Dawit ADAM Projet 1 : Environnement sécurité simulé via pare-feu

Thème : Réseau, cybersécurité, système

Mon premier projet consiste à simuler et sécuriser une petite entreprise dans un environnement virtualisé.

La première chose que j'ai mis en place ont été mes 3 cartes réseaux sur mon outil de virtualisation.

J'ai une carte réseau WAN par accès en pont via ma carte wifi permettant d'avoir un accès internet avec une attribution IP via DHCP, une carte réseau en LAN que j'ai nommé "LAN_FW" via une ip statique et une carte réseau pour ma DMZ aussi en ip statique .

La première machine virtuelle que j'ai crée est mon pfsense qui joue un rôle central dans la sécurité de mon entreprise virtuelle, il permet de filtrer les flux entrants et sortants à l'aide de règles adaptée à chacune de mes interfaces.

Sur mon LAN un accès internet est limité et contrôlé pour les postes utilisateurs de mon organisation, passage obligatoire par mon proxy pour filtrer les sites nécessaires et limiter les risques. Afin d'isoler les services exposés à Internet, j'ai mis en place une DMZ sur le pare-feu pfsense et qui héberge le serveur web windows IIS de l'organisation, elle permet de protéger le réseau interne tout en permettant aux externes d'accéder aux sites.

J'ai aussi mis en place un AD me permettant de centraliser la gestion des utilisateurs et des groupes de mon entreprise, cette AD est lié à mon pfsense via LDAP ce qui me permet de gérer les droits d'accès selon les groupes d'utilisateurs, dans cette AD j'ai simulé une petite organisation avec quelques utilisateurs et quelques services (développement, Rh, comptabilité) j'ai aussi créé un compte spécialement pour l'administration de l'AD, un compte de service pfsense et mis en place quelques GPO (bloquer

L'accès au panneau de configuration, gpo mot de passe ou encore fond d'écran). Côté cybersécurité, un IDS/IPS est intégré à mon pfsense afin de surveiller le trafic et détecter les tentatives d'intrusion ou de scans, cette solution permet de protéger le serveur web dans la DMZ, de bloquer les attaques depuis le WAN et de signaler toute activité suspecte sur le réseau interne.

Le projet comporte donc 4 machines virtuelles :

-VM PFSense

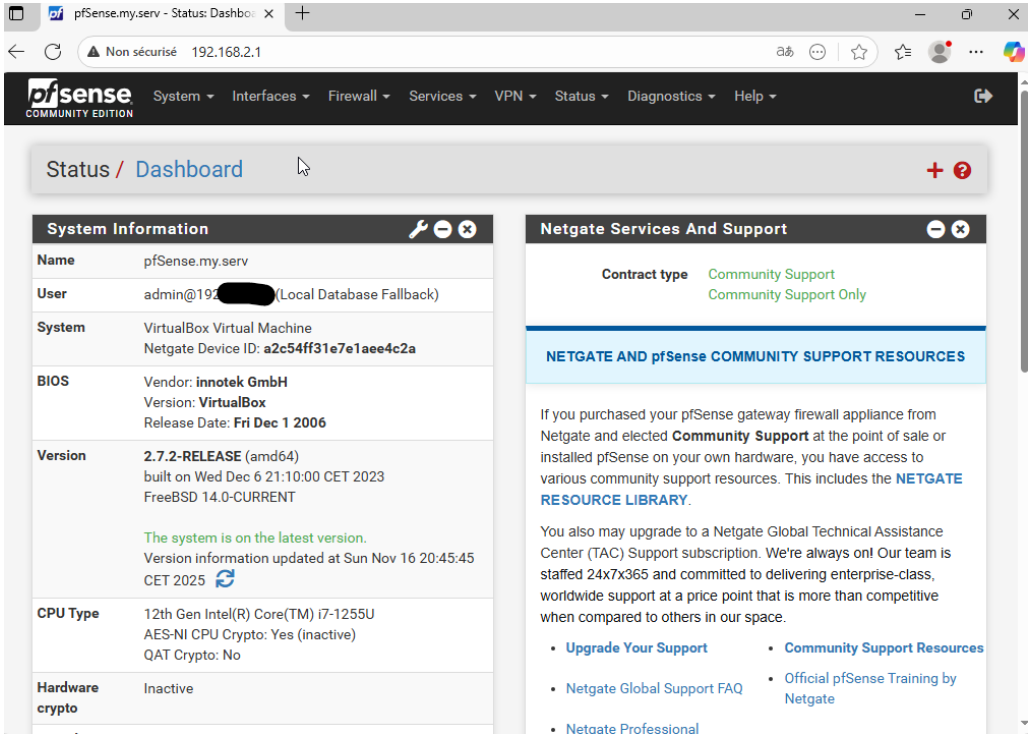
-VM Windows Server (et qui me sert à accéder à l'interface web pfsense et à mon AD)

-VM Server web (via IIS)

-VM Client (lié à mon AD qui me permet de tester mes configurations).

Screenshot de mon pfsense :

Mon interface web pfsense que j'administre via ma vm windows server :



Schema de mon infrascture réseau :