The Impact of Cyber Security on the Quality of Service in Optical Networks

Michal Walkowski, Jacek Oko, Slawomir Sujecki
Department of Telecommunications and Teleinformatics
Wroclaw University of Science and Technology,
Wroclaw, Poland
Emails: michal.walkowski@pwr.edu.pl.
jacek.oko@pwr.edu.pl
slawomir.sujecki@pwr.edu.pl

Stanislaw Kozdrowski
Department of Telecommunications and Teleinformatics
Wroclaw University of Science and Technology,
Wroclaw, Poland
Email: s.kozdrowski@tele.pw.edu.pl

***Abstract*— We analyze the impact of novel solutions for cloud computing implementation on the operation of an optical network in the context of cloud computing structures applied within a large corporation networking environment. We focus particularly on various aspects of the quality of service that are related to an implementation of a particular solution to an improvement of various aspects of cyber security. We present the methods of improving the cyber security, the quality of service and compare them with those currently in use.**

Keywords-cloud-computing; network; containcers, security, qualyty of service.

I. INTRODUCTION

With an increase in the data flow volume, we observe an introduction of ever newer technologies needed to support the network traffic. In recent years the dominant technology for the handling of large data throughput is based on the use of optical fibers. The maximum currently achievable data transmission rates have been achieved in Wavelength Division Multiplexed (WDM) systems and hence WDM, is the key technology used now for the realization of the backbone networks [1][2]. Also, large data transmission rates in access networks are realized using optical fiber technology. Obviously, new technological solutions need to be accompanied by new solutions in the higher layers of the OSI model in order to insure the quality of service. Also a careful analysis of potential weaknesses of new technology with respect to cyber security is needed and potentially new solutions are required to handle all potential threats [3]. All this poses new challenges to the quality of service in modern telecom networks. The general purpose of this research is an analysis of the impact of various cyber security measures on the operation of an optical network in the context of cloud computing structures applied within a large corporation networking environment. We focus particularly on various aspects of the quality of service that are related to an implementation of a particular solution to an improvement of various aspects of cyber security. We present the discussion in the context of several possible attack scenarios and draw conclusions on this basis. In particular, we consider the cyber security solutions that are implemented in the optical layer and discuss also the cost and network maintenance implications of such solutions. We present the methods of improving the cyber security within the optical layer and compare them with those potentially applicable in the higher layers of the OSI model. We stress particularly the impact of the various measures on the quality of service but also discuss the issues related to the cost and network maintenance. A specific issue that we address in this contribution is a specific new solution in the area of the cloud computing recently being pursued in the context of the ever increasing data transmission rates and cyber security requirements, which relies on the implementation of Docker containerization. This solution is particularly attractive for an implementation in large scale enterprise network systems.

II. LARGE SCALE ENTERPRISE NETWORK SYSTEMS

Large scale enterprise (LSE) network systems serve both the employees of the enterprise and the external customers. Such networks can spread over large geographical areas thus implying large distances between the network nodes.

A new trend of development in the large scale enterprise networks introduces concept of micro-services. The concept of micro-services means that each single service should provide only one solution for a particular problem as well as be stateless and independent at the same time. For the purpose of solving the requirements set by programmers, technology of Docker containerization has been created. The main difference when compared with the so far used virtual machine solution (Figure 1) [4] is that container does not need to run operating system stack for a new service. Additionally, it allows to run the same application without customizing the operating system on each side. This results in lesser overhead when delivering service to customer. The programmer gets exactly the same environment as the client, so potential problems with providing services should be this minimized.

In the industrial research context there are two important orchestrators for managing Docker ecosystem, Swarm and Kompose. The second one is provided by OpenShift software developed by RedHat (RHEL) (Figure 3) [5]. Software supporting both solutions is currently available on

 ISBN: 978-1-61208-606-4

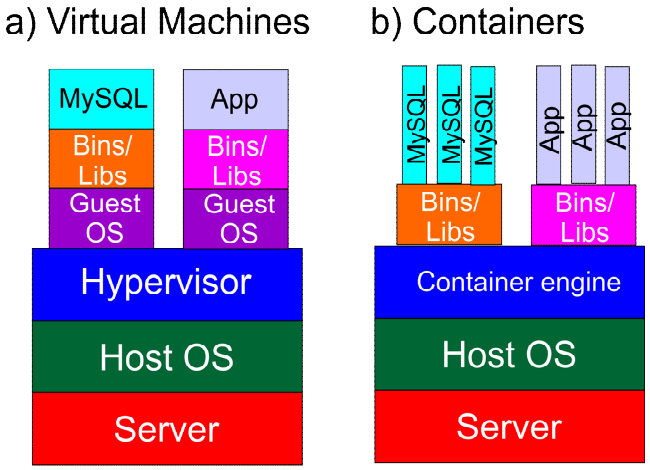

Figure 1. Comparison between virtual machines and containers

the internet and has already been implemented in many institutions (LSE) working on critical services from end users' point of view.

Technology consists of cloud computing, which is based on communication between machines serving services, divided into roles (master, node, load balancer, present master state storage, data storage). Currently the software supporting the Docker system allows achieving for one cluster up to 2 000 nodes and 120 000 containers.

III. SERVICE QUALITY

Container technology allows to measure and monitor services health (e.g., user CPU, system CPU usage) and thus provides for implementation of automatic vertical scaling when system is overloaded. This helps improving the service quality. Internal load balancer can successively control the external traffic coming from the clients of the network (Figure 2). When more capabilities are needed, usage of other software or hardware tools is possible. For instance we can implement an in-house developed balancer.

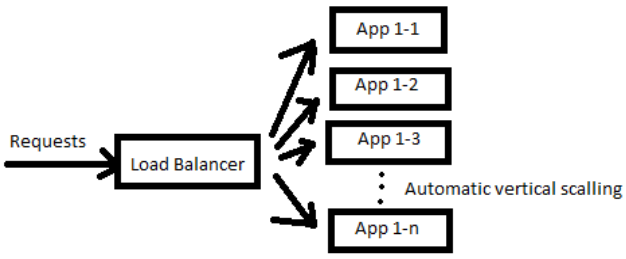

Figure 2. Load Balancer with automatic scaling

An additional advantage is that the Docker system can detect problem with internal network, cluster or machine and respond appropriately, preserving this way high Disaster Recovery (DR) and High Availability (HA) (Figure 4). If vertical scaling is not sufficient, system administrator can add new nodes to the existing infrastructure. The related research is carried out at several laboratories, e.g., [5] and aims to

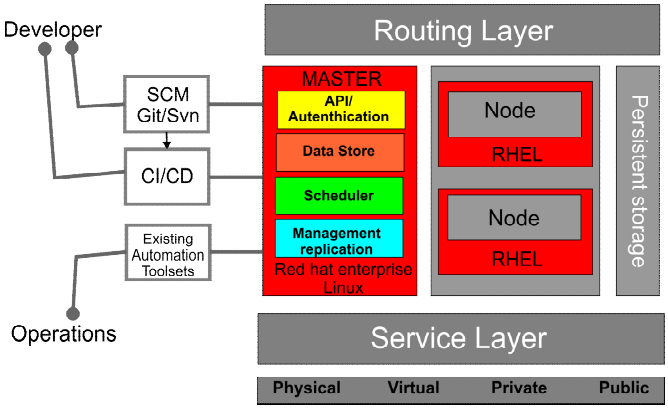

Figure 3. Architecture of OpenShift

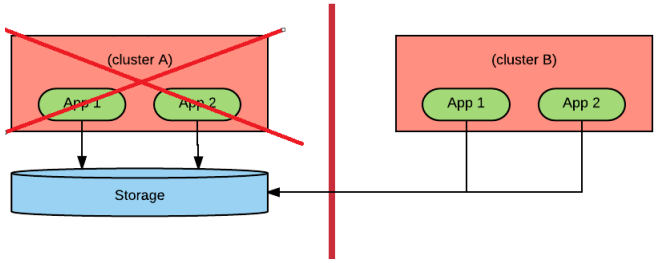

Figure 4. High availability mechanism

improve internal communication between the containers. Particular attention is devoted to the development of algorithms, which introduce priority for containers that speed up information exchange [6].

IV. POSSIBILE ATTACKS

Next, we consider the problem of insuring cyber-security within a Docker ecosystem. Firstly, we need to identify possible threats. There are several ways in which a cyber-attack can be performed on a Docker based system. Firstly we note that by default all Docker containers share the same network. Therefore, a specially prepared container can use Address Resolution Protocol (ARP) poisoning to disrupt or capture communication between services, thus essentially to perform potentially a man in the middle attack. Another problem concerning cyber-security is that in a Docker system the daemon is able to use an administrator's rights for proper operations. In this scenario an attacker can potentially escape from the container context and even attempt to overtake the control of all the system nodes.

The third possible threat emerges when Docker images are downloaded from untrusted sources, which results in risks of information leakage or botnet creation [7].

 ISBN: 978-1-61208-606-4

There is also a problem with identifying the container, which was attacked. For instance, if hypervisor host OS is not fully proof to an attack, a container can be successfully attacked without the possibility for carrying out a comprehensive forensic analysis because an attacker can remove all the traces of the attack. This is because when a container is created it has its own ID rather than IP address. Hence, from outside IP addresses are the same for more than one container. Containers are created and send log to the SIEM in LSE so after creating more the one container we cannot track them using an IP address. Consequently, we cannot do comprehensive forensics because we are not able to identify the container which was attacked.

V. PROTECTION MECHANISMS

The possible attack scenarios described in the previous section can be mitigated in several ways. First of all, it is worth to mention Center for Information Security (CIS) Security Benchmark documentation, which provides conditions needed to secure Docker configuration. This document gives general guidelines on how a Docker system security can be improved.

In this contribution, we propose and give special attention to the following methods/guidelines of improving cyber-security within a Docker system:

- application inside the container should not be run with an administrator rights
- each system component should log to system of logs correlation e.g. Security Information and Event Monitoring (SIEM)
- good practice is to run only one process inside the container.
- all of the libraries needed in development time and not needed anymore in the production should be removed
- running services for remote application configuration inside container is prohibited, e.g. ssh, telnet
- hardcoring keys, passwords and other sensitive data needed for communication or encryption is prohibited

We note however that all of the methods outlined above can only make it harder for an attacker to get into the system but they do not provide total security. In the future, we will continue research on how these measures improve the system stability and security and how they impact on the quality of service.

VI. CONCLUSION AND FUTURE WORK

In the era of progressing computerization, the threat to IT systems is increasing. The paper discusses the security and service quality issues within a large scale enterprise network based on cloud computing which uses the Docker system. This discussion shows that there is a real need to control and monitor possible threats, which prompts further research into this field.

Thus our future work will be focused on the development and implementation of an elastic solution for improving security in corporate networks based on cloud computing. Our main aim is to develop algorithms that will process the data compiled from the vulnerability and compliance scanners e.g., Qualys, Nessus or Inspect, in an optimal way. The algorithm should also provide useful information about the security level in the corporate assets (Figure 5). Further, the developed algorithm should be scalable to handle efficiently increasing amounts of data. Finally, the algorithm should communicate with the Docker orchestrator to dynamically respond to an increased demand by allocating more resources from the cloud server.

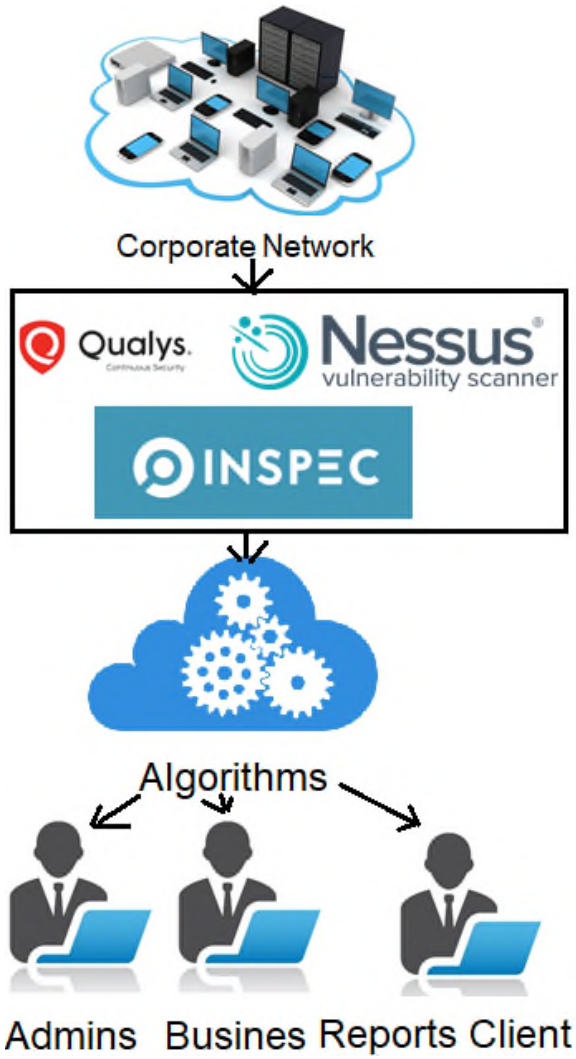

Figure 5. Architecture of proposed system

ACKNOWLEDGMENT

The authors wish to thank anonymous reviewers for valuable comments and remarks and Wrocław University of Science and Technology (statutory activity) for financial support.

 ISBN: 978-1-61208-606-4

REFERENCES

[1] Y. Li, L. Gao, G. Shen, and L. Peng, “Impact of ROADM Colorless, Directionless, and Contentionless (CDC) Features on Optical Network”, J. Opt. Commun. Netw. B58-B67, 2012.

[2] T. Zami, “Multiflow Application for WDM Networks With Multicarrier Transponders Serving Superchannels in Contentionless OXCs”, J. Opt. Commun. Netw. A114-A124, 2017.

[3] K. Hashizume, D. G. Rosado, E Fernandez-Medina, and E. B. Fernandez, “An analysis of securit issues for cloud computing”, Journal of Internet Serices And Applications, London , 2013.

[4] URL:https://qafe.com/what-is-docker-why-en-how-use-it/ [accessed: 15.12.201].

[5] URL:https://docs.openshift.com/container-platform/3.7/architecture/index.html, [accessed: 15.12.2017].

[6] A. Dusia, Y. Yang, and M. Taufer, “Network Quality of Service in Docker Containers”, IEEE Conference on Cluster Computing, Chicago, USA, 2015.

[7] T. Bui, “Analysis of Docker Security”, Aalto University, Helsinki, Finland, 2015

 ISBN: 978-1-61208-606-4