

# 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 créée 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 :

```
Bootup complete

FreeBSD/amd64 (pfSense.my.serv) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a2c54ff31e7e1aee4c2a

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.        '24
                           v6/DHCP6: 2001:861:3           7ff:fe6b:d68
0/64
LAN (lan)      -> em1          -> v4: 192.        ./24
DMZ (opt1)     -> em2          -> v4: 192.        ./24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: [
```

Mon interface web pfSense que j'administre via ma VM Windows Server :

The screenshot shows the pfSense web interface. At the top, there's a header bar with the pfSense logo and navigation links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the header, the main dashboard has two main sections:

- System Information:** Displays details about the server, including Name (pfSense.my.serv), User (admin@192.168.2.1), System (VirtualBox Virtual Machine, Netgate Device ID: a2c54ff31e7e1aee4c2a), BIOS (Vendor: innoteck GmbH, Version: VirtualBox, Release Date: Fri Dec 1 2006), Version (2.7.2-RELEASE (amd64), built on Wed Dec 6 21:10:00 CET 2023, FreeBSD 14.0-CURRENT), and CPU Type (12th Gen Intel(R) Core(TM) i7-1255U, AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No). It also shows a message: "The system is on the latest version." and "Version information updated at Sun Nov 16 20:45:45 CET 2025".
- Netgate Services And Support:** Shows Contract type (Community Support, Community Support Only) and a section titled "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES". This section contains text about community support resources and links to "Upgrade Your Support", "Community Support Resources", "Netgate Global Support FAQ", "Official pfSense Training by Netgate", and "Netgate Professional".

Schema de mon infrascture réseau :

