Activité : Analyse prélable de l'infrastructure à mettre en oeuvre

- En vous aidant du document 1 sur différences entre **pare-feu stateful simple** et pare-feu **UTM**, donner les arguments en faveur d'un boîtier UTM Stormshield par rapport à un routeur Cisco gérant des ACLs au niveau de la couche 3 et 4 du modèle OSI.
- En vous aidant du document 2 sur la souveraineté numérique, donner au moins 2 arguments en faveur d'un boîtier UTM Stormshield par rapport à ceux proposés par des entreprises concurrentes telles que Palo Alto ou CheckPoint.

> Palo Alto et Checkpoint sont respectivement des entreprises, l'une américaine, l'autre israélienne, spécialisées dans la sécurité informatique, concurrentes directes de la société Stormshield.

Document 1 : différences entre pare-feu stateful simple et pare-feu UTM.

Le pare-feu stateful intervient essentiellement jusqu'à la couche 4 du modèle OSI :

- Il inspecte les paquets IP
- les en-têtes au niveau de la couche de transport
- et dresse l'inventaire des connexions actives, permettant ainsi d'utiliser **l'état** d'une connexion (nouvelle, active, non-existante) pour définir une règle.

Le pare-feu **UTM (Unified Threat Management)**, ou gestion unifiée des menaces, est une solution de sécurité tout-en-un, généralement une appliance de sécurité unique, qui fournit plusieurs fonctions de sécurité en un seul point du réseau. Une appliance UTM réunit le plus souvent des fonctions telles que :

1. logiciel antivirus,
2. logiciel anti-espions,
3. protection antispam,
4. pare-feu réseau,
5. prévention et détection des intrusions,
6. filtrage des contenus et prévention des fuites.

Cette technologie de pare-feu positionne l'inspection de paquets au niveau de la couche applicative, la couche 7 du modèle OSI (couche 4 du modèle TCP/IP).

Ainsi, si les informations sur les connexions et leur statut peuvent être utilisées pour définir des règles, ces dernières peuvent désormais intégrer des informations liées à des opérations menées dans le cadre d'un protocole précis. De plus, plutôt que de recourir à des fournisseurs ou appliances dédiés à chaque tache de sécurité, les organisations peuvent regrouper toutes ces fonctions autour d'un seul et même fournisseur. L'administration est ainsi réduite à un seul segment ou à une seule équipe informatique utilisant une console centralisée qui facilite considérablement la lutte contre les nombreuses menaces actuelles.

Document 2 : qu'est-ce que la souveraineté numérique ?

La souveraineté numérique désigne l'application des principes de souveraineté au domaine des technologies de l'information et de la communication (TIC), c'est-à-dire à l'informatique et aux télécommunications. En France, la souveraineté est définie dans la Constitution de 1958. Elle désigne l'exercice du pouvoir par le peuple et pour le peuple par l'intermédiaire de ses représentants et du référendum.

En matière de numérique, elle consiste à ce qu'un pays et les citoyens qui la composent puissent garder la maîtrise des outils et données informatiques notamment lorsque ces derniers revêtent des enjeux stratégiques et démocratiques.

En France, une stratégie pour garantir la souveraineté numérique du pays a été élaborée en 2015 à la demande du 1er ministre par l'ANSSI et repose sur 5 objectifs majeurs :

1. Défendre et assurer la sécurité des **systèmes d'information critiques ou stratégiques** pour l'état (OIV).
2. Garantir une **confiance numérique** pour les citoyens en leur assurant le droit à la vie privée, le respect des données à caractère personnel et la lutte contre la cybermalveillance.
3. Renforcer la **sensibilisation des utilisateurs** aux enjeux liés à la cybersécurité ainsi que les formations initiales et continues dédiées au numérique.
4. Favoriser le **développement des entreprises numériques** et une politique industrielle à même de **garantir** la souveraineté du pays.
5. Créer une **souveraineté numérique** européenne et garantir la stabilité du cyberespace.

La prise en compte des conditions générales d'utilisation et de la juridiction qui s'appliquent à un produit ou à une entreprise sont des critères de choix importants. Ainsi, une entreprise qui choisit un nom de domaine en **.com** (juridiction américaine) ne sera pas soumise à la même juridiction que si elle choisit un nom de domaine en **.fr** (juridiction française).

Il en va de même pour certains produits ou services notamment américains qui sont soumis à l'extraterritorialité du droit américain.

Avec l'accroissement exponentiel de numérique, l'espionnage industriel devient un enjeu déterminant et il est important que les entreprises françaises soient sensibilisées à la capacité de surveillance numérique des puissances étrangères par l'intermédiaire de leurs produits informatiques (Apple, Google, Cisco, Huawei, Microsoft, Amazon).

Pour les entreprises qui n'ont pas les moyens d'auditer ou de pentester ces produits elles-mêmes, il est pertinent de faire confiance aux **certifications délivrées par l'ANSSI** suite à un audit rigoureux de leur part.

Retour

- Mise en oeuvre de l'UTM Stormshield