案例 1：

U.S.cellular 公司是美国第八大无线服务运营商，总部位于芝加哥，在美国 25 州开展无线电话和数据运营服务；拥有 500 个营业网点和 1800 个销售代理商。该公司的门户网站为用户及其代理商提供产品信息、产品支持、在线服务等功能其中用户及代理商的在线服务需要连接到网站后台的数据中心，因此数据中心运行的安全性、可用性非常突出。为了确保网站安全，U.S.cellular 公司首先采取了传统的安全解决方法：如采用防火墙保护网络、加密所有交易保护隐私、使用口令验证控制应用交互，记录访问日志并加强审计；然而 U.S.cellular 安全团队对于 Web 应用安全进行深入研究后发现其传统的安全措施无法消除网站安全风险：

1、针对大型在线网站的黑客攻击增加，数据窃取事件频发；而新的法律界定了信息防护的责任；一旦 U.S.cellular 网站被攻击，客户信息被泄露，损失无法估量。

2、在对网站进行应用漏洞测试发现了较多的安全漏洞，如果采用源代码安全修订防护，需要昂贵的费用，估算将超过 1000000 美元。并且需要长达 12-18

个月的时间，最为关键的是无法确保源代码完全被修复。

因此 U.S.cellular 决定必须采用新的安全防护设备。

U.S.cellular 的需求：

1、新的设备必须保障应用，Web 应用安全威胁的根源在于应用程序代码，而不是服务器和网络，因此新的设备不是更过的网络层工作设备，必须能检查 Web 应用流量并能对 HTTP 进行深度检测。

2、必须确保数据中心的可靠性和安全性。必须能够阻止透过 Web 应用对数据库的攻击。设备必须具备冗余和 failover 功能。

3、需要具备 SSL 卸载能力以减轻服务器负荷

4、需要具备用户认证功能以加强访问安全。

5、解决方案必须易于管理和使用，U.S.cellular 公司不希望新的设备需要大量人员培训和复杂维护时间，新的设备必须类似于目前数据中心设备。

案例 2：

2008 年，对于中国人民来说是特殊的一年，因为举世瞩目的奥运会这一年在北京举行。然而专门为销售奥运门票而搭建的 web 应用系统却很不光彩，具体

情况是这样的：“2007 年 10 月 30 日，北京奥运会门票面向境内公众第二阶段预售正式启动。上午 9：00 点一开始，不到半小时，网站系统便宣告瘫痪。访问者看到，官方票务网站当天上午开始，都只是显示‘系统繁忙，请稍后再访问。不便之处敬请原谅。’的提示信息。”根据事后官方的报道，其原因是并发访问量太大导致整个系统瘫痪。在技术人员对硬件进行一定的升级后，情况并没有很大好转，仍然没有彻底解决访问量太大而导致的性能问题。无独有偶，将在 2012 年举行的伦敦奥运会，其售票系统也重蹈了北京奥运会的覆辙。其网站订票系统抵挡不住巨大的客户访问而崩溃，最后不得不临时紧急延长了一个小时来解决这一尴尬问题。究其原因，乃是系统开发之前，对于性能需求的分析不到位，低估了系统上线后的并发用户量。