**什么是Web应用**[**防火墙**](http://www.fuancn.cn/html/HardWareSafe/Firewall)**？**

Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)是专门为保护基于web的应用程序而设计的，它不像传统的[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)，基于互联网地址和端口号来监控和阻止数据包。一个标准的端口号对应一种网络应用程序类型。例如，telnet接收发送到端口23的数据包，邮件服务器接收发送到端口25的数据包。  
  
传统的[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)允许向邮件服务器相对应的互联网地址发送数据，让数据包通过25端口送达目的地。发送数据包给一个不是邮件服务器系统的互联网地址和25端口，就是一个攻击。[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)会阻止这些数据包。   
  
Web服务器理应通过80端口传送数据包。所以所有发给支撑web服务器系统80端口的数据包必须被允许通过[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)。传统的[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)没有办法测定一个地址指向正确的数据包是否包含威胁，但Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)可以仔细检查数据包的内容来检测并阻止威胁。  
Web应用程序如何遭受攻击  
  
黑客们不断开发新的方法获得未经授权的Web应用程序访问，但是也有一些通用的技术。  
  
    \* SQL注入：一些应用程序通过复制Web客户端输入来创建数据库查询。黑客通过构造一些应用程序没有仔细检查和会被拒绝的字符串，来获取返回的机密数据。  
    \* 跨站点脚本：黑客插入脚本代码（如JavaScript或ActiveX）到一个输入字符串，导致Web服务器泄漏用户名和密码等信息。  
    \* 操作系统命令注入：一些应用程序从web输入来创建操作系统命令，就像访问一个文件和显示文件内容。如果输入的字符串没有仔细检查机制，黑客就可以创建输入来显示未经授权的数据、修改文件或系统参数。  
    \* 会话劫持：黑客通过猜测基于令牌格式知识的会话令牌的内容来获得登录会话的权利。这使得黑客能接管会话并可以得到原来的用户帐户信息。  
    \* 篡改参数或URL：web应用程序通常在返回的的web页面中嵌入参数和URL，或者用授权的参数更新缓存。黑客可以修改这些参数、URL或缓存，使Web服务器返回不应泄漏的信息。  
    \* 缓冲区溢出：应用程序代码应该检查输入数据的长度，以确保输入数据不会超出剩余的缓冲区和修改相邻的存储。黑客很快就会发现应用程序不检查溢出，并创建输入来导致溢出。  
  
**如何阻止web应用攻击**  
  
Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)检查每一个传入的数据包的内容来检测上述类型的攻击。例如，web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)会扫描SQL查询字符串，来检测和删除那些导致返回的数据多余应用程序要求的字符串。增值厂商应仔细监测新发展的攻击类型并跟踪检测他们的最新产品。  
  
Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)不仅检测上述已知类型的攻击，而且还监测异常的使用模式来检测目前未知的攻击方法。例如，通常Web应用程序与web客户端的信息交流数量是有限的。如果Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)检测到Web服务器正在返回一个比预期大很多的数据量，它就会及时切断传输，以防止更多的数据泄露。   
  
目前有基于软件和基于应用程序的web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)。基于软件的产品布置在Web服务器上，而基于应用程序的产品放置在Web服务器和互联网接口之间。两种类型的[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)都会在数据传入和传出web服务器之前检查数据。  
  
一般基于软件的产品成本低于基于应用程序的产品成本，基于软件的产品供应商声称这类[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)具有更低的延迟和更高的吞吐量。但是在web服务器上安装额外的软件势必会增加额外的处理负荷和系统上软件的复杂性。  
  
基于应用程序的[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)厂商声称，这类[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)安装和使用简单，因为没有额外的软件安装在Web服务器系统上。 Web服务器的性能不受Web应用程序[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)处理的影响。   
  
除了商业产品外，也有许多开放源码的Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)可用。这些产品成本低于商业产品（就开放的源代码工具来说，他们是免费的，或者就基于开放源代码的商业产品来说，极有可能降低成本）。过去开源代码关注的是，黑客们将检查代码并设法逃避保护措施。有了应用Linux这类开源代码软件的丰富经验，这些都不是什么问题

所有的产品，不论是购买的还是开源代码，无论是基于软件的还是基于应用程序的，都应该得到支持。商业产品得到了供应商的支持。开放源代码为增值厂商和系统集成商提供了一个整合安全知识的机会。为 Web应用程序[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)提供持续的支持，确保合作伙伴与客户保持密切的关系，给供应商在未来为客户提供更多产品和服务提供了机会。  
  
因为每个客户的环境和应用程序设置是不同的，VARs和系统集成商必须评估每个客户的独特需求，以确定哪种类型的Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)将是最合适的。但是，毫无疑问所有客户的Web应用程序都应该得到Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)的保护。如果用户不理解这种需求或者不同意该做法，一定要介绍给他们Web应用程序可能受到攻击的多种方式。  
  
仔细检查应用程序代码是一种替代web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)的方法。攻击都是在编译出错或者缺乏内部数据检查的地方取得成功。从理论上来讲，一个通过代码检查员逐行检查过错误的web应用程序，可以替代web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)。  
  
在实践中，尽管软件工程师通常不相信他们的代码有缺陷，但对应用程序的不断更新使得详细的代码检查变得几乎不可能，更不用说代码检查员很容易的就会忽略不安全的代码，特别是那些没有安全背景的检查员。此外，黑客技术迅速发展。网络[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)供应商时时关注新攻击类型的新闻、及时更新它们的产品。有些客户可能觉得经过代码审查的程序可以使他们避免实施一个web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)所带来的花费和工作量，但解决方案供应商应帮助客户认识到安全代码审查只能带来虚假的安全感，实际上并不能代替Web应用[防火墙](http://www.fuancn.cn/html/HardWareSafe/Firewall)提供的全面安全保护。