URL FILTERING

Des accès au web en toute sécurité, pour tous les utilisateurs

URL Filtering a pour mission de sécuriser les accès au web. Basé dans le cloud, ce service s'appuie sur le machine learning et des analyses statiques pour identifier et bloquer automatiquement les sites malveillants et les pages de phishing. Composant natif de la Palo Alto Networks Security Operating Platform, URL Filtering assure une sécurité web hors-pair, avec l'appui de politiques simples à définir et basées sur les applications et les utilisateurs.

URL Filtering

- Exploite une combinaison unique d'analyses statiques et de fonctions de machine learning pour protéger votre entreprise des sites malveillants, respecter ses obligations de conformité et veiller à des pratiques d'utilisation acceptable.
- Classifie et bloque immédiatement les URL malveillantes grâce à un moteur de catégorisation puissant, alimenté par la Threat Intelligence du service WildFire de prévention des malwares et de notre équipe de recherche Unit 42.
- Intègre un contrôle web granulaire à la politique de votre pare-feu nouvelle génération, y compris un déclenchement automatique de certaines mesures de sécurité avancées (par ex. le déchiffrement SSL sélectif sur les sites suspects).

Sécuriser les accès au web nécessite d'adopter une approche nativement intégrée qui renforce la politique de votre pare-feu nouvelle génération par des contrôles simples à définir et capables de détecter, prévenir et endiguer automatiquement les menaces.

Une protection coordonnée pour des accès web sécurisés

Le service URL Filtering de Palo Alto Networks s'appuie sur une combinaison de machine learning et d'analyses statiques et dynamiques pour examiner les sites web et leurs contenus, afin de catégoriser et d'attribuer un score de risque à chaque URL. Une URL est considérée soit inoffensive, soit malveillante. Ces deux catégories sont facilement intégrables à la politique de sécurité d'un pare-feu nouvelle génération pour un contrôle total du trafic web. Les URL nouvellement ajoutées dans la catégorie « malveillantes » sont immédiatement bloquées dès leur détection, sans que l'intervention d'un analyste ne soit nécessaire.

Quant aux autres URL, elles sont soumises à des analyses visant à leur attribuer un score de risque. Elles s'appuient pour cela sur des informations supplémentaires comme l'historique et la réputation du domaine, la réputation de l'hôte, l'utilisation de DNS dynamiques, ou encore la présence de contenus à haut risque. Ensemble, les catégories d'URL et les scores de risque permettent de créer des politiques équilibrées, capables de bloquer les sites web dangereux (utilisés par exemple pour les campagnes de phishing, le déploiement de kits d'exploits ou les communications CnC), tout en permettant aux utilisateurs d'accéder librement aux ressources web nécessaires à leur activité professionnelle.

Partie intégrante de la Security Operating Platform, URL Filtering agit dans le cadre d'une approche intégrée visant à neutraliser les menaces à la première opportunité. Lorsqu'une attaque est perpétrée contre votre réseau, ce service opère en synergie avec vos pare-feu nouvelle génération et la fonction Threat Prevention pour assurer une sécurité optimale. Hormis ses propres données d'analyse, URL Filtering exploite également la Threat Intelligence du service WildFire® de prévention des malwares et de diverses autres sources. Ainsi, seules quelques secondes suffisent pour mettre à jour sa base de sites web malveillants et renforcer la protection.

Étendre les politiques des pare-feu pour contrôler les contenus web

Lorsqu'il détecte du trafic web, un pare-feu nouvelle génération fait appel au service URL Filtering pour identifier la catégorie de l'URL et appliquer la politique de sécurité qui s 'impose. Contrairement aux règles qui soit autorisent, soit interdisent le trafic sans aucune nuance, de multiples catégories d'URL peuvent être combinées dans un même ensemble de politiques. Ceci permet d'établir un encadrement plus équilibré et facile à gérer, basé sur des exceptions et un contrôle granulaire du trafic web. De multiples catégories d'URL peuvent être intégrées aux politiques dans divers buts. Exemple :

- Bloquer tous les sites à « haut risque » tout en autorisant l'accès aux autres sites, mais en bloquant les téléversements / téléchargements de fichiers exécutables ou de fichiers potentiellement dangereux sur les URL à « moyen risque ».
- Autoriser l'accès à des sites d'information spécialisés, tout en bloquant ceux dont les domaines ont été récemment enregistrés.
- Accorder l'accès aux sites de freeware et shareware tout en interdisant les téléchargements et en bloquant les sites à « haut risque ».
- Établir des exceptions aux politiques générales de sécurité pour les utilisateurs appartenant à des groupes spécifiques de l'Active Directory® (par ex. interdiction d'accès aux sites de hacking à tous les utilisateurs, sauf ceux du groupe « sécurité »).
- Permettre l'accès aux sites web et blogs personnels avec déchiffrement SSL (le cas échéant) et application stricte de la fonction Threat Prevention pour bloquer les kits d'exploits incorporés dans les forums et les posts.

Création de politiques basées sur les catégories d'URL	
Politique	**Description**
Déchiffrement SSL sélectif	Procède au déchiffrement SSL en fonction des catégories d'URL.
Vol d'identifiant	Détermine les sites pouvant recevoir des identifiants professionnels et bloque, donne accès ou avertit les utilisateurs qui saisissent leurs identifiants sur des sites non autorisés.
Blocage des fichiers à « haut risque »	Empêche le téléversement/téléchargement d'exécutables ou de fichiers potentiellement dangereux.
Activation de profils IPS plus stricts	Utilise automatiquement des profils anti-spyware et anti-vulnérabilité stricts pour des catégories d'URL spécifiques, afin de bloquer les kits de phishing / d'exploits et d'éliminer les vulnérabilités côté client et serveur.
Politiques basées sur les utilisateurs	Permet à des groupes spécifiques d'accéder à certaines catégories d'URL, tout en bloquant les autres utilisateurs.

Outre le blocage des sites malveillants, la catégorisation d'URL permet d'appliquer des politiques de sécurité granulaires pour protéger les utilisateurs sans ralentir l'activité de l'entreprise.

Déchiffrement sélectif du trafic web

Vous pouvez établir des politiques visant à appliquer un déchiffrement sélectif du trafic web protégé par SSL. Vous renforcez ainsi votre visibilité sur les menaces potentielles tout en vous conformant aux règlementations en matière de confidentialité des données. Par exemple, le trafic issu de plateformes de réseaux sociaux, de messageries web et de plateformes de diffusion de contenu pourront faire l'objet d'un déchiffrement SSL, tandis que les transactions depuis/vers des sites sensibles (par ex. pouvoirs publics, établissements bancaires, prestataires de santé) resteront chiffrées. Vous pouvez par ailleurs mettre en place une politique simple de déchiffrement SSL des contenus de sites présentant un niveau de risque allant de moyen à élevé. Bref, le déchiffrement sélectif optimise votre sécurité, tout en respectant les obligations de confidentialité définies par vos politiques internes ou des réglementations externes.

Détection des menaces par machine learning

Le machine learning et l'automatisation permettent une détection rapide et précise des cybermenaces. Grâce à eux, nos systèmes examinent automatiquement les images, les contenus et la langue d'une URL donnée afin d'établir son degré de dangerosité. Pour classifier les sites web avec précision, nous nous appuyons sur des analyses textuelles et linguistiques qui nous permettent d'établir des corrélations entre les URL, les contenus du site et le contexte d'utilisation de ces contenus. Les images des sites web sont décortiquées pixel par pixel, puis comparées aux exemples existants à l'aide d'un algorithme ultra-sophistiqué conçu pour faciliter la détection des sites de phishing. L'examen de chaque élément d'une page web et les multiples classificateurs basés sur le machine learning nous permettent de nous adapter de manière rapide, précise et continue à des techniques d'attaques en perpétuelle évolution.

- **Analyse des contenus :** nos crawlers examinent minutieusement les attributs de multiples sites web à la recherche d'éléments à caractère malveillant. Les données de domaine corrélées, la présence de formulaires et les emplacements de certains types de contenus font partie des attributs analysés et assimilés par nos classificateurs. Chaque URL analysée est ajoutée à notre bibliothèque de données, ce qui nous permet de renforcer continuellement notre capacité à identifier les sites web potentiellement dangereux.
- **Analyse textuelle :** URL Filtering analyse la nature et le contexte du texte d'un site pour catégoriser ce dernier de la manière la plus précise qui soit.
- **Analyse des images :** pour contourner les dispositifs de détection, de plus en plus de sites de phishing utilisent des images et du code JavaScript masqué plutôt que du texte. L'analyse automatique des images de chaque URL nous permet de comparer le code du site web avec des indicateurs visuels, et ainsi de déterminer avec plus de précision l'éventuelle présence d'une menace de phishing.

Prévention du phishing d'identifiants

Le phishing est l'une des techniques les plus dangereuses, les plus malveillantes et les plus répandues pour faire main basse sur des identifiants légitimes d'utilisateurs. Muni de ce précieux sésame, les attaquants bénéficient d'un accès « autorisé » au réseau d'une entreprise, ce qui augmente considérablement leurs chances de passer inaperçus. Ils ont ainsi plus de temps pour accomplir leur mission, comme par exemple voler des informations sensibles ou causer toute autre forme de tort à l'entreprise.

URL Filtering analyse les pages susceptibles de servir au phishing d'identifiants, tout en bloquant systématiquement l'accès aux pages figurant dans la catégorie « phishing ». En plus de protéger les utilisateurs de cette menace, URL Filtering les empêche aussi de transmettre involontairement leurs identifiants aux cyberattaquants. Pour ce faire, les administrateurs peuvent définir une politique qui détermine les sites autorisés à recevoir des identifiants professionnels. Grâce à la technologie User-ID™ déployée sur les pare-feu

nouvelle génération de Palo Alto Networks, URL Filtering détecte les identifiants saisis sur les formulaires en ligne et vous permet de définir une politique visant à empêcher la saisie, l'autoriser ou avertir l'utilisateur du danger encouru.

Catégories personnalisables

URL Filtering s'appuie sur un ensemble défini de catégories. Cependant, chaque entreprise peut avoir ses spécificités en matière de tolérance au risque, de conformité, de réglementation et d'utilisation acceptable. Pour répondre à ces exigences et affiner les politiques de sécurité, les administrateurs peuvent créer leurs propres catégories en combinant plusieurs catégories existantes. Par exemple, la combinaison des catégories « haut risque », « services financiers » et « récemment enregistré » pourrait donner lieu à une nouvelle catégorie dont les politiques seraient applicables aux sites répondant à ces trois critères.

Contrôles renforcés sur les tactiques courantes de contournement

Les politiques de filtrage d'URL Filtering gardent leur efficacité face à des tactiques courantes de contournement, notamment celles qui utilisent les résultats de recherche mis en cache et les sites web de traduction.

- **Prévention de la mise en cache des résultats de recherche :** l'une des tactiques courantes de contournement consiste à accéder aux résultats mis en cache dans les moteurs de recherche connus. Pour lutter contre cette pratique, les politiques d'URL Filtering sont appliquées lorsque des utilisateurs tentent de consulter les résultats en cache des recherches Google et des archives Internet.
- **Filtrage des sites web de traduction :** les politiques d'URL Filtering s'appliquent aux URL copiées sur des sites de traduction (par ex. Google Traduction) comme moyen de contourner les politiques.

Safe Search Enforcement

La fonction Safe Search Enforcement empêche l'affichage de contenus inappropriés dans les résultats de recherche d'un utilisateur. Lorsqu'elle est activée, seules les recherches Google, Yandex, Yahoo et Bing répondant aux critères de recherche sécurisée les plus stricts seront autorisées. Toutes les autres recherches seront bloquées.

Notifications utilisateur personnalisables

Chaque entreprise a sa propre manière d'informer ses utilisateurs qui tentent d'accéder à des pages bloquées par une politique de filtrage URL Filtering. Ces derniers pourront par exemple être avertis via une page personnalisée faisant référence au nom d'utilisateur, à l'adresse IP, l'URL ciblée, la catégorie d'URL associée à la page et un message de l'administrateur. Toutefois, pour redonner aux utilisateurs un certain contrôle sur leur activité web, les administrateurs disposent de deux options :

- **URL Filtering – Continue :** lorsqu'un utilisateur accède à des pages potentiellement dangereuses pour l'entreprise, URL Filtering affiche une page d'avertissement contenant un bouton « Continuer ». Les utilisateurs sont ainsi sensibilisés aux risques encourus, tout en ayant le choix de poursuivre leur navigation s'ils jugent ces risques acceptables.
- **URL Filtering – Override :** cette option exige des utilisateurs qu'ils saisissent un mot de passe configurable pour créer une exception qui leur permettra de poursuivre leur navigation. Ils peuvent ainsi accéder à des sites potentiellement dangereux, mais bénéficient pour cela de l'aval de l'administrateur.

Reporting et journalisation des activités URL

Des rapports prédéfinis ou entièrement personnalisables offrent aux départements informatiques une visibilité sur les activités web en général et de filtrage (via URL Filtering) en particulier.

- **Rapports d'activité des utilisateurs :** le rapport d'activité individuel d'un utilisateur affiche les applications utilisées, les catégories d'URL visitées, les sites web consultés et une liste détaillée de toutes les URL auxquelles l'utilisateur a accédé pendant une période donnée.
- **Rapports d'activité sur les URL :** des rapports « Top 50 » établissent divers classements : catégories d'URL visitées ; utilisateurs d'URL données ; sites web consultés ; catégories, utilisateurs et sites bloqués, etc.

Sécurité maximum, TCO minimum

URL Filtering est fourni en natif sur les pare-feu nouvelle génération Palo Alto Networks. Notre approche « plateforme » élimine ainsi le besoin de recourir à de multiples logiciels et appliances de sécurité autonomes. En intégrant URL Filtering directement à votre politique existante de contrôle du trafic réseau, vous réduisez vos dépenses d'exploitation grâce à une base de règles simplifiées et une réduction des coûts de formation. La licence URL Filtering n'est soumise à aucun plafond du nombre d'utilisateurs. Vous pouvez ainsi protéger l'ensemble de vos utilisateurs, tout en réduisant le coût total de possession (TCO) et en renforçant votre sécurité.

Informations de licence

Le service URL Filtering est disponible via une licence Palo Alto Networks URL Filtering ou dans le cadre des contrats de licence d'entreprise (ELA) Palo Alto Networks Subscriptions ou Palo Alto Networks VM-Series.

Oval Tower, De Entrée 99 -179
1101HE Amsterdam, Pays-Bas

+31 20 888 1883

www.paloaltonetworks.fr

url-filtering-ds-012319-fr