ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 696—2007

信息安全技术
单机防入侵产品安全功能要求

Information security technology—Security functional requirements for products of protecting stand-alone computer from intrusion

2007-05-14 发布　　2007-07-01 实施

中华人民共和国公安部　　发布

前　言

本标准由公安部公共信息网络安全监察局提出。

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。

本标准主要起草人：陆臻、张奕、顾玮、沈亮、赵婷、张岚、顾健。

信息安全技术
单机防入侵产品安全功能要求

1 范围

本标准规定了信息安全技术单机防入侵产品的安全功能要求和保证要求。

本标准适用于信息安全技术单机防入侵产品的生产及检测。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求(idt ISO/IEC 15408-3:1999)

3 术语和定义

下列术语和定义适用于本标准。

3.1

单机防入侵产品 product of protecting and preventing intrusion on stand-alone computer

一个运行于单机上的软件。它可以截取单机上进行的入站和出站 TCP/IP 网络连接尝试，并使用预先定义的规则允许和禁止其连接。

4 单机防入侵产品的安全功能要求

4.1 IP 数据包过滤

依据 TCP/IP 协议中的网络数据包的数据格式约定，每一条匹配规则应由下列要素组成：

a) 数据包方向(连接发起方/接收方)。

b) 远程 IP 地址(任何 IP 地址/指定 IP 地址/指定 IP 地址范围)。

c) 协议的匹配，具体协议至少应包括：

1) ICMP 数据包过滤

根据 ICMP 网络数据包中的类型和代码字段进行设定，当匹配到相同类型和代码字段时则按对应规则中的数据包处理方式进行处理；

2) UDP 数据包过滤

根据 UDP 网络数据包中的本地端口[包括单一端口和(或)端口范围]和(或)远程端口[包括单一端口和(或)端口范围]进行规则匹配；

3) TCP 数据包过滤

根据 TCP 网络数据包中的本地端口[包括单一端口和(或)端口范围]和(或)远程端口[包括单一端口和(或)端口范围]，以及 TCP 数据包的标志位进行规则匹配过滤。

4.2 过滤动作

单机防入侵产品应具有对数据包进行下述过滤动作的能力：

a) 拦截；