International Conference on Industrial Technology and Management Science (ITMS 2015)

A Secure Architecture for Public Cloud Data Independency based on Virtual Private Cloud

Yingzhao.YAN
Beijing University of Posts and Telecommunications, Beijing, China

Baohui.LI
Beijing University of Posts and Telecommunications, Beijing, China

ABSTRACT: With the expansion of enterprises, more and more cloud infrastructures become widely used by enterprises. Public cloud service from third party can be accessed using internet. As a result, data is transmitted to the shared server. If there’s not a very good way to isolate different organizations, the information especially the critical sources may leak. In this work we focus on insecure data, intrusion in public cloud and in order to resolve this issue, we proposed a secure architecture called “one-control” based on virtual private cloud to improve data security. We discuss the structure of “one-control” and communications within and out of the system that separate different enterprises’ cloud logically. Driving each enterprise to an independent VPN (virtual private network), communicated by a secure channel provided by open flow routers. As a result, we realize logical isolation and improve data safety in public cloud.

KEYWORD: VPC; VLAN; VPN; cloud computing

1 GENERAL INSTRUCTIONS

Cloud computing describes system platform or a type of an application. At present, Amazon, icrosoft, Google, IBM, Intel and other companies have put up enterprise cloud platforms such as Amazon web services (VARIA, 2009), IBM “bluemix” (IBM, 2013), and google file System (GHEMAWAT S & GOBIOFF H'LEUNG P T, 2003). Because of cloud computing’s reliability, high availability, and transparency, it has widely adopted by many companies. Without hardware reliability components’ support, cloud use the data redundancy and distributed storage to ensure the reliability of data. It was developed based on distributed computing, virtualization and grid computing. Enterprise users can significantly reduce the computing storage and maintenance costs.

With the development of cloud computing in academy and industry, it may inevitably bring many security problems. In cloud computing, users lose control of data and computing operates in the cloud server so that clients don’t know whether the data is protected or the computing task is performed correctly. In a public cloud, a large number of customers can lease cloud resources and even infrastructures, and that lead to inevitable communication and data sharing among clients.

Gartner survey shows, more than 70% CTO will not using cloud computing with the primary reason of the data security and privacy concerns. In August of 2013, the internal file of some Japanese enterprises including Honda and Panasonic was leaked in a Chinese search engine service, even including a car images not released and sales materials. Only if those companies are using private cloud service, can the information keep secretly. However, that would cause high expense.

In this work, we propose an infrastructure named “one-control” which is based on VPC (virtual private cloud) to create a flexible and secure cloud services transparently connected to client’s VPN (virtual private network). In this way, we isolate the organizations logically. “One-control” gets those targets by controlling in a controller domain and providing secure network services.

2 RELATED WORK AND RESEARCHES

2.1 *Security in commercial platforms*

At present, the mature cloud computing products are Amazon Web Services (Amazon, 2012) and Windows Azure (Microsoft, 2012). Amazon Web Services belongs to the cloud infrastructure, providing convenient access to computing, storage and network resources for clients. Windows Azure belongs to Paas (platform as a service), making customers publish applications rapidly using Azure platform.

Amazon web service mainly provide EC2 (Elastic Compute Cloud) services (Amazon, 2012). In EC2, safety protection includes hosts operating system security, client’s operating system security, firewall and API (Application programming interface) protection. Security at the host end is based on physical machine itself and administration management. At clients end, security is based on completely controlling a virtual instance, using “token” or “key” identification to access non privileged account. In addition, customers are required to build a log for elevation mechanism, and generate a unique key for themselves. In the firewall, it uses the default mode, making network communication restricts from protocol, service port and IP source address. API protection refers to all API calls needs X.509 certificate or customers’ Amazon secret key to access with SSL (secure sockets layer) encryption. In addition, different instances on the same physical machine are separated by Xen monitoring application.

Windows Azure provides Paas cloud (Microsoft, 2012). In the confidentiality aspects, Windows Azure provide a self-signed digital certificate authority, least client authentication software, the internal mutual communication control based on SSL, certificate for controlling program hardware devices, Windows Azure document storage access control mechanism etc. And provide clients’ VM isolation from VM supervision procedures, Fabric controller separation, packets filtering by group, VLAN isolation and customer access separation mechanism. In addition, .Net service enable the customers easily realize the encryption, Hash key and cipher code management function in the data storage and transmission.

In this work, we focus on security of data. Since clients share the storage and resources in public clouds. Security technology usually consists of authentication technology, encryption and secret key management. Authentication technology prevents the data to be forged and tampered. Encryption protects data codes from being broken. And the secret key management ensures the transmission of the secret key.

3 VIRTUAL PRIVATE CLOUD (VPC)

3.1 *Virtual private network (VPN)*

Generally, VPN basically works under a situation that the host sends the message to a connected VPN devise as following. VPN equipment encrypts on the entire package and a digital signature at the head of data, including safety information and some initialized parameters required by the VPN destination. VPN equipment encapsulated encrypted data. Then the packages were passed by the virtual security channel through Internet. When Target VPN device receives the data packets, they unlock the data package, check the digital signature and get the plaintext information. After the processing, only the sending and receiving end user can read the information from channel, while other clients cannot get the correct information so that we can ensure the security of data transmission in public network.

3.2 *The concept of Virtual Private Cloud*

Virtual Private cloud is built for a certain enterprise or a single organization, so this kind of architecture provides security data and better QoS. Cloud service provider is responsible for building a system and support in the running period. It is a concept based on VPN. Different customers have their own VPN, but share public cloud storage. Virtual private cloud separate the customers logically, even they are sharing the storage physically in the same public cloud. It seems that the storage was divided into several groups belongs to each enterprise and communicated in a safe way.

3.3 *The advantage of VPC*

The advantage in using VPC is as following.

1) Data is secure, generally building fire wall to enterprises VPN. It prevents the invasion of hackers and external threat effectively.
2) Data transport with high quality and low cost when visiting a VPC application, regardless of public network.
3) Make full advantage of hardware and software resources in enterprise.

4 ONE-CONTROL ARCHITECTURE

Timothy Wood propose CloudNet(Wood T et al. 2009) system for enterprise. It is an application of VPC in public cloud for enterprise. We are designing a system called “one-control” which expected to optimize the monitor and control mechanism in the VPC system.

4.1 *One-control architecture overview*

In Order to meet the controlling request, “one-control” architecture based on VPC is proposed in this work as Fig 1 demonstrates. From the concept of fig1, enterprise VPC is based on IT infrastructure. The computing resource and the network is defined and controlled by controller domain. Enterprise VPN and data are belongs to controller domain too. Controller domain is responsible for all the interface association and network scheduling.

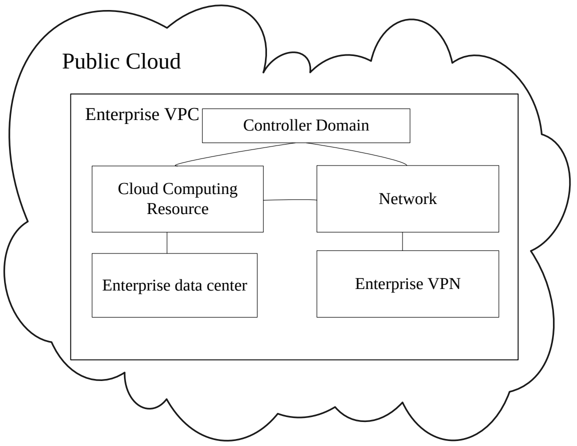

Figure 1. Logical structure of "one-control"

As shown in Figure 2, an example elaborates "one-control" idea further. Fig 2 described two enterprises establish virtual private cloud. The provider distributes each enterprise the virtual computing resources (such as virtual machine VM). Realize the isolation and network interaction by VLAN (virtual local area network) shown as V1 and V2. Two parts of VPC represents the 2 enterprise private network. The routers in this architecture were replaced by routers that supported openflow protocol, which means all the network deployment can be done by a single server—"controller domain". It means that although all the cloud resources are deployed in a public cloud, with the isolation mechanism can they realized data independence and data security. From the respect of controlling, clients can directly deploy the cloud resources and physical memory.

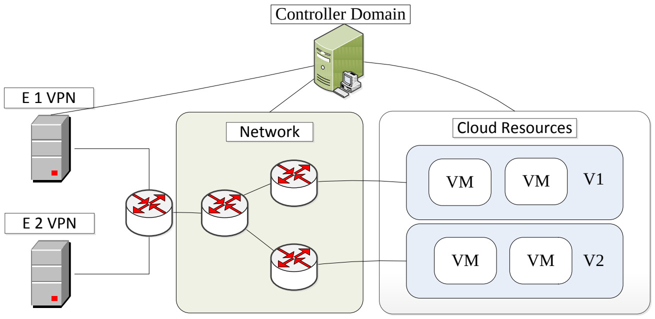

Figure 2. Enterprise VPC architecture example with "one-control"

4.2 *The advantage of "one-control"*

Many enterprises have used VPN before so that cloud instance can be easily added to the architecture as a secure part. In this system we chose strategy based VLAN division for its feasibility, availability and also automatic configuration. This kind of VLAN would connect all the related clients in logic. Network administrator only needs to make the rules for partition using network management software. Once a new instance is added in the logical VLAN, software would recognize the client and put the machine into correct VLAN. At the same time, VLAN could trace the change of location automatically. Routers support openflow protocol can be used for communication among those VLANs. In "one-control", VPN realized via specific channel through telecom network. As shown in Fig3, enterprises' resources are separated by VPC in different clouds. Network topology is maintained by controller domain. Since the routers and switches support openflow protocol. They are controlled only by controller server and as a result, the network architecture is opaque to clients.

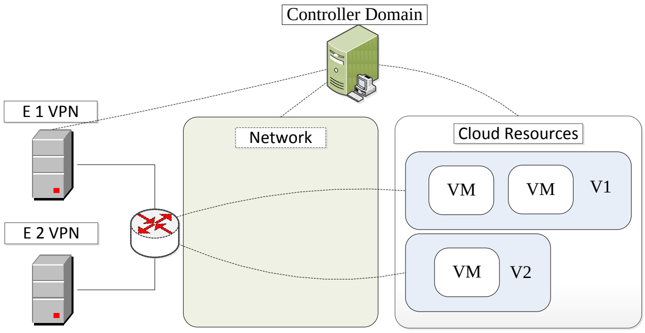

Figure 3. Network realize in "one-control"

As a result, clients don't have to maintain the network except ensure that their data is safe. Moreover, building a system like "one-control" can dynamically change the network distribution when the network damage by controller server. Especially when the data has to migrate, clients just need to apply a change. Then controller can change the topology in advance for the new network. All of these will decrease the work of web master and improve the feasibility of the architecture.

5 CONCLUSIONS

Public cloud has been used by many enterprises by its feasibility, availability, and flexibility. How to keep every client's resource isolated logically is a key function that cloud service provider should be taken into consideration. Virtual private cloud is the trend in networking because it can be maintained simply by operating in software. We propose "one-control" system to realize a simple-controlled network and data isolation in public cloud. And with the help of openflow routers, clients would control the network easily because they only have to configure the connection without designing architecture.

REFERENCES

[1] Amazon web Services. http://aws.amazon.com/ 2012-10-07

[2] Amazon. Amazon Elastic Compute Cloud 2012 *http://aws.amazon.com/ec2/.2012-03-15/2012-10-08*

[3] GHEMAWAT S & GOBIOFF H'LEUNG P T. The google file system[c] *Proceedings of the 19th ACM Symposium on Operating Systems Principles New York: ACM Press 2003:29—43*

[4] IBM. IBM bluemix service *http://www.ibm.com/developerworks/cloud/library/cl-bluemix-dbarnes/ 2013*

[5] Microsoft. Windows Azure *http://www.microsoft.com/windowsazure/2012-10-07*

[6] VARIA J. Cloud architectures-Amazon Web services *http://acmbangalore.Org/events/monthly-talk/may-2008 cloud-architectures -amazon--web -services.html 2009*

[7] Wood T, Gerber A, Ramakrishnan K K, et al. The case for enterprise-ready virtual private clouds. *Usenix HotCloud, 2009*.