



中华人民共和国公共安全行业标准

GA 370—2001

端设备隔离部件安全技术要求

Security requirements for end-equipment isolate components

2001-12-24 发布

2002-05-01 实施

前 言

本标准的全部技术内容为强制性。

本标准由公安部公共信息网络安全监察局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部公共信息网络安全监察局、公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人：朱建平、陆臻、沈亮。

端设备隔离部件安全技术要求

1 范围

本标准规定了端设备隔离部件的分类、安全功能技术要求和安全保证要求。
本标准适用于端设备隔离部件产品的研制、开发、测试、评估和产品的采购。

2 术语和定义

本标准采用下列术语和定义。

2.1

物理隔离 physical isolation

公共网络和专网在网络物理连线上是完全隔离的,且没有任何公用的存储信息。

2.2

逻辑隔离 logical isolation

公共网络和专网在物理上是有连线的,通过技术手段保证在逻辑上是隔离的。

2.3

协议转换 protocol conversion

把公共协议转换为专用协议。

3 端设备隔离部件分类

3.1 物理隔离部件

通过物理隔离的方式,在两个网间转换时,保证计算机的数据在网际间不被重用。该部件的连接如图 1 所示。

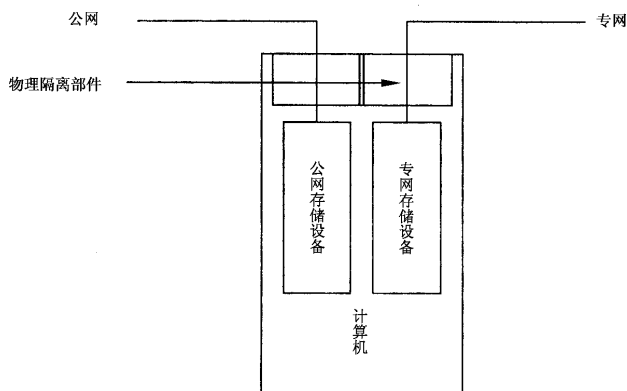


图 1 物理隔离部件连接示意图

3.2 逻辑隔离部件

通过逻辑隔离的方式实现网络间隔离,该部件的连接如图 2 所示。

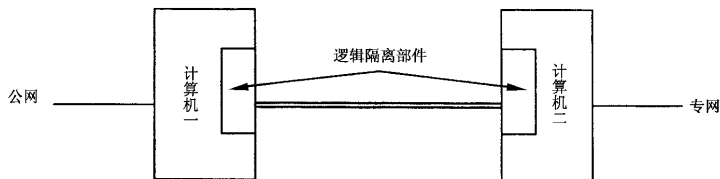


图 2 逻辑隔离部件连接示意图

3.3 单向隔离部件

- 数据流无法从专网流向公网。
- 数据流能在指定存储区域从公网流向专网,对专网而言,能使用公网的某些指定的要导入的数据。该部件的连接如图 3 所示。

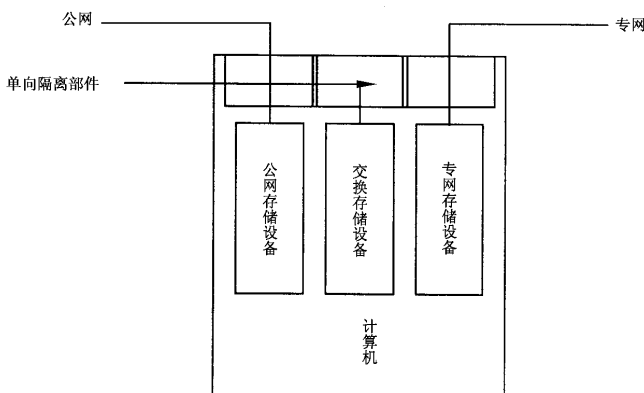


图 3 单向隔离部件连接示意图

4 端设备隔离部件安全功能的技术要求

- 物理隔离部件的安全功能应保证被隔离的计算机资源不能被访问(至少应包括硬盘、软盘和光盘),计算机数据不能被重用(至少应包括内存)。
- 逻辑隔离部件的安全功能应保证被隔离的计算机资源不能被访问,只能进行隔离器内外的原始应用数据交换。
- 单向隔离部件的安全功能应保证被隔离的计算机资源不能被访问(至少应包括硬盘/硬盘分区、软盘和光盘),计算机数据不能被重用(至少应包括内存)。
- 逻辑隔离部件应保证其存在泄露网络资源的风险不得多于开发商的评估文档中所提及的内容。
- 逻辑隔离部件的安全功能应保证在进行数据交换时数据的完整性。
- 逻辑隔离部件的安全功能应保证隔离措施的可控性,隔离的安全策略应由用户进行控制,开发者必须提供可控方法。

5 端设备隔离部件安全功能的保证要求

5.1 最低限度支持

开发商应提供有关隔离安全策略的说明文档。

5.2 开发过程保证

开发商应提供隔离部件产品的技术开发文档。

5.3 交付和操作保证

开发商应提供隔离部件产品的安装说明。

5.4 指南文件保证

开发商应提供隔离部件产品的使用指南。

5.5 测试保证

开发商应提供隔离部件产品的测试文档。

5.6 脆弱性分析保证

开发商应提供隔离部件产品的脆弱性分析文档。

中华人民共和国公共安全
行业标准
端设备隔离部件安全技术要求
GA 370—2001

*

中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行 各地新华书店经售

*

开本 880×1230 1/16 印张 1/2 字数 8 千字
2002 年 4 月第一版 2002 年 4 月第一次印刷
印数 1—1 000

*

书号: 155066·2-14220 定价 8.00 元

网址 www.bzcb.com

版权专有 侵权必究
举报电话:(010)68533533



GA 370-2001