山石网科 WEB 应用防火墙 -W 系列 SSL 卸载技术白皮书

随着人类对网上业务依赖程度越来越大，网上购物、网上银行、网上证券交易、网上办公在人们日常生活中显得日益重要。同时，人们对相关应用的数据安全性要求越来越高。这种背景下，SSL 协议技术应用越来越广泛，大大提升了应用的认证安全和数据安全。但是，日益增长的 SSL 通信量也对系统设计者们提出了更高的要求和前所未有的挑战，尤其是大型网站和数据中心的场景中，往往需要同时处理数以万计的安全交易，SSL 的加解密过程需要消耗大量的服务器性能，同时各种网络设备对这些加密内容也会变得难以处理，例如：负载均衡器无法提取用户会话中的 cookies、URL、路径等信息进行细化的分发调度等。所以，要实现高性能的 SSL 处理，涉及到两个方面的改进：一方面通过 SSL 和 TCP/IP 包处理的一体化设计，全面卸除系统负荷，另一方面要将 SSL 数据处理融入新型网络设备，以便于保持与一般网络结构有良好的契合性。

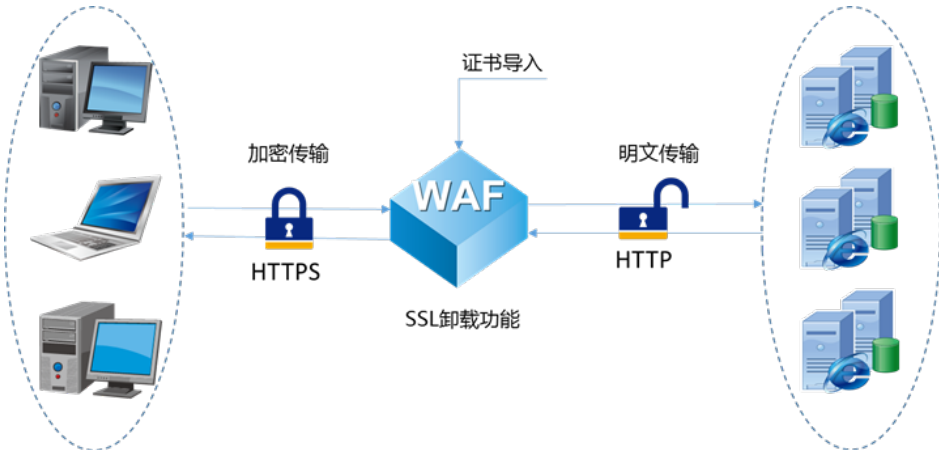
WAF 产品中实现 SSL 卸载功能能够帮助用户有效减少 Web 服务器的负担，从而达到保证安全性条件下得到站点加速的效果。

SSL 卸载技术原理

• 什么是 SSL 卸载技术?

SSL 卸载技术通过将应用访问过程中的 SSL 加解密环节转嫁到相应提供加解密能力的设备上来实现，在满足高并发访问需求的同时，能够降低服务器的性能压力，提升网站的访问速度，一定情况下，能够帮助用户减少服务器的硬件资源，节省运营成本。

• 山石网科 WAF 实现 SSL 卸载的技术原理



SSL 卸载技术原理

• 证书秘钥说明

密钥对包含公钥和私钥，公钥用于加密信息，私钥用于解密信息。管理员在山石网科 WAF 系统中导入 SSL 证书链，证书公钥、证书私钥后，WAF 会解密来自客户端的加密流量，会对来自 Web 服务器的流量加密后反馈给客户端。而 WAF 与后端 Web 服务器之间采用的是明文传输。

某些浏览器不接受公信力不足的机构颁发的证书，此时需要同时使用服务器证书和颁发机构的 CA 证书链。具体做法是将证书链按照从叶子节点到根节点的顺序合并到一个文件中，再将该文件作为证书进行配置。合并时每个文件另起一行，中间不能有空格或空行。

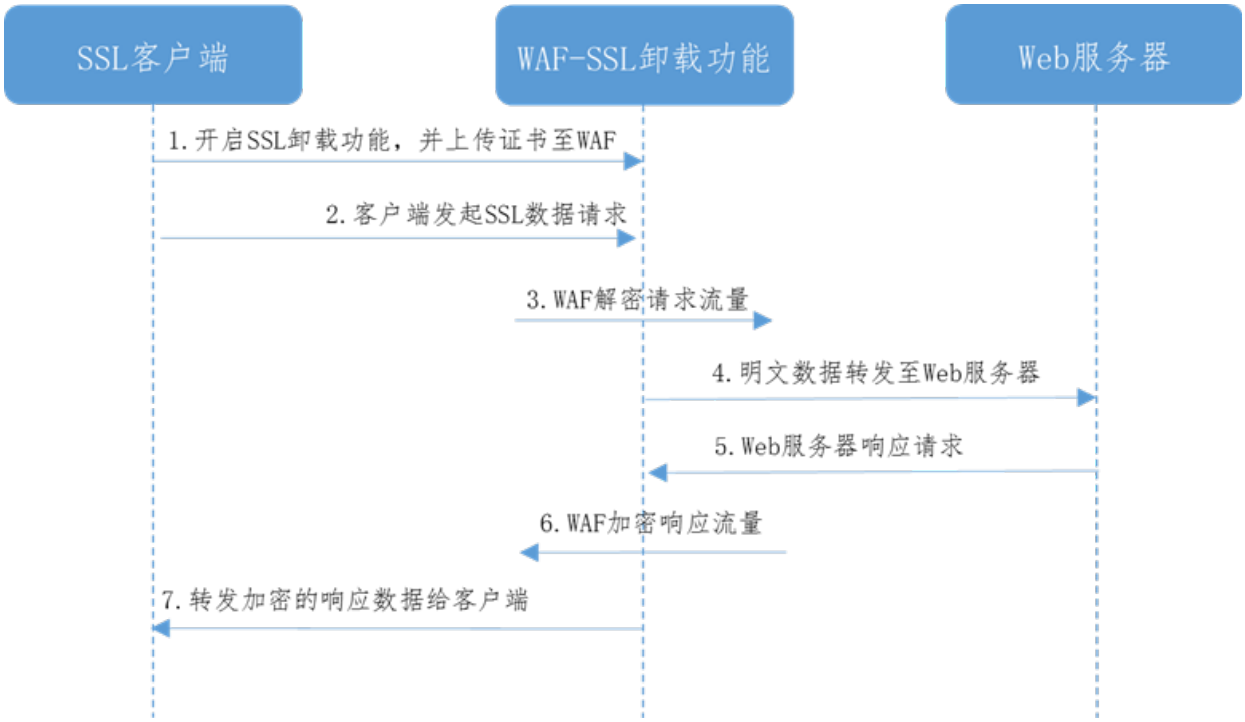
• 多站点支持

山石网科 WAF 中的 SSL 卸载功能支持多站点实现，各个站点可以使用不同的证书，但是如果多个站点共用一个 IP 地址，则只有一个证书会生效，这是 SSL 协议本身特性限制所致。

• 部署要求

山石网科 WAF 的 SSL 卸载功能只在反向代理模式和单臂模式下支持，其他部署模式不支持。功能的配置可以在站点配置的同时实现。

SSL 卸载业务流程



SSL 卸载应用场景

通过 SSL 卸载技术，一般可以为两类用户场景代理不同的解决方案:

场景一：用户需要在已有的网站系统上扩容。随着访问人数的增加，当前使用的 SSL 加密应用的网站访问速度开始变慢，甚至影响了访问者的访问体验。网站提供商的选择要么是增加更多的服务器，要么是通过 SSL 卸载技术来减轻当前服务器压力。

前一种方法虽然能够在短时间内解决性能瓶颈问题，但是随着用户进一步增加，就需要不断采购更多的服务器，导致硬件成本投入越来越大;

后一种方法不需要持续增加硬件投入，能极大介绍投资成本，同时由于没有新增的服务器，所以没有增加额外的运维的投入。

场景二：对于需要新建 SSL 加密应用系统的单位而言，如何规划才能在长期满足不断增加的用户访问需求?有两个执行方案:

方案一就是提前采购足够多的硬件服务器;

方案二则是通过 SSL 卸载技术，仅采购必要的服务器。

相比之下，第一种方案不仅成本投入过高，随着时间的推移，后续的资源扩容仍无法避免；而第二种方案不仅能够节省硬件成本同时满足当前的访问需求，而且，即使后续需要进行硬件扩容，其硬件投资的费用也远远低于方案一，更经济更有效。