ICS 03.120.20
A 00
备案号：46945

RB

中华人民共和国认证认可行业标准

RB/T 205—2014

抗拒绝服务系统安全评价规范

Security evaluation specifications for anti-denial-of-service system

2014-08-20 发布　　2015-03-01 实施

中国国家认证认可监督管理委员会　　发 布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 2
4　评价过程 …… 2
4.1　总体说明 …… 2
4.2　评价的主要环节 …… 2
4.3　结果判定 …… 3
5　评价要求 …… 4
5.1　功能要求 …… 4
5.2　安全要求 …… 5
5.3　性能验证要求 …… 7
5.4　保证要求 …… 7
5.5　质量保证能力基本要求 …… 10
5.6　产品一致性检查 …… 11
6　测评要求 …… 11
6.1　总体说明 …… 11
6.2　功能评价 …… 11
6.3　安全性评价 …… 14
6.4　性能评价 …… 18
6.5　保证要求测试 …… 19
参考文献 …… 24

图 1　功能测试环境图 …… 11
图 2　性能检测环境图 …… 18

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家认证认可监督管理委员会提出并归口。

本标准起草单位：中国信息安全认证中心、上海市信息安全测评认证中心、安徽中新软件有限公司。

本标准主要起草人：布宁、陈世翔、刘思蓉、吴迪、严妍、陈清明、李菁、毕强、徐佟海、徐航、储茂阳、王永华等。

引　言

本标准依据GB/T 18336《信息技术　安全技术　信息技术安全性评估准则》，提出了抗拒绝服务系统的功能要求、安全要求、性能验证要求和保证要求等四方面的测评方法。同时，本标准给出了工厂质量保证能力和产品一致性的要求。

GB/T 18336《信息技术　安全技术　信息技术安全性评估准则》是对评估对象(TOE)设计研发和评估安全性的基础性标准，给出了对TOE的信息技术、安全技术和信息安全技术安全评估的通用要求。本标准是参考GB/T 18336，结合抗拒绝服务系统的具体特点，选取GB/T 18336.2安全功能要求中的部分组件作为安全要求的评估内容；选取GB/T 18336.3安全保证要求中EAL2级的全部组件作为保证要求的评估内容。

制定本标准的意义在于，有利于认证机构、检测机构对抗拒绝服务系统进行检测、评估和认证，也有利于企业在抗拒绝服务系统的设计和实现时参照使用。

抗拒绝服务系统安全评价规范

1 范围

本标准规定了抗拒绝服务系统的测评方法，包括功能、安全、性能验证和安全保证要求。

本标准适用于抗拒绝服务系统的测试、评估和认证，抗拒绝服务系统的设计和实现也可参照使用。

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(所有部分) 信息技术 安全技术 信息技术安全性评估准则(ISO/IEC 15408)

GB/T 25069 信息安全技术 术语

3 术语、定义和缩略语

3.1 术语和定义

GB/T 18336 和 GB/T 25069 确立的以及下列术语和定义适用于本文件。

3.1.1

拒绝服务攻击 denial-of-service attack

拒绝服务攻击，即 DoS 攻击。造成拒绝服务的攻击行为被称为拒绝服务攻击。

3.1.2

抗拒绝服务系统 anti-denial-of-service system

对抗拒绝服务攻击的硬件设备或软硬件组合，通过监测和控制进出的数据流，及时发现背景流量中各种类型的拒绝服务攻击行为，对攻击流量进行过滤或旁路，保证正常流量的通过，实现对拒绝服务攻击的防护作用。

3.1.3

吞吐量 throughput

抗拒绝服务系统在不丢包情况下转发数据的能力，一般以所能达到线速的百分比(或称通过速率)来表示。

3.1.4

流量牵引 traffic redirection

通过旁路部署模式将攻击流量和正常流量进行分离，由抗拒绝服务系统来专门抵抗拒绝服务攻击，保证正常流量尽可能的不受到攻击的干扰的过程。

3.1.5

旁路 bypass

通过特定的触发状态(断电或死机)让两个网络不通过网络安全设备的系统，直接物理上导通。

3.1.6

文档审核 document review

文档审核是指认证机构对申请方提交的资料和文档，根据产品技术规范进行审核。