零信®
ZoTrus

公网版

零信国密HTTPS加密自动化网关

零改造实现公网HTTPS国密改造

https://www.zotrus.com

1 产品简介

零信国密HTTPS加密自动化网关（简称：零信网关）是一个通过商密产品认证的采用高性能密码卡打造的高端高性能网站安全硬件密码设备，是一个集https加密加速、https卸载转发、国密算法模块、SSL证书自动化、负载均衡等多项功能于一体的专用于https加速和卸载的硬件密码设备，内置专业级高性能硬件密码卡实现高速密码运算和网络包转发，并且对内置操作系统、网络协议、SSL/TLS协议、ECC算法和SM2算法都进行了专业的深度优化，实现了业界领先的极致性能：HTTPS新建连接可达到6万次/秒、HTTPS吞吐量可达到17Gbps、HTTPS并发量可达到300万个连接。


商用密码产品认证证书

证书编号：GM004410620230847

委托人名称及所在地

生产者（制造商）名称及所在地

生产企业名称及所在地

产品名称和型号、版本

国密HTTPS加密自动化网关

SM2-HTTPS-Auto-Gateway-ARG V1.0

产品标准和技术要求

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

上述产品经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 有效期至：2028 年 9 月 26 日

证书有效期内本证书的有效性信息发证机构应当予以公开

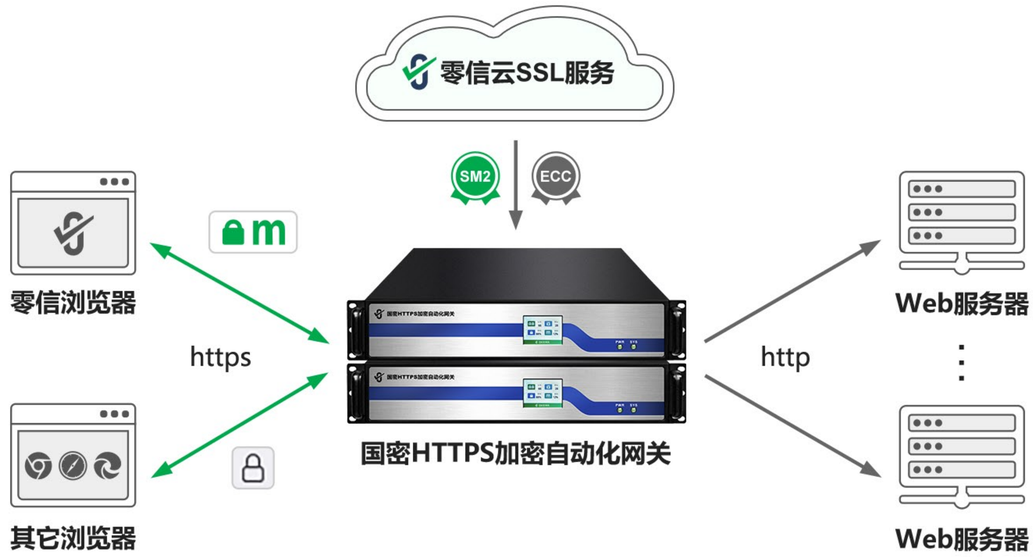
牛路云

国家密码管理局商用密码检测中心

零信国密HTTPS加密自动化网关最大的特点和特色是零申请SSL证书、零安装SSL证书、自动化实现国密HTTPS加密，自适应加密算法，支持国密算法和国密证书透明的浏览器采用SM2算法实现国密https加密，不支持国密算法和国密证书透明的浏览器采用ECC算法实现https加密。这是一个端云一体的创新解决方案，国密HTTPS加密自动化网关内置国密ACME客户端，自动对接零信云SSL系统完成自动化双SSL证书申请、部署和续期，确保业务系统零改造实现https加密，不间断地自动化为多达255个不同域名的业务系统提供自动化https加密服务和WAF防护服务。

2 主要功能

零信国密HTTPS加密自动化网关核心功能是原Web服务器零改造，无需在Web服务器上安装SSL证书，无需在Web服务器上安装ACME客户端软件，也无需升级改造Web服务器软件支持国密算法，只需在原服务器之前部署HTTPS加密自动化网关，即可自动化实现https加密，24小时365天不间断的提供https加密服务和WAF防护服务。推荐默认双机部署，互为热备，能时双机负载均衡，否时单机独当一面。支持国密算法和国密证书透明的完全免费的国密浏览器—零信浏览器优先采用国密算法实现国密https加密，其他不支持国密算法和国密证书透明的浏览器则采用ECC算法实现https加密。



加密所需的双算法双SSL证书由HTTPS加密自动化网关自动对接零信云SSL系统自动化完成双SSL证书的申请、域名验证、获取证书、安装证书和启用证书。自动配置的ECC SSL证书全球信任，支持国际证书透明安全，由零信自有品牌中级根证书ZoTrus ECC DV SSL CA签发，顶级根证书是全球最老的ECC算法根证书Sectigo ECC，全链采用ECC算法，加密速度比RSA算法快18倍，让用户访问网站更快。自动配置的国密SM2 OV SSL证书国密合规，支持所有国密浏览器，是支持国密证书透明安全的国密SSL证书，由零信自有品牌中级根证书SM2 SSL Pro CA签发，顶级根证书是拥有国密局和工信部CA许可证的贵州CA国密根证书Guizhou SM2 CA，全链采用SM2算法，加密速度比RSA算法快20倍，让用户访问网站更快。

零信国密HTTPS加密自动化网关自动配置的双SSL证书有效期都是90天，提前满足即将实施的90天证书政策。如下左图为网关默认配置的90天有效期的国密OV SSL证书，右图为网关默认配置的90天有效期的国际DV SSL证书，90天证书的自动化部署将大大提升HTTPS加密服务的安全性和敏捷性。同时，双SSL证书都是采用椭圆曲线算法，证书链文件最小，省机房流量和用户手机流量、省机房耗电量和用户手机耗电量，更环保。

零信国密HTTPS加密自动化网关默认内置WAF防护模块，此模块基于开源ModSecurity系统开发，支持常用的Web应用防火墙功能，如：阻止SQL注入、阻止跨站脚本攻击(XSS)、阻止利用本地文件包含漏洞进行攻击、阻止利用远程文件(包含漏洞)进行攻击、阻止利用远程命令执行漏洞进行攻击、阻止PHP代码注入、阻止违反HTTP协议的恶意访问、阻止利用远程代理感染漏洞进行攻击、阻止利用Shellshock漏洞进行攻击、阻止利用Session会话ID不变的漏洞进行攻击、阻止恶意扫描网站、阻止源代码或错误信息泄露、蜜罐项目黑名单、根据判断IP地址归属地来进行IP阻断等等。如果用户已经购买了WAF设备，则只需在WAF设备之前部署国密WAF加密自动化网关即可，WAF设备只需负责解析明文http内容做出相应的安全防护，无需向CA申请SSL证书部署在WAF设备上。

零信国密HTTPS加密自动化网关也是一个国密安全认证网关，支持CA签发的USB Key国密证书使用双向认证(SKF标准)，配合零信浏览器的双向认证支持功能，用户无需任何额外开发，只需在网关设置网站启用国密HTTPS加密自动化服务的同时选择启用双向认证即可，可设置多个客户端证书签发CA，并已默认预置国家根证书。同时支持RSA算法软证书和USB Key硬证书的双向认证。

零信国密HTTPS加密自动化网关主要十大功能：

01

零改造https加密

原Web服务器无需安装SSL证书，无需安装国密ACME客户端软件，零改造实现国密https加密，自适应加密算法，支持RSA/ECC/SM2算法https加密。

02

自动配置SSL证书

默认免费自动为用户设置的网站域名配置双SSL证书(ECC/SM2)，用户无需向CA申请SSL证书，无需安装和配置SSL证书，国际SSL证书全球信任，国密SSL证书国密合规。

03

高性能https卸载

完全接管和承担原服务器的SSL加解密功能，大大减轻原服务器的性能压力，让原服务器专用于业务系统，大大提升客户端访问响应速度。

04

用户端连接复用

采用动态连接池技术和复用技术，捆绑海量用户端连接请求，节省大部分服务器TCP连接并持续保持，显著减少了原服务器需要处理的用户端连接数(最高可减少90%)，加快连接处理速度，提高原服务器业务处理能力。

05

Web数据传输压缩

使用标准GZIP或Deflate压缩算法来压缩HTTP流量，降低带宽消耗和降低成本，提升服务器响应与带宽效率，缩短最终用户访问和下载时间，改进用户体验和提升满意度。

零信国密HTTPS加密自动化网关主要十大功能：

06

反向代理缓存

采用内存缓存和包存储结构的方式短时间缓存网站内容，降低用户访问对原服务器的负载压力，提高原服务器的处理能力和用户的访问体验。

07

会话保持机制

基于Cookie和源IP的会话保持机制，可以为用户选择曾连接的特定服务器，实现无缝地处理用户请求。同时可以减少新建连接的数量，有效减小相关设备和服务器的系统开销。

08

多算法负载均衡

零信网关支持多种负载均衡算法：轮询、加权轮询、最小连接数和IP Hash，用户可根据业务需要选择合适的负载均衡模式，以提供更高的服务性能、可用性和扩展性。

09

WAF模块（零信网关WAF）

基于业界领先的开源ModSecurity系统开发和深度优化，支持常用的Web应用防火墙功能，为https卸载后的Web流量提供安全清洗保护，仅将正常安全的流量转发到后面的内部Web服务器。

10

安全双向认证

集成安全双向认证功能，支持CA签发的USB Key国密证书使用双向认证(SKF标准)，无缝支持零信浏览器的双向认证功能，同时支持SM2/RSA算法客户端软证书实现双向安全认证。

3 性能指标

零信国密HTTPS加密自动化网关提供了一种高效、安全、透明、易部署、零改造、全自动的创新方案实现https加密和WAF防护，能够有效扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性、提升用户访问网站的用户体验。

零信国密HTTPS加密自动化网关提供全自主可控软硬件一体化产品，包括：完全自主知识产权SSL安全网关软件系统、通过商用密码产品认证的国产密码算法硬件加速卡、采用自主可控国产操作系统、支持海光/龙芯/飞腾等国产CPU自主可控芯片、采用配套国产自主可控主板、支持国产自主可控网卡芯片等等。全自主可控软硬件一体化国密HTTPS加密自动化网关能够满足各种对信息安全管控要求极高的行业应用需求。

每台零信国密HTTPS加密自动化网关最多支持自动配置255张ECC SSL证书(单证书)，同时最多支持255对国密SSL证书(一张签名证书和一张加密证书)，标准的双算法双SSL证书配置支持为255个网站域名自动配置双SSL证书，实现双算法自适应https加密。实际上能为多少个网站实现https加密受限于网关硬件所支持的新建连接数、吞吐量和并发量。

每台零信国密HTTPS加密自动化网关保用期为5年，5年内免费为最多不超过255个网站域名自动配置全球信任的ECC DV SSL证书和国密合规的SM2 OV SSL证书。按照证签OV SSL证书精简版双SSL证书的价格(4888元/年)计算，仅自动化配置的双SSL证书价值高达623万元(=5*255*4888)，全球独家提供超值https加密自动化解决方案!

零信国密HTTPS加密自动化网关目前提供4种不同规格的产品，可分别用于云平台高性能数据中心和大中型企业Web服务器自动化实现https加密、特别是零改造实现国密https加密的应用需求。各种型号的产品性能指标参数如下表所示，对于有不同指标要求的用户，可以定制产品满足要求。

ZOTRUS

产品型号	MG-1-1	MG-1-8	MG-1-9
CPU品牌	英特尔凌动	英特尔至强(双)	海光5380
支持网站数量	20个	100个 / 255个	100个 / 255个
含ECC SSL证书数量	20张	100张 / 255张	100张 / 255张
含SM2 SSL证书数量	20对	100对 / 255对	100对 / 255对
双SSL证书服务年限	5年	5年	5年
ECC SSL证书类型	DV SSL证书	DV SSL证书	DV SSL证书
SM2 SSL证书类型	OV SSL证书	OV SSL证书	OV SSL证书
每个网站独立密钥/证书	是	是	是
双SSL证书有效期	90天	90天	90天
双SSL证书更新周期	每80天	每80天	每80天
网站可信认证类型	EV认证	EV认证	EV认证
国密https加密吞吐	800Mbps	9 Gbps	9 Gbps
国际https加密吞吐	800Mbps	9 Gbps	9 Gbps
国密SSL请求数	3万/秒	12万/秒	6万/秒
国际SSL请求数	4万/秒	13万/秒	9万/秒
最大并发连接数	25万	150万	100万
WAF防护功能	内置	内置	内置
自定义WAF防护规则	支持	支持	支持
定期升级防护规则	支持	支持	支持
网络接口	6个千兆电口	6个千兆电口+4个万兆光口	6个千兆电口+4个万兆光口
机箱	155*240*40 (mm)	2U	2U
电源	单电源60W	双电源550W	双电源550W
仅证书项价值(5年)	49万元	244万元 / 623万元	244万元 / 623万元
节省人力成本(5年)	12万元	60万元 / 150万元	60万元 / 150万元
适用对象	中小企业 大学院校	大中型企业 云平台 政府/金融机构	政务云平台 政府机构 金融机构

4

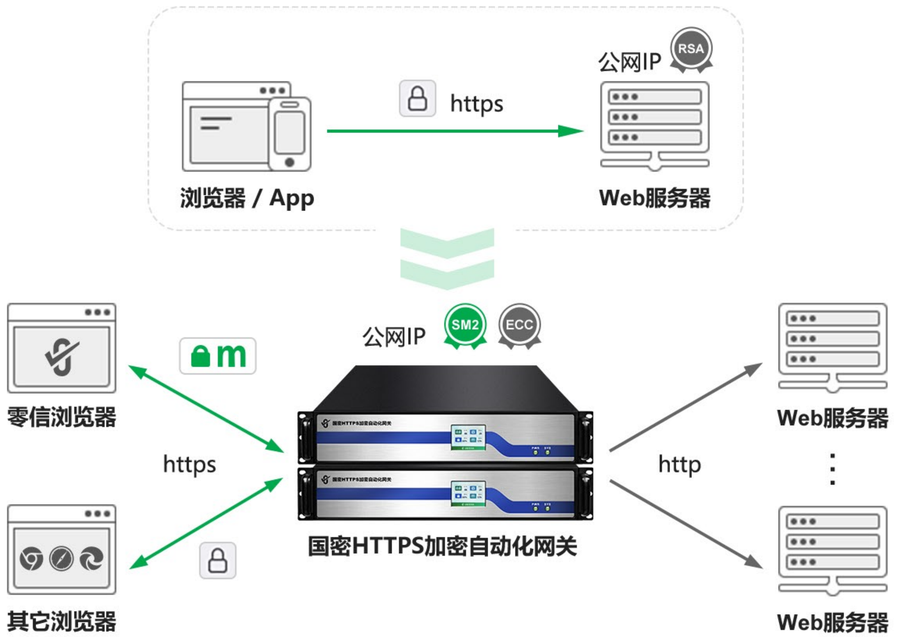
部署应用方案

ZOTRUS

https://www.zotrus.com

零信国密HTTPS加密自动化网关支持多种部署应用方式，支持多台设备集群部署。为了保证网关的高可用，强烈推荐双机部署，确保24*365天的不间断自动化提供https加密服务和WAF防护服务。

1. 为本地Web服务器(网站)提供HTTPS加密自动化服务



传统的HTTPS加密实现方式是用户向CA申请SSL证书，手动部署在Web服务器上实现HTTPS加密，对于有多个网站需要部署SSL证书的用户，这是一个非常费时费力的难事。而选购零信国密HTTPS加密自动化网关，部署在Web服务器前面，则用户无需向CA申请SSL证书，由零信网关自动化对接零信云SSL服务系统自动化为网站配置双SSL证书，自动化实现HTTPS加密和WAF防护。

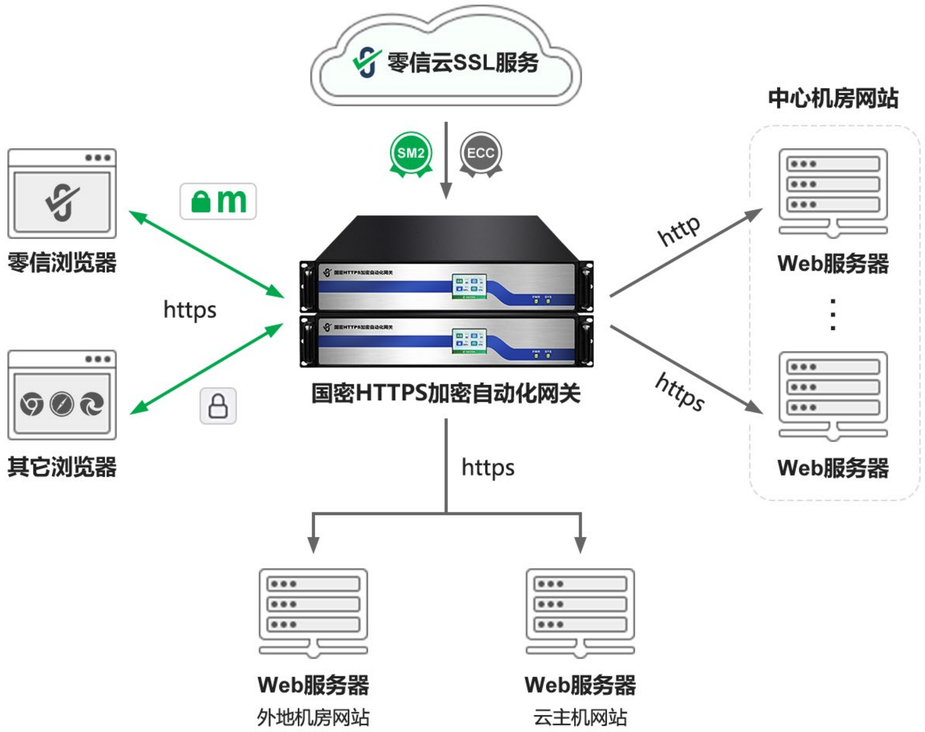
零信国密HTTPS加密自动化网关的一个网口连接到原先的公网接口，配置原先Web服务器的公网IP地址，而原先的Web服务器连接到其他网口，默认最多可以连接8台Web服务器，这些Web服务器改为配置内网IP地址。所有网络数据流量均通过HTTPS加密自动化网关进行https加速、卸载和转换处理，符合安全应用协议的数据包将根据负载均衡策略转发到对应内部Web服务器上，支持HTTP明文转发和HTTPS加密转发。

此部署方式让原先暴露在公网的Web服务器变成了内网服务器，保护了Web服务器的安全，并且把原Web服务器负责的HTTPS加解密工作负载全部移交给了网关，能节省20%-30%的算力给Web服务器，让Web服务器能更好地为业务系统提供算力。

本部署方式适用于有自己的机房和自己的Web服务器的用户，需要在机房增加部署网关设备，此方式会改变原Web服务器的IP地址，重新分配内网IP地址给原Web服务器，原公网IP地址配置给网关使用，网关支持IP V4和IP V6，原域名解析不用改变。

默认部署方式为双机热备模式，双网关采用主主模式即Active - Active模式，两台网关设备均作为主机并同时处理业务流量，同时也互为备机。双机共同承担业务流量，不浪费资源。当其中一台网关出现问题无法继续工作时，另一台网关承担起全部工作，从而保证业务系统的持续可靠运行。零信网关保用5年，5年内如有故障，免费更换，确保5年内不间断的HTTPS加密自动化服务和WAF防护服务。

2. 为不在本地的Web服务器(网站)提供HTTPS加密自动化服务



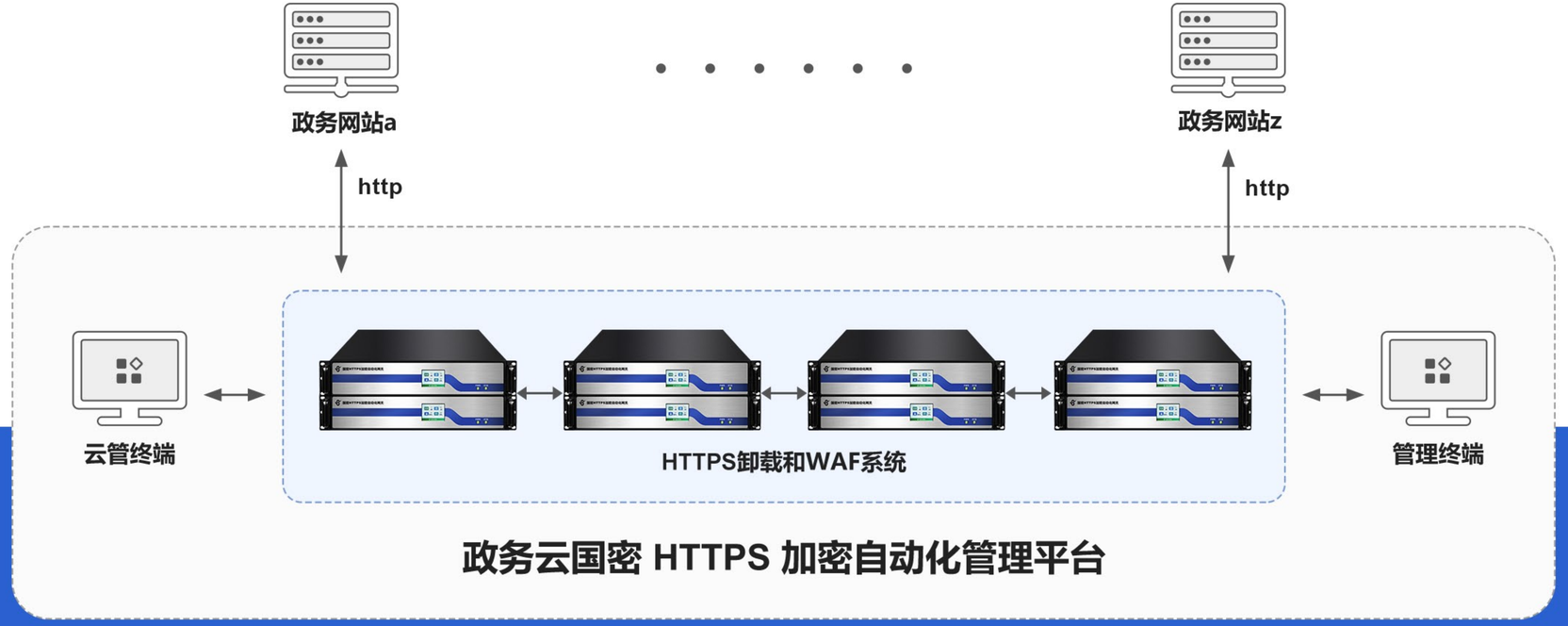
对于不仅有本地服务器需要实现HTTPS加密自动化服务，而且还有外地分支机构的Web服务器或有部署在云上的多个网站也需要HTTPS加密自动化服务的用户，零信网关同时支持本地转发模式和远程回源模式。无论Web服务器(网站)是在外地机房还是云主机，只要网关能通过公网或者内网能访问，则这些网站就是类似于CDN服务的回源源站，都可以由网关来为它们提供HTTPS加密自动化服务和WAF防护服务。双网关最多为255个网站提供HTTPS加密自动化服务和WAF防护服务，更多网站需要购置更多台网关。

为了保障不在中心机房的网站系统的数据安全，从网关到外地服务器的回源连接必须采用HTTPS加密方式，实现全链路加密。零信技术免费为回源网站提供5年有效期的自签回源专用SSL证书，原网站无需部署全球信任的有效期仅为一年的SSL证书。

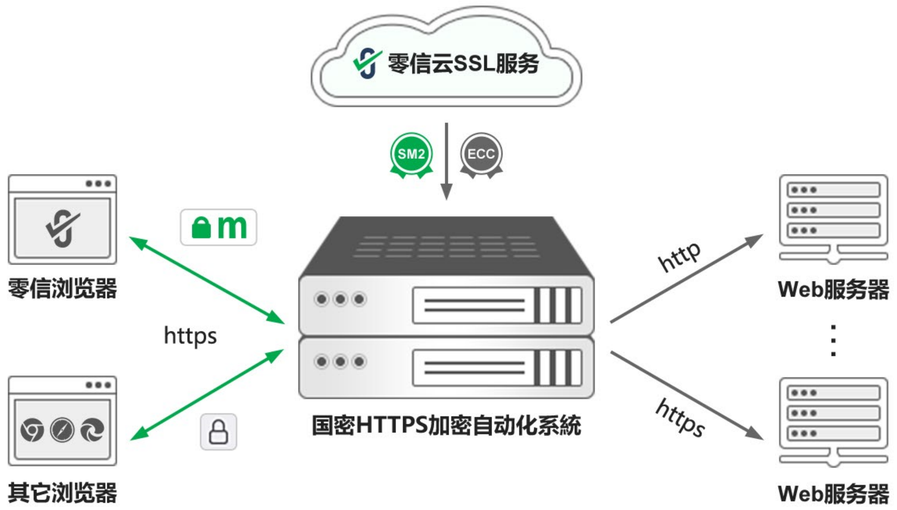
此部署方式也适用于为用户提供网站设计、虚拟主机、SSL证书销售的服务提供商，部署多台网关就可以既为自己的业务系统提供HTTPS加密自动化服务和WAF防护服务，也可以为其用户提供HTTPS加密自动化服务和WAF防护服务，而不用关心用户的网站托管在哪里，只有能HTTP或HTTPS方式访问即可。

3. 云平台国密HTTPS加密自动化管理集群部署方案

对于各种云平台，如政务云平台和公共云平台，有上万个甚至上百万个网站需要完成国密HTTPS加密改造，唯一的解决方案只有自动化才能胜任。需要部署多台国密HTTPS加密自动化网关组成集群阵列--HTTPS卸载和WAF系统，多台HTTPS加密自动化网关一起工作共同分担业务流量，同时互为热备设备。当某台网关发生故障时，运行在其上的服务会被其它网关接管，保证业务调度得到充分及时的响应。集群模式适合于强调极高性能吞吐率的冗余网络环境的部署需求。



4、可选：零信国密HTTPS加密自动化系统



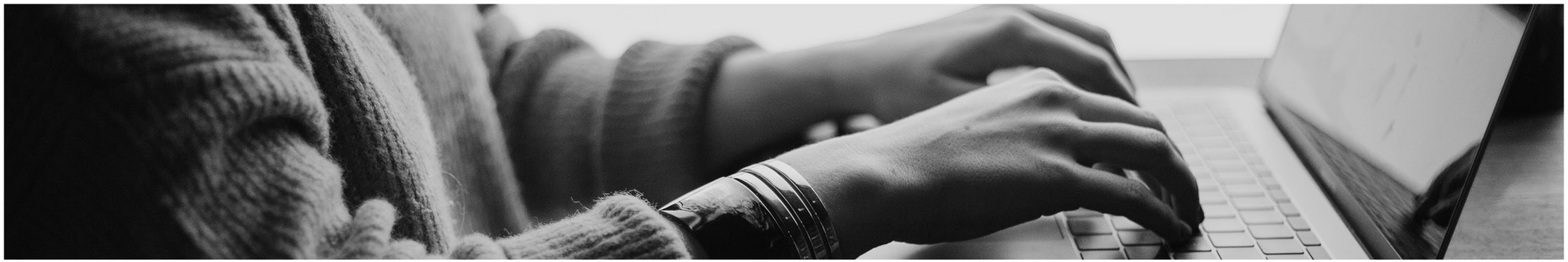
如果用户有闲置服务器，或者不方便部署零信国密HTTPS加密自动化网关硬件设备，可以选购零信国密HTTPS加密自动化系统，在自己的服务器裸机上部署网关系统，实现零信国密HTTPS加密自动化网关一样的卓越功能。

零信国密HTTPS加密自动化系统是一个集成了Linux操作系统(可选Ubuntu、麒麟OS和统信UOS)、Tengine Web服务器、铜锁SSL、零信国密ACME客户端、零信国密HTTPS加密自动化网关核心系统的、可以直接在服务器裸机上安装的、专用于实现国密HTTPS加密自动化的系统。系统安装完成后，用户只需登录Web管理界面，配置网站域名即可实现双算法SSL证书的自动化申请和部署，默认支持255个网站的5年不间断的双算法SSL证书的自动化部署，自动化实现自适应加密算法的HTTPS加密，支持国密算法的浏览器如零信浏览器优先采用国密算法实现国密HTTPS加密，不支持国密算法的浏览器则采用ECC算法实现HTTPS加密。

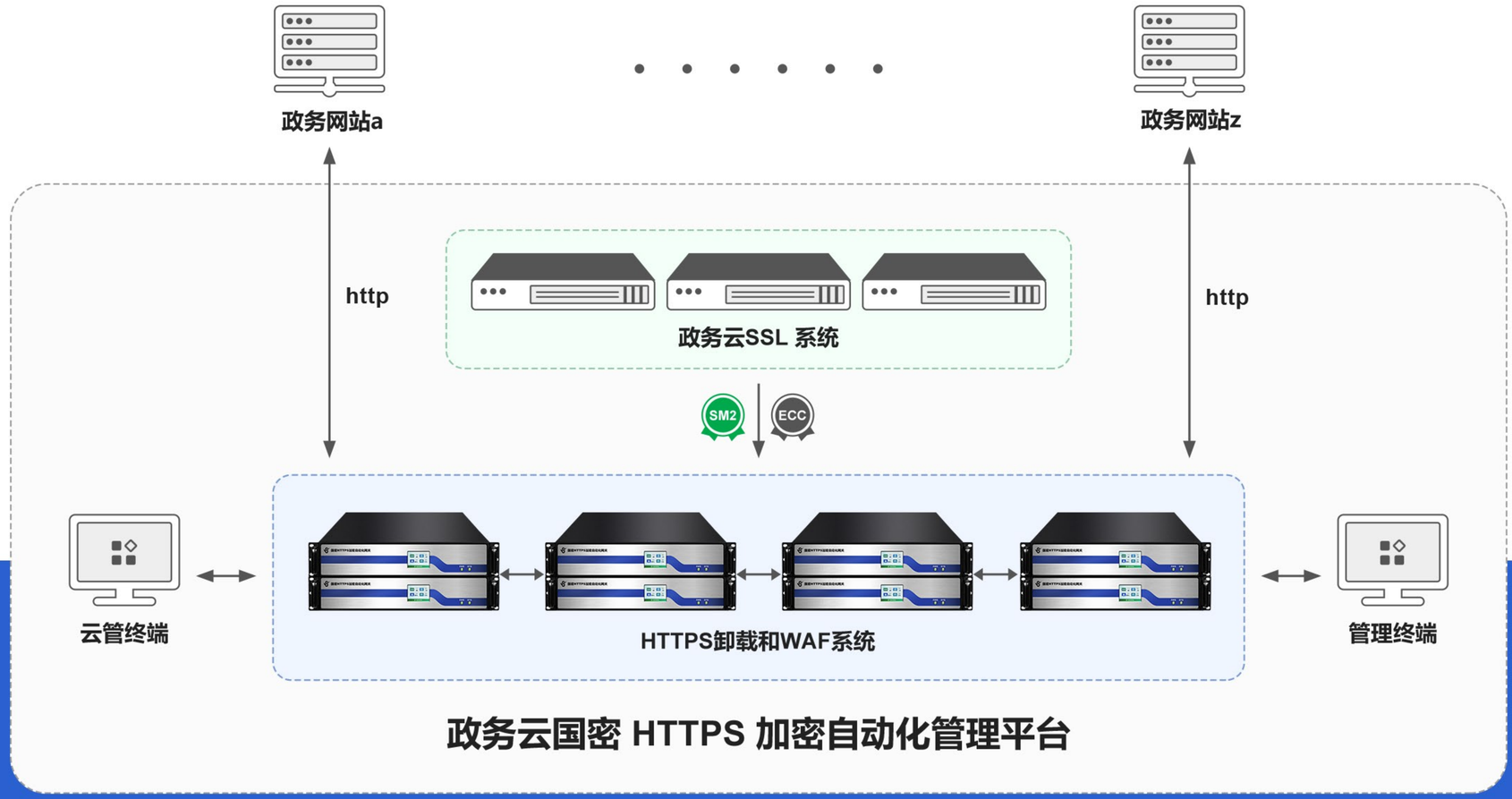
零信国密HTTPS加密自动化系统具有零信国密HTTPS加密自动化网关的所有功能，绑定物理服务器和用户账户，非常适合于自有服务器硬件的用户，如政务云平台、商业公共云平台、企业私有云平台等，充分利用现有闲置服务器为各种Web系统提供HTTPS加密自动化服务和WAF防护服务。

ZOTRUS

5、可选：云SSL系统本地部署



国密HTTPS加密自动化网关默认自动化对接零信云SSL系统获取双SSL证书后启用https加密，而对于希望能独立自主签发自有品牌的自动部署到网关中的双SSL证书的云平台用户，可以把零信云SSL系统本地化部署实现自动化从定制专用SSL中级根证书签发网关所需的双SSL证书，本地化部署的系统称之为政务云SSL系统或公共云SSL系统。



政务云SSL系统是一个本地化部署的用于签发国密合规的支持国密证书透明的国密SSL证书的CA系统，同时也是一个用于对接国际CA系统签发全球信任的国际SSL证书系统。全套系统的部署就是为了实现完全自主可控地签发和管理用于政务网站系统的国密SSL证书和相对独立自主的签发国际SSL证书。要做到自主可控的签发政务SSL证书，首先就必须有用于签发SSL证书的中级根证书，以便能可靠地实现所有政务系统只信任自己的中级根证书签发的SSL证书，有效地高效地阻止各种针对政务网站的SSL中间人攻击和其他假冒政务网站攻击。

5 小结

零信国密HTTPS加密自动化网关全球独家创新实现原Web服务器零改造全自动实现国密https加密和WAF防护，双算法自适应https加密，开机配置网站域名和IP地址即刻直接开通https加密和加速服务、WAF防护、TCP/DTLS安全交付、双SSL证书自动就绪、全球信任和国密合规、高速动态缓存和压缩、连接复用、会话保持和负载均衡等众多优化功能，在保证性能高效的同时，提供业界极高的性能价格比。

零信国密HTTPS加密自动化网关即插即用，部署在网站服务器的前端，原网站服务器无需任何改动，即可实现无缝从http升级到https工作方式，并且是满足国密合规的国密https加密方式，同时支持国际算法https加密以兼容不支持国密算法的浏览器。其强大的https加速卸载转发功能为网站服务器提供了额外的性能增强支持，不仅完全不增加https加解密负担，而且增强了对外响应能力和处理用户请求能力。零信国密HTTPS加密自动化网关的零改造、零维护、零影响的无缝切换，是国密https加密改造、WAF防护和系统安全从http升级到https的首选和必选。

联系电话: 0755-2660 4080
Email: help@zotrus.com