HAL
open science

Contrôle d'accès dans les réseaux haut débit

Jean-Michel Cornilleau, Patrice Tadonki, Sylvain Gombault, Jean-Luc Bernier

To cite this version:

Jean-Michel Cornilleau, Patrice Tadonki, Sylvain Gombault, Jean-Luc Bernier. Contrôle d'accès dans les réseaux haut débit. SETIT'03 : Conférence internationale Sciences électroniques, technologies de l'information et des télécommunications, Mar 2003, Madhia, Tunisie. hal-01833584

HAL Id: hal-01833584

https://hal.science/hal-01833584v1

Submitted on 9 Jul 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Contrôle d'accès dans les réseaux haut débit

J.M Cornilleau (a), P. Tadonki (b), S. Gombault (c).J.L Bernier (d)
a, b, c et d : Ecole Nationale Supérieure des Télécommunications de Bretagne.
{jean-michel.cornilleau | sylvain.gombault | patrice.tadonki| jlbernier}@.enst-bretagne.fr

Résumé :

Le pare-feu ou firewall *est* l'un des éléments clef de la sécurité actuelle des réseaux. Le terme firewall est un terme générique qui englobe généralement un ensemble de mécanismes permettant d'assurer plusieurs services de sécurité tels que l'authentification de l'origine des communications, la confidentialité des informations transmises sur le réseau, ou le contrôle d'accès réseau. Ces services peuvent varier d'un firewall à l'autre, cependant le service de contrôle d'accès réseau est généralement considéré comme un service de base et peut être assuré par tous les types de firewalls. Les constructeurs d'équipements de contrôle d'accès ne donnent aucune indication sur les temps de traitements (calcul, analyse, etc.) des paquets et leur impact sur la qualité de service. Ces temps de traitements peuvent parfois être inadapté et incompatible avec les exigences de QoS dans les réseaux Haut débit. Dans cet article, nous présentons un mécanisme de contrôle d'accès dont l'impact sur le délai et la gigue de la QoS est négligeable.

Mots clés : réseau, sécurité des réseaux, QoS, firewall, carte IFT, mémoire Trie, IPv6, Gigabit Ethernet.

Abstract:

Firewall is one of the elements key of the current security of the networks. Firewall is a generic term which generally includes a whole of mechanisms making it possible to render several services of security such as the authentication of the origin of the communications, the confidentiality of the information transmitted on the network, or it access control network. These services can vary from one firewall to another; however the access control of the network is generally regarded as a basic service and is ensured by all types of firewalls. These access control architectures can cause problems when they are used in combination with networks insuring high throughput: they are not adapted to the taking into account of the QoS negotiated by the users. We show an access control mechanism whose impact on QoS is quantifiable.

Keywords: Network, network security, QoS, firewall, IFT card, Trie memory, Ipv6, Gigabit Ethernet.

1 Introduction

Avec la naissance du Web, l'age de l'Internet commercial était inauguré, donnant naissance à de nouveaux types d'utilisateurs, toujours plus avides de services et donc de bande passante. La consommation des utilisateurs a donc évolué aussi rapidement que l'Internet, l'augmentation des débits étant très vite rattrapée par une consommation accrue de nouvelles applications.
C'est en considérant cette augmentation du volume des données informatiques qu'a été lancé en 1999 le projet **VTHD** (Vraiment Très Haut Débit): Plate-forme d'expérimentation IP/WDM Vraiment Très Haut Débit pour applications de l'Internet de nouvelle génération. Le réseau VTHD est la plate-forme support de l'initiative française pour l'Internet Nouvelle Génération menée sous l'égide du RNRT (Réseau National pour la Recherche en Télécommunications).
Par ailleurs, cette augmentation du volume des données informatiques soulève un nouveau problème, celui de la sécurisation de la transmission des informations à haut débit. En effet, des attaques menées sur les réseaux peuvent avoir des répercutions dramatiques : coût financier, divulgation d'informations secrètes, perte de l'image de marque, etc. Dans ce contexte de réseau haut débit où la QoS a une grande importance dans les services que proposent les opérateurs, il est nécessaire de disposer de mécanismes de sécurité qui n'empêchent pas un réseau de remplir ses engagements en terme de QoS. FT R&D et l'ENST Bretagne collaborent depuis 2 ans sur un projet de contrôleur d'accès haut débit à temps d'analyse faible et borné, deux qualités essentielles pour ne pas nuire à la QoS d'un réseau.

Cet article va s'attacher en premier lieu à démontrer l'importance de la sécurité informatique dans les réseaux. Ensuite, il posera la problématique concernant l'impact que peut avoir un équipement sur la QoS d'un réseau. Le chapitre suivant sera consacré au contrôleur d'accès développé par L'ENST de Bretagne et FT R&D dans le cadre du projet Carat, afin d'en montrer ses atouts en terme d'impact sur la QoS. Enfin, le dernier chapitre présentera l'état actuel du projet et ses évolutions possibles dans VTHD++ (suite de VTHD).

2 La sécurité dans les réseaux

La sécurité est aujourd'hui un élément incontournable à prendre en compte dans toute mise en œuvre de réseaux informatiques. Les attaques effectuées sur ces réseaux peuvent avoir des répercussions dramatiques : coût financier, divulgation d'informations secrètes, pertes des données, etc. Ainsi, le succès des réseaux à haut débit dépend de la confiance que les usagers placent dans leur sécurité. La sécurité des réseaux et des services est donc un besoin crucial tant pour l'opérateur de réseau de télécommunications que pour ses clients. Le débit croissant des réseaux implique des études spécifiques sur la sécurité des réseaux à haut débit. Les solutions [1] mises en oeuvre actuellement ont des limitations :

- Inhomogénéité dans les équipements et dans la définition et l'administration des politiques de sécurité,
- Faible ergonomie du processus de gestion du contrôle d'accès,
- Possibilité de trous de sécurité dans les architectures concurrentes,
- Nécessité de mettre en place dans les équipements de routage un grand nombre de règles de filtrage sur l'entête IP qui entraîne une baisse de performances.
- Performances dégradées, insuffisantes à terme pour satisfaire aux besoins sans cesse croissants.

Une fois la connexion établie, la sécurisation des applications véhiculées au dessus de la couche réseau IP nécessite un contrôle supplémentaire. Le contrôle d'accès IP, à lui seul, limite les performances lorsque des solutions purement logicielles sont mises en oeuvre et rend impossible de maintenir la QoS que peut supporter un réseau haut débit. Les systèmes en opération et les études en cours montrent les limitations des solutions opérationnelles utilisées actuellement [2]. La solution actuellement mise en oeuvre pour réaliser le contrôle d'accès dans les réseaux consiste à utiliser un contrôleur d'accès placé entre le réseau à protéger et le réseau public. Dans cette solution, qui permet le contrôle d'accès aux niveaux paquet, circuit et application, les actions sont filtrées par des équipements appelés proxies. Le trafic y est examiné au niveau application ce qui perturbe considérablement la QoS. De plus comme le filtrage est généralement réalisé en parallèle 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 [3] 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).

3 Problématique : QoS versus Equipements/Traitements intermédiaires

L'Internet est un réseau d'interconnexion de réseaux, s'appuyant sur divers moyens de transport, avec une grande variation de capacité de bande passante et de caractéristiques de délai. La nature sporadique des flux transportés conduit à de fortes variations de charge ; l'état des liens entre deux hôtes peut ainsi varier d'une milliseconde à l'autre. Plusieurs applications qui se partagent un lien peuvent par instant conduire à la congestion des ressources du réseau. La congestion génère délai de livraison et pertes d'information. La QoS est la capacité d'un élément réseau (une application, un hôte, un routeur) d'avoir un certain niveau d'assurance que la demande de trafic et les besoins de service puissent être satisfaits, même en présence de congestion dans le réseau [3]. Les ressources disponibles n'étant jamais infinies, le déploiement de la QoS passe forcément par un dimensionnement adapté des réseaux, afin de toujours bénéficier de suffisamment de ressources pour offrir des garanties (en terme de délais, gigues et pourcentage de pertes) aux différentes applications. Dans le cas où la QoS doit être est assurée de part et d'autre d'un équipement, les problèmes à gérer sont les suivants :

- réassemblage, le routage et la fragmentation des paquets ainsi que les opérations de filtrage provoquent une augmentation du délai de transit des paquets.

- Les opérations internes à l'équipement peuvent introduire des pertes de paquets. Ces pertes peuvent être par exemple dues à des débordements de files au niveau IP. La perte de paquets au niveau du firewall provoque l'augmentation du taux de perte de cellules de bout en bout.
- La taille des paquets IP n'est pas fixe. Ceci induit que le temps mis pour réassembler un paquet, le filtrer, le router et pour le fragmenter n'est pas fixe. Il peut donc se produire des variations de délai qui sont, entre autre, fonction de la taille des paquets.
- Le routage et le filtrage des paquets dans ce type d'architecture se font de manière logicielle. Il est donc possible que la charge de la machine implique des modifications dans le débit crête, le débit moyen et dans le débit minimum.

Cependant, comme le filtre est sensé être placé entre deux réseaux et que tout le trafic entre ces deux réseaux doit transiter par lui, il n'y a pas de déséquencement entre les différents flux. Au niveau application les problèmes sont similaires. Cependant, du fait que les informations remontent jusque dans l'espace utilisateur, les altérations peuvent être plus importantes. Pour régler ces problèmes, une solution a été proposée par l'ENST-Bretagne en collaboration avec France Telecom. Cette solution, sous la forme d'un contrôleur d'accès haut débit, garantit les aspects de QoS pré-cités.

4 Contrôleur d'accès haut débit : la solution ENST-Bretagne / France Telecom

Ce contrôleur d'accès est la convergence des travaux de FT R&D sur la carte IFT (Internet Fast Translator [4]) et des travaux de l'ENST Bretagne sur la sécurité des réseaux. Les qualités de cette carte IFT, associées au compilateur de politique de contrôle d'accès que l'ENST Bretagne a développé, ont été expérimentées en 2000 dans le projet CARAT (Contrôle d'Accès pour Réseau ATM) [5].

4.1 Cartes IFTs et mémoire Trie

4.1.1 Cartes IFTs

Les cartes IFTs (*Internet Fast Translator*) ont été développées par France Telecom R&D avec comme principal objectif d'effectuer du routage à haut débit. L'analyse des en-têtes se fait au moyen d'une mémoire Trie (*memory trie*) qui a été étendue afin de fournir un moyen d'analyse générique permettant d'analyser tous les champs d'une cellule dans n'importe quel ordre. Le comportement de l'IFT est dicté par plusieurs facteurs : le contenu de la mémoire trie, une machine à état permettant de conserver l'état de l'analyse et de lancer l'exécution d'actions adéquates, un composant physique capable d'accélérer ces actions et enfin une capacité de comptage permettant d'associer des compteurs à la reconnaissance de figures préétablies. La mémoire trie actuellement utilisée a une taille de 4 Mo.

4.1.2 La mémoire Trie

Le principe de la mémoire trie a été proposé au début des années 60. La mémoire trie est un moyen de stocker et de récupérer des informations. L'avantage principal de la mémoire trie vis à vis des autres types de mémoire est de fournir un temps d'accès à l'information relativement faible, une grande facilité d'ajout et d'effacement, une capacité à supporter des arguments de taille variable et la possibilité de tirer parti des redondances présentes dans les informations stockées.
Le processus de recherche dans une mémoire trie est basé sur une série d'indexations, indirections dans un tableau à deux dimensions. Comme présenté dans la figure 1, chaque ligne constitue un registre de 2^k cases où k est la longueur en bit de la tranche analysée (dans notre cas k est égal à 4). Les registres peuvent être situés n'importe où dans le tableau à l'exception de la première ligne du tableau qui est réservée à l'analyse de la première tranche de k bits. Chaque mot mémoire est donc adressé en ligne au moyen d'une adresse ou registre et en colonne au moyen du contenu des k premiers bits du champ à analyser. Ce mot mémoire contient un *status* qui permet d'adresser le registre suivant dans l'analyse afin de continuer celle-ci (cases présentant un motif RX dans le tableau présenté). Ce type de *status* est appelé *status* intermédiaire. Les *status* permettent également d'interrompre l'analyse et de renvoyer le résultat de celle-ci lorsque le champ analysé correspond à un motif stocké en mémoire (cases présentant un motif SX dans le tableau présenté). Ce dernier type de *status* est appelé *status final.*

	0x0 0000	0x1 0001	0x2 0010	0x3 0011	0x4 0100	0x5 0101	0x6 0110	0x7 0111	0x8 1000	0x9 1001	0xA 1010	0xB 1011	0xC 1100	0xD 1101	0xE 1110	0xF 1111
R0		R1						R2				R4				
R1				R4		R2										
R2			S2				R3			S1						
R3									S3					S3		
R4					S4								S5			

Figure 1. Mémoire Trie sur des donnés de 4 bits (16 valeurs possibles).

La figure 2 présente la structure d'un *status*. Comme on peut le voir, celui-ci est composé de cinq parties principales. Les deux premières parties appelées partie de contrôle et compteur ne sont pas utilisées dans notre cas. La troisième partie décrit le type de déplacement à réaliser pour atteindre le quartet de données suivant à analyser. Le champ déplacement contient la longueur du déplacement (en quartet de bits) à réaliser pour atteindre le prochain champ à analyser. Enfin le dernier champ indique dans le cas d'un status intermédiaire l'adresse du prochain registre. Dans le cas d'un status final, celui-ci indique un pointeur donnant le résultat de l'analyse.

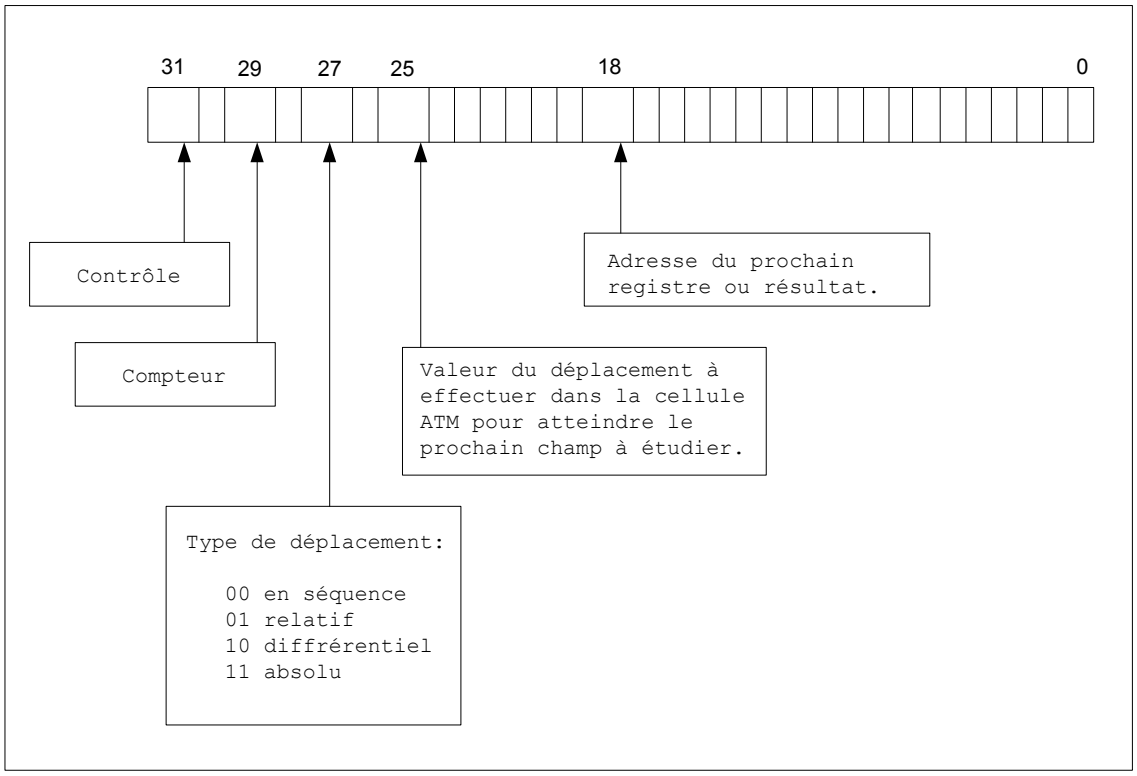

Figure 2. Structure des portiers (codés sur 32 bits)

Cette structure des quartets nous permet de distinguer deux types de registres. Les registres intermédiaires qui correspondent à l'analyse en séquence des tranches de k bits d'un champ. Les *status* permettant d'atteindre ces registres correspondent à une longueur de déplacement de un quartet et à une adresse de registre indiquant le registre suivant dans la mémoire trie. Les portiers correspondent au premier registre permettant de commencer l'analyse d'un champ. Ils sont atteints au moyen d'un *status* intermédiaire dont la longueur de déplacement est différente de un. Le type du déplacement pour atteindre un portier peut ne pas être en séquence.

4.1.3 Conclusion

L'utilisation des cartes IFTs et de leur mémoire trie permet le développement d'un algorithme de classement conçu de telle sorte que le temps de traitement nécessaire au classement ne dépende pas du nombre de règles de contrôle d'accès exprimant la politique de contrôle d'accès mais uniquement du nombre de champs à analyser. Cette propriété nous permet de garantir une borne maximale aux modifications concernant la QoS.

4.2 Algorithme de classification

Nous venons de voir comment était réalisée l'analyse d'un champ dans une mémoire trie. Nous allons montrer dans ce paragraphe comment il est possible d'utiliser ce mécanisme pour réaliser le contrôle d'accès.
La structure de classement est constituée d'un ensemble de graphes d'analyse chaînés entre eux afin de représenter les différentes possibilités exprimées par les règles de contrôle d'accès. A partir de cette structure de classement, l'algorithme de classement consiste à parcourir les graphes d'analyse en présentant à la structure de classement les champs à analyser. La progression dans les graphes se fait en suivant les opérations d'indexations et indirections de la mémoire trie implémentant les graphes d'analyse comme nous l'avons expliqué en section précédente. Le résultat est un *status* final indiquant l'action à réaliser, en l'occurrence PERMIT ou DENY (c'est à dire l'autorisation ou le rejet du paquet).

4.2.1 Principe de l'algorithme de base

Cet algorithme permet de créer la structure de classification. Une première partie des champs est parcourue de manière linéaire (cf.4.3), en fait jusqu'à la version du protocole IP. Ensuite pour chacun des protocoles de niveau supérieur (ICMP, TCP, UDP), on créé un nœud père à partir duquel l'algorithme récursif sera déroulé trois fois.

Algorithme simplifié:

- on initialise l'algorithme en calculant les intervalles élémentaires et on crée un portier initial
- pour chaque intervalle tant que ce n'est pas la dernière dimension :
    - On crée un portier que l'on insère dans la structure de classement et on fait le lien avec son portier père,
    - On restreint l'ensemble de règles de la politique à la dimension ou champ en cours de traitement,
    - On calcule les intervalles crée par ces différentes règles,
    - On appelle la fonction de manière récursive.
- dans la dernière dimension de l'analyse, on attribue au portier père un *status* désignant l'action correspondant aux règles restantes.

4.2.2 Compression de la structure

L'exécution de l'algorithme de création de la structure peut créer plusieurs fois certaines parties du graphe d'analyse. Ces réplications peuvent entraîner un graphe de grande taille et empêcher son stockage en mémoire trie, ce qui consiste un frein à l'utilisation de cette technique de classification rapide puisque cela limite la taille des politiques utilisables.
C'est pour cela que certaines parties du graphe sont compressées de telle sorte que les nœuds similaires soient remplacés par un seul nœud au moment de la construction du graphe d'analyse. Au moment de la création de fils, on cherche tout d'abord si un intervalle portant sur les mêmes règles de classement a déjà été traité dans la même dimension. On cherche également le portier correspondant. Pour cela, on utilise une structure qui stocke tous les portiers par niveau dans la structure de classement. Dans le cas où un portier existe déjà, on crée un lien entre celui-ci et le père courant. Dans le cas contraire, on suit la procédure normale en créant un nouveau portier.

4.3 Champs traités.

Lors de la création de la structure de classification, on parcourt différentes dimensions (ou champs). Ces champs sont ceux sur lesquels s'appliquent les politiques. Dans notre projet, nous nous sommes limités à certaines données des cellules ATM.
Les premiers champs traités dans la cellule ATM sont les suivants :

- Identificateur de connexion ATM (VCI)
- Encapsulation SNAP/LLC
- Protocole IP/ARP
- Version IP

Ce sont des champs dont le nombre de valeurs possibles est limité. Ainsi, la structure créée en mémoire trie est peu importante et occupe peu de place. C'est pourquoi, par la suite, nous ne nous intéresserons plus à cette partie de la structure qui ne peut pas être réellement optimisée. Ces champs seront toujours traités de façon linéaire.
Par contre, nous nous intéresserons plus particulièrement aux trois arbres créés pour les trois principaux protocoles supportés par IP.
La figure 3 ci-dessous présente les champs étudiés en fonction des différents protocoles de niveau supérieur à IP. Le numéro qui leur est attribué correspond à celui utilisé dans le programme.

Champ	Signification	ICMP	TCP	UDP
2	Protocole de niveau supérieur à IP	1	6	17
3	Adresse IP source	x	x	x
4	Adresse IP destination	x	x	x
5	Port Source TCP		x	
6	Port destination TCP		x	
7	Drapeaux TCP		x	
8	Port source UDP			x
9	Port destination UDP			x
10	Type ICMP	x		
11	Code ICMP	x		

Figure 3. Champs traités selon les différents protocoles

4.4 Résultats

Les performances des cartes IFTs sont limitées par deux facteurs. Le premier est le type de connecteur physique liant les cartes IFTs au processus d'analyse des cellules. Le type de support physique supporté par ce connecteur est actuellement de type SDH OC12 ce qui limite le débit supporté par le connecteur à 620 Mb/s. Le débit utile offert à la couche ATM est lui inférieur au débit nominal du fait du mode d'encapsulation des cellules ATM dans les PDUs utilisées par la couche physique, et est égal à 599 Mb/s)

La seconde limite aux performances des cartes IFTs provient de l'algorithme de classement (figure 3). Comme nous l'avons précisé, la vitesse de classement de notre algorithme ne dépend que du nombre de champs, de la taille des champs analysés et de la taille du motif reconnu à chaque cycle. Dans notre cas, la taille du motif est de 4 bits. Le nombre de champs est au maximum de 9. De ce fait, la durée maximale d'analyse en prenant en compte les différents champs pouvant être analysés, les différents types de sauts entre champs (les sauts entre champs non adjacents appelés dans le tableau sauts relatifs prennent plus de temps que les sauts séquentiels entre champs adjacents) et les pénalités de début et de fin de processus est de 51 cycles. Le temps de cycle actuellement proposé par le circuit d'analyse des IFTs, basé sur l'utilisation de composants FPGA (*Field-Programmable Gate Arrays*) et d'une mémoire de type ZBT

(*Zero Bus Turnaround*) est de 15 ns [4]. Il est cependant envisagé dans le futur d'utiliser des composants permettant un temps de cycle de 12ns. La figure 4 indique les temps d'analyse, les vitesses de classement et les vitesses de commutation minimales correspondant à ces deux latences en prenant en compte une taille minimale à analyser de la taille d'une cellule soit 53 octets.

Latence Circuit	Temps d'analyse	Vitesse min. de classement	Débit min de classement
12 ns	612 ns	1.634 Mc/s	692.8 Mb/s
15 ns	765 ns	1.307 Mc/s	554.6 Mb/s

Figure 4. Capacités de classement en fonction de la latence du circuit d'analyse.

Dans le cas d'une latence du circuit de 12 ns, on peut donc considérer que notre processus de classement n'est pas l'élément bloquant dans notre architecture de contrôle d'accès, celle-ci étant limitée par le débit physique du connecteur. Il en découle que notre processus de classement ne peut provoquer la bufferisation de cellule avant leur classement puisque le processus de classement est plus rapide que l'arrivée des cellules. De ce fait le délai maximal introduit par notre processus de classement est égal au temps maximal d'analyse, c'est à dire 648 ns [7].
Notre approche consiste donc à intégrer cet algorithme de classement dans une architecture fournissant un service de contrôle d'accès au centre du réseau de manière bloquante. Le respect des contraintes de débit et de qualité de service se fait par l'implémentation de notre algorithme sur une architecture matérielle performante appelée IFT. Celle-ci, lorsqu'elle est utilisée avec notre algorithme, garantit une borne maximale de modification de la QoS très faible tout en assurant un débit élevé.

5 Evolutions et perspectives dans VTHD++

Des évolutions sont prévues dans le cadre de VTHD++ : de IPv4 sur ATM, on passe à de l'IPv6 sur Gigabit Ethernet avec augmentation de la largeur d'analyse (de 4 bits vers 8 bits) et du nombre d'octets analysables (de 53 à 256 octets) avec possibilité de contrôle de données applicatives. Cela nécessite aussi la définition de nouveaux paramètres sur lesquelles s'effectue le contrôle d'accès (fig.5).
De nos jours, le Gigabit/10Gigabit Ethernet se présentent de plus en plus comme de sérieux concurrents au protocole ATM car ils assurent l'évolution des réseaux vers le tout IP. Dans cette perspective, France Telecom R&D a développé une nouvelle version des cartes IFT dans laquelle l'unité d'analyse n'est plus la cellule ATM mais le paquet IP. Ces nouvelles cartes permettent d'une part une largeur d'analyse plus importante et d'autre part l'utilisation de mémoires d'un type différent permettant la construction d'une mémoire Trie plus grande et moins onéreuse. Celle-ci permette l'utilisation d'un motif de reconnaissance plus grand, autorisant des vitesses d'analyse plus importantes. La taille de cette mémoire permet également le stockage de politiques de contrôle d'accès de plus grande taille. FT R&D travaille aussi sur une méthode permettant d'éviter la réplication des arbres d'analyse dans la mémoire Trie en conservant au cours de l'analyse d'un flux, l'ensemble des règles applicables. Cette technique permettrait de réduire fortement la taille nécessaire au stockage de la structure de classification sans perdre l'avantage d'une analyse en temps borné.
L'augmentation de la largeur d'analyse devrait faciliter l'utilisation des paramètres de contrôle d'accès tels que des paramètres applicatifs. Il n'est cependant pas évident que notre algorithme qui avait utilisé les redondances pouvant être trouvées dans les politiques de contrôle d'accès pour les réseaux ATM puisse de nouveau tirer partie de celles-ci dans le cas de politiques utilisant de nouveaux paramètres de contrôle d'accès. Il est de ce fait indispensable de pouvoir tester notre algorithme dans le cas de politiques de contrôle d'accès étendues. Ces tests permettront de juger de la nécessité de la définition d'un nouvel algorithme de classement, plus adapté au traitement de règles "longues".

	IPv4				IPv6		
Champs analysés	*Ignorés*	*Traités*	*Filtrés*	*Champs analysés*	*Ignorés*	*Traités*	*Filtrés*
Version		4		Version		6	
HLEN		5		Priority	X		
ToS	X			Ident. Flux	X		
Long totale	X			Long. Data	X		
Ident.	X					0;6;17	
Flags	X			Extensions		41;43;44	
Fragment.	X					50;51;58	
TTL	X					59;60	
Protocole		1;6;17		Lg Extensions		X	
Checksum	X			Nb sauts	X		
@ IP Src			X	@ IP src			X
@ IP Dst			X	@ IP dst			X
TCP port src			X	TCP port src			X
TCP port dst			X	TCP port dst			X
TCP flags			X	TCP flags			X
UDP port src			X	UDP port src			X
UDP port dst			X	UDP port dst			X
ICMP type			X	ICMP type			X
ICMP code			X	ICMP code			X

Figure 5. Tableau comparatif des paramètres de contrôle d'accès IPv4/IPv6

De nouvelles fonctionnalités ont vu le jour et qui cherche à exploiter au mieux cette technologie IFT couplée avec l'algorithme de classement. Le fil directeur de ces recherches étant le souci permanent d'améliorer les fonctions de sécurité offertes par ce contrôleur d'accès. Une première amélioration a porté sur le contrôle des données transitant dans les trames. Une seconde amélioration a été d'ajouter la possibilité de compter les trames. Enfin, la dernière amélioration a été de créer, à partir de la politique d'accès, deux politiques, une pour l'entrée du réseau et l'autre pour la sortie. Ceci permettant un gain de place en mémoire non négligeable.

Conclusion

Dans cet article, nous avons exposé le problème de la sécurité des réseaux informatiques en général, et en particulier les problèmes posés par les équipements intermédiaires dans un réseau haut débit en terme de respect de la QoS. Ces problèmes trouvent aujourd'hui une réponse dans une solution développée par L'ENST de Bretagne en partenariat avec France Telecom. Cette réponse, sous la forme d'un contrôleur d'accès haut débit, assure le maintien de QoS quelques soit le nombre de règles de la politique d'accès. Les nouvelles cartes IFT, récemment développées par France Telecom, permettront de préparer ce contrôleur d'accès pour l'avenir en intégrant notamment l'exploitation de Gigabit Ethernet et d'IPv6.

Remerciements

Les auteurs souhaitent remercier l'ensemble de leurs partenaires : MM. Christian Duret, Hervé Guesdon, Christian Guillemot, Valery Laspreses, Joël Lattmann, Jacques Le Moal, Jean-Louis Simon et O. Paul de FT R&D.

Bibliographie

[1] David Newman, Helen Holzbaur, and Kathleen Bishop, Firewalls: Don't Get Burned, Data Communications, March 1997.
[2] Celoteck Corporation, CellCase622, Security at OC-12c/STM-4 Data rates, Products for Hi-Speed Virtual Private Networking, data Sheet, Octobre 1999
[3] Nathalie Omnès, Analyse d'outils de contrôle de la qualité de service dans les réseaux de paquets haut débit, thèse Irisa Novembre 2001
[4] Centre National d'Etudes des Télécommunications – France Telecom, IP Fast Translator, FT.BD/CNET/DSE/SDL/226/CD, Décembre 1994
[5] Olivier Paul, Le contrôle d'accès dans les réseaux ATM, Thèse de doctorat, université de rennes 1, Février 2001
[6] M. Accarion, C. Boscher, C. Duret, J. Lattmann, Extensive packet header lookup at Gb/s speed for an application to IP/ATM multimedia switching router, in proc. of the WTC/ISS2000 Conference, May 2000.
[7] Olivier Paul, Maryline Laurent, Sylvain Gombault, an asynchronous and Distributed Access Control Architecture for IP over ATM networks, in proc. Of the 15th Annual Computer Security applications Conference, Phoenix, Décembre 1999