GTS 37

24 de Outubro de 2022 - São Paulo

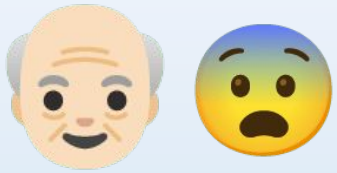
Indo além do RPZ de DNS para cumprir ordens Judiciais à ISPs para bloqueios de acesso à sites e domínios

Uma técnica simples, barata, e **Mikrotikiniana**.

IMPORTANTE -> Ponto de Vista do ISP

Autor: Douglas Fernando Fischer – fischerdouglas@gmail.com

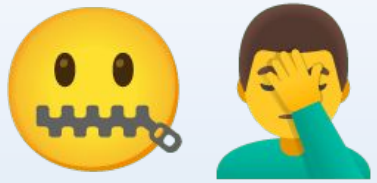
Douglas Fernando Fischer

- Engenheiro de Controle e Automação
- Atua na área de redes de telecomunicações desde 1999 
- Trabalhou como engenheiro de pré-vendas e implantação em integradores de tecnologia
- Consultor na área de redes e servidores nos segmentos corporativo e de provedores de Internet
- Tretísta com objetivos produtivos nas horas vagas
  - “O segredo de aborrecer é dizer tudo.” Voltaire

- BPF – http://brasilpeeringforum.org/

- Made4it - http://www.made4it.com.br/

Disclaimer

- Eu falo muitos palavrões! 
- Eles são direcionados a quem está fazendo coisa errada.
  - Se você está fazendo coisa errada:
    - Te mexa! Arrume isso logo! 
  - Se você não está fazendo coisa errada:
    - #FicaEmPaz e me ajude a conscientizar os aBiguinhos.
- Peço desculpas antecipadamente.
- Se observarem que estou fazendo coisa errada, POR FAVOR, me ajudem a corrigir e melhorar.

Intenções dessa apresentação?

- Comentar sobre as ordens judiciais de bloqueio de acesso à web sites no Brasil e demais países da américa latina.
  - NÃO ~~Discutir se esses bloqueios são ou não corretos juridicamente.~~ NÃO
- Expor algumas das metodologias técnicas para cumprimento dessas ordens de bloqueio.
  - Métodos de aplicação dos filtros.
  - Efeitos colaterais indesejados.
  - Maneiras de driblar esses bloqueios.
- Apresentar uma receita de bolo baseada em Mikrotik RouterOS com alto nível de eficácia, baixo custo, e baixo nível de efeitos colaterais indesejados.

Mas antes…

Aquela TRETA gostosa com objetivo PRODUTIVO

Você é um operador de ISP?

- Clientes finais

Seu ISP não tem um BOM serviço DNS Recursivo INTERNO?

- Seguro
- Rápido
- Com Privacidade
- Perto(em ms) dos seus clientes
- Tolerante a falhas

Você está sendo um PÉSSIMO operador de ISP!

Seu cliente deveria mudar de ISP! Tome vergonha na cara!

Assistam a palestra do Thiago Ayub amanhã - GTER - às 14:45

Intenções dessa apresentação?

- **Comentar sobre as ordens judiciais de bloqueio de acesso à web sites no Brasil e demais países da américa latina.**
  - NÃO ~~Discutir se esses bloqueios são ou não corretos juridicamente.~~ NÃO
- Expor algumas das metodologias técnicas para cumprimento dessas ordens de bloqueio.
  - Métodos de aplicação dos filtros.
  - Efeitos colaterais indesejados.
  - Maneiras de driblar esses bloqueios.
- Apresentar uma receita de bolo baseada em Mikrotik RouterOS com alto nível de eficácia, baixo custo, e baixo nível de efeitos colaterais indesejados.

Alvos frequentes das Ordens Judiciais de Bloqueio

- Pedofilia
- Sites de jogos
- Notícias Falsas

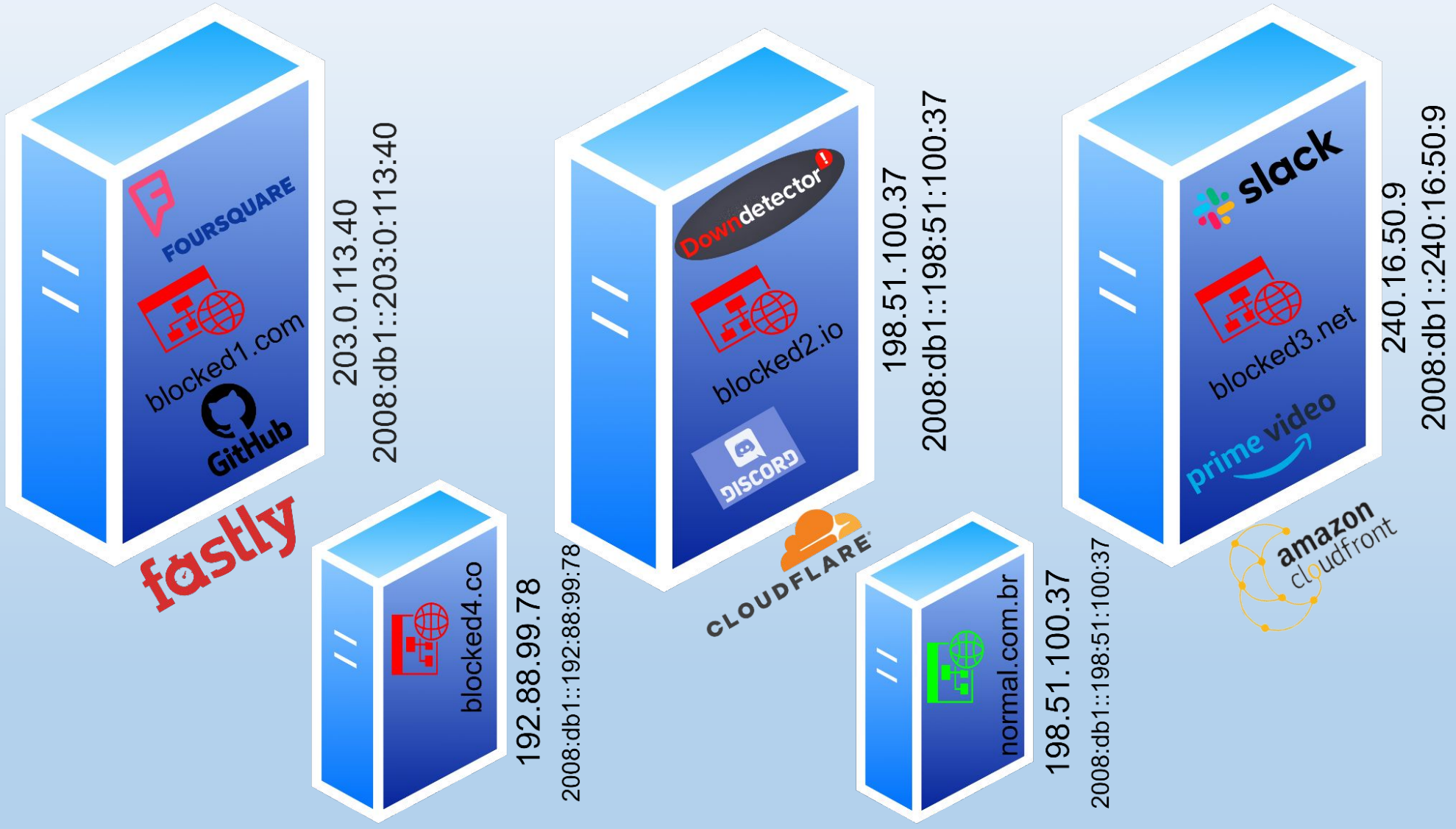
Erros ou Equívocos Frequentemente Cometidos

- Ordem ao ISP para bloqueio de um somente um conteúdo específico de um web-site.
  - https://www.redesocial.exemplo.zz/paginaespecifica/
- Ordem ao ISP para bloqueio de “tudo que for da empresa tal”
- Go-Horse na hora de bloquear tudão referente aos IPs de destino para os quais os FQDN apontam
- “Não preciso fazer nada”
- Provedores que vendem Trânsito IP fazem fazem as configurações para o bloqueio de maneira que isso afete os usuários de SISTEMAS AUTÔNOMOS que não os dela mesma.

Intenções dessa apresentação?

- Comentar sobre as ordens judiciais de bloqueio de acesso à web sites no Brasil e demais países da américa latina.
  - NÃO ~~Discutir se esses bloqueios são ou não corretos juridicamente.~~ NÃO
- Expor algumas das metodologias técnicas para cumprimento dessas ordens de bloqueio.
  - Métodos de aplicação dos filtros.
  - Efeitos colaterais indesejados.
  - Maneiras de driblar esses bloqueios.
- Apresentar uma receita de bolo baseada em Mikrotik RouterOS com alto nível de eficácia, baixo custo, e baixo nível de efeitos colaterais indesejados.

Sites bloqueados estão misturados com sites normais.



Sites bloqueados estão misturados com sites normais

```
fischerdouglas@fischer-vaio:~$ dig www.downdetector.com A +short
172.64.149.95
104.18.38.161
fischerdouglas@fischer-vaio:~$ whois 172.64.149.95 | grep OrgName:
OrgName:        Cloudflare, Inc.
fischerdouglas@fischer-vaio:~$ whois 104.18.38.161 | grep OrgName:
OrgName:        Cloudflare, Inc.
fischerdouglas@fischer-vaio:~$
fischerdouglas@fischer-vaio:~$
fischerdouglas@fischer-vaio:~$ dig www.downdetector.com AAAA +short
2606:4700:4400::ac40:955f
2606:4700:4400::6812:26a1
fischerdouglas@fischer-vaio:~$ whois 2606:4700:4400:: | grep OrgName:
OrgName:        Cloudflare, Inc.
fischerdouglas@fischer-vaio:~$
```

Bloqueio de Acesso a Sites e Domínios

Maneiras de se implementar bloqueio de acesso a sites e domínios em uma rede.							Como o usuário pode by-passar?	
Metodologia	Onde/como é Aplicado?	Custo	Complexidade	Efetividade	Quebra de Privacidade	Efeitos Colaterais	Método	Dificuldade
RPZ Alteração/Bloqueio de respostas DNS	Servidor DNS Recursivo	Baixo	Média Baixa	Baixa	Nula ou baixa	Muito Baixos	Troca DNS Endpoint	Fácil
							Troca DNS CPE	Fácil
							Serviços de VPN	Média
Filtro/ACL ou Blackhole dos IPs dos Servidores que hospedam os sites	B-RAS/BNGs Border BGP	Baixo	Baixa	Alta	Nula ou baixa	Muito Altos	Serviços de VPN	Média
Man-in-the-Middle Deep Inspection	Appliances especializados NGFW	Alto	Alta	Muito Alta	Muito Alta	Altos	Serviços de VPN	Média
Inspeção do TLS-Host ● Unidirecional ○ Somente Upload ● IPs específicos	BGP + Firewall Básico	Baixo	Média	Alta	Baixa	Baixos ou Muito Baixos	Serviços de VPN	Média

Intenções dessa apresentação?

- Comentar sobre as ordens judiciais de bloqueio de acesso à web sites no Brasil e demais países da américa latina.
  - NÃO ~~Discutir se esses bloqueios são ou não corretos juridicamente.~~ NÃO
- Expor algumas das metodologias técnicas para cumprimento dessas ordens de bloqueio.
  - Métodos de aplicação dos filtros.
  - **Efeitos colaterais indesejados.**
  - Maneiras de driblar esses bloqueios.
- Apresentar uma receita de bolo baseada em Mikrotik RouterOS com alto nível de eficácia, baixo custo, e baixo nível de efeitos colaterais indesejados.

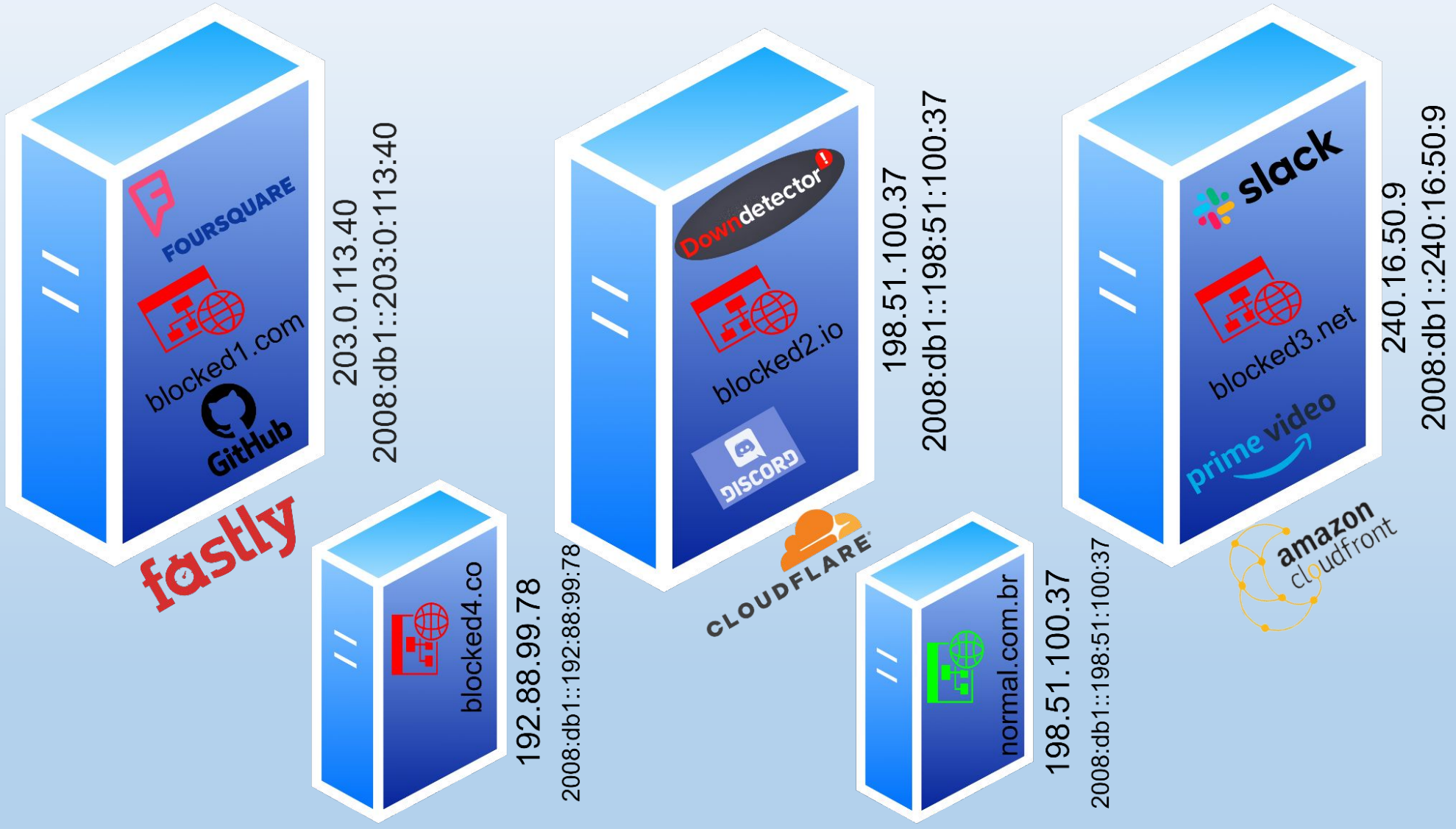
POSSÍVEIS efeitos colaterais

- Servidores DNS recursivos padecendo
  - Erros de configuração
  - Aumento da demanda computacional
- Falha na tarefa de bloquear
  - FQDNs com muitos IPs, TTLs baixos, e em constante alternância.
  - DoT no Browser -> By-Pass quase involuntário
- Não funcionamento de sites não bloqueados
  - HTTP 1.1 -> um IP e muitos domínios
- Quebra de Certificados SSL/TLS
  - Man-in-the-Middle -> Decrypt-Recrypt
- Desse último eu falo no final….

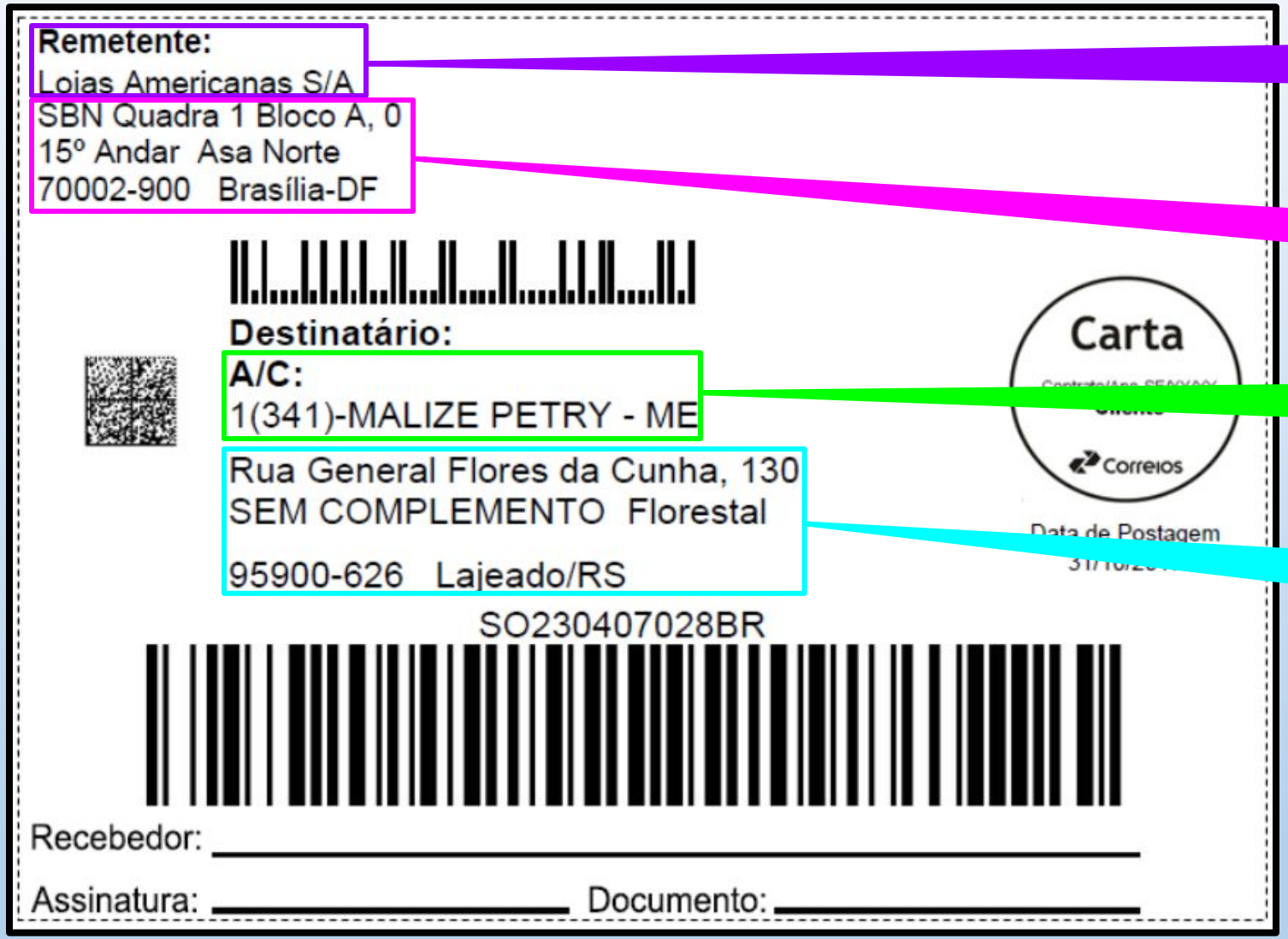
Intenções dessa apresentação?

- Comentar sobre as ordens judiciais de bloqueio de acesso à web sites no Brasil e demais países da américa latina.
  - NÃO ~~Discutir se esses bloqueios são ou não corretos juridicamente.~~ NÃO
- Expor algumas das metodologias técnicas para cumprimento dessas ordens de bloqueio.
  - Métodos de aplicação dos filtros.
  - Efeitos colaterais indesejados.
  - Maneiras de driblar esses bloqueios.
- **Apresentar uma receita de bolo baseada em Mikrotik RouterOS com alto nível de eficácia, baixo custo, e baixo nível de efeitos colaterais indesejados.**

Sites bloqueados estão misturados com sites normais.



Comparação de uma correspondência com um acesso HTTP 1.1



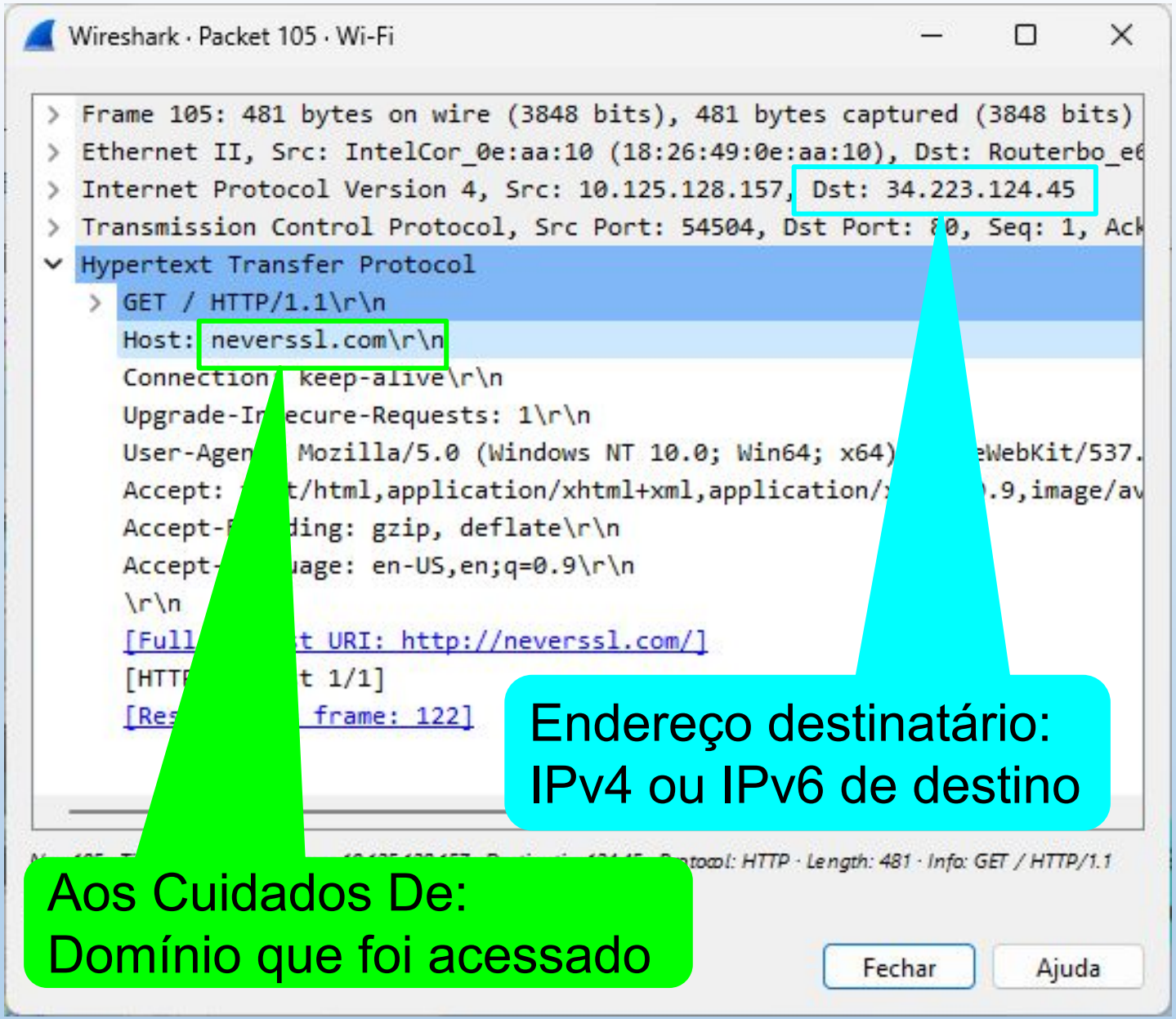
Remetente:
Usuário acessando o site

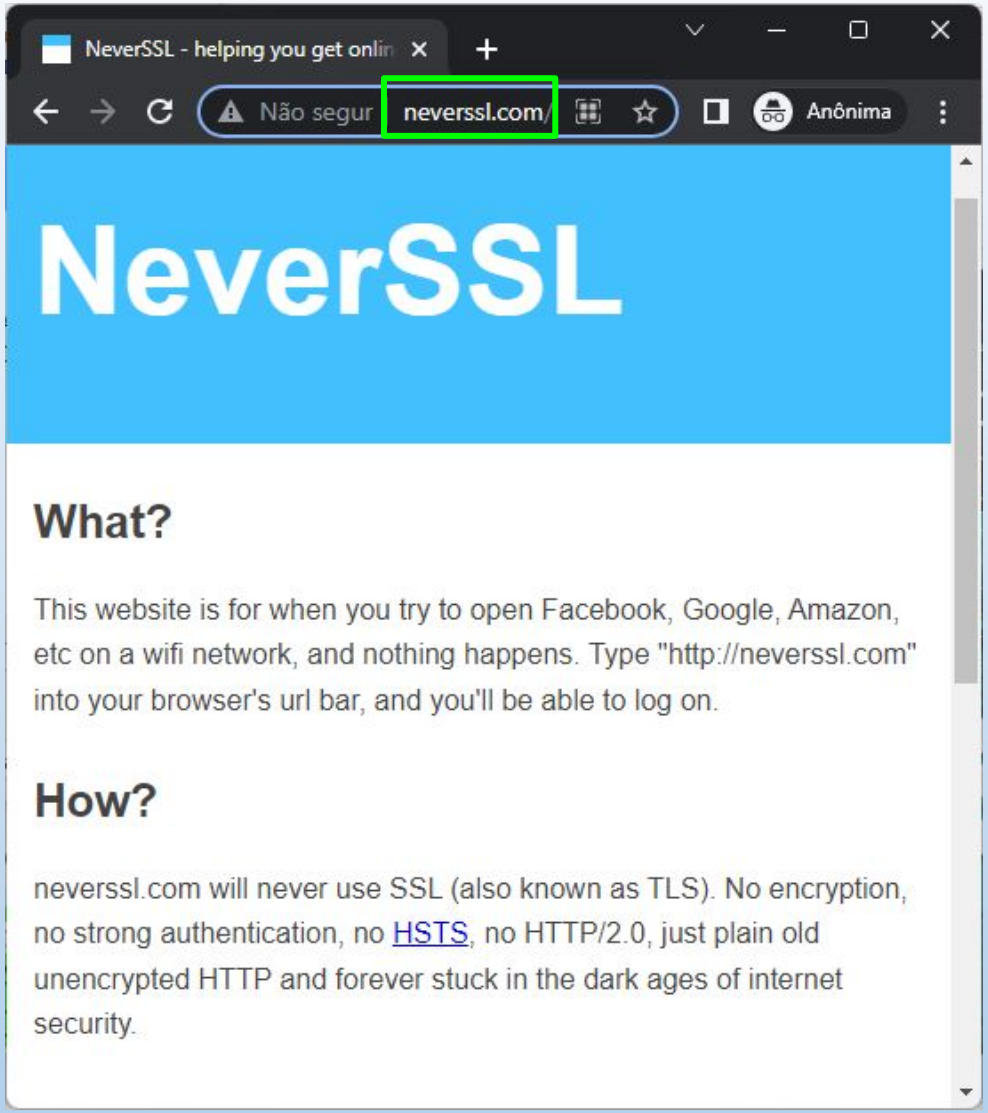
Endereço remetente:
IPv4 ou IPv6 de origem

Aos Cuidados De:
Domínio que foi acessado

Endereço destinatário:
IPv4 ou IPv6 de destino

https://www.correios.com.br/enviar/correspondencia/arquivos/nacional/guia-tecnico-de-enderecamento-de-correspondencias.pdf


Wireshark · Packet 105 · Wi-Fi
Frame 105: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits)
Ethernet II, Src: IntelCor_0e:aa:10 (18:26:49:0e:aa:10), Dst: Routerbo_e6
Internet Protocol Version 4, Src: 10.125.128.157, Dst: 34.223.124.45
Transmission Control Protocol, Src Port: 54504, Dst Port: 80, Seq: 1, Ack
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: neverssl.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.
Accept: text/html,application/xhtml+xml,application/x
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://neverssl.com/]
[HTTP request 1/1]
[Response in frame: 122]
Endereço destinatário:
IPv4 ou IPv6 de destino
Aos Cuidados De:
Domínio que foi acessado
Fechar
Ajuda


NeverSSL - helping you get onlin
Não segur
neverssl.com/
Anônima
NeverSSL
What?
This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be able to log on.
How?
neverssl.com will never use SSL (also known as TLS). No encryption, no strong authentication, no HSTS, no HTTP/2.0, just plain old unencrypted HTTP and forever stuck in the dark ages of internet security.

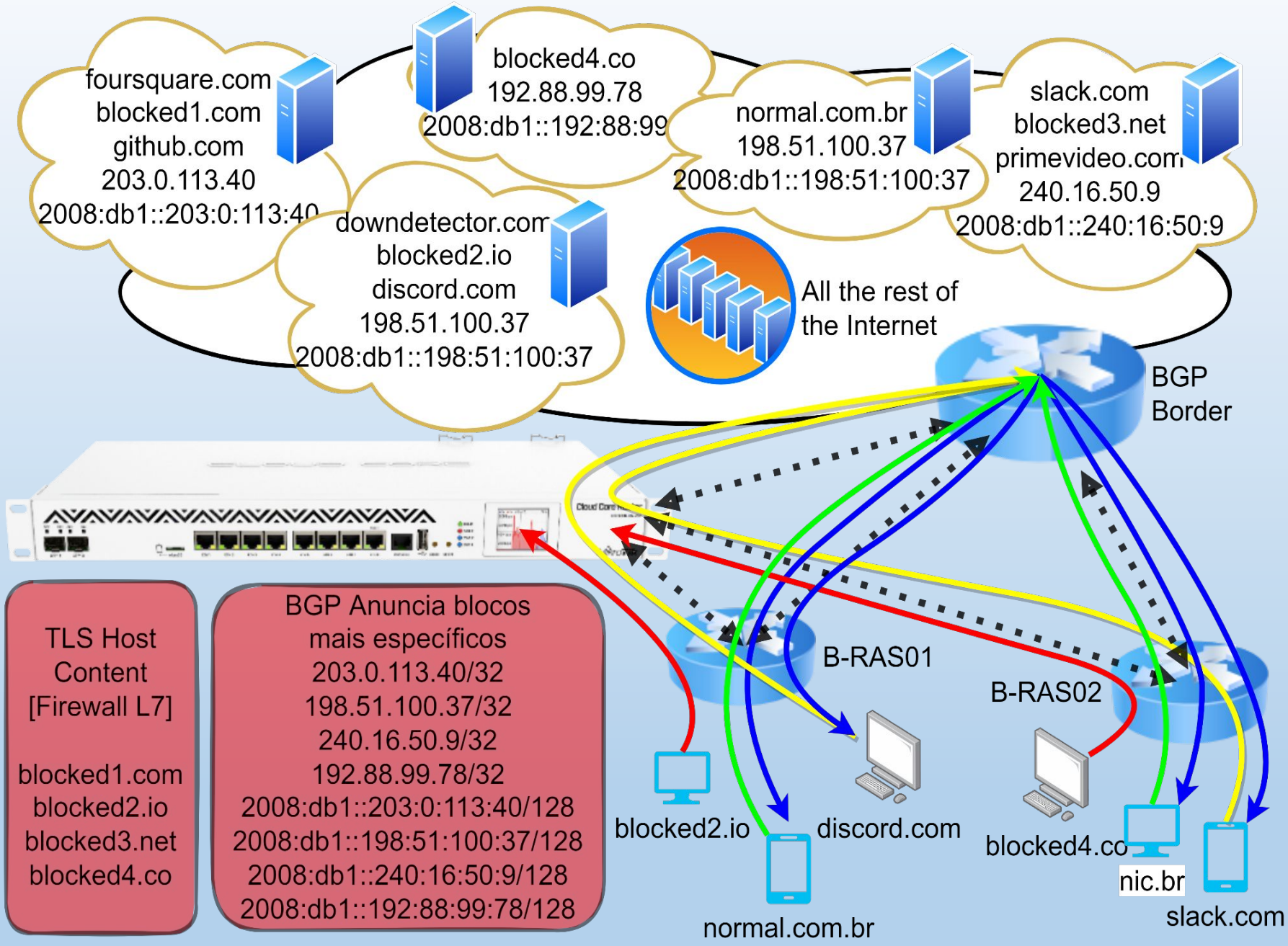
Wireshark · Packet 365 · Wi-Fi

```
Frame 365: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Devic
Ethernet II, Src: IntelCor_0e:aa:10 (18:26:49:0e:aa:10), Dst: Routerbo_e6:a3:4d (4c:5e:0c:e6
Internet Protocol Version 4, Src: 10.125.128.157, Dst: 200.160.4.153
Transmission Control Protocol, Src Port: 3436, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Client Hel
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
        Version: TLS 1.2 (0x0303)
        Random: 7aafcd007040364c8a4af3e8379ff418d970                    d55a0814fb57654
        Session ID Length: 32
        Session ID: e6dd8239969b4c542b589697a58f8ba                    e9b1113371b6d4f648
        Cipher Suites Length: 32
      > Cipher Suites (16 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 403
      > Extension: Reserved (GREASE) (len=0)
      v Extension: server_name (len=19)
            Type: server_name (0)
            Length: 19
        v Server Name Indication extension
              Server Name list length: 17
              Server Name Type: host_name (0)
              Server Name length: 14
              Server Name: gtergts.nic.br
      > Extension: extended_master_secret (le
      > Extension: renegotiation_info (len=1)
```

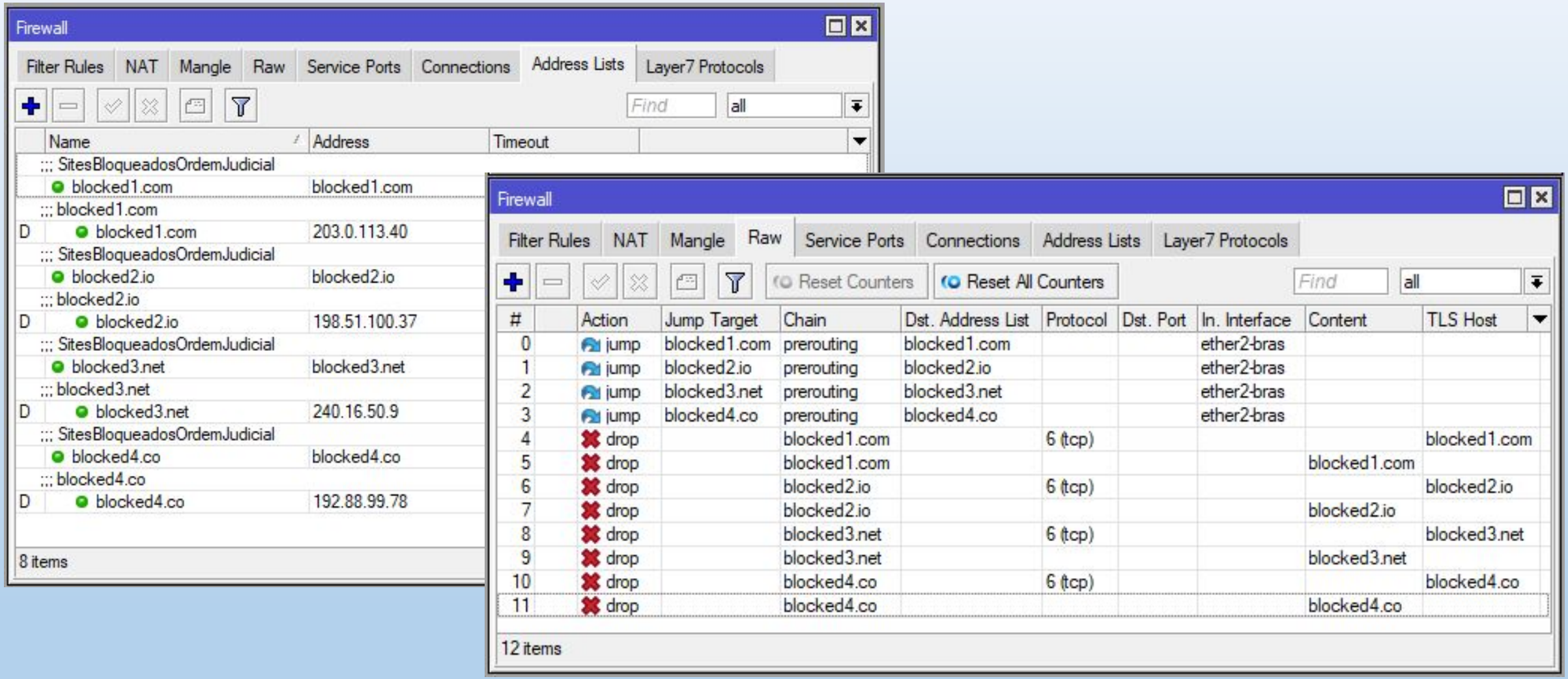
Show packet bytes

Endereço destinatário:
IPv4 ou IPv6 de destino

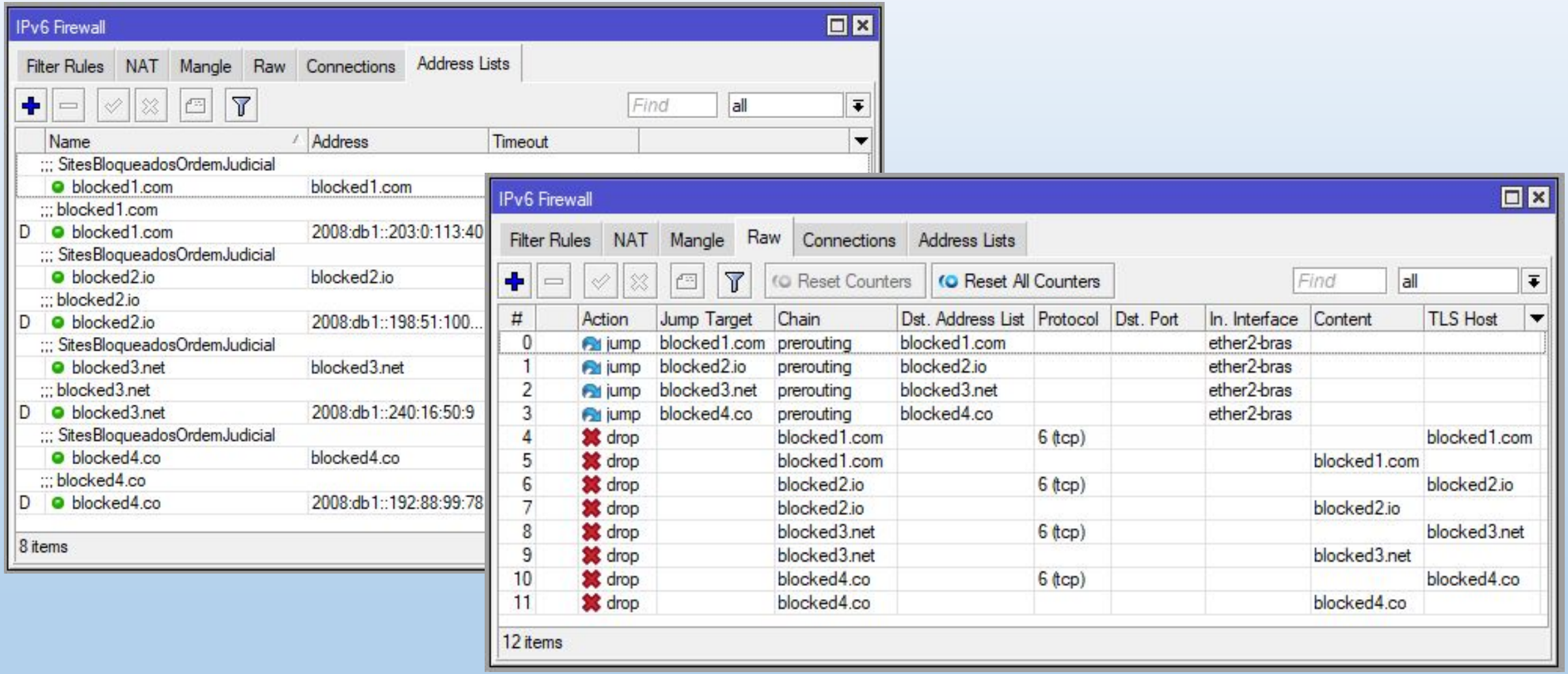
Aos Cuidados De:
Domínio que foi acessado


foursquare.com
blocked1.com
github.com
203.0.113.40
2008:db1::203:0:113:40
blocked4.co
192.88.99.78
2008:db1::192:88:99
normal.com.br
198.51.100.37
2008:db1::198:51:100:37
slack.com
blocked3.net
primevideo.com
240.16.50.9
2008:db1::240:16:50:9
downdetector.com
blocked2.io
discord.com
198.51.100.37
2008:db1::198:51:100:37
All the rest of the Internet
BGP Border
B-RAS01
B-RAS02
TLS Host Content [Firewall L7]
blocked1.com
blocked2.io
blocked3.net
blocked4.co
BGP Anuncia blocos mais específicos
203.0.113.40/32
198.51.100.37/32
240.16.50.9/32
192.88.99.78/32
2008:db1::203:0:113:40/128
2008:db1::198:51:100:37/128
2008:db1::240:16:50:9/128
2008:db1::192:88:99:78/128
blocked2.io
discord.com
blocked4.co
nic.br
normal.com.br
slack.com

Bloqueado a subida nos pacotes IPv4

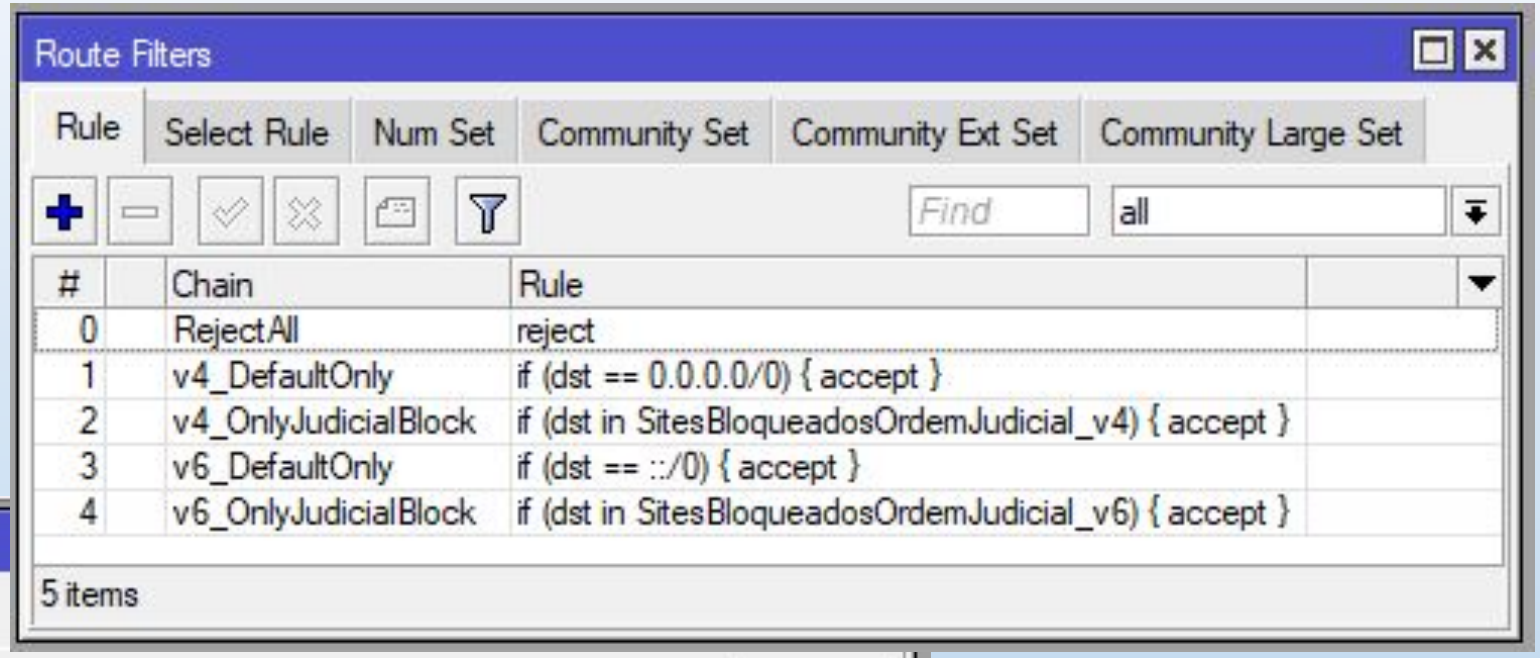


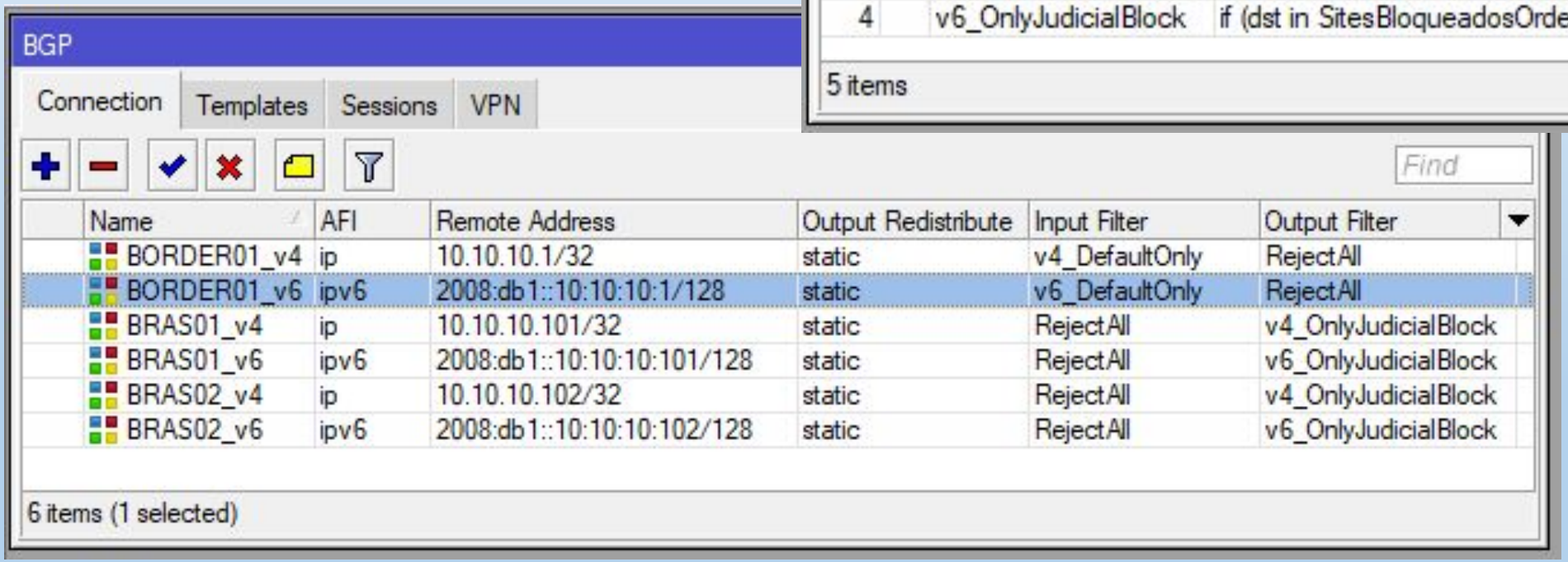
Bloqueado a subida nos pacotes IPv6



Atraindo o tráfego específico dos B-RAS

Como? Com BGP uai!





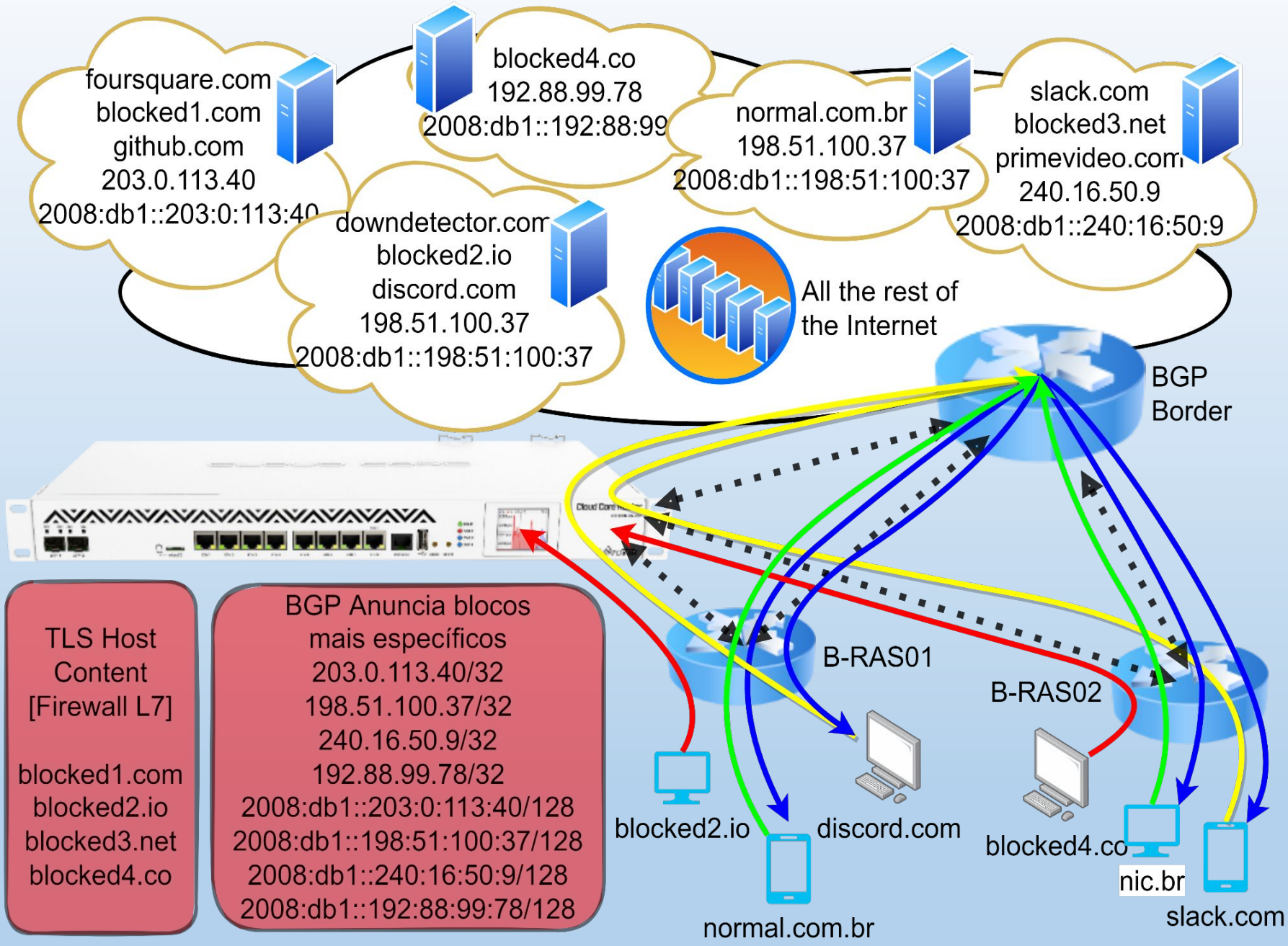
Atraindo o tráfego específico dos B-RAS

As rotas precisam estar na FIB.

```
[admin@chr-bloqueio-sites] > /ip/route/export compact
# oct/24/2022 09:11:36 by RouterOS 7.6
# software id =
#
/ip route
add comment=blocked1.com dst-address=203.0.113.40/32 gateway=10.10.10.1
add comment=blocked1.com dst-address=203.0.113.40/32 gateway=10.10.10.1
add comment=blocked2.io dst-address=198.51.100.37/32 gateway=10.10.10.1
add comment=blocked3.net dst-address=240.16.50.9/32 gateway=10.10.10.1
add comment=blocked4.co dst-address=192.88.99.78/32 gateway=10.10.10.1
[admin@chr-bloqueio-sites] >
[admin@chr-bloqueio-sites] >
[admin@chr-bloqueio-sites] > /ipv6/route/export compact
# oct/24/2022 09:11:44 by RouterOS 7.6
# software id =
#
/ipv6 route
add comment=blocked1.com dst-address=2008:db1::203:0:113:40 gateway=2008:db1::10:10:10:1
add comment=blocked2.io dst-address=2008:db1::198:51:100:37 gateway=2008:db1::10:10:10:1
add comment=blocked3.net dst-address=2008:db1::240:16:50:9 gateway=2008:db1::10:10:10:1
add comment=blocked4.co dst-address=2008:db1::192:88:99:78 gateway=2008:db1::10:10:10:1
```

POSSÍVEIS efeitos colaterais

- Servidores DNS recursivos padecendo
  - Erros de configuração
  - Aumento da demanda computacional
- Falha na tarefa de bloquear
  - FQDNs com muitos IPs, TTLs baixos, e em constante alternância.
  - DoT no Browser -> By-Pass quase involuntário
- Não funcionamento de sites não bloqueados
  - HTTP 1.1 -> um IP e muitos domínios
- Quebra de Certificados SSL/TLS
  - Man-in-the-Middle -> Decrypt-Recrypt
- **BGP/FIB**
  - **Muitas rotas na FIB de equipamentos com capacidade limitada**


foursquare.com
blocked1.com
github.com
203.0.113.40
2008:db1::203:0:113:40
blocked4.co
192.88.99.78
2008:db1::192:88:99
normal.com.br
198.51.100.37
2008:db1::198:51:100:37
slack.com
blocked3.net
primevideo.com
240.16.50.9
2008:db1::240:16:50:9
downdetector.com
blocked2.io
discord.com
198.51.100.37
2008:db1::198:51:100:37
All the rest of the Internet
BGP Border
B-RAS01
B-RAS02
TLS Host Content [Firewall L7]
blocked1.com
blocked2.io
blocked3.net
blocked4.co
BGP Anuncia blocos mais específicos
203.0.113.40/32
198.51.100.37/32
240.16.50.9/32
192.88.99.78/32
2008:db1::203:0:113:40/128
2008:db1::198:51:100:37/128
2008:db1::240:16:50:9/128
2008:db1::192:88:99:78/128
blocked2.io
discord.com
blocked4.co
nic.br
normal.com.br
slack.com

Automação é o caminho!

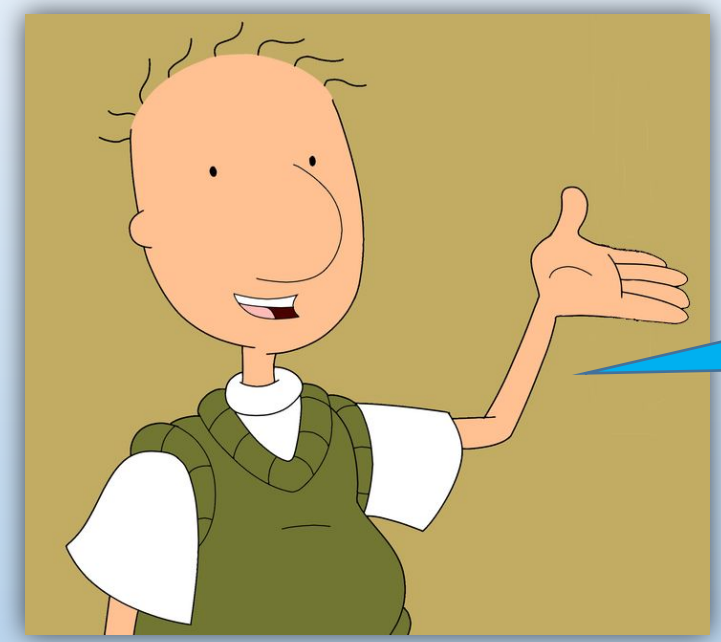
- SSH cru -
- Ansible - 😍
- Scripts dentro do próprio RouterOS - 😮
  - To be done
  - https://github.com/fischerdouglas/routeros-scripts/blob/main/Script_RouterOS_SetIPServicesAddressByAddressList.rsc

Pontos Fortes

- Vendor Lock-In = Off;
  - Apesar da Mikrotiquice, pode ser implementado com OpenSource (Ex.: FRR + NFtables)
- Não atua no Download, e no Upload “olha” para os pacotes de alguns destinos específicos
  - Evita a adição de latência e traz ganho de performance
- Bastante performático
  - Não faz abertura de payload - Somente Headers
    - Decrypt-Recrypt não é para ISP - Usado em Corporativo
  - Não necessita de Firewall Statefull / Contrack
  - Pode ser aplicado na Filter RAW(Mikrotik RouterOS)
- Permite Alta Disponibilidade e Balanceamento de Carga

Questões que precisam ser aprofundadas

- RouterOS - Layer7 Protocol no Firewall IPv6
- QUIC
  - Uber - TLS veio HTTP/TCP -> QUIC
- ESNI - SNI criptografado
- ECH - Encrypted Client Hello
- ?



Perguntas?
Sugestões?

“Você tem que ser o que você realmente é.

Pois se você não for quem você é, afinal quem é você?”
Doug Funnie