Dispositif assurant le filtrage des accès aux ressources électroniques via un annuaire LDAP

Document révisé en Mars 2006

Introduction, historique et rappels

Le filtrage des accès aux ressources électroniques (bases de données et revues) achetées dans le cadre de la politique nationale, s'effectuait entièrement **chez les éditeurs** (à l'exception du Wok) et de **deux façons**:

- par reconnaissance de numéros IP de machines. Le filtrage est effectué sur la base des déclarations de numéros de machines faites par l'INRA (déclarations établies à partir des inventaires du pôle SI). Les numéros déclarés appartiennent **exclusivement** aux tranches de réseaux IP gérées par l'établissement. Toutes les ressources contractualisées dans le cadre national étaient accessibles par ce moyen et rassemblées sur l'ancien **Portail 1**.

- par reconnaissance de **login/password** collectifs ou personnels, transmis par le GRAP aux ayants droit via les DU. Cette procédure était réservée aux ayants droit hors réseaux INRA et ne permettait d'accéder qu'à une partie des ressources disponibles. Celles-ci étaient rassemblées sur l'ancien **Portail 2**.

Ces deux procédures avaient chacune leurs avantages et leurs inconvénients, mais elles ne permettaient ni l'une ni l'autre d'exécuter pleinement les contrats en ce qui concerne les demandes de l'administration (en réponse aux besoins des chercheurs) et celles des éditeurs (délimitation précise des ayants droit).

L'INRA assure désormais lui-même et **nominativement** le filtrage de ses ayants droit à l'aide d'un dispositif d'annuaire utilisant le protocole LDAP.

Les intervenants et leur rôle

Rôle du pôle SI

- concevoir le dispositif
- le réaliser et le mettre en production
- le déployer pour l'ensemble des ayants droit (sur sites et hors sites INRA)

Rôle du GRAP

- délimiter les ayants droits (interfaçage avec l'équipe CompAct), tels que contractuellement décrits

- assurer l'interfaçage avec le pôle SI (cahier des charges, organisation du changement, ouvertures d'accès) et du 2R2E (tests, assistance aux utilisateurs finals)
- assurer l'interfaçage avec les éditeurs (informations sur le dispositif et sa mise en place, déclaration d'ajouts et de retrait des numéros IP et des login/mots de passe)

Rôle du 2R2E (et des utilisateurs finals volontaires)

- acquérir la compréhension du dispositif mis en place
- tester localement le dispositif et les solutions techniques, faire remonter au GRAP les résultats de ces tests
- expliquer le dispositif aux utilisateurs finals

Le dispositif de filtrage et ses composantes

Principe du filtrage des accès

Les requêtes d'un ayant droit sont dirigées vers des machines proxy dédiées qui assurent leur relayage, après que cet utilisateur ayant droit s'est identifié (via un nom d'utilisateur) et authentifié (via un mot de passe) soit:

- dans le cas d'une procédure d'accès classique via un navigateur (ou profil) dédié,
- ou dans le cas d'une procédure d'accès via un script de configuration automatique du proxy. Dans ce cas, seules les requêtes vers les ressources électroniques nationales sont redirigées automatiquement vers des machines proxy dédiées, toujours suivant le même principe après que l'utilisateur s'est identifié et authentifié.

Schéma général du filtrage d'accès

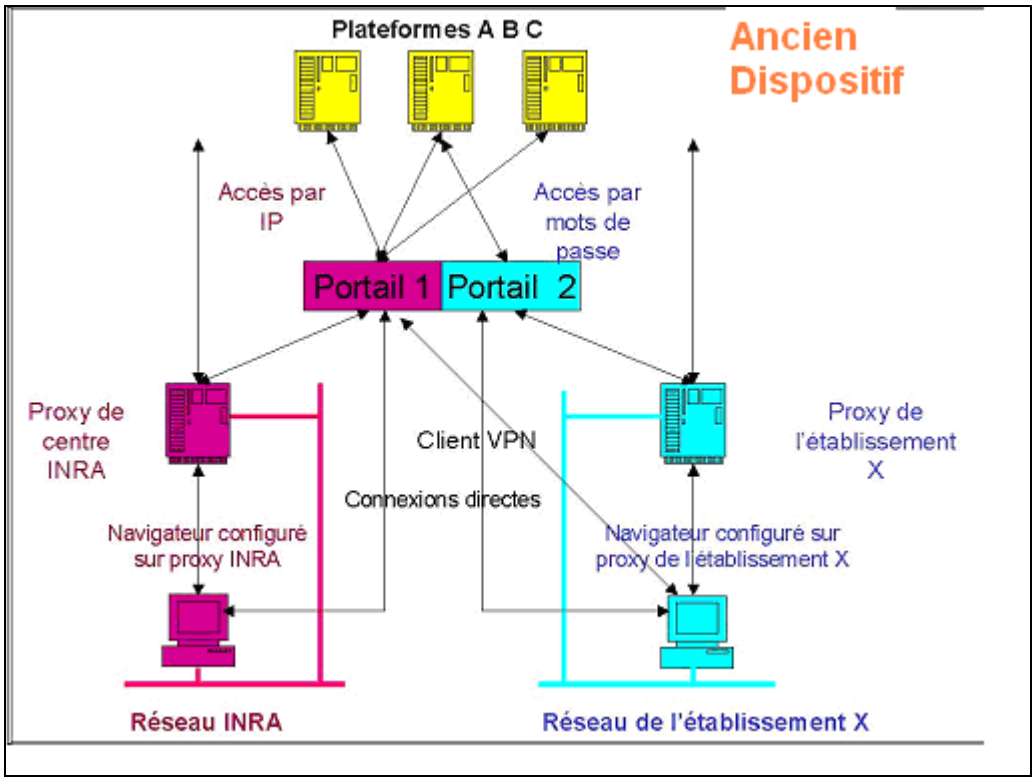
1/ Configuration en dur des navigateurs.
L'utilisateur ayant droit doit utiliser un navigateur (ou un autre profil de son navigateur habituel, nommé revelec du nom des machines composantes du dispositif) dédié à l'activité bibliographique. Ce navigateur est configuré avec l'adresse canonique **revelec.inra.fr** et le port **3128**. Derrière cette adresse figurent une ou plusieurs machines qui interrogent un annuaire LDAP et contrôlent ainsi les accès.

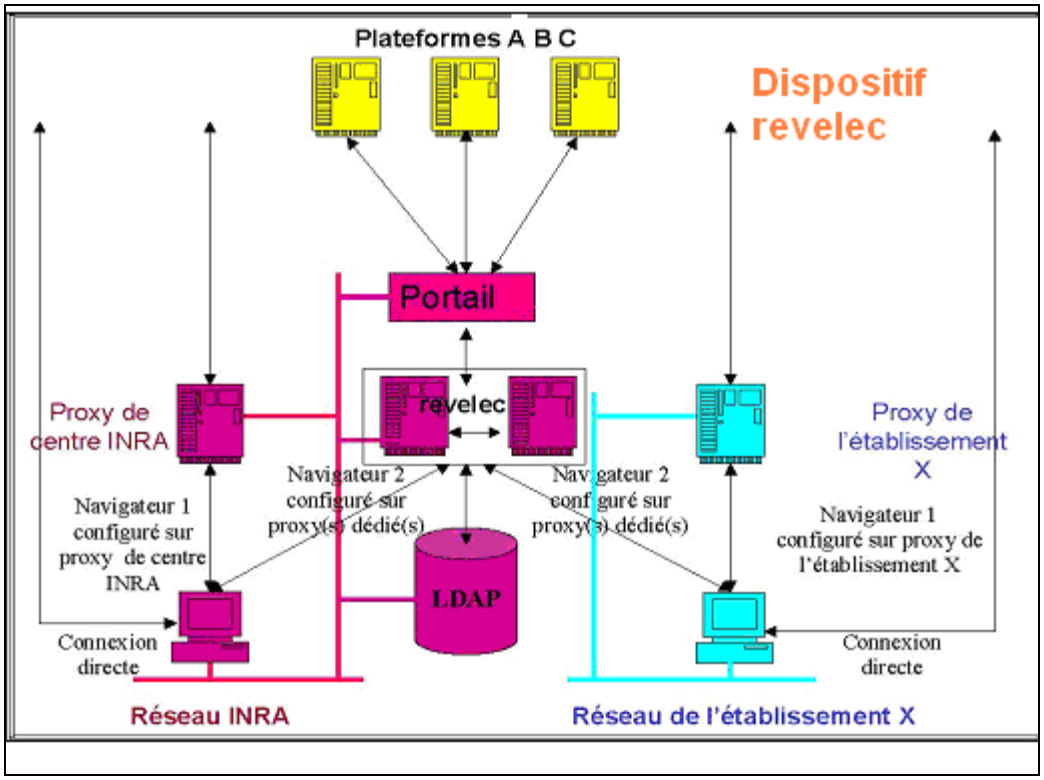
Lorsque l'utilisateur déclenche le navigateur ainsi configuré, il recoit une invite à entrer son nom d'utilisateur et son mot de passe LDAP. Après vérification du nom d'utilisateur et du mot de passe dans l'annuaire (identification et authentification), il reçoit la page qu'il a déclarée comme page d'accueil (c'est à dire celle du portail) et il est autorisé à accéder aux ressources électroniques.

2/ Utilisation d'un script de configuration automatique des proxy
L'utilisateur ayant droit doit utiliser un navigateur avec l'url de configuration automatique du proxy dédié à l'application plateformes positionné dans son navigateur (ou dans un autre profil de son navigateur habituel). Dans une session, ce script redirige

automatiquement les requêtes vers un des proxy dédié et à la première utilisation d'une ressource éditoriale nationale, l'utilisateur reçoit l'invite à entrer son nom d'utilisateur et son mot de passe LDAP et il est autorisé à accéder.

Accès aux ressources électroniques nationales





Ancien dispositif

Les utilisateurs sur réseaux INRA, accèdaient par reconnaissance IP aux ressources de l'ancien portail 1.
Les utilisateurs autorisés hors réseaux INRA, accèdaient par login/password éditeur, aux ressources de l'ancien portail 2 ou dans certains cas par reconnaissance IP, aux ressources de l'ancien portail 1 via un client VPN (Virtual Private Network). La plupart du temps les requêtes émises passent par un proxy/cache, serveur qui stocke provisoirement les résultats et les relaie vers la machine demandeuse, mais il existe aussi des connexions directes à l'Internet sans proxy et des connexions via un FAI (fournisseur d'accès Internet) .
Les utilisateurs se servent du même navigateur pour accéder à toute les applications auxquelles ils ont droit (internet, intranet achat, CompAct, plateformes etc.)

Nouveau dispositif / Dispositif revelec du nom des machines composantes du dispositif

Tous les utilisateurs (sur réseaux et hors réseaux INRA) accèdent aux mêmes ressources par un seul portail d'orientation et d'information, avec un seul nom d'utilisateur/mot de passe donné par le ldapmaster, sur la base d'un fichier nominatif des ayants droit validé par le GRAP. Toutes les requêtes vers les ressources du Portail sont envoyées vers des proxy dédiés, fonctionnant en parallèle, qui procèdent à l'identification et à l'authentification des ayants droit via un annuaire LDAP et contrôlent leur habilitation.

Soit les utilisateurs disposent de deux navigateurs, ou de deux profils d'un même navigateur (schéma dispositif revelec ci-dessus). Le premier (navigateur 1 ou profil par défaut) est utilisé pour les applications autres que l'application plateformes . Le second (navigateur 2 ou profil revelec) est réservé à l'application plateformes et paramétré avec une adresse - **revelec.inra.fr** - commune aux machines dédiées à ce dispositif (voir **Procédure d'accès nécessitant deux navigateurs**).
Soit les utilisateurs utilisent un seul navigateur pour toutes leurs applications, avec l'url du script de configuration automatique de proxy dédié à l'application plateformes positionné dans leur navigateur (voir **Procédure d'accès via un seul navigateur**).

Les utilisateurs - qu'ils soient sur réseaux INRA ou hors réseaux INRA, (sur un site INRA ou non, en mission ou depuis leur domicile),- **ont accès aux mêmes ressources, dans les mêmes conditions.**