Groupe de travail Réseau
Request for Comments : 4084
BCP : 104
Catégorie : Bonnes pratiques actuelles

J. Klensin
mai 2005

Traduction Claude Brière de L'Isle

Terminologie pour la description de la connexité Internet

Résumé
Avec l'évolution de l'Internet, de nombreux types d'arrangements ont été annoncés et vendus comme "connexité Internet". Comme il peut y avoir des différences significatives dans les capacités offertes, la gamme des options, et l'absence de toute terminologie standard, l'effort pour faire la distinction entre ces services a causé une confusion considérable chez les consommateurs. Le présent document donne une liste de termes et définitions qui pourrait être utiles aux fournisseurs, consommateurs, et éventuellement aux réglementeur pour préciser le type et le caractère des services offerts.

Table des Matières

1. Introduction

1.1 Le problème et ses exigences

Différent fournisseurs d'accès Internet et autres fournisseurs offrent une large variété de produits qui sont identifiés comme "Internet" ou "accès Internet". Ces produits offrent différents types de fonctionnalités et, par suite, certains peuvent être appropriés pour certains utilisateurs et utilisations et pas d'autres. Par exemple, un service qui offre seulement l'accès à la Toile (dans ce contexte, la portion de l'Internet qui est accessible via les protocoles HTTP et HTTPS) peut être approprié pour quelqu'un qui est exclusivement intéressé à la navigation dans les services de messagerie électronique fondés sur la Toile. Il ne sera pas approprié pour quelqu'un qui a besoin de télécharger des fichiers ou d'utiliser plus fréquemment la messagerie électronique. Et il est probable qu'il sera encore moins approprié pour quelqu'un qui a besoin de faire fonctionner des serveurs pour d'autres utilisateurs, qui a besoin de capacités de réseaux virtuels privés (VPN) ou d'autres accès sécurisés à un bureau distant, ou qui a besoin de synchroniser la messagerie pour une utilisation hors ligne.

Les changements rapides de l'environnement et l'évolution récente de la messagerie électronique de l'Internet ont conduit à des restrictions supplémentaires sur l'envoi et la restitution de la messagerie électronique. Ces restrictions, dont la plupart ont été développées au titre de tentatives bien intentionnées d'empêcher ou combattre les messages non désirés, peuvent être imposées indépendamment des types de service décrits ci-dessous et sont discutées séparément à la Section 3.

Le présent document décrit seulement les fonctions fournies ou permises par le fournisseur de service. Il ne spécifie pas les fonctions qui passent à travers et sont prises en charge par les divers équipements fournis par l'utilisateur.

Les termes DEVRAIT, DOIT, ou PEUT sont en majuscules dans ce document, comme défini dans la [RFC2119].

1.2 Adoption d'une terminologie non péjorative

Les définitions proposées ici n'ont de valeur que si les fournisseurs de service et les fabricants veulent bien les adopter. Les termes proposés sont destinés à n'être pas péjoratifs, en dépit de la croyance de certains membres de la communauté IETF que certains de ces modèles de connexité sont simplement "vieillots" et "pas vraiment un service Internet". La mention d'un service ou modèle particulier dans le présent document n'implique aucune officialisation de celui-ci, seulement la reconnaissance de quelque chose qui existe ou pourrait exister sur le marché. Donc, les bonnes pratiques actuelles décrites dans le présent document sont sur la terminologie et les informations qui devraient être fournies à l'utilisateur et non sur les types de service qui devraient être offerts.

2. Terminologie générale

Cette section fait la liste des principaux termes de service IP. On espère que les fournisseurs de services vont adopter ces termes, pour mieux définir les services aux utilisateurs ou consommateurs potentiels. Les termes se réfèrent à l'intention du fournisseur (FAI), comme exprimée dans les mesures techniques ou les termes et conditions de service. Il est possible de contourner des mises en œuvre particulières de ces caractéristique de types de connexité, mais cette liberté n'est généralement pas l'intention du fournisseur ; il est peu probable qu'elle soit soutenue si les contournements cessent de fonctionner.

Les termes de service sont énumérés dans l'ordre ascendant de capacité à atteindre la "pleine connexité Internet".

Connexité à la Toile :
Ce service fournit la connexité à la Toile, c'est-à-dire, aux services pris en charge au moyen d'un "navigateur de la Toile" *(Web browser)* (comme Firefox, Internet Explorer, Mozilla, Netscape, Lynx, ou Opera) en particulier les services qui utilisent les protocoles HTTP ou HTTPS. Les autres services ne sont généralement pas pris en charge. En particulier, il peut ne pas y avoir d'accès à la messagerie électronique POP3 ou IMAP4, aux tunnels chiffrés ou autres mécanismes de VPN.
Les adresses utilisées peuvent être privées et/ou non accessibles mondialement. Elles sont généralement dynamiques (voir la discussion d'adresse dynamique à la Section 3 pour des précisions sur cette terminologie et ses implications) et de relativement courte durée (heures ou jours plutôt que mois ou années). Ces adresses sont souvent annoncées comme "dynamiques" à ceux qui tiennent les listes des numéros de téléphone ou des adresses dynamiques. Le fournisseur peut imposer un mandataire de filtrage de la Toile sur les connexions ; ce mandataire peut changer et rediriger les URL sur d'autres sites que celui originellement spécifié par l'usager ou une liaison incorporée.

Connexité de client seul, sans adresse publique :
Ce service donne l'accès à l'Internet sans prise en charge des fonctions de serveur ou de la plupart des fonctions d'homologue à homologue. L'adresse IP allouée au consommateur est dynamique et est caractéristiquement allouée à partir d'un espace d'adresses non public. Les fonctions de serveurs et d'homologue à homologue ne sont généralement pas prises en charge par les systèmes de traduction d'adresse réseau (NAT) qui sont exigés par l'utilisation d'adresses privées. (La catégorisation plus précise des types de NAT donnée dans la [RFC2663] est assez divergente de celle du présent document, mais elle peut être fournie au titre des termes supplémentaires, comme décrit à la Section 4.) Les mandataires de filtrage de la Toile sont communs dans ce type de service, et le fournisseur DEVRAIT indiquer si il en est un de présent ou non.

Client seul, adresse publique :
Ce service donne accès à l'Internet sans prise en charge de fonctions de serveurs ou de la plupart des fonctions d'homologue à homologue. L'adresse IP allouée au consommateur est dans l'espace des adresses publiques. Elle est généralement nominalement dynamique ou autrement soumise à changement, mais elle peut ne pas changer pendant tout un mois. La plupart des VPN et connexions similaires vont fonctionner avec ce service. Le fournisseur peut interdire l'utilisation des fonctions de serveur par des restrictions légales (contractuelles) ou en filtrant les tentatives de connexion entrantes. Le filtrage des mandataires de la Toile est peu courant dans ce type de service, et les fournisseurs DEVRAIENT indiquer si il en est un présent.

Connexité Internet avec pare-feu
Ce service donne accès à l'Internet et prend en charge la plupart des fonctions de serveurs et d'homologue à homologue, avec (généralement) une ou plusieurs adresses publiques statiques. Il est similaire à la "pleine connexité Internet", ci-dessous, et toutes les qualifications et restrictions qui y sont décrites s'appliquent. Cependant, ce service place un "pare-feu" géré par le fournisseur entre le consommateur et l'Internet public, normalement à la demande du consommateur et pour un prix supérieur à celui des services sans pare-feu. Normalement par arrangement contractuel avec les consommateur, il peut en résulter un blocage de certains services. D'autres services peuvent être interceptés par des mandataires, des accords de filtrage de contenu, ou des passerelles d'applications. Le fournisseur DEVRAIT spécifier quels services sont bloqués, sont

interceptés, ou altérés de quelque autre façon. Dans la plupart des endroits, cet accord de service est offert en option supplémentaire, tarifée à part, de ce qui serait autrement la pleine connexité Internet. Il se distingue des modèles précédents par le fait que tout service de filtrage ou de blocage est en fin de compte effectué à la demande du client, plutôt que d'être imposé comme une restriction de service.

Pleine connexité Internet
Ce service fournit à l'usager la pleine connexité à l'Internet, avec une ou plusieurs adresses publiques statiques. Les adresses dynamiques qui ont une durée de vie assez longue pour rendre praticables des serveurs opérationnels sans entrées très dynamiques dans le DNS sont possibles, pourvu qu'elles ne soient pas caractérisées comme "dynamiques" pour les tiers.
Les mandataires filtrants de la Toile, les mandataires d'interception, les NAT, et autres restrictions imposées par le fournisseur sur les accès et le trafic d'entrée ou de sortie sont incompatibles avec ce type de service. Les serveurs sur un LAN de client connecté sont considérés comme normaux. Les seules restrictions compatibles sont les limitations de bande passante et les interdictions concernant les activités nuisibles ou illégales sur le réseau.

3. Questions et terminologie du filtrage ou de la sécurité

Comme mentionné dans l'introduction, les efforts de contrôle ou de limitation du trafic réseau condamnable ont conduit à des restrictions supplémentaires sur le comportement et les capacités des services Internet. Ce trafic condamnable peut inclure la messagerie non sollicitée de divers types (incluant les "pourriels") les vers, les virus, et leur impact, et dans certains cas, leur contenu spécifique.

En général, des restrictions significatives vont probablement se rencontrer avec la connexité à la Toile et les services d'adresses non publiques, mais certaines recommandations courantes pourraient appliquer des restrictions à tous les niveaux. Certaines de ces restrictions à la messagerie peuvent empêcher d'envoyer la messagerie sortante (sauf à travers les serveurs du FAI destinés à cet objet) peuvent empêcher l'utilisation des adresses de retour du choix de l'utilisateur, et peuvent même empêcher l'accès aux répertoires de messagerie (autres que ceux fournis par le FAI) par des protocoles d'accès distant tels que POP3 ou IMAP4. Parce que les utilisateurs peuvent avoir des raisons légitimes d'accéder à des services de fichiers à distance, à des serveurs de soumission de messagerie à distance (ou, au moins, à utiliser leurs adresse de messagerie électronique préférée à partir de localisations multiples) et d'accéder à des répertoires de messagerie distants (là encore, une presque exigence si une seule adresse doit être utilisée) il est important que les fournisseurs divulguent les services qu'ils rendent disponibles et les filtres et conditions qu'ils imposent.

Plusieurs questions clés du filtrage de la messagerie électronique sont d'une importance particulière.

Adresses dynamiques :
Un certain nombre de systèmes, incluant plusieurs systèmes de "liste noire", se fondent sur l'hypothèse que la plupart des messages électroniques non désirés proviennent de systèmes qui ont des adresses dynamiques, en particulier des systèmes de diffusion par des lignes téléphoniques et résidentiels. Par conséquent, ils tentent d'empêcher les adresses d'être utilisées pour envoyer de la messagerie, ou d'effectuer d'autres services, sauf par l'intermédiaire des systèmes du fournisseur qui sont destinés à cet objet.

Différentes techniques ont utilisées pour identifier les systèmes qui ont des adresses dynamiques, y compris l'annonce par le fournisseur de ces adresses aux opérateurs de liste noire, des heuristiques qui utilisent certaines gammes d'adresses, et l'inspection des noms de domaines par transposition inverse pour voir si ils contiennent des chaînes révélatrices telles que "dsl" ou "dial". Dans certains cas, l'absence d'une adresse DNS de transposition inverse est prise comme indication que l'adresse est "dynamique". (La prohibition des connexions fondée sur l'absence d'un enregistrement DNS de transposition inverse était une technique développée pour les serveurs FTP il y a bien longtemps ; elle s'est révélée avoir un taux d'échec très important , interdisant à la fois des tentatives de connexion légitimes et échouant à empêcher les tentatives illégitimes). Les fournisseurs de service DEVRAIENT décrire ce qu'ils font dans ce domaine pour le trafic de messages entrant et sortant, et les utilisateurs devraient savoir que, si une adresse est annoncée comme "dynamique", il peut être impossible de l'utiliser pour envoyer de la messagerie à un système arbitraire même si la pleine connexité Internet est par ailleurs fournie.

Adresses non publiques et NAT :
Les systèmes de NAT qui sont utilisés pour faire la transposition entre les espaces d'adresses privées et publiques peuvent prendre en charge des connexions à des systèmes de messagerie distants pour les messages sortants et entrants, mais les conditions d'abonnement interdisent souvent l'utilisation de systèmes non fournis par le fournisseur de la connexité et interdisent le fonctionnement de "serveurs" (normalement non définis avec précision) sur la connexion du client.

Filtrage de l'accès de sortie par le fournisseur :
Une autre technique courante implique de bloquer les connexions à des serveurs qui sont hors du contrôle de l'opérateur en bloquant les "accès" TCP qui sont couramment utilisés pour les fonctions de messagerie. Les différents opérateurs ont des théories différentes sur cette question. Certains interdisent à leurs clients d'accéder aux serveurs SMTP externes pour la soumission des messages, mais leur permettent d'utiliser le protocole de soumission de messages ([RFC2663]) avec l'authentification de l'envoyeur. D'autres essayent de bloquer tous les protocoles en rapport avec la messagerie sortante, incluant les protocoles de restitution à distance ; cependant, ceci est moins courant avec les services d'adresses publiques qu'avec ceux qui dépendent d'adresses privées et de NAT. Si ce type de filtrage est présent, en particulier avec les services "Client seul, adresse publique" et "Pleine connexité Internet", le fournisseur DOIT indiquer ce fait (voir aussi la Section 4).

D'autres encore peuvent détourner (réacheminer) le trafic de messagerie électronique sortant sur leurs propres serveurs, selon la théorie que cela éliminerait le besoin de reconfigurer les appareils portables lorsque ils se connectent à partir d'une localisation réseau différente. Là encore, de telles dérivations DOIVENT être révélées, en particulier parce que cela peut avoir des implications significatives sur la sécurité et la confidentialité.

Plus généralement, les filtres qui bloquent certains messages ou tous à l'envoi (ou à la soumission) à des systèmes distants (autres que via les serveurs pris en charge par le fournisseur) ou qui tentent de dérouter ce trafic sur leurs propres serveurs, sont, comme on l'a exposé ci-dessus, en train de devenir courants et DEVRAIENT être déconseillés.

4. Terminologie supplémentaire

Ces termes supplémentaires, bien qu'ils ne soient pas aussi basiques pour la compréhension d'une offre de service comme ceux identifiés ci-dessus, sont mentionnés comme des informations supplémentaires qu'un fournisseur de service pourrait choisir de fournir pour compléter ces définitions générales. Un client potentiel peut utiliser ceux qui relèvent de la construction d'une liste de questions spécifiques à poser, comme par exemple :

Prise en charge de version :
Le service inclut il la prise en charge de seulement IPv4, de IPv4 et IPv6 ou seulement IPv6 ?

Prise en charge de l'authentification :
Quels mécanismes techniques sont utilisés par le service pour établir et éventuellement authentifier les connexions ? Des exemples pourraient inclure des interceptions de DHCP, PPP, RADIUS, ou HTTP non authentifiées.

VPN et tunnels. :
IPsec est-il bloqué ou permis ? D'autres techniques de tunnelage à la couche IP ou en dessous, comme L2TP, sont elles permises ? Y a t-il une tentative de blocages des mécanismes de tunnel de couche applications comme SSH ?

Prise en charge de la diffusion groupée :
L'appareil de l'utilisateur a t-il accès aux paquets et services en diffusion groupée ?

Prise en charge de l'accès au DNS :
Les utilisateurs sont ils obligés d'utiliser les serveurs DNS fournis par le fournisseur de service, ou est-il permis aux interrogations au DNS d'atteindre des serveurs arbitraires ?

Services en rapport avec IP :
Les messages ICMP de et vers les sites d'usager final sont ils généralement bloqués ou permis ? Les fonctions spécifiques comme ping et traceroute sont elles bloquées et si oui, à quel point du réseau ?

Prise en charge de l'itinérance :
Le service inclut-il intentionnellement la prise en charge de l'itinérance IP, et si oui, comment est-elle définie ? Pour les connexions "haut débit", un arrangement de numérotation est il fourni pour la sauvegarde ou le déplacement de l'utilisateur ? Si il y en a un, cet arrangement a t-il un plein accès aux boîtes aux lettres de messagerie, etc.

Services d'applications fournis :
Les services de messagerie électronique et/ou d'hébergement de la Toile sont ils fournis au titre du service, et sur quelle base ? Une liste de services de messagerie électrique devrait identifier si POP3, IMAP4, ou l'accès à la Toile sont fournis et dans quelles combinaisons, et quels types de services d'authentification et de confidentialité sont pris en charge ou exigés pour chacun.

Utilisation et blocage de services d'applications sortants :

Le service bloque t-il l'utilisation de SMTP ou la soumission de messages aux serveurs autres que ceux du fournisseur ou intercepte t-il de telles soumissions et les achemine t-il à ses serveurs ? Ses serveurs interdisent ils à l'usager de se servir de ses noms de domaine sur la messagerie électronique sortante ? (Spécifiquement pour la messagerie électronique, voir aussi la Section 3.) La commande PASV de FTP est elle prise en charge ou bloquée ? Des blocages ou interceptions sont ils imposés aux autres mécanismes de partage de fichier ou de transfert de fichier, aux applications de conférence, ou aux services d'applications privées ? Plus généralement, le fournisseur devrait identifier toutes les actions du service pour bloquer, interdire, ou altérer la destination des services d'application, l'utilisation en sortie (c'est-à-dire, l'utilisation de services non fournis par l'opérateur ou sur les réseau de l'opérateur).

Blocage de services d'applications entrants :

En plus des questions soulevées par l'espace d'adresses dynamique ou privé (lorsque présent) le service prend il d'autres mesures qui restreignent spécifiquement les connexions qui peuvent être faites avec des équipements gérés par le consommateur ? Spécifiquement, les connexions entrantes SMTP, HTTP ou HTTPS, FTP, ou d'homologue à homologue diverses ou autres (incluant éventuellement des applications non spécifiquement reconnues par le fournisseur) sont elles interdites, et si oui, lesquelles ?

Filtrage de contenu d'application :

Le service devrait déclarer si il fournit des filtrages ou protections contre les attaques de vers ou de déni de service contre ses clients, le filtrage des virus et des pourriels pour ses services de messagerie (si il en est) le filtrage non discrétionnaire ou "contrôle parental" des contenus, et ainsi de suite.

Écoutes et interception :

Le service DEVRAIT indiquer si le trafic qui passe à travers lui est soumis à des interceptions légales, et si l'opérateur fera des tentatives actives pour informer l'usager de telles interceptions lorsque une telle information est légale Des questions analogues peuvent être posées pour les données de trafic qui sont mémorisées pour une éventuelle utilisation pour l'application de la loi.

5. Considérations pour la sécurité

Le présent document est sur la terminologie, et pas sur les protocoles, de sorte qu'il ne soulève aucune question particulière de sécurité. Cependant, si le type de terminologie qui est proposé est largement adopté, il peut devenir plus facile d'identifier les attentes des hôtes particuliers, des LAN et autres types de connexions en matière de sécurité.

6. Remerciements

Le présent document a été inspiré par une conversation par messagerie électronique avec Vernon Schryver, Paul Vixie, et Nathaniel Bornstein. Bien qu'il y ait eu des propositions pour produire de telles définitions depuis de nombreuses années, cette conversation a convaincu l'auteur qu'il était finalement temps de se mettre au travail pour voir si l'IETF pourrait faire avancer ce projet. Harald Alvestrand, Brian Carpenter, George Michaelson, Vernon Schryver, et d'autres ont fait plusieurs suggestions sur le projet initial qui ont amené à des précisions dans la seconde version, et Stephane Bortzmeyer, Brian Carpenter, Tony Finch, Susan Harris, David Kessens, Pekka Savola, et Vernon Schryver ont fait plusieurs suggestions utiles qui ont été incorporées dans les versions suivantes. Susan Harris a aussi apporté à la pénultième version un soin de relecture exceptionnel, qui est très apprécié, comme le sont les suggestions rédactionnelles de l'éditeur des RFC.

7. Références pour information

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2476] R. Gellens et J. Klensin, "Soumission de message", décembre 1998.

[RFC2663] P. Srisureshet M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau (NAT) IP", , août 1999.

Adresse de l'auteur

John C Klensin
1770 Massachusetts Ave, #322
Cambridge, MA 02140
USA
téléphone : +1 617 491 5735
mél : john-ietf@jck.com

Déclaration complète de droits de reproduction

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