ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1137—2014

信息安全技术
抗拒绝服务攻击产品安全技术要求

Information security technology—Security technical requirements for Anti-DoS attack products

2014-03-10 发布　　2014-03-10 实施

中华人民共和国公安部　发布

目　　次

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、安徽中新软件有限公司、北京神州绿盟信息安全科技股份有限公司、公安部第三研究所。

本标准主要起草人：李毅、张笑笑、赵婷、顾健、俞优、张艳、徐航、储茂阳、周忠。

引　言

本标准详细描述了与抗拒绝服务攻击产品安全环境相关的假设、威胁和组织安全策略，定义了抗拒绝服务攻击产品及其支撑环境的安全目的，通过基本原理论证安全功能要求能够追溯并覆盖产品安全目的，安全目的能够追溯并覆盖安全环境相关的假设、威胁和组织安全策略。

本标准基本级参照了 GB/T 18336.3—2008 中规定的 EAL2 级安全保证要求，增强级在 EAL4 级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

本标准仅给出了抗拒绝服务攻击产品应满足的安全技术要求，但对抗拒绝服务攻击产品的具体技术实现方式、方法等不做要求。

信息安全技术
抗拒绝服务攻击产品安全技术要求

1 范围

本标准规定了抗拒绝服务攻击产品的安全功能要求、安全保证要求及等级划分要求。

本标准适用于抗拒绝服务攻击产品的设计、开发及检测。

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 5271.8—2001 信息技术 词汇 第8部分：安全

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336—2008(所有部分) 信息技术 安全技术 信息技术安全性评估准则

3 术语和定义

GB/T 5271.8—2001、GB 17859—1999 和 GB/T 18336—2008(所有部分)界定的以及下列术语和定义适用于本文件。

3.1

拒绝服务攻击 denial of service attack

一种网络攻击，通过构造特定的网络服务请求，目的在于占用过多的带宽或服务器资源，从而使其他服务请求无法得到正常的响应。

3.2

抗拒绝服务攻击产品 Anti-DoS attack product

对拒绝服务攻击进行识别和拦截，从而减轻其危害程度的产品。

3.3

死亡之 ping 攻击 ping of death attack

通过发送恶意构造的 ICMP 超大报文导致目标服务器崩溃的一种攻击。

3.4

泪滴攻击 tear drop attack

通过发送恶意构造的重叠偏移的数据报文导致目标服务器崩溃的一种攻击。

3.5

UDP 洪水攻击 UDP flood attack

通过发送大量的 UDP 数据报文占用带宽或服务器资源的一种攻击。

3.6

syn 洪水攻击 syn flood attack

通过发送大量的 TCP 握手报文的第一个数据包，导致目标服务器的资源耗尽，无法响应正常的请求的一种攻击。