ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20277—2015
代替 GB/T 20277—2006

信息安全技术　网络和终端隔离产品测试评价方法

Information security technology—Testing and evaluation approaches 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。

本标准代替 GB/T 20277—2006《信息安全技术　网络和终端设备隔离部件测试评价方法》。

本标准与 GB/T 20277—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；

——增加了下一代互联网协议支持能力的测试内容。

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。

本标准所代替标准的历次版本发布情况：

——GB/T 20277—2006。

信息安全技术　网络和终端隔离产品测试评价方法

1　范围

本标准依据 GB/T 20279—2015 的技术要求，规定了网络和终端隔离产品的测试评价方法。

本标准适用于按照 GB/T 20279—2015 的安全等级要求所开发的网络和终端隔离产品的测试和评价。

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 20279—2015　信息安全技术　网络和终端隔离产品安全技术要求

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB 17859—1999、GB/T 25069—2010 和 GB/T 20279—2015 界定的术语和定义适用于本文件。

4　测试环境与工具

4.1　安全功能与环境适应性测试环境

4.1.1　终端隔离产品

安全功能与环境适应性测试环境参见图 1。

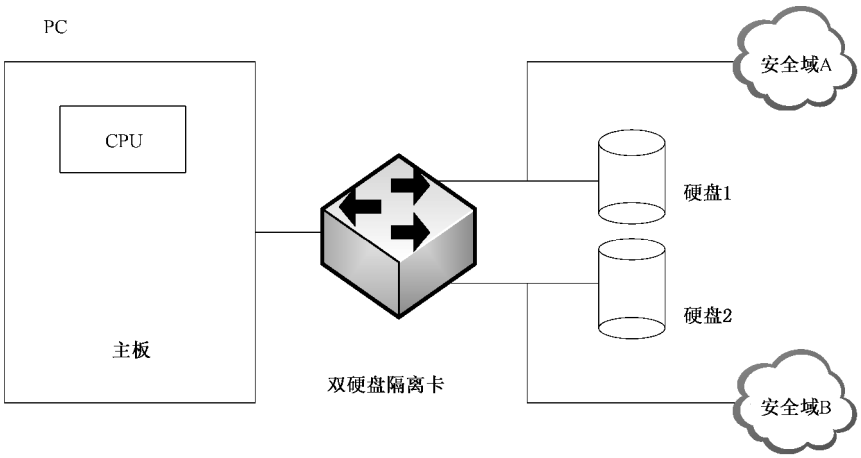

图 1　终端隔离产品安全功能及环境适用性测试环境图

4.1.2 网络隔离产品

安全功能与环境适应性测试环境参见图 2。

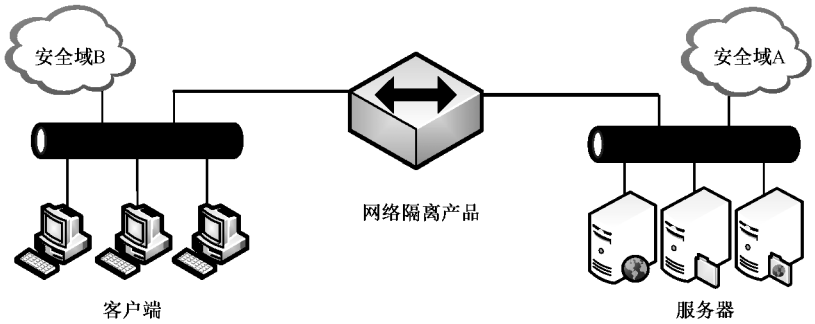

图 2 网络隔离产品安全功能与环境适用性测试环境图

4.1.3 网络单向导入产品

安全功能与环境适应性测试环境参见图 3。

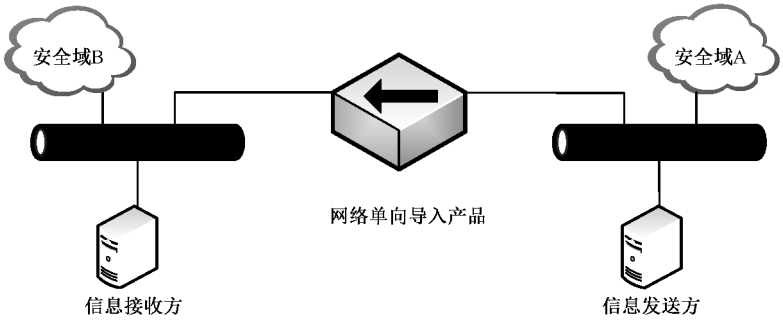

图 3 网络单向导入产品安全功能与环境适用性测试环境图

4.2 性能测试环境

性能测试环境参见图 4,采用专用性能测试仪,测试仪接口直接通过网线连接网络和终端隔离产品业务接口。

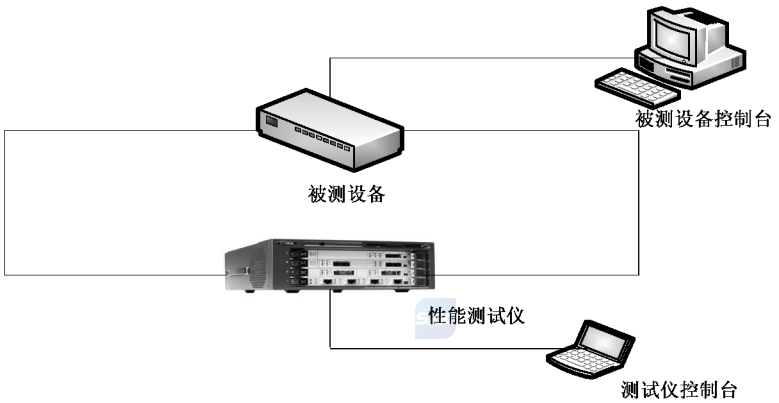

图 4 性能测试环境图

5 安全功能测试

5.1 总体说明

5.1.1 测试评价方法分类

本标准依据 GB/T 20279—2015 的技术要求，将网络和终端隔离产品测试与评价方法要求分为安全功能、安全保证、环境适应性和性能要求四个大类。

5.1.2 安全等级

与 GB/T 20279—2015 相对应，本标准将安全等级分为基本级和增强级。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 终端隔离产品

5.2.1 基本级测试

5.2.1.1 访问控制

5.2.1.1.1 安全属性定义

终端隔离产品的安全属性定义的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，对于信息存储与传输部件，终端隔离产品所必需的安全属性，并且说明具体的内容。测试产品的安全属性定义，记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

产品应能够设定安全属性，应至少包括不同安全域网络切换方式、光驱和软驱等存储设备处在哪个安全区域、网络设备接入方式和其他在开发者文档中提及的安全属性。

5.2.1.1.2 属性修改

终端隔离产品的属性修改的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括属性修改的详细描述。对安全属性进行修改操作，测试产品修改与安全相关属性的参数的功能，包括安全域网络切换。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

产品应能够修改与安全相关属性的参数，应至少包括安全域网络切换。

5.2.1.1.3 属性查询

终端隔离产品的属性查询的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供文档，说明属性查询的详细描述。对安全属性进行查询操作，测试终端隔离产品用户对安全属性的查询功能，包括对一个安全域网络状态进行查询。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

终端隔离产品用户应能够进行安全属性的查询，应至少包括对一个安全域网络状态进行查询。

5.2.1.1.4 访问授权与拒绝

终端隔离产品的访问授权与拒绝的测试评价方法和预期结果如下：

a) 测试评价方法：

依据开发者所提供的访问授权与拒绝的详细描述进行测试：

1) 信息物理传导隔断测试：当终端隔离产品状态为安全域 A 网络状态时，尝试跟安全域 A 网络和安全域 B 网络进行连接，产品保证跟安全域 A 网络主机可以互相访问，跟安全域 B 网络主机互相不可访问；当终端隔离产品状态为安全域 B 网络状态时，尝试跟安全域 A 网络和安全域 B 网络进行连接，产品保证跟安全域 B 网络主机可以互相访问，跟安全域 A 网络主机互相不可访问；

2) 信息物理存储隔断测试：测试对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，在网络转换时作清零处理的功能；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，安全域 A 网络与安全域 B 网络信息以不同存储设备分开存储，比如硬盘，终端隔离产品分别为安全域 A 网络与安全域 B 网络准备一个独立的硬盘；对移动存储介质，如光盘、软盘、USB 硬盘等，在网络转换前提示用户干预或禁止在双网都能使用这些设备；

3) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

1) 信息物理传导隔断测试：当终端隔离产品状态为安全域 A 网络状态时，尝试跟安全域 A 网络和安全域 B 网络进行连接，产品应保证跟安全域 A 网络主机可以互相访问，跟安全域 B 网络主机互相不可访问；当终端隔离产品状态为安全域 B 网络状态时，尝试跟安全域 A 网络和安全域 B 网络进行连接，产品应保证跟安全域 B 网络主机可以互相访问，跟安全域 A 网络主机互相不可访问；

2) 信息物理存储隔断测试：对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，应在网络转换时作清零处理；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，安全域 A 网络与安全域 B 网络信息应以不同存储设备分开存储，比如硬盘，终端隔离产品应分别为安全域 A 网络与安全域 B 网络准备一个独立的硬盘；对移动存储介质，如光盘、软盘、USB 硬盘等，应在网络转换前提示用户干预或禁止在双网都能使用这些设备。

5.2.1.1.5 切换信号一致性

终端隔离产品的切换信号一致性的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括切换信号一致性的详细描述。测试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，确保一致性的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.2.1.1.6 口令保护

终端隔离产品的口令保护的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括口令保护的详细描述。测试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保证用户必须输入切换口令，并通过猜测口令验证口令保护的有效性的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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保证应保证用户必须输入切换口令。

5.2.1.1.7 内存及 USB 端口的物理隔离

终端隔离产品的内存及 USB 端口的物理隔离的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括内存及 USB 端口的物理隔离的详细描述。若终端隔离产品以整机隔离系统的形态存在，测试终端隔离产品的安全功能能够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。通过观察硬件配置信息验证隔离的有效性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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能够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 不可旁路

终端隔离产品的不可旁路的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括不可旁路的详细描述。测试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确保其通过安全功能策略的检查。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.2.1.3 客体重用

终端隔离产品的客体重用的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括客体重用的详细描述。测试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能够保证不提供以前连接的任何信息内容的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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 增强级测试

5.2.2.1 访问控制

5.2.2.1.1 安全属性定义

终端隔离产品的安全属性定义的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，对于信息存储与传输部件，终端隔离产品所必需的安全属性，并且说明具体的内容。测试产品的安全属性定义，记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

产品应能够设定安全属性，应至少包括不同安全域网络切换方式、光驱和软驱等存储设备处在哪个安全区域、网络设备接入方式和其他在开发者文档中提及的安全属性。

5.2.2.1.2 属性修改

终端隔离产品的属性修改的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性修改的详细描述。对安全属性进行修改操作，测试产品修改与安全相关属性的参数的功能，包括安全域网络切换。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

产品应能够修改与安全相关属性的参数，应至少包括安全域网络切换。

5.2.2.1.3 属性查询

终端隔离产品的属性查询的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供文档，说明属性查询的详细描述。对安全属性进行查询操作，测试终端隔离产品用户对安全属性的查询功能，包括对一个安全域网络状态进行查询。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

终端隔离产品用户应能够进行安全属性的查询，应至少包括对一个安全域网络状态进行查询。

5.2.2.1.4 访问授权与拒绝

终端隔离产品的访问授权与拒绝的测试评价方法和预期结果如下：

a） 测试评价方法：

依据开发者所提供的访问授权与拒绝的详细描述进行测试：

1） 信息物理传导隔断测试：当终端隔离产品状态为安全域 A 网络状态时，尝试跟安全域 A 网络和安全域 B 网络进行连接，产品保证跟安全域 A 网络主机可以互相访问，跟安全域 B 网络主机互相不可访问；当终端隔离产品状态为安全域 B 网络状态时，尝试跟安全域 A 网络和安全域 B 网络进行连接，产品保证跟安全域 B 网络主机可以互相访问，跟安全域 A 网络主机互相不可访问；

2） 信息物理存储隔断测试：测试对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，在网络转换时作清零处理的功能；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，安全域 A 网络与安全域 B 网络信息以不同存储设备分开存储，比如硬盘，终端隔离产品分别为安全域 A 网络与安全域 B 网络准备一个独立的硬盘；对移动存储介质，如光盘、软盘、USB 硬盘等，在网络转换前提示用户干预或禁止在双网都能使用这些设备；

3） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

1） 信息物理传导隔断测试：当终端隔离产品状态为安全域 A 网络状态时，尝试跟安全域 A

网络和安全域B网络进行连接，产品应保证跟安全域A网络主机可以互相访问，跟安全域B网络主机互相不可访问；当终端隔离产品状态为安全域B网络状态时，尝试跟安全域A网络和安全域B网络进行连接，产品应保证跟安全域B网络主机可以互相访问，跟安全域A网络主机互相不可访问；

2） 信息物理存储隔断测试：对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，应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，安全域A网络与安全域B网络信息应以不同存储设备分开存储，比如硬盘，终端隔离产品应分别为安全域A网络与安全域B网络准备一个独立的硬盘；对移动存储介质，如光盘、软盘、USB硬盘等，应在网络转换前提示用户干预或禁止在双网都能使用这些设备。

5.2.2.1.5 网络非法外联

终端隔离产品的网络非法外联的测试评价方法和预期结果如下：

a） **测试评价方法：**

评估开发者提供文档，包括网络非法外联的详细描述。模拟非法外联事件的产生，测试终端隔离产品的安全功能能够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，一旦发现是否立即禁用网络并给出报警的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） **预期结果：**

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，一旦发现应立即禁用网络并给出报警，确保内网安全。

5.2.2.1.6 切换信号一致性

终端隔离产品的切换信号一致性的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括切换信号一致性的详细描述。测试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，确保一致性的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.2.2.1.7 硬盘非法调换

终端隔离产品的硬盘非法调换的测试评价方法和预期结果如下：

a） **测试评价方法：**

评估开发者提供的文档，是否包括硬盘非法调换的详细描述。测试终端隔离产品的安全功能能够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关系，确保内网硬盘数据的安全。模拟调换被测系统的硬盘，检查保护措施的有效性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） **预期结果：**

终端隔离产品的安全功能应能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关系，确保内网硬盘数据的安全。

5.2.2.1.8 口令保护

终端隔离产品的口令保护的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括口令保护的详细描述。测试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保证用户必须输入切换口令，并通过猜测口令验证口令保护的有效性的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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保证应保证用户必须输入切换口令。

5.2.2.1.9 内存及 USB 端口的物理隔离

终端隔离产品的内存及 USB 端口的物理隔离的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括内存及 USB 端口的物理隔离的详细描述。若终端隔离产品以整机隔离系统的形态存在，测试终端隔离产品的安全功能能够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。通过观察硬件配置信息验证隔离的有效性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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能够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。

5.2.2.2 不可旁路

终端隔离产品的不可旁路的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括不可旁路的详细描述。测试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确保其通过安全功能策略的检查。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.2.2.3 客体重用

终端隔离产品的客体重用的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括客体重用的详细描述。测试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能够保证不提供以前连接的任何信息内容的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.3 网络隔离产品

5.3.1 基本级测试

5.3.1.1 访问控制

5.3.1.1.1 基本的信息流控制策略

网络隔离产品的基本的信息流控制策略的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 评估开发者提供的文档，包括基本的信息流控制策略的详细描述。模拟生成设备所支持的信息流，测试对主体、客体以及经过网络隔离产品的主客体之间的所有操作，网络隔离产品基本的信息流控制策略能够执行以下端到端基本的信息流控制策略：

——所有主客体之间发送和接收的信息流是否执行了网络层协议剥离，查看还原成为应用层数据的能力；

——主客体之间发送和接收的信息流经过了安全策略允许后传输；

——授权管理员与网络隔离产品间发送的管理信息经过了安全策略允许后传输；

2) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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，网络隔离产品基本的信息流控制策略应能够执行以下端到端基本的信息流控制策略：

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

2) 主客体之间发送和接收的信息流应经过安全策略允许后传输；

3) 授权管理员与网络隔离产品间发送的管理信息应经过安全策略允许后传输。

5.3.1.1.2 基本的信息流控制功能

网络隔离产品的基本的信息流控制功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 评估开发者提供的文档，包括基本的信息流控制功能的详细描述。模拟生成设备所支持的信息流，测试网络隔离产品安全功能策略可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：

——网络隔离产品是否可通过配置 ACL 访问控制列表进行信息流控制，ACL 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；

——网络隔离产品可对经过的 HTTP、FTP、SMTP、POP3 等应用协议信息流进行合规性检查；

——网络隔离产品可对经过的 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；

——网络隔离产品可对经过的 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；

——网络隔离产品可通过协议隔离方式断开内部 TCP/IP 连接，完成信息传输；

2) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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

1） 网络隔离产品应可通过配置 ACL 访问控制列表进行信息流控制，ACL 访问控制列表的元素应包括：源 IP 地址、目的 IP 地址、源端口、目的端口、协议号；
2） 网络隔离产品应可对经过的 HTTP、FTP、SMTP、POP3 等应用协议信息流进行合规性检查；
3） 网络隔离产品应可对经过的 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；
4） 网络隔离产品应可对经过的 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；
5） 网络隔离产品应可通过协议隔离方式断开内部 TCP/IP 连接，完成信息摆渡传输。

5.3.1.1.3 残余信息保护

网络隔离产品的残余信息保护的测试评价方法和预期结果如下：

a） 测试评价方法：
评估开发者提供的文档，包括残余信息保护的详细描述。测试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能够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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：
网络隔离产品安全功能应能够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。

5.3.1.1.4 不可旁路

网络隔离产品的不可旁路的测试评价方法和预期结果如下：

a） 测试评价方法：
评估开发者提供的文档，包括不可旁路保护的详细描述。审查文档并且验证其是否真实。提供文档说明网络隔离产品采用何种机制和措施，确保安全策略的不可旁路性，即任何与安全有关的操作被允许执行之前，都必须通过安全策略的检查。文档应该分析并确认，网络隔离产品确实控制了端设备用户的每次访问请求，不存在其他可能旁路网络隔离产品的途径。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：
产品应不存在其他可能旁路网络隔离产品的途径。

5.3.1.2 抗攻击

网络隔离产品的抗攻击的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 配置启用网络隔离产品抗攻击功能；
2） 采用模拟攻击设备，通过网络隔离产品，发起产品声明支持带宽 10％的攻击流量（至少包括 SYN Flood、ICMP Flood 等），同时通过网络隔离产品建立正常的传输业务，持续时间 1 min；
3） 检查拒绝服务攻击包通过的比例，以及正常业务成功建立的比例。

b） 预期结果：
1） 网络隔离产品具备抗拒绝服务器攻击能力；
2） 攻击包通过的比例不大于 5％、正常业务建立成功率不低于 90％。

5.3.1.3 安全管理

5.3.1.3.1 区分安全管理角色

网络隔离产品的区分安全管理角色的测试评价方法和预期结果如下：

a) 测试评价方法：

依据开发者所提供的区分安全管理角色的详细描述进行测试：

1) 产品至少提供两类用户角色，至少有一类为管理员角色，保证此两类用户角色并不相同。评价者测试此两类用户角色是否不同，且有一类属于管理员角色；

2) 创建一未授予安全管理角色的普通用户，以此用户执行安全管理功能相关操作，网络隔离产品拒绝其操作；

3) 将安全管理角色授与此用户，再次执行安全管理功能的相关操作（应包括安装、配置和管理网络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），测试网络隔离产品是否允许其操作；

4) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

1) 产品应至少提供两类用户角色，至少有一类为管理员角色，保证此两类用户角色并不相同；

2) 网络隔离产品应拒绝未授予安全管理角色的普通用户执行安全管理功能相关操作；

3) 将安全管理角色授与此用户，再次执行安全管理功能的相关操作（应包括安装、配置和管理网络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），网络隔离产品应允许其操作。

5.3.1.3.2 管理功能

网络隔离产品的管理功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 评估开发者提供的文档，包括管理功能的详细描述。以授权管理员身份登录，测试能够进行如下操作：

——设置和更新与安全相关的数据；

——网络隔离产品的安装及初始化；

——系统启动和关闭；

——备份和恢复系统配置信息。

2) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络隔离产品应能执行上述操作，并且网络隔离产品的各种备份（如安全配置的备份，审计记录的备份）工作可以通过自动工具完成。如果网络隔离产品支持外部或内部接口的远程管理，尝试关闭内部和外部接口或其中之一及配置远程管理地址，网络隔离产品应允许这些操作的执行；从未授权远程管理的主机地址，尝试进行远程管理，网络隔离产品应予以拒绝；远程管理会话应进行加密保护。

5.3.1.3.3 独立管理接口

网络隔离产品的独立管理接口的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括独立管理接口的详细描述。测试网络隔离产品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，是否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，是否禁止其他用户非授权访问管理接口。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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，应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，应禁止其他用户非授权访问管理接口。

5.3.1.4 标识和鉴别

5.3.1.4.1 基本安全属性定义

网络隔离产品的基本安全属性定义的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括对于每一个授权管理员、构成系统的信息传输与控制部件、应用层数据采集与接受部件，网络隔离产品为其提供一套唯一的、为了执行安全功能策略所必需的安全属性，并且说明具体的内容。测试产品是否设定了这些安全属性，至少包括授权管理员的安全属性、构成系统的信息传输与控制部件的安全属性、应用层数据采集与接受部件的安全属性和其他在开发者文档中提及的安全属性。如果产品设定规定范围内的安全属性和开发者文档中存在的安全属性，则此项判定为合格。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

产品应设定至少包括授权管理员的安全属性、构成系统的信息传输与控制部件的安全属性、应用层数据采集与接受部件的安全属性和其他在开发者文档中提及的安全属性。

5.3.1.4.2 属性初始化

网络隔离产品的属性初始化的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性初始化的详细描述。按照开发者提供的初始化方法进行初始化，审查初始化结果是否与文档宣称的初始化值一致。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

测试结果应完全符合上述测试评价方法要求做出判断，测试和审查的初始化过程和结果应符合文档说明。

5.3.1.4.3 属性修改

网络隔离产品的属性修改的测试评价方法和预期结果如下：

a） 测试评价方法：

依据开发者提供的属性修改的详细描述进行测试：

1） 测试能以授权管理员的身份对源地址、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）和配置的安全参数（至少包括：最大鉴别失败次数等数据）进行修改；

2） 测试修改后的设置是否有效；

3） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

1） 应能以授权管理员的身份对源地址、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）和配置的安全参数（至少包括：最大鉴别失败次数等数据）进行修改；

2） 修改后的设置应能够生效。

5.3.1.4.4 属性查询

网络隔离产品的属性查询的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性查询的详细描述。测试能以授权管理员的身份对源地址、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）和配置的安全参数（至少包括：最大鉴别失败次数等数据）进行查询。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

应能以授权管理员的身份对源地址、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）和配置的安全参数（至少包括：最大鉴别失败次数等数据）进行查询。

5.3.1.4.5 鉴别数据初始化

网络隔离产品的鉴别数据初始化的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。根据开发者提供的网络隔离产品鉴别机制的详细描述，分别以授权管理员和普通用户的身份登录，测试该部件是否提供鉴别数据的初始化功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

以授权管理员和普通用户的身份登录网络隔离产品，产品应提供鉴别数据的初始化功能。

5.3.1.4.6 鉴别时机

网络隔离产品的鉴别时机的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。设置多个授权管理员，分别以所有这些授权管理员的身份登录，测试在所有授权管理员请求执行的任何操作之前，网络隔离产品对每个授权管理员都进行了身份鉴别。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

在所有授权管理员请求执行的任何操作之前，网络隔离产品应对每个授权管理员都进行身份鉴别。

5.3.1.4.7 最少反馈

网络隔离产品的最少反馈的测试评价方法和预期结果如下：

a) 测试评价方法：
评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。分别以授权管理员和普通用户的身份登录，并且输入正确或者错误的口令，测试网络隔离产品的反馈信息最少。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：
分别以授权管理员和普通用户的身份登录，并且输入正确或者错误的口令，网络隔离产品应反馈最少的信息。

5.3.1.4.8 鉴别失败处理

网络隔离产品的鉴别失败处理的测试评价方法和预期结果如下：

a) 测试评价方法：
评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。以错误的用户名—口令登录，在一定次数的鉴别失败后，测试网络隔离产品终止了进行登录尝试主机建立会话的过程。分别以授权管理员和普通用户的身份登录，测试该部件提供最多失败次数的设定功能，且最多失败次数仅由授权管理员设定。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：
以错误的用户名—口令登录，在一定次数的鉴别失败后，网络隔离产品应能够终止进行登录尝试主机建立会话的过程。分别以授权管理员和普通用户的身份登录，产品应提供最多失败次数的设定功能，且最多失败次数应仅由授权管理员设定。

5.3.1.5 审计

5.3.1.5.1 审计数据生成

网络隔离产品的审计数据生成的测试评价方法和预期结果如下：

a) 测试评价方法：
评估开发者提供的文档，包括评价所需的相关文档(例如：产品说明书产品测试文档)。根据开发者文档，使用不同角色用户模拟对产品不同模块进行访问、运行、修改、关闭以及重复失败尝试等相关操作。审查审计记录的正确性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：
网络隔离产品应能够准确记录不同角色用户对产品不同模块进行访问、运行、修改、关闭以及重复失败尝试等相关操作。

5.3.1.5.2 审计记录管理

网络隔离产品的审计记录管理的测试评价方法和预期结果如下：

a) 测试评价方法：
评估开发者提供的文档，包括评价所需的相关文档(例如：产品说明书产品测试文档)。模拟授权管理员进行审计操作，测试网络隔离产品安全功能允许授权管理员存档、删除和清空审计记录。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：
网络隔离产品应能够允许授权管理员存档、删除和清空审计记录。

5.3.1.5.3 可理解的格式

网络隔离产品的可理解的格式的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括评价所需的相关文档(例如：产品说明书产品测试文档)。审查网络隔离产品安全功能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(至少包括能为人理解的描述内容以及审计数据本身)。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络隔离产品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(至少包括能为人理解的描述内容以及审计数据本身)。

5.3.1.5.4 限制审计记录访问

网络隔离产品的限制审计记录访问的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，是否包括评价所需的相关文档(例如：产品说明书产品测试文档)。模拟授权与非授权管理员访问审计记录，测试网络隔离产品安全功能仅允许授权管理员访问审计记录。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络隔离产品应仅允许授权管理员访问审计记录。

5.3.1.5.5 可选择查阅审计

网络隔离产品的可选择查阅审计的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档是否包括评价所需的相关文档(例如：产品说明书产品测试文档)。测试网络隔离产品安全功能是否自身提供了审计查阅工具，能够按照主体 ID(标识符)、客体 ID、日期、时间进行逻辑组合对审计数据进行正确的查找和排序。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络隔离产品应自身提供审计查阅工具，能够按照主体 ID(标识符)、客体 ID、日期、时间进行逻辑组合对审计数据进行正确的查找和排序。

5.3.1.5.6 防止审计数据丢失

网络隔离产品的防止审计数据丢失的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 依据开发者提供的相关文档(例如：产品说明书产品测试文档)进行测试：

——测试网络隔离产品安全功能将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(测试是否提供了手段进行了限制)；

——模拟审计容量大量消耗相关的操作，测试网络隔离产品在审计存储容量达到事先规定的警戒值时发出警告信息，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；

2) 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

提供相应的分析结果(审查是否估计了审计数据丢失);

3) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果:

1) 网络隔离产品应能够将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(测试是否提供了手段进行了限制);

2) 网络隔离产品应在审计存储容量达到事先规定的警戒值时发出警告信息,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;

3) 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符合实际测试结果。

5.3.1.6 域隔离

网络隔离产品的域隔离的测试评价方法和预期结果如下:

a) 测试评价方法:

1) 评估开发者提供的文档,包括评价所需的相关文档(例如:产品说明书产品测试文档):

——网络隔离产品保护其免遭不可信主体的干扰和篡改;

——网络隔离产品将控制范围内的各个主体的安全区域分割开;

2) 审查文档并且验证其真实性;

3) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果:

1) 网络隔离产品应能够保护其免遭不可信主体的干扰和篡改;

2) 网络隔离产品应能够将控制范围内的各个主体的安全区域分割开。

5.3.1.7 容错

网络隔离产品的容错的测试评价方法和预期结果如下:

a) 测试评价方法:

评估开发者提供的文档,包括评价所需的相关文档(例如:产品说明书产品测试文档)。测试网络隔离产品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,容错功能能够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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果:

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,容错功能应能够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。

5.3.1.8 数据完整性

网络隔离产品的数据完整性的测试评价方法和预期结果如下:

a) 测试评价方法:

评估开发者提供的文档,包括网络隔离产品对外提供的所有接口及服务的详细描述。测试网络隔离产品确保通过所有接口对鉴别数据和信息传输策略的查阅、修改、删除等操作前必须经过身份鉴别,只有授权人员才能进行以上操作。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果:

网络隔离产品应确保通过所有接口对鉴别数据和信息传输策略的查阅、修改、删除等操作前必

须经过身份鉴别，只有授权人员才能进行以上操作。

5.3.1.9 密码支持

网络隔离产品的密码支持的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括国家密码委员会对加密算法的批文。审查开发者所提供的密码算法批文为国家密码委员会的正式有效批文。记录审查结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

开发者所提供的密码算法批文应为国家密码委员会的正式有效批文。

5.3.2 增强级测试

5.3.2.1 访问控制

5.3.2.1.1 增强的信息流控制策略

网络隔离产品的增强的信息流控制策略的测试评价方法和预期结果如下：

a) **测试评价方法：**

1) **评估开发者提供的文档，包括增强的信息流控制策略的详细描述。模拟生成设备所支持的信息流，测试对主体、客体以及经过网络隔离产品的主客体之间的所有操作，网络隔离产品基本的信息流控制策略能够执行以下端到端增强的信息流控制策略：**

——**所有主客体之间发送和接收的信息流执行网络层协议剥离，还原成应用层数据，还原后的应用层数据是否包括了应用层携带的较大的附件，例如大于 20 M 的邮件附件；**

——**主体与客体通讯之前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是否经过了安全策略控制允许后传输；**

2) **记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。**

b) **预期结果：**

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，网络隔离产品基本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：

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

2) **主体与客体通讯之前应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应经过安全策略控制允许后传输。**

5.3.2.1.2 增强的信息流控制功能

网络隔离产品的增强的信息流控制功能的测试评价方法和预期结果如下：

a) **测试评价方法：**

评估开发者提供的文档，包括增强的信息流控制功能的详细描述。模拟生成设备所支持的信息流，测试网络隔离产品安全功能策略是否可执行以下增强的信息流控制功能，是否提供明确的访问保障能力和拒绝访问能力。包括：

1) **网络隔离产品可通过配置 ACL 访问控制列表进行的信息流控制，ACL 访问控制列表的元素是否包括：源 IP 地址、目的 IP 地址、源端口、目的端口、协议号；**

2) **网络隔离产品可对经过的 HTTP、FTP、SMTP、POP3、SQL、RSTP、SIP 等应用协议信息流**

进行合规性检查；

3） 网络隔离产品可对经过的 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；

4） 网络隔离产品可配置文件同步任务，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；

5） 网络隔离产品可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；

6） 网络隔离产品可识别主体的应用类型，可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；

7） 网络隔离产品能够断开 TCP/IP 连接对内外网数据传输链路进行物理上的时分切换，即禁止内外网络在物理链路上同时与专用隔离部件连通。

b） 预期结果：

1） 网络隔离产品应可通过配置 ACL 访问控制列表进行信息流控制，ACL 访问控制列表的元素应包括：源 IP 地址、目的 IP 地址、源端口、目的端口、协议号；

2） 网络隔离产品应可对经过的 HTTP、FTP、SMTP、POP3、SQL、RSTP、SIP 等应用协议信息流进行合规性检查；

3） 网络隔离产品应可对经过的 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；

4） 网络隔离产品应可配置文件同步任务，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；

5） 网络隔离产品应可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；

6） 网络隔离产品应可识别主体的应用类型，应可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；

7） 网络隔离产品应能够断开 TCP/IP 连接对内外网数据传输链路进行物理上的时分切换，即禁止内外网络在物理链路上同时与专用隔离部件连通。

5.3.2.1.3 强制访问控制

网络隔离产品的强制访问控制的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括所设计的强制访问控制模型。根据强制访问控制模型，设定主体和客体的敏感标记，根据强制访问控制模型得出相应的强制访问控制规则。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

以授权主体和未授权主体分别访问客体，强制访问控制规则应能够生效。

5.3.2.1.4 残余信息保护

网络隔离产品的残余信息保护的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括残余信息保护的详细描述。测试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能够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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络隔离产品安全功能应能够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。

5.3.2.1.5 不可旁路

网络隔离产品的不可旁路的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括不可旁路保护的详细描述。审查文档并且验证其是否真实。提供文档说明网络隔离产品采用何种机制和措施，确保安全策略的不可旁路性，即任何与安全有关的操作被允许执行之前，都必须通过安全策略的检查。文档应该分析并确认，网络隔离产品确实控制了端设备用户的每次访问请求，不存在其他可能旁路网络隔离产品的途径。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

产品应不存在其他可能旁路网络隔离产品的途径。

5.3.2.2 抗攻击

网络隔离产品的抗攻击的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 配置启用网络隔离产品抗攻击功能；
2) 采用模拟攻击设备，通过网络隔离产品，发起产品声明支持带宽 10%的攻击流量(至少包括 SYN Flood、ICMP Flood 等)，同时通过网络隔离产品建立正常的传输业务，持续时间 1 min；
3) 检查拒绝服务攻击包通过的比例，以及正常业务成功建立的比例。

b) 预期结果：

1) 网络隔离产品具备抗拒绝服务器攻击能力；
2) 攻击包通过的比例不大于 5%、正常业务建立成功率不低于 90%。

5.3.2.3 安全管理

5.3.2.3.1 区分安全管理角色

网络隔离产品的区分安全管理角色的测试评价方法和预期结果如下：

a) 测试评价方法：

依据开发者所提供的区分安全管理角色的详细描述进行测试：

1) 产品至少提供两类用户角色，至少有一类为管理员角色，保证此两类用户角色并不相同。评价者测试此两类用户角色是否不同，且有一类属于管理员角色；
2) 创建一未授予安全管理角色的普通用户，以此用户执行安全管理功能相关操作，网络隔离产品拒绝其操作；
3) 将安全管理角色授与此用户，再次执行安全管理功能的相关操作(应包括安装、配置和管理网络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)，测试网络隔离产品是否允许其操作；

4） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

1） 产品应至少提供两类用户角色，至少有一类为管理员角色，保证此两类用户角色并不相同；

2） 网络隔离产品应拒绝未授予安全管理角色的普通用户执行安全管理功能相关操作；

3） 将安全管理角色授与此用户，再次执行安全管理功能的相关操作（应包括安装、配置和管理网络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），网络隔离产品应允许其操作。

5.3.2.3.2 管理功能

网络隔离产品的管理功能的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 评估开发者提供的文档，包括管理功能的详细描述。以授权管理员身份登录，测试能够进行如下操作：

——设置和更新与安全相关的数据；

——网络隔离产品的安装及初始化；

——系统启动和关闭；

——备份和恢复系统配置信息。

2） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

网络隔离产品应能执行上述操作，并且网络隔离产品的各种备份（如安全配置的备份，审计记录的备份）工作可以通过自动工具完成。如果网络隔离产品支持外部或内部接口的远程管理，尝试关闭内部和外部接口或其中之一及配置远程管理地址，网络隔离产品应允许这些操作的执行；从未授权远程管理的主机地址，尝试进行远程管理，网络隔离产品应予以拒绝；远程管理会话应进行加密保护。

5.3.2.3.3 独立管理接口

网络隔离产品的独立管理接口的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括独立管理接口的详细描述。测试网络隔离产品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，是否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，是否禁止其他用户非授权访问管理接口。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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，应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，应禁止其他用户非授权访问管理接口。

5.3.2.4 标识和鉴别

5.3.2.4.1 敏感标记

网络隔离产品的敏感标记的测试评价方法和预期结果如下：

a） **测试评价方法：**

评估开发者提供的文档，包括标记的相关文档。根据开发者提供的文档，对主体和客体设定敏感标记。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） **预期结果：**

产品应支持对主体和客体进行敏感标记。

5.3.2.4.2 基本安全属性定义

网络隔离产品的基本安全属性定义的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括对于每一个授权管理员、构成系统的信息传输与控制部件、应用层数据采集与接受部件，网络隔离产品为其提供一套唯一的、为了执行安全功能策略所必需的安全属性，并且说明具体的内容。测试产品是否设定了这些安全属性，至少包括授权管理员的安全属性、构成系统的信息传输与控制部件的安全属性、应用层数据采集与接受部件的安全属性和其他在开发者文档中提及的安全属性。如果产品设定规定范围内的安全属性和开发者文档中存在的安全属性，则此项判定为合格。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。测试产品应设定基本的安全属性，至少包括设备网络参数、设备接口属性、安全管理参数、安全参数、外部可信 IT 产品参数配置、系统参数、用户角色属性、用户管理属性、主机地址、服务端口、使用时间或时间段、内容关键字和其他在开发者文档中提及的基本的安全属性，如果产品设定规定范围内的基本的安全属性和开发者文档中存在的基本的安全属性，则此项判定为合格。

5.3.2.4.3 增强的安全属性定义

网络隔离产品的增强的安全属性定义的测试评价方法和预期结果如下：

a） **测试评价方法：**

评估开发者提供的文档，包括对于每一个授权管理员，网络隔离产品安全功能为其提供了一套唯一的、为了执行安全功能策略提供的增强的安全属性。测试产品设定了增强的安全属性，至少包括设备协议号、应用协议、应用类型和其他在开发者文档中提及的增强的安全属性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） **预期结果：**

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。测试产品应设定增强的安全属性，至少包括设备协议号、应用协议、应用类型和其他在开发者文档中提及的增强的安全属性，如果产品设定规定范围内的增强的安全属性和开发者文档中存在的增强的安全属性，则此项判定为合格。

5.3.2.4.4 属性初始化

网络隔离产品的属性初始化的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性初始化的详细描述。按照开发者提供的初始化方法进行初始化，审查初始化结果与文档宣称的初始化值一致。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

测试结果应完全符合上述测试评价方法要求做出判断，测试和审查的初始化过程和结果应符合文档说明。

5.3.2.4.5 属性修改

网络隔离产品的属性修改的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 测试能以授权管理员的身份对源地址、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）和配置的安全参数（至少包括：最大鉴别失败次数等数据）进行修改；

2） 测试修改后的设置是否有效；

3） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

1） 应能以授权管理员的身份对源地址、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）和配置的安全参数（至少包括：最大鉴别失败次数等数据）进行修改；

2） 修改后的设置应能够生效。

5.3.2.4.6 属性查询

网络隔离产品的属性查询的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性查询的详细描述。测试能以授权管理员的身份对源地址、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）和配置的安全参数（至少包括：最大鉴别失败次数等数据）进行查询。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

应能以授权管理员的身份对源地址、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）和配置的安全参数（至少包括：最大鉴别失败次数等数据）进行查询。

5.3.2.4.7 鉴别数据初始化

网络隔离产品的鉴别数据初始化的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。根据开发者提供的网络隔离产品鉴别机制的详细描述，分别以授权管理员和普通用户的身份登录，测试该部件是否提供鉴别数据的初始化功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

以授权管理员和普通用户的身份登录网络隔离产品，产品应提供鉴别数据的初始化功能。

5.3.2.4.8 鉴别时机

网络隔离产品的鉴别时机的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。设置多个授权管理员，分别以所有这些授权管理员的身份登录，测试在所有授权管理员请求执行的任何操作之前，网络隔离产品对每个授权管理员都进行了身份鉴别。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

在所有授权管理员请求执行的任何操作之前，网络隔离产品应对每个授权管理员都进行身份鉴别。

5.3.2.4.9 最少反馈

网络隔离产品的最少反馈的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。分别以授权管理员和普通用户的身份登录，并且输入正确或者错误的口令，测试网络隔离产品的反馈信息最少。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

分别以授权管理员和普通用户的身份登录，并且输入正确或者错误的口令，网络隔离产品应反馈最少的信息。

5.3.2.4.10 多鉴别机制

网络隔离产品的多鉴别机制的测试评价方法和预期结果如下：

a) **测试评价方法：**

评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。根据开发者提供的网络隔离产品鉴别机制的详细描述，验证提供了多鉴别机制功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) **预期结果：**

网络隔离产品应提供多鉴别机制。

5.3.2.4.11 鉴别失败处理

网络隔离产品的鉴别失败处理的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括网络隔离产品鉴别机制的详细描述。以错误的用户名—口令登录，在一定次数的鉴别失败后，测试网络隔离产品终止了进行登录尝试主机建立会话的过程。分别以授权管理员和普通用户的身份登录，测试该部件提供最多失败次数的设定功能，且最多失败次数仅由授权管理员设定。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

以错误的用户名—口令登录，在一定次数的鉴别失败后，网络隔离产品应能够终止进行登录尝试主机建立会话的过程。分别以授权管理员和普通用户的身份登录，产品应提供最多失败次数的设定功能，且最多失败次数应仅由授权管理员设定。

5.3.2.4.12 抗重放

网络隔离产品的抗重放的测试评价方法和预期结果如下：

a) **测试评价方法：**

评估开发者提供的文档，包括网络隔离产品抗重放的详细描述。网络隔离产品的鉴别机制具有抗重放的能力，授权管理员及其他用户无法复制使用上一次通过的鉴别信息再次鉴别成功。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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应无法复制使用上一次通过的鉴别信息再次鉴别成功。

5.3.2.4.13 受保护的鉴别反馈

网络隔离产品的受保护的鉴别反馈的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络隔离产品受保护的鉴别反馈的详细描述。测试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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.3.2.4.14 口令强度

网络隔离产品的口令强度的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络隔离产品口令强度的详细描述。测试网络隔离产品采用了口令校验机制对授权管理员生成的口令复杂度进行检查，口令强度是否保证口令长度大于6位，口令类型为数字＋大小写字母组合。并通过模拟口令登录验证措施的有效性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.3.2.5 审计

5.3.2.5.1 审计数据生成

网络隔离产品的审计数据生成的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括评价所需的相关文档(例如：产品说明书产品测试文档)。根据开发者文档，使用不同角色用户模拟对产品不同模块进行访问、运行、修改、关闭以及重复失败尝试等相关操作。审查审计记录的正确性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

网络隔离产品应能够准确记录不同角色用户对产品不同模块进行访问、运行、修改、关闭以及重复失败尝试等相关操作。

5.3.2.5.2 安全审计分析

网络隔离产品的安全审计分析的测试评价方法和预期结果如下：

a) **测试评价方法：**

1) **评估开发者提供的文档，包括网络隔离产品安全审计分析的详细描述。测试安全审计分析是否包括：**

——**网络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进行分类统计；**

——**网络隔离产品对应用流量、每个应用类别流量进行统计；**

——**网络隔离产品对 CPU、内存、磁盘占用率进行统计；**

——**对在线用户列表及在线用户时长进行了统计。**

2) **记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。**

b) **预期结果：**

1) **网络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应分类统计；**

2) **网络隔离产品应对总应用流量、每个应用类别流量进行统计；**

3) **网络隔离产品应对 CPU、内存、磁盘占用率进行统计；**

4) **应具有在线用户列表及在线用户时长的统计。**

5.3.2.5.3 用户身份关联

网络隔离产品的用户身份关联的测试评价方法和预期结果如下：

a) **测试评价方法：**

评估开发者提供的文档，包括评价所需的相关文档（例如：产品说明书产品测试文档）。使用不同角色用户执行所有产品功能相关的操作，测试网络隔离产品安全功能能将每个可审计事件与引起该事件的用户身份相关联。记录测试结果并对该结果完全符合上述测试评价方法要求做出判断。

b) **预期结果：**

网络隔离产品应能将每个可审计事件与引起该事件的用户身份相关联。

5.3.2.5.4 审计记录管理

网络隔离产品的审计记录管理的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括评价所需的相关文档（例如：产品说明书产品测试文档）。模拟授权管理员进行审计操作，测试网络隔离产品安全功能允许授权管理员存档、删除和清空审计记录。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络隔离产品应能够允许授权管理员存档、删除和清空审计记录。

5.3.2.5.5 可理解的格式

网络隔离产品的可理解的格式的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括评价所需的相关文档（例如：产品说明书产品测试文档）。审查网络隔离产品安全功能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（至少包括能为人理解的描述内容以及审计数据本身）。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络隔离产品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(至少包括能为人理解的描述内容以及审计数据本身)。

5.3.2.5.6 限制审计记录访问

网络隔离产品的基本的限制审计记录访问的测试评价方法和预期结果如下:

a) 测试评价方法:

评估开发者提供的文档,是否包括评价所需的相关文档(例如:产品说明书产品测试文档)。模拟授权与非授权管理员访问审计记录,测试网络隔离产品安全功能仅允许授权管理员访问审计记录。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果:

网络隔离产品应仅允许授权管理员访问审计记录。

5.3.2.5.7 可选择查阅审计

网络隔离产品的可选择查阅审计的测试评价方法和预期结果如下:

a) 测试评价方法:

评估开发者提供的文档是否包括评价所需的相关文档(例如:产品说明书产品测试文档)。测试网络隔离产品安全功能是否自身提供了审计查阅工具,能够按照主体 ID(标识符)、客体 ID、日期、时间进行逻辑组合对审计数据进行正确的查找和排序。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果:

网络隔离产品应自身提供审计查阅工具,能够按照主体 ID(标识符)、客体 ID、日期、时间进行逻辑组合对审计数据进行正确的查找和排序。

5.3.2.5.8 防止审计数据丢失

网络隔离产品的防止审计数据丢失的测试评价方法和预期结果如下:

a) 测试评价方法:

1) 依据开发者所提供的评价所需的相关文档(例如:产品说明书产品测试文档)进行测试:

——测试网络隔离产品安全功能将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(测试是否提供了手段进行了限制);

——模拟审计容量大量消耗相关的操作,测试网络隔离产品在审计存储容量达到事先规定的警戒值时发出警告信息,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。

2) 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提供相应的分析结果(审查是否估计了审计数据丢失)。

3) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果:

1) 网络隔离产品应能够将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(测试是否提供了手段进行了限制);

2) 网络隔离产品应在审计存储容量达到事先规定的警戒值时发出警告信息,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;

3) 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符合实际测试结果。

5.3.2.6 域隔离

5.3.2.6.1 基本的域隔离

网络隔离产品的基本的域隔离的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 评估开发者提供的文档，包括评价所需的相关文档(例如：产品说明书产品测试文档)；

——网络隔离产品保护其免遭不可信主体的干扰和篡改；

——网络隔离产品将控制范围内的各个主体的安全区域分割开。

2) 审查文档并且验证其真实性；

3) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

1) 网络隔离产品应能够保护其免遭不可信主体的干扰和篡改；

2) 网络隔离产品应能够将控制范围内的各个主体的安全区域分割开。

5.3.2.6.2 增强的域隔离

网络隔离产品的增强的域隔离的测试评价方法和预期结果如下：

a) **测试评价方法：**

评估开发者提供的文档，包括评价所需的相关文档(例如：产品说明书产品测试文档)。测试网络隔离产品安全功能为其自身的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，能否采用强制访问控制策略，授权管理员可以修改访问策略。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) **预期结果：**

网络隔离产品安全功能应为其自身的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，应能够采用强制访问控制策略，授权管理员无法修改访问策略。

5.3.2.7 容错

5.3.2.7.1 基本的容错

网络隔离产品的基本的容错的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括评价所需的相关文档(例如：产品说明书产品测试文档)。测试网络隔离产品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，容错功能能够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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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，容错功能应能够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。

5.3.2.7.2 增强的容错

网络隔离产品的增强的容错的测试评价方法和预期结果如下：

a） **测试评价方法：**

评估开发者提供的文档，包括评价所需的相关文档（例如：产品说明书产品测试文档）。测试网络隔离产品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，另一台主机应能够继续提供安全服务功能，保证安全功能的可用性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） **预期结果：**

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，另一台主机应能够继续提供安全服务功能，保证安全功能的可用性。

5.3.2.8 数据完整性

网络隔离产品的数据完整性的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络隔离产品对外提供的所有接口及服务的详细描述。测试网络隔离产品确保通过所有接口对鉴别数据和信息传输策略的查阅、修改、删除等操作前必须经过身份鉴别，只有授权人员才能进行以上操作。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

网络隔离产品应确保通过所有接口对鉴别数据和信息传输策略的查阅、修改、删除等操作前必须经过身份鉴别，只有授权人员才能进行以上操作。

5.3.2.9 密码支持

网络隔离产品的密码支持的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括国家密码委员会对加密算法的批文。审查开发者所提供的密码算法批文为国家密码委员会的正式有效批文。记录审查结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

开发者所提供的密码算法批文应为国家密码委员会的正式有效批文。

5.4 网络单向导入产品

5.4.1 基本级测试

5.4.1.1 访问控制

5.4.1.1.1 信息流控制策略

网络单向导入产品的基本的信息流控制策略的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 评估开发者提供的文档，包括基本的信息流控制策略的详细描述。测试网络单向导入产品是否具有如下的信息流控制策略：

——网络单向导入产品能够将数据发送方网络信息流协议剥离，还原成裸数据后单向导入信息接收方网络目的主机；

——网络单向导入产品可以根据单向同步任务安全属性值主动访问源主机，身份鉴别通过后读取数据，单向导入接收端后，可完成连接目的主机的身份鉴别并将数据写入目的主机；

——网络单向导入产品可以内置信息流接收服务，接收到数据后转换成裸数据单向导入信息接收方网络目的主机。

2） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

1） 网络单向导入产品应能够将数据发送方网络信息流剥离协议，还原成裸数据后单向导入信息接收方网络目的主机；

2） 网络单向导入产品应能够根据单向同步任务安全属性值主动访问源主机，身份鉴别通过后读取数据，单向导入接收端后，完成连接目的主机的身份鉴别并将数据写入目的主机；

3） 网络单向导入产品应能够内置信息流接收服务，接收到数据后转换成裸数据单向导入信息接收方网络目的主机。

5.4.1.1.2 基本的信息流控制功能

网络单向导入产品的基本的信息流控制功能的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括基本的信息流控制功能的详细描述。测试网络单向导入产品安全功能策略可执行以下基本的信息流控制功能，提供了明确的访问保障能力和拒绝访问能力。包括：

1） 网络单向导入产品可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；

2） 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；

3） 网络单向导入产品能够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；

4） 网络单向导入产品能够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；

5） 网络单向导入产品能够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；

6） 网络单向导入产品能够支持文件单向导入、数据库单向导入等服务类型。

b） 预期结果：

1） 网络单向导入产品应能够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，网络单向导入产品为拒绝任何数据的单向导入；

2） 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，应明确拒绝访问；

3） 网络单向导入产品应能够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；

4） 网络单向导入产品应能够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；

5） 网络单向导入产品应能够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；

6） 网络单向导入产品应能够支持文件单向导入、数据库单向导入等服务类型。

5.4.1.1.3 单向传输保证

网络单向导入产品的单向传输保证的测试评价方法和预期结果如下：

a） 测试评价方法：

按照提供的文档说明，检查产品提供通过物理方式构造信息单向传输的唯一通道，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

数据单向发送单元只具有单一的数据发送功能，单向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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

产品应提供通过物理方式构造信息单向传输的唯一通道，且不存在反馈信息。

5.4.1.1.4 残余信息保护

网络单向导入产品的残余信息保护的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括残余信息保护的详细描述。测试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，安全功能能够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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.1.1.5 不可旁路

网络单向导入产品的不可旁路的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络单向导入产品采用何种机制和措施，确保安全策略的不可旁路性，即任何与安全有关的操作被允许执行之前，都必须通过安全策略的检查。文档应该分析并确认，网络单向导入产品确实控制了端设备用户的每次访问请求，不存在其他可能旁路网络单向导入产品的途径。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

产品不存在其他可能旁路网络单向导入产品的途径。

5.4.1.1.6 数据完整性保证

网络单向导入产品的数据完整性保证的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络单向导入产品对外提供的所有接口及服务的详细描述。测试网络单向导入产品是否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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.1.2 抗攻击

网络单向导入产品的抗攻击的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 配置启用网络单向导入产品抗攻击功能；

2） 采用模拟攻击设备，通过网络单向导入产品，发起产品声明支持带宽10%的攻击流量（至少包括SYN Flood、ICMP Flood等），同时通过网络单向导入产品建立正常的传输业务，持续时间1 min；

3） 检查拒绝服务攻击包通过的比例，以及正常业务成功建立的比例。

b） 预期结果：

1） 网络单向导入产品具备抗拒绝服务器攻击能力；

2） 攻击包通过的比例不大于5%、正常业务建立成功率不低于90%。

5.4.1.3 安全管理

5.4.1.3.1 区分安全管理角色

网络单向导入产品的区分安全管理角色的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括区分安全管理角色的详细描述。测试网络单向导入产品安全功能包括：

1） 能够将与安全相关的管理功能与其他功能区分开；

2） 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，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；

3） 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；

4） 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；

5） 仅允许授权管理员承担安全管理职责；

6） 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。

b） 预期结果：

网络单向导入产品安全功能应包括：

1） 应能够将与安全相关的管理功能与其他功能区分开；

2） 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，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；

3） 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；

4） 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；

5） 应仅允许授权管理员承担安全管理职责；

6） 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。

5.4.1.3.2 管理功能

网络单向导入产品的管理功能的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 评估开发者提供的文档，包括管理功能的详细描述。测试网络单项导入产品向授权管理员提供的如下管理功能：

——设置和更新与安全相关的数据；

——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，备份能力有自

动工具的支持；

——设置隔离部件的双机热备等可用性参数；

——若支持远程管理，能限制可进行远程管理的地址及能通过加密来保护远程管理对话。

2） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

网络单项导入产品应能够向授权管理员提供如下管理功能：

1） 设置和更新与安全相关的数据；

2） 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；

3） 设置隔离部件的双机热备等可用性参数；

4） 若支持远程管理，应能够：

——限制可进行远程管理的地址；

——通过加密来保护远程管理对话。

5.4.1.3.3 独立管理接口

网络单向导入产品的基本的独立管理接口的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括独立管理接口的详细描述。测试网络单向导入产品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，采用的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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.1.4 标识和鉴别

5.4.1.4.1 安全属性定义

网络单向导入产品的安全属性定义的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 评估开发者提供的文档，包括安全属性定义的详细描述。测试对每一个授权管理员，网络单向导入产品安全功能是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：

——设备网络参数：包括接口地址、网关地址等；

——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；

——安全管理参数：管理控制台地址、管理方式（例如：SSH、SSL）等；

——安全参数：最大鉴别失败次数、管理空闲超时；

——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；

——系统参数：日志存储空间大小、设备名称等；

——用户角色属性：授权管理员、授权审计员、授权用户等；

——用户管理属性：用户名、用户角色、用户口令等。

2） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

对每一个授权管理员，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：

1） 设备网络参数：包括接口地址、网关地址等；
2） 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；
3） 安全管理参数：管理控制台地址、管理方式（例如：SSH、SSL）等；
4） 安全参数：最大鉴别失败次数、管理空闲超时；
5） 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；
6） 系统参数：日志存储空间大小、设备名称等；
7） 用户角色属性：授权管理员、授权审计员、授权用户等；
8） 用户管理属性：用户名、用户角色、用户口令等。

5.4.1.4.2 属性初始化

网络单向导入产品的属性初始化的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性初始化的详细描述。测试网络单向导入产品安全功能提供的用默认值对授权管理员和主机属性初始化的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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

5.4.1.4.3 属性修改

网络单向导入产品的属性修改的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性修改的详细描述。测试网络单向导入产品安全功能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：

1） 标识与角色（例如：配置管理员等）的关系；
2） 主体（数据采集方）和客体（数据接收方）的安全属性值；
3） 配置的安全参数（例如：最大鉴别失败次数等数据）；
4） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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：

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

5.4.1.4.4 属性查询

网络单向导入产品的属性查询的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 评估开发者提供的文档，包括属性查询的详细描述。测试网络单向导入产品安全功能仅向授权管理员提供以下查询：

——标识和角色的关系；
——主体（数据采集方）和客体（数据接收方）的安全属性值；

——配置的各安全参数。

2） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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：

1） 标识和角色的关系；

2） 主体(数据采集方)和客体(数据接收方)的安全属性值；

3） 配置的各安全参数。

5.4.1.4.5 鉴别数据初始化

网络单向导入产品的鉴别数据初始化的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括鉴别数据初始化的详细描述。测试网络单项导入产品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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.1.4.6 鉴别时机

网络单向导入产品的鉴别时机的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括鉴别时机的详细描述。测试网络单项导入产品在所有授权管理员请求执行的任何操作之前，确保对每个授权管理员进行身份鉴别。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

在所有授权管理员请求执行的任何操作之前，应确保对每个授权管理员进行身份鉴别。

5.4.1.4.7 最少反馈

网络单向导入产品的最少反馈的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括最少反馈的详细描述。测试网络单项导入产品在进行鉴别时，安全功能仅将最少的反馈提供给用户。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

网络单项导入产品在进行鉴别时，安全功能应仅将最少的反馈提供给用户。

5.4.1.4.8 鉴别失败处理

网络单向导入产品的鉴别失败处理的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括鉴别失败处理的详细描述。以错误的用户名—口令登录，在一定次数的鉴别失败后，测试单向导入设备终止了进行登录尝试主机建立会话的过程。分别以授权管理员和普通用户的身份登录，测试该部件提供的最多失败次数的设定功能，且最多失败次数仅由授权管理员设定。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出

判断。

b） 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。最多失败次数的实际情况与设置值相符。应能设置最多失败次数，或能设定的允许最大失败次数默认值和其他防止口令暴力猜测的措施。

5.4.1.4.9 超时重鉴别

网络单向导入产品的超时重鉴别的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括超时重鉴别的详细描述。按照所提供的文档说明设置产品的登录超时时间，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。最大超时时间是否仅可由授权管理员设定。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。在设定的时间段内没有任何操作的情况下，终止会话，产品需要再次进行身份鉴别才能够重新操作。最大超时时间仅可由授权管理员设定。

5.4.1.4.10 抗重放

网络单向导入产品的抗重放的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括抗重放的详细描述。测试网络单向导入产品的鉴别机制是否具有抗重放的能力，授权管理员及其他用户是否无法复制使用上一次通过的鉴别信息再次鉴别成功。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.1.4.11 保护的鉴别反馈

网络单向导入产品的保护的鉴别反馈的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括保护的鉴别反馈的详细描述。测试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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.1.5 审计

5.4.1.5.1 审计数据生成

网络单向导入产品的审计数据生成的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 评估开发者提供的文档，包括审计数据生成的详细描述。测试网络单向导入产品安全功能能对下列可审计事件生成审计记录：

——审计功能的启动和关闭；

——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；

——任何读取、修改、破坏审计记录的尝试；

——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；

——修改安全属性的所有尝试，以及修改后安全属性的新值；

——所有使用安全功能中鉴别数据管理机制的请求；

——所有访问鉴别数据的请求，以及访问请求的目标；

——任何对鉴别机制的使用；

——所有使用标识机制的尝试；

——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。

2） 对于每一个审计记录，安全功能是否能够记录以下信息：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；

3） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

1） 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：

——审计功能的启动和关闭；

——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；

——任何读取、修改、破坏审计记录的尝试；

——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；

——修改安全属性的所有尝试，以及修改后安全属性的新值；

——所有使用安全功能中鉴别数据管理机制的请求；

——所有访问鉴别数据的请求，以及访问请求的目标；

——任何对鉴别机制的使用；

——所有使用标识机制的尝试；

——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。

2） 对于每一个审计记录，安全功能应至少记录以下信息：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。

5.4.1.5.2 用户身份关联

网络单向导入产品的用户身份关联的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括用户身份关联的详细描述。使用不同角色用户执行所有产品功能相关的操作，测试网络单向导入产品安全功能是否能将每个可审计事件与引起该事件的用户身份相关联。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

产品能够将每个可审计事件与引起该事件的用户身份相关联。

5.4.1.5.3 审计记录管理

网络单向导入产品的审计记录管理的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括审计记录管理的详细描述。使用授权管理员进行审计操作，测试网络单向导入产品安全功能允许授权管理员存档、删除和清空审计记录的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络单向导入产品应允许授权管理员存档、删除和清空审计记录。

5.4.1.5.4 可理解的格式

网络单向导入产品的可理解的格式的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括可理解的格式的详细描述。审查网络单向导入产品安全功能是否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（至少包括能为人理解的描述内容以及审计数据本身）。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.1.5.5 限制审计记录访问

网络单向导入产品的限制审计记录访问的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括限制审计记录访问的详细描述。模拟授权与非授权管理员访问审计记录，测试网络单向导入产品安全功能仅允许授权管理员访问审计记录。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.1.5.6 可选择查阅审计

网络单向导入产品的可选择审阅的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括可选择查阅审计的详细描述。测试网络单向导入产品自身提供了审计查阅工具，能够按照主体 ID（标识符）、客体 ID、日期、时间进行逻辑组合对审计数据进行正确的查找和排序。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.1.5.7 防止审计数据丢失

网络单向导入产品的防止审计数据丢失的测试评价方法和预期结果如下：

a) 测试评价方法：

1） 测试单向导入设备安全功能将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（测试是否提供了手段进行了限制）；

2） 模拟审计容量大量消耗相关的操作，测试单向导入设备在审计存储容量达到事先规定的警戒值时发出警告信息，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。

3） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。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；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。

5.4.1.6 域隔离

网络单向导入产品的域隔离的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括基本的域隔离的详细描述。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可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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.1.7 配置数据保护

网络单向导入产品的配置数据保护的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括配置数据保护的详细描述。测试网络单项导入产品能够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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。网络单项导入产品应能够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。

5.4.1.8 运行状态监测

网络单向导入产品的运行状态监测的测试评价方法和预期结果如下：

a） 测试评价方法：

根据所提供的文档，检查单向导入设备对设备的工作状态进行监测的功能，至少包括 CPU 使用率、内存占用率和存储空间等信息。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。根据所提供的文档，检查网络单向导入

产品是否可以对设备的工作状态进行监测，至少包括 CPU 使用率、内存占用率和存储空间等信息。

5.4.2 增强级测试

5.4.2.1 访问控制

5.4.2.1.1 信息流控制策略

网络单向导入产品的信息流控制策略的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 评估开发者提供的文档，包括基本的信息流控制策略的详细描述。测试网络单向导入产品是否具有如下的信息流控制策略：

——网络单向导入产品能够将数据发送方网络信息流协议剥离，还原成裸数据后单向导入信息接收方网络目的主机；

——网络单向导入产品可以根据单向同步任务安全属性值主动访问源主机，身份鉴别通过后读取数据，单向导入接收端后，可完成连接目的主机的身份鉴别并将数据写入目的主机；

——网络单向导入产品可以内置信息流接收服务，接收到数据后转换成裸数据单向导入信息接收方网络目的主机。

2) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

1) 网络单向导入产品应能够将数据发送方网络信息流剥离协议，还原成裸数据后单向导入信息接收方网络目的主机；

2) 网络单向导入产品应能够根据单向同步任务安全属性值主动访问源主机，身份鉴别通过后读取数据，单向导入接收端后，完成连接目的主机的身份鉴别并将数据写入目的主机；

3) 网络单向导入产品应能够内置信息流接收服务，接收到数据后转换成裸数据单向导入信息接收方网络目的主机。

5.4.2.1.2 基本的信息流控制功能

网络单向导入产品的基本的信息流控制功能的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括基本的信息流控制功能的详细描述。测试网络单向导入产品安全功能策略可执行以下基本的信息流控制功能，提供了明确的访问保障能力和拒绝访问能力。包括：

1) 网络单向导入产品可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；

2) 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；

3) 网络单向导入产品能够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；

4) 网络单向导入产品能够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；

5) 网络单向导入产品能够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；

6) 网络单向导入产品能够支持文件单向导入、数据库单向导入等服务类型。

b) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

c) 预期结果：

1） 网络单向导入产品应能够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，网络单向导入产品为配置单向同步任务，拒绝任何数据的单向导入；
2） 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，应明确拒绝访问；
3） 网络单向导入产品应能够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；
4） 网络单向导入产品应能够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；
5） 网络单向导入产品应能够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；
6） 网络单向导入产品应能够支持文件单向导入、数据库单向导入等服务类型。

5.4.2.1.3 增强的信息流控制功能

网络单向导入产品的增强的信息流控制功能的测试评价方法和预期结果如下：

a） **测试评价方法：**

1） **评估开发者提供的文档，包括增强的信息流控制功能的详细描述。测试网络单向导入产品安全功能策略可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：**

——**网络单向导入产品能够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；**

——**网络单向导入产品能够支持文件单向导入、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；**

——**网络单向导入产品能够根据预设的时间周期性定时完成数据的单向导入。**

2） **记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。**

b） **预期结果：**

1） **网络单向导入产品应能够在 IPv4/IPv6 环境中进行数据的单向导入；**
2） **网络单向导入产品应能够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；**
3） **网络单向导入产品应能够支持文件单向导入、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；**
4） **网络单向导入产品应能够根据预设的时间周期性定时完成数据的单向导入。**

5.4.2.1.4 单向传输保证

网络单向导入产品的单向传输保证的测试评价方法和预期结果如下：

a） 测试评价方法：

按照提供的文档说明，检查产品提供通过物理方式构造信息单向传输的唯一通道，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。单向传输部件数据单向发送单元只具有单一的数据发送功能，单向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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

产品应提供通过物理方式构造信息单向传输的唯一通道，且不存在反馈信息。

5.4.2.1.5 强制访问控制

网络单向导入产品的强制访问控制的测试评价方法和预期结果如下：

a） **测试评价方法：**

评估开发者提供的文档，包括强制访问控制的详细描述。测试网络单项导入产品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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） **预期结果：**

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。

5.4.2.1.6 残余信息保护

网络单向导入产品的残余信息保护的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括残余信息保护的详细描述。测试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，安全功能能够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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.2.1.7 不可旁路

网络单向导入产品的不可旁路的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络单向导入产品采用何种机制和措施，确保安全策略的不可旁路性，即任何与安全有关的操作被允许执行之前，都必须通过安全策略的检查。文档应该分析并确认，网络单向导入产品确实控制了端设备用户的每次访问请求，不存在其他可能旁路网络单向导入产品的途径。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

产品不存在其他可能旁路网络单向导入产品的途径。

5.4.2.1.8 数据完整性保证

网络单向导入产品的数据完整性保证的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括网络单向导入产品对外提供的所有接口及服务的详细描述。测试网络单向导入产品是否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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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。

5.4.2.2 抗攻击

网络单向导入产品的抗攻击的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 配置启用网络单向导入产品抗攻击功能；

2) 采用模拟攻击设备，通过网络单向导入产品，发起产品声明支持带宽 10％的攻击流量（至少包括 SYN Flood、ICMP Flood 等），同时通过网络单向导入产品建立正常的传输业务，持续时间 1 min；

3) 检查拒绝服务攻击包通过的比例，以及正常业务成功建立的比例。

b) 预期结果：

1) 网络单向导入产品具备抗拒绝服务器攻击能力；

2) 攻击包通过的比例不大于 5％、正常业务建立成功率不低于 90％。

5.4.2.3 安全管理

5.4.2.3.1 区分安全管理角色

网络单向导入产品的区分安全管理角色的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括区分安全管理角色的详细描述。测试网络单向导入产品安全功能包括：

1) 能够将与安全相关的管理功能与其他功能区分开；

2) 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，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；

3) 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；

4) 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；

5) 仅允许授权管理员承担安全管理职责；

6) 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。

b) 预期结果：

网络单向导入产品安全功能应包括：

1) 应能够将与安全相关的管理功能与其他功能区分开；

2) 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，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；

3) 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；

4) 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；

5) 应仅允许授权管理员承担安全管理职责；

6) 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。

5.4.2.3.2 管理功能

网络单向导入产品的管理功能的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 评估开发者提供的文档，包括管理功能的详细描述。测试网络单项导入产品向授权管理员提供的如下管理功能：

——设置和更新与安全相关的数据；
——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，备份能力有自动工具的支持；
——设置隔离部件的双机热备等可用性参数；
——若支持远程管理，能限制可进行远程管理的地址及能通过加密来保护远程管理对话。

2） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

网络单项导入产品应能够向授权管理员提供如下管理功能：

1） 设置和更新与安全相关的数据；
2） 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，备份能力是否有自动工具的支持；
3） 设置隔离部件的双机热备等可用性参数；
4） 若支持远程管理，应能够：
——限制可进行远程管理的地址；
——通过加密来保护远程管理对话。

5.4.2.3.3 独立管理接口

网络单向导入产品的独立管理接口的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括独立管理接口的详细描述。测试网络单向导入产品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，采用的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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果

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。

5.4.2.4 标识和鉴别

5.4.2.4.1 敏感标识

网络单向导入产品的敏感标记的测试评价方法和预期结果如下：

a） **测试评价方法：**

评估开发者提供的文档，包括敏感标记的详细描述。测试网络单项导入产品安全功能是否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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） **预期结果：**

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。

5.4.2.4.2 安全属性定义

网络单向导入产品的安全属性定义的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 评估开发者提供的文档，包括安全属性定义的详细描述。测试对每一个授权管理员，网络

单向导入产品安全功能是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：

——设备网络参数：包括接口地址、网关地址等；

——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；

——安全管理参数：管理控制台地址、管理方式（例如：SSH、SSL）等；

——安全参数：最大鉴别失败次数、管理空闲超时；

——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；

——系统参数：日志存储空间大小、设备名称等；

——用户角色属性：授权管理员、授权审计员、授权用户等；

——用户管理属性：用户名、用户角色、用户口令等。

2） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

对每一个授权管理员，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：

1） 设备网络参数：包括接口地址、网关地址等；

2） 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；

3） 安全管理参数：管理控制台地址、管理方式（例如：SSH、SSL）等；

4） 安全参数：最大鉴别失败次数、管理空闲超时；

5） 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；

6） 系统参数：日志存储空间大小、设备名称等；

7） 用户角色属性：授权管理员、授权审计员、授权用户等；

8） 用户管理属性：用户名、用户角色、用户口令等。

5.4.2.4.3 属性初始化

网络单向导入产品的属性初始化的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性初始化的详细描述。测试网络单向导入产品安全功能提供的用默认值对授权管理员和主机属性初始化的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

网络单向导入产品安全功能应能够提供使用默认值对授权管理员和主机属性初始化的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

5.4.2.4.4 属性修改

网络单向导入产品的属性修改的测试评价方法和预期结果如下：

a） 测试评价方法：

评估开发者提供的文档，包括属性修改的详细描述。测试网络单向导入产品安全功能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：

1） 标识与角色（例如：配置管理员等）的关系；

2） 主体（数据采集方）和客体（数据接收方）的安全属性值；

3） 配置的安全参数（例如：最大鉴别失败次数等数据）；

4） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

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：

1) 标识与角色(例如：配置管理员等)的关系；

2) 主体(数据采集方)和客体(数据接收方)的安全属性值；

3) 配置的安全参数(例如：最大鉴别失败次数等数据)。

5.4.2.4.5 属性查询

网络单向导入产品的属性查询的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 评估开发者提供的文档，包括属性查询的详细描述。测试网络单向导入产品安全功能仅向授权管理员提供以下查询：

——标识和角色的关系；

——主体(数据采集方)和客体(数据接收方)的安全属性值；

——配置的各安全参数。

2) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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：

1) 标识和角色的关系；

2) 主体(数据采集方)和客体(数据接收方)的安全属性值；

3) 配置的各安全参数。

5.4.2.4.6 鉴别数据初始化

网络单向导入产品的鉴别数据初始化的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括鉴别数据初始化的详细描述。测试网络单项导入产品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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.2.4.7 鉴别时机

网络单向导入产品的鉴别时机的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括鉴别时机的详细描述。测试网络单项导入产品在所有授权管理员请求执行的任何操作之前，确保对每个授权管理员进行身份鉴别。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

在所有授权管理员请求执行的任何操作之前，应确保对每个授权管理员进行身份鉴别。

5.4.2.4.8 最少反馈

网络单向导入产品的最少反馈的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括最少反馈的详细描述。测试网络单项导入产品在进行鉴别时，安

全功能仅将最少的反馈提供给用户。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

网络单项导入产品在进行鉴别时，安全功能应仅将最少的反馈提供给用户。

5.4.2.4.9 鉴别失败处理

网络单向导入产品的鉴别失败处理的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括鉴别失败处理的详细描述。以错误的用户名—口令登录，在一定次数的鉴别失败后，测试单向导入设备终止了进行登录尝试主机建立会话的过程。分别以授权管理员和普通用户的身份登录，测试该部件提供的最多失败次数的设定功能，且最多失败次数仅由授权管理员设定。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。最多失败次数的实际情况与设置值相符。应能设置最多失败次数，或能设定的允许最大失败次数默认值和其他防止口令暴力猜测的措施。

5.4.2.4.10 超时重鉴别

网络单向导入产品的超时重鉴别的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括超时重鉴别的详细描述。按照所提供的文档说明设置产品的登录超时时间，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。最大超时时间是否仅可由授权管理员设定。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。在设定的时间段内没有任何操作的情况下，终止会话，产品需要再次进行身份鉴别才能够重新操作。最大超时时间仅可由授权管理员设定。

5.4.2.4.11 多鉴别机制

网络单向导入产品的多鉴别机制的测试评价方法和预期结果如下：

a) **测试评价方法：**

评估开发者提供的文档，包括多鉴别机制的详细描述。测试网络单项导入产品安全功能提供了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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) **预期结果：**

网络单项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。

5.4.2.4.12 抗重放

网络单向导入产品的抗重放的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括抗重放的详细描述。测试网络单向导入产品的鉴别机制是否具有抗重放的能力，授权管理员及其他用户是否无法复制使用上一次通过的鉴别信息再次鉴别成功。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.2.4.13 保护的鉴别反馈

网络单向导入产品的保护的鉴别反馈的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括保护的鉴别反馈的详细描述。测试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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.2.4.14 口令强度

网络单向导入产品的口令强度的测试评价方法和预期结果如下：

a) **测试评价方法：**

评估开发者提供的文档，包括口令强度的详细描述。测试网络单向导入产品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，口令强度保证了口令长度大于6位，口令类型为数字＋大小写字母组合。并通过模拟口令登录验证措施的有效性。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) **预期结果：**

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。

5.4.2.5 审计

5.4.2.5.1 审计数据生成

网络单向导入产品的审计数据生成的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 评估开发者提供的文档，包括审计数据生成的详细描述。测试网络单向导入产品安全功能能对下列可审计事件生成审计记录：

——审计功能的启动和关闭；

——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；

——任何读取、修改、破坏审计记录的尝试；

——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；

——修改安全属性的所有尝试，以及修改后安全属性的新值；

——所有使用安全功能中鉴别数据管理机制的请求；

——所有访问鉴别数据的请求，以及访问请求的目标；
——任何对鉴别机制的使用；
——所有使用标识机制的尝试；
——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。

2） 对于每一个审计记录，安全功能是否能够记录以下信息：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；

3） 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：

1） 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：
——审计功能的启动和关闭；
——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；
——任何读取、修改、破坏审计记录的尝试；
——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；
——修改安全属性的所有尝试，以及修改后安全属性的新值；
——所有使用安全功能中鉴别数据管理机制的请求；
——所有访问鉴别数据的请求，以及访问请求的目标；
——任何对鉴别机制的使用；
——所有使用标识机制的尝试；
——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；

2） 对于每一个审计记录，安全功能应至少记录以下信息：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。

5.4.2.5.2 用户身份关联

网络单向导入产品的用户身份关联的测试评价方法和预期结果如下：

a） 测试评价方法：
评估开发者提供的文档，包括用户身份关联的详细描述。使用不同角色用户执行所有产品功能相关的操作，测试网络单向导入产品安全功能是否能将每个可审计事件与引起该事件的用户身份相关联。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：
产品能够将每个可审计事件与引起该事件的用户身份相关联。

5.4.2.5.3 审计记录管理

网络单向导入产品的审计记录管理的测试评价方法和预期结果如下：

a） 测试评价方法：
评估开发者提供的文档，包括审计记录管理的详细描述。使用授权管理员进行审计操作，测试网络单向导入产品安全功能允许授权管理员存档、删除和清空审计记录的功能。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b） 预期结果：
网络单向导入产品应允许授权管理员存档、删除和清空审计记录。

5.4.2.5.4 可理解的格式

网络单向导入产品的可理解的格式的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括可理解的格式的详细描述。审查网络单向导入产品安全功能是否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（至少包括能为人理解的描述内容以及审计数据本身）。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.2.5.5 限制审计记录访问

网络单向导入产品的限制审计记录访问的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括限制审计记录访问的详细描述。模拟授权与非授权管理员访问审计记录，测试网络单向导入产品安全功能仅允许授权管理员访问审计记录。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.2.5.6 可选择查阅审计

网络单向导入产品的可选择查阅审计的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括可选择查阅审计的详细描述。测试网络单向导入产品自身提供了审计查阅工具，能够按照主体 ID（标识符）、客体 ID、日期、时间进行逻辑组合对审计数据进行正确的查找和排序。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

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。

5.4.2.5.7 防止审计数据丢失

网络单向导入产品的防止审计数据丢失的测试评价方法和预期结果如下：

a) 测试评价方法：

1) 测试单向导入设备安全功能将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（测试是否提供了手段进行了限制）；

2) 模拟审计容量大量消耗相关的操作，测试单向导入设备在审计存储容量达到事先规定的警戒值时发出警告信息，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。

3) 记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。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;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。

5.4.2.6 域隔离

5.4.2.6.1 基本的域隔离

网络单向导入产品的基本的域隔离的测试评价方法和预期结果如下:

a) 测试评价方法:

评估开发者提供的文档,包括基本的域隔离的详细描述。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可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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果:

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可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。

5.4.2.6.2 增强的域隔离

网络单向导入产品的增强的域隔离的测试评价方法和预期结果如下:

a) **测试评价方法:**

评估开发者提供的文档,包括增强的域隔离的详细描述。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,测试网络单向导入产品安全功能可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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) **预期结果:**

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。

5.4.2.7 容错

网络单向导入产品的容错的测试评价方法和预期结果如下:

a) **测试评价方法:**

评估开发者提供的文档,包括容错的详细描述。测试网络单向导入产品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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) **预期结果:**

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。

5.4.2.8 配置数据保护

网络单向导入产品的配置数据保护的测试评价方法和预期结果如下：

a) 测试评价方法：

评估开发者提供的文档，包括配置数据保护的详细描述。测试网络单项导入产品能够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。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。网络单项导入产品应能够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。

5.4.2.9 运行状态监测

网络单向导入产品的运行状态监测的测试评价方法和预期结果如下：

a) 测试评价方法：

根据所提供的文档，检查单向导入设备对设备的工作状态进行监测的功能，至少包括 CPU 使用率、内存占用率和存储空间等信息。记录测试结果并对该结果是否完全符合上述测试评价方法要求做出判断。

b) 预期结果：

开发者应提供相关文档且文档内容与实际情况相符。根据所提供的文档，检查网络单向导入产品可以对设备的工作状态进行监测，至少包括 CPU 使用率、内存占用率和存储空间等信息。

6 安全保证要求评估

6.1 基本级测试

6.1.1 配置管理

6.1.1.1 版本号

版本号的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 评价者应审查开发者提供的配置管理支持文件是否包含版本号，要求开发者所使用的版本号与所应表示的产品样本应完全对应，没有歧义；

2) 评价者应现场检查在配置管理活动中产品样本是否具备唯一版本号，该版本号是否与产品样本以及配置管理支持文件的描述完全对应。

b) 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

6.1.1.2 配置项

配置项的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 评价者应审查开发者提供的配置管理文档，是否包括配置清单、配置管理计划。配置清单是否描述了组成系统的全部配置项；

2） 评价者应现场检查配置管理系统中的配置项是否与配置清单的描述一致，配置管理系统是否对所有的配置项做出唯一的标识，配置管理系统是否对配置项进行了维护；

3） 评价者应审查开发者提供的配置管理文档，是否描述了对配置项进行唯一标识的方法。

b） 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

6.1.2 交付与运行

6.1.2.1 交付程序

交付程序的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 评价者应现场检查开发者是否使用一定的交付程序交付产品；

2） 评价者应审查开发者是否使用文档描述交付过程，文档中是否包含以下内容：在给用户方交付系统的各版本时，为维护安全所必需的所有程序。

b） 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

6.1.2.2 安装、生成和启动程序

安装、生成和启动程序的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 评价者应审查开发者是否提供了文档说明系统的安装、生成、启动和使用的过程；

2） 评价者按照文档描述的方式确认是否能够正确安装、生成和启动程序。

b） 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

6.1.3 开发

6.1.3.1 非形式化功能规格说明

非形式化功能规格说明的测试评价方法与预期结果如下：

a） 测试评价方法：

评价者应审查非形式化功能规格说明的如下内容，并确认功能设计是否是安全功能要求的精确和完整的示例：

——使用非形式化风格来描述产品安全功能与其外部接口；

——是内在一致的；

——描述使用所有外部产品安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和出错信息的细节；

——功能设计应当完整地表示产品安全功能。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

6.1.3.2 描述性高层设计

描述性高层设计的测试评价方法与预期结果如下：

a） 测试评价方法：

评价者应审查描述性高层设计的如下内容：

——使用非形式化风格来表示；
——是内在一致的；
——按子系统描述安全功能的结构；
——描述每个安全功能子系统所提供的安全功能性；
——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；
——标识安全功能子系统的所有接口；
——标识安全功能子系统的哪些接口是外部可见的。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.1.3.3 非形式化对应性证实

非形式化对应性证实的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 评价者应审查开发者是否在产品安全功能表示的所有相邻对之间提供对应性分析。
2） 其中，系统各种安全功能表示（如系统功能设计、高层设计、低层设计、实现表示）之间的对应性是所提供的抽象产品安全功能表示要求的精确而完整的示例。
3） 产品安全功能在功能设计中进行细化，并且较为抽象的产品安全功能表示的所有相关安全功能部分，在较具体的产品安全功能表示中进行细化。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.1.4 指导性文档

6.1.4.1 管理员指南

管理员指南的测试评价方法与预期结果如下：

a） 测试评价方法：
评价者应审查开发者是否提供了供授权管理员使用的管理员指南，并且此管理员指南是否包括如下内容：
——产品可以使用的管理功能和接口；
——产品提供给管理员的安全功能和接口的使用方法；
——在安全处理环境中应进行控制的功能和权限；
——所有对与产品的安全操作有关的用户行为的假设；
——所有受管理员控制的安全参数，如果可能，应指明安全值；
——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的实体的安全特性进行的改变；
——所有与授权管理员有关的 IT 环境的安全要求。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.1.4.2 用户指南

用户指南的测试评价方法与预期结果如下：

a） 测试评价方法：

评价者应审查开发者是否提供了供用户使用的用户指南，并且此用户指南是否包括如下内容：

——产品的非管理用户可使用的安全功能和接口；

——产品提供给用户的安全功能和接口的使用方法；

——用户可获取但应受安全处理环境控制的所有功能和权限；

——产品安全操作中用户所应承担的职责；

——与用户有关的 IT 环境的所有安全要求。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

6.1.5 测试

6.1.5.1 覆盖证据

覆盖证据的测试评价方法与预期结果如下：

a） 测试评价方法：

评价者应审查开发者提供的测试覆盖证据，在测试覆盖证据中，是否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。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

6.1.5.2 功能测试

功能测试的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 评价者应审查开发者提供的测试文档，是否包括测试计划、测试规程、预期的测试结果和实际测试结果；

2） 评价者应审查测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

3） 评价者应审查测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

4） 评价者应审查期望的测试结果是否表明测试成功后的预期输出；

5） 评价者应审查实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

6.1.5.3 独立测试

6.1.5.3.1 一致性

一致性的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 评价者应审查开发者提供的测试产品；

2） 评价者应审查开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致。

b） 预期结果：

开发者应提供能适合第三方测试的产品，并满足上述要求。

6.1.5.3.2 抽样

抽样的测试评价方法与预期结果如下：

a) 测试评价方法：
评价者应审查开发者是否提供一组相当的资源，用于安全功能的抽样测试。
b) 预期结果：
开发者提供的资源应满足上述要求。

6.1.6 脆弱性评定

6.1.6.1 产品安全功能强度评估

产品安全功能强度评估的测试评价方法与预期结果如下：
a) 测试评价方法：
评价者应审查开发者提供的指导性文档，是否对所标识的每个具有安全功能强度声明的安全机制进行了安全功能强度分析，是否说明了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。
b) 预期结果：
开发者提供的文档应满足上述要求。

6.1.6.2 开发者脆弱性分析

开发者脆弱性分析的测试评价方法与预期结果如下：
a) 测试评价方法：
1) 评价者应审查开发者提供的脆弱性分析文档，是否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了分析；
2) 评价者应审查开发者是否对被确定的脆弱性明确记录了采取的措施；
3) 对每一条脆弱性，评价者应审查是否有足够证据证明在使用产品的环境中该脆弱性不能被利用，并进行验证。
b) 预期结果：
开发者提供的文档应满足上述要求，提供的产品应通过脆弱性测试验证。

6.2 增强级测试

6.2.1 配置管理

6.2.1.1 部分配置管理自动化

部分配置管理自动化的测试评价方法与预期结果如下：
a) **测试评价方法：**
1) **评价者应审查配置管理系统是否提供一种自动方式来支持产品的生成，通过该方式是否能够确保只能对产品的实现表示进行已授权的改变。**
2) **评价者应审查配置管理计划是否描述配置管理系统中所使用的自动工具以及该工具的使用方法。**
b) **预期结果：**
开发者提供的现场活动证据内容应满足上述要求。

6.2.1.2 配置管理能力

6.2.1.2.1 版本号

版本号的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 评价者应审查开发者提供的配置管理支持文件是否包含版本号，要求开发者所使用的版本号与所应表示的产品样本应完全对应，没有歧义；

2) 评价者应现场检查在配置管理活动中产品样本是否具备唯一版本号，该版本号是否与产品样本以及配置管理支持文件的描述完全对应。

b) 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.1.2.2 配置项

配置项的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 评价者应审查开发者提供的配置管理文档，是否包括配置清单、配置管理计划。配置清单是否描述了组成系统的全部配置项；

2) 评价者应现场检查配置管理系统中的配置项是否与配置清单的描述一致，配置管理系统是否对所有的配置项做出唯一的标识，配置管理系统是否对配置项进行了维护；

3) 评价者应审查开发者提供的配置管理文档，是否描述了对配置项进行唯一标识的方法。

b) 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.1.2.3 授权控制

授权控制的测试评价方法与预期结果如下：

a) **测试评价方法：**

1) **评价者应审查开发者提供的配置管理计划文档，该文档是否描述配置管理系统的使用方法。**

2) **评价者应现场检查实施的配置管理活动是否与配置管理计划文档的描述相一致；**

3) **评价者应审查开发者提供的证据，这些证据应表明配置项得到了有效地维护。评价者应现场检查是否只有经过授权才能修改配置项。**

b) **预期结果：**

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.1.2.4 产生支持和接受程序

产生支持和接受程序的测试评价方法与预期结果如下：

a) **测试评价方法：**

1) **评价者应审查开发者提供的配置管理文档是否包括一个接受计划，接受计划是否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。**

2) **评价者应审查配置管理系统是否支持产品的生成。**

b) **预期结果：**

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.1.3 配置管理范围

6.2.1.3.1 配置管理覆盖

配置管理覆盖的测试评价方法与预期结果如下：

a) **测试评价方法：**

1) **评价者应审查开发者提供的配置管理支持文档是否说明了产品配置管理范围，配置管理范围至少包括产品实现表示、设计文档、测试文档、指导性文档、配置管理文档等配置项，从而确保这些配置项的修改是在一个正确授权的可控方式下进行的；**

2) **评价者应现场检查开发者所使用的配置管理系统至少能跟踪上述配置管理之下的内容；**

3) **评价者应审查开发者提供的配置管理支持文档是否说明了配置管理系统跟踪配置项的方法。**

b) **预期结果：**

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.1.3.2 问题跟踪配置管理覆盖

问题跟踪配置管理覆盖的测试评价方法与预期结果如下：

a) **测试评价方法：**

评价者应审查开发者是否将安全缺陷纳入配置管理范围，是否对安全缺陷进行跟踪。

b) **预期结果：**

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.2 交付与运行

6.2.2.1 交付程序

交付程序的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 评价者应现场检查开发者是否使用一定的交付程序交付产品；

2) 评价者应审查开发者是否使用文档描述交付过程，文档中是否包含以下内容：在给用户方交付系统的各版本时，为维护安全所必需的所有程序。

b) 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.2.2 修改检测

修改检测的测试评价方法与预期结果如下：

a) **测试评价方法：**

1) **评价者应审查开发者提供的文档是否描述了程序或技术措施，这些程序或技术措施可实现以下目的：**

——检测修改；

——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；

——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。

2) **评价者应现场检查开发者使用的程序是否与文档描述一致。**

b) **预期结果：**

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.2.3 安装、生成和启动程序

安装、生成和启动程序的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 评价者应审查开发者是否提供了文档说明系统的安装、生成、启动和使用的过程；

2) 评价者按照文档描述的方式确认是否能够正确安装、生成和启动程序。

b) 预期结果：

开发者提供的文档和现场活动证据内容应满足上述要求。

6.2.3 开发

6.2.3.1 功能规格说明

6.2.3.1.1 非形式化功能规格说明

非形式化功能规格说明的测试评价方法与预期结果如下：

a) 测试评价方法：

评价者应审查非形式化功能规格说明的如下内容，并确认功能设计是否是安全功能要求的精确和完整的示例：

——使用非形式化风格来描述产品安全功能与其外部接口；

——是内在一致的；

——描述使用所有外部产品安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和出错信息的细节；

——功能设计应当完整地表示产品安全功能。

b) 预期结果：

开发者提供的文档内容应满足上述要求。

6.2.3.1.2 充分定义的外部接口

充分定义的外部接口的测试评价方法与预期结果如下：

a) **测试评价方法：**

评价者应审查开发者所提供的功能规格说明和安全功能的对应性能够完备合理的表示安全功能。

b) **预期结果：**

开发者提供的文档内容应满足上述要求。

6.2.3.2 高层设计

6.2.3.2.1 描述性高层设计

描述性高层设计的测试评价方法与预期结果如下：

a) 测试评价方法：

评价者应审查描述性高层设计的如下内容：

——使用非形式化风格来表示；

——是内在一致的；

——按子系统描述安全功能的结构；

——描述每个安全功能子系统所提供的安全功能性；

——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；

——标识安全功能子系统的所有接口；

——标识安全功能子系统的哪些接口是外部可见的。

b) 预期结果：

开发者提供的文档内容应满足上述要求。

6.2.3.2.2 安全加强的高层设计

安全加强的高层设计的测试评价方法与预期结果如下：

a) **测试评价方法：**

1) **评价者应审查高层设计是否描述系统的功能子系统所有接口的用途与使用方法，是否适当描述效果、例外情况和错误消息的细节；**

2) **评价者应审查高层设计是否把系统分成安全策略实施和其他子系统来描述。**

b) **预期结果：**

开发者提供的文档内容应满足上述要求。

6.2.3.3 安全功能实现的子集

安全功能实现的子集的测试评价方法与预期结果如下：

a) **测试评价方法：**

评价者应审查开发者提供的实现表示是否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。

b) **预期结果：**

开发者提供的文档内容应满足上述要求。

6.2.3.4 描述性低层设计

描述性低层设计的测试评价方法与预期结果如下：

a) **测试评价方法：**

评价者应审查描述性低层设计的如下内容：

——使用非形式化风格来表示；

——是内在一致的；

——按模块描述安全功能；

——描述每个模块的用途；

——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；

——描述每个安全策略实施功能是如何被提供的；

——标识安全功能模块的所有接口；

——标识安全功能模块的哪些接口是外部可见的；

——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；

——把产品分为安全策略实施模块和其他模块来描述。

b) **预期结果：**

开发者提供的文档内容应满足上述要求。

6.2.3.5 非形式化对应性证实

非形式化对应性证实的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 评价者应审查开发者是否在产品安全功能表示的所有相邻对之间提供对应性分析。

2） 其中，系统各种安全功能表示（如系统功能设计、高层设计、低层设计、实现表示）之间的对应性是所提供的抽象产品安全功能表示要求的精确而完整的示例。

3） 产品安全功能在功能设计中进行细化，并且较为抽象的产品安全功能表示的所有相关安全功能部分，在较具体的产品安全功能表示中进行细化。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

6.2.3.6 非形式化产品安全策略模型

对非形式化产品安全策略模型的测试评价方法与预期结果如下：

a） **测试评价方法：**

评价者应审查安全策略模型的如下内容：

——使用非形式化风格来表示；

——描述所有能被模型化的安全策略的规则与特征；

——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；

——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。

b） **预期结果：**

开发者提供的文档内容应满足上述要求。

6.2.4 指导性文档

6.2.4.1 管理员指南

管理员指南的测试评价方法与预期结果如下：

a） 测试评价方法：

评价者应审查开发者是否提供了供授权管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

——产品可以使用的管理功能和接口；

——产品提供给管理员的安全功能和接口的使用方法；

——在安全处理环境中应进行控制的功能和权限；

——所有对与产品的安全操作有关的用户行为的假设；

——所有受管理员控制的安全参数，如果可能，应指明安全值；

——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的实体的安全特性进行的改变；

——所有与授权管理员有关的 IT 环境的安全要求。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

6.2.4.2 用户指南

用户指南的测试评价方法与预期结果如下：

a） 测试评价方法：

评价者应审查开发者是否提供了供用户使用的用户指南，并且此用户指南是否包括如下内容：

——产品的非管理用户可使用的安全功能和接口；

——产品提供给用户的安全功能和接口的使用方法；
——用户可获取但应受安全处理环境控制的所有功能和权限；
——产品安全操作中用户所应承担的职责；
——与用户有关的 IT 环境的所有安全要求。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.2.5 生命周期支持

6.2.5.1 安全措施标识

安全措施标识的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 评价者应审查开发者提供的开发安全文档，该文档是否描述了在系统的开发环境中，为保护系统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；
2） 评价者应现场检查产品的开发环境，开发者是否使用了物理的、程序的、人员的和其他方面的安全措施保证产品设计和实现的保密性和完整性，这些安全措施是否得到了有效的执行。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.2.5.2 开发者定义的生命周期模型

开发者定义的生命周期模型的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 开发者应提供证据证明使用了生命周期模型对产品的开发和维护进行的必要控制，评价者应对证据的内容进行审查；
2） 评价者应审查开发者提供生命周期定义文档是否描述了用于开发和维护产品的模型。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.2.5.3 明确定义的开发工具

明确定义的开发工具的测试评价方法与预期结果如下：

a） 测试评价方法：
评价者应审查开发者所提供的开发安全文档是否明确定义了用于开发产品的工具，并提供了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。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.2.6 测试

6.2.6.1 测试覆盖

6.2.6.1.1 覆盖证据

覆盖证据的测试评价方法与预期结果如下：

a） 测试评价方法：
评价者应审查开发者提供的测试覆盖证据，在测试覆盖证据中，是否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。
b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.2.6.1.2 覆盖分析

覆盖分析的测试评价方法与预期结果如下：
a） **测试评价方法：**
1） **评价者应审查开发者提供的测试覆盖分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的；**
2） **评价测试文档中所标识的测试，是否完整。**
b） **预期结果：**
开发者提供的文档内容应满足上述要求。

6.2.6.1.3 测试：高层设计

测试深度的测试评价方法与预期结果如下：
a） **测试评价方法：**
评价者应审查开发者提供的测试深度分析，是否说明了测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。
b） **预期结果：**
开发者提供的文档内容应满足上述要求。

6.2.6.1.4 功能测试

功能测试的测试评价方法与预期结果如下：
a） 测试评价方法：
1） 开发者提供的测试文档是否包括测试计划、测试规程、预期的测试结果和实际测试结果；
2） 开发者提供的测试计划是否标识了被测试的安全功能，是否描述了测试的目标；
3） 开发者提供的测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；
4） 开发者提供的测试文档中期望的测试结果是否表明测试成功后的预期输出；
5） 开发者提供的测试文档中实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。
b） 预期结果：
开发者提供的文档内容应满足上述要求。

6.2.6.2 独立测试

6.2.6.2.1 一致性

一致性的测试评价方法与预期结果如下：
a） 测试评价方法：
1） 评价者应审查开发者提供的测试产品；
2） 评价者应审查开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致。

b） 预期结果：

开发者应提供能适合第三方测试的产品，并满足上述要求。

6.2.6.2.2 抽样

抽样的测试评价方法与预期结果如下：

a） 测试评价方法：

评价者应审查开发者是否提供一组相当的资源，用于安全功能的抽样测试。

b） 预期结果：

开发者提供的资源应满足上述要求。

6.2.7 脆弱性评定

6.2.7.1 误用

6.2.7.1.1 指南审查

指南审查的测试评价方法与预期结果如下：

a） **测试评价方法：**

1） **评价者应审查开发者提供的指导性文档和分析文档，是否对产品的所有可能的操作方式（包括失败和操作失误后的操作）进行了说明，是否确定了它们的后果，以及是否确定了对于保持安全操作的意义；**

2） **评价者应审查开发者提供的指导性文档和分析文档，是否列出了所有目标环境的假设以及所有外部安全措施（包括外部程序的、物理的或人员的控制）的要求；**

3） **评价者应审查开发者提供的文档是否完整、清晰、一致、合理；**

4） **评价开发者提供的分析文档，是否阐明文档是完整的。**

b） **预期结果：**

开发者提供的文档应满足上述要求。

6.2.7.1.2 分析确认

分析确认的测试评价方法与预期结果如下：

a） 测试评价方法：

评价开发者提供的分析文档论证指导性文档是否是完备的。

b） 预期结果：

开发者提供的文档应满足上述要求。

6.2.7.2 产品安全功能强度评估

产品安全功能强度评估的测试评价方法与预期结果如下：

a） 测试评价方法：

评价者应审查开发者提供的指导性文档，是否对所标识的每个具有安全功能强度声明的安全机制进行了安全功能强度分析，是否说明了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。

b） 预期结果：

开发者提供的文档应满足上述要求。

6.2.7.3 脆弱性分析

6.2.7.3.1 开发者脆弱性分析

开发者脆弱性分析的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 评价者应审查开发者提供的脆弱性分析文档，是否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了分析；

2) 评价者应审查开发者是否对被确定的脆弱性明确记录了采取的措施；

3) 对每一条脆弱性，评价者应审查是否有足够证据证明在使用产品的环境中该脆弱性不能被利用。

b) 预期结果：

开发者提供的文档应满足上述要求，提供的产品应通过脆弱性测试验证。

6.2.7.3.2 独立的脆弱性分析

独立的脆弱性分析的测试评价方法与预期结果如下：

a) **测试评价方法：**

评价者应在开发者提供的脆弱性分析说明文档的基础上，执行穿透性测试，检验已标识的产品脆弱性是否能够抵御明显的穿透性攻击。

b) **预期结果：**

开发者提供的产品资源应满足上述要求，并通过穿透性攻击测试。

6.2.7.3.3 中级抵抗力

中级抵抗力的测试评价方法与预期结果如下：

a) **测试评价方法：**

评价者应根据开发者提供的脆弱性分析说明文档和独立穿透性测试的结果分析产品是否能够抵御中级强度的穿透性攻击，是否说明对脆弱性的搜索是系统化的。

b) **预期结果：**

开发者应提供完备的脆弱性分析说明文档，并通过中级强度的穿透性攻击测试。

7 环境适应性测试

7.1 下一代互联网支持

7.1.1 支持纯 IPv6 网络环境

支持纯 IPv6 网络环境的测试评价方法与预期结果如下：

a) 测试评价方法：

模拟纯 IPv6 网络环境，检测网络隔离产品/网络单向导入产品能够支持纯 IPv6 网络环境，在纯 IPv6 网络环境下其安全功能是否能够正常工作。

b) 预期结果：

网络隔离产品/网络单向导入产品能够支持纯 IPv6 网络环境，在纯 IPv6 网络环境下能够正常工作。

7.1.2 协议一致性

7.1.2.1 IPv6 Core 协议一致性

IPv6 Core 协议一致性的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 若网络隔离产品/网络单向导入产品为地址转换模式，将网络隔离产品/网络单向导入产品与协议一致性测试仪串联；
2) 在协议一致性测试仪上选择 IPv6 Core 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；
3) 若网络隔离产品/网络单向导入产品为透明模式，将网络隔离产品/网络单向导入产品、协议一致性测试仪和任意一台路由器串联；
4) 在协议一致性测试仪上选择 IPv6 Core 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；
5) 再将协议一致性测试仪和路由器串联，重新测试一次 IPv6 Core 协议一致性；
6) 比较两次 IPv6 Core 协议一致性结果的一致性。

b) 预期结果：

1) 若网络隔离产品/网络单向导入产品为地址转换模式，IPv6 Core 协议一致性中必选项均通过测试；
2) 若网络隔离产品/网络单向导入产品为透明模式，前后两次 IPv6 Core 协议一致性结果一致。

7.1.2.2 IPv6 NDP 协议一致性

IPv6 NDP 协议一致性的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 若网络隔离产品/网络单向导入产品为地址转换模式，将网络隔离产品/网络单向导入产品与协议一致性测试仪串联；
2) 在协议一致性测试仪上选择 IPv6 NDP 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；
3) 若网络隔离产品/网络单向导入产品为透明模式，将网络隔离产品/网络单向导入产品、协议一致性测试仪和任意一台路由器串联；
4) 在协议一致性测试仪上选择 IPv6 NDP 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；
5) 再将协议一致性测试仪和路由器串联，重新测试一次 IPv6 NDP 协议一致性；
6) 比较两次 IPv6 NDP 协议一致性结果的一致性。

b) 预期结果：

1) 若网络隔离产品/网络单向导入产品为地址转换模式，IPv6 NDP 协议一致性中必选项均通过测试；
2) 若网络隔离产品/网络单向导入产品为透明模式，前后两次 IPv6 NDP 协议一致性结果一致。

7.1.2.3 IPv6 Autoconfig 协议一致性

IPv6 Autoconfig 协议一致性的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 若网络隔离产品/网络单向导入产品为地址转换模式，将网络隔离产品/网络单向导入产品与协议一致性测试仪串联；

2） 在协议一致性测试仪上选择 IPv6 Autoconfig 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；

3） 若网络隔离产品/网络单向导入产品为透明模式，将网络隔离产品/网络单向导入产品、协议一致性测试仪和任意一台路由器串联；

4） 在协议一致性测试仪上选择 IPv6 Autoconfig 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；

5） 再将协议一致性测试仪和路由器串联，重新测试一次 IPv6 Autoconfig 协议一致性；比较两次 IPv6 Autoconfig 协议一致性结果的一致性。

b） 预期结果：

1） 若网络隔离产品/网络单向导入产品为地址转换模式，IPv6 Autoconfig 协议一致性中必选项均通过测试；

2） 若网络隔离产品/网络单向导入产品为透明模式，前后两次 IPv6 Autoconfig 协议一致性结果一致。

7.1.2.4 IPv6 PMTU 协议一致性

IPv6 PMTU 协议一致性的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 若网络隔离产品/网络单向导入产品为地址转换模式，将网络隔离产品/网络单向导入产品与协议一致性测试仪串联；

2） 在协议一致性测试仪上选择 IPv6 PMTU 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；

3） 若为透明模式，将网络隔离产品/网络单向导入产品、协议一致性测试仪和任意一台路由器串联；

4） 在协议一致性测试仪上选择 IPv6 PMTU 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；

5） 再将协议一致性测试仪和路由器串联，重新测试一次 IPv6 PMTU 协议一致性；

6） 比较两次 IPv6 PMTU 协议一致性结果的一致性。

b） 预期结果：

1） 若网络隔离产品/网络单向导入产品为地址转换模式，IPv6 PMTU 协议一致性中必选项均通过测试；

2） 若网络隔离产品/网络单向导入产品为透明模式，前后两次 IPv6 PMTU 协议一致性结果一致。

7.1.2.5 ICMPv6 协议一致性

ICMPv6 协议一致性的测试评价方法和预期结果如下：

a） 测试评价方法：

1） 若网络隔离产品/网络单向导入产品为地址转换模式，将网络隔离产品/网络单向导入产品与协议一致性测试仪串联；

2） 在协议一致性测试仪上选择 ICMPv6 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；

3） 若网络隔离产品/网络单向导入产品为透明模式，将网络隔离产品/网络单向导入产品、协议一致性测试仪和任意一台路由器串联；
4） 在协议一致性测试仪上选择 ICMPv6 协议一致性测试套件，并选择必选项进行测试，并记录测试结果；
5） 再将协议一致性测试仪和路由器串联，重新测试一次 ICMPv6 协议一致性；
6） 比较两次 ICMPv6 协议一致性结果的一致性。

b） 预期结果：
1） 若网络隔离产品/网络单向导入产品为地址转换模式，ICMPv6 协议一致性中必选项均通过测试；
2） 若网络隔离产品/网络单向导入产品为透明模式，前后两次 ICMPv6 协议一致性结果一致。

7.1.3 协议健壮性

协议健壮性的测试评价方法和预期结果如下：

a） 测试评价方法：
1） 将网络隔离产品/网络单向导入产品与协议健壮性测试仪串联；
2） 在协议健壮性测试仪上选择 IPv6 畸形报文攻击，记录测试结果；
3） 在协议健壮性测试仪上选择 ICMPv6 畸形报文攻击，记录测试结果；
4） 在协议健壮性测试仪上选择其他协议畸形报文攻击，记录测试结果。

b） 预期结果：
1） 网络隔离产品/网络单向导入产品能够抵御 IPv6 畸形报文攻击；
2） 网络隔离产品/网络单向导入产品能够抵御 ICMPv6 畸形报文攻击；
3） 网络隔离产品/网络单向导入产品能够抵御其他协议畸形报文攻击。

7.1.4 IPv6 网络环境下自身管理

IPv6 网络环境下自身管理的测试评价方法和预期结果如下：

a） 测试评价方法：
模拟 IPv6 网络环境，检测网络隔离产品/网络单向导入产品能够支持在 IPv6 网络环境下自身管理。

b） 预期结果：
网络隔离产品/网络单向导入产品能够支持在 IPv6 网络环境下自身管理。

7.2 支持 IPv6 过渡网络环境

7.2.1 双协议栈

双协议栈的测试评价方法和预期结果如下：

a） 测试评价方法：
模拟 IPv4 和 IPv6 两种协议同时存在的网络环境，检测网络隔离产品/网络单向导入产品能够同时支持 IPv4 和 IPv6 两种协议，在 IPv4/IPv6 双栈网络环境下是否能够正常工作。

b） 预期结果：
网络隔离产品/网络单向导入产品能够同时支持 IPv4 和 IPv6 两种协议，在 IPv4/IPv6 双栈网络环境下能够正常工作。

7.2.2 协议转换

协议转换的测试评价方法和预期结果如下：

a） 测试评价方法：

模拟 IPv4 和 IPv6 两种协议相互转换的网络环境，检测网络隔离产品/网络单向导入产品是否能够支持 IPv4 和 IPv6 两种协议相互转换，在 IPv4/IPv6 协议转换网络环境下是否能够正常工作。

b） 预期结果：

网络隔离产品/网络单向导入产品能够支持 IPv4 和 IPv6 两种协议相互转换，在 IPv4/IPv6 协议转换网络环境下能够正常工作。

7.2.3 隧道

7.2.3.1 6over4

6over4 的测试评价方法和预期结果如下：

a） 测试评价方法：

模拟 6over4 隧道的网络环境，检测网络隔离产品/网络单向导入产品是否能够支持 6over4 隧道，在 6over4 隧道网络环境下能够正常工作。

b） 预期结果：

网络隔离产品/网络单向导入产品能够支持 6over4 隧道，在 6over4 隧道网络环境下能够正常工作。

7.2.3.2 6to4

6to4 的测试评价方法和预期结果如下：

a） 测试评价方法：

模拟 6to4 隧道的网络环境，检测网络隔离产品/网络单向导入产品是否能够支持 6to4 隧道，在 6to4 隧道网络环境下能够正常工作。

b） 预期结果：

网络隔离产品/网络单向导入产品能够支持 6to4 隧道，在 6to4 隧道网络环境下能够正常工作。

7.2.3.3 ISATAP

ISATAP 的测试评价方法和预期结果如下：

a） 测试评价方法：

模拟 ISATAP 隧道的网络环境，检测网络隔离产品/网络单向导入产品是否能够支持 ISATAP 隧道，在 ISATAP 隧道网络环境下能够正常工作。

b） 预期结果：

网络隔离产品/网络单向导入产品能够支持 ISATAP 隧道，在 ISATAP 隧道网络环境下能够正常工作。

8 性能测试

8.1 交换速率

网络隔离产品的交换速率的测试评价方法和预期结果如下：

a） 测试评价方法：

查看网络隔离产品交换速率的详细描述。采用测试工具或专用测试设备对网络隔离产品的交换速率进行测试。

b） 预期结果：

网络隔离产品的交换速率性能指标应达到 GB/T 20279—2015 中 5.5.1 规定的最低要求。

8.2 硬件切换时间

网络隔离产品的硬件切换时间的测试评价方法和预期结果如下：

a） 测试评价方法：

查看网络单项导入产品硬件切换时间的详细描述。采用测试工具或专用测试设备对网络隔离产品的切换时间进行测试。

b） 预期结果：

网络隔离产品的硬件切换时间性能指标应达到 GB/T 20279—2015 中 5.5.2 规定的最低要求。

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