Rajashekhar* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.5, Issue No.3, April – May 2017, 6341-6344.

Automation of Network Micro Segmentation

RAJASHEKHAR
M.Tech Student, Department of CSE, R V College of Engineering, Bangalore, India

Prof. PRAPULLA S B
Assistant Professor, Department of CSE, R V College of Engineering, Bangalore, India

KRISHNA KISHORE V
Senior Engineer, Unisys global Services, Bangalore, India

Abstract— **Network Micro Segmentation is the ability to transmit data securely between systems over a network. Systems in a network uses advanced encryption technology and provides a mechanism for creating cryptographically enforced virtual networks based on the user's login credentials. Network Micro Segmentation is used to share the information between the selected users and protecting the sensitive data from hackers by allowing the data to be visible only to the selected users. Network Micro segmentation secures the data in motion and controls the sharing of information within or across the network by employing an innovative cloaking technique. The Automation of Network Micro Segmentation Environment is used to configure the network and systems automatically. The market value of network security reaches $15.5 billion by 2019.**

I. INTRODUCTION

'Network Micro-segmentation' is obtaining attention as the simplest way network virtualization will improve security. They have a tendency to believe that organizations should move faraway from security that is perimeter-centric, hardware-centric, and inflexible, and address the misconception that merely column on a lot of security merchandise somehow equates to raised security. Instead, administrator have a tendency to should bring security within the information center and obtainable for each work, not simply the important or regulated systems. They got referred to as this ability to produce fine-grained security with social control distributed to each hypervisor within the information center micro-segmentation. Clearly known 3 essential necessities of micro-segmentation that ultimately translates to a safer information center architecture: persistence, ubiquity, and extensibility.

Three Requirements for Network Micro-Segmentation are

Persistence: Security should be consistent within the face of constant modification. Security directors want assurance that after them provision security for an employment; social control of that security persists despite changes within the surroundings. This can be essential, as information centre topologies square measure perpetually changing: Networks square measure re-numbered, server pools square measure enlarged, and workloads square measure affected, and so on. The one constant within the face of all this alteration is that the employment itself, alongside it's want for security.

Ubiquity: Security should be accessible all over. Ancient information center architectures rate security for necessary workloads, too typically at the price of neglecting lower priority systems. Ancient network security is dear to deploy and manage, and since of this price, information center director's square measure forced into a scenario wherever they need to ration security. Attackers make the most of this reality, targeting low-priority systems with low levels of protection as their infiltration purpose into a knowledge center.

Extensibility: Security should adapt to new things. Apart from persistence and iniquitousness, security directors additionally have confidence micro-segmentation to adapt to new and development things within the same means that information center topologies square measure perpetually dynamic , thus too square measure the threat topologies within information centers. New threats or vulnerabilities square measure exposed, previous ones become inconsequential, and user behavior is that the inexorable variable that perpetually surprises security directors.

II. LITERATURE SURVEY

Network Segmentation is a process in which the network is split into small elements or pieces to control the data movement only among authorized users. This process protects sensitive data from unauthorized users by enabling restricted access only to the selected and authorized users. Network Segmentation acts as a critical defensive against cyber-attack [1] and hackers. The next problem for segmentation of the network is to decide which portion of the network or which network environment has to be considered for splitting [2].

Mahmud Hasan et. Al. talks about the firewalling and intrusion detection. This functionality will help in the project to make whenever making the network configuration. They have the capacity of monitoring the traffic in the network [3]. Network Segmentation design requires a full understanding of network environment which explains about the geometric environment of the network including the sensor nodes deployed on network. A massive sensor network can have issues such as irregular topology and can contain holes [4].

Convex partitioning and Concave Partitioning are most used types of network partitioning methods. Convex Partitioning is widely known as Convex Segmentation, in which network is divided into convex regions based on network geometry by applying traditional algorithms. In the existing solutions for Network segmentation has problems such as detecting concave node instead of convex, sink extraction form median axis that adds boundary noise to the network [5]. Cloud Computing is known for its scalability, flexibility and on-demand workload creation. Today, cloud-enabled data centers utilize VLAN, VxLAN or GRE segmentations but these techniques, despite being widely deployed, have a variety of inherent technical and architectural limitations [6].

In this paper we introduce a novel architecture leveraging UCC and IID for segmentation, rather than those traditionally used today (e.g., VLAN, VxLAN, etc.). The proposed architecture is entirely based on IPv6 and, for illustrative purposes only, is demonstrated using Open Stack as the cloud framework [7]. In the existing solution, for automatic target recognition in the network, neural network approach is used. In this neural network approach pulse couples network segmentation module is combined with a classifier which generates data based on virtual training [8].

In order to support competition and associated mode of transaction in the network with reference to congestion, Network Segmentation approach became necessary [9]. In the field of power systems, power Network Segmentation plays an important role by providing many applications for operation of power systems. Segmentation context changes with respect to application. Two step approaches is used to solve the problem of segmentation context changing in a competitive environment. First step clusters the nodes based on optimization using decision metric. The second step uses bus migration process to fine tune the results obtained in the first step [10].

In existing solution, time to configure the network is more. The manual configuration of the network will take huge amount of time as the number of systems in the network increases. Also the manual configuration will lead to human error while configuring the network. Therefor the proposed solution will give the infrastructure to configure the network through the Customer Simulation and Automation. Through this tool the administrator can configure the network easily.

III. ARCHITECTURE

The design and development of the Customer Simulation and Automation (CSA) tool is the following architecture.it includes the components like File Server, Database, Tomcat Server and the vSphere client. The tomcat server is used to host the web user interface for the administrator. Fig 1 shows the architecture of the proposed system.

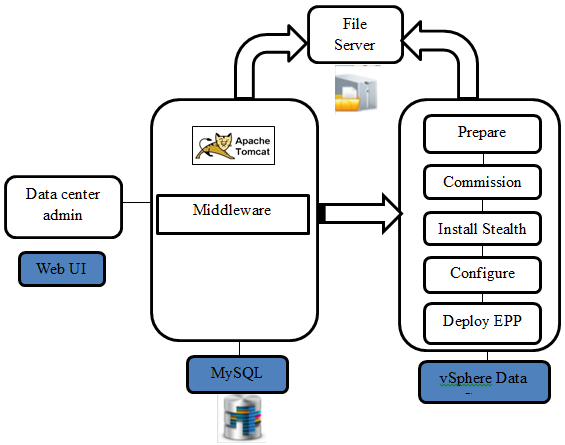

Fig. 1 Architecture of Network Micro Segmentation

File server component serves as global storage area which will be used to host Stealth installer MSIs, customization scripts and Post installation configuration files. All the content is distributed under clearly defined folder structure, which will help the automation scripts to locate respective files. CSA admin/user should ensure this File Server is accessible to commissioned virtual machines otherwise the installation/configuration will fail. CSA tool provides the flexibility to customize/edit File Server IP & Credentials.

The middleware will contain the source code. The middleware will communicate with the file server and vSphere client to get the information like operating system template and the data store name. The primary objective of project Customer simulation and Automation is to automate the process of bring up the infrastructure configure Stealth to stimulate the customer environment for testing the network security product of – Stealth. The figure 4.2 show bellow illustrates the architecture of the customer simulation and automation of network micro segmentation. The user interface is used to provide the information of the network like IP address, port group etc. The middleware will process the JSON object that comes from user interface. At the vCenter side the virtual machine will be commissioned and operating system will be installed automatically and the necessary software will be installed then the stealth core will be installed. At last the configuration will be applied for the commissioned system.

MYSQL and Hibernate adds persistence capabilities to CSA tool like (Saving deployment configurations, ability to clone them, also maintain JOB status and commissioned Stealth network information). MYSQL is light weight and open source and fits well in to CSA DB requirements. Hibernate helps us to seamlessly blend middleware logic developed in

JAVA to MYSQL database entities and relives the developer the pain of handling low level connection, transaction and data conversion activities.

DASEIN API is part of Middleware logic, which does execution of tasks on vCenter using open source DASEIN API calls. It acts as client to bridge the communication between CSA and VMware vCenter. It also adds design flexibility to replace/switch to any other on perm virtualization provider with our much changes to implemented code. The connections are pooled and tuned to optimize the commissioning process which improves performance of CSA tool to stand up large deployments.

IV. METHODOLOGY

The network micro segmentation follows layered architecture. It has Presentation layer, Middleware layer and Persistence layer. The presentation layer provides user interface for the administrator, to configure the network. The middleware implements business logic that acts as an communicate between user and the Database. This layer takes the input from Presentation layer, processes the input and stores the results back to the database. The persistence layer will store the information of the each commissioned machine. It stores the information like IP address, name, deployment name etc.

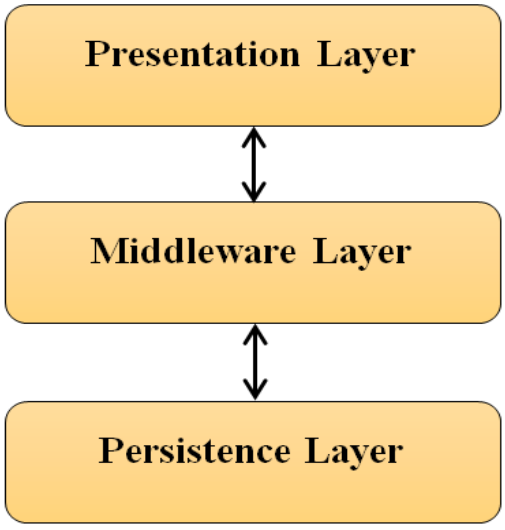

Fig. 2 Layered Architecture for Customer Simulation and Automation

Fig. 2 show the method that fallowed to develop the Customer Simulation and Automation. To use the Network Micro Segmentation, the user logs into the System through Graphical User Interface (GUI)/portal. The GUI generates the Java Script Object Notation (JSON) object which is then acts as input to the middleware. The Middleware component has Management server, Authorization Server and End Point Package (EPP) server, which gets selected based on the type of JSON object. The selected server gets the necessary software's and required configuration files for running the automation scripts that are implemented in the server.

V. RESULTS

The analysis is carried out to check whether the mentioned functional and non-functional requirements are met. In order to verify the results obtained Intel reference boards were used.

Fig. 3 shows the performance analysis of the time, the configuration of the network with various numbers of systems within network with respect to how much time it will take to configure the network without using the customer automation and simulation. The time to configure the network will grow exponentially as the numbers of systems in the network are increased.

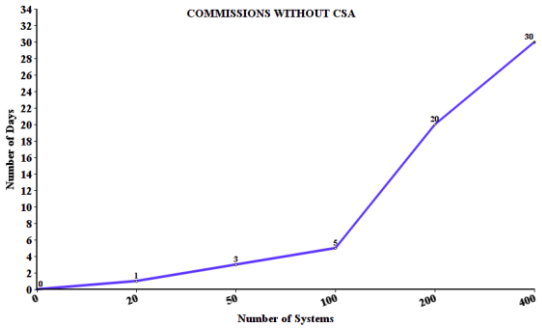

Fig. 3 Commissions without CSA

Fig. 4 shows the performance analysis of the time, the configuration of the network with various numbers of systems within network with respect to how much time it will take to configure the network with using the customer automation and simulation. The huge reduction of time to configure the network, from number of days to hours. From this project we achieved the one of the main object of the project.

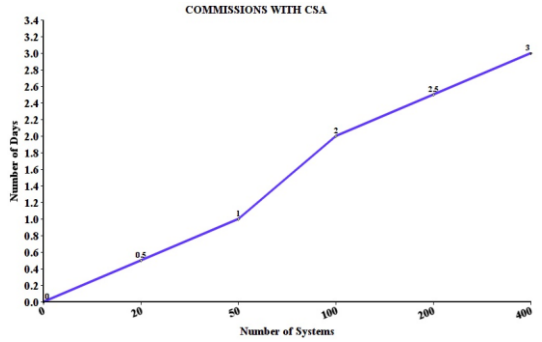

Fig. 4 Commissions with CSA

Fig. 5 shows the possible errors that are occurred in the network while manual configuring the network versus the automation of configuring the network. It's almost very less number of error that can occur when we commission through this portal. The automation process will reduce the human error rate

from 90% to 25% while configure the system, irrespective of number of systems in the network.

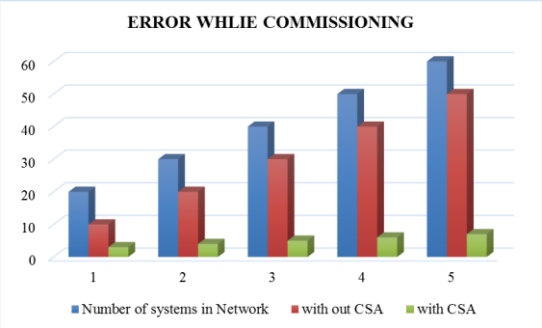

Fig. 5 Errors while commission

VI. ACKNOWLEDGMENTS

Any achievement, be it scholastic or otherwise does not depend solely on the individual efforts but on the guidance, encouragement and cooperation of intellectuals, elders and friends. I deeply express my sincere gratitude to my guide Professor Prapulla S B, Assistant Professor, Department of CSE, R.V.C.E, Bengaluru, for his able guidance, regular source of encouragement and assistance throughout this project. I also extend my cordial thank to Unisys global Services for providing me an opportunity to carry out the project work in its organization. I also would like to thank my mentor Mr. Krishna Kishore V and all team members for their support and guidance and also thanks to Dr S Sridhar Director RVCT RVCE Bangalore for communicating this paper for publication.

VII. REFERENCES

[1] Neal Wagner, Cem S. S. Ahin, Michael Winterrose, James Riordan, Jaime Pena, Diana Hanson, and William W. Streilein, "Towards Automated Cyber Decision Support: A Case Study on Network Segmentation for Security", Proc. Of the IEEE Conference, Athens, Greece 2016, pp. 222-224.

[2] Md. Mahmud Hasan and Hussein T. Mouftah, "Latency-Aware Segmentation and Trust System Placement in Smart Grid SCADA Networks", Proc. Of the IEEE Conference, Toronto, ON, Canada 2016, pp. 103-106.

[3] P. Godefroid, N. Klarlund, and K. Sen, "DART: Directed Automated Random Testing," Proc. Of the Conf. Programming Language Design and Implementation (PLDI 05), ACM Press, Zurich, Switzerland, 2005, pp. 213–223.

[4] B. Korel, "A Dynamic Approach of Test Data Generation," Proc. IEEE Conf. Software Maintenance (ICSM 90), IEEE CS Press, San Diego, CA, USA, 1990, pp. 311–317.

[5] P. Godefroid, "Model Checking for Programming Languages Using VeriSoft", Proc. of the Ann. Symp. Principles of Programming Languages (POPL 97), ACM Press, Lincoln, NE, USA ,1997, pp. 174–186.

[6] J. Larus et al., "Righting Software," IEEE Software, vol. 21, (3), May/June 2004, pp. 92–100.

[7] V.E. Neagoe, A.D. Ciotec, "New Approach for Accurate Classification of Hyperspectral Images Using Virtual Sample Generation by Concurrent Self-Organizing Maps," Proc. of the IEEE Internat. Geoscience and Remote Sensing Conf. (IGARSS 2013), , Melbourne (Australia), July 21-26 2013pp. 1031-1034.

[8] J.E. Forrester and B.P. Miller, "An Empirical Study of the Robustness of Windows NT Applications Using Random Testing," Proc. 4th Usenix Windows System Symp., Usenix Assoc., Maui, HI, USA, 2000, pp. 59–68.

[9] Zahir Hussain Shah, Packt Publishing Ltd, "Windows Server 2012 Hyper-V: Deploying the Hyper-V Enterprise Server Virtualization Platform" proc of IEEE conference, Birmingham, UK, March 2013, pp 58-59.

[10] Mastering VMware vSphere 6 – Nick Marshall, John Wiley & Sons, Indianapolis, Indiana, USA, 2015.

