

	DOCUMENT INFORMATIF	Diffusion par : PILNH - DSN	0085-DI-219
	Annexe technique - infrastructures réseaux	Page 1 / 5	V. 01

Processus : INF-CHU-Gestion des Services Numériques

1. OBJECTIF DU DOCUMENT

Ce document décrit le réseau informatique, en particulier les standards retenus et appliqués ainsi que l'infrastructure dans laquelle seront intégrées les solutions métiers acquises par le CHU de Nantes.

Cette annexe doit permettre aux candidats de répondre aux différentes consultations émises par le CHU de Nantes en proposant une solution technique adaptée et optimisée à l'environnement cible.

Les candidats devront se conformer aux infrastructures et standards techniques mis en place ainsi que [les « bonnes pratiques » recommandées par l'ANSSI](#).

Le respect de cette annexe technique ne présuppose pas de l'implémentation qui devra être validée par les équipes des services numériques.

2. DOCUMENTS DE REFERENCE

Sans objet

3. RESEAUX LOCAUX

3.1 LAN Datacenter

3.1.1 Présentation générale

Le Datacenter du CHU de Nantes est organisé autour de deux salles informatiques, situées, l'une sur le site de Saint-Jacques et l'autre sur celui de l'Hôpital Nord. L'ensemble de ces deux salles physiques assure une redondance géographique des serveurs en constituant une unique salle virtuelle.

Les liaisons réseaux entre les deux sites utilisent un multiplexage DWDM reposant sur deux liens physiques empruntant des chemins distincts, et sur lesquels transitent plusieurs liaisons virtuelles de 1 et 10 Gbits/s.

Au sein du Datacenter des solutions de micro-segmentation sont mises en œuvre pour le filtrage des flux nord/sud (entre les serveurs et leurs clients) et est/ouest (entre serveurs).

3.1.2 Caractéristiques et contraintes

- Les équipements du réseau offrent des ports physiques de 1 ou 10 Gbits/s cuivre ou fibre. Il est possible de les agréger pour augmenter le débit et/ou fiabiliser la connexion.
- La latence entre les deux salles Datacenter est inférieure à 5 ms.
- Il est de la responsabilité des éditeurs et intégrateurs de fournir la matrice exhaustive des flux (entre serveurs et entre serveurs et clients) nécessaires au bon fonctionnement de la solution.
- Afin d'assurer la pérennité des infrastructures, les équipements, virtuels ou physiques, intégrés au Datacenter du CHU de Nantes doivent supporter les protocoles IPv4 et IPv6.

3.2 LAN Campus 'utilisateurs'

3.2.1 Présentation générale

Le CHU de Nantes est composé de 4 campus 'utilisateurs' :

- L'Hôtel-Dieu.
- L'Hôpital Nord, Guillaume et René Laënnec.
- L'Hôpital Saint-Jacques.
- Le bâtiment Turner.

Une couverture sans-fil, suivant au minimum la norme Wi-Fi 802.11a, est assurée sur 80% des bâtiments. L'ensemble des bornes Wi-Fi est géré par des couples de contrôleurs à haute disponibilité fonctionnant selon un mode actif/passif. La solution sans-fil est administrée à l'aide d'un outil centralisé propriétaire. Plusieurs SSID, dépendant de l'authentification requise, sont diffusés sur l'établissement. Il est de la responsabilité du CHU de Nantes de décider de la diffusion d'un nouvel SSID.

REDACTEUR(S)	VERIFICATEUR(S)	APPROBATEUR(S)	Date d'application
Eric MALEVIALLE (Responsable - PILNH \Services Numériques\Infrastructures)	Pierrick MARTIN (Coordonnateur qualité - PILNH \Services Numériques)	<Ne pas modifier>	30/05/2023

3.2.2 Caractéristiques contraintes

- La connectivité au poste est fournie sous la forme de prises cuivres RJ45 offrant des débits de 100 Mbits/s ou 1 Gbits/s selon le commutateur de rattachement. *Optionnellement, après validation par la DSNT, une alimentation électrique au format PoE peut-être délivrée.*
- L'allocation des adresses IP et autres paramètres réseaux (Masque de sous-réseau, passerelle par défaut, serveurs de nom, serveurs de temps...) est faite par un serveur DHCP du CHU de Nantes. *Optionnellement il est possible d'avoir une adresse IP fixe par réservation dans les serveurs DHCP de l'adresse IP associée à une adresse MAC donnée. Il est de la responsabilité des éditeurs et intégrateurs de fournir la liste d'association Adresse MAC/Adresse IP à partir d'une plage d'adresse IP fournie par le CHU de Nantes.*
- Les équipements raccordés sur l'infrastructure du CHU de Nantes doivent supporter l'authentification selon le protocole 802.1x.
- Les équipements nécessitant un traitement différencié de leur trafic selon la qualité de service requise doivent procéder à un marquage des paquets au niveau 3 (Renseignement du champ DSCP de l'en-tête IP). *Optionnellement, après validation par la DSNT, un marquage des trames au niveau 2 (Renseignement du champ dot1p de l'en-tête Ethernet) pourra être utilisé.*
- En aucun cas les équipements raccordés au LAN du CHU de Nantes devront prendre part aux protocoles réseaux utilisés par l'infrastructure (RSTP, OSPF, BGP...).
- Les équipements (filaire et sans-fil) non conformes à la politique de sécurité du CHU de Nantes seront classés 'untrusted', les communications avec le reste de l'infrastructure seront filtrées par un pare-feu. Il est de la responsabilité des éditeurs et intégrateurs de fournir la matrice de flux nécessaire au bon fonctionnement de la solution.
- Pour des raisons d'architecture interne, il est possible qu'un système intègre un sous-réseau IP privé dédié à la communication entre sous-systèmes de la solution. Cependant, en aucun cas, ces sous-réseaux ne devront être visibles depuis les LAN des campus du CHU de Nantes, y compris pour des raisons de télémaintenance.

4. RESEAUX ETENDUS (WAN)

Pour l'accès haut débit à Internet et les échanges privés avec ses sites périphériques ou d'autres établissements de santé, le CHU de Nantes utilise les services de l'opérateur Gigalis.

4.1 Accès externes

Le CHU de Nantes dispose de deux plages d'adresses IPv4 publiques et d'une plage d'adresses IPv6. L'ensemble du trafic entrant et sortant est filtré par un pare-feu externe, de plus les flux HTTP(S) sont inspectés. Le pare-feu externe assure également la translation des adresses IPv4 pour communiquer avec des équipements dans les sous-réseaux privés du CHU de Nantes.

4.2 Réseaux privés virtuels

En plus de l'accès Internet, le CHU de Nantes dispose de réseaux privés virtuels dédiés à la communication entre utilisateurs au sein d'un groupe restreint :

- RPV Santé : Ce réseau, utilisant un plan d'adressage privé, non routable sur Internet, est réservé aux établissements de santé de Bretagne et Pays de la Loire.
- RPV GHT-44 : Ce réseau, utilisant un plan d'adressage privé, non routable sur Internet, est réservé aux seuls établissements du GHT de Loire-Atlantique. Il permet l'accès aux infrastructures mutualisées ainsi qu'aux applications dédiées, hébergées en mode IaaS, sur l'infrastructure du CHU de Nantes.
- RPV CHU : Ce réseau, utilisant un plan d'adressage privé, non routable sur Internet, est réservé aux sites périphériques du CHU de Nantes.

5. TELEPHONIE

Le CHU de Nantes utilise des infrastructures de téléphonie RTC et ToIP. Toute solution devant s'interfacer avec la téléphonie devra utiliser l'infrastructure ToIP.

La couverture réseaux mobiles n'est pas garantie sur l'ensemble des sites du CHU de Nantes, en particulier dans les locaux techniques.

6. CONNEXION D'UN EQUIPEMENT AU RESEAU CHU (FOURNITURE PAR SOCIETE EXTERNE)

6.1 Politique de sécurité

Un matériel est considéré comme "extérieur" dès lors qu'il ne dispose pas du socle et des composants validés et supportés par la DSN du CHU (ex pour un PC, le "Master CHU" windows10). Il n'est pas référencé dans l'ITSM, pas présent dans l'[Active Directory](#) et ne dispose pas de l'agent MECM\SCCM.

Dans le cas d'une nécessité de connexion d'un équipement extérieur au réseau interne du CHU, une justification doit être formalisée et approuvée par le RSSI. Les SN du CHU de Nantes se réservent la possibilité de proposer que l'acquisition projetée soit prise en charge dans le cadre d'un de ses marchés. Une demande ne pourra être approuvée sans respect des contraintes suivantes (source PSI SMSI SOA Doc PTS) :

A13 - Sécurité des communications

Gestion de la sécurité des réseaux

Les réseaux sont cloisonnés.

Les équipements informatiques (PC, MFP, équipements biomédicaux) sont déployés dans la version OS et patch officielle de la DSN, disposent d'un MASTER DSN avec le pack des outils (SCCM, intégration AD, AV à jour, PDM, GAIA, etc.) et sont intégrés au domaine AD et gérés de façon industrielle avec le reste du parc.

Les équipements qui ne peuvent pas respecter cette configuration sont isolés sur des VLAN filtrés derrière un pare-feu interne, il appartient au demandeur de fournir la liste des flux et des IP.

Toute exception à cette règle et toute modification du MASTER doit être explicitement validée par le RSSI.

Le VLAN des adminsys est isolé.

6.2 Types de réseaux disponible

Deux types de réseaux sont disponibles pour connecter un équipement au réseau CHU :

Réseau Bureautique (Zone de confiance, réseau "TRUSTED")	Réseau Isolé (Zone non fiable, réseau "UNTRUSTED")
<p>Types d'accès :</p> <ul style="list-style-type: none"> • Accès aux ressources internes (intranet) sans restriction • Accès aux ressources externes (internet) selon PSSI • Connexion Ethernet\Filaire (intra.chu-nantes.fr) ou wlan\Sans-fil (Wi-Fi avec authentification 802.1x par certificats au CHUN-MEDICAL) • Accès possible au réseau UNTRUSTED <p>Contraintes :</p> <ul style="list-style-type: none"> • Si Windows, réinstallation obligatoire du poste avec le master CHU Windows 10 • Si matériel Android, installation obligatoire de l'agent <u>WorkspaceOne</u> • Présence des mises à jour de sécurité système Microsoft (KB) et composants tiers (Framework, navigateurs, utilitaires...) à M+1 max • Présence d'un antivirus à jour 	<p>Types d'accès :</p> <ul style="list-style-type: none"> • Accès aux ressources internes (intranet) sur liste uniquement • Accès aux ressources externes (internet) sur liste uniquement <p>Contraintes :</p> <ul style="list-style-type: none"> • Système d'exploitation géré par l'intégrateur (acquisition, installation, configuration, maintenance) • Tous les flux réseaux sont fermés sauf ceux explicitement listés dans la matrice de flux • Aucun outil\logiciel\application CHU n'est présent sur le poste • La DSN ne propose pas de support en dehors des accords négociés lors de la connexion de l'équipement • <u>Pas de connexion Wifi</u> <p>Exigences pour l'intégrateur :</p> <ul style="list-style-type: none"> • Fourniture de la matrice de flux réseau (port\protocole\source\destination) • Obligation de mise à jour régulière du système et des applications • Formalisation de la méthode de prise de main • Obligation de présence d'un antivirus avec mise à jour régulière

7. GLOSSAIRE

CCTP	Cahier des Clauses Techniques Particulières – Document décrivant les différentes clauses techniques devant être remplies dans le cadre d'une réponse à appel d'offre.
DWDM	Dense Wavelength Division Multiplexing – Technologie de multiplexage par longueur d'onde permettant sur un même media physique d'exploiter plusieurs canaux de communications reposants sur des longueurs d'ondes différentes.
GHT	Groupeement Hospitalier de Territoire – Regroupement des établissements publics de santé d'une même zone géographique.

PoE	Power over Ethernet – Technologie utilisant le câble cuivre Ethernet pour l'alimentation électrique de petits équipements (Jusqu'à 13W sous 48V) et définie par la norme IEEE 802.3af.
RSTP	Rapid Spanning Tree Protocol – Evolution du protocole STP de gestion des boucles réseaux de niveau 2, défini par la norme IEEE 802.1w et permettant une amélioration du temps de convergence.
RTC	Réseau Téléphonique Commuté – Technologie utilisée pour la téléphonie analogique et numérique (Type Numéris).
STP	Spanning Tree Protocol – Protocole de gestion des boucles réseaux de niveau défini par la norme IEEE 802.1D.
ToIP	Telephony over IP – Technologie téléphonique reposant sur le réseau IP.