

ICS 35.030
CCS L70

YD

中华人民共和国通信行业标准

YD/T ××××—××××

支持拟态防御功能的防火墙技术要求

Technical requirements of firewall 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 缩略语.....	1
5 概述.....	1
6 支持拟态防御功能的防火墙通用技术要求.....	2
7 支持拟态防御功能的防火墙拟态功能要求.....	2
7.1 安全运维管理要求.....	2
7.2 网络层控制要求.....	2
7.3 应用层控制要求.....	3
7.4 输入输出代理要求.....	3
7.5 动态调度要求.....	3
7.6 拟态裁决要求.....	3
7.7 反馈控制要求.....	3
7.8 日志接口要求.....	4
8 支持拟态防御功能的防火墙性能要求.....	4
8.1 清洗时间.....	4
8.2 调度周期.....	4
8.3 系统恢复时间.....	4
9 支持拟态防御功能的防火墙安全要求.....	4
9.1 差模注入情况安全要求.....	4
9.2 N-1 模注入情况安全要求.....	4
9.3 N 模注入情况安全要求.....	5
附录 A（资料性）性能指标计算依据和参考阈值.....	6
A.1 清洗时间.....	6
A.2 调度周期.....	6
A.3 系统恢复时间.....	6

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，北京天融信网络安全技术有限公司，中国人民解放军战略支援部队信息工程大学，中国联合网络通信集团有限公司。