

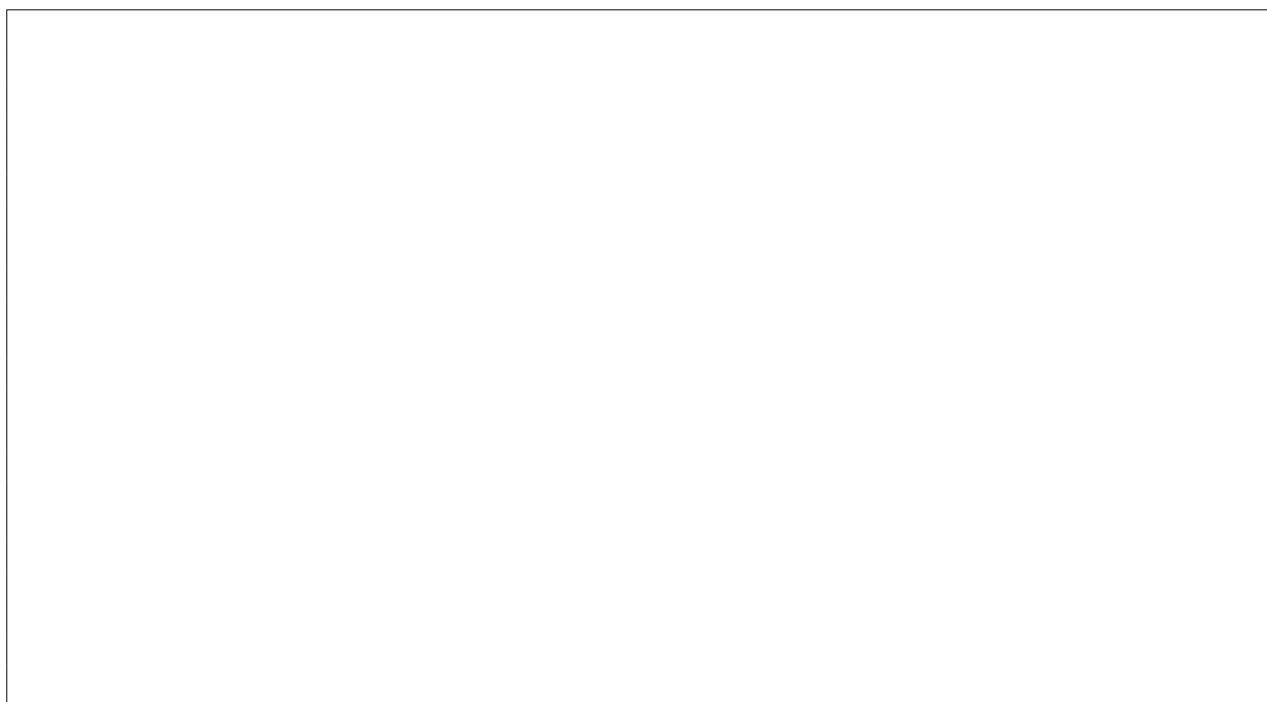
Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques

Situation 0 : Phase d'analyse préalable

- 1 . Expliquer ce qui a poussé le service RSSI à opter pour une solution UTM par rapport à un simple pare-feu stateful traditionnel.
- 2 . Donner 2 arguments en faveur d'un boîtier UTM Stormshield par rapport à ceux proposés par des entreprises concurrentes telles que Palo Alto ou CheckPoint¹.

L'équipe d'administrateurs réseau souhaite suivre les recommandations de l'ANSSI en matière de politique de sécurité à l'intérieur du réseau local de chaque agence.

- 3 . Dans le schéma proposé dans le document 1 du contexte, expliquer pourquoi la présence d'un réseau local unique au sein des agences pose des problèmes de sécurité. Puis proposer une solution qui prenne en compte les différents services recensés dans le document 1 du dossier documentaire. Il faudra s'assurer que l'administration des serveurs et des éléments actifs s'opère depuis une zone dédiée à cet usage.
- 4 . Réaliser un schéma réseau logique représentant votre nouvelle proposition. Ce schéma ne concerne uniquement que le site dont vous avez la charge.



- 5 . Réaliser une maquette de la nouvelle infrastructure du site à l'aide du logiciel Packet Tracer. Le pare-feu du site sera représenté par un routeur. Les hôtes du réseau local et de la DMZ doivent être en mesure de communiquer.

1 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.

Documents

Document 1 : description des services présents dans le réseau local de votre agence

Intitulé des services	Nombre d'hôtes par service
Production	60 hôtes
Client 1	16 hôtes
Administration systèmes et réseaux	3 hôtes

NB : L'évolution du réseau est un élément primordial à prendre en compte. Ainsi, en cas de découpage réseau, il est indispensable de prévoir un plan d'adressage capable d'accueillir au minimum le double d'équipements par rapport au recensement initial afin d'éviter toute possibilité de saturation.

Document 2 : 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 ainsi que 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 tâche 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 3 : 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 1^{er} 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 cyberspace.

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.

Document 4 : extrait du guide ANSSI « Recommandations relatives à l'administration sécurisée des systèmes d'informations »

Les ressources d'administration sont des cibles privilégiées par un attaquant. En effet, les droits élevés nécessaires à la réalisation des actions d'administration et les larges accès généralement attribués exposent ces ressources à une menace élevée. Dans de nombreux cas de compromission ou d'intrusion sur ces équipements, l'attaquant prend le contrôle de l'ensemble du SI.

Pour réduire la surface d'exposition aux attaques informatiques et les conséquences en cas de compromission, il est nécessaire de procéder à un découpage du SI administré en zones différenciées (sous-réseaux avec politique d'accès renforcée).

Des mécanismes techniques de cloisonnement sont alors mis en œuvre pour matérialiser les zones d'administration : filtrage, chiffrement, authentification, etc. Ainsi, en respectant le principe du moindre privilège, un administrateur donné n'a accès qu'à la ou les zones d'administration dont il a le juste le besoin opérationnel, sans possibilité technique d'accéder à une autre zone.

Le réseau d'administration se définit comme le réseau de communication sur lequel transitent les flux internes au SI d'administration et les flux d'administration à destination des ressources administrées. Ce réseau contiendra le poste d'administration et les outils associés ainsi que les éléments actifs du réseau. Ces derniers (commutateurs, routeurs, pare-feu) ne seront administrables que par le poste d'administration à l'aide d'un protocole chiffré adéquat comme HTTPS ou SSH. La mise en place d'une authentification type 802.1x ou TACACS+ pourra être envisagée pour renforcer davantage le niveau de sécurité de cette zone sensible.