密级	公开

知道网站统一防护平台

技术白皮书

KNOWNSEC

知 道 创 宇

北京知道创宇信息技术有限公司

2011-8-11

版本说明

修订人	修订内容	修订时间	版本号	审阅人
金皓	修改	2011-8-11	V1.2	

文档信息

文档名称	技术白皮书	文档编号	
文档版本号	1.2	保密级别	公开
扩散范围			
扩散批准人			

版权声明

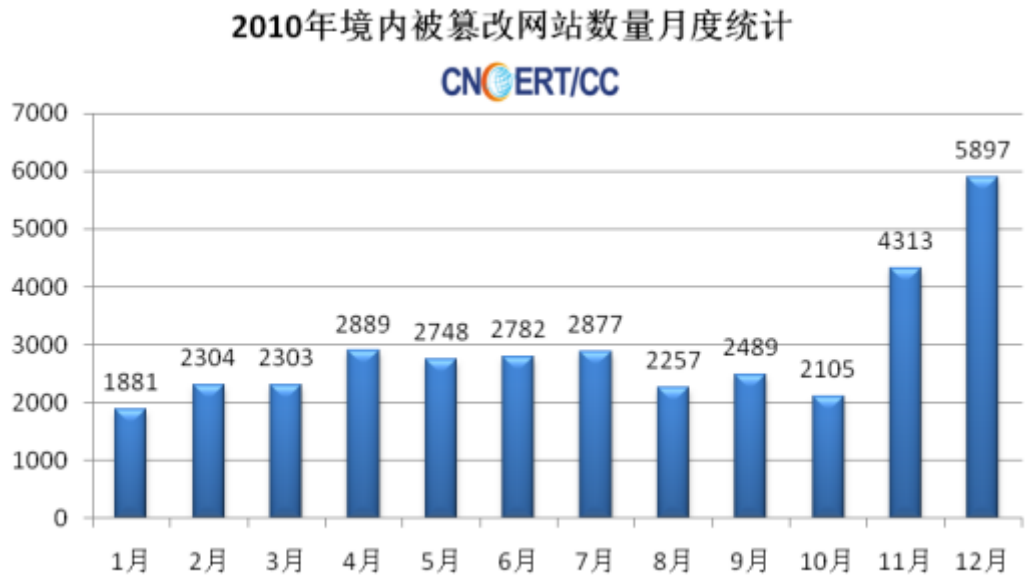
目　录

插图索引

1. 您需要知道

1.1. Web 应用的威胁

CNCERT/CC 国家互联网应急中心的 2010 年度报告及各类统计数据表明，以往的病毒木马感染主机的事件下降 21.3%，而网页恶意代码类、网站入侵类安全事件进入了快速增长阶段，Web 攻击手段正在不断日新月异地升级。



图表 1 2010 被篡改网站数量

目前，利用网上随处可见的攻击软件，攻击者不需要对网络协议有深厚的理解，即可完成更换 Web 网站主页、盗取管理员密码、破坏整个网站数据等攻击。

根据 Gartner 的调查，信息安全攻击有 75% 都是发生在 Web 应用层而非网络层面上，而这方面的投资却只有 10%，也就是防护 25%的攻击却消耗了 90%的投入。同时，数据也显示，三分之二的 Web 站点都相当脆弱，易受攻击，这些攻击可导致声誉损失、经济损失甚至政治影响。

Web 应用安全刻不容缓！

1.2. 传统设备的局限

Gartner 公司的调查显示，目前成功的攻击案例中有 75%发生在应用层。这些攻击这么有效得原因？答案很简单：它们绕过了过去 10 年安全人员实施的所

有以网络为中心的控制措施，如防火墙、IDS、IPS。

1. 传统防火墙

传统防火墙工作在 OSI 模型的三、四层，不能理解 HTTP 协议所承载的数据，也无从判断对 Web 应用服务器的访问行为是否合法，防火墙完全向外部网络开放 HTTP 应用端口。

以 Web 应用攻击为例，传统防火墙为了保护 Web 服务器所包含的规则是通过阻止所有非预期数据流，仅允许流量通过 80 和 443 端口。不幸的是，防火墙不能区分出 80 端口中的哪些数据流是预期数据流，哪些是非预期的。

2. IDS/IPS

入侵检测系统作为防火墙的有力补充，加强了网络的安全防御能力。但是，入侵检测技术使用消极防御模型，基于已知漏洞和攻击行为形成特征进行比对从而实现的防护，需要预先构造攻击特征库来匹配网络数据，对于未知攻击和不能有效提取攻击特征的攻击，入侵检测系统不能检测和防御。对于应用攻击，入侵防御系统可以有效的防御部分攻击，但不是全部。

3. 网页防篡改

网页防篡改对攻击行为并不进行分析和识别，属于事后缓解攻击危害的产品，不会阻止攻击的发生。

1.3. 解决之道

为了应对 Web 应用安全威胁的高成本、难以提供简单有效防御多变攻击的困境，可以使用威胁模型（threat modeling）来识别和评估应用程序的风险，以三大关键风险为例，比较好的处理方式有：代码审计、漏洞评估和 Web 应用防火墙（以下简称 WAF）产品。

WAF 被设计用于处理所有常见的 Web 应用安全威胁，即保护以 HTTP/HTTPS 相关应用协议为基础，运行在 OSI 第七层（应用层）的 Web 应用

在线业务。WAF 真正实现了对网络应用的保护，是传统安全技术的有效补充。传统安全设备阻挡攻击者从正面入侵，着重进行网络层的攻击防护；而 WAF 着重进行应用层的内容检查和安全防御，与传统安全设备共同构成全面、有效的安全防护体系，并着重为用户提供以下功能：

1. 安全防护管控体系

提供区分攻击行为类别的多种防御引擎、对攻击行为进行针对性的事件处理策略配置、定义具体攻击行为的匹配规则定制，对已知和未知的 Web 攻击进行全面防护，将攻击行为的细节直观、详尽地展示给用户，达到防护、管控 Web 应用业务安全的目的。

2. 方便有效网管运维

在安全防护能力给 Web 应用的安全性带来保障的同时，也为 Web 应用复杂的网络管理、日常运维带来快捷和便利，能够实时了解网站可用性状态、安全性状态、客户端访问流量、客户类型和地域分析、服务器承载压力；能够对网站提供负载均衡加速、缓存页面加速、数据压缩加速，使 Web 应用完全发挥其最大性能。

3. 满足行业/国家标准、通过安全审计

随着安全问题的不断浮现和社会影响的深化，Web 应用的安全性越来越受到人们的重视和关注，由此促进了部分行业的安全标准制定，如 PCI-DSS 标准要求；国家公安部、国务院下发的指示。

WAF 可协助 Web 应用程序满足相关的安全性要求，确保在线业务安全、合规地运作，帮助客户通过安全审计。

对于面向公众的 Web 应用程序，经常解决新的威胁和漏洞，并确保保护这些应用程序不受到以下任一方法的攻击：

通过手动或自动应用程序漏洞安全评估工具或方法检查面向公众的 Web 应用程序，至

少每年一次并在所有更改后进行检查。

在面向公众的 Web 应用程序前端安装 Web 应用程序防火墙。

摘自支付卡行业 (PCI)数据安全标准(DSS)1.2 版本

全面检查，切实解决政府网站管理中的突出问题

各地区、各部门要对本地区、本部门政府网站进行全面检查，重点检查以下内容：一是网站页面能否正常访问，各栏目及其子栏目内容是否及时更新；二是信息发布审核和保密审查机制是否健全；三是网站提供的各项服务和互动功能是否正常；四是网站链接是否经过管理单位审核把关，是否存在错链和断链；五是网站安全防范工作是否到位，是否采取了防攻击、防篡改、防病毒等安全防护措施，并制订了应急处置预案；六是网站管理单位和运行维护单位职责是否明确。对检查清理中发现的问题要及时整改，确保上网信息准确、真实，不发生失泄密问题，确保公众能够及时获取政府信息、获得便利的在线服务，确保链接正确有效、网站安全平稳运行。对确实无力管好的网站或栏目，要果断予以关闭。

摘自国办函〔2011〕40 号

2. 您可以选择

在您购买产品之前，需要明确 WAF 不是简单地放在应用服务器前面的组件，为了选择合适的安全设备，您需要回答几个问题：

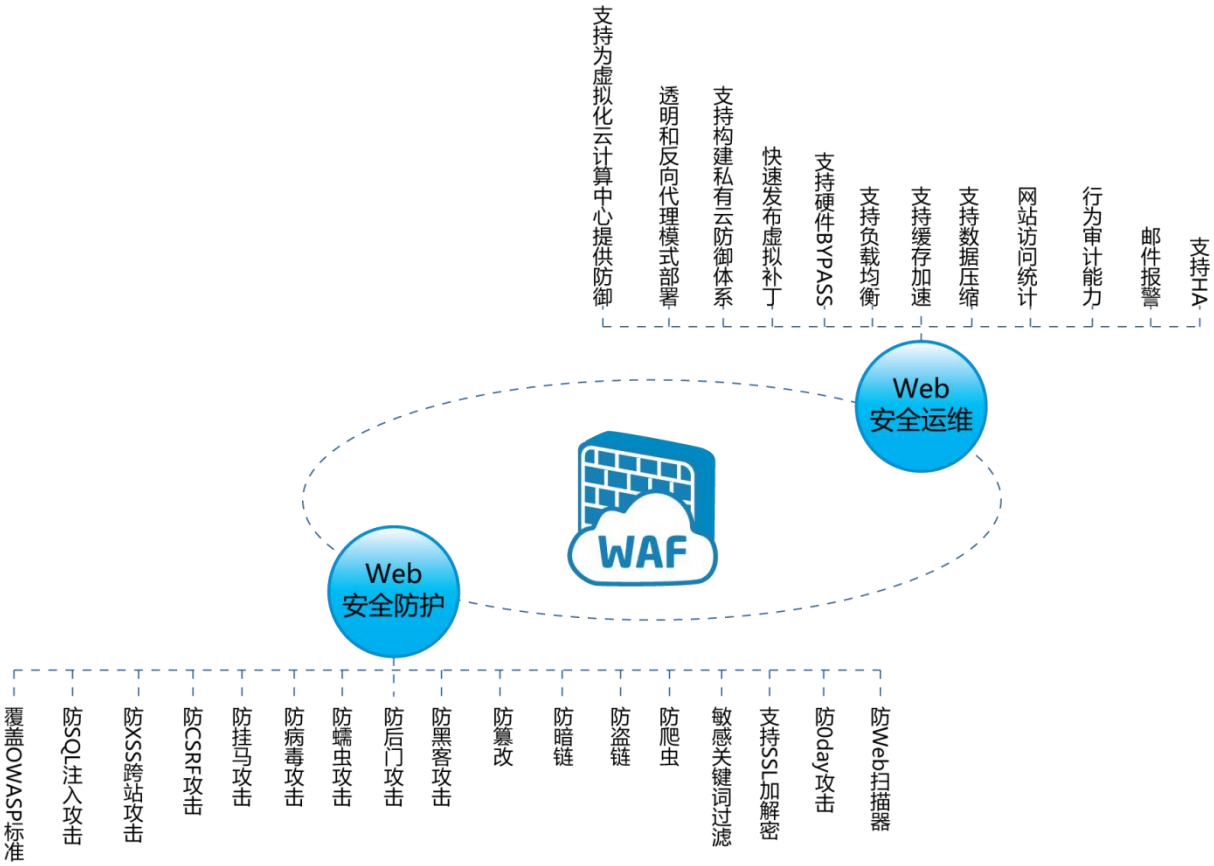
1）根据您的安全政策目标或者合规性需求，该产品需要做什么？

2）它怎样才能融入到现有网络？

3）有哪些有价值的附加收益？

针对以上问题，知道网站统一防护平台（以下简称知道 WAF、KS-WAF）为您提供了一些选择。

2.1. 产品需要做什么

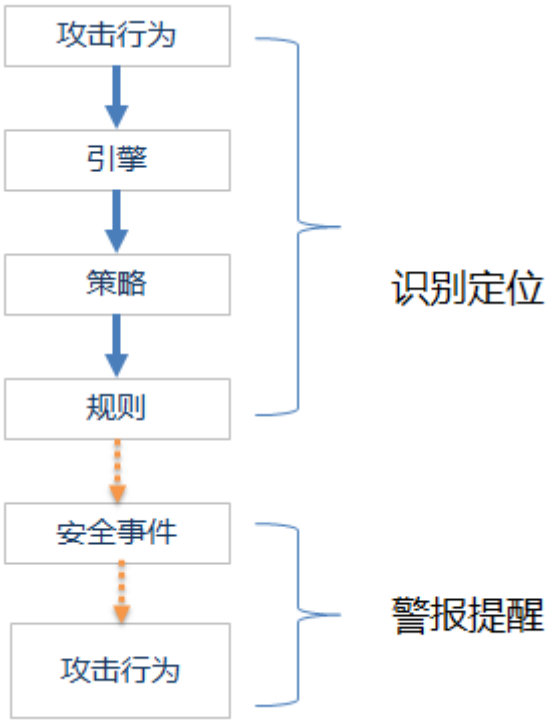


图表 2 双维度防护体系

KS-WAF 构建的双维度保障体系，针对 Web 安全防护和 Web 安全运维两大方面提供安全的保障。

2.1.1. Web 应用安全防护

KS-WAF 针对用户所面临的安全问题，监控 HTTP/HTTPS 双向流量，通过防御引擎、防护策略、行为规则的多层次安全防护模型分析来识别定位攻击行为，提供便捷有效的全方位防护功能，充分保障 Web 应用的安全性和高可用性、连续性。



图表 3 安全防护模型

1. 防攻击

防攻击功能主要关注黑客攻击 Web 应用并试图入侵网络服务器的攻击事件过程。全面覆盖 OWASP TOP 10，如 SQL 注入攻击、XSS 跨站攻击、CSRF 跨站请求伪造攻击等。

在事前，“SQL 注入漏洞防护策略”、“XSS 跨站攻击防护策略”、“Web 应用缺陷防护策略”可避免黑客进行攻击前的安全性测试；事中，“URL 权限控制策略”可中断攻击行为，阻止每个恶意请求，“上传文件限制策略”可阻止黑客通过非法手段上传恶意程序，“Web 应用缺陷防护策略”持续对抗攻击行为；事后，

“后门检测策略”可发现成功入侵的痕迹，通过“URL 权限控制策略”限制黑客无法再次通过管理后台、后门进行入侵。

图表 4 攻击事件防护示意图

2. 防泄露

KS-WAF 可对其中的敏感信息、服务器信息进行屏蔽或伪装，达到避免数据泄露的隐患。成功的攻击往往需要利用服务器的 IP、操作系统信息、应用信息、服务器出错信息、数据库出错信息，KS-WAF 接管所有返回给客户端的信息，并可中止会话，避免黑客利用敏感信息及服务器信息发动社会工程学攻击、各类黑客入侵攻击。

3. 防暗链

系统内置了针对当前流行的暗链攻击建立的恶意指纹库，在服务器端已被植入暗链的情况下可准确识别并进行报警，协助管理员清除暗链代码。

4. 防盗链

KS-WAF 通过实现 URL 级别的访问控制，对客户端请求进行检测，如果发现图片、文件等资源信息的 HTTP 请求来自于其它网站，则阻止盗链请求，节省

因盗用资源链接而消耗的带宽和性能。

5. 防爬虫

KS-WAF 将爬虫行为分为搜索引擎爬虫及扫描程序爬虫，可屏蔽特定的搜索引擎爬虫节省带宽和性能，也可屏蔽扫描程序爬虫，避免网站被恶意抓取页面。

6. 防挂马

通过检查 HTML 页面中特征、用户提交数据，查看是否出现 IFrame 、Javascript 引用挂马源 URL 及其他挂马特征以决定是否拦截请求。

7. 防篡改

将静态页面 Cache 在 KS-WAF 中，当管理员确认自己修改了自己的网站，再到“云接入服务器”上手工点击“刷新网站 Cache”按钮重新载入网页。通过此方法提供防篡改功能。

8. 防 Web 扫描器和黑客工具

利用网上随处可见的扫描器或者攻击软件，攻击者不需要对网络协议有深厚的理解，即可完成更换 Web 网站主页、盗取管理员密码、破坏整个网站数据等攻击。

KS-WAF 可以屏蔽 Web 扫描器的检测，如：Acunetix Web Vulnerability Scanner，也可以防护黑客工具的检测，如：Pangolin。

9. 抗拒绝服务

支持网络层、应用层的拒绝服务攻击，通过简单有效的方式缓解拒绝服务攻击。

2.1.2. Web 应用安全运维

运维人员需要监控保障 Web 应用的健康稳定运行，KS-WAF 不仅提供安全防护功能协助确保 Web 应用的业务不受入侵和中断，在此基础上还实现了 Web

应用的便捷管理、优化、合规运作功能。

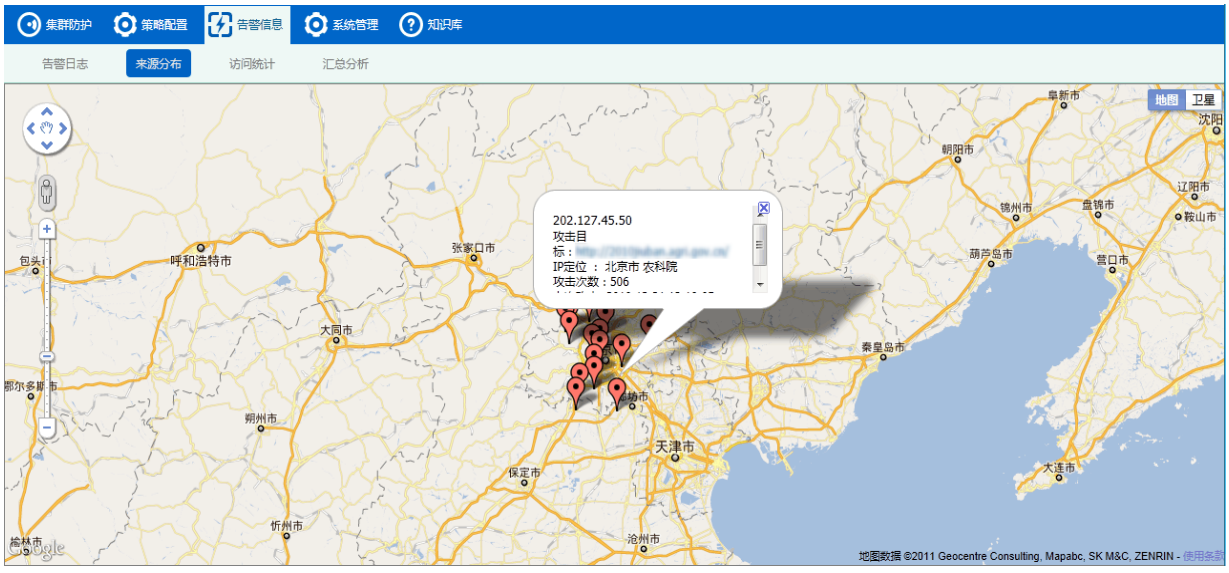
KS-WAF 针对运维过程关注的带宽资源、服务器计算资源、客户端请求分析统计提供便捷的网管运维功能。

1. 行为审计

研究分析表明，90%以上的网站缺乏行为分析的意识及手段，网站运维人员对于：“网站有多少用户访问？”、“网站是否遭到过攻击或扫描？”、“用户更关心你的哪些内容？”、“用户一般在什么时间段访问你的网站？”等问题时，无从回答。在网站管理者越来越关注这类数据的时候，KS-WAF 可以提供专业的结果和数据关联分析。

2. 攻击源定位

通过记录攻击者的源 IP，并在在线地图中进行定位，帮助运维人员分析攻击来源。



图表 5 攻击事件定位示意图

3. 过滤敏感词

KS-WAF 内置低俗、政治类别的关键词库，并可自定义敏感关键词，规避由于开发性高的 Web 应用带来的不可控风险。

4. 快速发布虚拟补丁

Web 应用安全问题的本质源于软件质量及配置管理的不足。KS-WAF 的安全防护管控体系可发现并有效解决部分脆弱点，而软件质量还可能是由于业务需要而开发的功能设计不够严谨，可被利用作为安全漏洞进行攻击。Web 应用的开发一般会处于频繁变更、临时修改而导致无序的开发周期，并且会出现经常更新换代、上线交付后无人维护的问题。

据统计，每 1000 行代码就有约 15 个严重的安全漏洞，最普通的安全漏洞需要 75 分钟来诊断以及 6 个小时来修复，而一般的商业应用程序大致有 150,000-250,000 行代码，仅仅用于修复代码的时间，就需要 562.5 天-937.5 天，修改代码的代价太大。

针对 Web 应用的发布窘境，KS-WAF 可自定义针对 Web 应用漏洞的规则，基于接管所有访问请求，无需开发团队重新修改 Web 应用源代码即可通过“打补丁”的方式快速解决开发时无意制造的漏洞。

5. 缓存加速

支持对所有网页进行缓存，在多个客户端请求同一个资源时，KS-WAF 可作为前端缓存服务器的角色，将该资源的请求结果缓存至系统中，直接为客户端发送未过期的缓存资源，通过智能计算资源过期时间，在资源缓存期间，只需为客户端转发一个请求给服务器端，节省重复请求 Web 服务器资源导致带宽、计算资源的消耗。

6. 数据压缩

支持对服务器端返回页面进行压缩，可有效节省带宽同时提升吞吐率。

7. URL ACL

KS-WAF 实现了 URL 级别的访问控制，可针对需要保护的 URL（如管理后台登陆入口）进行来源限制，避免未授权访问。

8. 负载均衡

在 Web 应用面临大量请求压力时，KS-WAF 可作为多台前端负载均衡节点，缓解 Web 应用的请求压力。

9. HA

Cloud WAF 支持集群部署，形成具备高容错（HA）机制的集群防护。

10. 零接入

通过修改 DNS，KS-WAF 可实现零接入方式，不会增加运维人员的部署实施、后续管理的工作，可无需改变已有的机房网络拓扑结构、无需接入硬件设备达到安全防护的目的。

11. 集中管理

使用 KS-WAF 可帮助在管理多个 Web 应用时，集中统一在系统中完成安全防护、网管运维工作，减少管理成本。

12. 汇总报表

汇总报表提供从整体进行管理分析的视角、也提供体现工作价值供业绩考核。KS-WAF 不仅提供实时的事件警报，并将所有数据自动进行汇总分析，为网管运维工作提供便利。

13. 实时告警

实时告警将还原安全事件的场景和攻击行为细节，并支持线上线下的警报，及时告知最新事件信息。

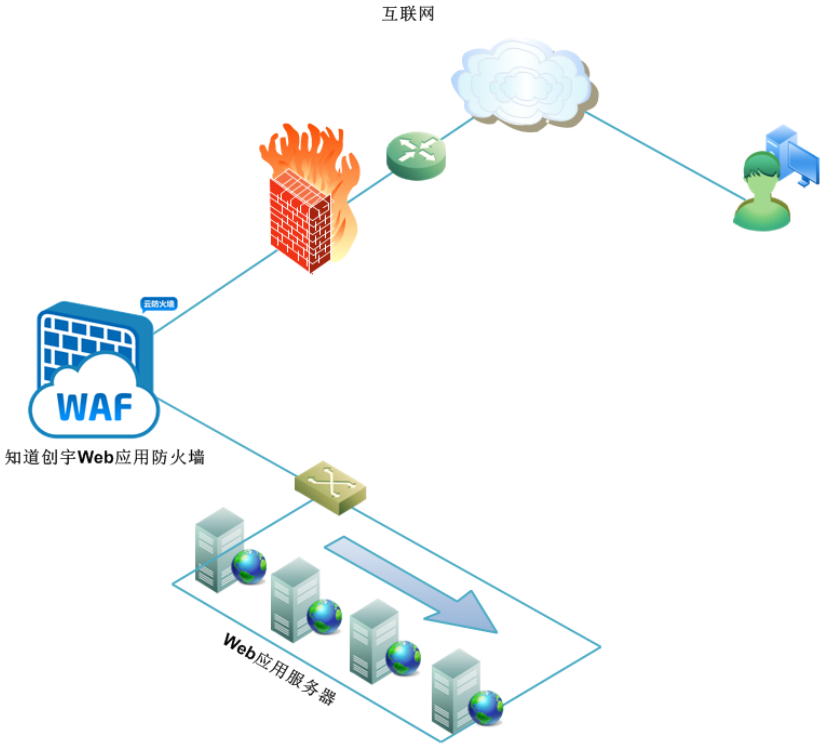
2.2. 如何融入现有网络

KS-WAF 支持两种部署模式：透明模式和反向代理模式。透明模式部署更加简单方便；而反向代理模式则比较灵活，只需修改 DNS 指向即可实现。

	透明模式	反向代理
部署复杂度	即插即用	需要修改 DNS 指向
数据处理延时	几乎无延时	略有延时
获取源 IP	可以获取	需要单独设置

2.2.1. 透明模式

通过透明模式，KS-WAF 只需接入网关与服务器的流量路径中，即可工作。



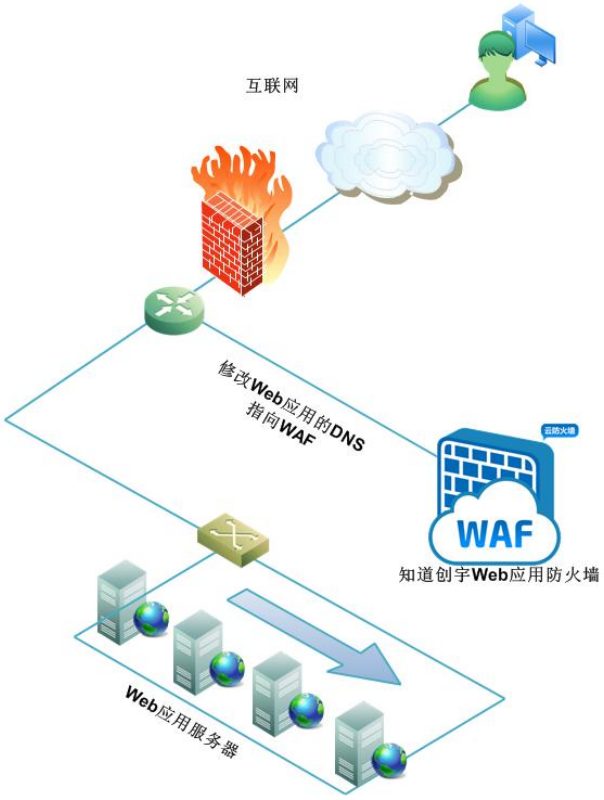
图表 6 直连部署模式

2.2.2. 反向代理模式

反向代理模式通过修改 Web 应用服务器的网关或者 DNS，将流量路径牵引至 KS-WAF。

KS-WAF 接受来自客户端的连接请求，然后将请求转发给内部网络上的服务器，并将从服务器上得到的结果返回给请求连接的客户端，此时代理服务器对客

户端就表现为 Web 应用服务器，避免了真实服务器直接对外暴露。



图表 7 反向代理部署模式

2.3. 附加收益

对于大规模集群网站的防护场景和基于云架构网站群体系的防护场景，我们可以来考虑几个问题：

1) 如何为集群网站提供有效的安全防护技术；

2) 如何让在云计算中心中托管的网站应用也能获得有效的防护；

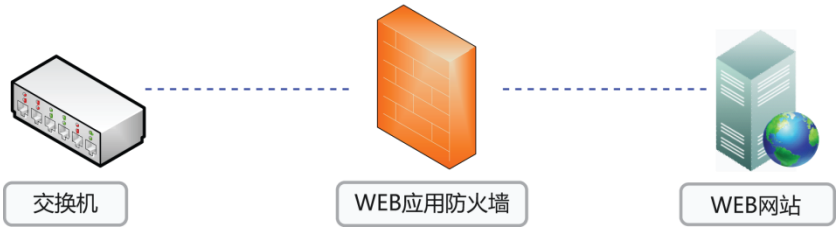
3) 如何使用云相关技术，通过整合资源，以最低的成本构建防护中心，使不同类型的网站都能获得最高的安全保障；

4) 如何让未来的云计算中心拥有 Web 安全防护能力。

这些因为云的出现而产生的问题一直困扰着市场。在云计算环境下很多网站应用托管于沙盒系统中或虚拟机系统中，对于沙盒中的系统管理员不具备 OS 层访问权限，例如 Google App Engine 和国内的 Sina App Engine，均不允许管理员

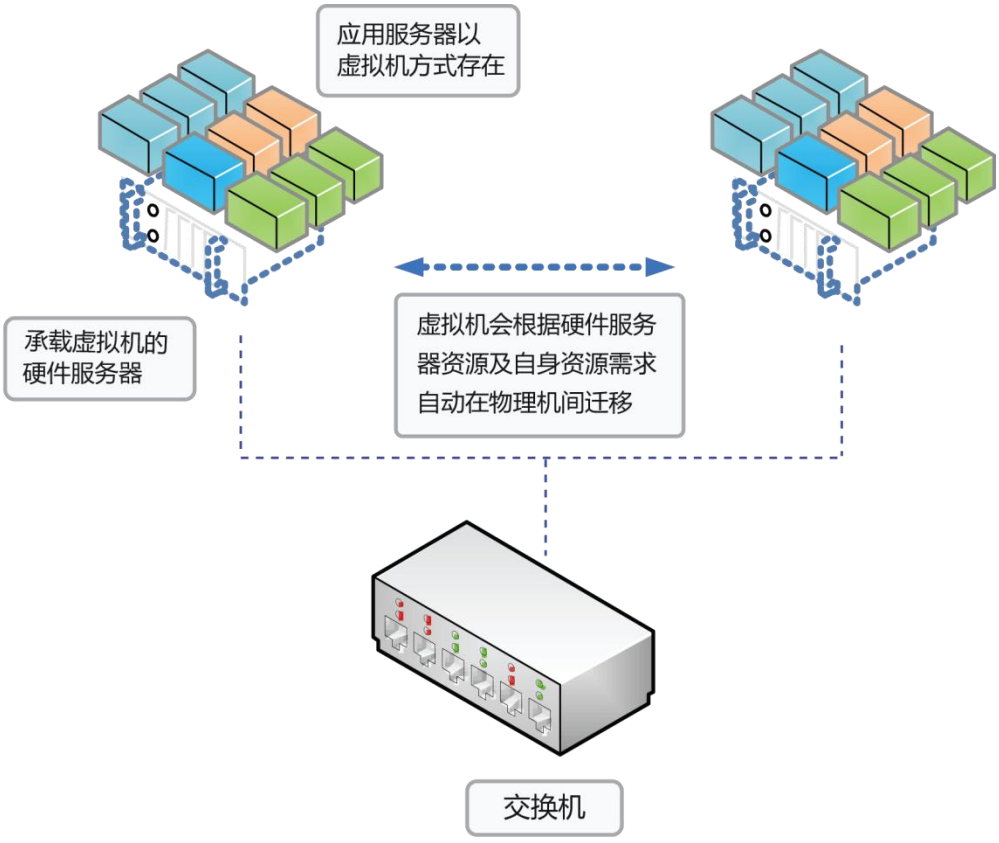
访问系统底层，此时无法安装软件版本防护软件。

对于硬件版本的应用防火墙，必须安装在网站前方如图：



图表 8 传统安装模式

但云计算环境与传统 Web 应用部署环境存在很大差别，Web 应用此时以虚拟化形式存在，而且并不限定于某个具体硬件：

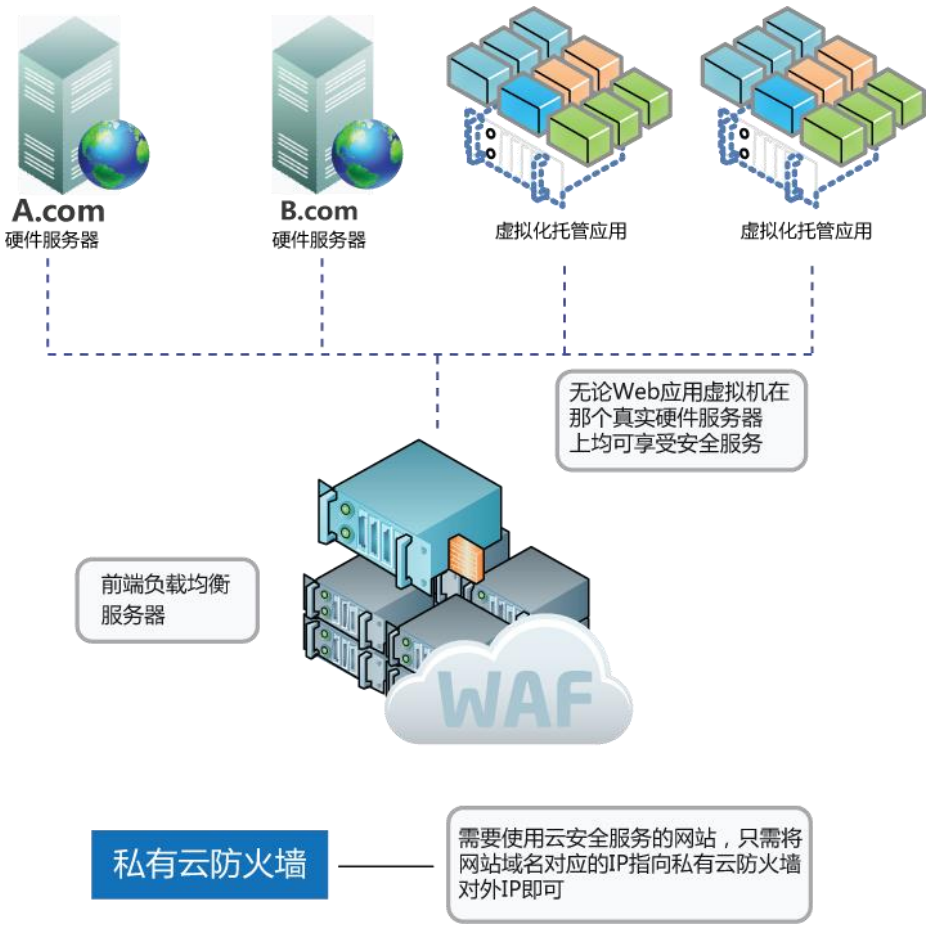


图表 9 应用虚拟化

如上图，Web 应用以虚拟机方式存在，而且一个服务器硬件上承载大量虚拟机，并且虚拟机会根据双机热备份、资源需求等情况在虚拟化环境中进行自动迁移，这导致传统的 WAF 防火墙没有位置部署。

2.3.1. 私有云

在建设云计算中心时，通过将 KS-WAF 进行小型化、私有化，在中心内部构建一套私有 KS-WAF 系统，即可对云计算中心内的 Web 应用提供安全防护。架构如下：



图表 10 私有云防火墙部署图

私有 KS-WAF 集群对网站提供安全服务，构建在云计算中心机房中，服务器角色包括：

- 负载均衡服务器
- Web 应用防火墙服务器
- 缓存加速服务器
- 反向代理服务器
- Web 安全问题和网站结构主动探测学习服务器
- 数据库服务器

- Web UI 服务器

2.3.2. 关键技术

- 负载均衡技术
- 反向代理技术
- 动态 DNS 解析技术
- 漏洞跟踪和研究相关技术
- 高效检测技术
- 容错技术
- 海量数据存储技术
- 海量数据统计分析技术
- 可扩展性

3. 结论

知道创宇信息技术有限公司拥有国际一流的专业技术团队，团队成员曾从业于国际、国内多个著名网络安全厂商，平均拥有 10 年以上安全研究及开发经验。多位成员均是国内著名安全专家，并专注于提供互联网 Web 安全综合解决方案。

为解决中国恶意网站泛滥、网络欺诈猖獗、网站安全事件层出不穷等问题，知道创宇推出了 Web 应用防火墙，用于弥补目前安全防护产品（如网络防火墙/入侵检测系统/网页防篡改系统）对 Web 应用攻击的防护能力的不足，旨在帮助客户降低 Web 应用的安全风险，确保不影响业务正常运作的情况下进行实时安全防护。

在兼顾 Web 应用的安全性及高可用性、连续性的同时，知道网站统一防护平台简化了 Web 应用安全防护的应用流程，降低安全投入的成本和实施的复杂度，并提供针对 Web 应用的网管运维能力，不仅通过加速来提升 Web 应用的业务能力，而且对 Web 应用采用集中式安全管理，兼容分布式和分层的网络结构，可以有效降低管理成本，保证在网络中安全策略的一致性，可进行快速响应和快速防御。

知道创宇

Knownsec

公司地址：北京市海淀区蓝靛厂南路 55 号金威大厦 803 室

邮编：100097

电话：010-51295887

传真：010-52723966

网站：http://www.knownsec.com

邮箱：sec@knownsec.com

