ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 5, 674-679 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Multi-layered Security Design and Evaluation for Cloud-based Web Application: Case Study of Human Resource Management System

Gautama Wijaya[*], Nico Surantha

Computer Science Department, BINUS Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia

ARTICLE INFO

Article history:
Received: 05 May, 2020
Accepted: 23 September, 2020
Online: 05 October, 2020

Keywords:
Multi-layered Security
NGFW
WAF
SQL Injection
Malicious File Injection

ABSTRACT

Cloud computing is the development of information technology to provides resources that can be accessed through network. Security and privacy in cloud computing are major concern for companies. Therefore, cloud computing architecture strategy and design are needed to reduce costs and ensure the security of company assets in cloud computing. In this study, we are using multi-layered security strategy that contain of Next-Generation Firewall and Web Application Firewall technologies. We conducted an evaluation on the design by using the SQL injection and malicious file injection method. The results of the evaluation show that the cloud computing architecture design that we proposed manage to prevent SQL injection and malicious file injection threats.

1. Introduction

Security and privacy are two major issues for companies that are adopting cloud computing [1]. Hence, companies are unwilling to move their assets to cloud computing [2], [3]. We need the right strategy and architecture design to reduce costs and ensure the security of the (applications and data) in cloud computing [4]. Therefore, we need to pay attention to this issue and the availability of security technology. Cloud computing architecture design is important to secure company assets. Most importantly, company assets in cloud computing are crucial for a company.

In this research, we conducted a case study on a company's cloud-based web application service that they provide for their human resources management. The main problem of this company is the security of their cloud-based web application. In cloud computing, the company uses only the security technology provided by the cloud service. Even more, the technology is not equipped with the ability to analyze and detect threats [5], which can endanger the company assets.

In this research, we use the System Development Life Cycles (SDLC) design method in the top-down network design to increase security for the company assets in cloud computing. We use a top-down network design because this method is considered the company's business goals and technical goals. Hopefully, our design can help companies to achieve business goals and technical goals [6], [7]. In this research, we are using multi-layered security by combining 2 security technologies, which are, Next-Generation Firewall and Web Application Firewall. We use multiple layers of security to increase protection against threats and create a safe cloud environment for the company [8]. Each layer of security has its technology, functions, and role to detect and prevent threats to enter the cloud environment.

The paper is organized, as follows; In part 2, we will discuss the basic concept of top-down network design using SDLC, multi-layered security, and the literature review from other researchers about secure cloud environment. In part 3, we will discuss the detailed method of the top-down network design using SDLC on the company. In section 4, we will discuss how the multi-layered security design is implemented and secure the cloud environment. In part 5, we will conclude the whole research.

2. Literature Review

2.1. Top-Down Network Design

Cloud computing architecture design is the way that companies use to ensure the efficiency, cost, and security control on the applications and cloud environments that they are using [9].

[*] Corresponding Author: Gautama Wijaya, Binus University, gautama.wijaya@binus.ac.id

https://dx.doi.org/10.25046/aj050583

Top-down network design is a method to make designs, ranging from the top layer of the OSI (application layer) to the bottom layer of the OSI (physical layer) [7].

In the design making process, we are using the top-down network design, which is divided into several stages. The following are the 4 (four) main stages that we took to create a cloud computing architecture design [6].

- Analyzing the requirements: We translated the business goal and technical goal that we are going to implement in the cloud computing architecture design. We also analyze the cloud computing architecture that they used recently to look for possible threats in the company's cloud computing environment.
- Developing logical design: We made a logical design of cloud computing architecture that we are going to use to secure the company's cloud environment.
- Developing physical design: We chose the security technology that we are going to implement on the logical design that we have made previously.
- The final stage: in the final stages, we implement the design that we have made, create a prototype, evaluates the security, and make documentation on the design.

2.2. Multi-layered security

A security strategy is needed to prevent threats and protect the cloud environment. Multi-layered security is one of many security strategies that can secure company asset. It is because each layer of security has function, role, and technology that can detect and prevent threats [8]. By layering security technology, as seen in figure 1, it can maximize the security of company assets.

In this study, we use the Next-Generation Firewall and Web Application Firewall security technologies to protect the company assets in cloud computing. These are the explanation of each security layer.

1. Layer 1, we use the Next-Generation Firewall (NGFW) as security technology. There are many features found in the Next-Generation Firewall (NGFW). Here are the features that we use in the first layer of the cloud computing architecture design [10]:

- IPS (Intrusion Prevention System)
- DPI (Deep Packet Inspection)
- TLS/SSL Encrypted Traffic Inspection
- Antivirus Inspection

2. Layer 2, we use the Web Application Firewall (WAF) as security technology, because it focuses on the security process at the application layer and analyzes each packet for any suspicious activity [11]. There are many features in the Web Application Firewall, so we utilize these features for our design. Here are the features that we use to secure cloud-based web application:

- SQL Injection and XSS
- CSRF Prevention
- Inspect HTTPS
- Traffic Encoded Traffic
- Virus Protection
- DOS Protection
- Data Theft Protection
- Brute Force Approach

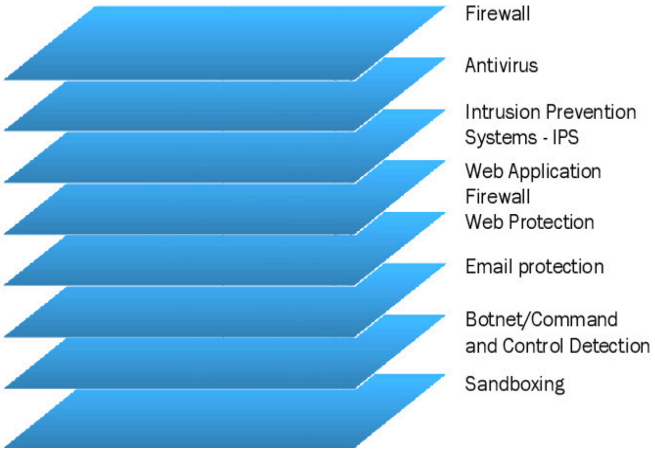


Figure 1: Multi-layered security by [8]

2.3 Previous Research to Secure Cloud-based Service

Here are some studies related to the design and security in cloud computing. The first study is titled "Towards Achieving Data Security with the Cloud Computing Adoption Framework" [12], and the research title is "Cloud computing adoption framework: A security framework for business clouds" [13]. Cloud computing architecture is a process of adopting cloud computing in a company. Making the right cloud computing architecture design can maximize the company's efficiency, cost, and service quality. Besides, a cloud computing architecture design is useful to improve the security of services and environments by ensuring that all data stored in the cloud are safe from attacks and threats. In this study, the authors made a cloud computing architecture design using the Cloud Computing Adoption Framework (CCAF). The framework creates 3 (three) layers of security that are used to protect data. The authors created the following layers of security: 1) Access Control and Firewall Layer, 2) Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), dan 3) Encryption / Decryption Control Layer.

Multi-layered security is a strategy implemented to protect the environment. Based on Artur Rot and Boguslaw Olszewski's research, multiple layers of security can protect the environment from Advanced Persistent Threat (APT) threats. The results prove that it can improve cloud environment security. It is because each layer has its role, function, responsibility, and technology to protect the environment [8]. Based on a research from Mouna Jouini and Latifa Ben Arfa Rabai, there are 3 (three) requirements to secure a cloud computing environment, which are Availability, Integrity, and Confidentiality.

Therefore, the authors use research methods that refer to research [12], [13], and [8], which made of a combination between Next-Generation Firewall (NGFW) and Web Application Firewall (WAF) technologies to secure cloud-based web application services a company made for human resource management.

3. Research Methodology

In this part, we will explain the process of creating an architecture design using the SDLC method in the top-down network design that we have mentioned previously in section 2. Here are the following steps:

3.1. Analyze Requirement

In this step, we do an analysis and identification on the company needs. There are 2 (two) stages carried out in this initial step:

1. Business Purpose Analysis: understanding the company's goals and limitations are important in the design process. For this reason, we conducted interviews with the supervisor and the company's management. The results are:

- Providing IT solution services for companies
- Increase satisfaction by using the cloud-based HRM services provided
- Increase the level of service provided

2. Technical analysis: In the second stage, we were doing technical analysis. The purpose is to recommend one or two technologies that we were going to use in making the design. To reach this technical goal, we have to analyze the business objectives of the company. Then we mapped it to suit the company's technical purpose. We can adjust the technical purpose to suit the company's business objectives. The company's main problem is the security technology that they have been using was unable to secure the company's assets and service. Therefore, we need a design that can improve the security and support the business goal of the company. Several technologies can be used to secure cloud-based web applications, such as Next-Generation Firewall and Web Application Firewall. Both technologies are able to support security at OSI layer 7.

3.2. Creating a Logical Design

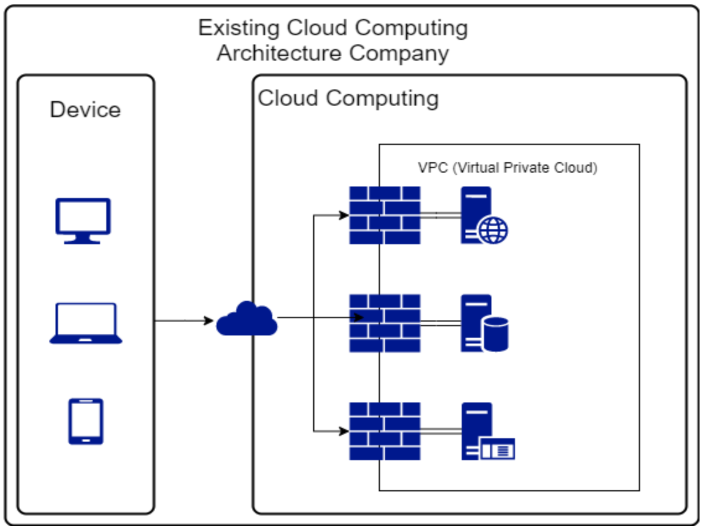


Figure 2: Existing Cloud Architecture at Company

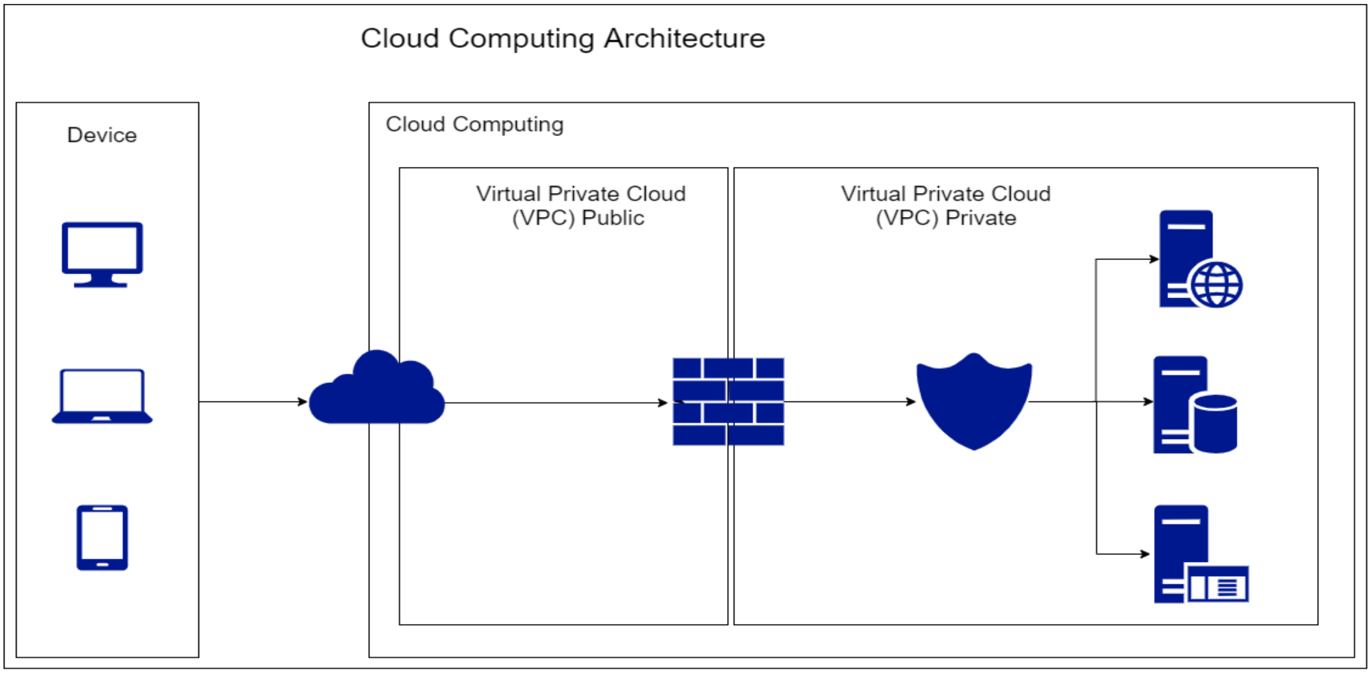


Figure 3: Propose Cloud Computing Architecture

In designing cloud-computing architecture, we need to know what kind of technology the company uses in providing services such as, operating systems, storage, servers, and other supporting services. After finding out the technology, we can make the design that meets their need.

Figure 3 is the logical design that we propose to improve the security of the company assets. We use a multi-layered security strategy by combining the Next-Generation Firewall and Web Application Firewall security technologies to secure the company assets. In our proposed design, we also take advantage of Virtual Private Cloud (VPC) technology. We separate between public and private networks using VPC so that the company assets cannot be accessed directly through the public network.

3.3. Creating Physical Design

After the logical design is complete, the next step is making the physical design. At this point, we had to determine which security technology that we were going to implement in each security layer. Here are the security technologies that we were using in each layer of security.

1. Next Generation Firewall Server: In the first layer, we used Next-Generation Firewall technology with 2vCPU server specifications, 8 GB of memory, SSD 1 = 10 GB, SSD 2 = 30 GB, whereas the Next Generation Firewall is using 2 NICs.
2. Web Application Firewall: The second layer is the Web Application Firewall with 2vCPU server specifications, 8 GB of memory, SSD 1 = 10 GB, SSD 2 = 30 GB.

To increase cloud-based web application services security provided by companies, we chose both technologies mentioned above. In cloud computing, we can use Pay as You Go (PAYG) services. So, companies do not have to purchase licenses to use the technologies.

4. Result and Discussion

In this chapter, we are going to evaluate our proposed cloud computing architecture to find out their capabilities. There will be 2 steps, the first step is to determine the cloud computing architecture design that is being used. Second, we create a prototype based on our cloud computing architecture design. We are doing the penetration testing by using the SQL injection and malicious file injection testing methods to evaluate the design. These are the test scenario by using the penetration testing method:

1. We use the SQLMAP tool to execute 3 (three) SQL command scripts, which can be seen in table 3 to attack the cloud-based web application.
2. We use the upload feature on the company's web application to send 200 Malicious Files to the cloud environment.

After the penetration testing process is complete, we collected logs and reports from each security layer. Afterward, we analyze the logs and reports. The results of the SQL injection can be seen in table 3 and the results of the malicious file injection can be seen in figure 7.

4.1. SQL Injection

The first penetration testing method that we use was SQL Injection using SQLMAP tools. According to [14], SQL Injection is a method to test web application security by sending malicious code to the server. We did this practice in order to prevent any threat in the future because every client's personal data are stored in the cloud-based web application. Table 2 is a comparison between using firewall security provided by the Cloud Service Provider (CSP) and multi-layered security cloud computing architecture.

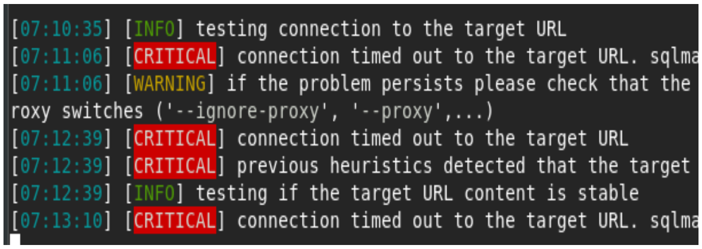
Table 2 shows that the firewall that the company currently using unable to prevent or detect SQL Injection threats. This confirms that the database server and cloud computing environments are in danger.

Table 1: SQL Injection Script

NO	SQL Injection Script
1	Python sqlmap.py -u “https://apps.gautamaawijaya.com/Login.aspx?ReturnUrl=%2f” --risk=2 --dbs --dbms= MySQL -- randmon-agent
2	Python sqlmap.py -u "https://apps.gautamawijaya.com/Login.aspx?ReturnUrl=%2f"--data="log=test&pwd=test&wp-submit=Log+in" --dbs --level=3 --risk=2 --dbms=MySQL -- randmon-agent
3	python sqlmap.py -u "https://apps.gautamawijaya.com/Login.aspx?ReturnUrl=%2f" --data="log=test&pwd=test&wp-submit=Log+in" --dbs --level=3 --risk=2 --dbms=MySQL -- randmon-agent --tamper=between,charencode,charunicodeencode,equaltolike,greatest,multiplespaces,percentage,randomcase,sp_password,space2comment,space2dash,space2mssqlblank,space2mysqldash,space2plus,space2randomblank,uionalltounion

Table 2: Comparison of Result

No	Firewall	Cloud Computing Multi-layered Security
1	Pass	Block
2	Pass	Block
3	Pass	Block



```
[07:10:35] [INFO] testing connection to the target URL
[07:11:06] [CRITICAL] connection timed out to the target URL. sqlma
[07:11:06] [WARNING] if the problem persists please check that the
roxy switches ('--ignore-proxy', '--proxy',...)
[07:12:39] [CRITICAL] connection timed out to the target URL
[07:12:39] [CRITICAL] previous heuristics detected that the target
[07:12:39] [INFO] testing if the target URL content is stable
[07:13:10] [CRITICAL] connection timed out to the target URL. sqlma
```

Figure 4: SQL Injection using SQL Map Tools

Figure 4 gives details of the SQL injection process using SQLMAP tools. The figure shows that “CRITICAL connection time out to the target URL”. The message appears because the Next-Generation Firewall and Web Application Firewall have blocked the requests to SQLMAP tools.

Table 3: SQL Injection Result

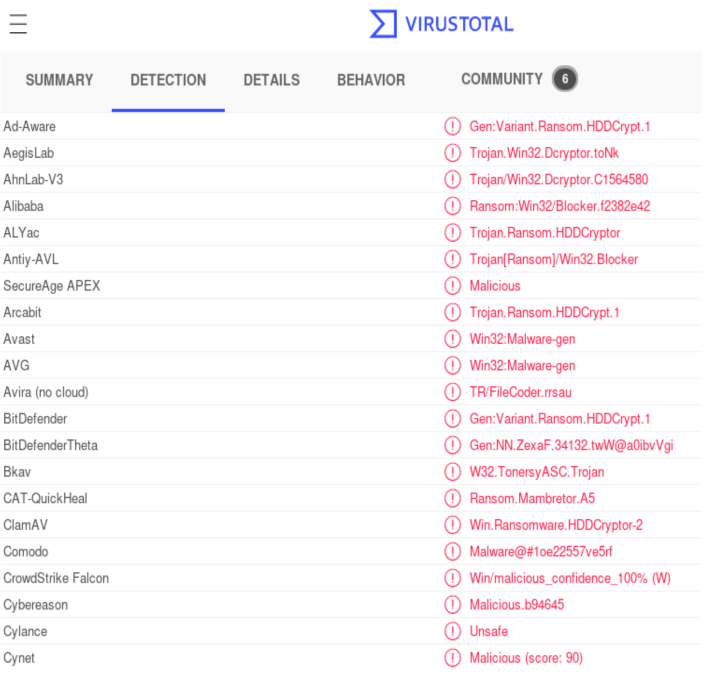
Command	Layer 1	Layer 2
1	Block	-
2	Block	-
3	Pass	Block

Table 3 gives an overview on the ability of each layer to detect SQL injection threats. As explained in the test scheme before, in table 1, there are 3 SQL injection scripts used to evaluate the cloud computing design that we have proposed. The first layer, which is the Next-Generation Firewall, successfully prevent the SQL injection attack script 1 and 2 with the IPS features. Whereas the injection attack script 3 pass the first layer but successfully prevented by the second layer, which is the Web Application Firewall using SQL Injection and XXS features.

4.2. Malicious File Injection

The second method that we use to evaluate the cloud computing architecture design is Malicious File Injection. This method attacks the cloud computing architecture design by sending Malicious Files that have been infected by malware [15]. This method will attack the weakest part of the company's cloud-based web applications. Vulnerability was found in the photo upload feature which can be seen on figure 6. In those features, various types of file extensions can have access. Therefore, we take advantage of this weakness by uploading 200 malicious files.

In the attack process, we download 200 malware sample from the malware-sample-library, malware-sample, the Zoo, and Malware Database-master source. After the download process is complete, we verify 200 files that we are going to use in the evaluation. We confirm the malicious files and upload it to www.virustotal.com.



Ad-Aware	Gen:Variant.Ransom.HDDCrypt.1
AegisLab	Trojan.Win32.Dcryptor.toNk
AhnLab-V3	Trojan/Win32.Dcryptor.C1564580
Alibaba	Ransom:Win32/Blocker.f2382e42
ALYac	Trojan.Ransom.HDDCryptor
Antiy-AVL	Trojan[Ransom]/Win32.Blocker
SecureAge APEX	Malicious
Arcabit	Trojan.Ransom.HDDCrypt.1
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen
Avira (no cloud)	TR/FileCoder.rrsau
BitDefender	Gen:Variant.Ransom.HDDCrypt.1
BitDefenderTheta	Gen:NN.ZexaF.34132.twW@a0ibvVgi
Bkav	W32.TonersyASC.Trojan
CAT-QuickHeal	Ransom.Mambretor.A5
ClamAV	Win.Ransomware.HDDCryptor-2
Comodo	Malware@#1oe22557ve5rf
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.b94645
Cylance	Unsafe
Cynet	Malicious (score: 90)

Figure 5: Virus Total Result

Figure 5 is the test result for one of the Malicious Files that we use. After the verification process complete, we begin the malicious file injection process.

We do the injection process to the weakest part of the photo upload feature. Figure 6 shown the photo upload feature that we used as a test.

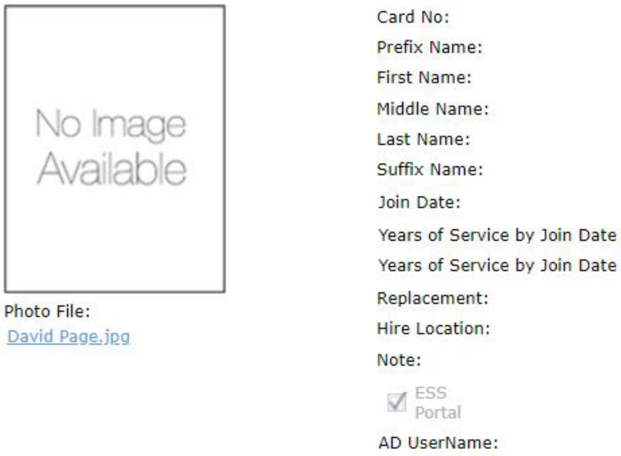


Photo File:
David Page.jpg

Card No:
Prefix Name:
First Name:
Middle Name:
Last Name:
Suffix Name:
Join Date:
Years of Service by Join Date
Years of Service by Join Date
Replacement:
Hire Location:
Note:
☑ ESS Portal
AD UserName:

Figure 6: Feature of Cloud-based Web Application

In these features, we upload 200 malicious files that we have verified before. We repeat the process until all 200 malicious files are successfully uploaded.

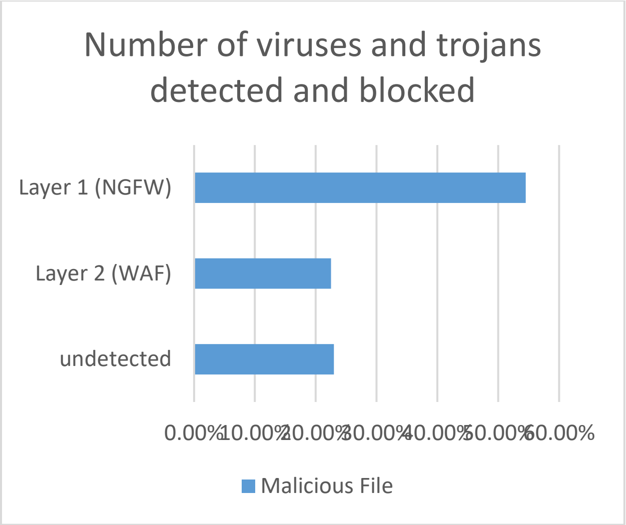


Figure 7: Number of viruses, trojans detected, and blocked

After the attack process is complete, we collect the logs and report from each layer. The logs and reports contain action information on how each layer detect and prevent threats. Figure 7 shows us information about the ability of each layer to identify malicious files. Next-Generation Firewall manage to identify 54.5% of threat on layer one, while at layer 2, the Web Application Firewall manage to detect 22.5% of threat. The total amount detected from this multi-layer security cloud computing architecture is 77%. While there are still 23% of malicious files that are not successfully identified by this architecture.

Table 4 shows the evaluation result using the malicious file injection method. In this evaluation, we divided the type of malware into 4 (four) categories shown in table 4. There is 23% undetected malware pass our proposed cloud computing architecture. To identify the malware, layers 1 and 2 use information from the malware signature database located in each layer. Therefore, the availability of malware information is important to be able to identify malware threats.

Table 4: File Injection Result

Virus Type	Total	L1	L2	detected	Undetected
Ransomware	38	23	7	30	8
Trojan	129	67	34	101	28
Worm and Virus	16	11	3	14	2
Other (Adware, Riskware, Backdoor and EXE infector)	17	8	1	9	8
Total	200	109	45	154	46

Evaluation using penetration testing with malicious file injection provides an overview on the ability of each layer to detect and prevent malicious files from reaching the environment through the application layer. The following is the comparison between firewall security provided by the Cloud Service Provider (CSP) and multi-layer security. The result shows that the firewall cannot detect and prevent malicious file threats. In comparison, multi-layer security manages to detect and prevent 154 file threats, equivalent to 77% of malicious files that have been identified and blocked.

5. Conclusion

Based on the evaluation and testing results, multi-layer security cloud computing architecture can protect company's cloud-based web applications. By using multi-layered security cloud computing, it is proven that it improves the security of cloud-based human resource management services.

Table 5: Comparison Security

NO	Evaluation Method	Existing Security	Multi-Layered Security
1	SQL Injection	PASS	Block
2	Malicious File Collection	PASS	Block

Table 5 is the comparison between security used by company and cloud computing multi-layer security. The current technology used by the company cannot optimally protect company assets. This makes the application, database, and the company's environment is under threat because it cannot detect and prevent threats.

In conclusion, it is important to create a cloud computing design that meets the needs of the company, because the design is going to be implemented to the company as well. Using the System Development Life Cycle (SDLC) method, the author is able to identify the needs, goals, technology, and problems experienced by the company. To improve the security of cloud-based web applications, the authors use multi-layer security architecture by creating several layers of security that can increase security for services provided by companies. The advantages of multi-layer security are each layer can cover its weaknesses in preventing and detecting threats. The result can be seen in our evaluation using the SQL Injection and Malicious File Injection methods. Assessment using these two methods provide an overview on how the multi-layer security architecture secures cloud-based web applications.

The result of this paper is to describe how to secure cloud-based web applications using multiple layers of security methods. Combining the Next Generation Firewall (NGFW) and Web Application Firewall (WAF), can maximize cloud-based web applications security as well. Many security technologies can be combined to secure cloud-based web applications.

Acknowledgment

The research publication is fully supported by Bina Nusantara University.

References

[1] H. Takabi, J.B.D. Joshi, G.J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security and Privacy, **8**(6), 24–31, 2010, doi:10.1109/MSP.2010.186.

[2] M. Almorsy, J. Grundy, I. Müller, "An Analysis of the Cloud Computing Security Problem," International Surgery, **47**(3), 288–290, 2016, doi:arXiv:1609.01107.

[3] E. Abdurachman, F.L. Gaol, B. Soewito, "ScienceDirect ScienceDirect Survey on Threats and Risks in the Cloud Computing Environment Survey on Threats and Risks in the Cloud Computing Environment," Procedia Computer Science, **161**, 1325–1332, 2019, doi:10.1016/j.procs.2019.11.248.

[4] M. Jouini, L.B.A. Rabai, "A Security Framework for Secure Cloud Computing Environments," International Journal of Cloud Applications and Computing, **6**(3), 32–44, 2016, doi:10.4018/ijcac.2016070103.

[5] G.I.P. Duppa, N. Surantha, "Evaluation of network security based on next generation intrusion prevention system," Telkomnika (Telecommunication Computing Electronics and Control), **17**(1), 39–48, 2019, doi:10.12928/TELKOMNIKA.v17i1.9191.

[6] P. Oppenheimer and T.-D. N, Top-Down Network Design Top-Down Network Design, 2010.

[7] M. Wairisal, N. Surantha, "Design and Evaluation of Efficient Bandwidth Management for a Corporate Network," Proceedings of 2018 International Conference on Information Management and Technology, ICIMTech 2018, (September), 98–102, 2018, doi:10.1109/ICIMTech.2018.8528162.

[8] A. Rot, B. Olszewski, "Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection," in Position Papers of the 2017 Federated Conference on Computer Science and Information Systems, 113–117, 2017, doi:10.15439/2017f488.

[9] N. Khan, A. Al-Yasiri, "Cloud Security Threats and Techniques to Strengthen Cloud Computing Adoption Framework," International Journal of Information Technology and Web Engineering, **11**(3), 50–64, 2016, doi:10.4018/ijitwe.2016070104.

[10] J. Surana, K. Singh, N. Bairagi, N. Mehto, N. Jaiswal, "Survey on Next Generation Firewall," IJEDR - International Journal of Engineering Development and Research, **5**(2), 984--988, 2017.

[11] C, "Web application firewall using XSS," International Journal of Engineering & Technology, **7**(2.7), 941, 2018, doi:10.14419/ijet.v7i2.7.11429.

[12] V. Chang, M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," IEEE Transactions on Services Computing, **9**(1), 138–151, 2016, doi:10.1109/TSC.2015.2491281.

[13] V. Chang, Y.H. Kuo, M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," Future Generation Computer Systems, **57**, 24–41, 2016, doi:10.1016/j.future.2015.09.031.

[14] A. Hasan, D. Meva, "Web Application Safety by Penetration Testing," 4TH International Conference on Cyber Security (ICCS), (January), 159–163, 2018.

[15] K. Pooj, S. Patil, "Understanding File Upload Security for Web Applications," International Journal of Engineering Trends and Technology, **42**(7), 342–347, 2016, doi:10.14445/22315381/ijett-v42p261.