

6 motivos para atualizar a versão do RouterOS

Pietro Scherer
MUM Brazil 2018 - São Paulo

Apresentador

● **Pietro Scherer**

- MikroTik Certified Trainer - Riga, Latvia (2018)
- MikroTik Consultant - MTCNA, MTCWE, MTCRE, MTCINE, MTCIPv6E (2015).
- MUM Presenter - BR16, BR17 e BR18.
- Pós Graduação - Redes de Computadores.

Sponsor time :)

- www.tchesolutions.com.br - Assessoria e Consultoria para ISPs.
- www.routermage.com - Sistema de backups e gerenciamento para RouterOS.
- www.alivesolutions.com.br - Treinamentos Oficiais MikroTik

Objetivos

- Mostrar as novas funcionalidades que estão sendo incorporadas ao RouterOS.
- Mostrar a importância destas novas funcionalidades e como podem fazer a diferença na sua rede.

Agenda

- Tabela Raw;
- FastPath e FastTrack;
- Melhorias Nv2;
- Bridge e switching;
- Filtro de conteúdo;
- Segurança.

Tabela Raw

- Introduzido na versão 6.36 do RouterOS;
- Atua **antes** da **connection tracking**;
- Reduz significativamente o uso de CPU;
- Importante na mitigação de DDoS.
- IPv4 e IPv6.

Tabela Raw

- Possui duas chains apenas:
 - Prerouting: Qualquer pacote que **entra** no roteador;
 - Output: Pacotes que **originam do roteador**;
- **Não** possui matchers que dependem da Connection tracking.

Tabela Raw - Exemplo

- Drop DNS externo

The screenshot shows the Mikrotik WinBox interface. On the left, the 'Tools' menu is open, and 'Firewall' is selected. In the center, the 'DNS' service is highlighted. On the right, the 'Firewall' configuration window is open, showing the 'Raw' tab. The 'Raw' rule table is displayed, showing two rules for dropping recursive DNS traffic.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst.
6	✗ drop	prerouting			17 (udp)		53
7	✗ drop	prerouting			6 (tcp)		53

;;; Drop recursive DNS

Tabela Raw - Exemplo.

The image shows a screenshot of the Mikrotik WinBox Firewall configuration interface. On the left, the 'Firewall' window displays a table of rules. On the right, the 'Raw Rule <53>' configuration window is open, showing the 'General' tab with various settings. Arrows indicate the mapping between the configuration window fields and the table entries.

Firewall Rule Table:

#	Action	Chain	Src. Ad
;;; Drop recursive DNS			
6	drop	prerouting	
7	drop	prerouting	

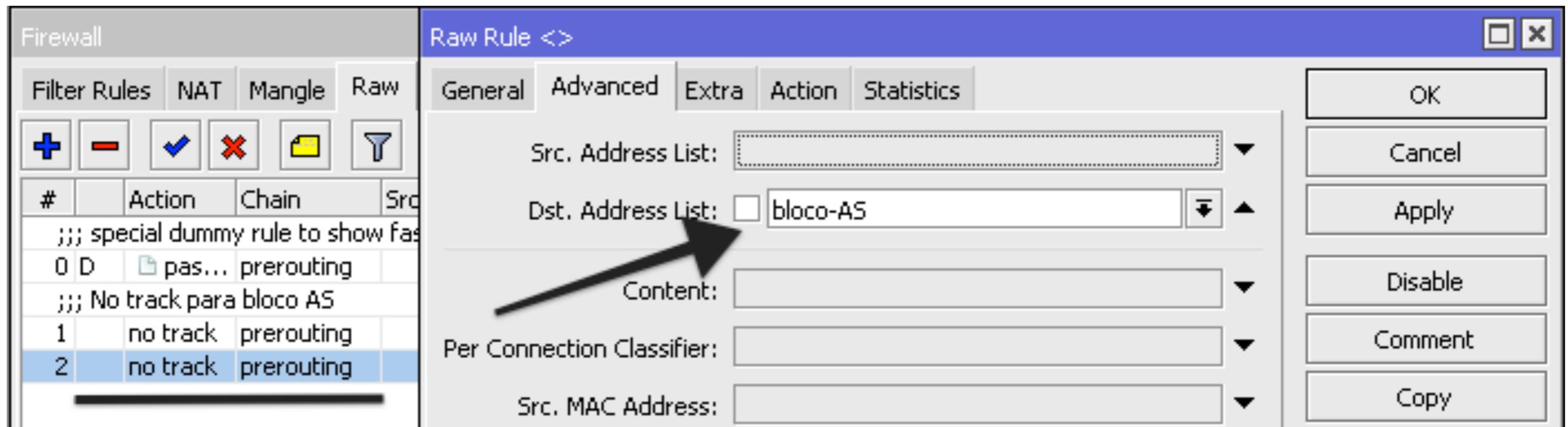
Raw Rule <53> Configuration (General Tab):

- Chain: prerouting
- Src. Address: [Empty]
- Dst. Address: [Empty]
- Protocol: 17 (udp)
- Src. Port: [Empty]
- Dst. Port: 53
- Any. Port: [Empty]
- In. Interface: [Empty]
- Out. Interface: [Empty]
- In. Interface List: WAN
- Out. Interface List: [Empty]

Buttons on the right side of the Raw Rule window: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters.

Tabela Raw - Exemplo.

- No Track para bloco AS



The screenshot shows the Mikrotik WinBox Firewall configuration interface. On the left, the 'Raw' tab is selected in the 'Filter Rules' section. A table lists the rules:

#	Action	Chain	Src
0	D pas...	prerouting	
;;; No track para bloco AS			
1	no track	prerouting	
2	no track	prerouting	

The 'Raw Rule' configuration window is open, showing the 'General' tab. The 'Dst. Address List' is set to 'bloco-AS'. A black arrow points to the 'Dst. Address List' field. The 'Content' field is empty. The 'Per Connection Classifier' and 'Src. MAC Address' fields are also empty. The 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', and 'Copy' buttons are visible on the right side of the window.

FastPath e FastTrack

- Introduzido na versão 6.29 do RouterOS;
- Permite um encaminhamento mais rápido de pacotes;
- Melhora significativamente o **encaminhamento** de pacotes e conseqüentemente o **desempenho** do roteador.

FastPath

- Suportado em todas as interfaces, na maioria dos roteadores.
 - CCR: Todas as interfaces;
 - RBR 100 series: ether 1-11;
 - Bridges: A partir da versão 6.29;
 - Vlan, bonding, vrrp: A partir da versão 6.30;
 - EoIP, GRE, IPIP: A partir da versão 6.33;

FastPath

- Condições para habilitar o FastPath:
 - Nenhuma regra de firewall ou address-list;
 - Nenhuma simple queue ou queue tree;
 - Connection tracking desabilitada;
 - Accounting desabilitado;
 - E mais alguns: https://wiki.mikrotik.com/wiki/Manual:Fast_Path#IPv4_handler

FastPath

The image shows the Mikrotik WinBox interface. On the left is a sidebar menu with categories like IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, and various utility options. The 'IP' category is selected, and the 'Settings' option is highlighted with a black arrow. The main window displays the 'IP Settings' configuration panel. In this panel, the 'Allow Fast Path' checkbox is checked. Below it, the 'IPv4 Fast Path Active' checkbox is also checked, with a black arrow pointing to it. Other settings include 'IP Forward' (checked), 'Send Redirects' (checked), 'Secure Redirects' (checked), 'Route Cache' (checked), 'RP Filter' (set to 'no'), 'Max Neighbor Entries' (8192), 'ARP Timeout' (00:00:30), and 'ICMP Rate Limit' (10). There are also fields for 'IPv4 Fast Path Packets' and 'IPv4 Fast Path Bytes', both showing 0. At the bottom, there are fields for 'IPv4 Fasttrack Packets' and 'IPv4 Fasttrack Bytes', both showing 0. The 'OK', 'Cancel', and 'Apply' buttons are visible on the right side of the window.

FastTrack

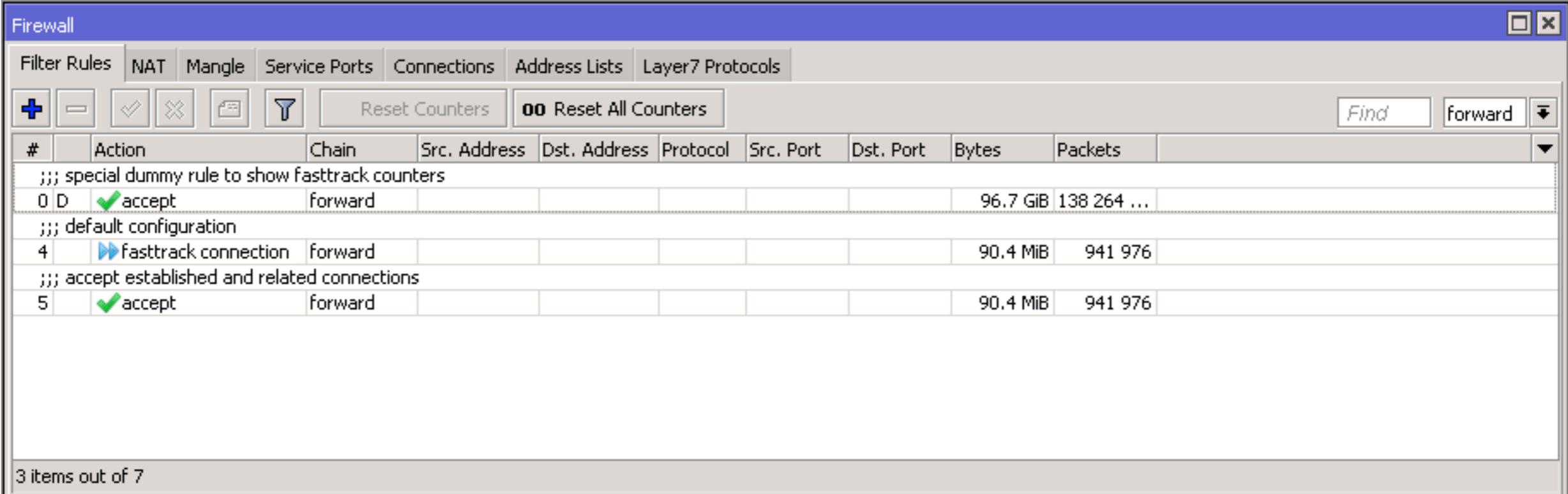
- FastPath + Connection tracking;
- Suporte a TCP e UDP;
- Conexões NATeadas também podem usar o FastTrack;
- Também possui uma lista de hardware compatível, bem como o FastPath:
 - https://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack#Supported_hardware

FastTrack

- Condições para habilitar o FastTrack:
 - Sem configuração de mesh e metarouter;
 - Sniffer, torch e traffic-generator não estão em uso;
 - Mac-scan e IP-scan não estão em uso.

FastTrack

- Para habilitar o FastTrack, as conexões precisam ser marcadas no firewall com a **ação** “fasttrack-connection”;



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active, and the 'forward' chain is selected. The table below shows the configuration of three filter rules. Rule 0 is a dummy rule for fasttrack counters, rule 4 is the 'fasttrack connection' rule, and rule 5 is a rule to accept established and related connections.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	Bytes	Packets
;;; special dummy rule to show fasttrack counters									
0	D ✓ accept	forward						96.7 GiB	138 264 ...
;;; default configuration									
4	▶▶ fasttrack connection	forward						90.4 MiB	941 976
;;; accept established and related connections									
5	✓ accept	forward						90.4 MiB	941 976

3 items out of 7

FastTrack

- A configuração inicial (e de fábrica) é a seguinte:
 - *lip firewall filter add chain=forward action=**fasttrack-connection** connection-state=**established,related***
 - *lip firewall filter add chain=forward action=accept connection-state=**established,related***

FastTrack

- Porém, pode ser modificada de acordo com a necessidade:
- *lip firewall filter add chain=forward action=fasttrack-connection **in-interface-list=LAN** connection-state=established,related*
- *lip firewall filter add chain=forward action=accept connection-state=established,related*

FastTrack

Without	With
360Mbps	890Mbps
CPU 100%	CPU 86%
44% CPU on firewall	6% CPU on firewall

* tested on RB2011 with single TCP stream

FastTrack



- Pacotes marcados na FastTrack são **ignorados** por:
 - Firewall;
 - Connection Tracking;
 - **Simple queues** and queue tree com parent=global;
 - IP accounting, e outros: <https://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack#Description>

Nv2

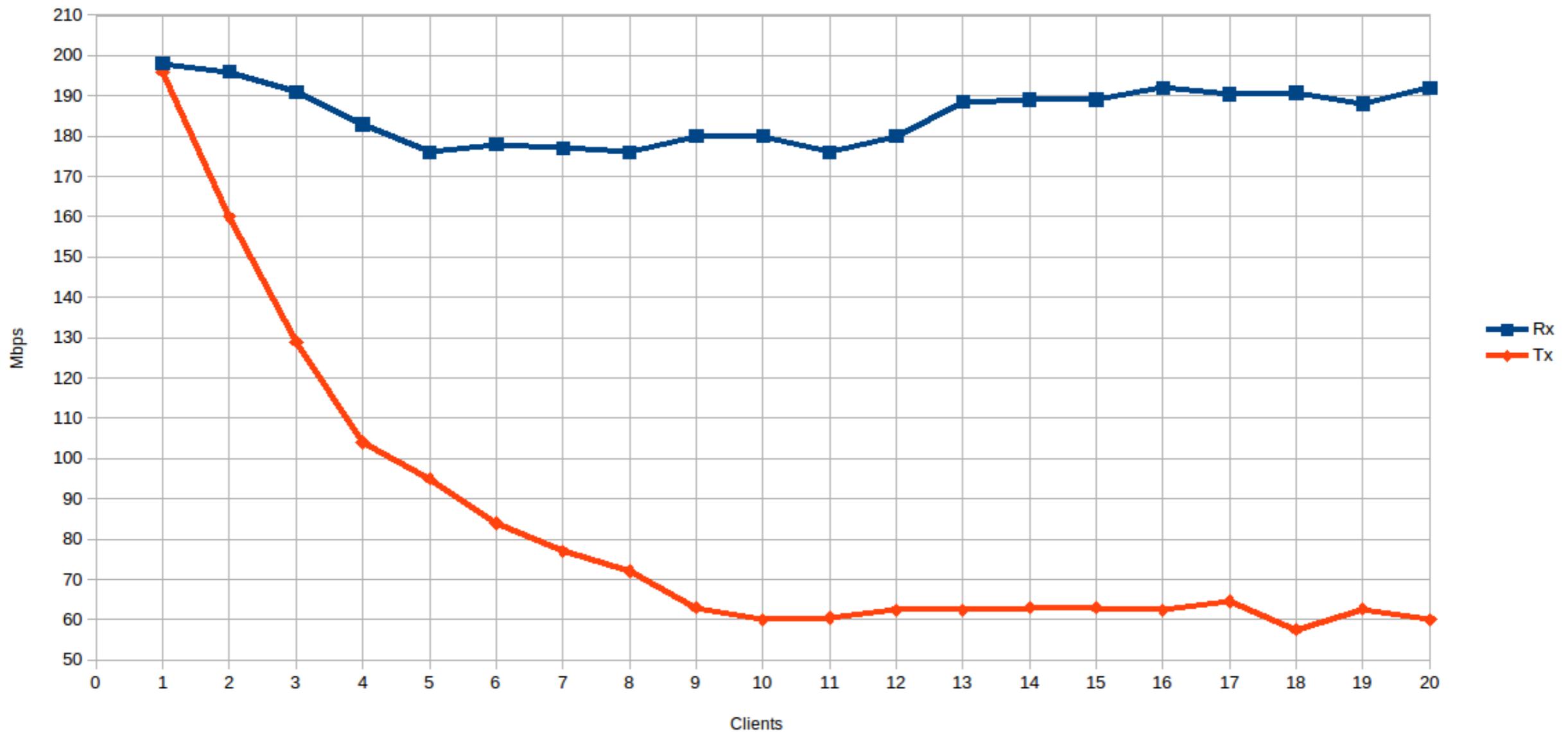
- Protocolo wireless - proprietário MikroTik;
- Baseado em TDMA;
- Resolve o problema do nó oculto (802.11);
- Melhora o throughput e a latência, especialmente em redes multi-ponto (ptmp).

Nv2 - Melhorias

- A partir da versão 6.42, há melhorias consideráveis no protocolo Nv2, baseado no ambiente multi ponto (ptmp);
- Modulação individual do Time-slot de cada cliente;
- Clientes “ruins” não afetarão a célula como um todo.

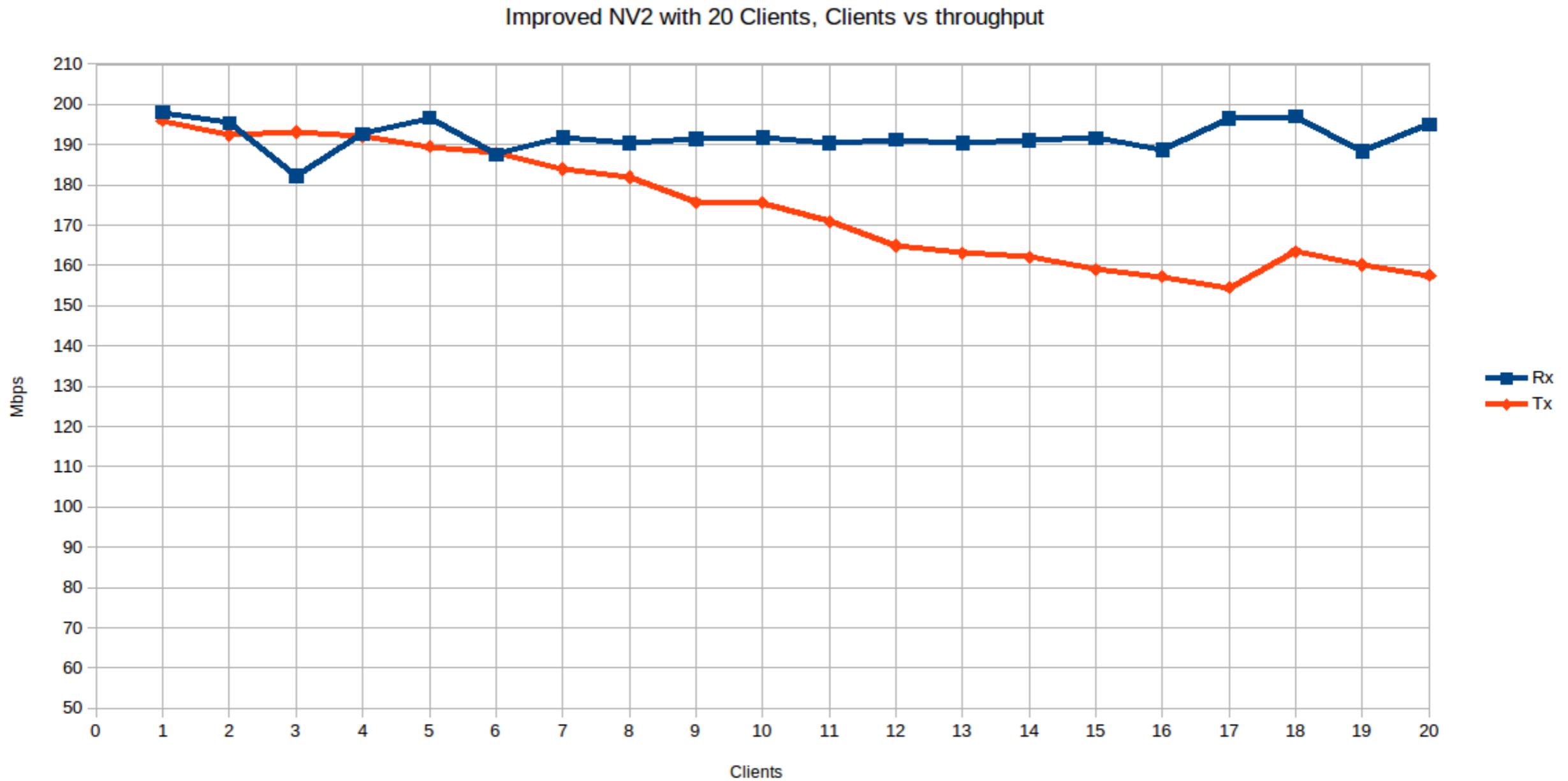
Nv2 - Melhorias

NV2 with 20 Clients, Clients vs throughput



<http://forum.mikrotik.com>

Nv2 - Melhorias



<http://forum.mikrotik.com>

Bridge e Switching

- Bridge: L2 controlado por software;
- Switching: L2 controlado pelo switch chip;
- Antes da versão 6.41: switching através do parâmetro “master-port”;
- A partir da versão 6.41: switching **incorporado** no menu “Bridge”, através da funcionalidade de **“hardware-offloading”**;

Bridge e Switching

The screenshot displays a network configuration window titled "Bridge". It features a tabbed interface with "Ports" selected. A table lists 17 bridge ports, with "sfp-sfpplus1" selected. A secondary window, "Bridge Port <sfp-sfpplus1>", is open, showing configuration options for the selected port. The "General" tab is active, showing fields for "Interface" (sfp-sfpplus1) and "Bridge" (bridge1). Below these are fields for "Horizon" and "Learn" (set to auto). Three checkboxes are checked: "Unknown Unicast Flood", "Unknown Multicast Flood", and "Broadcast Flood". A fourth checkbox, "Hardware Offload", is also checked and highlighted by an arrow. The bottom status bar shows "enabled", "inactive", and "Hw. Offload".

#	Interface	Bridge
0	H sfp-sfpplus1	bridge1
1	H sfp-sfpplus2	bridge1
2	H sfp-sfpplus3	bridge1
3	IH sfp-sfpplus4	bridge1
4	IH sfp-sfpplus5	bridge1
5	IH sfp-sfpplus6	bridge1
6	IH sfp-sfpplus7	bridge1
7	IH sfp-sfpplus8	bridge1
8	IH sfp-sfpplus9	bridge1
9	IH sfp-sfpplus10	bridge1
10	IH sfp-sfpplus11	bridge1
11	IH sfp-sfpplus12	bridge1
12	IH sfp-sfpplus13	bridge1
13	IH sfp-sfpplus14	bridge1
14	IH sfp-sfpplus15	bridge1
15	H sfp-sfpplus16	bridge1
16	H ether1	bridge1

Bridge Port <sfp-sfpplus1>

General STP VLAN Status

Interface: sfp-sfpplus1

Bridge: bridge1

Horizon:

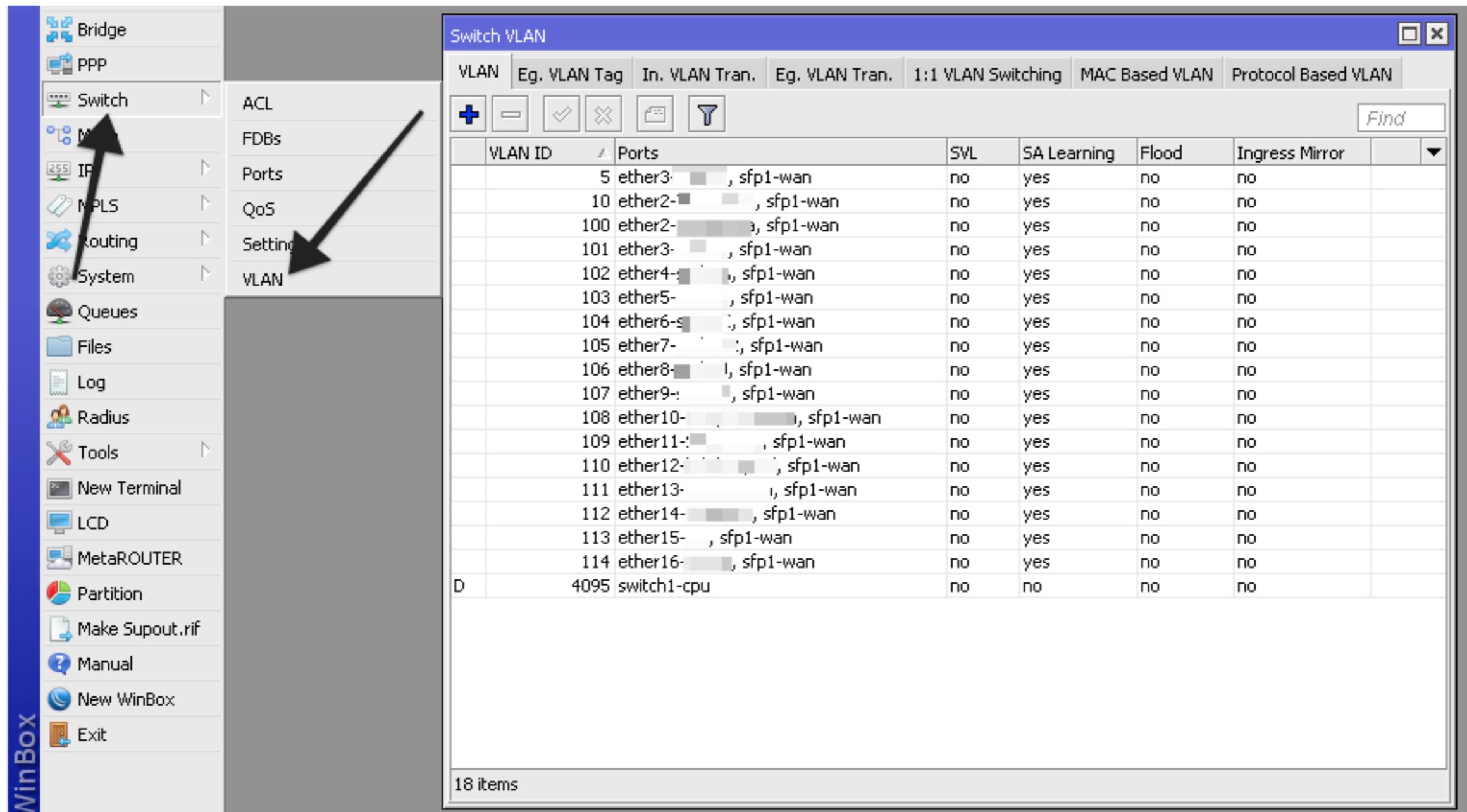
Learn: auto

- Unknown Unicast Flood
- Unknown Multicast Flood
- Broadcast Flood
- Hardware Offload

17 items (1 selected) enabled inactive Hw. Offload

Bridge e Switching

- Anterior à versão 6.41:



The screenshot shows the WinBox interface with the 'Switch' menu item selected in the left sidebar. The 'VLAN' sub-menu is open, and the 'Switch VLAN' configuration window is displayed. The window shows a table of VLAN configurations with columns for VLAN ID, Ports, SVL, SA Learning, Flood, and Ingress Mirror. The table contains 18 items, including VLANs 5 through 114 and a CPU VLAN 4095.

VLAN ID	Ports	SVL	SA Learning	Flood	Ingress Mirror
5	ether3- , sfp1-wan	no	yes	no	no
10	ether2- , sfp1-wan	no	yes	no	no
100	ether2- , sfp1-wan	no	yes	no	no
101	ether3- , sfp1-wan	no	yes	no	no
102	ether4- , sfp1-wan	no	yes	no	no
103	ether5- , sfp1-wan	no	yes	no	no
104	ether6- , sfp1-wan	no	yes	no	no
105	ether7- , sfp1-wan	no	yes	no	no
106	ether8- , sfp1-wan	no	yes	no	no
107	ether9- , sfp1-wan	no	yes	no	no
108	ether10- , sfp1-wan	no	yes	no	no
109	ether11- , sfp1-wan	no	yes	no	no
110	ether12- , sfp1-wan	no	yes	no	no
111	ether13- , sfp1-wan	no	yes	no	no
112	ether14- , sfp1-wan	no	yes	no	no
113	ether15- , sfp1-wan	no	yes	no	no
114	ether16- , sfp1-wan	no	yes	no	no
4095	switch1-cpu	no	no	no	no

Bridge e Switching

- Igual ou posterior a versão 6.41:

Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	500	sfp1	ether1-
bridge1	501	sfp1	ether2-
bridge1	502	sfp1	ether3-
bridge1	503	sfp1	ether4-
bridge1	504	sfp1	ether5-
bridge1	505	sfp1	ether6-
bridge1	506	sfp1	ether7-
bridge1	507	sfp1	ether8-
bridge1	508	sfp1	ether9-
bridge1	509	sfp1	ether10-
D bridge1	1		bridge1, sfp1

Filtro de conteúdo

- Muito procurado;
- Resultados mais relevantes em sites de busca sugerem o uso de L7;
- Uso de L7 é por vezes configurado de forma incorreta e ocasiona outros problemas;
- Bloqueio de conteúdo não traz o resultado esperado, se configurado incorretamente.

Filtro de conteúdo



bloquear facebook mikrotik



bloquear facebook mikrotik **2017**

bloquear facebook mikrotik **layer7**

bloquear facebook mikrotik **https**

bloquear facebook mikrotik

bloquear facebook mikrotik **por ip**

bloquear facebook mikrotik **web proxy**

bloquear facebook mikrotik **2015**

bloquear facebook mikrotik **rb750**

bloquear facebook mikrotik **750**

bloquear facebook mikrotik **content**

Pesquisa Google

Estou com sorte

[Denunciar previsões inadequadas](#)

Filtro de conteúdo

- Alternativas:
 - TLS-Host
 - Kid-control

TLS-Host

- Introduzido **funcionalmente** na versão 6.41.2 do RouterOS;
- Capaz de identificar o tráfego HTTPS;
- Aceita sintaxe GLOB, que permite o uso de *;
 - Exemplo: *.facebook.com.br

TLS-Host

/ip firewall filter

```
add chain=forward dst-port=443 protocol=tcp  
tls-host=*.facebook.com action=reject
```

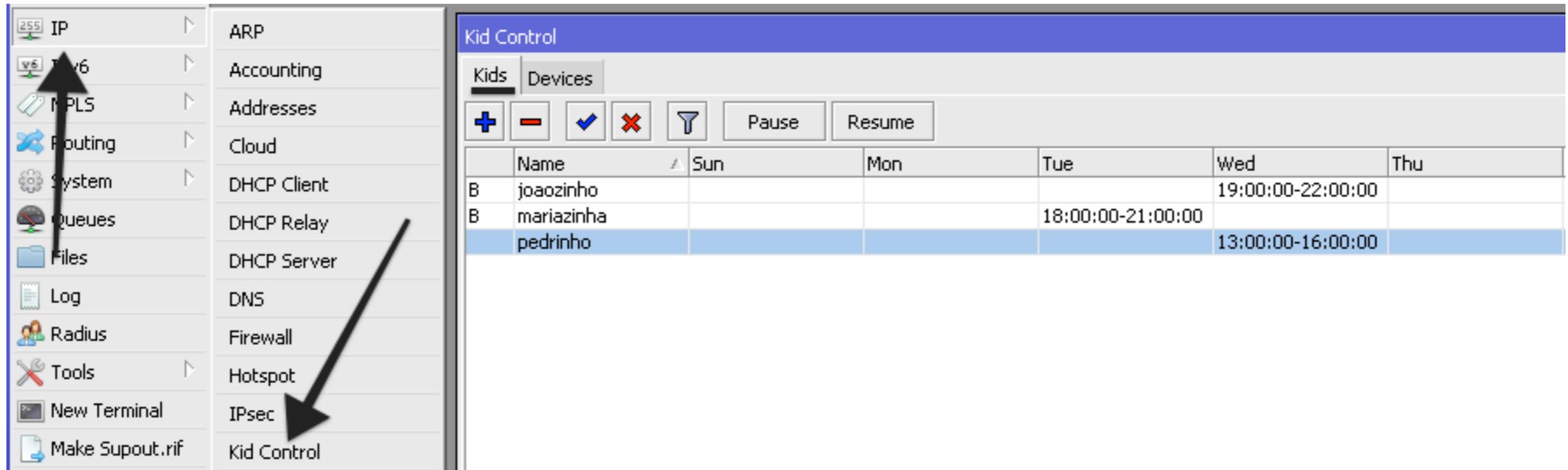
```
add chain=forward dst-port=443 protocol=tcp  
tls-host=*.youtube.com action=reject
```

❖ **Lembrar do FastTrack**

Kid Control

- Introduzido na versão 6.41 do RouterOS;
- Fornece controle parental para limitar a conectividade à Internet para crianças (e até mesmo adultos, rsrs...);
- Melhorias e novas funcionalidades serão adicionadas em versões futuras.

Kid Control

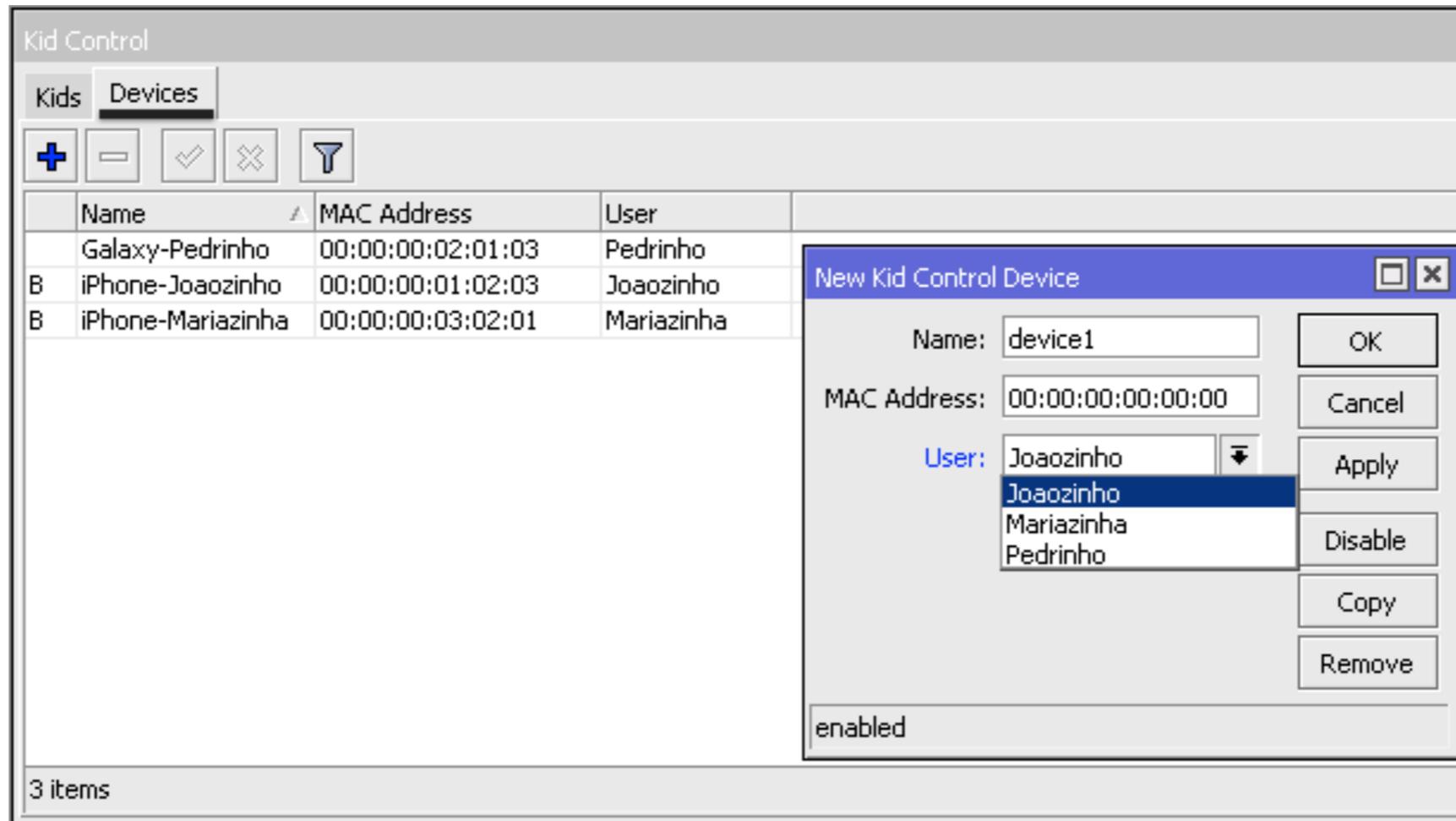


The screenshot displays the Mikrotik WinBox interface for configuring Kid Control. The left sidebar shows the navigation tree with 'IPsec' and 'Kid Control' highlighted. The main window shows the 'Kid Control' configuration page with a table of kids and their blocked times.

	Name	Sun	Mon	Tue	Wed	Thu
B	joaozinho				19:00:00-22:00:00	
B	mariazinha			18:00:00-21:00:00		
	pedrinho				13:00:00-16:00:00	

- Kids - Define as “crianças”;
- B - Blocked.

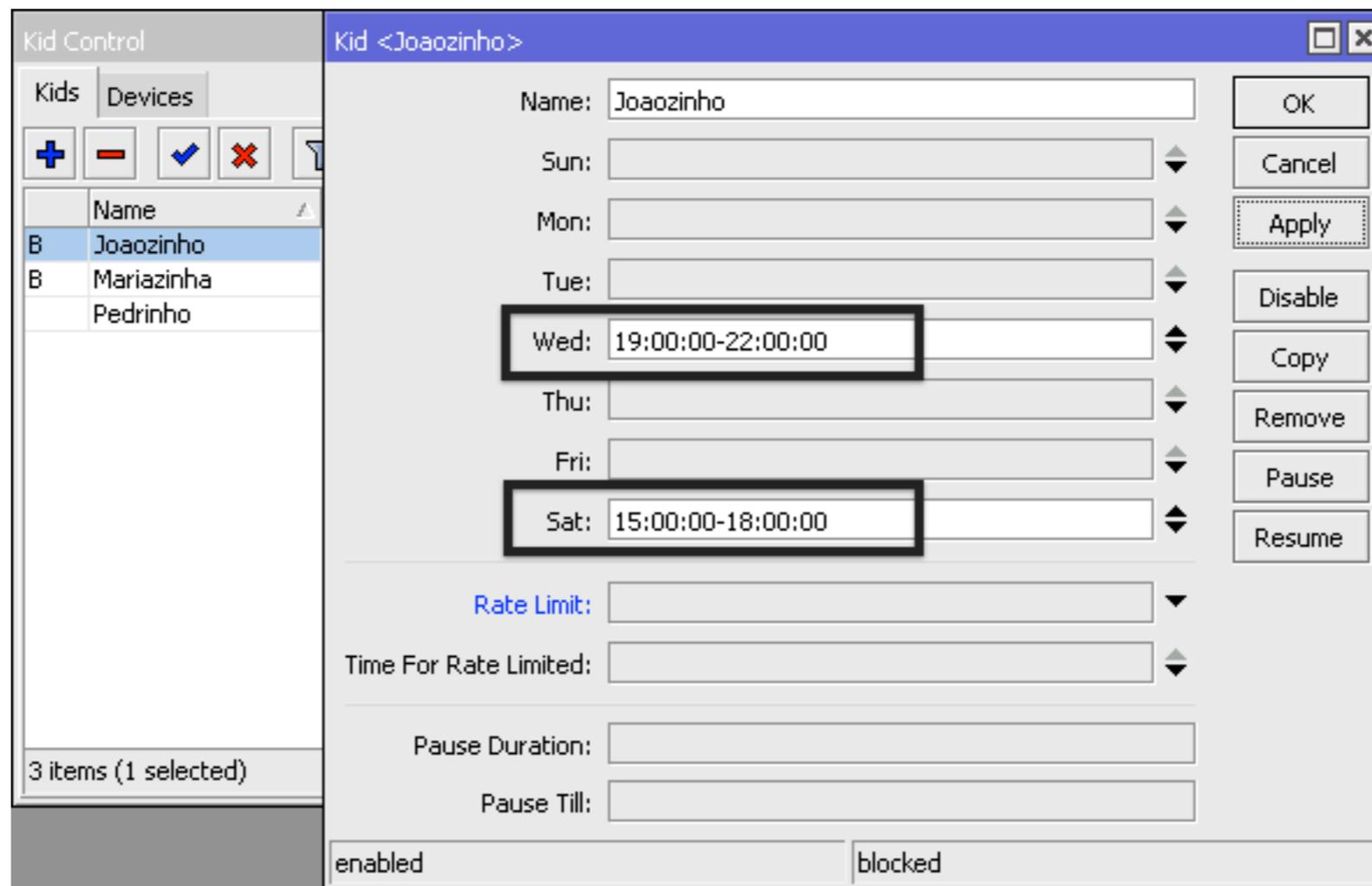
Kid Control



- **Devices** - Define os dispositivos atrelados a cada criança.

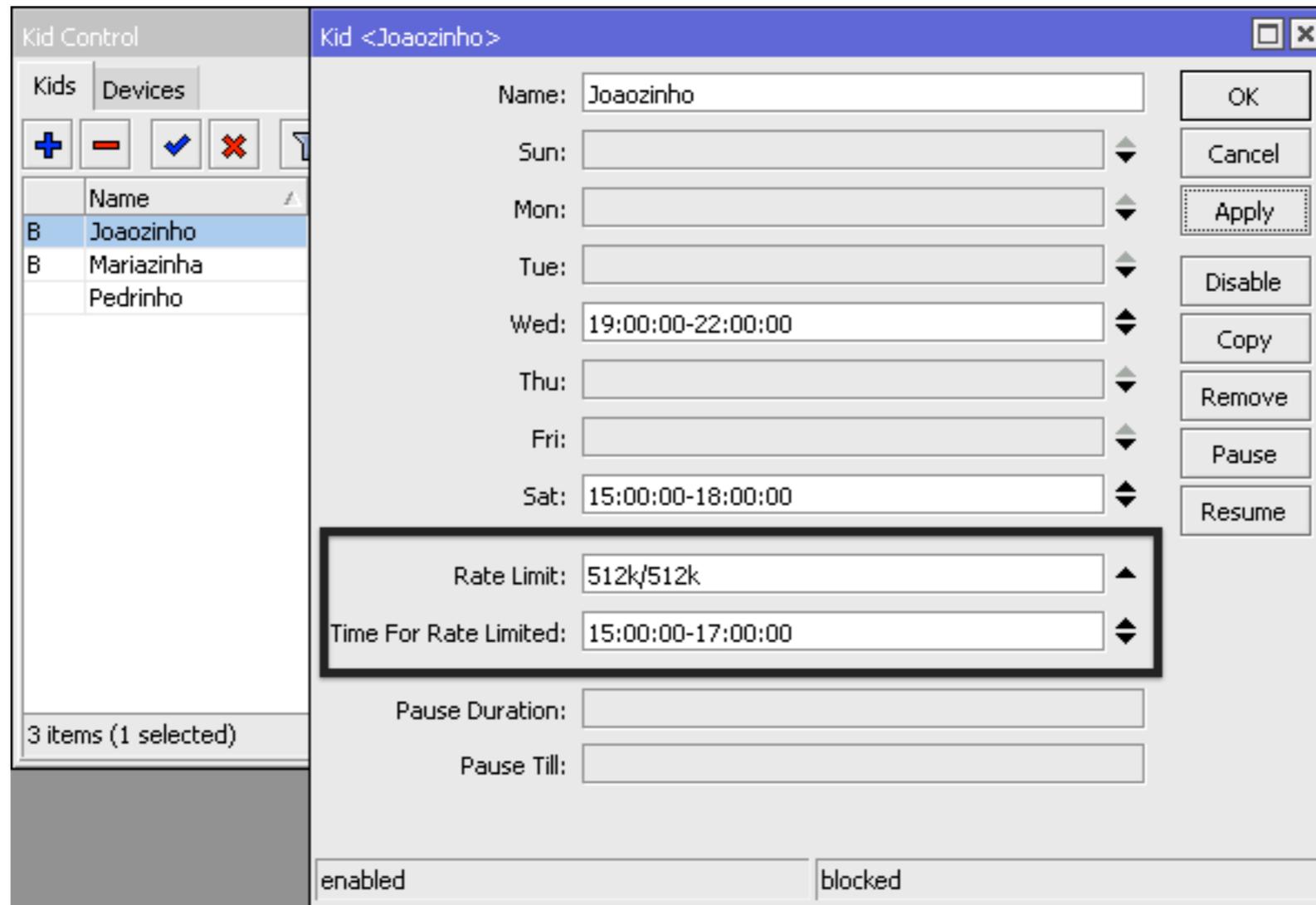
Kid Control

- Possibilidade de escolher diferentes horários de funcionamento:



Kid Control

- Possibilidade de configurar limitação de banda e o tempo desta limitação:



Filtro de conteúdo - Dica

- Na versão 6.36 do RouterOS, foi introduzida a resolução de DNS, por meio da Address-list no firewall, auxiliando no filtro de conteúdo:

The screenshot displays the RouterOS Firewall configuration interface, specifically the 'Address Lists' tab. The main window shows a table of address lists with the following data:

Name	Address	Timeout	Creation Time
bloqueio	www.ubnt.com		May/25/2018 11:...
;;; www.ubnt.com			
D bloqueio	52.34.248.163		May/25/2018 11:...
;;; www.ubnt.com			
D bloqueio	54.68.78.110		May/25/2018 11:...
;;; www.ubnt.com			
D bloqueio	52.41.83.111		May/25/2018 11:...

A modal dialog box titled 'Firewall Address List <bloqueio>' is open, showing the configuration for a specific list. The dialog includes the following fields and buttons:

- Name: bloqueio
- Address: www.ubnt.com
- Timeout: (empty)
- Creation Time: May/25/2018 11:57:40
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: enabled

Arrows labeled '1' and '2' point to the dialog box and the main table respectively.

Segurança

- Vulnerabilidade no serviço www do RouterOS - 2017
 - Corrigida em **Março de 2017** (6.37.5 e 6.38.5);
 - Também conhecido como VPNfilter, Hajime, etc;
 - Apenas para quem não tinha firewall e a porta www estava exposta.

<https://blog.mikrotik.com/security/>

Segurança

- Vulnerabilidade no serviço Winbox - 2018
 - Corrigida em **Março de 2018** (6.40.8 e 6.42.1);
 - Afeta versões igual ou posterior a 6.29;
 - Apenas para quem não tinha firewall ou controle de acesso à porta 8291.

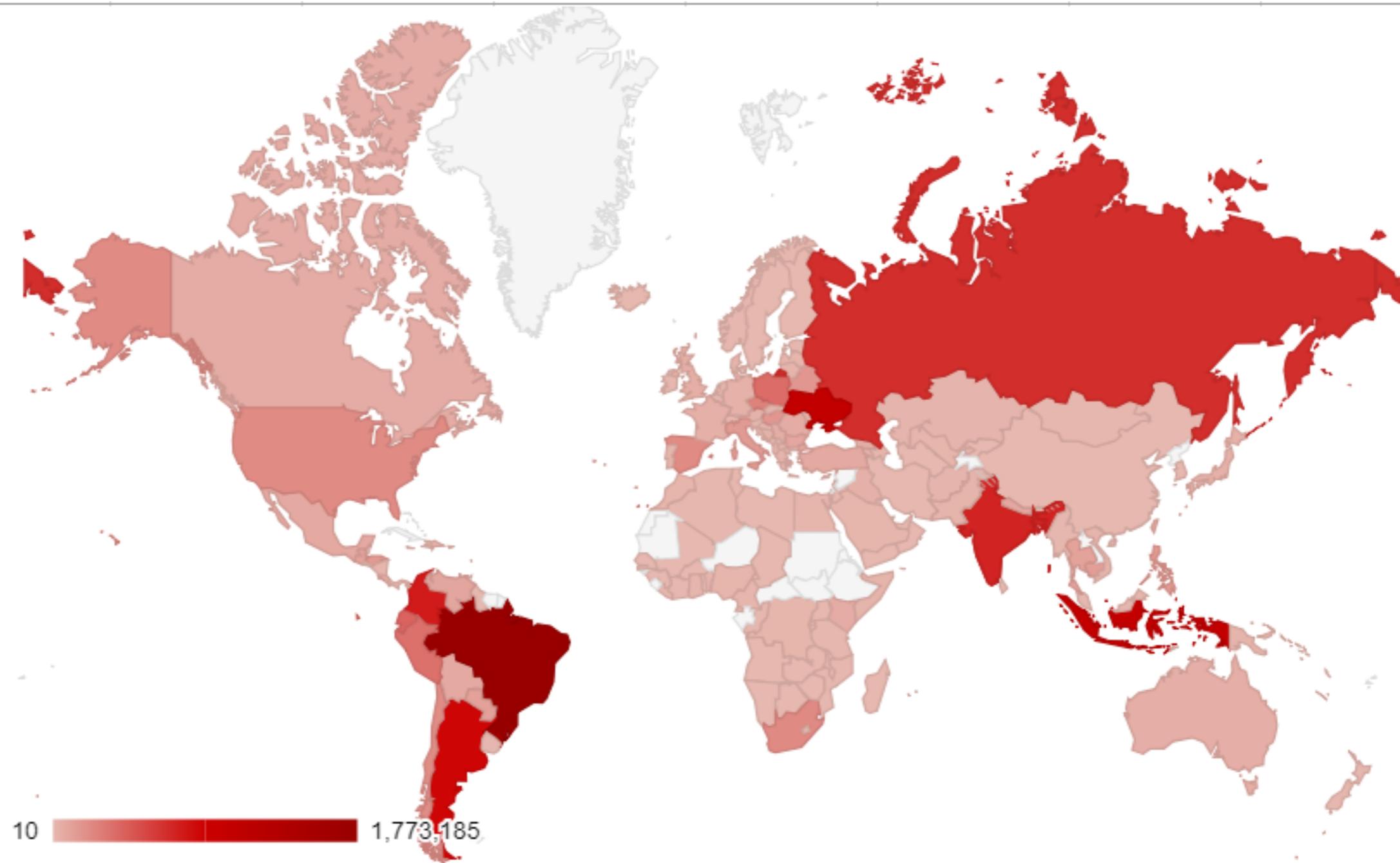
<https://blog.mikrotik.com/security/>

Segurança

- Vulnerabilidade no serviço www do RouterOS - 2018
 - Descoberta pela Tenable Inc e definidas nas CVEs: CVE-2018-1156, CVE-2018-1157, CVE-2018-1158 e CVE-2018-1159
 - Corrigida em **Agosto de 2018** (6.40.9 e 6.42.7 e 6.43);
 - Afeta apenas usuários autenticados no RouterOS;
 - Causa uso excessivo de RAM e/ou crash no serviço www.

<https://blog.mikrotik.com/security/>

Segurança



MikroTik router attacks blocked by Avast around the world

Segurança

1	Brazil	85,230
2	Poland	43,677
3	Indonesia	27,102
4	Argentina	24,255
5	Colombia	15,300
6	Turkey	15,144
7	India	11,809
8	Ukraine	11,614
9	Bangladesh	9,867
10	Venezuela	9,527

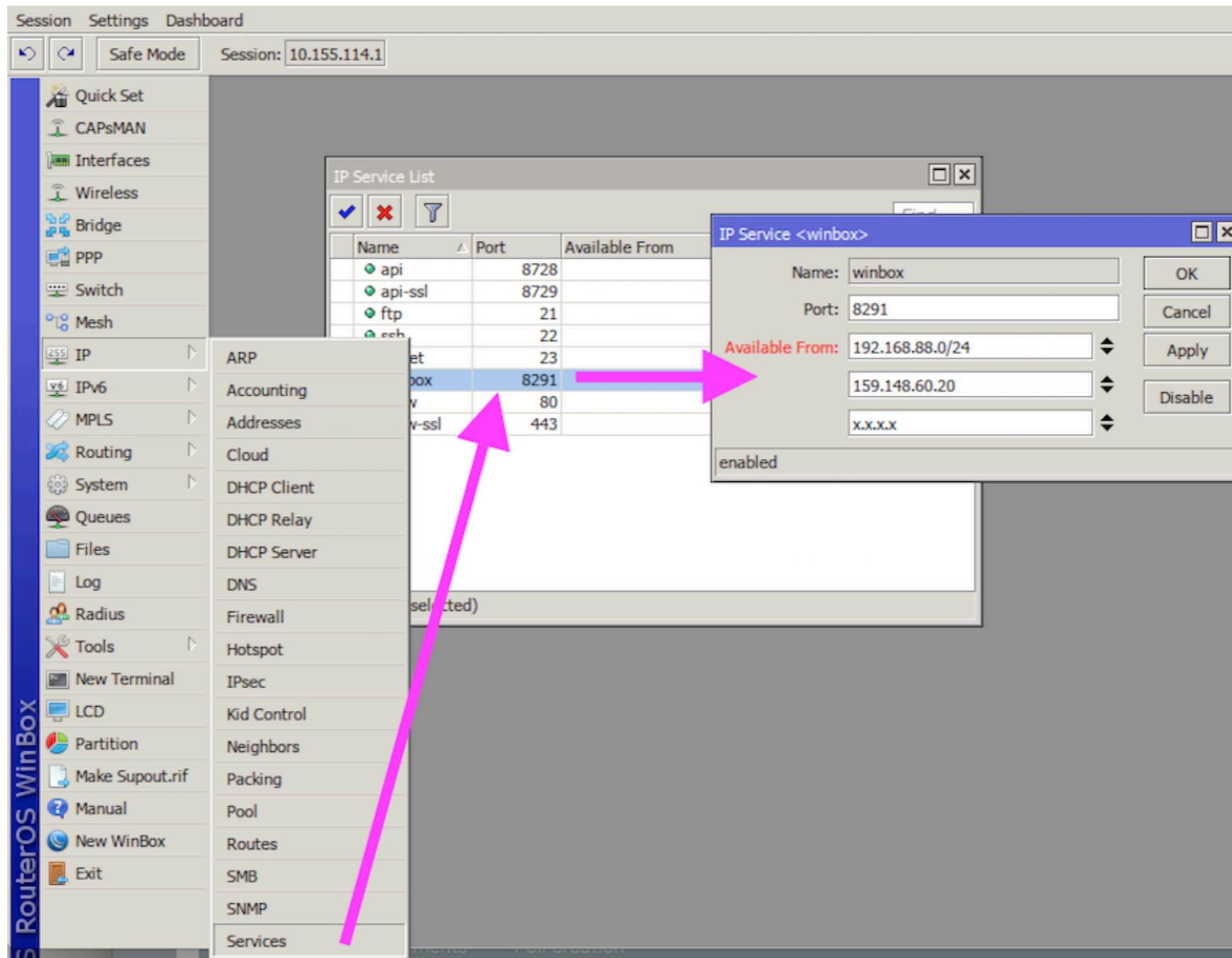
Top ten countries targeted by JS:InfectedMikroTik

Segurança

- Como garantir a proteção:
 - Usar versões atualizadas do RouterOS (já corrigidas);
 - Usar versões atualizadas do Winbox;
 - Firewall e/ou controle de acesso (IP > Services);
 - Troca de usuário/senha (e remoção do usuário admin);

<https://blog.mikrotik.com/security/>

Segurança



<https://blog.mikrotik.com/security/>

Dúvidas?

Obrigado!