

Apresentação Reverse NAT

- Introdução
- Conceitos
- Técnicas similares
- Discussões
- Problemas
- Soluções
- Exemplo com Iptables
- Laboratório
- Atividade extra

Intro

- NAT é o mecanismo pelo qual o elemento que encaminha pacotes, faz a substituição de cabeçalho e desvio de tráfego
- RFC 3022
- Técnica que causa muita polêmica, com pontos favoráveis de desfavoráveis
- Objetivo principal: Mitigar exaustão de IPv4

Conceitos

- NAT tem de ser realizado por elemento de roteamento ativo. Uma tabela deve ser mapeada neste elemento indicando as origens/destinos originais de um fluxo
- [Video](#)
- Egress NAT ou Ingress NAT (Reverse NAT ou Reverse proxy)

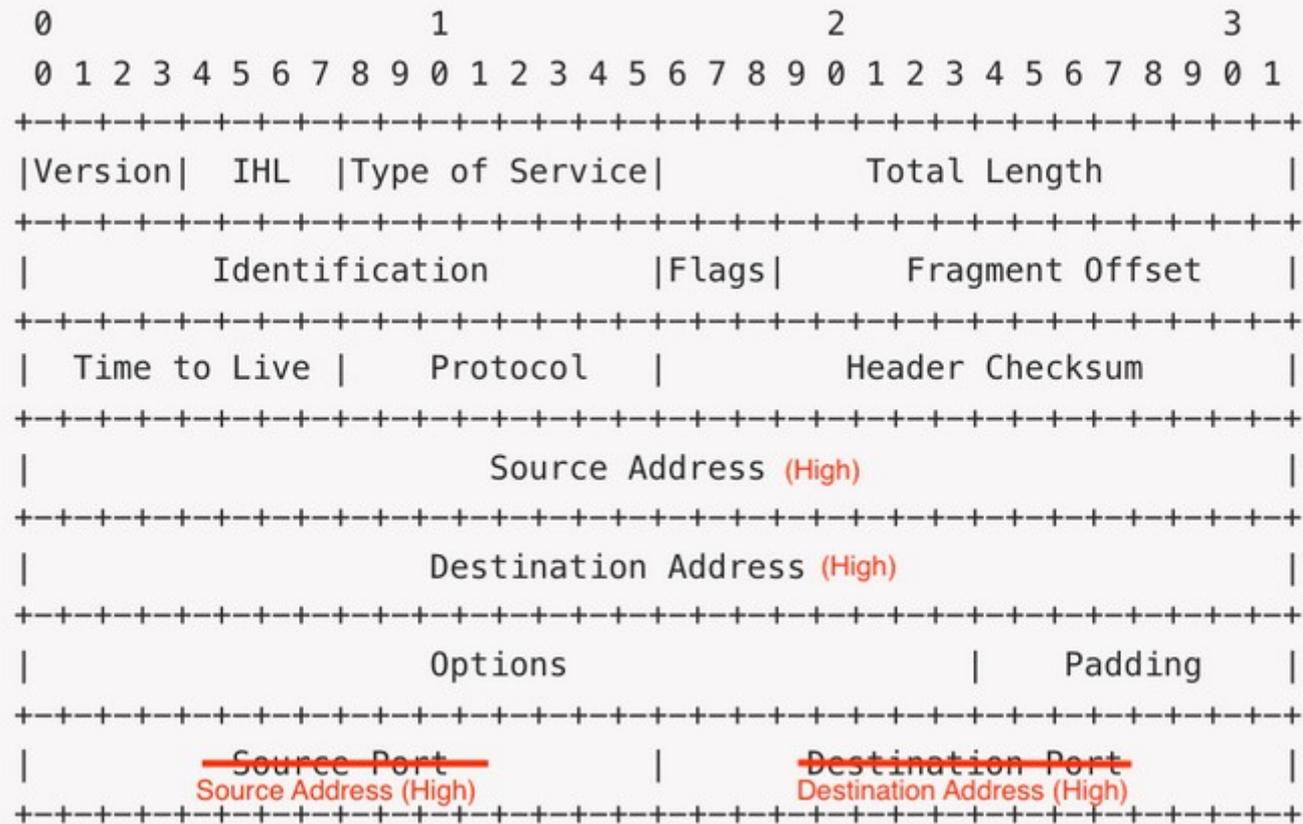
Técnicas Similares

- Reverse proxy (squid, apache, etc)
- Load balancers (nginx, kong, haproxy, etc)
- Application Ingress/Egress
- API Gateway

Discussões

- Controvérsia. Retardar o término do IPv4 vs princípios da Internet.
- Uso de NAT introduz overhead e pode ser crucial em certos contextos.
- Segurança e quebra de funcionamento de protocolos que usam criptografia

Discussões



Problemas

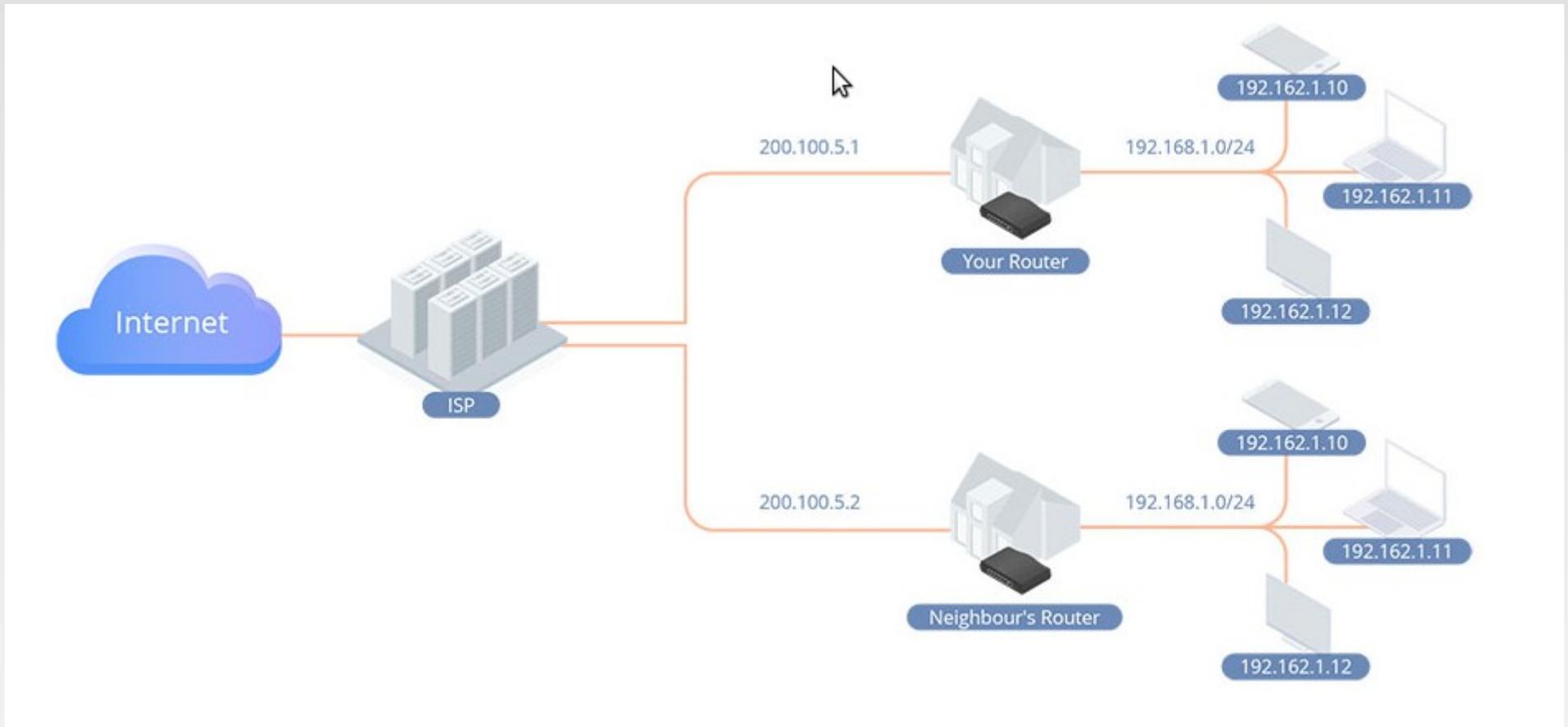
- Servidores dependentes de NAT reverso ineficientes (VoIP SIP, Game server, etc).
- Serviço atrás de NAT reverso pode ter problema com resolução DNS e redirecionamentos.
- Fragmentação.
- FTP, P2P, H323, SIP, etc.
- <https://www.excentis.com/blog/the-ugly-side-of-nat/>
- <https://web.mit.edu/6.033/2002/wwwdocs/papers/what-nats-break.html>

Problemas

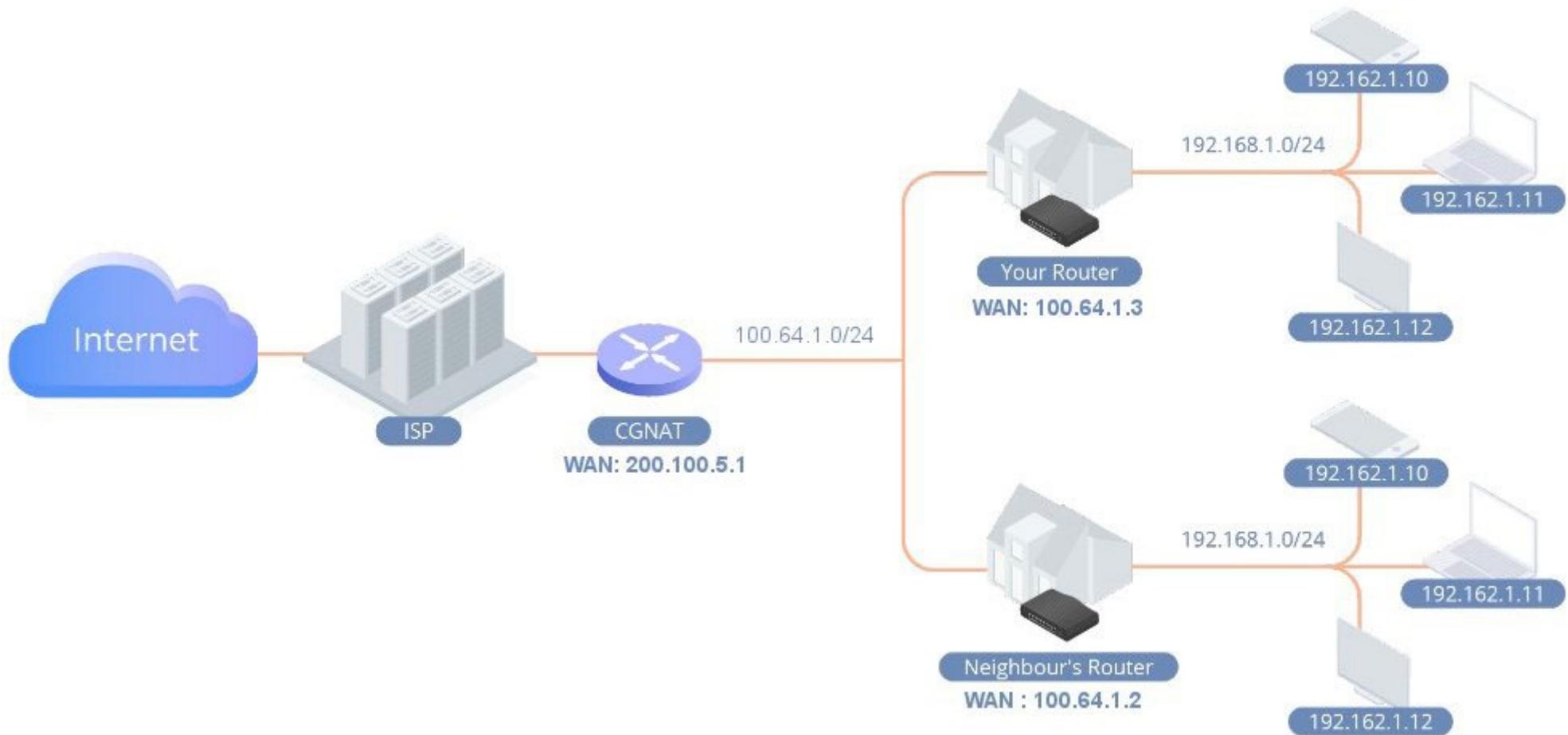
- CGNAT (LSNAT) é um outra técnica que causa ainda mais problemas.
- 100.64.0.0/10 (100.64.0.0 to 100.127.255.255)
- RFC 6598



Problemas

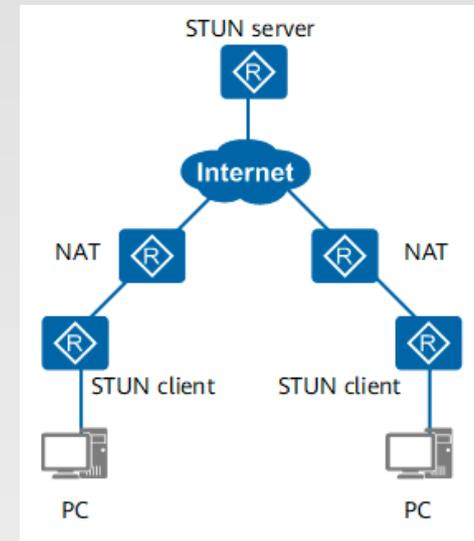


Problemas



Soluções

- STUN RFC 3489 (NAT Traversal)
- SSH tunnel
- VPNs
- NAT 64



Reverse NAT Iptables

```
#> iptables -F -t nat
```

```
#> sysctl -w net.ipv4.ip_forward=1
```

```
#> iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.100:80
```

```
#> iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -d 192.168.1.100 -j ACCEPT
```

```
#> iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
#> netfilter-persistent save
```



Reverse NAT nftables



```
#> nft add rule nat prerouting iifname "eth0" tcp  
dport 80 dnat to 192.168.1.100:80
```

Laboratório

- Configurar um serviço na rede interna (portátil) e garantir que exista um reverse NAT para habilitar o acesso ao mesmo

Atividade Extra

- Faça o exercício extra em <http://rzuolo.com/2025/grs/atividade-extra-05-NAT.pdf>

The End

