ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35277—2017

信息安全技术　防病毒网关安全技术要求和测试评价方法

Information security technology—Security technical requirements and testing and evaluation approaches for antivirus gateway products

2017-12-29 发布　　2018-07-01 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。

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:国家计算机病毒应急处理中心、国家信息中心、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、中国科学院大学、北京安天网络安全技术有限公司、北京瑞星信息技术股份有限公司、亚信科技(成都)有限公司、北京冠群金辰软件有限公司、北京网御星云信息技术有限公司、网神信息技术(北京)股份有限公司、华为技术有限公司。

本标准主要起草人:陈建民、杜振华、张瑞、刘威、曹鹏、黄一斌、刘健、禄凯、肖新光、叶荣军、张玉清、王文杰、白日、高晓立、王光宇、杨黎鸿、刘振华、刘彦、张泰然、张喆、邓莹、彭立炜、孙波、李冬、舒心、张韫菁、冯军亮、马天成、刘杨、王文一、徐双双。

信息安全技术　防病毒网关安全技术要求和测试评价方法

1　范围

本标准规定了防病毒网关的技术要求和测试评价方法。

本标准适用于防病毒网关的设计、开发及检测。

2　术语和定义

下列术语和定义适用于本文件。

2.1

防病毒网关　antivirus gateway

部署于网络和网络之间，通过分析网络层和应用层的通信，根据预先定义的过滤规则和防护策略，实现对网络内的病毒防护。

2.2

病毒　virus

能够影响计算机操作系统、应用程序和数据的完整性、可用性、可控性和保密性的计算机程序或代码，包括文件型病毒、蠕虫、木马程序、宏病毒、脚本病毒等恶意程序。

2.3

隔离　quarantine

防病毒网关在对病毒进行处理时，为保留病毒样本以及受感染的文件，而采取将病毒以及受感染的文件存储在一个被称之为“隔离区”的受限制存储空间的处理方式。

2.4

内部网络　internal network

通过防病毒网关隔离的可信任区域或保护区域。

2.5

外部网络　external network

通过防病毒网关隔离的不可信任区域或非保护区域。

2.6

最大并发连接数　maximum concurrent connection capacity

防病毒网关所能保持的最大并发连接数量。

2.7

最大新建连接速率　maximum connection establishment rate

防病毒网关在单位时间内所能建立的最大连接数，一般是每秒新建的连接数。

2.8

恶意 URL　malicious URL

指向的资源中含有病毒的 URL。