(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
14 novembre 2013 (14.11.2013)

WIPO | PCT

(10) Numéro de publication internationale
WO 2013/167745 A1

(51) Classification internationale des brevets : *H04L 12/28* (2006.01)

(21) Numéro de la demande internationale : PCT/EP2013/059754

(22) Date de dépôt international : 10 mai 2013 (10.05.2013)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1254238 9 mai 2012 (09.05.2012) FR

(71) Déposant : **INTERCLOUD** [FR/FR]; 12-14 rue Camille Desmoulins, F-92300 Levallois Perret (FR).

(72) Inventeurs : **DILOUYA, Jérôme**; 115, Avenue Achille Peretti, F-92200 Neuilly-sur-Seine (FR). **RYZMAN, Benjamin**; 69, Boulevard Richard Lenoir, F-75011 Paris (FR). **TESTE, Grégory**; 4, rue Jean-Jacques Rousseau, F-94200 Ivry-sur-Seine (FR).

(74) Mandataire : **LE SAUX, Gaël**; 90333, B, Technopole Atalante, 16B, rue de Jouanet, Bretagne, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

WO 2013/167745 A1

(54) **Title** : DATA TRANSMISSION SYSTEM

(54) **Titre** : SYSTEME DE TRANSMISSION DE DONNEES

(57) **Abstract** : The invention relates to a gateway for access to an interconnection network (ICB) of a data transmission system comprising a first local network, termed the client network, a second local network termed the cloud network and an interconnection network connecting said client network and said cloud network. According to the invention, such a gateway comprises means for identifying and routing data of said client network destined for said cloud network.

(57) **Abrégé** : L'invention se rapporte à une passerelle d'accès à un réseau d'interconnexion (ICB) d'un système de transmission de données comprenant un premier réseau local, dit réseau client, un deuxième réseau local dit réseau cloud et un réseau d'interconnexion connectant ledit réseau client et ledit réseau cloud. Selon l'invention, une telle passerelle comprend des moyens d'identification et de routage de données dudit réseau client à destination dudit réseau cloud.

Système de transmission de données.

1 DOMAINE DE L'INVENTION

L'invention concerne une technique de gestion de transmission de données. Plus particulièrement, l'invention est relative à une technique de multihoming pour l'interconnexion de services IP (« Internet Protocol »). Le multihoming consiste, de manière générale, pour un réseau, à être connecté à plusieurs fournisseurs d'accès à Internet afin d'améliorer la fiabilité de la connexion à Internet.

Plus particulièrement, dans le cadre des réseaux interconnectés par le protocole IP, le multihoming consiste, pour un réseau d'hôtes considéré, à être capable d'atteindre d'autres réseaux en passant à travers au moins deux réseaux voisins distincts au choix. L'objectif poursuivi est l'augmentation de la qualité et/ou de la résilience de l'interconnexion réseau. Le principe de base est d'éliminer, autant que faire se peut, tout point unique de défaillance sur le chemin de réseau considéré.

L'invention s'inscrit plus particulièrement dans la cadre de la mise en œuvre de services de Cloud Computing. Le Cloud Computing, technique désormais bien connue, consiste pour une part à délocaliser dans des salles d'hébergement les capacités de stockage et de calcul nécessaires pour répondre aux besoins des utilisateurs. Il s'agit d'une évolution de la mise en œuvre de l'informatique, dans laquelle la responsabilité de l'approvisionnement et de l'opération quotidienne n'incombe plus aux entreprises utilisatrices. La commercialisation de ces ressources informatiques s'effectue dans une granularité fine en termes d'unités de services et d'unités de temps. Ces deux ressources sont revendues aux entreprises utilisatrices.

On distingue fréquemment trois modes de mise en œuvre du Cloud Computing, selon le niveau de responsabilité du fournisseur :

a. le mode SaaS, pour « Software as a Service », désigne la mise à disposition de logiciels métiers ou bureautiques sous forme de services par abonnement ou par achat d'unités d'utilisation (un certain nombre d'utilisateurs pendant 1 an, par exemple), alors que, traditionnellement, ce type de logiciels est vendu sous forme de licence d'utilisation valide pour un ou plusieurs postes clients ;

b. le mode PaaS, pour « Platform as a Service », comprend la fourniture de briques logicielles permettant le développement de services complexes et sur mesure pour une ou plusieurs entreprises utilisatrices. Il tend à remplacer la mise en œuvre de ces

mêmes services sur des plates-formes déployées et gérées sur le site des entreprises utilisatrices ;

c. le mode *IaaS*, pour « *Infrastructure as a Service* », implique que le fournisseur fournisse de la capacité de calcul ou de stockage brute, sous forme de machines et disques virtuels hébergés sur sa propre infrastructure.

2 SOLUTIONS DE L'ART ANTERIEUR

Plusieurs problématiques se posent pour les entreprises désireuses d'utiliser des techniques de *Cloud Computing* et qui disposent d'un réseau virtuel d'interconnexion entre leurs sites. En effet, les infrastructures publiques permettent un gain en productivité et une réduction des investissements nécessaires puisqu'elles servent de nombreux clients et profitent ainsi des économies d'échelle. Or ces infrastructures ne sont joignables qu'au travers d'Internet et donc d'une infrastructure réseau par définition peu sûre. Les données à destination des « SaaS » sont fréquemment transportées par TLS 1.0, qui reste vulnérable en pratique de par sa fragilité intrinsèque mais aussi par les externalités telles que le filoutage.

Entre les différents sites d'une société et l'infrastructure publique qui pourrait héberger ses services critiques, les données sont mélangées au trafic Internet banalisé (dans lequel elles sont difficilement identifiables). Elles traverseront alors plusieurs réseaux : le réseau local du site, le réseau étendu de l'entreprise (à travers les circuits virtuels établis sur le réseau de transport de l'opérateur choisi), plusieurs réseaux d'opérateurs aux règles d'ingénierie et aux ratios de contention variables (suivant le chemin emprunté sur Internet), puis le *réseau d'interconnexion* au fournisseur d'infrastructure Cloud et enfin le réseau local de connexion aux serveurs Cloud.

On observe que l'entreprise n'a de relation contractuelle qu'avec un seul des opérateurs : celui qui lui fournit son réseau étendu. Par ailleurs, le mélange des données critiques dans le trafic Internet rend la mise en œuvre d'une politique de qualité de service difficilement envisageable de bout en bout, et même uniquement sur le réseau étendu de l'entreprise, puisqu'il est impossible de qualifier la criticité, et donc la classe de service, de données chiffrées sans d'abord les décrypter.

Une solution à ce problème pourrait être de mettre en œuvre deux accès Internet parallèles, l'un étant utilisé pour le transport des données critiques à destination du Cloud Computing, et l'autre pour le transport du trafic Internet classique (consultation d'informations, commandes de biens ou de services, échange de courrier, etc). Dès lors l'entreprise utilisatrice devrait mettre en œuvre un mécanisme de multihoming, capable de

qualifier les différentes données à transmettre entre son réseau étendu et les différentes destinations sur Internet.

Or, le mécanisme de multihoming couramment employé, BGP (pour « Borger Gateway Protocol »), n'est pas bien adapté à ce type d'ingénierie du trafic : il n'oriente les données qu'en fonction de leur adresse source et destination, mais pas du contenu des paquets IP. Par ailleurs, les fournisseurs d'accès Internet ne sont pas en mesure de garantir le chemin parcouru par les données à destination de tel ou tel réseau, puisque les différentes routes possibles varient dans le temps.

Une autre solution consisterait en la mise en place de boitiers d'optimisation WAN, mettant en œuvre un certain nombre de techniques améliorant les métriques de performances des applications métiers vis-à-vis des autres données transportées à travers le réseau étendu : déduplication, compression, optimisation de la latence TCP, proxy/cache, correction préventive des erreurs, échange de protocole, ajustement de trafic, égalisation, limitation des connexions ou du débit par utilisateur, etc. Pour autant, ce type de solution nécessite le déploiement d'équipements aux deux extrémités du réseau, ce qui peut s'avérer délicat, voire impossible.

3 RESUME DE L'INVENTION

L'invention ne présente pas ces inconvénients de l'art antérieur. Plus particulièrement, l'invention se rapporte à une passerelle d'accès à un réseau d'interconnexion (ICB) d'un système de transmission de données comprenant un premier réseau local, dit réseau client, un deuxième réseau local dit réseau cloud et un réseau d'interconnexion connectant ledit réseau client et ledit réseau cloud, caractérisée en ce que ladite passerelle comprend des moyens d'identification et de routage de données dudit réseau client à destination dudit réseau cloud.

Selon une caractéristique particulière, ladite passerelle comprend en outre des moyens de création d'au moins deux tunnels de transmission de données au travers dudit réseau d'interconnexion et des moyens de sélection, parmi lesdits au moins deux tunnel, d'au moins un tunnel d'au moins un tunnel de transmission de paquet, en fonction d'au moins un paramètre prédéterminé.

Selon une caractéristique particulière, lesdits types de tunnels sont basés sur le protocole UDP (de l'anglais pour « User Datagram Protocol »).

Selon une caractéristique particulière, ledit au moins un paramètre prédéterminé appartient au groupe comprenant :

- un état de disponibilité d'un lien entre ledit réseau local et ledit réseau d'interconnexion ;
- un état de disponibilité d'un lien entre ledit réseau local et un réseau maillé étendu ;
- une classe de trafic associée à au moins un paquet de données à transmettre.

Selon une caractéristique particulière, ladite passerelle comprend en outre des moyens d'identification d'une destination d'un paquet en fonction d'au moins une adresse de destination dudit paquet.

Selon une caractéristique particulière, ladite passerelle comprend en outre :

- des moyens de détection d'une coupure d'accès dudit réseau client vers un réseau maillé étendu, auquel ledit réseau client est connecté par l'intermédiaire d'une passerelle d'accès (BFAI) ;
- des moyens d'attribution d'une adresse IP préalablement attribuée à ladite passerelle BFAI à une interface de communication de ladite passerelle ;
- des moyens de filtrage de paquet de sorte que seuls des paquets à destination dudit réseau cloud soient transmis sur ledit réseau d'interconnexion.

Selon un autre aspect, l'invention concerne également un système de transmission de données, comprenant un premier réseau local, dit réseau client, un deuxième réseau local dit réseau cloud et un réseau d'interconnexion connectant ledit réseau client et ledit réseau cloud, ledit réseau client comprenant en outre une passerelle d'accès à un réseau maillé étendu (BFAI). Selon une caractéristique particulière ledit système comprend en outre, au niveau du réseau client, une passerelle d'accès audit réseau d'interconnexion (ICB) comprenant des moyens d'identification et de routage de données dudit réseau client à destination dudit réseau cloud.

4 DESCRIPTION DETAILLEE DE L'INVENTION

4.1 Rappel du principe de l'invention

La technique présentement décrite propose de résoudre les problématiques posées par l'accès « public » à des applications et ou des services de type « Cloud Computing » en déployant une infrastructure privée, de bout en bout (allant du réseau du Client au réseau du fournisseur de l'application et/ou du service, i.e. réseau cloud), sans jamais traverser de réseau Tiers, en particulier le réseau Internet.

En maitrisant l'intégralité du chemin entre le réseau Client et le réseau Cloud de « destination », la technique de l'invention permet d'adresser les enjeux de Sécurité, de

Qualité de Service et de Conformité posés par le « Cloud Computing ». La solution décrite vise particulièrement les entreprises multi-utilisatrices de « Cloud Computing », car un unique accès à une passerelle dédiée permet de sécuriser l'intégralité des destinations connectées au réseau privé fourni à l'entreprise utilisatrice. Cette solution se déploie en parallèle de la solution principale d'accès à Internet de l'entreprise, en ne venant perturber nullement ses habitudes de travail. Elle est pour ainsi dire « transparente » aux flux non critiques, et améliore de façon drastique les flux critiques et les flux métiers, aussi bien en matière de sécurité qu'en matière de Qualité de Service.

Le principe général de l'invention est de disposer, au sein du réseau de l'utilisateur (i.e. de l'entité cliente qui souhaite accéder à des services de Cloud Computing), d'une passerelle d'interconnexion intelligente. L'objet de cette passerelle et de permettre une différenciation des flux sortants (et entrants), afin qu'ils soient routés de manière adéquate. L'objet de cette passerelle est également d'assurer un niveau de qualité de service prédéfini tout en assurant une tolérance aux pannes.

Cette passerelle est également nommée ICB par la suite.

La passerelle ICB comprend des moyens d'interconnexion du réseau de client avec un réseau d'interconnexion. Ce réseau d'interconnexion permet en quelque sorte de réaliser une interconnexion entre un client et un fournisseur de service de cloud computing (CSP). Ce réseau d'interconnexion agrège des liens dédiés. Un lien dédié est un lien physique qui est « tiré » entre le client et le réseau d'interconnexion. Il peut par exemple s'agir d'une fibre optique. Un lien physique peut également être tiré entre le réseau d'interconnexion et le fournisseur de service de cloud computing (CSP). Le réseau d'interconnexion gère à la fois la transmission/réception de données en provenance des clients et le routage de ces données vers les CSP. Pour pouvoir assurer une bonne qualité de service, la passerelle d'interconnexion intelligente est capable de transmettre et recevoir des données sur le réseau d'interconnexion. La passerelle d'interconnexion dispose également d'une capacité de transmission de données directement par l'intermédiaire d'un réseau maillé, tel que le réseau internet, lorsque le lien dédié n'est pas ou plus opérationnel. C'est en ce sens que la passerelle peut être qualifiée d'intelligente.

Pour garantir cette tolérance aux pannes du lien principal, la passerelle comprend des mécanismes d'établissement de tunnels d'une part et utilise un protocole qui autorise une grande liberté dans le transport de données.

4.2 Description d'un mode de réalisation

On présente dans ce mode de réalisation, une passerelle d'interconnexion intelligente, nommée ICB, qui, selon l'invention, permet (dans une architecture de multihomming), de réaliser une séparation entre les données transmises aux fournisseurs de service Cloud (CSP) et les données générales transitant par un réseau d'opérateur.

Cette passerelle possède deux modes de fonctionnement.

- en coupure d'une passerelle d'accès d'un fournisseur d'accès comme un opérateur (cette passerelle d'accès est nommée BFAI) ;

  Dans ce mode, l'ICB est placé en coupure de la passerelle BFAI. Son rôle est d'intercepter et de dévier les données à destination des CSP vers le réseau dédié à la transmission de données vers les fournisseurs de servies cloud ;

- serveur DNS (de l'anglais pour « Domain Name Server ») dans une DMZ (de l'anglais pour « DeMilitarized Zone »).

  Dans cette configuration, le serveur DNS des machines clientes du LAN sera le serveur DNS du fournisseur de l'infrastructure d'interconnexion. L'ICB placé dans une DMZ sera le « next-hop » (mécanisme consistant à ne connaître que l'adresse du prochain maillon menant à la destination est appelé routage par sauts successifs) de la route vers le fournisseur de l'infrastructure d'interconnexion au niveau de la passerelle BFAI.

La passerelle possède de nombreuses caractéristiques qui lui permettent de fonctionner de manière transparente pour le client chez qui elle est mise en œuvre. Cette passerelle, comme cela a été exposé de manière général, permet de transporter les flux en provenance et à destination des fournisseurs de services Cloud par l'intermédiaire d'un réseau d'interconnexion.

4.2.1 Démarrage

L'ICB démarre sur le réseau (via PXE, de l'anglais « Pre-boot eXecution Environment ») et charge son noyau, son environnement et sa configuration via un serveur situé en cœur de réseau d'interconnexion.

Le système chargé depuis le réseau est placé dans la mémoire vive de l'ICB. Cela assure qu'il est possible de modifier la configuration de la passerelle à distance pour répondre aux besoins d'évolution en relation avec l'infrastructure des réseaux par exemple.

L'adresse IP fournie par le serveur est attribuée en fonction de l'adresse MAC (adresse machine) de l'ICB. Le serveur est capable de connaître le lien depuis lequel l'ICB fait sa demande, et peut alors fournir à celle-ci la configuration idoine.

4.2.2 Contraintes du lien dédié du fournisseur de l'infrastructure d'interconnexion

On a trois types de flux à destination de l'ICB : les accès directs, indirects et le lien d'administration. Les inventeurs ont constaté qu'il est préférable de séparer ces trois flux.

Il est possible d'utiliser tout simplement des VLAN (de l'anglais « *Virtual Local Area Network* » ou « *Virtual LAN* », en français *Réseau Local Virtuel*) pour réaliser cette opération. Chaque flux serait alors isolé dans un VLAN sur le lien dédié. Cependant, le lien dédié (depuis l'ICB jusqu'au réseau d'interconnexion) est fourni par un opérateur tierce. Aucune garantie n'est apportée quant au support d'un transport de données par l'intermédiaire d'un VLAN n'est assuré.

Pour remédier à ce problème, les inventeurs proposent de faire transiter chaque flux dans un tunnel différent pour garantir l'isolation. Ce tunnel est par exemple un tunnel OpenVPN.

4.2.3 Sécurité des ponts et du routage

Pour éviter de laisser passer tout et n'importe quoi sur les réseaux connectés à l'ICB, une politique de filtrage est appliquée au niveau de l'interface connectée au fournisseur de l'infrastructure d'interconnexion. On n'applique aucun filtrage pour ce qui est à destination du fournisseur d'accès à Internet.

4.2.4 Tunnels sécurisés

L'ICB monte des tunnels (avec OpenVPN) jusqu'à un concentrateur de tunnels en bordure du réseau d'interconnexion.

Bien que chacun des tunnels montés fourni une connectivité Ethernet (tap), on distingue deux types de tunnels différents :

- Indirect (**tun0**) : ce tunnel permet de faire les accès indirects vers les CSP. Il offre une connectivité au niveau IP. Ce tunnel est commun à tous les accès indirects.
- Directs (**tap***) : ce type de tunnel assure la connectivité Ethernet pour tout élément qui apparait dans le réseau du client lorsque le lien vers le réseau d'interconnexion est disponible. Les données qui circulent sur ce type de tunnel sont privées et sont chiffrées avant d'être transmises sur Internet. On utilise un tunnel par CSP par client.

L'avantage d'utiliser des tunnels est qu'il résulte qu'une seule configuration de routage doit être mise en place, en privilégiant les routes via le lien dédié. Lorsque le lien dédié devient indisponible, le tunnel passe par Internet de manière automatique afin de garantir une continuité de service.

Pour les tunnels, on a le choix entre les protocoles sur lesquels les données du tunnel circulent : TCP (« Transmission Control Protocol ») ou UDP (« User Datagram Protocol »).

- TCP : L'avantage de TCP est qu'il fournit une suite de mécanismes de gestion de congestion, de contrôle d'erreur, etc. Le problème est que l'ICB fournit une connectivité Ethernet à travers ces tunnels, et que les flux qui transitent dans le tunnel ont déjà un mécanisme de contrôle d'erreur (au niveau du protocole réseau, ou au niveau applicatif) : le fait de le faire passer de nouveau sur TCP constitue un double emploi.

  De plus, lorsque le lien dédié devient indisponible, la session TCP du tunnel est brisée et le tunnel est remonté sur l'interface coté BFAI. Cependant, lorsque le lien dédié devient à nouveau disponible, l'ICB continuera à utiliser l'interface coté BFAI puisque la session TCP est toujours active. Il faudra manuellement couper le tunnel et le remonter pour qu'il passe à nouveau par le lien dédié.

  Au niveau du concentrateur de tunnels, l'intérêt d'utiliser des sessions TCP est qu'il est possible de détecter lorsque les sessions TCP sont brisées et transmettre cette information à la supervision.

- UDP : L'avantage d'UDP est sa simplicité. Il n'est pas nécessaire, comme dans TCP, de maintenir des sessions. UDP ne gère pas la congestion et le contrôle d'erreur : le flux qui transite dans le tunnel gère ces aspects de congestion et de contrôle d'erreur seul.

  Lorsque le lien dédié devient indisponible, le tunnel est routé sur Internet, et lorsque le lien dédié deviendra à nouveau disponible, le tunnel repasse par ce lien grâce à la route statique vers le réseau d'interconnexion.

  Au niveau du concentrateur de tunnels, dans la mesure où il n'y a pas de session maintenue, il est seulement possible de détecter que l'ICB n'a pas réussi à monter les tunnels. Il faut alors transmettre les informations à la supervision depuis l'ICB.

Dans ce mode de réalisation particulier, l'utilisation du protocole UDP pour les tunnels est privilégiée. En effet, le protocole UDP permet de passer d'un lien à l'autre instantanément en fonction de la table routage, plutôt que d'avoir à démonter et remonter

les tunnels manuellement. De plus, UDP est plus léger que TCP et il n'est pas nécessaire d'avoir des mécanismes de contrôle d'erreur avancés au niveau du tunnel puisque les flux qui y circulent disposent de leurs propres mécanismes.

4.2.5 Accès direct

Certains CSP acceptent de gérer une adresse IP du réseau local LAN ou de la DMZ du client comme point d'accès à leur service. En fonction du mode de fonctionnement de l'ICB, l'adresse IP gérée par le CSP est soit une adresse IP du réseau local LAN du client soit une adresse IP de sa DMZ. L'ICB transmet des données par un des tunnels. Au bout du tunnel, des équipements en cœur du réseau d'interconnexion sont capables d'étendre le réseau local LAN du client jusqu'au CSP. La sécurité des données transitant sur ce réseau local LAN étendu est à la charge du client, puisqu'il fait partie de son réseau.

On a le choix entre deux technologies pour faire la jonction Ethernet entre l'équipement en cœur du réseau d'interconnexion et les CSP :

- VLL (de l'anglais « Virtual Leased Line ») est un lien point-à-point complètement transparent qui laisse passer la totalité du trafic. Une VLL est très peu couteuse en ressources.
- VPLS (de l'anglais « Virtuial Private LAN Service ») permet d'assurer une connectivité Ethernet un-à-plusieurs mais est plus gourmand en ressources que VLL car VPLS agit comme un commutateur et conserve, en mémoire, une table ARP (c'est une table de couples adresse IPv4-adresse MAC contenue dans la mémoire d'un ordinateur qui utilise le protocole ARP, « Address Resolution Protocol »").

Or, pour chaque nouveau CSP auquel le client veut s'interconnecter, il est nécessaire de monter une VLL ce qui peut rendre la configuration complexe. Il a donc été décidé de choisir VPLS qui permet une configuration plus simple. Lorsque le client veut accéder à un nouveau CSP, il suffit d'ajouter cette nouvelle destination dans VPLS.

Le nombre de clients et de CSP prévu n'entraine pas une pénurie de ressources au niveau des équipements qui devront gérer VPLS.

On parle dans cette partie d'adresse IP car c'est le protocole le plus fréquemment utilisé. En revanche, l'ICB faisant office de pont Ethernet, il est possible d'utiliser n'importe quel protocole au-dessus d'Ethernet.

4.2.6 Accès indirect

Pour les accès indirects, on a plusieurs choix quant à l'adresse IP qu'il est possible d'utiliser :

- Soit directement l'adresse IP publique du CSP ;
- Soit une adresse privée du réseau d'interconnexion associée au CSP ;
- Soit une adresse publique du réseau d'interconnexion associée au CSP ;
- Soit une adresse privée dans une plage d'adresse réservée fournie par le client.

Pour les données à destination des CSP qui transitent sur le réseau d'interconnexion, on utilise l'adresse IP publique du CSP. Si on constate une perte de lien entre le réseau d'interconnexion et un CSP, les mécanismes de routage mis en place basculent le trafic vers le réseau de transit (Internet) et acheminent le trafic vers les CSP via le réseau Internet.

Lorsque l'ICB est en coupure, il est possible d'utiliser les adresses IP publiques sans problème. En revanche lorsque l'ICB est installée en DMZ, l'utilisation directe des adresses IP publiques nécessite une reconfiguration d'une route statique pour chaque CSP au niveau de la passerelle BFAI. On préfère donc regrouper tous les CSP sur une plage d'adresses IP.

Si on utilise les adresses IP du réseau d'interconnexion, un mécanisme de saturation rapide de la classe d'adresse de départ se produit. De plus, il va être nécessaire de transformer ces adresses IP du réseau d'interconnexion en adresses IP publiques des CSP. Il n'est pas possible d'utiliser des adresses IP publiques pour faire uniquement de la translation d'adresse. Les registres d'attribution de plage d'adresses IP publiques sont contre cette pratique et peuvent interdire l'accès à d'autre IP voire retirer l'accès à une plage.

De plus, s'il est choisi d'utiliser des adresses IP privées du réseau d'interconnexion, il n'est pas possible garantir que la plage d'adresses choisie dans le réseau d'interconnexion n'est pas déjà utilisée par le client.

Pour ce cas, le client fourni une plage d'adresses IP privées, cette plage étant réservée pour les CSP. Cela permet de garantir que la plage n'est pas déjà utilisée dans le réseau du client et il n'est pas nécessaire d'utiliser d'adresse IP publique.

Chaque client dispose donc d'une configuration DNS spécifique avec une bijection entre les adresses IP fournies (par lui) et les adresses IP des CSP auxquels il veut accéder : pour chaque adresse IP du CSP, on dispose d'une adresse IP privée associée. Cela permet également de tirer parti des éventuels mécanismes de répartition de charge (comme du *« round robin »*) que les CSP ont pu mettre en place au niveau de leur DNS.

Ainsi, pour régler ces problèmes, l'ICB dispose de la table de correspondance entre ces adresses IP pour pouvoir faire un NAT (« Network Address Translation ») sur la destination des paquets.

Un des autres avantages à utiliser une plage d'adresses IP privée pour les CSP est la classe de trafic perçue par l'opérateur *« VPN »* du client à travers des VPN entre les sites du client. Si on utilisait des adresses IP publiques, le trafic à travers le VPN serait classé comme « Best Effort ». Si on utilise des adresses IP privées, l'opérateur classera le trafic comme « Business », avec une meilleure qualité de service au travers du VPN. Ainsi, l'utilisation d'adresses IP privées permet en quelque sorte de « leurrer » l'opérateur du client.

Lorsque le client accède aux CSP, l'adresse IP source contenue dans les paquets est l'adresse IP de la machine cliente dans le réseau local LAN (dans le réseau local LAN du client). Cette adresse IP étant privée, elle ne sera pas routée sur Internet (ou dans le réseau d'interconnexion) et le CSP ne saurait pas où envoyer sa réponse.

Il faut donc faire un NAT (« Network Address Translation ») sur l'adresse source des paquets. On a deux possibilités pour l'emplacement du NAT :

- Juste avant le CSP dans le réseau d'interconnexion.
- Au niveau de l'ICB dans le réseau du client.

Compte-tenu des limitations du NAT en terme de connexions simultanées, la solution à ce problème n'est pas de réaliser le NAT au niveau du CSP car on pourrait se retrouver à court de ports de substitution ou même écrouler le serveur avant d'arriver à ce stade.

En revanche, au niveau de l'ICB, il est fort peu probable d'atteindre plus de 60'000 connexions simultanées. Il est donc préférable de réaliser une translation d'adresse au niveau de l'ICB.

4.2.7 Sécurité

Il n'est pas souhaitable que des machines (éventuellement compromises) dans les réseaux des CSP puissent attaquer les clients par l'intermédiaire du réseau d'interconnexion. Ainsi, il est nécessaire de mettre en place des règles de filtrage de sécurités pour filtrer le trafic à destination des clients.

Il est possible d'appliquer ces règles dans les tables de filtrage de chaque ICB. Il est également possible de réaliser un filtrage commun à tous les clients en cœur de réseau d'interconnexion. Cette deuxième solution présente l'avantage de centraliser la prise de décision et de bloquer les flux « illégaux » en amont, avant qu'ils ne soient propagés vers les clients.

4.2.8 Service dégradé

Lorsque le lien entre l'ICB et le réseau d'interconnexion devient indisponible, l'ICB est capable de basculer la transmission et la réception de flux sur le réseau Internet.

L'indisponibilité du lien invalide les routes statiques vers le réseau d'interconnexion et l'ICB bascule automatiquement les tunnels vers un accès au réseau d'interconnexion par le biais d'Internet.

Lorsque c'est l'ICB qui est indisponible (problème matériel ou logiciel), le client est en mesure de retirer l'ICB de son réseau (en connectant 2 câbles réseau avec un coupleur par exemple) et peut continuer à utiliser ses services et tout ou partie des services proposés sans avoir à reconfigurer ses équipements.

Selon un mode de réalisation spécifique de l'invention, l'ICB dispose d'une fonctionnalité de court-circuit : l'utilisateur n'a pas à retirer l'ICB de son réseau. L'ICB se comporte comme un simple câble d'interconnexion. Cette fonctionnalité peut être mise en œuvre de deux manières différentes : la première est de laisser l'ICB détecter seule que le lien d'interconnexion est indisponible. Dans ce cas la fonctionnalité de coupe circuit est mise en œuvre par l'ICB. La deuxième est matérielle : lorsque l'ICB n'est plus alimentée (par exemple l'ICB est débranchée), le court-circuit est réalisé de manière automatique, du fait de l'absence d'alimentation.

4.2.9 Trap SNMP

Lors d'une dégradation de service, un trap SNMP (« Simple Network Management Protocol ») doit être envoyé au serveur de supervision pour être traité et pour avertir immédiatement les administrateurs d'une panne. L'ICB transmet un trap SNMP lorsqu'elle détecte une anomalie sur un lien, ou si un service critique est indisponible.

Le concentrateur de tunnel est en mesure de détecter qu'une ICB n'a pas réussi à remonter ses tunnels.

Les traps SNMP sont transmis via le tunnel d'administration.

4.2.10 Reprise du service

En fonction du mode de fonctionnement, lorsque le lien dédié est à nouveau disponible, l'ICB repasse automatiquement dans sa configuration initiale. L'ICB transmet également un trap SNMP pour avertir de la reprise du service.

4.2.11 Adresses IP

Pour le bon fonctionnement de l'ICB, on a besoin de plusieurs adresses IP différentes :

- Une adresse IP sur l'interface coté fournisseur de l'infrastructure d'interconnexion, pour monter les tunnels quand le lien est disponible. Cette adresse IP est distribuée

par un serveur DHCP en cœur de réseau d'interconnexion, sur une plage d'adresses IP privées.

- Une adresse IP sur l'interface coté BFAI, pour monter les tunnels quand le lien dédié est indisponible. On ne maitrise pas l'adresse IP sur cette interface, il n'est pas possible choisir arbitrairement une adresse IP dans le réseau local du client. Il faut qu'il fournisse une adresse IP non utilisée pour éviter un conflit d'adressage.
- Une adresse IP publique du fournisseur de l'infrastructure d'interconnexion dans le tunnel pour le trafic indirect, nécessaire pour faire le NAT et pour les réponses des CSP.
- Une adresse IP privée Fournisseur de l'infrastructure d'interconnexion dans le tunnel pour le lien d'administration.
- En DMZ :
  - adresse IP du *next-hop*, dans la DMZ du client.
  - adresse IP du serveur DNS, dans le réseau d'interconnexion.
  - adresse IP du CSP, dans la plage d'adresse fournie par le client.

4.2.12 QoS

Parmi les objets de l'invention, la gestion de la qualité de service tient une place prépondérante. Le fait d'avoir des ICB chez les clients permet de maîtriser des équipements de bout-en-bout du réseau jusqu'au CSP (tout du moins sur une très grande partie du trajet). Il est alors possible d'utiliser les ICB pour faire des tests sur la qualité du réseau de bout-en-bout (mesures EtherSAM). Il est également possible d'identifier les heures pleines et heures creuses d'utilisation du service par le client.

Selon l'invention, l'ICB dispose également de moyens de monter un tunnel sur Internet en plus des tunnels sur le lien dédié. Dès lors, il est possible de lancer des scénarios en parallèle sur les deux liens pour les comparer. Ainsi, il est possible, de manière dynamique, d'ajuster des paramètres de transmission de données, voire de décider d'utiliser un tunnel supplémentaire pour réaliser une transmission de données dans un contexte donné.

4.3 Cas d'utilisation : site unique

4.3.1 En coupure

4.3.1.1 Description

Dans ce mode, l'ICB est placé en coupure de la BFAI. Son rôle est d'intercepter et de dévier les données à destination des CSP vers le réseau d'interconnexion. Les éléments suivants permettent de décrire le fonctionnement de la passerelle, et plus généralement du système dans cette configuration. Il est important de noter que la passerelle comprend des moyens de mise en œuvre des méthodes qui sont décrites par la suite, et notamment des moyens de mise en œuvre des méthode de routage et de différentiation du traitement des données en provenance et à destination du réseau d'interconnexion et du réseau « public » qui fournisseur d'accès à l'Internet. Ces moyens sont constitués par un processeur (qui est apte à appliquer des traitements distincts aux paquets en fonction d'une situation du réseau et d'une configuration), au moins une mémoire (qui comprend les fichiers de configuration nécessaires au traitement des paquets) et au moins trois interfaces de réseau. Ces interfaces peuvent être des modules physiques d'accès au réseau qui peuvent être de technologies identiques ou différentes, selon les cas. L'objet de l'invention étant de rendre aussi transparent que possible le routage des données entre les réseaux et d'assurer une continuité de service en cas de panne de l'un ou l'autre des réseaux. Bien entendu, la continuité de service est assurée vers le réseau d'interconnexion : il s'agit d'assurer une continuité de service lors d'une défaillance de la BFAI et lors d'une défaillance de l'ICB. Pour ce faire des moyens spécifiques sont développés pas les inventeurs.

4.3.1.2 Interfaces et pont

Pour les trois interfaces de l'ICB, on a :

- **eth0** : relie le réseau local LAN du client à l'ICB.
- **eth1** : relie la BFAI du client à l'ICB. Cette interface possède une adresse IP dans le réseau local LAN du client.
- **eth2** : relie le réseau d'interconnexion à l'ICB. Cette interface possède une adresse IP qui n'est pas maitrisée.

Le pont entre les interfaces se nomme br0.

Si le client fait transiter ses données dans des VLAN, on dispose également des interfaces sensibles aux VLAN (eth0.x par exemple), ainsi qu'un second pont br1.

4.3.1.3 Intégration dans le réseau de l'entreprise

Il est préférable que l'ICB soit le plus transparent possible dans le réseau du client. On monte un pont Ethernet au niveau de l'ICB pour continuer à assurer la connectivité Ethernet entre le réseau local LAN et la BFAI. Le réseau local LAN du client continuera à fonctionner comme avant (ARP, BOOTP, ...), la BFAI sera toujours la passerelle par défaut des machines clientes.

Les inventeurs ont eu l'idée de privilégier le pont Ethernet qui permet une configuration plus simple au niveau de l'ICB et qui évite d'avoir deux fois la même adresse IP dans le réseau local LAN du client. Il permet également d'étendre facilement le réseau local LAN du client jusqu'aux CSP.

4.3.1.4 Serveur DNS

L'invention réside en partie sur le postulat selon lequel le fournisseur d'accès à internet (FAI) n'est pas fiable. Les inventeurs ont eu l'idée changer le serveur DNS secondaire fourni par le serveur DHCP par un serveur DNS du fournisseur de l'infrastructure d'interconnexion (en IP privée). Cela est utile lorsque le lien vers l'opérateur ou la BFAI devient indisponible.

On a deux cas :

- Le client peut modifier la configuration DHCP fournie soit par la BFAI, soit par un serveur DNS dans son réseau local LAN et on modifie directement le serveur DNS secondaire.
- L'ICB est en coupure du serveur DHCP et les inventeurs ont eu l'idée de réécrire les réponses DHCP qui traversent l'ICB en changeant le serveur DNS secondaire.

4.3.1.5 Chargement des configurations

L'ICB placé en coupure a besoin de connaître les plages d'adresses IP qu'il doit détourner vers le réseau d'interconnexion. Il doit donc être capable de récupérer ces informations depuis le réseau d'interconnexion.

L'ICB doit également être capable de rafraîchir périodiquement ces plages d'adresses.

4.3.1.6 802.1Q

Les données à destination de la BFAI peuvent potentiellement être encapsulées dans des VLAN.

L'ICB en coupure doit être capable de comprendre les trames taguées. Pour la simplicité de la configuration et des mécanismes mis en œuvre dans l'ICB, on considère que le trafic Internet n'est pas séparés en plusieurs VLAN. Il est possible d'avoir plusieurs VLAN qui traversent l'ICB mais un seul contiendra le trafic Internet qu'on doit analyser et éventuellement dévier vers le fournisseur de l'infrastructure d'interconnexion.

4.3.1.7 Filtrage

Des règles spécifiques sont intégrées afin de réaliser un filtrage conforme à l'objectif de l'invention.

4.3.1.8 Filtrage avec VLAN

Si le trafic internet est isolé dans un VLAN, les inventeurs ont eu l'idée de faire un pont Ethernet br1 entre les interfaces eth0 et eth1. Sur ce pont circuleront tous les trames tagués ou non. Les inventeurs ont eu l'idée de extraire les trames du VLAN qui sont intéressantes en les décapsulant.

Une fois décapsulés, ces paquets arriveront non tagués sur l'interface **eth0.vlan** (avec vlan le VLAN ID). Le trafic direct sera dévié vers l'interface tap* jusqu'aux CSP. Le trafic indirect sera quant à lui routé par l'ICB. Le trafic sur ce VLAN qui n'est pas à destination des CSP sera réinjecté tagué dans le réseau local LAN via l'interface **eth1.vlan**. Les inventeurs ont eu l'idée de donc faire un pont Ethernet **br0** entre les interfaces **eth0.vlan**, **eth1.vlan** et **tap***. Ce pont dispose des mêmes règles de filtrage que le pont sans VLANs.

4.3.1.9 Wi-Fi

Si des machines du client sont connectées directement en wifi sur la BFAI, on n'a aucun moyen de pouvoir intercepter le trafic vers les CSP.

Pour ces utilisateurs :

- Soit ils accèderont aux CSP classiquement par Internet.
- Soit le client devra installer un point d'accès wifi dans son réseau pour que le trafic puisse être intercepté.

4.3.1.10 Fonctionnement normal

Un pont Ethernet (br0) est monté entre les 3 interfaces eth0, eth1, tap*.

Les requêtes DNS passent à travers le pont Ethernet sans être altérées. Le serveur DNS de l'opérateur retourne l'adresse IP publique des CSP.

Les accès indirects aux CSP sont interceptés par l'ICB, qui les considère comme pour lui et les route vers le réseau d'interconnexion. Si les paquets se trouvent dans un VLAN, ils sont décapsulés avant d'être routés. Un *masquerading* est réalisé sur les paquets sortant par l'interface tun0.

Les accès directs traversent le pont Ethernet jusqu'aux CSP via le réseau d'interconnexion. Si les paquets se trouvent dans un VLAN, ils sont décapsulés avant d'être transmis à l'interface de sortie.

4.3.1.11 Lien vers le fournisseur de l'infrastructure d'interconnexion indisponible

Lorsque le lien ver le fournisseur de l'infrastructure d'interconnexion devient indisponible, la route statique vers le réseau d'interconnexion est rendue obsolète. Les tunnels passeront par la route par défaut et par Internet.

Le fonctionnement de l'ICB et la configuration des clients restent inchangés.

4.3.1.12 ICB indisponible

Lorsque l'ICB devient indisponible, le service fourni au client est interrompu et son réseau local LAN est impacté. Le client doit retirer l'ICB de son réseau pour rétablir la connectivité avec la BFAI.

Si l'ICB possède un mode court-circuit, le client n'aura rien à faire à moins que le plantage soit au niveau logiciel.

4.3.1.13 BFAI indisponible

1. **Un mot sur ARP**

Lorsqu'une machine cherche à envoyer un paquet à une adresse IP sur son réseau local, elle doit d'abord connaître son adresse MAC. Les adresses connues sont stockées dans une table (qui fait la correspondance IP <-> MAC) au niveau du système d'exploitation appelé cache ARP. On a deux cas :

- Soit l'adresse IP est présente dans le cache ARP et on récupère directement l'adresse MAC.
- Soit l'adresse n'est pas présente dans le cache ARP et on doit faire une requête sur le réseau pour demander l'adresse MAC. Pour se faire, la machine envoie en diffusion sur le réseau un message ARP *who-has* en indiquant l'adresse IP concernée. La

machine possédant cette adresse IP répondra avec un message *is-at*, contenant son adresse MAC.

Le cache ARP est régulièrement nettoyé. Toutes les adresses MAC n'ayant pas été utilisées récemment sont supprimées.

2. Différenciation des flux

On distingue 3 flux qui peuvent émaner du client :

- Le trafic internet (Facebook, Yahoo ! News, YouTube, …)
- Le trafic CSP indirect où les services Cloud sont accédés via les noms publics des fournisseurs de service (Google Apps, Salesforce, …)
- Le trafic CSP direct où les services Cloud sont visibles par le client comme si ils étaient directement intégrés dans son réseau local (Instances Amazon EC2, …)

3. Mécanismes sollicités jusqu'à la sortie du réseau

On suppose que tous les caches (ARP, DNS) sont vides.

a. Trafic internet

1. Le navigateur analyse la saisie de l'utilisateur dans la barre d'adresse pour en extraire le nom DNS (ou l'adresse IP) de la cible.
2. Le navigateur demande au système d'exploitation de réaliser une résolution de nom pour obtenir l'adresse IP de la cible.
3. Le système d'exploitation recherche l'information sur tous les moyens à sa disposition (fichier hosts, cache DNS, serveur DNS).
4. Le système d'exploitation doit contacter le serveur DNS du FAI, il ne se trouve pas sur le réseau local.
5. Le système d'exploitation doit transmettre la requête à sa passerelle par défaut car ce n'est pas une adresse IP locale (déterminé par la table de routage).
6. Le système d'exploitation recherche si l'adresse MAC de la passerelle est disponible dans le cache ARP.
7. Le système d'exploitation effectue une résolution ARP pour obtenir la MAC de la passerelle.
8. L'ICB (qui agit comme un commutateur Ethernet) laisse passer la requête jusqu'au BFAI qui répond au client.
9. Le système d'exploitation transmet la requête DNS à sa passerelle par défaut.

10. L'ICB laisse passer la requête.
11. Une fois l'adresse IP de la cible récupérée, le navigateur établi une connexion avec le site cible en transmettant les données à sa passerelle (car encore une fois on a une adresse IP non locale) qui se chargera de les router.
12. L'ICB laisse passer la connexion puisqu'elle ne concerne pas un CSP.

b. Trafic CSP indirect

Des étapes 1. à 11., le fonctionnement du procédé est identique. L'étape 12 est modifiée comme suit :

12. L'ICB a détecté que la connexion concerne un CSP et détourne les données vers le réseau d'interconnexion.

c. Trafic CSP direct

1. L'application tente une connexion à l'adresse IP cible.
2. Le système d'exploitation détecte que c'est une adresse IP locale, accessible directement.
3. Le système d'exploitation recherche si l'adresse MAC de la passerelle est disponible dans le cache ARP.
4. Le système d'exploitation effectue une résolution ARP pour obtenir la MAC de la passerelle.
5. L'ICB qui agit comme un commutateur Ethernet entre le LAN, la BFAI et le fournisseur de l'infrastructure d'interconnexion laisse la requête ARP se diffuser au travers du réseau d'interconnexion.
6. La machine distante va répondre à cette requête au travers du réseau d'interconnexion
7. L'application peut établir sa connexion avec la cible
8. L'ICB (qui agit comme un commutateur Ethernet) va envoyer les données vers la cible à travers le réseau d'interconnexion

4. Défection du boitier d'accès du fournisseur d'accès à Internet

Lorsque la BFAI devient indisponible, les machines clientes ne peuvent plus y accéder et toutes les connexions en cours sont rompues. Au bout d'un certain temps, l'adresse IP ne répondant plus aux sollicitations, la route va être invalidée dans la table de routage du système d'exploitation. À partir de ce moment, le client n'a plus aucune entrée dans sa table de routage pour joindre l'adresse IP distante. Le système d'exploitation considère que la

route est injoignable et retourne directement un code d'erreur à l'application sans transmettre aucune donnée sur le réseau.

Le trafic direct n'est pas affecté car il ne dépend pas de l'entrée de la route par défaut dans la table de routage. En effet il dépend d'une autre entrée qui indique que la plage d'adresse IP du réseau local est directement joignable. Puisque l'ICB est toujours en fonction, il continuera à relayer d'éventuelles requêtes ARP vers la machine distante, et il continuera à agir comme un commutateur Ethernet et relaiera les données vers la machine cible à travers le réseau d'interconnexion.

Pour le trafic indirect, bien qu'il ne transite jamais par la BFAI, il dépend de l'entrée de la route par défaut dans la table de routage du système d'exploitation, puisque les adresses IP contactées sont les adresses IP « normales » des CSP. Lorsque la BFAI devient indisponible, bien que le chemin physique jusqu'aux CSP (client – ICB – IC – CSP) soit toujours disponible, les machines resteront muettes car dépourvues de route par défaut.

Pour pallier ce problème, les inventeurs ont eu l'idée de mettre en place un mécanisme qui, quand il détecte que le lien vers la BFAI est indisponible, monte l'adresse IP de la BFAI sur l'interface LAN de l'ICB (eth0) pour rétablir la route par défaut des clients. En IPv4, on pourra également envoyer un *Gratuitous* ARP pour accélérer le processus de rafraichissement du cache des machines clientes.

Pour les requêtes DNS, celle vers le serveur principal va faire un *timeout*. En effet, même si l'ICB faisait transiter le trafic DNS par le réseau d'interconnexion, le serveur DNS de l'opérateur refuserait la connexion car il ne proviendrait pas d'un de ses clients. On laisse donc la requête DNS vers le serveur primaire expirer, et on bascule alors sur le serveur DNS secondaire (celui du fournisseur de l'infrastructure d'interconnexion). Les requêtes DNS seront alors routées vers le réseau d'interconnexion par l'ICB.

Pour le trafic indirect, l'ICB est devenu passerelle par défaut des machines du LAN du client. Le trafic est donc adressé à l'ICB (et plus au BFAI). L'ICB va router les paquets sans qu'on force le processus comme avant.

Si le trafic est encapsulé dans un VLAN, on n'aura pas à le décapsuler puisqu'il arrivera directement sur l'interface eth0.vlan.

Pour éviter de router tout le trafic en provenance du LAN, les inventeurs ont eu l'idée de laisser passer uniquement les paquets vers les CSP et le serveur DNS du fournisseur de l'infrastructure d'interconnexion. Le trafic à destination d'Internet ne transitera pas par le réseau d'interconnexion et recevra des messages d'erreur ICMP.

Un deuxième problème existe également lorsque la BFAI fait également office de serveur DHCP. En effet les machines dont l'adresse IP a été servie via DHCP finissent par arrêter d'utiliser ces IP si le serveur DHCP ne répond plus (testé sous Linux et Windows).

Une première solution serait de déployer un serveur DHCP à part entière qui remplacerait l'ICB pour ce rôle. Ainsi lorsque la BFAI devient indisponible, le serveur DHCP répond toujours, les machines clientes gardent leurs IP et continuent de communiquer avec les CSP directs.

Une autre solution serait d'avoir un serveur DHCP secondaire qui communiquerait avec celui de la BFAI pour se tenir à jour et prendre le relai en cas de défaillance de la BFAI. On éliminerait ainsi le *single point of failure*.

Cependant, ces deux solutions ne sont pas convenables car on se veut le moins intrusif possible dans le réseau de l'utilisateur.

La solution consiste à simuler un serveur DHCP au niveau de l'ICB pour assurer une continuité du service. On ne va pas allouer de nouvelles adresses IP afin d'éviter d'avoir des conflits. En revanche, au niveau de l'ICB, les inventeurs ont eu l'idée de simuler les messages qu'aurait renvoyés le serveur DHCP en temps normal afin que les clients ne se rendent pas compte que le serveur DHCP de la BFAI est indisponible et continuent à transmettre sur le réseau.

4.3.1.14 Lien opérateur indisponible

La perte du lien avec l'opérateur Internet (mais pas de la BFAI) provoquera l'expiration du temporisateur de la requête DNS vers le DNS primaire, puis la bascule sur le DNS du fournisseur de l'infrastructure d'interconnexion. L'ICB routera les requêtes DNS vers le serveur du fournisseur de l'infrastructure d'interconnexion.

Les accès indirects se feront comme auparavant et seront interceptés par l'ICB. Le contenu à destination d'Internet ne transitera pas par le réseau d'interconnexion et recevrai des messages d'erreur ICMP.

Les accès directs ne sont ainsi pas impactés.

4.3.1.15 Reprise

Lorsque l'ICB détecte que l'environnement est à nouveau dans son état normal, il reprend sa configuration d'origine. La route statique vers le fournisseur de l'infrastructure d'interconnexion redevient à nouveau disponible et les tunnels peuvent à nouveau passer par le réseau d'interconnexion.

4.3.1.16 Spanning tree

Si le réseau de l'utilisateur est dans une configuration en triangle avec du *spanning tree* pour sécuriser son réseau local LAN, et que la BFAI jouant le rôle d'un des commutateurs, on ne pourra pas mettre en coupure l'ICB classique. Il faudrait un boitier avec au moins une interface réseau en plus pour pouvoir jouer le rôle que jouait la BFAI. Le fait de placer ce boitier ne change pas la capacité de redondance du réseau du client. Si la BFAI (dans l'ancienne configuration) ou l'ICB (dans la nouvelle configuration) devient indisponible, l'accès à Internet devient également indisponible.

Il également est possible, avec un boitier comprenant deux paires de cartes avec un court-circuit, d'améliorer la robustesse du nouveau réseau. Si l'ICB devient indisponible, les deux cartes passent en court-circuit et l'accès à Internet est toujours possible. Pour des raisons de faisabilité du boitier et de coût, cette solution n'est pas envisageable comme une offre normale, mais plutôt comme une option à laquelle le client peut souscrire moyennant un surcout.

Une autre solution pourrait être d'ajouter un commutateur avant l'ICB. Cependant cette solution n'est pas envisageable pour plusieurs raisons :

- Il faudrait ajouter un commutateur dans le réseau du client. C'est un équipement dont on ne veut pas avoir la responsabilité.
- Ce changement d'architecture permettrait de garder la redondance dans le LAN, mais on perdrait la redondance avec la BFAI et Internet.

4.3.1.17 Apprentissage et liste blanche

La décision de dévier ou non le trafic vers le réseau d'interconnexion est basé sur l'adresse IP de destination du paquet. Lorsque l'adresse IP est inconnue, le comportement par défaut est de laisser passer les données vers la BFAI.

Il est cependant possible d'apprendre certaines informations des paquets qui traversent l'ICB.

Le scénario d'accès à un CSP peut se diviser en trois étapes :

1. À partir de l'adresse d'accès au CSP, le client va tout d'abord en extraire le nom de domaine et effectuer une résolution DNS pour savoir vers qu'elle adresse IP destination il doit se connecter ;
2. Une fois le canal de communication ouvert avec le serveur cible, le client va émettre une requête ;

3. Le serveur, après avoir analysé la requête soumise va renvoyer le contenu idoine et fermer le canal de communication.

Si un client accède au CSP en effectuant une requête DNS, et si l'ICB est en coupure du serveur DNS, il détecte la requête DNS vers un CSP et écoute la réponse pour apprendre l'adresse IP.

Plus particulièrement, Lorsque l'ICB est en coupure du serveur DNS (par exemple, si ce service est intégré au BFAI), l'ICB peut observer le processus de résolution DNS. Ainsi, l'ICB détecte la requête DNS concernant un domaine émise par le client. Cette requête contient le type d'information souhaité ainsi que la cible de la question. En revanche, cette requête ne contient pas l'information intéressante pour le processus présentement décrit, à savoir l'adresse IP du serveur cible. Il n'est donc pas nécessaire d'effectuer un traitement particulier les paquets DNS de type « question ». Par contre, les paquets DNS de type « réponse » présente un intérêt dans le cadre du processus d'apprentissage. En effet, ces paquets contiennent à la fois la réponse du serveur DNS avec les données demandées, et une copie de la question initiale.

En analysant ces paquets, on peut par exemple récupérer les adresses IP associées à un domaine.

Dans ce mode de réalisation, l'analyse d'un paquet DNS commence par une étape de vérification d'au moins une partie des champs d'état et de comptage. L'objectif est de vérifier le type de paquet DNS, le code de réponse, le nombre de questions et de réponses. Cette vérification permet de ne pas traiter les paquets d'un mauvais type ou ne contenant pas de réponse et évite que le processus ne soit trop gourmand en ressources.

Lorsque les champs d'état conviennent, la question (c'est-à-dire la requête initiale) comprise dans le paquet est analysée. Plus particulièrement une question du type (champs Qtype) est recherchée. Dans le cas d'adresses IP, la question doit porter sur un enregistrement DNS de type A. L'analyse se poursuit donc par une étape de recherche, au sein du paquet, d'un type QType dont la valeur est à « A ».

Lorsqu'une question de type « A » est identifiée, le nom de domaine associé est extrait, par l'intermédiaire d'une étape d'extraction. Ce nom de domaine est comparé, dans une étape de comparaison, à des entrées d'une base de données. Cette base de données comprend des noms de domaines qui sont associés à du trafic « CSP ». La structure de cette base de données est optimisée pour tirer parti de la structuration en arborescence du DNS.

Lorsque le nom de domaine du paquet DNS correspond à une entrée dans la base de données, on poursuit l'exploration du paquet DNS en analysant chaque réponse. Après s'être assuré que la réponse est du bon type, on en extrait l'adresse IP.

Cette adresse est ensuite comparée aux entrées d'une deuxième base de données, qui contient les adresses IP apprises, et pour lesquelles le processus de déviation de trafic sera mis en œuvre. Cette deuxième base de données est appelée liste d'adresses IP apprises. Si l'adresse IP n'a pas déjà été apprise, elle est alors ajoutée en tant qu'entrée dans cette base de données, ainsi qu'au processus de déviation de trafic. Lorsque l'adresse a déjà été apprise, la date d'utilisation de cette adresse est mise à jour (pour pouvoir être suivie par la suite).

Cette deuxième base de données est optimisée pour pouvoir effectuer des recherches rapides. Ainsi, chaque insertion ou suppression est réalisée de telle sorte que la liste d'adresses IP apprises soit toujours ordonnée. Cela permet de faire une recherche dichotomique lorsqu'on cherche à savoir si l'IP est apprise ou non.

Si l'ICB n'est pas en coupure du serveur DNS, il est toujours possible d'apprendre des informations, depuis le champ *Host* des requêtes HTTP par exemple. Plus particulièrement, il est possible d'apprendre des adresses IP en observant les échanges réalisés sur le réseau. Par exemple, une requête HTTP à destination d'un serveur de CSP contiendra l'adresse IP cible dans les en-têtes TCP, mais également le nom de domaine cible dans le champ Host des en-têtes HTTP. Cependant, cette méthode, bien qu'intéressante en tant que méthode de secours est sous optimale pour deux raisons :

- Pour accéder au champ Host d'une requête HTTP, il faut reconstruire la session TCP pour pouvoir en extraire les données effectives, puis remonter dans les couches pour accéder aux en-têtes HTTP. Ceci est lent et couteux en termes de ressources.
- La quasi-totalité des échanges avec les CSP se fait de manière sécurisée via le protocole HTTPS. Il n'est pas possible d'accéder trivialement aux entêtes HTTP sous la couche de sécurité.

Ainsi, lorsque cela est possible, l'apprentissage en observant les échanges DNS, tel que décrit préalablement, est privilégié.

Pour garder le processus de déviation de trafic le plus efficace et le plus pertinent possible, il est important que la liste d'adresses IP apprises ne contiennent aucune entrée superflues et se limite rigoureusement à l'ensemble des IP cibles utilisées par le client.

Le premier mécanisme consiste à procéder à un nettoyage automatique des adresses IP, nettoyage basé sur leur fréquence d'utilisation et leur date d'apprentissage. Il n'est en effet pas nécessaire de conserver en mémoire une adresse IP qui n'a pas été utilisée depuis un long moment. Dans ce cas, un processus automatisé se charge de détecter ces adresses IP obsolètes et de les supprimer de la base de données et du processus de décision. Pour ce faire, comme explicité plus haut, la base de données des adresses IP apprises comprend en outre un champ permettant de marquer la date de dernière utilisation de l'adresse IP en question.

Lorsqu'un ICB apprend une nouvelle adresse IP, il transmet une alerte à un serveur de vérification dans le réseau d'interconnexion. Le serveur peut éventuellement vérifier si cette nouvelle IP correspond à un changement dans les enregistrements DNS du CSP. Ainsi, l'apprentissage d'une nouvelle adresse IP peut-être soumise à une validation par un serveur maître. En effet, une adresse IP apprise en observant les requêtes DNS peut finalement être confiée à un transitaire Internet par le réseau d'interconnexion, car elle n'est pas présente dans les tables de routages spécifiques vers les CSP. Si tel est le cas, on aura dévié le trafic pour finalement le renvoyer vers Internet. Pour éviter ce saut inutile par le réseau d'interconnexion, l'ICB peut soumettre l'adresse IP apprise à un serveur de validation au sein du réseau Cloud. Ce serveur se charge de vérifier la pertinence de l'adresse IP et en informe l'ICB. Tant que l'adresse IP n'est pas validée par le serveur maitre, elle n'est pas ajoutée à la base de données et au processus de déviation.

De plus, pour accélérer le traitement des adresses IP inconnues, l'ICB peut utiliser ce mécanisme d'apprentissage pour constituer une liste blanche des adresses IP qu'il faut constamment laisser passer vers la BFAI (typiquement toutes les adresses IP utilisées qui ne correspondent pas à des CSP). Ainsi, la remontée de ces informations permet également, lors d'une mise à jour du système, de lancer directement l'ICB avec cette liste statique, ce qui a pour effet d'accélérer le traitement des flux à destination des CSP.

La présence de cette liste évitera à l'ICB de devoir remonter au niveau applicatif à chaque IP inconnue qu'il rencontre.

Pour éviter que la liste soit trop importante, un système de nettoyage basé sur la fréquence d'utilisation et l'âge de l'adresse IP supprime les adresses IP superflues.

Cependant, cette solution comporte plusieurs problèmes techniques qui font que ce mécanisme peut être remplacé par un autre.

Pour les flux sécurisés, on ne peut rien apprendre du niveau applicatif (HTTPS par exemple).

Bien que pour les requêtes DNS, la lecture des informations soit un processus assez simple (grâce à UDP), cela devient beaucoup plus complexe et gourmand en ressource s'il est préférable de faire ça sur toutes les requêtes HTTP par exemple. Il faut reconstruire la session TCP avant de pouvoir accéder à la couche applicative et au champ *Host*.

Si un ICB apprend une nouvelle IP, il se peut que lorsqu'elle transite sur le réseau d'interconnexion, elle soit directement routée vers l'extérieur car inconnue des routeurs. On aura consommé des ressources pour finalement renvoyer le paquet sur Internet.

Bien que les serveurs DNS du fournisseur de l'infrastructure d'interconnexion sont censés être le plus à jour possible, on pourra éventuellement utiliser le mécanisme de détection d'adresse IP inconnue via les requêtes DNS uniquement (et si ce n'est pas trop couteux) pour émettre des alertes et forcer une vérification active des enregistrements DNS au cœur du réseau d'interconnexion.

Les méthodes précédemment décrites sont mise en œuvre par des moyens équivalents, lesquels peuvent se présenter sous la forme de modules, logiciels ou matériels, pouvant être intégrés au sein de l'ICB.

REVENDICATIONS

1. Passerelle d'accès à un réseau d'interconnexion (ICB) d'un système de transmission de données comprenant un premier réseau local, dit réseau client, un deuxième réseau local dit réseau cloud et un réseau d'interconnexion connectant ledit réseau client et ledit réseau cloud, caractérisée en ce que ladite passerelle comprend des moyens d'identification et de routage de données dudit réseau client à destination dudit réseau cloud, lesdits moyens d'identification et de routage comprenant des moyens d'apprentissage d'adresses IP à router en fonction de données transmises sur ledit réseau client à destination d'un troisième réseau dit réseau BFAI.

2. Passerelle selon la revendication 1, caractérisé en ce qu'elle comprend en outre des moyens de création d'au moins deux tunnels de transmission de données au travers dudit réseau d'interconnexion et des moyens de sélection, parmi lesdits au moins deux tunnel, d'au moins un tunnel d'au moins un tunnel de transmission de paquet, en fonction d'au moins un paramètre prédéterminé.

3. Passerelle selon la revendication 2, caractérisé en ce que lesdits type de tunnels sont basés sur le protocole UDP.

4. Passerelle selon la revendication 2, caractérisé en ce que ledit au moins un paramètre prédéterminé appartient au groupe comprenant :

- un état de disponibilité d'un lien entre ledit réseau local et ledit réseau d'interconnexion ;
- un état de disponibilité d'un lien entre ledit réseau local et un réseau maillé étendu ;
- une classe de trafic associée à au moins un paquet de données à transmettre.

5. Passerelle selon la revendication 1, caractérisé en ce qu'elle comprend en outre des moyens d'identification d'une destination d'un paquet en fonction d'au moins une adresse de destination dudit paquet.

6. Passerelle selon la revendication 1, caractérisé en ce qu'elle comprend en outre :

- des moyens de détection d'une coupure d'accès dudit réseau client vers un réseau

maillé étendu, auquel ledit réseau client est connecté par l'intermédiaire d'une passerelle d'accès (BFAI) ;

- des moyens d'attribution d'une adresse IP préalablement attribuée à ladite passerelle BFAI à une interface de communication de ladite passerelle ;
- des moyens de filtrage de paquet de sorte que seuls des paquets à destination dudit réseau cloud soient transmis sur ledit réseau d'interconnexion.

7. Système de transmission de données, comprenant un premier réseau local, dit réseau client, un deuxième réseau local dit réseau cloud et un réseau d'interconnexion connectant ledit réseau client et ledit réseau cloud, ledit réseau client comprenant en outre une passerelle d'accès à un réseau maillé étendu (BFAI), ledit système étant caractérisé en ce qu'il comprend en outre, au niveau du réseau client, une passerelle d'accès audit réseau d'interconnexion (ICB) comprenant des moyens d'identification et de routage de données dudit réseau client à destination dudit réseau cloud.

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/059754

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/28
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/236855 A1 (PELES AMIR [IL]) 25 November 2004 (2004-11-25) abstract; figures 1,4 paragraph [0026]	1-7
A	US 2009/252044 A1 (BHASKARAN SAJIT [US] ET AL) 8 October 2009 (2009-10-08) abstract; figure 1	1-7

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 June 2013	18/06/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Fantacone, Vincenzo

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/059754

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004236855 A1	25-11-2004	NONE	
US 2009252044 A1	08-10-2009	US 7620037 B1	17-11-2009
		US 2009252044 A1	08-10-2009

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2013/059754

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L12/28
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2004/236855 A1 (PELES AMIR [IL]) 25 novembre 2004 (2004-11-25) abrégé; figures 1,4 alinéa [0026]	1-7
A	US 2009/252044 A1 (BHASKARAN SAJIT [US] ET AL) 8 octobre 2009 (2009-10-08) abrégé; figure 1	1-7

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
11 juin 2013	18/06/2013

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Fantacone, Vincenzo

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2013/059754

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2004236855 A1	25-11-2004	AUCUN	
US 2009252044 A1	08-10-2009	US 7620037 B1	17-11-2009
		US 2009252044 A1	08-10-2009