nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.br

Comitê Gestor da Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

KINDNS: Boas Práticas Operacionais para o DNS

ceptro.br nic.br cgi.br

Knowledge-Sharing and Instanting Norms for DNS and Name Security

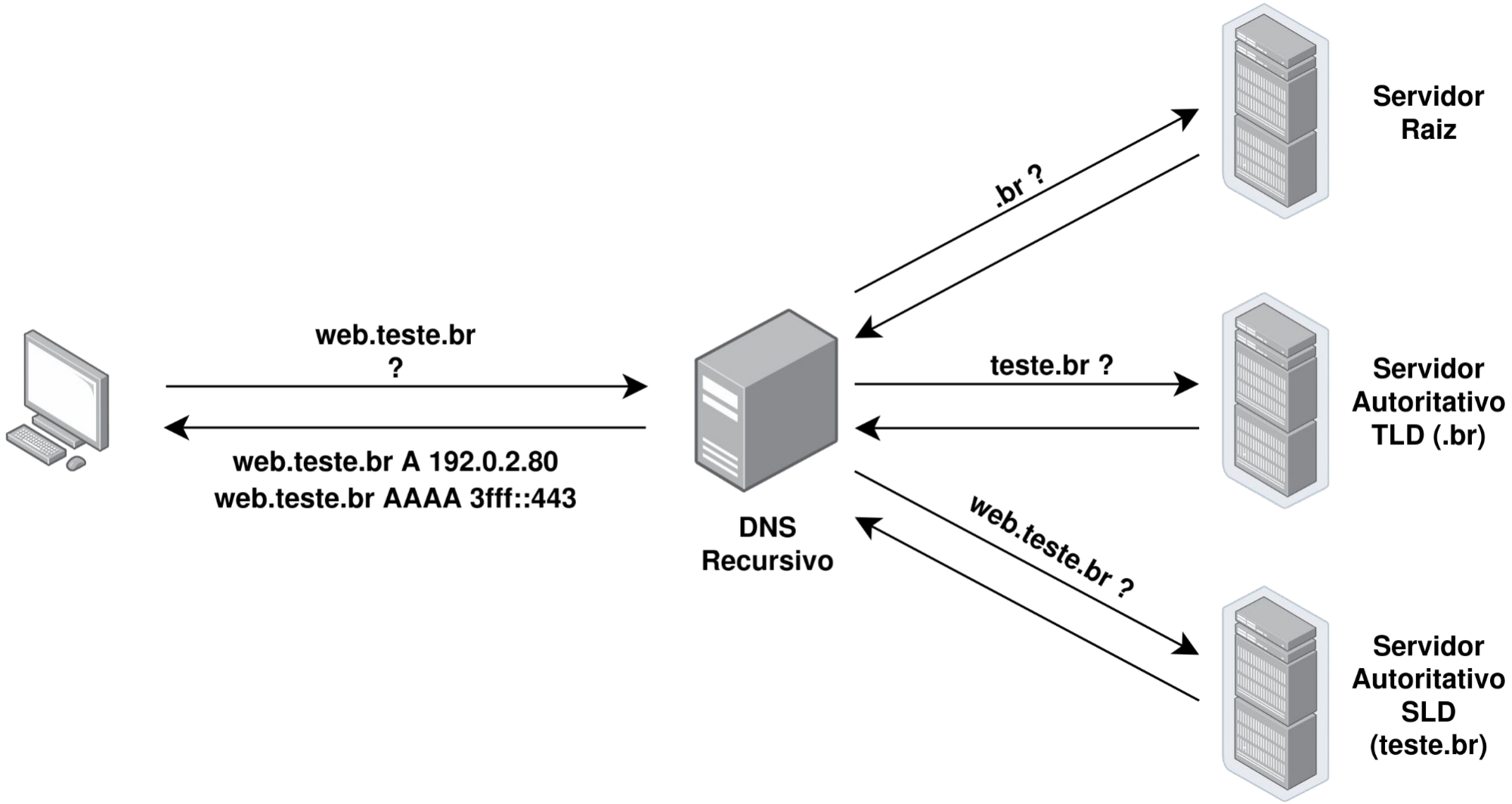
Normas de Compartilhamento de Conhecimento e Instanciamento para DNS e Segurança de Nomes de Domínio

KINDNS

DNS

ceptro.br nic.br cgi.br

Domain Name System (DNS)



DNS Security Extensions (DNSSEC)

RFC 9364 (Fev, 2023)

- Veio para tornar as consultas de DNS mais segura.
  - Garante a autenticidade da resposta da consulta.
  - Garante a integridade da resposta.
  - Garante a não existência de um domínio.
- Ele estabelece uma cadeia de confiança na consulta do DNS.

- Ele NÃO traz criptografia as consultas.
- Ele NÃO protege contra ataques de negação de serviço.

KINDNS

ceptro.br nic.br cgi.br

O que é o KINDNS?

É uma iniciativa da ICANN para disseminar boas práticas operacionais para os operadores de serviço de DNS.

Promover essas boas práticas, elas ajudam operadores de DNS a se protegerem, evitarem vulnerabilidades, serem vetores de ataques.

Princípios do KINDNS

- **DNS Security:**
  - Melhorar a segurança
  - Prevenir usuários de receber respostas DNS maliciosas
  - Diminuir as chances de corrupção de dados

- **DNS Availability and Resilience:**
  - Robustez
  - Resiliência
  - Estabilidade

Para quem é o KINDNS?

- **Operadores de Autoritativos**
  - TLDs e Zonas Críticas
  - Outros SLDs

- **Operadores de Recursivos**
  - Privados
  - Privados Compartilhados
  - Públicos

- **Todos Operadores de DNS**
  - Fortalecimento da Infraestrutura e Hardening

KINDNS para Operadores de Autoritativos

ceptro.br nic.br cgi.br

KINDNS para Operadores de Autoritativos

- TLDs (Top-level Domain) e Zonas Críticas
  - Operadores de domínios de topo **(.com, .org, .net, .br)**
  - Servidores raízes e seus espelhos. E SLDs críticos.

DNS Security (Segurança do DNS)

1. As zonas autorizadas **DEVEM** ser assinadas pelo DNSSEC e as melhores práticas para gerenciamento de chaves **DEVEM** ser seguidas.

2. O acesso à transferência de zona entre servidores autoritativos **DEVE** ser limitado. Configure ACLs e TSIG no pacote de software de DNS Autoritativo para restringir transferências de zona somente para servidores secundários.

3. A integridade do arquivo de zona **DEVE** ser controlada para evitar modificações inesperadas (maliciosa ou acidental).

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.

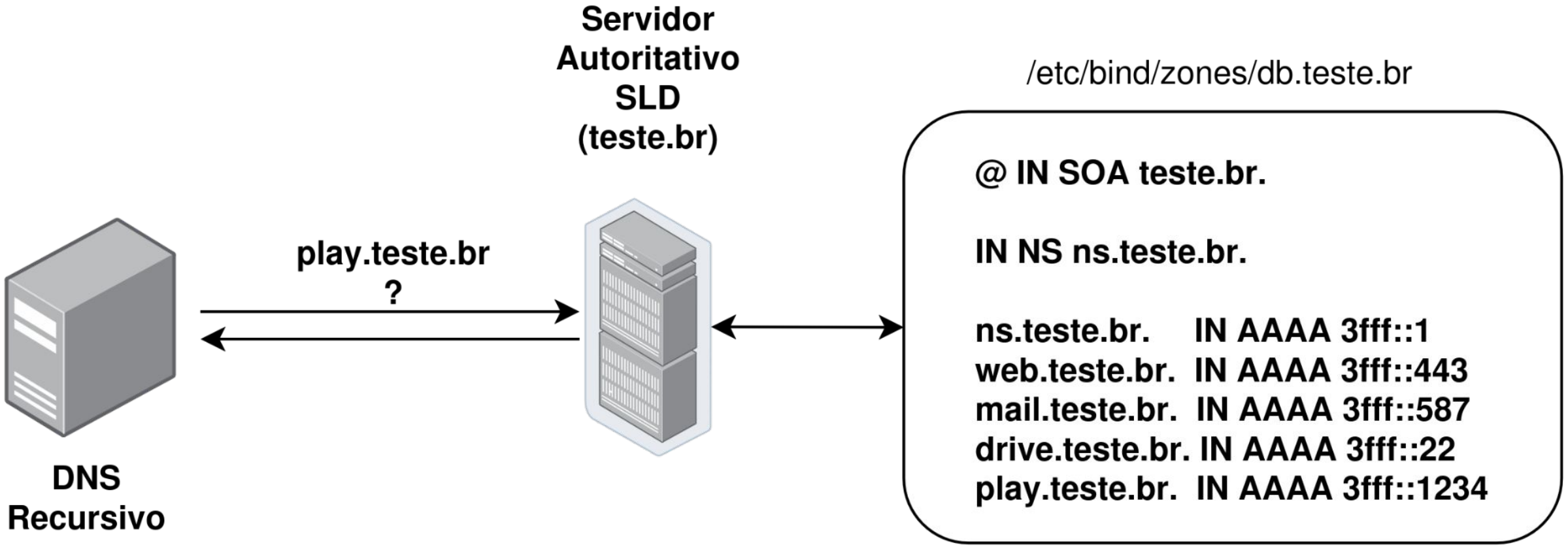
5. Pelo menos dois servidores de nomes distintos **DEVEM** ser usados para qualquer zona.

6. DEVE haver diversidade nas operações autoritativas para promover resiliência. Isto **DEVE** abranger uma ou mais das práticas seguintes: Programas, Redes e Geográfica

7. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

KINDNS para Operadores de Autoritativos

- SLDs (Second-level Domain)
  - Operadores de domínios de segundo nível não críticos.



KINDNS para Operadores de Autoritativos

- SLDs (Second-level Domain)
  - Operadores de domínios de segundo nível (**.com.br**, **.eng.br**, **.salvador.br, .gov.br**)

DNS Security (Segurança do DNS)

1. As zonas autorizadas **DEVEM** ser assinadas pelo DNSSEC e as melhores práticas para gerenciamento de chaves **DEVEM** ser seguidas.

2. O acesso à transferência de zona entre servidores autoritativos **DEVE** ser limitado. Configure ACLs e TSIG no pacote de software de DNS Autoritativo para restringir transferências de zona somente para servidores secundários.

3. A integridade do arquivo de zona **DEVE** ser controlada para evitar modificações inesperadas (maliciosa ou acidental).

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.

5. Pelo menos dois servidores de nomes distintos **DEVEM** ser usados para qualquer zona, tendo em mente a diversidade nas práticas operacionais e geográficas.
  1. Todos os servidores autoritativos para uma determinada zona **NÃO DEVEM** ser colocados na mesma sub-rede.
  2. Todos os servidores autoritativos para uma determinada zona **DEVEM** estar em locais físicos diferentes (não no mesmo rack, sala, cidade ou país).

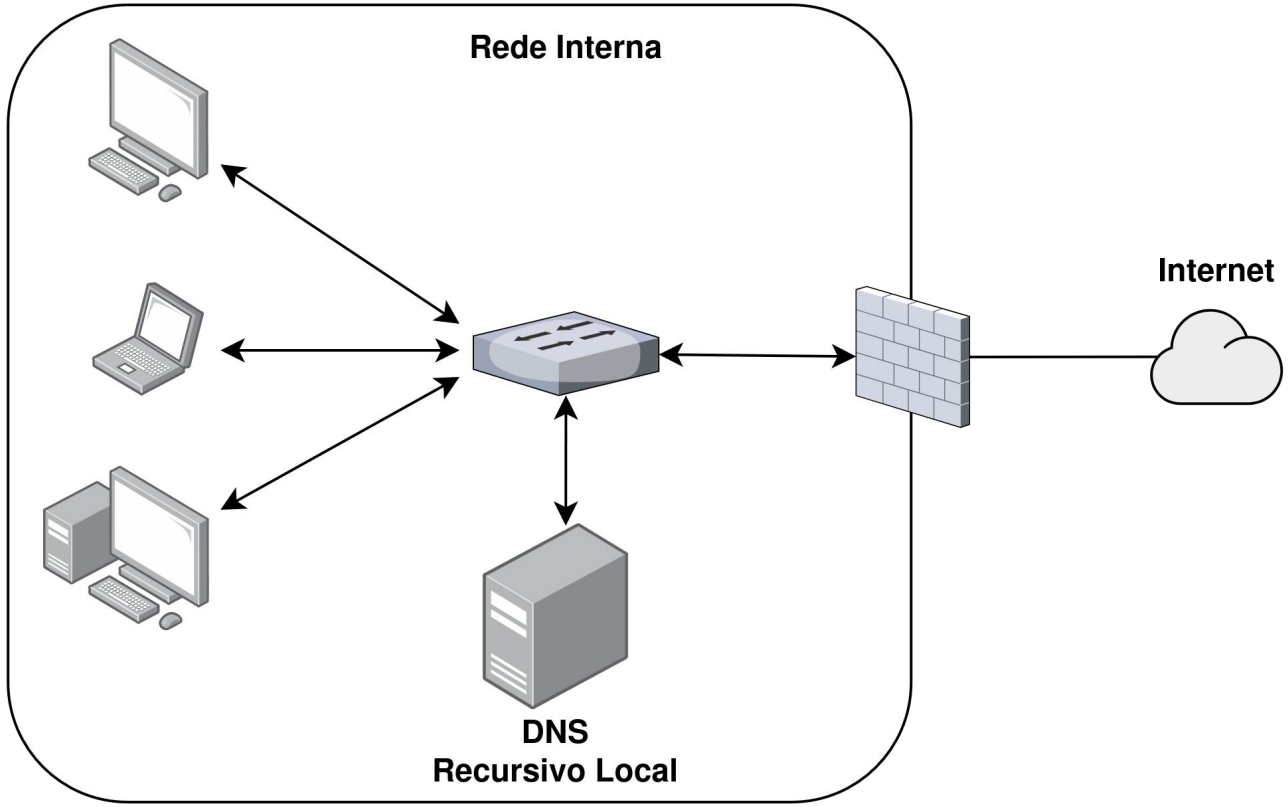
6. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

KINDNS para Operadores de Recursivo

ceptro.br nic.br cgi.br

KINDNS para Operadores de Recursivos

- Privado
  - Não acessíveis pela Internet.
  - Encontrado em redes corporativas, podem fazer parte de um domínio interno.



KINDNS para Operadores de Recursivos

- Privado
  - Não acessíveis pela Internet.
  - Encontrado em redes corporativas, podem fazer parte de um domínio interno.

DNS Security and Privacy (Segurança e Privacidade do DNS)

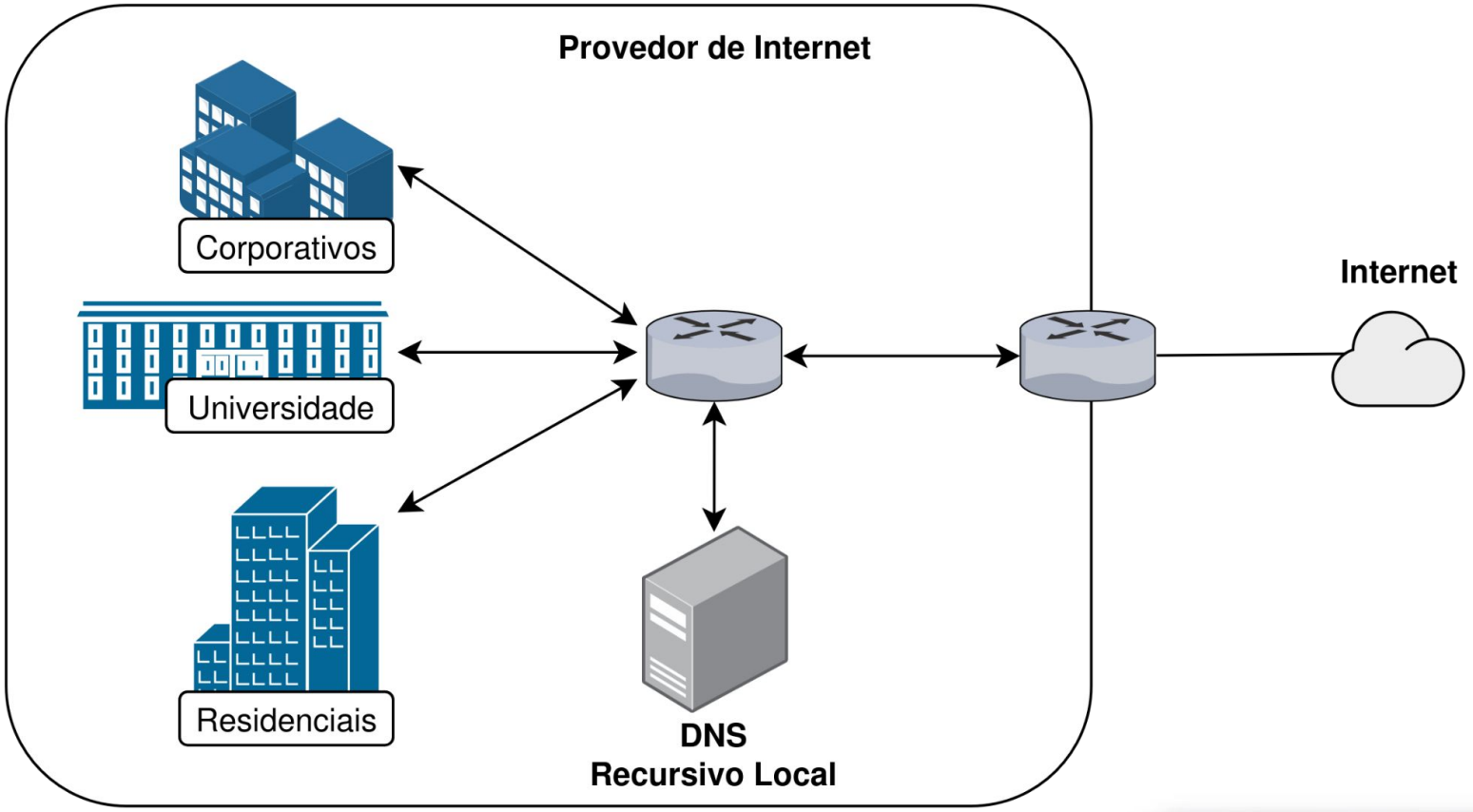
1. A validação DNSSEC **DEVE** ser habilitada para servidores recursivos.
2. ACLs **DEVEM** ser usadas para restringir quem pode enviar consultas recursivas aos seus servidores/validadores DNS.
3. A minimização de QNAME **DEVE** ser habilitada para mitigar o vazamento de nomes de domínio.

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.
5. Pelo menos dois servidores distintos DEVEM ser usados para fornecer serviços de recursão.
6. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

KINDNS para Operadores de Recursivos

- Privado Compartilhado
  - Serviço fornecido normalmente por ISPs.
  - Seus clientes possuem acesso, sejam residenciais, corporativos, empresariais ou móveis.



KINDNS para Operadores de Recursivos

- Privado Compartilhado
  - Serviço fornecido normalmente por ISPs.
  - Seus clientes possuem acesso, sejam residenciais, corporativos, empresariais ou móveis.

DNS Security (Segurança do DNS)

1. A validação DNSSEC **DEVE** ser habilitada para servidores recursivos.
2. ACLs **DEVEM** ser usadas para restringir quem pode enviar consultas recursivas aos seus servidores/validadores DNS.
3. A minimização de QNAME **DEVE** ser habilitada para mitigar o vazamento de nomes de domínio. **(Privacidade)**

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.
5. Seus serviços de recursivo **DEVEM** ter resiliência, usando pelo menos dois servidores distintos que levem em consideração a diversidade (Programas, Redes e Geográfica).
6. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

Bônus (prática adicional recomendada acima e além dos requisitos mínimos do KINDNS).

7. DoT (DNS sobre TLS) ou DoH (DNS sobre HTTPS) **DEVEM** estar habilitados.

KINDNS para Operadores de Recursivos

- Públicos
  - **Abertos**: acessíveis para todos pela Internet.
  - **Fechados**: acessíveis mediante a contratação do serviço.

DNS Security (Segurança do DNS)

1. A validação DNSSEC **DEVE** ser habilitada para servidores recursivos.
2. A minimização de QNAME **DEVE** ser habilitada para mitigar o vazamento de nomes de domínio. **(Privacidade)**
3. DoT (DNS sobre TLS) ou DoH (DNS sobre HTTPS) **DEVEM** ser habilitados e oferecidos aos clientes junto com o DNS Tradicional e não criptografado. **(Privacidade)**

DNS Availability and Resilience (Disponibilidade e Resiliência do DNS)

4. Os serviços DNS autoritativos e recursivos **NÃO DEVEM** coexistir no mesmo servidor DNS.
5. Os dados coletados por meio do registro passivo de consultas DNS **DEVEM** ser retidos apenas pelo tempo necessário para o bom funcionamento do serviço oferecido, incluindo solução de problemas, pesquisa e atendimento aos requisitos legais locais sobre retenção de dados.
6. Seus serviços de recursivo **DEVEM** ter resiliência, usando pelo menos dois servidores distintos que levem em consideração a diversidade (Programas, Redes e Geográfica).
7. O monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS **DEVE** ser implementado.

KINDNS para Todos

ceptro.br nic.br cgi.br

KINDNS para Todos

- Fortalecimento da Segurança de Rede
  - Prevenindo acesso não autorizado aos servidores.
  - Garantir que o tráfego interno não vaze para outras redes.

Network Security (Segurança de Rede)

1. As ACLs **DEVEM** ser implementadas para restringir o tráfego de rede aos seus servidores DNS.

1.1 Para operadores autoritativos, as ACLs **DEVEM** permitir apenas tráfego DNS e códigos de resposta ICMP associados aos seus servidores DNS autoritativos; o acesso a todos os outros serviços e portas da sua rede para servidores DNS **DEVE** ser negado.

1.2 Para todos os tipos de operadores DNS (autoritativos e recursivos), o tráfego de entrada de todas redes Bogons **DEVE** ser bloqueado, incluindo endereços privados (RFC 1918) e possivelmente, RFC 6598 (espaço de endereço IPv4 compartilhado) para IPv4. É claro que os operadores de DNS recursivos **NÃO** devem bloquear o espaço de endereços IP privados/compartilhados implantado na organização. Consulte: https://ipgeolocation.io/resources/bogon.html

2. A filtragem de saída **DEVE** ser implementada para que nenhum tráfego de rede possa sair da sua rede com um endereço IP de origem que não esteja atribuído a você ou a seus clientes (conforme BCP38/MANRS).

KINDNS para Todos

- Segurança de Hosts e Serviços
  - Aprimorar a segurança dos dispositivos operando serviço de DNS, reduzindo a chance destes dispositivos serem comprometidos, sofrerem ataques de negação de serviço ou outros ataques.

Host and Service Security (Segurança de Hospedeiros e Serviços)

3. A configuração de cada servidor DNS DEVE ser bloqueada. Isso inclui o seguinte:

3.1 Todos os serviços e pacotes de software que não são necessários para oferecer o serviço DNS no sistema **DEVEM** ser desinstalados ou desativados.

3.2 Os equipamentos hospedam os serviços DNS **DEVEM** executar apenas software DNS. Em outras palavras, os servidores DNS **NÃO DEVEM** executar outros serviços, como servidores web ou de e-mail.

3.3 Todos os *logs* relevantes para o subsistema DNS **DEVEM** estar habilitados. Os registros **DEVEM** ser enviados para um local central para arquivamento, inspeção e auditoria, e **DEVEM** ser retidos por um período razoável, de acordo com as políticas de retenção.

KINDNS para Todos

- Segurança de Hosts e Serviços
  - Aprimorar a segurança dos dispositivos operando serviço de DNS, reduzindo a chance destes dispositivos serem comprometidos, sofrerem ataques de negação de serviço ou outros ataques.

4. As permissões do usuário e o acesso de aplicações aos recursos do sistema **DEVEM** ser limitados. As permissões de arquivo e as restrições de propriedade **DEVEM** ser definidas para que os usuários e serviços não diretamente associados ao gerenciamento do subsistema DNS não tenham acesso de leitura ou gravação à configuração do serviço DNS, aos arquivos de dados e aos subsistemas de banco de dados.

5. Os arquivos de configuração do sistema e do serviço **DEVEM** ter controle de versão. Para operadores autorizados, os arquivos/dados de zona também **DEVEM** ser versionados.

6. O acesso aos serviços de gerenciamento (por exemplo, SSH, ferramentas de configuração baseadas na web) **DEVE** ser restrito. Todos os serviços não necessários para DNS ou gerenciamento **DEVEM** ser desabilitados ou desinstalados se possível, caso contrário, o acesso à rede aos serviços desnecessários **DEVE** ser bloqueado.

7. O acesso ao console do sistema **DEVE** ser protegido por meio de chaves criptográficas, protegidas por uma senha (por exemplo, chaves SSH) ou por meio de autenticação de dois fatores adequada (gerador de OTP ou baseada em token).

KINDNS para Todos

- Portal do Cliente e Segurança de Serviço
  - Prestação de suporte às necessidades de segurança do seu cliente.

Customer-Facing Portal and Service Security (Portal do Cliente e Segurança de Service)

8. As credenciais para acesso do cliente (registrantes e outros contatos do domínio) **DEVEM** seguir práticas sólidas de gerenciamento de credenciais, incluindo a oferta de autenticação de dois fatores como opção.

Como estou em relação ao KINDNS?

- Preenchendo a Autoavaliação
  - Os operadores de cada categoria podem realizar uma autoavaliação de suas práticas operacionais no serviço de DNS e utilizar os relatórios para corrigir as práticas em seu sistema que necessitam de atenção.
  - As autoavaliações serão preenchidas de forma anônima.

Como fazer parte do KINDNS?

- Formulário de Inscrição
  - Operadores podem se inscrever para participar de uma ou mais categorias do KINDNS.
  - A organização participante se compromete a implementar e seguir as boas práticas.
  - Os participantes aceitos se tornam embaixadores e promovem as boas práticas ao serviço.

Saiba mais!

Obrigado!

CEPTRO.br Cursos: cursosceptro@nic.br
CEPTRO.br IPv6: ipv6@nic.br
pvieira@nic.br

@comunicbr
@nicbr
@NICbrvideos

nic.br cgi.br

www.nic.br | www.cgi.br