[Date]

Xavier Martin

CHU Ynov

Architecture réseau et configuration

Table des matières

[1 Introduction et objectifs 2](#_Toc202475309)

[2 : Périmètre général du réseau 3](#_Toc202475310)

[3 : Schéma global d’architecture 4](#_Toc202475311)

[4 : Zones réseau et VLAN 5](#_Toc202475312)

[5. PARE-FEU PFSENSE 6](#_Toc202475313)

[6. Serveur DHCP 12](#_Toc202475314)

[7. Serveur DNS 16](#_Toc202475315)

[8. Serveur Oracle 19](#_Toc202475316)

# 1 Introduction et objectifs

Ce document présente l’architecture réseau et la configuration détaillée des principaux équipements d’infrastructure du CHU Ynov, avec un accent sur la sécurité, la segmentation réseau, et la conformité réglementaire.

Il vise à :

Formaliser l’architecture réseau pour l’équipe DSI/SSI.

Documenter les flux, VLAN, ACL et règles.

Décrire la configuration des services critiques (pare-feu, DHCP, DNS, Oracle).

Assurer l’auditabilité et la maintenabilité.

Respecter les obligations PGSSI-S, HDS, RGPD.

# 2 : Périmètre général du réseau

Le réseau du CHU est conçu pour :

Séparer les zones fonctionnelles (clinique, administrative, biomédicale, DMZ).

Protéger les données sensibles de santé.

Garantir la disponibilité des applications DPI, RIS/PACS, LIMS, etc.

Supporter des environnements Production, Préproduction, Test.

L’architecture s’appuie sur :

VLAN dédiés

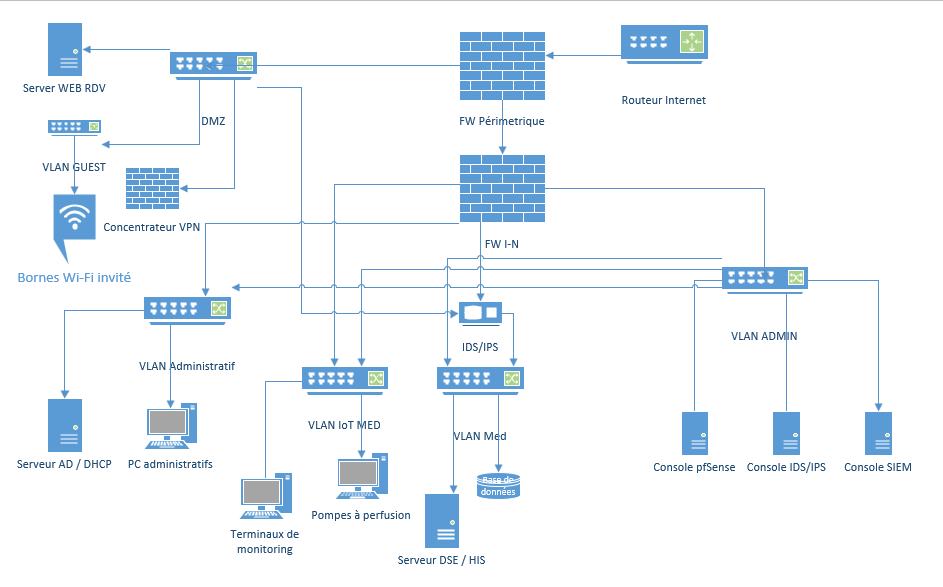
Pare-feu centralisé Pfsens

Services DHCP et DNS centralisés

Bases de données Oracle isolées

# 3 : Schéma global d’architecture

Voici un schéma de l’infrastructure du CHU :



# 4 : Zones réseau et VLAN

Dans cette partie va être présenter les différents réseaux du CHU.

Le principe de cloisonnement : diviser le réseau du CHU en sous-segments logiques/physiques (ex. « Admin », « Soins », « DMZ/public », « Guest Wi-Fi », « Imagerie », « Objets médicaux connectés »). Chacun fait l’objet de règles distinctes.

Vlan administratif : 192,168,16,0/20

Vlan IoT MED : 172,16,0,0/16

Vlan med : 10.17.0.0/16

VLAN ADMIN : 10.24.0.0/24

DMZ : 192.,168.254.0/24

Objectif : limiter la propagation des attaques en cas de compromission d’un segment. Sans ce cloisonnement, « le manque de cloisonnement favorise la propagation de codes malveillants et le chiffrement généralisé des infrastructures » Par exemple, un ransomware qui infecte un PC de secrétariat ne doit pas pouvoir chiffrer tous les serveurs de soins.

Techniques : VLAN et sous-réseaux IP couplés à des pare-feux internes pour filtrer le trafic inter-segments. Par exemple, un accès de la DMZ (serveurs web publics) vers le réseau interne doit être strictement controlé. Mise en place de zones de sécurité au niveau 3 (pare-feu L3) et ACL réseau. L’approche Zero-Trust (authentification/micro-segmentation constante) peut aussi être envisagée.

DMZ : services exposés (web de prise de RDV, VPN externe) isolés dans une DMZ filtrée. Le routage inter-DMZ vers réseau interne doit passer par des contrôles (pare-feu, inspection).

Chaque VLAN = 1 sous-réseau / 1 zone de sécurité. Les Pare-feu applique filtrage inter-zone strict.

# 5. PARE-FEU PFSENSE

**5.1. Présentation et principes généraux**

Le pare-feu Pfsense constitue le point de contrôle central du réseau du CHU.

Il est conçu pour :

Segmenter logiquement le SI en zones de sécurité.

Appliquer le principe deny by default sur tous les flux interzones.

Filtrer en profondeur avec App-ID, User-ID, Content-ID.

Inspecter le trafic entrant et sortant, y compris le trafic chiffré.

Fournir des fonctionnalités NAT, haute disponibilité et journalisation avancée.

Le pare-feu s’intègre dans la démarche PGSSI-S / HDS, garantissant la confidentialité, l’intégrité et la traçabilité des flux de données de santé.

**5.2. Architecture et intégration réseau**

Le pare-feu Pfsense est placé en frontière entre les zones internes, la DMZ et l’Internet. Il dispose de plusieurs interfaces physiques ou sub-interfaces en trunk :

|  |  |  |  |
| --- | --- | --- | --- |
| Interface | VLAN associé | Zone Palo Alto | Description |
| ethernet1/1 | Untrust | Untrust | Vers Internet / opérateur WAN |
| ethernet1/2 | DMZ | DMZ | Serveurs exposés (portails, proxy) |
| ethernet1/3 | Trust | Trust | Réseaux internes (Clinique, Admin, etc.) |
| ethernet1/4 | Infra | Infra | DNS, DHCP, NTP |
| ethernet1/5 | BDD | BDD | Serveurs Oracle |

Trunk 802.1q possible sur interfaces pour plusieurs VLAN.

Routage statique ou dynamique (OSPF/BGP si inter-sites).

**5.3. Concept de Zones**

Les zones sont des containers logiques pour appliquer des politiques.

Les flux sont autorisés entre zones uniquement via des policies explicites.

Aucune règle inter-zone par défaut (deny all).

Inspection stateful (sessions suivies bidirectionnelles).

Exemple de zones définies :

Untrust : Internet public

DMZ : Serveurs exposés (HTTPS, Apicrypt, MSSanté)

Trust : Réseaux internes (DPI, RIS/PACS, LIMS)

Infra : Services d’infrastructure

BDD : Serveurs Oracle

**5.4. Politiques de sécurité (Security Policies)**

**5.4.1. Politique générale**

Deny by default.

Politique explicite pour chaque flux autorisé.

Logging systématique des allow et deny.

**5.4.2. Exemples de règles**

|  |  |  |  |
| --- | --- | --- | --- |
| Source Zone | Dest Zone | Application/Service | Action |
| Trust | Untrust | HTTPS, SMTP | Allow |
| Untrust | DMZ | HTTPS (portail) | Allow |
| Trust | BDD | Oracle (TCP/1521) | Allow |
| DMZ | Trust | Aucun par défaut | Deny |
| Infra | Trust | DNS/UDP53, DHCP | Allow |

Bonnes praitques :

Nommage clair des règles (« Trust\_to\_BDD\_Oracle »).

Regroupement des règles par zones.

Description obligatoire dans chaque policy.

**5.5. NAT (Network Address Translation)**

Dans le cadre de la segmentation réseau du CHU, chaque VLAN interne voit son trafic sortant vers Internet NATé sur l’IP publique du pare‑feu, tandis que les services exposés en DMZ bénéficient d’un DNAT entrant. Les VLAN et plans d’adressage sont :

|  |  |  |
| --- | --- | --- |
| VLAN | Sous‑réseau | Zone Palo Alto |
| Administratif | 192.168.16.0/20 | Trust/Admin |
| IoT Médical | 172.16.0.0/16 | Trust/IoT |
| Médical (DPI, PACS) | 10.17.0.0/16 | Trust/Med |
| Support (Admin 2) | 10.24.0.0/24 | Trust/Admin2 |
| DMZ | 192.168.254.0/24 | DMZ |

**5.5.1. Source NAT (SNAT) – trafic sortant**

Objectif : masquer toutes les IP privées des VLAN internes derrière l’adresse publique du pare‑feu (203.0.113.10) pour les accès Internet.

Règle type :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nom de règle | Source Zone | Source Address | Dest Zone | Translation Type | IP publique |
| SNAT\_Administratif | Trust/Admin | 192.168.16.0/20 | Untrust | Dynamic IP and Port (Hide) | 203.0.113.10 |
| SNAT\_IoT\_Medical | Trust/IoT | 172.16.0.0/16 | Untrust | Dynamic IP and Port (Hide) | 203.0.113.10 |
| SNAT\_Medical | Trust/Med | 10.17.0.0/16 | Untrust | Dynamic IP and Port (Hide) | 203.0.113.10 |
| SNAT\_Admin2 | Trust/Admin2 | 10.24.0.0/24 | Untrust | Dynamic IP and Port (Hide) | 203.0.113.10 |

Notes

Chaque VLAN interne NATe vers la même IP publique pour centraliser les flux sortants.

Le pare‑feu conserve l’état des sessions pour restituer correctement les paquets entrants.

**5.5.2. Destination NAT (DNAT) – trafic entrant**

Objectif : rendre accessibles depuis Internet certains services hébergés en DMZ (192.168.254.0/24).

Règles typiques :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nom de règle | Source Zone | Dest Zone | Public IP | Public Port | Private IP | Private Port | Service |
| DNAT\_Web\_DMZ | Untrust | DMZ | 198.51.100.20 | TCP/443 | 192.168.254.20 | TCP/443 | HTTPS portail |
| DNAT\_Mail\_DMZ | Untrust | DMZ | 198.51.100.21 | TCP/25 | 192.168.254.21 | TCP/25 | SMTP serveur |

Notes

Utiliser des IP publiques distinctes pour chaque service (portail web, mail, VPN SSL, etc.).

Les règles DNAT doivent toujours être suivies d’une policy de sécurité Untrust → DMZ autorisant le port et l’IP privée cible.

**5.5.3. Configuration CLI / GUI**

CLI Example – SNAT:

set rulebase nat rules SNAT\_Administratif source-zone Trust\_Admin destination-zone Untrust source-address 192.168.16.0/20 service any to interface ethernet1/1 translation-type dynamic-ip-and-port interface-address 203.0.113.10

CLI Example – DNAT:

set rulebase nat rules DNAT\_Web\_DMZ source-zone Untrust destination-zone DMZ source-address any destination-address 198.51.100.20 service https translated-address 192.168.254.20 translated-port 443

**5.6. Inspection Applicative et Content-ID**

App-ID : Identification des applications (HTTPS, SSH, SMB).

User-ID : Intégration Active Directory pour policies basées sur users/groups.

Content-ID :

Antivirus

Anti-spyware

URL Filtering

File Blocking

SSL Decryption (optionnel pour flux internes si RGPD-compliant).

**5.7. Threat Prevention**

Signature-based IDS/IPS.

Mises à jour quotidiennes.

Blocage des exploits connus.

Protection contre les C2 / malware.

Intégration WildFire (sandboxing cloud ou local).

**5.8. Journalisation et SIEM**

Logs de trafic envoyés vers SIEM centralisé.

Logs de configuration (admin audit trail).

Export syslog sécurisé (TLS/UDP 514).

Corrélation d’événements (alertes phishing, ransomware).

**5.9. Haute Disponibilité (HA)**

Mode Active/Passive :

Configuration synchronisée

Monitoring des interfaces et des liens

Failover automatique sur panne

Tests annuels planifiés.

**5.10. Supervision et monitoring**

Supervision via SNMPv3.

Monitoring via Zabbix/Centreon.

Intégration avec SOC régional GHT.

Alertes en temps réel sur :

Chute interface

Haute CPU

Tentatives d’attaque

Blocage en failover

**5.11. Configuration de sauvegarde**

Export automatique hebdomadaire de la configuration.

Sauvegarde chiffrée sur espace réseau sécurisé.

Politique de rétention 12 mois.

Vérification manuelle après modification majeure.

# 6. Serveur DHCP

**6.1. Positionnement et rôle**

Le serveur DHCP est un service critique, placé dans le VLAN Infra (192.168.16.0/20), zone dédiée aux services d’infrastructure. Il fournit automatiquement :

L’adresse IP, le masque de sous‑réseau et la passerelle par défaut.

L’adresse des serveurs DNS (option 6), NTP (option 42), WINS (option 44) si nécessaire.

D’autres options spécifiques (option 15 : nom de domaine, option 66/67 : Bootp pour PXE).

Architecture :

Serveur principal : machine Windows Server ou Linux (ISC DHCP), hébergée en VM HDS.

Serveur secondaire (facultatif) : instance failover en mode hot standby pour assurer la disponibilité.

Relais DHCP (IP Helper) : activé sur les routeurs/firewall inter-VLAN pour distribuer les baux aux clients de chaque VLAN.

**6.2. Pool, scopes et plan d’adressage**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VLAN | Sous‑réseau | Plage DHCP | Réservations | Commentaires |
| Administratif | 192.168.16.0/20 | 192.168.16.100–16.199 | Imprimantes, Wi‑Fi AP | 4 096 adresses – plage restreinte + réservations |
| IoT Médical | 172.16.0.0/16 | 172.16.0.100–0.65534 | Capteurs, pompes à perfusion | Séparer IoT pour sécurité |
| Médical (DPI, PACS) | 10.17.0.0/16 | 10.17.0.100–17.65534 | Terminaux médicaux | Flux critiques, RTO/RPO stricts |
| Support (Admin 2) | 10.24.0.0/24 | 10.24.0.50–24.200 | Serveurs internes | Petits pool pour management |

Plages dimensionnées pour laisser de la marge pour les réservations et l’évolution.

Réservations statiques identifiées dans un fichier CSV ou base de données interne pour tracer les équipements critiques.

**6.3. Options DHCP et configurations avancées**

**6.3.1. Options globales**

|  |  |  |  |
| --- | --- | --- | --- |
| Option | Description | Valeur type | Utilisation |
| 3 | Default Gateway | IP (routeur) | Définir la passerelle par défaut pour le VLAN |
| 6 | DNS Servers | Liste d’IP | 192.168.16.10, 192.168.16.11 (serveurs DNS du CHU) |
| 15 | Domain Name | Chaîne | chu.local |
| 42 | NTP Servers | Liste d’IP | 192.168.16.20 (NTP interne) |
| 66/67 | TFTP Server / Boot File | IP / Fichier | Pour PXE des terminaux ou mises à jour BIOS |

**6.3.2. Réservations**

Principe : associer l’empreinte MAC d’un équipement à une IP fixe hors plage dynamique.

Exemples :

00-1A-2B-3C-4D-5E → 10.17.0.10 (Scanner IRM)

AA-BB-CC-DD-EE-FF → 172.16.0.25 (Capteur IoT)

**6.3.3. Options spécifiques par pool**

Pool IoT Médical : Désactivation de l’option 150, activation de l’option 43 pour diffuser l’adresse du serveur de gestion IoT.

Pool Médical : délai de bail réduit à 4 h (RPO strict), bail par défaut 8 h.

Pool Administratif : bail 24 h, bail renouvelable toutes les 12 h.

**6.4. Haute disponibilité et robustesse**

**6.4.1. Mode failover**

Active/Passive :

Serveur principal attribue les baux.

Serveur secondaire en écoute, prend le relais en cas de défaillance.

Synchronisation des baux toutes les 15 minutes via protocole ISC DHCP failover.

Priorité (split = 50/50 ou 100/0 selon criticité).

**6.4.2. Sécurisation et durcissement**

Hébergement sur VM :

Sécurité hyperviseur (vSphere hardened).

Disques chiffrés (LUKS ou BitLocker).

Restriction de l’accès SSH/RDP par ACL (IP management station uniquement).

Gestion des comptes service via Managed Service Account (Windows) ou systemd user (Linux).

**6.4.3. Supervision et alerting**

Logs : journalisation des événements (dhcpd.log) sous /var/log, export vers SIEM.

KPIs :

Taux d’échec de baux < 1 %.

Disponibilité du service ≥ 99,9 %.

Alertes :

Service DHCP down (snmptrap / Zabbix).

Saturation de pool (80 % d’adresses délivrées).

**6.5. Sauvegarde et reprise d’activité**

Configuration : export régulier du fichier dhcpd.conf ou de la base SQL (selon implémentation).

Fréquence : quotidienne, stockée sur SAN HDS et replica cloud.

Procédure de reprise :

Provisionner VM secondaire.

Importer la configuration et les baux sauvegardés.

Rebasculer le relais DHCP sur la nouvelle instance.

**6.6. Sécurité réseau et ACL**

DHCP Snooping : sur les switchs Cisco pour autoriser uniquement les ports de serveurs DHCP.

IP Helper : activé sur les VLAN non-Infra pour relayer les requêtes DHCP vers l’IP du serveur.

ACL Cisco :

ip access-list extended DHCP-ONLY

permit udp host 192.168.16.5 any eq bootps

permit udp any host 192.168.16.5 eq bootpc

deny udp any any eq bootps

deny udp any any eq bootpc

permit ip any any

interface Vlan16

ip helper-address 192.168.16.5

ip access-group DHCP-ONLY in

# 7. Serveur DNS

**7.1. Rôle et architecture**

Le ou les serveurs DNS du CHU fournissent :

Résolution interne : traduction noms → adresses IP pour tous les services et hôtes du SI (VLAN Clinique, Admin, IoT Médical…).

Résolution externe : relais vers les DNS publics ou racines pour accéder à Internet.

Réponse aux requêtes inverses : association des IP aux noms d’hôtes pour les opérations d’audit et de contrôle (PTR).

Positionnement :

Installé(s) dans le VLAN Infra (192.168.16.0/20), zone dédiée aux services d’infrastructure.

Accessible uniquement depuis les VLAN internes via l’option DHCP (serveur relay).

Non accessible en écriture depuis Internet (zone Untrust), sauf éventuellement pour un serveur en DMZ dédié au DNS public.

Plateforme : Windows DNS (Active Directory–integrated) ou BIND9 sur Linux HDS.

Ports utilisés : UDP/TCP 53.

Mode maître/esclave ou cluster anycast selon la solution retenue.

**7.2. Zones internes**

|  |  |  |  |
| --- | --- | --- | --- |
| Type de zone | Nom de zone | Contenus | Mode de stockage |
| Directe | chu.local | Enregistrements A, CNAME | DNS intégré AD ou fichier |
| Inverse | 16.168.192.in-addr.arpa | Enregistrements PTR | Fichier ou AD |

**7.2.1. Zone directe (chu.local)**

Contient tous les hôtes internes :

dhs-chu.medical.chu.local → 10.17.0.10

srv-dhcp.infra.chu.local → 192.168.16.5

sql1-bdd.chu.local → 10.24.0.10

Utilisation de CNAME pour alias (ex. printer01.infra.chu.local CNAME → hp-printer01.infra.chu.local).

**7.2.2. Zone inverse**

Permet la correspondance IP → nom.

Utilisée par les logs, SIEM, et outils d’audit.

Doit couvrir chaque sous‑réseau (administratif, médical, IoT…).

**7.3. Résolution externe et forwarders**

Forwarders : pointer vers les DNS de l’Opérateur ou les root hints sécurisés (ex. 8.8.8.8, 1.1.1.1) selon la politique HDS.

Cache : activer le cache pour limiter la latence et la charge externe. TTL court (~5 min) pour les enregistrements dynamiques.

ACL de requête : autoriser uniquement les sous‑réseaux internes (192.168.16.0/20, 10.17.0.0/16, 172.16.0.0/16, 10.24.0.0/24) à interroger le serveur.

**7.4. Sécurisation et DNSSEC**

**7.4.1. DNSSEC**

Signature des zones (dnssec-signzone ou intégré AD) pour garantir l’authenticité des enregistrements.

Publication des clé KSK/ZSK dans les DS records auprès d’un parent si externe, ou utilisation uniquement interne pour validation.

Configuration du validate sur les résolveurs internes pour refuser les réponses non signées.

**7.4.2. RPZ (Response Policy Zone)**

Optionnel : utiliser une RPZ pour bloquer les domaines malveillants (ex. listes ANSSI, Cisco Talos).

Implémentation via BIND RPZ ou solution intégrée Cisco Umbrella.

7.4.3. Accès et ACL

Interdiction du transfert de zone (AXFR/IXFR) vers tout hôte non maître/esclave désigné.

TSIG pour authentifier les transferts entre maître et esclave.

**7.5. Intégration DHCP & mises à jour dynamiques**

Si DNS intégré à AD (Windows) ou BIND dynamique, activer Secure Dynamic Updates pour que le serveur DHCP écrive automatiquement les enregistrements A/PTR lors de l’attribution d’un bail.

Configurer les credentials sécurisés (groupe de services ou clé TSIG) pour autoriser uniquement le serveur DHCP à mettre à jour la zone.

Vérifier la cohérence des TTL et la suppression des enregistrements obsolètes (scavenging si AD, ndc control flush sur PowerDNS).

7.6. Haute disponibilité et clustering

7.6.1. Mode maître/esclave

Maître : principallement en écriture, version active.

Esclave : reçoit les transferts de zone, répond aux requêtes, peut prendre le relais (CNAME circulaire).

Refresh/Retry : configurés à 1 h/15 min, expire après 1 j.

7.6.2. Anycast (optionnel)

Déployer plusieurs instances DNS accessibles via la même IP anycast pour répartition de charge et résilience.

**7.7. Supervision et journalisation**

|  |  |  |
| --- | --- | --- |
| Élément | Métrique / Log | Outil |
| Service DNS | Disponibilité (UDP/TCP port 53) | Zabbix |
| Résolutions réussies | Nombre, taux d’échec | Grafana |
| Requêtes suspectes | Requêtes externes inhabituelles | SIEM (Elastic) |
| Transferts de zone | AXFR autorisés, erreurs | Logs BIND/Windows |
| Scavenging/DNSSEC | Erreurs de validation | SIEM |

Alertes : service down, échec TSIG, échecs DNSSEC.

Logs centralisés (> 12 mois) pour audit HDS/RGPD.

**7.8. Sauvegarde et reprise d’activité**

Configuration : export des fichiers de zone et de la configuration DNS (BIND named.conf, files .zone ou export AD).

Fréquence :

Zones dynamiques : toutes les 15 min (snapshots), quotidien pour les fichiers statiques.

Full backup : hebdomadaire, stocké sur SAN HDS et répliqué cloud.

Procédure de reprise :

Lancer l’instance DNS secondaire ou basculer le VIP (Cluster).

Importer les fichiers de zone ou restaurer la partition AD DNS.

Redémarrer le service DNS, vérifier la résolution interne/externe.

# 8. Serveur Oracle

(Configuration détaillée, architecture et bonnes pratiques – CHU La Timone, RSSI/DSI)

**8.1. Architecture et positionnement**

Le ou les serveurs Oracle hébergent les bases de données médicales critiques (DPI, RIS/PACS, LIMS). Ils sont déployés dans le VLAN BDD (10.24.0.0/24) – zone la plus sécurisée du réseau interne.

Topologie

Primaires : nœuds de production en cluster (RAC) ou VM individuelles selon la taille.

Standby : serveur Data Guard en PRA (automatique ou manuel).

Préproduction : clones isolés pour tests et recettes.

Infrastructure

Stockage SAN chiffré (RAID‑10), snapshots réguliers.

Réseau 10 Gbps isolé, trunk vers VMware ou hôtes physiques.

QoS garantissant la priorité aux flux BDD sur le LAN.

**8.2. Ports et flux réseau**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port | Protocole | Usage | Source | Destination (VLAN BDD) |
| 1521 | TCP | Listener Oracle (SQL\*Net) | VLAN Trust (10.17.0.0/16) | 10.24.0.0/24 |
| 5500 | TCP | Enterprise Manager (EM Express) | VLAN Admin (192.168.16.0/20) | 10.24.0.0/24 |
| 2483/2484 | TCP | TNS direct (avec SSL pour 2484) | VLAN Trust | 10.24.0.0/24 |
| 22 | TCP | SSH pour administration | VLAN Admin2 (10.24.0.0/24) | 10.24.0.0/24 |
| 2049 | TCP/UDP | NFS (si stockage distant) | VLAN BDD | SAN Storage VLAN |

ACL Pfsense :

Trust → BDD : permit tcp 10.17.0.0/16 → 10.24.0.0/24 eq 1521

Admin2 → BDD : permit tcp 10.24.0.0/24 → 10.24.0.0/24 eq 5500,22

Tout autre flux vers VLAN BDD est deny all.

**8.3. Contrôle d’accès et durcissement**

**8.3.1. Isolation réseau**

VLAN BDD uniquement accessible depuis VLAN Trust (applications) et Admin2 (supervision).

Pas de route directe depuis DMZ ou Untrust.

**8.3.2. RBAC Oracle**

Users : comptes nominatifs, jamais SYS/SYSTEM pour les applications.

Profiles : limitation des ressources (sessions, CPU).

Roles : GRANT/REVOKE pour privileges minimaux (least privilege).

Audit : audit all statements by privileged users.

**8.3.3. OS & listener**

OS : comptes UNIX restreints, sudoers limités.

Listener : sqlnet.ora configuré pour sqlnet.authentication\_services = (NONE), tcp.validnode\_checking = yes avec liste tcp.invited\_nodes.

SSL/TLS : mise en place de TCPS sur port 2484, certificats signés par PKI interne (AKV).

**8.4. Sécurisation des données**

**8.4.1. TDE (Transparent Data Encryption)**

Activation : ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "passphrase";

Clés maître : stockées dans Azure Key Vault (HSM-Backed).

Encryption wallets : auto-open via master key au démarrage.

**8.4.2. Chiffrement des backups**

RMAN configuré pour ENCRYPTION ALGORITHM 'AES256' et ENCRYPTION FOR ALL DATABASE.

Stockage des backups chiffrés sur SAN HDS et copies off-site.

**8.4.3. Data at Rest**

Disques VM chiffrés au niveau hyperviseur (vSphere VM Encryption) ou via LUKS/BitLocker sur OS.

**8.5. Haute disponibilité et reprise**

**8.5.1. Oracle RAC**

Plusieurs nœuds en cluster partageant le même stockage SAN.

Service transparent pour les applications.

**8.5.2. Data Guard**

Physical Standby en PRA : apply seul redo log.

Fast-Start Failover possible pour bascule automatique.

**8.5.3. RMAN & snapshot**

Plan : full backup hebdo, incrémental quotidien, archivelog every 15 min.

Recovery catalog centralisé sur un schéma dédié.

Test de restauration mensuel en environnement préprod.

**8.6. Supervision et alerting**

|  |  |  |
| --- | --- | --- |
| Composant | Métrique | Seuil/Action |
| Listener | Status (up/down) | Alert if down > 5 min |
| Tablespace usage | % utilisé | Alert if > 80 % |
| ASM Diskgroup health | State ok | Alert on any offline |
| Redo lag | Seconds | Alert if > 300 s |
| Backup status | RMAN job success/fail | Alert on fail |

Collecte via Oracle Enterprise Manager ou scripts SNMP.

Intégration Zabbix agent + plugin Oracle.

**8.7. Journalisation et auditabilité**

AUD$ table pour audit Oracle.

Listener logs dans $ORACLE\_HOME/network/log.

OS syslog pour SSH et root activity.

Archive logs RMAN stockés dans /u01/app/oracle/archivelog.

Export de logs vers SIEM HDS (via Filebeat ou syslog-ng).

**8.8. Sauvegarde de la configuration**

Parameter files (init.ora, spfile.ora) versionnés dans GitLab interne.

Wallet files pour TDE exportés et stockés offline.

Scripts d’automatisation (Ansible/RMF) pour patch, backup, healthcheck.

**8.9. Plan de reprise**

Échec d’un nœud RAC → bascule automatique du service.

Panne totale DC1 → activation Data Guard → bascule vers PRA (target role convert).

Corruption data → RMAN restore + flashback database si possible.

Reconstruction de la wallet → import de la master key depuis AKV.

**8.10. Conformité**

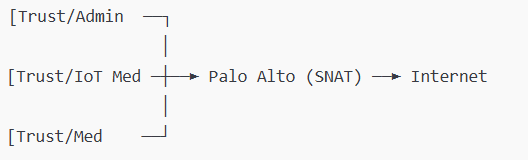
PGSSI-S / HDS : TDE, séparation des zones, audit complet.

RGPD : chiffrement, accès strict, suppression client.

ANSSI : bonnes pratiques OS, listener, RBAC.

9. Schémas de flux réseau

9.1. Flux sortant Internet



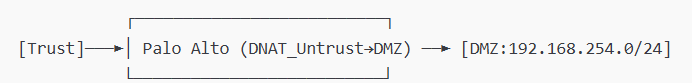
Pare-feu

Description : Tout trafic issu des VLAN internes (Administratif, IoT Médical, Médical) vers Internet est NATé par le pare-feu (203.0.113.10).

Protocols : HTTP(S), SMTP, DNS, NTP, MFT.

Security : Security Policy Trust → Untrust, App-ID + Threat Prevention.

**9.2. Flux interne vers DMZ**

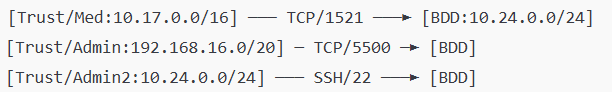


Pare-feu

Accès contrôlé : Les requests HTTP/HTTPS publics adressées à IP 198.51.100.20 sont traduites vers 192.168.254.20 (serveur portail).

Règle : Untrust → DMZ : HTTPS, NAT statique.

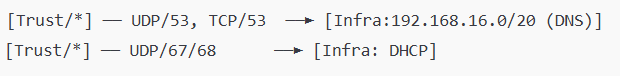
**9.3. Flux applicatifs internes**



Objectif : isoler les bases Oracle dans VLAN BDD, n’autoriser que les ports nécessaires depuis les zones applicatives et d’administration.

Sécurité : Security Policy Trust/Med → BDD (TCP/1521), Trust/Admin → BDD (TCP/5500), Trust/Admin2 → BDD (TCP/22).

**9.4. Flux DNS et DHCP**



Description : Tous les VLAN internes reçoivent IP et DNS du serveur DHCP/DNS situé en VLAN Infra.

Règles : Security Policy Trust → Infra pour DNS et DHCP, SNAT non appliqué (dans zone interne).

**9.5. Flux IoT Médical**



Contexte : Les capteurs médicaux publient leurs données sur un broker MQTT sécurisé en VLAN Infra, puis les dashboards internes récupèrent ces données via HTTPS.

Sécurité : Policies Trust/IoT → Infra, App‑ID pour MQTT, certificat mutuel TLS.

**9.6. Flux de sauvegarde**

[VM Hosts (VLAN BDD/Trust)] ─ replication ─► Rubrik/Veeam (VLAN Infra) ──► Azure Backup

Description : Les appliances de sauvegarde (Rubrik, Veeam) situées en VLAN Infra se connectent en SMB/NFS/HTTPS aux serveurs et VM dans les VLAN Trust et BDD pour effectuer snapshots et transferts vers le cloud HDS.

Ports : SMB 445, NFS 2049, HTTPS 443.

Sécurité : Security Policy Trust → Infra, Content-ID pour l’intégrité.

**9.7. Flux inter-datacenters (PRA)**

[DC1 Rubrik/Veeam] ── IPsec VPN ──► [DC2: replique PRA]

Objectif : Répliquer les sauvegardes et Data Guard redo logs vers le site secondaire via tunnel chiffré.

Protocoles : IPsec (ESP), AES-256-GCM.

Sécurité : Tunnel P1/P2 avec authentification certificat+PSK.

**9.8. Flux d’administration et supervision**



Description : Les consoles d’administration (dans VLAN Admin2) accèdent aux équipements et serveurs via SSH ou RDP, tandis que l’outil de supervision interroge en SNMP les équipements réseau et les serveurs.

Règles : Security Policy Trust/Admin2 → All Zones (ports management) et ACL SNMPv3.

**9.9. Flux de mise à jour OS et patch management**

[WSUS/Ansible (Infra)] ─ TCP/80,443 ─► Patch Targets (Trust, BDD, DMZ)

Contexte : Les serveurs et VM contactent le serveur WSUS/Ansible pour récupérer les correctifs.

Sécurité : Security Policy Trust/Admin2 → Trust, BDD, DMZ pour HTTP/HTTPS.