# Recommandations d'architecture de réseau avec filtrages pour améliorer la sécurité

en particulier pour mieux se protéger des attaques venant de l'Internet

Jean-Luc Archimbaud CNRS/UREC (http://www.urec.fr)
25 janvier 2000

**Ce document est destiné aux administrateurs de réseaux et de systèmes**, personnes qui doivent mettre en place ou faire évoluer l'architecture des systèmes d'information (informatique et réseaux) d'un campus, d'un groupe de laboratoires ou d'un laboratoire (dans ce qui suit le terme site désignera ces 3 environnements). Un autre document plus didactique, moins détaillé et moins technique est disponible en ligne : http://www.urec.cnrs.fr/securite/articles/archi.reseau.court.pdf.

Cet article n'essaie pas de résoudre tous les problèmes de sécurité, loin de là. **Il se focalise sur les vulnérabilités liées au réseau**, en particulier aux attaques provenant de l'Internet et essaie de proposer **un modèle d'architecture associé à des contrôles d'accès pour limiter ces vulnérabilités**. Ce modèle devrait être acceptable par la communauté enseignement-recherche. Concrètement il ne demande pas d'investissements lourds et peut-être facilement adopté par les utilisateurs, voire transparent pour eux. Comme tout modèle il est à adapter à chaque environnement.

Les recommandations ci-dessous ne sont pas nouvelles, depuis de nombreuses années nous les avons exprimées de diverses manières. Maintenant, il s'agit de les généraliser à tous les sites car les risques et les attaques augmentent de jour en jour. Mais les fonctionnalités que l'on recommande d'utiliser sont à présent disponibles sur tous les produits installés sur les sites et les administrateurs ont acquis la compétence réseau suffisante pour comprendre et configurer ces mécanismes.

# 1. Situation

## 1.1 Le succès de l'Internet n'était pas prévu …

Nos sites sont connectés à l'Internet depuis longtemps. Lors du choix de l'architecture des points d'accès de ces sites à l'Internet, concrètement à Renater, la sécurité n'était pas un critère prioritaire. Le but principal était alors que toutes les machines des sites, sans exception, puissent accéder et être accédées de l'Internet avec le meilleur débit possible. La connectivité totale (full connectivity) était l'objectif. On pensait qu'il pourrait y avoir des problèmes de sécurité dans le futur mais ce n'était pas prioritaire dans les choix techniques. L'Internet n'était qu'un ensemble de réseaux de recherche où « tout le monde se connaissait ». On n'avait pas d'attaque de spam, scan, smurf, flood, spoofing, sniffer, … (se référer aux articles de la presse informatique grand public). Maintenant l'Internet est devenu un outil de communication mondial, utilisé par des bons et mauvais citoyens et toutes les déviances courantes y sont présentes. Même le terme de village global, qui désignait l'Internet avec sa note de convivialité et de quiétude, semble avoir disparu. L'Internet n'est pas plus noir que le monde mais il n'est pas plus blanc non plus.

On a pu voir rapidement que cette connectivité totale était une aubaine pour les personnes mal intentionnées qui pouvaient ainsi essayer très facilement de tester toutes les machines d'un site et découvrir rapidement un maillon faible. Quand sont arrivées les premières attaques que nous connaissons maintenant tous les jours, une réaction extrémiste a été de préconiser l'installation d'un **garde-barrière** en entrée de chaque site. Mot magique, assurance tous risques ! Cet équipement qui au départ désignait un ensemble de relais d'applications allait résoudre tous les problèmes. Mais les gardes-barrières de l'époque se sont avérés très contraignants. Ils ne supportaient (laissaient passer) que certaines applications, demandaient (et demandent toujours) une administration lourde, étaient des goulots d'étranglements en terme de débit (ce qui est toujours vrai pour les relais d'applications), ... Nous n'avons pas recommandé de généraliser cette solution pour tous les sites. Une autre raison très

pragmatique est que nous n'avons pas les moyens financiers et humains pour installer et administrer ce type d'équipement dans chaque laboratoire.

Rapidement ces gardes-barrières relais d'applications ont évolué pour devenir plus « supportables ». Aujourd'hui, on serait bien en peine de définir ce qu'est un garde-barrière car il peut regrouper une ou plusieurs fonctions très différentes telles que le filtrage de paquets, le filtrage (statique ou dynamique) de sessions, la translation d'adresses, le relais d'applications, l'authentification des utilisateurs, la détection d'intrusions, … Ces gardes-barrières se retrouvent dans des boites noires dédiées ou dans des logiciels sur PC ou dans des routeurs ou … Et il faut des compétences pour choisir un garde-barrière adapté à ses besoins et le configurer. La sécurité ne s'est pas simplifiée. Le garde-barrière au sens boite ou logiciel dédié n'est pas une solution à rejeter systématiquement, dans certains environnements elle se justifie, mais elle n'est pas à généraliser à tous les laboratoires. Fermons la parenthèse.

**Le choix du « tout ouvert », au moment où il a été fait, n'était pas une erreur ; mais rester maintenant dans la même logique en est une**. Il faut absolument limiter les possibilités de communication entre l'extérieur et l'intérieur, non en restreignant les utilisateurs mais en ne laissant passer que ce qui est utile, ceci sur tous les sites. La méthode est expliqué dans ce document. De la même manière que l'on ferme à clé son appartement ou sa voiture, que l'on contrôle l'accès à son bâtiment, il ne faut pas laisser complètement ouvert son accès Internet. Les sociétés commerciales qui se sont raccordées à l'Internet bien plus tard n'ont pas eu la même démarche que nous. Elles ont considéré l'Internet dès le départ comme un monde externe, hostile. Elles ont construit un réseau interne privé pour connecter leurs sites, un Intranet, où circule toutes leurs communications (souvent confidentielles) intra-entreprise. Elles ne sont connectées avec l'Internet qu'en un ou deux points par lesquels transitent principalement des informations publiques. Ces portes sont contrôlées par un équipement de type garde-barrière. Nous, nous utilisons Renater comme un Intranet, alors que Renater c'est l'Internet. Nous avons ainsi plusieurs centaines de points d'accès à l'Internet d'où une situation totalement différente, beaucoup plus dangereuse.

En interne sur les sites, lorsque les réseaux locaux ou de campus ont été mis en place, le but était le même que pour l'accès Internet. Il fallait raccorder le maximum de postes, tous les postes devant pouvoir communiquer avec tous les autres, installer un service universel, le même pour tous. Sur les petits sites, un seul réseau Ethernet suffisait, sur les grands sites plusieurs réseaux Ethernet étaient construits connectés par des routeurs, avec un découpage géographique pour réduire la charge et s'affranchir des limites de distance d'Ethernet. Aucun critère de sécurité n'a été pris en compte dans la conception des premiers réseaux de campus.

L'usage du réseau se généralisant on a pris conscience que sur un même site, certains groupes comme les étudiants avaient de grandes chances de compter parmi eux un pirate, que certains laboratoires (avec de nombreux contrats industriels par exemple) avaient besoin de plus de sécurité que d'autres, que certaines machines de gestion contenaient des informations sensibles, … ; et qu'Ethernet était un réseau à diffusion où avec un simple logiciel d'écoute installé sur un PC utilisateur on pouvait récupérer tous les mots de passe qui circulent sur le réseau (ceci n'est qu'un exemple de vulnérabilité d'une architecture non segmentée).

Dans la seconde vague de mise en place des réseaux de grands sites, la segmentation (découpage du réseau) a été mise en œuvre, de manière physique d'abord (une « fibre » pour l'enseignement, une pour la recherche, une pour l'administration), logique ensuite avec les VLANs (Virtual LAN, Local Area Network) quand cette fonction a été disponible sur les équipements.

Il s'agit maintenant d'essayer de **généraliser cette segmentation à tous les moyens et grands sites**.

## 1.2 Des systèmes informatiques imparfaits

Quel est le risque de la connectivité totale, c'est à dire de la liberté totale de communication entre les machines internes et l'Internet ?

### 1.2.1 Systèmes avec des bogues

Si tous les systèmes étaient parfaits et si toutes les machines étaient administrées avec un suivi quotidien, il n'y aurait aucun risque supplémentaire. Mais on est très très loin de cette image d'Epinal. **Presque quotidiennement un avis d'un CERT (Computer Emergency Response Team) annonce un bogue dans un logiciel avec le correctif approprié**. Généralement cet avis fait suite à la diffusion sur l'Internet d'un outil d'attaque qui utilise ce bogue pour acquérir les droits d'administrateur de la machine vulnérable. Pour manier cette arme logicielle gratuite et disponible pour tous, inutile d'être un génie, il suffit de lancer un programme. Heureusement pour nous la grande majorité des internautes a d'autres objectifs que d'essayer de pirater les machines de recherche. Autrement, quelle hécatombe dans les laboratoires ! Mais dans les dizaines de millions d'internautes, il y a une poignée de petits psychopathes ou délinquants, et il y en aura toujours, qui pour montrer leur capacité, par jeu, par vengeance, prennent plaisir à pénétrer les systèmes, les casser ... Les laboratoires ont aussi quelques concurrents scientifiques ou commerciaux qui n'hésitent pas à se servir de ces outils pour s'approprier leur travail. Plusieurs attaques dans des unités étaient ciblées pour récupérer des résultats de recherche ou des développements intéressants. Ainsi au CNRS, en moyenne 2 attaques violentes par semaine nous sont remontées (sans compter les scans).

### 1.2.2 Systèmes ouverts par défaut

L'autre talon d'Achille d'un système d'information distribué en réseau tel qu'on l'a aujourd'hui est le très lourd travail d'administration des multiples systèmes Unix et NT qui sont de base des serveurs. Or qui dit serveurs, dit logiciels serveurs réseau (démons sous Unix, services sous NT), qui sont autant de fenêtres qui peuvent permettre d'entrer par effraction dans un ordinateur. Le travail serait grandement simplifié si les ordinateurs livrés avaient toutes les fenêtres fermées et que l'administrateur n'ait qu'à ouvrir une à une celles nécessaires. Il n'en est rien ! **La tendance d'Unix et de NT est au contraire de lancer le maximum de services par défaut, sans en informer l'administrateur**. Celui-ci doit donc fermer ces ouvertures inutiles. Une première étape consiste à découvrir toutes les ouvertures, la seconde à ne conserver que celles utiles, les services réseaux vraiment utilisés. Une simple commande suffit me direz vous. Que nenni ! Sur Unix, on commence à avoir l'expérience nécessaire et avec *inetd.conf*, les fichiers de démarrage et les commandes *ps* et *netstat* on arrive à faire l'inventaire et à faire ce ménage. Sur NT, on peut arriver à un résultat similaire avec le menu *Services* dans *Panneau de configuration* et le *Gestionnaire de tâches* mais l'expérience manque cruellement et on ne sait même pas avec certitude le numéro des ports utilisés par tous les services NT. **Ainsi sur la plupart des ordinateurs d'un site, sont lancés des serveurs réseaux inutiles, pas ou mal configurés et qui sont autant de fenêtres grandes ouvertes ignorées**.

### 1.2.3 Systèmes trop nombreux

Lorsqu'il y avait peu de machines (en particulier peu de serveurs) sur les sites, une recommandation forte a été de maintenir toutes les machines des sites dans un bon état de sécurité, bien configurées avec les derniers correctifs. Mais cet objectif est irréaliste maintenant. Un administrateur qui a essayé d'appliquer tous les correctifs des avis des CERTs sur l'ensemble de son parc hétérogène et qui a essayé de contrôler les services réseaux sur tous les Unix ou NT de ses utilisateurs a vite compris que c'était une course perdue d'avance. Avec ces logiciels bogués à modifier régulièrement et des serveurs livrés ouverts qu'il faut reconfigurer, tâches qui se rajoutent à leur travail quotidien, **les administrateurs n'ont matériellement pas le temps de maintenir l'ensemble des systèmes d'un site dans un état acceptable pour la sécurité**.

### 1.2.4 Alors ?

Il faut trouver une autre solution. C'est le but de ces recommandations qui proposent une architecture réseau avec les restrictions d'accès nécessaires et qui permettent de **restreindre à une poignée le nombre de systèmes à configurer avec soin, mettre à jour régulièrement et surveiller quotidiennement**, en laissant la grande majorité des autres stations dans un état plus laxiste sans trop de risques pour la sécurité de l'ensemble.

# 2. L'architecture

## 2.1 Principes

On peut faire le constat que tous les systèmes d'un site n'ont pas besoin de la même ouverture d'accès vis à vis de l'Internet.

**Dans le sens sortant**, du site vers l'Internet, tous les postes doivent pouvoir accéder à des serveurs Web, échanger des messages, … Généralement on limitera peu les communications dans ce sens. Néanmoins on peut considérer que certains groupes comme les étudiants peuvent se comporter en pirate pour l'extérieur et limiter leurs actions dans ce sens sortant.

Mais **dans le sens entrant**, de l'Internet vers le site, sens qui permet d'accéder aux services réseau sur les stations locales, le besoin de connexion est généralement très faible : évidemment le serveur WEB doit être accessible par tout l'Internet mais les serveurs locaux (de calcul par exemple) et les postes de travail utilisateur en ont rarement besoin. Si c'est néanmoins le cas, le besoin est souvent temporaire (accès à des fichiers lors de missions, depuis le domicile) et identifié (depuis certains sites). Or c'est ce sens entrant qui présente un danger. On va donc essayer de limiter autant que faire ce peut les flux dans cette direction.

Partant de ce constat le principe de l'architecture est simple. Dans un premier temps il faut séparer les machines qui ont besoin d'être accédées de l'Internet (les serveurs réseaux) des autres (les machines utilisateurs clientes et les serveurs locaux) et disposer les premières dans une zone semi-ouverte entre l'Internet et le réseau purement local.

Dans un second temps, sur le réseau local, il faut identifier les différentes communautés (unités, laboratoires, écoles, UFRs, services, serveurs généraux internes, …). Les machines de ces groupes seront réparties dans différents sous-réseaux physiques ou logiques. On arrive ainsi a une architecture segmentée.

Les critères à prendre en compte pour ce tri peuvent être le rattachement administratif mais aussi les besoins réseau (connectivité complète avec l'Internet ou non), les besoins de sécurité (confidentialité de certains contrats, données, …), les types d'utilisateurs (permanents ou de passage), le mode d'administration des machines (par le service informatique, un ITA ou sans administration reconnue).

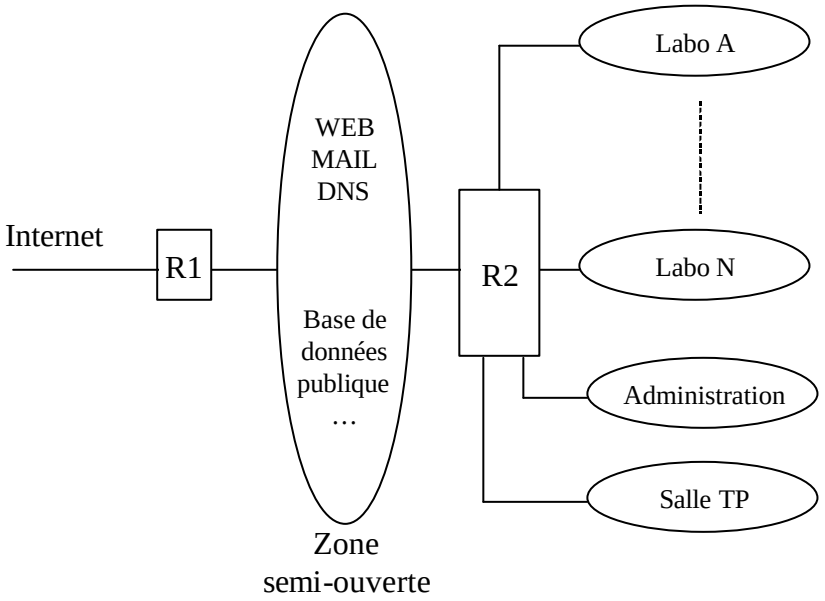


Fig 1 : principe de l'architecture

Dans un troisième temps on installera des filtres dans les équipements de connexion (routeurs R1 et R2) pour isoler certaines machines sensibles ou certains groupes à risque et n'autoriser que les services utiles et contrôlés à circuler. Le tri des machines étant fait, ces filtres seront simples à écrire.

## 2.2 Les services dans la zone semi-ouverte

Dans la zone semi-ouverte, en entrée de site, il faut installer toutes les machines qui assurent les **services réseau avec l'extérieur : DNS, messagerie, Web, FTP anonyme, News, serveur d'accès commuté, cache Web, bases de données publiques**, et tout autre service qui a besoin de communication intensive avec l'Internet. Cette zone sera typiquement un réseau Ethernet 10 ou 100 M, selon le débit de la prise d'accès à l'Internet. Inutile d'avoir du Gigabit si on n'a qu'un accès à 2 M avec l'Internet. Ce réseau sera connecté à l'Internet par un routeur (R1 sur le schéma) dans lequel on aura installé un ensemble de filtres décrits ci-après. Les services réseau pouront être éclatés sur plusieurs machines ou concentrés sur une ou deux, selon la taille du site, le budget, le mode d'administration … L'éclatement conseillé sur plusieurs machines permet de mieux limiter et surveiller les accès.

**Ces machines constituent la poignée de machines qu'il faut parfaitement gérer**.

**Chaque machine sera dédiée à sa ou à ses fonctions**, elle ne sera pas utilisée comme station de travail « classique » et n'hébergera pas d'autres applications.

Les systèmes pourront être Unix ou NT. Le critère de choix doit être la compétence des administrateurs. Les services NT peuvent paraître plus simples à installer mais NT est un système complet qu'il faut maîtriser et connaître comme Unix si on veut assurer sa sécurité et globalement son bon fonctionnement.

**Sur ces machines, les versions des systèmes et des applications seront régulièrement mises à niveau et les correctifs de sécurité seront installés dès qu'ils seront diffusés**.

Tous **les services réseaux inutiles seront inhibés** (ménage dans inetd.conf sur Unix ou dans Panneau de configuration – Services sur NT). Un minimum d'utilisateurs avec un accès interactif seront déclarés, uniquement les administrateurs qui en ont besoin. Sur chacune sera installé un **outil de contrôle et de trace des connexions** tel que tcp_wrapper sur Unix. Dans ces serveurs, tous les messages de journalisation (logs) seront renvoyés sur un serveur interne, appelé « Serveur logs » sur le schéma ci-après.

Regardons quelques services qui demandent certaines adaptations :

- Sur le serveur de messagerie seront déclarés tous les utilisateurs avec un compte de messagerie POP ou IMAP pour accéder à leur boite aux lettres mais sans possibilité de travail interactif (pas de shell, d'où le nom «Mail sans sh »). Si pour lire leur courrier certains utilisent des commandes Unix (qui nécessitent un shell), leurs messages seront renvoyés vers un serveur de messagerie interne, appelé « Mail avec sh » dans le schéma, où ces utilisateurs auront des comptes interactifs. Pour chaque utilisateur, le mot de passe utilisé pour accéder au serveur de messagerie de la zone semi-ouverte sera différent de tous les autres mots de passe utilisés pour accéder aux autres systèmes, en particulier de celui de leur machine de travail.
- Le serveur Web contiendra uniquement des pages publiques. Si le site désire avoir des pages privées elles seront sur un serveur interne, appelé « Serveur Web interne » sur le schéma. De même que pour les autres serveurs, il faut le minimum de compte interactif sur cette machine. Ainsi la construction des pages du serveur Web public qui nécessite ce type d'accès sera faite sur le serveur Web interne. La mise à jour du serveur public se fera par transfert de fichiers quotidien entre les deux serveurs, par montage NFS si les administrateurs maîtrisent parfaitement les mécanismes de protection de ce système, ou tout autre système similaire et bien maîtrisé.
- Si le site compte un ou des serveurs de bases de données publiques accédées depuis l'Internet, on installera ces machines dans cette zone, et on appliquera les mêmes recommandations d'exploitation et de mise à jour que pour le serveur Web.
- Si le site dispose d'un service d'accès commuté (RTC), il se placera aussi dans cette zone. Dans ce serveur, on authentifiera tous les utilisateurs et on gardera une trace des appels, transmise au « serveur logs ». On appliquera les restrictions d'accès par utilisateur, en particulier on ne permettra pas par défaut une connexion à l'Internet via ces accès.
- Pour interdire l'accès direct en telnet ou FTP depuis l'Internet sur les machines du réseau interne, une machine relais pourra être installée. Ainsi un utilisateur qui depuis l'extérieur voudra accéder en interactif avec telnet sur sa machine de laboratoire devra d'abord se connecter sur ce relais puis ensuite faire un autre telnet. Sur ce relais seront déclarés uniquement les utilisateurs qui auront besoin de ce service avec un mot de passe particulier. Une trace de tous les accès sur ce relais sera

conservée. Un contrôle très fin des comptes utilisateurs (durée de vie des comptes, solidité des mots de passe, …) sera effectué. Ce passage obligé permet de concentrer toutes les bonnes mesures de sécurité sur la gestion des comptes utilisateurs sur une seule station, ce qui est beaucoup plus facile à faire que sur plusieurs dizaines voire centaines de machines en interne.

Les nouveaux services réseau qui se généraliseront, on peut le penser, comme l'annuaire LDAP (Light Directory Access Protocol), pourront être intégrés de la même manière : un serveur LDAP avec des informations «publiques » (comme le numéro de téléphone ou l'adresse électronique) dans la zone semi-ouverte, un autre dans la zone « Services communs internes » pour les informations « privées » (comme le mot de passe).

En un point de cette zone on peut scruter tous les échanges avec l'Internet. C'est l'endroit où installer un outil qui mesure l'activité et repère certains trafics anormaux, analyseur de trafic comme IPtrafic ou détecteur d'intrusions. Ce type d'équipement peut être très utile pour détecter des attaques et pour connaître l'utilisation de l'Internet faite par le site. Le seul problème est le temps nécessaire à l'installation et l'exploitation des résultats de ce genre de produit.

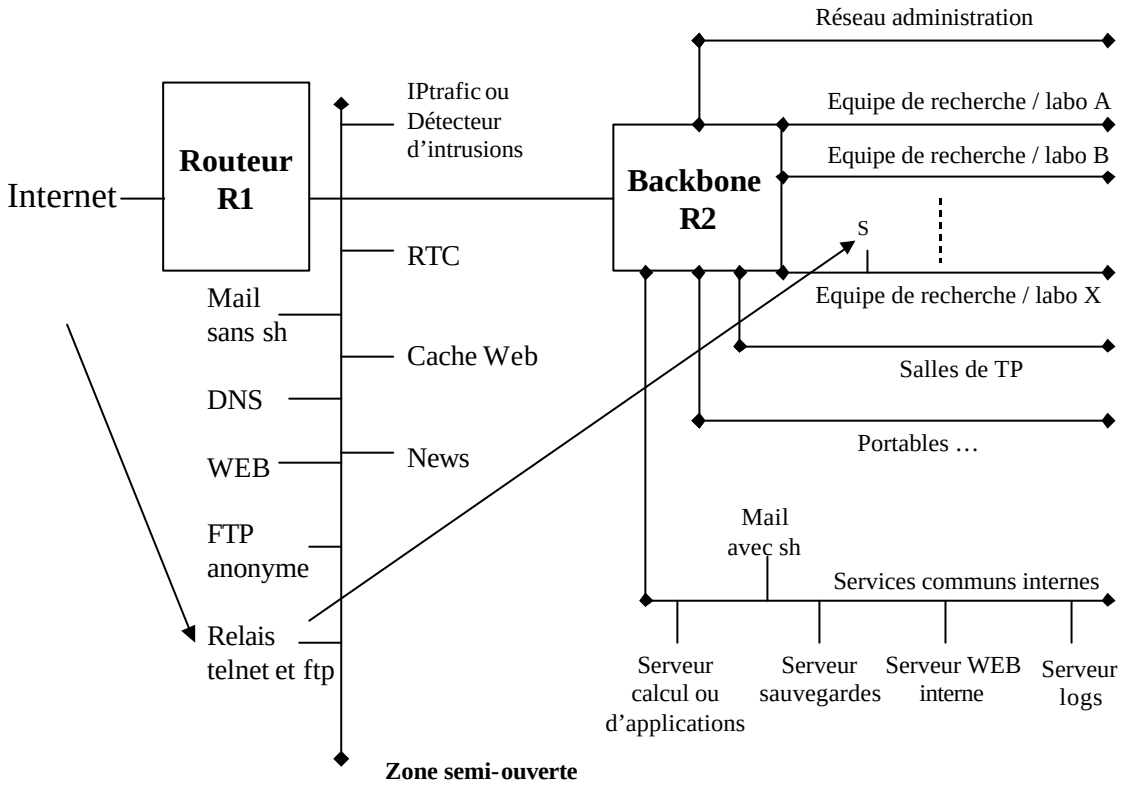


Fig 2 : architecture détaillée

## 2.3 L'architecture interne

Sur le réseau interne, typiquement un réseau Ethernet 10-100-1000 Mbits/s, un découpage du réseau sera effectué. L'équipement appelé Backbone R2 est un ensemble d'éléments qui font du routage (routeurs, commutateurs niveau 3-4-5-6-7, …) avec des fonctions de filtrage. Chaque sous-réseau connecté à R2 peut être physique, un câble dédié par réseau, ou logique si les équipements ont des fonctions de réseaux virtuels (VLAN). Un des avantages des VLANs est de pouvoir faire évoluer cette architecture, au gré des déménagements et restructurations très courants chez nous, sans intervention sur le câblage. Néanmoins, cela impose certaines contraintes comme la centralisation de l'administration et l'homogénéité presque obligatoire des équipements.

Bien que la définition des groupes et la segmentation dépendent entièrement du site, le schéma donne un exemple dont on peut s'inspirer. On trouve les sous-réseaux :

• Administration : il regroupe les stations de gestion, avec des données souvent confidentielles (courriers officiels, fichiers nominatifs, contrats, informations comptables, évaluations des personnels et des étudiants, …). Les utilisateurs de ce groupe ont les besoins « domestiques » de l'Internet, Mail et Web uniquement, pas vraiment de telnet ou de FTP. Il peut y avoir plusieurs sous-réseaux « administration » sur le site, quand plusieurs services administratifs sont présents par exemple.

• Equipes de recherche ou laboratoires : un sous-réseau par équipe de recherche ou laboratoire ou entité administrative avec une autorité décisionnelle propre. Ces réseaux auront souvent des besoins particuliers de connectivité : accès vers des serveurs de calcul ou des bases de données ou des gros équipements scientifiques nationaux ou internationaux, coopérations avec des équipes étrangères, …

• Salles de TP (Travaux pratiques) : réseaux où on contrôle les ordinateurs mais mal les utilisateurs, jugés dangereux car attaquants potentiels, autant pour le site local que pour les sites distants. On voudra limiter leur utilisation de l'Internet et leurs accès vers les autres groupes locaux.

• Portables et plus globalement les machines non administrées : si ce type d'équipement est courant, peut-être faut-il envisager un sous-réseau (ou plusieurs) pour connecter les stations des personnes du site ou de passage qui ont « leur » ordinateur personnel que n'administre pas l'équipe informatique. Ces machines peuvent être mal configurées, elles le sont certainement, et sont donc dangereuses. Il faudra certainement les isoler et les considérer comme des machines externes.

• Services communs internes : peuvent être regroupées sur un ou plusieurs sous-réseaux les machines qui offrent des services à l'ensemble du site ou à plusieurs groupes du site. Les utilisateurs de ces services sont uniquement locaux, les stations n'ont donc pas besoin d'accès depuis l'extérieur (par opposition aux serveurs de la zone semi-ouverte). Ce peuvent être des serveurs de calcul, de sauvegardes, de Web interne, … si besoin serveurs de messagerie internes avec des utilisateurs interactifs (cf avant). Une machine de sécurité qui centralise et récupère les logs utiles des serveurs de la zone semi-ouverte et des routeurs est obligatoire. Cette machine pourra être installée dans ce sous-réseau.

## 2.4 Les filtres

L'architecture mise en place ne devient vraiment utile pour la sécurité que si l'on installe des mécanismes qui limitent les trafics avec l'Internet et entre les différents sous-réseaux. Sur les routeurs ou équipements équivalents cela peut être réalisé de différentes façons :

• Par contrôle du routage : en effet il est très simple de ne pas annoncer (faire connaître) un sous-réseau à Renater par exemple, ainsi l'ensemble des machines du sous-réseau ne seront pas atteignables depuis l'Internet car le numéro IP du sous-réseau sera inconnu dans les tables de routage nationales et internationales.

• Par filtrage statique sur les adresses IP : on interdit tout trafic vers et depuis certaines machines, certains sous-réseaux.

• Par filtrage statique sur les numéros de ports associés à des adresses IP : on autorise ainsi l'utilisation que de certaines applications depuis ou vers certaines stations ou sous-réseaux.

• Par filtrage dynamique pour des applications qui utilisent des numéros de port dynamiques comme H323 pour la téléphonie sur IP.

Les 3 premières manières sont couvertes par les fonctionnalités de presque tous les routeurs du marché (pour les commutateurs-routeurs ou équipements « hybrides » de ce type il faut vérifier). Le filtrage dynamique relativement nouveau nécessite souvent un équipement ou un logiciel routeur spécifique, classé comme garde-barrière.

### 2.4.1 Les filtres sur le routeur d'entrée R1

**La politique de R1 sera de tout interdire dans le sens entrant sauf des services que l'on connaît et maîtrise vers certaines machines**. Tous les autres accès seront rejetés.

Dans un premier temps, on installera les filtres habituels pour éviter les problèmes de mascarade IP et de broadcast IP.

Ensuite le but de ces filtres pourra être de :

• **Interdire l'accès depuis l'Internet aux machines de l'administration (trop sensibles) et aux portables (pas administrés)**. On peut procéder de plusieurs manières avec les 4 types de filtrages ci-dessus. La méthode la plus simple, à laquelle on ne pense souvent pas, est de « cacher » les sous-

réseaux « Administration » et « Portables » à l'Internet. En effet ces groupes ont pour seules demandes la messagerie et l'accès Web (pas besoin de telnet par exemple). Dans ce cas, si le site possède un cache Web, les machines de ces sous-réseaux n'ont pas utilité d'un accès IP direct avec l'Internet, un accès vers la zone semi-ouverte suffit (où on trouve le serveur de messagerie et le cache Web). On pourra ainsi ne pas annoncer (faire connaître) ces sous-réseaux à Renater ou plus simplement de numéroter les machines avec des adresses privées (RFC1918).

- On peut appliquer le même remède pour le sous-réseau « Salle de TP » avec un but différent : **limiter les possibilités d'attaques vers des sites externes depuis ce sous-réseau**. En ne permettant pas une connectivité complète avec l'Internet, les éventuels pirates internes ne pourront accéder ni en telnet, ni en ftp aux sites externes. Cela limitera fortement leurs possibilités de nuire.
- **Interdire tout trafic avec certaines machines sensibles** et qui n'ont pas besoin de connexion Internet, comme la station IPtrafic, la station avec le logiciel de détection d'intrusions, le serveur logs, certaines machines utilisées pour des contrats de recherche sensibles, et pourquoi pas les machines de service internes telles que le serveur de calcul… Cela pourra être réalisée par filtrage sur les adresses IP. On interdit tout entrée de paquet avec comme adresse de destination l'adresse IP des machines sensibles
- **Ne « laisser entrer » les services courants et connus (messagerie, Web, …) que vers les machines de la zone semi-ouverte**, c'est à dire n'autoriser le trafic mail entrant que vers le serveur Mail sans sh de la zone semi-ouverte, Web que vers le serveur Web de la zone semi-ouverte, … et interdire ces services et tous les autres vers toutes les autres machines. N'oublions pas la politique qui est d'interdire tout ce que l'on autorise pas. Cela peut-être réalisé par du filtrage statique sur les numéros de ports et adresses IP.

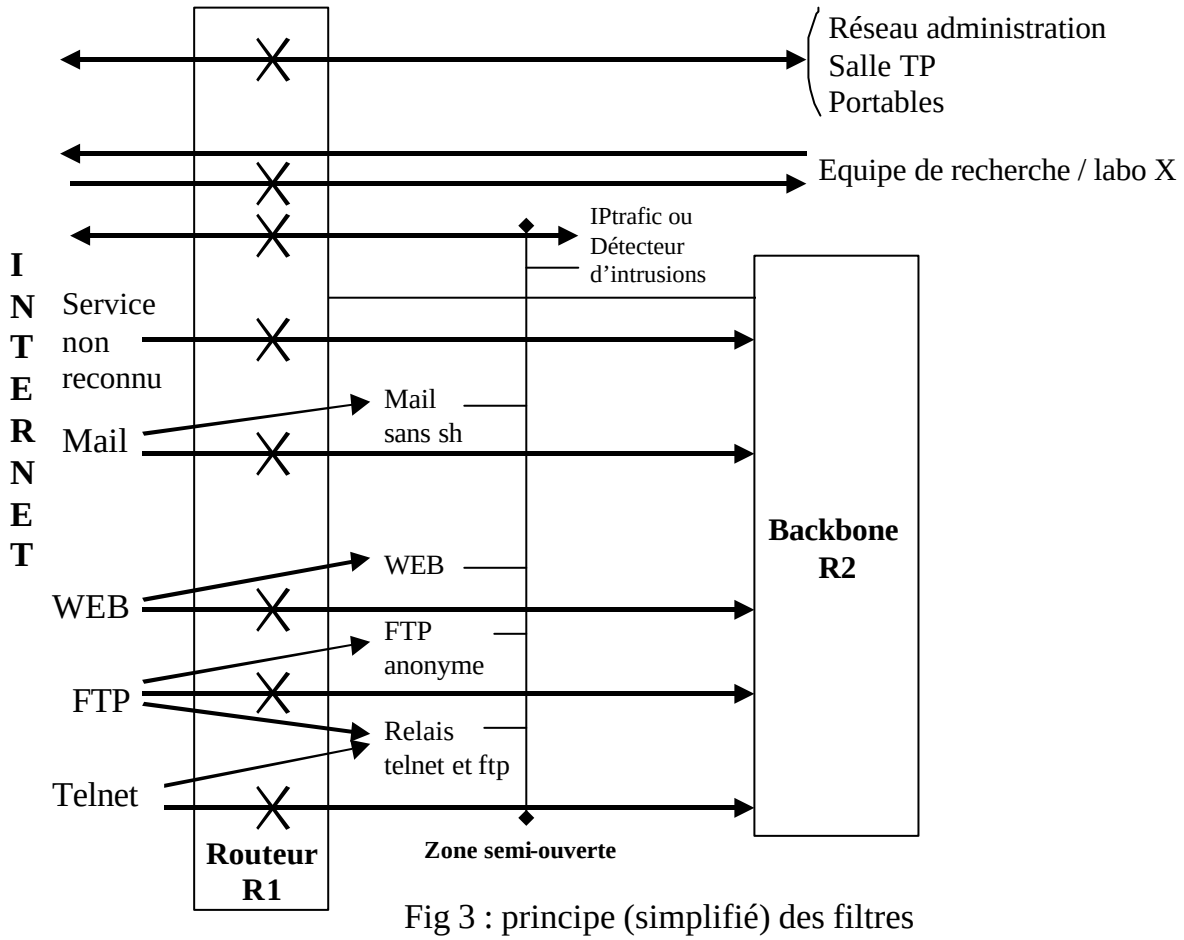


Fig 3 : principe (simplifié) des filtres

Ces filtres offrent une très grande protection mais pas à 100 % comme on pourrait le penser en première analyse. Deux vulnérabilités restent présentes :

. Le rebond : lorsque sur R1 on interdit « telnet entrant » vers une station interne S1 mais qu'on l'autorise vers une autre station interne S2, un pirate pourra d'abord se connecter sur S2 pour ensuite se connecter sur S1. Dans ce cas le filtre sur R1 aura aucun d'effet.

. Le démarrage de démons avec des ports non standard. Si un pirate est déjà dans la place, administrateur sur une station, il pourra lancer un démon *telnetd* sur un port différent de 23. Dans ce cas un accès telnet vers cette station risque de ne pas être détecté par les filtres (cela dépend de l'écriture des filtres), pour un routeur le service telnet est synonyme de port 23.

Attention, ne nous méprenons pas sur les objectifs de ces restrictions d'accès. Le but de ces filtres n'est pas de brimer les utilisateurs mais de ne laisser passer que ce qui est vraiment utile. Les besoins particuliers par exemple peuvent et doivent être pris en compte. Si une équipe de recherche à une station de son réseau interne qui doit impérativement communiquer avec une autre station externe (interactif X, calcul à distance, applications distribuées, …) on ouvrira un filtre pour permettre le dialogue. Mais on le fera de manière la plus restrictive possible, c'est à dire qu'on autorisera uniquement l'application utilisée (repérée par son numéro de port) entre deux stations (repérées par leur numéro IP).

### 2.4.2 Les filtres sur le backbone R2

**Ces filtres seront surtout destinés à protéger les différentes entités internes entre elles**. Pourquoi ? Parce qu'un groupe trop laxiste peut héberger des pirates en son sein ou avoir des machines si peu protégées que des pirates extérieurs s'y introduiront facilement sans être détectés et pourront depuis cette base attaquer d'autres machines du site (problème du rebond signalé avant).

Techniquement, l'équipement « backbone R2 » peut avoir des fonctionnalités de sécurité plus primaires que R1. Son rôle est d'abord de transporter (commuter ou router) le trafic le plus rapidement possible entre les différents sous-réseaux.

Comme filtre on peut interdire tout ou partie des communications entre entités qui ne se font pas confiance : « Administration » versus « Réseau de TP », équipes de recherche entre elles, … On peut aussi reporter une partie du filtrage décrit pour R1 sur R2 si il est trop difficile pour des raisons techniques ou d'organisation de concentrer tous les contrôles sur R1.

L'efficacité de ces filtres peut-être vérifiée avec des logiciels de simulation d'intrusions comme Internet Scanner lancés depuis l'extérieur du réseau, l'Internet, vers les machines internes. C'est un très bon test à réaliser régulièrement.

## 2.5 Et NAT ?

NAT comme Network Address Translation est un mécanisme placé généralement dans un routeur qui modifie les adresses IP dans les datagrammes. Concrètement, en sortie de site, il affecte dynamiquement des adresses aux machines clientes du site lorsque celles-ci accèdent à l'Internet. Il permet ainsi d'avoir un adressage privé quasi illimité sur le site et d'utiliser une poignée de numéros officiels pour les communications avec l'extérieur. C'est la seule solution lorsque l'on ne peut pas obtenir d'adresses IP officielles pour l'ensemble de ses machines. C'est une verrue non conforme aux principes de TCP/IP mais qui est maintenant incontournable pour certains sites vue la pénurie d'adresses.

Pour mettre en œuvre cette fonction, il faut faire l'inventaire des serveurs du site, qui doivent eux avoir toujours la même adresse statique non privée, attribuer des intervalles d'adresses aux machines clientes, … donc tout un travail de recensement et de classification des stations et des services. Avec NAT, une machine cliente du site a une adresse différente chaque fois qu'elle se connecte à l'Internet. Elle peut ainsi être très difficilement attaquable depuis l'Internet. C'est pour ces raisons que certains classent NAT dans les mécanismes de sécurité. De manière indirecte c'est exact, car il oblige à faire tout le travail de recensement des services utilisés … Mais si on fait ce travail, que l'on bâtit l'architecture décrite avant avec les filtres recommandés, NAT n'ajoute pas vraiment de protection supplémentaire.

Donc **si vous avez un manque d'adresses IP officielles pour votre site utilisez NAT mais ne l'installez pas uniquement pour des fonctions de sécurité, suivez d'abord ces recommandations**.

# 3. Bilan

## 3.1 Quelle est l'utilité d'une telle architecture ?

Actuellement, la technique la plus courante d'attaque d'un site Internet est de découvrir toutes les machines du site (par « scan »), de détecter tous les services réseaux installés sur ces machines, de tester les trous de sécurité connus de ces logiciels serveurs et enfin d'utiliser ces trous pour acquérir les privilèges d'administrateur sur les machines. Inutile d'être un expert pour réaliser ces attaques, de nombreux outils sont disponibles sur des serveurs connus et sont utilisables par n'importe quel utilisateur. Si vous n'avez pas de filtre en entrée de votre site, sans effort, ces outils détecteront des machines vulnérables chez vous et … Par contre si vous avez les filtres recommandés, les attaques n'atteindront que la poignée de machines de la zone semi-ouverte, machines correctement administrées qui seront peu vulnérables. Toutes les autres attaques vers les machines internes seront arrêtées par les filtres. Pour prendre un exemple, début 2000, le CERT Renater a publié des statistiques indiquant que les ports des applications Sendmail, rpc, DNS, NFS et http ainsi que les ports utilisés par les chevaux de Troie Back Orifice et NetBus avaient été les plus scannés en ce début d'année. Avec les filtres installés au chapitre 2, ces attaques Sendmail, DNS et HTTP n'atteindront que les serveurs de messagerie, de noms et Web de la zone semi-ouverte, serveurs correctement administrés et très surveillés, les attaques rpc, NFS, Back Orifice et Netbus n'atteindront aucune machine car filtrées sur R1.

Ainsi si des stations de réseaux internes sont peu surveillées avec une mauvaise gestion des comptes utilisateurs (vieux comptes dormants, mots de passe faibles …) ou des logiciels sans correctif de sécurité … le risque d'attaque réussie depuis l'extérieur sera très faible. En effet, avec les filtres en place, il sera impossible depuis l'extérieur d'atteindre directement ces stations. Le pirate pourra éventuellement passer par le relais telnet-FTP, mais il faudra qu'il franchisse cette barrière bien surveillée et administrée avec soin, donc très peu vulnérable.

Le problème des mots de passe sera aussi moins critique. Ainsi si un utilisateur divulgue, volontairement ou non, le mot de passe de sa station personnelle à un tiers, celui-ci ne pourra pas accéder à cette station depuis l'extérieur. Dans le même registre, si un pirate installe un sniffer (logiciel d'écoute sur un réseau) sur la zone semi-ouverte il ne découvrira pas les mots de passe des utilisateurs sur leur station de travail interne ou sur les serveurs internes. Si c'est un étudiant fait la même chose sur le sous-réseau « Salle de TP » il ne découvrira que les mots de passe des autres stations de cette salle.

De nombreuses autres protections découlent de cette architecture et de ces filtres, mais il serait trop fastidieux de les énumérer ici.

Autre avantage, la mise en place d'une telle architecture oblige à connaître le réseau et les systèmes de son site et l'utilisation qui en est faite. Et ceci est un bon point et même un pré-requis pour assurer la sécurité : **on ne protège bien que ce que l'on connaît**.

Enfin cette architecture permettra au fil du temps une intégration aisée de protections supplémentaires pour certaines communautés comme des filtres dynamiques, gardes-barrières applicatifs, logiciels de détection d'intrusions, mécanismes d'authentification forte … sans remise en cause de l'existant.

On pourrait penser que la banalisation de l'utilisation des produits de chiffrement rendra très prochainement inutile ce type d'architecture et de filtres. Il n'en sera rien.

D'abord, il va s'écouler plusieurs années avant que chaque utilisateur possède un certificat et que toutes les applications soient sécurisées. On peut même penser que une grande partie des application resteront non sécurisées. Car le déploiement mondial d'infrastructures de gestion de clés risque d'être lent et coûteux. Ceux qui ont commencé à étudier et tester les ICP (Infrastructure à Clés Publiques, alias PKI - Public Key Infrastructure, alias IGC - Infrastructure de Gestion de Clés) peuvent en témoigner.

Ensuite, même si certaines de ces applications sont sécurisées, les stations auront toujours des démons ou services réseau en attente qui auront des bogues … et répondront à des attaques comme

aujourd'hui. **L'utilisation du chiffrement ne va pas faire disparaître les vulnérabilités décrites dans ce document**.

## 3.2 Où appliquer ce modèle ?

**Le modèle proposé est à adapter à chaque environnement**.

Nous avons choisi le terme vague « site » dans ce document volontairement. Il peut désigner un campus, un groupe de laboratoires, un laboratoire, ... Sur un même site on pourra avoir plusieurs zones semi-ouvertes. Si on prend comme exemple un campus, on pourra mettre en place une seule zone semi-ouverte pour l'ensemble du campus, ou plusieurs zones semi-ouvertes, une pour chaque gros laboratoire ou groupe de laboratoires (institut, université, …). On pourra aussi avoir la réunion des deux solutions, une zone semi-ouverte en entrée de campus (serveurs pour les petites unités démunies) et autant de zones semi-ouvertes que de groupes de laboratoires qui ont leurs propres serveurs réseaux.

Pour les services il faut effectuer la même adaptation. Le but de cette architecture n'est pas de forcer les sites à centraliser tous les services réseau sur des machines de site. S'il est vrai que cette centralisation est bénéfique pour la sécurisation (limitation du nombre de stations à surveiller, …) il faut aussi tenir compte de l'existant, des compétences dans chaque entité et de la volonté de certains groupes à avoir leur propre autonomie quand ceux-ci ont les informaticiens nécessaires pour administrer les services. Ainsi sur un campus, en prenant comme exemple la messagerie, un laboratoire peut vouloir administrer son propre serveur de messagerie différent du serveur général. Ce n'est pas en contradiction avec nos recommandations si ce serveur est administré suivant les recommandations que l'on a faites, si ce serveur est placé dans une zone semi-ouverte et si les filtres sont adaptés. Dans le cas de la messagerie, une autre solution pour le laboratoire peut être de mettre son serveur de messagerie dans le sous-réseau du laboratoire et de faire transiter les messages par le serveur mail de la zone semi-ouverte du site. Donc, il ne faut pas hésiter à adapter. Par contre, il faut dans tous les cas bien discriminer pour chaque machine son type (station utilisateur, serveur réseau, serveur interne), le service qu'elle rend, la placer « au bon endroit » et le type d'exploitation à faire.

Ces choix dépendent ainsi de la présence ou non de services réseau communs à tous les laboratoires du site mais aussi d'administrateurs ou non affectés à ces services communs, l'un ne va sans l'autre.

## 3.3 Comment l'appliquer ?

Certains diront que les utilisateurs ne vont pas accepter ces changements. S'ils sont correctement mis en œuvre cela devrait être transparent pour eux.

Pour ce faire il faut dans une première phase connaître l'environnement, les entités, les serveurs, les services utilisés … Un chef d'orchestre doit avoir la vision globale de l'ensemble du site et de la sécurité à mettre en place. Mais il doit impliquer tous les administrateurs informatiques. Ainsi dès le départ, pour effectuer l'état des lieux, il doit **regrouper les administrateurs de tous les laboratoires**, de manière très officielle avec l'aval de la direction de chaque entité. Cela permettra aussi de s'assurer de l'adhésion de tous les administrateurs mais aussi des directions et en conséquence des utilisateurs.

Ce groupe **pourra ensuite définir l'architecture à mettre en place**. Il faut un objectif a atteindre mais il sera certainement préférable de **procéder pas à pas** pour y arriver lorsque cela est possible, par exemple service réseau par service réseau en terminant par le relais telnet-FTP qui implique un changement d'habitude pour les utilisateurs.

La création et l'installation des filtres pourront être réalisées par le chef d'orchestre qui devra s'engager à réagir très rapidement pour ouvrir ou fermer un service à la demande d'un laboratoire. Ce travail pourra éventuellement être réparti entre plusieurs personnes si la compétence existe, mais avec une très bonne coordination. Les filtres sont des outils puissants mais toute erreur ou incohérence peut bloquer certains services réseau.

Je recommande les deux articles de Sophie Nicoud (GLM Marseille) et de Marie-Laure Minuissi (CNRS Sophia) cités dans les références qui présentent des exemples très concrets de mise en place de filtres sur un campus.

## 3.4 Quel suivi ?

En conclusion, **cette architecture ne vous mettra pas à l'abri de toutes les attaques, mais vous protégera disons de 98% des attaques courantes**, ce qui n'est pas négligeable.

Par contre, il faut rester vigilent. La lecture régulière des avis CERTs et l'installation des correctifs permettront de maintenir les systèmes et les applicatifs des serveurs de la zone semi-ouverte dans un état sécurisé. Il sera bon **d'assurer une surveillance régulière de ces serveurs** suivant les modalités indiquées ci-avant, **mais aussi des journaux** alimentés par les rejets des paquets filtrés et les outils tels que IPtrafic.

# 4. Références

## Architecture


- La sécurité réseau du campus du GLM (Sophie Nicoud CNRS Marseille) : http://www.dr12.cnrs.fr/d12/si/sr/pub/securite/secu-info-court.htm
- Mise en place de filtre en entrée de laboratoires (Marie-Laure Miniussi CNRS Sophia) : http://www.dr20.cnrs.fr/reseau_de_campus/filtres.pdf
- Contrôle des accès au LMCP Politique et mise en oeuvre (François Mauris, Yves Epelboin, Laboratoire de Minéralogie-Cristallographie) : http://www.csiesr.jussieu.fr/pole2/lmcp/index.htm
- Mise en place d'un garde-barrière (Sylvaine Roy et Jean-Paul Eynard IBS) actes du congrès JRES99 (http://www.univ-montp2.fr/~jres99/)
- Du garde-barrière au cloisonnement de réseau (Hervé Schauer HSC) : http://www.hsc.fr/ressources/presentations/jres99/jres99001.html
- Réseaux Virtuels VLANs (Jean-Paul Gautier CNRS/UREC) : http://www.urec.cnrs.fr/cours/Liaison/vlan/sld001.htm


## Logiciels


- Tcp_wrapper : http://www.urec.cnrs.fr/securite/outils/index.html
- IPtrafic : http://www.urec.cnrs.fr/iptrafic/
- Simulation et détection, un pas de plus dans la sécurité informatique (Nicole Dausque CNRS/UREC) : http://www.urec.cnrs.fr/securite/articles/confRaid98.html
- Utilisation de produits de simulation d'intrusions (Nicole Dausque CNRS/UREC) : http://www.urec.cnrs.fr/securite/articles/actes_ND_JRES99.pdf


## Filtres


- Filtres statiques (JL Archimbaud CNRS/UREC) : http://www.urec.cnrs.fr/cours/securite/commencer/3.0.0.filtres.html
- Filtres dynamiques (Gabrielle Feltin LORIA) : http://www.loria.fr/services/moyens-info/securite/CBAC-JRES.html


## Adressage privé


- RFC1918 - Address Allocation for Private Internets : http://www.pasteur.fr/cgi-bin/mfs/01/19xx/1918


## NAT


- RFC2663 - IP Network Address Translator (NAT) Terminology and Considerations : http://www.pasteur.fr/cgi-bin/mfs/01/26xx/2663
- NAT à l'échelle d'une université (Didier Benza Univ Toulon) : http://www.univ-tln.fr/~benza/jres99/


Sans oublier les serveurs sécurité de référence pour le milieu académique français du CRU (http://www.cru.fr/Securite) et de l'UREC (http://www.urec.cnrs.fr/securite)