Boas práticas para obter o máximo de desempenho com equipamentos da MikroTik.

Redes Brasil

Informações sobre o palestrante

Redes Brasil

Nome: Francisco Ribeiro de Souza Neto

Resumo:

- Trabalha com telecomunicações desde 2005.
- Possui todas as certificações da MikroTik (MTCNA,MTCRE,MTCWE,MTCINE,MTCTCE,MTCUME,MTCIPv6E).
- Consultor e instrutor oficial MikroTik.
- Consultor e instrutor oficial Ubiquiti.

Objetivos da apresentação

Redes Brasil

- Mostrar uma série de funcionalidades e recursos que irão te ajudar a usar 100% da capacidade de seus equipamentos.

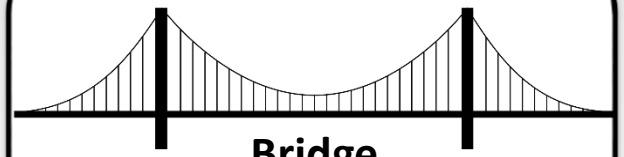
- Fazer uma explicação detalhada sobre cada um dos tópicos, para que você consiga definir quando e onde utilizar tais recursos.

Agenda

- Bridge X Switch;
- Connection tracking (conntrack);
- Fasttrack;
- Tabela RAW;
- FastPath;

Bridges e Switchs

Redes Brasil



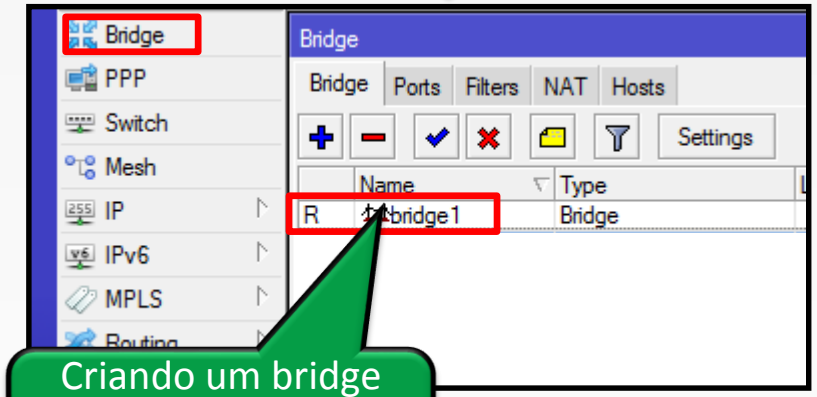
Bridge

Comutação de frames passa pelo CPU (software)

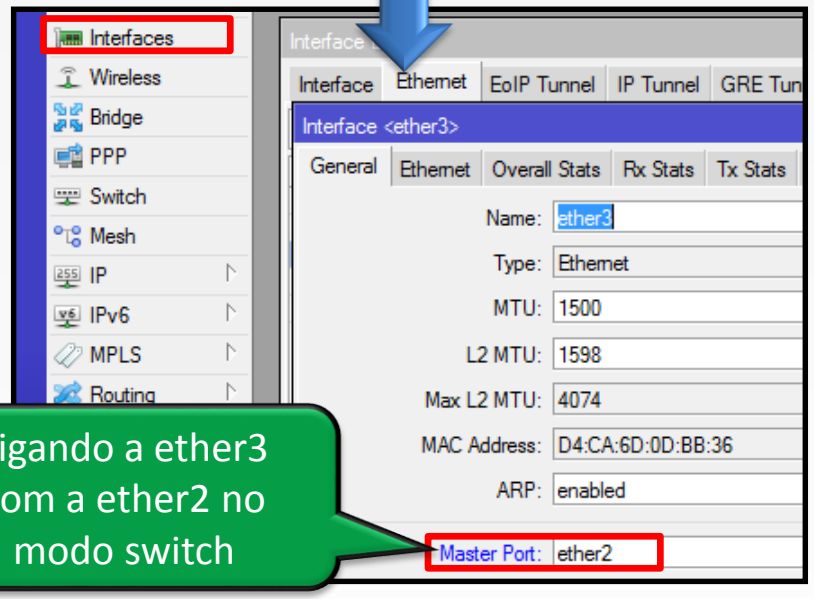
- Trabalham na camada 2
- Comutação de frames acontece em um nível diferente.

Switch

Comutação de frames passa somente pelo switchchip (hardware)



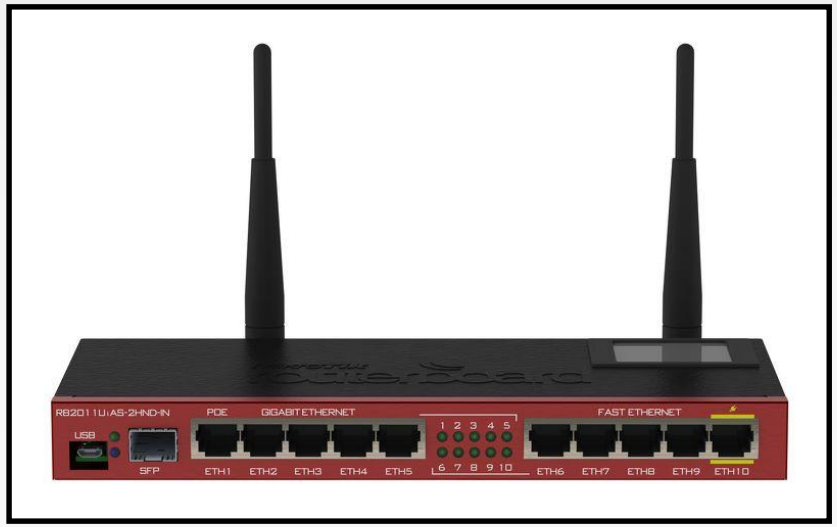
Criando um bridge para futura inclusão de interfaces

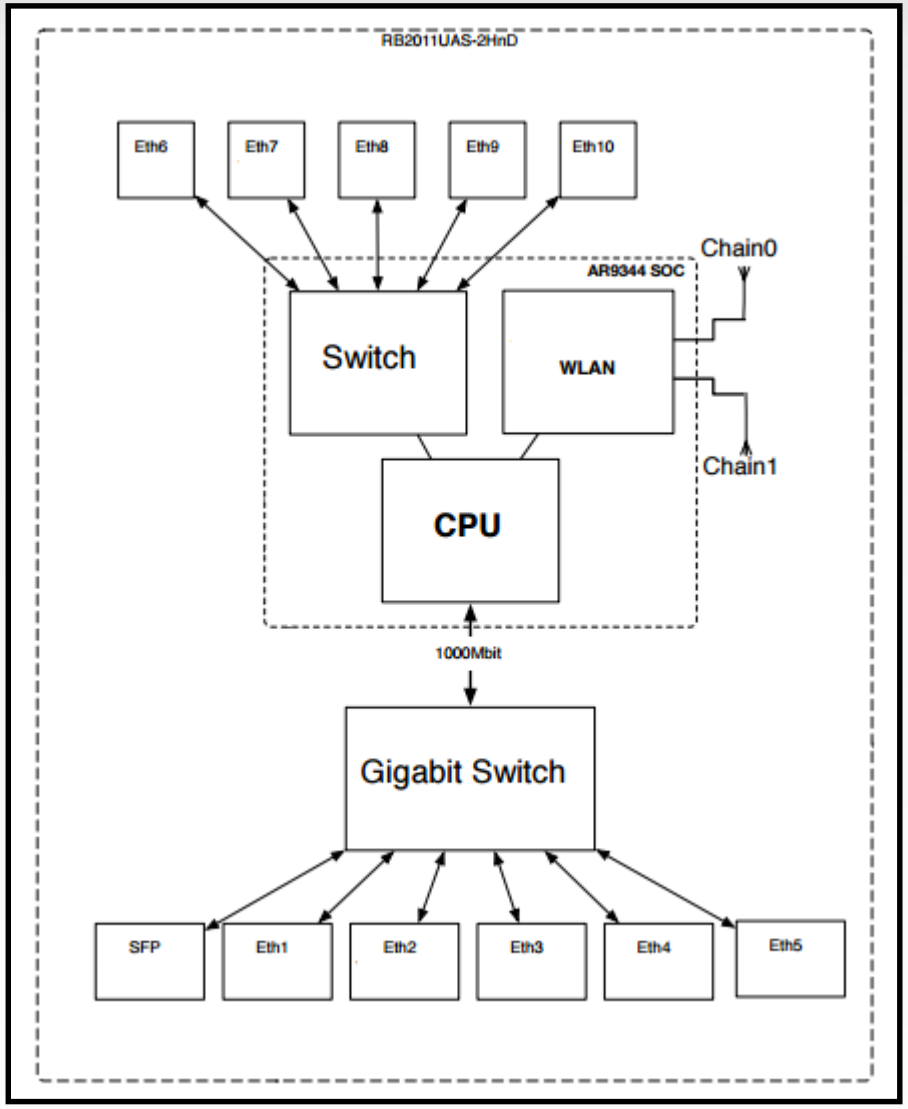


Ligando a ether3 com a ether2 no modo switch

Diagrama de bloco resumido

RB2011UiAS-2HnD-IN



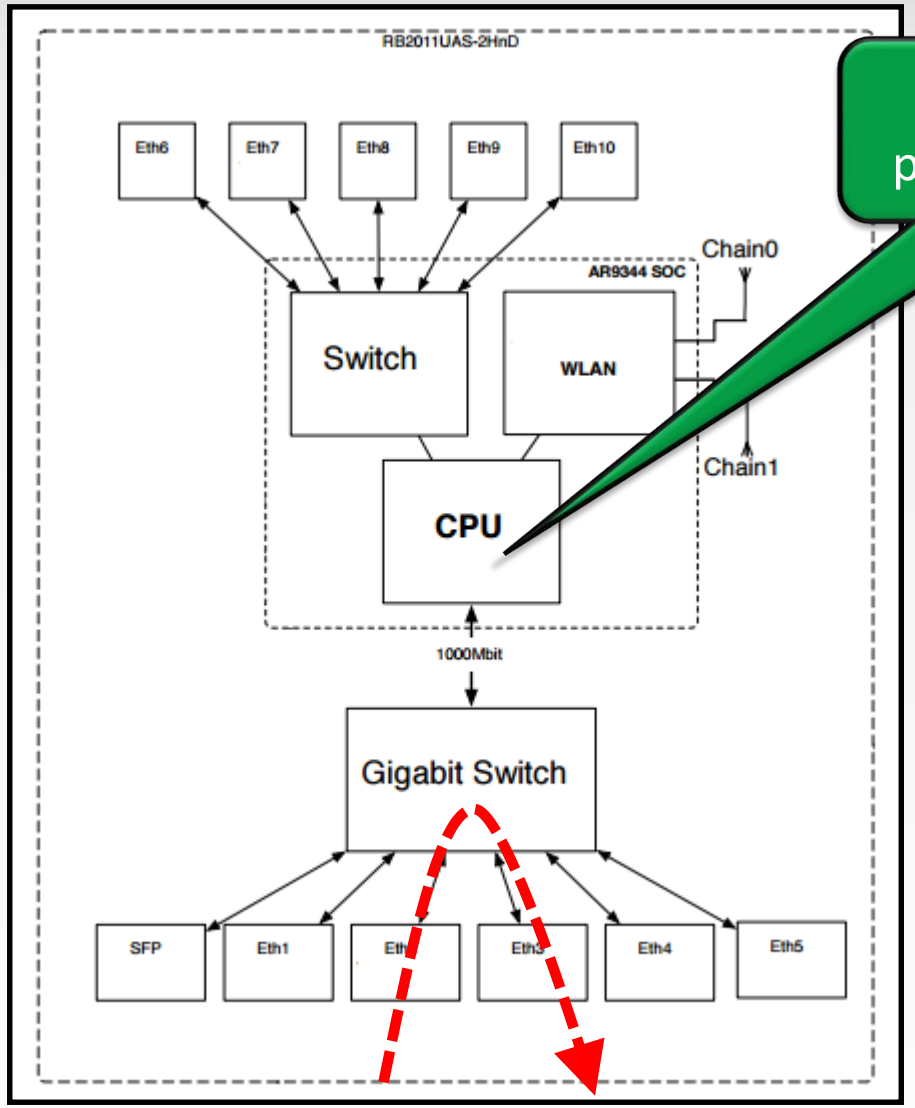


Usando a funcionalidade de switch

Redes Brasil

Onde usar o modo switch

Mesmo segmento de rede.



O tráfego não passa pela CPU.

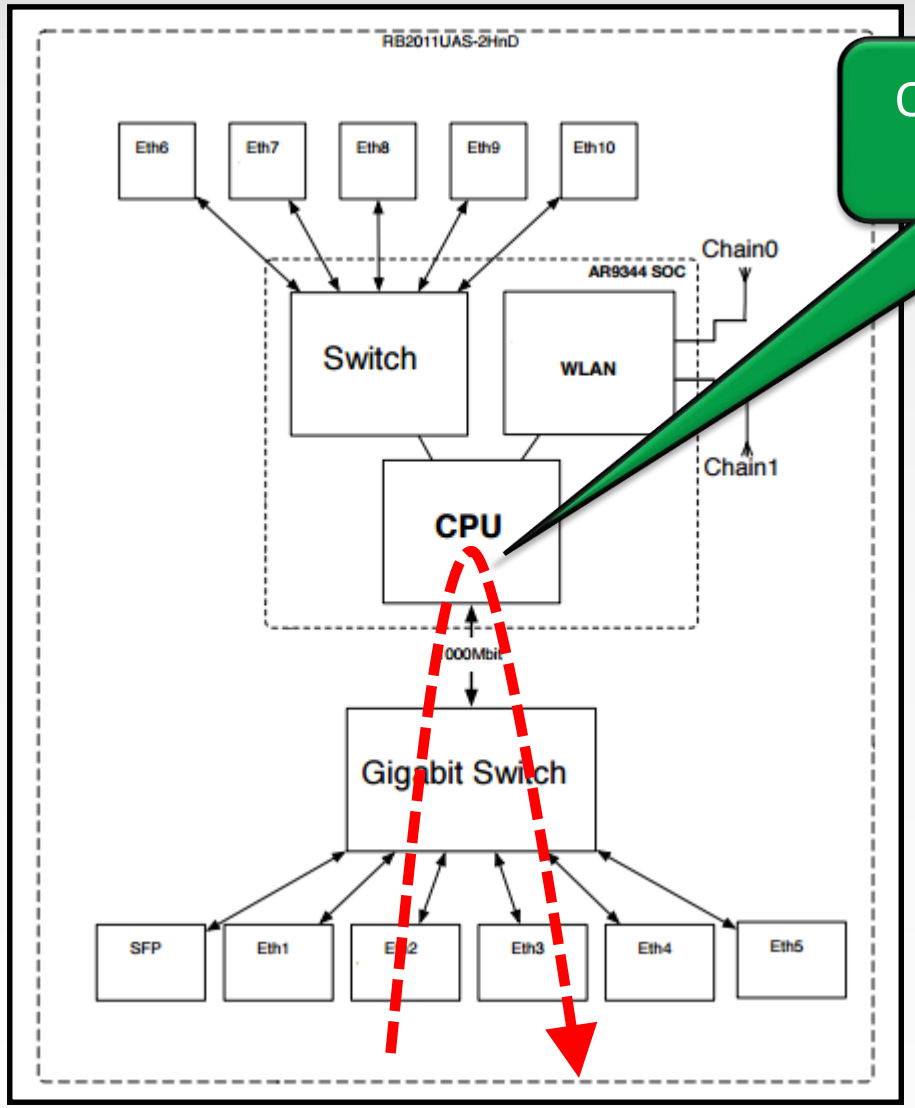
Usando a funcionalidade de bridge

Redes Brasil

Onde usar o modo bridge

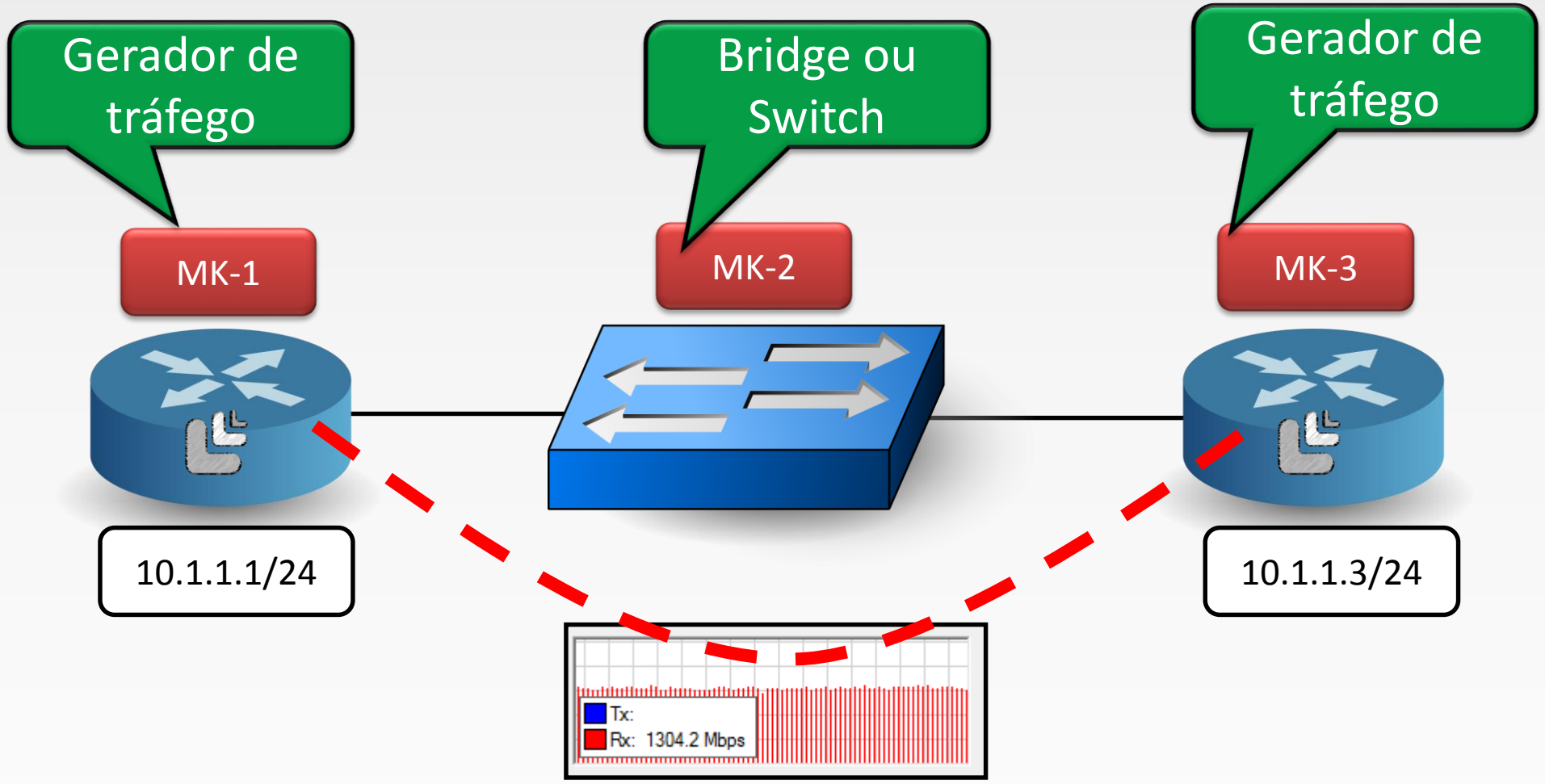
- Firewall
- QoS avançado
- Torch

Mesmo segmento de rede.



O tráfego passa pela CPU.

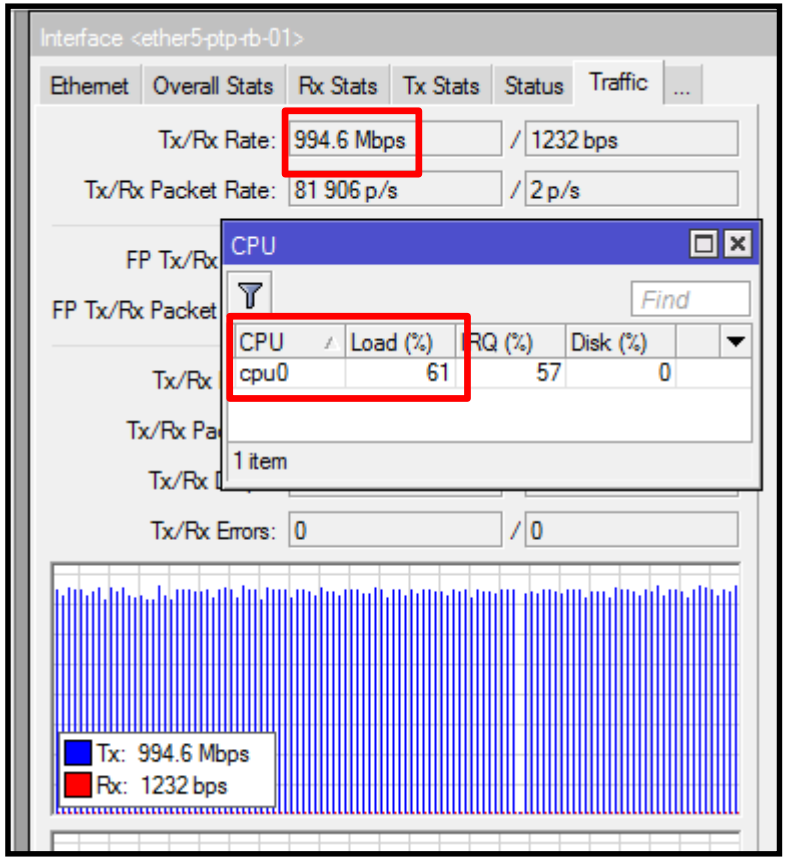
Testes de bancada Bridge e Switch



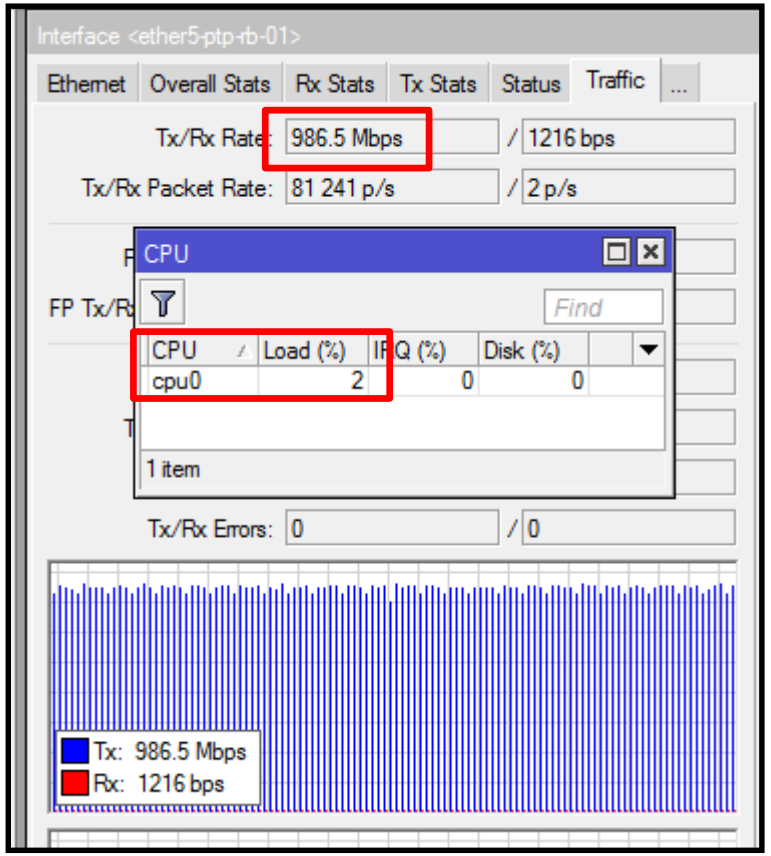
Testes de bancada Bridge e Switch

Redes Brasil

Bridge

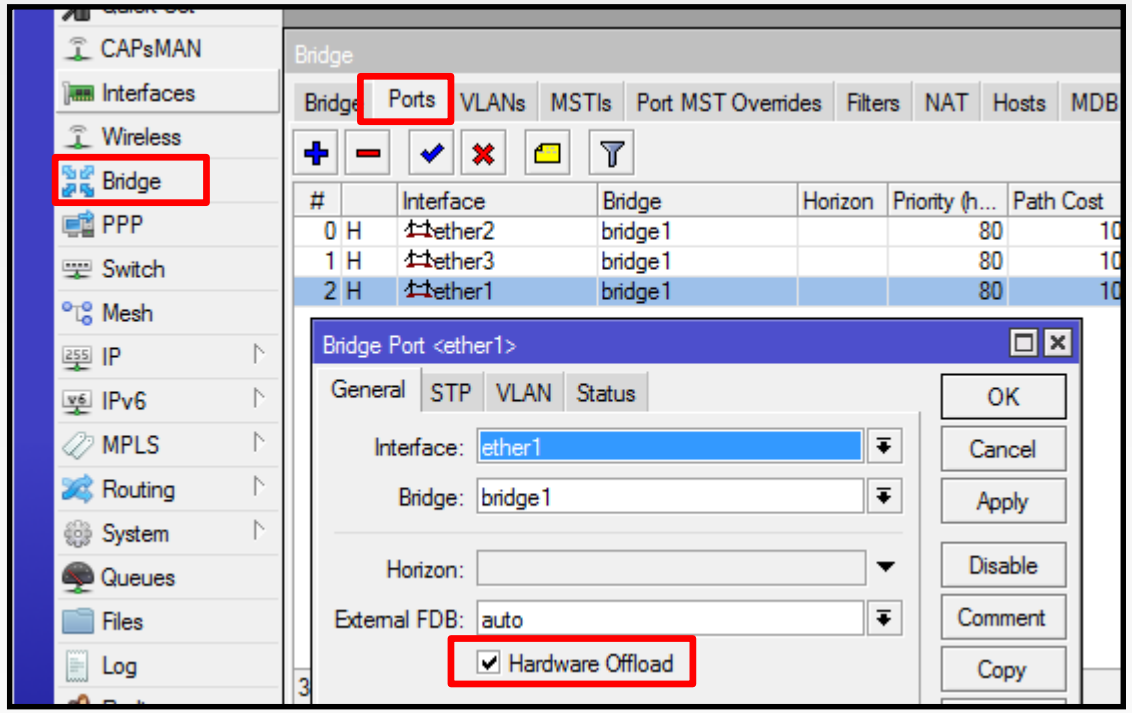


Switch



Vídeo com teste de desempenho https://www.youtube.com/watch?v=tNEhExMOJyw

Bridge Hardware Offloading



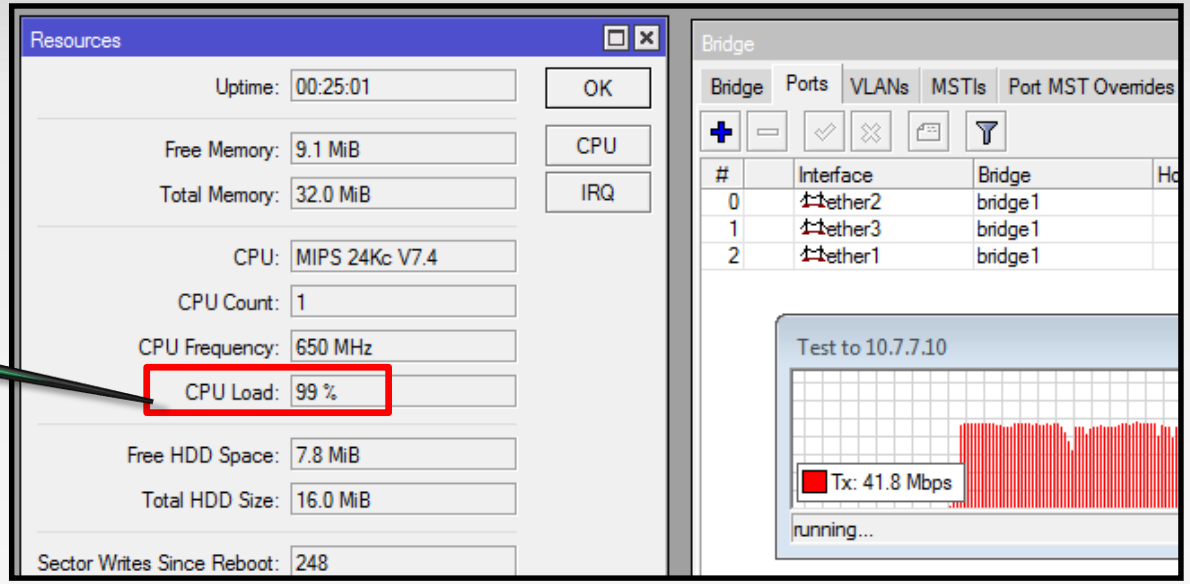
- A partir da versão v6.40rc29 o RouterOS conta com a funcionalidade de **Bridge Hardware Offloading**.

- Com esse recurso uma bridge terá a capacidade de fazer encaminhamento Layer2 usando o switch chip.

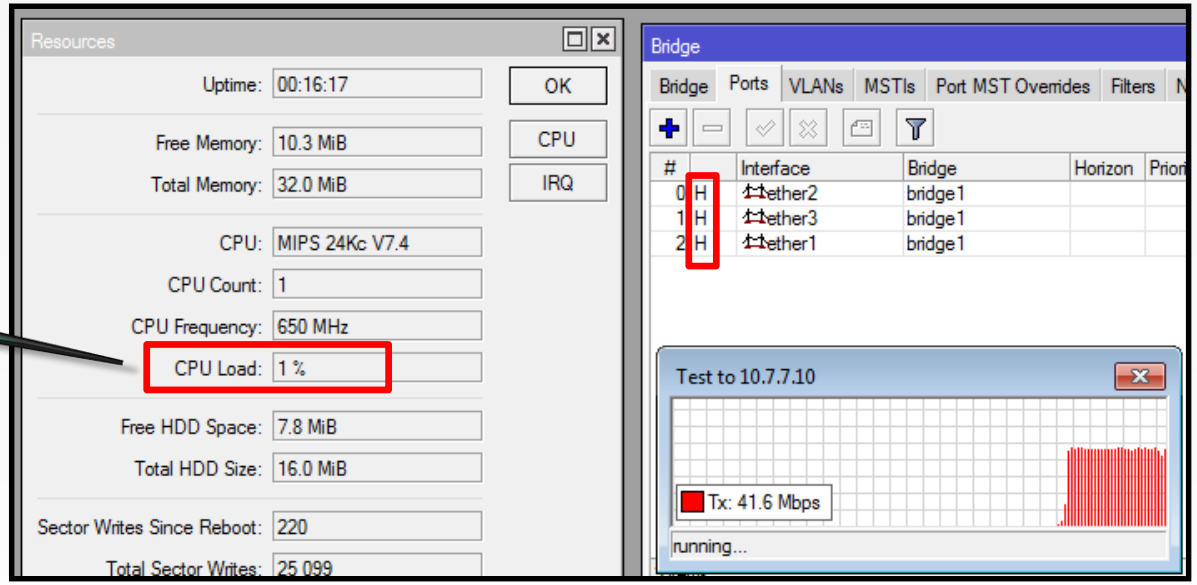
Resultados com hw-offload

Redes Brasil

Sem hardware-offload

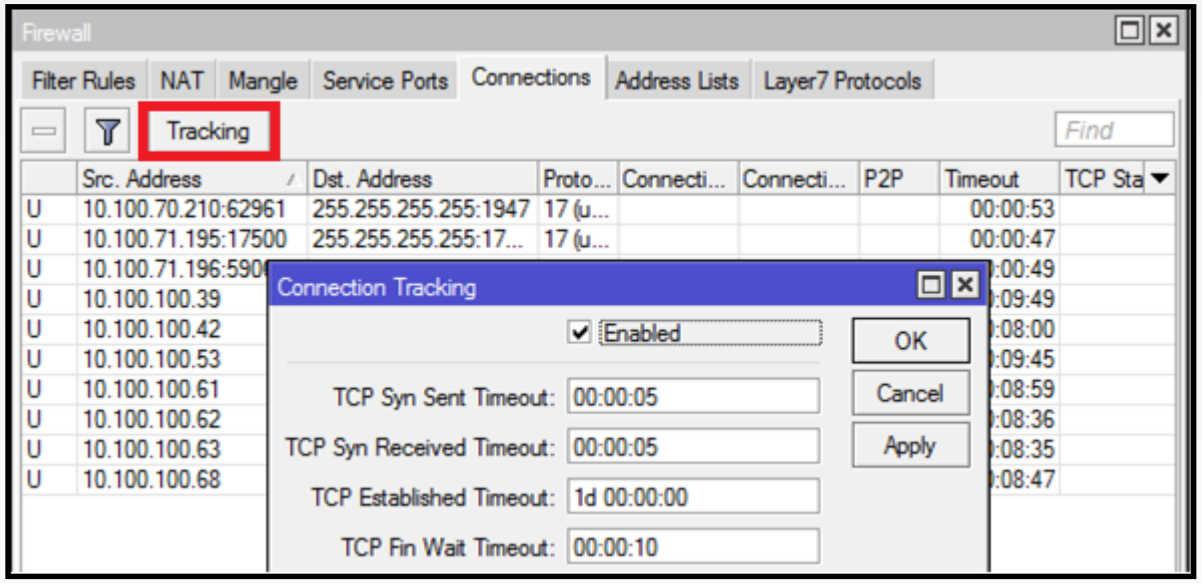


Com hardware-offload



Connection Tracking

- Utilizando a connection tracking o firewall consegue armazenar os estados das conexões.



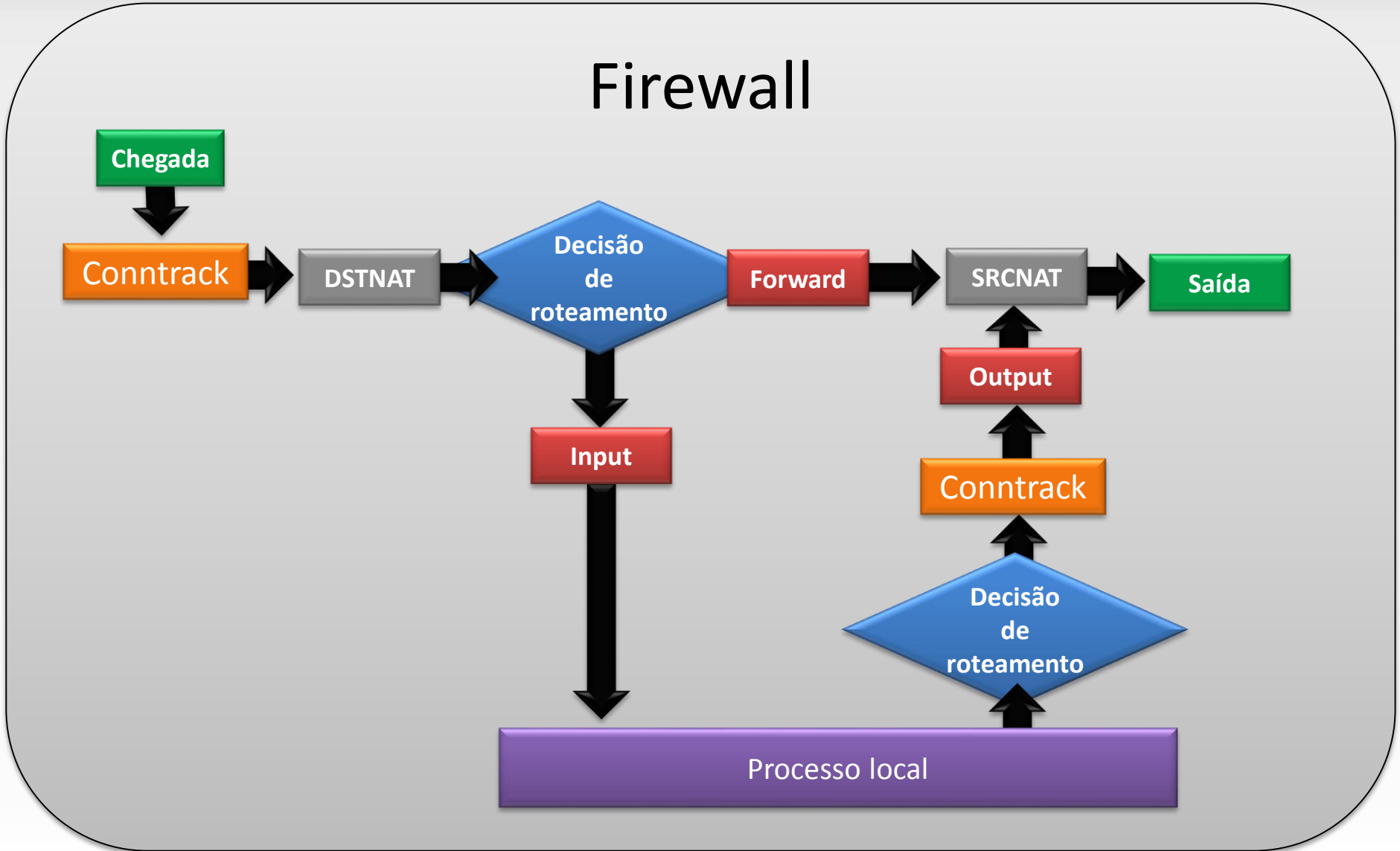
Connection Tracking

Cuidado com Connection Tracking (Conntrack).

Ajuda em algumas tarefas.

Rouba seu CPU

Localização da Connection Tracking



Quando preciso da conntrack habilitada?

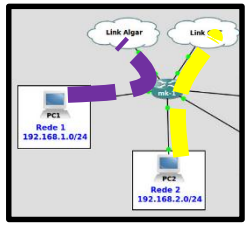
- NAT
- firewall:
  - connection-bytes
  - connection-mark
  - connection-type
  - connection-state
  - connection-limit
  - connection-rate
  - layer7-protocol
  - p2p
  - new-connection-mark
  - tarpit
- p2p matching in simple queues

Marcas de conexões

Para que serve marcas de conexões?

QoS

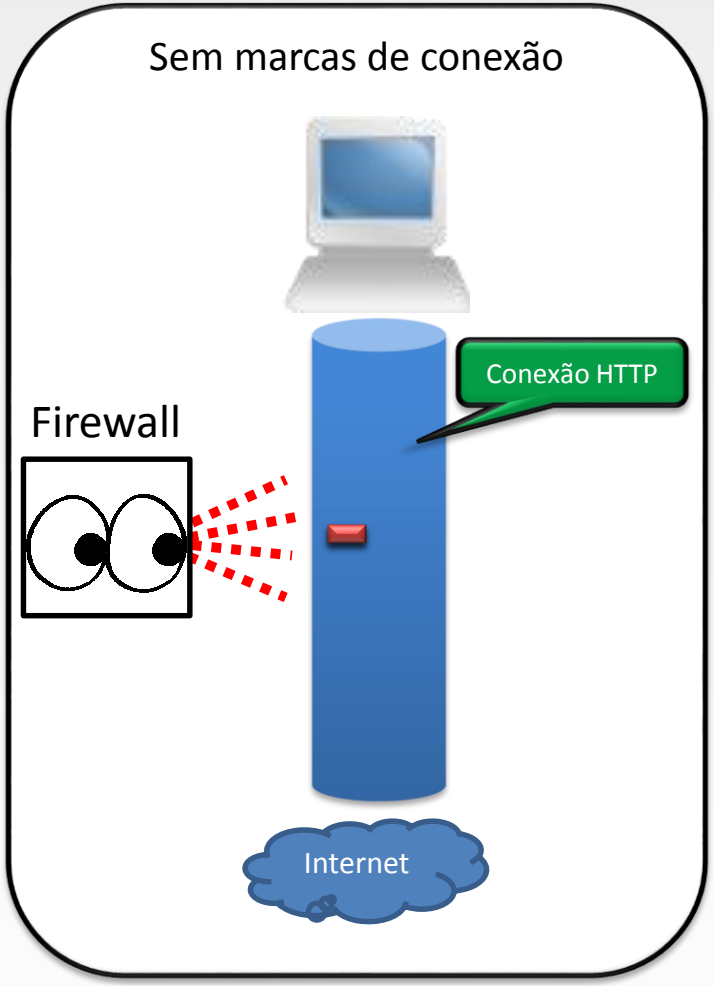
Marcas de pacotes

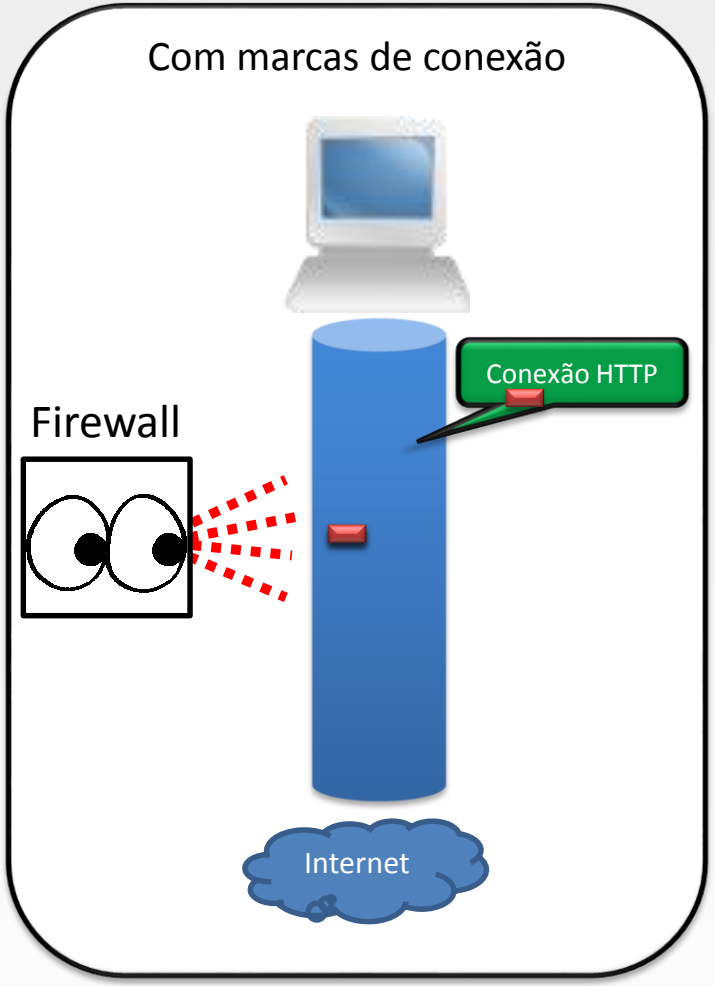


Marcas de roteamento

- Auxiliar as marcas de pacotes e marcas de roteamento
- Evitar que todos os pacotes sejam inspecionados no firewall
- Economia de uso de recursos da CPU
- Ajudar em algumas politicas de roteamento

Marcas de conexão

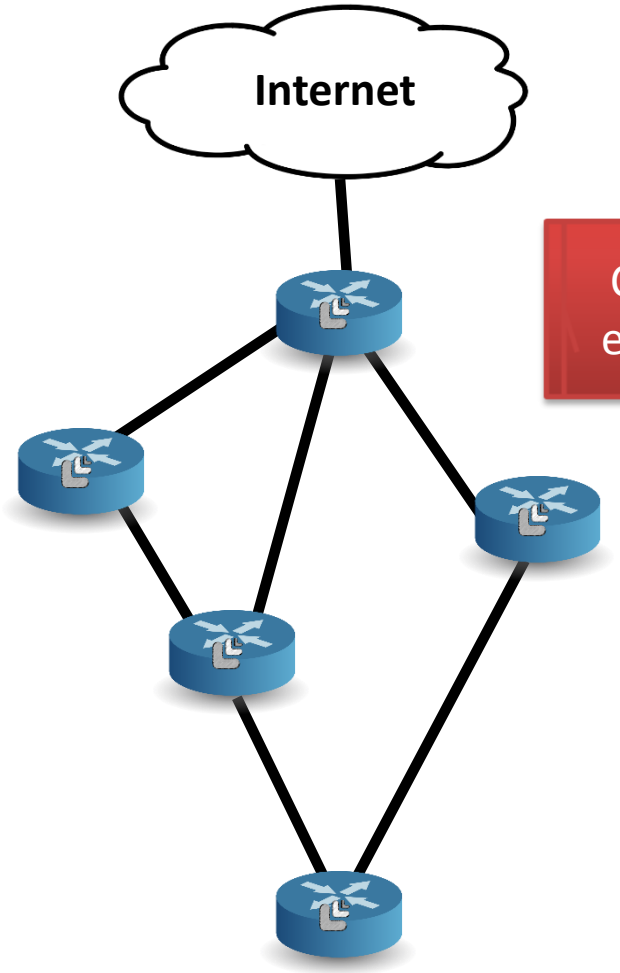




Onde posso desabilitar?

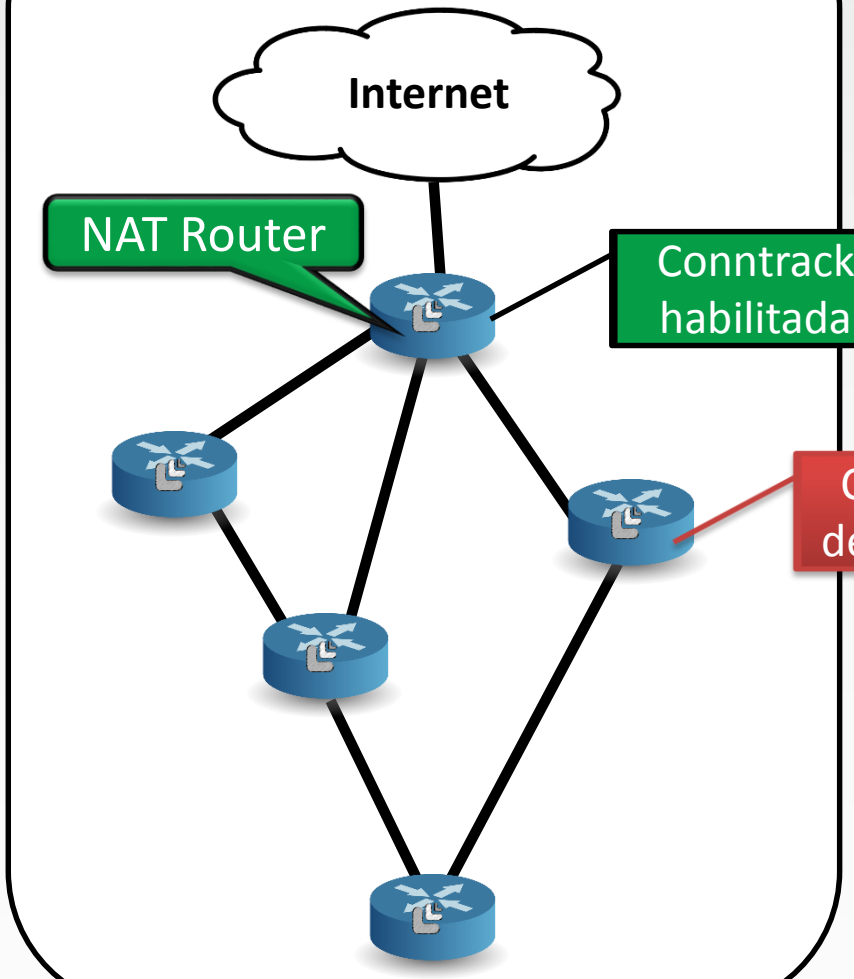
Redes Brasil

IPs públicos



Conntrack desabilitada
em todos os roteadores

IPs privados



NAT Router

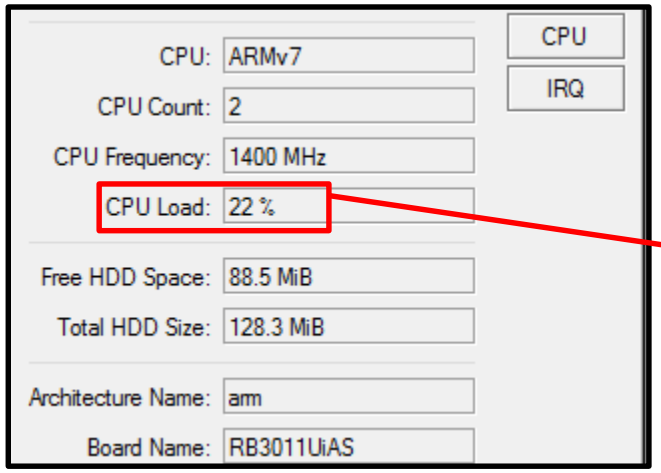
Conntrack
habilitada

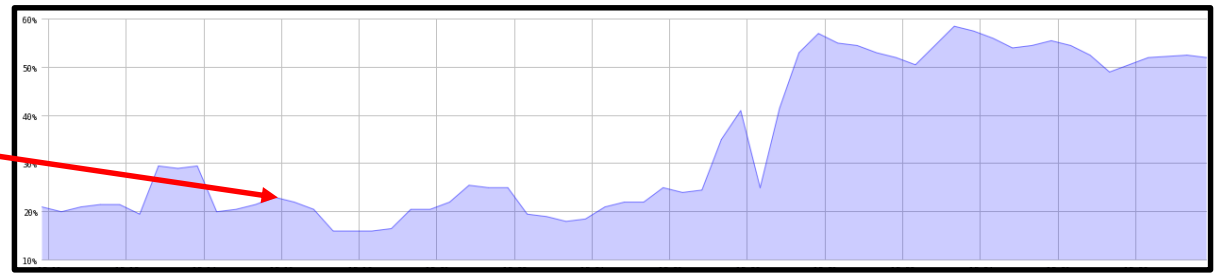
Conntrack
desabilitada

Consumo de CPU

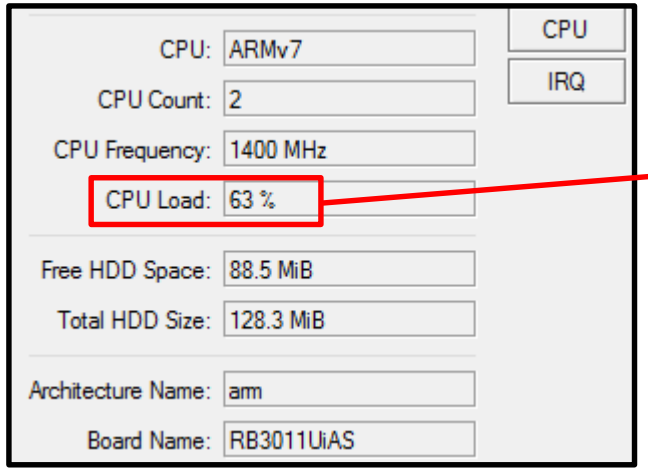
Redes Brasil

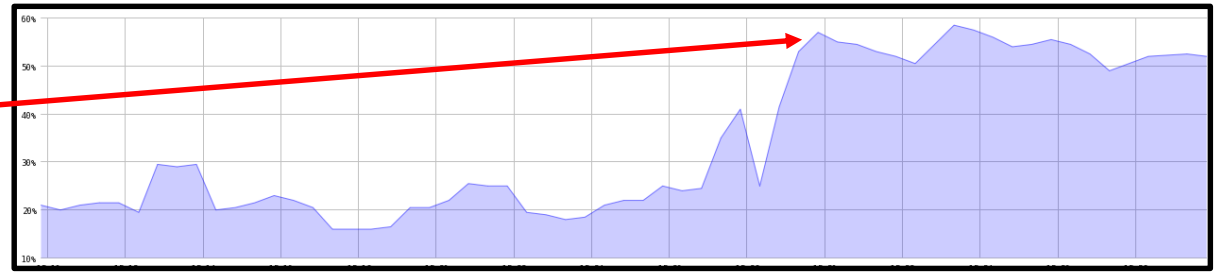
Conntrack desabilitada





Conntrack habilitada





Ainda precisa parcialmente do NAT ?

Fasttrack

Sem controle de banda

Sem filtros no firewall

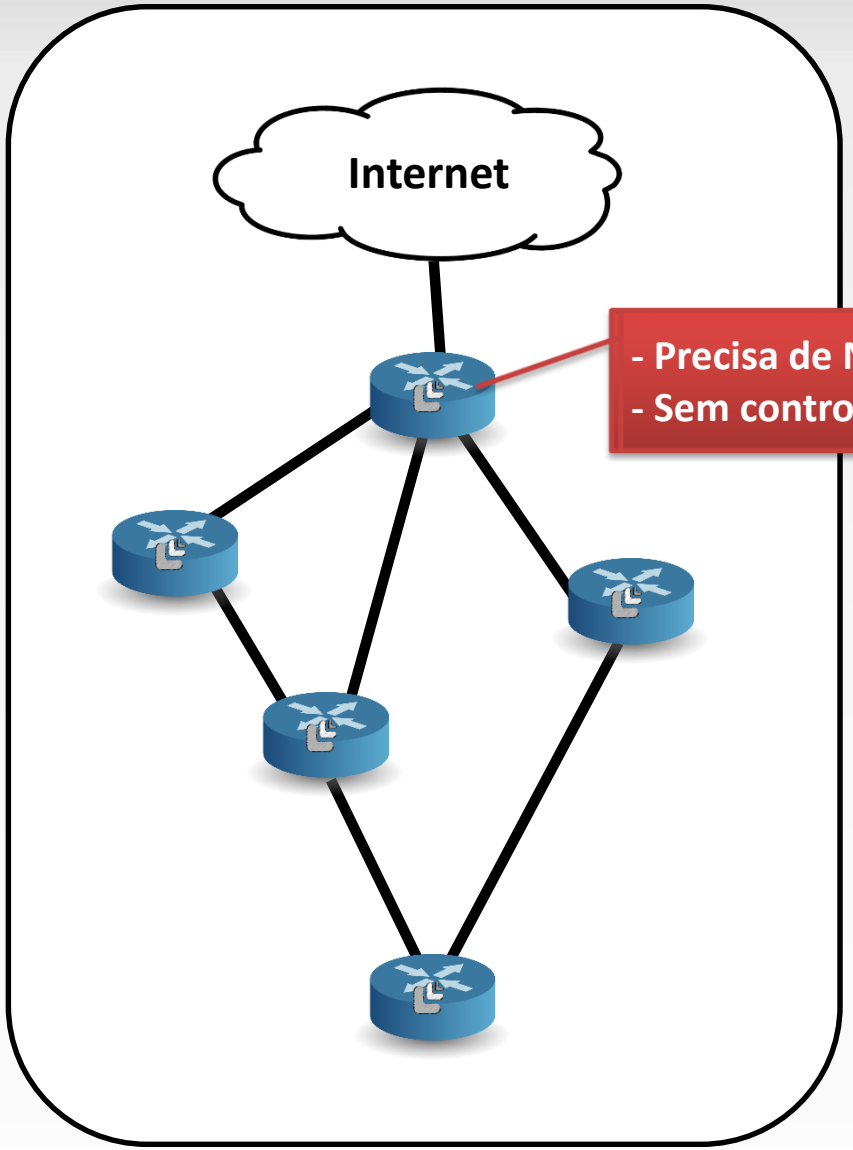
No-track

Controle de banda

Filtros de firewall

Onde aplicar fasttrack ?

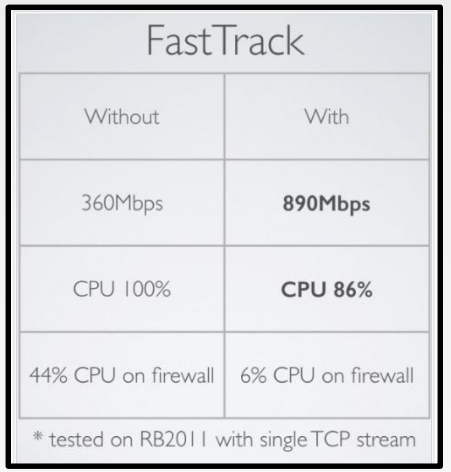
Redes Brasil



- Precisa de NAT
- Sem controle de banda e outros recursos

Fasttrack

- Com o recurso de Fasttrack ativo os pacotes irão fazer um bypass dos seguintes recursos.
  - Firewall
  - Connection tracking
  - Simple queues e queue tree com parent=global
  - IP accounting
  - IPSec
  - Hotspot
  - Universal client
  - VRF



FastTrack

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

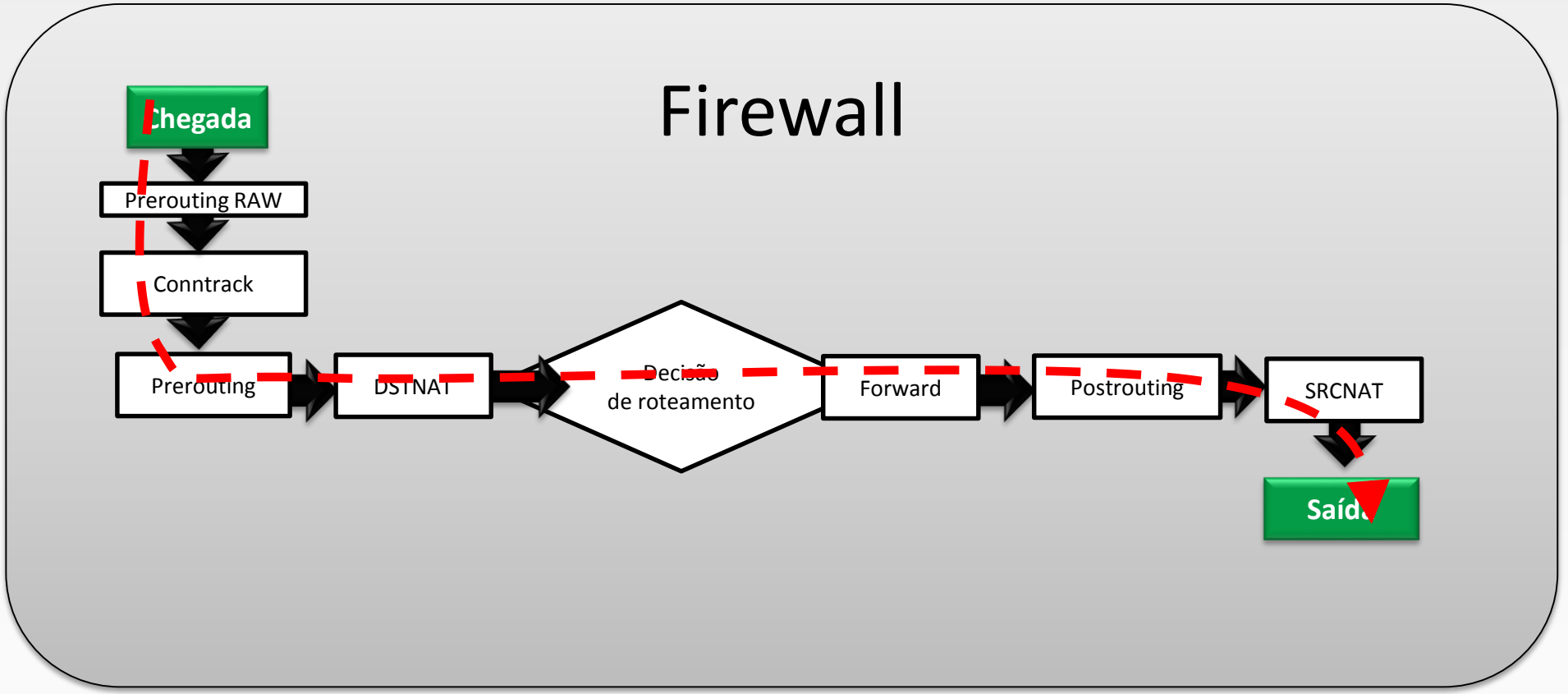
* tested on RB2011 with single TCP stream

- Ativando Fasttrack você pode aumentar em até 5x a performance do roteador.
- Para mais informações visite http://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack

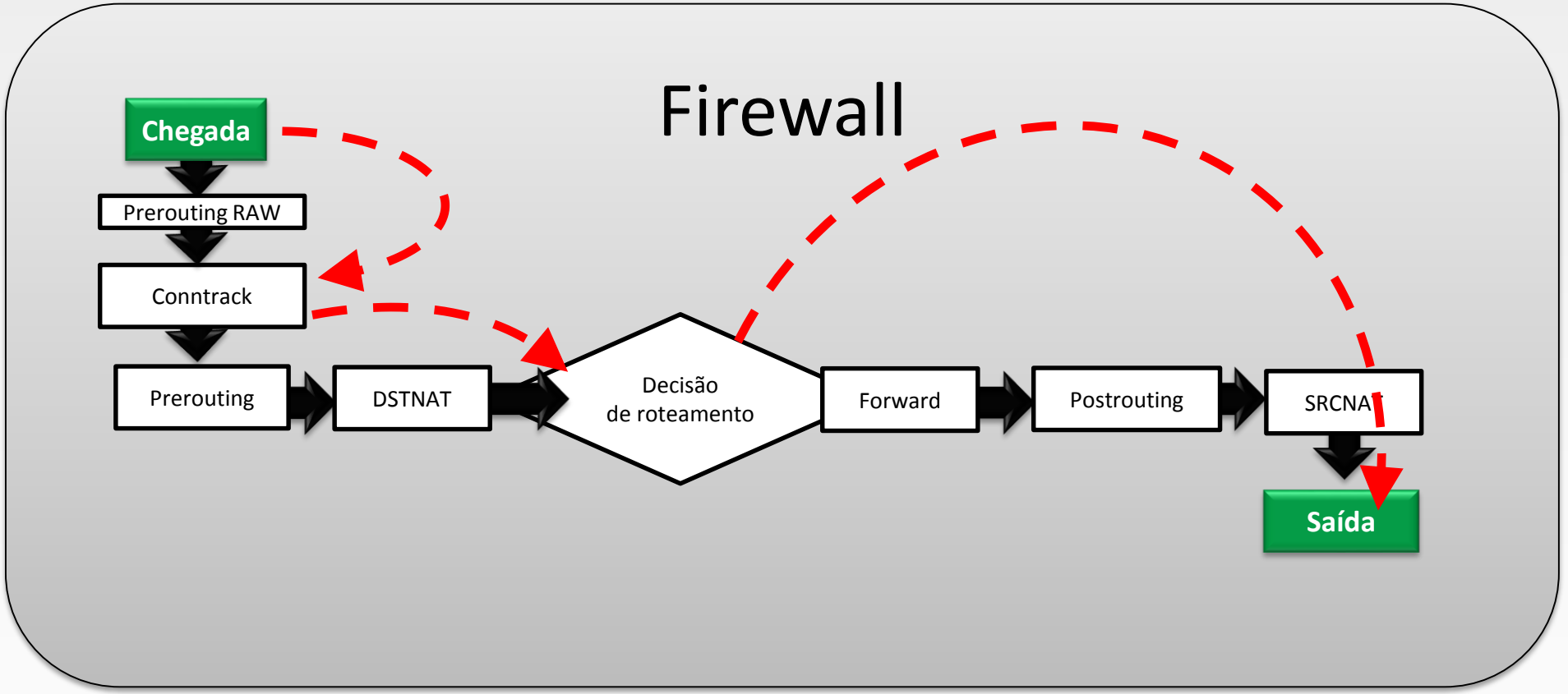
Comandos

```
/ip firewall filter
add chain=forward action=fasttrack-connection connection-state=established,related
```

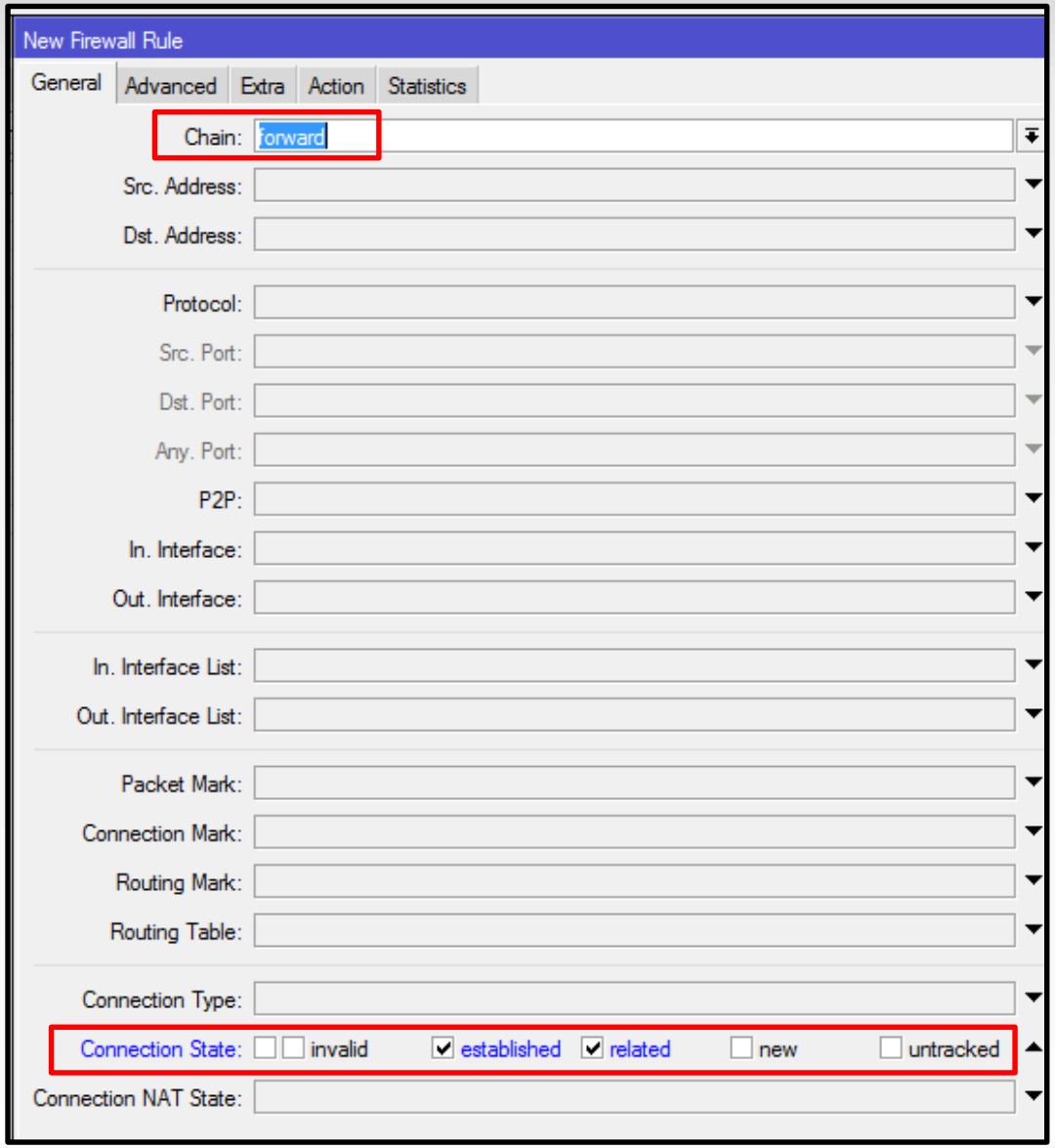
Fluxo do firewall sem fasttrack

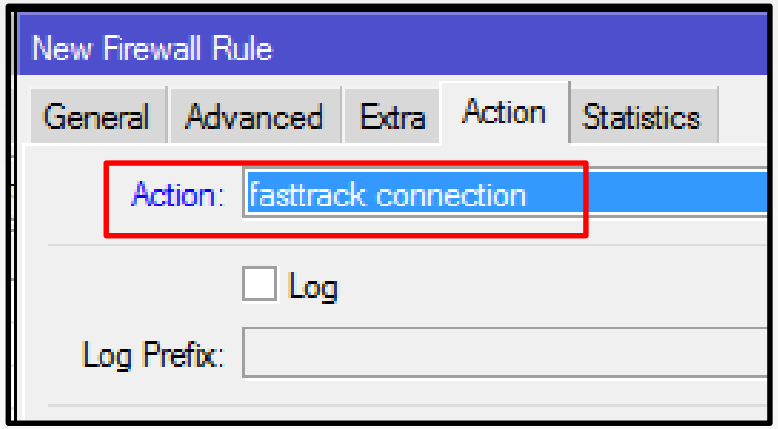


Analogia do fluxo com fasttrack



Regra para Fasttrack

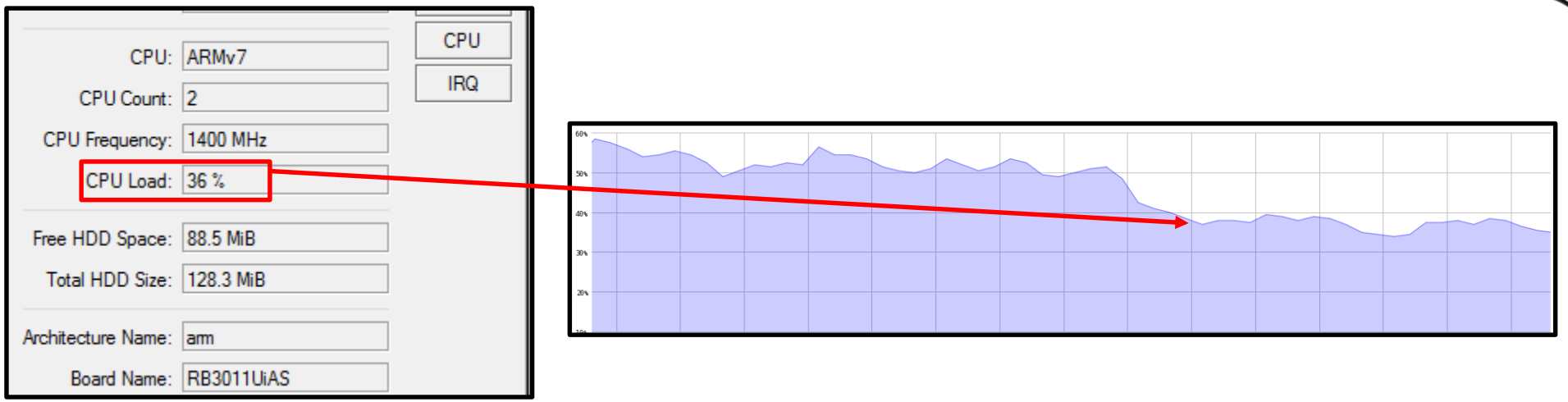




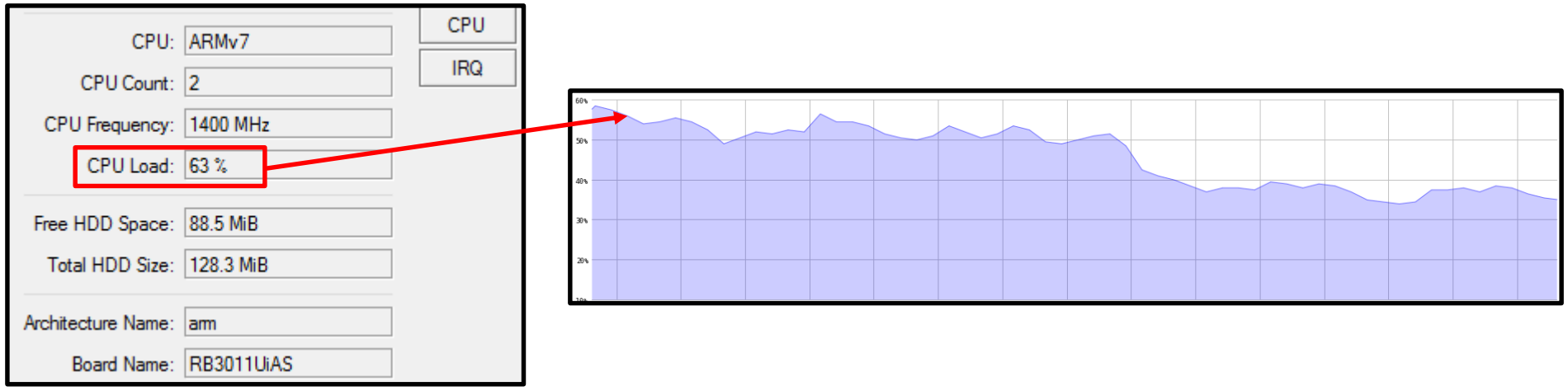
Consumo de CPU

Redes Brasil

Com Fasttrack

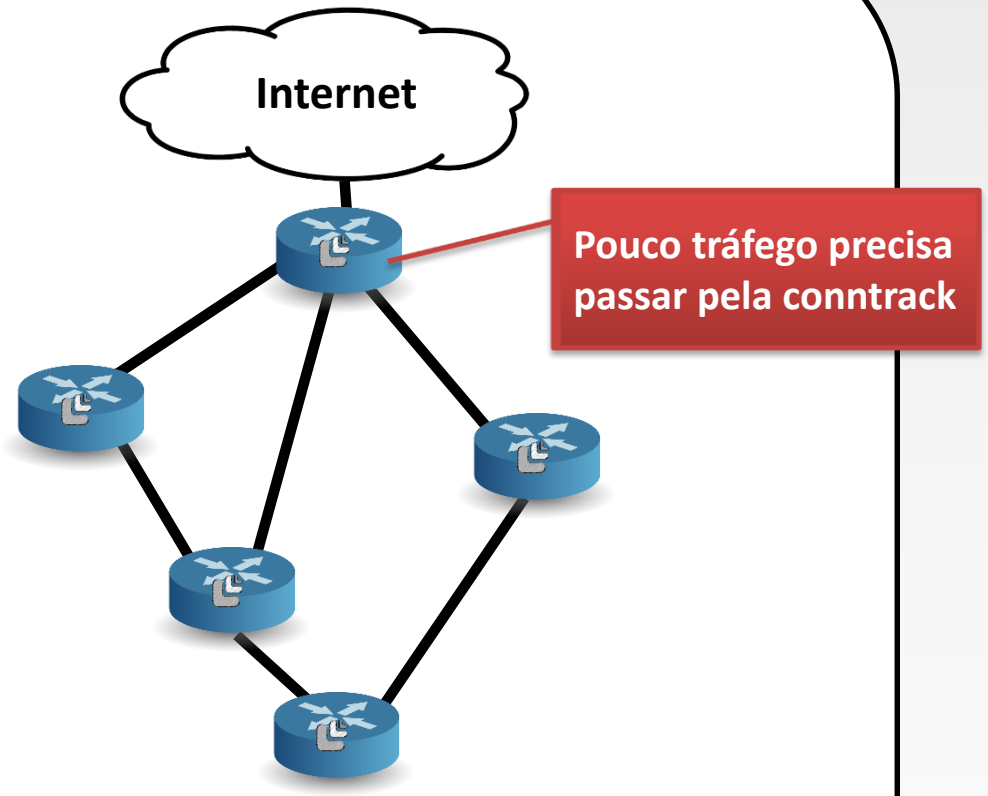


Sem Fasttrack

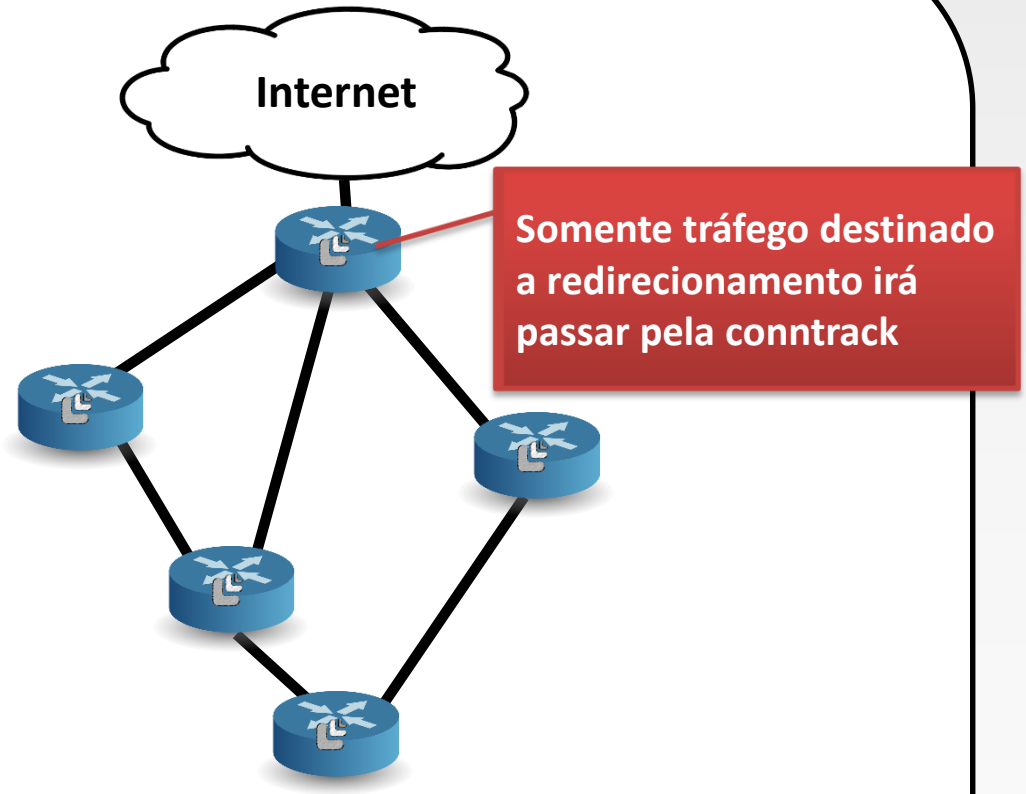


Onde aplicar a ação no-track ?

Redes Brasil

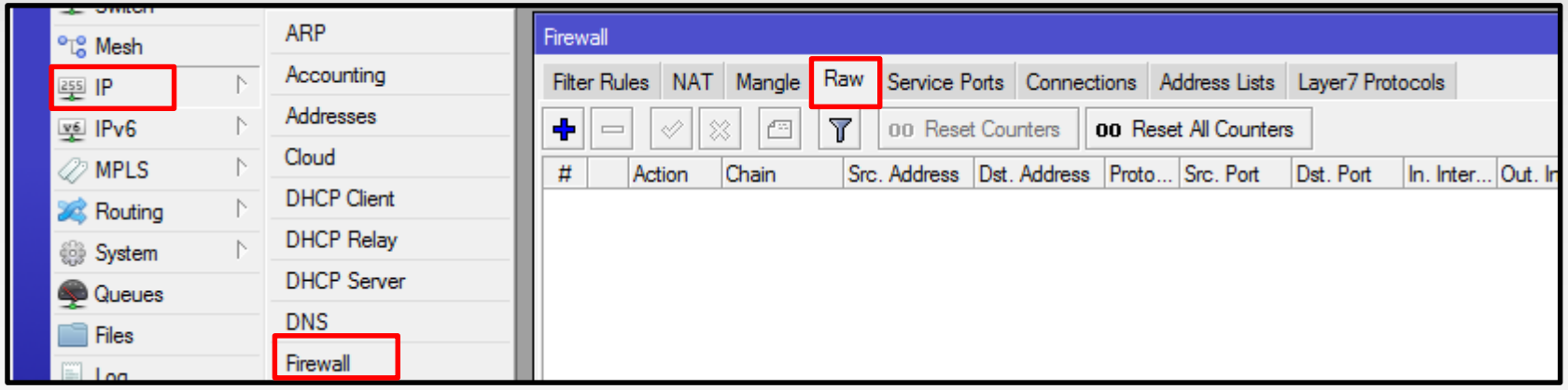


Grande parte do tráfego usa IPs públicos
Pequena parte do tráfego usa IPs privados



Precisa ativar NAT nos roteadores internos para fazer algum tipo de redirecionamento.
Ex: Pág de bloqueio

Tabela RAW

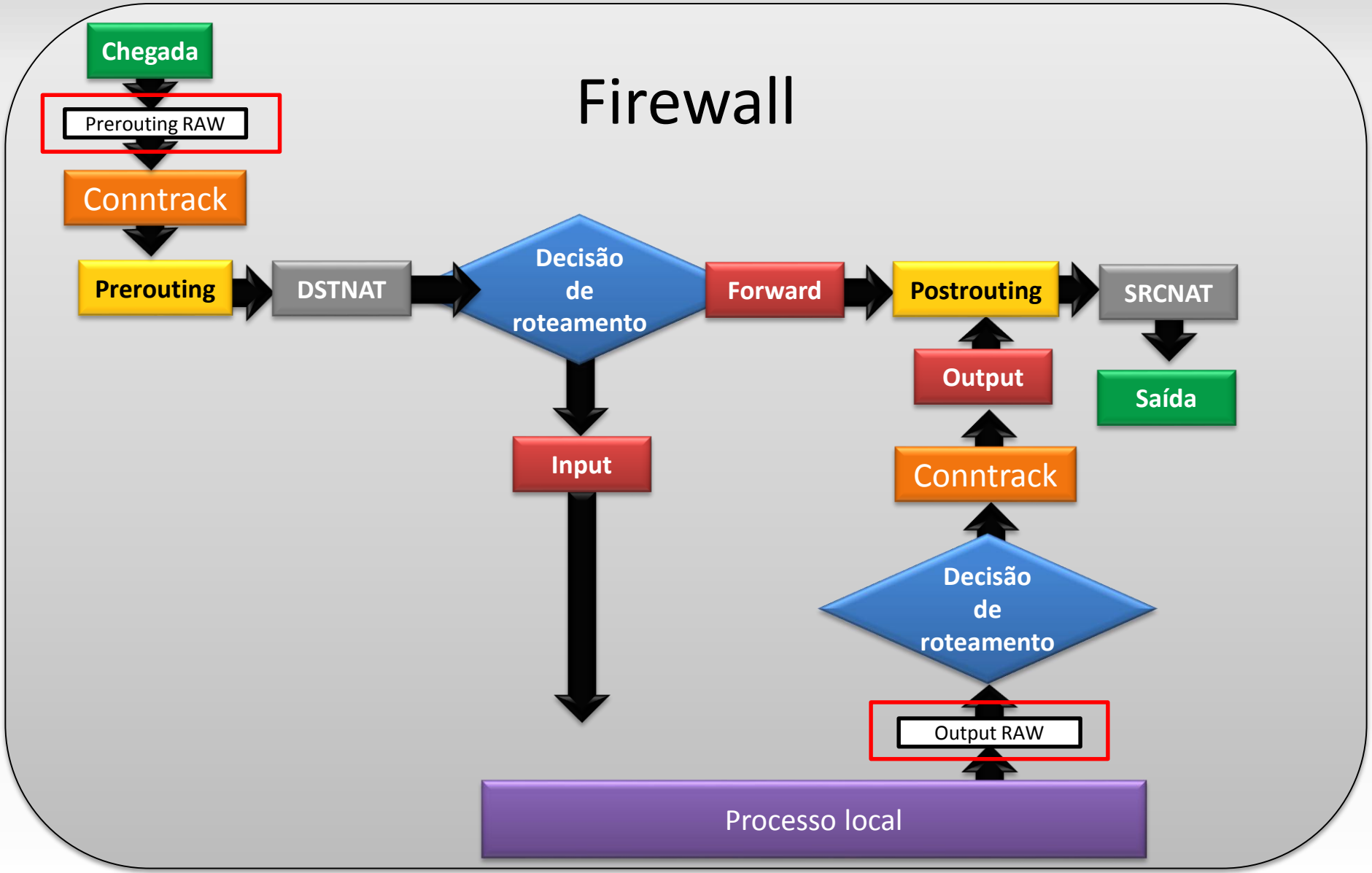


- A tabela RAW pode ser usada para fazer um bypass ou drop de pacotes antes que os pacotes cheguem até a connection tracking e com isso consegue reduzir drasticamente a sobrecargas na CPU.

- Filtros contra ataque de DoS e ou DDoS devem preferivelmente ser aplicados na tabela RAW.

- As ações mais comuns da tabela RAW são:
  - Drop: Usada para dropar pacotes antes que ele avance para processos internos.
  - No track: Usada para fazer com que pacotes façam um bypass da connection tracking.

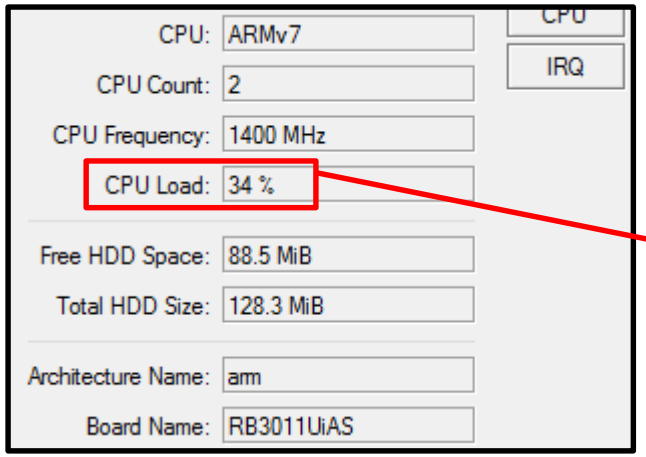
Canais da tabela RAW

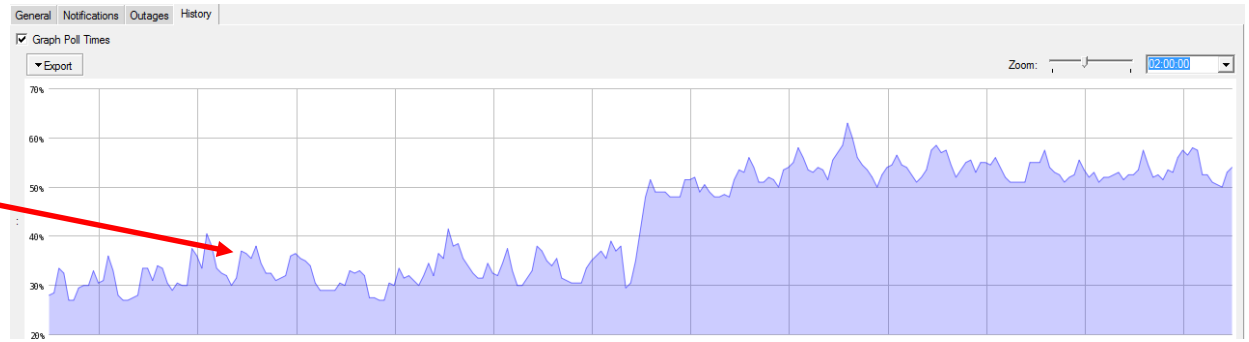


Consumo de CPU

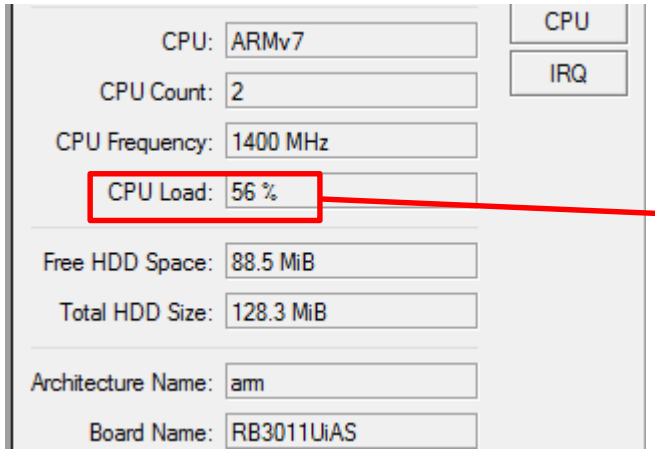
Redes Brasil

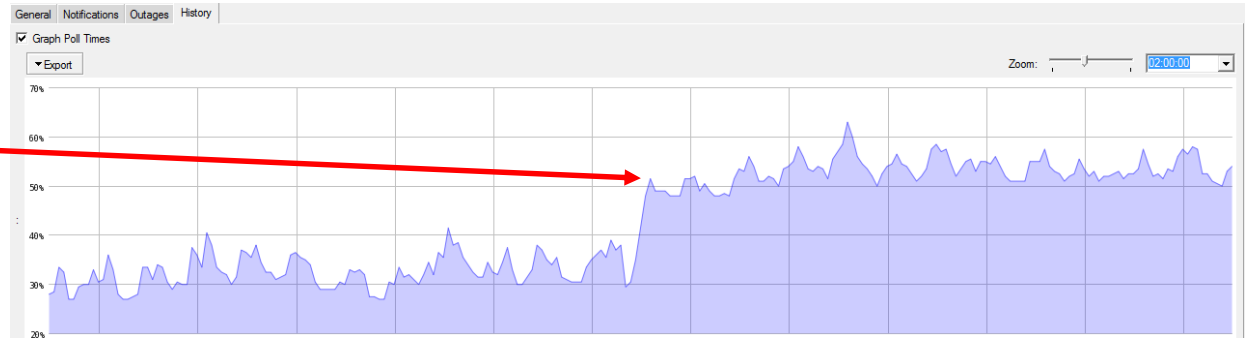
Com no-track





Sem no-track

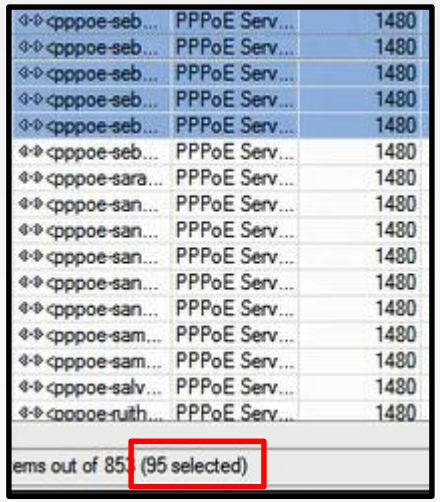


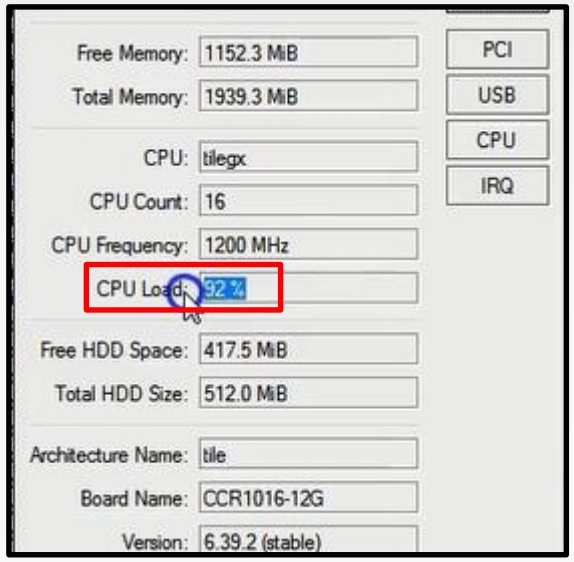


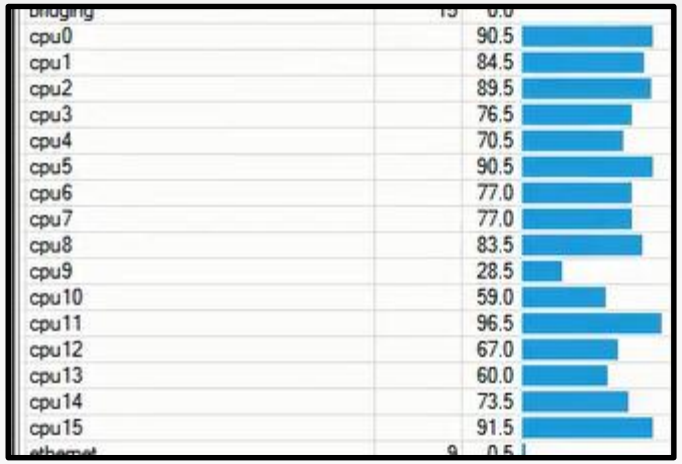
Problemas ao cair vários túneis PPPoE

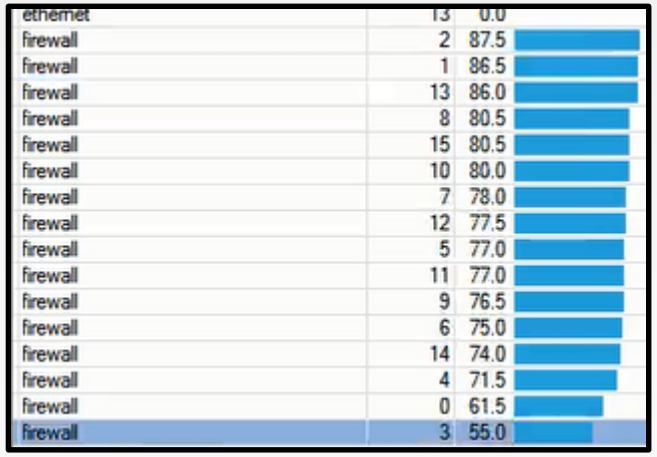
Redes Brasil

- Mais de 120 mil entradas na conntrack





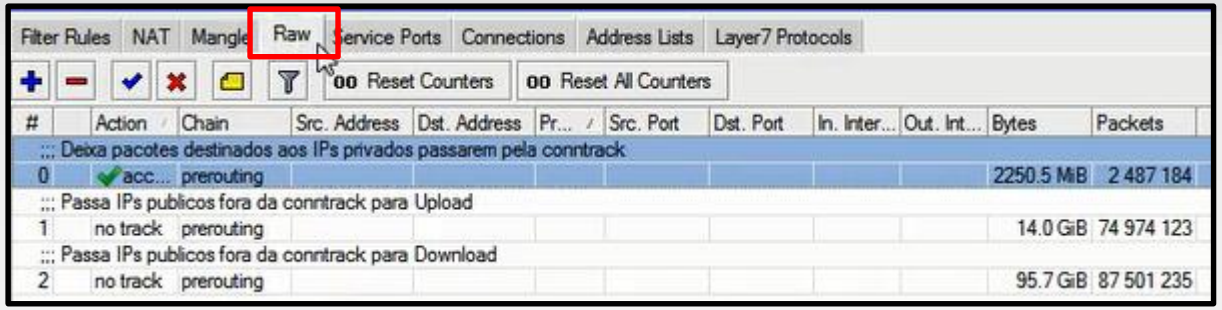




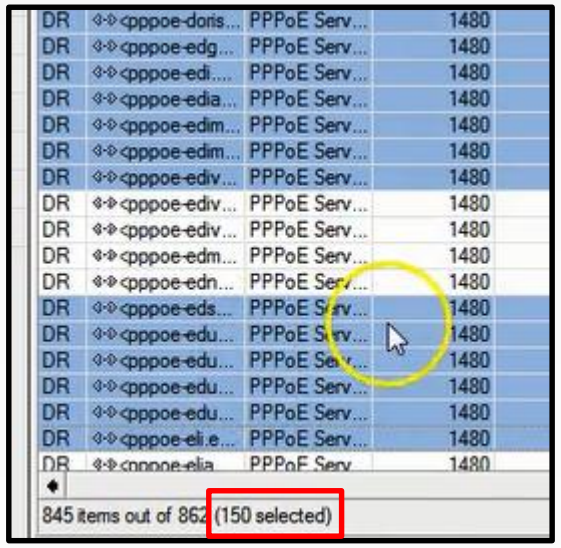
- Roteador ficava travado por mais de 10 minutos

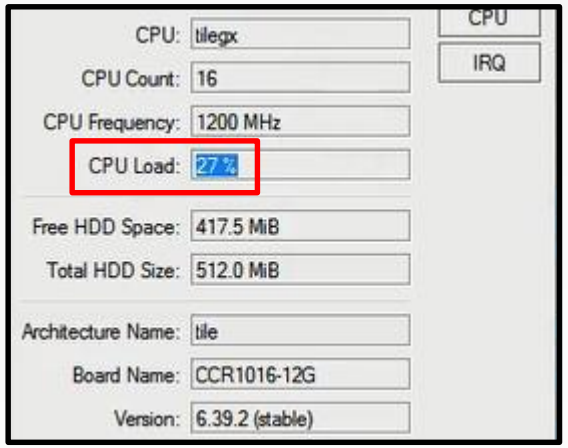
Problemas ao cair vários túneis PPPoE

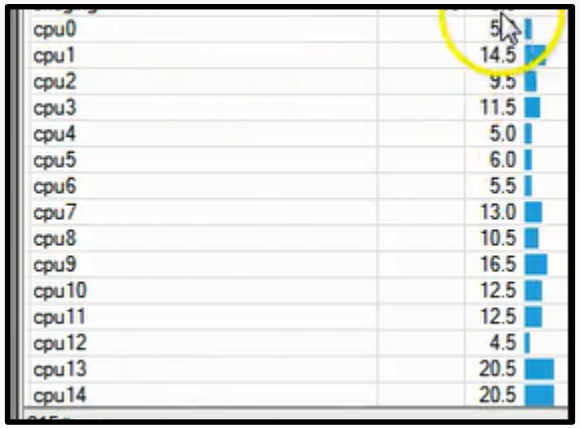
Redes Brasil



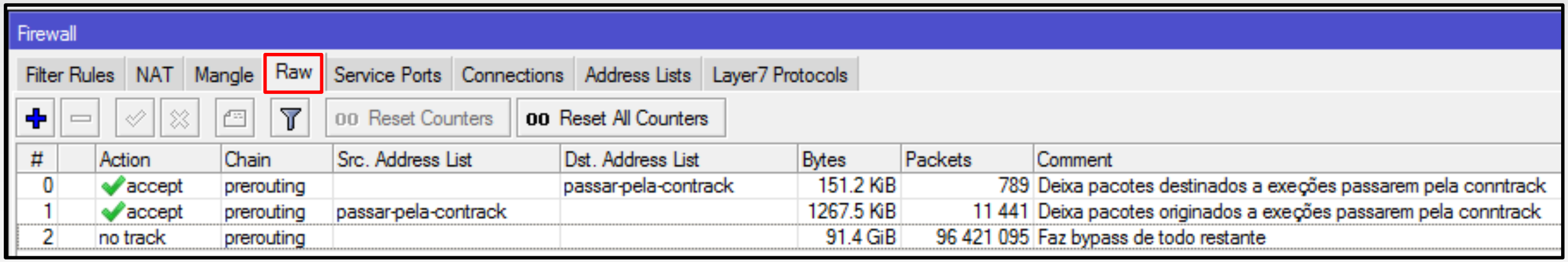
- Pouco mais de 5 mil entradas na Conntrack
- Sem travamentos







Regras de no-track



#	Action	Chain	Src. Address List	Dst. Address List	Bytes	Packets	Comment
0	accept	prerouting		passar-pela-contrack	151.2 KiB	789	Deixa pacotes destinados a exeções passarem pela conntrack
1	accept	prerouting	passar-pela-contrack		1267.5 KiB	11 441	Deixa pacotes originados a exeções passarem pela conntrack
2	no track	prerouting			91.4 GiB	96 421 095	Faz bypass de todo restante

Comandos

```
/ip firewall raw
add action=accept chain=prerouting comment="Deixa pacotes destinados a exe\E7\F5es passarem pela conntrack" dst-address-list=passar-pela-contrack
add action=accept chain=prerouting comment="Deixa pacotes originados a exe\E7\F5es passarem pela conntrack" src-address-list=passar-pela-contrack
add action=notrack chain=prerouting comment="Faz bypass de todo restante"
```

Resumo para ter mais desempenho.

Redes Brasil

Desativar a Conntrack

- Sem NAT
- Sem marcas de conexão
- Sem analise de estado de conexões.

Fasttrack

- Sem controle de banda
- Sem filtros no firewall
- Salta alguns recursos, mas deixa os pacotes passarem pela conntrack.

No-track

- Controle de banda
- Filtros de firewall
- Preservar alguns recursos e salta a conntrack para um tráfego específico

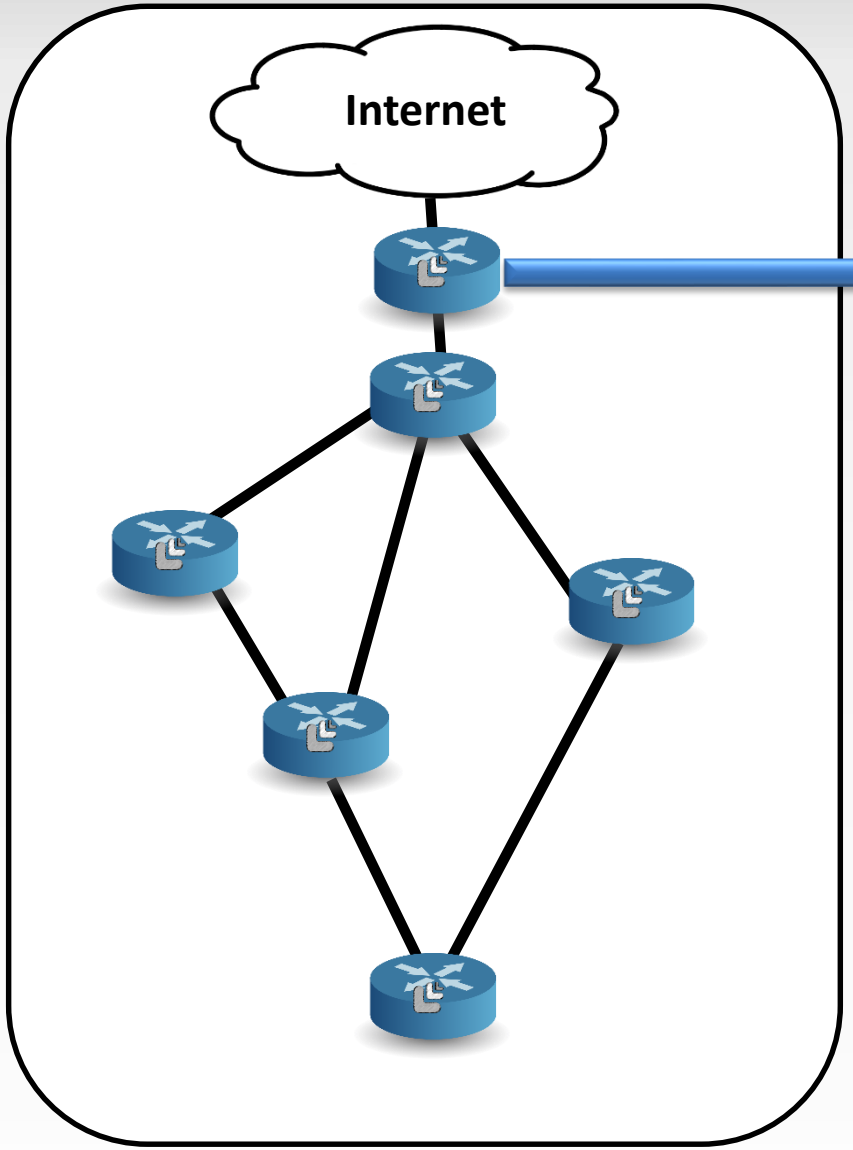
Fast-path

Se você não usa:

- Conntrack
- Firewall
- Queues
- VRFs
- HotSpot
- IPSec

Onde aplicar o FastPath?

Redes Brasil



Não utiliza os recursos abaixo?

Firewall

Controle de banda

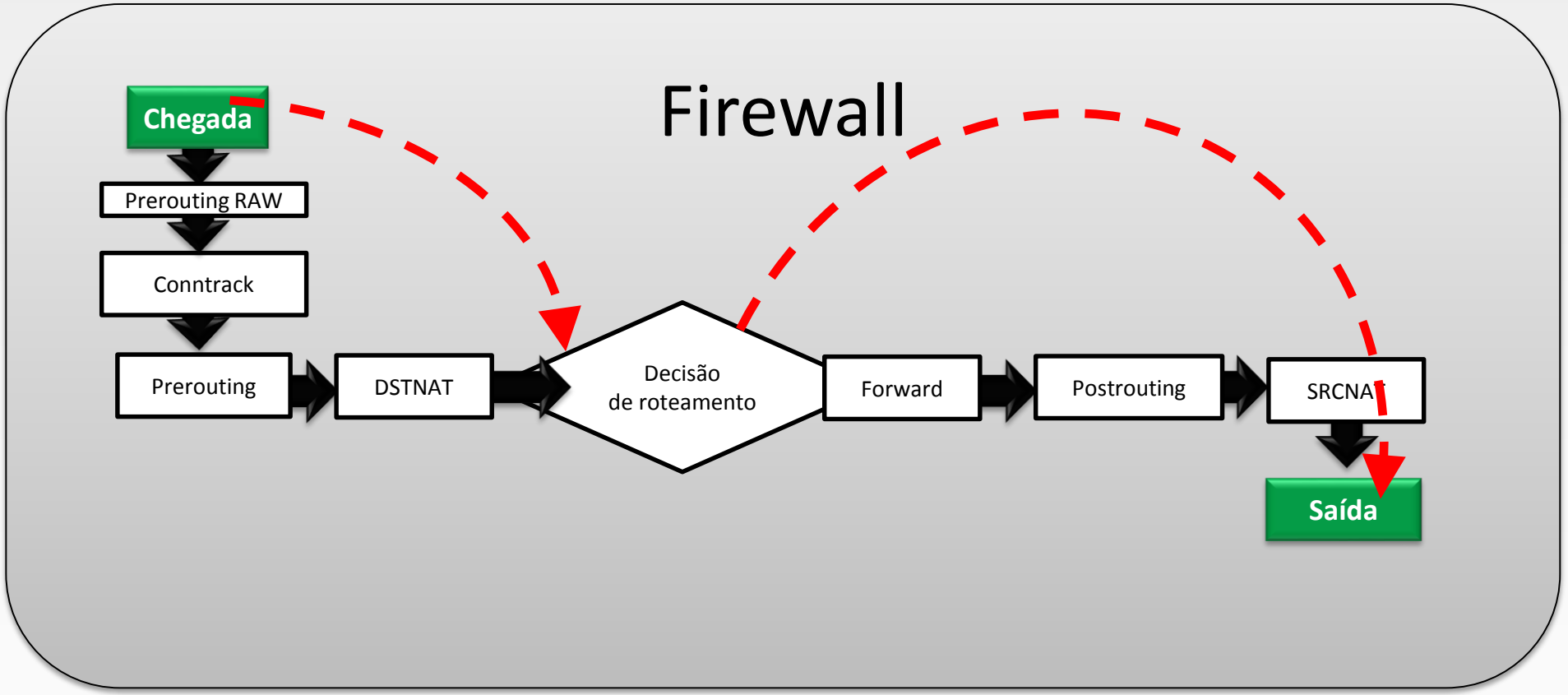
VRF

IPSec

FastPath

- A função de **fastpath** permite encaminhar pacotes sem processamento adicional no Kernel Linux.
- Com essa funcionalidade ativada conseguimos melhorar significativamente a velocidade de encaminhamento de pacotes e reduzir muito a sobrecarga no CPU.
- Fastpath será automaticamente usado se as condições abaixo forem satisfeitas.
  - firewal rules não estar configurado.;
  - firewall address lists não estar configurado.;
  - Simple e queue trees with parent=global não estar configurado.;
  - no mesh, metarouter interface configuration;
  - sniffer, torch and traffic generator is not running;
  - connection tracking não estar ativa;
  - ip accounting is disabled (/ip accounting enabled=no);
  - VRFs are not set (/ip route vrf is empty);
  - Hotspot is not used (/ip hostspot has no interfaces);
  - IpSec policies não estar configurado. (ROS v6.8);
  - /tool mac-scan is not actively used;
  - /tool ip-scan is not actively used;
  - route cache must be enabled

Analogia do fluxo com fastpath



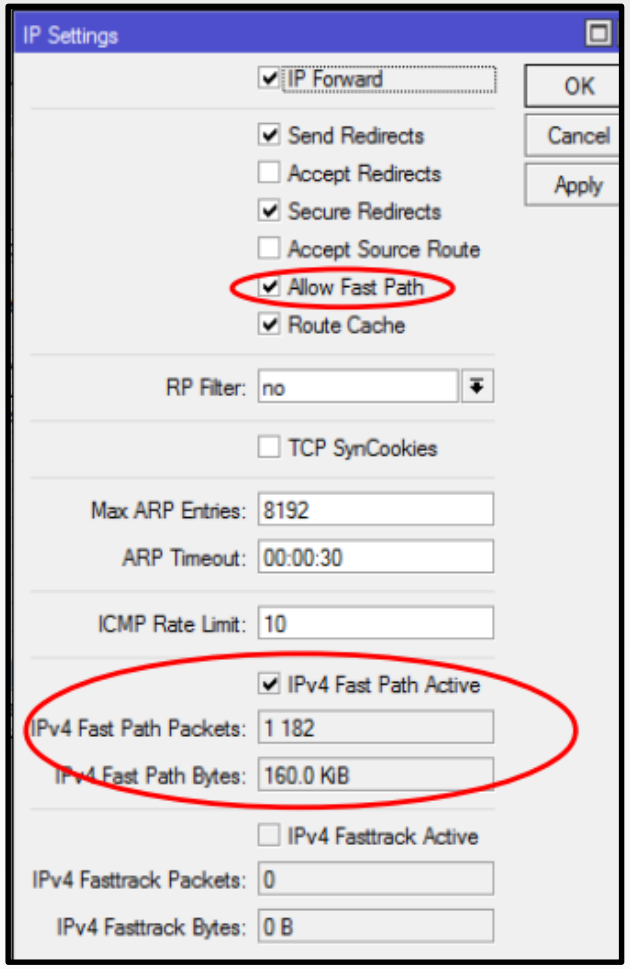
Testes de performance com fastpath.

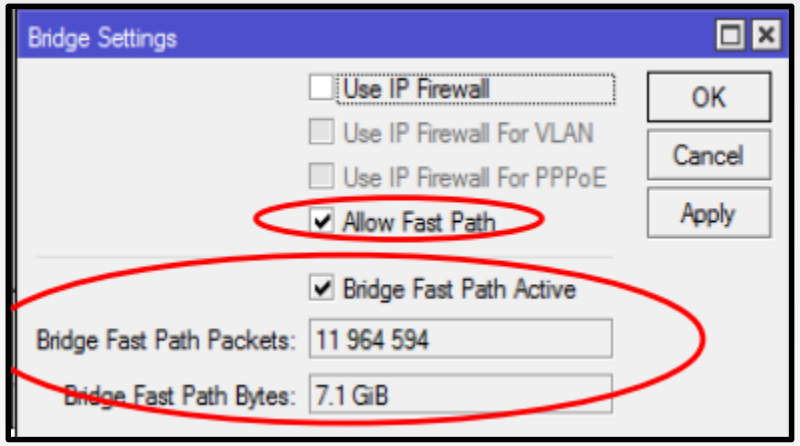
Redes Brasil

RB3011UiAS-RM		IPQ-8064 All port test					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none (fast path)	325.0	3,946.8	939.8	3,849.4	1,530.2	783.5
Bridging	25 bridge filter rules	325.0	3,946.8	384.2	1,573.7	348.6	178.5
Routing	none (fast path)	325.0	3,946.8	939.8	3,849.4	1,437.6	736.1
Routing	25 simple queues	325.0	3,946.8	419.6	1,718.7	419.7	214.9
Routing	25 ip filter rules	202.0	2,453.1	204.1	836.0	188.4	96.5

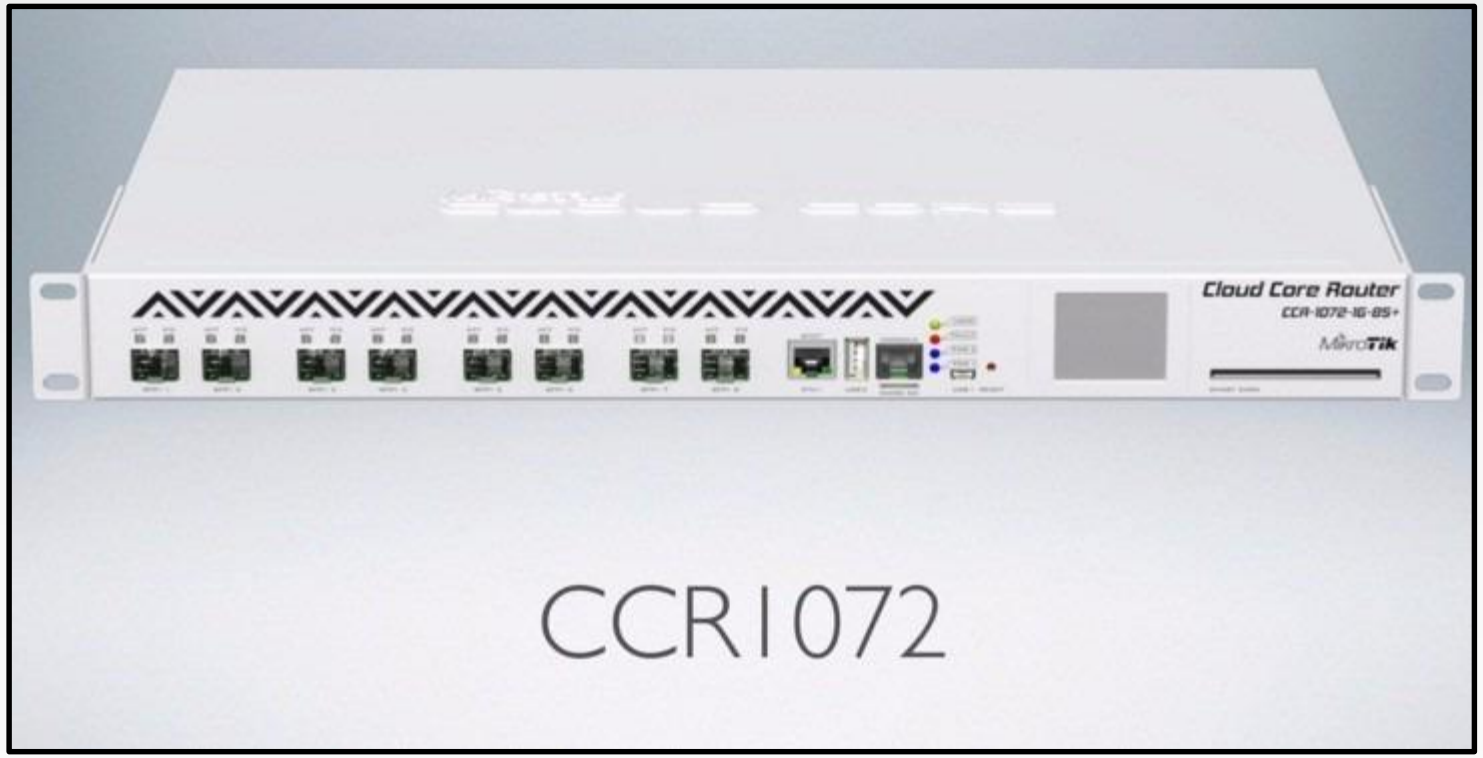
RB1100Dx4		AL21400 1G all port test					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none (fast path)	606.5	7,365.3	1,736.4	7,112.3	5,509.7	2,821.0
Bridging	25 bridge filter rules	606.5	7,365.3	1,107.8	4,537.5	1,153.2	590.4
Routing	none (fast path)	606.5	7,365.3	1,736.4	7,112.3	5092.3	2,607.3
Routing	25 simple queues	606.5	7,365.3	933.6	3,824.0	960.3	491.7
Routing	25 ip filter rules	543.7	6,602.7	561.8	2,301.1	564.6	289.1

Ativando FastPath





Roteador com FastPath



www.redesbrasil.com

Página no

facebook

Canal do

YouTube