ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 25068.4—2022/ISO/IEC 27033-4:2014
代替 GB/T 25068.3—2010

信息技术　安全技术　网络安全 第4部分:使用安全网关的网间通信安全保护

Information technology—Security techniques—Network security—Part 4: Securing communications between networks using security gateways

（ISO/IEC 27033-4:2014,IDT）

2022-10-12 发布　　2023-05-01 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。

本文件是GB/T 25068《信息技术　安全技术　网络安全》的第4部分。GB/T 25068已发布了以下部分:

——第1部分:综述和概念;

——第2部分:网络安全设计和实现指南;

——第3部分:面向网络接入场景的威胁、设计技术和控制;

——第4部分:使用安全网关的网间通信安全保护;

——第5部分:使用虚拟专用网的跨网通信安全保护。

本文件代替GB/T 25068.3—2010《信息技术　安全技术　IT网络安全　第3部分:使用安全网关的网间通信安全保护》。与GB/T 25068.3—2010相比,除结构调整和编辑性改动外,主要技术变化如下:

a) 更改了陈述“范围”时所使用的推荐条款和表述方式(见第1章,2010年版的第1章);

b) 更改了“术语和定义”的内容(见第3章,2010年版的第3章);

c) 删除了“IT”“IDP”“V.35”等缩略语,增加了“ACL”“ASIC”“CPU”“DDoS”“URL”等缩略语(见第4章,2010年版的第4章);

d) 增加了“文档结构”“概述”“安全威胁”三章(见第5章～第7章);

e) 将“安全要求”更改为“安全需求”,增加了“表1”,并将2010年版的有关内容更改后纳入(见第8章,2010年版的第5章);

f) 将“安全网关技术”更改为“安全控制”(见第9章,2010年版的第6章),增加了要素“通则”(见9.1)、“入侵防御系统和入侵检测系统”(见9.6)、“安全管理API”(见9.7),删除了要素“网络地址转换(NAT)”(见2010年版的6.4);

g) 删除了“状态包检测防火墙”与“应用代理防火墙”的优缺点比较,并将2010年版的有关内容更改后纳入(见9.3,2010年版的6.2);

h) 将“应用代理”更改为“应用防火墙”,并将2010年版的有关内容更改后纳入(见9.4,2010年版的6.3);

i) 将“内容分析和过滤”更改为“内容过滤”,增加了“内容分析”列项“协议分析”,并将2010年版的有关内容更改后纳入(见9.5,2010年版的6.5);

j) 将“安全网关组件”与“安全网关体系结构”两章合并为“设计技术”一章,删除了悬空段引导词,重新绘制了示意图(见图3～图6,2010年版的图1～图4),并将2010年版的有关内容更改后纳入(见第10章,2010年版的第7章、第8章);

k) 增加了“可能存在负载均衡交换机”的使用规则(见10.1.1,2010年版的7.1);

l) 将“应用级网关”更改为“应用层网关”,增加了“SIP网关”的使用规则,并将2010年版的有关内容更改后纳入(见10.1.3,2010年版的7.3);

m) 增加了“监控功能”的使用规则(见10.1.5);

n) 将“安全网关体系结构”更改为“部署安全网关控件”,删除了悬置段(见10.2,2010年版的8.1);

o) 删除了要素“层次化方法”(见2010年版的8.2);

p) 删除了关于“屏蔽主机体系结构”优缺点的表述段落(见 2010 年版的 8.1.3);

q) 增加了“包过滤防火墙”的使用规则(见 10.2.1);

r) 增加了要素“通则”(见 11.1);

s) 将“安全特点和设置”更改为“安全功能设置”,增加了“支持对打包的企业或其他业务应用程序的代理服务”和“支持识别协议流中运行的应用(如办公效率应用、嵌入式视频、即时消息等)”的推荐条款,并将 2010 年版的有关内容更改后纳入(见 11.5,2010 年版的 9.4);

t) 增加规定了“细粒度的访问权限”(见 11.6,2010 年版的 9.6);

u) 删除了要素“文档化”(见 2010 年版的 9.7);

v) 增加了要素“实现类型”和要素“高可用性和运行模式”(见 11.10、11.11)。

本文件等同采用 ISO/IEC 27033-4:2014《信息技术 安全技术 网络安全 第 4 部分:使用安全网关的网间通信安全保护》。

本文件做了下列最小限度的编辑性改动:

——用资料性引用的 GB/T 20985.2—2020 替换了 ISO/IEC 27035(见 9.1);

——用资料性引用的 GB/T 28454—2020 替换了 ISO/IEC 27039(见 9.5);

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。

本文件由全国信息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:黑龙江省网络空间研究中心、中国电子技术标准化研究院、安天科技集团股份有限公司、黑龙江安信与诚科技开发有限公司、上海工业控制安全创新科技有限公司、哈尔滨理工大学、哈尔滨工业大学。

本文件主要起草人:方舟、曲家兴、谷俊涛、于海宁、肖鸿江、李琳琳、李锐、宋雪、杨霄璇、白瑞、王大萌、上官晓丽、甘俊杰、杜宇芳、呼大永、马遥、黄海、树彬、张国华、燕思嘉、许言、吴琼、姜天一、周莹、曹威、方伟、童松华、赵超、祝宇琳、石冬青、单建中、孟庆川、倪华。

本文件及其所代替文件的历次版本发布情况为:

——2010 年首次发布为 GB/T 25068.3—2010;

——本次为第一次修订,编号调整为 GB/T 25068.4—2022。

引　言

GB/T 25068 的目的是为信息系统网络的管理、运行、使用及互联互通提供安全方面的详细指导。方便组织内负责信息安全特别是网络安全的人员能够采纳本文件以满足其特定需求。拟由六个部分构成。

——第 1 部分：综述和概念。目的是定义和描述与网络安全相关的概念并提供管理指导。

——第 2 部分：网络安全设计和实现指南。目的是为组织如何规划、设计、实现高质量的网络安全体系，以确保网络安全适合相应的业务环境提供指导。

——第 3 部分：面向网络接入场景的威胁、设计技术和控制。目的是列举与典型的网络接入场景相关的具体风险、设计技术和控制，适用于所有参与网络安全架构方面规划、设计和实施的人员。

——第 4 部分：使用安全网关的网间通信安全保护。目的是确保使用安全网关的网间通信安全。它提供了如何识别和分析与安全网关相关的网络安全威胁、基于威胁分析定义安全网关的网络安全需求、介绍了以解决典型网络场景相关的威胁和控制方面的网络技术安全结构设计技术实现，并解决与使用安全网关实施、操作、监视和审查网络安全控制相关问题的指南。本文件适用于所有参与安全网关详细规划、设计和实施的人员（例如网络架构师和设计人员、网络管理员和网络安全主管）。

——第 5 部分：使用虚拟专用网的跨网通信安全保护。目的是定义使用虚拟专用网络建立安全连接的具体风险、设计技术和控制要素。

——第 6 部分：无线网络访问安全。目的是为选择、实施和监测使用无线网络提供安全通信所必需的技术控制提供指南，并用于第 2 部分中涉及使用无线网络的技术安全架构或设计选项的审查与选择。

GB/T 25068 是在 GB/T 22081《信息技术　安全技术　信息安全控制实践指南》的基础上，进一步对网络安全控制提供了详细的实施指导。GB/T 25068 仅强调业务类型等因素影响网络安全的重要性而不做具体说明。

本文件凡涉及采用密码技术解决保密性、完整性、真实性、抗抵赖性需求的，遵循密码相关国家标准和行业标准。

信息技术　安全技术　网络安全
第4部分:使用安全网关的网间通信安全保护

1　范围

本文件提供了使用安全网关(防火墙、应用防火墙、入侵防护系统等)的网络间通信安全保护指南,这些安全网关按照文档化的信息安全策略进行通信,指南包括:

a)　识别和分析与安全网关相关的网络安全威胁;

b)　基于威胁分析来定义安全网关的网络安全需求;

c)　使用设计和实现的技术来解决与典型的网络场景相关的威胁和控制方面的问题;

d)　指出实施、操作、监视和评审网络安全网关控制措施相关的问题。

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。

ISO/IEC 27033-1　信息技术　安全技术　网络安全　第1部分:综述和概念(Information technology—Security techniques—Network security—Part 1: Overview and concepts)

注:GB/T 25068.1—2020　信息技术　安全技术　网络安全　第1部分:综述和概念(ISO/IEC 27033-1:2015,IDT)

3　术语和定义

ISO/IEC 27033-1界定的以及下列术语和定义适用于本文件。

3.1

堡垒主机　bastion host

用于拦截进出网络的数据包、经加固操作系统的特定主机,任何外部人员访问组织防火墙内的服务和系统时,应连接该主机系统。

3.2

终端软件防火墙　end-point software-based firewall

根据终端用户自定义的安全策略允许或拒绝通信,保护进出单机的网络流量的软件应用程序。

3.3

加固操作系统　hardened operating system

专门配置或设计的操作系统,以最大限度地减少潜在的不良内容或攻击的可能性。

注:可能是通用操作系统,例如为适应环境专门配置的Linux系统,或具有更高自定义程度的解决方案。

3.4

互联网网关　Internet gateway

接入互联网的端口设备。