NOTE DE SYNTHÈSE

RÉSOUDRE DES DÉFIS INATTENDUS AVEC DOT ET DOH

RÉSUMÉ

La sécurisation de votre infrastructure DNS n'a jamais été aussi cruciale : plus de 90 % des incidents de malware et plus de la moitié des attaques de ransomware et de vol de données s'appuient sur le vecteur DNS.

La bonne nouvelle ? Deux technologies nouvelles et évolutives conçues pour améliorer la protection de la vie privée dans le domaine des DNS progressent de manière significative.

La mauvaise nouvelle ? Ces technologies orientent les serveurs et les applications vers des résolveurs DNS externes, ce qui permet aux appareils abonnés de contourner les mécanismes DNS classiques pour accéder à des services DNS échappant à votre contrôle et exposant l'entreprise à des risques potentiels en matière de sécurité. Ce sont là des problèmes qui sont en pleine réflexion.

Infoblox fournit aux organisations des solutions qui résolvent ces défis de confidentialité DNS. Grâce à la possibilité de bloquer l'accès aux résolveurs DNS externes et de fournir une résolution DNS interne cryptée, les organisations peuvent garder le contrôle sur le DNS.

POSSIBILITÉ D'AMÉLIORATION

Le concept d'ouverture est une caractéristique fondamentale de l'internet depuis sa création. Bien que les utilisateurs transmettent des informations sensibles telles que les numéros de carte de crédit, les adresses e-mail et les mots de passe entre leurs navigateurs web et les sites web à l'aide du protocole sécurisé HTTPS, les requêtes initiales pour les adresses Internet et les réponses ultérieures pour les emplacements des sites web sont transmises en texte clair. Par conséquent, le DNS a traditionnellement souffert de ce que nous décrivons comme un problème de sécurité du « dernier kilomètre ». Les communications entre un client DNS et son serveur DNS local sont presque toujours non cryptées et donc sujettes à l'usurpation d'identité, à l'interception, au détournement et à d'autres problèmes. Bien que des améliorations aient été apportées par le passé pour intégrer une plus grande sécurité de bout en bout, la dernière étape de la communication avec le navigateur web restait exposée à l'usurpation d'identité.

PRÉSENTATION DU DNS AND DOH

Des groupes industriels travaillant au sein de l'IETF (Internet Engineering Task Force) ont proposé deux systèmes pour résoudre ces problèmes. Ils fonctionnent en chiffrant la communication DNS entre le résolveur stub de votre système d'exploitation ou une application locale et votre résolveur DNS récursif. L'un est connu sous le nom de DNS over TLS (transport layer security) ou DoT, et l'autre sous le nom de DNS over HTTPS ou DoH. Bien que le DoT et le DoH aient été conçus pour résoudre les problèmes de confidentialité du DNS, ils introduisent également des modifications importantes du comportement du DNS dans la façon dont les navigateurs et les applications fonctionnent. Ces changements créent une complexité supplémentaire et des conséquences involontaires sur la sécurité du réseau et affectent directement la fourniture par les entreprises de services de sécurité et de filtrage de contenu. Les DoT et DoH peuvent orienter les serveurs et les applications vers des résolveurs DNS externes, ce qui permet aux appareils clients de contourner les mécanismes DNS classiques pour accéder à des services DNS échappant à votre contrôle et expose l'entreprise à des risques de sécurité potentiels. Un exemple concret : l'Agence nationale de sécurité des États-Unis (NSA) a récemment publié des recommandations recommandant aux organisations d'héberger leurs propres résolveurs DoH et d'éviter d'envoyer le trafic DNS interne vers des résolveurs tiers externes.

DNS OVER TLS (DOT)

Le DNS over TLS est une norme IETF qui utilise le protocole de contrôle de transfert (TCP) comme protocole de connexion pour superposer le chiffrement et l'authentification TLS entre un client DNS et un serveur DNS. Fonctionnant souvent au niveau du système d'exploitation, il communique via le port Protocole de contrôle de transfert 853. Ce port bien connu est utilisé pour tout le trafic DNS chiffré, et les administrateurs réseau le connaissent très bien. Le trafic DNS over TLS est chiffré, mais son utilisation d'un port bien connu facilite la surveillance et le contrôle du DNS chiffré par les administrateurs réseau lorsqu'il apparaît. DOT est également une norme mature soutenue par les acteurs classiques du secteur du DNS.

DNS OVER HTTPS (DOH)

Soutenu par Apple, Apple, Microsoft, the Mozilla Foundation et Chromium Projects, DoH est l'autre protocole de sécurité de l'IETF qui traite de la sécurité des communications entre le client DNS et le serveur DNS. Il utilise l'extension du protocole de sécurité HTTPS pour fournir le chiffrement et l'authentification entre un client DNS et un serveur.

Un problème potentiel avec le DoH est qu'il utilise le même port TCP (443) que tout le trafic HTTPS. Il pourrait s'avérer difficile de résoudre les problèmes DNS liés au DoH en raison de l'incapacité à distinguer les requêtes DNS basées sur DoH des requêtes HTTPS classiques. Par exemple, si un administrateur de réseau utilise la surveillance DNS pour bloquer les requêtes DNS vers des domaines malveillants connus, il ne verra pas ces requêtes en HTTPS. Ainsi, ce trafic malveillant passerait inaperçu.

De plus, le DoH est souvent implémenté au niveau de la couche applicative plutôt qu'au niveau du système d'exploitation, ce qui introduit la possibilité pour le trafic du navigateur de contourner les contrôles DNS de l'entreprise. Le contournement des contrôles DNS pourrait nuire à la capacité de l'équipe d'assistance à assurer les niveaux de performance, de sécurité, d'évolutivité et de fiabilité que les entreprises exigent du DNS.

DÉFIS LIÉS À DOT ET DOH EN ENTREPRISE

Les administrateurs de réseaux et de sécurité s'appuient sur le DNS en tant qu'élément important du plan de contrôle du réseau pour garantir un accès rapide aux applications et protéger les utilisateurs des malwares et autres menaces véhiculées par l'internet. Les nouvelles normes du DoT et du DoH peuvent poser des défis importants aux équipes chargées de la mise en réseau et de la sécurité :

- **DNS centralisé :** le contrôle externe du DNS peut permettre aux clients d'utiliser des résolveurs DNS centralisés contrôlés par des tiers et non fournis par le service informatique, ce qui présente des risques et complique la gestion et la sécurisation efficaces des ressources réseau.
- **Contournement des mesures de contrôle de l'entreprise :** le DoH introduit spécifiquement la possibilité pour des centaines d'applications et de sites web, chacun ayant ses propres paramètres DoH, de contourner les contrôles DNS. En plus de compliquer la surveillance des exploits des DNS tels que le détournement des DNS, le DoH pourrait également permettre de contourner les filtres de contenu des entreprises, tels que le contenu pour adultes, les jeux, le streaming et les sites avec des malwares.
- **Exposition à l'exfiltration de données et à la prolifération de malwares :** si non contrôlé, le DoH peut accroître l'exposition à l'exfiltration de données et à la prolifération de malwares car il peut ouvrir des portes dérobées vers des réseaux protégés. Les cybercriminels utilisent souvent le DNS comme porte dérobée pour obtenir et exporter des informations commerciales sensibles et pour diffuser des malwares via des communications de type C&C (commande et contrôle) avec des appareils. La requête DNS du DoH est chiffrée et, de ce fait, invisible pour les tiers, y compris les logiciels de cybersécurité qui peuvent s'appuyer sur la surveillance passive du DNS pour bloquer les requêtes vers des domaines malveillants connus. En règle générale, les équipes de sécurité peuvent bloquer efficacement ces attaques en utilisant des Threat Intelligence sur l'infrastructure DNS interne, associées à des analyses basées sur l'intelligence artificielle et l'apprentissage automatique. Comme le DoH contourne ces mesures de sécurité DNS, il y a un nouveau potentiel pour que les entreprises soient exposées à ces filtres DNS et à d'autres filtres basés sur le DNS.

  Par exemple, les versions récentes du malware PsiXBot utilisent le DoH pour chiffrer les communications malveillantes, ce qui lui permet de se dissimuler dans le trafic HTTPS normal et d'installer des malwares capables de voler des données ou d'ajouter une victime à un botnet.

- **Augmentation de la charge de travail du serveur DNS/diminution des performances du serveur DNS :** DoT et DoH augmentent la charge que chaque requête DNS impose au serveur, ce qui peut affecter la qualité d'expérience utilisateur. Le DNS traditionnel repose sur le protocole UDP (User Datagram Protocol) et génère un faible surcoût. En revanche, DoT et DoH fonctionnent sur TCP, plus gourmand en ressources pour le serveur DNS. De plus, DoT et DoH obligent le serveur DNS à déchiffrer la requête et à chiffrer la réponse, ce qui accroît encore la charge serveur. Les administrateurs doivent donc s'attendre à ce que leurs serveurs ne puissent gérer qu'une fraction du nombre de requêtes basées sur DoH et DoT comparé au DNS traditionnel.

NAVIGATEUR ET SYSTÈME D'EXPLOITATION DIFFÉRENTS

Plans de déploiement

De nombreux fournisseurs publics de DNS récursifs, tels que Google DNS, Cloudflare et Quad9, intègrent DoT et DoH à leurs services. De nombreux clients de systèmes d'exploitation doivent opter pour DoT (bien que de nombreux clients Android soient configurés pour utiliser DoT par défaut). Cependant, avec le DoH, les navigateurs web tels que Chromium et Mozilla nécessitent chacun leurs propres méthodes pour que les clients puissent satisfaire leurs besoins.

Chromium

L'implémentation du DoH par Chromium affecte tous les navigateurs basés sur le Chromium Project, y compris Google Chrome, Microsoft Edge et Opera. Chromium utilise par défaut un mode automatique qui interroge une liste de résolveurs configurés par le système d'exploitation pour vérifier la disponibilité du DoH, puis utilise le résolveur configuré pour le DoH uniquement s'il est disponible. Cela prévoit également de respecter les paramètres DoT du client OS sous Android et d'adopter un comportement prévisible et maîtrisable. Pour la plupart des clients Infoblox, les modifications de Chromium peuvent ne pas vous obliger à changer votre résolveur ou votre réseau.

Mozilla

Mozilla propose Cloudflare comme résolveur récursif de confiance par défaut utilisant le DoH. Mozilla tentera de détecter et de désactiver l'utilisation du DoH lorsqu'il le jugera nécessaire. Malheureusement, les méthodes utilisées dans le cadre d'une solution de repli gracieuse vers la résolution DNS classique n'ont pas encore fait leurs preuves et peuvent ne pas convenir à toutes les situations. Certaines entreprises peuvent ne pas avoir un contrôle total sur les navigateurs installés au sein de leur organisation. Par exemple :

Il peut s'avérer difficile de garantir le respect des préférences de l'entreprise concernant les paramètres du navigateur dans le cadre du BYOD, du télétravail et d'autres scénarios mobiles. De même, les fournisseurs de services de communication, avec leurs divers utilisateurs finaux, auront encore moins d'influence sur les paramètres du navigateur sur les appareils du réseau.

Apple

Les versions récemment publiées d'iOS et de macOS par Apple prennent en charge les protocoles DoT et DoH. Ces paramètres peuvent être appliqués de manière sélective, de l'ensemble du système d'exploitation aux applications individuelles ou aux requêtes réseau sélectionnées des applications, en passant par les profils MDM ou l'extension du réseau.

Selon Apple, il existe trois manières d'activer un DNS chiffré. L'une des options consiste à appliquer des paramètres DNS chiffrés à l'échelle du système, ce qui permet aux utilisateurs ou aux administrateurs de choisir un seul serveur DNS chiffré comme résolveur par défaut pour toutes les applications du système d'exploitation. Les développeurs peuvent écrire des applications d'extension de réseau qui configurent le système d'exploitation pour utiliser ce serveur, ou des profils MDM peuvent être transmis aux clients qui configurent les paramètres DNS cryptés. Si cette option n'est pas utilisée, les deux autres options sont automatiquement activées et le propriétaire de l'appareil ne peut pas les désactiver directement.

La deuxième option est destinée aux propriétaires de domaines. Vous pouvez configurer des paramètres au niveau du domaine qui signalent l'existence d'un résolveur chiffré pour le domaine. Si ces paramètres sont détectés et vérifiés, le trafic DNS pour ce domaine est redirigé vers le résolveur chiffré fourni par le domaine.

La dernière option est le DNS crypté au niveau de l'application. Ici, les développeurs peuvent créer des applications qui permettent aux applications d'utiliser DoT et DoH directement à partir d'applications individuelles. Cette option signifie que les développeurs peuvent choisir un serveur spécifique pour certaines ou toutes les connexions de leur application lorsque le système d'exploitation n'est pas configuré.

Apple prévoit d'avertir les utilisateurs par un message spécifique si un réseau particulier bloque les communications DNS cryptées sur le réseau conformément à sa politique. Les réseaux spécifiques seront visuellement marqués d'un avertissement de confidentialité, et les applications configurées pour utiliser des résolveurs DoH spécifiques ne fonctionneront pas correctement.

Microsoft

Microsoft a annoncé en 2019 son intention de prendre en charge DoH et l'a intégré au client DNS de Windows, avec une prise en charge de DoT envisagée dans de futures versions. Microsoft a conçu son approche en partant du principe que les utilisateurs ne devraient pas avoir besoin de connaissances spécialisées pour utiliser le DoH, tout en permettant aux administrateurs réseau de garder le contrôle en autorisant un retour au protocole DNS classique.

Une fois configuré, le client DNS fonctionnera en « mode opportuniste », ce qui signifie qu'il tentera d'utiliser le protocole DoH au lieu du DNS classique. Toutefois, le client peut être configuré pour revenir au DNS conventionnel si les protocoles DoH ne sont pas disponibles ou ne répondent pas. Les résolveurs de confiance DoH initiaux seraient Cloudflare, Google et Quad9.

INFOBLOX RÉSOUT LES DÉFIS POSÉS PAR DOT ET DOH

En tant que leader du secteur des services réseau sécurisés et gérés sur le cloud, Infoblox soutient que le contournement de l'infrastructure DNS interne existante renforce la complexité opérationnelle. Ces nouvelles options de confidentialité DNS ne font que commencer. Les organisations devraient prendre des mesures dès maintenant pour réduire les risques que posent ces technologies. Un excellent point de départ consiste à bloquer le trafic DNS direct (y compris DoT et DoH) entre les adresses IP internes et les serveurs DNS sur Internet (figure 1). Cette mesure garantira que les utilisateurs finaux utilisent l'infrastructure DNS interne de leur entreprise, ce qui permettra à leur service informatique d'appliquer une politique de résolution DNS complète et de résoudre les problèmes. Infoblox fournit aux organisations des solutions qui résolvent ces défis de confidentialité DNS. Grâce à la possibilité de bloquer l'accès aux résolveurs DNS externes et de fournir une résolution DNS interne cryptée, les organisations peuvent garder le contrôle sur le DNS.

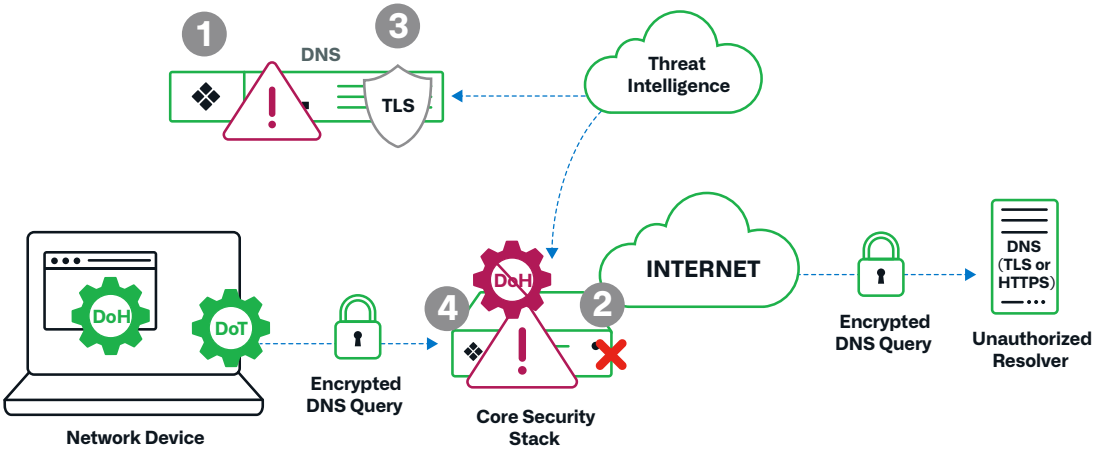

Figure 1 : les meilleures pratiques DoT/DoH protègent vos utilisateurs et vos appareils

Bloquez la résolution vers les domaines DoH

BloxOne® Threat Defense, une solution de sécurité hybride fondamentale d'Infoblox, utilise le DNS comme première ligne de défense. Elle bloque la résolution des domaines DoH et facilite un retour en douceur vers le DNS interne existant. Ces fonctionnalités aident à prévenir l'utilisation abusive du DoH et à atténuer les risques.

BloxOne Threat Defense inclut plusieurs fonctionnalités pour vous aider à gérer DoH :

- Les flux de threat intelligence pour le DoH fournissent aux administrateurs de réseau la possibilité de contrôler la méthode d'accès au DNS utilisée pour détecter et atténuer les menaces en désactivant les politiques de sécurité basées sur le DoH. Les navigateurs reviendront automatiquement au DNS géré par l'organisation sans interrompre l'activité des utilisateurs.
- Un flux de politiques DoH pour les adresses IP et les domaines DoH connus a été ajouté à Threat Intelligence Data Exchange, la plateforme d'agrégation et de distribution de threat intelligence d'Infoblox. D'autres outils de sécurité, tels que les NGFW, peuvent ensuite utiliser ce flux de données et les renseignements connexes pour bloquer le trafic DoH vers des serveurs externes.
- Les utilisateurs peuvent examiner les domaines et les adresses IP liés au DoH dans Dossier, l'outil d'investigation des menaces d'Infoblox.

Ces fonctionnalités sont disponibles pour tous les niveaux d'abonnement de BloxOne Threat Defense.

DNS chiffré Infoblox

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 est une fonctionnalité NIOS qui offre un chiffrement efficace tout en fournissant les services DNS de premier ordre d'Infoblox. Les capacités de lancement incluent la prise en charge du DOH et DoT

Infoblox Encrypted DNS offre une approche unique pour chiffrer votre trafic DNS. Contrairement aux méthodes qui font appel à des équilibreurs de charge ou à un surprovisionnement, Infoblox Encrypted DNS fonctionne comme un service unique pour tous vos besoins en DNS. Nos fonctionnalités standard, y compris la protection DNS avancée et l'optimisation du cache DNS, sont toutes disponibles via le même service DNS hautement évolutif.

CONCLUSION

Infoblox s'engage à aider ses clients à maintenir la performance, la sécurité, l'échelle et la fiabilité des réseaux d'entreprise modernes. Ces changements se produisent en ce moment même, car les récentes mises à jour des navigateurs et les versions des systèmes d'exploitation les déploient aujourd'hui sur les réseaux. Si la résolution du problème du « dernier kilomètre » est essentielle et utile, nous reconnaissons également que les entreprises doivent conserver la visibilité et le contrôle de leur trafic DNS. D'éminentes agences de sécurité, dont la NSA, recommandent aux organisations de prendre des mesures pour réduire les risques posés par ces technologies. Les clients peuvent s'appuyer sur les solutions Infoblox pour garder le contrôle de leur DNS et atténuer les problèmes imprévus en aval des nouvelles initiatives en matière de confidentialité du DNS. Pour plus d'informations, consultez la communauté Infoblox pour en savoir plus sur ces technologies en évolution et sur les solutions Infoblox.

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

+1.408.986.4000
www.infoblox.com/fr

Version : 20230919v1