# 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.
- Coordenadora do departamento de Engenharia da Solintel.

# Objetivo

Mostrar os riscos que ocorrem no ambiente de redes e mecanismos para mitigar os ataques mais  comuns, dentro do grande universo que são as boas praticas de segurança.

# Você acredita que sua rede está realmente segura?

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

- Sobre o CERT.br
- CSIRTs
- Estatísticas
  - Incidentes
  - Spam
- Cursos
- Projetos
- Publicações
- Palestras
- Links
- FAQ
- Mapa do site
- Contato
- RSS

Busca

ok

Núcleo de Informação e Coordenação do Ponto BR

English

CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTRO.br - W3C.br

Imprensa

Você está em: CERT.br > Estatísticas > Incidentes > Janeiro a Dezembro de 2017 - Análise

Início

## Incidentes Reportados ao CERT.br -- janeiro a dezembro de 2017

## Análise de alguns fatos de interesse observados neste período

O total de notificações recebidas em 2017 foi de 833.775, número 29% maior que o total de 2016.

Segue uma breve análise de alguns fatos de interesse observados neste período, agrupados por categorias de incidentes:

**Ataques de Negação de Serviço**

- No ano de 2017 recebemos 220.188 notificações sobre computadores que participaram de ataques de negação de serviço (DoS). Este número foi quase 4 vezes maior que o número de notificações recebidas em 2016;
- A maioria das notificações de ataques de DoS foi recebida em julho de 2017, referente a um ataque originado por equipamentos de IoT (Internet das Coisas) infectados e fazendo parte de botnets.

**Tentativas de Fraude**

- As notificações de tentativas de fraude totalizaram 59.319 incidentes em 2017, correspondendo a uma queda de 42% em relação a 2016;
- Em 2017, as notificações de casos de páginas falsas de bancos e sites de comércio eletrônico (*phishing* clássico) caíram 46% em relação a 2016;
- As notificações sobre Cavalos de Troia, utilizados para furtar informações e credenciais, tiveram uma queda de 7% em relação ao ano de 2016;
- Em 2017, o número de notificações de casos de páginas falsas que não envolvem bancos e sites de comércio eletrônico teve um aumento de 6% em relação a 2016. Nesses casos estão incluídos os serviços de *webmail* e redes sociais, por exemplo.

## O que veremos nesta apresentação:

- Entendendo DoS e DDoS;
- Quais os tipos de ataque DDoS ;
- Estatísticas das vulnerabilidades;
- Soluções e mecanismos para evitar e/ou mitigar ataques;
- Benefícios da implementação de boas práticas.

# 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

Convergência Digital

Convergência Digital | Carreira | Cloud Computing | Internet Móvel 3G 4G | CDTV

Quem somos | Anuncie | Fale conosco | Newsletter

Gestão | Governo | Inclusão Digital | Inovação | Internet

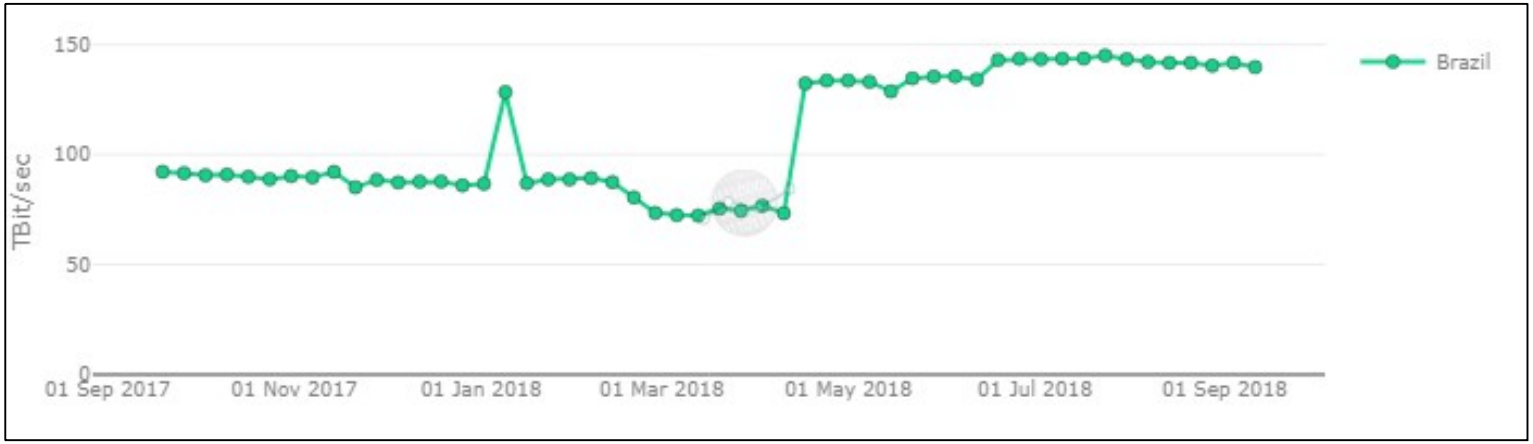
SEGURANÇA

## Brasil foi alvo do maior ataque DDoS do mundo

Convergência Digital* ... 19/02/2018 ... Convergência Digital

O 13º Relatório Anual sobre Segurança da Infraestrutura Global de Redes (WISR - Worldwide Infrastructure Security Report) da NETSCOUT Arbor registrou no ano de 2017 um total de 264.900 ataques DDoS – Distributed Denial of Service – dirigidos ao Brasil, o que corresponde a 728 ataques por dia/30 por hora. Em escala global, houve 7,5 milhões de ataques DDoS em 2017. Entre os ataques dirigidos ao Brasil, a maioria – 34,09% – tem origem no próprio país. Em seguida, as principais fontes de ataque ao Brasil são Estados Unidos – 30,30%; Canadá – 17,80%; e Reino Unido – 17,80%.

http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=47296&sid=18



# Ranking de potencial DDoS

| Country | Open Recursive DNS | Open NTP | Open SNMP | Open SSDP | Open CHARGEN | DDOS Potential TBit/sec | DDOS Rank |
|---|---|---|---|---|---|---|---|
| United States | 2,067,384 | 1,965,745 | 409,086 | 130,840 | 6,455 | 1,188 | 1 |
| China | 2,031,792 | 1,694,503 | 152,883 | 129,936 | 2,512 | 1,033 | 2 |
| Italy | 229,295 | 769,505 | 136,312 | 47,151 | 6,538 | 443 | 3 |
| Russian Federation | 329,190 | 525,279 | 103,142 | 248,762 | 1,171 | 315 | 4 |
| South Korea | 210,552 | 352,973 | 388,736 | 116,139 | 12,083 | 216 | 5 |
| Germany | 215,440 | 351,103 | 24,271 | 7,910 | 1,057 | 205 | 6 |
| France | 267,626 | 314,330 | 50,646 | 4,624 | 473 | 187 | 7 |
| Brazil | 220,384 | 231,867 | 587,689 | 51,081 | 780 | 144 | 8 |
| United Kingdom | 202,428 | 214,937 | 41,242 | 3,717 | 455 | 129 | 9 |
| Switzerland | 22,772 | 227,454 | 18,526 | 1,739 | 104 | 128 | 10 |

# 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).

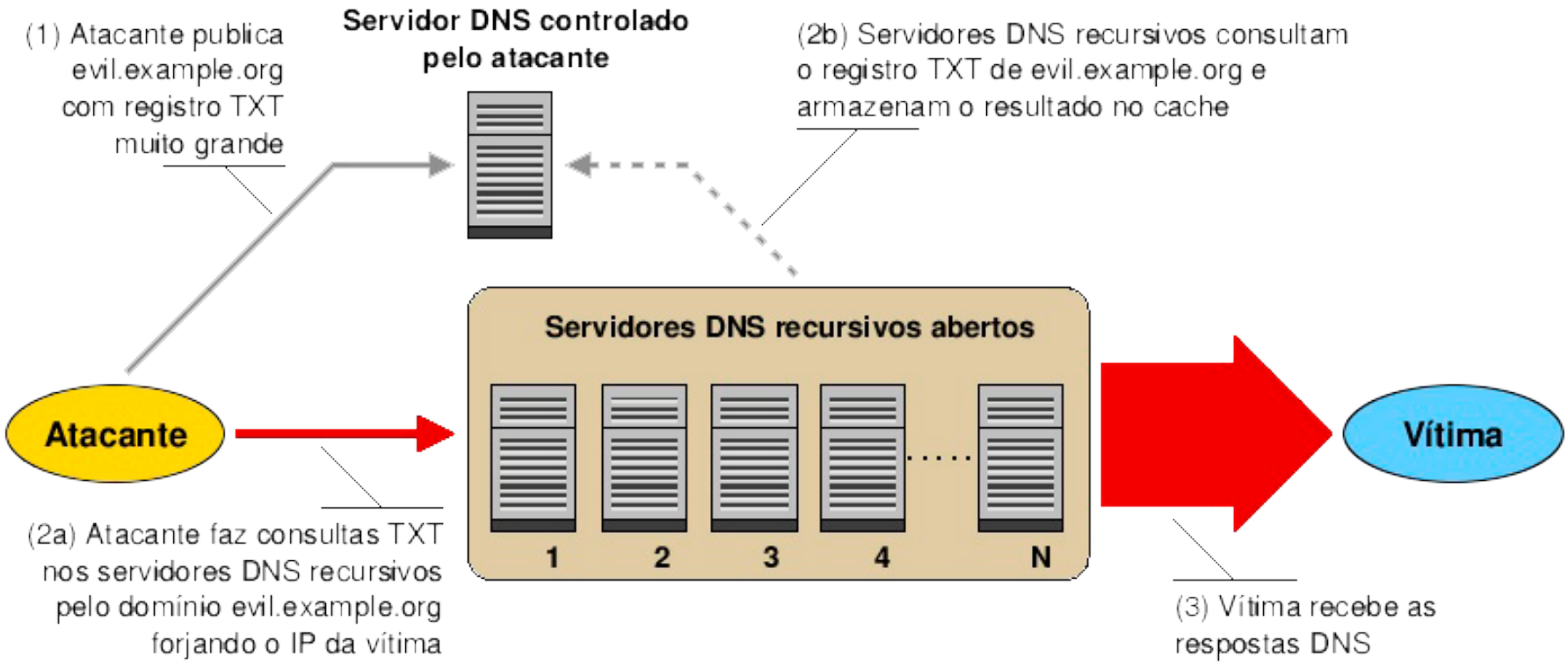
- Em firewalls e IPSs: tentam consumir a capacidade da tabela de estado de conexões, impedindo que novas conexões sejam estabelecidas.

# Ataque Volumétrico

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

- Exemplo: DRDoS (Distributed Reflective Denial of Service)

# Ataque Volumétrico

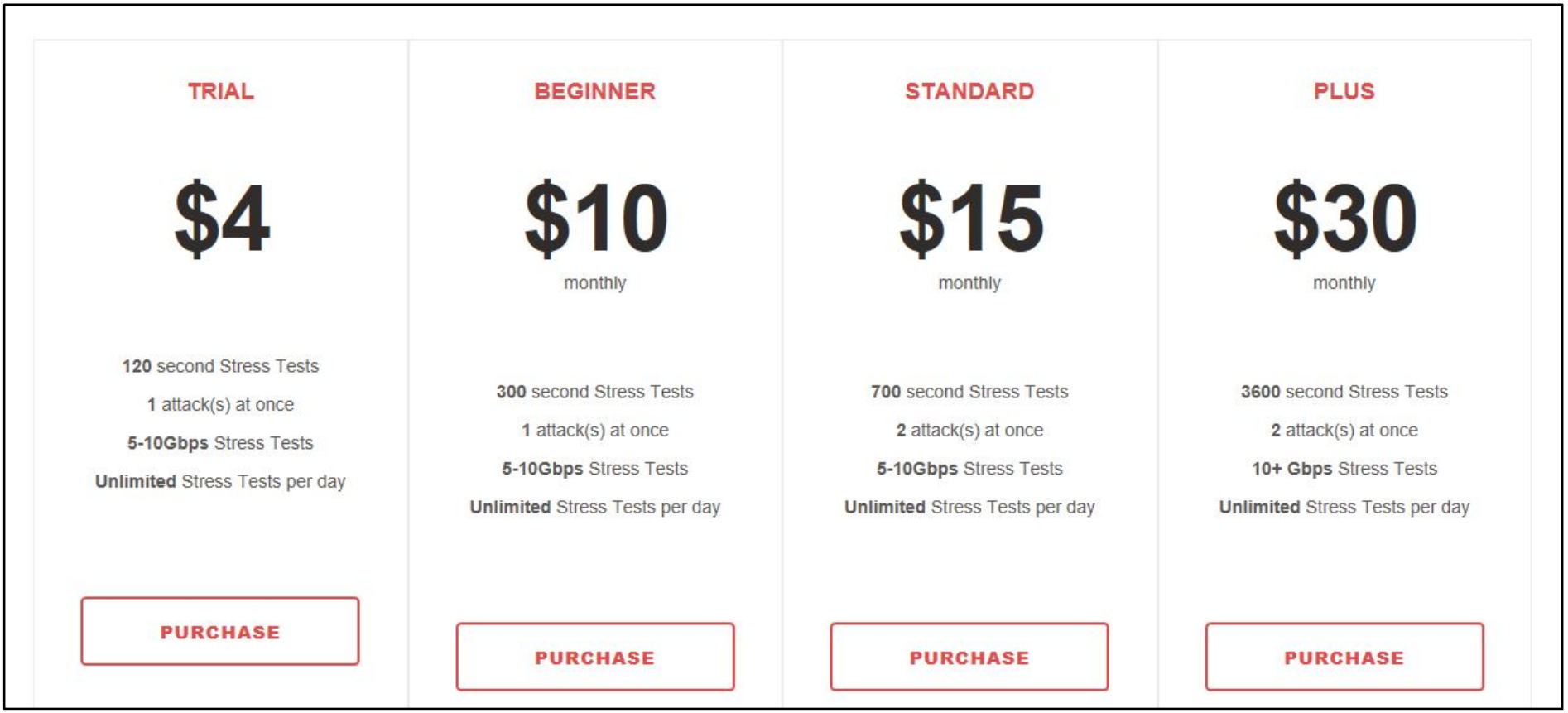


# Soluções e mecanismos para evitar e/ou mitigar ataques

# Relatório de Vulnerabilidade:

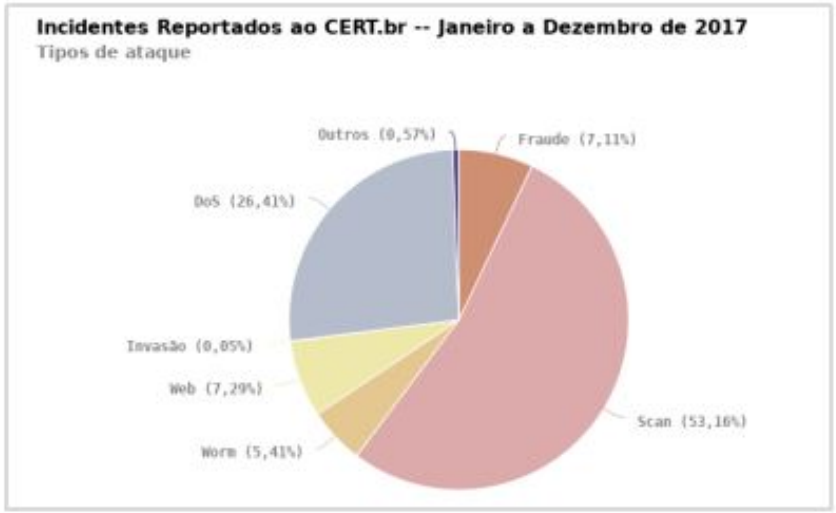
Os cyber ataques tornaram-se fonte de renda de muitos criminosos, conforme vemos na imagem abaixo, ataques são comercializados na rede de forma transparente e a um preço muito acessível, o que é preocupante, pois, com apenas $19,99 por mês é possível tirar algumas redes do ar por um certo tempo, os motivos para se contratar este tipo de serviço são de natureza diversa, mas geralmente estão ligados a concorrência desleal gerada por competição de mercado regional:

# Relatório de Vulnerabilidade:



| TRIAL | BEGINNER | STANDARD | PLUS |
|---|---|---|---|
| $4 | $10 monthly | $15 monthly | $30 monthly |
| **120** second Stress Tests | **300** second Stress Tests | **700** second Stress Tests | **3600** second Stress Tests |
| **1** attack(s) at once | **1** attack(s) at once | **2** attack(s) at once | **2** attack(s) at once |
| **5-10Gbps** Stress Tests | **5-10Gbps** Stress Tests | **5-10Gbps** Stress Tests | **10+ Gbps** Stress Tests |
| **Unlimited** Stress Tests per day | **Unlimited** Stress Tests per day | **Unlimited** Stress Tests per day | **Unlimited** Stress Tests per day |
| PURCHASE | PURCHASE | PURCHASE | PURCHASE |

# Relatório de Vulnerabilidade:




***Sua entidade está contribuindo com este problema?!***

Após a análise nas ferramentas, notamos que a entidade está em desacordo com algumas padronizações de segurança, dentre elas:

1. **RFC 1786;**
2. **RFC 5735;**
3. **RFC 2827;**
4. **Necessário realizar validação da RFC 4272.**

# Relatório de Vulnerabilidade:

***Vulnerabilidades encontradas***


***A classificação de segurança obtida foi a seguinte:***

**Security Issues**

# 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:

- SYN filtering

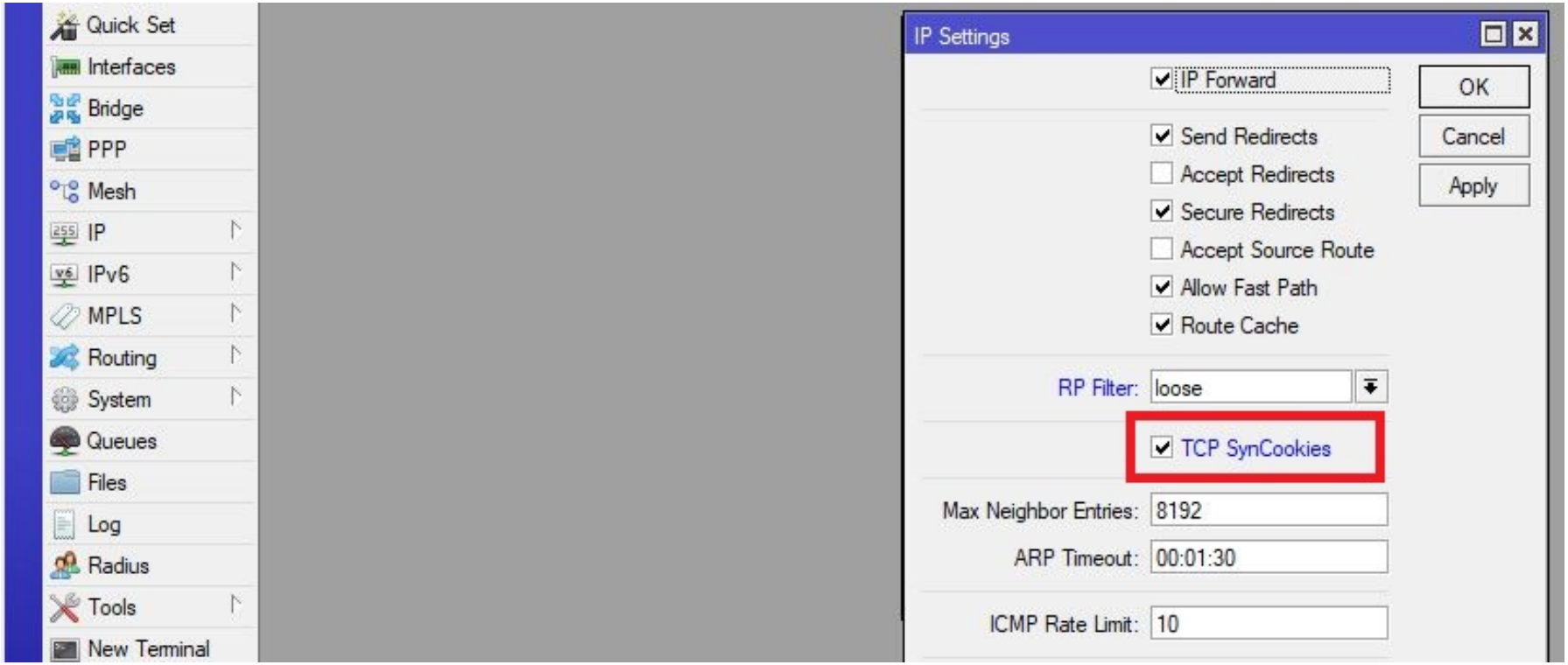
Some advanced filtering can by applied to tcp packet state.

```
/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

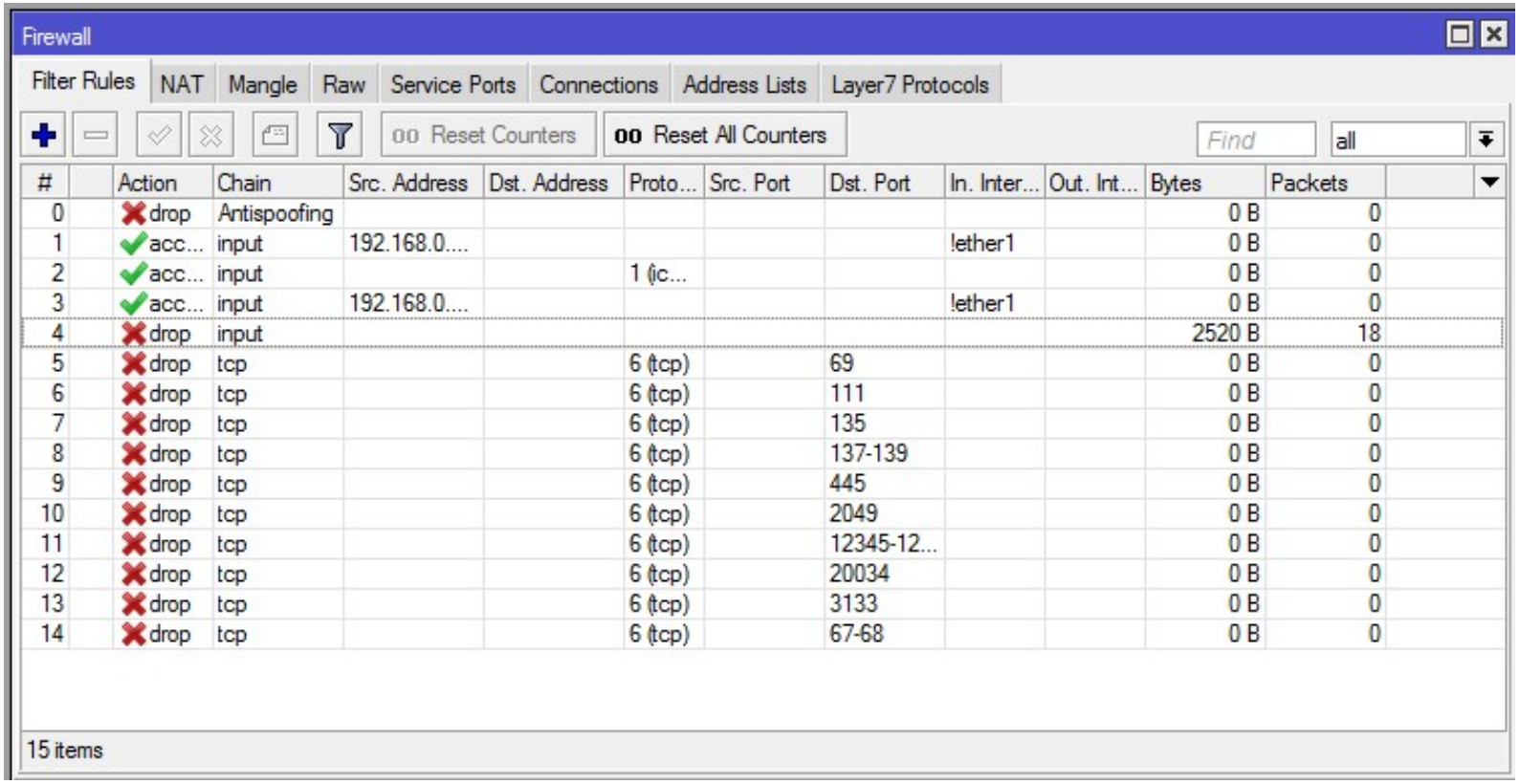
# Filtragem SYN:



# 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.

# Anti Spoofing

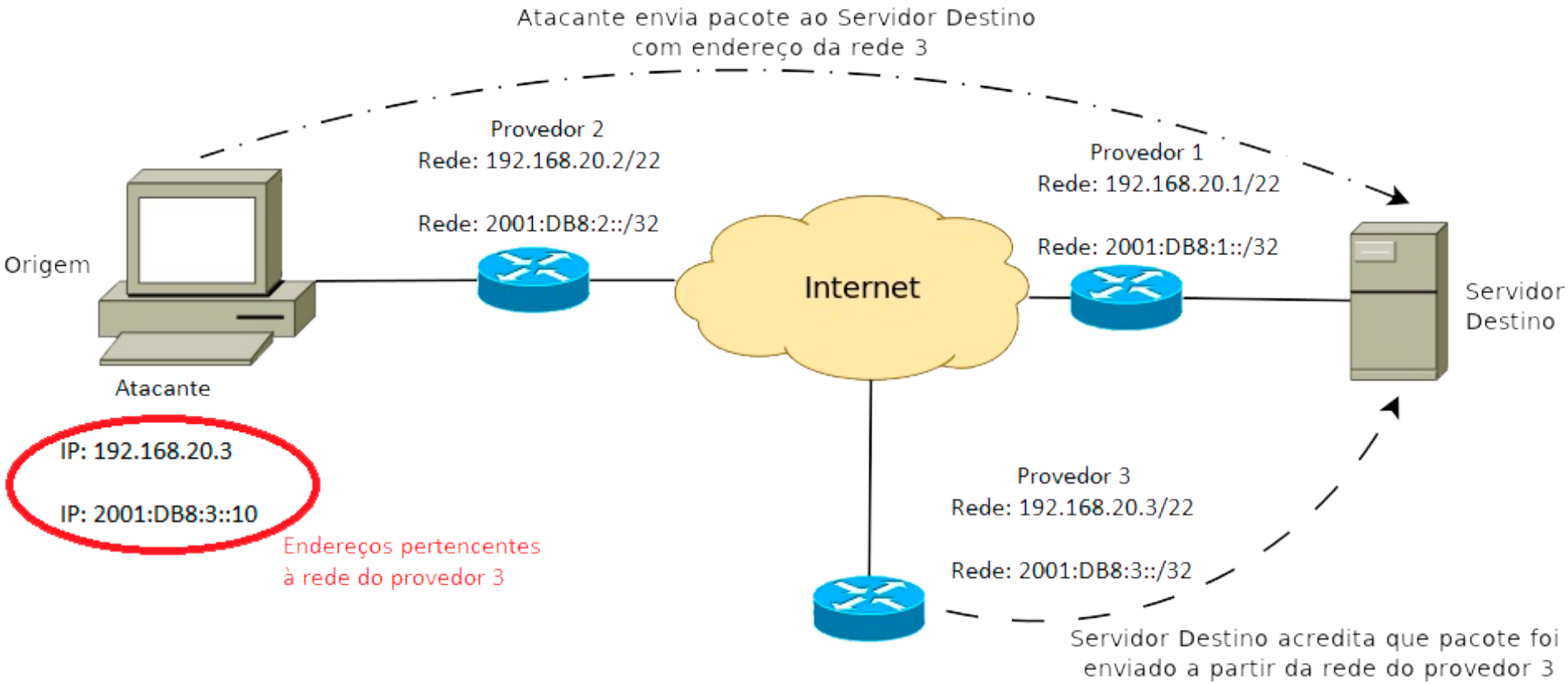
- Spoofing basicamente são pacotes com origens inválidas e muitas vezes é utilizado para ataques de negação de serviço. Apenas um filtro aplicado no próprio provedor de acesso, preferencialmente na interface do roteador conectada diretamente ao usuário, é eficaz.

# Anti Spoofing

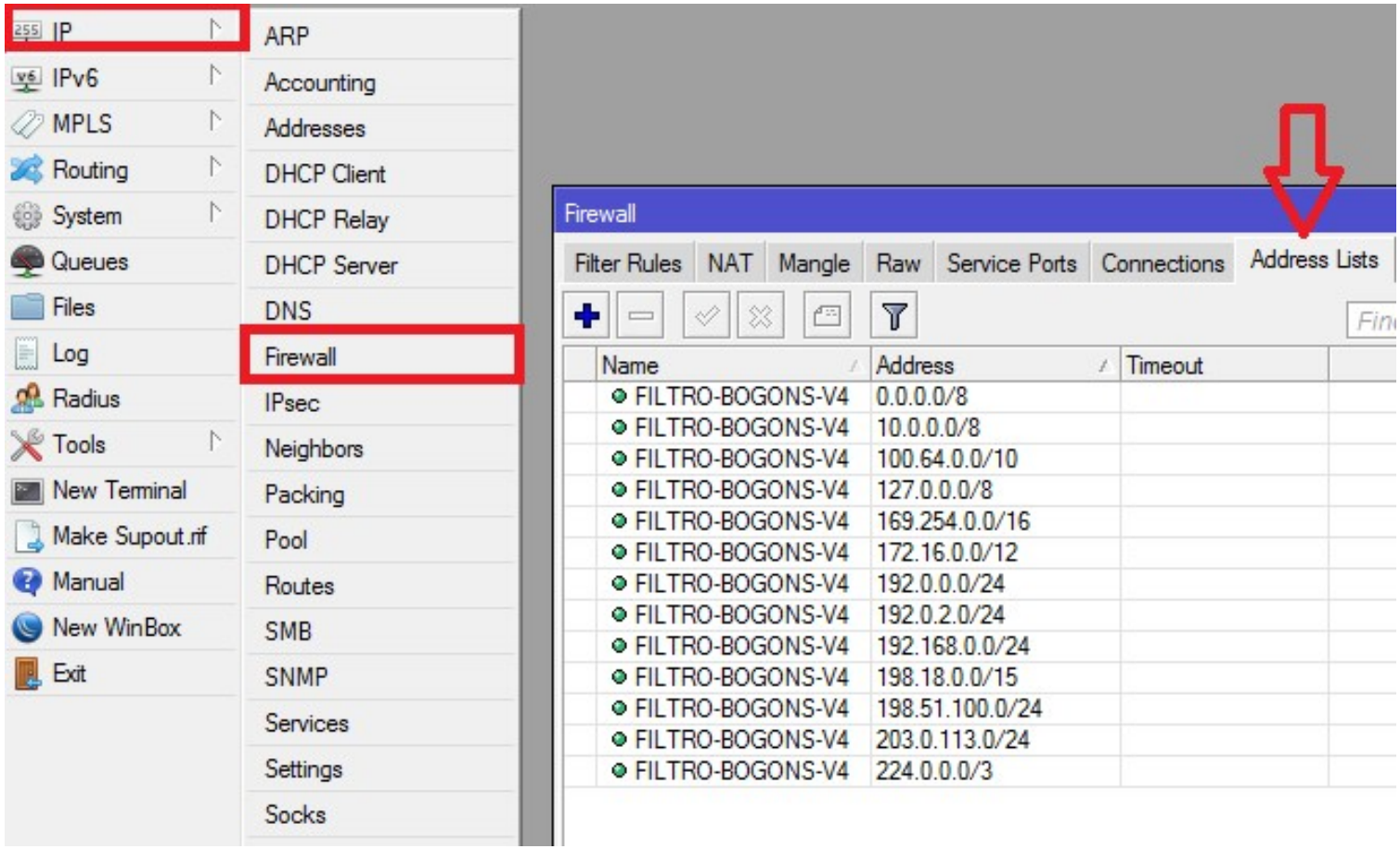
- Se os equipamentos na rede onde os pacotes se originam não verificam sua origem, qualquer ação posterior para identificá-los ou bloquea-los é muito dificultada.

- 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.

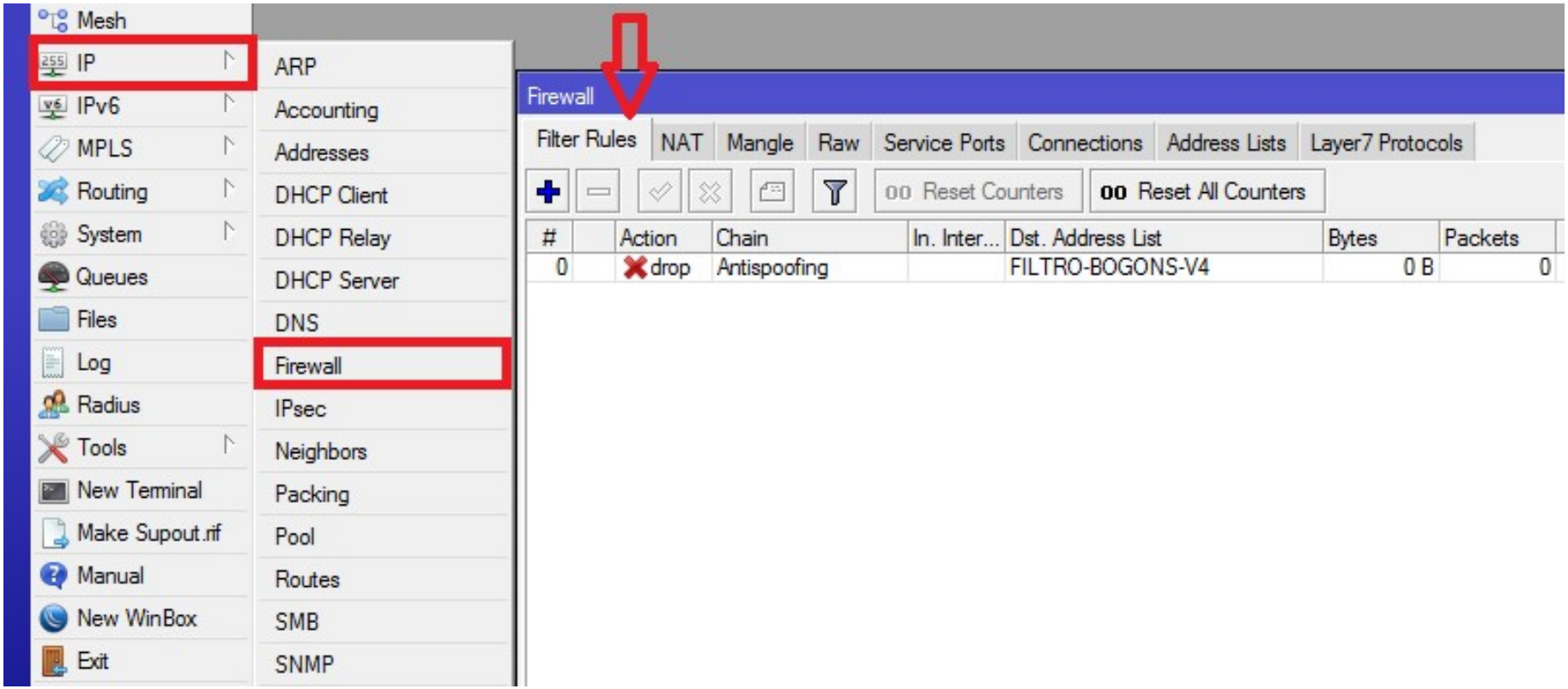
# Anti Spoofing



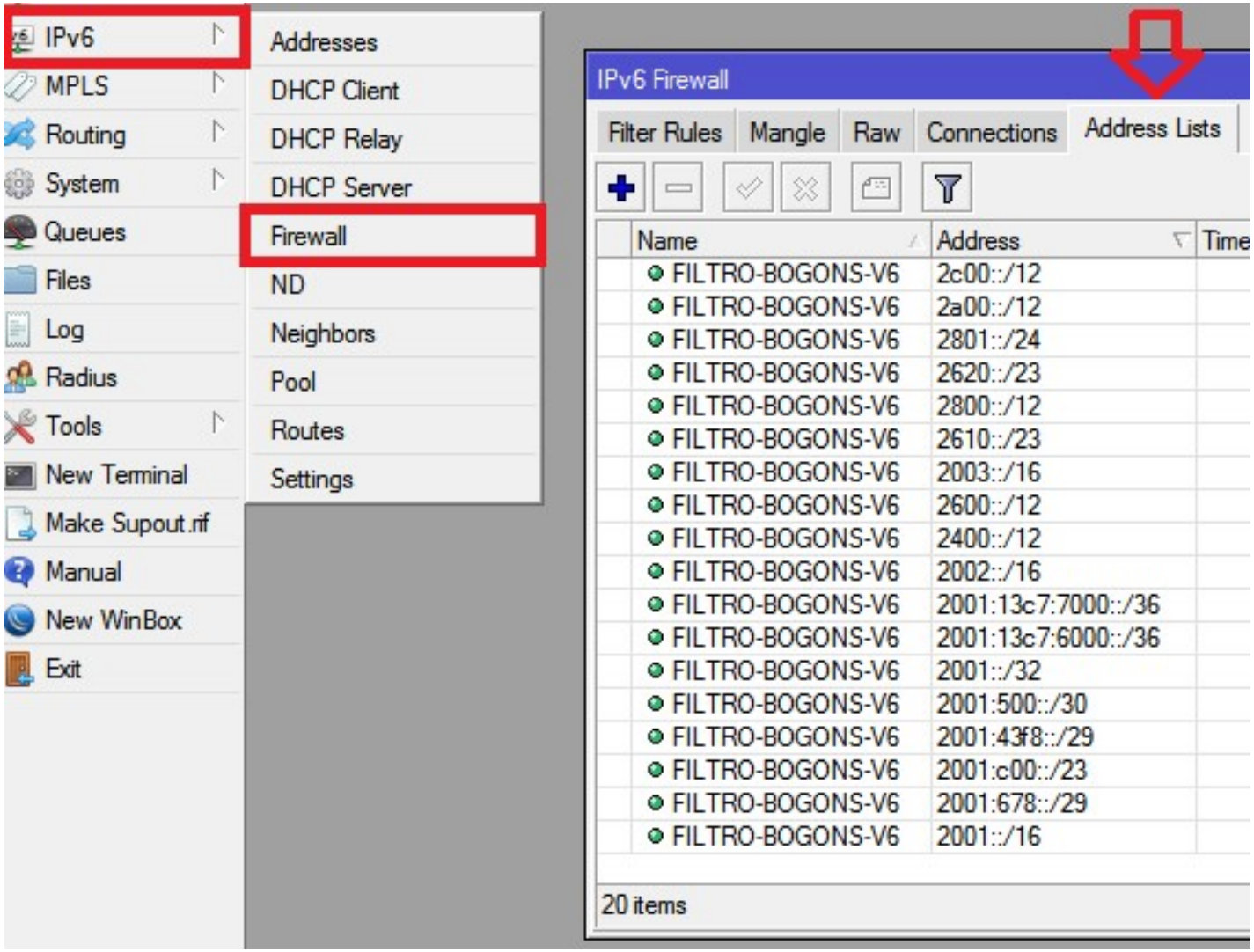
# Configuração de Anti Spoofing IPv4 no RouterOS:



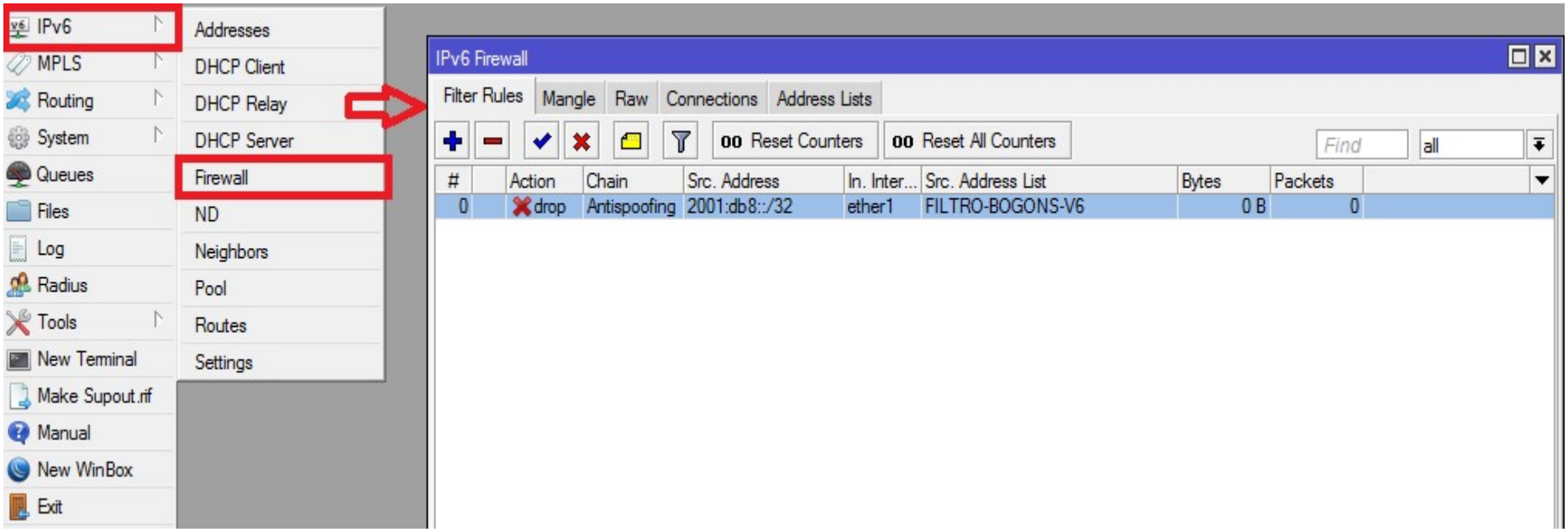
# Configuração de Anti Spoofing IPv4 no RouterOS:



# Configuração de Anti Spoofing IPv6 no RouterOS:



# Configuração de Anti Spoofing IPv6 no RouterOS:



# Normas de Acordo Mútuo para Segurança de Roteamento

MANRS

Mutually Agreed Norms for Routing Security

Objetivos

1. Aumentar a conscientização e incentivar ações, pela demonstração do compromisso crescente do grupo de apoiadores.

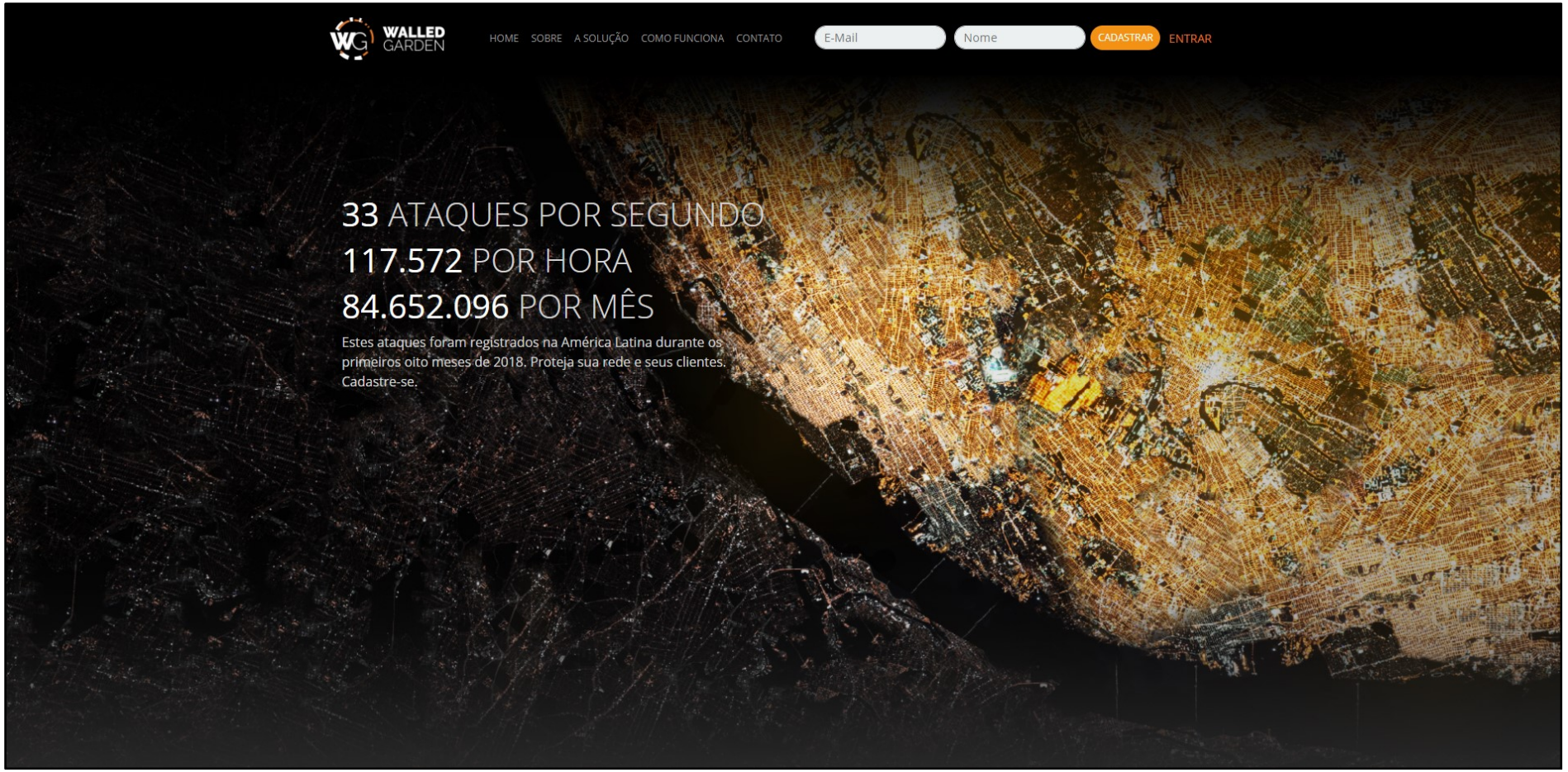
2. Promover a cultura de responsabilidade coletiva para a resiliência e segurança do sistema de roteamento global da Internet.

3. Demonstrar a capacidade do setor para abordar questões de resiliência e segurança do sistema de roteamento global da Internet com o espírito da responsabilidade coletiva.

4. Fornecer uma estrutura para que os provedores de acesso à Internet (ISPs) compreendam melhor e ajudem a solucionar problemas relacionados à resiliência e à segurança do sistema de roteamento global da Internet.

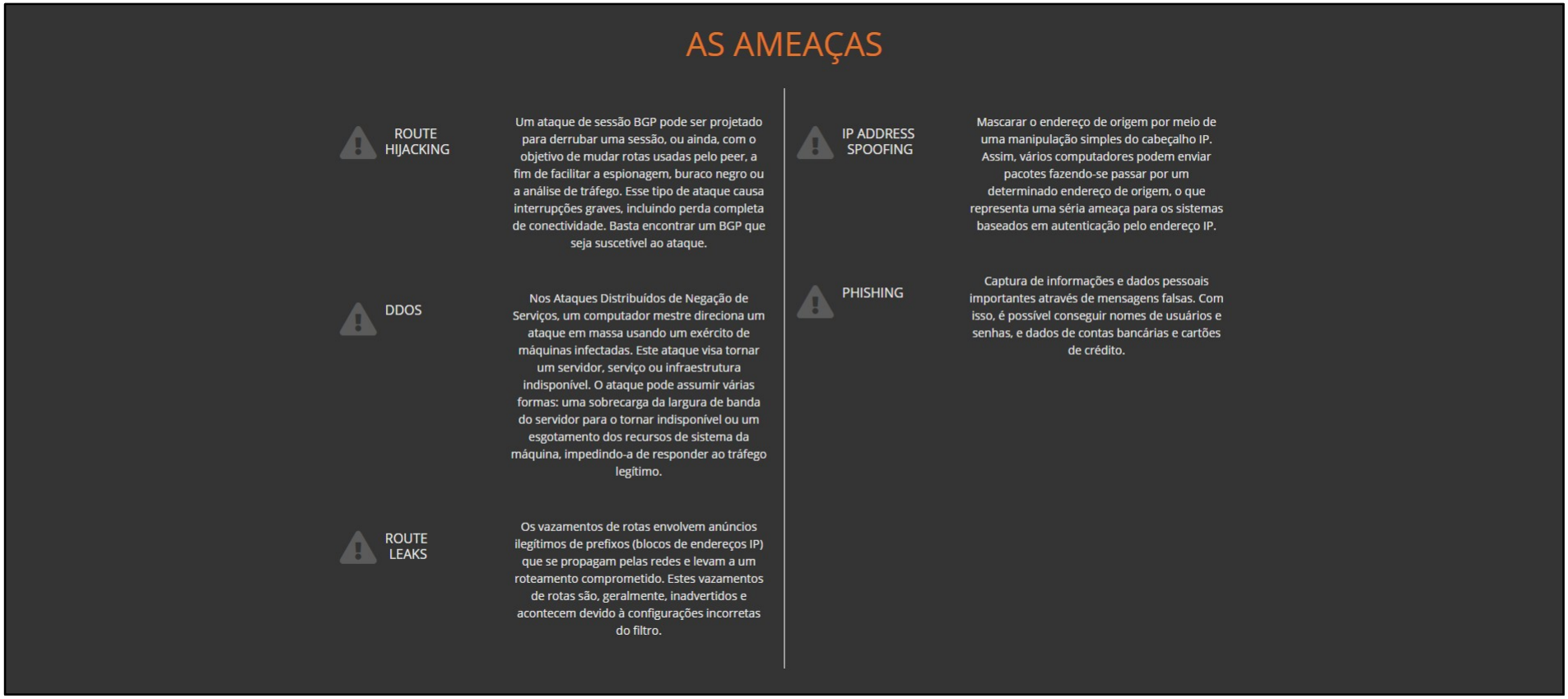
https://www.manrs.org/isps/

# WALLED GARDEN



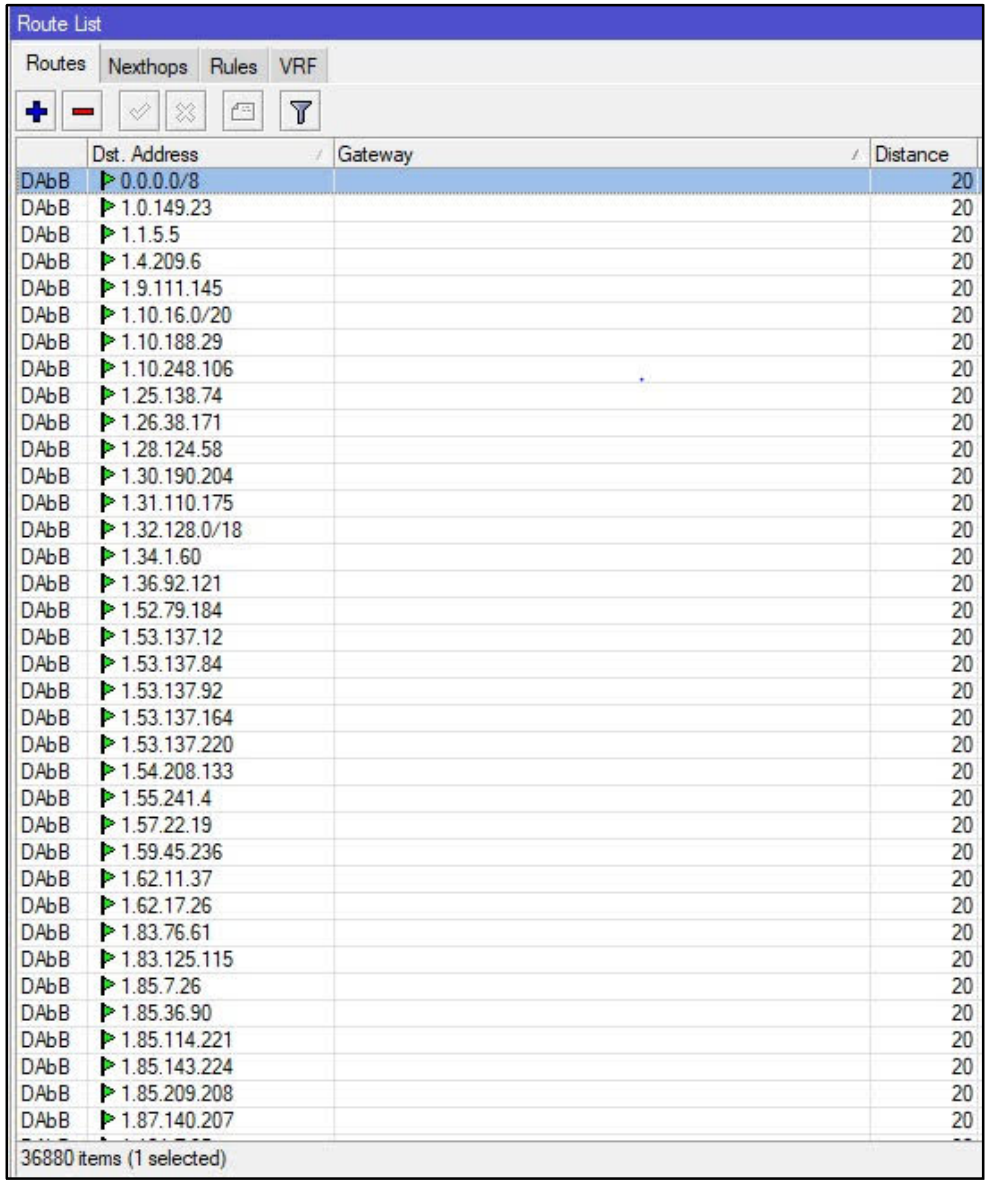
# WALLED GARDEN

# WALLED GARDEN

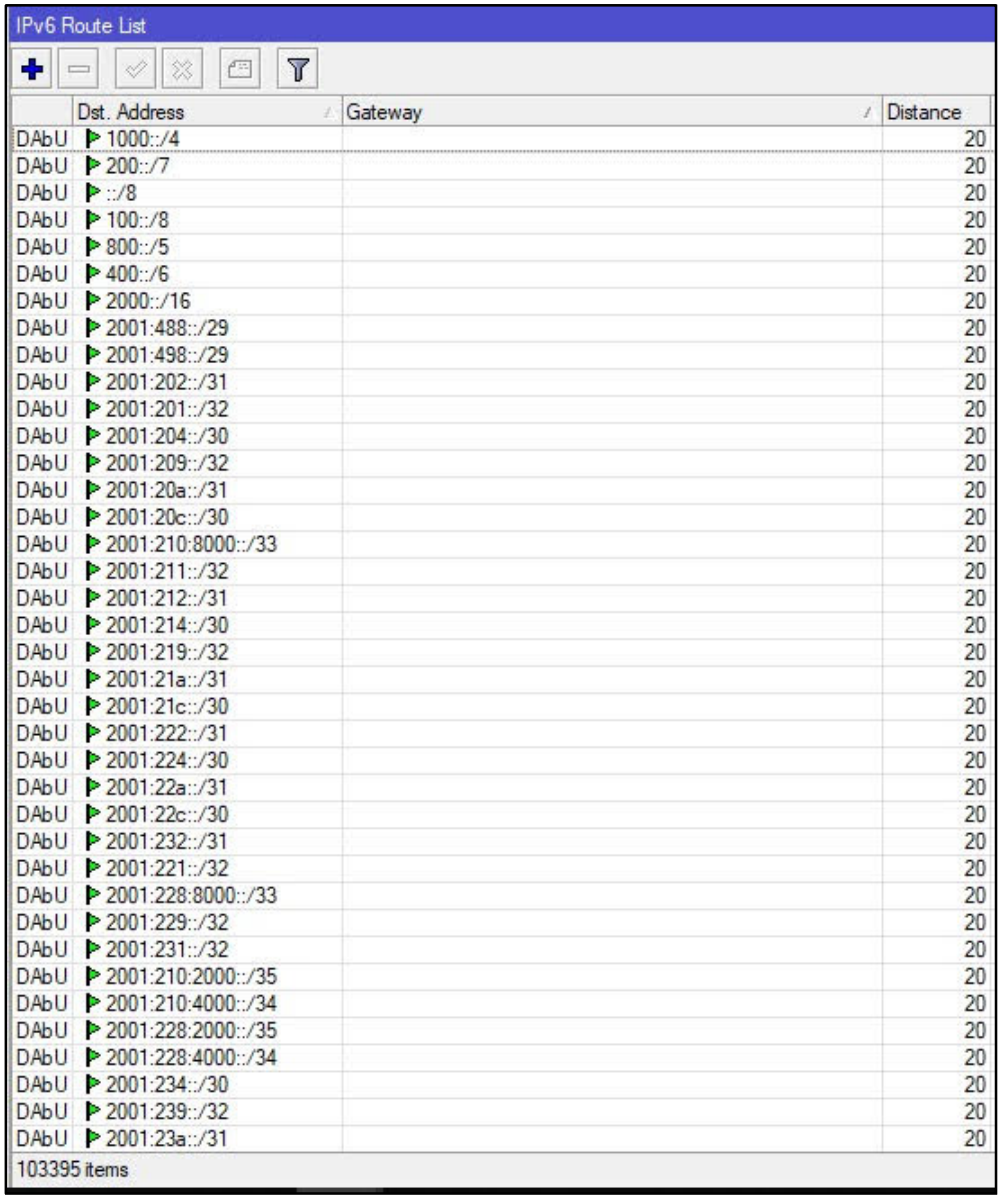



**https://walledgarden.global/**

# Exemplo do Walled Garden no RouterOS:



# Exemplo do Walled Garden no RouterOS:

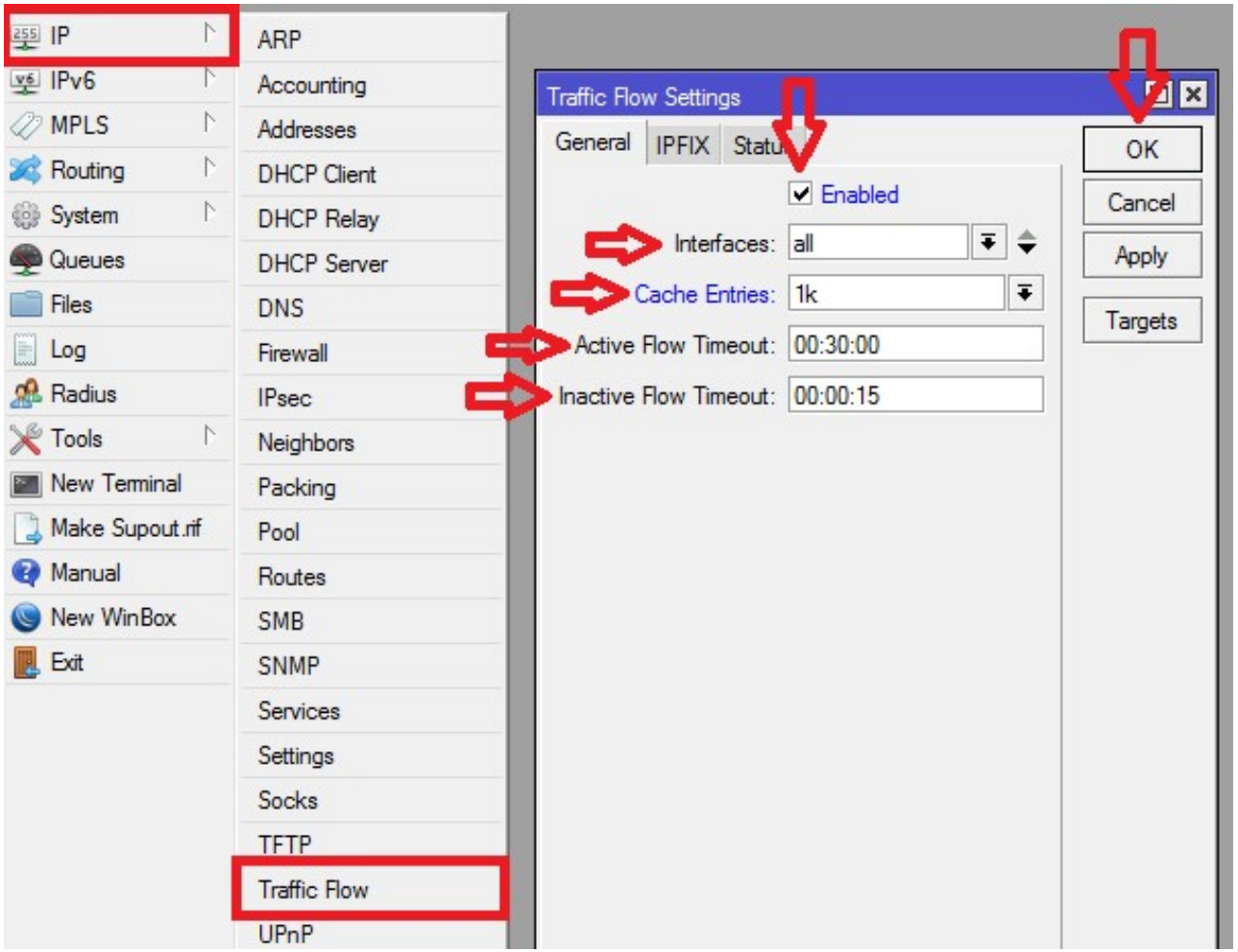


# NetFlow

- 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.

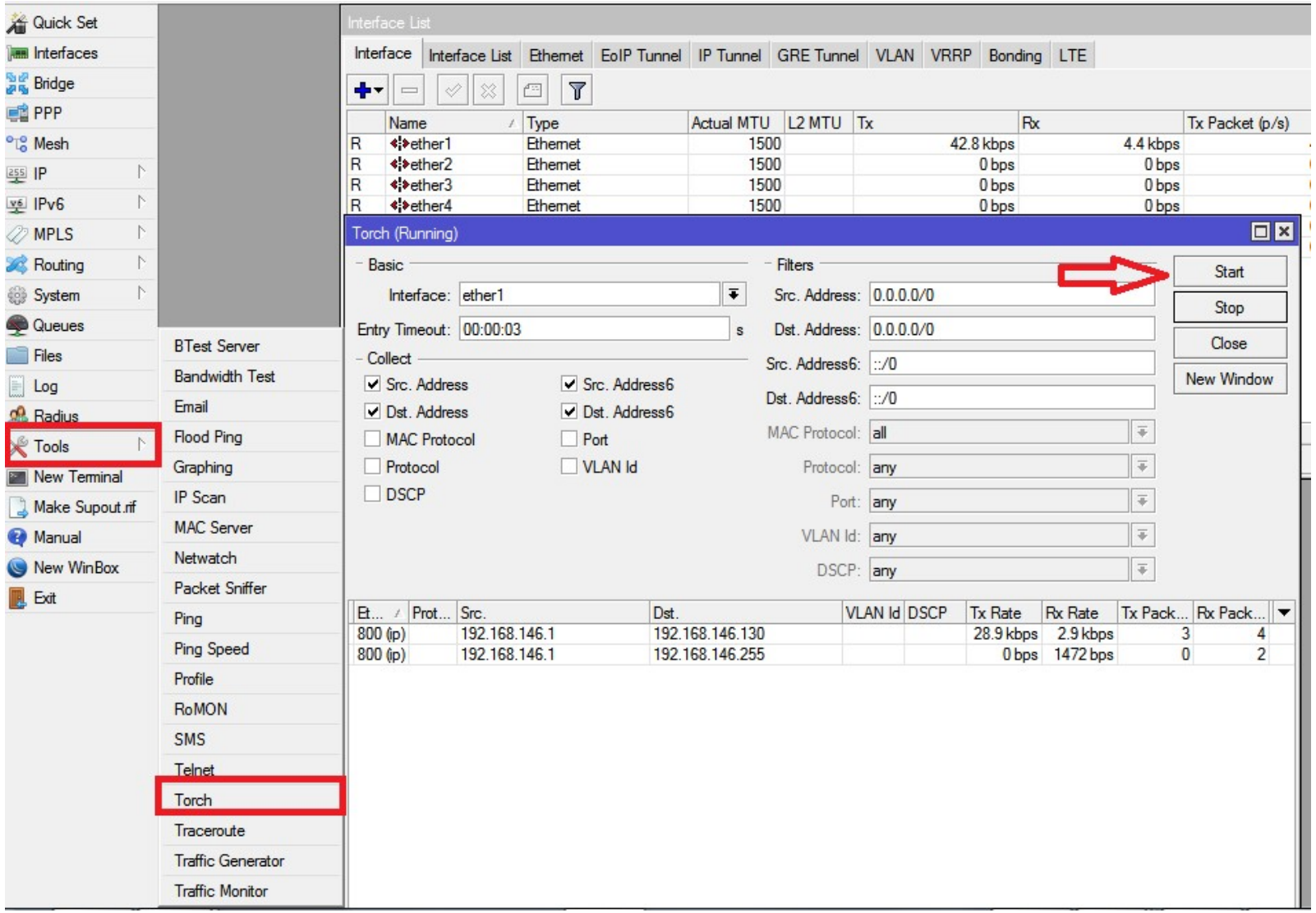
# Configuração de NetFlows no RouterOS



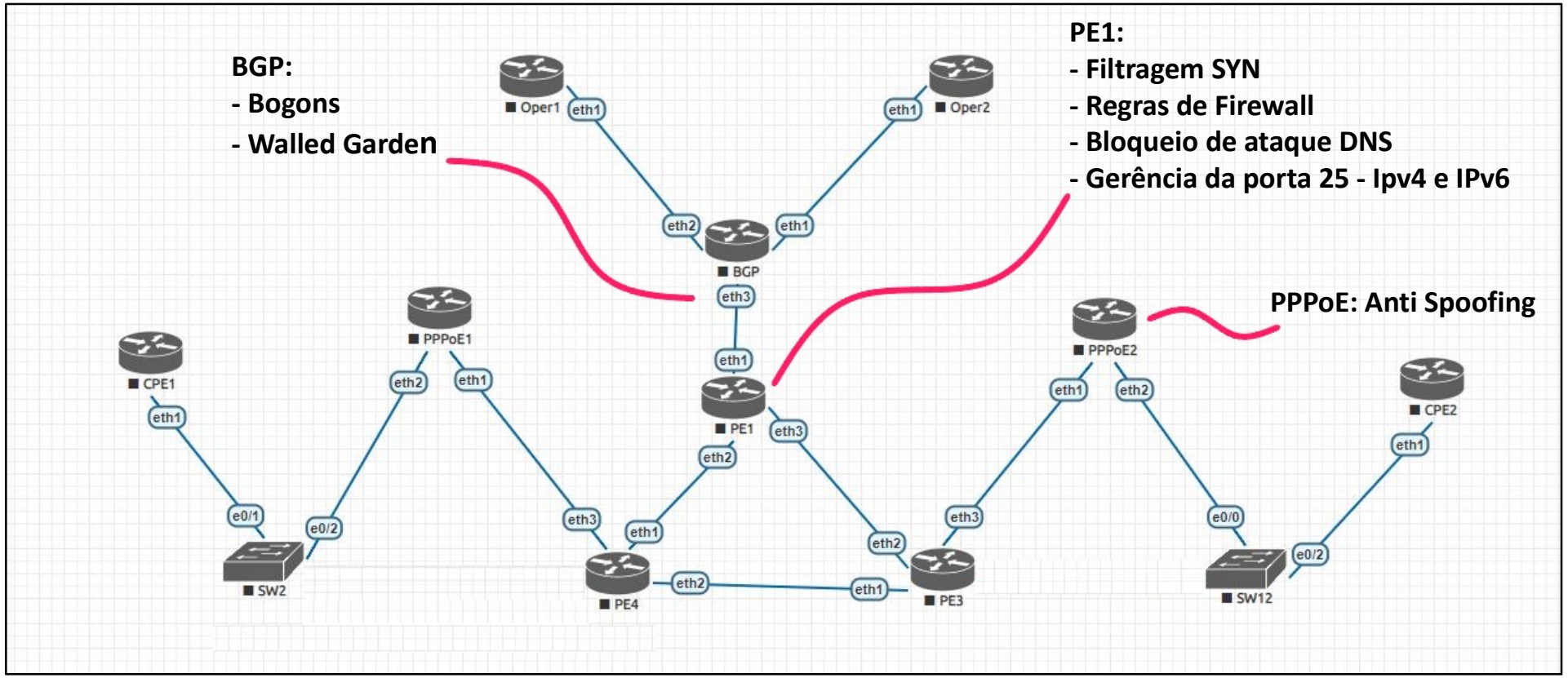
# Torch

- 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:



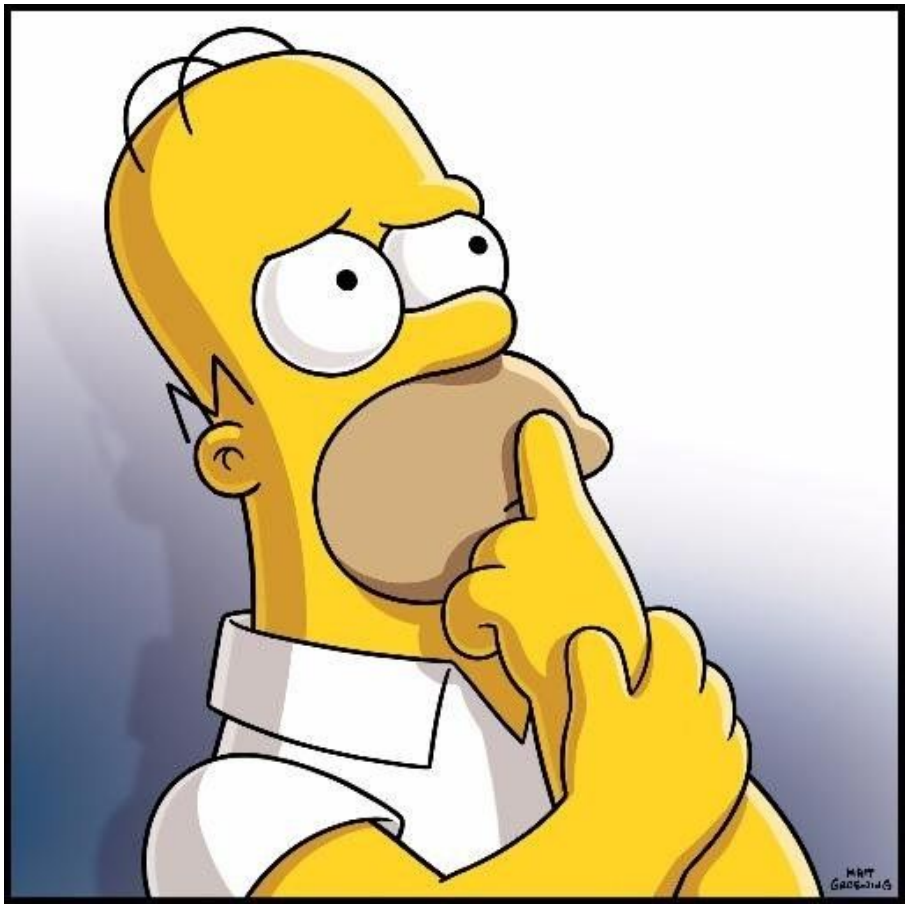
# Onde os filtros são implantados



# Benefícios da implementação das boas práticas de segurança:

- 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;
- Consistencia e confiabilidade das informações trafegadas pela rede;
- Estabilidade na rede.

# Dúvidas?



# OBRIGADA!!


- **Tayla Guimarães Oliveira**

**tayla.oliveira@solintel.com.br**

**solintel.engenharia8**

**+55 (43) 99101-4142; +55 (43) 3373-9356**

**https://www.linkedin.com/in/tayla-guimaraes**