FICHE TECHNIQUE

Infoblox DNS Infrastructure Protection

Réduisez les interruptions d'activité liées aux attaques DNS

DÉFI : INTERRUPTIONS DE SERVICE

Le DNS constitue l'infrastructure fondamentale cachée des opérations numériques. Chaque site web, application et utilisateur dépend de lui pour rester connecté. Une panne des services DNS peut entraîner des pertes de revenus de plusieurs millions et nuire à la confiance des clients. Cela est particulièrement vrai pour les services DNS externes, qui maintiennent vos sites web, vos emails et d'autres applications accessibles au public. Parallèlement, les serveurs DNS externes doivent être exposés à l'Internet public, ce qui en fait une cible constante pour les cyberattaques, notamment :

- **Les attaques DDoS**, qui submergent les serveurs avec un trafic massif provenant de plusieurs sources, provoquant le plantage des sites web
- **Le détournement de DNS**, où les pirates falsifient les enregistrements DNS pour rediriger le trafic vers un site malveillant
- **L'empoisonnement du cache**, où les pirates injectent des données malveillantes ou invalides dans le cache d'un réseau, soit pour diffuser du contenu malveillant, soit pour rediriger les utilisateurs vers des sites malveillants
- **Les exploits NXDOMAIN**, qui inondent les serveurs DNS de requêtes pour des domaines inexistants, provoquant des interruptions de service

De plus, les enregistrements DNS autoritatifs externes sont distribués sur des serveurs Internet dans le monde entier. Si un pirate parvient à les modifier, il peut s'écouler des heures, voire des jours, avant de corriger toutes ces données erronées, période pendant laquelle vos sites web et autres applications en ligne peuvent devenir totalement inaccessibles.

Infoblox DNS Infrastructure Protection (anciennement Advanced DNS Protection) arrête les attaques DDoS et autres ciblant les serveurs DNS. Ce module logiciel NIOS permet à vos applications essentielles connectées à Internet de rester opérationnelles, même lorsque l'infrastructure DNS subit de massives attaques.

SOLUTION : PROTÉGEZ VOTRE ENTREPRISE CONTRE LES INTERRUPTIONS LIÉES AUX ATTAQUES DNS

DNS Infrastructure Protection détecte et bloque en permanence un large éventail de menaces visant les services DNS essentiels et empêche les pirates de manipuler l'intégrité du DNS. Elle bloque à la fois les attaques volumétriques, comme les DDoS et NXDOMAIN, et les exploits non volumétriques, tels que le détournement de DNS, l'empoisonnement du cache et d'autres menaces ciblant les serveurs DNS externes et internes.

Contrairement aux approches uniformisées qui peuvent bloquer le trafic légitime, DNS Infrastructure Protection utilise des informations continuellement mises à jour pour identifier les menaces réelles. Parallèlement, elle maintient le flux de trafic réel afin que votre entreprise reste opérationnelle, même lorsque l'infrastructure DNS est attaquée.

FONCTIONNALITÉS CLÉS

Réduire les interruptions d'activité : Infoblox DNS Infrastructure Protection surveille, détecte et bloque en continu tous les types d'attaques DNS, y compris les attaques volumétriques et non volumétriques, telles que les exploits DNS et le détournement de DNS, tout en répondant aux requêtes légitimes. Elle préserve également l'intégrité du DNS, que les attaques de détournement de DNS peuvent compromettre. Infoblox aide à garantir que les sites Web et les applications critiques restent en ligne et disponibles.

S'adapter à l'évolution des menaces : Infoblox DNS Infrastructure Protection utilise la technologie Infoblox Threat Adapt™ pour mettre automatiquement à jour la protection contre les menaces nouvelles et émergentes. Threat Adapt applique des analyses et recherches indépendantes sur les techniques d'attaque en évolution, y compris celles observées par les spécialistes Infoblox dans les réseaux clients, afin d'actualiser la protection. Elle s'adapte automatiquement aux changements de configuration DNS.

ACTIVER LE DNS CRYPTÉ (DoH ET DoT)

La communication entre le résolveur DNS client (stub resolver) et le serveur DNS local (résolveur récursif) n'est pas chiffrée. Ces communications non chiffrées sont vulnérables à l'espionnage, à l'interception et à l'exfiltration de données — un problème de sécurité appelé le « dernier kilomètre » du DNS. Pour y remédier, l'industrie a développé les protocoles DNS over TLS (DoT) et DNS over HTTPS (DoH) afin d'assurer la confidentialité et le chiffrement entre les clients DNS et les serveurs DNS Internet externes. Mettre en œuvre le chiffrement via le résolveur DNS de votre réseau vous permet de garder le contrôle de l'expérience réseau de vos utilisateurs tout en appliquant vos politiques de sécurité et de filtrage de contenu. DNS Infrastructure Protection optimise le chiffrement DNS afin que vous puissiez terminer les connexions DoT et DoH chiffrées directement sur votre réseau.

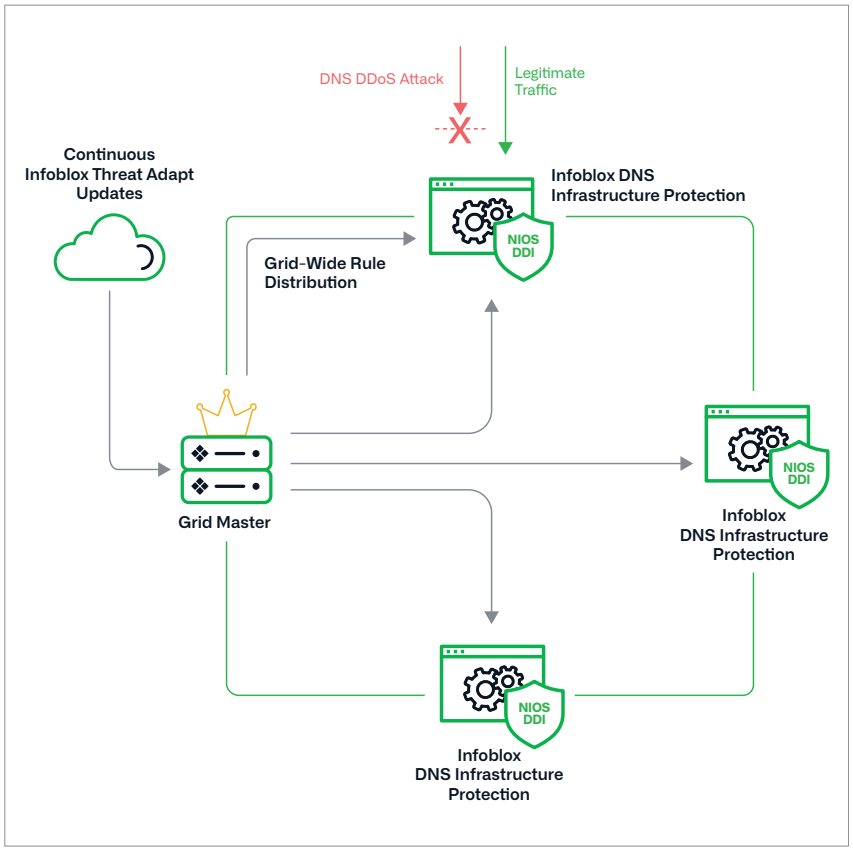

Figure 1. La Infoblox DNS Infrastructure Protection offre une défense unique contre les attaques basées sur le DNS.

Obtenir une visibilité centralisée : DNS Infrastructure Protection offre une visibilité étendue et centralisée sur les modèles d'attaque DNS, à la fois en temps réel et en historique. Les équipes NetOps et SecOps peuvent suivre les sources de menaces et visualiser les points d'attaque dans l'ensemble de l'environnement afin d'accélérer la mitigation et d'améliorer continuellement les défenses.

Disponible sur plateformes physiques, virtuelles et cloud : avec Infoblox, vous pouvez déployer la solution en tant que module logiciel sous abonnement sur des appliances Trinzic virtuelles et physiques, permettant aux services de fonctionner selon un modèle commun et prenant en charge les environnements sur site, cloud privé et cloud public.

TÉMOIGNAGES CLIENTS

« Le nombre d'incidents de service dus aux attaques DDoS a été réduit de moitié, et les plaintes des clients concernant la lenteur de chargement des pages ont considérablement diminué. »

Vice-Président du service client,
Grand fournisseur de services

« J'utilise Infoblox pour la gestion du DNS, le DHCP et des adresses IP depuis quatre ans. C'est un excellent produit. Nous avons pu redéployer nos ressources, car la solution est très efficace. Notre empreinte mondiale est gérée par 1,5 FT E— et cela concerne 65 appareils. »

Responsable de l'infrastructure mondiale,
Adobe

TABLEAU 1 : TYPES D'ATTAQUES CONTRE LESQUELLES LA DNS INFRASTRUCTURE PROTECTION VOUS PROTÈGE

Nom de l'attaque	Type	Comment ça marche
Attaques de réflexion DNS / DDoS	Volumétrique	Utilisation de serveurs DNS tiers (résolveurs ouverts) pour propager une attaque DoS ou DDoS
Amplification DNS	Volumétrique	Utilisation de requêtes spécialement conçues pour générer une réponse amplifiée, destinées à inonder la cible de trafic
Inondations TCP/ UDP/ICMP	Volumétrique	Déni de service au niveau 3 en saturant le réseau ou le service avec un volume élevé de trafic
NXDOMAIN	Volumétrique	Inondation du serveur DNS avec des requêtes vers des domaines inexistants, provoquant une saturation du cache et un ralentissement du temps de réponse
Sous-domaines aléatoires (attaques lentes), blocage de domaine, attaques de domaines fantômes	Attaques furtives à faible volume	Inondation du serveur DNS avec des requêtes vers des domaines fantômes ou dysfonctionnels, mis en place dans le cadre de l'attaque, entraînant un épuisement des ressources, une saturation du cache, un dépassement des limites de requêtes sortantes et une dégradation des performances
Exploits basés sur le DNS	Exploits	Attaques exploitant les vulnérabilités du logiciel DNS
Empoisonnement du cache DNS	Exploits	Corruption des données du cache DNS avec une adresse frauduleuse
Anomalies de protocole	Exploits	Envoi de paquets et requêtes malformés provoquant un plantage du serveur
Reconnaissance	Exploits	Reconnaissance — Collecte d'informations sur l'environnement réseau avant une attaque DDoS ou autre.
Détournement de DNS	Exploits	Attaques qui modifient les informations d'enregistrement de domaine pour rediriger vers un serveur DNS malveillant
Exfiltration de données (via des tunnels connus)	Exploits	Attaque consiste à encapsuler un autre protocole dans le port DNS 53 (autorisé si le pare-feu est configuré pour acheminer du trafic non DNS), à des fins d'exfiltration des données

OPTIONS D'APPAREILS

DNS Infrastructure Protection : disponible sur plateformes physiques et virtuelles

Infoblox DNS Infrastructure Protection protège contre un large éventail d'attaques DDoS ciblant le DNS, garantissant un service ininterrompu pour votre entreprise. C'est un module logiciel sous abonnement compatible avec une variété d'appliances matérielles et logicielles Trinzic, vous permettant de préserver l'intégrité du DNS et de prévenir les attaques DDoS externes et internes susceptibles de perturber vos opérations dans des environnements sur site et dans vos clouds privés et publics.

infoblox.

Infoblox réunit réseaux, sécurité et cloud avec une plateforme DDI protectrice, offrant résilience et agilité aux sociétés. Nous nous intégrons aux environnements hybrides et multicloud, automatisons les services réseau essentiels et sécurisons l'entreprise de manière proactive, tout en fournissant la visibilité et le contexte nécessaires pour agir rapidement sans compromis

Siège social
2390 Mission College Boulevard, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/fr

Version : 20251007v3