3d security and virtualized collaborative Network Security in Cloud Computing

[1]Sowmya B, [2]Swathi S
M.Tech, CSE, KIT, Tiptur
[1]sapnavasavi@gmail.com, [2]sowmyabnaik@gmail.com
[3]*Mr.Santhosh S*,Asst Prof. CSE dept. KIT,Tiptur santhukit@gmail.com

***Abstract*:-A data center is an infrastructure that supports Internet service.In this scenario, multiple tenants save their data and applications in shared datacenters, blurring the network boundaries between each tenant in the cloud. In addition, different tenants havedifferent security requirements, while different security policies are necessary for different tenants. Networkvirtualization is used to meet a diverse set of tenant-specific requirements with the underlying physical network, enabling multi-tenant datacenters to automatically address a large and diverse set of tenant's requirements. In thispaper, we propose the system implementation of vCNSMS, a collaborative network security prototype system usedin a multi-tenant data center. We demonstrate vCNSMS with a centralized collaborative scheme and deep packetinspection with an open source UTM system. A -security level based protection policy is proposed for simplifyingthe security rule management for vCNSMS also 3d security.**

I. INTRODUCTION

A cloud data center is an infrastructure that supports Internet services. The debut of VMware NSX provides the virtualization of networks with Software-Defined Network (SDN) inside a data center. The Google B4 network also uses an OpenFlow-based SDN to implement all the interconnections among cloud data centers in different locations. The challenge posed by SDN is the dynamic characteristic of network boundaries that is the "twin" of the network topology with expanded flexibility provided by virtualization. In other words, the original static, natural, and physical boundaries within the traditional network are
replaced by the dynamic and virtual logical boundaries of SDN.

A. State-of-the-art network security in data center networks

- In multi-tenant cases, the network boundaries are blurring. How to ensure network security is a challenge in such a complex network environment.
- The deployment location of Middleboxes also has new changes.How to properly deploy these security devices is also an important issue.
- Security requirements for different tenants are different.how to provide effective enforcement important issue.
- The migration of the virtual machine results in the switchover of security domain.How to protect the apping of the security policies from the logical network to the physical network and maintain its correctness and consistency will be a major challenge to the control function of a data center network.

B. Software-defined network in data center network

To enable network virtualization, SDN is one of the supporting technologies to build cloud data center virtual networks. Cloud data center virtual networks need to ensure tenants' security domains have complete and isolated network boundaries. This is not a simple network security technology, because the virtual network itself provides services for multiple tenants or basic virtual private cloud services that should be guaranteed in the implementation of the network. Due to the different virtual machines of different tenants sharing the same physical resources, system security guarantees such as preventing the virtual machine from escaping its boundaries are also the issue of network Virtualization security.

II. RELATED WORK

A. Network security in data center networks

Among the security research in data center networks, SDN security is a hot topic both for academia and industry.
FRESCO [1] introduces a new security application development framework. It is used to solve several key issues when implementing security service components on demand.

SIMPLE[3] allows network operators to specify routing policies in a logical Middle box[3], and automatically update forwarding rules according to the physical topologies, switching capacity, and resource constraints of Middle boxes to guide traffic to the proper Middle boxes queues.

B. Network virtualization with VMware NSX

The core components of VMware NSX are logic switches, logical routers, NSX APIs, logical Firewalls, logical load balancing, logical VPN, etc. NSX provides a network virtualization approach.. The overall structure of NSX is shown in Fig 1.

Fig. 1 Network virtualization platform of VMware NSX.

The scalability in NSX provides services of other network security vendors. The NSX platform uses a distributed service framework that allows multiple hosts to integrate the network service, and can easily insert new service modules using the NSX API.

III. vCNSMS

In this section, we propose vCNSMS; a collaborative network management prototype system derived from CNSMS for multi-tenant data center networks. In our experiments, we demonstrate that vCNSMS can be integrated into virtualized cloud environments.

The principle of collaborative network security in DCN

A. Basic network topology

Figure 2 shows the vCNSMS configuration and the registration process in the bootstrap stage[2].

B. Collaborative security in DCN

- Security center interacts with the peer-UTMs

1) Security Center issues rules: There is a help option for rule creation and an option for the rule issued, in web User Interface (UI).
2) Peer-UTM reports events: The Security Center needs a web interface to display the security events reported by peer-UTMs.
3) Events inform between peer-UTMs: There is a web-based UI in the peer-UTM collaborative security module.

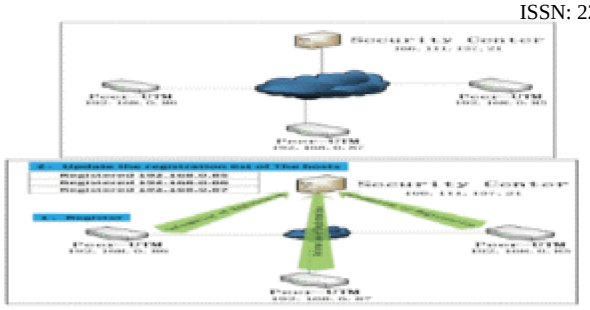

Fig. 2 vCNSMS configuration settings and registration process in the bootstrap stage.

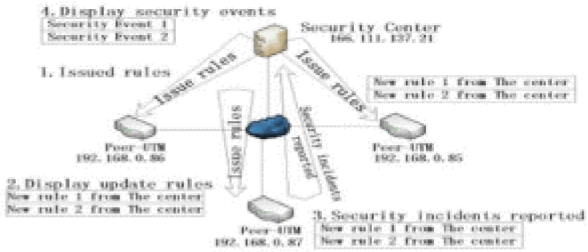

Fig. 3 Security rules issued.

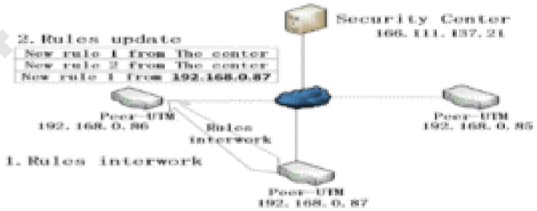

Fig. 4 Security rules interwork.

C. Antivirus module in collaborative security

Workflow of Antivirus module is shown in Fig. 5

Fig.5 Workflow of signature database updating in Antivirus module.

(1) The Security Center imports the virus signature db.
(2) The Security Center issues the virus signature database. 3) An interface displays that the virus database has been updated: The time changes.
(4) Virus signature database synchronization between peer-UTMs is performed using the p2p mode.

- Firewall module in collaborative security

Workflow of Firewall module is shown in Fig 6.

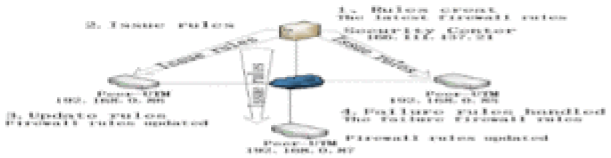

Fig. 6 Workflow of rules issuing to Firewall module.

(1) Importing Firewall rules to Security Center: The option of importing Firewall rules to the Security Center.
(2) Security Center issues the Firewall rules: The option of issuing the Firewall rules.
(3) Interface displays that the Firewall rules have been updated: There is a web UI in the peer-UTM collaborative security Firewall module..
(4) The peer-UTMs choose to implement the rules that are updated by the Security Center:

- Protocol control and content matching module in collaborative security

  Functions and principles are the same as Section 3.1.2.3

.

D. Security rule center

The security rule center in security center runs on Debian Linux, and includes a rule distribution module and an event alarm module.

The rule distribution module is divided into server and client, and the server program is a socket communication module written in Java that is manually activated in the Security Center. The client program is running in the peer-UTM Firewall and Rules control module. When the server and client programs are running normally, the Security Center can quickly transfer rules in a specific folder to the peer-UTM's rule control module.The event alarm module is a web application based on Apache Tomcat that opens port 443 for this service. It listens for any security event reported from the peer- UTM, and dynamically displays these on the web UI.

E. Virtualization network based on SDN

An experimental platform based on Openflow SDN is shown in Fig. 7, and the detailed configuration is shown in Table 1.

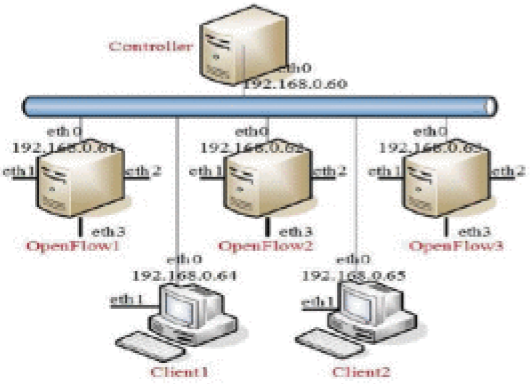

Fig. 7 Virtualization network based on SDN.

VMs	IP	Hostname	Host alias	System
Controller	192.168.0.60	Saimo-controller	Control	Ubuntu 13.10 (floodlight)
OpenFlow1	192.68.0.61	Saimo-openflow1	OF1	Ubuntu 15.04
OpenFlow2	192.68.0.62	Saimo-openflow2	OF2	Ubuntu 15.04
OpenFlow3	192.68.0.63	Saimo-openflow3	OF3	Ubuntu 15.04
Client1	192.68.0.64	Client1	Client1	Ubuntu 15.04
Client2	192.68.0.65	Client2	Client2	Ubuntu 15.04

Table 1 Detailed configuration settings in virtualization network based on DN.

Network topology and the host IPs are allocated in the following 2 rules[4]:
(1) Each virtual machine is bridged to eth0 (192.168.0.0) segment for easy ssh control.
(2) Another controller is also present in this section and controls Openflow switch communication.

Here are some details of the set up deployment.
(1) In Openflow 1.0, there is only a single userspacedatapath. (2) Ofdatapath is the implementation of a datapath. It is responsible for forwarding packets based on the flow table and communicates through ofprotocol and floodlight.
(3) Ofprotocol is a middle program that controls ofdatapath and is controlled by floodlight.
(4) dpctl can still be used to view the flow table in the Openflow switch, but cannot be used to manage the datapath.
(5) To change the behavior of the Openflowswitch, the component (C or python) must pass through floodlight, and the component will be loaded with floodlight.

Deep security check in vCNSMS

- *Function settings*

The Security Center, centrally manages security rules, collects the feedback information from the rule deployment, and stores the data into the security log.

(1) Security rules are incrementally downloaded.
2) Firewall module. Firewall rules will be downloaded from the Security Center and loaded in the Firewall module.
(3) UDP content filtering module. It blocks or drops the specified types of data packets under the current rules.

- *Enhanced security functions*

Protocol Control module in the prototype system mainly enforces UDP protocol rules.

(1) UTMs routinely update rules. UTMs regularly obtain Firewall rules.
(2) Filtering based on the content of a UDP packet.

(3) Blocking function with a blacklist. Block rule based on "quintuple" filtering". The Firewall module can quickly apply the update rule.

- *Implementation in peer-UTM*

(1) Update Firewall rules. The administrator puts a new Firewall rule file in the specified folder FirewallRule in the Security Center. The corresponding rules are then downloaded to the local rule database and are activated in real time.

(2) Firewall module blocks a specified network flow. The Firewall module provides a blocking function of rules based on "quintuple" filtering, and sends the corresponding log info to the Security Center through an announcement message too.
(3) UDP content filtering. UDP content filtering module uses the same mechanism as the Firewall module, and has the specified tag indicated in the announcement message. .

3.3 Intelligent flow processing in vCNSMS

Intelligent flow processing is an advanced method for intrusion detection. Intelligent flow processing in vCNSMS is based on the smart packet verdict scheme. In this section, we propose the security level based protection policy for intelligent flow processing in vCNSMS.

3.4. Data classification
The user has to categorize the data on the basis of confidentiality, integrity and availability. Now the user have to give the value of C – confidentiality I – integrity and A – availability. After Appling proposed formula the value of Cr criticality raring is calculated.

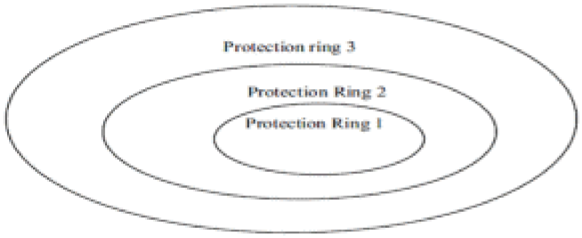

Fig 8.data classification

Now allocation of data on the basis of Cr is done in protection ring. This suggests that internal protection ring is very critical and it require more security technique to ensure confidentiality.

3.5 Dimentional technique for security.

After classification of data in above step, three entity is considered, first one is cloud provider itself, second is organization whose data resides at cloud and last one is employee or anonymous user who request for access of cloud data.

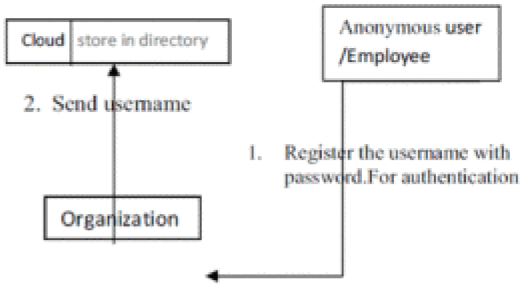

Fig 9 . security

Now the above figure gives overview of first step of second phase, in which if a user (either employee or anonymous) want to access the data if it belongs to protection ring 2 then user have to register itself (if he is already registered need not require further registration), if the data belongs to ring 1 it require strong authentication, if the data belongs to ring 3 then it is public need not require any authentication. Now suppose the user registered itself for accessing data, organization will provide username and password for authentication. At the same time organization sends theusername to cloud provider.

Now the user sends password for authentication, and after authentication it redirect the request to cloud provider to access resource.

3.6 Performance of Shield parallelization

Because of the amount of traffic is throttled from a single IP, UDP packets sent by traffic generator Smart Bit will lead the original Shield to block these packets. To avoid this, we modify Shield to make all packets pass through. The performance measured in this manner should reflect the capability of Shield module.
The test environment is described as follows:

(1) Hardware: Intel(R) Core(TM) 2 Quad CPU Q9400 @ 2.66 GHz, 4 cores, 2GB memory, 8 Gbit ports.

(2) Software: Ubuntu 13.04, Shield untangle module.

(3) SmartBit settings: 4-way UDP streams with different IP and Ports. Packet loss ratio is collected in each experiment. Each experiment is conducted in a 1-Gbps link with varied input traffic ratio from 10% to 100%.

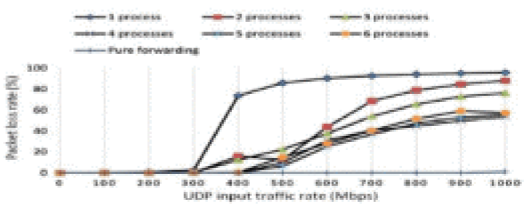

Fig.10 Throughput for smart packet verdict scheme invCNSMS.

As shown in Fig 10, five parallel Shield processes can handle 400-500 Mbps. The CPU usage is about 40%. Memory consumption is quite low. As Shield only deals with the headers of packets in this test, the

performance result is expectable, but it is slower than 0he Snort.

IV. CONCLUSIONS

In this paper, we propose vCNSMS to address network security in multiple-tenants data center and demonstrate vCNSMS with a centralized collaborative scheme. vCNSMS can further integrate a smart packet verdict scheme for packet inspection to defend from possible network attacks inside the data center network. An SDN-based virtualization network in a data center can deploy vCNSMS for flexibility and scalability to protect multiple tenants with different network policies and security requirements. This technique provides a new way to authenticate in 3dimensional approaches. It provides availability of data byovercoming many existing problem like denial of services,data leakage. As additional it also provides more flexibilityand capability to meet the new demand of today's complexand diverse network.

FUTURE WORK

Based on the practical deployment and operational experience gained from evaluating vCNSMS in a data center network, vCNSMSs security center is able to deploy more and more security rules and collect data of network events. It should be possible to detect network policy violations and intrusion with an artificial intelligence based on unsupervised learning methods. This is a promising area for exploration in the future.

REFERENCES

[1] Collaborative Network Security in Multi-Tenant Data Center for Cloud Computing
Zhen Chen_, Wenyu Dong, Hang Li, Peng Zhang, Xinming Chen, and Junwei Cao_ S.

[2] Shin, P. Porras, V. Yegneswaran, M. Fong, G. F.Gu, and M. Tyson, FRESCO: Modular composable security services for software-defined networks, presented at Network and Distributed Security Symposium, 2013.

[3] B. Anwer, T. Benson, N. Feamster, D. Levin, and J.Rexford, A slick control plane for network middleboxes, in Proc. Association for Computing Machinery, Hong Kong, China, 2013, pp. 147-148.

[4] VMware NSX network virtualization platform, http://www.vmware.com/products/nsx, 2013.

[5] [3 Dimensional Security in Cloud Computing
Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan shahi, Ratan Lal *Abhishek Vaish, *Utkarsh Goel
Indian Institute of Information Te chnology, Allahabad U.P India.