

JP CONSULTING · LAB TSSR · 2026

Projet d'Infrastructure Informatique d'Entreprise

Mon lab d'entreprise, de la formation à l'exercice du métier

Jean-Philippe Rebischung

octobre 2026

SOMMAIRE

Présentation **3**

La carte du Lab **4**

1. Le socle : virtualisation, réseau et pare-feu **5**

1.1 La virtualisation 5

1.2 Le plan d'adressage 5

1.3 Le pare-feu pfSense 6

2. Les deux domaines d'identité **7**

2.1 Le domaine Windows : Active Directory 7

2.2 Le domaine Linux : FreeIPA 8

2.3 L'approbation entre les deux 8

3. Les deux sites et les VPN **9**

3.1 Le site B sous Proxmox 9

3.2 Le tunnel IPsec entre les deux sites 9

3.3 L'accès distant OpenVPN 9

4. Journaux et détection **10**

4.1 Le collecteur rsyslog 10

4.2 Sysmon et NXLog sur Windows 10

4.3 Suricata sur les pare-feux 10

5. Supervision, tickets et automatisation **12**

5.1 Zabbix 12

5.2 GLPI 12

5.3 Ansible et le durcissement SSH 12

6. Les rôles Windows d'entreprise et les certificats **13**

6.1 Fichiers et droits 13

6.2 Postes et mises à jour 13

6.3 L'autorité de certification 13

6.4 Sauvegarde et restauration 14

7. La cybersécurité : les deux postes Kali **14**

7.1 Deux Kali, deux points de vue 14

7.2 Pourquoi les Kali restent hors domaine 15

7.3 Wireshark : lire ce qui circule 15

7.4 Attaquer pour vérifier : deux exemples 16

7.5 Détecter, journaliser, comprendre : la boucle complète 16

7.6 D'autres attaques que le Lab permet de rejouer 17

Conclusion **19**

Les limites du projet 19

Présentation

Ce projet a été réalisé dans le cadre de ma formation au titre professionnel de Technicien Supérieur Systèmes et Réseaux. Au départ, il permettait de présenter, en partie, l'infrastructure informatique d'une petite entreprise mettant en évidence une grande partie des connaissances acquises pendant cette formation.

Par la suite, je me suis posé la question : *Pourquoi s'arrêter là ?*

J'avais déjà la base de l'architecture, un environnement Windows régi par Windows Server avec les rôles Active Directory, DNS, DHCP, des postes clients, un routeur, des outils de supervision, de sauvegarde, de ticketing.

J'avais également quelques machines virtuelles sous environnement Linux, des distributions comme Ubuntu, Mint, Kali et Oracle qui avaient servi pendant ma formation, mais qui n'apportaient rien de concret si ce n'est que de développer mes compétences en matière de script.

J'ai donc eu l'idée d'étoffer ce « Lab ». J'avais un domaine Windows fonctionnel mais limité, alors j'ai ajouté des rôles supplémentaires à Windows Server, (tout ce que l'on peut retrouver en entreprise), des postes clients, j'ai développé le routeur (pfSense), puis j'ai créé un domaine sous Linux avec les autres machines virtuelles.

Pour mener à bien ce projet, j'ai utilisé mon ordinateur personnel avec l'installation d'un hyperviseur de type 2, VMware Workstation. J'ai également recyclé un ancien PC qui tournait sous Windows 7 et que j'ai transformé en hyperviseur de type 1 avec Proxmox. Pendant la formation, nous avions appris à utiliser les outils VMware (Workstation, ESXi, vCenter), l'utilisation de Proxmox m'a permis d'étendre mes connaissances à d'autres logiciels.

Tout ceci est bien beau, avoir un domaine Windows et un domaine Linux, je découvre de nouvelles choses, mais au fond dans quel but.

Tout simplement dans le but de pouvoir m'exercer à mon métier de Technicien Supérieur Systèmes et Réseaux, de développer mes connaissances et mes compétences, d'en acquérir de nouvelles et de pouvoir être rapidement opérationnel pour exercer ce métier dans les meilleures conditions.

Je vais donc vous présenter mon projet, ce « Lab », comment il est constitué, les chantiers dans l'ordre où ils se sont construits : le socle (virtualisation et pare-feu), les deux domaines d'identité, les deux sites et leurs VPN, les journaux et la détection, la supervision et l'automatisation, les rôles Windows d'entreprise et les certificats, enfin la cybersécurité avec les deux postes Kali. Les annexes regroupent le lexique, des questions de compréhension, la liste des pannes rencontrées et l'index des fiches.

La carte du Lab

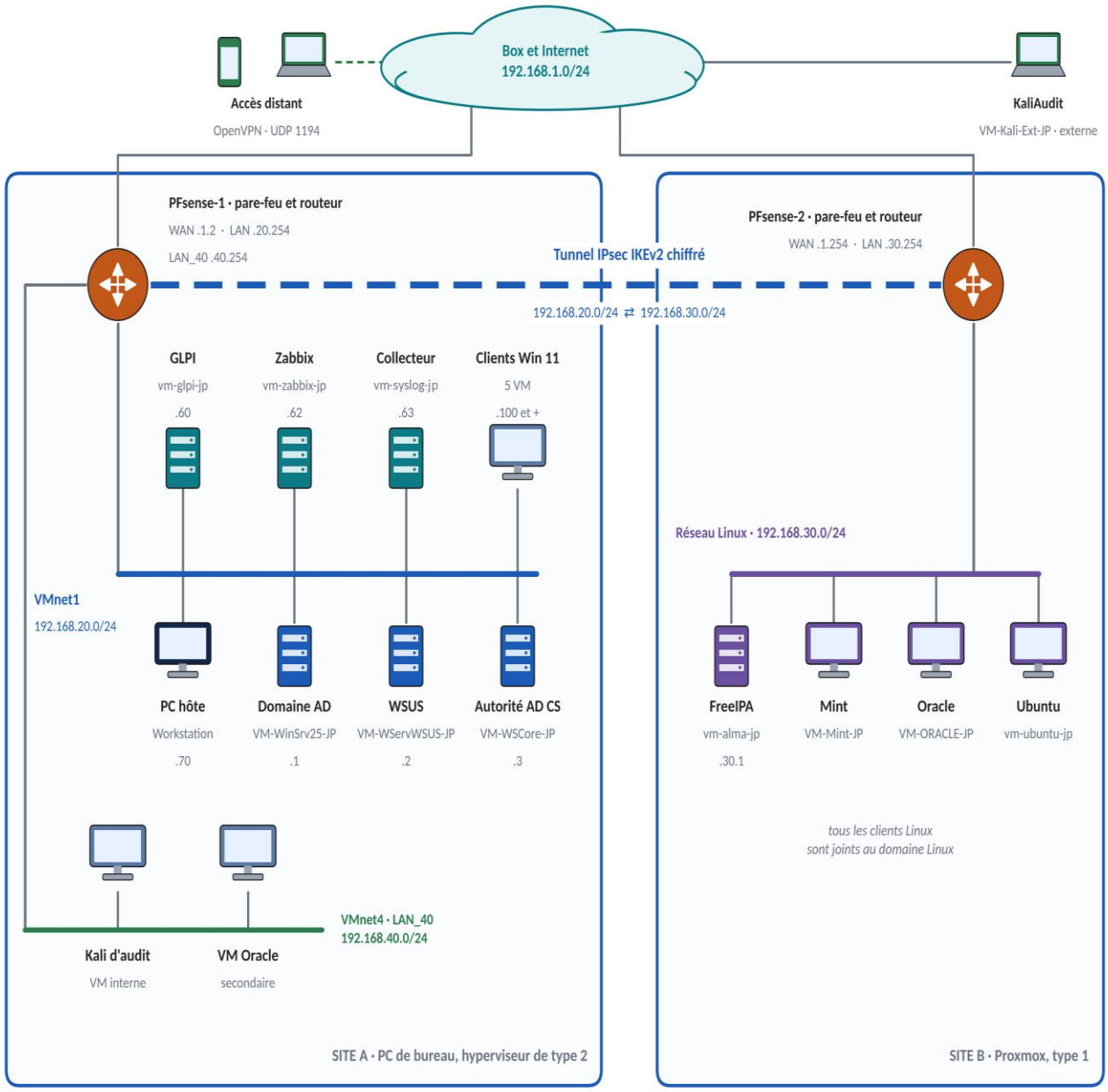


Figure 1 — Carte du Lab : deux sites reliés par un tunnel IPsec, un accès distant et un poste externe.

Ce Lab comporte **deux sites**. Le **site A** est mon PC de bureau : l'hyperviseur VMware Workstation y héberge le domaine Windows, les serveurs d'outils (GLPI, Zabbix, collecteur de journaux), l'autorité de certification et les postes clients. Le **site B** est un second ordinateur, plus modeste, sous **Proxmox VE** : il héberge le domaine Linux, géré par FreeIPA, et ses clients.

Chaque site est protégé par son propre pare-feu **pfSense**. Les deux pare-feux sont reliés par un **tunnel IPsec** chiffré, ce qui permet aux deux domaines de se parler comme s'ils étaient sur le même réseau. Un **accès distant OpenVPN** me permet de rejoindre le Lab depuis l'extérieur, et une machine Kali placée côté Internet joue le rôle de l'attaquant pour tester les défenses.

1. Le socle : virtualisation, réseau et pare-feu

1.1 La virtualisation

Le site A repose sur **VMware Workstation**, un **hyperviseur de type 2** : il s'exécute comme un programme dans Windows 11, sur un PC équipé d'un processeur i7-11700K et de 32 Go de mémoire. Chaque serveur ou poste du Lab est une **machine virtuelle**. Les machines sont réparties sur des **réseaux virtuels** (VMnet) isolés les uns des autres :

- **VMnet1** (192.168.20.0/24) : le réseau Windows et les serveurs d'outils ;
- **VMnet4** (192.168.40.0/24, appelé LAN_40) : un réseau de tests, isolé ;
- **VMnet0** : un pont vers la box, pour la sortie sur Internet.

Rien ne passe d'un réseau à l'autre sans traverser pfSense. C'est ce qui permet de décider, flux par flux, ce qui est autorisé.

1.2 Le plan d'adressage

Réseau	Rôle	Passerelle	Remarque
192.168.1.0/24	Box et Internet (WAN des deux pfSense)	la box	PFsense-1 en .2, PFsense-2 en .254, hôte Proxmox en .18
192.168.20.0/24	Site A : domaine Windows et outils (VMnet1)	192.168.20.254	serveurs en .1 à .3 et .60 à .70, clients dès .100
192.168.30.0/24	Site B : domaine Linux	192.168.30.254	FreeIPA en .30.1
192.168.40.0/24	LAN_40 : machines de test (VMnet4)	192.168.40.254	réseau isolé

Les serveurs ont des **adresses fixes**, placées hors de la plage distribuée par le DHCP (les adresses .10 à .99 sont exclues de l'étendue). Les postes clients reçoivent leur adresse du DHCP, à partir de .100.

1.3 Le pare-feu pfSense

pfSense est à la fois le pare-feu et le routeur de chaque site. Celui du site A, PFsense-1 (version 2.7.2), a trois pattes : le WAN (192.168.1.2), le LAN (192.168.20.254) et LAN_40 (192.168.40.254). Il fait aussi de la **traduction d'adresses (NAT)** pour la sortie Internet et héberge le serveur OpenVPN.

Ma méthode de filtrage : **tout ce qui n'est pas explicitement autorisé est bloqué**, et les règles sont écrites à partir des **flux observés** dans le journal du pare-feu, pas à partir d'hypothèses. Quand quelque chose ne passe pas, le journal donne le numéro de la règle qui bloque ; quand j'ouvre un flux, je l'ouvre pour une source, une destination et un port précis.

> **Dans le Lab**
>
> Les deux pfSense journalisent leur activité vers le collecteur central (chapitre 4) et sont surveillés par Zabbix (chapitre 5). Leur interface web est servie en HTTPS avec un certificat de l'autorité interne (chapitre 6).

2. Les deux domaines d'identité

Une infrastructure d'entreprise s'organise autour d'un **annuaire** : un registre central des comptes, des machines et des droits. Le Lab en compte deux, un par monde : Windows et Linux.

2.1 Le domaine Windows : Active Directory

Le domaine **domaineJP.infra** est porté par un contrôleur de domaine sous Windows Server 2025, `VM-WinSrv25-JP` (192.168.20.1), qui cumule trois rôles : **AD DS** (l'annuaire), **DNS** (la résolution de noms, dont les enregistrements de localisation des services du domaine) et **DHCP** (la distribution des adresses, avec exclusions, réservations et options de passerelle, de DNS et de suffixe). Son rôle d'**émulateur PDC** se synchronise sur pool.ntp.org : les domaines Kerberos exigent des horloges accordées.

L'annuaire est organisé en **UO** (unités d'organisation) et en groupes de sécurité selon le modèle **AGDLP**. Les **GPO** appliquent les réglages aux postes et aux utilisateurs : mappage de lecteurs, fond d'écran, déploiement de logiciels, mises à jour. Les postes Windows 11 sont joints au domaine.

Le domaine compte **sept GPO** : les deux GPO par défaut (domaine et contrôleurs de domaine) et cinq GPO créées pour le Lab. Leur nom dit quelle moitié sert, « Utilisateurs - … » ou « Ordinateurs - … », l'autre moitié étant désactivée. Une GPO se crée, se **lie** à une UO, puis s'applique ; créée mais non liée, elle ne fait rien.

GPO	Liée à	Ce qu'elle fait
WSUS - Serveurs	Serveurs et contrôleurs de domaine	Adresse du serveur de mises à jour (HTTPS, port 8531), groupe cible « Serveurs », téléchargement automatique, installation décidée par l'administrateur
WSUS - Postes	Postes de travail	Même serveur, groupe « Postes de travail », installation tous les jours à 12 h
Utilisateurs - Mappage lecteurs	JP Consulting	Lecteur P: (Commun) pour tous, lecteur I: (Informatique) réservé au groupe Informatique par ciblage au niveau de l'élément
Ordinateurs - LAPS	Postes et serveurs	Mot de passe administrateur local de 14 caractères, renouvelé tous les 30 jours, stocké chiffré dans l'annuaire
Utilisateurs - Imprimantes	JP Consulting	Connecte l'imprimante partagée du serveur d'impression et la définit par défaut

Quand une GPO ne s'applique pas, la commande `gpresult` indique où chercher : **absente**, c'est le lien ou l'emplacement ; **refusée**, le filtrage de sécurité ou la délégation ; **appliquée sans effet**, les paramètres eux-mêmes. J'ai provoqué volontairement la panne classique du correctif **MS16-072** :

une fois le filtrage réduit à un seul groupe, la GPO était refusée pour « raison inconnue », parce que depuis 2016 une GPO utilisateur est lue avec l'identité de l'ordinateur ; il fallait redonner la lecture aux ordinateurs du domaine.

2.2 Le domaine Linux : FreeIPA

Le domaine **domainejp-linux.infra** est géré par **FreeIPA** (version 4.13.1), installé sur AlmaLinux 10.2 dans la machine `VM-Alma-JP` du site B. FreeIPA réunit un annuaire LDAP, une autorité Kerberos, un DNS et une gestion des droits **sudo par rôle**. Les clients Linux (Oracle Linux, Linux Mint, Ubuntu) sont joints au domaine avec **ipa-client-install** : un seul compte, une seule politique, au lieu de comptes locaux qui divergent.

2.3 L'approbation entre les deux

Les deux domaines sont reliés par une **approbation unidirectionnelle** : FreeIPA fait confiance à Active Directory. Un compte Windows peut donc ouvrir une session sur une machine Linux sans être recréé. L'approbation s'appuie sur plusieurs ports ouverts entre les deux sites (DNS, Kerberos, LDAP, SMB, RPC et catalogue global) et sur une correspondance d'identifiants : l'UID Linux d'un compte AD vaut 1366800000 plus son **RID**.

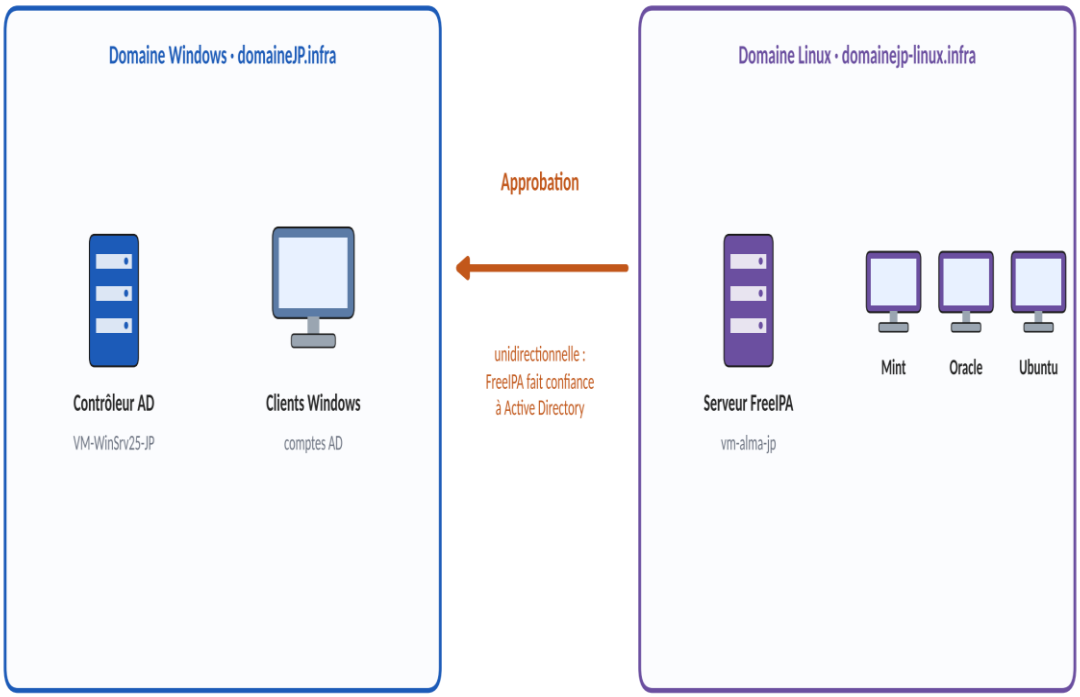


Figure 2 — L'approbation entre les deux domaines : FreeIPA fait confiance à Active Directory.

3. Les deux sites et les VPN

3.1 Le site B sous Proxmox

Le site B est un ordinateur de 2014 (i5-4690K, 16 Go) sous **Proxmox VE**, un **hyperviseur de type 1** : il est installé directement sur le matériel, sans système d'exploitation intermédiaire. Il est joignable en 192.168.1.18. Les machines Linux, d'abord hébergées sur VMware, y ont été **migrées** : conversion du disque virtuel, création de la machine avec la même adresse MAC, démarrage, puis correction du nom de l'interface réseau et installation de l'agent invité. La migration d'une machine n'est considérée comme finie que lorsque ses flux, ses journaux, sa supervision et sa sauvegarde sont revérifiés.

Les machines sont sauvegardées avec **vzdump**, l'outil de sauvegarde intégré à Proxmox.

3.2 Le tunnel IPsec entre les deux sites

Le site A et le site B sont reliés par un **tunnel IPsec** entre PFsense-1 et PFsense-2, qui relie 192.168.20.0/24 à 192.168.30.0/24. C'est lui qui permet l'approbation entre les deux domaines et la remontée des journaux.

3.3 L'accès distant OpenVPN

Pour travailler depuis l'extérieur, j'ai monté un **serveur OpenVPN** sur PFsense-1. Chaque appareil (PC portable, téléphone) possède son propre certificat, délivré par une autorité dédiée. Le principe du moindre privilège s'applique : le VPN n'atteint que le PC hôte, où j'ouvre une session Bureau à distance, et rien d'autre du Lab.

	Tunnel IPsec	OpenVPN
Usage	relier les deux sites	accès distant depuis un PC portable ou un téléphone
Protocole	IKEv2	UDP 1194
Chiffrement et identification	AES256-GCM, SHA256, DH 14, PFS 14, clé pré-partagée	tls-crypt, un certificat par appareil
Portée	192.168.20.0/24 et 192.168.30.0/24	uniquement le PC hôte (Bureau à distance)
Maintien	PFsense-1 initie le tunnel en permanence ; une tâche Cron surveille son état toutes les 5 minutes	à la demande du client

4. Journaux et détection

Centraliser les journaux, c'est pouvoir relire ce qui s'est passé sur une machine même quand elle ne répond plus, et comparer plusieurs machines entre elles. Tout part vers un seul point : le **collecteur**.

4.1 Le collecteur rsyslog

Le collecteur est la machine `VM-syslog-JP` (192.168.20.63), sous **rsyslog**. Il reçoit les journaux par trois canaux selon la nature de la source :

- **RELP avec TLS mutuel, port 20514** : sept machines Linux. Chaque émettrice présente son propre certificat, et le collecteur n'accepte que les noms de sa liste (`tls.permittedPeer`) ;
- **syslog en TLS, port 6514** : les trois serveurs Windows, par l'intermédiaire de NXLog ;
- **syslog UDP, port 514** : les deux pfSense, au format RFC 5424.

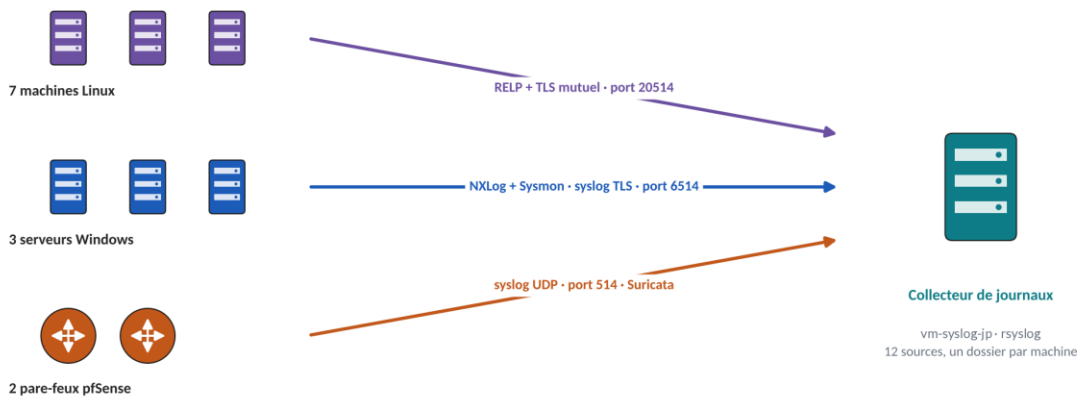


Figure 3 — Les trois canaux d'envoi des journaux vers le collecteur.

Le collecteur reçoit **12 sources**, range chaque machine dans son propre dossier, applique une rotation vérifiée et utilise des files d'attente sur disque pour ne rien perdre si la connexion tombe. Il stocke environ 79 Mo, sans aucun filtrage. Ce n'est **pas un SIEM** : il conserve et classe, il ne corrèle pas les événements et ne déclenche pas d'alerte.

4.2 Sysmon et NXLog sur Windows

Sur les trois serveurs Windows, **Sysmon** enrichit les événements du système (création de processus, connexions réseau) et **NXLog** les lit pour les envoyer au collecteur en TLS. La clé privée du certificat d'envoi est protégée par des droits restreints au système et aux administrateurs.

4.3 Suricata sur les pare-feux

Suricata est un système de détection d'intrusion installé sur PFsense-1 et sur PFsense-2, avec les règles **ET Open** (16 catégories). Il fonctionne en détection seule : l'option qui bloquerait automatiquement les sources d'alertes est désactivée, pour observer avant de bloquer. Pour vérifier la chaîne complète, j'ai déclenché une alerte de test (un User-Agent connu, SID 2008983) et retrouvé l'alerte dans les journaux du collecteur.

5. Supervision, tickets et automatisation

Outil	Rôle	Dans le Lab
Zabbix 7.4.15	supervision : état et mesures	agents sur les serveurs, SNMP v2c pour les pfSense, API de Proxmox avec un compte en lecture seule, surveillance de l'échéance d'un certificat
GLPI 10.0.28	inventaire et tickets	inventaire par agent (contrôleur de domaine), gestion des tickets
Ansible	automatisation de la configuration	playbooks de durcissement, d'environnement shell et de clés SSH

5.1 Zabbix

Zabbix tourne sur `VM-zabbix-JP` (Rocky Linux 9, 192.168.20.62). Il interroge les serveurs par des **agents**, les pare-feux par **SNMP**, et Proxmox par son API avec un compte limité à la lecture. L'interface est en HTTPS. Nagios XI, présenté dans mon Dossier Professionnel, est resté installé (192.168.20.61) mais n'est plus maintenu : Zabbix l'a remplacé. J'ai gardé NAGIOS XI pour superviser uniquement mon PC hôte, cela me permet de garder la main sur un logiciel vu en cours.

5.2 GLPI

GLPI (`VM-glpi-JP`, 192.168.20.60) sert à l'inventaire et au suivi des demandes. L'agent GLPI installé sur le contrôleur de domaine remonte l'inventaire de la machine, et plusieurs tickets complets sont traités de l'ouverture à leur clôture.

5.3 Ansible et le durcissement SSH

Ansible tourne sur la machine Alma, avec un inventaire de machines, des `group_vars` et des `host_vars`. Trois playbooks sont en service : `durcissement.yml` (SSH, pare-feu, fail2ban), `environnement_shell.yml` (invite et bannière) et `cles_ssh.yml` (clés publiques). Un playbook est **idempotent** : le rejouer ne change rien si la machine est déjà conforme, ce que prouve une simulation (`--check`) qui rend zéro modification.

Le **durcissement SSH** repose sur l'authentification par clé, un pare-feu local (`ufw` sur Debian et Ubuntu, `firewalld` sur la famille Red Hat) restreint aux sources utiles, et **fail2ban** pour bannir les tentatives répétées. Sur les serveurs Windows, OpenSSH est activé avec une règle de pare-feu limitée au poste d'administration.

6. Les rôles Windows d'entreprise et les certificats

6.1 Fichiers et droits

Les **partages de fichiers** suivent le modèle AGDLP : les comptes entrent dans des groupes globaux, eux-mêmes placés dans des groupes de domaine local qui portent les permissions NTFS. Les partages sont masqués aux personnes qui n'y ont pas accès (**ABE**), regroupés derrière un **espace de noms DFS** qui ne dépend d'aucun serveur en particulier, et encadrés par **FSRM** (quotas et filtrage de fichiers).

6.2 Postes et mises à jour

WSUS distribue les mises à jour Windows depuis un serveur interne, en HTTPS sur le port 8531. Le parc de postes Windows 11 est à la version 25H2, à l'exception d'un poste en 26H2, qui sert de poste test. **Windows LAPS** donne à chaque machine un mot de passe administrateur local unique et renouvelé, stocké dans l'annuaire. Un **serveur d'impression** complète le tableau.

WSUS en pratique. Le modèle est « tiré » : le serveur n'envoie rien, chaque poste vient chercher ce que l'administrateur a approuvé pour son groupe, « Serveurs » ou « Postes de travail ». La synchronisation avec Microsoft est manuelle, le Lab n'étant pas allumé en permanence ; elle ne rapatrie que les descriptions des mises à jour, et les fichiers ne sont téléchargés qu'après approbation. Les produits suivis sont Windows 11 et Windows Server 2025. La mise à niveau de version de Windows 11 (de la 23H2 à la 25H2) est passée par WSUS sur le poste pilote ; elle a buté sur l'erreur 0xC1900107, un nettoyage de tentative précédente resté en attente, corrigé en vidant les dossiers de Windows Update.

LAPS. Chaque machine gère elle-même un mot de passe administrateur local unique, de 14 caractères, renouvelé tous les 30 jours et rangé chiffré dans son objet ordinateur de l'annuaire. La mise en place tient en quatre gestes : étendre le schéma de l'annuaire (une seule fois), autoriser les machines d'une UO à écrire leur mot de passe, créer la GPO, puis lire le mot de passe le jour où l'on en a besoin. Un attaquant qui récupère le mot de passe d'un poste ne peut plus rebondir sur les autres.

Impression. Le serveur d'impression tourne sur la machine WSUS, jamais sur un contrôleur de domaine, où le spouleur est désactivé depuis les failles PrintNightmare. L'imprimante partagée IMP-Commun (port TCP/IP, pilote de classe Microsoft) est publiée dans l'annuaire et déployée par la GPO Utilisateurs - Imprimantes. L'imprimante du Lab est simulée : la chaîne de déploiement, elle, est réelle.

6.3 L'autorité de certification

Une **autorité de certification** interne (**AD CS**) est installée sur un serveur **Server Core**, `VM-WSCore-JP`. C'est une racine en ligne à un seul niveau, `JPConsulting-RootCA`, sans OCSP.

Elle délivre les certificats HTTPS des interfaces d'administration : GLPI, Zabbix, les deux pfSense, Proxmox et WSUS.

La **liste de révocation** (LCR) est publiée en HTTP, derrière un alias `pki` porté par la machine WSUS, en plus de LDAP : un pare-feu, un serveur Linux ou un poste hors domaine ne savent pas lire une adresse LDAP. J'ai testé la révocation d'un certificat : elle ne prend effet qu'au renouvellement de la liste chez chaque client.

IIS (Internet Information Services), le serveur web de Windows, tourne sur la machine WSUS. Il remplit deux rôles : héberger le site de WSUS, et publier les listes de révocation et le certificat de l'autorité, dans un dossier accessible en HTTP sous l'alias `pki`.

Le rôle **NPS** (RADIUS) a été installé et testé pour l'authentification de l'interface de pfSense. J'ai laissé la connexion web de pfSense sur la base locale : la faire dépendre d'un serveur qui n'est pas toujours allumé aurait été une erreur.

6.4 Sauvegarde et restauration

Le contrôleur de domaine est sauvegardé avec **Windows Server Backup**. Je me suis exercé à trois niveaux : la restauration d'un fichier, la récupération d'un objet supprimé avec la **corbeille Active Directory**, et la **restauration faisant autorité** d'une UO entière, réalisée en mode **DSRM** avec `wbadmin` et `ntdsutil`. La restauration complète d'un contrôleur sur un matériel vierge a été pratiquée lors d'un exercice de mise en situation.

J'utilise également le logiciel AOMEI Backupper pour mon ordinateur personnel. Comme il gère une grande partie de l'infrastructure, il est important que les sauvegardes soient faites régulièrement afin qu'en cas de problème il puisse être restauré.

Les deux pare-feux sont sauvegardés par l'export de leur configuration, un fichier XML. Je le chiffre à l'export, j'exclus les données de graphiques (RRD), j'inclus les clés SSH, puis je vérifie le chiffrement en ouvrant le fichier dans un éditeur de texte : il doit être illisible. Je refais l'export après chaque série de modifications (SNMP, journaux, Suricata, certificats HTTPS) et je range deux copies identiques, sur le disque interne du PC hôte. Ces fichiers pèsent quelques dizaines de Ko : après un sinistre, reconstruire un pare-feu de mémoire prendrait bien plus de temps que restaurer les serveurs.

Sur Proxmox, les six machines du site B sont sauvegardées avec vzdump, en mode snapshot (la machine reste allumée), compressées en zstd, vers un SSD externe. J'ai testé la restauration de la machine FreeIPA : une sauvegarde qui n'a jamais été restaurée n'est pas une sauvegarde.

Avant toute action importante ou risquée sur une machine virtuelle, quelle qu'elle soit, je prends un instantané (snapshot). Je l'ai fait sur GLPI avant la mise à jour en 10.0.28, et sur le contrôleur de domaine avant la restauration faisant autorité. Un instantané est un point de retour provisoire, pas une sauvegarde : il reste sur le même disque que la machine, et chaque écriture traverse la chaîne de fichiers de différences, qui ralentit la machine en grandissant. Je le supprime donc dès que la modification est validée. J'en ai déjà payé le prix : le contrôleur de domaine traînait cinq instantanés vieux de quatre mois.

7. La cybersécurité : les deux postes Kali

Une infrastructure ne se juge pas seulement à ce qu'elle fait fonctionner, mais aussi à ce qu'elle résiste à une attaque. Le Lab contient donc deux machines **Kali Linux**, une distribution conçue pour l'audit de sécurité, qui jouent le rôle de l'attaquant : elles servent à vérifier que les pare-feux, la détection d'intrusion et les journaux des chapitres précédents effectuent bien leur travail.

> **Règles du jeu**
>
> On ne teste que ce que l'on possède et que l'on a isolé. La cible est toujours désignée précisément, jamais un réseau entier. Les tests qui perturbent le réseau local (ARP, DHCP) se font sur un réseau isolé, jamais sur le réseau de la maison. La Kali externe est éteinte par défaut.

7.1 Deux Kali, deux points de vue

Une attaque ne vient pas toujours du même endroit. La première Kali arrive de l'extérieur et ne connaît rien du Lab ; la seconde représente ce qui se passe quand un poste de l'intérieur est tombé aux mains d'un attaquant.

	Kali externe	Kali interne
Machine	VM-Kali-Ext-JP, sur Proxmox (site B)	VM-Kali-int-JP, sur VMware (site A)
Réseau	Réseau de la box, face au WAN de PFsense-2, adresse reçue par DHCP	LAN_40, isolé, adresse fixe 192.168.40.103
Rôle	Attaquant venu de l'extérieur	Poste interne compromis, simulé
Question posée	Que voit et qu'atteint un inconnu depuis l'extérieur ?	Que peut atteindre un attaquant qui a pris pied sur un poste ?
Domaine	Hors domaine	Hors domaine

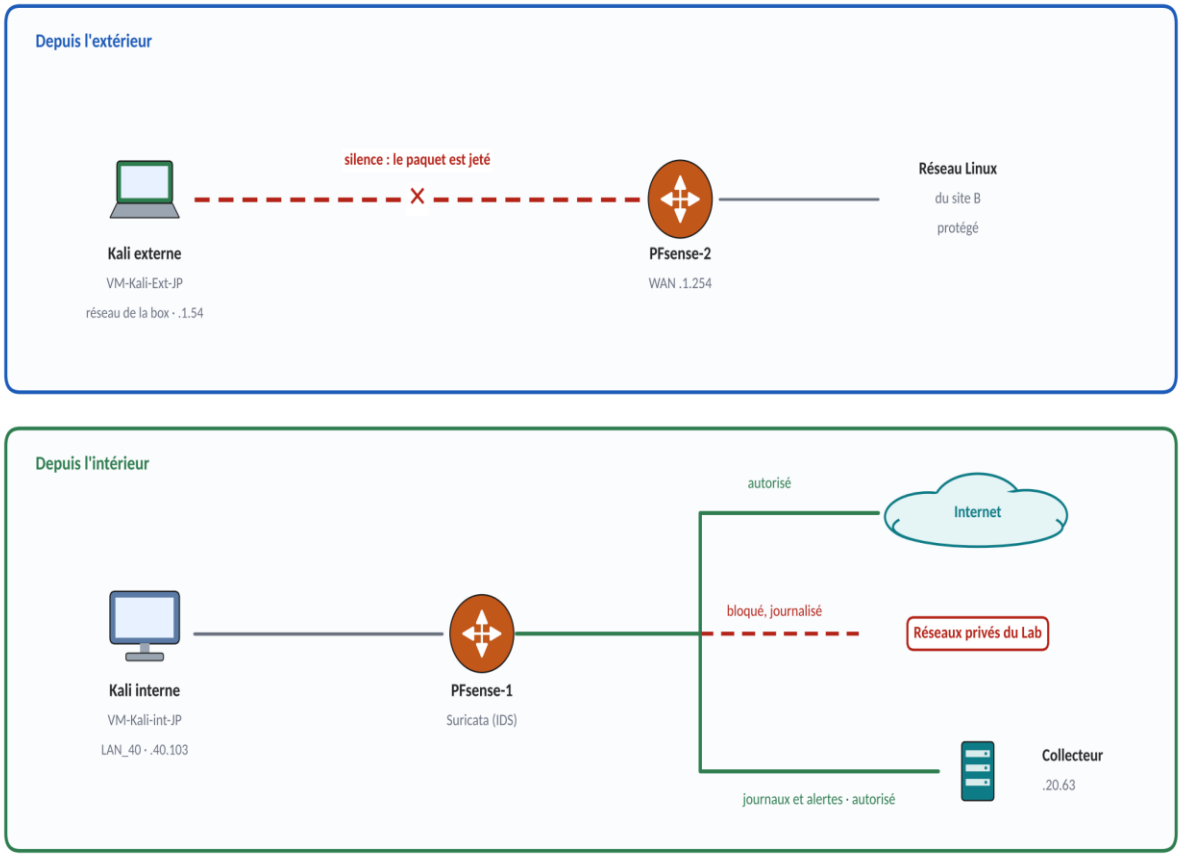


Figure 4 — Les deux Kali : l'externe face au WAN de PFsense-2, l'interne enfermée dans LAN_40 sous la surveillance de Suricata.

La Kali interne est la machine d'origine ; la Kali externe en est une copie. Pour que les deux ne se confondent pas, j'ai régénéré l'identité de l'une : nom d'hôte, identifiant de machine et clés SSH, l'équivalent Linux d'un Sysprep. La Kali interne envoie aussi ses journaux au collecteur, comme les autres machines Linux, car les journaux d'un poste compromis sont ceux que l'on veut voir dans un collecteur de sécurité.

7.2 Pourquoi les Kali restent hors domaine

J'ai d'abord essayé de joindre Kali au domaine Linux, comme les autres clients. Les paquets nécessaires à la jonction n'ont pas pu être installés : Kali est une distribution d'audit, elle n'est pas faite pour cet usage. Plutôt que de forcer, j'ai changé son rôle.

Ce choix est cohérent avec le métier : **une machine d'audit n'a rien à faire dans l'annuaire qu'elle audite.** Jointe au domaine, elle aurait une identité et des droits qu'un vrai attaquant n'a pas, et ses résultats seraient faussés. Elle reste donc extérieure, comme le serait un intrus, et aucune trace des Kali ne subsiste dans FreeIPA.

7.3 Wireshark : lire ce qui circule

Wireshark est un analyseur de trafic : il capture les paquets qui passent sur une carte réseau et les affiche un par un, décodés par protocole. Sa version en ligne de commande, **tshark**, analyse une capture dans un script. La Kali sert de poste d'analyse : Wireshark y est installé. Dans le Lab, il a servi à deux choses.

- **Lire une authentification Kerberos.** Sur une capture de 20 paquets, l'erreur PREAUTH_REQUIRED apparaît au milieu d'une connexion réussie : le client envoie une première demande sans preuve, le contrôleur de domaine en réclame une, le client la fournit et reçoit son ticket. Une erreur dans une capture ne prouve donc pas une panne. On y voit aussi que le mot de passe ne circule jamais, alors que le nom d'utilisateur et le domaine circulent en clair.
- **Établir la liste réelle des flux avant d'écrire les règles du pare-feu.** Une capture de 4 minutes d'usage normal, puis de 3 minutes sans rien faire : 674 paquets, analysés avec tshark. Le flux DNS du contrôleur de domaine vers FreeIPA, qui n'aurait jamais figuré dans une liste faite de mémoire, n'est apparu que parce que la capture tournait pendant que personne n'agissait.

7.4 Attaquer pour vérifier : deux exemples

Chaque test suit le même schéma : un objectif, une cible précise, et un résultat lu dans le pare-feu, dans Suricata ou dans les journaux.

Exemple 1 : la Kali externe face au pare-feu du site B. L'objectif est de savoir ce qu'un inconnu peut atteindre depuis l'extérieur. La Kali externe joint Internet, mais elle n'obtient aucune réponse de l'adresse WAN de PFsense-2 (192.168.1.254), pourtant sur le même réseau : le paquet est jeté sans un mot. Pour un attaquant, ce silence est tout ce qu'il y a à voir : il ne sait même pas si la machine existe. Il se lit « timed out » et non « refused » : une machine qui répond « refusé » existe, un pare-feu qui jette ne répond rien.

Exemple 2 : la Kali interne et l'audit du contrôleur de domaine. L'objectif est de voir le contrôleur comme un attaquant le verrait. Un scan nmap des ports courants a montré dix services ouverts (DNS, web, Kerberos, RPC, NetBIOS, LDAP, partages de fichiers, changement de mot de passe Kerberos, catalogue global, bureau à distance) et 92 ports « filtrés ». Sans aucune authentification, le scan a aussi appris le nom du domaine, le site et l'heure du serveur. Ce n'est pas une faille : l'annuaire (LDAP) et Kerberos doivent publier ces informations pour fonctionner. On limite cette exposition en cloisonnant le réseau, pas en désactivant le service.

Depuis LAN_40, le pare-feu ne laisse aujourd'hui à la Kali interne que le DNS vers le contrôleur de domaine, l'envoi de ses journaux au collecteur et la sortie vers Internet, sans aucun réseau privé. Le blocage est journalisé, et le journal du pare-feu prouve qu'une règle précise est responsable : un poste compromis du Lab ne peut pas rebondir vers les autres machines.

7.5 Détecter, journaliser, comprendre : la boucle complète

Une attaque simulée n'a de valeur que si elle laisse des traces exploitables. La chaîne du Lab est la suivante :

Étape	Outil	Ce que l'on observe
1. Attaque simulée	Kali (nmap, requête de test)	Un scan ou une requête volontairement suspecte
2. Filtrage	pfSense	Une règle autorise ou bloque ; le journal donne le numéro de la règle responsable
3. Détection	Suricata, règles ET Open	Une alerte, par exemple celle du User-Agent de test « BlackSun » (SID 2008983)
4. Centralisation	Collecteur rsyslog	L'alerte et les journaux du pare-feu sont retrouvés sur le collecteur, rangés par machine
5. Enseignement	Annexe C	Chaque anomalie rencontrée est notée avec sa cause

Cette boucle a une origine précise. Le premier scan lancé depuis Kali vers Mint n'a laissé aucune trace dans Suricata, alors installé sur une machine en simple écoute. Le commutateur virtuel n'envoie les trames qu'à leur destinataire, et le mode « espion » d'une carte permet d'accepter des trames qui ne lui sont pas adressées, pas d'en faire arriver. Conclusion : **un IDS doit être placé sur un point de passage obligé.** Il a donc été installé sur les deux pare-feux.

Pour vérifier la chaîne de bout en bout, un User-Agent connu déclenche l'alerte, qui remonte jusqu'au collecteur. Le jour où elle n'est pas arrivée, la cause était simple : l'interface de Suricata n'avait pas été redémarrée après le réglage. On a remonté la chaîne maillon par maillon.

7.6 D'autres attaques que le Lab permet de rejouer

Le même principe s'applique aux attaques courantes en entreprise. Le tableau indique, pour chacune, d'où elle part, ce qu'elle vise et ce que le Lab permet d'observer. Le pare-feu interdit par conception à la Kali interne d'atteindre les réseaux privés : pour certains tests, on déplace donc volontairement le poste d'audit dans le réseau testé, puis on le remet.

Attaque	Depuis	Cible	Ce que l'on observe
Force brute sur SSH	Une Kali placée sur le réseau des serveurs	Serveurs Linux avec fail2ban et pare-feu local	Les tentatives échouent, l'adresse est bannie, les échecs remontent au collecteur
Scan de ports et de services	Kali externe ou interne	Pare-feux et serveurs	Réponses « filtered », règle de blocage dans le journal, alerte Suricata
Sondage du VPN	Kali externe	Port UDP 1194 de PFsense-1	Aucun échange sans la clé tls-crypt : un paquet sans signature valide est ignoré, le port reste muet
Rebond depuis un poste compromis	Kali interne	Réseaux privés du Lab	Blocage journalisé par le pare-feu ; seule la sortie vers Internet est permise
Écoute du trafic non chiffré	Capture sur pfSense, lue dans Wireshark	SNMP v2c, syslog UDP 514	La communauté SNMP et les messages se lisent en clair : la raison de passer au SNMP v3 et à du syslog chiffré

Conclusion

Parti d'un dossier professionnel qui simulait une petite entreprise sur un seul PC, j'ai construit un Lab qui réunit les briques d'une infrastructure d'entreprise : deux sites reliés par VPN, deux annuaires, un pare-feu et un système de détection, des journaux centralisés, de la supervision, de l'inventaire, de l'automatisation, une autorité de certification et des sauvegardes testées. Chaque brique est documentée dans une fiche et a été vérifiée par un test, pas seulement installée.

Les limites du projet

Je préfère les dire honnêtement, je ne maîtrise pas l'ensemble des actions que j'ai menées, elles dépassent les compétences acquises pendant la formation. Pendant celle-ci, j'ai monté seul le premier domaine Windows, l'installation et la configuration des postes clients, de Windows Server et des rôles DNS, DHCP et Active Directory, ainsi que les UO et GPO, le routeur pfSense, les règles de pare-feu, l'outil de ticketing GLPI et les logiciels de sauvegarde (AOMEI Backupper) et de supervision (NAGIOS XI).

Pour la suite, j'ai installé Claude IA sur mon PC, cela m'a permis d'apprendre à utiliser Claude, de rédiger des prompts et de mener d'autres projets comme la construction d'un site Internet, la réalisation d'un petit film d'animation, le développement d'un logiciel de tri pour pouvoir faire le ménage sur mon ordinateur.

Attention : je n'ai pas cherché à ce que Claude fasse tout lui-même, je l'ai configuré pour qu'il m'apprenne à concevoir et à mettre en pratique ce Projet d'Infrastructure Informatique d'Entreprise. Je lui ai demandé d'agir comme un professeur afin d'apprendre et d'étoffer mes connaissances et de développer d'autres compétences. Je me sers également de Claude pour simuler des journées de travail d'un Technicien Systèmes et Réseaux afin de m'exercer sur ce Lab aux pratiques du métier.

C'est principalement dans ce but que j'ai entrepris ces chantiers afin de démontrer à un recruteur que même sans avoir de l'expérience professionnelle dans le domaine de l'informatique (qui reste indispensable, par la pratique, pour la maîtrise des compétences) il est malgré tout possible d'acquérir de l'expérience.

J'ai pris beaucoup de plaisir à mettre en place tout ça. Cela me conforte dans l'idée que ma reconversion professionnelle a un sens, pratiquer un métier que j'aime, qui m'attire et dans lequel j'ai envie de m'épanouir et d'évoluer.