DNS Recursivo

O que é, como funcionam e como implantar de forma segura

Lucas Rayan Guerra

Introdução

O Sistema de Nome de Domínio, ou Domain Name System (DNS) em inglês, é um dos pilares fundamentais da internet, atuando como a "lista telefônica" que traduz nomes de domínio legíveis por humanos (como www.google.com) em endereços IP compreensíveis por máquinas (como 172.217.194.101, que é um dos IPs da Google). Dentro desse ecossistema, o servidor DNS recursivo, ou resolver, desempenha um papel crucial, mas frequentemente subestimado. Ele é o intermediário que busca a resposta para as consultas dos usuários, e sua configuração impacta diretamente a performance, a segurança e a privacidade da rede.

Esta cartilha oferece um guia completo sobre o que é um DNS recursivo, como ele funciona e, mais importante, como implementá-lo de forma segura, com foco na ferramenta mais tradicional do mercado, o BIND 9, além de apresentar alternativas modernas.

O que é um DNS Recursivo?

Um servidor DNS recursivo (ou resolver) é um servidor que aceita consultas de clientes (como um navegador web em um notebook ou um aplicativo em um smartphone) e se encarrega de encontrar a resposta completa para essa consulta. Ele faz isso "recursivamente", consultando outros servidores DNS na internet em nome do cliente. Mas é crucial diferenciá-lo de um servidor DNS autoritativo.

Tipos de Servidor DNS	
Tipo	**Função Principal**
Autoritativo	Fornece a resposta "oficial" para domínios que ele hospeda. O servidor DNS autoritativo do NIC.br, por exemplo, sabe qual é o IP do servidor que está responsável pelo site “https://nic.br/”.
Recursivo	Busca a resposta para uma consulta em nome do cliente e armazena essa resposta por um tempo. Ele atua como um cache local, mais próximo do cliente.

Em uma analogia simples, o servidor recursivo é como um bibliotecário que vai a várias seções da biblioteca (outros servidores DNS) para encontrar o livro (a resposta) que você pediu. O servidor autoritativo é o próprio autor do livro, que detém a informação original.

Como Funciona o Processo de Resolução Recursiva de Domínios?

Quando um usuário tenta acessar o site “cienciaembarcada.com.br” em seu navegador, uma série de etapas ocorre em milisegundos:

1 - Consulta do Cliente: O navegador ou aplicação precisa resolver o nome de domínio “cienciaembarcada.com.br” em um endereço IP para estabelecer a conexão.

2 - Verificação do Cache do Navegador: O navegador verifica primeiro seu próprio cache DNS. Se ele já acessou esse site recentemente e a entrada ainda é válida (dentro do TTL - Time To Live), usa essa informação imediatamente.

3 - Verificação do Cache do Sistema Operacional: Se o navegador não encontrou a resposta, o sistema operacional verifica seu cache DNS local. Caso encontre uma entrada válida, retorna o endereço IP ao navegador sem precisar fazer consultas externas.

4 - Consulta ao Servidor DNS Recursivo: Se a informação não está em nenhum cache local, o sistema operacional (stub resolver) envia uma consulta para o servidor DNS recursivo configurado na rede (geralmente fornecido pelo provedor de internet ou configurado manualmente, como o 8.8.8.8 do Google ou 1.1.1.1 da Cloudflare).

5 - Verificação do Cache do Servidor Recursivo: O servidor recursivo primeiro verifica seu próprio cache. Se ele já resolveu “cienciaembarcada.com.br” recentemente e a resposta ainda é válida (dentro do TTL), ele a retorna imediatamente ao cliente, acelerando significativamente o processo.

6 - Consulta aos Root Servers: Se a informação não está em cache, o servidor recursivo inicia a busca na hierarquia DNS. Ele contata um dos 13 clusters de servidores raiz (.) da internet, enviando a consulta completa: "Qual o endereço IP de cienciaembarcada.com.br?". Os servidores raiz analisam o domínio da direita para a esquerda e respondem com os endereços dos servidores TLD (Top-Level Domain) responsáveis por ".br".

7 - Consulta aos TLD Servers: O servidor recursivo envia a mesma consulta completa a um dos servidores TLD de .br: "Qual o endereço IP de cienciaembarcada.com.br?". O servidor TLD analisa o domínio e responde com os endereços dos servidores DNS autoritativos (nameservers) responsáveis especificamente pelo domínio "cienciaembarcada.com.br".

8 - Consulta aos Servidores Autoritativos: Finalmente, o servidor recursivo pergunta ao servidor autoritativo de cienciaembarcada.com.br: "Qual é o endereço IP de cienciaembarcada.com.br?". O servidor autoritativo, que possui os registros DNS definitivos desse domínio, fornece a resposta final com o endereço IP correspondente.

9 - Resposta ao Cliente: O servidor recursivo recebe o endereço IP do servidor autoritativo e o entrega ao cliente (sistema operacional do usuário).

10 - Armazenamento em Cache (Múltiplos Níveis): O endereço IP é armazenado em cache em vários níveis: no servidor recursivo, no cache do sistema operacional e no cache do navegador. Cada um respeita o TTL (Time To Live) definido pelo servidor autoritativo do domínio. Isso permite que consultas futuras ao mesmo domínio sejam respondidas muito mais rapidamente, sem precisar repetir todo o processo de resolução.

11 - Estabelecimento da Conexão: Com o endereço IP em mãos, o navegador pode finalmente estabelecer a conexão TCP/IP com o servidor web e solicitar o conteúdo da página.

Por que um DNS Recursivo Seguro é Importante?

Um servidor DNS recursivo mal configurado ou desprotegido não é apenas um risco para a própria organização, mas para toda a internet. Os principais riscos incluem:

- **Ataques de Amplificação DDoS (Open Resolvers):** Se o seu servidor recursivo aceita consultas de qualquer pessoa na internet (tornando-se um "Open Resolver"), ele pode ser abusado por atacantes para participar de ataques de negação de serviço. O atacante envia uma pequena consulta ao seu servidor com o endereço IP de origem falsificado (spoofing) para o da vítima. Seu servidor, tentando ser prestativo, envia uma resposta muito maior para a vítima, amplificando o tráfego do ataque [1].

- **Envenenamento de Cache (Cache Poisoning):** Atacantes podem tentar injetar respostas falsas no cache do seu servidor recursivo. Se bem-sucedidos, eles podem redirecionar os usuários da sua rede para sites maliciosos (phishing, malware) quando eles tentam acessar sites legítimos.

- **Vazamento de Dados e Privacidade:** Servidores recursivos processam todas as consultas DNS dos usuários de uma rede. Se não forem devidamente protegidos, podem vazar informações sobre os hábitos de navegação e os serviços acessados pelos usuários.

Implementando um Servidor DNS Recursivo Seguro com BIND 9

O BIND (Berkeley Internet Name Domain) é a implementação de DNS mais utilizada na internet. Embora robusto, sua configuração padrão não é otimizada para segurança [2].

Requisitos e Boas Práticas Iniciais

- **Servidor Dedicado:** Execute o BIND em um servidor dedicado exclusivamente à função de DNS recursivo. Isso minimiza a superfície de ataque e evita que outros serviços impactem ou sejam impactados pelo DNS [3].

- **Execução com Usuário Não Privilegiado:** Configure o BIND para rodar com um usuário sem privilégios (named, por exemplo) para limitar o dano em caso de uma exploração de vulnerabilidade.

- **Manter o Software Atualizado:** Inscreva-se nas listas de anúncios de segurança do ISC (Internet Systems Consortium) e aplique patches de segurança assim que forem disponibilizados.

Configuração Essencial de Segurança (named.conf.options)

A maior parte da configuração de segurança de um BIND recursivo é feita no bloco **options** do arquivo **named.conf**.

Controle de Acesso (Prevenção de Open Resolver)

Esta é a medida mais crítica. Use Access Control Lists (ACLs) para definir explicitamente quem pode fazer consultas recursivas.

```
acl "trusted-clients" {
    192.168.0.0/16;    // Sua rede local
    10.0.0.0/8;        // Outro bloco de IPs confiáveis
    localhost;
    localnets;
};

options {
    // ... outras opções

    allow-query { trusted-clients; };
    allow-recursion { trusted-clients; };
    allow-query-cache { trusted-clients; };
};
```

- allow-query: Permite que apenas clientes confiáveis façam qualquer tipo de consulta.

- allow-recursion: Restringe a recursão apenas para clientes confiáveis.

Ocultar a Versão do BIND

Evite que atacantes identifiquem a versão do seu BIND para buscar exploits conhecidos.

```
options {
    // ...
    version "not currently available";
};
```

Rate Limiting (Limitação de Taxa)

O BIND possui mecanismos para limitar o número de respostas a consultas idênticas, ajudando a mitigar ataques de amplificação.

```
options {
    // ...
    rate-limit {
        responses-per-second 5; // Limita respostas idênticas para 5 por segundo
        window 5; // Janela de tempo de 5 segundos
    };
};
```

Ativando a Validação DNSSEC

O DNSSEC (DNS Security Extensions) garante a autenticidade e a integridade das respostas DNS, prevenindo ataques de envenenamento de cache. A ativação no BIND é simples:

```
options {
    // ...
    dnssec-validation auto;
};
```

Exemplo de Configuração Segura (named.conf.options)

```
acl "trusted-clients" {
    192.168.0.0/16;
    10.0.0.0/8;
    localhost;
    localnets;
};

options {
    directory "/var/cache/bind";

    // --- Segurança Essencial ---
    allow-query { trusted-clients; };
    allow-recursion { trusted-clients; };
    allow-query-cache { trusted-clients; };

    // --- Prevenção de Amplificação e Abuso ---
    rate-limit {
        responses-per-second 5;
        window 5;
    };

    // --- Validação DNSSEC ---
    dnssec-validation auto;

    // --- Ocultar Informações ---
    version "not currently available";

    // --- Otimizações ---
    listen-on-v6 { any; };
    listen-on { any; };
    recursion yes;
};

// Logging (opcional, mas recomendado)
logging {
    channel default_log {
        file "/var/log/named/default.log" versions 3 size 5m;
        severity info;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
    category default { default_log; };
};
```

Outras Soluções de DNS Recursivo

Embora o BIND seja o padrão da indústria, várias alternativas modernas oferecem vantagens em performance, segurança e facilidade de uso para a função de recursão.

Soluções de DNS Recursivo		
Serviço	**Foco Principal**	**Fator de Amplificação**
Unbound	Segurança e Performance	Leve, projetado do zero com foco em segurança (DNSSEC), configuração mais simples para recursão [4].
PowerDNS Recursor	Alta Performance e Flexibilidade	Excelente performance, suporte a scripting em Lua para políticas avançadas de filtragem e roteamento.
Knot Resolver	Modernidade e Performance	Rápido, com funcionalidades modernas como prefetching de cache e uma arquitetura modular.

Unbound: Desenvolvido pela NLnet Labs, é a escolha preferida para muitos ambientes que necessitam de um resolver puro, seguro e de alto desempenho. Sua configuração é notavelmente mais enxuta que a do BIND quando o objetivo é apenas recursão.

PowerDNS Recursor: Parte da suíte PowerDNS, é conhecido por sua performance extrema e pela capacidade de customização via scripts Lua, permitindo que operadores criem lógicas complexas de resolução e segurança.

Knot Resolver: Desenvolvido pela CZ.NIC, destaca-se pela arquitetura modular e alto desempenho com uso eficiente de memória. Oferece customização via scripts Lua e suporte nativo a DNS-over-TLS e DNS-over-HTTPS, sendo ideal para ambientes que priorizam privacidade e escalabilidade.

Monitoramento e Logs

Um servidor DNS recursivo em produção requer monitoramento contínuo para garantir disponibilidade, identificar problemas de desempenho e detectar possíveis ataques ou comportamentos anômalos. Logs bem configurados são fundamentais para troubleshooting e análise de segurança.

Configuração de Logs no BIND 9

O BIND permite configuração granular de logs através de canais e categorias. Uma configuração básica de logs seria adicionar o seguinte bloco **logging** no arquivo **named.conf**:

```
logging {
    channel default_log {
        file "/var/log/named/default.log" versions 3 size 5m;
        severity info;
        print-time yes;
        print-severity yes;
        print-category yes;
    };

    channel security_log {
        file "/var/log/named/security.log" versions 5 size 10m;
        severity info;
        print-time yes;
    };

    channel query_log {
        file "/var/log/named/queries.log" versions 3 size 20m;
        severity info;
        print-time yes;
    };

    category default { default_log; };
    category security { security_log; };
    category queries { query_log; };
    category rate-limit { security_log; };
};
```

Métricas Importantes a Monitorar

Taxa de Cache Hit: Percentual de consultas respondidas diretamente do cache sem necessidade de recursão completa. Uma taxa saudável geralmente fica acima de 80-90%, indicando que o cache está efetivo.

Consultas por Segundo (QPS): Volume total de consultas processadas. Monitore picos anormais que podem indicar ataques ou problemas na rede.

Falhas de Validação DNSSEC: Erros na validação DNSSEC podem indicar problemas de configuração ou tentativas de ataque. Devem ser investigados imediatamente.

Latência de Resposta: Tempo médio para responder consultas. Aumentos significativos podem indicar problemas de rede, sobrecarga do servidor ou problemas com servidores autoritativos upstream.

Consultas Bloqueadas por Rate Limiting: Alto volume pode indicar tentativa de ataque de amplificação.

Ferramentas de Monitoramento

BIND Statistics Channel: O BIND pode expor estatísticas em tempo real via HTTP. Configure no **named.conf**:

```
statistics-channels {
    inet 127.0.0.1 port 8053 allow { 127.0.0.1; };
};
```

Acesse via navegador em http://127.0.0.1:8053 para visualizar estatísticas detalhadas.

Scripts de Análise de Logs: Ferramentas como dnstop e dnstracer ajudam a analisar padrões de tráfego DNS em tempo real.

Prometheus e Grafana: Use exporters como o bind_exporter para coletar métricas do BIND e visualizá-las em dashboards do Grafana, permitindo monitoramento histórico e alertas automatizados.

Alertas Recomendados

- Queda do serviço DNS
- Taxa de cache hit abaixo de 70%
- Aumento súbito de QPS (>200% da média)
- Alto volume de falhas DNSSEC
- Espaço em disco baixo para logs
- Número elevado de consultas bloqueadas

Listas de Bloqueio (RPZ - Response Policy Zones)

Zonas de Política de Resposta, ou Response Policy Zones (RPZ) em inglês, é um mecanismo que permite que servidores DNS recursivos apliquem políticas de segurança bloqueando ou redirecionando consultas a domínios específicos. Funciona como um firewall no nível DNS, protegendo usuários de acessar conteúdo malicioso, phishing, malware ou categorias indesejadas de sites.

O servidor DNS carrega zonas RPZ que contêm listas de domínios a serem bloqueados. Quando uma consulta corresponde a um domínio listado, o servidor pode:

- Retornar NXDOMAIN (domínio não existe)
- Redirecionar para um endereço IP específico (página de aviso)
- Retornar uma resposta vazia
- Bloquear completamente a consulta

Fontes Confiáveis de Listas RPZ

- **Spamhaus:** Oferece feeds RPZ gratuitos e comerciais focados em malware, phishing e botnet C&C (command-and-control).

- **Abuse.ch:** Mantém listas atualizadas de domínios associados a malware, incluindo URLhaus e ThreatFox.

- **SURBL:** Lista de domínios usados em spam e phishing.
- **Listas comunitárias:** Projetos como Pi-hole e Steven Black's hosts oferecem listas de bloqueio que podem ser convertidas para formato RPZ.

Configuração Básica no BIND 9

Primeiro, adicione a configuração RPZ no **named.conf**:

```
options {
    // ... outras opções ...

    response-policy {
        zone "rpz.malware" policy given;
        zone "rpz.phishing" policy given;
    } qname-wait-recurse no;
};

zone "rpz.malware" {
    type master;
    file "/etc/bind/zones/rpz.malware.zone";
};

zone "rpz.phishing" {
    type master;
    file "/etc/bind/zones/rpz.phishing.zone";
};
```

Agora é só criar os arquivos de RPZ com as configurações pertinentes para a organização.

Exemplo de arquivo de zona RPZ (rpz.malware.zone):

```
$TTL 60
@   IN  SOA localhost. root.localhost. (
        2024010101  ; Serial
        3600        ; Refresh
        1800        ; Retry
        604800      ; Expire
        60 )        ; Minimum TTL
    IN  NS  localhost.

; Bloquear domínio malicioso específico
malicious-site.com  CNAME .

; Bloquear todos os subdomínios
*.phishing-domain.com  CNAME .

; Redirecionar para página de aviso
badsite.net  A  10.0.0.100
```

Políticas de Resposta

- **NXDOMAIN (CNAME .):** Retorna que o domínio não existe. É a opção mais comum.
- **Redirecionamento (A/AAAA):** Redireciona para um servidor web local com página explicativa.
- ***NODATA (CNAME .):** Retorna uma resposta vazia (sem erro, mas sem dados).
- **DROP:** Simplesmente descarta a consulta sem resposta.

Boas Práticas

- **Atualize as listas regularmente:** Automatize o download e reload das zonas RPZ (diariamente ou semanalmente).
- **Monitore falsos positivos:** Mantenha um processo para usuários reportarem bloqueios incorretos.

- **Documente políticas:** Seja transparente sobre o que está sendo bloqueado e por quê.

- **Teste antes de produção:** Valide novas listas em ambiente de teste.

- **Mantenha lista de permissões:** Crie zonas RPZ de whitelist para domínios que não devem ser bloqueados.

Considerações Legais e Éticas

Transparência com usuários sobre filtragem aplicada: Usuários têm o direito de saber quando e quais tipos de conteúdo estão sendo filtrados. Comunique claramente as políticas de bloqueio.

Conformidade com legislação local sobre privacidade: Garanta que a implementação esteja em conformidade com leis como LGPD (Brasil), GDPR (Europa) e outras regulamentações aplicáveis à sua jurisdição.

Processo para contestação de bloqueios: Estabeleça canais claros para que usuários possam reportar falsos positivos e contestar bloqueios indevidos.

Documentação das políticas de bloqueio: Mantenha registro detalhado das categorias bloqueadas, fontes das listas e justificativas técnicas.

Neutralidade de Rede e Provedores de Internet: Provedores de Serviço de Internet (ISPs) devem ter extremo cuidado ao implementar filtragem de DNS via RPZ. Em muitas jurisdições, incluindo o Brasil através do Marco Civil da Internet (Lei 12.965/2014), existe o princípio da neutralidade de rede, que estabelece que provedores não devem discriminar, filtrar ou interferir no tráfego de dados de seus usuários, exceto em casos específicos determinados por ordem judicial ou para garantir a segurança da rede.

Provedores de Internet NÃO devem:

- Bloquear ou filtrar conteúdo baseado em decisões unilaterais.
- Implementar censura sem determinação judicial.
- Discriminar tipos de conteúdo ou serviços arbitrariamente.
- Usar RPZ para vantagens comerciais ou competitivas.

Exceções legítimas para ISPs:

- Cumprimento de ordens judiciais específicas.
- Bloqueio de ameaças de segurança comprovadas (malware, phishing, botnets).
- Proteção da própria infraestrutura de rede contra ataques.
- Implementação de controles parentais opcionais e explicitamente solicitados pelos assinantes.

Ambientes apropriados para RPZ:

- Redes corporativas internas (proteção de funcionários).
- Instituições educacionais (políticas de uso aceitável).
- Redes residenciais (controle parental voluntário).
- Ambientes governamentais (conformidade com políticas de segurança).
- Serviços DNS públicos que explicitamente oferecem filtragem como recurso opcional (ex: Cloudflare 1.1.1.2 para famílias).

Em todos os casos, a implementação deve ser transparente, documentada e respeitar os direitos dos usuários e a legislação vigente.

Troubleshooting Básico

Mesmo com configurações adequadas, problemas podem surgir em servidores DNS recursivos. A capacidade de diagnosticar e resolver rapidamente essas falhas é essencial para manter a disponibilidade dos serviços de rede. Esta seção apresenta algumas ferramentas de diagnóstico DNS, os problemas mais comuns e suas soluções práticas, permitindo identificar rapidamente a origem dos problemas e minimizar o tempo de inatividade.

Comandos Essenciais

dig (Domain Information Groper): A ferramenta mais poderosa para diagnóstico DNS.

```
# Consulta simples
dig example.com

# Consulta específica de tipo de registro
dig example.com MX

# Consulta a um servidor específico
dig @8.8.8.8 example.com

# Trace completo da resolução
dig +trace example.com

# Verificar DNSSEC
dig +dnssec example.com

# Resposta curta
dig +short example.com
```

nslookup: Ferramenta mais simples, útil para verificações rápidas.

```
# Consulta básica
nslookup example.com

# Consultar servidor específico
nslookup example.com 1.1.1.1

# Modo interativo
nslookup
> set type=MX
> example.com
```

host: Ferramenta simples para consultas rápidas.

```
# Consulta básica
host example.com

# Todos os registros
host -a example.com

# Servidor específico
host example.com 8.8.8.8
```

rndc (Remote Name Daemon Control): Controla o servidor BIND em execução.

```
# Recarregar configuração
rndc reload

# Ver estatísticas
rndc stats

# Limpar cache
rndc flush

# Status do servidor
rndc status

# Verificar se há erros de validação DNSSEC
rndc validation status
```

named-checkconf: Valida a sintaxe da configuração do BIND antes de reiniciar.

```
# Verificar configuração
named-checkconf

# Verificar arquivo específico
named-checkconf /etc/bind/named.conf

# Verificar e mostrar configuração
named-checkconf -p
```

named-checkzone: Valida arquivos de zona.

```
named-checkzone example.com /etc/bind/zones/example.com.zone
```

Problemas Comuns e Soluções

Problema: Servidor DNS não responde
Sintomas: Timeout em todas as consultas, serviços web inacessíveis

Diagnóstico:

```
# Verificar se o serviço está rodando
systemctl status named

# Verificar se está escutando na porta correta
netstat -tulpn | grep :53
# ou
ss -tulpn | grep :53

# Testar conectividade local
dig @localhost example.com
```

Soluções:

```
# Reiniciar o serviço DNS
systemctl restart named

# Verificar logs:
journalctl -u named -f

# Checar configuração de firewall
iptables -L | grep 53

# Validar configuração
named-checkconf
```

Problema: Falhas de validação DNSSEC
Sintomas: SERVFAIL em domínios com DNSSEC habilitado

Diagnóstico:

```
# Verificar validação DNSSEC
dig +dnssec example.com

# Verificar se há problemas específicos
delv @localhost example.com
```

Soluções:

- Verificar sincronização de relógio (DNSSEC depende de timestamps precisos)
- Confirmar que **dnssec-validation** está corretamente configurado
- Verificar conectividade com servidores autoritativos
- Checar logs para erros específicos de validação

Problema: Alta latência nas respostas
Sintomas: Navegação lenta, timeouts ocasionais

Diagnóstico:

```
# Medir tempo de resposta
dig example.com | grep "Query time"

# Trace para identificar gargalo
dig +trace example.com

# Verificar cache hit rate (via statistics channel)
curl http://localhost:8053
```

Soluções:

- Aumentar tamanho do cache no **named.conf**
- Verificar recursos do servidor (CPU, memória, rede)
- Considerar servidores DNS forwarders mais rápidos
- Investigar problemas de rede com servidores upstream

Problema: Open Resolver (servidor responde para qualquer um)
Sintomas: Servidor sendo usado em ataques DDoS, alto tráfego de saída

Diagnóstico:

```
# Testar de um IP externo
dig @SEU_IP_PUBLICO example.com

# Verificar configuração de ACL
named-checkconf -p | grep -A 10 allow-recursion
```

Soluções:

- Configurar ACLs restritivas imediatamente
- Implementar rate limiting
- Bloquear porta 53 no firewall para IPs não autorizados

Problema: Cache envenenado (poisoning)
Sintomas: Usuários sendo redirecionados para sites errados

Diagnóstico:

```
# Verificar respostas em cache
rndc dumpdb -cache
grep "dominio-suspeito.com" /var/cache/bind/named_dump.db

# Verificar DNSSEC
dig +dnssec dominio-suspeito.com
```

Soluções:

- Limpar cache: **rndc flush**
- Habilitar DNSSEC imediatamente
- Atualizar BIND para versão mais recente
- Investigar logs para identificar fonte do ataque

Problema: Erros de permissão
Sintomas: BIND não inicia, erros de acesso a arquivos nos logs

Diagnóstico:

```
# Verificar logs
journalctl -u named | grep -i permission

# Verificar propriedade dos arquivos
ls -la /etc/bind/
ls -la /var/cache/bind/
```

Soluções:

- Corrigir propriedade: **chown -R bind:bind /etc/bind/**
- Corrigir permissões: **chmod 755 /etc/bind/zones/**
- Verificar SELinux/AppArmor policies

DNS sobre HTTPS (DoH) e DNS sobre TLS (DoT)

DNS tradicional trafega em texto claro pela porta 53 UDP/TCP, permitindo que intermediários (ISPs, administradores de rede, atacantes) visualizem e até modifiquem consultas DNS. DNS-over-HTTPS (DoH) e DNS-over-TLS (DoT) são protocolos que criptografam as consultas DNS, protegendo a privacidade dos usuários.

DNS-over-HTTPS (DoH): Encapsula consultas DNS dentro de requisições HTTPS na porta 443, tornando-as indistinguíveis de tráfego web normal. Isso dificulta o bloqueio seletivo, mas também torna mais difícil para administradores de rede aplicar políticas de segurança.

DNS-over-TLS (DoT): Estabelece uma conexão TLS na porta 853, criando um túnel criptografado dedicado exclusivamente para tráfego DNS. É facilmente identificável e pode ser gerenciado separadamente por firewalls.

Benefícios para Privacidade

Ambos os protocolos impedem:

- Espionagem de consultas DNS por terceiros
- Manipulação de respostas DNS (man-in-the-middle)
- Análise de hábitos de navegação baseada em consultas DNS
- Censura baseada em DNS por ISPs ou governos

Considerações de Implementação

Vantagens:

- Proteção contra escuta passiva
- Previne manipulação de tráfego DNS
- Conformidade com regulamentações de privacidade (GDPR, LGPD)

Desafios:

- Maior complexidade de configuração
- Sobrecarga de processamento (criptografia)
- DoH pode contornar políticas de segurança corporativas
- Necessidade de certificados TLS válidos
- Nem todos os clientes suportam nativamente

Conclusão

Um servidor DNS recursivo é uma peça crítica da infraestrutura de rede. Configurá-lo de forma segura não é apenas uma boa prática, mas uma responsabilidade para com seus usuários e para a saúde da internet como um todo. Ao restringir o acesso, habilitar a validação DNSSEC e manter o software atualizado, os operadores de rede podem mitigar drasticamente os riscos de abuso e garantir um serviço de resolução de nomes rápido, confiável e seguro.

Referências

[1] Cloudflare. "DNS amplification DDoS attack".

[2] ISC. "BIND 9 Administrator Reference Manual".

[3] ISC. "BIND Best Practices - Recursive"

[4] NLnet Labs. "Unbound - A validating, recursive, and caching DNS resolver".