让网安设备都回归本职，加密流量卸载交给 HTTPS 加密自动化网关

2026 年 7 月 28 日

当前，大型组织网络安全架构普遍采用“糖葫芦串”式的多设备串联部署，防火墙、入侵防御系统（IPS）、Web 应用防火墙（WAF）、抗 DDoS 设备、上网行为管理、负载均衡设备等等，一台接一台串在流量路径上。这种架构在过去 HTTP 明文的时代运转良好，每台设备各司其职。然而，随着 HTTPS 流量占比超过 95%，一个严重的问题出现了：**每一台网络安全设备都不得不具备 SSL 解密能力，否则就无法检测加密流量中的威胁**。

这不仅导致了严重的性能浪费，每台设备都要消耗大量 CPU 资源做重复的 SSL 加解密运算，更是带来了运维噩梦：当故障出现时，需要协调不同厂商的设备逐一排查，定位难度极大；设备扩容只能靠“换更高性能硬件”来实现纵向扩展，无法横向弹性扩容。更深层的问题是，随着国密 SM2 算法的强制部署、混合 PQC 算法的加速迁移，以及 SSL 证书有效期不断缩短，每一台安全设备都要同时适配多套密码体系和不断短寿的 SSL 证书，**这让本应专注各自网络安全功能的多台设备，全部陷入了“样样通、样样松”的困境**。

怎么办？

一、网络安全设备的“本职”到底是什么？

要想找到正确的解决路径，先得搞清楚每台设备的本职工作到底是什么，以及它们现在正在承受哪些本不该由它们承受的负担。

让我们逐一盘点大型组织网络架构中常见设备的设计初衷：

防火墙（FW） 的本职，是基于 IP 地址、端口和协议做网络层访问控制，决定“谁可以访问什么”。它不应该消耗算力去解密 HTTPS 流量，这不是它的设计目标。

入侵防御系统（IPS） 的本职，是检测网络流量中的已知攻击特征和异常行为模式。它应该专注于特征匹配和行为分析，而不是把 CPU 浪费在 SSL 握手和解密上。

Web 应用防火墙（WAF） 的本职，是深度检测 HTTP 应用层流量，识别并拦截 SQL 注入、XSS 等 Web 攻击。它只应该处理明文 HTTP 流量，解密不是它的任务。

抗 DDoS 设备 的本职，是识别和清洗大流量攻击，关注的是流量速率和连接数。SSL 解密的计算密集型操作会严重挤占其攻击检测资源。

上网行为管理 的本职，是识别用户访问的网站和应用，做访问控制和审计。它需要看到 URL 和域名就够了，不应该做完整的 SSL 解密。

负载均衡设备 的本职，是按照既定算法（轮询、最小连接数、源 IP 哈希等）将访问请求均衡地分发到后端的多台应用服务器，确保每一台服务器都不会过载或空闲。它只负责流量的分配调度，SSL 解密和证书管理同样不是它的职责范围。

每一台设备都有自己最擅长的领域。让防火墙去做 SSL 解密，就像让交警去修高速公路，专业不对口，效果自然不佳。换句话说，问题的根源并非设备本身不行，而是它们被要求做了不该做的事。

那么，既然每台设备都不应该承担 SSL 解密的任务，谁来负责这件事？答案其实很清晰：**把 SSL 卸载这件事，从每一台网络安全设备中剥离出来，交给一台专职的 SSL 卸载网关去做，如零信技术的 HTTPS 加密自动化网关**。让所有网络安全设备都不再关心加密、解密和 SSL 证书，只需处理明文流量，做好自己的本职工作。

二、SSL 卸载不该是所有设备都有份的负担

在传统架构下，每一台网络安全设备都要独立完成 SSL 解密，这带来了三重浪费：

第一重：算力浪费。 SSL/TLS 解密，尤其是 TLS 1.3 的密钥交换和国密 SM2 的非对称运算，是计算密集型操作。让防火墙、IPS、WAF、抗 DDoS、负载均衡等四五台设备各自做一遍解密，等于把同一件繁重的工作重复做了四五遍，每台设备的 CPU 都被大量占用，真正用于本职工作的资源反而不足。

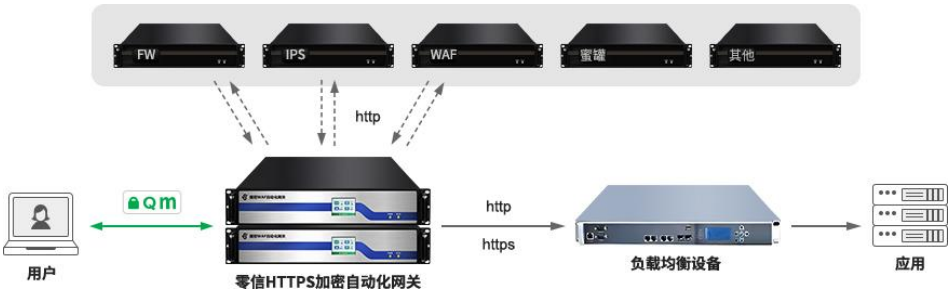
第二重：管理浪费。 每一台设备都需要独立配置 SSL 证书、管理证书生命周期。证书有效期缩短到 47 天后，如果 5 台设备各管各的证书，运维团队每 47 天就要更新 5 张证书，如果每个证书还涉及不同的 CA、不同的算法（RSA、SM2、混合 PQC），工作量将呈指数级增长。

第三重：投资浪费。 当密码算法从 RSA 演进到 SM2、再到混合 PQC 时，每一台安全设备都需要升级固件甚至更换硬件才能支持新算法。这意味着防火墙要升级、IPS 要升级、WAF 要升级，整个安全堆栈全部“推倒重来”，成本高昂且周期漫长。

更关键的是，随着 HTTPS 流量的全面普及，**不解密就看不到攻击，解密又拖垮性能，**安全设备陷入了两难境地。而攻击者恰恰利用这个盲区，将 85%的攻击隐藏在加密流量中，绕过那些无法解密或解密性能不足的安全设备。

三、解决方案：SSL 卸载网关专职卸载，所有网络安全设备回归本职

解决上述困境的正确做法，是在所有网站安全设备之前部署一台**专职的 SSL 卸载网关**（如零信国密 HTTPS 加密自动化网关等），由它统一负责所有加密流量的卸载工作。



SSL 卸载网关专职做三件事：

第一，SSL/TLS 集中卸载。所有入站和出站的 SSL/TLS 加密流量（包括国际 RSA 算法、国密 SM2 算法、混合 PQC 算法以及未来纯 PQC 算法），统一由网关集中解密。网关内置高性能硬件密码卡，解密性能远超任何一款网络安全设备的软件解密能力。

第二，SSL 证书全生命周期自动化管理。 网关通过标准 ACME 协议自动对接 CA 系统，完成双算法 SSL 证书的申请、部署和续期。无论证书有效期缩短到 90 天还是 47 天，全部自动化完成，无需人工干预，更不需要每一台网络安全设备各自人工管理 SSL 证书。

第三，流量智能编排。解密后的明文流量，由网关按照预设的安全服务链，依次调度给后端的防火墙、IPS、WAF、抗 DDoS、负载均衡等设备进行处理。网关支持多种明文流量的输出方式（二层、三层、TAP 镜像等），并具备健康检查机制，可自动屏蔽故障设备、执行 Bypass 逃生，保障业务连续性。

经过 SSL 卸载网关处理之后，后端每一台设备收到的都是**明文流量**。防火墙只管做访问控制，IPS 只管做入侵检测，WAF 只管做 Web 攻击清洗，抗 DDoS 只管做流量清洗，负载均衡只管做流量分配，**每一台设备都回到了自己最擅长的岗位，只做自己的本职工作**。

四、密码算法怎么变，各司其职的原则不变

这套架构的最大价值在于**面向未来的适应性和密码敏捷性**。

国密 SM2 算法已在政务、金融等行业全面落地，零信国密 HTTPS 加密自动化网关早已实现对国密流量的完整支持。后端所有网络安全设备无需任何改动，它们处理的仍然是明文流量，

根本不知道前端已经换成了国密算法加密。

混合 PQC（传统算法+抗量子算法）的部署也已进入快车道，零信 HTTPS 加密自动化网关也已经支持双混合 PQC 算法解密。后端防火墙、IPS、WAF、负载均衡等设备可以纹丝不动，它们处理的仍然是明文流量，PQC 是什么、怎么混合，完全不需要它们关心。

现在，SSL 证书有效期已经从 398 天缩短为 200 天，明年将缩短到 90 天，再接着缩短到 47 天。网关自动完成证书续期和重新部署，后端所有网络安全设备不受任何影响，**它们甚至不需要知道证书换过没有**。

这就是“各司其职”的真正价值：**把复杂的变化隔离在网关层，让后端所有网络安全设备获得永久的稳定性**。密码算法再怎么变、证书有效期再怎么短，只需要升级 SSL 卸载网关即可，整个安全堆栈岿然不动。用户的每一分钱安全投资，无论是防火墙、IPS 还是 WAF，都不会因为算法演进而被淘汰。

让 SSL 卸载网关专职做 SSL 卸载，让防火墙做访问控制，让 IPS 做入侵检测，让 WAF 做流量清洗，让抗 DDoS 做攻击清洗，让负载均衡做流量分配，各司其职，才是真正的专业分工。 这不是某一个厂商的产品策略，而是应对 HTTPS 全面普及、密码算法多元化和证书有效期不断缩短的**必然架构选择**。加密环境再复杂、技术迭代再快，只要守住“各司其职”这一原则，组织的安全架构就永远不会过时。

王高华

2024 年 7 月 28 日于深圳

王高华 Date: 2026.07.28 21:47:20 +08'00'
