Mise en place d'une Infrastructure Active Directory et Sécurité Réseau

Rapport Technique Détaillé - Phases 1 et 2

Guide d'installation, configuration et administration

Informations Projet

Réalisé par : Louay Njah , Maram Souidi , Bader Hamdi , Omar Karoui , Safia Nasr

Date : 1er février 2026

Table des matières

Introduction et Concepts Clés

1.1 Objectif du projet

L'objectif est de simuler un réseau d'entreprise réaliste. Dans un environnement réel, les ordinateurs ne sont pas connectés "en vrac". Ils sont gérés de manière centralisée pour garantir la sécurité. Nous allons construire ce réseau de zéro.

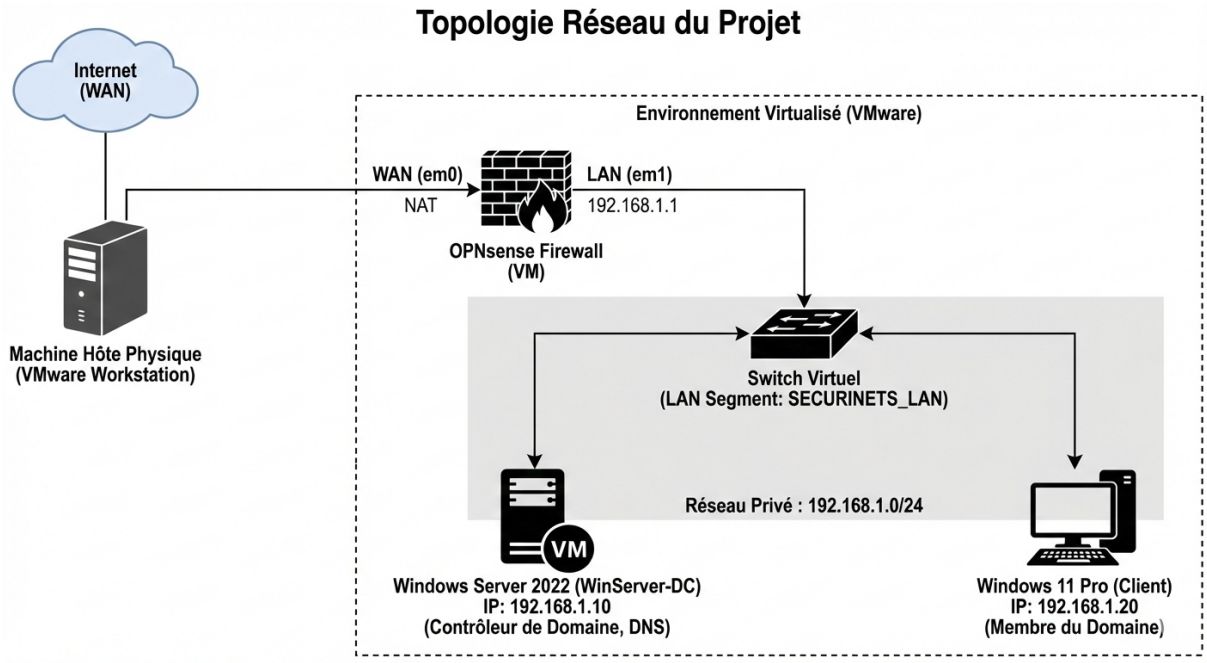

FIGURE 1.1 – Topologie réseaux du projet

1.2 Définitions des concepts utilisés

Pour comprendre la suite, voici les notions fondamentales mises en œuvre :

Virtualisation (VMware) : Technique permettant de créer des ordinateurs virtuels (VM) à l'intérieur d'un ordinateur physique. Cela permet de simuler un réseau complet (Serveurs, Clients, Routeurs) sur une seule machine.

Active Directory (AD) : C'est le "cerveau" du réseau Windows. C'est une base de données centralisée qui contient tous les utilisateurs, les mots de passe et les ordinateurs de l'entreprise.

Contrôleur de Domaine (DC) : C'est le serveur qui héberge l'Active Directory. C'est lui le "chef" du réseau.

DNS (Domain Name System) : C'est l'annuaire du réseau. Il traduit les noms (ex : `securinetsenit.local`) en adresses IP (ex : `192.168.1.10`). Sans DNS, les ordinateurs ne peuvent pas se trouver.

GPO (Group Policy Object) : Des "règles" envoyées par le serveur pour contrôler les PC à distance (ex : interdire le panneau de configuration, changer le fond d'écran).

Phase 1 : Infrastructure Réseau (Le Socle)

2.1 Configuration de l'Hyperviseur (VMware)

Avant d'installer les machines, nous devons créer les "câbles virtuels".

2.1.1 Création du LAN Segment

Nous n'utilisons pas le mode "Bridge" ou "NAT" par défaut pour le réseau interne, car nous voulons une isolation totale.

1. Dans VMware, clic-droit sur une VM > **Settings**.
2. Bouton **LAN Segments...**
3. Création d'un segment nommé : `SECURINETS_LAN`.

Ce segment agira comme un switch virtuel privé : seules les machines connectées à ce segment pourront se parler.

2.2 Mise en place du Pare-feu OPNsense

OPNsense est notre routeur de sécurité. Il fait le pont entre Internet et notre réseau privé.

2.2.1 Configuration des interfaces

La VM OPNsense dispose de deux cartes réseau :

— **WAN (em0) :** Connectée en NAT (pour avoir Internet depuis l'hôte).

— **LAN (em1) :** Connectée au `SECURINETS_LAN`.

Une configuration manuelle via la console a été nécessaire pour assigner l'adresse IP de la passerelle : **192.168.1.1**. Tous les futurs clients utiliseront cette adresse pour sortir sur Internet.

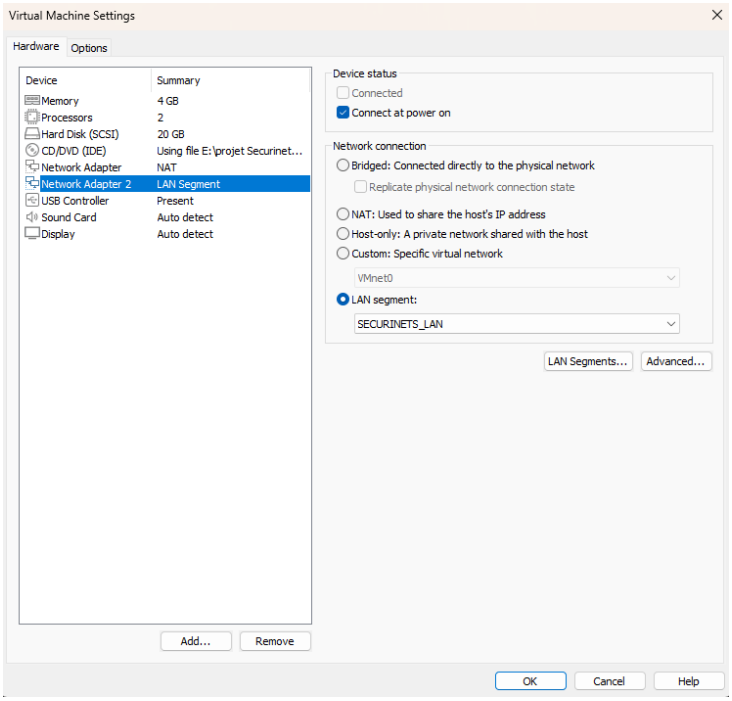

FIGURE 2.1 – Création du segment LAN isolé dans VMware

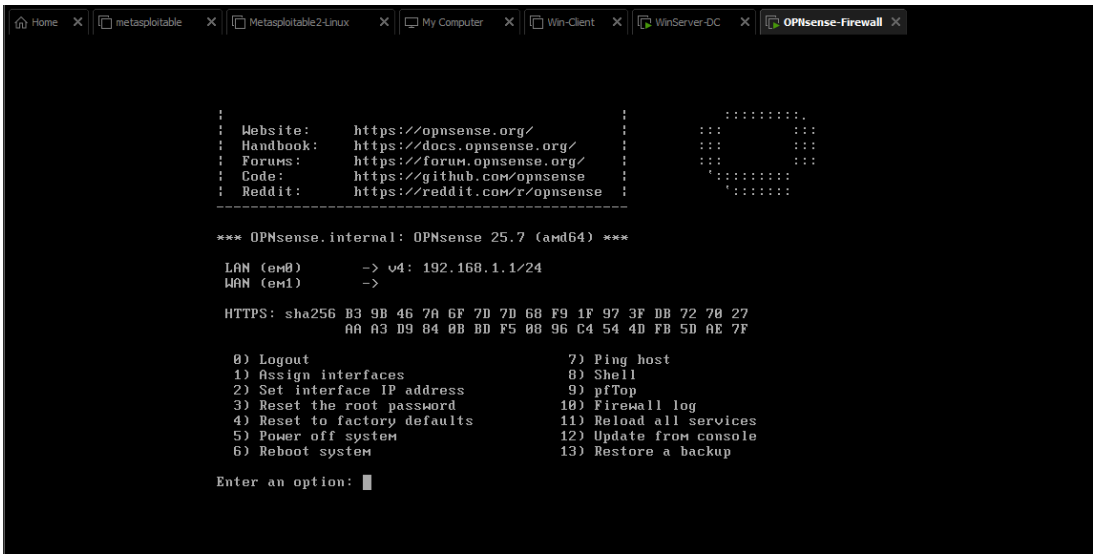

FIGURE 2.2 – Interface console OPNsense : Vérification des assignations WAN et LAN

Phase 2 : Installation du Cerveau (Active Directory)

3.1 Préparation de Windows Server 2022

Une fois Windows Server installé, trois étapes critiques sont nécessaires avant toute installation de rôle.

3.1.1 Adressage IP Statique

Un serveur ne doit jamais changer d'adresse IP.

— **IP :** 192.168.1.10

— **Masque :** 255.255.255.0

— **Passerelle :** 192.168.1.1 (L'IP d'OPNsense)

— **DNS :** 127.0.0.1 (Car le serveur sera son propre DNS)

3.1.2 Renommage du serveur

Le nom par défaut (ex : `WIN-458D...`) est incompréhensible. Nous l'avons renommé `WinServer-DC` pour identifier clairement son rôle de Contrôleur de Domaine (DC).

3.2 Installation du rôle AD DS

Dans le *Server Manager*, nous avons ajouté le rôle **Active Directory Domain Services**. Cela installe les fichiers nécessaires, mais le serveur n'est pas encore opérationnel.

3.3 Promotion du Serveur (Dcpromo)

C'est l'étape de transformation du serveur simple en Contrôleur de Domaine.

1. Dans le gestionnaire, cliquer sur le drapeau jaune (Notifications).
2. Choisir **"Promote this server to a domain controller"**.
3. Sélectionner **"Add a new forest"** (car c'est le premier serveur).
4. Nom du domaine racine : `securinetsenit.local`.

Une fois l'installation terminée, le serveur redémarre et nous pouvons nous connecter en tant qu'**Administrateur du Domaine**.

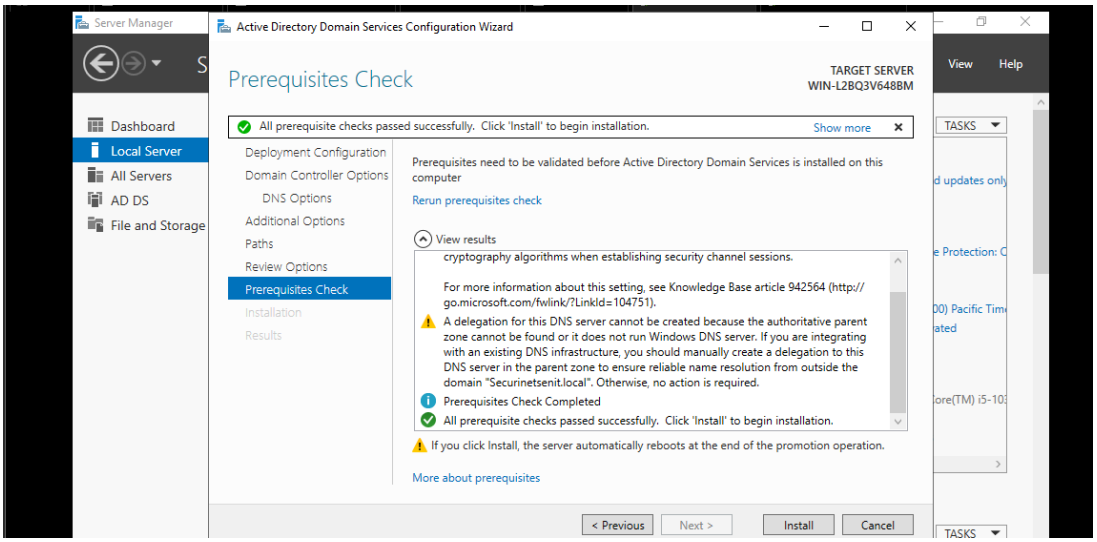

FIGURE 3.1 – Connexion réussie au nouveau domaine

3.4 Organisation Structurée (Best Practices)

Par défaut, AD place tout dans des dossiers génériques. Pour un projet professionnel, nous devons structurer les données.

3.4.1 Création des Unités d'Organisation (OU)

Nous avons créé une arborescence pour séparer les comptes de service, les utilisateurs et les ordinateurs. Pour éviter les conflits avec les noms système, nous avons utilisé un préfixe ("_").

— **_USERS** : Contient les sous-dossiers *Admins*, *IT*, *Finance*, *Marketing*.

— **_COMPUTERS** : Contient *Workstations* et *Servers*.

3.4.2 Création des Utilisateurs

Nous avons créé des comptes fictifs pour tester les départements :

— **Sami IT** (Login : `sami.it`)

— **Sarra Finance** (Login : `sarra.fin`)

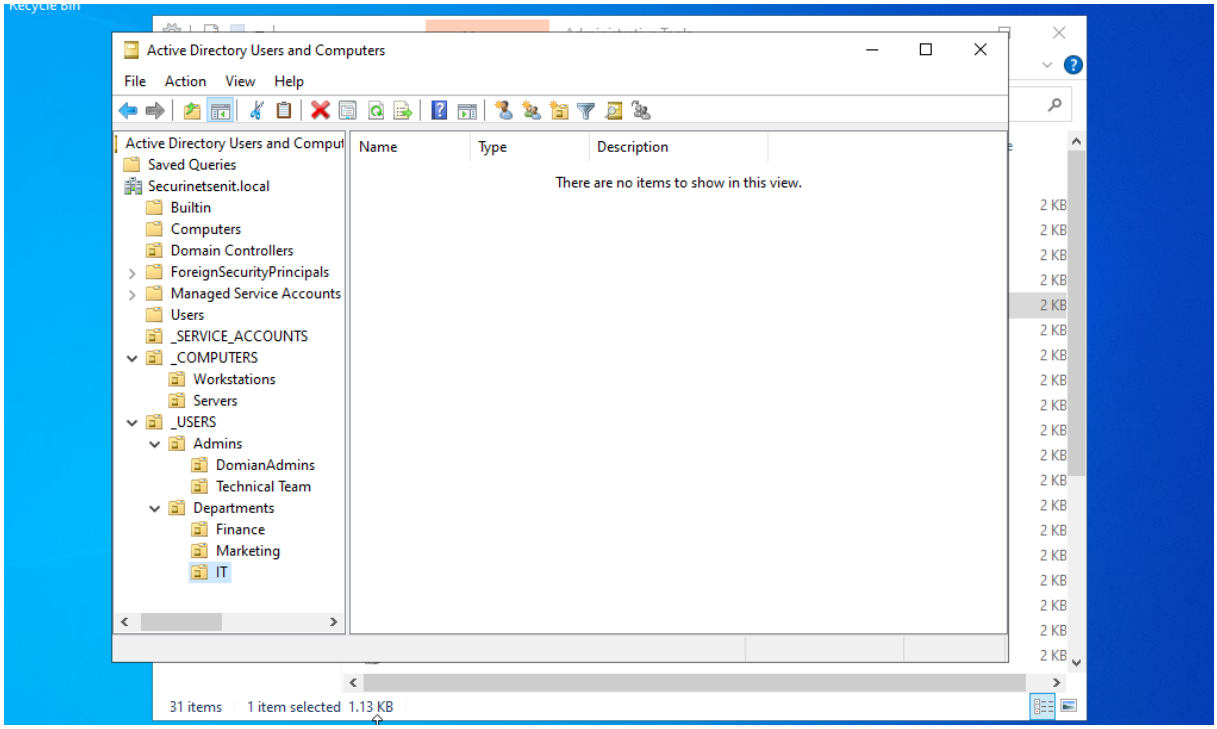

FIGURE 3.2 – Structure organisationnelle finale dans Active Directory

Intégration Client et Stratégies (GPO)

4.1 Installation du Client Windows 11

Pour le poste client, le choix de la version est crucial. Nous avons installé **Windows 11 Pro**. *Note : La version "Famille" (Home) a été écartée car elle ne possède pas les fonctionnalités pour rejoindre un domaine d'entreprise.*

4.2 La Jonction au Domaine

C'est l'étape où le PC client prête allégeance au serveur.

4.2.1 Configuration DNS (Le secret de la connexion)

Pour que le PC trouve le domaine `securinetsenit.local`, il doit impérativement interroger le serveur qui détient la zone DNS.

— **Sur Windows 11 :** Nous avons configuré le DNS préféré sur **192.168.1.10** (IP du Serveur).

— Sans cette étape, la jonction est impossible (Erreur "Domaine introuvable").

4.2.2 Validation de la jonction

Dans les paramètres système, nous avons modifié le groupe de travail pour passer en "Domaine". Après authentification administrateur, le message "Bienvenue dans le domaine" confirme le succès.

4.3 Déploiement d'une GPO (Group Policy Object)

Pour prouver le contrôle du serveur sur le client, nous avons mis en place une restriction.

4.3.1 Création de la GPO

1. Ouverture de la console **Group Policy Management**.
2. Création d'une GPO nommée `GPO_Restrict_ControlPanel` liée à l'OU **_USERS**.
3. Modification : *User Config > Admin Templates > Control Panel > Prohibit access...* réglé sur **Enabled**.

4.3.2 Test final

Nous nous sommes connectés sur Windows 11 avec l'utilisateur **Sami IT**. En tentant d'ouvrir les paramètres, un message d'erreur système apparaît, prouvant que la règle de sécurité est bien descendue du serveur vers le client.

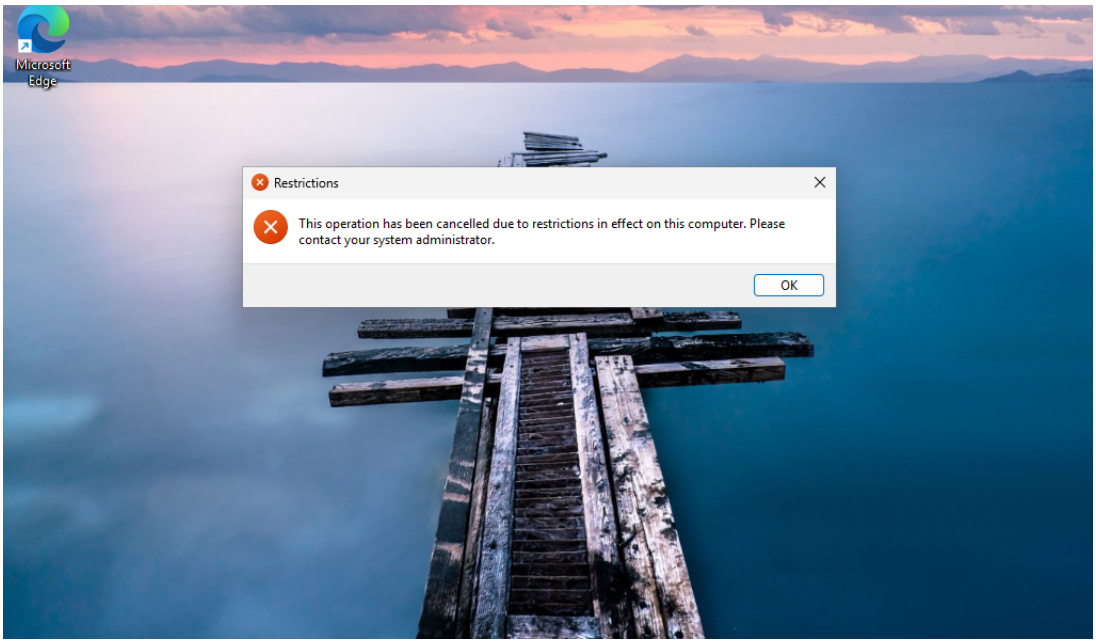

FIGURE 4.1 – Preuve de fonctionnement : L'accès aux paramètres est bloqué

Conclusion Générale

Le projet a permis de bâtir une infrastructure complète partagée en deux phases. Nous avons réussi à :

1. Isoler le trafic réseau grâce aux segments VMware et au pare-feu OPNsense.
2. Installer et configurer un Contrôleur de Domaine Windows Server 2022.
3. Structurer l'annuaire d'entreprise (OU, Users).
4. Connecter un client Windows 11 et lui appliquer des restrictions de sécurité centralisées.

Cette base est désormais prête pour l'évolution vers des services dynamiques (DHCP) et des tests d'intrusion (Phase 3).