

ANNEXE CONNEXION AU RESEAU DU CHU DE TOULOUSE

Ce document est à joindre impérativement paraphé et tamponné avec l'offre du postulant

La présente charte a pour objet, de définir les règles de connexion des équipements fournis et installés hors des procédures de la DSN (Direction des Systèmes d'Information et Organisation) sur le réseau Ethernet, et/ou WiFi, et des ressources gérées par la DSN. La structure CHU émettrice de la demande de connexion est la garante de l'application de cette charte de sécurité par son fournisseur.

A) Domaine d'application

Les règles et obligations énoncées ci-dessous s'appliquent à tout utilisateur des ressources informatiques des Hôpitaux de Toulouse. Ces ressources comprennent :

- le câblage interne (câbles et prises)
- les réseaux Ethernet (ou réseau IP)
- les réseaux WiFi
- les stations de travail et micro-ordinateurs et leurs périphériques
- les serveurs

B) Connexion au réseau du CHU de Toulouse

1 - Identification au CHU

L'équipement à raccorder est identifié. Son identification comprend :

- Pour le CHU
 - la structure CHU à l'origine de la demande
 - le contact CHU responsable du fournisseur
 - le contact CHU en charge de la demande
 - le contact CHU utilisateur de l'équipement
- Pour le fournisseur
 - le fournisseur de l'équipement
 - le contact « Fournisseur », responsable du projet
 - le contact « Fournisseur », responsable technique en charge de la demande de connexion et de sa réalisation
- l'emplacement physique dans les locaux du CHU (ex : N° de pièce ou de local)
- le contact « chargé d'affaire » à la DSN

La collecte des informations nécessaires au raccordement de l'équipement est à la charge des responsables projet du CHU et du fournisseur.

2 - Raccordement physique au réseau filaire contrôlé

2.1 - Authentification sur le réseau

L'accès au réseau filaire de l'Hôpital est soumis à l'authentification de l'équipement par notre serveur Radius (service NAC - Network Access Control).

La mise en service de l'équipement du fournisseur ne peut, en aucun cas, remettre en cause la politique de sécurité du CHU et notamment des mesures d'authentification mises en place sur son réseau informatique.

Pour pouvoir être authentifié, le terminal doit impérativement :

1. Être compatible avec le standard 802.1x

Ou

2. Présenter son adresse MAC à l'infrastructure LAN.

L'équipement du fournisseur doit impérativement être capable de présenter son adresse MAC dès la mise sous tension et à la connexion du port Ethernet sur le commutateur du CHU. Pour cela le terminal du fournisseur ne doit pas être « muet », il de lui-même émettre régulièrement du trafic (requêtes TCP, UDP ou ICMP) sans attendre d'être sollicité.

Exemples : requêtes NETBIOS, DHCP, BOOTP, FTP, TFTP, PING...

Pour rappel :

- Les équipements qui ne sont pas compatibles avec le standard 802.1x ou qui ne présentent pas leur adresse MAC ne seront jamais authentifiés et resteront isolés du réseau.
- Le fournisseur de solutions qui ne respectent pas ce prérequis sera seul responsable des retards du projet et des conséquences associées

Les trois méthodes d'authentification supportées par notre serveur Radius sont les suivantes :

1. **Authentification du terminal en EAP-TLS (certificat machine embarqué) :**

Certificat géré est fourni par le « fournisseur » :

- le fournisseur de la solution informatique remettra, à l'équipe d'administration Réseau du CHU, une copie du certificat public de l'autorité racine utilisé
- le fournisseur de la solution informatique prendra en charge le cycle de vie des certificats, le renouvellement du certificat de l'équipement et fournira une copie du certificat public de l'autorité racine lorsque celui-ci est mise à jour

2. **L'authentification de l'utilisateur ou du terminal en EAP-PEAP, également identifié sous le protocole MS-CHAPv2) (Login/Mot de Passe) :**

Le service informatique du CHU fournira les identifiants d'authentification

Authentification de l'adresse MAC :

- a. Le fournisseur de la solution informatique remettra, à l'équipe d'administration Réseau du CHU, l'adresse MAC du terminal

Le raccordement physique est réalisé :

- Sur le câblage mural (Cat 6) défini par le CHU et avec une connectique normalisée de type RJ/45
- Aucun ajout, d'équipement supplémentaire de type doubleurs de prise ou « mini-hub / mini-switch » n'est autorisé. Un seul équipement autorisé par prise RJ/45 murale !

La carte Ethernet de l'équipement à connecter est configurée en mode « auto-négociation ».

Pour les actions de télémaintenance et/ou de communication de l'équipement avec le monde extérieur, se reporter aux paragraphes :

- Communication « CHU vers extérieur »
- Communication « Extérieur vers CHU »

Aucun périphérique de type modem (réseau téléphonique commuté, Numéris, XDSL, GSM, etc...) ne doit être présent et utilisé sur l'équipement connecté.

Le poste informatique doté de 2 cartes Ethernet à vocation d'établir un pont entre le réseau institutionnel du CHU Toulouse et un réseau privé est strictement interdit.

3 - Connexion au réseau sans fil

Les seuls réseaux WiFi supportés et acceptés par les établissements du CHU est exclusivement celui fourni et administré par les équipes réseau de la DSN.

Le fournisseur et son référent DSN doivent, en amont de tout projet de mobilité, interpellier les services du CHU afin de s'assurer que la couverture WiFi est en adéquation avec le périmètre géographique du projet.

Le fournisseur prend connaissance des caractéristiques et prérequis décrits ci-dessous avant de proposer une solution technique reposant sur le réseau sans-fil.

Le client WiFi de la carte embarqué dans l'équipement fournis doit respecter les prérequis suivants :

- il doit être compatible les normes IEEE 802.11ac/n/a/g. La norme 802.11b n'est pas acceptée sur le réseau sans-fil du CHU
- la bande de fréquence des 5GHz, moins soumise aux perturbations, est privilégiée
- il doit supporter la méthode de cryptage WPA2 AES ainsi que l'authentification par certificat EAP-TLS (certificat délivré par le CHU), ou EAP-PEAP-MSCHapV2 si la première méthode n'est pas supportée et justifiée
- les certificats délivrés par le CHU sont au format X509V3 et l'intégration de ces certificats se font au format PKCS12

Les applications transportées sur le réseau sans-fil du CHU doivent respecter les prérequis suivants :

- elles sont obligatoirement routées et utilisent exclusivement le protocole IP. Les équipements filaires et sans-fils sont sur des plans d'adressage totalement distincts.
- le terminal WiFi, tout comme pour le terminal filaire (se reporter au paragraphes « Identification sur le réseau »), supporte et s'appuie sur les services des serveurs DHCP et DNS. L'adressage IP fixe est interdit sur le réseau sans-fil.
- les protocoles de routage multicast ne sont pas supportés sur le réseau sans-fil du CHU

4 - Identification sur le réseau

L'équipement raccordé est nommé. Son identification comprend :

- une adresse MAC à communiquer à l'équipe d'administration Réseau du CHU
- un nom (hostname) défini en relation avec l'équipe d'administration Réseau du CHU
- des paramètres IP aux standards du CHU. Ces paramètres comprennent :
 - une adresse IP conforme au plan d'adressage du CHU.
 - Cette adresse est exclusivement dynamique et fournie par le serveur DHCP du CHU de Toulouse.
 - Si le terminal, pour des besoins d'exploitation, a besoin d'être identifié par son adresse IP, cette adresse IP peut lui être réservée sur le serveur DHCP.
 - Si le terminal nécessite l'usage d'une adresse IP statique, le fournisseur devra expressément **le justifier et le motiver** auprès des équipes de la DSN
 - les autres paramètres IP (masque, passerelle, nom de domaine et serveur(s) DNS et NTP) seront automatiquement attribués par le serveur DHCP, ou par les équipes de la DSN dans les cas d'adressage statique

5 - Services Réseau

La connexion au réseau du CHU est subordonnée aux principes suivants :

- seul le protocole IP est autorisé sur le réseau de transport du CHU
Les autres protocoles Réseau pouvant entrer en conflit avec le réseau existant du CHU (IPX, AppleTalk, ...) sont désactivés sur les drivers des cartes Ethernet
- les services et protocoles Réseau nécessaires au bon fonctionnement de l'équipement sont décrits (IGMP, Multicast, ...).
Le routage Multicast est possible sur le réseau filaire du CHU, par contre il est totalement **interdit** sur le réseau WiFi.
Toute solution s'appuyant sur des flux Multicast doit faire l'objet d'une validation des équipes réseau du CHU

- les applications non routées ne sont pas autorisées
Les modes de communication par diffusion sont **interdits**, les broadcast Ethernet sont interdits sur le réseau.
Tout taux de broadcast anormal entraîne automatiquement la mise hors service du port Ethernet via un mécanisme d'autodéfense de l'infrastructure réseau
- Aucun réseau Ethernet (même domaine de Broadcast) ne sera autorisé à être étendu au-delà du premier point de routage
- les services Réseau standard du CHU sont utilisés à l'exclusion de toute autre source.
Ceci concerne par exemple les services comme NTP, DNS, DHCP-Server, relais SMTP, PKI...

6 - Configuration logicielle

L'équipement raccordé est livré avec :

- un OS à jour et une procédure de suivi des correctifs de sécurité
- un logiciel ou dispositif Antivirus à jour et actif et une procédure de suivi des mises à jour

7 - Communication « CHU vers extérieur »

Si l'équipement doit communiquer avec des ressources extérieures, la solution de communication est fournie par le CHU, et le fournisseur adresse à la DSN :

- la liste des noms, adresses IP et descriptions des équipements internes au CHU de Toulouse
- la liste des noms, adresses IP et descriptions des serveurs externes au Système d'Information du CHU de Toulouse, ainsi que la liste leurs ports de communication (TCP ou UDP)
- la description des moyens de sécurisation/cryptage des communications avec ces serveurs

L'équipe d'administration Réseau du CHU, définit avec le fournisseur les moyens et les modes de communication pouvant être utilisé.

Ceux-ci peuvent être l'usage d'un tunnel VPN IPSec, de l'EAI (Enterprise Application Integration également appelé Echanges Inter-applicatifs de Données en français) ou d'un flux au travers de nos firewall (se reporter au paragraphes « Matrice de flux »).

Précision : Au travers d'une connexion site à site de type VPN IPSEC, les accès de type SSH/SSL ou tout autre moyen (SSL par exemple) de connexion permettant une prise de main à distance et/ou une élévation de privilège seront contrôlés via notre PAM. L'accès direct aux ressources du SI CHU Toulouse sont interdites.

8 - Communication « extérieur vers CHU » de type télé-administration / télémaintenance

Si de la télé administration et/ou télémaintenance doivent être exécutées sur l'équipement, la solution de communication est fournie par le CHU, et le fournisseur adresse à la DSN :

- le contact « Fournisseur », responsable du projet
- le contact technique « Fournisseur » administration Réseau et sécurité du fournisseur

L'équipe d'administration Réseau du CHU, définit avec le fournisseur les moyens et les modes de communication à utiliser.

Les moyens de télé administration et/ou télémaintenance s'appuient sur des services « Accès Réseau à distance » disponibles et fournies par le CHU. Toute autre solution est exclue.

Le passage par un service de type PAM (Privilege Access Management) est une obligation.

L'accès au PAM est fourni via une connexion nomade VPN (client de connexion à installer sur le ou les postes distants). L'authentification de type login/mot de passe est spécifique à cette modalité de connexion.

9 – Communication « extérieur vers CHU » de type Reverse Proxy transparent

La nature des flux est de type exclusivement SSL (au-delà de TLS1.2)

Ces flux entrants sont interceptés pour permettre l'analyse virale systématique des données encapsulées.

Le Reverse Proxy porte l'implémentation du certificat SSL public.

10 – Communication « extérieur vers CHU » de type Portail SSL

La nature des flux est de type exclusivement SSL (au-delà de TLS1.2)

Ce type de connexion permet l'accès à des applications en mode Web hébergées sur le SI du CHU Toulouse.

L'authentification se base sur un couple login/mot de passe couplé à de l'OTP SMS.

Tout utilisateur de ce service doit au préalable fournir au CHU Toulouse un numéro de portable via lequel il recevra le token SMS. A défaut d'avoir ou vouloir fournir un numéro de téléphone portable, l'utilisateur pourra se doter à sa charge d'une solution de numéro GSM virtuel qui permet l'accès à ce service.

Le Reverse Proxy porte l'implémentation du certificat SSL public.

11 - Matrice de flux

Le Système d'Information du CHU de Toulouse est découpé en domaines de confiance protégés par des firewalls.

Toute communication entre domaines de confiance, qu'il soit interne entre solutions techniques au CHU ou externe (se reporter au paragraphes Communication « CHU vers extérieur ») doit être identifiée et présentée aux équipes sécurité de la DSN afin qu'ils puissent l'implémenter dans les règles de filtrage des firewalls.

Voici ci-dessous un exemple de matrice de flux CHU à compléter :



Matrice de flux

Date :
Nom et description du projet :
Responsable du projet :
Numéro de la demande C4U :

[illegible]

Contact cellule Sécurité CHU Toulouse : dsio-supportsecu@chu-toulouse.fr

L'ensemble des champs de la matrice de flux devront être complétés, et le fournisseur devra identifier chacun d'eux selon l'application (Niveau 7 du modèle OSI) ou du port TCP ou UDP (Niveau 4 du modèle OSI).

C) Droits et Devoirs

1 - Des fournisseurs

Le fournisseur a obligation de :

- signer la présente charte
- la faire appliquer par ses équipes
- signaler aux responsables du CHU toute violation, tentative de violation ou toute violation suspectée d'un système informatique et, de façon générale, toute anomalie constatée (mauvaise gestion des protections, faille système, logiciel suspect...) pouvant nuire au bon niveau de sécurité du système.

2 - Des structures CHU responsable du projet

Les structures CHU responsables du projet ont obligation de :

- être le correspondant entre ses fournisseurs et la DSN
- faire signer la présente charte à ses fournisseurs
- contrôler son application
- Signaler aux administrateurs du CHU (DSN) toute violation, tentative de violation ou toute violation suspectée d'un système informatique et, de façon générale, toute anomalie constatée (mauvaise gestion des protections, faille système, logiciel suspect...) pouvant nuire au bon niveau de sécurité du système.

3 - De la DSN

Les équipes de la DSN ont obligation de :

- assurer un bon fonctionnement des réseaux et des services Réseau.
- assister les structures CHU responsables du projet et le fournisseur pour la mise en service de l'équipement.

Cette assistance s'applique, par exemple aux domaines suivants :

- configuration de l'équipement : partage de ressources, installation imprimante, déclaration de compte « utilisateur », etc.
- sécurisation de l'équipement : suppression de logiciels installés, comme Internet Explorer, verrouillage de la configuration de l'équipement, et c...
- Installation des moyens de communication avec le monde extérieur (mise à jour logiciel antivirus, télémaintenance, et c ...)

La DSN assure une assistance, mais ne se substitue en aucun cas au fournisseur pour les interventions sur l'équipement.

- prendre toutes dispositions nécessaires pour assumer cette responsabilité tout en respectant la déontologie professionnelle.

En particulier, les équipes de la DSN peuvent être amenées, après concertation avec toutes les parties prenantes, de prendre toute mesure conservatoire jugée nécessaire. Dans ce cadre, les équipes de la DSN peuvent intervenir pour déconnecter physiquement et/ou logiquement des équipements ne respectant pas cette charte.

Cachet de la société, nom et signature
de la personne habilitée à engager la société :