ZoTrus®

Internet Edition

ZoTrus HTTPS Automation Gateway

SSL certificate automation management to realize https encryption

https://www.zotrus.com

1 Product Introduction

ZoTrus HTTPS Automation Gateway (Abbr.: ZoTrus Gateway) is a high-end high-performance website security hardware gateway device built by ZoTrus Technology using high-performance cipher cards that have passed the SSL VPN Product / Security Gateway class Security Level 2 China Commercial Cryptography Product Certification. It is a hardware gateway including https encryption acceleration, https offloading and forwarding, SM2 algorithm module, SSL certificate automatic management, and load balancing, it is dedicated to https acceleration and offloading 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.

Commercial Cryptography Product Certification Certificate

商用密码产品认证证书

Cert No.
证书编号：GM004410620230847

委托人名称及所在地 Client Name and Location

零信技术(深圳)有限公司 ZoTrus Technology Limited
深圳市南山区粤海街道滨海社区高新南十道 87、89、91 号深圳市软件产业基地 2 栋 C301C

产品名称和型号、版本 Product Name, Model, Version

国密 HTTPS 加密自动化网关
SM2-HTTPS-Auto-Gateway-MG V1.0

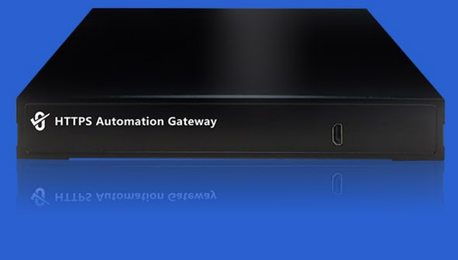
产品标准和技术要求 Product standards, technical requirement

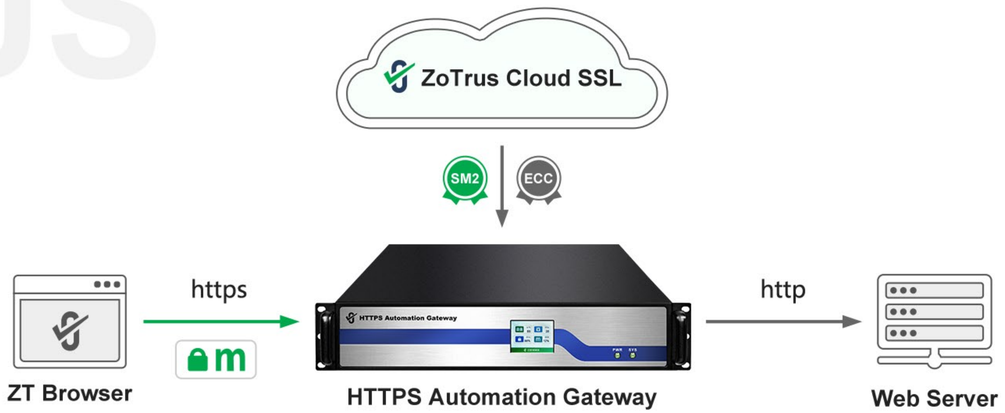
GM/T 0025《SSL VPN 网关产品规范》
GM/T 0028《密码模块安全技术要求》第二级要求

上述产品符合商用密码产品认证规则的要求，特此发证。

颁发日期：2023 年 9 月 27 日 Issue date:

有效期至：2028 年 9 月 26 日 Valid until:



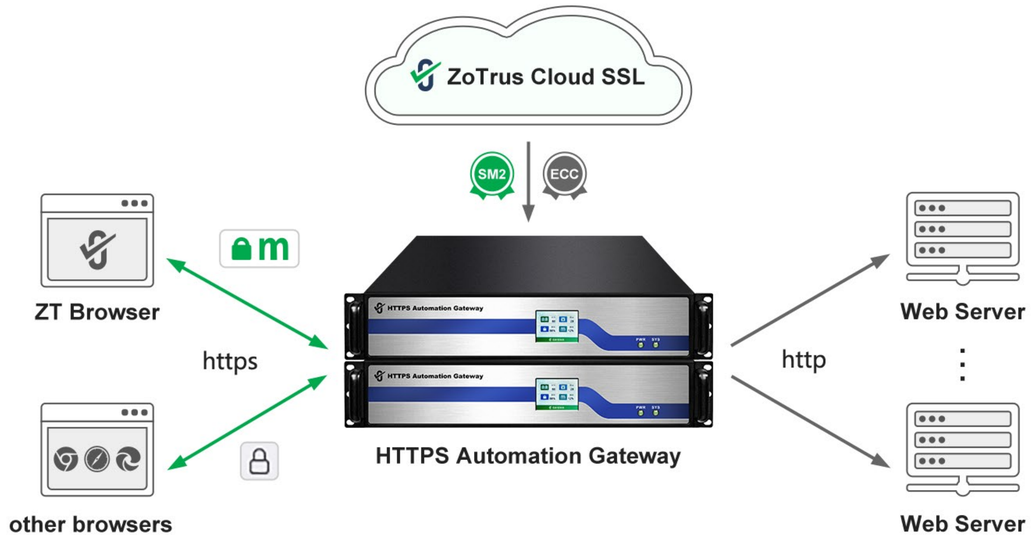


The biggest features and characteristics of the ZoTrus HTTPS Automation Gateway are zero application for SSL certificates, zero installation of SSL certificates, automatic implementation of HTTPS encryption, adaptive encryption algorithms. The browsers that support SM2 algorithm and SM2 Certificate Transparency 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 SM2 HTTPS 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 https encryption service and WAF protection service uninterrupted for business systems with up to 255 different domain names.

2

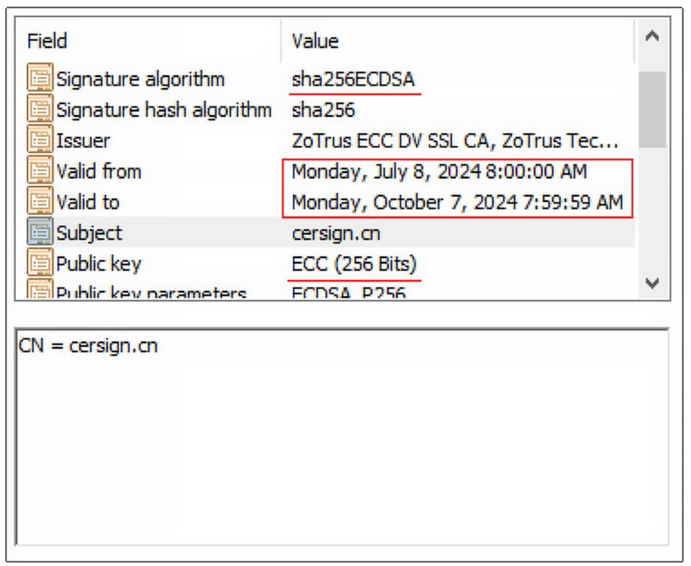
Main Functions

The core function of the ZoTrus HTTPS Automation Gateway is zero reconstruction of the original Web server, no need to install an SSL certificate on the Web server, no need to install ACME Client software on the Web server, and no need to upgrade the Web server software to support the SM2 algorithm, just deploy HTTPS Automation Gateway before the original server, then it can automatically implement https encryption, and provide https encryption services and WAF protection service 24 hours 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. A 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.



All browsers are showing HTTP website as "Not secure" today, and HTTPS encryption is a must for website security. The dual-algorithm dual-SSL certificate required for HTTPS encryption is automatically completed by the HTTPS Automation 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 OV 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 validity period of the dual SSL certificates automatically configured by ZoTrus HTTPS Automation Gateway is 90 days, which meets the upcoming 90-day certificate policy in advance. The following figure on the left shows the 90-day SM2 OV SSL certificate configured by the gateway by default, and the ECC DV SSL certificate with a 90-day validity period configured by the gateway on the right, and the automatic deployment of the 90-day certificate will greatly improve the security and agility of the HTTPS encryption service. And the dual SSL certificates are based on the elliptic curve algorithm, the certificate chain file is the smallest, which saves the traffic of the IDC and the traffic of user's mobile phone, save the power consumption of the IDC and the power of user's mobile phone, this is more environmentally friendly.



ZoTrus HTTPS Automation Gateway has a built-in WAF module by default, this 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 only necessary to deploy a HTTPS Automation 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.

ZoTrus HTTPS Automation Gateway is also a security authentication gateway, which supports the USB Key SM2 certificate issued by China CA to use two-way authentication (SKF standard), with the two-way authentication support function of ZT Browser, users do not need any additional development, just choose to enable two-way authentication while setting the SM2 HTTPS automation service on the Gateway, users can set multiple client certificate issuance CAs, and the China Public SM2 Root CA certificate has been preset by default. And it supports two-way authentication of RSA algorithm soft certificate and USB Key hard certificate.

The main ten functions of ZoTrus HTTPS Automation Gateway are:

01

Zero reconstruction for https encryption

The original Web server does not need to install an SSL certificate, no need to install ACME client software, zero reconstruction to realize https encryption, adaptive encryption algorithm, support RSA/ECC/SM2 algorithm to realize https encryption.

02

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.

03

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.

04

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.

05

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.

The main ten functions of ZoTrus HTTPS Automation Gateway are:

06

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.

07

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.

08

Multi-algorithm load balancing

The Gateway supports multiple load balancing algorithms: round robin, weighted round robin, minimum number of connections, and IP hash, allowing customer to select the appropriate load balancing mode according to their business needs to provide higher service performance, availability, and scalability.

09

Web Application Firewall Module (ZoTrus Gateway WAF)

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.

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 HTTPS Automation 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.

ZoTrus HTTPS Automation 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 HTTPS Automation Gateway can meet the application requirements of these industries that have extremely high requirements for information security control.

Each ZoTrus HTTPS 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 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.

Each ZoTrus HTTPS Automation Gateway has a warranty period of 5 years, and automatically configures a globally trusted ECC DV SSL certificate and cryptography compliance SM2 OV SSL certificate for no more than 255 website domain names within 5 years. Calculated according to the price of CerSign OV SSL Certificate Lite (4888 Yuan/year), the value of the SSL certificates that are automatically configured is as high as 6.23 million RMB Yuan (=5*255*4888, equal to US$865K), and the world's exclusive super-value https encryption automation solution!

ZoTrus HTTPS 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 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 table below. For users with different index requirements, products can be customized to meet the requirements.

ZOTRUS

Model	MG-1-1	MG-1-8	MG-1-9
CPU	Intel Atom	Intel Xeon (dual)	Hygon 5380
Number of Websites	20	100 / 255	100 / 255
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
WAF Function	Built-in	Built-in	Built-in
Customize WAF Rule	Yes	Yes	Yes
Regularly upgrade rule	Yes	Yes	Yes
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

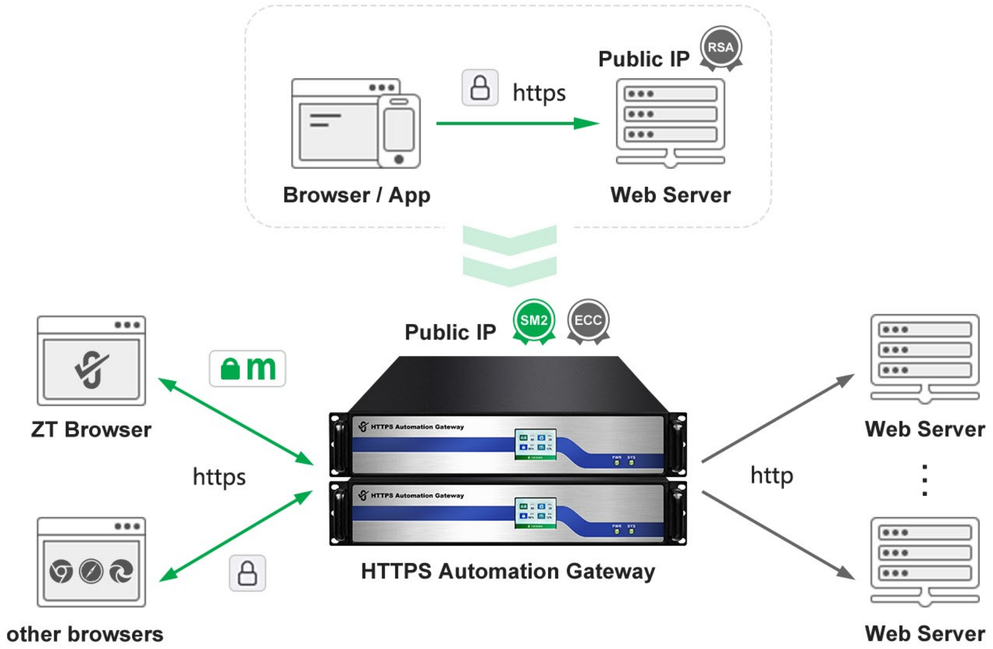
4

Deployment Solutions

https://www.zotrus.com

ZoTrus HTTPS Automation Gateway supports multiple deployment and application modes and supports cluster deployment of multiple devices. In order to ensure the high availability of the gateway, it is highly recommended to deploy two gateways to ensure 24*365 days of uninterrupted automatic provision of HTTPS encryption service and WAF protection service.

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



The traditional implementation of HTTPS encryption is that the user applies for an SSL certificate from the CA and manually deploys it on the web server to implement HTTPS encryption, which is a very time-consuming and laborious task for users who need to deploy SSL certificates for multiple websites. If user purchase ZoTrus HTTPS Automation Gateway and deploy it in front of the Web server, user don't need to apply for an SSL certificate from the CA, and the ZoTrus Gateway will automatically connect with the ZoTrus Cloud SSL Service System to automatically configure dual SSL certificates for the website, and automatically realize HTTPS encryption and WAF protection.

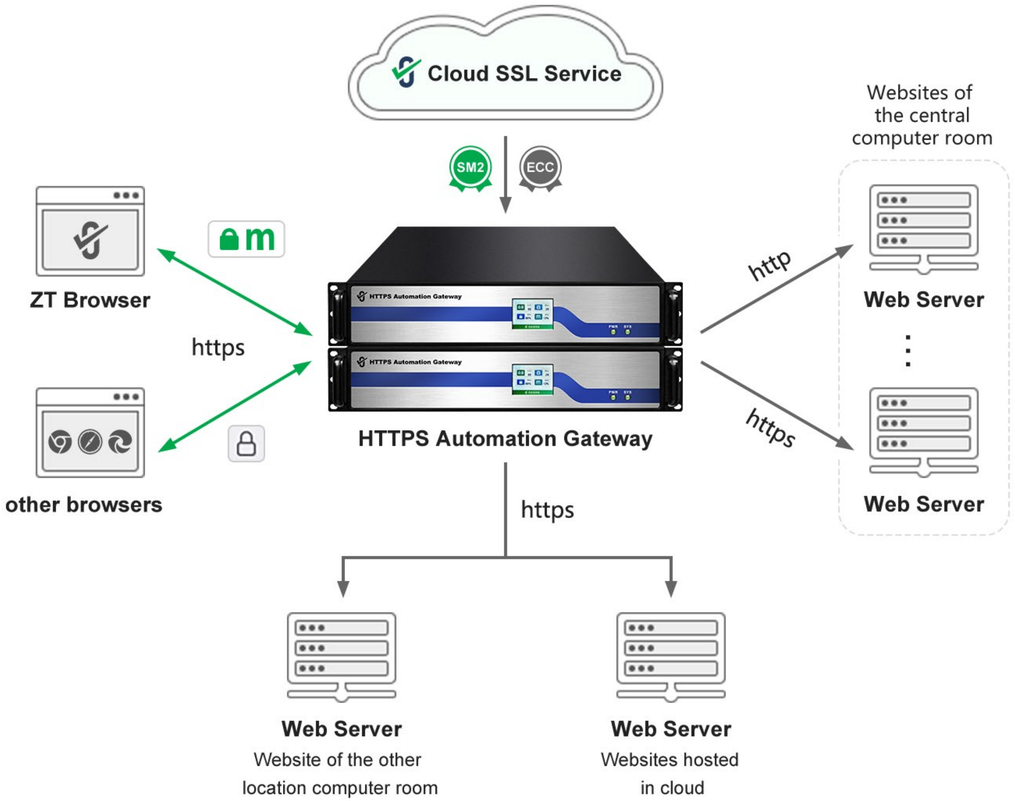
One network port of the ZoTrus HTTPS Automation Gateway is connected to the original public network interface, and the public IP address of the original web server is configured, and the original web server is connected to other ports, and a maximum of 8 web servers can be connected by default, and these 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 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.

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 HTTPS encryption automation service and WAF protection service within 5 years.

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



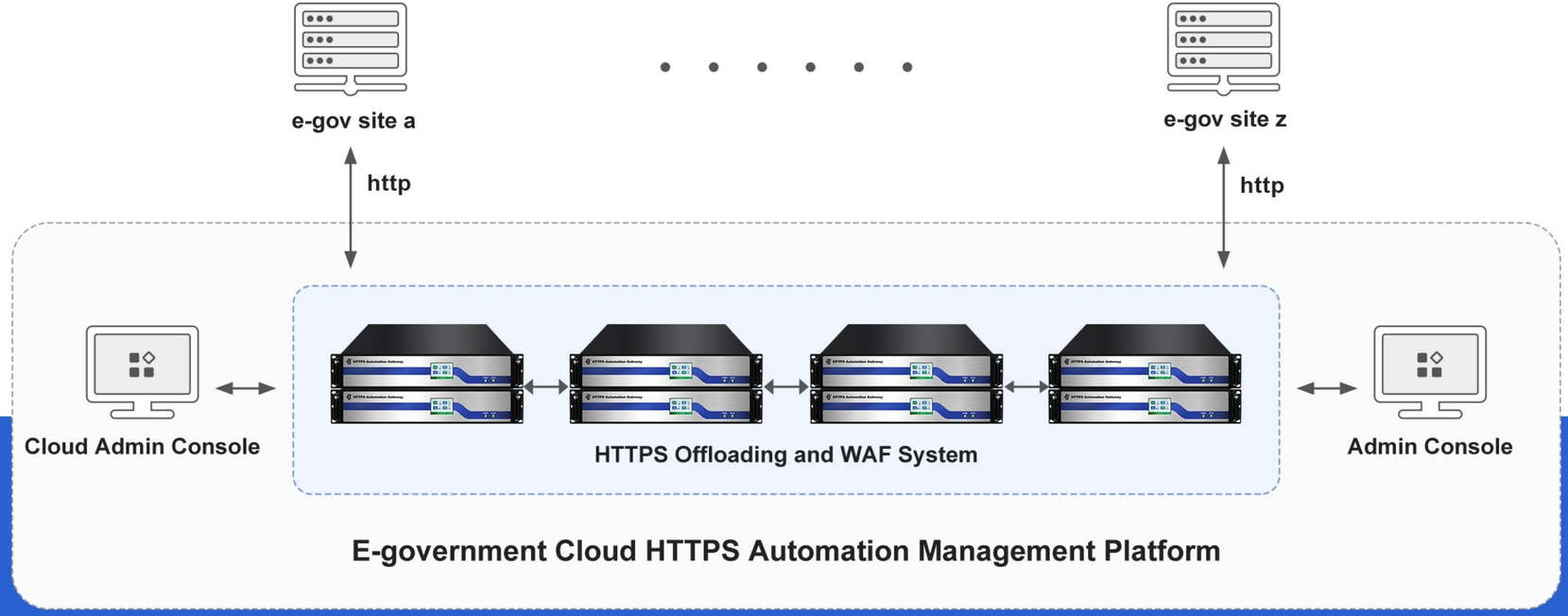
For users who not only need to implement HTTPS encryption automation services on local servers, but also have web servers in branches or multiple websites deployed on the cloud that also need HTTPS automation service, ZoTrus Gateway supports both local forwarding mode and remote back-to-origin mode. 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 HTTPS encryption automation service and WAF protection service for them all. Dual gateways provide HTTPS encryption automation service and WAF protection service 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.

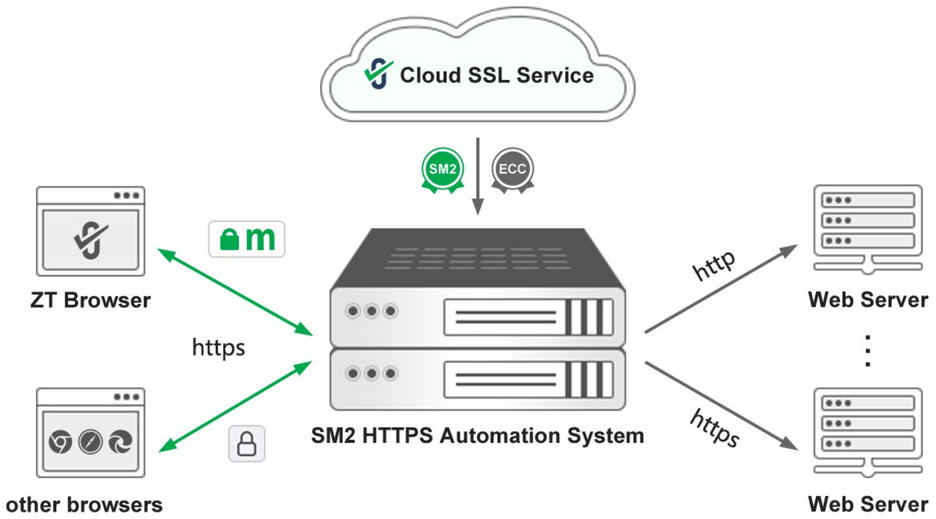
This deployment method is also suitable for service providers who provide website design, web hosting, and SSL certificate sales, and deploy multiple gateways to provide HTTPS encryption automation service and WAF protection service for their own business systems, as well as HTTPS encryption automation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

3. Cloud platform HTTPS encryption 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 HTTPS encryption, and the only solution can only be done by automation. It is necessary to deploy multiple HTTPS encryption automation gateways to form a cluster array - HTTPS Offloading and WAF System, and multiple HTTPS encryption automation gateways 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.



4. Optional: ZoTrus HTTPS Automation System

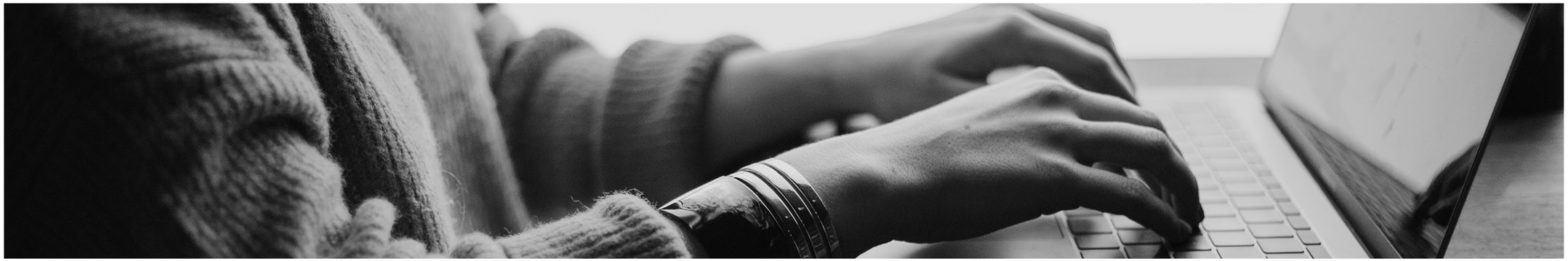


If you have an idle server or are not convenient to deploy the ZoTrus HTTPS Automation Gateway hardware device, you can purchase the ZoTrus HTTPS Automation System and deploy the gateway system on your own server bare metal to achieve the same excellent functions as the ZoTrus HTTPS Automation Gateway.

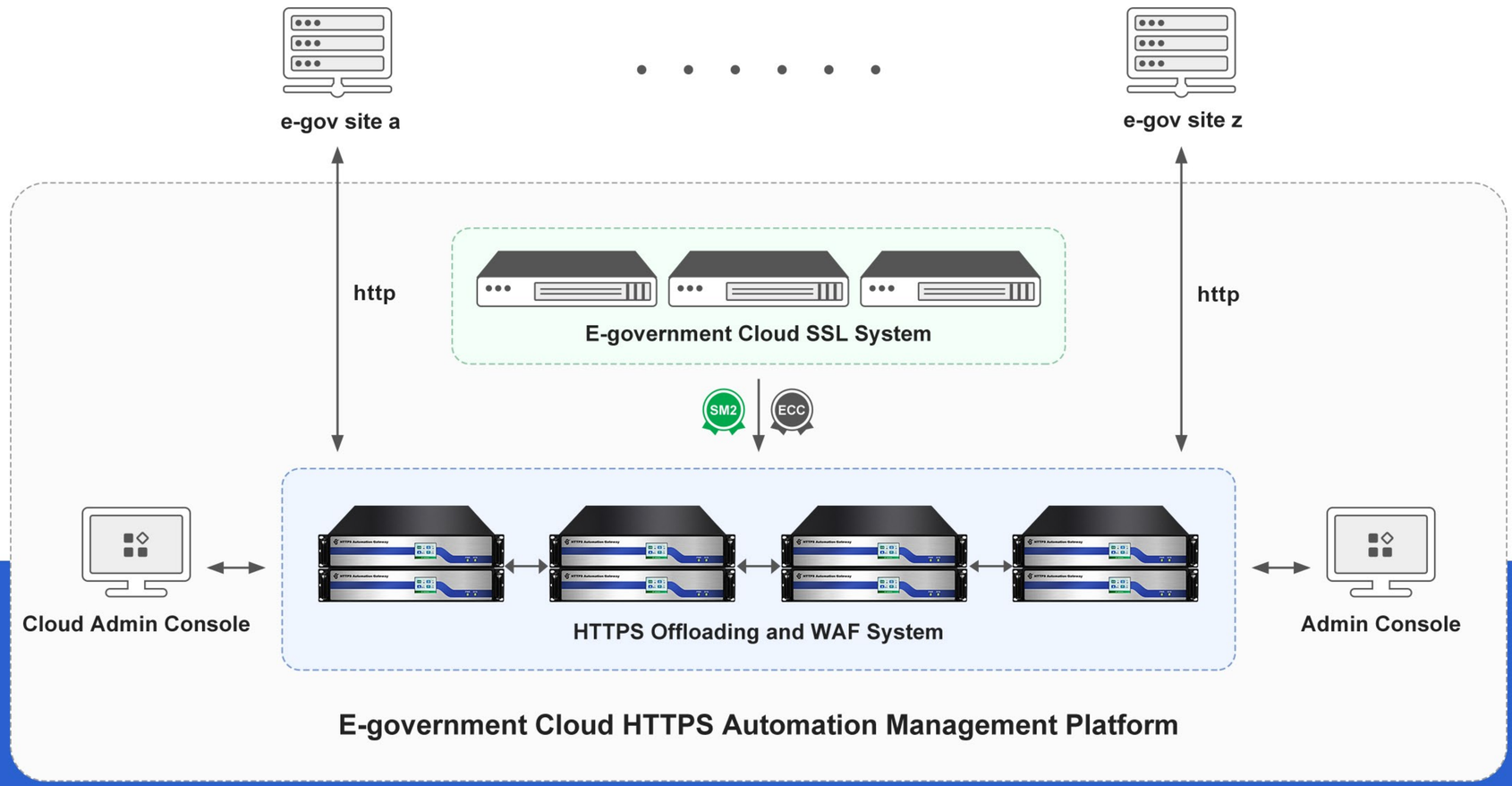
ZoTrus HTTPS Automation System is a system that integrates Linux operating system (Ubuntu, Kylin OS and UOS optional), Tengine Web server, Tongsuo SSL, ZoTrus HTTPS Automation Gateway core system, which can be directly installed on the bare metal of the server and is dedicated to realizing SM2 HTTPS automation. After the system is installed, the user only needs to log in to the web management interface, configure the website domain name to realize the automatic application and deployment of the dual-algorithm SSL certificate, and support the automatic deployment of the dual-algorithm SSL certificate for 5 years of uninterrupted service of 255 websites by default, and automatically realize the HTTPS encryption of the adaptive algorithm, and the browsers that support the SM2 algorithm such as ZT Browser preferentially use the SM2 algorithm to achieve SM2 HTTPS encryption, and the browsers that do not support SM2 algorithm use the ECC algorithm to achieve HTTPS encryption。

ZoTrus HTTPS Automation System has all the functions of the ZoTrus HTTPS Automation Gateway, binds the physical server and user account, and it is very suitable for customers with their own server hardware, such as e-government cloud platform, commercial public cloud platform, enterprise private cloud platform, etc., and makes full use of the existing idle servers to provide HTTPS Automation service and WAF protection service for various web systems.

5. Optional: Local deployment of Cloud SSL System



By default, the HTTPS 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 HTTPS Automation Gateway global exclusive innovation to achieve zero change of the original Web server to realize automatic https encryption, WAF protection service, 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 HTTPS Automation Gateway is plug-and-play, deployed on the front end of the website server, 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, 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 HTTPS Automation Gateway is the first choice and must for the https encryption, WAF protection and system security upgrade from http to https.

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