GJB

中华人民共和国国家军用标准

FL 0112

GJB 7175—2011

军用网络安全隔离交换产品通用要求

General requirements for military network secure separation and exchange products

2011—01—20 发布

2011—04—01 实施

中国人民解放军总装备部 批 准

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：解放军信息安全测评认证中心、航天科工集团706所、网御神州科技(北京)有限公司。

本标准主要起草人：姚　兰、桂坚勇、荀京京、刘向东、李智勇、阮　强、李锦山、隋迎春、李　蒙、王利君、刘建锋。

军用网络安全隔离交换产品通用要求

1 范围

本标准规定了军用网络安全隔离交换产品的等级划分以及各级产品的功能、性能、安全性和可用性技术要求。

本标准适用于军用网络安全隔离交换产品。

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。

GB/T 18336-2001 信息技术 安全技术 信息技术安全性评估准则

GB/T 20279-2006 信息安全技术 网络和终端设备隔离部件安全技术要求

3 术语和定义

GB/T 18336-2001 和 GB/T 20279-2006 中确立的以及下列术语和定义适用于本标准。

3.1 网络安全隔离交换产品 network secure separation and exchange products

能够保证内部网络和外部网络之间在网络协议终止的基础上，以信息摆渡的方式，通过安全控制与检查机制实现网络安全隔离和适度信息交换的软硬件组合。

3.2 内部网络 inner network

网络安全隔离交换产品所连接的网络中安全级别相对较高的网络。

3.3 外部网络 outer network

网络安全隔离交换产品所连接的网络中安全级别相对较低的网络。

4 产品类型和构成

4.1 产品类型

产品分为网络安全隔离与信息双向交换产品和网络安全隔离与信息单向传输产品。

4.2 产品构成

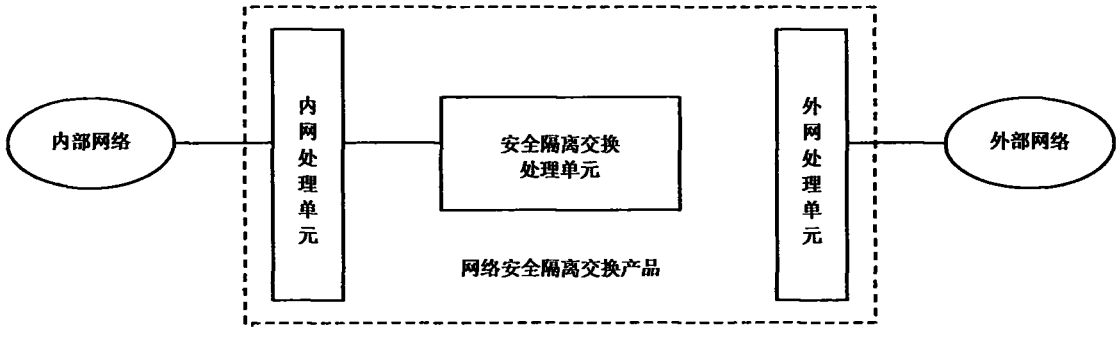

图 1 网络安全隔离交换产品构成

产品在结构上主要由内网处理单元、外网处理单元、安全隔离交换处理单元三个模块组成，如图 1 所示。其中内网处理单元连接内部网络，外网处理单元连接外部网络，安全隔离交换处理单元分时连通

内、外网处理单元，是内、外网处理单元之间唯一的数据传输通道。

5 等级划分

依据产品的功能、性能、安全性和可用性的不同，产品划分为一级、二级、三级三个等级，其中一级为最低级，三级为最高级。

6 一级产品要求

6.1 第一级产品功能要求

6.1.1 隔离功能

产品应具有网间安全隔离功能，具体要求如下：

a) 内网处理单元和外网处理单元应采用独立的主机系统，分别具有独立的运算单元和存储单元；

b) 安全隔离交换处理单元是内、外网处理单元之间唯一的数据传输通道，不可旁路；

c) 网络协议应在内、外网处理单元被完全终止，所有经过数据流都应从网络协议包中剥离，还原为应用层数据。

6.1.2 信息交换

产品应具有适度的信息交换功能，具体要求如下：

a) 内、外网处理单元应具有协议解析功能，处理用户的网络访问请求，解析、提取出应用层数据，然后封装成系统专用协议在隔离网间进行交换；

b) 网络安全隔离与信息双向交换产品宜支持常用的网络应用及其应用协议；

c) 网络安全隔离与信息单向传输产品应采用安全控制措施确保数据只能单方向传输。

6.1.3 访问控制

产品应具有访问控制功能，提供内、外网间数据交换的安全控制机制，只有符合安全策略的数据才被允许进行交换，具体要求如下：

a) 应支持 IP/MAC 地址绑定；

b) 应禁止断点续传；

c) 应提供细粒度的数据包过滤功能(包括多种控制选项，如源地址、目的地址、端口、时间等属性)。

6.1.4 安全管理

6.1.4.1 用户管理

产品应具有对用户的管理、识别能力，包括认证和授权，具体要求如下：

a) 应具有添加、删除、修改用户及信息的能力；

b) 应仅允许授权管理员承担安全管理职责；

c) 应为每一个用户提供一套唯一的、执行安全策略所必需的安全属性，包括用户标识、鉴别数据、授权信息等；

d) 应对用户进行身份鉴别与权限控制。

6.1.4.2 网络管理协议的支持

产品宜支持轮询或陷阱形式的典型网络管理。

6.1.5 鉴别

6.1.5.1 身份鉴别

产品应具有身份鉴别能力，保证在授权管理员、可信主机执行任何管理操作之前，对每个授权管理员和可信主机进行鉴别认证。

6.1.5.2 鉴别安全管理

产品应具有鉴别安全管理功能，具体要求如下：

a) 当用户鉴别尝试失败连续达到限定次数后，系统应锁定该帐号，并进行审计记录；
b) 应保护鉴别数据不被未授权查阅和修改。

6.1.6 日志审计

6.1.6.1 审计数据生成

产品应具有日志审计功能，为产品的配置、使用和运行状态产生审计记录，具体要求如下：
a) 应能够对管理员的配置管理操作进行日志记录；
b) 应能够对信息交换活动(数据和行为)进行日志记录；
c) 审计记录的内容应完整、准确，记录方式应便于用户理解；
d) 应详细记录事件发生的时间、事件类型、主体身份、内容和事件的结果(成功或失败)。

6.1.6.2 审计记录管理

产品应能对审计记录进行管理维护，具体要求如下：
a) 支持日志的浏览、查询、导出和删除等操作；
b) 应仅允许授权管理员实现审计功能的启动、关闭和配置；
c) 应保证审计记录只能被授权管理员访问，审计查阅工具只能被授权管理员使用。

6.1.6.3 审计数据安全

产品应确保审计数据安全，具体要求如下：
a) 应保护审计记录不受未授权的查阅、修改和破坏；
b) 应将删除或清空审计记录的事件记入审计日志；
c) 应采用安全控制措施防止审计数据丢失。

6.2 第一级产品性能要求

6.2.1 可靠性

产品至少应实现 MTBF 不低于 10000h。

6.2.2 延迟

产品的网络延迟应满足以下要求：
a) 对网络中文件的传输不应产生明显影响，与未使用产品时达到基本相同的传输效率；
b) 对网络中属于开放服务的访问，经过产品时不应受到明显影响，与未使用产品时达到基本相同的访问效率。

6.3 第一级产品安全性要求

6.3.1 自我保护

产品应具有自我保护能力，具体要求如下：
a) 应提供初始启动时的默认最小安全集策略；
b) 对异常断电应具有自我保护能力。

6.3.2 客体重用

在为所有内部或外部网络主机连接进行资源分配时，产品应保证不提供以前连接的任何信息内容，保障数据交换的安全性和可靠性。

6.3.3 系统平台安全

应确保系统平台安全，主要包括系统的脆弱性、专用协议的安全等，具体要求如下：
a) 应能够对操作系统进行裁剪和安全加固；
b) 应该弥补操作系统上已知的安全漏洞；
c) 应不存在已知的高、中风险安全漏洞；
d) 应保证系统专用协议的安全。

6.3.4 抗攻击能力

产品应能有效地抵御和防止多种网络攻击，具体要求如下：

a) 应能对扫描类网络攻击进行隔离；
b) 应能对木马类网络攻击进行隔离；
c) 具有一定的抗拒绝服务、分布式拒绝服务攻击能力。

6.4 一级产品可用性要求

6.4.1 易用性

产品应具有使用的方便性和友好性，要求操作简单，提示清晰，能提供友好的中文管理界面，且具有用户输入的错误提示。

6.4.2 文档

开发者应提供各种必要的文档，包括技术报告、自测报告、用户手册、管理员指南、配置管理文档等。文档资料应描述准确、相关内容一致。具体要求如下：

a) 应对产品的使用具有明确的指导作用，与实际产品一致；
b) 应对产品的安装、启动、使用的过程以及操作步骤进行详细描述；
c) 应提供产品的功能规范；
d) 应提供产品的安全策略；
e) 应描述用户可使用的功能、接口与使用方法；
f) 应描述产品的所有外部接口的用途与使用方法；
g) 开发者应确认所提供的信息能满足在内容和表述上的所有要求。

6.4.3 安装与卸载

产品的管理端软件应能正常安装与卸载，且卸载后系统中无残留信息(安装后生成的信息除外)。

7 二级产品要求

7.1 二级产品功能要求

7.1.1 隔离功能

产品应具有网间安全隔离功能，具体要求如下：

a) 应达到6.1.1的要求；
b) 应采用硬件隔离部件保证在任何时刻网络之间物理断开。

7.1.2 信息交换

产品应具有信息交换功能，具体要求如下：

a) 应达到6.1.2的要求；
b) 网络安全隔离与信息双向交换产品宜支持包括用户自定义协议在内的广泛的网络应用及其应用协议，例如支持视频会议、流媒体等应用。

7.1.3 访问控制

产品应具有访问控制功能，提供内、外网间数据交换的安全控制机制，只有符合安全策略的数据才被允许进行交换，具体要求如下：

a) 应达到6.1.3的要求；
b) 应根据不同应用协议特性提供应用层的安全检查控制机制，例如对所支持应用协议的命令、访问路径、内容、访问的文件资源、关键字等进行安全检查和控制。

7.1.4 病毒防护

产品宜对所传输的数据进行病毒查杀。

7.1.5 安全管理

7.1.5.1 用户管理

产品应具有对用户的管理、识别能力，包括认证和授权，具体要求如下：

a) 应达到6.1.4.1的要求；

b) 应保证用户身份鉴别的有效性和安全性，例如检测口令强度等。

7.1.5.2 网络管理协议的支持

产品宜支持轮询或陷阱形式的典型网络管理。

7.1.5.3 远程管理

如果产品支持远程管理，则应满足以下要求：

a) 应仅允许可信主机进行远程管理；

b) 应通过加密来保护远程管理信息。

7.1.5.4 管理接口

产品应提供独立的管理接口，使管理接口和业务接口分离。

7.1.6 鉴别

7.1.6.1 身份鉴别

产品应提供身份鉴别功能，具体要求见 6.1.5.1。

7.1.6.2 鉴别安全管理

产品应具有鉴别安全管理功能，具体要求如下：

a) 应达到 6.1.5.2 的要求。

b) 应具有登录超时认证功能。管理员在一段时间内无任何操作，需要再次进行身份鉴别才能重新管理设备，最大超时时间仅由授权管理员设定。

c) 应预防有关管理鉴别数据的重用，例如不应显示默认的登录用户名等。

7.1.7 日志审计

7.1.7.1 审计数据生成

产品应具有日志审计功能，具体要求见 6.1.6.1。

7.1.7.2 审计记录管理

产品应具有审计记录管理功能，具体要求见 6.1.6.2。

7.1.7.3 审计数据安全

产品应确保审计数据安全，具体要求如下：

a) 应达到 6.1.6.3 的要求；

b) 应确保遇到故障或遭受攻击时，能够完整保留已经保存的审计数据，并限制审计事件丢失的数量。

7.2 二级产品性能要求

7.2.1 可靠性

产品至少应实现 MTBF 不低于 10000h。

7.2.2 延迟

产品的网络延迟应达到 6.2.2 的要求。

7.3 二级产品安全性要求

7.3.1 自我保护

产品应具有自我保护能力，具体要求如下：

a) 应达到 6.3.1 的要求；

b) 在异常断电的情况下，重新启动时应能够恢复断电前的原有设置状态。

7.3.2 客体重用

产品应达到 6.3.2 的要求。

7.3.3 系统平台安全

应确保系统平台安全，主要包括系统的脆弱性、专用协议的安全等，具体要求如下：

a) 产品应达到 6.3.3 的要求；

b） 应对系统平台中的敏感信息具有自我保护能力。

7.3.4 抗攻击能力

产品应能有效地抵御和防止多种网络攻击，具体要求如下：

a） 产品应达到 6.3.4 的要求；

b） 应具有实时入侵检测机制，提供对网络攻击的检测及防御能力。

7.4 二级产品可用性要求

7.4.1 易用性

产品应达到 6.4.1 的要求。

7.4.2 文档

产品应达到 6.4.2 的要求。

7.4.3 安装与卸载

产品应达到 6.4.3 的要求。

8 三级产品要求

8.1 三级产品功能要求

8.1.1 隔离功能

产品应具有网间安全隔离功能，具体要求如下：

a） 应达到 7.1.1 的要求；

b） 宜具有多网络隔离能力，实现内网处理单元、外网处理单元直接通过独立的网络接口连接两个以上相同安全级别的网络。

8.1.2 信息交换

产品应具有信息交换功能，具体要求见 7.1.2。

8.1.3 访问控制

产品应具有访问控制功能，具体要求见 7.1.3。

8.1.4 病毒防护

产品应对所传输的数据进行病毒查杀。

8.1.5 安全管理

8.1.5.1 用户管理

产品应具有对用户的管理、识别能力，包括认证和授权，具体要求如下：

a） 应达到 7.1.5.1 的要求；

b） 应实现分权管理，不同角色的管理员具有不同的管理权限。

8.1.5.2 网络管理协议的支持

产品宜支持轮询或陷阱形式的典型网络管理。

8.1.5.3 远程管理

如果产品支持远程管理，则应满足 7.1.5.3 的具体要求。

8.1.5.4 管理接口

产品应提供独立的管理接口，使管理接口和业务接口分离。

8.1.5.5 集中安全管理

产品应能通过集中管理控制台对全局网络中的多台设备集中完成配置、管理和系统监控等工作。

8.1.6 鉴别

8.1.6.1 身份鉴别

产品应具有身份鉴别功能，具体要求见 6.1.5.1。

8.1.6.2 鉴别安全管理

产品应具有鉴别安全管理功能，具体要求见 7.1.6.2。

8.1.6.3 多鉴别机制

产品应提供多种鉴别机制以支持用户多鉴别，例如为管理员和普通用户提供选择不同的身份鉴别方式。

8.1.7 日志审计

8.1.7.1 审计数据生成

产品应具有日志审计功能，具体要求如下：

a) 应达到 6.1.6.1 的要求；

b) 应能够对所有与安全相关的活动进行日志记录，如系统的启动、停止，鉴别失败等。

8.1.7.2 审计记录管理

产品应具有审计记录管理功能，具体要求如下：

a) 应达到 6.1.6.2 的要求；

b) 应能够对安全事件进行关联分析，发现可能的安全隐患。

8.1.7.3 审计数据安全

产品应确保审计数据安全，具体要求如下：

a) 应达到 7.1.7.3 的要求。

b) 当审计数据存储容量达到预定警戒值时，应能够自动产生告警。如果审计数据存储空间已满，应采取忽略审计数据，或者覆盖最早存储的审计数据，或者自动转存等措施，并发出告警。

8.2 三级产品性能要求

8.2.1 可靠性

产品至少应实现 MTBF 不低于 10000h。

8.2.2 延迟

产品的网络延迟应达到 6.2.2 的要求。

8.3 三级产品安全性要求

8.3.1 自我保护

产品应达到 7.3.1 的要求。

8.3.2 客体重用

产品应达到 6.3.2 的要求。

8.3.3 系统平台安全

应确保系统平台安全，主要包括系统的脆弱性、专用协议的安全等，具体要求如下：

a) 应达到 7.3.3 的要求；

b) 应采用经国家主管部门指定的检测机构检测合格的安全操作系统。

8.3.4 抗攻击能力

产品应能有效地抵御和防止多种网络攻击，具体要求如下：

a) 应能对扫描类网络攻击进行隔离；

b) 应能对木马类网络攻击进行隔离；

c) 具有抗拒绝服务、分布式拒绝服务攻击的能力，当攻击发生时能保障对正常应用请求的应答；

d) 应具有实时入侵检测机制，提供对网络攻击的检测及防御能力。

8.4 三级产品可用性要求

8.4.1 易用性

产品应达到 6.4.1 的要求。

8.4.2 文档

产品的开发者应提交相关文档，应达到 6.4.2 的要求。

8.4.3 安装与卸载

产品应达到6.4.3的要求。

中 华 人 民 共 和 国
国家军用标准
军用网络安全隔离交换产品通用要求
GJB 7175-2011
*
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 1 字数 24 千字
2011 年 5 月第 1 版 2011 年 5 月第 1 次印刷
印数 1-1000
*
军标出字第 8193 号 定价 15.00 元