# 企业网络安全防护
# 职业技能等级标准

# 目　次

# 前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准起草单位：上海海盾安全技术培训中心

本标准主要起草人：赵云霞、黄镇、江雪、樊亦胜、何晓霞、金波、宋好好、陆臻、赵瑞华、姜开达、吴鸣旦、苗春雨、杨木超。

起草人来自以下单位：上海海盾安全技术培训中心、公安部网络安全保卫局、公安部第三研究所、上海交通大学、安恒信息技术有限公司、北京天融信科技有限公司。

## 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　第1部分：网络安全管理

GB/T 25068.2　信息技术　安全技术　IT网络安全　第2部分：网络安全体系结构

GB/T 25068.3　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

GB/T 25068.4　信息技术　安全技术　IT网络安全　第4部分：远程接入的安全保护

GB/T 25068.5　信息技术　安全技术　IT网络安全　第5部分：使用虚拟专用网的跨网通信安全保护

GB/T 36635-2018　信息安全技术　网络安全监测基本要求与实施指南

GA/T 1390.2-2017　信息安全技术　网络安全等级保护基本要求　第2部分：云计算安全扩展要求

GA/T 1390.3-2017　信息安全技术　网络安全等级保护基本要求　第3部分：移动互联安全扩展要求

GB/T 29246-2017　信息技术　安全技术　信息安全管理体系　概述和词汇

GB/T 31496-2015　信息技术　安全技术　信息安全管理体系实施指南

GB/T 22080-2016　信息技术　安全技术　信息安全管理体系　要求

GB/T 20008　信息安全技术　操作系统安全评估准则

GB/T 22239　信息安全技术　信息系统安全等级保护基本要求

GB/T 22240　信息安全技术　信息系统安全等级保护定级指南

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

## 3 术语和定义

GB/T 29246-2017、GB/T 25068.1、GB/T 22080-2016、GA/T 1390.3-2017国家、行业标准界定的以及下列术语和定义适用于本标准。

### 3.1 信息安全 information security

对信息的保密性(3.2)完整性(3.3)和可用性(3.4)的保持。

### 3.2 保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的特性。

### 3.3 完整性 integrity

准确和完备的特性。

### 3.4 可用性 availability

根据授权实体的要求可访问和可使用的特性。

### 3.5 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。

3.6 攻击 attack

企图破坏、泄露、算改、损伤、窃取、未授权访问或未授权使用资产的行为。

3.7 鉴别 authentication

为一个实体声称的特征是正确的而提供的保障措施。

3.8 信息系统 information system

应用、服务、信息技术资产或其他信息处理组件。

3.9 网络管理 network management

对网络进行规划、设计、实施、运行、监视和维护的过程。

3.10 网络监视 network monitoring

连续观察和评审在网络活动和运行中所记录数据（包括审计日志和报警）的过程以及相关分析。

4 对应院校专业

中等职业学校：网络信息安全、网站建设与管理、计算机网络技术、计算机应用、软件与信息服务、移动应用技术与服务等相关专业。

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、移动应用开发、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、大数据技术与应用等相关专业。

应用型本科学校：信息安全、网络工程、计算机科学与技术、数据科学与大数据技术、软件工程等相关专业。

5 面向工作岗位

【企业网络安全防护】（初级）：主要面向全国重点联网企事业单位如银行、基础电信运营企业、互联网服务企业、网络安全服务企业、上网服务企业、

网络安全协会、党政机关，企业网络安全防护初级岗位。根据网络安全防护初级工作任务需求，能够进行网络设备安全配置，识别常见网络攻击，掌握常见操作系统安全加固、网络安全防护、应用安全分析与防御、数据安全分析与防御、数据备份等操作技能，开展初级企业网络安全防护工作。

【企业网络安全防护】（中级）：主要面向全国重点联网企事业单位如银行、基础电信运营企业、互联网服务企业、网络安全服务企业、上网服务企业、网络安全协会、党政机关，企业网络安全防护中级岗位。根据网络安全防护中级工作任务需求，能够熟练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，掌握企业网络、系统进行安全渗透测试、基线检查，入侵行为检测、流量监测、各类日志分析、应急处置、数据取证等操作技能。能够设计企业级数据容灾、应急响应方案，开展中级企业网络安全防护工作。

【企业网络安全防护】（高级）：主要面向全国重点联网企事业单位如银行、基础电信运营企业、互联网服务企业、网络安全服务企业、上网服务企业、网络安全协会、党政机关，企业网络安全防护高级岗位。根据网络安全防护高级工作任务需求，能够进行企业级网络安全架构、企业网络安全风险评估，能够做信息系统安全风险评估与处置、信息系统安全等级保护建设、企业网络安全分析与整体加固方案、规划和指导建设企业网络安全管理体系，并指导初级、中级网络安全人员共同完成企业网络安全体系建设，开展高级企业网络安全防护工作。

## 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 企业网络安全防护职业技能等级要求（初级）

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| 1.网络和通信安全管理 | 1.1 网络设备安全配置 | 1.1.1 能根据企业 LAN 需求，通过命令行界面/Web 界面，创建、删除、修改 VLAN<br>1.1.2 能根据企业 LAN 管理需求合理确定各 VLAN 模式，能使用相关协议自动管理 VLAN<br>1.1.3 能根据企业 IP 地址规划，配置路由器各接口 IP 地址，并启动接口<br>1.1.4 能根据企业网络通信需求，选择合适的动态路由协议，并通过命令行界面/Web 界面配置动态路由协议<br>1.1.5 能根据企业网络的访问控制需求，制定访问控制规则，并应用访问控制策略<br>1.1.6 能根据企业安全需求对交换机、路由器登录账号进行相应安全程度的安全认证<br>1.1.7 能根据企业网络管理需求远程管理交换机、路由器 |
| | 1.2 安全设备应用与分析 | 1.2.1 能根据企业网络区域间的访问控制需求，通过防火墙 Web 管理界面，熟练制定访问控制规则，使用防火墙进行访问控制<br>1.2.2 能通过防火墙 Web 管理界面，查看防火墙的日志，并分析出防火墙基本的运行状况<br>1.2.3 能根据企业扫描需求合理选择扫描产品，并熟练使用扫描产品进行扫描<br>1.2.4 能对扫描报告进行分析，准确判断出系统服务是否最小化、准确定位高风险漏洞等 |
| 2.设备和计算安全管理 | 2.1 Windows 系统安全加固与防护 | 2.1.1 能根据操作系统本地文件安全需求/数据传输安全需求，在 Windows 系统上熟练部署加密策略对数据进行保护<br>2.2.2 能根据服务器提供服务的情况，合理管理系统服务或端口<br>2.1.3 能根据企业对服务器的安全需求，配置相应的安全策略，利用安全策略保护 windows 服务器<br>2.1.4 能根据企业的共享需求，合理的划分共享的权限，并正确配置 Windows 共享 |

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| | | 2.1.5 能定期查阅系统日志，并通过系统日志了解系统的运行情况，若发现问题能及时的处理<br>2.1.6 能根据企业防病毒部署计划，对企业级防病毒软件进行配置、更新 |
| | 2.2 Linux 系统安全加固与防护 | 2.2.1 能通过相应的 Linux 命令查看进程信息，并能根据需求启动、结束进程<br>2.2.2 能通过相应的 Linux 命令查看服务信息，并能根据需求启动、停用、重启服务<br>2.2.3 能通过相应的 Linux 命令查看网络信息，了解网络连接情况，并根据需求对网络连接进行管理<br>2.2.4 能根据 Linux 服务器远程连接安全需求合理选择登录认证方式，并进行 SSH 登录配置、测试<br>2.2.5 能根据 Linux 服务器日志记录需求配置 syslog 日志<br>2.2.6 能通过相应的 Linux 命令查看系统日志，了解系统的运行情况，若发现问题能及时的处理<br>2.2.7 能根据 Linux 服务器的访问控制需求，配置 iptables 的 IUPUT 链策略，并进行测试 |
| 3.应用和数据安全管理 | 3.1 应用安全分析与防御 | 3.1.1 能找到可能存在弱口令的页面，并利用 burpsuite 等工具尝试对弱口令进行脆弱性测试<br>3.1.2 能找到可能存在 SQL 注入漏洞的页面，并手工对网站进行 SQL 注入验证测试<br>3.1.3 能找到可能存在跨站漏洞的页面，并输入相应的测试代码尝试对网站进行跨站验证测试<br>3.1.4 能找到可能存在上传漏洞的页面，若存在上传漏洞，能通过上传相应的 WebShell 进行验证<br>3.1.5 能根据企业网站服务器对各自 Web 应用漏洞的防护需求进行 WAF 的配置，并测试防护效果 |
| | 3.2 数据安全分析与处理 | 3.2.1 能根据企业数据库管理需求，创建相应的数据库账户，并分配合理的权限<br>3.2.2 能根据企业数据库安全需求，使用常见数据库的一些安全函数<br>3.2.3 能根据企业数据库安全需求，设置 |

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| | | 常见数据库的一些安全配置<br>3.2.4 能根据数据库备份方式对备份数据进行相应的恢复 |
| | 3.3 移动安全分析与处理 | 3.3.1 能根据不同的屏幕解锁方式，选择对应的锁屏密码存储文件<br>3.3.2 能通过相应的工具，下载手机中的指定文件至电脑中<br>3.3.3 能破解/删除 Android PIN 码（设备已 root）<br>3.3.4 能破解/删除 Android 屏幕图形锁（设备已 root）<br>3.3.5 能使用相应的工具对 Android APP 签名进行验证<br>3.3.6 能使用相应的工具对 Android APP 进行反编译<br>3.3.7 能通过分析反编译后的代码发现 Android APP 中可能存在的一些常见安全问题 |

**表 2 企业网络安全防护职业技能等级要求（中级）**

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| 1.安全组网技术应用 | 1.1 网络安全准入与审计分析 | 1.1.1 能根据企业组网需求，制定新设备接入方案，并实现安全接入<br>1.1.2 能根据企业内复杂的访问控制需求，规划访问控制策略，并在路由器上进行实施 |
| | 1.2 网络流量分析及安全优化 | 1.2.1 能根据企业相关业务需求，合理优化网络传输<br>1.2.2 能使用流量分析工具对流量进行分析，若有异常流量能发现并能进行处理 |
| | 1.3 企业级虚拟专用网络设计 | 1.3.1 能根据企业网络安全传输需求，设计基于预约共享密钥方式的虚拟专用网络方案，并进行实施、调试<br>1.3.2 能根据企业网络安全传输需求，设计 MPLS VPN，并进行实施、调试 |
| | 1.4 负载均衡与双机热备方案设计 | 1.4.1 能根据企业网络正常通信需求，设计网络负载均衡方案，并进行实施、调试<br>1.4.2 能根据企业网络正常通行需求，选择合适的双机热备方案，并进行实施、调试 |
| 2.操作系统安全管理 | 2.1 Windows 操作系统行为管理 | 2.1.1 能根据企业内部组织规划，设计活动目录，并进行架构实现、安全管理 |

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| | | 2.1.2 能根据企业内部组织间安全需求，设计组策略，并进行部署<br>2.1.3 能根据企业主机保护要求，设计主机隔离方案，并进行部署<br>2.1.4 能根据企业规章要求，对行为日志进行分析<br>2.1.5 能根据企业灾备要求，实现灾备，并在需要时进行迁移 |
| | 2.2 Unix/Linux 安全管理 | 2.2.1 能根据企业对 Linux 服务器的相关安全要求，编写 Shell 脚本，使用脚本安全管理<br>2.2.2 能根据企业对 Linux 服务器的相关要求，通过作业调度实现系统管理任务自动化<br>2.2.3 能根据企业对 Linux 服务器的相关安全要求，管理和分析系统日志<br>2.2.4 能根据企业对 Linux 服务器的数据加密要求，设计企业级加密方案实现数据加密<br>2.2.5 能分析 Linux 服务器中出现的一些复杂安全问题，并进行解决<br>2.2.6 能根据企业对 Linux 服务器的相关安全级别，通过账户管理、服务管理、配置安全策略、iptables 策略等实现主机安全级别 |
| 3.应用服务安全管理 | 3.1 企业级上网行为管理 | 3.1.1 能根据企业各部门业务情况，分析网络使用需求，并定制相应的上网行为管理方案<br>3.1.2 能根据制定的上网行为管理方案，部署行为管理策略<br>3.1.3 能根据制定的上网行为管理方案，实施访问控制和权限<br>3.1.4 能根据制定的上网行为管理方案，针对代理服务器实现安全加固<br>3.1.5 能根据制定的上网行为管理方案，对行为日志进行分析 |
| | 3.2 安全管理文件共享 | 3.2.1 能根据企业文件共享需求，选择合适的共享方式，并制定详细的共享策略<br>3.2.2 能根据制定的共享策略，实现安全共享 |
| | 3.3 企业级邮件服务安全管理 | 3.3.1 能根据企业邮件的归档需求，设计并实现邮件归档方案<br>3.3.2 能根据企业邮件的规模及企业邮件 |

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| | | 服务器的性能，实现邮件服务器性能优化<br>3.3.3 能根据企业及用户的垃圾邮件处理需求，设计反垃圾邮件策略，并进行实施 |
| | 3.4 基于 PKI 认证体系的安全性建设 | 3.4.1 能根据企业证书需求，选择合适的 PKI 软件，并实现 PKI 的基础架构<br>3.4.2 能在 PKI 平台上进行证书的签发、撤销等 |
| 4.网络防御 | 4.1 脚本分析与应用 | 4.1.1 能借助相关工具，分析常见类型的恶意脚本<br>4.1.2 能针对日常管理中的各类安全任务编写脚本 |
| | 4.2 防御基于网站的入侵 | 4.2.1 能在理解相关攻击的原理基础上对典型应用注入攻击进行有针对性的防御<br>4.2.2 能在理解相关攻击的原理基础上对典型劫持攻击与钓鱼攻击进行有针对性的防御<br>4.2.3 能在理解相关攻击的原理基础上对典型跨站脚本攻击进行有针对性的防御<br>4.2.4 能配合使用相关工具识别网站配置漏洞及应用程序逻辑缺陷<br>4.2.5 能在理解相关攻击的原理基础上对共享主机间的攻击进行有针对性的防御<br>4.2.6 能在理解相关问题的原理基础上预防网站信息泄露 |
| | 4.3 网站安全风险评估 | 4.3.1 能通过对网站的访问，分析网站应用程序的功能，并确定安全边界<br>4.3.2 能使用多种手段，分析、查找应用程序中潜在的缺陷与漏洞<br>4.3.3 能评估应用程序中缺陷与漏洞的潜在风险并提出加固措施<br>4.3.4 能使用自动化工具全面评估网站风险 |
| | 4.4 防御基于 Linux 的入侵 | 4.4.1 能通过使用相关工具识别、应对防御典型数据驱动攻击<br>4.4.2 能通过分析网络连接情况等发现常见远程攻击并采取对应防范措施<br>4.4.3 能采取措施预防各类本地提权攻击<br>4.4.4 能借助相关工具识别、分析典型内核 rootkit，并对系统进行修复<br>4.4.5 能采取适当措施保全系统入侵证据 |
| 5.病毒分析与防御 | 5.1 常见病毒分析与防御技术 | 5.1.2 能借助相关工具分析当前流行病毒的工作机理 |

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| | | 5.1.3 能分析当前流行病毒（木马），并根据其传播机制、感染情况等提供防病毒解决方案<br>5.1.4 能分析网络病毒，并根据其传播机制、感染情况等提供解决方案 |
| | 5.2 rootkit 病毒分析与查杀 | 5.2.1 能借助相关工具分析利用计算机驱动技术的病毒<br>5.2.2 能借助相关工具分析 Rootkit 病毒，并对病毒进行处理 |
| 6.安全技术体系架构 | 6.1 典型应用环境安全解决方案的分析与设计 | 6.1.1 能根据中小型企业网络区域划分情况、边界防护要求、服务器防护要求、数据容灾需求等提供整体安全解决方案<br>6.1.2 能根据大型企业网络业务连续性需求、区域划分情况、边界防护要求、服务器防护要求、数据容灾需求等提供整体安全解决方案<br>6.1.3 能根据带有数据中心的网络业务连续性需求、区域划分情况、边界防护要求、服务器防护要求、服务器负载均衡要求、数据容灾、数据备份需求等提供整体安全解决方案<br>6.1.4 能根据多种接入访问的网络接入点安全需求、区域划分情况、边界防护要求、服务器防护要求等提供整体安全解决方案 |
| 7.应急响应 | 7.1 数字取证 | 7.1.1 能熟练掌握 WINHEX 的基本应用<br>7.1.2 能使用 WINHEX 对常见存储介质进行证据固定<br>7.1.3 能借助相关工具对攻击系统行为进行分析<br>7.1.4 能借助相关工具对恶意代码行为进行分析 |
| | 7.2 数据容灾 | 7.2.1 能根据企业数据容灾需求设计企业级灾备方案，并进行实施、调试<br>7.2.2 能根据企业数据备份需求组建基于存储局域网的备份架构 |

**表 3 企业网络安全防护职业技能等级要求（高级）**

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| 1.网络安全综合技能 | 1.1 网络渗透与防御 | 1.1.1 能借助相关工具，对企业网络环境中的各类设备、服务与系统进行渗透测试<br>1.1.2 能针对渗透测试过程中暴露出的漏洞进行修补和系统加固 |

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| | | 1.1.3 能借助相关工具，在系统中搜寻入侵痕迹，还原入侵过程，分析并得出解决方案 |
| | 1.2 恶意代码分析 | 1.2.1 能借助相应的恶意代码分析工具，分析常见类型的恶意代码<br>1.2.2 能借助相应的病毒分析工具分析当前流行病毒的工作机制<br>1.2.3 能借助相应的分析工具，分析网络病毒的传播机制、感染机制等，并提供解决方案<br>1.2.4 能借助相应的分析工具，分析利用驱动技术的病毒<br>1.2.5 能借助相应的分析工具分析 Rootkit 病毒，并进行处理 |
| | 1.3 网站安全风险评估 | 1.3.1 能通过浏览网站，分析网站应用程序的功能，确定安全边界及可能的安全风险点<br>1.3.2 能使用相关方法全面评估网站风险，进行威胁建模，查找潜在的缺陷（包括人工分析及使用自动化工具）<br>1.3.3 能评估潜缺陷可能带来的风险并提出加固措施 |
| 2.企业网络安全规划与建设 | 2.1 企业网络安全管理体系规划、建设、运行 | 2.1.1 熟悉网络安全管理体系，并能在实际工作中熟练运用信息安全管理方法<br>2.1.2 能根据企业网络安全管理需求，进行网络安全管理体系的规划<br>2.1.3 掌握网络安全管理体系的基本流程<br>2.1.4 能根据企业及企业网络实际情况定制网络安全相关制度和规范 |
| | 2.2 信息系统安全风险评估与处置 | 2.2.1 能在实际工作中合理运用信息安全风险评估方法<br>2.2.2 能采用相应方法对企业信息系统实施信息安全风险评估<br>2.2.3 能根据企业业务目标调整信息安全风险计算方法<br>2.2.4 能根据企业信息系统安全需求、信息系统安全风险评估结果，制定信息系统整体安全策略<br>2.2.5 熟悉灾难恢复的技术、工具和流程 |
| | 2.3 信息系统安全等级保护建设 | 2.3.1 能根据国家网络安全等级保护定级标准为信息系统合理定级<br>2.3.2 能根据相应的等级保护标准，组织实施信息系统安全建设 |

| 工作领域 | 工作任务 | 职业技能要求 |
| --- | --- | --- |
| | | 2.3.3 能根据信息系统的定级，指导等级保护整改工作 |
| | 2.4 企业网络安全分析与整体加固 | 2.4.1 能针对不同规模的企业，分析其物理安全问题，并提供解决方案。<br>2.4.2 能针对不同规模的企业，分析其网络结构安全问题，提供解决方案，并实施加固。<br>2.4.3 能针对不同规模的企业，分析其系统安全问题，提供解决方案，并实施加固。<br>2.4.4 能针对不同规模的企业，分析其应用安全问题，提供解决方案，并实施加固。 |
| 3.企业网络安全培训 | 3.1 网络安全意识和技能宣贯 | 3.1.1 能向决策层和管理层介绍网络安全理念，推进网络安全实施<br>3.1.2 能推进网络安全及其相关技术人员的网络安全技术培训，制定培训规划并提供网络安全培训<br>3.1.3 能向普通用户或信息受众普及网络安全知识，提高其网络安全意识 |
| | 3.2 指导工作 | 3.2.1 能对中级及初级企业网络安全防护岗位人员进行技术培训<br>3.2.2 能撰写企业网络安全防护相关论文或指导性技术文件 |

## 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 第1部分：网络安全管理

[11] GB/T 25068.2 信息技术 安全技术 IT网络安全 第2部分：网络安全体系结构

[12] GB/T 25068.3 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

[13] GB/T 25068.4 信息技术 安全技术 IT网络安全 第4部分：远程接入的安全保护

[14] GB/T 25068.5 信息技术 安全技术 IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护

[15] GB/T 36635-2018 信息安全技术 网络安全监测基本要求与实施指南

[16] GA/T 1390.2-2017　信息安全技术　网络安全等级保护基本要求 第2部分：云计算安全扩展要求

[17] GA/T 1390.3-2017　信息安全技术　网络安全等级保护基本要求 第3部分：移动互联安全扩展要求

[18] GB/T 29246-2017　信息技术　安全技术　信息安全管理体系　概述和词汇

[19] GB/T 31496-2015　信息技术　安全技术　信息安全管理体系实施指南

[20] GB/T 22080-2016　信息技术　安全技术　信息安全管理体系　要求

[21] GB/T 20008　信息安全技术　操作系统安全评估准则

[22] GB/T 22239　信息安全技术　信息系统安全等级保护基本要求

[23] GB/T 22240　信息安全技术　信息系统安全等级保护定级指南

[24] 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