PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction scientifique et technique
Laboratoire Technologies de l'Information

PROBLÉMATIQUE D'INTERCONNEXION DES RÉSEAUX IP

Version 1.9

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP - Tél 01.71.75.80.19 - Fax 01.71.75.80.40

Suivi des modifications

1.9	18/03/2004	Version diffusée (suppression des références nominatives, modification de mise en page)
1.8	23/05/2003	Version diffusée
1.7	14/05/2003	Version modifiée suite aux commentaires internes.
1.6	07/05/2003	Version de validation.
1.4	07/05/2003	Version de travail. Modifications suite aux commentaires internes. Suppression des descriptions d'IP. Gestion de configuration.
1.1	19/12/2002	Version initiale diffusée en interne

Table des matières

Table des figures

1 Introduction

Ce document introduit une réflexion sur les problèmes posés par les interconnexions de réseaux IP de politiques de sécurité différente. Il distingue un réseau "interne" *a priori* maîtrisé d'un réseau "externe" sur lequel il n'est pas fait d'hypothèse. On suppose par contre qu'une politique de sécurité de cette interconnexion a été réalisée au préalable. Cette politique doit avoir identifé les flux autorisés à traverser l'interconnexion, ainsi que les objectifs éventuels d'authentification forte de ces derniers. Ce document propose des architectures d'interconnexion pouvant être utilisées dans la conception de passerelles ou d'équipements intégrés. Il est présenté dans le cadre du premier forum sur les interconnexions de réseaux à titre d'introduction à cette problématique de protection aux limites d'enclaves et ne constitue en l'état qu'un document de travail pour lancer le travail d'identification d'architectures génériques et modulables.

2 Problématique générale

2.1 Cas d'école

Les problèmes d'interconnexions interviennent toujours entre deux systèmes d'information entre lesquels doit exister un certain cloisonnement. Il s'agit, par exemple, de la connexion d'un réseau local (LAN) à un réseau étendu (WAN) par une liaison (cf. figure 1). Les exigences naturelles dans ce type de situation sont que les flux sortants et entrants soient contrôlés. En particulier, certaines informations du réseau local sont considérées comme privées et ne doivent donc pas être accessibles de l'extérieur. Inversement, il peut être interdit par la politique du réseau local d'accéder à certaines données sur le réseau étendu[1].

Par souci pédagogique, nous allons nous concentrer sur le protocole HTTP qui est majoritairement utilisé sur l'Internet pour la consultation et la mise à disposition de données. Notre hypothèse de base est que seul le réseau local est sous contrôle. Le réseau étendu est considéré par hypothèse comme non sûr, c'est-à-dire, en particulier, qu'il n'y a aucune garantie de respect des protocoles de communication usuels sur l'interface réseau local – réseau étendu.

La politique de sécurité voulue dans notre cas d'école est que le réseau étendu ne doit pouvoir accéder qu'aux données explicitement autorisées au niveau local. Inversement, le réseau local peut accéder à toutes les données disponibles sur le réseau étendu (l'Internet) à l'exception des données interdites. Il y a là une dissymétrie imposée par l'hypothèse de travail. En effet, nous supposons qu'il n'est pas possible d'imposer au réseau local de n'accéder qu'à des données explicitement autorisées, puisque l'origine des données issues du réseau étendu ne peut être garantie. Dans ces conditions, on ne peut qu'interdire *a posteriori* l'accès à certains sites une fois qu'ils ont été identifiés, en espérant (vœu pieux) que ces sites ne changeront pas.

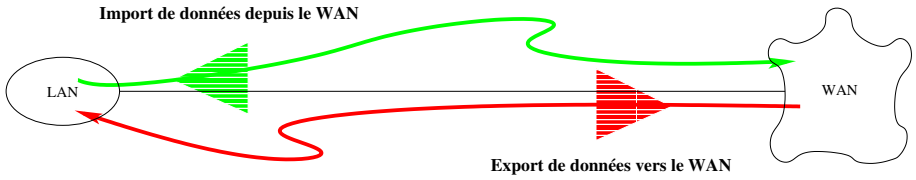

FIG. 1 – Cas d'école

Le flux vert de la figure 1 est donc un flux de consultation HTTP sortant. Le flux rouge est quant à lui le flux de consultation entrant sur le ou les serveurs du réseau local.

[1] Par exemple, des données issues de sites reconnus comme piégés.

Il est important de bien comprendre que ces deux flux sont techniquement réalisés par des communications généralement bi-directionnelles. Dans ces deux cas, des paquets de données sont échangés dans les deux sens et non uniquement dans le sens indiqué par la flèche.

Pour fixer les idées, dans le cas du protocole HTTP qui utilise le protocole TCP, le sens de la petite flèche indique uniquement le sens du premier paquet d'initialisation de connexion (SYN)[2]. Au contraire, le transfert d'information utile se fait en sens inverse de l'établissement de la connexion[3] comme indiqué par la grosse flêche grisée.

Dans toute la suite un flux sortant est donc réalisé à l'initiative du réseau "interne". Un flux entrant est quant à lui initié par "l'extérieur".

2.2 Analyse des causes de vulnérabilités potentielles

L'émission et la réception de données se font par l'intermédiaire d'un protocole de communication. Ce protocole est implanté des deux côtés de la transmission, mais rien ne garantit le respect des spécifications protocolaires. Or le comportement d'une implantation par rapport à des entrées non conformes n'est pas toujours satisfaisant. Dans certains cas, l'envoi de données incorrectes peut provoquer des erreurs, voire permettre à un attaquant de s'introduire sur la machine réceptrice.

Par ailleurs, les spécifications elles-mêmes sont souvent soumises à interprétation. Or la possibilité de réaliser une même opération de plusieurs façons différentes ouvre des possibilités de transmission par des canaux cachés.

Dans un premier temps, nous allons donc chercher à garantir deux propriétés au niveau du réseau local pour les données entrantes et sortantes :

1. Les données sont conformes à un protocole spécifié.
2. Les données sont toujours codées de façon déterministe, c'est-à-dire que les éventuelles imprécisions possibles du protocole sont traitées à chaque instant de la même façon.

Ces deux propriétés sont nécessaires mais largement insuffisantes pour garantir la sécurité d'une interconnexion.

[2]Dans le cas du protocole HTTP, la première requête applicative se fait dans le même sens que l'établissement de la connexion TCP. Ceci n'est pas toujours vrai.

[3]Il peut néanmoins arriver que des informations circulent aussi dans le sens de la connexion initiale, par exemple lors du choix d'un lien à cliquer ou lors de l'envoi du contenu d'un formulaire.

3 Architectures d'interconnexion

3.1 Connexion directe

La connexion directe du réseau local sur le réseau étendu est techniquement faisable. C'est même cette solution qui va offrir les meilleures performances en matière de bande passante. Toutefois, même s'il s'avère possible d'héberger sur une même machine à la fois le client qui va butiner sur le réseau étendu et le serveur qui offre au réseau étendu les données publiques du réseau local, on observe très rapidement que la séparation des deux fonctions sur des machines différentes offre de nombreux avantages (cf. figure 2).

En effet, du point de vue des performances, celles du client ne sont pas affectées par les requêtes venues de l'extérieur. D'autre part, du point de vue de la sécurité, si le client est compromis, les données sur le serveur public ne sont pas immédiatement modifiables (ceci dépend du contrôle effectué au niveau du serveur). Inversement, si le serveur est compromis les données du client quant à elles ne le sont pas, en théorie.

Cette séparation permet de concentrer au niveau du serveur les données publiques et fait apparaître un autre flux de mise à jour des données du serveur depuis le client. Ce flux est de nature différente des précédents. Il nécessite une authentification du client par le serveur pour éviter que les données publiées ne soient altérées par un tiers non autorisé.

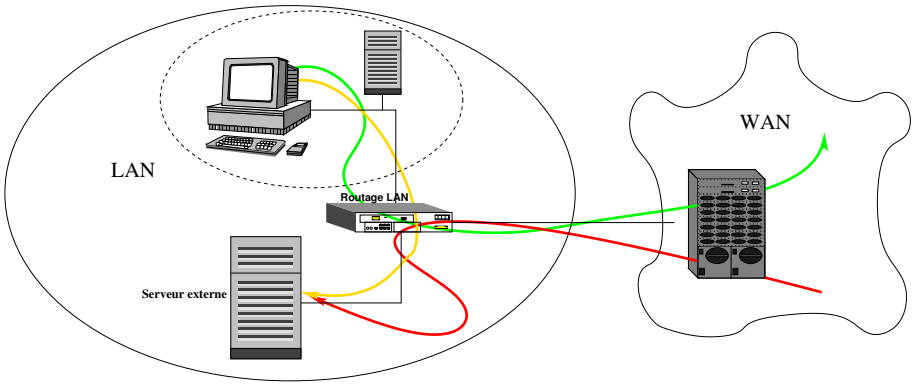

FIG. 2 – Connexion directe

La figure 2 fait clairement apparaître que dans cette architecture, la majeure partie de la sécurité repose sur le système de routage du réseau local. Si ce dernier n'est pas sûr, alors le cloisonnement est immédiatement remis en cause. Il est donc intéressant de poursuivre la logique de séparation des fonctions de base de ce cloisonnement pour en déduire une architecture d'interconnexion plus sûre.

3.2 Séparation des fonctions de base

Le protocole HTTP de notre cas d'école s'appuie sur le protocole TCP. Il est donc intéressant d'utiliser une architecture qui va séparer les traitements au niveau IP et TCP de ceux du niveau applicatif HTTP. En outre, nous allons aussi pouvoir séparer les outils de traitement de chaque flux. On obtient ainsi une architecture de type DMZ[4] avec des filtres de paquets TCP/IP qui assurent l'aiguillage des flux vers un serveur de délégation (proxy) pour le flux sortant et le serveur interne pour le flux entrant[5].

En ajoutant la distinction entre le routage vers l'extérieur et le routage interne du LAN on obtient ainsi l'architecture de la figure 3.

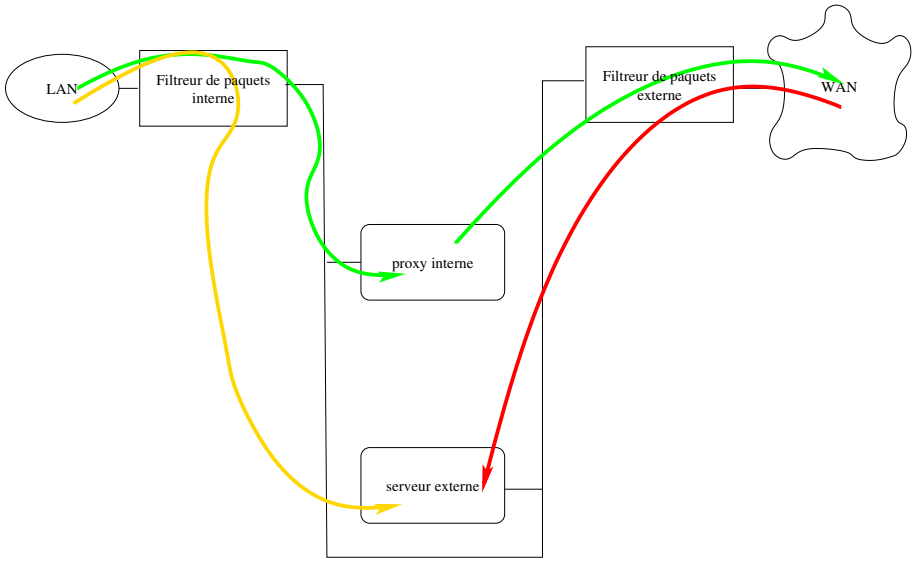

FIG. 3 – Zone franche

Cette architecture peut toutefois être encore améliorée en introduisant une certaine redondance pour accroître la robustesse vis-àvis de l'hypothèse de compromission d'un élément. Plus exactement, si le serveur a une vulnérabilité, celle-ci peut être exploitée. La séparation de la fonction opérationnelle de la fonction de contrôle permet dans une certaine mesure de pallier cette difficulté. Ainsi, on séparera le serveur proprement dit, mis à jour depuis le réseau local, d'un filtre applicatif externe qui vérifiera la cohérence et la conformité de la session HTTP. De même, pour accélérer la consultation des pages du réseau externe, on distinguera un service de cache local du service de délégation comportant les règles de filtrage des requêtes vers l'extérieur (cf.figure 4).

[4] *De-Militarized Zone*, en français "zone franche".

[5] La notion de flux entrant et sortant est celle définie au paragraphe 2.1.

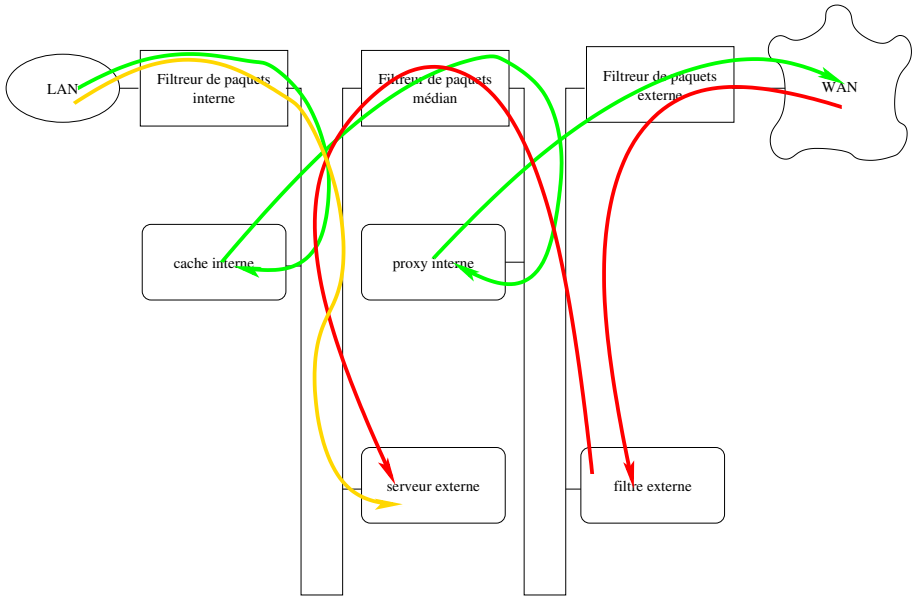

FIG. 4 – Séparation des fonctions de base

Cette nouvelle architecture est complétée par un troisième filtre de paquets qui va cloisonner la partie vérification de la partie fonctionnelle. Ainsi, les deux DMZ créées n'auront pas d'interaction directe possible. Mais cette architecture présente encore l'inconvénient de reposer sur les filtres de paquets pour réaliser le cloisonnement. Une modification de l'architecture est donc à envisager pour que chaque fonctionnalité soit effectivement en coupure, rendant l'ensemble de l'architecture d'interconnexion robuste.

L'architecture de la figure 5 suppose que chaque serveur, cache, proxy ou filtre applicatif est configuré en coupure, c'est-à-dire avec deux adresses distinctes[6]. En fait, les produits du commerce de type "firewall" peuvent être utilisés à la place de chacune des composantes de cette architecture d'interconnexion. Toutefois, l'emploi de fonctions redondantes ne prend pleinement son sens que si celles-ci sont assurées par des équipements différents.

Il est à noter que beaucoup de passerelles d'interconnexion actuelles hébergent tout ou partie de ces différentes fonctions dans un ou deux équipements. Cette situation est par nature moins robuste du point de vue de la sécurité. Toutefois, si l'équipement adopte en interne un cloisonnement logiciel et/ou matériel suffisant il est alors possible de le considérer en remplaçant potentiel de tout ou partie de l'architecture proposée. C'est ainsi que l'architecture de la figure 5 peut aussi être envisagée pour la conception interne d'équipements d'interconnexion.

[6]Bien entendu, les éléments de type proxy ou cache ne doivent pas router le trafic au niveau IP, puisqu'ils travaillent au niveau applicatif.

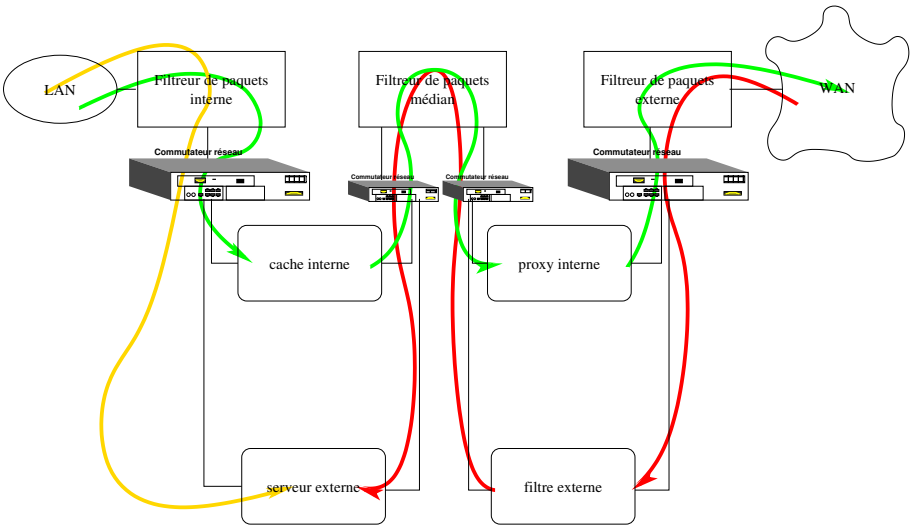

FIG. 5 – Séparation optimale des fonctions de base

4 Discussion sur les architectures d'interconnexion

4.1 Généralités

L'architecture proposée initialement (cf. figure 5) a pour principal avantage de faire reposer la sécurité à chaque niveau protocolaire sur au moins deux équipements. Bien entendu, ceci ne présente d'intérêt que dans la mesure où ces équipements sont différents. L'objectif recherché est de rendre plus difficile une attaque indétectable en réduisant le risque d'une attaque exploitable sur deux équipements différents. Une attaque reste toutefois toujours possible. En particulier, l'implantation d'un cheval de Troie sur le réseau interne reste envisageable. Toutefois, l'utilisation de canaux cachés pour interagir de l'extérieur avec ce programme malin est rendue plus difficile par une normalisation systématique des protocoles. La prise de contrôle de l'un des équipements de la passerelle d'interconnexion ne donne pas non plus d'avantage irréversible à l'attaquant puisque celui-ci reste tributaire des contrôles d'au moins un autre équipement. La prise de contrôle de cet équipement en redondance revient à effectuer une attaque qui doit se dérouler à l'intérieur du périmètre de sécurité des deux DMZ. Il est donc naturel d'implanter dans cet environnement maîtrisé un système contrôlant de façon indépendante la normalité des échanges, ce qui s'avère une tâche plus aisée que de réaliser de la détection d'intrusion au niveau d'un réseau local[7]. Le but ici est moins de détecter des attaques connues que de disposer d'un outil d'alerte sur des réactions anormales du réseau d'interconnexion qui peuvent être l'indice d'une attaque inconnue.

4.2 Administration

L'administration des différents équipements est bien entendu un problème à envisager ; il doit même faire l'objet d'une étude à part entière. En effet, pour une passerelle gérant de nombreux protocoles et des quantités de flux importantes, une administration centralisée paraît indispensable à la bonne détection des anomalies. Cette administration centralisée s'avère aussi nécessaire pour assurer la cohérence des configurations des équipements. Mais le risque est aussi très grand que cette administration devienne le maillon faible de tout le système. En effet, si une faille de sécurité de l'un des équipements permet de prendre la main sur le système d'administration, alors tout l'édifice de sécurité peut s'effondrer. Il est donc important, là encore, d'assurer une certaine redondance.

En toute rigueur, il faut distinguer dans l'administration les flux de configuration et de remontée d'informations, notamment alarmes, qui sont de nature différente et doivent être traités sur des circuits différents. Les flux de configura-

[7] La détection d'intrusion au niveau du réseau local reste indispensable, ne serait-ce que pour se protéger des attaques internes, mais ce n'est pas l'objet de cette étude.

tion doivent être authentifiés par chaque équipement. Les remontées d'information doivent être authentifiées par l'équipement de collecte de ces informations. La remontée d'information doit notamment permettre de contrôler la configuration de l'équipement et de garantir sa cohérence avec le reste du système.

Il est prudent de considérer un réseau d'administration physiquement isolé du réseau opérationnel. En effet, dans le cas contraire, la panne ou l'attaque d'un équipement du réseau opérationnel pourrait constituer un déni de service sur l'administration et nuire gravement à la sécurité de la passerelle.

4.3 Cas des VPN

Il est courant d'intégrer dans une passerelle d'interconnexion des fonctionnalités d'accès distants pour d'autres réseaux LAN ou des postes nomades. Les données qui transitent par ces réseaux privés sont de nature différente de celles qui sont publiées sur Internet. Elles sont toutefois aussi *a priori* différentes de nature de celles présentes sur le LAN. Un mécanisme de mise à disposition explicite des données internes doit donc être mis en place à destination de ces réseaux. Par ailleurs la branche de réseau VPN doit être distincte de la branche publique (cf. figure 6).

Bien que présentée ici dans le cas d'un chiffrement IPSEC, cette séparation de flux s'applique aussi pour d'autres VPN (SSL, SSH, etc.) voire des flux non nécessairement chiffrés (IPSEC en mode d'authentification AH seul, par exemple).

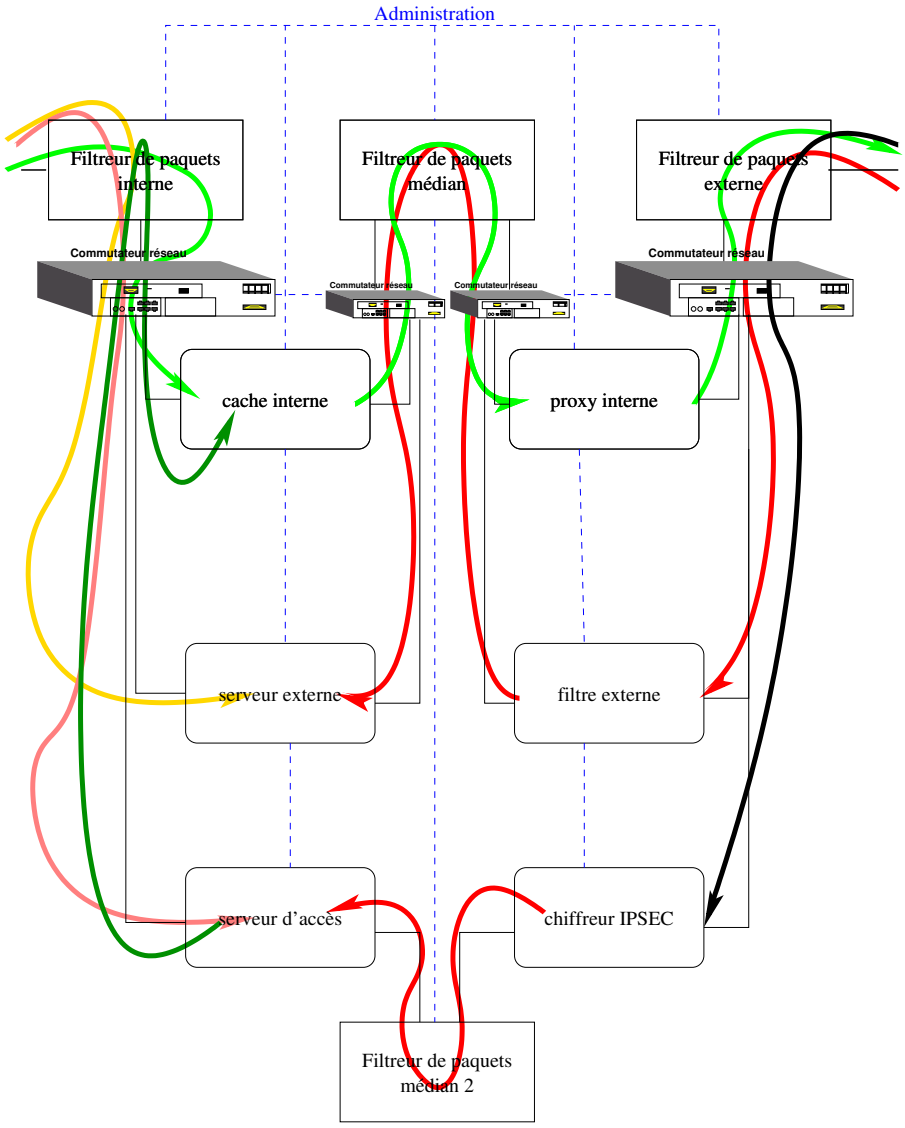

FIG. 6 – Architecture complète

5 Conclusion

L'interconnexion de réseaux IP fait apparaître la nécessité d'une architecture d'interconnexion permettant de séparer les fonctions élémentaires nécessaires à l'interconnexion. Ces fonctions se répartissent à tous les niveaux protocolaires pour garantir un comportement "normal" du réseau. La définition de cette normalité découle à la fois de considérations techniques générales (protocoles utilisés) et de la politique de sécurité définie. Il est du ressort de l'administrateur de la passerelle d'interconnexion d'administrer en conséquence (et en cohérence) ses différents équipements.

Il paraît intéressant, pour étudier une telle passerelle, de la considérer par comparaison aux fonctions élémentaires regroupées dans l'architecture représentée figure 6. Il est toutefois évident que chaque passerelle d'interconnexion peut adopter une architecture d'interconnexion différente de celle proposée, qui rappelons-le, résulte de l'étude d'un cas d'école. Il conviendra donc d'étudier en fonction de chaque cas particulier l'architecture qui présente le meilleurs compromis.

Les équipements d'interconnexion, quant à eux, peuvent réaliser tout ou partie des fonctions élémentaires identifiées en utilisant les principes d'architecture proposés de façon logicielle ou matérielle.