

Document de conception

Tristan Petit, Nils Hubert, Toni Rey, Majd El Sebeiti , Vianney Miquel

February 21, 2025



Table des matières

1	Introduction	1
2	Architecture Réseau	1
3	Choix des logiciels	2
4	Choix du wiki	3
5	Solutions mises en oeuvre	3

1 Introduction

Dans le cadre de notre SAE4.01, nous avons choisi une infrastructure réseau de niveau 2 (améliorée). Ce choix se justifie notamment par la contrainte de temps, ou des compétences techniques à appréhender. Nous pensons néanmoins réaliser certaines parties du niveau 3 (avancé) selon le temps restant et nos affinités avec les technologies, car les 2 niveaux d'infrastructure réseaux ne sont pas incompatibles et la transition est continue, nous donnais la liberté d'évoluer vers un niveau supérieur si besoin.

2 Architecture Réseau

Nos objectifs pour ce projet sont de **concevoir** et **mettre en œuvre** une **infrastructure de réseau** qui soit capable d'accueillir les postes de travail des utilisateurs d'une organisation en apportant à ces utilisateurs un certain nombre de services.

Cette **infrastructure devra être sécurisée** : on cherche à protéger les machines, les réseaux et les données de cette organisation contre les cybermenaces courantes. Pour remplir ces objectifs, nous avons imaginé une architecture réseau en plusieurs sous-réseaux :

- **Utilisateurs** : ce sous-réseau sert à contenir les postes utilisateurs.
- **Administrateurs** : le sous-réseau administrateur donne un accès privilégié à tous les réseaux de l'entreprise, il sert aussi à stocker des données administrateurs.
- **Serveurs internes** : pour les bases de données, applications internes, etc.
- **DMZ** : la DMZ contient les sites web publics.

Nous mettrons aussi en place un **serveur de fichiers** pour les postes de travail.

Pour **relier notre réseau à Internet**, nous devons mettre en place un **routeur**. Pour **sécuriser ce routeur**, nous ajouterons un **pare-feu** pour filtrer les entrées et sorties réseau.

La communication avec Internet nécessite une adresse IP ; nous les attribuerons **dynamiquement** avec un **serveur DHCP** par sous-réseau afin de ne pas surcharger un DHCP central.

Enfin, nous devons résoudre les URLs en adresses IP grâce à un **serveur DNS**, le premier sera **interne** pour résoudre les **adresses des sous-réseaux** non accessibles depuis l'extérieur, et le deuxième **externe** pour résoudre les **adresses en ligne**.

Cette architecture nous donne le schema suivant :

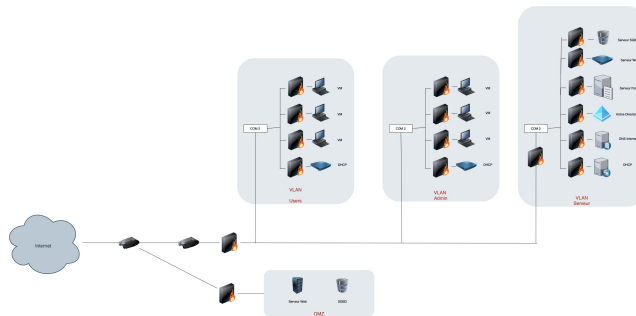


Figure 1: Schema de l'architecture réseau

Plan d'Adressage IP

Pour un plan d'adressage IP, on choisit une **plage privée (RFC1918)**, ici $10.X.X.0/24$, puis nous attribuons ensuite les adresses des sous-réseaux et des machines :

Sous-Réseau	Adresse IP	Masque
Routeur	10.0.1.1	255.255.255.0
Réseau Utilisateurs	10.0.10.0	255.255.255.0
Réseau Admins	10.0.20.0	255.255.255.0
Réseau Serveurs	10.0.30.0	255.255.255.0
DMZ	10.0.40.0	255.255.255.0
DHCP Server	10.0.30.10	255.255.255.0
DNS Interne	10.0.30.20	255.255.255.0
DNS Externe	10.0.40.20	255.255.255.0
Pare-feu	10.0.1.254	255.255.255.0

Table 1: Plan d'adressage IP

On notera que tous les postes clients **reçoivent leurs IPs via DHCP** et que les serveurs ont des **adresses IP statiques**.

3 Choix des logiciels

- Os pour serveurs :
- Os pour poste de travail :
- Proxmox :
- Serveur web :
- Supervision du réseaux :
- SIEM :

4 Choix du wiki

Dans le cadre de la mise en oeuvre de cette infrastructure, nous devons concevoir un wiki détaillé expliquant à un intervenant extérieur comment fonctionnera cette infrastructure réseau afin qu'il ou elle puisse être en mesure d'administrer ce réseau.

- Critères de Choix :
- Comparaison des solutions :

5 Solutions mises en oeuvre