了解更多详情，请下载查阅Imperva安全白皮书：[这里](https://www.imperva.com/lg/lgw.asp?pid=382)

欢迎订阅Imperva数据安全博客，查看更多数据安全前沿信息：<http://blog.imperva.com/>

**【Imperva白皮书】**

**网络安全的未来**

**——WAF应当具备的十大特性**

**概述**

**据Forrester统计，2013年有超过半数的企业的Web应用被泄露**，其中不少因此遭到严重的财务损失。近年来，企业安全事件屡见报端：2011年，多家公司和政府网站被黑客攻击；2012年的DDoS攻击令众多美国银行网站瘫痪；更不用提那些造成数百万用户信用卡信息泄露的网络安全事故了。**传统的网络安全防护体系已无法招架如今的黑客们了。**

今天，网络罪犯已不仅仅把目光锁定在知名大公司上，每一个存在漏洞的网站都可能成为被攻击的目标。黑客们的攻击方式一般可以分为以下三种：技术性Web攻击、业务逻辑处理攻击、以及网络欺诈。

**技术性Web攻击**

技术性Web攻击恐怕是黑客们最热衷的攻击方式了。SQL注入以及跨站点脚本攻击绝对是网络罪犯的最爱， 在黑客论坛里，有关SQL注入的讨论占据了全部话题的五分之一。相关安全研究也表明，**全球超过97%的数据泄露与SQL注入有关。**

**业务逻辑处理攻击**

黑客们不会局限于传统的Web攻击方式，近年来，他们开始利用企业的业务逻辑漏洞发起攻击，例如在论坛中张贴垃圾评论广告，破坏网站以窃取其中的高价值知识产权内容，执行重复的暴力破解攻击，或是在搜索中运用通配符令应用程序中断。这类攻击往往令公司束手无策，因为应用程序扫描通常无法检测到业务逻辑漏洞，而在安全开发中也难以规避此类问题。

**网络欺诈**

黑客还会把目标转向没有防备的网站访客，用欺诈软件如Zeus和SpyEye潜入上百万台电脑。这些欺诈软件会盗取用户的信任凭证、通过追踪键击和操纵网络内容进行劫持会话。尽管欺诈软件针对的是最终用户，但受害者实际是网站的拥有者，如银行和电商网站，因为需要支付高昂的赔偿和修复费用。

**网络安全防护为何失效？**

当上个世纪90年代企业开始业务联网时，他们遇到的是现代黑客的先行者—通过开放端口和平台的漏洞进行恶意攻击的入侵者。针对此类攻击，企业开始部署防火墙和IPSs。然而，当这些企业开始部署web应用时，黑客很快就学会规避这些防火墙，而通过编码和恶意评论等绕过技术规避IPS特征检测。

下一代防火墙（NGFW）在几年后进入视野，提供鉴别应用流量（如HTTP或即时通信）等新功能。然而，这类功能并不能阻止网络攻击。NGFW不能拦截针对定制的web应用漏洞的攻击，也无法侦查针对cookie，会话、参数值篡改的攻击。NGFW同样不能阻拦被欺诈软件入侵的终端设备，或者业务逻辑攻击。仅仅依赖这类网络安全解决方案的企业，实际无法保护网络应用安全。

**Web应用安全是企业业务安全的核心**

**WAF已成为企业为应用提供安全防护的的核心平台**，能够全面抵御包括技术性Web攻击、业务逻辑攻击以及网络欺诈在内的网络威胁。WAF通过对Web应用的深入理解和输入验证， 能有效阻拦SQL注入、跨站点攻击和目录遍历攻击，阻止恶意扫描并修补漏洞。WAF还能够自动进行更新，预防新的攻击对企业核心应用造成的安全威胁。

作为企业战略层面的防护，企业在选择WAF产品时必须对其安全性能、管理方式以及调度方式进行全面仔细的评估。下文中列举的内容即WAF应当具备的十大特性：

**WAF应当具备的十大特性：**

**1：充分了解Web应用**

**挑战：**

**当今企业面临的是日益先进且多样的Web攻击。**丰富的Java脚本和SQL给了黑客们无数可乘之机。特定代码可以帮助检测Web攻击，但它要么由于检测的范围过于宽泛而导致误报威胁，要么由于对句法限定过于精确而造成威胁漏报。黑客们完全可以通过一些逃避手段或创新方法绕过传统的安全防护，威胁Web应用的安全。

**对WAF的要求：**

为了对Web应用进行精确的防护，**WAF必须对受保护的应用进行充分了解，包括URLs，各项参数以及Cookies**。了解受保护的应用和输入验证可以有效防止SQL注入、参数篡改以及Cookie中毒。为实现输入验证，WAF需要检查特定字符的参数值，如省略号、括号等，预测其是否具有攻击意图。由于企业更新应用愈发频繁，WAF必须能够自动地捕捉到应用的更新，从而在保证WAF最高防护水平的情况下，实现对WAF的有效管理。

**2：领先黑客一步**

**挑战：**

黑客总是在创新。无论是发明新的攻击工具，通过更隐秘的方式扩大黑客组织，还是不断优化现有攻击技术，**总之，应用威胁在不断升级。**在黑客们的秘密论坛中，不断有新的攻击向量和漏洞被曝光。骗子们也不闲着，欺诈软件开发者开发出可以自我突变的文件来逃避病毒特征代码的检测。如今的网络罪犯可以规避物理认证、智能卡和外带认证来进行欺诈。目前应用安全解决方案面临的最大障碍恐怕就是如何跟上这些层出不穷、花样百出的威胁的脚步。

**对WAF的要求：**

WAF必须具备最新的防护以应对层出不穷的网络威胁，充分利用来自全世界的活跃攻击信息和欺诈数据来识别攻击和攻击者。**WAF应能够对安全代码、政策、信誉数据和欺诈情报自动进行更新**。除此之外，**关注其安全调研部门的报告也是非常重要的**。此安全调研是否关注Web应用安全？是否具备抵御最新应用攻击的能力？如果答案是否定的，则应该研究替代方案。

**3：逃逸拦截技术 Thwart Evasion Techniques**

**挑战：**

企业需要在不阻碍合法流量的前提下抵御Web攻击。这个要求听起来相当合理，但对于多数安全解决方案来说却并非如此。如前所述，WAF需要输入验证，但它不应该阻止无意的错误输入。如果黑客于在线表格邮编一栏内输入常见的Web攻击字符，如方括号或省略号，那么WAF应该检测到这一反常行为。但如果这个行为是发生在合法用户的无意输入时呢？如何区分这是网络罪犯在发起攻击还是普通网络用户正在填表？又如何创建攻击代码对SQL关键词进行监测，并确保在合法请求中不出现这些关键词？答案是：通过先进的分析方法和智能关联。

**对WAF的要求：**

**WAF必须拥有一个分析引擎，对多样的攻击行为进行检测，以避免漏报。**这个分析引擎不仅要能识别攻击字符串，同时要能够对攻击关键词、特定字符、违反协议等因素进行评估分析。它不仅要能识别违规行为，还应运用风险评分和正规表达式对恶意请求和非常规但无害的流量进行区分。WAF还要能够关联超时请求，以检测重复的攻击行为，例如暴力登录和DDoS攻击。只有具备了灵活而智能的关联引擎的WAF才能抵御那些老练的黑客攻击，同时不阻碍合法用户的正常使用。

**4：防止自动攻击和僵尸网络**

**挑战：**

当今的网络犯罪已经产业化，黑客们利用自动化操作发起更具效率和规模的攻击，并将之转化为价值数万亿美元的生意。通过网络漏洞扫描和僵尸网络，网络罪犯们可以发现易受攻击的网站，再利用诸如Havij这样的SQL自动注入工具，便可获取到敏感数据资源。除了这类由职业黑客发起的攻击以外，企业还被另一类自动攻击所威胁，比如竞争对手自动抓取网页内容，以及网站垃圾评论注入。

**对WAF的要求：**

**WAF必须有能力阻拦自动攻击行为，包括网站抓取、垃圾评论、DDoS和漏洞扫描等。**鉴于如今自动攻击频发，拦截恶意用户与拦截恶意请求同样重要。正确地识别恶意用户需要多重防御。第一，WAF要能够识别僵尸网络，它们是绝大多数自动攻击的元凶。可以通过测试网络用户的浏览器来确定它们是否正常，还是已经成为僵尸网络或是被脚本注入。第二，WAF要能够检测用户在短时间内出现大量的页面请求，这是僵尸网络的一个重要信号。其它信号还包括重复下载大容量文件，或者要求长时间的响应。通过僵尸检测，WAF可以广泛而有效地拦截自动攻击行为，保护网站不受到恶意破坏。

**5：攻击者的来源**

**挑战：**

恶意的网页访问者会千方百计地寻找漏洞、窃取数据、实施欺诈，甚至攻陷网站，但他们可不全是人类，很多时候是僵尸机器人在自动地对一个接一个的网站发起持续攻击；人类黑客就聪明和复杂得多了，他们会用匿名Proxy或木马掩藏身份；而网络欺诈者有着独特的攻击方式，比如说通过钓鱼盗取用户数字证书。

对于当今的企业，最大的问题是**只有攻击造成一定范围的影响之后，才能判断是否是恶意用户或非法网站。**

**对WAF的要求：**

**为了保护web应用，WAF必须能够识别已知的恶意攻击来源和网站。**WAF需要鉴别出那些对其他网站已有攻击历史的恶意来源，在损害造成之前拦截；而由于黑客通常匿名，WAF需能识别来自Proxy和木马的访问；针对钓鱼行为，则需识别来自于钓鱼网站的用户；而地理位置也很重要，WAF需能限制来自特定地区的访问，以减少不需要的流量及拦截来自某个高攻击率地区的DDoS攻击。另外，由于WAF是防护网络攻击的最有效的解决方案，也理应能够收集和分享关于攻击行为和来源的信息。基于云的社区防护产品则应能发布精准、实时的攻击数据。**这才是未来的应用安全。**

**6：虚拟补丁漏洞**

**挑战：**

目前的现实情况是，**大部分的Web应用都有漏洞**。而**修复一个被发现的漏洞平均需要至少38天**，意味着这是些应用会长时间曝光在攻击之下。除了修复漏洞所需的时间和花费，企业还需考虑那些多年闲置的遗留应用以及应用包里的漏洞带来的麻烦。

**对WAF的要求：**

WAF必须能够预防那些利用漏洞乘虚而入的行为，**诸如输入校验（Input Validation）、HTTP协议校验、攻击特征这样的防护功能必须能够阻拦大部分漏洞攻击。**除此之外，企业还需实施精细管控，以确保对已知Web应用漏洞的严格识别。企业可通过整合WAF和应用扫描，配合自定义的安全策略，对扫描到的漏洞进行补丁。

**7：阻止恶意软件**

**挑战：**

**欺诈软件是金融机构的头号敌人。**网络罪犯开始把他们在网上银行的成功攻击经验复制到电商和网络支付上：他们先通过Zeus病毒，或者SpyEye木马入侵终端，然后当被感染的用户登陆目标Web应用比如说网上银行时，这些恶意软件就会进行未授权交易，或者窃取个人登陆信息。一旦欺诈软件入侵个人用户，由于涉及庞大的修复和赔偿费用，最大的受害者实际是银行和电商本身。

**对WAF的要求：**

**WAF必须能缓解欺诈软件的持续攻击**。置于网络用户和应用之间，WAF能够清晰看到应用层的交易，并分析终端用户的行为特点、网络流量的模式，以及时发现及拦截被感染的终端。其他功能还需包括：在特定时间段监测用户，发出警报，联合欺诈管理解决方案进行侦查等，同时无需修改应用。

**8：减少支付和账户欺诈**

**挑战：**

近期全球发生多个电商巨头的网络攻击事件，损失巨大。如何防护Web应用被恶意欺诈，如何在昂贵而漫长的应用开发和更新完成之前，尽快实施抵御措施？

**对WAF的要求：**

**WAF 需要联合基于云的防欺诈解决方案，辨识并分析可疑现象**：浏览器不规则使用(browser irregularities)，被入侵的设备、可疑的支付信息等。WAF需能在不改动web应用的情况下，把历史欺诈数据和网络攻击、用户行为关联起来，识别并阻止入侵。

**9：支持本地和云端部署**

**挑战：**

**应用的基础架构和网络攻击一样，呈多样化和快速进化态势，**这导致安全需求和配置也日趋多样化：有的企业在本地部署应用，有的在云端；有的需要透明的安全解决方案，对web应用零影响，有的则需重写URLs和编码，从而改变web应用内容；有的企业需要高性能的硬件部署，有的只需灵活的虚拟部署；大企业要求全套部署，则需多样化的部署选择，以支持不同部门、不同地理位置托管的远程应用。

**对WAF的要求：**

**WAF需要提供灵活的配置选择，以满足不同企业的不同需求。**在许多企业逐渐向云迁移的过程中，WAF需能支持针对私有云的虚拟配置方案，提供基于云的安全服务，保护被托管的web应用。

在本地部署应用的企业需求也很复杂：有的需要高性能、不改变现有web应用或网络设备的解决方案；有的需要WAF能修改内容、标记cookies、重写HTML；有的需要非联机的部署。企业在选择WAF时应考虑一个既满足现有、又能满足未来需求的解决方案。

**10：自动化和规模化运营**

**挑战：**

**WAF可以很复杂，但阻止入侵不能复杂。**安全管理员应无需学习脚本语言就能创建定制化的安全政策；另一挑战来自于**企业往往运行上十数百个位于不同数据中心，甚至不同国家的网络服务器**，这意味着企业需能实施集中化应用安全策略管理，并监测全球范围的事件；最后，企业需能细致地侦查安全事故，这有赖于WAF提供细致的安全报警和定制化的监测和鉴别。

**对WAF的要求：**

**WAF需简单易用，同时提供灵活的政策配置，**不单是初始配置，还能让安全管理员方便地审核其他同事创建的安全政策；除了定制化政策之外，WAF需能支持集中化管理，使企业能在全球不同数据中心的不同WAF间实现政策和应用管理的同步；最后，WAF需能提供细致、响应迅速的安全事件信息。详尽的监测和报告、集中化管理、灵活的政策配置，使得企业能管理、监测和保护web应用。

**结论**

**今天，web应用已成为驱动业务的核心力量。企业要保障业务安全，则要保护应用和数据安全，而一般的防火墙和IPS并不是为此而设，只有Web应用防火墙，才能真正做到这一点。以上列举的十点应是每一个WAF都具备的基本特性，企业可据此标准来判断WAF的部署。**

###

* 了解更多详情，请下载查阅Imperva安全白皮书：[这里](https://www.imperva.com/lg/lgw.asp?pid=382)
* 欢迎订阅Imperva数据安全博客，查看更多数据安全前沿信息：<http://blog.imperva.com/>