ICS 35.040
L 80

GA

中华人民共和国公共安全行业标准

GA/T 1541—2018

信息安全技术
虚拟化安全防护产品安全技术要求和测试评价方法

Information security technology—Security technical requirements and evaluation approaches for virtualization security products

2018-12-27 发布　　2018-12-27 实施

中华人民共和国公安部　　发 布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　术语和定义 …… 1
3　缩略语 …… 2
4　虚拟化安全防护产品描述 …… 2
4.1　功能概述 …… 2
4.2　工作模式概述 …… 2
5　技术要求 …… 3
5.1　总体说明 …… 3
5.2　功能要求 …… 3
5.3　性能要求 …… 9
5.4　安全保障要求 …… 9
6　测试评价方法 …… 15
6.1　总体说明 …… 15
6.2　功能测试 …… 15
6.3　性能测试 …… 25
6.4　安全保障评估 …… 25
附录A（资料性附录）　测试样本库 …… 32
参考文献 …… 33

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：国家计算机病毒应急处理中心、公安部十一局七处、天津市公安局网络安全保卫总队、趋势科技（中国）有限公司、北京瑞星信息技术有限公司、卡巴斯基技术开发（北京）有限公司、北京启明星辰信息安全技术有限公司、恒安嘉新（北京）科技股份公司、北京安天网络安全技术有限公司、北京天融信科技有限公司。

本标准主要起草人：陈建民、杜振华、张俊兵、陆磊、曹鹏、张韫菁、刘彦、黄一斌、赵晓明、张鑫、冯军亮、王文一、杨人玮、童宁、刘思宇、冷健波、徐雨晴、崔婷婷、赵焕菊、王龑。

信息安全技术
虚拟化安全防护产品安全技术要求和测试评价方法

1 范围

本标准规定了虚拟化安全防护产品的安全功能要求、性能要求、安全保障要求及等级划分要求。

本标准适用于虚拟化安全防护产品的设计、开发及检测。

2 术语和定义

下列术语和定义适用于本文件。

2.1

虚拟化安全防护产品 virtualization security product

为IT虚拟化环境提供安全防护的产品。除了对病毒、网络攻击等传统的网络安全风险以外，能够针对IT虚拟化带来的新型安全风险进行防护，同时产品运行和产品管理更加适应IT虚拟化环境。

2.2

虚拟化环境 virtualization environment

将计算机资源进行抽象后形成的IT环境，这些资源包括操作系统、计算机系统、CPU、内存、硬盘、负载均衡、路由器等，通过虚拟化出来的计算机资源，用户可以像用未虚拟化访问物理资源的形式，来访问虚拟化后的资源。并且这种抽象后的资源，不会受到物力资源配置、地域、实现等因素的影响。

2.3

安全防护虚拟设备 security virtual appliance

以无代理的透明方式在虚拟机上实施安全策略，包括无代理恶意软件防护、无代理防火墙、无代理的IDS/IPS/Web应用防护以及相关的网络安全策略、无代理的系统完整性监控。

2.4

安全防护客户端 security virtual client

以在虚拟机上安装安全防护客户端的方式实施安全策略，包括恶意软件防护、防火墙、IDS/IPS/Web应用防护以及相关的网络安全策略、系统完整性监控。

2.5

安全防护管理平台 security management platform

用于管理部署于用户虚拟化环境中的安全防护虚拟设备以及安全防护客户端，对安全策略进行统一管理和部署，对所有安全事件进行管理。

2.6

病毒检测 virus detection

在虚拟化安全防护产品进行病毒处理时，对于确定的测试环境，能够准确地报出病毒文件和病毒名称，并记录检测结果的处理方式。

2.7

隔离 quarantine

在虚拟化安全防护产品进行病毒处理时，为保留病毒样本以及受感染的用户文件，而采取的将病毒