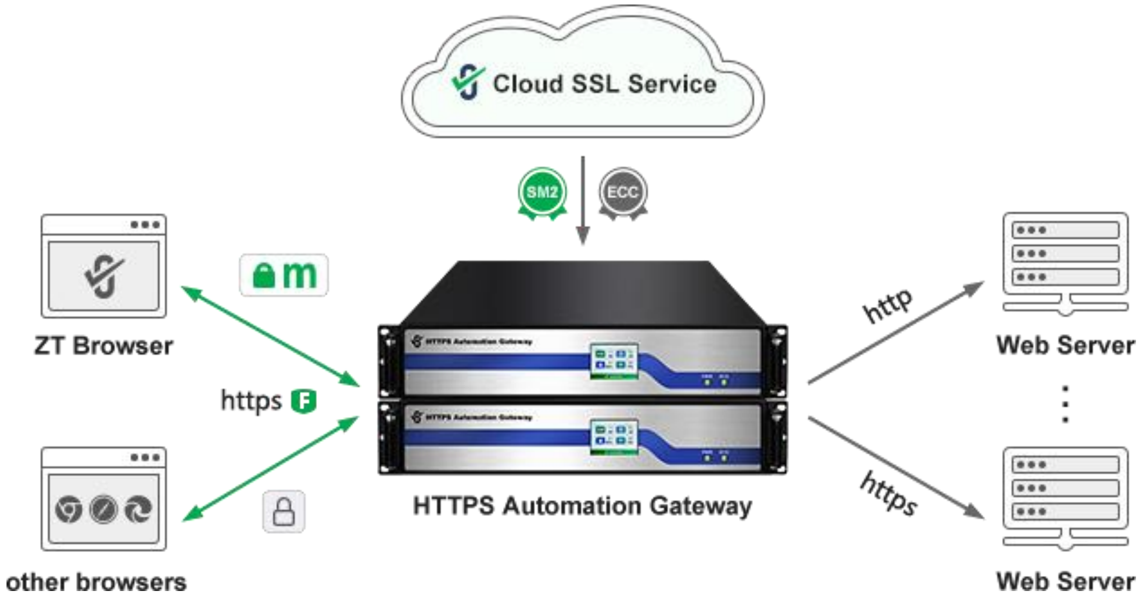
Get done the Two protection compliance with One click

"Cybersecurity Protection" is the abbreviation of the Graded Protection of Cybersecurity. It is based on article 21 of "Cyber Security Law" – "The state shall implement the rules for graded protection of cybersecurity. Network operators shall, according to the requirements of the rules for graded protection of cybersecurity, fulfill the following security protection obligations, so as to ensure that the network is free from interference, damage or unauthorized access, and prevent online data from being leaked, stolen or tampered." and article 31 – "The State implements focus protection for critical information infrastructure on the basis of the graded cybersecurity protection structure in important sectors and areas such as public telecommunications and information services, energy, transportation, irrigation works, finance, public services, e-government, etc., as well as other critical information infrastructure that, whenever it is destroyed, loses its ability to function or encounters data leaks, may gravely harm national security, the national economy, the people's livelihood and the public interest." All websites must "adopt technical measures such as preventing computer viruses and cyber-attacks, network invasion and other hazardous cyber security behaviors" and "adopt technical measures such as data classification, important data backup and encryption" to ensure the website system security and meet the requirements of cybersecurity protection compliance.

"Cryptography Protection" is the abbreviation of encryption protection and security authentication. It is based on article 2 of "Cryptography Law" – ""cryptography" refers to technologies, products, and services utilized for encryption protection and security authentication on information and the like by using specific transformation methods." and article 27 – "Operators of critical information infrastructure shall adopt commercial cryptography to protect such infrastructure." All websites and information system, especially the CII systems must use cryptographic technologies, products, and service to protect its security.

In summary, the critical information infrastructure must meet the compliance requirements of both "Cyber Security Law" and "Cryptography Law". Government official websites and e-government service systems are critical information infrastructure. However, according to the 9th issue of "Cybersecurity Information and Dynamic Weekly" released by CNCERT/CC on April 26, 738 websites have been implanted in the back door within a week, of which 12 government websites. And within a week, 3611 websites were tampered with, of which 17 government websites. In 2020, 53,171 websites in China were implanted in the back door, of which 256 were government websites. It can be seen from these data that many websites are still in a state of no protection, especially government websites, which are seriously illegal! What to do?

It is recommended to deploy the ZoTrus HTTPS Automation Gateway to achieve cybersecurity protection compliance requirements with one click, and cryptography compliance requirements with one click. Users do not need to apply for an SSL certificate from the CA, the web server does not need to be reconstructed to support the SM2 algorithm, and there is no need to install an SSL certificate, but only need to deploy the HTTPS Automation Gateway in front of the web server, and the gateway will automatically connect to the ZoTrus Cloud SSL Service system to apply for and deploy a dual-algorithm (ECC/SM2) SSL certificate for the website, automatically enable the HTTPS encryption, and meet the cryptography compliance requirements with one click. Users do not need to purchase cloud WAF services or WAF devices separately, ZoTrus Gateway has built-in WAF system to provide high-performance WAF protection services with HTTPS encryption for websites, to realize https encryption and WAF protection for websites at the same time. With only one deployment, it perfectly realizes the compliance requirements of key parts of "cybersecurity protection " and "cryptography protection" at the same time, and to support up to 255 websites for 5 years of compliance operation.



The WAF protection function of ZoTrus Gateway can meet the user's cybersecurity protection compliance requirements in three aspects, such as "intrusion prevention", "malicious code prevention" and "data integrity (tamper-proof)", and the HTTPS encryption function of ZoTrus Gateway can not only meet the user's cybersecurity protection compliance requirements in the three aspects of "communication transmission", "data integrity" and "data confidentiality", but also meet the user's "network and communication security" - using cryptography technology to ensure the integrity of data in the communication process. Confidentiality and authenticity of entity identity, "application and data security" - the use of cryptography technology to ensure the confidentiality and integrity of important data in the transmission and storage process of information system applications.

ZoTrus HTTPS Automation solution is an innovative solution integrating the client and cloud to realize HTTPS encryption and WAF protection automatically that the original web server with zero transformation to meet the requirements of cybersecurity protection compliance and cryptography compliance. The core product is the ZoTrus HTTPS Automation Gateway, which can automatically complete the SM2 transformation and WAF protection in one deployment, which not only greatly reduces the website security compliance cost, but also, most importantly, protects the important data security of the website and ensures the smooth operation of the business of the website owner.

Richard Wang

June 1, 2022
In Shenzhen, China