Mitigando Ataques DDoS Usando NFSEN.

Alexandre Giovaneli

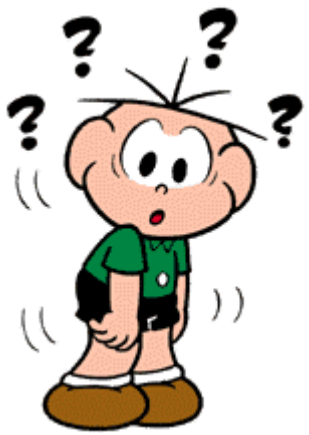
Giovaneli Consultoria

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.

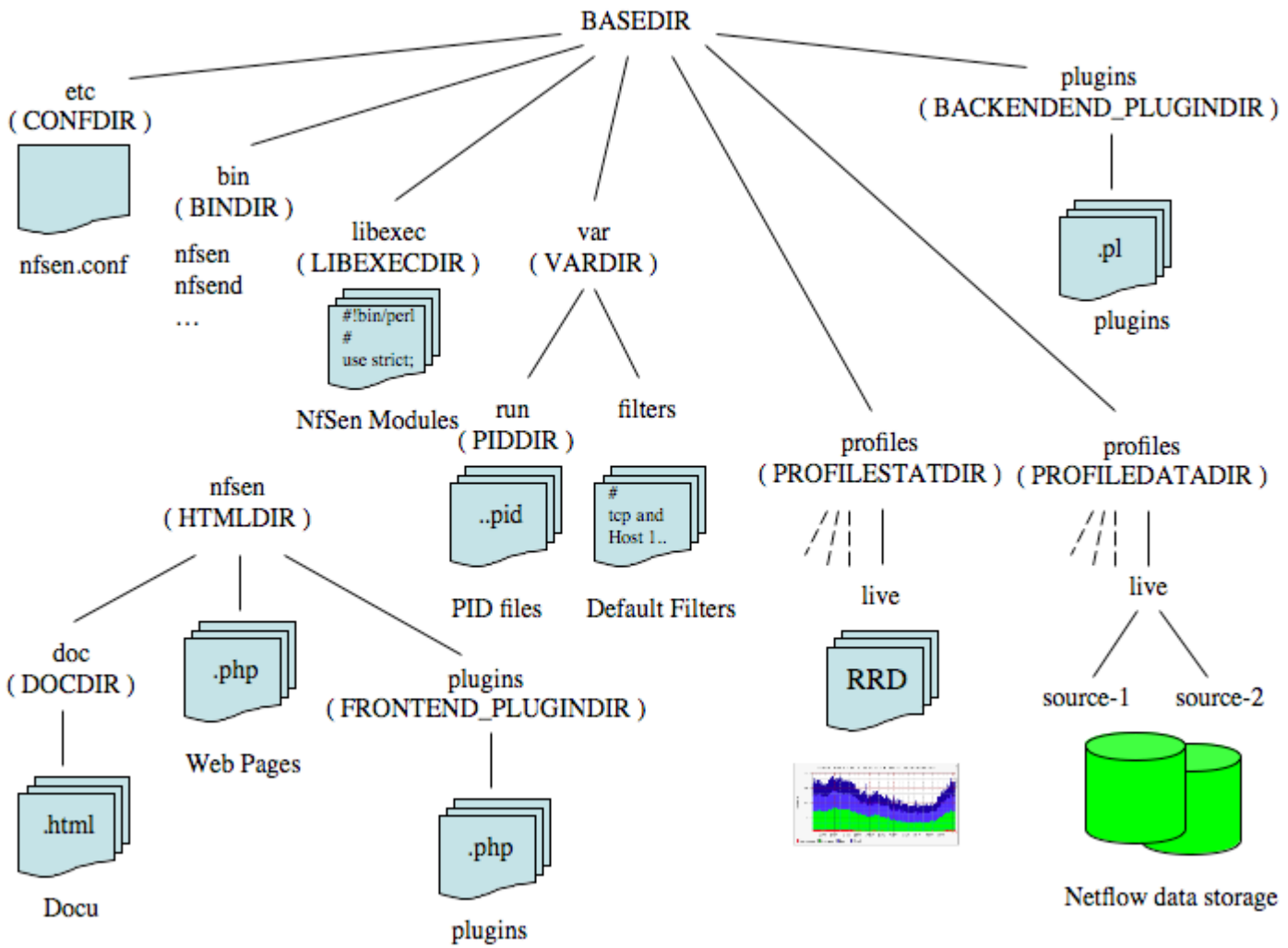
O que é NfSen ?

- 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 .



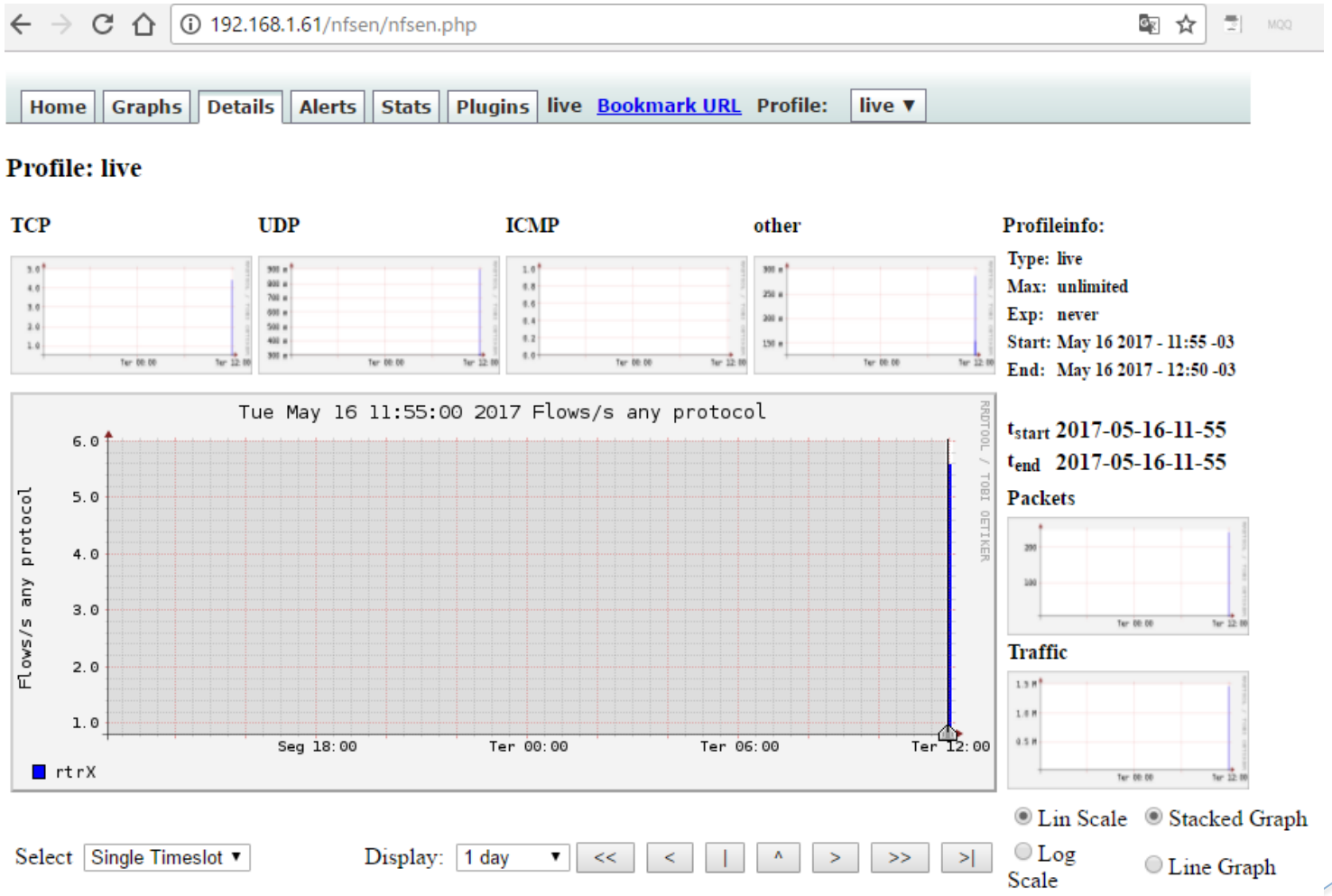
Fonte: http://nfsen.sourceforge.net/#mozTocId764303

Estrutura NfSen

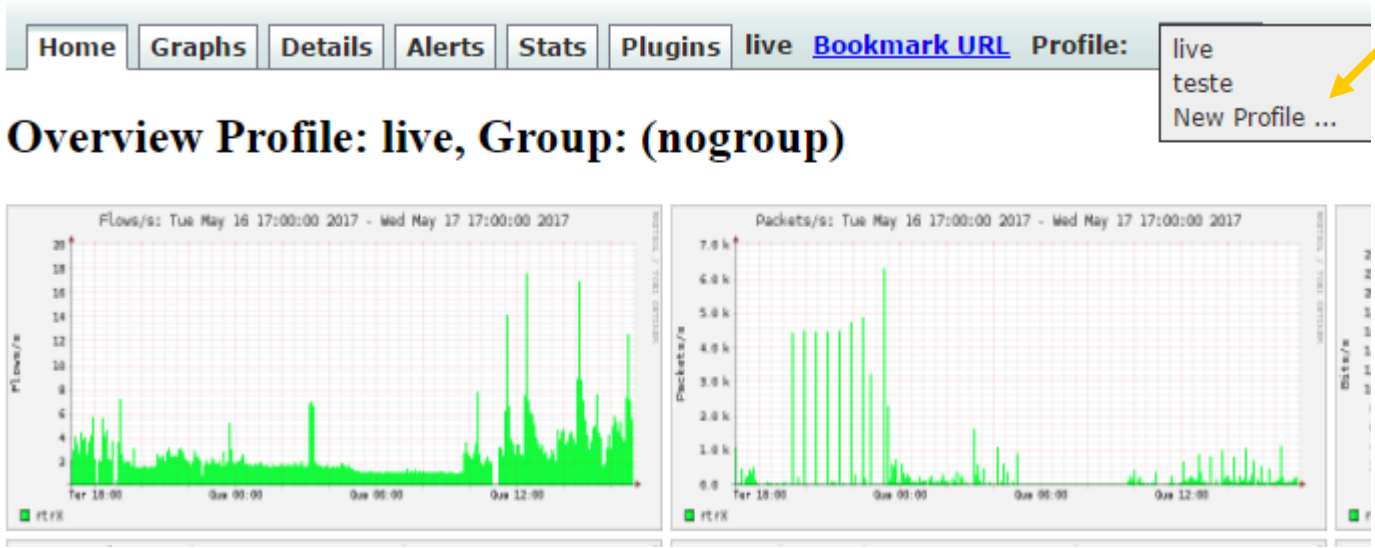


Acessando NfSEN

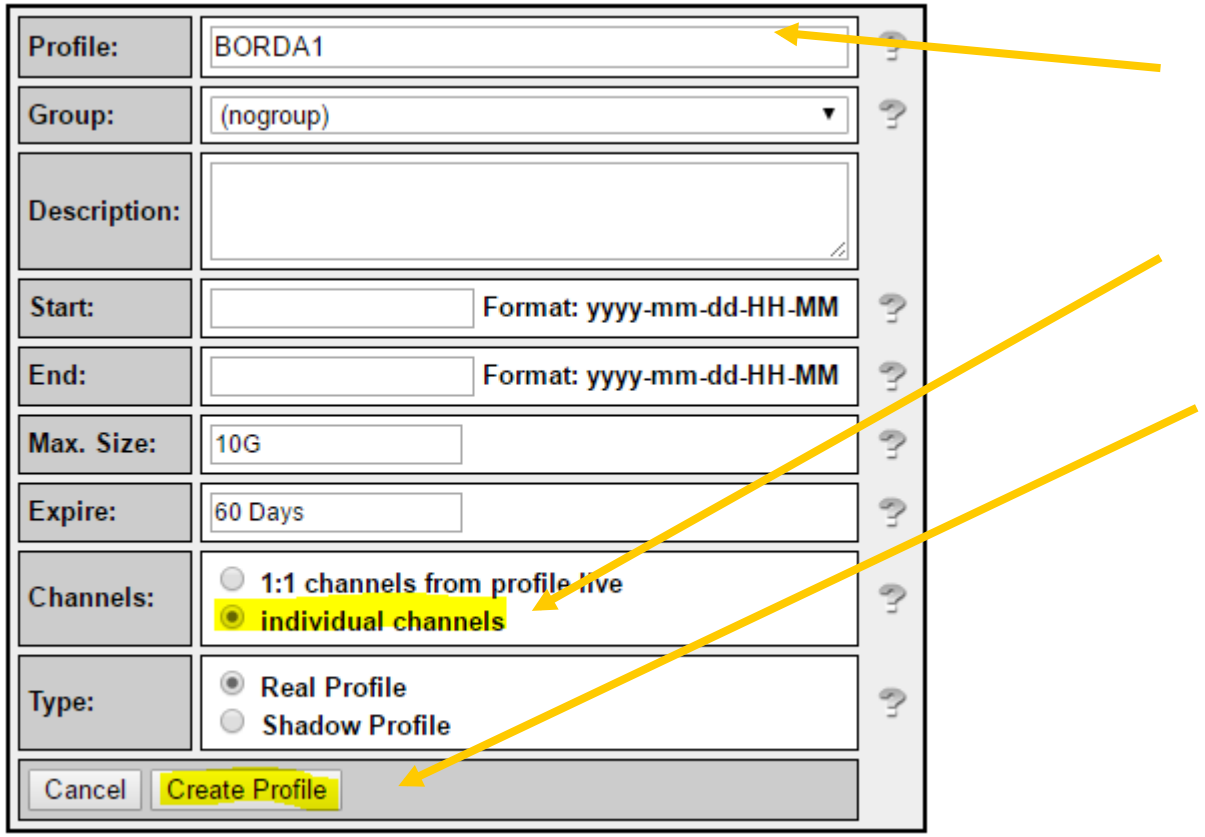
- http://ip.do.servidor/nfsen/nfsen.php



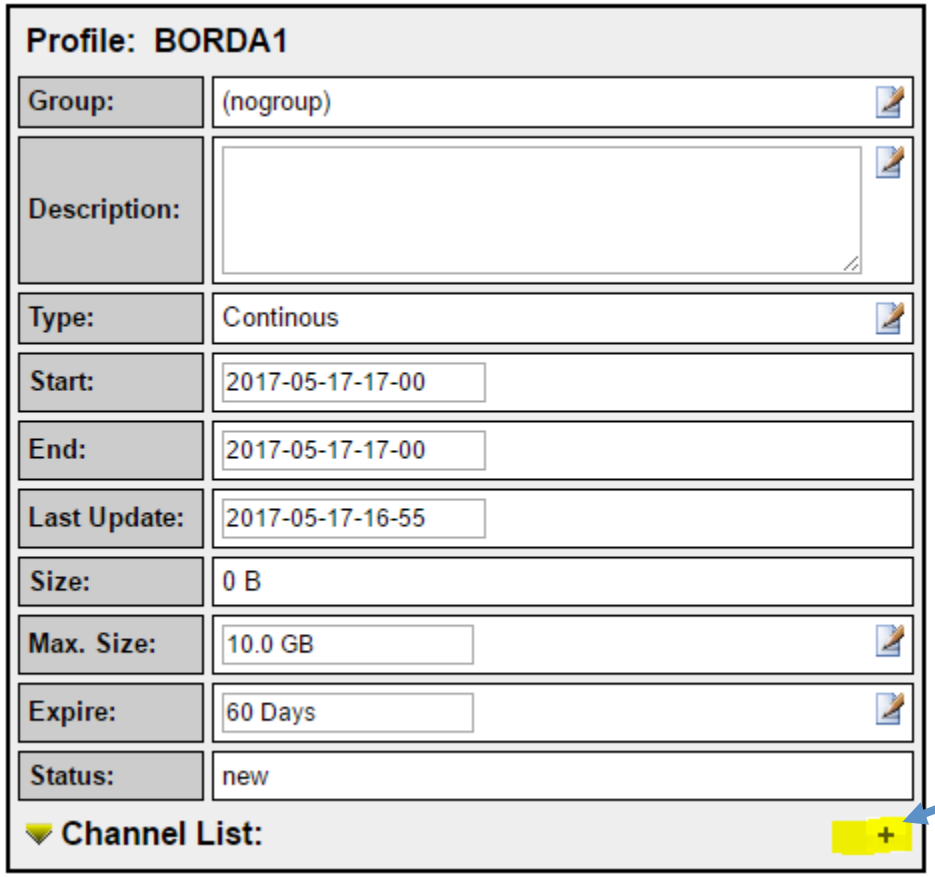
Configurando Perfis de leitura no NfSen e filtros



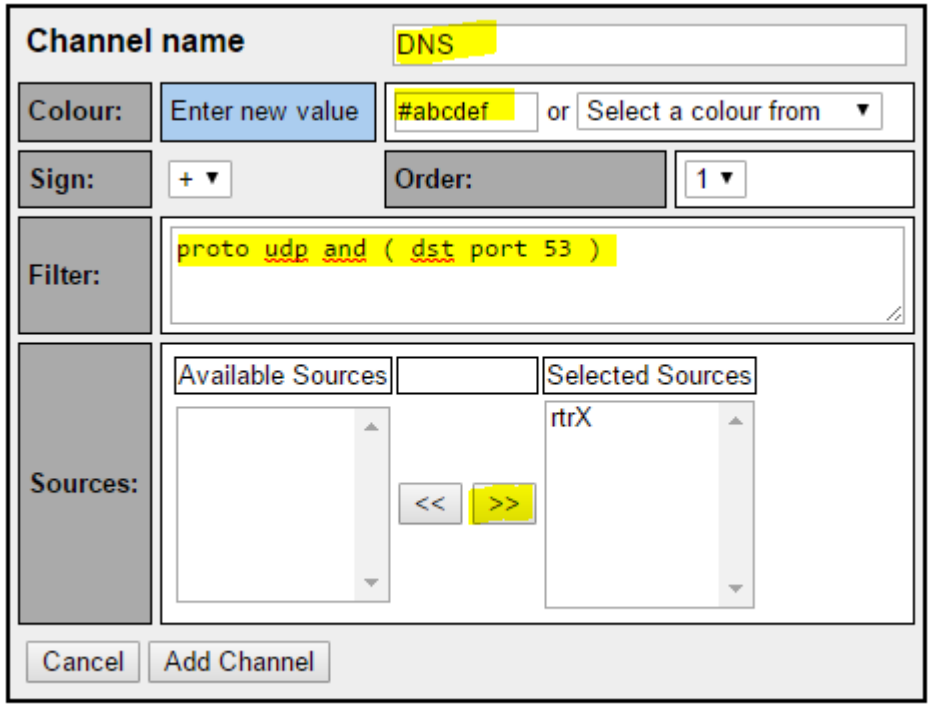
Criando perfil de coleta



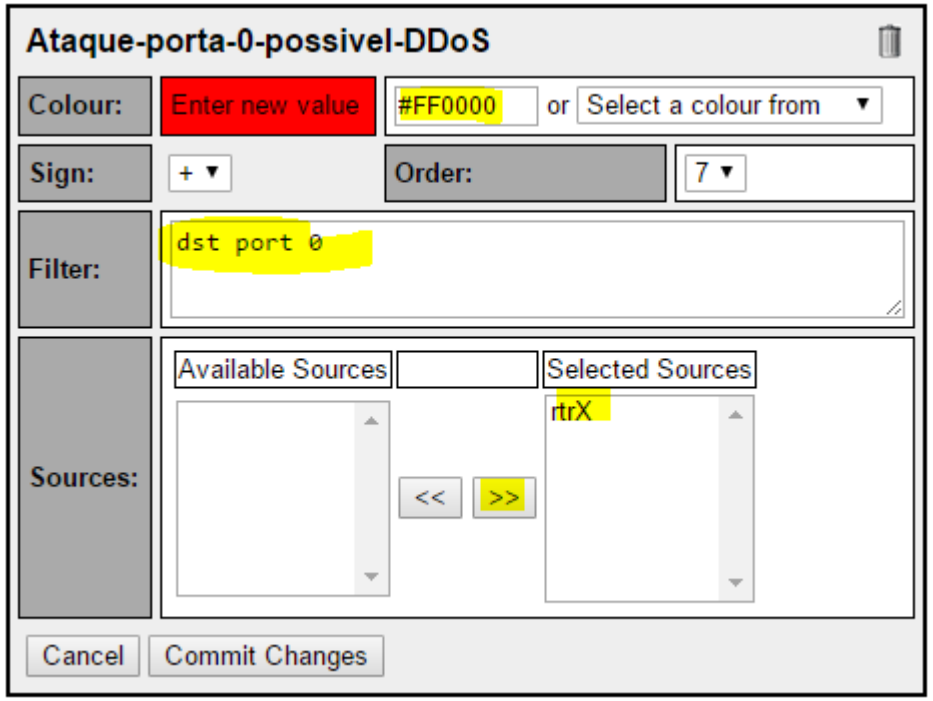
Criando perfil de coleta



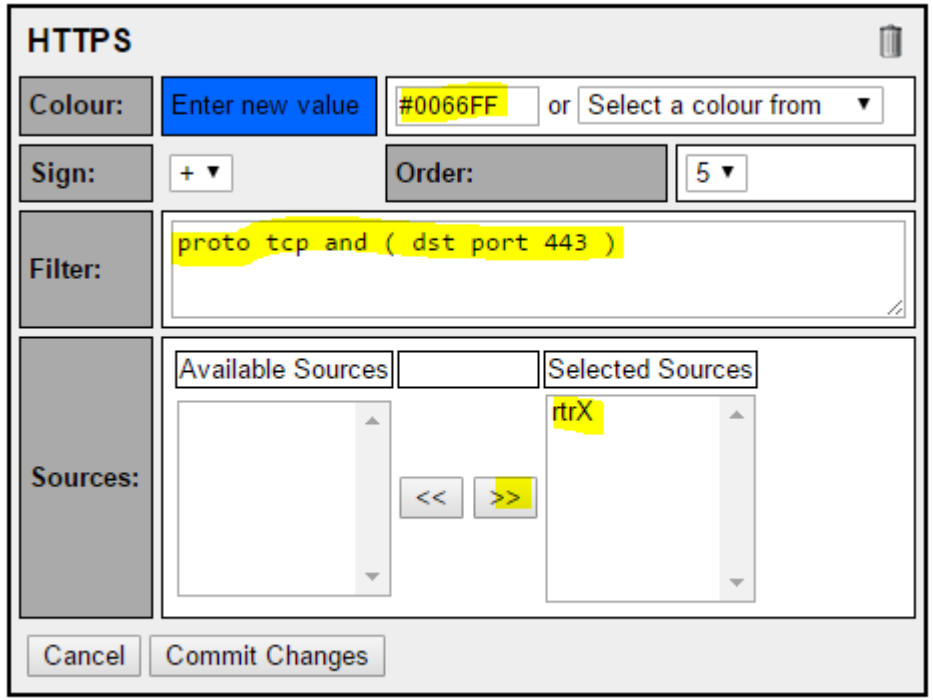
Filtro DNS


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

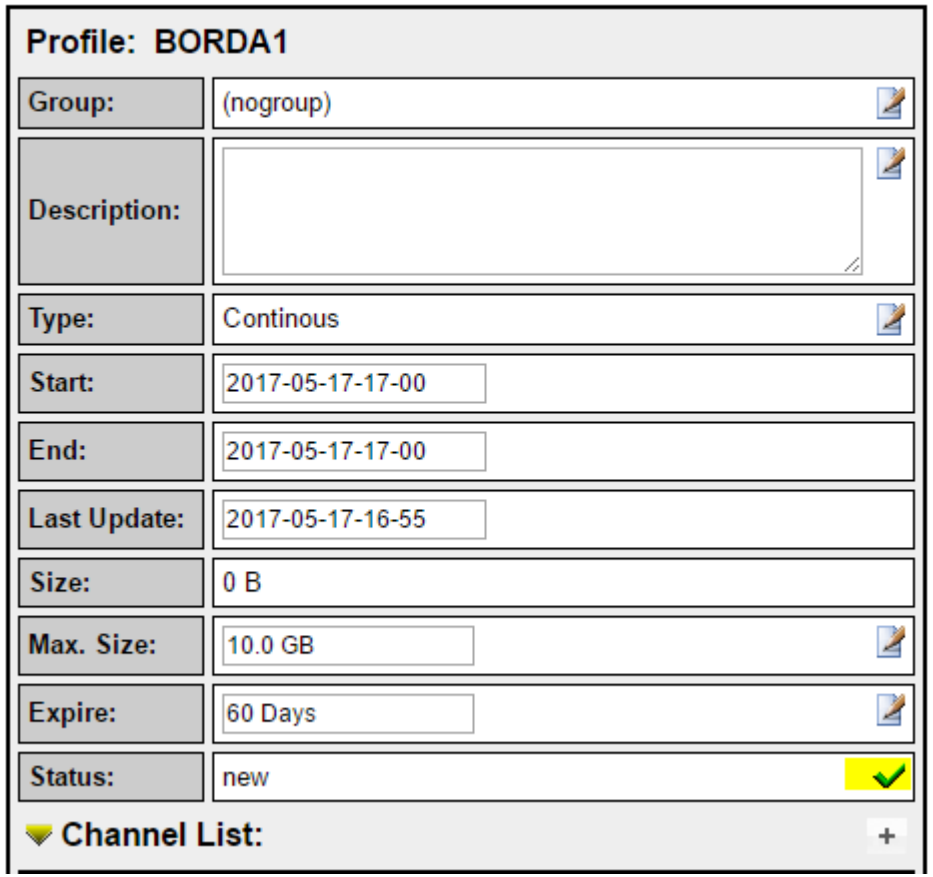
Filtro ataque porta 0 DDoS (o mais comum dos ataques)



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

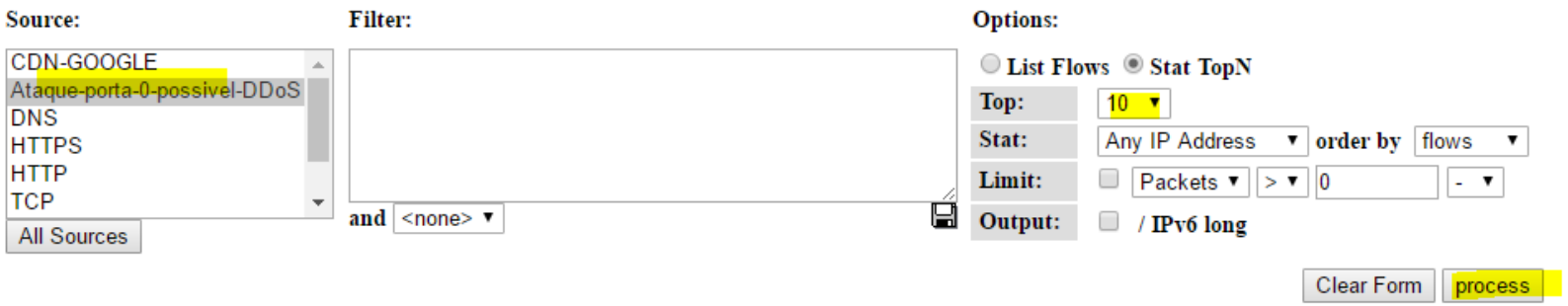
Select Single Timeslot ▼ Display: 1 day ▼ << < | ^ > >> >|

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

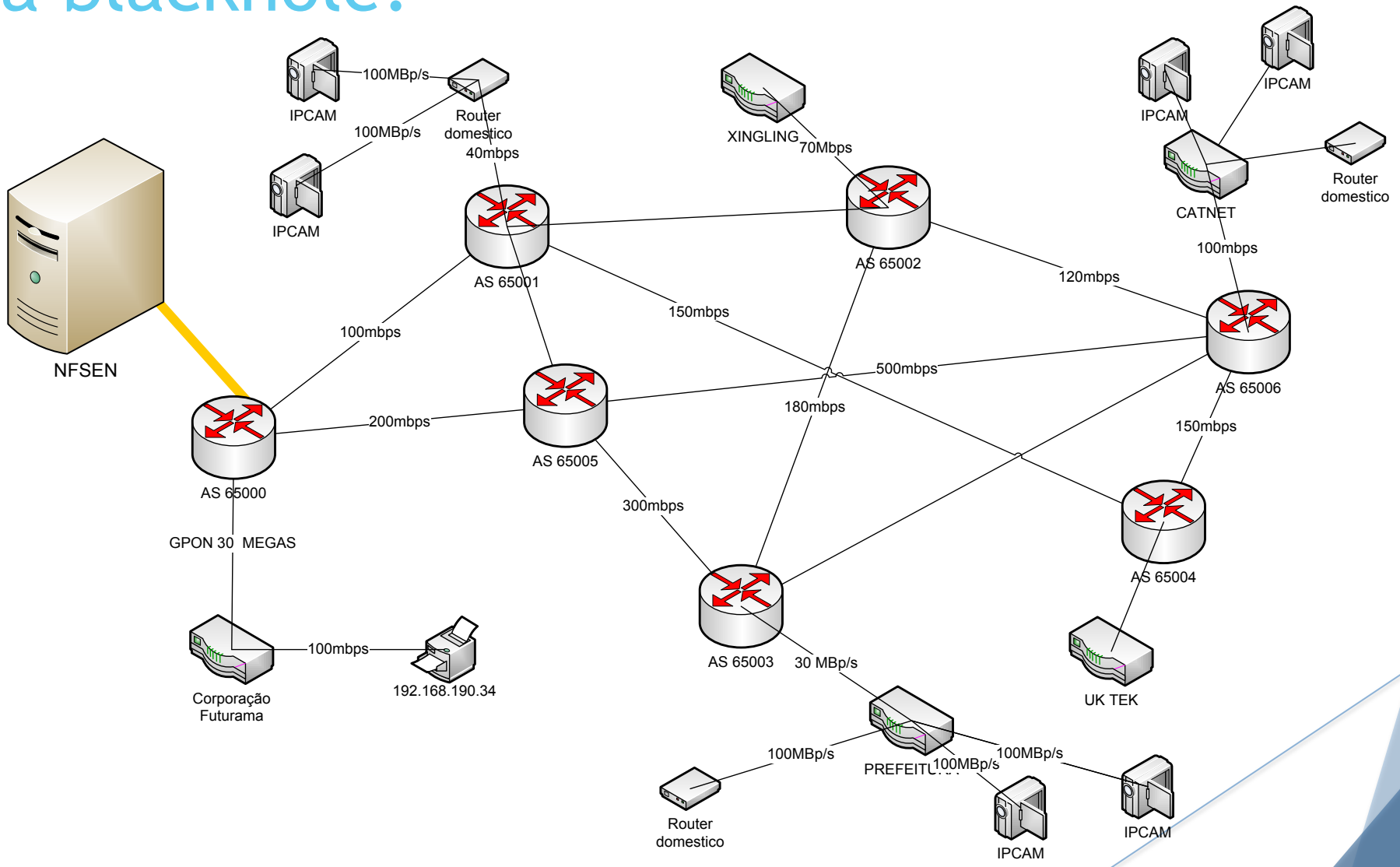
Consulta de uma simulação de ataque DDoS porta 0



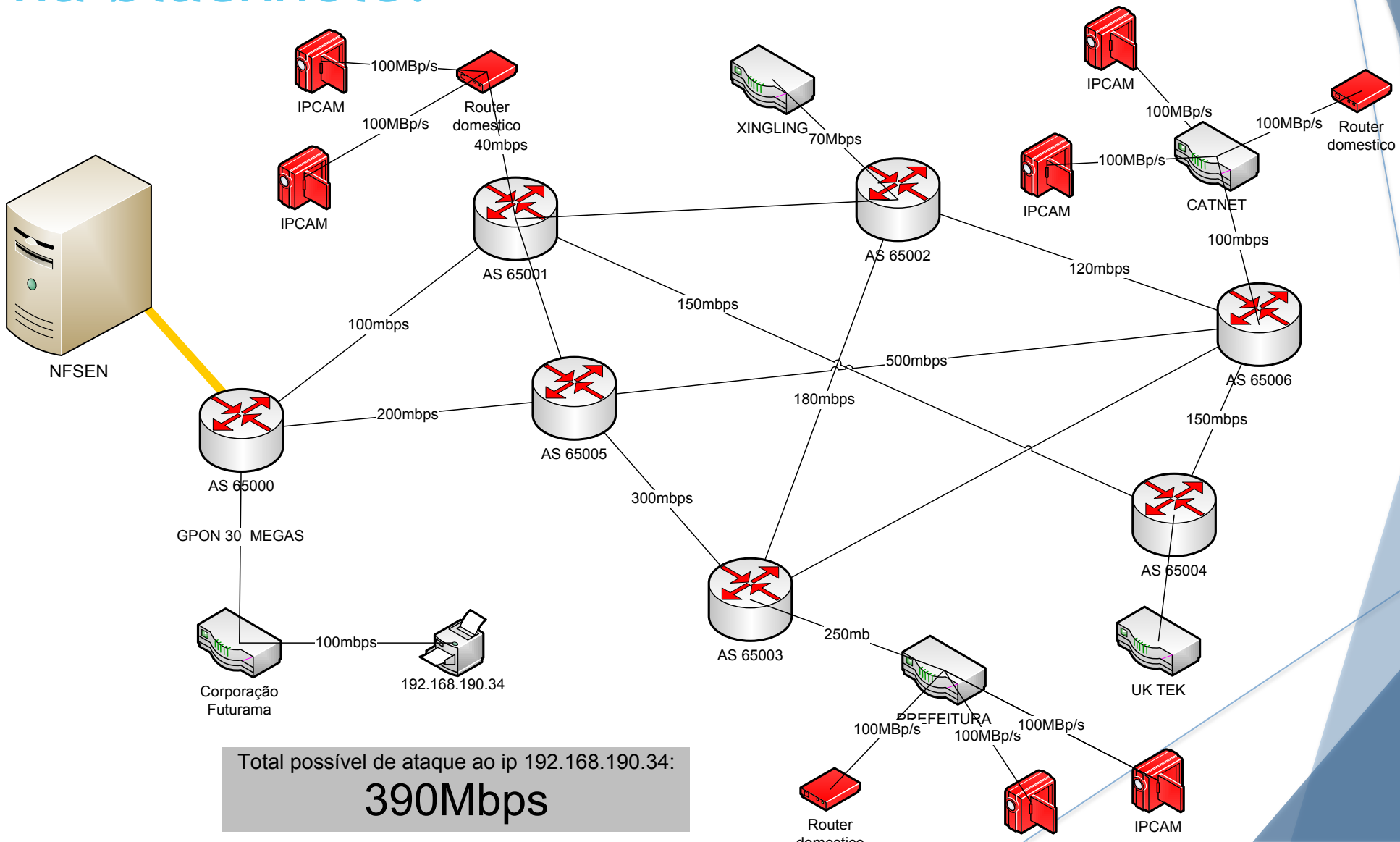

```
'* nfdump -M /var/nfsen/profiles-data/teste/Ataque-porta-0-possivel-DDoS  -T  -r 2017/05/17/nfcapd.201705171225 -n 10 -s ip/flows
ıfdump filter:
ıny
'op 10 IP Addr ordered by flows:
)ate first seen          Duration Proto           IP Addr    Flows(%)     Packets(%)       Bytes(%)         pps      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
```

Como funciona o processo de bloqueio na blackhole:



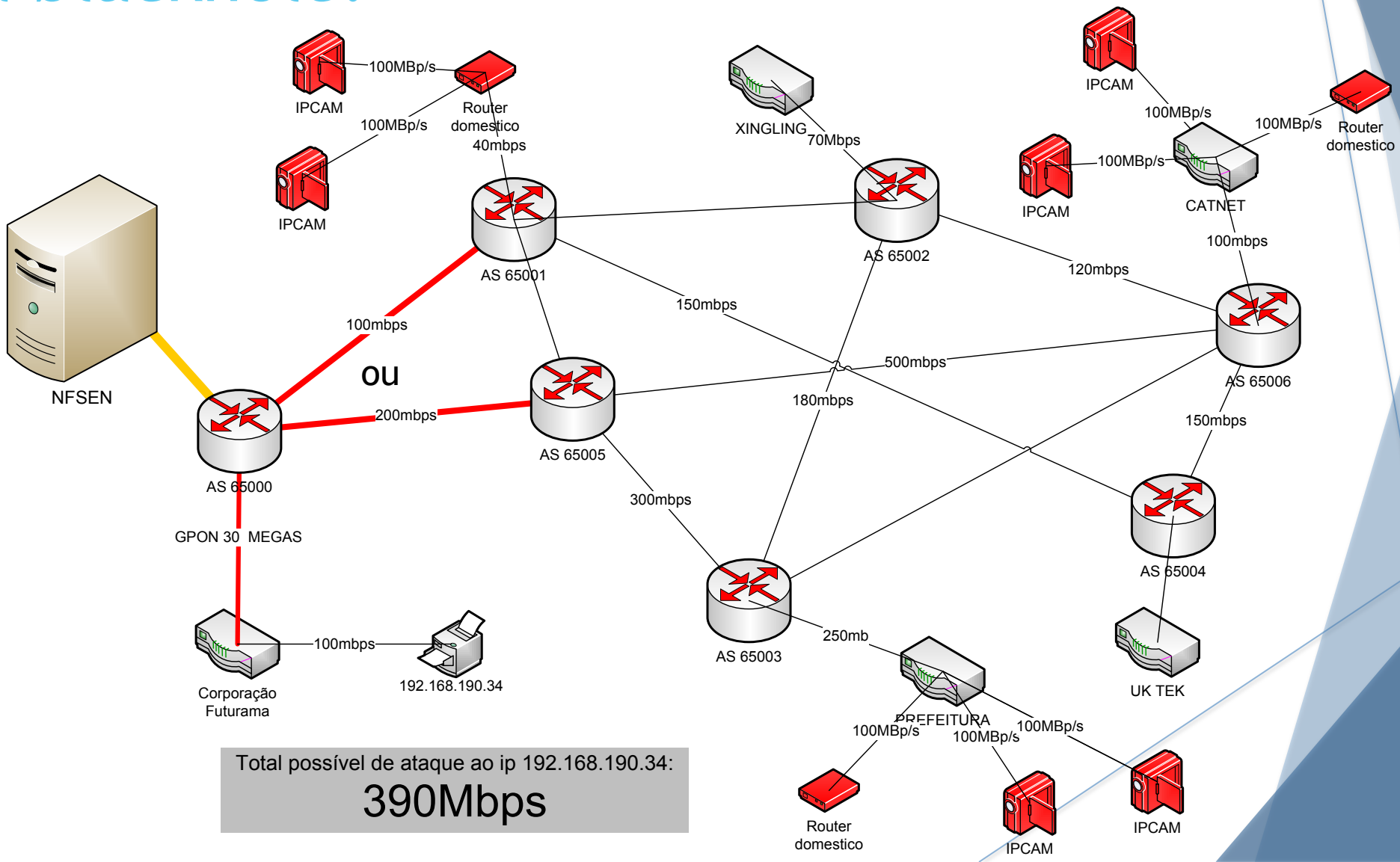
Como funciona o processo de bloqueio na blackhole:



Total possível de ataque ao ip 192.168.190.34:

390Mbps

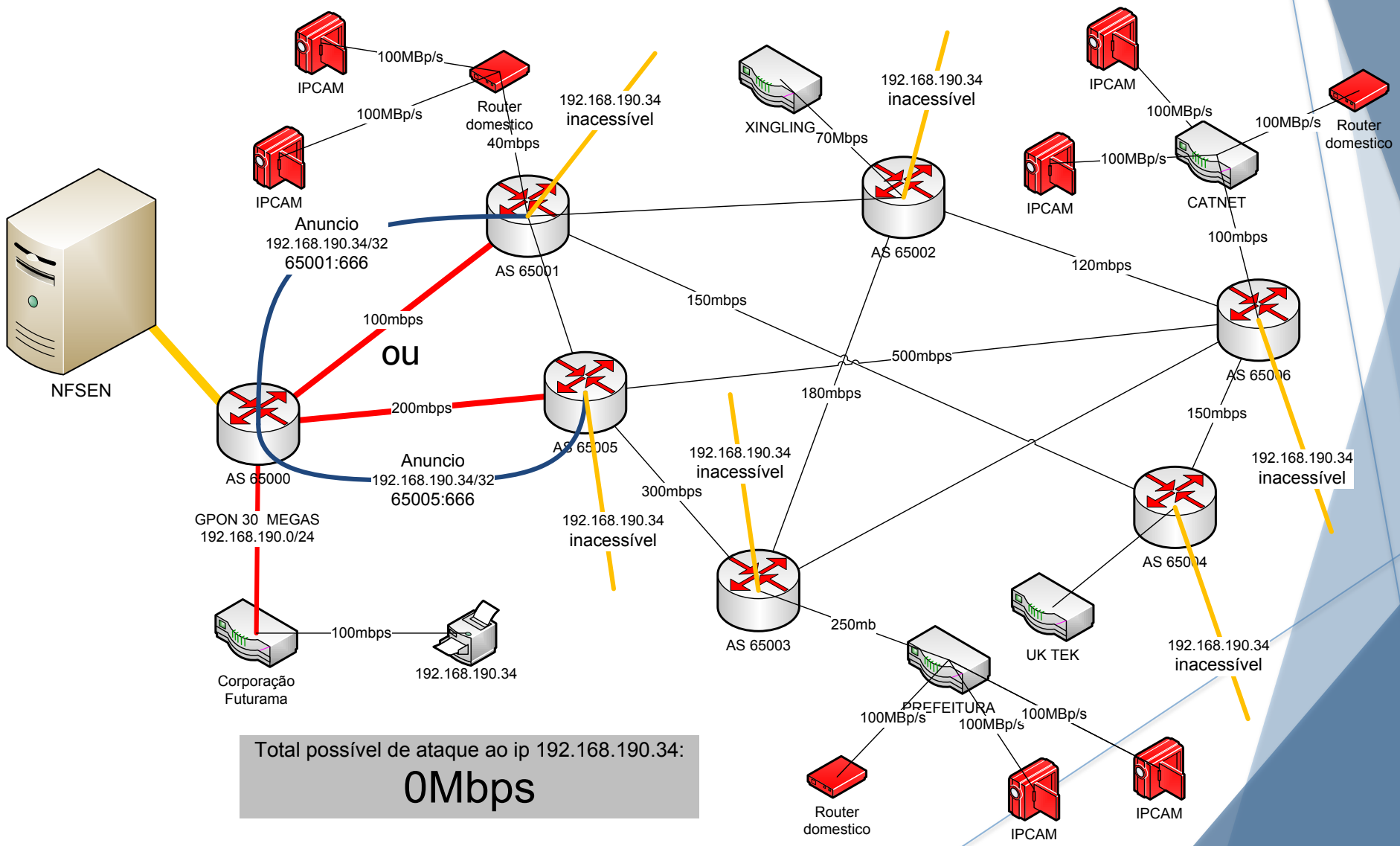
Como funciona o processo de bloqueio na blackhole:



Total possível de ataque ao ip 192.168.190.34:

390Mbps

Como funciona o processo de bloqueio na blackhole:



Total possível de ataque ao ip 192.168.190.34:

0Mbps

Consequências da não mitigação do ataque

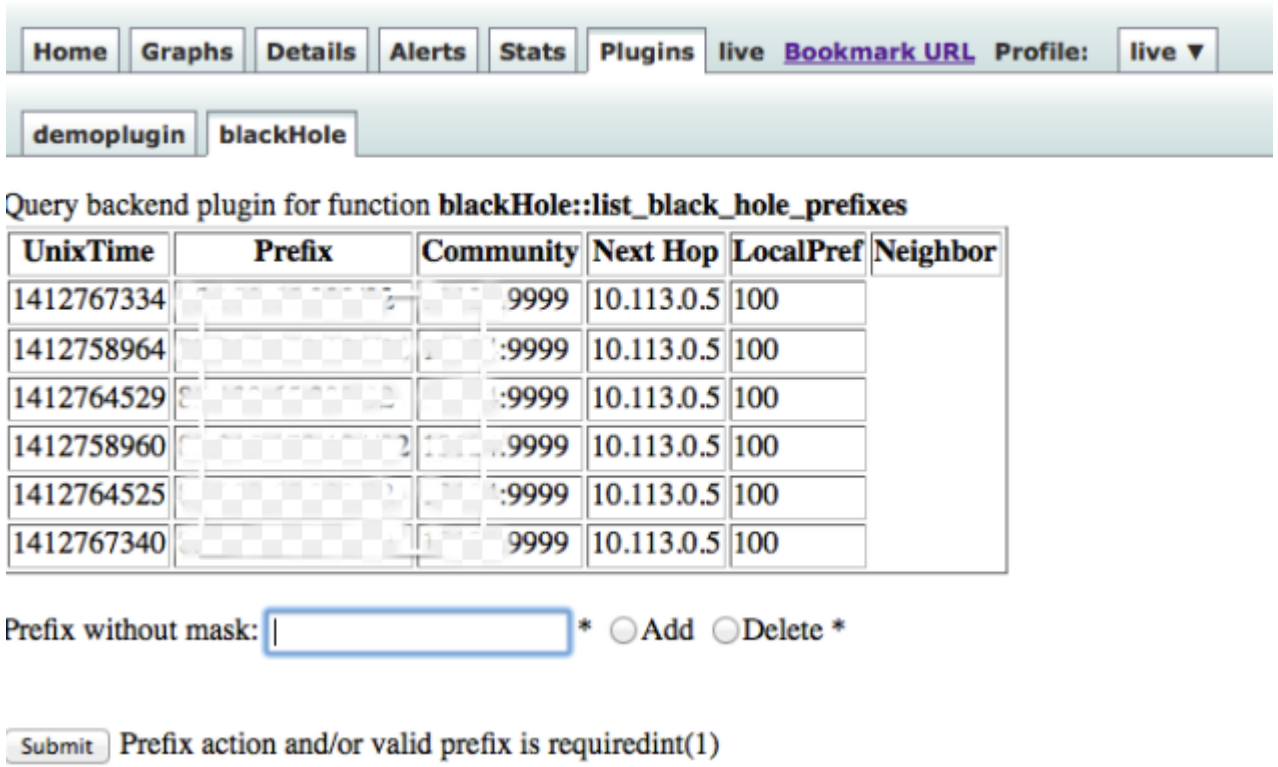
- Lentidão no acesso a internet de seus clientes caso o ataque seja maior do que o link pode comportar.
- Travar seu roteador de borda caso não tenha proteções de router-engine / control-plane.
- Ataques pequenos pode dar uma ilusão do que realmente sua rede consome de largura de banda durante horários 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

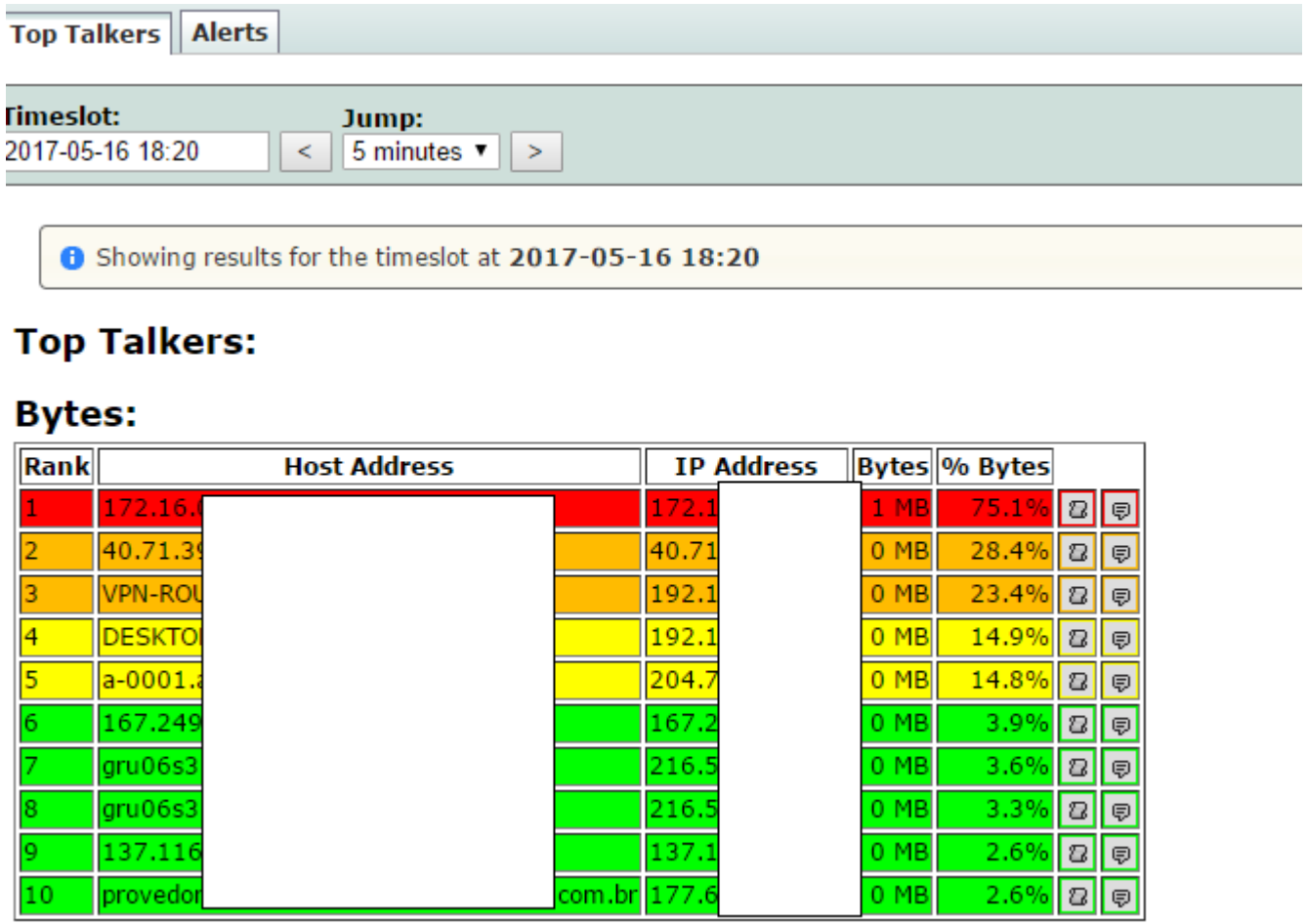
- Se você tivesse vários roteadores em sua rede enviando fluxos para o mesmo coletor, você poderá configurá-los para enviar para diferentes portas no coletor ou pode informar no nfsen o endereço IP de origem de cada roteador. Isso permite que nfsen mostre dados distintos de cada fonte.
-

Ajuste fino

- Blackhole



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



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

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

Case de sucesso: Intercampo ataque DNS

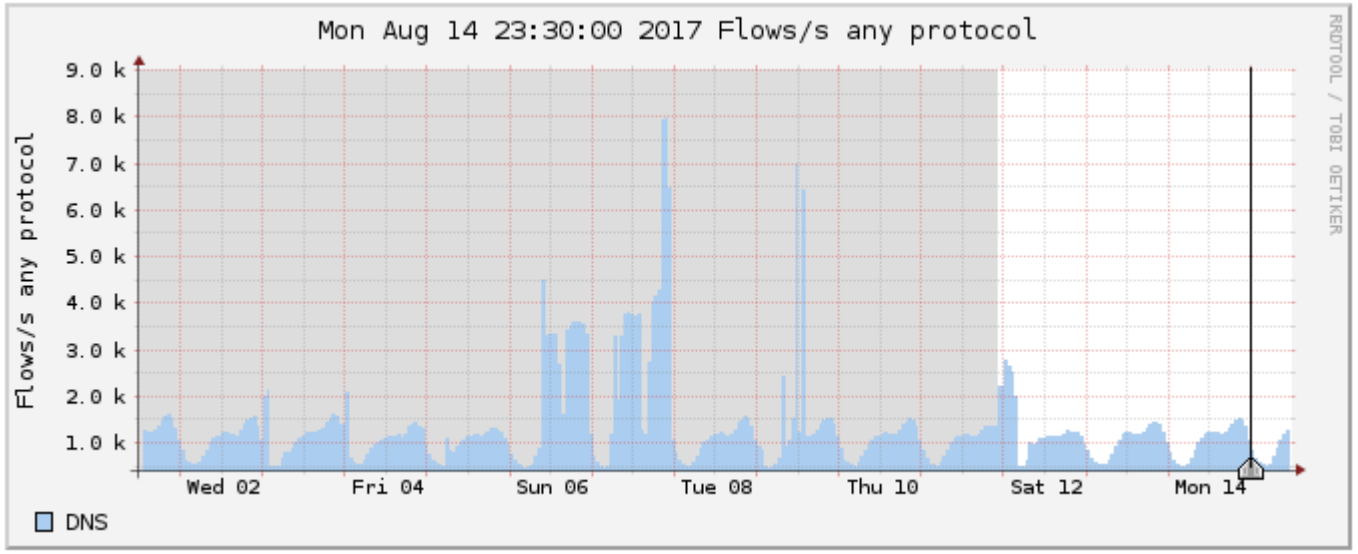
- Provedor começou a receber ataques de query ao DNS do provedor com origem de um cliente que possuia um sistema de hostpot
- O NFSen automaticamente enviou um e-mail relatando o ataque ao DNS
- Foi criado uma regra de firewall no na borda isolando consultas deste cliente até que o cliente resolva a situação
- Sistema normalizou
- Segue abaixo um exemplo de alarme ativo:

Alerts overview:

No.	Status	Name	Last Triggered
1	armed	POSSIVEL-ATAQUE	Tue Aug 15 11:20:00 2017
2	fired	NTP	Tue Aug 15 11:25:00 2017
3	armed	DNS	Sat Aug 12 06:20:00 2017
4	armed	SNMP	Mon Jul 24 15:45:00 2017
5	armed	SSDP	Tue Aug 15 02:25:00 2017
6	armed	UDP	Mon Aug 7 19:45:00 2017

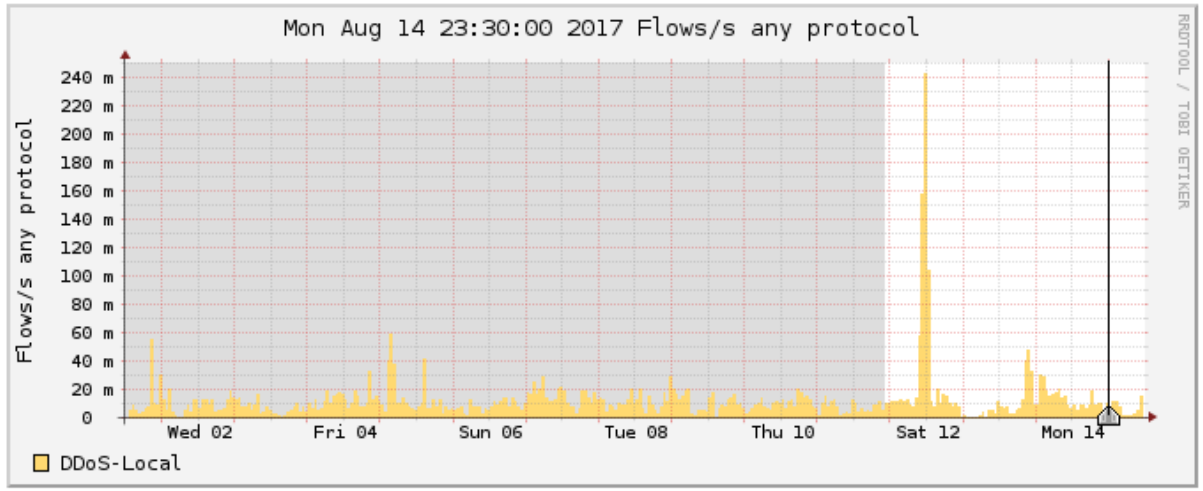
Case de sucesso: Intercampo ataque DNS

- O ataque ao DNS é muito dificil mitigar sem uma ferramenta de analise de flow.

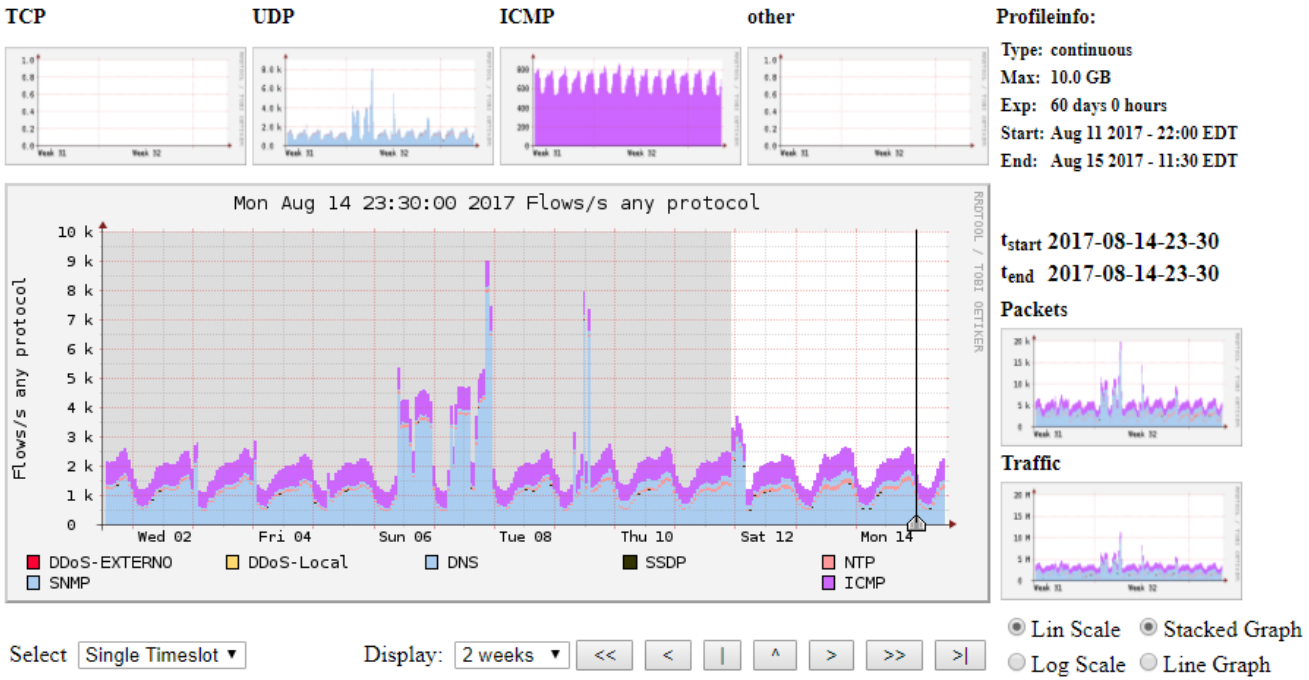


Case de sucesso: Intercampo DDoS

- Provedor começou a receber ataques volumetricos após expansão da rede para outras cidade.
- Após instalação do NFSen
- Foi idedificado em menos de 5 minutos o destino do ataque na rede local usando o nfsen
- Foi feito o anucio do ip de destino da balckhole.
- E em menos de 5 minutos o ataque não chegou mais na borda
- Exemplo abaixo de um sensor na porta 0.



Dashboard exemplo para UDP:



Statistics timeslot Aug 14 2017 - 23:30

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
ICMP	608.1 /s	0 /s	0 /s	608.1 /s	0 /s	1.5 k/s	0 /s	0 /s	1.5 k/s	0 /s	1.1 Mb/s	0 b/s	0 b/s	1.1 Mb/s	0 b/s
SNMP	173.9 /s	0 /s	173.9 /s	0 /s	0 /s	1.2 k/s	0 /s	1.2 k/s	0 /s	0 /s	939.7 kb/s	0 b/s	939.7 kb/s	0 b/s	0 b/s
NTP	57.4 /s	0 /s	57.4 /s	0 /s	0 /s	201.7 /s	0 /s	201.7 /s	0 /s	0 /s	114.0 kb/s	0 b/s	114.0 kb/s	0 b/s	0 b/s
SSDP	6.0 /s	0 /s	6.0 /s	0 /s	0 /s	15.6 /s	0 /s	15.6 /s	0 /s	0 /s	17.1 kb/s	0 b/s	17.1 kb/s	0 b/s	0 b/s
DNS	853.8 /s	0 /s	853.8 /s	0 /s	0 /s	1.8 k/s	0 /s	1.8 k/s	0 /s	0 /s	969.5 kb/s	0 b/s	969.5 kb/s	0 b/s	0 b/s
DDoS-Local	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	5.0 b/s	0 b/s	5.0 b/s	0 b/s	0 b/s
DDoS-EXTERNO	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	18.8 b/s	0 b/s	18.8 b/s	0 b/s	0 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	1.7 k/s	0 /s	1.1 k/s	608.1 /s	0 /s	4.8 k/s	0 /s	3.3 k/s	1.5 k/s	0 /s	3.1 Mb/s	0 b/s	2.0 Mb/s	1.1 Mb/s	0 b/s

All None Display: Sum Rate

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
- _
- MANUAL DE INSTALAÇÃO DO NFSEN

ftp://ftp.registro.br/pub/gts/gts29/04-NFSEN.pdf

Contato

- Alexandre.gioavaneli@gmail.com
- Skype:live:alexandre.Giovaneli
- Movel:+55 31 9 8255 5555
- https://www.facebook.com/alexandre.giovaneli