ZoTrus®

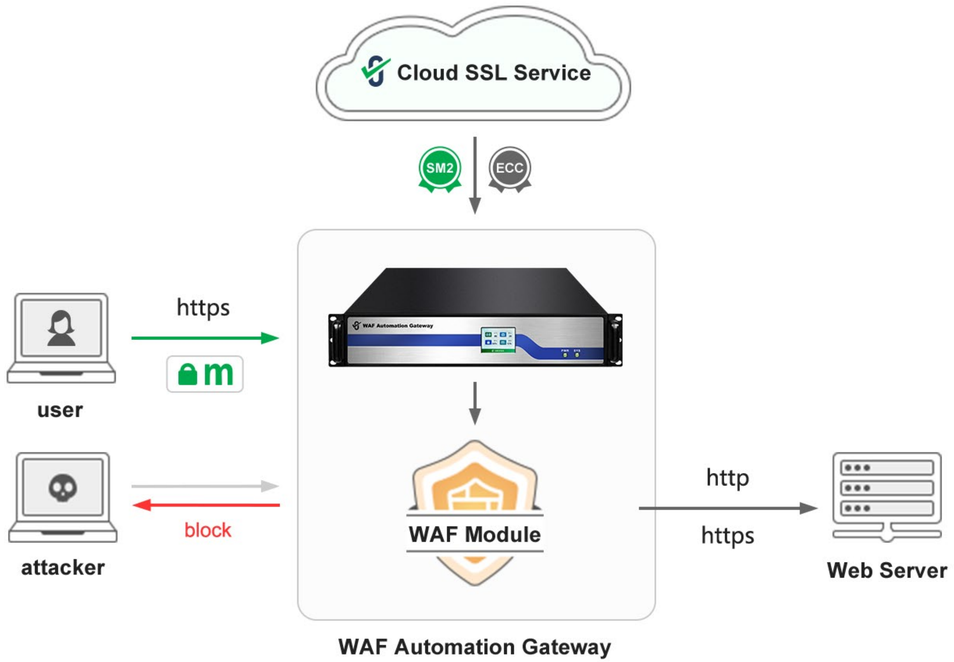
ZoTrus WAF Automation Gateway

Automatically implement WAF protection with https encryption

https://www.zotrus.com

1 Product Introduction

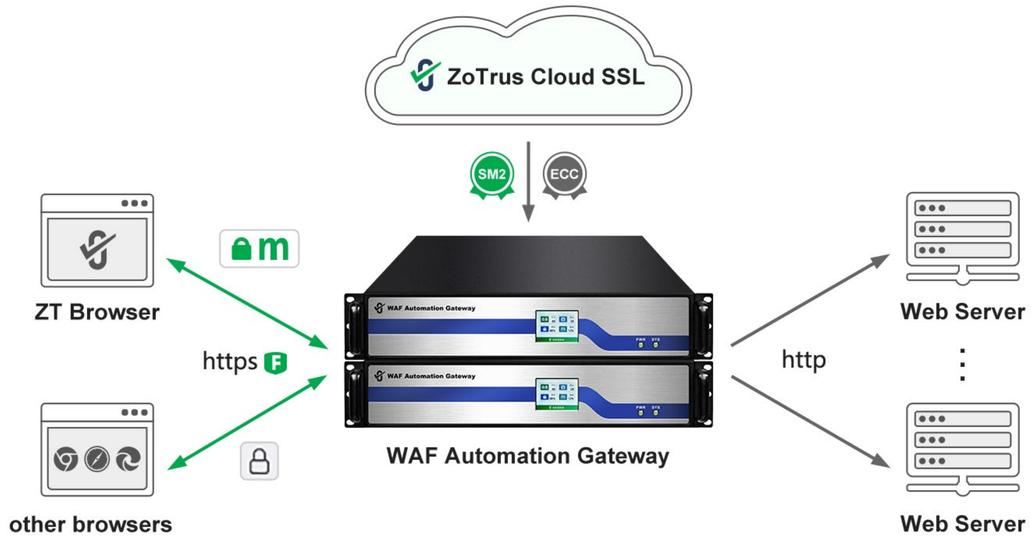
ZoTrus WAF Automation Gateway is another innovative product that protects website security based on the SM2 HTTPS Automation Gateway that has passed the commercial cryptography product certification to increase WAF protection function, which is the first in China, and is a new generation of WAF equipment that integrates WAF protection, https encryption acceleration, https offloading and forwarding, SM2 algorithm module, SSL certificate automation, load balancing and other functions, while realizing high-quality web application firewall to protect website security. It automatically supports WAF protection in the HTTPS encryption mode, because website security requires both WAF protection and HTTPS encryption to ensure the transmission security of confidential data on the website, and it is the HTTPS encryption of the adaptive encryption algorithm, and the SM2 algorithm is preferred to achieve HTTPS encryption. ZoTrus WAF Automation Gateway innovatively provides both WAF protection services and HTTPS encryption automation services, while ensuring the data "in-transit" encryption security and "onshore" protection.



The biggest features and characteristics of the ZoTrus WAF Automation Gateway are zero application for SSL certificates, zero installation of SSL certificates, automatic implementation of WAF protection with HTTPS encryption, 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 WAF Automation 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 automatically, to provide WAF protection with https encryption service uninterrupted for business systems with up to 255 different domain names.

2 Main Functions

There are three core functions of ZoTrus WAF Automation Gateway: (1) WAF protection; (2) Support SM2 HTTPS encryption; (3) Automate HTTPS encryption. It is not only a WAF device but also an HTTPS encryption automation gateway, no need to apply for an SSL certificate from the CA, automatically configure a dual-algorithm SSL certificate, automatically realize the WAF protection with HTTPS encryption, and the original web server has zero change, just deploy the WAF Automation Gateway before the original server, it can automatically realize WAF protection with https encryption, and provide WAF protection services and https encryption automation services 24 hours a day, 365 days a year. It is recommended to deploy the default dual-machine deployment, which is 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.



The WAF protection function of ZoTrus WAF Automation Gateway is developed and optimized based on the open-source ModSecurity system, and supports common web application firewall functions, such as: blocking SQL injection, blocking cross-site scripting (XSS), preventing attacks using local file inclusion vulnerabilities, preventing attacks using remote files (including vulnerabilities), preventing attacks using remote command execution vulnerabilities, blocking PHP code injection, blocking malicious access that violates HTTP protocol, Prevent attacks by exploiting remote proxy infection vulnerabilities, Shellshock vulnerabilities, Attack attempts using Session ID unchanged, Malicious website scanning, Source code or error information leakage, Honeypot blacklists, IP blocking based on IP address attribution, etc. And up to 12 different types of custom rules are supported to achieve personalized protection, such as allowing an IP to access a specific website and website directory.

Today, all browsers are showing HTTP website as "Not secure", HTTPS encryption is a mandatory configuration for the security of a website, of course, it is a necessary function of the WAF device, and the innovation of the ZoTrus WAF Automation Gateway is to automatically configure the dual-algorithm SSL certificate by connecting 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 all SM2 browsers. 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 - SM2 SSL Pro CA, its root CA certificate is Guizhou SM2 CA that Guizhou CA has the CA license issued by MIIT and SCA, 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 main ten functions of ZoTrus WAF Automation Gateway are:

01

High performance Web Application Firewall protection

Based on the industry-leading open-source ModSecurity system development and in-depth optimization, it supports the commonly used web application firewall function, provides security cleaning protection for web traffic after https encrypted traffic is offloaded, and only forwards normal and secure traffic to the internal web server behind.

02

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.

03

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.

04

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.

05

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.

The main ten functions of ZoTrus WAF Automation Gateway are:

06

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.

07

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.

08

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.

09

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

Security Authentication

Integrated security authentication function, support the use of two-way authentication (SKF standard) for USB Key SM2 certificates issued by China CAs, seamlessly support the two-way authentication function of ZT Browser, and support SM2/RSA algorithm client soft certificate for secure authentication.

3 Performance Indicators

ZoTrus WAF Automation Gateway provides an efficient, secure, transparent, easy-to-deploy, zero-reconstruction, fully automatic innovative solution to realize WAF protection with https encryption, 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.

The WAF protection performance of ZoTrus WAF Automation Gateway has been tested by the authoritative third-party online testing software WAFER, and its attack behavior detection and distinguishing capabilities are all A-level (the highest level), with a true positive detection rate of 97.34% and a false positive rate of 0 (it will not intercept false positive behaviors that are not attacks), which can meet the needs of website security protection applications.

WAFER Report 2024.05.29

Type	Total Requests	Detected	Error	%
True Positives	413	402	0	97.34%
False Positives	72	0	0	0%

Performance Scores

Detection Ability	Distinguishing Ability
A	A

The actual protection effect test result shows that the SQL Injection launched a total of 128 attacks and blocked 126 times. There were also 2 false negatives, that is, missed blocks, with a True Positive Rate of 98.44%. For Cross Site Scripting, a total of 149 attacks were launched and 147 were blocked. There were also 2 false negatives, that is, missed blocks, and the True Positive Rate was 98.66%. For Command Injection attacks, a total of 41 attacks were launched and 37 were blocked. There were also 4 false negatives, that is, missed blocks, with a True Positive Rate of 90.24%. For SSI Injection, a total of 24 attacks were launched and 24 were blocked. There are no false negative, and the True Positive Rate is 100%. Other test results are not analyzed one by one. For attacks that are not blocked, the Gateway WAF Module needs to be continuously improved in the WAF protection rules and the rules need to be updated regularly. Of course, customer also need to pay attention to analyzing WAF logs and constantly customize protection rules based on attacks.

Attack Type	Total	True Positives	False Negatives	True Positive Rate
SQL Injection	128	126	2	98.44%
Cross Site Scripting	149	147	2	98.66%
Command Injection	41	37	4	90.24%
SSI Injection	24	24	0	100%
File Upload	29	29	0	100%
Directory Traversal	20	17	3	85%
Buffer Overflow	10	10	0	100%
LFI (Local File Inclusion)	10	10	0	100%
RFI (Remote File Inclusion)	2	2	0	100%

ZoTrus WAF Automation Gateway provides fully independent and controllable software and hardware integration products, including Open source WAF system, 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 WAF Automation Gateway can meet the application requirements of these industries that have extremely high requirements for information security control.

Each ZoTrus WAF Automation 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 WAF protection with 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 WAF Automation 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 988 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 1.25 million RMB Yuan (=5*255*988, equal to US$172K), and the world's exclusive super-value WAF protection with https encryption automation solution!

ZoTrus WAF Automation Gateway currently provides 3 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 WAF protection with https encryption, especially the application requirements of zero reconstruction to realize WAF protection with https encryption. The product performance index parameters of various models are shown in the table below. For users with different index requirements, products can be customized to meet the requirements.

Model	MG-2-1	MG-2-8	MG-2-9
CPU	Intel Atom	Intel Xeon (dual)	Hygon 5380
WAF Performance	Level A	Level A	Level A
Customize WAF Rule	Yes	Yes	Yes
Regularly upgrade rule	Yes	Yes	Yes
Incl ECC SSL Qty	20	100 / 255	100 / 255
Incl SM2 SSL Qty	20	100 / 255	100 / 255
Dual SSL supply	5 years	5 years	5 years
ECC SSL Type	DV SSL	DV SSL	DV SSL
SM2 SSL Type	OV SSL	OV SSL	OV SSL
Unique Key/Certificate per Website	Yes	Yes	Yes
SSL Certificate Period	90 days	90 days	90 days
Certificate Update Cycle	Every 80 days	Every 80 days	Every 80 days
WTIV Type	EV	EV	EV
SM2 https throughput	800 Mbps	9 Gbps	9 Gbps
ECC https throughput	800 Mbps	9 Gbps	9 Gbps
SM2 SSL Request	30 K/S	120 K/s	60 K/s
ECC SSL Request	40 K/S	130 K/s	90 K/s
Max concurrent	250K	1.5M	1M
Network Interface	6xG	6xG + 4x10G	6xG + 4x10G
Chassis size	155*240*40 (mm)	2U	2U
Power	Single supply 60W	Dual supply 550W	Dual supply 550W
Cert value (5 Years)	490K RMB	2.44M / 6.23M RMB	2.44M / 6.23M RMB
Save HR value (5Y)	120K RMB	600K / 1.5M RMB	600K / 1.5M RMB
Suitable Scope	SME Colleges and Universities	Large Enterprise Public Cloud E-gov Cloud	Large Enterprise Gov / Financial E-gov Cloud

ZOTRUS

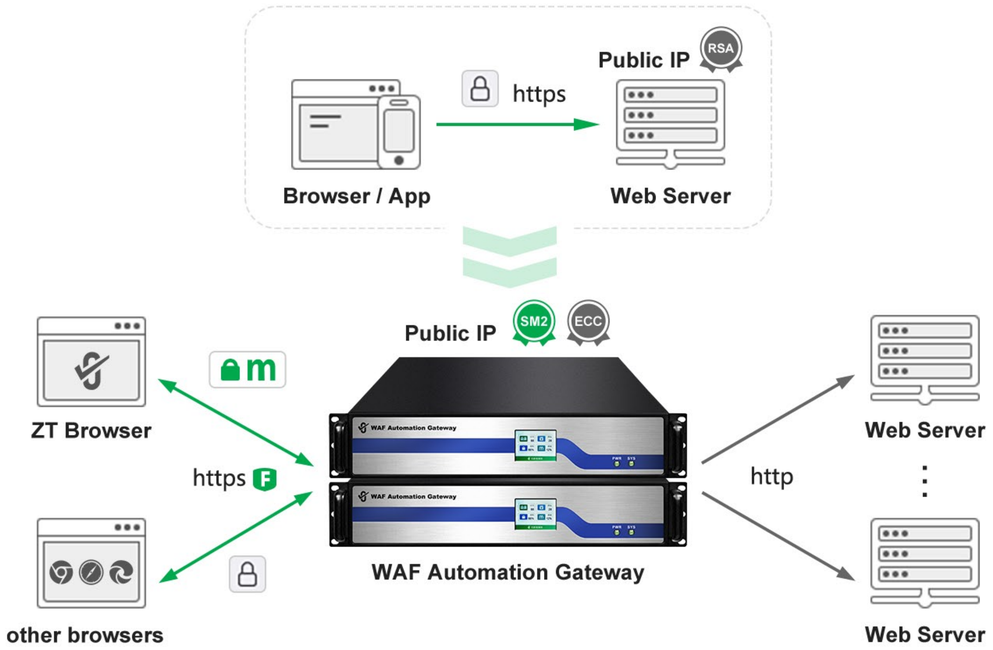
4

Deployment Solutions

https://www.zotrus.com

ZoTrus WAF Automation 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 WAF Automation 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 WAF protection and https encryption services.

1. Provide HTTPS encryption automation service for local web servers (websites)



To provide WAF protection, user must deploy the WAF device in front of the Web server, and the WAF device can protect HTTP/HTTPS traffic and forward the normal plaintext traffic and the decrypted plaintext traffic to the subsequent Web server. However, if user purchase a traditional WAF device, user need to apply for an SSL certificate from a CA and manually deploy it on the WAF device, which is very time-consuming and laborious. With ZoTrus WAF Automation Gateway, user do not need to apply for an SSL certificate from the CA, and the ZoTrus WAF Automation Gateway automatically connects to the ZoTrus Cloud SSL service system to automatically configure dual SSL certificates for the user's website, and automatically realizes HTTPS encrypted WAF protection.

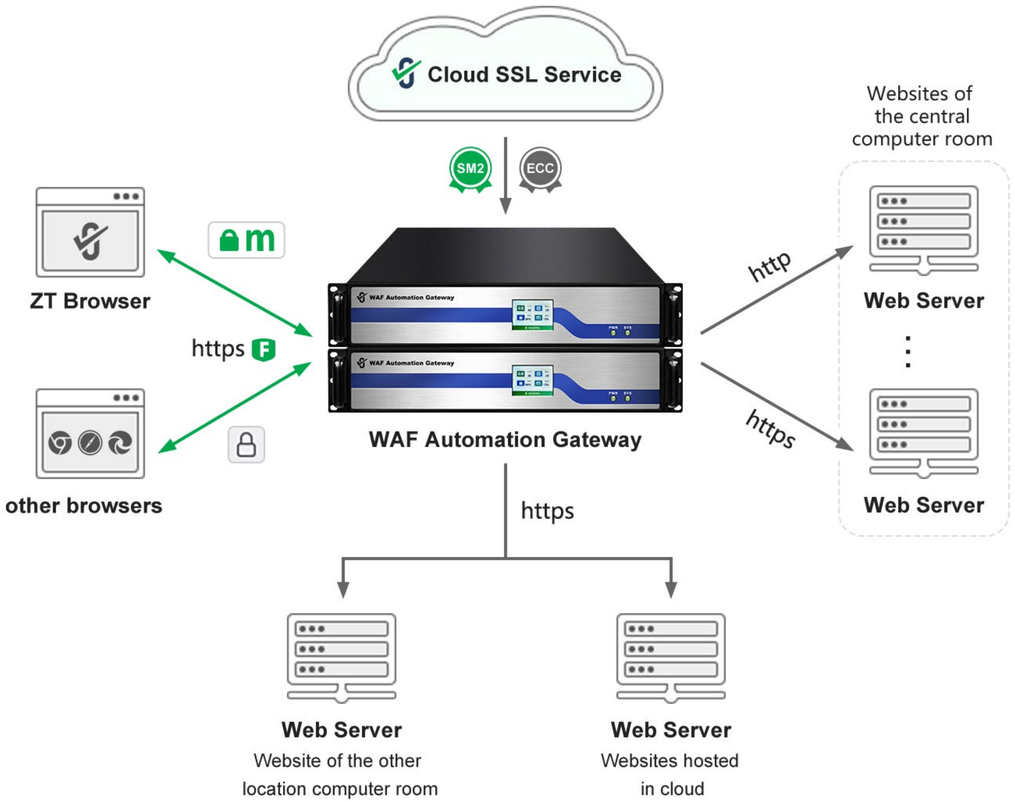
One network port of the ZoTrus WAF Automation Gateway is connected to the original public network interface, and the public IP address of the original web server is configured, and the original web server is connected to other ports, and a maximum of 8 web servers can be connected by default, and these web servers are configured with private IP addresses instead. All network data traffic is accelerated, offloaded, and transferred through the gateway, and data packets that comply with the security application protocol by WAF policy will be forwarded to the corresponding internal web server according to the load balancing policy, supporting HTTP plaintext forwarding and HTTPS encrypted forwarding.

This deployment method turns the original web server exposed in Internet into an intranet server, protects the security of the web server, and transfers all the HTTPS encryption and decryption workloads that the original web server is responsible for to the gateway, which can save 20%-30% of the computing power to the web server, so that the web server can better provide computing power for the business system.

This deployment method is suitable for users who have their own computer room and their own web server, and need to add a gateway device in the computer room, which will change the IP address of the original web server, reassign the private IP address to the original web server, configure the original public IP address for the gateway, and the gateway supports IP V4 and IP V6, and the original domain name resolution does not need to be changed, and Web server no need to support IP V6.

The default deployment mode is the hot standby mode of two gateways, and the two gateways are in the active-active mode, in which both gateways act as hosts and process service traffic at the same time and are also standby servers for each other. The two gateways share the service traffic and do not waste resources. When one of the gateways has a problem and cannot continue to work, the other gateway takes on all the work, so as to ensure the continuous and reliable operation of the business system. The Gateway is guaranteed for 5 years, and if there is a failure within 5 years, the gateway will be replaced free of charge to ensure uninterrupted WAF Protection and HTTPS encryption automation services within 5 years.

2. Provide HTTPS encryption automation service for web servers (websites) that are not local



For users who not only need to implement WAF protection and HTTPS encryption automation services on local servers, but also have web servers in branches or multiple websites deployed on the cloud that also need WAF protection and HTTPS automation service, ZoTrus WAF Gateway supports both local forwarding mode and remote back-to-origin mode. Regardless of whether the web server (website) is in a foreign computer room or a cloud host, as long as the gateway can access it through the public network or intranet, these websites are back-to-origin origin servers similar to CDN services, and the Gateway can provide WAF protection and HTTPS encryption automation services for them all. Dual gateways provide WAF protection and HTTPS encryption automation services for up to 255 websites, and more websites need to purchase more gateways.

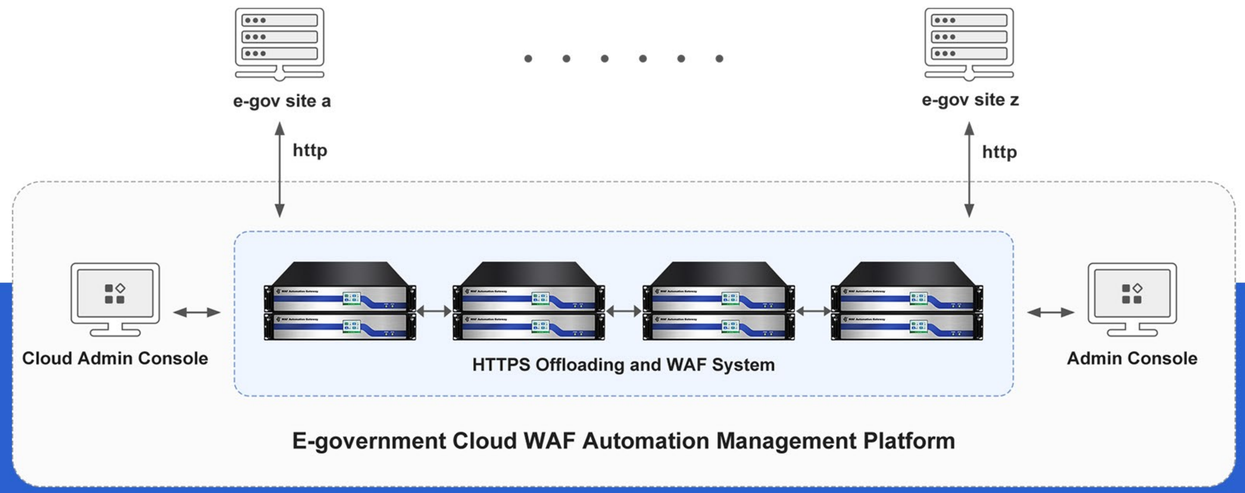
In order to ensure the data security of the website system that is not located in the central computer room, the back-to-origin connection from the gateway to the other location server must be encrypted by HTTPS to achieve full-link encryption. ZoTrus Technology provides a self-signed back-to-origin SSL certificate with a validity period of 5 years for back-to-origin websites for free, and the original website does not need to deploy a globally trusted SSL certificate with a validity period of only one year.

This deployment method is also suitable for service providers who provide website design, web hosting, and SSL certificate sales, and deploy multiple gateways to provides WAF protection and HTTPS encryption automation services for their own business systems, as well as WAF protection and HTTPS encryption automation services for their customers, regardless of where the customer's website is hosted, only need it is accessible for HTTP or HTTPS.

3. Cloud platform WAF automatic management cluster deployment solution

For various cloud platforms, such as e-government cloud platforms and public cloud platforms, there are tens of thousands or even millions of websites that need WAF protection and HTTPS encryption, and the only solution can only be done by automation. It is necessary to deploy multiple WAF Automation Gateway to form a cluster array - HTTPS Offloading and WAF System, and multiple WAF Automation Gateway work together to share business traffic and serve as hot standby gateways for each other. When a gateway fails, services running on it will be taken over by other gateways to ensure adequate and timely response to service scheduling. Cluster mode is suitable for the deployment of redundant network environments with an emphasis on extremely high-performance throughput.

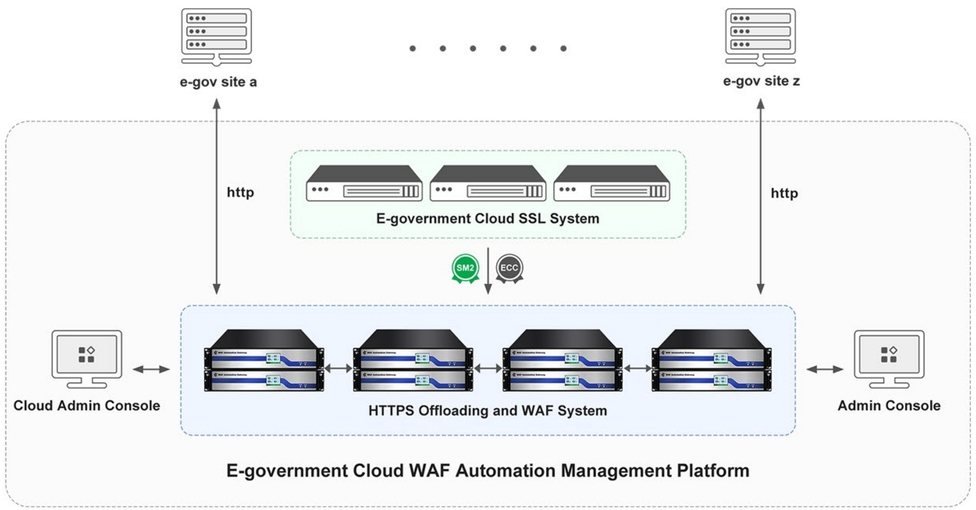
Different from other traditional WAF device deployment solutions, the innovation is that it automatically configures dual-algorithm SSL certificates, automatically realizes HTTPS encryption and offloading and WAF protection, and does not need to manually apply for and manually deploy dual-algorithm SSL certificates from CAs after purchasing WAF devices on the cloud platform and renew the application and deployment every year. This solution includes 5 years of automatic application and deployment of dual-algorithm SSL certificates, and 5 years of automatic WAF protection with HTTPS encryption, meeting the requirements of cloud platform commercial cryptography compliance and globally trusted HTTPS website protection applications.



4. Local deployment of Cloud SSL System

By default, the ZoTrus WAF Automation Gateway automatically connects with the ZoTrus Cloud SSL System to enable https encryption 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 WAF Automation Gateway global exclusive innovation to achieve zero change of the original server to realize WAF protection and https encryption automation, SM2/ECC dual-algorithm adaptive https encryption, just configure website domain name and IP address at startup, immediately enable WAF protection, https encryption and acceleration service, 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 WAF Automation Gateway is plug-and-play, deployed on the front end of the website server, not only provided WAF protection, but also the original website server can be seamlessly upgraded from http to 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 and offloading ability provide power support for WAF module, and the after-WAF-protected 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 WAF Automation Gateway is the first choice and must for WAF protection, SM2 https encryption automation and system security upgrade from http to https.

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