(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 811 494**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 08986**

(51) Int Cl[7] : **H 04 L 9/32,** H 04 L 12/28

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 10.07.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 11.01.02 Bulletin 02/02.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *MERCI Société à responsabilité limitée* — FR.

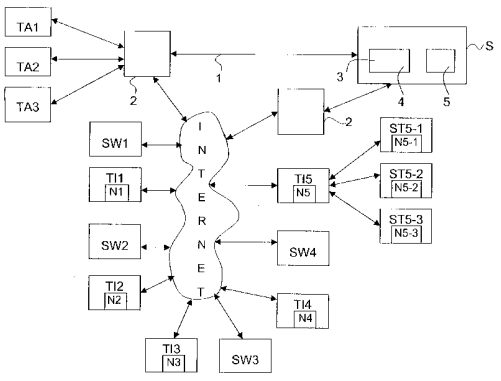
(72) **Inventeur(s) :** VERET GREGORY.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** ERNEST GUTMANN YVES PLASSERAUD SA.

(54) DISPOSITIF DE GESTION D'ACCES A DES DONNEES D'UN RESEAU ET INSTALLATION DE TELECOMMUNICATION ET PROCEDE ASSOCIES.

(57) Un dispositif de gestion de données comprend une première mémoire (3) pour stocker des identifiants de client en correspondance d'au moins un identifiant de cible, une seconde mémoire (4) pour stocker des identifiants de sites informatiques (SWj), raccordés à un réseau, en correspondance d'au moins un identifiant de cible, un serveur (S) raccordé aux première et seconde mémoires (3, 4) et au réseau, et propre à recevoir de terminaux distants (TIi) appartenant aux clients, via le réseau, des requêtes d'accès à des sites (SWj) comportant chacune un identifiant de client et au moins un identifiant de site, et à permettre au client ayant transmis une requête d'accéder, via son terminal (TIi), au contenu du site désigné par cette requête lorsque l'identifiant de cible associé dans la première mémoire (3) à l'identifiant du client, contenu dans la requête, est également associé dans la seconde mémoire (4) à l'identifiant dudit site.



FR 2 811 494 - A1

L'invention concerne la gestion de l'accès à des données contenues dans des sources d'informations accessibles via un réseau de communication. L'expression « réseau de communication » désigne ici les réseaux publics, comme par exemple Internet, et les réseaux privés, comme par exemple les réseaux Intranet.

Ces réseaux permettent à leurs utilisateurs d'accéder à de très nombreuses données par des opérations élémentaires effectuées à partir de terminaux équipés d'un « navigateur » (ou browser). On entend ici par « terminal » tout type de dispositif de (télé)communication permettant l'échange de données via un réseau de (télé)communication, comme par exemple les ordinateurs fixes ou portables, les téléphones fixes ou portables, les Assistants Personnels Numériques (APN), les décodeurs.

Cette possibilité d'accès pose de nombreux problèmes, notamment lorsque les données ne concernent, ou ne devraient concerner, que certains utilisateurs. C'est notamment le cas des données contenues dans les sites Internet à caractère pornographique ou pédophile, qui devraient être interdites d'accès aux personnes mineurs, et qui sont totalement prohibées à la population dans certains pays. Mais, cela concerne également les entreprises, dans la mesure où des employeurs peuvent souhaiter que certains de leurs employés ne puissent pas accéder à certaines données ou sources d'informations ou encore à certains sites ou domaines.

Pour tenter de remédier à ce problème, il a été proposé d'équiper les serveurs d'accès aux sites Internet de programmes informatiques de filtrage. De tels programmes recherchent, généralement, des mots clés dans les pages de données des sites (« pages « web »). Cela n'est que très partiellement efficace dans la mesure où, d'une part, certaines pages web ne contiennent que des données photographiques, et par conséquent dénuées

contiennent que des données photographiques, et par conséquent dénuées de tout texte, et d'autre part, certaines personnes malintentionnées qui connaissent les mots clés des programmes de filtrage fabriquent des pages web dénuées de tels mots clés. Par ailleurs, ces programmes autorisent implicitement l'accès aux sites qui ne sont pas répertoriés. Il a également été proposé des moteurs de recherche « sécurisés », mais du fait des liens qui existent entre de nombreux sites, il est facile de les tromper.

L'invention a pour but de remédier à cet inconvénient.

Elle propose à cet effet un dispositif de gestion des données contenues dans des sites informatiques (sites ou pages web ou bases de données ou analogue) accessibles via un réseau (public ou privé), qui comprend :

- une première mémoire dans laquelle peuvent être stockés des identifiants de client en correspondance d'au moins un identifiant de cible, et de préférence plusieurs,
- une seconde mémoire dans laquelle peuvent être stockés des identifiants de sites informatiques, raccordés au réseau, en correspondance d'au moins un identifiant de cible, et de préférence plusieurs,
- un serveur informatique raccordé aux première et seconde mémoires ainsi qu'au réseau, de manière à pouvoir recevoir de terminaux distants des requêtes d'accès à des sites, chaque requête comportant un identifiant de client et au moins un identifiant de site, et agencé pour permettre au client qui a transmis une requête d'accéder, par son terminal, au contenu du site désigné par cette requête lorsque l'identifiant de cible qui est associé dans la première mémoire à l'identifiant du client qui est contenu dans la requête est également associé dans la seconde mémoire à l'identifiant du site.

Le mot « cible » doit être ici compris dans une définition très générale. Il pourra désigner l'âge d'un client, son sexe, son lieu de résidence, sa fonction au sein d'une entreprise, par exemple. Mais, il peut

également désigner une autorisation, par exemple « droit d'accès aux informations culturelles ou sportives », ou bien une interdiction, par exemple « interdiction d'accéder aux informations boursières ou ludiques ». Par ailleurs, le mot « mémoire » doit également être compris dans une définition générale. Il pourra désigner tout type de support d'enregistrement, destiné à mémoriser des données par exemple sous la forme d'une table de correspondance, ou d'une base de données, ou encore de multiplets comportant au moins deux données telles que des identifiants. D'autre part, le mot «site » n'est pas limité à ce que l'on appelle usuellement un site « web ». Il désigne ici aussi bien une fraction d'un tel site web, tel qu'une ou plusieurs pages web, ou un groupement de sites web traitant d'un même domaine, ou des pages dites « personnelles » (du type de celles que l'on trouve dans les « forums d'informations »), ou encore tout ou partie d'une base de données (en tant que matériel permettant le stockage de données texte, image, vidéo, son et analogue). En conséquence, un « identifiant de site » est une information permettant de localiser tout ou partie d'un site web ou d'une base de données, ou différents sites web traitant d'un même domaine, et une « requête d'accès à un site » désigne toute requête d'accès à un ou plusieurs sites web ou bases de données, ou aux sites web traitant d'un même domaine. A titre d'exemple, dans le cas de sites Internet, les identifiants de site web sont, de préférence, des URL (acronyme anglais de « Uniform Resource Locator »).

De la sorte, un client ne peut accéder aux données contenues dans un site qu'à condition, tout d'abord, que ce site ait déjà été analysé, et ensuite, que la (ou les) cible(s) qui le caractérise(nt), caractérise(nt) également ce site. Par exemple, toute requête issue d'un pays dans lequel sont prohibées des données d'un certain type, par exemple pornographiques, entraînera immédiatement une interdiction d'accès à l'intégralité des sites contenant ce type de données et répertoriés dans la seconde mémoire.

Selon l'invention, seuls les sites qui ont été répertoriés peuvent faire

l'objet d'une éventuelle autorisation d'accès, après comparaison des identifiants de cible associés au site requis et au client.

Préférentiellement, dans l'hypothèse où un site désigné dans une requête n'est pas répertorié dans la seconde mémoire, il fait immédiatement l'objet d'une analyse de son contenu (s'il existe réellement) sur demande du serveur, laquelle analyse débouche sur l'association de l'identifiant du site, dans la seconde mémoire, à un ou plusieurs identifiants de cible, puis à la détermination de l'autorisation ou de l'interdiction d'accès à ce site (ou à une partie de ce site) pour le client ayant émis la requête.

Dans un mode de réalisation préférentiel, la seconde mémoire est également agencée pour stocker la multiplicité d'identifiants de sites informatiques en correspondance d'au moins un identifiant de contenu, celui-ci servant à la détermination de l'identifiant de cible qui est associé au site.

Par ailleurs, il est avantageux que la seconde mémoire puisse stocker chaque identifiant de site informatique en correspondance d'une donnée représentative de la fréquence suivant laquelle le contenu du site associé doit être vérifié. Dans ce cas, on prévoit des moyens de comptage pour gérer les données de fréquence associées à chaque identifiant de site et pour fournir au serveur chaque identifiant de site dont le contenu doit être vérifié. Cela permet de vérifier régulièrement les contenus des sites, et par conséquent de mettre à jour les identifiants de cible et de contenu auxquels ils sont associés. Bien entendu, les fréquences de vérification peuvent varier d'un site à l'autre.

Selon une autre caractéristique de l'invention, le dispositif comprend un ou plusieurs terminaux d'analyse raccordés au serveur et dédiés à l'analyse des sites informatiques et à la génération des identifiants de cible associés aux identifiants de site, lesquels sont ensuite stockés dans la première mémoire. Dans ce cas, il est avantageux que ce soit le serveur qui transmette aux terminaux d'analyse les identifiants des sites dont les contenus doivent être vérifiés ou analysés (en cas de site inconnu).

Préférentiellement, le serveur est agencé pour interdire l'accès aux sites dont le contenu est en cours de vérification ou d'analyse. Dans ce cas, on peut prévoir que le serveur adresse au terminal interrogateur un message lui demandant de renouveler sa requête quelques instants plus tard.

Selon encore une autre caractéristique de l'invention, on adapte dans chaque terminal d'interrogation de client l'un au moins de ses modules de navigation, pour qu'il puisse échanger des données avec le serveur et lui transmettre des requêtes d'accès. Dans ce cas, il est avantageux d'utiliser un module logiciel (« plug-in ») pour adapter le module de navigation de chaque terminal de client, ce module logiciel étant de préférence adapté spécifiquement en fonction de chaque identifiant de cible du client et/ou d'au moins un identifiant personnel complémentaire. Il est également particulièrement avantageux que le module logiciel comporte l'identifiant du client et soit agencé pour interdire l'utilisation d'autres modules de navigation que celui adapté. Il est en outre particulièrement avantageux que le module logiciel soit agencé, en cas de requête d'accès à un site, émise par un terminal d'un client, pour autoriser le chargement immédiat du contenu du site dans une zone (fenêtre cachée ou mémoire cachée de préférence de type mémoire tampon) du terminal, inaccessible au client, et à permettre au client d'accéder sur son terminal au contenu chargé lorsque l'identifiant de cible associé dans la première mémoire à l'identifiant du client contenu dans la requête, est également associé dans la seconde mémoire à l'identifiant du site.

L'invention concerne également une installation de communication comprenant une multiplicité de terminaux d'interrogation et de sites informatiques raccordés à un réseau, ainsi qu'un dispositif de gestion de données du type de celui présenté ci-avant.

L'invention concerne en outre un procédé de gestion de données contenues dans des sites informatiques accessibles via un réseau, pour la mise en oeuvre des dispositifs et installations présentés ci-avant. Ce procédé comprend au moins les étapes suivantes :

a) stocker une multiplicité d'identifiants de sites informatiques, raccordés au réseau, en correspondance d'au moins un identifiant de cible,

b) stocker une multiplicité d'identifiants de client en correspondance d'au moins un identifiant de cible,

c) recevoir d'un terminal d'interrogation distant, via le réseau, une requête d'accès à au moins un site, comportant un identifiant de client et au moins un identifiant de site, et

d) autoriser l'accès, via ce terminal, au contenu du site désigné par la requête lorsque l'identifiant de cible associé à l'identifiant du client, contenu dans cette requête, est également associé à l'identifiant dudit site désigné.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés, sur lesquels :

- la figure 1 illustre de façon très schématique une installation de communication équipée d'un dispositif de gestion d'accès à des données, selon l'invention, et
- la figure 2 est un algorithme décrivant les principales étapes d'un exemple de réalisation d'un procédé de gestion d'accès à des données, selon l'invention.

Les dessins annexés sont, pour l'essentiel, de caractère certain. En conséquence, ils pourront non seulement servir à compléter l'invention, mais aussi contribuer à sa définition, le cas échéant.

On se réfère tout d'abord à la figure 1 pour décrire une installation de communication équipée d'un dispositif de gestion de l'accès à des données accessibles via un réseau de communication, tel qu'Internet. Bien entendu, l'invention ne se limite pas à ce seul type de réseau. Elle concerne les réseaux publics comme les réseaux privés, de type Intranet ou analogue. L'invention concerne également les réseaux de type Intranet couplés à un réseau public.

L'installation de communications comporte donc un réseau public de type Internet auquel sont raccordées une multiplicité de terminaux d'interrogation TIi (dans l'exemple illustré, i = 1 à 5) ainsi qu'une multitude de sites Internet (ou sites Web) SWj (dans cet exemple, j = 1 à 4). Comme illustré, l'un des terminaux TI5 peut être un serveur d'entreprise couplé à des sous-terminaux STIm (ici m = 1à 3) au sein d'un réseau privé.

De façon connue, les terminaux d'interrogation TIi sont équipés d'un module de navigation Ni qui leur permet, éventuellement par l'intermédiaire d'un fournisseur d'accès, d'accéder aux données qui sont contenues dans les sites Web SWj. Pour ce faire, l'utilisateur d'un terminal d'interrogation TIi saisit dans une fenêtre de son navigateur Ni soit un ou plusieurs mots, soit directement l'adresse du site auquel il veut accéder (plus connue sous l'acronyme anglais URL pour "Uniform Resource Location").

Généralement, la connexion s'effectue par l'intermédiaire d'un fournisseur d'accès, au travers d'un "routeur".

Dans ce type d'installation, chaque personne peut donc en se connectant au réseau Internet, par l'intermédiaire de son terminal d'interrogation TIi, accéder à n'importe quel type de données, y compris les données qui lui sont interdites, par exemple du fait de la législation du pays dans lequel il réside, ou pour d'autres raisons, comme par exemple pour des questions de moralité ou de bonnes mœurs. On comprendra, par exemple, que des données de texte ou d'image à caractère pornographique ou pédophile ne doivent pas être rendues accessibles aux enfants. On peut également envisager des cas dans lesquels les directions de certaines entreprises ne souhaitent pas que certains au moins de leurs employés puissent accéder à des sites ou domaines, ou bases de données, qui ne présentent pas de rapport direct avec leur fonction au sein de l'entreprise. On peut encore citer le cas de certains pays dans lesquels les données de textes et d'images de caractère pornographique sont totalement prohibées. Dans toutes ces situations, comme dans de nombreuses autres, il peut s'avérer indispensable d'interdire l'accès à certaines données selon des

critères choisis.

L'invention vient apporter une solution à ce problème. Elle propose pour ce faire un dispositif de gestion de l'accès à des données qui sont accessibles sur le réseau (ici Internet).

Ce dispositif comporte, tout d'abord, un serveur S raccordé, d'une part au réseau Internet, et d'autre part à un réseau privé 1, auquel sont raccordés des terminaux d'analyse TAk (ici, k = 1 à 3). De préférence, la connexion au réseau public Internet du serveur S et des terminaux TAk s'effectue via des serveurs "pare-feu" 2 (plus connu sous le nom anglais "Firewall").

Dans l'exemple illustré sur la figure 1, les terminaux d'analyse TAk, sur lesquels on reviendra plus loin, sont agencés en parallèles, mais, bien entendu, ils pourraient être agencés en série.

Chaque personne qui souhaite que l'on contrôle (ou gère) l'accès aux données qui sont accessibles sur le réseau Internet, via son terminal, peut contacter le gestionnaire du serveur S. Ce dernier va soit enregistrer les critères d'autorisation ou d'interdiction d'accès de la personne, soit lui demander de remplir un questionnaire qu'elle devra lui retourner. Ce questionnaire, comme les critères, permet de caractériser le client par des identifiants que l'on appelle « identifiant de cible ». Comme indiqué précédemment, un identifiant de cible peut représenter de très nombreuses informations, comme par exemple l'âge, le sexe, le pays de résidence, la fonction au sein d'une entreprise, mais également les goûts, par exemple en matière musicale ou littéraire, ou sportive, etc, ou encore une interdiction ou une autorisation d'accès à des informations choisies. Bien entendu, toutes ces informations sont conservées par le gestionnaire du serveur S à titre confidentiel.

Ces identifiants de cibles sont associés à l'identifiant du client, lequel peut être, par exemple, l'adresse de son terminal d'interrogation TIi, ou bien un code confidentiel. Mais, on peut tout à fait envisager qu'à un client soit

associée une multiplicité de sous-identifiants de clients. Cela peut être utile, par exemple dans une entreprise ou dans une famille.

Il est clair que dans le cas d'Internet, l'adresse IP du terminal d'interrogation d'un « internaute » est contenue dans les données qu'il émet et qui sont au format du réseau, si bien que lorsque le terminal interrogateur adresse un message ou une requête au serveur S, celui-ci est en mesure de déterminer instantanément son origine. Cette caractéristique pourrait être utilisée pour déterminer l'identifiant du client, sans que celui-ci n'ait besoin de le communiquer. Cependant, lorsque plusieurs terminaux sont associés à un même client, par exemple dans une entreprise, il arrive fréquemment que des réarrangements des adresses IP surviennent entre terminaux. Par conséquent, il est préférable que le serveur S attribue à chaque browser de client, un numéro d'identification qui constitue l'identifiant client.

Un code confidentiel, en complément de l'identifiant du client, peut également être envisagé pour permettre la différenciation des différents utilisateurs d'un même terminal Tli, de manière à leur offrir une gestion sur mesure.

Le serveur comporte, de préférence, une première mémoire 3 dans laquelle sont stockés les identifiants des clients, accompagnés éventuellement du ou des codes confidentiels associés, en correspondance d'un ou plusieurs identifiants de cibles qui caractérisent les clients, ou les différents utilisateurs d'un terminal d'interrogation Tli d'un client.

Cette première mémoire 3 peut stocker ces informations sous la forme d'enregistrements, de type multiplet, chaque multiplet comportant au moins un identifiant de client et un identifiant de cible. Mais, comme indiqué précédemment, un multiplet peut comporter plus de deux informations.

Ainsi, dans le serveur S, les données auxquelles peut accéder chaque client sont représentées par le ou les identifiants de cibles qui caractérisent ce client.

Le serveur S comporte, également de préférence, une seconde

mémoire 4 dans laquelle se trouvent stockés des identifiants de sites en correspondance d'au moins un identifiant de cible. Comme pour la première mémoire 3, les informations (identifiant de site et identifiant de cible) sont mémorisées sous la forme d'enregistrements de type multiplet. Bien entendu, à un identifiant de site peuvent être associés plusieurs identifiants de cibles.

Dans le cas du réseau public Internet, l'identifiant de site est de préférence son adresse Internet ou URL (acronyme pour "Uniform Resource Location") mais, bien entendu, il pourrait s'agir de tout autre type d'identifiant direct ou indirect.

L'association d'un ou plusieurs identifiants de cible à un identifiant de site s'effectue par une analyse préalable du contenu des données qui sont accessibles sur le site concerné.

Cette analyse s'effectue au niveau des terminaux d'analyse TAk auxquels est connecté le serveur S via son réseau privé 1 de type Intranet, par exemple.

Chaque terminal d'analyse TAk est raccordé au réseau public Internet, de préférence par l'intermédiaire du pare-feu 2, si bien qu'il peut accéder à n'importe quel site ou page Web SWj, ou base de données, raccordé au réseau public Internet.

Préférentiellement, chaque terminal d'analyse TAk est piloté par un opérateur qui, une fois qu'il a téléchargé les données d'un site, ou une partie de celles-ci, va en analyser le contenu et lui associer des identifiants de cible. Plus préférentiellement, chaque opérateur associe au contenu d'un site SWj un ou plusieurs identifiants de contenu, puis il attribue des identifiants de cible en fonction desdits identifiants de contenu. Dans ce cas, il est avantageux de mémoriser dans la seconde mémoire 4 non seulement l'identifiant du site et un ou plusieurs identifiants de cible, mais également le ou les identifiants de contenu associés.

Egalement de préférence, lorsqu'un site fait l'objet d'une analyse, le

terminal d'analyse TA accède à son contenu, mais également à tous ses liens internes et externes. Il possède par conséquent, en direct, toutes les adresses des liens internes et externes, si bien qu'il est possible de vérifier les contenus des sites ou parties de sites désignés par ces liens. Cela permet d'améliorer très notablement la productivité des analyses et de gérer les rattachements (ou liens) internes et externes au niveau de chaque page.

Par ailleurs, les terminaux d'analyse TA peuvent, de préférence, se transmettre des adresses de sites. Cela est particulièrement intéressant lorsque chaque terminal d'analyse TA est spécialisé dans l'analyse de thèmes ou domaines particuliers.

D'autre part, il est particulièrement avantageux d'associer à chaque identifiant de site une donnée temporelle représentative de la fréquence (ou période) suivant laquelle le contenu du site doit être vérifié, de manière à détecter toute modification. Mais d'autres données peuvent être également associées à l'identifiant de site.

Les principales étapes d'analyse d'un site sont résumées ci-après. Dans une première étape le terminal d'analyse TAk charge le contenu d'un site à analyser, y compris ses liens internes et externes. Dans une seconde étape, on vérifie tous les liens internes de chaque page du site. Dans une troisième étape, on vérifie tous les liens externes de chaque page du site. L'analyse de chaque lien externe renvoie à chaque fois à la première étape. Dans une quatrième étape, on associe au site une fréquence de vérification, ou plusieurs fréquences de vérification pour chacune des parties d'un site. Les vérifications peuvent être partielles ou complètes. Dans une cinquième étape, on associe au site des identifiants de cible et, éventuellement, des identifiants de contenu. L'ordre des étapes indiquées ci-avant n'est pas figé.

La gestion des fréquences de vérification est assurée par un module de comptage 5 qui est préférentiellement logé dans le serveur S. Cette gestion peut s'effectuer, par exemple, par un balayage régulier des contenus de la seconde mémoire 4 de manière à lire les données temporelles qui s'y

trouvent stockées et à extraire les identifiants des sites qui n'ont pas été vérifiés (ou analysés) depuis un temps sensiblement égal à la période mémorisée et qui par conséquent doivent être vérifiés. Ces identifiants de sites sont transmis aux terminaux d'analyse TAk de sorte qu'ils puissent immédiatement vérifier les contenus respectifs des sites correspondants. Plus précisément, et de préférence, on stocke dans la mémoire 4, ou bien dans une autre mémoire, l'identifiant du terminal d'analyse TAk (en fait celui de son opérateur), qui a effectué l'analyse du contenu du site, en correspondance de l'identifiant de site.

Cette vérification s'effectue, de préférence, par une procédure automatisée qui ne fait pas appel à un opérateur. Elle consiste, par exemple, en une comparaison entre des champs représentatifs du contenu en cours du site web SWj et les champs représentatifs de son contenu précédent. Il pourra s'agir, par exemple des champs « date », « nombre de pages », « poids », « mots clés d'émission », que l'on stocke en correspondance de chaque identifiant de site dans la mémoire 4.

Mais la vérification pourrait également consister en une comparaison entre le contenu en cours du site web SWj et son contenu précédent (mode dit « full text »). A cet effet, on stocke le contenu des sites dans une mémoire, puis on compare le contenu en cours (téléchargé) au contenu stocké. Puis, en cas de modification, on remplace l'ancien contenu par le nouveau.

Cette vérification pourrait également consister en une combinaison des deux exemples présentés ci-dessus, le contenu en cours (full text) du site étant comparé au contenu précédent en cas de différence d'un ou plusieurs champs choisis.

En cas de modification, le terminal d'analyse TAk crée un message d'alerte qu'il affiche sur son moniteur (ou écran), et qu'il adresse de préférence au serveur S, de sorte que celui-ci interdise, momentanément, l'accès aux données du site modifié. Un opérateur (de préférence celui qui a

effectué l'analyse précédente de ce même site) va alors déterminer les modifications qui ont été apportées au site, et revoir éventuellement les identifiants de contenus et les identifiants de cibles qui lui étaient précédemment associés. Ces nouveaux identifiants de cibles et de contenus sont alors adressés au serveur S de sorte qu'il les stocke en correspondance de l'identifiant de site concerné dans la seconde mémoire 4, en remplacement du multiplet précédent. Le site peut alors être de nouveau mis à la disposition des clients.

Le dispositif selon l'invention est capable d'analyser et de vérifier tout type de site, qu'il soit « statique » ou « dynamique ».

De préférence, lorsqu'un client souhaite accéder à un site qui fait l'objet d'une vérification, le serveur S adresse au terminal d'interrogation Tli de ce client un message lui demandant de renouveler ultérieurement sa requête (ou demande). En variante, le serveur S peut traiter la requête d'un client, laissée de côté du fait d'une vérification, à réception des nouveaux identifiants de cible et de contenu.

Selon une autre caractéristique de l'invention, il est particulièrement avantageux d'adapter l'un des browsers (ou navigateurs) qui équipent les terminaux des clients de sorte qu'il puisse dialoguer avec le serveur S, et d'interdire l'utilisation des autres browsers (plus précisément, on interdit au terminal d'accéder directement au réseau public Internet en utilisant un autre browser que celui adapté). Pour ce faire, on fournit au client un programme destiné à ajouter au browser choisi de son terminal des fonctionnalités lui permettant de communiquer avec le serveur S, et comportant un sous-programme (ou « patch ») destiné à rendre inutilisable (ou désactiver) un ou plusieurs autres navigateurs (ou browsers) que celui permettant au client d'accéder aux services offerts par le serveur S du dispositif selon l'invention. Ce type de programme, qui permet d'ajouter des applications dédiées à un logiciel, est connu de l'homme du métier sous le nom anglais « plug-in ». Dans le cas présent, le plug-in comporte en plus, de préférence, l'identifiant du client.

Le plug-in peut être soit communiqué directement par le serveur, par téléchargement lors de la première connexion, par exemple, soit transmis par l'administrateur du serveur S sur un support de type CD-ROM.

Ce mode de fonctionnement est particulièrement bien adapté au fonctionnement dit « de proximité », c'est-à-dire en réseau privé.

Comme indiqué dans l'introduction, le dispositif selon l'invention permet de traiter des requêtes d'accès à des sites (sites ou pages web ou domaines ou bases de données). Par conséquent, à réception d'une requête d'accès désignant un domaine, le serveur S va déterminer tous les sites web qui sont associés au domaine requis et transformer la requête en une multiplicité de sous-requêtes désignant chacune un site web. Ainsi, seuls les sites qui possèdent des identifiants de cibles correspondant à ceux du client ayant émis la requête pourront faire l'objet d'une autorisation d'accès.

Par ailleurs, le plug-in comporte de préférence un sous-programme permettant au browser adapté du client de se connecter directement au site qui est désigné dans une requête, et de charger son contenu dans une sous-fenêtre, cachée, inaccessible au client. Le contenu ainsi chargé ne pourra être rendu accessible au client qu'en cas d'accord du serveur S, c'est-à-dire après comparaison des identifiants de cible du client aux identifiants de cible du site requis. De la sorte, dès que le serveur donne son autorisation, le contenu du site, ou une partie de ce contenu, est rendu accessible. En cas d'interdiction, le contenu chargé et caché est détruit. Un gain de temps important est ainsi obtenu.

On pourra également utiliser une mémoire cachée, de préférence de type mémoire tampon, pour charger le contenu du site, ou tout autre zone du terminal à laquelle ne peut pas accéder l'utilisateur.

D'autre part, le serveur S est préférentiellement agencé pour gérer les liens inter-sites et intra-site. En effet, l'une des caractéristiques principales du World Wide Web (ou Internet) est de permettre la navigation d'un premier site vers un ou plusieurs sites sans qu'il faille effectuer des

opérations explicites de connexion, et donc sans changement apparent de site. De même, certains sites possèdent des pages qui proposent des liaisons internes vers certaines de leurs autres pages, si bien qu'il est possible de naviguer à l'intérieur d'un site après s'y être connecté. Or, il peut arriver que la quasi totalité d'un site corresponde aux critères (cibles) d'un client, mais qu'une toute petite partie n'y corresponde pas.

Afin de contrôler les liens externes, chaque fois qu'un client sélectionne un site lié au site auquel il est connecté, le browser du client adresse au serveur S une requête d'accès à ce site sélectionné, si bien qu'une nouvelle comparaison est effectuée et que le client ne peut accéder à ce nouveau site qu'en cas de correspondance entre ses identifiants de cibles et ceux dudit site. On évite ainsi les accès à des sites par des chemins détournés.

De même, pour contrôler les liens internes, chaque fois qu'un client se trouve dans une page de site web qui propose des liens vers d'autres pages et qu'il sélectionne l'un de ces liens, le browser du client adresse au serveur S une requête d'accès à la page désignée par ledit lien sélectionné. Cela est rendu possible par le fait que les pages web possèdent leurs propres adresses (page URL). A réception de la requête, le serveur va donc effectuer une nouvelle comparaison de manière à déterminer si le client peut accéder à la page web. Cela est particulièrement intéressant par exemple lorsqu'une page renvoie vers des photographies, ou des textes, ou des plans, ou encore des thèmes dont les contenus sont interdits au client.

Le traitement de la requête adressée par un client, via son terminal d'interrogation TIi et le réseau public Internet, s'effectue au niveau du serveur S. Un exemple de traitement va maintenant être décrit en référence à la figure 2.

Dans une étape 10, le serveur S réceptionne la requête d'un client adressée par le terminal TI1, par exemple. Si la requête désigne un domaine, elle est décomposée en sous-requêtes désignant chacune un site

(cette décomposition peut être effectuée à l'étape 30). Préférentiellement, on télécharge immédiatement dans une zone du terminal TI1, inaccessible au client (par exemple une fenêtre cachée), le contenu du « site » requis.

Dans une étape 20, l'identifiant du client est extrait de la requête, puis comparé aux identifiants de clients qui sont stockés dans la première mémoire 3. Si l'identifiant du client n'est pas stocké dans cette seconde mémoire 3, alors la requête est rejetée (étape 25). Le serveur S peut alors être agencé de manière à établir un dialogue avec le client pour lui proposer de s'abonner ou bien de s'identifier par une procédure de saisie auxiliaire proposée dans une fenêtre ou sur une page spécifique. A l'issue de cette procédure d'identification, le serveur S adresse au terminal un plug-in permettant d'adapter l'un de ses browsers, et comportant un identifiant de client, accompagné éventuellement d'un pseudonyme et d'une demande d'accusé de réception. L'identifiant de client et le pseudonyme sont alors stockés dans un registre du terminal client. Bien entendu, le plug-in peut être transmis sur un support de type CD-ROM.

En revanche, si le client est abonné, le serveur S extrait de la requête, dans une étape 30, l'identifiant du site auquel le client souhaite accéder. Puis, il compare cet identifiant de site aux identifiants de site qui sont stockés dans la seconde mémoire 4. Si le site est répertorié dans cette seconde mémoire 4, alors on passe à l'étape 40.

En revanche, si ce site n'est pas répertorié, ou bien s'il fait l'objet d'une vérification, on rejette la requête (étape 32) ou, en variante, le serveur demande aux terminaux d'analyse TAk d'effectuer l'analyse du contenu du site non répertorié (étape 34). Si le site non répertorié n'existe pas, la requête est rejetée (étape 35). En variante, on adresse au client un message lui demandant de vérifier sa requête, ou bien d'en effectuer une nouvelle. En revanche, si le site non répertorié existe, on procède dans une étape 36 à l'analyse de son contenu de manière à générer un multiplet comportant l'identifiant du site, un ou plusieurs identifiants de contenu et un ou plusieurs identifiants de cible. Ce multiplet est transmis au serveur S de sorte qu'il le

stocke dans la seconde mémoire 4, puis on passe à l'étape 40.

Dans cette étape 40, le serveur S extrait de la première mémoire 3 le ou les identifiants de cible associés au client qui a émis la requête, et dans la seconde mémoire 4 le ou les identifiants de cible qui sont associés au site auquel ledit client souhaite accéder.

Dans une étape 50, le serveur S effectue une comparaison entre ces identifiants de cible extraits des première 3 et seconde 4 mémoires, et s'il y a correspondance, le serveur S autorise le terminal d'interrogation TI1 à afficher le contenu du site qui avait été téléchargé et caché à l'étape 10 (étape 60). En revanche, si les deux jeux d'identifiants de cible ne correspondent pas, alors la requête est rejetée (étape 62). Dans ce cas un message est préférentiellement adressé au client pour lui indiquer la raison du rejet de sa requête. Le contenu téléchargé et caché est alors détruit.

De préférence, dans l'étape 60 après autorisation d'accès au contenu, au moins partiel, d'un premier site, toute tentative d'accès à un site lié à ce premier site (lien externe) renvoie à l'étape 10. Il en va de même lorsqu'il s'agit d'une tentative d'accès à un lien interne à ce site.

Bien entendu dans l'étape 60, lorsque l'on ne télécharge pas immédiatement le contenu du site requis à l'étape 10, l'accession au contenu au moins partiel de ce site s'effectue après que le serveur ait délivré une autorisation de connexion du terminal émetteur au site requis.

L'invention porte également sur un procédé de gestion de données contenues dans des sites informatiques SWj accessibles via un réseau public et/ou privé. Ce procédé comprend au moins les étapes présentées ci-dessous.

Tout d'abord, on mémorise une multiplicité d'identifiants de sites informatiques, raccordés au réseau, en correspondance d'au moins un identifiant de cible (étape a), puis on mémorise une multiplicité d'identifiants de client en correspondance d'au moins un identifiant de cible (étape b). On constitue ainsi une base de données contenant des informations sur les

clients abonnés et sur les sites accessibles sur le réseau public.

Ensuite (étape c), à réception d'une requête d'accès à au moins un site, émise par le terminal distant d'un client via le réseau, et comportant un identifiant de client et au moins un identifiant de site, on détermine si l'identifiant de cible associé à l'identifiant du client qui est contenu dans la requête est également associé à l'identifiant du site désigné. Si tel est le cas, on autorise l'accès, via le terminal distant du client, au contenu du site désigné par la requête (étape d).

Préférentiellement, et comme indiqué dans la description du dispositif, on mémorise à l'étape a) les identifiants des sites informatiques en correspondance d'un ou plusieurs identifiants de contenu, de manière à simplifier le traitement des requêtes, notamment.

De même, et toujours dans l'étape a), on mémorise préférentiellement chaque identifiant de site informatique en correspondance d'une donnée représentative d'une fréquence de vérification du contenu du site associé, de sorte que l'on puisse effectuer, en parallèle des étapes a) à d) une étape de gestion des données de fréquence associées aux identifiants de site, pour déterminer les identifiants de site dont le contenu doit être vérifié.

Le procédé peut également permettre le stockage, de préférence lors de l'étape b), d'un ou plusieurs identifiants personnels complémentaires en correspondance de chaque identifiant client. Il pourra s'agir, par exemple, de données permettant de définir la personnalisation du browser du client.

Le procédé peut également permettre la connection à des sites dont l'accès est demandé mais qui ne sont pas répertoriés. Pour ce faire, et à réception d'une requête comportant un identifiant de site inconnu, on effectue à l'étape c) une analyse du contenu de ce site pour déterminer ses identifiants de cible. Puis, on mémorise les identifiants de cible en correspondance de l'identifiant de site. Il est alors possible de déterminer si le client est autorisé à accéder au site qui vient d'être analysé, compte tenu

de ses identifiants de cible personnels.

Il est par ailleurs avantageux, lors de l'étape c), d'interdire l'accès aux sites dont le contenu est en cours de vérification ou d'analyse.

Il est également avantageux, comme indiqué dans la partie relative au dispositif, de charger immédiatement, dans l 'étape c), le contenu du site requis dans une zone du terminal qui est inaccessible au client, puis de permettre au client d'accéder sur son terminal au contenu chargé lorsque l'identifiant de cible associé à l'identifiant du client contenu dans la requête, est également associé à l'identifiant du site.

Grâce aux dispositif, installation et procédé selon l'invention, il est possible de contrôler (ou gérer) l'accès aux données qui sont accessibles sur un réseau public de type Internet (ou privé). Les identifiants de cible permettent en effet d'interdire à certains clients l'accès à certains sites ou à certaines parties de certains sites. Cela permet également à certains pays d'interdire de façon systématique l'accès à certaines données, de sorte que les "Internautes" résidant dans ces pays ne puissent enfreindre les lois propres auxdits pays, même involontairement. Cela permet en outre aux dirigeants de certaines entreprises de sélectionner les informations accessibles sur certains postes (ou terminaux), de manière à ne plus avoir à s'en préoccuper. Cela permet encore d'équiper les terminaux des écoles, des universités ou des habitations privées de moyens de filtrage assurant une impossibilité d'accès à des informations choisies.

En résumé, l'invention permet à des clients « abonnés » de "surfer" tranquillement, sans se soucier de ce sur quoi ils peuvent tomber.

L'invention pourra présenter de nombreuses variantes. Par exemple, le serveur S peut être agencé de manière à permettre une personnalisation du module de navigation (ou browser) de chaque client.

Pour ce faire, on associe, de préférence, à chaque identifiant de client un ou plusieurs identifiants personnels complémentaires qui vont définir son browser personnel. Ces identifiants personnels complémentaires

peuvent être stockés soit dans une troisième mémoire, en correspondance de l'identifiant du client, soit directement dans le multiplet du client, contenu dans le première mémoire 3. Bien entendu, certains identifiants personnels complémentaires peuvent être utilisés pour d'autres objets que la personnalisation du browser.

Comme indiqué précédemment, la personnalisation du browser est transmise par le serveur S au terminal du client sous la forme d'un plug-in, lors de la première connexion. Mais, elle peut être adressée au client sur un support physique de type CD-ROM.

On pourrait envisager d'adresser à chaque client un browser spécifique et personnalisé par le plug-in, pour accéder au serveur S du dispositif. Mais, il est avantageux d'adapter l'un des browsers (ou navigateurs) qui est déjà installé dans le terminal du client, puis de le personnaliser en fonction des informations définissant le client.

Cela peut permettre d'offrir une mise en page (ou décoration) personnalisée. Mais, cela peut également permettre de prévoir sur la page d'accueil du module de navigation personnalisé une zone (ou bandeau) destinée à présenter des informations personnalisées, telles que de la publicité pour des marques ou des événements, ou autres. Bien entendu, lorsque les messages publicitaires proposent au client des liens vers des informations complémentaires, le serveur S effectue une vérification du contenu de ces informations complémentaires avant d'en autoriser l'accès au client, toujours selon le mode de comparaison décrit précédemment, qui repose sur une analyse des identifiants de cible.

L'invention ne se limite pas aux modes de réalisation de dispositif, d'installation et de procédé décrits ci-avant, seulement à titre d'exemple, mais elle englobe toutes les variantes que pourra envisager l'homme de l'art dans le cadre des revendications ci-après.

Ainsi, il a été décrit un serveur S dans lequel étaient logées les première et seconde (et éventuellement troisième) mémoires, mais ces

mémoires pourraient être externes au serveur, et être éventuellement délocalisées. Ces mémoires pourraient être des parties d'une même mémoire ou d'une base de données.

Par ailleurs, dans ce qui précède il a été décrit un mode de fonctionnement dans lequel les identifiants cible définissaient des critères d'autorisation ou d'interdiction à des sites. De tels critères ne sont pas obligatoirement définitifs. Ils peuvent en effet concerner des autorisations ou interdictions passagères. Par exemple, on peut autoriser un nombre choisi d'accès à un même site, sur une période définie ou indéfinie. On peut également interdire ou autoriser momentanément l'accès à un ou plusieurs sites. Dans ce cas, on prévoit dans le serveur du dispositif un module permettant de contrôler, lors de chaque réception d'une requête d'accès à un site, si le critère temporel et/ou numérique associé au client et au site est vérifié. De la sorte, si le critère n'est pas vérifié, la requête est immédiatement rejetée.

REVENDICATIONS

1. Dispositif de gestion de données contenues dans des sites informatiques (SWj) accessibles via un réseau, caractérisé en ce qu'il comprend :

- une première mémoire (3) propre à stocker une multiplicité d'identifiants de client en correspondance d'au moins un identifiant de cible,
- une seconde mémoire (4) propre à stocker une multiplicité d'identifiants de sites informatiques (SWj), raccordés au réseau, en correspondance d'au moins un identifiant de cible,
- un serveur (S) raccordé aux première et seconde mémoires (3,4) et au réseau, et propre à recevoir de terminaux distants (Tli), via ledit réseau, des requêtes d'accès à des sites (SWj) comportant chacune un identifiant de client et au moins un identifiant de site, et à permettre au client ayant transmis une requête d'accéder, via son terminal (Tli), au contenu du site désigné par cette requête lorsque l'identifiant de cible associé dans la première mémoire (3) à l'identifiant du client, contenu dans la requête, est également associé dans la seconde mémoire (4) à l'identifiant dudit site.

2. Dispositif selon la revendication 1, caractérisé en ce que la seconde (4) mémoire est propre à stocker la multiplicité d'identifiants de sites informatiques en correspondance d'au moins un identifiant de cible et d'au moins un identifiant de contenu.

3. Dispositif selon la revendication 2, caractérisé en ce que chaque identifiant de cible associé à un identifiant de site est fonction de l'identifiant de contenu associé audit identifiant de site.

4. Dispositif selon l'une des revendications 1 à 3, caractérisé en ce que la seconde mémoire (4) est propre à stocker chaque identifiant de site informatique en correspondance d'au moins un identifiant de cible et d'une donnée représentative d'une fréquence de vérification du contenu du site associé, et en ce qu'il comprend des moyens de comptage (5) propres à

gérer les données de fréquence associées à chaque identifiant de site et à fournir audit serveur (S) chaque identifiant de site dont le contenu doit être vérifié.

5. Dispositif selon l'une des revendications 1 à 4, caractérisé en ce qu'il comprend au moins un terminal d'analyse (TAk) raccordé au serveur (S) et destiné à l'analyse des sites informatiques (SWj) en vue de la génération des identifiants de cible associés aux identifiants de sites, susceptibles d'être stockés dans la seconde mémoire (4).

6. Dispositif selon la combinaison des revendications 4 et 5, caractérisé en ce que le serveur (S) est agencé pour transmettre au terminal d'analyse (TAk) chaque identifiant de site dont le contenu doit être vérifié.

7. Dispositif selon l'une des revendications 5 et 6, caractérisé en ce que le serveur (S) est agencé pour transmettre au terminal d'analyse (TAk) chaque identifiant de site qui n'est pas stocké dans la seconde mémoire (4), de sorte que son contenu soit analysé.

8. Dispositif selon l'une des revendications 1 à 7, caractérisé en ce que chaque terminal d'analyse (TAk) est agencé pour charger conjointement le contenu d'un site à analyser ou à vérifier et tous les liens internes et/ou externes que ce site possède avec d'autres sites et/ou avec lui-même.

9. Dispositif selon l'une des revendications 1 à 8, caractérisé en ce que chaque terminal d'analyse (TAk) est agencé pour analyser et/ou vérifier les contenus des sites dynamiques.

10. Dispositif selon l'une des revendications 4 à 9, caractérisé en ce que le serveur (S) est agencé pour interdire l'accès aux sites (SWj) dont le contenu est en cours de vérification ou d'analyse.

11. Dispositif selon l'une des revendications 1 à 10, caractérisé en ce qu'il est agencé pour adapter l'un au moins des modules de navigation implantés dans le terminal de chaque client pour permettre l'échange de données et la transmission des requêtes entre le terminal (TIi) et le serveur

(S).

12. Dispositif selon la revendication 11, caractérisé en ce qu'il est agencé pour former un module logiciel propre à adapter le module de navigation de chaque terminal (Tli) de client.

13. Dispositif selon la revendication 12, caractérisé en ce qu'il est agencé pour adapter spécifiquement chaque module logiciel transmis au client en fonction de chaque identifiant de cible dudit client et/ou d'au moins un identifiant personnel complémentaire.

14. Dispositif selon l'une des revendications 12 et 13, caractérisé en ce que le module logiciel comporte l'identifiant du client et est agencé pour interdire l'utilisation d'autres modules de navigation que celui adapté.

15. Dispositif selon l'une des revendications 12 à 14, caractérisé en ce que le module logiciel est agencé, en cas de requête d'accès à un site, émise par un terminal d'un client (Tli), pour autoriser le chargement immédiat du contenu du site dans une zone du terminal inaccessible audit client et à permettre au client d'accéder sur son terminal audit contenu chargé lorsque l'identifiant de cible associé dans la première mémoire (3) à l'identifiant du client contenu dans la requête, est également associé dans la seconde mémoire (4) à l'identifiant dudit site.

16. Dispositif selon l'une des revendications 13 à 15, caractérisé en ce que l'identifiant personnel complémentaire est stocké dans la première mémoire (3) en correspondance de l'identifiant de client.

17. Dispositif selon l'une des revendications 13 à 15, caractérisé en ce que l'identifiant personnel complémentaire est stocké dans une troisième mémoire en correspondance de l'identifiant de client.

18. Dispositif selon l'une des revendications 1 à 17, caractérisé en ce que lesdites première et seconde mémoires (3,4) sont logées dans ledit serveur (S).

19. Installation de communication, du type comprenant une multiplicité de terminaux (Tli) et une multiplicité de sites informatiques (SWj)

raccordés à un réseau, caractérisée en ce qu'elle comprend un dispositif de gestion de données selon l'une des revendications 1 à 18.

20. Procédé de gestion de données contenues dans des sites informatiques (SWj) accessibles via un réseau, caractérisé en ce qu'il comprend les étapes suivantes :

a. stocker une multiplicité d'identifiants de sites informatiques, raccordés au réseau, en correspondance d'au moins un identifiant de cible,

b. stocker une multiplicité d'identifiants de client en correspondance d'au moins un identifiant de cible,

c. recevoir d'un terminal distant, via le réseau, une requête d'accès à au moins un site, comportant un identifiant de client et au moins un identifiant de site, et

d. autoriser l'accès, via ledit terminal, au contenu du site désigné par la requête lorsque l'identifiant de cible associé à l'identifiant du client, contenu dans cette requête, est également associé à l'identifiant dudit site désigné.

21. Procédé selon la revendication 20, caractérisé en ce qu'à l'étape a) on stocke la multiplicité d'identifiants de sites informatiques en correspondance d'au moins un identifiant de cible et d'au moins un identifiant de contenu.

22. Procédé selon la revendication 21, caractérisé en ce que chaque identifiant de cible associé à un identifiant de site est fonction de l'identifiant de contenu associé audit identifiant de site.

23. Procédé selon l'une des revendications 20 à 22, caractérisé en ce qu'à l'étape a) on stocke chaque identifiant de site informatique en correspondance d'au moins un identifiant de cible et d'au moins une donnée représentative d'une fréquence de vérification du contenu du site associé, et en ce qu'il comprend en parallèle des étapes a) à d) une étape de gestion des données de fréquence associées aux identifiants de site, destinée à déterminer les identifiants de site dont le contenu doit être vérifié.

24. Procédé selon l'une des revendications 20 à 23, caractérisé en ce qu'à l'étape b) on stocke la multiplicité d'identifiants de client en correspondance d'au moins un identifiant personnel complémentaire.

25. Procédé selon l'une des revendications 20 à 24, caractérisé en ce qu'à l'étape c), en cas de réception d'une requête comportant un identifiant de site inconnu, on effectue une analyse du contenu dudit site de manière à déterminer ses identifiants de cible, puis de les stocker en correspondance de l'identifiant de site.

26. Procédé selon l'une des revendications 20 à 25, caractérisé en ce qu'à l'étape c) on interdit l'accès aux sites dont le contenu est en cours de vérification ou d'analyse.

27. Procédé selon l'une des revendications 20 à 26, caractérisé en ce qu'à l'étape c) on charge immédiatement le contenu du site dans une zone du terminal, inaccessible au client, et on permet audit client d'accéder sur son terminal au contenu chargé lorsque l'identifiant de cible associé à l'identifiant du client contenu dans la requête, est également associé à l'identifiant dudit site.

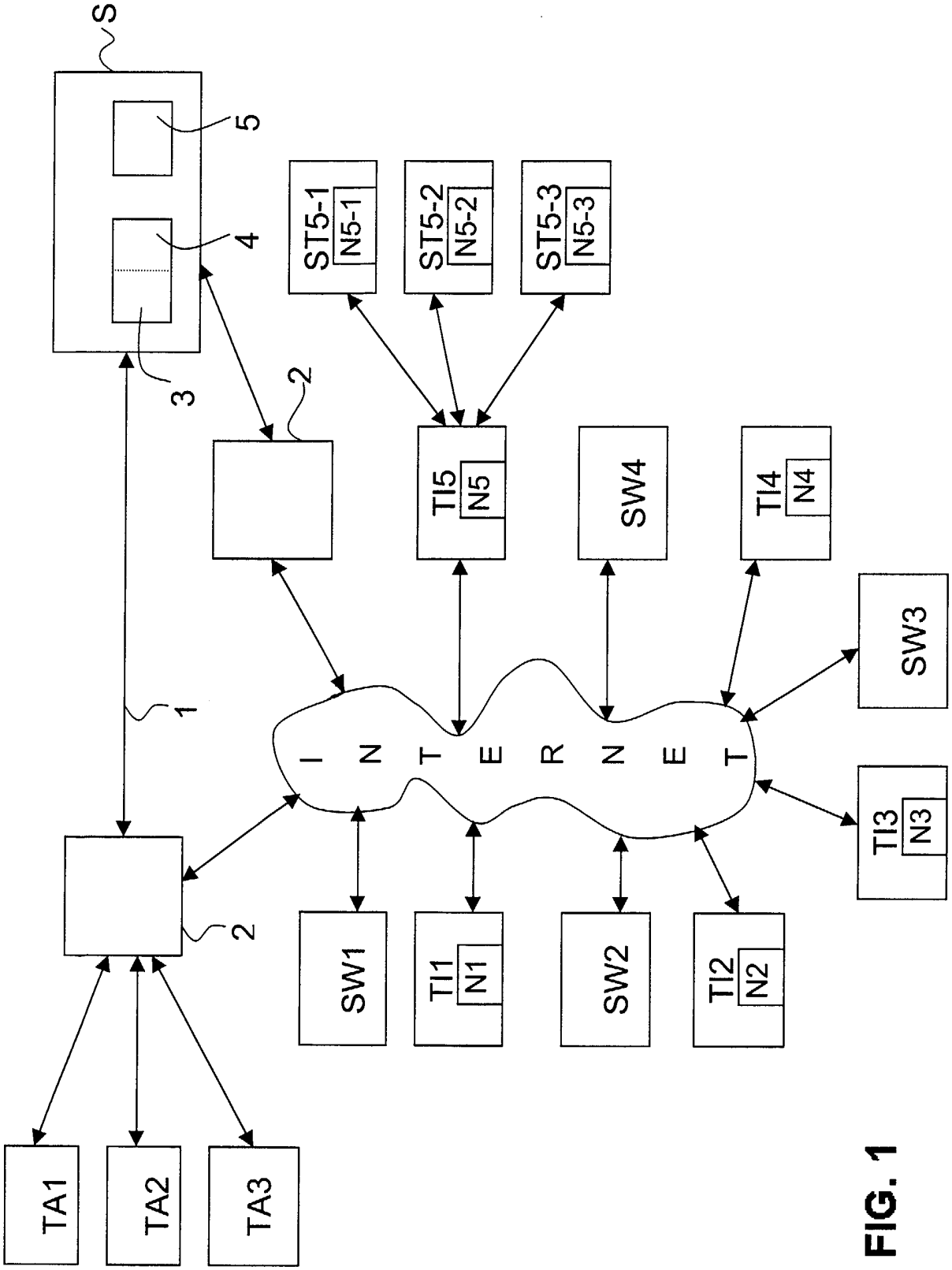

S
5
4
3
2
1
2
ST5-1
N5-1
ST5-2
N5-2
ST5-3
N5-3
TI5
N5
SW4
TI4
N4
SW3
TI3
N3
I N T E R N E T
SW1
TI1
N1
SW2
TI2
N2
TA1
TA2
TA3

FIG. 1

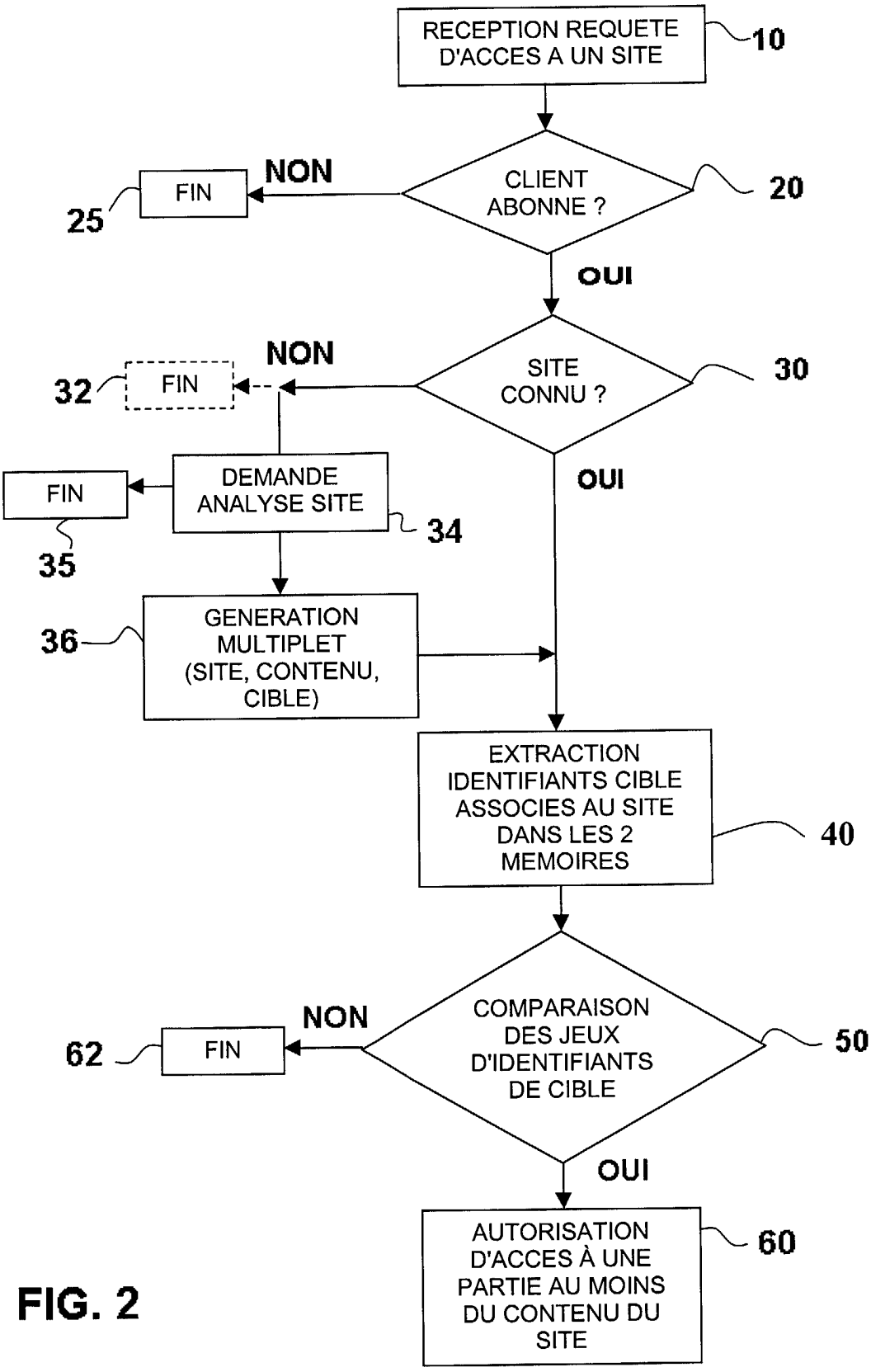

RECEPTION REQUETE D'ACCES A UN SITE
10
CLIENT ABONNE ?
20
NON
FIN
25
OUI
SITE CONNU ?
30
NON
FIN
32
OUI
DEMANDE ANALYSE SITE
34
FIN
35
GENERATION MULTIPLET (SITE, CONTENU, CIBLE)
36
EXTRACTION IDENTIFIANTS CIBLE ASSOCIES AU SITE DANS LES 2 MEMOIRES
40
COMPARAISON DES JEUX D'IDENTIFIANTS DE CIBLE
50
NON
FIN
62
OUI
AUTORISATION D'ACCES À UNE PARTIE AU MOINS DU CONTENU DU SITE
60

FIG. 2

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2811494

N° d'enregistrement national

FA 594101
FR 0008986

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 98 41913 A (DEROSA ROBERT ;CIRASOLE PETER (US); FOX ROBERT (US); BASCOM GLOBAL) 24 septembre 1998 (1998-09-24)	1-3, 5-22, 24-27	H04L9/32 H04L12/28
A	* abrégé; figures 1-3,7-9 * * page 9, ligne 24 - page 13, ligne 25 * * page 16, ligne 7 - page 17, ligne 25 * ---	4,23	
A	US 5 835 722 A (SHIH GEORGE Y ET AL) 10 novembre 1998 (1998-11-10) * abrégé; figure 2 * -----	1-27	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
H04L G06F

Date d'achèvement de la recherche	Examinateur
10 mai 2001	Stergiou, C

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)