TROUBLESHOOTIN G LIKE A BOSS

DANIEL DAMITO

ANDRÉ ALMEIDA

TEMOS TRÊS MOTIVAÇÕES

Motivação 1:

Medidas de segurança na Internet têm causado muitos problemas de abertura de conteúdo e as pessoas têm dificuldades de diagnosticar.

Estes problemas de conteúdo geralmente acontecem em dois lugares diferentes:

1) No provedor de conteúdo que faz bloqueio, acidental ou propositalou

2) Algum trânsito ou sistema autônomo no meio do caminho tomando alguma medida de manipulação de tráfego, geralmente com intuito de combater DDoS.

Motivação 2:

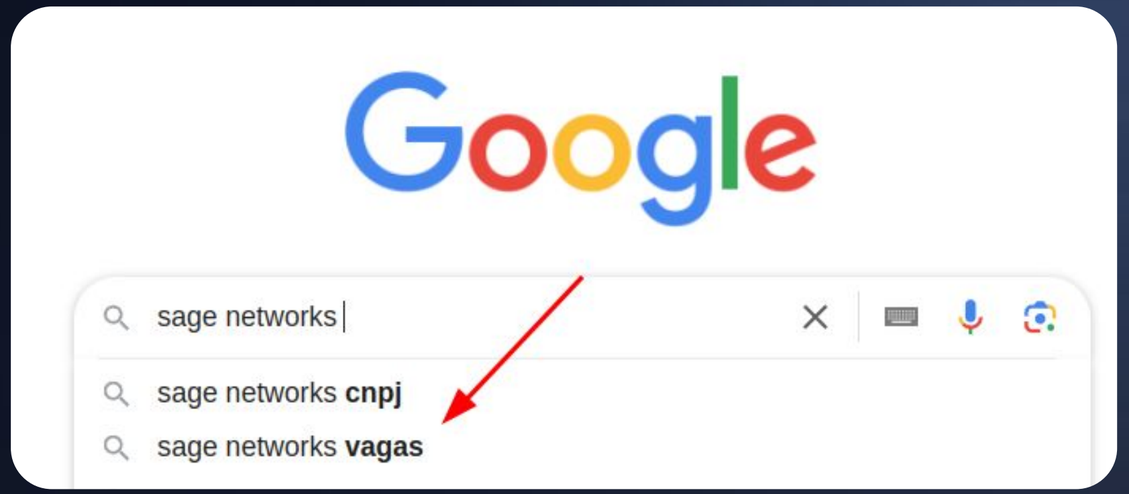
Normalmente vemos profissionais experientes falando groselhas, como:

- IPv6 ainda é pouco usado
- Portas abertas atraem ataques DDoS*
- O 8.8.8.8 é mais rápido que um DNS local
- Perdas de pacote no meio do traceroute indicam problemas

*Ataques onde você é a vítima de fato, excluindo-se casos onde você é usado apenas para reflexão.

Motivação 3:

Processo seletivo recente mostrando que as pessoas não entendem conceitos básicos, como DNS.



SAGE NETWORKS

Especialistas em mitigação de ataques DDoS e consultoria técnica e estratégica para provedores de internet.

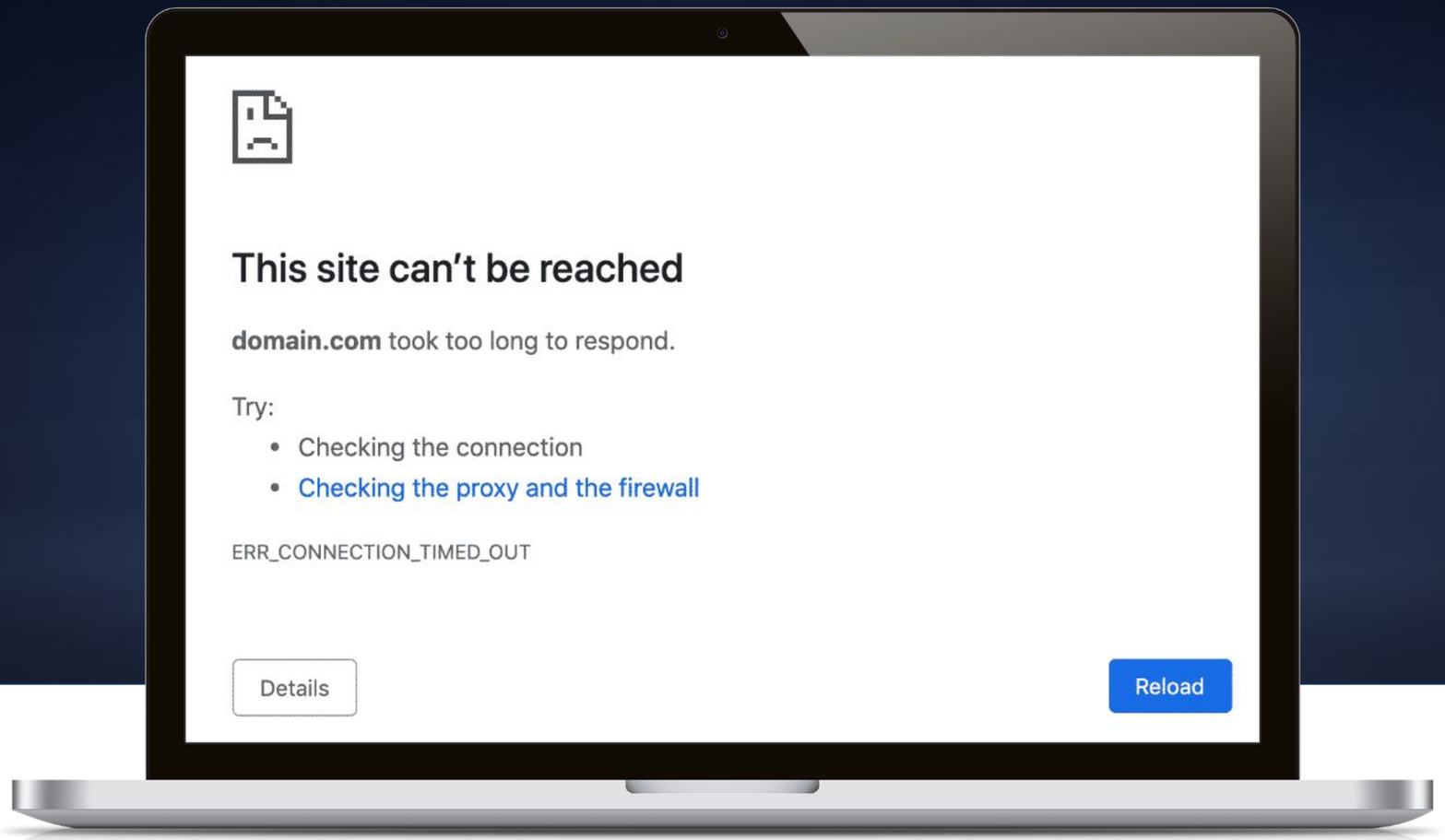
- Serviços de Redes
- Soluções Anti-DDoS
- Cibersegurança
- Venda de Equipamentos
- Link Dedicado

CONCEITOS BÁSICOS

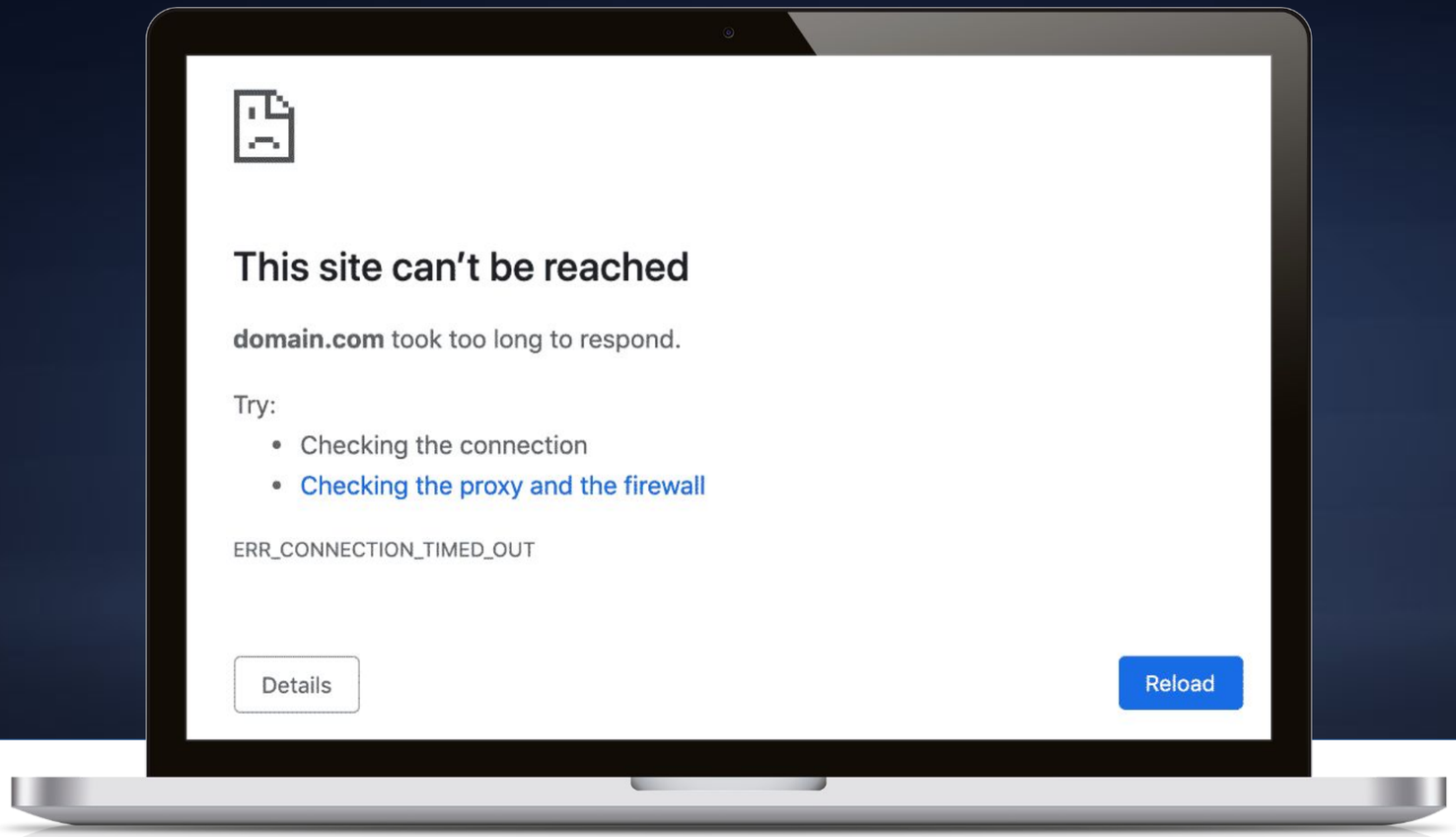
Para que você seja considerado um profissional de **Internet** realmente experiente, você deve entender **plenamente** (entre outras coisas):

- Entendimento das camadas do modelo OSI
- Como uma conexão TCP funciona
- Conceitos de DNS, inclusive a diferença de recursivo para autoritativo
- Como fazer e ler uma captura de pacotes no Wireshark
- Conceitos de roteamento estático e dinâmico
- BGP

COMO INICIAR ESTE TROUBLESHOOTING ?



COMO INICIAR ESTE TROUBLESHOOTING ?



Se você não começou pela mensagem de erro, deveria!
ERR_CONNECTION_TIMED_OUT

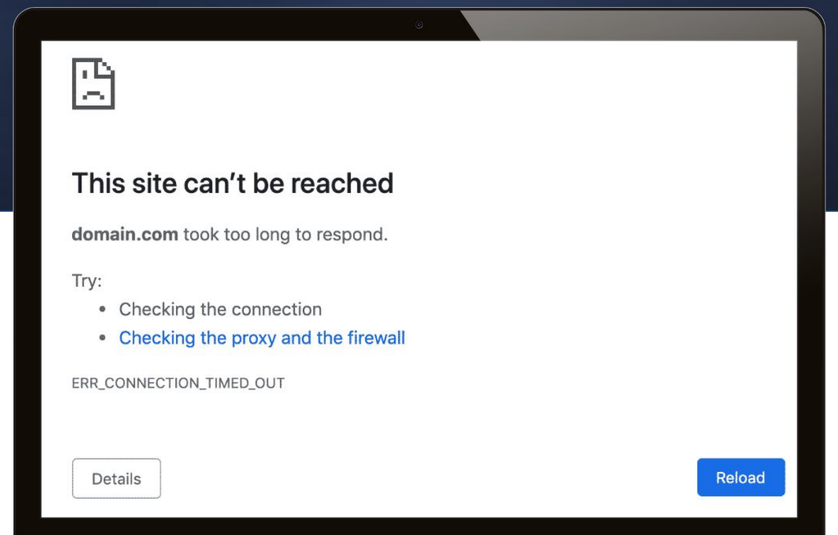
POSSÍVEIS ERROS

NAVEGADOR

Você não chegou a ter comunicação em camada 4 com o servidor ou teve **falha com o certificado.** Exemplos: Falhas de roteamento, DNS, bloqueios e etc.

DO HTTP, DEFINIDO NA RFC 9110

Você chegou a estabelecer conexão com o servidor, mas teve algum problema.



POSSÍVEIS ERROS

ERROS DE HTTP

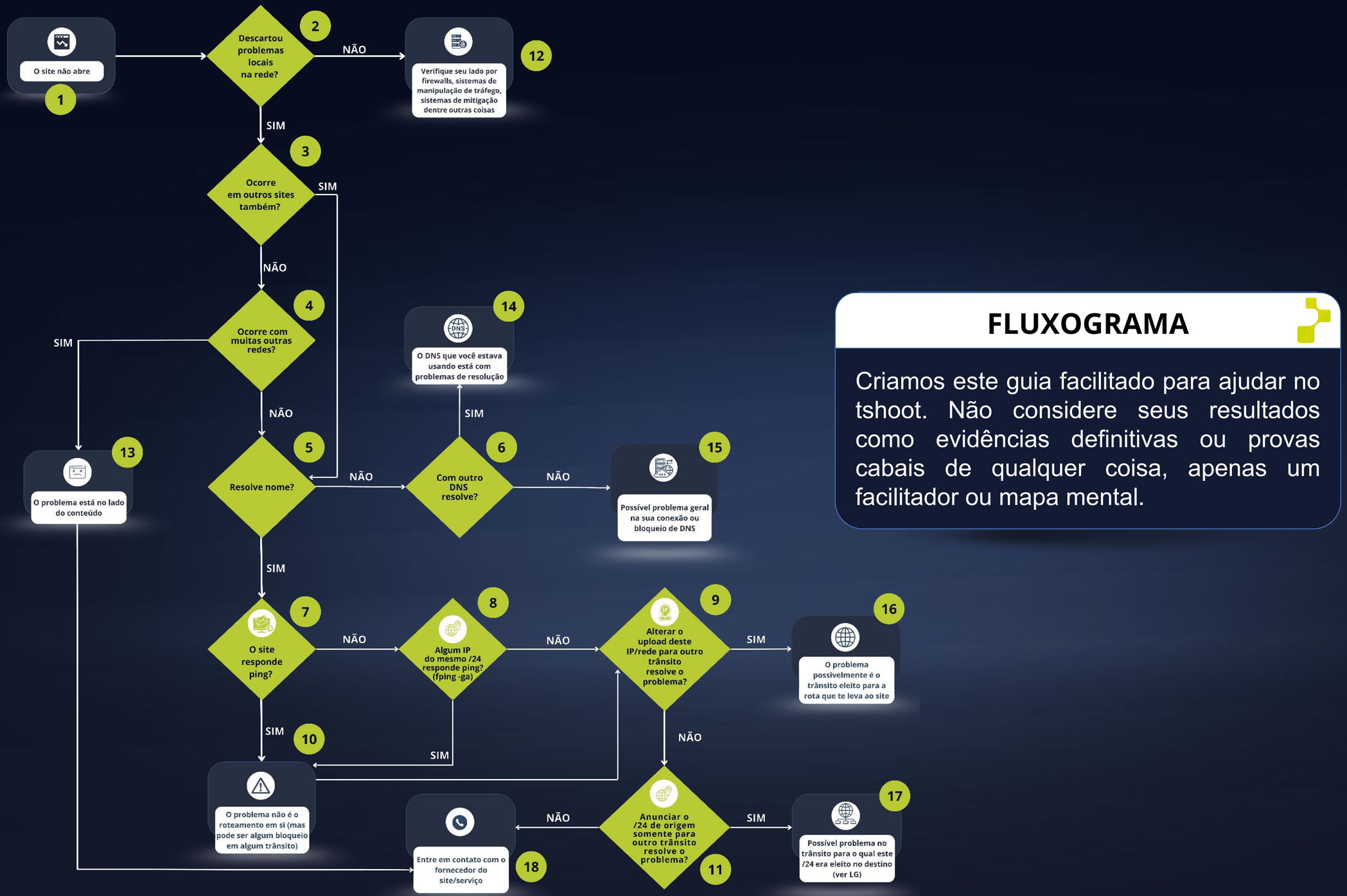
- De 100 a 199: Respostas Informativas.
- De 200 a 299: Respostas Bem-sucedidas.
- De 300 a 399: Mensagens de Redirecionamento.
- De 400 a 499: Respostas de Erro do Cliente.😕
- De 500 a 599: Respostas de Erro do Servidor.😀

- A bucha pode ser sua 😕
- Esta bucha provavelmente não é tua 😀

ERROS DO NAVEGADOR

Cada navegador exibe as mensagens de erro de uma forma diferente. Mas as mensagens mais comuns contém as seguintes palavras e significados:

- TIMED OUT: demorou muito tempo para abrir. 😕
- DNS / NAME NOT RESOLVED: problemas com DNS. 😕
- REJECTED / REFUSED: o site negou tua conexão. 😀
- SSL / CERTIFICADO: problemas com certificado inválido.



FLUXOGRAMA

Criamos este guia facilitado para ajudar no tshoot. Não considere seus resultados como evidências definitivas ou provas cabais de qualquer coisa, apenas um facilitador ou mapa mental.

NÃO CONFIE CEGAMENTE NO PING

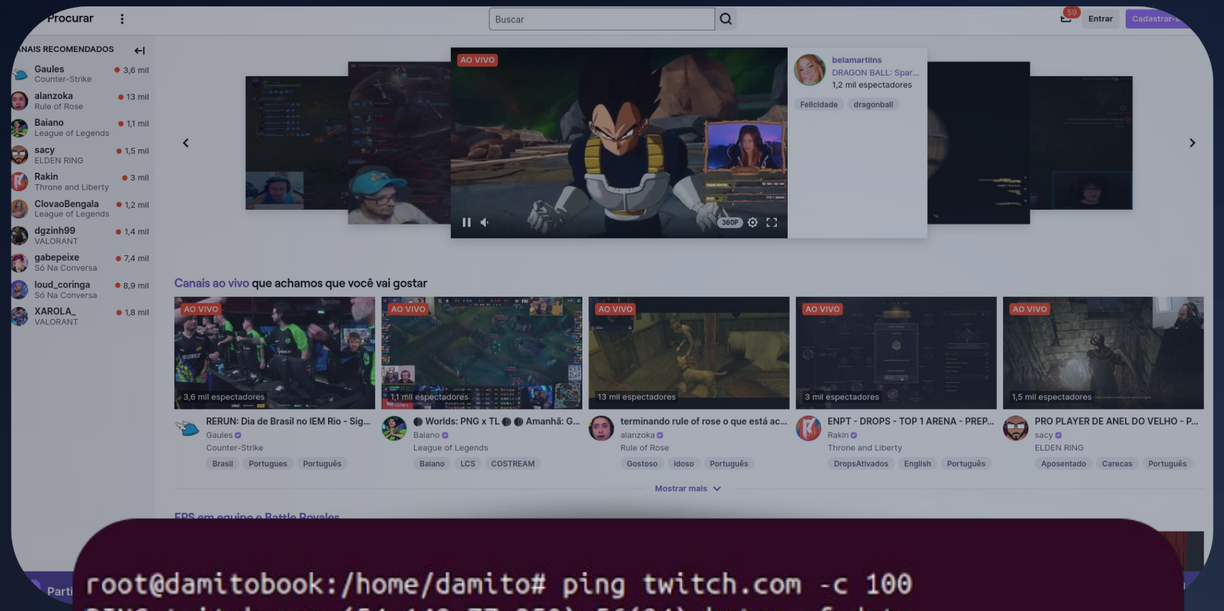
MAS POR QUE NÃO?

O ping não é necessariamente uma evidência de problema. É possível o site não responder ping mas funcionar normalmente. **Exemplos:**

- xvideos.com e twitch.com (v4 only, eca! 🥵);
- Qualquer outro bloqueio de ICMP por qualquer razão, como DDoS.

A maior utilidade do ICMP é facilitar o troubleshooting de duas formas:

- Evidenciando que o problema não é de roteamento;
- Identificando rapidamente quando uma mudança surtir efeito.



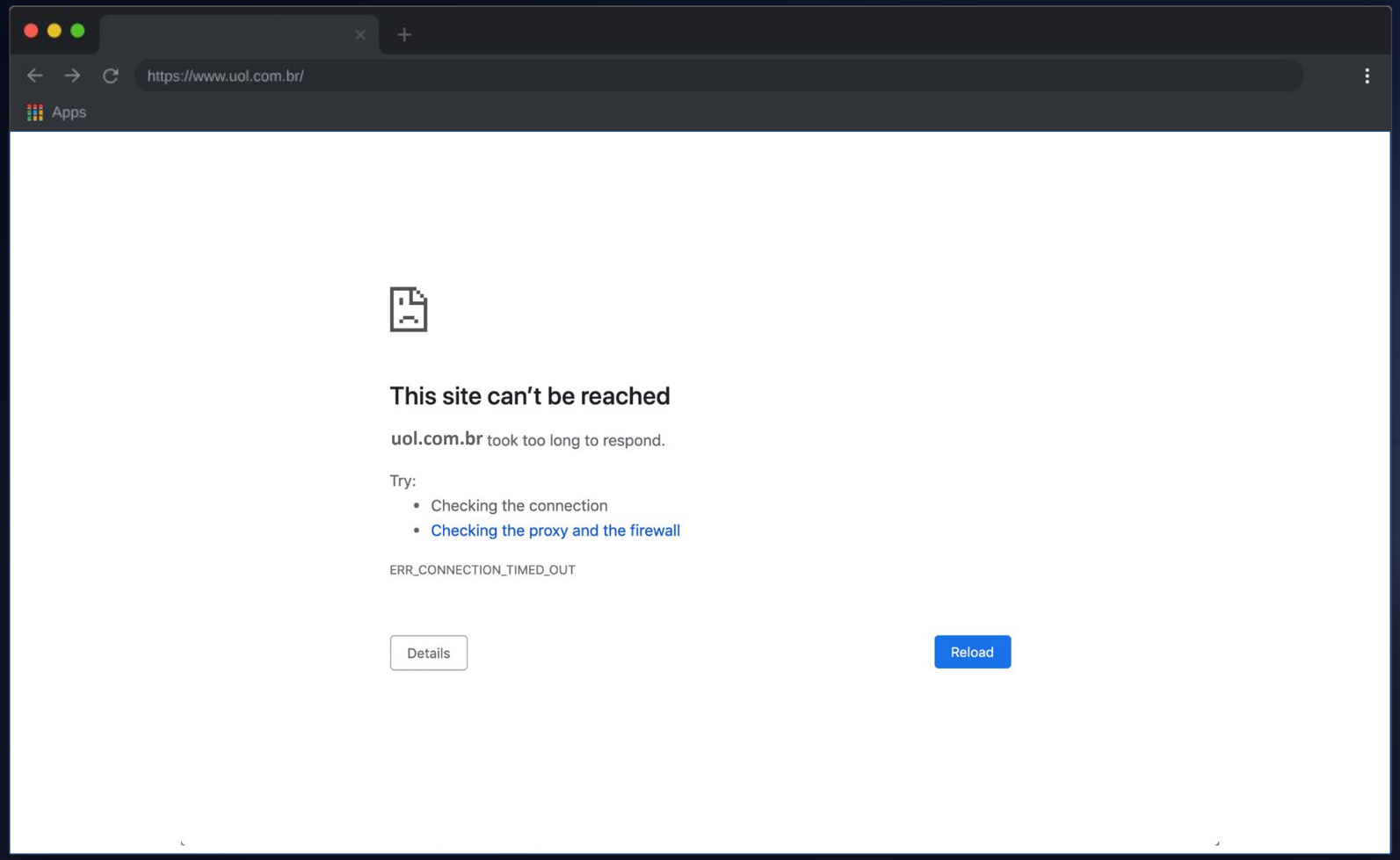

```
root@damitobook:/home/damito# ping twitch.com -c 100
PING twitch.com (54.148.77.250) 56(84) bytes of data.

--- twitch.com ping statistics ---
100 packets transmitted, 0 received, 100% packet loss, time 101361ms

root@damitobook:/home/damito#
```

ESTUDO DE CASO

SITE NÃO ABRE



IPV4

Usuário só usa IPV4

Cliente não consegue abrir o site:
UOL.COM.BR

ESTUDO DE CASO

SITE NÃO ABRE

ETAPA 5 - Testar a resolução de nome (DNS)

```
damito@damitobook:~$ host uol.com.br
uol.com.br has address 200.147.35.149
```

RESOLVE NOME?
SIM

ESTUDO DE CASO

SITE NÃO ABRE

ETAPA 7 - Teste de ICMP (ping) para o site

```
damito@damitobook:~$ ping 200.147.35.149 -Ac 5
PING 200.147.35.149 (200.147.35.149) 56(84) bytes of data.

--- 200.147.35.149 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4005ms
```

O site responde ping?

NÃO

ESTUDO DE CASO

SITE NÃO ABRE

ETAPA 8 - Teste de ICMP (ping) pro /24

```
damito@damitobook:~$ fping -gae 200.147.35.0/24
damito@damitobook:~$
```

Algum IP do mesmo /24 responde ping? (fping -ga)

NÃO

ESTUDO DE CASO

SITE NÃO ABRE

ETAPA 9 - Trocar o upload para outro trânsito

```
[~GTER2024] ip route-static 200.147.35.0 255.255.255.0 GigabitEthernet0/5/16
```

Não esqueça de remover esta rota depois do teste

Alterar o upload deste IP/rede para outro trânsito resolve o problema?

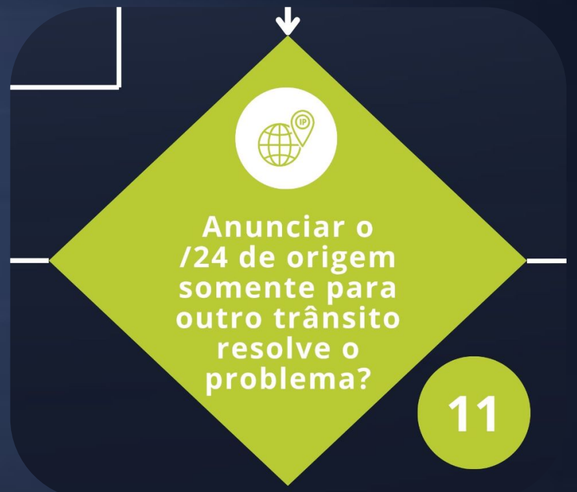
NÃO

ESTUDO DE CASO

SITE NÃO ABRE

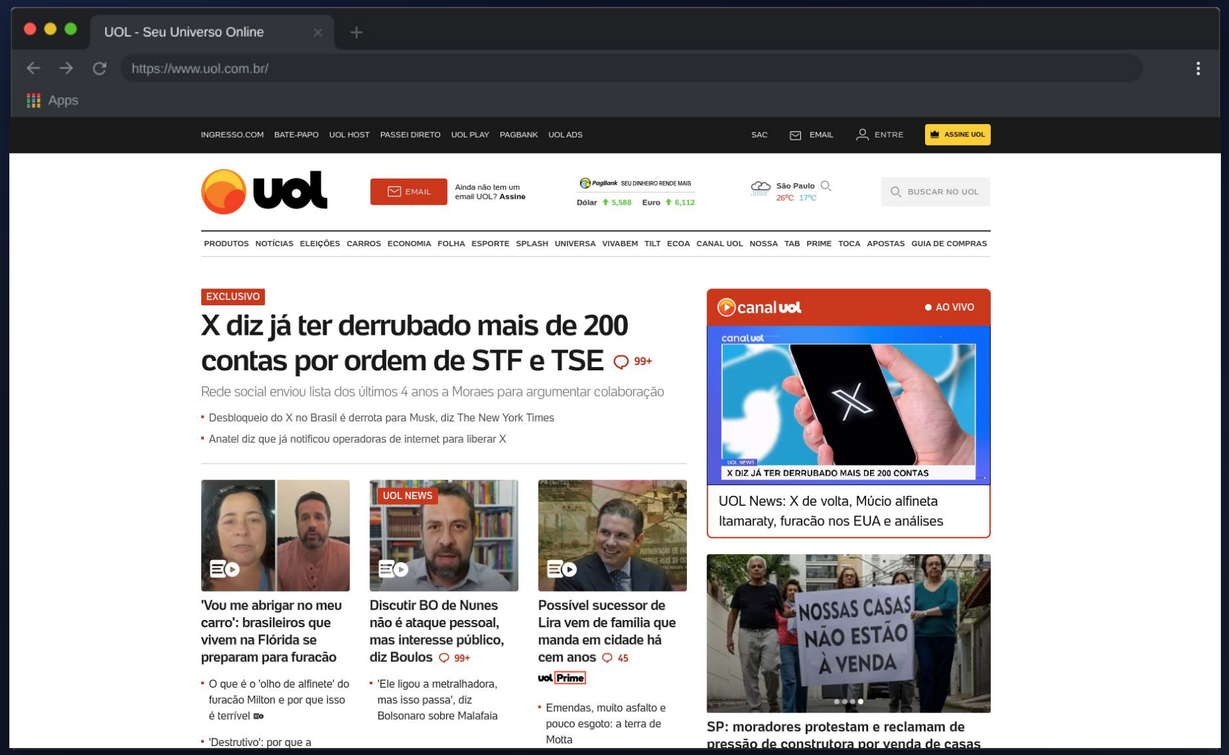
ETAPA 11 - Anunciar mais específico pra outro trânsito

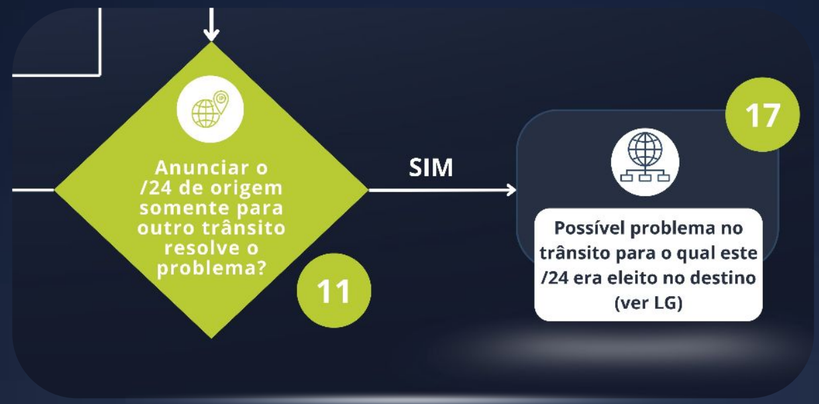
```
[~GTER2024-route-policy]dis th
#
route-policy PL-TRANSITO1-OUT permit node 1
 if-match ip-prefix REDE-24-ORIGEM
#
return
```



ESTUDO DE CASO

SITE NÃO ABRE





CONCLUSÃO

Como o site voltou a abrir após a manipulação do anúncio, já temos uma suspeita forte de que o problema é no trânsito.

Isto não é uma evidência incontestável, mas já é o mínimo que você precisa pra abrir um chamado com o fornecedor solicitando ajuda sobre isso.

REFERÊNCIAS E LINKS ÚTEIS

FURTADO, Leonardo. Tutorial de BGP: boas vindas ao BGP 101!. 2024. Disponível em: https://www.youtube.com/watch?v=mh-P8NWXKic&list=PL1ohpeRa0gZ_QPowFpzaUfLjlNthU9KUc. Acesso em: 10 out. 2024.

KALAU, Gustavo. **Looking Glass BGP - Demonstração e explicação!**. YouTube, 2023. Disponível em: https://www.youtube.com/watch?v=BY3PVyCsqDM. Acesso em: 10 out. 2024.

DAMITO, Daniel. **Fluxograma Simplificado para Troubleshooting de Problemas com Sites**. Brasil Peering Forum Wiki, 2023. Disponível em: https://wiki.brasilpeeringforum.org/w/Fluxograma_Simplificado_para_Troubleshooting_de_Problemas_com_Sites. Acesso em: 10 out. 2024.

FIGUEIREDO, Jean. Troubleshooting com Wireshark. Disponível em: https://www.youtube.com/watch?v=oQVO51j9StE. Acesso em: 10 out. 2024.

SAGE NETWORKS. Relembre por que você deveria dar mais importância ao IPv6. 2023. Disponível em: https://sagenetworks.com.br/en/relembre-por-que-voce-deveria-dar-mais-importancia-ao-ipv6/. Acesso em: 10 out. 2024.

SAGE NETWORKS

WWW.SAGENETWORKS.COM.BR

sage_networks Sage Networks +55 (19) 3500-6269