
成都思维定制科技有限公司



全球名品-云上安全架构方案

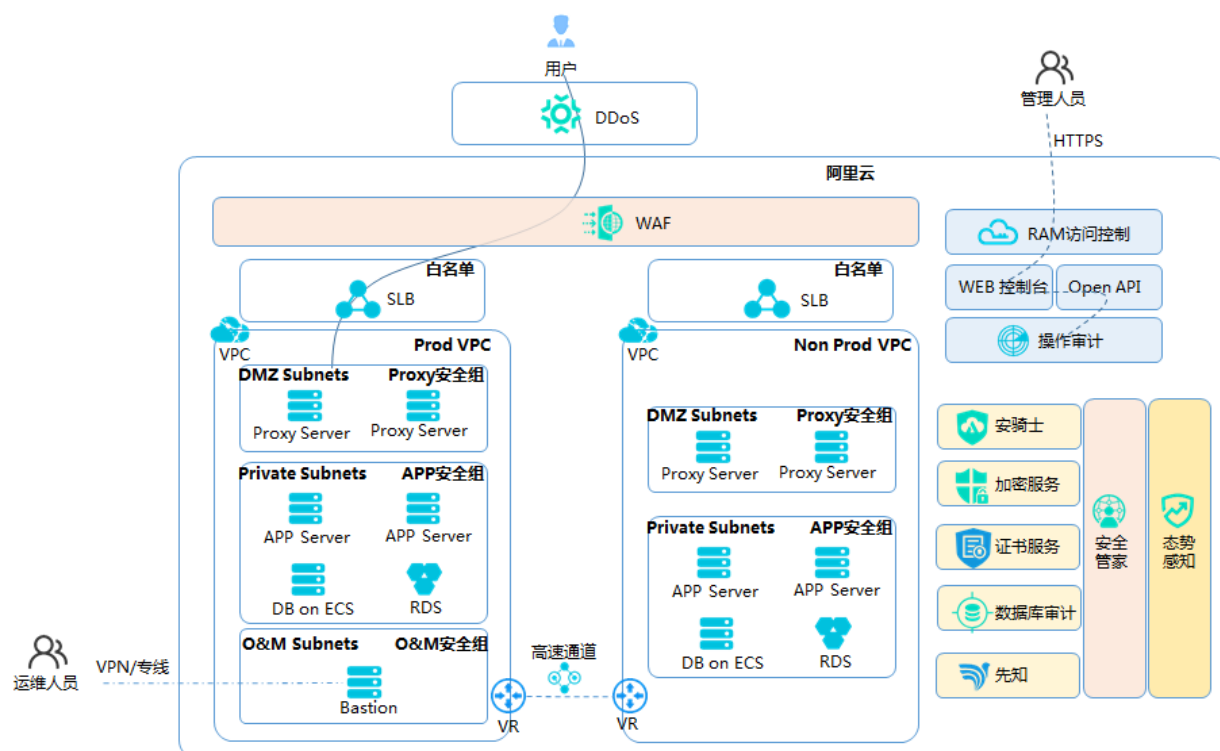
方案提供：成都思维定制科技有限公司

联系人：贺智强

电话：15881188848

2019年8月3日

电商安全产品及安全配置，可从“系统-业务-内容”全方位防护，以完善的云端纵深防御，提高整体的安全性。安全产品及安全机构如下图所示。



- 抗 DDoS 攻击：避免业务因为大规模的拒绝服务攻击而瘫痪，针对不同的 DDoS 攻击场景提供不同类别和等级得防护机制。
- Web 应用防火墙 (WAF)：OSI 的七层网络模型覆盖了所有的互联网的协议，WAF 是确保第七层协议（主要是 HTTP 和 HTTPS）安全的防御机制，而互联网的业务访问大多数是以 HTTP 或 HTTPS 的形式与服务器交互的。网站所有的 HTTP/S 流量都会先经过 WAF，恶意攻击流量在 WAF 上被检测过滤，而正常流量返回给源站 IP，从而确保源站 IP 安全、稳定、可用。
- 入侵防御系统 (IPS)：OSI 的七层网络模型覆盖了所有的互联网的协议，IPS 是确保第四~六层协议（1~2 层由阿里云负责，3 层由自带的安全组功能覆盖）安全的防御机制，如病毒、木马均是作用在这几层的协议上的。网站所有的公网流量都会先经过 IPS，恶意攻击

流量在 IPS 上被检测过滤，而正常流量返回给源站 IP，从而确保源站 IP 安全、稳定、可用。

- 安骑士 (HIPS) : 服务器内部的行为本身并不产生任何网络流量，所以当服务器内部出现异常，或使恶意流量已经达到服务器的时候，服务器入侵防御系统就起作用了。常见的服务器安全事件如病毒木马，勒索软件，挖矿病毒，进程可疑行为，网站后门，主机异常事件，敏感文件篡改，异常网络连接，异常账号，应用入侵事件等。
- 威胁检测：云上安全监控和诊断服务，面向云上资产提供安全事件检测、漏洞扫描、基线配置核查等服务。
- 数据安全：越来越多的企业核心资产成了数据，而越来越多恶意行为的攻击目标也变成了数据，通过数据库审计、敏感数据加密、密钥管理、加密服务等保障核心数据完整、机密、可用。
- 业务安全风控：作用于不针对网络，也不针对系统漏洞，而是针对业务逻辑的攻击。防御的常见威胁如羊毛党、内容违规、接口滥刷、敏感数据爬虫等。
- 其他安全防护/服务：通过渗透测试、应急响应、安全合规、安全培训、安全评估、安全加固、堡垒机等多维安全产品，全方位提高主机、业务的安全性。