Fiche savoirs : proxy HTTP

Présentation

Le web est un des principaux vecteurs d'attaque informatique. De nombreux malwares, chevaux de troie, ransomware, virus, contaminent des réseaux ou des hôtes d'entreprise par ce biais. Le filtrage **stateful** traditionnel s'avère insuffisant lorsque l'on souhaite traiter cette problématique.

L'UTM SNS Stormshield intègre le service proxy web pour permet de renforcer la sécurité liée à ces usages.

Principe du proxy web

Un proxy est un **composant logiciel et/ou matériel informatique** qui joue le rôle d'**intermédiaire** (mandataire) en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. Le proxy se situe au niveau de la **couche application**.

Le service proxy web est indispensable en entreprise, car il assure les fonctions suivantes :

- **examine le trafic web** afin d'identifier les contenus suspects ;
- **bloque** des catégories de **sites**, des **URL**, des **mots-clés** ;
- **journalise** l'ensemble des informations liées au protocole **http** (couche 4 du modèle TCP/IP ou couche 5 à 7 du modèle OSI) et offre ainsi des informations plus complètes que les logs émanant d'un pare-feu **stateful** standard.
- dispose d'une **fonction de cache** lui permettant de stocker les pages web consultées et de les fournir, par la suite, aux clients souhaitant accéder à ces mêmes pages.

Proxy web non transparent et proxy web transparent

Il y a deux manières d'utiliser un proxy web : proxy non transparent et proxy transparent.

proxy non transparent

- Le proxy non transparent **doit être déclaré sur le poste client** afin que ce dernier soit configuré de manière à passer par le proxy lorsqu'une requête est envoyée ;
- Le proxy **se connecte au site demandé** à la place du client et **retourne** la page Web demandée au poste client ,
- Le serveur qui héberge le site demandé, ne communique qu'avec le serveur proxy et ignore la présence du poste client.

Si le serveur proxy n'est pas configuré sur le poste client, alors la requête sera envoyée directement au serveur distant, comme si le serveur proxy n'existait pas.

> Le serveur **proxy non transparent** peut être dans en **DMZ**, ou bien la fonction de proxy est assurée directement par le **pare-feu** (pas de DMZ).

proxy transparent

- Le **proxy transparent** n'a pas à être configuré sur le poste client et ce lui-ci l'utilise sans s'en rendre compte.
- Le proxy est utilisé comme **passerelle** au niveau de la configuration du poste client. C'est la configuration idéale pour filtrer le trafic émis par les postes clients.

Dans ce cas, la fonction de pare-feu et de serveur proxy transparent sont généralement regroupée sur un même serveur/équipement c'st à dire le **pare-feu**. Il est bien sûr possible que le pare-feu soit configuré pour relayer les trames vers le proxy

Pour en savoir plus : https://www.it-connect.fr/les-serveurs-proxy-et-reverse-proxy-pour-les-debutants/

Mise en place du filtrage applicatif

La mise en place d'une **politique de filtrage**, permet à l'administrateur de définir les règles qui permettront d'autoriser ou de bloquer des flux au travers du pare-feu SNS. Selon les flux, certaines **inspections de sécurité** (analyse antivirale, analyse antispam, filtrage URL, etc.)

peuvent être activées sur les pare-feu SNS afin de :

- **contrôler** les accès à certains sites web d'Internet (**filtrage d'URL et filtrage SSL**) ;
- créer une **politique anti-relais et antispam** (filtrage SMTP) ;
- effectuer une **analyse antivirale** sur les flux DATA (HTTP, SMTP, FTP, POP3, etc.) ;
- **bloquer** les maliciels à l'aide d'une **analyse comportementale** sur des machines de détonation (sandboxing Breachfighter).

Configuration du service proxy Web HTTP

La fonction de **filtrage des URL** permet de contrôler l'accès aux sites web d'Internet pour l'ensemble des utilisateurs. Pour contrôler ces accès, la politique de filtrage URL va se baser sur une **liste d'URL** classées en **catégories** ou de **mots clés personnalisés**.

Les bases d'URL disponibles

Deux fournisseurs de base URL sont disponibles sur les pare-feu SNS :

- **Base URL embarquée** composée de 16 catégories téléchargées sur les serveurs de mise à jour,
- **Base Extended Web Control (EWC)** constituée de 65 catégories, toutes hébergées dans le Cloud. Cette base est disponible en option payante, elle est néanmoins incluse dans les VM du partenariat Stormshield Academy.

Le menu **Configuration / Objets / Objets Web** puis l'onglet **Base d'URL**. La base par défaut est la Base URL embarquée. http://www.reseaucerta.org juillet 2022 – v1.0 Page 1/14 Les catégories prédéfinies pour la Base URL embarquée sont disponibles. Le contenu des catégories ne peut pas être consulté. Cependant, l'appartenance d'une URL à un groupe peut être vérifiée par le biais des champs de classification. Ces champs sont disponibles depuis le menu Objets Web ou au sein d'une politique de filtrage URL. Par exemple, pour vérifier l'appartenance de Stormshield à une des catégories de la base :Ouvrir Configuration / Objets / Objets Web onglet URL.Dans la zone Vérifier l'utilisation saisir stormshield.eu et cliquer Classifier.

Retour

- Mise en oeuvre de l'UTM Stormshield