

# 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.
- Coordenadora do departamento de Engenharia da Solintel.





MOGA  
Telecom



# Você acredita que sua rede está realmente segura?



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

- Sobre o CERT.br
- C-SIRTs
- Estadísticas
  - Incidentes
  - Spam
- Cursos
- Projetos
- Publicações
- Palestras
- Links
- FAQ
- Mapa do site
- Contato
- RSS

Busca

Núcleo de Informação e Coordenação do Ponto BR

CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTR0.br - W3C.br

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

## 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**







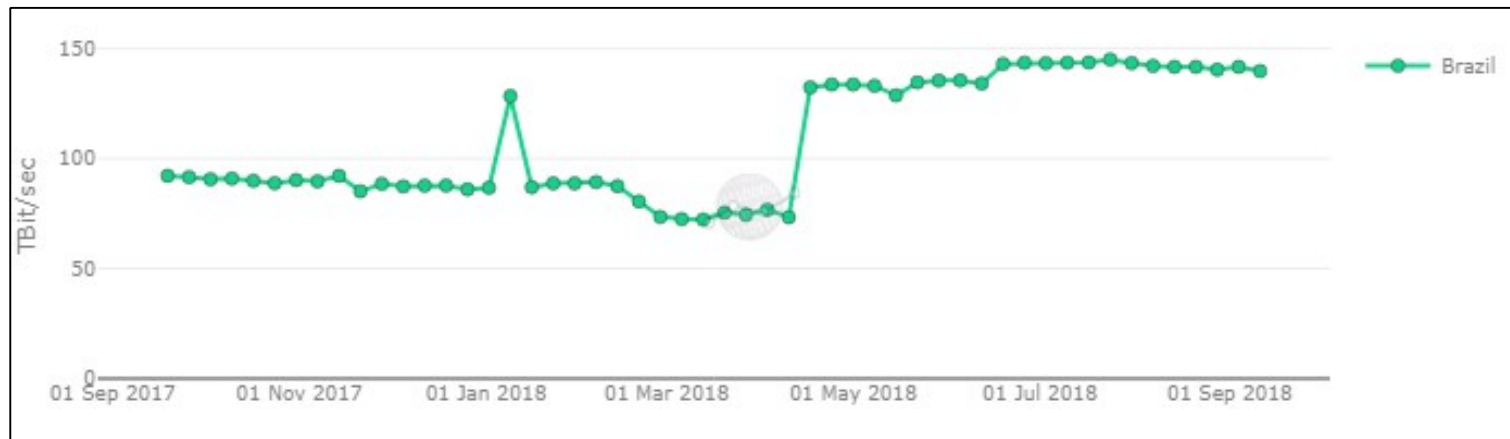

## Brasil foi alvo do maior ataque DDoS do mundo

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 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.

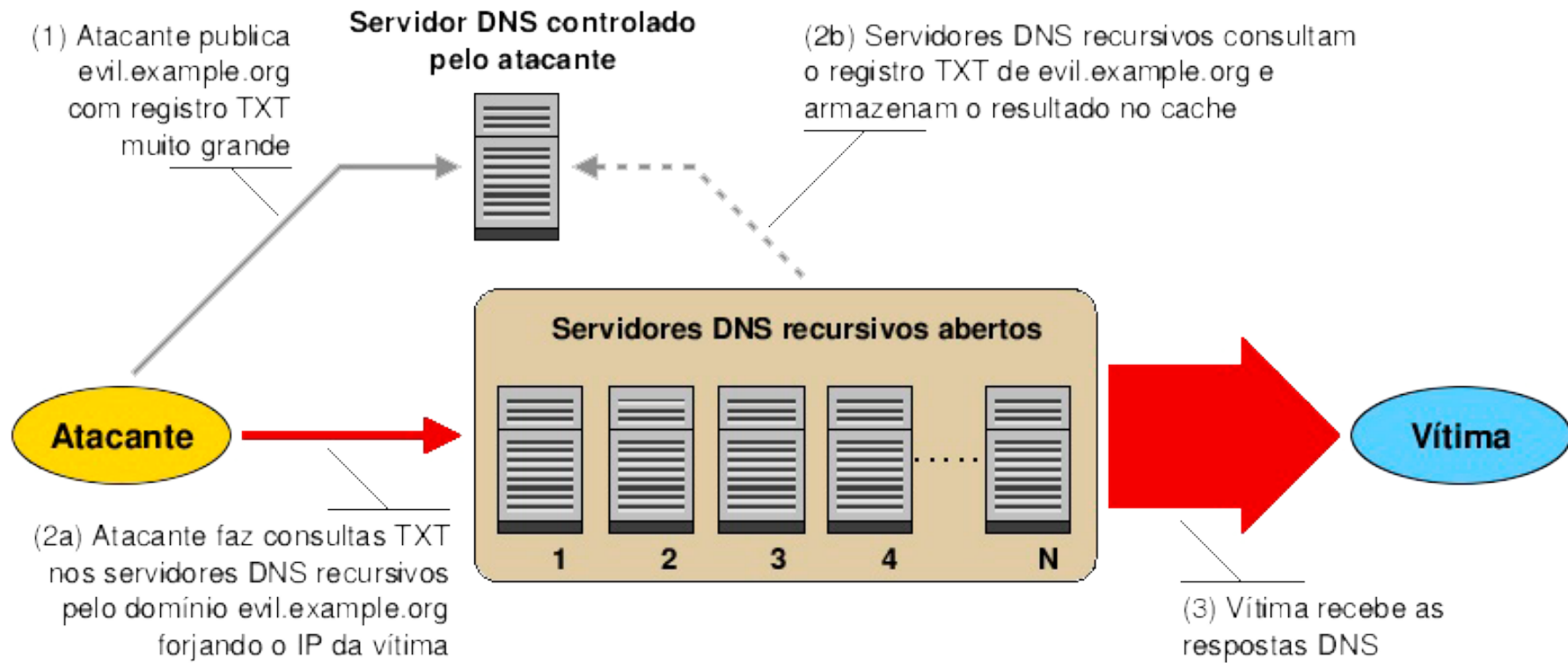
## Ataque de exaustão de hardware

- 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 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
<b>\$4</b>	<b>\$10</b> monthly	<b>\$15</b> monthly	<b>\$30</b> monthly
120 second Stress Tests 1 attack(s) at once 5-10Gbps Stress Tests Unlimited Stress Tests per day	300 second Stress Tests 1 attack(s) at once 5-10Gbps Stress Tests Unlimited Stress Tests per day	700 second Stress Tests 2 attack(s) at once 5-10Gbps Stress Tests Unlimited Stress Tests per day	3600 second Stress Tests 2 attack(s) at once 10+ Gbps Stress Tests Unlimited Stress Tests per day
<b>PURCHASE</b>	<b>PURCHASE</b>	<b>PURCHASE</b>	<b>PURCHASE</b>



# 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

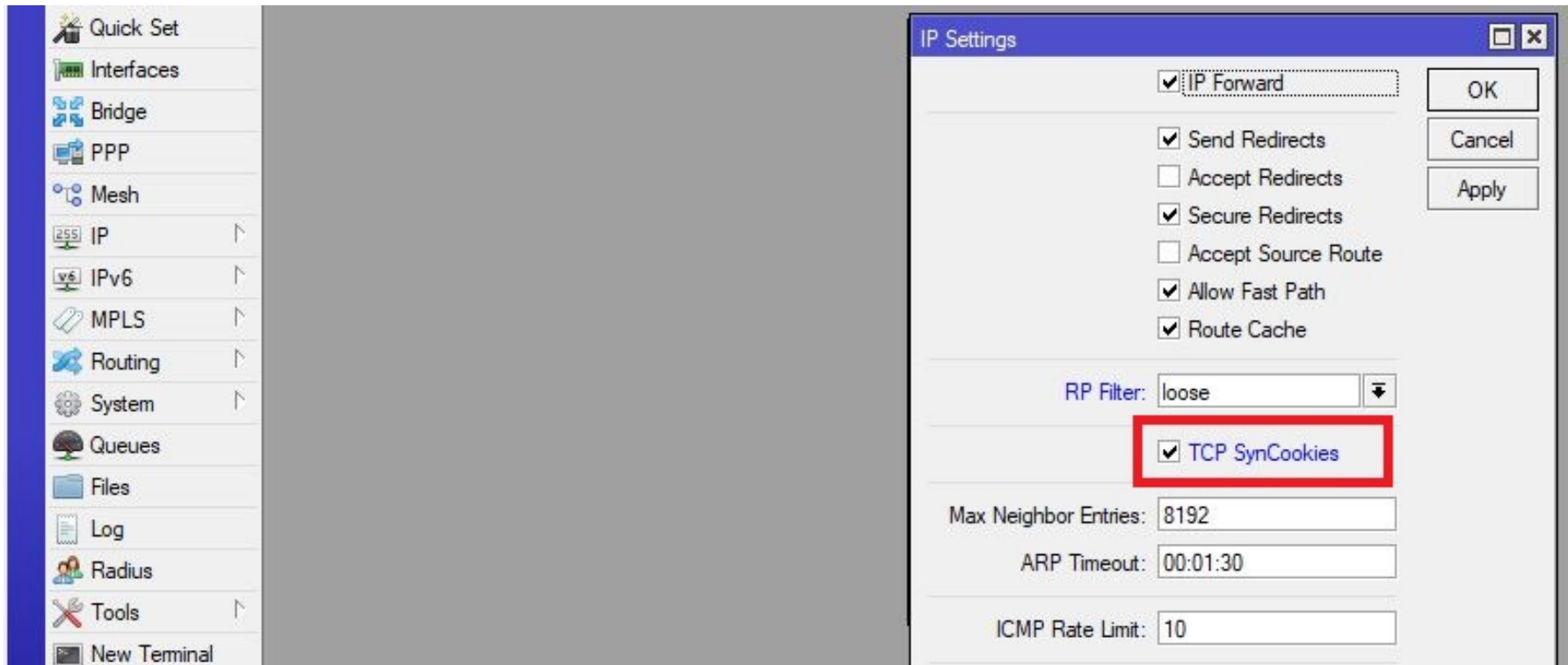
Some advanced filtering can be applied to tcp packet state.

```
/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](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 (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.





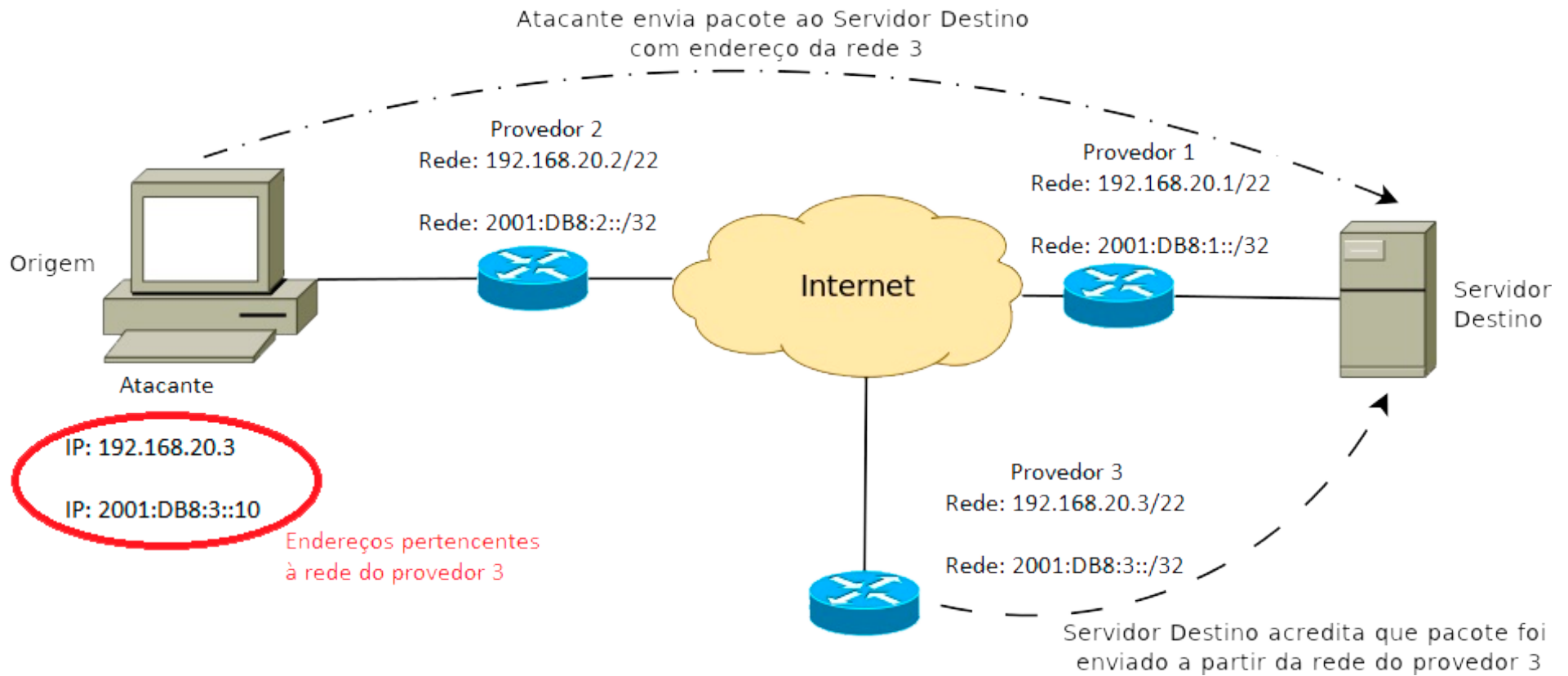
## Anti Spoofing

- 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.

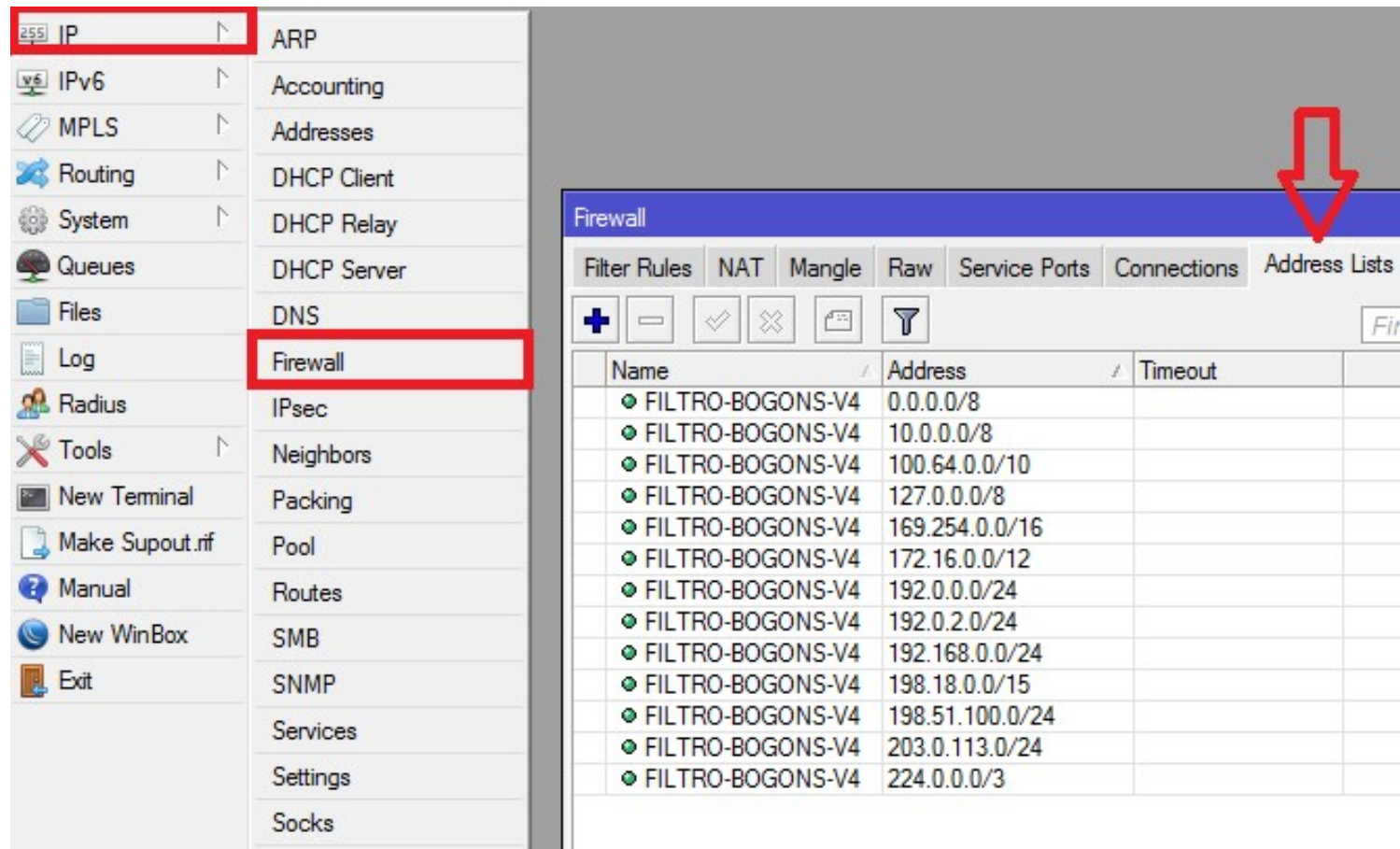
## Anti Spoofing

- 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 Mikrotik WinBox interface. On the left, the 'IP' menu is highlighted with a red box, and the 'Firewall' sub-menu is also highlighted with a red box. On the right, the Firewall configuration window is open, showing the 'Address Lists' tab. A red arrow points to this tab. Below the tabs, there is a table of configured address lists.

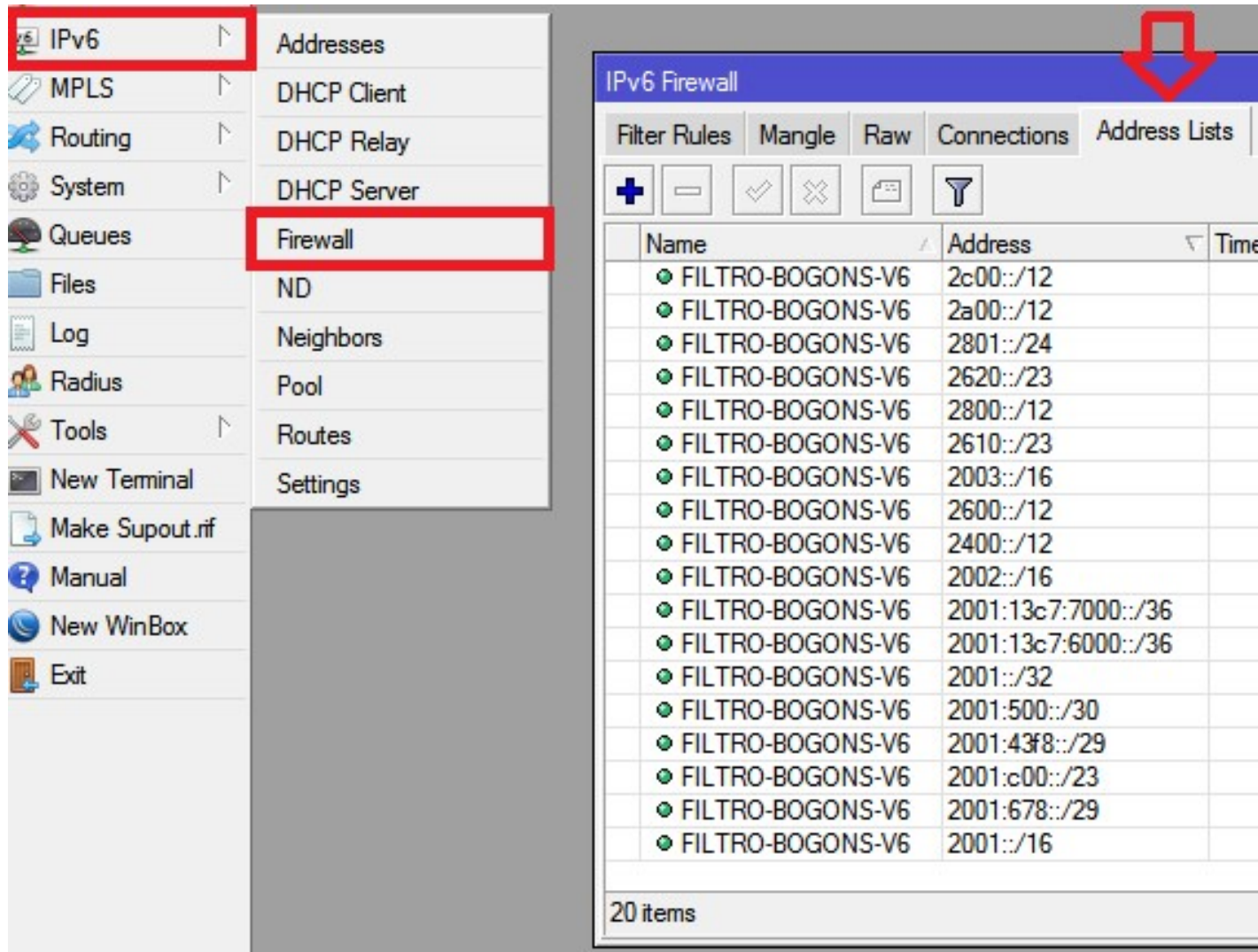
Name	Address	Timeout
FILTRO-BOGONS-V4	0.0.0.0/8	
FILTRO-BOGONS-V4	10.0.0.0/8	
FILTRO-BOGONS-V4	100.64.0.0/10	
FILTRO-BOGONS-V4	127.0.0.0/8	
FILTRO-BOGONS-V4	169.254.0.0/16	
FILTRO-BOGONS-V4	172.16.0.0/12	
FILTRO-BOGONS-V4	192.0.0.0/24	
FILTRO-BOGONS-V4	192.0.2.0/24	
FILTRO-BOGONS-V4	192.168.0.0/24	
FILTRO-BOGONS-V4	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. On the left sidebar, the 'IP' 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 'Firewall' tab in the main window. The 'Filter Rules' tab is active, showing a table with one rule:

#	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:

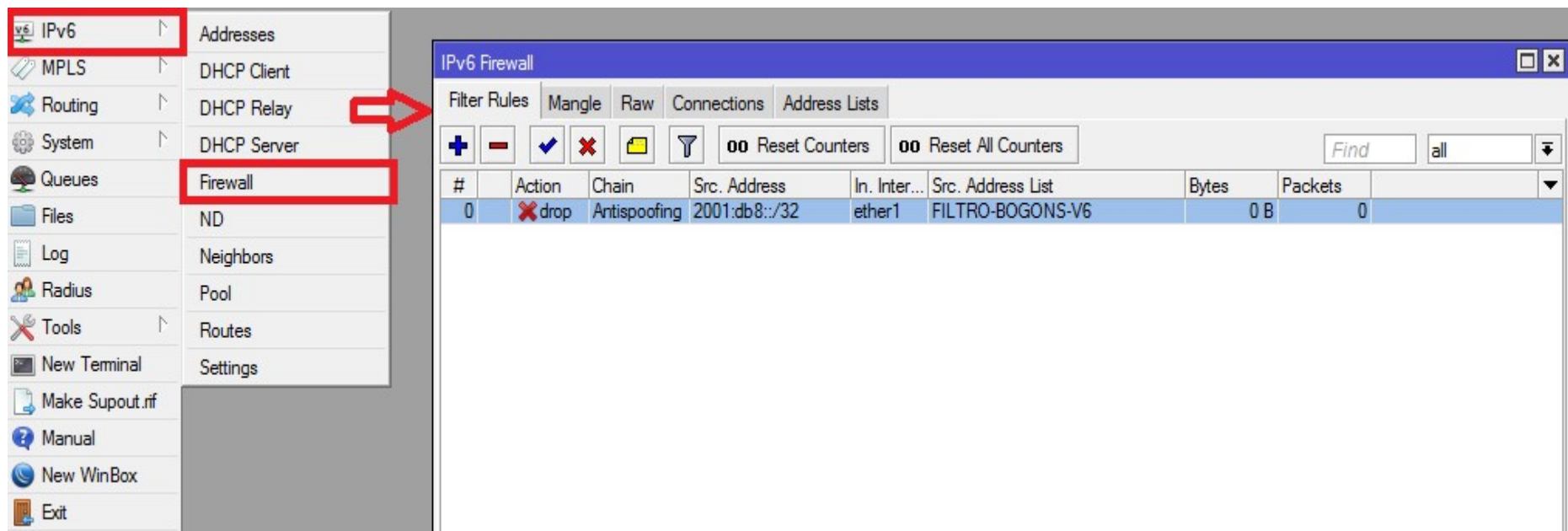


The screenshot shows the RouterOS WinBox interface. On the left, the 'IPv6' menu is expanded, and the 'Firewall' sub-menu is selected. The main window displays the 'IPv6 Firewall' configuration page, showing a list of 20 bogon address ranges. A red arrow points to the 'IPv6 Firewall' window title bar.

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 displays the RouterOS configuration interface for IPv6 Firewall. The left sidebar shows the 'IPv6' menu expanded, with 'Firewall' selected. The main window shows the 'IPv6 Firewall' configuration for the 'Filter Rules' tab. The table below shows the configuration for a rule named 'Antispoofing'.

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

---

## Normas de Acordo Mútuo para Segurança de Roteamento



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

The screenshot shows the Walled Garden website interface. At the top left is the logo 'WG WALLED GARDEN'. To its right is a navigation menu with links: HOME, SOBRE, A SOLUÇÃO, COMO FUNCIONA, and CONTATO. Further right are two input fields labeled 'E-Mail' and 'Nome', followed by two buttons: 'CADASTRAR' (highlighted in orange) and 'ENTRAR'. The main content area features a dark background with a satellite-style map of a city. Overlaid on the map is the following text:

**33 ATAQUES POR SEGUNDO**  
**117.572 POR HORA**  
**84.652.096 POR MÊS**

Estes ataques foram registrados na América Latina durante os primeiros oito meses de 2018. Proteja sua rede e seus clientes. Cadastre-se.

# WALLED GARDEN



## SOBRE

A Walled Garden traz um novo marco para segurança da internet global. Nossa solução consiste em estratégias coletivas de segurança de roteamento pensadas em conjunto com diversos especialistas do setor para proteger a rede contra milhares de ameaças que a internet possui, aumentando a disponibilidade e confiabilidade dos serviços. Com isso, asseguramos que a proteção aconteça logo que algum ataque for identificado em qualquer lugar da rede mundial de internet, evitando sua propagação.

## A SOLUÇÃO



### SURGE UMA AMEAÇA

A internet traz um fluxo de informações rápido e constante. Por ser acessível a todos, ela passa a ser incerta, e oferece riscos que colocam a prova a segurança e a privacidade da sua rede



### SEU BGP COMUNICA NOSSA CENTRAL

Para assegurar a estabilidade e proteção da sua rede a Walled Garden atua de duas formas



### NEUTRALIZAMOS A AMEAÇA

Criando uma barreira que mantém sua rede imune da grande quantidade de lixo que a internet produz



### COMUNICAMOS OUTROS BGPS

Prevenindo que seus usuários e equipamentos sejam atacados e/ou usados para ataques, garantindo a qualidade do seu serviço sempre

# WALLED GARDEN

## AS AMEAÇAS

### ROUTE HIJACKING

Um ataque de sessão BGP pode ser projetado para derrubar uma sessão, ou ainda, com o objetivo de mudar rotas usadas pelo peer, a fim de facilitar a espionagem, buraco negro ou a análise de tráfego. Esse tipo de ataque causa interrupções graves, incluindo perda completa de conectividade. Basta encontrar um BGP que seja suscetível ao ataque.

### DDOS

Nos Ataques Distribuídos de Negação de Serviços, um computador mestre direciona um ataque em massa usando um exército de máquinas infectadas. Este ataque visa tornar um servidor, serviço ou infraestrutura indisponível. O ataque pode assumir várias formas: uma sobrecarga da largura de banda do servidor para o tornar indisponível ou um esgotamento dos recursos de sistema da máquina, impedindo-a de responder ao tráfego legítimo.

### ROUTE LEAKS

Os vazamentos de rotas envolvem anúncios ilegítimos de prefixos (blocos de endereços IP) que se propagam pelas redes e levam a um roteamento comprometido. Estes vazamentos de rotas são, geralmente, inadvertidos e acontecem devido à configurações incorretas do filtro.

### IP ADDRESS SPOOFING

Mascarar o endereço de origem por meio de uma manipulação simples do cabeçalho IP. Assim, vários computadores podem enviar pacotes fazendo-se passar por um determinado endereço de origem, o que representa uma séria ameaça para os sistemas baseados em autenticação pelo endereço IP.

### PHISHING

Captura de informações e dados pessoais importantes através de mensagens falsas. Com isso, é possível conseguir nomes de usuários e senhas, e dados de contas bancárias e cartões de crédito.

<https://walledgarden.global/>

# Exemplo do Walled Garden no RouterOS:

Route List

Routes Nexthops Rules VRF

+ - [check] [cross] [info] [filter]

	Dst. Address	Gateway	Distance
DAbB	▶ 0.0.0.0/8		20
DAbB	▶ 1.0.149.23		20
DAbB	▶ 1.1.5.5		20
DAbB	▶ 1.4.209.6		20
DAbB	▶ 1.9.111.145		20
DAbB	▶ 1.10.16.0/20		20
DAbB	▶ 1.10.188.29		20
DAbB	▶ 1.10.248.106		20
DAbB	▶ 1.25.138.74		20
DAbB	▶ 1.26.38.171		20
DAbB	▶ 1.28.124.58		20
DAbB	▶ 1.30.190.204		20
DAbB	▶ 1.31.110.175		20
DAbB	▶ 1.32.128.0/18		20
DAbB	▶ 1.34.1.60		20
DAbB	▶ 1.36.92.121		20
DAbB	▶ 1.52.79.184		20
DAbB	▶ 1.53.137.12		20
DAbB	▶ 1.53.137.84		20
DAbB	▶ 1.53.137.92		20
DAbB	▶ 1.53.137.164		20
DAbB	▶ 1.53.137.220		20
DAbB	▶ 1.54.208.133		20
DAbB	▶ 1.55.241.4		20
DAbB	▶ 1.57.22.19		20
DAbB	▶ 1.59.45.236		20
DAbB	▶ 1.62.11.37		20
DAbB	▶ 1.62.17.26		20
DAbB	▶ 1.83.76.61		20
DAbB	▶ 1.83.125.115		20
DAbB	▶ 1.85.7.26		20
DAbB	▶ 1.85.36.90		20
DAbB	▶ 1.85.114.221		20
DAbB	▶ 1.85.143.224		20
DAbB	▶ 1.85.209.208		20
DAbB	▶ 1.87.140.207		20

36880 items (1 selected)

# Exemplo do Walled Garden no RouterOS:

IPv6 Route List

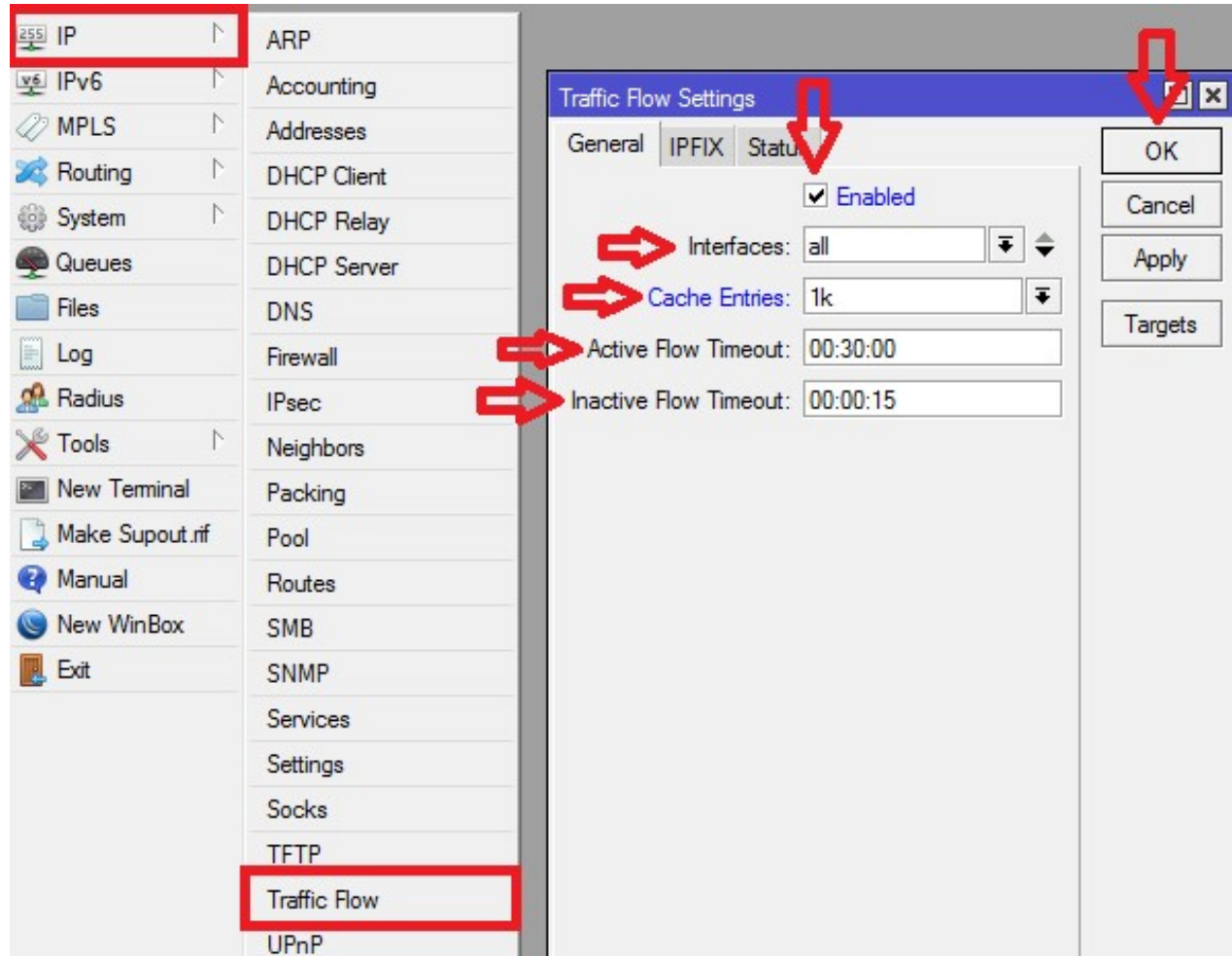
	Dst. Address	Gateway	Distance
DAbU	▶ 1000::/4		20
DAbU	▶ 200::/7		20
DAbU	▶ ::/8		20
DAbU	▶ 100::/8		20
DAbU	▶ 800::/5		20
DAbU	▶ 400::/6		20
DAbU	▶ 2000::/16		20
DAbU	▶ 2001:488::/29		20
DAbU	▶ 2001:498::/29		20
DAbU	▶ 2001:202::/31		20
DAbU	▶ 2001:201::/32		20
DAbU	▶ 2001:204::/30		20
DAbU	▶ 2001:209::/32		20
DAbU	▶ 2001:20a::/31		20
DAbU	▶ 2001:20c::/30		20
DAbU	▶ 2001:210:8000::/33		20
DAbU	▶ 2001:211::/32		20
DAbU	▶ 2001:212::/31		20
DAbU	▶ 2001:214::/30		20
DAbU	▶ 2001:219::/32		20
DAbU	▶ 2001:21a::/31		20
DAbU	▶ 2001:21c::/30		20
DAbU	▶ 2001:222::/31		20
DAbU	▶ 2001:224::/30		20
DAbU	▶ 2001:22a::/31		20
DAbU	▶ 2001:22c::/30		20
DAbU	▶ 2001:232::/31		20
DAbU	▶ 2001:221::/32		20
DAbU	▶ 2001:228:8000::/33		20
DAbU	▶ 2001:229::/32		20
DAbU	▶ 2001:231::/32		20
DAbU	▶ 2001:210:2000::/35		20
DAbU	▶ 2001:210:4000::/34		20
DAbU	▶ 2001:228:2000::/35		20
DAbU	▶ 2001:228:4000::/34		20
DAbU	▶ 2001:234::/30		20
DAbU	▶ 2001:239::/32		20
DAbU	▶ 2001:23a::/31		20

103395 items

## 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

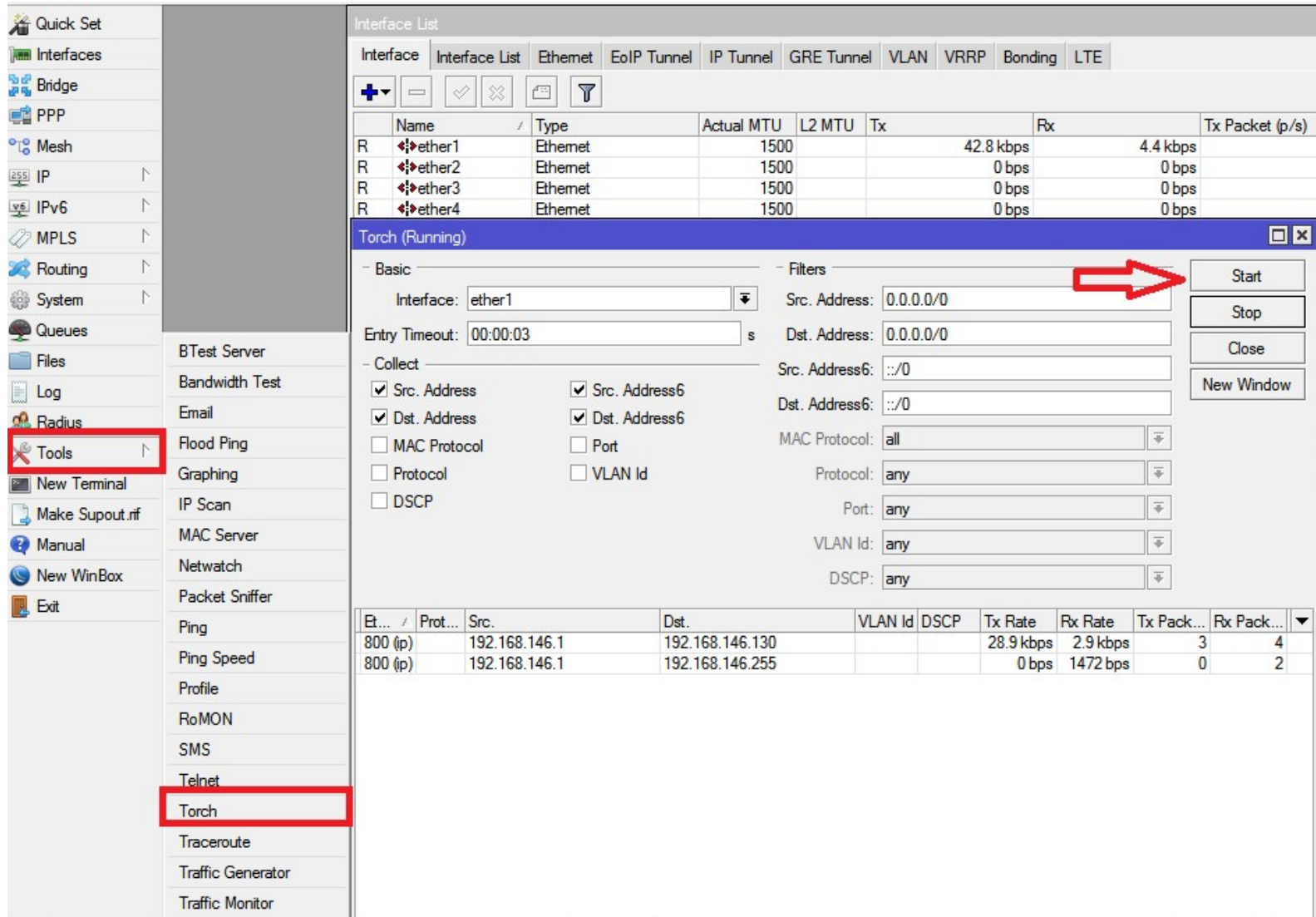


## Torch

- 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:



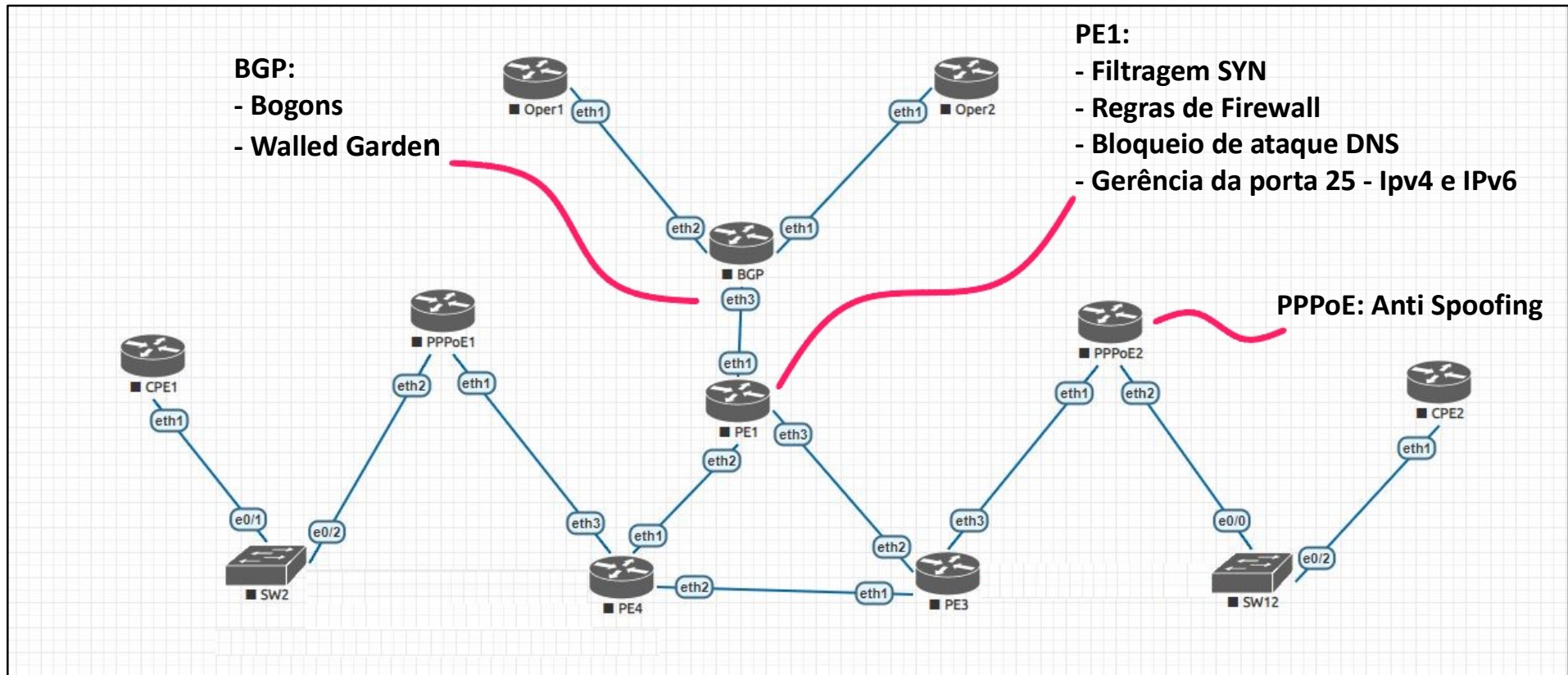
The screenshot shows the RouterOS web interface. On the left sidebar, the 'Tools' menu is highlighted with a red box. In the main area, the 'Torch (Running)' configuration window is open, also with a red box around its title bar. A red arrow points to the 'Start' button. The configuration includes the following fields:

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

At the bottom of the Torch window, there is a table showing traffic statistics:

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

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

# Dúvidas?




# OBRIGADA!!

- Tayla Guimarães Oliveira

 [tayla.oliveira@solintel.com.br](mailto:tayla.oliveira@solintel.com.br)

 solintel.engenharia8

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

 <https://www.linkedin.com/in/tayla-guimaraes>

