

## SSL VPN 网关不是 HTTPS 加密网关

笔者最近参加了广西密码铸盾八桂行和武汉网安创新论坛两个重要的会议，同时走访了湖南、湖北、广东、广西和福建 5 省的合作伙伴和意向客户，发现无论是密码企业还是网安企业，还有用户，都对 SSL VPN 网关的作用和用途有误解和歧义。所以，笔者认为应该写篇文章来讲清楚 SSL VPN 网关与 HTTPS 加密网关有什么不同，应该如何选购合适的产品来满足用户业务系统的 HTTPS 加密需求。

### 一、 SSL VPN 网关仅用于远程安全接入

根据百度百科的定义：SSL VPN 指采用 SSL 协议来实现远程接入的一种 VPN(虚拟专用网)技术。它包括：服务器认证、客户认证、SSL 链路上的数据完整性和保密性。SSL VPN 是一种既简单又安全的远程隧道访问技术，使用非常简单。与 IPSec VPN 相比，SSL VPN 具有架构简单、运营成本低、安全性能高的特点，所以在企业用户中得到大规模的使用。

SSL VPN 网关是一种远程接入设备，实现在外地的员工可以通过互联网使用浏览器以 HTTPS 加密方式访问位于内网的 Web 应用系统。SSL VPN 网关当然也需要部署 SSL 证书实现 HTTPS 加密，国内厂商的 SSL VPN 网关是默认配置了一张自签的浏览器不信任的 SSL 证书，用户要么在使用时接受不安全警告继续使用，要么自己花钱向 CA 购买一张 SSL 证书部署后使用。

但是，现在大家都把这个用于远程安全接入内网 Web 应用的设备当成了实现公网网站 HTTPS 加密的设备，这就是用错地方了，不仅达不到公网 HTTPS 加密所需的快速响应用户请求的要求，而且有可能把整个内网都暴露到了互联网上，非常不安全。因为用于 SSL VPN 接入的用户应该是内部员工，但如果用于互联网用户都可以访问的公网网站那就有很大的安全隐患了。

### 二、 HTTPS 加密网关专用于实现网站 HTTPS 加密

笔者试图搜一下百度百科对“HTTPS 加密网关”的定义，很遗憾没有搜到，这很正常，因为这是一个专用于公网网站实现 HTTPS 加密的新型网关产品。

网站要实现 HTTPS 加密，通常是直接在 Web 服务器上部署 SSL 证书。但是有些用户不希望 Web 服务器暴露在互联网上，就得部署一个前置网关来实现 HTTPS 加密，SSL VPN 网关就变成了首选，因为大家都熟悉这个产品，也可以实现 HTTPS 加密，但是这是一个错误的选择，因为用户需要的是实现网站 HTTPS 加密，而不是用户远程接入内网。但是，对于用户来讲，这也是一个无奈的选择，因为安全厂商给用户推荐的方案就是部署 SSL VPN 网关，没有别的选择。

所以，HTTPS 加密网关就应运而生了，这是在普及 HTTPS 加密应用的市场环境下诞生的新产品，一个可以实现 HTTPS 加密、HTTPS 卸载和高速转发的网关产品，一个 Web 应用反向代理网关产品，一般采用具有高性能的反向代理能力的 Nginx 实现，类似于常用 CDN 和 WAF 服务的实现原理。

HTTPS 加密网关一般内置高速密码卡，也就是早期常用的安装在 Web 服务器上的 SSL 加密卡或 SSL 卸载卡，以实现快速 HTTPS 加密响应和 HTTPS 解密卸载，并把卸载后的明文流量转发给网关后面的 Web 服务器。这就是与 SSL VPN 网关的最大不同，不给访问者分配内网 IP 地址直接访问内网 Web 服务器，而且转发访问者的数据请求到内网 Web 服务器。

当然，HTTPS 加密网关也必须有 SSL 证书才能实现 HTTPS 加密，也需要用户向 CA 购买 SSL 证书并部署在网关上使用。这是同 SSL VPN 网关一样的，但是不同的，HTTPS 加密网关是为了减轻 Web 服务器的 HTTPS 加密负担，无需在 Web 服务器上安装 SSL 证书，专用于为 Web 服务器提供 HTTPS 加密卸载转发服务的网关，不是用于用户远程接入内网 Web 服务器的网关。

用户在选购网关产品时一定要搞清楚自己的需求是为单位员工远程接入到单位内网 Web 服务器，还是为公众用户提供 HTTPS 加密方式的 Web 服务(如公网网站和服务系统)，前者选用 SSL VPN 网关，后者则选用 HTTPS 加密网关。

### 三、 HTTPS 加密自动化网关和国密 HTTPS 加密自动化网关，自动化配置 SSL 证书

HTTPS 加密网关提供的是一个前置 Web 代理服务，替 Web 服务器分担了 HTTPS 加密工作，从而减轻 Web 服务器的加解密负担而专用于业务系统，并且使得 Web 服务器不用直接暴露在互联网上，让位于网关后面的 Web 服务器更安全。

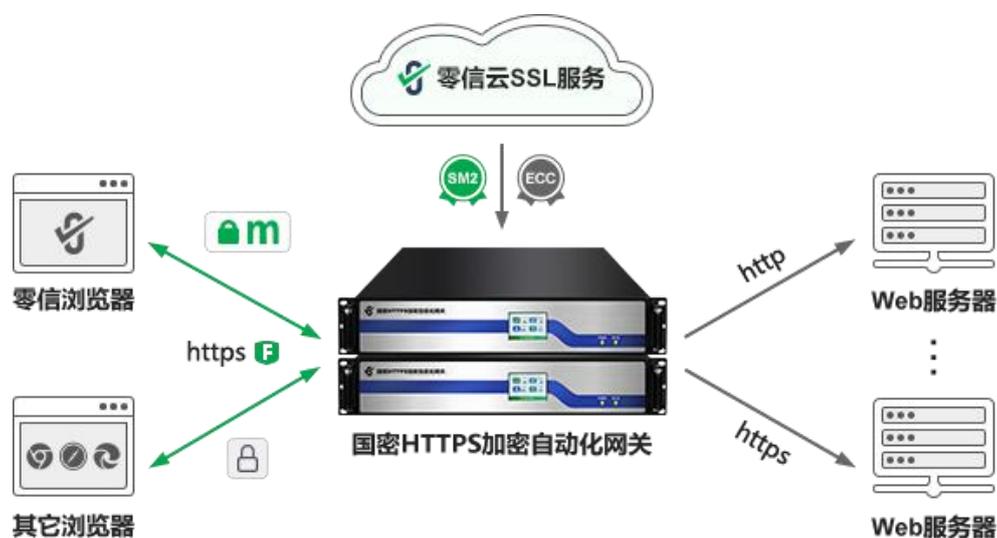
HTTPS 加密自动化网关，多了“自动化”三个字，则是一个升级产品，实现了自动化为网关配置 SSL 证书，用户无需向 CA 申请 SSL 证书，这是把国际上流行的在 Web 服务器上安装 ACME 客户端软件实现 HTTPS 加密的方案集成到网关上，国际网安大厂的所有相关设备都已

经实现了这个 SSL 证书自动化管理功能。这当然是用户喜爱的功能。

国密 HTTPS 加密自动化网关,则是自动化配置国密 SSL 证书实现国密算法 HTTPS 加密,当然一般都同时自动化配置国际 SSL 证书,实现自适应算法的 HTTPS 加密,这非常适合于我国要求完成的 Web 应用国密改造,因为用户无需向 CA 申请国密 SSL 证书和国际 SSL 证书,只需配置网站域名即可自动化部署双算法双 SSL 证书,实现 HTTPS 加密自动化。

#### 四、 零信国密 HTTPS 加密自动化网关, 自动化配置双算法 SSL 证书和集成 WAF 服务

零信国密 HTTPS 加密自动化网关就是一个自动化配置双算法(ECC/SM2)双 SSL 证书的国密 HTTPS 加密自动化网关产品,是我国首个也是目前唯一一个通过商用密码产品认证的专用于国密 HTTPS 加密自动化的网关产品。不仅如此,为了保障 Web 应用安全,还集成了高性能 WAF 系统,为用户提供检测能力和识别能力都为 A 级的 Web 应用防火墙服务,所以,零信国密 HTTPS 加密自动化网关也同时是一个国密 WAF 自动化网关,可用于替代需要用户手动申请和部署 SSL 证书的传统 WAF 设备。



零信国密 HTTPS 加密自动化网关是一个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、WAF 防护、负载均衡、双向认证等多项功能于一体的专用于 Web 网站系统 https 加速和卸载的硬件网关产品,内置专业级高性能双算法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、RSA/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 并发连接数可达到 150 万、HTTPS 加密吞吐量可达到 9Gbps。

零信国密 HTTPS 加密自动化网关最大的特点和特色是无需在原 Web 服务器上安装 SSL 证书、自动化为网站域名配置双算法 SSL 证书，自动化实现 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，内置国密 ACME 客户端，自动对接零信云 SSL 服务系统，自动化完成双 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 个不同域名的网站和业务系统提供 5 年无忧的自动化 https 加密服务和 WAF 防护服务。

零信国密 HTTPS 加密自动化网关自动化完成了三种不同网络协议的转换工作，一是实现了 HTTP 明文传输协议到 HTTPS 密文传输协议的转换；二是实现了两个不同密码体系(RSA 和 SM2)的转换，使得原 Web 服务器零改造完成了国密改造，三是实现了两个不同 IP 地址体系(IPv4 和 IPV6)的转换，使得原 Web 服务器也无需改造支持 IPv6，但用户可以使用 IPv6 网络访问 Web 应用。零信技术端云一体创新实现了一个网关搞定三个协议转换难题，是网站和 Web 系统实现 HTTPS 加密的不二之选。

## 五、 选对网关产品，保障 Web 应用安全

SSL VPN 网关是实现远程安全接入的首选，但不是网站实现 HTTPS 加密的选项，这个产品选型不能错！要想网站和 Web 系统实现 HTTPS 加密，就得选购 HTTPS 加密网关，但是这类网关需要用户人工申请和部署 SSL 证书到网关上，费钱费时费力，特别是 SSL 证书有效期即将缩短为 47 天，用户必须选购支持 SSL 证书自动化管理的 HTTPS 加密自动化网关。而对于要求完成国密改造的用户，不仅仅是为了密评和等保，更重要的是为了满足四部委发布的《互联网政务应用安全管理》要求所有互联网应用都必须实现国密 HTTPS 加密的合规要求，应该选购同时支持国密 SSL 证书和国际 SSL 证书自动化管理的国密 HTTPS 加密自动化网关。

正确选对网关产品，不仅能实现保障 Web 应用安全所需的目的，而且能简化网络管理和提升网络安全水平，这非常重要，希望本文能对合作伙伴和用户选购所需的网关产品有所帮助。

**王高华**

2025 年 5 月 12 日于深圳

---

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。  
已累计发表中文 212 篇(共 62 万 8 千多字)和英文 91 篇(12 万 1 千多单词)。

