The Security Challenges and Opportunities of New Network Under the Hybrid Cloud Environment

Yuxiang Dong, Huijun Zhang and Linong Zhao

Abstract A hybrid cloud becomes the preferred solution when enterprises deploy cloud service. Using new technology such as software-defined network (SDN) and network virtualization to form a network will be the trend of the future. This paper introduces the new safety protection opportunities brought by new network technologies, and analyzes the challenges and risks of hybrid cloud system using these technologies. Finally, it puts forward the corresponding solution.

Keywords Hybrid cloud · Software-defined network · Network function virtualization · Network security

1 Introduction

In the past five years, the Internet has undergone tremendous changes. New IT Infrastructure and applications such as Cloud computing (Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet [1]), big data, Mobile Internet, and the Internet of things (IOT) are becoming more and more widely used [2]. For enterprise users, 26.1% of users choose Cloud computing as an investment focus, while 27.4% of Small and Medium Enterprises (SMEs) tend to choose SDN center as the focus of investment over the next 12 months [3]. These companies are likely to merge IT systems in physical office environment and virtual private cloud to form a hybrid cloud (hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms [4]).

Y. Dong · H. Zhang (✉) · L. Zhao
China Mobile Group Chongqing Co., Ltd, Chongqing 401122, China
e-mail: mms@139.com

S.K. Bhatia et al. (eds.), *Advances in Computer and Computational Sciences*,
Advances in Intelligent Systems and Computing 553,
DOI 10.1007/978-981-10-3770-2_18

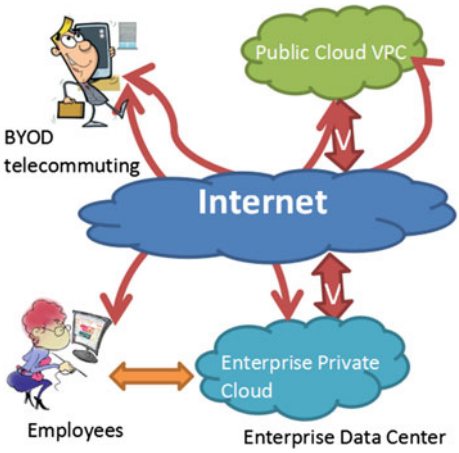

Fig. 1 Fusion border of hybrid cloud

On the other hand, in order to achieve office automation, many enterprises allow the use of mobile devices, so Bring Your Own Device (BYOD) combines with the Cloud computing information system for the office has emerged [5]. Popularization of cloud platform increases the risk of data leakage and network attack. There are all kinds of threats in network, host, virtual resource management, data security, etc. Using mobile office and BYOD hybrid cloud blurs the boundaries between different IT systems of enterprise. As shown in Fig. 1, BYOD blurs the boundaries between fixed assets and mobile assets, so there is not a fixed border. Mobile office enables employees to access internal resources outside of the workplace, so that the entire boundary is beyond the scope of the enterprises physical area. Hybrid cloud is a blend of enterprise of physical devices and virtual assets, and it makes the whole boundary cannot rely on simple physical facilities to control [6]. All safety protective equipment and safety mechanism depend on the boundary will fail, and the attackers can always find the inconsistencies between physical boundaries and logical boundaries to invade. Even if the cloud system builders build a consistent boundary, with the change of virtual resources (such as virtual machines migration), these boundaries may antiquate too, so an attacker can also bypass the boundaries.

At the same time, some new technologies such as SDN and network function virtualization (NFV) appear. On the one hand, these new technologies speed up the Internet industry resource change and flow rate control, and they provide a new technical support for safety protection. On the other hand, these new technologies also bring new risks and challenges for the system.

This paper introduces new challenges of security hybrid cloud system brought by SDN/NFV, and analyzes the new security risks. At last, it gives the appropriate response suggestions.

2 New Opportunities of SDN/NFV in the Security Protection

Networks of hybrid Cloud computing information system include Cloud computing physical networks, virtual networks in virtual system, and networks of customer system. In general, security domain is used to isolate networks, so the access control mechanism is deployed on the border. At last, different safety equipment and protective measures are deployed in inner areas. The emergence of SDN and NFV brings a new concept of protection for traditional security system [7]. Mixing a variety of hybrid cloud protective mechanisms will accelerate the speed and efficiency of safety protection greatly [8]. There are three advantages as follows:

2.1 Global and Real-Time Flow View

With the help of a centralized architecture, SDN controller has real-time flow information of a global network, including topology, routing, and so on. The flow information is very useful in many protective scenarios. For example, when we take Distributed Denial of Service (DDoS) detection, we can get information of sampled flow (Sflow, it is an industry standard for packet export at Layer 2 of the OSI model. It provides a means for exporting truncated packets, together with interface counters) or OpenFlow (OpenFlow is a communications protocol that gives access to the forwarding plane of a network switch or router over the network). Then, we judge whether there is any malicious attack according to the statistical characteristics of packet stream.

With the aid of flow information based on the global network equipment, we can build real-time and historical knowledge base which based on the flow. Then, we can analyze any access at run time, and confirm whether there is a similar pattern in the history of knowledge base. If answer is no, it may be a malicious attacker existing. So we can deploy virtual safety equipment for deep packet inspection with the aid of NFV technology.

2.2 Flexible Security Services

Using NFV technology, security service providers may allocate resources dynamically and it will save resources. For example, they can generate a large number of virtual Web firewalls for the flow of large e-commerce sites in sales season, but reduce number of security virtual machines at other times to get more profit.

2.3 *Software-Defined Security*

Gartner puts forward the Software-Defined Security (SDS) [9] first, and emphasizes the underlying abstract is a kind of resources in safety resource pool. Intelligent and automation business arrangement and management can be realized in the software programming way at the top-level design, to complete the corresponding security functions. Since then, the combination of the definition and security of software become the forefront of the industry development.

NFV can start virtual safety equipment by the software, and with the aid of SDN controller, the appropriate flow can be pulled or mirrored to one or more of the above safety equipment. Then, we can make fine-grained test and form a security service chain. So SDN and NFV naturally become the underlying software-defined security support technology. Security resources and flow control are decided by north security application programming, and thus the entire scheme is flexible and quick.

3 Security Challenges of New Network

Adding SDN and NFV into hybrid cloud, the architecture of the whole system will be shown in Fig. 2. The network architecture is divided into enterprise networks, Internet, and cloud system network. The enterprise network contains employee office network, self-built enterprise private cloud, and public wireless network. Cloud system environment contains multiple tenants of the virtual network, and virtual network connects to enterprise network.

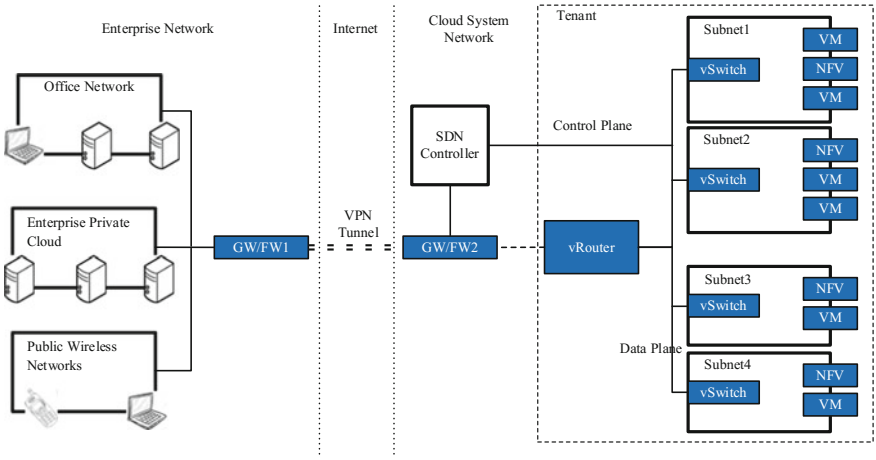

Fig. 2 Architecture of hybrid cloud

In the cloud environment, SDN controller connects to physical network device or virtual network device in the cloud system. Security management platform deploys virtual safety equipment with the aid of NFV technology, and completes the deep packet inspection, attack prevention and load balancing, and so on.

SDN and NFV technology brought convenience for security protection, but new technology is also associated with new risks and challenges.

3.1 Architecture

From an architectural point of view, SDN use centralized control but the cloud system is usually elastic distributed. So when the Cloud computing system scales out, as shown in Fig. 2, the virtual network on the right side is becoming more and more, a single SDN controller may not be able to handle all the network flow. In addition, if SDN controller uses reactive work mode, not issue flow table in advance but do it when received PACKET_IN, it will be easy to be rejected in the larger network services.

3.2 System Implementation

SDN architecture includes applications, controllers, switches, and the management system. Virtualization system includes control nodes, management nodes, storage nodes, and the compute nodes. All these components rely on software running. But the software may be fragile, and the attacker can use and gain unauthorized access, thereby blocking of malicious manipulation of the flow.

For example, most of Switches use the open operating system based on Linux, some use unsafe Telnet service, or use the Secure Shell (SSH) service which owns default user name and password, and some use Plaintext communication. Even if the system design and deployment is perfect, some services also have loopholes in themselves. For example, many services use Secure Sockets Layer (SSL, a cryptographic protocol) to encrypt communications, but some use outdated SSL with implementation loopholes, such as Heartbleed (Heartbleed is a security bug disclosed in April 2014, which is a widely used implementation of the Transport Layer Security protocol). It will reveal information of SDN controller or tenant's privacy information in a virtualized system, and it brings great risks to the whole system. In some Cloud computing systems, data network may be shared with management or control network. If tenants attempted successfully, they can access the control node of SDN or virtualized systems, then manipulate the underlying route bypassing safety equipment.

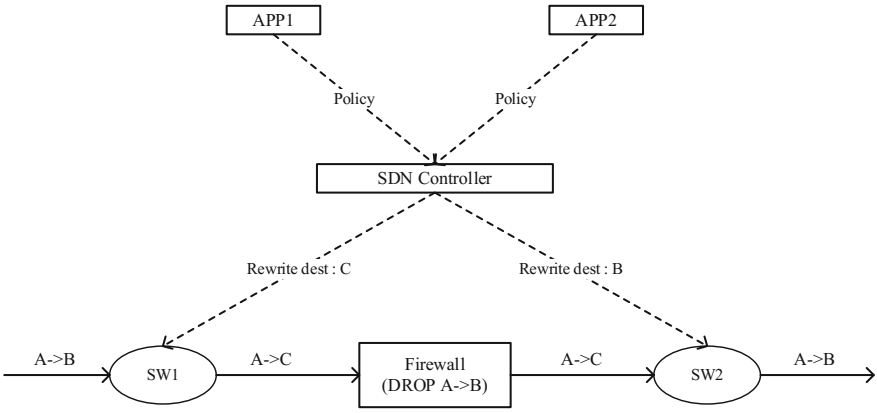

Fig. 3 Policy inconsistencies cause the firewall be bypassed

3.3 Policy Consistency

SDN Controller issues upper application policy to the underlying network equipment, and controls all network flow ultimately. But if the SDN controller policy lacks of consistency checking mechanism, it may appear multiple applications issuing policies conflicted and cause network problems. In more severe cases, a malicious attacker can bypass many strategies security deployment in advance.

As shown in Fig. 3, the firewall strategy is to ban all A -> B packets, but the attackers may issue instructions by different applications, and two SDN controllers will issue strategies which rewrite the destination address to SW1 and SW2 respectively. Then strategy 1 rewrites the destination address of packet A -> B for C, strategy 2 rewrites the destination address of packet A -> C packet for B, and manages to bypass the firewall security strategy, implementing unauthorized access control at last.

3.4 Compatibility of SDN and the Virtualization System

In a typical scene, if the virtualization system use Openstack (Openstack is a free and open-source software platform for cloud computing), and the underlying drivers are OpenVswitch plunging (The main purpose of OpenVswitch is to provide a switching stack for hardware virtualization environments, while supporting multiple protocols and standards used in computer networks), and SDN controller using the Floodlight (an enterprise, Apache license, OpenFlow controller based on Java) or RYU (a kind of controller for OpenFlow) etc., then the Floodlight or RYU cannot

distinguish whether flow of different virtual switch port belongs to the same tenant or not. So they can only send packet of tenants' virtual port with no difference, and destroy the tenant isolation which is the fundamental principles of virtualization, and cause a security risk.

3.5 Compatibility of NFV and Hypervisor

Migrating the physical security devices to virtualized systems to form a middle box (middle box is a computer networking device that transforms, inspects, filters, or otherwise manipulates traffic for purposes other than packet forwarding) of NFV, is a big challenge for two reasons: First, many devices, such as firewalls and Intrusion prevention system (IPS, a network security appliance), require customized NIC driver and kernel, in order to achieve better performance. But there are compatibility problems existing if you are deploying on the common hypervisor of compute nodes. Second, some virtualization systems offer hypervisor application interface for flow traction. Although it is a solution for SDN controller which is not deployed, but security personnel tend to consume a lot of energy to adapt these nonstandard interface. Even some virtualization systems do not open this interface, resulting in the deployment in L2 network in virtual environment is impossible such as network intrusion prevention system NIPS (Network Intrusion Prevention System, appliances that monitor network and/or system activities for malicious activity).

3.6 System Availability

Although the flexible deployment and resource pooling features of virtual safety equipment provide a great convenience for cloud security mechanism, but it is also need to solve the problem of high availability, especially when deploying equipment such as firewall and IPS. In the physical environment, they commonly deploy the active-standby equipment, using the heartbeat message and special line to achieve synchronization, and achieve a high availability. But under the condition of virtualization, network itself is not reliable, so the heartbeat mechanism cannot guarantee the security mechanism of usability.

In addition, virtualization security equipment has performance bottlenecks, so when there are a large number of simultaneous connections in a Website, the virtual safety equipment may deny service.

4 Security Advice

Considering the security risks involved in the third chapter, we need to make security design of the whole SDN and NFV architecture, the following aspects should be considered and implemented in system design phase.

4.1 The Global System Design

When deploying SDN system in a cloud environment, you should ensure the SDN controller is not a bottleneck of the whole system. There should be many controllers for collaboration to ensure the availability. Meanwhile, the cloud should have a hierarchical design, such as by reducing the size of each sub-domain in order to reduce the number of broadcast packets and reduce the load of SDN controller. When the network is designing, the scale of virtual network should be reduced to let down network flow of virtual security equipment.

When designing and implementing the SDN controller, we should eliminate safety hazards as far as possible. We can use application authentication, policy checks and control channel encryption to ensure security of application programming interface (API) and third-party libraries.

At the same time, we should give full consideration to combine SDN and virtualized systems, such as OpenDaylight (The OpenDaylight is a collaborative open-source project hosted by The Linux Foundation) which is a SDN controller platform, is a good adaptation to Openstack, it supports the association of tenants and flow, to ensure network resources and flow isolation.

4.2 Multiple Inspection Service Chain

Someone discusses the strategy of how to resolve the SDN application conflict, in order to solve the safety problems mentioned in 3.3. But there are loopholes exist in controllers always, and attackers may use a series of Attack China and avoid the security check to carry out targeted attacks. But defenders can also use the new features of SDN and NFV mentioned in Chap. 2, and compose multiple security mechanism. Security mechanisms can be deployed in any position, such as the proprietary safety hardware, or computing nodes of L2 network, or the gateway on the network nodes. Using SDN to tract flow, we can implement such as access control, Deep packet inspection (DPI, a form of computer network packet filtering) or behavior analysis, etc.

Even if the attacker escape some of the security mechanisms, but also the safety plans are in the dynamic changes, so abnormal phenomenon is found in a very short

time. The response process such as depth inspection, forensics, and restore is corresponding at once.

Considering the hypervisor implementation and openness of virtualization system are quite different, so the security resources deployment and flow traction mechanism should be as standardized as possible. For example, the security resources deployment should be deployed on Openvswtich and use Intel DPDK (The Data Plane Development Kit is a set of data plane libraries and network interface controller drivers for fast packet processing) acceleration card, and the flow traction mechanism can use OpenFlow/SDN to carry on traction of traffic, blocking and mirror.

4.3 Failure Recovery Mechanisms

If the device is not reliable, in order to guarantee the availability of the security mechanism, we should use fast recovery mechanisms after a failure. If the virtual safety equipment cannot response, we should use hot start technology of original image to start a new virtual machine quickly, and guide the network flow, issue the existing security policies and complete online quickly at the same time. This is different from the traditional scheme, and put forward higher requirements for resources generate (Provision) of virtualization system and collaborative scheduling mechanism.

5 Conclusion

Hybrid cloud merges Intranet, mobile office, BYOD, and Public clouds to a complete information system, and it improves the efficiency of the office. But at the same time, it changes the traditional security domain division and increases the attack risks. This paper introduces the new safety protection opportunities brought by SDN and NFV, and analyzes the challenges and risks of hybrid cloud system using these technologies. Finally, it puts forward the corresponding solution.

References

1. J Rhoton, R Haukioja. Cloud Computing Architected: Solution Design Handbook. Recursive Press, 2016
2. Kim, H., Feamster, N.Improving network management with software defined networking. Communications Magazine, IEEE. 2013
3. XL Wang, L Wang, A Bi, YY Li, Y Xu. Cloud computing in human resource management (HRM) system for small and medium enterprises (SMEs).International Journal of Advanced Manufacturing Technology, 2016:1–12

4. A Gordon. The Hybrid Cloud Security Professional. IEEE Cloud Computing, 2016,3(1):82–86
5. M Dhingra. Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). Procedia Computer Science, 2016,78:179–184
6. J Weinman.Hybrid Cloud Economics. IEEE Cloud Computing, 2016,3(1):18–22
7. Zhou T, Xiangyang G, Hu Y, et al. PindSwitch: A SDN-based protocol-independent autonomic flow processing platform. Globecom Workshops (GC Wkshps) 2013 IEEE. 2013
8. Seugwon Shin, Philip Porras, Vinod Yegneswaran, Martin Fong, Guofei Gu, Mabry Tyson. FRESCO: Modular composable security services for software-defined networks. Proceedings of Network and Distributed Security Symposium, 2013
9. Gartner, The Impact of Software-Defined Data Centers on Information Security, https://www.gartner.com/doc/2200415/