零信®
ZoTrus

内网版

零信国密HTTPS加密自动化网关

零改造实现内网HTTPS国密改造

https://www.zotrus.com

1 产品简介

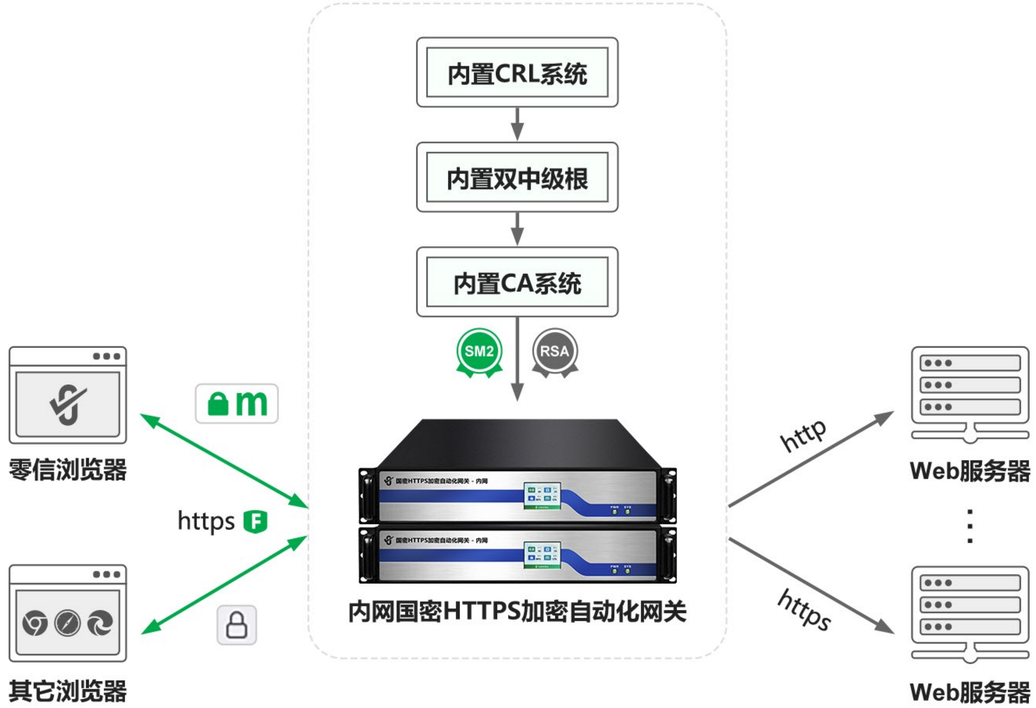
零信国密HTTPS加密自动化网关（简称：零信网关、零信公网网关）是一个通过商密产品认证的用于公网Web系统零改造自动化实现国密HTTPS加密的创新产品。由于此网关需要连接零信云SSL服务系统自动化为用户网站配置双算法SSL证书，所以仅适用于为公网网站和Web系统提供HTTPS加密自动化服务，不支持无法连接互联网的内网部署使用。但是，内网流量加密也需要自动化HTTPS加密服务，为此，零信技术在公网版国密HTTPS加密自动化网关的基础上研发了适用于内网HTTPS加密自动化的内网专用版，这就是零信国密HTTPS加密自动化网关(内网版)。

ZOTRUS

零信国密HTTPS加密自动化网关(内网版)(简称：零信内网网关，或称：零信内网国密HTTPS加密自动化网关)是一个适用于保障内网Web系统HTTP流量安全的自动化实现国密HTTPS加密的创新产品，同公网网关核心功能一样，也是自动化为内网Web系统配置双算法双内网SSL证书，不同的是自动配置由内置CA系统签发的内网SSL证书支持内网IP地址、内部域名和内部主机名，同时也支持公网域名。零信浏览器信任自动配置的内网SSL证书，并优先采用国密算法实现HTTPS加密，真正实现用国密算法来保障内网机密信息安全。零信内网网关使得内网Web系统零改造实现国密HTTPS加密，自适应加密算法，兼容RSA算法HTTPS加密。

2 主要功能

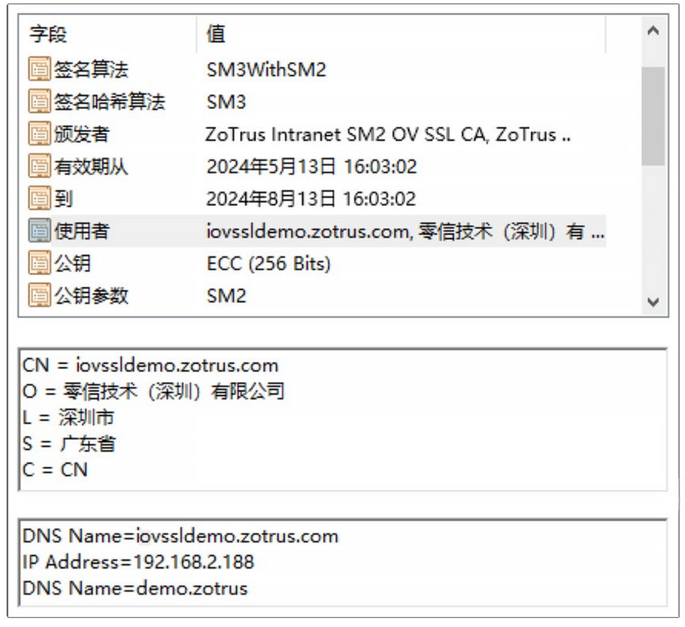
同零信公网网关最大的不同是：内网国密HTTPS加密自动化网关内置一个CA系统和在内置密码卡里内置双SSL中级根，一个是用于签发内网国密SSL证书的国密SSL中级根密钥及其证书，另一个是用于签发内网国际SSL证书的国际SSL中级根密钥及其证书，使得零信内网网关的内置CA系统能直接为用户网站本地自动签发双算法内网SSL证书，这就解决了内网无法连接零信云SSL系统获取双SSL证书的难题。同时，内网网关内置CRL系统，可以用于吊销内网SSL证书和浏览器查询证书吊销信息，为内网用户提供公网SSL证书一样的证书吊销服务。推荐默认双机部署，互为热备，能时双机负载均衡，否时单机独当一面。



零信内网网关的核心功能是原内网Web服务器零改造，无需在服务器上安装SSL证书，也无需升级改造服务器软件支持国密算法，只需在原服务器之前部署内网网关，即可自动化实现HTTPS加密，24小时365天不间断的为内网Web应用提供HTTPS加密自动化服务。支持国密算法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的浏览器则采用RSA算法实现HTTPS加密。

HTTPS加密所需的双算法双SSL证书由网关内置的CA系统自动化签发。自动配置的 RSA算法SSL证书零信浏览器信任，安装零信浏览器后会自动使得谷歌浏览器和微软Edge浏览器也信任，由专为用户定制的用户专用RSA算法中级根证书签发，顶级根证书 AAA Intranet RSA Root 为零信浏览器信任的专用于签发内网SSL证书的RSA算法根证书，自动配置的RSA算法SSL证书为内网OV SSL证书，每张SSL证书O字段固定为用户单位名称，CN字段固定为用户单位的公网域名，SAN字段为用户设置的内网IP地址、主机名、公网域名等。

零信内网网关自动配置的国密SM2算法SSL证书零信浏览器信任，由专为用户定制的用户专用SM2算法中级根证书签发，顶级根证书 AAA Intranet SM2 Root 为零信浏览器信任的专用于签发内网SSL证书的SM2算法根证书，自动配置的SM2算法SSL证书为内网OV SSL证书，每张SSL证书O字段固定为用户单位名称，CN字段固定为用户单位的公网域名，SAN字段为用户设置的内网IP地址、主机名、公网域名等。零信内网网关自动配置双OV SSL证书不支持证书透明，因为无法连接互联网获取证书透明日志签名数据。



零信内网网关默认配置WAF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。

零信国密HTTPS加密自动化网关(内网版)主要十二大功能：

01

零改造https加密

原内网Web服务器无需安装SSL证书，无需升级改造支持国密算法，零改造实现国密https加密，自适应加密算法，支持RSA/SM2算法https加密。

02

自动配置SSL证书

默认免费自动为内网网站配置双内网SSL证书(RSA/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证书常用浏览器信任，国密SSL证书零信浏览器信任。

03

高性能https卸载

完全接管和承担原Web服务器的SSL加解密功能，大大减轻原服务器的性能压力，让原服务器专用于内部业务系统，大大提升内网用户访问响应速度。

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Web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(内网版)主要十二大功能：

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

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服务器。

10

安全双向认证

集成安全双向认证功能，支持国内CA机构签发的USB Key国密证书实现双向认证(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认证。

3 性能指标

零信内网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、全自动的创新方案为内网Wen系统实现https加密，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、提升用户访问内部网站的用户体验。

零信内网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政府、军工以及其他对信息安全管控要求极高的行业应用需求。

每台零信内网网关最多支持自动配置510张RSA 内网SSL证书(单证书)，同时最多支持510对国密内网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510个内网网站域名和内网IP地址自动配置双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。

每台零信内网网关保用期为5年，5年内免费为最多不超过510个内网网站域名和内网IP地址自动配置RSA OV SSL证书和SM2 OV SSL证书。按照证签内网OV SSL证书双SSL证书的价格(1800元/年)计算，仅自动化配置的SSL证书价值高达459万元(=5*510*1800)，全球独家提供超值内网https加密自动化解决方案！

零信内网网关目前提供3种不同规格的产品，可用于政务外网、政务内网和大中型企业内网的内部Web应用系统自动化实现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-3-1	MG-3-2	MG-3-3
CPU品牌	英特尔凌动	英特尔至强(双)	海光5380
支持网站数量	100个	200个 / 510个	200个 / 510个
含RSA SSL证书数量	100张	200张 / 510张	200张 / 510张
含SM2 SSL证书数量	100对	200对 / 510对	200对 / 510对
双SSL证书服务年限	5年	5年	5年
双SSL中级根证书有效期	10年	10年	10年
RSA SSL证书类型	OV SSL证书	OV SSL证书	OV 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
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功能模板	内置	内置	内置
自定义WAF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)	90万元	180 / 459万元	180 / 459万元
节省人力成本(5年)	60万元	120 / 300万元	120 / 300万元
适用对象	中小企业 大学院校	大中型企业 政府/金融机构	政务外网/内网 政府/金融机构

4

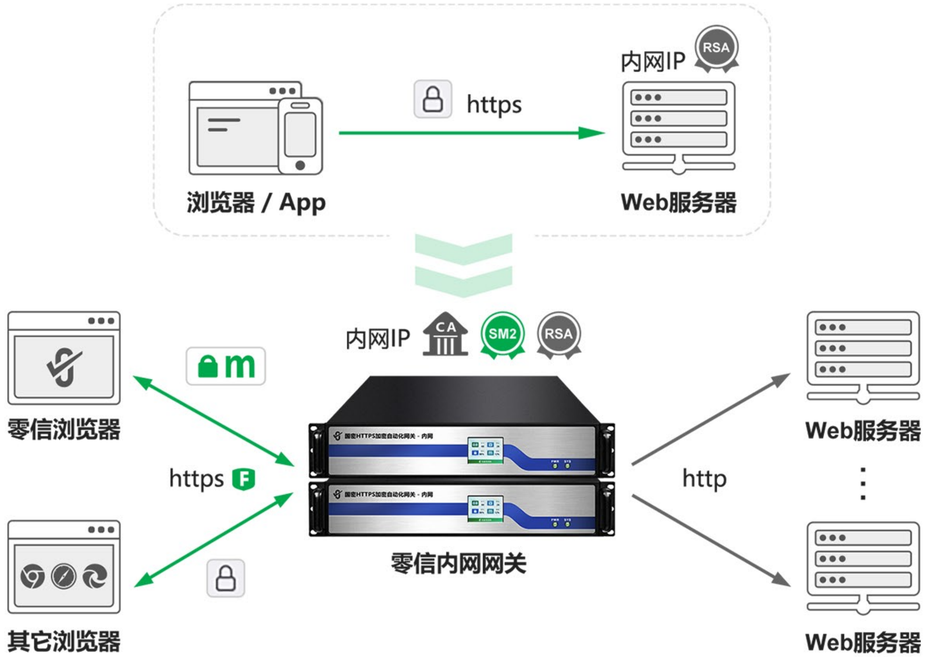
部署应用方案

ZOTRUS

https://www.zotrus.com

零信内网国密HTTPS加密自动化网关支持多种网络部署方式，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天的不间断为内网Web服务器提供https加密服务和WAF防护服务。

1. 为本地内部Web服务器(网站)提供HTTPS加密自动化服务



传统的内网HTTPS加密实现方式是用户自己签发自签SSL证书，手动部署在内网Web服务器上实现HTTPS加密，并且所有内网用户电脑都需要手动安装签发自签SSL证书的根证书，这对于有多个内网Web网站系统需要部署SSL证书的用户，这是一个非常费时费力的难事。用户可以选购零信内网网关，部署在Web服务器前面，由两台网关来为多达510个内部Web网站系统提供HTTPS加密自动化服务，更多网站系统需要购置更多台网关。

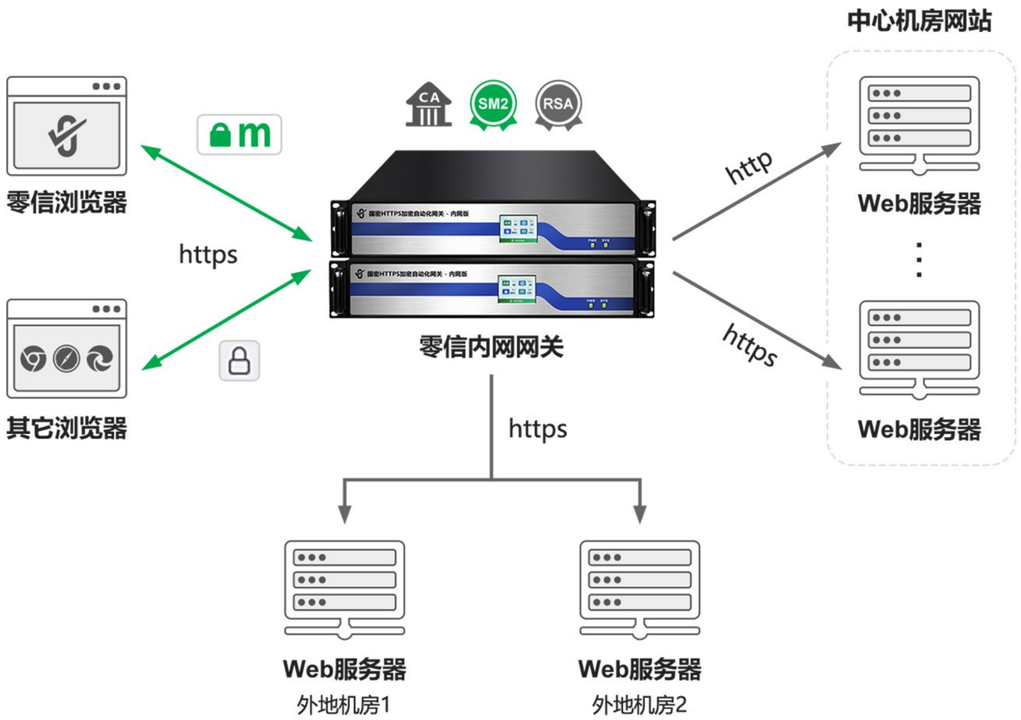
零信内网网关的一个网口连接到内网交换机接口，配置原先内网Web服务器的内网IP地址，而原先的Web服务器连接到其他网口，默认最多可以连接8台内部Web服务器，这些Web服务器改为配置其他网段的内网IP地址。所有网络数据流量均通过零信内网网关进行https加速、卸载和转换处理，符合安全应用协议的数据包将根据负载均衡策略转发到对应内部Web服务器上，支持HTTP明文转发和HTTPS加密转发。用户无需在原Web服务器上部署SSL证书，由内网网关自动申请和签发双算法SSL证书和自动部署双SSL证书，自动化实现自适应加密算法的HTTPS加密服务和WAF防护服务，满足用户国密合规和兼容RSA的应用需求。

此部署方式让原先只能使用明文HTTP不安全协议的Web服务器变成了安全的HTTPS加密访问Web服务器，真正保护了内部管理信息系统的机密信息传输安全，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服务器能更好地为内部业务系统提供算力。

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，原内网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。零信内网网关保用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. 为不在本地的内部Web服务器(网站)提供HTTPS加密自动化服务

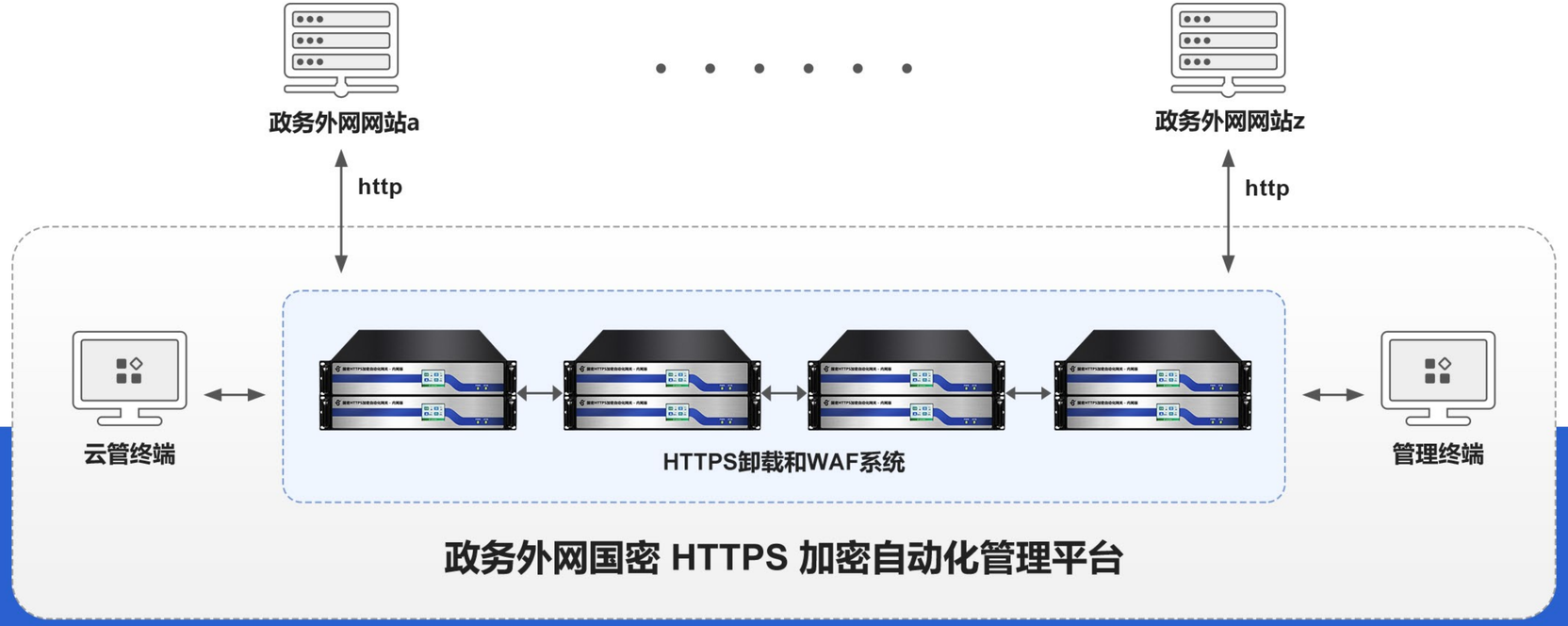


对于不仅有本地内部Web服务器需要实现HTTPS加密自动化服务，而且还有外地分支机构的内部Web服务器的多个网站系统也需要HTTPS加密自动化服务的用户，零信内网网关同时支持本地转发模式和远程回源模式。无论内部Web服务器(网站)是在外地哪个机房，只要网关能通过内网访问，则这些网站都可以由网关来为它们提供HTTPS加密自动化服务和WAF防护服务。双网关最多为510个网站系统提供HTTPS加密自动化服务，更多网站系统需要购置更多台网关。

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。零信技术免费为外地网站提供5年有效期的自签回源专用SSL证书，一次安装证书一直可用于HTTPS加密回源。

3. 政务外网和内网平台国密HTTPS加密自动化管理集群部署方案

对于政务外网和内网平台，有几千甚至上万个网站系统需要完成国密HTTPS加密改造，唯一的解决方案只有自动化才能胜任。需要部署多台零信内网网关组成集群阵列-HTTPS卸载系统和WAF系统，多台内网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。



5 小结

零信国密HTTPS加密自动化网关(内网版)全球独家创新实现原内网Web服务器零改造全自动实现国密https加密和WAF防护，双算法(SM2/RSA)自适应https加密，开机配置内网网站域名和/或内网IP地址即刻直接开通https加密和https加速服务、WAF防护、TCP/DTLS安全交付、双SSL证书自动就绪、国密合规、兼容RSA、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(内网版)即插即用，部署在内网Web服务器的前端，原内网Web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内网Web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。零信内网网关的零改造、零维护、零影响的无缝切换，是国密https加密改造和内部Web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