网神
SECWORLD

可控安全
Controllable
Security

技术白皮书

网神 SecWAF 3600 Web 应用防火墙

网神信息技术（北京）股份有限公司
http://www.legendsec.com

版权声明

文档信息

文档名称	网神 SecWAF 3600 Web 应用防火墙		
扩散范围	销售/售前/客服/渠道商/用户	文档版本号	V16.8.1
作者	王嘉	日期	2016/08/01
初审人		复审人	

版本变更记录

时间	版本	说明	作者
2016-08-01	V1.0	文档建立	王嘉

目 录

1.产品概述

1.1 产品背景

近些年，政府部门对于网站安全问题越来越重视，从 2005 年开始至今，公安部、国务院办公厅、中央网络安全和信息化领导小组都多次针对网站安全问题进行明确政策导向通知。2015 年 9 月，由公安部、中央网信办、工业和信息化部联合发布“公信安 2562 号”通知，《党政机关、事业单位和国有企业互联网网站安全专项整治行动方案》。此次网站安全整治行动是第一次由国家多部委联合网站安全问题专项整改方案。

回顾 2015 年的安全事件，主要与篡改事件、数据库拖库、中间件系统漏洞、网站 CMS 漏洞等安全问题事件相关：

Apache 的 Struts2 漏洞问题，自从 2013 年第一个 Struts2 漏洞被曝光之后，至到 2016 年 4 月份，最新的 Struts2 的 S2-033 远程代码执行漏洞又被曝光公布。

2015 年 2 月 11 日，CMS 系统漏洞导致桔子酒店、锦江之星、速八酒店，甚至高端万豪酒店、丽思卡尔顿酒店、喜来登、洲际酒店等房客信息泄露，包括顾客姓名、身份证、手机号等大量涉及个人信息的信息泄露

同年 6 月，内蒙古财政厅发现其网站被人恶意攻击篡改，被篡改的都是参加当年会计从业资格证考试的考生考试信息。黑客以篡改考试成绩谋求经济回报。

2016 年 4 月中国高等教育学生信息网（学信网）遭受黑客攻击，黑客窃取了大量大学生个人信息，导致大量学生个人信息遭到泄露。

1.2 常见安全问题

近几年，网站安全事业频繁被媒体报告，在乌云、补天等漏洞平台的网站安全事件频繁曝光，其中让大家最直观发现是“拖库“事件、“网页篡改”、网站漏洞（CMS 漏洞）等安全问题。

1.2.1 “拖库”事件

“拖库”事件有专业名词就是 SQL 注入攻击。SQL 注入的成因在于对用户提交 CGI 参数数据未做充分检查过滤，用户提交的数据可能会被用来构造访问后台数据库的 SQL 指令。如果这

些数据过滤不严格就有可能被插入恶意的 SQL 代码，从而非授权操作后台的数据库，导致敏感信息泄露、破坏数据库内容和结构、甚至利用数据库本身的扩展功能控制服务器操作系统。利用 SQL 注入漏洞可以构成对 Web 服务器的直接攻击，还可能用于网页挂马。

几乎所有 SQL 数据库都是潜在易受攻击的，但需要注意的是，并不是数据库本身存在漏洞，而是互联网网站开发人员在开发页面时，没有遵循安全代码开发的要求所引起的。

1.2.2 网页篡改

网页篡改是最频繁发生的网站安全事件，黑客为了达到政府目的或谋求经济回报往往会对政府网站、电商网站进行篡改攻击。从而达到自己的目的诉求。

网页篡改事件的发生主要来源于网页代码编写不规范、网站服务器植入后门程序（webshell 等）。这些安全问题导致网页可以被第三方轻易入侵，篡改网站内容、替换网站图片、视频文件等。

1.2.3 CMS 漏洞

所有的网站维护都离不开 CMS 系统，很多网站开发商在开发时图时效性，往往会使用公有代码，导致安全问题频繁出现。CMS 系统是一个网站维护、内容更新的重要组成部分，一旦 CMS 系统出现安全问题，给网站会带来致命的安全问题。

1.3 网神 SecWAF 3600 Web 应用防火墙

网神 SecWAF 3600 Web 应用防火墙是网神公司重点打造的针对网站安全的防护产品。产品主要围绕三个概念“重塑网站边界”、“智能化防护理念”、“纵深防御体系”。

网神 SecWAF 3600 Web 应用防火墙为网站服务器提供安全保障，提供 Web 防护、网页防篡改、DDoS 防护等多功能于一身的网站安全防护产品。

2.产品特色

2.1 重塑网站边界

随着网络的高速的发展，网络边界越来越模糊。网站因与外界进行交互数据导致长期暴露

在互联网中。何为网站的边界，实际以“网站”为中心，接入网站就是网站的边界。网神 SecWAF 3600 Web 应用防火墙产品首先在网站服务器的物理前端进行防护，实现物理的第一道网站防护边界。因网站需要与互联网进行互联。在互联网中，网神 SecWAF 3600 Web 应用防火墙在互联网中架设第二道虚拟防护拦截，实现互联网的第二道网站防护边界。

网神 SecWAF 3600 Web 应用防火墙为网站安全启到了重塑网站安全边界的概念。实现物理与逻辑的双重防护拦截手段。

2.2 智能化防护理念

传统安全产品都有标准的特征库，实际防护产品依靠的就是流量与特征库进行特征匹配。当特征匹配上了就发现攻击行为，进行防护拦截。

网神 SecWAF 3600 Web 应用防火墙实现了智能化防护理念，以“云端”数据与“本地”数据进行数据交流，让一个传统的安全产品成为“安全防护的大脑”，实现自我判断的人工智能防护效果。实现具有完全自动判断能力的新一代网站安全防护产品。

2.3 纵深防御体系

“纵深防御体系”一词源于战争学概念，是指防御地区或防御部署的纵向深度。网神 SecWAF 3600 Web 应用防火墙产品把此体系放到了网站安全防护的理念中进行运用。实现了从漏洞到流量、再到系统本身的纵向深度防护体系。

网神 SecWAF 3600 Web 应用防火墙实现以“事件”为中心的纵深防御体系。

首先，事前评估。根据黑客攻击经验，每次黑客在攻击前都会对目标事物进行漏洞扫描。评估客户网站在开发过程中，开发人员忽视的安全问题。

其次，事中防护。根据常见对黑客攻击技术的研究，制作出了一套黑客 Web 攻击行为的特征库，针对黑客的攻击流量进行逐一特征匹配，匹配上的流量就是黑客攻击流量，此时进行 Web 安全过滤

然后，事后弥补。针对网站网页频繁被篡改事件的发生，提出多重防护组合模型：内核保护、本地备份、异地备份。客户可以根据自身网神情况进行多种防护组合。

3.技术优势

3.1 双存储结构

传统的安全设备，软件系统都是存储在硬盘中，为了提高稳定传统厂商都会使用企业级硬盘或是固态硬盘，因软件系统长时间运行，硬盘反复读写数据，就是稳定性高的固态硬盘都会出现硬盘故障。

网神 SecWAF 3600 Web 应用防火墙使用双存储硬件结构，使用传统的硬盘只作为存储日志，软件系统使用专用的系统存储卡来保障软件稳定运行。

双存储结构屏蔽因硬盘故障导致系统不能启动，双存储硬件结构设计，即使硬盘出现故障，软件系统也能保障正常运行，只是因硬盘故障导致日志无法进行记录。

3.2 串联透明部署

随着网神 SecWAF 3600 Web 应用防火墙的不断更新发展，从传统的透明代理模式已经转变为透明部署方式。透明部署方式就是网神 SecWAF 3600 Web 应用防火墙的工作在 OSI 七层模型中的第二层（数据链路层）。网神 SecWAF 3600 Web 应用防火墙在第二层截获数据包，对数据包的进行特征库匹配，匹配上就是攻击行为，直接把数据包丢弃。如果数据是正常的，过滤引擎重新构造 Web 和 SQL 事务生产数据包发送给后端的 Web 服务器。

透明部署方式是串联在 Web 服务器的前端，在物理层面是 Web 服务器的前端多了一台硬件设备。在网络层面是 Web 服务器的前端没有任何硬件设备。透明部署方式不改变客户的网络拓扑结构。Web 服务器看到的都是浏览者的源地址，也不会给审计类安全产品造成无法工作等现象的出现。

3.3 自适应网络

传统的 Web 应用防火墙都是人工输入网站域名、网站服务器 IP 地址、服务器端口等相关详细信息。网神 Web 安全团队针对纯透明部署方式的特性开发了自动学习功能，针对数据流中包含的相关数据进行自动分析和摘取。可以自动学习到网站域名、网站服务器 IP 地址、服务器端口等相关信息，并自动生成防护列表。降低人工输入的繁琐配置，避免造成因人工输入错误导致网站无法防护的安全事件发生。

3.4 细粒度特征库

网神 SecWAF 3600 Web 应用防火墙提供了细粒度的特征库，产品支持 HTTP 协议效验、Web 特征库（基于 OWASP 标准）、爬虫规则、防盗链规则、跨站请求规则、文件上传/下载、敏感信息、弱密码检测等多种细粒度检测的特征库匹配规则。

3.6 镜像分析模式

网络安全产品有 IPS（入侵防御系统）和 IDS（入侵检测系统）。IPS（入侵防御系统）是串联部署在网络中的，主要是对网络流量进行过滤。IDS（入侵检测系统）是旁路部署在网络中，对交换机接口镜像出来的流量进行分析和监控预警。

网神 Web 安全团队对网神 SecWAF 3600 Web 应用防火墙进行综合部署考虑，串联在网络中可以对应用层攻击流量进行监测和阻拦。旁路部署可以对交换机的接口镜像流量进行分析并进行告警功能。

3.5 泛域名防护

互联网的网站各式各样的，针对一些网站提供的个人主页访问系统。每个用户都可以申请个人主页，系统会根据个人主页的名字自动生成域名。浏览者可以通过自动生成的域名直接访问个人主页。但是这些主页的域名都是按照定义好的规则进行自动生成的。每天都有新用户申请个人主页。

网神 SecWAF 3600 Web 应用防火墙推出泛域名防护机制，定义好网站生成的域名规则，自动生成的域名直接就受到 Web 安全保护。防护无需做任何添加的人工动作。快捷方便智能化提供网站安全防护机制

3.7 旁路阻断模式

网神 SecWAF 3600 Web 应用防火墙自主开发的旁路阻断模式，大部分的 Web 应用防火墙都是串联部署在网络中进行流量过滤的。但是有些客户的网络只允许旁路部署产品。网神 SecWAF 3600 Web 应用防火墙使用镜像分析功能与交换机、网站服务器进行联动，实现旁路部署阻断 Web 攻击行为。

3.8 威胁情报中心

网神 SecWAF 3600 Web 应用防火墙内置有威胁情报中心功能，实际就是 Web 应用防火墙制作了一个人工智能大脑，与云端实现数据交流。实现 Web 应用防火墙自主发现攻击行为，并智能化判定对于攻击行为的是阻断或是放行，支持国内外各大安全情报中心联动功能，提供联动方式与情报中心数据情况。

3.9 网站云防护

网神 SecWAF 3600 Web 应用防火墙产品实现了重塑网站防护边界，在物理服务器的前端构建了硬件产品的物理网站防护边界。在互联网利用虚拟化技术构建了虚拟的网络边界网站防护体系。两个网站防护边界实现多层过滤，多层拦截的多边界协同防护体系。

3.10 网页防篡改

网神 SecWAF 3600 Web 应用防火墙内置有网页防篡改监控平台，可以对网页防篡改客户端进行实时监控。当网页防篡改客户端与网神 SecWAF 3600 Web 应用防火墙的网络中断时，网页文件会被自动锁定，所有“写”的权限进行封锁，只有“读”的权限。当网络恢复中，所有相关权限会自动下发，网站正常恢复更新。

3.11 DDoS 清洗

应用层除了 SQL 注入、XSS 跨站脚本、信息泄露、溢出等攻击方式外，还有像 CC 攻击、flood 攻击等洪水攻击方式。针对洪水攻击方式，网神 SecWAF 3600 Web 应用防火墙有 DDoS 清洗功能，主要是针对 CC 攻击、Flood 攻击、并发连接数进行平均值和突发值进行设置。

当监测中网络流量突破突发值的时候，网神 SecWAF 3600 Web 应用防火墙会把流量降低至平均值。避免网站服务器因洪水攻击造成 CPU 负载过高，无法对访问流量进行处理导致服务器出现宕机现象

3.12 冗余螺旋系统

网神 SecWAF 3600 Web 应用防火墙硬件出现掉电问题时，设备可以自动跳 bypass，保障网络畅通。但是如果软件出现问题时，我们往往不知道如何处理。很多实践证明，设备软件出现异常问题，除了找专业人员进行处理之外。很多管理员对设备都无从下手。

网神 SecWAF 3600 Web 应用防火墙内置冗余螺旋系统，针对软件自身出现异常问题时，可以手工切换到另外一套系统，配置依然保存可以使用，保证软件的正常运行和网站的安全防护。

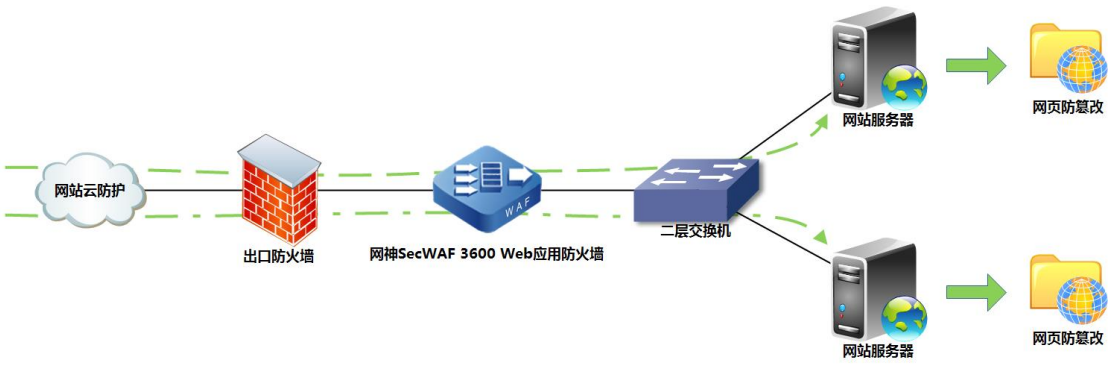
3.13 bypass 机制

网神 SecWAF 3600 Web 应用防火墙内置有 bypass 机制。bypass 机制是由硬件 bypass 和软件 bypass 组成。硬件 bypass 主要针对于谁被掉电后，设备本身没有电力供应，设备会自动变为网络直通。软件 bypass 主要针对软件性能问题，如果 CPU、内存、软件出现异常。软件 bypass 功能会自动启动。软件会把所有通过第二层（OSI 模型的数据链路层）直接变为数据转发。

4.典型应用

4.1 拓扑图

网神 SecWAF 3600 Web 应用防火墙系统属于串联部署产品，产品部署在网站服务器的前端。对外来访问网站的流量进行过滤。网神 SecWAF 3600 Web 应用防火墙需要配置 DNS 服务器，可以实现威胁情报中心、网站云防护等功能。在网站服务器上按照客户端，可以实现网页防篡改功能。



拓扑图

4.2 总结

随着 Web 应用的丰富，各类攻击工具不断的普遍和强大，互联网上的安全隐患越来越多。随着客户核心业务系统对网络依赖程度的增加，Web 应用攻击事件数量将会持续增长，损失严

重程度也会剧增。因此，政府、企业等各类组织都必须有所对策以保护其投资、利润和服务。

网神 SecWAF 3600 Web 应用防火墙系统实现真正意义上的 WEB 安全解决方案，采用围绕三个概念“重塑网站边界”、“智能化防护理念”、“纵深防御体系”。产品提供了业界领先的 Web 应用攻击防护能力，通过多种机制的分析检测，网神的产品和技术能够有效的阻断攻击，保证 Web 应用合法流量的正常传输，这对于保障业务系统的运行连续性和完整性有着极为重要的意义。同时，针对当前的热点问题，如 SQL 注入攻击、网页篡改、网页挂马等，网神 SecWAF 3600 Web 应用防火墙按照安全事件发生的时序考虑问题，优化最佳安全-成本平衡点，有效降低安全风险。