Fiche Projet : Architecture Réseau Sécurisée & Supervision (VLAN + VPN)



📋 Description du Projet

Mise en place d'une infrastructure réseau virtualisée sous **pfSense** visant à isoler un serveur de supervision **Nagios** au sein d'un VLAN dédié. L'accès à l'administration est restreint et sécurisé par un tunnel **OpenVPN**, empêchant toute connexion directe depuis le réseau local standard.

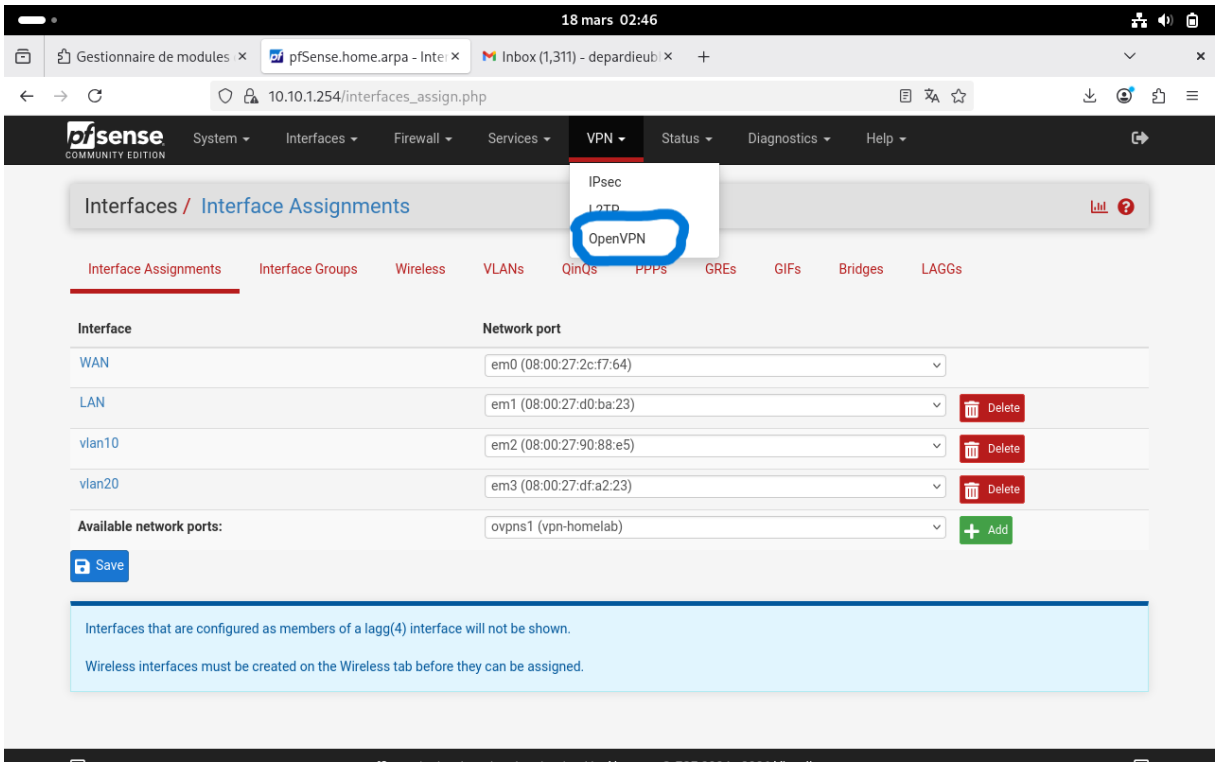
- **Environnement :** VirtualBox
- **Systèmes :** pfSense (Firewall), Debian 12 (Nagios), Windows 11 (Client)
- **Compétences clés :** Segmentation réseau (VLAN), Sécurité (VPN/Firewall), Supervision (SNMP/ICMP).

🛡️ 1. Segmentation et Architecture (VLANs)

Le cœur du réseau est géré par **pfSense**. J'ai créé plusieurs interfaces virtuelles pour segmenter les flux :

- **VLAN 10 & 20 :** Pour isoler les machines à superviser et le serveur Nagios.
- **Objectif :** Appliquer une politique de sécurité stricte où chaque zone est étanche.

Configuration des interfaces réseau et des VLANs sous l'interface pfSense.

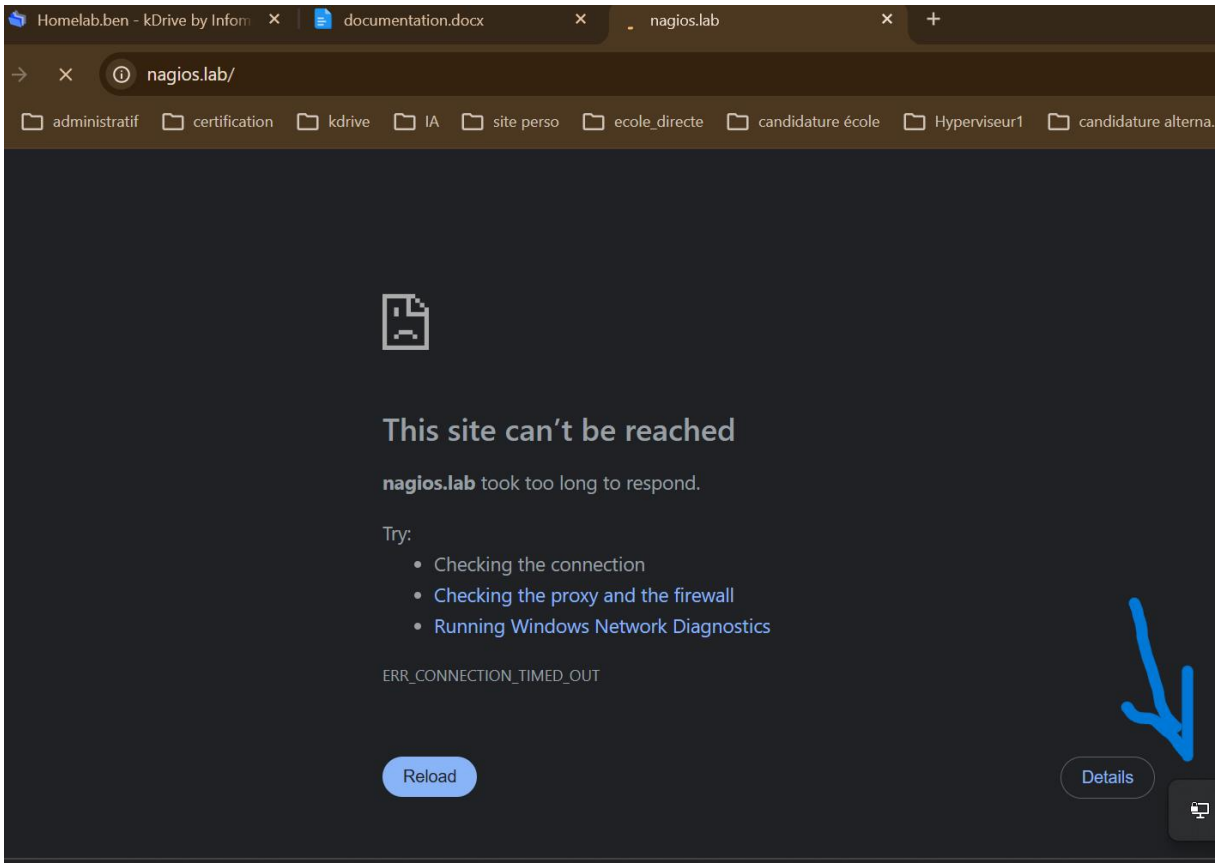


🔒 2. Accès Sécurisé via OpenVPN

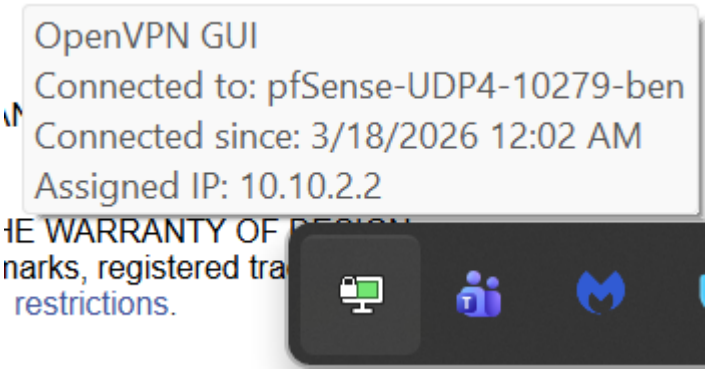
Pour administrer le serveur Nagios situé dans une zone protégée, l'utilisation d'un tunnel VPN est obligatoire.

- **Authentification :** Certificats SSL/TLS.
- **Sécurité :** Sans le tunnel actif, le serveur Nagios est totalement injoignable (Timeout), protégeant ainsi l'infrastructure contre les accès internes non autorisés.

Test d'accès sans VPN : Échec de la connexion (Site inaccessible).



Connexion établie : Le client reçoit l'IP 10.10.2.2 via le tunnel OpenVPN.

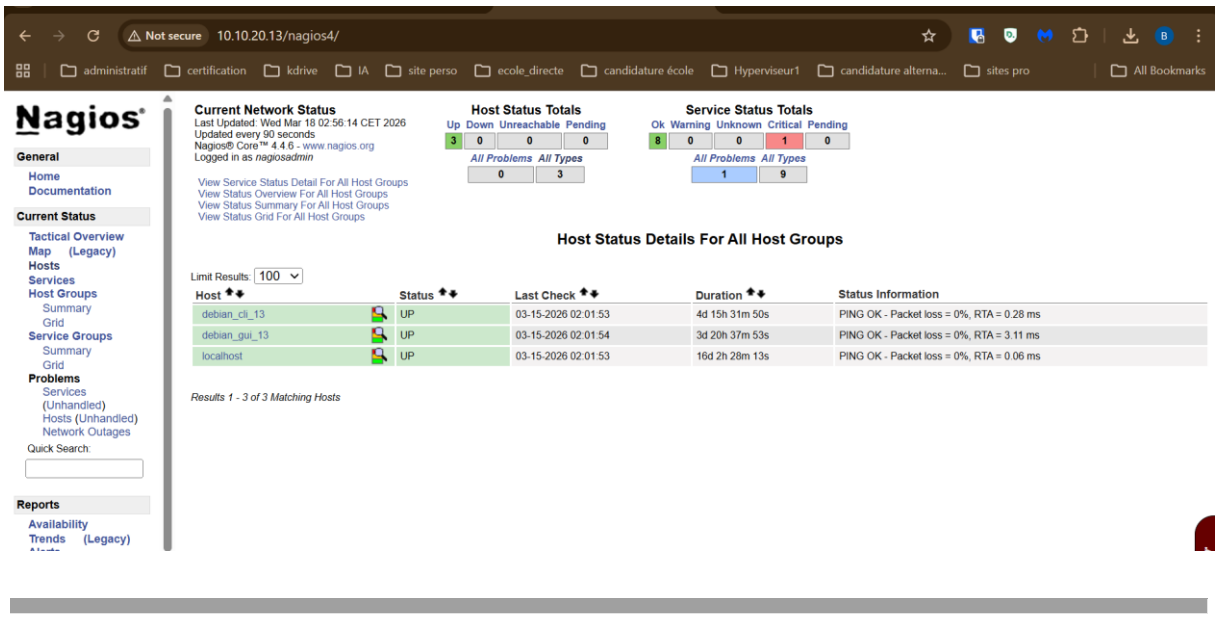


📊 3. Déploiement de la Supervision (Nagios)

Une fois le tunnel monté, le routage inter-VLAN permet d'accéder à l'interface de **Nagios Core 4**.

- **Configuration :** Définition des hôtes (Debian CLI, Debian GUI) et des services.
- **Monitoring :** Surveillance de l'état "UP/DOWN" et de la latence (RTT).

Dashboard Nagios validant la supervision active de l'ensemble du parc VM.

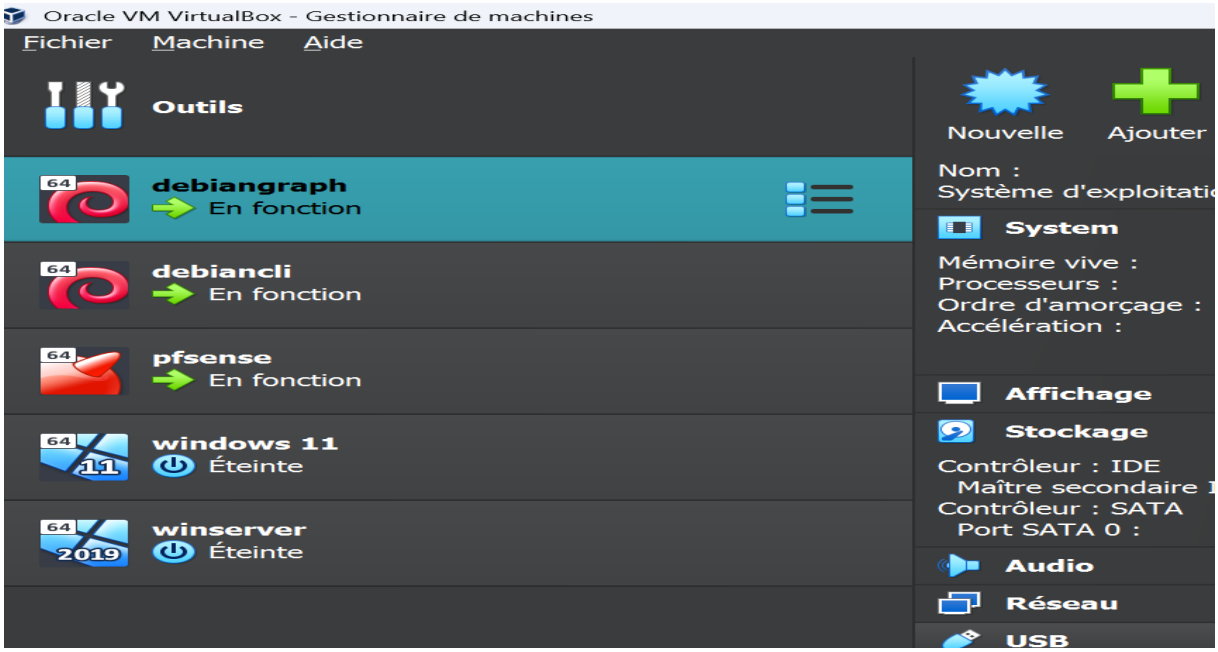


🛠 4. Gestion du parc et Dépannage

Le projet a nécessité une gestion rigoureuse des ressources sous VirtualBox et le debug des services Linux (Systemd).

- **Virtualisation :** Gestion de 5 VMs simultanées (pfSense, 2x Debian, Windows Server, Windows 11).
- **Analyse de logs :** Utilisation de journalctl et systemctl status pour valider le bon fonctionnement du démon Nagios.

Vue d'ensemble de l'infrastructure virtualisée sur VirtualBox.



Vérification du statut du service nagios4 via terminal SSH.

```
(c) Microsoft Corporation. All rights reserved.

C:\Users\depar>ssh nagios
ben@192.168.1.254's password:
Linux debian 6.12.73+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.73-1 (2026-02-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Mar 18 02:51:47 2026 from 192.168.1.14
ben@debian:~$ sudo systemctl status nagios4
[sudo] Mot de passe de ben :
● nagios4.service - nagios4
     Loaded: loaded (/usr/lib/systemd/system/nagios4.service; disabled; preset: enabled)
     Active: active (running) since Wed 2026-03-11 18:36:55 CET; 6 days ago
 Invocation: faccb7c0b40641c59881012b9c7e502e
       Docs: man:nagios4
    Process: 2278 ExecStartPre=sh -c nagiospipe=$$(sed -n "s/^command_file=\(.*\)/\1/p" ${NAGIOSCFG}); [ -z "$${nagiospipe}" -o ! -e
   Main PID: 2281 (nagios4)
      Tasks: 6 (limit: 1093)
     Memory: 21.8M (peak: 29.6M)
        CPU: 6min 43.032s
     CGroup: /system.slice/nagios4.service
             ├─2281 /usr/sbin/nagios4 /etc/nagios4/nagios.cfg
             ├─2282 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
             ├─2283 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
             ├─2284 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
             ├─2285 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
             └─2286 /usr/sbin/nagios4 /etc/nagios4/nagios.cfg
```

✅ Résultats obtenus

- **Isolation réussie :** Le serveur de supervision n'est plus exposé sur le LAN.
- **Accès distant sécurisé :** Seuls les utilisateurs avec certificat VPN peuvent administrer le réseau.

- **Visibilité totale :** Centralisation des alertes et de l'état de santé du réseau sur une interface unique.