(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 981 237**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **11 59029**

(51) Int Cl[8] : ***H 04 L 29/02*** *(2013.01), H 04 L 12/66*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 06.10.11.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 12.04.13 Bulletin 13/15.

(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) :** *PEUGEOT CITROEN AUTOMOBILES SA Société anonyme* — FR.

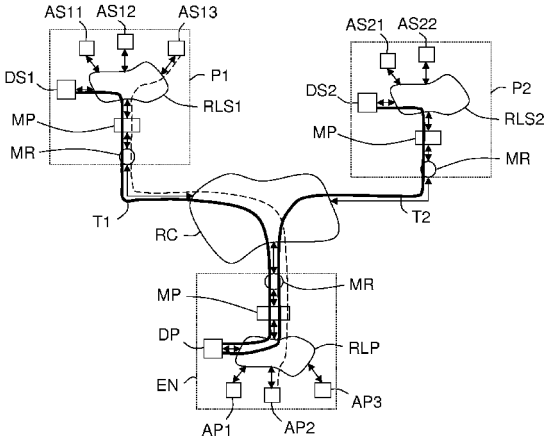
(72) **Inventeur(s) :** RAULET MICHEL et MOUFAKKIR HAKIM.

(73) **Titulaire(s) :** PEUGEOT CITROEN AUTOMOBILES SA Société anonyme.

(74) **Mandataire(s) :** PEUGEOT CITROEN AUTOMOBILES SA Société anonyme.

(54) DISPOSITIFS D'AIGUILLAGE POUR LA TRANSMISSION UNIDIRECTIONNELLE DE REQUETES DANS DES TUNNELS SECURISES, ET SYSTEME DE COMMUNICATION ASSOCIE.

(57) Un système de communication comprend un réseau local principal (RLP), auquel est couplée au moins une première application (AP1-AP3) et connecté à un réseau de communication (RC), et au moins un réseau local secondaire (RLS1-RLS2), auquel est couplée au moins une seconde application (AS11-AS22) et connecté au réseau de communication (RC). Ce système comprend en outre i) un dispositif d'aiguillage principal (DP), couplé au réseau local principal (RLP), ii) des dispositifs d'aiguillage secondaires (DS1-DS2), couplés respectivement aux réseaux locaux secondaires (RLS1-RLS2), et iii) des tunnels sécurisés établis chacun entre le dispositif d'aiguillage principal (DP) et l'un des dispositifs d'aiguillage secondaires (DS1-DS2) via le réseau de communication (RC) et utilisables chacun exclusivement à l'initiative d'une première application (AP1-AP3).



FR 2 981 237 - A1

DISPOSITIFS D'AIGUILLAGE POUR LA TRANSMISSION UNIDIRECTIONNELLE DE REQUÊTES DANS DES TUNNELS SÉCURISÉS, ET SYSTÈME DE COMMUNICATION ASSOCIÉ

L'invention concerne les systèmes de (télé)communication, et plus précisément le contrôle de l'échange de requêtes et de messages de réponse entre des réseaux locaux que comprennent de tels systèmes de (télé)communication.

On entend ici par « système de (télé)communication » un réseau local de communication dit « principal » auquel est couplée au moins une première application, éventuellement de type web (ou Internet), et qui est connecté à un réseau de communication, éventuellement l'Internet, auquel est également connecté au moins un réseau local de communication dit « secondaire », auquel est couplée au moins une seconde application, éventuellement de type web (ou Internet).

Par ailleurs, on entend ici par « réseau local de communication » un système informatique comprenant au moins un équipement de communication (terminal, ordinateur ou serveur), connecté par voie filaire ou non filaire, directement ou indirectement, éventuellement via un module de protection (comme par exemple un pare-feu), à un réseau de communication d'un opérateur public, offrant éventuellement l'accès à l'Internet. Il est important de noter qu'un tel système informatique peut comprendre plusieurs terminaux et/ou serveurs de communication pouvant échanger entre eux (c'est-à-dire en réseau) des données numériques, éventuellement de façon sécurisée et/ou hiérarchisée.

De plus, on entend ici par « réseau local principal » un réseau local appartenant à une première entreprise ou un premier groupe de sociétés et par « réseau local secondaire » un réseau local appartenant à une seconde entreprise constituant un partenaire d'une première entreprise. A titre d'exemple non limitatif une première entreprise peut être un constructeur de véhicules, éventuellement automobiles, alors qu'un partenaire peut être un

concessionnaire de véhicules, un point de distribution ou de vente de véhicules et/ou de pièces de rechange ou détachées, un fournisseur de pièces détachées ou de matériaux pour une usine, ou un entrepôt dans lequel sont stockés des véhicules et/ou des pièces détachées.

Le développement de l'Internet et la généralisation de son accès permet aux entreprises d'offrir des services, éventuellement à valeur ajoutée et éventuellement en temps réel, à leurs partenaires ou clients. Ces services peuvent être offerts par des applications, éventuellement web (ou Internet), qui s'exécutent (ou sont implantées) dans des terminaux de communication ou des serveurs d'applications, éventuellement au sein d'architectures orientées services (ou SOA (pour « Software Oriented Architecture »)).

Les technologies développées pour l'Internet, notamment les protocoles TCP/IP et HTTP, permettent d'établir des connexions entre les ordinateurs qui sont connectés via l'Internet et donc de transférer entre eux des données (numériques). Techniquement, lorsque deux ordinateurs (ou analogues) veulent communiquer par l'Internet, l'un se met à l'écoute des demandes de connexion (ou requêtes) et l'autre émet des demandes de connexion (ou requêtes). L'ordinateur qui écoute les demandes de connexion doit être accessible par l'Internet via une adresse de communication IP ou une URL (« Uniform Resource Locator ») connue par l'ordinateur qui émet les demandes de connexion. Le protocole de connexion n'est pas symétrique, mais une fois qu'une connexion TCP est établie, elle peut être utilisée par chaque ordinateur pour transmettre des données, à son initiative, et donc elle est bidirectionnelle.

Très souvent les connexions Internet et les transmissions de données sont à l'initiative d'une seule et unique entité. C'est notamment le cas lorsqu'un navigateur web établit une connexion HTTP avec un serveur de site web désigné par son URL, puis demande lui-même des pages web qui lui sont alors transmises en retour par le serveur précité. C'est également le cas lorsqu'un serveur central d'une entreprise doit transmettre, à son initiative, des données ou des requêtes à l'un au moins de ses partenaires, par exemple pour déterminer l'état d'un stock local, ou connaître un planning local d'activité ou de livraison, ou mettre à jour des données client locales ou des grilles de

tarifs, ou encore demander un approvisionnement.

On comprendra que ces capacités à échanger des données ou des requêtes peuvent permettre à des personnes mal intentionnées de pénétrer dans les systèmes informatiques des entreprises et/ou de leurs partenaires, afin de voler des données et/ou de les infecter. Cela résulte notamment du fait que la plupart des serveurs d'application(s) disposent d'une adresse IP ou URL connue, et donc qu'un tiers peut attaquer l'entrée d'un serveur d'application(s) et par conséquent les services qui sont attachés à l'adresse IP de ce serveur d'application(s) depuis un ordinateur connecté à l'Internet.

Afin de maîtriser les risques d'intrusion et d'infection il est préférable d'effectuer une gestion et une surveillance centralisées des échanges via un point d'accès de l'entreprise, et de disposer de fonctions d'administration de la sécurité logique.

Par ailleurs, le système de communication qui supporte un échange de données doit être robuste aux aléas de fonctionnement de l'Internet (comme par exemple des (micro)coupures du fournisseur d'accès), et donc il doit permettre un rétablissement automatique du service concerné, de préférence sans intervention de celui qui n'est pas l'initiateur de l'échange (lequel est le réseau principal qui adresse une requête à un réseau local secondaire).

Plusieurs solutions ont été proposées pour tenter de remédier aux problèmes présentés ci-avant.

Une première solution consiste à relier les partenaires avec l'entreprise au moyen d'un réseau privé, éventuellement de type MPLS, fourni par un opérateur de (télé)communication. Le réseau étant privé, il peut être considéré par l'entreprise et ses partenaires comme suffisamment sûr pour mettre en œuvre des échanges bidirectionnels. Cette solution doit cependant intégrer un dispositif additionnel qui assure le cloisonnement des échanges exclusivement entre les partenaires et l'entreprise et la mise en œuvre d'une politique de droits d'accès.

On comprendra que le déploiement d'une telle solution pour une entreprise et des partenaires implantés dans une zone géographique importante (éventuellement mondiale) est relativement long et que les coûts

d'exploitation d'une telle solution peuvent s'avérer élevés. En particulier, le coût de location de l'accès au réseau privé pour un partenaire est significativement plus élevé que le coût d'un accès illimité à l'Internet.

Une deuxième solution consiste à rendre le réseau local (ou système informatique) secondaire de chaque partenaire accessible depuis l'Internet. Mais tout ordinateur appartenant à ce réseau local se retrouve couplé à l'Internet et donc exposé aux attaques de tiers malintentionnés. Ce risque est d'autant plus élevé lorsqu'un ordinateur offre des services web. En effet, l'ordinateur doit alors disposer d'une adresse réseau fixe et connue (URL ou adresse IP fixe) dans le système de noms de domaine (ou DNS (pour « Domain Name System »)) de l'Internet afin que les clients puissent accéder à ses services web. Certes les connexions peuvent être chiffrées et sécurisées afin qu'aucun tiers ne puisse lire les données échangées. En outre, chaque ordinateur qui écoute des demandes de connexion (et qui est repérable par son adresse IP et donc accessible) doit être protégé par des équipements informatiques spécifiques, comme par exemple des pare-feux (ou firewalls) ou des « proxies », et l'on doit assurer l'administration et la mise à jour (notamment sécuritaire) permanentes de ces équipements informatiques. On comprendra que l'installation, l'administration et la mise à jour de ces équipements informatiques nécessitent des compétences et du temps et s'avèrent relativement onéreuses.

Une troisième solution consiste à mettre en œuvre un réseau informatique privé virtuel (ou VPN (pour « Virtual Private Network »)) entre le réseau local principal d'une entreprise et les réseaux locaux secondaires de ses partenaires, via l'Internet. Cette solution intervient au niveau de la couche réseau IPSEC ou au niveau de la couche de transport SSL/TLS du modèle OSI (« Open Systems Interconnection »). Les connexions sont établies par les partenaires grâce à un logiciel spécialisé s'exécutant (ou implanté) dans leurs ordinateurs (ou analogues), sans nécessiter d'équipement informatique particulier au niveau de leurs réseaux locaux.

Le déploiement de cette solution a généralement deux conséquences. Tout d'abord, chaque partenaire est intégré techniquement dans le réseau local principal de l'entreprise. Ensuite, pour des raisons de

sécurité chaque ordinateur d'un partenaire est logiquement isolé par le logiciel spécialisé de tout autre réseau (réseau local secondaire du partenaire et accès logique à l'Internet via le réseau local secondaire du partenaire ou un modem), pendant la durée des échanges via le VPN, ce qui lui interdit de communiquer lui-même en temps réel avec les autres ordinateurs du réseau local secondaire auquel il est connecté. Certes, il est possible de remédier partiellement au dernier inconvénient cité en mettant en œuvre une technique de type dit « split-tunneling » assurant un accès simultané au réseau local principal de l'entreprise et à l'Internet, mais cela induit une vulnérabilité au niveau de la sécurité qui est souvent inacceptable pour une entreprise (l'ordinateur d'un partenaire peut en effet être utilisé par un tiers connecté à l'Internet pour s'introduire dans et/ou infecter le réseau local principal de l'entreprise). Cette solution ne convient donc pas aux appels d'un service web en temps réel d'un réseau local principal d'une entreprise, à l'initiative de cette dernière, vers un réseau local secondaire d'un partenaire.

Une quatrième solution consiste à contraindre chaque réseau local secondaire d'un partenaire à demander périodiquement au réseau local principal d'une entreprise s'il existe des requêtes à traiter ou des données à recevoir le concernant. Chaque demande peut être par exemple une requête HTTP, transmise du réseau local secondaire d'un partenaire vers le réseau local principal d'une entreprise, et à laquelle ce dernier répond par un message contenant une réponse négative ou des données à transférer ou bien une ou plusieurs requêtes de service web. Cette solution intervient au niveau de la couche application du modèle OSI. Chaque partenaire prenant lui-même l'initiative des échanges, il n'est donc pas nécessaire que le réseau local secondaire d'un partenaire soit accessible par une URL ou une adresse IP (publique).

L'inconvénient principal de cette solution réside dans le nombre de requêtes que le réseau local principal d'une entreprise doit recevoir et traiter. Ce nombre est en effet directement proportionnel au nombre de partenaires et à la périodicité des requêtes. Plus ce nombre est important plus l'infrastructure informatique de traitement des requêtes doit être importante, et donc plus elle est onéreuse.

Une cinquième solution, notamment décrite dans le document brevet US 2009/0300750, consiste à implanter dans l'Internet un routeur central (ou « tunnel hub ») commun à plusieurs partenaires, et dans chaque réseau local secondaire d'un partenaire une passerelle (ou « tunnel gateway »). Cette solution permet un fonctionnement parfaitement bidirectionnel, via des connexions techniques sécurisées bidirectionnelles (appelées tunnels) établies entre chaque passerelle et le routeur central à l'initiative de chaque partenaire.

Le rôle symétrique des partenaires et de l'entreprise et la nature bidirectionnelle des échanges induisent une vulnérabilité globale au niveau de la sécurité qui dépend de la plus grande des vulnérabilités des partenaires. Il est donc important que le routeur central assure un cloisonnement des échanges exclusivement entre les partenaires et l'entreprise, ce qui implique un bridage des capacités intrinsèques du routeur central par un paramétrage spécifique. L'efficacité d'un tel cloisonnement dépend alors de la qualité du paramétrage et reste dépendante d'éventuelles erreurs.

Par ailleurs, cette dernière solution ne propose pas de mécanisme destiné à assurer la robustesse des tunnels aux aléas de fonctionnement de l'Internet.

L'invention a donc pour but d'améliorer la situation, et en particulier de permettre au réseau local principal d'une entreprise d'appeler de manière sécurisée des applications privées (éventuellement de type web (ou Internet)) offertes par les réseaux locaux secondaires de ses partenaires (connectés à un réseau de communication (éventuellement l'Internet)), sans utiliser leurs éventuelles URL dans le DNS Internet ou adresses IP publiques.

Elle propose notamment à cet effet un dispositif d'aiguillage dit « principal » propre à être couplé à un réseau local principal auquel est couplée au moins une première application et qui est connecté à un réseau de communication auquel est également connecté au moins un réseau local secondaire, auquel est couplée au moins une seconde application.

Ce dispositif d'aiguillage principal se caractérise par le fait qu'il comprend des moyens d'aiguillage propres :

- à aiguiller une requête, qui est issue d'une première application, vers un

réseau local secondaire auquel est couplée une seconde application destinataire de cette requête, via un tunnel sécurisé établi via le réseau de communication entre lui et un dispositif d'aiguillage secondaire couplé à ce réseau local secondaire, et utilisable exclusivement à l'initiative d'une première application, et

- à aiguiller un message de réponse à une requête, qui est issu d'une seconde application via le tunnel sécurisé utilisé pour transmettre cette requête, vers une première application destinataire de ce message de réponse.

Un tel dispositif d'aiguillage principal impose que chaque connexion soit initiée par une première application (d'une entreprise) et interdit toute remontée d'une requête issue d'un tunnel sécurisé jusqu'à une première application.

Le dispositif d'aiguillage principal selon l'invention peut comporter d'autres caractéristiques qui peuvent être prises séparément ou en combinaison, et notamment :

- il peut comprendre des moyens de stockage propres à stocker une table d'aiguillage qui établit une correspondance entre des identifiants de réseau local secondaire et des identifiants de tunnel sécurisé utilisable. Dans ce cas, ses moyens d'aiguillage peuvent être propres à aiguiller une requête en fonction de l'identifiant de tunnel sécurisé utilisable qui correspond dans cette table d'aiguillage à l'identifiant de réseau local secondaire qui est contenu dans cette requête ;
  - ➢ les moyens de stockage peuvent être propres à stocker dans la table d'aiguillage des informations temporelles qui sont représentatives de la plus récente date à laquelle un tunnel sécurisé était utilisable en correspondance de l'identifiant de ce tunnel sécurisé utilisable ;
- ses moyens d'aiguillage peuvent comprendre des moyens de contrôle propres à identifier et authentifier un réseau local secondaire qui requiert l'établissement d'un tunnel sécurisé, et à autoriser ou interdire un tel établissement en fonction d'informations qui font partie d'une configuration définissant son fonctionnement ;
  - ➢ il peut comprendre des moyens de gestion propres à permettre la

génération de sa configuration de fonctionnement.

L'invention propose également un dispositif d'aiguillage secondaire propre à être couplé à un réseau local secondaire auquel est couplée au moins une seconde application et qui est connecté à un réseau de communication auquel est également connecté un réseau local principal, auquel est couplée au moins une première application.

Ce dispositif d'aiguillage secondaire se caractérise par le fait qu'il comprend des moyens d'aiguillage propres :

- à aiguiller une requête, qui est issue d'une première application via un tunnel sécurisé établi via le réseau de communication entre lui et un dispositif d'aiguillage principal couplé au réseau local principal, et utilisable exclusivement à l'initiative d'une première application, vers une seconde application destinataire de cette requête, et
- à aiguiller un message de réponse à une requête, qui est issu d'une seconde application, vers une première application destinataire de ce message de réponse, via le tunnel sécurisé qui a été utilisé pour transmettre cette requête.

Un tel dispositif d'aiguillage secondaire interdit tout transfert d'une requête vers une première application (d'une entreprise) via un tunnel sécurisé, et n'autorise un transfert de message de réponse vers une première application (d'une entreprise) via un tunnel sécurisé qu'à condition qu'il réponde à une requête issue d'une première application via ce même tunnel sécurisé.

Le dispositif d'aiguillage secondaire selon l'invention peut comporter d'autres caractéristiques qui peuvent être prises séparément ou en combinaison, et notamment :

- ses moyens d'aiguillage peuvent être propres à aiguiller une requête vers une seconde application destinataire en fonction d'un identifiant de communication qui est stocké dans une table d'aiguillage en correspondance de l'identifiant de cette seconde application qui est contenu dans cette requête ;
  - il peut comprendre des moyens de stockage propres à stocker la table

d'aiguillage ;

- il peut comprendre des moyens de gestion propres à permettre la génération de sa configuration de fonctionnement ;
- ses moyens d'aiguillage peuvent comprendre des moyens de contrôle propres à requérir auprès d'un dispositif d'aiguillage principal l'établissement d'un tunnel sécurisé entre lui et ce dispositif d'aiguillage principal.

L'invention propose également un système de communication comprenant un réseau local principal, auquel est couplée au moins une première application et connecté à un réseau de communication, et au moins un réseau local secondaire, auquel est couplée au moins une seconde application et connecté au réseau de communication.

Ce système se caractérise par le fait qu'il comprend en outre ;

- un dispositif d'aiguillage principal du type de celui présenté ci-avant, couplé au réseau local principal,
- des dispositifs d'aiguillage secondaires du type de celui présenté ci-avant, couplés respectivement aux réseaux locaux secondaires, et
- des tunnels sécurisés établis chacun entre le dispositif d'aiguillage principal et l'un des dispositifs d'aiguillage secondaires via le réseau de communication et utilisables chacun exclusivement à l'initiative d'une première application.

Un tel système de communication s'avère avantageusement compatible avec les infrastructures de communication existantes et assure un cloisonnement des partenaires d'une entreprise qui préserve leur sécurité et celle de cette entreprise.

Par ailleurs, un tel système s'avère particulièrement bien adapté, bien que non limitativement au cas d'une grande entreprise disposant d'un vaste réseau de partenaires, en particulier lorsque ces derniers disposent de réseaux locaux (ou systèmes informatiques) secondaires réduits et d'une compétence informatique réduite. On notera que l'invention concerne essentiellement les échanges entre une entreprise et ses partenaires, mais pas la médiation entre partenaires.

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 schématiquement et fonctionnellement un exemple de système de communication selon l'invention comportant un réseau local principal, appartenant à une entreprise, et deux réseaux locaux secondaires, appartenant à deux partenaires, interconnectés via un réseau de communication,
- la figure 2 illustre schématiquement et fonctionnellement un exemple de réalisation d'un dispositif d'aiguillage principal selon l'invention, destiné à être connecté à un réseau local principal, et
- la figure 3 illustre schématiquement et fonctionnellement un exemple de réalisation d'un dispositif d'aiguillage secondaire selon l'invention, destiné à être connecté à un réseau local secondaire.

Les dessins annexés pourront non seulement servir à compléter l'invention, mais aussi contribuer à sa définition, le cas échéant.

L'invention a pour but de permettre à un réseau local principal RLP, connecté à un réseau de communication RC et par exemple appartenant à une entreprise EN ou un groupe de sociétés, d'appeler de façon sécurisée et à son initiative des (secondes) applications ASjk privées (éventuellement de type web (ou Internet)), accessibles via des réseaux locaux secondaires RLSj connectés à ce réseau de communication RC et par exemple appartenant à des partenaires Pj de cette entreprise EN.

Dans ce qui suit, on considère, à titre d'exemple non limitatif, que le réseau local principal RLP appartient à un constructeur de véhicules automobiles EN, et que les réseaux locaux secondaires RLSj appartiennent à des partenaires Pj de ce constructeur EN, comme par exemple des concessionnaires de véhicules, des points de distribution ou de vente de véhicules et/ou de pièces de rechange ou détachées, des fournisseurs de pièces détachées ou de matériaux pour une usine, ou des entrepôts de stockage de véhicules et/ou de pièces détachées. Mais l'invention n'est pas limitée à cette application.

On a schématiquement représenté sur la figure 1 un exemple de

système de communication permettant de mettre en œuvre l'invention.

Un système de communication, selon l'invention, comprend un réseau local principal RLP, connecté à un réseau de communication RC et appartenant ici à une entreprise EN, et au moins un réseau local secondaire RLSj (ici j = 1 ou 2), connecté au réseau de communication RC et appartenant ici à un partenaire Pj de l'entreprise EN.

Dans ce qui suit, on considère, à titre d'exemple non limitatif, que le réseau de communication RC est l'Internet. Mais cela n'est pas obligatoire.

On notera que le réseau local principal RLP peut être interconnecté via le réseau de communication RC à plus de deux réseaux locaux secondaires RLSj. En fait, le nombre de réseaux locaux secondaires RLSj peut prendre n'importe quelle valeur supérieure ou égale à un.

Le réseau local principal RLP est un système informatique auquel est connecté au moins un équipement de communication dans lequel s'exécute (ou est implantée) au moins une première application APi, par exemple de type web. Il est rappelé qu'une application web est un logiciel applicatif qui offre au moins un service web et qui est manipulable au moyen d'un navigateur Internet (ou web). On notera qu'un service web peut être consommé par une autre application que la sienne et pas nécessairement par un navigateur Internet.

Par exemple, cet équipement de communication peut être un serveur d'applications web. Dans l'exemple non limitatif illustré sur la figure 1, trois premières applications AP1 à AP3 (i = 1 à 3) sont accessibles via le réseau local principal RLP. Ces premières applications APi peuvent être implantées dans un ou plusieurs équipements de communication (non représentés).

On notera que le réseau local principal RLP peut éventuellement, et comme illustré non limitativement, être connecté au réseau de communication RC par l'intermédiaire d'un routeur MR et/ou d'un module de protection MP, comme par exemple un pare-feu ou une « zone démilitarisée » (ou DMZ - zone délimitée par deux pare-feux et comportant de multiples équipements de sécurité tels que des proxies ou des passerelles applicatives).

Chaque réseau local secondaire RLSj est un système informatique auquel est connecté au moins un équipement de communication dans lequel

s'exécute (ou est implantée) au moins une seconde application ASjk, par exemple de type web.

Par exemple, cet équipement de communication peut être un serveur d'applications web. Dans l'exemple non limitatif illustré sur la figure 1, trois secondes applications AS11 à AS13 (j = 1 et k = 1 à 3) sont accessibles via le premier réseau local secondaire RLS1, et deux secondes applications AS21 à AS22 (j = 2 et k = 1 ou 2) sont accessibles via le second réseau local secondaire RLS2. Les secondes applications ASjk de chaque réseau local secondaire RLSj peuvent être implantées dans un ou plusieurs équipements de communication (non représentés).

On notera que l'un au moins des réseaux locaux secondaires RLSj peut éventuellement, et comme illustré non limitativement, être connecté au réseau de communication RC par l'intermédiaire d'un routeur MR et/ou d'un module de protection MP, comme par exemple un pare-feu ou une zone démilitarisée.

L'invention propose, d'une première part, de connecter au réseau local principal RLP un dispositif d'aiguillage principal DP, d'une deuxième part, de connecter à chaque réseau local secondaire RLSj un dispositif d'aiguillage secondaire DSj, et, d'une troisième part, d'établir des tunnels sécurisés Tj entre le dispositif d'aiguillage principal DP et respectivement les différents dispositifs d'aiguillage secondaires DSj, via le réseau de communication RC, chaque tunnel sécurisé Tj n'étant utilisable exclusivement qu'à l'initiative d'une première application APi.

Il est important de noter que l'entreprise EN pourrait mettre en œuvre simultanément plusieurs dispositifs d'aiguillage principaux DP, par exemple pour répartir les tunnels sécurisé Tj sur plusieurs serveurs en parallèle gérant des ensembles disjoints de partenaires Pj. De même, un partenaire Pj pourrait mettre en œuvre simultanément plusieurs dispositifs d'aiguillage secondaires DSj établissant chacun des tunnels sécurisés Tj avec des dispositifs d'aiguillage principaux DP différents appartenant à une ou plusieurs entreprises EN.

On a schématiquement représenté sur la figure 2 un exemple de réalisation de dispositif d'aiguillage principal DP selon l'invention. Comme

illustré, un tel dispositif d'aiguillage principal DP comprend au moins des moyens d'aiguillage MAP agencés de manière à effectuer deux types d'aiguillage.

Le premier type d'aiguillage concerne les requêtes qui sont générées par une première application APi et qui sont destinées à l'une au moins des secondes applications ASjk accessibles par l'un au moins des réseaux locaux secondaires RLSj. Plus précisément, les moyens d'aiguillage MAP sont propres à aiguiller une requête, issue d'une première application APi, vers un réseau local secondaire RLSj auquel est couplée une seconde application ASjk qui en est le destinataire, via un tunnel sécurisé Tj établi entre le dispositif d'aiguillage principal DP et le dispositif d'aiguillage secondaire DSj qui est couplé à ce réseau local secondaire RLSj.

Le second type d'aiguillage concerne les messages de réponse qui ont été générés par une seconde application ASjk et qui sont destinés à l'une au moins des premières applications APi accessibles par le réseau local principal RLP. Plus précisément, les moyens d'aiguillage MAP sont propres à aiguiller un message de réponse, généré par une seconde application ASjk en réponse à une requête et transmis via le tunnel sécurisé Tj précédemment utilisé pour transmettre cette requête, vers une première application APi qui en est le destinataire.

Ainsi, une personne mal intentionnée qui arriverait à se connecter au réseau local secondaire RLSj d'un partenaire Pj ne peut adresser aucune requête de service à l'entreprise EN en utilisant le tunnel sécurisé Tj préétabli entre le dispositif d'aiguillage secondaire DSj (qui est couplé à ce réseau local secondaire RLSj) et le dispositif d'aiguillage principal DP. Cela constitue par conception une barrière de sécurité intrinsèque, et ainsi un avantage par rapport aux solutions de l'art antérieur, notamment du fait qu'il n'y a pas de paramètre (pouvant être erroné) à positionner par exemple pour interdire les requêtes des partenaires Pj vers l'entreprise EN, ou le cloisonnement des échanges exclusivement entre les partenaires Pj et l'entreprise EN.

Une requête comprend un identifiant désignant la seconde application ASjk qui en est le destinataire et un identifiant désignant le réseau local secondaire RLSj auquel est couplée cette seconde application ASjk. Dans le

cas du format SOAP, ces identifiants peuvent être indiqués dans l'entête de la requête.

De préférence, l'identifiant d'une seconde application ASjk n'est pas une « adresse de communication publique », comme par exemple une URL ou une adresse IP du domaine DNS de l'Internet. Il s'agit par exemple d'un ensemble de caractères alphanumériques dont la signification est connue du dispositif d'aiguillage secondaire DSj qui est couplé au réseau local secondaire RLSj concerné. De même, l'identifiant d'un réseau local secondaire RLSj n'est pas une « adresse de communication », de préférence. Il s'agit par exemple d'un ensemble de caractères alphanumériques qui désigne un tunnel sécurisé Tj établi entre le dispositif d'aiguillage principal DP et le dispositif d'aiguillage secondaire DSj qui est connecté au réseau local secondaire RLSj.

A cet effet, le dispositif d'aiguillage principal DP peut comprendre des moyens de stockage MSP propres à stocker une table d'aiguillage établissant une correspondance entre des identifiants de réseau local secondaire RLSj et des identifiants de tunnel sécurisé Tj utilisable. Ces moyens de stockage MSP peuvent se présenter sous n'importe quelle forme, y compris logicielle. Par conséquent il pourra s'agir d'une mémoire, d'un registre, d'un fichier sur un disque de stockage ou d'une base de données dans une mémoire ou un disque de stockage.

Dans ce cas, les moyens d'aiguillage MAP sont agencés pour aiguiller une requête en fonction de l'identifiant de tunnel sécurisé Tj utilisable qui correspond dans la table d'aiguillage à l'identifiant de réseau local secondaire RLSj qui est contenu dans cette requête.

On notera que lorsque le réseau local principal RLP comprend un module de protection (ou une barrière de sécurité) MP, il suffit qu'il soit configuré de manière à accepter et laisser passer jusqu'au dispositif d'aiguillage principal DP les flux qui entrent sur un port qui a été attribué à la connexion des tunnels sécurisés Tj, comme par exemple le port 443 qui est utilisé par défaut pour les flux HTTPS (mais tout autre port peut être utilisé à la convenance de l'entreprise EN). C'est l'un des avantages du système de communication selon l'invention que de ne pas imposer d'autre pré-requis au

niveau des barrières de sécurité MP, en particulier auprès des partenaires Pj qui ne sont pas obligés de modifier la configuration de leur sécurité existante pour mettre en œuvre l'invention. On notera également que le fonctionnement du système de communication selon l'invention n'est pas altéré en cas d'absence de barrière de sécurité MP chez un partenaire Pj et/ou chez l'entreprise EN.

Afin de mettre en œuvre leurs fonctionnalités, les moyens d'aiguillage MAP peuvent, comme illustré non limitativement sur la figure 2, comprendre des moyens de contrôle MCP, un serveur SHP (par exemple de type HTTP), un client CHP (par exemple de type HTTP), un module de détermination de tunnel (ou « dispatcher de tunnel ») MDP, ainsi que les moyens de stockage MSP (présentés ci-avant) et un éventuel (mais avantageux) module de vérification MVP. Dans ce cas, les moyens d'aiguillage MAP peuvent être réalisés d'une façon similaire à un serveur d'application standard.

Le serveur SHP constitue une interface d'accès pour les premières applications APi. Cette interface, par exemple HTTP, peut traiter des services web qui s'appuient notamment sur un format standard tel que SOAP, ou sur un format de messages XML ou encore sur un format propriétaire quelconque. On notera que ce serveur SHP pourrait être d'un autre type si l'on utilisait un autre protocole que HTTP.

Les moyens de contrôle MCP constituent une interface de tunnel, par exemple de type SSL/TLS. Ils sont propres au moins à recevoir, identifier, authentifier et autoriser (ou refuser) les demandes de création de tunnel sécurisé Tj qui proviennent préférentiellement des dispositifs d'aiguillage secondaires DSj, et éventuellement à recevoir d'éventuels « signaux de vie » issus des dispositifs d'aiguillage secondaires DSj, destinés à l'éventuel module de vérification MVP et sur lesquels on reviendra plus loin. Cette interface de tunnel MCP utilise, par exemple, le protocole TCP/IP sécurisé par SSL/TLS, ou un protocole de niveau supérieur comme HTTPS.

L'identification et l'authentification mutuelles des partenaires Pj et de l'entreprise EN peut être réalisée au moyen du protocole SSL/TLS en utilisant des certificats électroniques, par exemple. Elle sert à établir un tunnel sécurisé Tj.

La fonction de contrôle de l'autorisation des partenaires Pj à établir un tunnel sécurisé Tj avec le dispositif d'aiguillage principal DP peut être gérée à l'aide d'éventuels moyens de gestion MGP, sur lesquels on reviendra plus loin. Elle sert à autoriser ou interdire l'utilisation d'un tunnel sécurisé Tj qui vient juste d'être établi.

On notera que l'identification, l'authentification et l'autorisation pourraient être effectuées dans une même étape au lieu de deux étapes. Dans ce cas, lorsque le dispositif d'aiguillage principal DP reçoit une requête d'établissement de tunnel sécurisé Tj d'un dispositif d'aiguillage secondaire DSj, il procède à l'identification, l'authentification et l'autorisation et ce n'est qu'à condition que ces trois opérations se sont déroulées correctement que le tunnel sécurisé Tj est établi.

L'éventuel module de vérification MVP a pour fonction de traiter les signaux de vie des partenaires Pj pour gérer les tunnels sécurisés. Ces signaux de vie sont des messages qui peuvent être transmis par les dispositifs d'aiguillage secondaires DSj, de préférence périodiquement, dans leurs tunnels sécurisés Tj respectifs afin de déterminer si ces derniers sont encore utilisables (ou activés). En effet, les tunnels sécurisés Tj étant préférentiellement établis à l'initiative des dispositifs d'aiguillage secondaires DSj, ces derniers (DSj) ont régulièrement besoin de savoir s'ils sont toujours actifs (ou utilisables ou encore ouverts) afin, lorsque ce n'est pas le cas, de requérir immédiatement leur ré-établissement. Lorsque le module de vérification MVP reçoit des signaux de vie associés à un tunnel sécurisé Tj, il en déduit que ce tunnel sécurisé Tj est toujours actif. Le module de vérification MVP adresse alors un accusé de réception au dispositif d'aiguillage secondaire DSj qui est à l'autre extrémité de ce tunnel sécurisé Tj utilisable (ou actif), ce qui l'informe de la situation. Dans le cas contraire, le module de vérification MVP peut ne rien faire, et donc l'absence de réception d'un accusé de réception informe de la situation le dispositif d'aiguillage secondaire DSj concerné.

L'instant de réception de ces signaux de vie par le module de vérification MVP peut constituer un marquage temporel (ou horodatage) qui constitue des informations temporelles représentatives de la plus récente date

à laquelle un tunnel sécurisé Tj a été utilisé et qui peuvent être stockées par les moyens de stockage MSP dans la table d'aiguillage en correspondance de l'identifiant de ce tunnel sécurisé Tj utilisable.

Un signal de vie peut, par exemple, être un message court comportant typiquement un identifiant (sur quelques octets). Il peut, par exemple, être transmis toutes les 60 secondes (mais n'importe quelle autre période peut être utilisée selon les besoins).

On notera que lorsqu'un tunnel sécurisé Tj n'est plus utilisable, son identifiant est préférentiellement supprimé, ou bien associé à une marque spécifique au sein, de la table d'aiguillage ou bien associé à une marque spécifique.

On notera également que le dispositif d'aiguillage principal DP peut comprendre un système d'exploitation SE, par exemple de type standard.

Par ailleurs, comme évoqué plus haut, le dispositif d'aiguillage principal DP peut comprendre des moyens de gestion MGP propres, au moins, à permettre la génération d'une configuration de fonctionnement pour le dispositif d'aiguillage principal DP.

Ces moyens de gestion MGP peuvent, comme illustré non limitativement sur la figure 2, comprendre un serveur SHP', par exemple de type HTTP, et un module d'administration MNP.

La génération d'une configuration de fonctionnement peut être contrôlée par l'interface homme-machine d'un terminal d'administration TGP. Plus précisément, ce dernier (TGP) permet à l'entreprise EN de paramétrer le fonctionnement du dispositif d'aiguillage principal DP au sein d'une configuration qui est par exemple stockée dans une base de configuration MSP'. Ce paramétrage peut être similaire à celui d'un modem ADSL. Il peut par exemple concerner des temporisations, des dates de déclenchement d'action(s) ou de fin d'action(s), des adresses de communication (URL ou IP), des paramètres de gestion de la sécurité (ports TCP/IP, profils d'administrateur), des paramètres d'interface avec l'annuaire des partenaires Pj et avec l'annuaire des services web, des paramètres indiquant les fichiers journaux, des paramètres indiquant le fichier magasin de certificats, ou des paramètres d'activation d'options de fonctionnement.

Ces moyens de gestion MGP peuvent également et éventuellement permettre au terminal d'administration TGP de piloter les moyens d'aiguillage MAP.

On notera que la base de configuration MSP' peut également stocker la liste des identifiants des réseaux locaux secondaires RLSj des partenaires Pj en correspondance de certificats électroniques associés.

Dans une première variante de réalisation, les moyens d'aiguillage MAP peuvent être raccordés à une base de données B1 stockant un annuaire des partenaires Pj géré et administré par une application spécifique. Cet annuaire peut contenir les identifiants des partenaires Pj ainsi que d'autres données administratives et/ou de sécurité associées à chaque partenaire Pj. Le dispositif d'aiguillage principal DP peut, par exemple, s'interfacer avec cet annuaire et exploiter directement ses données pour réaliser la fonction de vérification des identifiants des partenaires Pj et le contrôle de leurs droits (notamment de création de tunnels sécurisés).

Dans une deuxième variante de réalisation, les moyens d'aiguillage MAP peuvent être raccordés à une autre base de données B2 stockant un annuaire des services web (ou secondes applications ASjk) des partenaires Pj géré et administré par une application spécifique. Cet annuaire peut contenir des données administratives et/ou de sécurité associées à chaque service web (ou seconde application ASjk). Le dispositif d'aiguillage principal DP peut, par exemple, s'interfacer avec cet annuaire et exploiter directement ses données pour réaliser des fonctions de contrôle de validité des requêtes émises par les premières applications APi, ou de vérification de conformité des services web demandés, ou encore de contrôle / filtrage des droits des premières applications APi à envoyer des requêtes aux partenaires.

Dans une troisième variante de réalisation, notamment lorsque les requêtes de services web se limitent à transmettre une même information à plusieurs partenaires Pj, les premières applications APi peuvent indiquer dans une même requête les identifiants de plusieurs partenaires Pj destinataires.

En résumé le dispositif d'aiguillage principal DP peut, par exemple, gérer en parallèle cinq événements : le traitement des demandes de tunnel sécurisé Tj émanant des dispositifs d'aiguillage secondaires DSj des

partenaires Pj, le traitement des requêtes de services web provenant des premières applications APi et destinées aux secondes applications ASjk des partenaires Pj, le traitement des messages de réponse de services web provenant des secondes applications ASjk et destinées aux premières applications APi, le traitement des signaux de vie et des demandes de suppression de tunnel sécurisé Tj émanant des dispositifs d'aiguillage secondaires DSj, et le traitement des ordres de fermeture du dispositif d'aiguillage principal DP à la demande de l'administrateur du réseau local principal RLP via le terminal d'administration TGP.

On notera que le dispositif d'aiguillage principal DP peut être réalisé sous la forme d'un équipement matériel spécialisé (comme par exemple un appareil (ou en anglais « appliance » - ordinateur spécialisé installable dans un centre de données (ou « datacenter »)), ou une « BOX ADSL » ou « BOX TV » contenant un ordinateur spécialisé) intégrant un logiciel spécialisé assurant les fonctions décrites ci-avant, ou bien d'un logiciel spécialisé assurant les fonctions décrites ci-avant et installé dans un équipement de communication, comme par exemple un terminal ou un ordinateur standard (éventuellement de type portable) muni d'un système d'exploitation standard, ou bien une tablette tactile, ou encore un assistant personnel numérique (ou PDA).

On a schématiquement représenté sur la figure 3 un exemple de réalisation de dispositif d'aiguillage secondaire DSj selon l'invention. Comme illustré, un tel dispositif d'aiguillage secondaire DSj comprend au moins des moyens d'aiguillage MAS agencés de manière à effectuer deux types d'aiguillage.

Le premier type d'aiguillage concerne les requêtes qui sont issues d'une première application APi via un tunnel sécurisé Tj et qui sont destinées à l'une au moins des secondes applications ASjk accessibles par le réseau local secondaire RLSj auquel le dispositif d'aiguillage secondaire DSj est couplé. Plus précisément, les moyens d'aiguillage MAS sont propres à aiguiller une requête, issue d'une première application APi via un tunnel sécurisé Tj, vers une (chaque) seconde application ASjk destinataire de cette requête.

Le second type d'aiguillage concerne les messages de réponse qui ont été générés par une seconde application ASjk en réponse à une requête transmise via un tunnel sécurisé Tj, et qui sont destinés à l'une au moins des premières applications APi accessibles par le réseau local principal RLP. Plus précisément, les moyens d'aiguillage MAS sont propres à aiguiller un message de réponse, généré par une seconde application ASjk en réponse à une requête, vers une première application APi qui en est le destinataire, via le tunnel sécurisé Tj précédemment utilisé pour transmettre cette requête.

Un message de réponse comprend au moins un identifiant désignant la première application APi qui en est le destinataire. Dans le cas du format SOAP, cet identifiant peut être indiqué dans l'entête du message de réponse.

De préférence, l'identifiant d'une première application APi n'est pas une « adresse de communication publique », comme par exemple une URL ou une adresse IP du domaine DNS de l'Internet. Il s'agit par exemple d'un ensemble de caractères alphanumériques dont la signification est connue du dispositif d'aiguillage principal DP.

On notera que pour effectuer les aiguillages du premier type, le dispositif d'aiguillage secondaire DSj peut comprendre des moyens de stockage MSS propres à stocker une table d'aiguillage établissant une correspondance entre des identifiants de seconde application ASjk et des identifiants de communication de seconde application ASjk, comme par exemple des URLs ou des adresses IP du domaine DNS de l'Internet. Ces moyens de stockage MSS peuvent se présenter sous n'importe quelle forme, y compris logicielle. Par conséquent il pourra s'agir d'une mémoire, d'un registre, d'un fichier sur un disque de stockage ou d'une base de données dans une mémoire ou un disque de stockage.

Dans ce cas, les moyens d'aiguillage MAS sont agencés pour aiguiller une requête reçue de leur tunnel sécurisé Tj en fonction de l'identifiant de communication de la seconde application ASjk destinataire qui correspond dans la table d'aiguillage à l'identifiant de cette seconde application ASjk qui est contenu dans cette requête.

On notera qu'un avantage de l'invention réside dans le fait qu'un réseau local secondaire n'est pas obligé d'ouvrir des ports en lecture sur le

réseau Internet. Effectivement, les flux de questions (ou requêtes) en provenance du réseau principal, via le tunnel sécurisé associé, vont circuler du réseau principal vers le réseau local secondaire, mais le port 443 (par exemple) n'a pas à être ouvert dans le réseau local secondaire pour cela. Le port 443 (par exemple) doit en revanche être ouvert dans le réseau principal pour permettre au dispositif d'aiguillage secondaire d'atteindre la passerelle et d'établir un tunnel sécurisé.

Afin de mettre en œuvre leurs fonctionnalités, les moyens d'aiguillage MAS peuvent, comme illustré non limitativement sur la figure 3, comprendre des moyens de contrôle MCS, un serveur SHS (par exemple de type HTTP), un client CHS (par exemple de type HTTP), et un éventuel (mais avantageux) module de vérification MVS. Dans ce cas, les moyens d'aiguillage MAS peuvent être réalisés d'une façon similaire à un serveur d'application standard.

Les moyens de contrôle MCS constituent une interface de tunnel, par exemple de type SSL/TLS. Ils sont propres à gérer leur tunnel sécurisé Tj, notamment sa requête d'établissement. Ils sont client des moyens de contrôle MCS du dispositif d'aiguillage principal DP. Ils sont par ailleurs chargés d'authentifier le dispositif d'aiguillage principal DP qui leur adresse des requêtes. Ils peuvent être également chargés de transmettre les éventuels signaux de vie générés par le module de vérification MVS. Cette interface de tunnel MCS utilise, par exemple, le protocole TCP/IP sécurisé par SSL/TLS, ou un protocole de niveau supérieur comme HTTPS.

Le serveur SHS a pour fonction de traiter les requêtes de services web (transmises par les moyens de contrôle MCS associés) et de les transmettre au client CHS.

Le client CHS a pour fonction de transmettre chaque requête de service web (transmise par le serveur SHS) vers chaque seconde application ASjk qui en est le destinataire après avoir déterminé son adresse de communication, stockée dans la table d'aiguillage en correspondance de son identifiant contenu dans la requête.

L'éventuel module de vérification MVS est chargé de traiter les accusés de réception reçus qui correspondent aux signaux de vie qu'ils

génèrent, et d'ordonner aux moyens de contrôle MCS de requérir le ré-établissement du tunnel sécurisé Tj lorsqu'il n'a pas reçu d'accusé de réception.

Le mécanisme de gestion des coupures intempestives de tunnel sécurisé Tj constitue un avantage du système de communication selon l'invention, étant donné qu'il le rend raisonnablement robuste aux aléas de coupure des communications de type « bout-en-bout », ou à un arrêt momentané du dispositif d'aiguillage principal DP. Sans ce mécanisme, la coupure d'un tunnel sécurisé Tj serait définitive et l'entreprise EN perdrait la capacité d'adresser des requêtes en temps réel à une partie de ses partenaires Pj. Le trafic global généré par les signaux de vie des dispositifs d'aiguillage secondaires DSj est maîtrisable, même avec un grand nombre de partenaires et une périodicité de l'ordre de la minute.

On notera également qu'un dispositif d'aiguillage secondaire DSj peut comprendre un système d'exploitation SE, par exemple de type standard.

Par ailleurs, comme évoqué plus haut, un dispositif d'aiguillage secondaire DSj peut comprendre des moyens de gestion MGS propres, au moins, à permettre la génération d'une configuration de fonctionnement pour le dispositif d'aiguillage secondaire DSj.

Ces moyens de gestion MGS peuvent, comme illustré non limitativement sur la figure 3, comprendre un serveur SHS', par exemple de type HTTP, et un module d'administration MNS.

La génération d'une configuration de fonctionnement peut être contrôlée par l'interface homme-machine d'un terminal d'administration TGSj. Plus précisément, ce dernier (TGSj) permet au partenaire Pj de paramétrer le fonctionnement du dispositif d'aiguillage secondaire DSj au sein d'une configuration qui est par exemple stockée dans les moyens de stockage MSS (qui stockent également la table d'aiguillage), ou bien dans d'autres moyens de stockage dédiés.

Ces moyens de gestion MGS peuvent également et éventuellement permettre au terminal d'administration TGSj de piloter les moyens d'aiguillage MAS.

On notera que les moyens de stockage MSS peuvent également

stocker le certificat électronique de l'entreprise EN qui sert aux moyens de contrôle MCS lors de leurs authentifications. En variante ou en complément, les moyens de stockage MSS peuvent contenir l'identifiant de l'entreprise EN et les certificats des autorités de certification reconnues pour l'émission du certificat de l'entreprise EN. Seule l'entreprise EN désignée pourra être en session avec le dispositif d'aiguillage secondaire DSj. Cela permet en particulier de mettre en place un contrôle d'habilitation dès le début de session.

Dans une première variante de réalisation, les moyens d'aiguillage MAS, les moyens de gestion MGS et les moyens de stockage MSS pourraient être installés dans le même équipement que celui qui contient l'une au moins des secondes applications ASjk d'un partenaire Pj. Cet équipement peut être un serveur ou un ordinateur (éventuellement portable), ou un terminal de communication quelconque disposant d'un système d'exploitation standard. Dans ce cas, les URLs d'accès aux secondes applications ASjk peuvent être simplifiées et peuvent désigner l'équipement (« localhost »).

Dans une deuxième variante de réalisation, les moyens de gestion MGS pourraient être installés dans le dispositif d'aiguillage principal DP, permettant ainsi une administration centralisée des dispositifs d'aiguillage secondaires DSj des partenaires Pj.

Dans une troisième variante de réalisation, la table d'aiguillage d'un dispositif d'aiguillage secondaire DSj peut être stockée dans la base de configuration MSP' du dispositif d'aiguillage principal DP, permettant ainsi une administration centralisée des configurations des dispositifs d'aiguillage secondaires DSj des partenaires Pj.

Dans une quatrième variante de réalisation, la liste des identifiants de seconde application ASjk pourrait être initialisée et mise à jour dans la table d'aiguillage de chaque dispositif d'aiguillage secondaire DSj par le dispositif d'aiguillage principal DP. Par exemple, cette mise à jour pourrait avoir lieu par échange de données entre le dispositif d'aiguillage principal DP et le dispositif d'aiguillage secondaire DSj au moment où ce dernier requiert l'établissement de son tunnel sécurisé Tj.

Optionnellement, un dispositif d'aiguillage secondaire DSj peut mettre

en œuvre un mécanisme d'alerte lorsque la configuration de sa table d'aiguillage n'est pas correcte (par exemple du fait d'erreurs de saisie), ou lorsqu'un serveur du réseau local secondaire RLSj du partenaire Pj n'est pas joignable par son dispositif d'aiguillage secondaire DSj (par exemple par ce qu'un serveur est éteint, ou en raison d'un changement de nom d'un serveur, ou d'un changement d'adresse de serveurs lorsque la table d'aiguillage le désigne par une URL qui contient son adresse IP). Ce mécanisme d'alerte peut alerter le partenaire Pj et/ou l'entreprise EN par différents moyens usuels (par exemple un courriel ou un appel signalé dans le journal des messages).

Egalement optionnellement, un dispositif d'aiguillage secondaire DSj peut mettre en œuvre un mécanisme de sécurité logique permettant à son partenaire Pj de contrôler le filtrage des requêtes de service web en provenance de l'entreprise EN qu'il autorise vers son réseau local secondaire RLSj (par exemple pour filtrer les droits ou les horaires).

Dès qu'un dispositif d'aiguillage secondaire DSj a établi un tunnel sécurisé Tj avec le dispositif d'aiguillage principal DP, il peut gérer en parallèle trois événements : le relai des requêtes et des messages de réponse des services web (première APi et secondes ASjk applications), l'envoie périodique d'un signal de vie au dispositif d'aiguillage principal DP et le traitement des demandes de fermeture de tunnel sécurisé Tj qui peuvent être à l'initiative du partenaire Pj via le terminal d'administration TGSj.

On notera que l'implantation d'un dispositif d'aiguillage secondaire DSj ne nécessite aucune modification du système d'exploitation standard. Notamment, il ne nécessite pas de remplacer les composants logiciels standards de la pile de communication TCP/IP. Son implantation est ainsi facilitée et ses moyens d'aiguillage MAS et moyens de gestion MGS peuvent cohabiter plus aisément avec d'autres applications sur un même équipement.

On notera également qu'un dispositif d'aiguillage secondaire DSj peut être réalisé sous la forme d'un équipement matériel spécialisé (comme par exemple un équipement boîtier ressemblant à un modem ou un routeur ADSL, de petite taille et comportant un ordinateur) intégrant un logiciel spécialisé assurant les fonctions décrites ci-avant, ou bien d'un logiciel spécialisé assurant les fonctions décrites ci-avant et installé dans un

équipement de communication, comme par exemple un terminal ou un ordinateur standard (éventuellement de type portable) muni d'un système d'exploitation standard, ou bien une tablette tactile, ou encore un assistant personnel numérique (ou PDA), qui peut également et éventuellement faire fonctionner les secondes applications ASjk (lesquelles peuvent être éventuellement des applications personnelles répondant à des requêtes par service web).

On notera également qu'il n'est pas obligatoire qu'un dispositif d'aiguillage secondaire DSj soit accessible par l'Internet. C'est d'ailleurs l'un des avantages du système de communication selon l'invention. Cependant, cela est possible, et le fonctionnement du système de communication selon l'invention n'est pas altéré lorsque les secondes applications ASjk des partenaires Pj sont accessibles par l'Internet.

On notera également que l'invention n'interdit pas qu'une seconde application ASjk d'un partenaire Pj envoie des requêtes de service web vers l'entreprise EN (comme illustré par la ligne en tirets de la figure 1). A cet effet, les services web (ou premières applications) APi offert(e)s par l'entreprise EN peuvent être rendu(e)s accessibles via l'Internet (par exemple à une adresse de type « www.entreprise.com »), tout en étant protégé(e)s par le module de protection MP, un mécanisme d'authentification instauré par l'entreprise EN (par exemple par certificat numérique) et le chiffrement des flux par le protocole HTTPS.

L'invention offre plusieurs avantages et notamment :

- chaque dispositif d'aiguillage secondaire vient compléter l'infrastructure informatique d'un partenaire, et donc ce dernier n'est pas obligé de modifier les caractéristiques et la configuration de sa liaison Internet (notamment il n'est pas obligé d'avoir une adresse URL entrante déclarée sur l'Internet et peut conserver privés les services web de ses secondes applications),
- l'installation d'un dispositif d'aiguillage secondaire est aussi simple que celle d'un modem ADSL ou d'un logiciel sur un ordinateur. Elle peut donc être effectuée par un partenaire sans qu'il ait besoin de faire appel à des compétences externes ou d'une formation spécifique,

- l'implantation du système de communication peut se faire pour un coût raisonnable y compris lorsque le nombre de partenaires est (très) élevé,
- elle ne nécessite aucune implantation d'équipement intermédiaire dans le réseau de communication public (ou « hub »), ce qui permet d'éviter des surcoûts et des opérations d'implantation et de maintenance,
- elle offre un niveau de sécurité mieux maîtrisé pour l'entreprise du fait de son caractère unidirectionnel, et répond au besoin de cloisonnement des partenaires (démarche de réduction au strict nécessaire de la surface d'attaque),
- chaque dispositif d'aiguillage principal vient compléter l'infrastructure informatique d'une entreprise, et donc cette dernière n'est pas obligée de modifier l'infrastructure d'accès à ses services web qu'elle fournit déjà à ses partenaires,
- elle permet d'améliorer la robustesse aux déconnexions et coupures intempestives sur l'Internet, ou aux arrêts intempestifs du dispositif d'aiguillage principal ou d'un équipement réseau intermédiaire, ou en cas d'interruption programmée par un équipement réseau intermédiaire.

L'invention ne se limite pas aux modes de réalisation de dispositif d'aiguillage principal, de dispositif d'aiguillage secondaire et de système de communication 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.

REVENDICATIONS

1. Dispositif d'aiguillage principal (DP) propre à être couplé à un réseau local principal (RLP) auquel est couplée au moins une première application (APi) et connecté à un réseau de communication (RC) auquel sont également connectés au moins un réseau local secondaire (RLSj), auquel est couplée au moins une seconde application (ASjk), caractérisé en ce qu'il comprend des moyens d'aiguillage (MAP) propres i) à aiguiller une requête, issue d'une première application (APi), vers un réseau local secondaire (RLSj) auquel est couplée une seconde application (ASjk) destinataire de cette requête, via un tunnel sécurisé établi via ledit réseau de communication (RC) entre ledit dispositif (DP) et un dispositif d'aiguillage secondaire (DSj) couplé à ce réseau local secondaire (RLSj), et utilisable exclusivement à l'initiative d'une première application (APi), et ii) à aiguiller un message de réponse à une requête, issu d'une seconde application (ASjk) via le tunnel sécurisé utilisé pour transmettre cette requête, vers une première application (APi) destinataire de ce message de réponse.

2. Dispositif selon la revendication 1, caractérisé en ce qu'il comprend des moyens de stockage (MSP) propres à stocker une table d'aiguillage établissant une correspondance entre des identifiants de réseau local secondaire (RLSj) et des identifiants de tunnel sécurisé utilisable, et en ce que lesdits moyens d'aiguillage (MAP) sont propres à aiguiller une requête en fonction de l'identifiant de tunnel sécurisé utilisable qui correspond dans ladite table d'aiguillage à l'identifiant de réseau local secondaire (RLSj) contenu dans cette requête.

3. Dispositif selon la revendication 2, caractérisé en ce que lesdits moyens de stockage (MSP) sont propres à stocker dans ladite table d'aiguillage des informations temporelles représentatives de la plus récente date à laquelle un tunnel sécurisé était utilisable en correspondance de l'identifiant de ce tunnel sécurisé utilisable.

4. Dispositif selon l'une des revendications 1 à 3, caractérisé en ce que lesdits moyens d'aiguillage (MAP) comprennent des moyens de contrôle

(MCP) propres à identifier et authentifier un réseau local secondaire (RLSj) requérant l'établissement d'un tunnel sécurisé, et à autoriser ou interdire un tel établissement en fonction d'informations faisant partie d'une configuration définissant le fonctionnement dudit dispositif (DP).

5. Dispositif selon la revendication 4, caractérisé en ce qu'il comprend des moyens de gestion (MGP) propres à permettre la génération de ladite configuration de fonctionnement dudit dispositif (DP).

6. Dispositif d'aiguillage secondaire (DSj) propre à être couplé à un réseau local secondaire (RLSj) auquel est couplée au moins une seconde application (ASjk) et connecté à un réseau de communication (RC) auquel est également connecté un réseau local principal (RLP), auquel est couplée au moins une première application (APi), caractérisé en ce qu'il comprend des moyens d'aiguillage (MAS) propres i) à aiguiller une requête, issue d'une première application (APi) via un tunnel sécurisé établi via ledit réseau de communication (RC) entre ledit dispositif (DSj) et un dispositif d'aiguillage principal (DP) couplé audit réseau local principal (RLP), et utilisable exclusivement à l'initiative d'une première application (APi), vers une seconde application (ASjk) destinataire de cette requête, et ii) à aiguiller un message de réponse à une requête, issu d'une seconde application (ASjk), vers une première application (APi) destinataire de ce message de réponse, via le tunnel sécurisé utilisé pour transmettre cette requête.

7. Dispositif selon la revendication 6, caractérisé en ce que lesdits moyens d'aiguillage (MAS) sont propres à aiguiller une requête vers une seconde application (ASjk) destinataire en fonction d'un identifiant de communication qui est stocké dans une table d'aiguillage en correspondance de l'identifiant de cette seconde application (ASjk) qui est contenu dans cette requête.

8. Dispositif selon la revendication 7, caractérisé en ce qu'il comprend des moyens de stockage (MSS) propres à stocker ladite table d'aiguillage.

9. Dispositif selon l'une des revendications 6 à 8, caractérisé en ce qu'il comprend des moyens de gestion (MGS) propres à permettre la génération d'une configuration de fonctionnement dudit dispositif (DSj).

10. Dispositif selon l'une des revendications 6 à 9, caractérisé en ce que

lesdits moyens d'aiguillage (MAS) comprennent des moyens de contrôle (MCS) propres à requérir auprès d'un dispositif d'aiguillage principal (DP) l'établissement d'un tunnel sécurisé entre ce dernier (DP) et ledit dispositif (DSj).

11. Système de communication comprenant un réseau local principal (RLP), auquel est couplée au moins une première application (APi) et connecté à un réseau de communication (RC), et au moins un réseau local secondaire (RLSj), auquel est couplée au moins une seconde application (ASjk) et connecté audit réseau de communication (RC), caractérisé en ce qu'il comprend en outre i) un dispositif d'aiguillage principal (DP) selon l'une des revendications 1 à 5, couplé audit réseau local principal (RLP), ii) des dispositifs d'aiguillage secondaires (DSj) selon l'une des revendications 6 à 10, couplés respectivement auxdits réseaux locaux secondaires (RLSj), et iii) des tunnels sécurisés établis chacun entre ledit dispositif d'aiguillage principal (DP) et l'un desdits dispositifs d'aiguillage secondaires (DSj) via ledit réseau de communication (RC) et utilisables chacun exclusivement à l'initiative d'une première application (APi).

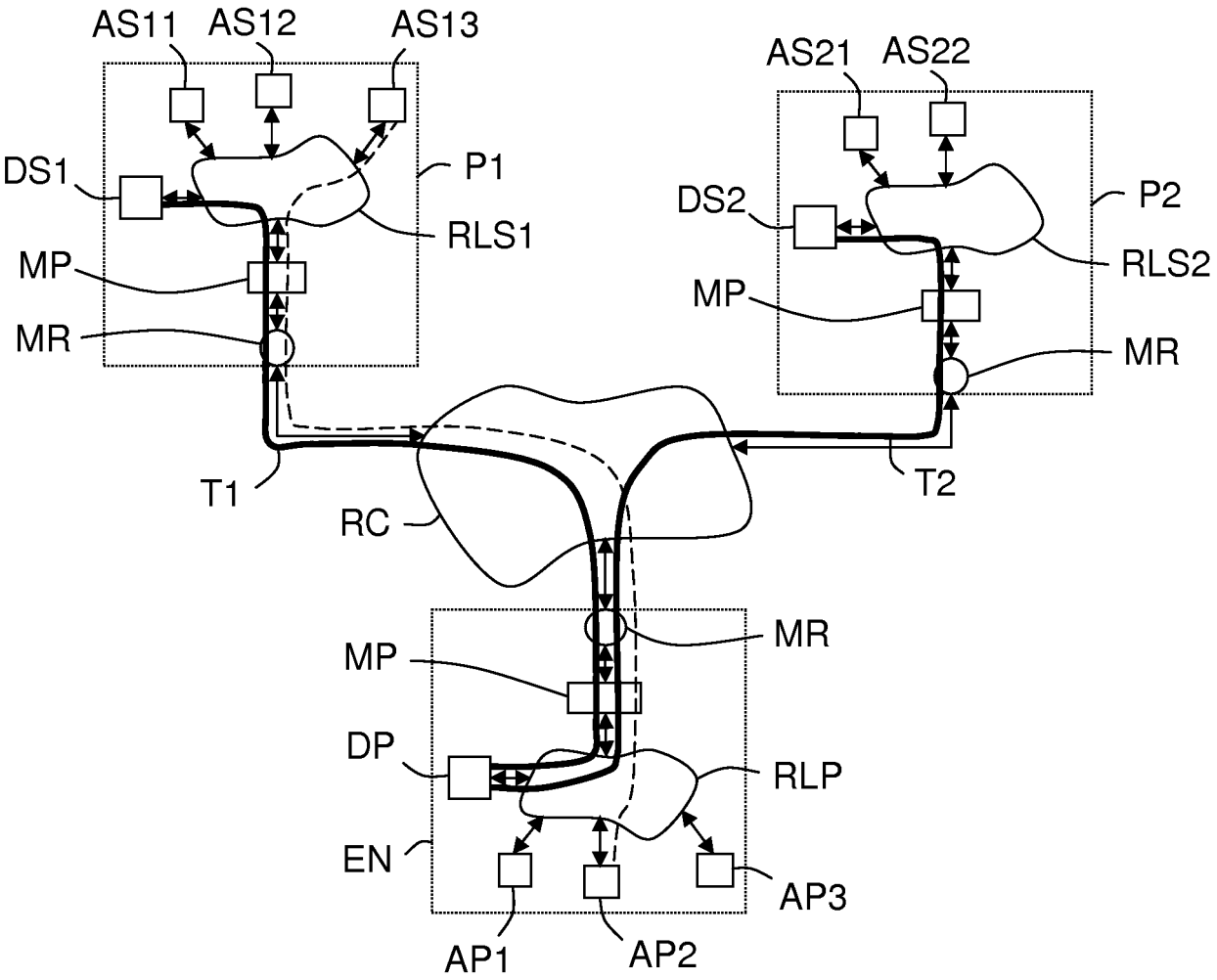

AS11
AS12
AS13
AS21
AS22
DS1
DS2
P1
P2
RLS1
RLS2
MP
MP
MR
MR
T1
T2
RC
MR
MP
DP
RLP
EN
AP3
AP1
AP2

FIG.1

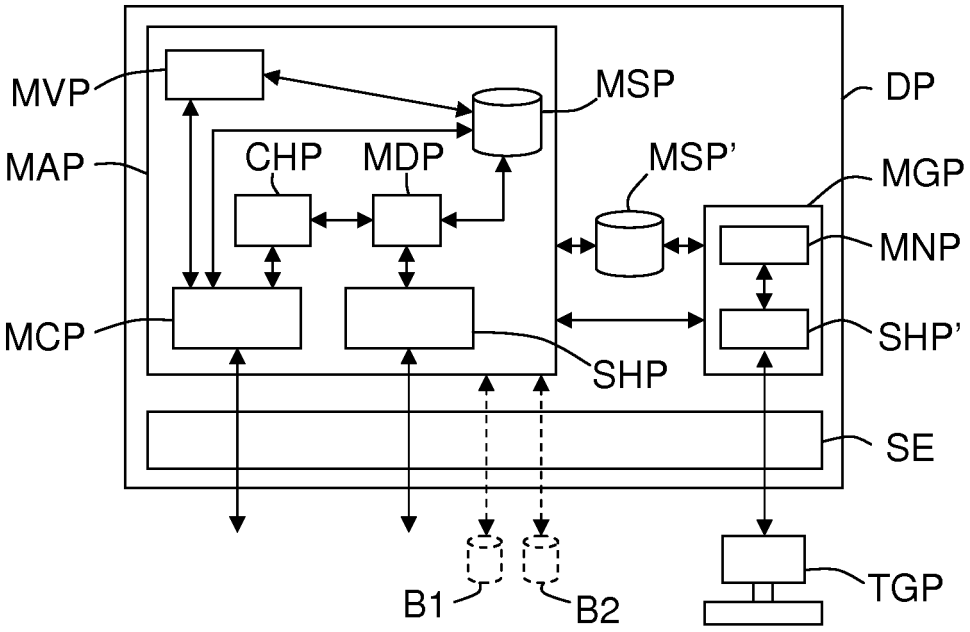

MVP
MAP
MCP
CHP
MDP
MSP
MSP'
DP
MGP
MNP
SHP'
SHP
SE
B1
B2
TGP

FIG.2

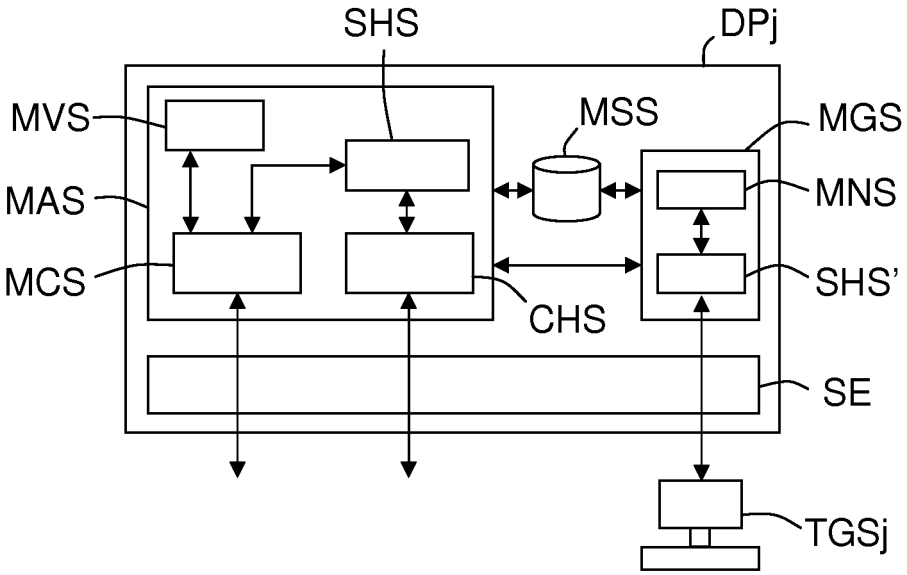

SHS
DPj
MVS
MAS
MCS
MSS
MGS
MNS
SHS'
CHS
SE
TGSj

FIG.3

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 759859
FR 1159029

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	US 7 685 292 B1 (KINSELLA JOE [US] ET AL) 23 mars 2010 (2010-03-23) * abrégé; figure 8 * * colonne 1, ligne 22 - colonne 19, ligne 49 *	1-11	H04L29/02 H04L12/66
A	EP 1 496 666 A1 (SIEMENS AG [DE]) 12 janvier 2005 (2005-01-12) * abrégé * * alinéa [0009] - alinéa [0017] * * alinéa [0025] *	1-11	
A,D	EP 2 129 078 A1 (AVAYA INC [US]) 2 décembre 2009 (2009-12-02) * abrégé; figure 1 * * alinéa [0017] - alinéa [0045] *	1-11	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L

Date d'achèvement de la recherche	Examinateur
4 mai 2012	Lebas, Yves

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)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1159029 FA 759859

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 04-05-2012
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 7685292 B1	23-03-2010	AUCUN	
EP 1496666 A1	12-01-2005	DE 10331309 A1	10-02-2005
		EP 1496666 A1	12-01-2005
EP 2129078 A1	02-12-2009	BR PI0903078 A2	25-05-2010
		EP 2129078 A1	02-12-2009
		JP 2009290861 A	10-12-2009
		KR 20090123800 A	02-12-2009
		US 2009300750 A1	03-12-2009

EPO FORM P0465