绿盟 WEB 应用漏洞扫描系统

产品白皮书

【绿盟科技】

目录

一. 概述

近年来，Web 应用系统随着互联网技术的不断发展呈现出爆炸式的增长。据中国互联网络信息中心(CNNIC)发布的《第 34 次中国互联网络发展状况统计报告》①显示，截至 2014 年 6 月，中国网站数量为 273 万个，中国网民数量达到 6.32 亿，半年共计新增网民 1,422 万人。

Web 应用系统已广泛应用于各个公共领域（政治、经济、文化、国防等）以及个人领域（娱乐、咨询、交流、沟通等），其中蕴含了越来越多的经济价值，而 Web 应用系统在被广泛应用的同时，因其互联、开放等特性，更容易遭受黑客的攻击。从 2005 年到 2006 年跳跃式增加至今，每年发现的 Web 漏洞数量一直居高不下，这也是导致 Web 应用频繁遭受攻击的重要原因。

从 IBM 2014 年风险报告可看到，2013 年全年漏洞已达到 8,330 个，而其中 Web 漏洞占 33%，达到 2,749 个。

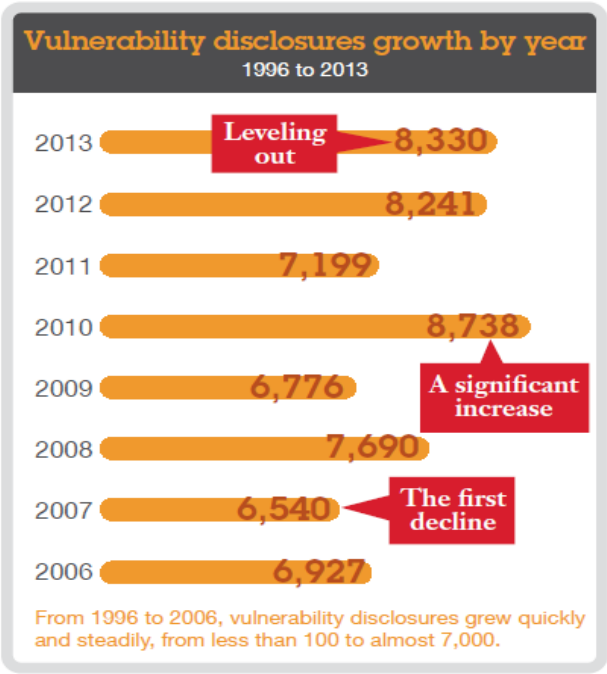

图 1.1　1996-2013 年漏洞数量增长趋势图①

① http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201407/P020140721507223212132.pdf

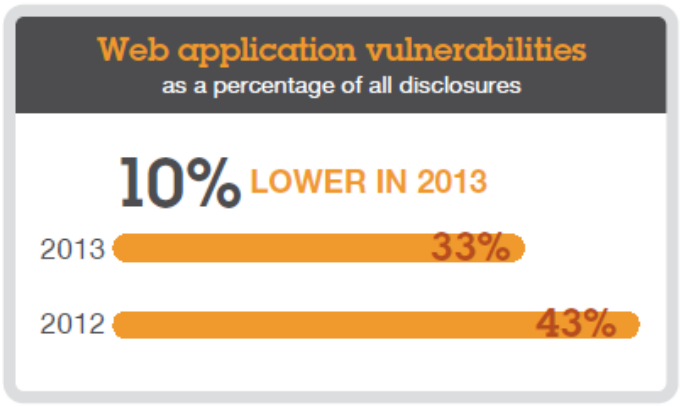

图 1.2　2012-2013 年 Web 应用漏洞数与总漏洞数比较图[①]

因 Web 漏洞引起的安全事件极大困扰着网站维护部门，影响了用户体验，甚至对信息网络等核心业务造成严重的破坏，导致了机构门户的经济受损和公信力的下降：

1) 网站数据库被拖库——导致注册用户身份信息、银行卡信息、密码等被盗取；
2) 网站被挂马、被篡改——导致网站信誉受损、网站资源被滥用，以及给访问该网站的用户带来被入侵甚至成为僵尸主机的风险。

从 CNCERT 发布的中国互联网网络安全报告可看到， 2013 年我国境内被篡改网站数量为 24,034 个，其中包括政府网站 2,430 个，较去年分别增长了 46.7%和 34.9%；被暗中植入后门的网站有 76,160 个，较 2012 年增长 45.6%，其中政府网站 2,425 个，较 2012 年下降 19.6%。2013 年 10 月，“查开房”网站公开曝光 2000 万条客户酒店入住信息，涉及大量个人隐私信息，严重影响公众生活。2013 年 7 月，Apache Struts2 被披露存在远程代码执行高危漏洞，可直接导致服务器被远程控制或数据被窃取，多家大型电商和互联网企业以及大量政府、金融机构网站受到影响，上亿用户信息面临严重泄露风险②。

① IBM X-Force Threat Intelligence Quarterly 1Q 2014
② CNCERT/CC《2013 年中国互联网网络安全报告》

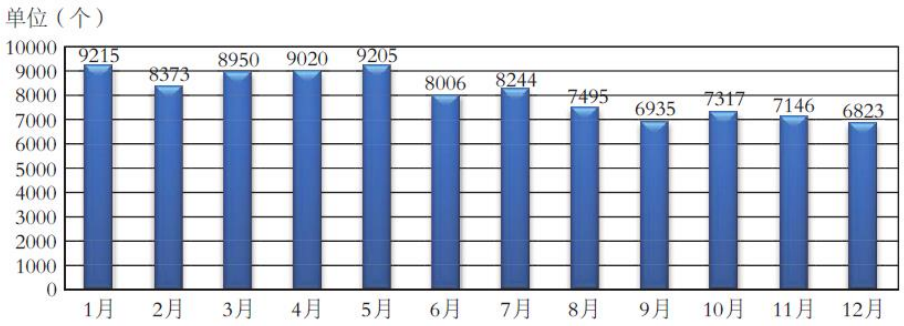

图 1.3　2013 年我国境内被篡改网站数量月度统计（来源：CNCERT/CC）

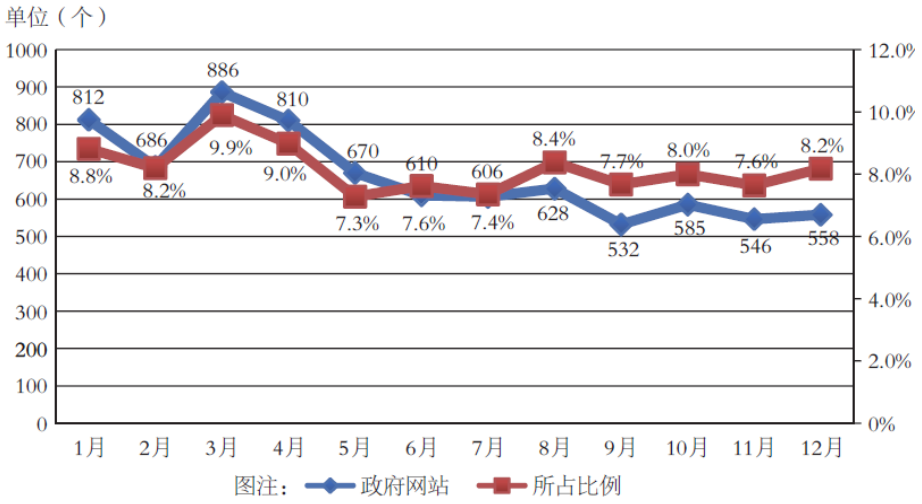

图 1.4　2013 年我国境内政府网站被篡改数量及所占比例月度统计（来源：CNCERT/CC）

如何应对频频发生的 Web 应用安全事件，给网站维护部门及其安全监管部门带来新的挑战。

二. 网站安全管理面临的挑战

■ “源码”带来的挑战

Web 应用系统通常是供应商针对不同业务目标进行定制化开发，并以“源码”的形式交付，依靠各种应用环境进行动态解析以实现特定功能。因此，对于 Web 漏洞而言，供应商往往也很难提供类似于 Windows 漏洞补丁的通用补丁，这给 Web 应用系统的维护带来了新的

挑战——不能仅依靠被动的“打补丁”方式，而需要采用更主动的方式——使用专业 Web 漏洞扫描器进行评估，提前发现 Web 应用系统中隐藏的漏洞，根据评估工具给出详尽的漏洞描述和修补方案，指导维护人员进行安全加固，防患于未然。

然而对于一些网站维护部门，由于“人力资源缺乏”或者“Web 系统本身使用的是第三方代码”等原因，造成很难及时的去修补已发现的漏洞。开放式 Web 应用安全组织 OWASP（Open Web Application Security Project）对造成这类现象的原因——“源代码修补面临的挑战”，进行了分析，如图 2.1 所示，这些众多的挑战使得在面向网站的安全建设中需要采取与传统 IT 维护手段不一样的方式，不仅需要能够及时发现潜在的漏洞，还需要能够有效缓解因为 Web 漏洞修复不及时而引起的风险。

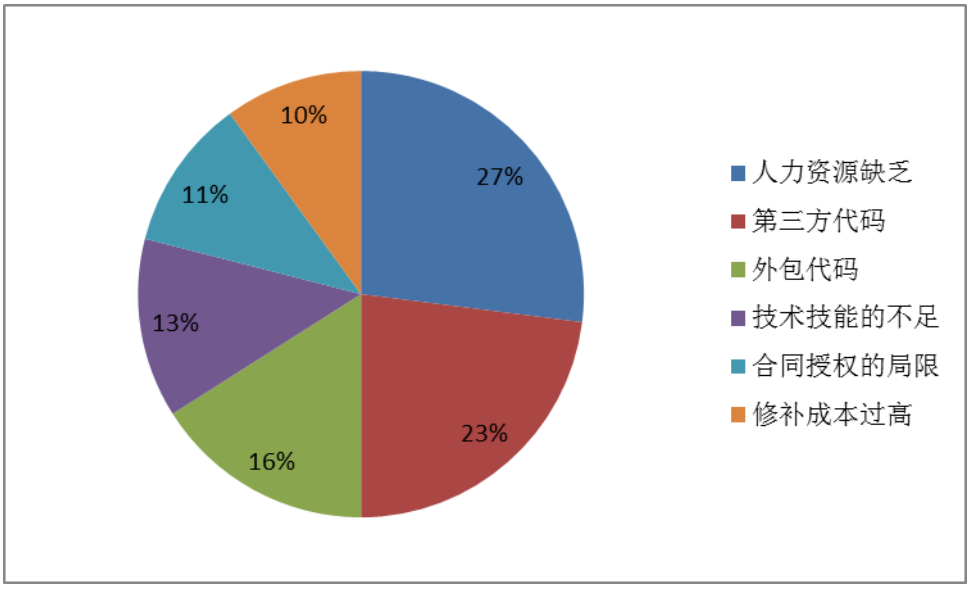

图 2.1　Web 漏洞源代码修复面临的挑战[①]

■　“海量”带来的挑战

先来看几组数据：一个省市级监管机构往往需要检查上万数量级别的网站，一个省级运营商往往需要检查上千数量级别的网站，一个大中型企业往往需要管理上百数量级别的业务站点。同时，随着网站数量越来越庞大，网站自身的规模也越来越大，一个包含百万级别页面的网站也是不难寻见。

[①] OWASP Web Application Virtual Patching Survey

这些海量级规模给本来就繁重的网站安全检查任务带来了极大的压力，如何在规定时间内完成对海量网站的检查任务？如何在面对更新频繁的大网站时，能够在下一次更新前完成检查任务，保障检查结果的有效性？这些都成为网站安全管理工作中亟待解决的难点。

因此，在面对网站安全管理挑战时，需要解决的主要问题包括以下三点：

1) 如何在发现漏洞后，把结果权威有效地传递到漏洞修复方，比如网站开发维护人员，并且需要降低其学习成本，做到“简单、有效、权威”；
2) 如何对大网站(群)进行快速、准确、稳定的安全评估；
3) 如何在网站安全检测时减少对网站的影响，以及业务健康性的保障。

三. 绿盟 WEB 应用漏洞扫描系统

若能够主动发现网站的风险隐患，并及时采取修补措施，则可以降低风险、减少损失。绿盟科技针对该需求，推出了绿盟 WEB 应用漏洞扫描系统（NSFOCUS Web Vulnerability Scanning System 简称：NSFOCUS WVSS），该系统可自动获取网站包含的所有资源，并全面模拟网站访问的各种行为，比如按钮点击、鼠标移动、表单复杂填充等，通过内建的“安全模型”检测 Web 应用系统潜在的各种漏洞，为用户构建了从急到缓的修补流程，以及易读易懂、权威有效的分析报告，并通过与 NSFOCUS WAF 的联合形成了“漏洞自动修补”的机制，能够有效解决网站安全管理面临的挑战，也能较好满足安全检查工作中所需要的高效性和准确性，以实现网站安全管理水平的提升。

◆ 全面深入的 Web 应用安全检测，检测范围覆盖了各企事业单位的门户网站、电子政务的互动平台和政务信息公开服务系统等，覆盖了论坛、内容管理系统（CMS）和电子商务应用系统等平台。

◆ 采用高效稳定的扫描引擎，基于嵌入式系统平台，通过内核级优化，实现了单设备的快速、稳定扫描；同时，通过 URL 级别的负载均衡技术，以集群的方式实现了多设备间的性能叠加和设备冗余的效果，从而实现了面向“海量”级别网站的快速稳定的扫描。

◆ 采用创新的“无损”漏洞扫描技术，可以根据网站、带宽等关键因素的负载情况，自动调整扫描策略，避免对网站的业务连续性造成影响；同时，扫描过程中采用的检测手段，均不会在网站遗留任何可造成网站异常的干扰性代码，比如 XSS 漏洞检测时在网站上遗留的“弹框”代码等，避免对网站的业务健康性造成影响。

◆ 采用全流程的“漏洞跟踪”技术，以及引入了“漏洞判断依据”、“过程文件取证”等新技术，为客户提供了“简单、有效、权威”的漏洞分析报告，极大降低了网站维护人员的学习成本，以及为进一步的漏洞整改提供了更有效的手段。

◆ 通过统一的“安全模型”与 NSFOCUS WAF 无缝对接，实现了从漏洞发现到威胁防护的快速响应，达到了“漏洞自动修补”的效果，极大缩减了网站从漏洞发现到漏洞修补期间所面临的风险“空窗期”。

3.1 产品体系结构

NSFOCUS WVSS 是基于 Web 的管理方式，用户使用浏览器通过 SSL 加密通道和系统进行交互，方便用户管理。NSFOCUS WVSS 采用模块化设计，整个系统可分为：UI、web 应用服务、扫描引擎、状态引擎、调度引擎、升级系统、证书系统、报表系统和基础系统。

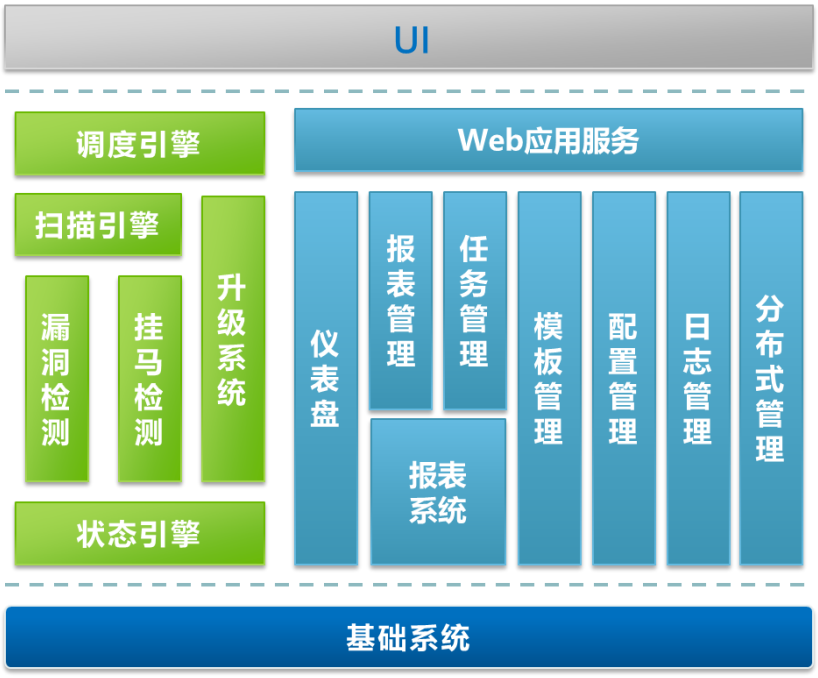

图 3.1 NSFOCUS WVSS 系统架构

主要模块说明：

a) 调度引擎模块

该模块采用内置的算法实时监控系统任务的运行情况，并依据结果对各任务进行优化和调整，以达到系统资源的充分利用和任务的高效运行。

b) 扫描引擎模块

该模块根据配置的策略，对被扫描站点进行全面准确的 web 漏洞和网页挂马检测。

c) Web 应用模块

该模块通过友好的 UI 设计为用户提供了便捷的操作，同时还负责对扫描结果的数据分析和呈现。

d) 基础系统

该模块采用嵌入式操作系统平台，通过内核级优化，为系统的高性能、高稳定性和安全性提供了基础。

3.2 产品特性

3.2.1 全面 Web 应用安全评估

NSFOCUS WVSS 可对包括门户网站、电子商务、网上营业厅等各种 Web 应用系统进行安全检测，同时其全面性还体现在以下两个方面：

检测范围：

- 覆盖 Ajax、Flash、JavaScript 等 Web2.0 环境
- 支持 PHP、ASP、.NET 和 Java 等编程语言
- 支持 IIS、Apache、Nginx、Tomcat 等 Web 服务器
- 支持各种静态页面（后缀名为：html、htm 等）和动态页面（后缀名为：asp、jsp、php、asp、jsp、php、aspx、phtml、shtml、xhtml、do 等）
- 支持 Flash 攻击检测、复杂字符编码、会话令牌管理、多种认证方式（Basic、NTLM、Cookie、SSL 等）
- 支持代理扫描，HTTPS 扫描等

风险分析：

- 支持 WASC 的漏洞分类，以及按照威胁严重性分高中低三个等级进行风险分析
- 支持两个版本的 OWASP TOP10 漏洞分类和风险分析，为用户提供权威的分析结果

- 支持风险的对比分析和趋势分析，既可以帮助用户进行多站点差异化风险管理，还可以助其更准确的了解和分析站点的历史风险状况和未来的风险趋势，提高风险管理的水平

3.2.2 快速稳定扫描

NSFOCUS WVSS 基于绿盟科技多年技术积累自主研发的统一基础平台，采用嵌入式系统，通过内核级修改实现了多任务、多线程、数据存储、数据访问等多方面的优化，使系统相比使用第三方平台产品拥有更好的性能、稳定性和安全性；同时通过 URL 级别的负载均衡技术，以集群的方式实现了多设备间的性能叠加和设备冗余的效果，实现了面向“海量”级别网站的快速稳定的扫描。

3.2.3 可视化漏洞检测

NSFOCUS WVSS 引入了“漏洞判断依据”、“过程文件取证”等新技术，对漏洞检测的全过程进行跟踪、说明，并通过易读易懂的语言对每一个漏洞都进行了详细说明，比如针对每一个发现的漏洞，通过高亮、注解、文字说明等直观的方式，给出判断的依据以及在检测过程中的取证数据，极大降低了网站维护人员的学习成本，以及为进一步的漏洞整改提供了更加“简单、有效、权威”的数据。

3.2.4 全流程漏洞跟踪

NSFOCUS WVSS 采用了全流程的漏洞跟踪技术，对于每一个网站，无论是在哪个任务或者哪种任务中进行了扫描，都会自动汇总到统一的漏洞跟踪平台进行分析；这个漏洞跟踪平台基于时间轴用直观图表的方式，可针对包括漏洞发现、修补、增减等漏洞管理全生命周期进行详细的跟踪分析。

3.2.5 无损漏洞扫描

在网站运维过程中网站的业务健康性是至关重要的，因此 NSFOCUS WVSS 采用了无损的漏洞扫描技术，以避免对网站业务的健康性造成影响。主要采用了两种独创的技术，一种

是自适应扫描——根据网站、带宽等关键因素的负载情况，自动调整扫描策略和强度，避免对网站的业务连续性造成影响；一种是无损扫描——扫描过程中采用的检测手段，均不会在网站遗留任何可造成网站异常的干扰性代码，比如 XSS 漏洞检测时在网站上遗留的“弹框”代码等，避免对网站的业务健康性造成影响。

3.2.6 网站安全闭环管理

在网站安全管理时，往往因为人力资源不足、代码不可控、修补成本高等原因造成很难及时修补已发现的 Web 漏洞，这给企业带来了风险。NSFOCUS WVSS 和 NSFOCUS WAF 使用一体化的“安全模型”，形成联合防护手段，通过 WVSS 向 WAF 提供被防护网站的漏洞扫描报告，WAF 以此为依据自动生成防护策略应用于被保护网站，实现了“检测”与“防护”的安全闭环管理。

3.2.7 全面支持虚拟化环境

虚拟化应用业已成为 IT 技术的发展趋势，随着在数据中心，云计算，智慧城市，智慧园区等方面的应用，如何有效针对运行于虚拟化环境的网站进行安全管理成为急需解决的问题。NSFOCUS WVSS 可完全支持虚拟环境下的部署和扫描，可轻松融入这些环境的网站安全管理。同时，NSFOCUS WVSS 无需安装的虚拟化软件形态，相比一般软件产品，不仅具备了按需启用的特性，还能避免因为依托第三方宿主操作系统而带来的额外维护开销，并且在稳定性和性能上更具优势。

3.3 典型应用方式

NSFOCUS WVSS 适用于各种网站，部署灵活简单，只需要对目标站点“网络可达”即可进行 Web 漏洞、挂马等检测，同时具备了丰富的部署应用场景。

3.3.1 独立部署

单台 NSFOCUS WVSS 通过其多路扫描的特性，可以对网站的生产环境、发布环境和运行环境进行同步扫描，获得汇总、对比、负载均衡等由单路扫描无法获得的特性。

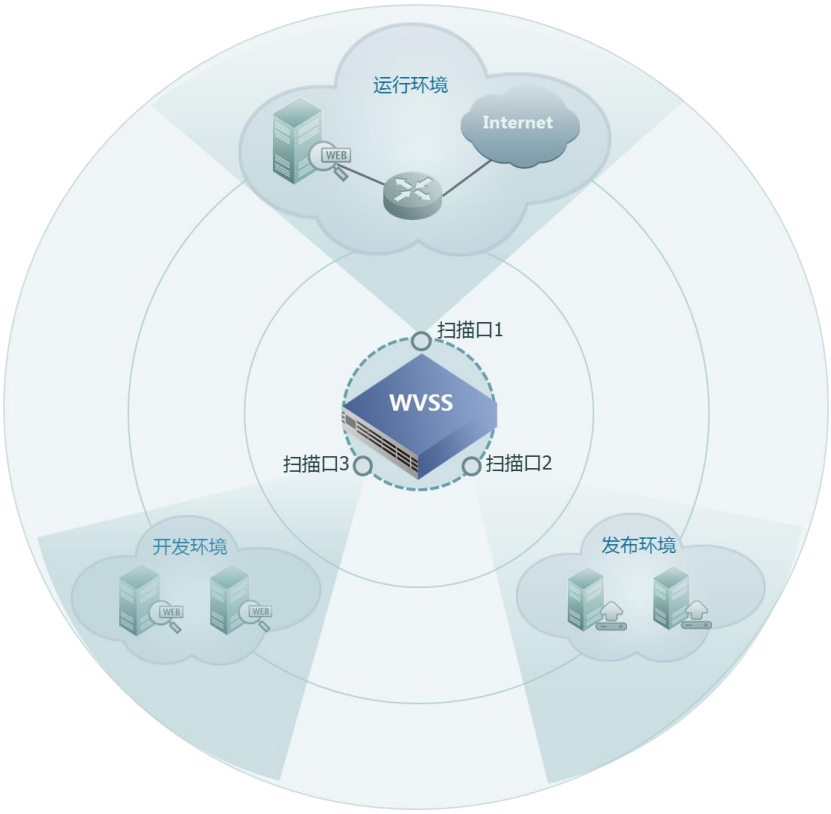

图 3.2 NSFOCUS WVSS 独立部署

3.3.2 分布式部署

NSFOCUS WVSS 通过分布式管理功能，可集中管理多台 WVSS 设备，并支持“URL 级别”的负载均衡技术，以实现性能叠加和设备冗余的效果，从而实现了面向“海量”级别网站的快速稳定的扫描。

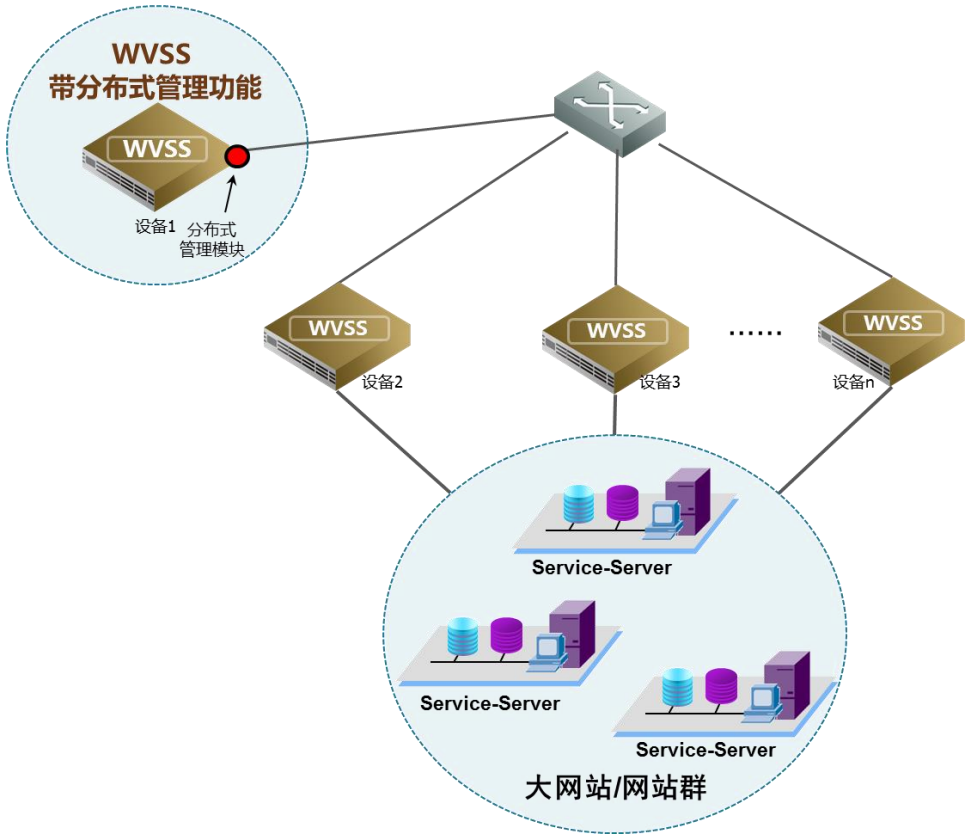

图 3.3 NSFOCUS WVSS 分布式部署

3.3.3 与 WAF 联动部署

为更好满足网站运维时的安全管理要求，NSFOCUS WVSS 通过一体化的安全模型与 NSFOCUS WAF 实现了无缝对接，形成联合防护手段，通过 WVSS 向 WAF 提供被防护网站的漏洞扫描报告，WAF 以此为依据自动生成防护策略应用于被保护网站，实现了“检测”与“防护”的安全闭环管理。

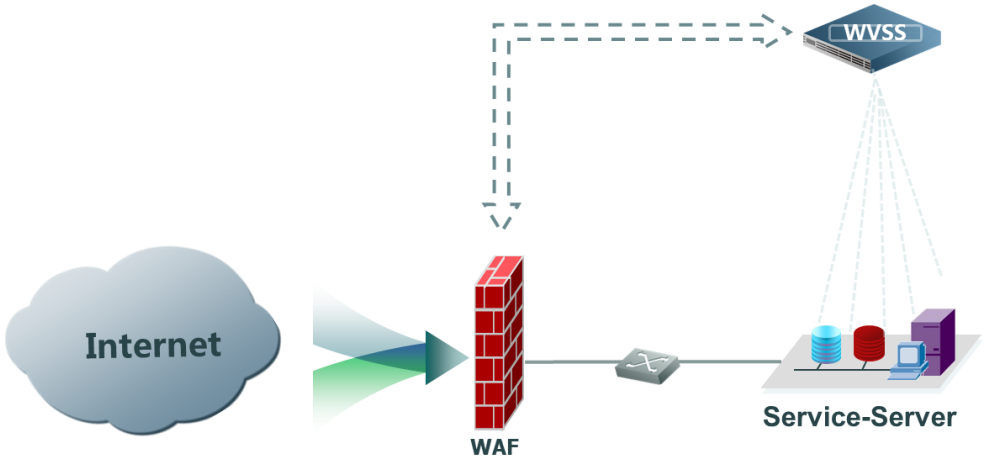

图 3.4 NSFOCUS WVSS 与 WAF 联动部署

3.3.4 虚拟化部署

NSFOCUS WVSS 可完全支持虚拟环境下的部署和扫描，可轻松融入这些环境的网站安全管理。同时，NSFOCUS WVSS 无需安装的虚拟化软件形态，相比一般软件产品，不仅具备了按需启用的特性，还能避免因为依托第三方宿主操作系统而带来的额外维护开销，并且在稳定性和性能上更具优势。

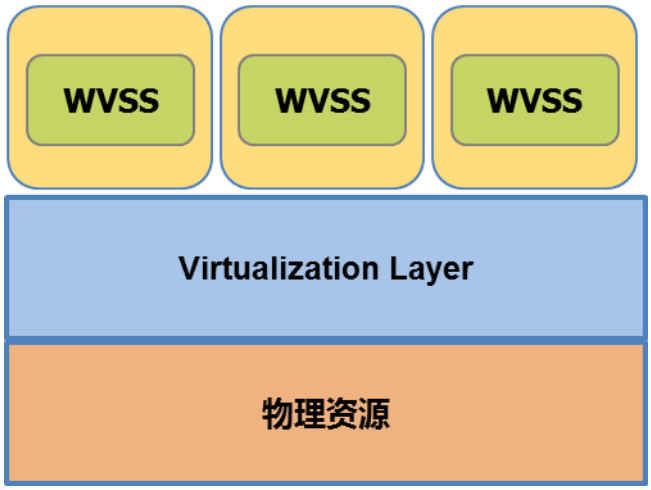

图 3.5 NSFOCUS WVSS 虚拟化部署

四. 结语

随着互联网的高速发展，越来越多的行业通过互联网为公众提供信息以及数字服务，而随着应用的深入，越来越多的经济价值融入其中。在这个生态链中，安全保障业已成为重要的一环，如何保障数据的安全、如何保障业务安全、如何保障可用性安全均成为新的挑战，同时每一个网站也担负着保护访问者安全的责任。

安全评估是保障网站安全的重要手段，通过扫描评估发现目标网站是否存在挂马，以及是否存在能被黑客利用的各种漏洞，进而促进网站漏洞修补工作，这是从根本上解决安全问题的有效途径。

NSFOCUS WVSS 以其便捷的配置、全面快速的检测能力和多环境适应性成为企业网站风险管理的有力助手，其广泛适用于政府、等级保护测评机构、公安、运营商、金融、能源、教育、医疗、互联网等行业，适应于针对 Web 应用的安全检查和风险自评。