DNS Seguro: DoT e DoH

Protegendo consultas DNS contra interceptação e manipulação

O problema do DNS tradicional

Como funciona o DNS clássico

Tradicionalmente, consultas DNS utilizam:

- 53/UDP
- 53/TCP

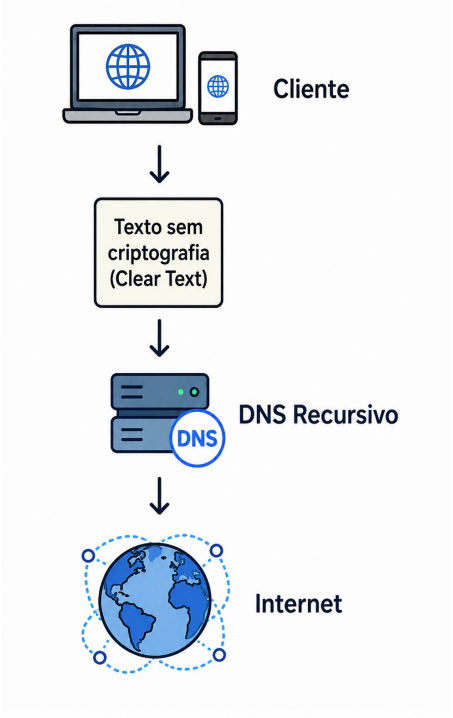
Essas consultas são enviadas em **texto claro**.
Isso significa que:

- Qualquer equipamento intermediário pode visualizar os domínios consultados.
- Um atacante na mesma rede pode interceptar respostas.
- Um provedor de acesso pode registrar todo o histórico de consultas DNS do usuário.
- Redes públicas podem sofrer de ataques de **DNS Cache Poisoning**.

A consulta DNS pode ser observada por terceiros mesmo que o site utilize **HTTPS**.

Importante: HTTPS protege o conteúdo do site, mas não necessariamente protege a **resolução DNS**.

Importante 2: Estar em HTTPS com certificado válido, não quer dizer que o site seja **confiável**.



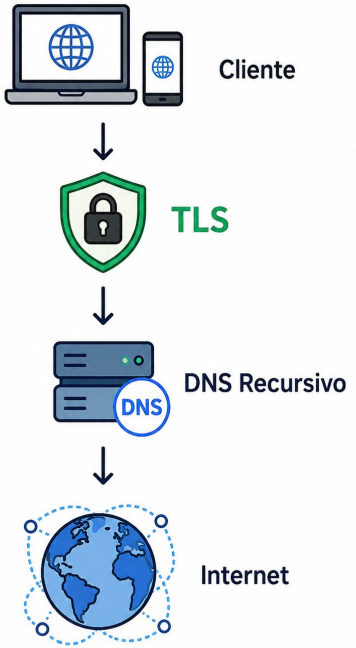
O que é DNS over TLS (DoT)

DNS over TLS

Padronizado pela **Internet Engineering Task Force** na **RFC 7858**.
O DoT encapsula consultas DNS dentro de uma sessão TLS.

Características:

- Porta padrão: **853/TCP**
- Criptografia ponta a ponta entre cliente e resolvedor
- Impede espionagem das consultas DNS
- Impede alterações durante o transporte
- **TLS 1.2+**



O que é DNS over HTTPS (DoH)

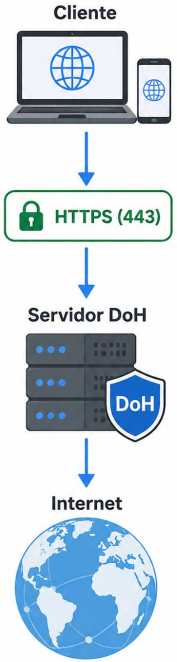
DNS over HTTPS

Padronizado pela Internet Engineering Task Force na **RFC 8484**.

Transporta consultas DNS dentro de conexões HTTPS.

Características

- **Porta 443/TCP**
- Utiliza **HTTP/2**
- Compartilha a mesma infraestrutura do tráfego web
- Difícil de distinguir do restante do tráfego HTTPS
- **TLS 1.2+**



Característica	DoT	DoH
Porta padrão	853	443
Usa TLS	Sim	Sim
Usa HTTP	Não	Sim
Fácil identificar na rede	Sim	Não
Fácil filtrar	Sim	Mais difícil
Overhead	Menor	Maior
Integração com navegadores	Limitada	Muito comum

Resumo

- **DoT** foi criado especificamente para DNS.
- **DoH** utiliza a infraestrutura já existente da Web.

O que eles protegem?

Benefícios quanto à Privacidade

Protegem contra:

- Espionagem de consultas DNS.
- Captura de tráfego em Wi-Fi público.
- DNS Spoofing em redes locais.
- Alteração de respostas DNS durante o transporte.

Não protegem contra:

- Malware instalado no equipamento.
- Comprometimento do resolvedor DNS.
- Monitoramento baseado em SNI (Server Name Indication), IP ou tráfego HTTPS.
- Sites inseguros.

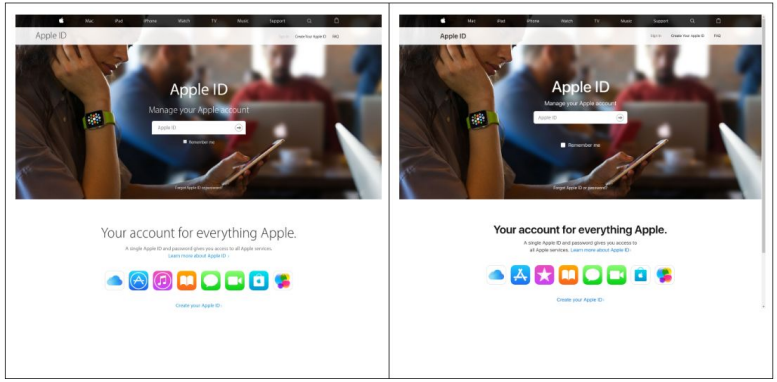
Locais perigosos

Cenário com Wi-Fi Público

Usuário conectado em:

- Aeroportos
- Hoteis
- Cafés

Um atacante responde consultas DNS antes do servidor legítimo (**DNS Cache Poisoning**).
Resultado é um direcionamento para um IP falso com um site muito parecido com o verdadeiro. Com **DoT** ou **DoH** isso não acontece.



Site de phishing **Site legítimo**

Qual escolher?

Quando usar DoT:

Indicado para:

- Sistemas operacionais
- Smartphones
- Roteadores
- Equipamentos de rede

Vantagens:

- Simples
- Menor overhead
- Fácil gerenciamento

Desvantagens:

- **Probing TLS Oportunista** massivo em DNS(s) Recursivos. Diversos dispositivos com Android fazem uso desse recurso na porta **853/TCP**.
- Consumo mais alto de recursos levando em consideração a base total de clientes do ISP e de dispositivos oportunistas.

Quando usar DoH:

Indicado para:

- Navegadores
- Aplicações específicas
- Ambientes onde a porta 853 é bloqueada

Vantagens:

- Funciona pela porta 443/TCP
- Grande compatibilidade com navegadores modernos
- Menos sujeito a bloqueios.
- Não possui **Probing Oportunista**

Desvantagem:

- Dificuldade para uso sem ser em navegadores.

Resolvedores públicos que suportam DoT/DoH

CloudFlare

DoT:
- **tls://cloudflare-dns.com**

DoH:
- **https://cloudflare-dns.com/dns-query**

Quad9:

DoT:
- **tls://dns.quad9.net**

DoH:
- **https://dns.quad9.net/dns-query**

Google

DoT:
- **tls://dns.google**

DoH:
- **https://dns.google/dns-query**

Exemplos DoH: https://developers.cloudflare.com/1.1.1.1/encryption/dns-over-https/encrypted-dns-browsers/

Bloqueio de malware e conteúdo adulto

CloudFlare bloqueio de malware

DoT:

- **tls://security.cloudflare-dns.com** (1.1.1.2, 1.0.0.2, 2606:4700:4700::1002 e 2606:4700:4700::1112)

DoH:

- **https://security.cloudflare-dns.com/dns-query**

CloudFlare bloqueio de malware e conteúdo adulto

DoT:

- **tls://family.cloudflare-dns.com** (1.1.1.3, 1.0.0.3, 2606:4700:4700::1003, 2606:4700:4700::1113)

DoH:

- **https://family.cloudflare-dns.com/dns-query**

Referência: https://developers.cloudflare.com/1.1.1.1/setup/

Seu DNS Recursivo também pode fazer isso

Unbound com RPZ

- Existem listas já prontas ou você pode construir a sua e hospedar. Um exemplo de configuração do Unbound:
- Esse site contém listas atualizadas de hora em hora: **https://oisd.nl/**

```
# Bloqueio de malware, phishing, ransomware, ...
server:
   rpz:
      name: "malware"
      zonefile: "/var/lib/unbound/malware-rpz.zone"

auth-zone:
   name: "malware"
   url: "https://big.oisd.nl/rpz"
   for-downstream: no
   for-upstream: yes
   fallback-enabled: no
   zonefile: "/var/lib/unbound/malware-rpz.zone"
```

```
# Bloqueio de conteúdo adulto
server:
    rpz:
        name: "porn"
        zonefile: "/var/lib/unbound/porn-rpz.zone"

auth-zone:
    name: "porn"
    url: "https://nsfw.oisd.nl/rpz"
    for-downstream: no
    for-upstream: yes
    fallback-enabled: no
    zonefile: "/var/lib/unbound/porn-rpz.zone"
```

Problema do DoT com Unbound no Debian Trixie

Foram observados travamentos de CPU em **100%**, quando utilizando DoT no Unbound do Debian Trixie. Tudo indica que é uma condição de loop durante o uso da **libevent**. Um **Bug Report** já foi aberto sobre isso.

Enquanto não temos uma solução por parte do Debian, podemos utilizar o **DNSDIST** como um proxy para DoH e DoT.
Exemplo de **/etc/dnsdist/dnsdist.conf**:

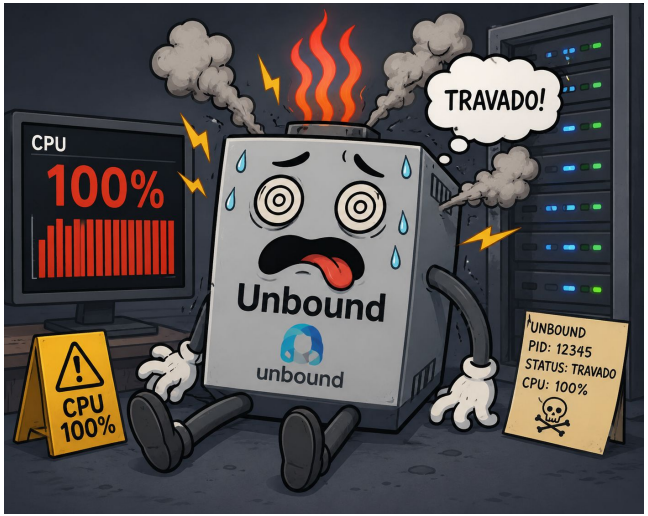
```
setSecurityPollSuffix("")

setLocal("127.0.0.1:5353")

addACL('100.64.0.0/10')
addACL('192.168.0.0/16')
addACL('172.16.0.0/12')
addACL('10.0.0.0/8')
addACL('2001:db8::/32')

newServer("127.0.0.1:53")
newServer("[::1]:53")

local certFile = "/etc/unbound/fullchain.pem"
local keyFile  = "/etc/unbound/privkey.pem"
```



```
local tlsOpts = {
   reusePort = true,
   tcpFastOpenSize = 0,
}
local dohOpts = {
   doTCP = true,
   reusePort = true,
   tcpFastOpenSize = 0,
}

– DoT
addTLSLocal("10.10.10.10:853", certFile, keyFile, tlsOpts)
addTLSLocal("10.10.9.9:853",   certFile, keyFile, tlsOpts)
addTLSLocal("[fd00::10:10:10:10]:853", certFile, keyFile, tlsOpts)
addTLSLocal("[fd00::10:10:9:9]:853",   certFile, keyFile, tlsOpts)

– DoH
addDOHLocal("10.10.10.10:443", certFile, keyFile, {"/dns-query"}, dohOpts)
addDOHLocal("10.10.9.9:443",   certFile, keyFile, {"/dns-query"}, dohOpts)
addDOHLocal("[fd00::10:10:10:10]:443", certFile, keyFile, {"/dns-query"}, dohOpts)
addDOHLocal("[fd00::10:10:9:9]:443",   certFile, keyFile, {"/dns-query"}, dohOpts)

controlSocket('127.0.0.1:5199')
webserver("127.0.0.1:8083")
setWebserverConfig({password=hashPassword("SENHA_FORTE"), apiKey=hashPassword("SENHA_FORTE")})
```

Outra alternativa interessante

Outra alternativa seria instalar a última versão disponível no repositório oficial do Debian. Para isso disponibilizei no Github o projeto abaixo que faz isso automaticamente para você. Baixa, compila, gera os arquivos **.deb** e instala se quiser:

```
# apt policy unbound
unbound:
  Instalado: 1.25.1-1
  Candidato: 1.25.1-1
  Tabela de versão:
 *** 1.25.1-1 100
        100 /var/lib/dpkg/status
     1.22.0-2+deb13u3 500
        500 http://security.debian.org/debian-security trixie-security/main amd64 Packages
     1.22.0-2+deb13u2 500
        500 http://deb.debian.org/debian trixie/main amd64 Packages
```

Projeto Github:
https://github.com/gondimcodes/unbound-pkg

Um DNS Recursivo local com DoH e DoT bem configurado, é sempre melhor que opções públicas

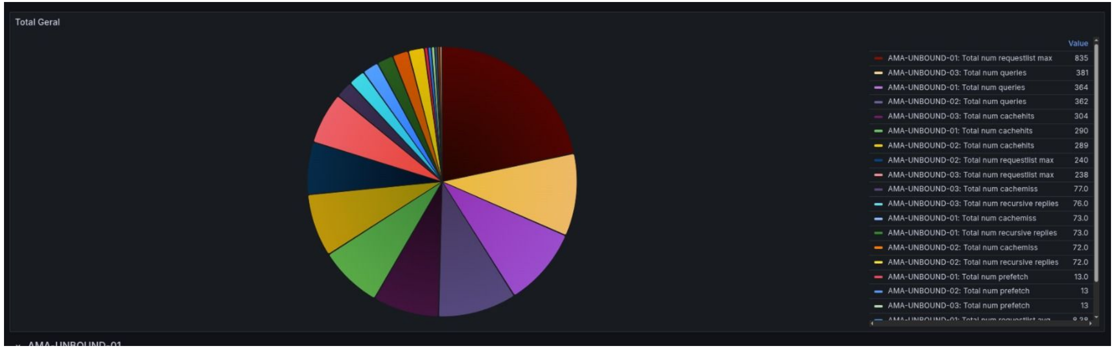
Projeto que disponibilizei para a comunidade, que instala em um Debian 13 os containers: **Unbound latest** direto da NLnet Labs, **Chrony** para um NTP/NTS moderno, **Zabbix Agent2 7.0.x** e **FRR** se for configurar DNS(s) Recursivos Anycast:

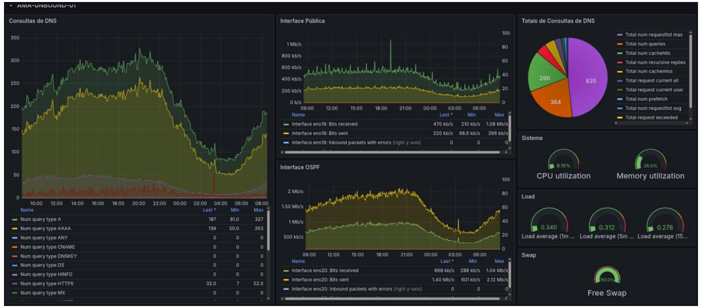
Artigo sobre o projeto:

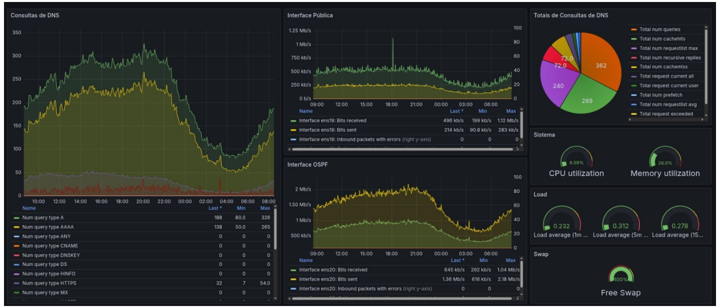
https://wiki.ispup.com.br/w/Unbound-kindns

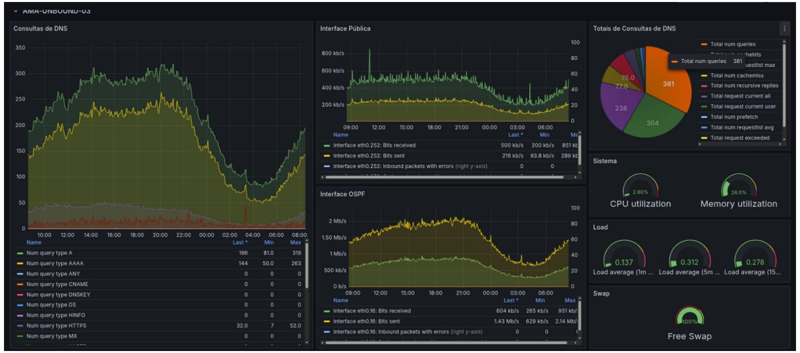
Projeto:

https://github.com/gondimcodes/unbound-kindns









https://ispfocus.net.br

Exemplos de configuração do cliente

Debian

 # apt install systemd-resolved
 # mkdir -p /etc/systemd/resolved.conf.d/

Em **/etc/systemd/resolved.conf.d/resolved.conf** crie esse exemplo configuração para CloudFlare:

```
# Some examples of DNS servers which may be used for DNS= and FallbackDNS=:
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-dns.com 2606:4700:4700::1111#cloudflare-dns.com
2606:4700:4700::1001#cloudflare-dns.com
# Google:     8.8.8.8#dns.google 8.8.4.4#dns.google 2001:4860:4860::8888#dns.google 2001:4860:4860::8844#dns.google
# Quad9:      9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9.net 2620:fe::fe#dns.quad9.net 2620:fe::9#dns.quad9.net

[Resolve]
DNS=1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-dns.com 2606:4700:4700::1111#cloudflare-dns.com
2606:4700:4700::1001#cloudflare-dns.com
DNSOverTLS=yes
```

 # systemctl restart systemd-resolved

Conclusão

- DNS tradicional expõe consultas em texto claro.
- DoT e DoH criptografam a comunicação DNS com o usuário.
- Ambos aumentam privacidade e segurança.
- DoT é mais simples e focado em DNS (853/TCP).
- DoH aproveita a infraestrutura HTTPS existente (443/TCP).
- A escolha depende do ambiente e dos requisitos operacionais.

"HTTPS protege o conteúdo que você acessa. DoT e DoH protegem a pergunta que você faz antes de acessá-lo."

ISPFocus
NETWORK SOLUTIONS

1 DNS Seguro: DoT e DoH

Protegendo consultas DNS contra interceptação e manipulação

2 O problema do DNS tradicional

Como funciona o DNS clássico

Consultas DNS utilizam UDP/53 ou TCP/53 em texto claro.

- Qualquer equipamento intermediário pode visualizar os domínios consultados.
- Um atacante na mesma rede pode interceptar respostas.
- Um provedor de acesso pode registrar todo o histórico de consultas DNS.
- Redes públicas podem realizar ataques de DNS Spoofing.

Exemplo:
Ao acessar www.banco.com.br, a consulta DNS pode ser observada por terceiros mesmo que o site utilize HTTPS.

⚠ HTTPS protege o conteúdo do site, mas não necessariamente protege a resolução DNS.

3 O que é DNS over TLS (DoT)

Padronizado pela IETF na RFC 7858.

O DoT encapsula consultas DNS dentro de uma sessão TLS.

- Porta padrão: 853/TCP
- Criptografia ponta a ponta entre cliente e resolvedor
- Impede espionagem das consultas DNS
- Impede alterações durante o transporte

4 O que é DNS over HTTPS (DoH)

Padronizado pela IETF na RFC 8484.

Transporta consultas DNS dentro de conexões HTTPS.

- Porta padrão: 443/TCP
- Utiliza HTTP/2
- Compartilha a mesma infraestrutura do tráfego web
- Difícil de distinguir do restante do tráfego HTTPS

5 Comparação direta

Característica	DoT	DoH
Porta padrão	853	443
Usa TLS	Sim	Sim
Usa HTTP	Não	Sim
Fácil identificar na rede	Sim	Não
Fácil filtrar	Sim	Mais difícil
Overhead	Menor	Maior
Integração com navegadores	Limitada	Muito comum

Resumo:
DoT foi criado especificamente para DNS.
DoH utiliza a infreestrutura já existente da Web.

6 O que eles protegem?

Protegem contra:

- ✓ Espionagem de consultas DNS
- ✓ Captura de tráfego em Wi-Fi público
- ✓ DNS Spoofing em redes locais
- ✓ Alteração de respostas DNS durante o transporte

Não protegem contra:

- ✗ Malware instalado no equipamento
- ✗ Comprometimento do resolvedor DNS
- ✗ Monitoramento baseado em SNI, IP ou tráfego HTTPS
- ✗ Sites inseguros

Protegem o transporte da consulta DNS (confidencialidade e integridade).

7 Casos reais que poderiam ser evitados

Cenário 1 – Wi-Fi Público
Em redes como aeroportos, hotéis ou cafés, um atacante pode responder consultas DNS antes do servidor legítimo, redirecionando o usuário para sites falsos (ex.: www.banco.com.br para um IP malicioso).
→ **Com DoT ou DoH:** o atacante não consegue forjar respostas válidas.

Cenário 2 – Captura de Navegação
Um terceiro observa os domínios que você consulta (banco.com.br, hospital.com.br, advogado.com.br), mesmo sem ver o conteúdo HTTPS, conseguindo inferir suas atividades.
→ **Com DoT ou DoH:** as consultas DNS ficam criptografadas.

Cenário 3 – Manipulação de DNS
Redes comprometidas ou mal configuradas podem redirecionar consultas, injetar publicidade ou bloquear domínios.
→ **Com DoT ou DoH:** a conexão criptografada com o resolvedor reduz esse risco.

8 Qual escolher?

Quando usar DoT

Indicado para:
- Sistemas operacionais
- Smartphones
- Roteadores
- Equipamentos de rede

Vantagens:
- Simples
- Menor overhead
- Fácil gerenciamento

X

Quando usar DoH

Indicado para:
- Navegadores
- Aplicações específicas
- Ambientes onde a porta 853 é bloqueada

Vantagens:
- Funciona pela porta 443
- Grande compatibilidade
- com navegadores modernos

DoH não é automaticamente "mais seguro" que DoT.
Ambos utilizam TLS e fornecem confidencialidade e integridade semelhantes.

9 Resolvedores públicos com DoT e DoH

	IPv4	DoT	DoH
CLOUDFLARE	1.1.1.1 1.0.0.1	tls://1dot1dot1dot1 .cloudflare-dns.com	https://cloudflare-dns.com/ dns-query
Google Public DNS	8.8.8.8 8.8.4.4	tls://dns.google	https://dns.google/ dns-query
quad9	9.9.9.9 149.112.112.112	tls://dns.quad9.net	https://dns.quad9.net/ dns-query

Quad9 inclui recursos de bloqueio de domínios maliciosos e phishing.

10 Exemplos de configuração

Linux (systemd-resolved)

Arquivo: /etc/systemd/resolved.conf

```
[Resolve]
DNS=1.1.1.1#cloudflare-dns.com
DNSOverTLS=yes
```

Reiniciar:

```
systemctl restart
systemd-resolved
```

Android (9 ou superior)

Configurações > Rede e Internet > DNS Privado

Selecione um provedor:
- dns.google
- 1dot1dot1dot1.cloudflare-dns.com
- dns.quad9.net

Windows 11

Configurações > Rede e Internet >
Propriedades da rede > Atribuição de servidor DNS
Ativar: Atribuição manual
IPv4 DNS sobre HTTPS

```
oniconocone    dns.google (https://dns.google/dns-query)
```

Obs.: Nem todos os sistemas suportam DoH nativamente.

11 Limitações e observações

Nem tudo fica invisível

Mesmo com DoT ou DoH ainda é possível observar:

Além disso
DoT e DoH não substituem:

Eles resolvem um problema específico: proteger o transporte da consulta DNS.

12 Conclusão

- ✓ DNS tradicional expõe consultas em texto claro.
- ✓ DoT e DoH criptografam a comunicação DNS.
- ✓ Ambos aumentam privacidade e segurança.
- ✓ DoT é mais simples e focado em DNS.
- ✓ DoH aproveita a infraestrutura HTTPS existente.
- ✓ A escolha depende do ambiente e dos requisitos operacionais.

> "HTTPS protege o conteúdo que você acessa. DoT e DoH protegem a pergunta que você faz antes de acessá-lo."

Marcelo Gondim

Precisando de algo?

MANRS

KINDNS

TOP
TESTE OS PADRÕES