International Journal of Education and Humanities
ISSN: 2770-6702 | Vol. 14, No. 2, 2024

Thinking and Research on the Construction of Web Application Firewall in Smart Campus Environment

Lingyun Hu[1], Shuai Wen[2], Hongjun Yuan[3, *]

[1] School of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu, Anhui 233030, China
[2] Library and Information Center, Anhui University of Finance and Economics, Bengbu, Anhui 233030, China
[3] School of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu, Anhui 233030, China
[*] **Corresponding Author:** 120081388@aufe.edu.cn

Abstract: With the rapid development of information technology, the Internet has penetrated into various fields, especially the field of education. As an important carrier of education informatization, smart campus provides strong support for improving education quality and management level. However, the network security problems of smart campus also come up, especially the security problems of Web applications. Web Application Firewall, as an important network security technology, plays a vital role in the construction of smart campus, and is of great significance for guaranteeing the information security of smart campus. This paper mainly discusses how to effectively build a Web Application Firewall in a smart campus environment, including the design, configuration, and management of the firewall, in order to safeguard the security of the smart campus network.

Keywords: Smart Campus, Web Application Firewall, Design, Configuration, Management.

1. Introduction

With the rapid development of Internet technology, Web applications have penetrated into people's daily life, especially in the field of education, Web applications have become an important tool for teaching, management and other important aspects. However, the security problems of Web applications are also becoming more and more prominent, especially in a special environment like smart campus. The security problems of Web applications in the smart campus environment are mainly manifested in the following aspects:

First, the problem of insufficient information protection is prominent. A large part of the information security risks in colleges and universities is due to insufficient information protection, including browser vulnerabilities, cross-site scripting attacks (XSS), cross-site request forgery (CSRF), clickjacking, SQL injection, code injection, file uploading vulnerabilities, etc., leading to information theft, leakage, or tampering. The main users of the network system of colleges and universities are college students, but college students lack sufficient attention to information security, and colleges and universities do not carry out information security education, which may lead college students to log into illegal websites during the process of browsing information, which results in the invasion of hackers and Trojan horses.

Second, information security management loopholes. At present, in the process of information security management in colleges and universities, the problem of unsound system is more common, which leads to more information security management loopholes, thus causing information leakage and virus invasion. According to the current stage of the situation, the college information security management system is not sound resulting in information leakage, Trojan horse invasion accounted for a higher proportion, to the development of information technology in colleges and universities has brought a very negative impact.

Third, the investment in security facilities is insufficient. The development of information security design work in colleges and universities has made certain achievements with the development of informationization in colleges and universities, but there are still many shortcomings. There are some differences in the construction of security facilities in various colleges and universities, some colleges and universities attach great importance to it, invest more in security facilities, and improve security facilities. In view of this situation, the process of information security management in colleges and universities, it is necessary to increase the investment in security facilities and build a perfect protection system in order to prevent the risk of information security in colleges and universities.

These problems not only threaten the security of the campus network, but also have a serious impact on students' learning and life. Therefore, how to build an effective Web Application Firewall in the smart campus environment has become an important issue nowadays.

2. Web Application Firewall

Web Application Firewall, also known as Web Application Firewall (hereinafter referred to as: WAF), is a product that specifically protects Web applications by enforcing a series of security policies against HTTP/HTTPS. It is mainly used to defend against attacks on the Web application layer, such as SQL injection, Web page tampering, cross-site scripting, command injection, Cookie/Session hijacking, parameter tampering, buffer overflow, log tampering, application platform vulnerabilities, HTTP attacks and other attacks, detect and verify user-initiated access in order to ensure the legitimacy of the user, and block the illegitimate users in a timely manner, thus effectively protecting Web applications. It detects and verifies user-initiated access requests, ensures the legitimacy of users, and blocks illegitimate users in a timely manner to effectively protect Web applications.

WAF is like a protection guard for web servers, and the protection of Web sites is divided into the following three stages:

Firstly, beforehand: Web vulnerability scanning. Using WAF's built-in scanning tools, we can scan the website for vulnerabilities, get a security level assessment, and remind

users to raise their security awareness.

Secondly, during the process: policy configuration, self-learning policies. By configuring various types of policies, WAF is able to protect the server in real time according to the user's needs, such as blocking the entry of blacklists and allowing whitelists to pass. By configuring self-learning policies, WAF can learn from site data and traffic characteristics to configure accurate whitelisting policies, realizing more accurate protection for servers.

Thirdly, after the fact: security delivery. Even if the attacker breaks through the pre-protection and in-protection and maliciously tampers with the Web page content, the WAF blocks the tampered content through the anti-tampering policy, protects the files on the Web server, and lets the user get the normal Web page.

The necessity of Web Application Firewall applied in campus network is mainly reflected in the following three aspects:

Firstly, it can realize centralized security management. The centralized security management of campus network is an important guarantee for the security of campus network. The universality of the network attracts millions of people to exchange and collect information on the network, in which case unethical behavior or illegal rules can not be avoided. Therefore, in the design of campus network, it is necessary to apply Web Firewall to screen all requests and allow only the requests that meet the requirements to pass, and then limit the bad behaviors on the network.

Secondly, effective protection of the campus network: Web Firewall can disconnect the network segments from the network, so that when one of the network segments has a problem, it can cut off the connection to protect other network segments in the network, preventing the problem from affecting the entire network propagation process, leading to paralysis of the campus network. At the same time, Web Firewall can provide effective defense against common viruses on the network, so as to avoid the leakage of information on the campus network, or the website being invaded by viruses.

Thirdly, realize the statistics of network usage. As the Web Firewall is an intrusion prevention system, it is the channel through which all information must enter and exit. Therefore, the use of Web Firewall can realize the information on the actual use of the system or network. In addition, as the only access point of the network, Web Firewall can record the communication between its own network and the external environment to facilitate the statistics of network access.

In the smart campus environment, Web Application Firewall can help schools resist various network attacks, protect the personal information of students and staff, and ensure the normal operation of teaching and management information systems. Therefore, building an effective Web Application Firewall is of great significance to safeguard the security of campus network.

3. Design of Web Application Firewall

In a smart campus environment, the design of Web Application Firewall needs to consider the following aspects:

Security: Ensure Web applications are protected from various network attacks, such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), etc. The WAF should have the ability to monitor and intercept malicious traffic in real time, as well as the ability to respond quickly to known vulnerabilities.

Performance: While ensuring security, WAF should not affect the performance of Web applications. Low latency, high throughput and scalability should be considered in the design.

Flexibility: WAF should be able to adapt to different types of Web applications, including static and dynamic content. In addition, the WAF should support multiple security policies and rules so that it can be adapted to different application scenarios.

Integration: WAF should seamlessly integrate with existing security infrastructure (e.g., IDS/IPS, SIEM, etc.) for unified management and reporting. At the same time, WAF should also support integration with other security technologies (e.g. SSL/TLS, HTTPS, etc.).

Ease of use: WAF should be simple to configure and manage so that administrators can quickly deploy and maintain it. In addition, the WAF should provide detailed logging and reporting capabilities for analysis and optimization of security policies.

Automation: The WAF should have certain automation capabilities, such as automatically updating the rule base and automatically identifying new threats. This will help improve the response speed and accuracy of the WAF.

Cost-effectiveness: When designing and selecting a WAF, its cost-effectiveness should be fully considered. This includes the cost of hardware and software, operation and maintenance costs, and potential business losses.

In summary, the design of Web application firewalls in a smart campus environment should focus on security, performance, flexibility, integration, ease of use, automation and cost-effectiveness. By taking these factors into consideration, a WAF solution that is both efficient and secure can be designed. The following is the process of Web Application Firewall design in a smart campus environment:

Hardware and Software Selection: Choose a high-performance, high-availability WAF hardware platform, such as Fortinet's FortiGate. Meanwhile, select a mature commercial WAF software, such as Imperva Incapsula.

Security policy formulation: Formulate an appropriate security policy based on the characteristics and needs of the smart campus. This includes access control (e.g., IP address filtering, user authentication, etc.), data protection (e.g., SSL/TLS encryption, data desensitization, etc.), and vulnerability management (e.g., regular patch updates, vulnerability scanning, etc.).

Rule base management: Establish a comprehensive rule base containing rules for detecting and blocking various network attacks. These rules should be updated regularly to adapt to emerging threats. At the same time, provide the function of customizing rules so that they can be adjusted according to specific scenarios.

Real-time monitoring and alerting: WAF has the ability to monitor malicious traffic in real-time and provide timely alerts when abnormal behavior is detected. This helps to quickly detect and respond to security incidents. Alerting methods can include email, SMS, phone calls, etc.

Integration and Collaboration: Integrate WAF with other security devices (e.g. IDS/IPS, SIEM, etc.) to achieve unified management and collaborative defense. In addition, it needs to be integrated with other school systems (e.g., academic affairs system, library system, etc.) to realize more comprehensive security protection.

Logging and Reporting: WAF provides detailed logging and reporting capabilities for analysis and optimization of security policies. This includes access logs, attack logs,

performance logs, and more. Meanwhile, report generation and export functions are supported for regular reviews and audits.

Training and publicity: Provide network security training and publicity to school teachers and students to improve their security awareness and prevention capabilities, which helps reduce security incidents caused by human factors and improve the overall level of security protection.

Automated Operation and Maintenance: Automate the deployment, configuration and management of WAF through automation tools and technologies (e.g. Ansible, Puppet, etc.). This helps to reduce operation and maintenance costs and improve response speed.

With the above solutions, an efficient and secure WAF solution can be realized to effectively protect Web applications in the smart campus environment from various network attacks.

4. Configuration of the Web Application Firewall

In the smart campus environment, the configuration of Web Application Firewall needs to be carried out according to the specific network environment and business requirements. The number of network attacks on university website system is increasing year by year, such as SQL injection attack, XSS attack, etc., which makes the website being tampered, mounted, or even blocked, and seriously affects the normal access of teachers, students and staff to the university website, so it is necessary to deploy Web Application Firewall to improve the security of the website.

The deployment of Web Application Firewall mainly has transparent mode, routing mode, bypass monitoring mode and HA double-click mode to meet the application needs of users of different network structures.

4.1. Transparent Deployment Mode

Transparent deployment mode is to insert WAF between web server and firewall. In transparent mode, Web Application Firewall only analyzes the data flowing through OSI application layer and does not control the traffic of other layers, so the biggest feature of transparent mode is fast, convenient and simple.

4.2. Routing Deployment Mode

The concept of "transparency" of a device deploying a WAF in bridge transparent mode is similar to that in bridge transparent mode. It can be regarded as a routing device, deployed as a router, and ensured that the HTTP traffic to be detected (specified IP address and port) passes through the WAF device. This deployment mode is the highest degree of protection in network security, but it requires certain adjustments to the firewall and the routing settings of the Web application service, which is more demanding for network administrators.

4.3. Bypass Deployment Mode

Bypass deployment mode is to place the WAF under the LAN switch, and all connections to the Web server point to the WAF through the security policy. The advantage is that it has less impact on the network, but in this mode, the Web server cannot obtain the real IP address of the visitor.

4.4. Offline Deployment Mode

In offline mode, the protection engine of WAF is usually deployed on the mirroring port of a switch (switch support is required), which acts as a bystander and listener, only detecting HTTP streams and logging access and attack information without intercepting attacks. The advantage of this mode is that it can not modify the existing network and does not have any impact on the access to the Web server. You can deploy the offline mode to understand the access situation of the Web site and the attack situation, and adjust the configuration parameters of the WAF to adapt to the specific situation of the Web server, in order to prepare for the subsequent deployment of other work modes.

When configuring a Web Application Firewall, you first need to select hardware and software according to the design requirements. Then, it is necessary to configure the rules of the firewall, including access control rules, security policies and so on. In the configuration process, it is necessary to pay attention to the rationality and effectiveness of the rules to avoid rule conflicts or loopholes. The following are some specific configuration measures:

(1) Requirements Analysis: Before you begin, understand the specific needs of your campus network, including the assets to be protected, the types of attacks most commonly encountered, and compliance requirements.

(2) Select WAF type: Choose the appropriate type of WAF for your needs, which may be network-level or host-based, a cloud service or a physical appliance.

(3) Deployment Location: Determine the best location for the WAF to be deployed, typically at the edge of the campus network, between the external Internet and the internal network, to protect all incoming and outgoing HTTP/HTTPS traffic.

(4) Policy Customization: Based on the default policy, adapt and create a rule set appropriate for the campus environment. This may include special protection against attacks such as SQL injection, cross-site scripting (XSS), file uploads, command injection, and more.

(5) Authentication and Authorization: Configure the WAF to support campus authentication mechanisms, such as integrating with the school's LDAP or Active Directory for user authentication and assigning permissions based on roles.

(6) Rule optimization: Refine rules to allow legitimate requests while blocking malicious traffic. Security and usability need to be balanced to avoid false positives affecting normal teaching and learning activities.

(7) Logging: Enable detailed logging to facilitate post-mortem analysis and investigation of potential security incidents.

(8) Monitoring and Reporting: Set up real-time monitoring and regular reporting mechanisms to detect abnormal behavior or potential threats in a timely manner.

(9) Response Measures: When an attack is detected, the WAF should be able to automatically take response measures, such as blocking the attacking IP, sending alerts.

(10) Updates and Maintenance: Regularly update the WAF's firmware, signatures, and rule sets to address emerging threats, and develop and test a disaster recovery plan to ensure that services can be quickly restored in the event of a WAF problem.

(11) Integrate other defenses: WAFs should be integrated with other security measures (e.g., intrusion detection systems, antivirus software, data breach protection systems) to form a multi-layered defense strategy.

(12) Testing and auditing: Regularly test the effectiveness of the WAF, e.g., through penetration testing to verify its effectiveness, and make necessary adjustments.

Through these specific measures, smart campuses can effectively configure and utilize Web Application Firewalls to enhance their network security level.

5. Management of the Web Application Firewall

In a smart campus environment, the management of the Web Application Firewall requires a series of measures to ensure the security and stability of the network. Security is a dynamic process, and the way to maximize the effect of security devices at any time is to use and maintain them effectively, so the daily management of Web Application Firewall is as follows:

(1) Regular system upgrades are performed to strengthen system functions.

(2) Rules are upgraded to improve the protection effect of the system by increasing the files of the built-in rule base.

(3) Backup and restore. Enable the restore point backup function for the Web Application Firewall, so that once the WAF has an abnormal situation and the configuration information (such as the user's policy configuration and system configuration under the security management and system management) is corrupted, you can restore the configuration through the created restore file to realize the restoration.

(4) Check the protection logs on the Web Application Firewall every once in a while, handle intrusion events in a timely manner, and add malicious IPs to the blacklist. For intrusion events that cannot be resolved, contact the WAF vendor for assistance.

(5) Regularly check whether there is any omission in the protection policy and whether the site protection has been realized.

The above management strategies can effectively protect the security of the campus network, and at the same time improve the network security awareness and behavior of users to build a safe campus network environment.

6. Conclusion

In the smart campus environment, the construction of Web Application Firewall is an important means to guarantee the security of campus network. Through in-depth thinking and research on the design, configuration and management of Web Application Firewall, strengthening the security protection of Web applications, as well as improving the awareness of network security, it can effectively safeguard the security of the campus network and provide strong support for the construction of the smart campus. However, since the methods of Web attacks are changing day by day, the construction of Web Application Firewall is an ongoing process that requires continuous research and improvement.

Acknowledgments

This paper is supported by the Undergraduate Teaching Research Project of Anhui University of Finance and Economics (Project number: acjyyb2022019) and the Research Project on Network Security and Informatization of Anhui University of Finance and Economics (Project number: acxxhyb2022005).

References

[1] Chu UK. Research and practice on defense-in-depth system of Web application layer[J]. Computer Age, 2009(11):21-23.

[2] Zhao Lei,Sun Haixing.Research on the application of WAF in enterprise website system[J]. Industrial Technology Innovation, 2015(3):330-333.

[3] Luo Guanghua. An introduction to web application firewall[J]. Technology and Market, 2011, 18(8):9-9.

[4] LIN Meiqin, LI Zhishu, YUAN Xiaoling,et al. Distributed denial-of-service attacks and their prevention[J]. Computer Application Research, 2006, 23(8):136-138.

[5] Zhang Yuqing. Network Attack and Defense Technology [M]. Beijing: Tsinghua University Press, 2011.

[6] Zhao Lei,Sun Haixing.Research on the application of WAF in enterprise website system[J]. Industrial Technology Innovation, 2015(3):330-333.

[7] Jiao Congrong.Application of Web application firewall in university library[J]. Heilongjiang Historical Journal, 2013(15): 184.

[8] Xiang Jingli. Campus network design program based on Web application firewall[J]. Shanxi Electronic Technology, 2016(1): 68-69.

[9] Deng Jing,Gong Jian. Research on WAF based on college private cloud[J]. Journal of Cebu College, 2014, 29(1):80-82.

[10] Chen Jiuzhong,Wang Hao.Application and Security Analysis of Web Application Firewall[J]. Electronic Technology and Software Engineering, 2013(20):249-249.