ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1345—2017

信息安全技术　云计算网络入侵防御系统安全技术要求

Information security technology—Security technical requirements for cloud computing network intrusion prevention system

2017-11-20 发布　　2017-11-20 实施

中华人民共和国公安部　　发布

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：顾建新、顾健、张笑笑、沈亮、赵婷、顾玮。

信息安全技术　云计算网络入侵防御系统安全技术要求

1　范围

本标准规定了云计算环境下的网络入侵防御系统产品的安全功能要求、安全保障要求和等级划分要求。

本标准适用于云计算环境下的网络入侵防御系统产品的设计、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

3　术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

TCP 流重组　TCP reassembly

攻击者将发送的攻击数据分别在一个会话连接中的多个数据包发出，以躲避入侵防御系统的检测行为。

3.2

SHELL 代码变形　SHELL deformation

攻击者利用其他方式替代原有程序指令并以一种伪随机的方式结合到一起，以躲避入侵防御系统检测缓冲区溢出攻击的行为。

3.3

报警　alert

当产品发现有入侵行为时，向用户发出的紧急通知。

3.4

南北向流量　north-south flow

云计算平台内部与外部交互的流量。

3.5

东西向流量　east-west flow

云计算平台内部交互的流量。

4　缩略语

下列缩略语适用于本文件。

DDOS:分布式拒绝服务(Distributed Denial of Service)
IP:网际协议(Internet Protocol)
IPS:入侵防御系统(Intrusion Prevention System)
TCP:传输控制协议(Transmission Control Protocol)
URL:统一资源定位器(Universal Resource Locator)
VLAN:虚拟局域网(Virtual Local Area Network)
VXLAN:虚拟可扩展局域网(Virtual eXtensible Local Area Network)

5 云计算网络入侵防御系统描述

用户与各类云服务端资源进行交互过程中,从用户端至云端的各个虚拟服务器之间都有可能存在网络入侵攻击行为,云计算环境下的网络入侵防御系统产品能够通过分析判断用户所访问资源的安全性,经过协议分析、内容识别、特征提取匹配等方式,实现对入侵事件的有效识别和拦截,该产品通常以服务模块或者虚拟机的形式呈现,由后台服务器与多个引擎组成,引擎部署于云环境下的多个节点。如图 1 所示。

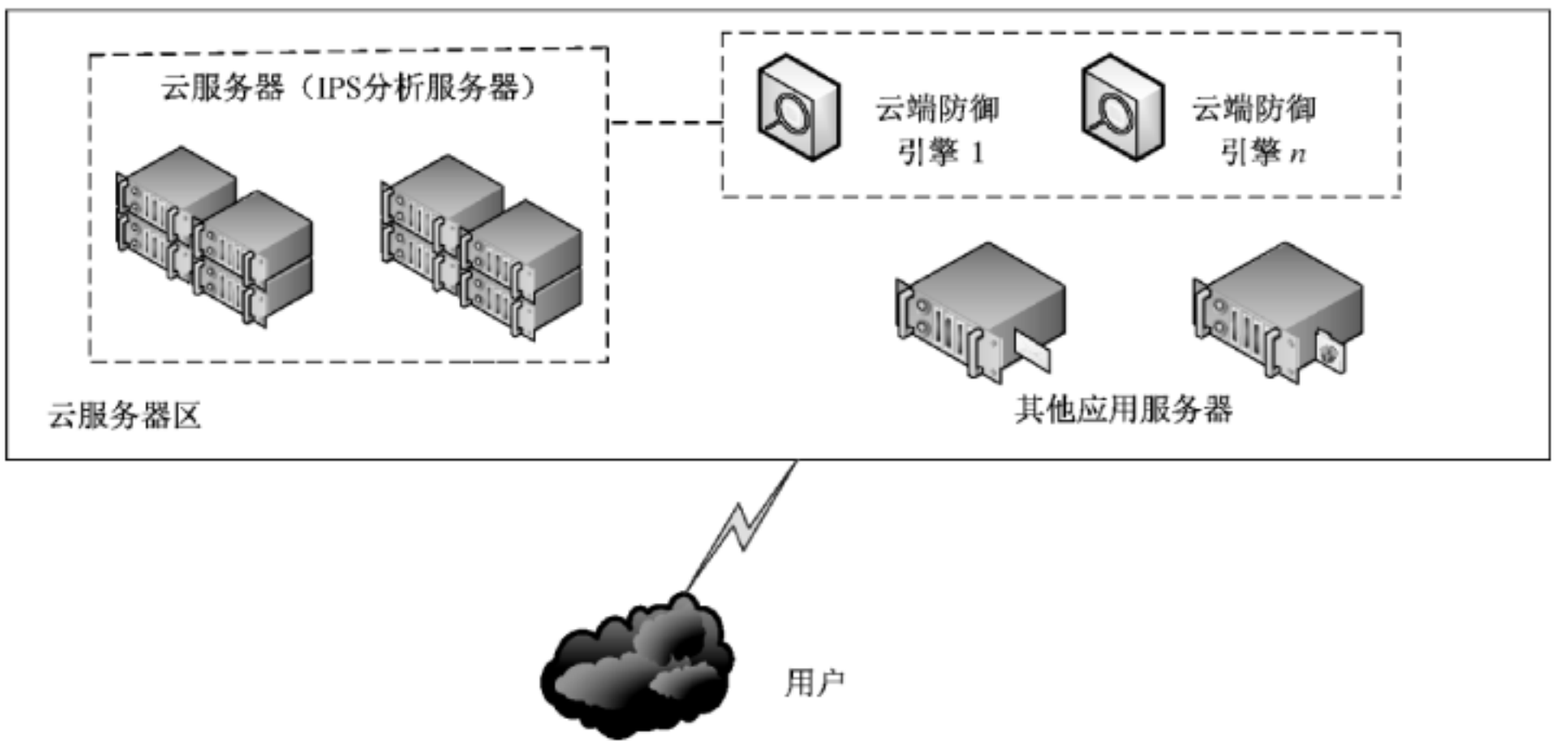

图 1 云计算网络入侵防御系统网络示意图

6 总体说明

6.1 安全技术要求分类

本标准将云计算网络入侵防御系统产品的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网络入侵防御系统产品应具备的安全功能提出的具体要求,包括入侵事件分析功能要求、入侵事件响应功能要求、入侵事件审计功能要求、管理控制功能要求和自身安全功能要求;安全保障要求是针对云计算网络入侵防御系统产品的开发和使用文档的内容提出的具体要求,例如开发、指导性文档、生命周期支持、测试和脆弱性评定等。

6.2 安全等级

本标准按照云计算网络入侵防御系统产品安全功能的强度划分安全功能要求的级别,参照 GB/T 18336.3—2015 划分安全保障要求的级别。安全等级突出安全性,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。

7 安全功能要求

7.1 入侵事件分析功能要求

7.1.1 同一虚拟网络内的协议分析

产品应具有对同一虚拟网络内，东西向流量和南北向流量进行协议分析的功能。

7.1.2 不同虚拟网络间的协议分析

产品应具有对不同虚拟网络间，东西向流量和南北向流量进行协议分析的功能。

7.1.3 数据收集

产品应具有实时收集流入目标网络内所有数据包的能力。

7.1.4 协议分析

产品应对收集的数据包进行协议分析，以采集、识别、特征提取等方式，自动分析判断用户所访问资源过程的安全性。

7.1.5 入侵发现

产品应能发现协议中的入侵行为。

7.1.6 入侵逃避发现

产品应能发现躲避或欺骗检测的行为，如 IP 碎片重组、TCP 流重组、协议端口重定位、URL 字符串变形、shell 代码变形等。

7.1.7 流量监测

产品应基于不同应用或者协议对目标环境中的流量进行监测。

7.1.8 IPv6 支持

产品应支持 IPv6 协议接入方式。

7.2 入侵事件响应功能要求

7.2.1 拦截能力

产品应对发现的入侵行为进行预先拦截，防止入侵行为进入目标网络。

7.2.2 安全报警

产品应在发现并拦截入侵行为时，采取相应动作发出安全警告。

7.2.3 报警方式

产品的报警方式应采取手机短信实时报警、E-mail 报警、屏幕实时报警等一种或多种方式。

7.2.4 事件合并

产品应具有对高频度发生的相同安全事件进行合并报警，避免出现报警风暴的能力。

7.3 入侵事件审计功能要求

7.3.1 事件生成

产品应能对拦截行为及时生成审计记录。

7.3.2 事件记录

产品应记录并保存拦截到的入侵事件。入侵事件信息应至少包含以下内容:事件名称、事件发生日期时间、源 IP 地址、源端口、目的 IP 地址、目的端口、危害等级等。

7.3.3 事件地图显示

产品应能基于地图进行安全事件的展示,包括以下内容:

a) 包括按源地区和目的地区展现进行查询;
b) 地图上展现的威胁类型包括:病毒、入侵防范、僵尸、木马、蠕虫等;
c) 包括最近一个小时、一天、一个月或者可以按指定日期段进行详细查询;
d) 基于地理位置的威胁分析;
e) 严重程度能有所区分;
f) 基于威胁事件类型的地图展示。

7.3.4 报表生成

产品应能生成详尽的结果报表,包括以下内容:

a) 支持报表内容设定功能;
b) 支持日报、周报、月报以及自定义时间报表功能。

7.3.5 报表查阅

产品应具有浏览结果报表的功能。

7.3.6 报表输出

产品应支持管理员按照自己的要求修改和定制报表内容,并输出成方便阅读的文件格式,至少支持以下报表文件格式中的一种或多种:DOC、PDF、HTML、XLS、WPS 等。

7.4 管理控制功能要求

7.4.1 管理界面

产品应提供用户界面用于管理、配置产品。管理配置界面应包含配置和管理产品所需的所有功能。

7.4.2 入侵规则库

产品应提供入侵事件规则库。规则库应包括规则名称、详细描述定义、响应措施配置等。

7.4.3 事件分级

产品应按照事件的严重程度对事件进行分级,以使授权管理员能从大量的信息中捕捉到危险的事件。

7.4.4 规则定义

产品应允许授权管理员自定义策略规则。

7.4.5 产品升级

产品应具备更新、升级产品的入侵规则库和软件版本的能力。

7.4.6 虚拟化支持

产品应支持虚拟化服务功能，包括以下内容：

a) 支持基于 VLAN、VXLAN 进行安全设备虚拟化防护；

b) 支持为多个不同租户提供虚拟化入侵防御服务功能。

7.4.7 云平台支持

产品应支持对两种及以上云计算平台进行安全防护。

7.4.8 对云主机进行安全防护

针对不同虚拟化平台内部的虚拟机，可以根据虚拟机的特征标记从云平台获取到虚拟机的 IP 地址，且 IP 地址可以动态更新，在虚拟机发生 IP 变更时，在保持原安全策略不变的前提下，对虚拟机仍实现有效的安全防护，具体包括以下内容：

a) 支持动态地址组功能；

b) 支持 IPS 与多个云平台虚拟机 IP 进行认证交互功能；

c) 支持动态地址组 IP 定时更新删除功能；

d) 支持动态地址组能够被 ACL 和安全策略引用功能。

7.5 自身安全功能要求

7.5.1 用户鉴别

产品应在用户执行任何与安全功能相关的操作之前对用户进行鉴别。

7.5.2 鉴别失败的处理

产品应在用户鉴别尝试失败连续达到指定次数后，阻止用户进一步进行尝试，并将有关信息生成审计事件。

7.5.3 鉴别数据保护

产品应保护鉴别数据不被未授权查阅和修改。

7.5.4 标识唯一性

产品应保证所设置的用户标识全局唯一。

7.5.5 用户属性定义

产品应为每一个用户保存安全属性表，属性应包括：用户标识、鉴别数据、授权信息或用户组信息、其他安全属性等。

7.5.6 安全数据管理

产品应仅限于指定的授权用户访问事件数据，禁止其他用户对事件数据的操作。

7.5.7 升级安全

产品应确保事件库和软件版本升级时的安全，保证升级包是由开发者提供的。

7.5.8 审计数据生成

产品应至少为下述可审计事件记录审计信息：

a） 试图登录产品管理界面和管理身份鉴别请求；

b） 所有对安全策略更改的操作；

c） 修改安全属性的所有尝试。

应在每个审计记录中至少记录如下信息：事件的日期和时间，事件类型，主体身份，事件的结果（成功或失败）等。

7.5.9 审计查阅

产品应为授权管理员提供从审计记录中读取全部审计信息的功能，并可对审计记录进行排序。

7.5.10 受限的审计查阅

除了具有明确访问权限的授权管理员之外，产品应禁止非授权用户对审计记录的访问。

8 安全保障要求

8.1 开发

8.1.1 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。

8.1.2 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。

8.1.3 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。

8.1.4 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。

8.2 指导性文档

8.2.1 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。

8.2.2 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。

8.3 生命周期支持

8.3.1 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。

8.3.2 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。

8.3.3 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。

8.3.4 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。

8.3.5 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。

8.3.6 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。

8.4 测试

8.4.1 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。

8.4.2 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。

8.4.3 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测试结果的一致性。

8.4.4 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。

8.5 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） 具有增强型基本攻击潜力的攻击者的攻击。

9 等级划分要求

9.1 概述

依据云计算网络入侵防御系统产品的开发、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两个等级。

9.2 安全功能要求等级划分

云计算网络入侵防御系统产品的安全功能要求等级划分如表 1 所示。

表 1 云计算网络入侵防御系统产品安全功能要求等级划分

安全功能要求		基本级	增强级
入侵事件分析功能要求	同一虚拟网络内的协议分析	7.1.1	7.1.1
	不同虚拟网络间的协议分析	7.1.2	7.1.2
	数据收集	7.1.3	7.1.3
	协议分析	7.1.4	7.1.4
	入侵发现	7.1.5	7.1.5
	入侵逃避发现	—	7.1.6
	流量监测	7.1.7	7.1.7
	IPv6 支持	—	7.1.8
入侵事件响应功能要求	拦截能力	7.2.1	7.2.1
	安全报警	7.2.2	7.2.2
	报警方式	—	7.2.3
	事件合并	—	7.2.4
入侵事件审计功能要求	事件生成	7.3.1	7.3.1
	事件记录	7.3.2	7.3.2
	事件地图显示	—	7.3.3
	报表生成	—	7.3.4
	报表查阅	—	7.3.5
	报表输出	—	7.3.6

表 1（续）

安全功能要求		基本级	增强级
管理控制功能要求	管理界面	7.4.1	7.4.1
	入侵规则库	7.4.2	7.4.2
	事件分级	7.4.3	7.4.3
	规则定义	—	7.4.4
	产品升级	7.4.5	7.4.5
	虚拟化支持	7.4.6	7.4.6
	云平台支持	7.4.7	7.4.7
	与云主机进行安全防护	7.4.8	7.4.8
自身安全功能要求	用户鉴别	7.5.1	7.5.1
	鉴别失败的处理	7.5.2	7.5.2
	鉴别数据保护	7.5.3	7.5.3
	标识唯一性	7.5.4	7.5.4
	用户属性定义	7.5.5	7.5.5
	安全数据管理	7.5.6	7.5.6
	升级安全	—	7.5.7
	审计数据生成	—	7.5.8
	审计查阅	—	7.5.9
	受限的审计查阅	—	7.5.10

9.3 安全保障要求等级划分

云计算网络入侵防御系统产品的安全保障要求等级划分如表 2 所示。

表 2 云计算网络入侵防御系统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	9.1.1	9.1.1
	功能规范	9.1.2 a）～f）	9.1.2
	实现表示	—	9.1.3
	产品设计	9.1.4 a）～d）	9.1.4
指导性文档	操作用户指南	9.2.1	9.2.1
	准备程序	9.2.2	9.2.2

表 2（续）

安全保障要求		基本级	增强级
生命周期支持	配置管理能力	9.3.1 a）～c）	9.3.1
	配置管理范围	9.3.2 a）	9.3.2
	交付程序	9.3.3	9.3.3
	开发安全	—	9.3.4
	生命周期定义	—	9.3.5
	工具和技术	—	9.3.6
测试	测试覆盖	9.4.1 a）	9.4.1
	测试深度	—	9.4.2
	功能测试	9.4.3	9.4.3
	独立测试	9.4.4	9.4.4
脆弱性评定		9.5 a）	9.5 b）

中华人民共和国公共安全
行业标准
信息安全技术 云计算网络
入侵防御系统安全技术要求
GA/T 1345—2017
*
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
2018年3月第一版
*
书号:155066·2-32732

GA/T 1345-2017