Document de conception

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

February 23, 2025

Table des matières

1 Introduction

Dans le cadre de notre SAE4.01, nous avons choisi une infrastructure réseau de niveau 2 (améliorée). Ce choix se justiffie notamment par la contrainte de temps, ou des compétences techniques à apréhender. Nous pensons néamoins réaliser certaines parties du niveau 3 (anvacé) 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 :

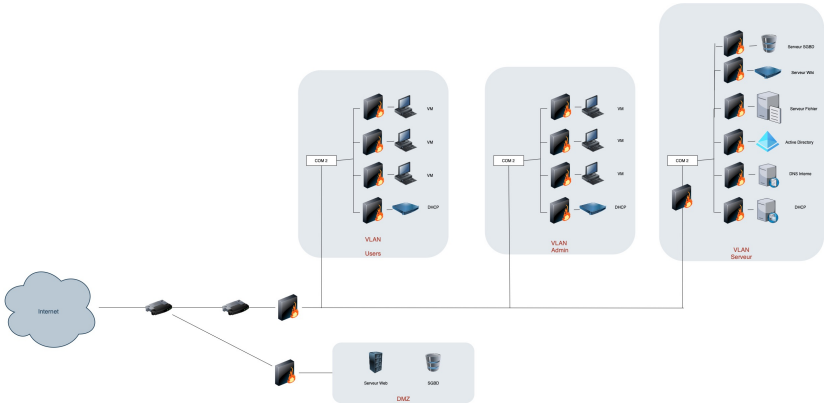

Figure 1: Schema de l'architecture réseau

2.1 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

3.1 Supervision et Logs

Conclusion : Zabbix est le choix idéal car il offre une **supervision complète avec alertes avancées**.

Critères	systemd-journald	Nagios	Icinga	Zabbix	Centreon	Thruk	Shinken
Facilité d'installation	Facile	Complexe	Moyenne	Moyenne	Moyenne	Peu doc.	Moyenne
Interface Web	Non	Oui	Oui	Oui	Oui	Oui	Oui
Supervision réseau	Non	Oui	Oui	Oui	Oui	Oui	Oui
Alertes et notifications	Non	Basique	Oui	Très avancé	Oui	Oui	Oui
Performance	Très bonne	Limité	Bonne	Très bonne	Bonne	Bonne	Bonne
Scalabilité	Local	Limité	Moyenne	Très bonne	Très bonne	Moyenne	Moyenne

Table 2: Comparaison des outils de supervision et logs

Alternative : Centreon si on veut une interface plus simple pour les grandes entreprises.

3.2 OS pour postes de travail

Critères	Windows	MacOS	Ubuntu	Debian
Facilité d'utilisation	Très facile	Très facile	Moyenne	Plus technique
Compatibilité matérielle	Très large	Matériel Apple	Large	Large
Infra compatible	Windows/Mac	Mac uniquement	Windows/Linux	Windows/Linux
Sécurité	Bonne (MAJ)	Très bonne	Très bonne	Très bonne
Support/Doc.	Très actif	Actif	Actif	Actif
Usage entreprise	Standard	Standard	Devs/serveurs	Serveurs/Devs

Table 3: Comparaison des OS pour postes de travail

Conclusion : Windows est le choix le plus adapté car il est compatible avec la majorité des logiciels et infrastructures d'entreprise.

Alternative : Ubuntu pour les environnements Linux ou les postes de développement.

3.3 Serveur Web

Critères	Apache	Nginx	Caddy
Facilité d'installation	Facile	Moyenne	Très facile
Performance	Bonne	Excellente	Bonne
Gestion de la charge (Load Balancing)	Oui	Très performant	Basique
Gestion HTTPS intégrée	Non (besoin de Let's Encrypt)	Oui	Automatique
Sécurité & Mises à jour	Bonne	Bonne	Bonne
Modules & Extensions	Très nombreuses	Moins nombreuses	Peu d'extensions
Utilisation en entreprise	Très répandu	Répandu	Moins courant

Table 4: Comparaison des serveurs web

Apache est le choix idéal car il est compatible avec tous les logiciels en entreprise et dispose d'une large documentation.

3.4 SIEM

Critères	Prelude OSS	OSSEC	Wazuh	Apache Metron
Facilité d'installation	Complexe	Facile	Facile	Très complexe
Interface Web	Non	Non	Oui (Dashboard Kibana)	Oui
Détection des Intrusions (IDS)	Oui	Oui	Oui	Oui
Corrélation des événements	Avancée	Basique	Bonne	Très avancée
Analyse en temps réel	Oui	Non	Oui	Oui
Gestion centralisée des logs	Oui	Non	Oui	Oui
Scalabilité (adapté aux grandes infrastructures)	Limité	Limité	Évolutif	Très évolutif
Intégration avec d'autres outils (Elastic, Kibana, etc.)	Non	Non	Oui (Elastic Stack)	Oui
Communauté & Support	Faible	Active	Très active	Faible

Table 5: Comparaison des solutions SIEM

Wazuh : • Facile à installer et configurer comparé à Metron et Prelude OSS.

3.5 Serveur de Fichiers

Critères	Samba	NFS (Linux)	Nextcloud
Facilité d'installation	Moyenne	Facile	Facile
Compatibilité OS	Windows & Linux	Linux	Web & Mobile
Gestion des permissions avancées	Oui (ACL, Active Directory)	Limité	Oui
Partage multi-utilisateurs	Oui	Oui	Oui
Sécurité (Chiffrement, Authentification)	Oui	Basique	Très sécurisé
Performance sur gros volumes	Bonne	Excellente	Moins adapté
Support & Documentation	Très actif	Actif	Actif

Table 6: Comparaison des solutions de serveurs de fichiers

Samba est le plus adapté car il supporte Active Directory, Windows/Linux et offre une bonne gestion des permissions.

3.6 Authentification Centralisée (LDAP)

Critères	OpenLDAP	FreeIPA	389 Directory Server	Microsoft AD
Facilité d'installation	Complexe	Moyenne	Complexe	Facile (Windows)
Interface Web	Non	Oui	Oui	Oui
Intégration Active Directory	Non	Partielle	Partielle	Native
Sécurité et Authentification	Bonne	Très bonne	Bonne	Très avancée (Kerberos)
Gestion des permissions avancées	Oui	Oui	Oui	Oui (GPO, ACL avancées)
Utilisation en entreprise	Courant	Moyen	Moins courant	Standard
Support & Documentation	Actif	Actif	Plus limité	Très actif (Microsoft)

Table 7: Comparaison des solutions LDAP

Microsoft Active Directory est le plus adapté, car il est déjà largement

utilisé en entreprise et intègre de nombreuses fonctionnalités de sécurité et de gestion.

4 Choix du wiki

Dans le cadre de la mise en oeuvre de cette infrastructure, nous devrons 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 :
  - Facilité d'utilisation
  - Fonctionnalités
  - Gestion des utilisateurs
  - Sécurité
  - Cout
  - Support et communauté
- Comparaison des solutions :

Wiki	**Avantages**	**Inconvénients**
DokuWiki	Léger, pas besoin de base de données, bon contrôle des accès, support LDAP.	Interface de base au design moins moderne.
MediaWiki	Utilisé par Wikipedia, puissant, support des extensions, bonne gestion des droits.	Configuration plus lourde, nécessite MySQL/PostgreSQL.
Wiki.Js	Moderne, supporte Markdown, bonne intégration LDAP/SSO, interface intuitive.	Plus lourd, nécessite une base de données et Node.js.
XWiki	Très complet, bon support des macros et extensions.	Installation plus complexe.

Moteur de Wiki choisi : **Wiki.Js**

- Interface intuitive
- Support de plusieurs méthodes d'authentification (dont LDAP et SAML 2.0)

- Licence Gratuit : Open-source sous licence AGPL
- Gestion avancée des utilisateurs
- Facilement installable et déployable sur de nombreuses plateformes serveur et support d'un SGBD déjà maîtrisé : PostgreSQL
- Beaucoup de fonctionnalités incluses
- Programmé contre les failles de sécurité avec possibilité de faire des retours en cas de vulnérabilités constatées

5 Mise en place des cannaux de communication

Pour la communication sécurisée au sein du groupe, nous avons décidé d'utiliser une messagerie chiffrée, qui permet une messagerie instantanée, le partage de fichiers et la sécurisation des échanges. Plusieurs choix se sont offerts à nous :

- Notre premier était Mattermost. Nous donne l'avantage d'être open-source, compatible LDAP/SSO. Son inconvénient est qu'il a une configuration complexe.
- Le deuxième était Rocket Chat, il est plus simple à configurer mais il est moins sécurisé que ses autres concurrents.
- notre 3ème option, Matrix.org à l'aide de Element, c'est le plus sécurisé et intuitif, il n'a pas d'inconvénients notables

Nous avons donc décidé de prendre la troisième option car c'était la moins contraignante en termes de mise en place avec une bonne sécurité. Nous utilisons le client Element pour utiliser le réseau matrix.org. En effet, c'est le client qui est disponible sur le plus de plateformes. Nous l'utilisons donc pour l'échange de mots de passe et de documents importants. Nous utilisons avons aussi mis en place Thunderbird pour un canal de communication alternatif. Nous avons choisi cette boîte mail chiffrée car l'ayant vu en TP chaque membre de notre groupe la maîtrise, nous avons seulement dû nous partager nos clés privées. Pour l'échange de documents volumineux et de code, nous utilisons un dépot Github privé. Sur le dépot Github, nous stockons les scripts utiles au projet, chiffrés à l'aide de GPG, et possiblement compréssés avec 7zip ; commme par exemple pour les images ISO. Nous avons choisi 7zip car il est open-source, gratuit, et il permet de chiffrer les fichiers avec AES-256, une méthode de chiffrement très sécurisée.

5.1 Exemples imagés

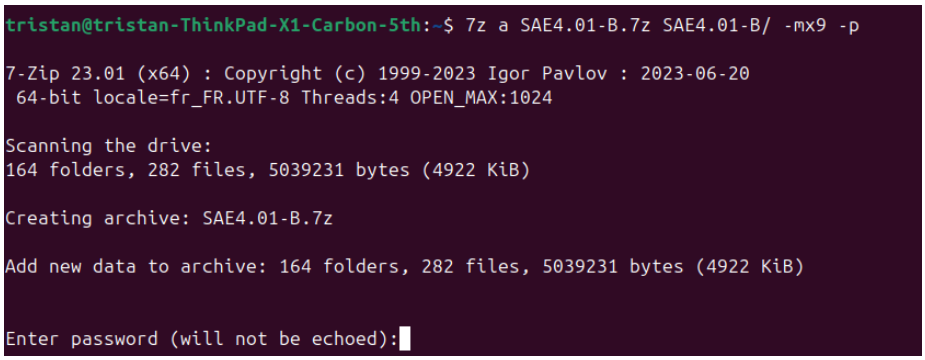

Figure 2: exemple de chiffrement avec 7zip

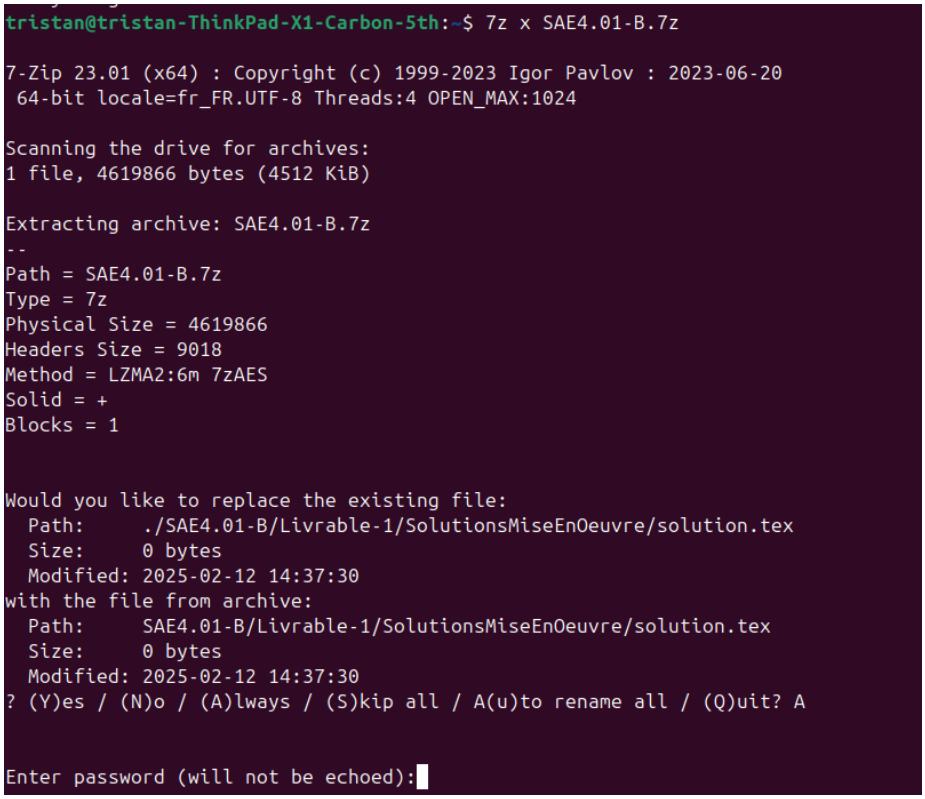

Figure 3: exemple de déchiffrement avec 7zip

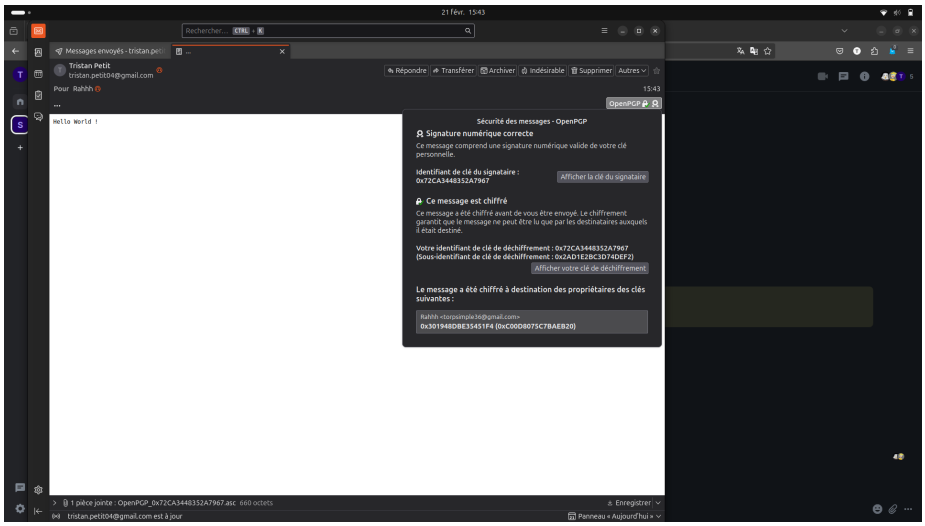

Figure 4: exemple d'envoi chiffré avec Thunderbird

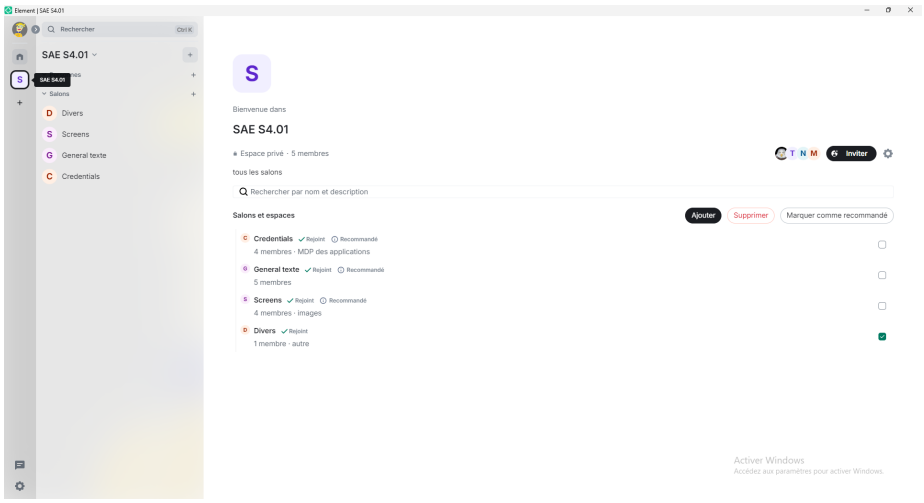

Figure 5: Espace de discussion et ses salons dans Element (matrix.org)