服务器 SSL 压力卸载解决方案

——深信服 AD 系列应用交付产品

背景介绍

SSL(Secure Sockets Layer 安全套接层)协议是在互联网上广泛应用于交易安全性保障的一种主导技术。在一般情况下，HTTP 采用明文的方式在互联网上进行传输，但是对于认证口令等敏感信息而言，会存在被非法窃听的风险。为了消除这一方面的隐患，可采用 SSL 协议对 HTTP 协议进行加密（即 HTTPS），以确保在整个数据传输过程中的信息安全性。

问题分析

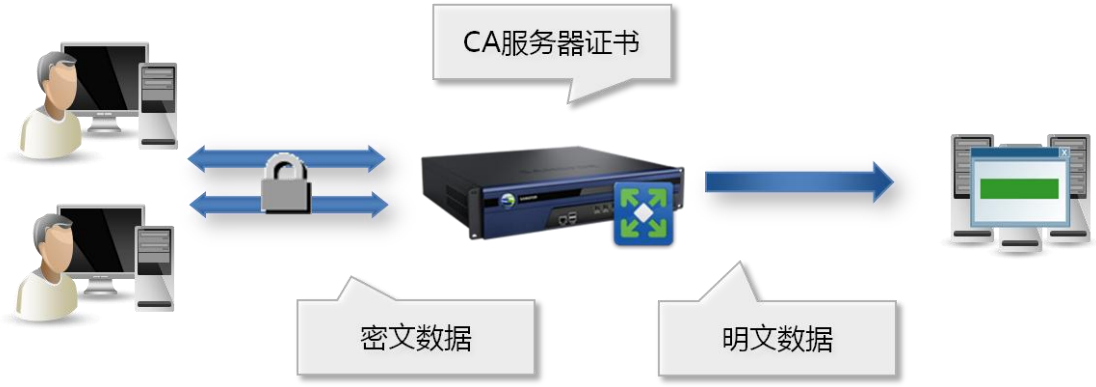
服务器性能过载 - 借助 SSL 加密机制，但凡涉及敏感信息的互联网服务，便可利用数据传输加密来增强其安全性。诸如电子商务、账单支付、纳税申报、股票与证券交易等线上业务，纷纷得以通过互联网实现安全交付。然而，SSL 的联机加密运算不可避免会消耗服务器的处理性能，在相同的硬件性能下，处理 SSL 加密数据所消耗的时间是处理明文数据的 5 倍。一台服务器启用 SSL 加密之后,其性能往往只达到原来的 20%，其余 80%的计算性能都消耗在了 SSL 的加密运算方面。与日俱增的 SSL 通信量 ,将会给网络服务器带来严重的负担。

传统方法的不足 - 为了缓解服务器的性能压力，一度较为流行的方法是安装 SSL 加速卡。但是加速卡对 SSL 数据的处理还是建立在服务器主机之上，并且过分注重于加速 SSL 数据处理，而不是完全卸除系统负荷。随着网络应用的日益丰富、数据流量的迅猛增长、线上用户数量的不断增加，单纯的 SSL 加速卡已经越来越难以胜任。另一方面，SSL 加速卡一般都存在系统兼容性不佳、性能受制于总线技术瓶颈、对主机的依赖性大等问题，越来越无法满足大型应用的需求。

安全管理的需要 - 日益增长的 SSL 通信量已经对系统设计者们提出了前所未有的挑战，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。传统的 SSL 加速卡解决方案在面对如此规模信息处理的时候，显得捉衿见肘。此外，由于 SSL 对应用层数据进行了加密，防火墙和交换机等各种网络设备面对这些内容也就变得难以处理，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。

深信服解决方案

针对 SSL 处理的高性能需求，深信服科技的服务器 SSL 卸载解决方案，通过将应用访问过程中的 SSL 加解密过程转到 AD 应用交付设备之上，一举解决应用系统的性能问题。



整体规划

- 通过 SSL 和 TCP/IP 包处理的一体化设计，全面卸除系统负荷，减少服务器端的性能压力。
- 将 SSL 数据处理融入 AD 应用交付设备，以保持与一般网络结构有良好的契合性，同时保障业务应用的性能优化和安全方面。
- 专业的 AD 应用交付设备具有强劲的 SSL 处理能力，不但能够实现端到端的 SSL 加密，同时支持全面的加密算法配置，并可管理服务器证书。

实现机制

- 配备 SSL 卸载功能的深信服 AD 应用交付设备，可以充当起 SSL 代理服务器的角色，将专用的 SSL 应用程序置于网络服务器的前端，不影响后台服务器主机的 CPU 资源，从而全面卸除 SSL 数据处理的负荷。
- 当客户端发起的 HTTPS 连接，经过 AD 设备处理后，变成明文的 HTTP 数据，即可被 WEB 服务程序（例如 IIS、APACHE）直接读取，无需特殊的驱动程序来传送和接受网络数据。

方案价值

- 利用 AD 应用交付设备对后台服务器进行 SSL 卸载处理，保障通讯数据的安全传输。
- 减少后台应用服务器的性能消耗，显著提升整个业务应用系统的安全性和稳定性。
- 节省应用系统的服务器数量，降低业务系统建设的硬件投资。
- 缩短了用户请求的响应处理时间，提升用户的访问体验。