

VISON : Vers un Intranet Sécurisé Ouvert au Nomadisme

Eric Gautrin

▶ **To cite this version:**

Eric Gautrin. VISON : Vers un Intranet Sécurisé Ouvert au Nomadisme. JRES 2005, 2005, Marseille, France. hal-00018292

HAL Id: hal-00018292
https://hal.science/hal-00018292

Submitted on 31 Jan 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

VISON : Vers un Intranet Sécurisé Ouvert au Nomadisme

Eric Gautrin
Comité de Concertation des Moyens Informatiques
Eric.Gautrin@inria.fr

Résumé

L'INRIA est un institut implanté dans 6 sites principaux, et dans une dizaine d'autres sites. Le nomadisme y est très présent. Ceci ne va pas sans poser de problèmes pour l'accès aux informations et ressources internes mises à disposition principalement sur les sites principaux.

L'amélioration des accès repose sur une authentification utilisateur et des modes d'accès sécurisés mis en œuvre par un service d'authentification LDAP auxquelles s'interfacent quelques applications (WEB, Sympa, …) et par un service VPN offrant une solution d'accès aux ressources générique, sécurisé et authentifié.

L'utilisation d'ordinateurs portables par les nomades pose des problèmes de protection. Pour limiter les risques de vols ou piratages lorsqu'ils se connectent à des réseaux extérieurs (autres établissements, conférences, hot-spots, …), deux actions ont porté sur le chiffrement des données et sur les pare-feux personnels.

Mots clefs

Nomadisme, annuaire LDAP, authentification LDAP, VPN (Virtual Private Network), protection des ordinateurs portables, chiffrement des données, pare-feux.

1 L'INRIA

L'INRIA, Institut National de Recherche en Informatique et en Automatique placé sous la double tutelle des ministères de la recherche et de l'industrie, a pour vocation d'entreprendre des recherches fondamentales et appliquées dans les domaines des sciences et technologies de l'information et de la communication (STIC). L'institut assure également un fort transfert technologique en accordant une grande attention à la formation par la recherche, à la diffusion de l'information scientifique et technique, à la valorisation, à l'expertise et à la participation à des programmes internationaux.

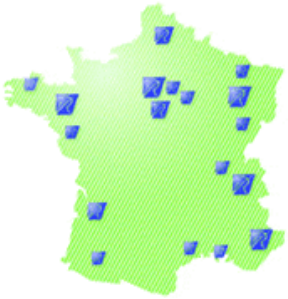


Figure 1 - *Implantations de l'INRIA*

L'INRIA accueille dans ses 6 unités de recherche situées à Rocquencourt, Rennes, Sophia Antipolis, Grenoble, Nancy, Futurs (Bordeaux, Lille, Saclay) et sur d'autres sites à Paris, Marseille, Lyon, Metz, Montpellier, Nantes, Lannion, … (voir Figure 1). 3500 personnes dont 2700 scientifiques, issus d'organismes partenaires de l'INRIA (CNRS, universités, grandes écoles) qui travaillent dans plus de 120 "projets" (ou équipes) de recherche communs. Un grand nombre de chercheurs de l'INRIA sont également enseignants et leurs étudiants (environ 950) préparent leur thèse dans le cadre des projets de recherche de l'INRIA.

Outre les nombreuses implantations géographiques, le nomadisme est très présent à l'INRIA comme en témoigne le taux d'utilisation des ordinateurs portables : 60 à 70% des scientifiques en sont équipés, ainsi que de nombreux ingénieurs et techniciens.

Les principales ressources informatiques de l'INRIA sont réparties dans les 6 unités de recherche. Un service informatique rattaché à chaque unité de recherche administre l'ensemble de l'infrastructure locale (réseau local, services de bases, sécurité informatique, …). Une coordination nationale entre ces services informatiques permet d'assurer une cohérence globale. Par ailleurs, l'interconnexion réseau entre les sites INRIA est basée sur le réseau Renater.

Concernant les autres sites, les infrastructures auxquelles accèdent les utilisateurs INRIA sont administrées par le service informatique de l'établissement partenaire (universités, grandes écoles, …). Leurs besoins d'accès aux ressources sont similaires aux besoins d'utilisateurs nomades.

2 Objectifs du projet VISON

2.1 Situation fin 2002

Fin 2002, l'INRIA dispose de quelques solutions techniques pour accéder, depuis l'extérieur, aux informations internes ou aux ressources informatiques :

- accès PPP, One Time Password sur une machine bastion… Mais ces solutions étaient jugées lourdes, lentes, peu ergonomiques par nos utilisateurs ;
- ouvertures de plages d'adresses IP entre les sites principaux. Cette solution est lourde à gérer, voire difficile à mettre en œuvre pour des personnes étant sur un site non géré par un service informatique de l'INRIA ou encore se trouvant dans des situations comme un réseau privé et service NAT, un hot spot...
- gestion de comptes d'accès spécifiques aux services pour les utilisateurs hors sites principaux.

2.2 Objectifs fonctionnels

Début 2003, la direction de l'institut lance le projet national VISON : Vers un Intranet Sécurisé Ouvert au Nomadisme. Facteur d'unité de l'INRIA (*L'INRIA pour tous, depuis partout et à tout moment*), les objectifs fonctionnels du projet sont de :

- **Rendre transparente la localisation géographique** : quel que soit le lieu de travail (unité de recherche ou autre site), chaque utilisateur INRIA doit accéder de la manière la plus transparente possible à l'ensemble des informations et ressources informatiques ;
- **Faciliter le nomadisme sous toutes ses formes** : la transparence d'accès est là aussi importante ;
- **S'ouvrir tout en sécurisant** : rendre accessible les informations et les ressources informatiques de l'INRIA doit s'accompagner de mesures de protection : authentification des utilisateurs, connexions sécurisées, protection des données, …

2.3 Axes de travail

De ces objectifs fonctionnels, deux axes de travail principaux découlent :

- rendre accessible les ressources depuis l'extérieur après authentification utilisateur et depuis une connexion sécurisée ;
- mieux protéger les données sur un ordinateur portable se connectant à l'extérieur ;

Accès aux ressources depuis l'extérieur

De nombreuses applications présentes à l'INRIA (WEB, Sympa …) sont paramétrables pour offrir un mode d'accès authentifié et sécurisé depuis l'Internet : d'une part, en interrogeant un annuaire extérieur comme LDAP (Lightweight Directory Access Protocol) pour y vérifier l'identité d'un utilisateur grâce à un couple login / mot de passe, d'autre part, en offrant des modes d'accès sécurisés (HTTPs, POPs, IMAPs, …). Nous avons décidé de mettre en place l'élément manquant dans notre architecture : **un service d'authentification unique basé sur un annuaire LDAP** cohérent avec les bases de comptes informatiques gérées par chacune des unités de recherche.

En complément du service d'authentification LDAP, nous avons décidé **d'étudier, puis de déployer une architecture d'accès VPN.**

Mieux protéger les données sur les portables

Les données enregistrées sur les disques durs des ordinateurs sont le patrimoine de l'établissement. Un vol, une destruction pouvant être très dommageable, nous avons mené 2 actions pour mieux les protéger.

En hypothèse de départ, nous avons considéré que les machines connectées sur un site principal étaient dans un domaine de confiance. Par contre, les ordinateurs portables physiquement hors des murs, connectés sur un réseau extérieur, sont plus exposés à des risques de piratage ou de vol : pas de garantie de protection d'entrée de site comme sur un site INRIA ; risque accru de vol et de piratage des données du disque interne.

Au delà de certaines recommandations de sécurité à l'attention des utilisateurs de portable (anti-virus actif et à jour ; mises à jour et applications automatiques de patches de sécurité), nous avons décidé de mettre l'accent sur le **chiffrement des données enregistrées sur le disque dur** de la machine, et sur **les systèmes de protection pare-feux.**

3 L'organisation du projet VISON

Dans le contexte d'administration répartie des ressources informatiques entre les 6 services informatiques des unités de recherche, nous avons mis en place une organisation transversale à 3 niveaux:

- **un comité de pilotage** représentant la direction de l'institut, chargé d'orienter les axes de travail, de valider les choix techniques et résultats. Ce comité se réunit 3 fois par an ;
- **un comité opérationnel** regroupant les responsables des services informatiques, le responsable du projet VISON, le directeur des réseaux et systèmes d'informations. Ce comité a pour but de coordonner et d'animer le travail d'étude et de réalisation, de soumettre les choix et résultats au comité de pilotage pour validation ;
- des **groupes de travail** pour réaliser des études ou des maquettes, et des **équipes transversales** pour opérer un service national. Pour chaque groupe ou équipe, une lettre de mission est donnée. Elle précise le contexte, les objectifs, les livrables attendus et le planning. Dans le contexte réparti d'administration informatique de l'INRIA, un groupe ou une équipe regroupe des ingénieurs de plusieurs services informatiques des unités de recherche.

Cette organisation a permis de mener à bien les 4 actions détaillées plus loin.

4 Service d'authentification

L'objectif d'un service d'authentification (appelé iLDAP) est de répondre à la question : « L'utilisateur est-il bien celui qu'il prétend être ? ». Le déploiement d'un tel service à l'échelle de l'INRIA passe par la mise en place d'un dispositif fédérateur de gestion qui assure la visibilité et la cohérence des identifiants pour toute application ou toute ressource INRIA devant vérifier l'identité de l'utilisateur.

La technologie LDAP a été retenue sur les critères suivants :

- Compétences techniques existantes en interne sur cette technologie,
- Nombre de services d'authentification s'interfaçant en standard à LDAP,

– Potentialité d'évolutivité et d'opérabilité à terme avec un service SSO.

La mise en place d'un tel dispositif fédérateur nécessite des réflexions sur l'infrastructure logicielle et matérielle qui se doit d'être robuste et fiable, sur la structuration et l'organisation des données (et plus particulièrement leur cohérence) qui sont alimentées par plusieurs sources (bases des comptes informatiques de chaque unité de recherche).

Janvier 2003, 2 groupes de travail sont constitués, l'un travaillant sur l'infrastructure logicielle et matérielle, l'autre sur la structuration et l'organisation des données. 11 ingénieurs des différents sites de l'INRIA ont participé, pour partie de leur temps (1,3 équivalent temps plein), sur une période de 10 mois (janvier à octobre 2003).

Les résultats des 2 groupes ont consisté en un rapport incluant des préconisations et une maquette du service. Les caractéristiques principales sont :

– OpenLDAP jugé suffisant pour un annuaire comportant moins de 4000 entrées ;
– une architecture de service composée de 7 serveurs (un maître et 6 esclaves répartis sur les sites des unités de recherche) qui assure un bon niveau de robustesse et de fiabilité ;
– une première version d'un schéma d'annuaire et des règles de gestion des identifiants pour garantir la cohérence dans un modèle d'alimentation des données distribué.

Pour mener à bien cette étude, les groupes de travail se sont appuyés sur les travaux et recommandations de l'ADAE (Agence pour le Développement de l'Administration Electronique) et du groupe de travail SUPANN (annuaires dans l'enseignement supérieur**).**

Novembre 2003, suite au feu vert du comité de pilotage, une équipe transversale de 9 ingénieurs de différents sites pour partie de leur temps (1 équivalent temps plein) a été constituée pour mettre en place le service d'authentification de l'INRIA suivant les préconisations des groupes de travail.

Plusieurs tâches ont été réalisées pour le déploiement :

– mise en place de l'architecture de 7 serveurs (coût d'investissement : 28 K€ HT). Chaque serveur tourne sous la distribution GNU/Linux propre à chaque site ;
– mise au point dans chaque unité de recherche des procédures d'alimentation cohérentes avec la gestion des bases de comptes informatiques ;
– travail de dé-doublonnage pour garantir une seule entrée par utilisateur : utilisateurs ayant des comptes sur plusieurs sites, homonymies ;
– scripts de vérification de la cohérence des données ;
– sécurisation des échanges entre les serveurs ;
– documentations techniques et transfert de compétences auprès des services informatiques des unités de recherche pour appropriation comme un service de base administré par leurs soins ;
– accompagnement des gestionnaires de services WEB et Sympa à la mise en place de l'authentification iLDAP (documentation technique et assistance).

Le service d'authentification a été officiellement déclaré ouvert en octobre 2004. Il est désormais interfacé par plusieurs types d'applications : serveurs WEB internes, Sympa, News, authentification VPN, et quelques applications du système d'information.

Les sous-sections suivantes présentent l'état actuel de la structuration et l'organisation des données, de l'infrastructure logicielle et matérielle, et enfin les évolutions envisagées.

4.1 Les données

Actuellement, les 3 identifiants principaux sont :

– **l'identifiant global utilisateur (GUID)** servant de clé interne pour nos outils de gestion des comptes iLDAP ;
– **l'identifiant institutionnel utilisateur** servant de "logname" de connexion pour les applications qui s'authentifieront auprès de l'annuaire iLDAP ;
– **l'identifiant VPN utilisateur** sert de "logname" pour le service VPN ;

En complément à ces identifiants, qui permettent de s'authentifier, l'annuaire LDAP contient d'autres attributs qui apportent des fonctionnalités supplémentaires : adresses électroniques, groupes d'appartenances. Ci-après, la structure des informations d'un "objet" personne est organisée comme attribut ayant un type et une valeur.

dn:	uid=[guid],ou=people,dc=inria,dc=fr
objectclass:	top
objectclass:	person
objectclass:	organizationalPerson
objectclass:	inetOrgPerson
objectclass:	inriaPerson
uid:	[guid]
inriaLogin:	[login ou GUID si login existe déjà]
inriaLocalLogin:	[login]
inriaVPNLogin:	[login@domaine_dns_UR]
sn:	[NOM(s)]
givenname:	[Prenom(s)]
cn:	[NOM Prenom]
mail:	[Prenom.Nom@suffix_mail_UR]
userpassword:	[{crypt}xxxxxxx]
ou:	[domaine_UR]
employeeType:	[{nis},{manual}]
inriaGroupMemberOf: [cn=GROUPEprefixUR],ou=groups,dc=inria,dc=fr	
owner:	[DN(s) personne ou groupe]
inriavalidate:	[{0},{1}]

La préoccupation majeure est d'assurer la cohérence des identifiants pour toute application ou tout service INRIA

devant vérifier l'identité de l'utilisateur. Les principes suivants pour les identifiants doivent être vérifiés :

- la pérennité et non réutilisation d'un identifiant pour garantir de référencer toujours la même personne quelles que soient ses affectations dans le temps : changement de responsabilité, mobilité interne INRIA, départs, retours, changement d'état civil…
- l'unicité d'un identifiant pour garantir de pointer sur une seule et même personne ;
- l'attribution des identifiants est faite par chaque service informatique des 6 unités de recherche INRIA. Dans cette phase de démarrage, nous nous appuyons sur les bases de comptes informatiques (toute personne travaillant pour l'INRIA a un compte dans une des 6 unités de recherche, qu'il soit ou non dans une unité de recherche).

Pour garantir ces principes, plusieurs règles ont été définies et adoptées :

- définition et adoption d'une nomenclature de construction des identifiants pour éviter les conflits potentiels de nommage. Exemples : l'identifiant institutionnel = première lettre du prénom, 7 premières lettres du nom, identifiant global = première lettre du prénom, 4 premières lettres du nom suivies d'un numéro d'ordre ;
- création automatique d'une entrée dans l'annuaire LDAP à chaque ouverture d'un compte informatique dans un des bases de comptes. Cette opération s'accompagne de vérifications comme « l'utilisateur a-t-il déjà une entrée dans l'annuaire ? » (un utilisateur peut avoir des comptes dans plusieurs sites) ;
- conservation de l'entrée dans l'annuaire en cas de fermeture de compte informatique. Ceci nous permet de garantir l'unicité et la non réattribution du GUID, l'identifiant institutionnel pouvant être réattribué.

Ces règles n'évitent cependant pas tous les conflits ou interrogations : homonymie (moins d'une dizaine sur 4000 entrées), changement de site ou ouverture d'un compte dans un autre site (dans ce cas, il n'y a pas création d'une nouvelle entrée) … La résolution de ces situations passe par une concertation entre les gestionnaires des données de chaque unité de recherche.

4.2 L'infrastructure du service

L'infrastructure du service d'authentification LDAP est constituée de 7 serveurs PC de configuration identique (bipro 3.06Ghz, 2 disques 36 Gigas, 1GB RAM) avec un système de type GNU/Linux. Ces machines ont des caractéristiques techniques censées assurer une haute disponibilité (double alimentation, disques amovibles à chaud en configuration RAID 1) nécessaire pour un service jugé comme critique.

Le logiciel utilisé est OpenLDAP en version 2. Il est configuré pour fonctionner dans une zone sécurisée du système (chroot) et dialoguer avec les autres serveurs et les clients sous forme chiffrée (SSL/TLS).

L'architecture est composée d'un serveur maître (hébergé à Rennes) et de 6 serveurs esclaves. Le maître reçoit les mises à jour des données transmises par chaque unité de recherche à partir des modifications de leurs bases locales des comptes informatiques. Ces mises à jour sont alors dupliquées en temps réel sur l'ensemble des **serveurs esclaves** répartis dans chacune des unités de recherche.

Les applications, quant à elles, s'adressent uniquement à un serveur esclave pour l'authentification, et en aucun cas au maître afin de limiter les risques de corruption.

Par ailleurs, pour mieux fiabiliser le service, des procédures de « crash recovery » ont été mises au point et testées : reconstruction d'un serveur (maître ou esclave), basculement sur un autre serveur.

4.3 Les évolutions

Plusieurs pistes de réflexion sont en cours sur les évolutions et usages possibles de cette infrastructure :

- une réflexion est en cours sur l'utilisation d'un SSO (Single Sign On) à l'INRIA. L'annuaire LDAP sera alors une brique essentielle de cette architecture ;
- l'authentification sur les postes de travail Unix repose actuellement sur le service NIS. Une étude est en cours pour utiliser les modules PAM pour s'interfacer avec le service d'authentification ;
- certaines applications utilisent LDAP pour gérer les profils utilisateurs (l'agenda partagé Oracle Calendar par exemple). Nous nous appuierons sur l'infrastructure actuelle pour créer et utiliser d'autres instances annuaires synchronisées à l'annuaire d'authentification ;
- nous envisageons de mettre en place une IGC (Infrastructure de Gestion de Clés). Les certificats utilisateurs seront stockés dans l'annuaire ;
- au delà de la simple authentification, l'annuaire iLDAP devra permettre de constituer des habilitations d'accès au service sur des critères tels que l'appartenance à un groupe, le statut ou la fonction de la personne. Ces caractéristiques seront fournies par différentes sources dont la principale sera le système d'information de l'INRIA.

A terme, c'est une infrastructure de type Meta Annuaire qui sera disponible à l'INRIA : un point d'entrée unique sous LDAP consolidant des données synchronisées depuis plusieurs référentiels selon des règles, et les distribuant aux applications concernées.

5 Virtual Private Network

L'objectif de cette action est de mettre en place une solution générique d'accès sécurisé et authentifié aux

ressources internes de l'INRIA depuis une machine vers une unité de recherche.

Pourquoi une technologie VPN ?

- Certains services ou applications n'ont pas de mécanisme de contrôle d'accès par authentification utilisateur. Ce contrôle est alors déplacé sur le niveau session par habilitation IP.
- Les technologies VPN permettent l'ouverture d'une connexion authentifiée et chiffrée. Vu de l'utilisateur et dans un contexte multi applicatif (Web, relais Mail, espaces partagés…), le VPN est plus simple à mettre en place comparé à une session SSH (applications locales et pas distantes, pas de modification des paramètres des applications…).

Janvier 2003, un groupe de travail est constitué : 11 ingénieurs des différents sites de l'INRIA pour partie de leur temps (estimation : 1,3 équivalent temps plein) sur une période de 9 mois.

Les résultats du groupe ont consisté en un rapport incluant des préconisations, des résultats de béta-tests utilisateurs, et une maquette de service. Les caractéristiques principales sont :

- une architecture redondante avec 2 routeurs (Rocquencourt et Nancy), des serveurs Radius dans chaque site pour l'authentification, des tunnels GRE entre les sites ;
- des clients développés par l'INRIA pour Windows et Linux.

Aucune acquisition n'a été faite lors de cette phase ; la maquette ayant été réalisée avec un routeur CISCO disponible et une solution logicielle sur Linux. Les résultats de cette première étude ont fait l'objet d'une présentation aux JRES2003 [1].

Novembre 2003, le comité de pilotage donne son feu vert pour déployer un service VPN. Une équipe transversale de 8 ingénieurs pour partie de leur temps (0,9 équivalent temps plein) des différents sites est constituée pour mettre en place le service VPN de l'INRIA. Le service a été ouvert officiellement en juin 2004 avec les clients INRIA.

Les tests menés sur la maquette nous ont orienté vers une architecture VPN nomade définitive reposant sur du matériel Cisco :

- plus grande facilité de mise en oeuvre et de maintenance,
- possibilités de gestion mutualisée des accès dans une configuration à deux serveurs redondants,
- utilisation des clients développés par Cisco permettant de s'affranchir du développement de clients INRIA et de couvrir l'architecture cliente MacOS.

Des études complémentaires et des béta-tests ont permis de valider ces possibilités. En décembre 2004, l'architecture complète est passée en client Cisco. Un investissement de 2 routeurs Cisco a été nécessaire (~22 K€ HT).

5.1 Le service VPN actuel

L'architecture actuellement en service (Figure 2) diffère peu de la maquette de service présentée aux JRES2003 [1]. Comme l'illustre la figure 2, elle est constituée de 2 routeurs VPN CISCO redondants, de serveurs Radius dans chacun des sites pour l'authentification utilisateur (ce qui permet une gestion distribuée des utilisateurs) et de tunnels GRE entre les routeurs VPN et les routeurs d'entrée de chaque unité de recherche.

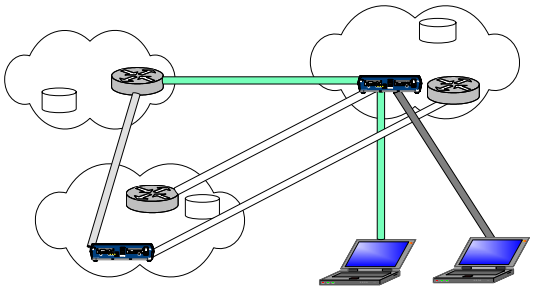


Figure 2 - Architecture du service VPN

Les évolutions principales ont porté sur le mode d'authentification et sur les clients. Lors de la mise en place de la première maquette, le client VPN (développé par l'INRIA) s'appuyait sur un mode de transfert et d'authentification L2TP / ISAKMP / IPsec. La raison principale de ce choix tenait à la fonctionnalité d'authentification utilisateur présente dans L2TP, mais inconnue dans le standard ISAKMP / IPsec. L'authentification utilisateur par login/password était indispensable (par opposition, par exemple, à une authentification par adresse IP), car l'architecture VPN envisagée visait en priorité les utilisateurs nomades disposant d'un accès quelconque au réseau Internet. L'architecture étudiée par la suite, reposant sur des clients VPN Cisco, intégrait un mécanisme d'authentification utilisateur dans ISAKMP appelé Xauth. Ce mécanisme ne fait pas partie du standard ISAKMP en raison de problèmes de sécurité explicités notamment lors de nos travaux [3]. L'évolution de L2TP / ISAKMP / IPsec vers ISAKMP / IPsec seuls (Xauth est inclus dans ISAKMP) est survenue parallèlement à la décision d'orienter notre architecture vers des clients VPN Cisco.

Les clients VPN développés par l'INRIA étaient disponibles pour des plates-formes Windows et Linux. La difficulté de maintenir et de faire évoluer ces clients logiciels s'est peu à peu révélée trop lourde pour le groupe de travail. Force est de constater que seul le client VPN Windows a réellement été exploité par les utilisateurs lors de cette période. Le choix du groupe de travail s'est finalement porté sur les clients logiciels VPN Cisco, régulièrement mis à jour et disponibles sur les plates-formes système d'exploitation couramment utilisées à l'INRIA (Windows, Linux et MacOS).

5.2 La gestion du service

La gestion du service est assurée par une équipe transversale aux unités de recherche.

L'accès administratif par les membres de l'équipe transversale aux deux serveurs VPN est réalisé en SSH à partir d'une machine dédiée sur chacun des deux sites. Un outil de gestion de configuration est utilisé.

Des statistiques sont effectuées tous les mois à partir des fichiers comptables de Radius et sont publiées. Elles fournissent le nombre d'utilisateurs, le nombre et les temps de connexion. MRTG permet de suivre la CPU, la mémoire, le nombre de tunnels IPSEC, le trafic. Nagios permet de vérifier le bon fonctionnement des serveurs Radius et la présence des serveurs VPN.

Préalablement au déploiement du service VPN définitif, une enquête a été réalisée auprès des utilisateurs de la maquette pour déterminer la portée et les moyens à accorder au service VPN pour nomades. Les résultats ont permis de définir deux profils de connexion :

- INTRANET_INRIA : les accès à l'intranet de chaque unité de recherche et à des serveurs non INRIA déclarés (exemple de serveurs de documentation scientifique autorisant une adresse IP INRIA) transitent par le VPN. Les accès aux autres ressources se font par le réseau local de connexion. C'est le profil par défaut ;
- VPN_TOTAL : tous les accès (route par défaut), sauf l'accès au réseau local, transitent par le VPN. Ce profil permet d'accéder toute ressource (interne ou externe) dont l'accès est autorisé depuis le domaine d'adressage IP du VPN INRIA.

La gestion a été la plus distribuée possible : chaque unité de recherche choisit et gère ses profils de groupe et les listes d'accès associées, ses comptes utilisateurs (implicites ou sur demande) et son serveur Radius. De même, les accords d'ouvertures des filtres sur les sites distants sont réalisés par chaque unité de recherche.

Une répartition des unités de recherche a été faite entre les deux serveurs ; les profils permettent de basculer automatiquement sur l'autre serveur en cas de non réponse.

Une documentation centralisée détaillant le service a été mise en place, afin de guider les utilisateurs et les membres de l'équipe d'exploitation.

Une cause fréquente de non fonctionnement du service VPN est le filtrage sur le réseau d'accueil du protocole ESP (data gramme IP de type 50) et du port UDP/500 (protocole ISAKMP). Nous n'avons pas aujourd'hui de solution de contournement, mais des techniques comme VPN-SSL/TLS sont à l'étude.

La remontée des problèmes se fait d'abord au niveau du support de chaque unité de recherche, puis en second recours, vers l'équipe transversale.

5.3 Utilisation du service VPN INRIA

Quelques chiffres d'utilisation pour septembre 2005 :

- 445 utilisateurs ont utilisé au moins une fois le service,
- 5306 connexions au service VPN pour un temps cumulé de 12474 heures.

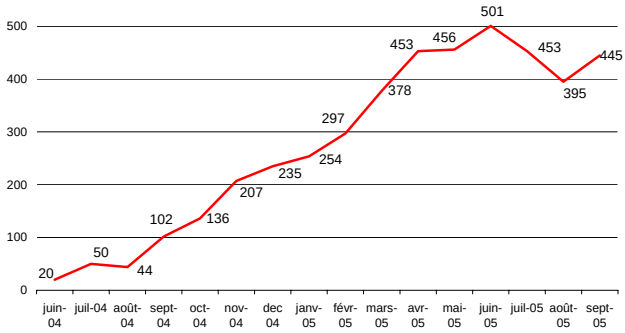


Figure 3 – Utilisateurs du service VPN

5.4 Les évolutions du service VPN

Une prochaine évolution du mode d'authentification des clients VPN Cisco est attendue afin de renforcer la sécurité de l'architecture. Les signatures RSA seront utilisées pour l'authentification des serveurs VPN et des clients. La gestion des certificats associés ne reposera pas sur une IGC complexe, puisqu'un certificat générique peut être assigné à l'ensemble des clients VPN.

De nouvelles applications, s'appuyant sur le service VPN sont à l'étude :

- utilisation du VPN pour l'accès au réseau WIFI : c'est actuellement le cas depuis les réseaux « invités » des différentes unités de recherche, d'autres utilisations restent envisageables ;
- la ToIP sur VPN : un service de téléphonie sur Internet pour utilisateurs nomades reposant sur VPN est actuellement testé. L'objectif est d'assurer la confidentialité de la communication (les logiciels de ToIP n'offrent à ce jour pas de fonction de chiffrement satisfaisante) et de pouvoir traverser les pare-feux (les protocoles standards sont SIP pour la signalisation, et RTP pour le transport de la voix. Le numéro de port UDP utilisé pour RTP est dynamique, et négocié lors de la signalisation SIP. Tout le trafic voix serait filtré par, entre autres, le pare-feu de l'INRIA si VPN n'était pas utilisé pour le transport).

Outre les applications envisagées pour une intégration au service VPN, certains thèmes étroitement liés à celui-ci font l'objet d'une attention particulière, et d'une éventuelle évolution du service.

Ainsi, la technique VPN-SSL/TLS, en retrait par rapport à IPsec à l'époque de la mise en place de la maquette

initiale, est actuellement étudiée et comparée à la technique VPN-IPsec que nous utilisons à ce jour.

Par ailleurs, d'autres produits Cisco (gamme VPN3000) permettent d'imposer un niveau de sécurité aux clients VPN (anti- virus, pare feu, …). Nous étudions l'évolution de ces produits et l'intégration de certaines de ces fonctionnalités dans notre solution actuelle (IOS) de manière à déterminer si une évolution vers d'autres types de serveurs VPN doit être envisagée puisque nous sommes dépendants des choix réalisés par Cisco (exemple : la non intégration de l'IPsec sur TCP dans l'IOS).

6 Chiffrement des données

Les données enregistrées sur les disques durs des ordinateurs font partie du patrimoine de l'établissement. Pour mieux les protéger, limiter les risques de piratage ou de vol, nous avons décidé de mener une action sur le chiffrement des données enregistrées sur les portables.

Une première étude technique est lancée en octobre 2003. Un groupe de travail de 9 ingénieurs (1 équivalent temps plein) s'est consacré à l'étude des outils de chiffrement des données sur les ordinateurs portables Windows, Linux et MacOS, pendant 1 an. Le groupe de travail a fourni un rapport incluant :

- une grille d'analyse des outils de chiffrement classés en deux grandes catégories confidentialité et coffre-fort,
- des résultats de béta-tests bien que peu de volontaires se soient manifestés,
- des recommandations d'outils pour les architectures Windows, Linux et MacOS,
- des préconisations en vue d'un déploiement (séquestre des clés).

Le comité de pilotage du projet VISON a approuvé les recommandations d'outils du groupe de travail. Il a par ailleurs estimé que ce premier travail devait être complété avant de décider d'un déploiement par la définition d'une politique de l'institut (usages recommandés, obligations de l'établissement) et par l'organisation du séquestre des clés.

Un second groupe de travail a été constitué regroupant des juristes, des chercheurs ayant manipulés des données sensibles, des représentants des relations industrielles de l'INRIA, … Les travaux de ce groupe ont débuté en février 2005, et ont fait l'objet d'un rapport et de propositions en juin 2005 :

- définition de catégorie de données et recommandations associées,
- mise en place d'un séquestre de clés, et définition des règles de dépôt et de recouvrement associées,
- amendements nécessaires à la charte informatique.

Les propositions de ce groupe de travail devront faire l'objet d'un débat et de décisions en comité de direction INRIA à l'automne avant de passer à une éventuelle phase de déploiement et d'information.

6.1 Recommandations techniques

Le groupe de travail technique a donné en conclusion des recommandations d'outils :

- EFS pour Windows XP,
- CryptoAPI pour Fedora Core 2,
- Loop-AES pour Mandrake 8.2, 9.1 et 9.2,
- GnuPG pour Linux ou MacOS

Ces recommandations datent de près d'un an. Si le suivi des évolutions de ces outils ne remet pas en cause ces recommandations, il nous apparaît plus important de présenter dans la présente publication la démarche et les principaux points à vérifier avant de recommander un outil.

La première étape est de définir les catégories d'outils de chiffrement ; les critères de choix et les études du produit à mener diffèrent d'une catégorie à l'autre. A l'INRIA, nous avons retenu deux catégories :

- **Catégorie confidentialité**. Le risque contre lequel il faut se prémunir est un accès trop facile aux données. Un outil de chiffrement résistant à tout type d'attaque connu n'est pas visé : l'essentiel de ces données finira par être public ou verra sa sensibilité décroître dans le temps. Les critères principaux à retenir sont l'ergonomie, la transparence et la facilité d'utilisation, la facilité de déploiement, l'interfaçage avec les outils de sauvegardes de données, le recouvrement par l'utilisateur de sa clé personnelle. L'excès attendu est une utilisation « tout venant » d'où une quantité de données chiffrées importante. Un critère supplémentaire peut être la rapidité de chiffrement/déchiffrement ;
- **Catégorie coffre-fort**. Il s'agit ici de protéger des données très sensibles et probablement peu nombreuses, mais dont la divulgation causerait un préjudice important. Les critères deviennent dans ce cas la robustesse, l'utilisation explicite, le séquestre de clé. De telles données étant peu nombreuses, le nombre d'accès limité, la rapidité de chiffrement/déchiffrement n'est plus une contrainte.

Détaillons un peu les critères mentionnés ci-dessus liés à chaque catégorie :

- ergonomie : importante pour susciter l'utilisation et donc la sécurisation des données ;
- transparence d'utilisation : nombre d'outils demandent de déchiffrer le fichier avant utilisation, et de re-chiffrer après utilisation. Un oubli : le fichier n'est plus protégé ;
- facilité de déploiement et d'utilisation : la non popularité des outils de chiffrement tient pour beaucoup aux difficultés d'utilisation et déploiement ;
- interfaçage avec les outils de sauvegarde : la sauvegarde des données sous forme chiffrée ne doit pas engendrer d'autres contraintes : coûts, modification du

fonctionnement, reconfiguration. Bon nombre d'outils utilisent un fichier conteneur pour stocker les fichiers chiffrés, fichier modifié à chaque accès. Une sauvegarde incrémentale ne présente donc plus d'intérêt ;

- recouvrement des clés de chiffrement (ou système de séquestre de clés) pour permettre à un agent de recouvrement (autorité de séquestre) de déchiffrer les données des utilisateurs en cas de besoin (perte de clé, départ, décès, ...) ;
- robustesse : au sens cryptographique, par l'implémentation d'algorithmes éprouvés, reconnus robustes, avec des tailles de clé assez grandes. Nous avons retenu en priorité les algorithmes Mars, RC6, Rijndael, Serpent, Twofish (finalistes du concours AES (Advanced Encryption Standard) organisé par le NIST (National Institute for Standards and Tecnology) dans le but de remplacer DES), et en second choix, les algorithmes 3DES, DESX, RC5, RC4, RC2, IDEA, DFC, Twofish, Blowfish, RSA et DSA. L'ensemble de ces algorithmes ne nécessite pas de déclaration supplémentaire auprès de la DCSSI;
- utilisation explicite : choisir, prendre conscience d'une mise au coffre, être prêt à réaliser des manipulations simples comme « fournir le code d'accès au coffre » ;

D'autres critères doivent être pris en considération dans le choix d'un outil de chiffrement :

- chiffrement des fichiers temporaires et du swap,
- utilisation de la mise en veille prolongée,
- gestion de clés de chiffrement,
- impact et liens entre mot de passe de session et pass-phrase de chiffrement,
- stockage de clés sur un support physique,
- état des données suite à un plantage de la machine,
- taille du fichier conteneur et performance,
- protection au démarrage du système d'exploitation,

Il est important d'étudier ces critères pour retenir et recommander un outil. L'objectif étant de faire accepter l'outil par l'utilisateur pour une meilleure sécurité des données de l'établissement. Il faut se garantir d'une non dégradation des performances, et de l'absence de failles de sécurité (un faux sentiment de sécurité chez l'utilisateur pouvant s'avérer plus néfaste).

6.2 Politique de chiffrement

En complément d'une étude technique sur les outils de chiffrement, nous avons mené une réflexion pour la définition d'une politique pour le chiffrement des données. Cette réflexion a porté essentiellement sur 3 axes :

- obligations légales et juridiques à respecter entre l'établissement et les agents, l'établissement et des tiers,
- recommandations et/ou des règles internes sur l'usage des outils par catégorie de données,
- organisation et règles du séquestre des clés.

Obligations légales et juridiques

Les agents ont une obligation de loyauté à l'égard de l'établissement, qui leur impose de communiquer sur demande de l'établissement, tout document professionnel nécessaire à la réalisation des missions de l'établissement. Cette obligation est renforcée en cas d'absence, départ de l'agent, et implique un séquestre des clés.

Les informations contenues dans les fichiers informatiques et courriels sont produites dans le cadre d'une relation de travail. Doivent alors être conciliés les principes de subordination entre l'employeur et l'agent et le droit au respect des libertés individuelles et collectives. Cette conciliation est mise en œuvre par trois principes :

- les limitations apportées aux libertés individuelles sont nécessaires pour remplir les finalités légitimes et reconnues de l'établissement : **principe de nécessité** ;
- les limitations apportées sont proportionnelles au but recherché : **principe de proportionnalité**. Ce principe oblige l'établissement à respecter le droit à la vie privée des agents, même sur leur lieu de travail ;
- les mesures limitatives font l'objet d'une négociation collective et d'une information préalable des agents : **principe de transparence**.

Les données

Certaines données sont protégées par un droit de propriété intellectuelle (droit d'auteur, titre de propriété industriel, droit *sui generis* sur les bases de données). Ce droit ou ce titre permet à son titulaire (agent ou établissement) de s'approprier l'information qui devient un bien meuble incorporel. Deux types de données sont à discerner :

- **donnée sensible** : donnée protégée ou non par un droit ou un titre, qui revêt un caractère secret ou confidentiel à raison d'un accord, d'un usage professionnel ou de la réglementation applicable ;
- **donnée ultra sensible** : donnée sensible dont la nécessité de protection par la confidentialité ou le secret a été spécifiée par un tiers ;
- D'autres données (la plupart) ne sont pas protégées et donc non appréhendées par le droit en tant qu'objet d'appropriation. Elles sont dans le « domaine public ».

L'établissement doit protéger les données sensibles dont il est le dépositaire ou l'initiateur, veiller au respect des droits de propriété intellectuelle des tiers, au respect des obligations de confidentialité et de secret souscrites. Pour ce faire, l'établissement peut recommander le cryptage des données sensibles et ultra sensibles (principe de nécessité).

Catégories de données et recommandations associées

De l'analyse ci-dessus découle 4 catégories de données pour lesquelles, le groupe de travail a proposé les recommandations suivantes :

- **données de la sphère « privée »** : aucune recommandation n'est faite, si ce n'est une identification claire ;

– **données sensibles** : recommandation de ne pas les stocker sur un portable. En cas de nécessité de les stocker sur un portable, recommandation d'utiliser un outil de chiffrement de classe « confidentiel » ;
– **données ultra sensibles** : recommandation de ne pas les stocker sur un portable. En cas de nécessité de les stocker sur un portable, recommandation d'utiliser un outil de chiffrement de classe « coffre-fort » ;
– **données non sensibles** pour lesquelles aucune recommandation de chiffrement n'est faite.

Séquestre des clés

Notre réflexion nous a mené à proposer de mettre en place un séquestre, et des règles de dépôt et de recouvrement :

– **dépôt** : laissé à l'initiative de l'utilisateur qui dépose sa clé et le logiciel utilisé,
– **recouvrement par l'utilisateur** : procédure souple mais en s'assurant de l'identité du demandeur,
– **recouvrement pour un tiers de l'établissement** : procédure exceptionnelle (longue absence, décès) à entourer de précautions : ne pas remettre des données de la sphère privée, vérifier l'habilitation du demandeur (lien hiérarchique par exemple),
– **recouvrement pour un tiers hors établissement** : procédure très exceptionnelle (action de justice) en veillant à vérifier la légitimité de la demande.

Idéalement, ce séquestre doit être placé sous la responsabilité des moyens informatiques ou du réseau RSSI de l'établissement.

Autres recommandations

Cette réflexion a mené à compléter les propositions ci-dessus par des recommandations aux utilisateurs pour :

– le choix du logiciel de chiffrement qui, comme souligné précédemment, est délicat ;
– la mémorisation des mots de passe sur un portable (qu'il convient de limiter) et leur sécurisation [2].
– la protection physique des portables contre le vol ou la destruction,
– l'avertissement en cas de vol ou de destruction du portable.

6.3 Les évolutions

Les propositions présentées ci-dessus sont soumises à l'approbation de la direction générale de l'INRIA. En cas de suite favorable, la mise en application nécessitera :

– des amendements à la charte informatique de l'institut pour prendre en compte les outils de chiffrement, le séquestre de clé et logiciel, et mieux définir l'usage des moyens informatiques à des fins privées,
– une négociation collective, une information et une sensibilisation préalable aux agents,
– l'organisation du séquestre de clés et logiciel.

Enfin, il sera nécessaire de continuer la veille technologique sur les outils de chiffrement pour réactualiser régulièrement les recommandations d'outils.

7 Pare-feux sur portables

L'objectif était d'étudier et de documenter les pare-feux natifs sur Windows et Linux, pour mieux en connaître les possibilités d'utilisation et de protection dans un cadre de nomadisme. Nous nous sommes limités à l'étude des pare-feux natifs : pas de déploiement, pas de surcoût, étude confiée à un ingénieur pour partie de son temps.

Le cas des ordinateurs portables est particulier car ils peuvent être connectés à des réseaux sur lesquels les risques encourus sont variables. Le pare-feu étudié doit donc être capable de répondre aux deux critères suivants :

– lorsque le portable est connecté au réseau de son site, le pare-feu doit offrir une bonne protection contre les attaques réseaux et autoriser les opérations habituelles de sauvegarde et d'administration ;
– lorsque le portable se trouve dans un autre réseau, la protection doit être maximale.

Cette étude a débutée en mars 2004 avec les premières recommandations et documentations d'utilisation et un premier transfert de compétences en interne en septembre 2004. Cette étude s'est poursuivie pour y intégrer Windows XP SP2.

7.1 Windows XP

La première étude a porté sur le pare-feu de Windows XP SP1, et s'est poursuivie sur Windows XP SP2. Seuls les résultats pour Windows XP SP2 sont présentés ici.

Le pare-feu de Windows XP SP2 est dérivé de celui de XP SP1 (lorsque le pare-feu est activé, tous les paquets entrants non sollicités sont rejetés). Il apporte des améliorations importantes comme l'utilisation de deux jeux de configurations (portable dans le réseau interne (profil « domaine ») ou à l'extérieur (profil « standard »)), ou la création d'une configuration répondant aux deux critères attendus.

La configuration proposée comprend :

– un profil « domaine » qui permet, en particulier, les sauvegardes, l'administration à distance, l'utilisation de XWin32,
– un profil « standard » qui bloque tout le trafic entrant non sollicité.

Si l'utilisateur est administrateur sur sa machine, il peut ajuster les règles selon ses besoins (mais sans pouvoir supprimer les règles de la configuration proposée).

Les actions entreprises pour le déploiement sont :

– diffusion par stratégie de groupe des deux profils de configuration,

– rédaction d'une documentation utilisateur expliquant comment adapter la configuration proposée.

7.2 Linux

Le pare-feu de Linux est basé sur les composants netfilter/iptables qui sont généralement utilisés sur des passerelles. Ses possibilités de configuration sont donc importantes et peuvent être mises en œuvre pour correspondre aux critères attendus.

La configuration proposée utilise des scripts exécutés lorsqu'une interface réseau est activée ou désactivée. Ceci permet une reconfiguration dynamique des règles de filtrage dont les principales caractéristiques sont :

– les paquets sortants ne sont pas filtrés ;
– les paquets entrants non sollicités sont rejetés sauf pour les exceptions définies selon le réseau utilisé ;
– dans le réseau du site : l'administration à partir d'un serveur dédié, les sauvegardes, l'utilisation de X11 et l'accès SSH sont autorisés ;
– dans les autres cas (y compris VPN) : seul l'utilisation de X11 et l'accès SSH sont autorisés.

Si l'utilisateur a accès au compte root de son portable, il peut modifier la configuration selon ses besoins.

Afin de déployer le pare-feu, plusieurs actions ont été entreprises :

– installation par défaut sur les nouveaux portables;
– création et diffusion d'un paquet RPM pour Fedora Core destiné aux portables plus anciens ;
– rédaction d'une documentation utilisateur expliquant comment adapter la configuration proposée.

7.3 Conclusion

L'usage des pare-feux est en cours de déploiement au sein de l'INRIA. A la suite des premiers retours, cette première étude pourra être complétée, si jugée nécessaire, avec d'autres outils non natifs.

8 Bilan et perspectives

Le projet VISON a permis à l'INRIA de faire un pas significatif vers « *L'INRIA pour tous, depuis partout et à tout moment* » en

– rendant plus transparente la localisation géographique des utilisateurs,
– facilitant le nomadisme sous toutes ses formes,
– s'ouvrant tout en sécurisant et authentifiant les accès.

Les évolutions techniques majeures ont été de progresser :

– d'une sécurisation basée essentiellement sur les @ IP des machines vers une sécurisation basée sur une authentification utilisateur INRIA.
– de rendre les ressources essentiellement accessibles à l'INRIA, accessibles depuis le monde entier.

Le projet VISON a duré 26 mois au total. Les coûts d'investissements (50 K€ globalement) sont modestes par rapport aux enjeux du projet. L'investissement humain a été le plus conséquent :

– une implication de membres de la direction de l'institut dans le comité de pilotage,
– une implication des chefs des services informatiques dans le comité opérationnel,
– une mobilisation d'ingénieurs de différents sites dans les groupes de travail et équipes transversales : 50 participations (estimées à 7 équivalents temps plein) réparties dans les services des moyens informatiques des 6 unités de recherche.

Au delà des avancées techniques, le projet a créé une véritable dynamique transversale, et est un élément fédérateur fort pour l'institut.

Le projet VISON est arrivé à son terme et a été clos en mai 2005. Les services mutualisés entre les unités de recherche sont pérennes et administrés par les services informatiques. Quant aux travaux de chiffrement des données sur les portables, ils seront menés à bien par le comité de concertation des moyens informatiques de l'INRIA.

Dans la continuité du projet VISON, de nouvelles actions sont ou seront lancées pour compléter notre infrastructure d'accès sécurisé et authentifié, pour proposer d'autres solutions techniques pour protéger les portables :

– authentification par certificats numériques, SSO,
– meilleure prise en compte des réseaux non filaires,
– environnements de travail coopératif,
– détection de vulnérabilités sur les portables.

Remerciements

Je tiens à remercier toutes les personnes impliquées dans le projet VISON, et particulièrement, celles qui ont contribué à la rédaction de ce papier : Mylène Crépin, Frédéric Giquel, Gabrielle Feltin, Laurent Mirtain, Philippe Sultan.

Bibliographie

[1] Benjamin DEXHEIMER, Bertrand WALLRICH, Architecture d'accès sécurisé multi-site. Dans *Actes du congrès JRES2003*, pages 269-282, Lille, Novembre 2003.

[2] Didier CHASSIGNOL et Frédéric Giquel, La mémorisation des mots de passe dans les navigateurs web modernes. Dans *Actes du congrès JRES2005*, Marseille, Décembre 2005.

[3] Philippe SULTAN et Frédéric GIQUEL, Vulnérabilités ISAKMP Xauth : description et implémentation. *MISC n°20*, juillet-août 2005.