a.alive SOLUTIONS

Os maiores equívocos cometidos pelos usuários na hora de usar os principais recursos e ferramentas do RouterOS.

Minha "guerra santa" contra o ***masquerade!!***

MUM Brasil 2017

Sobre o apresentador

Guilherme Ramires

MikroTik Official Trainer Partner - Riga, Latvia (2010)

MikroTik Official Consultant (2009)

MikroTik Academy Coordinator (2013)

MikroTik Certifications: MTCNA, MTCWE, MTCRE, MTCTCE, MTCINE, MTCUME e MTCIPv6

Graduação: Analista de sistemas

Apresentações nos MUMs:

2011 (Sao Paulo), 2012 (Natal/RN), 2013 (Zagreb – Croatia)

2013 (Curitiba/PR), 2014 (México), 2014 (Fortaleza/CE) e 2015 (Florianopólis/SC)

Treinamentos fora do Brasil:

Quito/Equador – MTCUME e MTCINE (2013 and 2014) Venice/Italy – MTCTCE e MTCUME (2014)

Cordoba/Argentina – MTCINE (2014)

Mexico City e Guadalajara/Mexico – MTCINE (2013, 2014 e 2016)

Prague/Chec. Republic – MTCUME e CapsMan (2015)

Milan/Itália – MTCNA e MTCUME (2017)

Objetivos dessa apresentação

- Ajudar você a entender e diagnosticar os erros de configuração mais comuns no RouterOS

- Mostrar as corretas aplicações de diversos recursos do RouterOS para evitar outros equívocos

- Demonstrar como é possível utilizar as últimas novidades das novas versões

- Reduzir o número de emails aberto no suporte devido a configurações equivocadas!

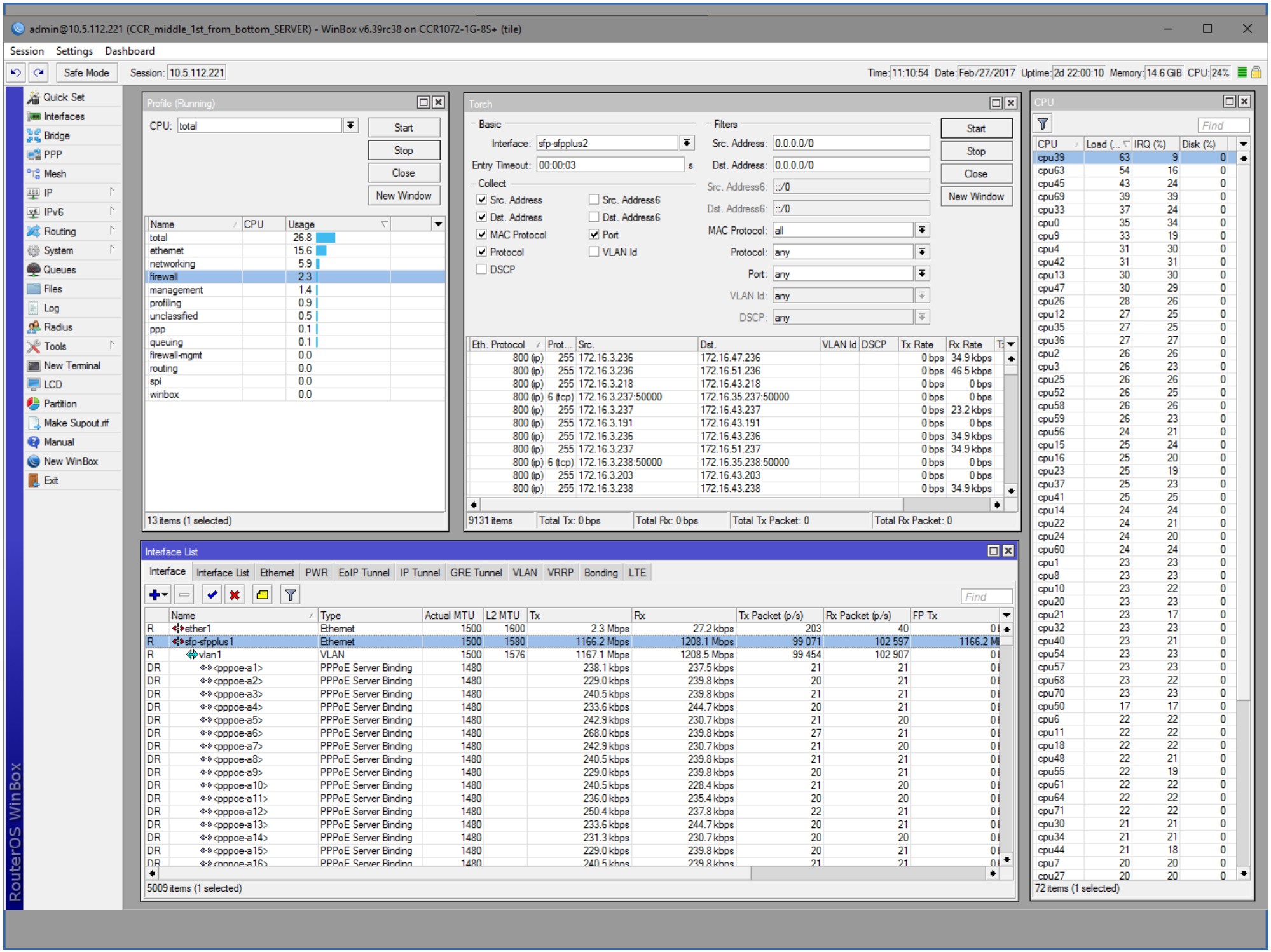
Sobre esta apresentação

- Essa apresentação tem como base as estatísticas do maior número de tickets enviados ao support@mikrotik.com

- Os exemplos demonstrados estarão comprimidos/combinados/simplificados para atender a demanda de tempo e de recursos desta apresentação

- Nesta apresentação vamos demonstrar configurações equivocadas e corrigidas.

(Por favor!!! Não se confunda!!)


admin@10.5.112.221 (CCR_middle_1st_from_bottom_SERVER) - WinBox v6.39rc38 on CCR1072-1G-8S+ (tile)
Session Settings Dashboard
Safe Mode
Session: 10.5.112.221
Time: 11:10:54 Date: Feb/27/2017 Uptime: 2d 22:00:10 Memory: 14.6 GiB CPU: 24%
Quick Set
Interfaces
Bridge
PPP
Mesh
IP
IPv6
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
Partition
Make Supout.rif
Manual
New WinBox
Exit
RouterOS WinBox
Profile (Running)
CPU: total
Start
Stop
Close
New Window
Name CPU Usage
total 26.8
ethernet 15.6
networking 5.9
firewall 2.3
management 1.4
profiling 0.9
unclassified 0.5
ppp 0.1
queuing 0.1
firewall-mgmt 0.0
routing 0.0
spi 0.0
winbox 0.0
13 items (1 selected)
Torch
Basic
Interface: sfp-sfpplus2
Entry Timeout: 00:00:03 s
Collect
Src. Address
Dst. Address
MAC Protocol
Protocol
DSCP
Src. Address6
Dst. Address6
Port
VLAN Id
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
Start
Stop
Close
New Window
Eth. Protocol Prot... Src. Dst. VLAN Id DSCP Tx Rate Rx Rate
800 (ip) 255 172.16.3.236 172.16.47.236 0 bps 34.9 kbps
800 (ip) 255 172.16.3.236 172.16.51.236 0 bps 46.5 kbps
800 (ip) 255 172.16.3.218 172.16.43.218 0 bps 0 bps
800 (ip) 6 (tcp) 172.16.3.237:50000 172.16.35.237:50000 0 bps 0 bps
800 (ip) 255 172.16.3.237 172.16.43.237 0 bps 23.2 kbps
800 (ip) 255 172.16.3.191 172.16.43.191 0 bps 0 bps
800 (ip) 255 172.16.3.236 172.16.43.236 0 bps 34.9 kbps
800 (ip) 255 172.16.3.237 172.16.51.237 0 bps 34.9 kbps
800 (ip) 6 (tcp) 172.16.3.238:50000 172.16.35.238:50000 0 bps 0 bps
800 (ip) 255 172.16.3.203 172.16.43.203 0 bps 0 bps
800 (ip) 255 172.16.3.238 172.16.43.238 0 bps 34.9 kbps
9131 items
Total Tx: 0 bps
Total Rx: 0 bps
Total Tx Packet: 0
Total Rx Packet: 0
CPU
Find
CPU Load (... IRQ (%) Disk (%)
cpu39 63 9 0
cpu63 54 16 0
cpu45 43 24 0
cpu69 39 39 0
cpu33 37 24 0
cpu0 35 34 0
cpu9 33 19 0
cpu4 31 30 0
cpu42 31 31 0
cpu13 30 30 0
cpu47 30 29 0
cpu26 28 26 0
cpu12 27 25 0
cpu35 27 25 0
cpu36 27 27 0
cpu2 26 26 0
cpu3 26 23 0
cpu25 26 26 0
cpu52 26 25 0
cpu58 26 26 0
cpu59 26 23 0
cpu56 24 21 0
cpu15 25 24 0
cpu16 25 20 0
cpu23 25 19 0
cpu37 25 23 0
cpu41 25 25 0
cpu14 24 24 0
cpu22 24 21 0
cpu24 24 20 0
cpu60 24 24 0
cpu1 23 23 0
cpu8 23 23 0
cpu10 23 22 0
cpu20 23 23 0
cpu21 23 17 0
cpu32 23 23 0
cpu40 23 21 0
cpu54 23 23 0
cpu57 23 23 0
cpu68 23 22 0
cpu70 23 23 0
cpu50 17 17 0
cpu6 22 22 0
cpu11 22 22 0
cpu18 22 22 0
cpu48 22 21 0
cpu55 22 19 0
cpu61 22 22 0
cpu64 22 22 0
cpu71 22 22 0
cpu30 21 21 0
cpu34 21 21 0
cpu44 21 18 0
cpu7 20 20 0
cpu27 20 20 0
72 items (1 selected)
Interface List
Interface Interface List Ethernet PWR EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE
Find
Name Type Actual MTU L2 MTU Tx Rx Tx Packet (p/s) Rx Packet (p/s) FP Tx
R ether1 Ethernet 1500 1600 2.3 Mbps 27.2 kbps 203 40 0
R sfp-sfpplus1 Ethernet 1500 1580 1166.2 Mbps 1208.1 Mbps 99 071 102 597 1166.2 M
R vlan1 VLAN 1500 1576 1167.1 Mbps 1208.5 Mbps 99 454 102 907 0
DR <pppoe-a1> PPPoE Server Binding 1480 238.1 kbps 237.5 kbps 21 21 0
DR <pppoe-a2> PPPoE Server Binding 1480 229.0 kbps 239.8 kbps 20 21 0
DR <pppoe-a3> PPPoE Server Binding 1480 240.5 kbps 239.8 kbps 21 21 0
DR <pppoe-a4> PPPoE Server Binding 1480 233.6 kbps 244.7 kbps 20 21 0
DR <pppoe-a5> PPPoE Server Binding 1480 242.9 kbps 230.7 kbps 21 20 0
DR <pppoe-a6> PPPoE Server Binding 1480 268.0 kbps 239.8 kbps 27 21 0
DR <pppoe-a7> PPPoE Server Binding 1480 242.9 kbps 230.7 kbps 21 20 0
DR <pppoe-a8> PPPoE Server Binding 1480 240.5 kbps 239.8 kbps 21 21 0
DR <pppoe-a9> PPPoE Server Binding 1480 229.0 kbps 239.8 kbps 20 21 0
DR <pppoe-a10> PPPoE Server Binding 1480 240.5 kbps 228.4 kbps 21 20 0
DR <pppoe-a11> PPPoE Server Binding 1480 236.0 kbps 235.4 kbps 20 20 0
DR <pppoe-a12> PPPoE Server Binding 1480 250.4 kbps 237.8 kbps 22 21 0
DR <pppoe-a13> PPPoE Server Binding 1480 233.6 kbps 244.7 kbps 20 21 0
DR <pppoe-a14> PPPoE Server Binding 1480 231.3 kbps 230.7 kbps 20 20 0
DR <pppoe-a15> PPPoE Server Binding 1480 229.0 kbps 239.8 kbps 20 21 0
DR <pppoe-a16> PPPoE Server Binding 1480 240.5 kbps 239.8 kbps 21 21 0
5009 items (1 selected)

a.alive SOLUTIONS

“CPU alta usando L7”

“CPU alta usando L7”

- ```
  /ip firewall layer7-protocol
     add name=youtube regexp="^.+(youtube).*\$"
     add name=facebook regexp="^.+(facebook).*\$"
  ```
- ```
  /ip firewall filter
     add action=drop chain=forward layer7-
  protocol=facebook
     add action=drop chain=forward layer7-
  protocol=youtube
  ```

Errado!!!

Analise do problema

- Problema:

– Alta carga de CPU, aumento de latência, perda de pacotes, jitter ruim e youtube/facebook não são bloqueados

- Diagnostico:

– “/tool profile” mostra alta carga de cpu no processo **layer7**

- Motivo:

– Cada **conexão** é re-verificada infinitas vezes!

– A regra de Layer7 está posicionada incorretamente e verificando a totalidade do tráfego

Layer7

- Layer7-protocol é um método de busca de parametros nas streams **ICMP/TCP/UDP**

- Quando existe um ”match” na regra de Layer7 o router coleta os próximos 10 pacotes ou 2KB de cada conexão e busca pelos parametros informados em cima dos dados coletados

- Os parametros de Layer7 disponiveis na Internet são destinados aos 10 primeiros pacotes ou 2KB de informação de cada conexão.

Implementação correta

- ```
  /ip firewall mangle
  add action=mark-connection chain=prerouting protocol=udp
  dst-port=53 connection-mark=no-mark layer7-
  protocol=youtube new-connection-mark=youtube_conn
  passthrough=yes
  ```
- ```
  add action=mark-packet chain=prerouting connection-
  mark=youtube_conn new-packet-mark=youtube_packet
  passthrough=no
  ```

- ```
  /ip firewall filter
  add action=drop chain=forward packet-mark=youtube_packet
  add action=drop chain=input packet-mark=youtube_packet
  ```

  (e o mesmo para o facebook)
  ```

a.alive SOLUTIONS

“Queues não funcionam corretamente”

“Queues não funcionam corretamente”

- ```
  /ip address
  add address=10.0.0.1/24 interface=local-one
  add address=10.0.1.1/24 interface=local-two
  ```

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

- ```
  /queue simple
  add max-limit=10M/10M dst=10.0.0.2/32
  add max-limit=10M/10M dst=10.0.0.3/32
  add max-limit=10M/10M dst=10.0.0.4/32
  ```

Errado!!!
  ```

Analise do problema

- Problema:

– Queues funcionam somente quando usa o “/tool torch”, ou quando o fasttrack está desabilitado;

– Somente tráfego de download é capturado;

– Tráfego lan-to-lan também é capturado.

- Diagnostico:

– Contadores nas queues e na regra de fasttrack

- Possíveis motivos:

– A regra do Fasttrack está capturando TODO tráfego

– O **target** da simple queue DEVE ser especificado

FastTrack

- Entradas na Conntrack possuem a flag “Fasttracked”
- Implementadas através da ação “fasttrack-connection” no firewall filter/mangle
- Os pacotes das conexões com flag “Fasttracked” tem permissão de usar o FastPath
- Funciona somente com IPv4/TCP e IPv4/UDP
- Tráfego que é encaminhado via FastPath vai ignorar firewall, queues, etc…
- Alguns poucos pacotes ainda vão seguir o fluxo regular do firewall para manutenção das entradas da conntrack

Simple queue “target”

- O “target” na simple queue é a única opção que determina a direção do tráfego
- Se o ”target” não for especificado(0.0.0.0/0) todo tráfego será capturado na direçãdo do download, já que todo download têm target 0.0.0.0/0
- A opção “dst” é somente um filtro adicional e não determina a direção do tráfego

Implementação correta

- ```
  /ip firewall filter
  add chain=forward action=fasttrack-connection
  connection-state=established,related in-
  interface=local-one out-interface=local-two
  add chain=forward action=fasttrack-connection
  connection-state=established,related in-
  interface=local-two out-interface=local-one
  add chain=forward action=accept connection-
  state=established,related
  ```

- ```
  /queue simple
  add max-limit=10M/10M target=10.0.0.2/32
  add max-limit=10M/10M target=10.0.0.3/32
  add max-limit=10M/10M target=10.0.0.4/32
  ```

“CPU alta no PPPoE server”

“CPU alta no PPPoE server”

- 3000 pppoe-clients em uma rede 10.0.0.0/20
- Caixas conectadas via redes 172.16.x.0/24 a outros PPPoE servers com redes 10.x.0.0/20 para outros clientes pppoe
- Todos PPPoE servers e gateways na mesma area backbone e ”redistribute-connected-routes” na instância

```
/routing ospf network
    add network=172.16.1.0/24 area=backbone
    add network=10.0.0.0/20 area=backbone
```

Errado d+!!!

Analise do problema

- Problema:

– CPU sobrecarregada, desconexões dos PPPoE clients, clientes não alcançam as velocidades desejada, as vezes é quase impossível acessar a caixa

- Diagnostico:

– A ferramenta /tool profile mostra o processo “routing” em alguma CPU em 100% o tempo todo, outros cores também alcançam 100% algumas vezes no processo “ppp” e “networking”

- Motivo:

– O OSPF está sendo spamado com os updates de rotas /32 dos clientes PPPoE

OSPF e PPPoE

- Todos protocolos de roteamento dinâmico (mais precisamente o **routing table updates** e calculos do protocolo) são limitados a um único core
- Toda vez que um pppoe-client conecta ou disconecta, é criado ou removido uma rota /32. Se está rota é pertencente a uma network do OSPF, o OSPF necessita um update
- Toda vez que um pppoe-client conecta ou disconecta uma interface pppoe é criada ou removida das interfaces do OSPF, o que também exige um update do OSPF

Interfaces passivas do OSPF e areas stub

- Areas stub permitem reduzir a quantidade de informações de roteamento inundadas nas areas e rotas externas não inundam areas stub
- Deve-se utilizar o recurso chamado ”area ranges” para agregar as informações das redes para as areas adjacentes, permitindo assim criar somente um sumário de LSA para multiplas rotas e um único aviso é enviado para as demais areas
- **A interface passiva deve ser adicionada para todas interfaces exceto as que efetuam comunicação OSPF com os demais routers**

Implementação correta

- /routing ospf area
  add area-id=0.0.0.1 name=pppoe1 type=stub
- /routing ospf network
  add area=pppoe1 network=10.0.0.0/20
- /routing ospf area range
  add advertise=yes area=pppoe1 range=10.0.0.0/20
- /routing ospf interface
  add interface=all passive=yes

Obs.: LEMBRE-SE de adicionar as interfaces de comunicação OSPF manualmente.

(A rota estática blackhole para a network do pppoe será criada automaticamente pelo MK)

Concentrador subindo demais trafego na porta wan/lan do concentrador

Concentrador subindo demais trafego na porta wan/lan

- O problema recorre da mesma configuração equivocada explicada anteriormente.
- Uma vez que você não possui nenhum mecanismo de sumarização que gerencie de forma correta seus pools do PPPoE você poderá sofrer um ataque baseado em loop estático.
- Basta que um IP que não esteja em uso seja requisitado de forma infinita.
- A solução proposta para o problema anterior já resolve também este problema.

“CPU alta no PPPoE server”

“CPU alta no PPPoE server”

- 3000 pppoe-clients em uma rede 10.0.0.0/20
- IP público fixo na interface WAN
- Nat Masquerade
- Nada mais

Errado d+!!!

Analise do problema

- Problema:

– CPU sobrecarregada, desconexões dos PPPoE clients, clientes não alcançam as velocidades desejada, as vezes é quase impossível acessar a caixa.

- Diagnostico:

– /tool profile mostra o processo “firewall” consumindo maior parte da CPU

- Motivo:

– Uso incorreto do masquerade

Masquerade

- **Firewall NAT action=masquerade** é um sub-versão da action=srcnat, designidado especificamente para casos onde o IP público é dinâmico.
- Cada vez que uma interface desconecta e/ou o IP address muda, o router vai rastrear e eliminiar as conexões relacionadas a esta interface/ip na connection tracking.

Implementação correta

- ```
  /ip firewall nat
  add action=src-nat chain=srcnat out-
  interface=<Public> to-addresses=<Public_IP>
  ```
  ```

a.alive SOLUTIONS

“IP Local vazando pra rede pública”

“IP Local vazando pra rede pública”

- Dispositivos multi gateway com politicas de roteamento e failover – (famoso balance)
- IP público estático nas interfaces wan
- Uma regra de masquerade em cada interface wan

Errado!!!

Analise do problema

- Problema:

– Após o failover acontecer, os pacotes com IP privado vazam pra rede pública.

- Diagnostico:

–/tool sniffer

- Motivo:

– Uso incorreto do masquerade ou insuficiente número de regras de salvo guardo

Masquerade

- No disconnect, todas conexões relacionadas na connection tracking são rastreadas e eliminidas
- O próximo pacote de cada conexão eliminida irá entrar no firewall como **connection-state=new**, e o pacote será roteado pra internet pelo próximo link indicado e portanto criará uma nova entrada de conexão
- Quando o link primário retorna, o roteamento é restaurado por ele, então os pacotes pertecentes a conexão existente serão enviados pelo link primário SEM masquerade

Implementação correta

- Use **action=src-nat** ao invés de **action=masquerade** sempre que possível
- Drop pacotes com connection-state=invalid
- Drop pacotes connection-state=new connection-nat-state=!dstnat a partir das interfaces wan
- Crie uma rota **backup** com “blackhole” pra cada routing-mark

a.alive SOLUTIONS

“DNS cache atacado”

“DNS cache atacado”

- ```
  /ip dns
  set allow-remote-requests=yes servers=8.8.8.8
  ```
- ```
  /ip firewall nat
  add action=masquerade chain=srcnat out-
  interface=Internet
  ```
- ```
  /ip firewall filters
  add action=fasttrack-connection chain=forward
  connection-state=established,related
  ```
- … nada mais

- IP público interface wan

Errado!!!
  ```

Analise do problema

- Problema:

– Consumo alto de CPU, tráfego muito alto sem explicação na interface wan

- Diagnostico:

–/tool torch, /tool profile > “dns” com alta carga

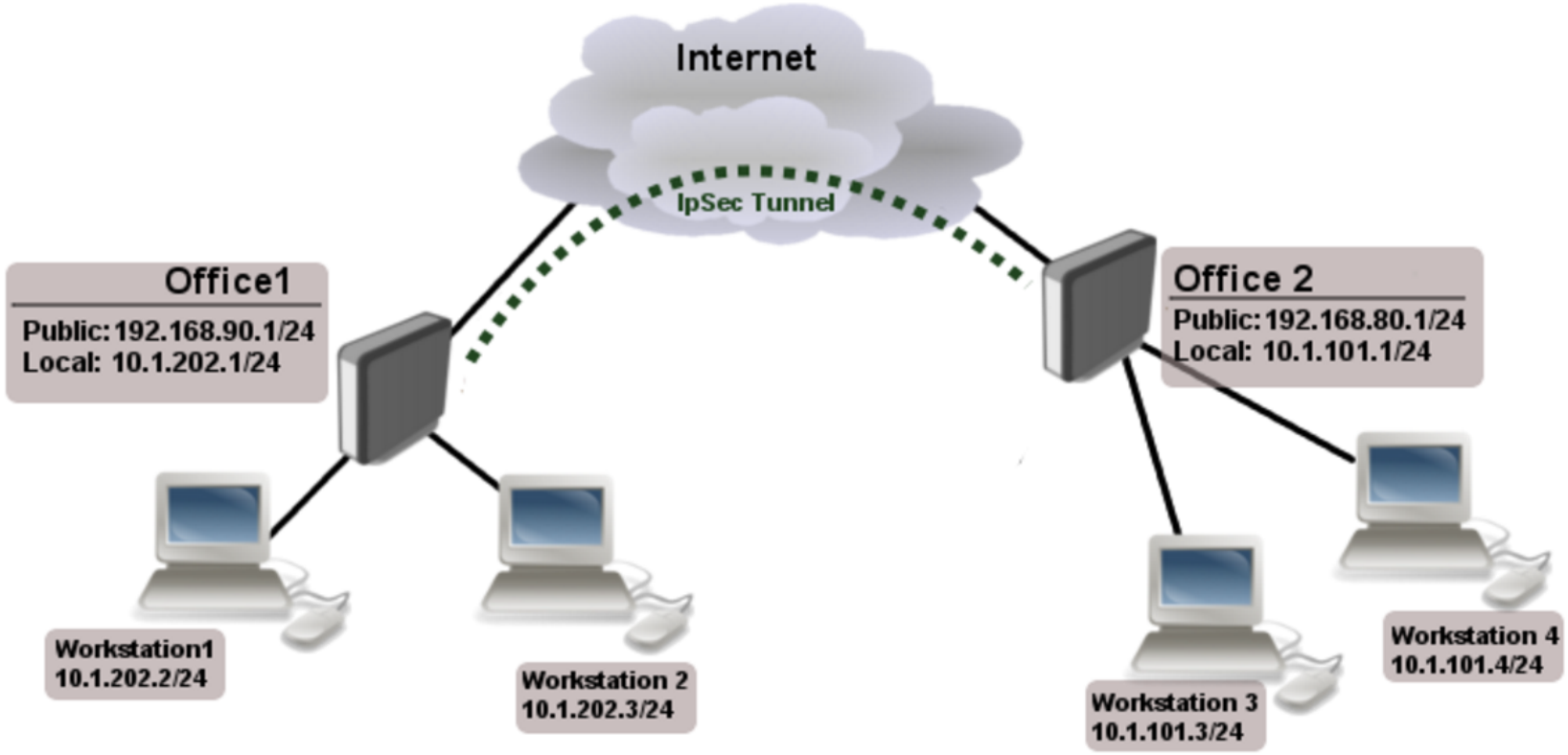
- Motivo:

– Seu router está sendo usado pra resolução de DNS por requisições externas. E possivelmente você está sendo usado como um amplificador de ataque.

Implementação correta

- ```
  /ip firewall filter
  add action=reject chain=input dst-port=53
  protocol=udp reject-with=icmp-port-unreachable
  add action=reject chain=input dst-port=53
  protocol=tcp reject-with=icmp-port-unreachable
  ```

  (e suas demais regras de firewall)

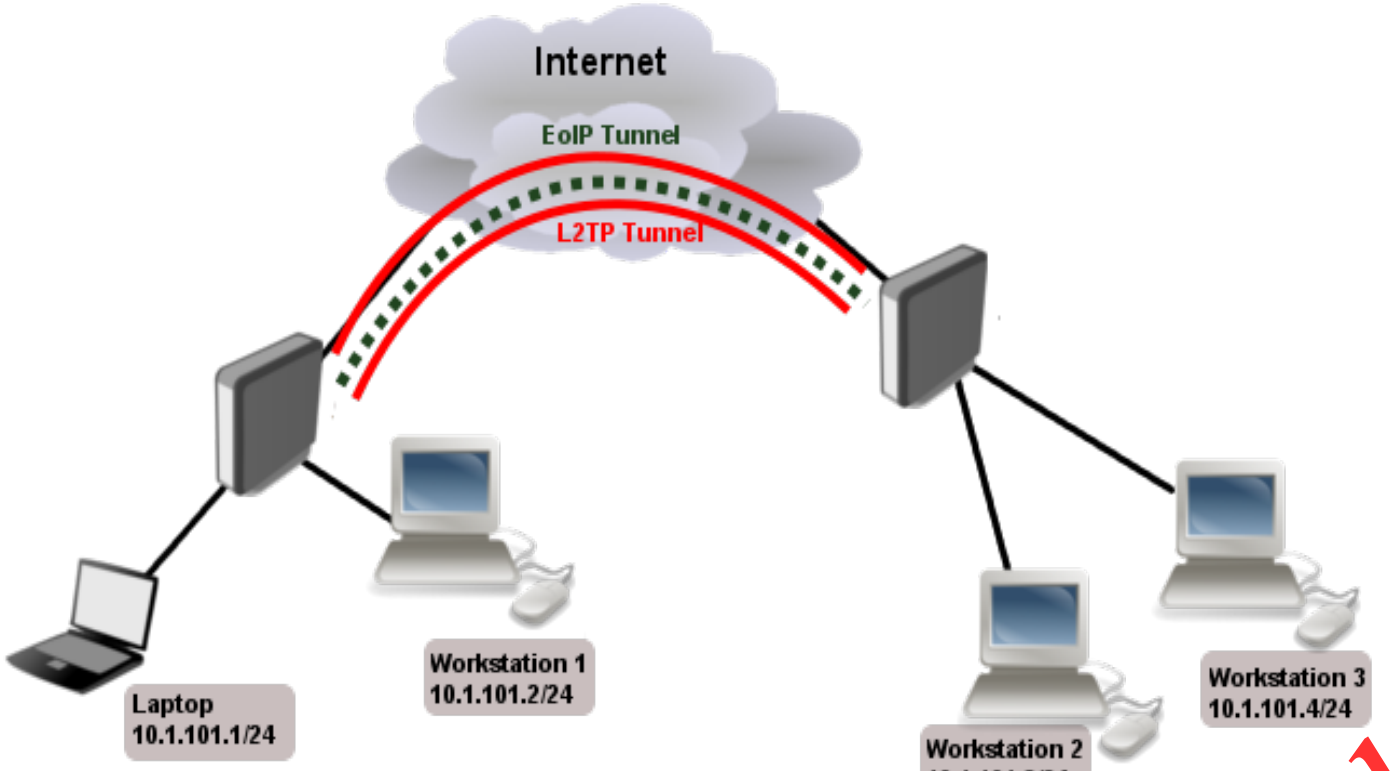
- Obs.: Caso seu router não seja multi-core troque as actions=reject pra action=drop
  ```

“Túnel IPSec não funciona”

“Túnel IPSec não funciona”



- Regra simples de masquerade em ambos os routers

Errado!!!

Analise do problema

- Problema:

– Pacotes IPsec são rejeitados, túnel não pode ser estabelecido

- Diagnostico:

– /tool sniffer

- Motivo:

– Regras de NAT estão alterando o src-address dos pacotes encriptados e/ou o scr-address não correspondem as politicas de IPsec

Raw table

- Firewall RAW permite você seletivamente criar um bypass ou dropar pacotes ANTES da connection tracking e desta forma você reduz significativamente a carga de CPU
- Se o pacote é marcado para dar um bypass na connection tracking:
  - controle de fragmentação dos pacotes não vão ocorrer
  - O NAT será ignorado
  - matchers que dependem da connection tracking não vão funcionar (fasttrack-connection, mark-connection, layer7, etc.)
  - serão marcados como connection-state=untracked

Implementação correta

- ```
  /ip firewall raw
  add action=notrack chain=prerouting src-
  address=10.1.101.0/24 dst-address=10.1.202.0/24

  add action=notrack chain=prerouting src-
  address=10.1.202.0/24 dst-address=10.1.101.0/24
  ```
  ```

a.alive SOLUTIONS

“Por em bridge duas LANs com segurança”

“Por em bridge duas LANs com segurança”



Errado!!!

Analise do problema

- Problema:

– Abertura de páginas muito lenta, velocidades de download baixa, aquela incerteza de que suas informações estão seguras :)

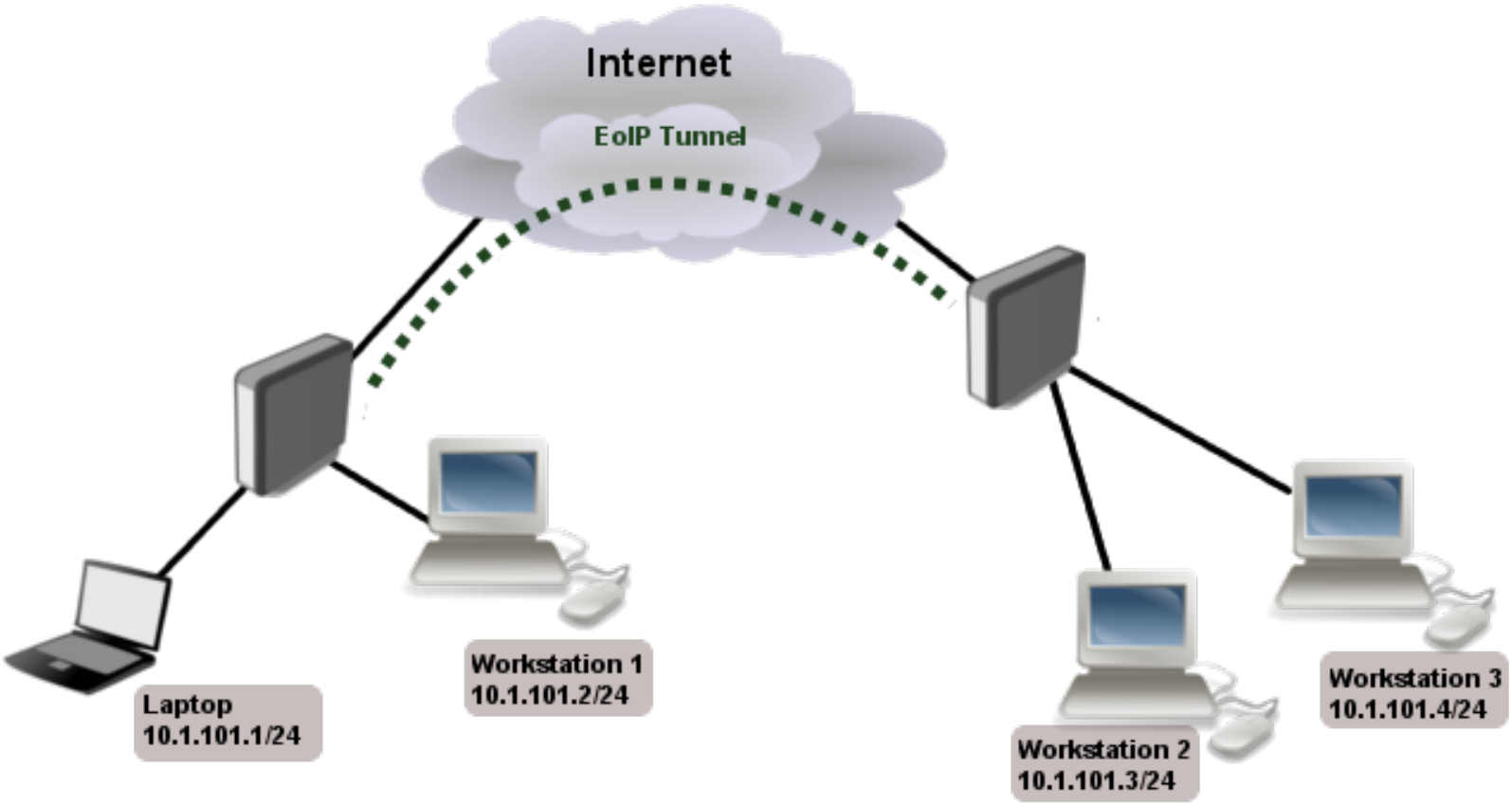
- Diagnostico:

–/tool bandwidth-test, /tool ping com pacotes maiores

- Motivo:

– PPTP/L2TP não são mais seguros, grande overhead causado por 2 túneis, fragmentação, redução de MTU

Implementação correta



- `/interface eoip set ipsec-secret=senha`

(sim… simples assim :D)

CCR HW encryption acceleration

- Completamente novo driver para aceleração de encriptação via hardware no RouterOS v6.39 para as CCR's
- Resolvido o problema para o tráfego out-of-order e performance melhorada. Testes com pacotes UDP de 1400 bytes as melhorias foram:

  - CCR1072 de 9,2Gbps para 13,8Gbps
  - CCR1036 de 3,4Gbps para 7Gbps
  - CCR1009 de 1,5Gbps para 2,2Gbps

a.alive SOLUTIONS

Perguntas???

Obrigado a todos!