

ICS 35.240

A 90

GF

公安部计算机信息系统安全产品质量监督检验中心检验规范

MSTL_JGF_04-012 0101—2006

信息安全技术 非授权外联监测产品检验规范

2006-01-01 发布

2006-02-01 实施

公安部计算机信息系统安全产品质量监督检验中心 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 产品安全功能要求	1
4.1 非授权外联监测	1
4.2 安全功能	2
4.3 审计功能	2
5 产品安全保证要求	2

前 言

为了规范全国非授权外联监测产品的开发与应用，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，本规范对非授权外联监测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批准。

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。

信息安全技术 非授权外联监测产品检验规范

1 范围

本规范规定了非授权外联监测产品的安全功能要求和安全保证要求。
本规范适用于非授权外联监测产品的开发及检测。

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

3.1 非授权外联监测 unauthorized outward connection monitor

主要监视受保护网络内部主机在安全策略允许之外通过 modem、双网卡、无线设备（如 CDMA、GSM、GPRS、WLAN 等）等非授权途径与外部网络进行连接的产品。

4 产品安全功能要求

4.1 非授权外联监测

4.1.1 内部在线主机扫描

应提供对局域网内部不同网段的所有主机进行扫描的功能，以查询所有在线主机，扫描结果至少应包括主机名、IP 地址。

如果采用的是 C/S 模式，要求能够区分在线主机是否安装客户端。

4.1.2 监测范围

受监测的主机应包括扫描到的所有主机，并且由管理员任意添加主机和网段。

4.1.3 监测非授权外联

能够完全、准确地探测出受监测的内部主机未经授权而联接到外部网络的行为，至少包括 modem、双网卡和一种无线方式。

4.1.4 报警

当监测到有非授权外联行为的主机时，能够通过一定的方式进行报警（比如消息、email 等），至少包括日志记录。

4.1.5 及时性

所有报警要具有及时性。

4.1.6 日志

对所有非授权外联情况进行记录，至少包括以下内容：

- a) 主机名
- b) 主机 IP
- c) 外联方式
- d) 非授权外联的起始和终止时间。

4.1.7 阻断

宜提供阻断功能,当监测到内部主机有非授权外联行为时,阻断其与局域网其它主机间的所有通信,或者阻断其外联行为。

4.2 安全功能

4.2.1 主机型非授权外联监测产品自身保护功能

有防止非授权人员删除和卸载该产品的措施。

如果采用的是 C/S 模式:

- a) 应采取防止非授权用户强行终止非授权外联监测产品运行的措施;
- b) 应采取防止非授权用户强制取消非授权外联监测产品在系统启动时自动加载的措施;
- c) 服务端应对客户端进行鉴别。

4.2.2 管理员身份鉴别

应保证只有授权管理员和可信主机才有权使用产品的管理功能,对授权管理员和可信主机应进行身份鉴别。

4.2.3 管理员权限

- a) 管理员属性修改(更改密码等);
- b) 启动、关闭全部或部分监测功能;
- c) 修改非授权外联监测产品其它安全策略。

4.3 审计功能

4.3.1 审计数据生成

应至少能对下列事件生成日志:

- a) 非授权外联监测产品的启动和关闭;
- b) 鉴别成功和失败;
- c) 其它重要操作,如增加、删除管理员,存档、删除、清空日志等。

应在每一个日志记录中记录事件发生的日期和时间、事件描述。

4.3.2 审计管理

应提供下列日志管理功能:

- a) 只允许授权管理员访问日志记录;
- b) 提供对日志记录的查询功能;
- c) 授权管理员能存档、删除和清空日志记录。

5 产品安全保证要求

保证要求按 GB/T 18336.3—2001 第二级执行。
