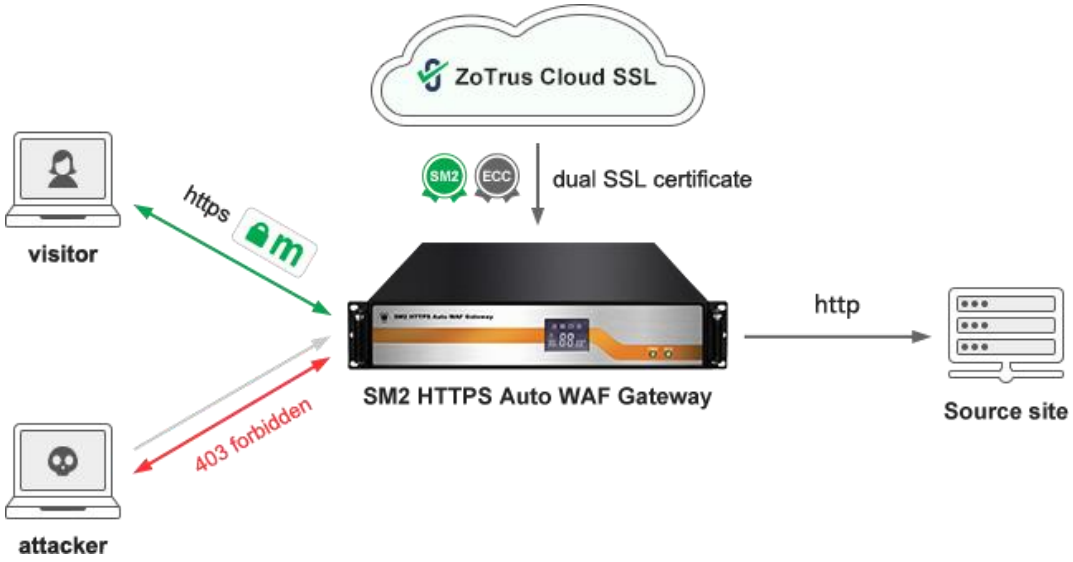
ZoTrus SM2 HTTPS Auto WAF Gateway

1. Product Introduction

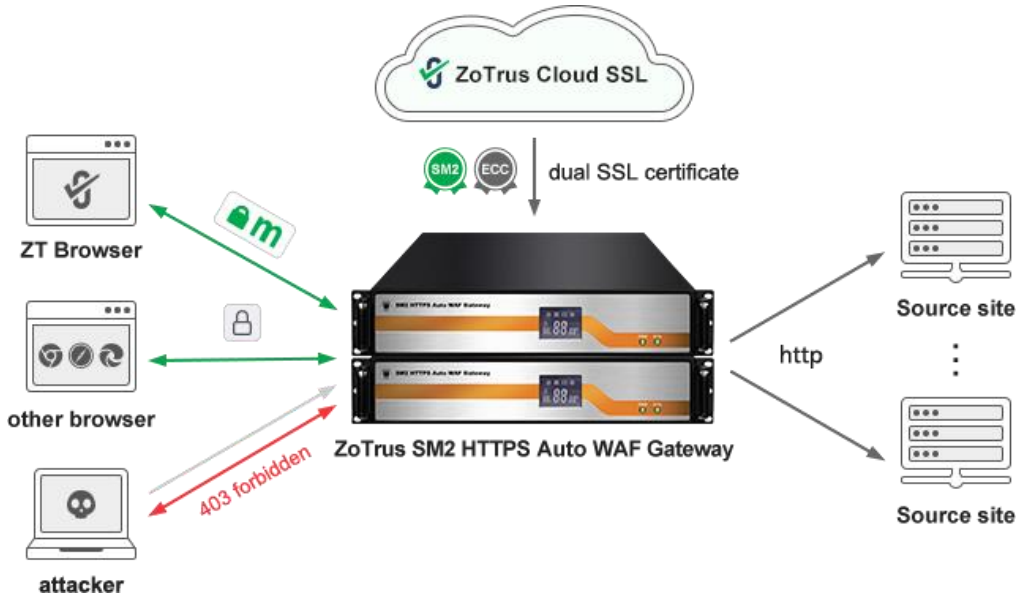
ZoTrus SM2 HTTPS Auto WAF Gateway is based on the ZoTrus SM2 HTTPS Gateway, which adds the Web Application Firewall (WAF) module, it is a high-end high-performance website security hardware gateway device built by ZoTrus Technology using high-performance cipher cards. It is a hardware gateway including https encryption acceleration, https offloading and forwarding, WAF protection, SM2 algorithm module, SSL certificate automatic management, and load balancing, it is dedicated to https acceleration and offloading, WAF protection with multiple functions in one, built-in professional-grade high-performance hardware cipher card to achieve high-speed encryption operations and network packet forwarding, and optimized the built-in operating system, network protocol, SSL/TLS protocol, ECC algorithm and the SM2 algorithm professionally to achieve industry leading extreme performance, such as: HTTPS new connections can reach 60,000 times per second, HTTPS throughput can reach 17Gbps, and HTTPS concurrent connections can reach 3 million connections.

The biggest features and characteristics of the ZoTrus SM2 HTTPS Auto WAF Gateway are zero application for SSL certificates, zero installation of SSL certificates, automatic implementation of HTTPS encryption, WAF protection, adaptive encryption algorithms. The browsers that support SM2 algorithm and SM2 Certificate Transparency use the SM2 algorithm to implement https encryption, browsers that do not support SM2 algorithm use ECC algorithm to implement https encryption. This is an innovative solution with client-cloud integration, the SM2 HTTPS Auto WAF Gateway has a built-in SM2 ACME Client, which automatically connects with the ZoTrus Cloud SSL System to complete the automatic application, deployment, and renewal of dual SSL certificates, ensuring zero change of the business system to achieve https encryption and WAF protection automatically, to provide https encryption and WAF protection service uninterrupted for business systems with up to 255 different domain names.



2. Main Functions

The core function of the ZoTrus SM2 HTTPS Auto WAF Gateway is zero reconstruction of the original server, no need to install an SSL certificate on the server, no need to install ACME Client software on the server, and no need to upgrade the server software to support the SM2 algorithm, just deploy HTTPS Auto WAF Gateway before the original server, then it can automatically implement https encryption and WAF protection, and provide https encryption services and WAF protection 24 x 365 days. It is recommended that the default dual-machine deployment be used as hot standby for each other. When it is available, the two-gateway work at load balance mode, and when it is not available, one gateway can take over all work. It intercepts attack traffic in real time and only allow legal traffic to pass normally, the free SM2 browser that supports the SM2 algorithm and SM2 Certificate Transparency – ZT Browser uses the SM2 algorithm to realize the SM2 https encryption preferentially, and other browsers that do not support the SM2 algorithm and SM2 Certificate Transparency use ECC algorithm to implement https encryption.



The dual-algorithm dual-SSL certificate required for HTTPS encryption is automatically completed by the HTTPS Auto WAF Gateway connected to the ZoTrus Cloud SSL System to apply for the dual-SSL certificate, validate the domain name, retrieve the issued SSL certificate, install the SSL certificate, and enable the SSL certificate. The automatically configured ECC SSL certificate is globally trusted and supports the certificate transparency, it is issued by ZoTrus brand intermediate root certificate - ZoTrus ECC DV SSL CA, its root CA certificate is the world oldest ECC algorithm root CA certificate - Sectigo ECC, and the entire chain uses ECC Algorithm, the encryption speed is 18 times faster than the RSA algorithm SSL certificate, to fast access the website by end users. The automatically configured SM2 SSL certificate is compliant with the Cryptography Law and trusted by ZT Browser. It is currently the only SM2 SSL certificate in the world that supports the SM2 Certificate Transparency. It is issued by ZoTrus brand intermediate root certificate - ZoTrus SM2 DV SSL CA, its root CA certificate is ZoTrus SM2 SSL Root, the root CA certificate of ZoTrus brand using SM2 algorithm, which is currently the only SM2 root CA certificate dedicated to issue SM2 SSL certificates, it is trusted by ZT Browser and ZoTrus SM2 Certificate Transparent Log System, the entire chain uses the SM2 algorithm, the encryption speed is 20 times faster than the RSA algorithm, to fast access the website by end users. The certificate chain file of the automatically configured dual SSL certificate is the smallest, saving IDC traffic and user mobile phone traffic, saving IDC power consumption and user mobile phone power consumption, and is more environmentally friendly.

The SM2 HTTPS Auto WAF Gateway is a WAF module added on the basis of the SM2 HTTPS Gateway, and the Web Application Firewall module is developed based on the open source ModSecurity system, which supports commonly used Web Application Firewall functions, such as: preventing SQL injection, preventing cross-site scripting attacks (XSS), preventing attacks using local files containing vulnerabilities, and preventing the use of remote File (including vulnerabilities) attacks, preventing attacks using remote command execution vulnerabilities, preventing PHP code injection, preventing malicious access that violates the HTTP protocol, preventing attacks using remote proxy infection vulnerabilities, preventing attacks using Shellshock vulnerabilities, and preventing the use of Session sessions Vulnerabilities with the same ID can be used to attack, prevent malicious scanning of websites, prevent source code or error information leakage, blacklist honeypot projects, and perform IP blocking based on judging the IP address attribution, etc.

If customer has already purchased a WAF device, it is recommended to purchase the SM2 HTTPS Gateway. It is only necessary to deploy a SM2 HTTPS Gateway before the WAF device. The WAF device only needs to be responsible for parsing the cleartext http content to make corresponding protection, and there is no need to apply for SSL certificate from the CA to be deployed on the WAF device.

The main ten functions of ZoTrus SM2 HTTPS Auto WAF Gateway are:

(1) Zero reconstruction for https encryption

The original server does not need to install an SSL certificate, no need to install SM2 ACME client software, zero reconstruction to realize SM2 https encryption, adaptive encryption algorithm, support RSA/ECC/SM2 algorithm to realize https encryption, and it supports two-way authentication.

(2) Automatically configure SSL certificates

By default, dual SSL certificates (ECC/SM2) are automatically configured for the website domain name set by the user for free. Users do not need to apply for an SSL certificate from a CA, and do not need to install and configure an SSL certificate.

(3) High-performance https offloading

Completely take over and assume the SSL encryption function of the original server, greatly reducing the performance pressure on the original server, allowing the original server to be dedicated to the business system, and greatly improving the response speed of client access.

(4) Web Application Firewall protection

Based on the development of the industry-leading open source ModSecurity system, it supports common Web Application Firewall functions, provides security cleaning protection for https offloading traffic, and only forwards normal and secure traffic to the internal server behind.

(5) Client connection multiplexing

Adopt dynamic connection pool technology and multiplexing technology to bundle a large number of client connection requests, save most server TCP connections and maintain them continuously, significantly reduce the number of client connections that the original server needs to handle (up to 90%), and speed up connection processing speed and improve the business processing capability of the original server.

(6) Web data transmission compression

Use standard GZIP or Deflate compression algorithm to compress HTTP traffic, reduce bandwidth consumption and cost, improve server response and bandwidth efficiency, shorten end user access and download time, improve user experience and increase satisfaction.

(7) Reverse proxy cache

Use the memory cache and package storage structure to cache website content for a short time, reduce the load pressure on the original server from user access, and improve the processing capacity of the original server and the user's access experience.

(8) Session retention mechanism

The session retention mechanism based on Cookie and Source IP can select the specific server that the user has connected to, and it realize seamless processing of user requests. And the number of new connections can be reduced, and the system overhead of related devices and servers can be effectively reduced.

(9) Multi-algorithm load balancing

Support seven-layer and four-layer protocols to allocate different server resources for users, support traffic load based on information such as URI, HOST, COOKIE, USER_AGENT and factors such as IP address, application type and content, and support NAT conversion.

(10) TCP/UDP/DTLS secure delivery

Support TCP/UDP/DTLS + SSL/TLS secure transmission channel delivery service, can meet the TCP/UDP/DTLS network application system based on SSL/TLS protocol, realize the encryption and

acceleration of the transmission channel, the original server system does not need any customization and transformation.

3. Performance Indicators

ZoTrus SM2 HTTPS Auto WAF Gateway provides an efficient, secure, transparent, easy-to-deploy, zero-reconstruction, fully automatic innovative solution to realize https encryption and WAF protection, which can effectively expand the bandwidth of network devices and servers, increase throughput, and strengthen network data processing capabilities, improve the flexibility and usability of the network, and improve the user experience of users visiting the website, improve the security protection capability of the internal Web server.

ZoTrus SM2 HTTPS Auto WAF Gateway provides fully independent and controllable software and hardware integration products, including SSL security gateway software system with completely independent intellectual property rights, cryptographic SM2/ECC/RSA algorithm hardware accelerator card certified by CCPC, self-controllable operating system, support CPU chips such as Haiguang, Loongson and Phytium, adopt supporting independent motherboards, support independent network card, etc. The fully autonomous and controllable software and hardware integrated SM2 HTTPS Auto WAF Gateway can meet the application requirements of the government, military industry and other industries that have extremely high requirements for information security control.

Each ZoTrus SM2 HTTPS Auto WAF Gateway supports automatic configuration of up to 255 ECC SSL certificates (single certificate) and supports up to 255 pairs of SM2 SSL certificates (one signing certificate and one encrypting certificate), dual-algorithm dual-SSL certificates configuration supports up to 255 website domain names to achieve dual-algorithm adaptive https encryption. How many websites can support for https encryption is limited by the number of new connections, throughput and concurrency supported by the Gateway hardware and cipher cards.

Each ZoTrus SM2 HTTPS Auto WAF Gateway has a warranty period of 5 years, and automatically configures a globally trusted ECC DV SSL certificate and cryptography compliance SM2 DV SSL certificate for no more than 255 website domain names within 5 years. Based on the calculation of 888 Yuan per year for each website's dual-algorithm and double-SSL certificate, the value of the SSL certificate that is automatically configured is as high as 1.13 million RMB Yuan (=5*255*888, equal to US$163K), and the world's exclusive super-value https encryption automation solution!

ZoTrus SM2 HTTPS Auto WAF Gateway currently provides 4 products of different specifications, which can be used for cloud high-performance data centers, large and medium-sized enterprise servers, and small organization servers to automatically implement https encryption, especially the application requirements of zero reconstruction to realize SM2 https encryption. The product performance index parameters of various models are shown in the figure below. For users with different index requirements, products can be customized to meet the requirements.

Edition	**Pro 1G**	**Pro Q10G**	**Pro 10G**	**Pro-XC**
Model	**MG-2-6**	**MG-2-7**	**MG-2-8**	**MG-2-9**
Max Supported Sites	100	150	255	100

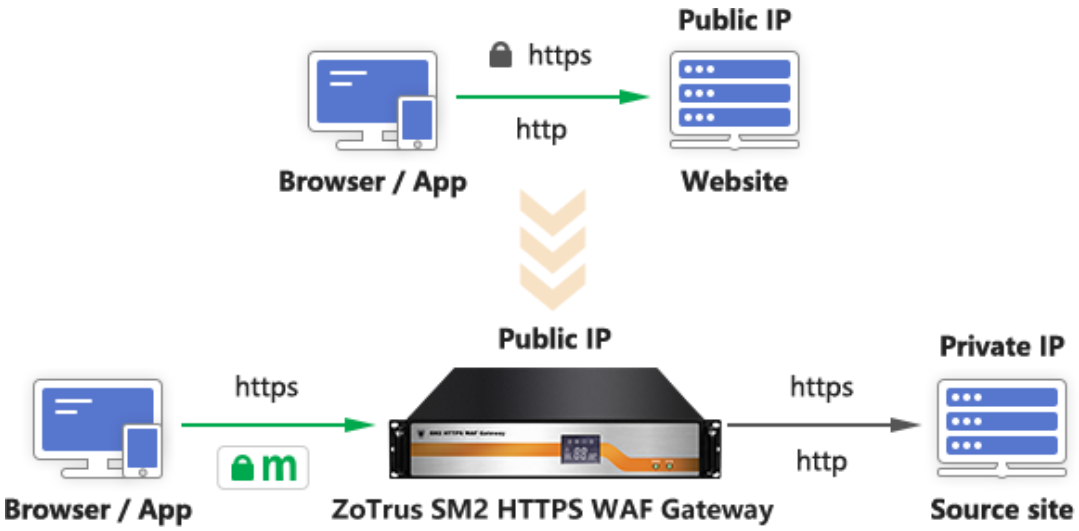
WAF Rules	Default + 10	Default + 20	Default + 30	Default + 10
Incl ECC SSL Qty	100	150	255	100
Incl SM2 SSL Qty	100	150	255	100
Dual SSL supply	5 years	5 years	5 years	5 years
ECC SSL Type	DV SSL	DV SSL	DV SSL	DV SSL
SM2 SSL Type	OV SSL	OV SSL	OV SSL	OV SSL
WTIV Type	EV	EV	EV	EV
SM2 https throughput	900 Mbps	3 Gbps	9 Gbps	900 Mbps
ECC https throughput	910 Mbps	3 Gbps	9 Gbps	910 Mbps
New connection (CPS)	10K	25K	50K	8K
Transaction (TPS)	40K	80K	150K	30K
Max concurrent	300K	1M	2M	100K
Network Interface	6xG	6xG + 2x10G	6xG + 4x10G	6xG
Chassis size	2U	2U	2U	2U
Power	Dual power	Dual power	Dual power	Dual power
Cert value (5 Years)	440K RMB	660K RMB	1.13M RMB	1.13M RMB
Save HR value (5Y)	600K RMB	1M RMB	1.5M RMB	1.5M RMB
Suitable Scope	**SME Financial**	**Large Enterprise Gov / Financial**	**Public Cloud E-gov Cloud**	**Government Financial**

4. Deployment Solutions

ZoTrus SM2 HTTPS Auto WAF Gateway supports multiple network deployment methods, supports cluster deployment of multiple devices, supports automatic docking with ZoTrus Cloud SSL System to automatically configure dual SSL certificates required for https encryption for the Gateway, and also supports localized deployment of ZoTrus Cloud SSL System for e-government cloud or public cloud, which automatically issues dual SSL certificates for local cloud users, and the local HTTPS Auto WAF Gateway device automatically connects to the locally deployed Cloud SSL System. In order to ensure the high availability of the Gateway, dual-machine deployment is strongly recommended to ensure 24*365 uninterrupted provision of https encryption service and WAF protection.

(1) Gateway routing mode deployment

The two network cards of the ZoTrus SM2 HTTPS Auto WAF Gateway are respectively responsible for processing the internal and external network interfaces of two different routes, and the HTTPS Auto WAF Gateway itself acts as a router or NAT device. All network data traffic is accelerated, offloaded, and converted through the HTTPS Auto WAF Gateway. Data packets conforming to the security application protocol will be forwarded to the corresponding internal server according to the load balancing strategy. Other NAT data will not be affected, and standard routing network communication is supported.

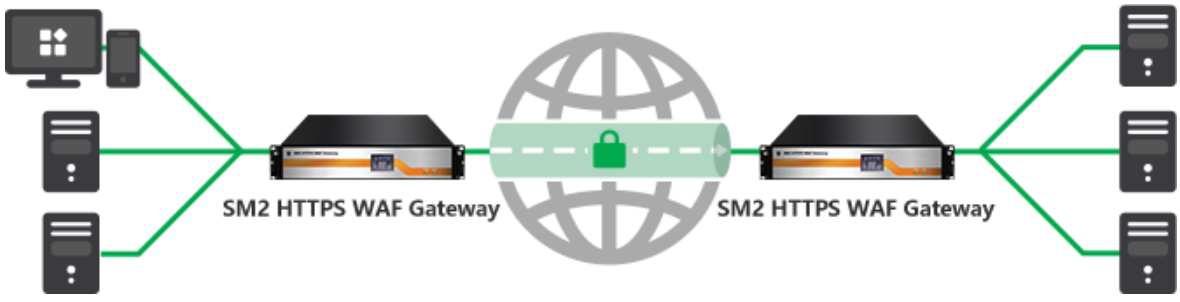


The routing mode deployment requires that the HTTPS Auto WAF Gateway and the internal server be deployed on different network segments. It is necessary to assign a public IP address and an intranet IP address to the HTTPS Auto WAF Gateway. And set the Gateway as an intranet gateway and enable the DHCP service, and the internal server is connected to the intranet switch. In this mode, the HTTPS Auto WAF Gateway provides HTTPS encryption, offloading, forwarding and routing service at the same time.

The routing mode deployment will change the IP address of the original server and reassign the intranet IP address to the original server. The original public network IP address is configured for the Gateway, supports IP V4 and IP V6, and the original domain name resolution does not need to be changed.

(2) Gateway to gateway deployment

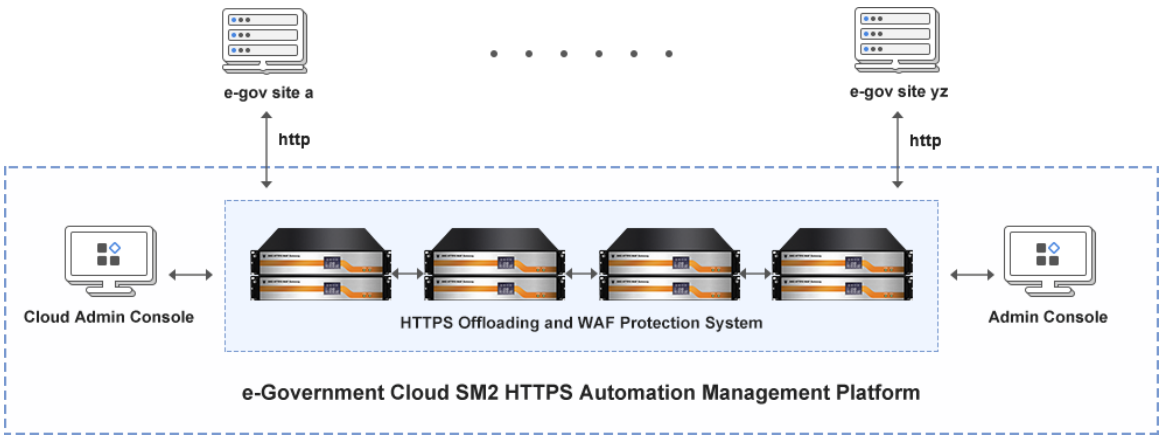
The ZoTrus SM2 HTTPS Auto WAF Gateway supports separate deployment on the client network and the server network to form a symmetrical "gateway to gateway" topology. The gateway-to-gateway deployment method is very suitable for business exchanges between the central office and the branch office. It can automatically encrypt a large number of application data requests of the branch office, transmit them to the central office through the Internet, and then automatically decrypt the data and send it to the business server. The entire application and the system itself do not need to deal with the https encryption of the communication link. The symmetrically deployed HTTPS Auto WAF Gateway can realize a transparent high-speed encrypted channel to ensure the security of data transmission.



The gateway-to-gateway deployment mode is extremely simple, without changing the original network topology, which greatly reduces the complexity of gateway deployment, and can be widely used in the "bank-enterprise direct connection" business in the financial industry, the ETC networking business in the transportation industry and application scenarios such as business data centralization of systems for enterprise groups and branches.

(3) Gateway cluster deployment

For https encryption applications on the high-traffic websites, e-government cloud platforms and public cloud platforms, multiple HTTPS Auto WAF Gateways must be deployed to form a cluster array-HTTPS offloading system. Multiple HTTPS Auto WAF Gateways work together to share business traffic and serve as hot backup for each other equipment. When one gateway fails, the services running on it can be taken over by other gateways to ensure that business scheduling can be fully and timely responded. The cluster mode is suitable for the deployment requirements of a redundant network environment that emphasizes extremely high-performance throughput.



For the deployment of small and medium-sized websites, it is recommended to deploy at least two HTTPS Auto WAF Gateways to realize dual-machine hot backup and ensure uninterrupted 24 hours x 365 days of https encryption services. Two dual-system hot standby modes are optional:

a) **Master-Master mode**

Master-Master mode is Active-Active mode: Two HTTPS Auto WAF Gateways are deployed in the network, and both devices act as hosts and process business traffic at the same time, and also serve as backups for each other. When one of the HTTPS Auto WAF Gateways has a problem and cannot continue to work, the other HTTPS Auto WAF Gateway undertakes all the services, so as to ensure that the service scheduling can still be responded to and processed, and there will be no partial interruption in the network. This mode is suitable for the deployment requirements of a redundant network environment (such as VRRP) that emphasizes high availability. This mode is recommended, and the two machines share business traffic without wasting resources.

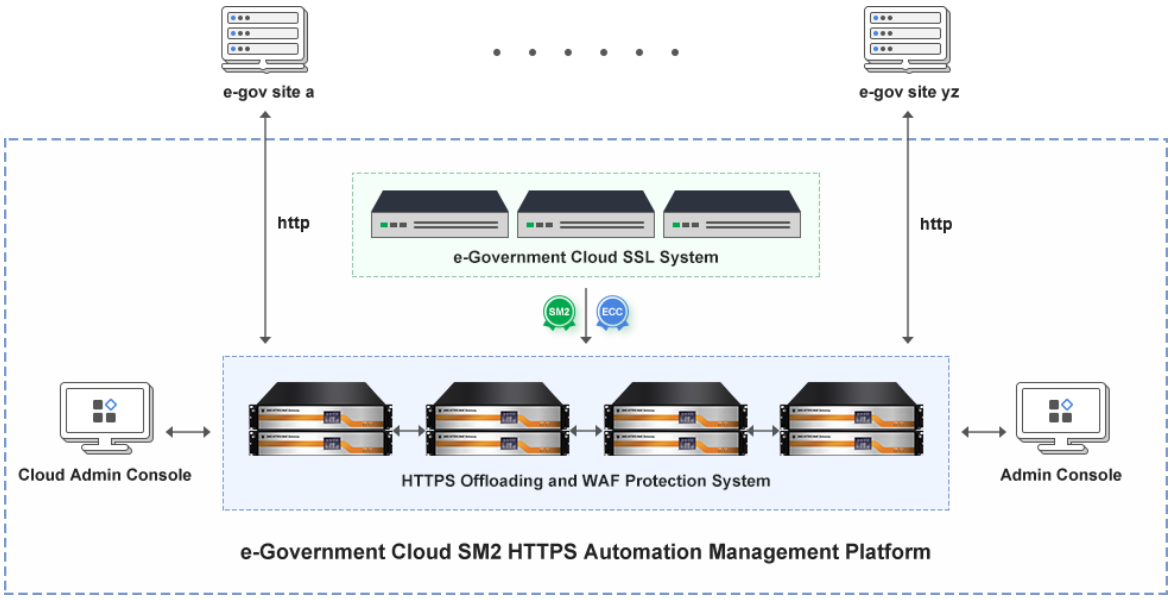
b) Master-Slave mode

The Master-Slave mode is Active-Backup mode: Two HTTPS Auto WAF Gateways are deployed in the network, one handles business traffic and is called the Master; the other is on standby and is called the Backup. While the master is processing business, it will synchronize the session information generated by the business to the backup machine, so as to ensure that after the switchover, the newly initiated business access can continue to be responded to and processed, and the current business access will not be interrupted. This mode is suitable for the deployment requirements of avoiding single point of failure in most network environments. The standby machine in this mode is idle and is not recommended.

(4) Local deployment of Cloud SSL System

By default, the HTTPS Auto WAF Gateway automatically connects with the ZoTrus Cloud SSL System to enable https encryption and WAF protection after obtaining the dual SSL certificates. For cloud platform customers who want to independently issue their own brand of dual SSL certificates that are automatically deployed to the gateway, they can deploy the ZoTrus Cloud SSL System locally to realize automatic issuance of the dual SSL certificates by the custom-branded dedicated SSL intermediate root certificate. The locally deployed system is called the E-government Cloud SSL System or the Public Cloud SSL System.

The E-government Cloud SSL System is a locally deployed CA system for issuing cryptography-compliant SSL certificates that support SM2 Certificate Transparency. The deployment of the whole system is to realize the completely independent and controllable issuance and management of SM2 SSL certificates for e-government website and the relatively independent issuance of ECC SSL certificates. To achieve independent and controllable issuance of e-government SSL certificates, first of all, there must be an intermediate root certificate for issuing SSL certificates, so that all e-government systems can reliably realize that all e-government systems only trust SSL certificates issued by their own intermediate root certificates, effectively preventing various SSL man-in-the-middle attacks against e-government websites and other fake e-government website attacks.



5. Summary

ZoTrus SM2 HTTPS Auto WAF Gateway global exclusive innovation to achieve zero change of the original server to realize automatic https encryption, WAF protection, SM2/ECC dual-algorithm adaptive https encryption, just configure website domain name and IP address at startup, immediately enable https encryption and acceleration service, WAF protection, TCP/DTLS secure delivery, automatic preparation of dual SSL certificates, global trust and cryptography compliance, high-speed dynamic caching and compression, connection multiplexing, session persistence and load balancing, etc. While ensuring high performance, it provides the industry's highest performance-price ratio.

The ZoTrus SM2 HTTPS Auto WAF Gateway is plug-and-play, deployed on the front end of the website server, the original website server can be seamlessly upgraded from non-protection Web http to Web protection https without any modification, and it is the SM2 https encryption that meets the cryptography compliance, and the ECC https encryption for compatible of all browsers that do not support SM2 algorithm. Its powerful https acceleration, offloading and forwarding function provides additional performance enhancement support for the website server, not only does not increase the burden of https encryption and decryption, but also enhances the external response capability and the ability to process user requests. The seamless switching of zero-reconstruction, zero-maintenance, and zero-impact of the ZoTrus SM2 HTTPS Auto WAF Gateway is the first choice and must for the SM2 https encryption and system security upgrade from http to https.

Contact us: +86-755-2660 4080, Email: help@zotrus.com

