

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

**CHARTRE POUR LE DEVELOPPEMENT DE L'OFFRE LEGALE
DE MUSIQUE EN LIGNE, LE RESPECT DE LA PROPRIETE
INTELLECTUELLE ET LA LUTTE CONTRE LA PIRATERIE NUMERIQUE**

**ETUDE DES SOLUTIONS DE FILTRAGE DES ECHANGES
DE MUSIQUE SUR INTERNET DANS LE DOMAINE
DU *PEER-TO-PEER***

RAPPORT D'ETUDE

<u>REF DOCUMENT</u>	
<u>AUTEURS</u>	A. Brugidou, G. Kahn
<u>DATE VERSION</u>	09/03/2005 18:19:00

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

Historique des modifications			
Version	Date	Auteur	Modification apportée
0.1	28 août 2004	A. Brugidou	Création et rédaction initiale du document
0.12	14 novembre 2004	A. Brugidou	Enrichissement du document pour intégrer les éléments issus des auditions et ajout de la synthèse
0.17	11 décembre	A. Brugidou	Finalisation du corps du document
0.20	17 décembre	A. Brugidou	Ajout des annexes
0.22	22 décembre	A. Brugidou	Modification de la table des matières
V3Jan	04 janvier	G. Kahn	Apport de compléments sur la synthèse
V4Jan	05 janvier	A. Brugidou, G. Kahn	Finalisation du document
V10	09 mars	A. Brugidou, G. Kahn	Prise en compte de remarques

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

Table des matières

1. Introduction	5
1.1. Charte et mission des experts	5
1.2. Structure de l'étude	6
1.3. Démarche adoptée	6
1.4. Technologies du <i>peer-to-peer</i>	7
1.4.1. Introduction	7
1.4.2. Importance du trafic <i>peer-to-peer</i>	7
1.5. Autres tendances et évolutions technologiques	10
1.5.1. NAT (Network Address Translation)	10
1.5.2. Encryptage et tunnelling	11
1.5.3. Protocole IP V6	12
2. Synthèse	13
2.1. Constats généraux	13
2.2. Le filtrage	14
2.3. L'approche « Radar »	16
2.4. Sur le plan technique, nécessité d'expérimenter	17
2.5. Besoin de mettre en œuvre plusieurs solutions en parallèle	18
3. Analyse des solutions de filtrage	19
3.1. Introduction	19
3.2. Modes de déploiement envisageables	19
3.3. Familles de solutions de filtrage	20
3.3.1. Familles identifiées dans l'étude du SNEP et présélection	20
3.3.2. Famille de solutions considérées dans la présente étude	22
3.4. Filtrage de protocole	24
3.4.1. Schéma de principe	24
3.4.2. Mode « Filtrage systématique »	25
3.4.3. Mode « Filtrage à la demande »	28
3.5. Filtrage de contenu	32
3.5.1. Schéma de principe	32
3.5.2. Mode « Radar »	34
3.6. Filtrage sur le poste client	36
3.6.1. Introduction	36
3.6.2. Schéma de principe des solutions à serveur central	37
3.6.3. Mode « Filtrage à la demande »	37
3.6.4. Conclusion	38

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

3.7. Synthèse	39
4. Expérimentations recommandées	40
4.1.1. (E1) Solution filtrage poste client, mode à la demande	40
4.1.2. (E2) Solutions orientées protocole et contenu, « observatoire de trafic P2P »	40
5. Annexe 1 – Auditions organisées	43
6. Annexe 4 – Etudes de cas	44
6.1. Introduction	44
6.2. Filtrage de protocole P_Cube dans le contexte d'un FAI 1	44
6.2.1. Architecture du FAI 1	44
6.2.2. Solution P_Cube	45
6.2.3. Positionnement des boîtiers – Scénario 1	45
6.2.4. Positionnement des boîtiers – Scénario 2	46
6.2.5. Contraintes induites chez le FAI	46
6.3. Filtrage de poste client dans le contexte d'un FAI 1	48
6.3.1. Introduction	48
6.3.2. Principe de mise en œuvre	49
6.3.3. Critères identifiés par le FAI 1 pour répondre aux besoins de filtrage de la charte	49
6.4. Filtrage de contenus Audible Magic dans le contexte d'un FAI 2	51
6.4.1. Solution Audible Magic	51
6.4.2. Architecture du FAI 2	51
6.4.3. Scénarios de positionnement des boîtiers	52
6.4.4. Décompte des boîtiers	53
6.4.5. Contraintes induites chez le FAI	54
6.4.6. Cas d'utilisation de la solution de filtrage de contenus	55
6.5. Filtrage de protocole Allot dans le contexte d'un FAI 3	55
6.5.1. Architecture du FAI 3	55
6.5.2. Solution Allot NetEnforcer	56
6.5.3. Scénarios de positionnement des boîtiers	56
6.5.4. Décompte des boîtiers	57
6.5.5. Contraintes induites chez le FAI	58

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

1. Introduction

1.1. Charte et mission des experts

La "Charte d'engagements pour la lutte contre la piraterie et pour le développement des offres légales de musique en ligne" a été signée le 27 juillet 2004 sous l'égide du Gouvernement français, entre les fournisseurs d'accès à Internet, les distributeurs, les distributeurs en ligne, les sociétés d'auteurs et les producteurs.

Le Ministre de la Culture et de la Communication, le Ministre délégué à l'Industrie et le Ministre délégué à la Recherche ont nommé deux experts, Gilles Kahn, président de l'Institut National de Recherche en Informatique et Automatique (INRIA) et Antoine Brugidou, responsable des activités Service Public au sein de la société de conseil et ingénierie Accenture.

La mission des experts est définie au chapitre 4.2 de la charte :

« Sous l'égide de deux experts désignés par les pouvoirs publics, étudier avant le 1er octobre 2004 les solutions proposées par les industriels de la musique (étude transmise par le SNEP) en matière de filtrage, à la demande des internautes, dans le domaine du peer to peer.

Si les experts l'estiment nécessaire et possible sur les plans techniques, notamment en terme de qualité de service, et économiques, et sous leur supervision, expérimenter via un ou plusieurs fournisseurs d'accès, dans les délais recommandés par les experts, certaines de ces solutions. Un bilan de l'expérimentation est établi de manière à proposer, si c'est possible sur les plans techniques et économiques, dans des conditions réellement incitatives, le bénéfice d'un de ces systèmes aux abonnés qui le souhaitent. Les conditions de l'expérimentation et sa prise en charge financière, ainsi que de l'éventuel déploiement, seront précisées dans des conventions particulières.

Pendant la durée de l'étude et de l'éventuelle expérimentation, les industriels de la musique s'abstiennent de solliciter des mesures de filtrage dans toute action contentieuse ».

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

1.2. Structure de l'étude

La mission des experts définie dans la Charte a été déclinée en deux volets :

- **Un volet technique avec l'analyse des solutions de filtrage.** Son objectif est d'établir un point de vue sur la faisabilité de mise en œuvre des solutions de filtrage dans le domaine du *peer-to-peer* disponibles à ce jour, sur la base de l'étude menée par le SNEP¹, de l'audition des différents acteurs notamment les fournisseurs de technologies et les FAI, et avec la mise en perspective des modalités prévues par la Charte.
- **Un volet de définition des expérimentations,** dont l'objectif est de proposer les objectifs d'une ou plusieurs expérimentations en grandeur réelle, en partenariat avec un ou plusieurs FAI et les fournisseurs de solutions techniques. Ces expérimentations permettront de valider les conclusions du volet précédent.

Chaque volet fait l'objet d'un chapitre particulier du rapport.

Par ailleurs, il nous a semblé opportun de rappeler en annexe un ensemble d'éléments de contexte sur les technologies du *peer-to-peer* et les principales évolutions technologiques qui impactent la problématique de filtrage.

1.3. Démarche adoptée

L'étude a été menée selon la démarche suivante :

- Préparation :
 - ◆ Identification des participants à convoquer aux auditions et prises de contact.
 - ◆ Formalisation des ordres du jour et convocations.
- Auditions individuelles :
 - ◆ Auditions individuelles des différentes catégories d'acteurs impliqués dans l'étude (Cap Gemini, FAI, ayants droits de l'industrie de la musique, fournisseurs de technologie).
 - ◆ Collecte des remarques sur les principaux aspects techniques de l'étude (familles de solutions envisageables, présélection de solutions et choix de la solution étudiée, étude de dimensionnement à la cible).

¹ Cette étude a été rendue publique et est par exemple accessible sur le site des Echos (http://www.lesechos.fr/lettrespro/presentation/telecom/flash/rapport_filtage_capgemini_france.pdf)

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- ♦ Elaboration de scénarios pour l'expérimentation.
- Sessions de travail technique complémentaires :
 - ♦ Réunions de travail menées afin de détailler la possibilité et le cas échéant les principales modalités techniques de la mise en œuvre de solutions de filtrage.
- Mise en œuvre de sessions plénières : réunions contradictoires rassemblant les différents acteurs concernés et discussion autour des solutions proposées :
 - ♦ Une première session portant sur les sujets techniques : revue de l'étude menée par le SNEP et analyse des différents acteurs.
 - ♦ Une seconde session de portant sur le cadrage d'une expérimentation : identification et analyse de scénarios d'expérimentation.
- Synthèse :
 - ♦ Rédaction du rapport d'étude.

1.4. Technologies du *peer-to-peer*

1.4.1. Introduction

L'étude de la pertinence de la mise en place de solutions de filtrage des protocoles *peer-to-peer* suppose de prendre en compte un ensemble d'éléments de contexte technique :

- Les technologies du *peer-to-peer* – importance du *peer-to-peer* au sein du trafic géré par les FAI, impact techniques, évolution des protocoles *peer-to-peer*.
- Les technologies de l'Internet – développement d'IP V6 et du cryptage, etc.

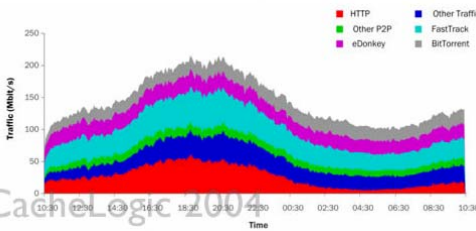
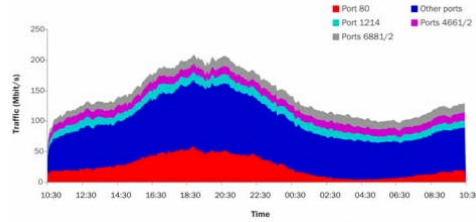
La société CacheLogic a publié en juillet dernier une analyse du trafic *peer-to-peer*. Elle porte sur le premier semestre 2004, et avait pour but de mettre en évidence l'intérêt que présente pour un fournisseur d'accès la gamme de produits de surveillance du trafic sur les réseaux IP.

Les FAI français n'ayant pas fourni d'informations détaillées sur le trafic *peer-to-peer* en France, nous reprenons ci-après les informations publiées dans l'étude de CacheLogic² qui fournissent un ordre de grandeur pertinent.

1.4.2. Importance du trafic *peer-to-peer*

Les quatre tableaux ci-dessous, fournis par la société CacheLogic illustrent l'importance et l'évolution rapide du trafic véhiculé par des protocoles *peer-to-peer*.

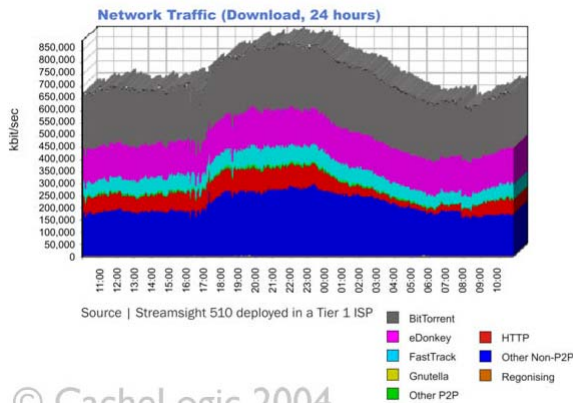
² <http://www.cachelogic.com/research/index.php>



© CacheLogic 2004

Le diagramme ci-contre montre la proportion du trafic par port TCP et par protocole constaté par CacheLogic chez un FAI grand public anglais.

Il fait apparaître que la reconnaissance par port n'est pas suffisante pour reconnaître le trafic *peer-to-peer*: l'utilisation de ports configurables dans les applications *peer-to-peer* clientes, l'allocation dynamique de ports ou l'utilisation des ports standard (http, mail, ...) par les applications *peer-to-peer* rend inefficace une reconnaissance au niveau du port.³



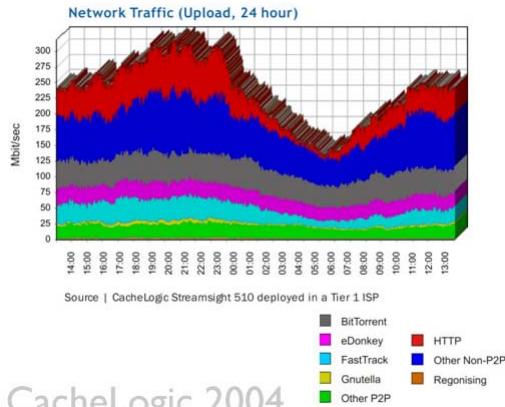
© CacheLogic 2004

Le diagramme ci-contre montre la proportion du trafic descendant réparti par protocole, constaté par CacheLogic chez un FAI grand public anglais.

Il fait apparaître que les flux *peer-to-peer* représentent la majeure partie du trafic chez ce FAI – le volume *peer-to-peer* représentant plus du double du trafic http (navigation web) pendant les périodes de pic de charge du soir et plus de dix fois le trafic http pendant les autres périodes.⁴

³ <http://www.cachelogic.com/research/slide5.php>

⁴ <http://www.cachelogic.com/research/slide3.php>

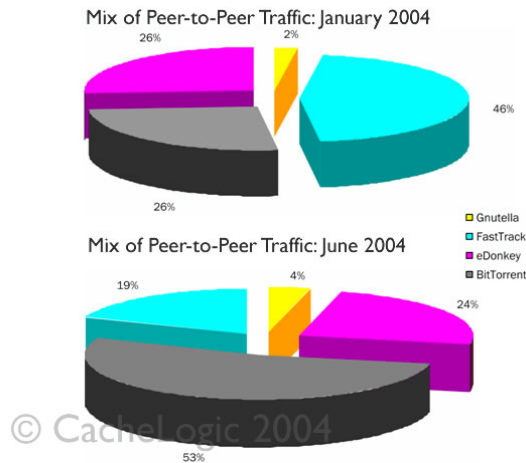


© CacheLogic 2004

Le diagramme ci-contre montre la proportion du trafic montant réparti par protocole, constaté par CacheLogic chez un FAI grand public anglais.

Il confirme que le trafic *peer-to-peer* est par nature un trafic symétrique en matière de ratio trafic descendant / montant (alors que les protocoles traditionnels type http sont asymétriques avec une proportion de trafic descendant beaucoup plus importante).⁵

⁵ <http://www.cachelogic.com/research/slide7.php>



Le diagramme ci-contre montre la proportion du trafic descendant par protocole *peer-to-peer* en comparaison entre janvier et juin 2004, constatée par CacheLogic chez un FAI grand public anglais.

Il fait apparaître que la répartition du trafic *peer-to-peer* évolue rapidement, les utilisateurs changeant de protocole : si l'utilisation de Kazaa diminue fortement (passage de 46% à 19% en 6 mois), Bittorrent augmente rapidement (passage de 26% à 53% en 6 mois).⁶

1.5. Autres tendances et évolutions technologiques

1.5.1. NAT (Network Address Translation)

Le déploiement de fonctions permettant la connexion de plusieurs équipements équipés de carte réseau (USB, Ethernet, WiFi) se fait progressivement avec la montée en puissance du nombre d'équipements aptes à une connexion réseau ou un accès Internet (PC fixes, PC portables, équipements de type AirPort Express permettant la diffusion de flux audio ou vidéo vers les matériels audiovisuels, etc.).

Ces fonctions sont soit intégrées aux boîtiers fournis par les FAI dans le cadre d'offre WiFi par exemple, soit prennent la forme de matériels externes au boîtier FAI achetés par les abonnés (routeur / hub et points d'accès WiFi) et positionnés en aval du modem.

Ces solutions fournissent pour la plupart des fonctions de gestion d'un plan d'adressage IP local (y compris DHCP) et de fonctions NAT (Network Address Translation).

Ceci ne présente pas a priori une contrainte dans le contexte de la Charte, puisque le filtrage se fait à la demande de l'abonné, donc pour l'adresse IP fournie par le FAI. Dans un contexte NAT chez un particulier, l'ensemble des équipements connectés au routeur ou point d'accès Wifi de l'abonné seraient bloqués.

⁶ <http://www.cachelogic.com/research/slide9.php>

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

1.5.2. Encryptage et tunnelling

Les solutions de filtrage de protocole se fondent sur la reconnaissance de signatures au niveau des trames réseau échangées depuis le poste client de l'internaute afin de déterminer s'il s'agit d'un flux *peer-to-peer* ou non.

Par exemple, la maquette mise en œuvre dans l'étude remise par le SNEP (§4.4) a consisté à paramétrer dans l'équipement ALLOT une règle bloquant de reconnaissance de signatures « k a z a a » et « .torrent » dans les messages réseaux.

La mise en place de cryptages pourrait rendre inopérante (ou complexifier) la détection de telles trames. Ce cryptage pourrait être mis en place :

- Soit par la modification des protocoles *peer-to-peer* (en faisant par exemple évoluer les trames de connexion ou le suffixe des fichiers) – ce qui suppose à la fois une modification des applications clientes installées sur les postes de travail des internautes et des serveurs (serveurs Kazaa, eDonkey ou trackers Bittorrent) ;
- Soit par la mise en place de protocole de tunneling de type SSL/HTTPS ou SSH, par exemple.

Certains protocoles *peer-to-peer* sont déjà encryptés, notamment :

- FreeNet (Winny) ;
- SSL (SoftEther, EarthStation5, Filetopia) ;
- SSH (SoftEther).

L'encryptage et le tunneling génèrent de fait une complexité supplémentaire pour les solutions techniques de filtrage. Néanmoins, la disponibilité du code source des clients, notamment pour les clients développés en mode Open Source ou équivalent (ex : eMule, Bittorrent), permettent d'analyser la manière dont ces protocoles sont mis en œuvre, et le cas échéant de mettre en place une reconnaissance sur la partie amont du protocole (connexion, négociation, passage en mode crypté) (analyse comportementale). Une telle solution est par exemple mise en place par Allot, qui affirme entre autres filtrer les protocoles SoftEther, EarthStation5 et Filetopia⁷.

⁷ Commentaires Capgemini / Note AFA – 091104

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
----------------------	------------------------	----------------------------------------------------------------------------

1.5.3. Protocole IP V6

L'évolution du protocole Internet vers IP V6 va apporter, outre l'extension des plages d'adressage IP disponibles, des évolutions sur les fonctions d'authentification et de sécurité de TCP/IP, avec notamment la généralisation du protocole IPSec et des fonctions de chiffrement DES.

IP V6 n'est néanmoins à ce stade pas encore entièrement déployé sur les plates-formes des FAI, et la montée en puissance de ce protocole pour le grand public reste à amorcer.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

2. Synthèse

2.1. Constats généraux

Les techniques de peer to peer sont en constante évolution :

Comme on peut s'y attendre pour un domaine technologique en émergence, les plates-formes peer to peer évoluent rapidement. Au-delà des quelques plates-formes les plus connues, il existe en réalité un très grand nombre de plates-formes qui utilisent différentes techniques rendant toujours plus difficiles le repérage des pirates et le filtrage des échanges. En fait cette évolutivité s'accélère, et une même plate-forme peut faire évoluer son protocole de connexion rapidement et le diffuser en quelques heures à l'aide de l'Internet. Il est donc important de comprendre que toute activité d'analyse ou de filtrage ne peut être que fortement évolutive et mise à jour régulièrement.

Il existe plusieurs familles de technologies dignes d'intérêt capables d'avoir un impact sur le piratage :

Il existe plusieurs technologies qui prétendent réduire l'activité de piratage : le filtrage des protocoles (par ex. Allot, Cisco P_Cube), la création de leurres (par ex. CoPeerRight), l'analyse des contenus (par ex. AudibleMagic), les solutions poste client (par ex. CyberPatrol, Cisco CSA). Ces technologies sont souvent assez sophistiquées et capables de s'adapter à l'évolution technologique des plates-formes. Il semble donc qu'il existe en vis-à-vis d'un déploiement d'applications « peer to peer » en pleine explosion, différentes sociétés présentant des solutions technologiques de haut niveau qui méritent d'être expérimentées.

Il est probable que les FAI⁸ disposent déjà d'outils d'analyse et qu'à défaut ils devraient s'en procurer :

Les technologies mises en avant par le SNEP (Allot) n'ont pas en fait comme mission première le filtrage du piratage. Elles ont été conçues pour l'analyse du trafic Internet et la mise en œuvre d'actions permettant de le réguler au mieux dans l'intérêt d'une entreprise ou d'un FAI. Ce type d'outil, qui permet d'avoir une analyse approfondie des trafics transitant sur le réseau, présente un intérêt évident pour tout fournisseur ou gros utilisateur de bande passante. Il est difficile d'imaginer que les FAI ne disposent d'aucun outil équivalent.

⁸ Fournisseur d'Accès Internet

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

2.2. Le filtrage

En dépit des réactions de défense probables la mise en œuvre d'actions de filtrage ou équivalent peut avoir un effet supérieur à un an :

Il est évident que si le filtrage des échanges (ou équivalent) prenait de l'envergure (au niveau national voire au niveau international) les actions de résistance se multiplieraient rendant d'autant plus difficile leur mise en oeuvre. Pour autant, compte tenu de l'évolution des technologies, nous pensons que les actions proposées peuvent avoir un effet sur une durée supérieure à une année, ce qui à l'échelle des évolutions Internet est déjà significatif. Ceci est d'autant plus vrai que les actions de filtrage couvrent un nombre d'internautes limités (filtrage à la demande en France) qui ne suscite pas une réaction internationale des plates-formes et des protocoles filtrés. On peut même penser que, comme pour les virus et les antivirus, les fournisseurs de solution pourront trouver jusqu'à un certain point (cryptage) des parades technologiques aux résistances identifiées. Les techniques de filtrage sur le poste de travail peuvent aussi permettre de traiter plus facilement ce point (blocage de l'installation ou l'exécution des clients peer to peer sur le poste de travail).

Il faut constamment garder à l'esprit que le filtrage à la demande obtiendra un nombre d'abonnés limité :

Le raisonnement qui conduit à la création d'un abonnement volontaire repose sur plusieurs appréciations :

- ◆ proposer une offre de filtrage permettra aux internautes d'être sensibilisés aux risques des échanges d'œuvres protégées (virus, sanctions...) et d'exercer leur responsabilité en toute connaissance de cause ;
- ◆ certaines personnes utiliseront cet abonnement pour se débarrasser d'un problème dont elles ne souhaitent pas s'occuper (exemple les entreprises mais aussi les parents) ;
- ◆ le succès de l'abonnement filtré sera très directement lié à la prise de conscience du caractère illégal des échanges d'œuvres protégées et des sanctions encourues.

Les opposants à ce type de filtrage remarquent que :

- ◆ les pirates adultes (qui sont nombreux) ne seront pas nécessairement enclins à s'auto filtrer et les parents auront du mal à imposer un abonnement filtré à leurs enfants ;
- ◆ l'existence d'usages licites d'échanges en peer to peer et le fait que les systèmes peer to peer n'aient pas, jusqu'à présent, été jugés illégaux en tant que tels pourrait créer une confusion chez les internautes, face à la proposition d'une offre de filtrage ;
- ◆ l'apport d'une formule d'abonnement limitée à quelques pourcents de la population apparaît bien limité et par ailleurs coûteux.

Ainsi, à ce jour, les supporters de l'abonnement volontaire comme leurs opposants semblent être d'accord sur un point : le pourcentage d'abonnés volontaires ne sera pas élevé.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

Cet élément est important car il signifie que les investissements pour réaliser du filtrage à la demande (si cette approche était retenue) doivent être cohérents avec le nombre d'internautes susceptibles de prendre ce type d'abonnement.

Le filtrage à grande échelle sur le réseau pourrait se heurter à une problématique de mise en œuvre :

Le filtrage à grande échelle du trafic peer to peer sur un très grand nombre d'internautes pourrait poser un problème de coûts de mise en œuvre et de maintenance. Compte tenu de l'évolution des architectures des FAI, un tel filtrage supposerait la mise en œuvre d'un nombre significatif de boîtiers dans le réseau, une administration de ces boîtiers et probablement des évolutions de l'architecture réseau proprement dite – ainsi que des évolutions au niveau des systèmes d'information.

Le filtrage à la demande au niveau des FAI apparaît en première analyse techniquement possible, mais sa mise en œuvre supposerait de mener un ensemble de projets techniquement complexes, avec un investissement et des coûts de fonctionnement très significatifs.

La mise en œuvre d'un filtrage à la demande chez les FAI suppose la création d'une dérivation (ex : routage et tunnels) vers une plate-forme susceptible de traiter l'ensemble des abonnements filtrés. Ceci suppose des évolutions significatives de l'architecture réseau du FAI (politiques de routage, mise en œuvre de tunnels L2TP, spécialisation de matériels ou le cas échéant déploiement de nouveaux matériels notamment de type BAS, etc.). Il s'agirait d'une évolution significative des architectures des FAI, comparable, pour certains FAI, à la création d'un FAI virtuel sur leur réseau.

Au-delà du réseau, la mise en œuvre d'un filtrage à la demande suppose également de lancer des projets d'évolution du système d'information (intégration entre le SI, l'OSS et les solutions de filtrage), ainsi que d'autres projets non techniques (vente et marketing, etc.).

Le filtrage sur le poste de travail apparaît comme techniquement le meilleur compromis pour une offre à la demande :

Plusieurs technologies sont dès aujourd'hui disponibles pour permettre un filtrage à la demande sur le poste de travail de l'internaute. Le filtrage sur le poste de travail est une solution techniquement plus facile à déployer que des solutions impactant l'architecture réseau. Elle est techniquement robuste et plus efficace que le filtrage sur le réseau dans le contexte d'une offre à la demande. Par ailleurs, les FAI proposent déjà des solutions dont la mise en œuvre est techniquement comparable (solutions de filtrage parental, d'antivirus ou de firewall par exemple).

La problématique de ce type de solution est donc moins technique qu'opérationnelle. Le mode de commercialisation de cette offre sera déterminant pour son succès.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

2.3. L'approche « Radar »

Au-delà des modes de mise en œuvre du filtrage déjà évoqués, il pourrait être intéressant d'explorer une approche de type « Radar » préventif :

Outre le filtrage systématique envisagé dans l'étude du SNEP et le filtrage à la demande de l'internaute figurant dans la charte, on peut imaginer une mise en œuvre de type « Radar », par référence aux systèmes utilisés pour le trafic routier. Dans une telle mise en œuvre, des mécanismes d'observation et de filtrage seraient mis en place sur certains points d'observation sur le réseau, de manière pérenne (« radars fixes ») ou temporaire (« radars mobiles »). Les radars permettraient d'identifier les événements frauduleux et d'enregistrer les informations nécessaires pour venir alimenter des opérations de sensibilisation voire juridiques.

Au niveau des FAI, une approche du type radar pourrait présenter des avantages :

Les FAI pourraient tirer avantage d'une analyse un peu plus systématique du trafic sous la forme de radars fixes ou mobiles, capables par exemple d'identifier les éventuels pirates et de les mettre en garde de façon à prévenir des abus. Une logique de radar automatique industriel pourrait être envisagée. Elle permettrait de :

- ◆ contourner le problème du nombre d'internautes abonnés volontaires (tout le monde peut se retrouver identifié par un radar),
- ◆ réduire les problèmes de mise en œuvre en évitant la mise en place d'une dérivation et en dimensionnant le nombre de radars à une hauteur acceptable par les FAI,
- ◆ donner des moyens d'investigation et de marketing puissants aux FAI.

Si un certain nombre de technologies semblent exister pour lutter contre le piratage, leur mise en œuvre est significativement simplifiée dans une approche de type radar où les volumes de boîtiers sont moins importants, et les impacts sur les architectures des FAI plus facilement maîtrisables (nombres de « radars » et localisation).

Dans la mesure où certains usages du peer to peer sont légaux, il paraît plus pertinent d'envisager une solution de type « analyse de contenus ».

Néanmoins cette approche soulève des questions de nature juridique et technique :

La mise en place d'une approche de type « radar » est susceptible de soulever des difficultés de mise en œuvre d'ordre juridique. Dès lors, et si le principe du radar est retenu, une étude de faisabilité juridique plus approfondie devra être menée afin de définir :

- ◆ s'il y a lieu d'aménager un régime juridique spécifique, ou si le potentiel législatif et réglementaire actuel permet d'envisager ce type de contrôle
- ◆ s'il n'y pas lieu d'adapter la législation, quels sont les critères permettant d'assurer le respect des droits précités (notamment sécurité et confidentialité des données

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

personnelles et le secret de la correspondance et d'une manière générale le respect de la vie privée) dans le cadre de la mise en oeuvre des radars systématiques (fixes ou mobiles) afin d'assurer leur licéité.

Un scénario « radar » alternatif pourrait consister à utiliser des systèmes situés en « bout de réseau » (du type de ceux proposés par CopeerRight Agency ou Advestigo) et non sur le réseau. Ce scénario présente l'avantage de lever, au moins partiellement, la contrainte topographique (pas de limite a priori au territoire observable par un équipement) mais l'inconvénient de ne pas s'auto-alimenter par la simple observation des flux (elle nécessite une recherche proactive).

2.4. Sur le plan technique, nécessité d'expérimenter

Seules des expérimentations avec les FAI permettront de mesurer réellement la faisabilité d'une solution :

La diversité des points de vue quant à l'appréciation des modalités techniques et des coûts de mise en oeuvre des différentes solutions proposées montrent que seules des expérimentations en grandeur réelle chez des FAI permettront de mesurer de façon factuelle les coûts et les charges de mise en oeuvre de ces solutions. A ce stade compte tenu des enjeux, ces coûts ne nous paraissent pas rédhitoires et justifient qu'un travail expérimental plus approfondi soit réalisé avec les acteurs techniques les mieux placés pour mesurer les coûts de mise en oeuvre et de maintenance de ces solutions (c'est-à-dire les FAI).

Plusieurs solutions doivent être évaluées en parallèle par plusieurs FAI :

Compte tenu de l'évolutivité technologique du peer to peer, il nous paraît dangereux de ne miser que sur une seule technologie. Outre les critiques que pourraient susciter une telle approche (les pouvoirs publics ont fait le mauvais choix avec le filtrage, il existe des techniques plus efficaces et meilleures), une véritable analyse in situ permettrait de comparer réellement les résultats aux moyens mis en oeuvre.

Nous recommandons deux expérimentations :

- ◆ Une solution de type filtrage sur le poste client (type Cyberpatrol ou Cisco CSA), expérimentée en mode à la demande ;
- ◆ Un « Observatoire du Peer to peer » s'appuyant sur une solution orientée protocole (type Allot ou Cisco P_Cube) et/ou contenu (type Audible Magic ou Advestigo) utilisée en mode observation et analyse statistique de trafic ;

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

2.5. Besoin de mettre en œuvre plusieurs solutions en parallèle

Au total, l'approche doit comprendre un ensemble de solutions mises en œuvre en parallèle. En effet, il n'existe pas une seule approche possible pour faire face au problème posé :

Offres légales de musique sur Internet, filtrage à la demande sur le poste client, mise en œuvre de radars chez les FAI, politique de communication forte pour décourager les pirates, contre-attaques sur le web par la création de leurres, c'est un ensemble de mesures coordonnées qui permettra de réduire le piratage à des proportions acceptables. Le caractère fortement évolutif des technologies mises en œuvre ne permet pas de parier sur une solution en particulier.

Les différentes approches retenues doivent être articulées pour se renforcer :

Le tableau ci-dessous synthétise les différentes approches, les conclusions des analyses effectuées dans l'étude et les recommandations associées :

Faisabilité et pertinence	Famille de solution	Observation et analyse de trafic	Filtrage systématique	Filtrage à la demande	Radar
Faisabilité technique	Filtrage de protocole	Pertinent Expérimentation recommandée	Difficile	Peu pertinent	Non retenu (pas de qualification des contenus)
	Filtrage de contenu	Pertinent Expérimentation recommandée	Non pertinent	Peu pertinent	A étudier
	Filtrage sur le poste client	Non applicable	Non applicable	Pertinent Proposable par les FAI Expérimentation recommandée	Non applicable
Faisabilité de mise en œuvre		Pertinent	Non retenu	Pertinent Option proposée par les FAI et souscrite par les internautes	A étudier en prenant en compte les apports additionnels (analyse des flux)
Pertinence		Pertinent Dans le cadre d'un « observatoire de trafic Peer to peer » pour étayer des actions de communication	Non retenu	Pertinent si le nombre d'internautes souscrivant à l'option est suffisant	A étudier pour dissuader les internautes

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

3. Analyse des solutions de filtrage

3.1. Introduction

Concernant les solutions de filtrage, la Charte signée le 27 juillet évoque au §4.2 « les solutions proposées par les industriels de la musique (étude transmise par le SNEP) en matière de filtrage, à la demande des internautes, dans le domaine du peer-to-peer ».

En l'absence d'expression de besoin formalisée à ce stade, nous présentons ci-après différents modes de déploiement envisageables qui apparaissent pertinents pour l'évaluation des solutions de filtrage.

Ces modes de déploiement s'appuient sur :

- La Charte signée le 27 juillet ;
- L'étude transmise par le SNEP ;
- Les fonctionnalités des solutions technologiques envisagées .

Ensuite, ce rapport d'étude présente une analyse des différentes solutions de filtrage vis-à-vis de chacun des modes de déploiement envisageables.

3.2. Modes de déploiement envisageables

Les principaux modes de déploiement envisageables sont les suivants :

- **« Filtrage systématique »**
Ce mode est celui envisagé dans l'étude transmise par le SNEP :
 - ◆ Filtrage de l'ensemble des internautes.
 - ◆ Filtrage de la totalité du trafic.
- **« Filtrage à la demande »**
Ce mode est celui envisagé par la Charte :
 - ◆ Filtrage uniquement des internautes en ayant fait la demande.
 - ◆ Filtrage de la totalité du trafic généré par les internautes ayant fait la demande de filtrage.
- **« Radar »**
Ce mode est un des modes proposés lors des auditions par les fournisseurs de solutions :

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- ◆ Mise en œuvre de points d'observation sur le réseau. Ces points d'observation peuvent être mis en place de manière pérenne (« radars fixes ») ou temporaire (« radars mobiles »).
- ◆ Observation de l'ensemble du trafic passant par les points d'observation.
- ◆ Observation de la totalité des internautes à l'origine du trafic observé.
- ◆ Identification d'évènements frauduleux (ex : téléchargement effectué par un internaute d'un fichier musical protégé par des droits d'auteurs) et historisation des caractéristiques techniques de cet évènement (adresse IP, nom du fichier, protocole P2P utilisé, etc.).
- ◆ Fourniture des éléments historisés afin d'alimenter des opérations de prévention ou juridiques.

3.3. Familles de solutions de filtrage

3.3.1. Familles identifiées dans l'étude du SNEP et présélection

L'étude fournie par le SNEP⁹ a identifié cinq familles de solutions :

Types de solutions	Principales acteurs du marché
Solutions orientées « QoS »	ALLOT - Netenforcer KAC1020 Packeteer - PS 8500 ISP Sandvine - PPE8200 IPANEMA
Solutions orientées « Flow based switch »	Ellacoya 1600 - E12TX - E2GIG - AC Caspian Networks - Apeiro P-Cube
Solutions orientées filtrage réseaux	Routeurs Firewall (Cisco, Checkpoint, ...)
Solutions orientées IDS/IDP	Netscreen IDP1000
Solutions orientées filtrage de contenu	Audible Magic

⁹ Rapport_filtfrage_capgemini_france.pdf

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

Caractérisations de certaines solutions effectuées dans l'étude du SNEP :

- Les outils d'optimisations de réseaux (QoS) :

Les outils de QoS (Qualité de Service) sont des « appliances » (solution packagées : matériel et logiciel) permettant la gestion des priorités des flux. Ils ont été conçus à l'origine pour classer les flux Internet afin de leur donner une priorité destinée à gérer la bande passante d'un réseau. Ils peuvent ainsi limiter (le blocage étant un cas particulier de limitation) le débit pour un type de flux, et garantir ainsi une qualité de service pour les flux de données critiques. L'implémentation de la QoS est systématiquement en « coupure », c'est à dire que le trafic à analyser doit passer au travers de l'appliance afin d'être traité.

- Les IDS/IDP (Intrusion Detection and prevention) :

Les IDS/IDP sont des appliances qui permettent de détecter et/ou de prévenir une attaque Internet. Ces outils ne possèdent pas la faculté de trier les différentes sessions par flux ; ils se contentent d'analyser chaque paquet afin d'y retrouver soit un comportement, soit une signature connue. Il est possible de placer ce type d'appliance soit en « coupure » (comme pour la QoS), soit en « port mirroring » (redirection du trafic pour analyse).

- Les Flow-Based Switches

Les « flow based switches » sont des commutateurs qui n'agissent plus par reconnaissance exacte du trafic mais par classification par flux. Il est en effet possible de catégoriser les flux générés par le trafic Internet en fonction du type de trafic. On différencie ainsi le trafic interactif du trafic non interactif qui est typiquement un trafic *peer-to-peer*. Cependant, la plupart de ces appliances n'intervenant pas au niveau applicatif, il est difficile de ne pas impacter d'autres trafics comme le FTP passif.

A l'issue d'une analyse de ces familles de solutions, l'étude du SNEP a constitué une présélection :

- D'une part en écartant les familles de solutions orientées filtrage réseaux, IDS/IDP et filtrage de contenu ;
- D'autre part, sur les familles QOS et Flow Based Switch, en identifiant une liste réduite de produits en vue d'une étude comparative détaillée :

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

Types de solutions	Shortlist (solutions retenues pour l'étude comparative)
Solutions orientées « QoS »	ALLOT - Netenforcer KAC1020 Packeteer - PS 8500 ISP
Solutions orientées « Flow based switch »	Ellacoya 1600 - E12TX - E2GIG - AC
Solutions orientées filtrage réseaux	Néant
Solutions orientées IDS/IDP	Néant
Solutions orientées filtrage de contenu	Néant

Enfin, l'étude du SNEP a retenu la solution ALLOT pour effectuer un ensemble de tests dont les résultats ont été documentés.

3.3.2. Famille de solutions considérées dans la présente étude

3.3.2.1. Analyse des familles identifiées dans l'étude du SNEP

Au-delà des solutions de filtrage de protocole présélectionnées dans l'étude du SNEP, nous avons effectué l'analyse suivante :

- Solution de filtrage réseau : ces solutions ne répondent effectivement pas aux besoins de filtrage tels que définis dans la Charte :
 - ◆ URL et adresse IP : Ces moyens sont adaptés pour interdire l'accès à des sites qui proposent des contenus illégaux mais ne répondent pas aux impératifs de neutralisation du *peer-to-peer*.
 - ◆ Ports : c'est un moyen basique pour filtrer certains ports qui sont spécifiques aux réseaux *peer-to-peer*, mais des moyens de contournements existent qui rendraient très rapidement inopérante cette solution si elle constituait l'unique filtrage mis en place. Ceci est conforté par l'étude menée par CacheLogic présentée plus haut.
- Solution Filtrage de contenu : il nous a semblé important de considérer ce type de solutions dans la présente étude. La société Audible Magic, notamment, dispose d'une solution de type industrielle et de partenariats avec des acteurs comme la RIAA aux Etats-Unis et SonyConnect qui la rendent pertinente.

Il est à noter que si le filtrage d'URL et d'adresses IP ne permettent pas de neutraliser le peer to peer à eux seuls, il peut apporter une contribution comme tout premier niveau de barrière – par exemple pour certains clients des FAI dont le niveau de connaissance techniques serait limité.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

3.3.2.2. Familles de solution considérées dans la présente étude

Ainsi, nous avons retenu les familles de solution de filtrage suivantes :

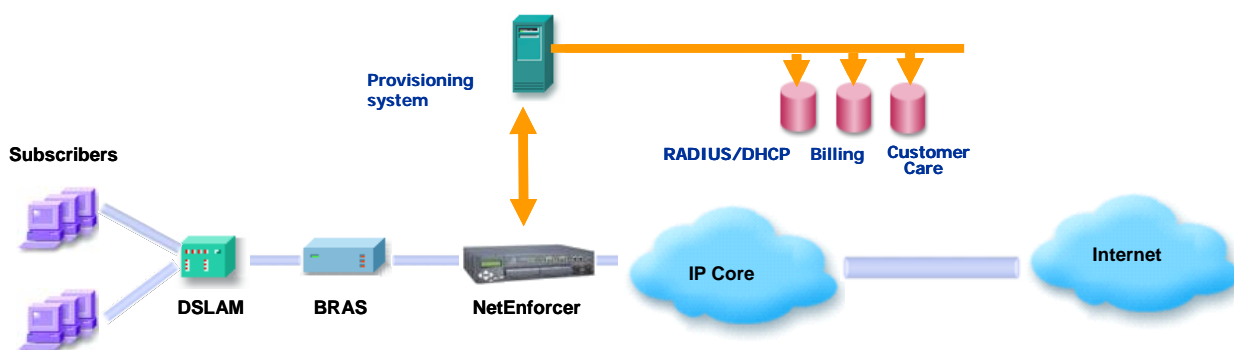
Famille de solutions	Définition	Exemple d'outils
Filtrage de protocole	<p>Solutions permettant d'identifier et le cas échéant de filtrer des flux sur la base d'éléments de niveau protocolaire :</p> <ul style="list-style-type: none"> • Protocoles classiques (smtp, http, etc.) • Protocoles <i>peer-to-peer</i> « traditionnels » (eDonkey, Bittorrent, Fastrack Kazaa, etc.) • Protocoles <i>peer-to-peer</i> cryptés (Freenet, SoftEther, EarthStation5, Filetopia, etc.) 	<p>Allot Cisco P_Cube etc.</p>
Filtrage de contenu	<p>Solutions permettant d'identifier et le cas échéant de filtrer des flux sur la base d'éléments de niveau contenu :</p> <ul style="list-style-type: none"> • Fichiers musicaux « bruts » (WAV, MP3, MPC, etc.) • Fichiers musicaux dans des formats liés aux solutions de DRM (AAC, WMA, Atrac+, etc.) • Archives (ZIP, RAR, ACE, etc.) contenant des images de CD ou des ensemble de fichiers musicaux bruts. 	<p>Audible Magic Advestigo</p>
Filtrage sur le poste client	<p>Solutions permettant d'identifier et le cas échéant d'interdire l'accès à un ensemble de fonctions sur le poste client de l'internaute. Ces fonctions peuvent être au niveau :</p> <ul style="list-style-type: none"> • Réseau – exemple : fermeture de certains ports ou interdiction d'échange avec des listes de nom DNS ou d'adresses IP répertoriés. • Contenu – ex. détection et alerte / interdiction en cas de création de fichier de type .MP3 par un applicatif (ex : client <i>peer-to-peer</i> à l'issue d'un téléchargement). • Applicatif – ex. détection, et alerte ou interdiction du lancement de certaines applications sur le poste client (ex : client eMule) 	<p>Firewall poste de travail Solutions de sécurité, type Cisco CSA ou SkyRecon Solutions contrôle parental, type CyberPatrol</p>

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

3.4. Filtrage de protocole

3.4.1. Schéma de principe

Le diagramme suivant, fourni par Allot¹⁰, illustre le principe de fonctionnement d'une solution de filtrage de protocole :



- Positionnement d'un équipement de filtrage en coupure, sur un point du réseau IP du FAI.
- Intégration avec le SI et l'OSS du FAI via une interface de provisioning qui permet d'alimenter l'équipement avec les informations qui lui sont nécessaires (correspondances adresses IP/internautes fournies par le radius, attribut « internaute ayant fait la demande de filtrage » en provenance du Customer Care dans le cas d'un filtrage à la demande, etc).

¹⁰ Allot-P2P-solutions.ppt, page 11

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

3.4.2. Mode « Filtrage systématique »

3.4.2.1. Scénario de déploiement original (scénario de l'étude du SNEP)

Le scénario de déploiement étudié par le SNEP est le suivant :

- Solution : Filtrage de protocole Allot
- Architecture :
 - ◆ DSL option 1 et 3 : boîtiers de filtrage positionnés entre les BAS et le réseau « IP Core »
 - ◆ DSL option 5 : boîtiers de filtrage positionnés après le LNS qui concentre les abonnés du FAI
 - ◆ Câble : boîtiers de filtrage à placer après le LNS (comme dans le cas DSL option 5).
- Dimensionnement du nombre de boîtiers pour un déploiement généralisé
 - ◆ Trafic moyen : 26 Kb/s par abonné
 - ◆ Un boîtier Gigabit Allot par BAS
 - ◆ Pour France Telecom, et sur la base de l'hypothèse prise dans l'étude du SNEP de 143 BAS, on obtient 143 boîtiers Gigabit Allot.

Le détail du scénario étudié figure dans le rapport d'étude fourni par le SNEP¹¹.

3.4.2.2. Difficultés posées par ce scénario

Le scénario présenté par le SNEP présente un ensemble de difficultés techniques :

- **Asymétrie du trafic**

Les FAI ont indiqué dans leurs commentaires sur l'étude du SNEP¹² que sur beaucoup de réseaux d'opérateurs, les paquets de données ne passent pas nécessairement par les mêmes équipements pour les flux descendants et remontants. Cette ingénierie réseau particulière est mise en place pour répondre à deux besoins :

- ◆ Offrir des latences basses aux abonnés, ce qui implique que le routage du paquet se fasse par le chemin le plus court vers et de l'Internet. Le chemin d'aller vers une destination particulière peut être différent du chemin de retour de par la nature du

¹¹ Rapport_filtrage_capgemini_france.pdf

¹² 041018 note AFA étude Cap Gemini.doc

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

protocole de routage Internet BGP mis en place par le FAI pour sa connectivité interne et/ou externe.

- ◆ Répondre à des nécessités de partage de charge.

La solution Allot dans la version testée dans l'étude SNEP ne permet effectivement pas de filtrer le trafic dans une configuration de réseau asymétrique. Par ailleurs, une modification en profondeur de l'ingénierie réseau des FAI entraînerait de fait des coûts supplémentaires importants dans l'implémentation qui limitent la pertinence d'une telle solution.

Note : Allot a indiqué avoir intégré dans le plan d'évolution de ses solutions la capacité à supporter les flux asymétriques, dont la disponibilité commerciale est prévue en 2005.

- **Dégradation de la qualité de service**

Les FAI ont indiqué dans leurs commentaires sur l'étude du SNEP¹³ que les attentes des consommateurs et des pouvoirs publics en ce qui concerne la qualité de service offerte par les fournisseurs d'accès Internet sont de plus en plus grandes. Le nouveau cadre réglementaire fixe des exigences à l'égard des fournisseurs de services de communications électroniques, dont les FAI. De plus, certains usages ont des exigences de qualité de service supérieures à d'autres, notamment pour la voix sur IP.

Les FAI ont indiqué que « *des expériences précédentes ont démontré que des solutions telles qu'Allot engendrent généralement des latences qui sont néfastes pour la qualité de service et sont incompatibles avec une bonne qualité de service.* ».

Une solution installée en coupure induit de fait un délai de latence – dont la valeur et l'impact peut être discutée mais qui est incontournable compte tenu de l'insertion d'un composant supplémentaire (matériel et logiciel, dans le cas d'Allot) dans la chaîne.

Par ailleurs, le positionnement de boîtiers Allot en coupure derrière les BAS (solution étudiée par le SNEP) pourrait induire de fait une augmentation du risque de panne logicielle ou matérielle donc un impact éventuel sur la disponibilité du service.

- **Evolution des architectures FAI vers équipements 10 Gbps**

Les FAI ont indiqué dans leurs commentaires sur l'étude du SNEP¹⁴ que les boîtiers Allot testés dans l'étude fonctionnent avec des équipements Gigabit Ethernet mais pas des équipements Ethernet 10 Gbps– ce qui induirait des contraintes rendant incompatible la migration par les FAI vers des équipements plus performants.

¹³ 041018 note AFA étude Cap Gemini.doc

¹⁴ 041018 note AFA étude Cap Gemini.doc

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

La solution Allot testée dans l'étude SNEP est effectivement limitée à 1 Gbps. Allot a annoncé pour 2005 un produit supportant 2,5 Gbps full duplex (soit 5 Gbps)¹⁵ et par ailleurs étudier une évolution vers le 10 Gbps. Son concurrent P-Cube supporte par ailleurs des débits supérieurs à 1 Gbps¹⁶.

- **Contournement du filtrage par protocole par cryptage SSL**

Les FAI ont indiqué dans leurs commentaires sur l'étude du SNEP¹⁷ que la tentative de bloquer un protocole conduira les développeurs de logiciels de *peer-to-peer* à faire passer les flux via des sessions d'échanges chiffrées (protocole https sur le port 443). Le protocole employé étant crypté, cela pourrait aboutir à l'impossibilité de détecter les contenus donc de les filtrer.

Le blocage du port 443 est peu envisageable puisque cela reviendrait à interdire l'usage du protocole https donc à entraver les échanges sécurisés (notamment le commerce en ligne).

Une des formes de contournement du filtrage de protocole consisterait donc à généraliser l'emploi du cryptage de type SSL intégré dans les protocoles et les applications clientes *peer-to-peer*.

Si le cryptage par SSL présente certes une difficulté supplémentaire, Allot affirme savoir filtrer plusieurs applications *peer-to-peer* utilisant du filtrage par protocole SSL (FileTopia, Softether, etc.)¹⁸. Ceci est réalisé en détectant une signature comportementale du protocole *peer-to-peer* à l'établissement de la session, avant transmission des flux chiffrés.

- **Positionnement des boîtiers**

Les FAI ont indiqué dans leurs commentaires sur l'étude du SNEP¹⁹ que les options d'architecture et de dimensionnement prises dans l'étude – un boîtier Allot par BAS – n'étaient pas réalistes. Ils ont indiqué, qu'il faudrait prévoir:

- ♦ Pour un FAI ayant une architecture avec BAS, au minimum un boîtier Allot par lien Gigabit BAS – Réseau de collecte (hors redondances nécessaires par ailleurs), avec le pré requis d'avoir une ingénierie réseau n'entraînant pas de trafic asymétrique.
- ♦ Dans le modèle dégroupé natif, ou dans un modèle où les éléments d'extrémité sont tout IP, comme c'est le cas des câblo-opérateurs ou des fournisseurs utilisant des DSLAMs IP, au minimum un boîtier Allot par DSLAM ou par CMTS (hors redondances).

¹⁵ http://www.allot.com/pages/news_content.asp?intGlobalId=476

¹⁶ <http://www.p-cube.com/products/SE2000.shtml>

¹⁷ 041018 note AFA étude Cap Gemini.doc

¹⁸ Allot-P2P-solutions.ppt

¹⁹ 041018 note AFA étude Cap Gemini.doc

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

Les FAI ont indiqué que sur cette base, un chiffre plus proche de la réalité serait de 4000 boîtiers Allot²⁰ – ce qui induirait par ailleurs un modèle de coût de la solution de filtrage très supérieur aux éléments modélisés dans l'étude du SNEP.

3.4.2.3. Conclusion sur le scénario original

Si des arguments et contre arguments existent, les difficultés techniques soulevées par les FAI sur le scénario original, combinées au manque de support des FAI, le rendent difficilement envisageable dans le contexte de la charte pour un déploiement généralisé dans un contexte grand public, en l'état des techniques, et probablement tant que les solutions de filtrage ne seront pas directement intégrées au sein des éléments du réseau tels que les routeurs.²¹

3.4.3. Mode « Filtrage à la demande »

3.4.3.1. Scénario de déploiement envisageable

Dans le cas d'un service de « filtrage *peer-to-peer* à la demande », il est possible d'envisager une architecture proposant l'acheminement par routage des flux à filtrer sur un point de concentration fournissant une architecture dédiée au trafic des internautes du FAI ayant fait la demande de filtrage, et localisée dans un des data centers du FAI.

L'acheminement se ferait par un routage au niveau de l'équipement de rattachement de l'internaute (BAS, DSLAM IP, ou routeur), qui dirigerait le trafic vers un point d'entrée de la plate-forme dédiée, le cas échéant via un tunnel L2TP.

Les hypothèses partagées avec les FAI sur le taux d'abonnement au service de filtrage par les internautes (ex. 10% des abonnés, à la cible et dans un scénario maximaliste) rendent une telle approche techniquement pertinente. Pour chaque FAI, l'architecture dédiée serait construite initialement en un point central, avec un coût raisonnable, et elle monterait progressivement en puissance en fonction du nombre de clients du FAI s'abonnant au service.

La pertinence d'un scénario de ce type a été confirmée avec les fournisseurs de telles solutions (Cisco, Allot).

²⁰ Note AFA, 041018 note AFA étude Cap Gemini.doc

²¹ Note : Un scénario de déploiement sur l'ensemble d'une architecture réseau pourrait en revanche être envisagé dans un contexte de grands utilisateurs, de type entreprises ou universités. La Charte visant principalement le grand public, ces scénarios n'ont pas été analysés en détail.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

3.4.3.2. *Éléments de dimensionnement - Première analyse*

Un calcul rapide montre que dans le scénario maximaliste partagé avec les FAI, le nombre de boîtiers qui serait nécessaire pour équiper l'ensemble des FAI français resterait raisonnable :

Sur la base des hypothèses suivantes :

- 6 millions de foyers abonnés au haut débit en France (prévision à fin 2004 / début 2005)
- 10% des abonnés souscrivent, soit 600 000 foyers
- Débit moyen par foyer abonné : 30 Kb/s

Estimation de la quantité théorique de boîtiers nécessaires :

- Trafic total à filtrer, tous FAI confondus : 30 Kb/s * 600 000 = 17,2 Gb/s de trafic
- Nombre théorique de boîtiers Gigabit nécessaires, hors redondance : 18 (soit un boîtier par Gb/s de trafic).

Le calcul ci-dessus globalise le trafic et ne prend pas en compte les caractéristiques induites par le fait que le trafic est réparti entre les différents FAI.

On pourrait estimer en première approche que le nombre de boîtiers réellement nécessaires serait un multiple par quelques unités du nombre de boîtiers théoriques, soit environ une centaine de boîtiers pour équiper l'ensemble des FAI français.

3.4.3.3. *Éléments de dimensionnement - approche pour préciser le décompte*

Si l'on souhaitait préciser le décompte, il serait nécessaire d'effectuer une analyse détaillée FAI par FAI, en prenant en compte les caractéristiques de chacun.

Le décompte détaillé du nombre de boîtiers nécessaires ne peut se faire sans entrer dans le détail de l'architecture de chacun des FAI concernés. Sont notamment à prendre en compte les spécificités de chaque FAI selon les dimensions suivantes :

- Option souscrite auprès de France Telecom (accès fourni en gros par France Telecom, dégroupage)
- Nature (Fast ethernet, Gb ethernet, etc.) et nombre de BAS
- Nature (DSLAM IP ou non) et nombre de DSLAM
- Politique de gestion des adresses IP (pool unique, pools multiples et règles d'affectation des pools, etc.)

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- Architecture du réseau (régionalisée ou non, etc.).

Des discussions détaillées ont été menées avec des FAI dans le cadre de l'étude afin d'effectuer un décompte plus détaillé dans le cadre d'une « étude de cas ». Les engagements de confidentialité demandés par les FAI dans le cadre de ces discussions ne permettent pas de faire apparaître ici les hypothèses prises, les scénarios envisagés et le résultat du décompte.

3.4.3.4. *Contraintes de mise en œuvre*

Le déploiement d'une solution de filtrage à la demande doit prendre en compte les contraintes suivantes.

En matière d'architecture et de réseau :

- Le déploiement d'équipements de filtrage dans l'architecture du FAI.
- La mise en place d'une solution de routage au niveau du BAS de rattachement et / ou à l'intérieur du réseau, avec le cas échéant le déploiement de nouveaux équipements ou la spécialisation d'équipements existants pour supporter ce routage.
- La mise en place des solutions d'administration, d'exploitation et de supervision des éléments ci-dessus – incluant des aspects techniques (ex : solution de supervision) et humains (ex : équipes d'exploitation).

En matière de SI, les contraintes identifiées sont les suivantes :

- Intégration de la prise d'abonnement à la solution de filtrage avec le Système d'Information (OSS – Operations Support Systems - et BSS – Business Support Systems).

En matière de coûts, les postes à prévoir seraient les suivants :

- Coûts d'investissement fixes :
 - ◆ Ingénierie générale
 - ◆ Intégration avec les systèmes BSS
 - ◆ Intégration avec les systèmes OSS
 - ◆ Gestion des impacts sur le réseau et configuration
 - ◆ Vente, Marketing et communication
 - ◆ Gestion générale du projet de nouveau service de filtrage
- Coûts d'investissement variables, fonction du nombre d'abonnés au filtrage :
 - ◆ Equipements réseau (le cas échéant) – type BAS, routeurs ou « load balancers »
 - ◆ Equipements de filtrage – exemple type Allot ou Cisco P_Cube
 - ◆ Installation

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- Coûts récurrents
 - ◆ Coûts récurrents sur la partie réseau (maintenance des matériels et logiciels, prestations d'administration, exploitation et supervision)
 - ◆ Coûts récurrents sur la partie SI (maintenance des matériels et logiciels, maintenance corrective et évolutive).

3.4.3.5. Conclusion

Le scénario de déploiement ci-dessus apparaît en première analyse techniquement pertinent, pour la solution technique, comme pour le nombre de boîtiers résultants. Les principes d'architecture ci-dessus resteraient à affiner et décliner FAI par FAI.

Néanmoins, sa mise en œuvre nécessiterait de mener un ensemble de projets (réseau, système d'information, vente et marketing et communication, etc.) et nécessiterait un investissement et engendrerait des coûts de fonctionnement significatifs (matériels et logiciels, projets, opérations).

Il est à noter qu'une étude détaillée du bilan économique supposerait de disposer de données détaillées issues des FAI (détail de l'architecture réseau, détail du SI, détail des coûts sur chacune des catégories, etc.) - ce qui ne pourrait s'envisager que FAI par FAI et avec une volonté du FAI de fournir une visibilité sur ces éléments dans le cadre d'une étude de type « business case ».

Au final, la pertinence économique (capacité à rentabiliser les coûts par un revenu de quelques euros par internaute ayant souscrit le service) de ce scénario apparaît néanmoins et en première analyse pour le moins hasardeuse.

De plus, les architectures réseau requises pour utiliser ces solutions, et notamment obtenir un routage des flux à traiter en un point central du réseau, apparaissent particulièrement problématiques avec le développement de nouveaux services haut débit basés sur des nouveaux types de flux, tels que la téléphonie sur ADSL, et la télévision ou vidéo sur ADSL. A titre d'exemple, la télévision sur ADSL utilise une diffusion de type multicast, nécessitant un routage particulier entre les flux des chaînes communs aux différents clients, et les flux parallèles personnels tels que l'accès au web.

Il est très probable que des problèmes de non compatibilité apparaissent entre une architecture réseau donnant satisfaction aux solutions de filtrage, et les besoins des nouveaux services haut débit.

Nous proposons donc de ne pas retenir le scénario « Filtrage de protocole – filtrage à la demande ».

En revanche, les solutions de fournissant des fonctions de filtrage de protocole peuvent être également utilisées en mode observation et analyse de trafic – ce qui lève un ensemble de contraintes techniques (positionnement en coupure, etc.) et peut s'envisager dans des scénarios de déploiements limités (quelques boîtiers en mode observation, pas d'intégration avec le SI, etc.).

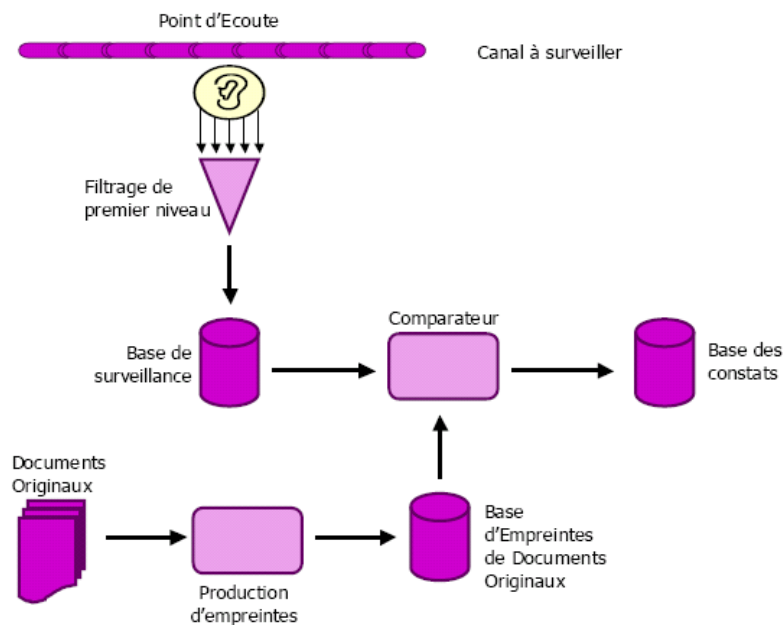
VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

Nous proposons donc de retenir l'utilisation d'une solution orientée protocole (type Allot ou Cisco P_Cube) en mode observation et analyse de trafic et pour une expérimentation « Observatoire du Peer to peer ».

3.5. Filtrage de contenu

3.5.1. Schéma de principe

Le diagramme suivant, fourni par la société Advestigo²², illustre le principe de fonctionnement d'une solution de filtrage de contenu :



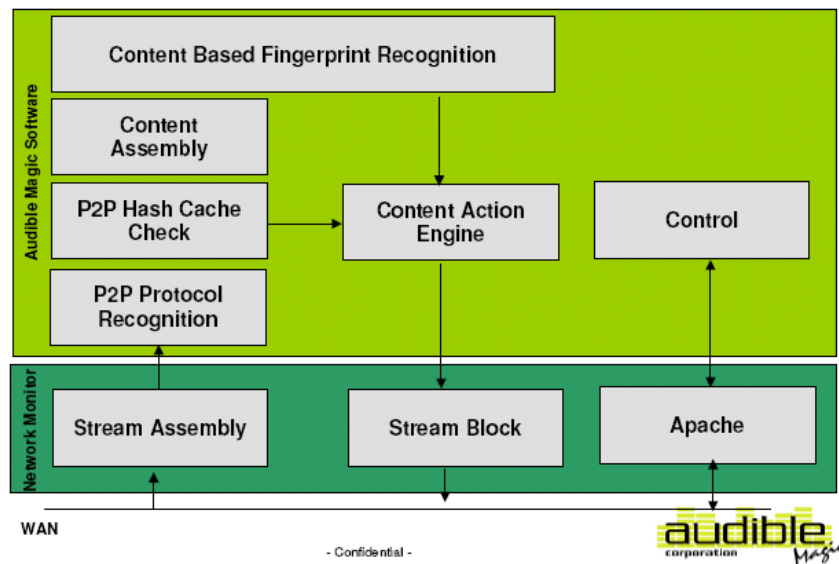
- Mise en place sur le réseau de points d'écoute non intrusifs (en dérivation et non en coupure).
- Mise en place et maintien à jour d'une base d'empreintes de fichiers originaux, contenant les signatures des fichiers protégés (en l'occurrence, des morceaux musicaux).

²² Radars sur le P2P (AdVestigo - 092004).pdf

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

- Comparateur permettant d'identifier les contenus *peer-to-peer* illégaux en comparant les flux écoutés avec les signatures figurant dans la base d'empreintes. Ce comparateur peut être à deux niveaux (contrôle par clé de hachage, afin d'effectuer un premier niveau d'analyse et éviter d'engorger le comparateur de second niveau qui effectue la comparaison complète).
- Historisation des évènements dans une base de données (« base des constats » sur le schéma ci-dessus).

Le diagramme suivant, fourni par la société Audible Magic²³, illustre le principe de fonctionnement des points d'écoute :



La solution d'Audible Magic comprend :

- Une composante réseau (Network Monitor) qui capture et assemble des paquets IP et les fournit à la composante de reconnaissance de contenu. Cette partie fournit également des fonctions annexes de déconnexion TCP en cas d'utilisation en mode « filtrage », et les services d'administration de la solution.
- Une composante logicielle d'analyse de contenu (Audible Magic Software) qui effectue la reconnaissance des protocoles *peer-to-peer*, la comparaison de premier et de second niveau, et la détermination des règles à appliquer (Content Action Engine).
 - ♦ Le premier niveau (P2P Hash Cache check sur le schéma) permet, par une vérification rapide de type hash code, non exhaustive mais nécessitant une puissance de calcul

²³ General ISP.pdf

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

limitée, de séparer les trames nécessitant pas d'analyse de niveau 2 des autres trames – et éviter ainsi de générer une charge CPU trop importante au niveau du boîtier

- ♦ Le second niveau (Content based fingerprint recognition sur le schéma) permet de comparer le contenu des trames aux signatures (fingerprint) de contenus et identifier de manière précise s'il s'agit d'un échange portant sur un contenu connu du boîtier.

3.5.2. Mode « Radar »

3.5.2.1. Scénario de déploiement

Le mode « radar » correspond à une pratique statistique qui peut être mise en place à différents niveaux :

- Sur les points d'échanges entre les principaux backbones ;
- Au niveau des BAS si le FAI en possède ;
- Au niveau DSLAM IP ou CMTS.

Audible commercialise des équipements de filtrage capables de traiter des débits de 2, 50 et 200 Mbits par seconde et par équipement, ainsi qu'une offre CSA-1000 capable de traiter jusqu'à un Gigabit par seconde (constituée de plusieurs boîtiers CSA-200 à compléter par un équipement d'équilibrage de charge) – ce qui rend pertinent d'envisager un déploiement au niveau BAS ou routeur.

Un scénario de déploiement pourrait être de :

- Déployer de manière fixe (« Radars fixes ») des équipements de filtrage au niveau de certains BAS (solution de type Gigabit) ou au niveau de DSLAMs IP / CMTS ou encore de routeurs ;
- Déployer ponctuellement, dans le cadre d'opérations de mesure de trafic et/ou afin d'alimenter des actions de prévention ou juridiques, des équipements de filtrage mis en place de manière temporaire (« Radars mobiles ») sur d'autres BAS, DSLAM IP, CMTS ou routeurs.

3.5.2.2. Eléments de dimensionnement

Le nombre d'équipements nécessaire dépend de différents facteurs :

- L'ambition donnée au déploiement (expérimentation, ou support d'actions de communication ponctuelles, ou mise en place pérenne et à plus grande échelle).
- Le nombre de « radars » fixes ou mobiles à mettre en place – de un (pour une expérimentation ponctuelle) à plusieurs milliers (un par DSLAM).

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- Le débit à observer par « radar » (d'une dizaine de Mb/s à un Gb/s sur les architectures actuelles, avec une extension prévue jusqu'à la dizaine de Gb/s).
- La nature du trafic observé (part du *peer-to-peer* dans le trafic observé).
- La nature des contenus échangés en *peer-to-peer* (proportion de contenus identifiés / figurant dans la base de signatures de la solution).
- La capacité de traitement des équipements (efficacité des algorithmes, etc.).

Compte tenu de ces éléments, il est difficile d'effectuer un dimensionnement a priori. Audible a recommandé d'effectuer une expérimentation en contexte réel afin de disposer d'éléments de retour d'expérience pour étayer un dimensionnement.

Advestigo a pour sa part fourni les éléments de dimensionnement ci-dessous²⁴ :

- Positionnement au niveau BAS, flux capté de l'ordre de 1 Gbps, dont 600 Mbps de *peer-to-peer* ;
- Examen statistique de 10 % du trafic soit 60 Mbps ;
- Le logiciel Advestigo permettrait de comparer entre 100 000 et 500 000 extraits par jour et par processeur (Intel à 3 GHz) pour un catalogue d'environ 100 000 titres musicaux et 1 000 films.

3.5.2.3. Conclusion

Les deux solutions de filtrage de contenus présentées lors des auditions (Advestigo et Audible Magic) pourraient être pertinentes pour un fonctionnement en mode « Radar », Audible présentant l'avantage de disposer d'une offre déjà commercialisée et de niveau industriel.

Les principes présentés ci-dessus restent à affiner, afin de :

- Valider la faisabilité technique dans une architecture FAI représentative ;
- Confirmer le nombre de boîtiers, et ainsi, estimer le coût d'investissement ;
- Apprécier les contraintes opérationnelles liées à l'exploitation de ces solutions.
- Valider la faisabilité juridique de cette approche

²⁴ Lutte antipiratage P2P_contribution adVestigo.pdf

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- Réaliser une analyse comparative avec le scénario de positionnement « en bout de réseau »

Préalablement, nous proposons d'analyser les technologies de filtrage de contenu (type Audible ou Advestigo) dans le cadre de l'expérimentation « Observatoire du peer to peer ».

3.6. Filtrage sur le poste client

3.6.1. Introduction

Il existe deux familles de solutions de filtrage sur le poste client :

- Les solutions avec serveur central - par exemple Cisco Security Agent (CSA) ;
- Les solutions orientées poste client - par exemple CyberPatrol (ces solutions ont des architectures comparables à celles des solutions de contrôle parental ou d'antivirus).

Pour le *peer-to-peer*, le filtrage sur le poste client peut s'envisager à différents niveaux :

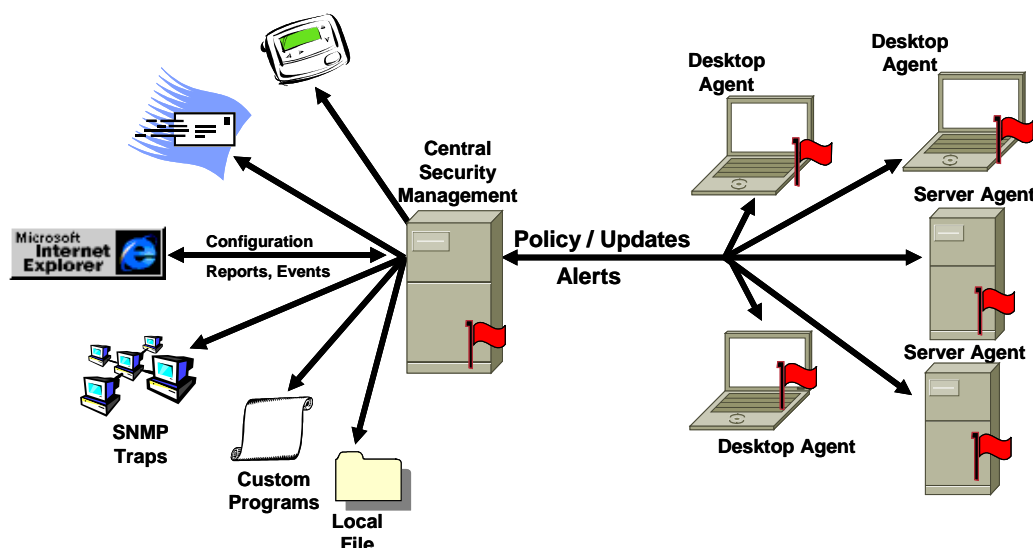
- Au niveau port – blocage des ports standard utilisés par les clients *peer-to-peer* (ex : 4661, 4662 pour eDonkey)²⁵ ;
- Au niveau applicatif – blocage du lancement des applications clientes *peer-to-peer* sur le poste de travail ou filtrage des communications d'une application qui n'y est pas autorisée ;
- Au niveau fichier, le cas échéant – blocage du stockage de fichiers mp3 sur le poste client par exemple.

²⁵ L'effet de cette mesure est faible, les clients *peer to peer* permettant de reconfigurer les ports utilisés.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

3.6.2. Schéma de principe des solutions à serveur central

Le diagramme suivant, fourni par Cisco²⁶, illustre le principe de fonctionnement d'une solution de filtrage sur le poste de travail avec serveur central :



- Un module client (Desktop Agent sur le schéma) qui contrôle les événements sur le poste client (lancement d'application, contrôle des accès au système de fichiers, à la base de registres, aux objets COM, aux services http, etc.). Il peut agir selon un modèle permissif (refuse toute action documentée comme néfaste ou interdite, et autorise toutes les autres) ou un modèle restrictif (autorise toute action documentée comme valide et refuse toutes les autres).
- Un module serveur (Central security management sur le schéma) qui permet d'une part s'assurer que le module client n'a pas été inhibé sur un PC qui se connecte, d'enregistrer les alertes remontées par les clients, et d'administrer les règles de fonctionnement (signatures d'applications, etc.).

3.6.3. Mode « Filtrage à la demande »

Dans le mode de « filtrage à la demande », une solution de filtrage sur le poste client est déployée sur les terminaux des internautes qui en font la demande. Ce mode est pertinent pour les solutions orientées poste client – type CyberPatrol, et ne nécessite pas l'installation d'infrastructures particulières chez le FAI.

²⁶ Secu_Miniculture-181004.ppt

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

La base de signatures (ex : signatures des exécutables clients des applications de *peer-to-peer*) est maintenue par l'éditeur de la solution - selon une approche équivalente à celle employée pour les solutions de contrôle parental et les solutions anti-virus.

3.6.4. Conclusion

Les solutions orientées poste client, type CyberPatrol, apparaissent pertinentes pour le mode « Filtrage à la demande » - et ne nécessitent pas d'expérimentation particulière.

La solution de filtrage avec serveur central présentée lors des auditions (Cisco CSA) apparaît pertinente pour un fonctionnement en mode « à la demande ». Les principes présentés ci-dessus restent à affiner, afin de :

- Prouver la faisabilité technique de cette solution en la mettant en œuvre en vraie grandeur ;
- Mesurer les impacts techniques du filtrage ;
- Fournir les éléments techniques permettant d'estimer le coût d'investissement ;
- Apprécier les contraintes opérationnelles liées à l'exploitation de ces solutions ;
- Définir un ou plusieurs scénarios de généralisation.

Nous proposons de retenir le scénario « Solution filtrage poste client, mode à la demande » pour une expérimentation.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

3.7. Synthèse

Le tableau suivant présente le résultat de l'analyse technique effectuée pour chacune des familles de solutions :

Mode de déploiement / Famille de solution	Observation et analyse de trafic	Filtrage systématique	Filtrage à la demande	Radar
Filtrage de protocole	Pertinent Expérimentation recommandée	Difficile en l'état des techniques	Peu pertinent Techniquement faisable, coût élevé, problème de compatibilité avec les évolutions du haut débit, peu réaliste	Non retenu (l'utilisation de protocoles peer-to-peer ne constitue pas en soi un acte frauduleux)
Filtrage de contenu	Pertinent Expérimentation recommandée	Non retenu Trop grande complexité de filtrage	Peu pertinent (suppose la détection de l'exhaustivité des contenus), et problèmes de mise en œuvre similaires au filtrage de protocole	A étudier
Filtrage sur le poste client	N/A	N/A	Pertinent Expérimentation recommandée	N/A

N/A : non applicable.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

4. Expérimentations recommandées

4.1.1. (E1) Solution filtrage poste client, mode à la demande

Nous proposons d'organiser l'expérimentation d'une solution de filtrage sur le poste client, en mode à la demande.

L'expérimentation consistera à :

- Mettre en œuvre, chez un ou plusieurs FAI, une solution de filtrage sur le poste client – de type CyberPatrol ou Cisco CSA ;
- Déployer cette solution (partie cliente et configuration au niveau du serveur central) pour un ensemble d'internautes volontaires;
- Expérimenter le fonctionnement du service pendant une durée suffisante (ex : deux à trois mois) pour obtenir un retour d'expérience technique et opérationnel.

L'objectif technique de l'expérimentation sera :

- De prouver la faisabilité technique de cette solution en la mettant en œuvre à l'échelle expérimentale ;
- De mesurer les impacts techniques du filtrage ;
- De fournir les éléments techniques permettant d'estimer le coût complet d'investissement ;
- D'apprécier les contraintes opérationnelles liées à l'exploitation de ces solutions ;
- De définir un ou plusieurs scénarios de généralisation.

4.1.2. (E2) Solutions orientées protocole et contenu, « observatoire de trafic P2P »

Nous proposons d'organiser l'expérimentation de solutions orientées protocole et contenu dans un objectif d'observation et d'analyse de trafic, établissant un « observatoire de trafic P2P ».

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

L'expérimentation consistera à :

- Mettre en œuvre, chez un ou plusieurs FAI, une ou plusieurs solutions orientées protocole et/ou contenu dans un mode observation et analyse de trafic (et non filtrage), localisée dans les data centers du / des FAI ;
- Analyser les données d'observation du trafic de manière statistique ;
- Obtenir un retour d'expérience technique et opérationnel sur la solution.

L'objectif technique de l'expérimentation sera :

- De confirmer la faisabilité technique de l'observation et l'analyse du trafic peer to peer en la mettant en œuvre à l'échelle expérimentale ;
- De confirmer le nombre de boîtiers, et, ainsi, d'estimer le coût d'investissement en cas de pérennisation ;
- D'apprécier les contraintes opérationnelles liées à l'exploitation de ces solutions ;
- De définir un ou plusieurs scénarios de pérennisation de l'observatoire.

L'expérimentation permettra, sur la dimension des internautes :

- De fournir des éléments d'information sur le trafic *peer-to-peer* (part de ce trafic, etc.) ;
- De mesurer les changements de comportement éventuels des internautes.

Lors des auditions réalisées par les experts, la société Audible Magic a proposé de contribuer à une telle expérimentation, en proposant²⁷ :

- De déployer cinq équipements Audible Magic (CopySense) pendant une durée de trois mois, en mode observation (et non blocage) ;
- D'analyser les meta-données des contenus identifiés afin de déterminer les signatures manquantes dans la base de données Audible Magic (contenant à date les signatures de 3,8 millions de titres) et d'acquérir des signatures additionnelles, le cas échéant ;
- De définir, à la fin de la période d'expérimentation, un scénario de déploiement généralisé :
 - ◆ Nombre d'équipements de filtrage de contenu ;
 - ◆ Nombre d'équipement d'équilibrage de charge (load balancing) ;

²⁷ General ISP.pdf

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
----------------------	------------------------	----------------------------------------------------------------------------

- De fournir les équipements et les services nécessaires pour réaliser les travaux précédents à des tarifs et honoraires significativement réduits.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

5. Annexe 1 – Auditions organisées

Le tableau ci-dessous liste les auditions organisées dans le cadre de la mission des experts.

Audition	Date	Participants
Audition individuelle 1	23 septembre 2004	SNEP, UPFI, Cap Gemini, YaCast
Audition individuelle 2	27 septembre 2004	SNEP, UPFI, Warner Music, Universal Music, EMI, Sony Music, BMG France
Audition individuelle 3	22 septembre 2004	Session 1 - Microsoft
Audition individuelle 4	18 octobre 2004	Session 1 – Cisco
	23 septembre 2004	Session 2 – Allot
	5 octobre 2004	Session 3 - Audible Magic
	5 octobre 2004	Session 4 – Advestigo
	7 octobre 2004	Session 5 – CEIS
	28 septembre 2004	Session 6 - CoPeerRight Agency
Audition collective 5	7 octobre 2004	AFA, Représentants des FAI
Audition individuelle 6	20 octobre 2004	Consommateurs
Session plénière	21 octobre 2004	AFA, représentants techniques des FAI
Réunion de travail	26 novembre 2004	FAI 1, Cisco, Représentants des experts, Cap Gemini
Réunion de travail	6 décembre 2004	FAI 2, Audible Magic, Représentants des experts, Cap Gemini
Réunion de travail	7 décembre 2004	FAI 3, Allot, Représentants des experts, Cap Gemini

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

6. Annexe 4 – Etudes de cas

6.1. Introduction

Des études de cas ont été menées dans le contexte de différents FAI et différents types solutions de filtrage. Ces études ont abordé les aspects suivants :

- L'architecture du FAI
- Pour une utilisation en mode Filtrage et/ou en mode Monitoring et analyse de trafic :
 - ♦ Scénario de positionnement des solutions
 - ♦ Principe de fonctionnement pour l'activation du service (« à la demande de l'internaute »)
 - ♦ Impacts techniques sur l'architecture FAI
 - ♦ Nombre de boîtiers nécessaires
 - ♦ Contraintes induites chez le FAI (impact administration, exploitation, ..)

Les études menées sont :

- Solution de filtrage de protocole P_Cube dans le contexte d'un FAI 1
- Solution de filtrage de contenus Audible Magic dans le contexte d'un FAI 2.
- Solution de filtrage de protocole Allot dans le contexte d'un FAI 3
- Compléments sur la solution de filtrage poste de travail Cisco CSA

Hypothèses techniques :

- 10% des abonnés font la demande filtrage (hyp. AFA)
- 26 à 30 kb/s trafic moyen par abonné (hypothèses de travail pour exemple)

6.2. Filtrage de protocole P_Cube dans le contexte d'un FAI 1

6.2.1. Architecture du FAI 1

L'architecture du FAI 1 est découpée de la manière suivante :

- RTC / DSLAM

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- NAS (bas débit) / BAS (broadband)
- Switch ethernet
- NC (Nœuds de collecte)
- NR (Nœud Régional)
- NT (Nœud de Transit)

Entre un niveau et le niveau suivant, des liens multiples sont établis afin d'optimiser le trafic et fournir une redondance en cas de panne.

Les switches fonctionnant au niveau 2, ils ne prennent pas de décisions de routage.

Les NC fonctionnent au niveau 3 et appliquent des règles de routage IP BGP.

Le trafic montant et descendant peut prendre des routes différentes, la majeure partie du trafic est effectivement asymétrique.

L'architecture est régionalisée, notamment pour l'affectation des pools d'adresses IP.

6.2.2. Solution P_Cube

La gamme P_Cube est composée de trois matériels :

- SE100 (10 000 users, 2 x Fast Ethernet)
- SE 1000 (40 000 users, 2 x Gigabit Ethernet)
- SE 2000 (100 000 users, 4 x Gigabit Ethernet)

Les matériels P_Cube effectuent de l'analyse protocolaire et fonctionnent en mode sonde, en mode anonyme ou en mode « subscriber aware ».

Ils doivent être positionnés en coupure sur le réseau du FAI et nécessitent une symétrie des flux aller et retour au niveau du même boîtier.

Les deux scénarios qui suivent n'ont pas été pré-établis par Cisco, mais élaborés au cours de la réunion par les experts tiers présents.

6.2.3. Positionnement des boîtiers – Scénario 1

Le premier scénario de positionnement consiste à positionner les boîtiers entre les BAS et le premier nœud d'agrégation, pour l'ensemble des BAS du FAI.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

Ceci suppose que le FAI mette en place une politique de routage spécifique à appliquer au niveau BAS (source routing), avec modification des priorités de routage afin d'assurer le flux retour par un lien connecté au même boîtier que le lien utilisé pour le flux aller.

Dans ce scénario de positionnement, un premier décompte du nombre de boîtiers nécessaires hors redondance et maintenance serait le suivant :

- Pour les BAS Gigabit reliés en moyenne par 4 liens, 2 boîtiers SE2000 par BAS soit plusieurs centaines de boîtiers
- Pour les BAS Ethernet reliés en moyenne par 2 liens, 2 boîtiers SE100 par BAS soit également plusieurs centaines de boîtiers.
- Soit un total d'environ un millier boîtiers hors redondance et spare (pour maintenance).

6.2.4. Positionnement des boîtiers – Scénario 2

Le second scénario de positionnement consiste à mettre en place une architecture dédiée afin de router le trafic des internautes ayant fait la demande de filtrage vers des équipements dédiés aux internautes ayant souscrit ce service.

Ceci suppose que le FAI mette en place des BAS dédiés (variante 1) ou une solution de routage (variante 2) afin d'acheminer le trafic depuis le BAS de rattachement de l'internaute vers l'équipement LNS.

Dans ce scénario de positionnement, un premier décompte du nombre de boîtiers nécessaires hors redondance et maintenance serait le suivant :

- Dans le cas de la variante n°1 : En raison de la régionalisation de l'architecture (POP IP) :
 - ♦ Le nombre de boîtiers minimum à déployer pour couvrir l'ensemble de l'architecture du FAI serait de un boîtier par région soit une cinquantaine de régions en plus du nombre de BAS dédié
 - ♦ En cas de répartition géographique non homogène des internautes faisant la demande de filtrage (ex : région parisienne), un nombre supplémentaires de boîtiers serait à prévoir.
- Dans le cas de la variante n° 2 : Dans l'hypothèse où 10% des abonnés font une demande de filtrage à la cible et que le trafic est équi-répartie, 10% du trafic serait concerné. Sur cette hypothèse, le nombre nominal de boîtiers nécessaire à la cible serait d'environ une centaine (soit 10% d'un millier), hors impact lié à la régionalisation.

6.2.5. Contraintes induites chez le FAI

En matière de réseau, les contraintes identifiées en réunion sont les suivantes :

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- Déploiement important de matériels P_Cube dans l'architecture du FAI
- Pour le scénario 1 :
 - ◆ Confection et mise en place de politiques nouvelles de routages spécialisées pour la totalité du réseau afin d'éliminer le trafic asymétrique
- Pour le scénario 2 : en fonction de la variante retenue (voir section 3.3) :
 - ◆ Soit le déploiement de BAS dédiés (ou spécialisation de BAS existants)
 - ◆ Soit le déploiement de solution de routage avec tunnelling vers les LNS
- Analyse et mise en place des solutions d'administration, d'exploitation et de supervision des éléments ci-dessus – incluant des aspects techniques (ex : solution de supervision) et humains (ex : équipes d'exploitation)

En matière de SI, les contraintes identifiées en réunion sont les suivantes :

- Intégration la prise de la solution de filtrage (à travers la solution P_Cube) avec le Système d'Information (OSS et BSS) (avec impacts techniques et financiers)

En matière de coût, les postes de coûts à prévoir seraient :

- Coûts d'investissement fixes :
 - ◆ Ingénierie générale
 - ◆ Intégration avec les systèmes BSS
 - ◆ Intégration avec les systèmes OSS
 - ◆ Marketing et communication
- Coûts d'investissement variables, fonction du nombre d'abonnés au filtrage :
 - ◆ BAS dédié (à dimensionner en détail)
 - ◆ Boîtier P_Cube (idem)
 - ◆ Installation
- Coûts récurrents
 - ◆ Coûts récurrents partie réseau (maintenance des matériels et logiciels, prestations d'administration, exploitation et supervision)
 - ◆ Coûts récurrents partie SI (maintenance des matériels et logiciels, maintenance corrective et évolutive)

En matière de pérennité / efficacité :

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- Il est nécessaire d'accepter le risque d'une interruption du filtrage notamment entre l'apparition de nouveaux protocoles, principalement les protocoles encryptés, et la disponibilité (à confirmer) de mises à jour des logiciels des boîtiers permettant de les filtrer.
- Par ailleurs, la capacité à filtrer des protocoles encryptés par les solutions de filtrage de protocole est liée soit à la reconnaissance des négociations préalable au passage au mode crypté, soit à l'exploitation de failles (via une analyse comportementale) dans les échanges cryptés.

6.3. Filtrage de poste client dans le contexte d'un FAI 1

6.3.1. Introduction

Les solution de filtrage sur le poste client a été jugée la plus réaliste par le FAI 1, aussi bien du point de vue client que de celui des FAI au regard du but recherché. L'orientation proposée par le FAI 1 est celle d'un filtrage décentralisé directement sur le poste client.

Le FAI 1 a indiqué que cette décentralisation présentait plusieurs avantages importants :

- elle évite des modifications profondes et impactantes de l'infrastructure technique du FAI.
- elle évite les risques de dysfonctionnement et de contention des réseaux très haut débits des FAI et ce même dans l'avenir.
- elle donne le choix au client d'activer ou non ce filtrage.
- elle permet de mutualiser cette fonctionnalité filtrage antiP2P avec d'autres logiciels déjà présents sur le poste client (FireWall, Contrôle parental ...).

Tout en permettant une efficacité comparable à celle d'une solution réseau, le FAI 1 a indiqué que ce principe permettait en plus un fonctionnement en mode autonome et réduit le risque de dysfonctionnement du réseau.

Les solutions de filtrage sur le poste client peuvent génériquement intervenir à trois niveaux :

- Au niveau port – blocage des ports standard utilisés par les clients *peer-to-peer* (ex : 4661, 4662 pour eDonkey) ;
- Au niveau applicatif – blocage du lancement des applications clientes *peer-to-peer* sur le poste de travail ou filtrage des communications d'une application qui n'y est pas autorisée ;
- Au niveau fichier, le cas échéant – blocage du stockage de fichiers mp3 sur le poste client par exemple.

Le FAI 1 s'est intéressé à la mise en œuvre de ces solutions au niveau applicatif.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

6.3.2. Principe de mise en œuvre

Le principe de mise en œuvre d'une solution de filtrage sur le poste client au niveau applicatif est le suivant :

- Un agent présent sur le poste client est responsable de ce filtrage.
- Cet agent possède une liste d'applicatif autorisés ou non à s'exécuter ou à communiquer.
- Lors du lancement ou de la tentative de communication d'un applicatif, plusieurs possibilités se présentent :
 - ♦ l'applicatif est présent dans la liste des applicatifs interdits : l'applicatif ne fonctionnera pas, l'utilisateur ne pourra donc pas l'utiliser.
 - ♦ l'applicatif est présent dans la liste des applicatifs autorisés : tout se passe normalement pour cet applicatif, rien n'est demandé à l'utilisateur.
 - ♦ l'applicatif n'est présent dans aucune liste : en fonction du paramétrage de l'agent plusieurs cas possibles :
 - 1 - L'agent pose immédiatement la question à l'utilisateur pour savoir si il faut autoriser l'applicatif à s'exécuter ou à communiquer. L'agent peut mémoriser la réponse pour ne plus poser cette question par la suite.
 - 2 - L'agent peut considérer que tout ce qui est inconnu est interdit et dans ce cas ne pose aucune question et bloque le fonctionnement de l'applicatif.
 - 3 - L'agent demande une identification de l'utilisateur, pour s'assurer que c'est bien l'administrateur de la machine qui est aux commandes, et après identification repasse au cas n°1.

Ce type de filtrage s'applique à tous les types de logiciels et peut donc s'appliquer pour les logiciels Peer To Peer. De plus, il est capable de fonctionner même pour les logiciels encore inconnus à ce jour.

Ce type de logiciel existe déjà aujourd'hui et se présente souvent sous la forme d'un FireWall personnel ou d'un contrôle parental.

Ce logiciel est activable et paramétrable par le client. Il permet à des parents d'interdire à leurs enfants d'utiliser des applicatifs permettant de pratiquer des activités illégales comme les logiciels Peer To Peer. Cela va même plus loin car il peut aller jusqu'à interdire l'accès au FTP ou au newsgroup qui sont d'autres moyens de récupérer des fichiers illégaux.

6.3.3. Critères identifiés par le FAI 1 pour répondre aux besoins de filtrage de la charte

Les critères identifiés par le FAI 1 pour répondre aux besoins de filtrage de la charte :

- L'agent de filtrage doit s'exécuter à chaque lancement de l'ordinateur.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
----------------------	------------------------	----------------------------------------------------------------------------

- Il ne doit être paramétrable par l'utilisateur qu'après identification de celui-ci.
- Il doit être capable de bloquer tous logiciels PeerToPeer existant (et à venir pour ce qui est prévisible)
- Il doit être transparent à l'utilisation « classique » d'Internet (Web, Messagerie, ..).
- Il doit être simple d'utilisation.

Le FAI1 a indiqué qu'une phase de sélection de produit (solution logicielle de filtrage sur le poste de travail) devrait notamment prévoir l'obtention d'informations sur :

- les applications bloquées par le produit
- les méthodes de blocage
 - ◆ Blocage de l'exécution
 - ◆ Blocage de la communication
 - blocage de port
 - blocage dns
 - blocage par signature
 - ...
- les OS compatibles
- Les autres applicatifs incompatibles
- Les langages supportés par leur produit et leur documentation s'y rapportant
- Les possibilités de customisation visuelle et fonctionnelle du produit
- Les possibilités d'activation/désactivation du produit
- Les possibilités d'identification de l'utilisateur
- Les modalités de mise à jour du produit

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

6.4. Filtrage de contenus Audible Magic dans le contexte d'un FAI 2

6.4.1. Solution Audible Magic

La solution de filtrage de contenus Audible Magic consiste à placer des « network appliances » *CopySense* en dérivation sur le réseau, à partir de ports de routeurs, configurés en miroir des ports de communication.

Etant placé en dérivation, la panne éventuelle d'un tel boîtier ne pose pas de problème pour la qualité de service. Ce boîtier est passif, sauf en cas de renvoi de paquets IP de fin de communication (« reset »), dans le contexte d'une détection de contenu à filtrer. Il est cependant à noter que le trafic étant redirigé vers le boîtier *CopySense* par les équipements de commutation du FAI, il existe néanmoins des risques. Par ailleurs, les ressources consommées sur les équipements du FAI seront plus importantes.

La solution *CopySense* détecte les contenus à partir d'une base centralisée de signatures de contenus et d'un cache local dans les boîtiers. La détection de morceaux de musique se base sur une séquence de 20 secondes de musique, indépendante du codec utilisé.

Dans le cas de protocoles peer-to-peer chiffrés, la solution détecte potentiellement les protocoles mais pas les contenus. La politique de filtrage, paramétrée selon les choix de mise en œuvre, pourrait alors couper les sessions peer-to-peer chiffrées.

La solution s'accompagne d'un contrat de maintenance des éléments de configuration, afin de suivre l'évolution des protocoles et des applications clientes de peer-to-peer, et afin de maintenir la base de données des signatures de contenus.

Un boîtier *CopySense* peut supporter environ 300 Mbps de trafic IP.

6.4.2. Architecture du FAI 2

Le FAI 2 utilise trois types d'architectures réseau, selon les cas, pour ses clients ADSL :

1. Réseau d'accès de l'opérateur historique (DSLAM / ATM / BAS), et backbone IP Gigabit Ethernet propre ;
2. Réseau d'accès d'un opérateur dégroupé avec DSLAM IP, et backbone IP Gigabit Ethernet propre ;
3. Réseau d'accès propre avec DSLAM IP, et backbone IP Gigabit Ethernet propre.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

6.4.3. Scénarios de positionnement des boîtiers

Le niveau de l'architecture réseau sous la maîtrise du FAI 2, et commun au trois cas d'architecture précédents, est le backbone Gigabit Ethernet.

Aussi, si le service de filtrage n'est pas rendu par les opérateurs fournisseurs de l'accès ADSL en gros du FAI 2, celui-ci doit mettre en œuvre le filtrage au niveau du backbone.

Or, les boîtiers CopySense ne peuvent traiter unitairement qu'un trafic de quelques centaines de Mbps. Ceci implique de désagréger le trafic.

Deux scénarios peuvent être envisagés pour l'insertion des boîtiers CopySense dans l'architecture du FAI 2 :

1. Scénario où l'ensemble du trafic du FAI serait analysé et potentiellement filtré : positionnement des boîtiers au niveau du backbone, après désagrégation.
2. Scénario où seule une partie du trafic du FAI serait analysée et potentiellement filtrée pour les internautes en ayant fait la demande : positionnement des boîtiers au niveau d'une plate-forme dédiée, impliquant un routage spécifique des flux des abonnés au filtrage, ainsi qu'une désagrégation comme dans le cas du scénario 1.

Commentaires relatifs au scénario 1 :

- L'inconvénient de ce scénario est que le trafic total est géré, ce qui implique un nombre important de boîtiers, et un donc un coût élevé.
- L'intégralité de l'architecture du réseau de FAI 2 est à modifier
- Ce scénario suppose de désagréger le trafic au niveau du backbone en utilisant plusieurs équipements de type :
 - Routeur pour d'une part ne récupérer que les flux des abonnés à filtrer, et d'autre part décomposer des flux de 10 Gbps en 3 flux de 4 Gbps, selon une politique de routage ;
 - « Load balancer » pour décomposer les flux 4 Gbps en au maximum 14 flux de 300 Mbps ;
 - Boîtier CopySense : un par flux de 300 Mbps.
- De plus, afin d'intercepter tous les flux, y compris ceux entre deux clients du FAI, un routage en fonction de la source (adresse IP) serait requis pour les abonnés au filtrage, afin de remonter à la plate-forme de filtrage.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

Commentaires relatifs au scénario 2 :

- Ce scénario suppose de désagréger le trafic au niveau du backbone en utilisant plusieurs équipements de type :
 - Routeur pour d'une part ne récupérer que les flux des abonnés à filtrer, et d'autre part décomposer des flux de 10 Gbps en 3 flux de 4 Gbps, selon une politique de routage ;
 - « Load balancer » pour décomposer les flux 4 Gbps en au maximum 14 flux de 300 Mbps ;
 - Boîtier CopySense : un par flux de 300 Mbps.
- Un pool d'adresses IP dédié serait utilisé pour les abonnés au filtrage, et permettrait au niveau des routeurs cités ci-dessus de séparer les flux à traiter du trafic total.
- De plus, afin d'intercepter tous les flux, y compris ceux entre deux clients du FAI, un routage en fonction de la source (adresse IP) serait requis pour les abonnés au filtrage, afin de remonter à la plate-forme de filtrage.

Il est à noter que le scénario 2 engendre des problématiques de gestion avec une infrastructure de collecte ADSL IP option 1. En effet, c'est l'opérateur dégroupéur qui attribue les adresses IP pour le compte des abonnés de FAI 2. Ainsi, chaque DSLAM de l'opérateur dégroupéur doit avoir un pool d'adresses IP dédié au filtrage.

6.4.4. Décompte des boîtiers

Dans le cas du scénario 2 :

- Sur un échantillon de 200 000 abonnés, dont 10% souscrivent au service de filtrage, et avec l'hypothèse d'un trafic moyen actuel par abonné de 30 Kbps, le trafic à filtrer serait de l'ordre de 600 Mbps. Il faut pouvoir distinguer le trafic général du trafic des services de voix sur IP et de vidéo, qui vont engendrer dans le futur un trafic moyen par abonné de plusieurs centaines de kbps.
- Sur cette base, deux boîtiers CopySense seraient suffisants dans un premier temps pour filtrer le trafic correspondant (hors redondance et maintenance), à condition de concentrer le trafic à filtrer vers un site central.

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

Le prix catalogue des boîtiers CopySense est de 44 000 Euros, soit 4,4 Euros par abonné au filtrage. Il faut ajouter à ce coût d'investissement, celui des routeurs et load balancers requis, le coût d'ingénierie et de gestion du projet de nouveau service, et les coûts récurrents de maintenance et de suivi opérationnel. Ces coûts supplémentaires peuvent être significatifs et beaucoup plus importants au final que le coût des boîtiers de filtrage, ramené à l'abonné.

6.4.5. Contraintes induites chez le FAI

Les boîtiers CopySense sont configurés pour traiter les flux en fonction des adresses IP. Ainsi, il est nécessaire d'indiquer les adresses IP des abonnés à filtrer. Or, ces adresses IP sont fournies par le FAI ou l'opérateur de gros en mode dynamique (DHCP), ce qui exige :

- soit de rafraîchir en permanence la liste des adresses IP au niveau des boîtiers (peu réaliste en mode opérationnel),
- soit de gérer des plages d'adresses IP spécifiques pour les clients abonnés au filtrage (avec les contraintes correspondantes au niveau de la gestion de l'attribution de ces adresses IP).

En matière de réseau, les contraintes identifiées sont les suivantes :

- Nécessité de router les flux des abonnés à filtrer vers un point central, avec un impact sur la configuration des différents routeurs dans le réseau.
- Risque d'incompatibilité avec d'autres services nécessitant des infrastructures réseau particulières (ex : voix sur IP, vidéo et télévision sur ADSL). Il en résulterait un manque à gagner important pour le FAI en terme de revenu, ainsi qu'en terme de prise d'abonnés.

En matière de SI, les contraintes identifiées sont les suivantes :

- Intégration de la prise d'abonnement à la solution de filtrage (à travers la solution CopySense) avec le Système d'Information du FAI (OSS et BSS).

En matière de coût, les postes de coûts à prévoir seraient les suivants :

- Coûts d'investissement fixes :
 - ◆ Ingénierie générale et gestion de projet
 - ◆ Intégration avec les systèmes BSS
 - ◆ Intégration avec les systèmes OSS
 - ◆ Marketing et communication
- Coûts d'investissement variables, fonction du nombre d'abonnés au filtrage :

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- ◆ Boîtiers CopySense
- ◆ Equipements de réseau supplémentaires requis (routeurs, load balancers, ...)
- ◆ Installation
- Coûts récurrents :
 - ◆ Coûts récurrents sur la partie réseau (maintenance des matériels et logiciels, prestations d'administration, exploitation et supervision)
 - ◆ Coûts récurrents sur la partie SI (maintenance des matériels et logiciels, maintenance corrective et évolutive).

6.4.6. Cas d'utilisation de la solution de filtrage de contenus

L'utilisation de la solution Copysense pour rendre un service de filtrage aux abonnés qui le souhaitent et ceci avec une bonne couverture des différents cas de trafic (ex. cas des échanges entre le FAI 2 et l'internet, ou cas des échanges avec tous les clients du FAI 2) apparaît difficile à mettre en œuvre, compte tenu des contraintes d'architecture réseau et des problèmes de compatibilité avec les nouveaux services haut débit (ex. téléphonie, télévision et vidéo sur ADSL).

Une utilisation alternative consisterait à placer quelques boîtiers au niveau du backbone, en dérivation, et pour analyser une partie seulement du trafic, selon une approche statistique. Le rôle de la plateforme de filtrage serait alors en mode « radar à la demande », au profit des ayant-droits, souhaitant analyser une partie du trafic du FAI. Ce pourrait être un service rendu par le FAI aux ayant-droits.

6.5. Filtrage de protocole Allot dans le contexte d'un FAI 3

6.5.1. Architecture du FAI 3

Le FAI3 dispose de trois types d'architectures :

- (DSLAM / ATM) appartenant à France Telecom + (BAS centralisés / LAC) appartenant au FAI 3
- (DSLAM + ATM / BAS centralisés / LAC) appartenant au FAI 3
- (DSLAM IP BAS intégrés /Réseau IP) appartenant au FAI3

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00
		DATE MODIF.: 10/03/05 12:00

6.5.2. Solution Allot NetEnforcer

La gamme Allot NetEnforcer est composée des matériels suivants (tableau communiqué lors de l'audition Allot):

Modèle	Débit/par Interface réseau	Policies (1 ^{er} niveau)	Policies (1 ^{eme} niveau)	Nombre d'interface
AC-1010-SP/155M	155 Mbps	10,000	80,000	2
AC-1010-SP/310M	310 Mbps	10,000	80,000	2
AC-1010-SP/620M	620 Mbps	10,000	80,000	2
AC-1010-SP/1000M	1Gbps	10,000	80,000	2
AC-1020-SP/155M	155 Mbps	10,000	80,000	4
AC-1020-SP/310M	310 Mbps	10,000	80,000	4
AC-1020-SP/620M	620 Mbps	10,000	80,000	4
AC-1020-SP/1000M	1Gbps	10,000	80,000	4

Ces matériels fournissent des fonctions d'analyse et de filtrage de trafic P2P au niveau protocole. Ils doivent être positionnés en coupure sur le réseau du FAI. A noter que ces matériels prennent en compte les flux chiffrés SSL (ex. Winny / Filetopia / Earthstation 5 / SoftEther ...) ainsi que l'asymétrie des flux.

6.5.3. Scénarios de positionnement des boîtiers

Deux scénarios sont été identifiés pour l'insertion des boîtiers Allot dans l'architecture du FAI 3 :

3. Scénario où l'ensemble du trafic du FAI serait analysé et potentiellement filtré : Positionnement des boîtiers au niveau des points de peering (point d'échange entre un ou plusieurs FAI)
4. Scénario où seule une partie du trafic du FAI serait analysé et potentiellement filtré pour les internautes en ayant fait la demande : Positionnement des boîtiers au niveau d'une plateforme dédiée

Commentaires relatifs au scénario 1 :

- L'inconvénient de ce scénario est que le trafic P2P entre abonnés du même FAI3 ne serait pas filtré

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- Les boîtiers seraient positionnés en coupure sur des liens critiques pour le FAI – induisant un risque potentiel de dégradation de la qualité de service (temps de latence) et de sécurité de fonctionnement. Ce dernier point est mitigé d'une part en raison du fait que les boîtiers Allot, en cas de défaillance, basculent en mode pass-through, d'autre part en raison de l'existence de stratégies de routage alternatives (passage du trafic par d'autres points de peering en cas de défaillance de l'un d'entre eux)

Commentaires relatifs au scénario 2 :

- Lors de l'authentification d'un abonné ayant souscrit l'option de filtrage du peer to peer, le radius demande au DSLAM d'ouvrir un tunnel L2TP vers un LNS placé en point d'entrée de la plateforme dédiée disposant de la solution de filtrage. Note : pour un fonctionnement sans authentification (radius), l'identification est effectuée à partir de l'adresse MAC de l'abonné
- Dans le cas d'un mode d'accès au réseau sans authentification, il y a nécessité de créer un pool d'adresses IP dédié pour ces abonnés. Pas de contrainte géographique particulière (notamment : les pools d'IP actuels sont gérés de manière globale, sans dimension géographique)
- Des architecture de routage particulières sont déjà en place chez le FAI3 (ex : trafic wholesale pour un FAI tiers)
- Du fait de la mise en place des infrastructure de réseau particulières, ce scénario peut impacter la capacité à combiner des services (ex. combinaison « contrôle parental + firewall + filtrage P2P ») notamment dans le contexte des nouvelles architectures DSLAM IP.
- Ce scénario induit la mise en place de LNS centralisé et dédiés, à l'opposé des évolutions d'architecture en cours chez les opérateurs. Il ne permettra pas toujours la transparence des services Vs les abonnés non filtrés.
- Enfin, ce scénario induit un surcoût important d'études / validation / intégration pour chaque nouveau service développé par le FAI (les chaînes de liaisons sont dupliquées).

6.5.4. Décompte des boîtiers

Dans le scénario 1 :

- Sur la base d'une vingtaine de routeurs backbone et d'une dizaine de routeurs de peering (deux par site de peering), une vingtaine de boîtiers Allot seraient nécessaires pour analyser et filtrer le trafic (hors redondance et maintenance)

Dans le scénario 2 :

- Sur une base de 200 000 abonnés, dont 10% souscrivent le service, et l'hypothèse d'un trafic moyen par abonné de 26 Kb/s, le trafic à filtrer serait de l'ordre de 520 Mb/s

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
---------------	------------------------	--------------------------------------------------------------

- Sur cette base, un seul boîtier Allot serait suffisant pour filtrer le trafic correspondant (hors redondance et maintenance)

6.5.5. Contraintes induites chez le FAI

En matière de réseau, les contraintes identifiées en réunion sont les suivantes :

- Impact des boîtiers sur la qualité de service (les boîtiers sont positionnés en coupure)

Il est à noter que si le boîtier NetEnforcer introduit, certes, une latence, sa vocation première est néanmoins de mettre en place des mécanismes de QoS (garantie temps de réponse VoIP...). Du point de vue d'Allot, le temps de latence peut être considéré comme négligeable, et ne constitue pas la contrainte première de mise en œuvre de la solution .

- Risque d'incompatibilité avec d'autres services nécessitant des infrastructure réseau particulières (ex : VOIP)

En matière de SI, les contraintes identifiées en réunion sont les suivantes :

- Intégration la prise de la solution de filtrage (à travers la solution Allot) avec le Système d'Information (OSS et BSS)

En matière de coût, les postes de coûts à prévoir seraient :

- Coûts d'investissement fixes quelque soit le nombre d'abonnés mais variable en fonction du nombre de services offerts* par les FAI :
 - ◆ Ingénierie générale
 - ◆ Intégration avec les systèmes BSS
 - ◆ Intégration avec les systèmes OSS
 - ◆ Marketing et communication
- Coûts d'investissement variables, fonction du nombre d'abonnés au filtrage :
 - ◆ Boîtiers Allot
 - ◆ LNS dédiés
 - ◆ Routeurs d'agrégation dans le BB
 - ◆ Plate-forme de service, eg. Serveurs de Mail & Hébergement de pages Web (partiellement au moins en fonction du niveau de sécurité souhaité)
 - ◆ Installation
- Coûts récurrents
 - ◆ Coûts récurrents partie réseau (maintenance des matériels et logiciels, prestations d'administration, exploitation et supervision)

VERSION : v10	RAPPORT D'ETUDE	DATE CREATION: 10/03/05 12:00 DATE MODIF.: 10/03/05 12:00
----------------------	------------------------	----------------------------------------------------------------------------

- ◆ Coûts récurrents partie SI (maintenance des matériels et logiciels, maintenance corrective et évolutive)
- (*) Un service peut être soit la création d'un nouveau débit d'accès, soit d'un nouveau bundle de service (VoIP+@) par exemple

En matière de pérennité / efficacité :

- Il est nécessaire d'accepter le risque d'une interruption du filtrage notamment entre l'apparition de nouveaux protocoles, principalement les protocoles encryptés, et la disponibilité (à confirmer) de mises à jour des logiciels des boîtiers permettant de les filtrer.
- Par ailleurs, la capacité à filtrer des protocoles encryptés par les solutions de filtrage de protocole est liée soit à la reconnaissance des négociations préalable au passage au mode crypté, soit à l'exploitation de failles (via une analyse comportementale) dans les échanges cryptés. Ces éléments sont particulièrement complexes dans le cas où les flux montants et descendants n'utilisent pas les mêmes liens (ce qui est un cas courant).