

Document de conception

SAE S4.Deploi.01

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

February 24, 2025

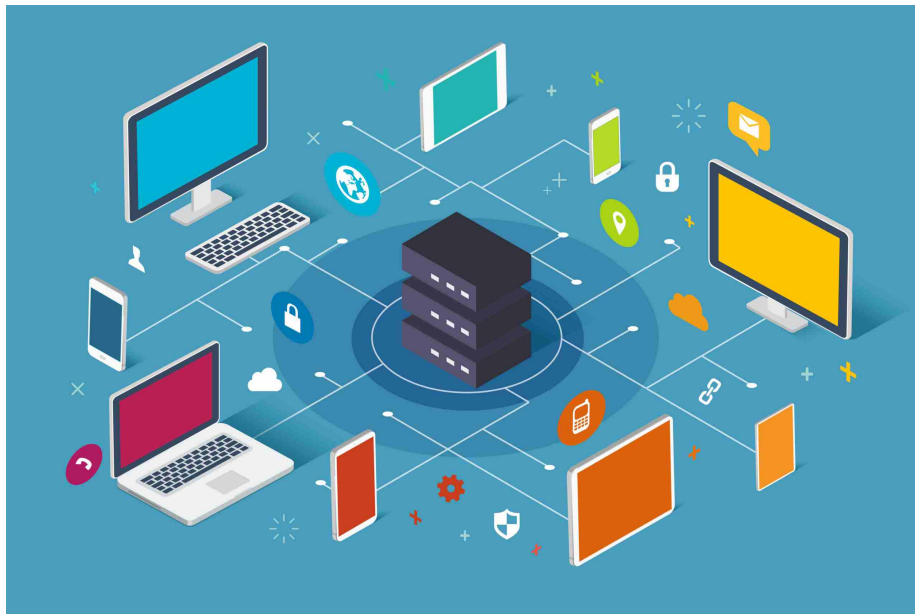


Table des matières

1	Introduction	1
2	Architecture Réseau	1
2.1	Plan d'Adressage IP	2
3	Choix des logiciels	2
3.1	serveur DNS	2
3.2	Supervision et Logs	3
3.3	Firewall	3
3.4	Serveur DHCP	4
3.5	OS pour postes de travail	4
3.6	Serveur Web	4
3.7	Logiciels de Virtualisation	5
3.8	SIEM	5
3.9	Serveur de Fichiers	6
3.10	Serveur SGBD	6
3.11	Authentification Centralisée (LDAP)	6
4	Choix du wiki	7
5	Mise en place des canaux de communication	8
5.1	Exemples imagés	9

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 :

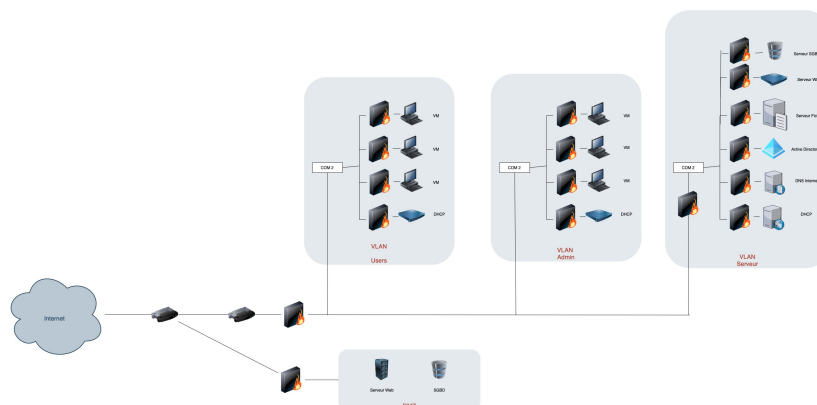


Figure 1: Schema de l'architecture réseau

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 serveur DNS

Critères	Bind9	PowerDNS	Unbound
Facilité d'utilisation	Complexe	Moyenne	Facile
Performance	Bonne	Très bonne	Très bonne
Sécurité (DNSSEC, DoT, DoH)	Oui	Oui	Oui
Caching DNS	Oui	Oui	Très performant
Utilisation en entreprise	Standard	Déployé	Moins courant
Communauté et Support	Très actif	Actif	Limité

Table 2: Comparaison des logiciel de DNS

Bind9 est le meilleur choix car il est puissant, standard de l'industrie et très flexible.

3.2 Supervision et Logs

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 3: Comparaison des outils de supervision et logs

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

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

3.3 Firewall

Critères	pfSense	OPNsense	IPFire	nftables
Facilité d'installation	Très facile	Facile	Facile	Complexe (CLI uniquement) Non
Interface Web	Oui	Oui	Oui	Non natif
Performance Excellente	Très bonne	Bonne	Excellente	Oui (avec iptables)
Support VPN (IPsec, OpenVPN, WireGuard)	Oui	Oui	Basique	Serveurs Linux
Gestion avancée du trafic (QoS, VLANs)	Oui	Oui	Oui	Peu de documentation grand public
Utilisation en entreprise	Courant	Courant	Moins répandu	
Support et Documentation	Très actif	Actif	Actif	

Table 4: Comparaison des outils de Firewall

Conclusion : Conclusion : pfSense est le meilleur choix car il est complet,

simple à utiliser et largement documenté.

Alternative : nftables si on veut un contrôle total en ligne de commande sous Linux.

3.4 Serveur DHCP

Critères	ISC DHCP Server	Kea DHCP	Dnsmasq
Facilité d'installation	Moyenne	Moyenne	Très facile
Gestion des sous-réseaux	Oui	Oui	Basique
DHCPv6 supporté	Oui	Oui	Partiel
Haute disponibilité (HA)	Possible	Oui	Non natif
Utilisation en entreprise	Standard	Standard moderne	Usage limité
Performance sur gros réseaux	Bonne	Excellente	Limité
Support et Documentation	Très actif	Actif (remplaçant d'ISC)	Actif

Table 5: Comparaison des logiciel pour le serveur DHCP

Conclusion : Kea DHCP est plus moderne et performant que ISC DHCP, tout en étant conçu pour évoluer.

Alternative : Dnsmasq pour un usage léger sur des petits réseaux.

3.5 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 6: 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.

3.6 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 7: 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.

3.7 Logiciels de Virtualisation

Critères	OpenStack	Qemu/KVM	libvirt	virsh
Facilité d'installation	Très complexe	Moyenne	Facile	Facile
Performance	Bonne	Excellente	Bonne	Bonne
Interface Web	Oui (Horizon)	Non	Oui (Virt-Manager)	Non
Gestion des VMs	Très avancée	Bonne	Bonne	Limité
Utilisation en entreprise	Cloud	Serveurs Linux	Serveurs Linux	Usage technique
Scalabilité	Très grande	Bonne	Bonne	Limité

Table 8: Comparaison des hyperviseurs

Conclusion : Qemu/KVM est la meilleure solution car il est performant, open-source et flexible pour les environnements Linux.

Alternative : OpenStack si on veut une solution cloud complète.

3.8 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 9: Comparaison des solutions SIEM

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

3.9 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 10: 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.

3.10 Serveur SGBD

Critères	PostgreSQL	MariaDB
Facilité d'installation	Moyenne	Facile
Performance	Excellente	Très bonne
Support SQL avancé	Très avancé	Moins complet
Scalabilité	Très évolutif	Évolutif
Sécurité	Très bonne	Bonne
Utilisation en entreprise	Très courant	Standard

Table 11: Comparaison des logiciel SGBD

Conclusion : PostgreSQL est le plus adapté car il offre plus de fonctionnalités avancées et une meilleure évolutivité.

Alternative : MariaDB si on veut une alternative MySQL plus légère et rapide.

3.11 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 12: 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. Il est également compatible avec les environnements Windows, MacOS, Linux et tout environnement supportant l'authentification LDAP et SAML 2.0.

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 :

- 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

Ainsi, étant donnée l'objectif de ce wiki, Wiki.Js s'est révélé être le choix le plus pertinent pour répondre aux exigences de ce projet.

5 Mise en place des canaux 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 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 dépôt Github privé. Sur le dépôt Github, nous stockons les scripts utiles au projet, chiffrés à l'aide de GPG, et possiblement compressés avec 7zip ; comme 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

```
tristan@tristan-ThinkPad-X1-Carbon-5th:~$ 7z a SAE4.01-B.7z SAE4.01-B/ -mx9 -p
7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=fr_FR.UTF-8 Threads:4 OPEN_MAX:1024

Scanning the drive:
164 folders, 282 files, 5039231 bytes (4922 KiB)

Creating archive: SAE4.01-B.7z

Add new data to archive: 164 folders, 282 files, 5039231 bytes (4922 KiB)

Enter password (will not be echoed):
```

Figure 2: exemple de chiffrement avec 7zip

```
tristan@tristan-ThinkPad-X1-Carbon-5th:~$ 7z x SAE4.01-B.7z

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=fr_FR.UTF-8 Threads:4 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 4619866 bytes (4512 KiB)

Extracting archive: SAE4.01-B.7z
--
Path = SAE4.01-B.7z
Type = 7z
Physical Size = 4619866
Headers Size = 9018
Method = LZMA2:6m 7zAES
Solid = +
Blocks = 1

Would you like to replace the existing file:
Path:      ./SAE4.01-B/Livable-1/SolutionsMiseEnOeuvre/solution.tex
Size:      0 bytes
Modified:  2025-02-12 14:37:30
with the file from archive:
Path:      SAE4.01-B/Livable-1/SolutionsMiseEnOeuvre/solution.tex
Size:      0 bytes
Modified:  2025-02-12 14:37:30
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? A

Enter password (will not be echoed):
```

Figure 3: exemple de déchiffrement avec 7zip

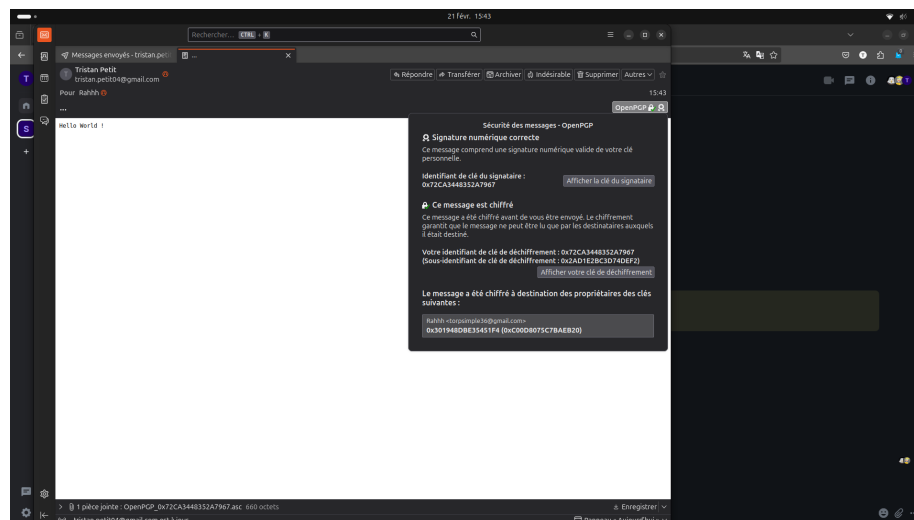


Figure 4: exemple d'envoi chiffré avec Thunderbird

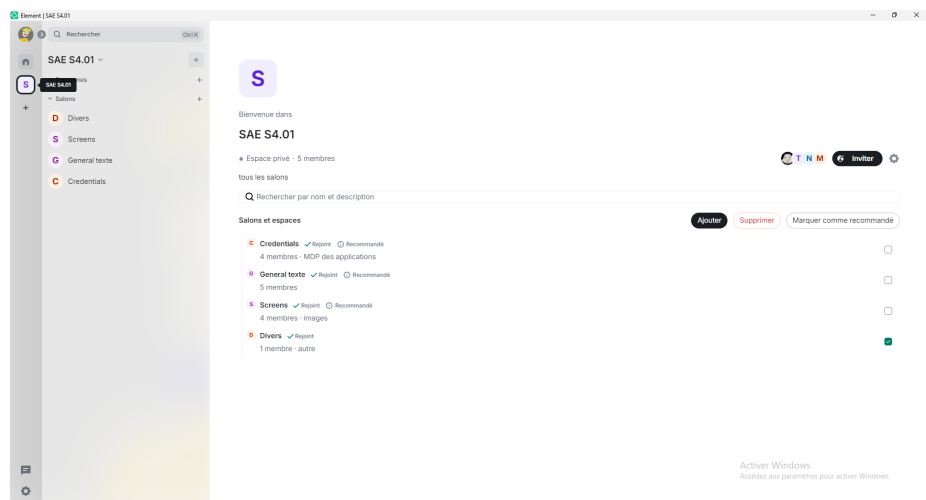


Figure 5: Espace de discussion et ses salons dans Element (matrix.org)