

---

# A importância de um CGNAT bem feito

20/09/2019

Fernando Frediani



# Tópicos Abordados

---

- **Introdução**
- **Aspectos Legais**
- **Tipos de CGNAT**
  - **Determinístico**
  - **Bulk Port Allocation**
- **Importância do IPv6**
- **Problemas com Jogos**
- **Política de Atribuição de IPv4 Público**
- **Aonde fazer**
- **Opções e Tecnologias disponíveis**
- **Conclusões**

# Introdução

---

- Surgiu devido à escassez de IPv4 disponível para os Provedores de Acesso
- Alocação de Endereços definida pela RFC6598
  - Range 100.64.0.0/10
  - Não é o mesmo que RFC1918
- Um maneira sustentável e organizada para continuar provendo acesso até a transição completa para IPv6
- CGNAT é NAT
- CGNAT “não é NAT”

# Aspectos Legais

---

- **Importância do registro e guarda de logs para identificação do usuário.**
  - Art. 10, Art. 13 e Art. 15 do Marco Civil
- **Somente o endereço IP não é suficiente. É necessário haver o registro da porta de origem também.**
  - Interpretações do Judiciário no sentido da obrigatoriedade da guarda também da porta de origem.
- **Não se deve jamaiz registrar endereço nem porta de destino para este propósito (violação da privacidade).**
- **Provedores de conteúdo devem também guardar os registros de porta de origem, caso contrário a identificação não é possível.**



# Tipos de CGNAT - Determinístico

---

- Mais utilizado pelos provedores em geral pela facilidade de implementação.
- Define um range limitado de portas TCP e UDP por usuário para ser utilizado.
- Permite uma economia razoável de endereços IPv4 Públicos à depender do nível de compartilhando realizado.
- Requer uma quantidade bem menor de log (apenas os de autenticação e atribuição do IP da range de CGNAT).

# Tipos de CGNAT - Determinístico

---

## ■ Exemplo 1 – Compartilhamento 1:32

- 32 assinantes compartilharão o mesmo IPv4 Público
- 2000 portas de origem alocadas para cada IP Privado

## ■ Exemplo 2 – Compartilhamento 1:16

- 16 assinantes compartilharão o mesmo IPv4 Público
- 4000 portas de origem alocadas para cada IP Privado

## ■ Exemplo 3 – Compartilhamento 1:8

- 8 assinantes compartilharão o mesmo IPv4 Público
- 8000 portas de origem alocadas para cada IP Privado

```
iptables -t nat -A CGNAT -s 100.64.18.10 -p tcp -j SNAT --to 192.0.0.1:2096-4096  
iptables -t nat -A CGNAT -s 100.64.18.10 -p udp -j SNAT --to 192.0.0.1:2096-4096
```

# Tipos de CGNAT – Bulk Port Allocation

---

- Realiza a atribuição de portas de origem para cada IP de CGNAT de maneira dinâmicas e em blocos, conforme a necessidade de cada assinante.
- Define um range limitado de portas TCP e UDP inicial por usuário e blocos adicionais à serem alocados posteriormente conforme a necessidade de cada um.
- Permite uma economia maior de endereços IPv4 Públicos pois a maioria dos usuários não utilizam um alto número de portas e um mesmo IPv4 pode ser utilizado por uma quantidade maior de usuários.
- Requer uma quantidade maior de log devido às alocações dinâmicas realizadas.

# Tipos de CGNAT – Bulk Port Allocation

---

## ■ Exemplo 1

- Assinante possui inicialmente 256 portas alocadas para uso.
- Quando atingir o número de portas alocadas o sistema alocará blocos adicionais de 64 portas (não contíguas) para o mesmo IP privado utilizado pelo assinante.

## ■ Exemplo 2

- Assinante possui inicialmente 512 portas alocadas para uso.
  - Quando atingir o número de portas alocadas o sistema alocará blocos adicionais de 256 portas (não contíguas) para o mesmo IP privado utilizado pelo assinante.
- 
- Cada nova alocação gera uma entrada nos logs.



# Tipos de CGNAT – Bulk Port Allocation

---

## ▪ Exemplo Log – Bulk Port Allocation

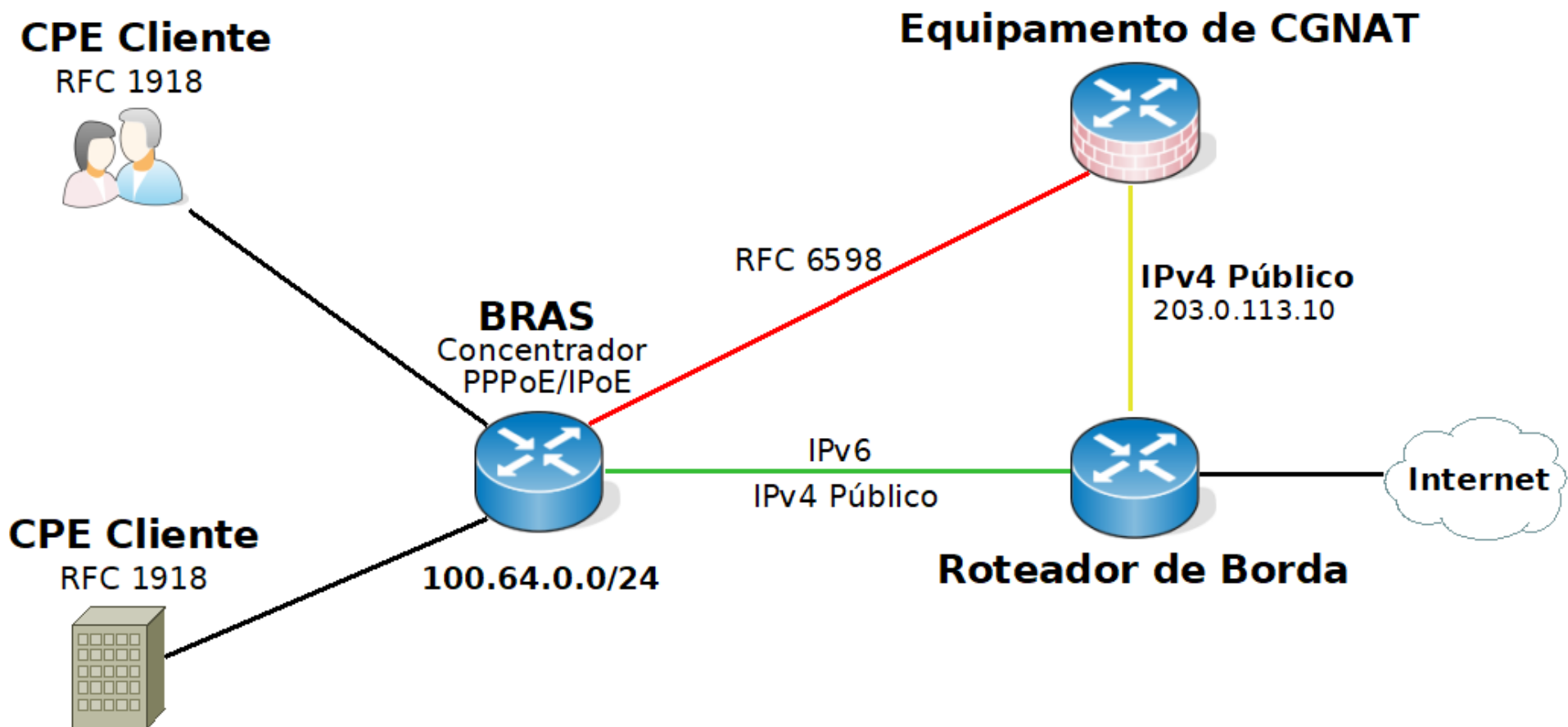
- Cliente típico TCP, UDP e ICMP
  - {"ip\_src": "100.64.14.163", "ip\_proto": "tcp", "post\_nat\_ip\_src": "203.0.113.14", "nat\_event": 1, "timestamp\_start": "2019-05-21 08:57:43.162000", "port\_block\_start": "7168", "port\_step\_size": "1", "number\_of\_ports\_in\_the\_block": "512"}
  - {"ip\_src": "100.64.14.163", "ip\_proto": "udp", "post\_nat\_ip\_src": "203.0.113.14", "nat\_event": 1, "timestamp\_start": "2019-05-21 08:57:43.159000", "port\_block\_start": "9216", "port\_step\_size": "1", "number\_of\_ports\_in\_the\_block": "512"}
  - {"ip\_src": "100.64.14.163", "ip\_proto": "icmp", "post\_nat\_ip\_src": "203.0.113.14", "nat\_event": 1, "timestamp\_start": "2019-05-21 08:58:16.213000", "port\_block\_start": "2560", "port\_step\_size": "1", "number\_of\_ports\_in\_the\_block": "512"}
- Cliente que alocou dois ranges de portas TCP
  - {"ip\_src": "100.64.159.188", "ip\_proto": "tcp", "post\_nat\_ip\_src": "203.0.113.18", "nat\_event": 1, "timestamp\_start": "2019-05-21 06:10:18.2000", "port\_block\_start": "57856", "port\_step\_size": "1", "number\_of\_ports\_in\_the\_block": "512"}
  - {"ip\_src": "100.64.159.188", "ip\_proto": "tcp", "post\_nat\_ip\_src": "203.0.113.18", "nat\_event": 1, "timestamp\_start": "2019-05-21 07:05:34.110000", "port\_block\_start": "62976", "port\_step\_size": "1", "number\_of\_ports\_in\_the\_block": "512"}

# Importância do IPv6

---

- É muito importante sempre implantar IPv6 junto com o CGNAT.
- A maioria dos conteúdos acessados pelos usuários possui suporte à IPv6. Isso significa que cada conexão realizada até estes conteúdos evita utilizar as portas limitadas destinadas ao CGNAT evitando assim um possível exaurimento de portas.
- Equipamentos para realizar CGNAT custam mais caro, então todo tráfego IPv4 que precisa passar ali terá um custo maior.
  - Todo tráfego IPv6 segue direto para a borda sem a necessidade de passar por esses equipamentos (evita gargalos).
- Manter um sistema de registros para CGNAT é mais complexo e pode ser mais custoso (Hardware, Storage, Tempo de Pessoal, etc). Quanto menor for a necessidade de utilizá-lo menor os custos para o provedor.

# Importância do IPv6



# Problemas com Jogos

---

- **Maioria dos jogos funcionam apenas em IPv4.**
- **Alguns jogos utilizam um número elevado de portas que podem causar exaurimento das portas compartilhadas para cada IPv4 Público.**
- **Amigos que se reúnem e utilizam uma única conexão para jogarem (pode causar exaurimento de portas).**
- **Impossibilidade de criação de partidas (hosting) por assinantes atrás de CGNAT (sem conexões entrantes).**
- **Alguns serviços podem interpretar múltiplas conexões desde um mesmo IP Público como ataque e aplicar filtros ou bloqueios.**

# Política de Atribuição de IPv4 Público

---

- **Elaborar uma boa política para atribuição de IPv4 Público (onerosa ou não)**
  - **Existem casos legítimos que ainda demandam um IP Público**
- **Algumas aplicações com a função Cloud já não necessitam mais de um IP Público para redirecionamento de portas e funcionam bem em cima de CGNAT**
- **Caso houver cobrança para atribuição do IPv4 Público faça o dever de casa e disponibilize também o IPv6**

# Aonde fazer CGNAT

---

## ■ No próprio BRAS

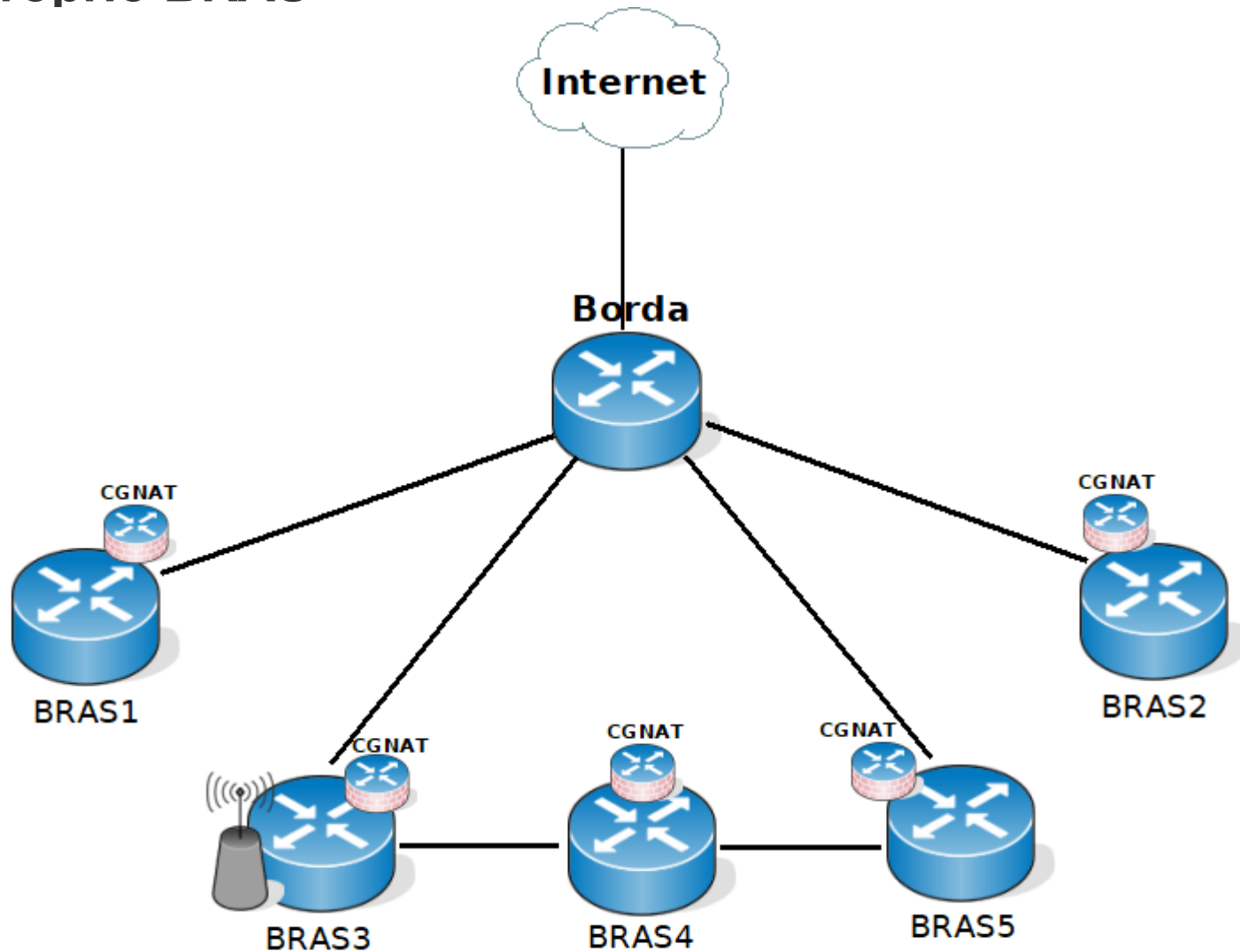
- Maior utilização de recursos e processamento para ambas as funções significa um menor número de usuários autenticados por equipamento.
- Redundância automática e intrínseca no caso de múltiplos BRAS

## ■ Centralizado / Regionalizado do backbone

- Garantia que apenas o tráfego de CGNAT irá passar pelo equipamento.
- Crescimento orgânico dos equipamentos destinados à BRAS ou à CGNAT.
- Maior clareza na organização do backbone.
- Necessidade de N+1 para redundância.

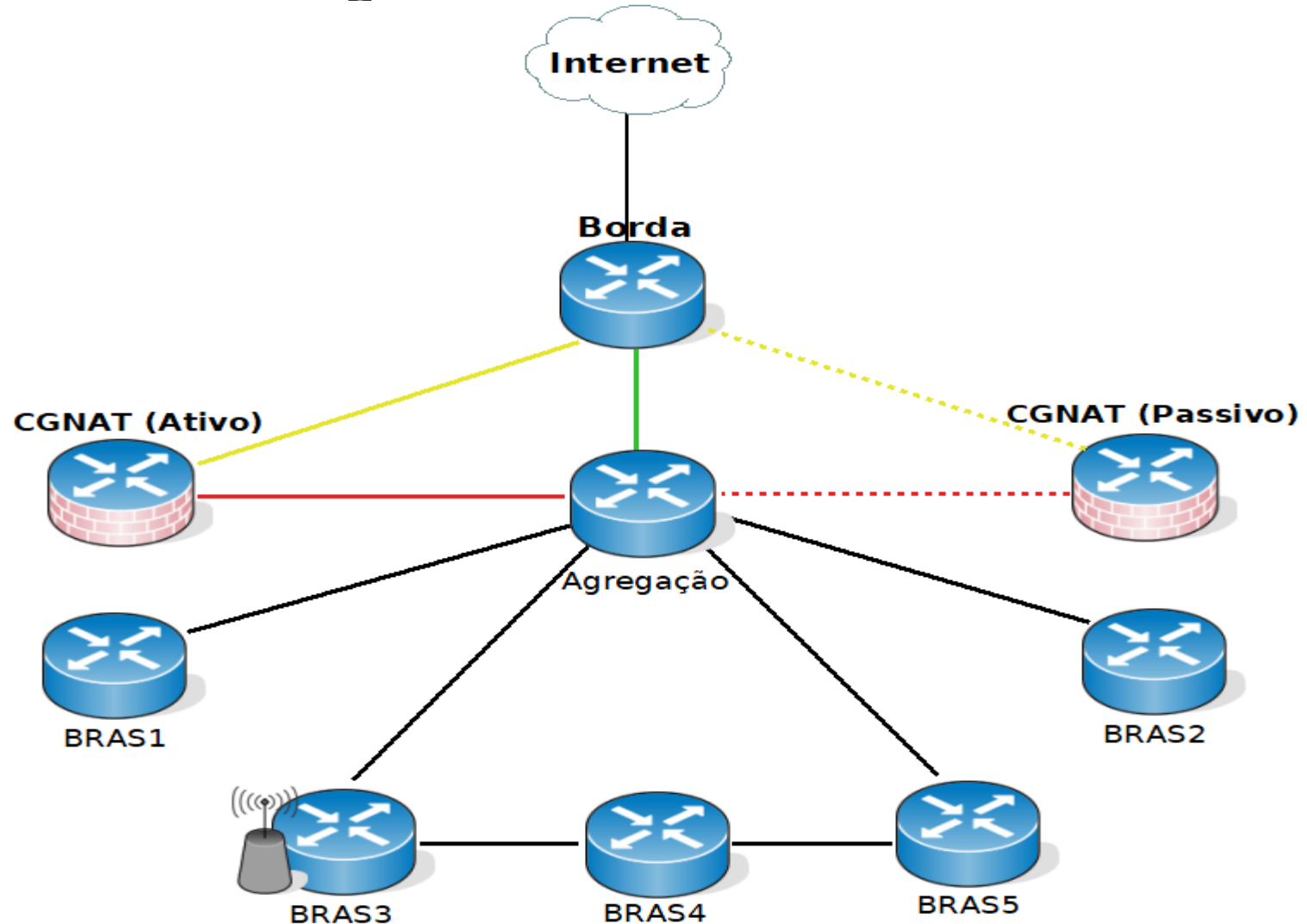
# Aonde fazer CGNAT

- No próprio BRAS



## Aonde fazer CGNAT

- **Centralizado / Regionalizado no backbone**





# Opções e Tecnologias Disponíveis

---

- Cisco ASR



- A10 Networks



- Mikrotik (RouterOS)



- Linux / netfilter



# Conclusões

---

- **CGNAT é inevitável para os provedores de acesso devido à escassez de IPv4**
- **Os registros (logs) são obrigatórios para atender a legislação e para identificação do usuário.**
- **CGNAT Determinístico e Bulk Port Allocation – Vantagens e Desvantagens e cada cenário.**
- **IPv6 é essencial para evitar problemas decorrentes do CGNAT e reduzir custos**
- **Atentar-se aos problemas relacionados à Jogos**
- **Escolher bem o local onde fazer o CGNAT.**



# Perguntas

Contato: [fhfrediani@gmail.com](mailto:fhfrediani@gmail.com)

---