



中华人民共和国国家标准

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

Information security technology—Testing and evaluation
techniques of separation components of network and terminal equipment

2006-05-31 发布

2006-12-01 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	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 隔离部件分级测试评价方法	1
4.1 物理断开隔离部件	1
4.1.1 测试评价环境	1
4.1.2 基本级要求	2
4.1.3 增强级要求	5
4.2 单向隔离部件	11
4.2.1 测试评价环境	11
4.2.2 基本级要求	11
4.2.3 增强级要求	15
4.3 协议隔离部件	20
4.3.1 测试评价环境	20
4.3.2 第一级	21
4.3.3 第二级	25
4.3.4 第三级	34
4.4 网闸隔离部件	46
4.4.1 测试评价环境	46
4.4.2 第一级	47
4.4.3 第二级	51
4.4.4 第三级	60
参考文献	74

前 言

本标准由全国信息安全标准化技术委员会提出并归口。

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。

本标准主要起草人：朱建平、陆臻、沈亮、邱梓华、张奕、张笑笑、顾玮、沈涛、赵婷、邹春明、顾健。

引 言

本标准用以指导测试评价者如何测试与评价隔离部件是否达到了相应的等级,主要从对隔离部件的安全保护等级进行划分的角度来说明其评价准则,以及各评价准则在不同安全级中具体实现上的差异。

本标准以 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》所划分的安全等级为基础,针对隔离部件的技术特点,对相应的测试评价方法做了详细描述。

在本标准文本中,加粗字体表示较高等级中新出现或增强的功能要求。

信息安全技术

网络和终端设备隔离部件测试评价方法

1 范围

本标准规定了网络端设备隔离部件测试评价方法。

本标准适用于按照 GB/T 20279—2006 的安全等级保护要求所开发的隔离部件的测试和评价。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

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

3 术语和定义

GB 17859—1999、GB/T 20271—2006 和 GB/T 20279—2006 确立的术语和定义适用于本标准。

4 隔离部件分级测试评价方法

4.1 物理断开隔离部件

4.1.1 测试评价环境

物理断开隔离部件连接示意如图 1 所示,在安全域 A 网络和安全域 B 网络环境内至少连入一台测试用计算机。

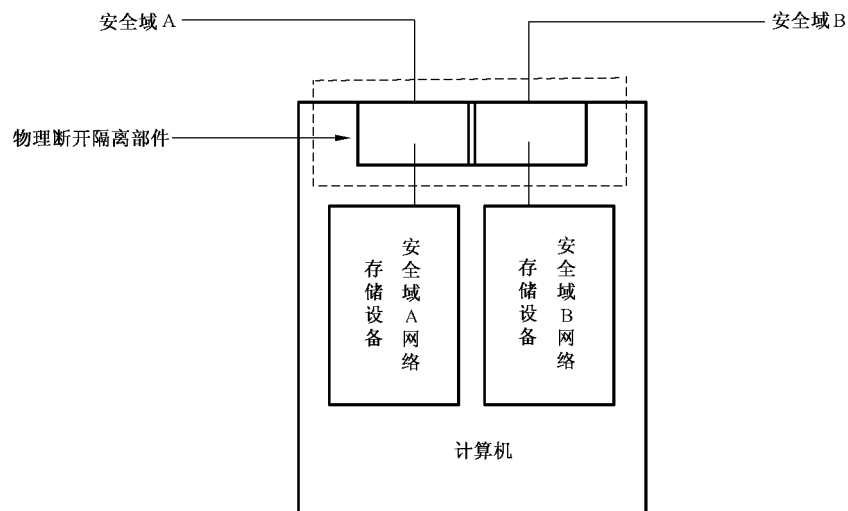


图 1 物理断开隔离部件连接示意图