零信网关特色之一：自动化

经常有朋友问我：零信网关同其他网关有什么不同？我总是回答三个字：**自动化**！这就是最大的不同，也是最重要的和最核心的不同—自动化实现 HTTPS 加密。

百度百科对“网关”的定义还是比较准确的：网关(Gateway)又称网间连接器、协议转换器。网关在网络层以上实现网络互连，是复杂的网络互连设备，仅用于两个高层协议不同的网络互连。网关既可以用于广域网互连，也可以用于局域网互连。 网关是一种充当转换重任的计算机系统或设备，使用在不同的通信协议、数据格式或语言，甚至体系结构完全不同的两种系统之间。网关是一个翻译器，与网桥只是简单地传达信息不同，网关对收到的信息要重新打包，以适应目的系统的需求。

维基百科对“Gateway(网关)”的定义要简单些：网关是网络中使用的一种网络硬件或软件，它允许数据从一个离散网络流向另一个离散网络。网关与路由器或交换机的不同之处在于，它们使用多个协议进行通信以连接多个网络，并且可以在 OSI 模型的七个层中的任何一层上运行。

根据以上两个百科对“网关”的定义，我们可以总结出零信网关有如下三个方面的重要特点：

第一：零信网关充当通信协议转换的重要角色

零信网关负责 HTTP 明文协议同 HTTPS 加密协议之间的转换，使得原 Web 服务器无需安装 SSL 证书也能为用户提供 HTTPS 加密连接，保障用户连接服务器的链路安全。用户浏览器使用 HTTPS 加密协议连接网关，由网关把 HTTPS 流量卸载为 HTTP 明文流量给 Web 服务器，Web 服务器处理后把用户所需数据明文给网关，由网关用 HTTPS 加密协议把数据回传给用户，实现 HTTP 协议和 HTTPS 协议的双向转换。

第二：零信网关充当两个不同密码体系转换的重要角色

这是国密改造的需要，两个不同的密码体系是指国际 RSA 密码体系和国密 SM2 密码体系。这个角色很厉害，让用户浏览器可以用国密算法实现 HTTPS 加密，但是原 Web 服务器仍然可以使用原先的 RSA 密码体系来连接网关，实现 RSA 算法 HTTPS 加密信息转发给 Web 服务器，服务器回传给用户的数据通过 RSA 算法 HTTPS 加密返回给网关，网关用 SM2 算法 HTTPS 加密返回给用户浏览器，两段用了不同的密码体系实现了从用户浏览器到 Web 服务器的全程加密。这就使得原来已经实现了 RSA 算法 HTTPS 加密的 Web 服务器可以零改造完成国密改造。

因为 RSA 密码体系在各种系统中的充分集成已经三四十年了，有些正在使用的系统是根本无法改造成国密体系，那就索性不改造，继续保留使用，由网关来完成密码系统的转换工作，完成密码协议的转换工作，负责 SM2 算法和 RSA 算法之间的相互转换。这是一个创新的国密改造思路，让国密改造不再难，很容易，在原 Web 服务器前面部署一个零信网关即可。

第三：自动化保证了两个转换角色的高效稳定运行

这一点是零信网关同其他任何网关的最大不同之处。第一角色的通信协议转换需要 SSL 证书，需要在网关上部署 SSL 证书才能实现 HTTP 明文协议同 HTTPS 加密协议之间的转换。而传统网关需要用户人工向 CA 购买和申请 SSL 证书，手动完成域名验证，拿到证书后手动部署

到网关上去使用，才能正常实现 HTTP 到 HTTPS 协议的转换。

这个人工处理过程如果是一个网站，一年申请一次，一年安装部署一次，视乎还能接受。但是，如果单位有 10 个网站系统、100 个、1000 个、甚至政务云平台的上万个，怎么办？不可能人工申请证书和部署证书了，这就是为何还有那么多政府网站系统和企业网站系统没有部署 SSL 证书的根本原因，人工搞不定。怎么办？答案只有一个：让机器自动化搞定，这个机器就是零信网关，零信网关能自动化连接零信云 SSL 服务系统申请 SSL 证书、自动化完成域名验证、自动化部署 SSL 证书，自动化实现 HTTPS 加密。这就是零信技术的创新解决方案，零信技术建设了一个云密码基础设施，其中重要的一块是零信云 SSL 服务系统，可以为零信网关自动化签发 SSL 证书，无需用户手动参与，最多为 255 个网站提供 5 年不间断的自动化完成证书申请、证书部署和证书续期工作。

零信网关就这样完美地自动化完成了第一个通信协议转换工作，而第二个密码体系转换工作则需要相关生态产品的支持:

(1) 零信云 SSL 服务系统自动化为用户网站签发国密 SSL 证书，而不单单是签发国际 SSL 证书，双算法双证书自动下发给零信网关;

(2) 零信网关收到双证书后自动化部署应用，支持 RSA/ECC/SM2 密码算法，优先采用国密算法实现国密 HTTPS 加密;

(3) 零信浏览器支持国密算法和国密 SSL 证书，优先采用国密算法连接零信网关实现国密

HTTPS 加密。

这是一个端云一体的解决方案，有云端系统自动化为端(零信网关)配置双证书，还有一个端(零信浏览器)为用户实现国密 HTTPS 加密连接，端云紧密配合，才能自动化完成通信协议的转换和密码体系的转换。

自动化配置 SSL 证书的更大优势在于：用户无需考虑 SSL 证书的有效期问题，目前 SSL 证书有效期是一年，而考虑到密钥安全，国际标准正在推动 90 天政策的落地，证书有效期为 90 天意味着每年需要 5 次申请和安装证书，原先为一年有效期的工作量将增加 5 倍，人工已经无法完成，就只能由网关来自动化完成了，仅这一点，两台双机热备网关最多支持 255 个网站的 5 年的证书自动化部署工作可以节省工程师人力成本 150 万元。实际上，为了保障用户密钥安全，零信网关在国际标准还没有落地之前的现在已经实现了自动化每 83 天更换新的密钥和新的 SSL 证书，让用户无忧迎接 90 天证书政策的落地而什么都不用做。

最后简单总结一下，零信国密 HTTPS 加密自动化网关的关键词是“自动化”，同其他网关的最重要的也是最核心的不同是自动化实现 HTTPS 加密，并且这个自动化实现符合国际标准 RFC8555(ACME)，遵循《自动化证书管理规范》商密标准草案，这是我国目前唯一一个通过商密产品认证的遵循双标准的国密 HTTPS 加密自动化网关。只有自动化配置 SSL 证书才能实现网关的通信协议转换功能，只有自动化同时配置国密 SSL 证书和国际 SSL 证书才能实现网关的密码体系转换功能，只有自动化申请和部署 SSL 证书才能节省运维工程师的人力成本，只有自动化证书管理才能为网站提供 5 年 365 天不间断的 HTTPS 加密服务，不间断地保证网站系统数据的安全流通。

有诗为证：

自动化，通信协议转换。
自动化，密码体系转换。
自动化，方能节省成本。
自动化，保障持续安全。

王高华

2024 年 2 月 26 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。
从 2021 年 12 月 9 日开始，已累计发表中文 152 篇(共 40 万多字)和英文 60 篇(7 万多单词)。