



中华人民共和国国家标准

GB/T 20279—2024

代替 GB/T 20279—2015, GB/T 20277—2015

网络安全技术 网络和终端隔离产品 技术规范

Cybersecurity technology—Technical specification for network and terminal
separation products

2024-09-29 发布

2025-04-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 通则	3
6 安全技术要求	5
6.1 安全功能要求	5
6.2 自身安全要求	9
6.3 性能要求	10
6.4 安全保障要求	11
7 测评方法	13
7.1 安全功能测评	13
7.2 自身安全测评	23
7.3 性能测评	26
7.4 安全保障测评	26
附录 A (规范性) 网络和终端隔离产品分类及安全技术要求级别划分	33
附录 B (规范性) 网络和终端隔离产品分类及测评方法级别划分	39

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 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》和 GB/T 20277—2015《信息安全技术 网络和终端隔离产品测试评价方法》，与 GB/T 20279—2015 和 GB/T 20277—2015 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 更改了网络隔离类产品的产品分类(见第 5 章,GB/T 20279—2015 年版的第 4 章)；
- 增加了通则(见第 5 章)；
- 更改了信息流控制策略要求(见 6.1.1.1,GB/T 20279—2015 年版的 5.2.2.1.1.1、5.2.2.2.1.1、5.2.3.1.1.1 和 5.2.3.2.1.1)；
- 更改了信息流控制功能要求(见 6.1.1.2,GB/T 20279—2015 年版的 5.2.2.1.1.2、5.2.2.2.1.2、5.2.3.1.1.2、5.2.3.2.1.2 和 5.2.3.2.1.3)；
- 增加了应用及协议支持要求(见 6.1.2)；
- 增加了信息过滤要求(见 6.1.3)；
- 更改抗攻击要求为攻击防护要求(见 6.1.5,GB/T 20279—2015 年版的 5.2.2.1.2、5.2.2.2.2、5.2.3.1.2 和 5.2.3.2.2)；
- 更改域隔离要求为安全隔离要求(见 6.1.6,GB/T 20279—2015 年版的 5.2.2.1.6、5.2.2.2.6、5.2.3.1.6 和 5.2.3.2.6)；
- 更改容错要求为高可用要求(见 6.1.7,GB/T 20279—2015 年版的 5.2.2.1.7、5.2.2.2.7 和 5.2.3.2.7)；
- 增加了联动要求(见 6.1.10)；
- 更改环境适应性要求为 IPv6 支持要求(见 6.1.11,GB/T 20279—2015 年版的 5.4)；
- 增加了虚拟化部署要求(见 6.1.12)；
- 增加了自身安全要求(见 6.2)；
- 更改了性能要求(见 6.3,GB/T 20279—2015 年版的 5.5)；
- 更改了安全保障要求(见 6.4,GB/T 20279—2015 年版的 5.3)；
- 增加了网络和终端隔离产品分类及安全技术要求级别划分(见附录 A)；
- 增加了网络和终端隔离产品分类及测评方法级别划分(见附录 B)。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：公安部第三研究所、国家工业信息安全发展研究中心、中国网络安全审查认证和市场监管大数据中心、中国电子技术标准化研究院、北京天融信网络安全技术有限公司、北京安盟信息技术股份有限公司、中孚信息股份有限公司、清华大学、深圳市利谱信息技术有限公司、启明星辰信息技术集团股份有限公司、珠海经济特区伟思有限公司、拓尔思天行网安信息技术有限责任公司、奇安信网神信息技术(北京)股份有限公司、中国科学院软件研究所、公安部第一研究所、腾讯云计算(北京)有限责任公司、西安交大捷普网络科技有限公司、北京数安行科技有限公司、山东首瀚信息科技有限公司、长扬科技(北京)股份有限公司、郑州信大捷安信息技术股份有限公司、新华三技术有限公司、国网区块链科技(北京)有限公司、蓝盾信息安全技术股份有限公司、广州天懋信息系统股份有限公司、南方电网电力科技股份有限公司、中电科网络安全科技股份有限公司、南京神易网络科技有限公司、蓝象标准

(北京)科技有限公司、杭州领信数科信息技术有限公司、成都赛波安全技术开发有限公司。

本文件主要起草人：陆臻、祝国邦、李旋、顾健、顾建新、沈亮、安高峰、刘智飞、马奥、杨晨、孙彦、张东举、王冲华、申永波、沈文杰、江军、路文立、焦蒙蒙、左安骥、张习雨、卢栋梁、晏敏、杨春华、胡维娜、王路晗、张凌云、乔华阳、余果、刘玉红、杨更、赵华、刘为华、何建锋、石竹玉、焦少波、万晓兰、李士奇、常媛媛、刘强、邹凯、林迪、李克鹏、韩秀德、张大伟、赵会敏、钱韵洁、丁稳所、杨威、张震宇、林丹生、李慧敏、郭爱波。

本文件及其所代替文件的历次版本发布情况为：

——GB/T 20279, 2006 年首次发布, 2015 年第一次修订；

——GB/T 20277, 2006 年首次发布, 2015 年第一次修订；

——本次为第二次修订。

网络安全技术 网络和终端隔离产品 技术规范

1 范围

本文件规定了网络和终端隔离产品的分类、级别划分、安全技术要求及测评方法。
本文件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

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第3部分:安全保障组件

GB/T 25069—2022 信息安全技术 术语

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求

3 术语和定义

GB/T 18336.3—2024、GB/T 25069—2022、GB/T 30279—2020 和 GB 42250—2022 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

遵从共同安全策略的资产和资源的集合。

[来源:GB/T 25069—2022,3.36]

3.2

物理断开 physical disconnection

使用物理方法保证不同安全域之间无法以直接或间接的方式相连接的技术。

注:实施不同安全域的物理断开,包括在物理传导、物理存储上的断开。

3.3

协议转换 protocol conversion

把基于网络的公共协议中的应用数据剥离出来,封装为系统专用的私有协议进行数据传输的技术。

3.4

信息摆渡 information ferry

信息由信息源所在安全域传输至中间缓存区域,再将中间缓存区域的信息传输至信息目的所在安全域的数据传输技术。

注:在任一时刻,中间缓存区域只与一端安全域相连。