企业网络安全防护
职业技能等级标准

（2020年3月1.0版）

上海海盾安全技术培训中心　制定

2020 年 3 月

目 次

前　　言

本标准按照GB/T1.1-2009给出的规则起草。

本标准起草单位：公安部网络安全保卫局、公安部第三研究所、西安交通大学、中国人民公安大学、国家网络与信息系统安全产品质量监督检验中心、国家反计算机入侵和防病毒研究中心、公安部信息安全等级保护评估中心、上海海盾安全技术培训中心、上海交通大学网络信息中心、北京网络行业协会、上海市信息网络安全管理协会、广西网络安全协会、杭州安恒信息技术股份有限公司、北京安博通科技股份有限公司、盾盟（上海）网络科技有限公司。

本标准主要起草人：赵云霞、黄镇、郑庆华、何晓霞、江雪、樊亦胜、胡巍、宋好好、黄淑华、姜开达、赵瑞华、朱政洪、向荣、罗艺、刘春梅、冯伟、荣漪涛、陆臻铭、崔孝晨、吴鸣旦、曾辉、陈奇。

1 范围

本标准规定了企业网络安全防护职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于企业网络安全防护职业技能培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 25068.1　信息技术　安全技术　IT 网络安全

GB/T 22239-2019　信息安全技术　网络安全等级保护基本要求

GB/T 25058-2019　信息安全技术　网络安全等级保护实施指南

GB/T 25069-2010　信息安全技术　术语

3 术语和定义

GB/T 25068.1、GB/T 22239-2019、GB/T 25058-2019、GB/T 25069-2010 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 25068.1、GB/T 22239-2019、GB/T 25058-2019、GB/T 25069-2010 中的某些术语和定义。

3.1 网络安全　cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.2 安全防护　security protection

抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态。

3.3 安全审计 security audit

对信息系统的各种事件及行为实行监测、信息采集、分析，并针对特定事件及行为采取相应的动作。

3.4 **虚拟专用网** virtual private network

一种采用隧道技术连接的虚拟网络，即受限使用的逻辑计算机网络，该网络基于物理网络系统资源所构建，穿越实际网络建立连接。

3.5 **加密** encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

3.6 **防火墙** firewall

设置在网络环境之间的一类安全网关或者屏障。防火墙可以是一台专用设备，也可以是若干部件和技术的组合。防火墙具有如下特性：网络环境间所有通信流量都要流经防火墙，且仅允许授权的流量通过。

3.7 **访问控制** access control

确保对资产的访问是基于业务和安全要求进行授权和限制的手段。

3.8 **入侵** intrusion

对某一网络或联网系统的未经授权的访问，即对某一信息系统的有意无意的未经授权的访问（包括针对信息的恶意活动）。

3.9 **入侵检测** intrusion detection

检测入侵的正式过程。该过程一般特征为采集如下知识：反常的使用模式，被利用的脆弱性及其类型、利用的方式，以及何时发生和如何发生。

3.10 **入侵检测系统** intrusion detection system IDS

在信息系统和网络中，一种用于辨识某些已经尝试、正在发生或已经发生的入侵行为，并可对其做出响应的技术系统。

3.11 **入侵防御系统** intrusion prevention system IPS

一种提供主动响应能力的入侵检测系统。

3.12 攻击 attack

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

3.13 证书 certificate

关于实体的一种数据，该数据由认证机构的私钥或秘密密钥签发，并无法伪造。

3.14 安全策略 security policy

用于治理组织及其系统内在安全上如何管理、保护和分发资产（包括敏感信息）的一组规则、指导和实践，特别是那些对系统安全及相关元素具有影响的资产。

4 适用院校专业

中等职业学校：计算机网络技术、计算机应用、软件与信息服务、电子与信息技术、通信技术、电子技术应用、网站建设与管理等、网络安防系统安装与维护等专业。

高等职业学校：信息安全与管理、计算机应用技术、计算机网络技术、计算机信息管理、计算机系统与维护、移动应用开发、移动互联应用技术、软件与信息服务、软件技术、电子商务技术、云计算技术与应用、通信技术等专业。

应用型本科学校：信息安全、网络工程、计算机科学与技术、电子信息工程、信息工程、软件工程等专业。

5 面向工作岗位（群）

企业网络安全防护（初级）：主要面向全国联网单位、互联网企业和网络安全企业中的网络安全技术岗位，根据业务和安全需求，进行常见操作系统安全配置、网络设备安全配置，应用服务器和客户端安全配置、数据备份等操作，履行网络安全义务，进行互联网安全管理和信息保护等。

企业网络安全防护（中级）：主要面向全国联网单位、互联网企业和网络安

全企业中的网络安全技术岗位，根据业务和安全需求，使用各类安全工具对企业网络安全事件进行分析、响应、溯源，对企业网络、系统进行安全检查，入侵行为检测、流量监测、日志分析、数据备份、应急处置等操作，进行互联网安全管理和信息保护等。

企业网络安全防护（高级）：主要面向全国联网单位、互联网企业和网络安全企业中的网络安全技术岗位，根据业务和安全需求，进行网络安全、系统安全、应用安全的诊断与加固，网络安全等级保护建设、关键基础设施保护、互联网安全管理等。

6 职业技能要求

6.1 职业技能等级划分

企业网络安全防护职业技能等级分为三个等级：初级、中级、高级。三个级别逐次递进，高级别涵盖低级别职业技能要求。

6.2 职业技能等级要求描述

表 1 企业网络安全防护（初级）

工作领域	工作任务	职业技能要求
1.操作系统安全配置	1.1 Windows 系统安全配置	1.1.1 能根据企业系统安全需求，合理配置、管理系统账户。 1.1.2 能根据企业系统安全需求，合理配置、管理文件访问权限。 1.1.3 能根据企业系统安全需求，合理配置、管理系统网络访问策略。 1.1.4 能根据企业系统安全需求，对系统进行安全审计、备份。
	1.2 Linux 系统安全配置	1.2.1 能根据企业系统安全需求，部署、配置 Linux 操作系统，安全管理 Linux 文件系统。 1.2.2 能根据企业系统安全需求，合理配置、管理 Linux 系统账户。 1.2.3 能根据企业系统安全需求，合理配置、管理 Linux 系统网络访问策略。 1.2.4 能根据企业系统安全需求，对系统进行安全审计、备份。

工作领域	工作任务	职业技能要求
	1.3 移动终端操作系统安全配置	1.3.1 能根据企业移动终端系统安全需求，安全管理移动终端操作系统。 1.3.2 能根据企业移动终端系统安全需求，安全管理移动终端操作系统上的应用。 1.3.3 能根据企业移动终端系统安全需求，配置移动端虚拟专用网络(VPN)。 1.3.4 能根据企业移动终端系统安全需求，加固移动终端操作系统，并备份、加密重要信息。
2.基础网络与安全设备配置	2.1 交换机安全配置	2.1.1 能根据企业业务网络拓扑安全需求，部署交换机，对交换机进行基本设置。 2.1.2 能根据企业业务网络拓扑安全需求，对交换机接口进行安全设置。 2.1.3 能根据企业业务网络拓扑安全需求，配置交换机安全远程管理。 2.1.4 能根据企业业务网络拓扑安全需求，对交换机进行安全加固。
	2.2 路由器安全配置	2.2.1 能根据企业业务网络拓扑安全需求，部署路由器，对路由器进行基本设置。 2.2.2 能根据企业业务网络拓扑安全需求，配置安全路由协议，设置合适的访问控制策略。 2.2.3 能根据企业业务网络拓扑安全需求，配置路由器安全远程管理。 2.2.4 能根据企业业务网络拓扑安全需求，对路由器进行安全加固。
	2.3 防火墙安全配置	2.3.1 能根据企业安全需求，部署防火墙，对防火墙进行基本设置。 2.3.2 能根据企业安全需求，配置防火墙基本安全策略。 2.3.3 能根据企业安全需求，配置防火墙安全远程管理。 2.3.4 能根据企业安全需求，对防火墙进行安全加固。 2.3.5 能根据企业安全需求，设置、管理防火墙日志。
3.应用安全配置	3.1 应用服务器安全配置	3.1.1 能根据企业 Web 服务设计方案，独立安装、部署、调试 Web 服务。 3.1.2 能根据企业 Web 服务设计方案，配置基础 Web 服务安全。 3.1.3 能根据企业安全需求，安装、部署、配置文件服务。 3.3.4 能根据企业安全需求，配置文件服务器安全策略。
	3.2 客户端安全配置	3.2.1 能根据企业安全需求，配置客户端访问规则。 3.2.2 能根据企业安全需求，配置客户端数据安全规

工作领域	工作任务	职业技能要求
		则。 3.2.3 能根据企业安全需求，配置客户端应用保护策略。 3.2.4 能根据企业安全需求，配置客户端安全策略。
	3.3 信息安全管理	3.3.1 能根据国家相关规定，履行网络安全义务，安全管理企业互联网应用。 3.3.2 能根据国家相关规定，对企业互联网涉及的各类信息（如公民个人信息等）实施保护。 3.3. 能根据国家相关规定和企业信息安全需求，安全管理企业员工的网络行为。 3.3.4 能根据国家相关规定和企业信息安全需求，识别、处理违法有害信息。

表 2 企业网络安全防护（中级）

工作领域	工作任务	职业技能要求
1.系统安全配置	1.1 Windows 系统安全配置	1.1.1 能根据企业系统安全需求，合理配置、管理系统账户。 1.1.2 能根据企业系统安全需求，合理配置、管理文件访问权限。 1.1.3 能根据企业系统安全需求，合理配置、管理系统网络访问策略。 1.1.4 能根据企业系统安全需求，对系统进行安全审计、备份。 1.1.5 能根据企业系统安全需求，配置合适的安全策略。 1.1.6 能根据企业系统安全需求，对数据进行安全加密。
	1.2 Linux 系统安全配置	1.2.1 能根据企业需求，部署、配置 Linux 操作系统，安全管理 Linux 文件系统。 1.2.2 能根据企业系统安全需求，合理配置、管理 Linux 系统账户。 1.2.3 能根据企业系统安全需求，合理配置、管理 Linux 系统网络访问策略。 1.2.4 能根据企业系统安全需求，对系统进行安全审计、备份。 1.2.5 能根据企业系统安全需求，配置系统安全策略。
	1.3 数据库安全配置	1.3.1 能根据企业数据库安全需求，安全设置、管理数据库账户。 1.3.2 能根据企业数据库安全需求，优化数据库的安全设置。 1.3.3 能根据企业数据库备份需求，配置合适的备份

工作领域	工作任务	职业技能要求
		方式对数据库进行备份。 1.3.4 能根据数据库备份情况，对备份数据进行相应的恢复。
2.网络安全设备配置	2.1 WAF 安全配置	2.1.1 能根据企业网站安全需求，部署 WAF。 2.1.2 能根据企业网站安全需求，配置合适的 WAF 策略。 2.1.3 能根据企业网站安全需求，配置合适的 WAF 日志与告警规则。 2.1.4 能根据企业网站安全需求，动态监控 WAF 数据，设置合适的应用防护策略。
	2.2 入侵检测/防御安全配置	2.2.1 能根据企业网络安全需求，部署入侵检测/防御系统。 2.2.2 能根据企业网络安全需求，配置合适的入侵检测策略。 2.2.3 能根据企业网络安全需求，配置合适的入侵防御策略。 2.2.4 能根据企业网络安全需求，配置、管理入侵检测/防御系统日志报表。
	2.3 安全网络构建	2.3.1 能根据企业网络安全需求，部署虚拟专用网络(VPN)。 2.3.2 能根据企业网络安全需求，配置合适的虚拟专用网络(VPN)策略。 2.3.3 能根据企业网络安全需求，监测企业无线连接情况，配置无线设备的安全防护功能。 2.3.4 能根据企业网络安全需求，配置、优化无线设备的安全扩展功能。
3.应用安全配置	3.1 应用服务安全配置	3.1.1 能根据企业安全需求，配置、应用 Web 服务安全策略。 3.1.2 能根据企业安全需求，配置、应用文件服务安全策略。 3.1.3 能根据企业安全需求，配置、应用邮件服务安全策略。 3.1.4 能根据企业安全需求，配置、应用证书服务器。 3.1.5 能根据企业安全需求，对应用服务器进行监控，配置合适日志审计策略。
	3.2 信息安全管理	3.2.1 能根据国家相关规定，履行网络安全义务，安全管理企业互联网应用。 3.2.2 能根据国家相关规定，对企业互联网涉及的各类信息（如公民个人信息等）实施保护。 3.2.3 能根据国家相关规定和企业信息安全需求，安全管理企业员工的网络行为。 3.2.4 能根据国家相关规定和企业信息安全需求，识别、处理违法有害信息。

工作领域	工作任务	职业技能要求
		3.2.5 能根据国家相关规定，安全管理企业电子信息及应用软件，设置相应的安全策略。
	3.3 数据安全处理	3.3.1 能根据国家相关规定，对企业的各类数据实施保护。 3.3.2 能根据企业信息安全需求，配置、应用合适的数据加解密策略。 3.3.3 能根据企业信息安全需求，配置、应用合适的应用备份、恢复策略。 3.3.4 能根据企业信息安全需求，配置、应用合适的数据分级存储策略。 3.3.5 能根据企业信息安全需求，配置、应用合适的数据销毁策略。

表 3 企业网络安全防护（高级）

工作领域	工作任务	职业技能要求
1.系统安全诊断与加固	1.1 恶意代码防护	1.1.1 能借助工具监控系统进程、文件、网络传输等状态，识别系统中的可疑程序。 1.1.2 能借助工具分析可疑代码的行为。 1.1.3 能借助工具清理系统中的病毒、后门等恶意程序，并提出防范建议。 1.1.4 能根据企业防病毒需求，部署、配置、更新防病毒软件。
	1.2 漏洞扫描	1.2.1 能根据企业安全需求，选择合适的扫描工具，设置适当的扫描参数，完成对系统进行漏洞扫描。 1.2.2 能根据漏洞扫描结果，对不同级别的漏洞进行验证。 1.2.3 能根据企业安全需求和漏洞扫描结果，形成系统漏洞风险评估报告。 1.2.4 能根据系统漏洞风险评估报告，修复漏洞。
	1.3 系统加固	1.3.1 能根据企业业务情况，设计并实施合适的安全策略。 1.3.2 能根据企业业务情况，设计并实施安全的网络访问策略。 1.3.3 能根据企业业务情况，对系统进行安全审计，找到潜在安全风险，设计加固策略并实施。 1.3.4 能根据服务器安全需求，编写脚本进行自动化安全管理。
2.网络安全诊断与加固	2.1 高可用网络部署	2.1.1 能根据企业网络安全需求，分析网络中的重要链路，配置高可用性链路。 2.1.2 能根据企业网络安全需求，分析网络中的关键节点，配置双机热备。 2.1.3 能根据企业网络安全需求，分析网络流量负载

工作领域	工作任务	职业技能要求
		情况，配置负载均衡。 2.1.4 能完成高可用网络部署环境下的网络故障诊断。
	2.2 网络安全事件监控	2.2.1 能根据任务要求,识别网络系统中的关键节点,在合适的位置抓取数据包。 2.2.2 能根据任务要求,使用工具监控当前网络流量,识别异常流量。 2.2.3 能根据任务要求，分析异常流量数据，识别网络攻击源。 2.2.4 能根据任务要求，配置合适的安全策略，消除异常网络安全事件造成的威胁。
	2.3 网络安全传输	2.3.1 能根据企业网络安全需求，设计、配置虚拟专用网络(VPN)。 2.3.2 能根据企业网络安全需求，部署、配置堡垒机，对网络设备和人员权限进行分类管理。 2.3.3 能根据企业网络安全需求，部署、配置终端准入控制系统。 2.3.4 能根据企业网络安全需求，配置分布式网络与系统监视工具,监控整个网络与系统的安全运行状态。 2.3.5 能根据企业网络安全需求，配置流量过滤和流量分发策略。
3.应用安全诊断与加固	3.1Web安全事件分析与加固	3.1.1 能根据任务需求，分析企业网站访问流量，识别特定的恶意流量。 3.1.2 监测企业 Web 服务运行情况，识别网站中的恶意代码，作出合理处置。 3.1.3 能根据企业网络安全需求，应用合理的网页防篡改、防暗链、防钓鱼等安全措施。 3.1.4 对网站代码进行审计，分析其中可能存在的安全隐患，并提供解决建议。 3.1.5 分析企业网络和应用日志，对其中的攻击行为进行溯源。
	3.2 数据安全与恢复	3.2.1 能根据企业网络安全需求，配置、应用合理的数据传输安全策略。 3.2.2 能根据企业信息安全需求，配置、应用合适的应用备份、恢复策略。 3.2.3 能根据企业信息安全需求，配置、应用合适的数据分级存储策略。 3.2.4 能根据企业信息安全需求，配置、应用数据防泄漏产品。 3.2.5 能根据任务需求，对常见应用数据进行提取、修复。 3.2.6 能根据任务需求，对特定数据进行提取、恢复。
	3.3 应用安	3.3.1 能根据企业网络安全需求，对企业应用安全进

工作领域	工作任务	职业技能要求
	全漏洞扫描	行基线检查。 3.3.2 能根据企业网络安全需求，对企业应用进行合适的渗透测试。 3.3.3 能根据企业网络安全需求，对企业应用漏洞进行分析，提供合适的解决建议。 3.3.4 能根据企业网络安全需求，分析企业应用潜在风险，并进行安全加固。
4.网络安全保障体系建设	4.1 网络安全等级保护	4.1.1 能依据国家有关政策和标准完成定级备案工作。 4.1.2 能依据国家有关政策和标准，对网络及系统配置进行核查及整改加固。 4.1.3 能根据网络安全等级保护要求对数据库、应用系统配置进行核查及整改加固。 4.1.4 能推进等级测评工作开展，阅读、分析测评报告，根据测评结果进行整改加固。
	4.2 关键基础设施保护	4.2.1 能梳理及初步认定关键信息基础设施。 4.2.2 能制定内部安全管理制度和操作规程，加强权限管理、身份认证。 4.2.3 能根据相关政策、法律法规，制定网络安全事件应急预案，组织开展网络安全检查和应急演练，应对处置网络安全事件。 4.2.4 能对重要系统和数据库进行容灾备份，及时对系统漏洞等安全风险采取补救措施。
	4.3 互联网安全管理	4.3.1 能根据国家相关规定，履行网络安全义务，安全管理企业互联网应用。 4.3.2 能根据国家相关规定，对企业互联网涉及的各类信息（如公民个人信息等）实施保护。 4.3.3 能根据国家相关规定和企业信息安全需求，安全管理企业员工的网络行为。 4.3.4 能根据国家相关规定和企业信息安全需求，识别、处理违法有害信息。 4.3.5 能根据国家相关规定，安全管理企业电子信息及应用软件，设置相应的安全策略。 4.3.6 能根据国家相关规定，履行网络安全义务，监测企业互联网应用运行状态，安全管理企业互联网应用。

参考文献

[1] GB/T 1.1-2009 标准化工作导则

[2] 中等职业学校专业目录（含2019增补专业）

[3] 普通高等学校高等职业教育（专科）专业目录及专业简介

[4] 普通高等学校本科专业目录（2012年）

[5] 中等职业学校专业教学标准（试行）

[6] 高等职业学校专业教学标准（2018年）

[7] 普通高等学校本科专业类教学质量国家标准（2018年发布）

[8] 国家职业技能标准编制技术规程（2018年版）

[9] 中华人民共和国职业分类大典（2015年版）

[10] GB/T 25068.1　信息技术安全技术　IT网络安全

[11] GB/T 22239-2019信息安全技术　网络安全等级保护基本要求

[12] GB/T 25058-2019　信息安全技术　网络安全等级保护实施指南

[13] GB/T 25069-2010　信息安全技术　术语

[14] GB/T 25070信息安全技术　信息系统等级保护安全设计技术要求

[15] GB/T 20281-2015　信息安全技术　防火墙安全技术要求和测试评价方法

[16] GB/T 28454-2012　信息技术 安全技术 入侵检测系统的选择、部署和操作