

(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
17 mars 2022 (17.03.2022)



(10) Numéro de publication internationale
WO 2022/053751 A1

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

(21) Numéro de la demande internationale :
PCT/FR2021/051473

(22) Date de dépôt international :
19 août 2021 (19.08.2021)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2009292 14 septembre 2020 (14.09.2020) FR

(71) Déposant : MBDA FRANCE [FR/FR] ; 1, avenue Réau-
mur, 92350 Le Plessis-Robinson (FR).

(72) Inventeurs : POINSARD, Sylvain ; 1 Avenue Réaumur,
92350 LE PLESSIS ROBINSON (FR). CHEVALIER,
Cédric ; 1 Avenue Réaumur, 92350 LE PLESSIS
ROBINSON (FR). RICHER DE FORGES, Romain ; 1
Avenue Réaumur, 92350 LE PLESSIS ROBINSON (FR).

(74) Mandataire : GEVERS & ORES et al. ; Immeuble PA-
LATIN 2, 3 Cours du TRIANGLE, CS 80165, 92939
PARIS LA DEFENSE CEDEX (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, DJ, DK, DM, DO, DZ,
EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,
HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,

(54) Title: METHOD AND FIREWALL CONFIGURED TO MONITOR MESSAGES TRANSITING BETWEEN TWO COMMUNI-
CATION ELEMENTS

(54) Titre : PROCEDE ET PARE-FEU CONFIGURES POUR CONTROLER DES MESSAGES TRANSITANT ENTRE DEUX
ELEMENTS DE COMMUNICATION.

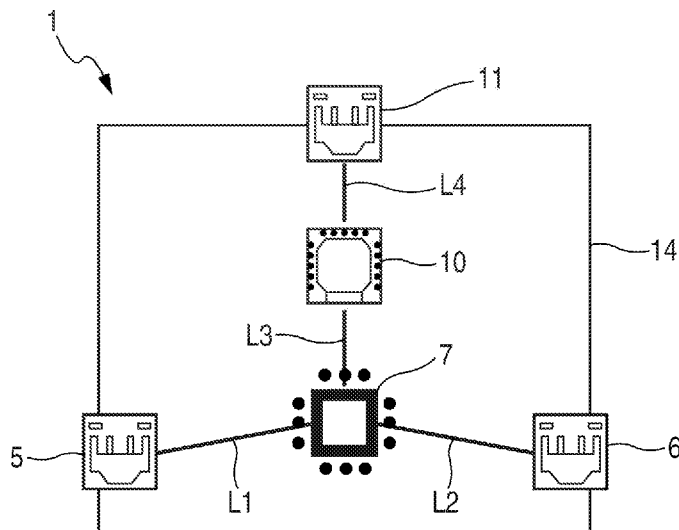


Fig. 2

(57) Abstract: - The firewall (1) comprises a verification unit (7) for comparing messages transiting between the two communication elements with data, called reference data, contained in a database and for detecting, where applicable, a lack of conformity of a message in transit with respect to these reference data, said reference data comprising predetermined messages and at least authorized values for fields of these predetermined messages, a central unit (10) for generating an alert signal in the event of the verification unit (7) detecting a lack of conformity of a message in transit, and a transmission interface (11) configured to transmit any alert signal to at least one alert signal management device, which will generate an appropriate protective action when an alert signal is generated.

OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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), eurasién (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))

(57) Abrégé : - Le pare-feu (1) comporte une unité de vérification (7) pour comparer des messages transitant entre les deux éléments de communication à des données dites de référence contenues dans une base de données et pour détecter, le cas échéant, une absence de conformité d'un message en transit par rapport à ces données de référence, lesdites données de référence comprenant des messages prédéterminés et au moins des valeurs autorisées pour des champs de ces messages prédéterminés, une unité centrale (10) pour générer un signal d'alerte en cas de détection par l'unité de vérification (7) d'une absence de conformité d'un message en transit, et une interface de transmission (11) configurée pour transmettre tout signal d'alerte à destination au moins d'un dispositif de gestion de signaux d'alerte, qui va générer une action de protection appropriée lors de la génération d'un signal d'alerte.

Procédé et pare-feu configurés pour contrôler des messages transitant entre deux éléments de communication.

DOMAINE TECHNIQUE

5

La présente invention concerne un procédé et un pare-feu configurés pour contrôler des messages transitant entre deux éléments de communication.

ÉTAT DE LA TECHNIQUE

10

Dans le cadre de la présente invention, on entend :

- par élément de communication, tout élément informatique tel qu'un ordinateur, un réseau informatique, ..., qui est apte à communiquer avec un autre élément informatique, en étant apte à transmettre et/ou à recevoir des messages ; et
- 15 - par message, un ensemble de données transmis d'un élément de communication à un autre.

On connaît différentes solutions de pare-feux applicatifs, comme des pare-feux de type WAF (« Web Applicative Firewall ») ou des pare-feux applicatifs à reconnaissance de « pattern ».

20

On connaît, en particulier, des pare-feux pour un modèle OSI (pour « Open System Interconnexion » en anglais). Ces pare-feux sont généralement, très performants sur les couches 2 à 6 du modèle OSI. Cependant pour les applications (à savoir la couche 7 du modèle OSI), les pare-feux usuels sont limités à une fonctionnalité dite de « pattern » ou de

25 « signature ». Le traitement se limite à regarder le contenu du message uniquement pour savoir si une forme de signature existe ou non. Ils ne permettent pas de couvrir dans la grande profondeur le besoin en sécurité des applications les plus critiques.

30

Ces solutions usuelles de pare-feu ne sont donc pas satisfaisantes, en particulier pour la couche applicative d'un modèle de communication.

EXPOSÉ DE L'INVENTION

La présente invention concerne un pare-feu configuré pour contrôler des messages transitant dans au moins un sens entre deux éléments de communication, par exemple deux réseaux informatiques ou un ordinateur et un réseau informatique, qui permet de remédier aux inconvénients précités, ledit pare-feu comportant des interfaces vers lesdits éléments de communication.

A cet effet, selon l'invention, ledit pare-feu comporte de plus :

- une unité de vérification configurée pour comparer des messages transitant entre les deux éléments de communication à des données dites de référence contenues dans au moins une base de données et pour détecter, le cas échéant, une absence de conformité d'un message en transit par rapport auxdites données de référence, lesdites données de référence comprenant des messages prédéterminés qui sont connus et au moins des valeurs autorisées pour des champs desdits messages prédéterminés. Avantageusement, les valeurs autorisées pour les champs des messages comprennent au moins certains des éléments suivants : des plages de valeurs, des valeurs minimales, des valeurs maximales, des types, des tailles, ... ;
- une unité centrale configurée pour générer un signal d'alerte en cas de détection par l'unité de vérification d'une absence de conformité d'un message en transit ; et
- au moins une interface de transmission configurée pour transmettre tout signal d'alerte qui est généré, à destination au moins d'un dispositif de gestion de signaux d'alerte.

Avantageusement, ledit pare-feu est configuré pour contrôler des messages d'une couche applicative d'un modèle de communication utilisé pour la communication entre les deux éléments de communication, en particulier une couche dite « 7 » d'un modèle OSI (pour « Open System Interconnexion » en anglais).

Ainsi, grâce à l'invention, ledit pare-feu (de type applicatif) permet de vérifier, en temps réel, la conformité du contenu des messages contrôlés par rapport à des données de référence prédéterminées (concernant des messages connus). Ces données de référence sont adaptées aux caractéristiques du système de communication considéré et aux données et

informations destinées à être échangées par ce système de communication, comme précisé ci-dessous.

Le pare-feu vérifie ainsi chaque message en transit pour des messages parfaitement connus et déterminés. Le pare-feu est ainsi particulièrement bien appliqué au domaine industriel, lorsque les messages considérés (reçus et/ou émis) sont connus.

Dans un mode de réalisation préféré, ledit pare-feu est configuré pour contrôler les messages transitant dans les deux sens entre les deux éléments de communication.

En outre, de façon avantageuse, l'unité de vérification est configurée pour reconnaître, parmi les messages transitant entre les deux éléments de communication, les mêmes messages que ceux des données de référence, et l'unité de vérification est configurée pour comparer aux données de référence, uniquement les messages qui sont ainsi reconnus.

Par ailleurs, avantageusement, les données de référence contenues dans la base de données sont transcrites dans un format informatique exploitable par l'unité de vérification, de préférence un format XML.

Dans un mode de réalisation préféré, les données de référence sont représentatives des informations destinées à être échangées entre les éléments de communication. Par exemple, pour des éléments de communication dans une unité industrielle, il peut s'agir d'informations relatives à des produits fabriqués ou utilisés par cette unité industrielle ou à des informations destinées au fonctionnement ou à la gestion de cette unité industrielle.

La présente invention concerne également un système de communication comportant au moins un élément de communication. Selon l'invention, ledit système de communication comporte, de plus, au moins un pare-feu tel que celui décrit ci-dessus.

Avantageusement, le système de communication comporte, de plus, au moins une base de données contenant les données de référence, lesdites données de référence comprenant donc des messages prédéterminés et au moins des valeurs autorisées pour des champs desdits messages prédéterminés.

En outre, de façon avantageuse, le système de communication comporte, de plus, un dispositif de gestion de signaux d'alerte configuré pour générer une action en cas de réception d'un signal d'alerte du pare-feu.

Avantageusement, le dispositif de gestion de signaux d'alerte est configuré pour ne pas laisser passer un message non conforme détecté. Dans le cadre de la présente invention, d'autres actions sont envisageables, comme précisé ci-dessous.

Dans un mode de réalisation particulier, le dispositif de gestion de signaux d'alerte est configuré pour pouvoir générer une pluralité d'actions différentes possibles et pour générer, le cas échéant, parmi ladite pluralité d'actions possibles, une action dépendant du message non conforme détecté.

Par ailleurs, dans un mode de réalisation particulier, le système de communication comporte également au moins un pare-feu auxiliaire usuel.

La présente invention concerne, en outre, un réseau de communication qui comprend au moins ledit pare-feu et lesdits deux éléments de communication.

La présente invention concerne également un procédé de traitement et de filtrage de messages transitant dans au moins un sens entre deux éléments de communication.

Selon l'invention, ledit procédé comprend au moins :

- une étape de vérification, mise en œuvre par une unité de vérification, consistant à comparer des messages transitant entre les deux éléments de communication à des données dites de référence contenues dans une base de données, et à détecter, le cas échéant, une absence de conformité d'un message en transit par rapport auxdites données de référence, lesdites données de référence comprenant des messages prédéterminés connus et au moins des valeurs autorisées pour des champs desdits messages prédéterminés ; et
- une étape d'alerte, mise en œuvre par une unité centrale, consistant à générer un signal d'alerte en cas de détection d'une absence de conformité par l'unité de traitement.

Avantageusement, ledit procédé comprend, de plus, une étape de protection, mise en œuvre par un dispositif de gestion de signaux d'alerte,

consistant à mettre en œuvre une action, notamment une action de protection, en cas de génération d'un signal d'alerte à l'étape d'alerte.

De plus, de façon avantageuse, l'étape de vérification comprend :

- une sous-étape d'identification consistant à reconnaître, parmi les messages transitant entre les deux éléments de communication, les messages correspondant aux données de référence ; et
- une sous-étape de comparaison consistant à comparer aux données de référence de ladite base de données, uniquement les messages qui sont ainsi reconnus.

10

BRÈVE DESCRIPTION DES FIGURES

Les figures du dessin annexé feront bien comprendre comment l'invention peut être réalisée. Sur ces figures, des références identiques désignent des éléments semblables.

15

La figure 1 est le schéma synoptique d'un réseau de communication pourvu d'un pare-feu conforme à l'invention.

La figure 2 montre schématiquement un mode de réalisation particulier d'un pare-feu conforme à l'invention.

20

La figure 3 illustre schématiquement les étapes principales d'un procédé de traitement et de filtrage de messages, mis en œuvre à l'aide d'un pare-feu conforme à l'invention.

DESCRIPTION DÉTAILLÉE

25

Le pare-feu 1 représenté schématiquement sur la figure 2 et permettant d'illustrer l'invention, est un dispositif informatique destiné à contrôler (ou surveiller) des messages transitant, selon au moins un sens (de communication) I1, I2, entre deux éléments de communication 2 et 3 représentés sur la figure 1. Dans le cadre de la présente invention, un élément de communication peut correspondre à tout élément informatique (tel qu'un ordinateur, un réseau informatique par exemple un réseau informatique local LAN (pour « Local Area Network » en anglais) ...), qui est apte à communiquer

30

avec un autre élément informatique, c'est-à-dire qui est apte à transmettre et/ou à recevoir des messages de ce dernier.

Le pare-feu 1 comporte des interfaces 5 et 6 (représentées sur la figure 2) permettant de le relier (de façon usuelle), respectivement, aux éléments de communication 2 et 3.

Dans un mode de réalisation particulier, ledit pare-feu 1 est configuré pour contrôler les messages transitant dans un seul sens I1 ou I2 entre les deux éléments de communication 2 et 3. A titre d'illustration, il peut s'agir des messages émis par l'élément de communication 3, par exemple un réseau informatique externe à un organisme ou à une entité locale telle qu'une entreprise, à destination de l'élément de communication 2, par exemple un ordinateur ou un réseau de l'entité locale, dans le but de protéger l'élément de communication 2 contre un message non autorisé qui pourrait être potentiellement malveillant et correspondre, notamment, à une tentative d'intrusion.

Dans un mode de réalisation préféré, représenté sur la figure 1, ledit pare-feu 1 est ainsi un élément de sécurité destiné, en premier lieu, à protéger l'élément de communication 2, contre des tentatives d'intrusion malveillantes provenant de l'élément de communication 3. Pour ce faire, il fait partie d'un système de communication 4 comprenant, notamment, ledit l'élément de communication 2 et ledit pare-feu 1.

Par ailleurs, dans une variante préférée de ce mode de réalisation préféré, ledit pare-feu 1 est configuré pour contrôler les messages transitant dans les deux sens I1 et I2 entre les deux éléments de communication 2 et 3, comme illustré par des doubles flèches F et G sur la figure 1, pour protéger les deux éléments de communication 2 et 3, l'un de l'autre.

Dans un mode de réalisation particulier, le pare-feu 1 et les deux éléments de communication 2 et 3 peuvent faire partie d'un réseau de communication 15, par exemple un réseau (de communication) militaire.

Le pare-feu 1 comporte, comme représenté sur la figure 2, sur une carte électronique 14, en plus des interfaces 5 et 6 :

- une unité de vérification (ou de contrôle) 7, par exemple un circuit intégré programmable de type FGPA (« Field-Programmable Gate Array » en anglais),

qui est configurée (et programmée) pour comparer des messages transitant entre les deux éléments de communication 2 et 3 à des données dites de référence d'une base de données 8. Ces données de référence (concernant des messages connus) sont reçues par le pare-feu 1 de la base de données 8, par l'intermédiaire d'une liaison 9, comme représenté sur la figure 1. Par la comparaison de chaque message (qui est pris en compte) avec lesdites données de référence, l'unité de vérification 7 est en mesure de détecter, si cela est le cas, toute absence de conformité d'un message en transit par rapport à ces données de référence. En particulier, les valeurs autorisées pour les champs des messages peuvent comprendre au moins certains des éléments suivants : des plages de valeurs, des valeurs minimales, des valeurs maximales, des types, des tailles, ... ;

- une unité centrale 10, par exemple un processeur ou unité centrale de traitement de type CPU (pour « Central Processing Unit » en anglais), qui est configurée pour générer un signal d'alerte en cas de détection par l'unité de vérification 7 d'une absence de conformité d'un message en transit ; et
- au moins une interface de transmission 11 configurée pour transmettre tout signal d'alerte généré par l'unité centrale 10, à destination d'au moins un dispositif utilisateur, et notamment d'un dispositif 12 de gestion de signaux d'alerte, comme précis ci-dessous.

L'unité de vérification 7 est configurée pour pouvoir reconnaître (ou identifier), parmi les messages transitant entre les deux éléments de communication 2 et 3, les messages de même type (par exemple de même protocole) que ceux qui sont enregistrés dans la base de données 8. L'unité de vérification 7 compare aux données de référence de ladite base de données 8, uniquement le contenu des messages (en transit entre les deux éléments de communication 2 et 3) qui sont ainsi préalablement reconnus.

En plus de générer les signaux d'alerte, l'unité centrale 10 est également configurée pour permettre la gestion de l'unité de vérification 7 et le téléchargement des données de référence de la base de données 8.

Comme représenté sur la figure 2, l'unité de vérification 7 est reliée par l'intermédiaire de liaisons L1, L2 et L3 respectivement à l'interface 5, à l'interface 6 et à l'unité centrale 10, et l'unité centrale 10 est reliée par

l'intermédiaire d'une liaison L4 à l'interface de transmission 11. Ces liaisons L1 à L4 permettent la communication de données entre les éléments reliés ensemble.

Les interfaces 5 et 6 sont chargées de transmettre et recevoir les messages qui passent à travers le pare-feu 1, en provenance ou à destination respectivement de l'élément de communication 2 et de l'élément de communication 3.

Le système de communication 4 comporte également une base de données 8, de préférence externe à la carte électronique 14, qui contient les données de référence précitées. Les données de référence comprennent au moins :

- une liste de l'ensemble des messages possibles (qui peuvent donc être traités par le pare-feu 1) ;
- l'ensemble des valeurs possibles, c'est-à-dire autorisées, pour chacun des champs qui composent chaque message.

Dans un mode de réalisation particulier, le pare-feu 1 peut également comporter plusieurs bases de données 8, dont chacune comporte par exemple des données relatives à des messages à chaque fois d'un type particulier, qui sont par exemple destinés à un projet particulier ou à un produit particulier. On entend par base de données, tout moyen électronique tel qu'une mémoire par exemple, qui fait partie du système de communication 4 et qui permet de stocker l'ensemble des données nécessaires pour permettre à l'unité de vérification 7 de réaliser les comparaisons envisagées.

Ainsi, ledit pare-feu 1 permet de vérifier, en temps réel, la conformité du contenu des messages contrôlés par rapport à des données de référence prédéterminées. Ces données de référence sont adaptées aux données échangées par le système de communication 4. Le pare-feu 1 vérifie ainsi chaque message en transit pour des messages parfaitement connus et déterminés.

En particulier, les messages (contrôlés par le pare-feu 1) sont parfaitement connus, et le contenu possible de chacun de ces messages est précisément identifié, par exemple, dans des documents d'interface utilisés pour définir ou mettre à jour les données de référence contenues dans la base

de données 8. Ils peuvent dépendre, notamment, des données et informations que l'on envisage que le système de communication 4 va échanger. Les documents spécifiant les interfaces et donc les messages à utiliser pour le système de communication 4 permettent d'établir de manière précise une liste de messages susceptibles d'être utilisés et l'ensemble des valeurs possibles pour chaque champ de ces messages. Le pare-feu 1 est donc particulièrement bien adapté au domaine industriel, et plus précisément dans les entreprises ou les secteurs d'activité dans lesquels les messages échangés sont parfaitement connus.

Le pare-feu 1 peut donc lire précisément chaque message et vérifier si les valeurs qui le composent dans les différents champs font partie des valeurs possibles, et si ce message est donc conforme ou non.

Pour ce faire, les données de référence de la base de données 8 sont transcrites dans un format informatique exploitable par l'unité de vérification 7 du pare-feu 1, de préférence un format XML.

Les fichiers XML (pour « Extensible Markup Language » en anglais, à savoir langage de balisage extensible) sont de simples documents texte qui utilisent des balises personnalisées pour décrire et structurer des données. Le format de message XML utilisé permet de décrire les messages qui doivent être analysés au niveau applicatif. Il contient la description des différents champs de chaque message (en précisant notamment des valeurs minimales, des valeurs maximales, des types, des tailles) qui sont spécifiés dans les documents d'interface.

La présente invention peut être appliquée à différents types de protocoles, par exemple des protocoles de type TCP (pour « Transmission Control Protocol » anglais) ou de type UDP (pour « User Datagram Protocol » en anglais).

Le pare-feu 1 est de type applicatif. Il est configuré pour contrôler des messages d'une couche applicative d'un modèle de communication utilisé pour la communication entre les deux éléments de communication 2 et 3.

De préférence, le pare-feu 1 est configuré pour contrôler des messages de la couche 7 du modèle OSI. Le modèle OSI qui représente une norme de communication, en réseau, des systèmes informatiques, comporte sept

couches. La couche 7 qui est une couche d'application est le point d'accès aux services réseaux. Dans le cadre de la présente invention, le pare-feu 1 peut également s'appliquer à la couche applicative d'un modèle de communication autre que le modèle OSI.

5 Le système de communication 4 comporte, de plus, un dispositif 12 de gestion de signaux d'alerte, par exemple de type SIEM (pour « Security Information and Event Management » en anglais, à savoir gestion de l'information et des événements de sécurité), qui est configuré pour générer une action, notamment une action de protection, en cas de réception d'un signal
10 d'alerte. A cet effet, le dispositif 12 est lié par l'intermédiaire d'une liaison 13 (figure 1) à l'interface de transmission 11 qui est en lien avec l'unité centrale 10 (génératrice de signaux d'alerte) via la liaison L4 (figure 2).

Dans un mode de réalisation préféré, le dispositif 12 de gestion de signaux d'alerte est configuré pour agir, de façon usuelle, en ne laissant pas
15 passer un message non conforme. Ainsi :

- un message reçu de l'élément de communication 3, qui est détecté comme non conforme par le pare-feu 1 n'est pas transmis à l'élément de communication 2 (et donc au système de communication 4) pour le protéger contre une éventuelle tentative d'intrusion ;
- 20 - et inversement (dans le mode de réalisation préféré d'une surveillance dans les deux sens de communication), un message émis par l'élément de communication 2 (et donc par le système de communication 4), qui est détecté comme non conforme par le pare-feu 1, n'est pas transmis à l'élément de communication 3.

25 Dans le cadre de la présente invention, d'autres actions (commandées ou gérées par le dispositif 12) sont envisageables en cas de détection d'un message non conforme. A titre d'illustration, il peut s'agir de la suppression du message, de l'archivage du message, de la transmission du message à un élément d'analyse (pour l'analyser), de la coupure de toute transmission
30 ultérieure entre les éléments de communication 2 et 3, d'opérations complexes sur les signaux d'alerte (telles que des corrélations dans le temps par exemple),
...

Dans un mode de réalisation particulier, le dispositif 12 de gestion de signaux d'alerte est configuré pour générer une action qui dépend du message non conforme détecté. On prévoit donc une pluralité d'actions différentes possibles, et lorsqu'un message est considéré comme non conforme, on met
5 en œuvre au moins une action (parmi lesdites actions possibles) qui dépend dudit message. Ces actions peuvent, par exemple, dépendre du type de système de communication 4, auquel est appliqué le pare-feu 1, ou de la nature des données échangées par le système de communication 4.

Par ailleurs, dans un mode de réalisation particulier, le système de
10 communication 4 comporte, en plus du pare-feu 1, un ou de préférence une pluralité de pare-feux auxiliaires usuels (non représentés). Il peut notamment s'agir d'un ou de plusieurs pare-feux usuels qui sont conçus pour analyser des messages qui ne sont pas reconnus par l'unité de vérification 7 et qui ne sont donc pas contrôlés par le pare-feu 1.

15 En particulier, il peut s'agir d'un ou de plusieurs pare-feux usuels qui sont conçus pour protéger les couches 2 à 6 du modèles OSI, et qui sont ainsi complémentaires du pare-feu 1 lorsqu'il est destiné à protéger la couche 7 du modèle OSI. Dans ce mode de réalisation particulier, le système de communication 4 dispose ainsi de protections efficaces contre l'ensemble des
20 couches 2 à 7 du modèle OSI.

Le pare-feu 1, tel que décrit ci-dessus, faisant partie du système de communication 4, permet de mettre en œuvre un procédé P de traitement et de filtrage de messages transitant dans au moins un sens (de communication) entre les deux éléments de communication 2 et 3 ou dans les deux sens.

25 Pour ce faire, ce procédé P comprend, comme représenté sur la figure 3 :

- une étape de vérification E1, mise en œuvre par l'unité de vérification 7, consistant à comparer des messages transitant entre les deux éléments de communication 2 et 3 aux données de référence de la base de données 8, et à
30 détecter, le cas échéant, une absence de conformité d'un message en transit par rapport auxdites données de référence. Les données de référence comprennent des messages prédéterminés qui sont connus et des valeurs autorisées pour des champs desdits messages prédéterminés ;

- une étape d'alerte E2, mise en œuvre par l'unité centrale 10, consistant à générer un signal d'alerte en cas de détection d'une absence de conformité par l'unité de vérification 7 à l'étape de vérification E1 ; et

5 - une étape de protection E3, mise en œuvre par le dispositif 12 de gestion de signaux d'alerte, consistant à générer une action en cas de génération d'un signal d'alerte par l'unité centrale 10 à l'étape d'alerte E2.

De plus, l'étape de vérification E1, mise en œuvre par l'unité de vérification 7, comprend :

10 - une sous-étape d'identification E1A consistant à reconnaître et identifier, parmi les messages transitant entre les deux éléments de communication 2 et 3, les messages qui font partie des données de référence de la base de données 8 ; et

15 - une sous-étape de comparaison E1B consistant à comparer auxdites données de référence de la base de données 8, uniquement les messages qui sont ainsi reconnus et identifiés.

Par conséquent, l'unité de vérification 7 essaie de reconnaître et identifier tous les messages en transit entre les éléments de communication 2 et 3. Un message qui n'est pas reconnu par l'unité de vérification 7 ne sera pas contrôlé par cette dernière, et il sera donc autorisé à passer à travers le pare-
20 feu 1. Ce message pourra être contrôlé par d'autres pare-feux usuels du système de communication 4 qui se chargeront de décider s'il est conforme ou non à la politique de sécurité en vigueur. Il sera alors soit bloqué par ce pare-feu usuel, soit laissé passer.

En revanche, un message qui est reconnu par l'unité de vérification 7
25 sera contrôlé par cette dernière qui émettra un signal d'alerte en cas d'absence de conformité de ce message contrôlé avec les données de référence correspondantes. Dans un tel cas, le dispositif 12 de gestion de signaux d'alerte générera une action appropriée. En particulier, il empêchera le message d'être communiqué à l'élément de communication 2, 3 qui est destinataire.

30 Le pare-feu 1 et le procédé P, tels que décrits ci-dessus, peuvent être utilisés dans beaucoup d'applications différentes. En particulier, ils sont particulièrement bien adaptés au domaine industriel (aviation, militaire, ...),

dans des entreprises ou des secteurs d'activité où les messages échangés sont parfaitement connus.

5 Dans le domaine militaire, le pare-feu 1 peut notamment être utilisé en complément des pare-feux usuels afin de disposer d'une protection efficace permettant des surveillances des flux de communication, en entrée et sortie de systèmes militaires tels qu'un centre de commandement, un poste de préparation de mission, un lanceur,

REVENDEICATIONS

1. Pare-feu configuré pour contrôler des messages transitant dans au moins un sens (11, 12) entre deux éléments de communication (2, 3), ledit pare-feu (1) comportant :
- des interfaces (5, 6) vers lesdits éléments de communication (2, 3) ;
 - une unité de vérification (7) configurée pour comparer des messages transitant entre les deux éléments de communication (2, 3) à des données et pour détecter, le cas échéant, une absence de conformité d'un message en transit par rapport auxdites données ; et
 - une unité centrale (10) configurée pour générer un signal d'alerte en cas de détection par l'unité de vérification (7) d'une absence de conformité d'un message en transit,
- caractérisé en ce que :
- l'unité de vérification (7) est configurée pour comparer les messages transitant entre les deux éléments de communication (2, 3) à des données dites de référence qui sont contenues dans au moins une base de données (8) et pour détecter, le cas échéant, une absence de conformité d'un message en transit par rapport auxdites données de référence, lesdites données de référence comprennent des messages prédéterminés qui sont connus et au moins des valeurs autorisées pour des champs desdits messages prédéterminés ;
 - l'unité de vérification (7) est configurée pour reconnaître, parmi les messages transitant entre les deux éléments de communication (2, 3), les mêmes messages que ceux des données de référence, et pour comparer aux données de référence, uniquement les messages qui sont ainsi reconnus ; et
 - le pare-feu (1) comporte de plus au moins une interface de transmission (11) configurée pour transmettre tout signal d'alerte à destination au moins d'un dispositif (12) de gestion de signaux d'alerte.
2. Pare-feu selon la revendication 1,
- caractérisé en ce qu'il est configuré pour contrôler des messages d'une couche applicative d'un modèle de communication utilisé pour la communication entre les deux éléments de communication (2, 3).

3. Pare-feu selon l'une des revendications 1 et 2, caractérisé en ce qu'il est configuré pour contrôler les messages transitant dans les deux sens (I1, I2) entre les deux éléments de communication (2, 3).

5 4. Pare-feu selon l'une quelconque des revendications précédentes, caractérisé en ce que les données de référence sont transcrites dans un format informatique exploitable par l'unité de vérification (7).

10 5. Pare-feu selon l'une quelconque des revendications précédentes, caractérisé en ce que les données de référence sont représentatives des informations destinées à être échangées entre les éléments de communication (2, 3).

6. Système de communication comportant au moins un élément de communication (2), caractérisé en ce qu'il comporte, de plus, au moins un pare-feu (1) selon l'une quelconque des revendications 1 à 5.

15 7. Système de communication selon la revendication 6, caractérisé en ce qu'il comporte au moins une base de données (8) contenant des données de référence, lesdites données de référence comprenant des messages prédéterminés et au moins des valeurs autorisées pour des champs desdits messages prédéterminés.

20 8. Système de communication selon l'une des revendications 6 et 7, caractérisé en ce qu'il comporte, de plus, un dispositif (12) de gestion de signaux d'alerte configuré pour générer une action en cas de réception d'un signal d'alerte du pare-feu (1).

25 9. Système de communication selon la revendication 8, caractérisé en ce que le dispositif (12) de gestion de signaux d'alerte est configuré pour ne pas laisser passer un message non conforme détecté.

30 10. Système de communication selon l'une des revendications 8 et 9, caractérisé en ce que le dispositif (12) de gestion de signaux d'alerte est configuré pour générer une action dépendant du message non conforme détecté.

11. Système de communication selon l'une quelconque des revendications 6 à 10, caractérisé en ce qu'il comporte au moins un pare-feu auxiliaire.

12. Procédé de contrôle et de filtrage de messages transitant dans au moins un sens entre deux éléments de communication (2, 3),

ledit procédé comprenant au moins :

- une étape de vérification (E1), mise en œuvre par une unité de vérification (7),
5 consistant à comparer des messages transitant entre les deux éléments de communication (2, 3) à des données dites de référence contenues dans une base de données (8), et à détecter, le cas échéant, une absence de conformité d'un message en transit par rapport auxdites données de référence, lesdites données de référence de la base de données (8) comprenant des messages
10 prédéterminés qui sont connus et au moins des valeurs autorisées pour des champs desdits messages prédéterminés, l'étape de vérification (E1) comprenant une sous-étape d'identification (E1A) consistant à reconnaître, parmi l'ensemble des messages transitant entre les deux éléments de communication (2, 3), les messages correspondant aux données de référence,
15 et une sous-étape de comparaison (E1B) consistant à comparer aux données de référence de ladite base de données (8), uniquement les messages qui sont ainsi reconnus ; et
- une étape d'alerte (E2), mise en œuvre par une unité centrale (10), consistant à générer un signal d'alerte en cas de détection d'une absence de conformité
20 par l'unité de vérification (7).

13. Procédé selon la revendication 12,
- caractérisé en ce qu'il comprend, de plus, une étape de protection (E3), mise en œuvre par un dispositif (12) de gestion de signaux d'alerte, consistant à mettre en œuvre une action en cas de génération d'un signal d'alerte à l'étape
25 d'alerte (E2).

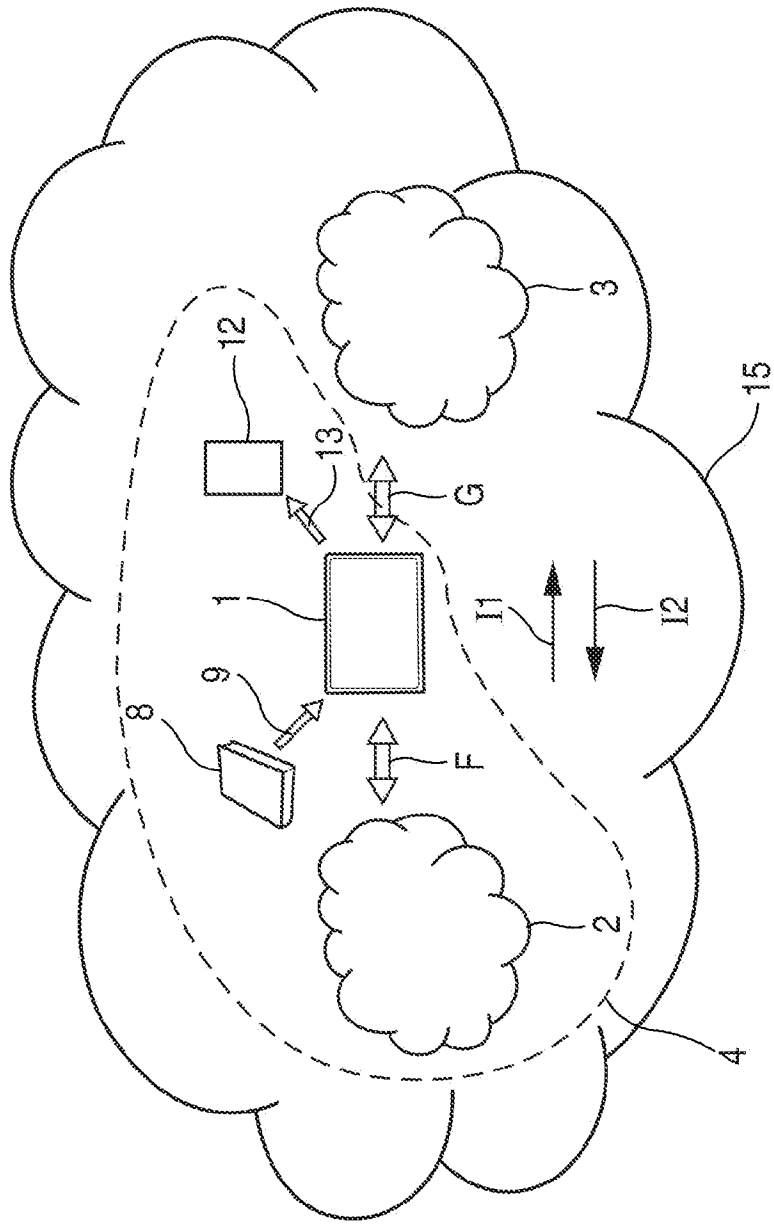


Fig. 1

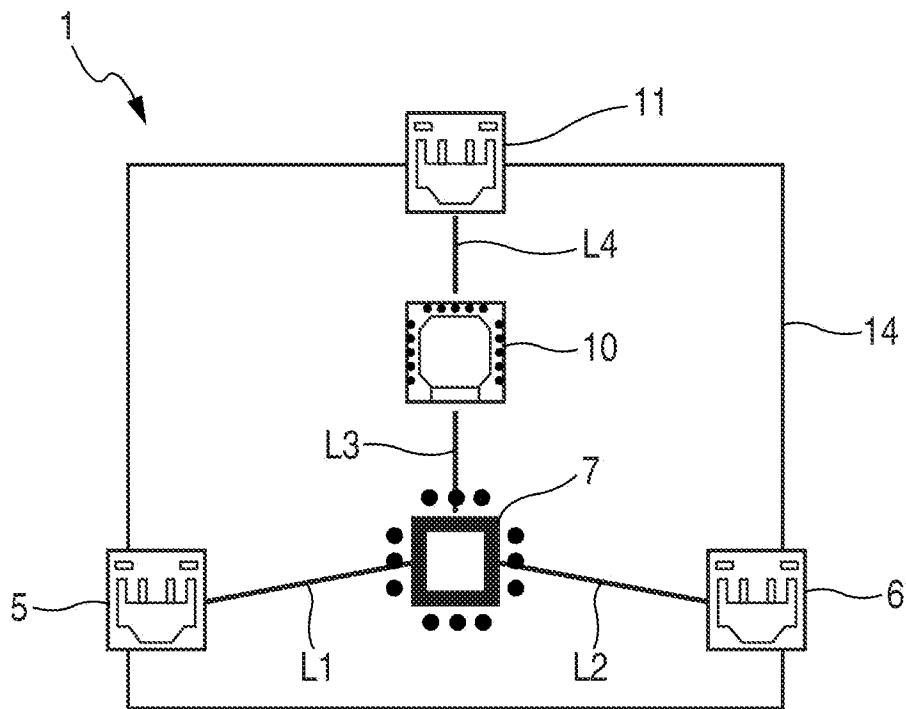


Fig. 2

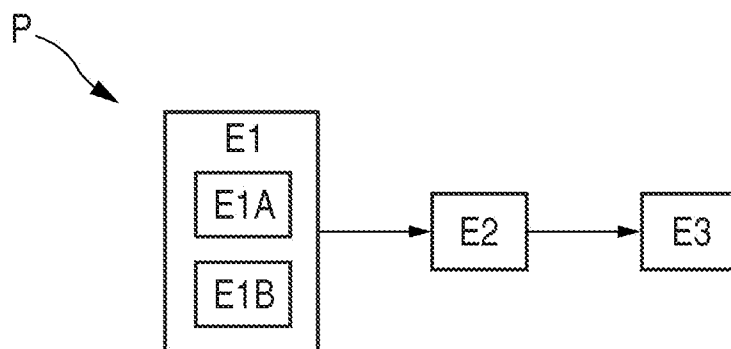


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FR2021/051473

A. CLASSIFICATION OF SUBJECT MATTER H04L 29/06(2006.01)i 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	EP 1802023 A1 (HUAWEI TECH CO LTD [CN]) 27 June 2007 (2007-06-27) paragraph [0003] - paragraph [0015]; figure 1 paragraph [0018] - paragraph [0033] paragraph [0036] - paragraph [0037]	1-13
X	SUSILO W ET AL. "Personal Firewall for Pocket PC 2003: Design & Implementation" <i>ADVANCED INFORMATION NETWORKING AND APPLICATIONS, 2005. AINA 2005. 19TH INTERNATIONAL CONFERENCE ON TAIPEI, TAIWAN 25-30 MARCH 2005, PISCATAWAY, NJ, USA, IEEE</i> , Vol. 2, 25 March 2005 (2005-03-25), pages 661-666 DOI: 10.1109/AINA.2005.279 ISBN: 978-0-7695-2249-4. XP010790093 the whole document	1-13
X	US 2009158428 A1 (WANG BAI LING [CN]) 18 June 2009 (2009-06-18) paragraph [0007] - paragraph [0010] paragraph [0031] - paragraph [0033] paragraph [0037] - paragraph [0040]	1-13
☐ 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 12 November 2021		Date of mailing of the international search report 22 November 2021
Name and mailing address of the ISA/EP European Patent Office p.b. 5818, Patentlaan 2, 2280 HV Rijswijk Netherlands Telephone No. (+31-70)340-2040 Facsimile No. (+31-70)340-3016		Authorized officer Figiel, Barbara Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/FR2021/051473

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
EP	1802023	A1	27 June 2007	AT	454781	T	15 January 2010
				CN	1905555	A	31 January 2007
				CN	101160774	A	09 April 2008
				EP	1802023	A1	27 June 2007
				ES	2355047	T3	22 March 2011
				US	2007234414	A1	04 October 2007
				WO	2007014507	A1	08 February 2007
US	2009158428	A1	18 June 2009	CN	101459660	A	17 June 2009
				US	2009158428	A1	18 June 2009
				US	2014223558	A1	07 August 2014

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 802 023 A1 (HUAWEI TECH CO LTD [CN]) 27 juin 2007 (2007-06-27) alinéa [0003] - alinéa [0015]; figure 1 alinéa [0018] - alinéa [0033] alinéa [0036] - alinéa [0037] -----	1-13
X	SUSILO W ET AL: "Personal Firewall for Pocket PC 2003: Design & Implementation", ADVANCED INFORMATION NETWORKING AND APPLICATIONS, 2005. AINA 2005. 19T H INTERNATIONAL CONFERENCE ON TAIPEI, TAIWAN 25-30 MARCH 2005, PISCATAWAY, NJ, USA, IEEE, vol. 2, 25 mars 2005 (2005-03-25), pages 661-666, XP010790093, DOI: 10.1109/AINA.2005.279 ISBN: 978-0-7695-2249-4 le document en entier ----- -/-	1-13



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

12 novembre 2021

Date d'expédition du présent rapport de recherche internationale

22/11/2021

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Figiel, Barbara

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2009/158428 A1 (WANG BAI LING [CN]) 18 juin 2009 (2009-06-18) alinéa [0007] - alinéa [0010] alinéa [0031] - alinéa [0033] alinéa [0037] - alinéa [0040] -----	1-13

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2021/051473

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1802023	A1	27-06-2007	AT 454781 T	15-01-2010
			CN 1905555 A	31-01-2007
			CN 101160774 A	09-04-2008
			EP 1802023 A1	27-06-2007
			ES 2355047 T3	22-03-2011
			US 2007234414 A1	04-10-2007
			WO 2007014507 A1	08-02-2007

US 2009158428	A1	18-06-2009	CN 101459660 A	17-06-2009
			US 2009158428 A1	18-06-2009
			US 2014223558 A1	07-08-2014
