Plan-projet de sécurisation – OpenPharma

Version du 27/08/2025

1. Contexte et objectifs

- Mettre l'architecture en conformité avec les **guides ANSSI** (« Cartographie du SI » 2018 ; « Administration sécurisée des SI » v3.0).
- Renforcer le **cloisonnement** (VLAN/zones), la **journali-sation**, l'**administration** via **bastion**, et le **maintien en condition de sécurité** (MCS).

2. Constats et failles (état initial)

- Administration non centralisée, absence de **bastion** et d'**authentification forte** pour l'administration distante.
- Protocoles non sécurisés détectés : LDAP → LDAPS, HTTP → HTTPS, Syslog → Syslog TLS, SIP → SIP TLS, FTP → SFTP/FTPS, Telnet → SSH.
- Segmentation **VLAN** incomplète / flux trop permissifs entre zones.
- Pas de **DMZ** dédiée pour l'exposition Web et le proxy inverse.
- Journalisation **dispersée**, absence de **SIEM** central et de synchronisation NTP de référence.
- Mises à jour dispersées et non centralisées, nécessitant la mise en place d'un **relais interne de mise à jour**.
- Sauvegardes locales sans séparation forte (**NAS** dédié + copie **offsite** chiffrée).

3. Cibles et mesures (état cible)

- **Cloisonnement** : VLAN par rôle (Directions / Labo / Études / Technique / Admin / DMZ / Serveurs / Impression / ToIP / Sauvegardes / Supervision) ; **transit P2P** FW↔L3 (IPv4 /31 ; IPv6 ULA /127).
- **Pare-feux** : FW externe (terminaison **IPsec/IKEv2**), FW interne (filtrage inter-VLAN, matrice des flux).
- **Bastion** (Teleport) : **MFA FIDO2**, enregistrement des sessions, accès restreint aux cibles d'admin.
- **Annuaire sécurisé** : **LDAPS** via **ADCS**, certificats internes ; comptes **admin dédiés** (R27/R29/R30).

- **Journalisation** : **Wazuh + rsyslog (TLS 6514)** ; NTP interne pour horodatage fiable (R46/R47).
- **MCS** : **WAPT** (Windows) + **apt-cacher-ng** (Linux) ; validation/recette correctifs (R42–R44).
- **Sauvegardes** : **Veeam** → NAS (**ZFS**) → **rclone** chiffré vers cloud (3-2-1).

3bis. Modalités d'hébergement

- **Salle serveur interne (local technique sécurisé)** :
    - Accueille le serveur **Hyper-V 2022** (hébergeant toutes les VMs d'infrastructure : ADDS/ADCS, Bastion, Wazuh, WAPT/apt-cacher-ng, Veeam, Monitoring, Traefik+Crowdsec).
    - Contrôles physiques (accès restreint, verrouillage baie 13U).
    - Alimentation secourue (onduleur, protections surtension).
- **DMZ (derrière FW externe, cloisonnée par FW interne)** :
    - Héberge la **VM Traefik + CrowdSec** pour l'exposition web publique.
    - Aucun serveur interne n'est exposé directement : seul le reverse proxy communique avec Internet.
- **NAS sauvegardes (Synology RS822+)** :
    - Installé dans la baie réseau (4U restants utilisés).
    - Dédié uniquement aux sauvegardes Veeam (snapshots immuables, réplication chiffrée via rclone).
    - Cloisonné dans un VLAN **Sauvegardes** séparé, non accessible aux postes utilisateurs.
- **Bastion d'administration (Teleport)** :
    - Hébergé en VM sur Hyper-V, mais isolé dans son propre VLAN **Admin**.
    - Accessible uniquement via VPN IPsec (terminaison FW externe).
    - Enregistre toutes les sessions, avec MFA obligatoire (clés FIDO2).
- **Supervision & journaux (Wazuh, Prometheus/Grafana, rsyslog)** :
    - Consolidés sur une VM dédiée (VLAN Supervision).
    - Journalisation centralisée de tous les équipements et serveurs (Syslog TLS 6514).
    - Accès réservé aux administrateurs via Bastion.

4. Équipements/logiciels (avec correspondance mesures)

- **FW interne NGFW** : filtrage inter-VLAN, IPS/AV/DPI ; terminaisons IPsec côté externe.
- **Switch L3 manageable** : SVI, ACL inter-VLAN…
- **Serveur Hyper-V 2022** : héberge ADDS/ADCS, Bastion, Wazuh, WAPT/apt-cacher-ng, Veeam, Monitoring, Traefik+Crowdsec.

- **NAS sauvegardes** : dépôt Veeam, snapshot immuable, réplication **offsite** chiffrée (rclone).
- **2 postes Admin dédiés** : VLAN Admin sans Internet, accès Bastion uniquement.
- **Clés FIDO2** : MFA pour accès Bastion.

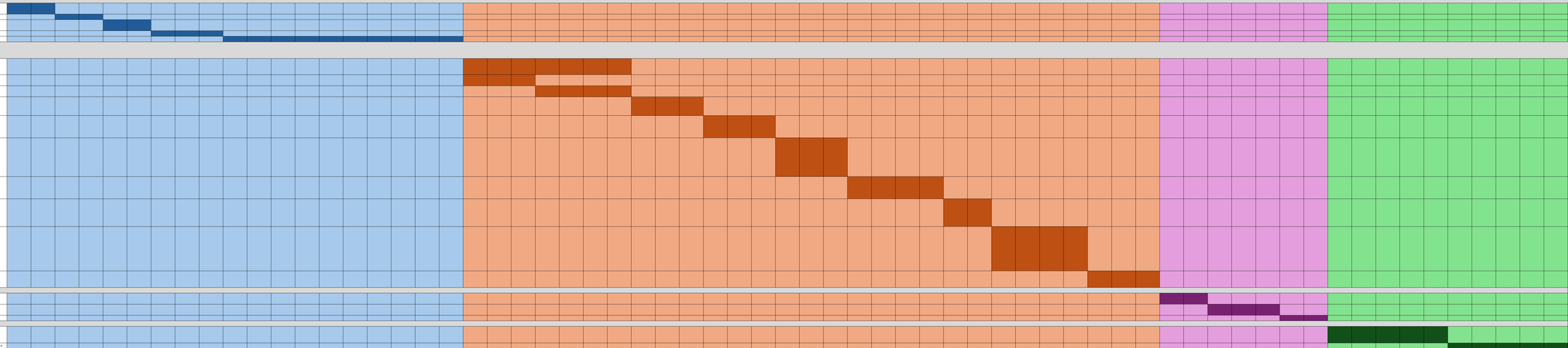
5. Chiffrage (HT)

Description	Qté	Total HT (€)
FortiGate-60F	2	2001.86
HPE Aruba 6000 24G 4SFP Switch	1	409.91
2 CS/TC ThinkCentre neo 50q Gen 4 730 - 12M20002FR	2	588.00
Ecrans Philips V-line 221V8A	2	150.00
Kensington VeriMark Guard	4	273.28
Synology RackStation RS822+	1	1109.95
Seagate IronWolf ST10000VN000 - disque dur - 10 To - SATA 6Gb/s - ST10000VN000	4	938.16
StarTech.com Étagère Rack 19 pouces 1U	1	52.99
Proliant Dl20 Gen11 Server - P65394-421	1	1718.48
Kingston Server Premier - DDR5 - module - 32 Go - DIMM 288 broches - 5200 MHz / PC5-41600 - mémoire sans tampon - KSM52E42BD8KM-32HA	4	755.16
Kingston DC600M - SSD - Mixed Use - 1.92 To - SATA 6Gb/s - SEDC600M/1920G	4	1134.68
Cable multibrin FUTP CAT6 gris CCA 100 m - 611922	1	55.28
Connecteur a sertir 8P8C RJ45 CAT6 UTP peigne separe pour monobrin lot de 10 - 920816	1	3,85
Manchon RJ45 jaune clipsable diametre 6 mm (sachet de 10 pcs) - 253016	1	2,25

Total HT estimé : **9193.85 €** (≤ 10 000 € HT).

6. Planning

ID	Tâche	Durée	Date début	Date limite	Attribution
1 Etude de la solution					
1.1	Etude de l'architecture actuelle	2 j	18/08/2025	19/08/2025	Maxi BENE
1.2	Choix du matériel	2 j	20/08/2025	21/08/2025	Maxi BENE
1.3	Vérification des délais de livraison	2 j	22/08/2025	25/08/2025	Maxi BENE
1.4	Création du devis	3 j	26/08/2025	28/08/2025	Maxi BENE
1.5	Validation du devis	10 j	29/08/2025	11/09/2025	Laurie Garrido
2 Déploiement					
2.1	Commande et réception du matériel	8 j	12/09/2025	22/09/2025	Maxi BENE
2.2	Fabrication des câbles	3 j	12/09/2025	16/09/2025	Cynthia Caouren
2.3	Câblage horizontal (plafond, murs)	4 j	17/09/2025	22/09/2025	Cynthia Caouren
2.4	Installation du serveur, switch L3 et firewalls	3 j	23/09/2025	25/09/2025	Maxi BENE + Hicham Laouini
2.5	Configuration Hyper-V & modèles VM (socle virtualisation + NTP AD)	3 j	26/09/2025	30/09/2025	Maxi BENE
2.6	Mise en place des VLANs & routage L3 (infrastructure réseau interne)	2 j	01/10/2025	03/10/2025	Maxi BENE
2.7	Configuration Firewalls (externe + interne)	2 j	06/10/2025	09/10/2025	Maxi BENE
2.8	Mise en place Bastion d'administration	2 j	10/10/2025	13/10/2025	Maxi BENE
2.9	Déploiement Services d'infrastructure (AD/DNS/DHCP, mises à jour, supervision)	4 j	14/10/2025	17/10/2025	Maxi BENE + Hicham Laouini
2.10	Déploiement DMZ (serveur web + règles FW)	3 j	20/10/2025	22/10/2025	Hicham Laouini
3 Test					
3.1	Validation des flux (matrice VLAN)	2 j	23/10/2025	24/10/2025	Maxi BENE
3.2	Tests de sécurité (bastion, règles FW)	3 j	27/10/2025	29/10/2025	Maxi BENE + Hicham Laouini
3.3	Mise en production	2 j	30/10/2025	31/10/2025	Maxi BENE
4 Support					
4.1	Documentation administrateurs + utilisateurs	5 j	03/11/2025	07/11/2025	Maxi BENE
4.2	Suivi des incidents	5 j	10/11/2025	14/11/2025	Cynthia Caouren + Hicham Laouini



Ressources humaines (estimation) :

- **Maël BENE : 46 JH** (Chef de projet et Administrateur système, réseau et sécurité)
- **Hicham Laouini : 23 JH** (Administrateur Systèmes)
- **Cynthia Caouren : 12 JH** (Technicien informatique)

7. Critères d'acceptation

- Tous les flux non listés dans la **matrice des flux** sont **bloqués** par défaut.
- Authentification **LDAPS** opérationnelle ; **Bastion** avec **MFA FIDO2** ; **journaux centralisés** horodatés (NTP).
- **Sauvegardes** : restauration testée (fichiers & VM), **offsite** chiffré.
- **MCS** : relais MAJ fonctionnels, procédure de recette validée.

8. Références ANSSI

- **Administration sécurisée des SI v3.0** : R15 (réseau d'admin dédié, p.23), R16 (filtrage & matrice des flux, p.24), R18 (interfaces d'admin dédiées, p.25-26), R19–R21 (flux d'admin & IPsec, p.26-27), R24 (protocoles chiffrés, p.30), R42–R44 (MCS & relais MAJ, p.39-40), R46-R47 (journalisation, p.41-42).
- **Cartographie du SI (2018)** : vues, jalons, responsabilités (p.6-7, 14), exemples de **postes dédiés** (p.50-52).