ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 31499—2026
代替 GB/T 31499—2015

网络安全技术　统一威胁管理产品(UTM)技术规范

Cybersecurity technology—Technical specification for the unified threat management products

2026-04-30 发布　　2026-11-01 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

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 31499—2015《信息安全技术　统一威胁管理产品技术要求和测试评价方法》，与GB/T 31499—2015相比，除结构调整和编辑性修改外，主要技术变化如下：

——更改了术语“统一威胁管理产品”“告警”的定义，增加了“威胁”的术语和定义（见第3章，2015年版的第3章）；

——增加了缩略语“BGP”“CC”“DMZ”“IKE”“IPv4”“IPv6”“MAC”“POP3”“SMB”“UTM”“VPN”（见第4章）；

——更改了概述的UTM架构图和分级说明（见第5章，2015年版的第5章、第6章）；

——更改了“访问控制”的要求和测评方法，增加了协议和应用类型，更改了垃圾邮件识别方式，增加了垃圾邮件处理方式（见6.1.2、7.2.2，2015年版的7.1.1.2、7.2.1.2、7.1.1.3、7.2.1.3、7.1.1.4、7.2.1.4、7.2.1.7、8.2.3.2、8.2.3.3、8.2.3.4、8.2.3.7）；

——更改了“入侵防范”的要求和测评方法，增加了能发现和检测的入侵行为类型（见6.1.3、7.2.3，2015年版的7.1.1.5、7.2.1.5、8.2.3.5）；

——更改了“恶意程序防范”的要求和测评方法，增加了恶意程序清单（见6.1.4、7.2.4，2015年版的7.1.1.6、7.2.1.6、8.2.3.6）；

——更改了“安全组网”的要求和测评方法，增加了虚拟专用网功能要求（见6.1.5、7.2.5，2015年版的7.1.1.1、7.2.1.1、8.2.3.1）；

——更改了“安全管理”的要求和测评方法（见6.1.6、7.2.6，2015年版的7.1.1.7、7.2.1.8、8.2.3.8）；

——更改了“安全审计”的要求和测评方法（见6.1.7、7.2.7，2015年版的7.1.1.5、7.2.1.5）；

——增加了“互联互通”的要求和测评方法（见6.1.8、7.2.8）；

——更改了“自身安全”的要求和测评方法（见6.2、7.3，2015年版的7.1.2、7.2.2、8.2.4）；

——更改了“性能”要求和测评方法（见6.3、7.4，2015年版的7.3、8.3）；

——增加了“环境适应性”要求和测评方法（见6.4、7.5）；

——更改了“安全保障”的要求和测评方法（见6.5、7.6，2015年版的7.1.3、7.2.3、8.2.5）；

——增加了规范性附录“统一威胁管理产品（UTM）安全技术要求分级和测试评价方法”（见附录A）。

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：启明星辰信息技术集团股份有限公司、公安部第三研究所、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、公安部第一研究所、上海市信息安全测评认证中心、北京天融信网络安全技术有限公司、中国电子科技集团公司第十五研究所、中科信息安全共性技术国家工程研究中心有限公司、北京山石网科信息技术有限公司、深信服科技股份有限公司、西安交大捷普网络科技有限公司、中国科学院信息工程研究所、中国信息通信研究院、奇安信网神信息技术（北京）股份有限公司、北京神州绿盟科技有限公司、新华三技术有限公司、中移动信息技术有限公司、长扬科技（北京）股份有限公司、北京数安行科技有限公司、北京浩瀚深度信息技术股份有限公司、南方电网数字电网集团信息通信科技有限公司、华为技术有限公司、南方电网数据平台与安全（广东）有限公司。

本文件主要起草人：张其华、胡月、牛国君、高鹏、俞优、胡石、李彦峰、申永波、韩龙、徐佟海、姜威、雷晓锋、安高峰、刘艺翔、董晶晶、马多贺、胡建勋、付巍、何建锋、戴方芳、董悦、周飞虎、王杨军、胡栋栋、孙松儿、周龙彬、张亚京、庞韶敏、刘玉红、黄国柱、李翔、邹文景。

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布为GB/T 31499—2015；

——本次为第一次修订。

引　言

本文件是GB 42250—2022《信息安全技术　网络安全专用产品安全技术要求》的配套标准。GB 42250—2022与本文件共同用于指导统一威胁管理产品(UTM)的设计、研发、生产、检测或认证工作。

网络安全技术　统一威胁管理产品(UTM)技术规范

1　范围

本文件规定了统一威胁管理产品(UTM)的安全功能要求、自身安全要求、环境适应性要求、性能要求、安全保障要求和分级要求,并描述了对应的测试评价方法。

本文件适用于统一威胁管理产品(UTM)的设计、研发、生产、检测或认证。

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—2024(所有部分)　网络安全技术　信息技术安全评估准则

GB/T 25069—2022　信息安全技术　术语

GB/T 36968—2018　信息安全技术　IPSec VPN 技术规范

GB 42250—2022　信息安全技术　网络安全专用产品安全技术要求

GB/T 44886.1—2024　网络安全技术　网络安全产品互联互通　第1部分:框架

GB/T 44886.2—2025　网络安全技术　网络安全产品互联互通　第2部分:资产信息格式

GB/T 44886.3—2025　网络安全技术　网络安全产品互联互通　第3部分:告警信息格式

3　术语和定义

GB/T 18336—2024(所有部分)、GB/T 25069—2022 和 GB 42250—2022 界定的以及下列术语和定义适用于本文件。

3.1

威胁　threat

可能对系统或组织造成危害的不期望事件的潜在因素。

[来源:GB/T 25069—2022,3.628]

3.2

统一威胁管理产品　unified threat management product

通过统一部署的安全策略,融合多种安全功能,对网络及应用系统的安全威胁进行综合管理与防御的设备或系统。

[来源:GB/T 25069—2022,3.601,有修改]

3.3

告警　alert

产品依据设定的规则,对采集到的网络安全信息自动进行规则匹配、归并、分析等活动后产生警示信息的动作。