13º Encontro de CSIRTs acadêmicos

Guilherme Ladvocat
Gerência de Operações
05/12/18

RNP

Ministério da **Cultura**

Ministério da **Saúde**

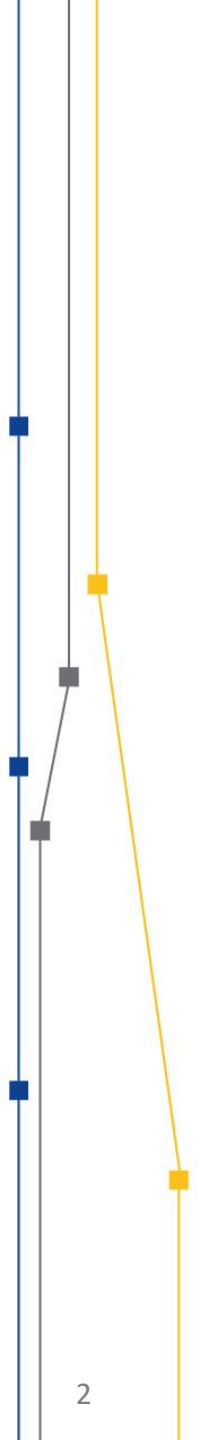
Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

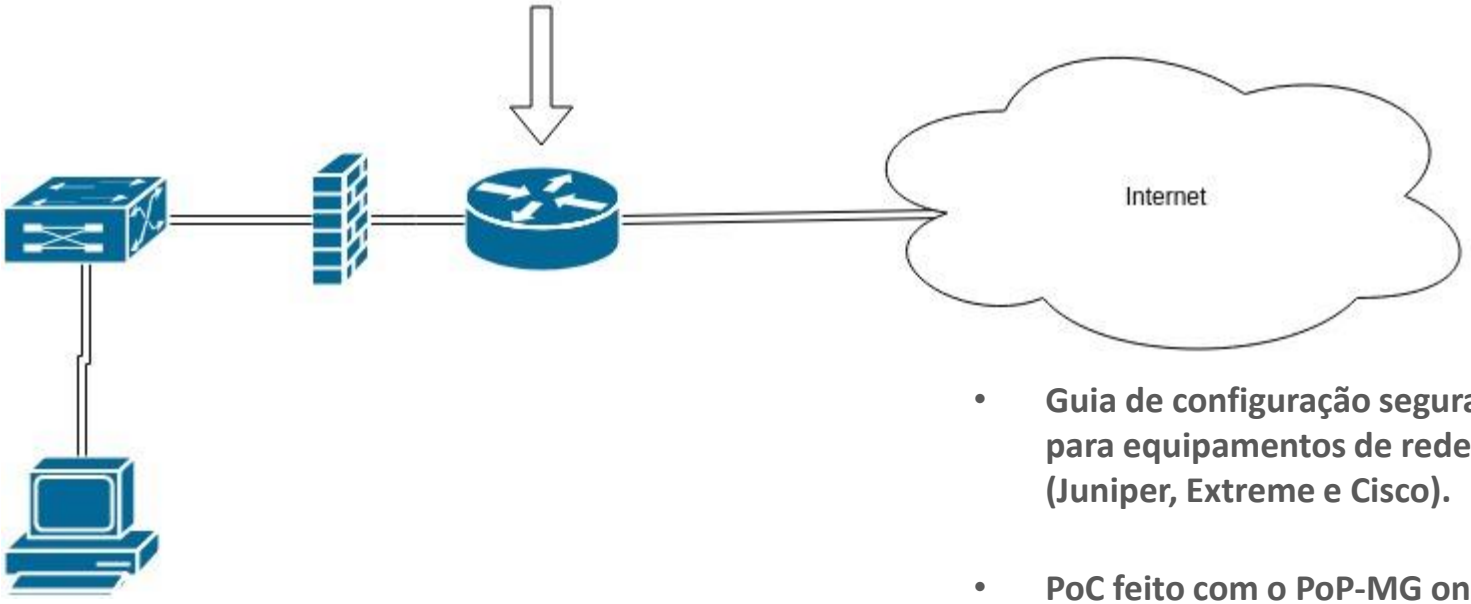
GOVERNO FEDERAL
BRASIL
PÁTRIA EDUCADORA

Agenda

- Hardening de equipamentos de rede
- Ataques DoS amplificados
- Recomendações (do ponto de vista de eng. de redes)

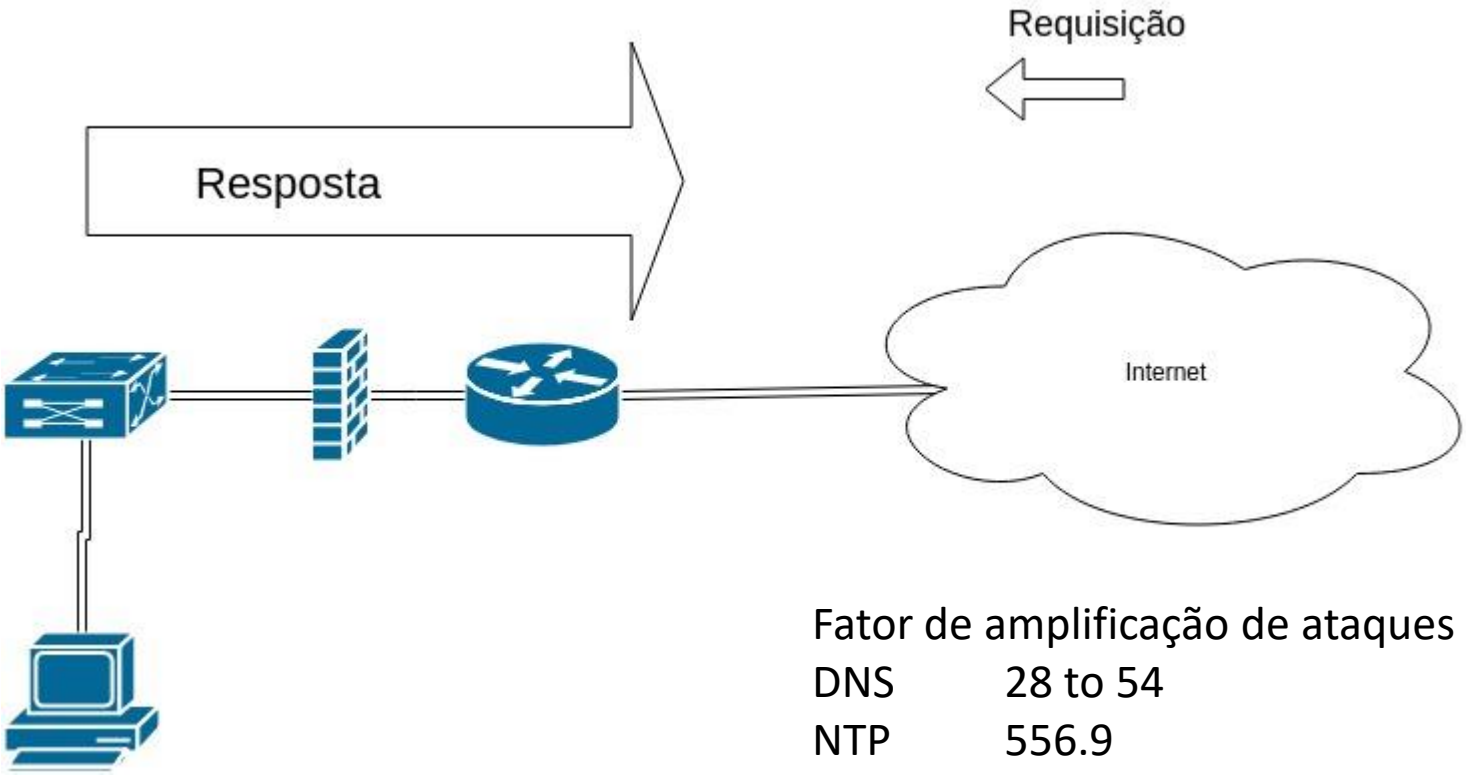


Hardening de equipamentos de rede



- Guia de configuração segura para equipamentos de rede (Juniper, Extreme e Cisco).
- PoC feito com o PoP-MG onde todos os roteadores da planta foram configurados e um guia gerado.
- As config. do guia previnem ataques ao control-plane do roteador e ataques spoofing originados na LAN (uRPF).

Ataques DoS amplificados



Fator de amplificação de ataques DoS:

DNS	28 to 54
NTP	556.9
LDAP	46 to 55

Memcached 10,000 to 51,000

Fonte: https://www.us-cert.gov/ncas/alerts/TA14-017A

Algumas tecnologias de rede voltadas para segurança

Segurança LAN:

Port-security

802.1x

Dhcp snooping

Firewall

IDS / IPS

uRPF

Segurança Control Plane (hardening)

Segurança WAN:

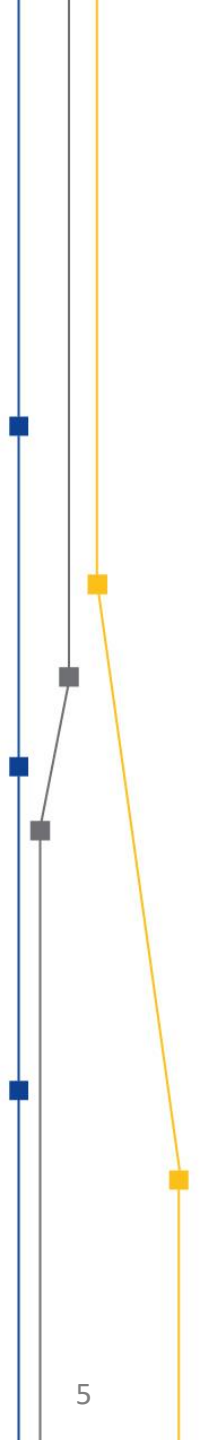
Análise de fluxos

Black-hole

Flowspec

Segurança de roteamento

DDOS



Recomendações (do ponto de vista de eng. de redes)

- Envio de logs para servidor.
- Análise de anomalias em gráficos de utilização de banda (ex.: tráfego de upload alto em situações não previstas).
- Análise de perfil de tráfego (aplicações, protocolos).
- Hardening de equipamentos, servidores e aplicações.
- Documentar procedimentos.

Obrigado!

Guilherme Ladvocat

guilherme.ladvocat@rnp.br

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

GOVERNO FEDERAL BRASIL PÁTRIA EDUCADORA