VISON
Vers un Intranet Sécurisé Ouvert au Nomadisme

Eric Gautrin
Comité de Concertation des Moyens Informatiques INRIA

6 décembre 2005

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

Plan

Contexte INRIA

Enjeux et objectifs de VISON

Service d’authentification

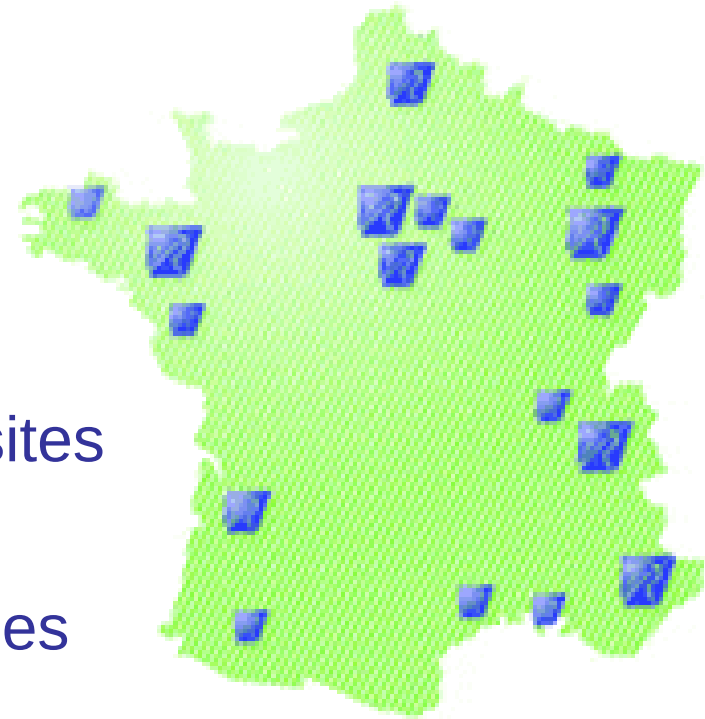
Service VPN

Chiffrement de données

Pare-feux

Bilan et perspectives

Contexte INRIA



6 unités de recherche, le siège

équipes ou chercheurs sur d’autres sites

3500 personnes dont 2700 scientifiques

nomadisme très présent

6 services informatique

Enjeux du projet VISON

Un des facteurs d'unité de l'INRIA

- Rendre transparente la localisation géographique
- Faciliter le nomadisme sous toutes ses formes
- S'ouvrir tout en sécurisant

Premier axe de travail

Rendre accessible les ressources depuis l'extérieur

- Authentification utilisateur
- Connexion sécurisée (HTTPs, POPs, IMAPs…)

Deux actions

- Service fédérateur d'authentification
- Service d'accès VPN

Second axe de travail

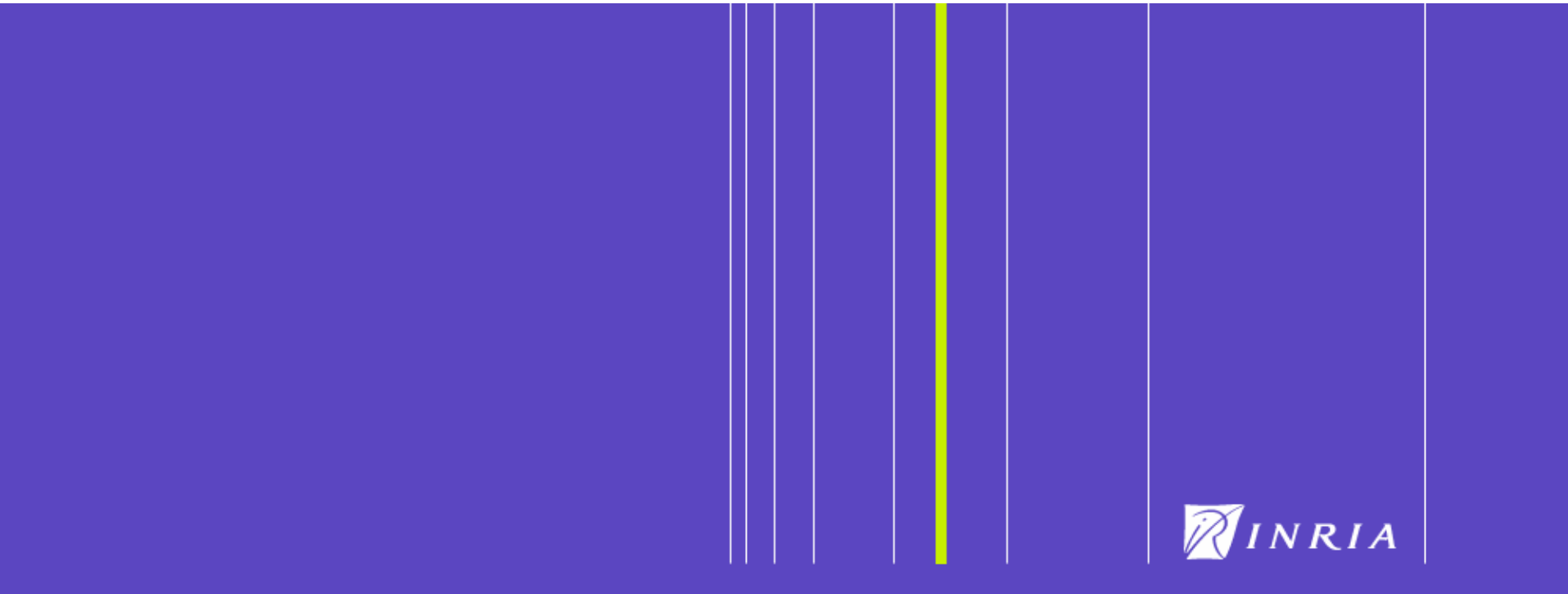
Mieux protéger les données sur les ordinateurs portables

- Données : partie du patrimoine de l'établissement
- Risque plus élevé de vol ou de piratage pour les portables

Deux actions

- Chiffrement des données enregistrées sur le disque dur
- Systèmes de protection pare-feux natifs

Service fédérateur d’authentification



Un dispositif fédérateur basé sur LDAP

Choix de LDAP

- Compétences techniques existantes
- Nombreux services s'interfaçant à LDAP

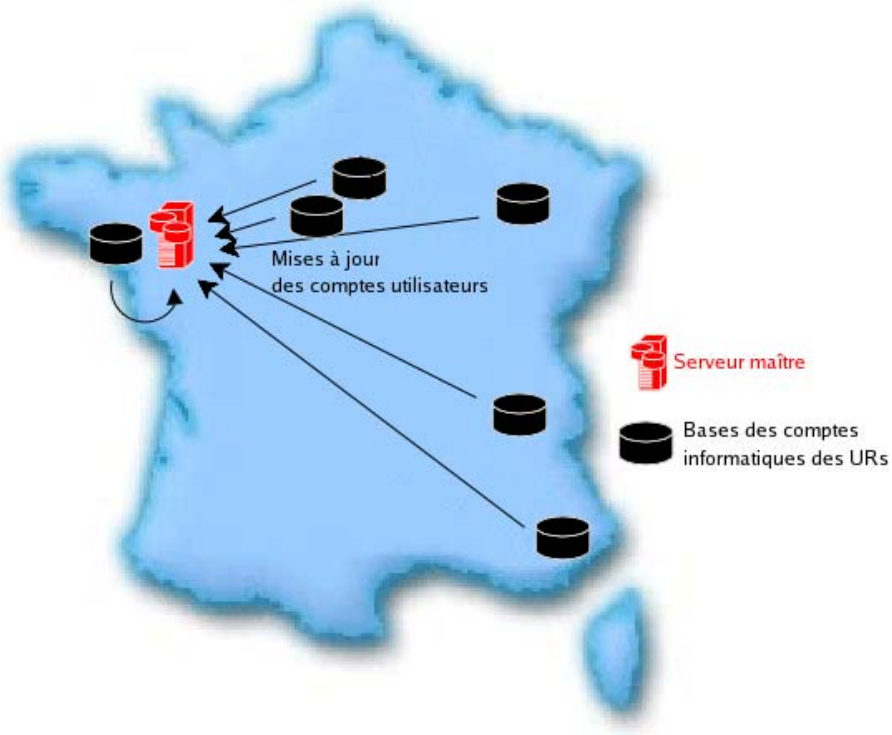
2 identifiants utilisateurs

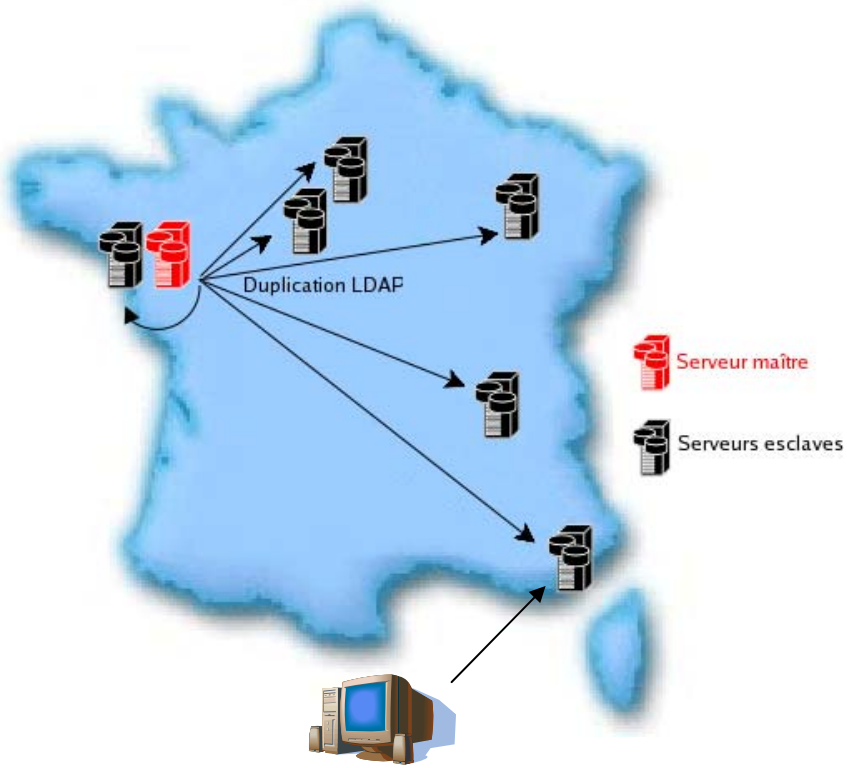
- Cohérence: non réutilisation, unicité, création déléguée

Règles

- Nomenclature, historique…
- Conflits réglés par concertation

L’architecture de service





Conclusion et évolutions

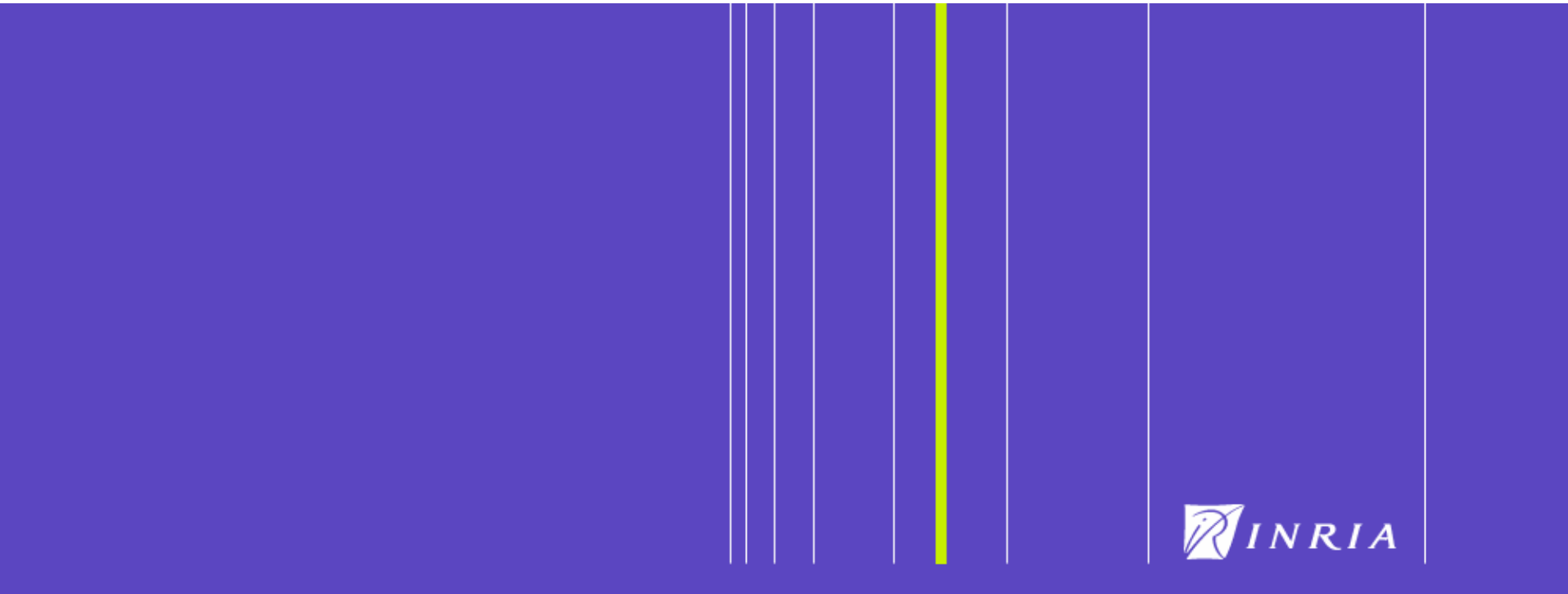
Un dispositif fédérateur opérationnel depuis oct 2004

- Géré par une équipe transversale
- 16 ressources interfacées (WEB, Sympa, News…)

Pistes de réflexion:

- Utilisation de la base globale pour d'autres usages
  - gestion de groupes d'utilisateurs (habilitations)
  - stockage de certificats numériques
  - …

Le service d’accès VPN



Le service VPN

Pourquoi une technologie VPN ?

- Pour des applications sans authentification utilisateur

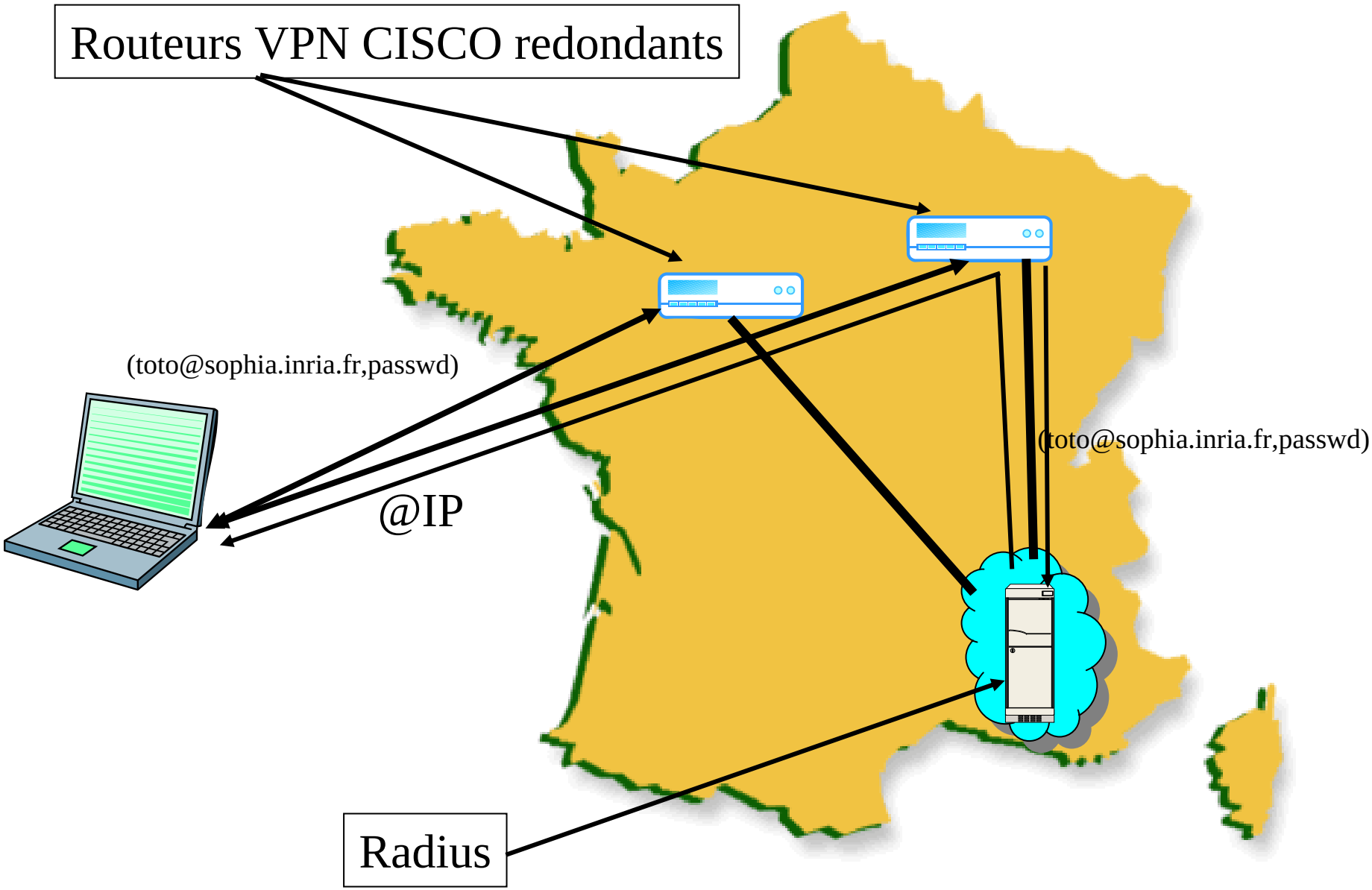
  sans connexion chiffrée

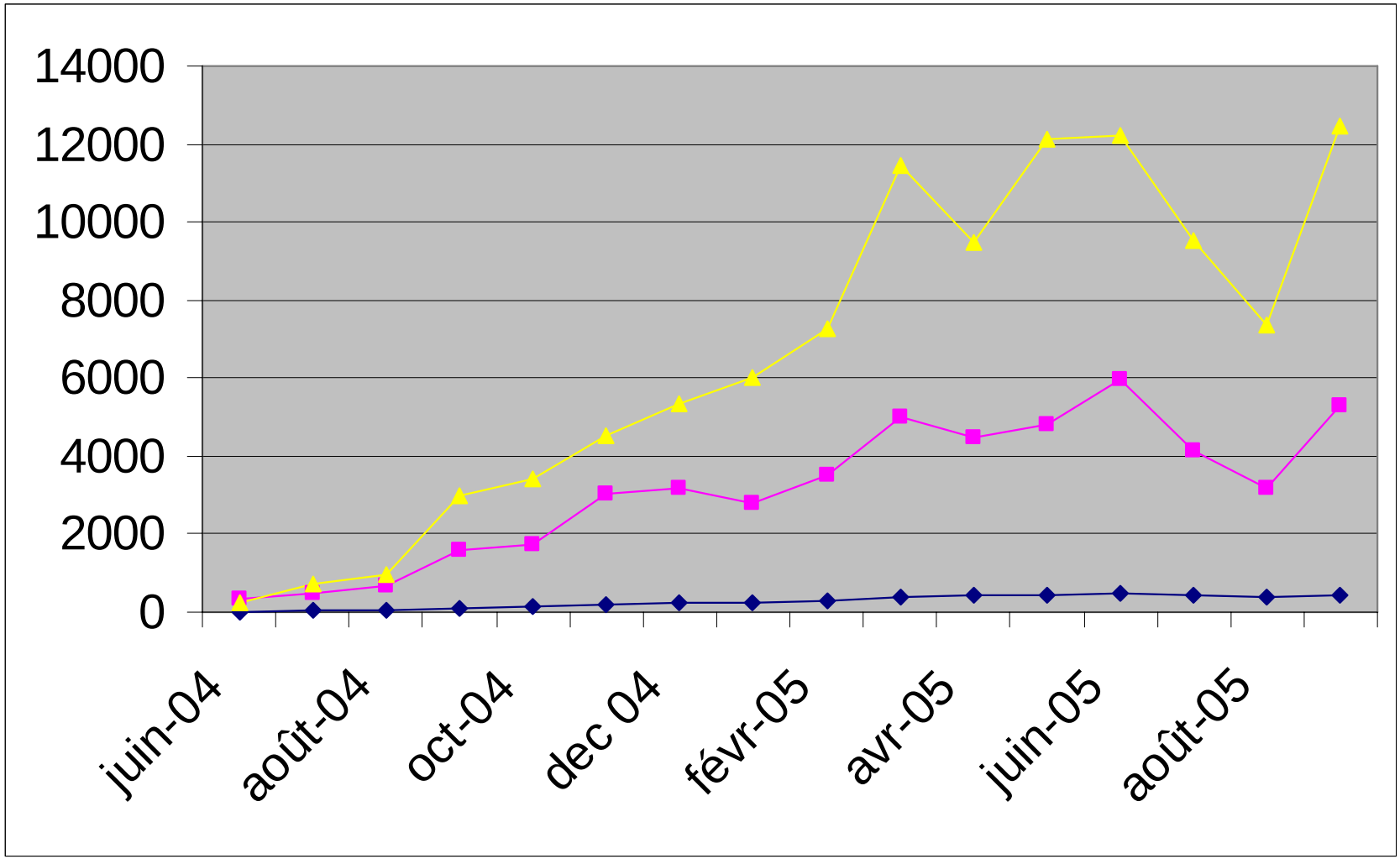
VPN : une solution générique

Utilisation du VPN

- **INTRANET-INRIA** : accès à l'intranet INRIA + quelques serveurs par le VPN. Le reste par le réseau local d'interconnexion

- **VPN-TOTAL** : tous les accès par le VPN


Routeurs VPN CISCO redondants
(toto@sophia.inria.fr,passwd)
@IP
(toto@sophia.inria.fr,passwd)
Radius


14000
12000
10000
8000
6000
4000
2000
0
juin-04
août-04
oct-04
dec 04
févr-05
avr-05
juin-05
août-05
Nb utilisateurs
Nb connexions
Nb heures

Conclusion et évolutions

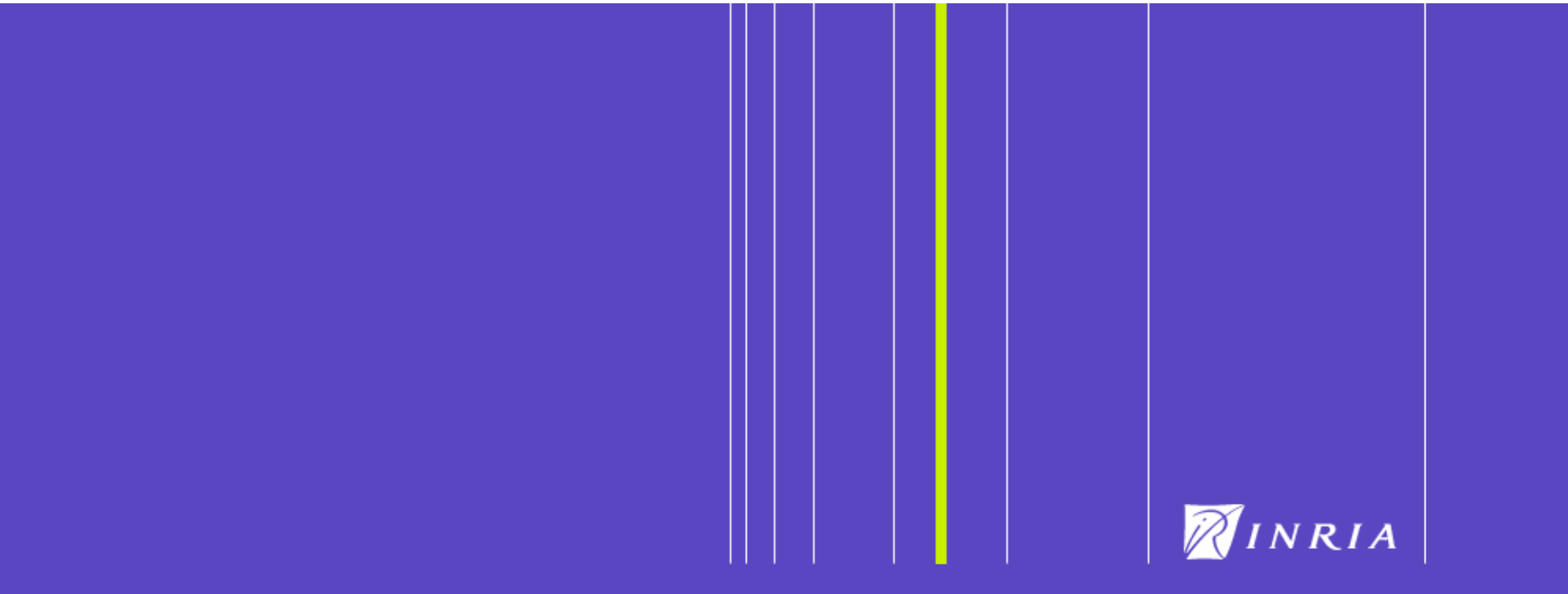
Service opérationnel depuis juin 2004

- Géré par une équipe transversale

Pistes de réflexion

- Évolution de l'authentification par signatures RSA
- Étude de VPN/SSL, OpenVPN
- Utilisation pour d'autres usages
  - Exemples : confidentialité pour ToIP, accès WIFI…

Chiffrement des données sur le disque dur d'un portable



Protéger le patrimoine de l'établissement

Risque élevé pour les portables: vol, piratage

Une politique de chiffrement des données

- Les obligations légales et juridiques
- Les données à protéger
- Les recommandations associées
- Le choix d'outils
- L'organisation

Obligations légales et juridiques

Obligations de l'agent ? de l'établissement ?

Loyauté de l'agent à l'égard de son établissement

- Appliquer les consignes de sécurité
- Communiquer sur demande tout document professionnel

A concilier

- Principe de subordination entre employeur et agent
- Respect des libertés individuelles

Suivant 3 principes

- **Nécessité**: limitations pour remplir les finalités de l'établissement
- **Proportionnalité**: limitations proportionnelles au but recherché
- **Transparence**: négociation collective et information

Données à protéger

Deux types discernés à l'INRIA

Données sensibles

- Protégées par un droit de propriété intellectuelle
- À caractère secret ou confidentiel

Données ultra sensibles

- Données sensibles avec protection demandée par un tiers

Moins de 20 % des données

Évolution au fil du temps

Catégories de données et recommandations

Données sensibles

- Ne pas les stocker sur un portable
- Si nécessaire, utiliser un outil de chiffrement pour se prémunir d'un accès trop facile.

Données ultra-sensibles

- Ne pas les stocker sur un portable
- Si nécessaire, utiliser un outil de chiffrement offrant la meilleure protection

Données non sensibles

- Aucune recommandation

Données de la sphère privée

- Aucune recommandation. Identification claire

Séquestre de clés et logiciels

Obligation de l'établissement

Dépôt

- Souple, à l'initiative de l'utilisateur

Recouvrement par l'utilisateur

- Souple, s'assurer de l'identité du demandeur

Recouvrement pour un tiers de l'établissement

- Exceptionnel, s'entourer de précautions

Recouvrement pour un tiers hors établissement

- Très exceptionnel, vérifier la légitimité de la demande

Niveaux de protection des outils

Adapté en fonction des besoins

Données sensibles: se prémunir d'un accès trop facile

- **Catégorie « confidentialité »**
  - Ergonomie, transparence et facilité d'utilisation
  - Déploiement aisé
  - Performance
  - Recouvrement de la clé par l'utilisateur

Données ultra sensibles : protéger au maximum

- **Catégorie « coffre-fort »**
  - Robustesse au sens cryptographie
  - Utilisation explicite
  - Séquestre de clé

Éléments d’analyse d’outils

Chiffrement des fichiers temporaires

Utilisation de la mise en veille prolongée

Gestion des clés de chiffrement

Impact entre passwd de session et passphrase de chiffrement

Stockage des clés sur support physique

Etat des données suite à un plantage

Taille du fichier conteneur et performance

Compatibilité avec système de sauvegarde

Protection au démarrage du système d’exploitation

Et encore

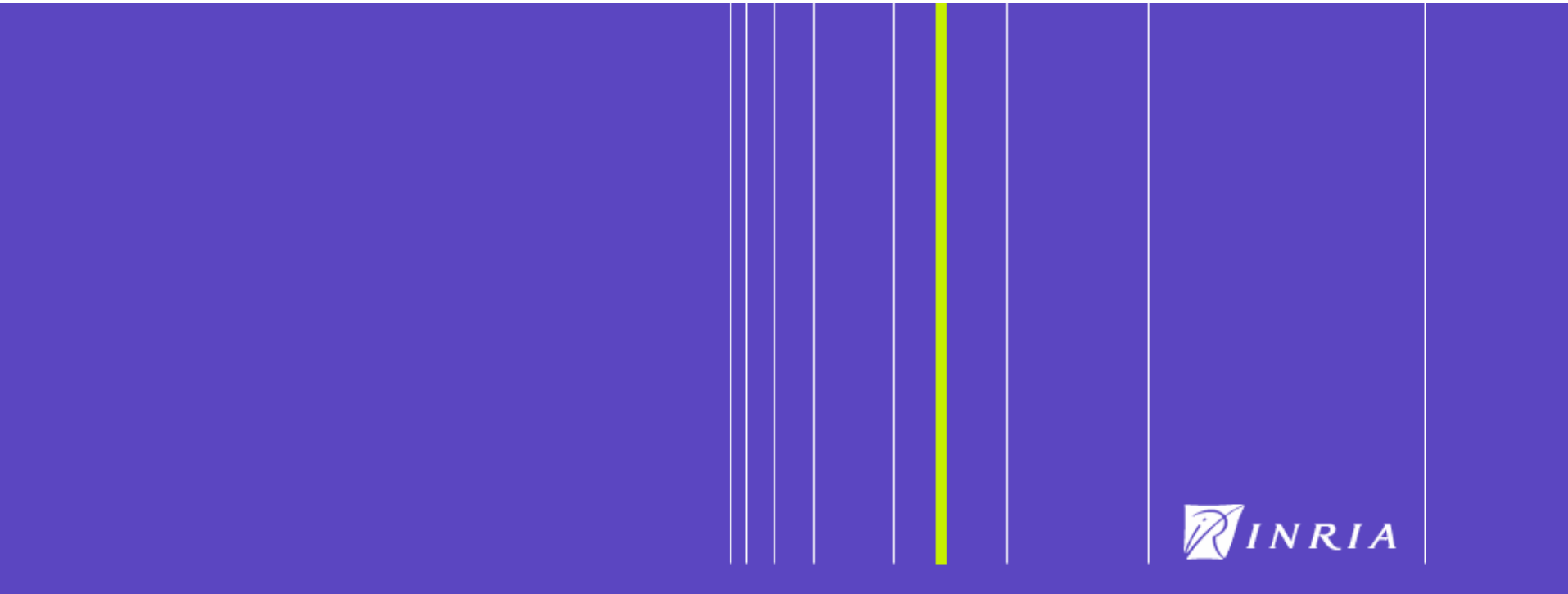
Charte informatique

Négociation collective, communication

Organisation du séquestre

Veille technologique sur les outils

Systèmes de protection pare-feux



Objectifs de l’étude

- Se limiter aux pare-feux natifs
  - Pas de surcoût, pas de déploiement

- 2 critères recherchés pour les portables
  - Connexion au réseau local du site
    - Offrir une bonne protection
    - Autoriser les opérations de sauvegarde et d’administration
  - Connexion à un autre réseau
    - Offrir la protection maximale

Windows XP SP2

Principe: le pare-feu activé rejette tous les paquets entrants non sollicités

Deux profils offerts

- « Domaine »: permet sauvegarde, administration, XWin
- « Standard »: bloque le trafic entrant non sollicité

Linux

Pare-feu basé sur les composants netfilter/iptables

Possibilités importantes de configuration

- Scripts exécutés lorsqu'une interface réseau est activée ou désactivée

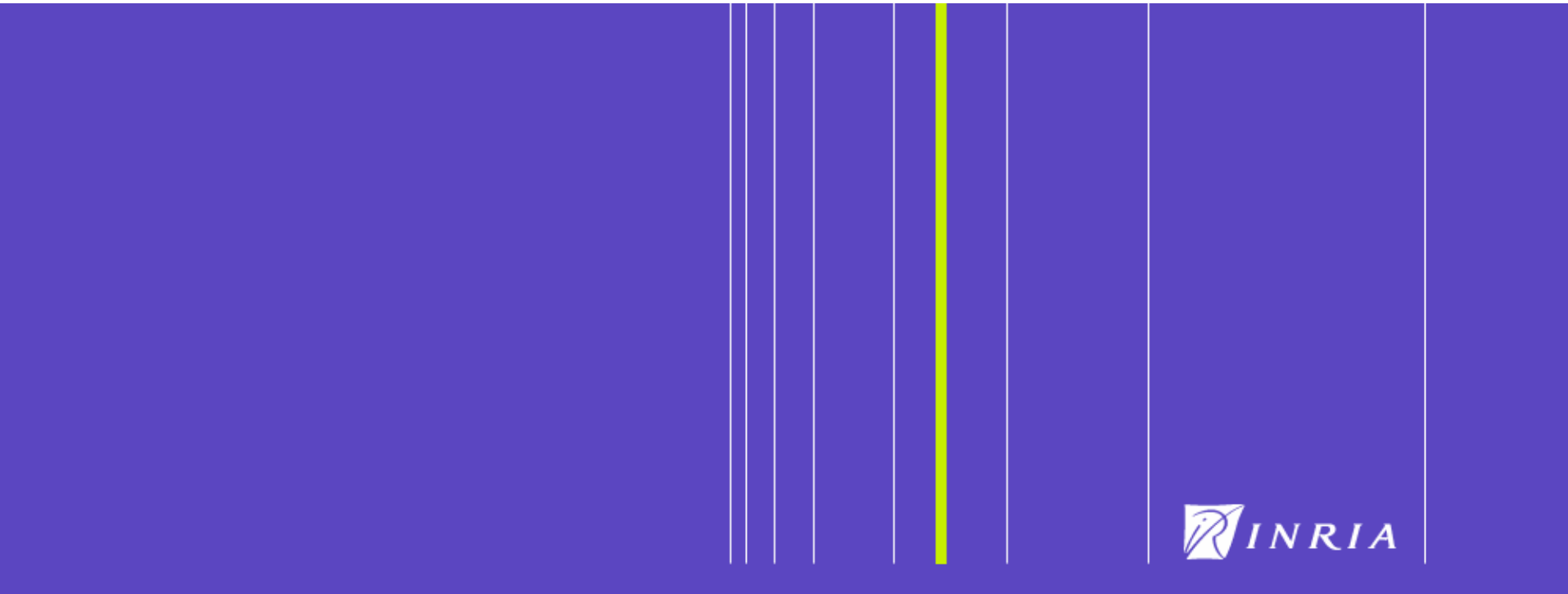
Conclusion

Recommandations d’utilisation des pare feux

Perspectives

- Étude d’autres solutions

Bilan de VISON



Bilan technique

D’une sécurisation basée sur @IP

Vers sécurisation basée authentification utilisateur

De ressources accessibles uniquement depuis l’INRIA

A des ressources accessibles depuis le monde entier

Disponibilité de briques de base pour d’autres usages

Bilan du projet

Durée : 26 mois (février 03 à mai 2005)

Coûts d'investissements: 50 K€

Humain :

- Forte implication à tous les niveaux
- 7 équivalents temps plein ingénieur

Véritable dynamique transversale

Un élément fédérateur fort pour l'INRIA

Après VISON

Un capital

- Des services mutualisés: authentification, VPN
- Une politique de chiffrement
- Des recommandations: pare-feux, mémorisation des mots de passe par les navigateurs
- Une dynamique transversale

Nouvelles actions

- Authentification par certificats numériques
- Réseaux non filaires
- Détection de vulnérabilités sur les portables
- Service global de messagerie, travail coopératif