

零信国密 WAF 加密自动化网关

一、产品简介

零信国密 WAF 加密自动化网关是在零信国密 HTTPS 加密自动化网关基础上增加了 Web 应用防火墙 (WAF) 功能模块的、采用高性能密码卡打造的高端高性能网站安全防护硬件设备，是一个集 https 加密加速、https 卸载转发、WAF 防护、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。

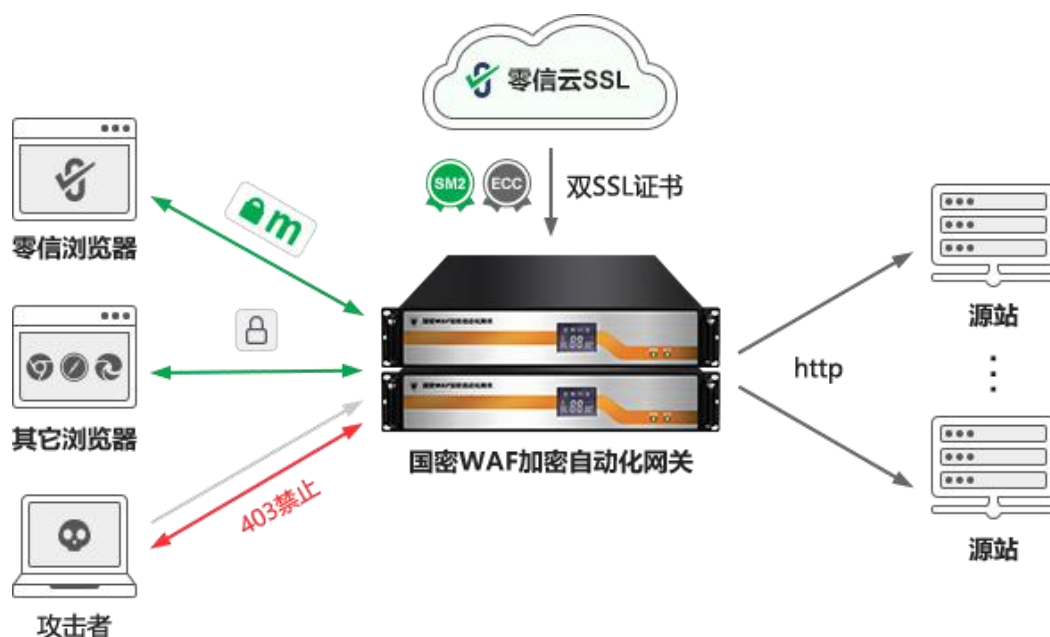


零信国密 WAF 加密自动化网关最大的特点和特色是零申请 SSL 证书、零安装 SSL 证书、自动化实现国密 HTTPS 加密和 WAF 防护，自适应加密算法，支持国密算法和国密证书透明的浏览器采用 SM2 算法实现国密 https 加密，不支持国密算法和国密证书透明的浏览器采用 ECC 算法实现 https 加密。这是一个端云一体的创新解决方案，国密 WAF 加密自动化网关内置国密 ACME 客户端，自动对接零信云 SSL 系统完成自动化双 SSL 证书申请、部署和续期，确保业务系统零改造实现 https 加密和 WAF 防护，不间断地自动化为多达 255 个不同域名的业务系统提供自动化 https 加密服务和 WAF 防护服务，实时检查每一次连接，放行正常流量和拦截攻击流量。



二、 主要功能

零信国密 WAF 加密自动化网关核心功能是原服务器零改造，无需在服务器上安装 SSL 证书，无需在服务器上安装 ACME 客户端软件，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 HTTPS 自动化网关，即可自动化实现 https 加密和 WAF 防护，24 小时 365 天不间断的提供 https 加密服务和 WAF 防护。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。实时拦截攻击流量，只允许合法流量正常通过，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。



HTTPS 加密所需的双算法双 SSL 证书由 HTTPS 自动化网关对接零信云 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。自动配置的双 SSL 证书的证书链文件最小，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 WAF 加密自动化网关自动配置的国密 SM2 SSL 证书国密合规，零信浏览器信任，是目前我国唯一一个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 ZoTrus SM2 DV SSL CA 签发，顶级根证书是零信自有品牌国密算法顶级根证书 ZoTrus SM2 SSL Root，这是我国目前唯一一个专用于签发国密 SSL 证书的国密根证书，已预置零信浏览器信任和零信国密证书透明日志系统信任，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 WAF 加密自动化网关自动配置的双 SSL 证书的证书链文件最小，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。

国密 WAF 加密自动化网关是在国密 WAF 加密自动化网关的基础上增加了 Web 应用防火墙模块，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 地址归属地进行 IP 阻断等等。

如果用户已经购买了 WAF 设备，则推荐选购国密 WAF 加密自动化网关，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 WAF 加密自动化网关主要十大功能：

(1) 零改造 https 加密

原服务器无需安装 SSL 证书，无需安装 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，支持双向认证。

(2) 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。

(3) 高性能 https 卸载

完全接管和承担原服务器的 SSL 加密功能，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。

(4) WAF 安全防护

基于业界领先的开源 ModSecurity 系统开发，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。

(5) 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。

(6) 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。

(7) 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。

(8) 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。

(9) 多算法负载均衡

支持七层和四层协议为用户分配不同的服务器资源，支持基于 URI、HOST、COOKIE、USER_AGENT 等信息和基于 IP 地址、应用类型和内容等因素实现流量负载，支持 NAT 转换。

(10) TCP/UDP/DTLS 安全交付

支持 TCP/UDP/DTLS + SSL/TLS 的安全传输通道交付服务，能够满足基于 SSL/TLS 协议的 TCP/UDP/DTLS 网络应用系统，实现传输通道的加密和加速，原服务器系统无需任何定制改造。

三、性能指标

零信国密 WAF 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、提升内部 Web 服务器的安全防护能力。

零信国密 WAF 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 WAF 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。

每台零信国密 WAF 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和密码卡所支持的新建连接数、吞吐量和并发量。

每台零信国密 WAF 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 DV SSL 证书。按照每个网站双算法双 SSL 证书每年 888 元计算，仅自动化配置的 SSL 证书价值高达 113 万元(=5*255*888)，全球独家提供超值 https 加密自动化解决方案！

零信国密 WAF 加密自动化网关目前提供 4 种不同规格的产品，可分别用于云端高性能数据中心、大中型企业服务器、小型组织服务器自动化实现 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图所示，对于有不同指标要求的用户，可以定制产品满足要求。

产品版本	标准千兆版	专业准万兆版	专业万兆版	专业信创版
产品型号	MG-2-6	MG-2-7	MG-2-8	MG-2-9
最多支持网站数量	100 个	150 个	255 个	100 个
WAF 防护规则	默认+10 条定制	默认+20 条定制	默认+30 条定制	默认+10 条定制
含 ECC SSL 证书数量	100 张	150 张	255 张	100 张
含 SM2 SSL 证书数量	100 张	150 张	255 张	100 张
双 SSL 证书服务年限	5 年	5 年	5 年	5 年
ECC SSL 证书类型	DV SSL 证书	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	OV SSL 证书
网站可信认证类型	EV 认证	EV 认证	EV 认证	EV 认证
国密 https 加密吞吐	900 Mbps	3 Gbps	9 Gbps	900 Mbps
国际 https 加密吞吐	910 Mbps	3 Gbps	9 Gbps	910 Mbps
新建连接数(CPS)	1 万	2.5 万	5 万	8 千
事务处理数(TPS)	4 万	8 万	15 万	3 万

最大并发连接数	30 万	100 万	200 万	10 万
网络接口	6 个千兆	6 个千兆+2 个万兆	6 个千兆+4 个万兆	6 个千兆
机箱	2U	2U	2U	2U
电源	双电源	双电源	双电源	双电源
仅证书项价值(5 年)	44 万元	66 万元	113 万元	113 万元
节省人力成本(5 年)	60 万元	100 万元	150 万元	150 万元
适用对象	中小企业 金融机构	大中型企业 政府/金融机构	商业云平台 政务云平台	政府机构 金融机构

四、部署方案

零信国密 WAF 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，支持自动化对接零信云 SSL 系统为网关自动配置 https 加密所需的双 SSL 证书，也支持本地化部署零信云 SSL 系统为政务云 SSL 系统或商业云 SSL 系统，为本地云平台用户自动化签发双 SSL 证书，本地网关设备自动对接本地部署的云 SSL 系统。为了保证网关的高可用，强烈推荐双机部署，确保 24*365 天的不间断提供 https 加密和 WAF 防护服务。

1. 网关路由模式部署

零信国密 WAF 加密自动化网关的两个网卡为分别负责处理两个不同路由的内外网接口，网关本身作为路由器或 NAT 转换设备。所有网络数据流量均通过网关进行 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服务器上，其他 NAT 数据不受影响，支持标准路由网络通讯。



路由模式部署方式，要求网关与内部服务器部署在不同网段，需要为网关分配公网 IP 地址和内网 IP 地址，同时设置 WAF 加密自动化网关为内网网关，并开启 DHCP 服务，内部服务器连接内网交换机。此

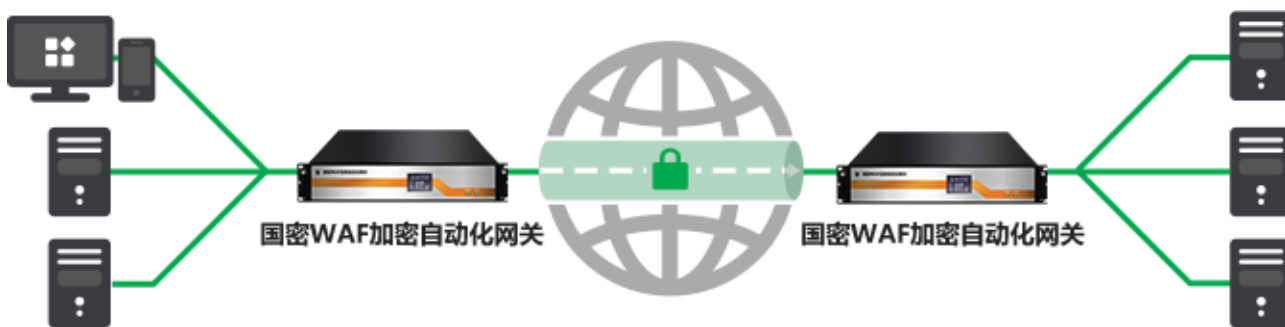
模式下网关同时提供 HTTPS 加密卸载、WAF 防护、转发服务和路由服务。

路由模式部署会改变原服务器 IP 地址，重新分配内网 IP 地址给原服务器。原公网 IP 地址配置给网关使用，支持 IP V4 和 IP V6，原域名解析不用改变。

2. 网关 to 网关部署

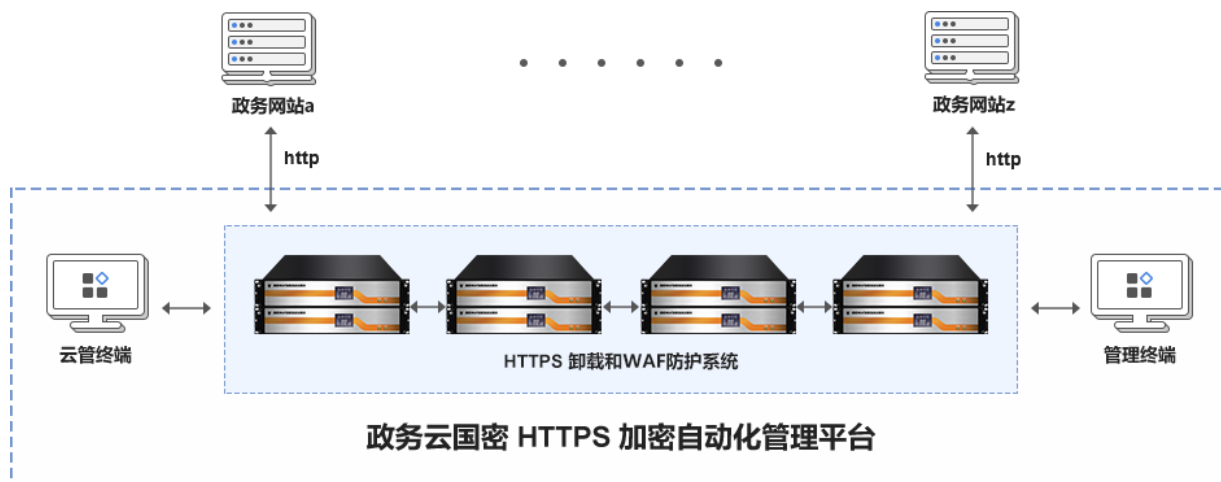
零信国密 WAF 加密自动化网关支持在客户端网络和服务器端网络分别部署，形成对称结构的“网关 to 网关”拓扑结构。网关 to 网关部署方式非常适用于中心机构与分支机构之间的业务往来，它可以将分支机构的大量应用数据请求自动 https 加密，通过互联网传输到中心机构，再自动将数据解密后发送到业务服务器。整个应用与系统本身无需处理通信链路的 https 加密工作，对称部署的 HTTPS 自动化网关可实现一条透明的高速加密通道，保障数据传输安全。

网关 to 网关部署模式极为简单，无需改变原有的网络拓扑结构，极大的降低了网关的部署复杂度，可以广泛应用与金融行业的“银企直联”业务、交通行业的 ETC 全国联网业务系统、企业集团与分支机构的业务数据集中等应用场景。



3. 网关集群方式部署

对于大流量的网站、政务云平台 and 公共云平台的 https 加密应用，必须部署多台国密 WAF 加密自动化网关组成集群阵列-HTTPS 卸载和 WAF 防护系统，多台 HTTPS 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，运行在其上的服务就可以被其它网关接管，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。



对于中小型网站的部署，推荐至少部署两台国密 WAF 加密自动化网关，实现双机热备，确保 https 加密服务的 24 小时 x 365 天的不间断。可选两种双机热备模式：

(1) 主主模式

主主模式即 Active - Active 模式：在网络中部署两台 WAF 加密自动化网关，两台设备均作为主机并同时处理业务流量，同时也互为备机。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的业务，从而保证业务调度依然能够得到响应处理，网络中不会发生局部中断。此种模式适合于强调高可用性的冗余网络环境（例如 VRRP）的部署需求，推荐此模式，双机共同承担业务流量，不浪费资源。

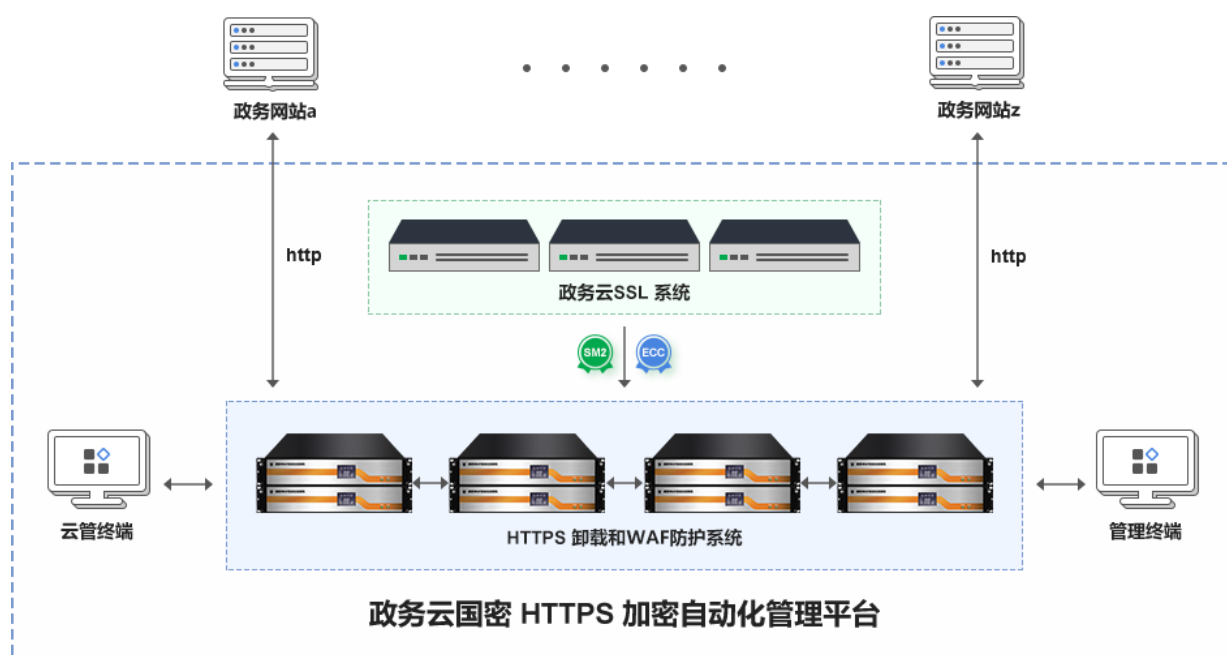
(2) 主备模式

主备模式即 Active - Backup 模式：在网络中部署两台 WAF 加密自动化网关，一台处理业务流量，称为主机；另一台处于待命状态，称为备机。主机在处理业务的同时，会将业务产生的会话信息同步到备机，从而确保双机切换后，新发起的业务访问能继续得到响应处理，当前正在进行的业务访问也不会因此而中断。此种模式适合于大多数网络环境中避免单点故障的部署需求，此模式的备机处于闲置状态，不推荐。

4. 云 SSL 系统本地部署

国密 WAF 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。



五、 小结

零信国密 WAF 加密自动化网关全球独家创新实现原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 WAF 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，即可实现无缝从无 Web 安全防护的 http 方式升级到有 Web 安全防护的 https 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 WAF 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 加密改造和系统安全从 http 升级到 https 的首选和必选。

联系我们：0755-2660 4080, Email: help@zotrus.com

