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

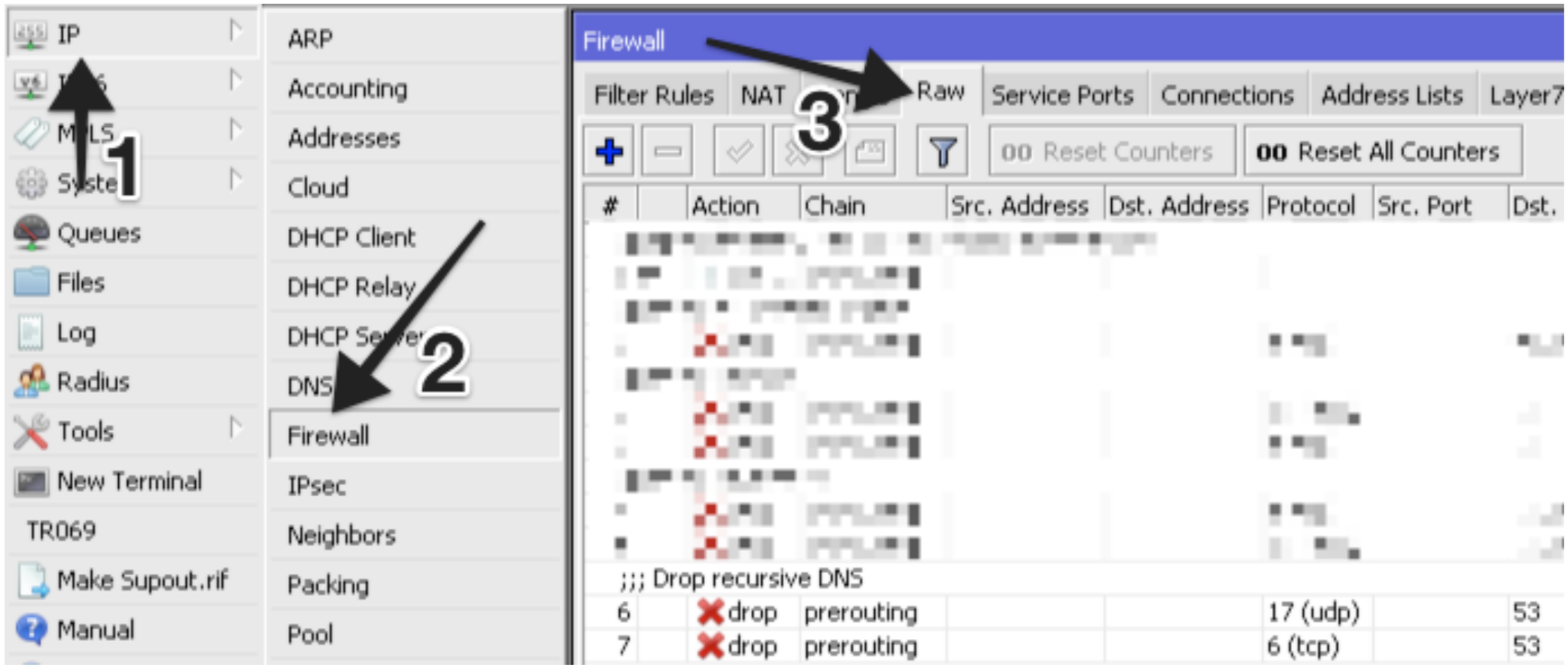


Tabela Raw - Exemplo.

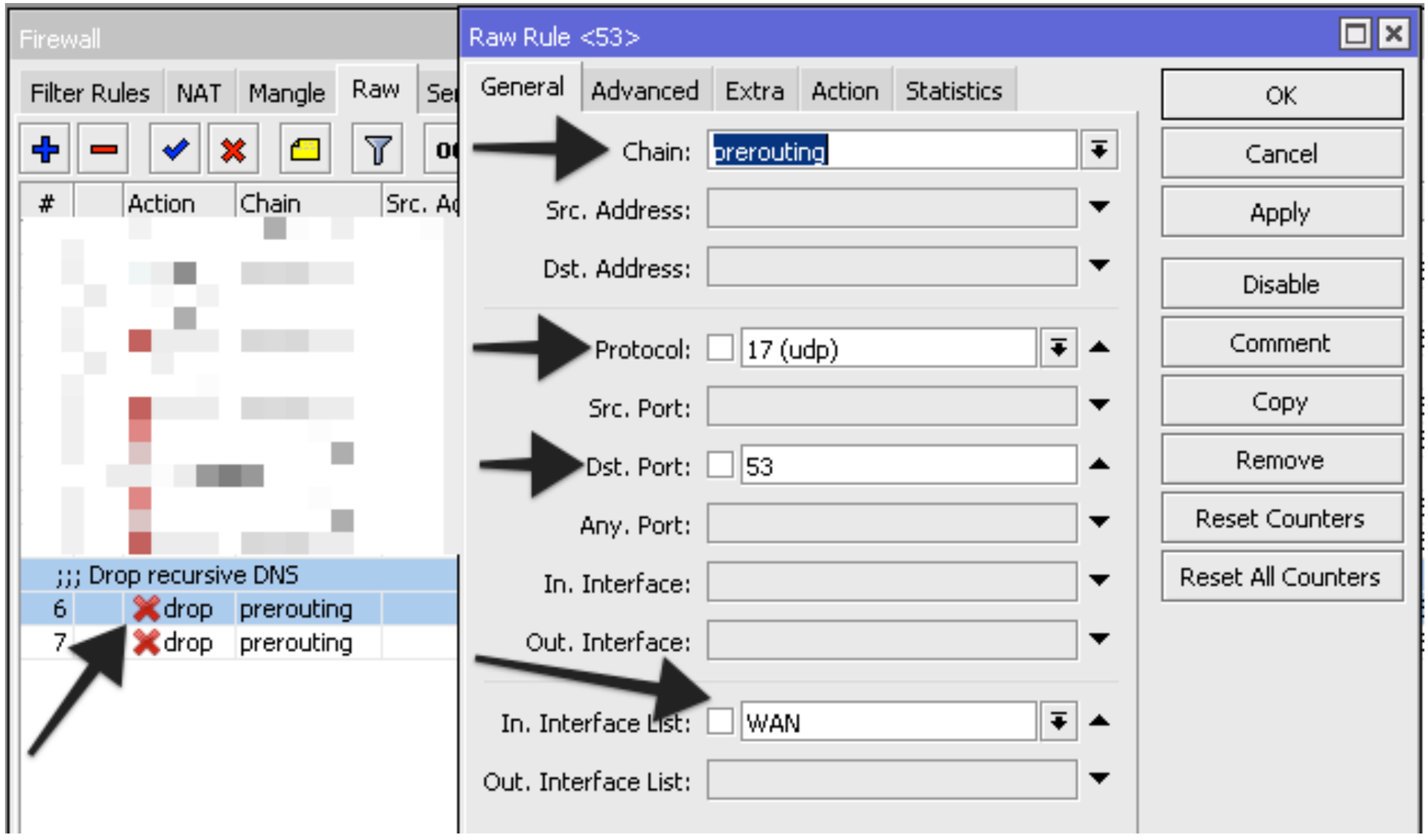
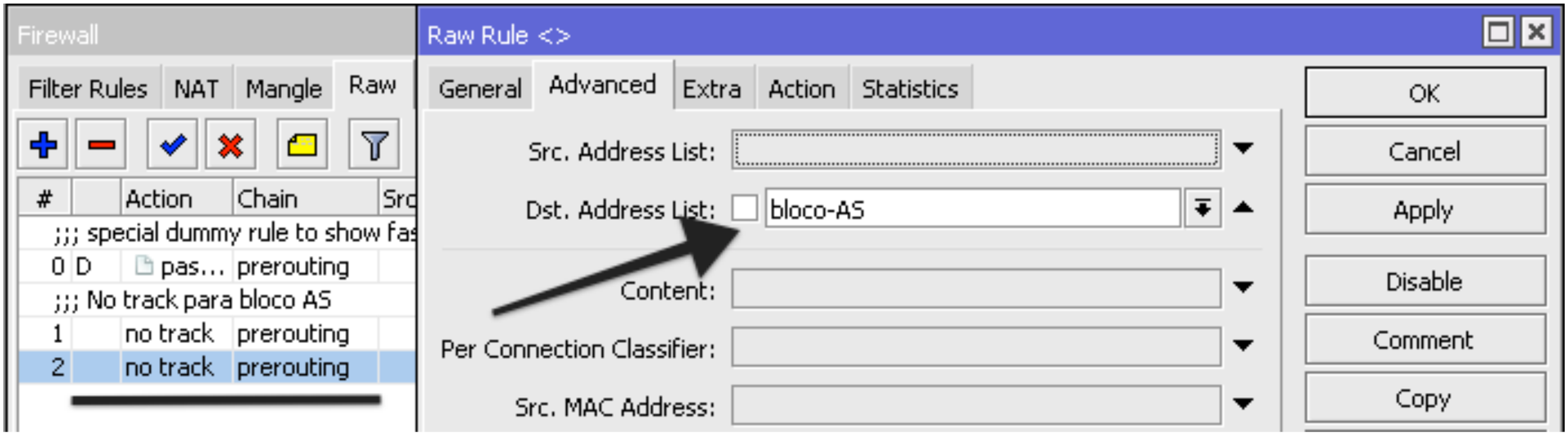


Tabela Raw - Exemplo.

- No Track para bloco AS



FastPath e FastTrack

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

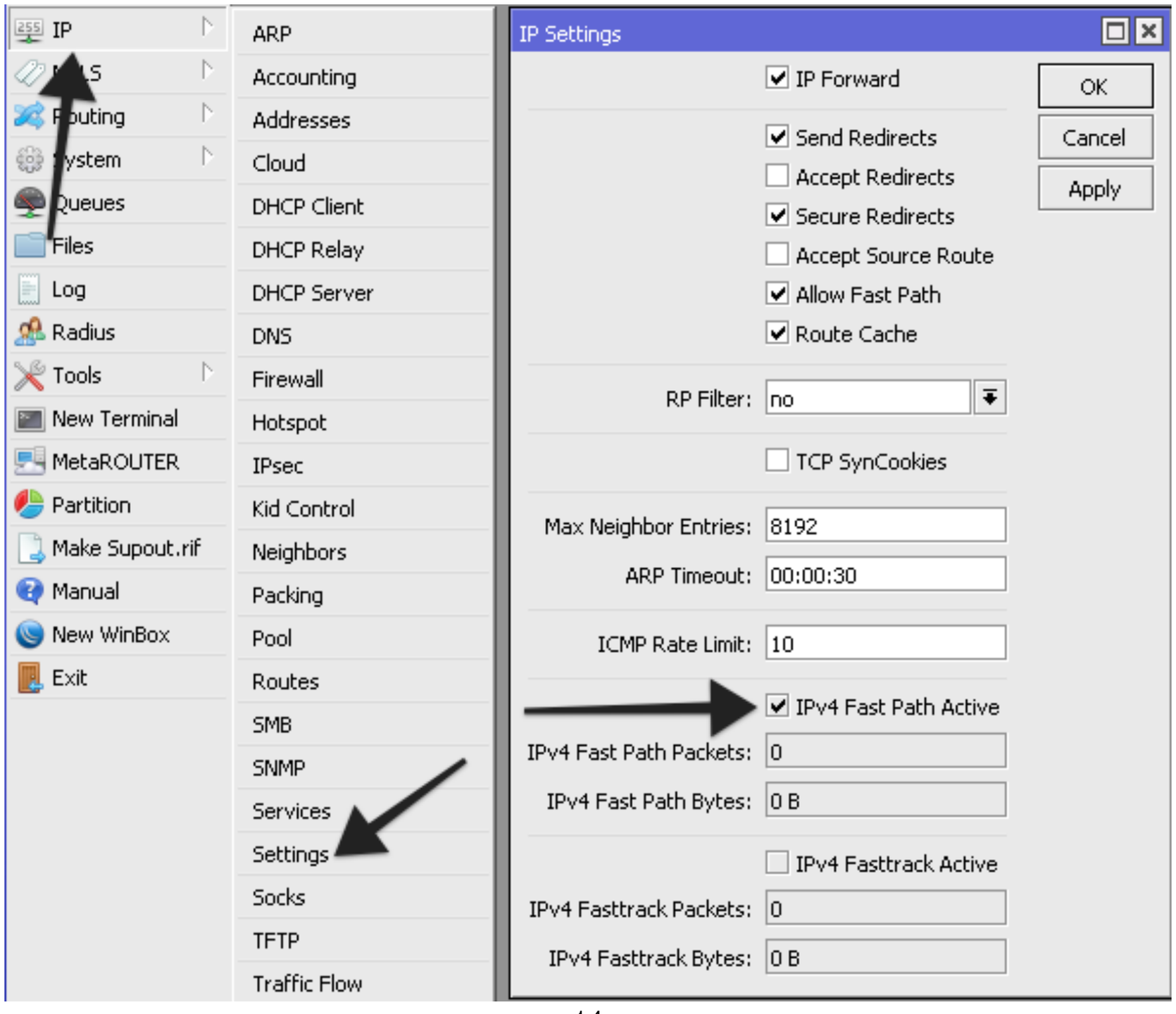
FastPath

- Suportado em todas as interfaces, na maioria dos roteadores.
    - CCR: Todas as interfaces;
    - RB1100 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


IP
ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Kid Control
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Settings
Socks
TFTP
Traffic Flow
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
IP Settings
IP Forward
Send Redirects
Accept Redirects
Secure Redirects
Accept Source Route
Allow Fast Path
Route Cache
RP Filter: no
TCP SynCookies
Max Neighbor Entries: 8192
ARP Timeout: 00:00:30
ICMP Rate Limit: 10
IPv4 Fast Path Active
IPv4 Fast Path Packets: 0
IPv4 Fast Path Bytes: 0 B
IPv4 Fasttrack Active
IPv4 Fasttrack Packets: 0
IPv4 Fasttrack Bytes: 0 B
OK
Cancel
Apply

FastTrack

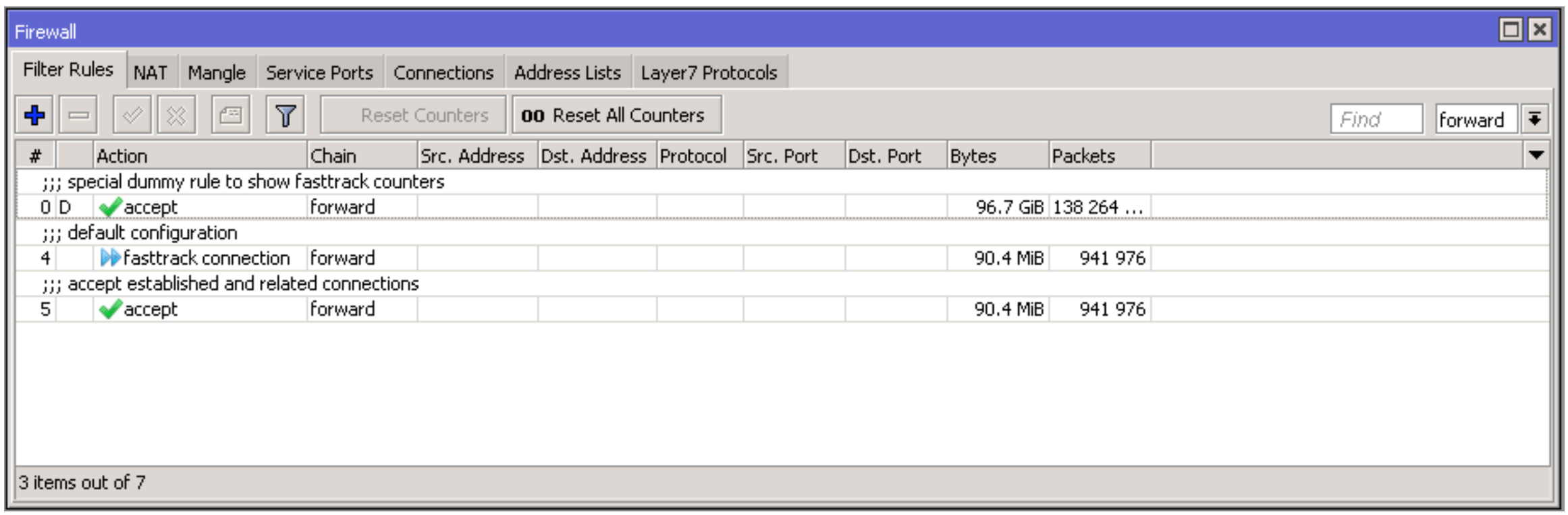
- FastPath + Connection tracking;
- Suporte a TCP e UDP;
- Conexões NATeadas também podem usar o FastTrack;
- Também possui uma lista de hardware compatível, bem como o FastPath:
    - https://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack#Supported_hardware

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”;



https://wiki.mikrotik.com

FastTrack

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

FastTrack

- Porém, pode ser modificada de acordo com a necessidade:

  - */ip firewall filter add chain=forward action=fasttrack-connection* **in-interface-list=LAN** *connection-state=established,related*

  - */ip 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

https://wiki.mikrotik.com

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).

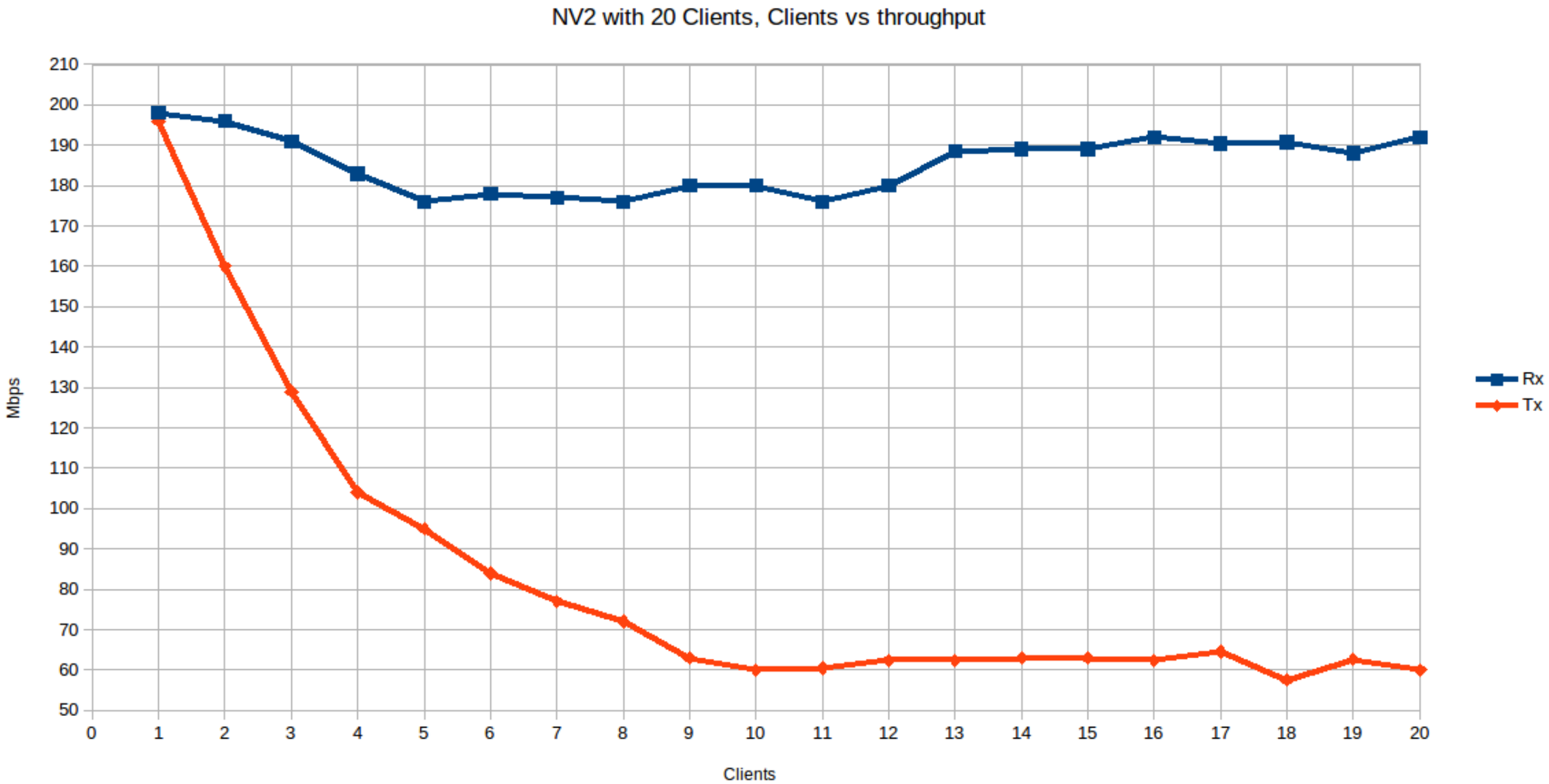
Nv2 - Melhorias

- 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;

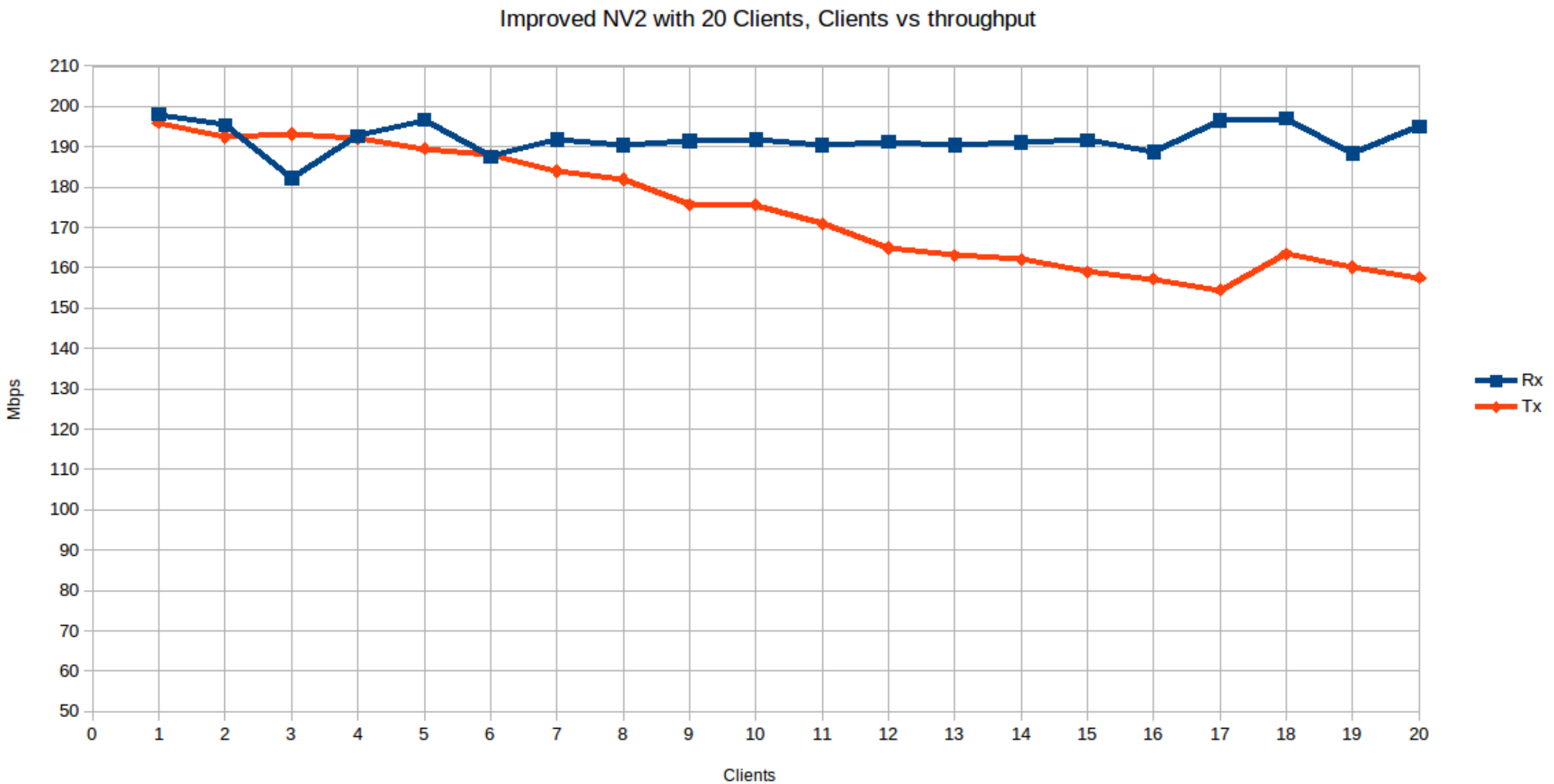
- Clientes “ruins” não afetarão a célula como um todo.

Nv2 - Melhorias



http://forum.mikrotik.com

Nv2 - Melhorias

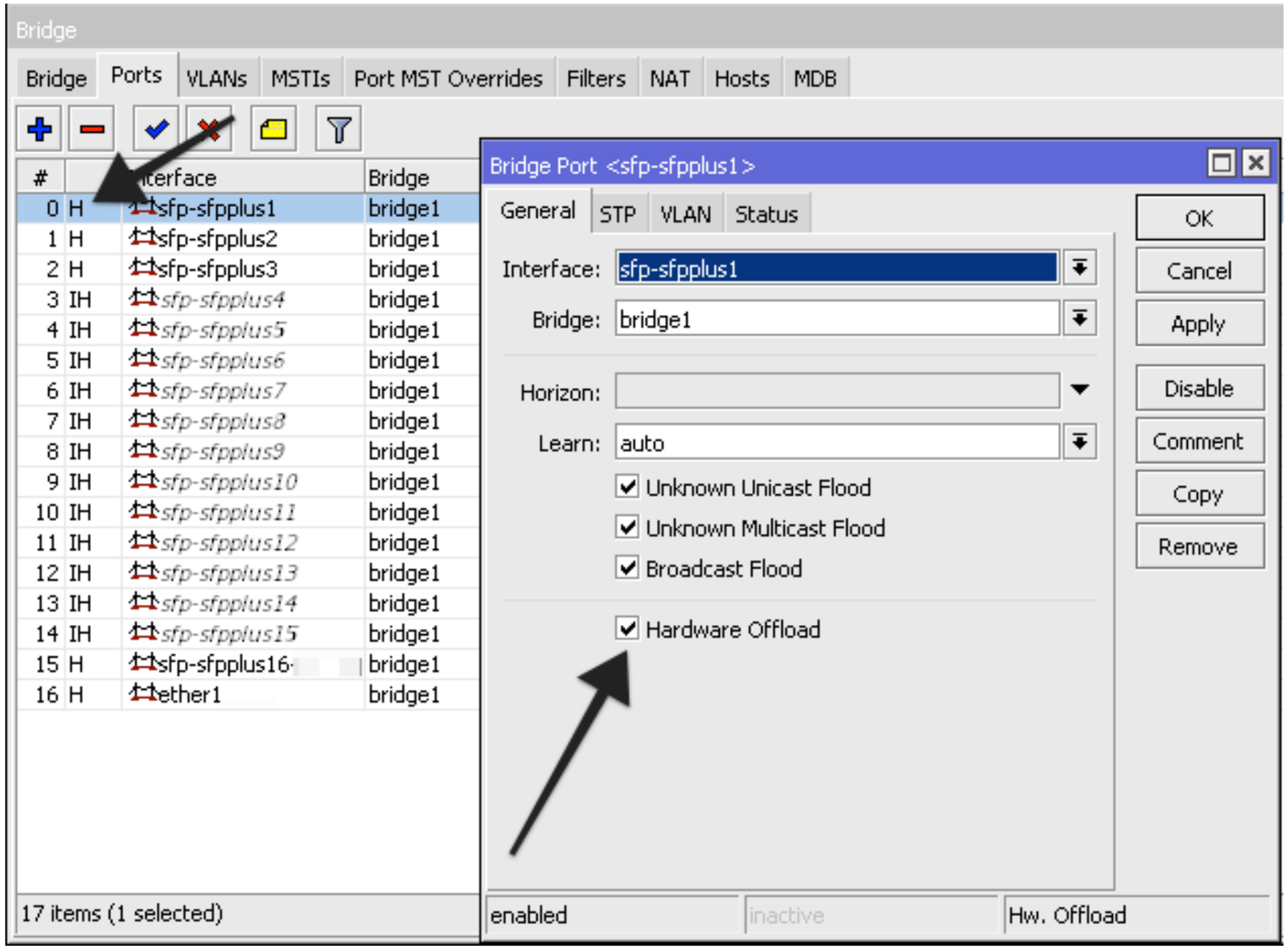


http://forum.mikrotik.com

Bridge e Switching

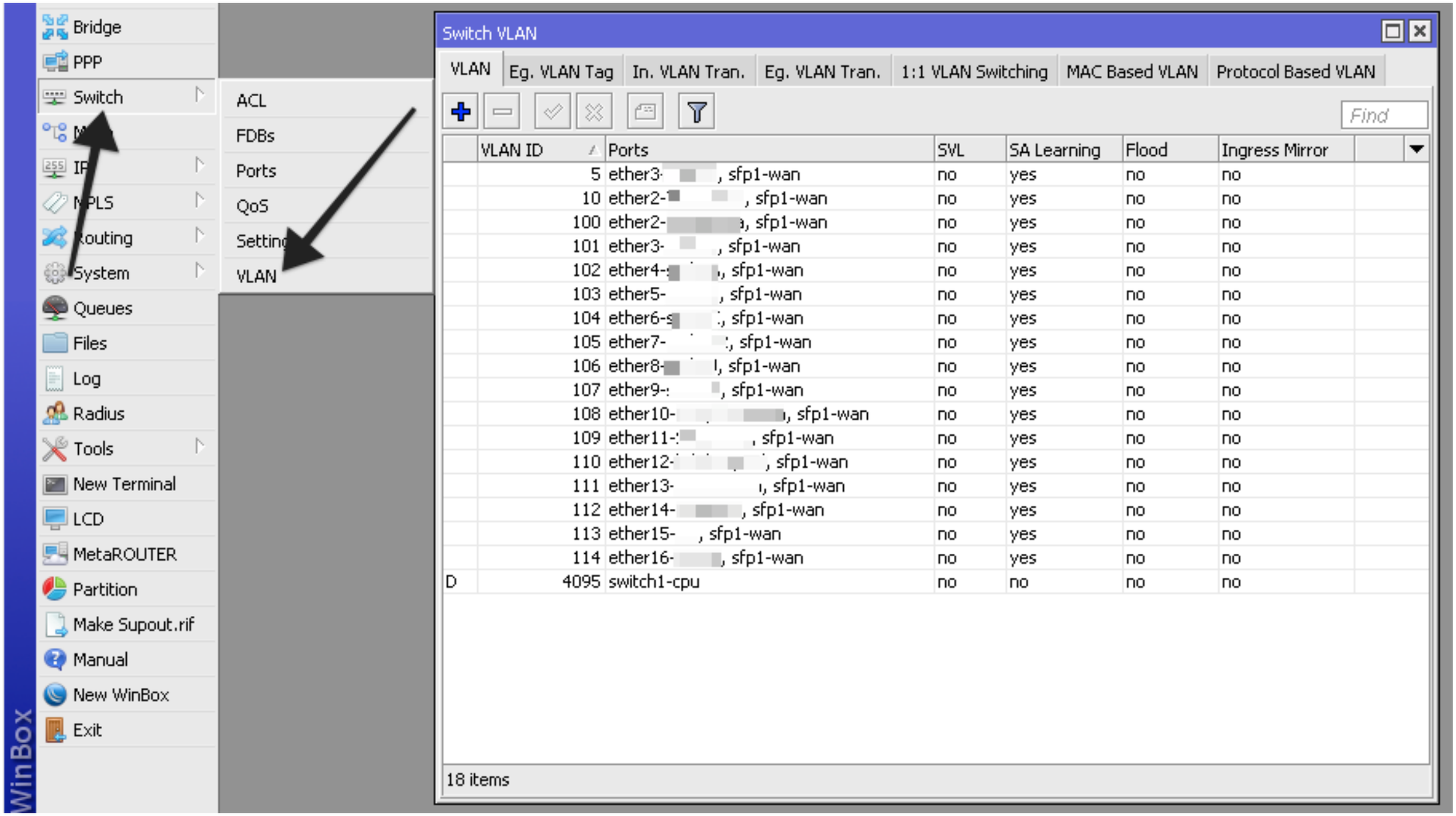
- Bridge: L2 controlado por software;
- Switching: L2 controlado pelo switch chip;
  - Antes da versão 6.41: switching através do parâmetro “master-port”;
  - A partir da versão 6.41: switching **incorporado** no menu “Bridge”, através da funcionalidade de **“hardware-offloading”;**

Bridge e Switching



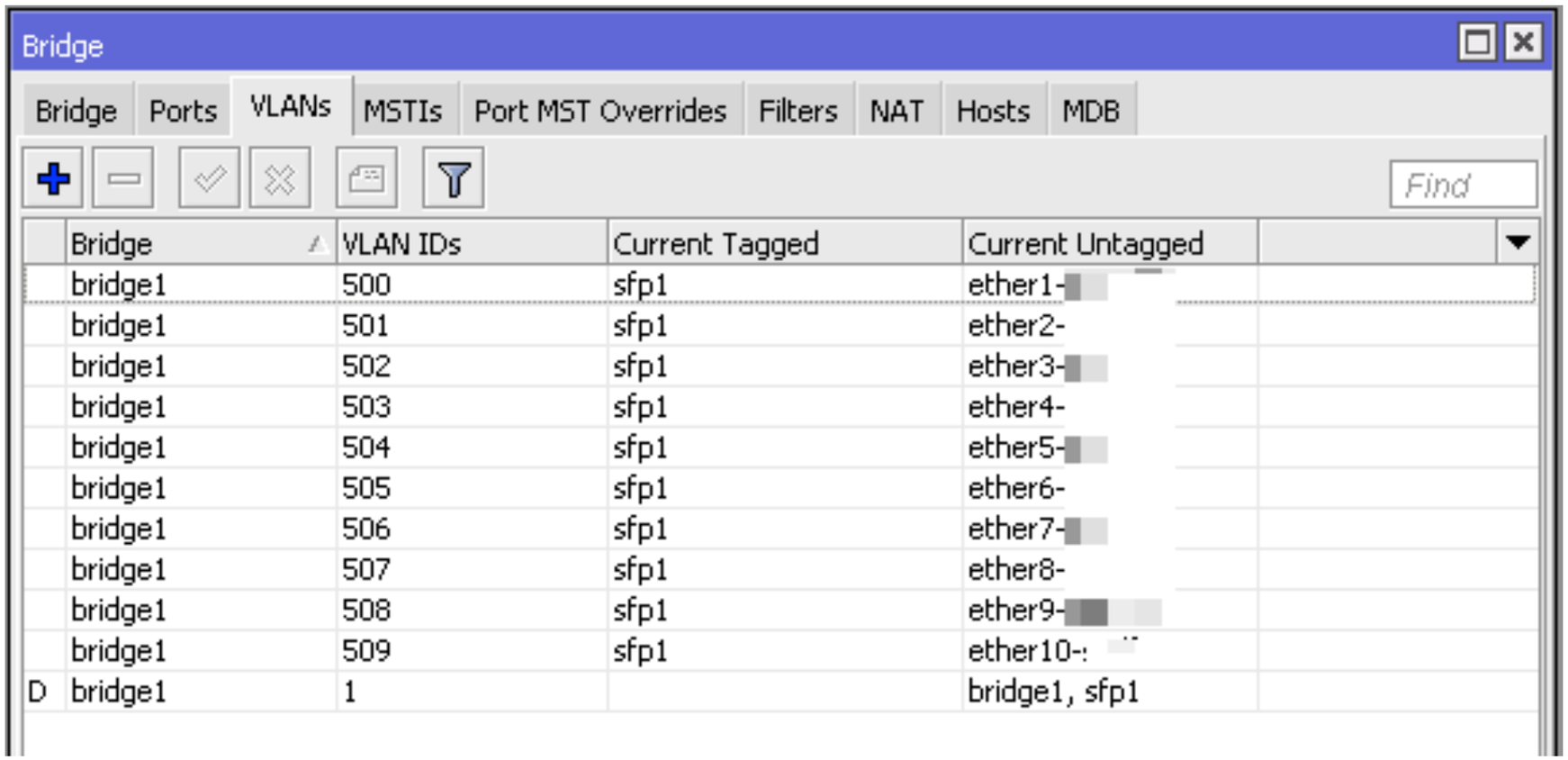
Bridge e Switching

- Anterior à versão 6.41:



Bridge e Switching

- Igual ou posterior a versão 6.41:



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



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

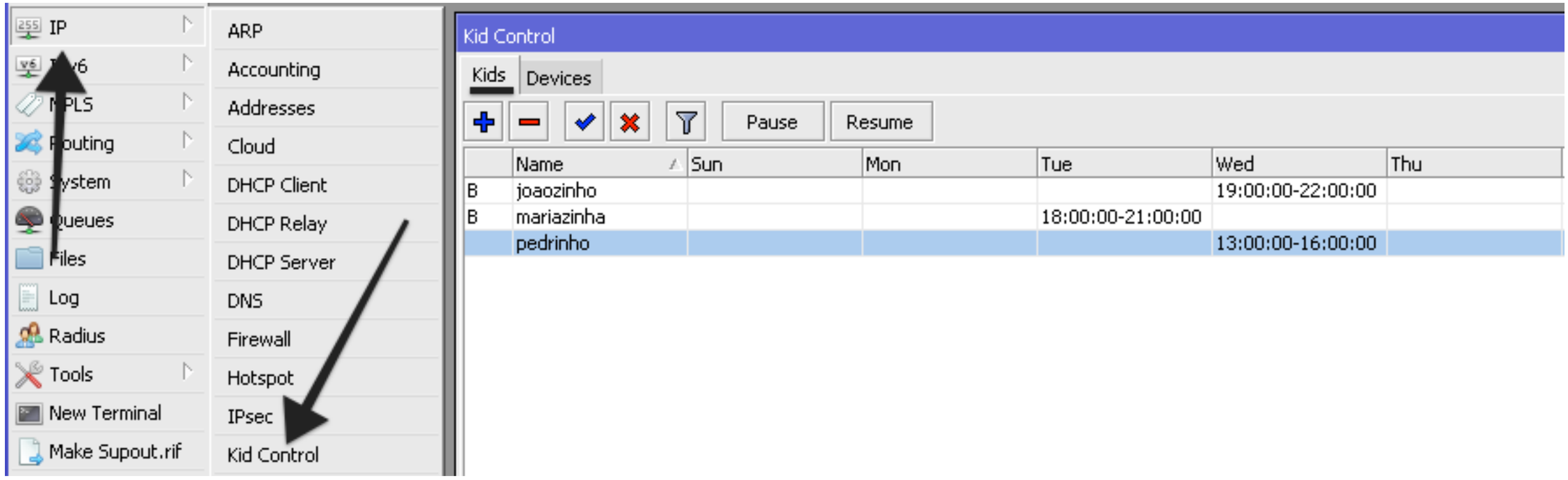
add chain=forward dst-port=443 protocol=tcp **tls-host=*.youtube.com** action=reject

✤ **Lembrar do FastTrack**

Kid Control

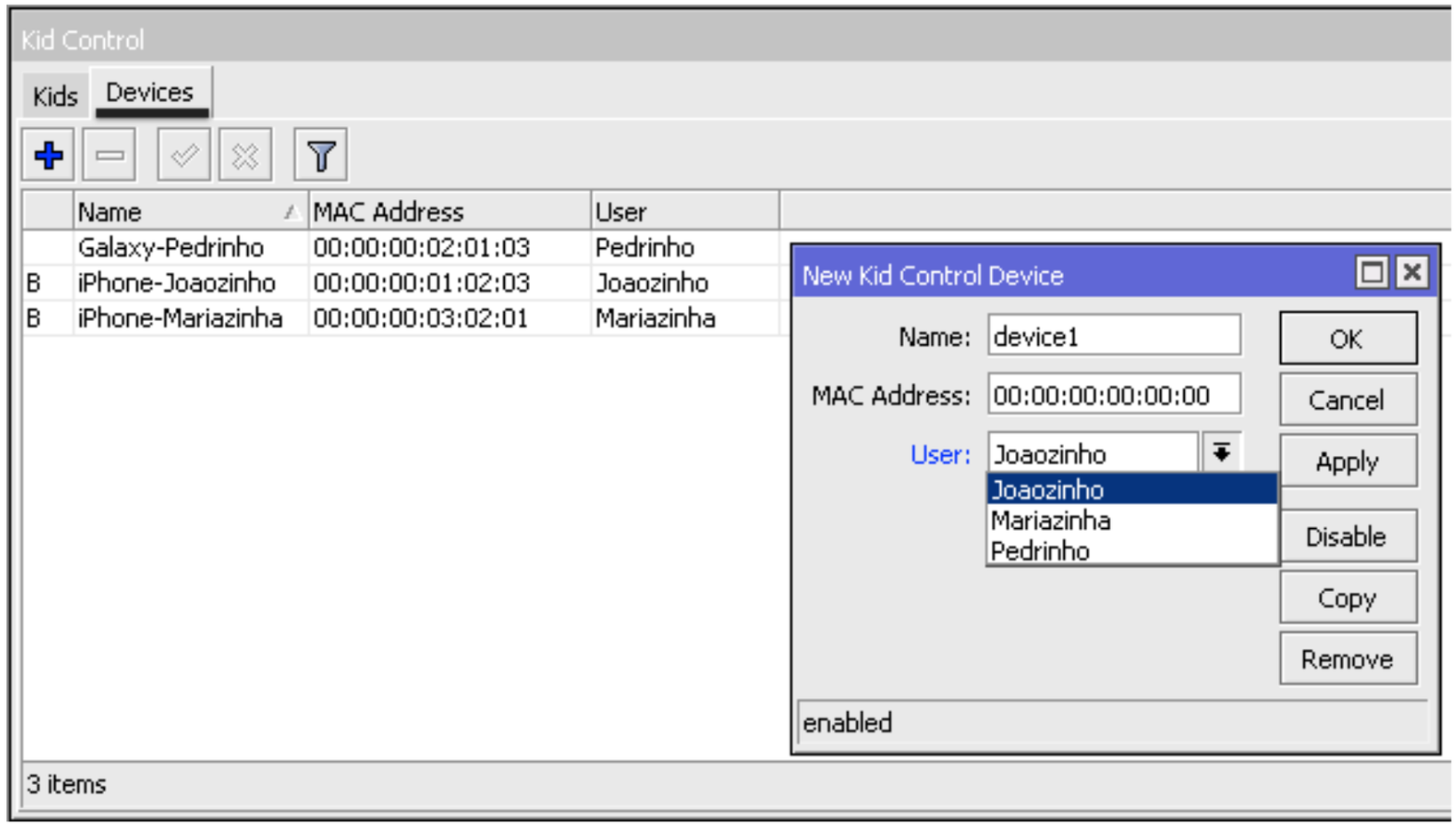
- Introduzido na versão 6.41 do RouterOS;
- Fornece controle parental para limitar a conectividade à Internet para crianças (e até mesmo adultos, rsrs…);
- Melhorias e novas funcionalidades serão adicionadas em versões futuras.

Kid Control



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

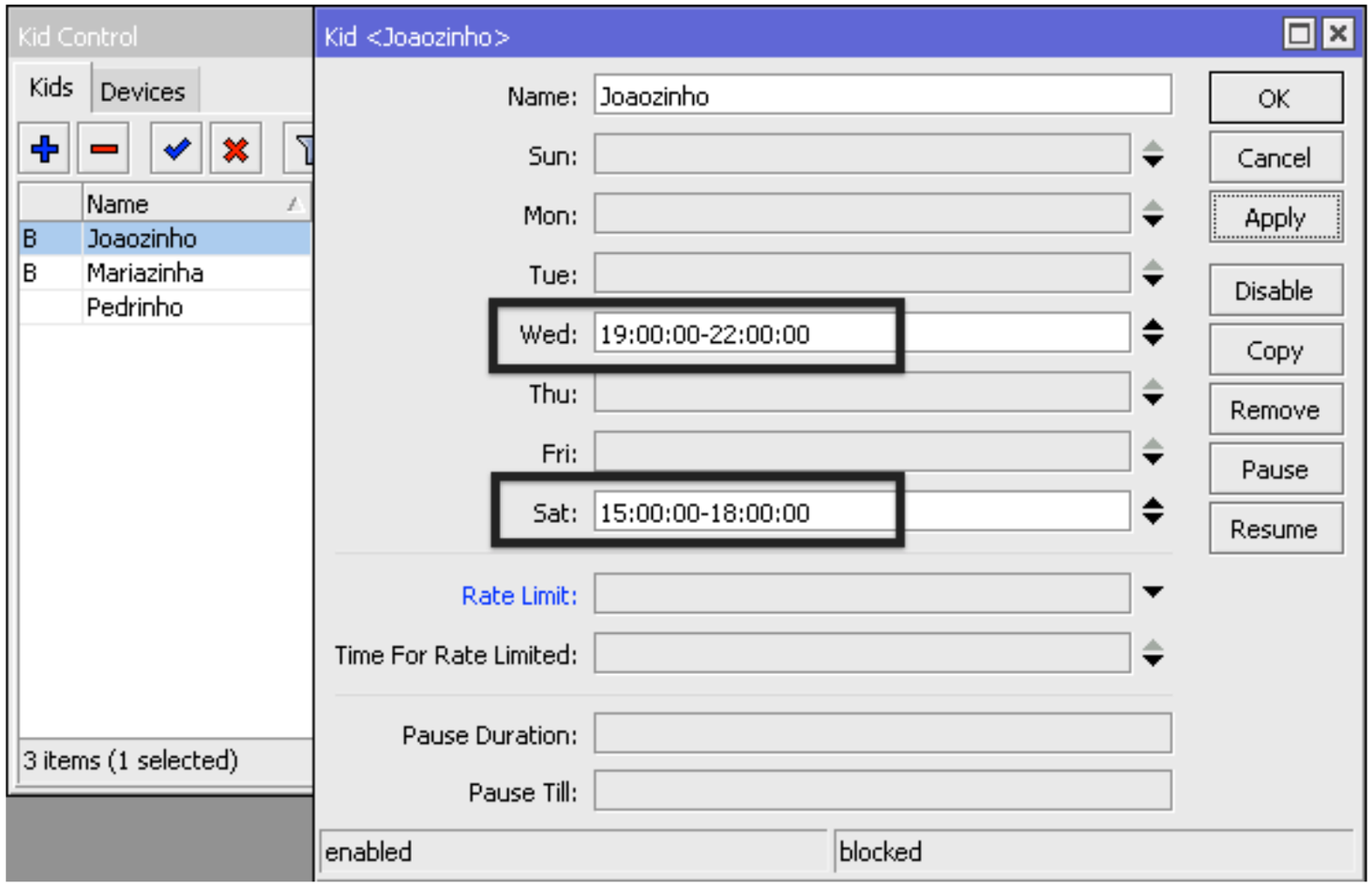
Kid Control



- Devices - Define os dispositivos atrelados a cada criança.

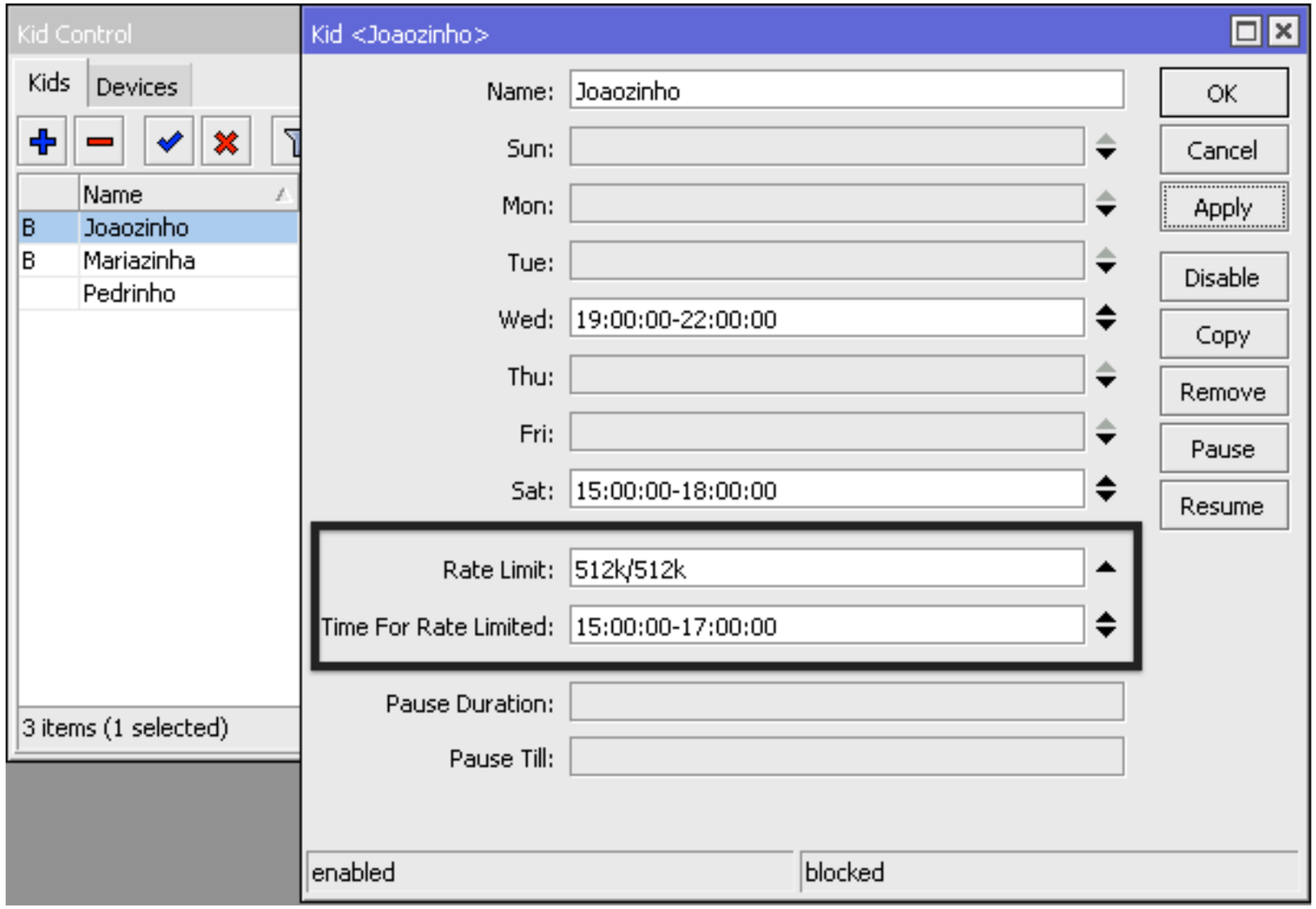
Kid Control

- Possibilidade de escolher diferentes horários de funcionamento:



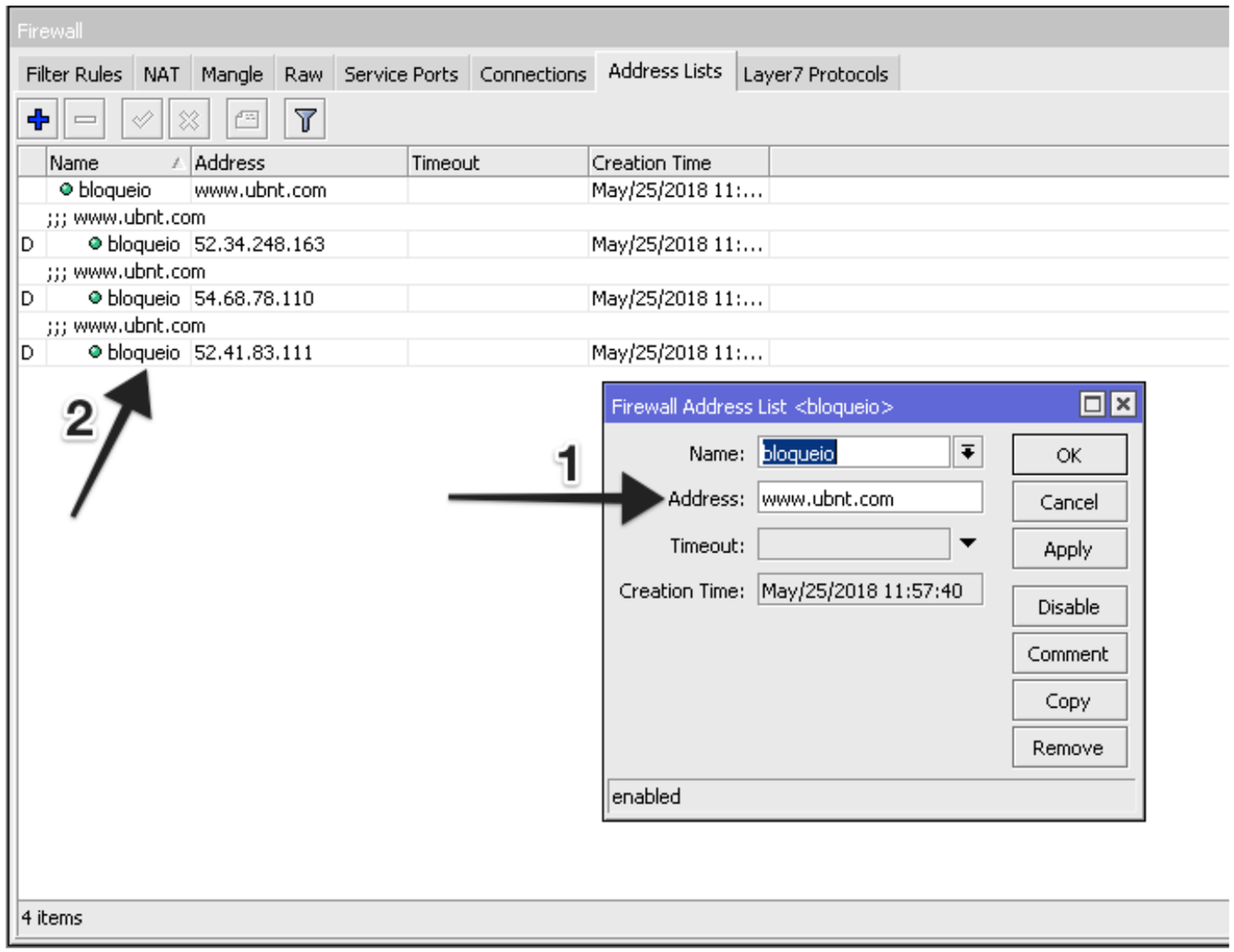
Kid Control

- 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:



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

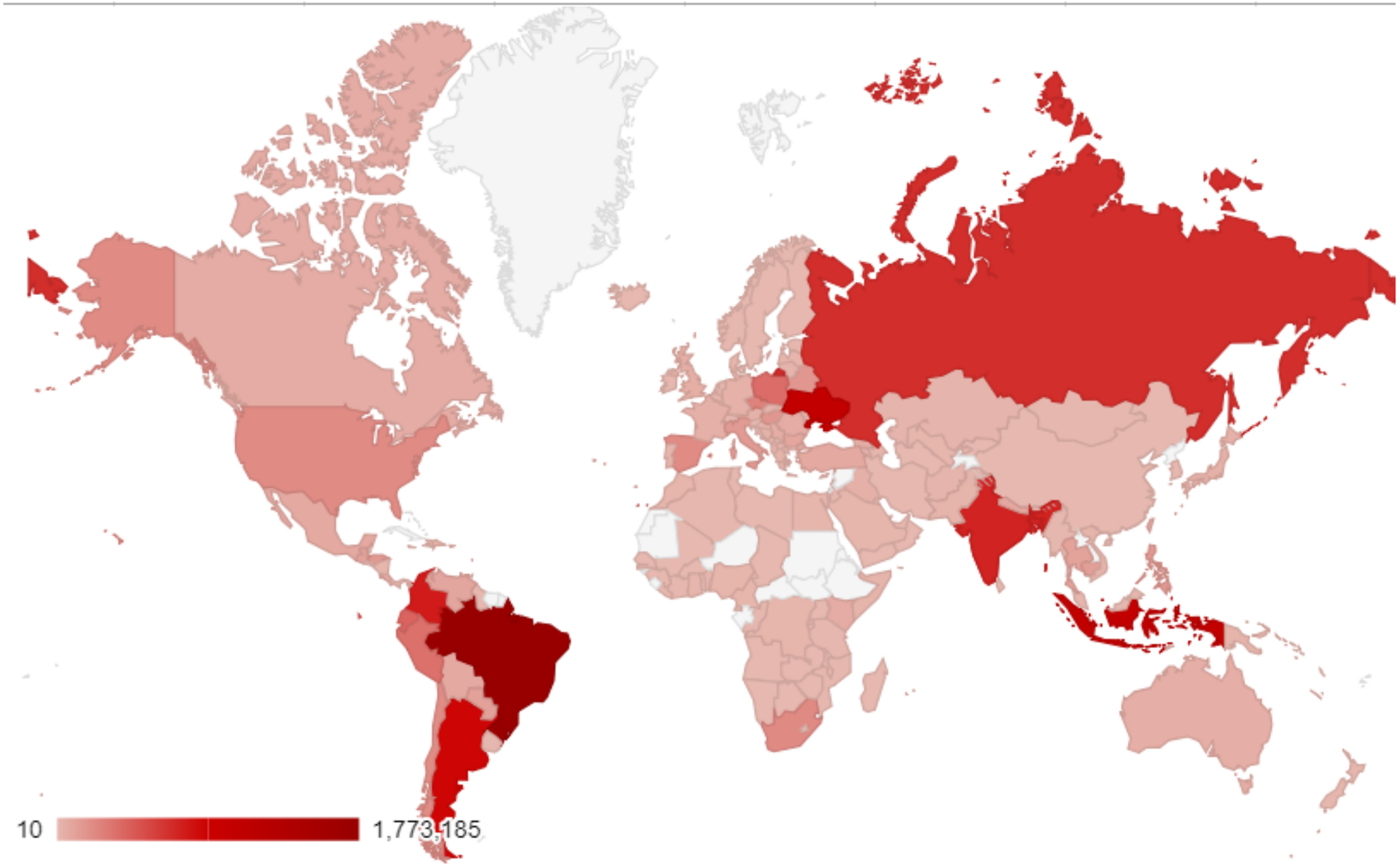
- Corrigida em Agosto de 2018 (6.40.9 e 6.42.7 e 6.43);

- 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

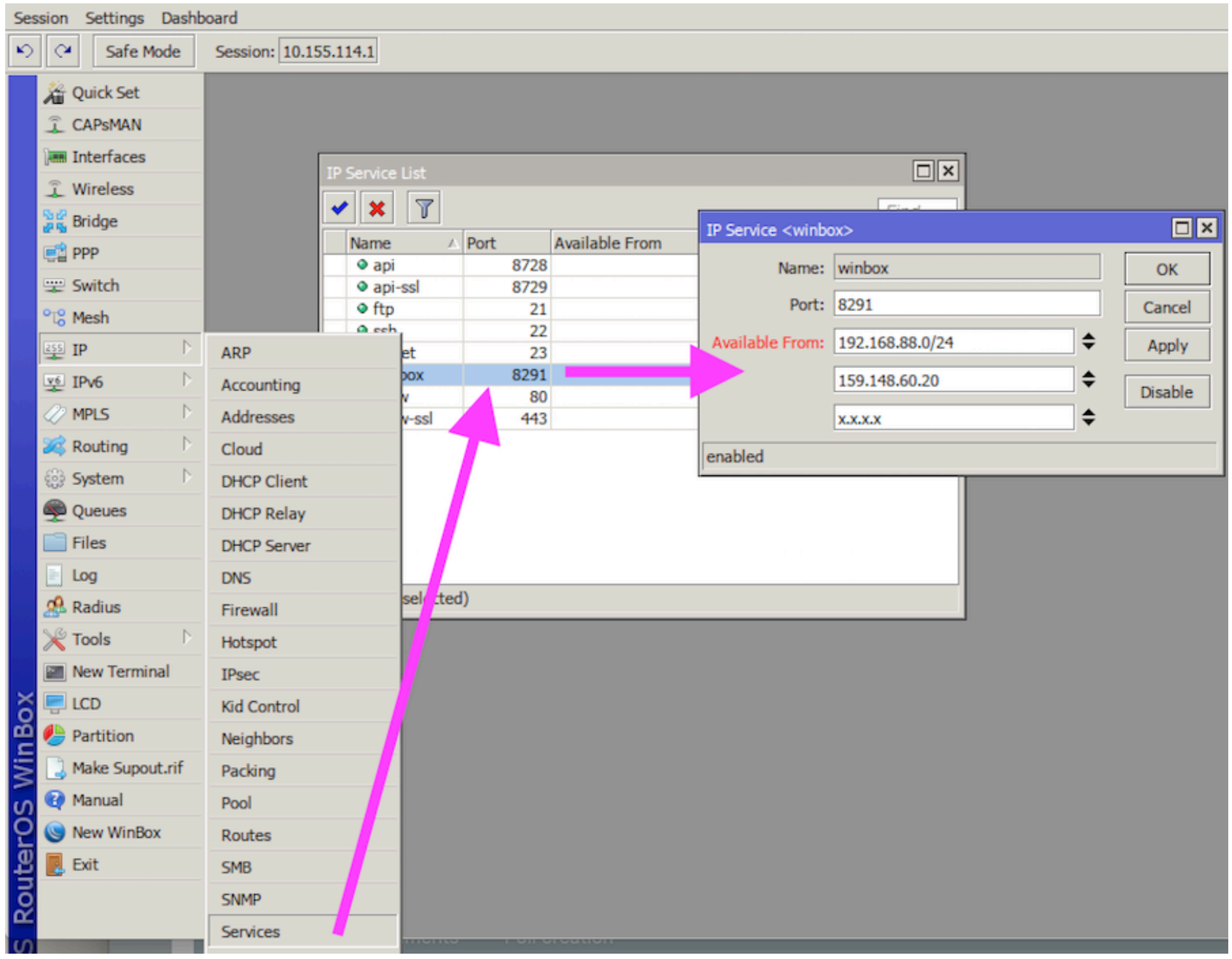
Top ten countries targeted by JS:InfectedMikroTik

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!