SM2 HTTPS encryption, just the SM2 HTTPS Auto Gateway

The author has communicated with the directors of several provincial and municipal e-government cloud platforms. Everyone is very aware of the importance and urgency of cryptography compliance. But when it comes to the cryptography reconstruction, everyone says that there is a lot of pressure, and it is not easy to do. The most important point is not to affect the normal and reliable operation of the existing system, all e-government websites are managed in a unified manner on the e-government cloud platform, there are thousands or ten thousand of e-government websites running normally. If the reconstruction of one server affects one key system’s normal operation, it will be a big accident! Absolutely no accidents, this is the most important thing. Upgrading the current http website to https encryption and SM2 https encryption has become a secondary matter. However, it must be done, which is very tangled and contradictory.

The author now really understands why many e-government websites have not yet deployed SSL certificate that still in "Not secure" status. It's not that they don't know that it is not secure, and all browsers will display “Not secure". And It's not a matter of money either, there are free SSL certificates everywhere. The core problem is that it is too difficult to deploy SSL certificates to implement https encryption, let alone implement SM2 https encryption! The premise of implementing https reconstruction is that it cannot affect the normal operation of existing business systems! The author tried to recommend that they can use the Website Security Cloud Service that does not need to change the current web system, but some executives do not accept this solution. They do not want the security and reliability of the e-government system to depend on external cloud services, no matter how good the cloud service provider is!

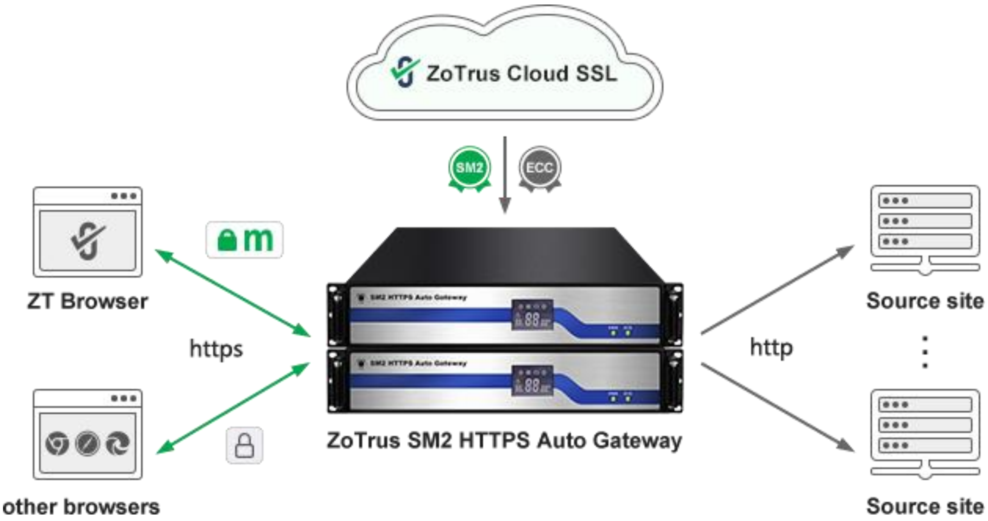
These executives put forward a common wish: if the existing system does not need to be changed, and there is no need to apply for and deploy SSL certificates, they can seamlessly switch from http to https or SM2 https encryption without business interruption, and it is not an external cloud service, such a solution can still be considered for implementation.

After getting this real demand from users, the author began to think of a solution. Isn't that the need to deploy the ZoTrus Website Security Cloud Service locally? This is a bit difficult, because it involves too many systems, and the investment is a bit large. Is there an easier solution? The author thinks of SSL Offloading card and SSL Accelerator card. I have come into connect with these products more than ten years ago. At that time, only foreign manufacturers made these products, now there are domestic manufacturers who have already supported SM2 algorithm and SM2 SSL certificate. However, the author has not been optimistic about such products before, thinking that to implement https encryption, it is only necessary to configure an SSL certificate on the web server, and such products are not required. Although the manufacturers advertise that such products can greatly reduce the crypto calculation burden of the Web server, the author has also seen some research results that the current server hardware only increases the server overhead by 3% when upgrading the website from http to https, which is less than the overhead of loading video streaming media.

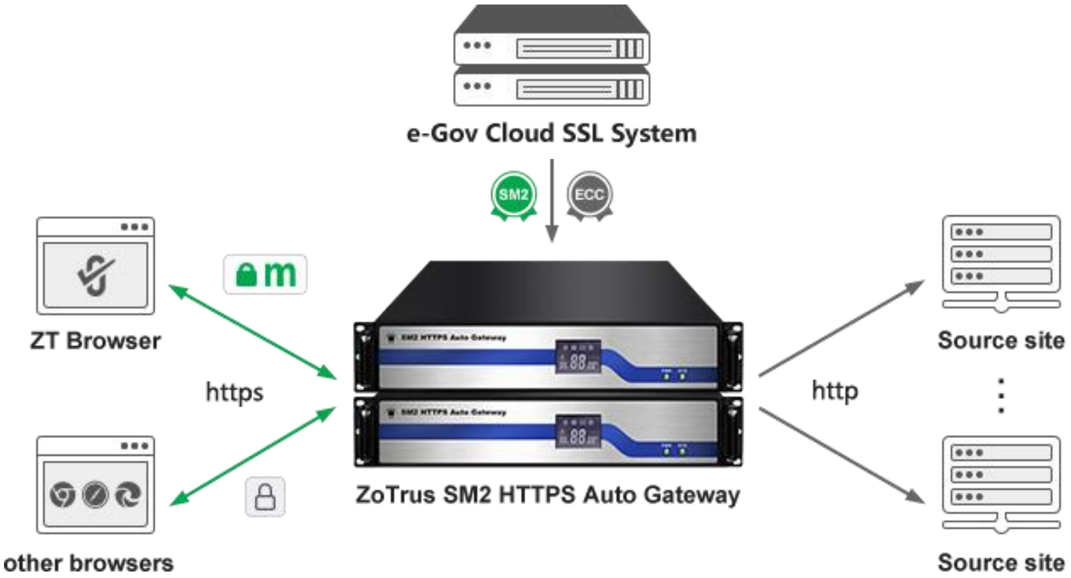
Now, the actual application requirements proposed by the executives of the e-government cloud platform have changed my view on the role of products such as SSL offloading cards and security gateways. The advantage of these products is that there is no need to modify the existing server, it can realize https encryption with zero modification, instead of other functions. The key point is that it can realize SM2 https encryption with zero modification! Of course, the prerequisite is to support SM2 ACME, which can automatically configure dual SSL certificates for SSL offloading card or security gateway, so that users don’t have to worry about applying for SSL certificates. Of course, it must also support SM2 algorithm and SM2 SSL certificate. With this idea, the author easily found a cooperative manufacturer, helping the manufacturer to integrate the SM2 ACME client into the gateway that can connect to the ZoTrus SM2 ACME Service System, to automatically apply for the dual-algorithm dual-SSL certificates, and automatically deploy dual-SSL certificates to support adaptive algorithms to realize https encryption, https offloading and forwarding, this is the hardware product launched today – ZoTrus SM2 HTTPS Auto Gateway .

ZoTrus SM2 HTTPS Auto Gateway is a high-performance website security hardware gateway device that integrates multiple functions such as https accelerator, https offloading and forwarding, SM2 algorithm module, SSL certificate automation, and load balancing. This is a hardware device based on products such as security gateway, SSL accelerator card, and SSL offloading card that integrated the

SM2 ACME client, which can automatically configure the SM2 SSL certificate and ECC SSL certificate to realize the SM2 https encryption and offload forwarding. It completely solves the problem that the e-government web system and large enterprise management system cannot deploy SSL certificate on the running web server. It can realize the SM2 https encryption without modifying the original web server, which meets the needs of users who want to deploy the system locally without relying on cloud services for self-controllable management application.



Some e-government cloud platforms with higher security requirements hope to independently issue e-government-specific SSL certificates instead of connecting to the ZoTrus Cloud SSL System, so they need to deploy the ZoTrus Cloud SSL System locally that it is the e-Government Cloud SSL System (including SM2 ACME Service System), and customize branding the dual-algorithm dual-SSL intermediate root certificate dedicated to e-government cloud platform, which is used to independently issue e-government-specific dual-algorithm dual-SSL certificates (SM2 SSL certificate and ECC SSL certificates) for e-government web systems. All e-government web systems only trust the SSL certificates that issued by the customized SSL intermediate root certificate, this can effectively protect e-government websites security from SSL man-in-the-middle attacks and counterfeit SSL certificate fraud. The SM2 HTTPS Auto Gateway only needs to be modified to connect to the e-Government Cloud SSL System and automatically apply for and deploy the dual algorithm SSL certificates dedicated to the e-government cloud platform to achieve more secure and controllable SM2 HTTPS encryption.



Finally, to sum up, there are two core points for the SM2 HTTPS Auto Gateway. First, it must realize the SM2 automatic certificate management, the existing gateway products must be upgraded, with a built-in SM2 ACME client, which can be connected to the ZoTrus SM2 ACME Service System and can automatically apply for SM2 SSL certificate and ECC SSL certificate, automatic deployment of dual SSL certificates to achieve https encryption. Second, it must support SM2 algorithm and SM2 SSL certificate. More related product manufacturers are welcome to provide similar products, and jointly provide zero-reconstruction SM2 https encryption solutions for e-government cloud platform and large enterprise private cloud platform, and work together with these cloud platforms to jointly improve the security of critical information infrastructure, jointly accelerate the popularization and application of SM2 https encryption for all web system in the critical information infrastructure.

Richard Wang

Jan 6, 2023
In Shenzhen, China