ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20279—2015
代替 GB/T 20279—2006

信息安全技术　网络和终端隔离产品安全技术要求

Information security technology—Security technical requirements of network and terminal separation products

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准代替 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》。

本标准与 GB/T 20279—2006 的主要差异如下：

——分类修改为终端隔离产品、网络隔离产品和网络单向导入产品三类；

——级别统一划分为基本级和增强级；

——增加了终端隔离产品、网络隔离产品和网络单向导入产品描述；

——增加了下一代互联网协议支持能力的要求；

——在附录中增加了技术要求基本原理，包括安全功能要求基本原理和安全保证要求基本原理。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、珠海经济特区伟思有限公司、南京神易网络科技有限公司、公安部第三研究所。

本标准主要起草人：陆臻、顾健、俞优、李旋、邓琦、左安骥、路文利、刘斌。

信息安全技术　网络和终端隔离产品安全技术要求

1　范围

本标准规定了网络和终端隔离产品的安全功能要求、安全保证要求、环境适应性要求及性能要求。

本标准适用于网络和终端隔离产品的设计、开发与测试。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999　计算机信息系统安全保护划分准则

GB/T 18336.3—2008　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

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB 17859—1999 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

安全域　security domain

具有相同的安全保护需求和相同安全策略的计算机或网络区域。

3.2

物理断开　physical disconnection

处于不同安全域的网络之间不能以直接或间接的方式相连接。

注：在一个物理网络环境中，实施不同安全域的网络物理断开，在技术上应确保信息在物理传导、物理存储上的断开。

3.3

协议转换　protocol conversion

协议的剥离和重建。在所属某一安全域的隔离产品一端，把基于网络的公共协议中的应用数据剥离出来，封装为系统专用协议传递至所属其他安全域的隔离产品另一端，再将专用协议剥离，并封装成需要的格式。

3.4

协议隔离　protocol separation

处于不同安全域的网络在物理上是有连接的，通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。

3.5

信息摆渡　information ferry

信息交换的一种方式，物理传输信道只在传输进行时存在。

注：信息传输时，信息先由信息源所在安全域一端传输至中间缓存区域，同时物理断开中间缓存区域与信息目的所在安全域的连接；随后接通中间缓存区域与信息目的所在安全域的传输信道，将信息传输至信息目的所在安全

域，同时在信道上物理断开信息源所在安全域与中间缓存区域的连接。在任一时刻，中间缓存区域只与一端安全域相连。

3.6

单向传输部件　unilateral transmission unit

一对具有物理上单向传输特性的传输部件，该传输部件由一对独立的发送和接收部件构成，发送和接收部件只能以单工方式工作，发送部件仅具有单一的发送功能，接收部件仅具有单一的接收功能，两者构成可信的单向信道，该信道无任何反馈信息。

3.7

终端隔离产品　terminal separation product

同时连接两个不同安全域，采用物理断开技术在终端上实现安全域物理隔离的安全隔离卡或安全隔离计算机。

3.8

网络隔离产品　network separation product

位于两个不同安全域之间，采用协议隔离技术在网络上实现安全域安全隔离与信息交换的产品。

3.9

网络单向导入产品　network unilateral transmission product

位于两个不同安全域之间，通过物理方式构造信息单向传输的唯一通道，实现信息单向导入，并且保证只有安全策略允许传输的信息可以通过，同时反方向无任何信息传输或反馈。

4　网络和终端隔离产品描述

网络和终端隔离产品从形态和功能上可以划分为终端隔离产品、网络隔离产品和网络单向导入产品三类，目的是在不同的网络终端和网络安全域之间建立安全控制点，实现在不同的网络终端和网络安全域之间提供访问可控的服务。此外，适用于下一代互联网网络环境的网络和终端隔离产品的协议栈除支持 IPv4 技术外，还应支持 IPv6 以及 IPv4/IPv6 过渡技术。

网络和终端隔离产品保护的资产是受安全策略保护的网络服务和资源等，此外，网络和终端隔离产品本身及其内部的重要数据也是受保护的资产。

图 1 为终端隔离产品的一个典型运行环境。终端隔离产品一般以隔离卡的方式接入目标主机，隔离卡通过电子开关以互斥的形式同时连通安全域 A 所连的硬盘 1 和安全域 A，或者安全域 B 所连的硬盘 2 和安全域 B，从而实现内外两个安全域的物理隔离。该类产品也可将隔离卡整合入主机，以整机的形式作为产品。

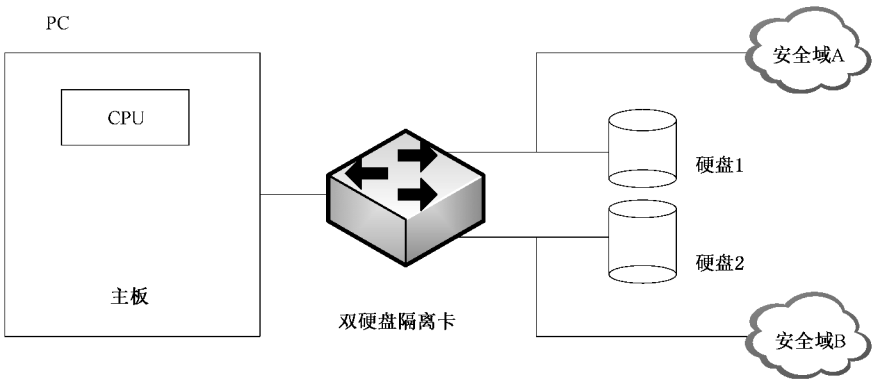

图 1　终端隔离产品典型运行环境

图 2 为网络隔离产品的一个典型运行环境。网络隔离产品一般以二主机加专用隔离部件的方式组成，即由内部处理单元、外部处理单元和专用隔离部件组成。其中，专用隔离部件既可以是采用包含电子开关并固化信息摆渡控制逻辑的专用隔离芯片构成的隔离交换板卡，也可以是经过安全强化的运行专用信息传输逻辑控制程序的主机。网络隔离产品用于连接两个不同的安全域，实现两个安全域之间应用代理服务、协议转换、信息流访问控制、内容过滤和信息交换等功能。网络隔离产品中的内、外部处理单元通过专用隔离部件相连，专用隔离部件是两个安全域之间唯一的可信物理信道。该内部信道裁剪了 TCP/IP 等公共网络协议栈，采用私有协议实现协议隔离。在一些安全性要求较低而实时性要求较高的场合，专用隔离部件采用私有协议以逻辑方式实现协议隔离和信息传输。在一些安全性要求较高而实时性要求相对较低的场合，专用隔离部件还会采用一组互斥的分时切换电子开关实现内部物理信道的通断控制，以分时切换连接方式完成信息摆渡，从而在两个安全域之间形成一个不存在实时物理连接的隔离区。

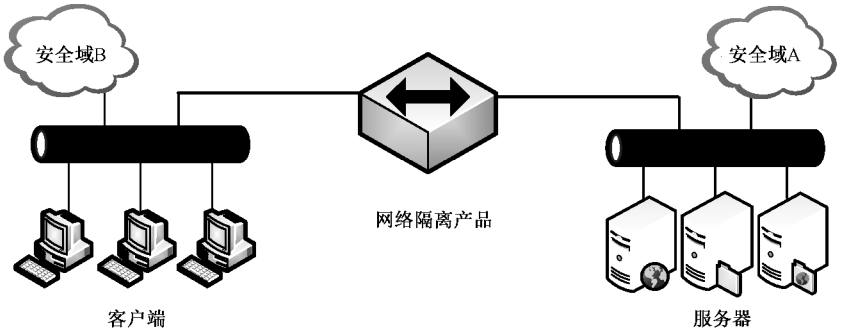

图 2　网络隔离产品典型运行环境

图 3 为网络单向导入产品的一个典型运行环境。网络单向导入产品一般以双机方式组成，即数据发送处理单元和数据接收处理单元，双机之间采用单向传输部件相连。网络单向导入产品部署在两个的安全域之间，其中，数据发送处理单元网络接口连接信息发送方安全域 A，数据接收处理单元网络接口连接接收信息接收方安全域 B，信息流由发送数据的安全域 A 单向流入接收数据的安全域 B。单向传输部件利用单向传输的物理特性建立两个安全域之间唯一的单向传输通道，数据在这个通道中只能沿数据发送处理单元向数据接收处理单元方向的可信路径单向传输，无任何反馈信号。单向传输部件由一对单向接收部件和单向发送部件构成，单向发送部件安装在数据发送处理单元中，单向接收部件安装在数据接收处理单元中。单向传输部件的单向物理传输特性固化不可修改，任何软件配置、物理跳线等方式都不能更改其部件的单向传输特性以及传输方向，从而实现数据单向导入的可靠性。

例：光通信，数据发送处理单元使用光发送模块，数据接收处理单元使用光接收模块，单向传输通道使用单根光纤，实现数据单向传输。

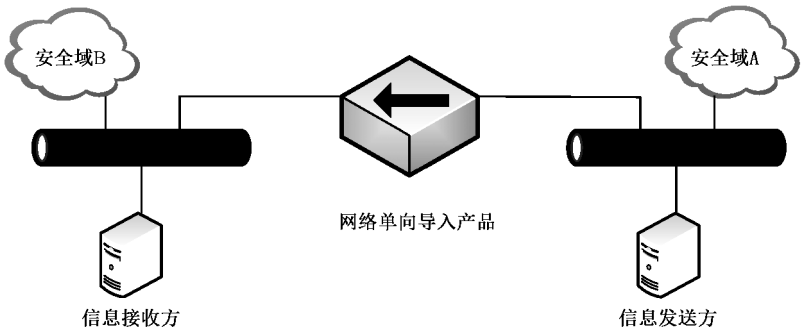

图 3　网络单向导入产品典型运行环境

5 安全技术要求

5.1 总体说明

5.1.1 安全技术要求分类

本标准将网络和终端隔离产品安全技术要求分为安全功能、安全保证、环境适应性和性能要求四个大类。其中，安全功能要求是对网络和终端隔离产品应具备的安全功能提出具体要求，终端隔离产品具体要求包括访问控制、不可旁路和客体重用，网络隔离产品具体要求包括访问控制、抗攻击、安全管理、标识和鉴别、审计、域隔离、容错、数据完整性和密码支持，网络单向导入产品具体要求包括访问控制、抗攻击、安全管理、标识和鉴别、审计、域隔离、配置数据保护和运行状态监测；安全保证要求针对网络和终端隔离产品的开发和使用文档的内容提出具体的要求，例如配置管理、交付和运行、开发和指导性文档等；环境适应性要求是对网络和终端隔离产品的应用环境提出具体的要求；性能要求则是对网络和终端隔离产品应达到的性能指标做出规定，包括交换速率和硬件切换时间。

5.1.2 安全等级

本标准按照网络和终端隔离产品安全功能的强度划分安全功能要求的级别，按照 GB/T 18336.3—2008 划分安全保证要求的级别。安全等级分为基本级和增强级，安全功能的强弱和安全保证要求的高低是等级划分的具体依据。安全等级突出安全特性，环境适应性要求和性能要求不作为等级划分依据。与基本级内容相比，增强级中要求有所增加或变更的内容在正文中通过“宋体加粗”表示。

5.2 安全功能要求

5.2.1 终端隔离产品

5.2.1.1 基本级要求

5.2.1.1.1 访问控制

5.2.1.1.1.1 安全属性定义

对于信息存储与传输部件（主要是处于不同安全域的存储设备、网络接入设备），终端隔离产品应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.2.1.1.1.2 属性修改

终端隔离产品的安全功能应包含向终端设备授权用户提供修改与安全相关属性的参数的功能。

5.2.1.1.1.3 属性查询

终端隔离产品的安全功能应包含向终端设备授权用户提供安全属性查询的功能。

5.2.1.1.1.4 访问授权与拒绝

终端隔离产品的安全功能应包含对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a) 在信息物理传输上使内外安全域隔断，确保外部安全域不能通过网络连接侵入内部安全域；同时阻止内部安全域信息通过网络连接泄露到外部安全域；

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存

部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部安全域与外部安全域信息要以不同存储设备分开存储；对移动存储介质，如光盘、软盘、USB 存储设备等，应在安全域转换前提示用户干预或禁止在双安全域都能使用这些设备。

5.2.1.1.1.5 切换信号一致性

对被隔离的计算机信息资源进行切换时，终端隔离产品的安全功能应由同一信号对隔离的计算机信息资源进行切换，确保一致性。

5.2.1.1.1.6 口令保护

对被隔离的计算机信息资源进行切换时，终端隔离产品的安全功能应保证用户必须输入切换口令。

5.2.1.1.1.7 内存及 USB 端口的物理隔离

若终端隔离产品以整机隔离系统的形态存在，终端隔离产品的安全功能应在物理上隔离内存及所有 USB 端口，确保所有的存储设备都是物理上隔断，从物理上保证数据安全性。

5.2.1.1.2 不可旁路

在与安全有关的操作（例如安全属性的修改）被允许执行之前，终端隔离产品安全功能应确保其通过安全功能策略的检查。

5.2.1.1.3 客体重用

在为所有内部或外部网络上的主机连接进行资源分配时，终端隔离产品安全功能应保证不提供以前连接的任何信息内容。

5.2.1.2 增强级要求

5.2.1.2.1 访问控制

5.2.1.2.1.1 安全属性定义

对于信息存储与传输部件（主要是处于不同安全域的存储设备、网络接入设备），终端隔离产品应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.2.1.2.1.2 属性修改

终端隔离产品安全功能应向终端设备授权用户提供修改与安全相关属性的参数的功能。

5.2.1.2.1.3 属性查询

终端隔离产品安全功能应向终端设备授权用户提供安全属性查询的功能。

5.2.1.2.1.4 访问授权与拒绝

终端隔离产品的安全功能应对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a) 在信息物理传输上使内外安全域隔断，确保外部安全域不能通过网络连接侵入内部安全域；同时阻止内部安全域信息通过网络连接泄露到外部安全域；

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存

部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部安全域与外部安全域信息要以不同存储设备分开存储；对移动存储介质，如光盘、软盘、USB 存储设备等，应在安全域转换前提示用户干预或禁止在双安全域都能使用这些设备。

5.2.1.2.1.5 网络非法外联

终端隔离产品的安全功能应保证用户在内网状态下，随时监测用户网络是否与互联网相连接，一旦发现则立即禁用网络并给出报警，确保内网安全。

5.2.1.2.1.6 切换信号一致性

对被隔离的计算机信息资源进行切换时，终端隔离产品的安全功能应由同一信号对隔离的计算机信息资源进行切换，确保一致性。

5.2.1.2.1.7 硬盘非法调换

终端隔离产品的安全功能应在初始安装时对对应网络的硬盘进行唯一标识，保证硬盘与网络一一对应，确保内网硬盘数据的安全。

5.2.1.2.1.8 口令保护

对被隔离的计算机信息资源进行切换时，终端隔离产品的安全功能应保证用户必须输入切换口令。

5.2.1.2.1.9 内存及 USB 端口的物理隔离

若终端隔离产品以整机隔离系统的形态存在，终端隔离产品的安全功能应在物理上隔离内存及所有 USB 端口，确保所有的存储设备都是物理上隔断，从物理上保证数据安全性。

5.2.1.2.2 不可旁路

在与安全有关的操作（例如安全属性的修改）被允许执行之前，终端隔离产品安全功能应确保其通过安全功能策略的检查。

5.2.1.2.3 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，终端隔离产品安全功能应保证不提供以前连接的任何信息内容。

5.2.2 网络隔离产品

5.2.2.1 基本级要求

5.2.2.1.1 访问控制

5.2.2.1.1.1 基本的信息流控制策略

针对对主体、客体以及经过网络隔离产品的主客体之间的所有操作，网络隔离产品应能够执行以下端到端基本的信息流控制策略：

a） 所有主客体之间发送和接收的信息流均执行网络层协议剥离，还原成应用层数据；

b） 主客体之间发送和接收的信息流均经过安全策略允许后传输；

c） 授权管理员通过独立的管理接口，经过身份验证后，授权管理员与网络隔离产品间发送的管理

信息经过安全策略允许后传输。

5.2.2.1.1.2 基本的信息流控制功能

网络隔离产品的安全功能策略应能够执行以下基本的信息流控制功能，提供明确的访问保障能力和拒绝访问能力。包括：

a) 通过配置访问控制列表进行信息流控制，访问控制列表的元素包括：源 IP 地址、目的 IP 地址、源端口、目的端口、协议号；
b) 对经过的 HTTP、FTP、SMTP、POP3 等应用协议信息流进行合规性检查；
c) 对经过的 HTTP、FTP、SMTP、POP3 等应用协议信息流的协议信令及参数关键字进行过滤；
d) 对经过的 HTTP、FTP、SMTP、POP3 等应用协议信息流中的内容包括文件附件进行关键字过滤；
e) 通过协议隔离方式断开内部 TCP/IP 连接，完成信息传输。

5.2.2.1.1.3 残余信息保护

网络隔离产品在为所有内部或外部网上的主机连接进行资源分配时，网络隔离产品安全功能应保证其分配的资源中不提供以前连接活动中所产生的任何信息内容。

5.2.2.1.1.4 不可旁路

在与安全有关的操作（例如安全属性的修改、内部网络主机向外部网络主机传送信息等）被允许执行之前，网络隔离产品安全功能应确保其通过安全功能策略的检查。

5.2.2.1.2 抗攻击

网络隔离产品应能够抵御各种 DoS/DDoS 攻击，应能够识别和防御 SYN Flood、ICMP Flood 等攻击。

5.2.2.1.3 安全管理

5.2.2.1.3.1 区分安全管理角色

网络隔离产品安全功能：

a) 应将与安全相关的管理功能与其他功能区分开；
b) 应包括安装、配置和管理隔离产品安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），查阅安全属性，分配、修改和撤销安全属性，查阅和管理审计数据；
c) 应把执行与安全相关的管理功能的能力限定为一种安全管理职责，该职责具有一套特别授权的功能和响应的责任；
d) 应能把授权执行管理功能的授权管理员与使用隔离产品的所有其他个人或系统分开；
e) 应仅允许授权管理员承担安全管理职责；
f) 应在提出一个明确的请求以后，才会让授权管理员承担安全管理职责。

5.2.2.1.3.2 管理功能

网络隔离产品安全功能应向授权管理员提供如下管理功能：

a) 设置和更新与安全相关的数据；
b) 执行隔离产品的安装及初始化、系统启动和关闭、备份和恢复功能，备份能力应有自动工具的

支持；

c） 设置双机热备或负载均衡等可用性参数；

d） 若隔离产品安全功能支持外部或内部接口的远程管理，应：

1） 有对两个接口或其中之一关闭远程管理的选择权；

2） 限制可进行远程管理的地址；

3） 通过加密来保护远程管理会话。

5.2.2.1.3.3 独立管理接口

网络隔离产品应使用与通讯接口相互独立的管理接口与授权管理员连接，授权管理员经过身份鉴别后，采用多因素身份鉴别和加密方式建立授权管理员与网络隔离产品间的可信路径，禁止其他用户非授权访问管理接口。

5.2.2.1.4 标识和鉴别

5.2.2.1.4.1 基本安全属性定义

对于每一个授权管理员，网络隔离产品安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的基本安全属性。包括但不限于：

a） 设备网络参数：包括接口地址、网关地址等；

b） 设备接口属性：接口类型（例如：管理接口、通信接口）、接口速率等；

c） 安全管理参数：管理控制台地址、管理方式（例如：SSH、SSL）等；

d） 安全参数：最大鉴别失败次数等；

e） 外部可信 IT 产品参数配置：包括时间同步服务器参数、日志服务器参数等；

f） 系统参数：日志存储空间大小、设备名称等；

g） 用户角色属性：授权管理员、授权审计员、授权用户等；

h） 用户管理属性：用户名、用户角色、用户口令等；

i） 主机地址：源主机地址、目的主机地址；

j） 服务端口；

k） 使用时间或时间段；

l） 内容关键字。

5.2.2.1.4.2 属性初始化

网络隔离产品的安全功能应包含使用默认值对授权管理员和主机属性初始化的功能。

5.2.2.1.4.3 属性修改

网络隔离产品安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的功能：

a） 标识与角色（例如：配置管理员等）的关系；

b） 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

c） 配置的安全参数（例如：最大鉴别失败次数等数据）。

5.2.2.1.4.4 属性查询

网络隔离产品安全功能应仅向授权管理员提供以下查询功能：

a） 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

b） 关键字；

c) 通过网络隔离产品传送信息的主机信息。

5.2.2.1.4.5 鉴别数据初始化

网络隔离产品安全功能应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.2.2.1.4.6 鉴别时机

在所有授权管理员请求执行的任何操作之前，网络隔离产品安全功能应确保对每个授权管理员进行身份鉴别。

5.2.2.1.4.7 最少反馈

当进行鉴别时，网络隔离产品安全功能应仅将最少的反馈提供给用户。

5.2.2.1.4.8 鉴别失败处理

在经过一定次数的鉴别失败以后，网络隔离产品安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.2.2.1.5 审计

5.2.2.1.5.1 审计数据生成

网络隔离产品安全功能应能对下列可审计事件生成一个审计记录，包括事件发生的日期和时间，事件的类型，主体身份和成功或失败事件等信息：

a) 审计功能的启动和关闭；
b) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；
c) 任何读取、修改、破坏审计记录的尝试；
d) 所有对隔离产品规则覆盖的客体(内部或外部网络上的主机)执行操作的请求，以及受影响客体的标识；
e) 修改安全属性的所有尝试，以及修改后安全属性的新值；
f) 所有使用安全功能中鉴别数据管理机制的请求；
g) 所有访问鉴别数据的请求，以及访问请求的目标；
h) 任何对鉴别机制的使用；
i) 所有使用标识机制的尝试；
j) 所有对安全功能配置参数的修改(设置和更新)，无论成功与否，以及配置参数的新值；
k) 因鉴别尝试不成功的次数超出了设定的限制，导致的会话连接终止，以及会话连接使用的标识符。

5.2.2.1.5.2 审计记录管理

网络隔离产品安全功能应使授权管理员能存档、删除和清空审计记录。

5.2.2.1.5.3 可理解的格式

网络隔离产品安全功能应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.2.2.1.5.4 限制审计记录访问

网络隔离产品安全功能应仅允许授权管理员访问审计记录。

5.2.2.1.5.5 可选择查阅审计

网络隔离产品安全功能应提供按主体 ID、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.2.2.1.5.6 防止审计数据丢失

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，网络隔离产品的开发者应提供相应的分析结果。并且网络隔离产品安全功能：

a) 应把生成的审计记录储存于一个永久性的审计记录中，并限制由于故障和攻击造成的审计事件丢失的数量；

b) 一旦审计存储容量达到事先规定的警戒值，应能发出警告信息，并保证在授权管理员所采取的审计行为以外，防止其他可审计行为的出现。

5.2.2.1.6 域隔离

为保护网络隔离产品安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，网络隔离产品安全功能应为其自身的执行环境设定一个安全区域，并把网络隔离产品控制范围内的各个主体（内部或外部网络上的主机）的安全区域分隔开。

5.2.2.1.7 容错

网络隔离产品应具有主备模式的容错能力，当一台主机因电源、CPU 等硬件出现故障或软件错误导致异常时，容错功能将当前安全服务功能自动切换到另一台备机上继续运行，保证安全功能的可用性。

5.2.2.1.8 数据完整性

网络隔离产品安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

5.2.2.1.9 密码支持

网络隔离产品安全功能应保证其所提供的与密码算法相关功能符合国家密码主管部门的有关规定。

5.2.2.2 增强级要求

5.2.2.2.1 访问控制

5.2.2.2.1.1 增强的信息流控制策略

针对主体、客体以及经过网络隔离产品的主客体之间的所有操作，网络隔离产品的信息流控制策略应能够执行以下端到端增强的信息流控制策略：

a) **所有主客体之间发送和接收的信息流均执行网络层协议剥离，还原成应用层数据，包括应用层携带的较大的附件，例如大于 20 M 的邮件附件；**

b) **主体与客体通讯之前需对主体授权用户进行基于用户名/口令、数字证书的多因素身份验证，通过验证后，主客体之间发送和接收的信息流均经过安全策略控制允许后传输；**

c) **授权管理员通过独立的管理接口，经过身份鉴别后，授权管理员与网络隔离产品间发送的管理信息经过安全策略允许后传输。**

5.2.2.2.1.2 增强的信息流控制功能

网络隔离产品的安全功能策略应能够执行以下增强的信息流控制功能，提供明确的访问保障能力和拒绝访问能力。包括：

a) **通过配置访问控制列表进行信息流控制，访问控制列表的元素包括：源 IP 地址、目的 IP 地址、源端口、目的端口、协议号；**

b) **对经过的 HTTP、FTP、SMTP、POP3、SQL、RSTP、SIP 等应用协议信息流进行合规性检查；**

c) **对经过的 HTTP、FTP、SMTP、POP3、SQL、RSTP、SIP 等应用协议信息流的协议信令及参数关键字进行过滤；**

d) **配置文件同步任务，根据网络隔离产品上配置的同步任务参数，从源主机读取文件摆渡传输到目的主机，实现文件同步；**

e) **配置数据库同步任务，根据网络隔离产品上配置的同步任务参数，从源主机数据库读取数据，还原成文件后摆渡传输到另一端网络后写入目的主机数据库，实现数据库同步；**

f) **识别主体的应用类型，并通过访问应用控制列表进行信息流控制，禁止非授权应用访问客体；**

g) **应断开 TCP/IP 连接对内外网数据传输链路进行物理上的时分切换，即内外网络在物理链路上不能同时与专用隔离部件连通，并完成信息摆渡。**

5.2.2.2.1.3 强制访问控制

网络隔离产品安全功能应通过授权管理员和授权管理员控制的安全功能数据的敏感标记，控制授权管理员对相关安全功能数据的直接访问。

5.2.2.2.1.4 残余信息保护

网络隔离产品在为所有内部或外部网络上的主机连接进行资源分配时，网络隔离产品安全功能应保证其分配的资源中不提供以前连接活动中所产生的任何信息内容。

5.2.2.2.1.5 不可旁路

在与安全有关的操作（例如安全属性的修改、内部网络主机向外部网络主机传送信息等）被允许执行之前，网络隔离产品安全功能应确保其通过安全功能策略的检查。

5.2.2.2.2 抗攻击

网络隔离产品应能够抵御各种 DoS/DDoS 攻击，应能够识别和防御 SYN Flood、ICMP Flood 等攻击。

5.2.2.2.3 安全管理

5.2.2.2.3.1 区分安全管理角色

网络隔离产品安全功能：

a) 应将与安全相关的管理功能与其他功能区分开；

b) 应包括安装、配置和管理隔离产品安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），查阅安全属性，分配、修改和撤销安全属性，查阅和管理审计数据；

c) 应把执行与安全相关的管理功能的能力限定为一种安全管理职责，该职责具有一套特别授权的功能和响应的责任；

d) 应能把授权执行管理功能的授权管理员与使用隔离产品的所有其他个人或系统分开；
e) 应仅允许授权管理员承担安全管理职责；
f) 应在提出一个明确的请求以后，才会让授权管理员承担安全管理职责。

5.2.2.2.3.2 管理功能

网络隔离产品安全功能应向授权管理员提供如下管理功能：
a) 设置和更新与安全相关的数据；
b) 执行隔离产品的安装及初始化、系统启动和关闭、备份和恢复功能，备份能力应有自动工具的支持；
c) 设置双机热备或负载均衡等可用性参数；
d) 如果隔离产品安全功能支持外部或内部接口的远程管理，则应：
   1) 有对两个接口或其中之一关闭远程管理的选择权；
   2) 限制可进行远程管理的地址；
   3) 通过加密来保护远程管理会话。

5.2.2.2.3.3 独立管理接口

网络隔离产品应使用与通讯接口相互独立的管理接口与授权管理员连接，授权管理员经过身份鉴别后，采用多因素身份鉴别和加密方式，建立授权管理员与网络隔离产品间的可信路径，禁止其他用户非授权访问管理接口。

5.2.2.2.4 标识和鉴别

5.2.2.2.4.1 敏感标记

网络隔离产品安全功能应维护授权管理员可直接访问的网络隔离产品中安全功能相关数据的敏感标记。

5.2.2.2.4.2 基本安全属性定义

对于每一个授权管理员，网络隔离产品安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的基本安全属性。包括但不限于：
a) 设备网络参数：包括接口地址、网关地址等；
b) 设备接口属性：接口类型(例如：管理接口、通信接口)、接口速率等；
c) 安全管理参数：管理控制台地址、管理方式(例如：SSH、SSL)等；
d) 安全参数：最大鉴别失败次数；
e) 外部可信 IT 产品参数配置：包括时间同步服务器参数、日志服务器参数等；
f) 系统参数：日志存储空间大小、设备名称等；
g) 用户角色属性：授权管理员、授权审计员、授权用户等；
h) 用户管理属性：用户名、用户角色、用户口令等；
i) 主机地址：源主机地址、目的主机地址等；
j) 服务端口；
k) 使用时间或时间段；
l) 内容关键字。

5.2.2.2.4.3 增强的安全属性定义

对于每一个授权管理员，网络隔离产品安全功能应为其提供一套唯一的、为了执行安全功能策略提

供的增强的安全属性。包括但不限于：

a） **协议号：TCP、UDP；**

b） **应用协议：例如 HTTP、FTP、SMTP、RTSP 等；**

c） **应用类型：例如 FTP 客户端、QQ、MSN、迅雷等；**

d） **数据库同步参数：数据库类型、源数据库地址、目的数据库地址、同步方式（例如：增量同步、定时同步、全表同步）、源数据库账号/口令、目的数据库账号/口令、源数据库表名、目的数据库表名；**

e） **文件同步参数：源文件服务器地址、目的文件服务器地址、账号、口令等。**

5.2.2.2.4.4 属性初始化

网络隔离产品安全功能应提供使用默认值对授权管理员和主机属性初始化的功能。

5.2.2.2.4.5 属性修改

网络隔离产品安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的功能：

a） 标识与角色（例如：配置管理员等）的关系；

b） 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

c） 配置的安全参数（例如：最大鉴别失败次数等数据）。

5.2.2.2.4.6 属性查询

网络隔离产品安全功能应仅向授权管理员提供以下查询功能：

a） 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

b） 关键字；

c） 通过网络隔离产品传送信息的主机信息。

5.2.2.2.4.7 鉴别数据初始化

网络隔离产品安全功能应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.2.2.2.4.8 鉴别时机

在所有授权管理员请求执行的任何操作之前，网络隔离产品安全功能应确保对每个授权管理员进行身份鉴别。

5.2.2.2.4.9 最少反馈

当进行鉴别时，网络隔离产品安全功能应仅将最少的反馈提供给用户。

5.2.2.2.4.10 多鉴别机制

网络隔离产品安全功能应提供多因素的鉴别机制以支持用户多鉴别，其中，至少应包含以下不可共用的鉴别数据中的一种：

a） **USBKEY 密码钥匙；**

b） **生物指纹；**

c） **一次性口令；**

d） **数字证书。**

5.2.2.2.4.11 鉴别失败处理

在经过一定次数的鉴别失败以后，网络隔离产品安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.2.2.2.4.12 抗重放

网络隔离产品的鉴别机制应具有抗重放的能力，授权管理员及其他用户不能复制使用上一次通过的鉴别信息再次鉴别成功。

5.2.2.2.4.13 受保护的鉴别反馈

网络隔离产品的授权管理员在鉴别过程中输入的口令等敏感信息应以不可见和不可推理的形式显示在鉴别信息的登录输入界面中。

5.2.2.2.4.14 口令强度

网络隔离产品应采用口令校验机制对授权管理员生成的口令复杂度进行检查，口令强度应保证口令长度大于6位，口令类型为数字+大小写字母组合。

5.2.2.2.5 审计

5.2.2.2.5.1 审计数据生成

网络隔离产品安全功能应能对下列可审计事件生成一个审计记录，包括事件发生的日期和时间，事件的类型，主体身份和成功或失败事件等信息：

a) 审计功能的启动和关闭；
b) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；
c) 任何读取、修改、破坏审计记录的尝试；
d) 所有对隔离产品规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；
e) 修改安全属性的所有尝试，以及修改后安全属性的新值；
f) 所有使用安全功能中鉴别数据管理机制的请求；
g) 所有访问鉴别数据的请求，以及访问请求的目标；
h) 任何对鉴别机制的使用；
i) 所有使用标识机制的尝试；
j) 所有对安全功能配置参数的修改（设置和更新），无论成功与否，以及配置参数的新值；
k) 因鉴别尝试不成功的次数超出了设定的限制，导致的会话连接终止，以及会话连接使用的标识符。

5.2.2.2.5.2 安全审计分析

网络隔离产品安全功能应提供以下统计分析功能：

a) **所有隔离产品规则覆盖的主体（内部或外部网络上的主机）对客体执行操作时使用的应用分类统计；**
b) **网络隔离产品总应用流量、每个应用类别流量的统计；**
c) **网络隔离产品CPU、内存、磁盘占用率的统计；**
d) **在线用户列表及在线用户时长的统计。**

5.2.2.2.5.3 用户身份关联

网络隔离产品安全功能应能将每个可审计事件与引起该事件的用户身份相关联。

5.2.2.2.5.4 审计记录管理

网络隔离产品安全功能应使授权管理员能存档、删除和清空审计记录。

5.2.2.2.5.5 可理解的格式

网络隔离产品安全功能应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.2.2.2.5.6 限制审计记录访问

网络隔离产品安全功能应仅允许授权管理员访问审计记录。

5.2.2.2.5.7 可选择查阅审计

网络隔离产品安全功能应提供能按主体 ID、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.2.2.2.5.8 防止审计数据丢失

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，网络隔离产品的开发者应提供相应的分析结果。并且网络隔离产品安全功能：

a) 应把生成的审计记录储存于一个永久性的审计记录中，并应限制由于故障和攻击造成的审计事件丢失的数量；

b) 一旦审计存储容量达到事先规定的警戒值，应能发出警告信息，并保证在授权管理员所采取的审计行为以外，防止其他可审计行为的出现。

5.2.2.2.6 域隔离

5.2.2.2.6.1 基本的域隔离

为保护网络隔离产品安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，网络隔离产品安全功能应为其自身的执行环境设定一个安全区域，并把网络隔离产品控制范围内的各个主体（内部或外部网络上的主机）的安全区域分隔开。

5.2.2.2.6.2 增强的域隔离

为保护网络隔离产品安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，网络隔离产品安全功能应为其自身的执行环境设定一个安全区域，该安全区域被标记为高安全等级，授权管理员以及网络隔离产品所覆盖的所有主体（内部或外部网络上的主机）授权后只能读取该区域存储的文件、程序，不能进行删除和修改，采用强制访问控制策略，授权管理员无法修改访问策略。

5.2.2.2.7 容错

5.2.2.2.7.1 基本的容错

网络隔离产品应具有主备模式的容错能力，当一台主机因电源、CPU 等硬件出现故障或软件错误导致异常时，容错功能将当前安全服务功能自动切换到另一台备机上继续运行，保证安全功能的可用性。

5.2.2.2.7.2 增强的容错

网络隔离产品应具有主主模式的容错能力，两台主机同时对内部和外部网络提供安全服务功能，当一台主机因电源、CPU 等硬件出现故障或软件错误导致异常时，另一台主机继续提供安全服务功能，保证安全功能的可用性。

5.2.2.2.8 数据完整性

网络隔离产品安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

5.2.2.2.9 密码支持

网络隔离产品安全功能应保证其所提供的与密码算法相关功能符合国家密码主管部门的有关规定。

5.2.3 网络单向导入产品

5.2.3.1 基本级要求

5.2.3.1.1 访问控制

5.2.3.1.1.1 信息流控制策略

网络单向导入产品应将数据发送方网络信息流剥离协议，重新封装后单向导入信息接收方网络目的主机。

5.2.3.1.1.2 基本的信息流控制功能

网络单向导入产品的安全功能策略应能够执行以下基本的信息流控制功能，提供明确的访问保障能力和拒绝访问能力。包括：

a) 通过配置单向同步任务的安全属性值，实现明确的源数据向目标数据的单向导入，缺省情况下，网络单向导入产品拒绝任何数据的单向导入；
b) 信息流所包含的源主机 IP 地址、目的主机 IP 地址、服务类型不匹配单向同步任务安全属性值的，明确拒绝访问；
c) 对单向导入的数据内容进行病毒扫描，阻断含病毒数据的导入；
d) 对单向导入的数据内容进行关键字检查，阻断非法数据的导入；
e) 对发送和接收数据流的主体进行身份鉴别，防止非法数据访问；
f) 支持文件单向导入、数据库单向导入等服务类型。

5.2.3.1.1.3 单向传输保证

网络单向导入产品安全功能应通过物理方式构造信息单向传输的唯一通道，实现信息单向导入，即信息只能由一个安全域向另一个安全域传输，并且保证反方向无任何信息传输或反馈。单向传输部件数据发送单元只具有单一的数据发送功能，数据接收单元只具有单一的数据接收功能，不存在可能导致物理特性改变的软、硬件。

5.2.3.1.1.4 残余信息保护

网络单向导入产品在为新创建的单向同步任务分配资源时，安全功能应保证其分配的资源中不提

供以前单向同步任务所产生的任何信息内容。

5.2.3.1.1.5 不可旁路

在与安全有关的操作(例如安全属性的修改、同步任务的建立等)被允许执行之前,网络单向导入产品安全功能应确保其通过安全策略的检查。

5.2.3.1.1.6 数据完整性保证

网络单向导入产品应具备数据单向导入过程的完整性保护功能,在没有任何反馈信息的前提下,保证单向导入的数据完整性。

5.2.3.1.2 抗攻击

网络单向导入产品应能够抵御各种 DoS/DDoS 攻击,应能够识别和防御 SYN Flood、ICMP Flood 等攻击。

5.2.3.1.3 安全管理

5.2.3.1.3.1 区分安全管理角色

网络单向导入产品安全功能:

a) 应将与安全相关的管理功能与其他功能区分开;
b) 应包括安装、配置和管理网络单向导入产品安全功能本身所需的所有功能,其中至少应包括:增加和删除主体(发送信息的主机)和客体(接受信息的主机),查阅安全属性,分配、修改和撤销安全属性,查阅和管理审计数据;
c) 应把执行与安全相关的管理功能的能力限定为一种安全管理职责,该职责具有一套特别授权的功能和响应的责任;
d) 应能把授权执行管理功能的授权管理员与使用隔离部件的所有其他个人或系统分开;
e) 应仅允许授权管理员承担安全管理职责;
f) 应在提出一个明确的请求以后,才会让授权管理员承担安全管理职责。

5.2.3.1.3.2 管理功能

网络单向导入产品安全功能应向授权管理员提供如下管理功能:

a) 设置和更新与安全相关的数据;
b) 能执行网络单向导入产品的初始化、系统启动和关闭、备份和恢复功能,备份能力应有自动工具的支持;
c) 能设置双机热备等可用性参数;
d) 若支持远程管理,则应:
   1) 能限制可进行远程管理的地址;
   2) 能通过加密来保护远程管理会话。

5.2.3.1.3.3 独立管理接口

网络单向导入产品应使用与通讯接口相互独立的管理接口与授权管理员连接,授权管理员经过身份鉴别后,采用多因素身份鉴别和加密方式建立授权管理员与网络隔离产品间的可信路径,禁止其他用户非授权访问管理接口。

5.2.3.1.4 标识和鉴别

5.2.3.1.4.1 安全属性定义

对于每一个授权管理员，网络单向导入产品安全功能应为其提供一套唯一的、为了执行安全功能策略提供的必须的安全属性，包括但不限于：

a) 设备网络参数：包括接口地址、网关地址等；
b) 设备接口属性：接口类型（例如：管理接口、通信接口）、接口速率等；
c) 安全管理参数：管理控制台地址、管理方式（例如：SSH、SSL）等；
d) 安全参数：最大鉴别失败次数、管理空闲超时；
e) 外部可信 IT 产品参数配置：包括时间同步服务器参数、日志服务器参数等；
f) 系统参数：日志存储空间大小、设备名称等；
g) 用户角色属性：授权管理员、授权审计员、授权用户等；
h) 用户管理属性：用户名、用户角色、用户口令等。

5.2.3.1.4.2 属性初始化

网络单向导入产品安全功能应提供使用默认值对授权管理员和主机属性初始化的功能。

5.2.3.1.4.3 属性修改

网络单向导入产品安全功能应仅向授权管理员提供修改下述（包括但不限于）参数的功能：

a) 标识与角色（例如：配置管理员等）的关系；
b) 主体（数据采集方）和客体（数据接收方）的安全属性值；
c) 配置的安全参数（例如：最大鉴别失败次数等数据）。

5.2.3.1.4.4 属性查询

网络单向导入产品安全功能应仅向授权管理员提供以下查询功能：

a) 标识和角色的关系；
b) 主体（数据采集方）和客体（数据接收方）的安全属性值；
c) 配置的各安全参数。

5.2.3.1.4.5 鉴别数据初始化

网络单向导入产品安全功能应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.2.3.1.4.6 鉴别时机

在所有授权管理员请求执行的任何操作之前，网络单向导入产品安全功能应确保对每个授权管理员进行身份鉴别。

5.2.3.1.4.7 最少反馈

当进行鉴别时，网络单向导入产品安全功能应仅将最少的反馈提供给用户。

5.2.3.1.4.8 鉴别失败处理

在经过一定次数的鉴别失败以后，网络单向导入产品安全功能应能终止进行登录尝试主机建立会

话的过程。最多失败次数仅由授权管理员设定。

5.2.3.1.4.9 超时重鉴别

网络单向导入产品应具有登录超时锁定或注销功能。在设定的时间段内没有任何操作的情况下，终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

5.2.3.1.4.10 抗重放

网络单向导入产品的鉴别机制应具有抗重放的能力，授权管理员及其他用户不能复制使用上一次通过的鉴别信息再次鉴别成功。

5.2.3.1.4.11 保护的鉴别反馈

网络单向导入产品的授权管理员在鉴别过程中输入的口令等敏感信息应以不可见和不可推理的形式显示在鉴别信息的登录输入界面中。

5.2.3.1.5 审计

5.2.3.1.5.1 审计数据生成

网络单向导入产品安全功能应能对下列可审计事件生成审计记录，包括事件发生的日期和时间，事件的类型，主体身份和成功或失败事件：

a) 审计功能的启动和关闭；
b) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；
c) 任何读取、修改、破坏审计记录的尝试；
d) 所有对访问授权与拒绝规则覆盖的主体执行操作的请求，以及受影响客体的标识；
e) 修改安全属性的所有尝试，以及修改后安全属性的新值；
f) 所有使用安全功能中鉴别数据管理机制的请求；
g) 所有访问鉴别数据的请求，以及访问请求的目标；
h) 任何对鉴别机制的使用；
i) 所有使用标识机制的尝试；
j) 所有对安全功能配置参数的修改(设置和更新)，无论成功与否，以及配置参数的新值。

5.2.3.1.5.2 用户身份关联

网络单向导入产品安全功能应能将每个可审计事件与引起该事件的用户身份相关联。

5.2.3.1.5.3 审计记录管理

网络单向导入产品安全功能应使授权管理员能存档、删除和清空审计记录。

5.2.3.1.5.4 可理解的格式

网络单向导入产品安全功能应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.2.3.1.5.5 限制审计记录访问

网络单向导入产品安全功能应仅允许授权管理员访问审计记录。

5.2.3.1.5.6 可选择查阅审计

网络单向导入产品安全功能应提供能按主体 ID(标识符)、客体 ID、日期、时间以及这些参数的逻辑

组合等参数对审计数据进行查找和排序的审计查阅工具。

5.2.3.1.5.7 防止审计数据丢失

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，网络单向导入产品的开发者应提供相应的分析结果，并且网络单向导入产品安全功能应把生成的审计记录储存于一个永久性的审计记录中，并应限制由于故障和攻击造成的审计事件丢失的数量。

5.2.3.1.6 域隔离

为保护网络单向导入产品安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，网络单向导入产品安全功能应为其自身的执行环境设定一个安全区域，并把网络单向导入产品控制范围内的各个主体（内部或外部网络上的主机）的安全区域分隔开。

5.2.3.1.7 配置数据保护

网络单向导入产品安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

5.2.3.1.8 运行状态监测

网络单向导入产品安全功能应能够实时监测单向导入产品内外网主机的状态，比如 CPU 使用率、内存占用率、存储空间等。

5.2.3.2 增强级要求

5.2.3.2.1 访问控制

5.2.3.2.1.1 信息流控制策略

网络单向导入产品应将数据发送方网络信息流剥离协议，重新封装后单向导入信息接收方网络目的主机。

5.2.3.2.1.2 基本的信息流控制功能

网络单向导入产品的安全功能策略应能够执行以下基本的信息流控制功能，提供明确的访问保障能力和拒绝访问能力。包括：

a) 通过配置单向同步任务的安全属性值，实现明确的源数据向目标数据的单向导入，缺省情况下，网络单向导入产品拒绝任何数据的单向导入；
b) 信息流所包含的源主机 IP 地址、目的主机 IP 地址、服务类型不匹配单向同步任务安全属性值的，明确拒绝访问；
c) 对单向导入的数据内容进行病毒扫描，阻断含病毒数据的导入；
d) 对单向导入的数据内容进行关键字检查，阻断非法数据的导入；
e) 对发送和接收数据流的主体进行身份鉴别，防止非法数据访问；
f) 支持文件单向导入、数据库单向导入等服务类型。

5.2.3.2.1.3 增强的信息流控制功能

网络单向导入产品的安全功能策略应能够执行以下增强的信息流控制功能，提供明确的访问保障能力和拒绝访问能力。包括：

a) **解析多种数据编码格式，识别文件中是否包含非文本型数据，并根据授权管理员配置的安全策**

略进行阻断或放行；

b） 支持文件单向导入、数据库单向导入、邮件单向导入和代理接收单向导入等服务类型；

c） 根据预设的时间周期性定时完成数据的单向导入。

5.2.3.2.1.4 单向传输保证

网络单向导入产品应通过物理方式构造信息单向传输的唯一通道，实现信息单向导入，即信息只能由一个安全域向另一个安全域传输，并且保证反方向无任何信息传输或反馈。单向传输部件数据发送单元只具有单一的数据发送功能，数据接收单元只具有单一的数据接收功能，不存在可能导致物理特性改变的软、硬件。

5.2.3.2.1.5 强制访问控制

网络单向导入产品应能根据单向同步任务的类型构建一个强制访问控制模型，安全功能应能识别用户和应用数据的敏感标记，根据标记执行强制访问控制策略。

5.2.3.2.1.6 残余信息保护

网络单向导入产品在为新创建的单向同步任务分配资源时，安全功能应保证其分配的资源中不提供以前单向同步任务所产生的任何信息内容。

5.2.3.2.1.7 不可旁路

在与安全有关的操作（例如安全属性的修改、同步任务的建立等）被允许执行之前，应确保其通过安全策略的检查。

5.2.3.2.1.8 数据完整性保证

网络单向导入产品应具备数据单向导入过程的完整性保护，在没有任何反馈信息的前提下，保证单向导入的数据完整性。

5.2.3.2.2 抗攻击

网络单向导入产品应能够抵御各种 DoS/DDoS 攻击，应能够识别和防御 SYN Flood、ICMP Flood 等攻击。

5.2.3.2.3 安全管理

5.2.3.2.3.1 区分安全管理角色

网络单向导入产品安全功能：

a） 应将与安全相关的管理功能与其他功能区分开；

b） 应包括安装、配置和管理网络单向导入产品安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），查阅安全属性，分配、修改和撤销安全属性，查阅和管理审计数据；

c） 应把执行与安全相关的管理功能的能力限定为一种安全管理职责，该职责具有一套特别授权的功能和响应的责任；

d） 应能把授权执行管理功能的授权管理员与使用隔离部件的所有其他个人或系统分开；

e） 应仅允许授权管理员承担安全管理职责；

f） 应在提出一个明确的请求以后，才会让授权管理员承担安全管理职责。

5.2.3.2.3.2 管理功能

网络单向导入产品安全功能应向授权管理员提供如下管理功能：

a) 设置和更新与安全相关的数据；
b) 能执行网络单向导入产品的初始化、系统启动和关闭、备份和恢复功能，备份能力应有自动工具的支持；
c) 能设置双机热备等可用性参数；
d) 若支持远程管理，则应：
   1) 能限制可进行远程管理的地址；
   2) 能通过加密来保护远程管理会话。

5.2.3.2.3.3 独立管理接口

网络单向导入产品应使用与通讯接口相互独立的管理接口与授权管理员连接，授权管理员经过身份鉴别后，采用多因素身份鉴别和加密方式建立授权管理员与网络隔离产品间的可信路径，禁止其他用户非授权访问管理接口。

5.2.3.2.4 标识和鉴别

5.2.3.2.4.1 敏感标记

网络单向导入产品安全功能应能维护用户和应用数据的敏感标记，并根据标记执行强访问控制。

5.2.3.2.4.2 安全属性定义

对于每一个授权管理员，网络单向导入产品安全功能应为其提供一套唯一的、为了执行安全功能策略提供的必须的安全属性，包括但不限于：

a) 设备网络参数：包括接口地址、网关地址等；
b) 设备接口属性：接口类型(例如：管理接口、通信接口)、接口速率等；
c) 安全管理参数：管理控制台地址、管理方式(例如：SSH、SSL)等；
d) 安全参数：最大鉴别失败次数、管理空闲超时；
e) 外部可信 IT 产品参数配置：包括时间同步服务器参数、日志服务器参数等；
f) 系统参数：日志存储空间大小、设备名称等；
g) 用户角色属性：授权管理员、授权审计员、授权用户等；
h) 用户管理属性：用户名、用户角色、用户口令等。

5.2.3.2.4.3 属性初始化

网络单向导入产品安全功能应提供用默认值对授权管理员和主机属性初始化的功能。

5.2.3.2.4.4 属性修改

网络单向导入产品安全功能应仅向授权管理员提供修改下述(包含但不仅限于)参数的功能：

a) 标识与角色(例如：配置管理员等)的关系；
b) 主体(数据采集方)和客体(数据接收方)的安全属性值；
c) 配置的安全参数(例如：最大鉴别失败次数等数据)。

5.2.3.2.4.5 属性查询

网络单向导入产品安全功能应仅向授权管理员提供以下查询：

a) 标识和角色的关系；
b) 主体(数据采集方)和客体(数据接收方)的安全属性值；
c) 配置的各安全参数。

5.2.3.2.4.6 鉴别数据初始化

网络单向导入产品安全功能应根据规定的鉴别机制提供授权管理员鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.2.3.2.4.7 鉴别时机

在所有授权管理员请求执行的任何操作之前，网络单向导入产品安全功能应确保对每个授权管理员进行身份鉴别。

5.2.3.2.4.8 最少反馈

当进行鉴别时，网络单向导入产品安全功能应仅将最少的反馈提供给用户。

5.2.3.2.4.9 鉴别失败处理

在经过一定次数的鉴别失败以后，网络单向导入产品安全功能应能终止进行登录尝试主机建立会话的过程。最多失败次数仅由授权管理员设定。

5.2.3.2.4.10 超时重鉴别

网络单向导入产品安全功能应具有登录超时锁定或注销功能。在设定的时间段内没有任何操作的情况下，网络单向导入产品安全功能应终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

5.2.3.2.4.11 多鉴别机制

网络单向导入产品安全功能应提供两种或两种以上的鉴别机制，以支持当发送方网络主体通过网络单向导入产品内置的信息流接收服务发送数据到接收方网络的情况下的用户多重身份鉴别。

5.2.3.2.4.12 抗重放

网络单向导入产品的鉴别机制应具有抗重放的能力，授权管理员及其他用户不能复制使用上一次通过的鉴别信息再次鉴别成功。

5.2.3.2.4.13 保护的鉴别反馈

网络单向导入产品的授权管理员在鉴别过程中输入的口令等敏感信息应以不可见和不可推理的形式显示在鉴别信息的登录输入界面中。

5.2.3.2.4.14 口令强度

网络单向导入产品应采用口令校验机制对授权管理员生成的口令复杂度进行检查，口令强度应保证口令长度大于6位，口令类型为数字＋大小写字母组合。

5.2.3.2.5 审计

5.2.3.2.5.1 审计数据生成

网络单向导入产品安全功能应能对下列可审计事件生成审计记录，包括事件发生的日期和时间，事

件的类型，主体身份和成功或失败事件：

a） 审计功能的启动和关闭；

b） 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；

c） 任何读取、修改、破坏审计记录的尝试；

d） 所有对访问授权与拒绝规则覆盖的主体执行操作的请求，以及受影响客体的标识；

e） 修改安全属性的所有尝试，以及修改后安全属性的新值；

f） 所有使用安全功能中鉴别数据管理机制的请求；

g） 所有访问鉴别数据的请求，以及访问请求的目标；

h） 任何对鉴别机制的使用；

i） 所有使用标识机制的尝试；

j） 所有对安全功能配置参数的修改（设置和更新），无论成功与否，以及配置参数的新值。

5.2.3.2.5.2 用户身份关联

网络单向导入产品安全功能应能将每个可审计事件与引起该事件的用户身份相关联。

5.2.3.2.5.3 审计记录管理

网络单向导入产品安全功能应使授权管理员能存档、删除和清空审计记录。

5.2.3.2.5.4 可理解的格式

网络单向导入产品安全功能应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.2.3.2.5.5 限制审计记录访问

网络单向导入产品安全功能应仅允许授权管理员访问审计记录。

5.2.3.2.5.6 可选择查阅审计

网络单向导入产品安全功能应提供能按主体 ID（标识符）、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.2.3.2.5.7 防止审计数据丢失

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，网络单向导入产品的开发者应提供相应的分析结果，并且网络单向导入产品安全功能应把生成的审计记录储存于一个永久性的审计记录中，并应限制由于故障和攻击造成的审计事件丢失的数量。

5.2.3.2.6 域隔离

5.2.3.2.6.1 基本的域隔离

为保护网络单向导入产品安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，网络单向导入产品安全功能应为其自身的执行环境设定一个安全区域，并把网络单向导入产品控制范围内的各个主体（内部或外部网络上的主机）的安全区域分隔开。

5.2.3.2.6.2 增强的域隔离

为保护网络隔离产品安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，网络单向导入产品安全功能应为其自身的执行环境设定一个安全区域，采用强制访问控制策略，该安全区域被

标记为高安全等级，授权管理员以及网络单向导入产品所覆盖的所有主体（内部或外部网络上的主机）授权后只能读取该区域存储的文件、程序，不能进行删除和修改，授权管理员无法修改访问策略。

5.2.3.2.7 容错

网络单向导入产品应具有主备模式的容错能力，当一台主机因电源、CPU 等硬件出现故障或软件错误导致异常时，容错功能将当前安全服务功能自动切换到另一台备机上继续运行，保证安全功能的可用性。

5.2.3.2.8 配置数据保护

网络单向导入产品安全功能应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏。

5.2.3.2.9 运行状态监测

网络单向导入产品安全功能应能够实时监测单向导入产品内外网主机的状态，比如 CPU 使用率、内存占用率、存储空间等。

5.3 安全保证要求

5.3.1 基本级要求

5.3.1.1 配置管理

5.3.1.1.1 版本号

开发者应为产品的不同版本提供唯一的标识。

5.3.1.1.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效维护的证据。

5.3.1.2 交付与运行

5.3.1.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

5.3.1.2.2 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

5.3.1.3 开发

5.3.1.3.1 非形式化功能规格说明

开发者应提供一个功能规格说明，功能规格说明应满足以下要求：

a） 使用非形式化风格来描述产品安全功能及其外部接口；

b） 是内在一致的；

c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；
d) 完备地表示产品安全功能。

5.3.1.3.2 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：
a) 表示应是非形式化的；
b) 是内在一致的；
c) 按子系统描述安全功能的结构；
d) 描述每个安全功能子系统所提供的安全功能性；
e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
f) 标识安全功能子系统的所有接口；
g) 标识安全功能子系统的哪些接口是外部可见的。

5.3.1.3.3 非形式化对应性证实

开发者应提供产品安全功能表示的所有相邻对之间的对应性分析。

对于产品安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备地细化。

5.3.1.4 指导性文档

5.3.1.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：
a) 管理员可使用的管理功能和接口；
b) 怎样安全地管理产品；
c) 在安全处理环境中应被控制的功能和权限；
d) 所有对与产品的安全操作有关的用户行为的假设；
e) 所有受管理员控制的安全参数，如果可能，应指明安全值；
f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；
g) 所有与管理员有关的 IT 环境安全要求。

5.3.1.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：
a) 产品的非管理员用户可使用的安全功能和接口；
b) 产品提供给用户的安全功能和接口的使用方法；
c) 用户可获取但应受安全处理环境所控制的所有功能和权限；
d) 产品安全操作中用户所应承担的职责；
e) 与用户有关的 IT 环境的所有安全要求。

5.3.1.5 测试

5.3.1.5.1 测试覆盖

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规格说明中所描述的产品的安全功能是对应的。

5.3.1.5.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a) 测试计划，应标识要测试的安全功能，并描述测试的目标；

b) 测试过程，应标识要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；

c) 预期的测试结果，应表明测试成功后的预期输出；

d) 实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。

5.3.1.5.3 独立测试

5.3.1.5.3.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.3.1.5.3.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

5.3.1.6 脆弱性评定

5.3.1.6.1 产品安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

5.3.1.6.2 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。

5.3.2 增强级要求

5.3.2.1 配置管理

5.3.2.1.1 部分配置管理自动化

配置管理系统应提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变。

配置管理计划应描述在配置管理系统中所使用的自动工具，并描述在配置管理系统中如何使用自动工具。

5.3.2.1.2 配置管理能力

5.3.2.1.2.1 版本号

开发者应为产品的不同版本提供唯一的标识。

5.3.2.1.2.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效维护的证据。

5.3.2.1.2.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

开发者应提供所有的配置项得到有效地维护的证据，并应保证只有经过授权才能修改配置项。

5.3.2.1.2.4 产生支持和接受程序

开发者提供的配置管理文档应包括一个接受计划，接受计划应描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

配置管理系统应支持产品的生成。

5.3.2.1.3 配置管理范围

5.3.2.1.3.1 配置管理覆盖

配置管理范围至少应包括产品实现表示、设计文档、测试文档、指导性文档、配置管理文档，从而确保它们的修改是在一个正确授权的可控方式下进行的。

配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

5.3.2.1.3.2 问题跟踪配置管理覆盖

配置管理范围应包括安全缺陷，确保安全缺陷置于配置管理系统之下。

5.3.2.2 交付与运行

5.3.2.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

5.3.2.2.2 修改检测

交付文档应描述如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方所收到版本之间的任何差异。还应描述如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付产品。

5.3.2.2.3 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

5.3.2.3 开发

5.3.2.3.1 功能规格说明

5.3.2.3.1.1 非形式化功能规格说明

开发者应提供一个功能规格说明，功能规格说明应满足以下要求：

a) 使用非形式化风格来描述产品安全功能及其外部接口；
b) 是内在一致的；
c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；
d) 完备地表示产品安全功能。

5.3.2.3.1.2 充分定义的外部接口

功能规格说明应包括安全功能是完备地表示的合理性。

5.3.2.3.2 高层设计

5.3.2.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：
a) 表示应是非形式化的；
b) 是内在一致的；
c) 按子系统描述安全功能的结构；
d) 描述每个安全功能子系统所提供的安全功能性；
e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
f) 标识安全功能子系统的所有接口；
g) 标识安全功能子系统的哪些接口是外部可见的。

5.3.2.3.2.2 安全加强的高层设计

开发者提供的安全加强的高层设计应满足以下要求：
a) **描述产品的功能子系统所有接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；**
b) **把产品分成安全策略实施和其他子系统来描述。**

5.3.2.3.3 安全功能实现的子集

开发者应为选定的安全功能子集提供实现表示。实现表示应当无歧义而且详细地定义安全功能，使得无须进一步设计就能生成安全功能。实现表示应是内在一致的。

5.3.2.3.4 描述性低层设计

开发者应提供产品安全功能的低层设计，低层设计应满足以下要求：
a) **表示应是非形式化的；**
b) **是内在一致的；**
c) **按模块描述安全功能；**
d) **描述每个模块的用途；**
e) **根据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系；**
f) **描述每个安全策略实施功能是如何被提供的；**
g) **标识安全功能模块的所有接口；**
h) **标识安全功能模块的哪些接口是外部可见的；**
i) **描述安全功能模块所有接口的用途和用法，适当时应提供效果、例外情况和错误消息的细节；**
j) **把产品分为安全策略实施模块和其他模块来描述。**

5.3.2.3.5 非形式化对应性证实

开发者应提供产品安全功能表示的所有相邻对之间的对应性分析。

对于产品安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备地细化。

5.3.2.3.6 非形式化产品安全策略模型

开发者应提供安全策略模型，安全策略模型应满足以下要求：

a) **表示应是非形式化的；**

b) **描述所有能被模型化的安全策略的规则与特征；**

c) **应包含合理性，即论证该模型相对所有能被模型化的安全策略来说是一致的，而且是完备的；**

d) **应阐明安全策略模型和功能规格说明之间的对应性，即论证所有功能规格说明中的安全功能对于安全策略模型来说是一致的，而且是完备的。**

5.3.2.4 指导性文档

5.3.2.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可使用的管理功能和接口；

b) 怎样安全地管理产品；

c) 在安全处理环境中应被控制的功能和权限；

d) 所有对与产品的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；

g) 所有与管理员有关的 IT 环境安全要求。

5.3.2.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；

b) 产品提供给用户的安全功能和接口的使用方法；

c) 用户可获取但应受安全处理环境所控制的所有功能和权限；

d) 产品安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

5.3.2.5 生命周期支持

5.3.2.5.1 安全措施标识

开发者应提供开发安全文档。

开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，并应提供在产品的开发和维护过程中执行安全措施的证据。

5.3.2.5.2 开发者定义的生命周期模型

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

5.3.2.5.3 明确定义的开发工具

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

5.3.2.6 测试

5.3.2.6.1 测试覆盖

5.3.2.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规格说明中所描述的产品的安全功能是对应的。

5.3.2.6.1.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与功能规格说明中所描述的产品的安全功能之间的对应性是完备的。

5.3.2.6.2 测试：高层设计

开发者应提供测试深度的分析。

深度分析应证实测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

5.3.2.6.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a) 测试计划，应标识要测试的安全功能，并描述测试的目标；

b) 测试过程，应标识要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；

c) 预期的测试结果，应表明测试成功后的预期输出；

d) 实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。

5.3.2.6.4 独立测试

5.3.2.6.4.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.3.2.6.4.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

5.3.2.7 脆弱性评定

5.3.2.7.1 误用

5.3.2.7.1.1 指南审查

开发者应提供指导性文档，指导性文档应满足以下要求：

a) **标识所有可能的产品运行模式（包括失败或操作失误后的运行）、它们的后果以及对于保持安全运行的意义；**

b) **是完备的、清晰的、一致的、合理的；**

c) **列出关于预期使用环境的所有假设；**

d) **列出对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。**

5.3.2.7.1.2 分析确认

开发者应提供分析文档论证指导性文档是完备的。

5.3.2.7.2 产品安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

5.3.2.7.3 脆弱性分析

5.3.2.7.3.1 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。

5.3.2.7.3.2 独立的脆弱性分析

开发者应提供文档证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

5.3.2.7.3.3 中级抵抗力

开发者应提供文档证明产品可以抵御中级强度的穿透性攻击，并提供证据说明对脆弱性的搜索是系统化的。

5.4 环境适应性要求

5.4.1 下一代互联网支持（有则适用）

5.4.1.1 支持纯 IPv6 网络环境

网络隔离产品/网络单向导入产品应支持纯 IPv6 网络环境，能够在纯 IPv6 网络环境下正常工作。

5.4.1.2 协议一致性

5.4.1.2.1 IPv6 Core 协议一致性

网络隔离产品/网络单向导入产品应支持 IPv6 Core 协议一致性。

5.4.1.2.2 IPv6 NDP 协议一致性

网络隔离产品/网络单向导入产品应支持 IPv6 NDP 协议一致性。

5.4.1.2.3 IPv6 Autoconfig 协议一致性

网络隔离产品/网络单向导入产品应支持 IPv6 Autoconfig 协议一致性。

5.4.1.2.4 IPv6 PMTU 协议一致性

网络隔离产品/网络单向导入产品应支持 IPv6 PMTU 协议一致性。

5.4.1.2.5 ICMPv6 协议一致性

网络隔离产品/网络单向导入产品应支持 ICMPv6 协议一致性。

5.4.1.3 协议健壮性

网络隔离产品/网络单向导入产品应保证协议的健壮性，能够抵御 IPv6 网络环境下畸形协议报文攻击。畸形协议报文包括：

a) IPv6 畸形报文；
b) ICMPv6 畸形报文；
c) 其他协议畸形报文。

5.4.1.4 IPv6 网络环境下自身管理

网络隔离产品/网络单向导入产品应支持在 IPv6 网络环境下自身管理。

5.4.2 支持 IPv6 过渡网络环境(可选)

5.4.2.1 双协议栈

网络隔离产品/网络单向导入产品应支持 IPv4/IPv6 双栈网络环境，能够在 IPv4/IPv6 双栈网络环境下正常工作。

5.4.2.2 协议转换

网络隔离产品/网络单向导入产品应支持将 IPv4 和 IPv6 两种网络相互转换，能够在协议转换网络环境下正常工作。

5.4.2.3 隧道

5.4.2.3.1 6over4

网络隔离产品/网络单向导入产品应支持 6over4 网络环境，能够在 6over4 网络环境下正常工作。

5.4.2.3.2 6to4

网络隔离产品/网络单向导入产品应支持 6to4 网络环境，能够在 6to4 网络环境下正常工作。

5.4.2.3.3 ISATAP

网络隔离产品/网络单向导入产品应支持 ISATAP 网络环境，保证在 ISATAP 网络环境下正常工作。

5.5 性能要求

5.5.1 交换速率

网络隔离产品的交换速率应大于 1 000 Mbit/s。

5.5.2 硬件切换时间

网络隔离产品的硬件切换时间应小于 5 ms。

参 考 文 献

[1] GB/T 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型(ISO/IEC 15408-1:2005,IDT)

[2] GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求(ISO/IEC 15408-2:2005,IDT)

[3] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[4] GA 370—2001 端设备隔离部件安全技术要求