

Boas práticas de segurança em redes

Tayla Guimarães



MOGA
Telecom



solintel



VLISM

#juntosomosmais

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 Olímpicos, Mario Rachid, negação de serviço, olimpíada, 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.

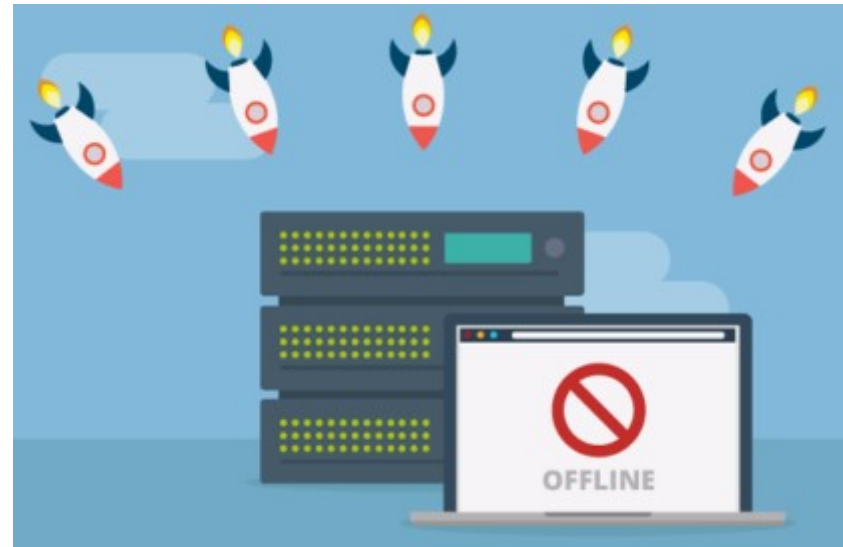
Rachid diz que os hackers já vinham se preparando para



<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 difíceis 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.

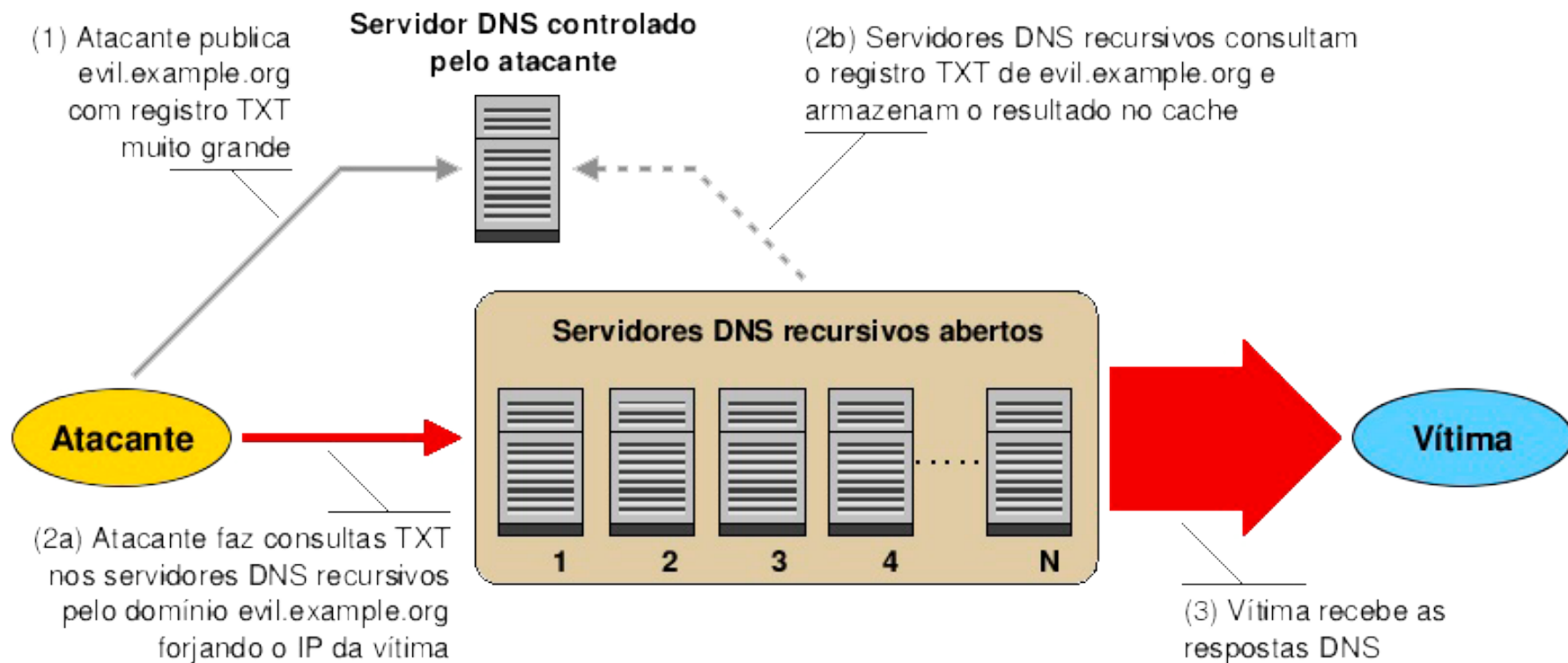
Ataque de exaustão de hardware

- 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

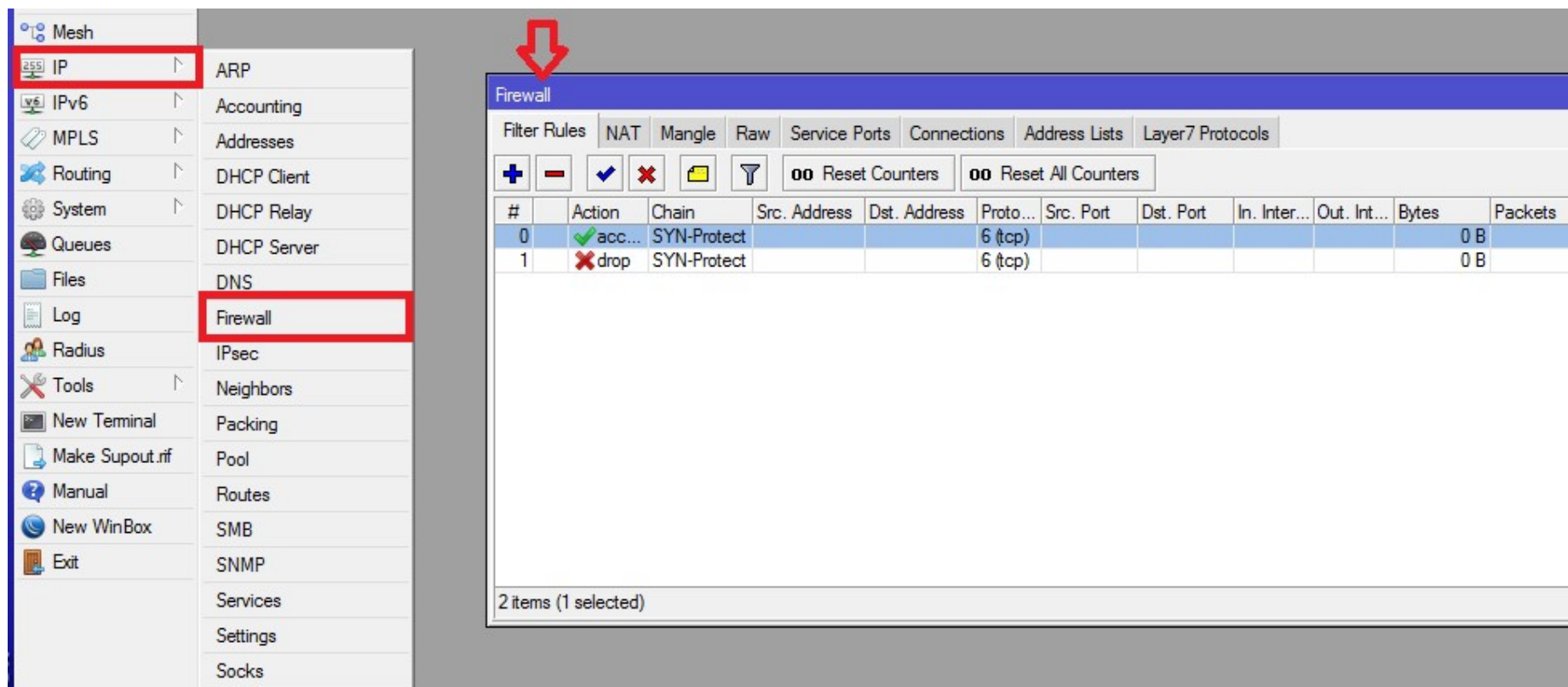


Filtragem SYN (DoS)

- 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:



The screenshot shows the Mikrotik WinBox interface for configuring Firewall Filter Rules. The left sidebar has the 'IP' menu expanded, and 'Firewall' is selected. The main window shows the 'Filter Rules' tab. A red arrow points to the 'Filter Rules' tab. The table below shows the configuration of two rules.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✓ acc...	SYN-Protect			6 (tcp)					0 B	0
1	✗ drop	SYN-Protect			6 (tcp)					0 B	0

2 items (1 selected)

Filtragem SYN:

- SYN filtering

Some advanced filtering can be 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:

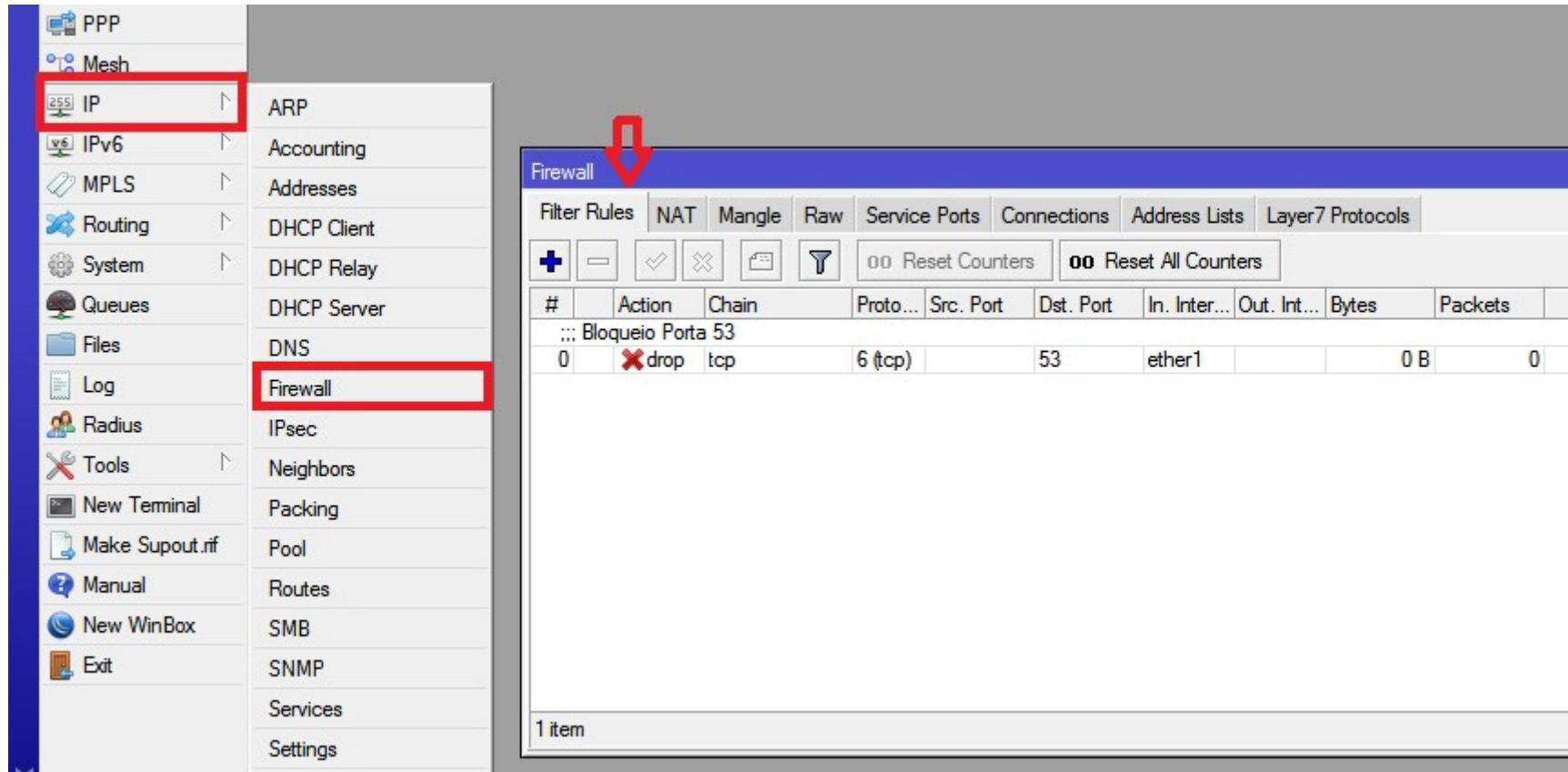
Firewall											
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols											
+ - ✓ ✗ 📄 🔍 00 Reset Counters 00 Reset All Counters Find all ▼											
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✗ drop	Antispoofing								0 B	0
1	✓ acc...	input	192.168.0...					ether1		0 B	0
2	✓ acc...	input			1 (c...					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
15 items											

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:



The screenshot shows the Mikrotik WinBox interface. In the left sidebar, the 'IP' menu item is highlighted with a red box, and the 'Firewall' sub-item is also highlighted with a red box. In the main window, the 'Firewall' tab is selected, and a red arrow points to the 'Filter Rules' sub-tab. A table displays a single rule:

#	Action	Chain	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✖ drop	tcp	6 (tcp)		53	ether1		0 B	0

Below the table, it indicates '1 item'.

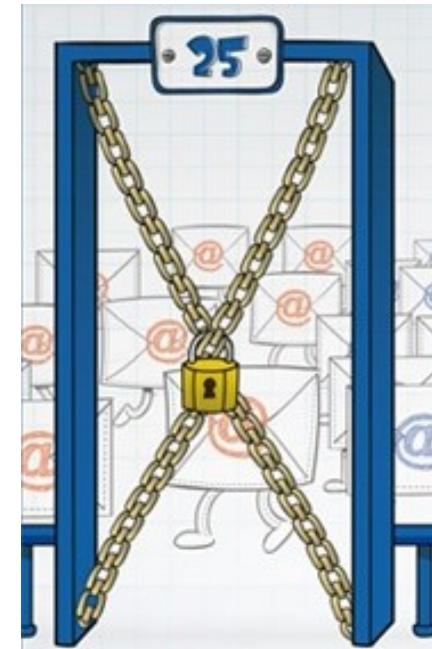
Gerência de porta 25

- 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.

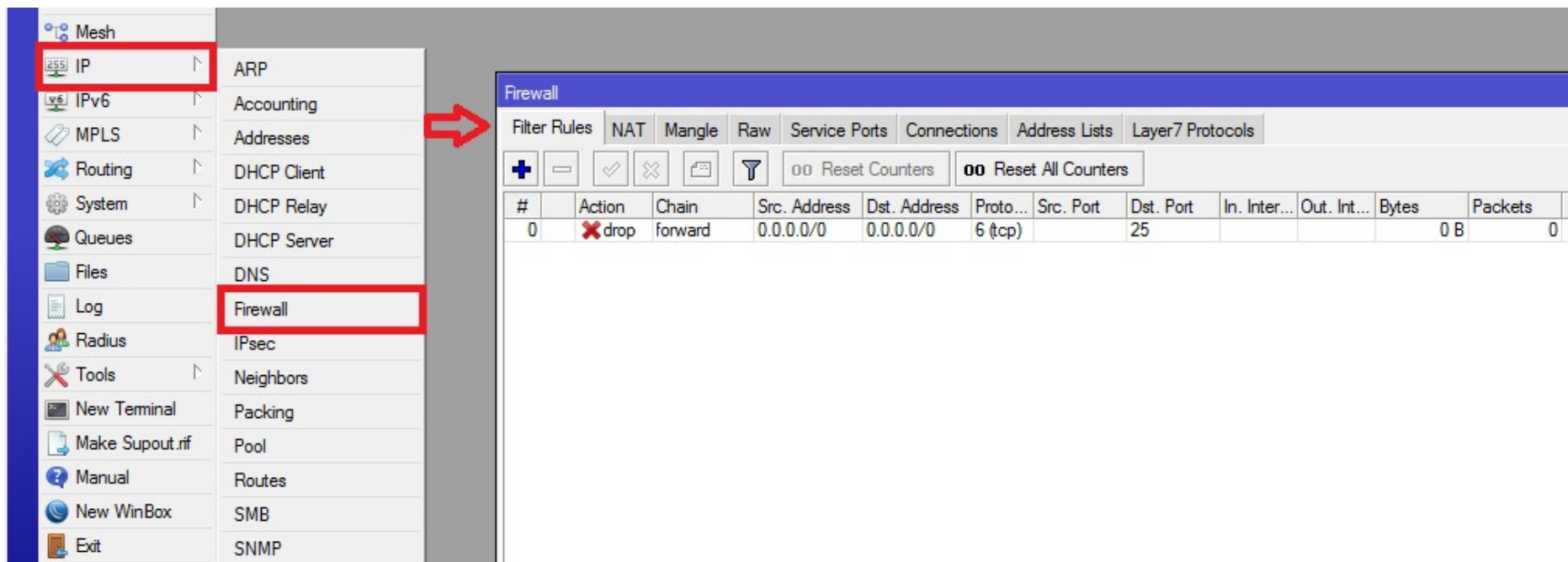


Gerência de porta 25

- 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:



The screenshot displays the Mikrotik WinBox interface for configuring a Firewall. In the left-hand menu, the 'IP' option is highlighted with a red box, and a red arrow points from it to the 'Firewall' option, which is also highlighted with a red box. The main window shows the 'Firewall' configuration page with the 'Filter Rules' tab selected. Below the tabs, there are buttons for adding (+), deleting (-), enabling/disabling (checkbox), and other actions, along with 'Reset Counters' and 'Reset All Counters' buttons. A table lists the configured filter rules:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✖ drop	forward	0.0.0.0/0	0.0.0.0/0	6 (tcp)		25			0 B	0

Gerência de porta 25 em IPv4 no RouterOS:

The image displays two Mikrotik WinBox Firewall Rule configuration windows side-by-side.

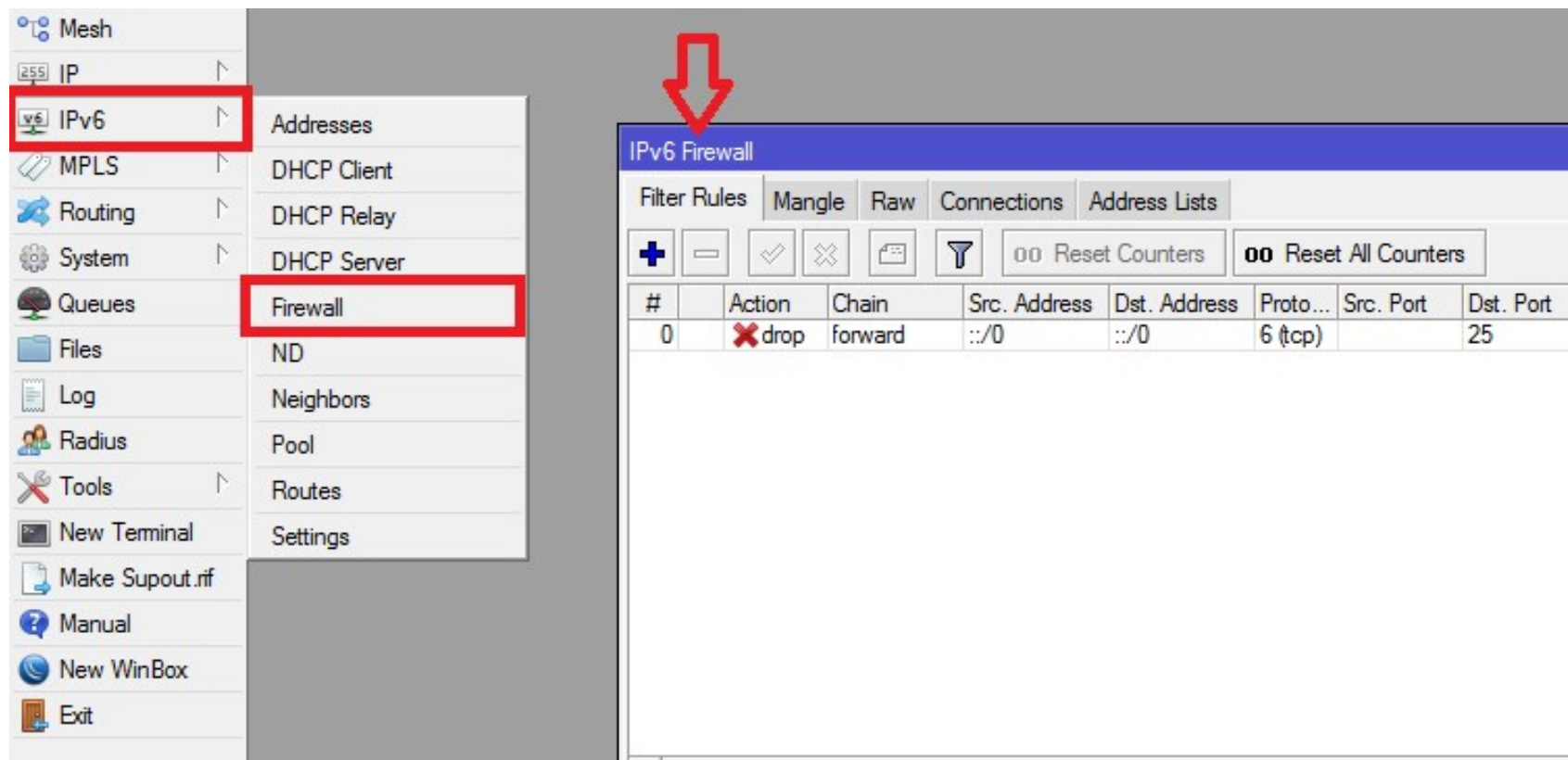
Left Window: Firewall Rule <0.0.0.0/0->0.0.0.0/0:25>

- General Tab:**
 - Chain:** forward
 - Src. Address:** 0.0.0.0/0
 - Dst. Address:** 0.0.0.0/0
 - Protocol:** 6 (tcp)
 - Dst. Port:** 25
- Action Tab:** (Not visible in this window)

Right Window: New Firewall Rule

- Action:** drop
- Log:** ☐
- Log Prefix:** (empty)

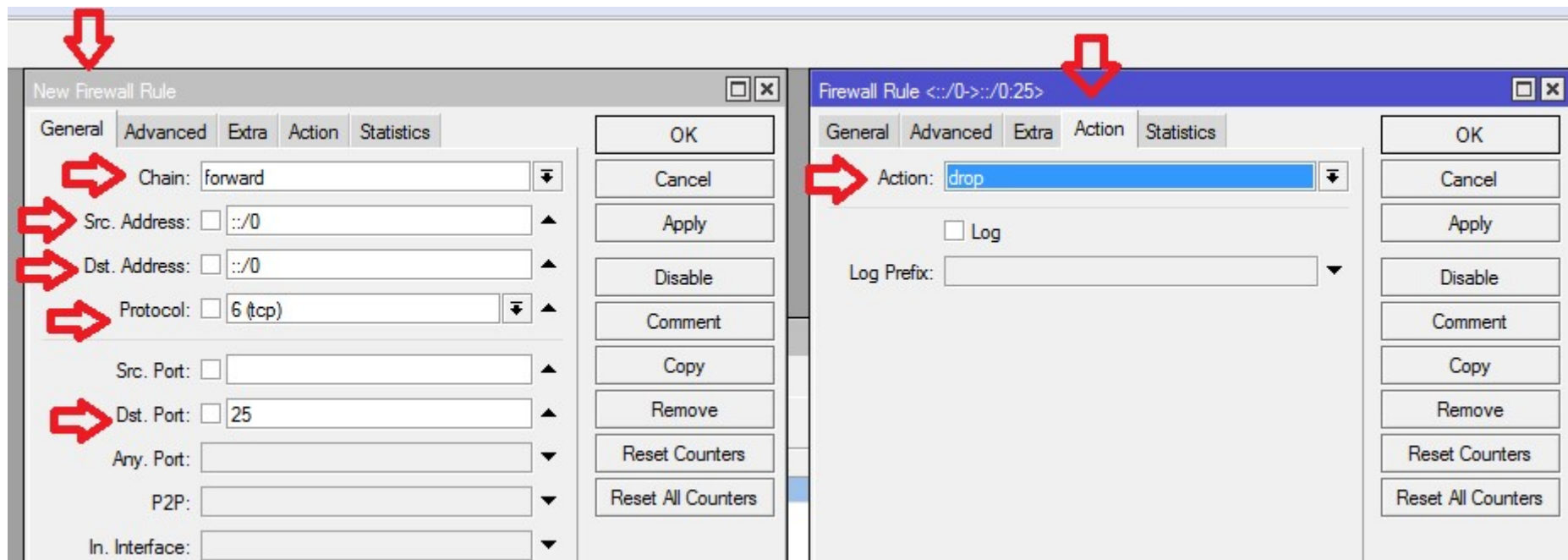
Gerência de porta 25 em IPv6 no RouterOS:



The screenshot shows the RouterOS WinBox interface. In the left sidebar, the 'IPv6' menu item is highlighted with a red box, and the 'Firewall' sub-menu item is also highlighted with a red box. A red arrow points to the 'IPv6 Firewall' tab in the main window. The main window displays the 'IPv6 Firewall' configuration page with the 'Filter Rules' tab selected. Below the tabs, there are buttons for adding (+), removing (-), enabling/disabling (checkbox), and deleting (X) rules, as well as buttons for 'Reset Counters' and 'Reset All Counters'. A table lists the configured rules:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
0	✖ drop	forward	::/0	::/0	6 (tcp)		25

Gerência de porta 25 em IPv6 no RouterOS:



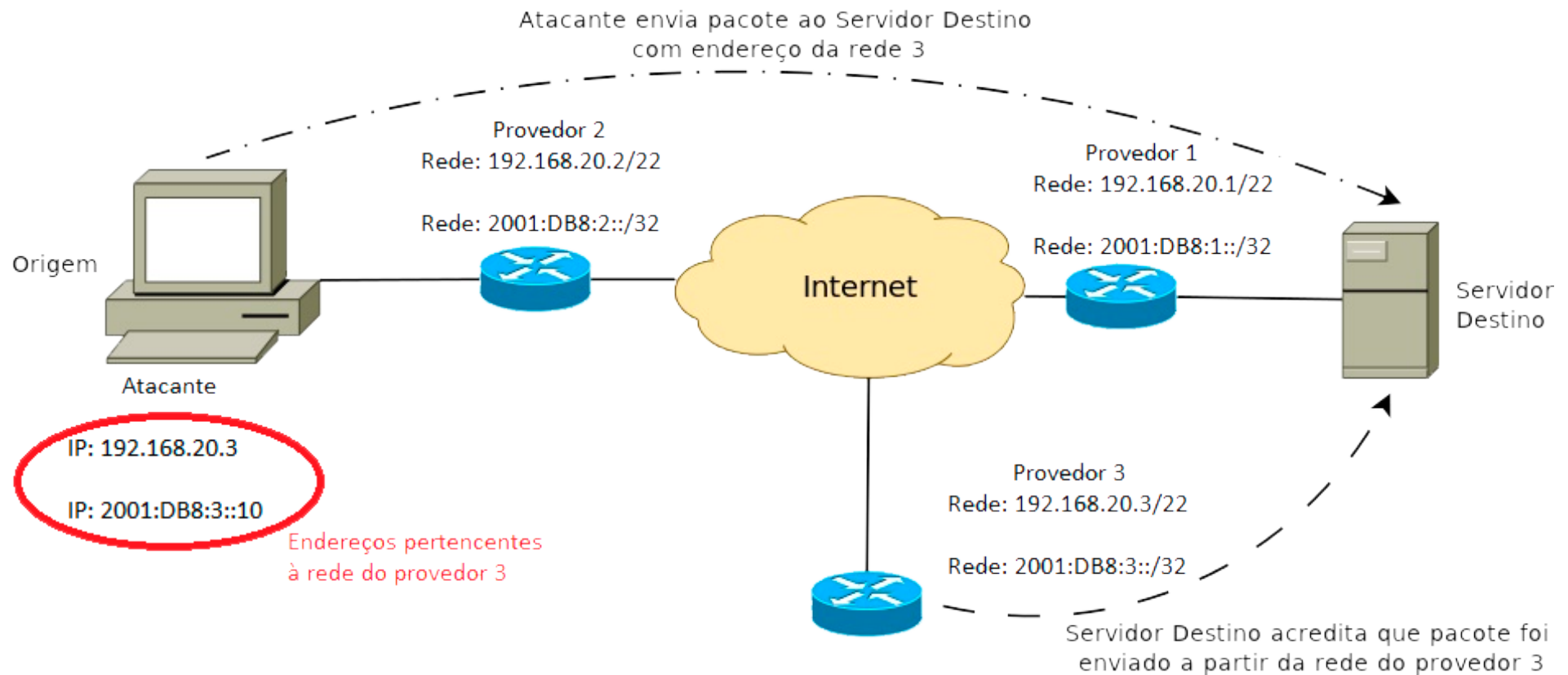
Anti Spoofing

- 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.

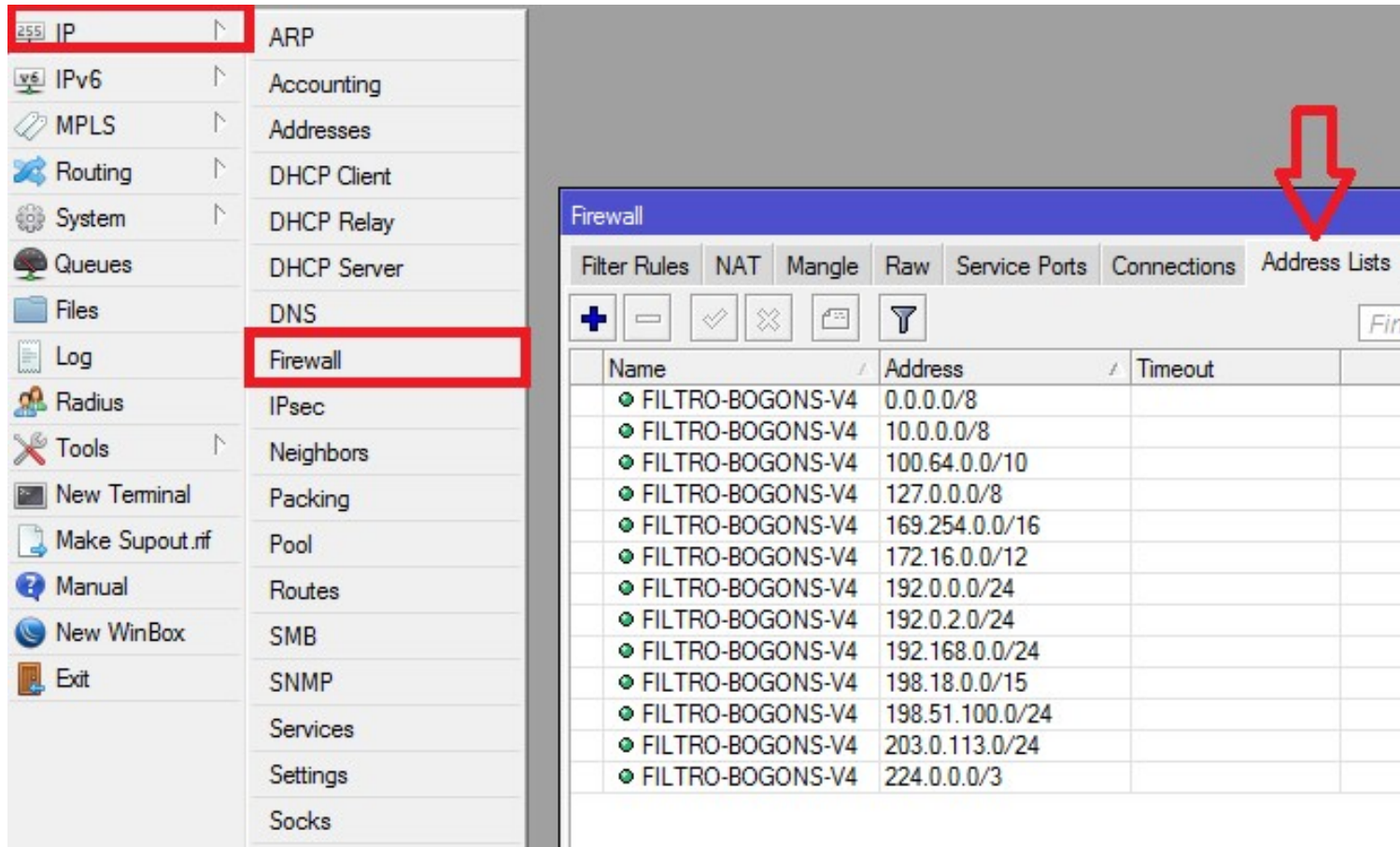
Anti Spoofing

- Se os equipamentos na rede onde os pacotes se originam não verificam sua origem, qualquer ação posterior para identificá-los ou bloqueá-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



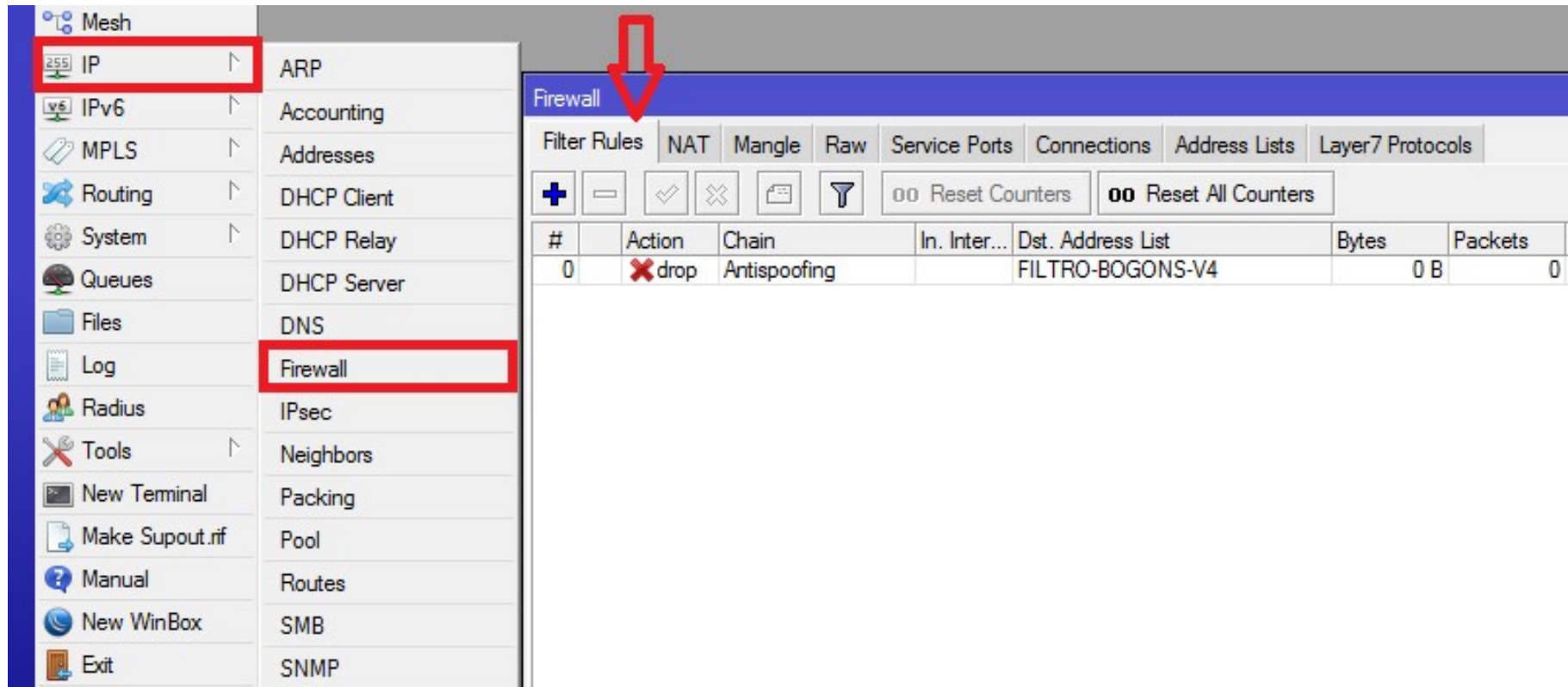
Configuração de Anti Spoofing IPv4 no RouterOS:



The screenshot shows the RouterOS WinBox interface. In the left sidebar, the 'IP' menu item is highlighted with a red box, and the 'Firewall' sub-item is also highlighted with a red box. The main panel displays the 'Firewall' configuration page, with the 'Filter Rules' tab selected. A red arrow points to the 'Filter Rules' tab. Below the tab, there is a table of filter rules.

Name	Address	Timeout
FILTRO-BOGONS-V4	0.0.0.0/8	
FILTRO-BOGONS-V4	10.0.0.0/8	
FILTRO-BOGONS-V4	100.64.0.0/10	
FILTRO-BOGONS-V4	127.0.0.0/8	
FILTRO-BOGONS-V4	169.254.0.0/16	
FILTRO-BOGONS-V4	172.16.0.0/12	
FILTRO-BOGONS-V4	192.0.0.0/24	
FILTRO-BOGONS-V4	192.0.2.0/24	
FILTRO-BOGONS-V4	192.168.0.0/24	
FILTRO-BOGONS-V4	198.18.0.0/15	
FILTRO-BOGONS-V4	198.51.100.0/24	
FILTRO-BOGONS-V4	203.0.113.0/24	
FILTRO-BOGONS-V4	224.0.0.0/3	

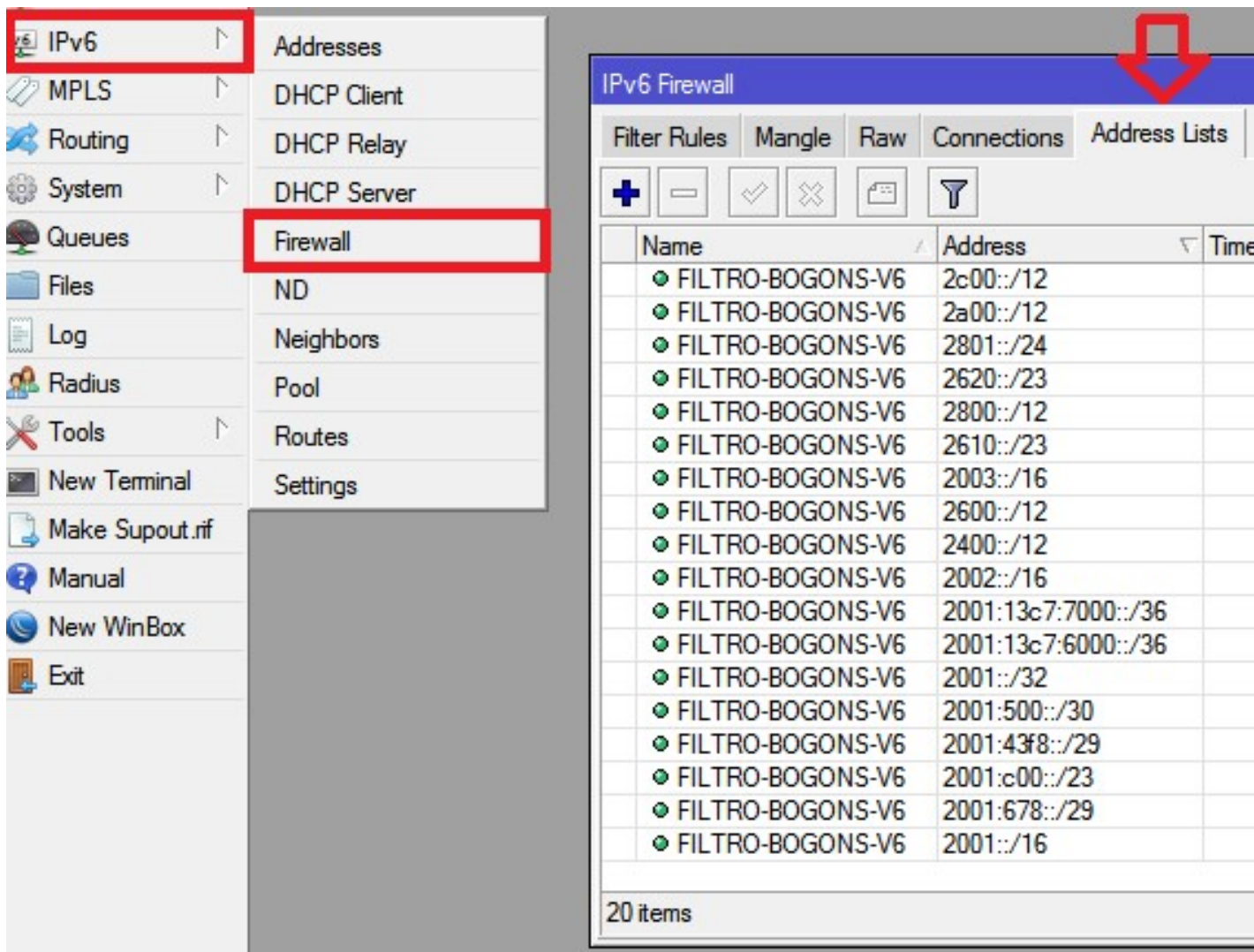
Configuração de Anti Spoofing IPv4 no RouterOS:



The screenshot displays the Mikrotik WinBox interface for configuring the Firewall. In the left sidebar, the 'IP' menu item is highlighted with a red box, and the 'Firewall' sub-menu is also highlighted. A red arrow points to the 'Firewall' tab in the main window. The 'Filter Rules' tab is active, showing a rule named 'Antispoofing' with the action 'drop' and the destination address list 'FILTRO-BOGONS-V4'.

#	Action	Chain	In. Inter...	Dst. Address List	Bytes	Packets
0	✖ drop	Antispoofing		FILTRO-BOGONS-V4	0 B	0

Configuração de Anti Spoofing IPv6 no RouterOS:

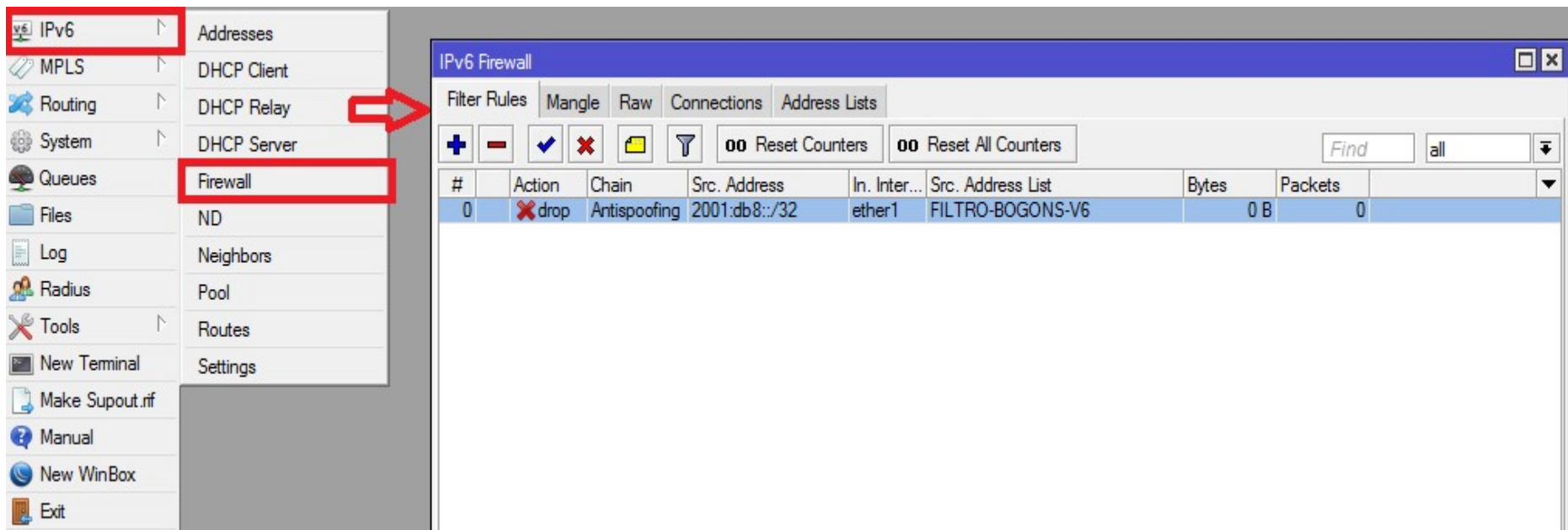


The screenshot shows the RouterOS WinBox interface. In the left sidebar, the 'IPv6' menu item is highlighted with a red box, and the 'Firewall' sub-item is also highlighted with a red box. The main window displays the 'IPv6 Firewall' configuration page, with the 'Filter Rules' tab selected. A red arrow points to the 'Filter Rules' tab. The table below lists 20 bogon filter rules.

Name	Address	Time
FILTRO-BOGONS-V6	2c00::/12	
FILTRO-BOGONS-V6	2a00::/12	
FILTRO-BOGONS-V6	2801::/24	
FILTRO-BOGONS-V6	2620::/23	
FILTRO-BOGONS-V6	2800::/12	
FILTRO-BOGONS-V6	2610::/23	
FILTRO-BOGONS-V6	2003::/16	
FILTRO-BOGONS-V6	2600::/12	
FILTRO-BOGONS-V6	2400::/12	
FILTRO-BOGONS-V6	2002::/16	
FILTRO-BOGONS-V6	2001:13c7:7000::/36	
FILTRO-BOGONS-V6	2001:13c7:6000::/36	
FILTRO-BOGONS-V6	2001::/32	
FILTRO-BOGONS-V6	2001:500::/30	
FILTRO-BOGONS-V6	2001:43f8::/29	
FILTRO-BOGONS-V6	2001:c00::/23	
FILTRO-BOGONS-V6	2001:678::/29	
FILTRO-BOGONS-V6	2001::/16	

20 items

Configuração de Anti Spoofing IPv6 no RouterOS:

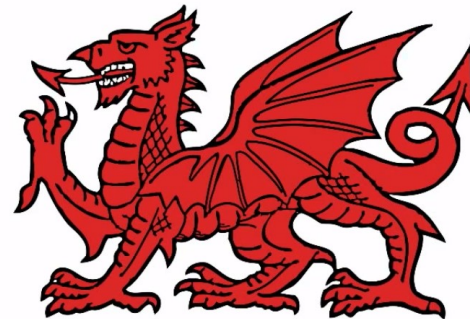


The screenshot shows the RouterOS WinBox interface. In the left sidebar, the 'IPv6' menu item is highlighted with a red box, and the 'Firewall' sub-item is also highlighted with a red box. A red arrow points from the 'Firewall' sub-item to the 'Filter Rules' tab in the main window. The 'Filter Rules' tab is active, showing a table of rules. The table has columns: #, Action, Chain, Src. Address, In. Inter..., Src. Address List, Bytes, and Packets. There is one rule listed: # 0, Action drop (indicated by a red X icon), Chain Antispoofing, Src. Address 2001:db8::/32, In. Inter... ether1, Src. Address List FILTRO-BOGONS-V6, Bytes 0 B, and Packets 0.

#	Action	Chain	Src. Address	In. Inter...	Src. Address List	Bytes	Packets
0	drop	Antispoofing	2001:db8::/32	ether1	FILTRO-BOGONS-V6	0 B	0

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



[Our Insight](#) [Our Initiatives](#) [Dragon News](#) [Who We Are](#)

HOW DO I OBTAIN A PEERING SESSION?

To peer with the bogon route servers, contact bogons@cymru.com. When requesting a peering session, please include the following information in your e-mail:

1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
2. Your AS number
3. The IP address(es) you want us to peer with
4. Does your equipment support MD5 passwords for BGP sessions?
5. Optional: your GPG/PGP public key

We will typically provide multiple peering sessions (at least 2) per remote peer for redundancy. If you would like more or less than 2 sessions please note that in your request. We try to respond to new peering requests within one to two business days, but, again, can provide no guarantees for this free service.

Remember that you must be able to accommodate up to 100 prefixes for traditional bogons, and up to 50,000 prefixes for fullbogons, and be capable of multihop peering with a private ASN. If you improperly configure your peering and route all packets destined for bogon addresses to the bogon route-servers, your peering session will be dropped.

LOCATE US

Team Cymru, Inc.
901 International Parkway

LOOKING FOR MORE INSIGHT?

TALK WITH US 

CONNECT WITH US

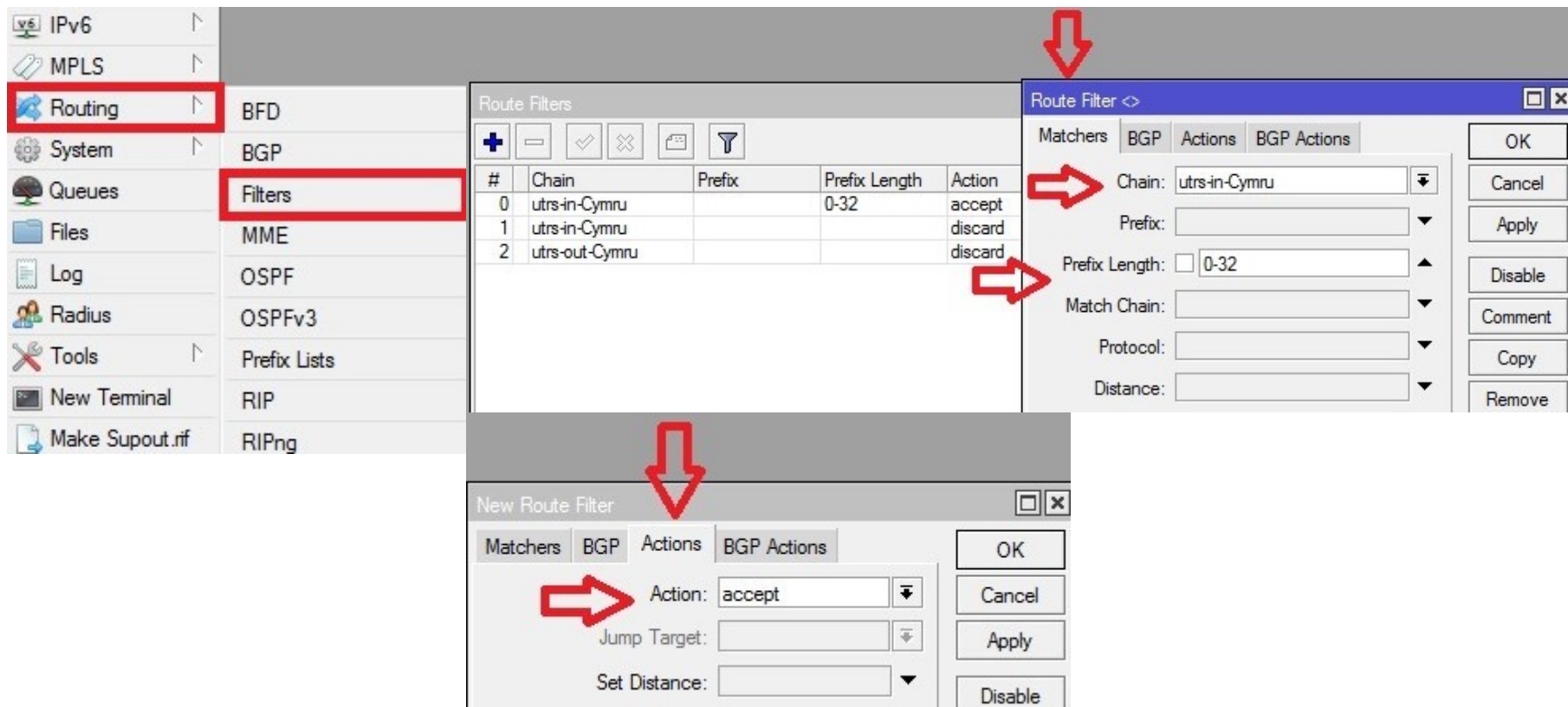


<http://www.team-cymru.org/bogon-reference.html>

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.

Configuração UTRS no RouterOS:

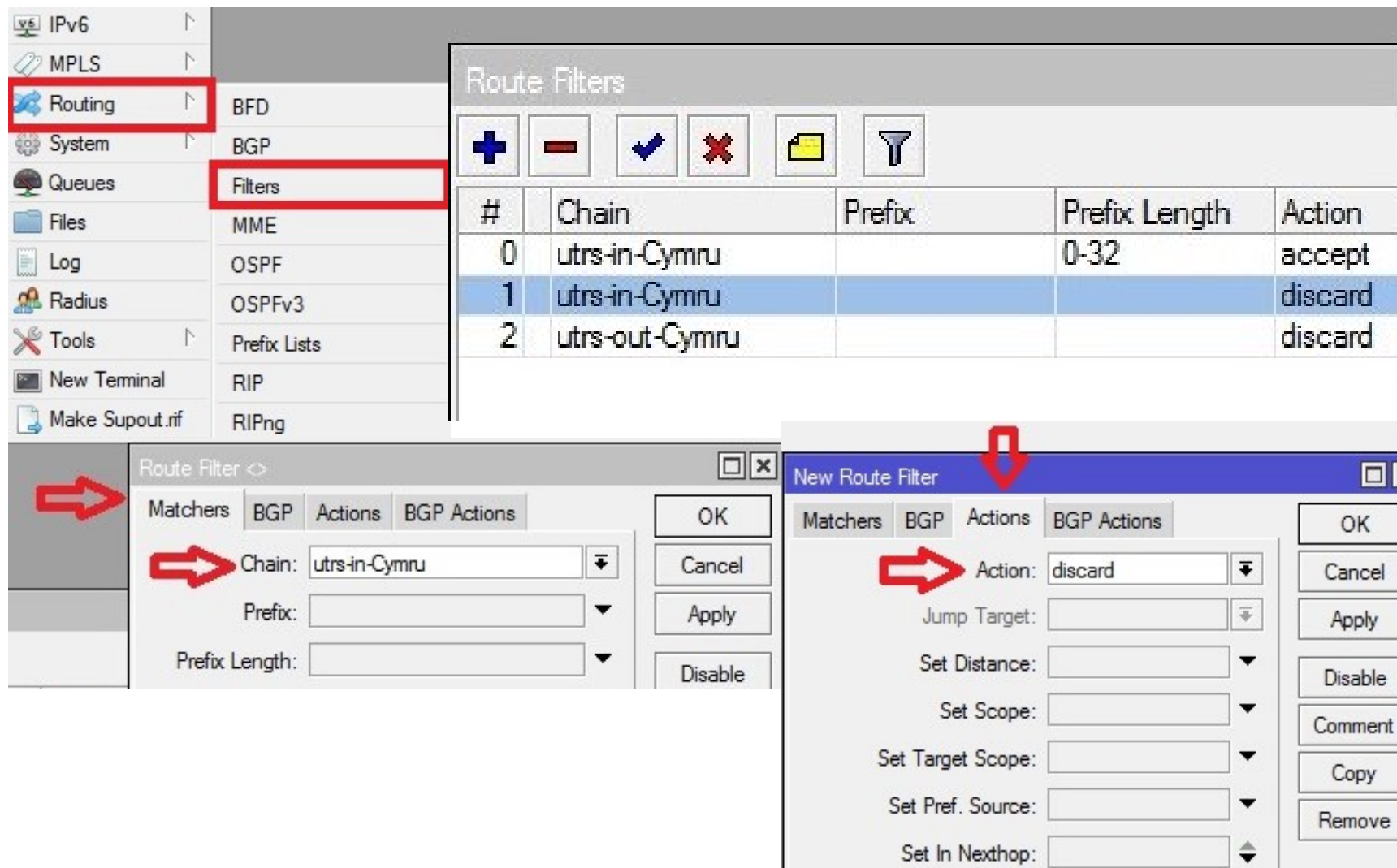


The screenshot illustrates the configuration steps for UTRS in RouterOS. The left sidebar shows the navigation menu with 'Routing' and 'Filters' highlighted. The main window displays the 'Route Filters' table and the 'New Route Filter' dialog.

#	Chain	Prefix	Prefix Length	Action
0	utrs-in-Cymru		0-32	accept
1	utrs-in-Cymru			discard
2	utrs-out-Cymru			discard

The 'New Route Filter' dialog shows the 'Actions' tab selected, with 'Action' set to 'accept'.

Configuração UTRS no RouterOS:



The screenshot shows the RouterOS WinBox interface. The 'Routing' menu is expanded, and 'Filters' is selected. The 'Route Filters' table is displayed, showing three filters:

#	Chain	Prefix	Prefix Length	Action
0	utrs-in-Cymru		0-32	accept
1	utrs-in-Cymru			discard
2	utrs-out-Cymru			discard

The 'New Route Filter' dialog is open, showing the 'Chain' set to 'utrs-in-Cymru' and the 'Action' set to 'discard'.

Configuração UTRS no RouterOS:

The screenshot illustrates the configuration of UTRS (User Traffic Routing) in RouterOS. The interface shows the 'Routing' menu expanded, with 'Filters' selected. A table lists existing filters, and two new dialog boxes show the configuration for a new filter named 'utrs-out-Cymru'.

#	Chain	Prefix	Prefix Length	Action
0	utrs-in-Cymru		0-32	accept
1	utrs-in-Cymru			discard
2	utrs-out-Cymru			discard

New Route Filter Configuration:

- Chain: utrs-out-Cymru
- Prefix: (empty)
- Prefix Length: (empty)
- Match Chain: (empty)
- Protocol: (empty)
- Distance: (empty)

Route Filter Configuration:

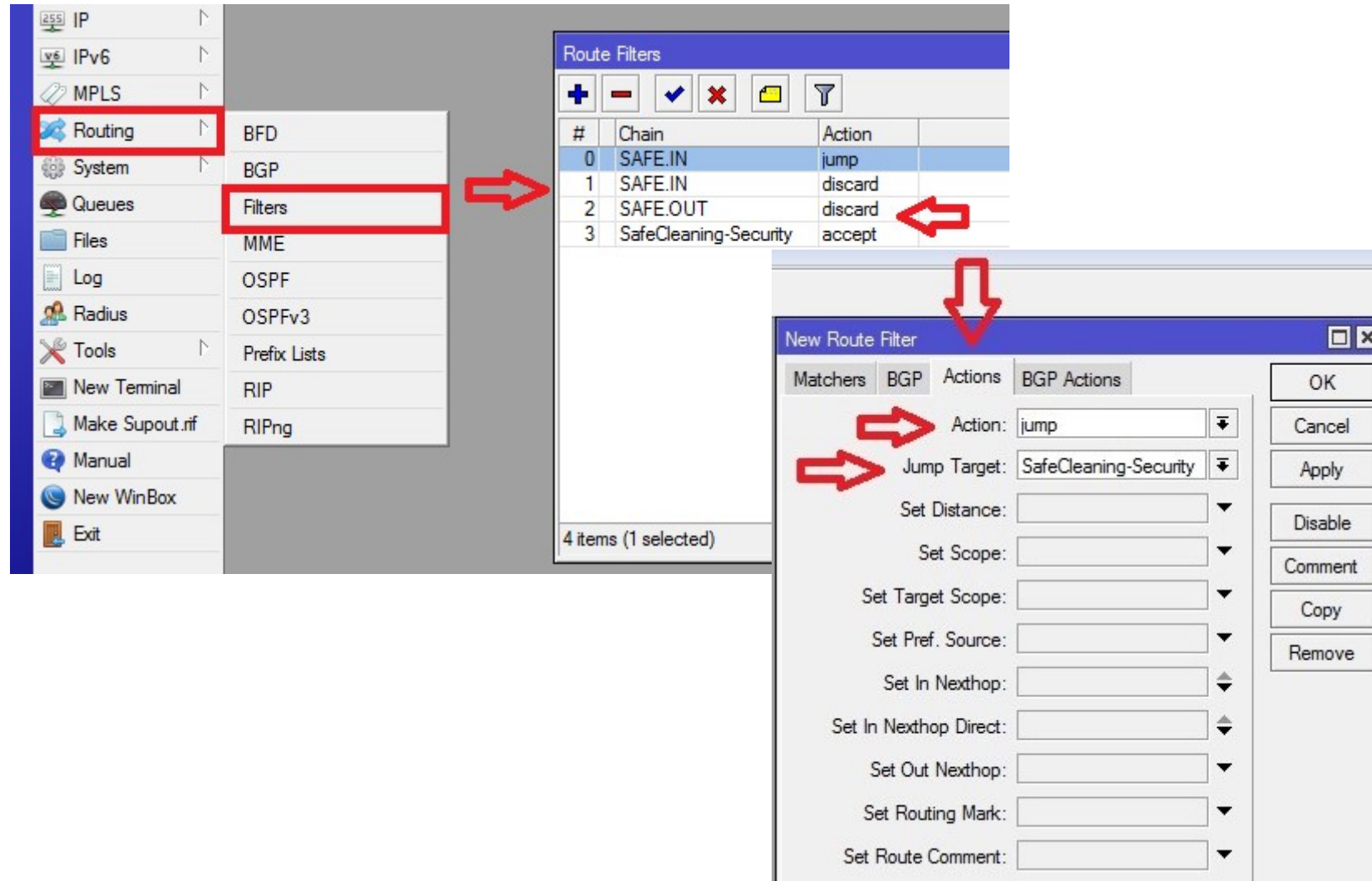
- Action: discard
- Jump Target: (empty)

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.



Configuração de SafeBGP no RouterOS:



The screenshot illustrates the configuration of SafeBGP in RouterOS. The left sidebar shows the 'Routing' menu with 'Filters' selected. The main window displays the 'Route Filters' table, which contains the following data:

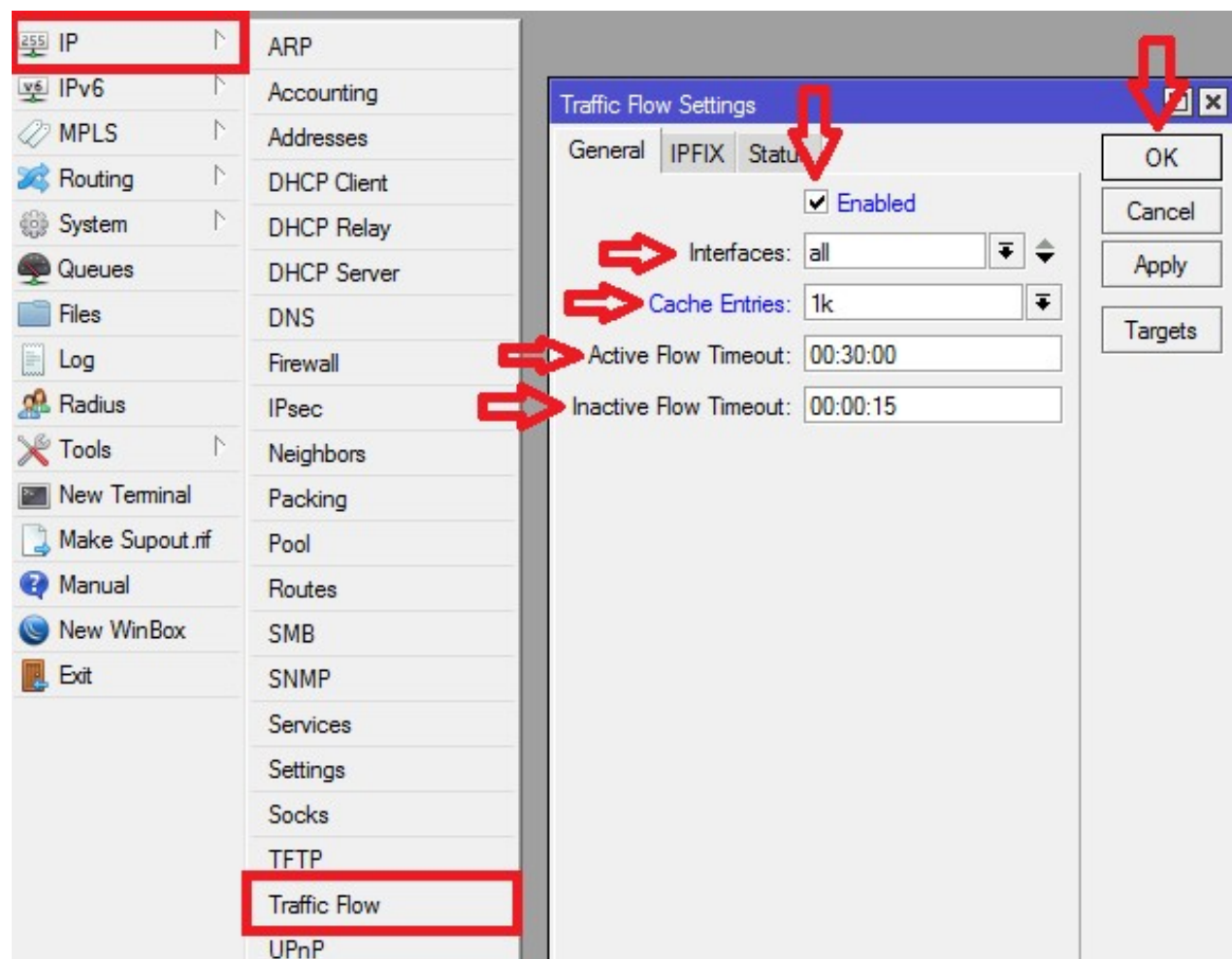
#	Chain	Action
0	SAFE.IN	jump
1	SAFE.IN	discard
2	SAFE.OUT	discard
3	SafeCleaning-Security	accept

The 'New Route Filter' dialog is open, showing the 'BGP' tab. The 'Action' is set to 'jump' and the 'Jump Target' is set to 'SafeCleaning-Security'. The dialog also includes fields for 'Set Distance', 'Set Scope', 'Set Target Scope', 'Set Pref. Source', 'Set In Nexthop', 'Set In Nexthop Direct', 'Set Out Nexthop', 'Set Routing Mark', and 'Set Route Comment'.

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.

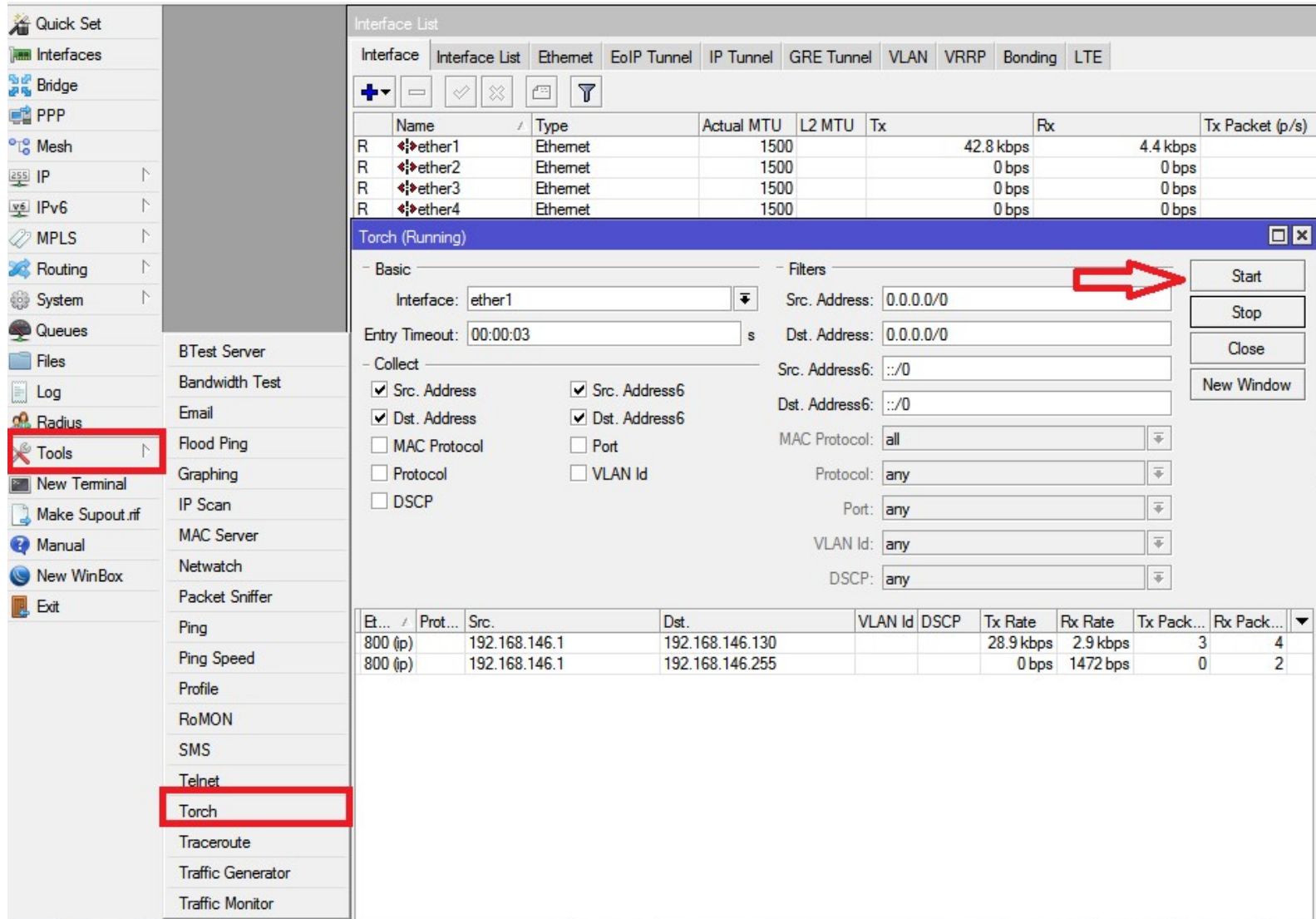
Configuração de NetFlows no RouterOS



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:



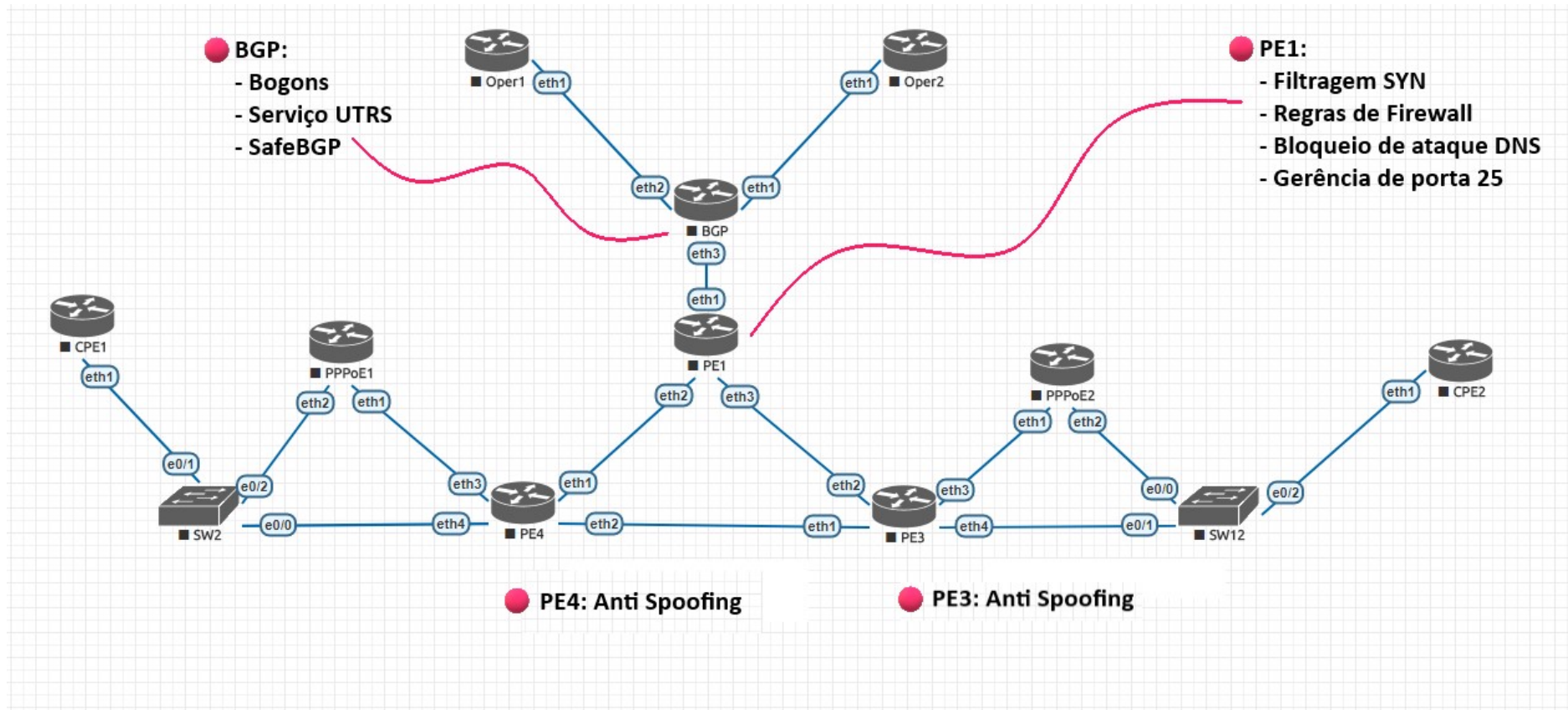
The screenshot shows the RouterOS WinBox interface. On the left sidebar, the 'Tools' menu is expanded, and 'Torch' is highlighted. The main window displays the 'Torch (Running)' configuration dialog. A red arrow points to the 'Start' button. The configuration includes the following fields:

- Basic:** Interface: ether1, Entry Timeout: 00:00:03 s
- Collect:**
 - ☒ Src. Address, ☒ Src. Address6
 - ☒ Dst. Address, ☒ Dst. Address6
 - ☐ MAC Protocol, ☐ Port
 - ☐ Protocol, ☐ VLAN Id
 - ☐ DSCP
- Filters:**
 - Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0
 - Src. Address6: ::/0, Dst. Address6: ::/0
 - MAC Protocol: all, Protocol: any
 - Port: any, VLAN Id: any
 - DSCP: any

At the bottom of the window, there is a table showing the results of the Torch test:

Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)		192.168.146.1	192.168.146.130			28.9 kbps	2.9 kbps	3	4
800 (ip)		192.168.146.1	192.168.146.255			0 bps	1472 bps	0	2

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

