Mise en place d'un garde-barrière

■ Jean-Paul EYNARD, Jean-Paul.EYNARD@ibs.fr
Institut de Biologie Structurale, CNRS/CEA Grenoble

■ Sylvaine ROY, Sylvaine.ROY@ibs.fr
Institut de Biologie Structurale, CNRS/CEA Grenoble

L'Institut de Biologie Structurale (IBS) est placé sous la double tutelle du CNRS et du CEA. Sa population (180 personnes) se répartit à peu près également entre ces deux organismes. Il est composé de dix laboratoires ou équipes de recherches.
L'institut est implanté sur un site propre « hors les murs » des sites géographiquement voisins du CNRS et du CEA, et son réseau informatique, ainsi que sa connexion à RENATER sont gérés indépendamment de ceux-ci. Toutefois des liens étroits sont nécessaires avec les départements de la Direction des Sciences du Vivant (DSV) du CEA. Ces relations privilégiées obligent à prendre en compte les règles de fonctionnement et de sécurité qui sont en vigueur au CEA. En particulier les intervenants « réseau » des départements de la DSV sont regroupés au sein de la Section pour les Systèmes d'Information et la Coordination des Réseaux (SSICR), et un ingénieur assure à Grenoble la fonction d'Agent de Sécurité des Systèmes d'information (ASSI).
L'IBS entretient aussi des liens privilégiés avec les organismes européens voisins : European Synchrotron Radiation Facility (ESRF), Institut Laue Langevin (ILL) et European Molecular Biology Laboratory (EMBL), qui ont leurs propres exigences concernant la sécurité des réseaux.
L'évolution de l'Internet et la mise en place chez nos partenaires de structures sécurisées nous ont amenés à reconsidérer l'architecture de notre propre réseau, conçu initialement comme un réseau unique fonctionnellement « plat ». Après consultation de l'UREC/CNRS et de la Direction Informatique du CEA nous l'avons fait évoluer vers une structure comprenant deux réseaux fonctionnellement et physiquement distincts : un réseau « public » accessible de l'Internet, et un réseau « prive » à priori non accessible de l'Internet, sauf par l'intermédiaire d'un garde-barrière, et après demande de dérogation.
Les aspects organisationnel et technique de cette démarche sont exposés dans ce qui suit.

■ Démarche

Pour réorganiser le réseau de l'Institut, notre démarche a consisté d'abord à analyser la population de l'IBS concernée par la restructuration de ce réseau, à impliquer fortement ses acteurs, notamment la Direction, dans l'étude de la politique à mettre en place, à proposer des solutions administratives qui apporteraient une amélioration de l'existant en matière de garde-barrière et pour emporter l'adhésion du plus grand nombre au sein interne de l'IBS.

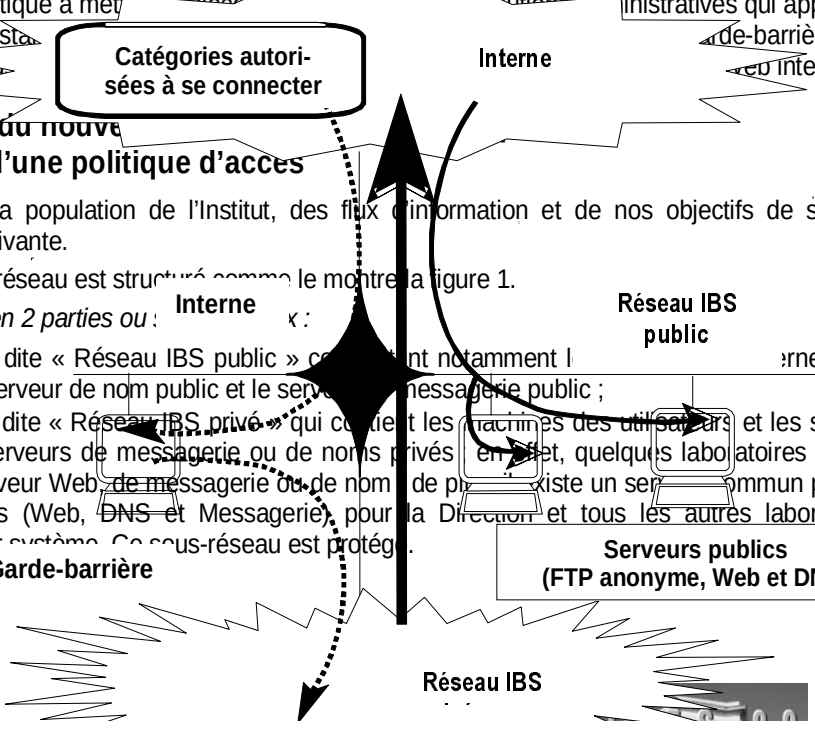
Structure du nouveau réseau et décision d'une politique d'acces

L'étude de la population de l'Institut, des flux d'information et de nos objectifs de sécurité a fait surgir l'organisation suivante.

Le nouveau réseau est structuré comme le montre la figure 1.

Il est divisé en 2 parties ou sous-réseaux :

- une partie dite « Réseau IBS public » contenant notamment le serveur Web externe, le service ftp anonyme, le serveur de nom public et le serveur de messagerie public ;
- une partie dite « Réseau IBS privé » qui contient les machines des utilisateurs et les serveurs Webs internes, les serveurs de messagerie ou de noms privés. En effet, quelques laboratoires ont désiré avoir leur propre serveur Web, de messagerie ou de nom ; de plus il existe un serveur commun pour chacune de ces 3 fonctions (Web, DNS et Messagerie), pour la Direction et tous les autres laboratoires n'ayant pas d'ingénieur système. Ce sous-réseau est protégé.



Les connections venant ou allant vers ces 2 sous-réseaux sont gérées à la fois par le routeur de l'IBS et le Garde-barrière de l'IBS.

Figure 1. Structure du Réseau de l'IBS.

La politique de sécurité est la suivante :

- Tout accès sortant du réseau IBS est totalement libre pour les principaux services utilisés à l'IBS (ftp, telnet, http).
- Les accès rentrants, qui viennent de l'Internet et qui vont vers le réseau public de l'IBS sont eux aussi totalement libres.
- Les accès rentrants vers le réseau protégé de l'IBS sont eux réservés à des catégories de connections bien identifiées ; l'accès est contrôlé par le Garde-barrière et la vérification (ou authentification de la personne se connectant) est plus ou moins forte selon la catégorie à laquelle elle appartient.

Les catégories de population ayant à accéder au réseau privé

Pour les connections entrant vers le réseau protégé de l'IBS, on distingue les catégories suivantes :

Les collaborateurs privilégiés :

- Ils sont traités ainsi parce qu'étant sur des réseaux extrêmement protégés ou pouvant être considérés comme une émanation de l'IBS.
- Ce sont les collaborateurs des départements des Sciences de la Vie du CEA sur réseau CEANet interne.
- Dans ce cas, la connexion passe par le garde-barrière : l'accès est enregistré (traces conservées), mais il n'y a pas d'authentification.

Les autres collaborateurs ou les Agents en mission :

- Leur connexion passe par le Garde-barrière et il leur faut « s'authentifier » par un nom de compte et un mot de passe ; un compte sur le garde-barrière est donc créé pour chacun d'entre eux pour une durée limitée.
- Il est important de noter que cette phase a été revue et corrigée en collaboration avec la Direction.

Implications techniques de cette politique d'accès

- Pour les collaborateurs privilégiés (ESRF, CEA…) le service informatique s'est occupé de recenser les adresses IP concernées.
- Pour les collaborateurs et les agents en mission, le gestionnaire du Garde-barrière a besoin de connaître les adresses IP concernées et d'ouvrir ou de valider le compte du collaborateur ou de l'agent en déplacement pour la durée nécessaire.

A l'époque, dans d'autres départements de la DSV du CEA par exemple, la procédure est la suivante :

- La demande d'ouverture de compte pour une adresse IP source et une personne considérées est faite sur un bordereau *papier* (disponible sur un serveur en format RTF ou HTML), bordereau transmis à l'ASSI. Cet ASSI valide la demande en la paraphant et la transmet par courrier interne au service informatique gérant le Garde-barrière concerné.
- Ceci nous a paru extrêmement lourd et impossible à appliquer à l'IBS ; une telle mesure aurait été rejetée d'emblée, y compris par la hiérarchie.
- *En accord avec le Directeur de l'Institut, cette politique a été assouplie en considérant 2 étapes :*
- La ***création*** du compte faite une fois pour toutes et soumise à l'autorité de la hiérarchie et de l'ASSI, qui doit vérifier si le demandeur satisfait certaines conditions de statut et de présence à l'IBS
- La ***validation*** du compte pour une durée déterminée, faite aussi souvent que demandée, en particulier à chaque déplacement

Accompagnement administratif

Pour que cette solution apporte de plus une certaine amélioration dans l'organisation existante, nous avons étudié *avec les Secrétaires et la Direction* comment la coupler avec l'organisation des déplacements et intégrer le tout au niveau du serveur Web interne de l'IBS

Les procédures suivantes ont été décidées :

- Création des comptes (pour les collaborateurs ou les agents nomades) :

  - La demande se fait via un bordereau HTML lié à un script CGI.
  - Ce script l'envoie par messagerie à l'ASSI qui acquiesce (ou non) électroniquement, en faisant une retransmission électronique du bordereau au gestionnaire du Garde-barrière. Ce script réaffiche le bordereau renseigné et rappelle à l'utilisateur d'imprimer cette page pour qu'elle reçoive parallèlement via sa secrétaire, les signatures de la hiérarchie et de l'ASSI. La validation « papier » n'est donc pas éliminée mais le compte est crée dès accord électronique de l'ASSI. (Il sera supprimé si le « papier visé » ne parvient pas au service informatique au bout d'un certain temps, ce qui ne s'est jamais produit).
- Validation/invalidation des comptes nomades couplées avec l'organisation des déplacements :
  - A l'époque, un chercheur prévoyant un déplacement griffonnait un bordereau papier ou même un post-tit à l'adresse de sa secrétaire pour qu'elle le lui organise.
  - Nous avons donc étudié avec les secrétaires le bordereau électronique de mission « idéal » pour elles. Aux informations dont elles avaient besoin (Lieu, date, heure, etc.) nous avons rajouté la demande éventuelle d'accès sur le réseau privé de l'IBS pendant le déplacement, avec mention des adresses IP sources concernées. Sur ce bordereau ont également été insérés des liens vers des sites aidant le chercheur à organiser son voyage (horaires SNCF, Air France, plan de métros, optimisation d'itinéraires automobiles, etc.)
  - Un script CGI traite ce bordereau, l'envoie à la secrétaire sous la présentation la plus utile pour elle en lui proposant d'accuser réception à l'utilisateur.
  - Si l'accès au réseau IBS privé a été demandé, le script prévient par messagerie le service informatique avec les informations nécessaires (compte à valider, dates, adresses IP à autoriser). Ce script réaffiche aussi bien sûr la page renseignée pour que l'utilisateur puisse éventuellement conserver une trace papier de sa demande de mission.
  - Il est entendu avec les secrétaires, que dans le cas où la hiérarchie exceptionnellement refuse la mission demandée, celles-ci avertissent par Email, le service informatique qui invalidera le compte, mais ceci ne s'est jusqu'ici jamais produit.
  - L'adhésion du personnel administratif et en particulier des secrétaires à un tel système a été totale. Le fait de les avoir fait participer à la définition de l'amélioration du système existant a beaucoup contribué à sa réussite.

Informations des utilisateurs

Il restait à informer et à impliquer aussi les chercheurs.

La Direction a envoyé à chaque agent de l'IBS (par Email et par courrier interne) une note expliquant la nouvelle organisation du réseau et les changements administratifs qui en découlaient.

Nous avons en même temps organisé plusieurs réunions d'informations d'abord au sein du conseil des chefs de laboratoires, puis globalement au niveau de tout le personnel de l'IBS et enfin par petits groupes dans certains laboratoires pour étudier, avec certains chercheurs inquiets, leur cas particulier. A la suite de ces réunions, nous avons proposé aux plus anxieux de servir de « cobayes » pendant la période transitoire de tests, pour les rassurer quant au fonctionnement de l'ensemble vis-à-vis de leur cas spécifique. Nous devons reconnaître que beaucoup d'autres se sont alors spontanément proposés et qu'une telle coopération a grandement facilité la période de tests.

Il est à noter aussi que lors de ces réunions, nous avons insisté sur la responsabilisation du personnel. Nous avons rappelé certains cas récents d'intrusion dans des organismes de recherche proches de l'IBS et réaffirmé que cette sécurisation était là pour protéger le fruit de leurs recherches et non pour les empêcher de travailler.

Nous avons répété que nous avions besoin de leur coopération et qu'il était primordial, en cas de problème particulier, de venir nous trouver pour que nous essayions de trouver une solution ensemble plutôt que de chercher à « truander » le système. La note de la Direction et les bordereaux utilisés rappellent d'ailleurs aussi cette notion de responsabilité pour chaque agent.

Toutes ces informations (Note de la Direction, Structure du réseau, questions/réponses posées lors des réunions, utilisation pratique du Garde-barrière) ont été déposées sur le serveur Web interne de l'IBS pour informer tout nouvel arrivant.

L'ensemble de la démarche a été globalement très bien accepté et ceci a permis de mettre en place en douceur le dispositif technique détaillé dans le chapitre suivant.

■ Aspects techniques

Routage et filtres

Le nouveau routeur est un CISCO 4500, sous IOS 11.0(9), équipé d'une carte à six ports RJ45.

Les filtres sont répartis dans deux « access-lists ».

La première série de filtres, sur le port de connexion externe, sert à la protection générale des réseaux de l'Institut. Les règles appliquées sont exposées dans le tableau ci-dessous qui répertorie le trafic autorisé :

Source	*Destination*	*Trafic autorisé*
Any	Firewall	IP
Any	Serveur DNS public	DNS
Any	Serveur W3 public	HTTP, FTP
Any	Serveur SMTP public	SMTP
Any	IBS-privé	TCP established
Any	IBS-privé	UDP > 1024
« trusted hosts »	IBS-prive	----------

La deuxième série de filtres **est en protection du réseau privé :**

Source	*Destination*	*Trafic autorisé*
Firewall	IBS-privé	Telnet, ftp, X11
Serveur DNS public	IBS-privé	DNS
Serveur SMTP public	Serveurs SMTP privés	SMTP
Any	IBS-privé	TCP established
Any	IBS-privé	UDP > 1024
« trusted hosts »	IBS-prive	----------

Service de noms

Deux serveurs de noms primaires pour la zone « ibs.fr » coexistent :

Un serveur primaire public déclaré à RENATER, accessible de l'Internet, répertorie les machines devant être connues de l'extérieur.

Un problèmes s'est rapidement posé avec les vérifications d'existence au DNS de la machine source faites par de plus en plus de serveurs.

Nous avons finalement entré un pseudonyme pour chaque numéro IP possible du réseau.

Un serveur primaire privé inaccessible de l'extérieur, répertorie les machines des réseaux public et privé. Ce serveur transmet les requêtes qu'il ne peut résoudre au serveur public (« forwarder » et « slave »), sans jamais établir de dialogue avec les routeurs de l'Internet.

Service de messagerie

Le service de messagerie est entièrement basé sur le protocole SMTP. Il est constitué d'un bureau de poste principal situé sur le réseau public et de plusieurs bureaux de poste secondaires situés sur le réseau privé.

Le DNS public publie un seul enregistrement MX pour le domaine « ibs.fr », celui correspondant au serveur SMTP public qui récupère ainsi tout le trafic venant de l'Internet et destiné à l'IBS.

Le programme sendmail du serveur public redistribue alors les messages vers les bureaux de poste privés adéquats annoncés dans les enregistrements MX du DNS privé.

Garde-barrière

La station utilisée est un PC Pentium II cadencé à 233 MHz, avec un BIOS permettant de booter directement sur CDROM.

Le système d'exploitation est la distribution Mandrake de LINUX, variante du RedHat 5.1 : pas de drivers video commerciaux, KDE, noyau 2.0.35. Le noyau compilé comporte le strict minimum.

Le logiciel garde-barrière est le package FWTK de TIS. Les proxies activés sont : TELNET, FTP, HTTP, POP, X11.

Dispositions générales de sécurité

Sauf pour le garde-barrière les stations utilisées pour les différents serveurs sont actuellement des stations SUN sous SOLARIS. Sur les machines publiques les services ont été réduits au minimum nécessaire, les patches de sécurité annoncés par le constructeur ont été appliqués et une image « TRIPWIRE » précédent la mise en exploitation est conservée.

Le garde-barrière est accompagné d'un « doublon » configuré à l'identique, connecté sur le réseau privé et récupérant régulièrement les bases du garde-barrière en exploitation de manière à pouvoir être mis en service rapidement en cas de défaillance de celui-ci.

Les différents « logs » des systèmes de protection (routeur et garde-barrière) sont redirigés vers un serveur privé pour y être analysés.

Conclusion

Cette organisation de réseau sécurisée est en exploitation depuis bientôt un an (Basculement le 1er/12/98)

Nous pouvons en tirer les enseignements suivants :

- La démarche utilisée (information intensive et implication des utilisateurs, notamment en premier lieu de la hiérarchie et du personnel administratif, souplesse des procédures, utilisation du Web) a porté ses fruits en nous apportant une adhésion pratiquement totale du personnel de l'IBS.
- Les besoins d'accès des utilisateurs quand ils sont en déplacement concernent la messagerie dans 80 % des cas.

Nous envisageons les améliorations suivantes :

- Mise en place sur la partie publique du réseau d'un serveur de messagerie avec migration automatique de la boîte à lettres d'un agent vers ce serveur au moment d'un déplacement
- Couplage avec la base de données du personnel (pour alléger le remplissage d'un bordereau côté utilisateur et faciliter le travail de l'ASSI)
- Automatisation de la validation/invalidation des comptes (actuellement le traitement est seulement semi-automatisé via l'usage de l'utilitaire « calendar » sous Unix)
- Amélioration du traitement des logs du garde-barrière (format, liaison avec les dates d'absence des agents, etc.).