

DNS Guardian

Protégez vos données et assurez la continuité des services DNS

Points Forts:

- Détection, protection et résolution d'incidents pour les fonctions DNS cache, récursives et d'autorité
- Inspection des transactions DNS en temps réel pour des analyses détaillées
- Détection comportementale des menaces pour des décisions mieux adaptées
- Filtrage granulaire de domaine par utilisateur pour un contrôle d'accès renforcé aux applications
- Des contre-mesures de sécurité adaptables pour une continuité de service optimale
- Gestion centralisée des polices de sécurité DNS sur l'ensemble du réseau
- Des statistiques DNS élaborées pour un reporting plus intelligent
- Intégration à Cisco Umbrella pour la protection des applis, des données et des utilisateurs sur/hors réseau

Le service DNS est un composant réseau critique, ce qui n'a pas échappé aux pirates. Ces dernières années, une nette augmentation des attaques ciblant les serveurs DNS a été observée (comme le souligne l'enquête sur les menaces DNS menée en 2020 par EfficientIP). La nature des menaces sur le DNS évolue rapidement, et les attaques deviennent de plus en plus sophistiquées, s'appuyant sur des modèles distribués, impliquant différents vecteurs et différentes étapes. Les solutions de protection DNS classiques se révèlent inadaptées ; plus grave encore, le risque qu'elles bloquent les requêtes légitimes est très élevé. En conséquence, il est nécessaire d'adopter une nouvelle approche de la sécurité si l'on souhaite prévenir les interruptions de service réseau et les éventuels vols de données préjudiciables aux organisations.

Fruit d'innovations technologiques majeures, DNS Guardian d'EfficientIP est la première solution de sécurité DNS offrant une inspection complète des transactions DNS et des analyses poussées pour une détection comportementale en temps réel des menaces. Des contre-mesures intelligentes et brevetées procurent une sécurité adaptative pour protéger plus efficacement la confidentialité des données et garantir une continuité des services DNS sans précédent, même en cas d'attaques les plus insidieuses.

Une infrastructure de sécurité renforcée

DNS Guardian s'appuie sur une architecture innovante qui sépare les fonctions cache et récursives, ainsi que d'autorité, permettant de renforcer considérablement la sécurité du service dans son ensemble. En cas d'attaque, chaque fonction est protégée séparément pour ce qui concerne ses propriétés spécifiques, évitant les effets latéraux et garantissant la disponibilité des services. Les contre-mesures brevetées de DNS Guardian peuvent être adaptées aux besoins spécifiques de chaque fonction et au type d'attaque détecté, pour une protection à l'efficacité inégalée.

Technologie d'inspection des transactions DNS

DNS Guardian est la première et l'unique solution du marché offrant l'inspection des transactions DNS (DTI: Deep Transaction Inspection) en temps réel et sans impact sur les performances. DNS Guardian examine, au cœur même du protocole, les séquences d'échanges de requêtes pour chaque transaction DNS :

- Fragments, requêtes et leur charge et réponses spécifiques
- Durée et taille des transactions

La méthode innovante d'inspection des transactions de DNS Guardian permet une compréhension complète du contexte du client, dépassant les limitations des systèmes de sécurité basés sur les signatures, qui n'offrent qu'une visibilité limitée du trafic. Cela est essentiel pour offrir de vraies capacités d'analyse et de détection comportementale des menaces.

Identification avancée des utilisateurs

DNS Guardian analyse en profondeur le comportement des clients, afin d'appliquer chaque fois que nécessaire les contre-mesures appropriées. Une identification client standard s'appuie sur l'adresse IP source de la requête DNS ; cependant, les topologies complexes imposent d'identifier le client au moyen d'autres paramètres. DNS Guardian peut s'appuyer sur les options EDNS comme source d'identification plutôt que sur l'adresse IP. Cela autorise des fonctionnalités telles que le contrôle parental, le CG-NAT pour les réseaux télécom, ou encore le « cascading » des requêtes DNS provenant d'un autre transitaire.

Proxy DNS transparent

Dans certaines situations, il est nécessaire d'intercepter les requêtes DNS adressées à des serveurs spécifiques, afin de bénéficier de services tels que le filtrage, la comptabilité ou l'analyse du trafic. DNS Guardian peut être configuré pour prendre en compte ce trafic, et être exploité en tant que proxy transparent. Dans ce cas, toute requête parvenant à DNS Guardian est analysée à l'aide de fonctionnalités de sécurité standard, puis transférée vers sa destination initiale ; la réponse est transmise au client dès réception. Cette solution est idéale pour le filtrage RPZ ou l'analyse en profondeur du trafic client, de manière à filtrer ou à placer en quarantaine les IPs malveillantes.

Gestion centralisée des polices de sécurité

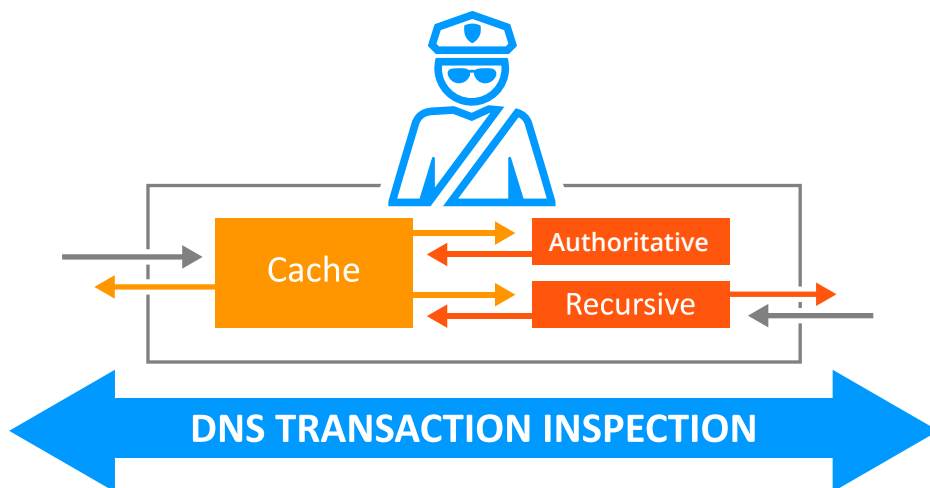
Les polices globales de sécurité à appliquer à de multiples appliances DNS Guardian peuvent être définies depuis une interface centrale. Ces polices appliqueront les paramètres de détection des menaces et de défense sur l'ensemble du réseau, pour une gestion unifiée des mécanismes de sécurité qui s'appuient et sécurisent les composants DNS. Cette capacité d'agir simultanément sur un groupe de serveurs permet de réduire les coûts d'administration et d'ajuster finement les seuils.

Des analyses en profondeur pour une détection comportementale des menaces

Visibilité en profondeur du trafic DNS

Les capacités d'inspection transactionnelle de DNS Guardian (DTI) procurent une visibilité en profondeur et une connaissance précise du trafic DNS sur la durée. DNS Guardian collecte, regroupe et enregistre en temps réel les statistiques les plus affinées, par client ou dans leur globalité :

- Hit/Miss Ratio du cache, requêtes mal formées, fragmentation, délai de récursivité, distribution des codes retour, latence
- Consommation de bande passante DNS
- Tête de liste : Clients, domaines demandés, code de retour (Nxdomain, SERVFAIL...), type de requête



L'infrastructure de sécurité innovante de DNS Guardian

Analyses multifactorielles des menaces

Cette visibilité sans précédent, couplée à des analyses multifactorielles (tendances globales, comportement des clients et performances des fonctions DNS) et en temps réel du trafic, garantissent une détection comportementale des menaces, s'appuyant sur les capacités d'analyse DNS les plus sophistiquées.

DNS Guardian étend la détection des menaces bien au-delà des schémas d'attaques connus et des mécanismes de listes noires rapidement obsolètes, permettant l'identification des attaques les plus élaborées telles que le tunneling DNS, ainsi que les attaques insidieuses ou par injections lentes.

DNS Guardian protège des attaques suivantes :

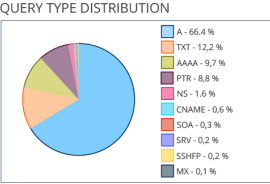
Requêtes invalides - DNS Guardian analyse les requêtes DNS, et rejette celles qui ne sont pas conformes au(x) RFC(s) concernés, avant qu'elles atteignent le moteur DNS récursif

- Attaques NXDOMAIN - DNS Guardian analyse la proportion de réponses nxdomain par adresse IP source. Cela permet une détection et une protection plus efficaces que toute approche basée sur les motifs d'expressions régulières, dégradant les performances du moteur DNS
- Attaques de sous-domaines aléatoires et de domaines fantômes - DNS Guardian analyse la proportion de réponses nxdomain et servfail par adresse IP source. Cela permet une détection et une protection plus efficaces que toute approche basée sur les motifs d'expressions régulières, dégradant les performances du moteur DNS
- Attaques par injections lentes - DNS Guardian analyse les temps d'attente des réponses DNS provenant de tout serveur de nom de domaine aux requêtes des clients. Cela permet l'identification et l'isolation rapides de tout client générant des requêtes ciblant un serveur de nom de domaine malveillant, conçu pour saturer le moteur récursif avec des réponses trop lentes
- Attaques par tunneling DNS - DNS Guardian analyse les requêtes hors cache DNS ainsi que leur taille. Cela permet une détection et une prévention du tunneling DNS bien plus efficaces qu'une approche basée sur la reconnaissance de motifs s'appuyant sur une base de données potentiellement obsolète
- Attaques par empoisonnement du cache - La prise en charge des cookies DNS EDNS et la randomisation du port source des requêtes, associée à un mot aléatoire chiffré sur 16 bits, réduit considérablement les chances de réussite de ce type d'attaques. Cependant, seule la prise en charge de DNSSEC garantit la validité des réponses fournies par les zones signées
- Attaques réflexives distribuées - DNS Guardian analyse les requêtes par adresse IP source. Cela permet de prévenir toute exploitation de votre infrastructure en tant que vecteur réflexif d'une attaque. (Remarque : le moyen le plus sûr de prévenir ce type d'attaques est encore d'éviter le spoofing d'adresses IP au sein d'un réseau)
- Flooding DNS - L'analyse des performances globales du trafic DNS permet l'isolation des clients suspects ou l'activation du mode Rescue, assurant la disponibilité du cache même en cas d'attaques virulentes

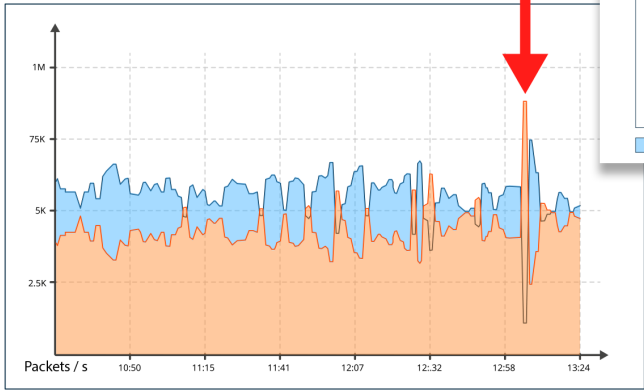
Display Top 50 Domains
☐ Automatic refresh

Domain	Total Queries	Number of hits	Ratio ▲
google.com	1275907	144621	11.3 %
facebook.com	1275907	140427	11 %
googleapis.com	1275907	85372	6.7 %
apple.com	1275907	74892	5.9 %
fbcdn.net	1275907	35118	2.8 %
akadns.net	1275907	27075	2.1 %
outlook.com	1275907	17714	1.4 %
doubleclick.net	1275907	17630	1.4 %
snapchat.com	1275907	16962	1.3 %
akamaiedge.net	1275907	16865	1.3 %
icloud.com	1275907	15453	1.2 %
apple-dns.net	1275907	15863	1.2 %
instagram.com	1275907	13662	1.1 %
gstatic.com	1275907	14214	1.1 %
crashlytics.com	1275907	12865	1 %
google.fr	1275907	13115	1 %
whatsapp.net	1275907	11069	0.9 %
amazonaws.com	1275907	11783	0.9 %
microsoft.com	1275907	10555	0.8 %
dail-once.com	1275907	8311	0.7 %
yahoo.com	1275907		
gipals.com	1275907		
google-analytics.com	1275907		
skype.com	1275907		
admxs.com	1275907		
ntp.org	1275907		
golesyndication.com	1275907		
googleadservices.com	1275907		
cloudfront.net	1275907		
appspot.com	1275907		
akamai.net	1275907		
googlevideo.com	1275907		
ksmobile.com	1275907		
live.com	1275907		
orange.fr	1275907		
youtube.com	1275907		
bing.com	1275907		
googleusercontent.com	1275907		
gmail.com	1275907		
snapsads.com	1275907		
flurry.com	1275907		
edgekey.net	1275907		
presage.com	1275907		
viber.com	1275907		
sumologic.com	1275907		
symcb.com	1275907		
ampproject.org	1275907		
xiti.com	1275907		
twitter.com	1275907		
criteo.com	1275907		

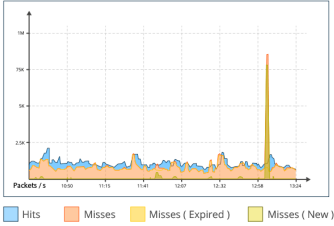
ATTACK



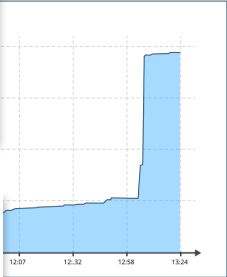
CACHE HIT RATIO



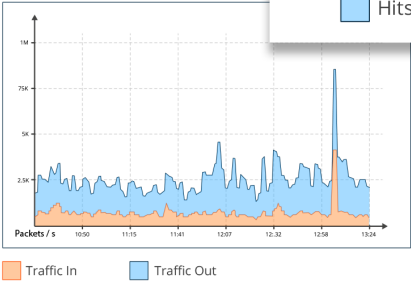
CACHE STATISTICS



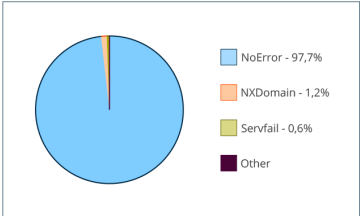
CACHE SIZE



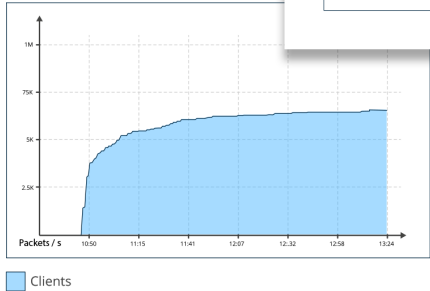
DNS TRAFFIC (Bytes)



RCODE DISTRIBUTION



TRAFFIC CLIENTS



Des contre-mesures intelligentes pour une sécurité adaptative

Les capacités d'analyse de DNS Guardian permettent une compréhension sans précédent des menaces DNS, et offrent la possibilité d'activer au bon moment les contre-mesures appropriées, selon le type d'attaque. Cette solution de sécurité adaptative et unique offre des contre-mesures intelligentes pour protéger à la fois la disponibilité des services et la confidentialité des données :

- Blocage des adresses IP sources des attaques
- Limitation du trafic DNS par IP source
- Mise en quarantaine des IP sources suspectes (breveté)
- Activation du mode Rescue : assure la continuité des services même si la source de l'attaque n'est pas identifiable (breveté)

Le mode Quarantaine isole les adresses IP aux comportements suspects, de sorte qu'elles n'ont accès qu'aux données en cache, tandis que leurs requêtes récursives sont bloquées. Cela préserve le serveur de l'attaque et réduit le risque de blocage des requêtes légitimes.

Dans des circonstances extrêmes, cependant, lorsque la source de l'attaque ne peut être identifiée (typiquement dans le cas d'une attaque par injection lente ou hautement distribuée), DNS Guardian détecte le risque d'épuisement des capacités du serveur et active le mode Rescue breveté. Cette contre-mesure unique garantit que les réponses DNS en cache restent pleinement disponibles pour les clients, même si la mise à jour de la validité des données est impossible, ce qui permet de maintenir une accessibilité totale aux applications et services critiques.



Actions de DNS Guardian

Protection contre les pannes de serveurs en amont

En cas de panne du système DNS en amont, ou de l'impossibilité d'y accéder, par exemple à cause d'une défaillance de la dorsale, un moteur DNS récursif pourra ne plus être en mesure de répondre aux requêtes récursives des clients. De ce fait, les clients ne peuvent plus accéder à des services qui sont peut-être encore accessibles et exploitables. La capacité d'adaptation de DNS Guardian permet d'empêcher cela. Lorsque se présente une requête pour un domaine présent en cache mais dont le délai a expiré, DNS Guardian ignore l'échec du moteur récursif local et répond au client en utilisant la réponse stockée en cache dont la valeur TTL est faible (30 secondes). La continuité du service est ainsi assurée en cas de panne de courte durée des serveurs en amont, comme c'est le cas avec le mode Rescue.

Renforcer le contrôle d'accès aux applications

La sécurité est un sujet important dans la gestion du trafic DNS. La solution Guardian met en œuvre un pare-feu DNS qui filtre les requêtes des clients au regard d'une liste de domaines devant être soit rejetés soit autorisés, selon la stratégie adoptée (approche de Whitelist ou de Blacklist). La fonction de pare-feu peut servir à différentes fins, allant de la protection des appareils et des utilisateurs contre les applications malveillantes à l'autorisation de certaines applications approuvées et spécifiques aux objets de l'IoT, aux périphériques partagés ou encore aux équipements industriels.

Outre la fonction de pare-feu axée principalement sur la destination du trafic des applications, DNS Guardian met en œuvre une approche orientée client avec la solution CQF (Client Query Filtering), qui contribue à réduire le risque d'exposition par l'ajout d'une barrière de sécurité contrôlant l'accès aux applications au point le plus précoce du flux. Avec CQF, il est possible d'appliquer des listes de filtrage granulaires supplémentaires au pare-feu pour un groupe de clients ou d'appareils. En combinant les listes de clients et de domaines à autoriser ou à rejeter, le nombre de cas potentiels d'utilisation augmente de façon significative. La nature dynamique des listes utilisées dans CQF permet de concevoir des scénarios dans lesquels les clients peuvent être ajoutés ou supprimés à la volée, de même que les domaines listés dans le pare-feu DNS. Ces mises à jour dynamiques offrent un renforcement immédiat de la sécurité du réseau. Cela permet une approche globale de la sécurité au sein de l'écosystème, avec davantage de points de contrôle entre le client et son application en associant le DNS à d'autres solutions classiques de pare-feu et de filtrage IP.

Confort d'utilisation accru

Des performances de cache sans équivalent

DNS Guardian intègre un système de cache DNS qui améliore significativement les performances de résolution du cache. Associé aux appliances SOLIDserver™ Blast, DNS Guardian est capable de résoudre jusqu'à 17 millions de requêtes par seconde.

Partage du cache multicast

Le partage du cache de DNS Guardian améliore les performances de la plateforme DNS dans son ensemble, en réduisant le nombre de requêtes récursives envoyées aux serveurs d'autorité et en minimisant la latence du service DNS. DNS Guardian s'appuie sur un mécanisme de multicast IP pour optimiser les performances. En association avec le mode Rescue et les mécanismes de sécurité de DNS Guardian, cela permet le déploiement de plateformes DNS récursives collaboratives et distribuées d'une très grande fiabilité, renforçant la sécurité globale de l'infrastructure.

Persistance du cache (Restart & Restore)

DNS Guardian permet de sauvegarder le cache. Les données présentes en cache peuvent ainsi être exploitées au redémarrage, pour des performances de résolution DNS immédiates. Cela évite au moteur DNS d'avoir à résoudre des requêtes récursives jusqu'à ce que son cache soit reconstruit, ce qui pourrait entraîner une charge excessive et dégrader considérablement les performances du service.

Chiffrement du trafic DNS local

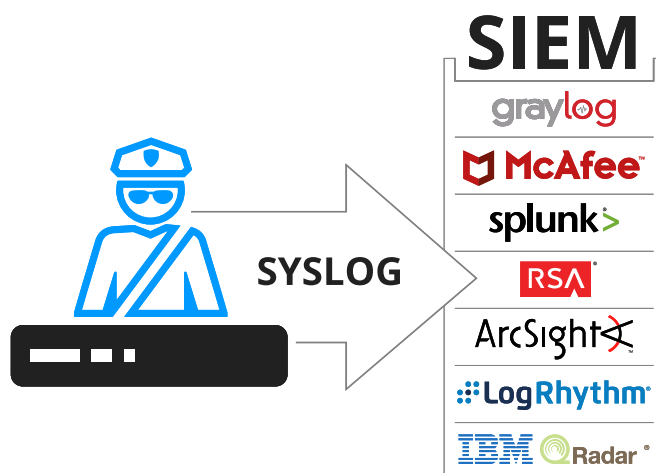
DNS Guardian permet de protéger le trafic utilisateur par le chiffrement en autorisant le DoT (DNS over TLS). Cette méthode d'accès vient en complément de DNS over UDP et de DNS over TCP, dans lesquels les requêtes circulent en clair sur le réseau. Dans le cas de DNS over TLS, le trafic est chiffré et l'accès peut être protégé au moyen de certificats numériques afin d'empêcher l'analyse après capture des requêtes DNS. Outre le DoT, le protocole de tunneling DoH (DNS over HTTPS) est également pris en charge, afin d'offrir au client une sécurité de navigation basée sur une norme éprouvée.

Centralisation performante de la journalisation

Service réseau essentiel, DNS constitue également une source de données précieuses à exploiter dans le cadre de la sécurisation du réseau. Le monitoring de DNS doit faire partie intégrante de la stratégie de sécurité, et la traçabilité de l'activité DNS est critique pour l'analyse des incidents. Cette surveillance permet la détection et la compréhension d'activités criminelles telles que la propagation de logiciels malveillants, les campagnes de phishing ou de toute attaque ayant pu compromettre le système d'information.

DNS Guardian intègre un système de journalisation unique et très efficace, qui ne dégrade pas les performances DNS. La journalisation asynchrone garantit une visibilité détaillée et en continu de l'historique des transactions même en cas d'attaques volumétriques, surpassant les limitations des services DNS classiques. La prise en charge du format standard Syslog permet l'interopérabilité avec les systèmes de journalisation existants. Les implémentations peuvent s'appuyer sur des solutions SIEM tierces telles que Splunk, Graylog ou ELK pour collecter et analyser l'énorme quantité de données archivées, et élaborer des rapports détaillés d'analyse du trafic.

DNS Guardian est un composant de la solution de sécurité EfficientIP à 360°, conçue pour protéger les infrastructures DNS publiques et privées à la fois des menaces internes et externes, quel que soit le type d'attaque.



High Performance Logging Technology



As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Copyright © 2021 EfficientIP, SAS. All rights reserved. EfficientIP and SOLIDserver logo are trademarks or registered trademarks of EfficientIP SAS. All registered trademarks are property of their respective owners. EfficientIP assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document.

REV: C-210128