

YD

中华人民共和国通信行业标准

YD/T ××××—××××

支持拟态防御功能设备的总体技术指南

Technical guideline of devices supported mimic architecture

××××-××-××发布

××××-××-××实施

中华人民共和国工业和信息化部发布

## 目次

前言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 支持拟态防御功能设备的架构和功能模块.....	3
4.1 支持拟态防御功能设备总体架构.....	3
4.2 输入代理器.....	3
4.3 输出裁决器.....	4
4.4 异构执行体.....	4
4.5 异构执行体池.....	4
4.6 负反馈控制器.....	4
5 支持拟态防御功能设备的工作流程.....	4
5.1 拟态防御流程.....	4
5.2 执行体清洗工作流程.....	5
5.3 差模注入测试工作流程.....	6
5.4 N-1 模注入测试工作流程.....	7
5.5 N 模注入测试工作流程.....	8

行业标准信息服务平台

## 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。

本文件是“支持拟态防御功能的设备”系列标准之一，该系列标准的结构和名称预计如下：

- 1) 支持拟态防御功能设备的总体技术指南
- 2) 支持拟态防御功能的Web服务器技术要求
- 3) 支持拟态防御功能的Web服务器检测规范
- 4) 支持拟态防御功能的路由器技术要求
- 5) 支持拟态防御功能的路由器检测规范
- 6) 支持拟态防御功能的域名服务器技术要求
- 7) 支持拟态防御功能的域名服务器检测规范
- 8) 支持拟态防御功能的交换机技术要求
- 9) 支持拟态防御功能的交换机检测规范
- 10) 支持拟态防御功能的防火墙技术要求
- 11) 支持拟态防御功能的防火墙检测规范
- 12) 支持拟态防御功能的分布式存储系统技术要求
- 13) 支持拟态防御功能的分布式存储系统检测规范
- 14) 支持拟态防御功能的安全网关技术要求
- 15) 支持拟态防御功能的安全网关检测规范
- 16) 支持拟态防御功能的云组件技术要求和测试方法

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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院，中国人民解放军战略支援部队信息工程大学，网络通信与安全紫金山实验室，之江实验室，珠海高凌信息科技股份有限公司，北京天融信网络安全技术有限公司，上海红阵信息科技有限公司。