FICHE TECHNIQUE

Protection DNS avancée Infoblox pour les fournisseurs de services

DÉFI : INTERRUPTIONS DE SERVICE

Les fournisseurs de services cloud (FSC), les opérateurs mobiles et les prestataires cloud dépendent fortement du DNS, à la fois en tant que composant essentiel de connectivité et comme service qu'ils proposent à leurs clients, de manière implicite ou explicite. Les FSC doivent protéger cet atout vital, pour leur réputation et pour leurs clients qui dépendent d'une connectivité Internet stable et permanente. Si les serveurs DNS tombent en panne, vos abonnés sont coupés de l'internet. Une interruption du DNS perturbe ou bloque vos applications informatiques critiques, telles que les e-mails, les sites web, la VoIP et les logiciels en tant que service (SaaS).

Selon les principaux rapports de sécurité, le DNS est le deuxième service le plus ciblé par les attaques de la couche applicative, avec 72 % des entreprises affectées en 2018. Neustar estime que le coût d'une attaque par déni de service distribué (DDoS) menée via le DNS est supérieur à 220 000 $ par heure, sans compter la perte d'abonnés et l'atteinte à la réputation de la marque. Les pirates recherchent les maillons faibles, les vecteurs d'attaque, de votre réseau, et le protocole DNS est facile à exploiter pour des attaques DDoS ou un détournement DNS ; de telles attaques compromettent l'intégrité du DNS.

UNE MULTITUDE DE DÉFENSES, MAIS TOUJOURS À L'AVEUGLE

De nombreux réseaux de FSC adoptent une série d'outils, notamment des systèmes de prévention des intrusions (IPS), des pare-feu et des systèmes d'équilibrage de charge, qui sont capables de protéger divers aspects de l'infrastructure du fournisseur. Toutefois, ces outils sont inefficaces lorsqu'ils sont appliqués au DNS, car ils ne sont pas intégrés aux serveurs DNS et n'ont pas de compréhension ou de visibilité du DNS.

Même si ces outils sont largement déployés, de nombreux FSC se plaignent encore que la première fois qu'ils ont connaissance d'attaques contre le DNS, c'est lorsque des clients leur signalent des lenteurs dans les performances du réseau ou d'autres problèmes similaires. La plupart des organisations n'ont que peu ou pas d'alerte précoce concernant les attaques sur les systèmes DNS. De nombreuses équipes d'exploitation ont même recours à l'analyse manuelle des données de journal des serveurs DNS pour déterminer si les niveaux de trafic ont augmenté et si les serveurs ont été exposés à des risques ou compromis.

ZONES CRITIQUES NÉCESSITANT UNE PROTECTION

Deux zones critiques nécessitant une protection au sein du réseau du fournisseur sont les serveurs DNS autoritaires et les serveurs de mise en cache DNS. Les serveurs DNS autoritaires situés à différents endroits du réseau du fournisseur répondent aux requêtes DNS et aux demandes de connectivité de leur base d'abonnés. Les serveurs DNS autoritaires permettent la présence sur le web, les fonctions de e-commerce et la localisation de plusieurs composants réseau pour la connectivité IP mobile, notamment l'itinérance et la localisation

AVANTAGES ET FONCTIONNALITÉS

Réduisez les interruptions d'activité : Infoblox Advanced DNS Protection (ADP) 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. ADP préserve également l'intégrité du DNS, souvent compromise lors de détournements. Infoblox fournit une base solide pour la sécurité, garantissant une disponibilité réseau de 99,999 %.

Adaptez-vous à l'évolution des menaces : Infoblox ADP utilise la technologie Threat Adapt™, qui met automatiquement à jour la protection contre les menaces nouvelles ou en évolution. Threat Adapt applique une analyse indépendante et les recherches de spécialistes Infoblox (basées notamment sur les techniques observées dans les réseaux clients) pour ajuster la protection. La protection s'adapte automatiquement aux changements de configuration DNS.

des passerelles dans les réseaux LTE et 5G. Afin de garantir une expérience Internet fluide aux abonnés, la couche de mise en cache DNS est essentielle pour assurer une réponse rapide aux requêtes DNS. Il est donc crucial de mettre en cache les réponses aux requêtes pour les sites Web et autres URL fréquemment consultés afin d'obtenir des temps de réponse acceptables.

UNE NOUVELLE VARIABLE : LE DNS CHIFFRÉ

De nouvelles normes DNS chiffrées ont émergé qui, tout en protégeant la confidentialité des requêtes DNS et l'intégrité des réponses, peuvent faire perdre aux fournisseurs de services cloud une partie du contrôle nécessaire pour régir l'utilisation du DNS au sein de leurs réseaux, à moins qu'ils ne fournissent leurs propres services DNS chiffrés. Les DNS over TLS (sécurité de la couche transport) ou DoT, et DNS over HTTPS ou DoH, fonctionnent en chiffrant la communication DNS entre le résolveur stub de votre système d'exploitation ou une application locale et votre résolveur DNS récursif. Les deux technologies assurent la confidentialité des données et l'authentification en chiffrant les communications entre les clients DNS et les serveurs. Toutefois, ce faisant, de nombreuses solutions sont modifiées pour pointer vers des résolveurs DNS externes, ce qui permet aux appareils clients d'accéder à des services DNS hors du contrôle du fournisseur et expose l'abonné à des risques de sécurité potentiels et à des expériences négatives pour les clients. Les fournisseurs devraient prendre dès maintenant des mesures pour réduire les risques que ces technologies posent. La mise en œuvre du chiffrement via le résolveur DNS de votre réseau vous permet de garder le contrôle de l'expérience réseau de vos abonnés. Cela permettra aux fournisseurs de continuer à fournir des services de sécurité, de filtrage de contenu et d'autres services critiques sur le réseau.

SOLUTION : PROTÉGEZ VOTRE ENTREPRISE CONTRE LES INTERRUPTIONS CAUSÉES PAR LES ATTAQUES CIBLANT LE DNS

Avec Infoblox Advanced DNS Protection (ADP), votre entreprise reste opérationnelle, même en cas d'attaque ciblant le DNS. Infoblox bloque le plus large éventail d'attaques, telles que les attaques volumétriques, les attaques NXDOMAIN, les exploits et le détournement de DNS. Contrairement aux méthodes reposant sur la surcapacité d'infrastructure ou la limitation simple du taux de réponses, ADP détecte et atténue intelligemment les attaques DNS tout en ne répondant qu'aux requêtes légitimes, grâce à une threat intelligence constamment mise à jour, sans nécessiter le déploiement de correctifs de sécurité. Avec Infoblox, vous renforcez la fiabilité de votre réseau en garantissant que votre infrastructure réseau essentielle, et donc votre activité, reste fonctionnelle, en tout temps.

PREND EN CHARGE LES NORMES DNS CHIFFRÉES

Le système d'exploitation de l'identité du réseau (NIOS) d'Infoblox est le système d'exploitation qui alimente les services réseau principaux d'Infoblox, garantissant le fonctionnement continu de l'infrastructure réseau. Infoblox Encrypted DNS for Service Providers est une fonction NIOS qui permet un chiffrement efficace tout en fournissant le meilleur DNS d'Infoblox et des services à valeur ajoutée pour les abonnés. Avec la prise en charge de DNS-over-TLS et DoH, Infoblox Encrypted DNS offre une approche unique pour chiffrer votre trafic DNS. Contrairement aux méthodes reposant sur des équilibreurs de charge ou la surcapacité, Infoblox Encrypted DNS fonctionne comme un service unique pour tous vos besoins en DNS. Disponible via des instances virtualisées d'ADP, Infoblox Encrypted DNS leur permet de chiffrer les communications DNS jusqu'au dernier kilomètre entre leurs endpoints et les serveurs DNS, quel que soit le protocole pris en charge par l'endpoint. Il prend en charge cette fonctionnalité tout en résolvant les préoccupations de performances liées à la surcharge supplémentaire associée aux communications DNS chiffrées. Grâce à ce même service, nous permettons aux FSC de mettre en place un DNS crypté avec une latence de l'ordre de la microseconde lorsque la connexion est déjà établie et que toutes les autres fonctions DNS sont en cours d'exécution.

AVANTAGES ET FONCTIONNALITÉS

Profitez d'une visibilité unifiée : avec Infoblox, les fournisseurs de services de communication (CSP) peuvent facilement visualiser les attaques DNS passées ou en cours et améliorer l'efficacité opérationnelle grâce à notre remédiation rapide des menaces. Infoblox Advanced DNS Protection offre également une vue d'ensemble des vecteurs d'attaque à travers le réseau et des sources d'attaque, fournissant les renseignements nécessaires à la gestion des menaces. Il est intégré à notre solution DNS.

Déployez avec flexibilité : les opérateurs peuvent déployer sur les appliances virtuelles Infoblox Trinzic Flex, ce qui leur permet d'ajouter des capacités spécifiques à l'ensemble de leur infrastructure Infoblox tout en profitant de l'évolutivité flexible et d'une tarification basée sur la capacité, spécifique aux fournisseurs de services.

Réduisez vos coûts : Infoblox Software ADP exploite le matériel existant, ce qui signifie que les clients n'ont qu'à mettre à jour le logiciel qui fonctionne sur le matériel, d'où des coûts de mise à jour minimes.

LES OPTIONS DE DÉPLOIEMENT FLEXIBLES

Infoblox Advanced DNS Protection est conçu pour les environnements des fournisseurs de services de télécommunications nécessitant des déploiements évolutifs en périphérie. Il est disponible dans de multiples options de niveau opérateur, y compris les fonctions de réseau virtualisées (VNF) orchestrées et les solutions cloud natives.

- Infoblox Trinzic Flex : une plateforme virtuelle évolutive basée sur les ressources allouées aux machines virtuelles. Le système d'exploitation Infoblox Network Identity Operating System (NIOS) détecte automatiquement la capacité de la machine virtuelle et l'adapte à la plateforme appropriée. En outre, les appliances Trinzic Flex sont couvertes par le Service Provider License Contrat Program (SPLA).
- Disponible sur des plateformes physiques et virtuelles : Software ADP est un module d'abonnement logiciel pour les appliances Trinzic TE-815/825/1415/1425/2215/2225/4015/4025.

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 de couche 3 visant à provoquer l'arrêt d'un réseau ou d'un service en le saturant 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
Attaques de sous-domaines aléatoires (slow drip), verrouillage 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 ou requêtes malformés provoquant un plantage du serveur
Reconnaissance	Exploits	Tentatives de collecte d'informations sur l'environnement réseau avant le lancement d'une attaque DDoS ou d'un autre type d'attaque.
Détournement de DNS	Exploits	Attaques qui modifient les informations d'enregistrement de domaine pour les faire pointer vers un serveur DNS malveillant
Exfiltration de données (via des tunnels connus)	Exploits	Cette 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

Tableau 1 : résumé des types d'attaques contre lesquels Advanced DNS Protection (ADP) assure une protection

PROTÉGER LES ABONNÉS ET LES MARQUES

Les solutions de qualité opérateur Infoblox pour les fournisseurs de services protègent les abonnés en utilisant la Threat Intelligence mondiale et des forfaits de protection automatisés. Les solutions assurent la disponibilité des services DNS critiques dans des réseaux en évolution rapide, avec un trafic croissant, et même lors d'une attaque DDoS malveillante.

- Infoblox Advanced DNS Protection est la solution de protection DNS la plus complète et intégrée du secteur pour l'infrastructure DNS des fournisseurs de services.
- Capacité avancée et automatisée de détection et d'atténuation des attaques basées sur le DNS, telles que l'amplification, la réflexion, les anomalies de protocole et le tunneling, le tout intégré au serveur DNS.
- De qualité opérateur et disponible dans de multiples facteurs de forme, y compris les solutions orchestrées de fonction de réseau virtualisé (VNF) et natives du cloud, avec le serveur de mise en cache DNS le plus rapide au monde et la prise en charge des déploiements de mise en cache DNS et de DNS autoritaire.
- Règles de threat intelligence et de mitigation avec mises à jour automatiques d'Infoblox.
- La technologie brevetée Infoblox Grid™ offre un contrôle, une automatisation et une distribution étendus des mises à jour, afin de réduire les coûts de support opérationnel et d'éliminer le risque de pannes causées par des erreurs de configuration manuelles.
- Prend en charge les protocoles DNS chiffrés, y compris les DNS-over-TLS (DoT) et DNS-over-HTTPS (DoH).

Pour en savoir plus, visitez www.infoblox.com/sp ou contactez votre représentant Infoblox local dès aujourd'hui.

infoblox.

Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et par des innovateurs émergents, nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

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

+1.408.986.4000
www.infoblox.com/fr