内网网站系统部署 SSL 证书宝典

内网是指不连接公网(互联网)的内网网络，内网网站系统是指用于内部业务管理的 Web 系统，为了保障内部管理系统的数据安全，内网网站系统也必须部署 SSL 证书，但是大家常用的 SSL 证书是不支持内网 IP 地址和内部域名的，因为 CA 无法验证用户对申请证书绑定的内网 IP 地址和内部域名的控制权。怎么办？本宝典详细讲解如何为内网网站系统部署 SSL 证书，特别是如何部署绑定内网 IP 地址的内网 SSL 证书。

一、 内网流量更需要 SSL 证书实现 HTTPS 加密保护

内网之所以称之为内网，是因为其流量都是单位机密数据，不能连接公网，以保护这些内部机密信息安全，但是内网已经不是一个办公室内的一台交换机内的网络，已经是一个跨楼层、跨楼栋、甚至跨城市的内联网，内部机密数据如果是明文 HTTP 方式流通，非常不安全，非常容易在数据传输过程中被非法窃取和非法篡改，所以比公网更需要加密保护。

而如何实现内网数据的加密保护，最简单的方案就是为内部 Web 网站部署 SSL 证书实现 HTTPS 加密，而不是采用加密机加密原始数据后仍然用明文 HTTP 协议传输，这个加密机方案实施成本更高，更复杂，并且不方便实现数据处理和 AI 应用。采用 SSL 证书实现传输加密的技术方案之所以是最容易实施和最低成本的方案，是因为整个应用生态都支持这个方案，包括浏览器和 Web 服务器，只需部署 SSL 证书即可。

二、 为内网网站系统部署 SSL 证书的三个可选方案

如何为内网 Web 网站部署 SSL 证书是一个一直在困扰内网管理员的难题，目前无外乎以下三个技术方案：

1. 自己签发自签 SSL 证书

签发自签 SSL 证书非常简单，只需使用 OpenSSL 软件，一行命令就可以实现：

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes
```

接着输入内网 IP 地址或主机名即可完成自签 SSL 证书的签发，就可以部署到内网 Web 服务器上使用。其最大的问题是要求每个内网用户在第一次访问网站时都必须点击信任此自签 SSL 证书。

2. 使用企业 CA 签发内网 SSL 证书

如果企业内网已经建立了企业 CA，为内网用户签发登录内网系统的客户端证书，则只需配置 SSL 证书签发参数，就可以签发内网 SSL 证书，部署使用即可。一般来讲，内网用户电脑都已经设置信任企业 CA 的根证书，只要签发的内网 SSL 证书的密钥长度为 RSA 2048 和 SHA256 或以上参数，常用浏览器应该是能正常实现 HTTPS 加密的。

3. 申请和部署公网 SSL 证书

以上两种实现方式的唯一问题是常用浏览器不信任自签证书和企业 CA 签发的 SSL 证书，需要在每个用户电脑上安装根证书和信任自签证书，这也是一个比较大的工作量。所以用户还可以选择第三个方案，那就是申请浏览器信任的公网 SSL 证书。

这就要求内网有 DNS 系统，用公网子域名申请全球信任的公网 SSL 证书，再解析公网子域名到内网 IP 地址，即可使用绑定公网子域名的公网 SSL 证书实现 HTTPS 加密，这样常用浏览器就不会有不安全警告，也无需为每个内网用户电脑安装企业 CA 根证书或信任自签证书。

三、 只有部署浏览器信任的内网 SSL 证书才能真正保障内网流量安全

从上面所述的现有 3 个解决方案可以看出，浏览器信任很重要，浏览器之所以信任，是因为这张 SSL 证书是按照国际标准和国密标准签发出来的，能保障密钥安全和 HTTPS 加密安全，而自签证书和企业 CA 签发的证书往往不可能做到完全符合国际标准 SSL 证书基线要求，这就是浏览器信任的 SSL 证书的价值。

上述的方案 3 是在内网部署浏览器信任的公网 SSL 证书，虽然解决了浏览器信任问题，但是并没有解决 SSL 证书必须绑定内网 IP 地址的用户需求，毕竟现有大量的内网 Web 系统都是基于内网 IP 地址来访问的，特别是跨单位的内联网，要实现一个跨单位的内网 DNS 解析来解决公网子域名为内部 IP 地址有一定的难度，也不可能把所有基于内网 IP 地址的系统都改为公网域名来访问。

零信技术也正是充分认识到用户需要同时满足绑定内网 IP 地址和浏览器信任两个应用需求，全球独家率先历时两年多打造了内网 SSL 证书应用生态，核心产品之一就是证签内网 SSL 证书，默认为双算法(RSA/SM2) SSL 证书，支持绑定内网 IP 地址和主机名，解决了内网 SSL 证书绑定内网 IP 地址的验证难题；核心产品之二就是零信浏览器，零信浏览器预置信任签发证签内网 SSL 证书的 RSA 和 SM2 算法根证书，不仅信任证签内网双算法 SSL 证书，并且支

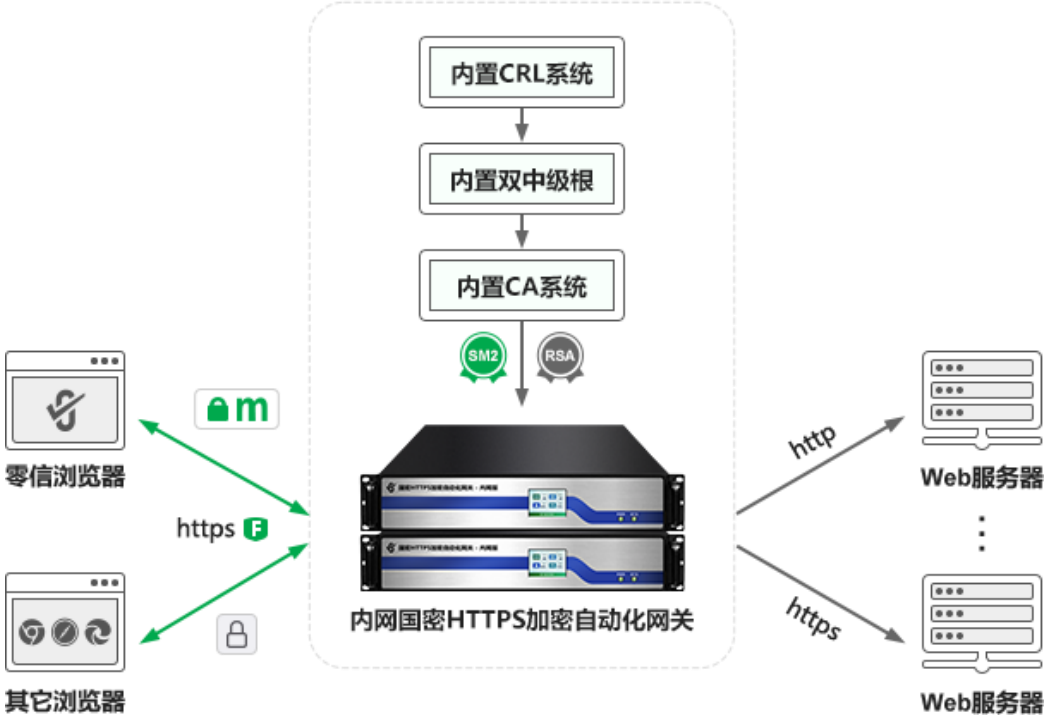
持证书透明，零信浏览器优先采用国密算法实现 HTTPS 加密，满足用户国密合规的要求。对于已经安装使用零信浏览器的用户，可以同时使用其他常用浏览器实现 RSA 算法 HTTPS 加密，这些浏览器也一样信任证签内网 RSA 算法 SSL 证书。

正是由于证签内网 SSL 证书满足了用户的两个核心应用需求，使得证签内网 SSL 证书上线后受到了用户的欢迎，很多用户申请并部署使用，为保障内网流量安全做出了应有的贡献。

四、 只有实现内网 SSL 证书自动化管理才能快速普及实现内网流量 HTTPS 加密

虽然证签内网 SSL 证书满足了用户需要绑定内网 SSL 证书和浏览器信任的两个应用需求，但是仍然同公网 SSL 证书一样需要人工申请证书，手动去内网 Web 服务器安装内网 SSL 证书，这个证书安装会影响正在运行的 Web 服务器正常提供 Web 服务，所以，内网 SSL 证书像公网 SSL 证书一样也需要实现自动化管理。

零信技术已经推出了内网国密 HTTPS 加密自动化网关，这是在 2023 年全球首发零信国密 HTTPS 加密自动化网关公网版之后的又一个产品创新，因为内网是不能连接互联网的，那就无法连接零信云 SSL 服务系统，无法实现端云一体的 SSL 证书自动化管理，唯一可行的解决方案就是由内网网关实现 SSL 证书“自给自足”。零信内网网关内置了迷你 CA 系统、商密产品认证的密码卡和双算法 SSL 中级根证书，用于自动化签发零信浏览器信任的双算法内网 SSL 证书。



零信内网国密 HTTPS 加密自动化网关采用了同公网 SSL 证书自动化管理(ACME)一样的技术思路，同时解决了内网无法连接云 SSL 证书自动化管理服务系统的难题，做到了双算法内网 SSL 证书的“自给自足”，比公网网关需要依赖 ACME 云端服务更可靠，彻底解决了内网流量明文传输裸奔的技术难题，必将成为解决内网流量安全的首选产品。

五、零信技术鼎力打造内网网站系统部署 SSL 证书最优方案

内网网站系统部署 SSL 证书除了第二节介绍的目前市场上的常用三种解决方案外，用户可选零信技术为内网流量安全打造的更加完美的第四个解决方案，那就是：

(1) 部署内网 SSL 证书：传统人工方式在线申请证签内网 SSL 证书，在内网 Web 服务器上人工安装内网 SSL 证书，可以仅安装 RSA 算法内网 SSL 证书，或升级改造 Web 服务器部署国密内网 SSL 证书。推荐选购 5 年有效期证书，一次安装保用 5 年，但这仅适用于只有少量内部 Web 服务器的单位。

(2) 或部署内网网关：部署零信内网国密 HTTPS 加密自动化网关，无需人工申请和部署内网 SSL 证书，原内网 Web 服务器零改造，最多支持 510 个内网 Web 网站系统自动化部署 90 天有效期的双算法 OV SSL 证书，实现 HTTPS 加密自动化和 WAF 防护自动化。密钥和证书每 80 天自动更新一次，更加安全敏捷地实现自适应加密算法的 HTTPS 加密自动化。此方案适用于有大量内网 Web 系统的不间断运行的单位。

零信技术打造的两个可选方案都可以用于保障内网流量安全(HTTPS 加密)，免费配套的完全免费的国密浏览器--零信浏览器已经是市场第一位的国密浏览器，优先采用国密算法实现国密 HTTPS 加密，其他浏览器则可信地实现 RSA 算法 HTTPS 加密。推荐只需在内网 Web 服务器前部署内网国密 HTTPS 加密自动化网关的原 Web 服务器零改造方案，实现零改造的从明文 HTTP 无缝升级到 HTTPS 加密，真正用国产密码来保障内网机密数据传输安全，切实保障内网流量安全，满足用户等保和密评合规要求。

王高华

2025 年 4 月 7 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 207 篇(共 60 万 8 千多字)和英文 89 篇(11 万 7 千多单词)。