ICS 35.040
L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术
网站安全云防护平台技术要求

Information security technology —

Technology requirement for website security cloud protection platform

点击此处添加与国际标准一致性程度的标识

文稿版次选择

（本稿完成日期：2017 年 8 月 15 日）

XXXX－XX－XX 发布　　XXXX－XX－

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009《标准化工作导则　第1部分：标准的结构和编写》给出的规则起草。

请注意本文件的其他内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：国家工业信息安全发展研究中心、公安部第三研究所、中国信息安全研究院有限公司、北京知道创宇信息技术有限公司、北京奇安信科技有限公司、阿里云计算有限公司、杭州安恒信息技术有限公司、深圳市深信服电子科技有限公司

本标准主要起草人：刘迎、张格、左晓栋、宋好好、杨晨、于盟、吴艳艳、唐旺、江浩、刘文胜、张哲宇、肖俊芳、李俊、郭娴、赵伟、赵光明、李鸿培、国艳松、陈雪秀、宋志明、周欣、刘伯仲、王朋涛、陈妍、陆臻、顾健、周俊、毛润平。

信息安全技术　网站安全云防护平台技术要求

1　范围

本标准规定了网站安全云防护平台的技术要求，包括平台功能要求和平台安全要求。

本标准适用于网站安全云防护平台的开发、运营及使用，为政府部门、企事业单位、社会团体等组织或个人选购网站安全云防护平台提供参考。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范

GB/T 25069-2010 信息安全技术 术语

GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

GB/T 32917-2016 信息安全技术 WEB应用防火墙安全技术要求与测试评价方法

3　术语和定义

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

3.1

网站安全云防护平台 Website security cloud protection platform

以云服务模式提供网站安全防护，运用集中管控、协同防御等方式，及时更新防护策略和规则，对网站访问请求和响应进行检测、分析、过滤的一组安全防护节点的集合。

3.2

网站安全云防护平台提供者Website security protection cloud platform providers

负责建立、运营网站安全云防护平台相关的基础设施、网络拓扑结构、防护功能组件等，在此平台上执行安全防护、保障网站安全的组织或机构。

3.3

网站安全云防护平台用户 Website security cloud protection platform users

使用网站安全云防护平台的组织或个人。

3.4

网站运营者

负责网站后期运作、维护、经营的组织或个人。

4　缩略语

HTTP：超文本传输协议（HyperText Transfer Protocol）

HTTPS：安全超文本传输协议（Hypertext Transfer Protocol over Secure Socket Layer）

OWASP：开放式网页应用程序安全项目（Open Web Application Security Project）
CSRF：跨站请求伪造（Cross-site request forgery）
DNS：域名系统（Domain Name System）
HTTP：超文本传输协议（Hyper Text Transfer Protocol）
ICMP：网际控制报文协议（Internet Control Message Protocol）
IP：网际协议（Internet Protocol）
SQL：结构化查询语言（Structured Quevy Language）
TCP：传输控制协议（Transport Control Protocol）
UDP：用户数据报协议（User Datagram Protocol）
URL：统一资源定位符（Uniform Resource Locator）
XSS：跨站攻击（Cross Site Scripting ）
SaaS：软件即服务（Software-as-a-Service）

5 概述

网站安全云防护平台由一组相互联系、统一调度的安全防护节点组成，平台通过DNS解析、路由转发、IP地址接入等方式引入网站流量，利用云服务模式，集中快速地更新防护策略和规则，对网站恶意访问流量的过滤和清洗，将安全访问流量转发到网站上，实现网站安全访问。

网站安全云防护平台位于网站访问者和网站系统之间，如图 1 所示。网站运营者无需部署软、硬件设施，可快速按需使用平台的防护资源。

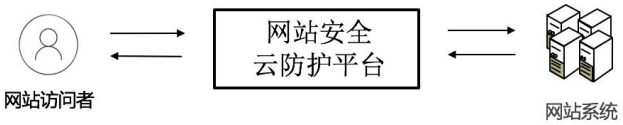

图 1 网站安全云防护平台部署位置示意图

本标准从网站安全云防护平台的功能要求、安全要求两个方面，规范了网站安全云防护平台的技术要求。其中，平台功能要求是对网站安全云防护平台应具备的功能提出具体要求，包括网站安全防护、集中管控、弹性可扩展等；平台安全要求是对为保障网站安全云防护平台的安全提出的要求，包括基本安全要求、平台资源监控及优化、安全事件响应等。

本标准规定的网站安全云防护平台技术要求按照平台的功能和安全要求的强度，分为一般要求和增强要求。一般要求是网站安全云防护平台在开展网站安全防护业务时应具备必要的功能及安全控制措施，保护网站抵御或应对常见的攻击、威胁。增强要求是对一般要求的补充和强化，是网站安全云防护平台保障网站安全时提供的更高级别的功能及安全控制措施。网站安全云防护平台用户根据自身业务需求及存储的信息敏感程度选择相应安全防护水平的网站安全云防护平台提供者。

6 平台功能要求

6.1 网站安全防护

6.1.1 WEB 攻击防御

一般要求：

平台应支持WEB攻击类型的识别及直接或间接阻断攻击行为，包括：

a) GB/T 32917-2016 中要求的安全防护功能；
b) 非授权访问防护；
c) 暴力破解防护；
d) Webshell 识别和拦截；
e) 目录遍历防护；
f) Cookie 注入攻击；
g) 恶意代码执行；
h) 其他 WEB 攻击的防护能力。

增强要求：

无。

6.1.2 DDoS 攻击防御

一般要求：

平台应支持DDoS清洗，应能够正常防御SYN Flood、ACK Flood、ICMP Flood、UDP Flood、HTTP Flood、DNS Flood、CC攻击等拒绝服务类攻击。

增强要求：

无。

6.1.3 协同防御

一般要求：

平台应支持：

a) 识别攻击常用 IP 地址信息，包括地理位置、国家、活跃时间等；
b) 对持续发起网站扫描的 IP 地址进行阻断；
c) 对恶意攻击者 IP 地址在整个云防护范围内进行阻断。

增强要求：

平台应支持对政府主管部门通报的域名拒绝接入或封禁。

6.1.4 内容安全

6.1.4.1 敏感信息过滤

一般要求：

平台应支持网站文字内容过滤：

a) 支持自定义敏感词汇；
b) 对出现的敏感词汇进行过滤。

增强要求：

无。

6.1.4.2 错误页面处理

一般要求：

平台应支持 GB/T 32917-2016 中要求的自定义错误页面功能。

增强要求：

无。

6.1.4.3 篡改应对

一般要求：

平台应支持向网站访问者提供未篡改页面功能。

增强要求：

无。

6.1.5 网站监控

一般要求：

平台应对网站被攻击情况监控。

增强要求：

平台应支持:

a) 网站可用性监控；

b) 异常发生时向平台用户发出告警。

6.1.6 网站访问控制

一般要求：

平台应支持：

a) 设置 IP 地址白名单或网站 URL 白名单，为网站访问者保留访问通道；

b) 设置 IP 地址黑名单，对列入 IP 地址黑名单的访问者进行阻断；

c) 在预定义时间段内，对网站的任何访问请求进行访问控制，设置为阻断/放过；

d) 预定义 URL 页面的来访请求进行阻断/放过；

e) 以上访问控制策略的组合使用。

增强要求：

平台应支持区域访问控制功能，可设置仅允许或禁止某个区域的访问。

6.1.7 防护策略管理

一般要求：

平台应支持：

a) 提供默认安全防护策略；

b) 平台用户配置与选择防护策略；

c) 提供检测、防护等多种策略模式。

增强要求：

无。

6.2 集中管控

6.2.1 策略集中管控

一般要求：

平台应支持：

a) 对网站防护策略和规则进行集中维护和管理；

b) 对策略及规则统一更新下发。

增强要求：

无。

6.2.2 资源集中管控

一般要求：

对平台资源集中管控，包括但不限于：

a) 安全防护节点；
b) 网站及用户配置信息；
c) 平台日志信息。

增强要求：

无。

6.3 弹性可扩展

6.3.1 基础资源动态扩展

一般要求：

平台应支持计算、网络和存储等资源在不间断服务情况下的动态扩展，包括但不限于：

a) 防护服务器的增加（扩容）、转移；
b) 防护带宽扩容；
c) 网络线路增加；
d) DNS 选路增加。

增强要求：

无。

6.3.2 系统扩展

一般要求：

平台应支持对外部系统提供各类API接口，以方便外部系统访问集成，包括但不限于日志接口，安全策略接口，报表接口。

增强要求：

无。

6.4 网站合法性验证

一般要求：

平台应支持在网站接入前进行网站备案情况检查，拒绝未备案网站的接入。

增强要求：

平台应支持定期复查已接入网站备案情况。

6.5 统计分析

一般要求：

平台应支持：

a) 对某一时间段内告警日志进行统计分析；
b) 对不同攻击类型事件数量进行统计分析；
c) 对攻击地理区域进行统计分析；
d) 对攻击源 IP 进行统计分析；
e) 以上数据统计的可视化图表，支持按照日、周和自定义时间等时间维度进行展示。

增强要求：

无。

7 平台安全要求

7.1 基本安全要求

一般要求：

平台应参照GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》中系统与通讯保护、访问控制、维护、审计、物理环境与安全等相关控制措施的一般要求及其他国家、行业或机构的有关信息安全标准规范落实平台自身的安全要求。

增强要求：

无。

7.2 平台运行监控

一般要求：

平台应：

a) 对支撑平台运行的分布式防护节点的处理器、网络、内存等资源的状态进行统一监控和管理；
b) 对软件系统的运行状态进行记录，并生成分析报告；
c) 及时发现资源使用异常和软件系统异常，记录并告警；
d) 对资源使用情况、平台承载业务量进行定期分析，评估是否满足当前业务、平台用户扩容及新用户接入的需求。

增强要求：

平台应：

a) 通过对平台运行监控发现的异常及报警采取自动应对措施；
b) 在评估当前资源不满足业务需求时，动态调整并按约定方式告知用户；
c) 提供对资源使用、软件运行、系统异常等记录的查询、统计，及报表输出功能。

7.3 平台优化更新

7.3.1 平台资源优化

一般要求：

平台应：

a) 支持对资源使用的快速增长通过技术手段进行快速扩容；
b) 对资源优化方案及软件系统上线在实施前进行充分测试，确保实施结果符合设计预期；
c) 对优化更新过程记录；
d) 在资源及软件系统优化更新不成功或有回退要求时，应能回退到变更前状态并记录；
e) 对资源及软件系统更新优化影响范围内的用户进行提示或通报。

增强要求：

无。

7.3.2 平台策略更新

一般要求：

平台应：

a) 定期及时优化网站安全防护策略和规则；

b) 具备未知攻击手段及 WEB 安全漏洞的及时跟踪、发现、应对能力；

c) 在 WEB 安全漏洞通报后 24 小时内增加相应安全防护规则或更新安全防护策略。

增强要求：

无。

7.4 安全事件响应

一般要求：

平台应：

a) 具备框架符合 GB/T 24363-2009 要求的安全事件处置预案；

b) 在安全事件发生时，及时通知平台用户安全事件的风险及威胁；

c) 依照 GB/Z 20986-2007 对事件的分级，在发生重大及以上安全事件后 4 小时内快速响应处置；

d) 对安全事件处置过程及结果进行记录，形成处置报告。

增强要求：

无。

7.5 平台容灾备份

一般要求：

平台应：

a) 具备数据级和应用级灾难备份及恢复的能力；

b) 对灾难备份和恢复过程进行记录存储；

c) 支持故障转移速度/时间符合合同或服务水平协议的约定。

增强要求：

平台应具备防护集群、运行数据中心多地理位置分布。

7.6 用户数据保护

一般要求：

平台对于用户网站数据（包括网站信息、原始访问流量、访问日志、操作日志、被攻击日志等），应：

a) 支持用户数据隔离，平台用户仅能访问自身的安全防护资源；

b) 明确用户网站数据归属于用户，不提供给任意第三方；

c) 在用户授权情况下进行漏洞分析、攻击数据挖掘等提升平台安全防护能力的行为；

d) 支持在法律允许范围内留存用户数据，并支持平台用户自定义保存期限；

e) 在用户退出平台服务时移交用户网站数据，并销毁所有用户网站数据。

增强要求：

无。

参 考 文 献

[1] 中华人民共和国全国人民代表大会常务委员会，中华人民共和国网络安全法， 2016年11月7日
[2] GB/T 28451-2012 信息安全技术 网络型入侵防御产品技术要求和测试评价方法
[3] GB/T 28827.1-2012 信息技术服务 运行维护 第1部分：通用要求
[4] GB/T 30276-2013 信息安全技术 信息安全漏洞管理规范
[5] GB/T 32914-2016 信息安全技术 信息安全服务提供方管理要求
[6] NIST SP800-53-r4,Security and Privacy Controls for Federal Information Systems and Organizations, June 2013