



中华人民共和国公共安全行业标准

GA/T 1527—2018

信息安全技术 云计算安全综合 防御产品安全技术要求

Information security technology—Security technical requirements for
cloud computing security comprehensive defense products

2018-11-05 发布

2018-11-05 实施

中华人民共和国公安部 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 云计算安全综合防御产品描述 1

5 总体说明 2

 5.1 安全技术要求分类 2

 5.2 安全等级 2

6 安全功能要求 2

 6.1 安全联动及响应 2

 6.2 防御功能 3

 6.3 集中管控 3

 6.4 弹性扩展 3

 6.5 安全管理 4

 6.6 通信安全 4

 6.7 审计功能 4

 6.8 升级安全 5

 6.9 运行安全 5

7 安全保障要求 5

 7.1 开发 5

 7.2 指导性文档 6

 7.3 生命周期支持 6

 7.4 测试 7

 7.5 脆弱性评定 8

8 等级划分要求 8

 8.1 概述 8

 8.2 安全功能要求等级划分 8

 8.3 安全保障要求等级划分 9

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心（公安部第三研究所）。

本标准主要起草人：宋好好、陈妍、邹春明、陆臻、沈亮、邱梓华、顾健。

信息安全技术 云计算安全综合 防御产品安全技术要求

1 范围

本标准规定了云计算安全综合防御产品的安全功能要求、安全保障要求及等级划分要求。
本标准适用于云计算安全综合防御产品的设计、开发及测试。

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 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件

GB/T 25069—2010 信息安全技术 术语

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

3 术语和定义

GB/T 25069—2010、GB/T 31167—2014 和 GB/T 31168—2014 界定的以及下列术语和定义适用于本文件。

3.1

云计算平台 cloud computing platform

由云服务商提供的云基础设施及其上的服务层软件的集合。

4 云计算安全综合防御产品描述

云计算安全综合防御产品是基于云计算平台构建的、可弹性扩展的、主要对云计算平台和云计算服务及上层业务应用进行综合安全防护的产品,具备防御来自云平台外部、虚拟机之间以及虚拟机对外部的恶意攻击的功能。该产品的安全能力主要体现在与云计算平台的联动及响应,以及各安全模块之间的联动及响应上,并且该产品的安全模块是可扩展的,至少包括抗拒绝攻击模块、虚拟机异常行为监测和识别模块、WEB应用安全扫描模块、WEB应用安全防护模块等。图1为云计算安全综合防御产品典型运行环境。

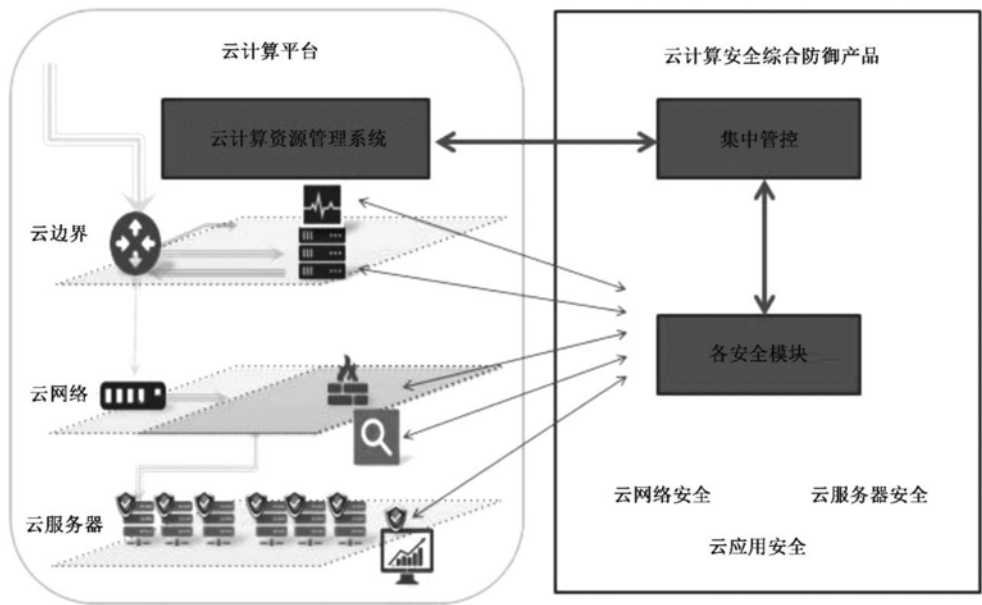


图 1 云计算安全综合防御产品典型运行环境

5 总体说明

5.1 安全技术要求分类

本标准将云计算安全综合防御产品安全技术要求分为安全功能要求和安全保障要求两个大类。其中,安全功能要求是对云计算安全综合防御产品应具备的安全功能提出具体要求,包括安全联动、集中管控和弹性扩展等;安全保障要求针对云计算安全综合防御产品的开发和使用文档的内容提出具体的要求,例如开发、指导性文档、生命周期支持、测试、脆弱性评定等。

5.2 安全等级

本标准按照云计算安全综合防御产品安全功能要求强度,以及按照 GB/T 18336.3—2015,对云计算安全综合防御产品安全等级进行划分。安全等级分为基本级和增强级,安全功能强弱和安全保障要求高低是等级划分的具体依据,安全等级突出安全特性。

6 安全功能要求

6.1 安全联动及响应

6.1.1 与云计算平台联动及响应

产品应具备与云计算平台进行协同联动及响应功能,支持:

- a) 及时同步更新云计算平台虚拟机的基础信息(如 IP 地址等);
- b) 检测发现虚拟机异常行为后进行告警,并协同云计算平台进行处置;
- c) 检测到外部攻击导致虚拟机宕机后,协同云计算平台禁止启动宕机迁移规则,从而避免大规模虚拟机宕机;
- d) 对待发布到互联网上的违禁/未备案信息进行检测和告警,并协同云计算平台进行分析,保存

所在虚拟机的镜像文件。

6.1.2 各安全模块联动及响应

产品各安全模块应具备协同联动及响应功能：

- a) 抗拒绝攻击模块能够调用虚拟机异常行为监测和识别模块的安全事件信息,并对异常行为进行处置；
- b) 虚拟机异常行为监测和识别模块能够调用抗拒绝攻击模块的安全事件信息,并对异常行为进行处置；
- c) WEB 应用安全扫描模块能够调用虚拟机异常行为监测和识别模块的安全事件信息,并对虚拟机上的 WEB 应用进行安全扫描；
- d) WEB 应用安全防护模块能够调用 WEB 应用安全扫描模块的扫描结果,对 WEB 应用进行安全防护；
- e) 其他安全模块协同联动及响应能力。

6.2 防御功能

产品应具备对拒绝服务攻击、WEB 攻击、主机入侵攻击等进行综合防御的功能：

- a) 对从云计算平台外部发起的对云平台攻击的检测、告警和全网阻断；
- b) 对从云计算平台内部发起的对外部攻击的检测和处置；
- c) 对从云计算平台虚拟机间发起攻击的检测和处置。

6.3 集中管控

6.3.1 策略管理

产品应具备安全策略管理功能,支持：

- a) 对安全策略(如 DDOS 防护策略,黑白名单等)进行配置,对安全策略库进行管理(如新增、删除或停用安全策略等)；
- b) 对安全策略进行分类分级管理,并支持自定义安全策略；
- c) 对安全策略进行集中维护和管理；
- d) 支持对漏洞特征库和攻击特征库进行统一管理和升级。

6.3.2 统计分析

产品应具备统计分析功能,支持：

- a) 对某一时间段内总体安全事件数量进行统计分析,并生成包含可视化图表的日报、周报；
- b) 对攻击事件进行统计分析,并生成包含可视化图表的日报、周报；
- c) 对云计算平台安全防护效果进行实时查询,并可视化展示；
- d) 对安全事件日志提供日志导出功能。

6.4 弹性扩展

产品应具备弹性扩展功能,支持：

- a) 集群部署、资源弹性伸缩；
- b) 独立扩展各安全功能模块的防护能力；
- c) 增加新的安全功能模块。

6.5 安全管理

6.5.1 属性初始化

产品应提供授权管理员属性(权限、口令等)的初始化能力。

6.5.2 唯一性标识

产品应为授权管理员提供唯一的身份标识,同时将授权管理员的身份标识与该授权管理员的所有可审计事件相关联。

6.5.3 属性修改

产品应提供授权管理员的属性(至少包括管理员口令)的修改能力。

6.5.4 身份鉴别

产品应在执行任何与安全功能相关的操作之前鉴别任何声称要履行授权管理员职责的管理员身份。

6.5.5 最少反馈

对管理员身份进行鉴别时,产品应仅将最少的信息反馈(如:鉴别的成功或失败)提供给被鉴别的管理员。

6.5.6 鉴别失败处理

当对授权管理员鉴别失败的次数达到指定阈值后,产品应阻止授权管理员进一步的鉴别请求。

6.5.7 管理能力

产品应提供授权管理员配置和管理产品安全功能的能力。

6.5.8 管理角色

产品应能对管理员角色进行区分:

- a) 具有系统管理员、安全管理员、安全审计员等至少 3 种不同权限的管理员角色;
- b) 根据不同的功能模块,自定义各种不同权限角色,并可对管理员分配角色。

6.6 通信安全

应对产品组件间通过网络传输的数据进行保护,实现保密传输。

6.7 审计功能

6.7.1 审计日志生成

产品应能对下列事件生成审计日志:

- a) 所有鉴别机制的使用,包括系统管理员的登录和注销日志;
- b) 管理员执行管理操作的行为,包括系统安全策略变更的操作日志,对系统管理员角色进行增加、删除和属性修改的操作。

应在每一个审计日志中记录事件发生的日期和时间、事件主体身份、事件描述、事件结果的标志。

6.7.2 审计日志管理

产品应提供以下功能对审计日志进行管理：

- a) 将审计日志存储在掉电非易失性存储介质中；
- b) 只允许授权管理员访问审计日志；
- c) 按日期、时间、用户标识、主机资源标识等条件对审计日志进行组合查询；
- d) 对审计日志进行备份；
- e) 当审计日志的存储容量到达阈值时，应能及时通知授权管理员。

6.8 升级安全

产品应确保漏洞库和攻击特征库升级时的安全。

6.9 运行安全

6.9.1 自我监测

产品在启动和正常工作时，应周期性地或者按照授权管理员的要求执行自检，以验证产品自身执行的正确性。

6.9.2 产品失效处理

产品失效时应及时向管理员报警。

6.9.3 冗余部署

应支持集群或多点部署，避免因单一硬件设备故障导致产品功能失效。

7 安全保障要求

7.1 开发

7.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

- a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
- b) 描述与安全功能要求一致的产品安全功能的安全域；
- c) 描述产品安全功能初始化过程为何是安全的；
- d) 证实产品安全功能能够防止被破坏；
- e) 证实产品安全功能能够防止安全特性被旁路。

7.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

- a) 完全描述产品的安全功能；
- b) 描述所有安全功能接口的目的与使用方法；
- c) 标识和描述每个安全功能接口相关的所有参数；
- d) 描述安全功能接口相关的安全功能实施行为；
- e) 描述由安全功能实施行为处理而引起的直接错误消息；
- f) 证实安全功能要求到安全功能接口的追溯；

- g) 描述安全功能实施过程中,与安全功能接口相关的所有行为;
- h) 描述可能由安全功能接口的调用而引起的所有直接错误消息。

7.1.3 实现表示

开发者应提供全部安全功能的实现表示,实现表示应满足以下要求:

- a) 提供产品设计描述与实现表示实例之间的映射,并证明其一致性;
- b) 按详细级别定义产品安全功能,详细程度达到无须进一步设计就能生成安全功能的程度;
- c) 以开发人员使用的形式提供。

7.1.4 产品设计

开发者应提供产品设计文档,产品设计文档应满足以下要求:

- a) 根据子系统描述产品结构;
- b) 标识和描述产品安全功能的所有子系统;
- c) 描述安全功能所有子系统间的相互作用;
- d) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口;
- e) 根据模块描述安全功能;
- f) 提供安全功能子系统到模块间的映射关系;
- g) 描述所有安全功能实现模块,包括其目的及与其他模块间的相互作用;
- h) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口;
- i) 描述所有安全功能的支撑或相关模块,包括其目的及与其他模块间的相互作用。

7.2 指导性文档

7.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南,操作用户指南与为评估而提供的其他所有文档保持一致,对每一种用户角色的描述应满足以下要求:

- a) 描述在安全处理环境中被控制的用户可访问的功能和特权,包含适当的警示信息;
- b) 描述如何以安全的方式使用产品提供的可用接口;
- c) 描述可用功能和接口,尤其是受用户控制的所有安全参数,适当时指明安全值;
- d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件,包括改变安全功能所控制实体的安全特性;
- e) 标识产品运行的所有可能状态(包括操作导致的失败或者操作性错误),以及它们与维持安全运行之间的因果关系和联系;
- f) 充分实现安全目的所必须执行的安全策略。

7.2.2 准备程序

开发者应提供产品及其准备程序,准备程序描述应满足以下要求:

- a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤;
- b) 描述安全安装产品及其运行环境必需的所有步骤。

7.3 生命周期支持

7.3.1 配置管理能力

开发者的配置管理能力应满足以下要求:

- a) 为产品的不同版本提供唯一的标识；
- b) 使用配置管理系统对组成产品的所有配置项进行维护,并唯一标识配置项；
- c) 提供配置管理文档,配置管理文档描述用于唯一标识配置项的方法；
- d) 配置管理系统提供一种自动方式来支持产品的生成,通过该方式确保只能对产品的实现表示进行已授权的改变；
- e) 配置管理文档包括一个配置管理计划,配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
- f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

7.3.2 配置管理范围

开发者应提供产品配置项列表,并说明配置项的开发者。配置项列表应包含以下内容：

- a) 产品、安全保障要求的评估证据和产品的组成部分；
- b) 实现表示、安全缺陷报告及其解决状态。

7.3.3 交付程序

开发者应使用一定的交付程序交付产品,并将交付过程文档化。在给用户方交付产品的各版本时,交付文档应描述为维护安全所必需的所有程序。

7.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中,为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

7.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制,并提供生命周期定义文档描述用于开发和维护产品的模型。

7.3.6 工具和技术

开发者应明确定义用于开发产品的工具,并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

7.4 测试

7.4.1 测试覆盖

开发者应提供测试覆盖文档,测试覆盖描述应满足以下要求：

- a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；
- b) 表明上述对应性是完备的,并证实功能规范中的所有安全功能接口都进行了测试。

7.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

- a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；
- b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

7.4.3 功能测试

开发者应测试产品安全功能,将结果文档化并提供测试文档。测试文档应包括以下内容：

- a) 测试计划,标识要执行的测试,并描述执行每个测试的方案,这些方案包括对于其他测试结果的任何顺序依赖性;
- b) 预期的测试结果,表明测试成功后的预期输出;
- c) 实际测试结果和预期的测试结果的一致性。

7.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源,以用于安全功能的抽样测试。

7.5 脆弱性评定

基于已标识的潜在脆弱性,产品能够抵抗以下攻击行为:

- a) 具有基本攻击潜力的攻击者的攻击;
- b) 具有增强型攻击潜力的攻击者的攻击。

8 等级划分要求

8.1 概述

依据云计算安全综合防御产品的开发、生产现状及实际应用情况,将安全功能要求和安全保障要求划分成基本级和增强级。

8.2 安全功能要求等级划分

云计算安全综合防御产品的安全功能要求等级划分见表 1。

表 1 云计算安全综合防御产品安全功能要求等级划分

安全功能要求		基本级	增强级
安全联动	与云计算平台联动及响应	6.1.1 a) ~6.1.1 c)	6.1.1
	各安全模块联动及响应	6.1.2 a) ~6.1.2 d)	6.1.2
防御功能		6.2	6.2
集中管控	策略管理	6.3.1	6.3.1
	统计分析	6.3.2	6.3.2
弹性扩展		6.4 a) ~6.4 b)	6.4
安全管理	属性初始化	6.5.1	6.5.1
	唯一性标识	6.5.2	6.5.2
	属性修改	6.5.3	6.5.3
	身份鉴别	6.5.4	6.5.4
	最少反馈	6.5.5	6.5.5
	鉴别失败处理	—	6.5.6
	管理能力	6.5.7	6.5.7
	管理角色	6.5.8 a)	6.5.8
通信安全		6.6	6.6

表 1（续）

安全功能要求		基本级	增强级
审计功能	审计日志生成	6.7.1	6.7.1
	审计日志管理	6.7.2	6.7.2
升级安全		6.8	6.8
运行安全	自我监测	6.9.1	6.9.1
	产品失效处理	6.9.2	6.9.2
	冗余部署	6.9.3	6.9.3

8.3 安全保障要求等级划分

云计算安全综合防御产品的安全保障要求等级划分见表 2。

表 2 云计算安全综合防御产品安全保障要求等级划分

安全保障要求		基本级	增强级
开发	安全架构	7.1.1	7.1.1
	功能规范	7.1.2 a) ~7.1.2 f)	7.1.2
	实现表示	—	7.1.3
	产品设计	7.1.4 a) ~7.1.4 d)	7.1.4
指导性文档	操作用户指南	7.2.1	7.2.1
	准备程序	7.2.2	7.2.2
生命周期支持	配置管理能力	7.3.1 a) ~7.3.1 c)	7.3.1
	配置管理范围	7.3.2 a)	7.3.2
	交付程序	7.3.3	7.3.3
	开发安全	—	7.3.4
	生命周期定义	—	7.3.5
	工具和技术	—	7.3.6
测试	测试覆盖	7.4.1 a)	7.4.1
	测试深度	—	7.4.2
	功能测试	7.4.3	7.4.3
	独立测试	7.4.4	7.4.4
脆弱性评定		7.5 a)	7.5 b)

中华人民共和国公共安全
行 业 标 准
信息安全技术 云计算安全综合
防御产品安全技术要求

GA/T 1527—2018

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址: www.spc.org.cn

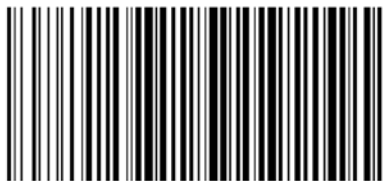
服务热线: 400-168-0010

2019年9月第一版

*

书号: 155066 • 2-34218

版权专有 侵权必究



GA/T 1527-2018