(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
1 octobre 2015 (01.10.2015)

WIPO | PCT

(10) Numéro de publication internationale
WO 2015/145018 A1

(51) Classification internationale des brevets : *H04L 29/06* (2006.01)

(21) Numéro de la demande internationale : PCT/FR2015/050616

(22) Date de dépôt international : 12 mars 2015 (12.03.2015)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1452550 26 mars 2014 (26.03.2014) FR

(71) Déposant : **BULL SAS** [FR/FR]; Rue Jean Jaurès, F-78340 Les Clayes sous Bois (FR).

(72) Inventeurs : **BOZGA, Liana**; 25 Le Routoir, F-38240 Meylan (FR). **DAVY, Louis**; 25 allée de Prémol, F-38320 Poisat (FR). **GERPHAGNON, Jean-Olivier**; 20 avenue du Grand Champ, F-38180 Seyssins (FR).

(74) Mandataire : **CAMUS, Olivier**; Cabinet Camus Lebkiri, 25 rue de maubeuge, F-75009 Paris (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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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, KM, ML, MR, NE, SN, TD, TG).

Publiée :

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

(54) **Title** : METHOD OF PROCESSING A MESSAGE IN AN INTERCONNECTION DEVICE

(54) **Titre** : PROCÉDÉ DE TRAITEMENT D'UN MESSAGE DANS UN DISPOSITIF D'INTERCONNEXION

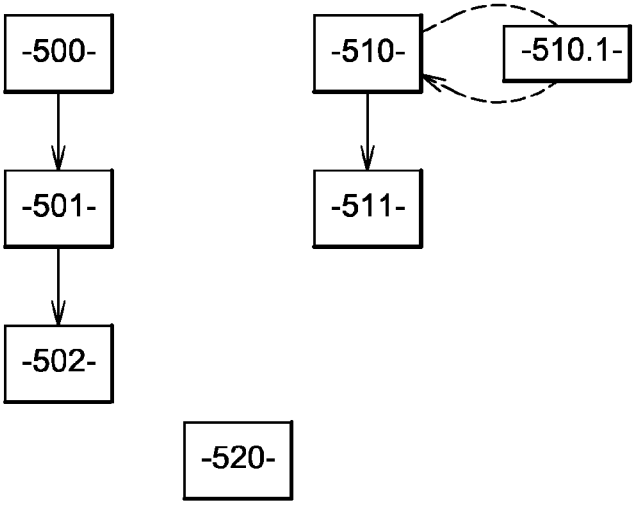

Fig. 2

(57) **Abstract** : The invention relates to a method of processing a message by means of a first interconnection device, said method being characterised in that it comprises the following steps: recording a first database of processing rules in the first interconnection device, recording an identifier of a second interconnection device in the first interconnection device, and processing a communication in accordance with local processing rules of the first local database of rules and with remote processing rules obtained from a second interconnection device which is identified by means of the identifier of the second interconnection device.

(57) **Abrégé** : L'invention se rapporte à un procédé de traitement d'un message par un premier dispositif d'interconnexion caractérisé en ce qu'il comporte les étapes suivantes : - Enregistrement, dans le premier dispositif d'interconnexion, d'une première base de données de règles de traitement - Enregistrement, dans le premier dispositif d'interconnexion, d'un identifiant d'un deuxième dispositif d'interconnexion, - Traitement d'une communication selon - Des règles de traitement locales de la première base de données locale de règles - Des règles de traitement distantes obtenues d'un deuxième dispositif d'interconnexion identifié par l'identifiant du deuxième dispositif d'interconnexion.

WO 2015/145018 A1

Procédé de traitement d'un message dans un dispositif d'interconnexion

DOMAINE TECHNIQUE DE L'INVENTION

[0001] L'invention se rapporte au dispositif d'interconnexion dans le domaine d'acheminements de messages à travers un réseau. L'invention se rapporte également à la sécurité de réseaux informatiques dans lesquels des paquets de données, ou messages, sont acheminés.

[0002] On entendra par dispositif d'interconnexion, dans le cadre de la présente demande, tout dispositif permettant d'interconnecter de façon intelligente au moins deux dispositifs de traitement de données. On parle de dispositif d'interconnexion. Sont en particulier visés les, commutateurs (switches) et routeurs.

ETAT DE LA TECHNIQUE ANTERIEURE

[0003] Dans un environnement réseau, pour la gestion de la sécurité, il est primordial de pouvoir définir des règles d'accès aux équipements qui sont reliés à travers lui. Dans une solution actuelle les équipements réseau permettent de définir des listes d'accès (ACL pour Access Control List) contenant des règles à appliquer sur les données (messages ou trames) circulant à travers les dits équipements. L'application desdites règles se fait sur chaque équipement de manière «autonome» et sans cohérence globale à l'échelle du réseau qu'il soit local ou étendu. Cela signifie que chaque équipement doit définir les règles et les appliquer à son propre niveau et pas d'une manière globale homogène.

[0004] De ce fait, si des configurations sont modifiées sur un équipement, en désaccord avec la politique globale, de manière volontaire ou involontaire, la détection sera complexe et une brèche de sécurité potentiellement ouverte. Cependant, cette solution est la meilleure si les règles de sécurité sont différentes sur chaque équipement et sans cohérence. Cependant cela est rarement, si ce n'est jamais, le cas.

[0005] Dans la pratique les configurations sont recopiées à l'identique sur tous les dispositifs ce qui est une source d'erreurs, d'incohérences et de perte de performance. En effet un dispositif se retrouve encombré avec des règles

correspondant à des paquets qu'il ne recevra jamais. Pour autant le dispositif essaie de tenir compte de ces règles.

[0006] Il est à noter que dans les solutions existantes, dans le cadre d'un réseau « routé » (i.e. un réseau dans lequel un ou plusieurs équipements sont chargés de définir les routes que doivent prendre les paquets selon leur origine et leur destination) la gestion des ACLs est souvent réalisée sur ces équipements et les règles non-définies sur les équipements terminaux.

[0007] De surcroît, si aucune ACL n'est définie au niveau des switches reliant les équipements terminaux (hosts) les contrôles d'accès ne seront appliqués que dans le cas où les trames réseaux sont obligées de passer par l'équipement de routage. Si les trames restent localisées au niveau du dit switch l'application des règles ne sera pas réalisée.

EXPOSE DE L'INVENTION

[0008] L'invention vise à remédier à tout ou partie des inconvénients de l'état de la technique identifiés ci-dessus, et notamment à proposer des moyens pour permettre à des dispositifs d'interconnexion de partager une configuration, cette configuration étant un ensemble de règles de traitements.

[0009] Dans ce dessein, un aspect de l'invention se rapporte à un procédé de traitement d'un message par un premier dispositif d'interconnexion caractérisé en ce qu'il comporte les étapes suivantes :

- Enregistrement, dans le premier dispositif d'interconnexion, d'une première base de données de règles de traitement
- Enregistrement, dans le premier dispositif d'interconnexion, d'un identifiant d'un deuxième dispositif d'interconnexion,
- Traitement d'une communication selon
    - Des règles de traitement locales de la première base de données locale de règles
    - Des règles de traitement distantes obtenues d'un deuxième dispositif d'interconnexion identifié par l'identifiant du deuxième dispositif d'interconnexion.

[0010] Outre les caractéristiques principales qui viennent d'être mentionnées dans le paragraphe précédent, le procédé/dispositif selon l'invention peut

présenter une ou plusieurs caractéristiques complémentaires parmi les suivantes, considérées individuellement ou selon les combinaisons techniquement possibles:

- les règles de traitement distantes sont obtenues pour chaque message traité.
- les règles de traitement distantes sont obtenues à des dates prédéterminées.
- les règles distantes, une fois obtenues, sont enregistrées localement de manière à pouvoir être réutilisées.
- qu'une règle de traitement distante est associée à un identifiant de dispositif d'interconnexion.
- qu'une règle de traitement distante est associée à un horodatage.
- les règles de traitement distantes sont effacées en fonction d'au moins leur horodatage.
- une règle comporte au moins :
    - Une adresse source,
    - Une adresse destination,
    - Un code instruction de traitement parmi au moins :
        -Bloquer le message,
        -Laisser passer le message
- chaque règle de traitement est associée à une priorité
- il comporte une étape d'authentification du premier dispositif d'interconnexion par le deuxième dispositif d'interconnexion

[0011] L'invention se rapporte également à un dispositif de stockage numérique comportant un fichier correspondant à des codes instructions mettant en œuvre le procédé selon l'une des revendications précédentes.

[0012] L'invention se rapporte également à un dispositif mettant en œuvre le procédé selon l'une des revendications précédentes.

BREVE DESCRIPTION DES FIGURES

[0013] D'autres caractéristiques et avantages de l'invention ressortiront à la lecture de la description qui suit, en référence aux figures annexées, qui illustrent :

- la figure 1, une illustration de moyens permettant l'illustration de la mise en œuvre de l'invention ;

- la figure 2, une illustration d'étapes du procédé selon l'invention.

[0014] [...]

[0015] Pour plus de clarté, les éléments identiques ou similaires sont repérés par des signes de référence identiques sur l'ensemble des figures.

[0016] L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci sont présentées à titre indicatif et nullement limitatif de l'invention.

DESCRIPTION DETAILLEE D'UN MODE DE REALISATION

[0017] La figure 1 montre une architecture matérielle dans laquelle l'invention peut être mise en œuvre. La figure 1 montre un premier dispositif 101 connecté et un deuxième dispositif 102 connecté par l'intermédiaire d'un premier dispositif 103 d'interconnexion.

[0018] Un dispositif d'interconnexion est au moins un dispositif de traitement de messages émis par les dispositifs auquel le dispositif d'interconnexion est connecté. En tant que dispositif de traitement le premier dispositif 103 d'interconnexion comporte au moins :

- Un microprocesseur 104,
- Une mémoire 105 de programme comportant au moins de codes instructions correspondant à tout ou partie de l'invention. Pour la présente description ces codes instructions sont au moins ceux d'une partie client de l'invention
- Une mémoire 106 de stockage,
- Un ensemble 107 de connecteurs permettant la connexion du dispositif 103 d'interconnexion.

[0019] Les éléments décrits sont ceux utiles pour une description claire de l'invention. Les mémoires sont des éléments, au sens ensemble d'au moins un composant électronique, séparés ou sont des zones distinctes d'un même élément.

[0020] On parle de tout ou partie de l'invention car celle-ci porte sur une application client-serveur. Il y a donc des codes instructions qui correspondent à la partie cliente, et des codes instructions qui correspondent à la partie serveur.

Dans les mises en œuvre de l'invention les parties clientes et serveurs peuvent être présente sur le même dispositif.

[0021] Dans la pratique lorsque l'on prête une action à un dispositif celle-ci est réalisée par un microprocesseur du dispositif commandé par des codes instructions enregistrés dans une mémoire du dispositif.

[0022] La figure 1 montre que la mémoire 106 de stockage du premier dispositif 103 d'interconnexion comporte une première base 108 de données de règles de traitement. Dans notre exemple cette première base de données de règles de traitement se limite à une table, chaque ligne de la table correspondant à une règle, chaque règle ayant des propriétés correspondant à des colonnes de la table. Une ligne est aussi appelée un enregistrement.

[0023] La figure 1 montre que la mémoire 106 de stockage du premier dispositif 103 d'interconnexion comporte une zone 109 pour enregistrer une adresse d'un deuxième dispositif 203 d'interconnexion connecté au premier dispositif 103 d'interconnexion. Cette zone est désignée comme mémoire d'identification du dispositif d'interconnexion distant. Il s'agit par exemple :

- d'un fichier de configuration dédié,
- d'une section d'un fichier de configuration existant,
- d'une zone située à une adresse prédéterminée sur le moyen de stockage,
- d'une ligne dans une base de données
- …

[0024] Le deuxième dispositif 203 d'interconnexion est lui aussi un dispositif de traitement. Il est similaire au premier dispositif 103 d'interconnexion. Le deuxième dispositif 203 d'interconnexion comporte une base de données de règles et des codes instructions correspondant à l'invention. Pour la présente illustration ces codes instructions correspondent à une partie serveur de l'invention.

[0025] Une adresse est par exemple une adresse au format IPV4, c'est-à-dire une adresse selon la version 4 du protocole IP. Ce pourrait être une adresse IPV6. Il ne s'agit qu'un exemple, dans la pratique il s'agit d'un identifiant routable sur un réseau, qu'il s'agisse d'un réseau Ethernet, InfiniBand, ARIES,… la liste n'est pas exhaustive. Dans ces cas l'adresse IP est à remplacer par son équivalent : adresse mémoire, identifiant matériel unique (GUID)…

[0026] Ainsi une règle comporte au moins :

- Une propriété 1081 identifiant source(s),
- Une propriété 1082 identifiant destination(s),
- Une propriété 1083 code action.

[0027] Pour les propriétés on parle d'identifiant pour désigner :

- Une adresse, telle que précédemment définie, ou
- Un réseau c'est-à-dire un ensemble d'adresses.

[0028] Un code action est au moins parmi :

- Laisser passer, ou
- Bloquer.

[0029] Ainsi le traitement d'un message consiste à déterminer quelles règles s'appliquent à lui, et ainsi de lui appliquer l'action correspondant à la ou les règles correspondantes. Si plusieurs règles correspondent avec des actions contradictoires, on applique un mode de résolutions de conflit connu comme par exemple :

- Chaque règle ayant un numéro d'ordre, c'est-à-dire de classement, c'est l'action de la première règle trouvée qui est appliquée, ou
- Le blocage est prioritaire, ou
- Chaque règle à une priorité, c'est l'action de la règle ayant la priorité la plus élevée qui est appliquée, ou
- … la liste n'est pas exhaustive.

[0030] La figure 1 montre un troisième dispositif 301 connecté, connecté au deuxième dispositif 203 d'interconnexion.

[0031] La figure 1 montre aussi que la mémoire 106 de stockage du premier dispositif 103 d'interconnexion comporte une deuxième base 110 de données ayant la même structure que la première base 108 de données de règles de traitement. Cette deuxième base 110 de données est destinée à enregistrer des règles de traitements issues d'autres dispositifs d'interconnexion. On peut alors parler d'une base 110 de règles de traitements distantes.

[0032] Dans la pratique il pourrait n'y avoir qu'une seule base de données avec des lignes ayant une propriété supplémentaire nommée « Origine » permettant d'enregistrer la provenance de la règle selon qu'elle est :

- Locale : c'est-à-dire propre au dispositif comportant la base de données, ou
- Distante : c'est à dire issue d'un autre dispositif que celui comportant la base de données. Cette propriété Origine peut aussi enregistrer un identifiant de dispositif d'interconnexion permettant de déterminer de quel dispositif elle est issue.

[0033] En général les dispositifs interconnectés suivants :

- Premier dispositif d'interconnexion, et
- Deuxième dispositif d'interconnexion

sont ensemble appelés un réseau. Par extension on considère que les dispositifs connectés à ceux précédemment cités font aussi parti du réseau qui sera désigné comme le premier réseau par la suite.

[0034] La figure 2 montre une étape 500 de configuration du premier dispositif 103 d'interconnexion. Dans cette étape un utilisateur, généralement administrateur du premier réseau, met à jour la première base 108 de données de règles de traitement. Une telle mise à jour requiert une connexion sécurisée et se fait de manière classique :

- A distance
  - Via une interface web (http), ou une interface web sécurisée (https), et un navigateur internet
  - Via une connexion ssh, c'est-à-dire en mode console,
  - …
- En locale
  - En ayant un accès physique au dispositif ce qui permet de s'y connecter via un câble connecté à un connecteur dédié, historiquement RS232, du dispositif : on est alors en mode graphique ou en mode console selon le dispositif.

[0035] Il s'agit là de modes de configuration d'un dispositif d'interconnexion connus.

[0036] Dans l'invention on passe de l'étape 500 à une étape 501 d'enregistrement d'un identifiant du deuxième dispositif 203 d'interconnexion dans la mémoire 109. Cela est réalisé en adaptant l'un des modes de configuration précédemment décrits. Dans le cas d'un mode de configuration graphique on

ajoute une zone de saisie permettant de saisir une valeur pour l'identifiant du deuxième dispositif d'interconnexion. La validation de cette zone de saisie provoque la mise à jour de la mémoire 109 d'identification du dispositif d'interconnexion distant. Dans le cas d'un mode de configuration en ligne de commande, on utilise une nouvelle commande, due à l'invention, dont l'exécution provoque la mise à jour de la mémoire 109 d'identification du dispositif d'interconnexion distant.

[0037] La mémoire 109 peut contenir :

- Une adresse IPV4, IPV6 ou autre.
- Une chaîne de caractère qui peut être résolue en une adresse par l'intermédiaire d'un serveur DNS ou équivalent.

[0038] De l'étape 501 on passe à une étape 502 d'obtention de règles de traitement distante. Dans l'étape 502 le premier dispositif 103 d'interconnexion produit un message de demande de règles de traitement comportant au moins :

- Une adresse de destination, l'identifiant enregistré dans la mémoire 109 d'identification du dispositif d'interconnexion distant,
- Une adresse de réponse, celle du premier dispositif 103 d'interconnexion.
- Un code instruction prédéterminé : ce code instruction est un code de demande de règles.

[0039] Une fois le message de demande de règles produit, il est émis par le premier dispositif 103 d'interconnexion.

[0040] Dans une étape 510 de réception d'un message de demande de règles le deuxième dispositif 203 d'interconnexion reçoit le message de demande de règles de traitement émis par le premier dispositif 103 d'interconnexion. Ce message est identifié comme un message de demande de règles de traitement car :

- Il est destiné au deuxième dispositif d'interconnexion, en effet l'adresse de destination est celle du deuxième dispositif d'interconnexion ;
- Il comporte un code instruction idoine.

[0041] Dans cette étape le deuxième dispositif produit un message de transmission de règles de traitement comportant au moins :

- Une adresse de destination qui vaut la valeur de l'adresse de réponse du message de demande de règles ;
- Une adresse d'émetteur qui vaut l'adresse du dispositif produisant et émettant ce message ;
- Un code instruction prédéterminé : ce code instruction est un code désignant le message comme un message de transmission de règles de traitements.
- Zéro ou N règles de traitement de messages, N étant supérieur ou égal à 1.

[0042] Une fois que le message de transmission de règles est produit, il est émis par le deuxième dispositif d'interconnexion.

[0043] Dans une étape 511, le premier dispositif 103 d'interconnexion reçoit le message de transmission de règles de traitement. Il y récupère les règles de traitement. Il a ainsi obtenu des règles de traitement distantes d'un deuxième dispositif d'interconnexion. Ce message est identifié comme un message de transmission de règles de traitement car :

- Il est destiné au premier dispositif d'interconnexion, en effet l'adresse de destination est celle du premier dispositif d'interconnexion ;
- Il comporte un code instruction idoine.

[0044] Selon des mises en œuvre de l'invention les règles de traitement distantes sont :

- Maintenues dans une mémoire de travail, ou
- Enregistrées dans une base de données locale, par exemple la base 110 de données de règles de traitement distantes.

[0045] L'étape 502 est mise en œuvre, par exemple, selon un intervalle prédéterminé. Cet intervalle prédéterminé permet de déterminer des dates auxquelles l'étape 502 est mise en œuvre.

[0046] Dans une étape 520 de traitement de message le premier dispositif de traitement reçoit un message. Ce message est traité en fonction de ses caractéristiques en particulier adresses source et destination. Ce traitement est effectué selon les règles de traitement locales et selon les règles de traitements distantes. Le traitement d'un message de communication est ici assimilable à un filtrage.

[0047] Dans une variante, qui n'est pas la plus optimale, des règles distantes sont demandées à chaque traitement d'un message de communication.

[0048] Dans un exemple pratique considérons que :

- Le premier dispositif 101 connecté a l'adresse A1,
- Le deuxième dispositif 102 connecté a l'adresse A2,
- Le troisième dispositif 301 connecté a l'adresse A3
- La base de données 108 de règles locales comporte la première règle suivante :
    - Source = A1, Destination = A2, Action = Passer
- Une base de données de règles locales du deuxième dispositif d'interconnexion comporte la deuxième règle suivante :
    - Source = *, Destination = A3, Action = Bloquer
- Le premier dispositif reçoit le message de communication suivant :
    - Source = A1,
    - Destination = A3,
    - Message = Bonjour le monde !

[0049] Sans l'invention, le message de communication serait bloqué par le deuxième dispositif d'interconnexion qu'il doit traverser pour atteindre le troisième dispositif 301 connecté.

[0050] Avec l'invention le premier dispositif d'interconnexion a obtenu la deuxième règle. Il sait donc que le message de communication doit être bloqué. Cela lui évite d'avoir à transmettre le message de communication et permet ainsi d'économiser de la bande passante.

[0051] De même, avant l'invention, dans un environnement réseau, pour la gestion de la sécurité, les équipements réseau permettaient de définir des listes d'accès (ACL pour Access Control List) contenant des règles à appliquer sur les messages circulant à travers les dits équipements. L'application desdites règles se fait sur chaque équipement de manière « autonome » et sans cohérence globale à l'échelle du réseau. Cela signifie que chaque équipement doit définir les règles et les appliquer à son propre niveau et pas d'une manière globale homogène. Cette homogénéité devait être maintenue à la main. Il n'est pas rare, sans l'invention, d'avoir certains équipement bloquant des messages alors que d'autres les laisse passer. Cela peut constituer des brèches de sécurité.

[0052] Avec l'invention il est possible d'avoir un dispositif de référence qui prend en charge la configuration d'un ensemble de dispositifs d'interconnexion.

[0053] Dans une variante de l'invention les règles de traitement locales et les règles de traitements distantes sont enregistrées dans la même base de données qui comporte alors une colonne supplémentaire pour enregistrer la provenance de la règle, par exemple l'adresse de son dispositif d'origine, ou simplement un marqueur booléen indiquant s'il agit ou non d'une règle locale.

[0054] Dans une autre variante de l'invention un dispositif d'interconnexion obtient des règles de traitement de plusieurs dispositifs distant. On note ici qu'un dispositif distant n'est pas nécessairement un dispositif d'interconnexion. Il est au moins un dispositif de traitement qui met en œuvre la partie serveur de l'invention. La partie serveur de l'invention est la capacité de répondre à des messages de demande de règles. La partie client de l'invention est la capacité d'émettre des messages de demande de règles et de traiter les réponses à ces messages.

[0055] Dans une variante de l'invention une règle distante est associée à un horodatage. Cela permet de définir une durée de vie par défaut pour la règle, et/ou une durée à l'échéance de laquelle il faut demander au dispositif distant d'où est issue la règle si celle-ci est encore valable. Un tel horodatage permet aussi de calculer un âge pour la règle. Un âge est le temps calculé entre la date courante et l'horodatage. Dans une variante les règles dont l'âge dépasse une valeur prédéterminée sont ignorées.

[0056] Dans une variante de l'invention une règle distante est associé à un identifiant de version ce qui permet de ne pas réémettre des règles distantes dont la version n'a pas changée sur le dispositif de référence.

[0057] Dans une variante de l'invention, chaque règle étant associée à un identifiant unique de règle, les règles distantes sont supprimées si elles ne sont pas reçues dans la réponse à un message de demande d'émission de règles. Cette absence signifie que les règles en question ont été supprimées sur le dispositif source des règles et que cette suppression et répercutée en cascade sur les dispositifs qui se synchronisent sur le dispositif source.

[0058] Dans une variante de l'invention chaque règle est associée à une priorité, la règle ayant la priorité la plus élevée s'appliquant prioritairement aux autres.

[0059] On vient de décrire un mode de mise en œuvre dans lequel le client, c'est-à-dire le premier dispositif d'interconnexion, demande des règles de traitements. On parle de mode « pull ».

[0060] L'invention reste valable avec un mode de mise en œuvre dans lequel le deuxième dispositif d'interconnexion, ou un dispositif distant, pousse des règles vers le premier dispositif d'interconnexion. Dans ce cas, par symétrie, l'équivalent de la mémoire 109 pour enregistrer une adresse d'un deuxième dispositif d'interconnexion sur le deuxième dispositif devient une zone pour enregistrer au moins une adresse d'un dispositif vers lequel il faut pousser des règles de traitement. Le message de transmission de règle est dans ce cas produit sans qu'une demande ait été reçue. On parle alors de mode « push » ou de mode par abonnement : un dispositif client s'abonne à un dispositif serveur.

Dans une variante de l'invention au niveau du dispositif serveur les règles à transmettre sont marquées comme telles. Ce marquage est, par exemple, réalisée via une colonne supplémentaire dans une table de règle. Il peut aussi s'agir d'un fichier comportant des règles à émettre. Le fait d'être dans ce fichier est alors un marquage.

[0061] Les étapes de l'invention se répartissent dans le temps. Dans la pratique les bases de données de règles de traitement sont à jour au moment du traitement d'un message.

[0062] Un horodatage est :

- une date,
- un marqueur temporelle (timestamp), ou
- un numéro de version. Dans le cas d'un numéro de version on peut utiliser un fonctionnement du type de celui utilisé pour la gestion des numéros de série des enregistrements SOA pour les DNS. Dans ce dernier cas on peut envisager des fichiers de règles gérés comme des fichiers de zone d'un serveur DNS.
- La liste n'est pas exhaustive.

[0063] L'invention a été décrite avec des règles de traitement simples, basées sur des adresses sources et destinations. Dans la pratique l'invention reste valable avec des règles plus complexes utilisant, par exemple, les notions de protocoles (tcp, udp, ftp, http…) ou d'inspection de paquets.

[0064] La description comporte implicitement la notion de récursivité. C'est-à-dire qu'un premier dispositif d'interconnexion, lorsqu'il récupère des règles d'un deuxième dispositif d'interconnexion, peut obtenir des règles que le deuxième dispositif a lui-même obtenu d'un troisième dispositif d'interconnexion.

[0065] Dans une variante de l'invention la zone 109 pour enregistrer une adresse d'un deuxième dispositif permet d'enregistrer plusieurs adresses, chacune de ces adresses correspondant à un dispositif d'interconnexion. Dans ce cas le premier dispositif d'interconnexion obtient des règles de traitements de plusieurs deuxièmes dispositifs d'interconnexion. Dans ce cas aussi on utilise, le cas échéant, un mode de résolution de conflit.

[0066] Dans une variante de l'invention, l'étape 510 de réception d'un message de demande de règles comporte une étape 510.1 préliminaire d'authentification de l'émetteur du message de demande de règles. Une version simple est le teste d'existence de l'adresse de réponse du message dans une liste de demandeurs autorisés. Si l'adresse de réponse existe, alors les règles sont émises. Si l'adresse n'existe pas alors aucune réponse n'est apportée au message de demande de règles.

[0067] Dans une variante plus élaborée, l'authentification est basé sur la mise en place d'un challenge, par exemple basé sur des certificats chaque dispositif ayant le sien, entre le dispositif émettre du message et le dispositif destinataire du message.

[0068] Dans une variante de l'invention, une tentative d'obtention de règles de traitements est déclenchée par la réception d'un message spécifique. Un tel message est, par exemple, émis en mode diffusion par un dispositif d'interconnexion dont au moins une règle de traitement vient d'être modifié.

REVENDICATIONS

1. Procédé de traitement d'un message par un premier dispositif (103) d'interconnexion caractérisé en ce qu'il comporte les étapes suivantes :
   - Enregistrement (500), dans le premier dispositif d'interconnexion, d'une première base (108) de données de règles de traitement
   - Enregistrement (501), dans le premier dispositif d'interconnexion, d'un identifiant (109) d'un deuxième dispositif d'interconnexion,
   - Traitement (520) d'une communication selon
     - Des règles de traitement locales de la première base (108) de données locale de règles
     - Des règles de traitement distantes obtenues (511) d'un deuxième dispositif d'interconnexion identifié par l'identifiant du deuxième dispositif d'interconnexion.

2. Procédé selon la revendication 1 caractérisé en ce que les règles de traitement distantes sont obtenues pour chaque message traité.

3. Procédé selon la revendication 1, caractérisé en ce que les règles de traitement distantes sont obtenues à des dates prédéterminées.

4. Procédé selon la revendication 1 ou 3 caractérisé en ce que les règles distantes, une fois obtenues, sont enregistrées localement de manière à pouvoir être réutilisées.

5. Procédé selon la revendication 4 caractérisé en ce qu'une règle de traitement distante est associée à un identifiant de dispositif d'interconnexion.

6. Procédé selon l'une des revendications 4 ou 5 caractérisé en ce qu'une règle de traitement distante est associée à un horodatage.

7. Procédé selon la revendication 6 caractérisé en ce que les règles de traitement distantes sont effacées en fonction d'au moins leur horodatage.

8. Procédé selon l'une des revendications précédentes caractérisé en ce qu'une règle comporte au moins :
   - Une adresse source,
   - Une adresse destination,
   - Un code instruction de traitement parmi au moins :
     - Bloquer le message,

- Laisser passer le message.

9. Procédé selon l'une des revendications précédentes, caractérisé en ce que chaque règle de traitement est associé à une priorité.

10. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte une étape d'authentification du premier dispositif d'interconnexion par le deuxième dispositif d'interconnexion.

11. Dispositif de stockage numérique comportant un fichier correspondant à des codes instructions mettant en œuvre le procédé selon l'une des revendications précédentes.

12. Dispositif mettant en œuvre le procédé selon l'une des revendications précédentes.

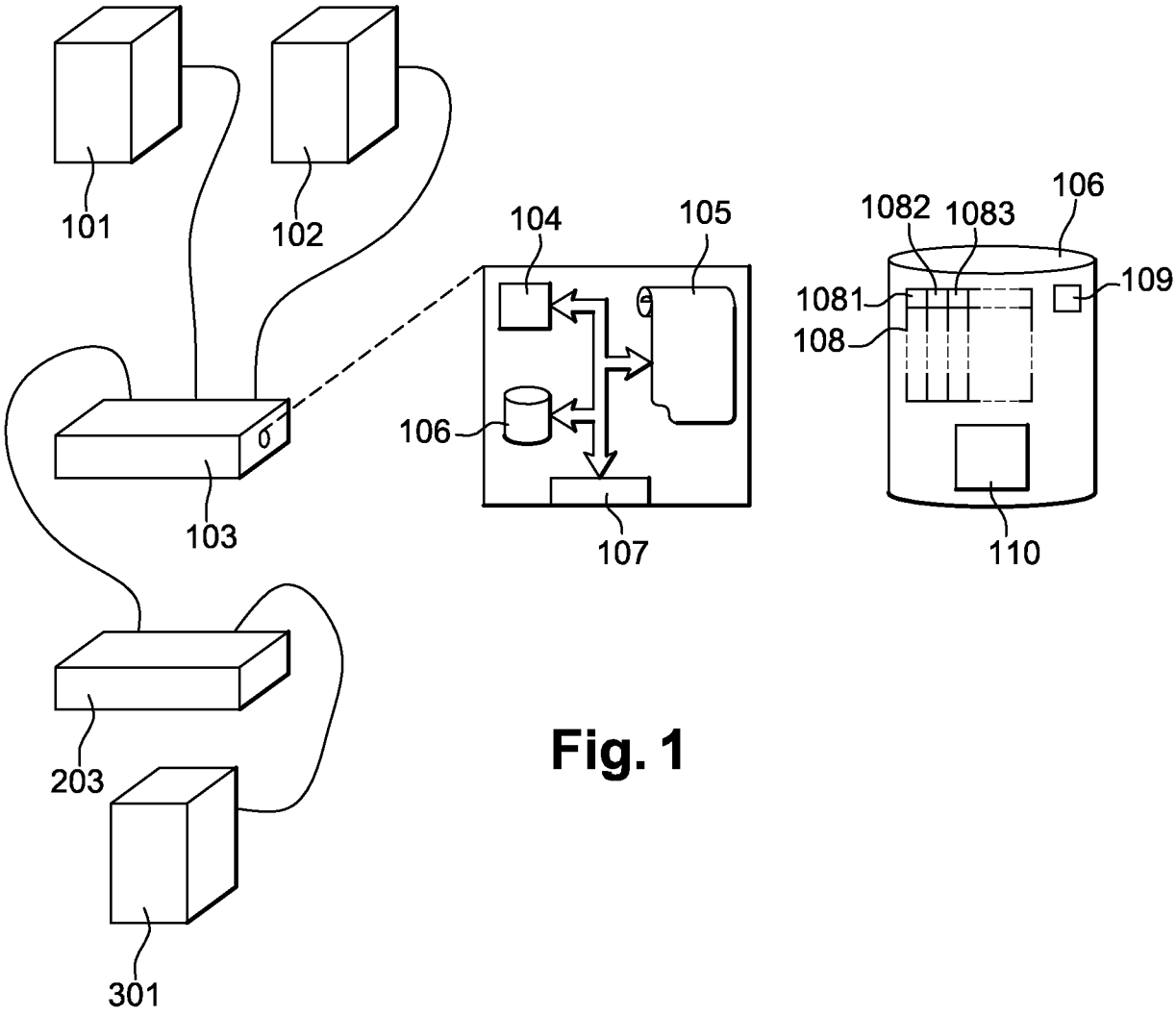
101
102
103
104
105
106
107
1082
1083
106
109
1081
108
110
203
301

Fig. 1

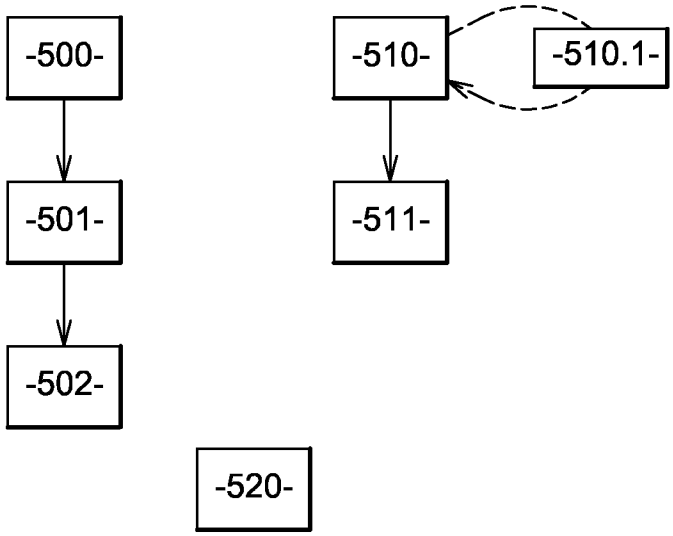
-500-
-501-
-502-
-510-
-510.1-
-511-
-520-

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/050616

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
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, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2012/163587 A1 (ALCATEL LUCENT [FR]; POTE PARAG NARAYANRAO [IN]) 6 December 2012 (2012-12-06) abstract; figure 1 paragraph [0023] - paragraph [0030] paragraph [0038] - paragraph [0045] paragraph [0052] - paragraph [0060] paragraph [0080] - paragraph [0083] -----	1-12
X	US 8 000 328 B1 (KANDEKAR KUNAL [US] ET AL) 16 August 2011 (2011-08-16) abstract column 18, line 10 - column 19, line 7 column 23, line 11 - column 24, line 30 column 25, line 3 - line 36 ----- -/--	1-12

[X] Further documents are listed in the continuation of Box C.

[X] 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
10 June 2015	17/06/2015

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	Lebas, Yves

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/050616

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7 054 930 B1 (CHERITON DAVID [US]) 30 May 2006 (2006-05-30) abstract column 2, line 17 - line 55 column 5, line 19 - column 6, line 23 -----	1-12

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2015/050616

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012163587 A1	06-12-2012	NONE	
US 8000328 B1	16-08-2011	NONE	
US 7054930 B1	30-05-2006	US 7054930 B1	30-05-2006
		US 7779126 B1	17-08-2010

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/050616

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06
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, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 2012/163587 A1 (ALCATEL LUCENT [FR]; POTE PARAG NARAYANRAO [IN]) 6 décembre 2012 (2012-12-06) abrégé; figure 1 alinéa [0023] - alinéa [0030] alinéa [0038] - alinéa [0045] alinéa [0052] - alinéa [0060] alinéa [0080] - alinéa [0083] -----	1-12
X	US 8 000 328 B1 (KANDEKAR KUNAL [US] ET AL) 16 août 2011 (2011-08-16) abrégé colonne 18, ligne 10 - colonne 19, ligne 7 colonne 23, ligne 11 - colonne 24, ligne 30 colonne 25, ligne 3 - ligne 36 ----- -/--	1-12

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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
10 juin 2015	17/06/2015

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	Lebas, Yves

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/050616

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 7 054 930 B1 (CHERITON DAVID [US]) 30 mai 2006 (2006-05-30) abrégé colonne 2, ligne 17 - ligne 55 colonne 5, ligne 19 - colonne 6, ligne 23 -----	1-12

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2015/050616

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2012163587 A1	06-12-2012	AUCUN	
US 8000328 B1	16-08-2011	AUCUN	
US 7054930 B1	30-05-2006	US 7054930 B1	30-05-2006
		US 7779126 B1	17-08-2010