Sécurité et annuaire LDAP

Retour d'expérience

Christophe.kersuzan@cls.fr

Sommaire

- CLS
- Problématique
- LDAP : la solution ?
- Meta-annuaire et synchronisation mot de passe
- HTTPS et Ichain
- Conclusion

CLS (Collectes et Localisations par Satellites)

- 250 employés sur Toulouse
- Protection de l'environnement par des systèmes Satellitaires.
  - **Le système Argos**

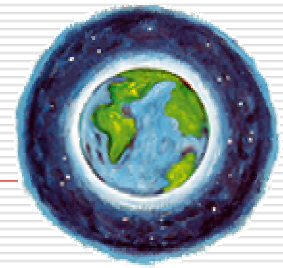
    Pour calculer des positions à 300 mètres près et mieux et collecter des données. Tout mobile (bouée océanographique ou météorologique, animal, bateau de pêche...) équipé d'une balise Argos peut être localisé avec cette précision.

  - **L'océanographie spatiale**

    Pour mesurer les variations du niveau de la mer, les courants océaniques ou la hauteur des vagues. La compétence de CLS s'étend du traitement de la mesure à la fourniture de résultats océanographiques directement exploitables.

  - **Le système Doris**

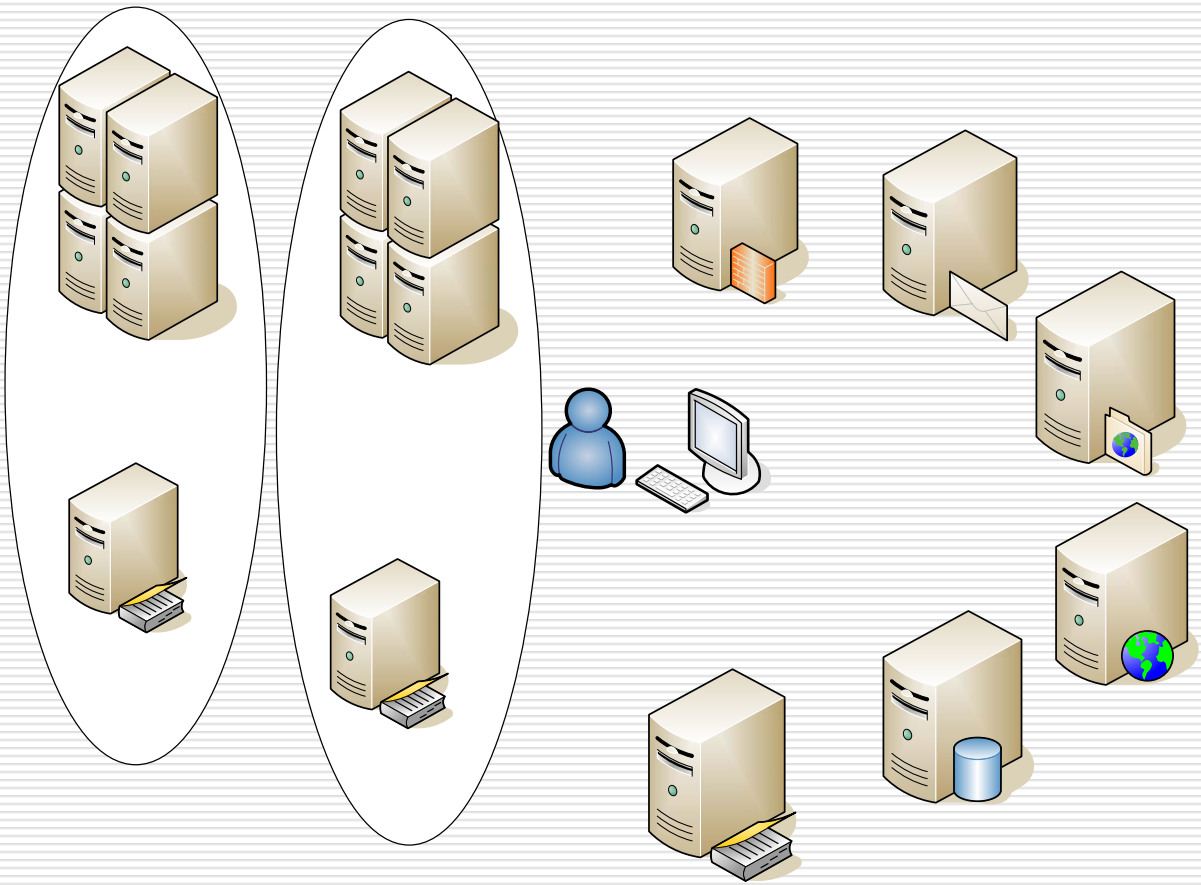
    Pour le calcul précis d'orbite, au centimètre près, et déterminer avec précision des coordonnées de balises au sol.



Problématique (1/3)

- L'accès aux ressources informatiques de l'entreprise doit être sécurisée
- Forte demande pour un accès WEB « crypté »
- Notion de « comptes utilisateurs »
  - Utilisateurs CLS
  - Utilisateurs NON-CLS (Argos, WFP, Novacom, …)
- Plusieurs comptes ?
  - Messagerie
  - Serveurs de calcul
  - Serveur de fichiers
  - Portail
  - …
- Indispensable de fédérer ces comptes

Problématique (2/3)
Plusieurs îlots d'authentification



Problématique (3/3)
Un annuaire universel ?

- Notion d'utilisateur et de profil
  - Utilisateur interne ou externe à l'entreprise
  - Utilisateur avec restriction d'accès à certaines ressources
- L'idéal serait de stocker les profils utilisateurs dans une même base de données
- Un annuaire normalisé est fait pour cela: LDAP (Lightweight Directory Application Protocol)

LDAP: La solution
La guerre des mots de passe ?

- L'annuaire LDAP Iplanet est en place à CLS depuis 1999
- Bonne connaissance du protocol LDAP à CLS
- Fédère la messagerie, l'intranet, l'extranet, ...
- Il manque la connexion avec le monde Windows et Unix
- IBM, Microsoft, Oracle, Iplanet, Novell et les logiciels libres essayent de dominer ce marché

LDAP: La solution
Deux types de besoins LDAP

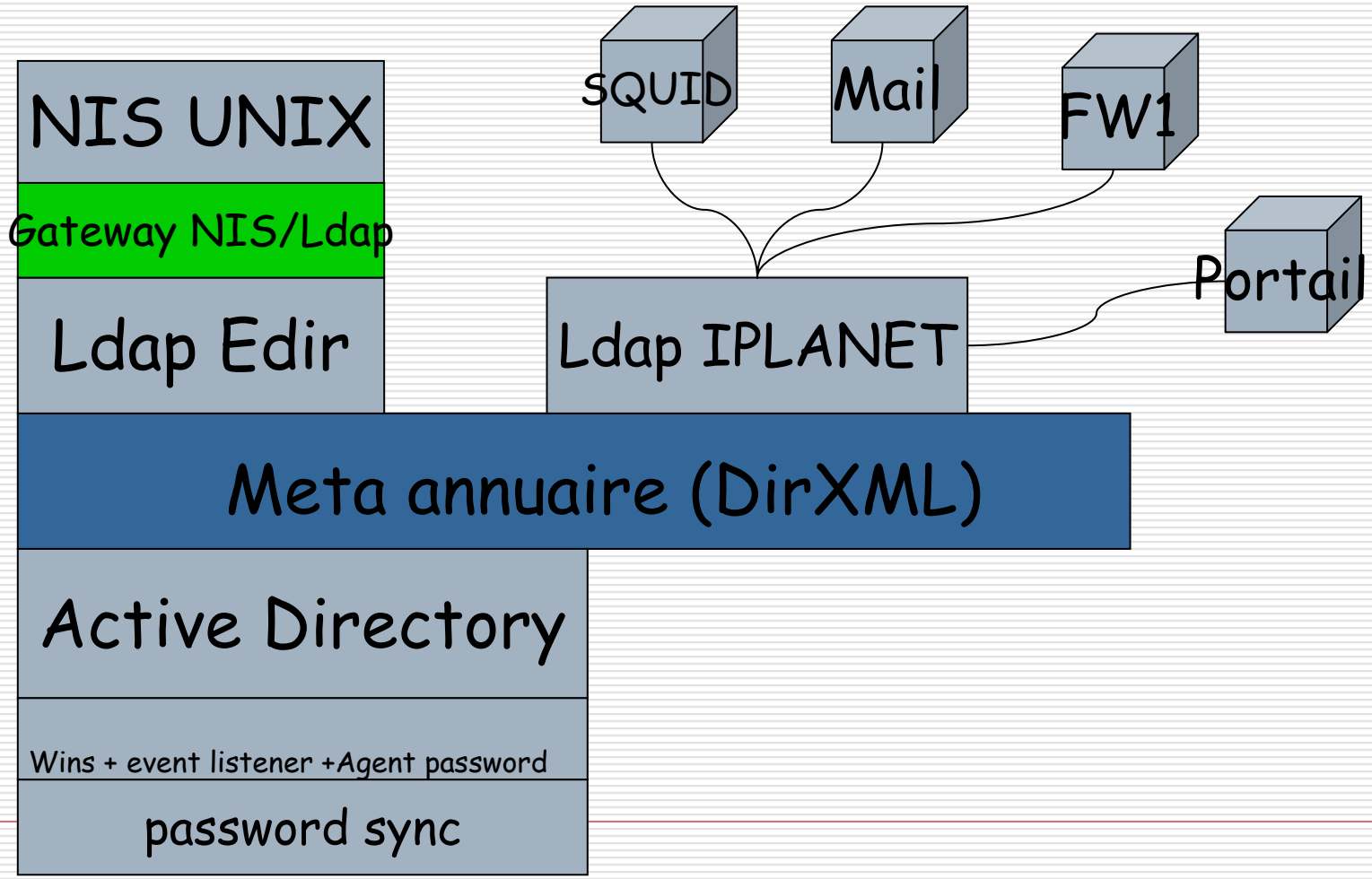
- **Ressources Humaines /communications**

  Les projets de type pages blanches (ou pages jaunes) souvent sponsorisés par les ressources humaines (et/ou la direction générale)

DSI

Les projets d'unification d'annuaires système poussés par le département informatique (en vu de la mise en place d'un SSO par exemple)

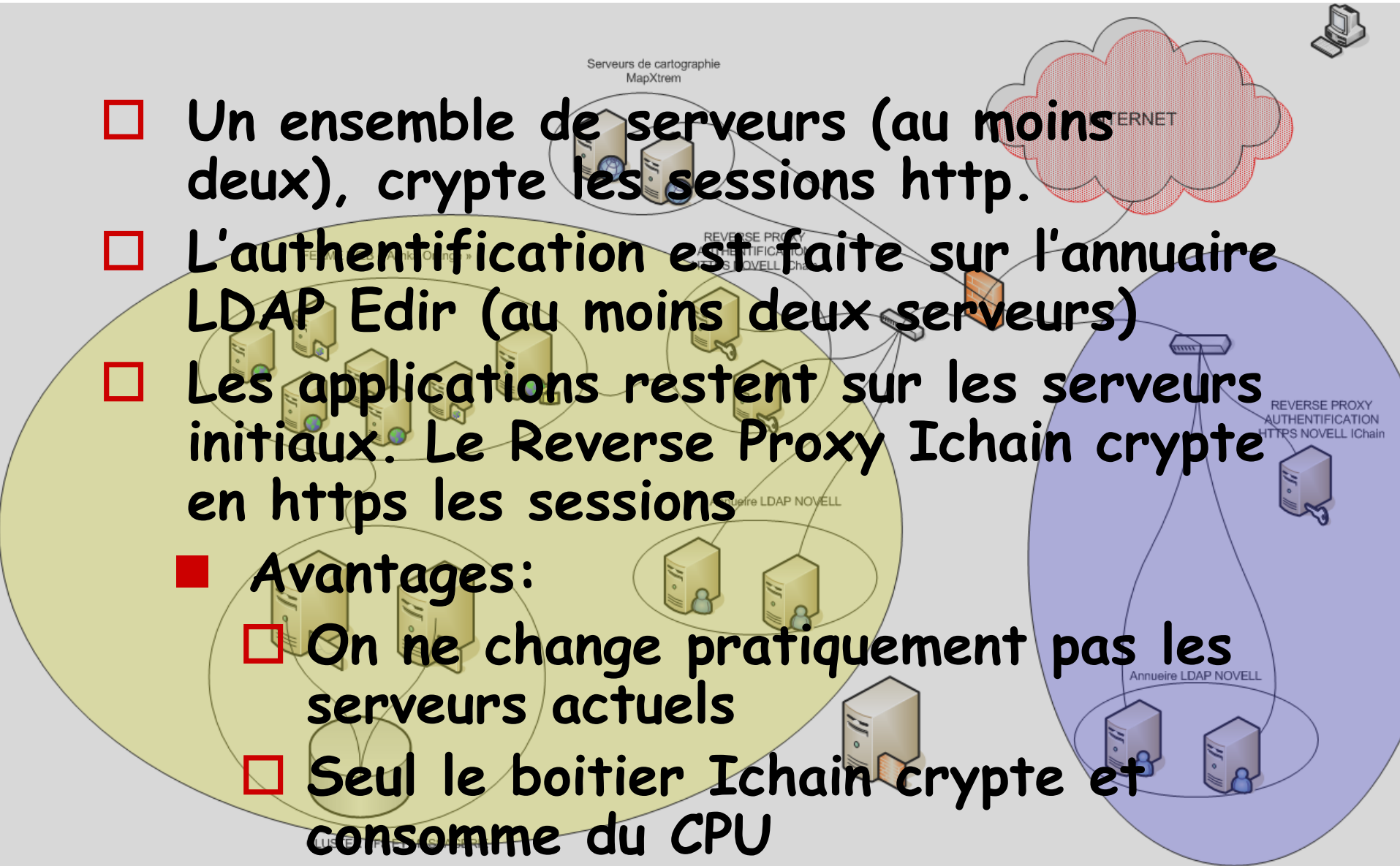
Meta-annuaire et synchronisation mot de passe



HTTPS et Ichain
Sécurité et annuaire

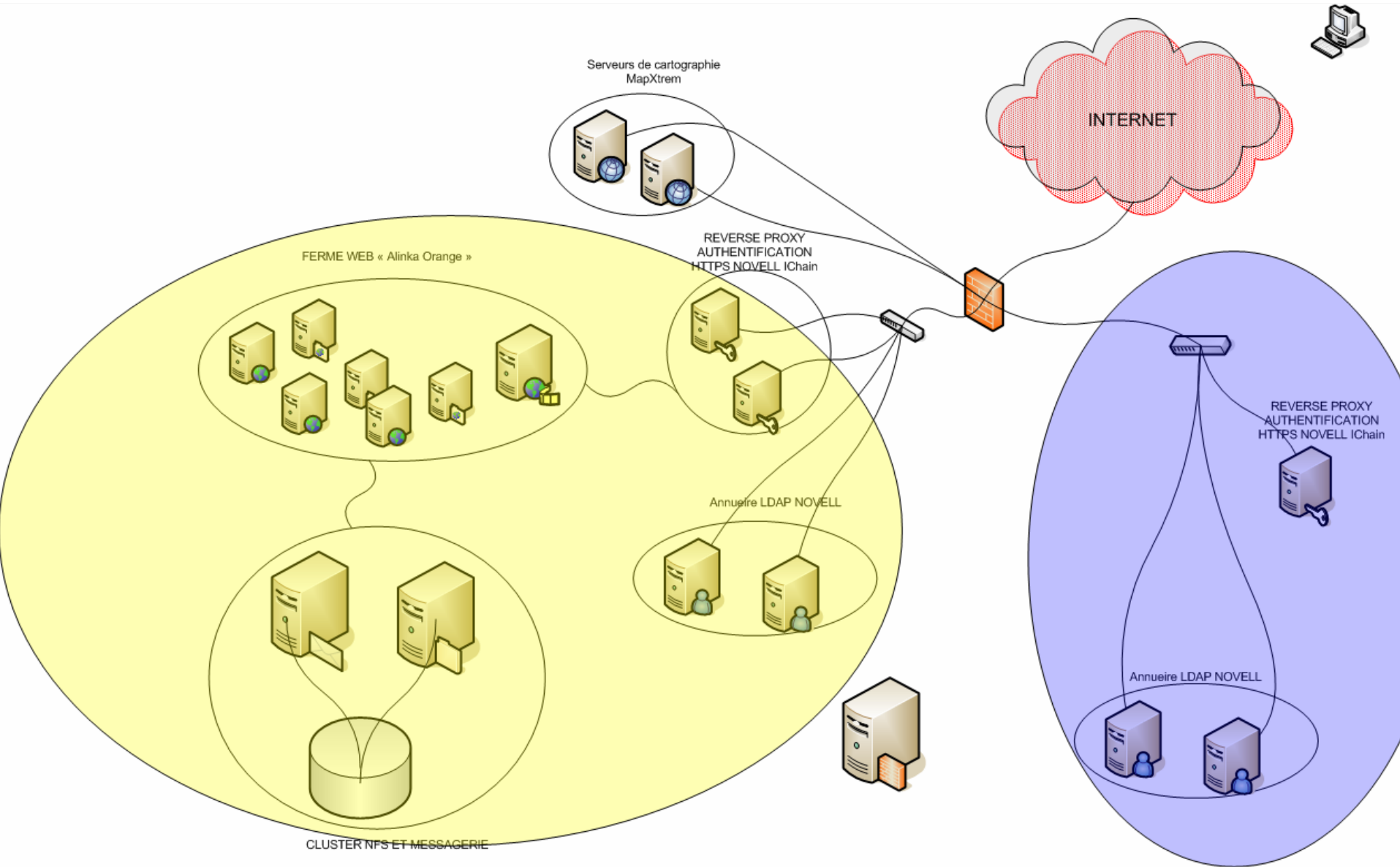
- Impossible de faire participer les utilisateurs à la politique de sécurité de CLS sans leur simplifier la gestion du mot de passe
- Un seul et même mot de passe pour tous les systèmes basés sur LDAP
- Un accès WEB crypté basé sur une authentification LDAP
- Choix: Edirectory de chez Novell

Https et reverse proxy



- Un ensemble de serveurs (au moins deux), crypte les sessions http.
- L'authentification est faite sur l'annuaire LDAP Edir (au moins deux serveurs)
- Les applications restent sur les serveurs initiaux. Le Reverse Proxy Ichain crypte en https les sessions
  - Avantages:
    - On ne change pratiquement pas les serveurs actuels
    - Seul le boitier Ichain crypte et consomme du CPU

Schéma de fonctionnement



Cryptage et annuaire: Principe de Novell iChain

Navigateur

iChain Proxy Server

User=xx Password=xx

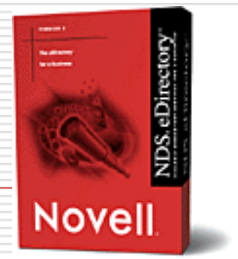
Security

Livres=Aventures

Serveurs Web et d'applications

1. Authentification—Qui êtes vous ?
2. Controle d'accès—A quoi avez-vous accès ?
3. Authentification unique
4. Personnalisation
5. Confidentialité des données

iChain Authorization Server



Conclusions

- Politique de licences
- Difficultés rencontrés
- Solutions alternatives
- Questions

Politique de licences Novell

- X,x € / entrée LDAP
- xx € / entrée pour le moteur DirXML
- X,x € pour la synchro passwd Windows
- X,x € pour la synchro NIS
- x € pour Ichain
- + les souscriptions annuelles

Difficultés rencontrées

- Environnement Informatique hétérogène dans les entreprises: Unix, Windows, OpenVMS, WEB, …
- Opposition forte entre Microsoft et Linux, peu d'informations de la part de Microsoft
- Gestion temporaire de deux annuaires LDAP avec quelques fonctionnalités différentes
- 5 serveurs supplémentaires

Solution alternative: le logiciel libre

- Utilisation de OpenLDAP
- La condition: On remplace les serveurs Windows par LINUX/SAMBA
- Postfix/Cyrus/Squid

Sécurité et annuaire LDAP

Retour d'expérience

Christophe.kersuzan@cls.fr