The first of three steps of zero trust security for websites: HTTPS encryption

Zero trust is a security principle that applies well to website security. One of the cores of website zero trust security is that never trust http website with cleartext transmission. All browsers display "Not secure" for HTTP websites, which is zero trust to HTTP cleartext transmission. The basic security of website security is HTTPS encryption, which realizes the encryption of information transmission from the browser (mobile app) to the web server, and effectively protects the transmission security of confidential information exchanged between the browser or mobile app and the cloud server.

The author found that many friends completely misunderstood zero trust and believed that zero trust is an identity authentication solution, which may be the reason that many traditional security vendors only focused on zero trust of identity. Look at one of the actions in the U.S. Federal Zero Trust Strategy is zero trust to cleartext network traffic, requiring federal agencies to encrypt all DNS requests, HTTP traffic, and email traffic, requiring federal agencies to encrypt all Internet-accessible web service and API.

To achieve HTTPS encryption is of course inseparable from the SSL certificate, or TLS/SSL certificate, TLS certificate. However, how to apply an SSL certificate, what cipher algorithm is used in the SSL certificate, and how to deploy an SSL certificate to implement HTTPS encryption, there are many things to learn here, which will be explained in detail in this article.

Since Netscape invented the SSL protocol in 1994, the Internet cleartext transmission protocol HTTP has become an encrypted transmission protocol - HTTPS. Users must apply for an SSL certificate from a CA, after getting the SSL certificate, they must install and use it on the Web server. Of course, the Web server must support the cipher algorithm of this SSL certificate, the browser must also trust this SSL certificate issued by this CA, thus forming an HTTPS encrypted application ecosystem. At present, the mature ecosystem only supports SSL certificates with RSA algorithm and ECC algorithm, China commercial cryptographic algorithm SM2 algorithm SSL certificate application ecosystem has not yet formed.

Since 1994, when an SSL certificate was used to implement HTTPS encryption, until October 2015, the ACME automatic deployment certificate protocol launched by Let's Encrypt. In the past 21 years, people have been manually applying for SSL certificates and manually deploying SSL certificates, which is time-consuming, labor-intensive, and expensive, Let's Encrypt has changed all this, mainly in three aspects: First, the automatic deployment of SSL certificates has been realized. Users only need to install an ACME client software on the Web server, and even some Web servers have directly integrated the ACME client, users only need to configure the ACME server URL. Second, it is completely free (three months period SSL certificate). This lays the foundation for the popularization of HTTPS encryption on a large scale, but for free, the certificate must be automatically issued by the machine, so it can only validate the domain name control, so it can only be a low-end DV SSL certificate. This brings about the third change: the SSL certificate has been downgraded from the dual function of proving website identity and transmission encryption to the single function of transmission encryption, making website identity proving a new problem. This problem will be discussed in detail on the third of three steps of zero trust security for websites.

Whether the user installs the SSL certificate manually or uses the ACME method to automatically deploy the SSL certificate, the user is required to have a physical server, at least a cloud server. For many virtual hosting website users, installing an SSL certificate is still a relatively difficult task. The good news is that some virtual hosting service providers have begun to provide SSL certificate deployment support, which is due to the extensive support of SNI technology, and of course, there is also pressure from the browser prompting "Not secure".

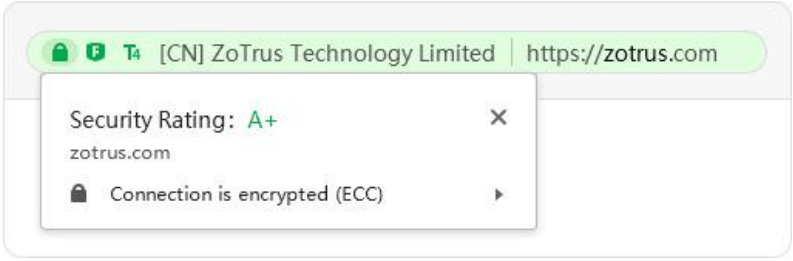
In addition to the traditional installation of the SSL certificate on the server for HTTPS encryption, users can also manually configure the SSL certificate applied for from the CA to the CDN and cloud WAF for HTTPS encryption. Some CDN and WAF service providers do well, such as Cloudflare, directly and automatically configures the SSL certificate for websites. This is the second solution for automatically deploying SSL certificates to implement HTTPS encryption. This solution will also be discussed in detail on the second of three steps of zero trust security for websites.

The above is about how to apply for and how to deploy an SSL certificate. Let’s talk about the algorithm for issuing an SSL certificate. The current international standard only allows the use of RSA

and ECC algorithms, and operating systems, browsers, and web servers only support these two algorithms. This is the reality that China hopes to promote the SSL certificate using SM2 algorithm. China must establish an ecosystem from operating system, at least from the browser (including mobile App) and web server to support the SM2 algorithm including SM3 and SM4. Of course, it must also include the support of the SM2 algorithm and the SM2 SSL certificate of the CDN and WAF service. Only in this way can the SM2 HTTPS encryption be seamlessly realized. Presumably, it is not difficult for readers to understand why the first product of ZoTrus Technology is a browser that supports the SM2 algorithm and the SM2 SSL certificate, because the browser is the entrance to the Internet, it is the key core component of the SM2 SSL certificate application ecosystem.

For HTTPS encryption, which is the first of three steps of zero trust security for websites, the slogan of ZoTrus Technology is not to provide SSL certificate for customers, because this is not what customers need, but need HTTPS encryption, so we directly provide HTTPS encryption services. Customers only need to set the CNAME domain name resolution for finishing the domain control validation, ZoTrus Cloud SSL service automatically issues the required SSL certificate for website and automatically configures it for use on the cloud WAF. And it only needs to set another CNAME domain name resolution to enable the cloud WAF plus HTTPS encrypted service. This is by far the most worry-free HTTPS encryption solution. Customers do not need to apply for a SSL certificate from the CA, nor do they need to install ACME client software on the web server. They only need to set two CNAME domain resolutions to automatically implement HTTPS encryption. Whether it is a virtual hosting or physical server, it is only required the website is Internet accessible. This is the ZoTrus Website Security Cloud Service, based on Alibaba Cloud WAF service and self-developed Cloud SSL service, perfect, fast, and fully automatic realization of HTTPS encryption. By default, the faster ECC algorithm is used. Customers can choose to enable the SM2 algorithm to achieve SM2 HTTPS encryption, and ZT Browser will preferentially use the SM2 algorithm to achieve HTTPS encryption.

If the website implements HTTPS encryption, all browsers no longer display "Not secure" but display the padlock icon. ZT Browser innovatively integrates the website security test and rating service. The scoring standard of this service uses HTTPS encryption to account for 60%, because HTTPS encryption is the basic security protection for website security and the first of three steps of website security. The SSL security rating will test and score from four dimensions: SSL certificate, protocol support, key exchange and cipher strength, accounting for 60%, 12%, 12% and 16% respectively. Through the testing of these four dimensions, users can fully understand the security status of HTTPS encryption, ensure the correct deployment and use of SSL certificate, and reliably implement the HTTPS encryption.



In order to create a SM2 certificate application ecosystem, ZT Browser not only supports the SM2 algorithm and the SM2 SSL certificate, but also preferentially adopts the SM2 algorithm to realize HTTPS encryption. And in order to let website visitors perceive the website has deployed SM2 SSL certificate to achieve HTTPS encryption, a SM2 encryption icon "m" is innovatively added to the address bar, so that visitors can see at a glance whether the website is protected by commercial cryptography, and clearly displays this website is Cryptography Protection Compliant. ZT Browser that preferentially adopts the SM2 algorithm provides a solid foundation for the application of website security cryptography protection for the popularization of SM2 HTTPS encryption, which is an important part of the application ecosystem of the SM2 SSL certificate.

In short, for website security, there must be zero trust to cleartext network traffic, especially government websites must enforce HTTPS encryption, and the SM2 algorithm must be preferentially

used to achieve HTTPS encryption. The website security solution of ZoTrus Technology not only enables customers to automatically realize HTTPS encryption, realizes the first of three steps of 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 20, 2022
In Shenzhen, China