Implementation of firewall for web server access management based on application gateway for TNI AD website

M L N Suryana*, N R S Muda, D Minggu, R Agustiady and C Herkariawan

Military Telecommunications, POLTEKAD. Jl. Ksatrian Arhanud, Junrejo, Batu 65324, Indonesia

*luthfinazif@gmail.com

Abstract. Along with the development of information technology, making information security is very important even more so on a network connected to the internet. The imbalance between each development of a technology not accompanied by development in the security system itself. As for the current problem is that there are still state website that are still working with outside companies in terms of network security systems. And most often the target of cyber attacks is the web server. Then any individual or organization is required to have a security system that minimizes of cyber crime. Instead of putting trust in an outside company I better make my own web server security system. The author uses the application gateway method in a firewall. Besides, firewall failover capabilities are evaluated. Based on the overall testing results, application gateway has better performance than other types of firewalls in another website. It has better ability in handling DoS attack, because this firewall works not only based on the secure, destination and attribute of the package, but can reach the contents of the package. It is concluded that application gateway is suitable and safe to use on TNI AD web server.

1. Introduction
The rapid development of information and communication technology is a place where important state secrets are placed. In addition, information and communication technology has a variety of influences as one of the country’s major cyber security strategies in facing the threat of cyber warfare because information and communication technology has various functions [1]. With the world’s concerns about the threat of cyber warfare, it is necessary to apply good national cyber security to provide protection for information held by military units. In carrying out military duties, the confidentiality of information and messages carried is a very important and risky activity in military operational duties [2]. In this case, website facilities especially those owned by TNI AD do not rule out the possibility of hacking or cracking the data from cyber threats. The attack was in the form of a hacker attack that intended to steal and damage the network on the website.

In this study, we will compare application gateways with other firewalls in another website, look for vulnerability assessment on several TNI AD websites, and firewall performance by running FTP service normally and under DoS attacks [3].

2. Vulnerability assessment
In this section, the author will compare the application gateway that is implemented on the poltekad website with the other websites, websites that will be tested for vulnerability belong of the ranks of the TNI AD [4]. Here I test two websites namely tniad.mil.id, and kodiklat-tniad.mil.id, to look for
vulnerability assessment of the website. The author uses two software namely ZAP (Zed Attack Proxy) and Acunetix. ZAP is an open source web application security scanner. And Acunetix is an automated web application security testing tool that can audit web applications.

2.1. ZAP (Zed Attack Proxy)
The first vulnerability process using ZAP generates vulnerability data obtained on the TNI AD website. Vulnerability data obtained amounted to 14 vulnerability data with details of 6 data at medium level and 8 data at low level, and at high level there were no vulnerabilities found as shown in table 1.

Table 1. The result of the vulnerability assessment using zap.

| Host          | Alert Group                                      | Severity | Alert Count |
|---------------|--------------------------------------------------|----------|-------------|
| Server Website | Style-src unsafe-inline                          | Medium   | 4           |
| Website       | Cross Origin Resource Sharing (CORS) misconfiguration on the web server | Medium   | 2           |
|               | Absence of Anti-CSRF tokens                      | Low      | 4           |
|               | Content-Security-Policy                          | Low      | 4           |

Table 1 shows some vulnerabilities, one of them at the medium level, namely Cross Origin Sharing (CORS) misconfiguration on the web server. The second process is on Kodiklat website. Vulnerability data obtained amounted to 83 vulnerability data with details of 11 data at the medium level and 72 at the low level, and at the high level there were no vulnerabilities found as shown in table 2.

Table 2. The result of the vulnerability assessment using zap.

| Host          | Alert Group                                      | Severity | Alert Count |
|---------------|--------------------------------------------------|----------|-------------|
| Server Website | Cross-Domain Misconfiguration                     | Medium   | 6           |
| Website       | X-Frame Options Header Not Set                    | Medium   | 5           |
|               | Cookie Without Samesite Attribute                 | Low      | 1           |
|               | Cookie Without Secure Flag                        | Low      | 1           |
|               | Incomplete or No Cache-control and Pragma HTTP Header set | Low      | 22          |
|               | Private IP Disclosure                              | Low      | 1           |
|               | X-Content-Type-Options Header Missing             | Low      | 47          |

Table 2 shows some vulnerabilities, one of them at the medium level, namely X-Frame Options Header Not Set, and not included in the HTTP response to protect against ‘ClickJacking’ attacks.

The third process is on poltekad website. Vulnerability data obtained amounted to 3 vulnerability data with details of 1 data at the medium level, 2 data of the low level, and at high level there were no vulnerabilities found as shown in table 3.
Table 3. The result of the vulnerability assessment using zap.

| Host     | Alert Goup                                | Severity | Alert Count |
|----------|-------------------------------------------|----------|-------------|
| Server   | HTML form without CSRF protection         | Medium   | 1           |
| Website  | poltekad.ac.id                           |          |             |

2.2. Acunetix

The first scanning process using Acunetix generates vulnerability data on the TNI AD website. Vulnerability data found amounted to 1 which is in the medium level, for high and low levels not found as seen in table 3.

Table 4. The result of the vulnerability assessment using acunetix.

| Host     | Alert Goup                                | Severity | Alert Count |
|----------|-------------------------------------------|----------|-------------|
| 1. Server|                                           |          |             |
| 2. Website | tniad.mil.id                             |          |             |
| 3. HTML form without CSRF protection |               | Medium   | 1           |
| 4. Medium |                                           |          |             |

Table 4 shows some of vulnerability, at the medium level, namely HTML form without CSRF protection, an attacker may force the users of a web application to execute actions of the attacker’s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

The second scanning process using acunetix generates vulnerability data on the Kodiklat website. Vulnerability data obtained amounted to 8 vulnerability data with details of 1 data at the high level, 6 data at the medium level, and 1 data at the low level as shown in table 5.

Table 5. The result of the vulnerability assessment using acunetix.

| Host     | Alert Goup                                | Severity | Alert Count |
|----------|-------------------------------------------|----------|-------------|
| Server   | Possible Database Backup                  | High     | 1           |
| Website  | kodiklat-tniad.mil.id                     |          |             |
| Website  | HTML form without CSRF protection         | Medium   | 6           |
| Website  | ClickJacking                              | Low      | 1           |

Table 5 shows some of vulnerability, at the high level, namely Possible Database Backup, this file may disclose sensitive information. This information can be used to launch further attacks.

The third process is on poltekad website. Vulnerability data obtained amounted to 2 vulnerability data with details of 2 data at the low level, at medium level and high level there were no vulnerabilities found as shown in table 6.

Table 6. The result of the vulnerability assessment using acunetix.

| Host     | Alert Goup | Severity | Alert Count |
|----------|------------|----------|-------------|
| Server   | Website    |          |             |
| Website  | poltekad.ac.id |     | ClickJacking | Low  | 2           |

2.3. Performance testing

In this testing, there were two test parameters discussed: page speed, loaded times. It can be see on Figure 1 and Figure 2.
3. Conclusion
In this study, we know that the application gateway method for securing a web server is not inferior to a security system outside the company even though there are still shortcomings, as we see from tables 1 to 6 implementation with the application gateway method on the poltekad website has a slight vulnerability compared on two other websites. and also on the performance tests, as we saw in Figure 1 and 2 the Poltekad website has a performance degradation that is not far enough between normal tests and attack tests compared to the other two besite. In conclusion, the implementation of the poltekad website is the application gateway method is suitable and safe on TNI AD web server.

Acknowledgments
The author would like to thank Politeknik of Army for supporting this research.

Reference
[1] Maheshwari R, Krishna C R and Brahma M S 2014 Defending network system against IP spoofing based distributed DoS attacks using DPHCF-RTT packet filtering technique Proc. 2014 Int.
[2] Maj S P, Makasiranondh W and Veal D 2010 *An Evaluation of Firewall Configuration Methods* IICSNS Int. J. Comput. Sci. Netw. Secur. pp 1–7

[3] Azzam A T, Munadi R and Mayasari R 2019 *Performance Analysis Of Firewall As Virtualized Network Function On VMware ESXi Hypervisor* J. Infotel pp 11-29

[4] Gupta S and Gupta B B 2017 *Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art* Int. J. Syst. Assur. Eng. Manag. pp 512–30