Groupe de travail Réseau
**Request for Comment : 4924**
Catégorie : Information
Traduction Claude Brière de L'Isle

B. Aboba, éditeur
E. Davies, Bureau de l'architecture de l'Internet
juillet 2007

# Réflexions sur la transparence de l'Internet



**Résumé**
Le présent document passe en revue les déclarations précédentes de l'IAB sur la transparence dans l'Internet, ainsi qu'un exposé sur les nouveaux problèmes de transparence. Loin d'avoir diminué en pertinence, les implications techniques des obstacles intentionnels ou involontaires à la transparence du réseau jouent un rôle critique dans la capacité de l'Internet à prendre en charge l'innovation et la communication mondiale. Le présent document fournit des illustrations spécifiques de ces impacts potentiels.

**Table des Matières**



## 1. Introduction

Dans le passé, l'IAB a publié un certain nombre de documents relatifs à la transparence dans l'Internet et sur le principe de bout en bout, et d'autres documents de l'IETF ont également traité aussi de ces questions. Ces documents argumentent les principes généraux sur lesquels est fondée l'architecture de l'Internet, ainsi que les valeurs centrales que la communauté de l'Internet cherche à protéger pour aller de l'avant. Le présent document réaffirme ces principes, décrit le concept de "transport transparent" tel que développé dans le projet [NewArch] du DARPA, et traite d'un certain nombre de nouveaux problèmes de la transparence.

Un réseau qui ne filtre ou transforme pas les données qu'il transporte peut être dit "transparent" ou "oublieux" à l'égard du contenu des paquets. Les réseaux qui fournissent un transport transparent permettent le développement des nouveaux services sans exiger de changements cruciaux. C'est cette souplesse qui est peut-être à la fois la caractéristique la plus essentielle de l'Internet tout comme le plus important contributeur à son succès.

Le Section 2 de "Principes de l'architecture de l'Internet" [RFC1958] décrit les principes qui sont au cœur de l'architecture de l'Internet :

> "Cependant, en termes très généraux, la communauté estime que le but est la connexité, que l'outil est le protocole Internet, et que l'intelligence est de bout en bout plutôt que cachée dans le réseau.
>
> La croissance exponentielle actuelle du réseau semble montrer que la connexité est sa propre récompense, et a plus de valeur que n'importe quelle application individuelle telle que la messagerie ou la Toile mondiale. Cette connexité exige la coopération technique entre les fournisseurs de service, et elle fleurit dans l'environnement de

télécommunications commerciales de plus en plus libérales et concurrentielles."

Le paragraphe 4.1.1 de "La montée du milieu et le futur du bout en bout : Réflexions sur l'évolution de l'architecture de l'Internet" [RFC3724], décrit certaines des conséquences souhaitables de cette approche :

"Une conséquence souhaitable du principe de bout en bout est la protection de l'innovation. Exiger la modification du réseau afin de déployer de nouveaux services est normalement encore plus difficile que de modifier les nœuds d'extrémité. Le contre argument – que de nombreux nœuds d'extrémité sont maintenant essentiellement des boîtes closes qu'on ne peut pas mettre à jour et que la plupart des utilisateurs ne veulent de toutes façons pas mettre à jour – ne s'applique pas à tous les nœuds et à tous les utilisateurs. De nombreux nœuds d'extrémité sont encore configurables par l'utilisateur et un pourcentage notable d'utilisateurs sont des "adopteurs précoces," qui veulent saisir une certaine quantité d'avancées technologiques afin d'essayer de nouvelles idées. Et, même pour les boîtes closes et les utilisateurs non impliqués, du code téléchargeable qui respecte le principe de bout en bout peut soutenir une innovation de service rapide. Exiger de quelqu'un qui a une nouvelle idée pour un service qu'il convainque un groupe d'administrateurs de FAI ou d'un réseau d'entreprise de modifier leurs réseaux est beaucoup plus difficile que de simplement créer une page de la Toile avec un logiciel téléchargeable qui met en œuvre le service."

Cependant, bien que l'Internet se soit largement développé à la fois en taille et en diversité d'applications, le degré de transparence a diminué. La [RFC2775] "Transparence de l'Internet" note certaines des causes de la perte de la transparence de l'Internet et analyse leur impact. Elle comporte la discussion des traducteurs d'adresse réseau (NAT, *Network Address Translator*), pare-feu, passerelles de niveau d'application (ALG, *Application Level Gateway*), relais, mandataires, antémémoires, partage du service de noms de domaine (DNS, *Domain Name Service*), équilibreurs de charge, etc. La [RFC2775] analyse aussi les directions potentielles qui devraient à l'avenir conduire à la restauration de la transparence. La Section 6 résume les conclusions :

"Bien que le scénario IPv6 pur soit le plus simple et le plus net, on ne peut pas l'atteindre directement. Les scénarios divers sans l'utilisation d'IPv6 sont tous confus et semblent finalement conduire à des impasses d'une sorte ou d'une autre. Le déploiement partiel d'IPv6, qui est une étape exigée sur le chemin du déploiement complet, est aussi confus mais évite les impasses."

Bien que la pleine restauration de la transparence de l'Internet grâce au déploiement d'IPv6 reste un objectif, le rôle croissant de l'Internet dans la société, la diversité accrue des applications, et la croissance continue des menaces contre la sécurité ont altéré l'équilibre entre transparence et sécurité, et le caractère disparate des objectifs des parties intéressées rend ces compromis complexes par nature.

Bien que la transparence procure une grande souplesse, elle rend aussi plus facile la livraison du trafic voulu aussi bien que non désiré. Le trafic non désiré est cité de plus en plus souvent comme la justification pour la limitation de la transparence. Porté à sa conclusion logique, cet argument conduirait au développement de barrières encore plus complexes à la transparence pour contrer les menaces de plus en plus sophistiquées contre la sécurité. La transparence, quand elle est perdue, est difficile à restaurer, de sorte que une telle approche, si elle échoue, conduirait à un Internet qui serait à la fois un lieu d'insécurité et sans transparence. L'autre solution de l'alternative est de développer des mécanismes de sécurité fondés sur l'hôte d'une sophistication accrue ; bien qu'une telle approche puisse aussi échouer à tenir en échec des menaces d'une sophistication croissante contre la sécurité, elle devrait moins y sacrifier la transparence.

Comme beaucoup des forces fondamentales qui ont conduit à la réduction de la transparence dans l'Internet IPv4 peuvent aussi jouer un rôle dans l'Internet IPv6, la transparence de l'Internet IPv6 ne va pas de soi, mais représente plutôt un idéal dont la maintenance exigera un effort constant significatif.

Comme noté dans [NewArch], la coopération technique qui a caractérisé dans le passé le développement de l'Internet a donné lieu de façon croissante à une bagarre entre les intérêts des abonnés, des fabricants, des fournisseurs de services, et de la société dans son ensemble. Le transport transparent peut être désiré par des développeurs qui cherchent à déployer de nouveaux services ; les fournisseurs peuvent souhaiter bloquer le trafic indésirable au niveau du cœur de réseau avant qu'il n'impacte les abonnés ; les fabricants et fournisseurs de services peuvent souhaiter permettre la livraison de "services à valeur ajoutée" dans le réseau qui leur permettent de différencier leurs offres ; les abonnés peuvent tourner leur sympathie vers l'un ou l'autre point de vue, selon leurs intérêts ; la société au sens large peut souhaiter bloquer le matériel "offensant" et surveiller le trafic qui montre des intentions malveillantes.

Bien qu'il n'y ait pas de "remède" architectural qui puisse restaurer le transport transparent tout en satisfaisant les intérêts de toutes les parties, il est possible aux fournisseurs d'offrir aux abonnés des informations sur la nature des services qui sont fournis. Les abonnés ont besoin de savoir si ils reçoivent du transport transparent, et si ce n'est pas le cas, comment le service affecte leur trafic.

Depuis la publication des déclarations de l'IAB précédemment citées, de nouvelles technologies ont été développées, et les

vues sur les technologies existantes ont changé. Dans certains cas, ces nouvelles technologies impactent le transport transparent, et les abonnés ont besoin de connaître les implications sur leur service.

## 2. Questions supplémentaires de transparence

### 2.1 Restriction d'application

Comme une des forces de l'architecture de l'Internet est la facilité avec laquelle peuvent être déployées les nouvelles applications, les pratiques qui restreignent la capacité à déployer de nouvelles applications portent en elles un potentiel de réduction de l'innovation.

Une de ces pratiques est le filtrage conçu pour bloquer ou restreindre l'usage d'applications, mis en œuvre sans le consentement de l'utilisateur. Cela inclut le filtrage des couches Internet, Transport, et Application, conçu pour bloquer ou restreindre le trafic associé à une ou plusieurs applications.

Bien que le filtrage par le fournisseur puisse être utile pour régler les questions de sécurité telles que les attaques contre les infrastructures du fournisseur ou les attaques de déni de service, une souplesse supérieure est fournie en permettant que le filtrage soit déterminé par le consommateur. Normalement cela devrait être mis en œuvre sur les bordures, comme dans les routeurs d'accès du fournisseur (par exemple, des services de pare-feu externalisés) dans les locaux du consommateur (par exemple, les pare-feu d'accès) ou sur les hôtes (par exemple, les pare-feu d'hôte). Le développement du filtrage aux bordures fournit aux consommateurs la souplesse de choisir quelles applications ils souhaitent bloquer ou restreindre, tandis que le filtrage au cœur de réseau peut ne pas permettre aux hôtes de communiquer, même lorsque la communication serait conforme aux politiques d'utilisation appropriées des domaines administratifs auxquels appartiennent ces hôtes.

En pratique, le filtrage destiné à bloquer ou restreindre l'usage d'applications est difficile à mettre en œuvre avec succès sans le consentement du consommateur, car avec le temps, les développeurs vont tendre à reconstruire les protocoles filtrés de façon à éviter les filtres. Donc au fil du temps le filtrage va vraisemblablement résulter en problèmes d'interopérabilité ou en une complexité inutile. Ces coûts surviennent sans le bénéfice d'un filtrage efficace car de nombreux protocoles d'application commencent à utiliser HTTP comme protocole de transport après que les développeurs d'application ont observé que les pare-feu permettent le trafic HTTP tout en éliminant les paquets pour les protocoles inconnus.

En plus des problèmes d'architecture, le filtrage pour bloquer ou restreindre l'utilisation d'applications soulève aussi des problèmes de divulgation et de consentement de l'utilisateur final. Comme cela est souligné dans la [RFC4084] "Terminologie pour décrire la connexité sur l'Internet", les services annoncés comme fournissant la "connexité Internet" diffèrent considérablement dans leurs capacités, ce qui conduit à une certaine confusion. Le document définit la terminologie qui se rapporte à la connexité Internet, y compris la "connexité de la Toile", "la connexité du client seul, sans adresse publique", "client seul, adresse publique, "connexité Internet à travers un pare-feu", et "pleine connexité Internet". Par rapport à la "pleine connexité Internet" la section 2 de la [RFC4084] note :

"Les mandataires de filtrage de la Toile, les mandataires d'interception, les NAT, et les autres restrictions imposées par les fournisseurs sur les accès d'entrée ou de sortie et sur le trafic sont incompatibles avec ce type de service. Les serveurs ... sont normalement considérés comme normaux. Les seules restrictions compatibles sont les limitations de bande passante et les interdictions portant sur l'abus du réseau ou des activités illégales."

La section 4 de la [RFC4084] décrit les obligations de divulgation qui s'appliquent à toutes les formes de limitation de service, qu'elles soient appliquées au trafic entrant ou sortant :

"Plus généralement, le fournisseur devrait identifier toutes les actions du service pour bloquer, restreindre, ou altérer la destination ou l'utilisation hors limite (c'est à dire, l'utilisation de services qui ne sont pas offerts par le fournisseur ou le réseau du fournisseur) des services d'application."

Par nature, la [RFC4084] invite les fournisseurs à déclarer la façon dont le service fourni se distingue du transport transparent. Comme l'absence de transport transparent au sein des réseaux de transit va aussi affecter la transparence, cela s'applique aussi aux fournisseurs sur les réseaux desquels le trafic de l'abonné peut voyager.

### 2.2 Qualité de service (QS)

Bien que la [RFC4084] note que les limitations de bande passante sont compatibles avec la "pleine connexité Internet", dans certains cas, les restrictions sur la QS peuvent aller au delà des simples limitations moyennes ou de crête de bande

passante. Lorsque ils sont utilisés pour restreindre la capacité à déployer de nouvelles applications, les mécanismes sont incompatibles avec la "pleine connexité Internet" telle que définie dans la [RFC4084]. Les obligations de divulgation et de consentement auxquelles se réfère la section 4 de la [RFC4084] s'appliquent aussi aux mécanismes de QS.

Le déploiement de la technologie de la QS a des implications potentielles sur la transparence de l'Internet, car la QS rencontrée par un flux peut rendre l'Internet plus ou moins transparent pour ce flux. Bien que la prise en charge de la QS soit désirable afin que les services en temps réel coexistent avec les services élastiques, cela n'est pas sans impacter la livraison des paquets.

Précisément, les classes de QS telles que "par défaut" [RFC2474] ou "moindre effort" [RFC3662] peuvent rencontrer de plus forts taux de pertes aléatoires que d'autres comme la "transmission assurée" [RFC2597]. À l'inverse, les classes de QS à bande passante limitée telles que la "transmission accélérée" [RFC3246] peuvent rencontrer des pertes systématiques de paquet si elles excèdent la bande passante qui leur est allouée. D'autres mécanismes de QS tels que l'équilibrage de charge peuvent avoir des effets collatéraux tels que le réarrangement des paquets, qui peut avoir un impact sérieux sur les performances perçues.

Les mises en œuvre de QS qui réduisent la capacité à déployer de nouvelles applications sur l'Internet ont un effet similaire à celui des autres barrières à la transparence. Comme des limitations arbitraires ou sévères de bande passante peuvent rendre une application inutilisable, l'introduction de limitations de bande passante spécifiques de l'application est équivalente au blocage ou à l'interdiction de l'application du point de vue de l'utilisateur.

L'utilisation de mécanismes de QS pour discriminer le trafic qui ne correspond pas à un ensemble de services ou d'adresses a un effet similaire à celui du déploiement d'un pare-feu très restrictif. Exiger pour un flux une réservation RSVP authentifiée [RFC2747], [RFC3182] pour éviter une perte sévère de paquets a un effet similaire au déploiement d'une traversée authentifiée de pare-feu.

Comme avec le filtrage, il peut y avoir des utilisations valides pour les restrictions de QS imposées par l'utilisateur. Par exemple, un consommateur peut souhaiter limiter la bande passante consommée par des services de partages de fichier d'homologue à homologue, afin de limiter l'impact sur des applications à la mission critique.

## 2.3 Passerelles de couche Application (ALG)

L'IAB a consacré une attention considérable à la traduction d'adresse réseau (NAT, *Network Address Translation*), de sorte qu'il n'est pas besoin de répéter ici cette discussion. Cependant, au fil du temps, il est devenu évident qu'il y a des problèmes qui sont inhérents au déploiement des passerelles de couche application (ALG, *Application Layer Gateway*) (fréquemment incorporées dans les pare-feu et les appareils qui mettent en œuvre les NAT).

Le paragraphe 3.5 de la [RFC2775] déclare :

"Si toute la gamme des applications de l'Internet doit être utilisée, les NAT doivent être couplés à des passerelles de niveau application (ALG) ou à des mandataires. De plus, l'ALG ou le mandataire doit être mis à jour chaque fois qu'une nouvelle application dépendante de l'adresse apparaît. En pratique, la fonctionnalité de NAT est incorporée dans de nombreux produits de pare-feu, et tous les NAT utiles ont des ALG associés, de sorte qu'il est difficile de démêler leurs divers impacts."

Avec le recul du temps et le développement des technologies de traversée de NAT telles que IKE NAT-T [RFC3947], Teredo [RFC4380], et STUN [RFC3489], il est devenu évident que les ALG représentent une barrière supplémentaire à la transparence. En plus d'opposer des barrières au déploiement de nouvelles applications non encore prises en charge par les ALG, celles-ci peuvent créer des difficultés dans le déploiement des applications existantes aussi bien qu'à leurs versions mises à jour. Par exemple, dans le développement de IKE NAT-T, des difficultés supplémentaires ont été présentées par les ALG "IPsec Helper" incorporées dans les NAT.

On doit souligner que ces difficultés sont inhérentes à l'architecture des ALG, plutôt qu'un simple artifice des mauvaises mises en œuvre. Quelle que soit la qualité de la mise en œuvre d'une ALG, des barrières à la transparence émergeront avec le temps, de sorte que la notion d'une "ALG transparente" porte une contradiction dans ses termes.

En particulier, les ALG DNS soulèvent une quantité de questions, y compris d'incompatibilités avec DNSSEC qui empêchent le déploiement d'une infrastructure de dénominations sécurisée même si tous les points d'extrémité sont mis à niveau. Pour des précisions sur ce sujet, voir la section 3 de "Raisons du passage du protocole de traduction d'adresse réseau (NAT-PT) au statut de Historique" [RFC4966].

## 2.4 Restrictions sur les adresses IPv6

Le paragraphe 5.1 de la [RFC2775] déclare :

"Noter que c'est une hypothèse de base d'IPv6 qu'aucune contrainte artificielle ne serait placée à la fourniture des adresses, étant donné qu'elles sont si nombreuses. Les pratiques actuelles par lesquelles certains FAI limitent fortement le nombre d'adresses IPv4 par client n'auront aucune raison d'exister pour IPv6."

Les contraintes sur la fourniture des adresses IPv6 fournissent une incitation au déploiement de NAT avec IPv6. L'introduction de NAT pour IPv6 représenterait une barrière à la transparence, et donc est à éviter autant que possible.

### 2.4.1 Allocation des adresses IPv6 pour les fournisseurs d'accès

Afin d'encourager les déploiements de IPv6 pour fournir le transport transparent, il est important que les réseaux IPv6 de toutes tailles reçoivent un préfixe suffisant pour permettre l'allocation d'adresses et de sous-réseaux pour tous les hôtes et liaisons au sein de leur réseau. La politique d'allocation initiale d'adresses suggérait d'allouer un préfixe /48 aux "petits" sites, ce qui devrait répondre aux exigences normales. Tout changement de la politique d'allocation devrait prendre en compte la réduction de transparence qui va résulter de nouvelles restrictions. Par exemple, les fournisseurs qui approvisionnent pour un seul /64 sans soutien pour une délégation de préfixe ou (encore pire) un préfixe plus long (interdit par le paragraphe 2.5.4 de la [RFC4291] pour les préfixes d'envoi individuel non-000/3) représenteraient une restriction de la disponibilité des adresses IPv6 qui pourrait constituer une barrière à la transparence.

### 2.4.2 IKEv2

Les problèmes posés par les mécanismes d'allocation d'adresses IPv6 dans IKEv2 [RFC4306] sont décrits dans la [RFC4718] :

"IKEv2 définit aussi les charges utiles de configuration pour IPv6. Cependant, elles se fondent sur les charges utiles IPv4 correspondantes, et ne suivent pas complètement la "façon normale dont IPv6 fait les choses"... En particulier, les messages IPv6 d'auto configuration sans état ou d'annonce de routeur ne sont pas utilisés, ni la découverte de voisin."

IKEv2 prévoit l'allocation d'une seule adresse IPv6, en utilisant l'attribut INTERNAL_IP6_ADDRESS. Si c'est le seul attribut pris en charge pour l'allocation d'adresse IPv6, une seule adresse IPv6 sera alors disponible. L'attribut INTERNAL_IP6_SUBNET permet à l'hôte de déterminer les sous-réseaux accessibles directement à travers le tunnel sécurisé créé ; il pourrait être utilisé pour allouer un ou plusieurs préfixes à l'initiateur IKEv2 qui pourrait être utilisé pour la création d'adresse.

Cependant, cela ne permet pas à l'hôte d'obtenir des préfixes qu'il pourrait déléguer. L'attribut INTERNAL_IP6_DHCP fournit l'adresse d'un serveur DHCPv6, qui peut éventuellement utiliser la délégation de préfixe DHCPv6 [RFC3633] pour obtenir des préfixes additionnels. Cependant, afin que les mises en œuvre utilisent ces options de façon interopérable, des éclaircissements à la spécification IKEv2 paraissent nécessaires.

## 2.5 Problèmes du DNS

### 2.5.1 Racine unique

Dans la [RFC2826] "Commentaire technique de l'IAB sur le DNS à racine unique", les arguments techniques en faveur d'une racine unique ont été présentés.

Une des prémisses de la [RFC2826] est qu'un espace de noms commun et qu'une sémantique commune s'appliquent à ces noms est nécessaire pour une communication efficace entre deux parties. L'argument du document est que ce principe ne peut être satisfait que lorsque une racine unique est utilisée et lorsque les domaines sont entretenus par un seul propriétaire ou gestionnaire.

Comme la [RFC4084] ne vise que les termes de service IP et ne parle pas des problèmes de l'espace des noms, elle ne se réfère pas à la [RFC2826]. Nous affirmons avec force que l'utilisation d'une racine unique pour l'espace de noms du DNS est essentielle pour un service IP correct.

### 2.5.2 Démantèlement de l'espace des noms

Depuis la publication de la [RFC2826], il y a eu des rapports de fournisseurs de service qui mettent en œuvre des serveurs de noms récurrents et/ou des transmetteurs du DNS qui remplacent les réponses qui indiquent qu'un nom n'existe pas dans la hiérarchie du DNS par un enregistrement de nom et d'adresse qui héberge un service de la Toile supposé être utile aux

utilisateurs finaux.

L'effet de cette modification est similaire au placement d'un caractère générique dans les domaines de niveau supérieur. Bien que les étiquettes de caractère générique dans les domaines de niveau supérieur conduisent à des problèmes qui sont décrits ailleurs (comme dans "Le rôle des caractères génériques dans le système des noms de domaines" [RFC4592]), elles ne violent pas strictement parlant le protocole DNS. Ce n'est pas le cas lorsque la modification des réponses a lieu au milieu du chemin entre les serveurs d'autorité et les résolveurs d'extrémité qui fournissent les réponses aux applications.

Le paragraphe 1.3 de la [RFC2826] déclare :

"La conception et les mises en œuvre du protocole DNS ont lourdement pesé sur l'hypothèse qu'il y a un seul propriétaire ou gestionnaire pour chaque domaine, et que tout ensemble d'enregistrements de ressources associé à un domaine est modifié par une seule copie en série."

En particulier, le protocole DNSSEC décrit dans "Modifications du protocole pour les extensions de sécurité du DNS" [RFC4035] a été conçu pour vérifier que les informations du DNS n'ont pas été modifiées entre le moment où elles ont été publiées sur un serveur d'autorité et le moment où a lieu la validation. Comme cette vérification peut avoir lieu au niveau application, toute modification par un transmetteur récurrent ou autre intermédiaire va causer un échec de validation, désactivant l'amélioration de la sécurité que DNSSEC est destiné à fournir.

### 2.6 Équilibrage de charge et redirection

Pour fournir des informations adaptées aux conditions locales de l'endroit d'où provient une demande, ou pour fournir un service plus rapide, ont été développées des techniques qui ont pour résultat que des paquets sont redirigés ou prennent un chemin différent selon l'endroit d'où provient la demande. Par exemple, les demandes peuvent être réparties entre les serveurs en utilisant le "NAT inversé" (qui modifie l'adresse de destination plutôt que de source) ; les réponses aux demandes du DNS peuvent être altérées ; les "get" HTTP peuvent être redirigés; ou des paquets spécifiques peuvent être détournés sur des réseaux superposés.

Pourvu que ces services soient bien mis en œuvre, ils peuvent être précieux ; cependant, il peut aussi en résulter une réduction de la transparence ou des perturbations de service :

[1] L'utilisation de "NAT inverse" pour équilibrer la charge entre les serveurs qui prennent en charge IPv6 aurait un effet négatif sur la transparence de l'Internet IPv6.

[2] La redirection du DNS est normalement fondée sur l'adresse de source de l'interrogation, qui peut ne pas fournir d'informations sur la localisation de l'hôte d'origine de l'interrogation. Il en résulte qu'un hôte configuré avec l'adresse d'un serveur DNS distant pourrait se trouver lui-même pointer sur un serveur près du serveur DNS, plutôt que sur un serveur près de l'hôte. La redirection HTTP ne rencontre pas ce problème.

[3] Si les filtres de paquet qui détournent les paquets sur des réseaux superposés sont mal configurés, cela peut conduire à ce que des paquets soient mal dirigés sur le réseau superposé et soient retardés ou perdus si l'extrémité distante ne peut pas les faire revenir sur l'Internet mondial.

[4] L'utilisation de l'envoi à la cantonade doit être mûrement réfléchie afin que le service puisse être maintenu en présence de changements d'acheminement.

## 3. Considérations pour la sécurité

Plusieurs des problèmes de transparence exposés dans le présent document (NAT, mandataires transparents, éclatement de l'espace de noms du DNS) affaiblissent les garanties existantes de sécurité de bout en bout et interfèrent avec le déploiement des protocoles qui renforceraient la sécurité de bout en bout.

La section 7 de la [RFC2775] déclare :

"La perte de la transparence à la frontière Intranet/Internet peut être considérée comme un problème de sécurité, car elle fournit un point bien défini auquel appliquer les restrictions. Cette forme de sécurité est sujette au risque "dur à l'extérieur, mou à l'intérieur", par lequel toute pénétration réussie de la frontière expose l'Intranet entier à des attaques triviales. Le manque de sécurité de bout en bout appliqué à l'intérieur de l'Intranet ignore aussi les menaces internes."

De nos jours, les logiciels malveillants ont évolué pour tirer de plus en plus parti de la couche application comme source riche et financièrement attractive de faiblesses de la sécurité, ainsi que comme mécanisme de pénétration de la frontière Intranet/Internet. Cela a affaibli la valeur de la sécurité des barrières existantes à la transparence et rend de plus en plus difficile d'empêcher la propagation des logiciels malveillants sans imposer de restrictions au comportement des applications. Cependant, comme avec les autres approches de restriction des applications (voir le paragraphe 2.1), ces limitations sont imposées de façon plus souple aux bordures.

## 4. Références


[NewArch] D. Clark et autres, "New Arch: Future Generation Internet Architecture", http://www.isi.edu/newarch/iDOCS/final.finalreport.pdf

[RFC1958] B. Carpenter, éd., "Principes de l'architecture de l'Internet", juin 1996. (*MàJ par* RFC3439) *(Information)*

[RFC2474] K. Nichols, S. Blake, F. Baker et D. Black, "Définition du champ Services différenciés (DS Field) dans les en-têtes IPv4 et IPv6", décembre 1998. (*MàJ par* RFC3168, RFC3260) *(P.S.)*

[RFC2597] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, "Groupe PHB Transmission assurée", juin 1999. (*MàJ par* RFC3260) *(P.S.)*

[RFC2747] F. Baker, B. Lindell, M. Talwar, "Authentification cryptographique RSVP", janvier 2000. (*MàJ par* RFC3097) *(P.S.)*

[RFC2775] B. Carpenter, "Transparence de l'Internet", février 2000. *(Information)*

[RFC2826] Bureau de l'architecture de l'Internet, "Commentaire technique de l'IAB sur le DNS à racine unique", mai 2000. *(Info.)*

[RFC3182] S. Yadav et autres, "Représentation d'identité pour RSVP", octobre 2001. *(P.S.)*

[RFC3246] B. Davie et autres, "Comportement de transmission par bond expédié ", mars 2002. *(P.S.)*

[RFC3489] J. Rosenberg et autres, "STUN - Simple traversée par le protocole de datagramme d'utilisateur (UDP) des traducteurs d'adresse réseau (NAT)", mars 2003. (*Obsolète, voir* RFC5389) *(P.S.)*

[RFC3633] O. Troan, R. Droms, "Options de préfixes IPv6 pour le protocole de configuration dynamique d'hôte (DHCP) version 6", décembre 2003. *(P.S.)*

[RFC3662] R. Bless, K. Nichols, K. Wehrle, "Comportement par domaine au moindre effort (PDB) pour services différenciés", décembre 2003. *(Information)*

[RFC3724] J. Kempf et R. Austein, éd., IAB "L'avenir du bout en bout : Réflexions sur l'évolution de l'architecture de l'Internet", mars 2004. *(Information)*

[RFC3947] T. Kivinen et autres, "Négociation de traversée de NAT dans IKE", janvier 2005. *(P.S.)*

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005.

[RFC4084] J. Klensin, "Terminologie pour décrire la connexité Internet", mai 2005. (BCP0104)

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. *(Remplace* RFC3513) *(D.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005.

[RFC4380] C. Huitema, "Teredo : Tunnelage IPv6 sur UDP à travers des traductions d'adresse réseau (NAT)", février 2006. *(P.S.)*

[RFC4592] E. Lewis, "Le rôle des caractères génériques dans le système des noms de domaines", juillet 2006. *(P.S.)*

[RFC4718] P. Eronen, P. Hoffman, "Précisions et lignes directrices pour la mise en œuvre de IKEv2", octobre 2006. *(Information)*

[RFC4966] C. Aoun, E. Davies, "Raisons du passage du protocole de traduction d'adresse réseau (NAT-PT) au statut de Historique", juillet 2007. (Remplace RFC2766) *(Information)*



**Remerciements**

Les auteurs tiennent à remercier Jari Arkko, Stephane Bortzmeyer, Brian Carpenter, Spencer Dawkins, Stephen Kent, Carl Malamud, Danny McPherson, Phil Roberts and Pekka Savola de leurs contributions au présent document.

## Appendice A – Membres de l'IAB au moment de l'approbation du document

Bernard Aboba
Loa Andersson
Brian Carpenter
Leslie Daigle
Elwyn Davies
Kevin Fall
Olaf Kolkman
Kurtis Lindqvist
David Meyer
David Oran
Eric Rescorla
Dave Thaler
Lixia Zhang

### Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
mél : bernarda@microsoft.com
téléphone : +1 425 706 6605
Fax : +1 425 936 7329

Elwyn B. Davies
Consultant
Soham, Cambs
UK
téléphone : +44 7889 488 335
mél : elwynd@dial.pipex.com

### Déclaration complète de droits de reproduction



### Propriété intellectuelle



### Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.