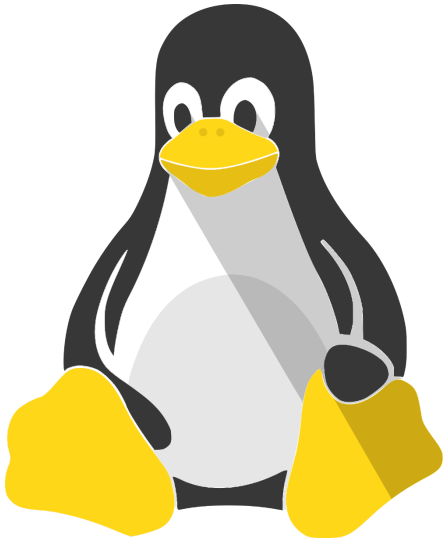
ATELIER PROFESSIONNEL n°4

Mise en place d'une solution antivirus client-serveur open source
Avec centralisation des logs et alertes automatisées

Konate Mamady

Projet AP4 – BTS SIO SISR



SOMMAIRE

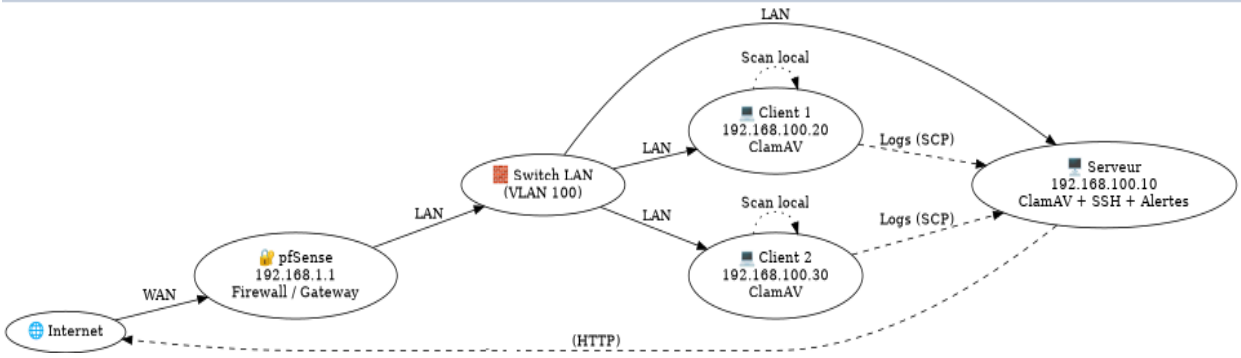
1. Objectifs du projet
2. Schéma réseau
3. Tableau d'adressage
4. Moyens matériels et logiciels
5. Procédure de déploiement
   5.1 Mise en place du serveur antivirus
   5.2 Déploiement des clients
   5.3 Centralisation des logs
   5.4 Mise en place des alertes
   5.5 Tests de validation
6. Conclusion

1. Objectifs du projet

L'objectif de ce projet est de mettre en place une solution antivirus open source permettant de sécuriser un parc informatique.

Objectifs techniques :
- Protection des postes clients et du serveur
- Mise à jour automatique des signatures
- Scan automatisé des systèmes
- Centralisation des logs antivirus
- Détection des infections
- Mise en place d'alertes automatiques

2. Schéma réseau



Le pare-feu pfSense permet l'accès à Internet et sécurise le réseau.

Le serveur antivirus, connecté au réseau local, centralise les logs envoyés par les clients via SCP.

Les clients effectuent des scans avec ClamAV et transmettent les résultats au serveur.

Le serveur analyse ces données et peut générer des alertes en cas de détection.

3. Tableau d’adressage

Équipement	Rôle	Interface	Réseau	Adresse IP	Masque	Passerelle
🌐 pfSense	Routeur / Firewall	WAN	192.168.1.0/24	DHCP	255.255.255.0	-
🌐 pfSense	Routeur / Firewall	LAN	192.168.100.0/24	192.168.100.1	255.255.255.0	-
🖥️ Serveur	Antivirus / Centralisation	ens192 (WAN)	192.168.1.0/24	DHCP	255.255.255.0	192.168.1.1
🖥️ Serveur	Antivirus / LAN	ens224	192.168.100.0/24	192.168.100.10	255.255.255.0	-
💻 Client 1	Poste utilisateur	ens192 (WAN)	192.168.1.0/24	DHCP	255.255.255.0	192.168.1.1
💻 Client 1	Poste utilisateur	ens224 (LAN)	192.168.100.0/24	192.168.100.20	255.255.255.0	-
💻 Client 2	Poste utilisateur	ens192 (WAN)	192.168.1.0/24	DHCP	255.255.255.0	192.168.1.1
💻 Client 2	Poste utilisateur	ens224 (LAN)	192.168.100.0/24	192.168.100.30	255.255.255.0	-

4. Moyens matériels et logiciels

Matériel :

🖥️ Serveur Debian : centralise les logs et gère l'antivirus

💻 Postes clients (x2) : effectuent les scans antivirus

🧱 Infrastructure vSphere : permet de virtualiser et tester le réseau

Logiciels :

🛡️ ClamAV

ClamAV est l'antivirus open source utilisé dans ce projet.
Il est installé sur le serveur et les clients afin de scanner les fichiers et détecter les menaces.

🔄 FreshClam

FreshClam est l'outil associé à ClamAV permettant de mettre à jour automatiquement les signatures antivirus.

🔐 OpenSSH

OpenSSH est utilisé pour permettre une communication sécurisée entre les clients et le serveur.
(Grâce au protocole SSH, les fichiers de logs sont transférés via SCP de manière chiffrée)

⏰ Cron

Cron est un service de planification de tâches sous Linux.
Il permet d'automatiser les scans antivirus et les scripts d'analyse sans intervention humaine.

5. Procédure de déploiement

5.1 Mise en place du serveur antivirus

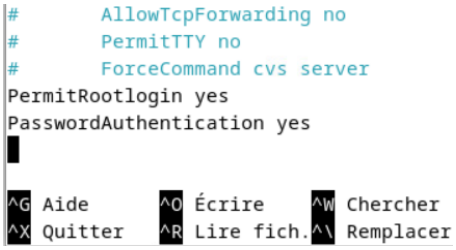
Installation :
apt update
apt install clamav clamav-daemon -y

Mise à jour :
freshclam

Installation SSH :
apt install openssh-server -y

Configuration :
nano /etc/ssh/sshd_config

Ajouter :
PermitRootLogin yes
PasswordAuthentication yes →



Redémarrage :
systemctl restart ssh

```
root@debian:~# clamscan --version
ClamAV 1.4.3/27944/Wed Mar 18 07:24:13 2026
root@debian:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Mon 2026-04-20 15:07:18 CEST; 2min 20s ago
```

d'après les commandes "clamscan –version" et "systemctl status ssh" nous montrent que ClamAV est bien installé, et que SSH est bien actif

5.2 Déploiement des clients

Installation :
apt install clamav -y

Scan :
clamscan -r /home

```
----------- SCAN SUMMARY -----------
Known viruses: 3627834
Engine version: 1.4.3
Scanned directories: 406
Scanned files: 2798
Infected files: 0
Data scanned: 205.45 MB
Data read: 168.81 MB (ratio 1.22:1)
Time: 76.700 sec (1 m 16 s)
Start Date: 2026:04:20 16:18:15
End Date:   2026:04:20 16:19:32
root@glpi:~#
```

5.3 Centralisation des logs

mkdir -p /var/log/antivirus/clients

scp /var/log/clamav/scan.log root@192.168.100.10:/var/log/antivirus/clients/client1.log

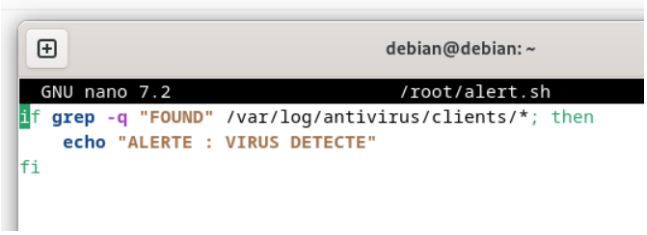
```
root@glpi:~# scp /var/log/clamav/scan.log root@192.168.100.10:/var/log/
antivirus/clients/client1.log
root@192.168.100.10's password:
scan.log                                      100% 9779KB   6.8MB/s
 00:01
root@glpi:~#
```

✔️ connexion SSH fonctionne

✔️ transfert SCP fonctionne

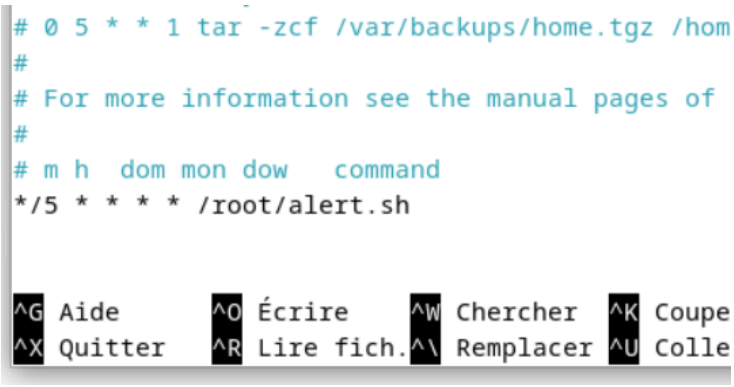
5.4 Mise en place des alertes

nano /root/alert.sh



crontab -e

*/5 * * * * /root/alert.sh

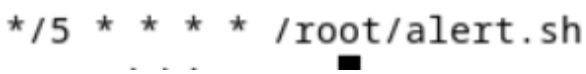


✔️ toutes les 5 minutes

✔️ toutes les heures

✔️ tous les jours

Pour vérifier que tout fonctionne, on peut faire la commande crontab -l, qui donera la réponse suivante



5.5 Tests de validation

ping 192.168.100.10

wget https://secure.eicar.org/eicar.com
clamscan eicar.com

Résultat attendu :

Eicar-Test-Signature FOUND

```
root@glpi:~# clamscan eicar.com
Loading:    11s, ETA:   0s [=========================>]    3.63M/3.63M
Compiling:   2s, ETA:   0s [=========================>]       41/41 tas

/root/eicar.com: Eicar-Test-Signature FOUND
```

6. Conclusion

Ce projet a permis de mettre en place une solution antivirus open source fonctionnelle basée sur une architecture client-serveur.

Il a permis de :

- sécuriser les postes clients grâce à des scans antivirus réguliers
- centraliser les logs de sécurité sur un serveur dédié
- automatiser les tâches grâce à l'utilisation de cron
- assurer des communications sécurisées via SSH et SCP
- détecter efficacement les menaces à l'aide de ClamAV

La mise en place d'un système d'alertes permet également une surveillance continue et une réaction rapide en cas d'infection.

Cette solution est efficace et évolutive, et peut être améliorée avec des outils de supervision plus avancés.