配置应用防火墙

配置应用防火墙

市场研究公司 Gartner 最近发表的研究报告强调了这种威胁并且预测当前成功的攻击有 75%以上发生在应用层。Gartner 甚至提出了一个更吓人的预测：到 2009 年年底，80%的企业将成为应用层攻击的受害者。这正是应用层防火墙发挥作用的地方。这些防火墙在 HTTP 通讯到达网络服务器之前对这些通讯进行应用层检查。这些设备能够检测到一个连接并且分析用户正在提供给这个应用程序的指令的性质和类型。然后，它们能够根据已知的攻击特征或者异常的应用状况分析这些通讯。

应用防火墙的选择原因

传统的防火墙技术，比如，信息报过虑和状态检测，已经不再合适，因为他们不能区分恶意和非恶意需求和数据。多样性和流量也使传统防火墙更难对过滤器实行单纯的“允许/阻止”原则。防火墙厂商通过开发应用层防火墙来应对这些威胁。和传统防火墙相比，应用防火墙过虑设备提供更好的内容过虑功能。应用防火墙还可以检查信息包的有效载荷，并根据内容作出判断，允许或拒绝具体的应用程序要求和命令。防火墙的功能使得管理员在网络流量的粒控制方面有很大的权限。

- 防火墙技术必须改变吗？
- 应用防火墙——足以保证当前网络服务的安全副标题所属文章

应用防火墙的创建和部署

在考虑应用层防火墙时，每个企业应该注意四个因素:首先，它真的是应用层防火墙吗、第二，应用层防火墙是否允许通过访问控制的精细保护,它与公司网络的兼容性如何以及应用层防火墙应当有能力将信息流记入日志。如果对于应用层防火墙没有预算，那该怎么办？答案是使用开源组件来构建你自己的应用层防火墙。一旦准备把应用防火墙应用到生产环境，就应该考虑建立防火墙规则库。

- 应用防火墙：一点一点地砌
- 建立部署应用层防火墙规则库的四个步骤
- 应用层防火墙选择与配置的最佳方式

应用防火墙的应用技巧

为了更有效，应用防火墙必须和应用程序以及需要保护的网络环境完全契合。配置较差的防火墙可能阻止合法用户、客户和伙伴——或者给予黑客访问系统和数据的权利。在本小节中，TechTarget 的特约专家将讨论应用防火墙的类型以及如何调整使他们适应机构的环境。

- 应用防火墙技巧

应用防火墙的缺点

Web 应用防火墙的主要缺点是成本和性能。性能通常都是问题，因为这些工具检查应用层的所有入站和出站流量。尽管如此，这种级别的检查通常被称为深度信息包检测，它检查信息包的实际有效负载，并提供比传统的包过滤防火墙更好的内容过滤功能。应用防火墙的另一个缺陷是每个协议，例如 HTTP、SMTP 等，都要求自己的代理应用程序，并支持新的网络应用程序，协议可以别限制或者降低出现的机会。

- 应用防火墙的缺点

应用防火墙的选购建议

在购买企业防火墙的时候需要考虑的第一点，也是最重要的一点就是防火墙的功能。。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？另外还要考虑到厂商是否可以提供长期支持。

- **购买企业防火墙的评估标准**

防火墙技术必须改变吗？

问 ：为了适应使用 HTTP（端口 80）的应用程序越来越多的现象，防火墙技术必须要改变吗？

答：大部分情况下，是这样的。在过去的几年中，Web 为基础的应用程序的增长速度令人难以置信。Web 浏览器是现在最常用的应用程序用户界面，而大部分的浏览器应用通信程序都使用端口 80。对于开放式通信系统（Open System Interconnection，OSI）的应用层，也就是第 7 层的攻击是对防火枪的一次真正的挑战，因为恶意代码“化装”成合法的客户需求和正常的应用数据。

传统的防火墙技术，比如，信息报过虑和状态检测，已经不再合适，因为他们不能区分恶意和非恶意需求和数据。多样性和流量也使传统防火墙更难对过滤器实行单纯的“允许/阻止”原则。 比如，某一个防火墙可能仅仅允许端口 80 上的 HTTP 流量，但是这样的限制条件也可能放过了类似合法 HTTP 要求的 SQL 注入攻击。间谍软件，同样也仍然依据外部服务器认证书，在端口 80 上运行信道。

防火墙厂商通过开发应用层防火墙来应对这些威胁。和传统防火墙相比，应用防火墙过虑设备提供更好的内容过虑功能。应用防火墙还可以检查信息包的有效载荷，并根据内容作出判断，允许或拒绝具体的应用程序要求和命令。防火墙的功能使得管理员在网络流量的粒控制方面有很大的权限。比如，管理员可以允许或拒绝来自某个用户的具体的引入远程命令。现在，很多的应用层防火墙允许创建过滤器，截取、分析或修改到达你网络的流量，使防火墙可以更好，跟简单地保护具体资产。

一个防火墙应该“学会”什么是，什么不是某个具体网络的正常流量，并据此改变行为。虽然，真正需要解决的问题，是把网络流量和前后连接起来.是不是有每周的电子新闻邮件带出的大量突然的带外邮件，或者由一个被攻击的机器发送垃圾邮件？是不是需要

一份黑客采样的数据库的数据库表格，或者管理员进行的必要任务？为了解决这些问题，防火墙将需要和认证系统以及其他的周界防护进行进一步整合，为监视流量增加关联。

对抗应用层攻击总是需要不只一个防火墙，不管他们变得多么复杂。应用程序开发团队也要负责任，保证通过防火墙的流量在进入应用程序前经过了检测和清洗，而应用程序可能会遭到破坏。无论安装的是什么防火墙或周界防御工具，假定所有的数据来源都不可信任，这一点非常必要。还要谨记防火墙永远不能防止网络钓鱼和社会工程攻击。也就是说，比如对所有的信息安全所作的努力的案例中，最后一道防线是员工的安全意识。

（作者：Michael Cobb 译者：Tina Guo 来源：TechTarget 中国）

应用防火墙——足以保证当前网络服务的安全

一年前，我开始着眼于研究网络服务安全；一年后，安全所涉及的问题仍然是客户不能接受网络服务配置的主要原因之一。网络服务安全标准仍然在发展之中，相对较少的客户正在使用网络服务，他们所依赖的是一种靠得住的新版本工具：防火墙。

当防火墙用于网络中时，它会检查数据包，比如，检查数据包是否来自一个可接受的IP 地址或者网址。当用于网络服务环境中时，防火墙会检查用可扩展标记语言（XML）编写的网络服务请求，或者简单对象访问协议（SOAP）所传输的网络服务请求。

所谓的应用防火墙、XML 防火墙或者 XML 通信网关，它们或者作为软件出售，可以在服务器上运行；或者作为专用的、严格安装的设备出售。许多产品将检测网络服务信息的功能与其它功能结合起来，比如专业芯片可以加速 XML 信息（XML 信息比网络防火墙扫描的数据包要大得多）的进程，或者提高执行身份管理的能力。

诸如身份管理之类的功能将会越来越重要。Jason Bloomberg 是马萨诸塞州瑟姆福雷斯特市的一家网络服务研究公司 ZapThink LLC 的高级分析家，他说：“如果有人仅仅能查看 SOAP 信息的内容，并获得你的信用卡号码，这并不会起到多大作用。”

Bloomberg 说：“可以防止这种偷窃行为的主要经销商有 Forum Systems 公司、Westbridge Technology 公司、Reactivity 公司、Vordel 公司、Sarvega 公司和 DataPower Technology 公司。每家公司都自夸将安全、加速度和策略管理性能进行了不同结合。比如，DataPower 公司的 XS40 XML 安全网关设备结合了一些安全特性：如将带有加密、解密功能的 XML/SOAP 防火墙与安全套接层(SSL)通信量的加速度结合起来。

KaVaDo 公司的创始人之一、技术总监 Yuval Ben-Itzhak 说：“KaVaDo 公司将其 InterDo 应用层防火墙与 ScanDo 网络服务安全扫描器结合起来，该网络安全扫描器可以分析配置在网络服务器上的应用程序，并构建一个可接受行为或者用户请求的框架。”他还

提到：“仅仅允许特殊准许的信息流通过，这样 InterDo 就减少了误报，否则误报会使安全管理员不安。使用 ScanDo 不仅仅为每个网络服务加速了创建合适安全策略的进程，也同时为网络服务中的特殊操作（诸如“核查目录级别”）加速了进程。”MagniFire WebSystems 公司对其 TrafficShield 设备也采取了类似的方法，TrafficShield 设备使用“智能、履带式技术”来编写应用程序，并自动创建一个策略来保护应用程序。

Westbridge 公司出售一种“XML 通信网关”，它可以储存特定的安全策略，比如说可以为不同级别的客户或者供应者进行存储，而无需将其硬编码到网络服务中。这使得审计更容易、更便宜，需要的时候可以执行并改变这些策略。

一些经销商也表示，他们正协商将其应用层防火墙与现有的网络防火墙结合起来，提供对数据包和 XML 文件的单点控制。Ben-Itzhak 说：“客户正寻求应用层防火墙和网络防火墙之间、认证产品和负载平衡产品之间的更多结合。”

但是，Champion 提到，他的客户，几乎没有一个想要这样的公用设备，理由是他们担心发送网络服务信息流到网络边缘附近，会更容易受到外部攻击的威胁。

Bloomberg 说，未来另一个大的挑战是企业身份管理——可以追踪哪个用户访问了组织内部哪些资源的能力，以及了解到何时特定用户请求访问应用程序、数据库或者其它资源的能力。他指出，这在网络服务环境中是非常重要的，对于某个特定用户而言，服务请求可能是无法追踪到的，但仅对于服务器或者应用程序而言，是可以追踪到的。

他指出，为了确保请求是来自一个合法用户，当用户进入网络时，必须要经过认证，不同的系统会产生或者接收网络服务的请求，认证之后在这些系统中必须分配一个令牌，以在其路径上跟踪这一请求。如果公司之间共用网络服务，“由于两家公司拥有独立的身份基础设施，这将是一个更大的挑战。”

两大组织正在为这些联合的身份管理制定标准。本月，BEA Systems 公司、IBM、微软、RSA Security 公司和 VeriSign 公司发布了 WS-Federation 互联网交易安全标准，该标准的设计目的是为了准许不同组织的应用程序所使用的认证与访问控制系统可以共同工

作。第二个是“自由联盟计划”（Liberty Alliance Project），该项目是由 Sun Microsystems 公司以及 170 多家公司、非赢利性组织和政府组织支持发起的。Bloomberg 说：“现在还不是很清楚，我们是否需要一个以上的联合身份标准，或者确切的说是他们将如何共同工作。”

直到那时，诸如 Netegrity 公司、RSA、Oblix 公司、Novell 和 Sun 之类的经销商会将其身份管理工具推向市场。Bloomberg 将 Netegrity 公司称为身份管理界的领袖之一，Netegrity 希望用网络服务安全的 TransactionMinder，来进一步推动其 SiteMinder 认证技术和认证工具的成功。TransactionMinder 配置了代理器，使用来自 Netegrity Policy Server 的数据进行身份认证，并确定谁有权访问特定的网络服务，进而对用来调用网络服务的 XML 文件内容进行扫描和分析。

通过将访问执行点（代理器）从策略服务器上分离，Netegrity 的机构体系比它的竞争者更容易在组织内衡量多个点——一个分布式的安全模式，许多分析家认为它比仅对网络中的点进行集中控制要好得多。

Oblix 和 Westbridge 最近宣布了身份管理工具和应用层防火墙的结合，这是各种各样的网络服务安全性能正集中到一个产品中的另一个标志。

Bloomberg 说，虽然经销商致力于将更多的性能融合到产品中，以及标准组织全心全意完善其标准，但那些需要网络服务的客户应该开始应用这些标准，并依赖现有的安全工具。他提出建议：“如果网络服务和以服务为标准的结构体系可以满足你现在的需求，不要再犹豫了，因为这些标准还不够成熟。”

（作者：Robert L. Scheier 译者：李娜娜 来源：TechTarget 中国）

应用防火墙：一点一点地砌

如果对于应用层防火墙没有预算，那该怎么办？答案是使用开源组件来构建你自己的应用层防火墙。

HTTP 正迅速成为任何以及所有的默认传输器。随着网络服务和以服务为标准的结构体系的出现，XML 已经成为一个粘合体，它将完全不同的应用程序和数据类型结合到一起。网络入口、内容管理系统、以及甚至企业博客和 wikis 正成为首选的沟通渠道。

但是，保护网络应用程序是一场艰难的战斗。虽然，传统的网络安全防御已经集中于 OSI（开放式系统互联）的前四层，但是，根据定义，大多数网络应用程序开发是通过代理器和防火墙的有效 HTTP 信息流。

该怎么办呢？你当然可以购买一个商业网络应用层防火墙产品，但是，也许你不能（或者不会）在预算中添加另一个年许可更新。另一个选择就是使用免费的开源工具，解析、重写并过滤 HTTP 信息流，以预防应用层攻击，进而构建一个网络应用层防火墙。你不会获得商业解决方案的所有功能（见右“开源网络应用层防火墙与商业网络防火墙”）。但是，你将在因特网所面临的网络服务和应用程序前面，添加一个亟需的保护层。

坚实的基础

网络应用层防火墙将完美地处在因特网所面对的防火墙之后，充当着所有网络信息流的核心出入路径。使用强化的 Unix 或者 Linux 平台，比如 OpenBSD 有堆栈保护、最小安装和积极的源代码审计。Bastille 也是一个出色的强化工具，可用于大多数 Linux 的分配。

由于防火墙会解析所欲的网络信息流，负载会大大高于典型的代理器。你需要很大的CPU，只有在你所能负担的范围内，此外还有大量的RAM。你可以构建一些备用的网关，并在多个安全网关前端使用HTTP负载平衡器。

然而，得出这样一个解决方案是复杂的。作为网络IDS或者IPS配置，你所配置的数量、进入站点的信息量、以及重新编写和解析操作的复杂度都会影响到性能。

此外，良好的浏览规则可以保证您的网络应用层防火墙与您最繁忙的网络服务器一样大。由于性能会因你的组织所使用的应用程序类型的不同而异，所以在任何生产制造之前，准备好调试、测试以及基准。

所需知识

作为网络应用层防火墙构建者，你需要有一个坚实的Unix/Linux背景知识，以及对网络应用程序、网络攻击、和HTTP协议有扎实的了解。一些会感觉有点像网络开发：你需要进行测试，并确保过滤不会影响任何网络应用程序，并运行诸如Nikto (www.cirt.net)之类的网络扫描工具，进而对比原始内容和代理内容。

你应该了解指令行周围的方式，并熟悉Apache配置语法，进而下载所需要的程序块，创建安全规则和过滤表达式。你会发现采用规则表达式（通常用于Snort规则中）工作的良好舒适程度也将派上用场。

现在，我们来探讨一些开源组件，你可以用来构建网络应用层防火墙。

奠基工作

在所有现有的商业代理器和开源HTTP代理器中，Apache网络服务器解析和改写内容的能力突出。Apache包括一个快速稳定的内置HTTP代理器，作为其核心分配的一部分，此外，其模块化设计允许你进行广泛的调试，这样你可以在单代理器配置中进行配置。你可以利用其内容感知来构建一个过滤和改写HTTP代理器。

Apache 从 2.0 版开始，包括作为内置模式匹配引擎的 PCRE (Perl 兼容正则表达式)库，这大大地提高了规则表达式的性能。它还允许指令多个基于内容类型的解析和改写操作。

这些特点与后面将讨论的第三方和内置式模块进行结合，为保护网络应用程序提供了一个强有力的工具包。

构建平台

Mod_security(www.modsecurity.org)是防火墙的网络入侵防御能力的核心。虽然，它从一个简单的基于模式的过滤引擎开始，阻止网络蠕虫信息流，但是，它已经发展成为一个成熟的网络安全套件。

Mod_security 签名使用一种规则的基于表达式的过滤语言，Snort 用户很熟悉这种语言，该签名可以通过 mod_security 站点自动更新，这与典型的 IDS 签名很相似。这些包括反跨站点脚本攻击的过滤器和 URL 中的 SQL 语句，以及包含界面指令和路径或者用户 ID 信息的信息流。

mod_security 需要经常更新签名，在 www.gotroot.com 上可以免费下载。

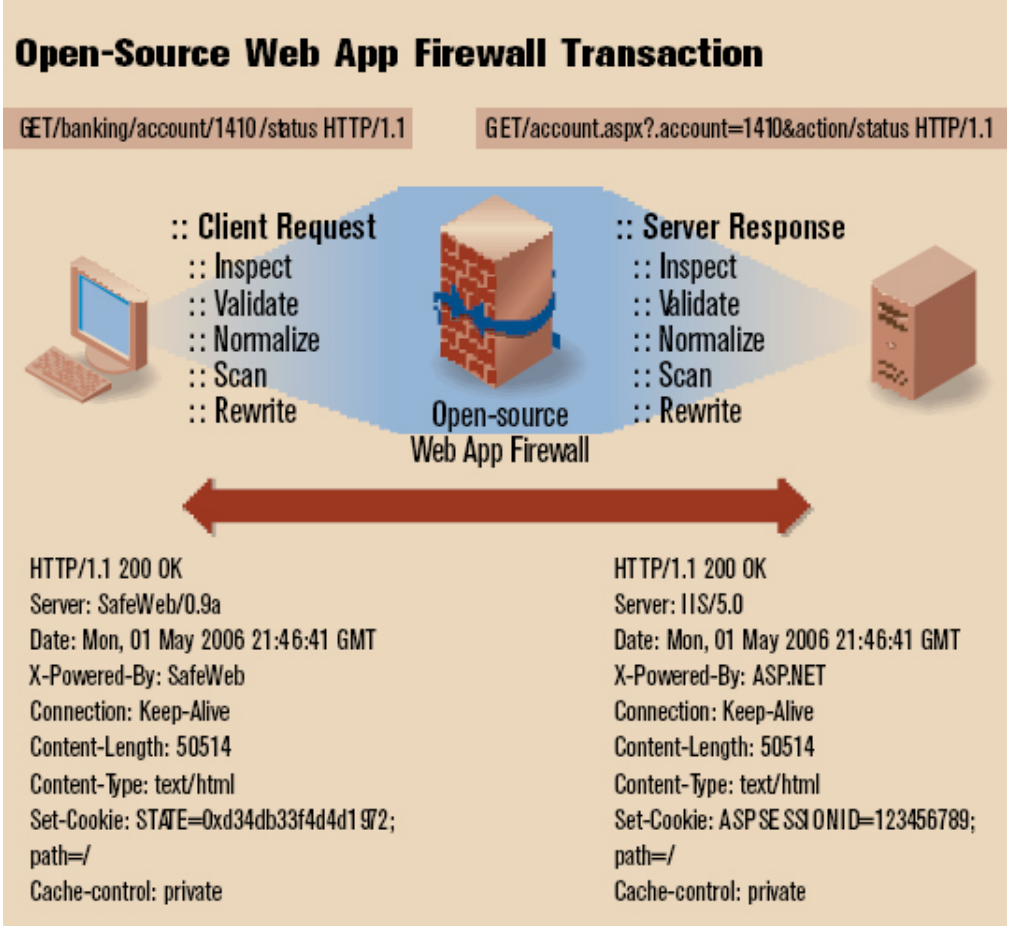
Mod_security 也使 Uni-code 信息流恢复正常，并对其净化，以防止 URL-解码攻击。

Mod_security 的模式匹配也能用于防止错误信息泄露。错误信息泄露可能会给攻击者提供有用信息。任何有可能泄露网络服务器配置的信息都会经过过滤，并将其改向为一个通用的错误信息。你也可以使用 mod_security 来执行环境所要求的文件类型，比如.php、.asp、.jsp、以及.html 文件。

万里长城

虽然 Mod_security 功能强大，但是，正如大部分 IDS/IPS 解决方案一样，它采用的是一种默认许可或者排斥性方法。对于一个开始阶段就获得了默认-否定情况的网络应用

层防火墙而言，你需要使用一些 Apache 中额外的模块。这里是一些完成任务所需要的额外模块：



这是一个典型的使用开源网络应用层防火墙的网络交易。客户请求一个静态的 HTML 页面，它按照网关后端的动态请求重新编写，经过监测、扫描与验证。HTTP 响应标头也进行了改写，以掩盖网络服务器，并隐藏其基础平台。

- 隐藏你的平台。网络服务器版本所标榜的是一种可以让攻击者识别到网络服务器平台的简捷方法。端口 80 的简单远程登录和 HTTP GET 请求将会产生版本号码，并且通常会有加载在服务器上的额外扩展。隐藏服务器标头和其它任何有 mod_headers 的特定平台标头，这是减少信息泄露的一个简单方法。

为了阻止更先进的指纹识别工具，你可以更进一步，修改 Apache 源，以发送独特的错误标头和重新排序响应。

- 重新编写内容并进行杀毒。只要运行在后端的编码没有任何变化，你就可以修改外部响应或者内部请求，并验证输入信息。所有这些都可以通过简单的规则操作实现。
- Mod_rewrite 可用于改写内部 HTTP 请求，是一个受欢迎的工具，通常以搜索引擎更容易解析的格式表述网络内容。使用规则的表达式，你可以创建一个过滤器，按照特定的安全规则（如参数为最大长度，仅包括字母和数字字符，请求也是最大长度），限制通过你网络环境的信息流，将所有其它的请求发送到一个通用的错误页面上。
- 虽然 Mod_proxy_html 的工作方式也类似，但是仅仅是输出方式相似，而非输入。它可以读取并替换服务器返回的 HTML。只要将 mod_proxy_html 和 mod_rewrite 结合起来，就可能运行网络应用层模拟，这与网络地址翻译、以及改写给定站点提供的内容类似。

这可以为欺骗攻击者带来几乎无限的可能性：ASP 页面可以模拟为 PHP，动态内容可以呈现为静态的内容，此外，站点可以向外部透明地分裂为多个服务器。

另一个工具是 mod_lineedit，它提供了和 mod_proxy_html 相同的改写功能：不仅仅在 HTML 方面，也包括 HTTP 信息中的任何内容。剔除信息泄露的其它来源，这是非常有用的，比如 META 标签可以命名创建网络页面的作者或者工具、开发者的注释和任何其它你的过滤器没有捕获的潜在危险数据。

砖瓦和砂浆

其它许多工具都可以配置在代理其上，监测所有网络信息流：

- 流量节流工具通过限制特定主机和网络每秒可以产生的请求数量，进而可以将蠕虫信息流和 DoS 攻击最小化。

- 日志解析器有助于检测网络请求日志中的异常情况。
- 当负载与标准不符时，流量分析应用程序会发出警报。
- 网络安全网关是添加多因素认证的最佳地点，要么使用 LDAP 或者其它机制，与单一签约的企业目录进行结合。

虽然构建你自己的网络应用层防火墙在前一阶段需要大量的艰苦工作，但是回报可能是相当高的。不论你创立一个解决方案还是购买一个，都要及早发现最难之处，即网络安全防御无法获知网络环境内部的情况。

（作者：Shawn Moyer 译者：李娜娜 来源：TechTarget 中国）

应用层防火墙选择与配置的最佳方式

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方式。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）

建立部署应用层防火墙规则库的四个步骤

在过去的 10 年里，大多数企业在网络和周边安全方面都进行了大量的投资。机构已经加强了控制并且进入了一种防御态势以显著限制黑客网络扫描的有效性。遗憾的是，虽然安全专业人员在忙于建立网络控制，但是，攻击者花时间开发了攻击下一个致命弱点的新技术。这个弱点就是应用层。市场研究公司 Gartner 最近发表的研究报告强调了这种威胁并且预测当前成功的攻击有 75%以上发生在应用层。Gartner 甚至提出了一个更吓人的预测：到 2009 年年底，80% 的企业将成为应用层攻击的受害者。

为什么这些攻击能够这样成功?这个答案非常简单：这些攻击绕过了安全专业人员在过去的十年里安装和运行的全部以网络为中心的控制，如端口封锁等。传统的保护一台服务器的防火墙包含封锁所有不需要的通讯的端口，仅允许 TCP 通讯通过端口 80 或者 443 穿过防火墙。遗憾的是，这种防火墙不能区分受欢迎的端口 80 通讯和不受欢迎的端口 80 通讯。

这正是应用层防火墙发挥作用的地方。这些防火墙在 HTTP 通讯到达网络服务器之前对这些通讯进行应用层检查。这些设备能够检测到一个连接并且分析用户正在提供给这个应用程序的指令的性质和类型。然后，它们能够根据已知的攻击特征或者异常的应用状况分析这些通讯。

虽然应用层防火墙有巨大的潜力，应用这些防火墙的过程应该是缓慢和审慎的。当这种网络防火墙最初进入企业的时候，实施管理员一般对这些计划都采取谨慎的方法，进行认真的分析和广泛的测试。在部署网络应用层防火墙的时候，也应该采取这种方法。认真的测试可以在机构的应用程序开发人员中建立信心。安全经理能够利用这种方法说服他们相信这个技术将对企业有帮助，而不会影响他们的日常生活。一旦一个机构准备把这个产品应用到生产环境，这就是他们考虑一个牢固的防火墙规则库的时候了。下面一步一步地介绍在一个机构中建立和部署应用层防火墙规则库的方法。

1.有一个适当的调整期。现代的 Web 应用层防火墙具有高级的监视通讯和学习异常行为的能力。经过一段时间，这种防火墙经过“训练”将能够识别这些方式和封锁异常的通讯。然而，这种防火墙需要足够长的一段时间的训练，这样，这个规则库才能反映出网络活动中定期的和季节性的趋势。例如，一个电子商务零售人员不会在淡季的夏天训练防火墙保护其网络然后在繁忙的冬季圣诞节购物季节部署这种规则库。

2.开发客户化规则以补充厂商提供的攻击特征。一个机构的基础设施的知识是非常重要的，客户化一个防火墙以满足一个公司的特殊需求能够显著提高这个工具的有效性。例如，如果在一个环境中只有一个 Web 应用程序应该接受文件上载，一项规则应该完全封锁所有其它系统的 PUT 指令。PUT 是用于文件上载的 HTTP 指令。

3.首先以被动模式开始运行。测试一个规则库经常需要一个“软开始”。采用这种策略，防火墙放置在网络上并且配置全部建议的规则，然后，在不封锁任何通讯的情况下以监视模式运行。在防火墙投入实际应用模式之前，应该用一些时间评估违反这个防火墙规则的通讯。负责安装和运行的人员在投入生产应用之前还应该调整错报率。由于程序员永远也不喜欢安全系统中断他们的应用程序，改善与你的开发人员之间的关系还有很长的路要走。

4.监视、监视、监视。一旦防火墙以活动模式部署完毕，就应该密切关注防火墙。通过封锁通讯创建的记录将告诉你一个重要的故事。封锁的攻击记录能够向管理层显示他们安全投资的回报。还会出现额外的错报。他们能够进一步帮助微调规则库。同网络防火墙一样，应用层防火墙也不是万灵药。WebInspect 和 AppScan 等工具能够用来测试 Web 应用程序的漏洞。除了进行这些努力之外，定期进行入侵测试也是一种坚固的防御策略并且能够消除许多安全专业人员对 Web 应用程序的担心。

(作者：Mike Chapple 来源：TechTarget 中国)

应用防火墙技巧

应用防火墙是在 TCP/IP 堆栈的应用层工作的，解析流向或流出浏览器等应用程序的信息报。这就提供了比网络放火强更彻底的全面检查。网络防火墙只检查传输层及以下的包信息。但是为了更有效，应用防火墙必须和应用程序以及需要保护的网络环境完全契合。配置较差的防火墙可能阻止合法用户、客户和伙伴——或者给予黑客访问系统和数据的权利。在本文中，TechTarget 的特约专家将讨论应用防火墙的类型以及如何调整使他们适应机构的环境。

硬件 VS 软件

应用防火墙有很多种，但是主要分为两类：硬件和软件。硬件防火运行在专一的应用程序上，通常有一个为防火墙的功能特别设计的坚固的操作系统。软件防火墙是在多用途的计算机上安装的，这种计算机为了网络边界等处的受信任的区域之间，或者在在个体防火墙的情况下，位于桌面计算机上。

特定目的的硬件应用程序通常性能更好，但是在安装和配置上更复杂。如果你选择软件防火墙解决方案，确保它是运行在你们的 IT 部门熟悉的平台上，这样就不需要另外的培训和支持问题了。软件解决方案通常比硬件解决方案更灵活，但是你需要确定运行防火墙的操作系统定期地打补丁和维护。

安装和规则设置

当安装防火墙的时候，大部门的 IT 安全资料都会告诉你开始的时候默认拒绝所有流量，然后只允许特别需要的流量——信息安全中的典型防火模式。但是，你应该知道这样的拒绝规则的影响和防火墙的变化。例如，当信息报和访问列表中的规则相符合时，这个信息包就会马上被拒绝规则放弃被允许规则放过。因为他不是对你在访问列中设置的其他

规则相对的，它实质是你总是在一般的过滤器前放置的特别的过滤器。另外，通常的规则可能允许信息包的访问，但是可能白访问列表中的特别规则拒绝。

如果你预先建立了一套规则，把拒绝规则放在最后，就像可以从庚本山改变防火墙管理流量的方式的特别的附加规则，它就会有帮助了。把访问列表规则从“允许你需要的”改为“拒绝你不要的”的方法还可以使每条规则的目的的理由更充分。

你还应该为带外流量设置规则，确保带有你的网络资源地址的信息包可以离开网络。这种外出的过滤本质上是为了阻止间谍软件和僵尸网络和它们的来源联系。

白名单、黑名单和审计

白名单喝黑名单确定哪一个站点、IP 地址、应用程序等可以相信，哪一个不可以。你可以使用一个或者另外一个，或者同时使用。白名单的方法更有限制性，对于对互联网访问有限制需求和稳定的应用要求的网络来说是理想的。但是，因为白名单通常比黑名单更加安全，它会造成安全的假象，因为恶意代码可以通过特洛伊木马和 Zombie 程序给黑客控制权，在几秒内就可以把受信任的计算机或者应用程序转变成不受信任的。黑名单的管理费用更高，因为它们需要定期的更新才能有效，它对于新的未知的威胁完全没有作用。

为了帮助保持白名单的更新，记录日志和审计通过你的应用防火墙的流量是必要的。日志对于检查防火墙是否有效的运行以及当问题或者攻击出现的时候的分析的价值是无限的。确保你有定期审计或者分析你的日志的能力。即使在较小的网络上，流量也会创建大大超过可以手动审计的日志文件，所以你需要全功能的日志分析器和时间来检查输出量。

（作者：Michael Cobb 译者：Tina Guo 来源：TechTarget 中国）

应用防火墙的缺点

问：Web 应用防火墙似乎对防御应用攻击很有效，但是我知道有些人犹豫是否安装。Web 应用防火墙有什么缺点呢？

答：Web 应用防火墙的主要缺点是成本和性能。性能通常都是问题，因为这些工具检查应用层的所有入站和出站流量。尽管如此，这种级别的检查通常被称为深度信息包检测，它检查信息包的实际有效负载，并提供比传统的包过滤防火墙更好的内容过滤功能。应用层放火强允许或者拒绝的决定可以基于每个包中的具体内容。他们可以允许或者拒绝某个应用程序或者应用程序的某个功能，提供深度的粒度控制（granular control）。这种防火墙也可以直接鉴别用户。这就是说，例如，他们可以允许或拒绝某个用户的特定引入命令。

深度包检测的数据也提供有价值的日志信息，这些信息有助于安全时间或者策略的实施。

当防火墙读取并解释每个包时，这个工具必须消耗 CPU 生命。检测的过程因此也比传统的包过滤防火墙要长，也会降低网络性能。

应用防火墙的另一个缺陷是每个协议，例如 HTTP、SMTP 等，都要求自己的代理应用程序，并支持新的网络应用程序，协议可以别限制或者降低出现的机会。虽然大部分的防火墙厂商提供一般代理，支持不确定的网络协议和应用程序，这次代理只是简单的允许流量通过防火墙，否决了很多首先采用应用防火墙的理由。

这些防火墙越来越复杂，也越昂贵，特别是和对网络性能影响极小的包过滤防火墙相比，并且包过滤防火墙是应用独立的。最后，和任何新设备一样，Web 应用防火的安装、配置和培训都需要评定。

很容易理解为什么有些人在配置应用防火墙时犹豫，特别是如果考虑到了时间和预算限制。尽管如此，在敌对环境中运行 Web 应用，应用防火墙的附加保护就几乎成为强制的了。因此，我想要明确防火墙的需要是为什么，因为这将决定所需要的功能。在选择防火墙的时候，回答下面这些问题：

- ✧ 防火墙需要做什么？
- ✧ 什么样的附加服务有价值？
- ✧ 它们将如何适应现有网络?
- ✧ 他们如何影响现有的服务和用户？

理解不用类型的 Web 应用攻击的执行方式对训练很有帮助。如果你在防火墙上的经验不足，容易安装和配置就成为了选择防火墙是的重要因素。还有，要提到在安装时厂商可能提供的支持级别，以及在防火墙的配置周期。

(作者：Michael Cobb 译者：Tina Guo 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）