FICHE TECHNIQUE

Renforcer la cybersécurité au niveau fédéral grâce au DNS crypté

Mise en œuvre d'un DNS chiffré conformément au décret présidentiel de la Maison-Blanche

APERÇU

Dans ses dernières recommandations, la Maison-Blanche a publié un décret présidentiel complet visant à renforcer et promouvoir la cybersécurité nationale. Le décret vise à renforcer la cybersécurité en améliorant la responsabilité des fournisseurs de logiciels et de services cloud, en renforçant les communications fédérales et les systèmes de gestion de l'identité, et en promouvant l'utilisation des technologies émergentes dans les départements et agences exécutifs. Parmi les principales mesures introduites figure notamment l'obligation d'utiliser des protocoles DNS cryptés qui garantissent la confidentialité et l'intégrité du trafic DNS. Cette mesure reconnaît que le DNS est un contrôle de sécurité de première ligne essentiel, soulignant son importance dans la stratégie de défense renforcée de la cybersécurité.

Conformément aux récents mandats fédéraux en cybersécurité, Infoblox Advanced DNS Protection (ADP) offre un soutien fiable pour le trafic DNS chiffré, garantissant la confidentialité et l'intégrité des communications DNS. Cette capacité est essentielle pour les agences fédérales qui cherchent à améliorer leurs mesures de cybersécurité et à se conformer au dernier décret présidentiel de la Maison-Blanche sur le DNS chiffré.

Les solutions d'Infoblox sont complètes, évolutives et faciles à mettre en œuvre, permettant une transition en douceur vers le DNS chiffré avec un minimum de perturbations. Il est important de noter que plus de 15 agences civiles fédérales américaines utilisent le chiffrement DNS Infoblox, qui est inclus dans la Protection DNS avancée. Cette adoption les aide à progresser dans la mise en œuvre du mandat de politique de sécurité Zero Trust en activant le chiffrement DNS pour soutenir leurs initiatives Zero Trust.

DÉFIS DES AGENCES

Le DNS chiffré nécessite des ressources informatiques supplémentaires, notamment sur les serveurs DNS, car il nécessite le chiffrement et le déchiffrement lors de l'envoi et de la réception des messages DNS. Les agences devraient anticiper cela et s'assurer que leurs serveurs DNS disposent de ressources suffisantes pour gérer la charge de requêtes avant de commencer tout déploiement à grande échelle de DNS chiffré. Un échec à mettre en œuvre correctement le DNS chiffré pourrait nuire à l'ensemble des réseaux, à leurs applications et à leurs utilisateurs.

Le DNS chiffré peut également compliquer la résolution des problèmes, car le personnel informatique utilisant des outils de dépannage réseau n'aura pas facilement accès au contenu des requêtes ou des réponses DNS. Le contenu des requêtes et des réponses DNS sera toujours disponible pour le personnel informatique sur les serveurs de noms eux-mêmes, bien sûr, parce que ces serveurs de noms auront effectué le décryptage requis.

FONCTIONNALITÉS CLÉS

Respect des exigences en cybersécurité
Garantit la conformité aux dernières directives fédérales en matière de cybersécurité.

Prise en charge du trafic DNS chiffré Intègre DNS-over-HTTPS (DoH) et DNS-over-TLS (DoT) pour des communications DNS sécurisées et authentifiées.

Protection avancée contre les menaces
Définit et maintient des blocs d'adresses et des domaines de routage pour NIOS et les locataires du cloud.

Enregistrement des requêtes à haute vitesse Capture et consigne le trafic DNS en temps réel sans impact significatif sur les performances.

Évolutif et fiable
Garantit une gestion efficace des volumes élevés de trafic DNS et DHCP grâce à une évolutivité et une fiabilité exceptionnelles.

Pour surmonter ces difficultés et garantir la résilience cybernétique, les agences devraient limiter la coexistence de plusieurs services critiques sur un même système. Compte tenu des exigences accrues en matière de calcul, cette séparation des tâches permettra d'obtenir la meilleure résilience possible. L'infrastructure hébergeant le service DNS doit être dédiée à cette tâche et renforcée à cet effet afin de réduire la surface d'attaque et de garantir que des ressources système adéquates soient disponibles pour le service DNS. L'infrastructure doit inclure une capacité suffisante pour les éléments du service DNS, tels que la journalisation, la prise en charge des protocoles DNS chiffrés et le DNS protecteur, le cas échéant. Cela peut être plus facile à réaliser avec des services DNS spécialisés, soit en tant que service, soit par le biais d'appliances virtuelles ou physiques.

INFOBLOX ADVANCED DNS PROTECTION

En tant que leader des solutions DNS sécurisées, Infoblox est idéalement positionné pour aider les agences fédérales à répondre à ces nouvelles exigences. Infoblox Advanced DNS Protection (ADP) est un module complémentaire logiciel sous forme d'abonnement pour divers appliances matérielles et logicielles Infoblox Trinzic. Il prend en charge les protocoles DNS chiffrés tels que DNS-over-HTTPS (DoH) et DNS-over-TLS (DoT), ce qui le rend adapté aux environnements sur site et sur le cloud. De plus, ADP est une solution de sécurité complète conçue pour protéger l'infrastructure DNS contre un large éventail de menaces, y compris les attaques DDoS, les malwares et l'exfiltration de données. Elle permet aux agences de préserver l'intégrité du DNS et de prévenir les attaques DDoS DNS externes et internes dans les environnements sur site, privés et publics sur le cloud.

Prise en charge du trafic DNS chiffré

- DNS-over-HTTPS (DoH) : ADP prend en charge le DoH, qui exécute le trafic DNS via HTTPS, en tirant parti de l'adoption généralisée et de la sécurité de HTTPS pour protéger les requêtes et réponses DNS.
- DNS-over-TLS (DoT) : ADP prend également en charge le DoT, qui utilise Transport Layer Security (TLS) pour chiffrer le trafic DNS. Ce protocole garantit que les communications DNS sont sécurisées et authentifiées.

Protection avancée contre les menaces

ADP fournit une Threat Intelligence avancée, une atténuation des menaces automatisée et une visibilité en temps réel sur le trafic DNS, garantissant ainsi l'intégrité et la disponibilité des services DNS.

- Surveille, détecte et bloque en permanence tous les types d'attaques DNS, y compris les attaques volumétriques et non volumétriques, telles que les exploits DNS et le détournement DNS, tout en répondant aux requêtes légitimes.
- Préserve l'intégrité du DNS, que les attaques de détournement de DNS peuvent compromettre.
- Infoblox ADP utilise la technologie Threat Adapt™ pour mettre à jour automatiquement la protection contre les menaces émergentes, en s'appuyant sur des analyses et des recherches indépendantes, tout en s'adaptant aux changements de configuration DNS.

Journalisation rapide des requêtes et des réponses

ADP inclut la journalisation des requêtes et des réponses DNS à haute vitesse, ce qui est essentiel pour capturer et analyser le trafic DNS en temps réel. Conçu pour être rapide et léger, il fournit une méthode rapide et flexible pour capturer et enregistrer le trafic DNS sans compromis significatifs en termes de performances.

- Contrairement à la journalisation intensive des requêtes et des réponses d'E/S, dnstap fonctionne de manière asynchrone, ce qui permet une journalisation des requêtes à grande vitesse avec une perte de performance minimale.
- Il utilise dnstap pour mettre en mémoire tampon les informations directement depuis le serveur DNS dans un format de journal structuré binaire flexible, puis transfère ces données vers un serveur récepteur.
- Les agences peuvent utiliser des outils de big data pour analyser ces données (et même les combiner avec d'autres sources) afin de dresser un tableau complet des schémas d'utilisation du réseau.

Scalabilité et fiabilité

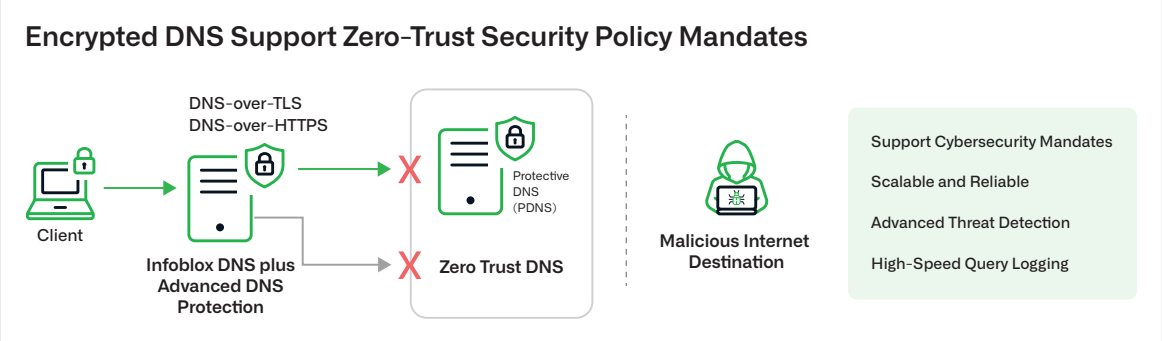
Les dernières appliances Infoblox Trinzic sont conçues pour offrir une évolutivité et une fiabilité exceptionnelles, ce qui les rend idéales pour les agences fédérales ayant des exigences réseau élevées.

- Conçues pour répondre aux exigences futures des réseaux, en tirant parti des dernières innovations d'Infoblox en matière de mise en réseau et de sécurité.
- Une amélioration de 50 % des performances en termes de requêtes DNS par seconde (QPS) et de baux DHCP par seconde (LPS) garantit une gestion efficace des volumes élevés de trafic DNS et DHCP.
- Plus facile à déployer et à gérer dans des architectures distribuées, elles garantissent la résilience et l'évolutivité du réseau.
- Inclut des fonctionnalités précédemment licenciées pour l'API Cloud Platform (CP) d'Infoblox, la prise en charge du pare-feu DNS (DFW) RPZ et l'équilibrage global de la charge des serveurs intégré au DNS Traffic Control (DTC).

Options de déploiement

- ADP est évolutif, facile à déployer et aide les agences à renforcer leur posture de cybersécurité en protégeant leur infrastructure DNS. Les agences peuvent déployer des serveurs DNS Infoblox avec la fonctionnalité ADP activée pour prendre en charge le trafic DNS chiffré.
- Ce déploiement peut être effectué sur site, sur le cloud ou dans un environnement hybride, offrant ainsi une flexibilité pour répondre à divers besoins opérationnels.

Pour plus d'informations sur la manière dont Infoblox peut aider votre organisation à implémenter un DNS crypté, contactez l'équipe Infoblox à l'adresse scsprogram@infobloxfederal.com ou leurs représentants de compte directement pour des informations supplémentaires.



APPEL À L'ACTION

Les agences fédérales sont invitées à donner la priorité à la sécurité DNS en adoptant Infoblox Advanced DNS Protection (ADP) suite au récent décret de la Maison-Blanche. Cette ordonnance impose l'utilisation de protocoles DNS chiffrés, reconnaissant le DNS comme un contrôle de sécurité de première ligne crucial. En mettant en œuvre ADP, les agences peuvent garantir la confidentialité et l'intégrité de leur trafic DNS, se protégeant ainsi contre les menaces potentielles de cybersécurité. Les solutions complètes et évolutives d'Infoblox prennent en charge le DNS-over-HTTPS et le DNS-over-TLS, rendant la transition vers un DNS chiffré transparente et efficace.

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

Version : 20250203v1