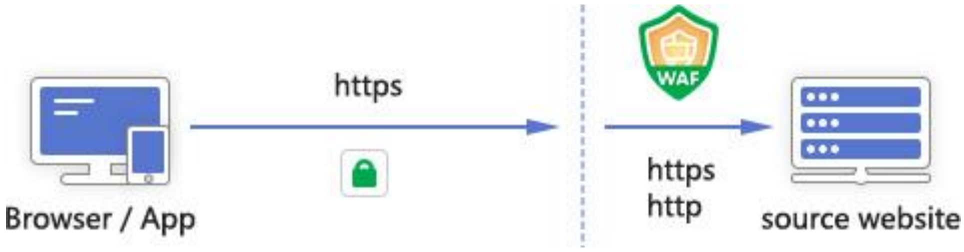
The second of three steps of zero trust security for websites is cloud WAF protection

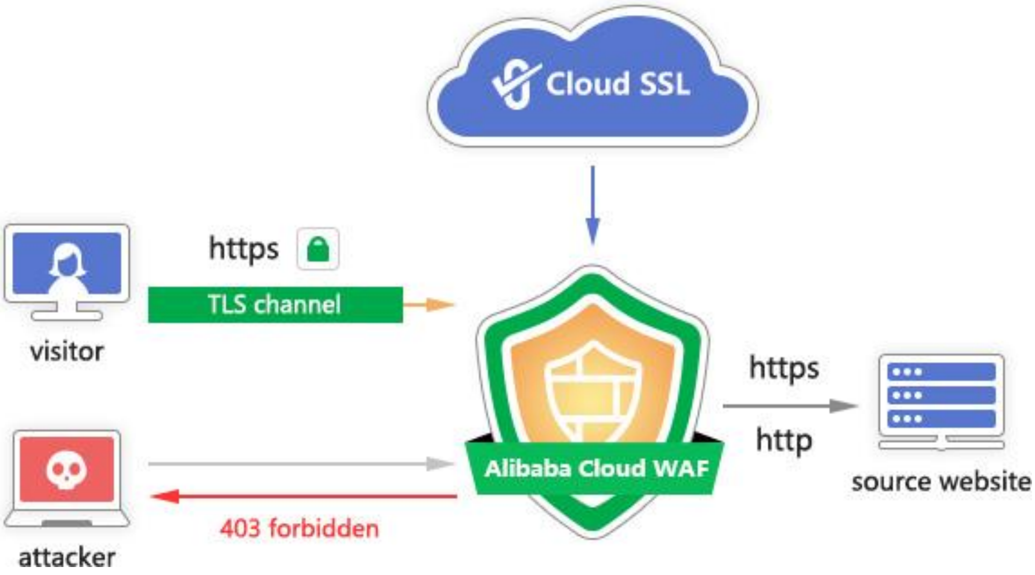
Zero trust is a security principle, it is also very suitable for website security. One of the cores of website zero trust security is never trust every web connection, always verify, allow normal connections, and block malicious connections. Readers familiar with WAF will know that this is the work of the Web Application Firewall (WAF), which is zero trust to network traffic. This article will explain the cloud WAF protection in detail.

The author explained in detail in another blog post "The first of three steps of zero trust security for websites: HTTPS encryption", which is the basis of website security. However, HTTPS encryption alone is not enough for a website. According to the data in "China Internet Network Security Report (2020)" released by CNCERT/CC, in 2020, CNCERT has monitored a total of 53,171 websites in China that have been implanted with backdoors, of which 256 are government websites. For web page tampering in 2020, the number of tampered websites in China is 100,484, of which 494 are government websites. For website trojan data in 2020, in the incidents of using trojans or bots to control servers to control hosts, the total number of IP addresses of the controlled servers was 65,865. Not only server data was stolen, but also these servers can be exploited to launch various attacks. Why so many websites are attacked is, of course, because the website is not any security protection.

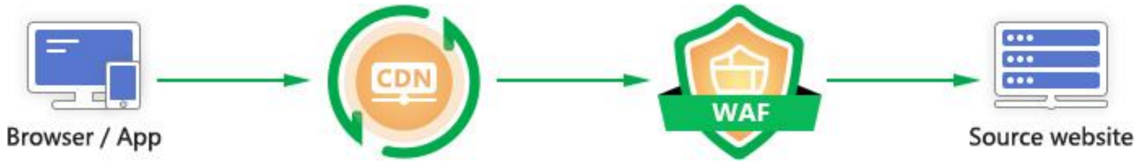
Therefore, website security requires not only HTTPS encryption, but also cloud WAF protection, both of which are indispensable. WAF can effectively prevent various attacks and prevent illegal stealing and illegal tampering after the information reaches the server from browser. HTTPS encryption guarantees 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. Without WAF protection, HTTPS encryption is also meaningful, this point is very important. HTTPS encryption and WAF protection are all duty and one section of each.



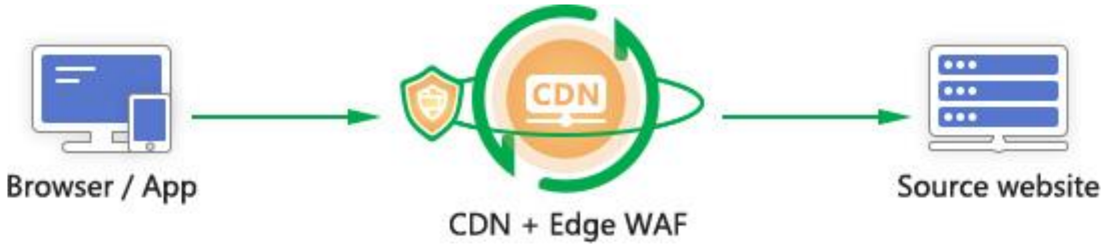
Since website security requires cloud WAF protection and HTTPS encryption, wouldn't it be very perfect if there was a technology that could achieve both HTTPS encryption and cloud WAF protection with one click? ZoTrus Website Security Cloud Service is such a perfect solution, a zero trust security solution for web traffic. Cloud WAF checks every web connection, allows normal connections and blocks malicious connections. Users only need to set CNAME domain resolution once as required to automatically complete domain name control validation. ZoTrus Cloud SSL service automatically issues the required SSL certificates for website and automatically configures it for use on cloud WAF. And needs to set another CNAME domain name resolution to enable Cloud WAF plus HTTPS encryption service. This is based on Alibaba Cloud WAF service and self-developed cloud SSL service, perfect, fast, and fully automatic realization of HTTPS encryption and cloud WAF protection, it can meet the five requirements of cybersecurity protection compliant such as "invasion prevention", "malicious code prevention", "data integrity (anti-tampering)", "communication transmission", and "data confidentiality".



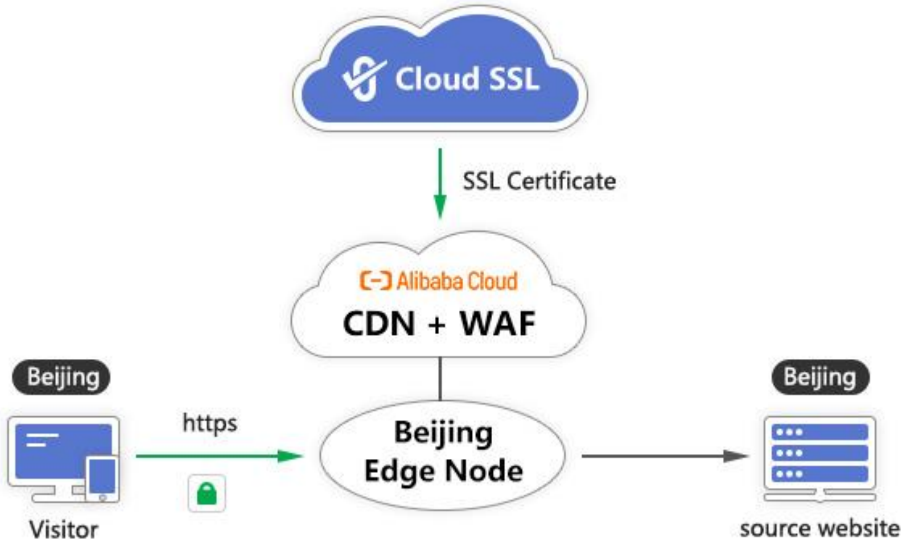
In order to improve website response speed and user experience, it is recommended that users adopt the CDN + WAF architecture. There are two implementation methods. The first method is shown in the figure below, browser or App traffic first goes to CDN, which is forwarded to WAF, and WAF cleans traffic and then arrives source Web server, to achieve website acceleration, traffic detection and attack interception.



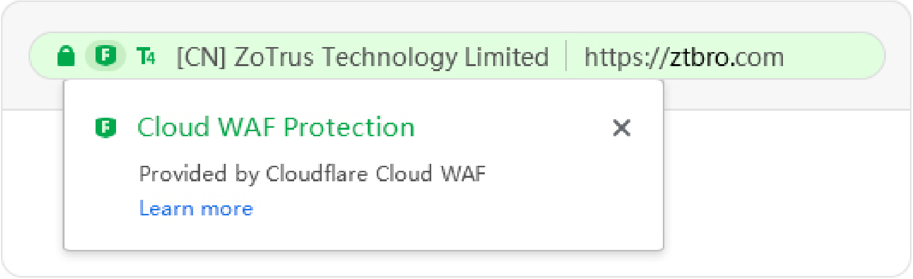
The advantage of this method is that the CDN service provider and the WAF service provider may not be the same service provider, and both access through CNAME. However, this method needs to concentrate all kinds of traffic, including malicious traffic, into the central WAF, which not only wastes traffic, but also fails to respond quickly to end user in the nearest node. The author recommends using the CDN + edge WAF method. As shown in the figure below, malicious traffic is intercepted at the edge of the traffic, and only normal traffic is forwarded through the CDN network, which not only saves traffic bandwidth, but also improves the forwarding speed of normal traffic, no need to forward all traffic to the central WAF for processing.



ZoTrus Website Security Cloud Service adopts the second method, which realizes rapid cleaning of local traffic and fast forwarding the source site data to local visitors and solves security protection problems directly in the "last mile" instead of having to go to the central cloud WAF to achieve security protection, this will greatly improve the response speed of the website and enhance the user experience.



The website implements cloud WAF protection, but website visitors don’t know it. Therefore, ZT Browser innovatively displays the cloud WAF protection icon directly in the address bar, allowing website visitors to check the website’s security protection status and whether it is protected by a ZT Browser certified WAF immediately, it can effectively enhance the online trust of website visitors. Whether a website has cloud WAF protection accounts for 20% of the website security test rating service integrated by ZT Browser. With cloud WAF protection, the website security test rating level can be effectively improved.



Cloud WAF Protection

Provided by Cloudflare Cloud WAF

In summary, for website security, it is necessary to have zero trust to each web connection and must detect whether each connection is a malicious attack, block the attack connection in real time, and allow normal connections, which requires that the website must be protected by cloud WAF. ZoTrus Website Security Cloud Service not only allows customers to fully automatically realize cloud WAF protection, and realizes the second of the three steps zero trust security for websites, but also let customers use ZT Browser to understand the actual situation of this step in real time, compare and understand the improvement of website security status before and after using ZoTrus Website Security

Cloud Service in a simple and clear way, so that customers can be assured of their website security status, and they can focus on doing their own business well.

Richard Wang

June 22, 2022
In Shenzhen, China