长亭科技
CHAITIN

雷池（SafeLine）
下一代Web应用防火墙
产品白皮书

长亭科技


长亭科技
CHAITIN

雷池（SafeLine）

下一代Web应用防火墙

产品白皮书

目录
CONTENTS

满足中国特色云化需求

0day漏洞防护能力

简易上手、快速部署、综合联动

- 典型应用

BOT管理

API防护

DDoS防护

威胁情报

全开放功能接口

- 符合多项国家和行业标准

等保2.0

国产化

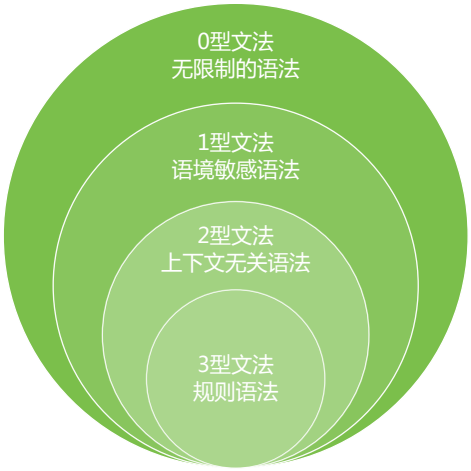
IPv4和IPv6双协议栈

概述

传统规则防护，在当下为什么失灵？

当下，Web应用防火墙大多采用规则匹配方式来识别和阻断攻击流量，但由于Web攻击成本低、方式复杂多样、高危漏洞不定期爆发等原因，管理者们在安全运维工作中不得不持续调整防护规则，以平衡业务的可用性和安全性，却依然面临着不少的误报和漏报，影响正常业务运转甚至导致Web失陷。

究其原因，这是由于基于规则匹配的攻击识别方法存在先天不足导致的。在乔姆斯基文法体系中，编写匹配规则的正则文法属于3型文法（规则语法），而用于构造攻击载荷（Payload）的程序语言属于2型文法（上下文无关语法），如下图所示：



图：乔姆斯基谱系

从文法表达能力比较，3型文法（规则语法）包含在2型文法（上下文无关语法）之内，基于正则的规则描述无法完全覆盖基于程序语言的攻击载荷，这也是基于规则维护的WAF防护效果低于预期的根本原因。

雷池（SafeLine）的解决之道：算法的革新重构WAF

一种算法在被产业主流确定下来后，可以通过一些简单的方式来自我强化(比如增加密钥长度、修补有问题的参数和代码实现等)。但在一定的时间过程内其算法强度随着计算能力和算法分析技术的发展，会让老的主流算法开始力不从心，包括暴露出更多的设计缺陷等等，从而被其他算法取代。

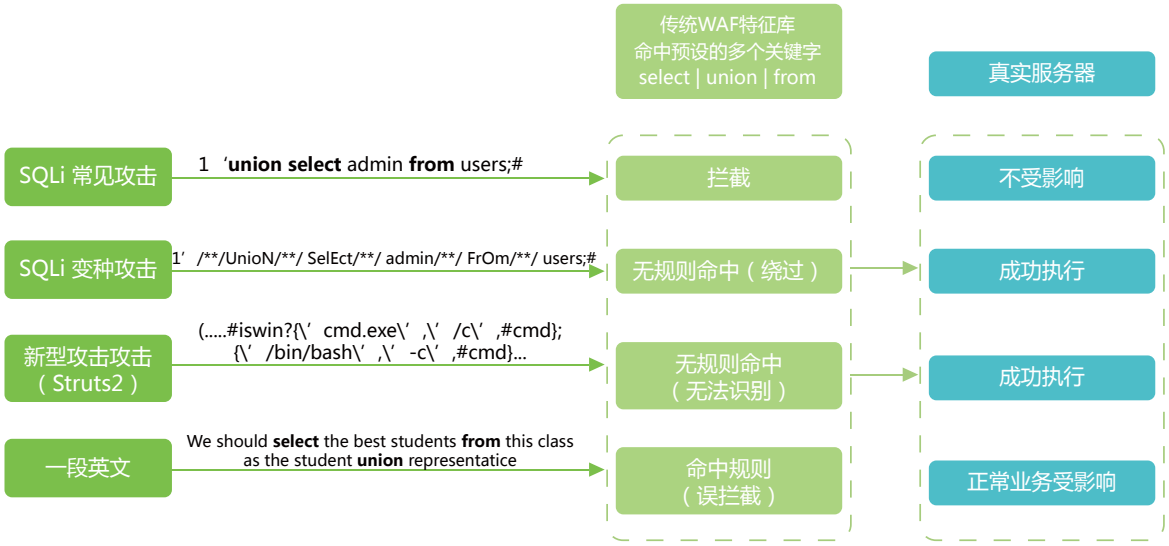
长亭雷池（SafeLine）下一代Web应用防火墙【下文简称：雷池（SafeLine）】就是典型的以算法的革新重构了WAF类产品的能力。长亭科技自成立起便深入探索Web安全防护的新思路，创新性提出以“智能语义分析算法”解决Web攻击识别问题，给WAF内置“智能大脑”，使其具备自主识别攻击行为的能力，同时结合学习模型，不断增强和完善“大脑”的分析能力，不依赖传统的规则库即可满足用户日常安全防护需求。

雷池（SafeLine）通过对Web请求和返回内容进行智能分析，使WAF具备智能判断攻击威胁的能力。智能语义分析算法由词法分析、语法分析、语义分析和威胁模型匹配4个步骤组成。

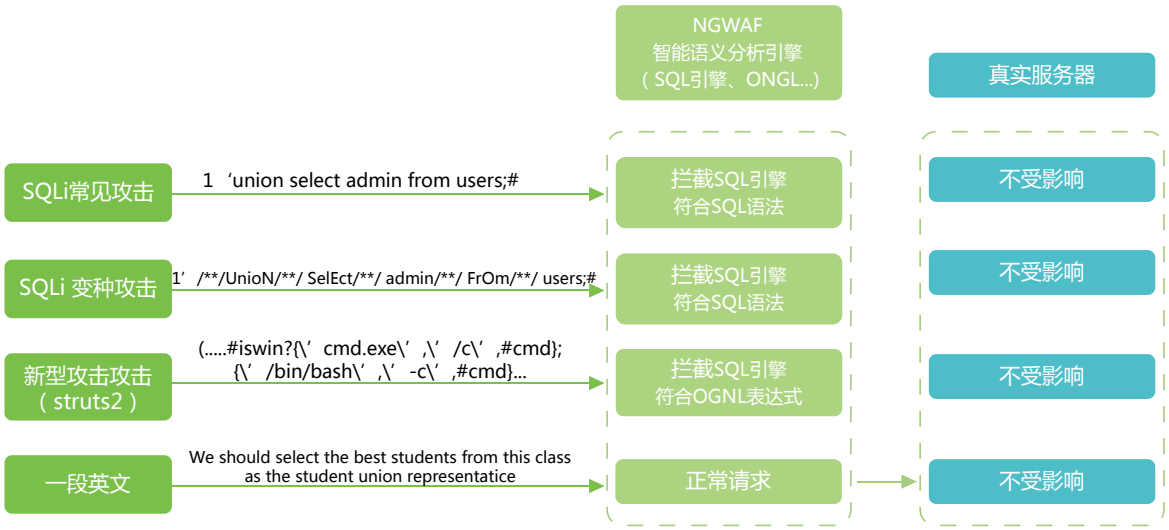
图：智能语义分析算法模型

雷池（SafeLine）内置涵盖常用编程语言的编译器，通过对HTTP/HTTPS的载荷内容进行深度解码后，按照其语言类型匹配相应语法编译器，进而匹配威胁模型得到威胁评级，阻断或允许访问请求。

与规则匹配型威胁检测方式相比，智能语义分析技术具有准确率高、误报率低的特点。以SQL注入检测为例：



图：传统WAF无法检测多种基于上下文无关文法的攻击



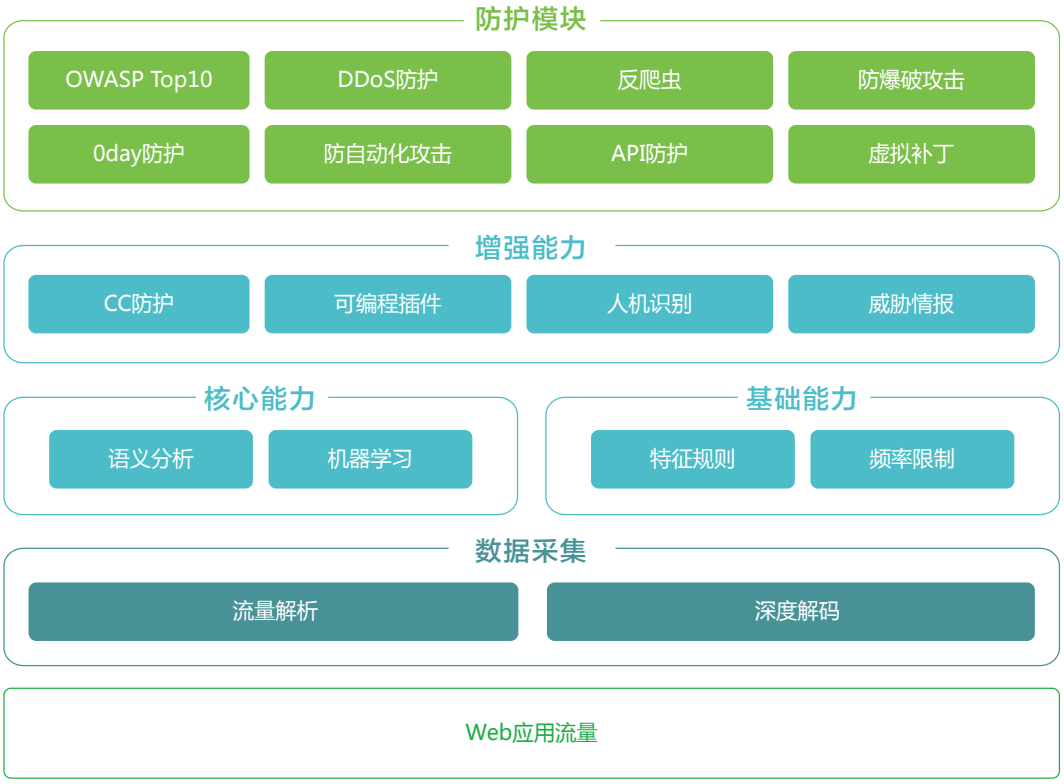
图：雷池（SafeLine）通过综合打分模型能够检测多种基于上下无关文法攻击

作为全球范围内第一款以智能语义分析算法为核心引擎能力打造的下一代WAF，雷池（SafeLine）展现出了更多让安全产品“更聪明”的可能。除了形成了质变的检测引擎的精准程度，它可以通过插件形式灵活扩展、实现瑞士军刀般的功能增加，可以变形适配、安装部署进各种网络环境，可以跟机器学习等前沿技术更好的融合、增强流量分析的能力等。

雷池（SafeLine）下一代Web应用防火墙

雷池（SafeLine）下一代Web应用防火墙，具备以智能语义分析为核心，结合流量学习、访问控制等多种防护技术于一体的攻击检测引擎，具有极少的漏报误报率和优秀的0day防护能力，采用多级熔断和高可用相结合的手段保障业务连续性，具备集群化、容器化等适用多种平台的部署模式，结合BOT管理、API防护、DDoS防护、威胁情报等能力，为用户提供安全、合规、稳定、易用的Web应用安全保障。

产品架构



图：雷池（SafeLine）产品系统架构图

雷池（SafeLine）下一代Web应用防火墙通过接入Web访问流量，进行协议解析与深度解码，调动语义分析、流量学习、访问控制和自定义插件引擎、BOT管理模块、威胁情报信息进行分析，根据预设策略允许或阻断访问流量。

核心功能

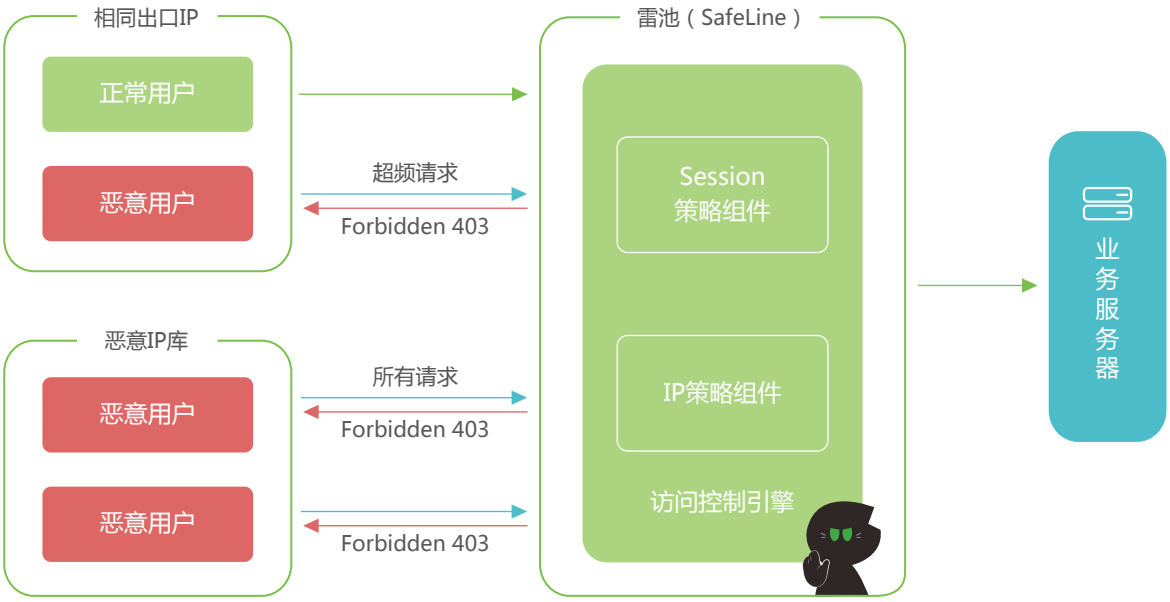
攻击行为智能检测

雷池（SafeLine）具有覆盖OWASP安全风险的智能检测引擎，不依靠传统规则匹配模型，通过智能识别和分析HTTP/HTTPS，发现和阻断安全威胁。

流量学习

雷池（SafeLine）具备基于用户流量特征的分析能力，通过机器学习，对一类请求进行学习，生成基于客户业务流量的特征模型。雷池（SafeLine）将依据特征模型对业务流量进行检测，阻断不符合业务特征的流量访问，有效防范非正常的访问。

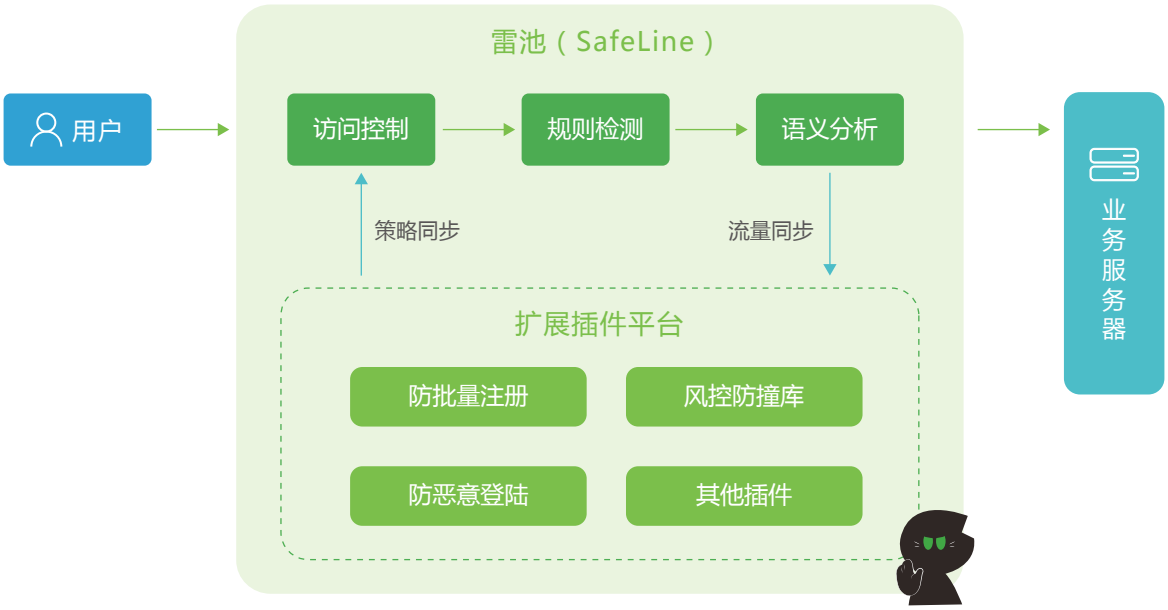
Web访问控制



图：Web访问控制原理

雷池（SafeLine）支持灵活的访问控制机制，内置访问控制引擎，根据源IP、Session来统计客户端访问行为，用户可通过设置针对特定域名、URL的访问频率和IP黑/白名单策略，限制相关源的访问行为。雷池（SafeLine）内置Session系统，可满足不同用户的访问控制需求。

可编程扩展插件



图：可编程插件应用

雷池（SafeLine）提供自定义扩展插件功能，支持Lua脚本语言编写扩展插件，能构建可与用户其他系统互动的业务安全防护体系。通过语义分析引擎检测后的实时流量，调用与业务相关的分析插件，实现与业务逻辑紧密相关的请求处理逻辑，使雷池（SafeLine）成为功能可插拔、信息可推送、流量可分析、应用可调用的灵活智能WAF，适用不同用户各类业务安全防护的定制需求。

部署方式

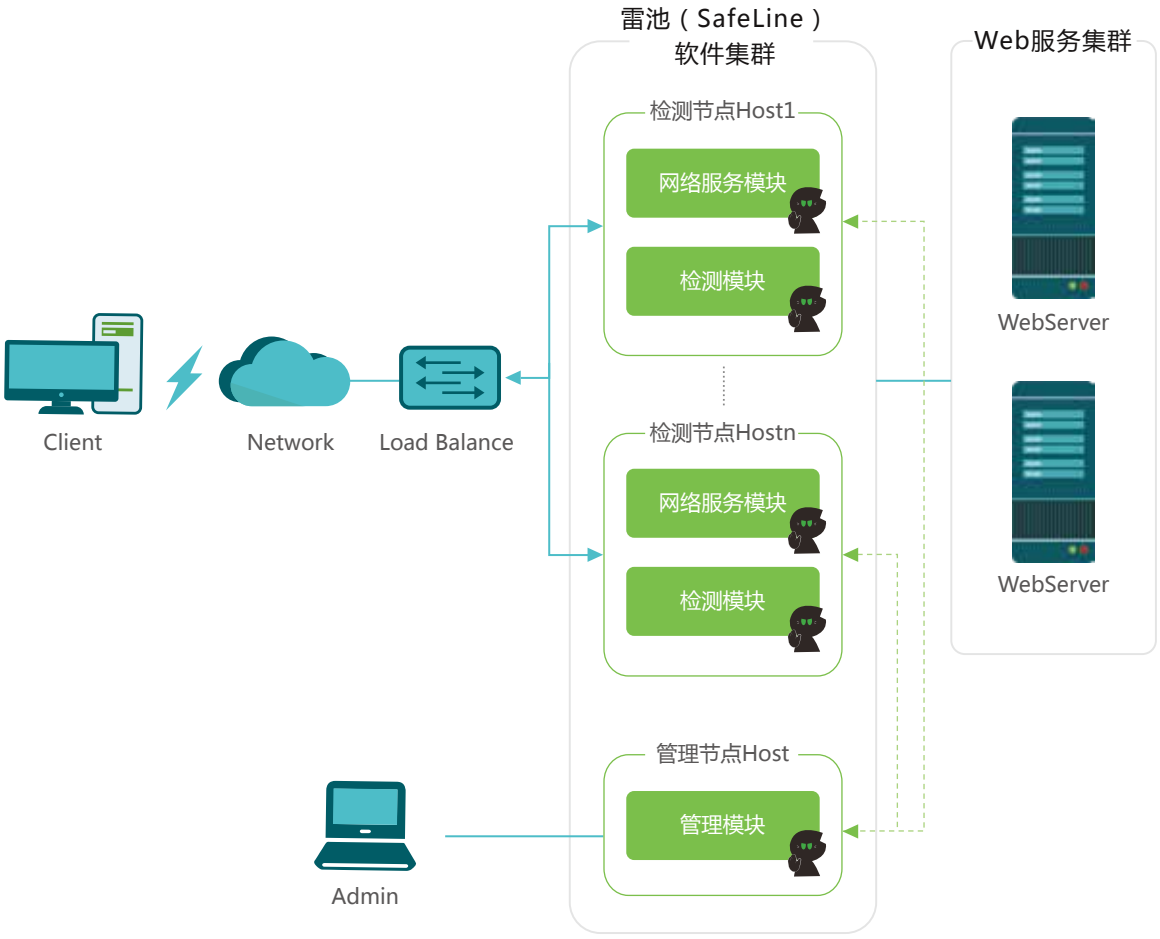
部署方式概览

雷池（SafeLine）具有硬件和软件两种形态，方便在不同用户系统环境中部署。雷池支持各种常规部署模式，例如旁路检测、透明桥、透明代理、反向代理、路由代理、集群反向代理、嵌入式反向代理等。在新的应用环境下，雷池（SafeLine）还支持服务器引流部署方式、Kubernetes编排部署方式等独有的新型部署模式。

类型	部署方式	部署形态	适用场景	特点
常规部署	旁路检测	软件 / 硬件	系统上线测试 防护策略调优 态势感知统筹	不改变用户原有网络架构
	透明桥	硬件	即插即用 可不配置站点 性能最高	不改变用户IP与路由配置
	透明代理	硬件	放过非Web流量 检测HTTP、HTTPS	不改变用户IP与路由配置， 可解析HTTPS
	路由代理	硬件	需记录访问者真实IP	将用户访问源IP传向服务器
	反向代理	软件 / 硬件	保护真实服务器IP 增强防护	隐藏用户服务器真实IP
	集群反向代理	软件	大流量场景	支持弹性扩容 、缩容，水平拓展
	嵌入式集群反向代理	软件	超低延迟的大流量场景	节约虚拟机资源，延迟低
终端部署	服务器引流	软件	客户通过VPN访问	处理VPN无法解密的流量
云端部署	Kubernetes 融合部署	软件	用户业务系统 采用 Kubernetes 编排	可弹性扩容、缩容 与用户业务系统统一编排

典型部署

- 集群反向代理

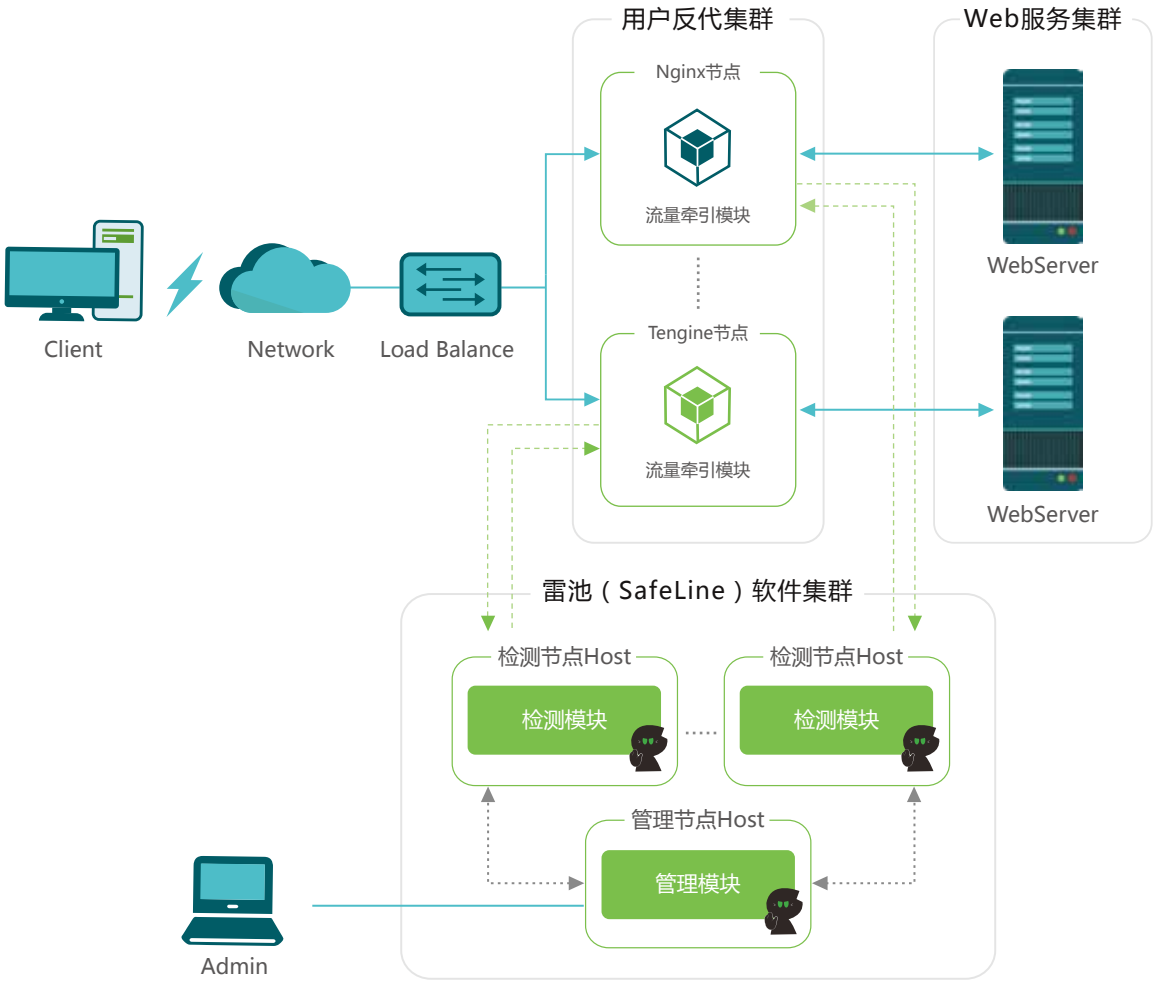


图：雷池（SafeLine）软件集群反向代理

雷池（SafeLine）软件集群模式部署，支持将网络服务和检测模块分布式部署在多个主机节点中，在管理模块统一调度下形成软件集群，通过反向代理模式实现对所有访问请求的检测，并支持对后端服务器的业务负载均衡，同时支持多节点冗余和扩展，保证WAF的高性能和业务高可用。软件集群可部署在公有云VPC环境中，保护部署在公有云环境的Web服务。

该模式具备高性能、高可靠和易扩展等特点，适合用户访问量大、业务并发高等应用场景。

- 嵌入式集群反向代理

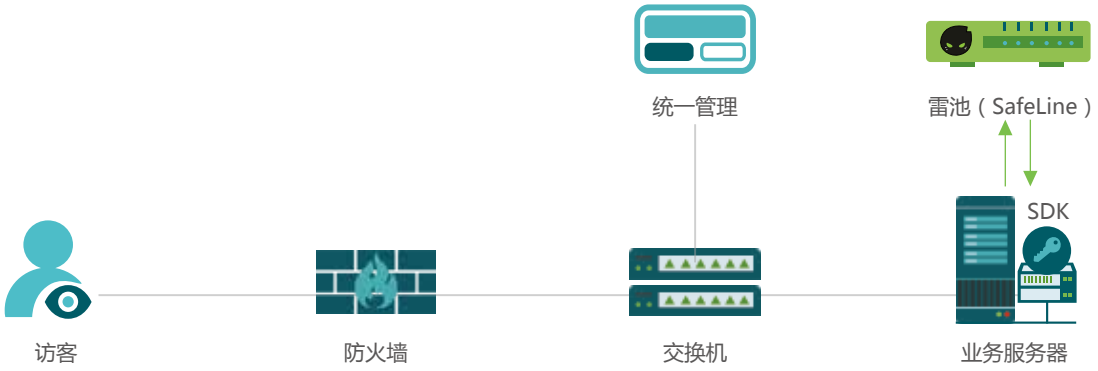


图：雷池（SafeLine）软件嵌入式集群反向代理

雷池（SafeLine）支持嵌入部署在用户已有Nginx、Tengine反向代理集群中，实现物理旁路、逻辑串联的部署模式。该模式需用户Nginx、Tengine集群支持加载动态模块，将雷池（SafeLine）流量牵引SO模块在用户环境中编译后，添加至反向代理集群中，从而将Web访问流量牵引至检测节点中，根据检测结果通知反向代理集群转发或阻断。

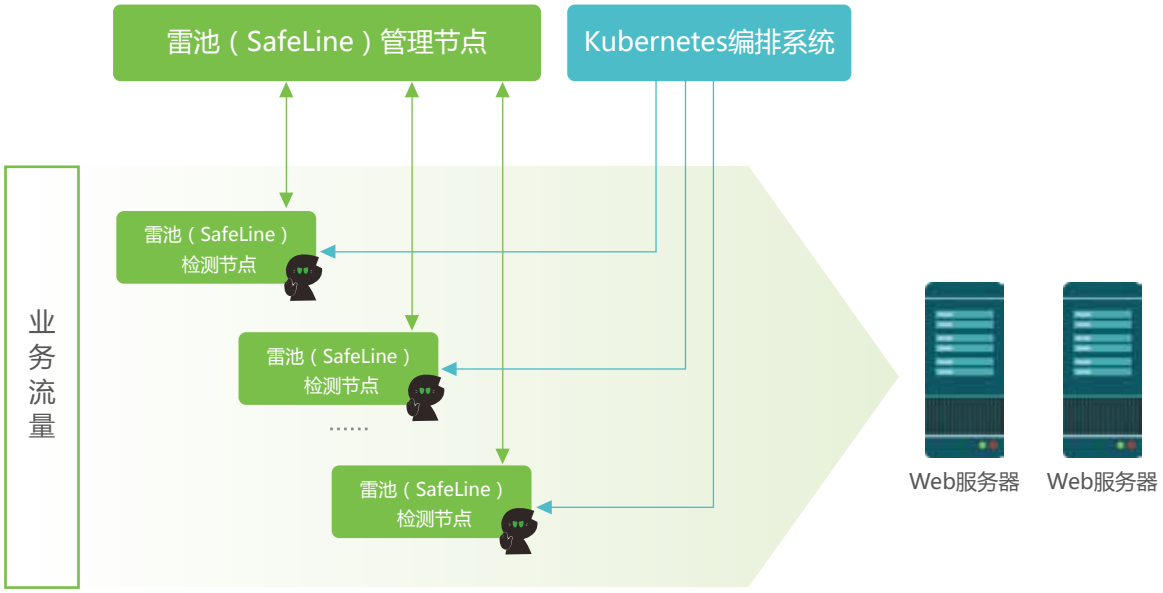
该模式可在不改变原有反代集群模式下实现雷池（SafeLine）的嵌入式部署，适合已建设反向代理集群，且运维管理能力较强的用户采用。

- 服务器引流部署模式



手机银行等带有非国际标准的加密流量或经VPN访问的加密流量的应用场景，无法使用WAF的代理模式进行检测。针对这种场景，雷池（SafeLine）提供了服务器引流部署模式，可以将非标准加密流量解密后再进行攻击检测，防护使用非通用加密措施进行加密的流量。

- 云上部署与Kubernetes统一编排



业务上云和容器化是当前网络服务的趋势，雷池（SafeLine）已经完成容器化实现，可以直接融合进入客户的Kubernetes系统，与客户的业务系统容器进行统一编排。雷池（SafeLine）能够以集群、容器化的方式进行部署，将检测节点以容器的方式，融合到客户的Kubernetes编排系统中统一管理，使得雷池（SafeLine）的检测能力与客户的Web服务提供能力始终保持一致。同时，雷池（SafeLine）也支持多租户的应用模式，可以使各个账户之间的防护策略和规则互不干扰。

核心优势

理解不同行业的业务需求

网络安全产品由于客户业务形态不同，需要具备快速且灵活的策略制定和调试能力。雷池（SafeLine）最早提出“插件市场”概念，以AppStore的理念方式为客户预置多样策略插件，并提供API接口让客户灵活通过简单代码实现最定制化的策略调整，以满足业务的需求。

弹性扩展适配新型应用场景

近年来，新基建带来的流量在逐渐增大，但是传统应用软件型WAF系统多为功能模块组合实现，在上云时仅能安装在一个个单独的虚拟机中使用，导致云平台的自动弹性伸缩等优秀特性很难被发挥出来，因此除了个别拥有大量数据的云服务企业外，没有较成熟的手段结合大数据等新技术能力使传统WAF与云生态深度融合。

雷池（SafeLine）容器化的底层架构，能够轻松实现弹性扩展，在极低能耗的基础上实现高可用、高效率，且能够满足快速上线、灵活增减策略等易用性需求，适配新基建时期云时代大流量、智能计算的应用场景。

满足中国特色云化需求

中国作为互联网超大流量头部公司的聚集地，每天都面临着巨大用户流量、海量

请求的安全问题。WAF作为传统的应用层防护工具，虽然已存在十几年，但已无法满足当前用户的需求。雷池（SafeLine）在与这些客户需求对接时，是当时中国市场上能够满足技术需求的唯一选择。

其次，不同于国外的公有云普及速度，我国存在大量自建私有云、政务云、混合云的需求场景，导致网络环境的架构复杂多样。雷池（SafeLine）灵活的底层架构决定了部署方式的灵活性，在众多客户需求情况下，已具备国内同类产品中最全的部署方式。其中，Kubernetes WAF的部署方式，在当前国际范围内也仅有不超过3家的厂商具备同等能力。

0day漏洞防护能力

雷池（SafeLine）创新性的威胁检测方法摆脱了传统规则型检测方法必须已知攻击和漏洞利用方式才能防御的短板，通过内置各类编程语言编译系统，对攻击Payload进行语义分析，识别其真正意图，依靠威胁模型识别其威胁等级，在面对突发0day漏洞威胁时，同样具备识别和防御能力。

Struts2系列漏洞让整个信息安全行业草木皆兵，雷池（SafeLine）研发团队自S2-045开始对引擎进行升级，完善基于OGNL语言的分析检测算法。当S2-048漏洞爆发时，雷池（SafeLine）无需升级即可拦截利用该漏洞的攻击访问。

威胁模型来自对各类攻击数据的深度学习，对攻击行为特征进行威胁定级，进而建立威胁模型。随着样本数据的增加，威胁模型越来越精准。长亭科技依托自身强大的安全研究团队，使用海量攻击样本打磨威胁检测引擎，并不断更新完善，为用户提供先人一步的防护能力。

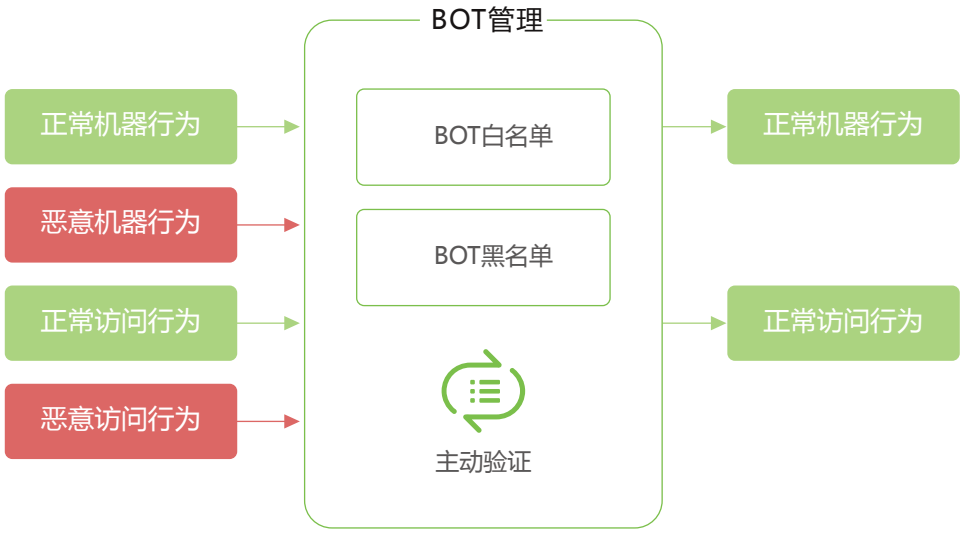
简易上手、快速部署、综合联动

雷池（SafeLine）提供软硬件形态的交付方式，支持旁路、透明代理、路由代理、反向代理等多种部署模式，适合各类部署环境。雷池（SafeLine）产品界面友好，无需维护庞杂的规则库，即可实现站点防护策略配置，同时具备良好的站点资产

管理视角，用户可按照站点灵活选取防护策略。对内，雷池（SafeLine）可以与长亭蜜罐、扫描器、集中管理平台等产品联动；对外，依托Open API，雷池（SafeLine）可嵌入客户安全防护体系，实现安全业务的联动。

典型应用

BOT管理



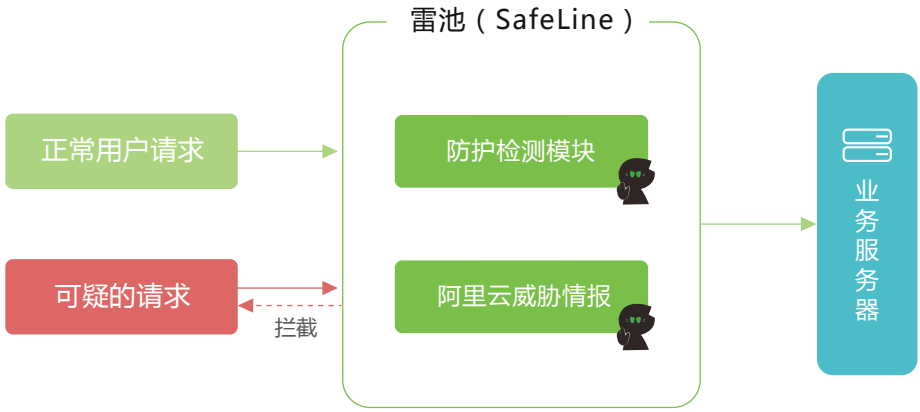
雷池（SafeLine）除了支持解析识别检测请求内容中的攻击行为，以及客户端的超频异常访问行为外，还可以针对发起请求的客户端进行多种主动校验识别，统一管理BOT请求，提高恶意BOT的攻击成本，有效保护业务的正常运营以及数据安全。

API防护

除了针对HTTP/HTTPS的Web应用服务站点的防护外，雷池（SafeLine）也支持针对API的防护，通过防护引擎对API流量进行安全检测，阻断攻击行为，有效的为微服务、物联网提供安全防护。

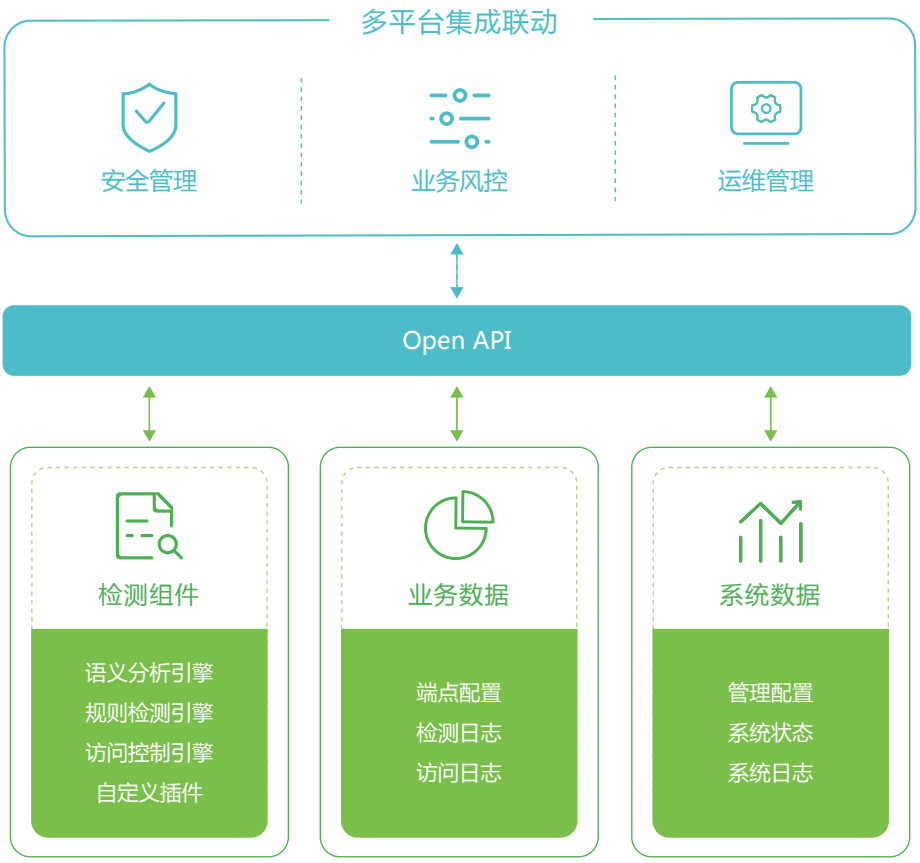
DDoS防护

雷池（SafeLine）支持与云端清洗服务联动，实现对各类DDoS攻击的防御，能够针对服务器资源消耗较大的访问进行重点监控，通过频率统计、人机识别等多种技术，有效保护服务器资源系统不被恶意消耗，保障业务连续性。



雷池（SafeLine）利用云端海量的威胁情报信息资源，结合自身安全防护管理能力进行防控联动，从而实施更多种针对已知风险进行的快速对抗响应措施，同时利用威胁情报查询机制获取更多IP标签信息，提升现有安全解决方案的检测和防御能力，甚至溯源能力。

全开放功能接口



图：Open API 架构

雷池（SafeLine）具备全功能开放接口（Open API），所有页面功能均可通过API实现调用，可通过SOC或SIEM平台调取雷池（SafeLine）检测日志、下发安全策略等，构建多平台、多设备的安全联动，提高安全和运维管理效率。雷池（SafeLine）提供基于REST-ful的标准API接口，可快速融入用户安全运维体系。

符合多项国家和行业标准

等保2.0

从网络安全法到等保2.0，对安全设备、包含安全设备的网络环境提出了一系列的安全要求。雷池（SafeLine）符合规范中对Web应用防火墙的技术要求，能够达

到等保三级建设标准的安全水平，其中包括对登录账户的密码复杂度要求，日志保留达到6个月等技术要求。

国产化

国产化是国家安全的重要战略。雷池（SafeLine）通过适配和验证，已经拥有完全国产化平台型号的版本，能够满足国产化安全可控的要求，保证自身从底层硬件到上层应用的安全控制。

IPv4和IPv6双协议栈

随着我国IPv6下一代互联网技术的快速推进，各个行业均在推动IPv4到IPv6协议的过渡更替。雷池（SafeLine）支持双协议栈技术，同时支持IPv4与IPv6网络协议，能够满足IPv4向IPv6过渡阶段的网络部署需求。

成功案例

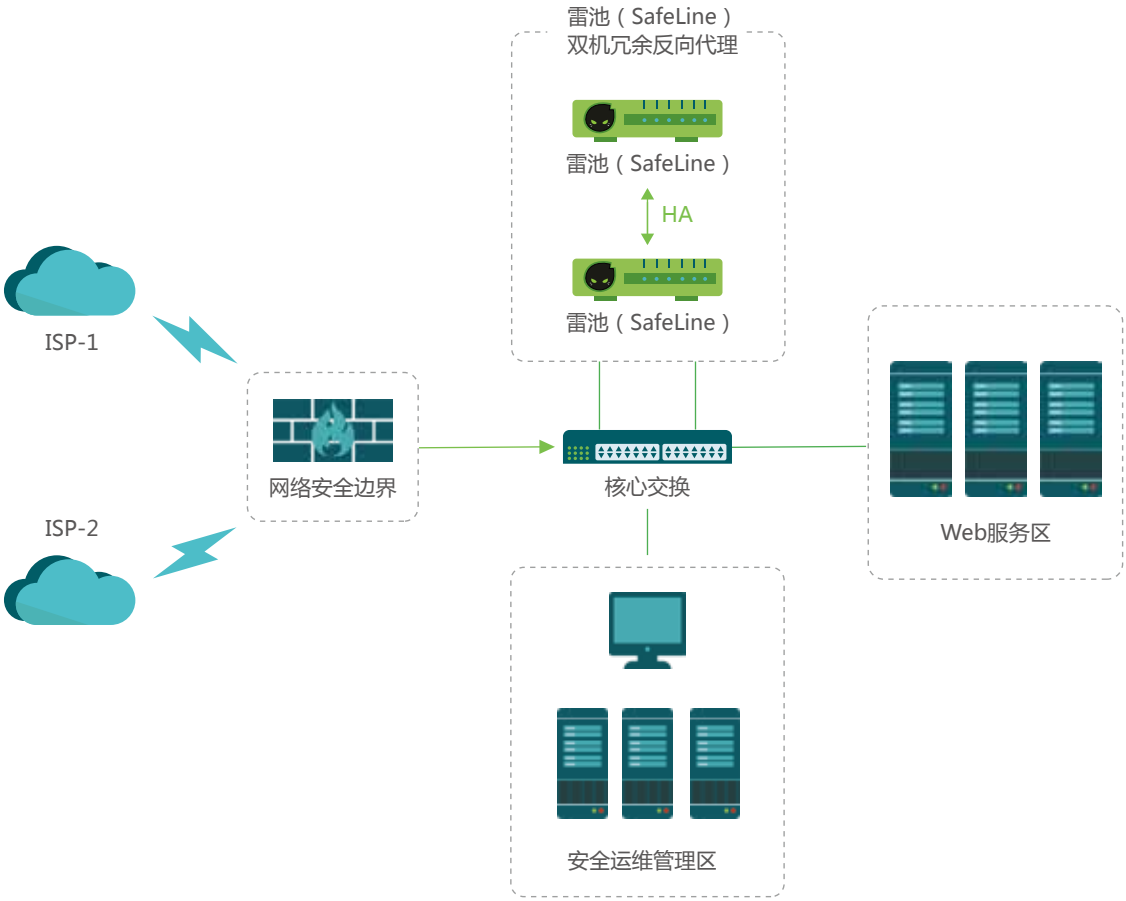
某上市证券公司

用户需求

某上市证券公司依托互联网建设了门户网站、网上营业厅、在线客服等线上应用，部署WAF是为了完善信息安全防护体系，也为了在网络安全形势日益严峻，监管趋于严格的情形下，进一步提升Web应用的防护等级，同时满足等保2.0和金融行业网络安全规范。

解决方案

该企业采用雷池（SafeLine）下一代Web应用防火墙硬件设备，选择硬件反向代理部署模式，部署在Web服务器区外部，实现对Web应用的安全防护。拓扑图如下所示：



图：雷池（SafeLine）硬件反向代理部署模式部署图

采在硬件反向代理部署模式下，Web访问流量经雷池（SafeLine）反向代理至Web服务区，实现实时Web安全防护，同时雷池（SafeLine）采用双机冗余配置，避免单点故障，提供业务可用性。

建设成效

1. 符合监管要求，实现对门户网站、网上营业厅、在线客服等业务系统的实时防护；

2. 安全运维管理系统通过API将雷池（SafeLine）纳入安全运维管理体系，实现运行状态和告警信息的自动上报，提升安全运维管理效率；

3. 协助用户通过了等保2.0的技术测评。

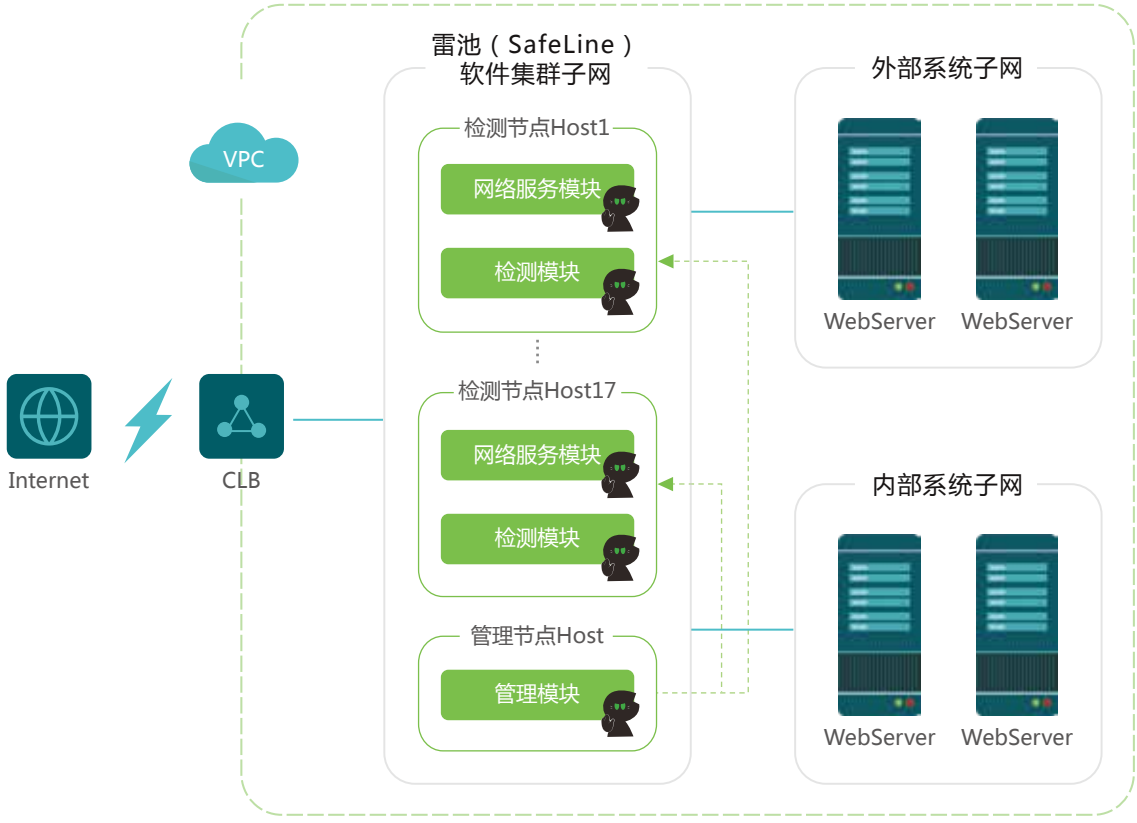
某大型电商平台

用户需求

某电商平台近年来迅猛发展，已成为国内电子商务平台佼佼者，拥有亿级用户群体，每日交易量千万级。该电商平台用户内部网络架构复杂，业务系统繁多，包括内部业务系统、电商网站、商家管理系统、BBS等，希望实现对内外部各类Web应用的安全防护体系，并且纳入安全防护体系，与业务风控等系统实现联动。

解决方案

该企业采用雷池（SafeLine）下一代Web应用防火墙软件集群解决方案，共部署17个检测节点，采用反向代理集群方式，实现Web安全防护，同时紧密贴合业务需求，通过自定义插件实现防“羊毛党”、防爬虫的业务需求。



图：雷池（SafeLine）软件集群反向代理模式部署示意图

建设成效

1. 高效识别Web攻击行为，与现有安全防控体系实现有效联动；
2. 重大活动期间，通过自定义业务防护插件防护“薅羊毛”等异常访问行为；
3. 平均日业务处理量10万QPS，业务稳定性不低于99.9%。

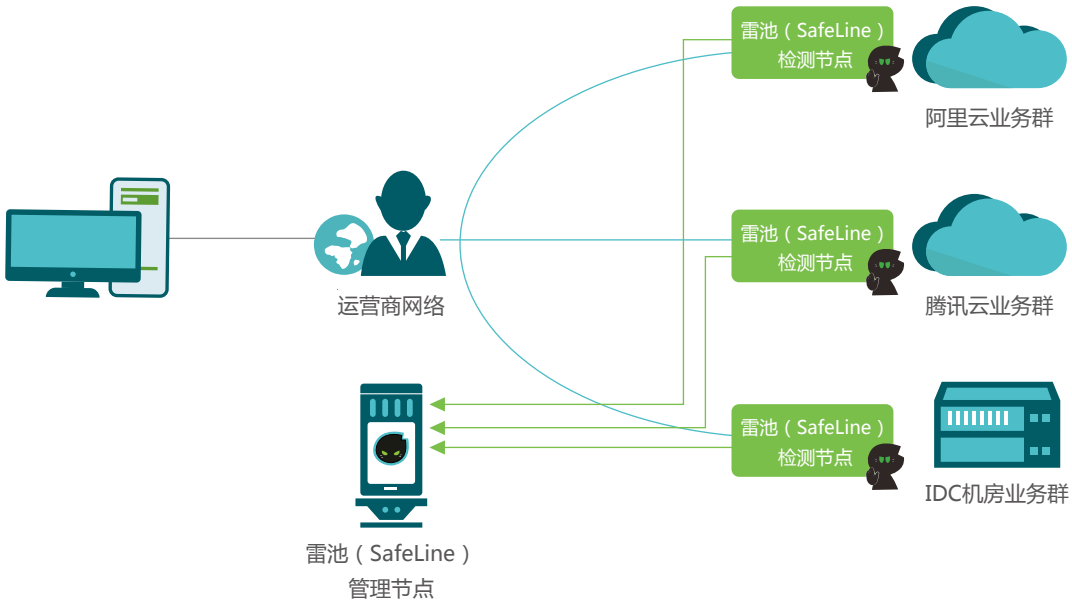
某在线教育平台

用户需求

因为业务需求考虑，某客户的服务器分别部署在阿里云、腾讯云和IDC机房。虽然业务不相同，但是随着该用户的业务范围逐渐扩大，用户希望对WAF能够实现统一管理。

解决方案

该用户采用该分布式集群部署方案，将所有云上、机房的流量统一集中到一个管理中心进行集中防护，采用统一日志分析、策略下发和访问统计，有效防护针对不同服务器的踩点攻击等行为。



图：雷池（SafeLine）分布式集群模式部署示意图

建设成效

1. 通过全业务群联合防护，有效做到统一管理、集中控制，及时发现同一IP对不同业务发起的攻击行为；

2. 减少运维时策略的配置下发和调试工作。


卡亭科技
CHAITIN