ACME vs CWAF

First explain the two names used in the title, "**ACME**" is the abbreviation of Automated Certificate Management Environment, which is an RFC 8555 standard for automated applying SSL certificate and automated deployment of SSL certificate, including ACME clients, protocol both for CA side and server side. "**CWAF**" is the abbreviation of Cloud Web Application Firewall (Cloud WAF). It is a cloud service used to identify and protect malicious features of traffic of websites or APPs, return normal traffic to the web server, and intercept malicious attack traffic.

Today, the ZoTrus Website Security Cloud Service is launched, and this article talks about how we choose the technical route: ACME or CWAF? The company's original product development plan was to provide https encryption services based on ACME standards to provide automatic deployment of SSL certificates, but the product launched today is not this, but https encryption based on cloud WAF services for automatic deployment of SSL certificates. Why this major change in research and development direction, this article discloses more insider details.

In order to ensure the security of the cersign.com website, we chose the Alibaba Cloud WAF service to protect the security of the website when we launched the website. With the cloud WAF service, not only the security of the website can be guaranteed, but also the https encryption service can be realized. This makes me rethink an important question: Do customers still need ACME-style automatic SSL certificate service? Is it necessary for us to develop the ACME client and the SSL certificate issuance system that connects to the ACME client? The ZoTrus Website Security Cloud Service launched today has given the answer, which is a wise choice for my company as a cloud WAF customer, and an

inevitable choice for the technical route of the https encryption service that my company plans to provide.

As we all know, all browsers have already displayed websites without SSL certificates as "Not secure". This is not to scare people by browsers, but it is really NOT secure, because http is transmitted in cleartext. If https is not used for encrypted transmission, then all the confidential information entered on the website is very easy to be illegally stolen and illegally tampered with. To achieve https encryption, you must purchase and apply for an SSL certificate from the CA. After you finally get the SSL certificate, you must install and configure the SSL certificate on the web server to achieve https encryption, and the browser will not display "Not secure" but display the secure padlock.

Applying and deploying an SSL certificate is a relatively painful thing. The author has been with many customers for 17 years, so I have always wanted to provide a solution that can alleviate the pain. Fortunately, there is already a completely free service on the market that can automate the application and deployment of SSL certificates - Let's Encrypt. This free SSL certificate service has won 60% of the global SSL certificate market in just 6 years. Leading other CAs, it has issued 443 million SSL certificates for global users (including Chinese users, of course). The secret of its success is that users only need to install an ACME client software on the server to automatically obtain the free DV SSL certificate valid for 90 days. Why Let's Encrypt is so popular is because users need a simple and hassle-free solution, preferably free. Therefore, other CAs have also started to support the ACME protocol to provide SSL certificates automatically, which is what I originally planned.

However, when we used Alibaba Cloud WAF, I decisively terminated the original R&D plan and changed it to automatic https encryption based on cloud WAF service. This solution is simpler and more convenient than ACME and does not need to install anything on the web server, only need to do CNAME resolution twice. We integrated the cloud SSL service into Alibaba Cloud WAF, realized the automatic configuration of SSL certificate for Alibaba Cloud WAF, thus realizing automatic https encryption based on Alibaba Cloud WAF, different technical routes achieve the same goals we have set to achieve, and it is simpler and more advanced, and at the same time realizes https encryption and website security protection, because only https encryption cannot guarantee the security of the website. The only little regret is that it can't be free because all security guard services have to pay. Fortunately,

cloud services have greatly reduced costs, making cloud WAF services an affordable website security protection service. Our innovative solution has been strongly supported by Alibaba Cloud WAF, and customized an annual subscription plan that customer can afford, which further reduces the cost of using cloud WAF.

What is even more unexpected, and exciting is that the solution of cloud SSL plus cloud WAF has completely solved a technical problem that has puzzled me for many years - virtual hosting customers cannot install an SSL certificate, because this solution does not need to install SSL certificate on the server at all. The website only needs to be converted into the source site of WAF through CNAME resolution, then all browsers will not display "Not secure" for the website.

This is to say, website owner can still choose the ACME solution to realize website https encryption but must have a server and install an ACME client. Now, website owners have a new choice. If they choose our solution, they can not only ensure the website has https encryption but also protect the website from malicious attacks, and but also do not need to install SSL certificate or ACME client software on the server, and does not need to have its own server, still can be virtual hosting. The original website remains intact, just only needs to do CNAME domain name resolution twice, and it can eliminate the "Not secure" warning displayed on all browsers within 10 minutes with anti-attack protection at the same time, and this security protection is provided by the industry-leading Alibaba Cloud WAF. Of course, it doesn't matter whether the website is on Alibaba Cloud or not, just requires it is an Internet accessible website. Our innovative solution is a cloud service to ensure website security. This is definitely the best and perfect website security solution in the world.

When planning this new solution, we tested Alibaba Cloud WAF, Huawei Cloud WAF, Tencent Cloud WAF and JD Cloud WAF at the same time, but finally chose to develop an automated deployment solution for SSL certificate based on Alibaba Cloud WAF, because we believe that Alibaba Cloud WAF has better performance, functions and interfaces that easily integrate with our cloud SSL service. We also plan to test Microsoft Azure WAF and Amazon Cloud WAF, but the settings of these two cloud WAFs are too complicated for ordinary people to handle, so we gave up the test. On this point, the author must praise the 3 China cloud WAF services, all of which are one-click, very suitable for our "one-click SSL" solution. Therefore, I have planned to connect with more cloud WAF service providers in the future, so that our customers have more choices, meet their application needs and adapt to more cloud environments.

ACME vs CWAF, you got it? This is "HTTPS" vs " HTTPS +WAF"! "Web Security 1.0" vs "Web Security 2.0"!

Richard Wang

June 1, 2022
In Shenzhen, China