ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

Network Security in Data Centre

[1] **Nisha Nandini J P,**
[1] II MSc Information Technology,
[1] Dr N G P Arts and Science College.

Abstract:-

Data Centre is the usage infrastructure for supporting Internet services. Cloud computing is rapidly changing the face of Web Internet service infrastructure, enabling even small organizations to quickly create Web and mobile applications for millions of users by taking advantage of the scale and flexibility of the shared physical infrastructures provided by cloud providers. In this case, multiple users store their data and application in the same data centre with a virtual boundary between each occupant. As every occupant uses their own different security policies, it needs to create different security policies for them. Network virtualization is to compile a diverse set of occupant-specific requirements into a single configuration of the underlying physical cloud network, enabling multi-occupants data centres to automatically address a large and diverse set of occupants' requirements.

Mechanism design and system implementation of vCNSMS, a collaborative network security prototype system in multiple occupants' data centre network. A security level based protection policy is proposed for simplifying the security rule management for vCNSMS. Different security level has different packet inspection scheme and enforced with different security plugins. A smart packet verdict scheme is also integrated into vCNSMS for intelligence flow processing to defence possible network attack inside data centre network.

Keywords: - Network security, Software defined network, Collaborative network security, multi-occupant, Network virtualization

1. INTRODUCTION

The definition of cloud data centre can have a variety of perspective, the most popular one are categorized by IAAS, PAAS, SAAS and public cloud, private cloud, hybrid cloud and some other different categories, but also computing, networking, storage of a system perspective, archiving, transmission from a data perspective. Specific to the cloud network, there are different characteristics of cloud, within a cloud, between clouds network.

A. Network Security in data centre network:

With the development of cloud computing technology, more and more enterprises are moved into cloud as an occupant to take the advantage of scalability and flexibility of the cloud computing. The deployment of middle boxes, such as traditional firewalls, IDS, WAFs in between the inside and outside networks, is facing new challenges in the large-scale data centre network environment.

1. The network boundaries are blurring in the case of multi-occupants

- Multiple occupants put their data in cloud and the same occupant may utilize different servers with multiple backups, making the network boundaries between each occupant become blurred and virtualized rather than traditional physical isolation. The original static, natural physical boundaries within the network, is replaced by dynamic and virtual logical boundaries.

2. The deployment of middle boxes need repositioning
3. Security requirements for different occupant is different
4. The migrations of virtual machines result change in security domain

B. Software defined network in data centre network:

The cloud data centre needs to ensure the occupants or the security domains with complete and isolated network boundaries. Due to different virtual machines of different occupants shares the same physical resource, system security provides prevention from virtual machine escaping.

The core change of SDN is switches, routers and some other forwarding devices forwards according to flow table created by controller, which results in more efficiency and less cost. The controller collects network status information, discovers network topologies, checks the network forwarding policies, generates and updates the flow table. The traditional Packet Filtering Firewall or Access Control List should be deployed to the header so that, the first packet's header of a flow in the controller will not be forwarded to the controller again

Network access control deployed on physical gateway should still arrange to "logical" gateway. Openflow protocols and controllers, network security based on SDN in cloud data centre by setting flow table and guiding traffic that matches the policies, address the problems of Middle boxes deployment and "fragmentation" of security rules. It is possible to optimize the controller by configuration and management, and make rules for dynamic migration and reconfiguration to solve security policy inconsistencies caused by the Middle boxes reposition and the virtual machine migration.

2. COLLABORATIVE SECURITY IN DCN

A. Collaborative security for Antivirus

- Security Centre imports the virus signature database: There is an option to import the virus signature database in Security Centre and disseminate them to peer-UTMs.
- Security Centre issues the virus signature database: There is an option to issue the virus signature database in Security Centre.
- Interface displays the virus database has been updated in PEER-UTM: The time stamp or version number changes.
- Virus signature database synchronization among peer-UTMs, which use p2p mode.

B. Collaborative security for Firewall

- Importing Firewall rules to Security Centre: The option of importing Firewall rules to Security Centre.
- Security Centre issues the Firewall rules: The option of issuing the Firewall rules.
- Interface displays the Firewall rules have been updated: There is a web panel in peer-UTM collaborative security module. The web panel shows the new Firewall rules have loaded in.
- The peer-UTM chooses to apply the rules which are updated by Security Centre: In the display panel of the update rules, the peer-UTM can also invalid some rules as required.

3. VIRTUALIZATION BASED ON SDN

Network topology and host's IP allocated as follows, each virtual machine is bridged to eth0 192.168.0.0 segment for ssh control. Controller is also through ssh to communicate with openflow switch. In openflow switch, there are three Ethernet ports, which can be connected according to the experimental needs. Each client has an Ethernet port that can be connected to any openflow switch according to the experimental needs.Block rule based on the "quintuple". Firewall module can quickly apply the

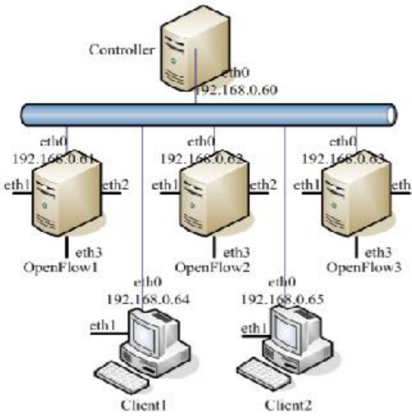

Figure-1 Virtualization based on SDN

4. DEEP SECURITY CHECK IN VCNSMS

A. Function settings

Security Centre, centrally managed security rules, collect the feedback information from the rule deployment, and store them into the security log.

1. Security rules are incrementally downloaded.

❧ The current rule set and temporary rule set is implemented. In the Security Centre, remove the duplicate rules in new rules. The new rule set will be added in a package and issued to the peer-UTM.

2. Firewall module.

❧ Firewall rules will be downloaded from the Security Centre and activated in the Firewall module, and the corresponding function will be achieved. Security events are collected and feedback to the Security Centre.

3. UDP content filtering module.

❧ Block the specified types of data packets matched with the specified patterns.

B. Enhanced security functions

The Protocol Control module in the prototype system to achieve the instant loading patterns and pattern matching for UDP protocol is modified.

1. UTM routinely update security rules.

❧ UTM regularly obtain and utilize configuration information of Firewall rule from the specified server. The configuration information includes the rules of content inspection of UDP and the blacklist based on “quintuple”.

2. Filtering based on the content of UDP packet.

❧ According to the rules, the packets which contain specified features will be blocked

3. Blocking with blacklist

C. Security Level based Protection Policy

The security level based protection policy is described as:

1. Security level settings are indicated by Red, Yellow, Orange and Green.

2. Intelligence network flow processing

❧ According to the security level setting, different security rule set and packet verdict scheme are used with the consideration of different performance and load requirements.

3. Multi-function security gateway Peer-UTM can configure different security plugins on the demand of security level, and incurs different processing costs. Working mode of peer-UTM is also divided into Red, Yellow, Orange and Green.

D. Smart packet verdict scheme with untangle Shield:

Shield is a module of untangle, which function is to prevent DDoS. Shield reads a packet from nfqueue, and starts four threads, including a main thread, an event dispatch thread, an admission packet processing thread and a frontend microhttpd daemon. The main task of shield is to collect packet

processing thread, and there is no parallel structure in the origin Shield implementation.

CONCLUSIONS

The usage of vCNSMS to address network security in data centre network with multiple occupants and vCNSMS with centralized collaborative scheme is explained.

vCNSMS can further integrate intelligence packet verdict algorithm for smart packet inspection to defence possible network attack inside data centre network. SDN based virtualization network in data centre can deploy vCNSMS for flexibility and scalability to protect multiple tenant with different scrutiny policy and security requirement. The smart packet verdict scheme can be used for deep defence in data centre network.

Future work

As the practical deployment and operation experience of vCNSMS in data centre network, vCNSMS Security Centre can collects more and more security rules and its events. It is possible to detect network policy violation and intrusion attack with AI (artificial intelligence).

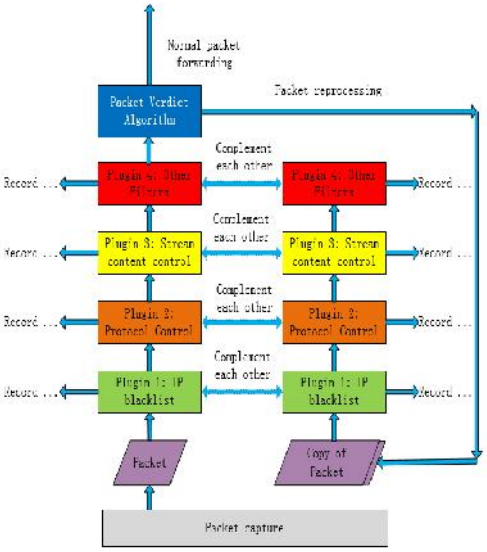

Figure 2: Smart packet verdict scheme used in vCNSMS