

PROJET TRANSVERSAL

INSTALLATION D'UNE INFRASTRUCTURE RÉSEAU

Fonctionnelle et Sécurisée

 STOCKME

2025-2026



SOMMAIRE

01 CONTEXTE & ENJEUX

02 ARCHITECTURE RÉSEAU

03 CONCEPTION HLD & LLD

04 PLAN D'ADRESSAGE IP

05 INVENTAIRE DES VM

06 DÉPLOIEMENT LAN

07 CYBERSÉCURITÉ

08 MONITORING (SOC)

09 CONCLUSION

STOCKME, entreprise spécialisée en infogérance, doit répondre à un besoin critique d'extension d'infrastructure. Le projet consiste à déployer un nouveau local de stockage de données clients tout en assurant une interconnexion sécurisée avec le siège existant.

OBJECTIF : Garantir l'accessibilité des services critiques depuis le siège et permettre aux commerciaux itinérants un accès VPN restreint au serveur applicatif Dolibarr.

Le nouveau site accueillera des serveurs vitaux, dont le site WEB migré, le monitoring ZABBIX, le SIEM WAZUH et le serveur de données clients, cœur de l'activité de l'entreprise.

INFRASTRUCTURE SIÈGE

- >> Active Directory & DHCP
- >> Serveur de Fichiers
- >> Switch L2 & pfSense
- >> Bornes Wi-Fi
- >> Effectif: 50 Personnes

NOUVEAU LOCAL (CIBLE)

- >> Site WEB (Migration) **CRITIQUE**
- >> Applicatif Dolibarr
- >> Monitoring ZABBIX
- >> SIEM WAZUH
- >> Serveur Données Clients

ARCHITECTURE RÉSEAU MULTI-SITES

03

□ INTERCONNEXION VPN

Liaison sécurisée entre le Siège (pfSense) et le Nouveau Local (OPNsense). Séparation stricte des réseaux applicatifs et clients.

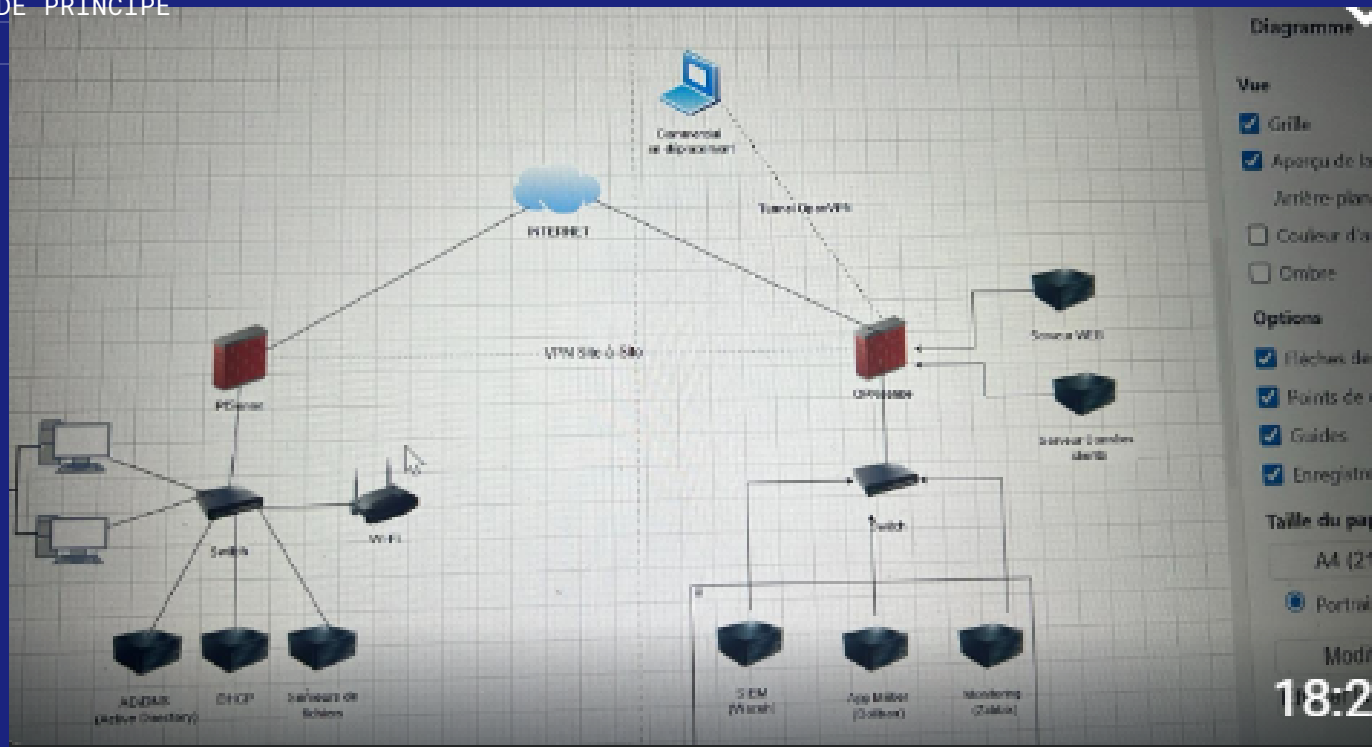
□ PLAN D'ADRESSAGE

Contrainte DSI : Interdiction des classes C.
Utilisation de segments /23 pour garantir l'évolutivité (510 hôtes).

□ ACCÈS SÉCURISÉS

Commerciaux itinérants connectés via OpenVPN. Accès restreint uniquement au serveur applicatif Dolibarr.

FIG 1.0 : SCHÉMA DE PRINCIPE



SCALE : N/A

CONCEPTION HLD & LLD

04

Mission 1 : HLD

High Level Design

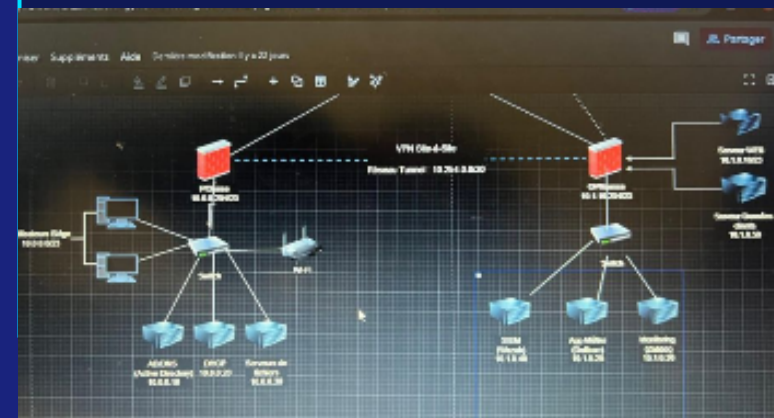
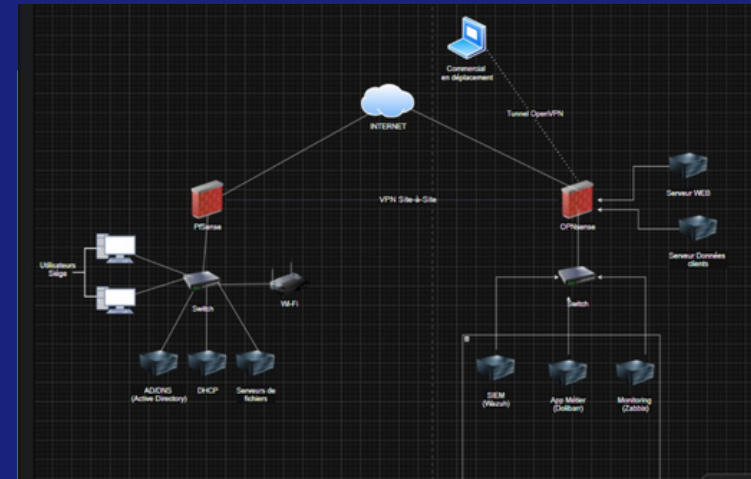
- Architecture globale (Siège + Nouveau Local)
- Migration stratégique du site WEB
- Outils : Microsoft Visio, draw.io

Mission 2 : LLD

Low Level Design

- Adressage IP détaillé par segment
- Utilisation de masques/23(510 hôtes)
- Interconnexion VPN Site-à-Site (/30)

⚠ CONTRAINTE DSI : Interdiction stricte des adresses de classe C



PLAN D'ADRESSAGE IP (LLD)

ZONE	RÉSEAU	MASQUE	HÔTES	PASSERELLE
Siège - Infrastructure	10.0.0.0/23	255.255.254.0	510	10.0.0.254
Siège - Utilisateurs	10.0.2.0/23	255.255.254.0	510	10.0.0.254
Nouveau Local - Serveurs	10.1.0.0/23	255.255.254.0	510	10.1.0.254
Nouveau Local - Clients	10.1.2.0/23	255.255.254.0	510	10.1.2.254
VPN Site-à-Site	10.254.0.0/30	255.255.255.252	2	N/A
VPN OpenVPN	10.254.1.0/24	255.255.255.0	254	10.254.1.1

- CONFORMITÉ DSI : Utilisation exclusive d'adresses privées de classe A (10.x.x.x). Masques /23 permettant une extension future jusqu'à 510 hôtes par segment.

INVENTAIRE DES VM (ESXI)

MACHINE VIRTUELLE	ÉTAT	SE INVITÉ	NOM D'HÔTE	MÉMOIRE
PFSENSE	Normal	FreeBSD 13 (64 bits)	Inconnu	1,99 Go
opnsense	Normal	FreeBSD 14+	Inconnu	4,05 Go
client	Normal	Debian GNU/Linux 12	CLIENT-01	2,05 Go
serveur-zabbix	Normal	Ubuntu Linux (64 bits)	srv-zabbix	2,05 Go
debian	Normal	Debian GNU/Linux 12	debian	1,86 Go
srv-wazuh	Normal	Ubuntu Linux (64 bits)	srv-wazuh	4,07 Go
srv-web	PAR DEFALT	Ubuntu Linux (64 bits)	web	2,06 Go

- ❑ INFRASTRUCTURE : Hôte VMware ESXi opérationnel. 8 machines virtuelles actives assurant la segmentation des services et la redondance des pare-feux.

DÉPLOIEMENT LAN & SERVICES

07

SITE_ID: HQ

□ Mission 4 : Siège

□ Routeur pfSense

Configuration des interfaces WAN/LAN selon le plan IP.

```
PFSense
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 5b23ebcbce12d60d6011

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> vmx0 -> v4/DHCP4: 10.92.233.121/24
LAN (lan) -> vmx1 -> v4: 10.0.0.254/23

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                   14) Enable Secure Shell (sshd)
6) Halt system                     15) Restore recent configuration
7) Ping host                       16) Restart PHP-FPM
8) Shell

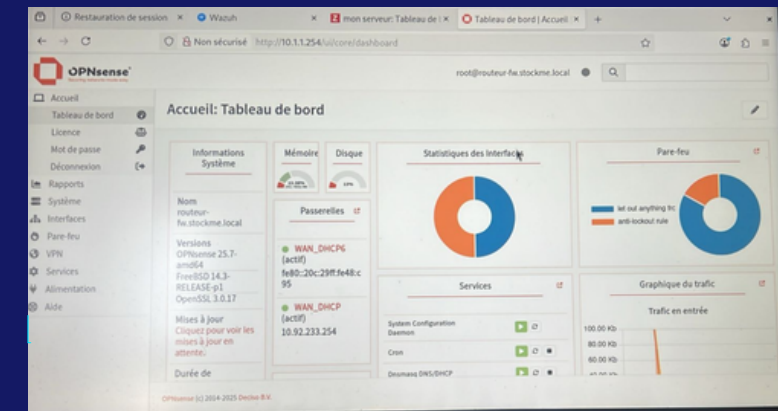
Enter an option: pcib19: Attention Button Pressed: Detaching in 5 seconds
vmx1: detached
pci5: detached
```

SITE_ID: NEW_LOC

□ Mission 5 : Nouveau Local

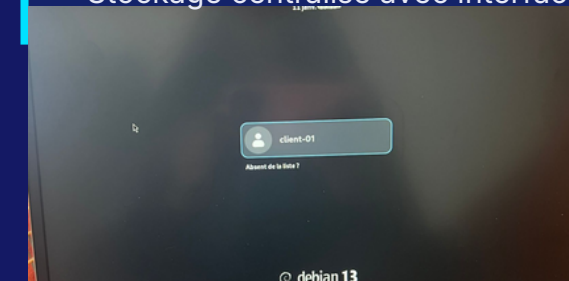
□ Routeur OPNsense

Sécurisation des flux et isolation des zones serveurs.



□ Serveur Données Clients

Stockage centralisé avec interface intuitive.



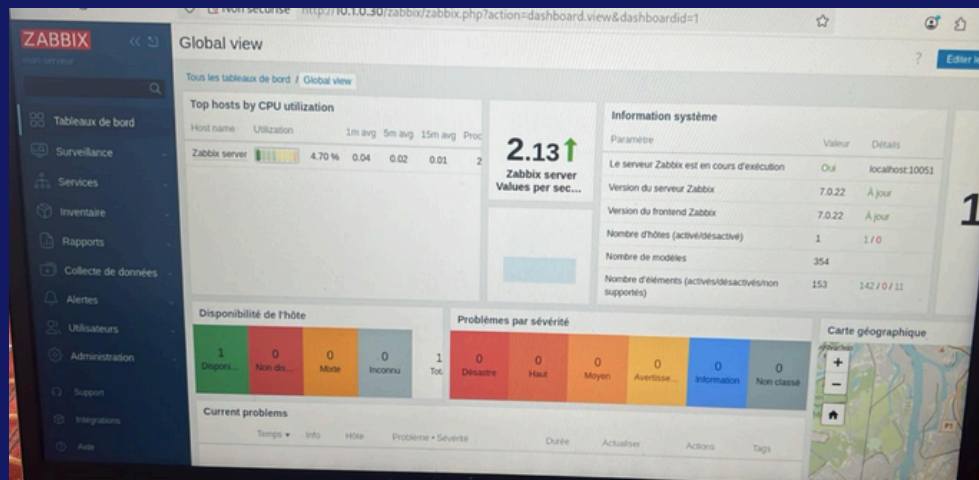
MONITORING & DÉTECTION (SOC)

09

❑ ZABBIX

DISPONIBILITÉ

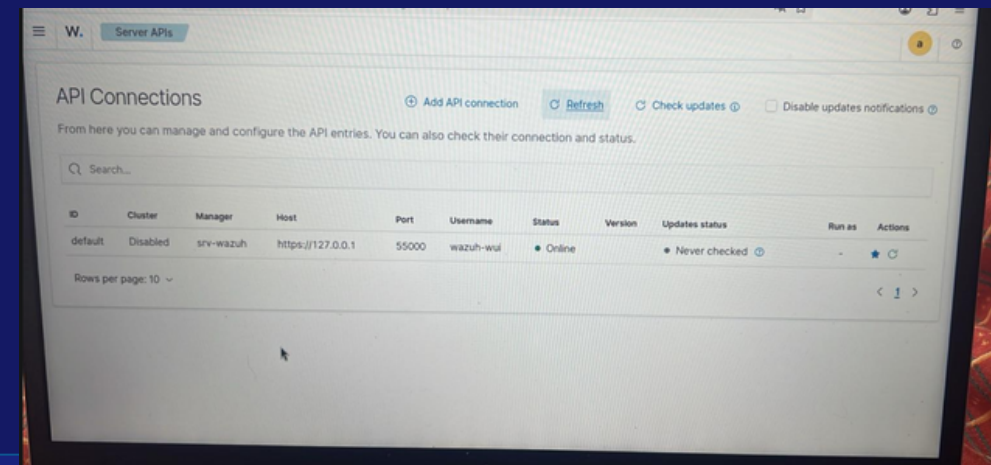
- ❑ Pare-feux (Firewalls)
Surveillance ICMP et SNMP des routeurs pfSense & OPNsense.
- ❑ Serveur WEB
Monitoring HTTP/S de la disponibilité du site institutionnel.
- ❑ Serveur Données Clients
Alerting critique sur les services de stockage et d'accès.



❑ WAZUH

SIEM / SÉCURITÉ

- fl Scan de Vulnérabilités
Identification proactive des failles sur les serveurs exposés.
- ❑ Analyse de Logs
Centralisation et corrélation des événements de sécurité.
- ❑ Réponse Active
Blocage automatique des tentatives de brute force (IPS).



Garantie de la disponibilité, de l'intégrité
et de la confidentialité

❑ CONFORMITÉ RGPD

Miseenconformitéobligatoire pour la protection des données. Documentation des
processus de collecte et de stockage sécurisé. Votre texte de paragraphe

❑ DURCISSEMENT (HARDENING)

SécurisationsystématiquedesOSetservices. Justification technique de chaque mesure via
des fiches méthodes détaillées.

- Mise en page d'une cybersecurité cohérente

SEC_CORE_V3



CONFIDENTIALITÉ



INTÉGRITÉ



DISPONIBILITÉ

STRATÉGIE : Accompagnement de STOCKME dans la
protection des données via une approche CIA Triad
rigoureuse.

CONCLUSION & PERSPECTIVES

12

✓ SYNTHÈSE DU PROJET

- 🏗️ Architecture multi-sites opérationnelle et sécurisée.
- 👤 Plan d'adressage IP conforme aux contraintes DSI (No Class C).
- 👤 Mise en conformité RGPD et durcissement des services.

🚀 ÉVOLUTIONS FUTURES

- 📁 Automatisation des sauvegardes et déploiement PRA/PCA.
- ☁️ Intégration du serveur Bare Metal SCALEWAY.
- 👁️ Extension du monitoring à l'ensemble du parc applicatif.

