如何选择应用防火墙

如何选择应用防火墙

那些急于达到 PCI 安全标准的企业在选择 Web 应用防火墙(WAF)时往往无所适从。怎样才知道该选择什么产品？如何才能有效地部署和管理这些工具和软件？如何把它们与现有的基础架构有机组合起来？下面我们将列出在评估产品时帮助你遵从法规的需要着重考虑的几点。Web 应用防火墙（Web application firewall）或应用层防火墙是一种旨在保护 Web 应用程序免受攻击和数据泄露危害的装置或软件。

应用防火墙的优缺点

应用防火墙或代理确实有优于包过滤型和全状态包检测型(stateful packet inspection)防火墙的地方。虽然这些类型的防火墙可以防止各种网络层的攻击，但它们却无法阻挡利用大多数 Web 应用程序漏洞进行的攻击。利用这些严重的漏洞，黑客们操纵 URL 地址就可以直接攻击目标网站。不过，这些防火墙可以通过允许或拒绝特定的应用程序或者应用的特定功能，实现很多精细化的控制

- ❖ 应用层防火墙的优点和缺点

应用防火墙选择

不管提出什么样的新法规或者安全要求，法规遵从负责人员往往会急于作决定。许多系统管理员作决定的依据是一个厂商的广告词或者是正好需要的特殊要求欧或功能。结果很可能会发现买的并不是最适合的产品，或是无法实现最佳的安全性。在选择 Web 应用防火墙等安全设备时，你首先应该给出下面这些问题的答案。

- ❖ 如何选择合适的应用防火墙（一）之准备工作

- 如何选择合适的应用防火墙（二）之功能
- 如何选择合适的应用防火墙（三）之软件还是硬件
- 如何选择合适的应用防火墙（四）之部署
- 如何选择合适的应用防火墙（五）之管理

应用防火墙的选购标准

问：我们公司想要购买新的防火墙，我们已经选择了三个厂商。我们在评估可选的防火墙时应该才采用什么标准？有选择合适的企业防火墙产品的最佳实践吗？答：第一点，也是最重要的一点，考虑防火墙的功能。

- 购买企业防火墙的评估标准

应用防火墙的选择与配置最佳实践

应用层防火墙已经成为那些对法规遵从感兴趣的人们谈论的热点话题。支付卡行业数据安全标准（PCI DSS）原来只推荐应用层防火墙作为最佳实践。该标准将要求公司要么安装这种防火墙，要么进行代码检查。在考虑应用层防火墙时，每个企业应该注意四个因素。我们来分别看一下这些因素，以及现在市场上的一些应用层防火墙。

- 应用层防火墙选择与配置的最佳实践

应用层防火墙的优点和缺点

问：为什么采用主动模型的应用层（第 7 层）防火墙不是系统设定的选项呢？

答：应用防火墙或代理确实有优于包过滤型和全状态包检测型(stateful packet inspection)防火墙的地方。虽然这些类型的防火墙可以防止各种网络层的攻击，但它们却无法阻挡利用大多数 Web 应用程序漏洞进行的攻击。利用这些严重的漏洞，黑客们操纵 URL 地址就可以直接攻击目标网站。不过，这些防火墙可以通过允许或拒绝特定的应用程序或者应用的特定功能，实现很多精细化的控制。应用防火墙还可以直接验证用户身份，这意味着它允许或拒绝特定用户发出的远程登录命令，而其他防火墙只能控制特定主机的传入请求。

应用层防火墙可以检测数据包的有效荷载根据这些实际内容作出相应决定，还能提供更好的内容过滤能力。它们还可以审查完整的网络数据包，而不仅仅是网络地址和端口，这就使得它们有更强大的日志记录功能，例如可以记录某个特定程序发出的命令这样的日志事件，这对于处理突发安全事件和实施安全策略提供了很有价值的信息。

既然应用层防火墙有这么多明显的安全优点，为什么它却不是默认选项呢？其主要原因在于成本和性能。如果所有进站和出站的网络流量都需要在应用层上进行检测，那么数据在检测前就必须首先通过 OSI 的七层，而包过滤型和全状态包检测型防火墙在只网络层对流量进行检测。由于防火墙对数据包进行读取和解析必然消耗 CPU 周期，尤其是解析过程特别耗费 CPU 资源，所以很有可能形成网络性能的障碍。这也意味着应用层防火墙更容易受到分布式拒绝服务攻击，因此不太适合高带宽或实时应用程序。而它也很可能会成为操作系统里的安全漏洞。

应用层防火墙的另一个缺点就是对每个协议（如 HTTP、MTP 等）都需要单独的代理程序，因此它对新的网络程序或网络协议的支持很有局限性。虽然大多数防火墙厂商为了应

对未定义的网络协议或应用程序都提供了一般的代理程序，但在这种情况下，它往往会完全允许流量通过防火墙，而忽略很多应用层防火墙应做的操作。相比之下，状态包检测防火墙和包过滤防火墙一样，只会对网络性能造成很小的影响，因而可以实现对应用程序的透明和独立。随着客户端或代理数目的增加，可扩充性也成为了的问题。应用层防火墙通常需要网络中的客户端安装专门的软件或更改某些配置，以便能够连接到应用代理。这在一个大的网络里会造成非常大的影响。为了减轻防火墙的负载压力，在对那些及时性要求不高的服务（如 e-mail 服务以及大部分的网络流量）进行安全处理的时候，可能会需要对部署专门的代理服务器，从而也增加了全部费用。

希望你能明白应用层防火墙并不是任何人都会选择的。那么，你问题里提到的主动模型(positive model)是怎么一回事呢？一个应用层防火墙有两种途径可以实现，一是主动采取措施的主动安全模型(positive security model)，另一种是通过与已知攻击特征进行比对来认定攻击行为的被动安全模型(negative security model)。被动安全模型的缺点是：它对新发现的攻击没有防御能力，对特征数据库的更新也完全就是一项与时间赛跑的任务。在被动安全模型里，不能被认定为非法的行为就会被视为合法行为。而主动安全模型则与之不同，它关注的是哪些操作是用户允许的，也就是说，除了已被许可的操作，其它都是非法的。尽管主动安全模型是更好的选择，但是往往这类产品价格更高也更复杂。所以，归结起来，需要对时间和费用进行权衡。

（作者：作者：Michael Cobb 译者：Sean　来源：TechTarget 中国）

如何选择合适的应用防火墙（一）

那些急于达到 PCI 安全标准的企业在选择 Web 应用防火墙(WAF)时往往无所适从。怎样才知道该选择什么产品？如何才能有效地部署和管理这些工具和软件？如何把它们与现有的基础架构有机组合起来？下面我们将列出在评估产品时帮助你遵从法规的需要着重考虑的几点。

Web 应用防火墙（Web application firewall）或应用层防火墙是一种旨在保护 Web 应用程序免受攻击和数据泄露危害的装置或软件。它位于 Web 客户端和 Web 服务器之间，根据既定的安全策略来分析应用层报文里的非法数据。Web 应用防火墙位与网络防火墙和入侵检测/防御系统相比解决的是不同的安全问题，后者主要目的是保护网络边界。在急急忙忙购买前，你可得先做好心理准备，它可不是即插即用的法规复选框，也不是摆到你的服务器前就能用的。

你需要知道的

不管提出什么样的新法规或者安全要求，法规遵从负责人员往往会急于作决定。许多系统管理员作决定的依据是一个厂商的广告词或者是正好需要的特殊要求欧或功能。

结果很可能会发现买的并不是最适合的产品，或是无法实现最佳的安全性。就算是时间紧迫，也并不能轻视对产品的考查。在选择 Web 应用防火墙等安全设备时，你首先应该给出下面这些问题的答案：

- 为了达到安全策略的目标法规的要求，需要执行哪些措施？
- 哪些附加的服务能真正起到作用？
- 它如何与你们现有的网络整合--你们自己是否有正确并且有效地使用它的技术？
- 它将对现有服务和用户造成怎样的影响，需要付出多大代价？

像 PCI DSS（支付卡行业数据安全标准）这样的新法规要求你在回答第一个问题之前先更新或者至少检查安全策略。一套良好的安全策略能够明确保护你的数据所需达到的目标和要求。在此基础上，你才知道哪些安全设备是适合你的需求的。因为每个 Web 应用程序都是互不相同的，所以必须在软件安全开发周期(secure lifecycle development)的威胁建模(threat modeling)阶段就对其安全策略进行定制，以杜绝潜在的安全隐患。另外还一定要注意你所中意的那一款应用防火墙是否有应对以下威胁的能力：分析通过 cookie 或 URL 传递的参数，防御开放 Web 软件安全项目（OWASP）提出的十大应用漏洞，以及安全标准里提出的其它要求。

（作者：Mike Cobb　译者：Sean 来源：TechTarget 中国）

如何选择合适的应用防火墙（二）

选择 WAF

为了确定一款 Web 应用防火墙(WAF)确实符合 PCI DSS，你还应该对照一下 PCI 安全标准委员会发布的《信息补编：需求 6.6 版 代码评估和应用防火墙阐述》(Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified) [链接：https：//www.pcisecuritystandards.org/pdfs/infosupp_6_6_applicationfirewalls_codereviews。PDF 格式]。

他们必须能够检查和处理 HTML ，动态 HTML （DHTML），级联样式表（CSS）等网页内容 ，另外还要有对你的程序所使用的 HTTP，HTTPS 等协议的检查和处理能力。

此外，最好再了解下厂商过去对新协议的反应速度有多快。你可以审查一下他们的开发和支持服务条款，以确定他们是否对自定义协议提供支持，是否对足够广泛的应用协议提供支持。另外，WAF 必须能够检查 Web 服务信息，通常包括的 SOAP 和 XML 。你可以问问供应商是如何进行自动更新以及如何应用动态签名(dynamic signature)的。这样的交流可以帮助评估他们的技术支持和服务能力。

最后，询问每项特殊功能所需的额外费用。例如，有些应用程序可能需要 FIPS 硬件密钥库的支持。有的 Web 应用防火墙(WAF)厂商的确能提供这一功能，但却价格奇高。

随着一项一项解决需求，建议你花些时间去了解一下每种 WAF 的用于为一个或者更多的安全区域提供支持的技术细节和处理深度。你能正确指出合法的数据类型和范围并创建组合使用白名单和黑名单的安全规则吗？WAF 在面临对它自身的攻击时，抵抗力有多强？比如，它应该运行在一个可靠的操作系统上，可能还有组件在一个无特权并且封闭的环境里运行。如果这套产品的安全性还未达到坚如磐石的程度，那你的讨论也该就此中止了。

(作者：Mike Cobb 译者：Sean 来源：TechTarget 中国)

如何选择合适的应用防火墙（三）

软件还是硬件

按照 PCI 信息补编(Information Supplement)的规定， WAF 可以在运行通用操作系统或设备的标准服务器上用软件实现。设备既可以是独立的，也可以是与其它网络组件集成到一起的。所以，你可以从市面上各种 WAF 里选择。

软件 WAF 通常更便宜、更灵活。硬件防火墙则更容易安装和配置，这是因为他们的操作系统已经固化在硬件里，而软件防火墙则还需要你自己去加固操作系统。（WAF 没法让你免受服务器上的错误配置或漏洞的危害）

如果你选择软件防火墙，那最好选用能在你们 IT 部门熟悉的平台上运行的产品。而且不管是选择哪种，都要留意厂商提供了怎样的培训，培训费要多少。

当然，还有许多开源软件 WAF 可供选择，如 ModSecurity[http://modsecurity.org] 和 AQTRONIX WebKnight [http://www.aqtronix.com] 。如果他们能满足你的需求，那就可以大大降低成本，但工作人员仍然需要学习、安装、配置和维护这些软件。许多开源项目都有很好的技术支持论坛，但不像那些商业软件，你在碰到紧急情况时没法呼叫服务台求援。

性能和可扩展性也是你在硬件防火墙和软件防火墙之间作选择时需要考虑的重要因素。有些设备每小时所能处理的事务数可能会受到限制。有些设备则可能有带宽的限制。如果你需要应对不断增长的网络活动或者不久之后添加一些应用，那就应该选择一款扩展性和灵活性好一些的产品。

软件产品往往比硬件升级起来更方便，但硬件系统的更适合高流量的网站，这些网站需要很高的吞吐量。

如果你运行的是一个大规模的应用，需要一个以上的 WAF ，那么集中管理可能就成了一项至关重要的功能，因为它能让你在一个地方集中地部署和管理防火墙规则。

我们的建议是不要在一颗树上吊死，只要它能满足你的要求，而且你有配置和管理的技术，那么软件防火墙和硬件防火墙都是很管用的。

(作者：Mike Cobb 译者：Sean 来源：TechTarget 中国)

如何选择合适的应用防火墙（四）

现成的帮手

准备好充足的时间来对 WAF 产品作彻底的评估吧。一旦你的选择范围缩小到了那些能满足你基本要求的产品，下一步该如何对这些不同的选择进行比较呢？

Web 应用安全协会（Web Application Security Consortium，WASC ） [链接：http://www.webappsec.org/]就是 Web 应用安全标准的制定者和拥护者。他们已经开发出了 Web 应用防火墙评价标准（ WAFEC ） [链接：http://www.webappsec.org/projects/wafec/]用于产品间的对比分析。任何一位熟练技术人员都可以用他们的测试方法来独立评估一套 WAF 解决方案的质量。

建议你把他们的评价标准作为你的评估过程的一部分。按照 WASC 的建议，密切留意所使用的部署架构，对 HTTP、HTML 和 XML 的支持，所采用的检测和防护技术，日志和报告能力以及管理和性能等方面。

部署 WAF

恭喜！到这一步，你已经选择，购买并安装好了 WAF，也达实现了必需的法规功能。但是，这并不意味着你已经遵从法规了。正确的定位，配置，管理和监控都是必不可少的。

安装过程需要遵循四步安全生命周期：防护，监控，测试和改进。这是一个循环往复，持续不断的保护过程。在把任何新设备连接到你的网络前，都必须确保已经将当前的网络结构记录在案，然后还要加固一下那个新设备以及它的运行环境。也就是通过打补丁和改进配置的方式来增强安全性。

配置结果是根据你在安全策略（如允许哪些字符集）里确定的业务规则直接生成的。如果你采用这种方式配置防火墙，那么防火墙规则和过滤器都将自我界定。在网络或应用里，WAF 还可能会暴露出一些技术问题，如误报或是传输瓶颈。

认真的测试是必不可少的，尤其是如果你的网站使用了特殊的 header、URL 或 cookie， 或者是网站的具体内容不符合 Web 标准。如果你运行的是一个提供多语言版本的应用，那就要计划出更多的测试时间，因为它可能要处理不同的字符集。

测试应尽可能与“真实”的应用环境相吻合。这将有助于在部署之前把 WAF 可能导致的系统集成问题暴露出来。使用微软的 Web Application Stress 和 Capacity Analysis Tools 或 AppPerfect Load Tester 对 WAF 进行压力测试也有助于发现配置 WAF 带来的瓶颈。

（作者：Mike Cobb 译者：Sean 来源：TechTarget 中国）

如何选择合适的应用防火墙（五）

WAF 管理

当防火墙启动并运行起来后，就得随时考虑将来 Web 应用防火墙的变动会对你的 Web 应用带来怎样的影响了，反之亦然。你还必须得对网络结构中的变动记录，以方便以后查找和解决问题。这要求你跟踪现在和将来对其配置所做的任何更改.

在生产环境下进行任何改动都只应该在监控维护窗口下进行。确保事先告知了公司里可能受影响的各方改动的时间和范围。为了杜绝对配置的意外改动或未经正常程序的改动，必须在逻辑上和物理上控制对安全设备的访问。严格遵守变更控制、业务连续性和灾难恢复策略，将在保护 WAF 和你的业务时发挥出作用。

由于应用层防火墙的检查整个网络数据包，而不是仅仅是网络地址和端口，因此他们有更强大的日志功能，可以记录特定应用命令。所以，不要让这种能力和信息浪费。分析日志文件可以警示你即将到来的或正在进行的攻击。确保你已经正确定义了那些你希望防火墙日志记录的信息--最好完整记录请求和响应数据，包括 header 和正文里的有效数据。确保你的工作人员足够专业-并有充足的时间-来审查和分析日志。

Web 应用将永远不会百分之百的安全。即使没有让你迅速部署 Web 应用的内部压力，也还是有漏洞会暴露出来。在适当地配置 Web 防火墙，并把它作为分层安全层模型的一部分，你可以观察、监控和搜寻入侵的线索。这也显示出了手忙脚乱地修复漏洞和有充足时间修补漏洞的差别。

（作者：Mike Cobb　译者：Sean 来源：TechTarget 中国）

购买企业防火墙的评估标准

问：我们公司想要购买新的防火墙，我们已经选择了三个厂商。我们在评估可选的防火墙时应该才采用什么标准？有选择合适的企业防火墙产品的最佳实践吗？

答：第一点，也是最重要的一点，考虑防火墙的功能。对于这些二选一的产品的一个好消息是主流防火墙都有相同的核心功能。每一种都可以执行信息包检测，并允许基本边界防御的实行。我建议研究一下功能的要求。问一下自己：你需要强调网络的吞吐量还是提高安全功能？

防火墙之间的一个主要区别是他们在应用层检测的能力。很多防火墙都没有应用层检测，而其他的可以实现基本的功能（例如 URL 过滤）。有些产品，例如 Secure Computing Corp.的 Sidewinder G2 防火墙和 F5 Networks 的 BIG-IP Application Security Manager 有深入的应用检测功能。这些类型的防火墙允许复杂的应用规则基础。这些规则可以限制连接上的行为。例如，你可能会限制从互联网到 GET 命令的入站 HTTP 请求，而互联网用户可能可以发出 POST 命令。这个功能可以允许你保护企业不受到应用攻击和网络攻击。

最后，考虑厂商自己。当投资到防火墙产品的时候，你正在制定长期的决定。财政问题只是冰上一角；你的防火墙管理员将会投入时间和精力为特定的产品创建和定制规则基础。总的来说，规则不是可以在平台之间移动的，所以任何进一步的平台的变化都需要实际的人力，因此，确保你选择的厂商都是经济实力强大的稳定的公司。你当然不希望登上可能沉没的船只。

（作者：Mike Chapple 译者：Tina Guo 来源：TechTarget 中国）

应用层防火墙选择与配置的最佳实践

应用层防火墙已经成为那些对法规遵从感兴趣的人们谈论的热点话题。支付卡行业数据安全标准（PCI DSS）原来只推荐应用层防火墙作为最佳实践。该标准将要求公司要么安装这种防火墙，要么进行代码检查。

今天，虽然多数机构多少拥有一些边界防火墙，可以保护网络不受恶意的因特网信息流的攻击，但是这些种类的防火墙并不能保护企业，使其免于受到穿越应用程序的威胁。

据反恶意软件经销商 Sophos plc 和 Symantec Corp.的报告称，最近，应用层防火墙已经出现，它是一种防御 Web 应用攻击的工具。Web 应用程序攻击是一种最常见的入侵类型。传统的网络防火墙不能检测到应用攻击，原因是它们在合法应用程序的开放端口上才能起作用。虽然网络防火墙检查端口和 packet headers，但是，它们并不能核查应用程序和应用程序数据，它们可以在通过开放防火墙端口时，不知不觉地隐藏恶意活动。由于大多数 Web 信息流通过端口 80 或者端口 443，而关闭这些端口是不现实的。

PCI DSS 也已经开始关注应用层防火墙。名声不太好的 Section 6.6 涵盖了 Web 应用程序安全，号召公司对其应用程序进行代码核查，或者使用应用层防火墙，来保护用于处理信用卡的代码。

不幸的是，PCI DSS Section 6.6 将应用程序安全解释为一种非此即彼的命题，但是它远比这个要复杂得多。应用安全不仅仅是关于代码核查或者防火墙；在一些情况下，它可以意味着两者兼而有之。网络安全是关于关闭端口和关闭不必要的服务，应用程序安全与此不同，它是有关保护编码和设计的。

正如任何安全工具或者做法，应用层防火墙应当仅仅被看作是较大规模安全程序的一部分，并不是单一的防御 Web 应用攻击的一种方式。它应当是多层防御的一种。多层防御包括应用漏洞、渗透测试以及个软件开发生命周期中的安全漏洞的代码核查。

选择并配置应用层防火墙

在考虑应用层防火墙时，每个企业应该注意四个因素。我们来分别看一下这些因素，以及现在市场上的一些应用层防火墙。

首先，它真的是应用层防火墙吗？或者仅仅是一种深度信息包检测器？该区别很重要。为了与 PCI 一致，它必须是一个真正的应用层防火墙，而不是一个冒名顶替的工具。

一个真正的应用层防火墙可以检测应用程序的信息流，以防诸如 SQL 注入或者跨站脚本攻击（XSS）之类的恶意代码。当然，这就要求深度信息包检测，但是深度信息包检测仅仅查找信息流中诸如恶意软件和间谍软件之类的攻击，而无法检测到通过应用程序发送的恶意代码。

传统的网络防火墙仅仅可以检测 packet headers，与之不同的是，深度信息包检测可以检测信息包内部及其内容。这虽然绝对可以增强防火墙的能力，但并不能算作一种防止攻击的防御，它仍然有一些局限性。

另一种常见的误解是将应用层防火墙与网络安全网关和内容过滤产品混为一谈。不要因为安装了一个应用层防火墙，就关闭你的 Blue Coat、Vontu 或者 Vericept 系统。这两种产品进行不同的工作。内容过滤产品可以阻止不合适的网站，或者基于 Web 的电子邮件，这些都可能包含恶意软件。但是同样地，它们不能捕获网络应用攻击，有时这仅仅是网站内容的一部分。虽然这两种产品都可以使用 URL 过滤，但是，应用层防火墙可以在 URL 中查找恶意代码：比如 XSS 攻击中使用的 JavaScript；而内容过滤器仅仅在网络地址本身中查找。

尽管如此，网络安全网关、内容过滤产品和应用层防火墙已经慢慢地融合为统一的工具。该发展是自然而然的，因为许多威胁也已经结合起来并且现在需要多层防御。比如，虽然该内容过滤器可能会也可能不会阻止恶意站点，但是应用层防火墙会阻止它所携带的恶意代码。

在最低程度上，应用层防火墙应该防止注入攻击，比如 SQL 注入和 XSS、会话劫持、扫描和检索、cookie 篡改、以及路径遍历（path traversal）企图。应用层防火墙可以核查尖峰或者不规则信息流模式，进而阻止拒绝服务(DoS)攻击，也可以能够处理标准的 HTTP 和 SSL 信息流。

第二，应用层防火墙是否允许通过访问控制的精细保护？访问控制是流程稽核的一大部分。不仅仅是 PCI，SOX 和 HIPAA 都要求全部核查哪些人访问了企业的系统，以及他们都访问了什么。应用层防火墙可以扮演监测这个访问的角色。

在应用层防火墙中搜索的第二个特征是其与身份和访问管理系统的结合能力。这使得防火墙调整到允许员工访问特定的 Web 应用程序，但是不允许公司其他任何人访问。一些员工可能需要访问基于 Web 的电子邮件或 WebEx，来进行其工作。如果防火墙与公司的诸如 Active Directory 或者 LDAP 之类的目录服务结合起来的话，这是可以调整的。访问应用程序可以添加到员工的配置里。

应用层防火墙本身，与其相对的网络防火墙一样，也应该有角色访问，仅允许授权的管理员访问，进行维护和更新。

应用层防火墙的第三个关键的问题是其与公司网络的兼容性。应用层防火墙是另一种可能会拖延网络的设备。如果没有合理配置的话，或者与公司的构架不兼容时，它会导致运行问题。它是否会拖延你的网络，减缓访问者登录你的网址；或者由于它在你的网络上是无形的，它是否就是透明的？

一般说来，应用层防火墙与网络防火墙同时运行，通常是在它们后面的网络内部。入局通信量首先通过网络防火墙，然后再通过应用层防火墙。在考虑完全安装一个产品之前，经常核查防火墙的吞吐量，并且在你的运行环境中对其进行彻底的负载测试。在配置产品之前，任何速度变慢、瓶颈、或者性能问题都应当解决。

最后，就像网络防火墙一样，应用层防火墙应当有能力将信息流记入日志。除了是一种安全最佳方式以外，追踪事件也时很必要的，在一些情况下，法规遵 conh 可能需要这

个功能。记录日志是否有能力追踪事件并对不合适的访问出具报告？PCI 在网络监测方面的要求是非常严格的。这是应用层防火墙功能的核心部分。

应用层防火墙的主要市场来自 Barracuda、Palo Alto Networks、F5 Networks、Breach Security 和 Imperva。其它提供应用层防火墙的厂商还有 Juniper、Fortify 和 SonicWall。

Barracuda Web Site Firewall 宣称自己适用于 Sections 6.5 和 PCI6.6。Section 6.5 要求 Web 应用满足开放 Web 软件安全计划（OWASP）的编码导则。Barracuda Web Site Firewall 代理所有网络信息流，防御通常熟知的 Web 攻击、会话劫持企图和来自所有在线形式的验证输入，以及最为常见的 XSS 攻击。

Palo Alto Networks PA-4000 系列的产品宣称自己是一种以应用程序为中心的防火墙。它可以与策略编辑器协调使用，而策略协调器可以在特定的应用程序中添加一个基于漏洞的防火墙规则。Palo Alto Networks PA-4000 系列产品还拥有 App-IDTM，这是可以实时进行应用程序信息流分析的信息流分类技术。

应用层防火墙，与其它新的安全技术一样，正越来越流行，并被引入到现有的安全产品中。此外，随着应用程序安全越来越重要，它们也越来越受到人们的欢迎。但是应当仔细检查产品，确保正确使用，以保护您的公司免于受到应用攻击。

（作者：Joel Dubin　译者：李娜娜 来源：TechTarget 中国）