-teste
- nfcapd -E  -p 9001 -l /tmp/nfcap-teste
- nfdump -r /tmp/nfcap-test/nfcapd.20**(aperte tab)** | less
- nfdump -r /tmp/nfcap-test/nfcapd.20**(aperte tab)** **-**s srcip/bytes

- Se aparecer algo assim seu flow já esta coletando gráfico, se não aparecer aguarde  5 minutos, ou verifique se existe firewall ativo entre seu roteador e o servidor de flow.

| ate first seen | Duration | Proto | Src IP Addr:Port | | Dst IP Addr:Port | Packets | Bytes | Flows |
|---|---|---|---|---|---|---|---|---|
| 017-05-16 11:52:25.178 | 0.000 | TCP | 192.168.1.216:40957 | -> | 177.66.103.206:1723 | 7 | 704 | 1 |
| 017-05-16 11:52:25.238 | 0.000 | TCP | 177.66.103.206:1723 | -> | 192.168.1.216:40957 | 5 | 464 | 1 |
| 017-05-16 11:52:27.118 | 0.000 | TCP | 192.168.1.216:40951 | -> | 177.66.103.206:1723 | 2 | 136 | 1 |
| 017-05-16 11:52:27.188 | 0.000 | TCP | 177.66.103.206:1723 | -> | 192.168.1.216:40951 | 2 | 80 | 1 |
| 017-05-16 11:52:27.508 | 0.000 | TCP | 192.168.1.216:46512 | -> | 167.249.236.17:1723 | 2 | 136 | 1 |
| 017-05-16 11:52:29.108 | 0.000 | TCP | 172.16.0.243:57689 | -> | 207.46.155.178:443 | 4 | 431 | 1 |
| 017-05-16 11:52:29.458 | 0.000 | TCP | 207.46.155.178:443 | -> | 172.16.0.243:57689 | 3 | 221 | 1 |
| 017-05-16 11:52:25.388 | 4.230 | GRE | 192.168.1.216:0 | -> | 177.66.103.206:0 | 26 | 1275 | 1 |
| 017-05-16 11:52:29.668 | 0.000 | TCP | 172.16.0.243:57705 | -> | 31.13.85.4:443 | 3 | 120 | 1 |
| 017-05-16 11:52:29.738 | 0.000 | TCP | 31.13.85.4:443 | -> | 172.16.0.243:57705 | 3 | 182 | 1 |
| 017-05-16 11:52:32.278 | 0.000 | TCP | 167.249.236.17:1723 | -> | 192.168.1.216:46519 | 3 | 156 | 1 |
| 017-05-16 11:52:32.508 | 0.000 | UDP | 172.16.0.243:54159 | -> | 94.245.121.253:3544 | 2 | 178 | 1 |
| 017-05-16 11:52:32.748 | 0.000 | TCP | 192.168.1.216:46519 | -> | 167.249.236.17:1723 | 2 | 128 | 1 |
| 017-05-16 11:52:32.798 | 0.000 | UDP | 94.245.121.253:3544 | -> | 172.16.0.243:54159 | 2 | 274 | 1 |
| 017-05-16 11:52:33.008 | 0.000 | TCP | 192.168.1.216:46525 | -> | 167.249.236.17:1723 | 7 | 704 | 1 |
| 017-05-16 11:52:33.068 | 0.000 | TCP | 167.249.236.17:1723 | -> | 192.168.1.216:46525 | 5 | 464 | 1 |

# Instalando NFSEN

- Para instalar o NFSEN digite os seguintes comandos
  - cd
  - wget https://ufpr.dl.sourceforge.net/project/nfsen/stable/nfsen-1.3.8/nfsen-1.3.8.tar.gz
  - tar xvzf nfsen-1.3.8.tar.gz
  - cd nfsen-1.3.8
  - cd etc
  - cp nfsen-dist.conf nfsen.conf

# Instalando NFSEN

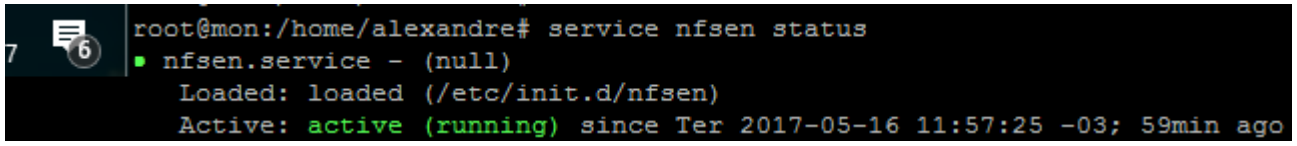
- Edite o arquivo nfsen.conf as linhas (nano nfsen.conf):
  - $BASEDIR = "/var/nfsen";
  - $WWWUSER = 'www-data';
  - $WWWGROUP = 'www-data';
  - $BUFFLEN = 2000;

```
%sources=(
'rtrX' => {'port'=>'9001','col'=>'#0000ff','type'=>'netflow'},
 );
```

  - $HTMLDIR    = "/var/www/html/nfsen/";
  - Para sair no nano aperte **CTRL + X depois S**

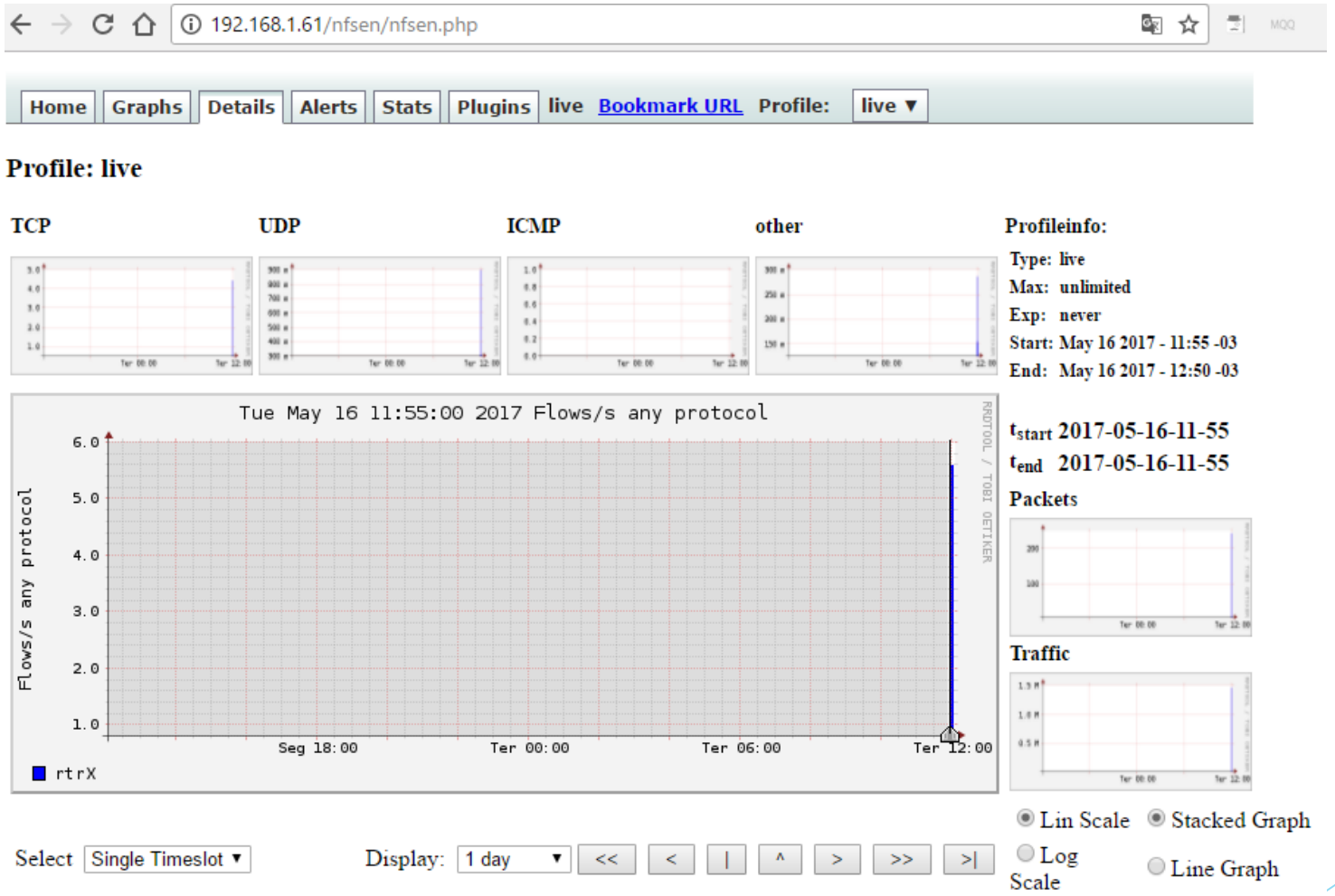
# Instalando NfSen

- Criando usuário para o NETFLOW dentro do sistema
  - useradd -d /var/nfsen -G www-data -m -s /bin/false netflow
- Agora finalmente instalando o NFSEN
  - cd
  - cd nfsen-1.3.8
  - perl install.pl etc/nfsen.conf
- Configurando o script de inicialização do NfSen
  - ln -s /var/nfsen/bin/nfsen /etc/init.d/nfsen
  - update-rc.d nfsen defaults 20
- Inicializando NfSen
  - service nfsen start
  - service nfsen status (para verificar se o serviço subiu)

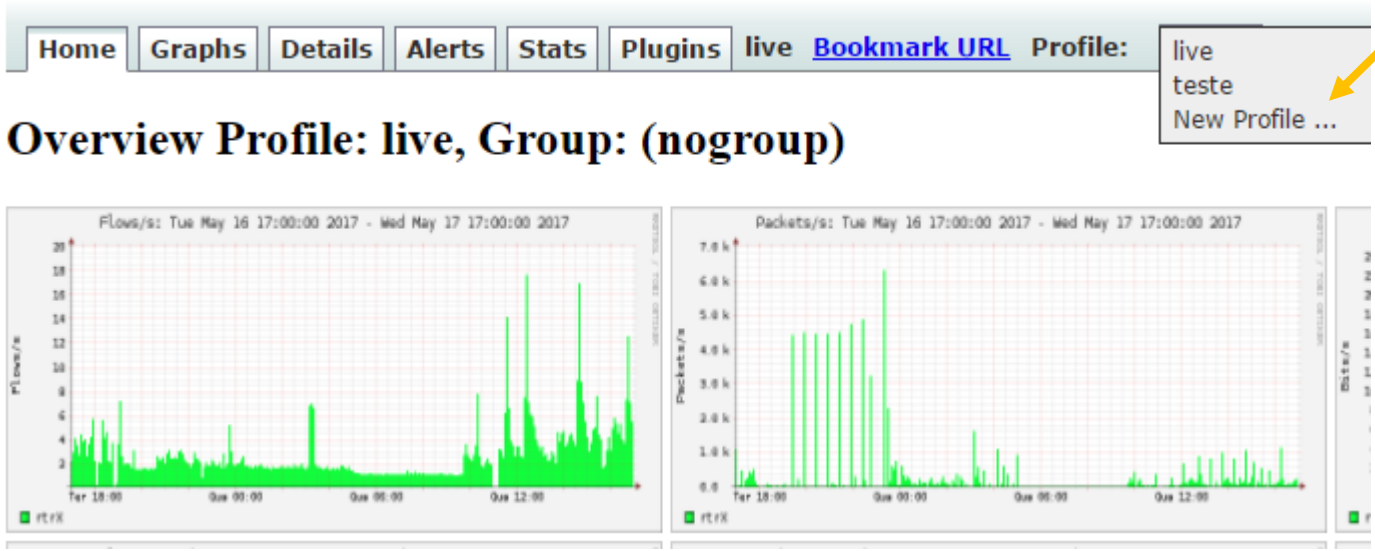


# Acessando NfSEN

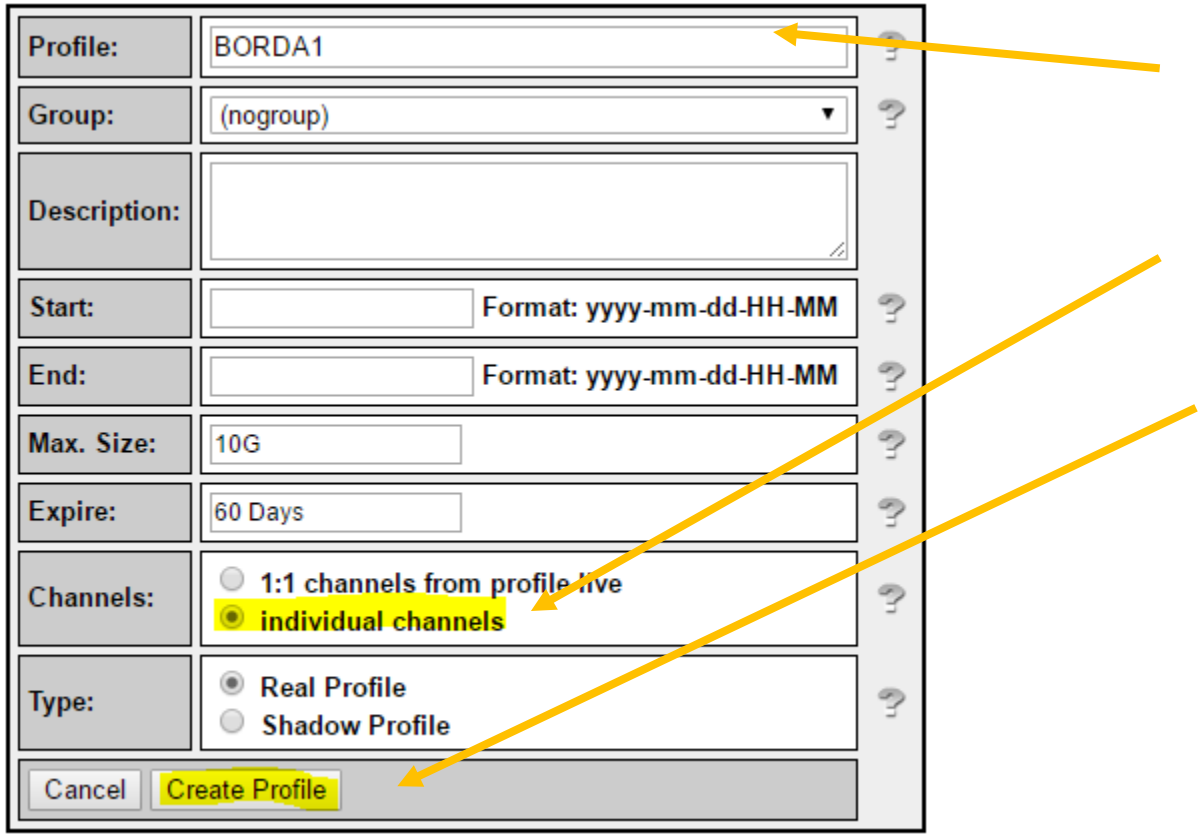
- http://ip.do.servidor/nfsen/nfsen.php



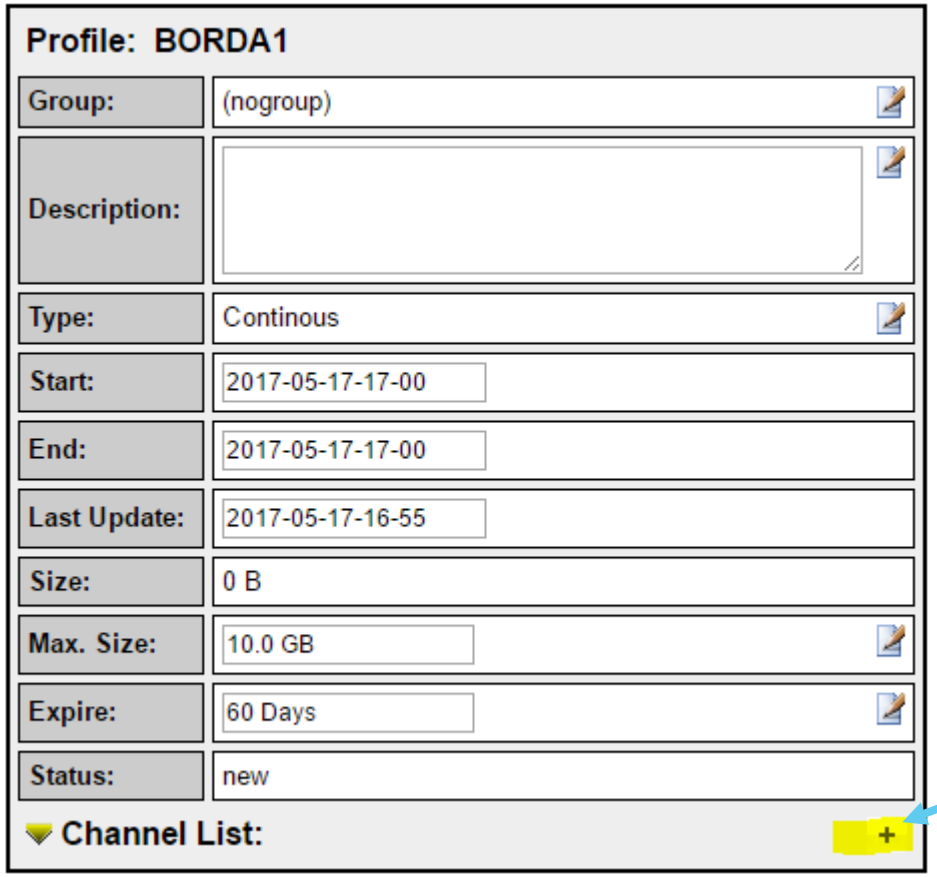
# Configurando Perfis de leitura no NfSen e filtros



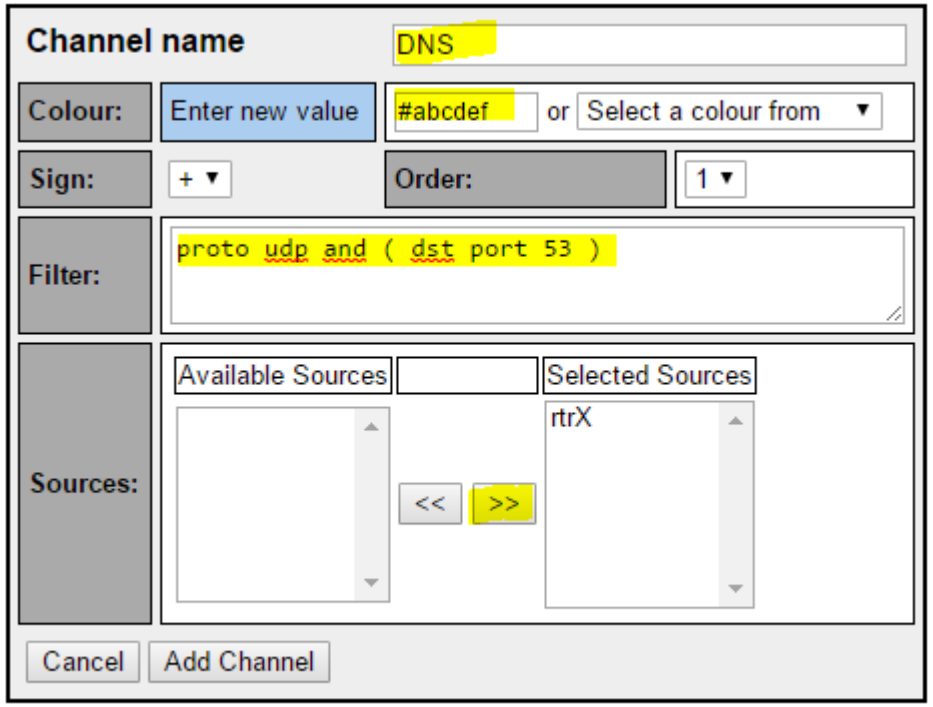
# Criando perfil de coleta



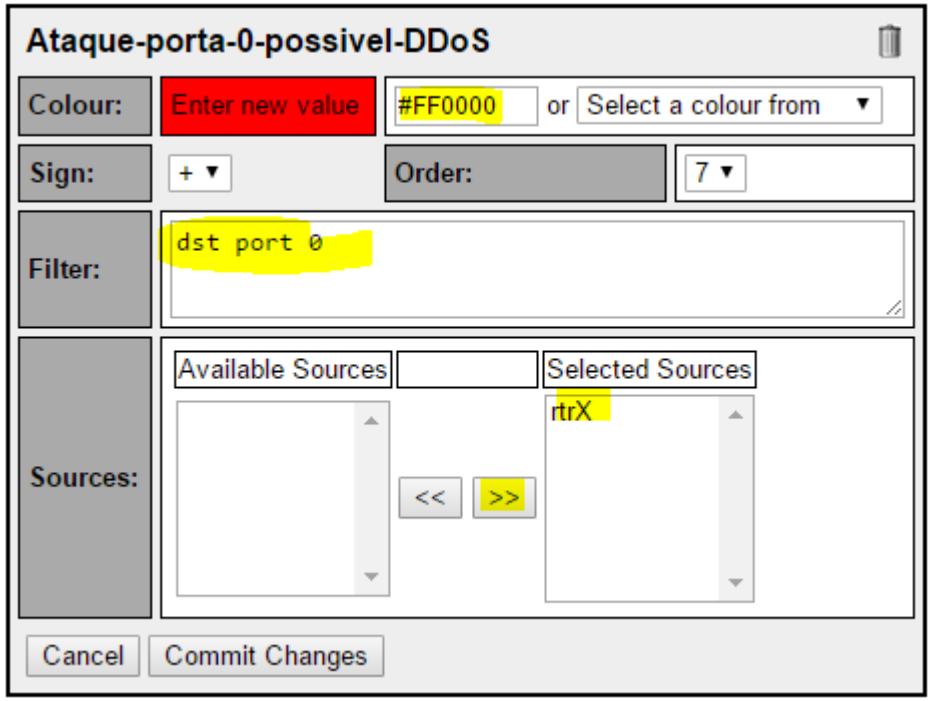
# Criando perfil de coleta



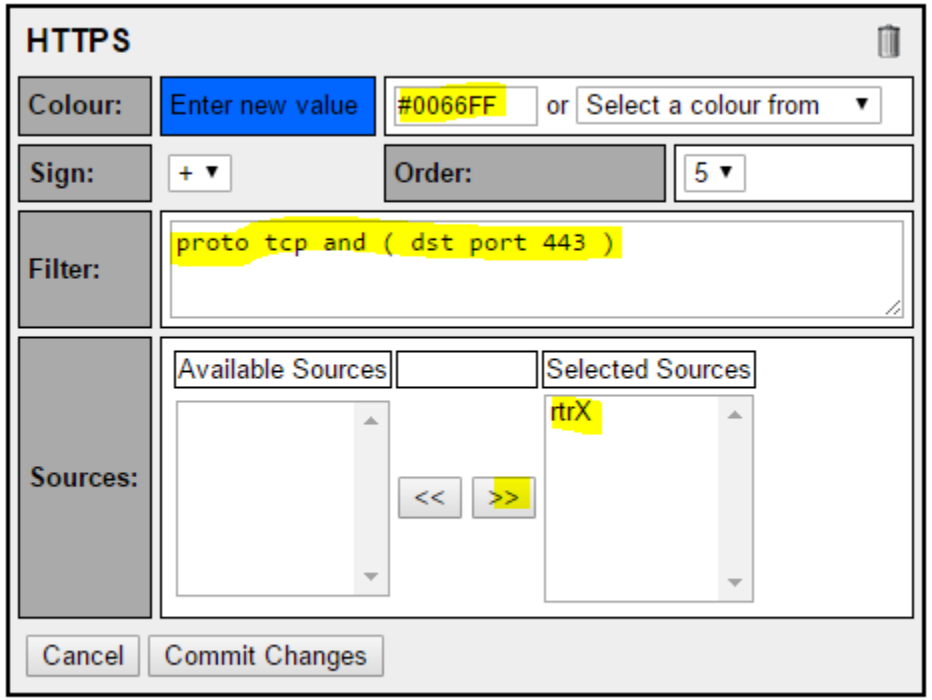
# Filtro DNS


Channel name
DNS
Colour:
Enter new value
#abcdef
or
Select a colour from
Sign:
+
Order:
1
Filter:
proto udp and ( dst port 53 )
Sources:
Available Sources
Selected Sources
rtrX
<<
>>
Cancel
Add Channel

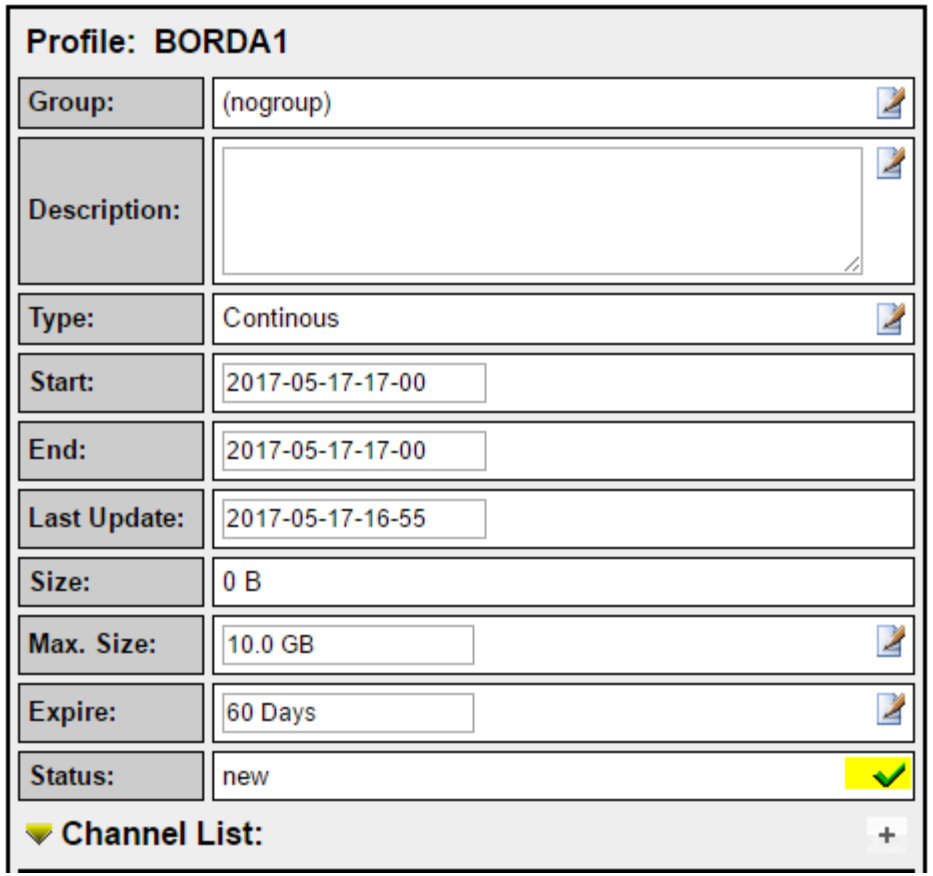
# Filtro ataque porta 0 DDoS  (o mais comum dos ataques)



# Filtro HTTPS



# Finalizando o perfil

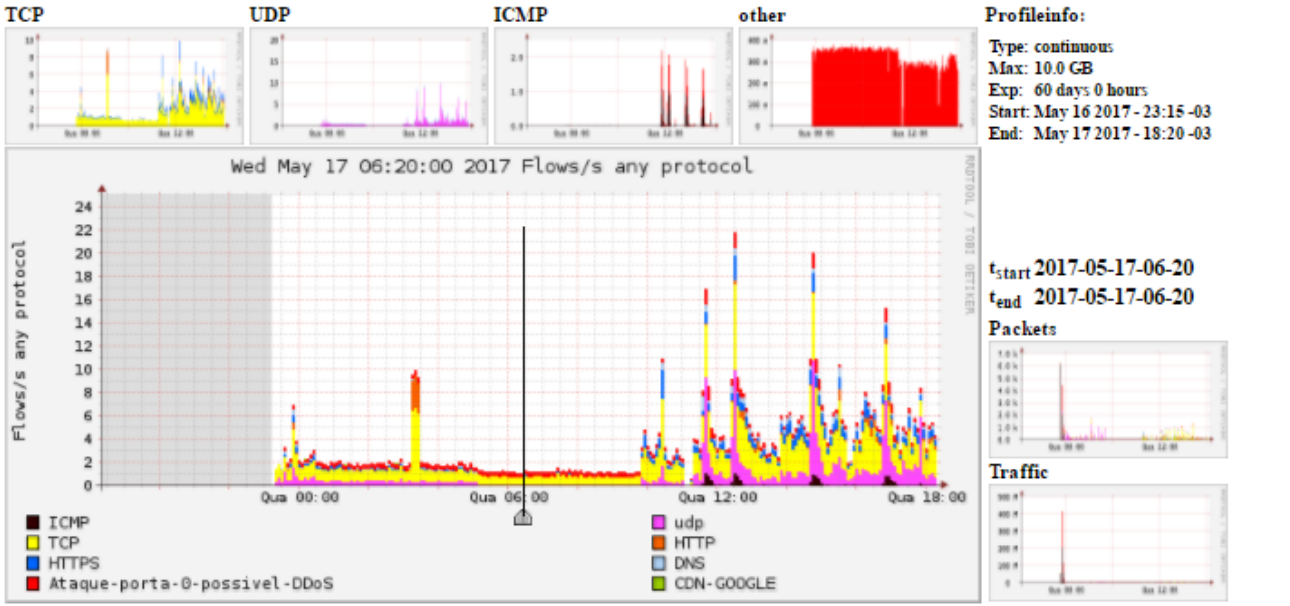


# Alguns exemplos de filtros

- Proto tcp and ( src ip 172.16.17.18 or dst ip 172.16.17.19)
- Proto tcp and ( net 172.16/16 and src port > 1024 and dst port 80 ) and bytes > 2048
- Proto tcp and ( net 172.16/16 and src port > 1024 and dst port 80 ) and bytes > 2048

# Resultado

**Profile: teste**




**Profileinfo:**

Type: continuous
Max: 10.0 GB
Exp: 60 days 0 hours
Start: May 16 2017 - 23:15 -03
End: May 17 2017 - 18:20 -03

$t_{start}$ 2017-05-17-06-20
$t_{end}$ 2017-05-17-06-20

**Packets**



**Traffic**



Select Single Timeslot ▼ Display: 1 day ▼ << < | ^ > >> >|

Lin Scale Stacked Graph
Log Scale Line Graph

**Statistics timeslot May 17 2017 - 06:20**

| Channel: | Flows: | | | | | Packets: | | | | | Traffic: | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: |
| CDN-GOOGLE | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 b/s | 0 b/s | 0 b/s | 0 b/s | 0 b/s |
| Ataque-porta-0-possivel-DDoS | 0.4 /s | 0 /s | 0 /s | 0 /s | 0.4 /s | 3.5 /s | 0 /s | 0 /s | 0 /s | 3.5 /s | 1.9 kb/s | 0 b/s | 0 b/s | 0 b/s | 1.9 kb/s |
| DNS | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 b/s | 0 b/s | 0 b/s | 0 b/s | 0 b/s |
| HTTPS | 0.0 /s | 0.0 /s | 0 /s | 0 /s | 0 /s | 0.0 /s | 0.0 /s | 0 /s | 0 /s | 0 /s | 4.3 b/s | 4.3 b/s | 0 b/s | 0 b/s | 0 b/s |
| HTTP | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 b/s | 0 b/s | 0 b/s | 0 b/s | 0 b/s |
| TCP | 0.6 /s | 0.6 /s | 0 /s | 0 /s | 0 /s | 2.6 /s | 2.6 /s | 0 /s | 0 /s | 0 /s | 1.6 kb/s | 1.6 kb/s | 0 b/s | 0 b/s | 0 b/s |
| udp | 0.1 /s | 0 /s | 0.1 /s | 0 /s | 0 /s | 0.3 /s | 0 /s | 0.3 /s | 0 /s | 0 /s | 225.6 b/s | 0 b/s | 225.6 b/s | 0 b/s | 0 b/s |
| ICMP | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 b/s | 0 b/s | 0 b/s | 0 b/s | 0 b/s |
| | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: |
| TOTAL | 1.1 /s | 0.6 /s | 0.1 /s | 0 /s | 0.4 /s | 6.5 /s | 2.6 /s | 0.3 /s | 0 /s | 3.5 /s | 3.7 kb/s | 1.6 kb/s | 225.6 b/s | 0 b/s | 1.9 kb/s |

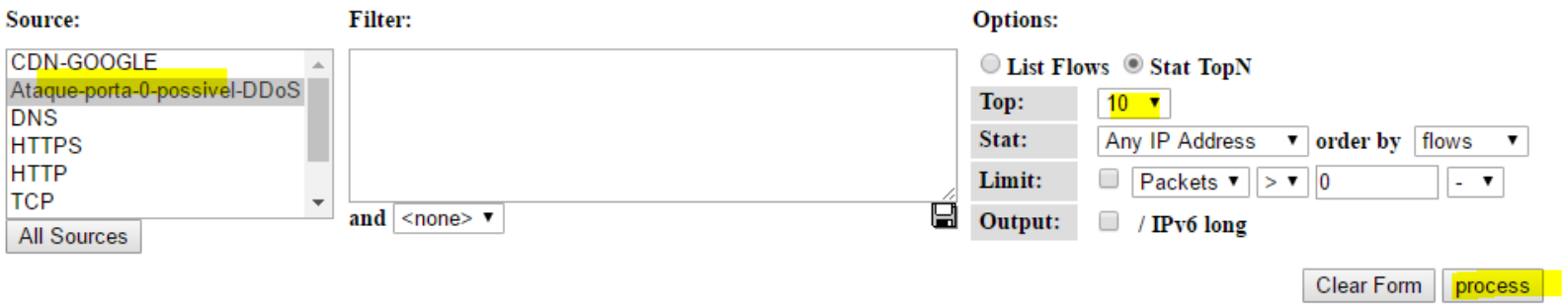
# Consulta de uma simulação de ataque DDoS porta 0

Statistics timeslot May 16 2017 - 23:35

| Channel: | Flows: | | | | | Packets: | | | | | Traffic: | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: |
| CDN-GOOGLE | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 /s | 0 b/s | 0 b/s | 0 b/s | 0 b/s | 0 b/s |
| Ataque-porta-0-possivel-DDoS | 0.4 /s | 0 /s | 0 /s | 0.0 /s | 0.3 /s | 2.1 k/s | 0 /s | 0 /s | 2.1 k/s | 3.5 /s | 208.5 Mb/s | 0 b/s | 0 b/s | 208.5 Mb/s | 1.8 kb/s |
| DNS | 0.2 /s | 0 /s | 0.2 /s | 0 /s | 0 /s | 0.5 /s | 0 /s | 0.5 /s | 0 /s | 0 /s | 281.6 b/s | 0 b/s | 281.6 b/s | 0 b/s | 0 b/s |
| HTTPS | 0.2 /s | 0.2 /s | 0 /s | 0 /s | 0 /s | 1.9 /s | 1.9 /s | 0 /s | 0 /s | 0 /s | 2.2 kb/s | 2.2 kb/s | 0 b/s | 0 b/s | 0 b/s |
| HTTP | 0.0 /s | 0.0 /s | 0 /s | 0 /s | 0 /s | 0.6 /s | 0.6 /s | 0 /s | 0 /s | 0 /s | 585.9 b/s | 585.9 b/s | 0 b/s | 0 b/s | 0 b/s |
| TCP | 1.3 /s | 1.3 /s | 0 /s | 0 /s | 0 /s | 8.0 /s | 8.0 /s | 0 /s | 0 /s | 0 /s | 15.3 kb/s | 15.3 kb/s | 0 b/s | 0 b/s | 0 b/s |
| udp | 1.2 /s | 0 /s | 1.2 /s | 0 /s | 0 /s | 119.6 /s | 0 /s | 119.6 /s | 0 /s | 0 /s | 844.4 kb/s | 0 b/s | 844.4 kb/s | 0 b/s | 0 b/s |
| ICMP | 0.0 /s | 0 /s | 0 /s | 0.0 /s | 0 /s | 2.1 k/s | 0 /s | 0 /s | 2.1 k/s | 0 /s | 208.5 Mb/s | 0 b/s | 0 b/s | 208.5 Mb/s | 0 b/s |
| | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: |
| TOTAL | 3.3 /s | 1.5 /s | 1.4 /s | 0.0 /s | 0.3 /s | 4.4 k/s | 10.5 /s | 120.2 /s | 4.3 k/s | 3.5 /s | 417.9 Mb/s | 18.1 kb/s | 844.6 kb/s | 417.1 Mb/s | 1.8 kb/s |

All None Display: Sum Rate

# Consulta de uma simulação de ataque DDoS porta 0



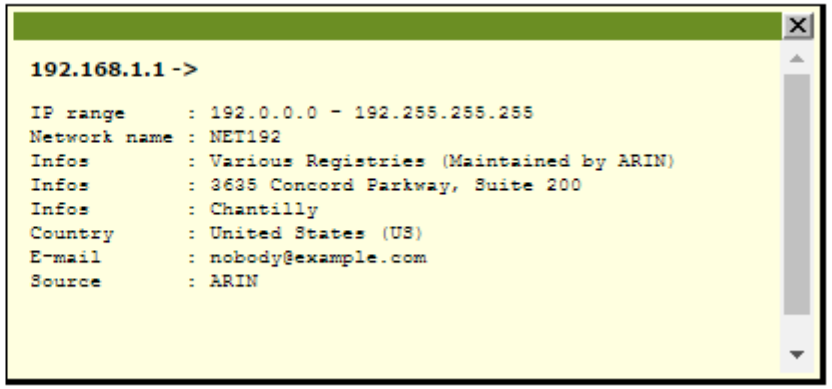

```
* nfdump -M /var/nfsen/profiles-data/teste/Ataque-porta-0-possivel-DDoS  -T  -r 2017/05/17/nfcapd.201705171225 -n 10 -s ip/flows
fdump filter:
ny
op 10 IP Addr ordered by flows:
ate first seen          Duration Proto           IP Addr    Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
017-05-17 12:26:41.538   180.710 any      192.168.100.254     106(54.1)      337( 2.3)     33978( 0.7)        1     1504   100
017-05-17 12:11:52.458  1049.560 any        192.168.1.216      90(45.9)    14507(97.7)     5.1 M(99.3)       13    38817   351
017-05-17 12:24:50.018   270.500 any        168.232.196.1      20(10.2)       50( 0.3)      2240( 0.0)        0       66    44
017-05-17 12:24:49.418   270.840 any          187.1.56.69      20(10.2)       48( 0.3)      2156( 0.0)        0       63    44
017-05-17 12:24:50.968   271.050 any        177.87.112.10      20(10.2)       51( 0.3)      2252( 0.0)        0       66    44
017-05-17 12:24:42.728   271.580 any       167.249.236.17      14( 7.1)      351( 2.4)     28342( 0.6)        1      834    80
017-05-17 12:23:26.818   336.690 any       177.66.103.206      10( 5.1)      567( 3.8)     34470( 0.7)        1      819    60
017-05-17 12:11:52.458  1026.270 any        132.255.240.3       7( 3.6)    13444(90.6)     5.0 M(98.0)       13    39160   373
017-05-17 12:26:41.538   177.680 any       132.255.240.22       5( 2.6)       29( 0.2)      2951( 0.1)        0      132   101
017-05-17 12:28:15.268    43.940 any          192.168.1.1       3( 1.5)       17( 0.1)      1836( 0.0)        0      334   108

ummary: total flows: 196, total bytes: 5126699, total packets: 14844, avg bps: 38337, avg pps: 13, avg bpp: 345
ime window: 2017-05-17 12:11:52 - 2017-05-17 12:29:42
otal flows processed: 196, Blocks skipped: 0, Bytes read: 11052
ys: 0.004s flows/second: 49000.0    Wall: 0.001s flows/second: 105660.4
```

# Consulta de uma simulação de ataque DDoS porta 0

Top 10 IP Addr ordered by flows:

| Date first seen | Duration | Proto | IP Addr |
|---|---|---|---|
| 2017-05-17 12:26:41.538 | 180.710 | any | 192.168.100.254 |
| 2017-05-17 12:11:52.458 | 1049.560 | any | 192.168.1.216 |
| 2017-05-17 12:24:50.018 | 270.500 | any | 168.232.196.1 |
| 2017-05-17 12:24:49.418 | 270.840 | any | 187.1.56.69 |
| 2017-05-17 12:24:50.968 | 271.050 | any | 177.87.112.10 |
| 2017-05-17 12:24:42.728 | 271.580 | any | 167.249.236.17 |
| 2017-05-17 12:23:26.818 | 336.690 | any | 177.66.103.206 |
| 2017-05-17 12:11:52.458 | 1026.270 | any | 132.255.240.3 |
| 2017-05-17 12:26:41.538 | 177.680 | any | 132.255.240.22 |
| 2017-05-17 12:28:15.268 | 43.940 | any | 192.168.1.1 |



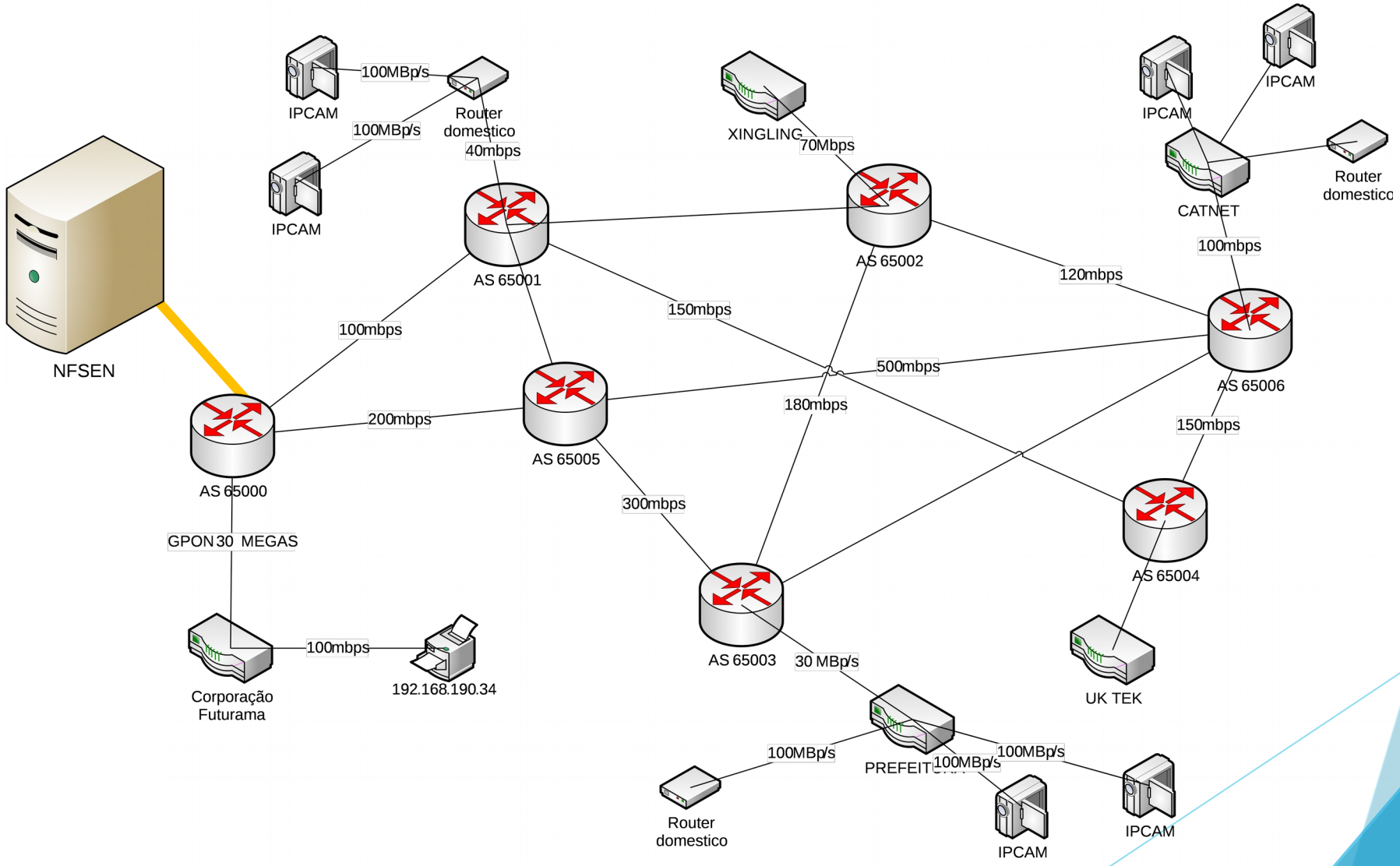
# Configurando Blackhole Level3 / Cemig Telecom no Mikrotik

- Passo1: Adcionar o ip  atacado na tabela de rotas como Blackhole
  - **Mikrotik usando o ip de exemplo 192.168.190.34:**
    - /ip route  add dst-address=192.168.190.34 type=blackhole
- Passo 2 preparando o prefixo para ser anunciado
  - **Mikrotik usando o ip de exemplo 192.168.190.34:**
    - /routing bgp network add network=192.168.190.34/32
- Passo 3 anunciando o prefixo
  - **Mikrotik usando o ip de exemplo 192.168.190.34:**
    - /routing filter add chain=BGP-IPV4-OPERADORA-EXP prefix= 192.168.190.34/32 action=accept
    - /routing filter Print
    - /routing filter Move (coloque o numero da regra e coloque ela antes da regra de dicard)

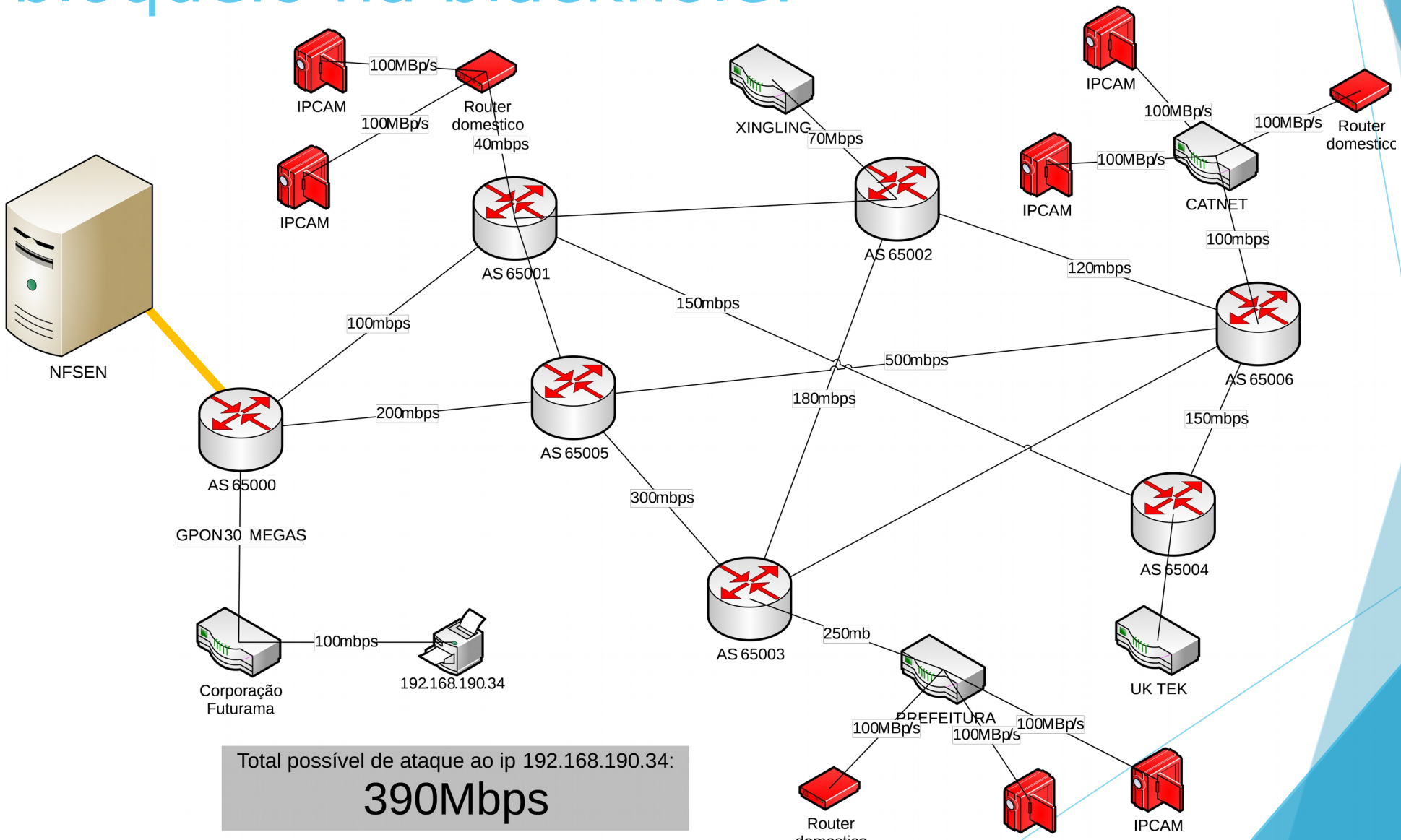
# Configurando Blackhole Level3 /Cemig Telecom

- **Em sistemas operacionais como os listados abaixo**
  - VYOS
  - QUAGGA
  - JunOs
  - Cisco IOS XE/XR
- , o processo é o mesmo que é adicionar a rota na tabela de rotas, adicionar a network no BGP, configura no filtro de saída dos anúncios em uma prefix-list ou policy statment, e marque o termo que referência esta lista ou termo com a comunity como as exemplificadas abaixo:
  - Cemig: 23106:666
  - Level 3: 3549:666

# Como funciona o processo de bloqueio na blackhole:



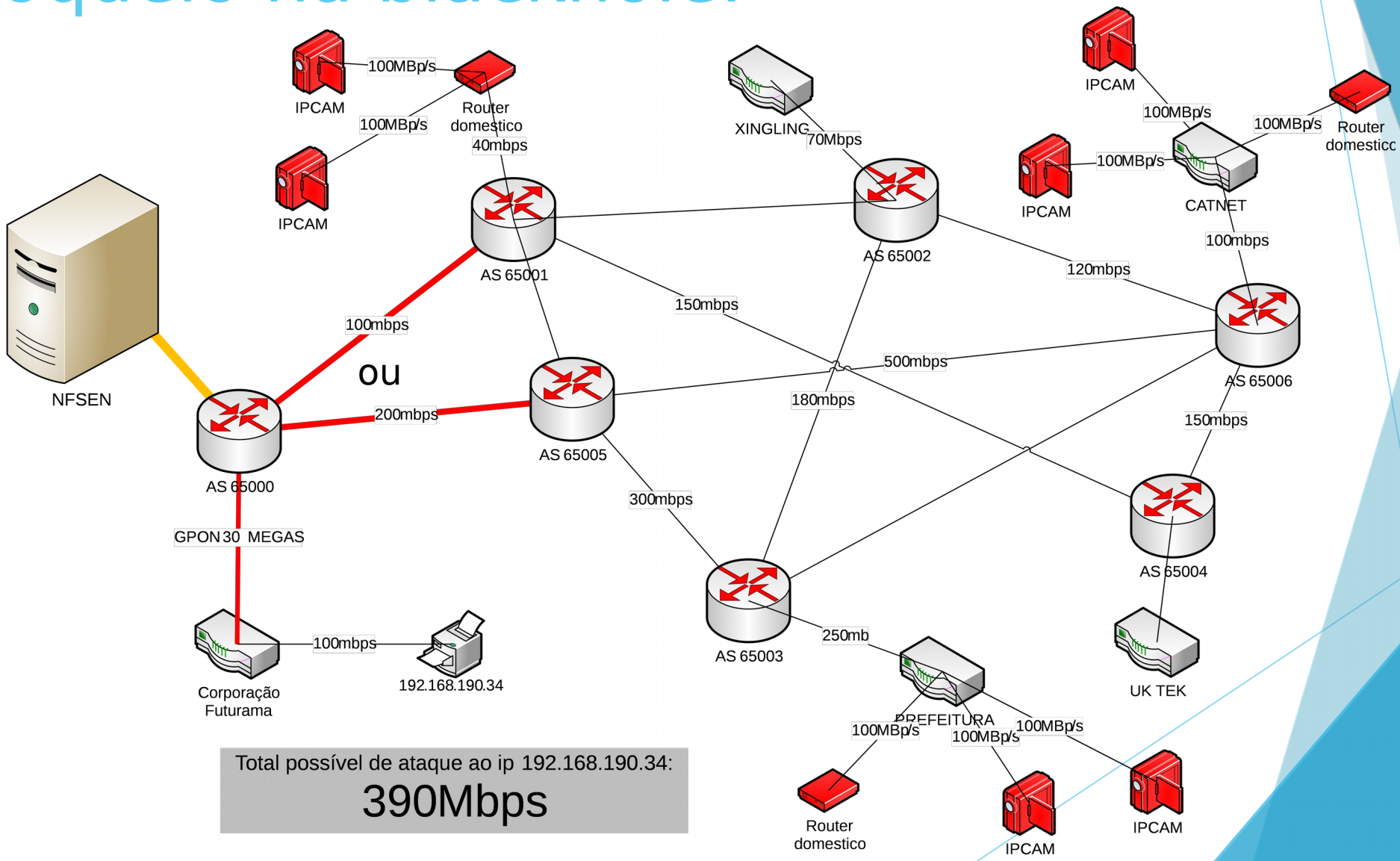
# Como funciona o processo de bloqueio na blackhole:




Total possível de ataque ao ip 192.168.190.34:

390Mbps

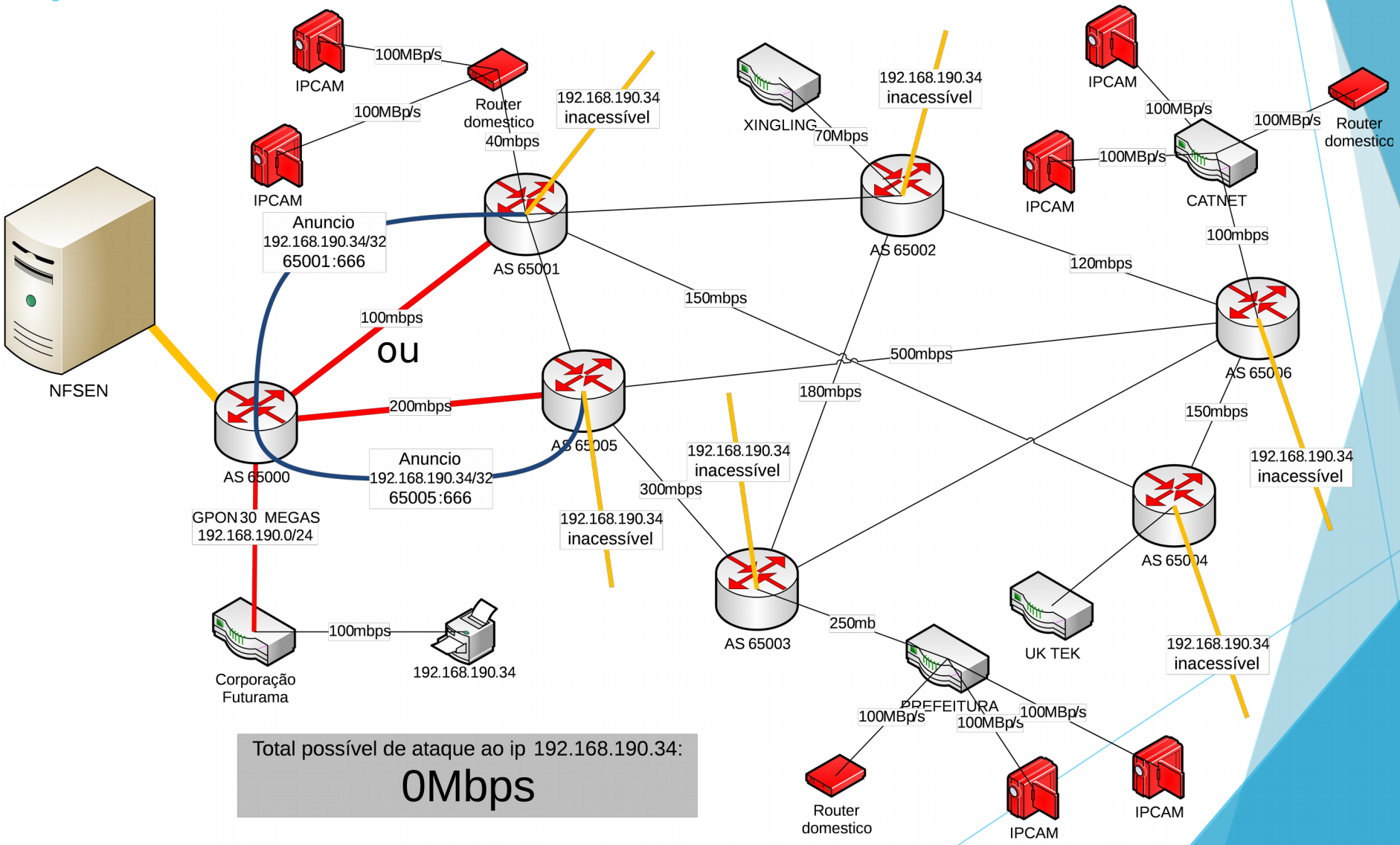
# Como funciona o processo de bloqueio na blackhole:




Total possível de ataque ao ip 192.168.190.34:

390Mbps

# Como funciona o processo de bloqueio na blackhole:



# Consequências da não mitigação do ataque

- Lentidão no acesso a internet de seus clientes caso o ataque seja maior do que o link pode comportar.
- Travar seu roteador de borda caso não tenha proteções de router-engine /control-plane.
- Ataques pequenos pode dar uma ilusão do que realmente sua rede consome de largura de banda durante horários de pico (de repente  parte de seu consumo é ataque DDoS.
- Lentidão de navegação por conta de ataques ao DNS recursivo (muita requisição sendo processada e seu DNS recursivo não aguenta responder).
- Dependendo do volume de trafego (já tivemos casos nas mãos de 40GBp/s de ataque a porta 0 DDoS e foi rapidamente mitigado com o NFSEN) derrubar toda a operação de fornecimento de internet do provedor ou AS.
- Prejuízos para  a imagem da empresa, por conta de ataques de um “concorrente”.

# Ajustes Finos

- Se você tivesse vários roteadores em sua rede enviando fluxos para o mesmo coletor, você poderá configurá-los para enviar para diferentes portas no coletor ou pode informar no nfsen o endereço IP de origem de cada roteador. Isso permite que nfsen mostre dados distintos de cada fonte.
- nano /var/nfsen/etc/nfsen.conf e adicione a (s) fonte (s), por exemplo:
- %sources = (
- ‘Borda'  => { 'port' => '9001', 'col' => '#0000ff', 'type' => 'netflow' },
- ‘Roteador 1'  => { 'port' => '9002', 'col' => '#00ff00', 'type' => 'netflow' },
- ‘Roteador 2'  => { 'port' => '9996', 'col' => '#ff0000', 'type' => 'netflow' },
- );

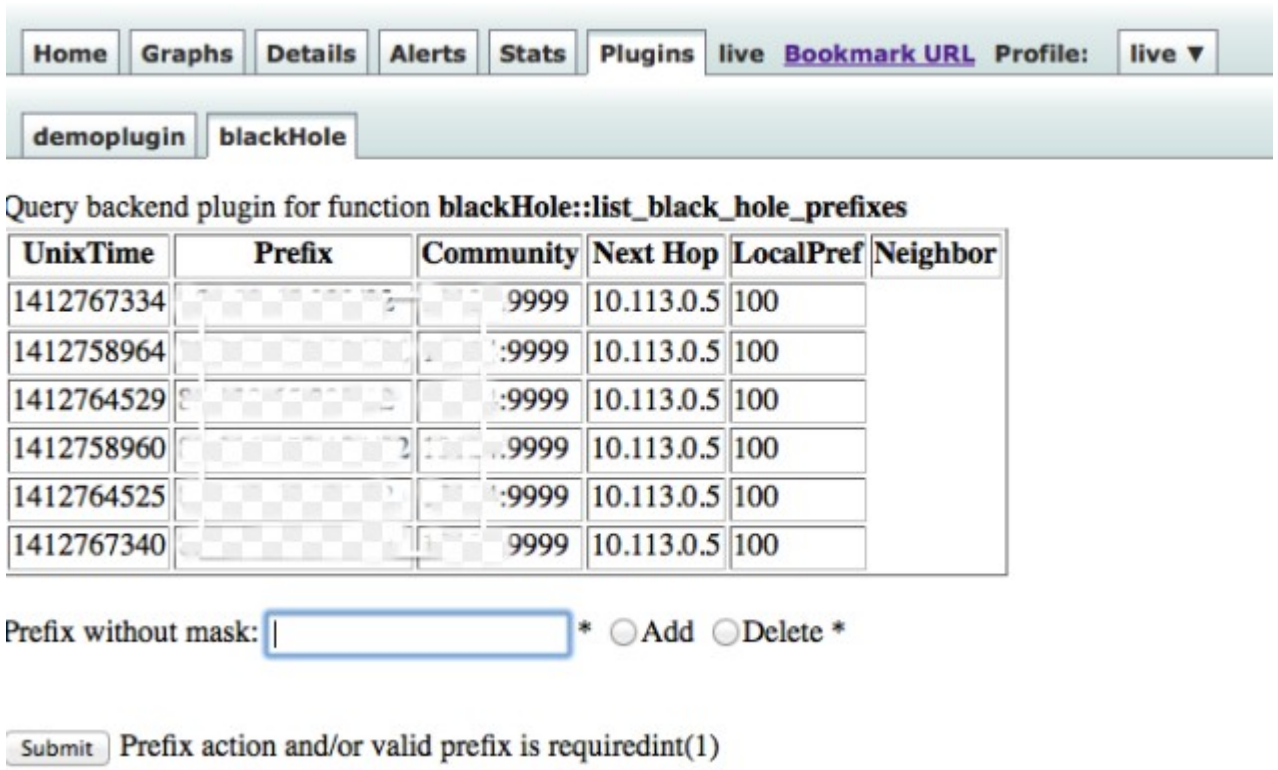
- Digite par atualizar as configurações: /etc/init.d/nfsen reconfig

# Ajuste fino Plugins

- https://github.com/mdjunior/nfsen-plugins
- SurfMap
- Nfsight
- HostStats
- FlowDoh
- SSHCure Github
- ddos
- dest
- blackHole
- IRCTrackerPlugin
- CCTrackerPlugin
- SMTPTrackerPlugin
- cndet
- delaywatch
- sshmonitor
- profiles-anomaly
- natdet
- rdpmonitor
- tss
- Honeyscan
- nfplugger - Plugin template generator

# Ajuste fino

- Blackhole



# Hotstat

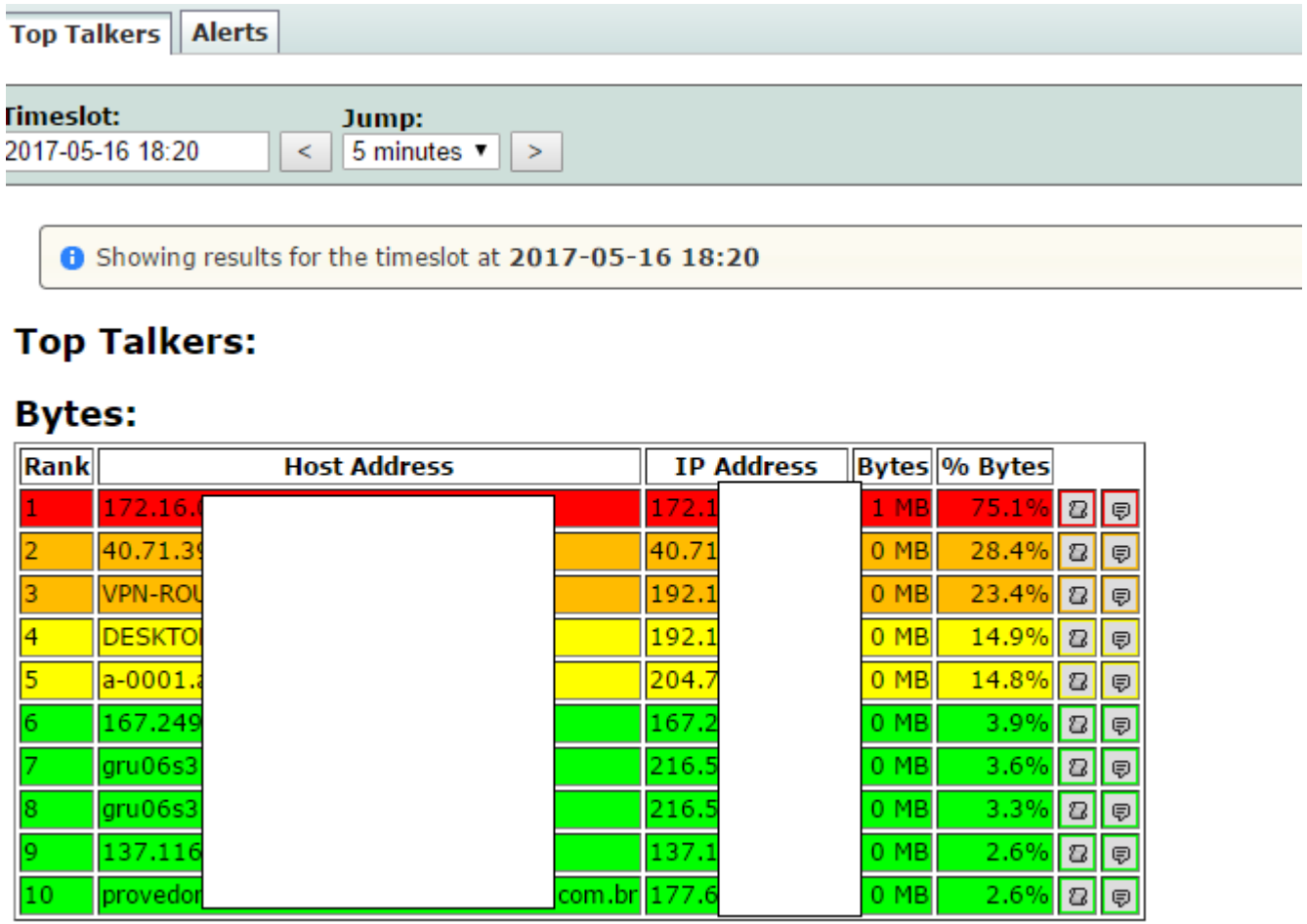
- Cd
- Wget https://ufpr.dl.sourceforge.net/project/libnfdump/libnfdump-0.1.1.tar.gz
- tar xvzf libnfdump-0.1.1.tar.gz
- cd libnfdump-0.1.1
- ./configure
- Make
- Make install
- apt-get install php5-gd

- Cd
- Wget https://ufpr.dl.sourceforge.net/project/hoststats/hoststats-1.1.5.tar.gz
- tar xvzf hoststats-1.1.5.tar.gz
- cd hoststats-1.1.5
- ./configure
- Make
- Make install
- /data/hoststats/hoststats start

# FlowDoh (para gerar em tempo real os top conversations).

- cd
- wget https://ufpr.dl.sourceforge.net/project/flowdoh/FlowDoh_1.0.2.tar.gz
- tar xvzf FlowDoh_1.0.2.tar.gz
- cd flowdoh/
- cd frontend/
- cp  -R * /var/www/html/nfsen/plugins/
- cp  -R * /var/www/html/nfsen/plugins/flowdoh
- cd ..
- cd backend/
- cp -R * /var/nfsen/plugins/
- cp  /var/nfsen/plugins/flowdoh/flowdoh.conf.defaults /var/nfsen/plugins/flowdoh/flowdoh.conf

# FlowDoh (para gerar em tempo real os top conversations).



# SshCure (recomendado)
# Gera um dashboard da rede

- cd
- wget https://ufpr.dl.sourceforge.net/project/sshcure/source/SSHCure_v2.4.1.tar.gz
- tar xvzf SSHCure_v2.4.1.tar.gz
- cd SSHCure
- apt-get install php5-sqlite
- apt-get install php5-json
- apt-get install libnet-ip-perl
- apt-get install libdbd-sqlite3-perl
- apt-get install libjson0 libjson0-dev
- apt-get install libjson-perl
- apt-get install libio-async-perl

- perl -MCPAN -e shell
- install LWP
- perl -MCPAN -e shell (para entrar o cpan)
- install LWP (dentro do cpan)
- exit (dentro do cpan)
- ./install.sh
- nano /var/nfsen/etc/nfsen.conf
  - Adicionar as linhas abaixo no arquivo e salvar
  - @plugins = (
  - # profile # module
  - [ '*', 'SSHCure' ],
  - );

Service nfsen restart

# SshCure Gera um dashboard da rede
# Licença BSD

- Acessando o SSHCURE
  - http://IP.DO.FLOW/nfsen/plugins/SSHCure/

# Observações

- É interessante se pensar como boa pratica  a sugestão de que toda a rota recebida de um parceiro que esteja com a comunity xxxxx:666 seja automaticamente enviada para blackhole do roteador local e assim aumentando o índice de mitigação de ataques em nosso ecossistema.
- **Sempre façam filtros de Anti−Spoofing**

# Firewall Recomendações

- Mantenha sempre atualizado
- Criar regras para que seu cliente não realize ataques DDoS e assim criarmos um ambiente de internet mais eficiente.
  - Limitar acesso a equipamentos de seus clientes a partir da internet.
  - Criar politicas de firewall eficientes
- Defina uma política padrão
- Não exponha serviços privados sem VPN
- Crie políticas de acesso por grupos de interesse
- Utilize uma DMZ ou rede privada para serviços públicos
- Crie um processo de gerenciamento de mudança no firewall
- Acompanhe o comportamento da rede e atualize as políticas de acesso
- Auditoria

# Outras ferramentas de FLOW

- NEMEA (Vamos tentar agendar para um próximo GTS :D)
  - Sistema (Análise de Medidas de Rede) NEMEA é um **stream-sábio** , **baseada em fluxo** e um **modular** sistema de detecção para análise de tráfego de rede. Consiste em muitos módulos independentes que são interligados através de interfaces de comunicação e cada um dos módulos tem sua própria tarefa. A comunicação entre os módulos é feita pela passagem de mensagens onde as mensagens contêm registros de fluxo, alertas, algumas estatísticas ou dados pré-processados.
  - Umas das melhores ferramentas para a detecção de anomalias na rede estendido em camada 7 de código aberto.
    - Oferece um dashboard muito rico.
  - http://nemea.liberouter.org/tfcsirt2017/#
  - https://github.com/CESNET/Nemea

# Fontes de dados:

- ftp://ftp.registro.br/pub/gter/gter18/03-bgp-bloqueio-dos-flood.ear.pdf
- https://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html
- http://nfsen.sourceforge.net/1.2.4/index.html

# Contato


- Alexandre.gioavaneli@gmail.com
- Skype:live:alexandre.Giovaneli
- Movel:+55 31 9 8255 5555