Research and Implementing of Software Defined Border Protection in Hybrid Cloud

Yuxiang Dong  
*China Mobile Group Chongqing Co., Ltd. Chongqing, China*

Wenmao Liu  
*NSFOCUS Information Technology Co., Ltd. Beijing, China*

Linong Zhao, Huijun Zhang & Kun Wang  
*China Mobile Group Chongqing Co., Ltd. Chongqing, China*

**ABSTRACT:** Hybrid cloud is composed of enterprise private cloud and public cloud tenant network. It has effectively reduced construction cost, improved enterprise IT construction efficiency and expansibility of private cloud, and brought security risk such as fuzzy boundary at the same time. This thesis studies the common access control means used in current hybrid cloud and has proposed a unified strategy control mechanism to address hybrid cloud. By applying software-defined network and network function virtualization, the mechanism has succeeded in multi-granularity of flow in east-west direction and in north-south direction of virtual network, realized internally unified access strategy, and improved the efficiency and flexibility of access control.

**Keywords:** hybrid cloud; access control; micro-segmentation; software-defined security; software-defined network

1 INTRODUCTION

In recent five years, Internet has witnessed huge changes. New IT infrastructure and applications have accelerated global informatization, such as cloud computing, big data analysis, and mobile Internet. Among enterprise users, 26.1% have set cloud computing as their investment priority while 27.4% small and medium-sized enterprises prefer to choose software-defined data center as their investment priority in the next 12 months [1]. It is very likely that these enterprises will combine physical IT system in officer environment with virtual private cloud in public cloud, so as to form hybrid cloud. Moreover, many enterprises have introduced employees’ devices for office automation. In this way, Bring Your Own Device can be combined with cloud computing information system, and thus can greatly improve office efficiency.

Chongqing Mobile has conducted research work on hybrid cloud and established Hybrid Cloud for enterprises which can effectively reduce construction cost and improve the expansibility of private cloud. However, popularization of cloud platform can cause more serious data leakage and network attack risks, such as various threats in management and data security of network, host, and virtual resources. In particular, hybrid cloud mentioned above can obscure the boundaries among different IT systems within enterprises. BYOD can obscure the boundary between physical devices and logic assets. As a result, all security defense devices and security mechanisms relying on boundary can almost lose all efficacies. It seems attackers can always find a place where physical boundary discords with logic boundary to invade. Even if cloud system constructers have made consistent boundaries in initial plans, these boundaries may expire and lose efficacy with the movement of virtual resources (such as migration of virtual machine). Thus, attackers will be able to bypass these boundaries. In short, traditional defense means can be used for existing investment while software-defined fast-reconstruction of boundary shall be applied when any new security problem appear in Hybrid Cloud. All these are problems demanding prompt solution.
2 RELATED WORK

Gartner first proposed Software Defined Security [2], and emphasized to abstract the bottom layer as resources in security resource pool. The top layer shall be unified through software programming into intelligentized and automated business schedule and management, so as to complete corresponding security functions and realize flexible security protection. Since then, combination of software definition and security has become frontier development hotspot in the industry.

Among studies around boundary protection, there are several models having appeared in this area, such as Software Defined Perimeter (SDP) from CSA [3]. It suggests a structure similar to SDN that has centralized controlled SDP controller. Any access between any two nodes of the system will need authorization from the controller. In this way, global centralized control can be realized. Besides, all strategies are flexibly determined by the top-layer controller software. Gartner also proposed an Adaptive Access Control [7] model emphasize on control of context access. If no abnormal situation occurs, access strength can be properly lowered; otherwise it shall be enhanced. This model became one of the ten 2014 Gamter technologies due to its difference from previous Role Based Access Control (RBAC) [4] and its capability of analyzing context and risks so as to improve the flexibility of control.

Besides Adaptive Access Control, some work are also related to risk analysis based on RBAC model, such as [5] using partial ordering relation of security to express ongoing accesses and using independent risk assessment program to manage these accesses. [6] A risk-perceptive RBAC model is proposed based on these risks to provide clearer authentication semantics and richer access control decisions than RBAC. In some work, new models different from RBAC are also applied, such as Attribute Based Access Control (ABAC) [8] which can make flexible decisions through various attributes of authentication main bodies and accessed objects.

In short, various access control models can synthesize access control of resources inside decision system through various factors of main bodies, objects, and environment. However, situation in hybrid cloud is more complicated, and thus it requires for access control model with higher flexibility, fine control strength and centralized control.

3 ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT

Information system network of hybrid cloud computing includes physical network of cloud computing, virtual network in virtualized system, and customer’s original system network. Therefore, access control must cover the unified decision of the network combined by internal virtualized environment, cloud computing system, and original system.

3.1 Access control of virtualized internal network

This sector will take micro-segmentation and firewall as examples to introduce the latest access control mechanism inside virtualized environment of cloud computing system.

3.1.1 Micro-segmentation

In traditional data center, boundary is generally divided by business area as shown in Figure 1(a). Same or similar businesses are deployed in different physical areas and firewall is applied for connection between areas. Hence, access control works on these area boundaries. If DMZ area is assumed as unsafe in security domain division, Web access and APP will be arranged here and rules for access to this area are relatively loose. However, for important areas such as database DB area which stores important data, corresponding security level is higher and rules of access are stricter.

Attackers always use hostile attack to obtain access to Web server. Unless access control of firewall is reasonable, it is hard for attackers to enter the area where database is arranged.

Nevertheless, security domain division may be divided by tenant in data center under cloud environment. Therefore, the most common access control mechanism is to realize access control on tenant’s boundary after accomplishing tenant isolation, so as to stop hostile attackers obtaining unauthorized access to other tenants as shown in Figure 1(b). But there’s another problem. If boundary of access control only exists between tenants, for a given tenant, for example maintainer of ERP system, his web and database can only be stored in tenant’s internal system. That means there’s no access control mechanism between DMZ domain and DB domain. If any attackers can break this tenant’s Web server, it will be very easy for him to visit database server. Hence, there’s serious hidden security danger in this access control mechanism.

As an idea to solve access control of east-to-west flow, Micro-Segmentation has been proposed in recent years. Its core lies in allowing several virtual machines in tenant network to divide a segment and then arrange access control mechanism on the boundaries among these segments. As segments are flexible, a segment can be a virtual machine, and can also be a collection of several virtual machines which can satisfy some condition. Therefore, several micro-segments can be divided as required in one subnet. Then, security strategies will be deployed on segment boundaries of these micro-segmentations. What is different from traditional boundary division is that micro-segmentation can be any part of a virtual network. If any security strategy can be deployed between mi-
micro-segmentations, flow in two-layer network can be monitored.

![Diagram of traditional boundary division and micro-segmentation](image)

(a) Traditional boundary division

(b) Boundary division in cloud environment

Figure 1. Comparison between traditional security domain and micro-segmentation.

3.1.2 Firewall as a service

Firewall as a Service (FWaaS) is an access control security service (Shown in Figure 2). It can issue security strategy to firewall through application interface. Different from micro-segmentation that controls flow in east-to-west direction, FWaaS mainly controls flow in south-to-north direction, meaning access to cross-network segment.

Openstack defines a set of API for FWaaS to manage control service and its strategy. It can be used in automated service launch. In the meantime, after universal application is realized, tenant’s flow can be isolated by Namespace through network nodes. IP-TABLES is applied inside Namespace to control NAT router and access. As FWaaS only set rules for API, a third party is allowed to deliver hardware or software access control service through different bottom layers.

3.2 Control of cloud physical network

Besides internal virtual network, cloud computing network also has physical network between internet and virtualized systems, especially the connection to management network of physical network. Behaviors of access to these areas must be under strict control. Moreover, in normal VPC situation, Virtual Middlebox can be used to construct FWaaS, so as to complete access control to flow in south-to-north direction under virtual environment. In some large-scale scenes, NFV technology is not enough to support mass flow load in single network and hardware firewall needs to be deployed.

In physical network of cloud environment, firewall can virtualize several virtual firewalls (vFW) inside device. Each vFW can be connected to a tenant and accomplish tenant isolation. As shown in Figure 3, firewall is connected to computational nodes in virtualized environment through tunnel, and can virtualize two vFWs inside to respectively deal with two tenants’ flow in virtualized environment.

![Diagram of access control based on hardware virtualization](image)

3.3 Unified strategy control of hybrid cloud

In Hybrid Cloud, if combination of customer’s original system and cloud computing system appears, sev-
eral physical and virtual networks are there. How to unify strategy control of these networks and how to reduce the attack surfaces of customer’s original system or cloud system are very important directions for research. On one hand, we need to synthesize network environment and give unified strategy; on the other hand, we need to flexibly deploy flows to pass multi-layer security check through service chain.

3.3.1 Overlay network access control

In current hybrid cloud, a common deployment mode is to connect customer’s original system and cloud system through tunnel technologies such as VPN. Figure 4 shows a classic Overlay network of hybrid cloud. Physical gateway/firewall FW1 of Tenant A’s enterprise network is connected to Tenant A’s virtual router/firewall FWaaS1 through tunnel technologies such as VPN and gateway of public cloud. Firewall of physical gateway in cloud system FW2 is connected to management system of cloud system and virtual gateway/firewall FWaaS of each tenant. Therefore, if access control strategies need to be unified and deployed, consistent rules shall be set for user’s enterprise network gateway, physical cloud network gateway, tenant’s virtual gateway, and firewall on micro-segmentation of tenant’s virtual subnet:

1. Rules for Tenant A’s enterprise network firewall FW1 and virtual firewall FWaaS1 shall be consistent.
2. Enterprise network firewall FW1 shall be connected to enterprise BYOD authentication system, so as to ensure devices in public wireless network can provide corresponding identifications and can only offer access to authorized cloud VM.
3. Physical cloud network firewall FW2s shall guarantee the control of isolation between network and data network. Flow from internet to cloud management network shall be under strict control especially.

(4) Users need to divide corresponding micro-segmentations according to business, and control flows in south-to-north direction in tenant’s enterprise network and flows in east-to-west direction between different micro-segmentations through FWaaS1 and security groups. Strict limit must be set on flows in DB sections.

3.3.2 Service chain

Service chain refers to using SDN and NFV in conducting different check and protection when any flow passes through several security devices. For example, in access control situation, RBAC or ABAC is used to set rules traditionally. However, context perception is not sufficient in general. When any threat occurs, it’s hard to regulate and control rules rapidly.

In cloud environment, attacks can happen in a very short time. Thus, strategy regulation needs to be done fast. Through service chain, various virtual DPI Security devices can be deployed in virtual or physical locations as required. Flows will pass through several devices from upper layers. When DPI device finds any suspicious attack, it can inform firewall to make timely adjustment and control over the suspicious flow.

4 ACCESS CONTROL UNDER HYBRID CLOUD AND BYOD ENVIRONMENT

As described above, BYOD environment exists in user’s enterprise, various mobile devices need to use cloud services. How to complete access control outside BYOD and other traditional boundaries will be a very important issue in future hybrid cloud security.

4.1 System design

Structure of the whole system is shown in Figure 5. Network structure can be divided into three parts:
enterprise network, internet, and cloud system network among which:

Enterprise network includes:
1) SDN switch. It is connected to wireless router deployed in physical environment through bridging. Internet is also connected to get through tenant’s virtual gateway in cloud environment by tunnel.
2) Authentication server. It is used to provide authentication support for employee’s username and password in LDAP and database under enterprise environment.

Cloud environment network includes:
1) Tenant’s virtual gateway. It is connected to enterprise network through tunnel. At the same time, it can provide router and three-layer access control service for internal virtual network of cloud environment.
2) Micro-segmentation. It is used inside virtual subnet to provide two-layer access control service.
3) NFV, firewall, IDS and other application-layer firewall. They can provide control mechanism in DPI and behavior layers.

There’re two parts in the main flow: user authentication and access control. The former part is to use SDN technology in introducing HTTP flow into authentication service, so as to realized user access authentication in global network. The later part is to deploy unified access control strategy according to users in enterprise network and cloud environment.

In initialization phase, SDN controller sends the following OpenFlow orders to SDN switch in (1):
1) Allow all data packages of DHCP and DNS.
2) Introduce all HTTP data packages into authentication service in (2).
3) Reject all the other data packages.

During operation, after users connect wireless router, all HTTP websites they visit through browser will be redirected to authentication server. The server will rewrite the request page as authentication page. For example, http://www.a.com/hello.php?key=value will be rewritten as http://auth.server/login?key=value. By this mean, users can enter their usernames and passwords for authentication on the page. Theoretically, all protocols can be supported after authentication and original authentication service of enterprise can be compatible.

After users complete authentication, SDN controller will regard this terminal as authorized in strategy library and send the following OpenFlow orders in the meantime:
1) Set the treatment for flow sent from authorized user’s terminal as action=CONTROLLER.
2) Next time, the data package sent from this terminal will firstly be delivered to SDN controller. The controller will judge:
   a) If destination address is normal virtual machine in internal network of cloud environment, it shall pass. According to security strategy, the flow can pass through several security devices described in (5).
   b) If destination address is internet, it shall pass.
   c) If destination address is internal network server of enterprise or important resource of internal network in cloud environment, the access to the resource shall be judged according to authorized user’s identification.
3) SDN controller sends the treatment result of the flow to related network devices. Then, the devices will deal with all data packages following the flow.

Figure 5. Schematic diagram of access control under hybrid cloud and BYOD environment.
4.2 Adaptive access control mechanism

In many APT attack situations, hostile attackers use social worker or Trojan horse to obtain user identification. They can bypass boundary check mechanism and have access to internal resources. In this situation, only relying on ACL is obviously not enough to defend these advanced directed attacks.

Therefore, Adaptive Access Control proposed by Gartner can help solve the problem. In the situation described in this thesis, we deployed many kinds of defense devices after virtual routers are set as required by applying SDN and NFV technologies, so as to form a service chain. For example, we introduced IDS to complete check on payload. After data is checked and enters the next sandbox, behavior related to the data will be checked in virtual operation. When any security mechanism sends an alarm, current security level can be adjusted higher, so as to offer limit or even stop related access control.

In the structure described in 4.1, after user is authenticated, software defined access control can still be aware of the security level of the environment by context sensing. When any suspicious attack is found in the DPI or behavior analysis engine described in (5), security system will make access control strategies stricter through SDN controller; otherwise, it will adjust it to a looser level. In this way, adaptive access control can be realized.

5 CONCLUSIONS

Hybrid cloud can integrate internal enterprise network and public cloud into a complete information system so as to improve working efficiency. However, it can also change the traditional division of security domain and increase attack surface at the same time. This thesis applies SDN and NFV technologies. Through software-defined principle, it has succeeded in unifying the access strategy of Overlay network, administrative network, and internal enterprise network; and has realized the control of multi-granularity of flows in east-west direction and in south-north direction of virtual network. It can also conduct multifaceted examination on quintuple, data package payload, and behavior through service chain, so as to realize self-adaptive access control at last.

REFERENCES