Boas práticas de segurança em redes

Tayla Guimarães

#juntossomosmais

Tayla Guimarães

- Cursando Engenharia Elétrica com ênfase em Telecomunicações.

- Experiência no mercado de Telecomunicações.

- Conhecimento regulatório para provedores.

Objetivo

Mostrar alguns ataques mais comuns que ocorrem no ambiente de redes e também, um conjunto de ferramentas para mitigar tais ataques, dentro de um grande universo de boas praticas de segurança.

Você acredita que sua rede está realmente segura?

O que veremos nesta apresentação:

- Entendendo DoS e DDoS
- Quais os tipos de ataque DDoS
- Soluções e tipos de filtros para evitar e/ou mitigar ataques:
  - Filtragem Syn
  - Regras de Firewall
  - Bloqueio de DNS
  - Gerência da porta 25
  - Anti Spoofing
  - Bogons - Team Cymru
  - Serviço UTRS
  - SafeBGP
  - Netflow
  - Torch
- Diagrama de rede onde os filtros são implantados
- Benefícios dos filtros implantados

Entendendo o que é DoS e DDoS

- Negação de serviço, ou DoS (Denial of Service), é uma técnica utilizada para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

- Quando um conjunto de equipamentos é utilizado no ataque recebe o nome de Ataque Distribuído de Negação de Serviço (DDoS - Distributed Denial of Service).

Ataque DDoS

Ataques DDoS acima de 500 Gbps se intensificam após Rio 2016, aponta Embratel

João Monteiro 27/10/2016 ataque volumétrico, DDoS, Embratel, Jogos Olimpicos, Mario Rachid, negação de serviço, olimpiada, Rio 2016, Segurança

Operadora responsável pela rede do evento avalia que os Jogos adiantaram o alto volume desse tipo de ameaça.

Durante palestra realizada hoje (27/10) no Gartner Symposium/ITXPO 2016, Mario Rachid, diretor executivo de Soluções Digitais da Embratel, revelou que os Jogos Olímpicos Rio 2016 mudou o padrão de ataques de negação de serviço (DDoS) no Brasil. Segundo dados da operadora, a média volumétrica dos ataques era de 30 Gbps entre janeiro e julho deste ano. Em agosto, quando começou o evento, a média passou para 500 Gbps, com a rede sendo atacada diariamente por volumes entre 500 e 600 Gbps.

Rachid diz que os hackers já vinham se preparando para

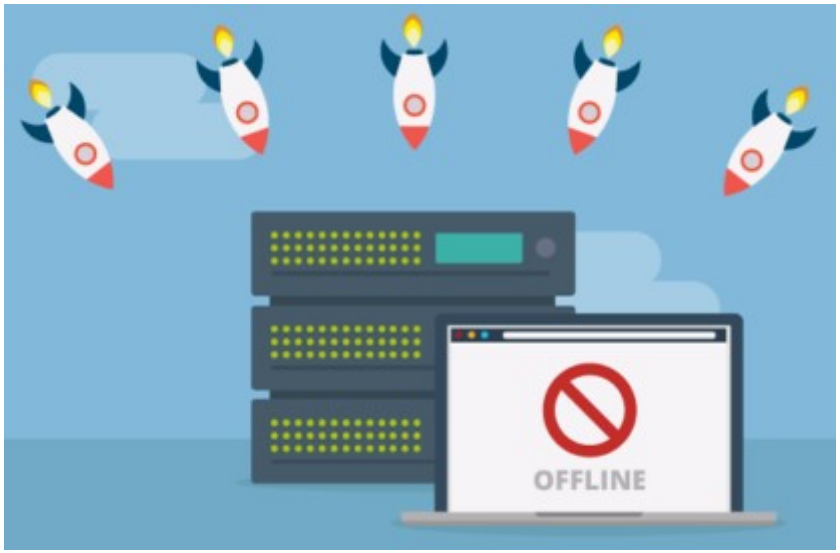
https://ipnews.com.br/ataques-ddos-acima-de-500-gbps-se-intensificam-apos-rio-2016-aponta-embratel/

Quais os tipos de ataque DDoS?

- Ataques a camada de aplicação

- Ataques de exaustão de hardware

- Ataques volumétricos



Ataque a camada de aplicação

- Exploram características específicas de uma aplicação ou serviço.

- São mais difícieis de serem identificados.

- Não necessitam de muitas máquinas e nem de muito tráfego para ser realizado.

- Exemplos: HTTP GET, HTTP POST, VoIP (SIP INVITE Flood) e Slow Read DDoS.

Ataque de exaustão de hadware

- Tentam consumir a capacidade de equipamentos e exaurir seus recursos.

- Em roteadores: tentar consumir recursos, como CPU e memória, e a capacidade de encaminhamento de pacotes por segundo (pps).

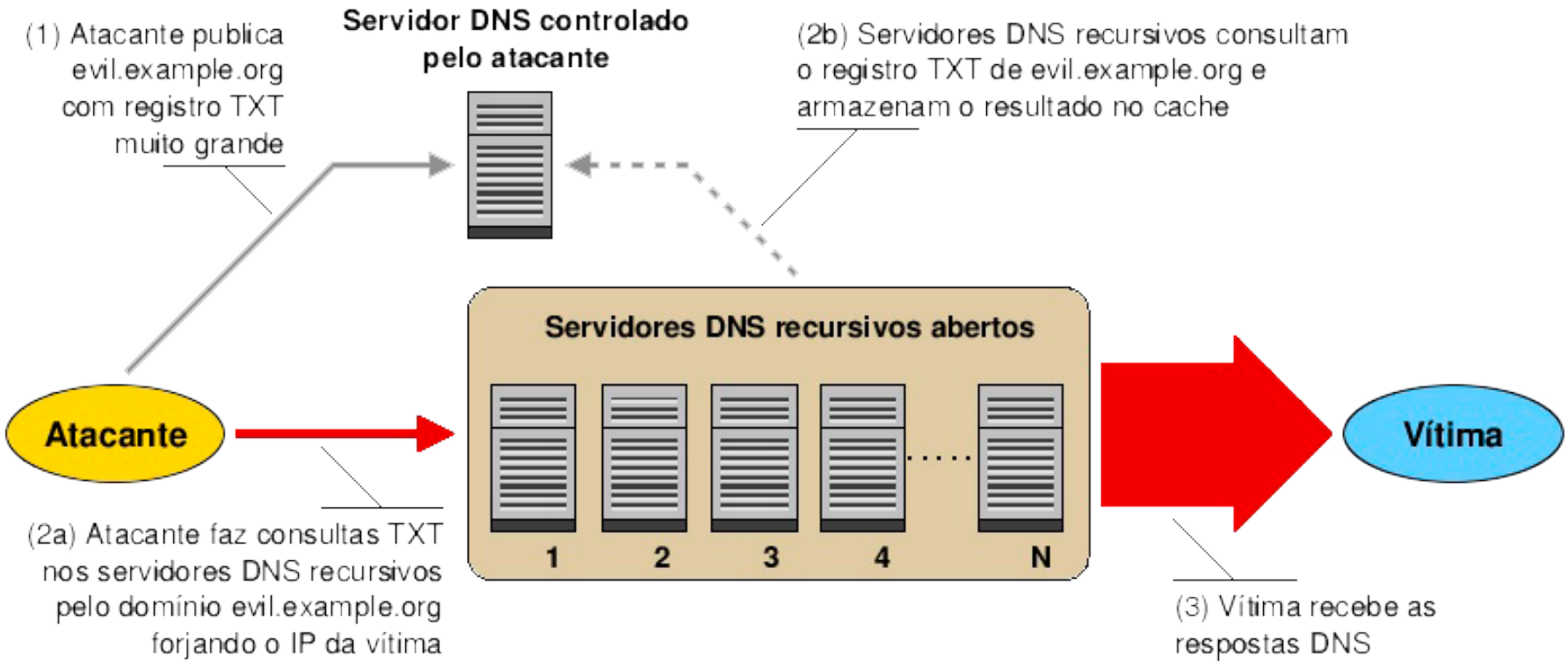
- Em firewalls e IPSs: tentam consumir a capacidade da tabela de estado de conexões, impedindo que novas conexões sejam estabelecidas.

Ataque Volumétrico

- Tentam consumir a banda disponível enviando ao alvo grande volume de tráfego.

- Exemplo: DRDoS (Distributed Reflective Denial of Service)

Ataque Volumétrico

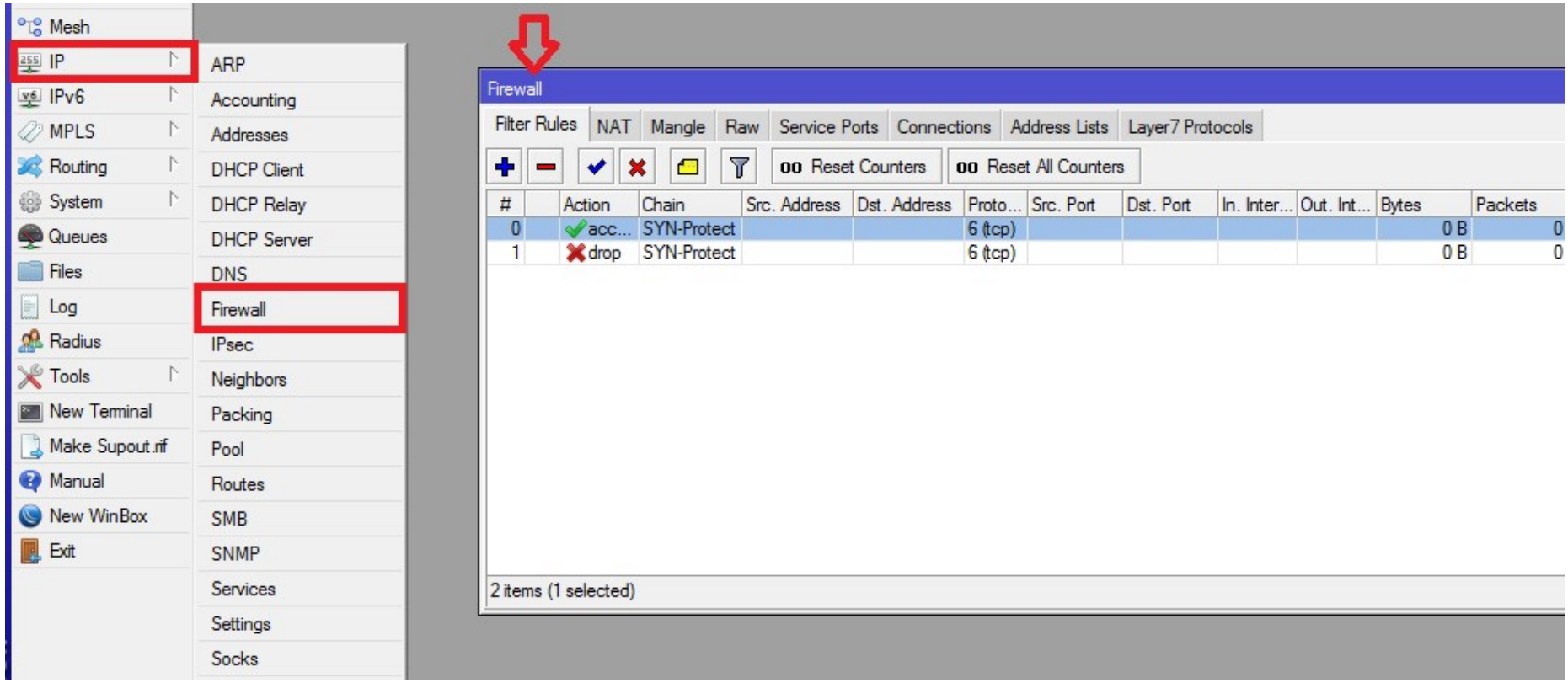


Soluções e tipos de filtros para evitar e/ou mitigar ataques

Filtragem SYN (DoS)

- É um conjunto de regras aplicadas ao Firewall para evitar o ataque SYN que é uma das formas de ataque de negação de serviço (também conhecido como Denial of Service - DoS).

Filtragem SYN no RouterOS:



Filtragem SYN:

- SYN filtering

Some advanced filtering can by applied to tcp packet state.

```
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new \
action=jump jump-target=SYN-Protect comment="SYN Flood protect" disabled=yes
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new \
action=accept comment="" disabled=no
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-state=new \
action=drop comment="" disabled=no
```

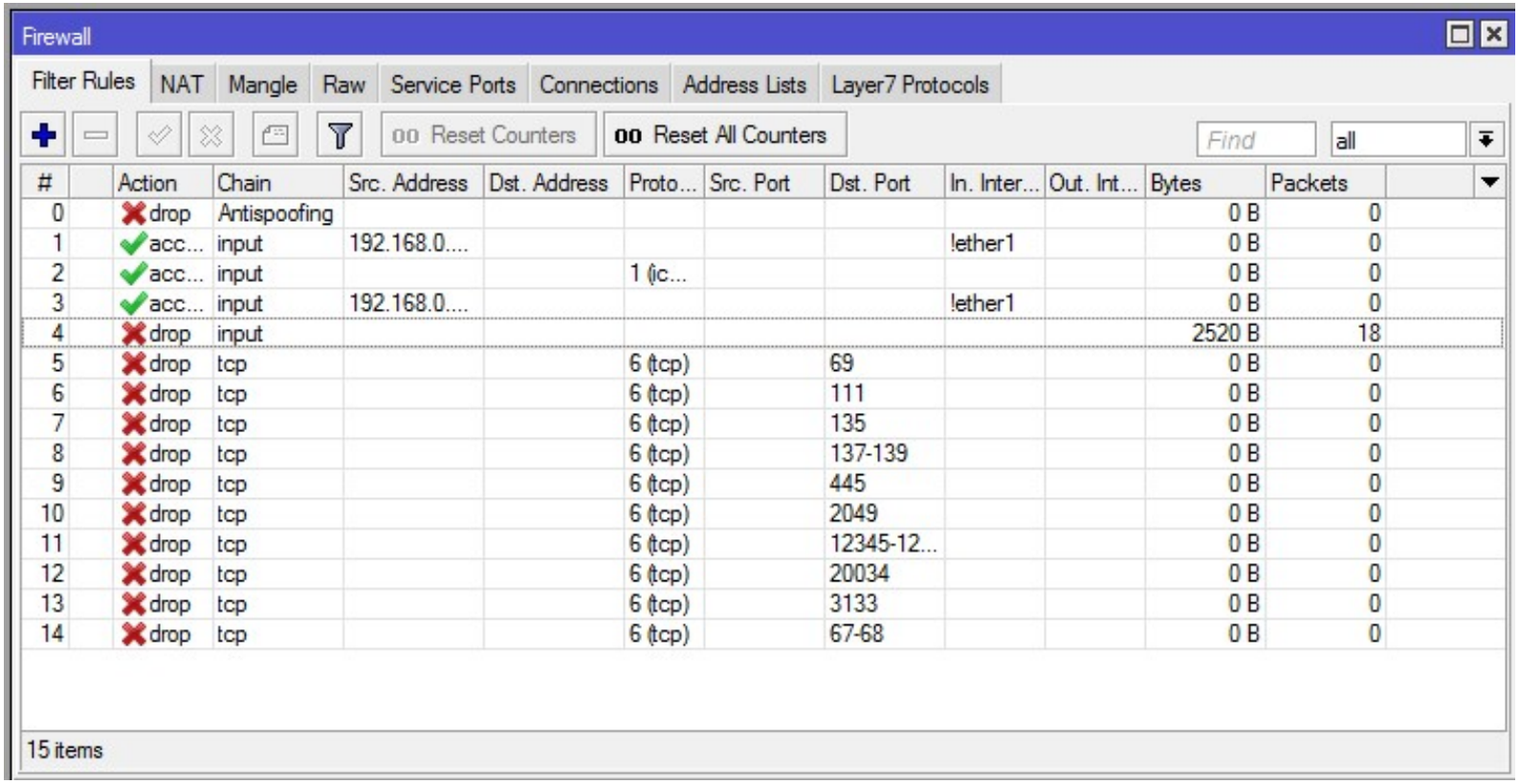
'syn limit=400' is a threshold, just enable rule in forward chain for syn packets to get dropped (for excessive amount of new connections)

https://wiki.mikrotik.com/wiki/DoS_attack_protection

Regras de Firewall

- Firewall é o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

Regras de Firewall no RouterOS:

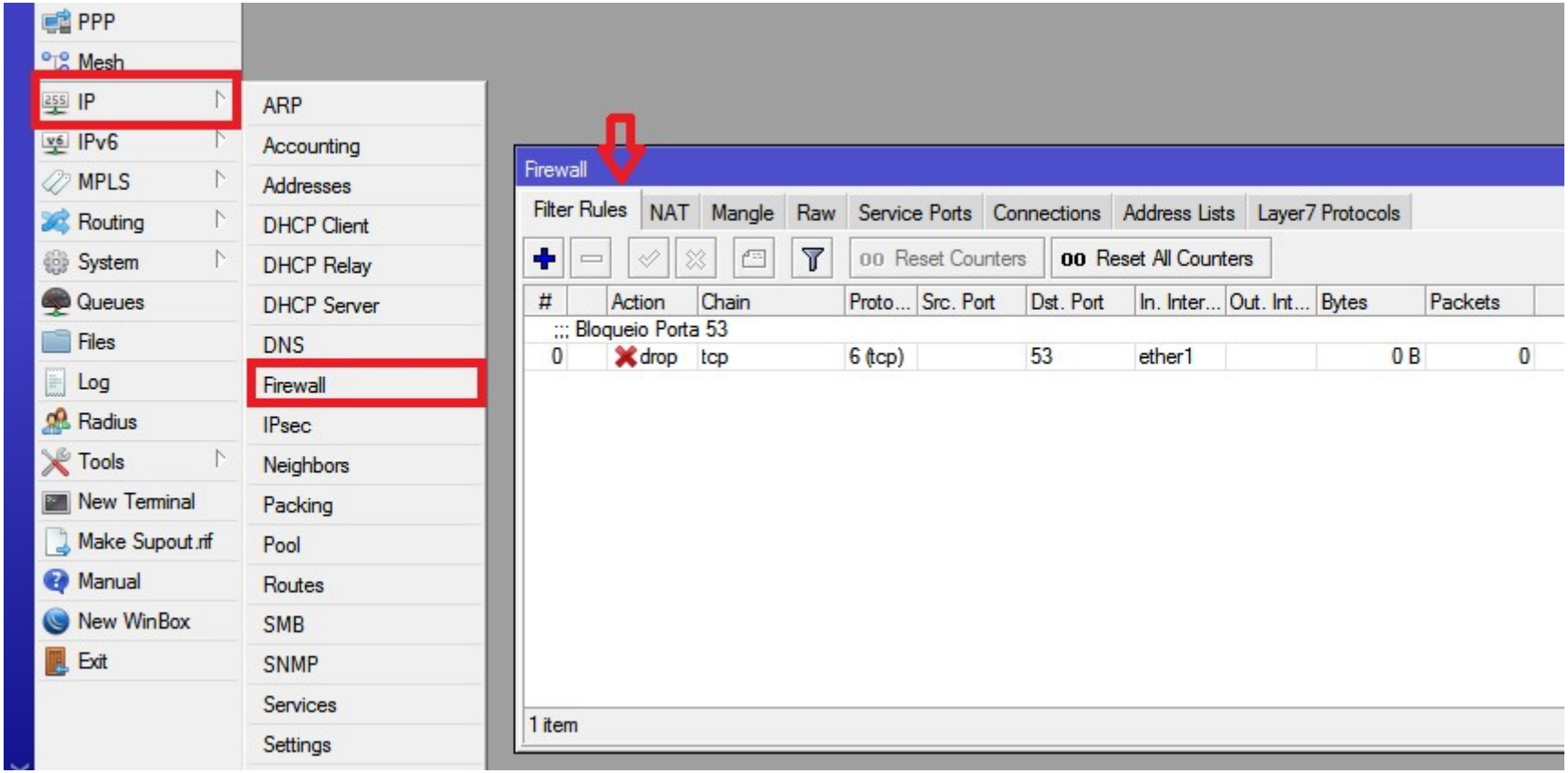


#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	drop	Antispoofing								0 B	0
1	acc...	input	192.168.0....					!ether1		0 B	0
2	acc...	input			1 (ic...					0 B	0
3	acc...	input	192.168.0....					!ether1		0 B	0
4	drop	input								2520 B	18
5	drop	tcp			6 (tcp)		69			0 B	0
6	drop	tcp			6 (tcp)		111			0 B	0
7	drop	tcp			6 (tcp)		135			0 B	0
8	drop	tcp			6 (tcp)		137-139			0 B	0
9	drop	tcp			6 (tcp)		445			0 B	0
10	drop	tcp			6 (tcp)		2049			0 B	0
11	drop	tcp			6 (tcp)		12345-12...			0 B	0
12	drop	tcp			6 (tcp)		20034			0 B	0
13	drop	tcp			6 (tcp)		3133			0 B	0
14	drop	tcp			6 (tcp)		67-68			0 B	0

Bloqueio de ataque DNS

- Os servidores DNS são contatados pelos clientes através da porta 53, UDP. Eles são responsáveis por converter nomes e domínios nos endereços IP dos servidores.

Bloqueio de ataque DNS no RouterOS:

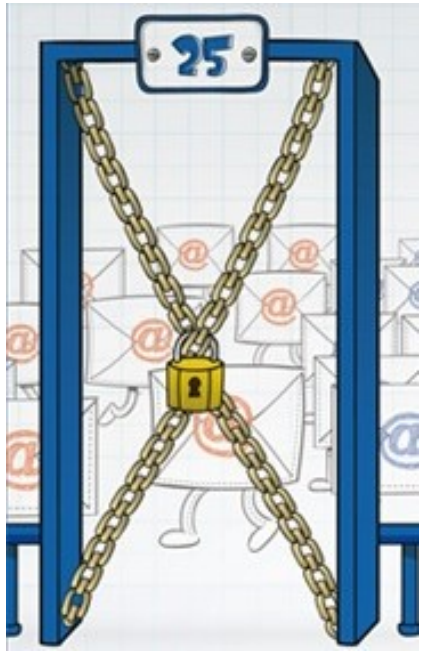


Gerência de porta 25

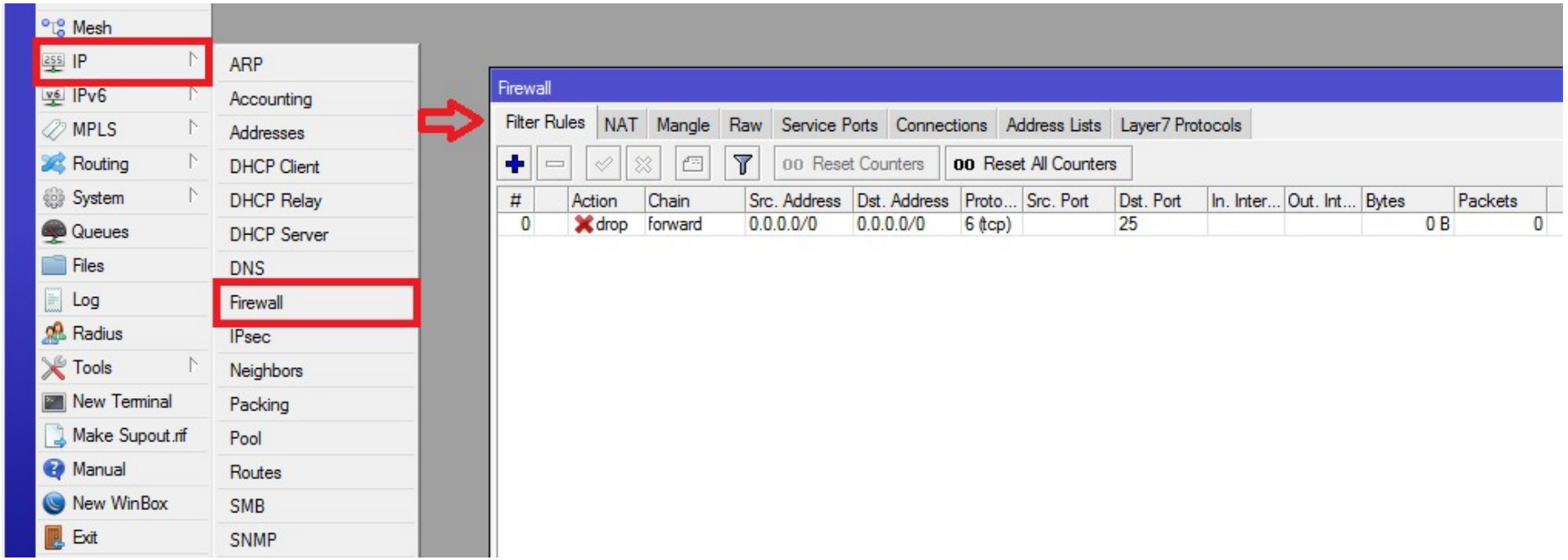
- A gerência de porta 25 é o nome dado ao conjunto de políticas e tecnologias, implantadas em redes de usuários finais ou de caráter residencial, que procura separar as funcionalidades de submissão de mensagens, daquelas de transporte de mensagens entre servidores.

Gerência de porta 25

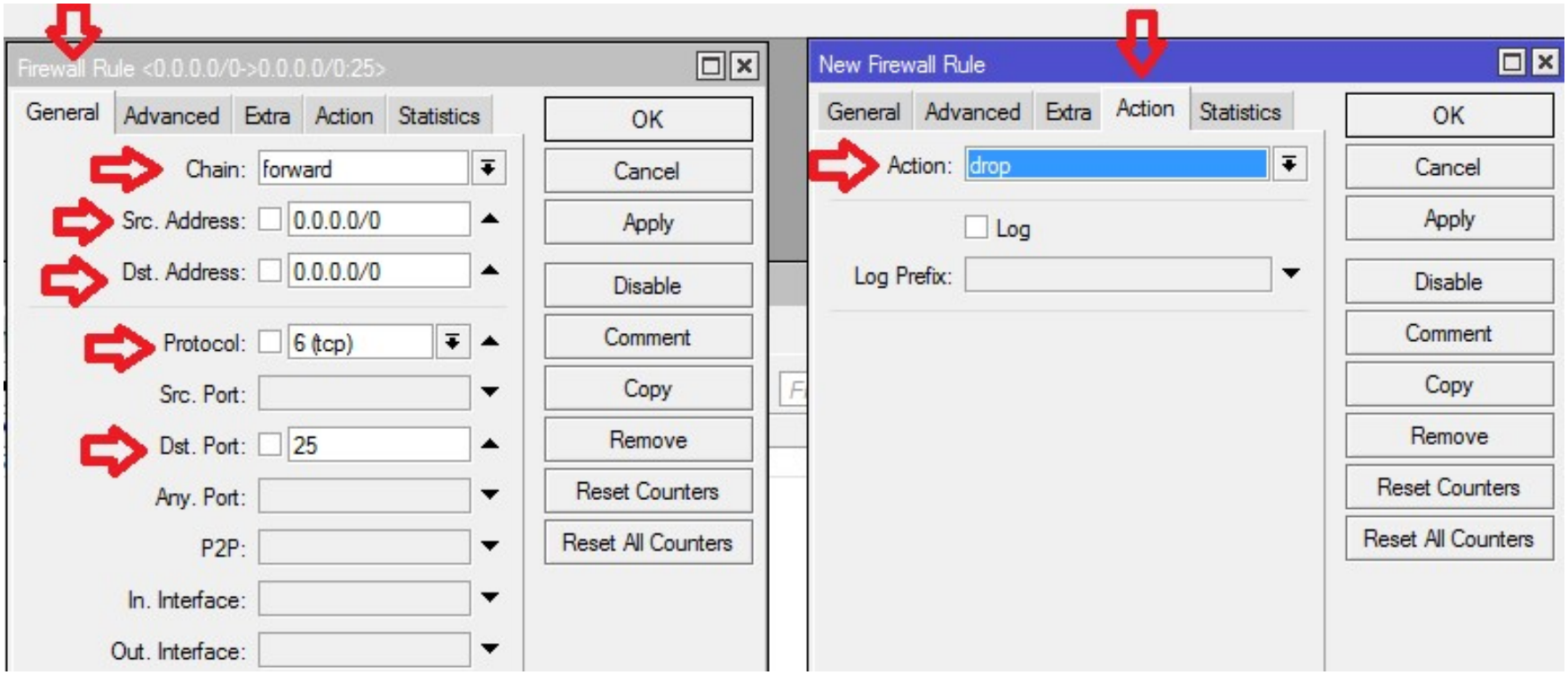
- Um filtro importante de ser configurado é o que impede a saída de tráfego da rede dos clientes domésticos com destino à porta 25/TCP, com o intuito de evitar o envio de spams.



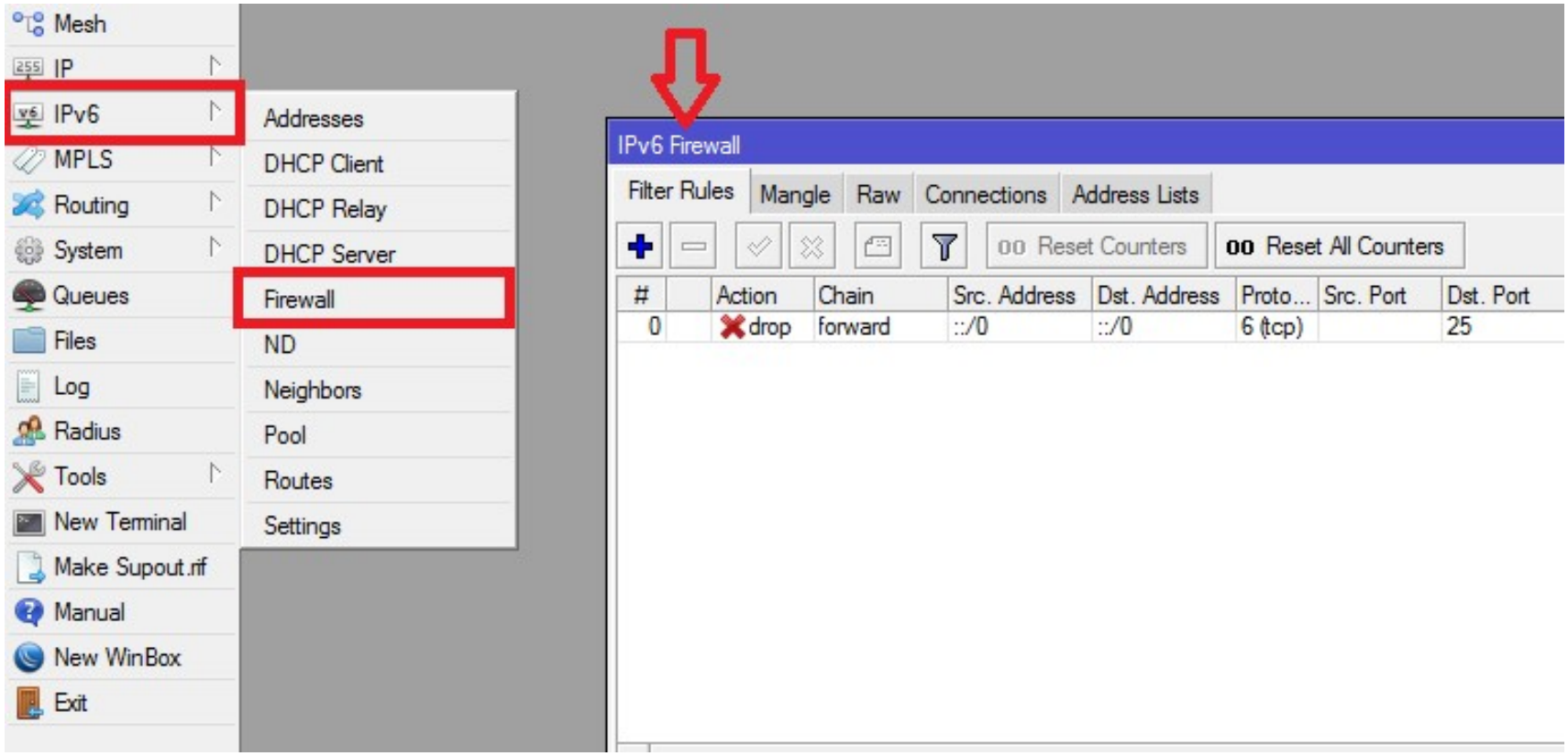
Gerência de porta 25 em IPv4 no RouterOS:



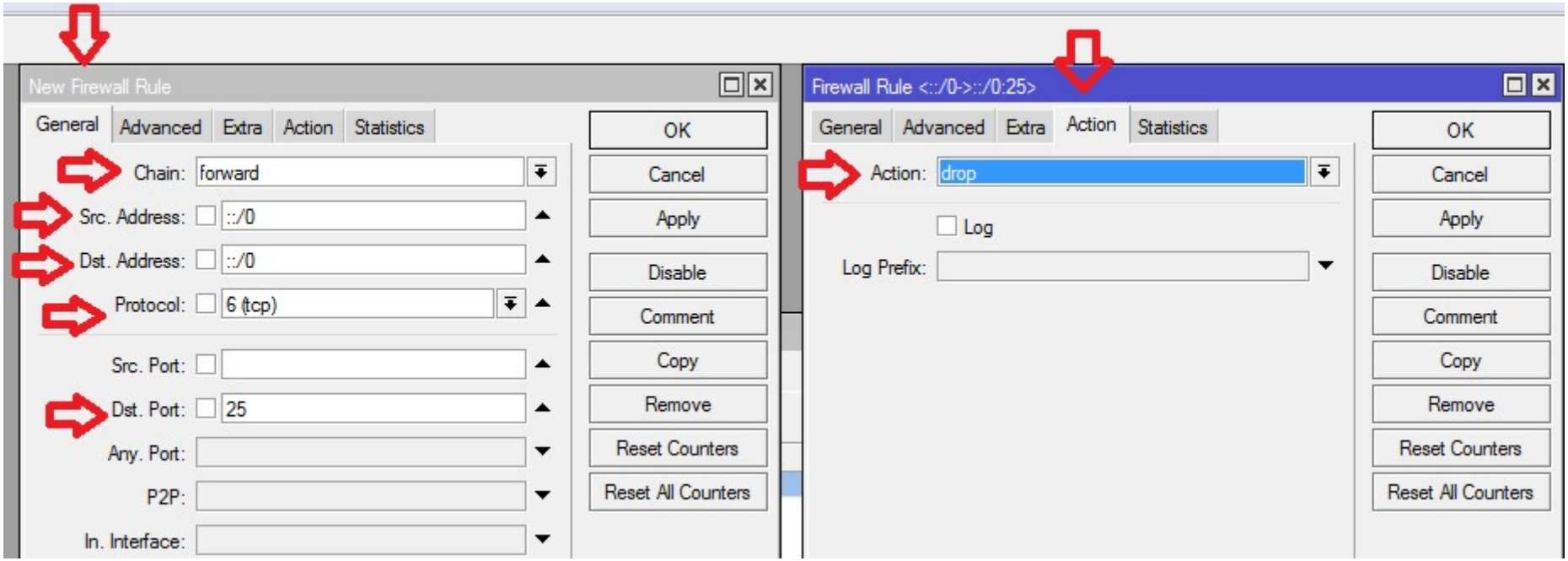
Gerência de porta 25 em IPv4 no RouterOS:



Gerência de porta 25 em IPv6 no RouterOS:



Gerência de porta 25 em IPv6 no RouterOS:



Anti Spoofing

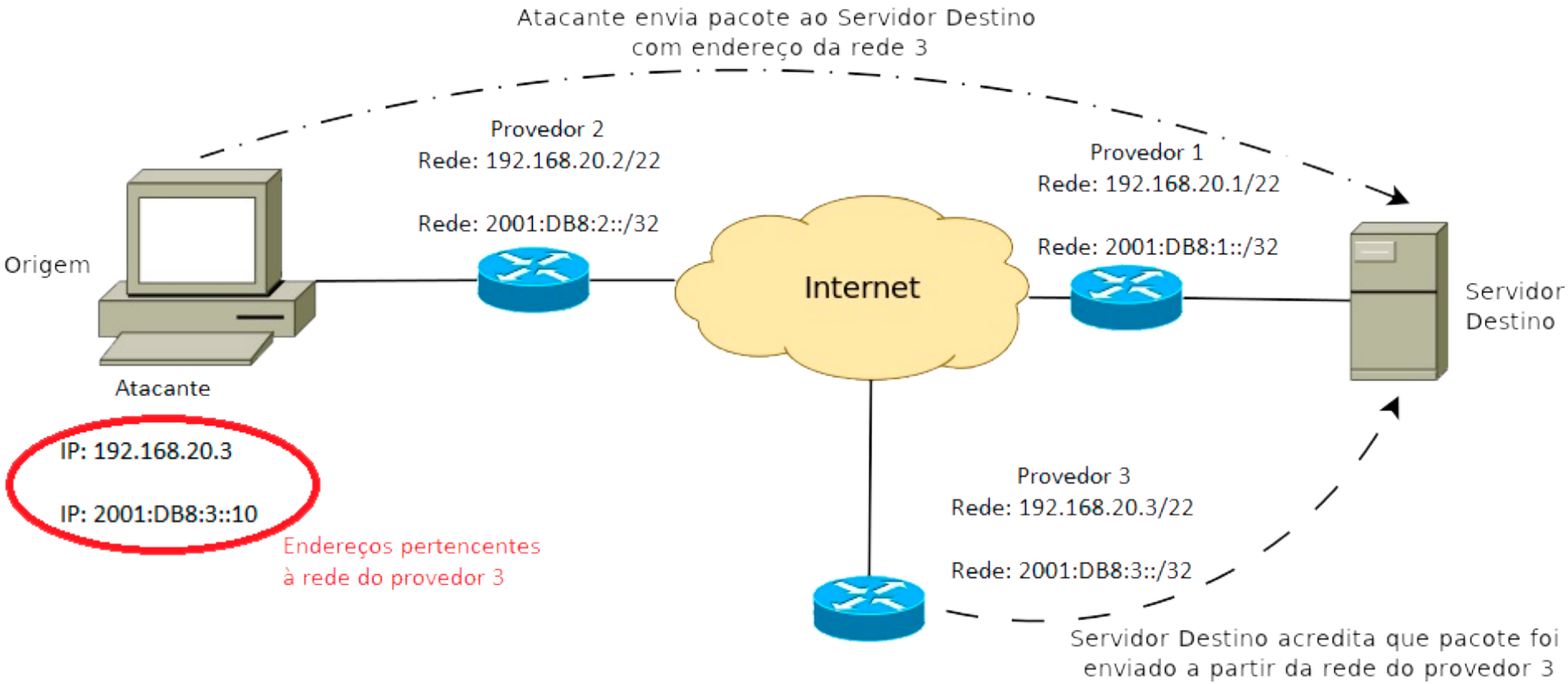
- Spoofing basicamente são pacotes com origens inválidas e muitas vezes é utilizado para ataques de negação de serviço. Apenas um filtro aplicado no próprio provedor de acesso, preferencialmente na interface do roteador conectada diretamente ao usuário, é eficaz.

Anti Spoofing

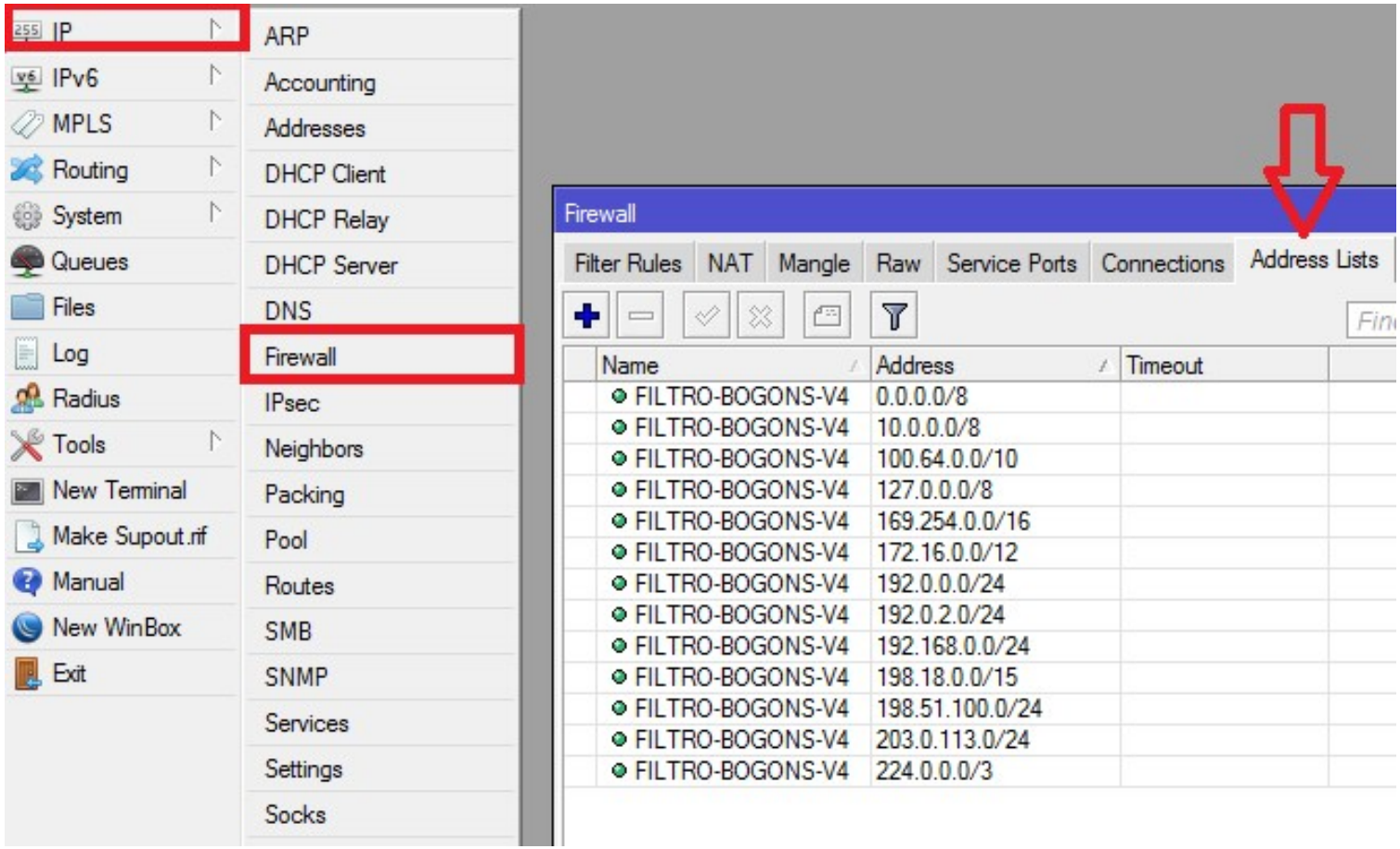
- Se os equipamentos na rede onde os pacotes se originam não verificam sua origem, qualquer ação posterior para identificá-los ou bloquá-los é muito dificultada.

- A BCP 38 (RFC 2827) recomenda que se filtrem pacotes na interface de entrada da rede do provedor, de forma a permitir somente aqueles cujo endereço de origem seja parte da rede conectada àquela interface.

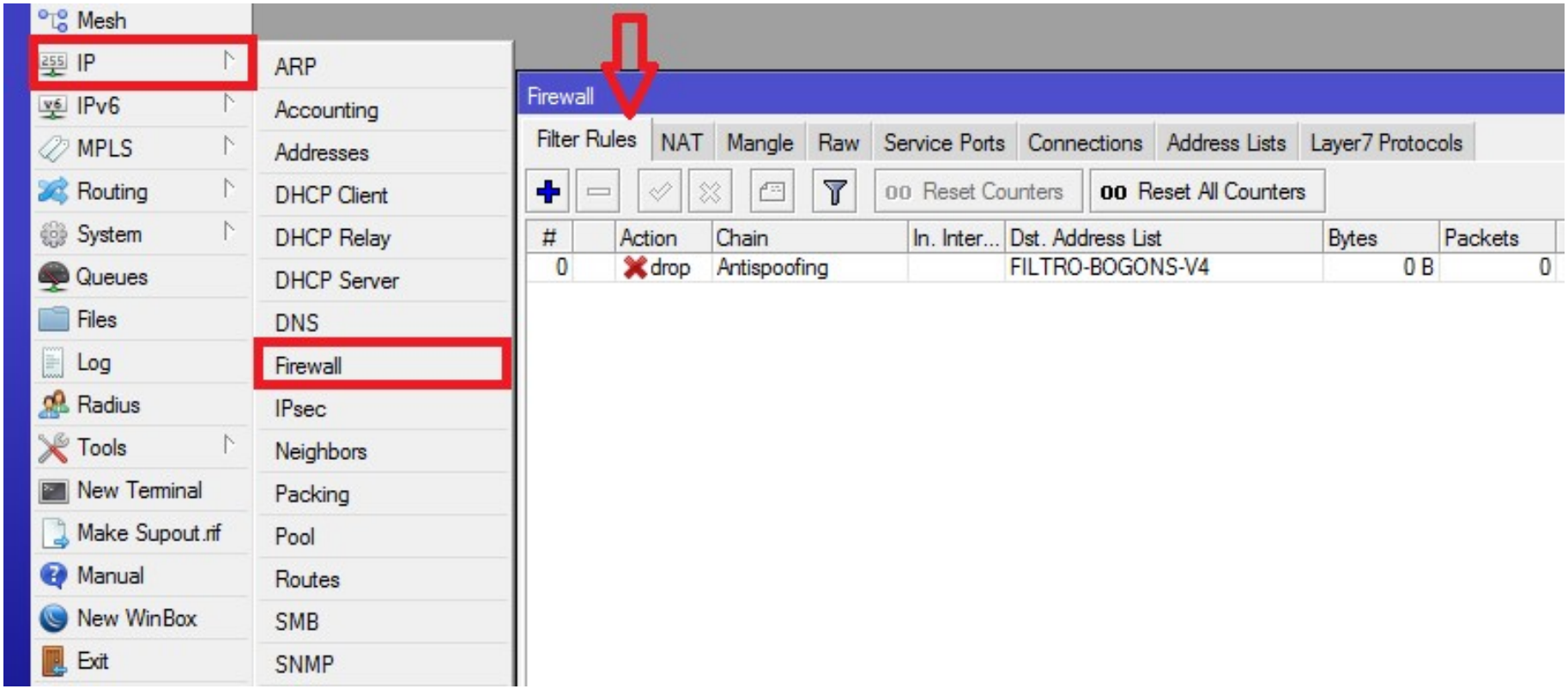
Anti Spoofing



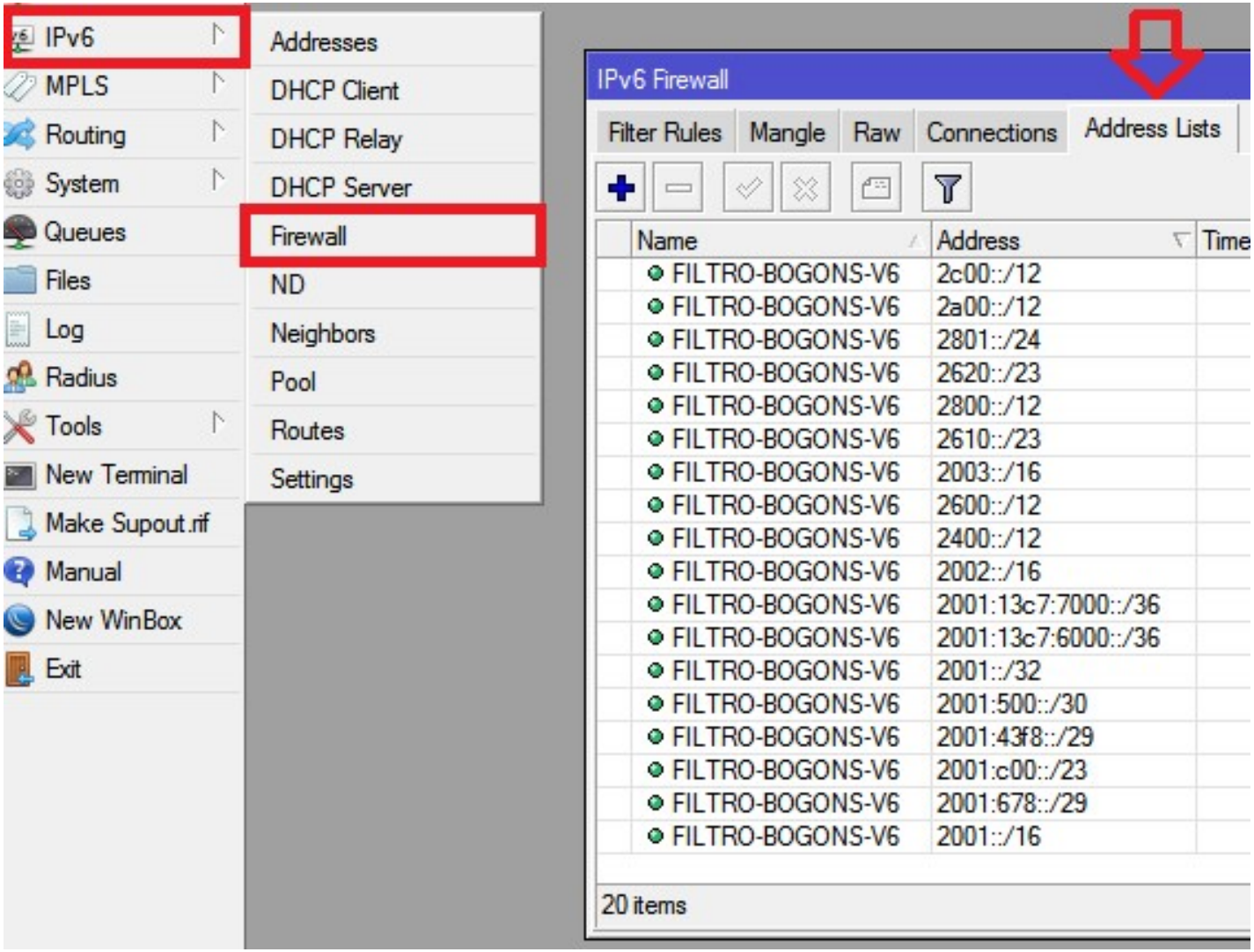
Configuração de Anti Spoofing IPv4 no RouterOS:



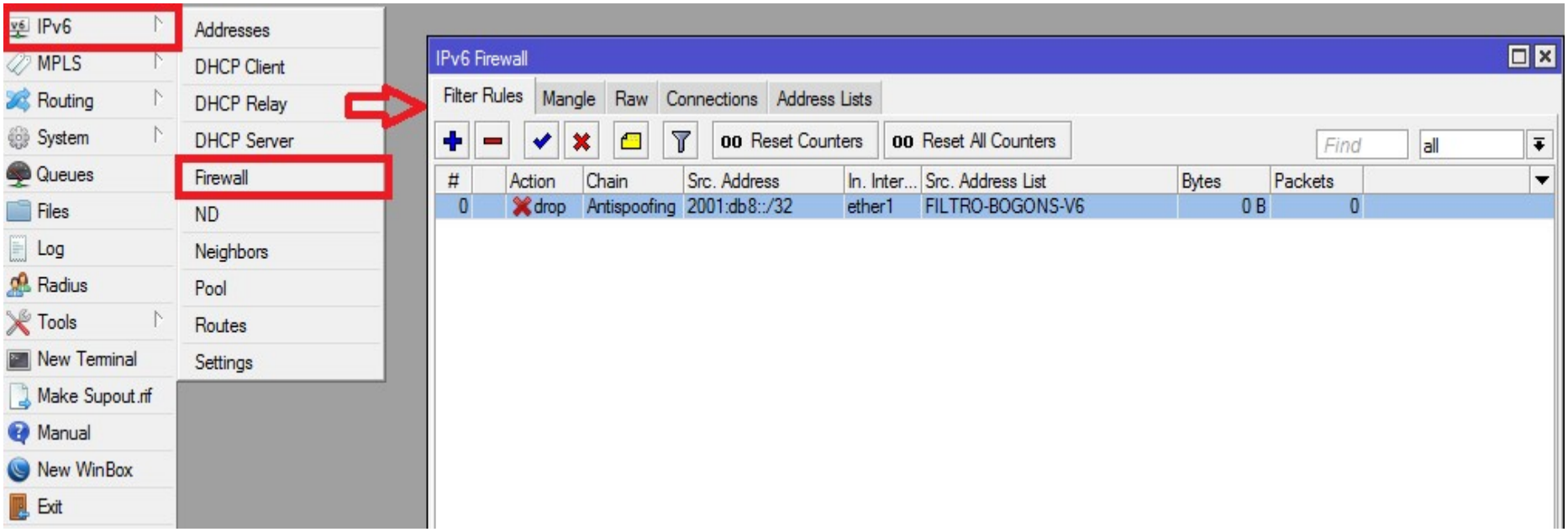
Configuração de Anti Spoofing IPv4 no RouterOS:



Configuração de Anti Spoofing IPv6 no RouterOS:

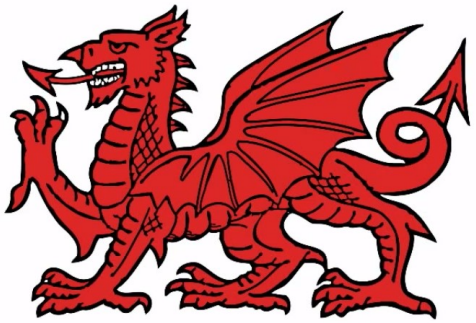


Configuração de Anti Spoofing IPv6 no RouterOS:



Bogons - Team Cymru

- Refere-se a um anúncio para um prefixo dentro de uma rede IP reservada ou não alocada. Bloquear rotas de bogon em um nível alto é bastante direto, uma série de listas de bogon são mantidas para facilitar a implementação de filtros de bogon, como os do Team Cymru.

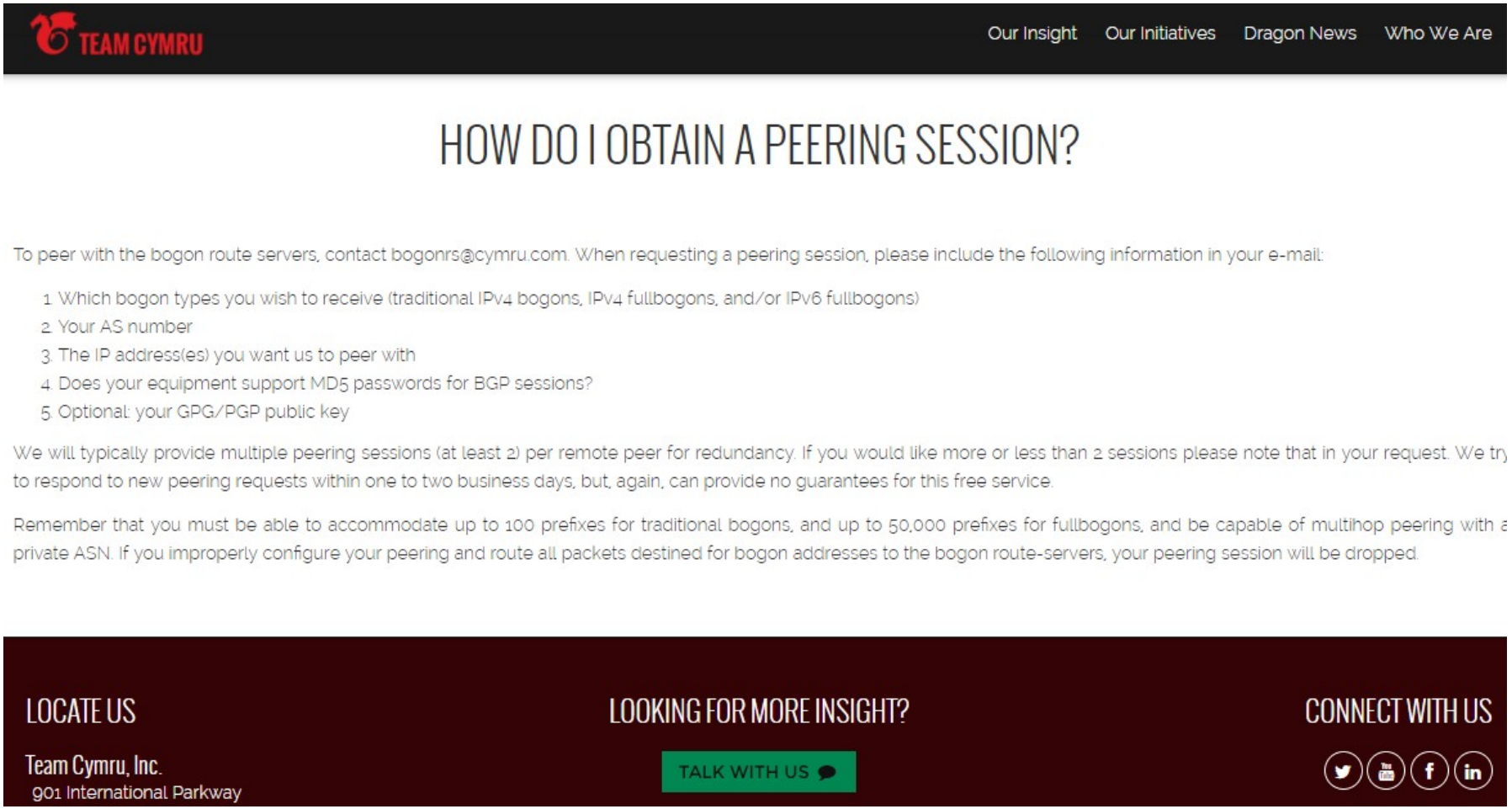


TEAM CYMRU NFP

INSIGHT THAT IMPROVES LIVES

https://www.team-cymru.org/

Bogons - Team Cymru



http://www.team-cymru.org/bogon-reference.html

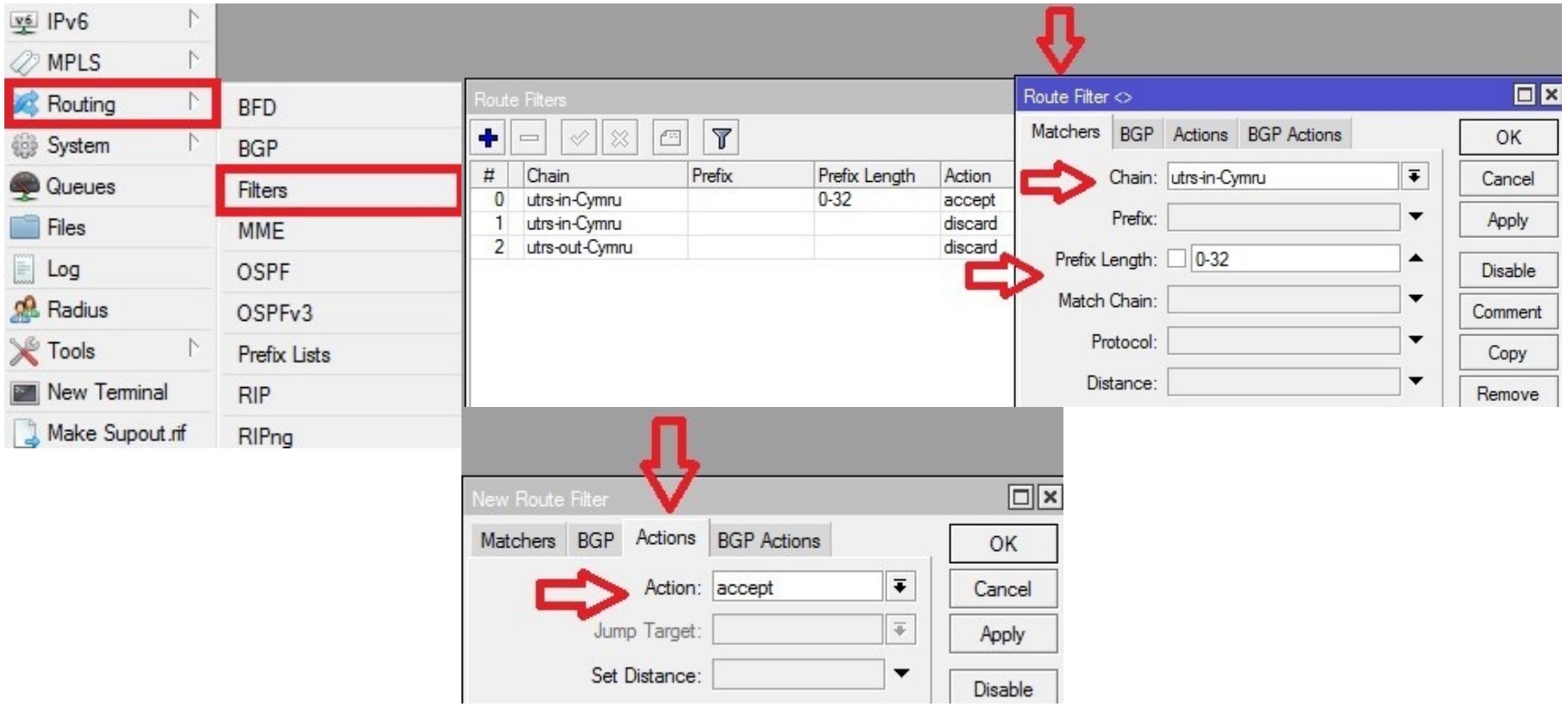
Serviço UTRS

- O UTRS é um sistema que ajuda a mitigar grandes ataques de infra-estrutura, alavancando uma rede existente de BGP speakers, ISPs, provedores de hospedagem e instituições educacionais que distribuem automaticamente regras de filtro baseadas em BGP verificadas de vítima para redes cooperantes.

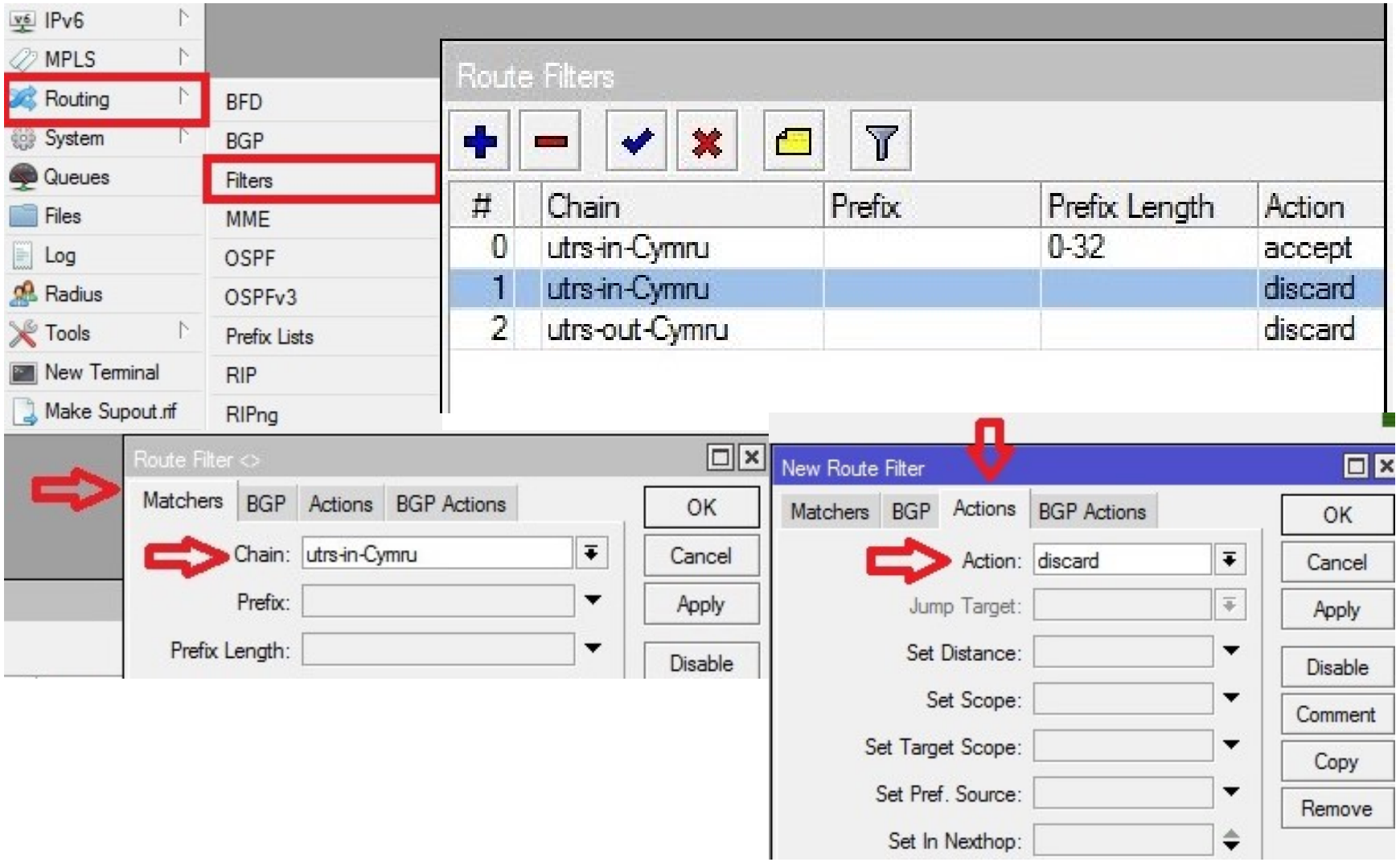
- Ao usar UTRS, as operadoras também estarão criando um bloqueio e interrompendo o tráfego de ataque na fonte, economizando muitos pacotes de ataque possíveis de sua própria rede, além de impedir que eles ocupem recursos de rede desnecessários em qualquer outra rede no meio.

TEAM CYMRU NFP
INSIGHT THAT IMPROVES LIVES
https://www.team-cymru.org/

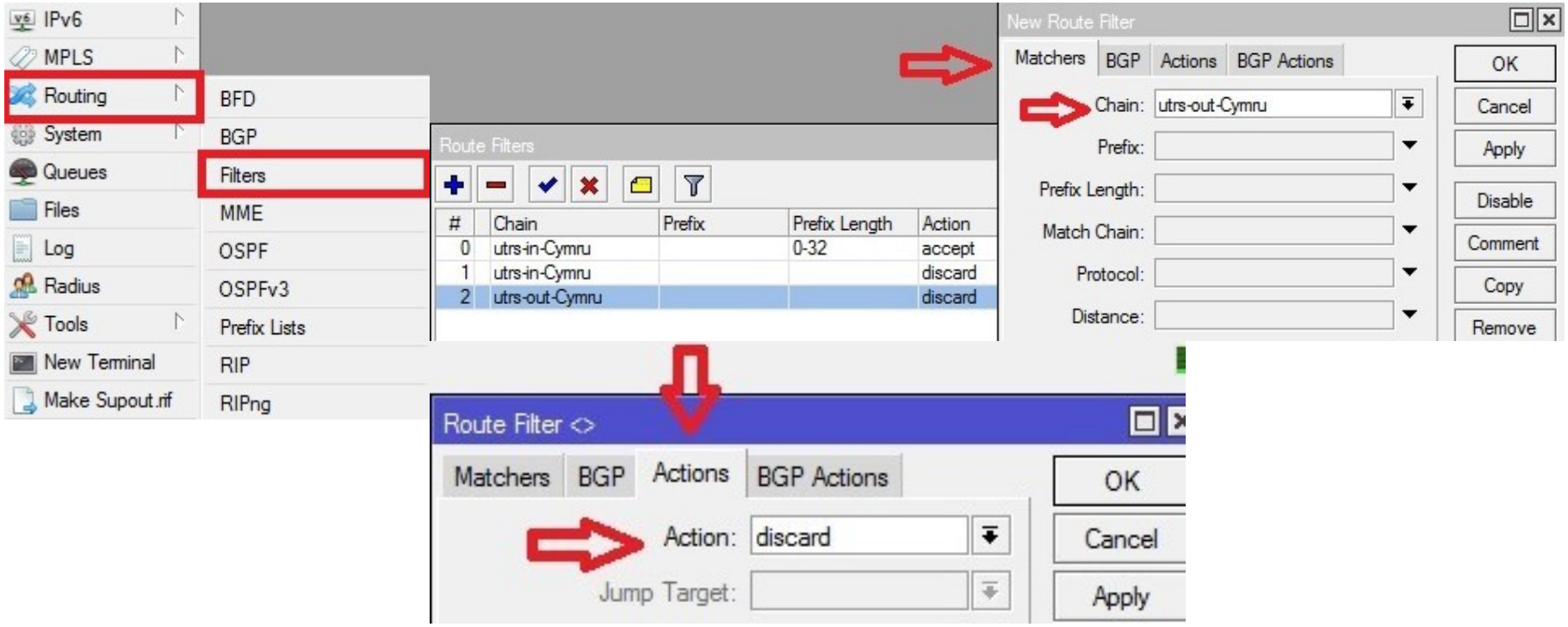
Configuração UTRS no RouterOS:



Configuração UTRS no RouterOS:



Configuração UTRS no RouterOS:

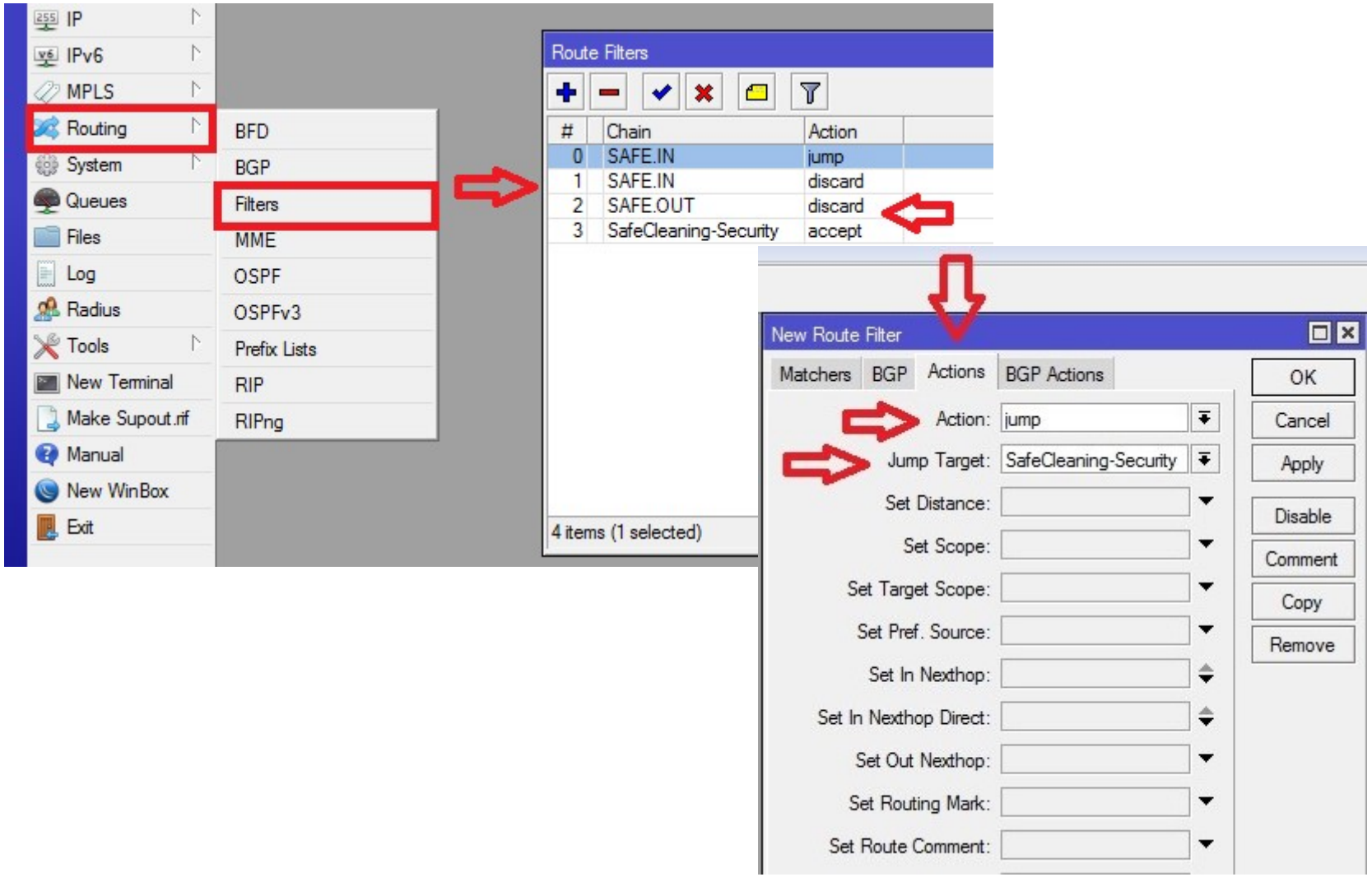


SafeBGP

- O Safe BGP Security é uma coletânea de IP’s que estão listados nas principais Blacklist, Bogons, e IP’s que mais fazem ataques, é como um escudo que inibi as investidas de IP’s maliciosos a sua rede, evitando a vulnerabilidade e os ataques.

SAFE
BGP

Configuração de SafeBGP no RouterOS:

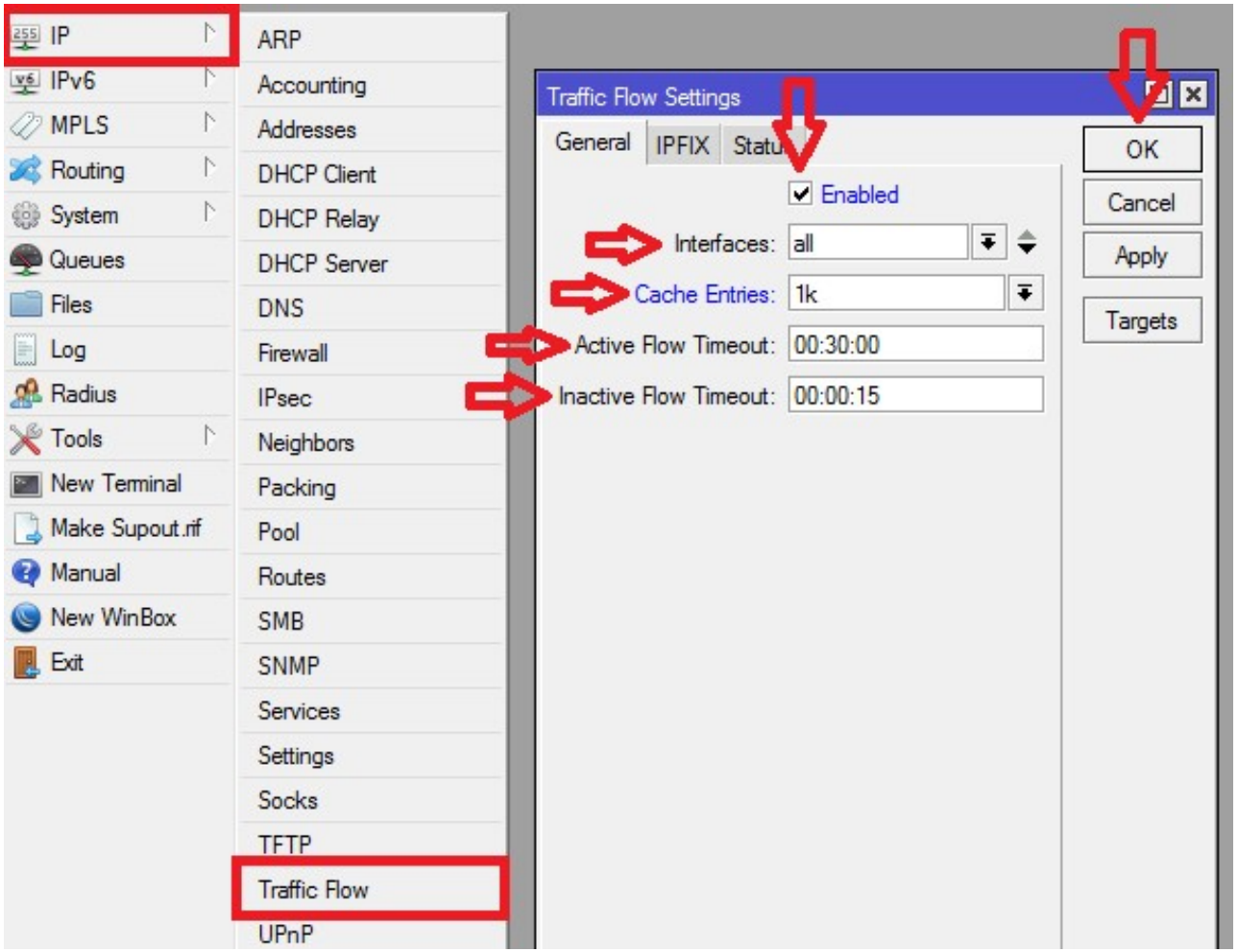


NetFlow

- Este recurso foi desenvolvido para monitorar o tráfego de rede e identificar quais são os principais fluxos de dados que passam por ela, visando compreender o que gera o tráfego e quais são os principais utilizadores da banda.

- A partir da ativação do NetFlow no roteador, ele passa a identificar os pacotes de dados não mais isoladamente, como outras tecnologias, mas como fluxos, com início, meio e fim. Quando os fluxos são identificados, eles são armazenados no NetFlow Cache para caracterização e compreensão do tráfego da rede. Após 30 minutos são apagados da memória.

Configuração de NetFlows no RouterOS



Torch

- É uma ferramenta de análise de tráfego em tempo real que pode ser usada para entender o fluxo de tráfego através de uma interface. Você pode verificar o tráfego classificado pelo nome do protocolo, endereço de origem, endereço de destino e porta. Torch mostra os protocolos que você escolheu e a taxa de dados tx/rx para cada um deles.

Configuração de Torch no RouterOS:

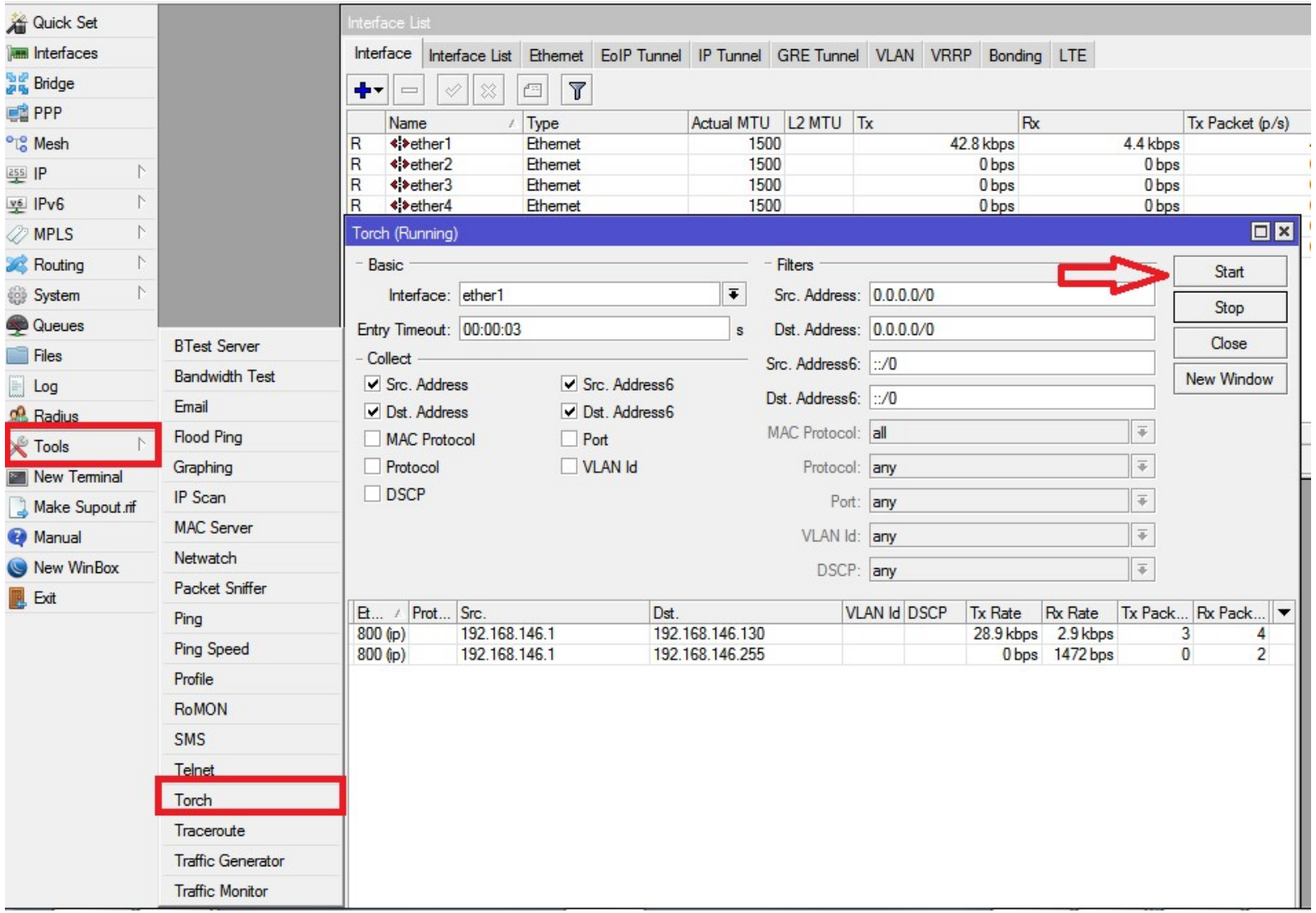
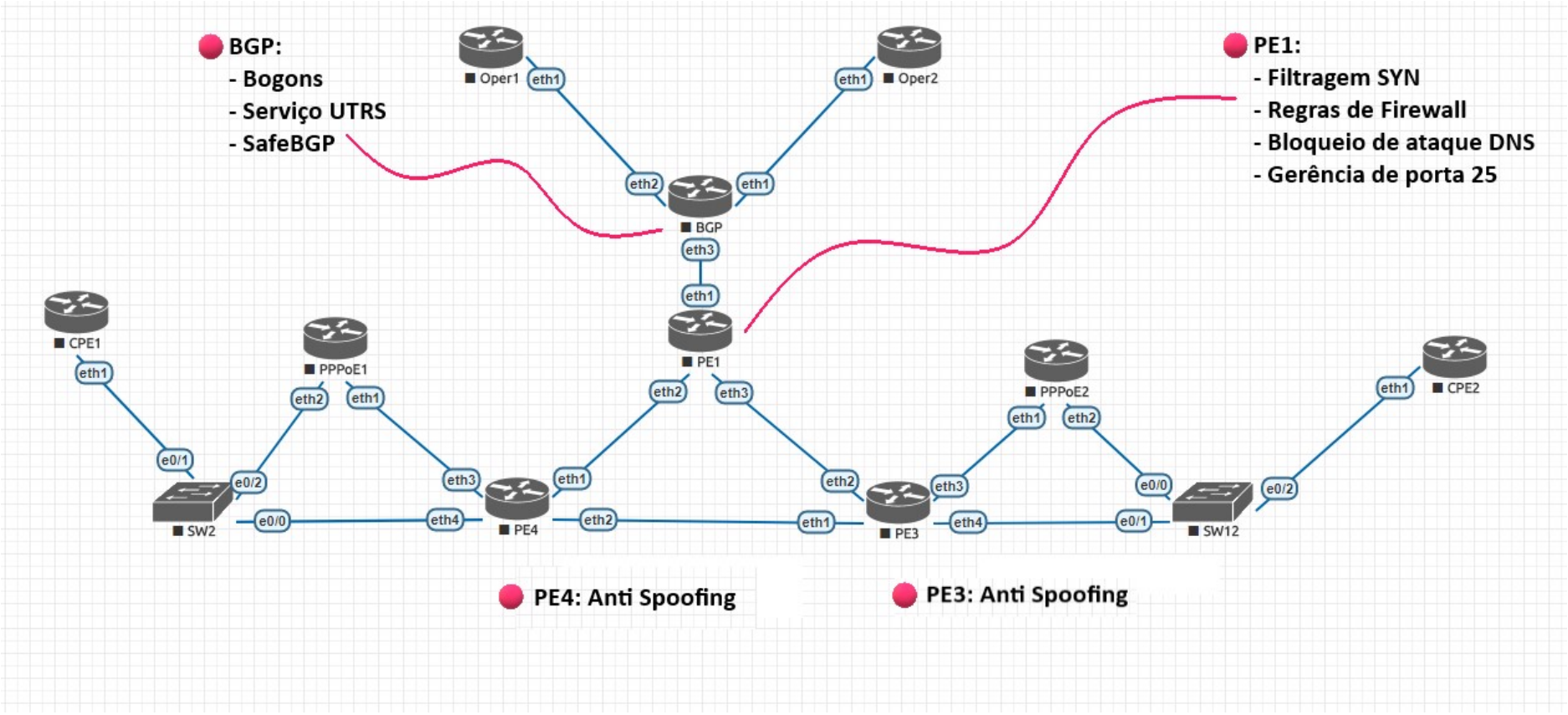


Diagrama de rede onde os filtros são implantados



Benefícios dos filtros implantados:

- Controle e monitoramento de tráfego

- Mitigar, ou seja, recuperar todos os pacotes IP que não são legítimos, deixando passar os pacotes legítimos

- Análise do tráfego e detecção de ataques em tempo real

- Aspirar o tráfego de entrada no seu servidor

- Estabilidade na rede

Dúvidas?

OBRIGADA!!

Tayla Guimarães Oliveira

E-mail: tayla.oliveira@solintel.com.br

Telefone: +55 43 3373-9356