(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 890 268 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.10.2021 Bulletin 2021/40

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(21) Application number: **21162173.5**

(22) Date of filing: **12.10.2016**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **13.10.2015 US 201514881649**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
16788322.2 / 3 363 176

(71) Applicant: **Cisco Technology, Inc.**
San Jose, CA 95134 (US)

(72) Inventors:
- **ARREGOCES, Mauricio**
  San Jose, California 95134 (US)
- **BAGEPALLI, Nagaraj**
  San Jose, California 95134 (US)
- **CHANDRASEKARAN, Subramanian**
  San Jose, California 95134 (US)

(74) Representative: **Coates, Robert James Patterson**
Kilburn & Strode LLP
Lacon London
84 Theobalds Road
London WC1X 8NL (GB)

Remarks:
This application was filed on 11-03-2021 as a divisional application to the application mentioned under INID code 62.

(54) HYBRID CLOUD SECURITY GROUPS

(57) In one embodiment, a request may be received from a first cloud network of a hybrid cloud environment to transmit data to a second cloud network of the hybrid cloud environment, wherein the request can include a security profile related to the data. The security profile may be automatically analysed to determine access permissions related to the data. Based at least in part on the access permissions, data can be allowed to access to the second cloud network.

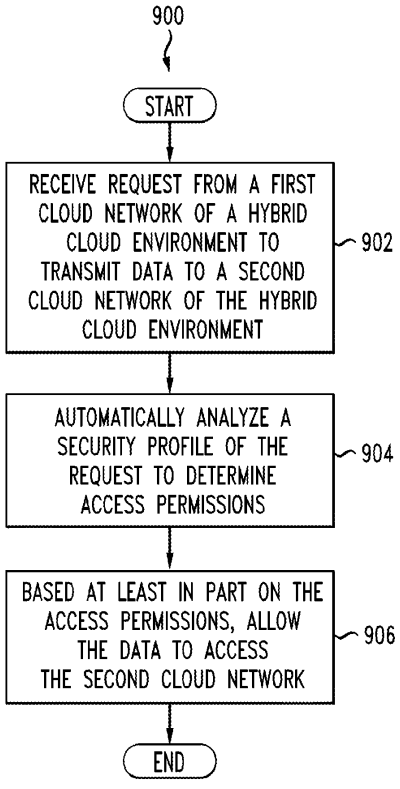

FIG. 9

EP 3 890 268 A1

Description

TECHNICAL FIELD

[0001] The present technology pertains to computer-based networking, and more specifically, to security groups in a hybrid cloud environment.

BACKGROUND

[0002] Recent industry-wide shifts toward cloud-based service delivery and data consumption present new challenges for service providers to route and deliver data while providing security for data stored in private cloud databases. For example, cloud-based providers may employ various real-time adjustment models to efficiently adapt and allocate network resources based on changing security needs. Furthermore, a hybrid cloud computing and storage environment can present added challenges for network security as some portions of a hybrid cloud computing and storage environment may be accessible to a public forum and other portions of a hybrid cloud may be designated for a private forum.

[0003] A hybrid cloud computing environment can be a target for unauthorized access to data stored in the hybrid cloud as potential security threats may attempt to penetrate vulnerabilities that can be associated with a hybrid cloud computing and storage environment. Emerging computer-based threats are accelerating a need for increasingly flexible and secure network operations. As data, software, services, applications, and databases are increasingly tied to cloud-based networks, added security functionality and flexibility is desired in cloud-based computing environments, including hybrid cloud computing and storage environments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] In order to describe the manner in which the above-recited features and other advantages of the disclosure can be obtained, a more particular description of the principles briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only exemplary embodiments of the disclosure and are not therefore to be considered to be limiting its scope, the principles herein are described and explained with additional specificity and detail through the use of the accompanying drawings in which:

FIG. 1 illustrates an example hybrid cloud environment;
FIG. 2 illustrates an example of migrating a virtual machine in a hybrid cloud environment;
FIG. 3 illustrates an example hybrid cloud environment with multiple cloud networks;
FIG. 4 illustrates an example hybrid cloud environment utilizing cloud security groups;
FIG. 5 illustrates an example hybrid cloud environment utilizing cloud security groups;
FIG. 6 illustrates an example hybrid cloud environment utilizing cloud security groups;
FIG. 7 illustrates an example hybrid cloud environment utilizing cloud security groups;
FIG. 8 illustrates an example hybrid cloud environment utilizing cloud security groups;
FIG. 9 illustrates an example process of the present technology; and
FIG. 10 illustrates an example architecture of the present technology.

[0005] A component or a feature that is common to more than one drawing is indicated with the same reference number in each of the drawings.

DESCRIPTION OF EXAMPLE EMBODIMENTS

[0006] Various embodiments of the disclosure are discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without parting from the spirit and scope of the disclosure.

Overview

[0007] In some embodiments, the present technology may receive a request from a first cloud network of a hybrid cloud environment to transmit data to a second cloud network of the hybrid cloud environment, wherein the request may include a security profile related to the data. The security profile can be automatically analyzed to determine access permissions related to the data. Moreover, based at least in part on the access permissions, the data may be allowed to access to the second cloud network.

Description

[0008] A communication network can include a system of hardware, software, protocols, and transmission components that collectively allow separate devices to communicate, share data, and access resources, such as software applications. More specifically, a computer network may be a geographically distributed collection of nodes interconnected by communication links and segments for transporting data between end points, such as personal computers, portable devices, and workstations. Many types of networks are available, ranging from local area networks (LANs) and wide area networks (WANs) to overlay and software-defined networks, such as virtual extensible local area networks (VXLANs), and virtual networks such as virtual LANs (VLANs) and virtual private networks (VPNs).

[0009] LANs may connect nodes over dedicated pri-

vate communications links located in the same general physical location, such as a building or campus. WANs, on the other hand, may connect geographically dispersed nodes over long-distance communications links, such as common carrier telephone lines, optical lightpaths, synchronous optical networks (SONET), or synchronous digital hierarchy (SDH) links. LANs and WANs can include layer 2 (L2) and/or layer 3 (L3) networks and devices.

[0010] The Internet is an example of a public WAN that connects disparate networks throughout the world, providing global communication between nodes on various networks. The nodes can communicate over the network by exchanging discrete frames or packets of data according to predefined protocols, such as the Transmission Control Protocol/Internet Protocol (TCP/IP). In this context, a protocol can refer to a set of rules defining how the nodes interact with each other. Computer networks may be further interconnected by intermediate network nodes, such as routers, switches, hubs, or access points, which can effectively extend the size or footprint of the network.

[0011] Networks can be segmented into sub-networks to provide a hierarchical, multilevel routing structure. For example, a network can be segmented into VLAN sub-networks using subnet addressing to create network segments. This way, a network can allocate various groups of IP addresses to specific network segments and divide the network into multiple logical networks. In a hybrid cloud environment, different sub-networks may be allocated to different parts of the hybrid cloud environment. For example, one or more VLAN sub-networks may be allocated to a private cloud network of the hybrid cloud environment and a public cloud network of the hybrid cloud environment based on security permissions associated with the one or more VLAN sub-networks.

[0012] Other networks, such as virtual networks (e.g., VLANs) are also available. For example, one or more LANs can be logically segmented to form a VLAN and allow a group of machines to communicate as if they were in the same physical network, regardless of their actual physical location. Thus, machines located on different physical LANs can communicate as if they were located on the same physical LAN. Interconnections between networks and devices can also be created using routers and tunnels, such as VPN tunnels, as is appreciated by those skilled in the art. In a hybrid cloud computing environment, such a tunnel may include encryption and/or firewalls at either end of the tunnel to serve as a gatekeeper for data transmitted between a private data center (DC)/private cloud network and a public cloud network such as a cloud network provided by a commercial entity. Example public cloud networks are the Microsoft Azure® Cloud, Amazon Web Services®, Oracle® Cloud, and the like.

[0013] The various networks can include various hardware or software appliances or nodes to support data communications, security, and provision services. For example, networks can include routers, hubs, switches, APs, firewalls, repeaters, intrusion detectors, servers, VMs, load balancers, application delivery controllers (ADCs), and other hardware or software appliances. Such appliances can be distributed or deployed over one or more physical, overlay, or logical networks. Moreover, appliances can be deployed as clusters, which can be formed using layer 2 (L2) and layer 3 (L3) technologies. Clusters can provide high availability, redundancy, and load balancing for flows associated with specific appliances or nodes. A flow can include packets that have the same source and destination information. Thus, packets originating from device A to service node B can all be part of the same flow.

[0014] Appliances or nodes, as well as clusters, can be implemented in cloud deployments. Cloud deployments can be provided in one or more networks to provision computing services using shared resources. Cloud computing can generally include Internet-based computing in which computing resources are dynamically provisioned and allocated to client or user computers or other devices on-demand, from a collection of resources available via the network (*e.g.*, "the cloud"). Cloud computing resources, for example, can include any type of resource, such as computing, storage, network devices, applications, virtual machines (VMs), services, and so forth. For instance, resources may include service devices (firewalls, deep packet inspectors, traffic monitors, load balancers, etc.), compute/processing devices (servers, CPU's, memory, brute force processing capability), storage devices (*e.g.*, network attached storages, storage area network devices), etc. In addition, such resources may be used to support virtual networks, virtual machines (VM), databases, applications (Apps), etc. Also, services may include various types of services, such as monitoring services, management services, communication services, data services, bandwidth services, routing services, configuration services, wireless services, architecture services, etc.

[0015] Cloud controllers and/or other cloud devices can be configured for cloud management. These devices can be pre-configured (i.e., come "out of the box") with centralized management, layer 7 (L7) device and application visibility, real time web-based diagnostics, monitoring, reporting, management, and so forth. As such, in some embodiments, the cloud can provide centralized management, visibility, monitoring, diagnostics, reporting, configuration (e.g., wireless, network, device, or protocol configuration), traffic distribution or redistribution, backup, disaster recovery, control, and any other service. In some cases, this can be done without the cost and complexity of specific appliances or overlay management software.

[0016] The present technology may address a need in the art for added security in hybrid cloud computing and storage environments ("hybrid cloud"). A hybrid cloud can refer to a cloud network architecture comprised of two or more cloud networks that communicate and/or

share data. A hybrid cloud can be an interaction between private and public clouds where a private cloud connects to a public cloud and utilizes public cloud resources in a secure and scalable way. The hybrid cloud model can provide advantages over other cloud models. For example, the hybrid cloud model allows enterprises to protect their existing investment, maintain control of their sensitive data and applications, and maintain control of their network, processing, and storage resources. Additionally, hybrid clouds may allow enterprises to scale their environment as their demand for processing resources and storage increase or decrease. This scaling up or down can occur with minimal to no effect on existing physical network resources such as on-site, physical servers.

[0017] While some applications are suitable for traditional physical enterprise data centers/private networks, there are others whose dynamic compute requirements make them ideal for cloud-based deployment. For such applications, a goal is to take advantage of the computing elasticity and economics of cloud computing without sacrificing the security that data assets (e.g., databases, directories, repositories) gain from being located on site within an enterprise's data center. To be a viable hybrid cloud solution, data should be kept secure, applications should not need to be redesigned, and cloud networks should be readily mobile.

[0018] **FIG. 1** illustrates an example hybrid cloud computing and storage network illustratively comprising a plurality of cloud networks or "clouds," including a private cloud 105 (e.g., enterprise data centers) and a public cloud 110 which may be utilized in a publicly-accessible network such as the Internet (not shown). Although current terminology refers to a hybrid cloud comprising a private cloud and a public cloud, it should be understood that many aspects of this disclosure can be practiced in various multi-cloud configurations (e.g., two clouds hosted by third party providers or two enterprise clouds in different locations). The private data center/private cloud 105 and public cloud 110 can be connected via a communication link 170 between private cloud gateway 125 and public cloud gateway 135. Data packets and traffic can be exchanged among the devices of the hybrid cloud network using predefined network communication protocols as will be understood by those skilled in the art.

[0019] As depicted in FIG. 1, each cloud network can have a cloud gateway such as private cloud gateway 125 and public cloud gateway 135. Each cloud network may also contain at least one virtual machine (VM) and/or nested VM containers. For example, FIG. 1 illustrates VM1 150 and VM2 152 in private cloud 105 and VM3 154 in public cloud 110. Private cloud gateway 125 can be configured as a VM-based gateway running in private cloud 105 that may be responsible for establishing communication link 170 for communication and data transfer between private cloud 105 and public cloud 110. Moreover, public cloud gateway 135 may be configured as a VM-based gateway running in public cloud 110 that can be responsible for establishing communication link 170 for communication and data transfer between private cloud 105 and public cloud 110.

[0020] Moreover, security group tags associated with private cloud gateway 125 and public cloud gateway 135 can enhance hybrid cloud network security by preventing data from reaching unauthorized areas of the hybrid cloud or preventing data from leaving areas of the hybrid cloud which the data is restricted to. In some embodiments, private cloud gateway 125 can screen requests for data stored in private cloud 105 destined for public cloud 110 by utilizing security group tags associated with, for example, sub-net VLANs from public cloud 110 that are authorized to receive data from private cloud 105 by virtue of access permissions associated with the sub-net VLANs from public cloud 110. This can prevent unauthorized data from leaving private cloud 105 by denying a request for data in private cloud 105 if, for example, the sub-net VLAN from public cloud 110 that makes the request does not have a security tag with access permissions to the requested data in private cloud 105.

[0021] Likewise, in some embodiments, public cloud gateway 135 can screen requests for data stored in public cloud 110 destined for private cloud 105 by utilizing security group tags associated with, for example, sub-net VLANs from public cloud 110 that are authorized to receive data from private cloud 105 by virtue of access permissions associated with the sub-net VLANs from public cloud 110. This can prevent unauthorized data from leaving public cloud 110 by not allowing the requested data from public cloud 110 to leave public cloud 110 if, for example, the sub-net VLAN from public cloud 110 related to the requested data does not have a security tag with access permissions to private cloud 105.

[0022] In some embodiments, one or more firewalls may be used in conjunction with private cloud gateway 125 and public cloud gateway 135 to facilitate screening of requests for entry and exit from private cloud 105 and public cloud 110. For example, private cloud gateway 125 and public cloud gateway 135 may complement each other by preventing entry of unauthorized data into their respective cloud networks and also preventing data from leaving their respective cloud networks if that data was not authorized to leave the cloud network due to insufficient access permissions for an intended destination (for example, a different cloud network of the hybrid cloud environment). In some embodiments, private cloud gateway 125 and public cloud gateway 135 may only prevent entry of unauthorized data into their cloud networks. In other embodiments, private cloud gateway 125 and public cloud gateway 135 may only prevent unauthorized data from leaving their respective cloud networks.

[0023] FIG. 1 also illustrates a hybrid cloud manager 175 within the private cloud 105 which can be a management plane VM for auto-provisioning resources within the hybrid cloud environment. Specifically, the hybrid cloud manager 175 may be a management platform (which could be a VM) operating in private cloud 105 or public cloud 110 (not shown), and may be generally responsible

for providing the hybrid cloud environment operations, translating between private cloud network and public cloud network interfaces, management of cloud resources, dynamic instantiating of cloud gateways and cloud VM components (for example, VM3 154 in public cloud 110) through, for example, the private virtualization platform and public cloud provider APIs. It may also health-monitor the components of the hybrid cloud environment (e.g., the cloud gateways, the one or more private application VMs, and the communication link 170, and provide high availability of those components.

[0024] FIG. 1 also illustrates a virtual supervisor module 130 (for example, the Nexus 1000V Switch by Cisco Systems, Inc.), a hypervisor 140 (also called a virtual machine manager) and one or more VM 150, 152. The virtual supervisor module 130 in the private cloud 105 can be used to create VMs in the public cloud 110 or private cloud 105, such as VM1 150, VM2 152, and VM3 154. Each VM can host a private application, even VM3 154 in the public cloud 110 can host a private application such that VM3 154 in the public cloud 110 executes as if it were within the private cloud 105. The hypervisor 140 can be configured by the virtual supervisor module 130 and may provide an operating system for one or more VMs.

[0025] FIG. 1 also illustrates communication link 170. Communication link 170 can take several forms to include a type of virtual private network (VPN) or a tunnel. Specifically, some embodiments may utilize an open VPN overlay or else an IP security (IPSec) VPN based L3 network extension to provide communication link 170. While offering secure transport connections in a cloud environment, a VPN may not provide a switch infrastructure for providing features such as switching network traffic locally at the cloud, providing consistent enterprise network polices, allowing insertion of various network services (e.g., load balancers, firewalls, etc.), and construction of a sophisticated network topology (e.g., the current systems are connected through a router and multiple VLANs). While IPsec-VPN-based technology can provide customers inter-datacenter network connectivity and relatively sophisticated network topologies, it can only extend the enterprise network at the network layer (Layer 3 or "L3" of the illustrative and well-known OSI model). This implies that the overlay networks created at the cloud datacenter (public cloud 110) can be a set of new subnets, where VMs in the public cloud are assigned with new network identities (e.g., IP and MAC addresses). Because of this, many enterprise infrastructures (e.g., access control lists, firewall policies, domain name services, etc.) can be modified in order for the newly attached VM systems to be able to work with rest of the enterprise systems. For example, the IPSec VPN tunnel may prevent penetration of corporate firewalls and Network Address Translation (NAT) devices deep within the enterprise data center (for example, private cloud 105).

[0026] Some hybrid cloud technologies, such as embodiments of the presently described technology, can utilize a secure transport layer (e.g., Layer 4 or "L4") tunnel as the communication link 170 between a first cloud gateway 125 in a private cloud 105 and a second cloud gateway 135 in a public cloud 110, where the secure transport layer tunnel is configured to provide a link layer 170 (e.g., Layer 2 or "L2") network extension between the private cloud and the public cloud. By establishing a secure transport layer (L4) tunnel 170 (e.g., transport layer security (TLS), datagram TLS (DTLS), secure socket layer (SSL), etc.) over the public cloud network 110, the techniques herein may build a secure L2 switch overlay that interconnects cloud resources (public cloud 110) with private cloud 105 (e.g., enterprise network backbones). In other words, the secure transport layer tunnel 170 can provide a link layer network extension between the private cloud 105 and the public cloud 110.

[0027] As noted, the cloud gateway 125 deployed at the private cloud 105 can use an L4 Secure Tunnel to connect to the cloud resources allocated at public cloud 110. The L4 secure tunnel is well-suited for use with corporate firewalls and NAT devices due to the nature of the transport level protocols (e.g., UDP/TCP) and the transport layer ports opened for HTTP/HTTPS in the firewall. The L2 network may extend and connect to each of the cloud VMs, e.g., VM1 150, VM2 152, VM3 154 through the cloud gateway 135 deployed at the public cloud 110. With an L2 network overlay, all instances of a particular private application VM, e.g, VM3 154 can be seamlessly migrated to the overlay network dynamically created at the public cloud, without any impacts to the existing corporate infrastructure.

[0028] As a general practice, a public cloud service provider offers only a limited number of network attachments for each of the cloud VMs, e.g., VM3 154, and network broadcasting capability. This can prevent enterprise customers from migrating their multi-VLAN network architectural environment into the public cloud datacenter. However, building an L2 network overlay on top of L4 tunnels as described herein reduces the network attachments requirements for cloud VMs and may provide cloud VMs with network broadcasting ability. The techniques herein can allow enterprise customers to deploy consistent enterprise-wide network architectures, even in a hybrid cloud network environment.

[0029] **FIG. 2** illustrates a hybrid cloud environment as illustrated in FIG. 1 being used to migrate a VM from private cloud 105 to public cloud 110. In some embodiments, a VM on the private cloud may need to be scaled beyond the current resources of the private cloud or the private cloud may need to be taken off line for a period of time. In some embodiments, it can be desirable to migrate an application on the private cloud 105 to the public cloud 110 or from public cloud 110 to private cloud 105 (not shown). FIG. 2 illustrates VM1 150 on private cloud 105 being migrated to public cloud 110. Migration can be managed using virtual supervisor module 130 to take VM1 150 offline, and may be migrated using hybrid cloud

manager 175 to copy the VM1 150 disk image to public cloud 110, and instantiate it in the public cloud 110.

[0030] **FIG. 3** illustrates an example hybrid cloud environment. In FIG. 3, a public cloud 114 can be running, for example, an application or service in VM4 156. The application or service can be shared by the enterprise private cloud 105 and partner private cloud 112. In some embodiments, private cloud 114 can act as an intermediary that provides limited access to the enterprise and the partner. It should be understood that many other hybrid cloud network architectures may be utilized besides the example architecture of FIG. 3. In some embodiments, a hybrid cloud network may include one or more enterprise private clouds, one or more physical enterprise servers, one or more public clouds, one or more physical public network servers, or any combination of such clouds and servers. In addition, embodiments of the present technology can provide for the secure migration of data, virtual machines, etc. among all of the different cloud networks (public and private) and physical servers in a hybrid cloud computing environment. For example, VM4 156 may be migrated to enterprise private cloud 105 and/or partner private cloud 112. Likewise, some embodiments can provide for the migration of, for example, VM3 to enterprise private cloud 105 and/or public cloud 114.

[0031] **FIG. 4** illustrates an example hybrid cloud environment. Data Center (DC)/private cloud 402 may be connected to provider/public cloud 412 via secure communication link 418. Private cloud 402 can be a cloud-based network designated for a particular enterprise. Private cloud 402 may contain sensitive data that is not intended to be shared outside of private cloud 402 without authorized access. Provider cloud 412 may be a publicly-accessible cloud-based network that is provided by a third party commercial vendor such as Oracle®, Amazon®, Microsoft®, etc. Item 404 represents one of many sub-nets, VLAN sub-nets, virtual machines, or other data that can be stored in data center/private cloud 402. Likewise, item 414 represents one of many sub-nets, VLAN sub-nets, virtual machines, or other data that can be stored in provider cloud 412. Items 406 and 416 can represent enforcements points for security policies/hybrid cloud security groups which may dictate the entry and exit of data/applications/VMs from private cloud 402 and provider/public cloud 412.

[0032] For example, items 406 and 416 may be gateways which are utilized to enforce hybrid cloud security groups/security policies. Hybrid cloud security groups can be automatically applied to data/applications/VMs that appear in the hybrid cloud network so that the data/applications/VMs are grouped according to authorized hybrid cloud access locations. For instance, an application represented by item 404 may be requested for migration to provider cloud 412. If VM 404 does not have the appropriate security group tag to exit private cloud 402 and enter provider cloud 412, gateway 406 can prevent VM 404 from leaving private cloud 402.

[0033] If VM 404 does have the appropriate security group tag to exit private cloud 402 and enter provider cloud 412, gateway 406 can allow VM 404 to leave private cloud 402 via secure link/tunnel 418. VM 404 may also have its data copied and instantiated in provider/public cloud 412 in some embodiments. Gateway 416 can act as a gatekeeper, in some embodiments only permitting data from an authorized security group to enter provider/public cloud 412. Secure link 418 may be secured with cryptography such that the communications between private cloud 402 and public cloud 412 are not detectable to outside parties. Furthermore, in some embodiments, secure link/secure tunnel 418 may not allow access to or from the Internet in order to enhance security by transmitting all sensitive data/applications/VMs via secure link 418 only.

[0034] Hybrid cloud security groups may be configured manually by an administrator of the private cloud 402 and/or public cloud 412. For instance, an administrator of private cloud 402 may configure the present technology to automatically apply security group tags to data/applications/VMs on the basis of, for example, origin IP address, type, author, date created, etc. Upon instantiation of an embodiment of the present technology, all or some of the data/applications/VMs may be assigned to one or more cloud security groups. For example, some data/applications/VMs can be authorized for use by the private cloud, the public cloud only, or both the private and public clouds. This can allow for greater flexibility of movement of data inside a particular cloud environment while preserving security because all data that has a cloud security group tag should only be permitted in authorized areas associated with their respective cloud security group(s).

[0035] **FIG. 5** illustrates an example hybrid cloud environment. As in FIG. 4, the example embodiment of FIG. 5 can include data center/private cloud 402, provider/public cloud 412, and secure link/tunnel 418. FIG. 5 illustrates an example application of hybrid cloud security groups wherein data/applications/VMs (not shown) are requesting exit from private cloud 402 in order to enter provider/public cloud 412. As discussed with respect to FIG. 4, private cloud gateway 406 can verify that any data, applications, VMs, etc. attempting to exit the private cloud 402 are authorized to leave private cloud 402.

[0036] For example, programming code 520 may provide private cloud gateway 406 with parameters for authorized entry/exit from private cloud 402. It is understood that programming code 520 may be implemented in many other forms besides that shown in FIG. 5. Moreover, embodiments of the present technology may utilize one or more programming languages to determine parameters for different hybrid cloud security groups. In some embodiments, programming code 520 may provide for entry parameters and/or exit parameters of private cloud 402. FIG. 5 illustrates that, in some embodiments, data may not be permitted to leave private cloud 402 if the hybrid cloud security group tag associated with the data, based on parameters that may be defined by

an administrator, does not authorize exit from private cloud 402. For example, if an application from private cloud 402 is not a part of a selected subnet that has a security group tag allowing for exit from private cloud 402, the application will be denied exit from private cloud 402 as shown at private cloud gateway 406.

[0037] In other embodiments, if data requested from private cloud 402 has a security group tag authorizing exit from private cloud 402, based on an allowed subnet, said data may be transmitted to provider public cloud 412 via secure tunnel 418. Some embodiments may provide for similar screening of transmitted data at provider public gateway 416 in order to ensure that the data is part of an authorized security group for access into provider public cloud 412. It is understood that a request for data from private cloud 402 may come from within private cloud 402, within provider public cloud 412, or from a third party/parties.

[0038] **FIG. 6** illustrates an example hybrid cloud environment. As in FIG. 4, the example embodiment of FIG. 6 can include data center/private cloud 402, provider/public cloud 412, and secure link/tunnel 418. FIG. 6 illustrates an example application of hybrid cloud security groups wherein data/applications/VMs (not shown) are requesting exit from provider public cloud 412 in order to enter private cloud 402. As discussed with respect to FIG. 4, public cloud gateway 416 can verify that any data, applications, VMs, etc. attempting to exit the public cloud 412 are authorized to leave public cloud 412.

[0039] For example, programming code 620 may provide public cloud gateway 416 with parameters for authorized entry/exit from public cloud 412. It is understood that programming code 620 may be implemented in many other forms besides that shown in FIG. 6. Moreover, embodiments of the present technology may utilize one or more programming languages to determine parameters for different hybrid cloud security groups. In some embodiments, programming code 620 may provide for entry parameters and/or exit parameters of public cloud 412. FIG. 6 illustrates that, in some embodiments, data may not be permitted to leave public cloud 412 if the hybrid cloud security group tag associated with the data, based on parameters that may be defined by an administrator, does not authorize exit from public cloud 412. For example, if an application from public cloud 412 is not a part of an extended VLAN that has a security group tag allowing for entry into private cloud 402 from public cloud 412, the application will be denied exit from public cloud 412 as shown at public cloud gateway 416.

[0040] In other embodiments, if data requested from public cloud 412 has a security group tag authorizing exit from public cloud 412, based on an allowed extended VLAN, said data may be transmitted to private cloud 402 via secure tunnel 418. Some embodiments may provide for similar screening of transmitted data at private gateway 406 in order to ensure that the data is part of an authorized security group for access into private cloud 402. It is understood that a request for data from provider public cloud 412 may come from within provider public cloud 412, within private cloud 402, or from a third party/parties.

[0041] **FIG. 7** illustrates an example hybrid cloud environment. As in FIG. 4, the example embodiment of FIG. 7 can include data center/private cloud 402, provider/public cloud 412, and secure link/tunnel 418. FIG. 7 illustrates an example application of hybrid cloud security groups wherein an instance (not shown) of the hybrid cloud environment is screened for authorization based on the security group associated with the instance. For example, FIG. 7 shows instance 702 attempting access to provider public cloud 412. Instance 702 does not have a security group tag authorized for entry into provider public cloud 412. Thus, public cloud gateway 416 denies access to instance 702 such that instance 702 is not allowed to reach hybrid VM 712. On the other hand, if an instance from private cloud 402 has a security group tag authorizing exit from private cloud 402 and entry into public cloud 412, the instance may be transmitted to provider public cloud 412 via secure tunnel 418.

[0042] In some embodiments, the present technology can utilize the security structure of the provider public cloud in order to enhance security. For example, if the provider public cloud has its own security parameters/security groups for data entering the public cloud (e.g., Amazon AWS® security groups), embodiments of the present technology may apply those security parameters in place of or in addition to the security parameters of the hybrid cloud security group associated with the data requesting entry into the public cloud.

[0043] For example, **FIG. 8** illustrates an example hybrid cloud environment utilizing security parameters/security group settings of a provider public cloud 412. As in FIG. 4, the example embodiment of FIG. 8 can include data center/private cloud 402, provider/public cloud 412, secure link/tunnel 418, and gateways 406 and 416. FIG. 8 illustrates example security parameters/security group settings 802. For example, security group settings 802 may be provided by Amazon AWS® and may complement the security features provided by the private cloud 402 security group settings by providing additional security requirements for entities requesting access to the provider public cloud 412. It is understood that many other security settings may be used besides what is shown in FIG. 8.

[0044] **FIG. 9** illustrates an example process 900 of the present technology. Process 900 begins at 902 where a request is received from a first cloud network of a hybrid cloud environment to transmit data to a second cloud network of the hybrid cloud environment. Process 900 continues at 904 where a security profile of the request is automatically analyzed to determine access permissions. Example process 900 concludes at 906 where, based at least in part on the access permissions, the data is allowed to access the second cloud network of the hybrid cloud environment. It is understood that embodiments of the present technology may include fewer or

more steps than process 900.

[0045] **FIG. 10** illustrates an example computer system 1050 having a chipset architecture that can be used in executing embodiments of the present technology and generating and displaying a graphical user interface (GUI). Computer system 1050 is an example of computer hardware, software, and firmware that can be used to implement embodiments of the disclosed technology. System 1050 can include a processor 1055, representative of any number of physically and/or logically distinct resources capable of executing software and/or firmware, and utilizing hardware configured to perform identified computations. Processor 1055 can communicate with a chipset 1060 that can control input to and output from processor 1055. In some embodiments, chipset 1060 outputs information to output 1065 (for example, a display) and can read and write information to storage device 1070 (for example, magnetic media and solid state media). Chipset 1060 can also read data from and write data to RAM 1075. In some embodiments, a bridge 1080 may be utilized by chipset 1060 for interfacing with a variety of user interface components 1085. Such user interface components 1085 can include a keyboard, a microphone, touch detection and processing circuitry, a pointing device, such as a mouse, and the like. In general, inputs to system 1050 can come from any of a variety of sources, machine generated and/or human generated.

[0046] Chipset 1060 can also interface with one or more communication interfaces 1090 that can have different physical interfaces. Such communication interfaces can include interfaces for wired and wireless local area networks, for broadband wireless networks, as well as personal area networks. Some applications of the methods for generating, displaying, and using the GUI disclosed herein can include receiving ordered datasets over the physical interface or be generated by the system itself by processor 1055 analyzing data stored in storage 1070 or 1075. Further, the system can receive inputs from a user via user interface components 1085 and execute appropriate functions, such as browsing functions by interpreting these inputs using processor 1055.

[0047] It can be appreciated that example system 1050 can have more than one processor 1055 or be part of a group or cluster of computing devices networked together to provide greater processing and/or storage capabilities.

[0048] For clarity of explanation, in some instances the present technology may be presented as including individual functional blocks including functional blocks comprising devices, device components, steps or routines in a method embodied in software, or combinations of hardware and software.

[0049] In some embodiments the computer-readable storage devices, mediums, and memories can include a cable or wireless signal containing a bit stream and the like. However, when mentioned, non-transitory computer-readable storage media expressly exclude media such as energy, carrier signals, electromagnetic waves, and signals per se.

[0050] Methods according to the above-described examples can be implemented using computer-executable instructions that are stored or otherwise available from computer readable media. Such instructions can comprise, for example, instructions and data which cause or otherwise configure a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. Portions of computer resources used can be accessible over a network. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, firmware, or source code. Examples of computer-readable media that may be used to store instructions, information used, and/or information created during methods according to described examples include magnetic or optical disks, flash memory, USB devices provided with non-volatile memory, networked storage devices, and the like.

[0051] Devices implementing methods according to these disclosures can comprise hardware, firmware, and/or software, and can use a variety of arrangements or form factors. Typical examples of such form factors include laptops, smart phones, small form factor personal computers, personal digital assistants, rackmount devices, standalone devices, and the like. Functionality described herein also can be embodied in peripherals or add-in cards. Such functionality can also be implemented on a circuit board among different chips or different processes executing in a single device, by way of further example.

[0052] The instructions, media for conveying such instructions, computing resources for executing them, and other structures for supporting such computing resources are means for providing the functions described in these disclosures.

[0053] Although a variety of examples and other information was used to explain aspects within the scope of the appended claims, no limitation of the claims should be implied based on particular features or arrangements in such examples, as one of ordinary skill would be able to use these examples to derive a wide variety of implementations. Further and although some subject matter may have been described in language specific to examples of structural features and/or method steps, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to these described features or acts. For example, such functionality can be distributed differently or performed in components other than those identified herein. Rather, the described features and steps are disclosed as examples of components of systems and methods within the scope of the appended claims. Moreover, claim language reciting "at least one of" a set indicates that one member of the set or multiple members of the set satisfy the claim.

[0054] The techniques disclosed herein can provide increased security with respect to network resources and

data in a hybrid cloud environment. Embodiments of the present technology can prevent harmful and/or unauthorized entities from entering the hybrid cloud network environment, which may result in more efficient network routing and high availability of network applications and systems, which in turn may result in fewer processor cycles required to route signals and thus improved efficiency and extended service life of the network processors used to implement some embodiments of the present technology. Thus, the present technology may improve related hardware used in its implementation.

[0055] Further, although the foregoing description has been directed to specific embodiments, it will be apparent that other variations and modifications may be made to the described embodiments, with the attainment of some or all of their advantages. For instance, it is expressly contemplated that the components and/or elements described herein can be implemented as software being stored on a tangible (non-transitory) computer-readable medium, devices, and memories (e.g., disks/ CDs/RAM/ EEPROM/ etc.) having program instructions executing on a computer, hardware, firmware, or a combination thereof. Further, methods describing the various functions and techniques described herein can be implemented using computer-executable instructions that are stored or otherwise available from computer readable media. Such instructions can comprise, for example, instructions and data which cause or otherwise configure a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. Portions of computer resources used can be accessible over a network. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, firmware, or source code. Examples of computer-readable media that may be used to store instructions, information used, and/or information created during methods according to described examples include cloud-based media, magnetic or optical disks, flash memory, USB devices provided with non-volatile memory, networked storage devices, and the like. In addition, devices implementing methods according to these disclosures can comprise hardware, firmware and/or software, and can take any of a variety of form factors. Typical examples of such form factors include laptops, smart phones, tablets, wearable devices, small form factor personal computers, personal digital assistants, and the like. Functionality described herein also can be embodied in peripherals or add-in cards. Such functionality can also be implemented on a circuit board among different chips or different processes executing in a single device, by way of further example. Instructions, media for conveying such instructions, computing resources for executing them, and other structures for supporting such computing resources are means for providing the functions described in these disclosures. Accordingly this description is to be taken only by way of example and not to otherwise limit the scope of the embodiments herein. Therefore, it is the object of the appended claims to cover all such variations and modifications as come within the true spirit and scope of the embodiments herein.

Claims

1. A method comprising:

receiving a request from a first cloud network of a hybrid cloud environment to transmit data to a second cloud network of the hybrid cloud environment, the request comprising a security profile related to the data;
automatically analyzing the security profile to determine access permissions related to the data; and
based at least in part on the access permissions, allowing the data to access to the second cloud network.

2. The method of claim 1, further comprising:
based at least in part on the access permissions, denying access to data that is not permitted access to the second cloud network.

3. The method of claim 1, further comprising:
transmitting the data to the second cloud network via a hybrid link, the hybrid link utilized for secure communications between the first cloud network and the second cloud network, wherein the hybrid link does not allow connection to the Internet.

4. The method of claim 1, wherein the security profile is automatically applied to applications initialized in the hybrid cloud environment.

5. The method of claim 1, further comprising:

receiving a request for a virtual machine in the hybrid cloud environment;
determining that the request originates from an Internet Protocol (IP) address of a private cloud network of the hybrid cloud environment; and
providing the virtual machine in the hybrid cloud environment.

6. The method of claim 1, further comprising:

receiving a request for access to a private cloud network of the hybrid cloud environment from a public cloud network of the hybrid cloud environment;
automatically determining that the request for access to the private cloud network is from an entity with access permission to operate in the private cloud network; and
based at least in part on the access permission,

allowing access to the private cloud network.

7. The method of claim 1, further comprising:

receiving a request for access to a public cloud network of the hybrid cloud environment from a private cloud network of the hybrid cloud environment;
automatically determining that the request for access to the public cloud network is from an entity with access permission to operate in the public cloud network; and
based at least in part on the access permission, allowing access to the public cloud network.

8. A network device comprising:

one or more servers facilitating a first cloud network of a hybrid cloud environment;
one or more servers facilitating a second cloud network of the hybrid cloud environment;
one or more processors; and
a memory configured to store a process, the process, when executed by the one or more processors, being operable to:

receive a request from the first cloud network of the hybrid cloud environment to transmit data to the second cloud network of the hybrid cloud environment, the request comprising a security profile related to the data;
automatically analyze the security profile to determine access permissions related to the data; and
based at least in part on the access permissions, allow the data to access to the second cloud network.

9. The network device of claim 8, the process further operable to:
based at least in part on the access permissions, deny access to data that is not permitted access to the second cloud network.

10. The network device of claim 8, the process further operable to:
transmit the data to the second cloud network via a hybrid link, the hybrid link utilized for secure communications between the first cloud network and the second cloud network, wherein the hybrid link does not allow connection to the Internet.

11. The network device of claim 8, the process further operable to:

receive a request for a virtual machine in the hybrid cloud environment;
determine that the request originates from an Internet Protocol (IP) address of a private cloud network of the hybrid cloud environment; and
provide the virtual machine in the hybrid cloud environment.

12. The network device of claim 8, the process further operable to:

receive a request for access to a private cloud network of the hybrid cloud environment from a public cloud network of the hybrid cloud environment;
automatically determine that the request for access to the private cloud network is from an entity with access permission to operate in the private cloud network; and
based at least in part on the access permission, allow access to the private cloud network.

13. The network device of claim 8, the process further operable to:

receive a request for access to a public cloud network of the hybrid cloud environment from a private cloud network of the hybrid cloud environment;
automatically determine that the request for access to the public cloud network is from an entity with access permission to operate in the public cloud network; and
based at least in part on the access permission, allow access to the public cloud network.

14. A non-transitory computer-readable medium having instructions encoded thereon, the instructions, when executed by a processor, being operable to perform a method according to any of claims 1 through 7.

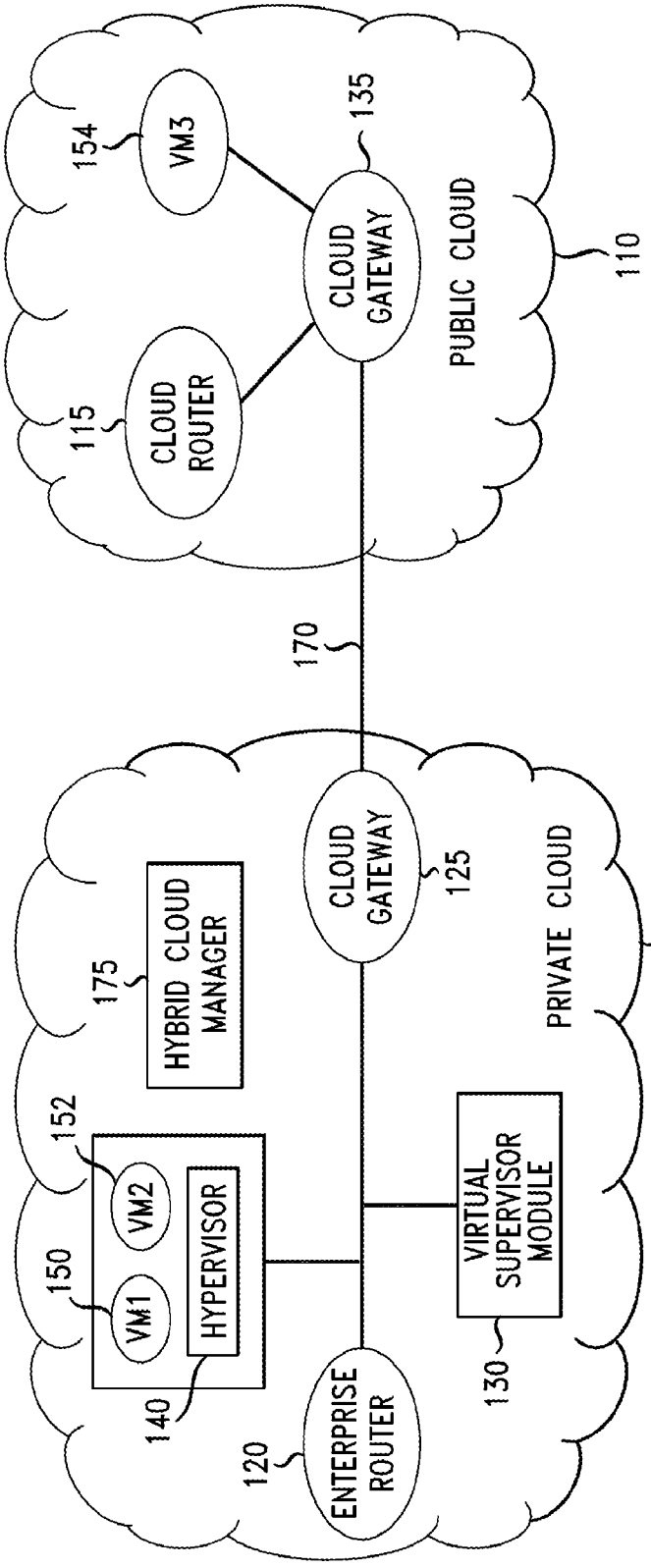
PUBLIC CLOUD
110
CLOUD GATEWAY
135
VM3
154
CLOUD ROUTER
115
170
PRIVATE CLOUD
105
CLOUD GATEWAY
125
HYBRID CLOUD MANAGER
175
152
VM2
HYPERVISOR
150
VM1
140
VIRTUAL SUPERVISOR MODULE
130
ENTERPRISE ROUTER
120

FIG. 1

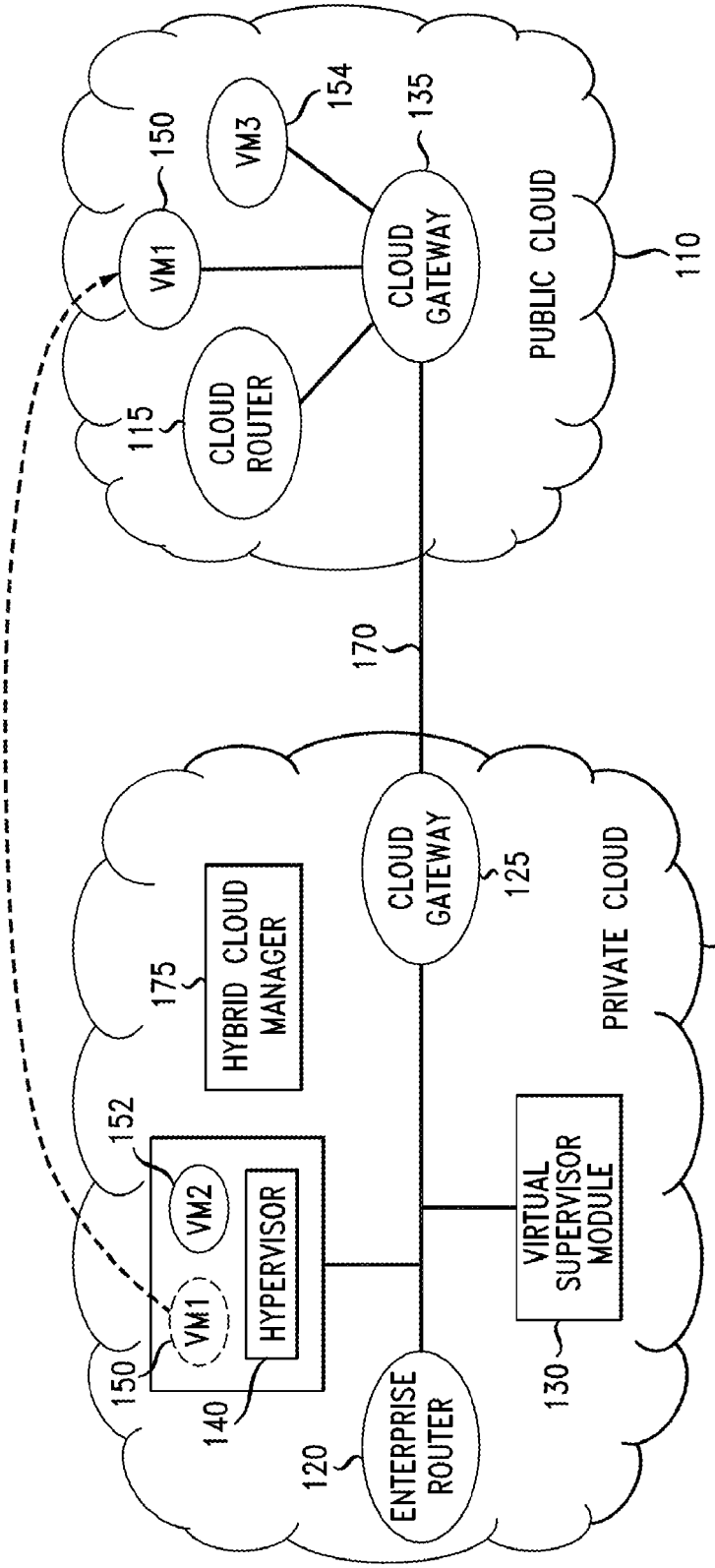
PUBLIC CLOUD
110
VM1
150
VM3
154
CLOUD GATEWAY
135
CLOUD ROUTER
115
170
PRIVATE CLOUD
105
CLOUD GATEWAY
125
HYBRID CLOUD MANAGER
175
152
VM2
VM1
HYPERVISOR
150
140
VIRTUAL SUPERVISOR MODULE
130
ENTERPRISE ROUTER
120

FIG. 2

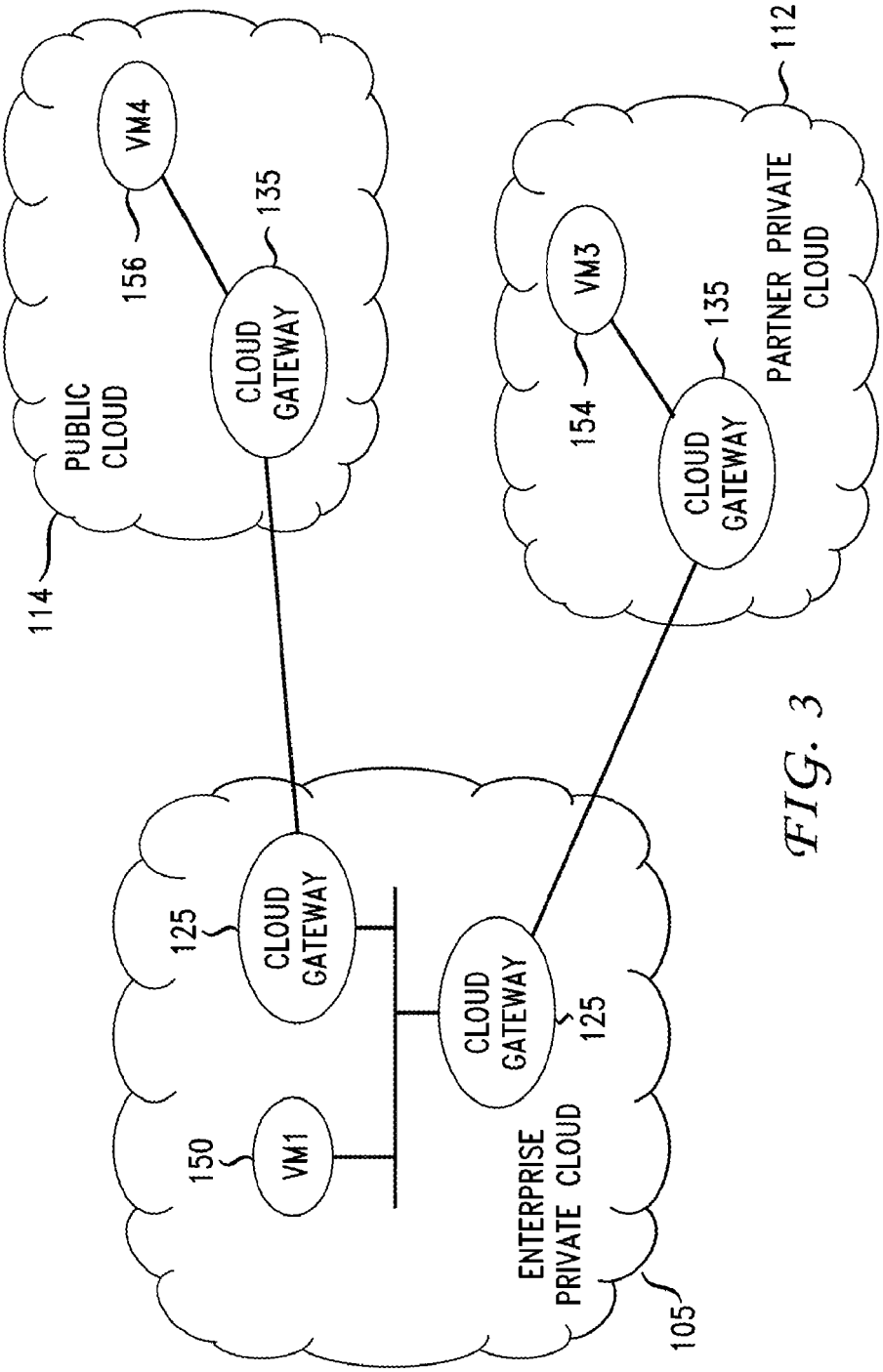
PUBLIC CLOUD
114
VM4
156
CLOUD GATEWAY
135
PARTNER PRIVATE CLOUD
112
VM3
154
CLOUD GATEWAY
135
CLOUD GATEWAY
125
CLOUD GATEWAY
125
VM1
150
ENTERPRISE PRIVATE CLOUD
105

FIG. 3

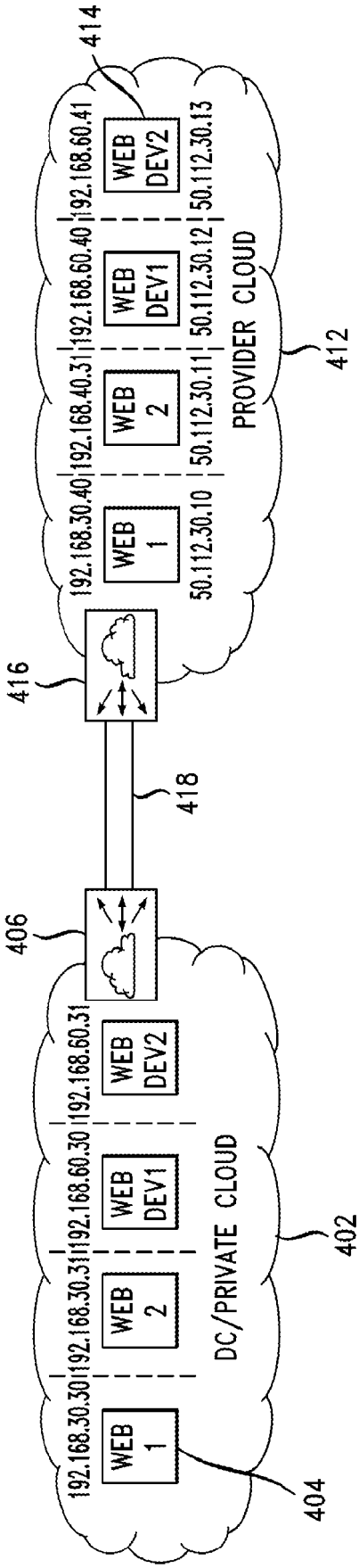
414
192.168.60.41
WEB DEV2
50.112.30.13
192.168.60.40
WEB DEV1
50.112.30.12
192.168.40.31
WEB 2
50.112.30.11
192.168.30.40
WEB 1
50.112.30.10
PROVIDER CLOUD
412
416
418
406
192.168.60.31
WEB DEV2
192.168.60.30
WEB DEV1
192.168.30.31
WEB 2
192.168.30.30
WEB 1
DC/PRIVATE CLOUD
402
404

FIG. 4

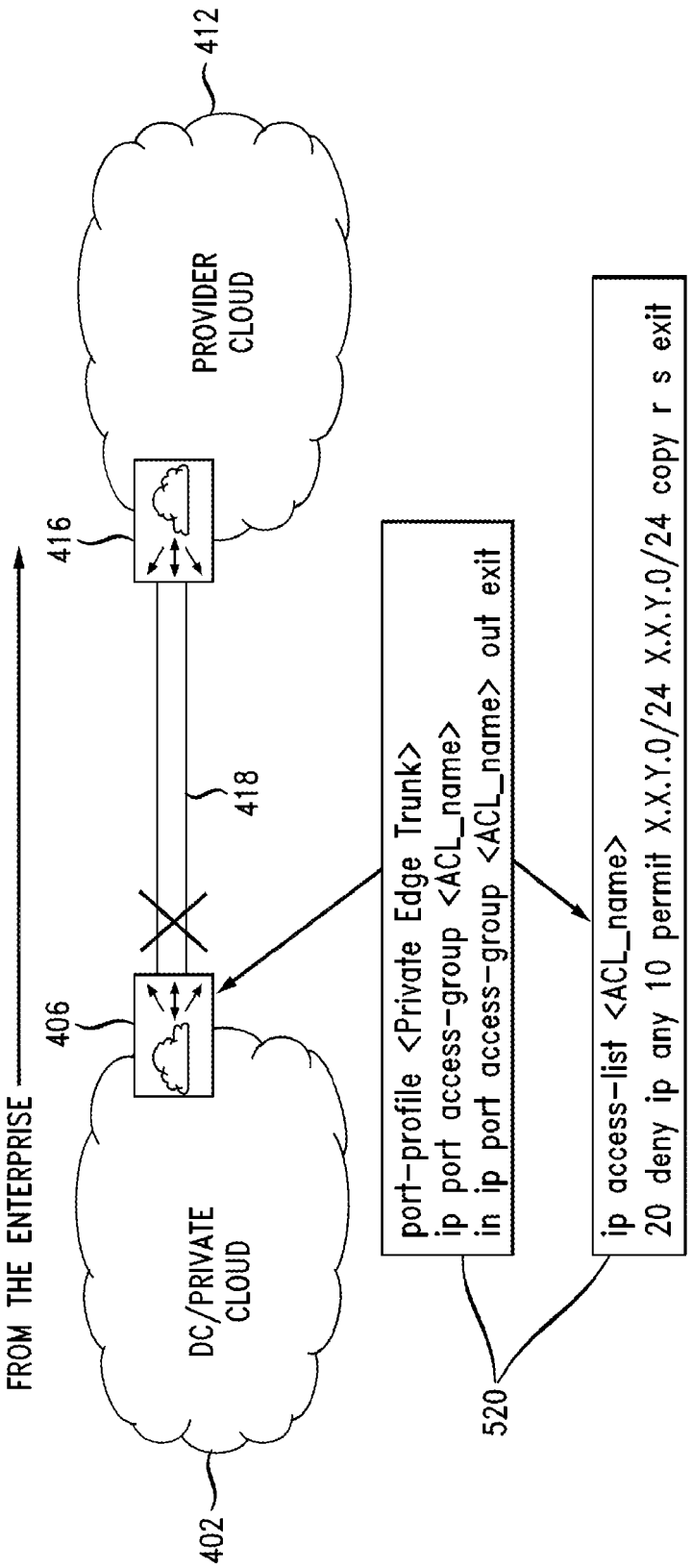
412
PROVIDER CLOUD
416
418
406
FROM THE ENTERPRISE
DC/PRIVATE CLOUD
402
port-profile <Private Edge Trunk>
ip port access-group <ACL_name>
in ip port access-group <ACL_name> out exit
ip access-list <ACL_name>
20 deny ip any 10 permit X.X.Y.0/24 X.X.Y.0/24 copy r s exit
520

FIG. 5

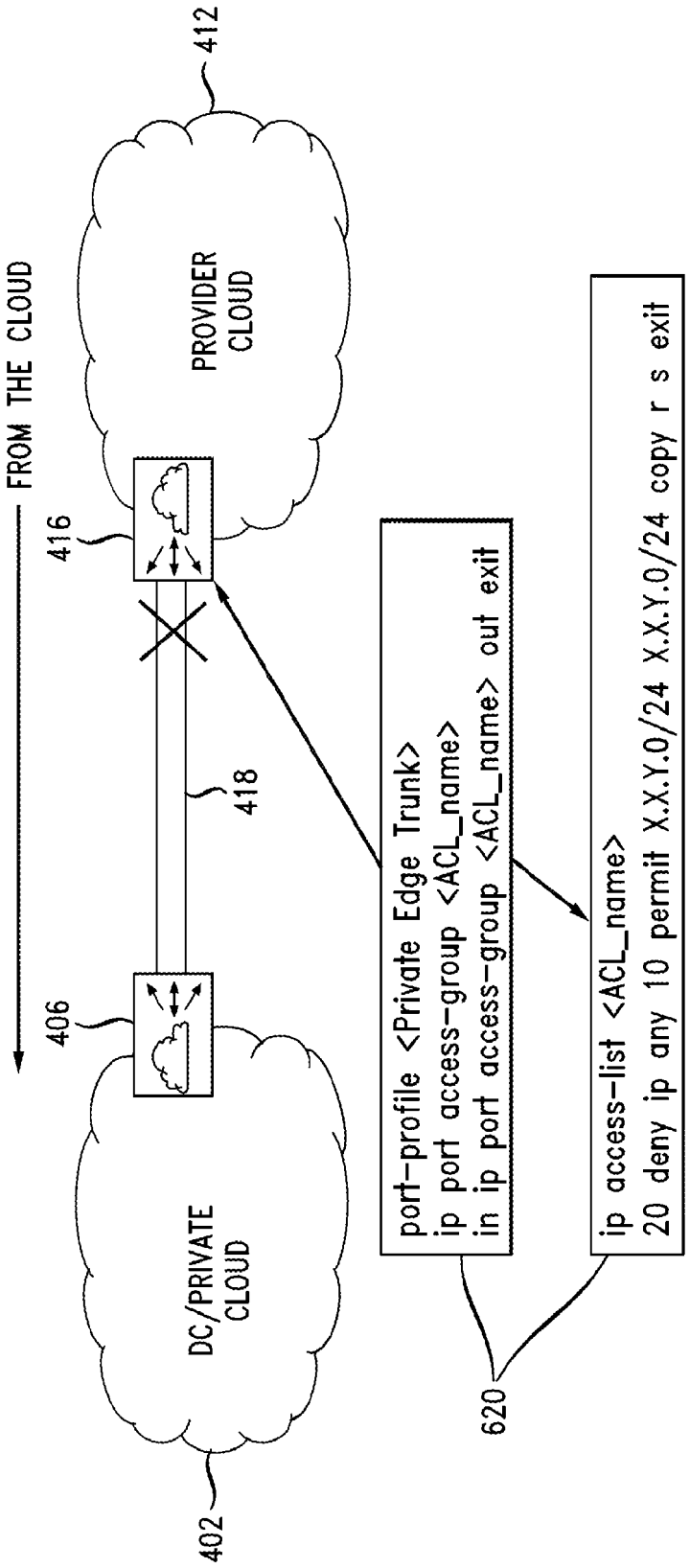
412
PROVIDER CLOUD
FROM THE CLOUD
416
418
406
DC/PRIVATE CLOUD
402
port-profile <Private Edge Trunk>
ip port access-group <ACL_name>
in ip port access-group <ACL_name> out exit
ip access-list <ACL_name>
20 deny ip any 10 permit X.X.Y.0/24 X.X.Y.0/24 copy r s exit
620

FIG. 6

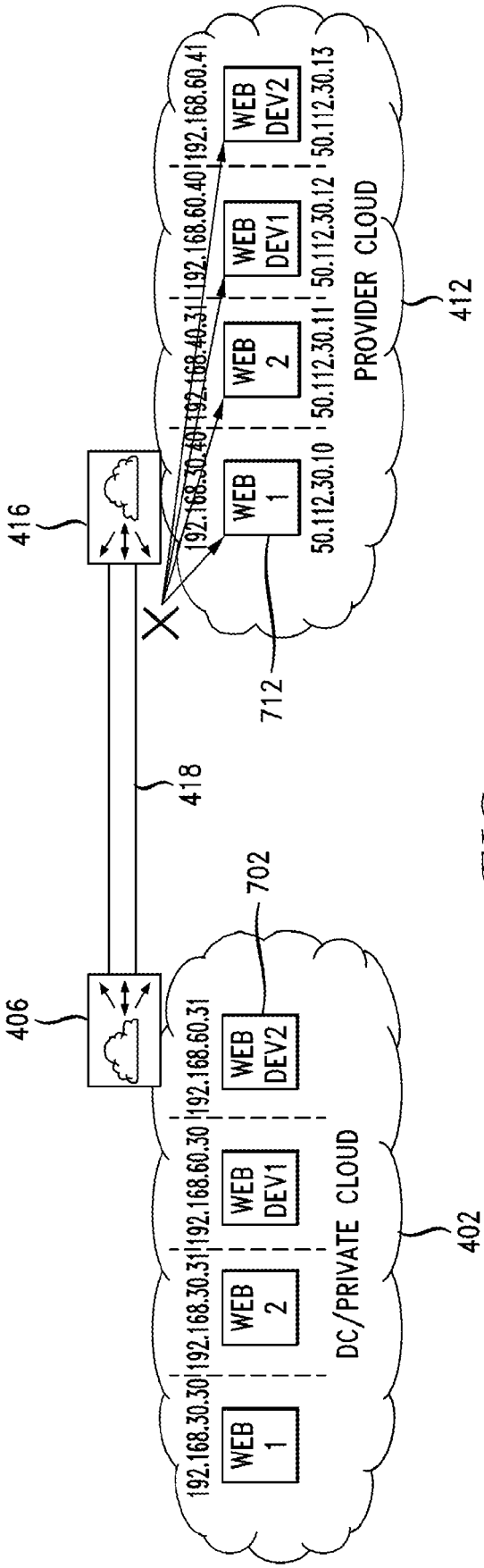
406
416
418
712
702
402
412
DC/PRIVATE CLOUD
PROVIDER CLOUD
WEB 1
WEB 2
WEB DEV1
WEB DEV2
192.168.30.30
192.168.30.31
192.168.60.30
192.168.60.31
192.168.60.40
192.168.60.41
50.112.30.10
50.112.30.11
50.112.30.12
50.112.30.13

FIG. 7

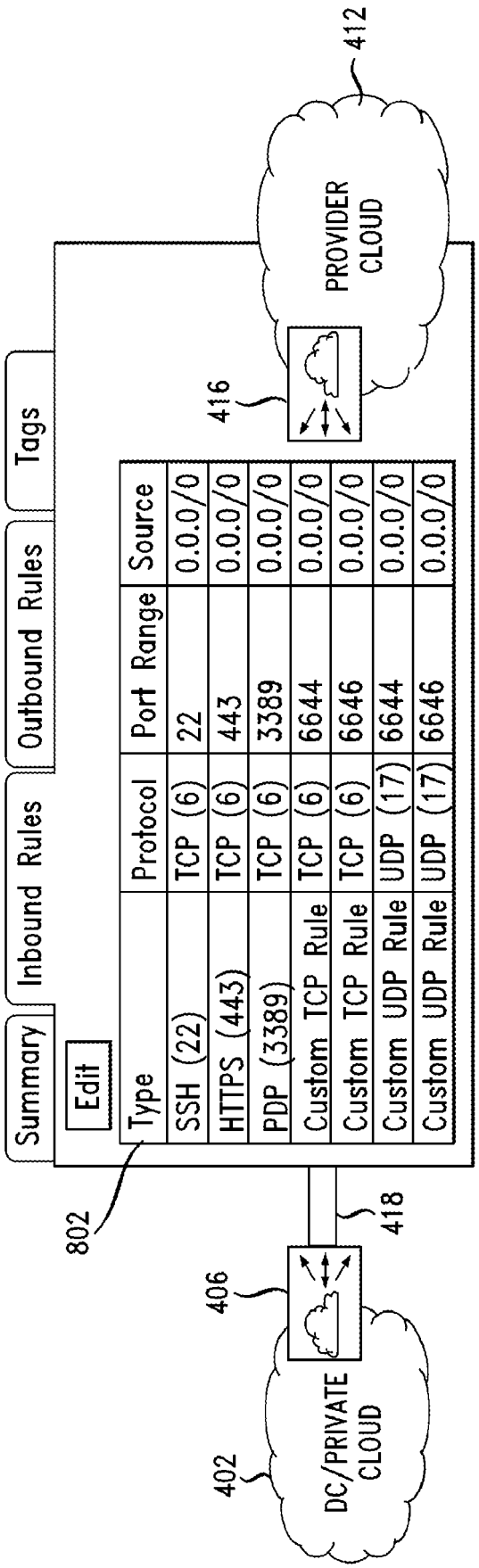
412
PROVIDER CLOUD
416
Summary
Inbound Rules
Outbound Rules
Tags
Edit
802
Type
Protocol
Port Range
Source
SSH (22)
TCP (6)
22
0.0.0/0
HTTPS (443)
TCP (6)
443
0.0.0/0
PDP (3389)
TCP (6)
3389
0.0.0/0
Custom TCP Rule
TCP (6)
6644
0.0.0/0
Custom TCP Rule
TCP (6)
6646
0.0.0/0
Custom UDP Rule
UDP (17)
6644
0.0.0/0
Custom UDP Rule
UDP (17)
6646
0.0.0/0
418
406
402
DC/PRIVATE CLOUD

FIG. 8

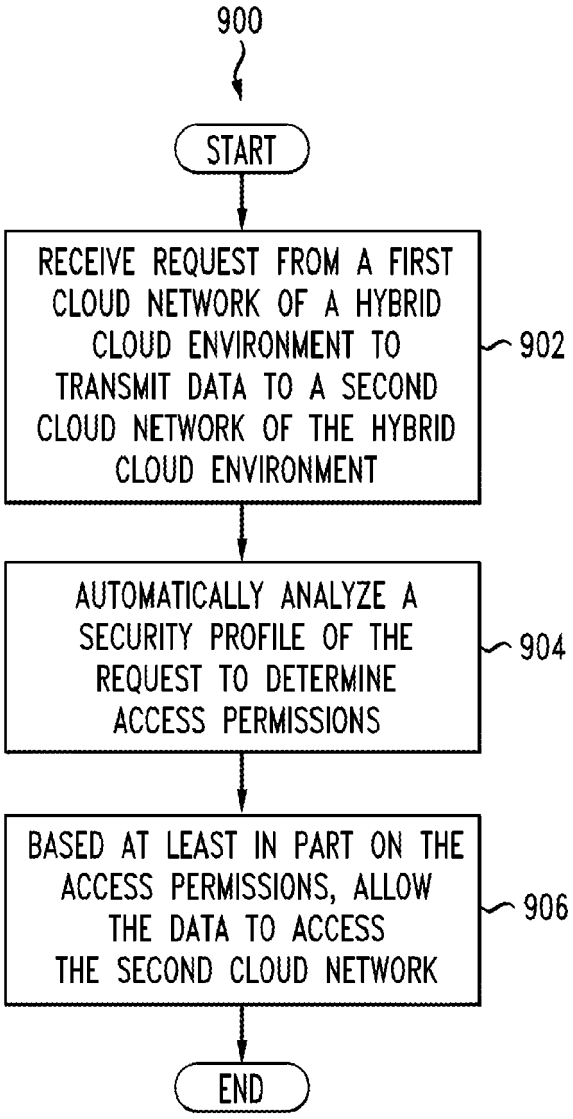
900
START
RECEIVE REQUEST FROM A FIRST CLOUD NETWORK OF A HYBRID CLOUD ENVIRONMENT TO TRANSMIT DATA TO A SECOND CLOUD NETWORK OF THE HYBRID CLOUD ENVIRONMENT
902
AUTOMATICALLY ANALYZE A SECURITY PROFILE OF THE REQUEST TO DETERMINE ACCESS PERMISSIONS
904
BASED AT LEAST IN PART ON THE ACCESS PERMISSIONS, ALLOW THE DATA TO ACCESS THE SECOND CLOUD NETWORK
906
END

FIG. 9

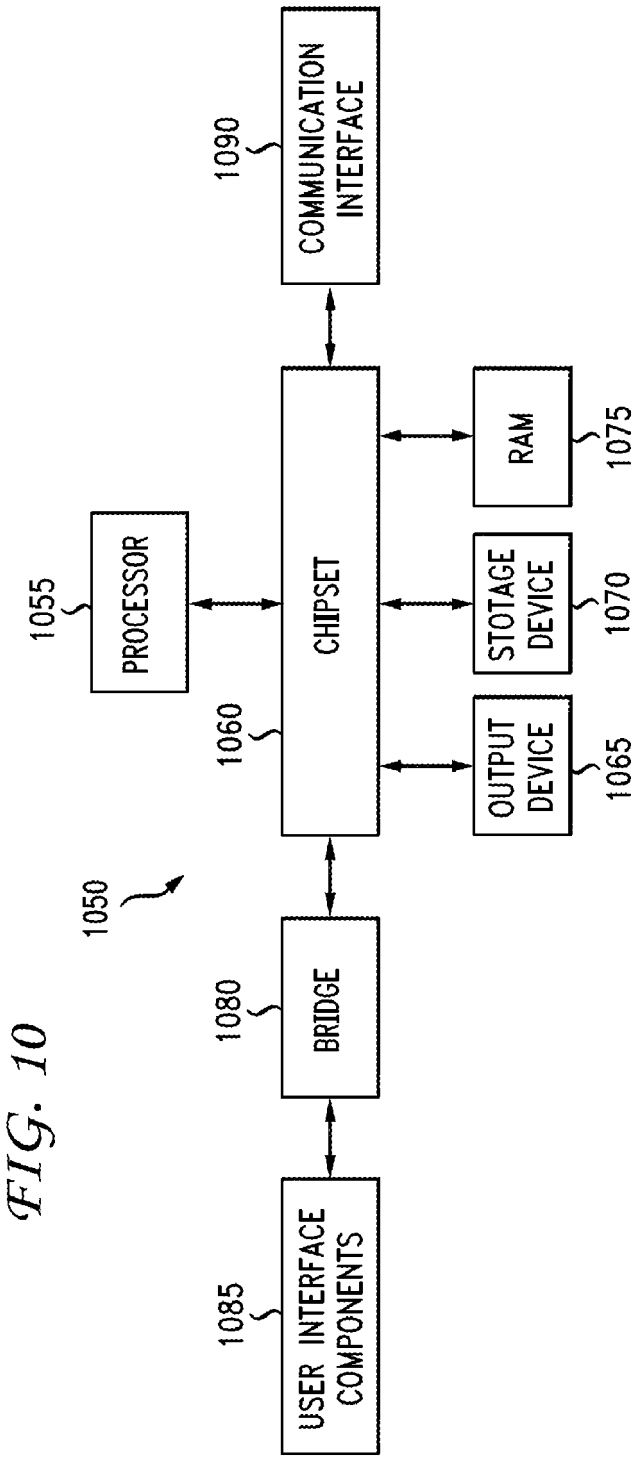
1050
1055
PROCESSOR
1060
CHIPSET
1080
BRIDGE
1085
USER INTERFACE COMPONENTS
1090
COMMUNICATION INTERFACE
RAM
1075
STOTAGE DEVICE
1070
OUTPUT DEVICE
1065

FIG. 10

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 16 2173

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 8 938 775 B1 (ROTH GREGORY B [US] ET AL) 20 January 2015 (2015-01-20) * col. 2, lines 3-30; col. 3, lines 38-52; col. 5, lines 9-21; col. 9, line 43 - col. 10, line 16; figures 1, 2, 5 *	1-14	INV. H04L29/06
A	US 2014/282889 A1 (ISHAYA VISHVANANDA [US] ET AL) 18 September 2014 (2014-09-18) * paragraphs [0007] - [0009], [0052] - [0067], [0102] - [0105], [0140] - [0141] *	1-14	
A	US 2012/185913 A1 (MARTINEZ FRANK R [US] ET AL) 19 July 2012 (2012-07-19) * paragraphs [0020] - [0035], [0092] - [0094], [0106] *	1-14	
			TECHNICAL FIELDS SEARCHED (IPC) H04L G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	30 June 2021	Winkelbauer, Andreas

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 21 16 2173

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-06-2021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8938775 B1	20-01-2015	NONE	
US 2014282889 A1	18-09-2014	AU 2014236872 A1	29-10-2015
		EP 2972843 A1	20-01-2016
		HK 1220781 A1	12-05-2017
		US 2014282889 A1	18-09-2014
		US 2015229629 A1	13-08-2015
		US 2017195306 A1	06-07-2017
		WO 2014151839 A1	25-09-2014
US 2012185913 A1	19-07-2012	US 2012185913 A1	19-07-2012
		US 2016112453 A1	21-04-2016
		US 2018131724 A1	10-05-2018
		US 2019245888 A1	08-08-2019
		US 2021014275 A1	14-01-2021

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82