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。