

# 服务器 SSL 压力卸载解决方案

——深信服 SSL 安全网关系列产品

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，它提供了客户端与服务器之间通讯数据的私密性与完整性。它主要应用于网银、电商业务的支付交易环节，企业核心应用系统的用户认证过程，移动办公的安全接入等场景，确保用户名/密码、网上交易信息的安全性，防止被窃取、盗用。由于 SSL 运算对服务器的性能消耗过大，通常会在服务器前端部署专用的安全网关设备作为代理，通过 SSL 卸载的工作机制进行 SSL 事务的加解密处理，减轻服务器端的性能消耗，让服务器有更多的资源处理应用。

深信服 SSL 安全网关作为应用层代理设备，提供了兼顾安全性与高性能的业务优化解决方案。SSL 安全网关利用 SSL 卸载技术及负载均衡机制，在保障通讯数据安全传输的同时，减少后台应用服务器的性能消耗，并实现服务器集群的冗余高可用，大幅度提升整个业务应用系统的安全性和稳定性。此外，借助多重性能优化技术更可缩短了业务访问的响应等待时间，明显提升用户的业务体验。

深信服 SSL 安全网关具备国家密码局颁发的商用密码产品型号证书，针对公共 SSL 算法的安全隐患问题，原生支持使用国密办 SM 系列算法进行 SSL 加密和认证，为企业和单位的敏感业务系统提供更可靠的安全加固，以满足未来的行业合规性要求。

## 安全结合与管控

- ▶ 对每种应用配置虚拟服务通道所需 IP、端口、CA 信任域及资源访问控制。
- ▶ 支持 HTTP 代理模式，为不需要加密的应用提供透明 HTTP 虚拟服务通道。
- ▶ 支持通过邮件、短信、SNMP TRAP 等途径发送系统故障告警信息。

## 完善的 SSL 卸载功能

- ▶ 支持标准 TLS1.0/1.1/1.2；支持多 CA 信任域、支持多级 CA 证书链；支持单双向认证选择（RSA 与国密）。
- ▶ 支持 SSL 弱算法过滤和算法优先级选择；支持客户端证书信息透传（HTTP Header、Cookie、URL 等方式）；支持设置允许客户端证书最小密钥长度。
- ▶ 支持错误重定向功能（错误类型自定义，低于指定加密强度等）。

## 可扩展负载均衡功能

- ▶ 深信服 SSL 安全网关在提供 SSL 事务卸载功能的同时还可以扩展支持服务器负载均衡功能，保障业务应用的性能优化和安全优化。
- ▶ 支持 HTTP 压缩、连接复用、RAM 高速缓存等功能，进一步释放服务器性能压力。



## 功能列表

### 功能分类

#### 详细指标

#### 部署及管理

支持路由模式、旁路模式（单臂/多臂模式、三角模式）

支持双机热备部署以及多台设备组成集群部署，并支持多种高可用性模式，包括 A/A 模式，A/S 模式，M+N 模式等组合内置告警系统，可自定义告警触发事件，在出现网络及应用系统安全问题时自动发送邮件和短信。

支持全中文管理界面和 HTTPS 方式登录、用户角色管理、多级授权管理；支持 SNMP 管理，SSH CLI，中心端集中管理。

#### 应用负载均衡

支持完善的 L4/L7 内容交换与负载均衡策略，可针对不同的业务应用系统划分配置成多个虚拟服务

支持服务器温暖上线和平滑退出，便于维护管理；支持服务器最大连接限制和并发限制，避免服务器过载

支持基于 SNMP、ICMP、UDP、TCP、DNS、RADIUS、HTTP、数据库(MYSQL/MSSQL/Oracle)及自定义健康检查方式

支持基于 TCP 和 HTTP 的被动式健康检查，通过对业务流持续观测来判定服务器节点是否有效

支持基于 TCP 行为观测的调控机制，当判断出服务器性能不足时对其过载保护，实现应用系统弹性负载

支持浪涌保护，对于超过服务器性能上限的新建连接在负载均衡器上缓存起来放入队列中缓慢发给服务器，不直接丢弃数据

支持图片优化技术，将网页中的图片做优化处理，保证图片清晰度的同时减少图片文件大小，提高传输速率

支持 HTTP 请求/应答改写、HTTP/HTTPS 请求内容匹配、页面跳转、丢弃等高级调度策略

支持 HTTP 压缩、内存缓存、连接复用技术，提升用户访问速度，同时节省硬件投资成本

支持轮询、加权轮询、加权最小连接、哈希、动态反馈、最快响应、UDP 强行负载、优先级等负载均衡算法

支持基于源 IP、Cookie(插入/ 被动/ 改写)、HTTP (Header/ Body)、RADIUS、SSL Session ID 的会话保持技术

支持节点智能恢复，当节点出现故障时，负载均衡能自动重启服务器上的相关进程或重启服务器，使其恢复正常状态并继续提供服务；如无法使其恢复正常，则将其从节点池中移除，保证业务正常访问。

支持用户自定义方式的健康检查，支持多种编程语言（如 Python、Java 等），用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。

通过某种编程语言（如 lua）实现自定义的流量编排，对 TCP、SSL、HTTP 和 HTTPS 等类型的流量进行分发、修改和统计等操作。

支持主动探测方式与被动观测方式结合使用的服务器健康检查手段，以便适应各种复杂应用交互流程，保障业务系统的高可用性。

#### SSL 事务卸载

支持 TLS 1.0、TLS 1.1、TLS1.2 等协议标准。

支持 SM2、SM3、SM4 国密 SSL 加密算法

支持多级 CA 证书链；支持单向/双向 SSL 认证，包括 RSA 与国密

支持各种标准服务器证书申请

支持证书字段的信息透传与过滤（HTTP Header、Cookie、URL 等方式），保持认证一致性

支持设置允许客户端证书最小密钥长度

支持为多种业务应用提供多应用通道，可单独为每种业务应用配置虚拟服务通道所需的 IP、端口、CA 信任域以及资源访问控制等。

支持错误重定向功能，出现错误时通过重定向指定页面告知用户具体错误原因

支持访问控制，根据被访问资源的安全等级决定使用的访问通道的类型（HTTP、单向 SSL、双向 SSL）

支持 LDAP、HTTP、FTP 等方式同步 CRL 证书吊销列表

支持 SNI 拓展特性，可在单个应用上启用多张证书，并可对请求 Host 校验，防止非法访问。



设备型号	SJJ1823	
性能参数	SSL 吞吐量	3Gbps
	SSL 新建 (SM2)	4500TPS
	SSL 新建 (RSA2048)	5000TPS
	SSL 并发连接数	1050000
硬件参数	内存	32G
	高度	2U
	千兆电口	4
	千兆光口 SFP	8
	万兆光口 SFP+	2