Evolution de l'architecture de réseau avec garde-barrière, VPN, accès distants

Marie-Claude Quidoz
UREC/CNRS
Marie-Claude.Quidoz@urec.cnrs.fr

Catherine Grenet
UREC/CNRS
Catherine.Grenet@urec.cnrs.fr

Résumé :

Dans le cadre des recommandations émises sur la sécurité des systèmes informatiques, l'UREC préconise depuis plus de cinq ans (cf. http://www.urec.cnrs.fr/securite/articles/archi.reseau.html) :

- *la mise en place d'un contrôle d'accès entre le réseau extérieur et le réseau du laboratoire*
- *la segmentation du réseau du laboratoire entre les différentes entités, avec contrôle d'accès entre les segments*

Ce document ne comportait pas de préconisation précise pour la mise en oeuvre du contrôle d'accès (filtrage « sans état », filtrage « avec états », ...) – le choix étant dépendant du matériel du laboratoire (routeur, commutateur-routeur, garde-barrière, ...). Le but de ce document était surtout de définir les segmentations à faire sur le réseau informatique du laboratoire.

Depuis cette date, de plus en plus de protocoles dynamiques (par exemple H.323) sont utilisés ; des failles ont été exploitées pour contourner le filtrage « sans état » ; de nombreuses offres de gardes-barrière offrant du filtrage « avec états » apparaissent…

Depuis cette date, de nouveaux besoins sont exprimés pour pouvoir accéder à l'informatique interne depuis l'extérieur (accès pour les nomades) ; les laboratoires sont de plus en plus éclatés sur plusieurs sites ; de nombreuses offres de VPN apparaissent…

Depuis cette date, le CNRS a commencé un déploiement des certificats dans les laboratoires…

Au vu de ces trois éléments, l'architecture sécurisée doit évoluer.

Mots clefs : architecture réseau, accès distants sécurisés, garde-barrière, VPN

1 Contexte

Lors du raccordement des laboratoires à Internet au début des années 90, concrètement 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. Le choix du « tout ouvert », au moment où il a été fait, n'était pas une erreur, mais le rester en était et en est toujours une ; c'est la raison pour laquelle l'UREC a défini, au début des années 2000, des recommandations d'architecture de réseau avec filtrages pour améliorer la sécurité [1].

Le but de ces recommandations était d'aider l'administrateur systèmes et réseaux à faire le point sur l'existant (services offerts, besoins des utilisateurs, etc.), à déterminer les segmentations à faire sur le réseau informatique du laboratoire et à définir les contrôles d'accès à mettre en place entre les segments ; l'objectif étant de diminuer le nombre de services et/ou de machines visibles depuis l'Internet et donc potentiellement vulnérables à des attaques réseau. Il ne s'agissait en aucune manière de restreindre l'utilisation professionnelle de l'Internet ; d'ailleurs, ce document contenait uniquement des conseils et des recommandations à adapter en fonction des sites et des besoins.

Dans l'article, le choix a été fait de représenter l'architecture de réseau à mettre en place de la manière suivante : une double protection (R1 et R2) pour isoler de façon plus sécurisée les données internes du laboratoire.

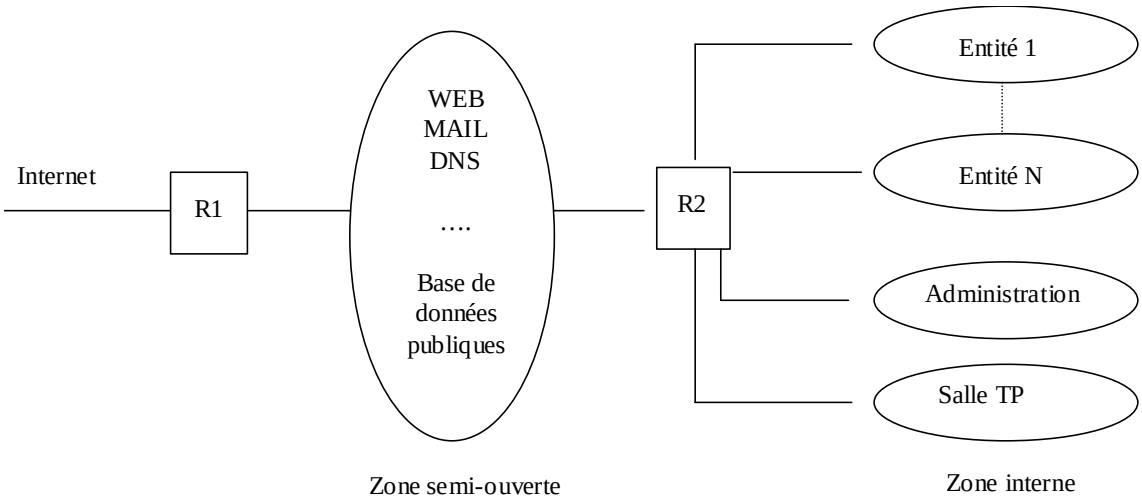

Figure 1 – *Principe de l'architecture*

Cette double protection repose sur un premier routeur R1 qui protège la zone semi-ouverte du monde Internet et sur un second routeur R2 qui protège la zone interne de la zone semi-ouverte, sachant que le routeur R2 peut être n'importe quel élément offrant du routage (routeur, commutateur niveau 3-4-5-6-7, ...). Cette architecture n'a de sens pour la sécurité que si et seulement si des mécanismes de limitation de trafic sont mis en place sur les équipements de connexion, ce qui est équivalent à dire, si et seulement si une politique de filtrage est définie et appliquée sur chacun des équipements de connexion. Dans ce principe d'architecture, la politique de filtrage « tout est interdit sauf des services que l'on connaît et maîtrise vers certaines machines » a été fortement recommandée ; par contre, aucune préconisation n'a été faite sur la mise en œuvre du contrôle d'accès, le choix étant laissé à la discrétion de l'administrateur systèmes et réseaux.

En pratique, cette architecture a été déclinée le plus souvent avec un seul routeur, parfois même avec un seul port interne, et des ACL statiques ; lors du renouvellement du matériel, il a été remplacé par un commutateur-routeur. Des exemples d'architecture sont disponibles dans les présentations [2] faites lors des opérations sécurité du CNRS, des formations SIARS, etc. (cf. exemples élaborés soit avec un seul routeur avec deux ou trois ports, soit avec un seul commutateur-routeur disposant de fonctions de réseaux virtuels « VLANS »). Cette architecture a été plus rarement déclinée avec un « garde-barrière[1] », nous reviendrons sur ce terme dans la suite de l'article, matériel que nous trouvions à l'époque coûteux en achat, gestion, … et peu performant en matière de débit.

A ce jour, le bilan suivant peut être fait :

Au fil des années, le modèle proposé a été adapté sans problème pour prendre en compte les nouveaux besoins. Ces adaptations ont été faites au niveau des services (remplacement de telnet par ssh, de pop par pops, de imap par imaps, de smtp par smtps, ajout de https, contrôleur de domaine NT, etc.).

Dans la pratique, la méthode utilisée pour la mise en œuvre du contrôle d'accès a été principalement l'utilisation des ACL « statiques », fonctionnalité disponible en standard sur la grande majorité des routeurs du marché. Cette solution, basée sur un filtrage jugé parfois « rudimentaire » (autoriser TCP si le bit ACK est positionné à 1 ; autoriser UDP > 1024), a évité à de nombreux laboratoires d'être piratés. Cependant cette situation risque de se détériorer dans le futur, si nous ne faisons rien : attaques de plus en plus sophistiquées, applications de plus en plus complexes, …

Parallèlement, sur le marché, apparaissent de plus en plus de « boîtiers de sécurité dédiés » (connus aussi sous le nom de « gardes-barrière ») qui semblent intégrer des méthodes de contrôle d'accès plus performantes et de nouvelles fonctionnalités (NAT, authentification des utilisateurs, …), le tout pour un coût non prohibitif. Faut-il investir dans ces

[1] Nous utilisons le terme « garde-barrière », mais il faut savoir que ce terme a de nombreux synonymes comme coupe-feu, pare-feu, bastion, sas, écluse, firewall, …

matériels pour améliorer la sécurité de notre réseau informatique ? C'est à cette question que nous allons essayer de vous aider à répondre dans le chapitre suivant.

2 Garde-barrière

2.1 Définition

Il existe de nombreuses définitions du terme « garde-barrière ». Pour notre part, nous retiendrons celle du RFC 2647 [3] « un garde-barrière est un dispositif permettant la mise en œuvre d'une politique de contrôle d'accès entre réseaux ». En ce sens, un routeur avec des ACL statiques est un garde-barrière ; garde-barrière de première génération comme nous le verrons par la suite.

Les différences entre les gardes-barrière se situent surtout au niveau des modes de filtrage utilisés. Nous avons choisi de présenter les différentes méthodes de filtrage de façon très synthétique ; pour une description plus exhaustive, le lecteur pourra se référer au dossier blanc de Cyberguard [4].

2.2 Modes de filtrage

La première technique est appelée « **filtre de paquets sans état** » (ou « filtre de paquets statique »). Le mécanisme de filtrage examine l'en-tête IP et l'en-tête du protocole de transport (TCP ou UDP) et décide de laisser passer ou de rejeter le paquet en fonction : des adresses IP source et destination, du protocole, des numéros de port TCP et UDP, des bits de code du segment TCP. Cette technique a l'avantage d'être peu onéreuse puisque les filtres de paquets sans état sont disponibles dans la plupart des routeurs et commutateurs-routeurs. Si les filtres ne sont pas trop nombreux, elle n'a pas d'impact significatif sur les performances ; par contre, elle oblige à laisser beaucoup de ports ouverts pour laisser passer les applications qui utilisent des ports dynamiques (sauf à interdire ces applications). De plus, le système peut devenir complexe à gérer s'il y a beaucoup de règles, car les règles sont examinées en séquence.

Parallèlement, une autre technique connue sous le nom de « **proxy** » a été proposée. Elle repose sur deux éléments : un mandataire (ou proxy) qui effectue les requêtes pour le compte d'une machine cliente (deux connexions sont établies : une entre la machine cliente et la machine mandataire, l'autre entre la machine mandataire et le serveur) et des agents spécifiques à chaque protocole applicatif ; ces derniers permettent de valider certaines commandes passées. C'est parce que cet agent est spécifique à l'application traitée qu'il permet un contrôle plus fin qu'avec un filtre de paquets : on peut par exemple interdire certaines commandes de certains protocoles applicatifs ou vérifier la conformité des paquets par rapport aux normes (ce qui permet d'éviter, par exemple, un certain nombre d'attaques de type débordement de mémoire).

Cette dernière solution offre sans conteste un très bon niveau de sécurité, à condition que les agents soient correctement écrits, c'est-à-dire qu'ils ne contiennent pas eux-mêmes de brèches de sécurité. Par contre elle ne peut traiter que les applications déjà programmées et l'impact sur les performances est non négligeable.

A la fin des années 90, la méthode de filtrage désignée par le terme « **filtre de paquets dynamique** » est apparue. Le filtrage est dit « à états » car il mémorise l'état des connexions TCP, de façon à ne laisser passer que les paquets entrants correspondant à une connexion initiée depuis le réseau interne. Une connexion est repérée par les adresses IP source et destination et les numéros de ports source et destination ; elle passe à l'état « établie » après les trois phases de la séquence de connexion. C'est la différence fondamentale avec les filtres de paquets sans état qui eux laissent passer toutes les trames TCP entrantes dont le bit ACK ou le bit RST est positionné (mot-clef *established*). Un mécanisme similaire a été mis en œuvre pour gérer les pseudo-connexions UDP.

Cette technologie est connue aussi sous le nom de « **stateful inspection** » (marque déposée par la société CheckPoint). C'est la technologie de base retenue par la majorité des constructeurs de garde-barrière actuellement. Cependant, même si presque tous les gardes-barrière disponibles sur le marché sont étiquetés « stateful inspection », ils n'offrent pas tous la même qualité de protection ; certains améliorent le filtrage en ajoutant une vérification des numéros de séquence TCP ; d'autres ajoutent des passerelles applicatives[2] très sophistiquées ; une explication détaillée de la puissance des passerelles

[2] Terme employé pour désigner des applications qui interceptent les connexions entrantes et sortantes, qui examinent le contenu du paquet (y compris les données) et qui décident de le laisser passer ou de le rejeter en fonction des règles définies par l'administrateur, sans réécrire les adresses (à la différence des « proxy »).

applicatives est disponible [5]. Mais comparer les subtilités entre les différentes propositions commerciales n'est pas l'objet de cet article[3].

En résumé, nous pouvons classer les gardes-barrière en quatre catégories (ou générations) :

- première génération : filtre de paquet sans état
- deuxième génération : proxy
- troisième génération : filtre de paquet à états
- quatrième génération : passerelles applicatives

Cette dernière génération est rarement citée dans la littérature, mais il nous a semblé important de faire la distinction entre les deux dernières générations. Bien que toutes les deux reposent sur des filtres de paquets à états et intègrent des passerelles applicatives, la dernière génération offre un traitement bien plus sophistiqué que la précédente qui se contentait de traiter les seules applications de type FTP.

Actuellement, le meilleur compromis sécurité / performance est offert par les gardes-barrière de quatrième génération, qui apportent un meilleur niveau de sécurité sans restreindre l'utilisation des réseaux. Ceci est essentiellement dû au mécanisme d'ouverture dynamique des ports TCP et UDP, qui permet de laisser passer certaines applications sans ouvrir complètement les ports correspondants (alors que le filtre de paquets sans état ne laisse le choix qu'entre ouvrir de grandes plages de ports ou interdire l'utilisation de l'application). Un niveau de sécurité supplémentaire, non négligeable, est apporté par l'analyse du contenu des paquets pour les protocoles les plus utilisés. Actuellement, la tendance est à développer de plus en plus de modules applicatifs, ce qui certes augmente le niveau de protection, mais qui risque à terme de nous ramener à des problèmes similaires à ceux des *proxies* : failles de sécurité au niveau des passerelles, impact sur les performances.

Comme nous l'avons vu, les différences entre les gardes-barrière se situent surtout au niveau des modes de filtrage utilisés mais il serait abusif de réduire un garde-barrière à un simple élément de filtrage ! Dans la réalité, un garde-barrière offre de nombreuses autres fonctionnalités, dont certaines, par définition, sont dans tous les gardes-barrière : authentification des utilisateurs, gestion des traces, facilité de configuration, …

2.3 Autres fonctionnalités

Les gardes-barrière peuvent intégrer d'autres fonctionnalités annexes, comme la gestion de NAT, l'authentification des utilisateurs, une passerelle anti-virus, la gestion des VPN, le contrôle des URL, la haute disponibilité, ... Ces fonctionnalités sont d'ailleurs souvent plus mises en avant par les commerciaux que celles propres aux méthodes de filtrage !

La majorité de ces fonctionnalités [6] sont utiles dans notre environnement, mais est-il nécessaire qu'elles soient toutes regroupées dans la même boîte ? Ne vaut-il pas mieux les répartir sur des équipements indépendants ? Actuellement, il semblerait que les constructeurs aient choisi. D'ailleurs dans les offres commerciales, le terme garde-barrière a tendance à être remplacé par celui de « boîtier de sécurité dédié ». S'agira-t'il d'un effet de mode ou d'une solution pérenne, l'avenir nous le dira. Nous pensons que le « boîtier de sécurité dédié » n'est pas la solution pour la grande majorité de nos laboratoires, exception faite peut-être des laboratoires sans informaticien système et réseau ; ce qui ne signifie pas que les fonctionnalités offertes ne soient pas intéressantes (par exemple, mettre un anti-virus sur un serveur de messagerie est très fortement conseillé).

2.4 Insertion dans le réseau

Les premiers gardes-barrière fonctionnaient tous comme des routeurs, c'est-à-dire qu'ils transféraient les paquets entre des réseaux IP distincts. Ensuite on a vu apparaître des gardes-barrière pouvant fonctionner comme des ponts Ethernet, c'est-à-dire qu'ils retransmettent les trames Ethernet d'une interface sur l'autre sans modification. Le terme commercial qui désigne ce mode de fonctionnement pour un garde-barrière est « transparent », en référence au « pont transparent » d'autrefois. L'avantage de ce mode de fonctionnement est qu'on peut insérer le garde-barrière dans le réseau sans aucune modification de celui-ci. Dans la suite, nous parlerons de « routeur » et de « pont ».

2.5 Faut-il acquérir un garde-barrière ?

[3] Des fiches synthétiques sont en cours de rédaction par un groupe de travail ; ces fiches sont consultables sur le site de l'UREC https://www.services.cnrs.fr/ars/ pour tous les membres du CNRS ayant en leur possession un certificat de l'autorité de certification du CNRS.

Historiquement, la fonction de garde-barrière dans les laboratoires du CNRS a été mise en œuvre à l'aide de « filtres de paquets sans état » disponibles sur de nombreux éléments de routage, routeurs ou commutateurs-routeurs et dans de nombreux systèmes d'exploitation libres utilisés dans notre environnement.

Cette solution a tendance à assimiler deux fonctionnalités bien distinctes : le routage et le filtrage ; normalement le rôle d'un routeur est de router les paquets IP et celui d'un garde-barrière est de contrôler l'accès au réseau local, éventuellement de faire du contrôle d'accès entre les différents segments du réseau local. L'intégration de ces deux fonctions dans un même équipement est tout à fait logique et a donné jusqu'à présent de bons résultats en termes de sécurité : un système de filtres sans état bien conçu, avec une politique de sécurité de type « tout est interdit sauf... », donne, d'après notre expérience, un niveau de sécurité tout à fait satisfaisant à l'heure actuelle. En d'autres termes, si vous avez adopté ce système et qu'il vous donne satisfaction, ne vous précipitez pas pour en changer ...

En revanche, si vous n'avez pas de contrôle d'accès à l'entrée de votre laboratoire ou si vous n'êtes pas satisfait du système en place, faut-il pour protéger votre informatique : acquérir un garde-barrière, acquérir un routeur ayant des capacités de filtrage évoluées, acquérir un routeur et un garde-barrière, demander au service qui vous offre la connexion au réseau Internet de vous offrir un filtrage ?

La première réponse qui vient à l'esprit est « qu'importe le moyen pourvu que votre laboratoire soit mieux sécurisé ! » ; cette réponse a l'air d'une boutade, mais il ne faut pas surestimer les risques encourus dans notre environnement et il faut prendre conscience qu'un équipement de cette catégorie n'est qu'un élément parmi d'autres pour assurer la sécurité de votre laboratoire. Par exemple, à quoi sert d'avoir un équipement ultra-sophistiqué si la politique de sécurité appliquée est « tout est autorisé sauf … » ?

La réponse à cette question doit être vue d'une part en fonction des besoins de routage (statique, dynamique, …), de filtrage (applications standard, applications « maison », …), d'autre part en fonction de votre équipement actuel et des moyens dont vous disposez. L'intégration d'un garde-barrière dans une architecture déjà existante n'est pas anodine ; elle dépend de la méthode avec laquelle vous êtes connecté au réseau Internet : par un simple commutateur Ethernet relié sur le routeur du campus, par un routeur propre, par un commutateur-routeur, … et du mode de fonctionnement du garde-barrière (mode routeur, mode transparent).

En conclusion, la méthode à suivre avant d'installer un garde-barrière en entrée du réseau du laboratoire pourrait être la suivante :

1. Faire l'inventaire des applications utilisées de façon à s'assurer de leur bon fonctionnement à travers le garde-barrière. En effet le traitement de certains protocoles nécessite l'utilisation de passerelles applicatives. Si FTP est intégré dans la quasi-totalité des produits, ce n'est pas le cas de H.323 par exemple.

2. Choisir le point d'insertion du garde-barrière dans le réseau et son mode de fonctionnement, routeur ou pont. Ces choix dépendent à la fois :
   - des caractéristiques de la connexion du laboratoire au réseau extérieur : type d'équipement et protocoles utilisés
   - de l'architecture du réseau interne : réseau segmenté ou non, avec ou sans zone semi-ouverte...

3 Evolution des besoins

Depuis quelques années, les besoins évoluent dans notre environnement ; dans leur grande majorité, ils sont connus depuis longtemps, par exemple, accéder à ses fichiers depuis son domicile. Dans la majorité des cas, des réponses techniques existent aussi, construire un VPN par exemple. Quelques solutions ont été mises en place dans les laboratoires pour offrir un accès VPN nomade mais ceci de façon assez parcellaire, par exemple, uniquement pour une poignée d'utilisateurs.

Une des raisons de la non-généralisation de ces solutions provient du fait qu'elles remettent en cause les recommandations d'architecture de réseau qui avaient été faites. Des adaptations sont donc nécessaires, c'est ce que nous verrons dans la quatrième partie de cet article. Mais auparavant nous allons passer en revue les besoins en indiquant pour certains les réponses possibles.

3.1 Nomadisme

De plus en plus d'utilisateurs désirent accéder aux ressources internes depuis l'extérieur des laboratoires. Au début, c'était principalement pour accéder à leur messagerie ou à l'intranet du laboratoire ; besoins « assez simples » à satisfaire grâce à l'utilisation de l'application SSH ou d'applications « SSLisées », associées aux certificats numériques [7]. Maintenant, de plus en plus d'utilisateurs souhaitent accéder à tout le système d'information du laboratoire ; en un mot, ils souhaitent bénéficier des mêmes services de l'extérieur du laboratoire que de l'intérieur et cela quel que soit l'endroit d'où ils se connectent (domicile, hôtel, autre laboratoire, …) voire même quel que soit le matériel avec lequel ils se connectent (portable, poste fixe, …).

Des éléments de réponse[4] aux besoins « simples » ont déjà fait l'objet d'une présentation aux Journées Réseaux 2001 [8]. Cependant dans cette présentation, nous n'avions pas abordé les changements qu'il fallait opérer au niveau de l'architecture du réseau afin d'intégrer en toute sécurité ces services ; nous allons y remédier dans le chapitre suivant. Concernant les besoins plus complexes, une réponse possible est la mise en place d'un réseau privé virtuel (VPN, *Virtual Private Network)*, qui est un tunnel sécurisé, c'est-à-dire authentifié et chiffré, entre le nomade et son laboratoire. Si l'extrémité du tunnel côté poste nomade est évidente, le problème n'est pas aussi simple pour l'autre extrémité : où doit-être localisée la terminaison dans le réseau du laboratoire ? En d'autres termes, le serveur de VPN doit-il être intégré au garde-barrière ? Si au contraire il s'agit d'un équipement dédié, où faut-il le placer par rapport au garde-barrière ?

3.2 Translation d'adresse

Lors de la connexion des laboratoires à Internet au début des années 90, nous avons affecté à toutes nos machines des adresses publiques et cela sans nous poser de questions ; nous disposions d'un nombre « infini » d'adresses IP et de peu de machines. Dix ans après, la situation a changé, les adresses sont attribuées au compte-gouttes et le nombre de machines a explosé. Le recours à l'adressage privé est devenu obligatoire, et par voie de conséquence l'utilisation de la translation d'adresses (NAT) est devenue indispensable pour beaucoup des laboratoires.

3.3 Segmentation

De façon identique, au début des années 90, lors de la mise en place des réseaux informatiques dans les laboratoires, nous nous sommes peu préoccupés des différentes populations présentes et tout le monde était ami. Au fil des années, les amis ne sont pas devenus des ennemis, mais le développement de l'informatique a fait que de plus en plus de données confidentielles sont maintenant traitées / stockées sur les postes informatique, par exemple les sujets de concours, la gestion d'un laboratoire. Il est donc devenu indispensable de segmenter notre réseau en sous-réseaux thématiques.

D'autres faits sont également à noter ; certains ont trait à des changements dans les habitudes de travail des utilisateurs : augmentation du nombre d'ordinateurs portables, dont l'état de santé laisse parfois à désirer, développement du sans-fil ; d'autres ont trait à des changements au niveau des attaques virales et de leurs méthodes de propagation, par exemple, le récent virus Blaster qui se propage par des RPC. Pour éviter qu'une attaque ne devienne une catastrophe, la solution est aussi de segmenter le réseau.

En résumé, il existe beaucoup de raisons de segmenter son réseau : en matière de performance pour diminuer le nombre de broadcast et pour des questions d'administration pour isoler plus facilement les dysfonctionnements, mais attention cependant à ne pas segmenter à l'infini.

3.4 Interconnexion de sites distants

De nos jours, le nombre de laboratoires répartis sur plusieurs lieux géographiques augmente. Dans quelques années, cela peut même devenir courant, avec des utilisateurs travaillant indifféremment dans un lieu ou un autre.

La solution se doit d'être totalement transparente pour l'utilisateur final ; l'utilisateur doit avoir à distance les mêmes fonctionnalités que celles qu'il aurait sur le réseau local ; par exemple, il ne doit pas avoir de crainte par rapport au transport de ses données confidentielles. Ce besoin étant assez analogue à celui exprimé par les nomades, à quelques différence près, la solution risque d'être basée sur la même technologie, c'est-à-dire la mise en place de tunnels sécurisés.

[4] Des fiches synthétiques sont disponibles sur le site de l'UREC https://www.services.cnrs.fr/corres-secu/ pour tous les correspondants sécurité du CNRS ayant en leur possession un certificat de l'autorité de certification du CNRS.

4 Réponses possibles

Nous allons maintenant essayer d'apporter quelques éléments de réponse aux questions précédentes et de présenter les choix possibles pour intégrer ces évolutions lorsqu'on conçoit l'architecture d'un réseau.

4.1 Nomadisme

Un certain nombre de laboratoires ont ouvert aux utilisateurs nomades le service SSH et/ou ont offert un petit nombre de services fonctionnant sur SSL/TLS. Où doit-on placer les machines qui hébergent ces services dans le schéma d'architecture réseau de la Figure 1 ? Si possible, pas dans la zone semi-ouverte car elles doivent être protégées des machines qui hébergent les services Internet. Il n'est pas non plus souhaitable de les installer dans la zone des serveurs internes car ce sont des machines ouvertes sur l'extérieur. La meilleure solution nous semble donc de créer un nouveau segment destiné aux machines accessibles par authentification forte.

La mise en place d'un service de VPN sur IP pour les accès distants suppose qu'on ait préalablement réfléchi aux questions suivantes :

Premièrement, quelles adresses va-t-on affecter aux machines distantes ? On peut choisir de les mettre dans un sous-réseau IP distinct ou de leur affecter des adresses prises dans une plage d'un sous-réseau du laboratoire. L'avantage de la première solution est qu'elle permet de distinguer facilement les machines distantes des machines locales. Le choix de l'un ou de l'autre a des conséquences sur le routage : dans le premier cas il faut une route vers le sous-réseau distant, dans le second cas le serveur de VPN fait du *proxy ARP* pour le compte des machines distantes.

Deuxièmement, veut-on contrôler l'accès aux ressources du laboratoire pour le client distant ou bien le laisser accéder à l'ensemble du réseau interne ? Ce point est important en termes d'architecture car les flux dans le tunnel sont chiffrés et ne peuvent être analysés qu'à la sortie du tunnel, après déchiffrement. Le plan d'adressage doit être aussi considéré de ce point de vue, car il est plus facile de filtrer sur un numéro de réseau que sur une liste d'adresses.

Troisièmement, comment les machines distantes vont-elles accéder à l'Internet lorsque le tunnel est établi ? Elles peuvent le faire soit par l'accès Internet du laboratoire soit par le réseau public. La première solution présente l'avantage d'empêcher les attaques par rebond[5] mais a l'inconvénient d'obliger les flux à transiter deux fois par le réseau du laboratoire et à être chiffrés et déchiffrés inutilement.

Certes, il ne faut pas surestimer le risque lié aux utilisateurs distants : le même utilisateur qu'on considère aujourd'hui comme un danger potentiel pour le réseau du laboratoire parce qu'il se trouve en Patagonie reviendra demain matin dans son laboratoire et connectera son portable dans le sous-réseau dédié à son équipe. Néanmoins, nous pensons que le fait d'utiliser un sous-réseau IP distinct, de se réserver la possibilité de filtrer les accès (même si on ne l'utilise pas dans un premier temps) et d'interdire le *split tunneling* sont des mesures dont il serait dommage de se priver si leur coût est marginal : il sera probablement plus difficile de les mettre en place après coup si elles n'ont pas été prévues au départ.

Parallèlement, et comme toujours en matière de sécurité, il faut sensibiliser les utilisateurs aux risques associés aux nouveaux services offerts et les inciter à installer un pare-feu personnel sur les portables et les postes de travail à domicile.

4.2 Translation d'adresses

NAT a été conçu pour pallier le manque d'adresses IP et non comme un mécanisme de sécurité. Sa mise en place impose de faire un travail de recensement des services qui doivent être accessibles de l'extérieur pour classer les machines en deux catégories : celles qui doivent être accessibles depuis l'Internet (les serveurs), à qui on affectera une adresse publique fixe, et celles qui n'ont pas besoin de l'être et qui auront une adresse publique affectée dynamiquement (les machines clientes). Par construction, toutes les connexions des machines clientes devront obligatoirement être initiées de l'intérieur : ce n'est qu'au moment de l'initialisation de la connexion que l'équipement qui gère le NAT attribue à la machine une adresse publique. L'association adresse privée/adresse publique doit rester constante pour la durée d'une connexion. Pour cela, l'équipement qui gère le NAT embarque ce que nous avons appelé un « filtre de paquets à états », qui lui permet d'une part, dans le sens sortant, d'attribuer à une machine la même adresse publique pour toute la durée de la connexion, d'autre part, dans le sens entrant, de traduire l'adresse destination pour que le paquet arrive à la machine à laquelle il est destiné. Il

[5] Intrusion dans le réseau du laboratoire par une méthode contre laquelle le laboratoire est protégé par son garde-barrière, mais pas la machine distante

embarque également des passerelles applicatives pour traiter certains protocoles « à problèmes » comme FTP (les protocoles à problèmes sont ceux qui utilisent des numéros de port négociés dans la partie données des paquets).

On voit donc d'une part qu'il y a beaucoup de similitudes de fonctionnement entre la fonction NAT et celle de garde-barrière ; d'autre part que la translation d'adresse constitue un mécanisme de protection pour les machines clientes, puisqu'elles sont inaccessibles depuis l'extérieur.

Du point de vue de l'architecture du réseau, la translation d'adresse nécessite la mise en place de deux DNS : le DNS externe qui répond aux requêtes externes et le DNS interne qui répond aux requêtes internes. Le DNS externe sera placé dans la zone semi-ouverte et le DNS interne dans la zone des serveurs internes.

Quant à la fonction NAT elle-même, où la placer ? Cette fonctionnalité existe sur les routeurs, les gardes-barrière et sur certains commutateurs-routeurs. Mais il y a deux raisons d'effectuer la translation d'adresses sur le garde-barrière plutôt qu'ailleurs. C'est plus efficace, inutile de faire subir aux paquets des traitements analogues sur deux équipements différents et surtout, souvent plus simple : les gardes-barrière sont très souvent configurés par défaut pour faire du NAT.

4.3 Segmentation

La segmentation physique du réseau s'est souvent révélée difficile dans notre environnement, les membres d'une même équipe ou d'un même service étant souvent répartis aléatoirement dans les locaux. Ce problème a été résolu avec l'apparition des VLAN, qui ont permis de segmenter les réseaux de manière logique et non plus physique. La norme IEEE 802.1Q [9] permet d'affecter un VLAN à chaque port d'un commutateur Ethernet et donc à chaque prise réseau, indépendamment de l'architecture physique. La mise en œuvre d'une segmentation fine demande une très bonne connaissance de son réseau (quelle machine est connectée à quelle prise ?) ; cet investissement s'avère rentable seulement si les machines ne se déplacent pas trop. Les réseaux sans fil peuvent être intégrés de cette manière : pour minimiser les risques qui leur sont liés, on pourra les mettre dans un VLAN spécifique, avec des filtres tels qu'ils n'aient qu'un accès restreint au réseau du laboratoire.

La généralisation des ordinateurs portables pose des problèmes spécifiques. Il est fortement recommandé de mettre les portables des visiteurs dans un VLAN à part, mais comment faire ? Avec le seul mécanisme du VLAN par port, il faut que seules certaines prises leur soient accessibles et les autres verrouillées, sur l'adresse MAC par exemple ; mais cela alourdit la tâche de l'administrateur et restreint la mobilité de l'utilisateur. Une solution intéressante est d'utiliser l'authentification IEEE 802.1X [10]. Ce mécanisme permet d'affecter de manière dynamique un VLAN à un port en fonction du résultat d'une authentification : on pourra ainsi faire en sorte que les machines inconnues soient dans un VLAN par défaut, ce qui permettra de contrôler ce à quoi elles peuvent accéder. Par ce biais, d'autres problèmes liés à la mobilité peuvent être résolus : dans une même salle de réunion, un visiteur peut être connecté au VLAN visiteur et un permanent connecté sur le VLAN de son équipe[6]. Pour une description du protocole 802.1X, on pourra se reporter à [11].

4.4 Interconnexion de sites distants

Les questions à se poser avant d'interconnecter deux sites distants au moyen d'un VPN IP sont analogues à celles que suscite la mise en place de VPN pour l'accès distant (l'interconnexion de plus de deux sites pose des problèmes supplémentaires qui ne seront pas abordés dans le cadre de cet article). Il faut d'abord définir un plan d'adressage unique pour l'ensemble des sites. Ensuite définir une politique de contrôle d'accès entre les sites. Et enfin décider si l'accès Internet sera centralisé ou si chaque site aura son accès propre.

En ce qui concerne l'adressage, il est préférable qu'il n'y ait pas de sous-réseau réparti entre les sites. Cela permettra de connaître immédiatement la localisation d'une machine et facilitera la mise en place d'une politique de contrôle d'accès, qui sera définie en fonction de l'organisation du laboratoire (ce pourra être : il n'y a pas de contrôle d'accès !). Le choix de l'accès Internet se fera en comparant les avantages de la solution centralisée (facilité de gestion...) aux inconvénients qu'elle génère (pas d'optimisation de l'utilisation de la bande passante...).

[6] Il existait déjà un mécanisme similaire, les VLAN par adresse MAC. Outre qu'il est moins sûr, ce mécanisme présente l'inconvénient de ne pas être normalisé.

5 Proposition d'architecture réseau

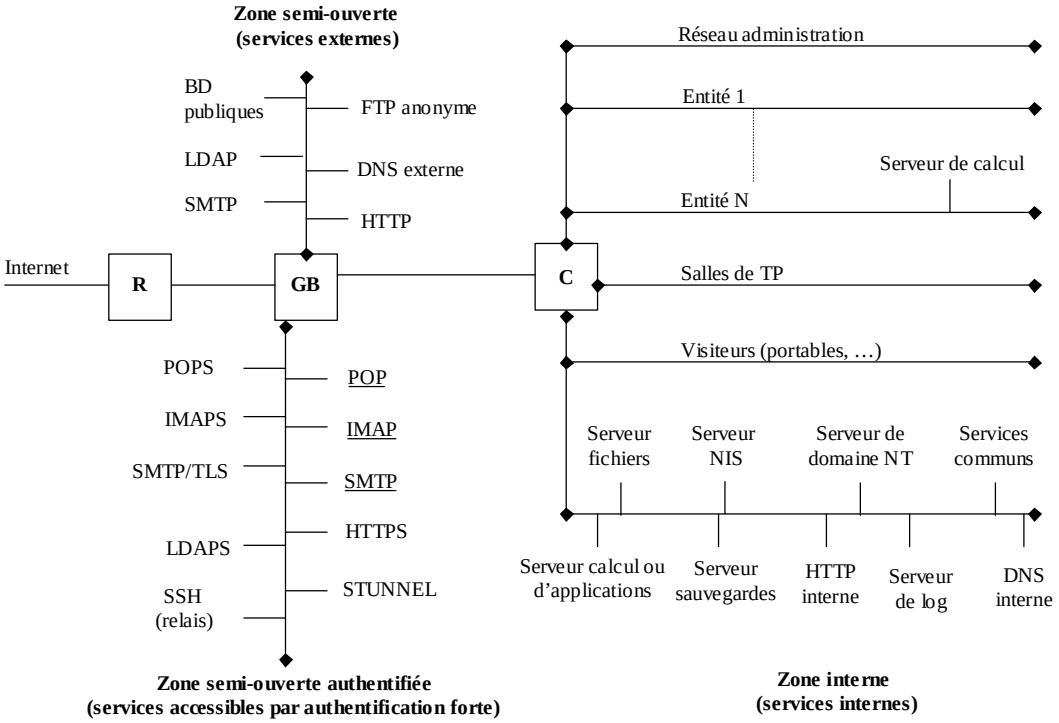

Figure 2 – *Nouvelle architecture réseau*

L'architecture de réseau proposée, très proche de celle diffusée il y a cinq ans, présente avec elle les différences suivantes :

- l'ajout d'un boîtier garde-barrière dédié
- le découpage du DNS en deux : un DNS interne et un DNS externe
- le découpage de la zone semi-ouverte en deux zones : une zone semi-ouverte et une zone semi-ouverte authentifiée

Dans cette nouvelle architecture, la zone semi-ouverte regroupe les services totalement ouverts sur Internet et accessibles par tous au contraire de la zone semi-ouverte authentifiée qui offre des services nécessitant une authentification forte à des populations ciblées (par exemple, la messagerie pour les membres du laboratoire, un intranet pour les correspondants sécurité, ...) et cela indépendamment de leur localisation. Comme le montre la figure 2, ces services sont majoritairement des services s'appuyant sur le protocole SSL/TLS offrant ainsi les services de base en sécurité (authentification du serveur et/ou du client, confidentialité et intégrité des données échangées). C'est dans cette zone que nous conseillons de mettre le service SSH. C'est dans cette zone aussi que les services de messagerie seront installés ; ces services seront accessibles de l'extérieur avec le protocole SSL et en interne éventuellement sans le protocole SSL ; ainsi quelle que soit la localisation, l'utilisateur aura accès à sa boîte aux lettres.

Pour accéder à sa messagerie, une autre réponse pourrait être d'utiliser des tunnels VPN pour accéder de façon sécurisée à la zone interne du réseau informatique ; ainsi localisées, les boîtes aux lettres, données assez sensibles par définition seraient plus en sécurité. Mais faire ce choix implique de limiter la consultation de sa boîte aux lettres à ce seul outil ; cette solution est difficilement généralisable dans notre environnement, pour des raisons de coût et d'habitudes de travail. Cependant, attention à ne pas faire de fausses interprétations à partir de cet exemple ; dans ce cas, le VPN n'est pas la solution, mais il l'est si votre ordinateur est connecté depuis un réseau sans fil dans un environnement non sécurisé et que vous souhaitez utiliser des applications non « SSLisées ». Il l'est aussi si vous souhaitez bénéficier des mêmes services de l'extérieur du laboratoire que de l'intérieur.

Le serveur de VPN n'est pas représenté sur ce schéma, car cette fonction peut être effectuée par un routeur, un garde-barrière, ou bien un équipement dédié. L'intégration de cette fonction dans le routeur ou le garde-barrière présente deux avantages :

- simplification du routage : tout est géré à l'intérieur du routeur ou du garde-barrière, il n'y a pas d'impact sur les autres équipements réseau
- possibilité de filtrer le trafic en sortie du tunnel (le filtrage est assuré par le routeur ou le garde-barrière)

Mais, pour des raisons de fonctionnalités ou de performance, on peut vouloir utiliser un boîtier dédié. Dans ce cas, si on veut pouvoir faire du contrôle d'accès en sortie des tunnels on le placera comme sur la figure 3 : les flux en clair peuvent alors être filtrés par le garde-barrière. Cette configuration a également l'avantage de limiter les modifications induites sur le routage : seuls le routeur et le garde-barrière ont à connaître les routes supplémentaires. Pour une présentation détaillée des éléments à prendre en considération voir [12].

6 Quelques exemples pratiques

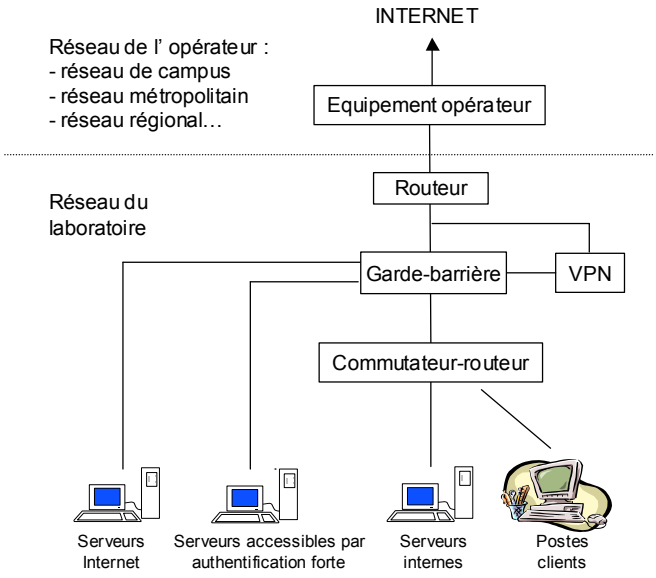

Figure 3 – *Architecture réseau*

Dans l'environnement des laboratoires du CNRS, pour des raisons d'organisation ainsi que de moyens financiers et humains, il est rarement possible d'appliquer le schéma classique représenté Figure 3. Cela n'est pas non plus souhaitable, en particulier dans les petites structures pour lesquelles une telle architecture est manifestement surdimensionnée. Nous allons examiner dans la suite, sur des exemples concrets pris dans des laboratoires du CNRS, comment mettre en oeuvre les fonctions de garde-barrière et de serveur de VPN dans un réseau existant. A noter que ces exemples d'une part sont des cas-types et ne prennent pas forcément en compte toute la complexité d'une situation réelle ; d'autre part que nous avons choisi délibérément de modifier le moins possible l'architecture existante, car on n'a pas toujours, même si c'est regrettable, la possibilité de reconstruire intégralement son réseau.

6.1 Intégration d'un garde-barrière dans un réseau non segmenté

Nous avons choisi de présenter deux cas : un laboratoire connecté par un commutateur Ethernet et un laboratoire connecté par un routeur IP à 2 ports**.**

Exemple 1 : laboratoire connecté par un commutateur Ethernet

Si le laboratoire dispose d'un sous-réseau IP en propre, il peut installer un garde-barrière soit en mode pont, soit en mode routeur, entre le commutateur Ethernet d'entrée du laboratoire et le routeur extérieur (voir Figure 4). En mode pont, aucune modification de l'adressage IP n'est nécessaire. En mode routeur, il faut créer un sous-réseau d'interconnexion entre le

garde-barrière et le routeur extérieur. Le choix sera fonction de la facilité de mise en oeuvre[7] comparée aux fonctionnalités supplémentaires apportées par le routage (translation d'adresse par exemple). Une bonne façon de procéder peut être de commencer par une phase de validation où on installe le garde-barrière en mode pont et où on met en place les filtres, avant de passer en mode routeur, sachant que beaucoup d'équipements peuvent fonctionner dans les deux modes.

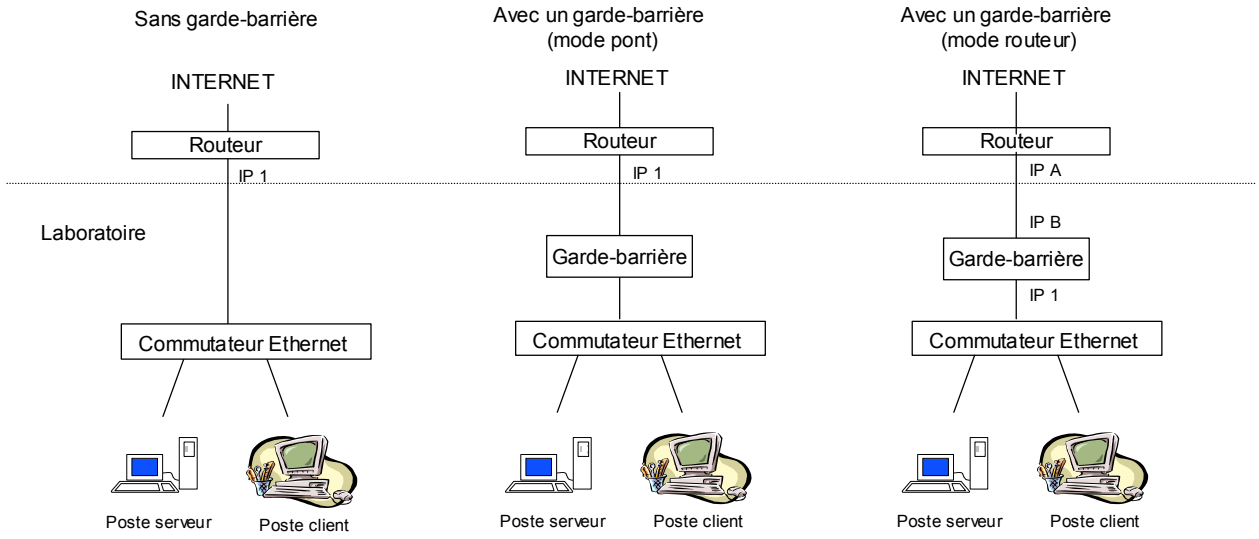

Figure 4 – *Laboratoire connecté par un commutateur Ethernet*

Remarque : si le laboratoire ne dispose pas d'un sous-réseau IP en propre (cas d'un laboratoire intégré dans une structure plus grande mais voulant appliquer sa propre politique de sécurité), la seule solution est d'installer un garde-barrière en mode pont.

Exemple 2 : laboratoire connecté par un routeur IP à 2 ports

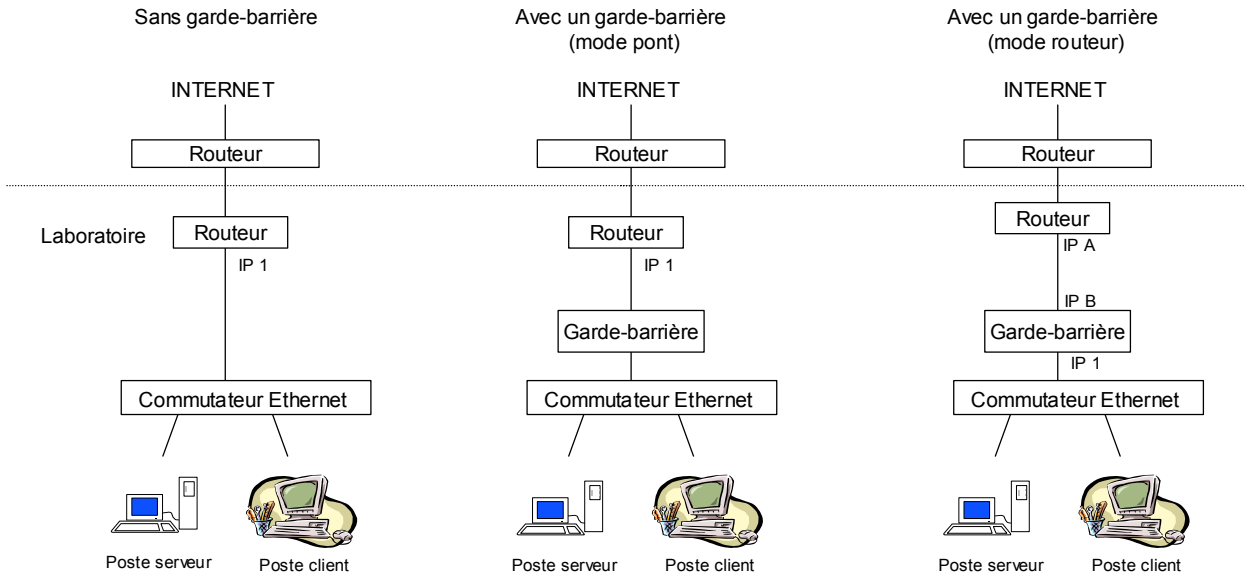

Figure 5 – *Laboratoire connecté par un routeur IP à 2 ports*

[7] Un garde-barrière en mode pont peut être installé et enlevé très rapidement si ça ne marche pas

Le garde-barrière peut être facilement inséré entre le routeur et le commutateur Ethernet raccordé à celui-ci, en mode routeur ou en mode pont (voir Figure 5). On peut également envisager de ne conserver que le garde-barrière en entrée du réseau si celui-ci intègre les fonctionnalités de routage nécessaires à l'interconnexion du laboratoire avec l'extérieur (routage statique, RIP, OSPF...), et si l'opérateur l'accepte.

Il existe toujours la possibilité d'installer sur le routeur un module logiciel « garde-barrière ». Dans ce cas, l'équipement initial peut suffire.

6.2 Intégration d'un garde-barrière dans un réseau segmenté

Nous avons choisi de présenter trois cas, selon que le laboratoire est connecté par un routeur IP multiport, un commutateur-routeur Ethernet/ IP ou un commutateur Ethernet avec transport de VLAN.

Exemple 1 : laboratoire connecté par un routeur IP multiport

Dans la configuration initiale, représentée à gauche de la Figure 6, le routeur sert à router et filtrer les paquets entre l'extérieur et le laboratoire, mais aussi entre les différents segments du réseau du laboratoire. S'il est possible de placer un garde-barrière en face de l'équipement de l'opérateur, le garde-barrière pourra être installé en entrée du réseau (schéma central Figure 6). Il pourra être équipé d'une troisième interface dédiée à la zone semi-ouverte. Le garde-barrière assurera alors la protection entre le réseau extérieur et le réseau du laboratoire, ainsi qu'entre le réseau interne et la zone semi-ouverte. Les segments du réseau interne seront isolés les uns des autres par le routeur. On peut aussi choisir de conserver le routeur en entrée du réseau et d'installer derrière un garde-barrière équipé du nombre d'interfaces nécessaires (schéma de droite Figure 6).

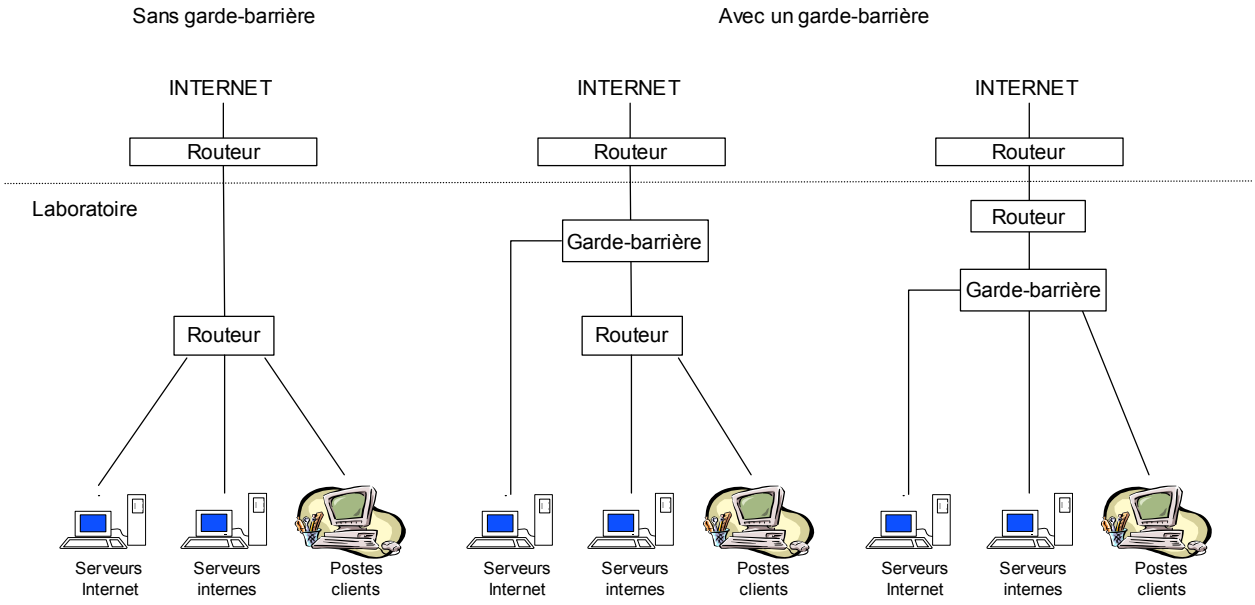

Figure 6 – *Laboratoire connecté par un routeur IP multiport*

Il existe toujours la possibilité d'installer sur le routeur un module logiciel « garde-barrière ». Dans ce cas, l'équipement initial peut suffire.

Exemple 2 : laboratoire connecté par un commutateur-routeur Ethernet/IP

Cette configuration présente des points communs avec la précédente. Suivant un schéma analogue, on pourra placer le garde-barrière en entrée du réseau, soit en mode pont, soit en mode routeur. En mode pont, si on veut placer les serveurs Internet sur une interface du garde-barrière, il faut soit changer leur numéro IP, soit changer celui des serveurs : c'est la raison pour laquelle on a préféré les laisser sur le commutateur-routeur. Par contre, en mode routeur, on peut choisir de les connecter sur une interface du garde-barrière ou du commutateur-routeur.

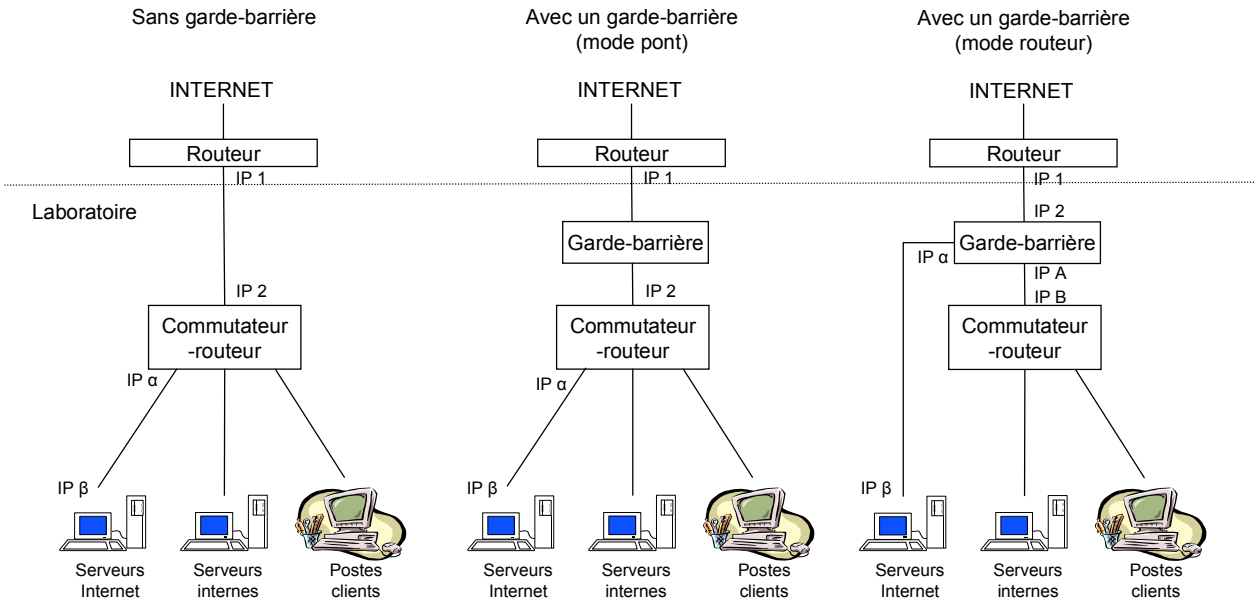

Figure 7 - *Laboratoire connecté par un commutateur-routeur Ethernet/IP*

Exemple 3 : laboratoire connecté par un commutateur Ethernet

Dans ce cas le routage entre les différents segments est assuré par un commutateur-routeur à l'extérieur du laboratoire (voir Figure 8). Si on ne veut pas modifier en profondeur l'architecture et qu'on veut malgré tout mettre en place en entrée du laboratoire un filtrage qu'on ne peut pas faire effectuer sur le routeur extérieur, il est possible d'insérer un garde-barrière en mode pont entre le commutateur Ethernet et le commutateur-routeur externe si le garde-barrière transporte les VLAN 802.1Q.

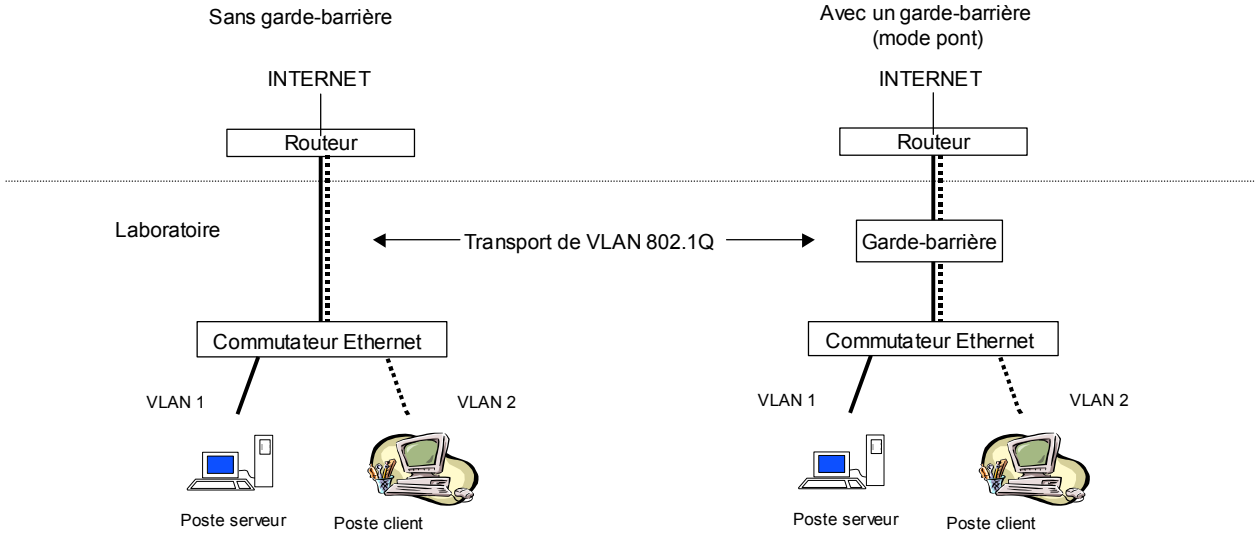

Figure 8 – *Laboratoire connecté par un commutateur Ethernet*

7 Conclusion

Tout au long de cet article, nous avons adopté le point de vue d'un laboratoire du CNRS, mais beaucoup de choses sont transposables à un institut, une école ou une université. Certains besoins n'ont pas été pris en compte. L'accès aux grilles de calcul par exemple pose deux problèmes : d'une part, les machines doivent être accessibles à la fois depuis l'intérieur du laboratoire et depuis l'extérieur ; d'autre part, les applications utilisées sont des applications « maison » qui négocient les numéros de port dans la partie données des paquets. Nous n'avons pas non plus intégré de machines IPv6 dans notre architecture réseau, ni abordé le problème de la de visioconférence.

Dans cet article, nous avons essayé d'apporter des réponses pour améliorer la sécurité du réseau du laboratoire ; c'est un élément très important, mais il ne faut pas oublier qu'une architecture construite à base de garde-barrière, VLAN et VPN n'est d'aucun secours en cas de vol physique d'une machine, vol qui peut être lourd de conséquences pour les recherches conduites au sein de notre organisme.

Références

[1] Archimbaud Jean-Luc, Recommandations d'architecture de réseau avec filtrages pour améliorer la sécurité, janvier 2000, http://www.urec.cnrs.fr/securite/articles/archi.reseau.pdf

[2] Archimbaud Jean-Luc et Quidoz Marie-Claude, Architecture de réseau sécurisée, octobre 2002, https://www.urec.cnrs.fr/securite/corres-secu/Architecture_securisee.pdf

[3] RFC 2647 : Benchmarking Terminology for Firewall Performance, http://www.ietf.org/rfc/rfc2647.txt?number=2647

[4] Paul Henry, An examination of firewall architectures, August 2001, http://www.cyberguard.com/pdf/Solutions_Whitepapers1.pdf

[5] Application Intelligence, Whitepaper, 2003, http://www.checkpoint.com/products/downloads/appint_whitepaper_fr.pdf

[6] Quidoz Marie-Claude, Synthèse de la réunion garde-barrière, mars 2003, https://www.services.cnrs.fr/ars/Garde-barriere/Synthese-reunion-garde-barriere.pdf

[7] Archimbaud Jean-Luc, Certificats (électroniques), pourquoi ? comment ?, décembre 2000, http://www.urec.cnrs.fr/securite/articles/certificats.kezako.pdf

[8] Quidoz Marie-Claude, Accès distants sécurisés : un essai de bilan des solutions possibles, JRES2001, Lyon, décembre 2001, http://www.urec.cnrs.fr/securite/articles/JRES01.ADS.pdf

[9] IEEE Std 802.1Q-1998, Virtual Bridged Local Area Networks, March 1999

[10] IEEE Std 802.1X-2001, Port-Based Network Access Control, July 2001

[11] Saccavini Luc, Le protocole IEEE 802.1X, vCARS 2003, Autrans, mai 2003, http://www.urec.cnrs.fr/securite/CNRS/vCARS2003/DOCUMENTS/saccavini.pdf

[12] Why choose integrated VPN/Firewall solutions over stand-alone VPNs, Whitepaper, 2003, http://www.checkpoint.com/products/downloads/why_choose_integration.pdf