# Technologie CTX

## 

## Sommaire :

Table des matières

[Technologie CTX 1](#_Toc145796875)

[Sommaire : 2](#_Toc145796876)

[Introduction : 3](#_Toc145796877)

[LAN : 4](#_Toc145796878)

[Pare-Feu : 5](#_Toc145796879)

[Proxy : 6](#_Toc145796880)

[Routeur : 7](#_Toc145796881)

[Serveurs : 8](#_Toc145796882)

[LAN : 8](#_Toc145796883)

[DMZ : 8](#_Toc145796884)

## Introduction :

Ce document décrit les technologies choisies pour la réalisation du réseau de l’Hôpital Sud Paris – Générale des Hôpitaux (HSP-GDH). Cet écrit détaille et explique les choix des différentes technologies sélectionné pour ce réseau.

Le domaine de ce réseau est hsp-gdh.fr.

## LAN :

Cette section concerne les équipements choisis pour assurer le fonctionnement et la connectivité du réseau local. Etant la nature de l’activité de notre établissement, il est nécessaire que ces équipements soient solides et prêt à encaisser des fortes sollicitations de manières plus ou moins régulière et ce sans répercussions tel que pourrait l’être des perturbations ou des ralentissements du réseau.

### Cœur de réseau :

Cet équipement sera l’élément central du réseau, distribuant via VTP les différents VLANs aux switchs d’étage. De plus il assurera aussi le routage du réseau local entre les VLANs, il est donc indispensable que cet équipement puisse assurer parfaitement les communications inter-vlan tout en pouvant gérer une grande quantité de requête.

Pour remplir ce rôle nous avons choisi un switch 3750 Catalyst de chez CISCO. Cet équipement est très largement reconnu pour son efficacité et sa fiabilité. De plus, étant un équipement CISCO, il profite aussi d’une documentation très fournit et d’un support solide particulièrement en ce qui concerne les règles et normes de cybersécurité.

### Commutateur d’étage :

Moins central que le cœur de réseau, mais tout de même important, le commutateur d’étage permet la liaison entre le cœur du réseau et les postes de travail. La quantité de requête est de facto moins important que pour l’équipement précédent, mais nécessite quand même un certain niveau d’efficacité pour éviter que cet équipement soit limitant en ce qui concerne les performances du réseau.

Le CISCO 2960 Catalyst assurera parfaitement à ce poste, il bénéficie des mêmes avantages que l’équipement choisi pour le cœur du réseau, ce qui en fait un choix plus qu’adéquat pour cette situation.

### Point d’accès :

Cet équipement sera chargé d’assurer la connectivité sans-fil du réseau destiné aux visiteurs, aux patients ainsi qu’aux praticiens. Il doit permettre une connexion constante au réseau, avec un débit convenable et pouvant gérer un grand nombre de connexion en simultanés.

Nous avons pour cela choisi un point d’accès CISCO {REF}, permettant notamment d’avoir sur un même équipement différent SSID, ce qui est parfait pour nous étant donné que certaines zones nécessiteront de rendre accessible les trois réseaux sans-fil. Nous permettant ainsi de réduire les coûts sans pour autant perdre en atomicité de réseau.

## Pare-Feu :

Notre infrastructure comportera deux pare-feu un physique Zyxel qui servira de pare-feu externe et un pare-feu logiciel Pfsense qui sera utilisé en tant que pare-feu interne et servira aussi de proxy/reverse-proxy. Pour l’instant seul le pare-feu interne est existant et en fonctionnement.

## Proxy/Reverse-Proxy :

Le proxy et le reverse-proxy sont mis en place sur le pfsense (pare-feu interne). Le proxy utilise le package Squid et le reverse-proxy utilise de son côté HAProxy.

HAProxy redirige les requêtes vers le serveur web.

Squid permet à l’intégralité des vlans internes d’accéder à internet.

## Routeur :

Le routeur fera le lien entre le WAN et le Pare-Feu/Proxy, il est donc un élément indispensable qui permettra la connexion à Internet. Il est donc primordial de choisir un équipement adéquat pouvant répondre à la demande de ce réseau.

Notre choix s’est donc porté sur un routeur physique CISCO RV016, CISCO étant une référence dans la production d’équipement réseau, il est assez naturel de se diriger vers l’un de leurs produits pour assurer une connexion fluide et stable vers Internet. De plus, comme nous maitrisons déjà la configuration des équipements CISCO, la mise en place de cet équipement ne demandera aucune formation supplémentaire.

## Serveurs :

Cette section concerne les serveurs ainsi que les caractéristiques de chacun d’entre eux. L’intégralité des serveurs fonctionneront sur un serveur principal tournant sur ProxmoxVE-8, un OS open source basé sur Debian optimisé pour la virtualisation et conteneurisation, intégrant une interface web permettant de faciliter la gestion des différents conteneurs et machines virtuelles. De plus, il permet aussi de gérer les VLANs et DMZ ce qui simplifier le sectionnement du réseau.

La quasi-totalité des services, à l’exception d’un seul, seront mis en place en un cluster de 3 conteneurs assurant ainsi la redondance ainsi que la répartition de charge. Nous avons essayé de séparer au maximum chaque service entre différent cluster dans le but de préserver au maximum la continuité de service. De telle sorte, que si un cluster tombe hors-service aucun un autre service que celui affecté par la panne ne soit affecté. Cela est bien évidemment bien plus demandant en ressource, mais est une chose nécessaire notamment au vu de la criticité de l’activité de l’établissement. C’est d’ailleurs pour essayer de réduire au strict nécessaire les ressources à allouer que nous avons décidés de structurer nos différents services dans des conteneurs et non dans des machines virtuelles qui sont bien plus consommatrices de ressources.

### LAN :

Cette sous-section portera sur les différents service intégrant le réseau local et n’étant donc pas accessible depuis l’extérieur du réseau.

#### Cluster DHCP :

Ce cluster fonctionnera sous Fedora, avec le package kea. Il sera chargé de la distribution des adresses IP sur les différents segments réseaux. Il permettra aux utilisateurs d’obtenir sur leur poste la configuration réseau nécessaire pour accéder aux services proposés sur le réseau.

#### Cluster DNS :

Ce cluster fonctionnera sous Fedora, avec le package adguard. Il assurera la résolution des noms en adresse IP facilitant ainsi l’accessibilité des services pour les utilisateurs.

#### Cluster LDAP AD DC primaire Kerberos (+ SMB) :

Ce cluster fonctionnera sous Debian, avec le package samba. Son rôle sera d’enregistrer les utilisateurs du domaine et de validé l’identité de chaque utilisateur souhaitant accéder aux différents services. Il permettra aussi le partage de fichier via le protocole SMB.

#### Serveur Windows LDAP AD DC secondaire :

Voici l’exception cité un peu plus tôt, ce serveur sera le seul qui ne sera pas en cluster et en voici les raisons, la première est que ce serveur est une roue de secours, qui sera utilisé si jamais l’intégralité du cluster AD DC primaire venait à tomber hors-service, ceci étant assez peu probable, il n’est donc pas nécessaire d’avoir un deuxième cluster. De plus, ce serveur tournera sur un environnement Windows qui est bien plus nécessiteux en ressource. Il est donc préférable de limiter sous instanciation à une seule et unique machine virtuelle qui sera utilisé exclusivement en cas de force majeur.

#### Cluster FTP :

Ce cluster fonctionnera sous Fedora, avec le package %. Il permettra aux utilisateurs de transférer des fichiers ainsi que d’en héberger sur le réseau de manière à les rendre accessible à tous depuis n’importe quel endroit du site.

#### Cluster iPXE :

Ce service ne fera pas l’objet d’un cluster mais sera mis en place sur le cluster DHCP, car pour fonctionner celui-ci nécessite d’être placé au même endroit que le serveur DHCP. Il fonctionne en tant que sous-service du cluster DHCP qui enverra donc un firmware de boot initramfs/PE au client PXE.

#### Cluster MariaDB :

Ce cluster fonctionnera sous Fedora, avec le package mariadb. Ce cluster permettra d’enregistrer toutes les données traitées par le cluster web et ce de manière de structuré.

#### Cluster API :

Ce cluster fonctionnera sous Fedora, avec le package caddy. Il servira d’interface entre le cluster MariaDB et le cluster web assurant ainsi la sécurité de la base de données en ne permettant pas un accès direct du cluster web sur ce dernier. Tout en rendant l’infrastructure web plus solide en divisant la charge des requêtes entre deux clusters. Il se chargera de la partie backend du site internet.

#### Cluster Supervision :

Ce cluster fonctionnera sous Fedora, avec le serveur Centreon. Il sera chargé de surveiller les constantes du réseau, nous permettant ainsi d’augmenter notre réactivité en cas de panne sur celui-ci.

#### Cluster Ticketing :

Ce cluster fonctionnera sous Fedora, avec le package GLPI. Ce cluster a pour but de simplifier la gestion des pannes utilisateurs en leur offrant une interface web permettant de centraliser toutes leurs demandes de résolutions d’incident ainsi que le suivi de ces dernières.

#### Cluster VPN :

Ce cluster fonctionnera sous Fedora, avec les packages openvpn et wireguard. Il offrira à nos utilisateurs internes à l’hôpital la possibilité de se connecter au réseau local depuis leur domicile. L’utilisation de ces 2 packages permettra d’assurer une meilleure redondance, garantissant une connexion optimale pour tous nos utilisateurs.

#### Cluster Miroir :

Ce cluster fonctionnera sous Fedora, avec le package %. Il servira de miroir distribuant les mis à jour aux différents serveurs et machines du réseau local.

### DMZ :

Cette sous-section abordera les services intégrant la DMZ, c’est-à-dire la section du réseau accessible depuis l’extérieur de celui-ci. Cette zone est bien évidemment bien plus à risque que le reste du réseau. C’est pour cette raison qu’il n’y a que le strict nécessaire des services qui se trouve dans cette zone.

#### Cluster Web :

Ce cluster fonctionnera sous Fedora, avec le package caddy. Il sera chargé de retourner les pages internet demandés par les utilisateurs que ce soit interne ou externe au réseau de l’hôpital. Le cluster API se chargeant déjà la partie backend, ce cluster se contentera de la gestion du frontend. Limitant ainsi les risques et conséquences d’une attaque sur ce serveur.

#### Serveur IMAP/SMTP :

Ce serveur fonctionne sous Alma Linux, et se base sur la suite de package de mail Zimbra, intégrant ainsi les différents services collaboratifs.