编号：MSCTC-GFJ-02

信 息 技 术 个 人 防 火 墙
产 品 安 全 检 验 规 范

公安部计算机信息系统安全产品质量监督检验中心

第一版 第 0 次修订

2003 年 11 月 01 日颁布 2003 年 12 月 01 日实施

前　　言

为了规范全国个人防火墙产品的开发与应用，保障公共信息网络安全，根据公安部公共信息网络安全监察局的要求，本规范对个人防火墙产品提出了安全功能要求和保证要求，作为对其进行检测的依据。

本规范由中华人民共和国公安部公共信息网络安全监察局提出。

本规范起草单位：公安部计算机信息系统安全产品质量监督检验中心。

公安部计算机信息系统安全产品质量监督检验中心负责对本规范的解释、提升和更改。

信息技术个人防火墙产品安全检验规范

1 范围

本规范规定了信息技术–个人防火墙产品的安全功能要求和保证要求。

本规范适用于信息技术-个人防火墙产品的生产及检测。

2 术语和定义

2.1 个人防火墙

个人防火墙是一个位于单台 PC 之上的软件。它可以截取 PC 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。

3 信息技术-个人防火墙产品的安全功能

3.1 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。

3.2 过滤动作

个人防火墙产品应具有对数据包进行下述过滤动作的能力：

a) 拦截；

b) 通行；

c) 继续匹配下一规则。

3.3 安全规则的修订：

a) 用户能选择使用或弃用单机保护防入侵产品提供的安全规则；

b) 用户能根据 3.1 中的格式规定添加、删除、修改自定义安全规则。

3.4 对特定网络攻击数据包的拦截：

a) 个人防火墙产品应具备对于一些特定攻击的抵挡及防御能力；

b) 配合抵御攻击的能力，个人防火墙产品宜具备建立可更新的攻击特征库的能力。

3.5 应用程序网络访问控制

个人防火墙产品的安全功能应能控制每个应用程序使用 Internet 网络权限，对应用程序网络访问控制包括以下三种方式：

a) 允许访问：允许该程序使用网络；

b) 禁止访问：禁止该程序使用网络；

c) 网络访问时询问：当应用程序访问网络时，个人防火墙产品应对其将进行的访问操作向用户提供详细的报告及询问，根据询问结果对应用程序访问网络的行为进行处理。

3.6 网络快速切断/恢复

以快捷的方式切断/恢复所有网络通讯。

3.7 包过滤、网络攻击的日志记录：

a) 应提供一个网络通讯日志，便于用户查阅网络系统近况。日志数据项的内部数据结构定义可参考如下：

通讯日期	8 字节
通讯时间	6 字节
接受/发送/拦截情况	1 字节（三种情况分别用 0、1、2 表示）
对方 IP 地址	12 字节
本机端口	5 字节
对方端口	5 字节
备注	50 字节（受攻击种类或内部通讯程序）

b) 系统应提供日志的清空功能。

c) 日志信息应为人所能理解的。

d) 日志信息应存储在永久性存储介质中。

3.8 网络攻击的报警

根据匹配系统指定规则发现异常网络数据包，个人防火墙产品应以一定方式警告用户，以及提示用户采取哪些措施。

3.9 产品自身安全

a) 个人防火墙产品应能抵御已知手段攻击，保证其正常运行不受影响。

b) 若产品具有屏蔽外部站点的安全功能要求（如控制孩子上网），则其管理控制还需具备基本的身份鉴别功能。

4 个人防火墙产品的保证要求

4.1 交付和运行

4.1.1 交付过程

4.1.1.1 开发者行为元素：

a) 开发者应将把个人防火墙产品及其部分交付给用户的程序文档化；

b) 开发者应使用交付程序。

4.1.1.2 证据元素的内容和表示

交付文档应描述，在给用户方分配个人防火墙产品的版本时，用以维护安全所必需的所有程序。

4.1.2 安装、生成和启动程序

4.1.2.1 开发者行为元素

开发者应将个人防火墙产品安全地安装、生成和启动所必需的程序文档化。

4.1.2.2 证据元素的内容和表示

文档应描述个人防火墙产品安全地安装、生成和启动所必要的步骤。

4.2 指导性文档

4.2.1 管理员指南

4.2.1.1 开发者行为元素

开发者应当提供针对系统管理员的管理员指南。

4.2.1.2 证据的内容和形式元素：

a) 管理员指南应当描述个人防火墙产品管理员可使用的管理功能和接口；

b) 管理员指南应当描述如何以安全的方式管理个人防火墙产品；

c) 管理员指南应当包含在安全处理环境中必须进行控制的功能和权限的警告；

d) 管理员指南应当描述所有与个人防火墙产品的安全运行有关的用户行为的假设；

e) 管理员指南应当描述所有受管理员控制的安全参数，合适时，应指明安全值；

f) 管理员指南应当描述每一种与需要执行的管理功能有关的安全相关事件，包括改变TSF 所控制的实体的安全特性；

g) 管理员指南应当与为评估而提供的其他所有文档保持一致；

h) 管理员指南应当描述与管理员有关的 IT 环境的所有安全要求。

4.2.2 用户指南

4.2.2.1 开发者行为元素

开发者应当提供用户指南。

4.2.2.2　证据的内容和形式元素：

a）　用户指南应该描述个人防火墙产品的非管理用户可用的功能和接口；

b）　用户指南应该描述个人防火墙产品提供的用户可访问的安全功能的用法；

c）　用户指南应该包含受安全处理环境中所控制的用户可访问的功能和权限的警告；

d）　用户指南应该清晰地阐述个人防火墙产品安全运行中用户所必须负的职责，包括有关在个人防火墙产品安全环境阐述中找得到的用户行为的假设；

e）　用户指南应该与为评估而提供的其它所有文档保持一致；

f）　用户指南应该描述与用户有关的 IT 环境的所有安全要求。

5　个人防火墙产品安全技术要求的等级划分

依据信息技术-个人防火墙产品的开发、生产现状及实际应用情况，我们对个人防火墙产品的安全功能要求划分成二个等级。

个人防火墙产品安全技术要求等级划分如表 1 所示。

表 1　　信息技术-个人防火墙产品安全等级划分表

安全功能类	基本要求	增强要求
数据包过滤	√	√
安全规则的修订（a）	√	√
安全规则的修订（b）		√
对特定网络攻击数据包的拦截（a）	√	√
对特定网络攻击数据包的拦截（b）		√
应用程序网络访问控制		√
网络快速切断/恢复		√
包过滤、网络攻击的日志记录	√	√
网络攻击的报警	√	√
产品自身安全	√	√
保证要求	√	√
a　基本要求：为个人防火墙产品的最底安全级别。		

b　增强要求：为进一步提升产品安全功能的附加要求。