FICHA TÉCNICA

# Proteção avançada contra DNS da Infoblox

## Minimize as interrupções nos negócios causadas por ataques baseados em DNS

### DESAFIO: INTERRUPÇÕES DE SERVIÇO

O DNS é fundamental para todas as organizações porque fornece conectividade de rede essencial para executar um negócio. Se o servidor DNS externo ficar inativo, toda a rede será desligada da Internet. A interrupção do DNS interfere ou desliga seus aplicativos críticos de TI, como e-mail, sites, VoIP e software como serviço (SaaS). Como um número significativo da força de trabalho começou a trabalhar remotamente em 2020, houve um grande aumento nos ataques DDoS. O DNS continua a ser um dos principais serviços direcionados para DDoS, porque é fundamental para manter uma empresa online. Além da perda de confiança e credibilidade dos clientes, ataques DDoS bem-sucedidos podem custar à organização centenas de milhares de dólares em receita perdida por mês.

A Infoblox oferece a mais ampla gama de proteção no mercado para proteger seus serviços DNS vitais contra ataques, garantindo a disponibilidade de cinco noves de que sua organização depende.  Ele oferece visibilidade centralizada sobre quem está usando a rede, em quais dispositivos estão e detalhes sobre o ataque para garantir uma resposta rápida.

### SOLUÇÃO: PROTEJA SUA EMPRESA CONTRA INTERRUPÇÕES CAUSADAS POR ATAQUES BASEADOS EM DNS

Com a Proteção avançada contra DNS (ADP) da Infoblox, sua empresa está sempre funcionando, mesmo sob um ataque baseado em DNS. Infoblox bloqueia a maior variedade de ataques, como ataques volumétricos, NXDOMAIN, explorações e sequestro de DNS. Ao contrário de abordagens que dependem do superdimensionamento da infraestrutura ou de limitação simples da taxa de resposta, a Proteção Avançada de DNS detecta inteligentemente e atenua ataques de DNS, respondendo apenas a consultas legítimas usando inteligência de ameaças constantemente atualizada, sem a necessidade de implantar patches de segurança. Com a Infoblox, você pode levar a confiabilidade da rede para o próximo nível, garantindo que sua infraestrutura crítica e seu negócio continuem operando em todos os momentos.

### CARACTERÍSTICAS PRINCIPAIS

**Reduzir interrupções nos negócios:** o Infoblox Advanced DNS Protection (ADP) monitora continuamente, detecta e impede todos os tipos de ataques DNS, incluindo ataques volumétricos e não volumétricos, como exploits DNS e sequestro de DNS, enquanto responde a consultas legítimas. Ele também mantém a integridade de DNS, que os ataques de sequestro de DNS podem comprometer. O Infoblox fornece uma base sólida para segurança, permitindo disponibilidade de cinco noves para sua rede.

**Adaptação a ameaças em evolução:** o Infoblox ADP utiliza a tecnologia Infoblox Threat Adapt™ para atualizar automaticamente a proteção contra novas ameaças e ameaças em evolução à medida que surgem. O Threat Adapt aplica análise e pesquisa independentes às técnicas de ataque em evolução, incluindo o que os especialistas em ameaças da Infoblox têm visto nas redes de clientes, para proteção contra atualizações. Ele adapta automaticamente a proteção para refletir as alterações na configuração do DNS.

## HABILITANDO PONTO E PONTO

A comunicação entre o cliente DNS (resolutor stub) e o servidor DNS local (resolutor recursivo) não é criptografada. Comunicações não criptografadas estão sujeitas a espionagem de dados, interceptação e exfiltração, também conhecido como o "último quilômetro" de segurança do DNS. Em resposta a isso, o setor iniciou o DNS sobre TLS (DoT) e o DNS sobre HTTPS (DoH) para fornecer privacidade e criptografia entre os clientes DNS e os servidores DNS externos da Internet. Implementar criptografia por meio do resolvedor DNS em sua rede permite que você permaneça no controle da experiência de rede do usuário, ao mesmo tempo em que fornece segurança e filtragem de conteúdo de acordo com os requisitos de sua política de segurança.
O ADP otimiza a criptografia DNS para nosso mecanismo de pacotes de alto desempenho chamado Fast Path para que você possa encerrar conexões DoT e DoH criptografadas em sua rede.

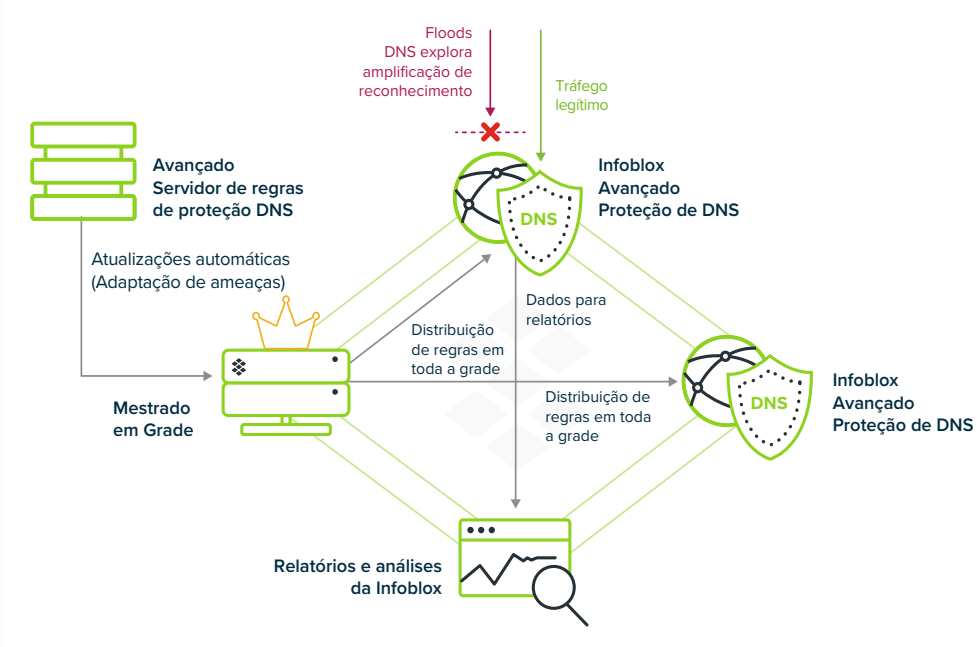


*Figura 1: A proteção avançada contra DNS da Infoblox oferece uma defesa exclusiva contra ataques baseados em DNS.*

## CARACTERÍSTICAS PRINCIPAIS (CONTINUAÇÃO)

**Obtenha visibilidade em painel único:**
Com a Infoblox, sua organização pode visualizar facilmente ataques DNS anteriores ou atuais e melhorar a eficiência operacional por meio de nossa rápida remediação de ameaças. A Infoblox Advanced DNS Protection também fornece uma visão única dos pontos de ataque em toda a rede e das fontes de ataque, fornecendo o inteligência necessária para o gerenciamento de ameaças. Está integrado com a nossa solução DNS.

**Implemente de forma flexível:**
Com o Infoblox, você tem a opção de implementar como complemento de assinatura para appliances Trinzic físicos e virtuais.

## O QUE NOSSOS CLIENTES DIZEM

"Os incidentes de serviço causados por ataques DDoS foram reduzidos pela metade, e as reclamações dos clientes sobre tempos de carregamento de página longos foram significativamente reduzidas."

**—VP de suporte ao cliente, grande provedor de serviços**

"Tenho usado o Infoblox para gerenciamento de endereços DNS, DHCP e IP há quatro anos. É um produto sólido. Movemos recursos porque o produto funciona muito bem. Nossa presença global é gerenciada por 1,5 FTE – ou seja, 65 dispositivos."

**—Gerente de infraestrutura global, Adobe**

## TABELA 1:
## RESUMO DOS TIPOS DE ATAQUE QUE A PROTEÇÃO AVANÇADA DE DNS (ADP) DEFENDE

| Nome do ataque | Tipo | Como funciona |
|---|---|---|
| Reflexão de DNS/ ataques de DDoS | Volumétrico | Uso de servidores DNS de terceiros (resolvedores abertos) para propagar um ataque de DoS ou DDoS |
| Amplificação do DNS | Volumétrico | Usando uma consulta especialmente criada para criar uma resposta amplificada para inundar a vítima com tráfego |
| TCP/UDP/ICMP inundações | Volumétrico | Negação de serviço na camada 3, derrubando uma rede ou serviço inundando-a com grandes quantidades de tráfego |
| NXDOMAIN | Volumétrico | Inundando o servidor DNS com solicitações de domínios inexistentes, causando saturação de cache e tempo de resposta mais lento |
| Subdomínio aleatório (ataques de gotejamento lento), ataques de bloqueio de domínio, ataques de domínio fantasma | Furtividade de baixo volume | Despejando o servidor DNS com solicitações para domínios fantasmas ou maliciosos configurados como parte do ataque, resultando em exaustão de recursos, saturação de cache, esgotamento do limite de consultas de saída e desempenho degradado. |
| Explorações baseadas em DNS | Explorações | Ataques que exploram vulnerabilidades no software DNS |
| Intoxicação por cache DNS | Explorações | Corrupção dos dados do cache DNS com um endereço não autorizado |
| Anomalias do protocolo | Explorações | Fazendo com que o servidor trave enviando pacotes e consultas malformados |
| Reconhecimento | Explorações | Tentativas de hackers de obter informações sobre o ambiente de rede antes de iniciar um grande DDoS ou outro tipo de ataque |
| Sequestro de DNS | Explorações | Ataques que substituem as informações de registro de domínio para apontar para um servidor DNS não autorizado |
| Exfiltração de dados (usando túneis conhecidos) | Explorações | O ataque envolve o túnel de outro protocolo através da porta 53 do DNS, o que é permitido se o firewall estiver configurado para transportar tráfego não relacionado ao DNS, com o objetivo de exfiltração de dados. |

## OPÇÕES DE ELETRODOMÉSTICOS

### ADP de software: Disponível em plataformas físicas e virtuais

Software ADP é um complemento de software para os appliances Trinzic TE-815/825/1415/1425/2215/2225/4015/4025.

**TE - 4015/4025**

**TE - 1415/1425**

**TE - 2215/2225**

**TE - 815/TE 825**

### Comece a fazer uma avaliação

Software gratuito de 60 dias ADP de avaliação com licença temporária para os clientes serão disponibilizados por meio de seus gerentes de conta/SEs.



**Sede corporativa**
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com