SearchSecurity.com.cn

技术手册

Web 应用防火墙

☆ 正确选择Web应用程序防火墙

☆ 如何选择：源代码审查还是Web应用程序防火墙

☆ PCI 6.6 Web应用安全强令加重小型公司负担

☆ 建立应用层防火墙规则基础

☆ 应用程序安全专业知识：WAF服务的附加值

TechTarget
TT中国

Web 应用防火墙

目 录

正确选择 Web 应用程序防火墙

那些急于满足 PCI 规则遵从要求的企业在选择 Web 应用程序防火墙时（WAF）可能会陷入困境。你怎么知道应该选择什么样的产品？你怎样才能有效地部署和管理这个工具或者软件？你如何让它与现存的基础设施相匹配？在本文中，我们将着重讨论这些产品评估中的关键问题，从而为你公司的规则遵从提供帮助。

Web 应用程序防火墙或者应用层防火墙指的是那些保护网络应用程序不受攻击、防止数据泄漏的工具或者软件。它位于 Web 客户端和 Web 服务器之间，分析应用层消息、查找违反安全政策的内容。Web 应用程序防火墙处理的安全问题与网络防火墙和入侵监测/防护系统处理的有所不同，后者是用来保护网络外围环境安全的。在你购买这种产品之前，你需要明确它并不是一个即插即用（plug-and-play）的规则遵从组件，只是简单地把它放在你的应用服务器前面是行不通的。

你需要知道的内容

每次新的立法或者新安全要求出现时，从事规则遵从工作的人往往草率地作出相应的决定。许多系统管理员只根据一个供应商的销售广告或者他们遇到的某个特殊要求就做出了决定。

选择 WAF 的步骤

请按照下面的步骤为你的应用程序选择合适的 Web 应用程序防火墙：

1、用安全政策目标来确定你的 WAF 需要具备哪些控制功能。

2、审查每种产品的风险类型。

3、测试性能和可扩展性。

4、评估供应商的技术支持。

5、评估你是否拥有维护和管理该产品的内部能力。

6、权衡安全、生产能力，以及整体成本。

——Michael Cobb

其结果极有可能不合适或者不是最优的安全决策。即便是工期很紧，你也不能抛弃你应有的谨慎。为了选择安全的设备，比如 Web 应用程序防火墙，你需要回答以下问题：

- 根据你的安全政策目标和法律要求，该产品需要做什么？
- 什么额外的服务是有价值的？
- 它怎样才能融入到你现在的网络中——你的公司具有正确、有效地使用它的能力吗？
- 它将如何影响现在的服务和用户，其费用如何？

新的遵从规则（比如 PCI DSS）要求你在回答第一个问题之前就要升级或者至少重新审查你的安全政策。一个好的安全政策确定了你保护数据安全的目标和要求。这个基础可以让你确定哪些安全设备能够满足你的要求。因为每个 Web 应用程序都是独特的，安全必须进行定制，从而覆盖在安全生命周期开发程序中威胁建模阶段所确定的全部潜在威胁。审查一下你中意的 WAF 产品能够防御哪些威胁（比如，能不能通过 cookie 或者 URL 分析参数去防御 OWASP 排名前十的应用程序漏洞），并考虑规则遵从所规定的附加要求。

选择你的 WAF

为了确保 WAF 能够满足 PCI DSS 规则遵从的要求，你应该把 WAF 的功能与 PCI 补充信息中所推荐的功能进行比较：PCI 安全标准委员会发布的要求_6_6_代码审查和应用程序防火墙的阐述。点击查看 PCI 安全标准委员会发布的要求_6_6_：(https://www.pcisecuritystandards.org/pdfs/infosupp_6_6_applicationfirewalls_codereviews.pdf)

他们必须能够检查并处理 HTML、动态 HTML（DHTML)、层叠样式表（CSS）等 Web 网页内容，以及你的应用程序使用的协议，比如 HTTP 和 HTTPS 等。

此外，请检查一下供应商过去采用新协议的速度如何。审查他们的开发和支持政策，以确定他们是否支持自定义协议，或保护一系列应用程序协议。另外，WAF 必须能够检查 Web 服务消息，尤其是 SOAP 和 XML。询问 WAF 供应商，他们的自动更新以及应用动态签名情况如何。这些工作会有助于你评估他们的技术支持和客服能力。

最后，询问供应商特定功能的额外费用。比如，有些应用程序可能需要 FIPS 硬件密钥存储支持。虽然 WAF 供应商可能会支持这个需求，但是费用会高得惊人。

当你完成上述工作之后，请抽出时间了解下每种 WAF 覆盖一个或多个安全区域时所使用的技术方法以及处理深度。你能用白名单列出数据类型和范围吗，你能创建结合了白名单和黑名单的规则吗？WAF 在自身受到攻击时安全情况如何？比如，它应该运行在一个固化的系统上，而它的组件却运行在没有特权、封闭的运行时（runtime）环境中。如果该产品的自身安全都不可靠，那么你完全没有必要阅读下面的内容了。

软件 WAF vs. 硬件 WAF

PCI 补充资料（PCI Information Supplement）表明，WAF 可以以软件的形式部署在运行有通用操作系统或者工具的标准服务器上。它也可以是一个单独的设备或者内置在网络器件中。所以，你可以在市场上选择各种类型的 WAF。

下一步是什么？

Web 应用程序防火墙仅仅是个开始。

为了防范日益复杂的应用程序攻击，WAF 提供的保护应该集成在应用程序保障平台中。F5 和 Barracuda 公司推行的这个结构结合了 WAF、数据库安全、XML 安全网关以及应用程序流量管理，能够提供更加全面的安全保障。

该结构的好处包括：能够对经过这些设备的信息进行比较，正确判断流量是否具有恶意。这使得流量控制、分析以及报告更加有效。管理员可以配置一系列政策规则和参数，而不是试图通过几个不同的设备来加强每个政策，大大减少了管理费用。

展望未来，WAF 产品或者任何取代他们的产品肯定能像它们所保护应用程序那样查看带内（inbound）的数据。这会使得某种形式的脚本引擎可以删除任何模糊的内容（obfuscation），以便安全设备像浏览器查看请求一样检查各种请求。这将让判断代码是否恶意变得容易很多。我们期待在下一代安全设备中看到这种动态的分析形式。

——Michael Cobb

软件 WAF 通常比较便宜，更加灵活。硬件工具更容易安装和配置，因为他们的操作系统已经固化在了芯片中，而软件防火墙则需要人工去进行配置。（WAF 不会去保护那些存在着问题的配置，也不会防护服务器中的漏洞。如果你倾向于使用以软件为基础的产品，那么请选择一款能够在你 IT 部门所熟悉的平台上运行的产品。不管怎样，请弄清楚防火墙供应商能够提供哪些培训和支持，以及相应的费用。

PCI DSS 入门知识：

关于 PCI DSS，你所需要了解的内容

支付卡行业数据安全标准（PCI DSS）是 PCI 安全标准委员会在 2006 年推出的，该委员会是一个开放的论坛。该委员会是 PCI 的一部分，而 PCI 是由几个大型信用卡公司建立的行业联合组织。该委员会负责目前 PCI DSS 的开发、管理、教育，以及认知等。

但是，它不会强制执行 PCI DSS，也不惩罚任何违反该标准的活动。标准的执行交由特定的信用卡公司和商户或收单银行(acquirer)去进行。PCI DSS 不会代替单个信用卡公司的遵从程序，但是已经成为了数据安全规则遵从方面的技术要求。所有的商店必须满足 PCI DSS，并接受大型信用卡公司发行的信用卡和借记卡。

根据 PCI DSS 标准，企业必须采用特定方法来确保数据安全，保证客户的信用卡数据、账户信息、以　及交易信息不被黑客或任何恶意的系统入侵获取。这些措施包括：建立并保持一个安全的 IT 网络、保护持卡人数据、配备漏洞管理程序和信息安全政策等。

该标准的规则遵从要求被分为四个级别，企业应该遵从哪个级别是根据企业每年的支付卡交易量确定的。级别 1，最高级别，被攻击过的企业或者被认为是高风险的企业都要遵从这个级别的要求。任何对这些要求小的违反都会触发全部的无抱怨状态，导致罚款，甚至停业或者取消卡片处理权限，直到商家遵从 PCI 规则为止。

如果你想了解更多情况，请参阅 PCI 安全标准委员会网站。

——Michael Cobb

当然，目前也存在着开源的软件 WAF， ModSecurity（http://modsecurity.org）和 AQTRONIX WebKnight （http://www.aqtronix.com）。如果它们能够满足你的要求，你就可以大大地降低成本，不过还需要人去学习、安装、配置，并对其

进行维护。许多开源工程具有非常好的支持论坛，但是与付费产品不同的是，你不能在紧急情况下向客服寻求帮助。

性能以及可扩展性是选择硬件或者软件 WAF 时需要着重考虑的另一个方面。有些设备每小时能够处理的工作有限，而有些工具可能还存在带宽限制。如果你以后想要增加 Web 活动，或者在不久的将来需要添加其他的应用程序，那么你可能更应该选择一款可扩展的、灵活的防火墙。

软件产品的升级往往比硬件设备简单，但是硬件 WAF 更适用于大容量网站，这些网站需要非常大的吞吐量。

软件产品的升级往往比硬件设备简单，但是硬件 WAF 更适用于大容量网站，这些网站需要非常大的吞吐量。

如果你在运行一个大型应用程序，那么你所需要的 WAF 将不止一个，这样集中化的管理可能是一个关键的功能，因为有了这个功能之后你就可以在一个地方部署和管理多个防火墙。

我们的建议是，不管 WAF 是硬件的还是软件的，只要它能够满足目标要求，并可以对其进行配置管理即可。

帮助信息

请花足够的时间对 WAF 产品进行评估。一旦你确定了可以满足基本要求的某些产品，你又应该如何确定最终要买哪款产品呢？

Web 应用程序安全联盟（WASC）（http://www.webappsec.org/）创建并推行了 Web 应用程序安全标准。他们已经制定出了可供参考的 Web 应用程序防火墙评估标准（http://www.webappsec.org/projects/wafec/）。任何具有一定技术水平的技术人员都可以单独使用 WASC 的测试方法对 WAF 方案进行质量评估。

请把 WASC 的标准作为你评估过程的一部分。遵循 WASC 的建议，仔细审查 WAF 产品所使用的配置架构，WAF 的 HTTP、HTML 和 XML、监测和保护技术、日志记录和报告能力，以及管理和性能等。

WAF 的部署

祝贺你。你已经选择、购买并安装了一款具有必要的遵从能力的 WAF。但是，这并不意味着你会一帆风顺。适当的安排、配置、管理以及监视是必不可少的。

WAF 的安装需要遵循四步安全生命周期：确保安全、监视、测试和完善。这是一个持续的过程，内部存在着反馈和多次循环，从而使得安全更加稳固。在把设备连接到你的网络前，你一定要用文档记录下网络基础设施，并且想办法让网络中

的设备或者系统更加稳固。这意味着要给设备打上补丁，还要花时间对设备进行配置，从而增强其安全性。

配置将直接追溯到你在安全政策中确定的业务规则（比如说允许的角色集合）。如果你按这种方式处理防火墙配置，规则和过滤器将会自动定义。WAF 能够发现网络或者应用程序中的技术问题，比如误报（false positive）警告或者流量瓶颈等。

仔细测试是必不可少的，尤其是你的网站使用了特殊的标题（header）、URL 或者 cookie，或者与 Web 标准不一致的特定内容。如果你运行了应用程序的多语言版本，你还应该预留额外的测试时间，因为它可能要处理不同的字符集。

用微软的 Web Application Stress 和 Capacity Analysis Tools 或者 AppPerfect Load Tester 等工具对 WAF 进行压力测试，也有助于发现部署 WAF 后可能引起的瓶颈。

测试环境应该尽量接近“真实的”应用程序环境。这有助于在部署 WAF 前发现 WAF 可能引起的系统整体问题。用微软的 Web Application Stress 和 Capacity Analysis Tools 或者 AppPerfect Load Tester 等工具对 WAF 进行压力测试，也有助于发现部署 WAF 后可能引起的瓶颈。

WAF 管理

一旦你配置完成并开始运行，请评估 Web 应用程序防火墙未来的变化将如何影响 Web 应用程序，反之亦然。当然，你必须记录下你对网络基础设施做的任何改变，作为将来的参考和故障处理的依靠。这个包括跟踪现在以及将来对配置所做的任何变化。

产品环境的改变必须在监测下进行。请确保把时间和变化的范围提前告知企业中所有受影响的部门。为了确保配置不被故意更改、确保配置具有合法程序，你必须控制安全设备的任何物理访问以及逻辑访问。严格坚持变化控制、业务连续性，以及灾难发现政策，因为它们可以保护 WAF 和你的业务。

因为应用程防火墙不仅检查网络地址和端口，还会检查整个网络的信息包，所以它们的日志记录能力更加宽泛，并且能够记录特殊应用程序命令。所以，请不要浪费这个功能和信息。日志文件分析可以提醒你即将来临或正在进行的攻击。一定要定义好你的防火墙所需要记录的信息，最好是全部请求和应答数据，包括头和身体负载。请确保你的员工具有这方面的专业技能和足够的时间，以便对日志进行审查和分析。

Web 应用程序永远不可能百分之百的安全。即便是没有短时间内部署 Web 应用程序的内部压力，系统也会存在漏洞、存在威胁。把 Web 应用程序防火墙作为安全模型的一部分，你就可以观察、监测并寻找那些入侵的苗头。防火墙与匆忙

去修补漏洞不同的是，它为你提供了一个可以喘息的地方，让你按照自己的时间进度去安排漏洞修复。

（作者：Michael Cobb　译者：Sean）

如何选择：源代码审查还是 Web 应用程序防火墙

在你决定用源代码审查或者 Web 应用程序防火墙来满足 PCI DSS 规则遵从的需求时，我建议你抽点时间，全面了解一下 PCI 的 Web 应用程序要求，包括澄清文档（clarification documents），并考虑这两种选择应该如何同你的架构和资源结合起来。目前，企业有多种途径进行规则遵从，如果执行恰当的话，任何一种选择都可以帮助企业达到规则遵从要求，而且能够提高 Web 应用程序的安全性。

当然，在应用程序安全方面并不存在万全之策。除非你很幸运，既能进行代码审查又能运行 WAF，不过这样做依然需要人工去完成。企业是否有员工可以完成以下工作：

- 配置和维护应用层防火墙？
- 进行代码审查？
- 使用第三方漏洞监测工具，并处理在审查中所发现的问题？

当然，这个决定还要考虑架构，以及 WAF 与现有系统及设备的兼容性如何。其中一个需要考虑的因素（尤其是对那些倾向于使用第三方代码审查的企业而言）是企业对其代码状态的满意度如何。随着时间的推移，支付卡应用程序的开发可能会包含来历不明以及目的不明确的遗留代码。安全人员可能不想冒破坏任务优先应

用程序的风险而删除这些遗留代码。在应用程序前面放置一个防火墙可能会比在代码审查中重写程序成本要低，或者破坏性要小。

另一种方法是用威胁模型（threat modeling）来识别和评估应用程序的风险。我们以三大关键风险为例，并确定哪些方法能最好地处理它们：代码审查、漏洞评估、WAF 产品。但是请注意，部署 WAF 并不能减少你的安全软件开发过程需求（要求 6.3）！而应用程序漏洞评估和代码审查却都能加强开发和质量保证周期。

对于小型商业网站来说，上述选择过于昂贵。所以，我建议把支付任务外包给第三方支付服务供应商，不必担心所有昂贵的安全要求，包括 Web 安全、以及实际的 PCI DSS 遵从等。只要你不处理任何卡支付，你就不需要遵从 PCI DSS 标准。

不管你选择什么方式，许多人都会争论 PCI 遵从是否同可接受的安全水平一致。

规则遵从与安全的权衡

不管你选择什么方式，许多人都会争论 PCI 遵从是否同可接受的安全水平一致。负责安全的人员需要了解上述每种选择的局限性和能力。源代码分析本身可以进行规则遵从，但它不是保障应用程序安全的好办法。事实上，没有一种方法能完全保证所有的要求。PCI DSS 侧重于与 PCI 相关的支付卡应用程序和组件，但它并不是以整体方式查看企业及其全部网络操作，而需要在整个企业中全面部署安全措施。

即使有了 PCI 要求 6.6 信息补充的澄清说明，许多商户还是不确定哪些行动能够很好地进行规则遵从。这就导致了典型的规则遵从困境（compliance dilemma）。如果你要公布一个可以增加安全性的标准，你就必须回答这个问题："我必须做哪些工作来满足这个标准？"而该问题又会迅速演变为："满足标准的最小工作量是多少？"如果你只是以"选中复选框并继续"的观点来看待 PCI 规则遵从的话，那么 WAF 将是快速、简单的选择。

然而，PCI DSS 的确给企业提供了创建安全架构和业务模型的基础。它还让企业高层关注安全问题。如果你关心安全，那么遵从 PCI 要求只是顺理成章的事情。在你的开发人员能够安全编程之前，多层次的安全方案将永远是减轻风险的最好方法，因为在这种情况下，安全方案包括了代码审查、漏洞评估和 WAF 产品。一旦漏洞扫描的结果整合到 WAF 的配置中，WAF 将更加有效。这样做将会为程序提供保护，同时对源代码进行分析和修正，以消除漏洞。

在 PCI 审查之后，漏洞还会不会暴露出来？当然会，但是不会那么多，也可能不会那么严重。降低成本和商业因素可能导致低水平的评估和保护，但在真实的商业世界中，安全必须引起人们的重视。

（作者：Michael Cobb　译者：Sean）

PCI 6.6 Web 应用安全强令加重小型公司负担

支付卡行业数据安全标准（PCI DSS）的 6.6 部分成为必要条件已经过去一年多了。PCI6.6 章节要求处理信用卡交易的组织解决 Web 应用安全，它要求公司要么实施人工或自动的源代码评审，要么在 Web 应用和客户终端间安装 Web 应用防火墙（WAF）。

Web 应用是流行的被攻击对象。SQL 注入攻击正变得日益猖獗，并因为利用漏洞经常能够直接访问组织的敏感数据而更加危险。

PCI 安全标准委员会强制规定 2008 年 6 月 30 日是遵从 PCI6.6 章节的最后期限，之前的 18 个月它只是建议遵从。这催促组织解决 Web 应用安全，而且对于那些小型的 3 级或 4 级商家来说是个压力，它们可能没有资源或专业技能来实施源代码评审或正确地配置 Web 应用防火墙。

“许多组织开始用 Web 应用防火墙来达到检查标准。从安全角度来说这不一定提高了标准，但它们会满足合规的要素。”

人工的源代码评审代价十分昂贵并且耗时。自动的漏洞扫描器相对好些，但仍然加重了负担。与此同时 Web 应用防火墙可能是满足合规检查最快速的方法，但是一些专家表示除非组织足够成熟能解决其专有的软件的问题，这才会是一个合适的出发点。

IBM Rational 的安全研究主任 Danny Allan 说道，“许多组织开始用 Web 应用防火墙来达到检查标准。从安全角度来说这不一定提高了标准，但它们会满足合规的要素。”

Allan 指出，组织应该两者兼顾，但是最有可能的情况是组织纠缠于如何比较 PCI 6.6 提供的两个选择并决定哪一个是最直接的方法。

Allan 说道，“这没有正确答案，一些人推荐开始时使用 Web 应用防火墙，但是 WAF 需要正确地配置来发挥作用。如果你处于一个变化不定的环境（应用不

断变化并日益复杂），那么这需要相当多的时间来配置。并且最终这不过是权宜之计，应用仍然存在问题。”

Web 应用防火墙，也被称为数据包深度检测防火墙（deep-packet inspection firewalls），用来检查应用层的消息是否违反了已建立的安全策略。一些防火墙提供了基于签名的保护，同时其它一些基于应用的行为建立合适的基线并监控偏离现象。它们以软件或者硬件的形式提供。WAF 努力侦测到某些类型的攻击因为它们并不总是理解应用接收输入时的上下文情景，如果 WAF 认为流量违反策略的话，合法的流量可能会被丢弃。同样，一些工具无法侦测到一些严重的 Web 应用威胁如跨站点脚本攻击。

“在我看来你们想同时做到 6.6 部分的选项，但是这就像将苹果和桔子进行比较。在短期看来哪个会给你更大的响声呢？这是一个需要回答的问题。”

Allan 说，“在我看来你们想同时做到 6.6 部分的选项，但是这就像将苹果和桔子进行比较。在短期看来哪个会给你更大的响声呢？这是一个需要回答的问题”。

PCI 知识库的建立者和 PCI 安全厂商联盟的研究主任 David Taylor 说，“如果能让他们达标的话，小型的商家会趋向于使用 WAF。这就是目前的状况，这没有错；这是最划算的方法。我不会建议 3 级或者 4 级的商家去花费更多的钱。”

与此同时，源代码评审是理想的解决方案。曾经有段时间专家们鼓励组织在软件的开发生命周期中加入安全的考虑。自动化的漏洞扫描器能测试应用的漏洞，特别是那些在开放 Web 应用安全工程（OWASP）网站上排名前 10 的缺陷。事实上，PCI DSS6.5 章节表明，Web 应用应该基于类似 OWASP 这样的指导方针进行开发，并且应用应该对比每年都更新的 10 大漏洞以确保安全。

Fortify 公司的产品及服务部高级副总裁 Barmak Meftah 表示，开发人员通常回避安全，因为这妨碍了开发效率和功能。人工的评审是困难的，尽管有时为了在一个应用的语义上下文环境中捕捉问题是必不可少的。除了费用以外，人工的评审经常需要检查几十万行代码，并且实际上几乎不可能遵循应用所有的逻辑路径。

他解释说，“黑客掌握的主要漏洞类型是输入字段——键入一个畸形的输入然后让应用做你意想不到的事情。这个数据包使用你意料之外的不同路径，而要完全理清头绪几乎是不可能的。”

IBM Rational 的 Allan 表示，最大的状况是组织需要在通盘考虑漏洞管理的背景下看待 6.6 合规要求。

Allan 说道，“安全的威胁每天都在变化。PCI6.6 章节是一个策略性的方法：我如何在这个今天会完全不同于明天的、不断改变的环境下解决安全攻击的问题？

这是关系到编写良好的、有质量的代码。如果我们不停地关注安全方面而不是去编写有质量的应用，我们将永远在追赶安全漏洞。”

（作者：Michael S. Mimoso　译者：Odyssey）

建立应用层防火墙规则基础

在过去的 10 年中，许多企业在网络和周边安全上进行了大量的投入。各组织均加强了他们的控制措施并且进入防御状态，极大地限制了黑客的网络扫描攻击的有效性。不幸的是，当安全专家们还在忙于建立网络控制措施时，攻击者们已经开始着手开发新的技术去攻击下一个致命的弱点：应用层。

近期 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。

近期 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。

为什么这些攻击这么有效？答案非常简单：它们绕过了过去 10 年中安全人员实施的所有以网络为中心的控制措施，例如端口禁用。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 TCP 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。

此时就出现了应用层防火墙。这些防火墙会在 Web 服务器之前的应用层对 HTTP 流量进行检查。这些设备可以检测一个链接，分析用户对应用程序发出的命令。然后就可以分析出哪些是已知攻击，哪些是标准应用的演变。

虽然应用层防火墙有很大的发展潜力，但是应当适度并且有意识的进行部署。在网络防火墙进入企业的最初阶段，实施的经理们普遍采取了谨慎的方式对待这些项目，他们进行了仔细的分析和大量的测试。在部署 Web 应用层防火墙时我们也应该采取同样的方式。仔细的测试为组织的应用开发人员建立信心，作为负责变更的安全经理也可以很有底气的说这项技术给企业带来的帮助将远远大于给他们增加的工作负担。

一旦组织准备将该产品应用到生产环境中时，就应当开始考虑一个稳定的防火墙规则基础了。下面是如何在组织中建立和部署应用层防火墙规则基础的步骤：

1．有一段足够长的调整期。当今的应用层防火墙拥有复杂的功能去监控数据流并且学习正常活动的模式。一段时间后，防火墙被“训练”得能识别出这些活动模式从而阻止非正常数据流。然而，防火墙需要有足够长的训练时间，这样规则基础才能反映出周期性和季节性的网络活动趋势。例如，电子商务零售商肯定不想在夏天这个销售淡季去训练防火墙保护其网站，然后在冬天这个销售旺季部署规则基础。

2．开发出适用于企业的个性化规则。对组织基础设施的了解是非常重要的，对防火墙进行个性化设置以满足公司的特殊需要可以极大的提高这些工具的效果。

例如，如果在一个应用环境中仅有一个 Web 应用应该接受文件上传，规则中就应当完全阻止 PUT 命令（用于上传文件的 HTTP 命令）在其他系统中使用。

3．以被动模式进行初次运行。对于规则基础的测试通常要求“软着陆”。在这样的策略下，防火墙上线时将按照建议的规则设置。接下来将在监控模式下运行，但并不阻止任何数据流。在防火墙正式进入激活模式前，应当花些时间去评估那些违反防火墙规则的数据流。负责实施的责任人还应在正式上线前调整防火墙的误判率。程序员们向来不喜欢安保系统破坏他们的应用程序，这无疑会更加影响跟他们之间的关系。

4．监视，监视，监视。一旦防火墙被激活使用，就应当认真地监控。被阻止的数据流记录会提供非常重要的线索。被阻止的攻击可以向管理者显示出他们安全投资的回报。此外，可能仍然存在误判的情况，但它们可以帮助调整规则基础。

就像网络防火墙一样，应用层防火墙也不是万灵药。可以使用 WebInspect 和 AppScan 之类的工具来检测 Web 应用的漏洞。作为补充，定期进行渗透性测试也是一项可靠的防护策略，且能打消许多安全专家们对 Web 应用的顾虑。

（作者：Mike Chapple　译者：李尧）

应用程序安全专业知识：WAF 服务的附加值

精明的应用程序安全解决方案提供商可以在 Web 应用程序防火墙（WAF）的选择、部署和管理中为客户提供额外的好处，协助客户建立有效的应用程序以及数据保护方案。

近年来，Web 应用程序防火墙已经成为企业满足某些规则遵从要求（包括数据保护）所需要的工具，可是很少有企业在部署和管理 WAF 方面具有专业知识。因此，许多公司将依靠方案提供商，让他们协助自己实现最好的产品部属。

“整个应用程序安全策略市场仍被严重低估”，位于美国密苏里州堪萨斯市的 Fishnet 安全公司常务董事 Mark Carney 表示，“情况正在改善，但是整个安全社区并不能很快地理解应用程序防火墙所需要的操作和管理水平，以及如何才能有效地对付 Web 应用程序漏洞。”

“整个应用程序安全策略市场仍被严重低估”

——Mark Carney

即使对于那些所谓的“复选框”规则遵从部署而言，这也可能是真的，因为他们需要满足某些特定的遵从规则，比如支付卡行业数据安全标准 (PCI DSS)中的要求 6.6，该规则要求用户要么部署 Web 应用程序防火墙，要么采用手动或自动的源代码审查或者应用程序漏洞扫描。

PCI DSS 要求对 Level 1 商家（每年交易量超过六百万份的企业）进行审计；MasterCard 最近增加了 Level 2 商家（每年的交易量在一百万份到六百万份之间的企业）的审计要求。经验丰富、积极的、合格的安全评估员（QSA）都希望公司能够证明他们已经安装了 Web 应用程序防火墙，并且正在运行。

位于美国宾夕法尼亚州梅卡尼克斯堡市的 ICSA Labs 公司（该公司是 Verizon Business 公司的独立部门，提供中立的安全产品测试和安全产品认证，其中包括 WAF 认证）负责 WAF 的经理 Brian Monkman 说道，“有些审计员会问，‘你

们有 Web 应用程序防火墙吗？’ 然后说， ‘好吧，检查一下’ 。但是有些审计员会问更具体的问题，而 Web 应用程序防火墙存在的时间越长，它们就越成熟，这些问题就越深入。”

位于美国加利福尼亚州 Redmond Shores 的 Imperva 公司首席安全战略家 Brian Contos 表示，企业通常需要确定用户如何与应用程序进行交互，以及应用程序可以访问哪些关键数据等。而合作伙伴所提供的预先发现（up-front discovery）功能可以当成一种 WAF 服务，从而确定应用程序和相关数据是否在规定的操作范围以内。

“毫无疑问，数据安全比网络安全更难管理，” Contos 表示。“如果你不知道敏感数据在哪儿，就很难搞清楚用户是如何进行交互的。”

“数据安全比网络安全更难管理，如果你不知道敏感数据在哪儿，就很难搞清楚用户是如何进行交互的。”

——Brian Contos

一般而言，WAF 是通过最初的规则标准进行“学习”的，其中包括一段时间的测试，以便确定哪些是可接受的行为、哪些有问题，以及哪些是恶意的。

这是方案提供商的另一个机会，因为测试结果必须加以分析，并把结果报告给客户。结果分析完成之后，方案提供商可以跟客户一起合作，根据公司策略以及潜

在的攻击，建立自定义规则，确定哪些行为是允许的，哪些需要警告，哪些需要阻止等。

Contos 指出，“这变成了一种顾问式关系，与只是提供技术相比大大提升了产品的附加值。”

大型的、复杂的 WAF 部署尤其如此。专家表示，为了能够最好地协助客户，VAR 应该懂得应用程序后面隐藏的业务逻辑、应用程序是如何工作的、它的开发平台式，以及它所使用的编程语言等。

Fishnet 公司的 Carney 表示，“我们需要了解的最重要的事情是应用程序都比较复杂。它们不像网络流量那么简单、那么容易预测。”

他指出，了解即将部署的新应用程序以及现存的应用程序是否有所变化尤其重要。客户必须经过培训，知道如何修改 WAF 规则来适应这些变化；或者必须与方案提供商约定好额外的服务，让他们来完成这些工作。

Carney 指出，“环境越是多变，产品就越需要照顾和管理。”

在动态的环境中，方案提供商可以用 Web 应用程序扫描器进行渗透测试，以发现变化引起的漏洞。Monkman 表示，消费者的 WAF 部署最好结合扫描工具或扫描服务。比如，WhiteHat Security 公司基于云的应用程序扫描服务就集成了多

个 WAF 产品。该服务（或者说产品）可以创建“虚拟补丁”，从而阻止某些特定的漏洞利用，直到问题代码被修复为止。

这对于不能离线的关键生产应用程序来说至关重要。创建和测试补丁都需要时间，尤其是当开发过程已被外包给别人时。

“你需要有人能够完全理解安全编码、Web 应用程序防火墙，以及漏洞扫描器是如何工作的、应该怎样整合它们，” Monkman 说道。

这种专业知识的整合非常短缺，这让方案提供商有了提供应用程序安全服务的机会，不仅仅是简单的 WAF 部署。

“为应用程序，尤其是为动态的应用程序设计安全特性，你最好有一个合作伙伴，” Contos 指出，“随着网络安全日益商品化，我认为这个领域将来会有很大的增长。”

（作者：NEIL ROITER　译者：Sean）