GJB

中华人民共和国国家军用标准

FL 0112 GJB 7170-2011

网络安全管理类产品测评方法

Test and evaluation approaches for network security management product

2011-01-20 发布 2011-04-01 实施

中国人民解放军总装备部 批 准

目　次

前言……II
1　范围……1
2　引用文件……1
3　术语和定义……1
4　测试分类与等级划分……1
4.1　测试分类……1
4.2　等级划分……1
5　测试条件与测试环境……1
5.1　测试条件……1
5.2　测试环境……1
6　功能测试……3
6.1　网络拓扑发现……3
6.2　网络管理……4
6.3　终端信息收集……7
6.4　终端管理……8
6.5　终端外设控制……12
6.6　终端网络访问控制……13
6.7　终端操作系统补丁管理……16
6.8　审计……16
6.9　日志管理……17
6.10　产品配置管理……18
7　性能测试……20
7.1　拓扑发现准确性……20
7.2　网络发现速度……20
7.3　网络轮询时间……20
7.4　并发采集进程……21
7.5　安全策略生效时间……21
7.6　稳定性……21
8　安全性测试……22
8.1　客户端安全……22
8.2　管理端安全……23
8.3　通信安全……24
8.4　容错性……25
9　等级评估……25

前　言

本标准由中国人民解放军总参谋部第三部提出。

本标准起草单位：中国人民解放军信息安全测评认证中心、北京启明星辰信息安全技术有限公司。

本标准主要起草人：桂坚勇、荀京京、李智勇、耿振国、唐　扬、董　玮、姚京祥、钟　毅、随　刚、李锦山。

网络安全管理类产品测评方法

1 范围

本标准规定了网络安全管理类产品的测评方法。

本标准适用于军用网络安全管理类产品的测试与评价，网络安全管理类产品的研发、生产和使用可参照本标准执行。

2 引用文件

下列文件中的有关条款通过引用而成为本标准的条款。凡注日期或版次的引用文件，其后的任何修改单（不包含勘误的内容)或修订版本都不适用于本标准，但提倡使用本标准的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件，其最新版本适用于本标准。

GJB 5794－2006 网络入侵检测产品测评方法

3 术语和定义

下列术语和定义适用于本标准。

3.1 网络安全管理类产品 network security management product

通过网络对网络设备、网络安全设备、服务器和终端进行统一集中安全管理的一种产品，可以分为集中安全管理和终端安全管理两大类。

3.2 管理端 management console

授权管理员进行产品配置、策略制定、日志审计等管理操作的特定平台。

4 测试分类与等级划分

4.1 测试分类

测试分为功能测试、性能测试和安全性测试三类。

4.2 等级划分

依据产品功能、性能和安全性的综合测评结果，分为 C、C＋、B、B＋和 A 五个等级，C 级为最低级，A 级为最高级。

5 测试条件与测试环境

5.1 测试条件

产品测试条件见 GJB 5794－2006 中的 4.3。

5.2 测试环境

5.2.1 产品测试环境拓扑图

网络安全管理类产品功能测试环境示意图见图 1。

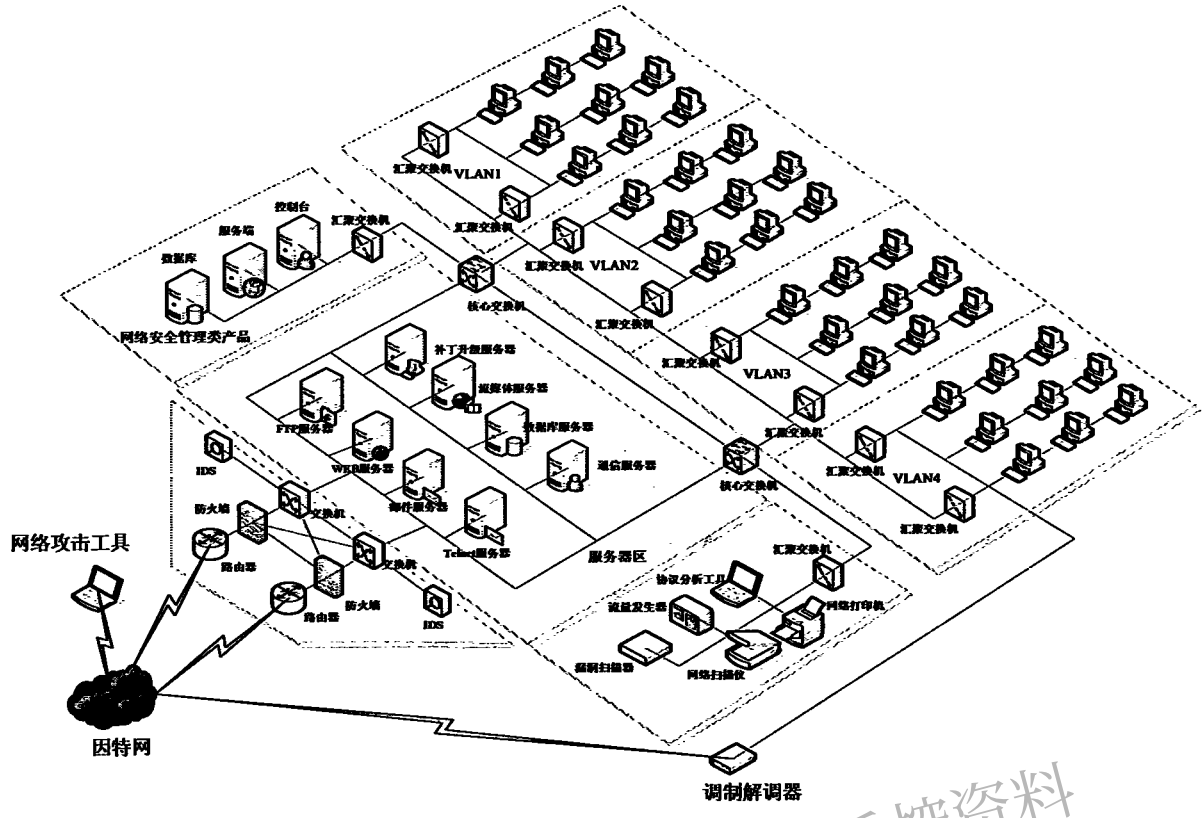

图 1　网络安全管理类产品功能测试环境示意图

5.2.2　典型测试环境说明

典型测试环境说明见表 1。

表 1　典型测试环境说明

类　别	名　　称	数　量	说　　明
硬件	核心交换机	2 台	24 口三层千兆交换机
	汇聚交换机	12 台	16 口二层/三层百兆交换机
	路由器	2 台	百兆/千兆
	防火墙	2 台	百兆/千兆
	IDS	2 台	百兆/千兆
	服务器	5 台	Web 服务器、邮件服务器、FTP 服务器、Telnet 服务器、补丁升级服务器
	终端计算机	36 台	平均分布于 4 个 VLAN 中 预装 Windows 2000/XP/7
	协议分析工具	1 台	支持千兆网络环境 接入核心交换机的镜像端口
	流量发生器	1 台	支持千兆网络环境 接入核心交换机
	漏洞扫描器	1 台	支持千兆网络环境 接入核心交换机
	网络打印机	1 台	
	网络扫描仪	1 台	
	网络攻击工具	1 台	形态：软件/硬件 功能：端口扫描、缓冲区溢出、DDOS 攻击、远程控制等
	调制解调器	1 台	

表 1(续)

类 别	名 称	数 量	说 明
软件	Oracle	1 套	9i/10g
	SQL Server	1 套	2000/2005
	Windows 2000	1 套	
	Windows xp	1 套	
	Windows7	1 套	
	Windows 2000 Server	1 套	
	Windows 2003 Server	1 套	
网络	逻辑区域/网段	5 个	VLAN1（PC 机）、VLAN2（PC 机）、VLAN3（PC 机）、VLAN4（PC 机）、VLAN5（其他区域统一划归一个 VLAN)共 5 个网段，保证各 VLAN 之间路由互通。
	因特网接入环境	1 个	从运营商直接接入的因特网
协议	产品支持的网络协议	1 个以上	IPV4 或 IPV6
	产品支持交换机管理协议	4 个	SNMP，CLI，RMON，SSH
	产品支持路由器管理协议	2 个	CLI、SNMP
	产品支持防火墙管理协议	2 个	SNMP、SSH
	产品支持 IDS 管理协议	2 个	SNMP、SSH

6 功能测试

6.1 网络拓扑发现

6.1.1 自动拓扑发现

6.1.1.1 测试内容

测试集中安全管理产品正确发现网络拓扑结构的能力。

6.1.1.2 测试步骤

测试步骤为：

a) 进行网络拓扑发现的相关设置；

b) 产品生成网络拓扑图。

6.1.1.3 预期结果

预期结果为：

应能查看到产品生成的网络拓扑图。

6.1.1.4 适用等级

C 级以上产品应通过此项测试。

6.1.2 网络拓扑编辑

6.1.2.1 测试内容

测试集中安全管理产品对网络拓扑图内容进行编辑的能力。

6.1.2.2 测试步骤

测试步骤为：

a) 进入网络拓扑图编辑选项；

b) 对网络拓扑图的内容进行增加、修改、删除和存储等操作。

6.1.2.3 预期结果

应能对网络拓扑图的内容进行增加、修改、删除和存储等操作。

6.1.2.4 适用等级

C+级以上产品应通过此项测试。

6.2 网络管理

6.2.1 网络资产管理

6.2.1.1 测试内容

测试集中安全管理产品对网络中资产进行管理的能力。

6.2.1.2 测试步骤

测试步骤为：

a) 增加网络资产并查看结果；

b) 修改网络资产并查看结果；

c) 删除网络资产并查看结果；

d) 根据预定的条件查询某个网络资产。

6.2.1.3 预期结果

预期结果为：

a) 应能成功的增加、修改、删除网络资产；

b) 根据条件查询后，应能正确显示出需要查询的内容。

6.2.1.4 适用等级

C 级以上产品应通过此项测试。

6.2.2 IP 地址管理

6.2.2.1 测试内容

测试终端安全管理产品对终端设备 IP 地址进行管理的能力。

6.2.2.2 测试步骤

测试步骤为：

a) 进入 IP 地址管理选项，设置禁止修改 IP 地址的策略并下发；

b) 显示网络中的已用 IP 地址或未用 IP 地址；

c) 显示的 IP 列表进行导出和打印操作；

d) 在终端修改 IP 地址并查看结果；

e) 进行 arp 欺骗并查看结果。

6.2.2.3 预期结果

预期结果为：

a) 应能正确显示 IP 地址分配使用情况；

b) 应能对 IP 列表进行打印和导出；

c) 在下发了禁止修改 IP 地址策略的情况下，无法修改终端 IP；

d) 无法进行 arp 欺骗。

6.2.2.4 适用等级

C+级以上产品应通过此项测试。

6.2.3 路由器状态监测

6.2.3.1 测试内容

测试集中安全管理产品对网络中路由器的监测能力。

6.2.3.2 测试步骤

测试步骤为：

a) 进行相关设置，对路由器进行状态监测；

b) 查看所监测的状态项内容；

c) 查看监测的状态是否与实际工作状态相符；

d) 查看对路由协议的检测是否与实际工作状态相符。

6.2.3.3 预期结果

预期结果为：

a) 应能对路由器的 PVC 速率、CPU 利用率、内存使用率和端口状态等情况进行监测；

b) 监测状态与实际工作状态一致；

c) 对路由协议的检测结果与实际工作状态一致。

6.2.3.4 适用等级

C＋级以上产品应通过此项测试。

6.2.4 交换机状态监测

6.2.4.1 测试内容

测试集中安全管理产品对网络中交换机的监测能力。

6.2.4.2 测试步骤

测试步骤为：

a) 进行相关设置，对交换机进行状态监测；

b) 查看所监测的状态项内容；

c) 查看监测的状态是否与实际工作状态相符。

6.2.4.3 预期结果

预期结果为：

a) 应能对交换机的 CPU 利用率、内存使用率和端口状态等情况进行监测；

b) 监测状态与实际工作状态一致。

6.2.4.4 适用等级

C＋级以上产品应通过此项测试。

6.2.5 安全设备状态监测

6.2.5.1 测试内容

测试集中安全管理产品对网络中安全设备的监测能力。

6.2.5.2 测试步骤

测试步骤为：

a) 进行相关设置，对安全设备进行状态监测；

b) 查看防火墙状态监测的内容是否与实际工作状态一致；

c) 查看入侵检测系统状态监测的内容是否与实际工作状态一致。

6.2.5.3 预期结果

预期结果为：

a) 能够对安全设备的状态进行监测；

b) 监测到的防火墙状态与实际工作状态一致；

c) 监测到的入侵检测系统状态与实际工作状态一致。

6.2.5.4 适用等级

B 级以上产品应通过此项测试。

6.2.6 终端状态监测

6.2.6.1 测试内容

测试集中安全管理产品对终端的监测能力。

6.2.6.2 测试步骤

测试步骤为：

a) 进行相关设置，对终端进行状态监测；

b) 查看所监测的状态项内容；

c) 查看监测的状态是否与实际工作状态相符。

6.2.6.3 预期结果

预期结果为：

a) 应能对终端的 CPU 利用率、内存使用率、磁盘使用率和端口状态等情况进行监测；

b) 监测状态与实际工作状态一致。

6.2.6.4 适用等级

C+级以上产品应通过此项测试。

6.2.7 其他设备监测

6.2.7.1 测试内容

测试集中安全管理产品对网络中其他设备（例如网络打印机、网络扫描仪等）的监测能力。

6.2.7.2 测试步骤

测试步骤为：

a) 进行相关设置，对其他设备进行状态监测；

b) 查看所监测的状态项内容；

c) 查看监测的状态是否与实际工作状态相符。

6.2.7.3 预期结果

预期结果为：

a) 应能对其他设备的工作状态进行监测；

b) 监测状态与实际工作状态一致。

6.2.7.4 适用等级

C+级以上产品应通过此项测试。

6.2.8 网络流量监测

6.2.8.1 测试内容

测试集中安全管理产品对网络流量进行实时监测的能力。

6.2.8.2 测试步骤

测试步骤为：

a) 进行网络流量监测的相关设置；

b) 开始监测网络对象端口流量；

c) 查看监测结果与实际流量是否一致。

6.2.8.3 预期结果

预期结果为：

a) 应能对网络对象端口的流量进行监测；

b) 监测到的流量与实际流量一致。

6.2.8.4 适用等级

B 级以上产品应通过此项测试。

6.2.9 日志集中管理

6.2.9.1 测试内容

测试集中安全管理产品对设备的日志信息进行采集和管理的能力。

6.2.9.2 测试步骤

测试步骤为：

a) 对指定设备进行日志采集；

b) 对采集的日志进行查询、分类、分析和输出等管理操作。

6.2.9.3 预期结果

预期结果为：

a) 应能采集指定设备的日志；

b) 应能对采集的日志进行查询、分类、分析和输出等管理操作。

6.2.9.4 适用等级

C+级以上产品应通过此项测试。

6.2.10 综合分析

6.2.10.1 测试内容

测试集中安全管理产品对网络运行状况和网络安全事件等进行关联分析的能力。

6.2.10.2 测试步骤

测试步骤为：

a) 进行关联分析的相关策略设置；

b) 开始对采集到的网络流量、网络设备工作状态和网络安全事件等数据进行关联分析；

c) 查看分析结果。

6.2.10.3 预期结果

预期结果为：

a) 具备关联分析策略模板；

b) 应能依据关联分析策略模板分析出网络异常流量、网络异常行为和网络安全态势；

c) 分析结果应包括图、表等形式。

6.2.10.4 适用等级

B+级以上产品应通过此项测试。

6.3 终端信息收集

6.3.1 系统信息

6.3.1.1 测试内容

测试终端安全管理产品对终端信息进行自动收集的能力。

6.3.1.2 测试步骤

测试步骤为：

a) 登录终端安全管理产品的管理端，查看收集到的终端信息；

b) 登录终端上查看相同的项目；

c) 将二者的结果进行比对。

6.3.1.3 预期结果

预期结果为：

a) 终端安全管理产品应能收集到终端信息包括操作产品版本、产品运行的进程、产品开放的服务和端口等；

b) 终端安全管理产品应能收集到终端 CPU 主频、内存容量、硬盘容量及外设情况；

c) 与终端显示的信息完全一致。

6.3.1.4 适用等级

C 级以上产品应通过此项测试。

6.3.2 安全事件日志

6.3.2.1 测试内容

测试终端安全管理产品自动收集终端安全事件日志信息的能力。

6.3.2.2 测试步骤

测试步骤为：

a) 在管理端查看收集到的终端日志信息；
b) 登录终端上查看相同的项目；
c) 将二者的结果进行比对。

6.3.2.3 预期结果

预期结果为：
a) 终端安全管理产品应能收集到终端的安全事件日志信息；
b) 与终端显示的安全事件日志信息完全一致。

6.3.2.4 适用等级

C+级以上产品应通过此项测试。

6.3.3 网络连接状态

6.3.3.1 测试内容

测试终端安全管理产品自动收集终端网卡信息和网络连接情况的能力。

6.3.3.2 测试步骤

测试步骤为：
a) 在管理端查看终端的网卡信息；
b) 在管理端查看终端的网络连接状态；
c) 登录终端上查看相同的项目；
d) 将二者的结果进行比对。

6.3.3.3 预期结果

预期结果为：
a) 管理端应能收集到终端的网卡信息，包括 IP 和 MAC 地址等；
b) 管理端应能收集到终端的网络连接状态信息；
c) 与终端显示的信息完全一致。

6.3.3.4 适用等级

C+级以上产品应通过此项测试。

6.4 终端管理

6.4.1 登录管理

6.4.1.1 测试内容

测试终端安全管理产品对终端的登录方式进行管理的能力。

6.4.1.2 测试步骤

测试步骤为：
a) 安装终端软件；
b) 登录终端管理产品的管理端添加或查找安装有终端软件的主机；
c) 添加终端的登录用户名和密码；
d) 查看终端的登录方式。

6.4.1.3 预期结果

预期结果为：

终端的登录采用自主设计的身份认证方式来实现，包括口令认证和智能卡认证等方式。

6.4.1.4 适用等级

B 级以上产品应通过此项测试。

6.4.2 钥匙的唯一性

6.4.2.1 测试内容

测试终端安全管理产品对每个终端分发钥匙的唯一性。

6.4.2.2 测试步骤

测试步骤为：

a) 登录管理端，针对不同的终端制作不同的钥匙；

b) 任选择两台终端，选择其中一台终端；

c) 使用本机钥匙登录终端，使用另一个钥匙登录终端；

d) 查看登录结果。

6.4.2.3 预期结果

管理端分发的钥匙应与终端一一对应。

6.4.2.4 适用等级

B 级以上产品应通过此项测试。

6.4.3 钥匙管理

6.4.3.1 测试内容

测试终端安全管理产品对钥匙的管理能力。

6.4.3.2 测试步骤

测试步骤为：

a) 管理端依据用户身份制作并下发钥匙并查看结果；

b) 管理端对已下发的钥匙进行锁定和解锁并查看结果；

c) 管理端对已下发的钥匙进行注销并查看结果。

6.4.3.3 预期结果

预期结果为：

a) 管理端应能依据用户身份制作并下发钥匙；

b) 管理端应能对已下发的钥匙进行锁定和解锁；

c) 管理端应能对已下发的钥匙进行注销。

6.4.3.4 适用等级

B 级以上产品应通过此项测试。

6.4.4 进程管理

6.4.4.1 测试内容

测试终端安全管理产品对终端进程进行管理的能力。

6.4.4.2 测试步骤

测试步骤为：

a) 在管理端打开/关闭选定终端的某个进程；

b) 在选定终端上查看该进程状态。

6.4.4.3 预期结果

预期结果为：

在管理端应能对终端的进程进行管理和控制。

6.4.4.4 适用等级

C+级以上产品应通过此项测试。

6.4.5 用户/组管理

6.4.5.1 测试内容

测试终端安全管理产品对终端的用户组和用户进行管理的能力。

6.4.5.2 测试步骤

测试步骤为：

a) 在管理端对选定终端的用户和用户组进行增加、修改和删除等操作；

b) 在管理端对选定终端的用户和用户组属性进行修改；

c) 在选定终端查看操作结果。

6.4.5.3 预期结果

预期结果为：

a) 应能在管理端对选定终端的用户和用户组进行增加、修改和删除等操作；

b) 应能在管理端对选定终端的用户和用户组属性进行修改。

6.4.5.4 适用等级

C+级以上产品应通过此项测试。

6.4.6 共享管理

6.4.6.1 测试内容

测试终端安全管理产品对终端共享进行管理的能力。

6.4.6.2 测试步骤

测试步骤为：

a) 在管理端对选定终端的共享进行增加和删除等操作；

b) 在选定终端查看操作结果。

6.4.6.3 预期结果

预期结果为：

应能在管理端对选定终端的共享进行增加和删除等操作。

6.4.6.4 适用等级

C+级以上产品应通过此项测试。

6.4.7 锁屏管理

6.4.7.1 测试内容

测试终端安全管理产品对终端的锁屏管理能力。

6.4.7.2 测试步骤

测试步骤为：

a) 在终端插入钥匙，登录产品；

b) 拔掉钥匙查看计算机是否被锁屏；

c) 在登录界面中输入用户名和口令后登录产品；

d) 重新插入钥匙，登录产品。

6.4.7.3 预期结果

预期结果为：

a) 拔掉钥匙后终端锁屏；

b) 在未插入钥匙时，用户无法登录产品；

c) 插入钥匙后，用户正常登录产品。

6.4.7.4 适用等级

C+级以上产品应通过此项测试。

6.4.8 服务管理

6.4.8.1 测试内容

测试终端安全管理产品对终端运行服务进行管理的能力。

6.4.8.2 测试步骤

测试步骤为：

a) 在管理端对选定终端的服务进行启动、关闭和禁用等操作；

b) 在选定终端查看操作结果。

6.4.8.3 预期结果

预期结果为：

应能在管理端对选定终端的服务进行启动、关闭和禁用等操作。

6.4.8.4 适用等级

C+级以上产品应通过此项测试。

6.4.9 注册表保护

6.4.9.1 测试内容

测试终端安全管理产品对终端注册表进行保护的能力。

6.4.9.2 测试步骤

测试步骤为：

a) 在管理端对选定终端下发注册表保护策略；

b) 在选定终端对注册表的键值进行增加、修改和删除操作；

c) 重启选定终端并查看操作结果。

6.4.9.3 预期结果

预期结果为：

用户无法修改选定终端的注册表内容。

6.4.9.4 适用等级

B+级以上产品应通过此项测试。

6.4.10 嗅探发现

6.4.10.1 测试内容

测试终端安全管理产品自动发现终端嗅探行为的能力。

6.4.10.2 测试步骤

测试步骤为：

a) 在终端安装并运行网络嗅探器；

b) 在管理端查看是否能够捕获到该终端的嗅探行为。

6.4.10.3 预期结果

预期结果为：

产品应能自动发现终端的嗅探行为。

6.4.10.4 适用等级

A 级产品应通过此项测试。

6.4.11 远程信息发送

6.4.11.1 测试内容

测试终端安全管理产品对终端发送消息的能力。

6.4.11.2 测试步骤

测试步骤为：

a) 在管理端向某个终端发送一条消息；

b) 在该终端查看是否正确接收到该消息。

6.4.11.3 预期结果

终端应能正确的接收到管理端发出的消息。

6.4.11.4 适用等级

C+级以上产品应通过此项测试。

6.4.12 主机防火墙

6.4.12.1 测试内容

测试终端安全管理产品具备对终端应用程序访问网络连接状态和端口进行保存，当发现有异常程序访问网络时能够作出相应的处理。

6.4.12.2 测试步骤

测试步骤为：

a) 在管理端对指定终端下发基于进程、地址、端口等的防火墙策略；

b) 在终端上进行违反下发策略的网络访问；

c) 通过网络对该终端实施攻击性扫描；

d) 查看结果。

6.4.12.3 预期结果

预期结果为：

a) 终端应能依据防火墙策略对用户的违规操作进行阻断；

b) 可以阻断攻击性扫描，并向管理端报警。

6.4.12.4 适用等级

B+级以上产品应通过此项测试。

6.5 终端外设控制

6.5.1 键盘鼠标控制

6.5.1.1 测试内容

测试终端安全管理产品是否能对终端的鼠标和键盘进行控制。

6.5.1.2 测试步骤

测试步骤为：

a) 在管理端设置策略，启用/禁用键盘鼠标；

b) 在终端查看结果。

6.5.1.3 预期结果

预期结果为：

终端应能依据设定策略控制使用键盘和鼠标。

6.5.1.4 适用等级

C 级以上产品应通过此项测试。

6.5.2 光驱/软驱控制

6.5.2.1 测试内容

测试终端安全管理产品是否能对终端的光驱和软驱进行控制。

6.5.2.2 测试步骤

测试步骤为：

a) 在管理端设置策略，启用/禁用光驱和软驱；

b) 在终端查看结果。

6.5.2.3 预期结果

预期结果为：

终端应能依据设定策略控制使用光驱和软驱。

6.5.2.4 适用等级

C 级以上产品应通过此项测试。

6.5.3 串口并口控制

6.5.3.1 测试内容

测试终端安全管理产品是否能对终端的串口和并口进行控制。

6.5.3.2 测试步骤

测试步骤为：

a） 在管理端设置策略，启用/禁用串口和并口；

b） 在终端查看结果。

6.5.3.3 预期结果

预期结果为：

终端应能依据设定策略控制使用串口和并口。

6.5.3.4 适用等级

C 级以上产品应通过此项测试。

6.5.4 USB 接口控制

6.5.4.1 测试内容

测试终端安全管理产品是否能对终端的 USB 接口的使用进行控制。

6.5.4.2 测试步骤

测试步骤为：

a） 在管理端设置策略，启用/禁用 USB 接口；

b） 在终端查看结果。

6.5.4.3 预期结果

预期结果为：

终端应能依据设定策略控制使用 USB 接口。

6.5.4.4 适用等级

C 级以上产品应通过此项测试。

6.5.5 其他接口控制

6.5.5.1 测试内容

测试终端安全管理产品是否能对终端的 1394、红外和蓝牙等接口进行控制。

6.5.5.2 测试步骤

测试步骤为：

a） 在管理端设置策略，启用/禁用 1394、红外和蓝牙等接口；

b） 在终端查看结果。

6.5.5.3 预期结果

预期结果为：

终端应能依据设定策略控制使用 1394、红外和蓝牙等接口。

6.5.5.4 适用等级

C＋级以上产品应通过此项测试。

6.6 终端网络访问控制

6.6.1 WEB 地址控制

6.6.1.1 测试内容

测试终端安全管理产品对终端访问的 URL 地址进行控制的能力。

6.6.1.2 测试步骤

测试步骤为：

a） 在管理端设置策略，禁止访问设定网址；

b） 在终端上分别输入设定网址，是否能正确获取到网页。

6.6.1.3 预期结果

预期结果为：

应能依据策略禁止访问设定网址。

6.6.1.4 适用等级

B 级以上产品应通过此项测试。

6.6.2 邮件收发控制

6.6.2.1 测试内容

测试终端安全管理产品对终端收发邮件进行控制的能力。

6.6.2.2 测试步骤

测试步骤为：

a) 在管理端设置策略，禁止终端收发邮件；

b) 在终端上收发邮件并查看结果。

6.6.2.3 预期结果

预期结果为：

应能依据策略禁止收发邮件。

6.6.2.4 适用等级

B 级以上产品应通过此项测试。

6.6.3 FTP 访问控制

6.6.3.1 测试内容

测试终端安全管理产品对终端 FTP 访问进行控制的能力。

6.6.3.2 测试步骤

测试步骤为：

a) 在管理端设置策略，禁止终端使用 FTP 上传下载文件；

b) 在终端上使用 FTP 上传下载文件并查看结果。

6.6.3.3 预期结果

预期结果为：

应能依据策略禁用 FTP。

6.6.3.4 适用等级

B 级以上产品应通过此项测试。

6.6.4 TELNET 访问控制

6.6.4.1 测试内容

测试终端安全管理产品对终端 TELNET 访问进行控制的能力。

6.6.4.2 测试步骤

测试步骤为：

a) 在管理端设置策略，禁止终端使用 TELNET 访问；

b) 在终端上使用 TELNET 远程登录并查看结果。

6.6.4.3 预期结果

预期结果为：

应能依据策略禁用 TELNET。

6.6.4.4 适用等级

B 级以上产品应通过此项测试。

6.6.5 邮件内容监控

6.6.5.1 测试内容

测试终端安全管理产品对终端收发邮件的内容进行监控的能力。

6.6.5.2 测试步骤

测试步骤为：

a) 在管理端对指定终端下发邮件内容控制策略；

b) 在终端收发带有关键字的邮件并查看结果。

6.6.5.3 预期结果

预期结果为：

终端依据策略无法收发携带关键字的邮件。

6.6.5.4 适用等级

A 级产品应通过此项测试。

6.6.6 网络打印控制

6.6.6.1 测试内容

测试终端安全管理产品是否能对终端的打印功能进行控制。

6.6.6.2 测试步骤

测试步骤为：

a) 在管理端对选定终端下发禁止打印的策略；

b) 终端进行打印操作。

6.6.6.3 预期结果

预期结果为：

终端依据策略无法进行打印操作。

6.6.6.4 适用等级

C+级以上产品应通过此项测试。

6.6.7 外联控制

6.6.7.1 测试内容

测试终端安全管理产品对终端外联行为进行控制的能力。

6.6.7.2 测试步骤

测试步骤为：

a) 在管理端对选定终端下发禁止外联的策略；

b) 在选定终端进行外联操作并查看结果。

6.6.7.3 预期结果

预期结果为：

终端依据策略无法进行外联操作。

6.6.7.4 适用等级

C 级以上产品应通过此项测试。

6.6.8 接入控制

6.6.8.1 测试内容

测试终端安全管理产品对终端接入网络行为进行控制的能力。

6.6.8.2 测试步骤

测试步骤为：

a) 在管理端设定接入控制的策略；

b) 将违反策略的终端接入网络并查看结果。

6.6.8.3 预期结果

预期结果为：

违反策略的终端无法访问网络。

6.6.8.4 适用等级

C 级以上产品应通过此项测试。

6.7 终端操作系统补丁管理

6.7.1 操作系统补丁检查

6.7.1.1 测试内容

测试终端安全管理产品对终端的操作系统补丁安装情况进行检查的能力。

6.7.1.2 测试步骤

测试步骤为：

a) 在管理端对选定终端，查看该终端操作系统补丁安装情况；

b) 在终端查看操作系统补丁安装情况；

c) 将上述结果进行对比。

6.7.1.3 预期结果

管理端应能正确显示终端操作系统补丁安装情况。

6.7.1.4 适用等级

C+级以上产品应通过此项测试。

6.7.2 操作系统补丁分发

6.7.2.1 测试内容

测试终端安全管理产品对终端进行操作系统补丁更新的能力。

6.7.2.2 测试步骤

测试步骤为：

a) 在管理端向指定终端下发操作系统补丁自动更新策略；

b) 在终端查看操作系统补丁安装情况。

6.7.2.3 预期结果

终端应能依据管理端下发的策略自动更新操作系统补丁。

6.7.2.4 适用等级

B 级以上产品应通过此项测试。

6.8 审计

6.8.1 告警信息审计

6.8.1.1 测试内容

产品是否具备对监控对象的告警信息进行审计的能力。

6.8.1.2 测试步骤

测试步骤为:

a) 选择告警信息审计；

b) 选择相应的监控对象查看审计结果。

6.8.1.3 预期结果

预期结果为：

应能根据预先设置的审计策略显示监控对象相关的告警信息。

6.8.1.4 适用等级

C+级以上产品应通过此项测试。

6.8.2 历史事件审计

6.8.2.1 测试内容

产品是否具备对监控对象的历史事件进行审计的能力。

6.8.2.2 测试步骤

测试步骤为：

a) 选择历史事件审计项；

b) 选择相应的监控对象查看审计结果。

6.8.2.3 预期结果

预期结果为：

应能根据预先设置的审计策略显示监控对象相关的历史事件。

6.8.2.4 适用等级

C+级以上产品应通过此项测试。

6.9 日志管理

6.9.1 日志生成

6.9.1.1 测试内容

检测终端安全管理产品对管理员操作进行日志记录的能力。

6.9.1.2 测试步骤

测试步骤为：

a) 进入日志管理界面；

b) 查看管理员操作日志。

6.9.1.3 预期结果

预期结果为：

应能对管理员操作进行日志记录。

6.9.1.4 适用等级

C 级以上产品应通过此项测试。

6.9.2 日志完整性

6.9.2.1 测试内容

检测终端管理产品所有的日志记录是否具备相关要素。

6.9.2.2 测试步骤

测试步骤为：

a) 进入日志管理界面；

b) 查看日志记录是否包括对象、时间、事件等要素。

6.9.2.3 预期结果

日志内容记录正确，要素完整，清晰易懂。

6.9.2.4 适用等级

C 级以上产品应通过此项测试。

6.9.3 授权访问日志记录

6.9.3.1 测试内容

测试终端安全管理产品日志记录的授权访问。

6.9.3.2 测试步骤

测试步骤为：

a) 审计管理员登录产品，查询日志记录；

b) 非授权的人员登录产品，查询日志记录。

6.9.3.3 预期结果

只有特定授权的审计管理员才能访问日志记录。

6.9.3.4 适用等级

C 级以上产品应通过此项测试。

6.9.4 日志报表

6.9.4.1 测试内容

测试终端安全管理产品的日志报表功能。

6.9.4.2 测试步骤

测试步骤为：

a) 在管理端依据日志记录的内容生成相关的报表；

b) 输出日志报表；

c) 查看日志报表的完整性和准确性。

6.9.4.3 预期结果

预期结果为：

a) 能够依据日志记录的内容生成相关报表；

b) 支持报表输出功能；

c) 日志报表内容准确完整。

6.9.4.4 适用等级

C+级以上产品应通过此项测试。

6.9.5 日志维护

6.9.5.1 测试内容

测试终端安全管理产品对日志的维护功能。

6.9.5.2 测试步骤

测试步骤为：

在管理端备份、清空和恢复日志记录并查看结果。

6.9.5.3 预期结果

预期结果为：

在管理端应能进行日志记录的备份、清空和恢复等操作。

6.9.5.4 适用等级

C+级以上产品应通过此项测试。

6.10 产品配置管理

6.10.1 策略管理

6.10.1.1 测试内容

测试终端安全管理产品对策略管理的能力。

6.10.1.2 测试步骤

测试步骤为：

a) 增加、修改和删除产品策略；

b) 设定策略执行方式，包括在线策略和离线策略；

c) 下发策略并查看结果。

6.10.1.3 预期结果

预期结果为：

a) 具备策略编辑功能；

b) 终端应能依据设定的策略执行方式执行在线和离线策略。

6.10.1.4 适用等级

C+级以上产品应通过此项测试。

6.10.2 策略备份与恢复

6.10.2.1 测试内容

测试终端安全管理产品对策略进行备份与恢复的能力。

6.10.2.2 测试步骤

测试步骤为：

a) 设置产品策略；

b) 进行策略备份并查看结果；

c) 进行策略恢复并查看结果。

6.10.2.3 预期结果

预期结果为：

应能正确进行策略备份与恢复。

6.10.2.4 适用等级

C+级以上产品应通过此项测试。

6.10.3 用户管理

6.10.3.1 测试内容

测试终端安全管理产品对用户的管理能力。

6.10.3.2 测试步骤

测试步骤为：

a) 以产品管理员身份登录产品；

b) 添加新用户，分别赋予不同用户拥有不同权限；

c) 退出产品后，以上述不同用户身份登录产品后，查看其拥有的权限。

6.10.3.3 预期结果

预期结果为：

用户登录产品后进行的操作应与管理员赋予的权限一致。

6.10.3.4 适用等级

C 级以上产品应通过此项测试。

6.10.4 口令强度管理

6.10.4.1 测试内容

测试产品对口令强度的要求。

6.10.4.2 测试步骤

测试步骤为：

a) 设置不符合口令策略的简单口令并查看结果；

b) 设置符合口令策略的复杂口令并查看结果。

6.10.4.3 预期结果

预期结果为：

不符合口令策略的简单口令不允许被设置。

6.10.4.4 适用等级

C 级以上产品应通过此项测试。

6.10.5 产品化程度

6.10.5.1 测试内容

测试产品的产品化程度。

6.10.5.2 测试步骤

测试步骤为：

a) 检查产品的在线帮助和产品提供开发商技术支持的接口；

b) 向相关技术人员提出问题进行考查。

6.10.5.3 预期结果

预期结果为：

a) 产品有在线帮助，对产品的全程使用具有明确的指导；

b) 产品提供开发商技术支持，例如电话、电子邮件或网站等，并对测试员提出的问题正确解答。

6.10.5.4 适用等级

C 级以上产品应通过此项测试。

7 性能测试

7.1 拓扑发现准确性

7.1.1 测试内容

测试集中安全管理产品发现全网拓扑结构的准确性。

7.1.2 测试步骤

测试步骤为：

a) 在一个网段内进行网络拓扑结构发现；

b) 查看发现结果和实际网络拓扑结构是否一致。

7.1.3 预期结果

预期结果为：

拓扑发现的结果与实际网络拓扑结构一致。

7.1.4 适用等级

C＋级以上产品应通过此项测试。

7.2 网络发现速度

7.2.1 测试内容

测试集中安全管理产品发现全网拓扑结构所用时间。

7.2.2 测试步骤

测试步骤为：

a) 进行网络拓扑结构发现；

b) 计算发现全网拓扑结构所用时间。

7.2.3 预期结果

预期结果为：

a) 网络节点在 1000 以下，发现时间应少于 1200s；

b) 网络节点在 5000 以下，发现时间应少于 3600s。

7.2.4 适用等级

C＋级以上产品应通过此项测试。

7.3 网络轮询时间

7.3.1 测试内容

测试集中安全管理产品对网络中新设备的接入和下线的轮询时间。

7.3.2 测试步骤

测试步骤为：

a) 对新接入的设备进行查询；

b) 对下线的设备进行查询；

c) 统计查询所用时间。

7.3.3 预期结果

预期结果为：

a) 新设备的接入查询时间应低于 600s；

b) 已接入设备下线查询时间应低于 120s。

7.3.4 适用等级

C+级以上产品应通过此项测试。

7.4 并发采集进程

7.4.1 测试内容

测试集中安全管理产品采集网络信息的并发数。

7.4.2 测试步骤

测试步骤为：

a) 开始采集网络信息；

b) 测试产品的并发数。

7.4.3 预期结果

预期结果为：

a) 200 个节点以下的网络，并发进程数应不小于 5；

b) 200—500 个节点以下的网络，并发进程数应不小于 10；

c) 1000 个节点以下的网络，并发进程数应不小于 20。

7.4.4 适用等级

A 级产品应通过此项测试。

7.5 安全策略生效时间

7.5.1 测试内容

测试终端安全管理产品下发的安全策略生效时间。

7.5.2 测试步骤

测试步骤为：

a) 对指定终端下发安全策略；

b) 指定终端进行违规操作；

c) 统计策略生效时间。

7.5.3 预期结果

预期结果为：

指定终端对安全策略生效时间应低于 30s。

7.5.4 适用等级

C 级以上产品应通过此项测试。

7.6 稳定性

7.6.1 测试内容

测试产品的稳定运行能力。

7.6.2 测试步骤

测试步骤为：

a) 在工作状态下连续运行 168h 以上；

b) 查看故障情况。

7.6.3 预期结果

预期结果为：

在指定时间内无故障发生。

7.6.4 适用等级

C 级以上产品应通过此项测试。

8 安全性测试

8.1 客户端安全

8.1.1 进程保护

8.1.1.1 测试内容

测试安装在终端上的客户端程序进程具备自我保护的能力。

8.1.1.2 测试步骤

测试步骤为：

a) 在终端上尝试利用任务管理器结束客户端程序进程并查看结果；

b) 在终端上尝试利用专用工具结束客户端程序进程并查看结果。

8.1.1.3 预期结果

预期结果为：

a) 客户端程序进程不能被任务管理器结束；

b) 客户端程序进程不能被专用工具结束。

8.1.1.4 适用等级

预期结果中的a)适用于C+级以上产品，预期结果中的b)适用于B级以上产品。

8.1.2 文件保护

8.1.2.1 测试内容

测试安装在终端上的客户端程序文件具备自我保护的能力。

8.1.2.2 测试步骤

测试步骤为：

在终端上尝试删除已安装的客户端程序文件并查看结果。

8.1.2.3 预期结果

预期结果为：

已安装的客户端程序文件不能被删除。

8.1.2.4 适用等级

B级以上产品应通过此项测试。

8.1.3 注册表保护

8.1.3.1 测试内容

测试安装在终端上的客户端程序注册表项具备自我保护的能力。

8.1.3.2 测试步骤

测试步骤为：

在终端上尝试修改或删除客户端程序的注册表项并查看结果。

8.1.3.3 预期结果

预期结果为：

客户端程序的注册表项不能被修改或删除。

8.1.3.4 适用等级

B+级以上产品应通过此项测试。

8.1.4 安全卸载

8.1.4.1 测试内容

测试安装在终端上的客户端程序仅能在授权下卸载。

8.1.4.2 测试步骤

测试步骤为：

a) 未经管理端授权，尝试卸载已安装的客户端程序并查看结果；

b) 经管理端授权，尝试卸载已安装的客户端程序并查看结果；

c) 重新安装客户端程序并查看结果。

8.1.4.3 预期结果

预期结果为：

a) 终端上的客户端程序仅能在授权下卸载；

b) 客户端程序卸载并重新安装后正常运行。

8.1.4.4 适用等级

B 级以上产品应通过此项测试。

8.2 管理端安全

8.2.1 安全风险引入

8.2.1.1 测试内容

测试安装服务端程序的主机存在的安全漏洞。

8.2.1.2 测试步骤

测试步骤为：

a) 使用安全扫描器对未安装服务端软件的主机进行扫描；

b) 在该主机上安装服务端软件；

c) 使用安全扫描器对该主机进行扫描；

d) 查看扫描结果。

8.2.1.3 预期结果

预期结果为：

不应在安装服务端软件后给主机带来新的安全风险。

8.2.1.4 适用等级

B 级以上产品应通过此项测试。

8.2.2 服务器安全

8.2.2.1 测试内容

测试硬件形态产品中提供的服务器存在的安全漏洞。

8.2.2.2 测试步骤

测试步骤为：

使用网络扫描器对服务器进行脆弱性扫描。

8.2.2.3 预期结果

预期结果为：

服务器不存在高、中风险安全漏洞。

8.2.2.4 适用等级

B 级以上产品应通过此项测试。

8.2.3 数据库安全

8.2.3.1 测试内容

检测管理端的数据库是否存在安全漏洞。

8.2.3.2 测试步骤

测试步骤为：

a) 使用安全扫描器对数据库进行扫描；

b) 查看扫描结果。

8.2.3.3 预期结果

预期结果为：

数据库不存在高、中风险安全漏洞。

8.2.3.4 适用等级

C+级以上产品应通过此项测试。

8.2.4 非正常关机

8.2.4.1 测试内容

测试产品在非正常关机条件下（掉电、强行关机等），重新启动后能够正常工作。

8.2.4.2 测试步骤

测试步骤为：

a) 在该产品正常运行状态下，承载器运行的主机突然掉电，重启产品后查看结果；

b) 该产品正常运行状态下，未作任何保存记录或采取保护措施，强行退出运行，重启产品后查看结果。

8.2.4.3 预期结果

预期结果为：

该产品在非正常关机条件下，重启产品后应能正常工作。

8.2.4.4 适用等级

C 级以上产品应通过此项测试。

8.2.5 口令防暴力猜解

8.2.5.1 测试内容

测试产品防止对管理员口令进行暴力猜解的能力。

8.2.5.2 测试步骤

测试步骤为：

a) 设置口令录入次数限制；

b) 用超过限制的次数连续使用不正确的口令登录产品；

c) 查看结果。

8.2.5.3 预期结果

预期结果为：

用超过限制的次数连续使用不正确的口令登录产品失败后，应有正确的提示，并对账户进行锁定。

8.2.5.4 适用等级

C+级以上产品应通过此项测试。

8.3 通信安全

8.3.1 测试内容

测试管理端与数据库服务器之间进行的通信加密。

8.3.2 测试步骤

测试步骤为：

a) 在被检测的网络中启动协议分析仪；

b) 在管理端对产品进行各项操作；

c) 利用协议分析仪对管理端和数据库服务器之间的通信数据进行分析。

8.3.3 预期结果

预期结果为：

管理端与数据库服务器之间的通信进行了加密处理。

8.3.4 适用等级

B 级以上产品应通过此项测试。

8.4 容错性

8.4.1 测试内容

测试终端安全管理产品是否具备输入容错性、错误提示信息可用性及引导能力。

8.4.2 测试步骤

测试步骤为：

a) 登录管理端，查看登录界面中的各项操作是否具有联机帮助和操作说明等；

b) 在录入界面的文本框中输入非常规字符，或录入超出范围的数字和字符长度，查看是否有错误提示。

8.4.3 预期结果

预期结果为：

a) 产品界面中应对各项操作有明确的解释和提示，指导用户正确的操作；

b) 如果用户出现误操作，产品应及时提示用户正确的输入方法。

8.4.4 适用等级

C 级以上产品应通过此项测试。

9 等级评估

产品等级确定应同时符合下列要求：

a) 应通过基本用例，见表 2；

b) C 级产品应通过测试用例总数的 50%，C+级产品应通过测试用例总数的 60%，B 级产品应通过测试用例总数的 78%，B+级产品应通过测试用例总数的 90%，A 级产品应通过测试用例总数的 95%。

表 2 关键用例要求

测试类	测试子类	测试项	适用等级					对应条款
			C	C+	B	B+	A	
功能测试	网络拓扑发现	自动拓扑发现	●	●	●	●	●	6.1.1
		网络拓扑编辑	—	●	●	●	●	6.1.2
	网络管理	网络资产管理	●	●	●	●	●	6.2.1
		IP 地址安全管理	—	●	●	●	●	6.2.2
		路由器状态监测	—	●	●	●	●	6.2.3
		交换机状态监测	—	●	●	●	●	6.2.4
		安全设备状态监测	—	—	●	●	●	6.2.5
		终端状态监测	—	●	●	●	●	6.2.6
		其他设备监测	—	●	●	●	●	6.2.7
		网络流量监测	—	—	●	●	●	6.2.8
		日志集中管理	—	●	●	●	●	6.2.9
		综合分析	—	—	—	●	●	6.2.10
	终端信息收集	系统信息	●	●	●	●	●	6.3.1
		安全事件日志	—	●	●	●	●	6.3.2
		网络连接状态	—	●	●	●	●	6.3.3
	终端管理	登录管理	—	—	●	●	●	6.4.1
		钥匙的唯一性	—	—	●	●	●	6.4.2
		钥匙管理	—	—	●	●	●	6.4.3
		进程管理	—	●	●	●	●	6.4.4
		用户组管理	—	●	●	●	●	6.4.5
		共享管理	—	●	●	●	●	6.4.6

表 2(续)

测试类	测试子类	测试项	适用等级					对应条款
			C	C+	B	B+	A	
功能测试	终端管理	锁屏管理	—	●	●	●	●	6.4.7
		服务管理	—	●	●	●	●	6.4.8
		注册表保护	—	—	—	●	●	6.4.9
		嗅探发现	—	—	—	—	●	6.4.10
		远程信息发送	—	●	●	●	●	6.4.11
		主机防火墙	—	—	—	●	●	6.4.12
	终端外设控制	键盘鼠标控制	●	●	●	●	●	6.5.1
		光驱软驱控制	●	●	●	●	●	6.5.2
		串口并口控制	●	●	●	●	●	6.5.3
		USB 接口控制	●	●	●	●	●	6.5.4
		其他接口控制	—	●	●	●	●	6.5.5
	终端网络访问控制	WEB 地址控制	—	—	●	●	●	6.6.1
		邮件收发控制	—	—	●	●	●	6.6.2
		FTP 访问控制	—	—	●	●	●	6.6.3
		TELNET 访问控制	—	—	●	●	●	6.6.4
		邮件内容监控	—	—	—	—	●	6.6.5
		网络打印控制	—	●	●	●	●	6.6.6
		外联控制	●	●	●	●	●	6.6.7
		接入控制	●	●	●	●	●	6.6.8
	终端操作系统补丁管理	操作系统补丁检查	—	●	●	●	●	6.8.1
		操作系统补丁分发	—	—	●	●	●	6.8.2
	审计	告警信息审计	—	●	●	●	●	6.9.1
		历史事件审计	—	●	●	●	●	6.9.2
	日志管理	日志生成	●	●	●	●	●	6.10.1
		日志完整性	●	●	●	●	●	6.10.2
		授权访问日志记录	●	●	●	●	●	6.10.3
		日志报表	—	●	●	●	●	6.10.4
		日志维护	—	●	●	●	●	6.10.5
	产品配置管理	策略管理	—	●	●	●	●	6.11.1
		策略备份与恢复	—	●	●	●	●	6.11.2
		用户管理	●	●	●	●	●	6.11.3
		口令强度管理	●	●	●	●	●	6.11.4
		产品化程度	●	●	●	●	●	6.11.5
性能测试	拓扑发现准确性	拓扑发现准确性	—	●	●	●	●	7.1
	网络发现速度	网络发现速度	—	●	●	●	●	7.2
	网络轮询时间	网络轮询时间	—	●	●	●	●	7.3
	并发采集进程	并发采集进程	—	—	—	—	●	7.4
	安全策略生效时间	安全策略生效时间	●	●	●	●	●	7.5
	稳定性	稳定性	●	●	●	●	●	7.6
安全性测试	客户端安全	进程保护	—	●/—	●	●	●	8.1.1
		文件保护	—	—	●	●	●	8.1.2
		注册表保护	—	—	—	●	●	8.1.3

表 2(续)

测试类	测试子类	测试项	适用等级					对应条款
			C	C+	B	B+	A	
安全性测试	客户端安全	安全卸载	—	—	●	●	●	8.1.4
	管理端安全	安全风险引入	—	—	●	●	●	8.2.1
	管理端安全	服务器安全	—	—	●	●	●	8.2.2
		数据库安全	—	●	●	●	●	8.2.3
		非正常关机	●	●	●	●	●	8.2.4
		口令防暴力猜解	—	●	●	●	●	8.2.5
	通信安全	通信安全	—	—	●	●	●	8.3
	容错性	容错性	●	●	●	●	●	7.7
注：“●”为基本用例；“—”为非基本用例。								

中 华 人 民 共 和 国
国家军用标准
网络安全管理类产品测评方法
GJB 7170—2011
*
总装备部军标出版发行部出版
（北京东外京顺路 7 号）
总装备部军标出版发行部印刷车间印刷
总装备部军标出版发行部发行
*
开本 880×1230 1/16 印张 2¼ 字数 66 千字
2011 年 5 月第 1 版 2011 年 5 月第 1 次印刷
印数 1—1200
*
军标出字第 8189 号 定价 34.00 元