Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2349773 A1 2001/12/08

(21) 2 349 773

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2001/05/29

(41) Mise à la disp. pub./Open to Public Insp.: 2001/12/08

(30) Priorité/Priority: 2000/06/08 (00 07 351) FR

(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 12/12, H04L 12/24

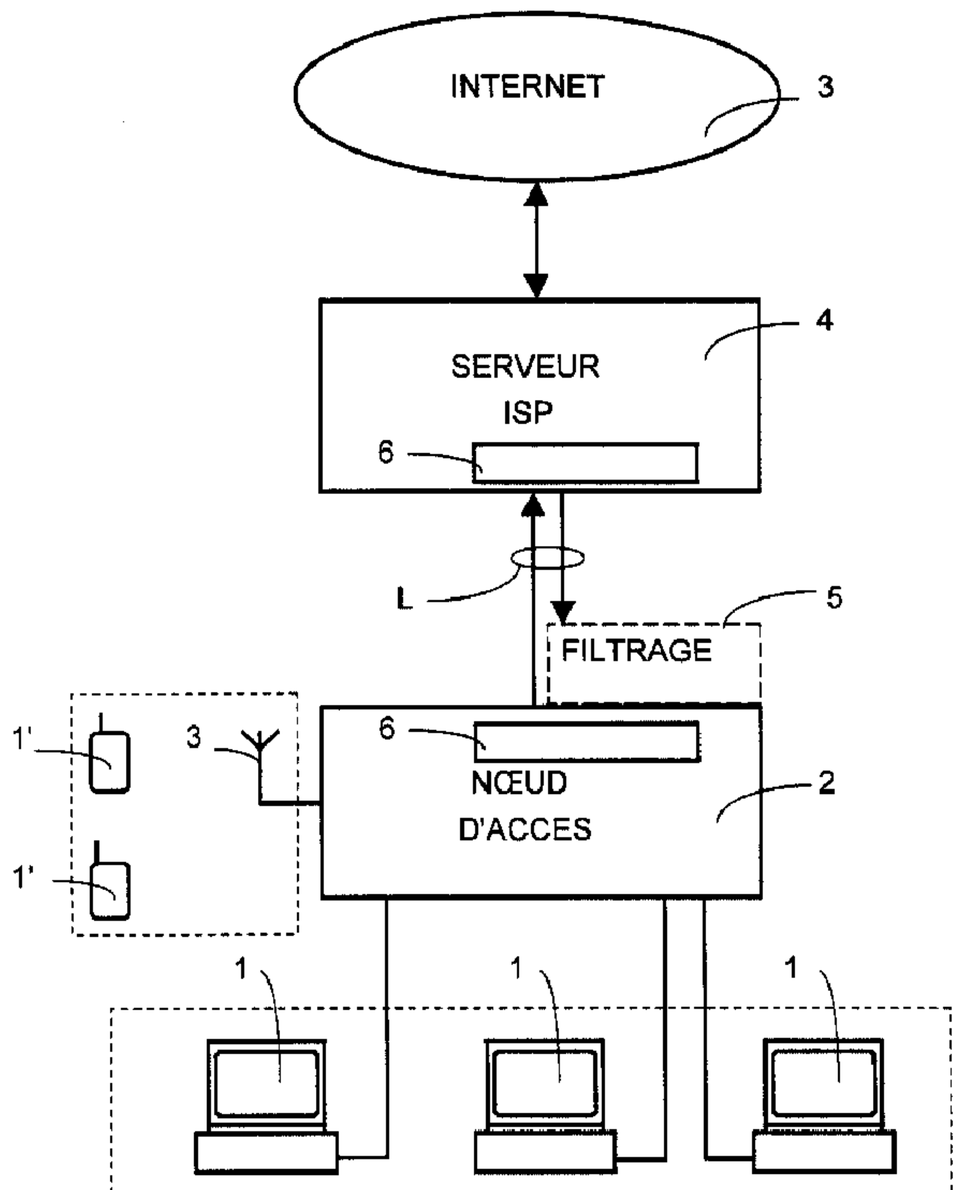
(71) Demandeur/Applicant:
ALCATEL, FR

(72) Inventeurs/Inventors:
GUIRAUTON, ALAIN, FR;
PINAULT, FRANCIS, FR

(74) Agent: ROBIC

(54) Titre : PROCEDE DESTINE A ASSURER UN CONTROLE D'ACCES POUR ET/OU VIS-A-VIS D'UTILISATEURS ACCEDANT PAR DES TERMINAUX AU RESEAU INTERNET, AU TRAVERS D'UN NOEUD D'ACCES PRIVE, ET AGENCEMENTS POUR LA MISE EN OEUVRE D'UN TEL PROCEDE

(54) Title: PROCESS TO PROVIDE ACCESS CONTROL FOR AND/OR WITH RESPECT TO USERS ACCESSING THE INTERNET FROM TERMINALS, THROUGH A PRIVATE ACCESS NODE, AND LAYOUTS FOR THE IMPLEMENTATION OF SAID PROCESS



(57) Abrégé/Abstract:
Procédé destiné à assurer un contrôle d'accès pour et/ou vis-à-vis d'utilisateurs qui accèdent à un réseau informatique (3) permettant des échanges d'informations, notamment au réseau Internet, au moyen de terminaux (1 ou l'), par l'intermédiaire

(21) 2 349 773

(13) A1

(57) Abrégé(suite)/Abstract(continued):
d'un noeud d'accès (2), partagé ou propre à une organisation, par exemple un autocommutateur d'une entreprise, auquel les terminaux se raccordent pour leurs accès au réseau informatique, via un serveur (4). Ce procédé prévoit un stockage temporaire, à des fins de filtrage aval, du flot de données multimédia reçues du réseau informatique à destination d'un terminal d'utilisateur, suite à une requête d'accès formulée à partir de ce terminal. Le filtrage aval est notamment réalisé par l'intermédiaire d'un agencement (5) pour autoriser ou bloquer la transmission de ce flot vers le terminal en fonction de critères déterminés, indépendants du terminal et du fournisseur d'accès.

ABREGE

Procédé destiné à assurer un contrôle d'accès pour et/ou vis-à-vis d'utilisateurs qui accèdent à un réseau informatique (3) permettant des échanges d'informations, notamment au réseau Internet, au moyen de terminaux (1 ou 1'), par l'intermédiaire d'un nœud d'accès (2), partagé ou propre à une organisation, par exemple un autocommutateur d'une entreprise, auquel les terminaux se raccordent pour leurs accès au réseau informatique, via un serveur (4).
Ce procédé prévoit un stockage temporaire, à des fins de filtrage aval, du flot de données multimédia reçues du réseau informatique à destination d'un terminal d'utilisateur, suite à une requête d'accès formulée à partir de ce terminal. Le filtrage aval est notamment réalisé par l'intermédiaire d'un agencement (5) pour autoriser ou bloquer la transmission de ce flot vers le terminal en fonction de critères déterminés, indépendants du terminal et du fournisseur d'accès.

Procédé destiné à assurer un contrôle d'accès pour et/ou vis-à-vis d'utilisateurs accédant par des terminaux au réseau Internet, au travers d'un nœud d'accès privé, et agencements pour la mise en œuvre d'un tel procédé

L'invention a pour objet un procédé destiné à assurer un contrôle d'accès pour et/ou vis-à-vis d'utilisateurs qui accèdent à un réseau informatique, tel que notamment, le réseau Internet, par l'intermédiaire d'un nœud d'accès privé, tel qu'un autocommutateur d'une entreprise. Elle concerne aussi divers agencements organisés pour permettre la mise en œuvre du procédé selon l'invention.

D'une manière plus particulière, l'invention est destinée à être exploitée par des organisations et notamment des entreprises où des utilisateurs sont équipés de terminaux qui leur permettent d'accéder à un réseau informatique, et en particulier à un réseau informatique externe à l'organisation dont ils dépendent, tel le réseau Internet, cet accès s'effectuant par l'intermédiaire d'un nœud d'accès privé, au moins partiellement réservé à cette organisation.

Tel est par exemple le cas, lorsqu'une organisation dispose d'une structure interne de communications, et par exemple d'un réseau de communication, câblé ou non, incluant au moins un nœud d'accès, tel que défini ci-dessus, par l'intermédiaire duquel il est prévu que s'effectuent les accès des utilisateurs qui sont réalisés à partir de terminaux propres à l'organisation. Ce nœud d'accès est, par exemple, un autocommutateur (PABX) et en particulier un PABX multimédia dont dispose une organisation pour ses communications, ou encore une structure privée, de type passerelle, d'accès pour un réseau local, de type LAN.

Pour différentes raisons et en particulier pour des raisons économiques, il est important pour une organisation de pouvoir vérifier que les possibilités d'accès qu'elle offre à un réseau informatique et en particulier au réseau Internet, sont exploitées d'une manière appropriée lui évitant en particulier des coûts ou surcoûts qu'elle n'a pas vocation de supporter, ainsi que des risques matériels ou financiers injustifiés.

Une solution de contrôle d'accès connue, dérivant de ce qui était antérieurement prévu en matière de téléphonie, consiste à interdire certains accès aux utilisateurs, lorsqu'ils exploitent des terminaux propres à une organisation. Il est ainsi possible d'empêcher l'accès à certains sites d'un

réseau informatique ou à certains types d'information à partir des terminaux d'une organisation, en agissant aux moyens de filtres filtrant les adresses des sites, par exemple au niveau d'une unité rempart ou "firewall" située entre le réseau informatique et le nœud d'accès exploité par les terminaux pour accéder à ce réseau informatique.

Toutefois cette solution n'est pas vraiment satisfaisante, dans la mesure où elle implique une mise à jour permanente des adresses interdites, ce qui est difficile à réaliser, lorsque les accès sont dirigés vers des sites d'un réseau évoluant en permanence comme l'est le réseau Internet, connaissant les possibilités de ré-aiguillage entre sites qu'autorise ce genre de réseau. De plus, le filtrage préalable ne s'effectue que dans des conditions prédéterminées et reste sans effet autrement, ce qui implique qu'il soit régulièrement réactualisé pour être capable de s'adapter aux évolutions techniques.

Certains fichiers multimédia peuvent être téléchargés moyennant un paiement, donnant des droits pour une utilisation limitée. Il est connu d'identifier de tels fichiers multimédia par une signature, appelée signature SDMI, permettant contrôler l'utilisation de ces fichiers après leur téléchargement. Un membre d'une organisation peut outrepasser ses droits d'utilisation, et la responsabilité de cette organisation peut donc être engagée. Une organisation encourt donc des risques lorsqu'elle reçoit de tels fichiers, suite à des demandes d'accès effectuées par l'intermédiaire des terminaux qui lui appartiennent.

Le document **US 5.987.606** décrit un dispositif de filtrage situé dans le serveur d'un fournisseur de service Internet. Il permet de détecter des mots interdits ou des phrases interdites, prédéterminés pour chaque client susceptible de se connecter à Internet via ce fournisseur de services. Cette solution est bien adaptée pour des particuliers, mais n'est pas bien adaptée pour une organisation.

L'invention propose donc un procédé destiné à assurer un contrôle d'accès pour et/ou vis-à-vis d'utilisateurs qui accèdent à un réseau informatique permettant des échanges d'informations, tel que notamment, le réseau Internet, au moyen de terminaux, par l'intermédiaire d'un nœud d'accès privé, partagé ou propre à une organisation, telle qu'une entreprise, auquel les terminaux se raccordent pour leurs accès au réseau informatique, via un serveur d'accès.

Selon une caractéristique de l'invention, ce procédé prévoit un stockage temporaire, à des fins de filtrage aval, du flot de données multimédia reçues du réseau informatique à destination d'un terminal d'utilisateur suite à une requête d'accès formulée à partir de ce terminal, le filtrage aval étant réalisé par l'intermédiaire d'un agencement permettant d'autoriser ou de bloquer la transmission de ce flot vers le terminal en fonction de critères déterminés appliqués au flot de données reçu, au niveau du nœud d'accès privé.

Le procédé ainsi caractérisé permet à une organisation de filtrer tout ce qui entre dans le réseau informatique de l'organisation, indépendamment du fournisseur ou des fournisseurs de service Internet, puisque le filtrage est réalisé au niveau du nœud d'accès privé. D'autre part, il est possible de définir des critères de filtrage propres à une organisation mais indépendants de l'idendité des membres de cette organisation.

Selon l'invention, le procédé prévoit que les données reçues du réseau informatique extérieur sont temporairement stockées avant d'être transmises ou non au terminal utilisateur, selon les résultats d'une analyse.

Selon l'invention, le procédé prévoit de conserver les données reçues du réseau informatique qui ne sont pas transmises, après une analyse ayant conduit à une décision de non transmission à l'utilisateur, pour pouvoir comparer ces données à des données d'un flot ultérieur, de manière à accélérer la prise de décision, en cas d'identité des données entre flots pour un ensemble déterminé de données, sans avoir à recourir à une analyse correspondant à celle qui avait conduit à ce que les données conservées ne soient pas transmises.

Selon une forme de mise en œuvre du procédé selon l'invention, il est prévu que le transfert de données reçues du réseau informatique à destination d'un terminal d'utilisateur est temporairement retardé au niveau de moyens de stockage temporaire, jusqu'à détermination de la conformité de ce qui a été reçu par rapport à des normes déterminées, avant transmission au terminal si la conformité est constatée.

Il est aussi prévu de conserver les données temporairement retardées relatives à un flot, qui sont stockées en phase de détermination de conformité, pour permettre un contrôle complémentaire en cas de non-conformité, cette conservation étant réalisée soit pour les données reçues, à détection de la non-conformité, le flot qui les transmet depuis le réseau informatique étant

alors interrompu, soit éventuellement pour l'ensemble de données reçues sans que soit interrompu le flot.

Il est également prévu de conserver les données pour lesquelles une non-conformité a été détectée dans un flot reçu et/ou l'origine de ces données, de manière à permettre une interruption d'un flot de données ultérieurement reçu avant analyse complète des données que ce flot transmet, lorsque de telles données et/ou une telle origine sont à nouveau détectées.

Selon l'invention, le procédé prévoit une comptabilisation, à des fins de contrôle, sur la base d'un contenu déterminé d'informations constitué par une combinaison caractéristique de données, lorsqu'un tel contenu est présent dans les données qui sont temporairement stockées après avoir été reçues du réseau informatique dans le cadre d'un ou de plusieurs flots destinés chacun à un terminal déterminé.

Selon une autre forme de mise en œuvre du procédé selon l'invention, il est prévu une analyse de signatures pour permettre de bloquer, au moins temporairement, la transmission de données reçues du réseau à destination d'un terminal d'un utilisateur, lorsque ces données incorporent une signature caractéristique de signalisation de droits restrictifs.

Il est aussi prévu une analyse de type recherche d'identifiant au niveau des données reçues à destination d'un terminal d'un utilisateur, de manière à autoriser la transmission de ces données à ce terminal, lorsqu'un ou plusieurs identifiants déterminés sont trouvés parmi les données reçues qui sont destinées à ce terminal.

L'invention propose aussi un agencement destiné à assurer un contrôle d'accès pour et/ou vis-à-vis d'utilisateurs qui accèdent à un réseau informatique permettant des échanges d'informations, notamment au réseau Internet, au moyen de terminaux, par l'intermédiaire d'un nœud d'accès privé, partagé ou propre à une organisation, telle qu'une entreprise, auquel les terminaux se raccordent pour leurs accès au réseau informatique, via un fournisseur de services.

Selon l'invention, cet agencement comporte des moyens matériels et/ou logiciels, notamment de type produits logiciels, organisés pour permettre la mise en œuvre du procédé, tel que défini ci-dessus.

Selon une forme particulière de réalisation, l'agencement, selon l'invention, est un équipement monté en amont ou en entrée d'un nœud de réseau de communication et par exemple d'un autocommutateur privé.

L'invention, ses caractéristiques et ses avantages sont précisés dans la description qui suit en liaison avec les figures évoquées ci-dessous.

La figure 1 présente un schéma de principe relatif au contrôle d'accès au réseau Internet à partir de terminaux d'utilisateurs et au travers d'un nœud d'accès privé.

La figure 2 présente un schéma d'un agencement de contrôle d'accès, selon l'invention.

Le procédé de contrôle d'accès, selon l'invention est destiné à être mis en œuvre dans le cadre d'un système où des terminaux sont mis à disposition d'utilisateurs au niveau d'une organisation, telle qu'une entreprise, afin de leur permettre, en particulier, d'accéder à un réseau informatique, tel qu'Internet permettant des échanges d'informations diverses, telles que des informations multimédia se transmettant sous forme de données numériques. Il est plus particulièrement prévu que l'accès des terminaux au réseau informatique s'effectue par l'intermédiaire d'un nœud d'accès privé relié au réseau par l'intermédiaire d'au moins un fournisseur de service, qui est couramment désigné par l'acronyme ISP (Internet Service Provider) dans le cas d'un réseau Internet.

Ceci est schématisé au niveau de la figure 1 où sont symbolisés deux types de terminaux susceptibles d'être mis à disposition des utilisateurs dans une organisation déterminée. Les terminaux 1 sont, par exemple, des ordinateurs reliés par des liaisons filaires à un nœud d'accès 2, les terminaux 1' sont, par exemple, des terminaux informatiques communiquant par voie radio avec le nœud d'accès 2, alors doté de moyens d'émission-réception, ici symbolisés par une antenne 3.

Le nœud d'accès 2 est susceptible d'être constitué de différentes manières en fonction des besoins. Quelle que soit l'option choisie, il dispose d'une fonction de routage pour permettre aux terminaux, tels que 1 ou 1', qu'utilisent les utilisateurs pour accéder à un réseau informatique 3, ici considéré comme étant le réseau Internet. Il est relié à un serveur 4 d'un fournisseur de services de ce réseau, tel un serveur ISP par l'intermédiaire d'une liaison de transmission L.

Le nœud d'accès 2 est, par exemple, un commutateur numérique, du type PABX, exploité pour la desserte de terminaux filaires et/ou éventuellement radio d'une installation de télécommunications privée propre à une organisation, telle qu'une société, ce commutateur étant doté de moyens de routage lui permettant de communiquer en mode paquet avec un serveur ISP

d'un fournisseur de services Internet. Ce serveur agit en tant qu'intermédiaire vis-à-vis des terminaux susceptibles d'accéder au réseau Internet que comporte l'installation de télécommunications. Le nœud d'accès 2 peut aussi être une unité de type passerelle, dotée d'une fonction de routage et agissant en tant qu'interface vis-à-vis de terminaux, susceptibles d'accéder au réseau Internet, qui sont comportés par un réseau local, tel que par exemple un réseau LAN (Local area network).

Selon l'invention, il est prévu un agencement de filtrage d'amont ou d'entrée 5 destiné à contrôler les données transmises en retour par le réseau informatique 3, via le serveur 4, à destination de tout terminal 1 ou 1' ayant effectué une demande d'accès au réseau 3. Suivant les configurations prévues en liaison avec les types d'exploitation possibles, cet agencement de filtrage 5 est susceptible d'être un équipement localisé au niveau du nœud d'accès 2 ou du serveur 4, voire de constituer une unité séparée. Quel que soit le cas, il est positionné en amont ou en entrée pour pouvoir intercepter toutes les informations, à destination des terminaux que dessert le nœud d'accès, qui sont transmises depuis le réseau informatique 3, via le serveur 4, suite aux demandes d'accès au réseau effectuées par ces terminaux, comme symbolisé sur la figure 1.

L'agencement de filtrage 5 est supposé plus ou moins directement lié aux logiques programmées de commande 6 d'au moins l'un des sous-ensembles que constituent le nœud d'accès 2 et le serveur 4, dans l'un ou l'autre desquels il peut éventuellement être inclus. Comme indiqué plus haut un nœud d'accès 2, privé, peut être un nœud propre à une organisation déterminée qui l'exploite pour ses besoins, ce peut aussi être un nœud partagé par plusieurs organisations et par exemple mise à disposition par une entreprise spécialisée.

Le procédé de contrôle d'accès, selon l'invention, est prévu pour n'intervenir qu'au niveau du trafic en retour destiné aux terminaux du nœud d'accès 2 où il s'applique, étant entendu qu'il peut bien entendu être prévu pour agir au niveau de plus d'un nœud d'accès et en liaison avec plus d'un serveur au profit d'une même organisation, telle qu'envisagée plus haut, l'exemple schématique donné en liaison avec la figure 1 ne devant pas être considéré comme limitatif.

Ce procédé de contrôle n'intervient pas lors de l'établissement d'une connexion d'un terminal 1 ou 1', avec le serveur 4 d'un fournisseur de services et via le nœud d'accès 2, dans le cadre d'une demande d'accès au réseau

informatique 3 effectuée par ce terminal. Comme connu, la logique programmée de commande du nœud d'accès comporte des moyens de stockage d'information lui permettant de conserver les informations qui sont nécessaires à la fonction de routage qu'elle comporte pour diriger le flot de données provenant du réseau informatique, suite à une demande d'accès qu'un terminal a effectué. L'agencement permettant la mise en œuvre du procédé, selon l'invention, peut éventuellement être associé à un dispositif rempart, de type "firewall" permettant d'interdire l'envoi de requêtes déterminées par les terminaux à destination du réseau informatique et de bloquer l'accès de données provenant de sites déterminés et/ou d'un type prédéterminé.

Selon l'invention, il est prévu qu'un stockage temporaire des données, transmises depuis le réseau informatique vers un terminal, soit effectué avant transmission de ces informations au terminal. Comme indiqué plus haut, ce stockage temporaire peut s'effectuer à différents niveaux de l'ensemble incluant le ou les serveur(s) 4 et le nœud 2 de desserte du terminal 1 ou 1' considéré.

Dans l'exemple schématique de réalisation illustré sur la figure 2, il est prévu un sous-ensemble de stockage temporaire de données 7 relié à la liaison de transmission L au niveau du nœud d'accès 2 qui reçoit les données parvenant du réseau informatique 3, par cette liaison L, à destination des terminaux alors connectés à ce réseau. Comme supposé ci-dessus, ce sous-ensemble de stockage 7 peut éventuellement être positionné au niveau du serveur par l'intermédiaire duquel les données provenant du réseau sont fournies au nœud d'accès, notamment si tous les accès à partir des terminaux desservis par le nœud s'effectuent au travers du même serveur. Les données multimédias reçus par flots du réseau informatique par l'intermédiaire de la liaison L transitent par le sous-ensemble de stockage temporaire 7 avant d'être transmises via une interface de distribution 8 aux terminaux qui en sont les destinataires. Ce dispositif de stockage temporaire est par exemple constitué d'une ou de plusieurs unités de stockage de type disque dur.

Un processus de filtrage est alors réalisé, par l'intermédiaire d'une logique de filtrage et d'analyse, au niveau des données propres à chacun des flots reçus qui sont temporairement présentes dans le dispositif de stockage 7. Cette logique est ici supposée incluse dans la logique de commande 6 qui contrôle le nœud 2 et, en particulier, l'interface de distribution 8 et l'interface de concentration 9 permettant de regrouper les flots de données émanant des

terminaux à destination du serveur pour transmission via la liaison. Les filtrages réalisés peuvent être spécifiquement adaptés aux besoins d'une organisation cliente et/ou exploitante pour lui permettre de contrôler l'exploitation des moyens d'accès au réseau informatique 1 qu'elle met à disposition des utilisateurs, par l'intermédiaire des terminaux qu'elle leur attribue.

Suite à une demande d'accès au réseau informatique librement effectuée par un utilisateur au moyen d'un terminal et au travers d'un nœud d'accès équipé d'un agencement de contrôle prévu pour permettre la mise en œuvre du procédé, selon l'invention, il est donc effectué un travail d'analyse sur le flot de données qui est reçu à destination du terminal utilisé par l'utilisateur, au niveau du dispositif de stockage temporaire 7 où ce flot est envoyé. Les moyens d'analyse et de filtrage susceptibles d'être exploités sont par exemple choisis parmi les moyens déjà connus de l'homme de métier ou spécifiquement réalisés, ils permettent par exemple de rechercher un contenu déterminé d'information dans la totalité ou dans certaines parties spécifiques d'un flot reçu à destination d'un terminal. Cette recherche peut être effectuée de manière systématique ou ponctuelle au niveau d'un flot, par exemple au fil de l'eau, ou périodiquement. Elle peut aussi s'effectuer dans le cadre de configurations particulières, par exemple lorsque le nombre d'accès simultanément actifs est grand ou lorsque certains terminaux ou certaines informations reçues sont prioritaires. Le stockage temporaire de tout ou partie d'un flot reçu ne s'effectue normalement que le temps nécessaire à l'analyse, il n'est donc pas détectable par l'utilisateur dans ces conditions et en particulier lorsque les données destinées à un utilisateur constituent un ensemble dont le volume est important. En effet le temps nécessité pour l'analyse est généralement très inférieur au temps nécessaire à la transmission de cet ensemble de données depuis le réseau informatique jusqu'au nœud d'accès au travers de la liaison L, dans les conditions actuelles. Si le processus d'analyse s'avère efficace et révèle que l'un des critères de filtrage choisi se retrouve au niveau des données reçues dans le cadre d'un flot destiné à un utilisateur, une décision est prise par l'intermédiaire de la logique de commande concernée. Cette décision conduit par exemple à une décision de non transmission qui conduit à bloquer la transmission du flot vers le terminal destinataire, en particulier, s'il est craint que ce qui est reçu présente un certain danger où contient des informations dont la communication n'est pas admise, selon les critères de l'organisation cliente et/ou exploitante. Le

blocage peut s'accompagner d'une interruption du flot de données reçues, sur initiative locale, notamment en cas de données susceptibles de constituer un risque au niveau des terminaux, du nœud et/éventuellement du serveur. Un blocage peut ne pas être accompagné par une interruption du flot de données reçues, dans certains cas, en particulier, s'il existe un doute susceptible d'être levé sur la légitimité de la transmission du contenu que constituent des données reçues, à l'utilisateur qui les a requises. Les données reçues peuvent alors être temporairement stockées jusqu'à ce que l'ensemble, par exemple de type fichier, qu'elles forment soit entièrement reçu. La transmission de cet ensemble peut alors être retardée temporairement jusqu'au moment où une décision concernant la légitimité est atteinte, éventuellement après intervention humaine, et où la transmission peut, soit être effectuée vers l'utilisateur, soit définitivement bloquée. Le contrôle de légitimité s'effectue par exemple selon des normes prédéterminées applicables dans des conditions déterminées, via la logique de commande. Il est aussi prévu que dans certaines conditions et notamment en raison de priorités préétablies, la transmission de certains contenus soit retardée au profit de contenus considérés comme prioritaires, ou éventuellement qu'elle soit suspendue, sur décision locale au niveau du nœud ou du serveur, par interruption volontaire des flots exploités pour leur transmission.

Dans une forme de mise en œuvre du procédé, il est prévu de conserver des données reçues du réseau informatique qui ne sont pas transmises à un utilisateur, après une analyse ayant conduit à une décision de non transmission, de manière à pouvoir exploiter ces données pour accélérer la prise de décision si ces données sont à nouveau reçues dans un flot ultérieur, sans avoir recours à une nouvelle analyse pour ces données reçues à nouveau. Une décision peut alors être prise pour un flot nouvellement entrant en cas d'identité d'un ensemble sélectionné de données nouvellement reçues avec un ensemble déterminé de données stockées. Il est aussi prévu de conserver les informations qui sont relatives à l'origine d'un flot de données et qui figurent dans ce flot pour pouvoir également les exploiter si elles sont trouvées à nouveau dans un flot ultérieur de manière à permettre une interruption de ce flot ultérieur avant que les données qu'ils comportent ne soient entièrement analysées, si cela est justifié.

Dans une variante de mise en œuvre, il est prévu de temporairement retarder le transfert de données reçues du réseau informatique à destination d'un terminal destinataire, au niveau de moyens de stockage temporaire,

jusqu'à détermination de la conformité de ce qui a été reçu, par rapport à des normes déterminées. Il est également prévu de conserver les données qui sont stockées en phase de détermination de conformité pour un flot donné, afin de permettre un contrôle complémentaire en cas de non-conformité. Cette conservation concerne par exemple les données reçues pour un flot jusqu'au moment où la non-conformité a été détectée. Elle peut aussi être réalisée pour l'ensemble des données reçues par l'intermédiaire d'un flot, sans que ce flot ne soit interrompu.

Le contrôle de contenu qui est susceptible d'être réalisé dans le cadre du procédé de contrôle d'accès, selon l'invention, peut aussi être exploité à d'autres fins que l'autorisation de la transmission, au fil de l'eau ou avec un retard contrôlé, des données transmises du réseau informatique vers un terminal ayant établi un accès avec ce réseau par l'intermédiaire du nœud d'accès et d'un serveur. Il est par exemple possible d'effectuer un filtrage relatif à des données caractéristiques d'un contenu déterminé d'informations, par exemple un type de fichier déterminé, en particulier, à des fins de comptabilisation du nombre de fois où ce groupe de données caractéristiques d'un contenu déterminé est reçu au niveau du nœud, à des fins de contrôle de trafic et/ou encore de contrôle sur le plan des coûts, dans le cas de contenus facturés.

Il est également prévu de doter l'agencement de contrôle de moyens essentiellement logiciels lui permettant d'effectuer des opérations d'analyse de signature sur les données d'un flot reçu du réseau, de manière à pouvoir bloquer, soit temporairement, soit encore définitivement, la transmission de données à un terminal destinataire, si ces données incorporent une signature caractéristique. Comme il est connu une telle signature peut par exemple signaler l'existence de droits restrictifs concernant l'exploitation des données qu'elle accompagne. Telle est notamment le cas des signatures SDMI (Secure Digital Music Initiative) destinées à accompagner des données constituant certains fichiers multimédia.

Il est alternativement prévu de faire réaliser des opérations d'analyse à des fins de recherche d'identifiant en vue d'autoriser la transmission de données reçues du réseau informatique dans le cadre d'un flot, si ces données contiennent un ou éventuellement plusieurs identifiants déterminés. Un tel identifiant est par exemple introduit à la création d'un ensemble de données, tel un fichier, destiné à être transmis dans le but d'authentifier la source de cet ensemble. Dans la forme de réalisation envisagée ici, sa reconnaissance à la

réception, au niveau d'un agencement de contrôle d'accès selon l'invention, est utilisée pour autoriser et éventuellement déclencher la transmission de l'ensemble de données reçu qu'il accompagne, au terminal destinataire.

Comme indiqué, plus haut la mise en œuvre du procédé, selon l'invention implique la mise en œuvre de moyens matériels et logiciels appropriés agencés d'une manière adaptée à l'installation de communication qu'ils équipent. Ces moyens ne seront pas développés plus avant ici, dans la mesure où ils sont connus par ailleurs de l'homme de métier. L'agencement lui-même est par exemple constitué sous la forme d'un équipement destiné à être placé en entrée ou éventuellement en amont du nœud de réseau de communication de manière à contrôler les données qui sont fournies à ce nœud à destination des terminaux d'usager desservis par ce nœud.

REVENDICATIONS

1. Procédé destiné à assurer un contrôle d'accès pour et/ou vis-à-vis d'utilisateurs qui accèdent à un réseau informatique (3) permettant des échanges d'informations, notamment au réseau Internet, au moyen de terminaux (1 ou 1'), par l'intermédiaire d'un nœud d'accès (2) privé, partagé ou propre à une organisation, telle qu'une entreprise, auquel les terminaux se raccordent pour leurs accès au réseau informatique, via un serveur d'accès (4), caractérisé en ce qu'il prévoit un stockage temporaire à des fins de filtrage aval du flot de données multimédia reçues du réseau informatique à destination d'un terminal d'utilisateur suite à une requête d'accès formulée à partir de ce terminal, le filtrage aval étant notamment réalisé par l'intermédiaire d'un agencement (5) pour autoriser ou bloquer la transmission de ce flot vers le terminal en fonction de critères déterminés appliqués au flot de données reçu, au niveau du nœud d'accès privé.

2. Procédé, selon la revendication 1, dans lequel les données reçues du réseau informatique sont temporairement stockées avant d'être transmises ou non au terminal utilisateur, selon les résultats d'une analyse.

3. Procédé, selon la revendication 2, dans lequel il est prévu de conserver les données reçues du réseau informatique qui ne sont pas transmises, après une analyse ayant conduit à une décision de non transmission à l'utilisateur, pour pouvoir comparer ces données à des données d'un flot ultérieur, de manière à accélérer la prise de décision, en cas d'identité des données entre flots pour un ensemble déterminé de données, sans avoir à recourir à une analyse correspondant à celle qui avait conduit à ce que les données conservées ne soient pas transmises.

4. Procédé, selon l'une des revendications 1, 2, dans lequel le transfert de données reçues du réseau informatique à destination d'un terminal d'utilisateur est temporairement retardé au niveau de moyens de stockage temporaire, jusqu'à détermination de la conformité de ce qui a été reçu, par rapport à des normes déterminées, avant transmission au terminal, si la conformité est constatée.

5. Procédé, selon la revendication 4, dans lequel il est prévu de conserver les données temporairement retardées relatives à un flot, qui sont stockées en phase de détermination de conformité, pour permettre un contrôle complémentaire en cas de non-conformité, cette conservation étant

réalisée soit pour les données reçues, à détection de la non-conformité, le flot qui les transmet depuis le réseau informatique étant alors interrompu, soit éventuellement pour l'ensemble de données reçues, sans que soit interrompu le flot.

6. Procédé, selon la revendication 4, dans lequel il est prévu de conserver les données pour lesquelles une non-conformité a été détectée dans un flot reçu et/ou l'origine de ces données de manière à permettre une interruption d'un flot de données ultérieurement reçu avant analyse complète des données que ce flot transmet, lorsque de telles données et/ou une telle origine sont à nouveau détectées dans ce flot ultérieurement reçu.

7. Procédé, selon la revendication 1, dans lequel il est prévu une comptabilisation, à des fins de contrôle, sur la base d'un contenu déterminé d'informations, constitué par une combinaison caractéristique de données, lorsque ce contenu est trouvé présent dans les données qui sont temporairement stockées, après avoir été reçues du réseau informatique, par l'intermédiaire d'au moins un flot destiné à un terminal déterminé.

8. Procédé, selon la revendication 2, dans lequel il est prévu une analyse de signatures pour permettre de bloquer, au moins temporairement, la transmission de données reçues du réseau à destination d'un terminal d'un utilisateur, lorsque ces données incorporent une signature caractéristique de signalisation de droits restrictifs.

9. Procédé, selon la revendication 2, dans lequel il est prévu une analyse de type recherche d'identifiant au niveau des données reçues à destination d'un terminal d'un utilisateur, de manière à autoriser la transmission de ces données à ce terminal, lorsqu'un ou plusieurs identifiants déterminés sont trouvés parmi les données reçues qui sont destinées à ce terminal.

10. Agencement destiné à assurer un contrôle d'accès pour et/ou vis-à-vis d'utilisateurs qui accèdent à un réseau informatique permettant des échanges d'informations, notamment au réseau Internet, au moyen de terminaux, par l'intermédiaire d'un nœud d'accès privé, partagé ou propre à une organisation, telle qu'une entreprise, auquel les terminaux se raccordent pour leurs accès au réseau informatique, via un fournisseur de services, caractérisé en ce qu'il comporte des moyens matériels (7) et/ou produits logiciels organisés pour autoriser ou bloquer la transmission de

ce flot vers le terminal en fonction de critères déterminés appliqués au flot de données reçu, au niveau du nœud d'accès privé.

FIG. 1

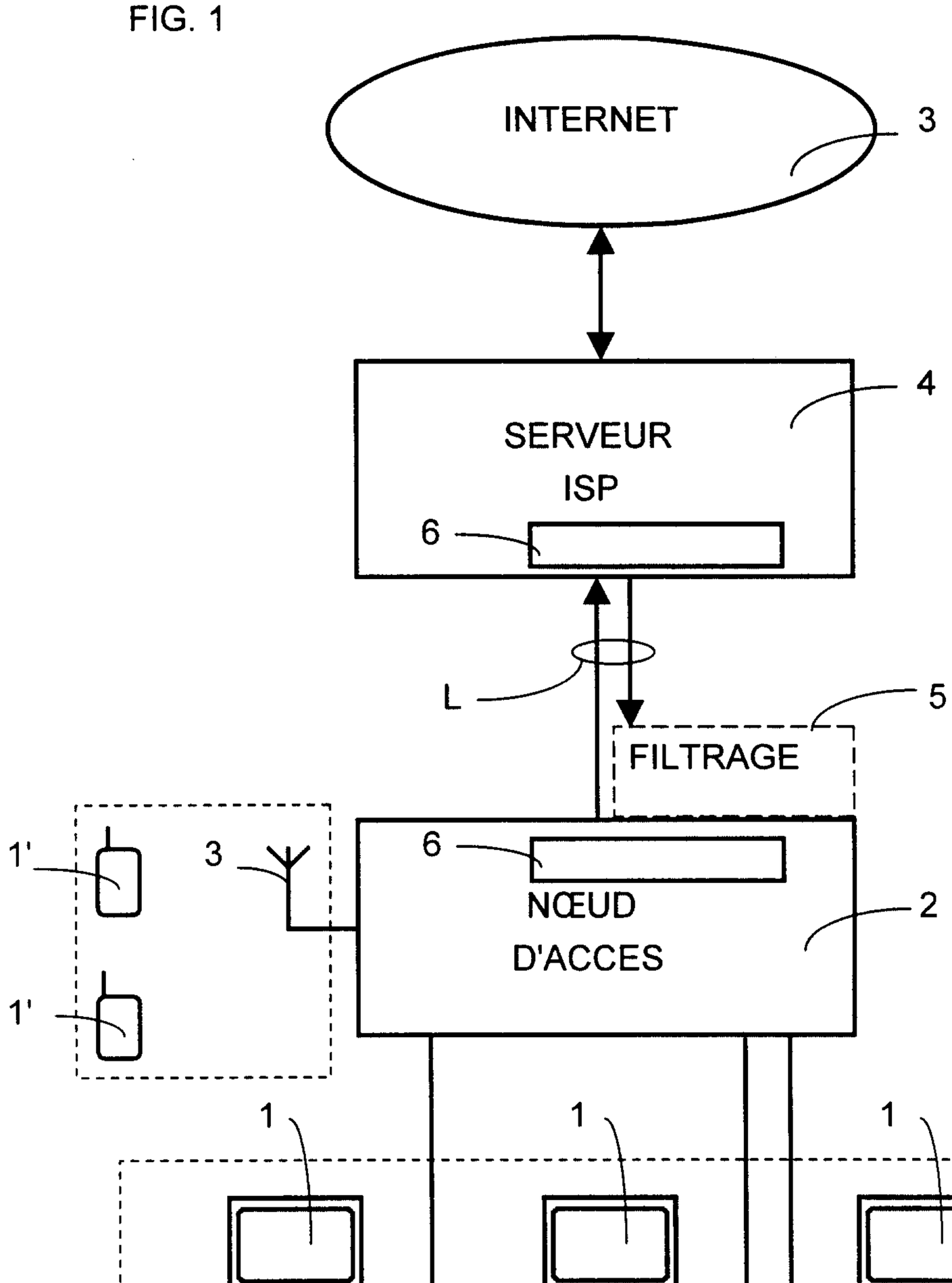
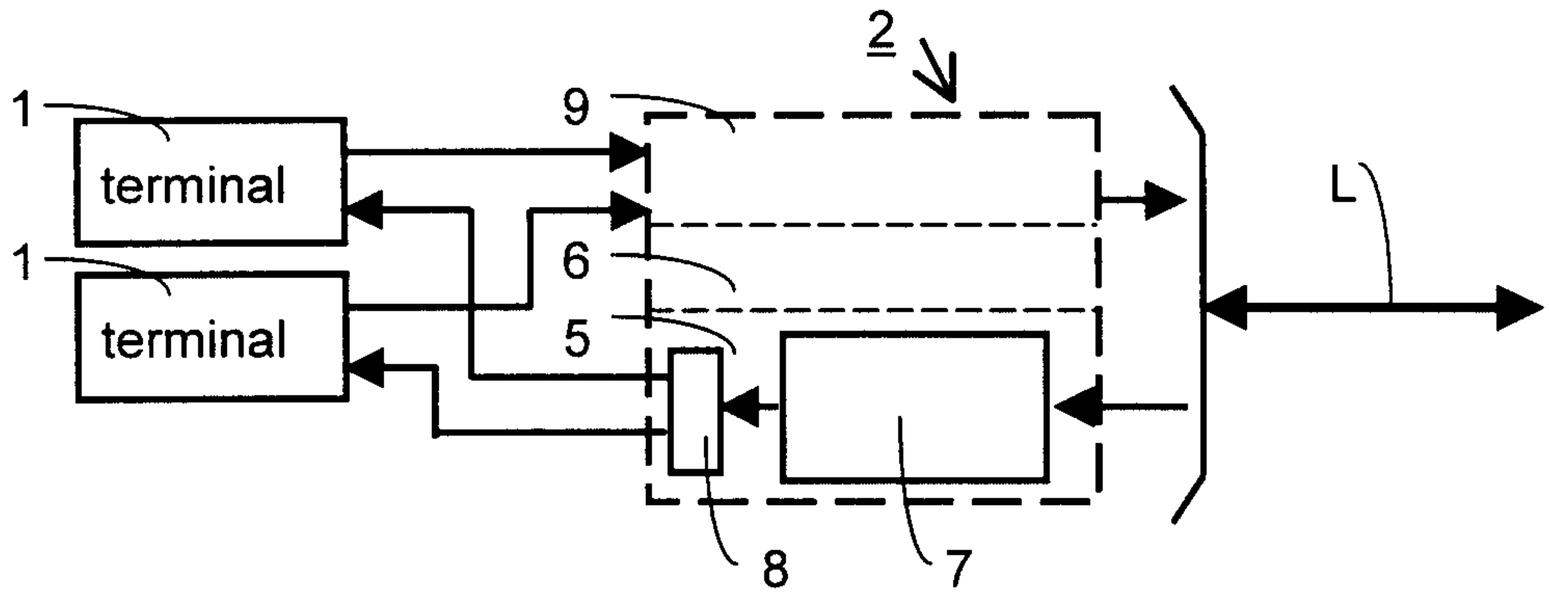
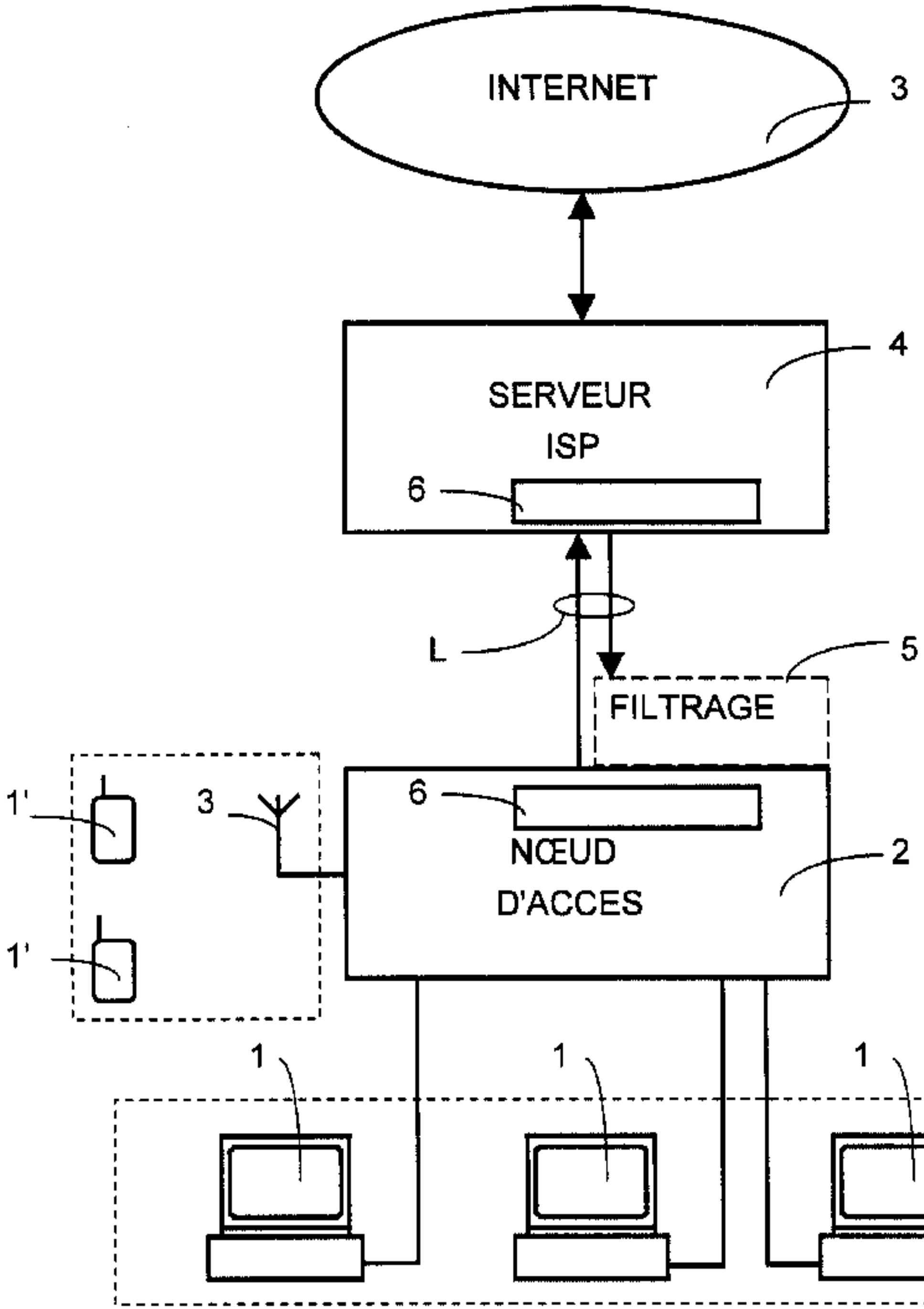

INTERNET
3
4
SERVEUR
ISP
6
L
5
FILTRAGE
1'
3
6
NŒUD
D'ACCES
2
1'
1
1
1

FIG. 2


2
1
terminal
1
terminal
9
6
5
L
8
7


INTERNET
3
4
SERVEUR
ISP
6
L
5
FILTRAGE
6
NŒUD
D'ACCES
2
1'
3
1'
1
1
1