## Analyse prélable de l'infrastructure à mettre en oeuvre GSB

- En vous aidant du document 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.
- Réalisez le schéma réseau logique représentant l'infrastructure que vous avez à mettre en œuvre pour les APs dans le contexte GSB. Vous devez préciser notamment les adresses IP de toutes les interfaces de l'UTM Stormshield ainsi que le plan d'adressage votre VLAN utilisateurs.

Pour cela aidez-vous du schéma global disponible dans les ressources des AP de 2e année : \* https://sioppes.lycees.nouvelle-aquitaine.pro/lib/exe/fetch.php/sisr/pages/sisr.ap3.2021\_2022/schema\_reseau\_gsb\_general.pdf Vous disposez également du fichier contenant le schéma modifiable avec l'application en ligne https://app.diagrams.net/

## Document : 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.

## Retour

• Mise en oeuvre de l'UTM Stormshield

From:

/ - Les cours du BTS SIO

Permanent link:

/doku.php/activite1analyse?rev=1664128064

Last update: 2022/09/25 19:47

