International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 3501-3510

Design of Implementation of a Zero Trust Approach to Network Micro-Segmentation

Muhammad Mujib[1] and Riri Fitri Sari[2]

[1,2]Department of Electrical Engineering, University of Indonesia, Indonesia
[1]muhammad.mujib@ui.ac.id, [2]riri@ui.ac.id

Abstract

The security of the data center network is carried out on the perimeter side. It is assumed that attacks always come from external parties via the traffic that enters and exits data center, as known as north-south traffic. This assumption proved to be incorrect because the data center is a resource center that is interconnected with one another, in which intra-data of server-to-server traffic, or so-called east-west traffic, makes a dominant of approximately 85 % of the total traffic. The perimeter security model is built adopting the trust and untrust concept. A trusted network is in the form of intranet networks, whereas the untrusted network is in the form of internet networks. Based on the Computer Security Institute, security incidents originating from intranet networks transpire of approximately 60 to 80 percent of the incident. One way to surmount this is by implementing the concept of security in the form of zero-trust networking (ZTN). Micro-segmentation is one of the ways of implementing ZTN. Micro-segmentation is a way to divide a network into smaller logical segments with the aim that only end-points that have been authorized can access resources on that segment. In this paper, micro-segmentation will be evaluated by implementing a Cisco Application Centric Infrastructure based software-defined network testbed. The simulation to determine the performance of micro-segmentation in restricting port scanning attacks and the spread of malware on east-west data center traffic as a use case. Performance evaluation results show that micro-segmentation is resilient to port scanning and the spread of malware to reduce the attack surface.

Keywords: *Data Center, East-West Traffic, Micro-Segmentation, Zero Trust Network*

1. Introduction

Traditionally, the security of the data center network is carried out on the perimeter side. It is assumed that attacks always come from external parties via the traffic that enters and exits data center, as known as north-south traffic. This assumption proved to be incorrect because the data center is a resource center that is interconnected with one another [1], in which intra-data of server-to-server traffic, or so called east-west traffic, makes a dominant of approximately 85% of the total traffic [2]. The perimeter security model is built adopting the trust and untrust concept. Trusted network is in the form of intranet networks, whereas the untrusted network is in the form of internet networks. Based on the Computer Security Institute (CSI), security incidents originating from intranet networks transpire of approximately 60 to 80 percent of the incident [3]. One way to surmount this is by implementing the concept of security in the form of zero trust networking (ZTN). ZTN is a new concept in network design by applying the same level of trust in intranet and internet networks. The primary key in achieving ZTN is to consider both the intranet and internet network to be the same, i.e as an untrusted network [4]. Micro-segmentation is one of the ways of implementing Zero Trust Network (ZTN). Micro-segmentation is a way to divide a network into smaller logical segments with the aim that only end-points that have been authorized can access resources on that segment [5][6].

ISSN: 2005-4238 IJAST

In this paper, micro-segmentation will be evaluated by implementing a Cisco Application Centric Infrastructure (ACI) based software-defined network (SDN) testbed. We conducted simulations to determine the performance of micro-segmentation in restricting port scanning attacks and the spread of malware on east-west data center traffic on the occurance of denial of services attack. The structure of the rest of this paper is as follows. We provide the literature review in Section 2. In Section 3, we show our methods and design scenario for evaluation of micro-segmentation. Section 4, we present the results and discussion of micro-segmentation simulation in details and provides evaluation performance studies. In Section 5, we present the conclusion.

2. Literature review

2.1. Fundamental of zero trust

Zero trust is a security idea based on the principle of never trust, always verify made by John Kindervag in Forrester's research [7]. The primary purpose of this idea is to replace the traditional perimeter-based security model with a security model called zero trust networking (ZTN). Some considerations in ZTN are that there are no concepts of trust and untrust in users, in network, and in security devices. This concept means that all data traffic is considered untrust in data communication systems [7].

2.2. Architecture of zero trust

Figure 1 shows the traditional security concept that requires different security devices at each layer, so it requires a significant investment, and management of the security system becomes ineffective. The zero trust architecture consolidates infrastructure such as firewalls, access control, cryptographic engines, package forwarding, and central content filtering using the segmentation gateway mechanism. The segmentation gateway system has a high level of scalability by implementing micro-segmentation without replacing current infrastructure.

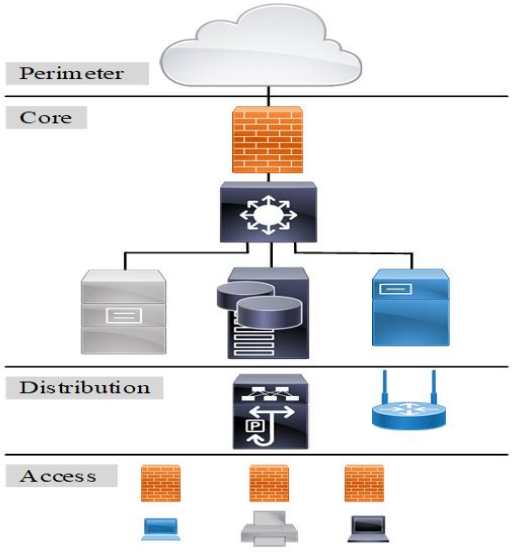

Figure 1. Architecture of Traditional Network [7]

Figure 2 shows one of the ZTN architectures that places security devices such as firewalls at the center of the network to control and inspect traffic on micro-

ISSN: 2005-4238 IJAST

segmentation networks. Micro-segmentation aims to limit the lateral movement of the attackers who gained into the internal resources and reduce the occurrence of more large damage [7].

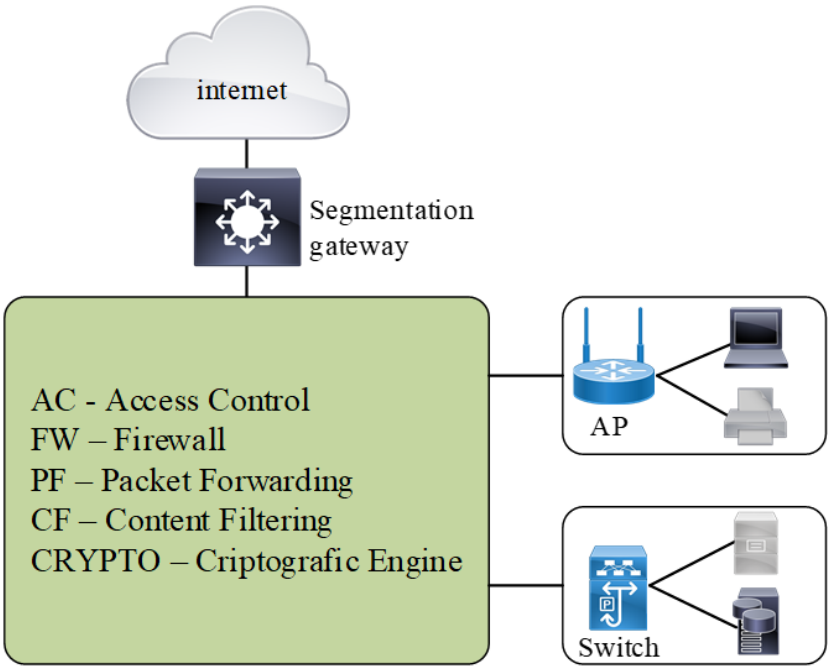

Figure 2. Architecture of Zero Trust Network [7]

2.3. Micro-segmentation

Micro-segmentation is a technique of splitting resources on the network into smaller logical segments with the purpose of only authorized end-points that can access resources according to policy. Micro-segmentation is implemented by dividing the data center network into smaller sections that are equipped with security systems between application tiers and even between devices within the tier, which will quarantine compromised resources into smaller domains to prevent more damage. Micro-segmentation is employed as a security system in east-west data center traffic by integrating resources so that traffic can be controlled to better security postures in the data center [8].

2.4. Cisco application centric infrastructure (ACI)

Cisco Application Centric Infrastructure (ACI) is one of the solutions of software define network by implementing the concept of micro-segmentation. Cisco ACI is one solution in the application of micro-segmentation with performance, scalability, and feasibility according to the needs of increasingly complex and modern applications. Figure 3 shows that the concept of micro-segmentation in Cisco ACI is built using logical networks, devices, and services in a hierarchical form. Security policies can be applied automatically to devices that are integrated, such as firewalls and Intrusion Prevention Systems (IPS). Interoperability between different vendors can run well by the policies that have been implemented so that it has a high level of scalability and flexibility. For example, virtual machines from vendor A can communicate with virtual machines from vendor B [9].

ISSN: 2005-4238 IJAST

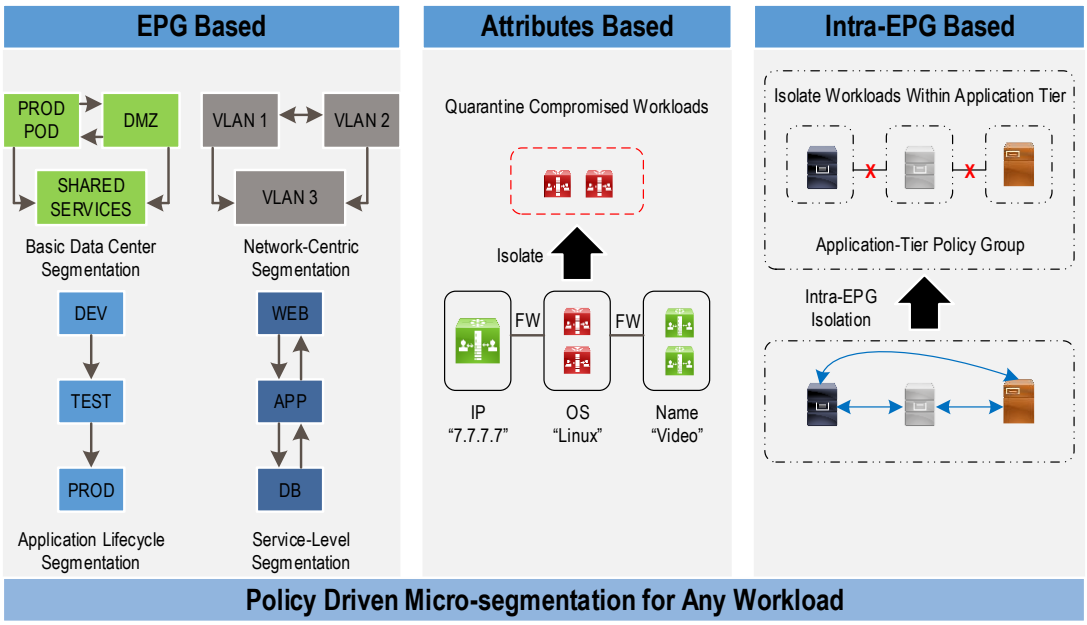

Figure 3. Cisco ACI Micro-segmentation Concept [9]

3. Methods and design scenario of evaluation of micro-segmentation

In this paper, the method of evaluation of micro-segmentation is done by implementing the simulation of the Cisco ACI testbed. Development and testing of this research are divided into three phases, scenario development, program preparation, and program testing.

3.1. Scenario development

This stage aims to design and to implement micro-segmentation using Cisco ACI. Subsequently, we created two application tiers in the form of a Web Server and Database in one network segmentation /24. We conducted the port scanning and malware spreading, which launch a denial of service (DoS) attack to evaluate the performance of a micro-segmentation process. We compared the test results related to the concept of micro-segmentation and without micro-segmentation.

3.2. Program preparation

This stage aims to conduct experimentation, and a Cisco ACI fabric was configured with the micro-segmentation process. The following is a list of equipment used to conduct experiments as shown in Figure 4.

ISSN: 2005-4238 IJAST

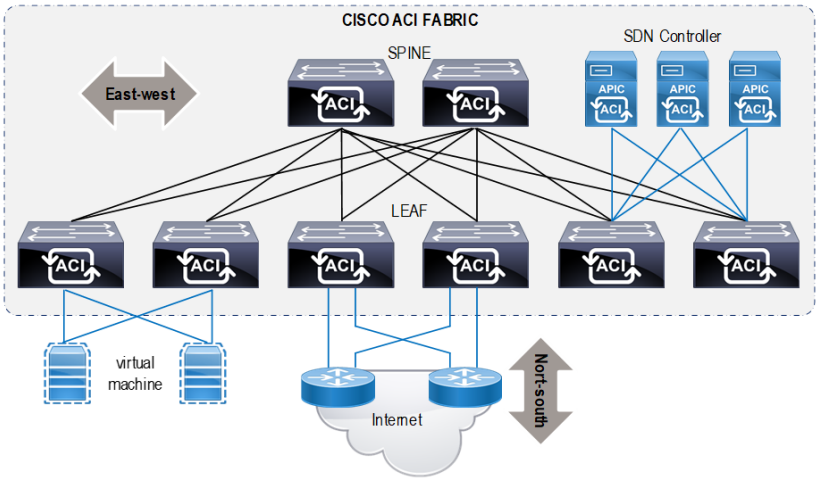

Figure 4. Environment Simulation Cisco ACI Testbed

3.2.1. Micro-segmentation network testbed: A network simulation environment with a micro-segmentation specialty using the Cisco ACI platform because of dynamically provisioned, scalable, and programmable fabrics, Cisco ACI is the leading choice [10]. Cisco ACI consists of leaf switches, which have micro-segmentation capabilities. The leaf switches are used to interconnect all workloads, spine switches are used to interconnect between leaf switches using a 40 Gbps uplink, and the Cisco Application Policy Infrastructure Controller (APIC) to perform policy configuration and accessibility traffic. Table 1 shows the list of a component of the Cisco ACI.

Table 1. The List of a Component of The Cisco ACI

Name	Bandwidth	Type	Firmware
Spine Switch	40 GB	Nexus 9336PQ	n900-14.2 (3I)
Leaf Switch	10 GB	Nexus 9372PX Nexus 93128TX	n900-14.2 (3I)
SDN Controller	10 GB	APIC Cluster M-1	version 4.2 (3I)

3.2.2. Service device and operating system testbed: Micro-segmentation performance testing scenarios are developed implementing application tiers consisting of Web Servers, Database, and Client employing virtual machines, as shown in Table 2.

Table 2. Virtual Machine Specification Testbed

Name	vMemory	vCPU	Operating System
Web Server	2 GB	1 vCPU	Windows Server 2008
Database	2 GB	1 vCPU	Windows Server 2008
Client	4 GB	2 vCPU	Linux Ubuntu

3.3. Program testing

ISSN: 2005-4238 IJAST

This stage aims to reproduce testbed simulation by conducted the port scanning and malware spreading, which launch a denial of service (DoS) attack to evaluate the performance of a micro-segmentation process. Port Scanning attack requires operating a test and listing all the open ports. This operation uses Nmap [11], which works from client host, a free port scanning utility. Such an attack is an active form of attack, where using a tool can be used to determine the hosts and services on a network. It can moreover be used to perform attacks on specific ports such as port 443 (HTTPS) and so on [12]. DoS attacks are endeavors by a nonlegitimate user to degrade or deny resources to authorized users [13]. We test the TCP SYN flood attack against a target web server and database from the client site. To produce the actual attack, we used the open-source hping3 tool [14]. The tool allows us to generate arbitrary packets with which to flood a target host. We commenced hping3 to generate TCP SYN packets and randomly selected the source address, which targeted an open port on the victim machine.

Figure 5 shows a simulation method using a micro-segmentation process, where client, web servers, and database are in one segment /24. The micro-segmentation process is conducted out by applying a policy end point group (EPG). EPG is the concept of applying policies on the Cisco ACI platform based on functions in application tiers, such as web servers and databases, used for mapping between applications and networks. EPGs can be formulated as having a provider/consumer connection with one another, where the communication between them is established by policy contracts (CT) [15]. In this experiment, there are three EPGs namely the EPG web server, the EPG database, and the EPG client.

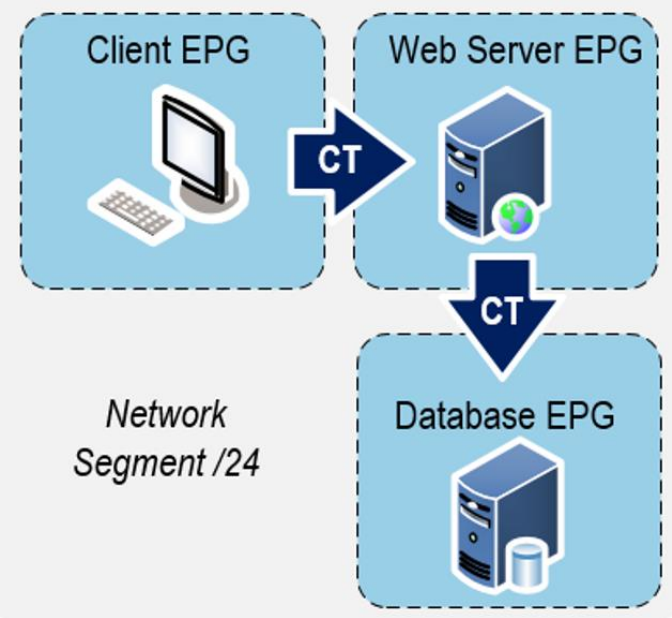

Figure 5. Experiment with Micro-Segmentation Process

Figure 6 shows the simulation method without a micro-segmentation process where the client, web server, and database in an EPG as one segment /24. In this design, all of the devices within that segment are outlined into an EPG namely the EPG all.

ISSN: 2005-4238 IJAST

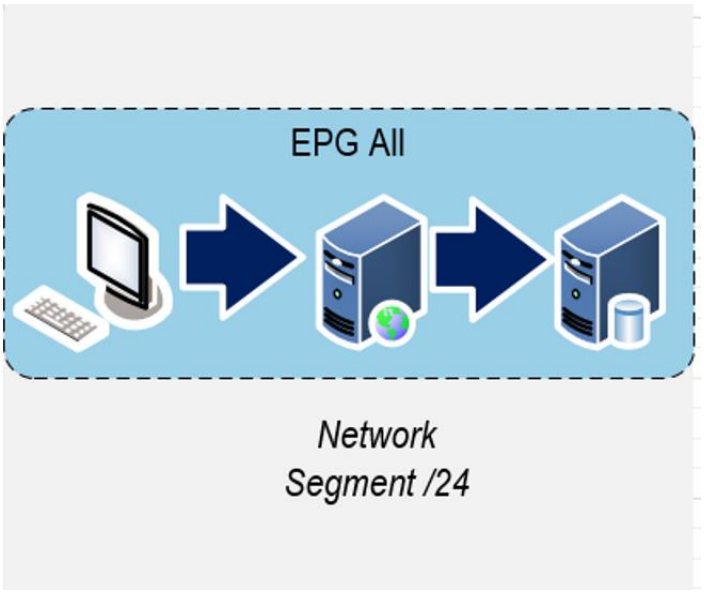

Figure 6. Experiment without Micro-Segmentation Process

4. Result and discussion

In this paper, the design and implementation of micro-segmentation are built using Cisco ACI. Subsequently we created two application tiers in the form of a Web and Database in one network segmentation /24. We conducted the port scanning and malware spreading which launch DoS attack to evaluate the performance of micro-segmentation process. We compared the test results related to the concept of micro-segmentation and without micro-segmentation.

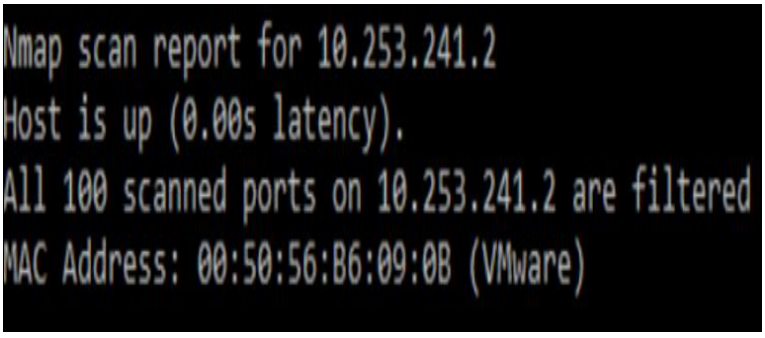

Figure 7. Result of Port Scanning with Micro-Segmentation

Figure 7 shows the micro-segmentation performance testing by applying port scanning using the NMAP tool with the result that on the server no open ports were detected. On the other hand, in cases without micro-segmentation some open ports on the server were identified as shown in Figure 8.

ISSN: 2005-4238 IJAST

```
Nmap scan report for 10.253.241.2
Host is up (0.00s latency).
Not shown: 91 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
MAC Address: 00:50:56:B6:09:0B (VMware)
```

Figure 8. Result of Port Scanning without Micro-Segmentation

Based on the results of the simulation conducted with micro-segmentation, the scan report shows that no port is open and available. Micro-segmentation gives no data whatsoever about the number of open ports and the service available on them. These results enforce the security of the service and prove the unavailability of access to unauthorized clients. On the other hand, it can be noticed that without micro-segmentation, some ports are open and available.

Micro-segmentation evaluation testing for the spread of malware is executed by adopting a type of malware based on the simulation of various kinds of malware, such as a denial of service attack. In this experiment, the offense is deployed through a client that runs in Kali Linux containing hping3 tool, which executes a command attack ***hping3 –c 1000 –d 128 –S –w 64 –p 80 --flood --rand-source ipdst*** [16] for 60 seconds.

The experiment results show that in cases with micro-segmentation, the DoS attack is not successful in interrupting a two-tier application based on CPU utilization of web server increase to 100 % neither the database, as shown in Figure 9. It means that the attacker has no lateral movement to do damage to other services, such as a database. On the other hand, a denial of service attack is carried out on servers that are on one network segment, when there is no micro-segmentation process.

Figure 9. The Utilization of CPU Under DoS Attack with Micro-Segmentation Process

ISSN: 2005-4238 IJAST

Figure 10 shows that CPU usage in web server and database increase to 100 %; it means that the attacker succeeds in compromising the one of service to make a lateral movement to other services.

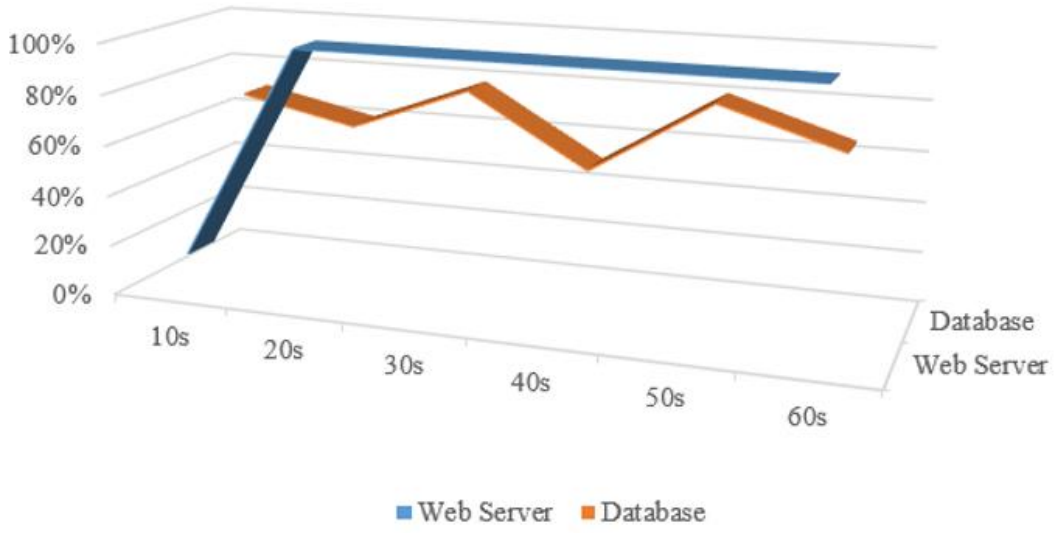

Figure 10. The Utilization of CPU Under DoS Attack without Micro-Segmentation Process

5. Conclussion

The performance evaluation of the implemented micro-segmentation testbed showed that micro-segmentation is more resilient to port scanning and the spread of malware that use a denial of service attacks by not providing any information and maintaining the availability of service applications, respectively. These results confirm the promising potential of zero trust network approach to micro-segmentation in protecting current and future networks to reduce the attack surface of data center network.

The future work to compare a zero trust network approach to micro-segmentation based on the Cisco ACI Platform, more open research areas exist. In particular, exploring how to evaluate the performance of micro-segmentation based on the NSX VMWare platform is essential since these models will show the best performance to be chosen in future networks.

References

[1] S. Newman, "Building Microservices Designing Fine-Grained Systems 1st edn", O'Reilly Media Inc, Sebastopol, **(2015)**.
[2] Cisco, "Cisco Global Cloud Index: Forecast and Methodology 2016–2021", Cisco White paper, San Jose, **(2018)**.
[3] R. Sivaraman, "Zero Trust Security Model", S3tel and C4ISR Global System White Paper, Cartersville, **(2015)**.
[4] E. Gilam and D. Barth, "Zero Trust Networks Building Secure Systems in Untrusted Networks 1st edn", O'Reilly Media Inc, Sebastopol, **(2017)**.
[5] VMware Inc, "Data Center Micro-Segmentation a Software Defined Data Center Approach for a "Zero Trust" Security Strategy", Palo Alto, **(2014)**.
[6] L. Miller and J. Soto, "Micro-segmentation for Dummies", John Wiley & Sons, Inc, Hoboken, **(2015)**.
[7] J. Kindervag, "Build Security into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research Tech. Rep, Cambridge, **(2010)**.
[8] Cisco, "Data Center Microsegmentation: Enhance Security for Data Center Traffic", Cisco White paper, San Jose, **(2015)**.

ISSN: 2005-4238 IJAST

[9] P. Jain, 'Microsegmentation in Heterogeneous Software Define Networking Environments", U.S. Patent 10,171,507 B2, **(2019)** January 1.
[10] P. Ijari, "Comparison between Cisco ACI and VMWARE NSX" IOSR Journal of Computer Engineering. (IOSR-JCE) vol. 19 Issue 1 ver. IV, **(2017)** January-February, pp 70-72.
[11] R. R. Rohrmann, J. V. Ercolani and W. M. Patton, "Large Scale Port Scanning Through Tor using Parallel NMAP Scans to Scan Large Portions of The IPv4 Range", IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, Tiongkok, **(2017)** July 22nd-24th.
[12] A. Moubayed, "Software-Define Perimeter (SDP) State of The Art Secure Solution for Modern Networks", IEEE Network vol. 33, **(2019)** September-October, p 226-33.
[13] R. Shea, "Performance of Virtual Machines Under Networked Denial of Service Attacks: Experiments and Analysis", IEEE System J. Vol. 7 No. 2, **(2013)** June.
[14] A. Saboor, M. Akhlaq and B. Aslam, "Experimental Evaluation of Snort Against DDoS Attack Under Different Hardware Configuration", 2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan, **(2013)** December.
[15] Cisco, "Cisco Application Centric Infrastructure (ACI) Endpoint Groups (EPG) Usage and Design", Cisco White paper, San Jose, **(2014).**
[16] D. V. Vuletic, "Realization of a TCP Syn Flood Attack Using Kali Linux", Military Technical Courier, Belgrade, Serbia, **(2018)** July.

ISSN: 2005-4238 IJAST