ZoTrus®

Intranet Edition

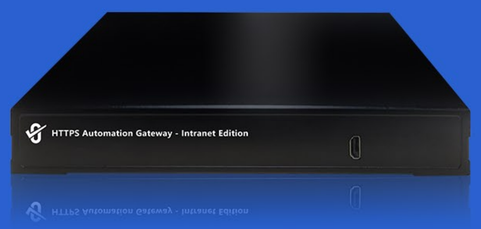
ZoTrus HTTPS Automation Gateway

Intranet SSL certificate automation management to realize https encryption for Intranet Web system

https://www.zotrus.com

1 Product Introduction

ZoTrus HTTPS Automation Gateway (abbreviated as: ZoTrus Gateway) is an innovative product that has passed the China Commercial Cryptography Product Certification and is used for zero-reconstruction automation of Internet Web systems to achieve HTTPS encryption. Since this Gateway needs to connect to ZoTrus Cloud SSL Service System to automatically configure SSL certificates for user websites, it is only suitable for providing HTTPS automation services for Internet websites and Web systems, and it does not support intranet deployment that cannot connect to the Internet. However, intranet traffic encryption also requires automatic SSL certificate management. For this reason, ZoTrus Technology has developed a special intranet edition suitable for intranet HTTPS automation based on the ZoTrus HTTPS Automation Gateway (Internet Edition). This is the ZoTrus HTTPS Automation Gateway (Intranet Edition).



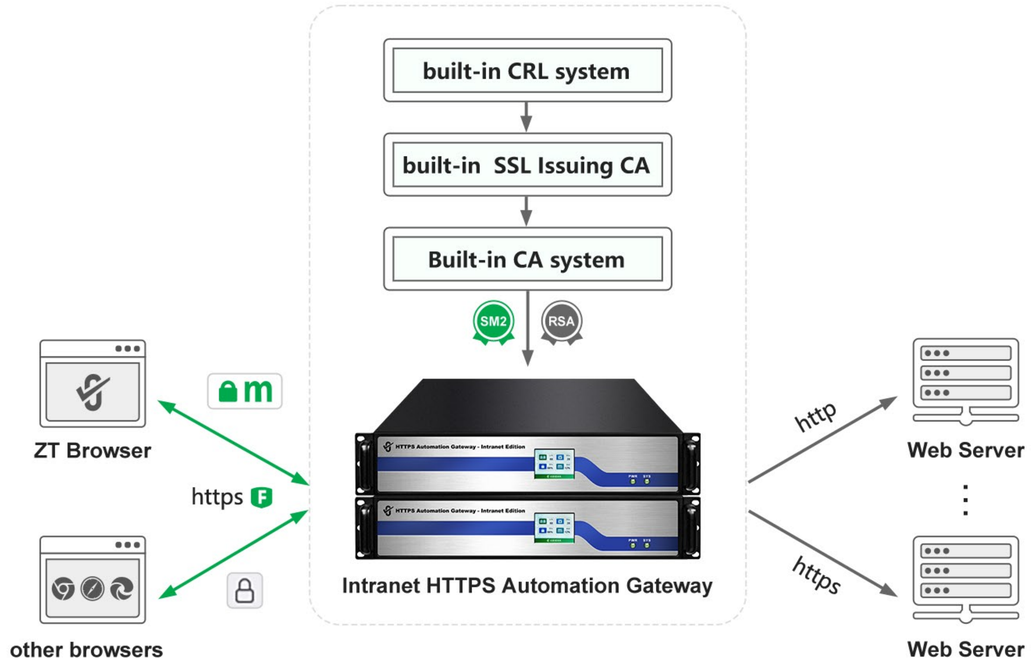
ZOTRUS

ZoTrus HTTPS Automation Gateway (Intranet Edition) (abbreviated as: ZoTrus Intranet Gateway, or ZoTrus Intranet HTTPS Automation Gateway) is an innovative product that automates the implementation of HTTPS encryption to ensure the security of HTTP traffic in intranet Web systems. Like the core functions of the Internet Edition Gateway, it also automatically configures dual-algorithm and dual intranet SSL certificates for intranet Web systems. The difference is that the automatic configuration of the intranet SSL certificate issued by the built-in CA system supports intranet IP addresses, internal domain names, and internal host names, and it also supports public domain names. ZT Browser trusts the automatically configured intranet SSL certificates and gives priority to the use of SM2 algorithms to implement HTTPS encryption, to ensure the security of confidential information in the intranet. ZoTrus Intranet Gateway enables the intranet Web system to implement HTTPS encryption automatically without any modification.

2

Main Functions

The biggest difference from the ZoTrus Gateway is that the Intranet HTTPS Automation Gateway has a built-in CA system and a built-in dual SSL Issuing CA in the built-in HSM card. One is the SM2 SSL intermediate root key and its certificate used to issue the Intranet SM2 SSL certificates, and the other is the RSA SSL intermediate root key and its certificate used to issue the Intranet RSA SSL certificates. This allows the built-in CA system of ZoTrus Intranet Gateway to automatically issue dual-algorithm Intranet SSL certificates for user websites locally, which solves the problem that the Intranet cannot connect to ZoTrus Cloud SSL System to obtain the dual algorithm SSL certificates. And, the Intranet Gateway has a built-in CRL system, which can be used to revoke the Intranet SSL certificate and for browsers to query the certificate revocation information, providing the same certificate revocation service for the public trusted SSL certificate for Intranet users. It is recommended to deploy two Gateways by default, with hot standby for each other, and load balancing between the two Gateways when available, otherwise a single machine can stand alone.



The core function of the ZoTrus Intranet Gateway is to eliminate the need to modify the original intranet Web server. There is no need to install an SSL certificate on the server, nor is there a need to upgrade the server software to support the SM2 algorithm. You only need to deploy the Intranet Gateway in front of the original server to automatically implement HTTPS encryption, and it provides HTTPS automation services for intranet Web applications 24 hours a day, 365 days a year. The completely free SM2 browser – ZT Browser preferentially uses the SM2 algorithm to implement the HTTPS encryption. Other browsers that do not support the SM2 algorithm use the RSA algorithm to implement HTTPS encryption.

The SSL certificates for HTTPS encryption are automatically issued by Gateway's built-in CA system. The RSA algorithm SSL certificate is trusted by ZT Browser. After installing ZT Browser, it will also be automatically trusted by Google Chrome and Microsoft Edge. It is issued by a user-specific RSA algorithm intermediate root certificate customized for users. The root CA certificate - AAA Intranet RSA Root is an RSA algorithm root certificate trusted by ZT Browser and used to issue intranet SSL certificates. The automatically configured RSA algorithm SSL certificate is an intranet OV SSL certificate. The O field of each SSL certificate is fixed to the user organization name, the CN field is fixed to the user's public domain name, and the SAN field is the intranet IP address, host name, public domain name, etc. set by the user.

The SM2 algorithm SSL certificate automatically configured by ZoTrus Intranet Gateway is trusted by the ZT Browser and is issued by a user-specific SM2 algorithm intermediate root certificate customized for the user. The root CA certificate -AAA Intranet SM2 Root is an SM2 algorithm root certificate trusted by ZT Browser and used to issue intranet SSL certificates. The automatically configured SM2 algorithm SSL certificate is an intranet OV SSL certificate. The O field of each SSL certificate is fixed to the user organization name, the CN field is fixed to the user's public domain name, and the SAN field is the intranet IP address, host name, public domain name, etc. set by the user. The dual OV SSL certificates automatically configured by ZoTrus Intranet Gateway do not support certificate transparency because it cannot connect to the Internet to obtain the signed certificate timestamp data.

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ZoTrus Intranet RSA OV SSL ...
Valid from	Monday, May 13, 2024 4:02:4...
Valid to	Monday, August 13, 2024 4:0 ...
Subject	iovssldemo.zotrus.com, ZoTru...
Public key	RSA (2048 Bits)
Public key parameters	05 00

CN = iovssldemo.zotrus.com
O = ZoTrus Technology Limited
L = Shenzhen
S = Guangdong
C = CN

DNS Name=iovssldemo.zotrus.com
IP Address=192.168.2.188
DNS Name=demo.zotrus

Field	Value
Signature algorithm	SM3WithSM2
Signature hash algorithm	SM3
Issuer	ZoTrus Intranet SM2 OV SSL CA, ...
Valid from	Monday, May 13, 2024 4:03:02 PM
Valid to	Monday, August 13, 2024 4:03:02 ...
Subject	iovssldemo.zotrus.com, ZoTrus T...
Public key	ECC (256 Bits)
Public key parameters	SM2

CN = iovssldemo.zotrus.com
O = ZoTrus Technology Limited
L = Shenzhen
S = Guangdong
C = CN

DNS Name=iovssldemo.zotrus.com
IP Address=192.168.2.188
DNS Name=demo.zotrus

ZoTrus Intranet Gateway is configured with the 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.

There are 12 main functional modules of ZoTrus Intranet HTTPS Automation Gateway:

01

Zero reconstruction for https encryption

The original 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 Intranet SSL certificates (RSA/SM2) are automatically configured for the Intranet website 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 internal 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.

There are 12 main functional modules of ZoTrus Intranet HTTPS Automation Gateway:

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 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.

10

Security Authentication

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

3 Performance Indicators

ZoTrus Intranet HTTPS Automation Gateway provides an efficient, secure, transparent, easy-to-deploy, zero-modification, fully automatic innovative solution to implement HTTPs encryption for intranet Web system. It can effectively expand the bandwidth of network devices and servers, increase throughput, enhance network data processing capabilities, improve network flexibility and availability, and enhance the user experience of users visiting internal websites.

ZoTrus Intranet 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 Intranet Gateway supports automatic configuration of up to 510 RSA Intranet SSL certificates and supports up to 510 pairs of SM2 Intranet SSL certificates (one signing certificate and one encrypting certificate). The standard dual-algorithm dual-SSL certificate configuration supports automatic configuration of dual SSL certificates for 510 intranet website domain names and intranet IP addresses, and it implements dual-algorithm adaptive https encryption. In fact, the number of websites that can implement https encryption is limited by the number of connections, throughput, and concurrency supported by the Gateway hardware.

Each ZoTrus Intranet Gateway has a 5-year warranty period, and RSA OV SSL certificates and SM2 OV SSL certificates are automatically configured for up to 510 Intranet website domain names and Intranet IP addresses for free within 5 years. According to the price of the double SSL certificate of the CerSign Intranet OV SSL certificate (1800 yuan/year), the value of the automatically configured SSL certificate alone is as high as 4.59 million yuan (=5* 510 * 1800, equal to US$632K), the world's exclusive super-value https encryption automation solution for Intranet Web system.

ZoTrus Intranet Gateway currently provides 3 different specifications of products, which can be used for government extranets, government intranets and internal Web application systems of large and medium-sized enterprise intranets to automatically realize HTTP encryption, especially to realize the application requirements of SM2 HTTP encryption without re-construction. The performance index parameters of various models are shown in the following table. For users with different index requirements, products can be customized to meet the requirements.

ZOTRUS

Product Model	MG-3-1	MG-3-8	MG-3-9
CPU Brand	Intel Atom	Intel Xeon (dual)	Hygon 5380
Number of Websites	100	200 / 510	200 / 510
Incl RSA SSL Certificate Qty	100	200 / 510	200 / 510
Incl SM2 SSL Certificate Qty	100	200 / 510	200 / 510
SSL Certificate Service Life	5 years	5 years	5 years
Validity Period of SSL Issuing CA Certificate	10 years	10 years	10 years
RSA SSL Certificate Type	OV SSL Certificate	OV SSL Certificate	OV SSL Certificate
SM2 SSL Certificate Type	OV SSL Certificate	OV SSL Certificate	OV SSL Certificate
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
SM2 HTTPS throughput	800M bps	9 Gbps	9 Gbps
RSA HTTPS throughput	800M bps	9 Gbps	9 Gbps
SM2 SSL Requests	30K / second	120K / second	60K / second
RSA SSL Requests	40K / second	130K / second	90K / second
Max concurrent	250K	1.5 million	1 million
WAF Function	built-in	built-in	built-in
Customize WAF Rule	support	support	support
Network Interface	6 Gigabit Ethernet ports	6 Gigabit Ethernet ports + 4 10G optical ports	6 Gigabit Ethernet ports + 4 10G optical ports
Chassis	155*240*40 (mm)	2U	2U
Power Supply	Single supply 60W	Dual supply 550W	Dual supply 550W
SSL Certificate value (5 years)	900K RMB Yuan	1.8M / 4.59M RMB Yuan	1.8M / 4.59M RMB Yuan
Save labor costs (5 years)	600K RMB Yuan	1.2M / 3M RMB Yuan	1.2M / 3M RMB Yuan
Target customers	SME Colleges and Universities	Large enterprises Government Financial	Government Financial

ZOTRUS

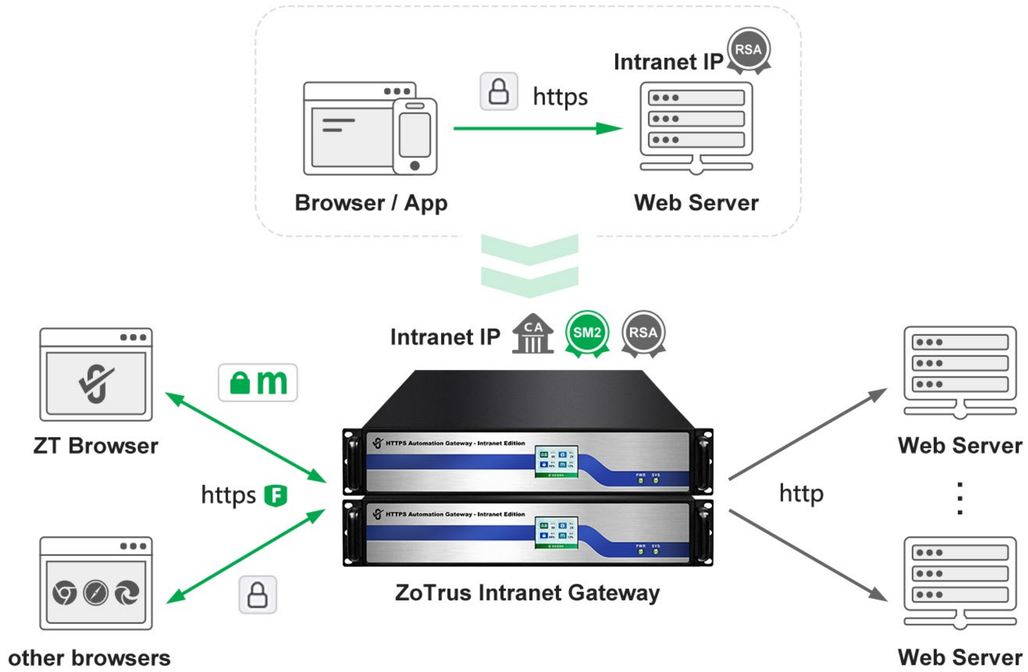
4

Deployment Solutions

https://www.zotrus.com

ZoTrus Intranet HTTPS Automation Gateway supports a variety of network deployment methods and supports cluster deployment of multiple devices. In order to ensure the high availability of the Gateway, dual-machine deployment is strongly recommended to ensure 24*365 days of uninterrupted provision of HTTPS automation and WAF protection for the Intranet Web servers.

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



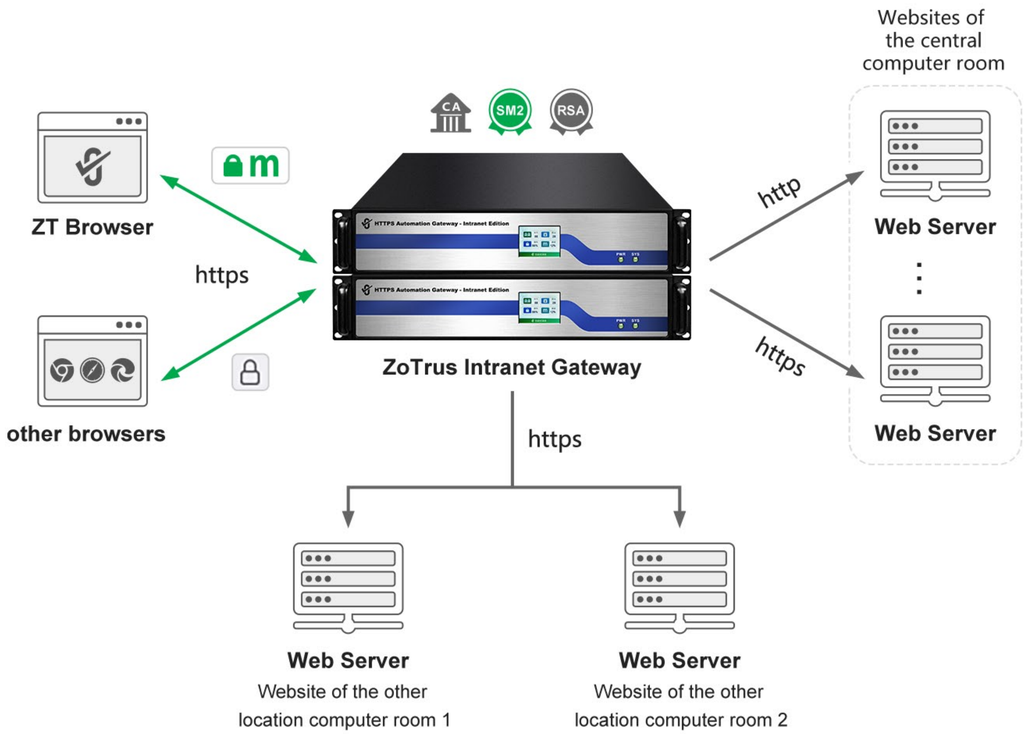
The traditional way to implement HTTPS encryption in the intranet is to issue self-signed SSL certificates and manually deploy them on the intranet Web server to implement HTTPS encryption. In addition, all intranet user computers need to manually install the root CA certificate that issues the self-signed SSL certificate. This is a very time-consuming and laborious task for customers who have multiple intranet Web systems that need to deploy SSL certificates. Customers can purchase a ZoTrus Intranet Gateway and deploy it in front of the Web server. Two gateways can provide HTTPS encryption automation services for up to 510 internal Web site systems. More web systems require the purchase of more gateways.

This deployment method transforms the original Web server that could only use the plaintext HTTP insecure protocol into a secure HTTPS encrypted access Web server, truly protecting the confidential information transmission security of the internal management information system, and transferring all the HTTPS encryption and decryption workloads that the original Web server was responsible for to the gateway, saving 20%-30% of the computing power for the Web server, allowing the Web server to better provide computing power for the internal business system.

This deployment method is suitable for customers who have their own equipment room and their own Web servers. They need to deploy gateway devices in the equipment room. This method will change the IP address of the original Web server, reallocate the intranet IP address to the original Web server, and configure the original intranet IP address for the gateway. 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 dual-machine hot standby mode. The dual gateways use the master-master mode, that is, Active-Active mode. Both gateway devices act as hosts and process business traffic at the same time, and also serve as backup machines for each other. The two machines share business 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, thereby ensuring the continuous and reliable operation of the business system. ZoTrus Intranet Gateway is guaranteed for 5 years. If there is a fault within 5 years, it will be replaced free of charge, ensuring uninterrupted HTTPS encryption automation services and WAF protection services within 5 years.

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

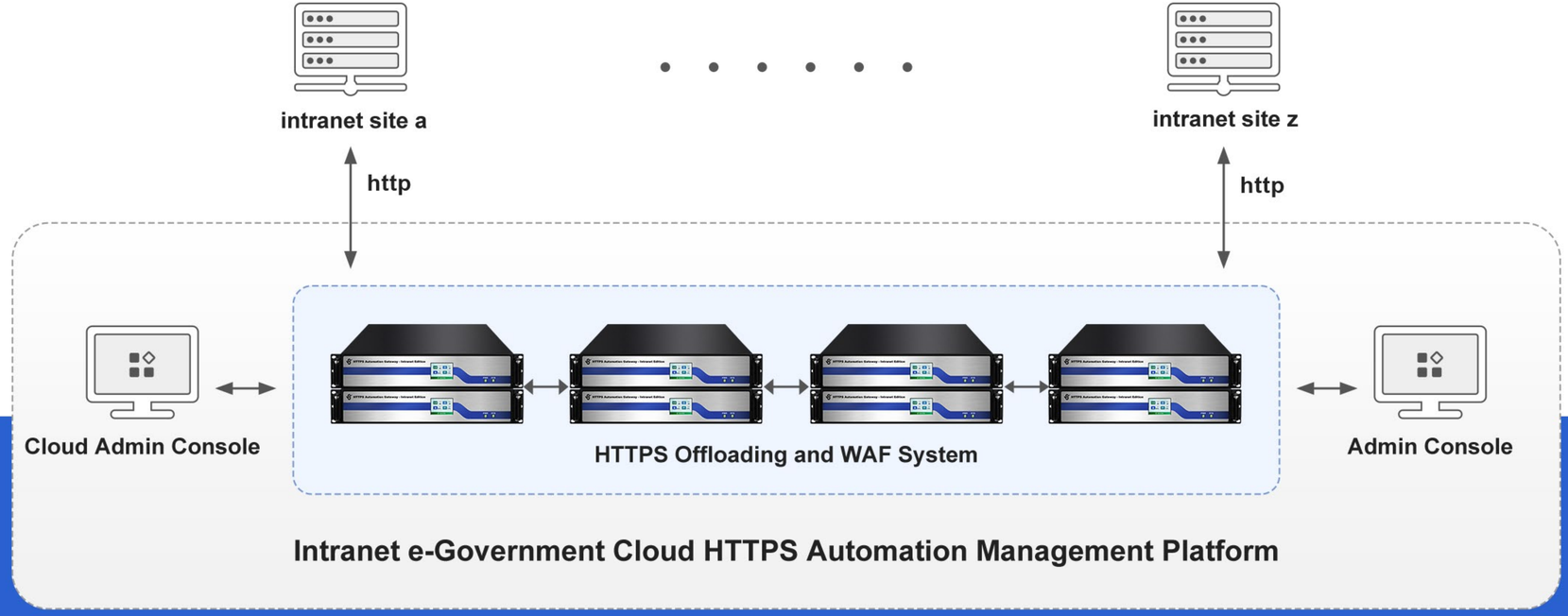


For customers who not only need to implement HTTPS automation services for local internal web servers, but also need HTTPS automation services for multiple website systems of internal web servers in foreign branches, ZoTrus Intranet Gateway supports both local forwarding mode and remote back-to-source mode. Regardless of which equipment room the internal web server (website) is in, as long as the gateway can be accessed through the intranet, these websites can be provided with HTTPS automation services and WAF protection services by the Gateway. Dual gateways provide HTTPS automation services for up to 510 website systems, and more website systems require the purchase of more gateways.

In order to ensure the data security of the internal web system that is not in the central computer room, the back-to-source connection from the gateway to the remote server must use HTTPS encryption to achieve full-link encryption. ZoTrus Technology provides a self-signed back-to-source dedicated SSL certificate with a validity period of 5 years for free for remote websites. Once the certificate is installed, it can be used for HTTPS encrypted back-to-source.

3. Cluster deployment solution for automatic management of government intranet platforms

For the government extranet and intranet platforms, there are thousands or even tens of thousands of website systems that need to complete the HTTPS encryption transformation. The only solution is automation. It is necessary to deploy multiple ZoTrus Intranet Gateways to form a cluster array - HTTPS offload system and WAF system. Multiple Intranet Gateways work together to share business traffic and serve as hot standby devices for each other. When a gateway fails, the services running on it will be taken over by other gateways to ensure that business scheduling is fully and timely responded. The cluster mode is suitable for the deployment requirements of redundant network environments that emphasize extremely high-performance throughput.



5

Summary

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

ZoTrus HTTPS Automation Gateway (Intranet Edition) is the world's exclusive innovation that realizes zero change of the original intranet Web server to fully automatically implement HTTPs encryption and WAF protection, dual algorithm (RSA/SM2) adaptive HTTPs encryption , setup the intranet website domain name and/or intranet IP address to immediately activate HTTPs encryption and https acceleration services, WAF protection, TCP/DTLS secure delivery, dual SSL certificates automatically ready, SM2 compliance, compatible with RSA, high-speed dynamic caching and compression, connection multiplexing, session persistence and load balancing and many other optimization functions, while ensuring high performance and efficiency, providing the industry's highest performance-price ratio.

ZoTrus HTTPS Automation Gateway (Intranet Edition) is plug-and-play and is deployed at the front end of the intranet Web server. The original intranet Web server can be seamlessly upgraded from http to https without any reconstruction. It supports SM2 algorithm https encryption that meets cryptography compliance. It also supports RSA algorithm https encryption to be compatible with browsers that do not support SM2 algorithms. Its powerful https acceleration unloading forwarding function provides additional performance enhancement support for intranet Web servers. Not only does it not increase the burden of https encryption and decryption at all, but also it enhances the ability to respond to external situations and process user requests. The seamless switching of ZoTrus Intranet Gateway with zero transformation, zero maintenance, and zero impact is the first choice and must-have for https encryption transformation and internal Web system security upgrade from http to https.