Politique générale de raccordement d'un laboratoire de recherche au Réseau de l'Université Paris-Saclay

Préambule

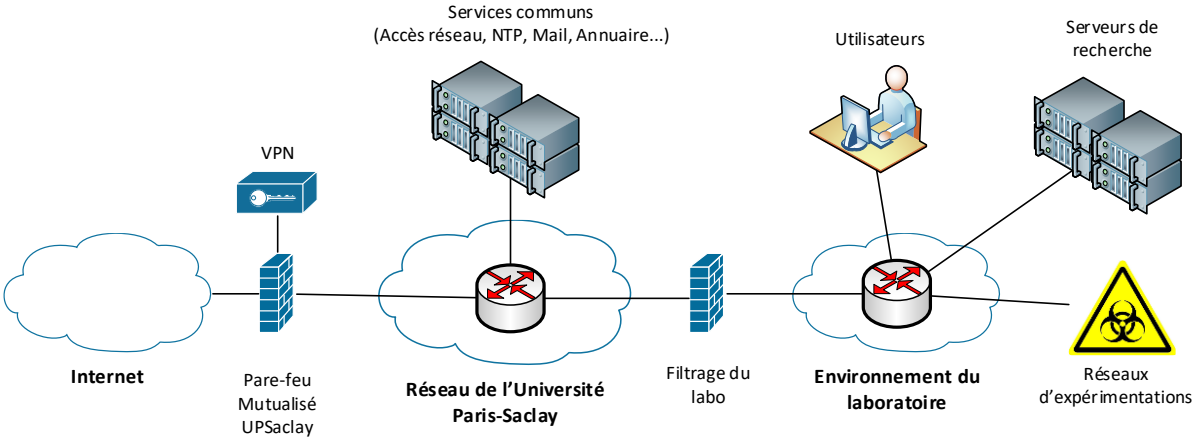
L'Université assure à travers son réseau la connexion des laboratoires de recherche aux services de l'Université, aux autres entités et partenaires, ainsi que la connexion à Internet.

L'Université est de fait responsable des communications entrantes et sortantes des laboratoires qu'elle raccorde et doit en assurer le contrôle. Les laboratoires doivent donc se conformer aux PSSI (Politique de Sécurité des Systèmes d'Information) de l'Université et de leurs tutelles.

L'architecture générale présentée dans ce document est un pré-requis minimal qui peut être amendé dans l'objectif d'augmenter encore le niveau de sécurité requis par le contexte spécifique d'un laboratoire (ex : ZRR, besoins de raccordements spécifiques vers des tutelles, ...)

Segmentation du laboratoire

Afin d'assurer un niveau minimal de sécurité du laboratoire, celui-ci est virtuellement isolé au sein du réseau de l'Université dans un environnement dédié et raccordé au reste de l'Université à travers un système de filtrage (pare-feu).



Le laboratoire est lui-même segmenté en zones de sécurité différentes, avec du filtrage possible entre ces zones (utilisateurs, serveurs de recherche, expérimentations, visiteurs, imprimantes, etc…).

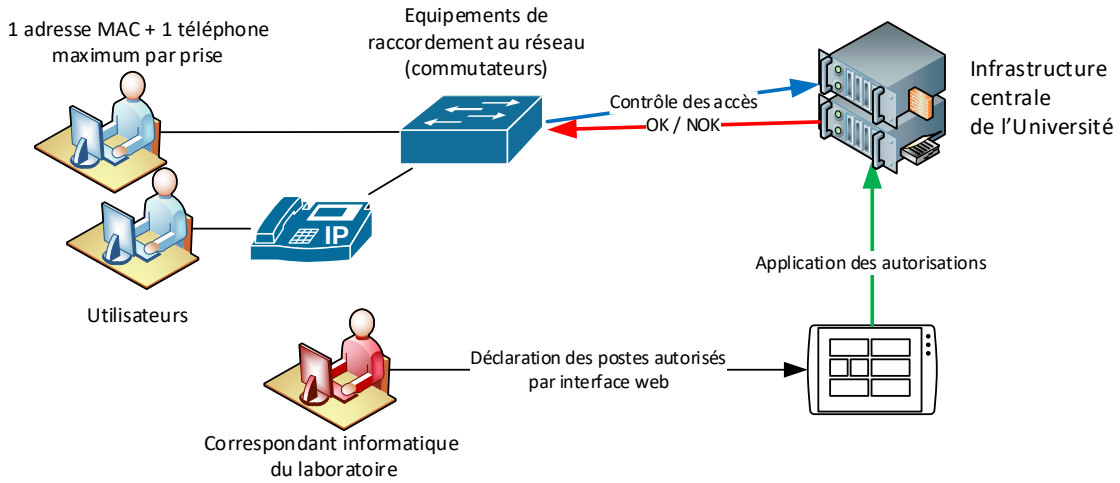
Nom des objets

Les objets sur le réseau sont déclarés sur l'université et éventuellement sur Internet sous la forme « nom.labo.universite-paris-saclay.fr »

Contrôle de l'accès réseau et sécurité

Les équipements assurant le raccordement des ordinateurs au réseau (commutateurs) sur lesquels aboutissent notamment les prises murales sont gérés par la DSI. Elle en assure la configuration, l'exploitation et la maintenance.

Les équipements sont paramétrés pour vérifier que les accès au réseau sont conformes à ceux déclarés par le correspondant informatique du laboratoire. Cette déclaration (nom complet de l'objet, adresse MAC et adresse IP) permet d'une part d'autoriser l'objet à accéder au réseau dans la zone de sécurité où il y a été déclaré, mais également d'enregistrer son nom sur l'université et éventuellement sur Internet.



Une prise réseau ne doit servir qu'à raccorder un seul objet, plus éventuellement un téléphone IP.

Au même titre que le réseau filaire, le réseau wifi est géré et exploité par la DSI avec la diffusion des réseaux Eduroam et Eduspot. Suivant la localisation et les besoins, des réseaux supplémentaires (IOT, visiteurs, colloques….) peuvent être déployés.

Services communs assurés par la DSI

Outre le respect des points précédemment évoqués et afin de garantir la sécurité, la conformité des accès, l'homogénéité et la cohérence de toute l'infrastructure en place, le laboratoire se repose obligatoirement sur les services communs suivants fournis par la DSI :

- les services réseaux (DNS/DHCP/NTP). Le correspondant informatique du laboratoire dispose des accès aux outils de délégation (IPAM) pour déclarer les objets du réseau. Leur utilisation est donc totalement transparente et automatique pour les utilisateurs.
- les serveurs de messagerie (SMTP). Dans le cadre de la lutte anti-spam, tous les mails doivent transiter par les serveurs de messagerie entrants et sortants de l'université.
- l'infrastructure VPN pour accéder au réseau du laboratoire depuis l'extérieur de l'Université.
- Les services d'annuaire pour les autorisations d'accès aux outils et la gestion de la téléphonie.

D'autres services peuvent être utilisés (hébergement web, AD, VM, hébergement sec, stockage, déploiement de parc…) peuvent être contractés.

Assistance et disponibilité des services

Toutes les demandes qui ne peuvent être traitées par les correspondants informatiques locaux sont effectuées sur la plate-forme d'assistance de la DSI. L'objectif de disponibilité des services réseau est de 99,999%. Le traitement des incidents est réalisé en best-effort.

Bonnes pratiques sur la segmentation interne des laboratoires

Il est recommandé de séparer dans des zones de sécurité différentes au minimum les utilisateurs et les serveurs du laboratoire, et si possible :

Zone de sécurité	**Adressage**	**Accès Internet**
Personnels connectés au réseau filaire	Recommandé : privé	Transparent via NAT
Les visiteurs connectés au réseau filaire	Privé	NAT ou Proxy
Les imprimantes et copieurs	Privé	Proxy web
Les serveurs internes	Privé	NAT ou Proxy
Les serveurs publics/DMZ	Public	Direct
Les réseaux d'expérimentations / manipulations	Privé	NAT ou Proxy
Les postes/stations obsolètes	Privé	Proxy

Il est possible de créer d'autres réseaux si l'activité ou les besoins du laboratoire le justifie.

Les personnels nomades connectés en wifi peuvent se connecter aux ressources du laboratoire via le VPN.

L'objectif est de bien séparer le réseau de production du réseau de recherche et d'expérimentation, et également de limiter la visibilité des ressources du laboratoire au maximum du réseau public.

Un filtrage spécifique pourra être mis en place par la DSI entre les différentes zones.