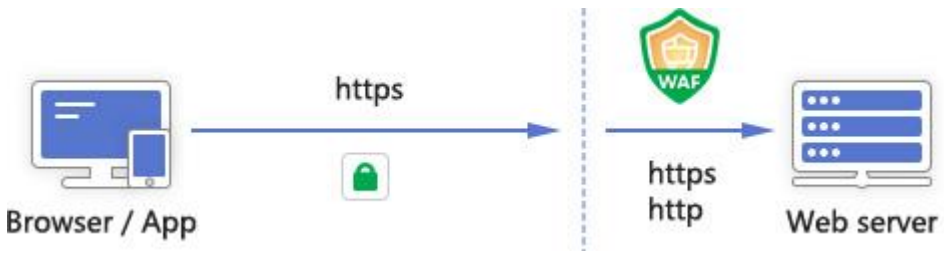
Website security cloud service will surely become the standard for all websites

ZT Browser was launched on June 1 and found that the download was slow, so we enabled Alibaba Cloud CDN. After used the CDN, we found that Alibaba Cloud CDN supports edge WAF protection. We decisively activated the WAF protection. Through these days running, we found that the edge WAF protection performance is good. Therefore, the author decided to add the CDN service for Website Security Cloud Service, and the author asserts that CDN distribution + cloud WAF protection + https encryption + trusted identity validation will become the standard for all websites. trusted identity validation. This article talks about my prediction.

The first element of website security is HTTPS encryption to realize the information transmission from the browser to the server is encrypted to prevent confidential information from leaking in the transmission process, effectively preventing various illegal stealing and illegal tampering. This is the basic requirement, without HTTPS encryption, all browsers will display "Not secure", which is a correct and accurate.

However, only https encryption is not enough, because if the website doesn't have any security protection, various attacks make https encryption meaningless. So, the second element of website security is WAF protection, which is also indispensable. WAF can effectively prevent various attacks and prevent illegal stealing and illegal tampering after the information reaches the server from browser. HTTPS encryption guarantees confidential information to reach the server security, and after the information arrives at the server, the work that prevent various attacks can only be completed by the Web Application Firewall. HTTPS encryption and WAF protection are all duty and one section of each.



However, it is still not enough to have https encryption and WAF protection, because a fake bank website can also easily obtain an SSL certificate to implement https encryption, and it is also very easy to obtain cloud WAF protection, but this is a fake bank website, the author believes no one will think this website is secure! Therefore, website security also needs an important element - website identity validation, which is as important as https encryption and WAF protection! If a website deploys identity validated IV SSL certificate, OV SSL certificate, and EV SSL certificate, it can effectively prove the trusted identity of the website. However, a DV SSL certificate that does not validate the identity of the website and only validates the domain control cannot prove the trusted identity of the website, and other methods are needed to prove the trusted identity, this is the Website Trusted Identity Validation service.

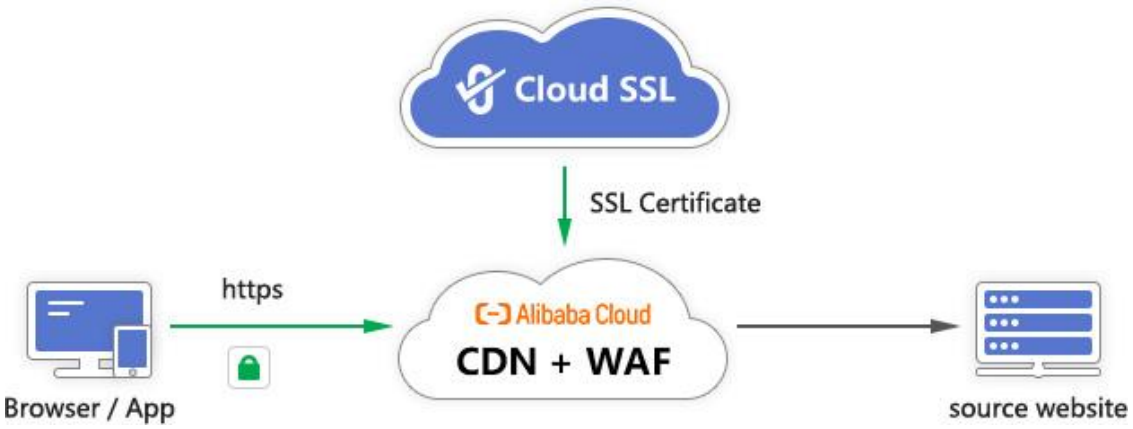
I believe that you have understood why website security requires three aspects of protection through the above explanation: https encryption, WAF protection and trusted identity validation. With these three aspects of protection, the security of the website can be guaranteed. However, how to realize the protection of these three aspects requires the full use of the technical advantages of cloud computing.

The first security protection technology is the realization of https encryption. The traditional way is that the user applies for an SSL certificate from the CA, and then deploys the SSL certificate to the server. However, this process is a relatively painful process and is very troublesome, and even if the virtual hosting website does not support installing the SSL certificate. This is why ZoTrus Technology launched the Cloud SSL service, which realizes the automatic deployment of SSL certificate. Users only need to set up a CNAME domain name resolution to quickly obtain the SSL certificate for https encryption, and whether the user has an independent server and whether it is a virtual host, as long as it is a website that can be accessed by http, https encryption can be easily implemented automatically. This is a typical cloud cryptography service.

The second security protection technology is the realization of WAF protection. The traditional way is that users purchase WAF devices and deploy them at the front of the server to provide security protection for the backend website. However, this protective measure is only suitable for government

agencies and large companies with their own independent computer rooms and servers, it is not suitable for other users who deploy their own websites in the public cloud servers, this case needs for cloud WAF service, users only need to set a CNAME resolution to achieve cloud WAF protection, as long as the website can be accessed by http, cloud WAF protection can be easily achieved. Coupled with the ZoTrus Cloud SSL service, the SSL certificate can be automatically deployed to the cloud WAF, and the cloud WAF protection with https encryption can be realized automatically. This is the technical advantage of the superposition of the two cloud services, so that the user only needs to set the CNAME domain name resolution twice. 10 minutes to achieve https encryption and cloud WAF protection.

In order to improve the response speed of users visiting the website, it is recommended to use CDN content distribution service for the website at the same time, so that the website content, especially the content with large files downloaded, can be distributed to the nodes close to the end user at high speed, thereby greatly improving the user experience. Of course, it must be a CDN service that integrates cloud WAF protection because the cloud WAF protection is a must, and the CDN is the icing on the cake.



The third security technology is the realization of website trusted identity validation. The traditional identity validation method requires the user to fill in the identity validation application form, provide a business license with official seal, the applicant's ID card, phone bill and other supporting documents, and manually finish the validation through the third-party trusted databases such as company registration databases, telephone yellow pages, etc. The Cloud Identity Validation service makes full use of the website filing database of the Ministry of Industry and Information Technology and other big data, once the user enters the domain name to be applied for website identity validation, the first

step verification of website identity can be automatically completed, so the second manual review and confirmation can be completed quickly. This is also due to the popular application of various cloud services.

It can be seen that to ensure the security of the website, https encryption, WAF protection and trusted identity validation must be provided at the same time. To realize these three security protection services, only the use of cloud services can reduce the user's burden, not only can reduce the cost of implementation, but also save users a lot of trouble. Therefore, the author asserts that CDN distribution + cloud WAF protection + HTTPS encryption + trusted identity validation will become the standard for all websites. This assertion is also well-founded. Gartner predicts in the WAF Magic Quadrant report released in September 2021 that by 2024, that is, 2 years later, 70% of organizations will choose cloud WAF services instead of purchasing WAF equipment or Rent WAF equipment.

Richard Wang

June 13, 2022
In Shenzhen, China