Magical CNAME

CNAME is the abbreviation of Canonical Name. It is a resource record in the domain name resolution system. It is used to map one domain name to another domain name. ZoTrus Website Security Cloud Service only requires performing two CNAME resolutions to achieve https encryption and cloud WAF protection in 10 minutes automatically. Customers do not need to apply for an SSL certificate from a CA, nor do they need to install an SSL certificate or install ACME client software. This article will tell you how to do it.

Everyone knows that to achieve https encryption, you must have an SSL certificate. This is something that no one can run away. However, customers that have purchased ZoTrus Website Security Cloud Service do not need to apply for an SSL certificate from the CA. The ZoTrus cloud SSL system automatically applies SSL certificate to the CA. To apply for a SSL certificate, you must complete the domain name control validation, which is required by international standards, and no one can bypass it. And how to validate domain name control? The international standard supports three methods. One is to send a verification code to the webmaster@domainname, customer need to paste the verification code on the certificate application system to finish the validation. Of course, 4 other email addresses are also supported: postmaster@, hostmaster@, admin@, administrator@. The inconvenience of this method is that the customer may not have these email addresses, or even if they have these email addresses, but they cannot receive the verification code sent by the domain name validation system. So, we don't use this method to validate the domain control. Another validation method is to require placing a verification file with a specific content in a specific directory on the web server. This method cannot be completed in real time because the customer may not be able to place the file to the server. Therefore, we have not adopted this method to validate the domain name control.

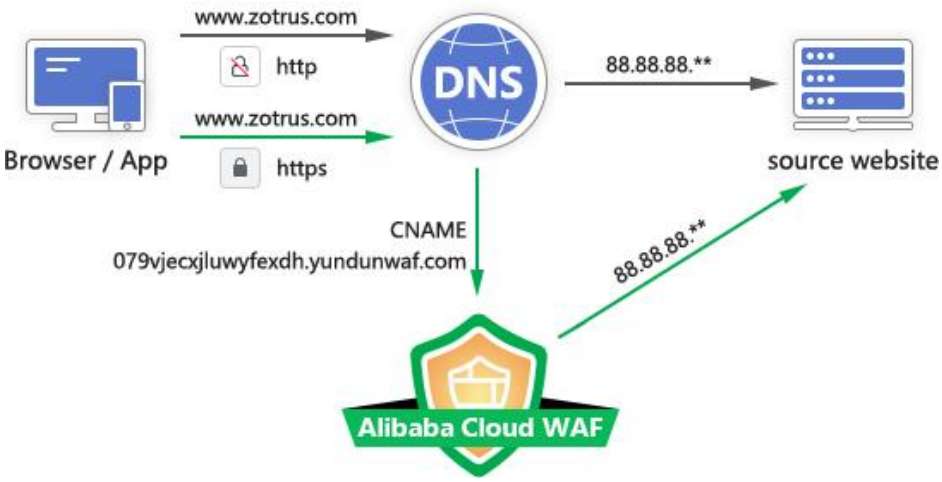
We use the third method - CNAME validation. The CA system automatically generates a short verification code for CNAME resolution, and another long verification code for the value of CNAME resolution. After the setting is completed, submit the verification, the domain name verification system will get the two verification codes through the domain name resolution system to complete the domain

name validation. The basis of this validation mechanism is that the customer can perform domain name resolution as required, and of course it can prove that the customer can control the domain name. After completing the CNAME domain name validation, the SSL certificate can be issued automatically.

This is the first CNAME resolution that must be done to use ZoTrus Website Security Cloud Service, which proves that the customer has the right to use this domain name, and after completing this validation, an SSL certificate bound to this domain name can be issued for this domain name. However, we do not give the SSL certificate to the customer, and the user does not need this SSL certificate. What the customer needs is https encryption service.

After the customer completes the domain name control validation, the system will set up the cloud WAF service and deploy the SSL certificate to the cloud WAF. After completing the setting, the customer will be given a CNAME WAF URL for using cloud WAF service. Customers need to resolve the www domain name CNAME to the WAF URL to instantly enable cloud WAF protection and https encryption services.

As shown in the direction of the black line arrow in the figure below, the website visitor accesses the website in an unsecure way of http cleartext before using ZoTrus Website Security Cloud Service. As shown in the direction of the green line arrow in the figure below, after the second CNAME resolution is done, the website visitor accesses the website in a secure way of https encrypted access. First, the cloud WAF service is accessed, and the cloud WAF checks whether it is a legitimate connection and then goes to the source website to retrieve the resource and return it to the website visitor. The CNAME resolution redirects the access route, instead of directly accessing the website, it first visits the cloud WAF, the cloud WAF is responsible for the security function to block malicious attacks and release normal access, thus protecting the website security.



Readers should see from the above figure that it is CNAME resolution that changes the route for website visitors to access the website and achieves the purpose of automatically providing security protection for the website. To use a metaphor, originally website visitors entered the website through an unsecured gate (port 80) without security guard. Now with Website Security Cloud Service, the unsecure gate is closed, website visitors are directed to another gate with security guard (port 443), which not only checks whether the visitor is a malicious attacker and blocks the attackers, but also provides normal visitors with an encrypted channel (https) to access website resources.

This dual-protection function can be done with only two CNAME domain name resolutions. CNAME resolution plays a key role, making the https encryption and WAF protection to be done automatically, no need to apply SSL certificate from the CA, no need to install SSL certificate or ACME client software. Therefore, the author praised CNAME as "Magical CNAME".

Richard Wang

June 6, 2022
In Shenzhen, China