

A Importância do Monitoramento de Servidores de DNS Recursivo voltada a aspectos de Disponibilidade, Performance e Segurança

ENG. PEDRO FILHO



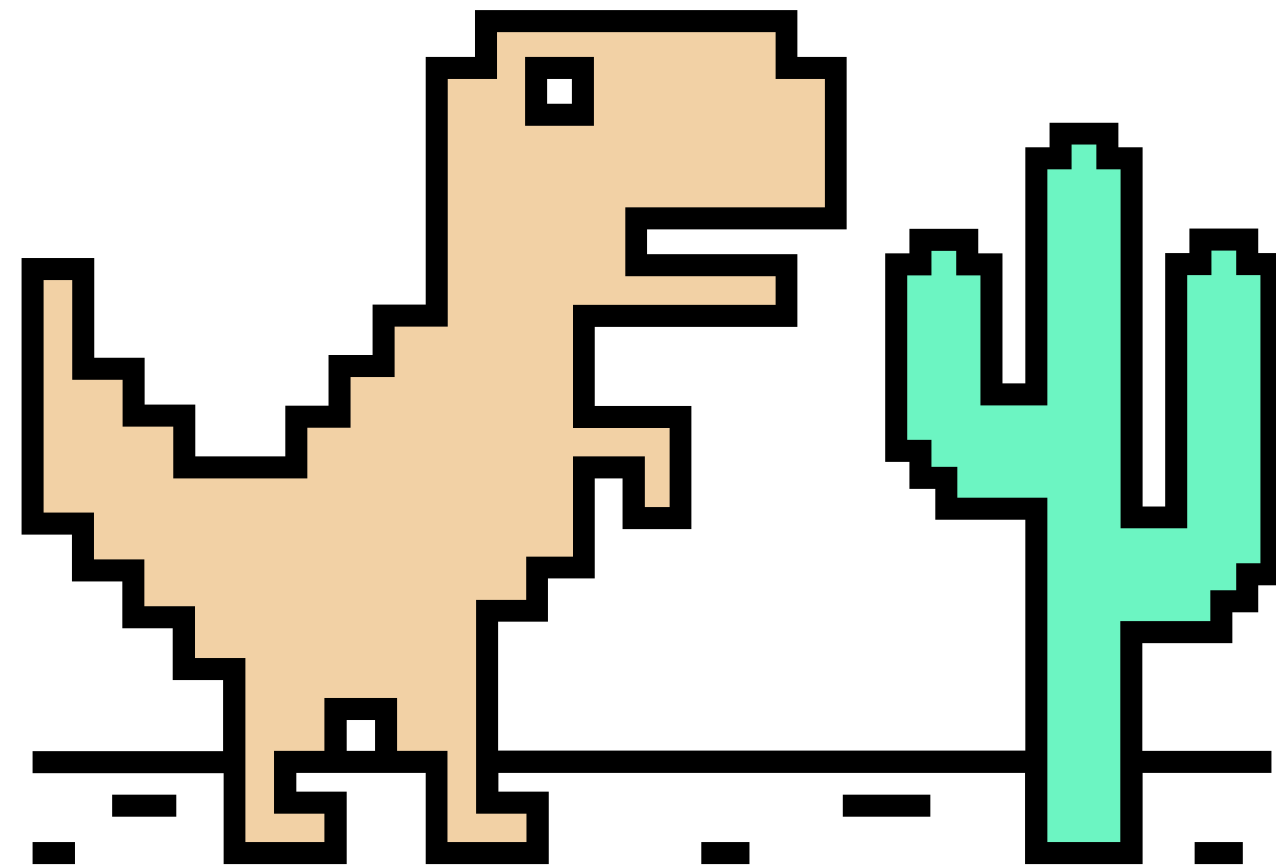
ASSINASOFT
TECNOLOGIA E CONSULTORIA

O serviço de DNS é invisível para o cliente, porém é **Essencial**

- Quando o usuário acessa um site na internet, tudo começa com uma consulta ao DNS recursivo



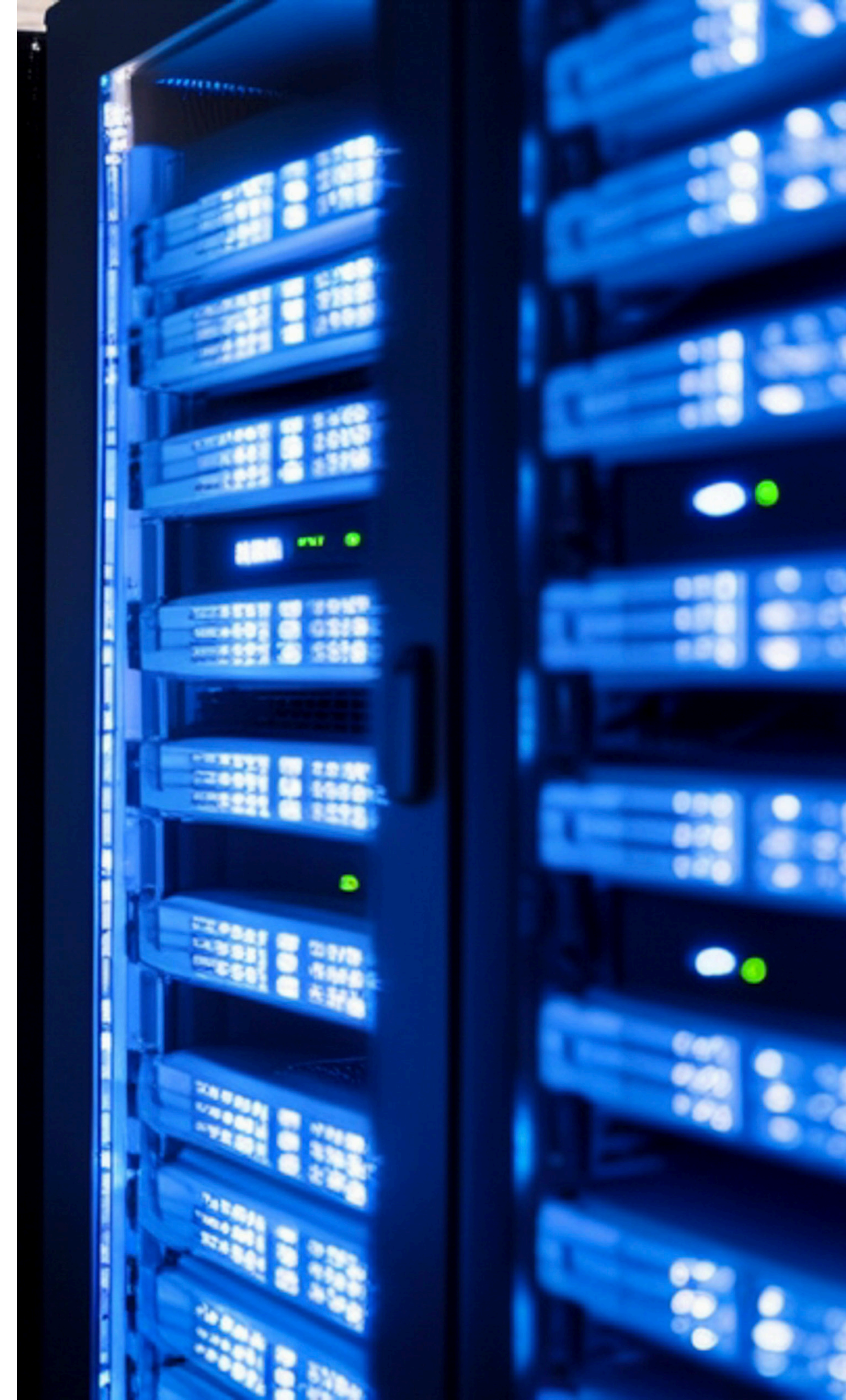
Se o DNS está lento ou indisponível, para o cliente
"A internet está lenta ou caiu!"



O que é **DNS Recursivo?**

O DNS recursivo é o servidor responsável por receber a solicitação do usuário e realizar toda a busca necessária para descobrir o endereço IP de um domínio.

- Sem ele, o acesso aos sites não funciona;
- Quanto mais perto do cliente, melhor;
- Ele faz cache sobre os conteúdos;



Os problemas de depender de **DNS públicos**

Pergunta???

- Você que nos assiste, tem algum contrato com os DNS Públicos?
- Eles te prometem SLA?
- Bloqueiam sites que a Anatel obriga?
- Garantem segurança sobre os serviços que prestam?
- Entregam relatórios e estatísticas sobre o serviço?



Os problemas de depender de DNS públicos

- **Perda da visibilidade da sua rede;**
- **Menor capacidade de diagnóstico;**
- **Maior latência;**
- **Dependência operacional;**
- **Questões de privacidade e LGPD**



Por que ter o servidor de DNS próprio?

- **Menor latência;**
- **Cache Local;**
- **Maior disponibilidade;**
- **Independência operacional;**
- **Possibilidade de filtragem DNS;**
- **DNSSEC Validation;**
- **Melhor experiência do cliente;**
- **Maior controle da rede.**



Principais servidores **Recursivos:**

Sistema Operacional Debian / Ubuntu Server / FreeBSD

- **Unbound;**
- **PowerDNS Recursor;**
- **Knot Resolver;**

- **Bind;**



Monitoramento: o DNS como um sensor da rede

- **Termômetro da rede (uplinks, latência, etc);**
- **Sensor de ataques DDoS;**
- **Detecta equipamentos comprometidos (TVbox, DVRs, Camera IP, IoT, etc)**



Como monitorar meu servidor?

Monitorar a VM pelo Zabbix ou similar

- CPU;
- Memória;
- Threads;
- Uptime;
- Disponibilidade UDP/TCP.

Qualquer desses itens, caso venha falhar ou sobrecarregar, já é um indicador que o serviço DNS na rede passa a ficar instável, logo, para o cliente, a internet passa a ter problemas.



Como monitorar meu servidor?

O Zabbix também pode ajudar com dados que fazem sentido voltados ao serviço de DNS

- **Tempo médio de resposta;**
- **QPS (Queries Per Second);**
- **Cache Hit Ratio.**
- **Cache Miss**
- **Timeout**

Esses parâmetros fazem toda a diferença na fluidez de seu serviço de DNS



Técnicas de Análise

unbound-control stats_noreset

```
total.num.queries=226266910
total.num.queries_ip_ratelimited=0
total.num.queries_cookie_valid=0
total.num.queries_cookie_client=0
total.num.queries_cookie_invalid=0
total.num.cachehits=185794883
total.num.cachemiss=40472027
total.num.prefetch=9890484
total.num.queries_timed_out=0
total.query.queue_time_us.max=0
total.num.expired=0
total.num.recursivereplies=39382042
```

Total de consultas

**Total de consultas
respondidas direto do cache
(otimização de desempenho)
ideal >80%**

**Total de consultas
que não utilizaram cache**

**Atualiza o cache do domínio
antes que ele expire**

**Indica problemas de conectividade
(perda de pacotes, problema de link)
ideal = 0**



Técnicas de Análise

unbound-control stats_noreset

```
total.requestlist.avg=2.35542  
total.requestlist.max=240  
total.requestlist.overwritten=0  
total.requestlist.exceeded=954471  
total.requestlist.current.all=11  
total.requestlist.current.user=11  
total.recursion.time.avg=0.099524  
total.recursion.time.median=0.032366  
total.tcpusage=0  
time.now=1782408080.331763  
time.up=3952983.501416  
time.elapsed=3952983.501416
```

Consultas simultâneas
aguardando resolução
(melhor mais próximo de 0)

Número máximo de consultas
simultâneas observado

O número de consultas recursivas
aguardando DNS externos

Tempo médio para resolver
consultas fora do cache

Uptime do Resolver



Técnicas de Análise

rndc status (bind)

```
[root@novons1:/var/cache/bind# rndc status
version: BIND 9.10.3-P4-Debian <id:ebd72b3> ([secured])
boot time: Sat, 04 Jul 2026 07:00:51 GMT
last configured: Sat, 04 Jul 2026 07:00:51 GMT
CPUs found: 4
worker threads: 4
UDP listeners per interface: 2
number of zones: 3071
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/0/1000
tcp clients: 0/100
server is up and running
```

Versão do Resolver

Boot Time do Server

Zonas carregadas

Numero de recursões

Status do Server



Parâmetros

Campo	Valor ideal
Cache Hit	>80%
Timeout	0
QPS	Variável *
Recursion Time	< 100ms
Request List (avg, max)	Monitorar



Parâmetros

Campo	Valor ideal
Query Queue	Monitorar
NXDOMAIN	Monitorar
SERVFAIL	Próximo de 0
DNSSEC Failures	0
Uptime	Monitorar



Técnicas de Análise

Conhecer o seu cenário de DNS na rede é o primeiro passo, após isso:

- **Firewall em seu DNS server (ip/ip6tables);**
- **Monitoramento de indicadores para tomada de decisão**
- **Regras de flowspec para proteger seu servidor (ratelimit, flags, packet-length, etc)**

Saber os parâmetros padrões de seus servidores é essencial para conseguir aplicar regras de proteção / mitigação.



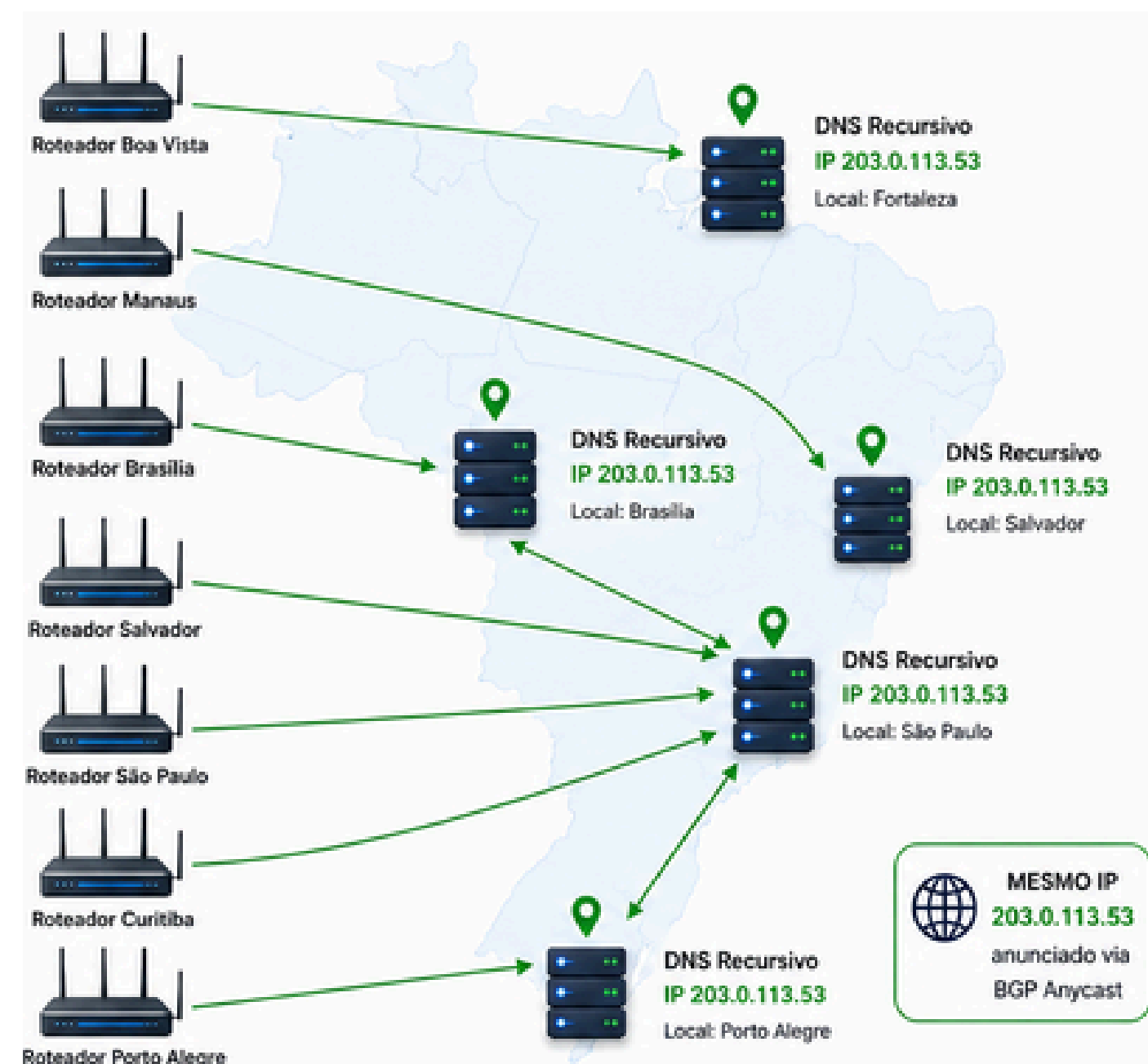
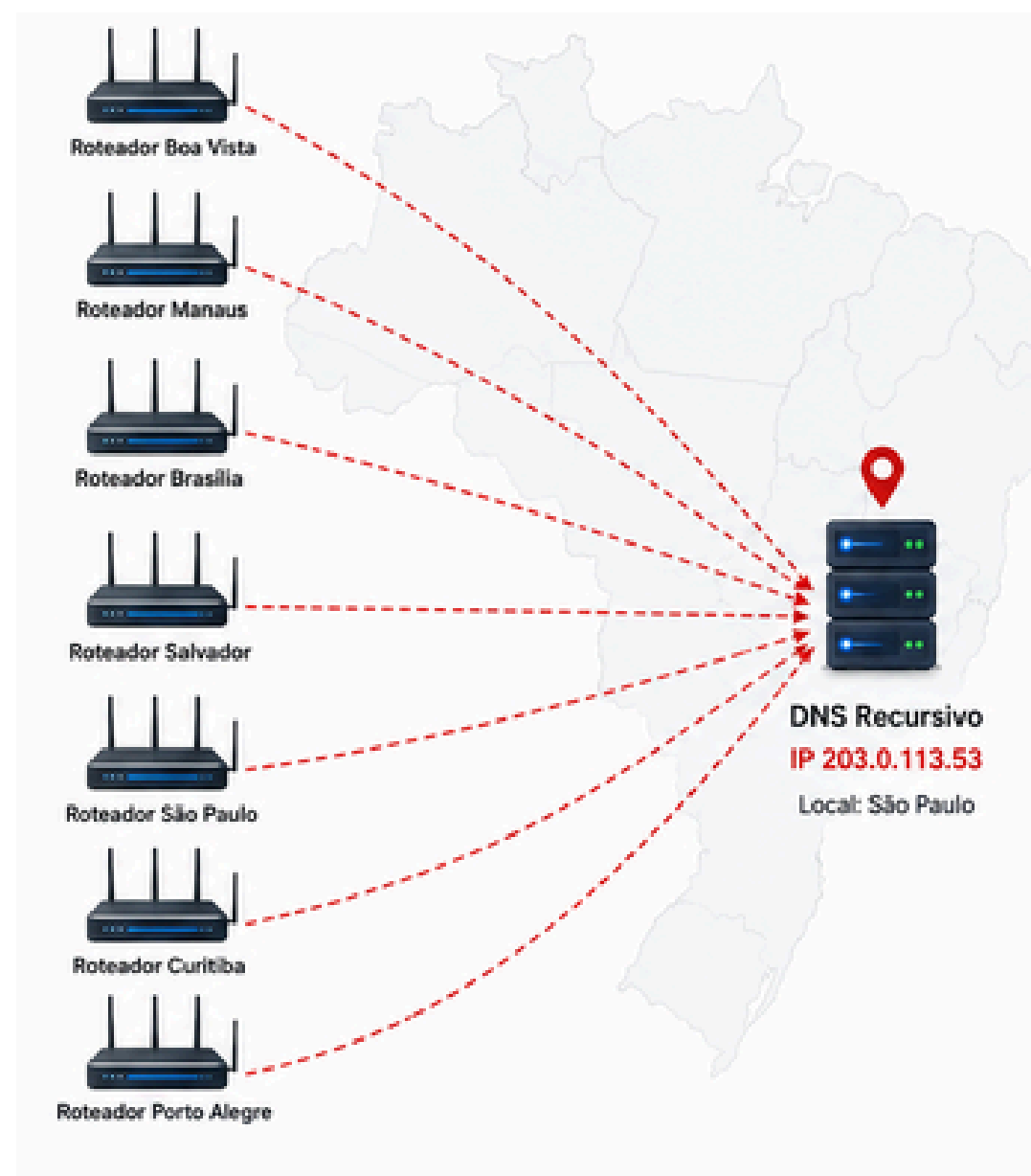
Técnicas de Análise

Cuidados ao trabalhar firewall

- **Definir allow-list; (nunca permitir recursão aberta)**
- **Separar redes para aplicar filtros;**
- **Criar regras de acordo com cada rede;**
 - **(CGNAT, Blocos Públicos, Servidores)**
- **Buscar estatísticas avançadas para definir estratégias;**
 - **rate-limit para clientes com excesso de consultas inválidas;**
 - **banir IPs com excesso de flags (synflood)**
 - **usar ferramentas de flow para diagnosticar problemas;**



Estabilidade e Confiança

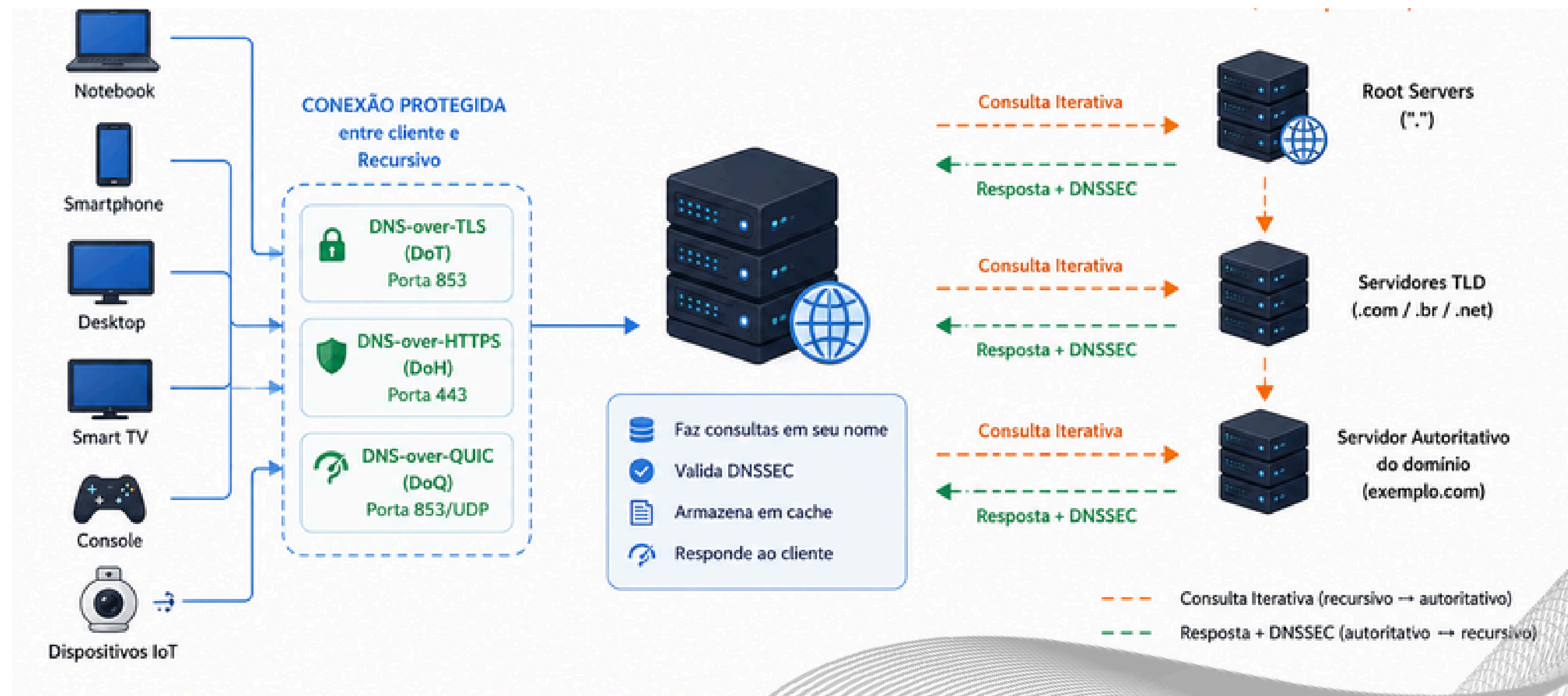


Permite a otimização do desempenho na rede, e descentraliza o processamento



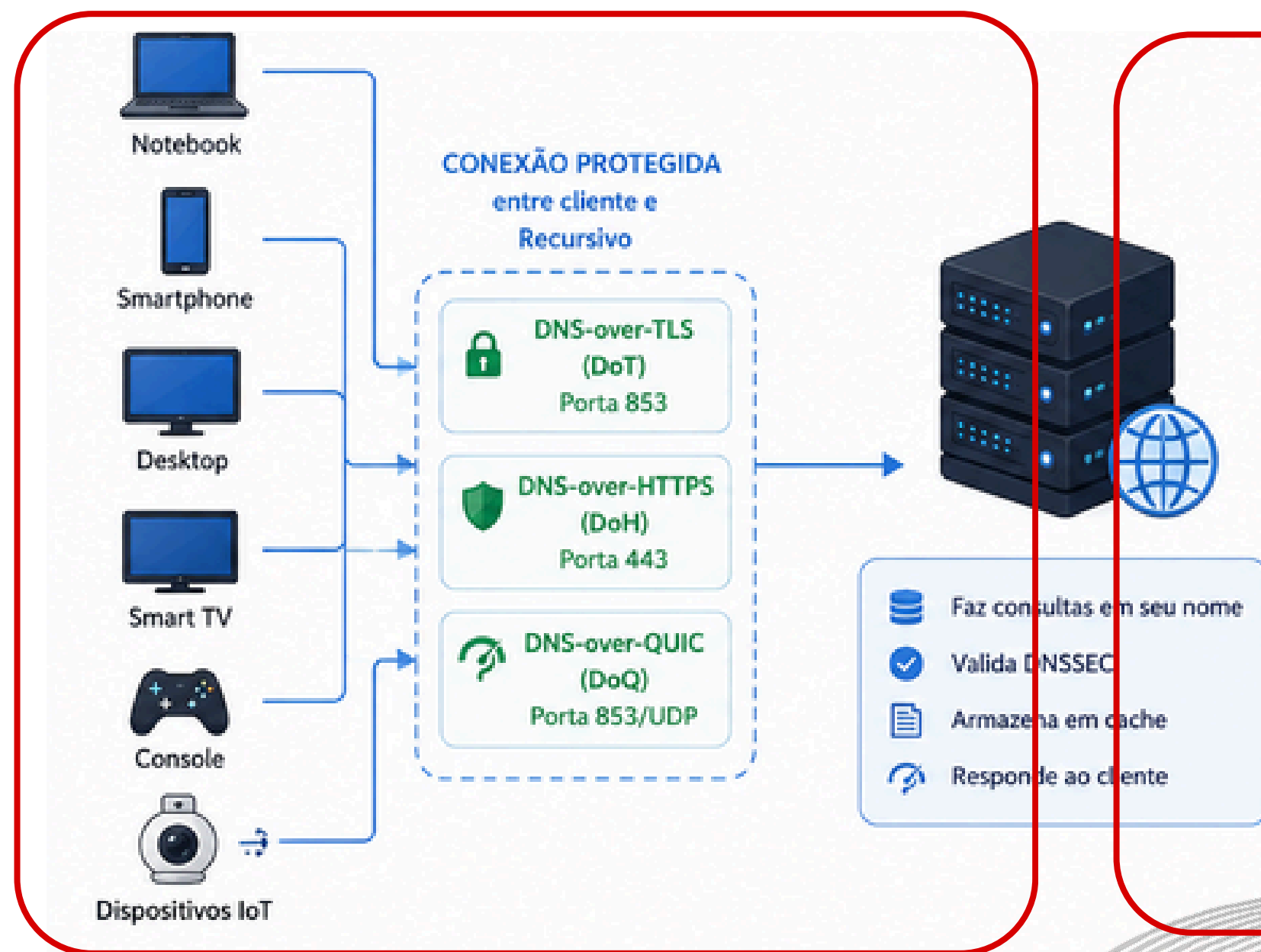
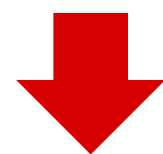
O DNSSEC em Recursivos

**Garante que a consulta entre
Recursivo / Autoritativo seja autêntica.**

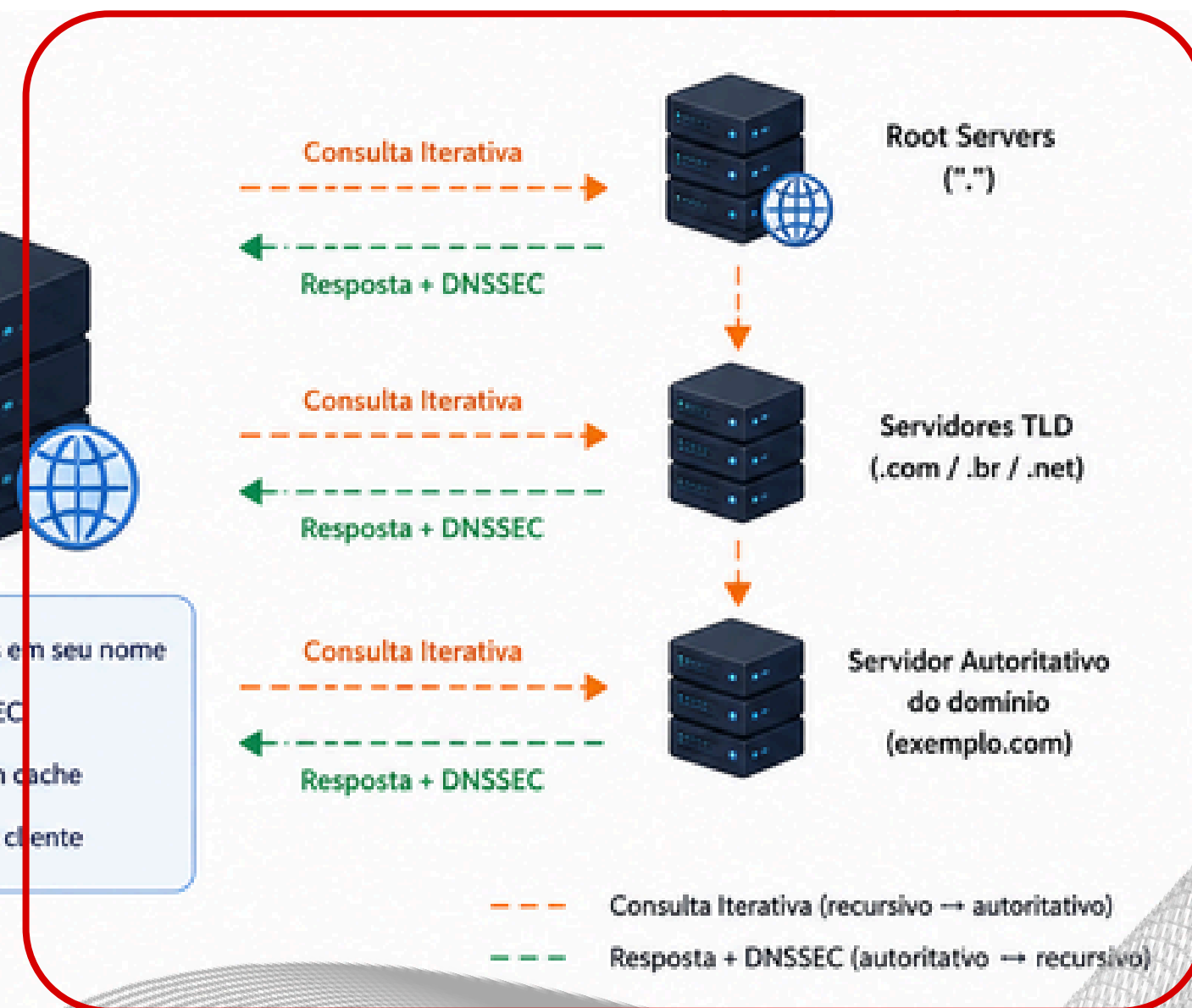
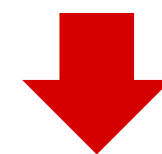


O DNSSEC em Recursivos

DoT / DoH / DoQ



DNSSEC



Como usar **DNSSEC**?

Unbound:

<https://nlnetlabs.nl/documentation/unbound/howto-anchor/>

Bind:

<https://bind9.readthedocs.io/en/stable/dnssec-guide.html>

**Em outubro de 2026 ocorrerá o rollover da Root KSK.
Operadores devem verificar se seus resolvedores suportam
atualização automática da Trust Anchor (RFC 5011).**



O DNS não é apenas mais um serviço

DNS Recursivo é:

- ✓ **Indicador**
- ✓ **Segurança**
- ✓ **Performance**
- ✓ **Diagnóstico**
- ✓ **Inteligência da rede**



O DNS deixou de ser apenas um serviço de resolução de nomes. Hoje ele é uma plataforma de observabilidade, desempenho e segurança para toda a rede. Quem monitora o DNS, também monitora a saúde da Internet dos seus clientes.



Obrigado!

Eng. Pedro Filho

+55 (43) 99919-5908

pedroorlandofilho@gmail.com

