International Journal of Engineering & Technology, 7 (3.33) (2018) 183-186

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Study on Comparison of Network Location Efficiency of Web Application Firewall

Sung-Ho Cho[1], Sung-Uk Choi*

[1]Research Scholar, Department of Computer Engineering, Incheon National University
**Research Scholar, Department of Computer Engineering, Incheon National University*
**Corresponding author E-mail: swchoi@inu.ac.kr*

Abstract

This paper proposes a method to optimize the performance of web application firewalls according to their positions in large scale networks. Since ports for web services are always open and vulnerable in security, the introduction of web application firewalls is essential. Methods to configure web application firewalls in existing networks are largely divided into two types. There is an in-line type where a web application firewall is located between the network and the web server to be protected. This is mostly used in small scale single networks and is vulnerable to the physical obstruction of web application firewalls. The port redirection type configured with the help of peripheral network equipment such as routers or L4 switches can maintain web services even when physical obstruction of the web application firewall occurs and is suitable for large scale networks where several web services are mixed. In this study, port redirection type web application firewalls were configured in large-scale networks and there was a problem in that the performance of routers was degraded due to the IP-based VLAN when a policy was set for the ports on the routers for web security. In order to solve this problem, only those agencies and enterprises that provide web services of networks were separated and in-line type web application firewalls were configured for them. Internet service providers (ISPs) or central line-concentration agencies can apply the foregoing to configure systems for web security for unit small enterprises or small scale agencies at low costs.

Keywords: *Web Application Firewall, In-Line Type, Port Redirection Type*

1. Introduction

Currently, basic personal information is frequently requested for the use of web services, attacks aimed to extort data and personal information are increasing, and when occurred, the resultant accidents lead to serious degradation of organizational images and economic losses. [1]

The overall web security measures consist of largely three kinds; measures on the client side such as the enhancement of security levels on the browser, periodic updates of security patches, and the reinforcement of user authentication; measures on the side of servers such as the monitoring of script security management and Java applets, control of access to web servers, and integrity protection; and measures on the side of the security of transmission between the server and clients such as the process of encryption intended to prevent falsification and HTTPS(Hypertext Transfer Protocol over Secure Socket Layer) using SSL(Secure Socket Layer) [2,3].

The web application firewall system is an essential piece of equipment to protect security on the server side and the security of transmission between the server and clients. The Open Web Application Security Project (OWASP) announces the status of vulnerability to web attacks of high priorities every year, and web application firewall engines are continuously updated against those attacks to prepare defense systems [4].

In addition to the system engine updates, efficient configuration of defense systems on networks is important. There are various methods to design web application firewall systems according to the scales of networks. In the dilemma of the situation where the enhancement of security levels leads to the degradation of web service performance and performance centered design leads the drop of security levels, the method to maintain the security level that would achieve the most efficient web services should be pursued[5,6].

In the case presented in this study, a web application firewall system is configured in an integrated network in which the lines of more than 600 agencies have been concentrated.

Since there are areas where web security is vulnerable other than the sections defended by the existing web application firewalls as shown in Figure 1, additional web application firewalls were introduced. Based on general previous studies, systems that satisfy both performance and security were designed so that good outcomes could be obtained[7,8].

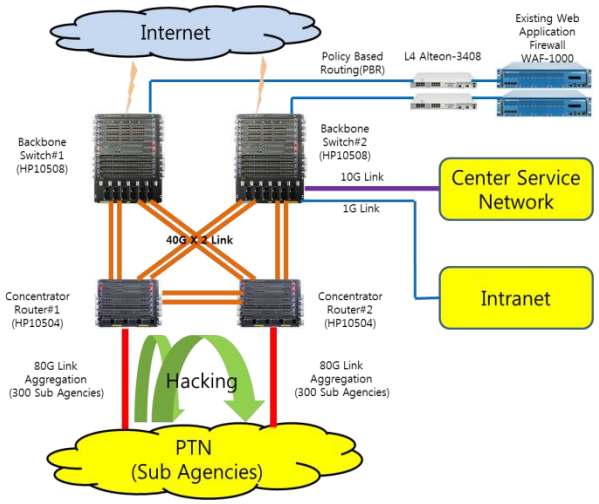

Fig. 1: The network being studied

2. The Related Technology Status

The positions of web application firewalls can be configured in various methods depending on network environments and web server environments. Basically, there are in-line type configurations and port redirection type configurations[9].

2.1. In-Line type

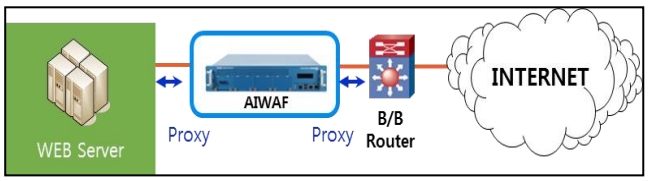

Fig. 2: In-Line type web application firewall configuration

This is a method to configure web application firewalls in-line in the form of bridges on network paths. This type of web application firewalls operates in the transparent proxy mode without any IP.

Theses web application firewalls provide most of the web security functions that can be provided by equipment. They are located between web server connection sections and are connected only with port links. They are mainly affected by switches and web server network interfaces.

They are mainly operated by agencies or enterprises consisting of small scale single networks. This type of configuration is used when network flows are lower than the network interface standard of the web application firewalls. This the simplest type of web application firewall equipment configuration that enables managers to pay attention to only the management of security policies. A disadvantage is that service interruptions may occur when the web application firewall is physically obstructed.

2.2. Port redirection type

In cases where multiple web servers are operated instead of a single web server farm, if the relevant web servers are configured on different networks, it will be too costly to configure the web servers in the in-line type on each of the relevant networks. This problem is solved by the port redirection type configuration.

L4 equipment for VIP (Virtual IP) configuration is required, and the port redirection function is required in L4. It is a structure in which bidirectional web traffic is redirected in both in/out directions. This type of configuration is used when multiple web services are operated and the services should be provided continuously without any stop even when web application firewalls fail.

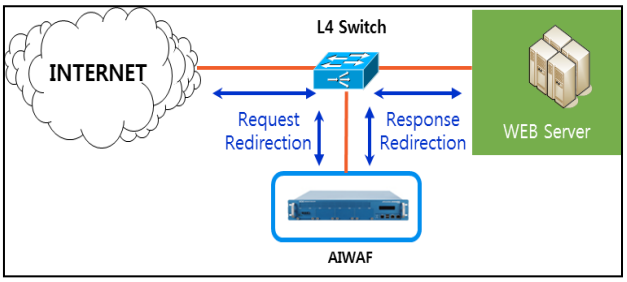

Fig. 3: Port redirection type web application firewall configuration

Even when web application firewalls have been interrupted due to a power supply problem, there is no problem in the provision of services only if the L4 Switch is free of faults.

The network currently studied is in this configuration.

3. Implementation

As can be seen in Fig. 1, web access from the outside is policy-based routed (PBR) by the backbone switch and sent to the L4 switch. Only those sessions that are permitted for web access by the web application firewall linked to the L4 switch can go to the center service network or the intranet.

Accesses from all the sub-agencies located at the bottom of the internal PTN (Packet Transfer Network) can also be connected to the center service network or the intranet only after going through the L4 and web application firewall by PBR at the backbone switch. The ports of all web services are unified as 80, 8080, 443. It can be said that all accesses to the center service network and the Intranet are controlled.

A problem is that cases where a web service of a sub-agency is accessed from another sub-agency are vulnerable to hacking because such accesses are not applied with PBR because such accesses do not go through the backbone switch. To solve this problem, new web application firewalls were introduced to configure the system. Because the system is a large scale network, it was configured as shown in Fig. 4 based on port redirection.

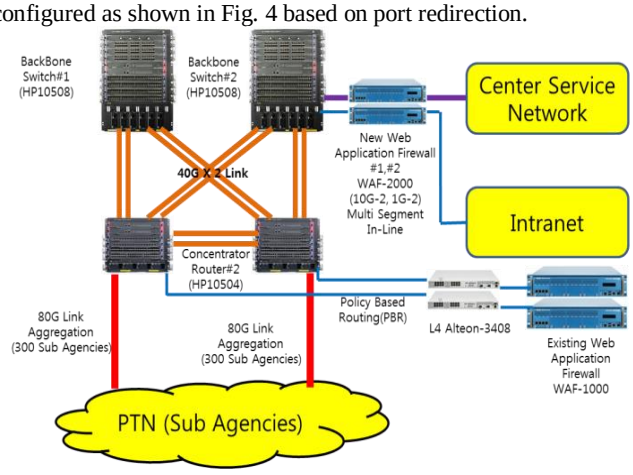

Fig. 4: Port redirection type based design

The PBR of the existing backbone switch was applied to the concentrator router and the new web application firewall was in-line configured in multi-segments on the center service network and the Intranet. This is a design that requires accesses from sub agencies to follow PBR and requires accesses from the outside to the center service network or the Intranet to go through the new web application firewall. In the concentrator router, 300 IP-Based VLANs are configured for each sub agency and when PBR was entered to apply 34 policies by 80,8080,443 port, around 10,000 commands were entered.

The router system was down because the ACL of the router could not accommodate the large volume of commands and the network service. This indicated that the entire performance was degraded

for security because the performance of the router could not support.

As shown in Fig. 5, among the sub agencies, only those agencies that provide web services were separated to configure one physical port and the traffic did not exceed 10G, which is allowed to the interface of the new web application firewall. Since PBR policies could not be implemented, the system was configured into an in-line type. The IP for access from the existing web application firewall to the web services of the sub agencies was changed into 'allowed' to further reduce the load and the web vulnerability of the web services of the sub agencies could be defended in the new web application firewall.

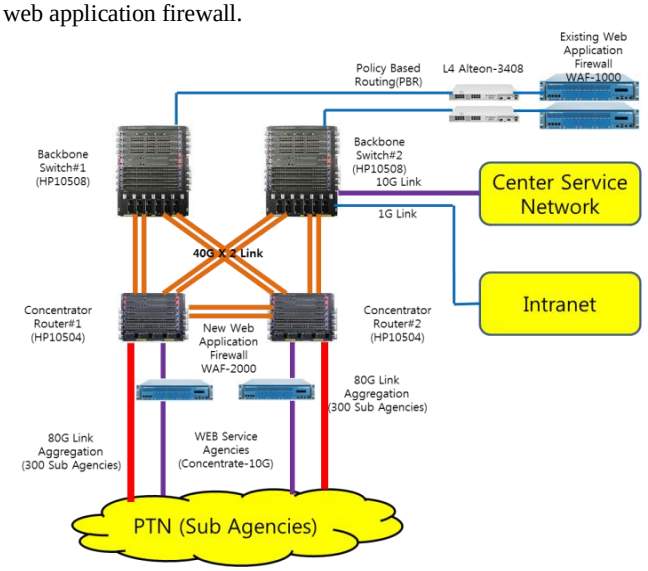

Fig. 5: Web service sub agency networks were separated to design the system into an in-line type

In the port redirection type based design, the new web application firewall covered the center service network and the intranet, which had been covered by the existing web application firewall and the system was in-line configured.

The network traffic was around 2.6 Gbps and accesses to all other ports were also controlled in addition to accesses to the 80, 8080, 443 port. The web traffic was also shown to be 250 ~ 300Mbps, which was the existing level, and the configuration enabled the maximum equipment performance compared to the network traffic. Since the existing web application firewall was transferred to the concentrator router to protect only the web services of the sub agencies, the web traffic was expected to be very small and the network traffic was expected to be at a similar level because of the PBR.

As a result, because of the IP-Based VLAN policy of the concentrator router, PBR was applied to each VLAN so that many commands were loaded on the router, and system down became to occur in the process of separating the web traffics.

Although this design is the most reasonable in terms of the performance of traffic management, problems occurred in the network configuration per se.

Since the sub-agency network was separated, the network traffic was set up to 3.6Gbps in the in-line type design, and the actual web traffic was below 200Mbps.

Table 1: Comparison of the performances of the two types of design

Division	Designed by Port Redirection type	Designed by In-Line type with sub-agencies network separating
Network environment and traffic	New WAF : 10Gbps + 1Gbps Multi-Segment (2.6Gbps traffic)	New WAF : 10Gbps (Max 3.6Gbps traffic)
	Existing WAF : 1Gbps (Cannot measure traffic : Router System Down)	Existing WAF: 1Gbps (300Mbps traffic)
Web traffic	New WAF : 10Gbps + 1Gbps Multi-Segment (250~300MbpsWeb traffic)	New WAF : 10Gbps (Under 200Mbps Web traffic)
	Existing WAF: 1Gbps (Cannot measure traffic: Router System Down)	Existing WAF: 1Gbps (250~300Mbps Web traffic)
WAF Spec	New WAF	Throughput : 9.8Gbps NIC : 10Gbps 2Port (In/Out),
	Existing WAF	Throughput : 4Gbps NIC : 1Gbps 4Port (In2/Out2)

Although this value is lower than that of existing web application firewalls, this design can be said to be the best choice considering the network bandwidth extension that will be implemented hereafter and that the situation where web service agencies are increasing.

4. Conclusion

It is costly to configure web security systems according to network capacities and allowed interfaces. Web application firewall systems should be designed considering future extendability from the beginning because they require not only simple installation but also continuous monitoring, relevant policies should be changed in real time according to the environment, and the systems cannot be easily upgraded.

The most hopeful outcome is that even in the case of large-capacity networks, web service security systems that have no problem in low cost high quality services can be constructed if only web service traffic is well separated and the system is appropriately configured when necessary.

Application security equipment is still expensive compared to general network equipment and requires many workers inputted into maintenance. By applying this study, ISP companies will be able to construct a system that can provide many small or medium enterprises that are reluctant to introduce expensive security application equipment with web application firewall services at low prices by combining only enterprise web servers with VPN or other ways.

In addition, if strong medium enterprises, which operate a computer room, provide e-commerce centered services without providing streaming or high-bandwidth services in particular, they can reduce the network bandwidth of web servers through QoS to introduce low-priced 100Mbps or lower level web application firewalls when they construct web security systems.

References

[1] Lee ST, LEE BK, "Web Security Threat and Security in the Cloud Computing Using Web Application Firewall", *Institute of Control, Robotics and Systems*, Vol. 2012, No. 7, (2012), pp. 239-248.

[2] Noh SC, Jun IS, Kim KN, "Verification Method of Insuring Web Application Security", *Journal of Information and Security*, Vol. 3, No. 2, (2003), pp. 11-20.

[3] Jang SM., Won YH. "Design and Implementation of a Web Application Firewall with Multi-layered Web Filter", *Journal of the Ko-*

rea Society of Computer and Information, Vol 14, No.12, (2009), pp. 157-167.
[4] http: //www.owasp.org, last visit: 02.06.2018.
[5] Kim JS, "A Study on the improvement for Authentication and Session Management in Web Application", *Master. Thesis*, Korea University, Seoul, Republic of Korea, 2005.
[6] Chang MS, Lee JI, "Harmful Traffic Analysis of Web Application" *The Korean Entertainment Industry Association*, Vol. 2, No. 1, (2008), pp. 74-77.
[7] Makiou, Abdelhamid S, Ahmed B, Youcef, "Toward a Novel Web Application Firewalls Architecture" *Journal of Information Assurance and Security*, Vol. 10, No. 4, (2015), pp.164-173.
[8] Baranov, Petr AB, Eldar R, Hong, "Securing Information Resources Using Web Application Firewalls", *BIZNES INFORMATIKA-BUSINESS INFORMATICS*, Vol. 34, No. 4, (2015), pp. 71-78.
[9] Monitorapp Tech Center, https://blog.naver.com/monitorapp_co/, last visit: 05.06.2018.