WTR

WORKSHOP

DE TECNOLOGIA DE REDES DO POP-RS

07 a 09 de novembro de 2018

Boas Práticas para Rede Interna

César Augusto Hass Loureiro

PoP-RS

Ponto de Presença da RNP no Rio Grande do Sul

RNP

Assuntos

- Segmentação da rede
- Endereçamento de Rede / NAT
- IPv6 / DHCPv6
- Registro de Logs

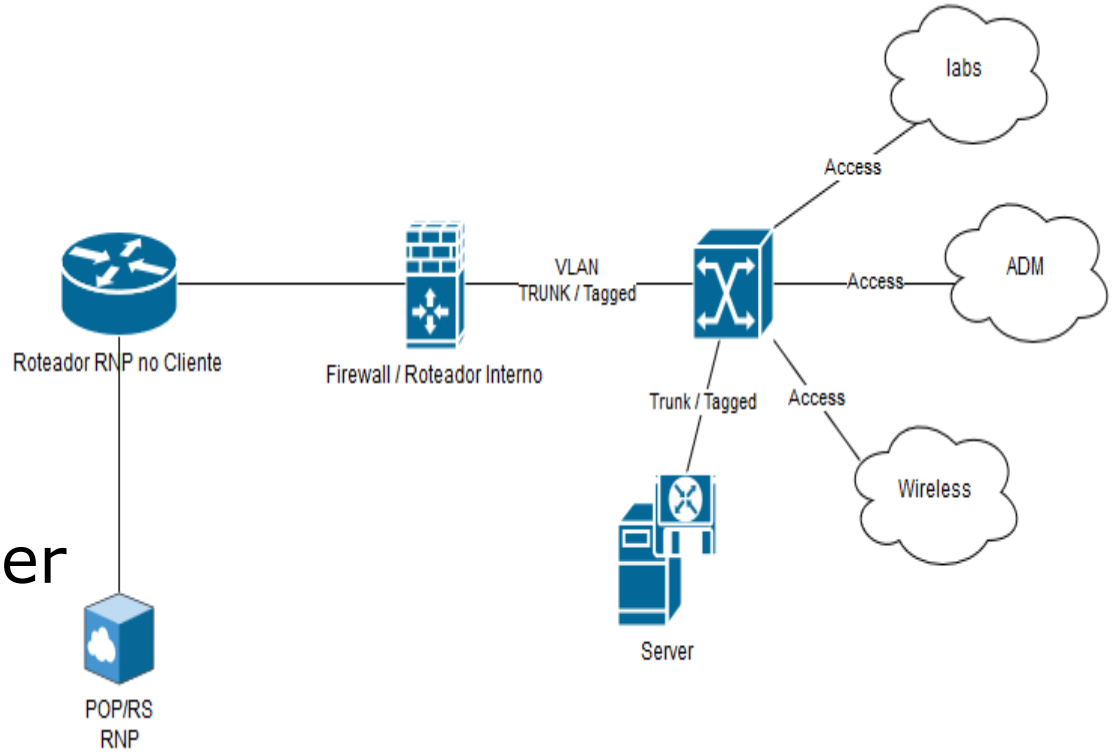
Segmentação da rede

Problemas encontrados

- Alguns clientes utilizando redes /23 diretamente no roteador
- Grande quantidade de broadcast IP
- Problemas de broadcast ARP, pois alguns equipamentos possuem uma tabela ARP pequena
- Dificuldade de localizar máquinas infectadas com Bots (controle do DHCP)

Utilização de VLAN

- Segmentar a rede em VLAN para diminuir o domínio de broadcast
- Cuidar para não segmentar demasiadamente, pois cada segmento deverá ter uma rede IP distinta
- Sugestão: Rede Administrativa, Rede Acadêmica, Wifi, ...



Endereçamento de Rede / NAT

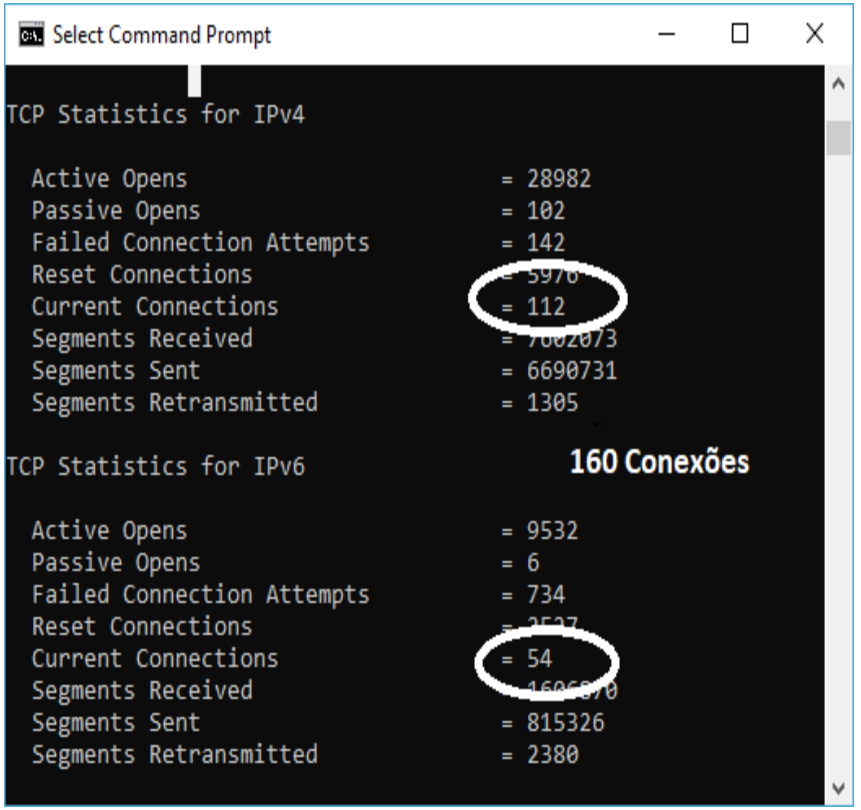
NAT - Criado para resolver a falta de endereços IPv4 em 1995.

Cuidado!!!

Quantidade de Portas Default no TCP do Ubuntu 16 LTS = 28.231

net.ipv4.ip_local_port_range = 32768 60999

28.231 portas / ~160 conexões = 176 clientes



Endereçamento de Rede / NAT

Soluções:

- *Utilizar os endereços roteáveis disponibilizados pela RNP (IPv4 e IPv6). NAT apenas se necessário.*

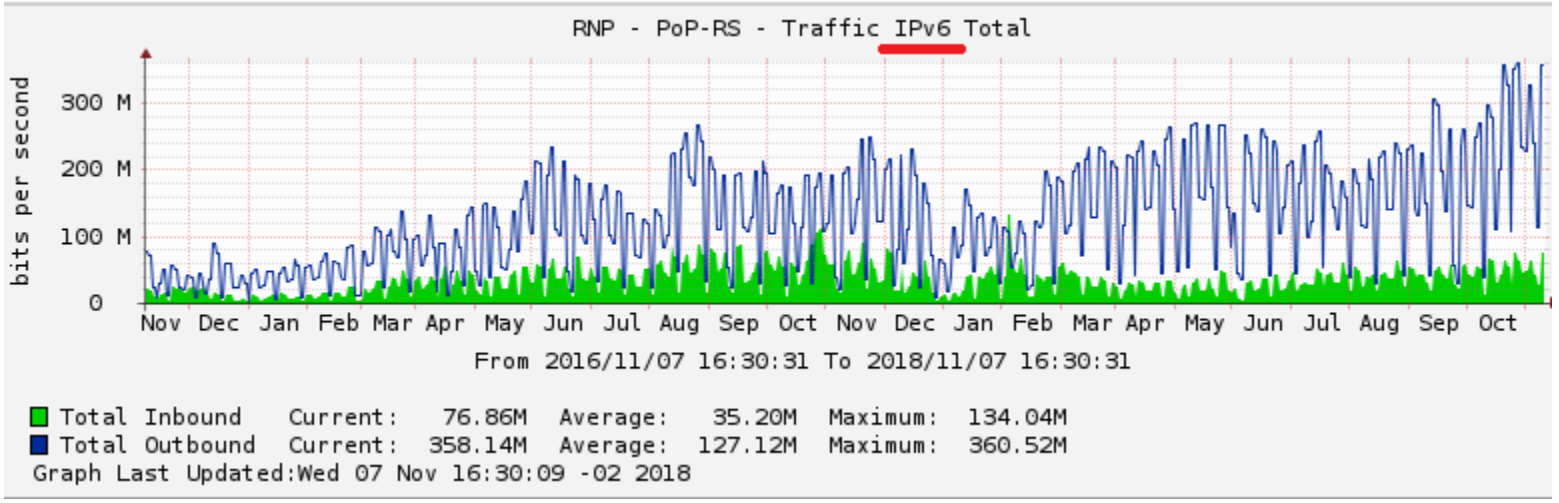
- *Em IPv4 - aumentar o pool de IPs no NAT e/ou aumentar o número de servidores de NAT.*

- *Em IPv6 – Distribuir endereços IPv6, pois como não existe NAT, vai melhor a performance*

Panorama

- *100 % dos clientes possuem uma rede /48 alocada para sua instituição.*
- *45% dos clientes, ainda não utilizam IPv6.*

Auxílio? suporte@pop-rs.rnp.br



Boas práticas IPv6

- Utilizar redes /64 para cada seguimento da rede
- Utilizar endereços fáceis para servidores. Ex: 2804:0:faca::1
- Desabilitar o RA (*router advertisement*)
- Configurar o DHCPv6 (para ter o registro de logs)
- Desabilitar endereços IPv6 temporários no Windows.

  netsh interface ipv6 set privacy state=disabled

  netsh interface ipv6 set global randomizeidentifiers=disabled

Registros de Logs

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

```
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}
```

Você sabe quais usuários estavam acessando a Internet de sua rede, as 10h da manhã de 3 de setembro de 2017 (Endereço IP, MAC e usuário) ?

- Cuidar para que todos seus recursos computacionais estejam como o horário correto – utilizar servidor de NTP
- Armazenar os acessos à rede (LDAP, AD, etc)
- Registros de DHCP/DHCPv6
- Armazenar esses registros em um servidor de log
- Cuidado: o Linux armazena por padrão os logs de acesso por 2 meses.

Obrigado(a)!

César Augusto Hass Loureiro

cesar@pop-rs.rnp.br