# Projet PPE

# Sécurité Informatique

# AFORP PN2

| | |
|---|---|
| **Projet:** | **Infrastructure Réseau & Système Sécurisée Pédagogique de l'AFORP** |
| **Chef de projet:** | **Zakaria BOUDHERA** |
| **Classe:** | **BTS SIO SISR/BTS CIEL IR (Groupe C)** |
| **Date/Période:** | **Octobre 2025** |

## Sommaire

## 1 — Introduction générale

Dans le cadre de ce projet PPE (Projet Pluridisciplinaire à Caractère Professionnel), le but est de mettre en place une infrastructure réseau complète et fonctionnelle, comme celle que l'on peut trouver dans une petite ou moyenne entreprise.

L'objectif principal est de créer un réseau local d'entreprise (LAN) comportant plusieurs services indispensables :

- Un **contrôleur de domaine** (Active Directory),
- Un **serveur DNS** (pour la résolution des noms),
- Un **serveur DHCP** (pour l'attribution automatique d'adresses IP),
- Un **proxy Squid** (pour filtrer et contrôler les accès à Internet),
- Et enfin un **pare-feu (firewall)**, garant de la sécurité du réseau.

Ce projet permet de comprendre comment ces différents éléments interagissent entre eux et comment assurer la sécurité d'un réseau interne tout en donnant accès aux services nécessaires.

## 2 — Présentation du domaine et du réseau

Le réseau appartient au domaine promethee.local et utilise la plage d'adresses 172.16.3.0/24. Les principales adresses sont :
- Windows Server (AD, DNS, DHCP) : 172.16.3.250
- Debian (Proxy Squid) : 172.16.3.251
- Passerelle : 172.16.3.254

## 3 — Objectifs techniques du projet

Ce PPE a pour objectif de mettre en œuvre une **infrastructure réseau complète**, comprenant plusieurs services essentiels :

- Mettre en place un Active Directory.
- Configurer DNS et DHCP.
- Déployer un proxy Squid.
- Sécuriser le réseau via un pare-feu.
- Intégrer les postes clients et appliquer les GPO.

## 4 — Mise en place du réseau physique

L'installation du réseau inclut la mise en place de la baie de brassage, regroupant serveurs, switchs et firewall. Chaque port RJ45 est correctement brassé pour assurer une maintenance simplifiée et une infrastructure stable.

Nous avons, avec toute l'équipe, c'est-à-dire Zakaria, Adam, William, Ibrahim et moi-même fait l'installation et la mise en place du réseau physique.

## 5 — Configuration du routeur et du pare-feu

Le **pare-feu** (ou firewall) joue un rôle essentiel dans la sécurité de l'entreprise. Il contrôle les flux de données qui entrent et sortent du réseau, afin d'empêcher toute intrusion ou fuite d'information. Le routeur lui sert à connecter plusieurs réseaux entre eux et à diriger les données vers leur destination, sa configuration à était faite par Zakaria.

Dans notre projet, le firewall gère la sécurité :

- ACL pour filtrer les flux internes/externes.
- NAT pour la translation d'adresses.
- Administration protégée par mot de passe.

Résultat : le réseau interne est isolé et sécurisé.

Cette configuration permet de protéger efficacement le réseau interne tout en laissant les utilisateurs naviguer sur Internet via le proxy.

## 6 — Installation du serveur Debian

Le serveur Debian 13 héberge le proxy Squid (172.16.3.251). Squid contrôle les connexions Internet, filtre les sites et stocke en cache les pages consultées. Seules les connexions internes sont autorisées pour renforcer la sécurité. Nous nous sommes occupées de cette partie avec Ibrahim et moi.

L'installation se déroule en plusieurs étapes :

- Installation du système d'exploitation Debian 13.
- Configuration de la carte réseau avec une adresse IP fixe (172.16.3.251).
- Installation du service **Squid**, qui permet de mettre en place le proxy.

Une fois installé, Squid agit comme un intermédiaire entre les ordinateurs internes et Internet.
Toutes les requêtes web des utilisateurs passent par lui, ce qui permet de :

- Filtrer les sites autorisés ou interdits,
- Mettre en cache les pages pour accélérer la navigation,
- Et surveiller les connexions sortantes pour renforcer la sécurité.

## 7 — Installation du serveur Windows

Le **serveur Windows** est le cœur du réseau d'entreprise, Adam, William et Adam, William et Ibrahim, ils se sont tous les trois occuper de la configuration et de l'installation du serveur Windows.
Il assure trois rôles essentiels :

- **Contrôleur de domaine (Active Directory)** : il centralise la gestion des utilisateurs, des groupes, des ordinateurs et des règles de sécurité.
- **Serveur DNS** : il traduit les noms de domaine internes (comme "promethee.local") en adresses IP.
- **Serveur DHCP** : il distribue automatiquement les adresses IP aux ordinateurs du réseau.

L’installation du serveur commence par l’attribution d’une adresse IP fixe (**172.16.3.250**) et la configuration des paramètres réseau (masque, passerelle et DNS).
Ensuite, les rôles nécessaires sont ajoutés à l’aide de l’outil “Gestionnaire de serveur” de Windows :

- Active Directory Domain Services (AD DS),
- DNS Server,
- Et DHCP Server.

## 8 — Configuration du DHCP et du DNS

### Le rôle du DHCP

Le **DHCP (Dynamic Host Configuration Protocol)** simplifie la gestion du réseau en attribuant automatiquement une adresse IP à chaque poste client.
Grâce à lui, il n’est plus nécessaire de configurer manuellement chaque ordinateur. Le DHCP a été réalisée par Ibrahim.

### Le rôle du DNS

Le **DNS (Domain Name System)** est tout aussi important : il permet aux ordinateurs d’utiliser des noms plutôt que des adresses IP.
Par exemple, au lieu de retenir “172.16.3.250”, les utilisateurs peuvent simplement taper “serveur.promethee.local”. Zakaria c’est occuper du DNS.

## 9 — Création et gestion d’une GPO

Une **GPO (Group Policy Object)** est un ensemble de règles que l’administrateur applique à tous les ordinateurs et utilisateurs du domaine.
Grâce aux GPO, on peut définir des paramètres de sécurité, des restrictions, ou encore des configurations automatiques (comme le proxy). La GPO a été réalisée par Ibrahim, Zakaria et moi-même.

## 10 — Intégration d’un poste client Windows 10

Une fois les serveurs configurés, il faut intégrer les **postes clients** au domaine **promethee.local**.
Cette opération permet aux utilisateurs de se connecter avec un **compte du domaine**, plutôt qu’un compte local. Adam et William on intégrer le poste client serveur Windows 10.

Pour cela, le poste client doit être configuré pour utiliser le DNS du serveur Windows (172.16.3.250).
Ensuite, il suffit de rejoindre le domaine depuis les paramètres système de Windows.
Une fois intégré, le poste redémarre et peut être utilisé avec les comptes du domaine.

## 11— Tests de bon fonctionnement

Une fois l’infrastructure installée, il est indispensable de **tester** chaque service pour vérifier que tout fonctionne correctement.

### Tests réseau de base :

- Vérifier la connectivité entre les serveurs et les postes (ping).
- Vérifier que le client peut accéder à Internet via le proxy.

### Tests Active Directory :

- Créer un utilisateur test dans le domaine.
- Se connecter sur un poste client avec ce compte.
- Vérifier que les GPO s’appliquent correctement.

### Tests DHCP et DNS :

- S’assurer que le poste client obtient une adresse IP dans la plage prévue.
- Vérifier que les noms de domaine internes se résolvent correctement.

### Tests Proxy (Squid) :

- Vérifier que la navigation Internet passe bien par le proxy.
- Contrôler que les requêtes apparaissent dans les journaux du serveur Debian.

L'ensemble de ces tests permet de confirmer la fiabilité du réseau avant sa mise en production.

## 12 — Synthèse du projet

La mise en place de cette infrastructure réseau a permis de comprendre le fonctionnement global d'un réseau d'entreprise.
L'étudiant a pu :

- Concevoir une architecture réseau complète,
- Installer et configurer plusieurs services complémentaires,
- Comprendre le rôle de chaque serveur,
- Et assurer la sécurité des échanges entre les postes.

Ce projet a également permis d'acquérir des compétences techniques concrètes : configuration d'un serveur Windows, gestion d'un domaine, mise en place d'un proxy et compréhension des mécanismes de sécurité réseau.