ICS 35.020
L04

GA

中华人民共和国公共安全行业标准

GA ×××× — ××××

移 动 终 端 防 火 墙 产 品 测 评 准 则

Testing and evaluation criteria for firewall products of mobile terminal

（试行）

201× −××−×× 发布　　201× −××−×× 实施

中华人民共和国公安部　发 布

前　言

本标准的全部技术内容为强制性。

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：国家计算机病毒应急处理中心、公安部计算机病毒防治产品检验中心、天津市公安局公共信息网络安全监察总队、天津市质量监督检验站第七十站。

本标准主要起草人：陈建民、刘威、曹鹏、杜振华、阚志刚、佟晓强、曹鹏、王琚、黄一斌、李菊。

移动终端防火墙产品测评准则

1 范围

本标准规定了移动终端防火墙产品的受检要求、测试指标要求、测试方法、报告格式及评级方法。

本标准适用于移动终端防火墙产品的检测和评级。

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。

GA 243-2000 计算机病毒防治产品评级准则

GA 849-2009 移动终端病毒防治产品评级准则

3 术语和定义

GA 243-2000、GA 849-2009 中确立的以及下列术语和定义适用于本标准。

3.1

移动终端防火墙 mobile terminal firewall

可以截取移动终端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的软件。

4 缩略语

下列缩略语适用于本标准。

IrDA	Infrared Data Association	红外
MMS	Multimedia Messaging Service	彩信
GPRS	General Packet Radio Service	通用无线分组业务
WLAN	Wireless Lan	无线局域网
CDMA	Code Division Multiple Access	码分多址
IDS	Intrusion Detection System	入侵检测系统
ICMP	Internet Control Messages	网间控制报文协议
IP	Internet Protocol	网际协议
TCP	Transport Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
HTTP	Hypertext Transfer Protocol	超文本传输协议

5 受检要求

5.1 检验周期

检验机构对程序版本发生重大升级或名称发生改变的移动终端防火墙产品应进行检验；同时，可以根据安全威胁的发展情况对移动终端防火墙产品进行专项检验。

5.2 测试用例要求

受检企业应提交其产品检验用的测试用例，提交的测试用例应是近期流行的有效攻击方式。

5.3 资料要求

5.3.1 受检企业应提交产品研发人员的个人简历。

5.3.2　受检企业应提交产品的中文使用说明书。

5.3.3　受检企业应提交核封完整的正式产品。

6　测试指标要求

6.1　测试指标

6.1.1 防火墙保护接入方式

移动终端防火墙产品通过配置后应保护以下接入方式：

a) 移动通信网接入

b) 数据连接线接入

c) 无线局域网接入

d) 蓝牙接入

6.1.2 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：

a) 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；

b) 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；

c) 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。

6.1.3 过滤动作

移动终端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) 支持默认动作。

6.1.4 产品配置

6.1.4.1 安全规则的修订

a) 用户能选择使用或弃用移动终端保护防入侵产品提供的安全规则；

b) 用户能根据6.1.2中的格式规定添加、删除、修改自定义安全规则，并且能够启用/禁止单条规则；

c) 用户能够定义规则优先级。

6.1.4.2应用程序网络访问控制

移动终端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，移动终端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。

6.1.5 对特定网络攻击数据包的拦截

a）移动终端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，移动终端防火墙产品应具备建立可更新的攻击特征库的能力。

6.1.6 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。日志数据项至少应包括日志类型、日期/时间、过滤动作、源/目的地址、目的端口、协议、方向、攻击类型；

b）系统应提供日志的清空功能；

c）系统应提供日志的导出功能；

d）日志信息应存储在永久性存储介质中。

6.1.7 产品自身安全

移动终端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。

7 测试方法

7.1 移动通信网接入

7.1.1 准备工作

a）通过移动终端网络浏览器，利用移动通信网可以正常访问普通 http 网站；

b）清除浏览器缓存。

7.1.2 检测步骤

a）在移动终端防火墙产品中设置安全级别，或者编辑防火墙规则表，目标对端口 80 的 TCP 协议发出包进行拦截；

b）再次通过移动终端网络浏览器，利用 GPRS/CDMA 1X 进行普通 http 网页的浏览。

7.1.3 预期结果

a）目标网页无法打开，网页浏览请求被拦截；

b）移动终端防火墙产品对该事件记录日志。

7.2 数据连接线接入

7.2.1 准备工作

a）通过移动终端网络浏览器，利用数据线连接可以正常访问普通 http 网站；

b）清除浏览器缓存。

7.2.2 检测步骤

a）在移动终端防火墙产品中设置安全级别，或者编辑防火墙规则表，目标对端口 80 的 TCP 协议发出包进行拦截；

b）再次通过移动终端网络浏览器，利用数据连接线进行普通 http 网页的浏览。

7.2.2 预期结果

a）目标网页无法打开，网页浏览请求被拦截；

b）移动终端防火墙产品对该事件记录日志。

7.3 无线局域网接入

7.3.1 ICMP 协议

7.3.1.1 准备工作

a）将移动终端接入无线局域网，并确定自身 IP 地址；

b）将另一电脑接入同一无线局域网内，并确定自身 IP 地址；

c) 利用该电脑，发送 ping 命令至移动终端，可以得到正确回应。

7.3.1.2 检测步骤

a）在移动终端防火墙产品中设置安全级别，或者编辑防火墙规则表，目标对特定 IP（设为上述电脑的 IP 地址）地址来源的 ICMP 协议的接收进行拦截；

b）再次利用电脑向移动终端发送 ping 命令。

7.3.1.3 预期结果

a）移动终端对 ping 命令无反馈；

b）移动终端防火墙产品对该事件记录日志。

7.3.2 TCP/UDP 协议

7.3.2.1 准备工作

a）建立好移动终端的无线局域网连接；

b）清除浏览器缓存。

7.3.2.2 检测步骤

a）编辑防火墙规则表，第一条为对端口 443 的 TCP 协议发出包进行拦截；

b）编辑防火墙规则表，第二条为对端口 80 的 UDP 协议接收包进行通行；

c) 设置防火墙默认动作，对所有进入的连接均拦截，所有发出的连接均通行，删除除以上两条以外的其他所有防火墙规则表；

d) 通过移动终端网络浏览器，利用无线局域网进行普通 http 网页的浏览；

e) 通过发包工具，在无线局域网内对移动终端发送 UDP 端口 80 的数据包；

f) 在无线局域网内，向移动终端发送 ping 命令。

7.3.2.3 预期结果

a）http 网页被拦截，无法打开；

b) UDP 端口 80 数据包可成功到达移动终端；

c) ping 命令被拦截，无法获得反馈；

d) 防火墙日志记录有被拦截的所有通讯内容。

7.4 红外接入

7.4.1 准备工作

a）启动移动终端红外传输功能；

b）通过红外功能，可以将移动终端中的文件传输至另一红外终端。

7.4.2 检测步骤

a）在移动终端中启用红外拦截功能；

b）再次通过红外功能，尝试将移动终端中的文件传输至另一红外终端。

7.4.3 预期结果

a）文件传输失败，红外传输被拦截。

7.5 蓝牙接入

7.5.1 准备工作

a）启动移动终端蓝牙传输功能；

b）通过蓝牙功能，可以将移动终端中的文件传输至另一蓝牙终端。

7.5.2 检测步骤

a）在移动终端中启用蓝牙拦截功能；

b）再次通过蓝牙功能，尝试将移动终端中的文件传输至另一蓝牙终端。

7.5.3 预期结果

a）文件传输失败，蓝牙传输被拦截。

7.6 特定网络攻击拦截

7.6.1 准备工作

a）将移动终端正确接入无线局域网。

7.6.2 检测步骤

a）在防火墙产品中启动防火墙功能，特定网络攻击拦截功能；

b）在无线局域网内，对移动终端进行特定网络攻击。

7.6.3 预期结果

a）特定攻击被拦截，并记录防火墙日志。

7.7 防火墙产品设置

7.7.1 检测步骤

a）进入防火墙产品设置界面；

b）检查默认配置；

c) 用户可以启用或禁用防火墙功能；

d) 用户可以添加，修改，删除安全规则，可以启用或禁用单条规则；

e) 用户可以定义规则的优先级。

7.7.2 预期结果

a）默认配置合理，不影响用户正常使用；

b）可以完成上述配置。

7.8 防火墙产品日志功能

7.8.1 检测步骤

a）通过以上测试步骤获得一定日志内容；

b）检查日志列表和日志详细信息，详细信息包括：日志类型、日期/时间、过滤动作、源/目的地址、目的端口、协议、方向、拦截类型；

c) 用户可以清空日志。

7.8.2 预期结果

a）日志内容正确，并可以被清空。

8 报告格式

8.1 产品检验结果及评分表格式见表 1。

表 1 产品检验结果及评分表

检验项目			检验结果	分数	备注
防火墙保护接入能力（20 分）	是否能够通过配置保护多种数据接入方式	移动通信网接入		5	▲
		数据连接线接入		5	▲
		无线局域网接入		5	▲
		蓝牙接入		5	▲
IP 数据包过滤（30 分）	过滤要素	包含数据包方向		5	▲
		包含远程 IP 地址		5	▲
		包含协议的匹配		5	▲
	协议支持	能否支持 ICMP 数据包过滤		5	▲
		能否支持 TCP 数据包过滤		5	▲
		能否支持 UDP 数据包过滤		5	▲
过滤动作（9 分）	拦截			3	▲
	通行			3	▲
	支持默认动作			3	▲

产品配置（24 分）	安全规则的修订	是否提供默认配置		8	▲
		用户能否添加、删除、修改规则、规则优先级管理		8	▲
		启用/禁止单条规则		2	▲
	能否支持开机启动			4	▲
	应用程序网络访问控制			2	▲
对特定网络攻击数据包拦截（2 分）	是否支持对特定网络攻击数据包的拦截			2	▲
日志记录（10 分）	能否记录过滤、拦截日志			5	▲
	能否管理日志			5	▲
产品自身安全（5 分）	能否抵御已知手段攻击			5	▲
过滤性能	实时监控关闭后文件传输时间				△
	实时监控开启后文件传输时间				△
总分					
注：▲表示此项列入产品评级；　△表示此项不列入产品评级，仅供参考。					

9 评级方法

9.1　按表 1 规定的检验项目对受检产品进行评级。

9.2　受检产品未满足检验项目要求,则该项分值为零，满足检验项目要求,则该项分值按表 1 计算。

9.3　按受检产品所得总分数确定产品的级别，级别划分见表 2。

表 2　级别划分

分值	级别
（71-80）分	一级
（81-90）分	二级
90 分以上	三级