

# Comment concilier contrôle d'accès et qualité de service dans les réseaux de type IP sur ATM ?

Olivier PAUL<sup>\*</sup>, Maryline LAURENT, Sylvain GOMBAULT  
ENST de Bretagne  
2 rue de la châtaigneraie - BP 78  
35512 CESSON Cedex - France  
Email: {paul/mlaurent/gombault}@rennes.enst-bretagne.fr

## Résumé

Dans cet article nous décrivons une nouvelle architecture fournissant le service de contrôle d'accès dans les réseaux de type ATM et IP sur ATM. Cette architecture est basée sur des agents distribués dans les équipements du réseau. Il est bien connu que la distribution rend le processus de gestion plus difficile. Afin de résoudre ce problème nous proposons une architecture permettant d'assurer une configuration efficace de nos agents de contrôle d'accès. La comparaison avec d'autres approches montre que notre architecture apporte des améliorations importantes en terme de contrôle d'accès au niveau ATM, de capacités à supporter les facteurs d'échelle et de respect de la qualité de service.

## Mots clef

Contrôle d'accès, Gestion, Sécurité, ATM, Agents, IP sur ATM.

## Abstract

In this article, we describe a new architecture providing the access control service in both ATM and IP-over-ATM networks. This architecture is based on agents distributed in the network equipment. It is well known that distribution makes the management process more difficult. This issue is raised and we provide an architecture to configure our access control agents efficiently. The comparison with other approaches shows that this architecture provides big improvements in ATM-level access control, scalability and QoS preservation.

## Keywords

Access Control, Management, Security, ATM, Agents, IP-over-ATM.

## 1 Introduction

La technologie ATM a été spécifiée pour assurer le transport de flux de natures diverses ayant des exigences variées en terme de QoS (qualité de service). Les communications sont orientées connexion, celles-ci étant établies, contrôlées et fermées au moyen d'un protocole de signalisa-

---

\*. Ce travail est financé par une bourse DRET.

tion. Dans cet article nous montrons que l'approche classique pour assurer le service de contrôle d'accès (appelée firewall) peut empêcher le réseau ATM de respecter ses engagements en terme de QoS.

Après avoir exposé les solutions actuellement proposées pour résoudre ce problème, nous présentons chapitre 3 une nouvelle architecture de contrôle d'accès pour les réseaux de type ATM et IP sur ATM. Cette solution tout en apportant des améliorations vis à vis des solutions actuelles, assure le respect de la qualité de service des connexions établies. Cette architecture se base sur l'utilisation d'agents distribués dans les équipements du réseau.

Un des problème principaux de ce type d'architecture est sa gestion. Nous présentons donc chapitre 4 et chapitre 5 une architecture de gestion permettant une gestion automatique et efficace de notre architecture de contrôle d'accès.

Pour conclure, nous présentons dans le chapitre 6 une comparaison de notre architecture avec les autres approches et montrons quelles pistes intéressantes s'offrent pour la poursuite de notre travail.

## 2 Autres propositions

Plusieurs solutions ont été proposées afin de fournir une certaine forme de contrôle d'accès dans les réseaux de type ATM et IP sur ATM. Cette partie est divisée en trois paragraphes. Dans le premier nous montrons les limites de l'application de la solution classique du «firewall» au contrôle d'accès dans les réseaux ATM. Dans un second paragraphe, nous montrons comment l'ATM Forum a pris en compte ces limites. Nous décrivons enfin dans une troisième partie les solutions proposées afin d'améliorer la solution du «firewall».

### 2.1 Solution classique

La solution la plus évidente pour réaliser le contrôle d'accès dans les réseaux ATM est d'utiliser un firewall ([Ran92]) entre le réseau à protéger et le réseau public non sûr. Cette solution permet le contrôle d'accès aux niveaux paquet, circuit et application. Dans ce cas, le réseau ATM est considéré comme une couche de niveau 2 dans le modèle OSI permettant l'établissement de connexions point à point. Deux connexions sont établies, l'une entre le firewall et l'équipement interne et l'autre entre le firewall et l'équipement externe. Avec ce type d'outil, le contrôle d'accès au niveau ATM n'est pas possible et la QoS associée aux connexions ATM n'est pas garantie.

Au niveau IP et au niveau circuit, les paquets IP sont réassemblés à partir des cellules ATM et le contrôle d'accès est réalisé au moyen des informations contenues dans les en-têtes des paquets IP, TCP et UDP. Les paquets sont filtrés en comparant des champs comme les adresses et les ports source et destination, la direction des paquets et les drapeaux TCP avec une description des paquets autorisés. Les paquets non autorisés sont détruits alors que les paquets autorisés sont transférés d'un réseau à l'autre. Lorsque la même QoS est négociée de part et d'autre du firewall, la qualité de service de bout en bout peut être affectée de la manière suivante :

- Les opérations de réassemblage, de routage et de fragmentation augmentent le délai de transit des cellules (CTD).

- Les opérations effectuées sur les informations transmises peuvent augmenter le taux de perte de cellule (CLR).
- Le temps passé à réassembler et fragmenter les paquets est proportionnel à leurs tailles. Celle-ci étant variable, la gigue dans le délai de transfert des cellules (CTDV) peut être modifiée.
- Les actions de routage et de filtrage se faisant de manière logicielle, la charge du système peut introduire des modifications dans les débits crête et moyen.

Les actions au niveau application sont filtrées au niveau applicatif par des logiciels appelés proxies. Comme aux niveaux IP ou circuit, la QoS est perturbée, mais de manière plus importante car le trafic est examiné au niveau application. De plus comme le filtrage se fait généralement dans un environnement multitâche, des désynchronisations peuvent se produire entre les flux filtrés.

Un dernier problème introduit par ce type d'architecture est son incapacité à supporter des débits importants. Plusieurs études ([JA98], [KL98]) ont montré que ce type d'architecture ne pouvait fournir pour le moment le service de contrôle d'accès de manière satisfaisante à la vitesse d'un lien OC-3 (155 Mb/s).

## 2.2 Le contrôle d'accès selon l'ATM Forum

Le service de contrôle d'accès tel qu'il est défini par les spécifications de l'ATM Forum ([SEC10]) est une extension du service de contrôle d'accès tel qu'il est considéré dans les systèmes classés A et B de l'orange book. Dans cette approche, un niveau de sensibilité est associé aux objets et un niveau d'autorisation est associé aux sujets. Chaque niveau est codé au moyen de deux paramètres, d'une part un niveau hiérarchique (p.e. publique, confidentiel, secret, très secret,...) et d'autre part un ensemble de domaines (p.e. gestion, recherche, production, ressources humaines,...). Un sujet peut accéder à un objet si son niveau hiérarchique est supérieur à celui de l'objet et si au moins un des domaines de l'objet est inclu dans un domaine du sujet.

Dans les spécifications de l'ATM Forum, ces deux niveaux sont codés sous forme d'étiquettes suivant la norme [FIPS188]. Les étiquettes caractérisant le niveau de sensibilité des données transmises sont échangées avant tout échange de données utilisateur au moyen de la signalisation ATM ou d'un protocole dans le plan utilisateur. Le contrôle d'accès en lui même est réalisé par les équipements du réseau qui vérifient que le niveau de sensibilité des données est compatible avec le niveau d'autorisation des liens et des interfaces sur lesquels les données sont transférées.

Le principal avantage de cette solution est son extensibilité car la décision de contrôle d'accès se fait au moment de l'ouverture de connexion et sans interférence avec les données des utilisateurs. Cependant certains problèmes peuvent être soulignés:

- Tous les équipements du réseau sont censés gérer les étiquettes de sécurité. Les équipements actuels ne disposent pas de telles fonctionnalités.
- Une connexion doit être établie pour chaque niveau de sensibilité.
- Le contrôle d'accès tel qu'il est considéré dans les firewalls traditionnels (accès aux équipements, aux services,...) est laissé volontairement en dehors des spécifications.

## 2.3 Solutions spécifiques

Les limitations décrites ci-dessus ont été rapidement identifiées et plusieurs propositions ont été faites afin de fournir le service de contrôle d'accès dans son sens traditionnel dans les réseaux ATM. Ces solutions peuvent se classer en deux catégories: solutions industrielles et solutions académiques.

### **Solutions industrielles.**

Le premier type de solution industrielle (Cisco, Fore) utilise un commutateur ATM classique modifié afin de filtrer les demandes de connexion ATM en fonction des adresses source et destination. Le problème principal de cette approche est que le service de contrôle d'accès n'est pas très puissant étant donné les paramètres considérés.

La seconde solution (Storagetek) est également basée sur un commutateur ATM. Ce commutateur a été modifié afin de rendre un service de contrôle d'accès au niveau IP. Au lieu de réassembler les cellules afin d'examiner les en-têtes des paquets comme dans un firewall traditionnel, cette approche cherche à obtenir ces informations directement dans la première cellule échangée sur une connexion. Cette approche empêche la perturbation de la qualité de service pendant la commutation des cellules. La solution proposée par Storagetek utilise également un type de mémoire particulier appelé CAM (Content Addressable Memory) afin de rendre les recherches dans la politique de contrôle d'accès plus rapides. Cette solution est intéressante car elle est la première à prendre en compte les limites du firewall traditionnel. Cependant elle n'est pas exempte de défauts:

- Le contrôle d'accès est limité aux niveaux 3 et 4 du modèle OSI. Les niveaux ATM et application ne sont pas considérés.
- Les paquets IP incluant des options ne sont pas filtrés au niveau transport. En effet les options peuvent repousser les informations concernant UDP et TCP dans une deuxième cellule. Ceci pose un problème de sécurité.
- L'équipement est difficile à gérer en particulier dans le cas des connexions dynamiques car la configuration des filtres se fait manuellement.
- Les performances de cet équipement ne sont pas très extensibles. En effet une version OC-12 (622 Mb/s) de ce produit a été annoncée en 1996 mais n'a pas été présentée depuis.

### **Solutions académiques.**

Les deux solutions académiques sont basées sur l'architecture proposée par Storagetek mais introduisent des améliorations afin de combler certaines des lacunes de cette solution.

La première approche [Da98] utilise un circuit spécialisé FPGA associé à un commutateur modifié. Au niveau ATM, le contrôle d'accès à l'établissement des connexions est amélioré en permettant un filtrage basé sur les adresses source et destination. Cette solution permet également le filtrage des informations de routage PNNI (Private Network to Network Interface). Aux niveaux IP et transport le service de contrôle d'accès est similaire à celui proposé par le produit de Storagetek.

Cette solution est intéressante car elle est la solution la plus complète ayant été actuellement im-

plémentée. Cependant elle possède quelques limitations:

- Les paquets IP avec options ne sont pas traités.
- Seule une partie des informations fournies par la signalisation est utilisée.
- Il n'y a pas de contrôle d'accès au niveau application.

La seconde solution [XS97] est l'architecture la plus complète actuellement proposée. Elle apporte de nombreuses améliorations vis à vis de la solution Storagetek. L'idée la plus intéressante est la classification du trafic. Celui est classé en quatre catégories en fonction de la QoS négociée au niveau ATM et du traitement à réaliser sur le flux. Cette classification permet d'assurer que les communications ayant des contraintes de qualité de service ne sont pas perturbées par des traitements complexes, les autres communications étant filtrées et perturbées de la même façon que dans un firewall. En dehors de la classification cette solution introduit également tout un ensemble d'idées d'implémentation intéressantes afin de réduire les délais engendrés par le contrôle d'accès. Cette approche est très intéressante. Elle possède cependant certains inconvénients:

- Peu de paramètres sont considérés au niveau ATM.
- Le contrôle d'accès au niveau application n'est pas fourni pour les applications ayant des contraintes de QoS.
- Les communications UDP reposant sur des connexions ATM ayant des contraintes de QoS ne sont pas contrôlées.
- L'architecture est complexe et on peut se demander quels seraient les débits supportés par une implémentation de cette architecture.
- L'architecture n'est actuellement pas implémentée.

Comme on peut le voir les problèmes les plus courants sont le manque d'extensibilité, l'impact du contrôle d'accès sur la qualité de service et la faiblesse du contrôle d'accès au niveau ATM. Il nous paraît donc intéressant de développer une architecture répondant à ces préoccupations.

### 3 Une architecture de contrôle d'accès asynchrone distribuée

Le but de notre architecture est de fournir le service de contrôle d'accès sans altération de la qualité de service négociée pour une connexion. Pour cela nous avons choisi une architecture distribuée afin d'obtenir une architecture moins sensible aux facteurs d'échelle. Les avantages de ce type d'architecture sont les suivants:

- Meilleure tolérance aux fautes. Si un équipement fournissant le contrôle d'accès tombe en panne, seuls les équipements servis par celui-ci sont affectés. Les autres peuvent continuer de fonctionner normalement.
- Amélioration de la sécurité. Il est plus difficile à un intrus de prendre le contrôle d'un réseau entier puisque pour cela il doit prendre le contrôle de tous les équipements.
- Protection contre les attaques internes. Les équipements placés à l'intérieur du réseau permettent le contrôle des communications internes.

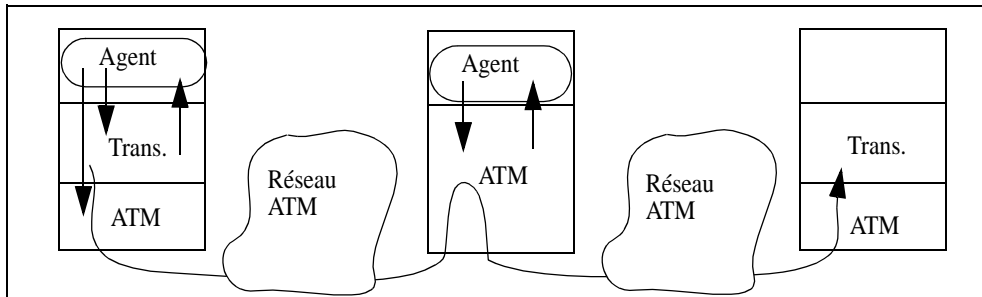
- Information réaliste sur les flux. [PN98] montre que les firewalls et les outils de détection d'intrusion se basent sur un mécanisme de récupération de l'information qui est erroné. En effet ces systèmes recherchent des attaques au moyen des informations présentes dans les flux de donnée les traversant. Or ces informations ne sont pas suffisantes pour pouvoir effectuer des décisions pertinentes. D'autres informations telles que la topologie du réseau, le type des équipements traversés ou les systèmes d'exploitation utilisés ont une grande importance. Les auteurs présentent deux classes d'attaques qui utilisent ces faiblesses. Une architecture distribuée est moins sensible à ce type d'attaque car les informations utilisées proviennent des équipements recevant ou émettant les informations à analyser.
- Amélioration des performances. Les équipements centralisés doivent effectuer des opérations de réassemblage et de fragmentation afin de décider quels flux doivent être filtrés. Ces opérations n'existent pas dans le cas d'une architecture distribuée car la distinction entre les trafics se fait de manière naturelle sur les équipements extrémité.
- Sensibilité faible au facteur d'échelle. Le processus de contrôle d'accès peut être distribué sur plusieurs équipements. Les opérations de contrôle d'accès seront alors réalisées en parallèle. Des équipements de contrôle d'accès extrêmement puissants ne sont donc pas nécessaires.
- Efficacité plus importante. Les réseaux ATM peuvent servir de support à de nombreuses piles protocolaires. Fournir des mécanismes de contrôle d'accès pour tous ces protocoles au moyen d'un seul équipement n'est pas une approche très efficace. Dans une architecture de contrôle d'accès distribuée les mécanismes et la politique de contrôle d'accès spécifique à un protocole peuvent être utilisés. Ceci donne lieu à des mécanismes moins complexes et donc plus performants.

Une architecture distribuée possède également certains inconvénients. Elle est plus difficile à gérer, ce problème sera abordé dans le chapitre 5. Cependant l'inconvénient principal est que chaque équipement doit être modifié afin qu'il fournisse le service de contrôle d'accès. Afin de limiter ce problème nous avons développé une architecture de contrôle d'accès nécessitant une modification mineure des équipements.

Il est bien connu que les équipements de communication gardent des informations sur les communications en cours dans les piles protocolaires qu'ils implémentent. Une partie de cette information a été normalisée afin de faciliter sa gestion [Sta93]. L'accès à ces données est réalisé au moyen d'un logiciel appelé agent de gestion. Nous avons montré dans [PL98] que les informations essentielles en terme de contrôle d'accès sont accessibles par ce type d'agent.

Notre architecture de contrôle d'accès est basée sur des agents de gestion modifiés. Ces agents peuvent aussi bien se situer dans des équipements terminaux que dans des équipements intermédiaires comme le montre la figure 1.

Figure 1 : Points de contrôle d'accès.



L'agent doit être modifié afin d'introduire les opérations de contrôle d'accès. Pour cela il lit de manière périodique la valeur des objets qui décrivent les communications et qui sont présents dans les piles protocolaires de l'équipement. Il compare ensuite les valeurs de ces objets avec les valeurs autorisées. Les valeurs autorisées décrivent la partie de la politique de contrôle d'accès appliquée à l'équipement. De ce fait les valeurs autorisées peuvent varier d'un agent à l'autre. Lorsque des valeurs interdites sont repérées, l'agent interagit avec les piles protocolaires afin de bloquer les actions interdites.

Notre architecture a les avantages suivants:

- L'information utilisée pour fournir le service de contrôle d'accès est examinée de manière asynchrone par l'agent au niveau application. De ce fait aucun impact sur la qualité de service des connexions établies ne peut être introduit.
- Les modifications du système afin de fournir le service de contrôle d'accès sont minimales. Celles-ci consistent uniquement à ajouter notre agent de contrôle d'accès.

Cependant la sélection de la fréquence avec laquelle les informations protocolaires doivent être lues n'est pas évidente. En effet un intervalle trop court introduira des dégradations inutiles dans les performances du système supportant l'agent alors qu'un intervalle trop long pourrait masquer certains événements importants et donc créer des trous de sécurité.

#### 4 Expression de la politique de contrôle d'accès

Afin de permettre l'expression de notre politique de contrôle d'accès nous définissons un Langage de Définition de Politique de Contrôle d'Accès (ACPDL). La définition de l'ACPDL est basée sur le Langage de Description de Politique (PDL) en cours de définition au sein du groupe de travail travaillant sur les politiques à l'IETF. Dans ce langage une politique est définie par un ensemble de règles, chaque règle étant elle même constituée d'un ensemble de conditions et d'une action qui est exécutée lorsque l'ensemble des conditions est rempli. L'expression suivante (exprimée dans le formalisme Backus Naur) décrit la forme générale d'une règle:

```
Rule ::= IF <Conditions> THEN <Action>
```

Toutes les conditions ont la même structure générique exprimée ci-dessous au moyen du formalisme BNF:

Condition ::= <ACCESS CONTROL PARAMETER> <RELATIONAL OPERATOR>  
<VALUE>

En fonction du niveau dans la pile de protocole, plusieurs types de paramètres de contrôle d'accès peuvent être utilisés:

- Au niveau ATM les paramètres intéressants sont décrits dans [PLG98]. Parmi ceux-ci nous avons choisi le type de trafic, les identificateurs de connexion, les informations d'adressage, les descripteurs de QoS et les descripteurs de service.
- Au niveau transport la plupart des paramètres que nous avons considérés sont ceux qui sont utilisés habituellement afin de réaliser le filtrage des paquets dans les routeurs filtrants (par exemple les informations d'adressage, les ports source et destination, les drapeaux dans le cas des connexions TCP,...).
- Au niveau application nous définissons deux paramètres génériques: l'identificateur de l'utilisateur de l'application ainsi que l'état de l'application.
- Des informations temporelles ont également été incluses afin de spécifier quand une règle doit être appliquée.

Les actions ont également une structure générique (notation BNF):

Action ::= <ACTION> <ACTION LEVEL> <LOG LEVEL>

Celle-ci se décompose en trois parties. La première indique si la communication décrite par les conditions doit être autorisée ou interdite. Le paramètre <ACTION LEVEL> correspond à la couche protocolaire dans laquelle doit être effectuée l'action. La dernière partie décrit l'importance accordée à l'évènement de contrôle d'accès et permet la classification des résultats.

La figure 2 montre comment notre langage peut être utilisé afin d'exprimer un service de contrôle d'accès. Dans cet exemple chaque équipement est identifié par son adresse source et son adresse destination. Le service WWW est identifié par les ports source et destination. La deuxième ligne de commande donnée dans l'exemple est utilisée afin d'interdire les demandes de connexion sur le port WWW de notre station interne.

Figure 2 : Exemple de règles de contrôle d'accès

```
IF (IP_SRC_ADDRESS = 192.165.203.5 255.255.255.255) AND  
(IP_DST_ADDRESS = 0.0.0.0 0.0.0.0) AND (SRC_PORT > 1023) AND  
(DST_PORT = 80) THEN PERMIT TRANSP_CONNECTION LEVEL1;  
IF (IP_SRC_ADDRESS = 0.0.0.0 0.0.0.0) AND (IP_DST_ADDRESS =  
192.165.203.5 255.255.255.255) AND (SRC_PORT = 80) AND (DST_PORT  
> 1023) AND (TCP_FLAG <> SYN) THEN PERMIT TRANSP_CONNECTION
```

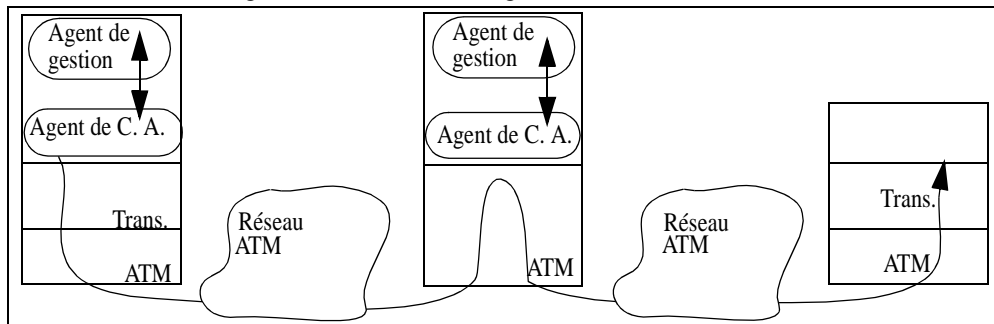
Une fois définie au moyen de l'ACPDL, la politique de contrôle d'accès doit être distribuée sur les équipements de gestion au moyen de notre architecture de gestion du contrôle d'accès.

## 5 Une architecture de gestion du contrôle d'accès

### 5.1 Fonctionnement général

Notre architecture est basée sur l'utilisation d'agents se plaçant sur les équipements fournissant le service de contrôle d'accès. Ces agents interagissent avec les équipements sur lesquels ils sont placés afin de configurer les mécanismes de contrôle d'accès de la manière la plus performante possible. La figure 3 présente les interactions entre agents et modules de contrôle d'accès.

Figure 3 : Architecture de gestion du contrôle d'accès.



L'objectif général de l'application des règles spécifiées par la politique de contrôle d'accès au niveau des équipements de contrôle d'accès est qu'un nombre minimal de règles de contrôle d'accès soit réellement appliquées au niveau de chaque équipement. Pour cela nous définissons un ensemble de conditions qui assure cette propriété lorsqu'elles sont appliquées. Les deux premières ont déjà été exprimées dans d'autres solutions de gestion distribuée du contrôle d'accès ([Hyl98], [Ft98]):

- (assertion 1): Une règle ne peut être attribuée qu'aux modules de contrôle d'accès contenant les objets de contrôle d'accès utilisés par la règle.
- (assertion 2): Une règle ne peut être attribuée à un module contenu dans un équipement que si celui-ci est situé sur le chemin entre la source et la destination décrit par la règle.

Une meilleure connaissance du type de politique de contrôle d'accès permet de donner des propriétés supplémentaires. Par exemple dans le cas d'une politique de type «Tout ce qui n'est pas explicitement autorisé est interdit», qui est le type de politique le plus répandu, il est possible de ne spécifier les interdictions qu'en un point du chemin qui interconnecte la source et la destination relatifs à une règle. Ceci se justifie par le fait que dans ce type de politique, chaque règle d'interdiction décrit un sous ensemble d'un ensemble décrit par une règle d'autorisation. De plus afin d'assurer une distribution maximale des règles et du fait de la structure généralement arborescente des réseaux, il est important que le placement de ces règles se fasse sur les équipements les plus proches des équipements source et destination relatifs à la règle.

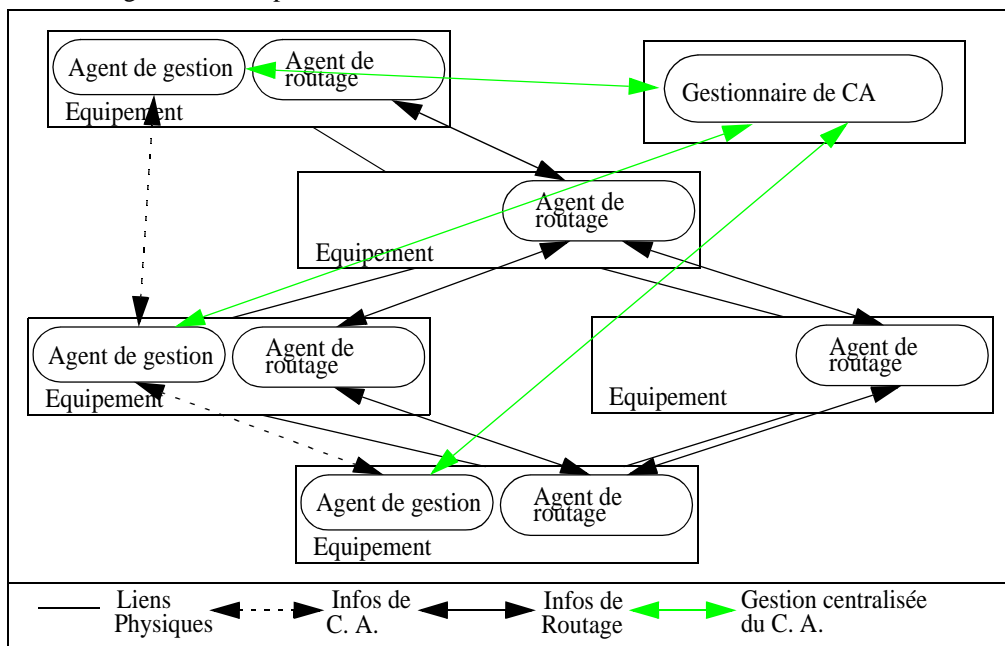
- (assertion 3): Si une règle d'interdiction peut être attribuée à des modules situés sur plusieurs équipements en cascade, la règle ne doit être attribuée qu'au module situé sur l'équipement le plus proche des extrémités.

La traduction de ces lois se fait par la prise en compte de paramètres comme la topologie du ré-

seau, les capacités de l'équipement en terme de contrôle d'accès, la place de l'équipement dans la topologie du réseau et la configuration des autres équipements de contrôle d'accès.

Ces paramètres impliquent des interactions entre les agents de configuration et d'autres éléments du réseau. Certaines de celles-ci, détaillées dans la section 5.2 sont internes à un équipement: entre l'agent de configuration et l'agent de routage correspondant ainsi qu'entre l'agent de configuration et les mécanismes de contrôle d'accès.

Figure 4 : Exemple de réseau et interfonctionnement des différents éléments.



D'autres interactions, détaillées figure 4, sont externes:

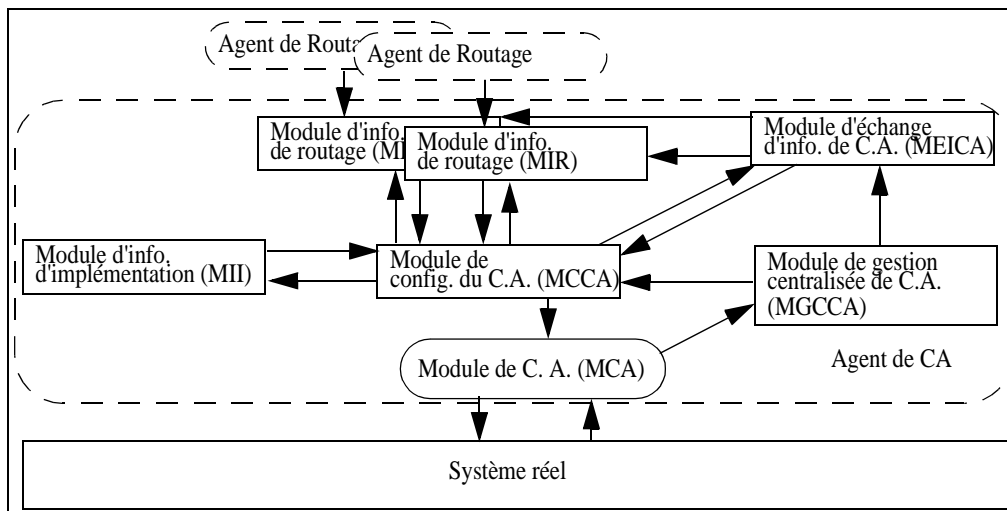
- Entre les agents de contrôle d'accès afin d'assurer une configuration efficace du contrôle d'accès.
- Entre les agents et le gestionnaire centralisé de contrôle d'accès. Celui-ci assure la distribution uniforme de toutes les règles de contrôle d'accès sur les agents et la récupération des résultats de l'application de celles-ci. Le protocole utilisé entre les agents et le gestionnaire doit assurer l'intégrité, l'authentification, la confidentialité et le contrôle d'accès sur les informations transportées. Les protocoles SNMPv2\* [Sta98] et SNMPv3 [Ba98] semblent être de bons candidats. Ils exigent cependant de gérer les informations de contrôle d'accès sous forme de bases de données de gestion (MIB) au niveau des agents. Ces informations comportent d'une part les règles de contrôle d'accès et d'autre part les résultats relatifs à l'application de ces règles.

Nous décrivons dans les sections suivantes comment ces règles peuvent être mises en oeuvre au moyen de notre architecture.

## 5.2 Architecture fonctionnelle

Comme on peut le voir figure 5, notre architecture de gestion se base sur l'utilisation de modules interagissant les uns avec les autres.

Figure 5 : Architecture fonctionnelle d'un agent de contrôle d'accès



Les rôles de ces différents modules sont les suivants:

### **Le module de contrôle d'accès (MCA).**

Ce module représente les mécanismes de contrôle d'accès implémentés par l'équipement auprès de l'agent de contrôle d'accès. Ce module reçoit les règles de contrôle d'accès de la part du module de configuration du contrôle d'accès (MCCA). Ces règles sont traduites par le MCA dans les syntaxes réelles des commandes nécessaires à la configuration des mécanismes implémentés par le système. En retour de ces commandes le MCA reçoit des résultats correspondant à l'application des commandes et transmet ces résultats au module de gestion centralisée du contrôle d'accès (MGCCA).

### **Le module d'information d'implémentation (MII).**

Le MII décrit au MCCA les capacités de l'équipement sur lequel se situe l'agent en terme de contrôle d'accès. Pour cela il possède une table de correspondance entre les paramètres présents dans les règles de contrôle d'accès et les mécanismes implémentés au niveau du système. La configuration de cette table se fait par l'officier de sécurité de manière manuelle ou de manière automatique par le logiciel d'installation des outils de contrôle d'accès. Lors de modifications dans cette base de donnée, le MCCA est averti par le MII.

### **Le module de gestion centralisée du contrôle d'accès (MGCCA).**

Ce module fait le lien entre l'agent et le gestionnaire centralisé de contrôle d'accès présenté dans la section précédente. Pour cela il gère une base de donnée de gestion (MIB) qui est mise à jour

par le gestionnaire. Celui-ci distribue au MGCCA toutes les règles de la politique de sécurité relative à l'équipement contrôlé par l'agent. Il avertit le MCCA de ces mises à jour en lui fournissant toutes les règles modifiées. En retour des règles de contrôle d'accès, le MGCCA reçoit les résultats du contrôle d'accès de la part du MCA. Ces résultats sont stockés de manière incrémentale dans une table de la MIB et sont récupérés par le gestionnaire de manière périodique.

#### **Le module d'échange d'informations sur le contrôle d'accès (MEICA).**

Le MEICA a pour objectif de fournir au MCCA l'information suivante: «Existe-t'il un équipement mieux positionné qui applique déjà la règle  $r$  ?». Afin de fournir cette information le MEICA interagit avec les MEICA des agents voisins au moyen du protocole d'échange d'informations de contrôle d'accès. Ce protocole permet l'élection d'un agent choisi pour appliquer la règle de contrôle d'accès. Pour cela, le MEICA envoie à chaque changement de configuration les informations suivantes à ses voisins: Identificateur de la règle, Adresse de l'agent appliquant la règle, distance. Pour chaque règle  $r$ , le MEICA compare les informations fournies par ses voisins avec la distance qui le sépare de la source et de la destination correspondant à  $r$  et en déduit si l'agent qu'il représente se trouve en position optimale afin d'appliquer la règle. Une position optimale signifie que la valeur minimale des distances entre la source ou la destination relative à la règle et notre MEICA est plus faible que celle annoncée par tous les autres agents. Cette distance est donnée par le module d'information de routage MIR. Des changements dans la topologie du réseau ou dans la configuration des équipements de contrôle d'accès peuvent avoir lieu en cours de fonctionnement et provoquer une modification des informations sur le contrôle d'accès. Dans ce cas le MEICA avertit le MCCA afin que celui-ci revoit sa configuration.

#### **Le module d'informations de routage (MIR).**

Le module MIR a un fonctionnement qui peut varier énormément en fonction du protocole de routage qui lui est associé. Cependant les fonctions qu'il remplit sont toujours les mêmes. D'une part il est utilisé par le MCCA afin de savoir si la communication relative à une règle  $r$  passe par l'équipement sur lequel est installé l'agent. D'autre part le MIR est chargé sur demande du MEICA de calculer la distance entre l'équipement supportant l'agent et un équipement  $y$ . Enfin lors de modifications dans la topologie du réseau, le MIR avertit le MCCA afin que celui-ci prenne en compte cette nouvelle topologie.

La figure 4 ne propose qu'une vision planaire de notre réseau qui ne correspond pas forcément à la réalité. Dans le cas de réseaux où le routage peut se faire à plusieurs niveaux (Par exemple du type IP sur ATM) il est nécessaire de considérer le fait que les informations de routage se rapportant aux règles peuvent provenir d'agents de routages différents, ce qui explique que le MCCA puisse être en relation avec plusieurs MIRs, chacun étant dédié au routage d'une couche particulière.

#### **Le module de configuration du contrôle d'accès (MCCA).**

Le module MCCA est le module central de notre architecture. Il est averti de l'arrivée de chaque nouvelle règle de contrôle d'accès par le MGCCA. Pour chacune de ces règles, il va appliquer les trois lois définies dans la section précédente. Afin d'appliquer chacune de ces lois, il interagit avec les modules MII, MIR, MEICA. L'algorithme de fonctionnement général de ce module est le suivant: Pour chaque règle reçue, le MCCA vérifie si celle-ci peut être appliquée à l'équipe-

ment au moyen du MII (assertion 1). Il vérifie ensuite au moyen du MIR que l'équipement peut se situer sur une des routes décrite par la règle (assertion 2). Si la règle de contrôle d'accès est une règle d'interdiction il s'adresse alors au MEICA afin de savoir si un équipement plus proche de la source ou de la destination décrite par la règle l'applique déjà (assertion 3). Les règles n'exprimant pas de notion de source et de destination sont appliquées sans cette vérification. Si toutes ces conditions sont vérifiées, le MCCA passe alors la règle au MCA afin que celui-ci l'implémente.

Théoriquement pour un ensemble de règle donné, une configuration des équipements de contrôle d'accès et une topologie stable, la configuration du contrôle d'accès dans le réseau converge vers un état stable dans lequel l'implémentation des règles est conforme à nos trois assertions.

## 6 Conclusion

En conclusion nous présentons dans le tableau 1 une comparaison des différentes approches visant à fournir le service de contrôle d'accès dans les réseaux de type ATM et IP sur ATM.

**Tableau 1 : Comparaison des différentes approches**

Propriété/ Approche	Firewall classique	ATM Forum	Switch filtrant	Firewall ATM	Dowd & al.	Xu & al.	Paul & al.
Contrôle d'accès au niveau ATM	Non	Non	Faible	Non	Faible	Faible	<b>Bon</b>
Contrôle d'accès au niveau transport	<b>Bon</b>	Non	Non	Moyen	Moyen	Moyen	Moyen
Contrôle d'accès au niveau applica- tion	<b>Bon</b>	Non	Non	Non	Non	Moyen	Moyen
Contrôle d'accès par étiquette	Non	<b>Bon</b>	Non	Non	Non	Non	Non
Extensibilité	Faible	<b>Bon</b>	<b>Bon</b>	Moyen	Moyen	Moyen	<b>Bon</b>
Niveau de modifi- cation	<b>Faible</b>	Important	<b>Faible</b>	<b>Faible</b>	<b>Faible</b>	<b>Faible</b>	Moyen
Impact sur la QoS	Important	<b>Non</b>	<b>Non</b>	Faible	Faible	Faible	<b>Non</b>
Niveau de sécurité	<b>Bon</b>	<b>Bon</b>	Faible	Moyen	Moyen	<b>Bon</b>	Moyen
Facilité de gestion	<b>Bon</b>	Faible	<b>Bon</b>	Faible	Faible	<b>Bon</b>	<b>Bon</b>
Implémentation	<b>Oui</b>	Non	<b>Oui</b>	<b>Oui</b>	<b>Oui</b>	Non	Non

Comme nous pouvons le voir, notre approche a les avantages suivants:

- Amélioration du contrôle d'accès au niveau ATM.
- Très bonne capacité à supporter les facteurs d'échelle grâce à une architecture distribuée.

- Pas d'impact sur la qualité de service au grâce à une méthode asynchrone d'analyse des informations des communications.
- Bonnes performances grâce à une méthode de configuration efficace.
- Facilité de gestion au moyen d'un langage générique de définition du contrôle d'accès et d'une méthode de configuration automatique des agents.

Ce travail pourrait être poursuivi dans deux directions principales. La première est l'implémentation de notre architecture afin d'en évaluer les performances réelles. D'autre part il pourrait être intéressant de considérer son adaptation à d'autres types de réseaux où la qualité de service est une contrainte importante.

## 7 Références

- [Ba98]** : Basking in Glory-SNMPv3, Dan Backman, Network Computing, Août 1998.
- [Da98]** : An FPGA-Based Coprocessor for ATM Firewalls, J. McHenry, P. Dowd, F. Pellegrino, T. Carrozzi, W. Cocks, in proceedings of IEEE FCCM'97, Avril 1997.
- [Ft98]** : Integrated Management of Network and Host Based Security Mechanisms, R. Falk, M. Trommer, 3rd Australasian Conference on Information Security and Privacy ACISP'98, Brisbane, Australia, 13.-15. Juillet 1998.
- [Hy98]** : Management of Network Security Application, P. Hyland, R. Sandhu, 1st National Information Systems Security Conference, Octobre 1998.
- [JA98]** : ATM Net Management: Missing Pieces, Joe Abusamra, Data Communications, Mai 1998.
- [KL98]** : Firewall Shootout Test Final Report, Keylabs, Networld+Interop'98, Mai 1998.
- [PDL98]** : Policy Framework Definition Language, draft-ietf-policy-framework-pfdl-00.txt, John Strassner, Stephen Schleimer, Internet Engineering Task Force, 17 Novembre 1998.
- [PL98]** : Où trouver les informations de contrôle d'accès dans le cas des réseaux ATM ?, Olivier Paul, Maryline Laurent, Rapport technique, Août 1998
- [PL99]** : .An Alternative Access Control Architecture for IP over ATM Networks, Olivier Paul, Maryline Laurent, IFIP Conference on Communications and Multimedia Security, Leuven, Belgium, Septembre 1999
- [PLG98]** : Manageable parameters to improve access control in ATM networks , Olivier Paul, Maryline Laurent, Sylvain Gombault, HP-OVUA Workshop, Rennes, France, Avril 1998.
- [PN98]** : Insertion, evasion, and denial of service: eluding network intrusion detection, T. Ptacek, T. Newsham, Rapport technique, Secure Network, Janvier 1998.
- [Ran92]** : A network firewall, M. Ranum, Proc. World Conference on System Administration and security, 1992.
- [Schu98]** : On the modeling , design and implementation of firewall technology, Christoph Schuba, Thèse de doctorat, Purdue University, Décembre 1997.
- [Sta93]** : SNMP, SNMPv2 and CMIP, The practical guide to network management Standards. William Stallings. Addison-Wesley. 1993.
- [XS97]** : Design of a High-Performance ATM Firewall, J. Xu, M. Singhal, Rapport technique, The Ohio State University, 1997.