// Rapport de projet technique — BTS SIO option SISR

Environnement virtualisé sécurisé

Active Directory, pare-feu pfSense et tests d'intrusion — VMware

Auteur : Sahed Arshed Ali Khan

Formation : BTS SIO — option SISR, CFA Aurlom

Période : 2025

Environnement : VMware Workstation

ACTIVE DIRECTORY GPO PFSENSE / NAT / VPN KALI LINUX

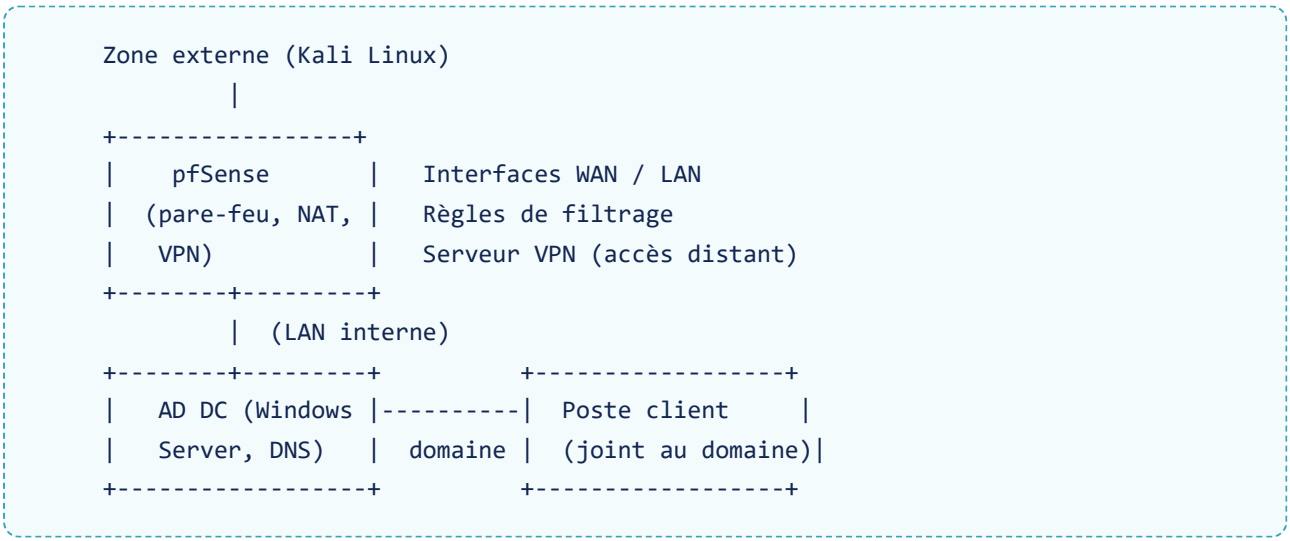
01. Contexte & objectifs

La plupart des PME reposent sur deux piliers pour la gestion de leur système d'information : un annuaire centralisé pour administrer utilisateurs et postes, et un pare-feu périmétrique pour protéger le réseau interne des menaces externes. Ce projet reconstitue ces deux briques dans un environnement virtualisé complet, avec pour objectif de maîtriser leur mise en œuvre et de valider leur robustesse par des tests d'intrusion.

> **OBJECTIFS TECHNIQUES VISÉS**
> Déploiement d'un contrôleur de domaine Active Directory (utilisateurs, OU, GPO) · mise en place d'un pare-feu pfSense en périphérie (règles de filtrage, NAT, VPN) · validation de la sécurité par des tests d'intrusion sous Kali Linux.

02. Architecture retenue

L'environnement est composé de quatre machines virtuelles représentant les différentes zones d'un réseau d'entreprise typique : la zone interne (annuaire et postes de travail), la zone périmétrique (pare-feu) et une zone externe simulant Internet, depuis laquelle sont menés les tests d'intrusion.



VM	RÔLE	OS	RÉSEAU
vm-dc01	Contrôleur de domaine (AD DS, DNS)	Windows Server	LAN interne
vm-client	Poste de travail joint au domaine	Windows	LAN interne
vm-pfsense	Pare-feu / routeur périphérique	pfSense	Interconnexion LAN / externe

VM	RÔLE	OS	RÉSEAU
vm-kali	Poste d'audit / tests d'intrusion	Kali Linux	Zone externe

03. Réalisation

Déploiement de l'annuaire

Installation du rôle AD DS et du service DNS associé sur le contrôleur de domaine, création de la structure d'unités d'organisation (OU) par service, création des comptes utilisateurs et des groupes de sécurité correspondants.

Stratégies de groupe (GPO)

Mise en place de plusieurs stratégies de groupe : politique de mot de passe (complexité, durée de vie), restrictions sur les postes de travail (panneau de configuration, exécution de programmes), et déploiement de scripts de connexion pour l'automatisation de tâches courantes (lecteurs réseau, mises à jour).

Jonction des postes

Jonction du poste client au domaine et vérification de l'application effective des GPO après ouverture de session.

Pare-feu périmétrique

Configuration de pfSense avec séparation claire des interfaces WAN/LAN, définition de règles de filtrage restreignant les flux entrants au strict nécessaire, mise en place de règles NAT pour l'accès sortant du réseau interne, et configuration d'un serveur VPN pour permettre un accès distant sécurisé.

Tests d'intrusion

Depuis une machine Kali Linux positionnée en zone externe, réalisation de scans réseau (Nmap) afin d'identifier les ports et services exposés par le pare-feu, dans une démarche d'audit de la surface d'attaque exposée.

04. Tests & validation

- **Application des GPO :** vérification sur le poste client que les stratégies de mot de passe et les restrictions sont bien appliquées après connexion au domaine.
- **Filtrage pfSense :** tentative de connexion sur des ports non autorisés depuis la zone externe — trafic bloqué comme attendu ; vérification des flux légitimes toujours autorisés.
- **VPN :** établissement d'une connexion VPN depuis un poste externe et vérification de l'accès aux ressources internes autorisées uniquement.

- **Audit Kali :** scan Nmap depuis la zone externe, analyse des ports détectés et confrontation avec les règles pfSense attendues.
- **Journalisation :** vérification des logs pfSense pour tracer les tentatives de connexion bloquées.

05. Conclusion

Ce projet a permis de couvrir les deux facettes complémentaires de la sécurité d'un système d'information : la gestion centralisée des identités et des postes via Active Directory, et la protection du périmètre réseau via pfSense. La phase de tests d'intrusion a permis d'adopter une posture d'audit, essentielle pour valider qu'une configuration de sécurité correspond réellement au niveau de protection visé plutôt que de se fier uniquement à la configuration déclarée.

> **COMPÉTENCES BTS SIO – SISR MOBILISÉES**
> Administration Active Directory (utilisateurs, OU, GPO) · configuration d'un pare-feu pfSense (filtrage, NAT, VPN) · sensibilisation aux tests d'intrusion (Nmap, Kali Linux) · démarche d'audit et de durcissement de la sécurité.

Document rédigé dans le cadre du portfolio de synthèse — BTS SIO, option SISR. Projet réalisé en environnement de virtualisation VMware.