Objectif

L'objectif global de ce projet est de concrétiser les connaissances acquises dans le module « **Sécurité des réseaux informatiques** ».

Description

Une entreprise souhaite sécuriser son réseau dont l'architecture est décrite comme suit :

- Un réseau local.
- Un accès WAN.
- Deux serveurs FTP et Web placés dans un zone DMZ .

Les clients dans le réseau local sont autorisés à naviguer sur le web (le protocole http est autorisé dans le sens LAN_ WAN).

Chaque utilisateur dispose d'un **identifiant** et d'un **mot de passe** stockés dans une base locale.

Parfois des clients distants doivent se connecter sur le réseau local pour faire des transactions sécurisées et ceci en utilisant une connexion à travers un VPN.

L'administrateur réseau doit accéder depuis la machine LAN vers la zone DMZ moyennant le protocole **SSH**.

L'authentification entre le serveur **SSH** et son client doit se faire avec des clés pas avec des mots de passes.

NB : Les différents @IP à attribuer aux différents segments ainsi que le tunnel VPN sont mentionnés dans un document à envoyer aux étudiants (un plan d'adressage par étudiant).

Travail demandé

1. Reproduire l'architecture de réseau en utilisant des machines virtuelles **sous Linux**. On vous demande de faire la connectique physique nécessaire ainsi que la configuration du routage pour tester la connectivité entre les trois zones (LAN, WAN et DMZ).
   Vérifier la création d'un segment LAN différent pour chaque zone de la maquette.
2. Etablir la politique de filtrage à adoptée pour contrôler l'accès vers les différentes zones de cette maquette.
3. Rendre le serveur http en **HTTPS**.

4. Installer et configurer **pfsense** comme firewall pour sécuriser l'accès à travers les différentes zones.
5. Configurer sous **pfsense** l'authentification sécurisée des utilisateurs via la base de données locale.
6. Installer et configurer **openvpn** sur les deux machines LAN et WAN avec la configuration suivante : type d'encapsulation **udp** , type du tunnel **ethernet tunnel.**
7. Installer et configurer **openssh** sur la machine DMZ et un client SSH sur la machine LAN et configurer une **authentification par clé publique**.
8. Installer et configurer **snort** comme sonde IDS sur la machine LAN avec l'interface graphique **BASE**.
9. **Réaliser une cartographie de la maquette réseau avec les adresses IP, les services, Toute la plateforme est à base de Linux.**

Tests :

HTTPS

Tester l'accessibilité au service HTTPS à partir du LAN et du WAN.

pfsense

Test d'accès aux différents services suivant à partir des différentes zones :

- Accès vers le web à partir du LAN.
- Accès vers les serveurs publics à partir du LAN et du WAN.

Openvpn

- Test d'établissement du tunnel **VPN** entre les deux machines LAN et WAN.
- Visualiser avec **wireshark** le trafic échangé entre ces deux machines pour l'établissement du tunnel **VPN**.

Snort

Lancer deux attaques **arpspoofing** et **synflooding** sur le réseau et visualiser les deux alertes sur l'interface graphique de **snort**.

SSH

Test de l'ouverture d'un accès à distance à travers SSH depuis la machine LAN vers la DMZ.