

BRAS de alta capacidade + CGNAT Com Mikrotik

MUM 2019 Brasil
Foz Iguaçu - PR

Flávio Gomes Figueira Camacho Junior

- ▶ Brasil, Rio de Janeiro
- ▶ 8 anos de experiencia com Telecomunicações
- ▶ Engenheiro de Rede na empresa TELECALL
- ▶ Consultor de Tecnologia empresa COMTXAI
- ▶ Trainer Oficial Mikrotik
- ▶ Certificações: MTCNA, MTCWE, MTCTCE, MTCUME, MTCIP, MTCINE e MTCSE
- ▶ Contato: flaviocamacho95@gmail.com
- ▶ Contato: +55 (21) 96978-4675
- ▶ <https://mikrotik.com/consultants>



Objetivo

- ▶ Apresentar como implementar uma solução com alta capacidade de cliente banda larga em dispositivos Mikrotik.
 - ▶ Switch de agregação
 - ▶ BRAS para autenticação e limitação de banda
 - ▶ Solução CGNat para todos clientes

Sumári

▶ Apresentação

- ▶ Descrever o que é um BRAS
- ▶ Tipos de BRAS
- ▶ Importância de uma boa solução BRAS para ISP

Introdução

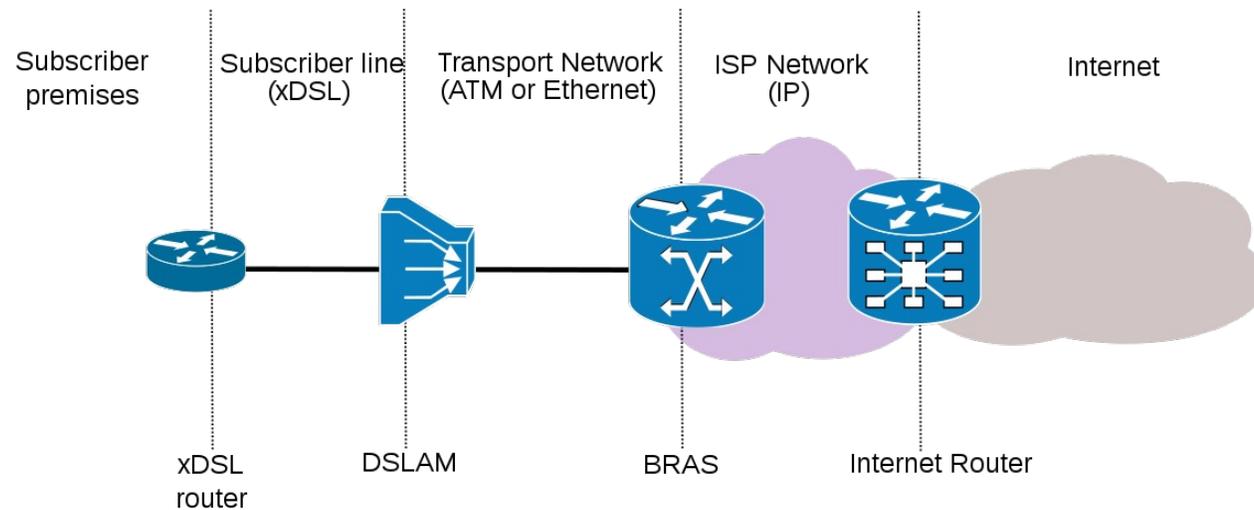
Importância de uma boa solução BRAS para ISP

- ▶ Autenticação de Usuários
- ▶ Exaustão do IPv4
- ▶ Mais com menos
- ▶ IPv6 Ready
- ▶ Pay as you grow (simples)
- ▶ Menos configurações necessárias
- ▶ Estável e resiliente
- ▶ Pronto para mudanças e upgrades
- ▶ Qualidade para os clientes

O que é um BRAS?

Broadband remote access

server



Tipo

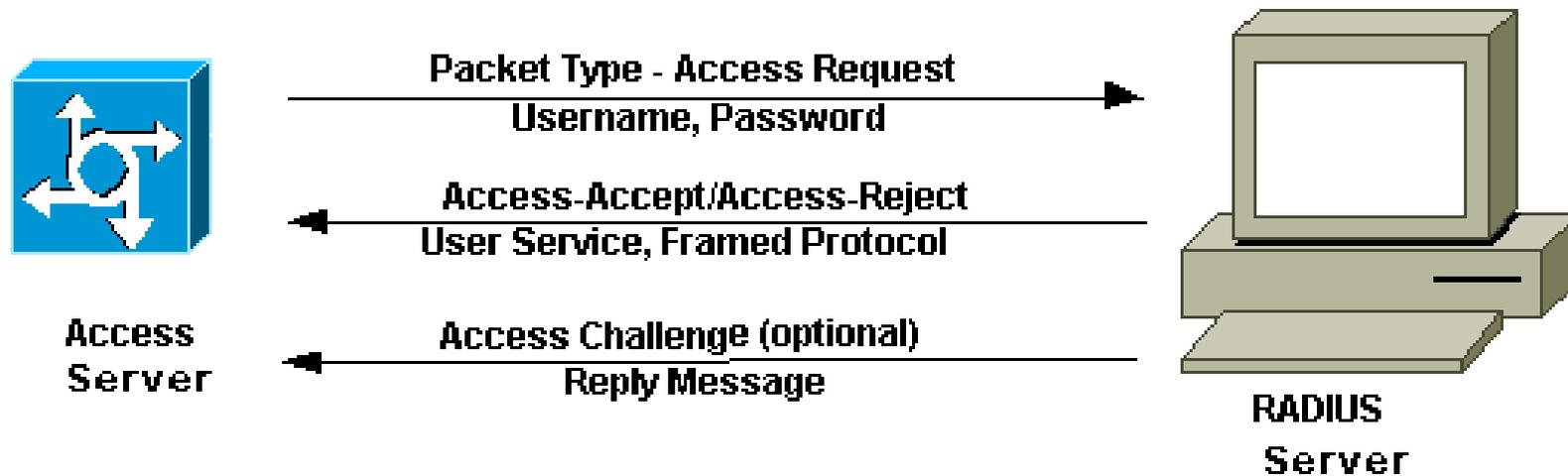
S

- ▶ PPPoE (PPPoE, PPPoA)
- ▶ DHCP
- ▶ DHCP + option 82 (IPoE)
- ▶ Hotspot

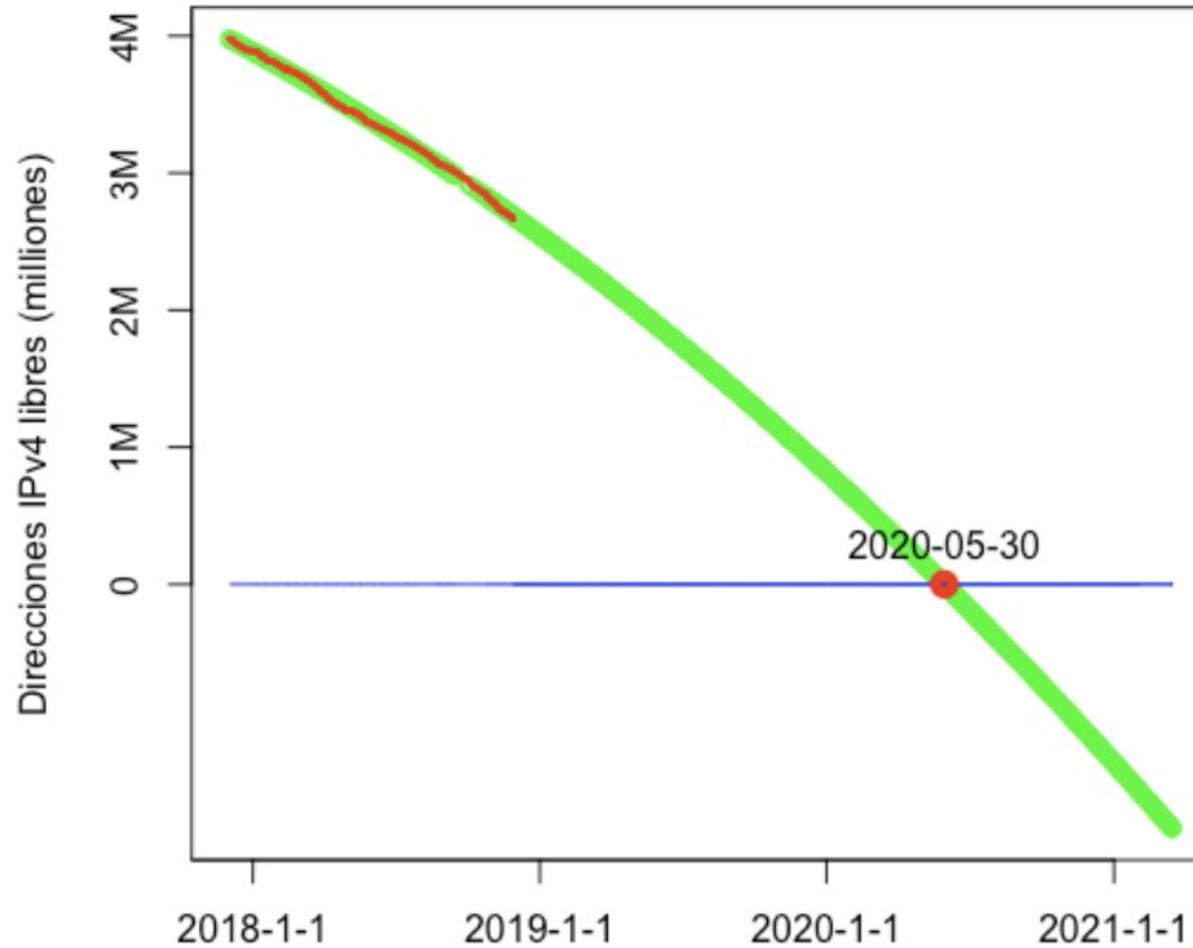
Autenticação dos clientes

- ▶ Bloqueio Automático
- ▶ Bandwidth (Limitação de Banda)
- ▶ Upgrade pelo sistema Radius (CoA)
- ▶ Sem interações/configurações no BRAS

Radius - O que é?



IPv4 Exhaustion



<https://www.lacnic.net/1077/3/lacnic/fases-de-esgotamento-do-ipv4>

Calculando

1 IP = 65535 tcp/udp ports

1 aproximadamente utiliza 300 portas

Então $65535/300 \approx 218$

1 IP público atende 218 clientes

Quanto maior a quantidade de clientes por IP,
maior poderá ser a perda de qualidade no serviço.

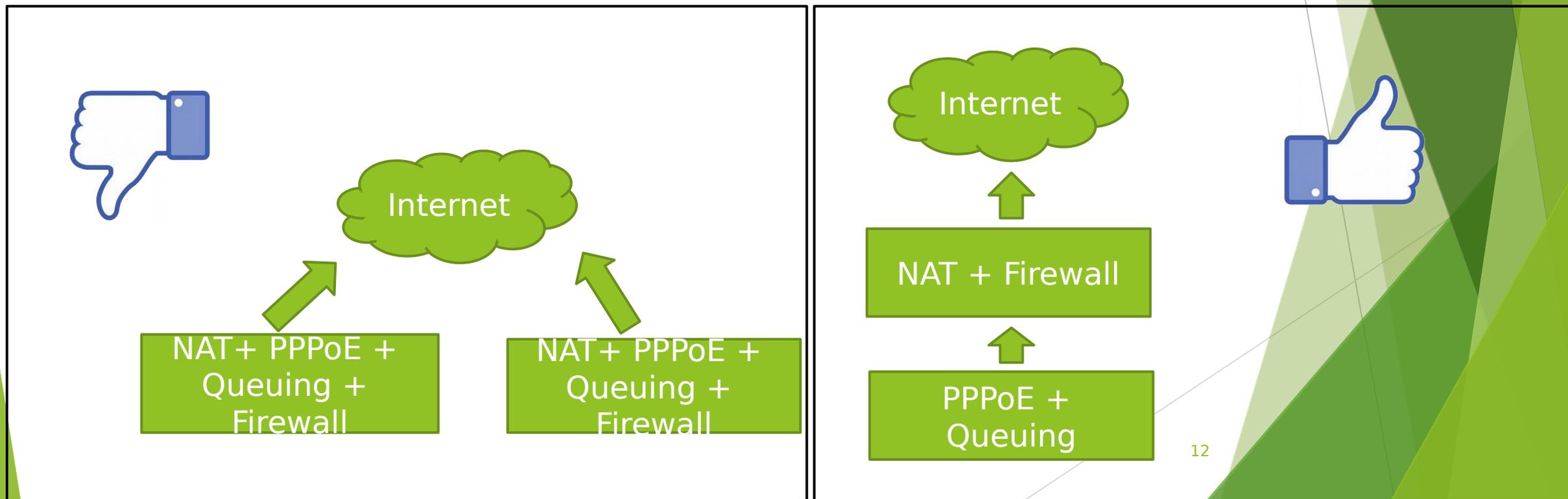
Obter melhor performance

O que é melhor?

2 routers fazendo NAT + Queuing + PPPoE + Firewall

OU

2 routers uma fazendo Queue + PPPoE, e a outra fazendo NAT + Firewall



IPv6 Ready

Dual Stack Network



Pay as you grow



Integração ERP

Integração com RADIUS faz o controle ficar mais SDN

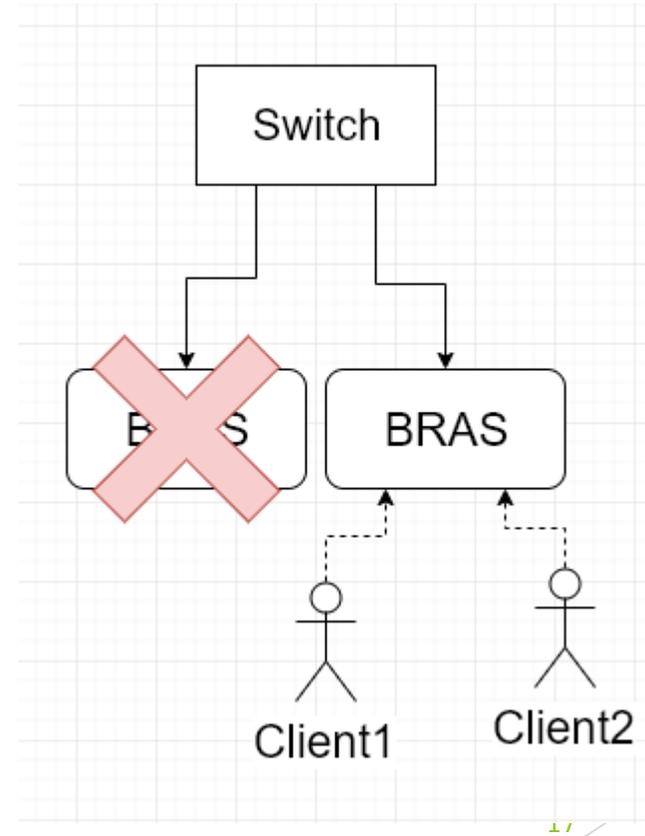
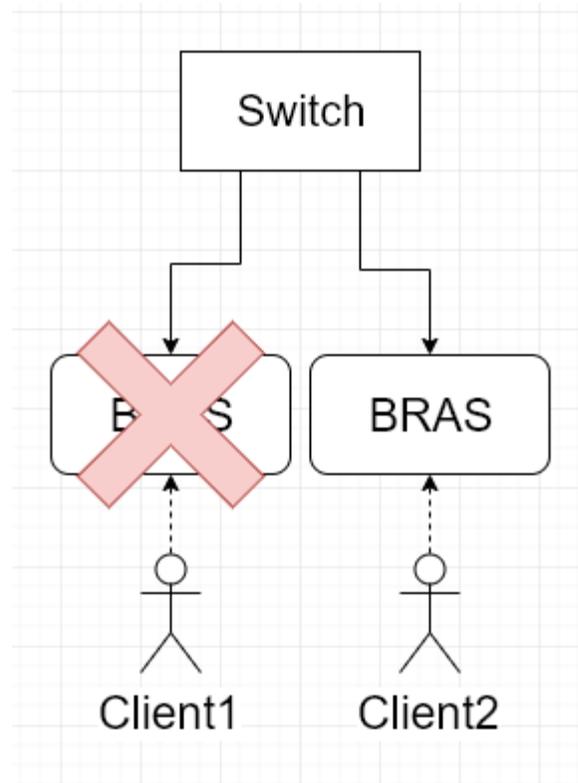
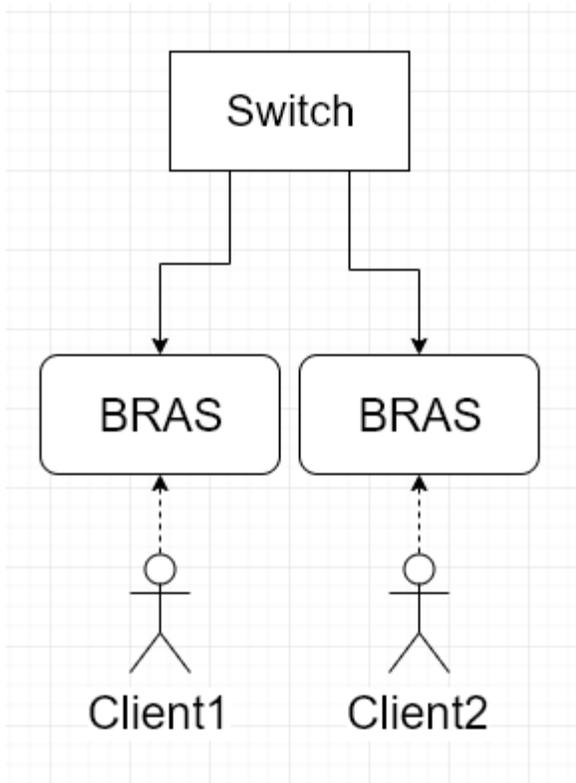


Escalável

O número e os tipos de BRAS são controlados conforme o crescimento.



Resiliente

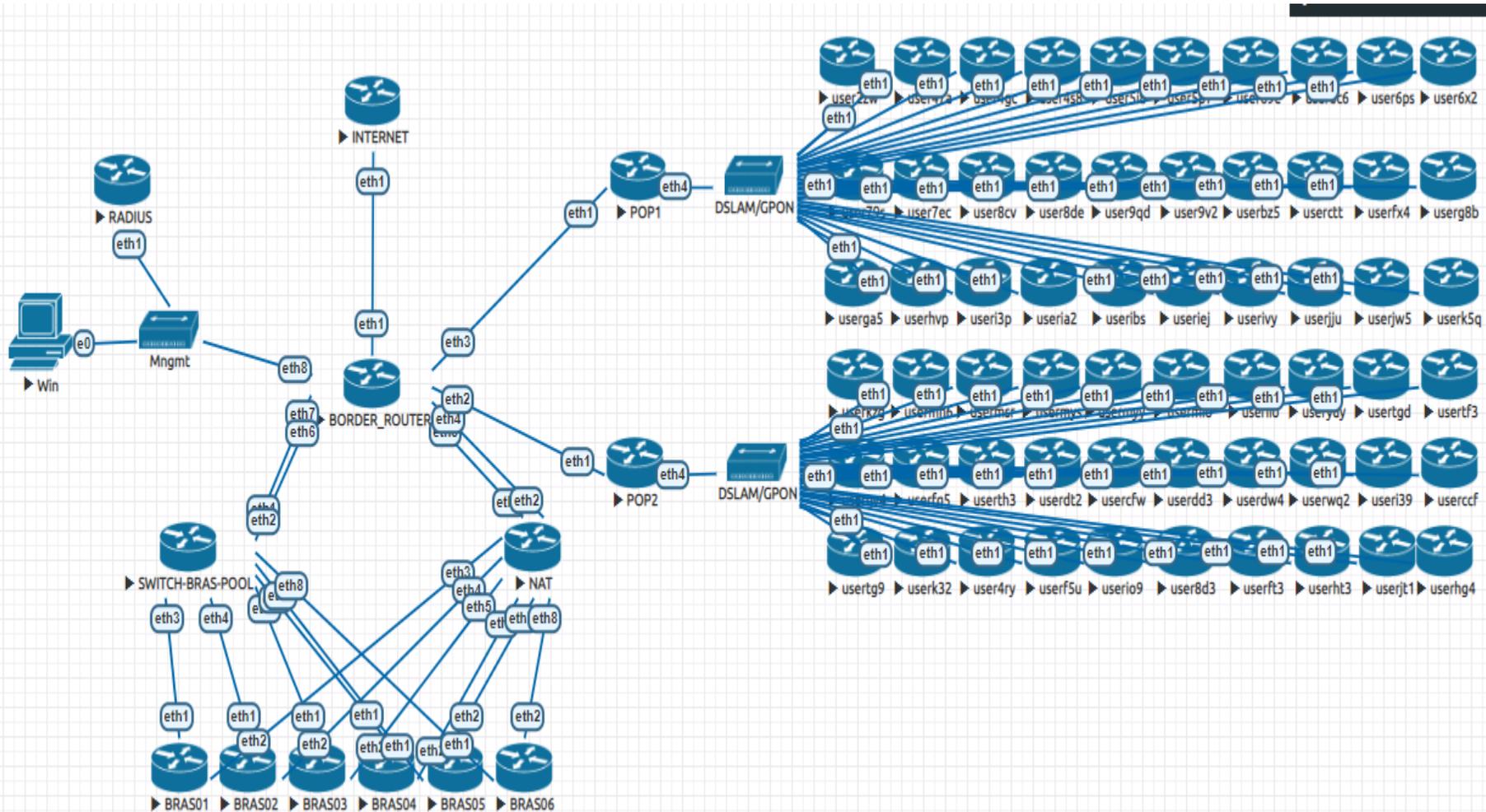


Qualidade para os cliente!



Como fazer isso?

Estudo de caso



Switch Concentrador

SWITCH-BRAS-POOL

► CRS317-1G-16S+RM

- 16 SFP+ ports
- Bounding Hardware offload
- 2 Power Supplies



BRAS para o Pool

BRAS

▶ CCR1036-8G-2S+EM

- ▶ 36 Cores
- ▶ 8GB RAM
- ▶ 2 SFP+ ports
- ▶ 2 Power Supplies



CGNat

NAT

▶ CCR1072-1G-8S

- ▶ 72 Cores
- ▶ 16GB RAM ECC
- ▶ 8 SFP+ ports
- ▶ 2 Power Supplies Hot Swap



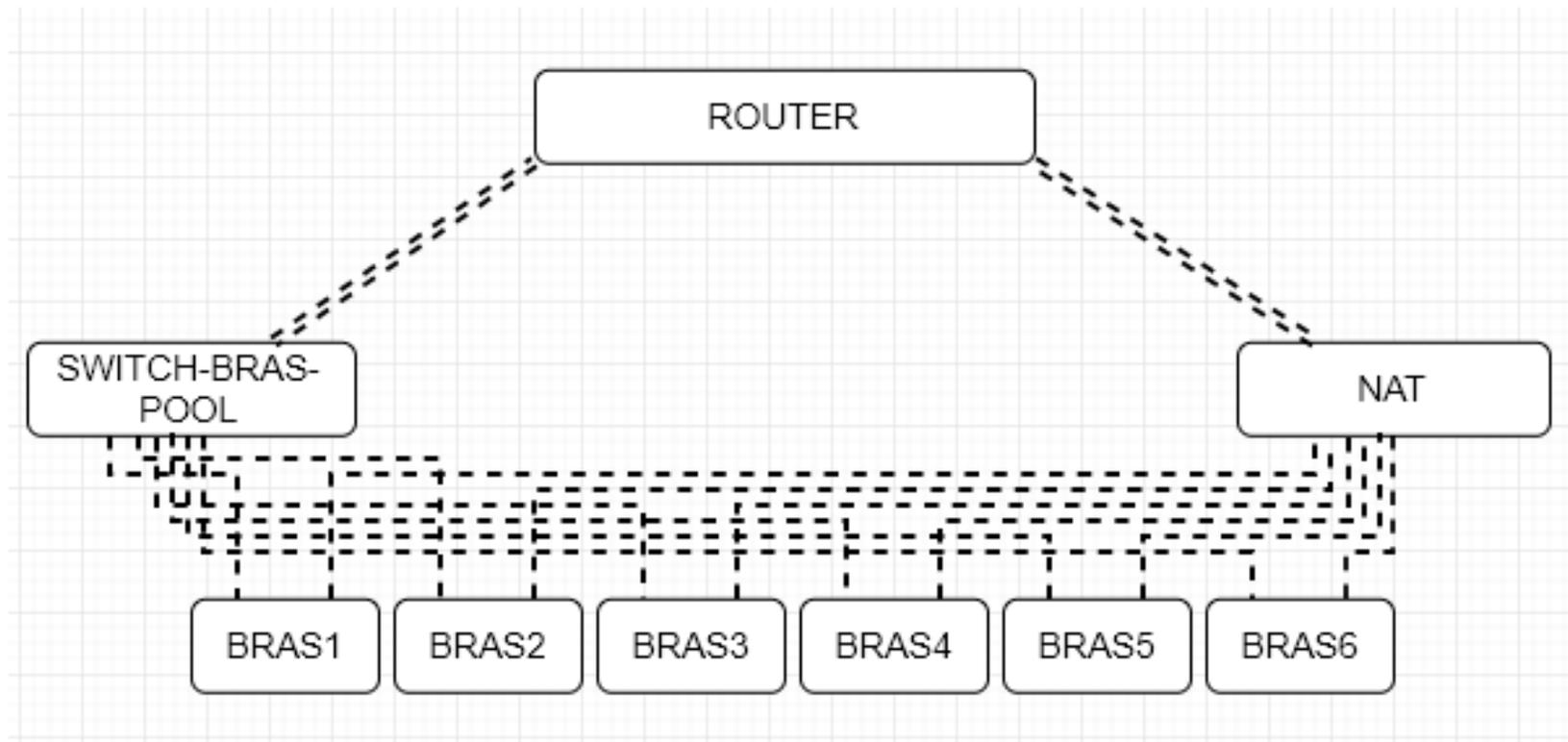
Direct Attach

▶ S+DA0001

- ▶ SFP+ direct attach cable, 1m



Diagrama de Conexões



Switch - Cenário Logico

- ▶ Hardware Offload: configurada uma interface Bond para o router onde os clientes serão transportados.
- ▶ Criar uma vlan na bounding para gerência do switch
- ▶ Utilizar Hardware Offload em todas interfaces com bridge

	Name	Type	Actual MTU	L2 MTU	Tx	Rx
RS	bonding-border-router	Bonding	1500	1500	102.7 kbps	74.4 kbps
R	vlan-mngmt:199	VLAN	1496	1496	95.9 kbps	8.4 kbps
R	bridge-pool-bras	Bridge	1500	1500	0 bps	58.2 kbps
::: BOARDER_ROUTER						
RS	ether1	Ethernet	1500		52.0 kbps	36.0 kbps
::: BOARDER_ROUTER						
RS	ether2	Ethernet	1500		50.6 kbps	38.3 kbps
::: BRAS01						
RS	ether3	Ethernet	1500		64.3 kbps	1280 bps

BRAS - Cenário Logico

- ▶ Use uma das interfaces para PPPoE IN, e a outra para OUT traffic
- ▶ A interface PPPoE IN vai conecta com o Switch Concentrador e a interface OUT com o CGNat

Name	Type	Actual MTU	L2 MTU	Tx	Rx
::: PPPoE IN					
R ether1	Ethernet	1500			240 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
DR <pppoe-user...	PPPoE Server Binding	1480			0 bps
::: OUT					
R ether2	Ethernet	1500			84.2 kbps

BRAS - Cenário Logico

- Configurado RADIUS do ER

RADIUS Incoming

Accept

Port: 3799

Requests: 0

Bad Requests: 0

Acks: 0

Naks: 0

OK

Cancel

Apply

Reset Status

RADIUS

Reset Status Incoming Find

#	Service	Called ID	Domain	Address	Secret
0	ppp			192.168.254.2	*****

BRAS - Cenário Logico

- Configurado ppp para usar Radius, PPPoE Server com PADO Delay para balancear usuário no Pool e Max Session para limitar a quantidade de usuários no BRAS

PPPoE Service <pppoe-server>

Service Name: pppoe-server

Interface: ether1

Max MTU: 1480

Max MRU: 1480

MRRU: 1600

Keepalive Timeout: 10

Default Profile: default

One Session Per Host

Max Sessions: 15

PADO Delay: 500 ms

Authentication: mschap2 mschap1
 chap pap

enabled

Buttons: OK, Cancel, Apply, Disable, Copy, Remove

PPP Authentication & Accounting

Use Radius

Accounting

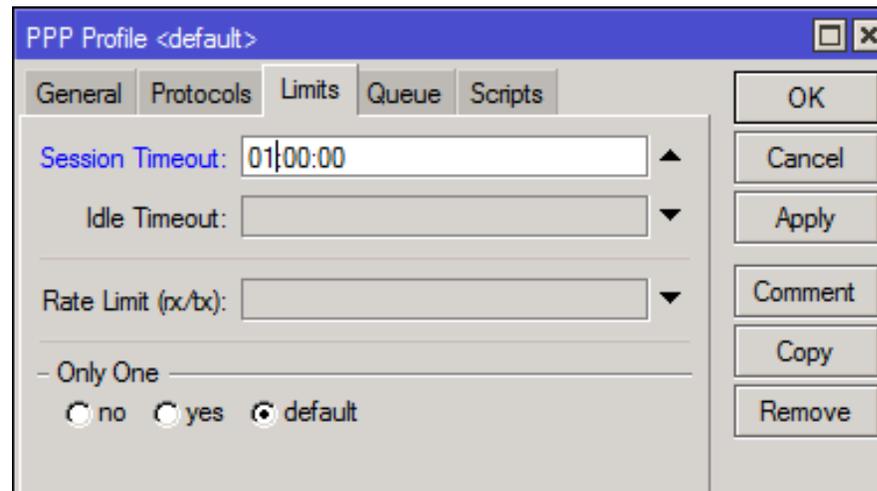
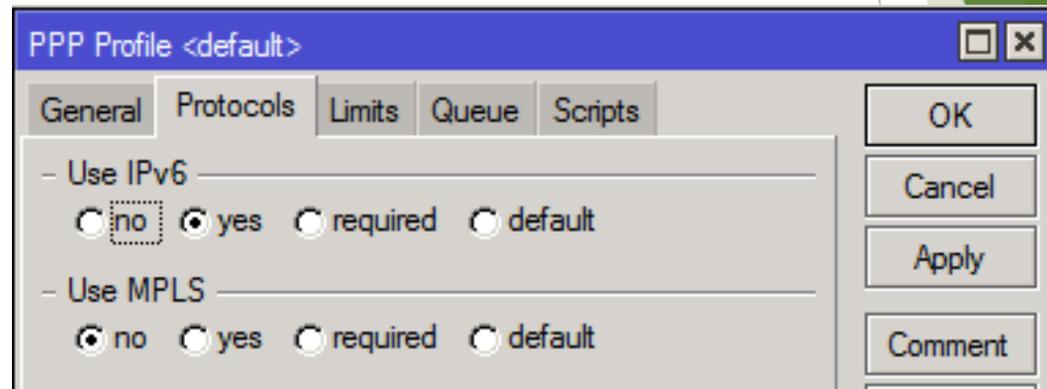
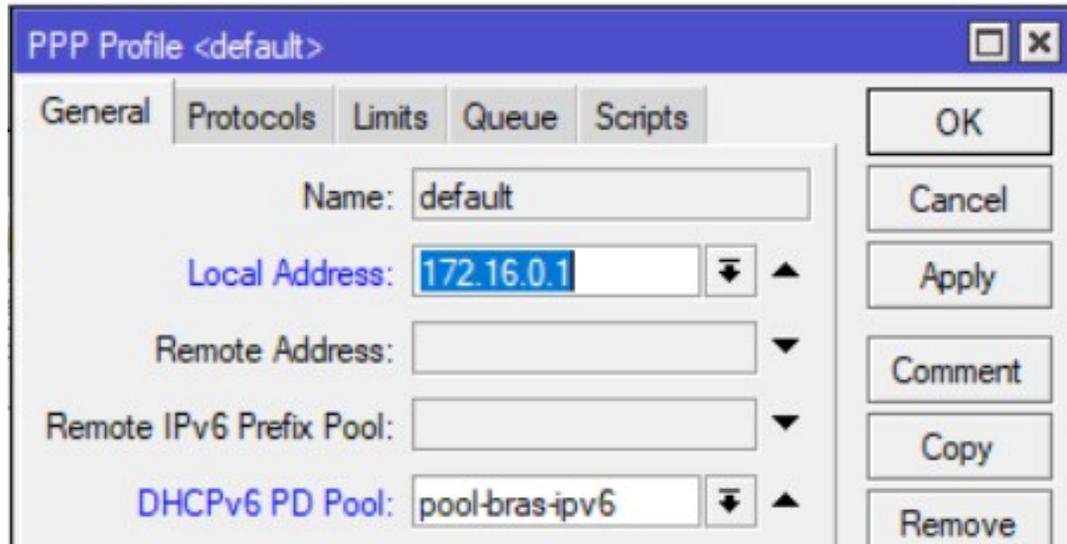
Use Circuit ID in NAS Port ID

Interim Update: []

Buttons: OK, Cancel, Apply

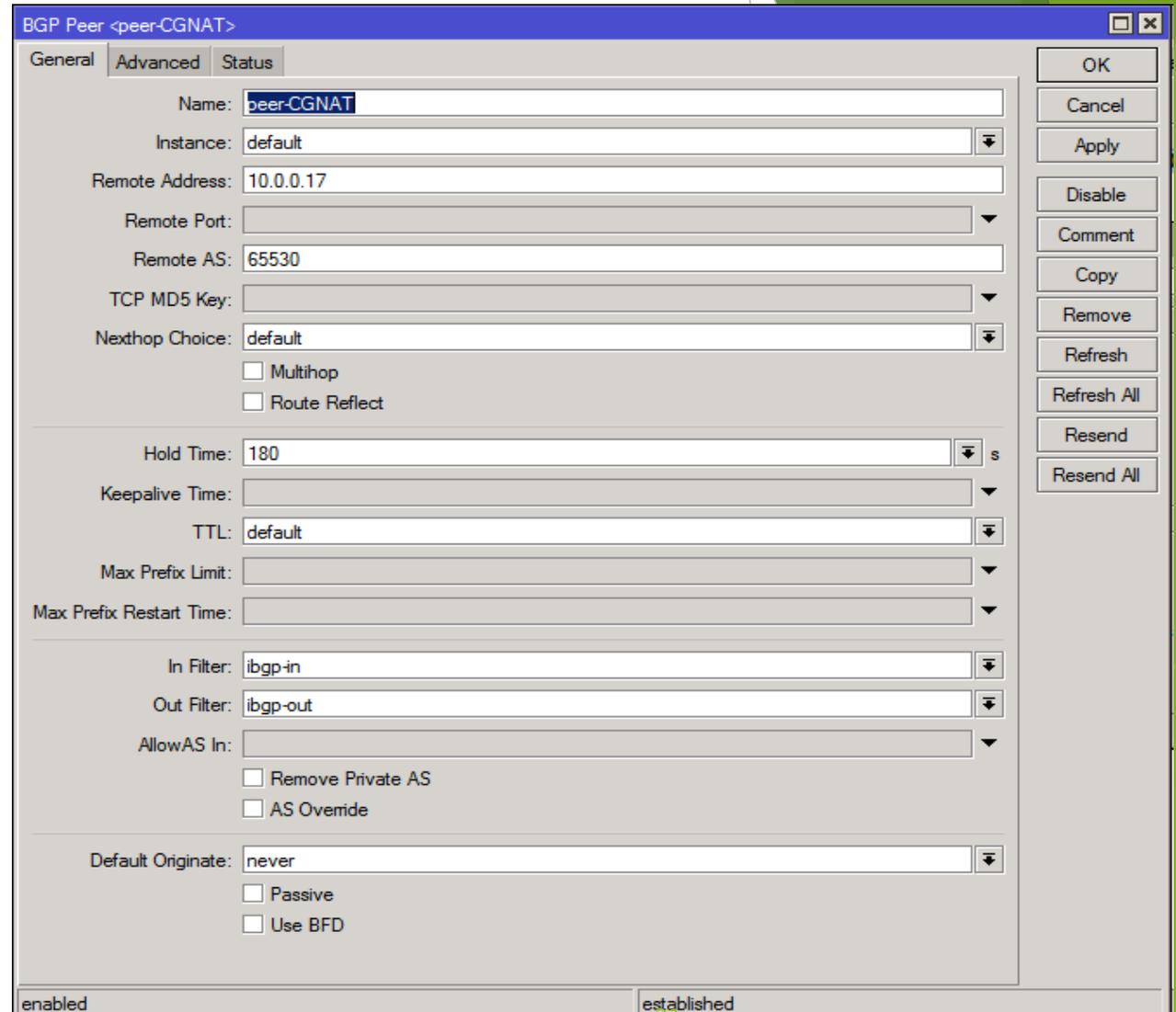
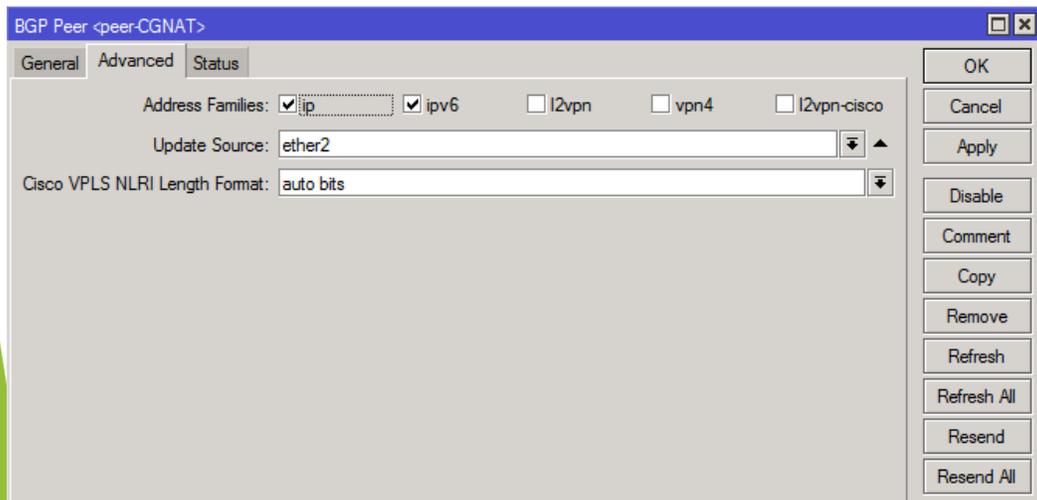
BRAS - Cenário Logico

- ▶ Configurado o ppp Profile Local Address, use IPv6 yes e a Session Timeout para janelas de manutenção
- ▶ Configurado o DHCPv6 PD pool



BRAS - Cenário Logico

- ▶ Configurado iBGP com a router de CGNat para redistribuir a rota dos cliente conectados e receber a rota default.
- ▶ Selecionado ip e ipv6 para o dual-stack



BRAS - Cenário Logico

- Configurado Firewall Raw com regra bloqueando ips da address-list lst_bloqueio, para bloqueio de clientes

The screenshot displays the Mikrotik WinBox Firewall configuration window. The 'Raw' tab is selected, showing a table of firewall rules. A rule named 'BLOQUEIO' is highlighted, with an action of 'drop' and a source address list of 'lst_bloqueio'. A 'Raw Rule' dialog box is open, showing the configuration for this rule. The 'Src. Address List' is set to 'lst_bloqueio', and the 'Action' is 'Drop'.

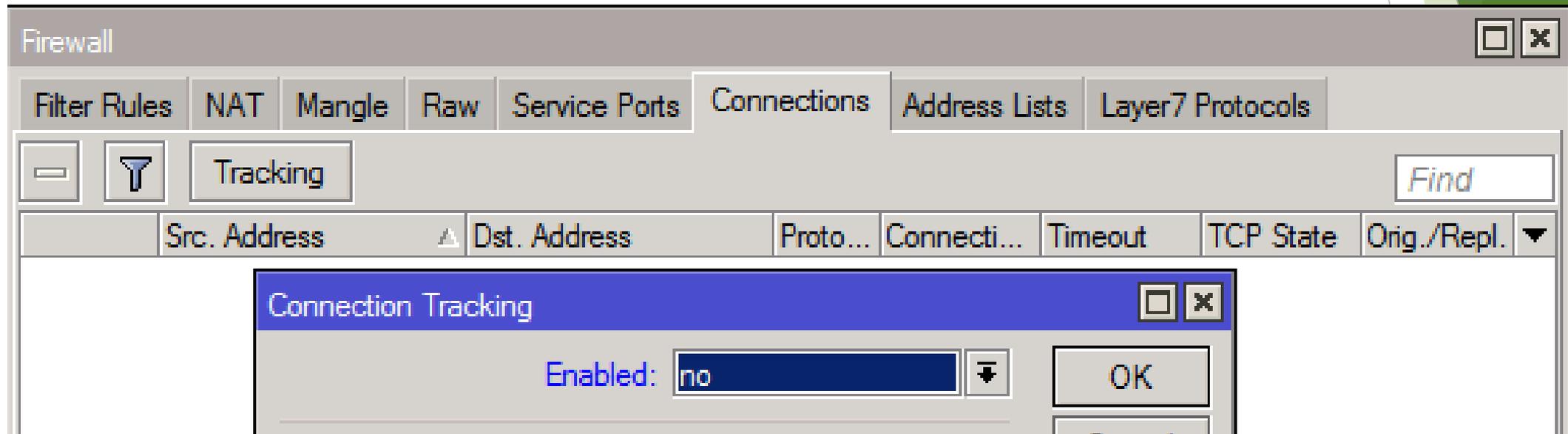
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
0	drop	prerouting							
1	D	no track							
2	D	no track							

Raw Rule Configuration:

- General: Name: BLOQUEIO
- Advanced: Src. Address List: lst_bloqueio
- Action: Drop

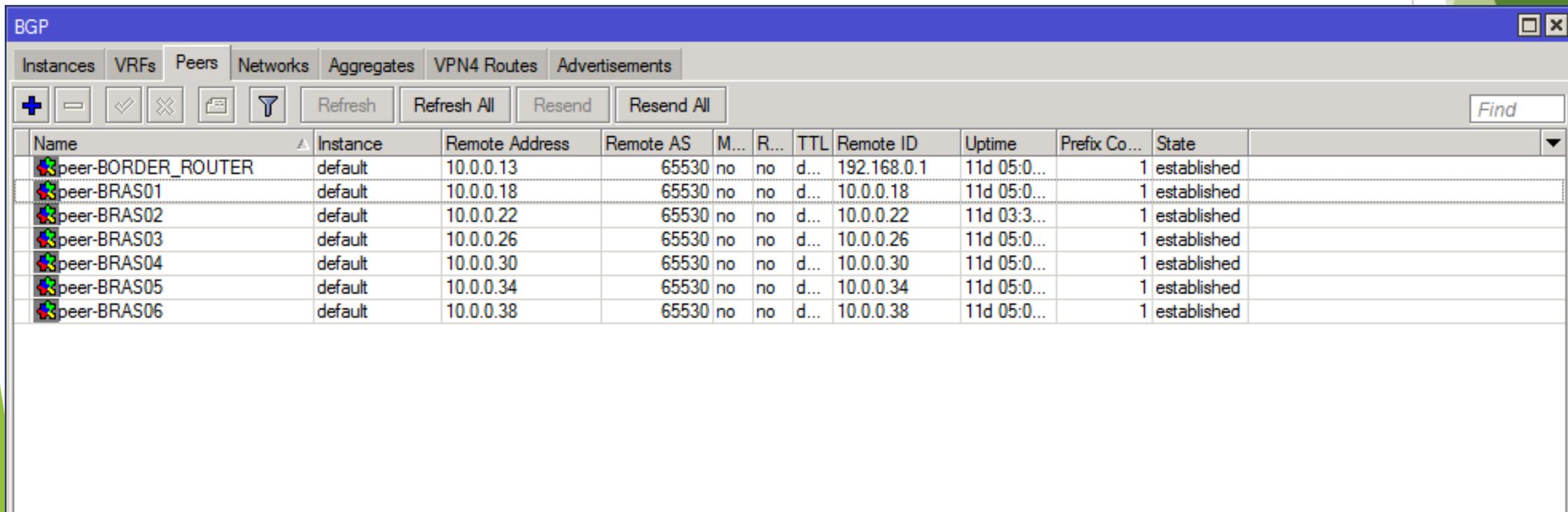
BRAS - Cenário Logico

- ▶ Desativado o Tracking para otimizar o BRAS



CGNAT - Cenário Logico

- ▶ Configurado iBGP com todos os BRAS enviando rota default, iBGP com a router de borda para receber a rota default e enviar as rotas do Pool BRAS
- ▶ Selecionado ip e ipv6 for para dual-stack



The screenshot shows a BGP configuration window with a table of BGP peers. The table has columns for Name, Instance, Remote Address, Remote AS, M..., R..., TTL, Remote ID, Uptime, Prefix Co..., and State. The peers listed are peer-BORDER_ROUTER, peer-BRAS01, peer-BRAS02, peer-BRAS03, peer-BRAS04, peer-BRAS05, and peer-BRAS06. All peers are in the 'established' state.

Name	Instance	Remote Address	Remote AS	M...	R...	TTL	Remote ID	Uptime	Prefix Co...	State
peer-BORDER_ROUTER	default	10.0.0.13	65530	no	no	d...	192.168.0.1	11d 05:0...	1	established
peer-BRAS01	default	10.0.0.18	65530	no	no	d...	10.0.0.18	11d 05:0...	1	established
peer-BRAS02	default	10.0.0.22	65530	no	no	d...	10.0.0.22	11d 03:3...	1	established
peer-BRAS03	default	10.0.0.26	65530	no	no	d...	10.0.0.26	11d 05:0...	1	established
peer-BRAS04	default	10.0.0.30	65530	no	no	d...	10.0.0.30	11d 05:0...	1	established
peer-BRAS05	default	10.0.0.34	65530	no	no	d...	10.0.0.34	11d 05:0...	1	established
peer-BRAS06	default	10.0.0.38	65530	no	no	d...	10.0.0.38	11d 05:0...	1	established

CGNAT - Cenário Logico

- Configurado Firewall RAW para proteger clientes e a internet, na table Filter configurado FASTTRACK para otimizar o CGNat

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✕ [Filter Icon] [Reset Counters] [Reset All Counters]

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interface	Out...
::: special dummy rule to show fasttrack counters									
0	D	pas...							
::: LST_BRAS_MGMT									
1	✓ acc...	prerouting							
::: BLOCK_SPOOF_BRAS									
2	✕ drop	prerouting	!100.64.0.0...						
::: BLOCK_LOW_PORT_TO_BRAS									
3	✕ drop	prerouting		192.168.1.0/24	6 (tcp)		0-1024	bonding-ROUTER-B...	
::: BLOCK_LOW_PORT_TO_BRAS									
4	✕ drop	prerouting		192.168.1.0/24	17 (u...		0-1024	bonding-ROUTER-B...	

Firewall

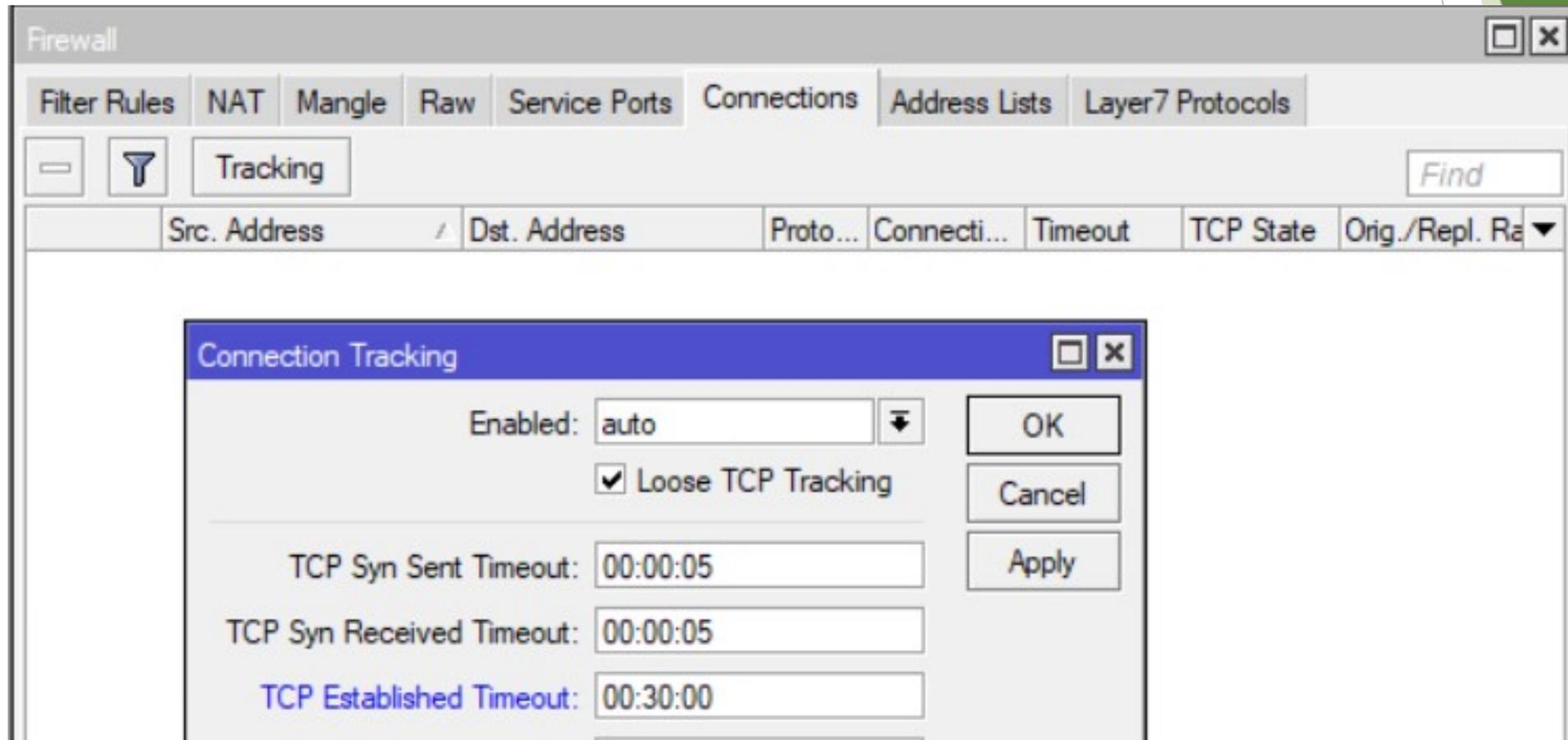
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists

+ - ✓ ✕ [Filter Icon] [Reset Counters] [Reset All Counters]

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interface	Out...
::: special dummy rule to show fasttrack counters									
0	D	pas...							
::: FASTTRACK									
1	▶▶ fastt...	forward	100.64.0.0/...						
::: ACCEPT ESTABLISHED/RELATED									
2	✓ acc...	forward							

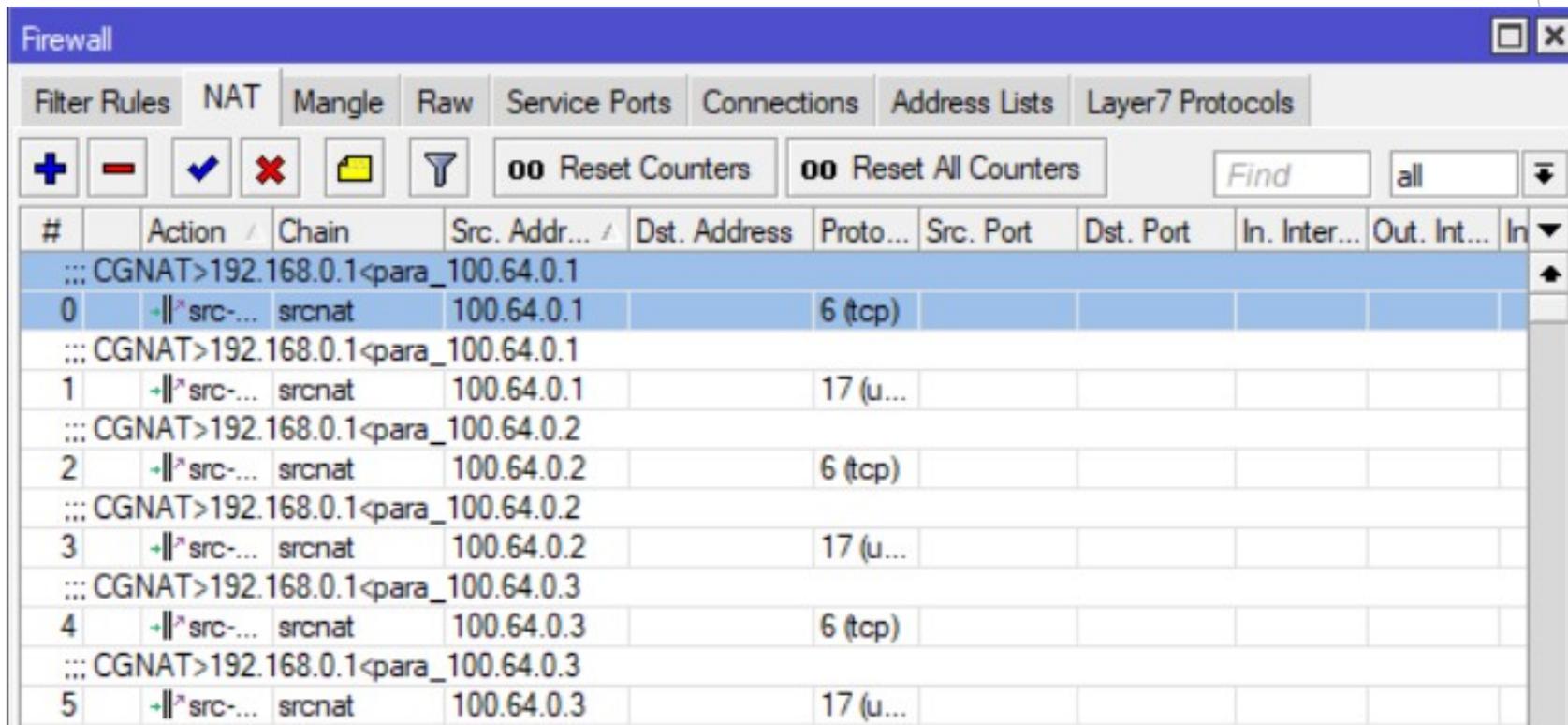
CGNAT - Cenário Logico

- ▶ Alterar o “TCP Established Timeout” para 30 minutos



CGNAT - Cenário Logico

- ▶ Ajustando a tabela NAT para o CGNat distribuindo as portas para os clientes.
- ▶ <https://github.com/helysonoliveira/cgnat-mikrotik>



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'NAT' tab is selected. The table below displays the configured NAT rules for CGNAT.

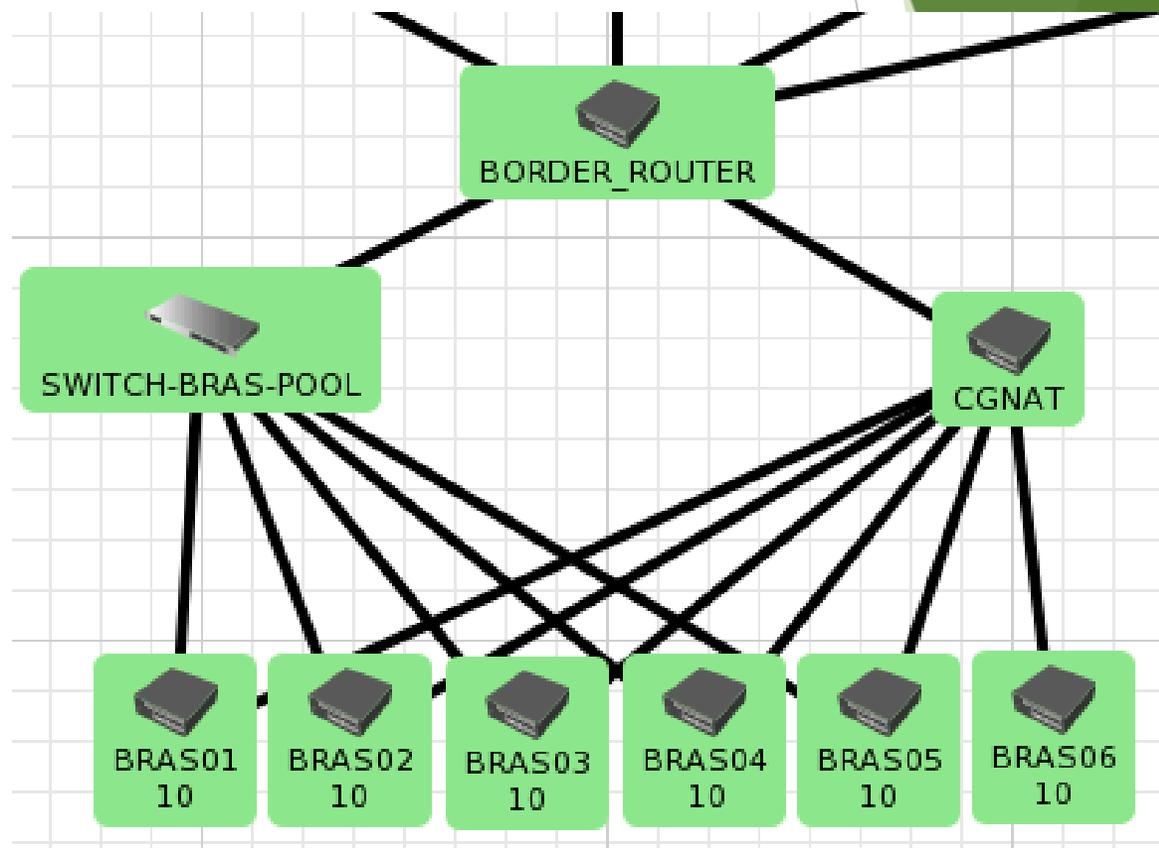
#	Action / Chain	Src. Addr...	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In
0	- *src-... srcnat	100.64.0.1		6 (tcp)					
1	- *src-... srcnat	100.64.0.1		17 (u...					
2	- *src-... srcnat	100.64.0.2		6 (tcp)					
3	- *src-... srcnat	100.64.0.2		17 (u...					
4	- *src-... srcnat	100.64.0.3		6 (tcp)					
5	- *src-... srcnat	100.64.0.3		17 (u...					

RFC 6269

RFC 6598

Tudo Pronto!

- ▶ IPv6 e CGNAT configurados.
- ▶ Simulado 60 clientes distribuídos no pool em 6 BRAS.
- ▶ Realizado testes de resiliência com sucesso.
- ▶ Firewall de proteção mantendo a rede segura.



Obrigado!

Flavio Gomes Figueira Camacho Junior

E-mail: flaviocamacho95@gmail.com

Telefone: +55 21 96978-467  

Skype: flaviocamacho95_1

