efficient iP™
DEFINING SMART DDI

Datasheet

DNS FIREWALL

Protection et défense de l'infrastructure réseau contre les malware

Le DNS est un service critique du réseau, qui permet l'accès à pratiquement n'importe quel service connecté. Par nature, il s'agit d'un service ouvert à tous les hôtes d'un réseau, afin d'assurer la connectivité à tout service intranet ou internet. Ce rôle à la fois central et critique des services DNS a été clairement identifié par les pirates, pour lesquels le DNS est devenu un vecteur d'attaque privilégié, servant à contrôler nombre de malware et à piloter les attaques furtives de type APT (91% selon le rapport 2016 de Cisco sur la sécurité).

Dans l'environnement actuel en évolution constante, où les périphériques mobiles et les objets de l'IoT prolifèrent et où le BYOD s'est banalisé, le module DNS Firewall d'EfficientIP procure une couche de défense dédiée, capable de combler les lacunes des solutions classiques de sécurité et d'offrir une protection contre les menaces DNS.

DNS Firewall offre des capacités élaborées de filtrage des flux DNS, à partir de bases de signatures mises à jour dynamiquement permettant l'identification rapide des activités suspectes sur le réseau. Il est ainsi possible de prévenir l'infection et la contamination du réseau par tout type de malware, de bloquer les tentatives de phishing ou encore d'exfiltration de données confidentielles.

Points Forts:

- Blocage actif du trafic DNS vers des destinations frauduleuses
- Veille automatisée de la connaissance des menaces afin d'adapter la protection à l'évolution constante des risques
- Protection proactive contre les malware
- Prévention du phishing
- Limitation des risques d'exfiltration des données
- Identification et localisation des hôtes infectés

DNS RPZ

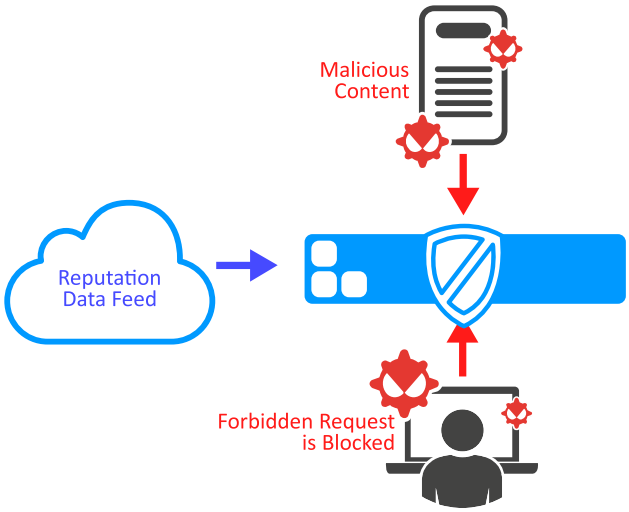
DNS RPZ (Domain Name Service Response Policy Zones) est un mécanisme implémenté dans tous les moteurs DNS récursifs modernes. Ce mécanisme permet la modification dynamique des réponses DNS obtenues du système DNS global, et fournit des réponses alternatives à toute requête DNS. Intégré à DNS Firewall, il permet aux administrateurs de définir avec précision les règles de filtrage et de redirection appliquées au trafic DNS selon :

- Le nom de domaine demandé
- Le serveur de noms (NameServer) demandé
- L'adresse IP, obtenue par résolution de la requête DNS

Cela permet l'application de différentes stratégies selon le type de trafic :

- Redirection vers un autre CNAME ou adresse IP
- Réponse avec domaine non existant (NXDOMAIN)
- Réponse avec absence de données (NODATA)
- « Force TCP »
- « Passthrough »
- « Drop »

La solution DNS Firewall d'EfficientIP procure une couche de sécurité supplémentaire à un système de sécurité réseau existant. Ce dernier est nécessairement limité en termes de filtrage des accès dès lors qu'il doit traiter autre chose que des adresses IP ou des caractéristiques statiques telles que des protocoles ou des ports. Cependant, si les pare-feu NG (Next-Generation) intègrent des fonctionnalités élaborées, ils sont malheureusement limités en termes de performances, devant traiter des quantités considérables de requêtes hétérogènes. A contrario, DNS Firewall est spécialisé dans la prévention de tout processus de résolution d'adresse IP pour les domaines frauduleux connus, et bloque toute connexion aux adresses IP associées.



Veille de connaissance des risques

La meilleure façon de protéger une infrastructure réseau et ses utilisateurs des risques liés au phishing et aux malware est d'empêcher toute connexion vers les services frauduleux connus, exploités par les pirates dans le but de dérober des identifiants ou d'amorcer la charge virale initiale d'un malware. Il est cependant difficile de maintenir des règles de filtrage appropriées concernant les domaines malveillants connus, à cause de la nature dynamique des menaces. Les pirates exploitent habituellement plusieurs domaines, souvent générés de façon aléatoire, pour contrôler leurs botnets, et s'appuient sur l'énorme quantité de serveurs faiblement sécurisés pour mener leurs attaques. La solution la plus pérenne consiste à s'appuyer sur un référentiel de règles de filtrage, mis à jour de façon dynamique, et pouvant être étendu via une stratégie de filtrage personnalisé.

DNS Firewall de SOLIDserver™ intègre ce type de flux dynamique de données, élaboré à partir de différentes sources distribuées. Il recoupe les rapports tels que ceux de MailSecurity, PhishTank, OITC et PhishLabs, concernant l'activité en provenance d'adresses IP ou de domaines suspects. Les listes fournies permettent différentes combinaisons de filtrage basées sur les catégories suivantes :

- Fraude et spam
- Phishing
- Malware
- Sites web piratés

Une protection proactive et efficace contre l'usage malveillant des services DNS

Prévention du phishing

Les pirates s'appuient sur des méthodes dites de phishing (hameçonnage) pour attirer les utilisateurs vers un service web frauduleux, ou les inciter à télécharger un logiciel malveillant, dans le but d'obtenir des informations sensibles. Grâce aux services de veille des connaissances des menaces, DNS Firewall de SOLIDserver™ bloque automatiquement l'accès des utilisateurs aux services web frauduleux, même si ces utilisateurs se servent de leurs propres appareils au sein du réseau de l'entreprise. Cela réduit considérablement les risques de détournement des utilisateurs vers des applications malveillantes, et donc de vol de leurs identifiants.

Contrer la propagation des malware et l'exfiltration des données

L'objectif des logiciels malveillants est de perturber l'exploitation des systèmes, de collecter des informations sensibles, d'obtenir l'accès à des infrastructures privées, de rançonner les utilisateurs, ou encore d'afficher du contenu non sollicité. Dès lors qu'un système se connecte à internet, il s'expose aux risques associés à des logiciels malveillants. Compte tenu du contexte actuel en termes de menaces, et de l'augmentation constante des actes de piratage, la prévention de la propagation des malware sur le réseau constitue une priorité absolue.

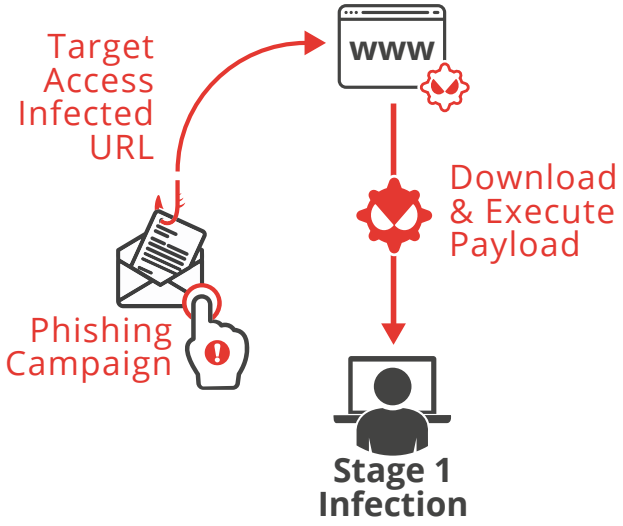
Les solutions de sécurité existantes couvrent une grande variété de vecteurs d'attaques possibles, tels que :

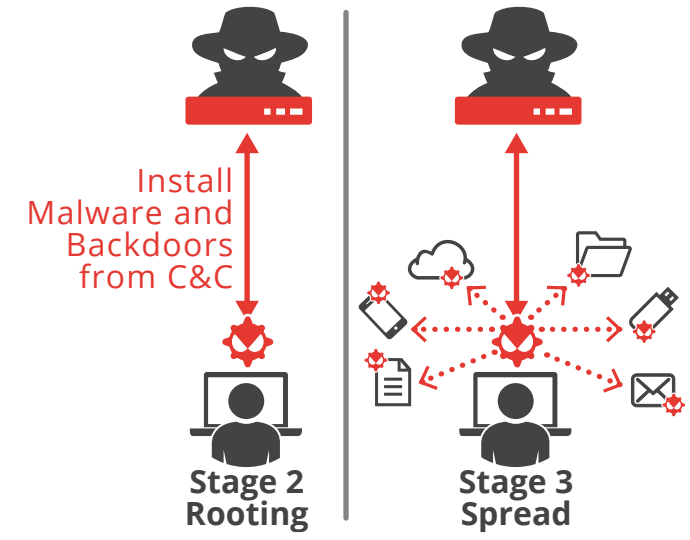
- Les tentatives de piratage via le courrier électronique, généralement contrées par les filtres anti-spam
- Les tentatives de piratage via des pages web ou des téléchargements, généralement contrées par les anti-virus installés sur les passerelles internet
- Les tentatives d'infection via le partage de fichiers, généralement contrées par les anti-virus installés localement

Il manque cependant à ces solutions la capacité d'identifier des menaces provenant des hôtes non sécurisés du réseau, ou des attaques spécifiquement élaborées qui ne correspondent à aucun motif connu. DNS Firewall de SOLIDserver™ empêche l'infection initiale d'un hôte en bloquant les requêtes susceptibles de rediriger l'utilisateur vers des adresses IP ou des domaines identifiés comme frauduleux, indépendamment du motif du trafic.

Il réduit également les capacités offensives des malware qui auraient déjà infecté un hôte « connecté mais mobile », tel qu'un laptop, une tablette ou un smartphone.

Il y parvient en bloquant les communications avec les serveurs dits de « Command & Control », empêchant ainsi les mises à jour des malware, le contrôle à distance, ainsi que la plupart des tentatives d'exfiltration de données.





Une protection encore plus complète peut être obtenue en associant DNS Firewall à DNS Guardian. Ce dernier s'appuie sur l'inspection du trafic DNS en temps réel et sur la détection des comportements suspects, et déclenche automatiquement, si nécessaire, des contre-mesures adaptées. Cela permet de contrer les techniques de tunneling DNS les plus sophistiquées, et de protéger de façon proactive les moteurs DNS récursifs contre tous types d'attaques, sécurisant ainsi l'accessibilité de toutes les applications du système d'information.

Identification des hôtes infectés

Contenir une infection ne se limite pas à bloquer le trafic et à isoler le ou les hôtes contagieux. Une intervention rapide sur l'hôte contaminé est également nécessaire afin d'analyser et de traiter l'infection.

En s'appuyant sur des procédures de journalisation appropriées, DNS Firewall permet l'identification rapide de toute adresse IP à l'origine des requêtes suspectes détectées. Ces capacités, associées à une solution IPAM et à ses outils de découverte réseau, permettent la localisation rapide des hôtes infectés afin de procéder immédiatement au traitement approprié.

Reporting avancé des menaces

Associer les capacités de journalisation de SOLIDserver™ à un gestionnaire d'événements (ou SIEM, pour Security Information and Event Manager) permet l'exportation aisée des journaux de DNS Firewall au format Syslog standard. Cela permet ensuite de procéder à des analyses poussées du trafic DNS suspect, et de générer des rapports appropriés à l'aide soit de modèles personnalisés, soit de plugins compatibles avec la solution déployée (par exemple Splunk ou Graylog).

DNS Firewall est un composant de la solution de sécurité unique 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.

efficient iP™

REV: B-1708

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.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
101C Telok Ayer Street #04-00
SINGAPORE 068574
+65 6678 7752