ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 698—2014
代替 GA/T 698—2007

信息安全技术　信息过滤产品技术要求

**Information security technology—
Technical requirements for information filtering products**

2014-03-24 发布　　2014-03-24 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。

本标准代替 GA/T 698—2007《信息安全技术　信息过滤产品安全功能要求》。与 GA/T 698—2007 相比，主要技术变化如下：

——标准名称改为《信息安全技术　信息过滤产品技术要求》(见封面，2007 年版的封面)；

——增加了缩略语(见第 4 章)；

——增加了信息过滤产品描述(见第 5 章)；

——增加了安全环境，包括假设、威胁和组织安全策略(见第 6 章)；

——增加了安全目的，包括产品安全目的和环境安全目的(见第 7 章)；

——增加了“策略应用范围”的要求(见 8.3)；

——增加了“标识与鉴别”的要求(见 8.4)；

——增加了“远程管理安全”的要求(见 8.9)；

——增加了安全保证要求(见第 9 章)；

——增加了技术要求基本原理，包括安全功能要求基本原理和安全保证要求基本原理(见第 10 章)；

——删除了“网页链接信息过滤”的要求(见 2007 年版的 4.1.5)；

——删除了“搜索引擎信息过滤”的要求(见 2007 年版的 4.1.6)；

——删除了“黑名单、白名单”的要求(见 2007 年版的 4.1.8)；

——删除了“TELNET 信息过滤”、“即时消息信息过滤”和“聊天室信息过滤”的要求(见 2007 年版的 4.4.2、4.4.4、4.4.5)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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、公安部网络安全保卫局、方正信息产业控股有限公司、蓝盾信息安全技术股份有限公司、公安部第三研究所。

本标准主要起草人：顾建新、顾健、陆磊、顾玮、俞优、张奕、吴新丽、杨育斌。

本标准所代替标准的历次版本发布情况为：

——GA/T 698—2007。

引　言

本标准详细描述了与信息过滤产品安全环境相关的假设、威胁和组织安全策略，定义了信息过滤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。

本标准仅给出了信息过滤产品应满足的安全技术要求，但对信息过滤产品的具体技术实现方式、方法等不做要求。

信息安全技术　信息过滤产品技术要求

1　范围

本标准规定了信息过滤产品的安全功能要求、安全保证要求及等级划分要求。

本标准适用于信息过滤产品的设计、开发和检测。

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 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

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB 17859—1999、GB/T 18336—2008(所有部分)和 GB/T 25069—2010 界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

FTP：文件传输协议(File Transfer Protocol)

HTTP：超文本传输协议(Hypertext Transfer Protocol)

IM：即时通讯(Instant Messenger)

IP：因特网协议(Internet Protocol)

MAC：介质访问控制(Media Access Control)

POP3：邮局协议第三版(Post Office Protocol 3)

SMTP：简单邮件传输协议(Simple Mail Transfer Protocol)

TELNET：远程登录(Telecommunication Network)

URL：统一资源定位符(Universal Resource Locator)

5　信息过滤产品描述

本标准中定义的信息过滤产品是指通过分析网络通讯数据，重点对网络上的 HTTP、FTP 和邮件等应用层协议中的一种或者多种进行实时分析，根据预先定义的规则对其内容进行筛选并拦截。

信息过滤产品一般位于访问客户端与目标服务器之间，对过滤策略中定义的流入或流出信息进行控制，并保护信息过滤产品自身及其内部的重要数据。该产品通常以串接或者旁路模式部署在访问客户端所在网络的出口处。