1. Mise en œuvre du filtrage pour le contexte GSB

Vous devez mettre en oeuvre une politique de filtrage protocolaire avec votre pare-feu Stormshield en tenant compte des recommandations de l'ANSSI.

1.1. Evolution de votre infrastructure

Vous devez placer dans le VLAN Serveurs :

- votre serveur Web GLPI
- votre serveur DNS

Pour cela respectez le plan d'adressage défini dans ce VLAN et utilisant les adresses IP statique mises à disposition de chaque équipes. Vous avez 4 adresses IP statiquse disponibles.

Lien : Ressources pour le APs

Vous devez placer dans le VLAN Utilisateurs un client Web d'administration.

- **Placez** vos deux VM Web et DNS dans le VLAN Serveurs ;
- **Modifiez** leur configuration IP
- **Vérifiez** que les VM accèdent à Internet et sont également accessibles depuis le réseau utilisateurs.

1.2. Mise en oeuvre d'une politique de filtrage

La mise en oeuvre de votre politique de filtrage doit s'appuyer sur les recommandations de l'ANSII.

1.2.1. Section 1 – Règles d’autorisation des flux à destination du pare-feu

- autoriser les flux d'administration (https 443 en TCP) depuis le poste administrateur vers le SBNSs serveurs (Web, résolveur DNS, serveur Web)
- un seul client doit pouvoir administrer le pare-feu depuis l'interface Web ou avec un accès SSH
- **autorisez** les flux vers
    - le serveur **Web** (http 80 en TCP) avec une **redirection de port**,
    - le serveur **résolveur DNS** (dns 53 en UDP) avec une **redirection de port**,

1.2.2. Section n°2 - Règles d’autorisation des flux émis par le pare-feu

Pour l'instant, ne définissez pas de règles

1.2.3. Section n°3 Règle de protection du pare-feu

- Cela est impératif pour prévenir l’ouverture de flux non légitimes à destination de la passerelle.
- journaliser cette règle afin de conserver la trace de ces flux illégitimes.

1.2.4. Section n°4 Règles d’autorisation des flux métiers

- pour l'instant autoriser les accès au Web (80, 443) sur Internet.
- et le serveur de temps de l'Université de Tours qui a l'adresse IP 193.52.212.3 et port UDP 123.
- autoriser les flux d'administration (22 SSH en TCP ; 3389 RDP en TCP - bureau à distance) depuis le poste administrateur vers les serveurs (Web, résolveur DNS, serveur Web)
- Interdire au PC d'administation l’accès à tout autre réseau (Ici Internet). En effet, ce poste ayant des privilèges élevés sur le réseau, le fait de lui bloquer entre autres l’accès internet permet de réduire considérablement sa surface d’attaque.
- pour pouvoir effectuer des tests, autorisez le protocole ICMP

1.2.5. Section n°5 Règles “antiparasites” (facultatif)

Pour l'instant, ne définissez pas de règles

1.2.6. Section n°6 Règle d'interdiction finale

L'ajout d'une règle explicite d'interdiction finale journalisée garantit l'application du modèle de sécurité positif (tout ce qui n'a pas été autorisé précédemment est interdit) et permet de conserver la trace des flux non légitimes.

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/activite4filtrage?rev=1667755231

Last update: **2022/11/06 17:20**