

Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques

Situation 4 : Proxy web HTTP et HTTPS

Fiche Stormshield associée : fiche 8 – Filtrage applicatif

Le web¹ 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.

Votre responsable vous demande de renforcer la sécurité liée à ces usages en utilisant le service proxy web intégré au boîtier UTM Stormshield.

Documentation

Document 1 : La notion de proxy web.....	4
Document 2 : Fonctionnement d'un serveur mandataire SSL/TLS.....	5
Document 3 : Extrait des recommandations de sécurité concernant l'analyse des flux HTTPS publiées par l'ANSSI en 2014.....	6
Document 4 : Article publié par Stormshield présentant un comparatif entre chaque méthode de filtrage disponible avec le proxy web HTTPS.....	7
Document 6 : Comment récupérer un flux https après déchiffrement du proxy SSL sur un pare-feu Stormshield.....	9

I Mise en œuvre du service proxy Web HTTP

Généralités

1. Expliquer en quoi un serveur proxy web améliore la sécurité et la traçabilité des événements liés au protocole HTTP.

Un serveur mandataire dédié peut être présent sur le réseau local de l'entreprise. Cependant la plupart des boîtiers UTM intègre cette fonction.

2. Fournir les avantages et les inconvénients des 2 solutions.
3. Préciser et justifier l'emplacement du serveur mandataire sur le réseau de l'entreprise.

Finalement, le DSI a décidé d'utiliser le service proxy du pare-feu SNS 210. Ce service proxy est dit « transparent ».

4. Expliquer la différence entre un serveur mandataire http classique et un serveur mandataire transparent.

1 Consultation de pages web hébergées sur des serveurs web à l'aide d'un navigateur utilisant les protocoles HTTP (port 80/TCP) ou HTTPS (port 443/TCP).

Cahier des charges

- A. Mettre en place un nouveau filtrage URL permettant d'interdire les publicités, la culture et les loisirs, les contenus illicites, les jeux en ligne et les réseaux sociaux, la pornographie, les proxys anonymes, ainsi que le piratage et les téléchargements (warez) pour les réseaux Production et Client.
- B. Faire en sorte que les sites `site.web.perso.free.fr` et `silc.fr` soient également bloqués. Une page de blocage personnalisée devra apparaître dans le navigateur des utilisateurs.
- C. De 12h00 à 14h00, il a été convenu que les employés de l'entreprise puissent avoir accès à certains sites pour se divertir. Ainsi, vous devez proposer un filtrage URL qui autorise la culture et les loisirs ainsi que les jeux en ligne, les réseaux sociaux pendant ce créneau horaire précis.
- D. L'antivirus par défaut du pare-feu (ClamAV) doit être activé concernant l'ensemble des requêtes http.
- E. Réaliser une recette afin de s'assurer que l'ensemble des demandes est bien opérationnel.

En 2020, 83 %² des sites web utilisent le protocole HTTPS par défaut. Cette démocratisation salutaire encouragée par des initiatives comme Let's Encrypt³ a permis d'avoir un web plus sûr. En effet, HTTPS permet de chiffrer les connexions web entre un client et un serveur. En revanche, cela complexifie la tâche des administrateurs réseaux d'entreprise et rend inopérant le serveur mandataire HTTP.

Votre responsable vous charge de mettre en place un serveur mandataire spécifique lié au protocole HTTPS sur le pare-feu.

II Mise en œuvre du service proxy web HTTPS

Généralités

1. Pourquoi un serveur proxy http n'est pas en mesure d'analyser des flux HTTPS ?
2. Expliquer pourquoi on parle d'un proxy « Man-in-the-middle » dans le cadre d'un proxy HTTPS ?
3. Quelles sont les obligations légales de l'entreprise pour pouvoir mettre en œuvre un tel service ?

Cahier des charges

- A. Activer le proxy SSL avec déchiffrement pour toutes les connexions HTTPS émanant de votre LAN vers Internet.
- B. Mettre en place un nouveau filtrage HTTPS permettant d'interdire les publicités, la culture et les loisirs, les contenus illicites, les jeux en ligne et les réseaux sociaux, la pornographie, les proxys anonymes, ainsi que le piratage et les téléchargements (warez).
- C. Faire en sorte que les sites discord.gg, discord.com, tinder.com et twitch.tv soient également bloqués.
- D. De 12h00 à 14h00, il a été convenu que les employés de l'entreprise puissent avoir accès à certains sites pour se divertir. Ainsi, vous devez proposer un filtrage URL similaire au précédent mais qui autorise la culture et les loisirs ainsi que les jeux en ligne et réseaux sociaux pendant ce créneau horaire précis.
- E. Interdire l'accès à linkedin.com sans déchiffrer (bloquer sans déchiffrer). Les sites contenus dans la catégorie « bank » doivent être autorisés sans être déchiffrés (passer sans déchiffrer).
- F. Pour quelles raisons un avertissement apparaît dans votre navigateur lorsque que vous tenter d'accéder à un site en https hormis la catégorie de sites bancaires ? Faire en sorte qu'aucun avertissement ne s'affiche dans le navigateur web des postes clients Windows 10 quand ils essayent de consulter des sites en HTTPS (privilégier Mozilla Firefox ou Edge à Google Chrome).
- G. Réaliser une recette permettant de s'assurer que le cahier des charges est respecté.
- H. EXPLORATION : Récupérer, à l'aide d'une capture de trames sur le pare-feu, le contenu d'une connexion https émise par un client après déchiffrement du proxy SSL (ex : récupération du login et du mot de passe lors d'une connexion à un compte ENT).
- I. En tant qu'administrateur réseau, avez-vous le droit d'effectuer cette action en entreprise ?

Questionnement complémentaire

Le service proxy HTTPS proposé par Stormshield permet de bloquer certains sites après déchiffrement ou sans déchiffrement.

4. Présenter les avantages et les inconvénients de chacune de ces méthodes.

2 source : https://w3techs.com/technologies/history_overview/ssl_certificate/all/y

3 <https://letsencrypt.org/>

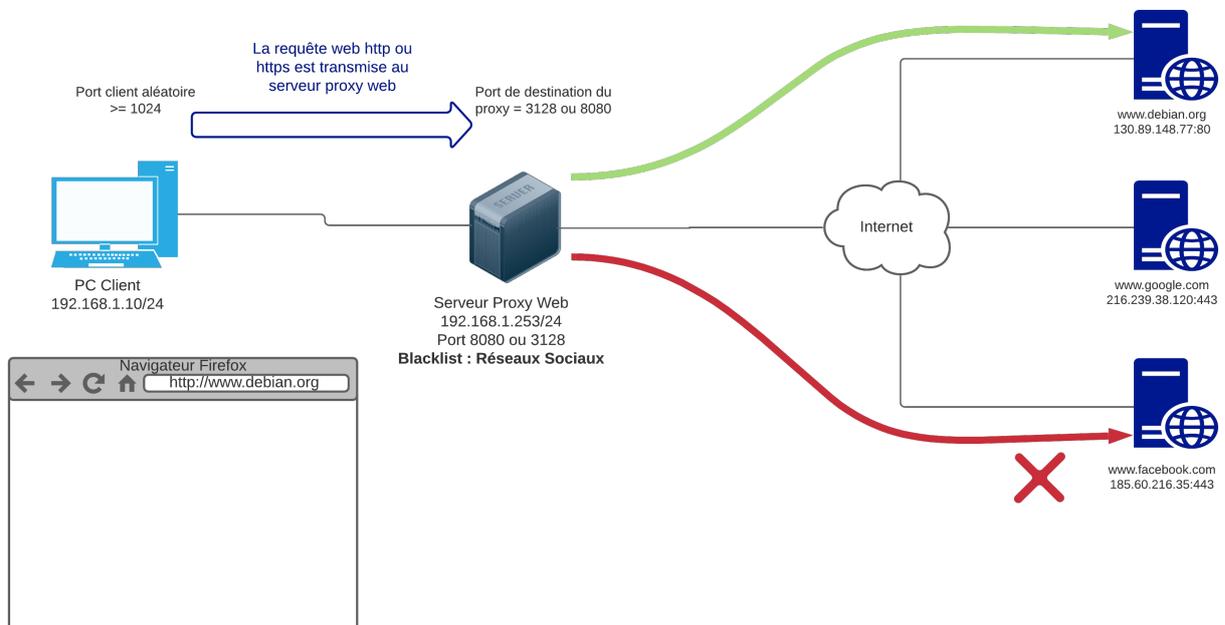
Documentation

Document 1 : La notion de proxy web

Un proxy est un composant logiciel et/ou matériel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. Le proxy se situe au niveau de la couche application.⁴

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.



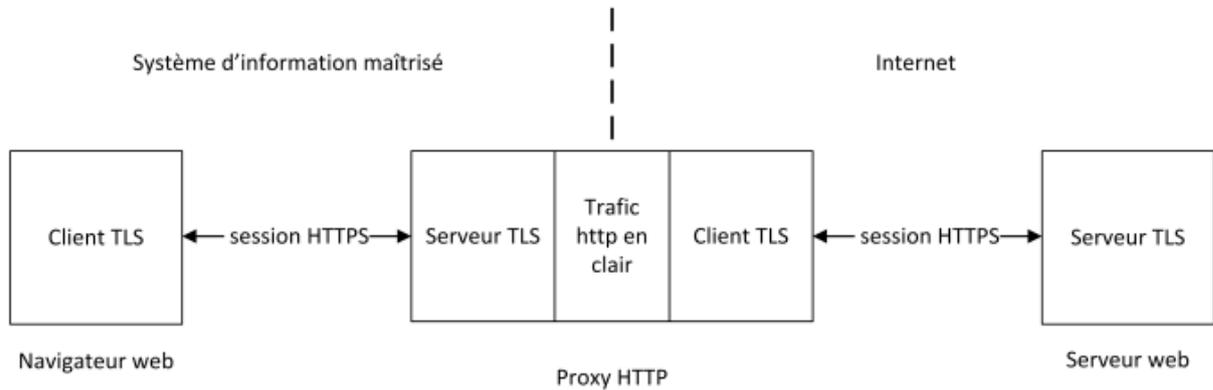
4 Définition issue du site Wikipédia : <https://fr.wikipedia.org/wiki/Proxy>

Document 2 : Fonctionnement d'un serveur mandataire SSL/TLS

Contrairement au proxy http, le serveur mandataire TLS est en mesure de disposer du trafic en clair échangé entre le client et le serveur cible. Cela est possible lorsque le proxy peut « duper » le client en interceptant la connexion TLS qu'il initie en direction du serveur cible.

Le proxy doit pour cela intégrer un serveur TLS pour pouvoir être le point de terminaison des sessions HTTPS. Le proxy joue ensuite le rôle de client vis-à-vis du serveur cible avec lequel il établit un autre tunnel TLS pour sécuriser les échanges qui transitent sur Internet.

Ce double rôle permet ainsi au proxy de disposer du trafic non chiffré entre les deux tunnels TLS établis.⁵



5 Paragraphe et schéma issus des recommandations de l'ANSSI pour l'analyse de flux HTTPS publiées en 2014

Document 3 : Extrait des recommandations de sécurité concernant l'analyse des flux HTTPS publiées par l'ANSSI en 2014

Avant de mettre en place des mécanismes de déchiffrement au niveau d'un proxy web, il est nécessaire de bien comprendre les avantages, les inconvénients et les problématiques que cela induit.

La possibilité de disposer du trafic HTTPS en clair au niveau d'un proxy web procure plusieurs avantages :

- il est possible d'analyser le trafic HTTPS afin de protéger le client de menaces émanant du serveur web cible : contenus inappropriés, fichiers malveillants, etc. ;
- il est possible de contrôler le contenu des données échangées entre le client et le serveur afin de s'assurer que les flux HTTPS ne sont pas utilisés pour faire sortir du système d'information des données confidentielles. L'analyse doit être réalisée en limitant autant que possible l'exposition des données à caractère personnel des clients ;
- il est possible d'appliquer la même politique de journalisation que celle mise en œuvre pour les flux HTTP non sécurisés. La journalisation doit être réalisée en accord avec le respect de la vie privée des clients ;
- le proxy a la possibilité de mettre en cache du contenu qu'il peut resservir à plusieurs clients qui souhaitent accéder au même serveur cible.

Cependant, le déchiffrement présente plusieurs inconvénients :

- des données normalement chiffrées sont présentes en clair au niveau du proxy. Si ce dernier est compromis, des informations sensibles peuvent être exposées ;
- l'authentification du client à l'aide d'un certificat n'est plus possible auprès d'un site web qui requerrait ce mode d'authentification. En effet, le proxy étant placé en coupure, le client ne dialogue pas directement en TLS avec le site web ; il ne reçoit donc pas les demandes d'authentification par certificat formulées par ce dernier. Les sites qui requièrent une authentification par certificat doivent donc être placés dans une liste blanche pour laquelle le déchiffrement n'est pas effectué ;
- le niveau de sécurité du tunnel TLS établi sur Internet avec le serveur cible ne dépend plus du navigateur web du client. Celui-ci n'est donc pas en mesure de connaître les risques qu'il prend. La sécurisation des tunnels TLS établis avec le monde extérieur repose uniquement sur les possibilités offertes par le proxy en tant que client, celui-ci étant potentiellement plus laxiste au niveau TLS que les navigateurs web les plus récents ;
- une Autorité de certification interne doit être employée pour générer les certificats que le proxy présente à ses clients.

En résumé, si le déchiffrement des flux HTTPS permet un meilleur contrôle des données échangées entre un système d'information et le monde extérieur, ce processus complexifie l'architecture d'accès à Internet et déporte la sécurisation du canal de communication avec l'extérieur sur le proxy. Ce type d'équipement devient ainsi très critique.

Document 4 : Article publié par Stormshield présentant un comparatif entre chaque méthode de filtrage disponible avec le proxy web HTTPS⁶

Filtrage sans déchiffrement des flux TLS

Cette méthode permet de bloquer les sites web HTTPS indésirables en vérifiant seulement leur certificat sans déchiffrer le flux. Il n'est donc pas nécessaire d'installer un certificat sur tous les navigateurs de chaque poste de travail. De plus, un message de certificat invalide apparaît en cas de blocage et vous ne pouvez pas personnaliser la page de blocage.

Filtrage avec déchiffrement des flux TLS

Cette méthode permet de bloquer les sites web HTTPS indésirables et d'analyser les connexions HTTPS. Vous pouvez utiliser les filtres URL créés initialement pour le protocole HTTP et personnaliser la page de blocage qui s'affiche sur le poste de travail lorsqu'un site web HTTPS est bloqué.

Puisque les flux SSL sont déchiffrés par le firewall SNS, ce dernier va générer un certificat auto-signé que le navigateur ne pourra pas considérer de confiance. Un message d'erreur s'affichera sur le navigateur des utilisateurs indiquant la provenance suspecte du certificat présenté par le firewall SNS. Pour éviter ce type de message, vous devrez déployer l'autorité auto-signée du firewall sur les navigateurs afin qu'elle soit reconnue.

Assurez-vous également de dresser une liste explicite des sites web HTTPS et/ou des catégories de sites web HTTPS que vous n'êtes pas autorisé à déchiffrer (cf RGPD et CNIL).

Le tableau ci-dessous résume les caractéristiques de chaque méthode de filtrage :

	Sans déchiffrement	Avec déchiffrement
Blocage des sites web HTTPS	X	X
Analyse anti-virus, sandboxing, SafeSearch, etc.		X
Affichage d'une page de blocage personnalisée		X
Un certificat doit être installé sur chaque poste de travail		X
Ne pas déchiffrer les sites et/ou catégories de sites non autorisés	N/A	X
Accès possible pour les périphériques sans certificat (BYOD)	X	

6 https://documentation.stormshield.eu/SNS/v4/fr/Content/HTTPS_filtering/Two_filtering_methods.htm

Document 5 : Aspects juridiques liés à l'utilisation d'un proxy TLS⁷

Le déchiffrement d'un flux chiffré peut porter atteinte aux libertés individuelles et engager la responsabilité de l'employeur qui n'aurait pas prévu les mesures destinées à préserver celles-ci :

- secret des correspondances privées ;
- protection des données à caractère personnel ;
- respect de la vie privée des utilisateurs ;
- protection du secret professionnel ou du secret défense.

La mise en place d'un dispositif de déchiffrement par l'entité doit être encadrée juridiquement :

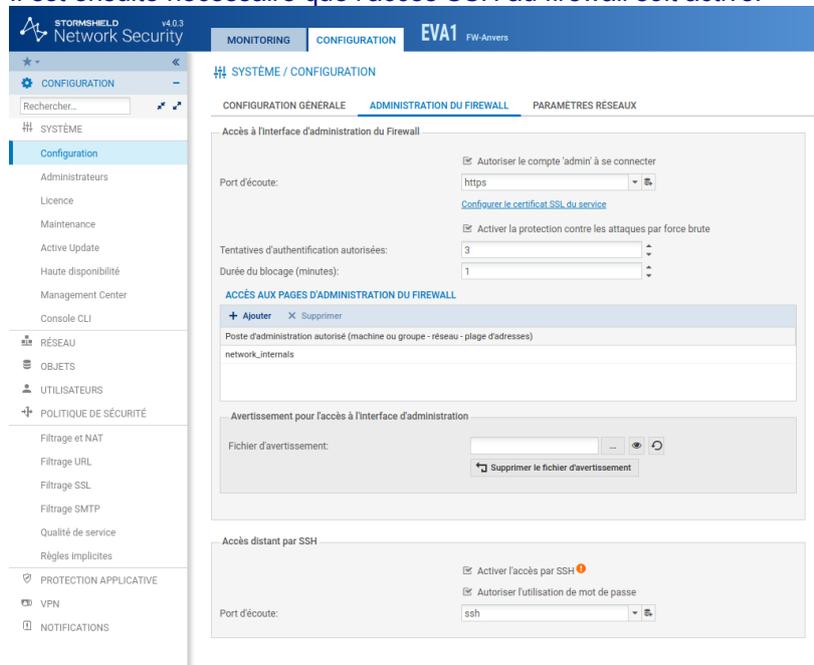
1. par la charte d'utilisation des moyens informatiques et de communications électroniques rédigée par l'employeur et annexée au règlement intérieur de l'entité, après consultation des instances représentatives du personnel. Celle-ci devra prévoir, notamment, les règles d'utilisation des moyens mis à disposition par l'employeur, les modalités d'accès aux données et aux équipements, l'hypothèse, les sanctions en cas de non-respect, etc ;
2. par la mise en place d'un administrateur expressément autorisé à accéder aux contenus déchiffrés moyennant le respect d'une obligation de confidentialité qui le lie, y compris à l'égard de l'employeur ;
3. par la politique de sécurité des systèmes d'information de l'entité qui devra envisager cette hypothèse, et éventuellement le cas des sous-traitants ;
4. par les déclarations adaptées à la CNIL en considérant avec soin les finalités pour lesquelles le déchiffrement est envisagé.

7 Source : Recommandations de sécurité concernant l'analyse des flux HTTPS publiées par l'ANSSI en 2014

Document 6 : Comment récupérer un flux https après déchiffrement du proxy SSL sur un pare-feu Stormshield

Au préalable, il est indispensable que le proxy SSL soit correctement paramétré et que le client web passe par lui.

Il est ensuite nécessaire que l'accès SSH au firewall soit activé.



The screenshot shows the Stormshield Network Security v4.0.3 interface. The main menu on the left includes Configuration, Système, Réseau, Objets, Utilisateurs, Politique de Sécurité, Filtrage et NAT, Filtrage URL, Filtrage SSL, Filtrage SMTP, Qualité de service, Règles implicites, Protection applicative, VPN, and Notifications. The main content area is titled 'SYSTÈME / CONFIGURATION' and 'ADMINISTRATION DU FIREWALL'. It contains three sections: 'Accès à l'interface d'administration du Firewall' with options for 'Autoriser le compte 'admin'' and 'Activer la protection contre les attaques par force brute'; 'ACCÈS AUX PAGES D'ADMINISTRATION DU FIREWALL' with a table for authorized administration pages; and 'Accès distant par SSH' with options for 'Activer l'accès par SSH' and 'Autoriser l'utilisation de mot de passe'.

Se connecter en SSH à l'aide du compte administrateur puis réaliser une capture de trame sur l'adresse IPv4 de boucle locale 127.0.0.2 port 8080 qui sera enregistrée dans un fichier .pcap.

```
FW-Anvers>tcpdump -w /log/ssldump.cap -i lo0 host 127.0.0.2 and port 8080
```

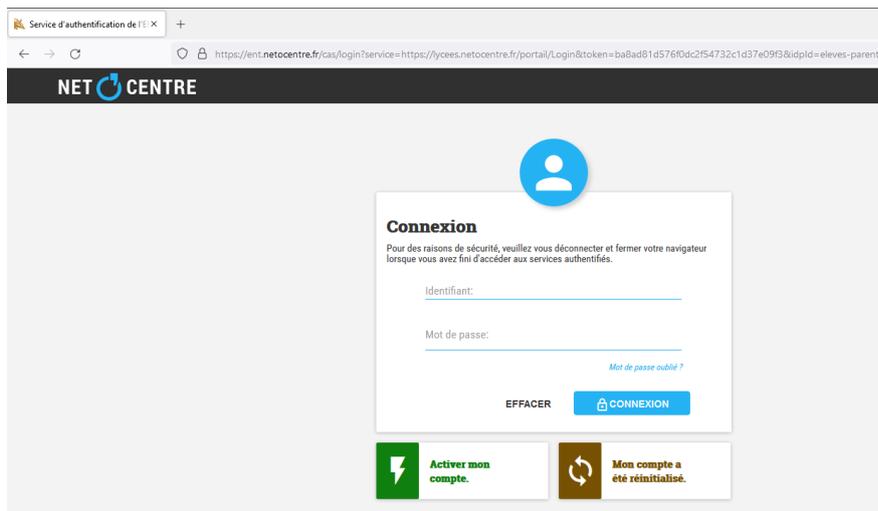
```
tcpdump: listening on lo0, link-type NULL (BSD loopback), capture size 262144 bytes
```

```
^C65 packets captured
```

```
148 packets received by filter
```

```
0 packets dropped by kernel
```

Sur un client web, lancer une connexion https vers un site qui demandera une authentification par login et mot de passe. Saisir le couple pour s'authentifier via le navigateur web.



Sur le pare-feu, stopper la capture de trame tcpdump à l'aide de la combinaison de touche Ctrl-C.

Récupérer le fichier pcap sur une machine cliente à l'aide de WinSCP sous Windows ou de la commande scp (SecureCopy) sous GNU/Linux.

```
adminleve@desktop:~$ scp admin@192.168.1.126:/log/ssldump.cap /home/adminleve
```

Password:

```
ssldump.cap 100% 3375KB 26.8MB/s 00:00
```

Ouvrir le fichier pcap à l'aide de Wireshark afin de pouvoir l'analyser. Vous trouverez les informations d'authentification en clair dans l'une des requêtes POST HTTP.

