[Date]

Xavier Martin

CHU Ynov

DOCUMENT D’ARCHITECTURE RÉSEAU ET SERVICES MÉTIERS

CHU Ynov

Table des matières

[Contexte et objectifs 2](#_Toc202478524)

[Objectifs et portée 3](#_Toc202478525)

[Contexte général et contraintes 4](#_Toc202478526)

[Infrastructure et Réseau 5](#_Toc202478527)

[Bonnes pratiques mises en œuvre 8](#_Toc202478528)

[Réseau 9](#_Toc202478529)

[Systèmes 10](#_Toc202478530)

[Services métiers 12](#_Toc202478531)

# Contexte et objectifs

Le CHU dispose d’un système d’information critique hébergeant des données de santé sensibles.

L’architecture réseau doit garantir sécurité, confidentialité et disponibilité des services (dossier patient, imagerie médicale, etc.) tout en isolant les différents environnements (Production, Pré-production, Développement) et segments du réseau.

Les règles de sécurité exigent notamment la segmentation stricte du réseau (VLAN, DMZ) et l’authentification de tous les équipements connectés.

Ce document détaille l’infrastructure réseau, la répartition des hôtes et services métiers, les bonnes pratiques appliquées et les configurations à mettre en œuvre.

Objectifs et portée

**Objectifs du document :**

Fournir une vue complète et formelle de l’architecture réseau du CHU

Décrire la segmentation en VLAN, le routage, les politiques de filtrage

Cartographier les services métiers et leur répartitio

Détail des configurations déjà mises en œuvre

Donner un support de référence pour la maintenance, l’évolution, l’audit

**Portée :**

Réseau interne (Production, Préproduction, Test, PRA)

Zone DMZ exposée à Internet

Services métiers hébergés (DPI, RIS/PACS, LIMS, pharmacie, annuaires, DNS/DHCP, etc.)

Infrastructure virtualisée et physique

# Contexte général et contraintes

Le CHU Ynov est un établissement de santé critique, soumis à :

PGSSI-S (Politique Générale de Sécurité des SI de Santé)

RGPD

Référentiels HDS (Hébergeur de Données de Santé)

Bonnes pratiques ANSSI pour la protection des SI critiques

Contraintes majeures :

Confidentialité des données patients

Intégrité des flux médicaux (RIS/PACS, prescriptions)

Disponibilité maximale (7j/7, 24h/24)

Auditabilité et traçabilité des accès et actions

# Infrastructure et Réseau

L’infrastructure réseau suit un modèle multicouche (cœur/distribution/accès) avec des commutateurs redondants (LACP, RSTP) et des pares-feux en cluster pour assurer la haute disponibilité.

Le trafic est segmenté en VLAN selon la nature des services (par exemple : admin, médical clinique, imagerie, IoT médical, invités, management, etc.) pour limiter le périmètre d’un incident.

Chaque VLAN correspond à un sous-réseau IP distinct géré par des serveurs DHCP ou des IP fixes selon le service.

Les couches de gestion (horodatage via NTP, DNS interne, authentification) sont sur un VLAN séparé pour réduire la surface d’attaque.

L’accès aux réseaux sensibles est contrôlé via 802.1X : tous les équipements autorisés doivent s’authentifier (802.1X sur commutateurs), et ceux ne le supportant pas sont isolés sur un VLAN invité ou bloqués.

**Zone démilitarisée (DMZ) :** Une ou plusieurs DMZ sécurisées isolent les services accessibles depuis Internet (site web institutionnel, serveur SMTP/IMAP, portail patient, passerelle VPN, etc.).

Par exemple, un pare-feu frontal sépare Internet du réseau interne et redirige uniquement les flux autorisés vers les serveurs hébergés en DMZ.

**Segmentation VLAN :** Chaque service métier critique (gestion administrative, explorations radiologiques, laboratoires, pharmacie, etc.) est sur un VLAN dédié.

Un VLAN séparé regroupe les équipements non gérés (imprimantes, accès visiteurs, IoT non critiques) pour les circonscrire.

Les VLANs doivent être accompagnés d’inspections L3 (ACL sur routeurs/pare-feu) pour interdire le trafic non autorisé.

Accès sans-fil : Le Wi-Fi est segmenté en au moins deux SSID : un pour les utilisateurs internes (authentification WPA2-Enterprise 802.1X, VLAN sécurisé) et un pour les invités (accès restreint, filtrage).

Le trafic interne ne doit pas transiter par les réseaux invités.

Interconnexion des sites : Si le CHU couvre plusieurs sites géographiques, ils sont reliés par des liens MPLS ou VPN chiffrés.

Des VLAN de management spécifiques (dans une DMZ privée de liaison) isolent la gestion des équipements (commutateurs, pare-feu) du trafic production.

Hôtes et services métiers

Les services métiers sont virtualisés sur un cluster de serveurs physique (par exemple VMware, Hyper-V ou cluster Linux KVM), avec stockage SAN/NAS centralisé pour la résilience des données (notamment PACS pour imagerie) et sauvegardes régulières.

Chaque service tourne sur un ou plusieurs hôtes virtuels selon la charge et la criticité.

Infrastructure : Commutateurs cœur, répartiteurs de charge (load balancers) et pare-feu en haute disponibilité. Serveurs virtuels pour le contrôle de domaine (AD/DNS/LDAP), DHCP, et services de sécurité (PKI, NTP).

Serveurs de base de données : Bases de données métier (hospitalisation, gestion pharmaceutique, etc.) sur serveurs dédiés en cluster ou haute disponibilité, sur VLAN interne fermé, accessibles uniquement depuis les applications métier.

**Applications métiers :**

Système d’information hospitalier (DPI/EHR) : Frontend web et middleware applicatif hébergés en DMZ interne (pour les portails) et VLAN interne, avec backends DB.

Imagerie médicale (PACS, DICOM) : Serveurs de stockage et serveurs d’accès PACS isolés sur un VLAN dédié (accès par consoles radiologues uniquement).

Gestion de laboratoire et pharmacie : Systèmes LIS/RIS sur VLAN métiers, communication uniquement avec le DPI et le réseau administratif.

Messagerie et collaboration : Serveur mail (SMTP/IMAP) en DMZ pour le trafic avec l’extérieur, connecté à un VLAN interne pour l’annuaire et stockage.

Appels d’urgence / téléphonie IP : Si VoIP, contrôleurs SIP en réseau de voix dédié, isolé du réseau data par VLAN et QoS.

Services transverses : Système de GED/documentation, plate-forme web (intranet), systèmes de recherche (biobanques), etc., chacun sur VLANs adaptés.

Environnements de développement : Les réseaux de test et préproduction sont strictement séparés (VLAN et sous-réseaux distincts) de la production pour éviter toute interférence.

Ils peuvent être placés en DMZ interne séparée ou sur un VLAN protégé, avec accès limité aux équipes de développement.

Voici un tableau de répartition des vlans par utilisation métier :

|  |  |  |  |
| --- | --- | --- | --- |
| Service | Environnement | VLAN cible | Hôtes/VM configurés |
| Dossier Patient Informatisé | Prod | Trust/Médical | 3 VM (frontend, middleware, DB) |
| RIS/PACS | Prod | Trust/Médical | 2 serveurs PACS, 1 serveur DICOM |
| LIMS/Pharmacie | Prod | Trust/Médical | 2 VM (app + DB) |
| AD/DNS/DHCP | Prod | Trust/Admin | 2 DC Windows 2019 en cluster |
| SMTP Relay | Prod | DMZ | 1 VM Postfix/Exchange Edge |
| Reverse Proxy / Portail | Prod | DMZ | 2 VM Nginx en load-balancing |
| Oracle RAC | Prod | BDD | 2 nœuds Oracle RAC sur VLAN BDD |
| Supervision (Zabbix) | Prod | Admin 2 | 1 VM Zabbix Server + agents sur tous hôtes |
| Préproduction | Préprod | VLAN dédiés séparés | Clones des VM prod sur réseau isolé |
| Test | Test | VLAN séparé | VM sur VLAN test, accès limité |
| PRA | PRA | Réplication distante | Oracle Data Guard + sauvegardes Rubrik/Veeam |

# Bonnes pratiques mises en œuvre

L’architecture intègre les principes de défense en profondeur et de sécurité recommandés pour le secteur de la santé :

Segmentation stricte : Réseaux segmentés (VLAN) et filtres entre segments (pare-feu/ACL) pour limiter la propagation d’attaques.

Chaque zone (frontend, middleware, backend) contient des fonctions homogènes afin qu’un compromis d’un serveur n’offre pas un accès immédiat à d’autres.

Les équipements critiques (PACS, DPI) sont dans des VLAN isolés avec règles de communication minimales.

Zone DMZ : Les services exposés à Internet sont hébergés en DMZ cloisonnée du SI interne.

Les flux entrants non sollicités sont bloqués par un pare-feu frontal configuré en liste blanche (toute connexion non explicitement autorisée est interdite).

De même, tout flux sortant de l’entreprise est conduit via des passerelles (proxy web, proxy mail, DNS protégé, etc.) qui inspectent et filtrent le trafic.

Contrôle d’accès réseau (NAC) : Mise en place d’authentification 802.1X sur les ports réseaux pour identifier les équipements connectés.

Les machines non autorisées sont soit cantonnées à un VLAN invité non-sensible (accès Internet très restreint), soit bloquées complètement.

Cette démarche empêche les équipements non gérés (par exemple équipements médicaux obsolètes) de menacer le reste du SI.

Gestion des mises à jour et durcissement :

Tous les serveurs et équipements réseau suivent les recommandations de sécurité (groupe de sécurité, hardening selon ANSSI/CIS, désactivation des services inutiles, parole de passe forte, etc.).

Les postes critiques (serveurs, stations médicales) appliquent régulièrement les patches de sécurité.

Surveillance et journalisation : Les pare-feu, serveurs et équipements réseau génèrent des logs centralisés (SIEM) afin de détecter toute activité anormale.

Les tentatives bloquées sur les frontières réseau sont archivées.

Des outils IDS/IPS peuvent être déployés sur les zones sensibles pour analyser les paquets en temps réel.

Haute disponibilité et continuité :

Tous les liens et équipements clés sont redondants (double commutateur cœur, pare-feu actif/actif ou active/passive, liaisons montantes agrégées, clusters de serveurs).

Les données critiques (bases médicales, images, sauvegardes) sont répliquées sur un site secondaire ou un cloud sûr. Des plans de reprise sont formalisés.

Inventaire et classification :

Un inventaire détaillé de tous les équipements et services (type, localisation, sensibilité des données, criticité) est tenu à jour pour piloter la segmentation et la sécurité.

Cette étape préalable est indispensable pour appliquer correctement les mesures de contrôle d’accès et de compartimentage.

# Réseau

VLAN et commutateurs :

Configurer les VLAN conformément au schéma réseau (par exemple VLAN 10: interne, 20: DMZ publique, 30: DMZ sortant/proxies, 40: administration, 50: imagerie, etc.).

Activer le trunking 802.1Q sur les liaisons montantes.

Définir le switch cœur en root STP et mettre en place des agrégats de liens (LACP) entre commutateurs critiques pour la tolérance de panne.

Appliquer des ACL de niveau 2/3 sur les switches pour interdire le flooding de paquets entre VLAN (Private VLAN si nécessaire pour blocs de postes).

Pare-feu / routage : Installer un pare-feu en frontale pour séparer Internet du LAN interne. Exemples de règles : n’autoriser en entrée que le port 443 (HTTPS) vers le serveur web DMZ et le port 25 (SMTP) vers le serveur mail DMZ.

Configurer le pare-feu interne pour qu’il filtre tout trafic inter-VLAN selon la politique de sécurité (par défaut DENY).

Le routage inter-VLAN peut être effectué par le pare-feu ou un routeur L3 central, avec routing statique ou OSPF entre sites si multi-sites.

Activer NAT pour les services internet nécessaires et enregistrer les logs de connexion.

Proxy et filtrage sortant : Déployer des serveurs proxy (web, FTP, SMTP) situés dans une DMZ « sortante ».

Par exemple, le proxy HTTP (Squid) écoute sur le port 3128 sur la DMZ et accepte uniquement le trafic sortant validé. Configurer les stations clientes pour utiliser le proxy, ou bloquer tout trafic HTTP/HTTPS sortant direct sur le pare-feu.

Idem pour SMTP (relay). Le DNS interne est séparé du DNS public ; les requêtes externes passent par un DNS proxy en DMZ.

NAC (802.1X) : Configurer les switches d’accès en mode authentification réseau (ex: Radius + 802.1X).

Les ports sans authentification valide basculent sur le VLAN invité. Mettre en place des politiques MAC-ACL pour les équipements non-802.1X (MAC Authentication Bypass), en les assignant à un VLAN spécifique.

# Systèmes

Contrôleurs de domaine : Déployer au moins deux DC Windows Server (ou LDAP Unix) par forêt/répertoire, en synchronisation (mode site AD).

Les DNS pointent sur ces DC. Assurer la redondance globale (réplication AD, zone DNS secondaire). Appliquer les GPO de sécurité ANSSI.

Serveurs de bases de données : Configurer des clusters ou master-slave (SQL Server AlwaysOn, MySQL replication, etc.) pour assurer la disponibilité.

L’accès réseau aux DB est restreint : seuls les serveurs applicatifs autorisés (VLAN applicatif) peuvent se connecter aux ports DB.

Stockage et sauvegarde : Provisionner du NAS/SAN avec snapshots.

Mettre en place un logiciel de sauvegarde qui copie les données critiques sur un site secondaire ou dans le cloud (chiffrage des données à repos et en transit).

Tester régulièrement la restauration.

Chiffrement et PKI : Déployer une PKI interne (serveur de certificats) pour émettre des certificats TLS aux serveurs internes (serveur web, VPN, AD, etc.).

Forcer l’usage de TLS sur tous les services compatibles (HTTPS, LDAPS, SMTPS, etc.).

Configurer des VPN IPsec ou SSL pour l’accès distant des administrateurs, avec segmentation des accès.

Time servers : Configurer NTP hiérarchique : un serveur NTP interne (éventuellement synchronisé sur un serveur public fiable) et tous les équipements et serveurs configurés pour le consulter.

**Plateformes de virtualisation**

Environnement virtualisé basé sur VMware vSphere 7 :

Cluster Prod

4 nœuds physiques Dell PowerEdge R750

Processeurs Intel Xeon Gold, 512 Go RAM par nœud

Stockage SAN Dell EMC PowerStore RAID10, double contrôleur

Réseau uplink 10 GbE

Cluster Préproduction/Test

2 nœuds physiques identiques, isolés en VLAN dédié

Cluster PRA

2 nœuds physiques sur site distant (>10 km)

Réplication asynchrone via Veeam/Rubrik

Répartition des VM métiers:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service | Environnement | Nombre VM | OS | Rôle |
| DPI/EHR | Prod | 3 | Linux RHEL 8 | Frontend web, Middleware, DB client |
| RIS/PACS | Prod | 3 | Windows Server | Serveurs PACS, DICOM, stockage imagerie |
| LIMS/Pharmacie | Prod | 2 | Linux RHEL 8 | App serveur + DB |
| AD/DNS/DHCP | Prod | 2 | Windows Server | DC en cluster, DNS AD-integrated |
| SMTP Relay | Prod | 1 | Linux Ubuntu | Postfix relay en DMZ |
| Reverse Proxy | Prod | 2 | Linux Ubuntu | Nginx + Certbot en DMZ |
| Oracle RAC | Prod | 2 | Oracle Linux | Cluster RAC, VLAN BDD |
| Supervision (Zabbix) | Prod | 1 | Linux Ubuntu | Server + agents installés partout |
| Préproduction | Préprod | ~10 | Linux/Windows | Clones de Prod |
| Test | Test | Variable | Linux/Windows | VM dédiées iso VLAN |
| PRA | PRA | ~12 | Linux/Windows | Réplicas, Data Guard, backup restores |

# Services métiers

Serveur Web / Application : Chaque application web (portail patient, intranet médical) est hébergée sur un ou plusieurs serveurs derrière un WAF/appliquer de règles.

Par exemple, n’ouvrir en DMZ que le port 443 vers le serveur web frontend.

Séparer les couches Web/Applicative dans différentes sous-réseaux ou serveurs virtuels, si possible.

Pare-feu interne et DMZ : Les serveurs applicatifs internals sont placés derrière un pare-feu interne.

Configurez des règles minimales : ex. seul le serveur Web DMZ peut se connecter au serveur d’applicatif interne sur le port nécessaire, et celui-ci au serveur de base de données sur le port SQL.

Tout accès externe doit transiter par la DMZ frontal.

Serveur mail : Le serveur SMTP public est en DMZ. Configurer un relais interne pour envoyer en sortie (ex: postfix avec restriction via proxy), et un relais pour le courrier entrant filtré.

Les ports SMTP (25) et MAPI/HTTPS pour les clients sont isolés sur leur VLAN.

Stockage et partage de fichiers : Configurez le serveur de fichiers (dossiers patients, documents) avec ACL Windows/Unix.

Montez-le sur un VLAN interne restreint. Appliquer des quotas et journaux d’accès.

Imagerie médicale (PACS) : Le serveur DICOM est sur un VLAN dédié. Limiter l’accès réseau aux seules stations radiologiques et aux systèmes PACS.

S’assurer que le volume des images ne surcharge pas le réseau principal (QoS si nécessaire).

Chaque configuration doit être documentée et testée. Les politiques de sécurité (firewall, VLAN, accès) font l’objet d’un plan de filtrage formalisé conforme aux règles internes.

Par exemple, la politique réseau rédigée clairement aidera à définir quels services sont autorisés entre chaque segment (cf. schéma réseau annexé).