(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 129 552***

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

(21) **N° d'enregistrement national :** **21 12451**

(51) Int Cl[8] : ***H 04 L 41/08*** *(2022.01), H 04 L 9/40, H 04 L 45/00, H 04 L 1/00*

(12) **BREVET D'INVENTION** **B1**

(54) Procédé de contrôle dans un système informatique, système informatique et programme d'ordinateur pour la mise en œuvre du procédé.

(22) **Date de dépôt :** 24.11.21.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 26.05.23 Bulletin 23/21.

(45) **Date de la mise à disposition du public du brevet d'invention :** 19.01.24 Bulletin 24/03.

(56) **Liste des documents cités dans le rapport de recherche :**

*Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ORANGE Société anonyme* — FR.

(72) **Inventeur(s) :** Carrière Jean-Christophe et Le Calloch Stéfane.

(73) **Titulaire(s) :** ORANGE Société anonyme.

(74) **Mandataire(s) :** Plasseraud IP.

FR 3 129 552 - B1

# Description

## Titre de l'invention : Procédé de contrôle dans un système informatique, système informatique et programme d'ordinateur pour la mise en œuvre du procédé

### Domaine technique

[0001] La présente invention se rapporte à un procédé de contrôle dans un système informatique, ainsi qu'à un programme d'ordinateur et un système informatique pour la mise en œuvre de ce procédé. Elle s'applique notamment aux systèmes informatiques au sein desquels une ou plusieurs fonctions réseau virtualisées sont mises en œuvre.

### Technique antérieure

[0002] Les opérateurs de télécommunications déploient depuis quelques années, notamment pour leurs clients entreprise, des solutions de communications de voix et de données mises en œuvre par des fonctions réseau virtualisées sur des plateformes généralistes de fourniture de services destinées à être installées chez leurs clients (en anglais, « universal Customer Premises Equipment », ou « uCPE »). Les plateformes uCPE permettent le déploiement, la configuration ainsi que la suppression à distance, par exemple par l'intermédiaire d'un réseau de communication étendu (en anglais « Wide Area Network », ou WAN), de machines virtuelles exécutées sur une plateforme matérielle orientée réseau. Ces machines virtuelles peuvent être configurées pour la fourniture de fonctions réseau virtualisées (en anglais « Virtual Network Function », ou « VNF »), comme par exemple des fonctions de routage, de communication de voix et/ou de données, de sécurité, etc.

[0003] Les plateformes de type uCPE sont notamment conçues pour des cas d'usage qui prévoient leur déploiement au sein d'agences ou de succursales de clients de l'opérateur, comme par exemple des agences d'un réseau d'une banque de détail. Dans le cadre de ces cas d'usage, certains clients peuvent souhaiter contrôler la configuration des uCPE déployés dans leurs agences, notamment pour prendre en charge la configuration au sein de ces uCPE de fonctions de sécurité qui sont spécifiques à leur environnement informatique.

[0004] L'accès à la configuration au niveau administrateur des fonctions virtualisées mises en œuvre au sein d'un uCPE peut conduire à des erreurs de configuration qui sont susceptibles d'impacter l'accès d'une ou plusieurs fonctions virtualisées de l'équipement uCPE, de causer des dysfonctionnements, voire une indisponibilité totale de l'équipement.

[0005] En outre, une mauvaise configuration d'un équipement uCPE peut aussi être la conséquence ou le résultat d'une tentative malveillante d'accès à l'équipement.

[0006] La possibilité d'une attaque de sécurité ou d'une erreur de configuration d'un équipement uCPE soulève le problème des risques de sécurité pour des équipements de type uCPE déployés sur site pour lesquels l'accès de configuration reste, au moins partiellement, ouvert.

**Résumé**

[0007] La présente divulgation vient améliorer la situation.

[0008] Selon un premier aspect, il est proposé un procédé de contrôle dans un système informatique comprenant au moins une machine virtuelle utilisateur pilotée par un hyperviseur et une unité de contrôle, le procédé étant mis en œuvre par l'unité de contrôle et comprenant : recevoir d'une machine virtuelle utilisateur un paquet de données associé à un flux d'administration, ledit paquet de données comprenant un identifiant de réseau et une première adresse physique identifiant la machine virtuelle utilisateur ; et lorsque l'identifiant de réseau est associé à une deuxième adresse physique différente de la première adresse physique, bloquer le paquet de données.

[0009] Le procédé proposé permet avantageusement de détecter la survenance d'une situation de duplication d'identifiant de réseau ou d'adresse physique utilisée par une machine virtuelle utilisateur d'un système informatique, situation qui peut, selon les cas d'usage, résulter d'une erreur de configuration de l'interface réseau de gestion de la machine virtuelle utilisateur ou d'une action malveillante. La sécurité du système informatique est ainsi améliorée par détection d'une anomalie dans le trafic associé à un flux d'administration, anomalie qui peut ensuite être corrigée. Par exemple, le procédé proposé permet avantageusement de détecter une situation d'anomalie dans laquelle deux machines virtuelles utilisateur d'un système informatique utilisent pour leurs interfaces réseau de gestion respectives un même identifiant de réseau (par exemple une même adresse IP), auquel cas une de ces deux machines virtuelles utilisateur usurpe l'identifiant de réseau de l'autre machine virtuelle utilisateur. Autre exemple de situation d'anomalie, le procédé proposé permet aussi avantageusement de détecter une situation dans laquelle une configuration d'interface réseau de gestion d'une machine virtuelle utilisateur a conduit à modifier l'association entre un identifiant de réseau et une adresse physique de l'interface réseau de gestion (par exemple, une adresse IP a été associée à une autre adresse MAC, ou une adresse IP a été associée à un autre port de communication). Le paquet de données ayant conduit à la détection de la situation d'anomalie est alors bloqué, afin d'isoler la machine virtuelle utilisateur à l'origine de ce paquet et d'éviter ainsi les disfonctionnements du système informatique.

[0010] Les caractéristiques exposées dans les paragraphes suivants peuvent, optionnellement, être mises en œuvre. Elles peuvent être mises en œuvre indépendamment les unes des autres ou en combinaison les unes avec les autres.

[0011] Dans un ou plusieurs modes de réalisation, l'unité de contrôle comprend une

machine virtuelle pilotée par l'hyperviseur, dite machine virtuelle de contrôle, configurée pour la mise en œuvre du procédé proposé. Dans ces modes de réalisation, le procédé proposé est mis en œuvre par une machine virtuelle de contrôle pilotée par l'hyperviseur au sein du système informatique. La mise en œuvre du procédé proposé par une machine virtuelle instanciée au sein du système informatique permet avantageusement une mise en œuvre logicielle qui peut être adaptée à l'architecture (matérielle et/ou logicielle) existante d'un système informatique (par exemple de type uCPE). Le procédé proposé peut ainsi avantageusement être mis en œuvre, par le biais de l'instanciation d'une machine virtuelle de contrôle configurée pour sa mise en œuvre, au sein d'un équipement, par exemple un uCPE.

[0012] Dans un ou plusieurs modes de réalisation, la deuxième adresse physique est stockée en association avec l'identifiant de réseau dans une table de correspondance, et le procédé proposé comprend en outre : déterminer que l'identifiant de réseau est associé à la deuxième adresse physique par lecture de la table. Le contrôle exercé selon le procédé proposé est alors avantageusement mis en œuvre par le biais d'une table de correspondance, qui peut être créée puis mise à jour, par exemple lors de chaque instanciation ou désinstallation d'une machine virtuelle utilisateur dans le système informatique, de manière centralisée, par exemple par un administrateur d'un réseau d'administration auquel la machine virtuelle utilisateur est connectée via une interface réseau de gestion.

[0013] Dans un ou plusieurs modes de réalisation, le procédé proposé comprend en outre : générer une alarme de duplication d'identifiant de réseau au sein du système informatique. Un administrateur du système informatique peut ainsi être avantageusement informé de la survenance d'une situation de duplication d'identifiant de réseau au sein du système informatique, et prendre des mesures pour corriger cette situation.

[0014] Dans un ou plusieurs modes de réalisation, l'adresse physique comprend une adresse MAC et/ou un numéro de port. Dans un ou plusieurs modes de réalisation, l'identifiant de réseau comprend une adresse IP.

[0015] Dans un ou plusieurs modes de réalisation, l'identifiant de réseau est associé à la deuxième adresse physique sur instanciation de la machine virtuelle utilisateur au sein du système informatique. Le contrôle selon le procédé proposé exercé pour la machine virtuelle utilisateur est alors avantageusement basé sur une association entre l'identifiant de réseau et la deuxième adresse physique initialisée dès l'instanciation de la machine virtuelle utilisateur. Le procédé proposé peut alors avantageusement être utilisé pour contrôler la machine virtuelle utilisateur dès lors qu'elle est instanciée au sein du système informatique.

[0016] Dans un ou plusieurs modes de réalisation, le procédé proposé comprend en outre :

extraire l'identifiant de réseau et la première adresse physique du paquet de données reçu. Le contrôle de la machine virtuelle utilisateur sur la base du paquet reçu peut alors avantageusement utiliser les informations extraites de ce paquet, afin de les comparer à des informations de référence pour détecter une éventuelle situation de duplication d'identifiant de réseau.

[0017] Dans un ou plusieurs modes de réalisation, le procédé proposé comprend en outre : instancier la machine virtuelle de contrôle à partir d'une configuration initiale du système informatique ne comprenant aucune machine virtuelle utilisateur. L'instanciation d'une ou plusieurs machines virtuelles utilisateur peut alors n'être effectuée qu'à partir du moment où la machine virtuelle de contrôle est instanciée, ce qui permet avantageusement d'assurer que la machine virtuelle de contrôle puisse être configurée pour contrôler chaque machine virtuelle utilisateur nouvellement instanciée au sein du système informatique.

[0018] Selon un autre aspect, un système informatique est proposé, qui comprend une unité de traitement comprenant un processeur et une mémoire couplée de manière opérationnelle au processeur, au moins une machine virtuelle utilisateur pilotée par un hyperviseur, l'unité de traitement étant configurée pour la mise en œuvre, par l'unité de contrôle, d'un procédé selon l'un des modes de réalisation proposés dans la présente demande.

[0019] Un autre aspect concerne un système informatique comprenant une unité de traitement comprenant un processeur et une mémoire couplée de manière opérationnelle au processeur, au moins une machine virtuelle utilisateur et une machine virtuelle de contrôle pilotées par un hyperviseur, l'unité de traitement étant configurée pour la mise en œuvre, par la machine virtuelle de contrôle, d'un procédé selon l'un des modes de réalisation proposés dans la présente demande.

[0020] Un autre aspect concerne une machine virtuelle dite de contrôle dans un système informatique comprenant au moins une machine virtuelle utilisateur et la machine virtuelle de contrôle pilotées par un hyperviseur, configurée pour la mise en œuvre d'un procédé selon l'un des modes de réalisation proposés dans la présente demande.

[0021] Un autre aspect concerne un programme d'ordinateur, chargeable dans une mémoire associée à un processeur, et comprenant des portions de code pour la mise en œuvre d'un procédé selon l'un des modes de réalisation proposés dans la présente demande lors de l'exécution dudit programme par le processeur.

[0022] Un autre aspect concerne un ensemble de données représentant, par exemple par voie de compression ou d'encodage, un programme d'ordinateur tel que proposé dans la présente demande.

[0023] Un autre aspect concerne un support de stockage non-transitoire d'un programme exécutable par ordinateur, comprenant un ensemble de données représentant un ou

plusieurs programmes, lesdits un ou plusieurs programmes comprenant des instructions pour, lors de l'exécution desdits un ou plusieurs programmes par un ordinateur comprenant un processeur couplé de manière opérationnelle à une mémoire, conduire l'ordinateur à mettre en œuvre un procédé selon l'un des modes de réalisation proposés dans la présente demande.

[0024] Un autre aspect concerne un support de stockage non-transitoire d'un programme exécutable par ordinateur, comprenant un ensemble de données représentant un ou plusieurs programmes, lesdits un ou plusieurs programmes comprenant des instructions pour, lors de l'exécution desdits un ou plusieurs programmes par un ordinateur comprenant une unité de traitement couplée de manière opérationnelle à des moyens mémoire, conduire l'ordinateur à mettre en œuvre un procédé selon l'un des modes de réalisation proposés dans la présente demande.

## Brève description des dessins

[0025] D'autres particularités et avantages de la présente divulgation apparaîtront dans la description ci-après d'exemples de réalisation non limitatifs, en référence aux dessins annexés, dans lesquels :

**Fig. 1**

[0026] [Fig.1] illustre un exemple d'architecture de système informatique dans lequel le procédé proposé peut être mis en œuvre selon un ou plusieurs modes de réalisation ;

**Fig. 2**

[0027] [Fig.2] est un diagramme illustrant un procédé selon un ou plusieurs modes de réalisation ;

**Fig. 3**

[0028] [Fig.3] illustre un exemple d'architecture de système informatique pour la mise en œuvre du procédé proposé selon un ou plusieurs modes de réalisation.

## Description des modes de réalisation

[0029] Dans la description détaillée ci-après de modes de réalisation particuliers, de nombreux détails spécifiques sont présentés pour apporter une compréhension plus complète. Néanmoins, l'homme du métier peut se rendre compte que des modes de réalisation peuvent être mis en pratique sans ces détails spécifiques. Dans d'autres cas, des caractéristiques bien connues ne sont pas décrites en détail pour éviter de compliquer inutilement la présente description.

[0030] La présente demande fait référence à des fonctions, moteurs, unités, modules, plateformes, et illustrations de diagrammes des méthodes et dispositifs selon un ou plusieurs modes de réalisation. Chacun des fonctions, moteurs, modules, plateformes, unités et diagrammes décrits peut être mis en œuvre sous forme matérielle, logicielle (y compris sous forme de logiciel embarqué («firmware»), ou de «middleware»),

microcode, ou toute combinaison de ces derniers. Dans le cas d'une mise en œuvre sous forme logicielle, les fonctions, moteurs, unités, modules, plateformes et/ou illustrations de diagrammes peuvent être mis en œuvre par des instructions de programme d'ordinateur ou du code logiciel, qui peut être stocké ou transmis sur un support lisible par ordinateur, incluant un support non transitoire, ou un support chargé en mémoire d'un ordinateur générique, spécifique, ou de tout autre appareil ou dispositif programmable de traitement de données pour produire une machine, de telle sorte que les instructions de programme d'ordinateur ou le code logiciel exécuté(es) sur l'ordinateur ou l'appareil ou dispositif programmable de traitement de données, constituent des moyens de mise en œuvre de ces fonctions.

[0031] Les modes de réalisation d'un support lisible par ordinateur incluent, de manière non exhaustive, des supports de stockage informatique et des supports de communication, y compris tout support facilitant le transfert d'un programme d'ordinateur d'un endroit vers un autre. Par «support(s) de stockage informatique», on entend tout support physique pouvant être accédé par ordinateur. Les exemples de support de stockage informatique incluent, de manière non limitative, les disques ou composants de mémoire flash ou tous autres dispositifs à mémoire flash (par exemple des clés USB, des clés de mémoire, des sticks mémoire, des disques-clés), des CD-ROM ou autres dispositifs de stockage optique de données, des DVD, des dispositifs de stockage de données à disque magnétique ou autres dispositifs de stockage magnétique de données, des composants de mémoire de données, des mémoires RAM, ROM, EEPROM, des cartes mémoires («smart cards»), des mémoires de type SSD («Solid State Drive»), et toute autre forme de support utilisable pour transporter ou stocker ou mémoriser des données ou structures de données qui peuvent être lues par un processeur d'ordinateur.

[0032] En outre, diverses formes de support lisible par ordinateur peuvent transmettre ou porter des instructions vers un ordinateur, telles qu'un routeur, une passerelle, un serveur, ou tout équipement de transmission de données, qu'il s'agisse de transmission filaire (par câble coaxial, fibre optique, fils téléphoniques, câble DSL, ou câble Ethernet), sans-fil (par infrarouge, radio, cellulaire, microondes), ou des équipements de transmission virtualisés (routeur virtuel, passerelle virtuelle, extrémité de tunnel virtuel, pare-feu virtuel). Les instructions peuvent, selon les modes de réalisation, comprendre du code de tout langage de programmation informatique ou élément de programme informatique, tel que, sans limitation, les langages assembleur, C, C++, Visual Basic, HyperText Markup Language (HTML), Extensible Markup Language (XML), HyperText Transfer Protocol (HTTP), Hypertext Preprocessor (PHP), SQL, MySQL, Java, JavaScript, JavaScript Object Notation (JSON), Python, et bash scripting.

[0033] De plus, les termes «notamment», «par exemple», «exemple», «typiquement» sont

utilisés dans la présente description pour désigner des exemples ou illustrations de modes de réalisation non limitatifs, qui ne correspondent pas nécessairement à des modes de réalisation préférés ou avantageux par rapport à d'autres aspects ou modes de réalisation possibles.

[0034] Par «serveur» ou «plateforme», on entend dans la présente demande tout point de service (virtualisé ou non) ou dispositif opérant des traitements de données, une ou plusieurs bases de données, et/ou des fonctions de communication de données. Par exemple, et de manière non limitative, le terme «serveur» ou le terme «plateforme» peut faire référence à un processeur physique couplé de manière opérationnelle avec des fonctions de communication, de base de données et de stockage de données associées, ou faire référence à un réseau, un groupe, un ensemble ou un complexe de processeurs et des équipements de stockage de données et de mise en réseau associés, ainsi qu'un système d'exploitation et un ou plusieurs système(s) de base de données et des logiciels applicatifs en support des services et fonctions fournies par le serveur. Un dispositif informatique peut être configuré pour envoyer et recevoir des signaux, par réseau(x) de transmission sans-fil et/ou filaire, ou peut être configuré pour des traitements et/ou du stockage de données ou de signaux, et peut donc fonctionner en tant que serveur. Ainsi, des équipements configurés pour opérer en tant que serveur peuvent inclure, à titre d'exemples non limitatifs, des serveurs dédiés montés sur rack, des ordinateurs de bureau, des ordinateurs portables, des passerelles de service (parfois appelées «box» ou «passerelle résidentielle»), des décodeurs multimédia (parfois appelés «set-top boxes»), des équipements intégrés combinant diverses fonctionnalités, telles que deux ou plus des fonctionnalités mentionnées ci-dessus. Les serveurs peuvent fortement varier dans leur configuration ou leurs capacités, mais un serveur inclura généralement une ou plusieurs unité(s) centrale(s) de traitement et une mémoire. Un serveur peut aussi inclure un ou plusieurs équipement(s) de mémoire de masse, une ou plusieurs alimentation(s) électrique(s), une ou plusieurs interface(s) réseau sans-fil et/ou filaire(s), une ou plusieurs interface(s) d'entrée/sortie, un ou plusieurs système(s) d'exploitation, tel(s) que Windows Server, Mac OS X, Unix, Linux, FreeBSD, or un équivalent.

[0035] Les termes «réseau» et «réseau de communication» tels qu'utilisés dans la présente demande font référence à une ou plusieurs liaisons de données qui peuvent coupler ou connecter des équipements, éventuellement virtualisés, de manière à permettre le transport de données électroniques entre des systèmes informatiques et/ou des modules et/ou d'autres dispositifs ou équipements électroniques, tel qu'entre un serveur et un dispositif client ou d'autres types de dispositifs, y compris entre dispositifs sans fil couplés ou connectés par un réseau sans fil, par exemple. Un réseau peut aussi inclure une mémoire de masse pour stocker des données, tel qu'un NAS (en anglais «network

attached storage», un SAN (en anglais «storage area network»), ou toute autre forme de support lisible par un ordinateur ou par une machine, par exemple. Un réseau peut comprendre, en tout ou partie, le réseau Internet, un ou plusieurs réseaux locaux (en anglais «local area networks», ou LANs), un ou plusieurs réseaux de type WAN (en anglais «wide area networks»), des connexions de type filaire, des connexions de type sans fil, de type cellulaire, ou toute combinaison de ces différents réseaux. De manière similaire, des sous-réseaux peuvent utiliser différentes architectures ou être conformes ou compatibles avec différents protocoles, et inter-opérer avec des réseaux de plus grande taille. Différents types d'équipements peuvent être utilisés pour rendre inter-opérables différentes architectures ou différents protocoles. Par exemple, un routeur peut être utilisé pour fournir une liaison de communication ou une liaison de données entre deux LANs qui seraient autrement séparés et indépendants.

[0036] Les termes «couplé de manière opérationnelle», «couplé», «monté», «connecté» et leurs variantes et formes diverses utilisés dans les présentes font référence à des couplages, connexions, montages, qui peuvent être directs ou indirects, et comprennent notamment des connexions entre équipements électroniques ou entre des portions de tels équipements qui permettent des opérations et fonctionnements tels que décrits dans la présente demande. De plus, les termes «connectés» et «couplés» ne sont pas limités à des connections ou des couplages physiques ou mécaniques. Par exemple, un couplage de manière opérationnelle peut inclure une ou plusieurs connexion(s) filaire(s) et/ou une ou plusieurs connexion(s) sans-fil entre deux équipements ou plus qui permettent des liaisons de communication simplex et/ou duplex entre les équipements ou des portions des équipements. Selon un autre exemple, un couplage opérationnel ou une connexion peut inclure un couplage par liaison filaire et/ou sans-fil pour permettre des communications de données entre un serveur du système proposé et un autre équipement du système.

[0037] Les procédés et systèmes proposés visent à éviter la survenance d'une situation dans laquelle une interface réseau de gestion d'une machine virtuelle d'un système informatique est configurée avec un identifiant (par exemple une adresse IP, une adresse MAC, etc.) déjà utilisée pour l'interface réseau de gestion d'une autre machine virtuelle du système informatique ou pour l'hyperviseur du système informatique. Ce type de situation, dans laquelle par exemple deux machines virtuelles utilisent une même adresse IP sur leurs interfaces réseau de gestion respectives, est susceptible de causer, lorsqu'il se produit pour une machine virtuelle, un disfonctionnement, une indisponibilité, ou un accès non autorisé des autres machines virtuelles, voire de l'hyperviseur du système informatique. L'interface réseau de gestion connecte la machine virtuelle avec un réseau d'administration géré par l'opérateur (non représenté sur la [Fig.1]). Ce réseau d'administration fournit différents services d'administration à

la machine virtuelle, par exemple un serveur de temps de type NTP (pour « Network Time Protocol ») ou un serveur de sauvegarde.

[0038] Les procédés et systèmes proposés concernent de manière générale le contrôle dans un système informatique comprenant une ou plusieurs machines virtuelles pilotées par un hyperviseur. Ils peuvent en particulier, mais de manière non limitative, avantageusement être utilisés pour le contrôle des flux d'administration sur les interfaces réseau de gestion. Les machines virtuelles sont par exemple configurées pour la mise en œuvre de fonctions réseau virtualisées (VNF) au sein d'un équipement de type uCPE.

[0039] En fonction du mode de réalisation choisi, différents types ou architectures d'équipements peuvent être envisagés pour la mise en œuvre des procédés de contrôle proposés. Ainsi, dans un ou plusieurs modes de réalisation, un équipement configuré pour la mise en œuvre des procédés et systèmes proposés peut être un équipement de type uCPE installé par un opérateur de télécommunications chez un client entreprise, par exemple dans une agence d'un réseau d'agences de ce client. Dans un ou plusieurs modes de réalisation, différents types ou architectures d'équipements uCPE peuvent être utilisés au sein d'un même système tel que proposé pour la mise en œuvre des procédés de contrôle proposés.

[0040] La [Fig.1] illustre un exemple d'architecture de système informatique (1) dans lequel le procédé proposé peut être mis en œuvre selon un ou plusieurs modes de réalisation.

[0041] En référence à la [Fig.1], le système (1) comprend une plateforme matérielle (2) sur laquelle est mis en œuvre un environnement logiciel de virtualisation, par exemple d'une ou plusieurs fonctions réseau, comprenant une ou plusieurs machines virtuelles (3a, 3b, 3c) et un hyperviseur (4a) configuré pour piloter l'une ou plusieurs machines virtuelles (3a, 3b, 3c) qui ont été instanciées.

[0042] Le système (1) peut être configuré pour être intégré à un réseau de communication, et par exemple comprendre une plateforme généraliste de fourniture de services réseau destinée à être installée chez les clients d'un opérateur (uCPE). Une ou plusieurs des machines virtuelles peuvent mettre en œuvre des fonctions réseau virtualisées (VNF), comme par exemple une VNF X fournissant une fonction de routeur périphérique (en anglais, « edge router »), une VNF Y fournissant une fonction de sécurité pour le système informatique (1), et une VNF Z fournissant une fonction de stockage virtualisé. La flexibilité de l'architecture des équipements de type uCPE permettant le déploiement, la modification et la suppression à distance de VNFs, par exemple par le biais d'un réseau étendu (WAN), d'autres VNF peuvent être mis en œuvre au sein du système informatique (1) en fonction du mode de réalisation des procédés et équipements proposés.

[0043] La plateforme matérielle (2) comprend un ou plusieurs serveurs, comprenant chacun

un ou plusieurs processeurs et une ou plusieurs mémoires couplées de manière opérationnelle au(x) processeur(s) (non illustrés sur la figure), ainsi qu'une ou plusieurs interfaces physiques de communication de données (2a, 2b, 2c), comme par exemple des interfaces de format de type port Ethernet.

[0044] Certains des ports de communication (2a) peuvent être configurés pour des communications de données sur réseau local (ports « LAN Ge1/0 » à « LAN Ge1/7 »), tandis que d'autres ports de communication (2b, 2c) peuvent être configurés pour des communications de données sur réseau étendu (ports « Wan0 Eth port » et « Wan1 Eth port »).

[0045] Une ou plusieurs des machines virtuelles instanciées sur le système informatique (1) peuvent être configurées pour accéder à un ou plusieurs des ports de communications de données sur réseau local et/ou pour accéder à un ou plusieurs des ports de communications de données sur réseau étendu, éventuellement par l'intermédiaire d'une ou plusieurs unités de commutation réseau (en anglais, « switch »). Par exemple, comme illustré sur la figure, la VNF Y (3b) peut être configurée pour avoir accès à un ou plusieurs des ports de communications de données sur réseau local (2a), par l'intermédiaire d'une unité (5a) de communication réseau local (« lan-net 0 »), et pour avoir accès à un ou plusieurs des ports de communications de données sur réseau étendu, par l'intermédiaire d'une unité (5b) de commutation interne (« Glue-net0 ») effectuant la liaison réseau interne avec la VNF Z (3c) et d'une unité (5c) de commutation réseau étendu (« wan-net 1 »). De même, la VNF Z (3c) peut être configurée pour avoir accès à un ou plusieurs des ports de communications de données sur réseau étendu (2a), par l'intermédiaire de l'unité (5c) de communication réseau étendu (« wan-net 1 »), et pour avoir accès à un ou plusieurs des ports de communications de données sur réseau local, par l'intermédiaire de l'unité (5b) de commutation interne (« Glue-net0 ») et de l'unité (5a) de commutation réseau local (« lan-net 0 »).

[0046] Comme illustré sur la [Fig.1], l'environnement logiciel de virtualisation peut être mis en œuvre au sein du système informatique (1) selon une architecture en étoile, utilisant par exemple une unité logicielle de commutation (4b) fournissant une interface de communication de données entre chacune des machines virtuelles (3a, 3b, 3c) instanciées dans le système informatique (1) et l'hyperviseur (4a).

[0047] Un (2d) des ports de communication de la plateforme (2) est en outre configuré comme interface réseau de gestion de l'hyperviseur (4a) et pour permettre l'acheminement des flux d'administration des machines virtuelles via leurs interfaces réseau de gestion respectives.

[0048] On décrit ci-après des procédés de contrôle qui peuvent avantageusement être mis en œuvre dans un système informatique tel que celui (1) illustré sur la [Fig.1], dans un ou plusieurs modes de réalisation.

[0049] En référence à la [Fig.2], on envisage un système informatique comprenant au moins une machine virtuelle utilisateur pilotée par un hyperviseur formant un environnement logiciel virtualisé.

[0050] Dans un ou plusieurs modes de réalisation, une ou plusieurs des au moins une machine virtuelle utilisateur est configurée pour remplir une fonction réseau virtuel, comme par exemple une fonction de routage réseau, de communication de voix et/ou de données (par exemple une fonction voix sur réseau IP (VoIP), une fonction sécurité du réseau, ou une fonction stockage en réseau (par exemple une fonction de stockage de données virtualisé dans un environnement Cloud).

[0051] Dans un ou plusieurs modes de réalisation, le contrôle du système informatique peut être mis en œuvre par une unité de contrôle, par exemple une machine virtuelle (dite « machine virtuelle de contrôle ») pilotée par l'hyperviseur, connectée à l'au moins une machine virtuelle utilisateur par un lien de communication de données. Dans un ou plusieurs modes de réalisation dans lesquels plusieurs machines virtuelles utilisateurs ont été instanciées au sein du système informatique, l'unité de contrôle peut être connectée à chacune des machines virtuelles utilisateur par des liens de communication de données respectifs.

[0052] Dans un ou plusieurs modes de réalisation, le procédé proposé comprend la réception (11), depuis une machine virtuelle utilisateur, d'un paquet de données associé à un flux d'administration émis sur l'interface réseau de gestion de cette machine virtuelle. Ce paquet de données associé à un flux d'administration comprend un identifiant de réseau et une adresse physique. L'identifiant de réseau et l'adresse physique identifient la machine virtuelle utilisateur pour le réseau d'administration.

[0053] Par exemple, le paquet de données associé à un flux d'administration peut être reçu par l'unité de contrôle (par exemple par la machine virtuelle de contrôle) lors d'une configuration, par exemple par un utilisateur au moyen d'une interface homme-machine de configuration, d'une interface réseau de gestion de la machine virtuelle utilisateur.

[0054] L'homme du métier comprendra que les procédés et systèmes proposés ne sont pas limités à un ou plusieurs types de protocole de communication de données, d'identifiant de réseau ou d'adresse physique. Ainsi, en fonction du mode de réalisation choisi, les procédés et systèmes proposés peuvent être mis en œuvre en utilisant des paquets de données au format IP (pour « Internet Protocol »), des identifiants de réseau de type adresse IP, et des adresses physiques comprenant une adresse de contrôle d'accès au média (en anglais, « Medium Access Control » ou « MAC ») et/ou un numéro de port de communication. De même, en fonction du mode de réalisation choisi, le paquet de données peut être reçu dans un message d'un protocole de communication de données, comme par exemple le protocole HTTP (de l'anglais « HyperText

Transfer Protocol ») ou le protocole sécurisé HTTPS (de l'anglais « HyperText Transfer Protocol Secure »).

[0055] Dans un ou plusieurs modes de réalisation, l'unité de contrôle est configurée pour, sur réception du paquet de données, et lorsque l'identifiant de réseau est associé à une deuxième adresse physique différente de la première adresse physique, bloquer (12) le paquet de données.

[0056] En fonction du mode de réalisation, le blocage du paquet comprend une mise à l'écart du paquet (en anglais, « discard ») ou une suppression du paquet de données. Le blocage du paquet permet avantageusement de ne pas le transmettre à son destinataire, et ainsi d'éviter l'utilisation de l'identifiant de réseau et/ou de l'adresse physique d'une machine virtuelle utilisateur par une autre machine virtuelle utilisateur. On peut en outre utiliser un fichier d'anomalies dans lequel sont consignées des données (comprenant par exemple des données d'en-tête) de paquets de données bloqués selon le procédé proposé.

[0057] Dans un ou plusieurs modes de réalisation, l'adresse physique a été associée à l'identifiant de réseau dans le cadre de la configuration initiale de l'interface réseau de gestion de la machine virtuelle utilisateur effectuée en lien avec son instanciation dans le système informatique.

[0058] Le contrôle effectué sur le paquet de données reçu comprend la vérification que l'identifiant de réseau de l'interface réseau de gestion porté par le paquet de données est bien associé pour l'unité de contrôle (par exemple mise en œuvre dans une machine virtuelle de contrôle) à l'adresse physique de l'interface réseau de gestion portée par le paquet de données. Ceci permet de détecter une anomalie dans le trafic acheminé via le port de communication dédié 2d. Cette anomalie résulte par exemple d'une modification de l'adresse physique associée à un identifiant de réseau avec lequel la machine virtuelle utilisateur a été configurée pour l'interface réseau de gestion, ou bien encore d'une modification de l'identifiant de réseau associée à une adresse physique donnée avec laquelle la machine virtuelle utilisateur a été configurée pour cette interface réseau de gestion.

[0059] Ainsi, dans les cas où le paquet de données associé au flux d'administration d'une interface réseau de gestion de la machine virtuelle utilisateur est émis suite à une reconfiguration par un utilisateur, le procédé proposé permet avantageusement d'isoler cette machine virtuelle, et en particulier en bloquant le paquet de données émis afin d'éviter les disfonctionnements qui peuvent s'ensuivre. Le procédé proposé permet ainsi d'éviter une erreur de configuration d'une interface réseau de gestion d'une machine virtuelle, qui autrement conduirait par exemple à associer deux identifiants de réseau (par exemple deux adresses IP) d'interfaces réseau de gestion à une même adresse physique (par exemple une adresse MAC) d'interface réseau de gestion, ou

deux adresses physiques (par exemple deux adresses MAC) d'interfaces réseau de gestion à un même identifiant de réseau (par exemple une adresse IP) d'interface réseau de gestion.

[0060] Comme indiqué précédemment, cette tentative de reconfiguration de l'interface de gestion de la machine virtuelle utilisateur peut aussi être un acte malveillant, auquel cas le procédé proposé fournit avantageusement une stratégie de défense du système informatique.

[0061] Dans un ou plusieurs modes de réalisation, le procédé proposé est mis en œuvre pour chaque paquet associé à un flux d'administration émis par cette machine virtuelle.

[0062] Dans un ou plusieurs modes de réalisation, la détermination que l'identifiant de réseau est associé à une adresse physique différente de l'adresse physique mémorisée par l'unité de contrôle conduit à bloquer le trafic associé à un flux d'administration émis par la machine virtuelle utilisateur à l'origine de ce paquet de données. Par exemple, le procédé proposé comprend l'action de bloquer l'ensemble des paquets de données associés à un flux d'administration et émis par la machine virtuelle utilisateur identifiée par la première adresse physique.

[0063] Dans un ou plusieurs modes de réalisation, l'identifiant de réseau et l'adresse physique sont extraits du paquet de données reçu par l'unité de contrôle. Par exemple, dans les modes de réalisation dans lesquels le paquet reçu est un paquet IP, l'adresse IP du paquet et l'adresse MAC associée sont extraits de l'en-tête du paquet IP, et utilisés pour détecter toute anomalie dans le trafic du flux d'administration relatif à la machine virtuelle utilisateur.

[0064] En fonction du mode de réalisation, et notamment en fonction du type de système d'exploitation utilisé par la machine virtuelle utilisateur, la configuration d'une interface réseau de gestion de la machine virtuelle utilisateur peut utiliser toute commande appropriée de configuration d'interface réseau.

[0065] Par exemple, dans les modes de réalisation dans lesquels la machine virtuelle utilisateur utilise un système d'exploitation de type Linux, une commande de type « ifconfig » ou de type « ip » peut être utilisée pour attribuer une adresse physique à une interface réseau de gestion de la machine virtuelle utilisateur, et une commande de type « ip » peut être utilisée pour attribuer une adresse IP à une interface réseau de gestion de la machine virtuelle utilisateur.

[0066] Par exemple, la ligne de commande suivante peut être utilisée pour configurer ou reconfigurer (c'est-à-dire modifier) l'adresse MAC d'une interface réseau de gestion de la machine virtuelle utilisateur : ifconfig [interface] hw ether [nouvelle adresse_MAC].

[0067] Selon un premier type de cas d'usage, un administrateur du système informatique ou de la machine virtuelle utilisateur peut donc être amené à modifier la configuration d'une interface réseau de gestion d'une machine virtuelle utilisateur, par exemple en

modifiant l'identifiant de réseau, ce qui entraîne une modification de l'association identifiant de réseau / adresse physique établie lors d'une configuration précédente de l'interface réseau de gestion d'une machine virtuelle utilisateur. Selon un deuxième type de cas d'usage, une commande de modification de configuration de l'interface réseau de gestion d'une machine virtuelle utilisateur peut émaner d'un utilisateur malveillant cherchant à perturber, voire interrompre, le bon fonctionnement du système informatique ou à prendre le contrôle de la configuration de la machine virtuelle utilisateur.

[0068] La modification de la configuration de l'interface réseau de gestion d'une machine virtuelle utilisateur du système informatique peut conduire à la situation décrite ci-dessus dans laquelle deux interfaces réseau de gestion distinctes, parmi lesquelles l'interface réseau de gestion de la machine virtuelle utilisateur, utilisent un même identifiant de réseau (par exemple une même adresse IP) et/ou une même adresse physique (par exemple une même adresse MAC ou un même identifiant de port de communication). Cette situation présente le risque de bloquer l'interface réseau de gestion d'une autre machine virtuelle utilisateur, qui elle continue d'utiliser l'identifiant de réseau qui lui a été attribué, cette interface réseau de gestion devenant inaccessible.

[0069] Une tentative de modification de la configuration de l'interface réseau de gestion d'une machine virtuelle utilisateur du système informatique conduisant à cette situation est avantageusement détectée par le procédé proposé, le paquet de données reçu associé à un flux d'administration correspondant par exemple dans ce cas de figure à la tentative de modification de configuration de l'interface réseau étant testé puis bloqué. Le risque qu'une machine virtuelle du système informatique utilise par configuration de son interface réseau de gestion un identifiant de réseau (par exemple une adresse IP) et/ou une adresse physique (par exemple une adresse MAC) déjà attribué à une autre machine virtuelle ou à l'hyperviseur du système informatique est ainsi avantageusement atténué en empêchant cette situation de se produire.

[0070] Dans un ou plusieurs modes de réalisation, le procédé proposé peut comprendre, outre le blocage du paquet de données comprenant un identifiant de réseau et une adresse physique qui n'auraient pas dû être associés, la génération d'une alarme système, permettant avantageusement d'alerter un administrateur du système informatique d'une situation anormale de duplication d'identifiant de réseau au sein du système.

[0071] Dans un ou plusieurs modes de réalisation, l'unité de contrôle peut en outre être configurée pour bloquer le trafic de données émis par l'adresse physique incriminée, par exemple en coupant le port de communication correspondant à l'adresse MAC en cause.

[0072] Dans un ou plusieurs modes de réalisation, l'unité de contrôle est configurée pour gérer une table de correspondance stockée en mémoire du système informatique comprenant une liste d'identifiants de réseau et d'adresses physiques respectivement associés lors de la configuration des interfaces réseau de gestion utilisées par différentes entités logicielles du système informatique (comprenant par exemple l'hyperviseur et l'ensemble des machines virtuelles instanciées du système). Par exemple, la table de correspondance liste des associations adresse IP/adresse MAC/ port définies lors de la configuration d'entités logicielles correspondantes, et comprend pour chaque machine virtuelle hébergée au sein du système informatique une entrée indiquant une adresse IP, une adresse MAC et un port associés lors de la configuration de la machine virtuelle. Dans un mode de réalisation, la table de correspondance peut comprendre une liste d'identifiants de réseau et d'adresses physiques respectivement associés et certifiés, par exemple par un opérateur (par exemple dans les modes de réalisation dans lesquels l'identifiant de réseau est attribué pour une utilisation dans le système informatique de manière centralisée par un administrateur du système informatique), à partir de la configuration initiale de déploiement des entités logicielles (comme par exemple des machines virtuelles) hébergées au sein du système informatique.

[0073] En fonction du mode de réalisation, l'unité de contrôle peut être configurée pour générer la table de correspondance, la consulter et la modifier (pour par exemple la mettre à jour sur instanciation au sein du système informatique d'une nouvelle machine virtuelle ou sur suppression d'une machine virtuelle précédemment instanciée), pour la modifier et la consulter, ou uniquement pour la consulter. Dans un ou plusieurs modes de réalisation, la table de correspondance peut être générée et/ou modifiée par un processus automatique ou manuel (initialisation et/ou modification de la table par un utilisateur administrateur du système informatique), qui de préférence ne sera pas basé sur une découverte des configurations définies pour les entités logicielles du système informatique afin de se baser sur une source d'information certifiée.

[0074] Dans un ou plusieurs modes de réalisation, la table de correspondance peut être mise à jour sur instanciation d'une nouvelle machine virtuelle avec des données de configuration d'interface réseau de gestion utilisées pour la configuration de cette nouvelle machine virtuelle.

[0075] Dans un ou plusieurs modes de réalisation, l'unité de contrôle peut être configurée pour, sur réception du paquet de données associé à un flux d'administration, consulter la table de correspondance stockée en mémoire afin de déterminer par lecture de la table de correspondance si l'identifiant de réseau porté par le paquet de données est associé dans la table de correspondance à une autre adresse physique que celle portée par le paquet de données.

[0076] En référence à l'exemple d'architecture de système de la [Fig.1], l'unité de contrôle peut, dans un ou plusieurs modes de réalisation, être mise en œuvre au sein de l'unité logicielle de commutation (4b), tirant ainsi parti de l'architecture en étoile dans laquelle chacune des machines virtuelles (3a, 3b, 3c) instanciées dans le système informatique (1) est connectée à l'unité de commutation (4b), afin de permettre à l'unité de contrôle d'être connectée à chacune des machines virtuelles instanciées de manière à contrôler la configuration des interfaces réseau de gestion respectives de chacune de ces machines virtuelles.

[0077] La [Fig.3] illustre un exemple d'architecture de système informatique pour la mise en œuvre du procédé proposé selon un ou plusieurs modes de réalisation.

[0078] L'architecture du système informatique (1') de la [Fig.3] correspondant à celle du système (1) illustré sur la [Fig.1], on peut se référer à la description ci-dessus des éléments de la [Fig.1] pour une description plus détaillée des modes de réalisation du système informatique (1').

[0079] En référence à la [Fig.3], le système (1') comprend une plateforme matérielle (2') sur laquelle est mis en œuvre un environnement logiciel de virtualisation, par exemple d'une ou plusieurs fonctions réseau, comprenant une ou plusieurs machines virtuelles (3a', 3b', 3c') et un hyperviseur (4a') configuré pour piloter l'une ou plusieurs machines virtuelles (3a', 3b', 3c') qui ont été instanciées.

[0080] Le système (1') peut aussi être configuré pour être intégré à un réseau de communication, et par exemple comprendre une plateforme généraliste de fourniture de services réseau destinée à être installée chez les clients d'un opérateur (uCPE). Une ou plusieurs des machines virtuelles peuvent mettre en œuvre des fonctions réseau virtualisées (VNF).

[0081] La plateforme matérielle (2' du système informatique (1')) comprend un ou plusieurs serveurs, comprenant chacun un ou plusieurs processeurs et une ou plusieurs mémoires couplées de manière opérationnelle au(x) processeur(s) (non illustrés sur la figure), ainsi qu'une ou plusieurs interfaces physiques de communication de données (2a', 2b', 2c'), comme par exemples des interfaces de format de type port Ethernet.

[0082] Une ou plusieurs des machines virtuelles instanciées sur le système informatique (1') peuvent être configurées pour accéder à un ou plusieurs des ports de communications de données sur réseau local et/ou pour accéder à un ou plusieurs des ports de communications de données sur réseau étendu, éventuellement par l'intermédiaire d'une ou plusieurs unités de commutation réseau.

[0083] Comme illustré sur la [Fig.3], l'environnement logiciel de virtualisation peut être mis en œuvre au sein du système informatique (1') selon une architecture en étoile, utilisant par exemple une unité logicielle de commutation (4b') prévue pour fournir une interface de communication de données entre chacune des machines virtuelles

(3a', 3b', 3c') instanciées dans le système informatique (1') et l'hyperviseur (4a').

[0084] Un (2d') des ports de communication de la plateforme (2') est en outre configuré comme interface réseau de gestion de l'hyperviseur (4a') et pour permettre l'acheminement des flux d'administration des machines virtuelles via leurs interfaces réseau de gestion respectives.

[0085] La [Fig.3] illustre un exemple d'architecture de système informatique dans lequel l'unité de contrôle est mise en œuvre au sein d'une machine virtuelle de contrôle (6') configurée pour la mise en œuvre du procédé proposé selon un ou plusieurs modes de réalisation.

[0086] Dans un ou plusieurs modes de réalisation, la machine virtuelle de contrôle est configurée pour recevoir, en provenance d'une des machines virtuelles (3a', 3b', 3c') instanciées dans le système informatique (1'), un ou plusieurs paquets de données associés à un flux d'administration émis sur l'interface réseau de gestion de cette machine virtuelle (3a', 3b', 3c'). Par exemple, la machine virtuelle de contrôle (6') est configurée pour recevoir en entrée les paquets de données associés à un flux d'administration émis sur l'interface réseau de gestion de la machine virtuelle utilisateur (3a', 3b', ou 3c') qui sont dirigés vers l'unité logicielle de commutation (4b'), et pour transmettre en sortie ces paquets vers l'unité logicielle de commutation (4b') lorsqu'ils ne sont pas bloqués selon le procédé proposé.

[0087] Comme illustré sur la [Fig.3], dans un ou plusieurs modes de réalisation, la machine virtuelle de contrôle (6') peut être configurée pour recevoir en entrée les paquets de données associés à des flux d'administration respectifs émis sur une interface réseau de gestion respective et issus de plusieurs machines virtuelles utilisateur (3a', 3b', 3c'), voire de toutes les machines virtuelles utilisateur (3a', 3b', 3c') instanciées dans le système informatique (1'), qui sont dirigés vers l'unité logicielle de commutation (4b'), et pour transmettre en sortie ces paquets vers l'unité logicielle de commutation (4b') lorsqu'ils ne sont pas bloqués selon le procédé proposé.

[0088] Ainsi, dans un ou plusieurs modes de réalisation, la machine virtuelle de contrôle (6') peut être configurée pour recevoir en entrée les paquets de données associés à des flux d'administration respectifs émis sur une interface réseau de gestion respective et issus d'une ou de plusieurs machines virtuelles utilisateur (3a', 3b', 3c'), voire de toutes les machines virtuelles utilisateur (3a', 3b', 3c') instanciées dans le système informatique (1'), afin de contrôler ces paquets de données selon le procédé proposé.

[0089] En référence aux figures 1 et 3, la machine virtuelle de contrôle (6') peut ainsi être configurée pour contrôler que chaque interface réseau de gestion connectée dans l'architecture de la [Fig.1] à l'unité logicielle de commutation (4b) est bien configurée avec une interface de réseau unique dans le plan de gestion, et ne change pas (notamment suite à une modification d'identifiant de réseau (par exemple d'adresse IP)

et/ou d'adresse physique (par exemple d'adresse MAC)). Dans un ou plusieurs modes de réalisation, les interfaces réseau de gestion respectives des machines virtuelles utilisateurs sont connectées à la machine virtuelle de contrôle comme illustré sur la [Fig.3], et non plus à l'unité logicielle de commutation (4b) comme illustré sur la [Fig.1].

[0090] Dans un ou plusieurs modes de réalisation, la machine virtuelle de contrôle (6') sera instanciée préalablement à l'instanciation de toute machine virtuelle utilisateur (3a', 3b', 3c') dans le système informatique (1'), afin de permettre avantageusement la mise en œuvre du procédé proposé lors de l'instanciation de chaque nouvelle machine virtuelle utilisateur dans le système informatique (1'). Par exemple, la configuration initiale du système informatique (1') est renseignée, par exemple par un administrateur habilité (auquel cas l'identifiant de réseau est typiquement attribué pour une utilisation dans le système informatique de manière centralisée par l'administrateur du système informatique), et non pas détectée.

[0091] L'homme du métier comprendra que les procédés et systèmes proposés ne sont pas limités à un ou plusieurs types d'architecture logicielle et/ou matérielle du système informatique (1, 1'). En particulier, les procédés et systèmes proposés ne sont pas limités à un ou plusieurs types particuliers d'environnement logiciel de virtualisation, d'interfaces logicielles et/ou matérielles, ou de lien(s) de communication. De même, les procédés et systèmes proposés ne sont pas limités à un ou plusieurs types particuliers et/ou d'architecture(s) de réseau. Ainsi, en fonction du mode de réalisation choisi, les procédés et systèmes proposés peuvent être mis en œuvre avec des interfaces de communication de données permettant de connecter le système proposé à un réseau de communication de données par paquets (en anglais, « Packet Data Network », ou « PDN »), comme par exemple, un ou plusieurs réseaux IP interconnectés, dont par exemple le réseau Internet, ou une combinaison de plusieurs types de réseaux de communication de données comprenant un réseau de communication de données par paquets. De même, les procédés et systèmes proposés ne sont pas limités à un ou plusieurs types particuliers de protocole de communication de données ou de protocole de gestion de machine virtuelle.

[0092] L'homme du métier comprendra que les systèmes, équipements et unités proposés ne sont pas limités à une architecture particulière pour la mise en œuvre du procédé proposé.

[0093] En fonction du mode de réalisation choisi, certains actes, actions, évènements ou fonctions de chacune des méthodes décrites dans le présent document peuvent être effectués ou se produire selon un ordre différent de celui dans lequel ils ont été décrits, ou peuvent être ajoutés, fusionnés ou bien ne pas être effectués ou ne pas se produire, selon le cas. En outre, dans certains modes de réalisation, certains actes, actions ou

évènements sont effectués ou se produisent concurremment et non pas successivement.

[0094] Bien que décrits à travers un certain nombre d'exemples de réalisation détaillés, le procédé proposé et le dispositif pour la mise en œuvre d'un mode de réalisation du procédé comprennent différentes variantes, modifications et perfectionnements qui apparaîtront de façon évidente à l'homme de l'art, étant entendu que ces différentes variantes, modifications et perfectionnements font partie de la portée de l'invention, telle que définie par les revendications qui suivent. De plus, différents aspects et caractéristiques décrits ci-dessus peuvent être mis en œuvre ensemble, ou séparément, ou bien substitués les uns aux autres, et l'ensemble des différentes combinaisons et sous-combinaisons des aspects et caractéristiques font partie de la portée de l'invention. En outre, il se peut que certains systèmes et équipements décrits ci-dessus n'incorporent pas la totalité des modules et fonctions décrits pour les modes de réalisation préférés.

# Revendications

[Revendication 1] Procédé de contrôle dans un système informatique comprenant au moins une machine virtuelle utilisateur pilotée par un hyperviseur et une unité de contrôle, ledit procédé mis en œuvre par l'unité de contrôle, comprenant :
recevoir d'une machine virtuelle utilisateur un paquet de données associé à un flux d'administration émis sur une interface de réseau de gestion de ladite machine virtuelle, ledit paquet de données comprenant un identifiant de réseau et une première adresse physique identifiant la machine virtuelle utilisateur ; et
lorsque l'identifiant de réseau est associé à une deuxième adresse physique différente de la première adresse physique, bloquer le paquet de données.

[Revendication 2] Procédé selon la revendication 1, mis en œuvre par une machine virtuelle de contrôle pilotée par l'hyperviseur et comprise dans l'unité de contrôle.

[Revendication 3] Procédé selon l'une quelconque des revendications précédentes, dans lequel la deuxième adresse physique est stockée en association avec l'identifiant de réseau dans une table de correspondance, le procédé comprenant en outre : déterminer que l'identifiant de réseau est associé à la deuxième adresse physique par lecture de la table.

[Revendication 4] Procédé selon l'une quelconque des revendications précédentes, comprenant en outre : générer une alarme de duplication d'identifiant de réseau au sein du système informatique.

[Revendication 5] Procédé selon l'une quelconque des revendications précédentes, dans lequel l'adresse physique comprend une adresse MAC et/ou un numéro de port.

[Revendication 6] Procédé selon l'une quelconque des revendications précédentes, dans lequel l'identifiant de réseau comprend une adresse IP.

[Revendication 7] Procédé selon l'une quelconque des revendications précédentes, dans lequel l'identifiant de réseau est associé à la deuxième adresse physique sur instanciation de la machine virtuelle utilisateur au sein du système informatique.

[Revendication 8] Procédé selon l'une quelconque des revendications précédentes, comprenant en outre : extraire l'identifiant de réseau et la première adresse physique du paquet de données reçu.

[Revendication 9] Procédé selon l'une quelconque des revendications précédentes,

comprenant en outre : instancier la machine virtuelle de contrôle à partir d'une configuration initiale du système informatique ne comprenant aucune machine virtuelle utilisateur.

[Revendication 10] Système informatique comprenant une unité de traitement comprenant un processeur et une mémoire couplée de manière opérationnelle au processeur, au moins une machine virtuelle utilisateur pilotée par un hyperviseur et une unité de contrôle, l'unité de traitement étant configurée pour la mise en œuvre, par l'unité de contrôle, d'un procédé selon l'une quelconque des revendications 1 à 9.

[Revendication 11] Programme d'ordinateur, chargeable dans une mémoire associée à un processeur, et comprenant des portions de code pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 9 lors de l'exécution dudit programme par le processeur.

[Fig. 1]

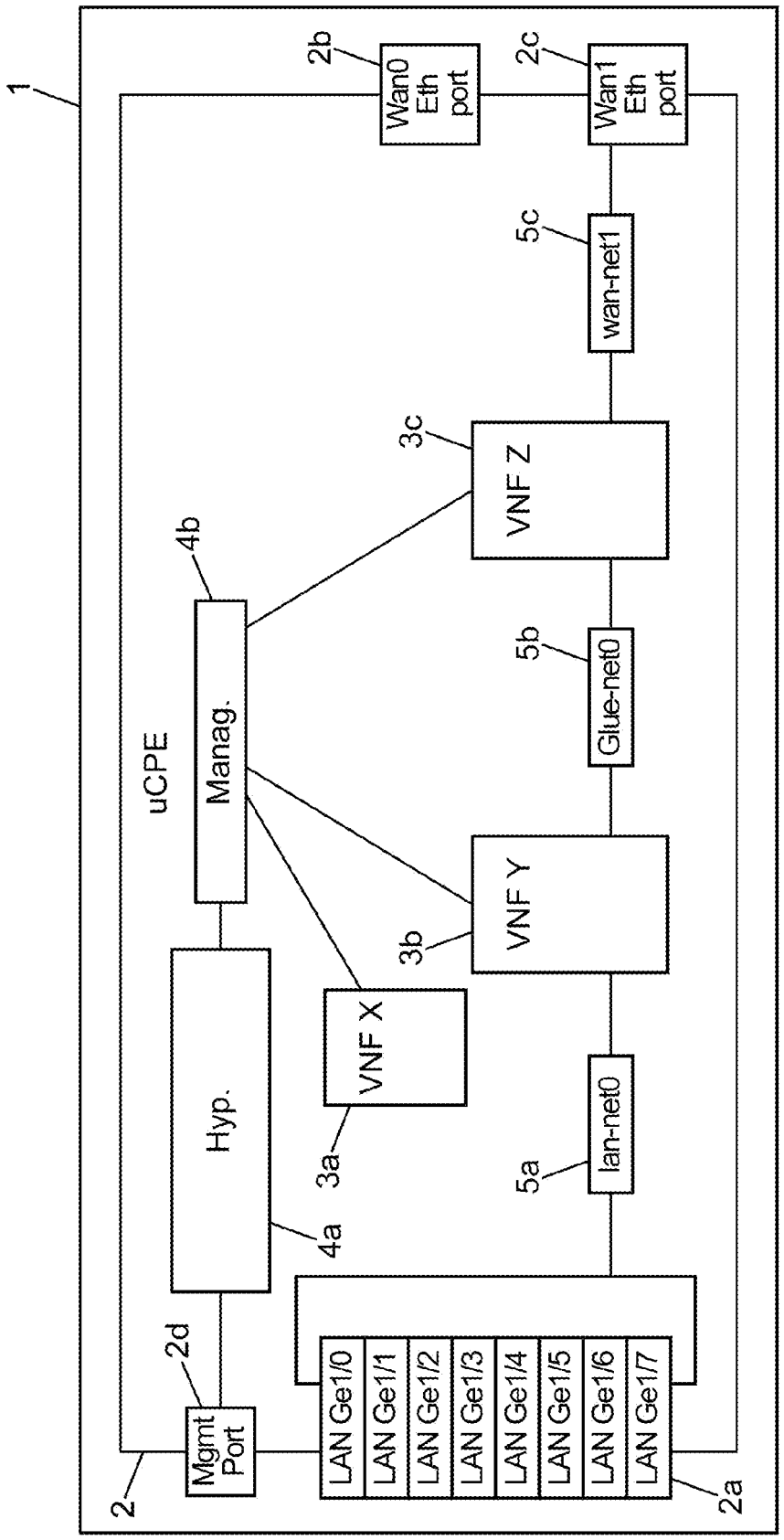
1
2
2a
2b
2c
2d
Wan0 Eth port
Wan1 Eth port
Mgmt Port
LAN Ge1/0
LAN Ge1/1
LAN Ge1/2
LAN Ge1/3
LAN Ge1/4
LAN Ge1/5
LAN Ge1/6
LAN Ge1/7
uCPE
Manag.
Hyp.
VNF X
VNF Y
VNF Z
3a
3b
3c
4a
4b
lan-net0
Glue-net0
wan-net1
5a
5b
5c

FIG. 1

[Fig. 2]

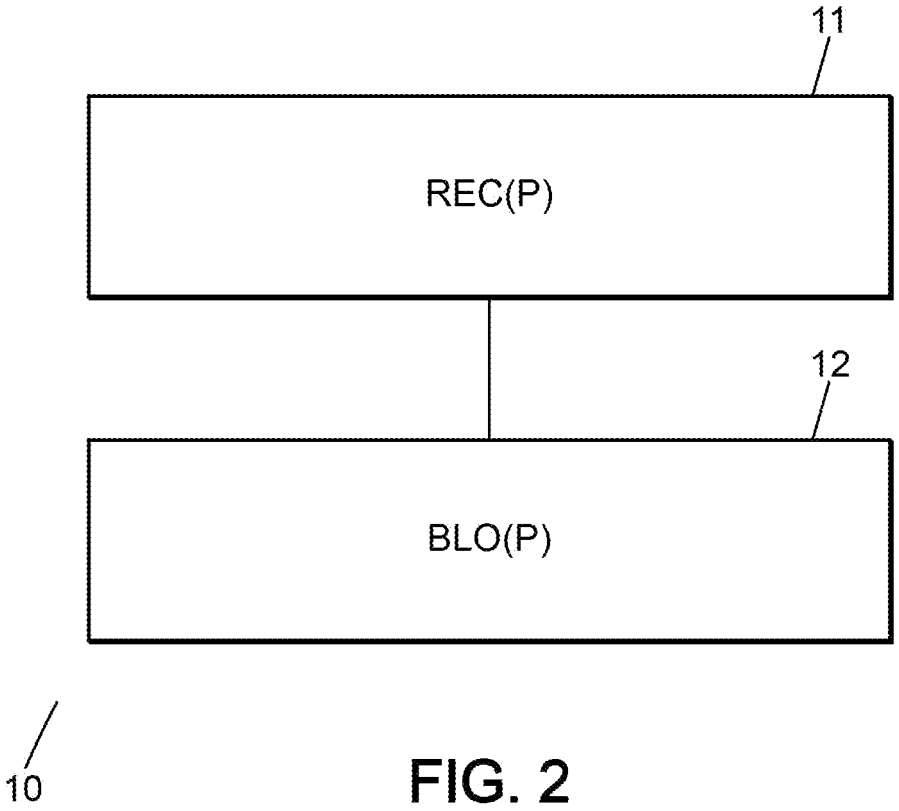


FIG. 2

[Fig. 3]

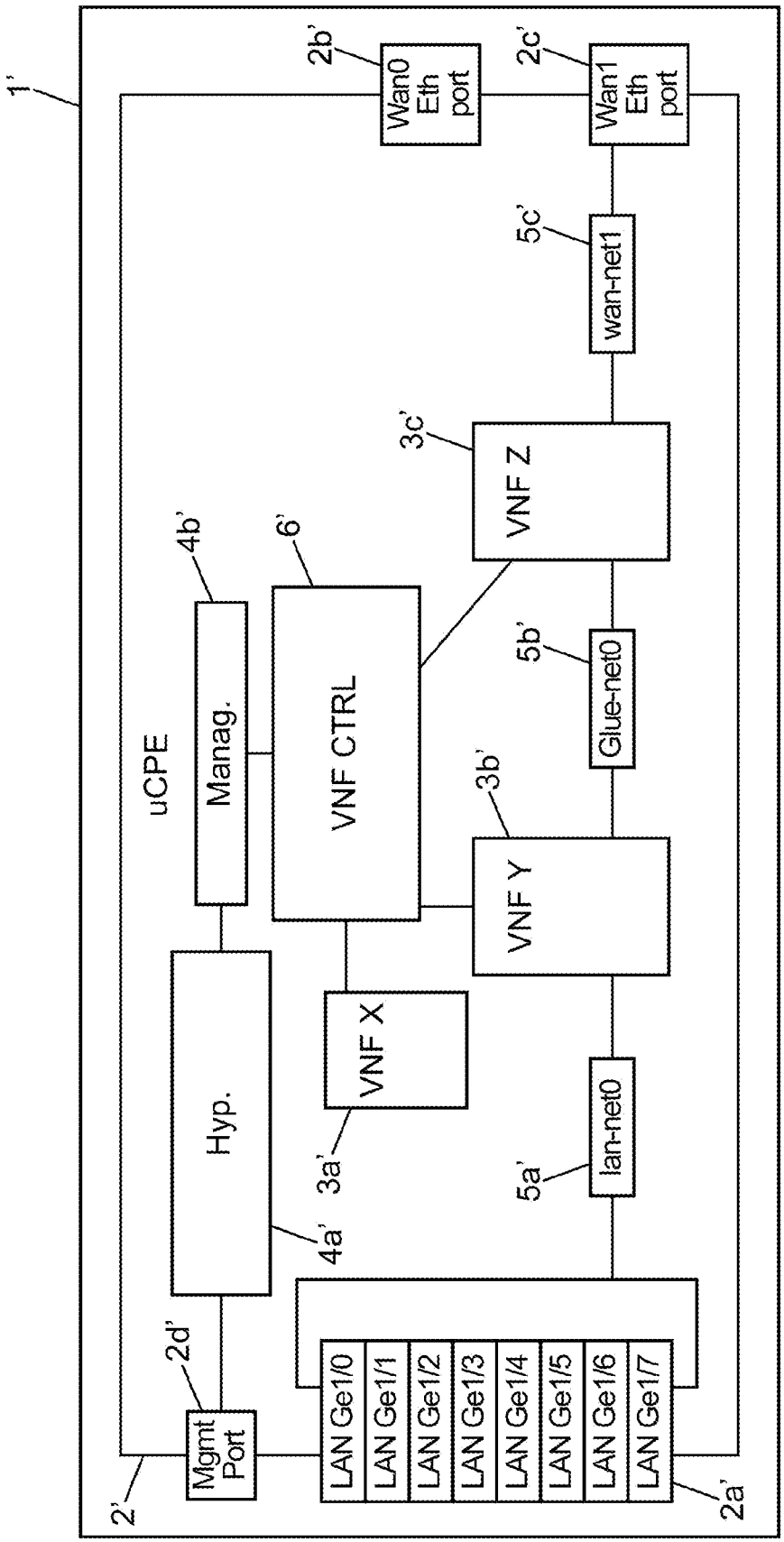
1'
2'
2a'
2b'
2c'
2d'
3a'
3b'
3c'
4a'
4b'
5a'
5b'
5c'
6'
uCPE
Wan0 Eth port
Wan1 Eth port
wan-net1
VNF Z
VNF CTRL
Manag.
Glue-net0
VNF Y
VNF X
Hyp.
lan-net0
Mgmt Port
LAN Ge1/0
LAN Ge1/1
LAN Ge1/2
LAN Ge1/3
LAN Ge1/4
LAN Ge1/5
LAN Ge1/6
LAN Ge1/7

FIG. 3

# RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

## OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

## CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

[x] Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

## DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

[x] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

**1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION**

US 2015/281274 A1 (MASUREKAR UDAY [US] ET AL) 1 octobre 2015 (2015-10-01)

**2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL**

US 2020/280537 A1 (ALAPATI RISHI KANTH [US] ET AL) 3 septembre 2020 (2020-09-03)

US 2014/044134 A1 (RAJAMANICKAM SUPRIYA [IN] ET AL) 13 février 2014 (2014-02-13)

US 2015/095505 A1 (ANTONY JINTO [IN]) 2 avril 2015 (2015-04-02)

WO 2014/203113 A1 (ERICSSON TELEFON AB L M [SE]; QIANG ZU [CA]) 24 décembre 2014 (2014-12-24)

**3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES**

NEANT