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