(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
09 janvier 2020 (09.01.2020)

WIPO | PCT

(10) Numéro de publication internationale
WO 2020/008126 A1

(51) Classification internationale des brevets :
G06F 9/455 (2018.01)

(21) Numéro de la demande internationale :
PCT/FR2019/051586

(22) Date de dépôt international :
27 juin 2019 (27.06.2019)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1856129 03 juillet 2018 (03.07.2018) FR

(71) Déposant : **ORANGE** [FR/FR] ; 78 rue Olivier de Serres, 75015 Paris (FR).

(72) Inventeur : **CHAWKI, Jamil** ; Orange Gardens - TGI/OLR/IPL/Patents -, 44 avenue de la République -, CS 50010, 92326 Châtillon 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, 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, 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:** MANAGEMENT OF THE APPLICATION OF A POLICY IN AN SDN ENVIRONMENT OF A COMMUNICATION NETWORK

(54) **Titre :** GESTION DE LA MISE EN APPLICATION D'UNE POLITIQUE DANS UN ENVIRONNEMENT SDN DE RÉSEAU DE COMMUNICATION

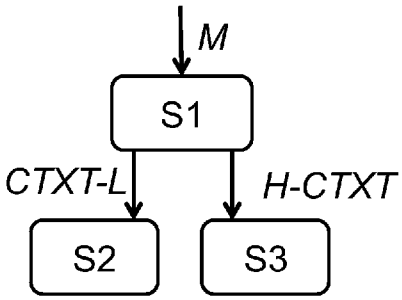

Fig. 4a

(57) **Abstract:** Management of the application of a policy in an SDN environment of a communication network. The present technique relates to a method for managing a policy for applying rules in a virtualized communication network comprising virtualized functions, called service functions (SF), the method comprising the following steps implemented by an SDN controller of said network: · generation (S1), on the basis of a set of rules describing said policy, referred to as model (M), of an encapsulation header comprising a context relating to said model (M) and of at least one local application policy context associated with at least one of said service functions (SFi); · transmission (S2) of said at least one local context to said at least one service function (SFi); · transmission (S3) of said encapsulation header to at least one packet router, called classifier (SCL).

(57) **Abrégé :** Gestion de la mise en application d'une politique dans un environnement SDN de réseau de communication. La présente technique concerne un procédé de gestion d'une politique d'application de règles dans un réseau de communication virtualisé comprenant des fonctions virtualisées, dites fonctions service (SF), le procédé comprenant les étapes suivantes mises en œuvre par un contrôleur SDN dudit réseau : · génération (S1), à partir d'un ensemble de règles décrivant ladite politique, dit modèle (M), d'un entête d'encapsulation comprenant un contexte relatif audit modèle (M) et d'au moins un contexte local de politique d'application associé à au moins une desdites fonctions service (SFi); · transmission (S2) dudit au moins un contexte local à ladite au moins une fonction service (SFi); · transmission (S3) dudit entête d'encapsulation à au moins un routeur de paquets, dit classificateur (SCL).

WO 2020/008126 A1

Gestion de la mise en application d'une politique dans un environnement SDN de réseau de communication.

1. Domaine de l'invention

Le domaine de l'invention est celui de la virtualisation des fonctions dans un réseau de télécommunication. Plus précisément, l'invention concerne la gestion de politique d'application via de fonctions logicielles virtualisées dans une architecture SDN (en anglais « Software-Defined Networking »).

2. Art antérieur et ses inconvénients

On rappelle que l'architecture SDN propose de découpler les fonctions de contrôle du réseau des fonctions d'acheminement des données à proprement parler, de sorte à permettre le contrôle du réseau par des fonctions logicielles programmables et à isoler l'infrastructure sous-jacente du réseau des applications et services réseau. Selon la recommandation Y.3300 (« Framework of software-defined networking ») de l'organisme de normalisation ITU-T (en anglais « International Telecommunication Union – Telecommunication »), l'architecture SDN est définie comme un ensemble de techniques permettant de programmer, d'orchestrer, de contrôler et de gérer directement les ressources du réseau, ce qui facilite la conception, la fourniture et l'exploitation de services réseau.

La couche de contrôle SDN, ou contrôleur SDN (en anglais « SDN control layer »), permet de contrôler dynamiquement le comportement des ressources/éléments du réseau selon les instructions d'une application SDN. Les applications SDN spécifient comment les ressources réseau doivent être contrôlées et allouées, en interagissant avec la couche de contrôle SDN via les interfaces de contrôle d'application NBI (en anglais « North Bound Interface » NBI).

Les informations de commande de la couche de contrôle SDN vers les ressources/éléments de réseau sont ensuite délivrées via des interfaces de contrôle de ressources SBI (en anglais « South Bound Interface).

Cette architecture SDN permet ainsi la mise en œuvre d'une plateforme logicielle (dite « plateforme SDN ») programmable et flexible offrant une vue globale et logique du réseau et une gestion dynamique des ressources hétérogènes du réseau.

Plus précisément, et en référence à la **figure 1**, l'architecture SDN est structurée en trois couches principales, séparées entre elles par les interfaces SBI et NBI, à savoir :

- une couche de ressources réseau constituée par des éléments de réseau NE (en anglais « Network Elements ») physiques ou virtuels, par exemple des routeurs, commutateurs, réseaux de diffusion de contenus (en anglais « Content Delivery Network », CDN) ;
- un contrôleur SDN-CTRL comportant des fonctions d'abstraction et de programmation

des éléments de réseau NE de la couche de ressources réseau et offrant des gestionnaires de service de base comme la gestion des nœuds et des liens associés ;

- une couche de services applicatifs réseau NAP (en anglais « Network Applications ») comportant un ensemble d'applications de gestion (par exemple de gestion de réseaux privés virtuels VPN), de supervision, de connectivité vers une plateforme d'un réseau en nuage.

Dans une telle architecture SDN, une fonction service SF désigne une fonction embarquée dans un environnement, qui peut être co-localisée avec d'autres fonctions service au sein du même équipement, comme par exemple un routeur, un serveur, un commutateur, etc. Une fonction service SF correspond par exemple à une fonction de traduction d'adresse réseau (en anglais NAT « Network Address Translation »), une fonction de pare-feu, une fonction d'optimisation du protocole de contrôle de transmission TCP (en anglais « Transmission Control Protocol Optimizer »), une fonction de détection et d'élimination de malware, une fonction de control parental, une fonction d'optimisation du cache, une fonction d'inspection de paquet de type DPI (en anglais « Deep Packet Inspection »), une fonction de répartition de charge ...

Par ailleurs, le chainage de fonctions service SFC (en anglais « Service Function Chaining ») tel que décrit dans le document IETF RFC 7665 (en anglais « Internet Engineering Task Force Request For Comments 7665 »), permet de simplifier le déploiement des fonctions service SF (en anglais « Service Function »). Un domaine de fonctions service permet de mettre en œuvre ce chainage en fournissant une pluralité de fonctions service SF pouvant être liées les unes aux autres pour fournir un service. Ce domaine est attaché à des classificateurs de service (en anglais « Service Function Classifier ») qui classent les flux de trafic et décident quel(s) paquets entre(nt) dans une chaîne du domaine, grâce à des règles fournis par le contrôleur SDN.

Un exemple d'un tel domaine SFC, illustré **en figure 2**, comprend notamment les composants suivants :

- un classificateur SCL permettant, tel que décrit ci-dessus, de déterminer quel(s) paquet(s) doit entrer dans une chaine de fonctions service, à partir d'une table de politique ;
- un transmetteur de fonctions service SFF (en anglais « Service Function Forwarder ») redirigeant les paquets vers la fonction de service SF adéquate, sur la base d'information d'encapsulation SFC ;
- un proxy de fonctions service SFP gérant les informations d'encapsulation SFC pour les fonctions service SF non compatibles *SFC-una* (dites « unaware » en anglais) ;
- une pluralité de fonctions service SF responsables du traitement spécifique des paquets.

Ces différents composants gèrent par exemple un graphe défini par un utilisateur, via une

application, ce graphe décrivant un chainage de fonctions service SFC, dans lequel chaque nœud du graphe est une fonction service SF.

En particulier, le chainage de fonctions service SFC permet donc de définir une liste ordonnée de fonctions service réseau créant ainsi une chaine, ou un enchainement, de fonctions service, à travers laquelle un paquet doit passer.

Pour ce faire, le chainage de fonctions service SFC s'appuie sur l'entête d'encapsulation SFC (en anglais « SFC encapsulation »), qui fournit des informations sur le chainage de fonctions de service à travers lequel un paquet du flux de trafic doit passer. L'entête NSH (en anglais « Network Service Header »), tel que décrit dans le document IETF RFC 8300, est un exemple d'encapsulation SFC qui permet de définir un plan de service complet portant des informations de fonctions de service.

Cet entête NSH est ajouté, par un classificateur, aux paquets d'un flux de trafic et indique à travers quelles fonctions service SF (pare-feu, DPI, répartition ou équilibrage de charge ...) ils doivent passer. Un entête NSH est composé notamment des éléments suivants, illustrés en figure 3 :

- Base Header (B.H.) : comprend des informations sur l'entête de service et le protocole de charge utile ;
- Service Path Header (S.P.H.) : reflète la sélection d'un chemin identifié par un identifiant SPI (en anglais « Service Path Identifier »). La localisation du paquet dans le chemin est donnée par l'index de service SI (en anglais Service Index). L'identifiant SPI et l'index de service SI indiquent au paquet le chemin à suivre, sans nécessiter la configuration de métadonnées ou d'informations de paquet.
- Context Header (C.H.) : porte des métadonnées relatives à un chemin pouvant être partagées par les fonctions service SF.

L'encapsulation NSH permet notamment un chainage de service indépendant de la topologie du réseau, en fournissant les informations d'identification de chemin nécessaires pour réaliser un chemin de fonctions service.

De plus, l'encapsulation NSH fournit un mécanisme de transport de métadonnées partagées entre les entités du réseau (classificateurs, transmetteurs de fonctions service ...) et les fonctions service SF. Ainsi, le partage de métadonnées permet aux fonctions service SF de partager des résultats de classification initiaux et intermédiaires avec des fonctions service SF plus loin dans un chemin.

La sémantique des métadonnées est communiquée via une couche de contrôle aux nœuds participants d'un chemin.

Enfin, l'encapsulation NSH est indépendante de l'encapsulation de transport dans le

réseau et l'entête NSH constitue donc un entête commun et standard pour le chainage de fonctions service dans tout le réseau. L'encapsulation NSH permet donc la définition de chaines de fonctions service flexibles dans un plan de services dirigé par application.

Par ailleurs, il est connu de définir des politiques applicables à des éléments ou groupes d'éléments ou d'équipements physiques d'un réseau, par exemple via un composant du contrôleur SDN, appelé module de politique de groupe GBP (en anglais « Group-Based Policy »).

Chaque équipement du réseau (par exemple, une machine hôte, un port de machine, une machine virtuelle, etc.) est vu comme un point de terminaison (en anglais « endpoint »), plusieurs points de terminaison pouvant être groupés selon des règles de politique communes et formant donc des groupes de points de terminaison (en anglais « End Point Group »). Des contrats définissent comment les points de terminaison et/ou les groupes de points de terminaison peuvent communiquer.

Dans l'état actuel de la technique de virtualisation de fonctions d'un réseau SDN, la mise en application d'une politique est centralisée, et nécessite qu'une fonction service SF transmette le paquet à un contrôleur qui lui retourne les actions de la politique à mettre en œuvre, entraînant un grand nombre d'échanges entre le contrôleur et les fonctions service SF. De plus, lorsqu'une politique doit être mise en application, la configuration de chaque fonction service SF doit être modifiée, pour tous les nœuds du réseau concernés par la politique, ou alors cela nécessite l'instanciation d'une nouvelle chaine de fonctions service.

Les techniques actuelles ne permettent donc pas la gestion d'une politique d'application granulaire et dynamique, permettant de viser tous les points de terminaison d'un réseau, sans allouer de nouvelles ressources (en terme de calcul et de stockage).

La présente technique propose un mécanisme de gestion d'une politique d'application dans un réseau qui ne présente pas ces inconvénients.

3. Exposé de l'invention

La présente invention concerne un procédé de gestion d'une politique d'application de règles dans un réseau de communication virtualisé comprenant des fonctions virtualisées, dites fonctions service SF, comprenant les étapes suivantes mises en œuvre par un contrôleur SDN du réseau :

- génération S1, à partir d'un ensemble de règles décrivant la politique, dit modèle M, d'un entête d'encapsulation comprenant un contexte relatif au modèle M et d'au moins un contexte local de politique d'application associé à au moins une des fonctions service SF*i* ;
- transmission S2 du contexte local à la fonction service SF*i* ;

- transmission S3 de l'entête d'encapsulation à au moins un routeur de paquets, dit classificateur SCL.

Selon un aspect particulier, l'étape de génération comprend les sous-étapes suivantes :

- obtention, à partir du modèle M d'au moins un ensemble de règles de traitement de paquets par au moins une des fonctions service SF*i*, dit chaine de politique d'application EC1 ;
- obtention, à partir de la chaine de politique d'application EC1, d'un entête de contexte et du contexte local de politique d'application pour au moins une des fonctions service SF*i* ;
- génération de l'entête d'encapsulation à partir de l'entête de contexte.

Par exemple, la chaine de politique d'application EC1 décrit au moins un enchainement SFC1 d'au moins une des fonctions service SF*i* en fonction d'au moins une information représentative d'un ensemble prédéfini de règles de communication, dit contrat, entre un premier et un deuxième groupe d'équipements du réseau de communication EPG1, EPG2, le premier groupe EPG1 comprenant au moins un équipement émetteur d'au moins un paquet et le deuxième groupe EPG2 comprenant au moins un équipement destinataire d'au moins un paquet, et/ou d'une information représentative d'au moins un équipement EP10 dans le premier groupe EPG1 et/ou d'au moins une caractéristique de paquet.

Selon une caractéristique particulière, le contexte local comprend au moins une définition d'au moins une action à effectuer par la fonction service SF*i*.

Selon un mode de réalisation particulier, la transmission de l'entête d'encapsulation à au moins un classificateur SCL comprend une étape de configuration du classificateur de service SCL de sorte à ce que le classificateur de service SCL délivre, pour au moins un paquet entrant, au moins un paquet enrichi avec l'entête d'encapsulation.

Selon un autre aspect, la présente invention concerne un procédé de traitement d'une politique d'application de règles dans un réseau de communication comprenant des fonctions virtualisées, dite fonctions service SF, comprenant, dans au moins une des fonctions service SF*i*, une étape préalable de réception S4, en provenance d'un contrôleur SDN du réseau, d'un contexte local de politique d'application associé à la fonction service (SF*i*), et les étapes suivantes :

- réception S5 d'au moins un paquet enrichi avec un entête d'encapsulation par un routeur de paquets, dit classificateur SCL, du réseau;
- traitement S6 du paquet enrichi, en tenant compte du contexte local de politique d'application associé à la fonction service SF*i*.

Selon une caractéristique particulière, le traitement comprend une étape d'exécution

d'au moins une action définie dans le contexte local de politique d'application, en tenant compte d'au moins une caractéristique du paquet enrichi et délivrant un résultat comprenant au moins une information d'identification d'au moins une fonction de service destinatrice *SFj* du paquet enrichi traité.

Selon un mode de réalisation particulier, le traitement comprend également une étape de mise à jour de l'entête d'encapsulation en fonction du résultat de l'étape d'exécution.

Selon un autre aspect, l'invention concerne un module contrôleur SDN, comprenant :

- des moyens de génération, à partir d'un ensemble de règles, dit modèle M, décrivant une politique d'application de règles dans un réseau de communication virtualisé comprenant des fonctions virtualisées, dites fonctions service SF, d'un entête d'encapsulation comprenant un contexte relatif au modèle M et d'au moins un contexte local de politique d'application associé à au moins une des fonctions service SF*i* ;
- des moyens de transmission du contexte local à la fonction service SFi ;
- des moyens de transmission de l'entête d'encapsulation à au moins un routeur de paquets, dit classificateur SCL.

Le module contrôleur SDN est notamment apte à mettre en œuvre les étapes du procédé de gestion d'une politique d'application de règles tel que décrit précédemment et ci-après, selon ses différents modes de réalisation.

La présente invention concerne également un module fonction virtualisée, dit module fonction service, dans un réseau de communication virtualisé, comprenant un module de logique de politique d'application (PEL) comprenant :

- des moyens de réception, en provenance d'un contrôleur SDN du réseau, d'un contexte local de politique d'application associé au module fonction service ;
- des moyens de réception d'au moins un paquet enrichi avec un entête d'encapsulation par un routeur de paquets, dit classificateur SCL du réseau;
- des moyens de traitement du paquet enrichi, en tenant compte du contexte local de politique d'application.

Le module de logique de politique d'application (PEL) est notamment apte à mettre en œuvre les étapes du procédé de traitement d'une politique d'application de règles tel que décrit précédemment et ci-après, selon ses différents modes de réalisation.

Selon encore un autre aspect, l'invention concerne un système comprenant un module contrôleur SDN et un module fonction service, tels que décrits précédemment et ci-après, selon ses différents modes de réalisation, ainsi qu'un routeur de paquets, dit classificateur SCL recevant

un entête d'encapsulation du contrôleur SDN et délivrant, pour au moins un paquet entrant, au moins un paquet enrichi avec l'entête d'encapsulation.

Un autre aspect concerne un ou plusieurs programmes d'ordinateur comportant des instructions pour la mise en œuvre d'un procédé de gestion et/ou d'un procédé de traitement d'une politique d'application de règles, tels que décrits ci-dessus et ci-après, lorsque ce ou ces programmes sont exécutés par au moins un processeur.

Selon encore un autre aspect, il est proposé un ou plusieurs supports d'enregistrement non transitoire lisibles par un ordinateur, et comportant des instructions d'un ou plusieurs programmes d'ordinateur comprenant des instructions pour la mise en œuvre d'un procédé de gestion et/ou d'un procédé de traitement d'une politique d'application de règles, tels que décrits ci-dessus et ci-après, lorsque ce ou ces programmes sont exécutés par au moins un processeur.

4. Liste des figures

D'autres buts, caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante, donnée à titre de simple exemple illustratif, et non limitatif, en relation avec les figures, parmi lesquelles :

- La **figure 1** déjà décrite représente l'architecture SDN de l'état actuel de la technique ;
- la **figure 2** déjà décrite représente un exemple de domaine SFC de l'état actuel de la technique ;
- la **figure 3** déjà décrite représente un exemple de contenu d'un entête NSH de l'état actuel de la technique ;
- **la figure 4a** illustre les principales étapes du procédé de gestion d'une politique d'application de règles selon un mode de réalisation de l'invention ;
- **la figure 4b** illustre les principales étapes du procédé de traitement d'une politique d'application de règles selon un mode de réalisation de l'invention ;
- **la figure** 5 illustre un exemple d'intégration, dans une architecture SDN, du procédé et des modules de gestion d'une politique d'application selon un mode de réalisation de l'invention ;
- **la figure** 6 illustre un exemple de chaine d'une politique d'application selon un mode de réalisation de l'invention ;
- **la figure** 7 illustre un exemple de module/plugin de logique de politique d'application (PEL) d'une fonction service SF selon un mode de réalisation de l'invention ;
- **les figures 8 et 9** illustrent respectivement, pour un exemple de mise en œuvre de l'invention, les entités d'un réseau et une chaine de politique d'application, selon un mode de réalisation de l'invention.

5. Description détaillée de modes de réalisation de l'invention

Le principe général de la technique proposée repose sur une coopération entre le plan de transfert et le plan de contrôle, dans un réseau de communication virtualisé comprenant des fonctions virtualisées, ou fonctions de service.

Cette coopération est notamment mise en œuvre d'une part via la prise en compte, pour le transfert des paquets, d'un contexte relatif à un ensemble de règles décrivant une politique, et d'autre part via la prise en compte d'un contexte local à chaque fonction service.

Ainsi, la technique proposée permet de gérer un chainage de fonctions service pour appliquer les règles de la politique, de manière dynamique et distribuée, par rapport aux techniques de l'art antérieur.

De plus, la technique proposée est basée sur une modélisation d'une politique d'application de règles dans un réseau, afin de gérer de manière contextualisée cette politique au niveau des fonctions réseau requises.

Pour ce faire, la technique proposée repose par exemple sur une architecture SDN existante et les fonctionnalités de chainage de fonctions service connues.

Ainsi, selon la technique proposée, un modèle, défini par un utilisateur comme un ensemble de règles décrivant une politique d'application de règles, est interprété par le contrôleur SDN qui le traduit en configurations techniques, via la création notamment d'une chaine de fonctions service, correspondant à un ensemble de règles de traitement de paquets par une fonction service et des actions à mettre en œuvre par les fonctions service de la chaine.

Cette chaine de fonctions service, dite chaine de politique d'application, peut être créée sous la forme d'un graphe de politique d'application, lequel est traité par exemple par un module de politique d'application, dans le contrôleur SDN, de façon à délivrer une pluralité de contextes locaux destinés au fonctionnement de chacune des fonctions service de la chaine prédéfinie.

De cette manière, la gestion d'une nouvelle politique d'application de règles ne nécessite pas d'instancier de nouvelles ressources car le contexte local associé à chaque fonction service permet de gérer de manière granulaire la politique globale.

En effet, grâce à ce contexte local, chaque fonction service dispose d'une « intelligence » propre lui permettant d'être capable de mettre en œuvre les actions adéquates définies par le modèle.

La technique proposée permet donc un chainage de politique d'application de règles distribué au niveau de chaque fonction service, via un module de politique d'application qui gère le contexte local reçu et les actions de politique d'application. Ce module de politique d'application permet la sélection, via le modèle préalablement interprété par le contrôleur SDN, de l'action adéquate, basée sur la chaine de politique d'application préalablement définie. Ce

module de politique d'application d'une fonction service permet de plus d'indiquer à la fonction service suivante quelle sera l'action suivante de politique d'application à mettre en œuvre.

La technique proposée peut aisément être mise en œuvre dans un environnement de type orienté-modèle tel que OpenDaylight, ou ONOS. En effet, ces techniques proposent un contrôleur SDN capable de communiquer à des équipements physiques et virtuels via différents interfaces et protocoles (Netconf, OpenFlow, OVSDB...), intégrant notamment les modules de chainage de fonctions service SFC avec le protocole NSH de paquets, ainsi qu'un module de politique de groupe GBP, déjà décrit ci-dessus.

Plus précisément, la technique proposée se base sur le protocole NSH, et plus particulièrement l'entête de contexte NSH, prévu dans la norme mais non défini, qui permet de transporter des métadonnées propres au service délivré. La technique proposée permet de structurer ces métadonnées à partir d'un modèle qui exprime les cas d'usages client de politique d'application, de manière simple et agnostique (indépendante du réseau, des éléments virtuels ou physiques mis en œuvre, du protocole de transport, ...).

La technique proposée permet donc de gérer une chaine de politique d'application au niveau d'une fonction service, en partant d'un modèle qui permet de faire abstraction de la complexité de configuration du réseau et des différentes fonctions service à mettre en œuvre, et qui permet de se focaliser sur l'expression du besoin fonctionnel, d'un point de vue applicatif (par exemple, interdire aux abonnés d'un réseau mobile l'accès à certains sites internet).

On décrit d'abord, en relation avec la figure 4a, les principales étapes du procédé de gestion de politique d'application de règles dans un réseau de communication comprenant des fonctions virtualisées, dite fonctions service SF, mises en œuvre dans un dispositif correspondant à un contrôleur SDN du réseau, selon un premier mode de réalisation de la technique proposée.

Comme déjà indiqué ci-dessus, la technique proposée tire parti d'une description par un modèle M d'une politique d'application de règle de réseau, lequel modèle correspond donc à un ensemble de règles décrivant cette politique.

Lors d'une étape S1, le contrôleur SDN génère un entête d'encapsulation comprenant un contexte relatif au modèle, ainsi qu'au moins un contexte local associé à au moins une fonction service du réseau.

Lors des étapes S2 et S3, le contrôleur SDN transmet respectivement le contexte local à la fonction service auquel il est associé, afin d'assurer le traitement des paquets, et l'entête d'encapsulation à au moins un routeur de paquets, ou classificateur SCL, afin d'assurer le transfert des paquets.

Plus précisément, l'étape de génération S1 comprend une sous étape d'obtention d'au moins une chaine de politique d'application EC1, correspondant à un ensemble de règles de traitement de paquets par au moins une fonction service, à partir du modèle M décrit ci-dessus.

Une telle chaine de politique d'application EC1 décrit au moins un enchainement SFC1 d'au moins une des fonctions service SF du domaine donné, en fonction d'au moins une information représentative :

- d'un contrat de politique prédéfini entre un premier et un deuxième groupe d'équipements ou de points de terminaison, EPG1, EPG2, du réseau de communication , un tel contrat correspondant à un ensemble prédéfini de règles de communication entre les deux groupes ;
- d'au moins un point de terminaison EP10 dans le premier groupe EPG1 ;
- d'au moins une caractéristique de paquet, comme par exemple une indication du fait que le paquet est un paquet Internet.

En effet, lorsque l'utilisateur, via son application, a défini les règles de politique dans les contrats entre des groupes de points de terminaison, il peut définir le chainage des fonctions service à mettre en œuvre pour la politique d'application, via une ou plusieurs chaines de politique d'application EC*i*.

Ainsi, chaque chaine de politique d'application EC*i* est liée à un contrat donné entre deux groupes de points de terminaison et concerne uniquement les points de terminaison qui respectent les exigences/clauses particulières.

L'étape de génération S1 comprend également une sous-étape d'obtention, à partir de la chaine de politique d'application (EC1), d'un entête de contexte et d'un contexte local de politique d'application pour au moins une fonction service.

Ensuite, une sous-étape de génération d'un entête d'encapsulation est mise en œuvre, à partir de l'entête de contexte, de manière à ce que les paquets encapsulés portent cet entête de contexte.

Ainsi, chaque paquet à transférer dans le réseau est modifié, par un des classificateurs SCL du réseau, par encapsulation, et chaque fonction service a reçu un contexte local lui permettant de mettre en œuvre les actions adéquates requises par le modèle décrivant la politique d'application de règles.

Lorsque plusieurs fonctions service sont présentes dans un réseau, ce qui est le cas en général (par exemple une fonction service d'inspection de paquet, une fonction service de pare-feu, ...), plusieurs contextes locaux sont obtenus et associés à chacune de ces fonctions service.

On décrit maintenant, en relation avec la figure 4b, les principales étapes du procédé de traitement d'une politique d'application de règles dans un réseau de communication comprenant

des fonctions virtualisées, dite fonctions service SF, mises en œuvre dans au moins une fonction service SF*i* du réseau, selon un premier mode de réalisation de la technique proposée.

Lors d'une étape préalable de réception S4, la fonction service donnée SF*i* reçoit, en provenance du contrôleur SDN du réseau, un contexte local de politique d'application qui lui est associé (I.e. l'un des contexte locaux obtenus lors de l'étape S1 décrite ci-dessus).

Ce contexte local est utilisé par la fonction service pour traiter chaque paquet qu'elle reçoit.

Ainsi, lors d'une étape réception S5, la fonction service reçoit au moins un paquet enrichi avec un entête d'encapsulation par un routeur de paquets, ou classificateur SCL du réseau, et le traite, lors d'une étape de traitement S6, en tenant compte du contexte local de politique d'application associé.

Selon ce mode de réalisation, le traitement appliqué au paquet enrichi par la fonction service correspond par exemple à une étape d'exécution d'au moins une action définie dans le contexte local de politique d'application, en tenant compte d'au moins une caractéristique du paquet enrichi reçu. Par exemple, le type de paquet permet de sélectionner l'action à exécuter, tout comme l'équipement émetteur du paquet, ou encore la chaine de fonctions service qui lui est associée.

L'exécution d'une action délivre notamment un résultat comprenant au moins une information d'identification d'au moins une fonction de service destinatrice *SFj* du paquet enrichi traité, à parti d'informations de l'entête d'encapsulation, du contexte local et de caractéristiques du paquet.

De plus, le traitement du paquet comprend également une étape de mise à jour de l'entête d'encapsulation en fonction du résultat de l'exécution de l'action, notamment pour modifier, le cas échéant, le chemin définissant les fonctions service ultérieures à mettre en œuvre.

Comme décrit ci-après en relation avec la figure 5, la technique proposée met en œuvre un module de chainage de politique d'application ECM au niveau du contrôleur SDN, ainsi qu'un module de logique de politique d'application PEL au niveau de chaque fonction service.

Le module de chainage de politique d'application ECM est notamment en charge d'obtenir l'entête de contexte et de le contexte local et de les transmettre respectivement à au moins un classificateur en vue d'une encapsulation des paquets et au module de logique de politique d'application PEL de chaque fonction service SF concernée.

Selon une mise en œuvre particulière de la technique proposée, cet entête de contexte correspond précisément au « Context Header » de l'entête NSH. La prise en compte de cet entête par un classificateur correspond donc à une encapsulation NSH du paquet, de sorte à ce que les

métadonnées transportées dans le « Context Header » NSH puissent être interprétées par les transmetteurs de fonctions service SFF en vue de la transmission du paquet vers la fonction service adéquate.

Ces principales étapes permettent donc, à partir d'un modèle d'une politique d'applications de règle dans un réseau, la mise en application granulaire et distribuée de cette politique, au niveau de chaque fonction service du domaine, grâce à des chaines de politique d'application dynamiques et à la gestion d'un contexte local pour chaque fonction service.

Les étapes plus détaillées et les interactions entre les différents éléments sont décrites ci-après, en relation avec la figure 5.

Comme déjà indiqué ci-dessus, la mise en œuvre de la technique proposée se situe au niveau du contrôleur SDN, grâce à un module de chainage de politique d'application ECM, ainsi qu'au niveau de chaque fonction service SF, grâce à un module de logique de politique d'application PEL.

La première étape 1, une fois le modèle défini par l'utilisateur, consiste donc à recevoir, dans le contrôleur SDN, une « intention » pour un chainage de fonctions service. En effet, le principe du modèle est de définir des intentions, sans tenir compte des contraintes/caractéristiques techniques du réseau, permettant ainsi une grande facilité d'utilisation et de définition.

Ce modèle est reçu par le contrôleur SDN via les interfaces de contrôle d'application NBI, puis interprété pour définir un chainage de fonctions service et des actions associées. Cette interprétation est mise en œuvre par un module SFC-M (en anglais « Service Function Chaining Module »), qui n'a pas connaissance des équipements (ou points de terminaisons) du réseau, mais qui sait duquel partir et auquel arriver. La connaissance des équipements est maitrisée par le module de gestion de la politique groupée GBP-M.

L'interprétation du modèle délivre donc une ou plusieurs chaines de politique d'application EC*i* décrivant au moins un enchainement SFC1 d'au moins une des fonctions service SF du domaine donné.

Par exemple, ces chaines EC*i* sont délivrées sous forme de graphe de mise en application, tel que décrit ci-après en relation avec la figure 6.

Ensuite, lors d'une étape 2, le module de chainage de politique d'application ECM stocke le graphe de mise en application d'une politique, en stockant d'une part le contexte général de chainage et en distribuant d'autre part des contextes de chainage locaux à chaque module de logique de politique d'application PEL des fonctions service du domaine.

Pour ce faire, le module de chainage de politique d'application ECM crée les clauses relatives aux actions des fonctions service (chaque clause correspond à une action d'une fonction

service) et génère le contexte NSH correspondant au chainage de politique d'application choisi. Des exemples de clauses et actions seront décrits ci-après, en relation avec la figure 6 également.

Lors d'une étape 3, le module/plugin de chainage de politique d'application ECM envoie le contexte NSH au module GBP-M pour que ce dernier l'ajoute à l'entête NSH qui est envoyé, lors d'une étape 5 aux classificateurs du domaine. Ces derniers sont en effet en charge de déterminer quel paquet du flux doit entrer dans une chaine donnée de fonctions service, à partir d'une table de politique, et ainsi encapsuler chaque paquet avec l'entête NSH correct.

Par ailleurs, lors d'une étape 4, le module de chainage de politique d'application ECM envoie le contexte local de politique d'application à chaque module de logique de politique d'application PEL des fonctions service du domaine.

Ainsi, pour un ensemble de règles d'une politique donnée entre deux points de terminaison et un chainage utilisé, la présente technique permet de définir des chaines de politique d'application pouvant s'appliquer à chaque fonction service, lesquelles ont un ensemble d'actions possibles à effectuer et ont la connaissance d'une logique de chainage de politique d'application à un niveau local.

On décrit maintenant plus en détails, en relation avec la figure 6, un exemple de chaine de politique d'application.

Comme illustré sur la **figure 6**, chaque nœud d'une chaine de politique d'application *ECi* fait référence à une chaine de fonctions service SF (SFC*i*) donnée et à une fonction service SF*i* donnée. De plus, chaque nœud correspond à des actions de politique d'application à mettre en œuvre au niveau de la fonction service SF*i* donnée (pas de traitement spécifique, refus du paquet, exécution d'une fonction propre à la fonction service comme par exemple inspection du paquet si la fonction service est un inspecteur de paquet ou ajout de règles de pare-feu si la fonction service est un pare-feu).

Comme déjà indiqué, une chaine de politique d'application EC*i* est relative à un contrat donné entre deux groupes de points de terminaison, et s'applique uniquement aux paquets qui sont concernés, i.e. les paquets qui respectent certaines conditions notamment définies dans les informations de contexte, décrites ci-après.

Dans l'exemple illustré en figure 6, on considère un contrat *contract1* défini entre les deux groupes de points de terminaison EPG1 et EPG2, le groupe EPG1 comprenant par exemple deux points de terminaison EP10 et EP11.

Le domaine comprend quatre fonctions service SF1, SF2, SFa et SFb, et le contrat définit par exemple les deux chaines de fonctions service suivantes :

- SFC1 : SF1 -> SF2 (enchainement des fonctions service SF1 et SF2) ;
- SFC2 : SF1 -> SFa -> SFb (enchainement des fonctions service SF1, SFa et SFb).

Enfin, une chaine de politique d'application EC1 a été générée pour le contrat *contract1*, définissant les clauses et actions décrites ci-après, grâce à l'entête NSH et aux contextes locaux associés aux différentes fonctions service.

Par exemple, les informations de contexte portées par l'entête NSH sont les suivantes : une application A, un tenant B (titulaire pour les ressources), les points de terminaison EP10 et EP11, le groupe de points de terminaison EPG1, les chaines SFC1 et SFC2, ainsi que des informations relatives au service, comme par exemple une caractéristique indiquant qu'il s'agit d'un trafic Internet.

La chaine de politique d'application EC1 décrit donc les différents enchainements de fonctions service, en fonction du point de terminaison concerné, d'au moins une caractéristique du paquet, et de son contenu, ainsi que les différentes actions de chaque fonction service, en fonction du résultat de l'action de la fonction service précédente.

Ainsi, pour chaque fonction service, un contexte local décrit les différentes clauses de définition des actions de la fonction service. Ces différentes clauses sont notamment stockées au niveau de la fonction service et leur interprétation et mise en œuvre sont effectuées par le module de logique de mise en application PEL de la fonction service concernée, comme illustré en figure 7 décrite ci-après.

Par exemple, pour la fonction service SF1, le contexte local définit les deux clauses suivantes :

- clause 1 : {SFC1, Internet traffic, EP10} ; cette première clause indique qu'un paquet de type « Internet », en provenance du point de terminaison EP10, doit être routé dans la chaine de fonction service SFC1 ;
- clause 2 : {SFC1, Internet traffic, EP11} ; cette deuxième clause indique qu'un paquet de type « Internet », en provenance du point de terminaison EP11, doit être routé dans la chaine de fonction service SFC1.

Par ailleurs, une action de politique d'application EA contient l'action proprement dite à effectuer par la fonction service SF pour traiter le paquet. Chaque action EA peut générer une sortie, et l'action EA suivante peut être mise en œuvre sur la base de la sortie de l'action EA précédente. Cette logique est notamment définie par l'utilisateur au niveau du modèle, et est stockée dans le module de logique de politique d'application PEL.

Pour la fonction service SF1, les actions définies dans les clauses sont par exemple les suivantes :

- clause 1 : action EA1 : *« Action Inspect 1 »* : requiert l'inspection du paquet, lorsqu'il provient du point de terminaison EP10, qu'il correspond à du trafic Internet et qu'il doit être routé dans la chaine de fonctions service SF1. Cette

action peut donner deux résultats « a » ou « c », comprenant notamment respectivement les sorties « v » et « w », associées à une information représentative de la fonction service suivante qui traitera le paquet en question, dans la chaine SF1 ; les résultats « v » et « w » peuvent par exemple correspondre respectivement au cas où l'inspection du paquet n'a rien révélé d'anormal et au cas où l'inspection du paquet a détecté une anomalie ;

- clause 2 : action EA2 : « *Action Inspect 2* » : requiert l'inspection du paquet, lorsqu'il provient du point de terminaison EP11, qu'il correspond à du trafic Internet et qu'il doit être routé dans la chaine de fonctions service SF1. Le résultat de cette action est noté « b » et comprend notamment la sortie « t », associée à une information représentative de la fonction service suivante qui traitera le paquet en question, dans la chaine SF1.

Pour la fonction service SF2, le contexte local définit par exemple les trois clauses suivantes :

- clause 1 : {SFC1, EP10, v} ; cette première clause indique qu'un paquet en provenance du point de terminaison EP10 et dont la sortie du traitement par une fonction service précédente est égale à « v » doit être routé dans la chaine de fonction service SFC1 ;
- clause 2 : {SFC1, EP11, t} ; cette deuxième clause indique qu'un paquet en provenance du point de terminaison EP11 et dont la sortie du traitement par une fonction service précédente est égale à « t » doit être routé dans la chaine de fonction service SFC1 ;
- clause 3 : {SFC1, x} ; cette troisième clause indique qu'un paquet dont la sortie du traitement par une fonction service précédente est égale à « x » doit être routé dans la chaine de fonction service SFC1.

Les actions définies dans ces clauses sont les suivantes :

- clause 1 : action EA1 : « *Action Deny* » : refus du paquet (celui-ci n'est pas traité et ne sera pas transmis au groupe EPG2), lorsqu'il provient du point de terminaison EP10, qu'il doit être routé dans la chaine de fonctions service SF1 et que la sortie de l'action précédente était « v » ;
- clause 2 : action EA2 : « *Action Allow* » : autorisation du paquet (celui-ci ne subit pas de traitement propre à une clause définie et est directement transmis à la prochaine fonction service), lorsqu'il provient du point de terminaison EP11, qu'il

doit être routé dans la chaine de fonctions service SF1 et que la sortie de l'action précédente était « t » ;

- clause 3 : action EA3 : « *Specific Action* » : ce type d'action correspond à une action propre à la fonction service, comme par exemple l'ajout de règles de pare-feu si la fonction service est un pare-feu, à mettre en œuvre dans cet exemple lorsque la sortie de la précédente action était « x ».

Pour la fonction service SFa, le contexte local définit la clause suivante :

- clause 1 : {SFC2, EP10, w} ; cette clause indique qu'un paquet en provenance du point de terminaison EP10 et dont la sortie du traitement par une fonction service précédente est égale à « w » doit être routé dans la chaine de fonction service SFC2 ;

et l'action suivante :

- action EA1 : « *Action DoS* » : une attaque par déni de service est détectée, et le paquet est rejeté (« *Drop* »), lorsqu'il provient du point de terminaison EP10, qu'il doit être routé dans la chaine de fonctions service SF2 et que la sortie de l'action précédente était « w ». Le résultat de cette action est « f » et comprend notamment la sortie « z ». Si les conditions d'applications de la clause ne sont pas remplies, alors le paquet ne relève pas d'une attaque par déni de service et le paquet est transmis à la fonction service SFb.

La description des actions EA reflète donc les fonctionnalités des fonctions service et peuvent être déclinées sur la base des différents types existants de fonctions service.

La figure 7 illustre un exemple de dispositif correspondant à un module de logique de politique d'application PEL, pour la fonction service SF1 intervenant dans la chaine de politique d'application EC1 décrite ci-dessus en relation avec la figure 6.

Le contexte de chainage local stocké dans cette fonction service SF1 est relatif à toutes les informations nécessaires au module de logique de politique d'application PEL pour :

- gérer la sortie de l'action EA précédente (par exemple a, b ...g) ;
- envoyer la bonne action à effectuer à la fonction service proprement dite, en se basant sur la logique de chainage définie ;
- recevoir le résultat de l'action effectuée pour pouvoir renvoyer le paquet à la fonction service suivante, en se basant sur la logique de chainage définie, et en générant une sortie (par exemple x, y, z).

Ainsi, la technique proposée permet une gestion d'une politique d'application de manière granulaire, dynamique et distribuée en permettant de viser tous les points de terminaison d'un réseau, sans allouer de nouvelles ressources (en terme de calcul et de stockage). De plus, la

technique proposée tire parti de la définition d'une politique par un modèle, permettant ainsi une grande facilité d'utilisation et de définition, sans tenir compte des contraintes/caractéristiques techniques du réseau.

Les figures 8 et 9 illustrent l'exemple d'une entreprise présentant un réseau privé, comprenant des machines clientes, ou équipements h-1, ..., h-200, appartenant à un premier groupe EPG1. Ces machines clientes disposent d'un accès vers des serveurs d'application s-1, s-2, appartenant à un deuxième groupe EPG2.

La communication entre ces deux groupes est décrite à l'aide des modules GBP et SFC d'un contrôleur SDN, par exemple « OpenDaylight », sous la forme d'un contrat C1 et de deux chaines de fonctions service « *SFC-trafic* » et « *SFC-nettoyeur* ».

La première chaine « *SFC-trafic* » comprend les trois fonctions service suivantes : SF1 correspondant à un inspecteur de paquets DPI1, SF3 correspondant à un pare-feu FW1 et SF4 correspondant à un répartiteur de charge LB1,

La deuxième chaine « *SFC-nettoyeur* » comprend les deux fonctions service suivantes : SF1 correspondant à l'inspecteur de paquets DPI1 et SF2 un nettoyeur de trafic DoS1.

Ainsi, les paquets échangés entre ces deux groupes EPG1 et EPG2 sont routés dans la chaine « *SFC-trafic* » et passent par l'inspecteur de paquets DPI1 pour récupérer des informations de diagnostiques réseaux, le pare-feu FW1 et un répartiteur de charge LB1.

L'autre chaine de services « *SFC-nettoyeur* » est définie dans le cas où l'inspecteur de paquets DPI1 détecte un comportement malicieux et permet de se débarrasser des paquets concernés.

Ainsi, le modèle de politique d'application de règles permet de déterminer que certaines machines clientes du groupe EPG1 doivent être soumises à une inspection de paquets par l'inspecteur de paquets DPI1 en vue de détecter un éventuel comportement malicieux. En fonction du comportement détecté, s'il est avéré, les paquets concernés se verront soit attribuer dynamiquement l'autre chaine de service « *SFC-nettoyeur* », qui acheminera les paquets vers le nettoyeur de trafic DoS1, soit subiront des restrictions de la part du pare-feu FW1.

Pour permettre l'application de cette logique, une chaine de politique d'application EC1 est définie, et illustrée en figure 9.

Cette chaine de politique d'application EC1 permet, de manière granulaire et dynamique, de soumettre par exemple les paquets des machines clientes h-1 et h-2 à une détection de comportement malicieux et se débarrasser des paquets suspicieux. En revanche, les paquets non concernés par la chaine de politique d'application EC1 sont traités tel que défini initialement par les modules GBP et SFC.

Ainsi, pour la chaine de politique d'application EC1 associée au contrat C1, les clauses et actions sont décrites ci-après, grâce à l'entête NSH et aux contextes locaux associés aux différentes fonctions service.

Par exemple, pour la chaine de politique d'application EC1, les informations de contexte portées par l'entête NSH sont les suivantes : une application A, un tenant B (titulaire pour les ressources), les machines clientes h-1 et h-2, le groupe de machines clientes EPG1, les chaines *SFC-trafic* et *SFC-nettoyeur*.

Cette description du contrat et de la chaine de politique d'application EC1 peut s'écrire comme suit :

Contract name: C1

Endpoint Groups: EPG1, EPG2

Enforcement Chain: EC1

Context information: {ApplicationA, tenantB, h-1/h-2, EPG:EPG1, *SFC-trafic*, *SFC-nettoyeur*}

Ensuite, pour la fonction service SF1 (DPI1), le contexte local définit la clause d'inspection de paquets suivante :

- clause *Inspect* : {*SFC-trafic*, application A, tenant B, équipements h-1/h-2} ; cette première clause ne comprend pas d'indication relative au paquet et spécifie qu'un paquet en provenance de l'équipement h-1 ou h-2, doit être routé dans la chaine de fonction service *SFC-trafic*.

Cette description du contexte local peut s'écrire comme suit :

DPI1 local context chain:

ClauseInspect

{

chain: "*SFC-trafic*",

app:"ApplicationA"

tenant: "tenant"

endpoints: ["h-1","h-2"]

Service_related: {}

}

Par ailleurs, une action de politique d'application EA contient l'action proprement dite à effectuer par la fonction service SF1 pour traiter le paquet.

Pour la fonction service SF1, les actions définies dans les clauses sont par exemple les suivantes :

- clause *Inspect* : *« Action Inspect »* : requiert l'inspection du paquet, lorsqu'il provient de l'équipement h-1 ou h-2 et qu'il doit être routé dans la chaine de fonctions service *SFC-trafic*. Cette action peut donner deux résultats R1 ou R3, correspondant respectivement au cas où l'inspection du paquet n'a rien révélé d'anormal (le paquet est alors transmis à la fonction service suivante de la chaine *SFC-trafic*, c'est-à-dire à la fonction service SF3 (pare-feu FW1), avec une liste de restrictions *restriction_list* pour configurer le pare-feu), et au cas où l'inspection du paquet a détecté une anomalie, auquel cas le paquet change de chaine de fonctions service et est routé dans la chaine *SFC-nettoyeur*, c'est-à-dire vers la fonction service SF2 (nettoyeur DoS1) ;
- clause *Default* : « *Action Allow* » : autorisation du paquet (celui-ci ne subit pas de traitement propre à une clause définie et est directement transmis à la prochaine fonction service), lorsqu'il provient de l'équipement h-1 ou h-2 et qu'il doit être routé dans la chaine de fonctions service *SFC-trafic.* Cette action donne le résultat R2 et le paquet alors transmis à la fonction service suivante de la chaine *SFC-trafic*, c'est-à-dire à la fonction service SF3 (pare-feu FW1).

Pour la fonction service SF3 (le pare-feu FW1), le contexte local définit la clause d'application de règles de pare-feu suivante :

- clause *Rules* : {*SFC-trafic*, application A, tenant B, *restriction_list*} ; cette première clause spécifie qu'un paquet dont la sortie du traitement par une fonction service précédente est égale à R1 (*restriction_list)* doit être routé dans la chaine de fonction service *SFC-trafic*.

Cette description du contexte local peut s'écrire comme suit :

FW1 local context chain:
ClauseRules
{
chain: "*SFC-trafic",*
app:"ApplicationA"
tenant: "tenant"
Service_related: {
Output: {
restriction_list: [...]
}
}
}

Pour la fonction service SF3 (le pare-feu FW1), les actions définies dans les clauses sont par exemple les suivantes :

- clause *Rules* : « *Action AddRules* » : application des règles de pare-feu définie par la liste *restriction_list* et transmission du paquet vers la fonction service suivante de la chaine *SFC-trafic*, c'est-à-dire SF4 (répartiteur de charge LB1) ;
- clause *Default* : « *Action Allow* » : autorisation du paquet (celui-ci ne subit pas de traitement propre à une clause définie et est directement transmis à la prochaine fonction service), lorsque la sortie du traitement par une fonction service précédente est égale à R1 (*restriction_list)* et qu'il doit être routé dans la chaine de fonction service *SFC-trafic.* Le paquet est alors transmis à la fonction service suivante de la chaine *SFC-trafic*, c'est-à-dire SF4 (répartiteur de charge LB1).

La fonction service SF2 (nettoyeur DoS1) est quant à elle en charge de vérifier que le paquet entrant est malicieux et le supprime si tel est le cas.

Ainsi, on a vu que les paquets en provenance des équipements h-1 ou h-2 peuvent être routés, selon leur contenu, dans la chaine *SFC-trafic* ou la chaine *SFC-nettoyeur* (lorsqu'ils sont détectés comme ayant un comportement malicieux), alors que les paquets en provenance des autres équipements du groupe EPG1 ne sont pas concernés par la chaine de politique d'application EC1.

REVENDICATIONS

1. Procédé de gestion d'une politique d'application de règles dans un réseau de communication virtualisé comprenant des fonctions virtualisées, dites fonctions service (SF), caractérisé en ce qu'il comprend les étapes suivantes mises en œuvre par un contrôleur SDN dudit réseau :

- génération (S1), à partir d'un ensemble de règles décrivant ladite politique, dit modèle (M), d'un entête d'encapsulation comprenant un contexte relatif audit modèle (M) et d'au moins un contexte local de politique d'application associé à au moins une desdites fonctions service (SF*i*) ;
- transmission (S2) dudit au moins un contexte local à ladite au moins une fonction service (SF*i*) ;
- transmission (S3) dudit entête d'encapsulation à au moins un routeur de paquets, dit classificateur (SCL).

2. Procédé de gestion selon la revendication 1, caractérisé en ce que ladite étape de génération comprend les sous-étapes suivantes :

- obtention, à partir dudit modèle (M) d'au moins un ensemble de règles de traitement de paquets par au moins une desdites fonctions service (SF*i*), dit chaine de politique d'application (EC1) ;
- obtention, à partir de ladite au moins une chaine de politique d'application (EC1), d'un entête de contexte et dudit au moins un contexte local de politique d'application pour au moins une desdites fonctions service (SF*i*) ;
- génération dudit entête d'encapsulation à partir dudit entête de contexte.

3. Procédé de gestion selon la revendication 2, caractérisé en ce que ladite au moins une chaine de politique d'application (EC1) décrit au moins un enchainement (SFC1) d'au moins une desdites fonctions service (SF*i*) en fonction d'au moins une information représentative d'un ensemble prédéfini de règles de communication, dit contrat, entre un premier et un deuxième groupe d'équipements dudit réseau de communication (EPG1, EPG2), ledit premier groupe (EPG1) comprenant au moins un équipement émetteur d'au moins un paquet et ledit deuxième groupe (EPG2) comprenant au moins un équipement destinataire d'au moins un paquet, et/ou d'une information représentative d'au moins un équipement (EP10) dans ledit premier groupe (EPG1) et/ou d'au moins une caractéristique de paquet.

4. Procédé de gestion selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit au moins contexte local comprend au moins une définition d'au moins une action à effectuer par ladite au moins une desdites fonctions service (SF*i*).

5. Procédé de gestion selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite transmission dudit entête d'encapsulation à au moins un classificateur (SCL) comprend une étape de configuration dudit classificateur de service (SCL) de sorte à ce que ledit classificateur de service (SCL) délivre, pour au moins un paquet entrant, au moins un paquet enrichi avec ledit entête d'encapsulation.

6. Procédé de traitement d'une politique d'application de règles dans un réseau de communication comprenant des fonctions virtualisées, dite fonctions service (SF),
caractérisé en ce qu'il comprend, dans au moins une desdites fonctions service (SF*i*), une étape préalable de réception (S4), en provenance d'un contrôleur SDN dudit réseau, d'un contexte local de politique d'application associé à ladite au moins une fonction service (SF*i*), et les étapes suivantes :

- réception (S5) d'au moins un paquet enrichi avec un entête d'encapsulation par un routeur de paquets, dit classificateur (SCL) dudit réseau;
- traitement (S6) dudit au moins un paquet enrichi, en tenant compte dudit contexte local de politique d'application associé à ladite au moins une fonction service (SF*i*).

7. Procédé de traitement selon la revendication 6, caractérisé en ce que ledit traitement comprend une étape d'exécution d'au moins une action définie dans ledit contexte local de politique d'application, en tenant compte d'au moins une caractéristique dudit au moins un paquet enrichi et délivrant un résultat comprenant au moins une information d'identification d'au moins une fonction de service destinatrice (*SFj*) dudit paquet enrichi traité.

8. Procédé de traitement selon la revendication 7, caractérisé en ce que ledit traitement comprend également une étape de mise à jour dudit entête d'encapsulation en fonction dudit résultat de ladite étape d'exécution.

9. Module contrôleur SDN, caractérisé en ce qu'il comprend :

- des moyens de génération, à partir d'un ensemble de règles, dit modèle (M), décrivant une politique d'application de règles dans un réseau de communication

virtualisé comprenant des fonctions virtualisées, dites fonctions service (SF), d'un entête d'encapsulation comprenant un contexte relatif audit modèle (M) et d'au moins un contexte local de politique d'application associé à au moins une desdites fonctions service (SF*i*) ;

- des moyens de transmission dudit au moins un contexte local à ladite au moins une fonction service (SFi) ;
- des moyens de transmission dudit entête d'encapsulation à au moins un routeur de paquets, dit classificateur (SCL).

10. Module fonction virtualisée, dit module fonction service, dans un réseau de communication virtualisé, caractérisé en ce que ledit module comprend un module de logique de politique d'application (PEL) comprenant :

- des moyens de réception, en provenance d'un contrôleur SDN dudit réseau, d'un contexte local de politique d'application associé audit module fonction service ;
- des moyens de réception d'au moins un paquet enrichi avec un entête d'encapsulation par un routeur de paquets, dit classificateur (SCL) dudit réseau;
- des moyens de traitement dudit au moins un paquet enrichi, en tenant compte dudit contexte local de politique d'application.

11. Système comprenant un module contrôleur SDN selon la revendication 9, un module fonction service selon la revendication 10 et un routeur de paquets, dit classificateur (SCL) recevant un entête d'encapsulation dudit contrôleur SDN et délivrant, pour au moins un paquet entrant, au moins un paquet enrichi avec ledit entête d'encapsulation.

12. Produit programme d'ordinateur comprenant des instructions de code de programme pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 5 ou 6 à 8, lorsqu'il est exécuté par un processeur.

13. Support d'informations comportant des instructions de programme adaptées à la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 5 ou 6 à 8, lorsque ledit programme est exécuté par un processeur.

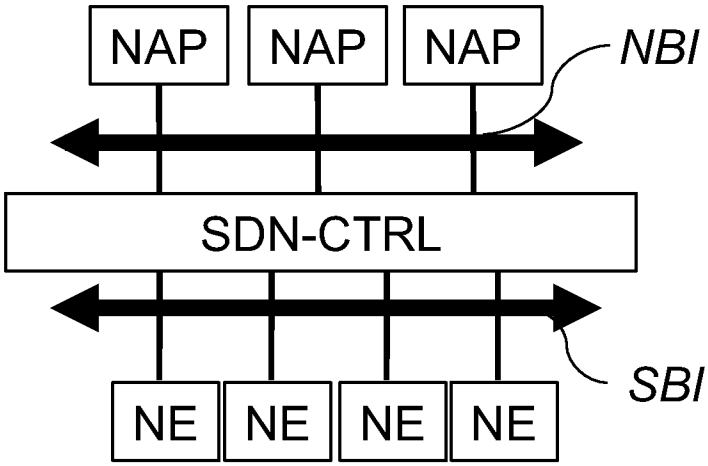

Fig. 1
(Art Antérieur)

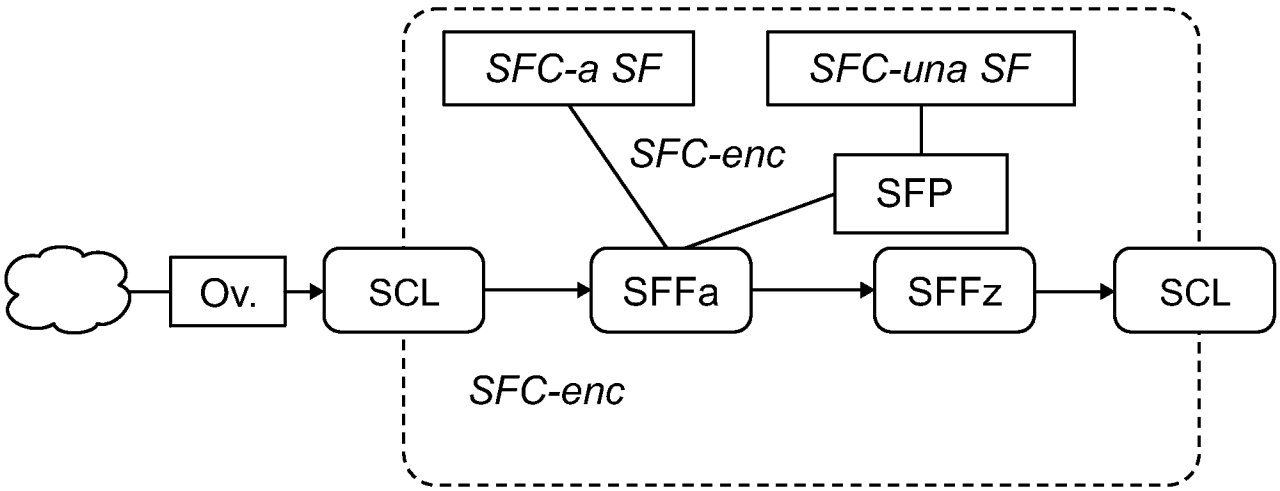

Fig. 2
(Art Antérieur)

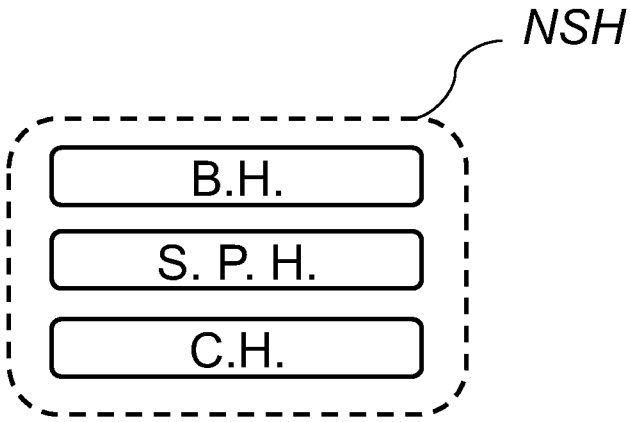

Fig. 3
(Art Antérieur)

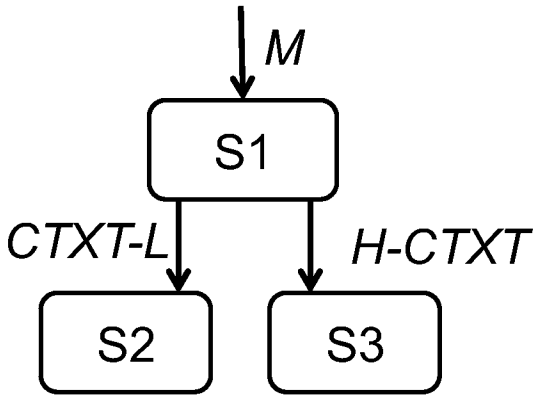

Fig. 4a

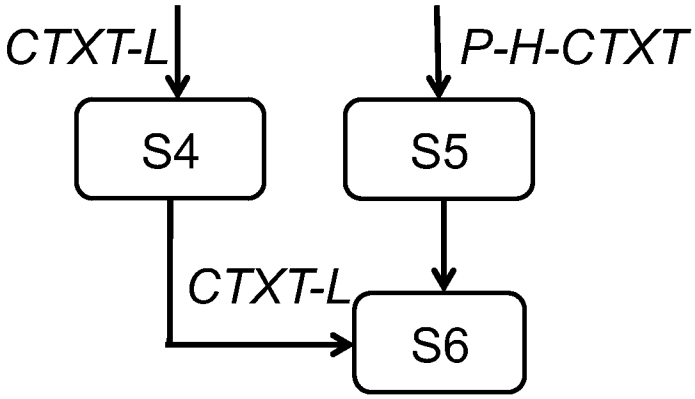

Fig. 4b

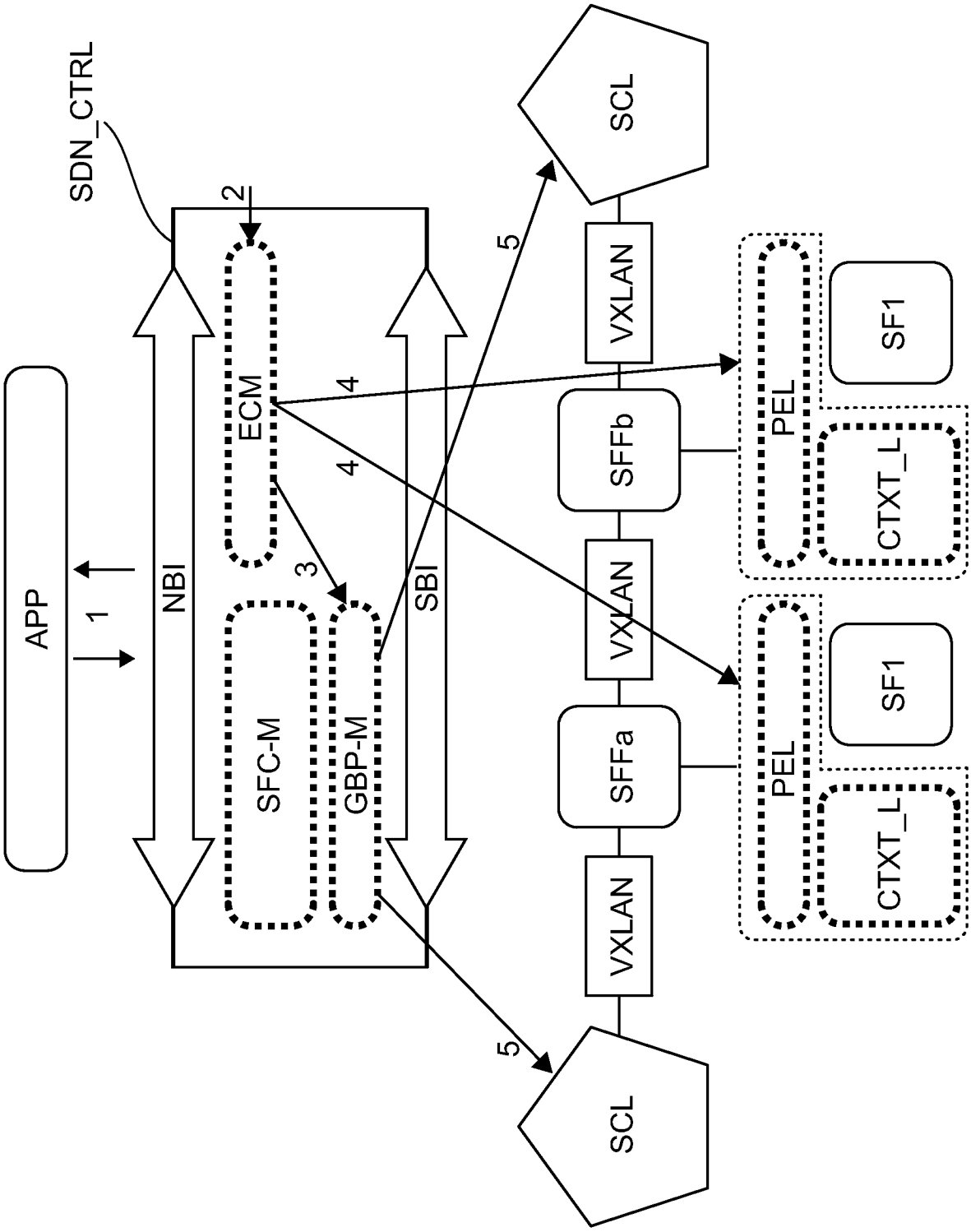
SDN_CTRL
APP
1
NBI
2
ECM
3
SFC-M
GBP-M
SBI
4
4
5
5
SCL
VXLAN
SFFb
VXLAN
SFFa
VXLAN
SCL
PEL
CTXT_L
SF1
PEL
CTXT_L
SF1

Fig. 5

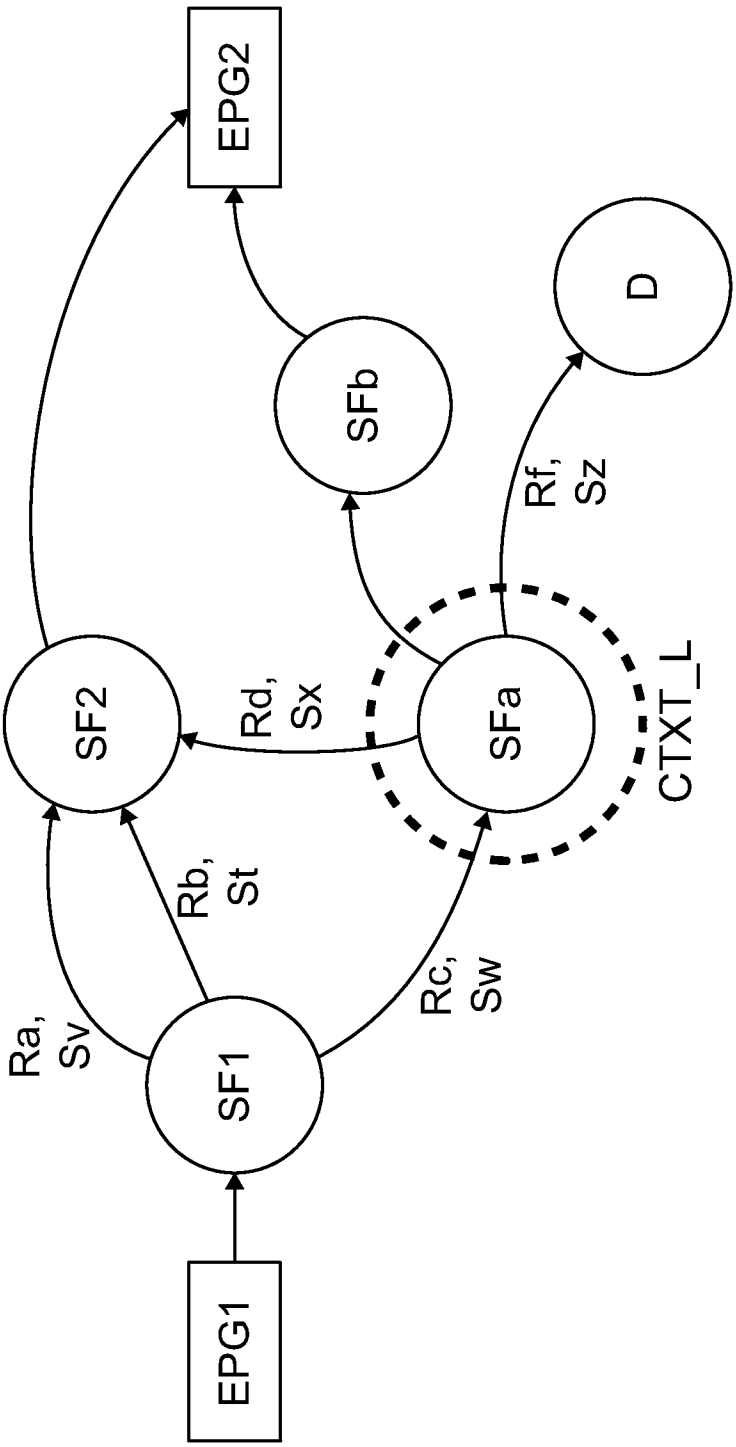
EPG2
SFb
D
Rf,
Sz
SF2
Rd,
Sx
SFa
CTXT_L
Ra,
Sv
Rb,
St
Rc,
Sw
SF1
EPG1

Fig. 6

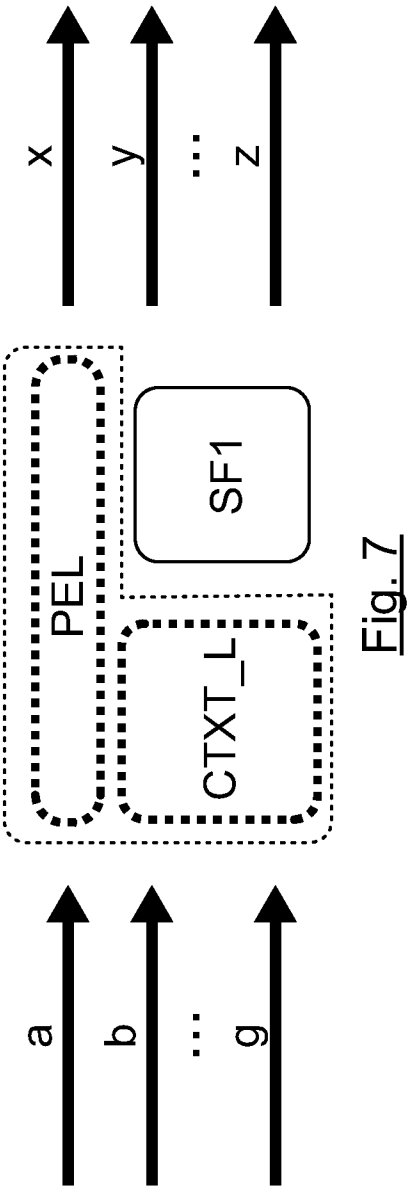
x
y
...
z
PEL
SF1
CTXT_L
a
b
...
g

Fig. 7

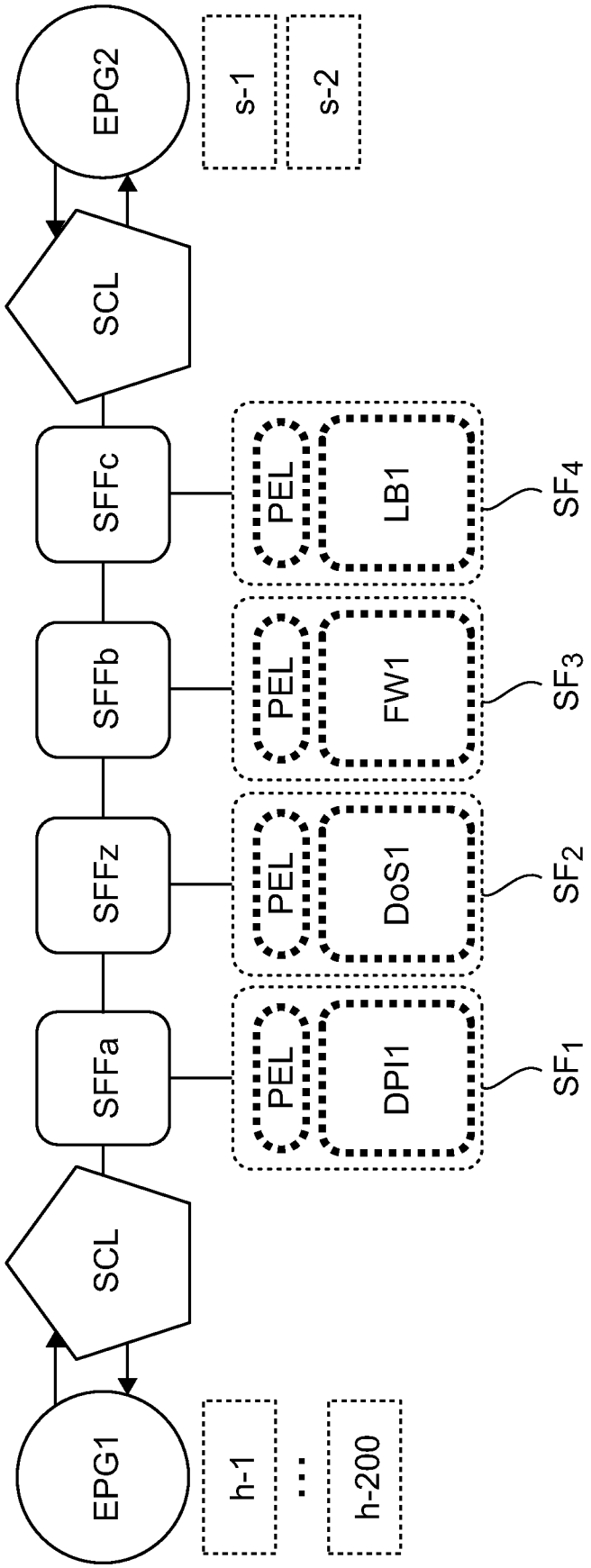
EPG2
s-1
s-2
SCL
SFFc
SFFb
SFFz
SFFa
PEL
LB1
FW1
DoS1
DPI1
SF4
SF3
SF2
SF1
SCL
EPG1
h-1
...
h-200

Fig. 8

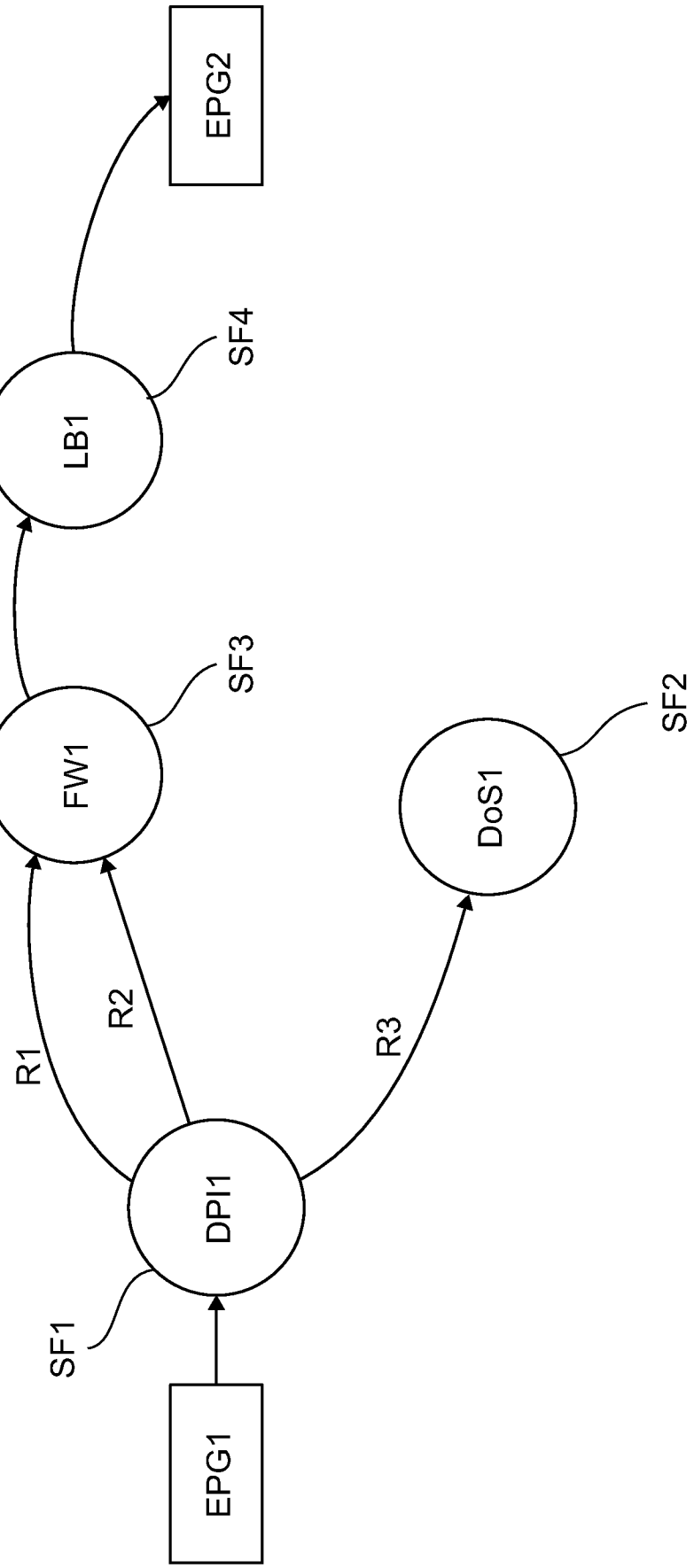

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FR2019/051586

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/455(2018.01)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)

G06F

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, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHAITHAN PRAKASH ET AL. "PGA: Using Graphs to Express and Automatically Reconcile Network Policies" *SPECIAL INTEREST GROUP ON DATA COMMUNICATION, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA*, 17 August 2015 (2015-08-17), pages 29-42 DOI: 10.1145/2785956.2787506 ISBN: 978-1-4503-3542-3. XP058071210	1-5,9,12,13
Y	abstract page 29, right-hand column, last paragraph - page 30, left-hand column, paragraph 6 page 32, left-hand column, last paragraph - page 33, right-hand column, paragraph 1 page 34, left-hand column, last paragraph - page 34, right-hand column, paragraph 3 page 35, right-hand column, paragraph 3 page 38, left-hand column, paragraph 1 - page 38, right-hand column, paragraph 2	11

☑ 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
30 September 2019	**15 October 2019**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Lelait, Sylvain** Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HANTOUTI HAJAR ET AL. "A Novel SDN-based Architecture and Traffic Steering Method for Service Function Chaining" *2018 INTERNATIONAL CONFERENCE ON SELECTED TOPICS IN MOBILE AND WIRELESS NETWORKING (MOWNET), IEEE,* 20 June 2018 (2018-06-20), pages 1-8 DOI: 10.1109/MOWNET.2018.8428930 XP033383130	6-8,10,12,13
Y	abstract page 1, left-hand column, paragraph 1 - page 1, right-hand column, paragraph 3 page 2, left-hand column, last paragraph - page 6, left-hand column, paragraph 1	11
X	WO 2017137004 A1 (HUAWEI TECH CO LTD [CN]) 17 August 2017 (2017-08-17) abstract page 3, paragraph 7 - page 4, paragraph 11 page 6, paragraph 30 - page 10, paragraph 38 page 12, paragraph 47 - page 18, paragraph 70; figures 2,3A	6-8,10,12,13
A	GUANGLEI LI ET AL. "Application-aware and Dynamic Security Function Chaining for Mobile Networks" *JOURNAL OF INTERNET SERVICES AND INFORMATION SECURITY,* Vol. 7, No. 4, 01 November 2017 (2017-11-01), pages 21-34 XP055568831 abstract page 21, paragraph 1 - page 22, paragraph 5 page 24, paragraph 4 - page 28, paragraph 3	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FR2019/051586

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2017137004 A1	17 August 2017	US 2017237656 A1	17 August 2017
		WO 2017137004 A1	17 August 2017

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2019/051586

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F9/455
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)
G06F

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, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	CHAITHAN PRAKASH ET AL: "PGA: Using Graphs to Express and Automatically Reconcile Network Policies", SPECIAL INTEREST GROUP ON DATA COMMUNICATION, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 17 août 2015 (2015-08-17), pages 29-42, XP058071210, DOI: 10.1145/2785956.2787506 ISBN: 978-1-4503-3542-3	1-5,9, 12,13
Y	abrégé page 29, colonne de droite, dernier alinéa - page 30, colonne de gauche, alinéa 6 page 32, colonne de gauche, dernier alinéa - page 33, colonne de droite, alinéa 1 page 34, colonne de gauche, dernier alinéa - page 34, colonne de droite, alinéa 3 page 35, colonne de droite, alinéa 3 page 38, colonne de gauche, alinéa 1 - -/--	11

[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
30 septembre 2019	15/10/2019

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	Lelait, Sylvain

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
	page 38, colonne de droite, alinéa 2	

X	HANTOUTI HAJAR ET AL: "A Novel SDN-based Architecture and Traffic Steering Method for Service Function Chaining", 2018 INTERNATIONAL CONFERENCE ON SELECTED TOPICS IN MOBILE AND WIRELESS NETWORKING (MOWNET), IEEE, 20 juin 2018 (2018-06-20), pages 1-8, XP033383130, DOI: 10.1109/MOWNET.2018.8428930	6-8,10, 12,13
Y	abrégé page 1, colonne de gauche, alinéa 1 - page 1, colonne de droite, alinéa 3 page 2, colonne de gauche, dernier alinéa - page 6, colonne de gauche, alinéa 1	11

X	WO 2017/137004 A1 (HUAWEI TECH CO LTD [CN]) 17 août 2017 (2017-08-17) abrégé page 3, alinéa 7 - page 4, alinéa 11 page 6, alinéa 30 - page 10, alinéa 38 page 12, alinéa 47 - page 18, alinéa 70; figures 2,3A	6-8,10, 12,13

A	GUANGLEI LI ET AL: "Application-aware and Dynamic Security Function Chaining for Mobile Networks", JOURNAL OF INTERNET SERVICES AND INFORMATION SECURITY, vol. 7, no. 4, 1 novembre 2017 (2017-11-01), pages 21-34, XP055568831, abrégé page 21, alinéa 1 - page 22, alinéa 5 page 24, alinéa 4 - page 28, alinéa 3	1-13

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2019/051586

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2017137004 A1	17-08-2017	US 2017237656 A1	17-08-2017
		WO 2017137004 A1	17-08-2017