江苏省交通运输厅

网络安全技术指导手册

江苏省交通运输厅

2021 年 12 月

目 录

前言

目前，国内外网络安全形势日益严峻，我国各重要行业网络系统面临的网络攻击、破坏、窃密等安全威胁层出不穷，时刻威胁着我国的国家安全、社会秩序与公民利益。2014 年 2 月中共中央成立了以习近平总书记为组长的中央网络安全和信息化领导小组，明确指出“没有网络安全就没有国家安全，没有信息化就没有现代化”。

网络安全工作要求高，任务重，做好网络安全工作不仅是业务问题，还是政治问题、大局问题。为了普及网络安全技术知识，确保我省交通运输行业信息化建设的安全与稳定，健全江苏交通运输行业网络安全保障体系，厅科技处会同信息中心查阅梳理了大量资料，并结合我厅网络安全管理实际，编制了《江苏省交通运输厅网络安全技术指导手册》，重点介绍了网络安全相关的法律法规、网络安全技术要求、主要网络安全设备以及常见安全漏洞预防及处置等方面的内容，供大家在网络安全工作中参考。

本指导手册涉及内容多，整理和编写过程中难免有疏漏，如发现有瑕疵，敬请谅解，并及时反馈，以便进一步修改完善。

第一部分：网络安全法律法规及管理办法

本手册主要依据《中华人民共和国网络安全法》《交通运输部网络安全管理办法》《江苏省政务信息化项目建设网络安全管理规定》等有关规定，在网络安全的管理和建设中要遵循“积极利用、依法管理、科学发展、确保安全”的方针，根据“同步规划、同步建设、同步使用”的要求，坚持“谁主管谁负责，谁建设谁负责，谁运行谁负责”和“属地管理”的原则，实行分级管理和分工负责。

1、 《中华人民共和国网络安全法》

《中华人民共和国网络安全法》是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定的法律。

《中华人民共和国网络安全法》由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过，自 2017 年 6 月 1 日起施行

2、 《中华人民共和国数据安全法》

《中华人民共和国数据安全法》是为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定的法律。[8]

2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》，自 2021 年 9 月 1 日起施行。

3、 《中华人民共和国个人信息保护法》

《中华人民共和国个人信息保护法》是一部保护个人信息的法律条款，涉及法律名称的确立、立法模式问题、立法的意义和重要性、立法现状以及立法依据、法律的适用范围、法律的适用例外及其规定方式、个人信息处理的基本原则、与政府信息公开条例的关系、对政府机关与其他个人信息处理者的不同规制方式及其效果、协调个人信息保护与促进信息自由流动的关系、个人信息保护法在特定行业的适用问题、关于敏感个人信息问题、法律的执行机构、行业自律机制、信息主体权利、跨境信息交流问题、刑事责任问题。对个人及行业有着很大的作用。

2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》。自 2021 年 11 月 1 日起施行。

4、 《信息安全技术网络安全等级保护基本要求》

为了配合《中华人民共和国网络安全法》的实施，同时适应云计算、移动互联、物联网、工业控制和大数据等新技术、新应用情况下网络安全等级保护工作的开展，2019 年《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）正式实施。等保 2.0 针对共性安全保护需求提出安全通用要求，针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用领域的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护基本要求标准。

新标准将云计算、移动互联、物联网、工业控制系统等列入标准范围，构成了“安全通用要求+新型应用安全扩展要求”的要求内容。

同时，新标准“基本要求、设计要求和测评要求”分类框架统一，形成了“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心” 支持下的三重防护体系架构。

5、 《关键信息基础设施安全保护条例》

为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。

2021 年 4 月 27 日，经国务院第 133 次常务会议通过，自 2021 年 9 月 1 日起施行。

6、 《交通运输部网络安全管理办法》

为加强交通运输网络安全管理，落实网络安全工作责任，健全网络安全保障体系，依据《中华人民共和国网络安全法》、国家网络安全政策制度和标准规范，以及党委（党组）落实网络安全工作责任制的有关规定，制定本办法。

交通运输网络安全工作遵循“积极利用、依法管理、 科学发展、

确保安全”方针，根据“同步规划、同步建设、同步使用”要求，坚持“谁主管谁负责，谁建设谁负责，谁运行谁负责”和“属地管理”原则，实行分级管理和分工负责。

交通运输网络安全工作以关键信息基础设施保护为核心，以数据资源保护为基础，以健全政策制度体系、加强技术能力建设为重点，围绕网络全生命周期、全要素覆盖，提升网络安全监管和防护水平。

本办法自 2021 年 1 月 1 日起施行。

7、 《江苏省政务信息化项目建设网络安全管理规定》

本规定适用省级财政投资建设的政务信息化项目，含新建、改建、扩建和在用的政务信息化项目。省政务信息化项目按照“谁主管谁负责、谁运营谁负责”的原则落实网络安全工作责任.保证安全技术措施同步规划、同步建设、同步使用。

省委网信办加强统筹协调.会同省发展改革委、财政厅、政务办、工业和信息化厅、公安厅、密码管理局等部门建立省政务信息化项目建设网络安全管理工作机制，按照职责分工，强化对省政务信息化项目的网络安全监管，组织开展督促检查和评估评价。

8、 《江苏省交通运输厅网络安全管理办法》

为加强厅网络安全管理，进一步压实网络安全工作责任，健全网络安全保障体系，厅科技处会同信息中心编制了《江苏省交通运输厅网络安全管理办法》，重点针对我厅网络安全职责分工、建设管理、运行安全、数据安全、监测预警及应急处置等方面进行了细化明确，同时还对监督检查与责任追究、保障措施提出了相关要求。

本办法适用于省交通运输厅及厅属单位在规划、建设、运行、使用及监管网络等过程中，为保障网络系统稳定可靠运行和数据的完整性、保密性、可用性所执行的各项工作。

第二部分：网络安全防护要求

依据信息安全技术网络安全等级保护基本要求，针对基础信息网络、信息系统、云计算平台/系统、大数据平台/系统、物联网、工业控制系统等，面临的威胁有所不同，安全保护要求也有所差异。为此安全防护要求分为安全通用要求和安全拓展要求。

1、安全通用要求

1.1 机房物理环境要求

1.1.1 物理访问控制

本项要求包括：

（a）机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

（b）重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入人员。

1.1.2 物理位置选择

本项要求包括：

（a）机房场地应选择在具有防震、防风和防雨等能力的构建内。

（b）机方场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

1.1.3 防盗窃和防破坏

本项要求包括：

（a）应将设备或主要部件进行固定，并设置明显的不易除去的标识。

（b）应将通信线缆设在隐藏安全处。

（c）应设置机方防盗报警系统或者设置专人值守的视频监控系统。

1.1.4 防雷击

本项要求包括：

（a）应将各类机柜、设施和设备等通过接地系统安全接地。

（b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

1.1.5 防火

本项要求包括：

（a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警、并自动灭火。

（b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

（c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

1.1.6 防水和防潮

本项要求包括：

（a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

（b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透.

（c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

1.1.7 温湿度控制

应设置必要的温湿度调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

1.1.8 电力供应

本项要求包括：

（a）应在机房供电线路上配置稳压器和过电压防护设备。

（b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

（b）应设置冗余或并行的电力电缆线路为计算机系统供电；

（d）应提供应急供电设施。

1.1.9 防静电

本项要求包括：

（a）应采用防静电地板或地面并采用必要的接地防静电措施。

（b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

1.1.10 电磁防护

本项要求包括：

（a）电源线和通信线缆应隔离铺设，避免互相干扰。

（b）应对关键设备或关键区域实施电磁屏蔽。

实现方式：配备屏蔽机柜或屏蔽机房，同时建议部署动环系统。

1.2 网络通信环境要求

1.2.1 网络架构

本项要求包括：

（a）应保证网络设备的业务处理能力满足业务高峰期需要；

（b）应保证网络各个部分的带宽满足业务高峰期需要；

（c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

（d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术 隔离手段；

（e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性；

（f）应按照业务服务的重要程度分配带宽，优先保障重要业务。

1.2.2 通信传输

本项要求包括：

（a）应采用密码技术保证通信过程中数据的完整性；

（b）应采用密码技术保证通信过程中数据的保密性；

（c）应在通信前基于密码技术对通信的双方进行验证或认证；

（d）应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。

1.2.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

实现方式：科学合理划分网络区域，并采用可信根芯片或硬件。

1.3 安全区域边界要求

1.3.1 边界防护

本项要求包括：

(a)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

(b)应能够对非授权设备私自联到内部网络的行为进行检查或限制。

(c)应能够对内部用户非授权联到外部网络的行为进行检查或限制。

(d)应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

(e)应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断。

(f)应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。

1.3.2 访问控制

本项要求包括:

(a)应在网络边界或区域之间根据访问控制策略设置控制规则，默认情况下除允许通信外受控接口拒绝所有通信。

(b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

(c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，已允许/拒绝数据包进出。

(d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

(e)应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。

1.3.3 入侵防范

本项要求包括：

(a)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。

(b)应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

(c)应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

(d)当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

1.3.4 恶意代码和垃圾邮件防范

本项要求包括：

(a)应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

(b)应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

1.3.5 安全审计

本项要求包括：

(a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

(b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

(c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

1.3.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

实现方式：在边界区域配置必要的安全设备。

1.4 主机服务器环境要求

1.4.1 身份鉴别

本项要求包括：

(a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

(b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

(c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

(d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

1.4.2 访问控制

本项要求包括：

(a) 应对登录的用户分配账户和权限。

(b)应重命名或删除默认账户，修改默认账户的默认口令。

(c)应及时删除或停用多余的、过期的账户，避免共享账户的存在。

(d)应授予管理用户所需的最小权限，实现管理用户的权限分离。

(e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

(f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。

(g)应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访间。

1.4.3 安全审计

本项要求包括：

(a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

(b)审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等。

(c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

(d)应对审计进程进行保护，防止未经授权的中断。

1.4.4 入侵防范

本项要求包括：

(a)应遵循最小安装的原则，最低权限的原则，仅安装需要的组件和

应用程序。

(b)应关闭不需要的系统服务、默认共享和高危端口。

(c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

(d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

(e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

(f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

1.4.5 恶意代码防范

应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

1.4.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

实现方式：对设备定期巡检，及时更新策略。

1.5 数据安全要求

1.5.1 数据完整性

本项要求包括：

(a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

(b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

1.5.2 数据保密性

本项要求包括：

(a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

(b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

1.5.3 数据备份恢复

本项要求包括：

(a) 应提供重要数据的本地数据备份与恢复功能，本地数据备份文件应采用与生产系统非同一物理环境的存储方式，并检查其有效性；

(b) 应提供异地实时备份功能，要将重要数据实时备份至备份场地；

(c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。

实现方式：定期检查数据备份情况，采用可靠容灾方式。

1.6 系统及安全设备管理要求

1.6.1 系统管理

本项要求包括：

(a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

(b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

1.6.2 审计管理

本项要求包括：

(a)应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。

(b)应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

1.6.3 安全管理

本项要求包括：

(a)应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。

(b)应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

1.6.4 集中管控

本项要求包括：

(a)应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

(b)应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

(c)应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

(d)应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

(e)应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

(f)应能对网络中发生的各类安全事件进行识别、报警和分析；

(g)应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。

实现方式：配置安全管理中心 SOC。

1.7 安全管理制度要求

1.7.1 安全策略

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

1.7.2 管理制度

本项要求包括：

(a)应对安全管理活动中的各类管理内容建立安全管理制度；

(b)应对管理人员或操作人员执行的日常管理操作建立操作规程；

(c)应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

1.7.3 制定和发布

本项要求包括：

(a)应指定或授权专门的部门或人员负责安全管理制度的制定；

(b)安全管理制度应通过正式、有效的方式发布，并进行版本控制。

1.7.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

实现方式：对安全管理制度做好核查记录。

1.8 安全管理机构要求

1.8.1 岗位设置

本项要求包括：

(a)应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；

(b)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

(c)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

1.8.2 人员配备

本项要求包括：

(a)应配备一定数拔的系统管理员、审计管理员和安全管理员等；

(b)应配备专职安全管理员，不可兼任；

(c)关键事务岗位应配备多人共同管理。

1.8.3 授权和审批

本项要求包括：

(a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

(b)应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

(c)应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

1.8.4 沟通和合作

本项要求包括：

(a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；

(b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

(c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

1.8.5 审核和检查

本项要求包括：

(a)应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

(b)应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

(c)应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

实现方式：做好安全检查表格，安全检查记录，安全检查报告等台账。

1.9 安全管理人员

1.9.1 人员录用

录用本项要求包括：

(a)应指定或授权专门的部门或人员负责人员录用；

(b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；

(c)应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；

(d)应从内部人员中选拔从事关键岗位的人员。

1.9.2 人员离岗

本项要求包括：

(a)应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

(b)应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

1.9.3 安全意识教育和培训

本项要求包括：

(a)应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

(b)应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；

(c)应定期对不同岗位的人员进行技术技能考核。

1.9.4 外部人员访问管理

本项要求包括：

(a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

(b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限， 并登记备案；

(c)外部人员离场后应及时清除其所有的访问权限；

(d)获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；

(e)对关键区域或关键系统不允许外部人员访问。

实现方式：外部人员签字的保密协议，明确其保密义务。

1.10 安全建设管理要求

1.10.1 定级和备案

本项要求包括：

(a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

(b)应组织相关部门和有关安全技术专家对定级的结果的合理性和正确性进行论证和审定；

(c)应保证定级结果经过相关部门的批准；

(d)应将备案材料报主管部门和相应公安机关备案。

1.10.2 安全方案设计

本项要求包括：

(a)应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

(b)应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；

(c)应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施；

1.10.3 产品采购和使用

本项要求包括：

(a)应确保网络安全产品采购和使用符合国家的有关规定；

(b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；

(c)应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

(d)应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

1.10.4 等级测评

本项要求包括：

(a)应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；

(b)应在发生重大变更或级别发生变化时进行等级测评；

(c)应确保测评机构的选择符合国家有关规定。

实现方式：按要求对系统进行等级保护测试。

1.11 软件开发安全要求

1.11.1 自行软件开发

本项要求包括：

(a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

(b)应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

(c)应制定代码编写安全规范，要求开发人员参照规范编写代码；

(d)应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

(e)应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；

(f)应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

(g)应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

1.11.2 外包软件开发

本项要求包括：

(a)应在软件交付前检测其中可能存在的恶意代码；

(b)应保证开发单位提供软件设计文档和使用指南；

(c)应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

1.11.3 工程实施

本项要求包括：

(a)应指定或授权专门的部门或人员负责工程实施过程的管理；

(b)应制定安全工程实施方案控制工程实施过程；

(c)应通过第三方工程监理控制项目的实施过程。

1.11.4 测试验收

本项要求包括：

(a)应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

(b)应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

1.11.5 系统交付

本项要求包括：

(a)应制定交付清单，并根据交付清单对所交接的设备、软件和文档

等进行清点；

(b)应对负责运行维护的技术人员进行相应的技能培训；

(c)应提供建设过程文档和运行维护文档。

实现方式：编制交付清单、技术培训相关文档、指导维护的文档。

1.12 安全运维管理要求

1.12.1 环境管理

本项要求包括：

(a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿　度控制、消防等设施进行维护管理；

(b)应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理做出规定；

(c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸质文件和移动介质等；

(d)应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等。

1.12.2 资产管理

本项要求包括：

(a)应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容，并进行动态管理；

(b)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

(c)应对信息分类与标识方法做出规定，并对信息的使用、传输和存

储等进行规范化管理。

1.12.3 介质管理

本项要求包括：

(a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

(b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

1.12.4 设备维护管理

本项要求包括：

(a)应对各种设备（包括备份和冗余设备）、线路等制定专门的部门或人员定期进行维护管理；

(b)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

(c)信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；

(d)含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

1.12.5 漏洞和风险管理

本项要求包括：

(a)应采取必要的措施识别安全漏洞和隐患，对发现的漏洞和隐患及时进行修补或评估可能的影响后进行修补；

(b)应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

1.12.6 网络和系统安全管理

本项要求包括：

(a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

(b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

(c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定；

(d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

(e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

(f)应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；

(g)应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

(h)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏

感数据；

(i)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

(j)应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

1.12.7 恶意代码防范管理

本项要求包括：

(a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；

(b)应定期验证防范恶意代码攻击的技术措施的有效性。

1.12.8 配置管理

本项要求包括：

(a)应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

(b)应将基本配置信息改变纳入系统变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

1.12.9 密码管理

本项要求包括：

(a)应遵循密码相关的国家标准和行业标准；

(b)应使用国家密码管理主管部门认证核准的密码技术和产品；

(c)应采用硬件密码模块实现密码运算和密钥管理。

1.12.10 变更管理

本项要求包括：

(a)应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

(b)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

(c)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

1.12.11 备份与恢复管理

本项要求包括：

(a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；

(b)应规定备份信息的备份方式、备份频度、存储介质、保存期等；

(c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和回复程序等。

1.12.12 安全事件处置

本项要求包括：

(a)应及时向安全管理部门报告所发现的安全弱点和可疑事件 ；

(b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

(c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原

因，收集证据，记录处理过程，总结经验教训；

(d)对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序；

(e)应建立联合防护和应急机制，负责处置跨单位安全事件。

1.12.13 应急预案管理

本项要求包括：

(a)应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

(b)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

(c)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

(d)应定期对原有的应急预案重新评估，修订完善；

(e)应建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练。

1.12.14 外包运维管理

本项要求包括：

(a)应确保外包运维服务商的选择符合国家的有关规定；

(b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

(c)应保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明

确；

(d)应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

实现方式：编制相关运维管理制度，并在外包运维服务协议中对责任进行明确。

2、云计算安全扩展要求

2.1 安全物理位置

2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

2.2 安全通信网络

2.2.1 网络架构

本项要求包括：

(a)应保证云计算平台不承载高于其安全保护等级的业务应用系统；

(b)应实现不同云服务客户虚拟网络之间的隔离；

(c)应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；

(d)应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；

(e)应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务；

(f)应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服

务客户可以依据安全标记和　　强制访问控制规则确定主体对客体的访问；

(g)应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求　　自主选择边界数据交换方式；

(h)应为第四级业务应用系统划分独立的资源池。

2.3 安全区域边界

2.3.1 访问控制

本项要求包括：

(a)应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

(b)应在不同等级的网络区域边界部署访间控制机制，设置访问控制规则。

2.3.2 入侵防范

本项要求包括：

(a)应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

(b)应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

(c)应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；

(d)应在检测到网络攻击行为、异常流量情况时进行告警。

2.3.3 安全审计

本项要求包括：

(a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审

计，至少包括虚拟机删除、虚拟机重启；

(b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

2.4 安全计算环境

2.4.1 身份鉴别

当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

2.4.2 访问控制

本项要求包括：

(a)应保证当虚拟机迁移时，访问控制策略随其迁移；

(b)应允许云服务客户设置不同虚拟机之间的访问控制策略。

2.4.3 入侵防范

本项要求包括：

(a)应能检测虚拟机之间的资源隔离失效，并进行告警；

(b)应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；

(c)应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

2.4.4 镜像和快照保护

本项要求包括：

(a)应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；

(b)应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

(c)应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。

2.4.5 数据完整性和保密性

本项要求包括：

(a)应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

(b)应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；

(c)应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受　到破坏时采取必要的恢复措施；

(d)应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。

2.4.6 数据备份恢复

本项要求包括：

(a)云服务客户应在本地保存其业务数据的备份；

(b)应提供查询云服务客户数据及备份存储位置的能力；

(c)云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；

(d)应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

2.4.7 剩余信息保护

本项要求包括：

(a)应保证虚拟机所使用的内存和存储空间回收时得到完全清除；

(b)云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

2.5 安全管理中心

2.5.1 集中管控

本项要求包括：

(a)应能对物理资源和虚拟资源按照策略做统一管理调度与分配；

(b)应保证云计算平台管理流蜇与云服务客户业务流量分离；

(c)应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；

(d)应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

2.6 安全建设管理

2.6.1 云服务商选择

本项要求包括：

(a)应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应 等级的安全保护能力；

(b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

(c)应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

(d)应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；

(e)应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。

2.6.2 供应链管理

本项要求包括：

(a)应确保供应商的选择符合国家有关规定；

(b)应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；

(c)应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

2.7 安全运维管理

2.7.1 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

实现方式：基于安全域部署相应的防护措施，实现纵深防御，通过构建安全监测、识别、防护、审计和响应的综合安全能力，保障云计算资源和服务的安全，满足云计算平台的安全保障要求。

3、物联网安全扩展要求

3.1 安全物理环境

3.1.1 感知节点设备物理防护

本项要求包括

(a)感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；

(b)感知节点设备在工作状态所处物理环境应能正确反映环境状态

（如温湿度传感器不能安装在阳光直射区域）。

(c)感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；

(d)关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）。

3.2 安全区域边界

3.2.1 接入控制

应保证只有授权的感知节点可以接入，对感知节点数据传输时进行数据通讯认证。

3.2.2 入侵防范

本项要求包括：

(a)应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；

(b)应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

3.3 安全计算环境

3.3.1 感知节点设备安全

本项要求包括：

(a)应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更；

(b)应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力；

(c)应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。

3.3.2 网关节点设备安全

本项要求包括：

(a)应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力；

(b)应具备过滤非法节点和伪造节点所发送的数据的能力；

(c)授权用户应能够在设备使用过程中对关键密钥进行在线更新；

(d)授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

3.3.3 抗数据重放

本项要求包括：

(a)应能够鉴别数据的新鲜性，避免历史数据的重放攻击；

(b)应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

3.3.4 数据融合处理

本项要求包括：

(a)应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用；

(b)应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令。

3.4 安全运维管理

3.4.1 感知节点管理

本项要求包括：

(a)应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；

(b)应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；

(c)应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

实现方式：建议使用代码签名，用来保护设备不受攻击，确保所有运行代码都是被签名授权的，并在签名后代码不会被篡改，而确保恶意代码不会被运行和覆盖正常代码。代码签名技术可以应用在应用级别，也可应用在固件级别异常检测，输出详细的日志信息，进行日志汇总、日志总结分析，及时发现攻击行为进行告警和干预处理。同时，物联网的设备需要接入互联网，针对 TCP/IP 协议栈的网络风险控制。

4、工业控制系统安全扩展要求

4.1 安全物理环境

4.1.1 室外控制设备物理防护

本项要求包括：

(a)室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；

(b)室外控制设备防止应原理强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

4.2 安全通信网络

4.2.1 网络架构

本项要求：

(a)工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用符合国家或行业规定的专用产品实现单项安全隔离；

(b)工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；

(c)涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离。

4.2.2 通信传输

在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密。

4.3 安全区域边界

4.3.1 访问控制

本项要求包括：

(a)应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-Mail,Web、Telnet、Rlogin、FTP 等通用网络服务；

(b)应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

4.3.2 拨号使用控制

本项要求包括：

(a)工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数数，并采取用户身份鉴别和访问控制等措施；

(b)拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施；

(c)涉及实时控制和数据传输的工业控制系统禁止使用拨号访间服务。

4.3.3 无线使用控制

本项要求包括：

(a)应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

(b)应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；

(c)应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；

(d)对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。

4.4 安全计算环境

4.4.1 控制设备安全

本项要求包括：

(a)控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访

问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

(b)应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

(c)应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理；

(d)应使用专用设备和专用软件对控制设备进行更新；

(e)应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序；

4.5 安全建设管理

4.5.1 产品采购和使用

工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

4.5.2 外包软件开发

应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。

实现方式：断开工业控制系统同公共网络之间的所有不必要连接，对确实需要的连接，系统运营单位要逐一进行登记，采取设置防火墙、单向隔离等措施加以防护，对外包人员实行严格的合同约束，对无线组网采取严格的身份认证，密切关注产品漏洞和补丁发布，严格软件

省级、补丁安装管理，严防病毒、木马等恶意代码侵入。

5、电子政务外网要求

5.1 落实网络安全主体责任

接入电子政务外网的各部门各单位是本部门（单位）政务网络和政务信息系统的网络安全责任主体，应当按照“谁主管谁负责、谁运行谁负责、谁使用谁负责” 的原则认真落实网络安全主体责任。要明确工作机构，配置专门力量，做好网络和信息系统运行维护工作。要切实加强对电子政务外网安全工作的统筹协调，及时研究解决电子政务外网安全工作中遇到的问题，把网络安全工作责任和各项措施落到实处。

5.2 加强电子政务外网接入管理

各部门各单位应当按照《网络安全法》规定和电子政务外网安全管理的相关规范，落实电子政务外网接入管理的安全措施。接入电子政务外网的网络应与其他网络隔离，并加强边界管理和内部网络安全管理。接入电子政务外网的信息系统上线前应做好安全检测工作，确保系统无安全 隐患和风险后方可上线运行。接入电子政务外网的终端实行专机专用，所有终端和设备在入网前，应采取安装安全防护软件、定 期更新并查杀病毒等有效安全措施。定期开展网络安全风险排查 和评估工作，及时采取针对性整改措施，切实消除安全隐患，保障本部门（单位）接入电子政务外网的网络、信息系统、终端和设备运行稳定、数据安全可控。建立健全网络安全处置机制，经常性开展应急演练，提升网络安全应急响应能力，坚决防范有重大影响的网络安全事件发生。

5.3 做好电子政务外网网络安全等级保护工作

各部门各单位要对照网络安全等级保护要求，按照大平台大系统原则，认真梳理政务信息系统，有机整合相关子系统和功能模块，科学划定系统边界范围，及时开展等级保护备案和测评整改工作。新增政务信息系统，完成等级保护备案后再申请政务云资源，完成等级保护测评和整改后方可上线运行。

第三部分：主要网络安全设备

目前各种安全威胁充斥着网络，信息的安全性、可靠性难以保证，需要部署相关网络安全设备进行必要的防护。目前主流网络安全设备包括防火墙、网闸、入侵检测、VPN 等，熟悉常见的网络安全设备的功能及使用方法有助于更好地优化网络安全防护手段，提升防护能力。

同时要加强网络安全设备日常运维，所有设备均要求及时更新版本，建立系统和特征库的许可有效期台账，同时设备端口必须连接在网络安全区域，并通过堡垒机进行访问控制管理。

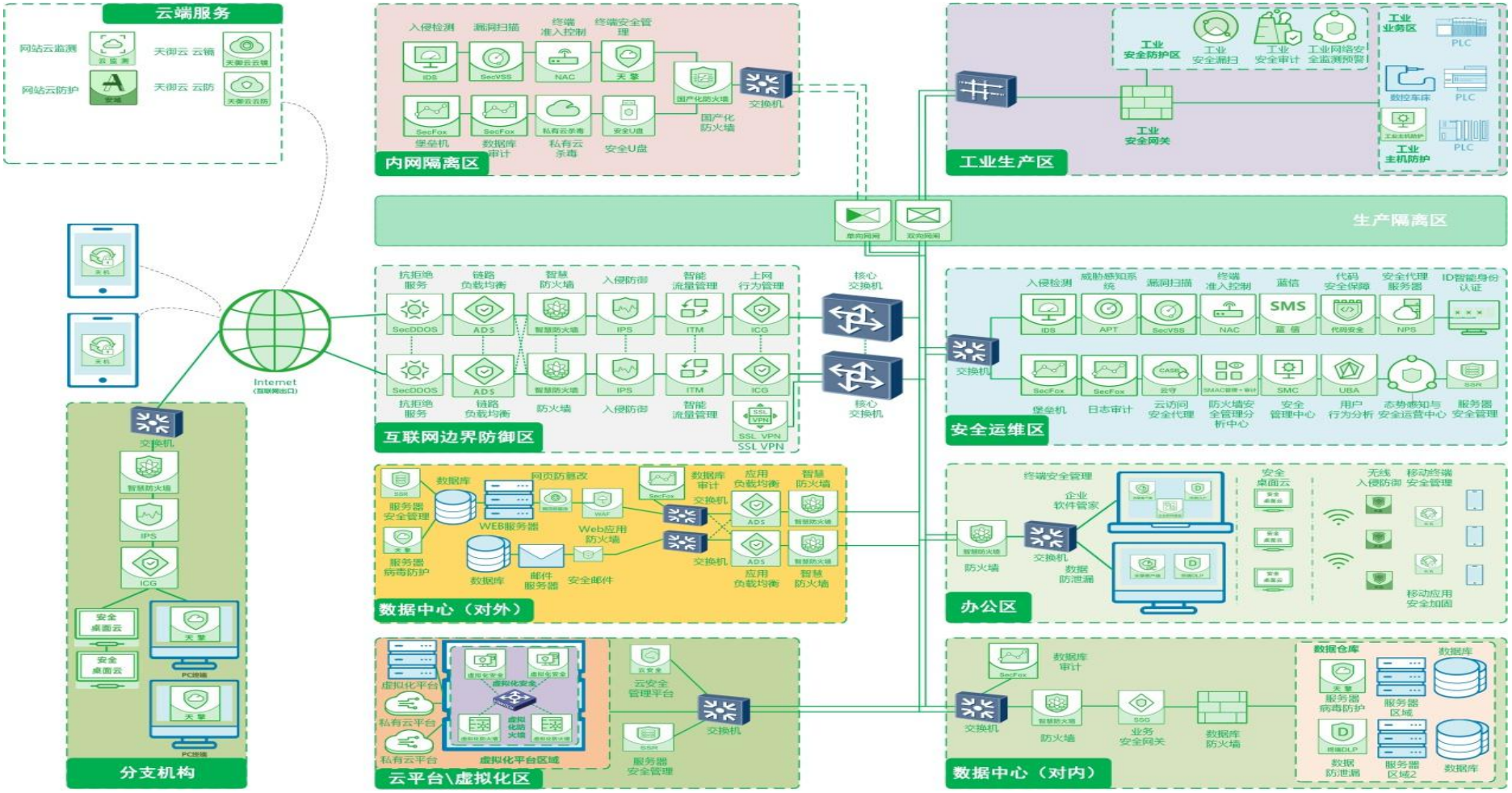

图 3.1 标准网络拓扑示意图

1、防火墙设备

1.1 设备介绍

防火墙（Firewall），也称防护墙，是由 Check Point 创立者发明的。它是一个信息安全的防护系统，依照特定的规则，允许或是限制传输的数据通过，主要是网络层的安全防护设备。防火墙是一个由软件和硬件设备组合而成，在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。

下一代防火墙,即 Next Generation Firewall,简称 NG Firewall，是一款可以全面应对应用层威胁的高性能防火墙，提供网络层应用层一体化安全防护。防火墙主要用于边界安全防护的权限控制和安全域的划分。

1.2 设备功能

在网络中,所谓“防火墙”,是指一种将内部网和公众访问网（如 Internet）分开的方法，它实际上是一种隔离技术。 防火墙是在两个网络通讯时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。

1.3 设备拓扑示意

部署于内、外网边界和各个区域之间，用于权限访问控制和安全域划分。

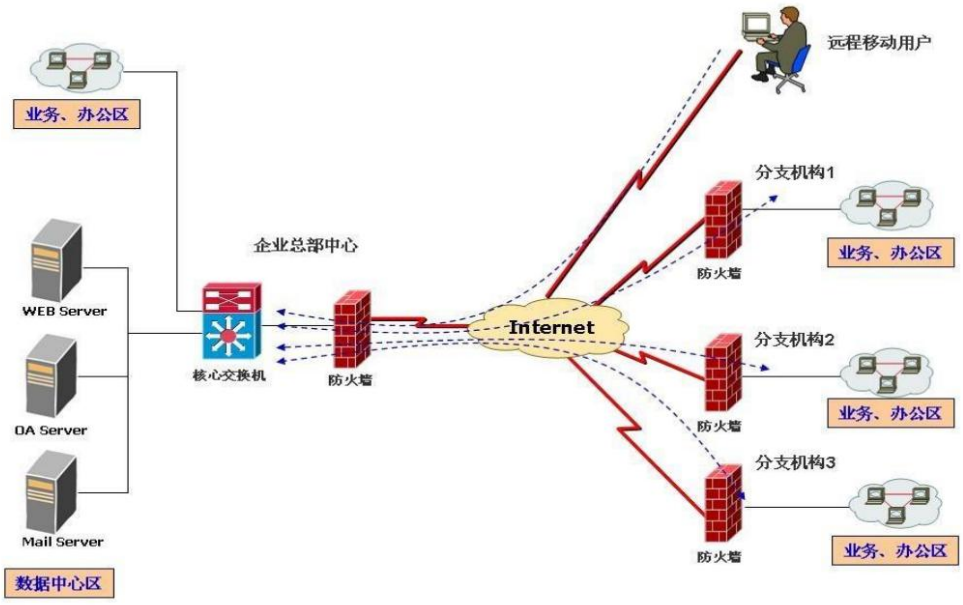

图 3.2 防火墙设备部署方式

2、网闸设备

2.1 设备介绍

网闸（GAP）全称安全隔离网闸。安全隔离网闸是一种由带有多种控制功能专用硬件在电路上切断网络之间的链路层连接，并能够在网络间进行安全适度的应用数据交换的网络安全设备。相比于防火墙，能够对应用数据进行过滤检查，防止泄密、进行病毒和木马检查。

2.2 设备功能

网闸是使用带有多种控制功能的固态开关读写介质连接两个独立主机系统的信息安全设备。由于网闸所连接的两个独立主机系统之间，不存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议，不存在依据协议的信息包转发，只有数据文件的无协议"摆渡"，且对固态存储介质只有"读"和" 写"两个命令。所以，网闸从物理上隔离、阻断了具有潜在攻击可能的一切连接，使"黑客"无法入侵、无法攻击、无法破坏，实现了真正的安全。

主要功能有：安全隔离、内核防护、协议转换、病毒查杀、访问控制、安全审计、身份认证。

2.3 设备拓扑示意

部署于不同区域之间物理隔离、不同网络之间物理隔离、网络边界物理隔离，也常用于数据同步、信息发布等。

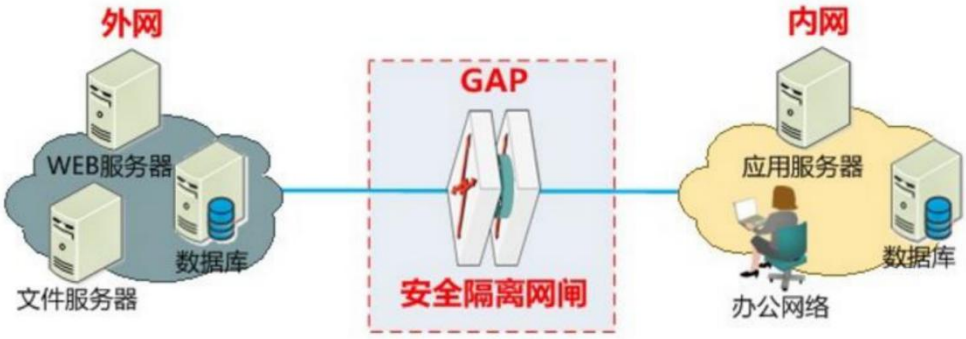

图 3.3 网闸设备部署方式

3、漏洞扫描系统设备

3.1 设备介绍

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为。如果把网络信息安全工作比作一场战争的话，漏洞扫描器就是这场战争中，盘旋在终端设备，网络设备上空的 “全球鹰”。它和防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。通过对网络的扫描，网络管理员能了解网 络的安全设置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置，在黑客攻击前进行防范。漏洞扫描系统可以针对主机、web 应

用、数据库进行扫描，发现漏洞后提供漏洞说明、漏洞影响、漏洞验证和 漏洞修复建议。

3.2 设备功能

漏洞扫描技术是一类重要的网络安全技术。它和防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。 通过对网络的扫描，网络管理员能了解网络的安全设置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置，在黑客攻击前进行防范。如果说防火墙和 网络监视系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，能有效避免黑客攻击行为，做到防患于未然。

1. 定期的网络安全自我检测、评估

配备漏洞扫描系统，网络管理人员可以定期的进行网络安全检测服务，安全检测可帮助客户最大可能的消除安全隐患，尽可能早地发现安全漏洞并进行修补，有效的利用已有系统，优化资源，提高网络的运行效率。

2. 安装新软件、启动新服务后的检查

由于漏洞和安全隐患的形式多种多样，安装新软件和启动新服务都有可能使原来隐藏的漏洞暴露出来，因此进行这些操作之后应该重新扫描系统，才能使安全得到保障。

3. 网络建设和网络改造前后的安全规划评估和成效检验

网络建设者必须建立整体安全规划，以统领全局，高屋建瓴。在可以容忍的风险级别和可以接受的成本之间，取得恰当的平衡，在多

种多样的安全产品和技术之间做出取舍。配备网络漏洞扫描/网络评估系统可以进行安全规划评估和成效检验网络的安全系统建设方案和建设成效评估。

4. 网络承担重要任务前的安全性测试

网络承担重要任务前应该多采取主动防止出现事故的安全措施，从技术上和管理上加强对网络安全和信息安全的重视，形成立体防护，由被动修补变成主动的防范，最终把出现事故的概率降到最低。配备网络漏洞扫描/网络评估系统可以进行安全性测试。

5.网络安全事故后的分析调查

网络安全事故后可以通过网络漏洞扫描/网络评估系统分析确定网络被攻击的漏洞所在，帮助弥补漏洞，尽可能多得提供资料方便调查攻击的来源。

6.重大网络安全事件前的准备

重大网络安全事件前网络漏洞扫描/网络评估系统能够帮助用户及时的找出网络中存在的隐患和漏洞，帮助用户及时的弥补漏洞。

3.3 设备拓扑示意

部署在服务器区域或在核心网络区域进行接入，能够保证所有网络可达即可。通过浏览器控制台创建扫描任务和扫描策略定制。

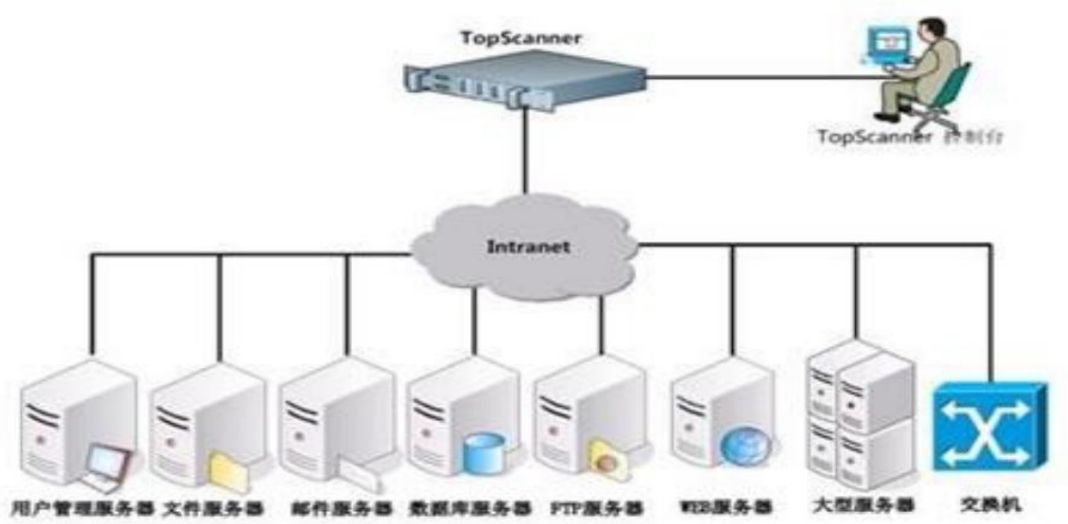

图 3.4 漏扫系统备部署方式

4、入侵防御系统设备（IPS）

4.1 设备介绍

入侵防御系统(Intrusion-prevention system,简称 IPS) 位于防火墙和网络的设备之间，依靠对数据包的检测进行防御（检查入网的数据包，确定数据包的真正用途，然后决定是否允许其进入内网。能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备，能够即时的中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。防火墙可以拦截低层攻击行为，但对应用层的深层攻击行为无能为力,IPS 是对防火墙的补充。

4.2 设备功能

在 ISO/OSI 网络层次模型(见 OSI 模型) 中，防火墙主要在第二到第四层起作用，它的作用在第四到第七层一般很微弱。而防病毒软件主要在第五到第七层起作用。

为了弥补防火墙和防病毒软件二者在第四到第五层之间留下的空档，几年前,工业界已经有入侵检测系统(IDS: Intrusion

Detection System）投入使用。入侵检测系统在发现异常情况后及时向网路安全管理人员或防火墙系统发出警报。可惜这时灾害往往已经形成。

随后应运而生的入侵响应系统(IRS: Intrusion Response Systems) 作为对入侵检测系统 的补充能够在发现入侵时，迅速做出反应，并自动采取阻止措施。而入侵预防系统则作为二者的进一步发展，汲取了二者的长处。

入侵防御系统也像入侵检测系统一样，专门深入网络数据内部，查找它所认识的攻击代码 特征，过滤有害数据流，丢弃有害数据包，并进行记载，以便事后分析。除此之外，更重要的是，大多数入侵防御系统同时结合考虑应用程序或网路传输中的异常情况，来辅助识别入侵和 攻击。比如，用户或用户程序违反安全条例、数据包在不应该出现的时段出现、作业系统或应 用程序弱点的空子正在被利用等等现象。入侵防御系统虽然也考虑已知病毒特征，但是它并不仅仅依赖于已知病毒特征。

应用入侵防御系统的目的在于及时识别攻击程序或有害代码及其克隆和变种，采取预防措施，先期阻止入侵，防患于未然。或者至少使其危害性充分降低。入侵防御系统一般作为防火 墙和防病毒软件的补充来投入使用。在必要时，它还可以为追究攻击者的刑事责任而提供法律上有效的证据。

4.3 设备拓扑示意

入侵检测系统部署在服务器区域前端，能够保证所有服务器流

量从本设备经过。

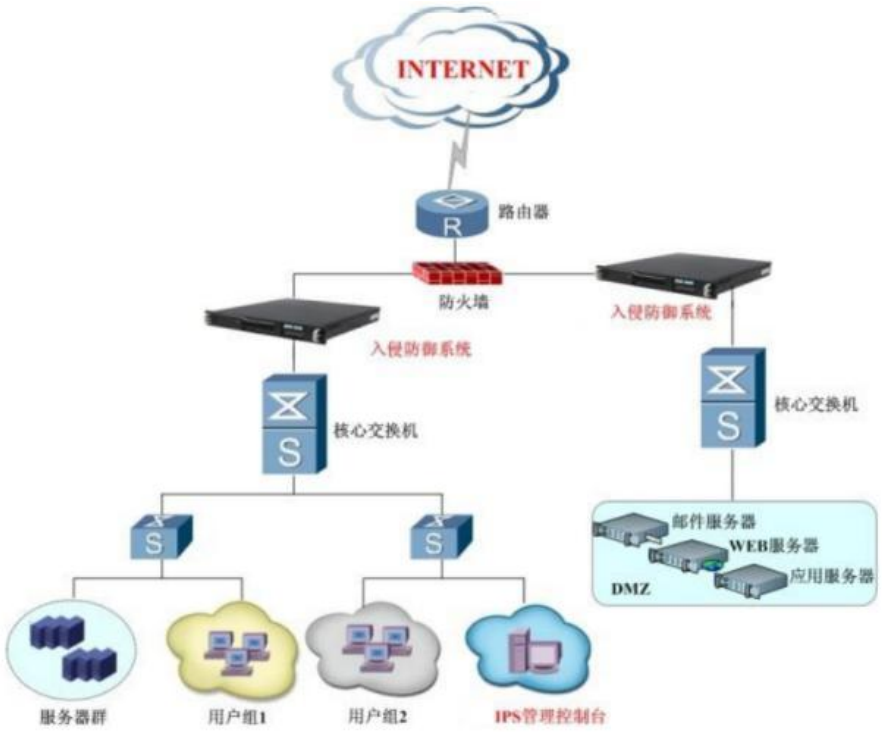

图 3.5 入侵防御系统设备部署方式

5、Web 应用防火墙设备（WAF）

5.1 设备介绍

Web 应用防火墙(Web Application Firewall,简称 WAF) 用以解决诸如防火墙一类传统设备束手无策的 Web 应用安全问题。与传统防火墙不同，WAF 工作在应用层，因此对 Web 应用防护具有先天的技术优势。WAF 对来自 Web 应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护。

5.2 设备功能

WEB 应用防火墙是集 WEB 防护、网页保护、负载均衡、应用交付于一体的 WEB 整体安全防护设备的一款产品。它集成全新的安全理念与先进的创新架构，保障用户核心应用与业务持续稳定的运行。

WEB 应用防火墙还具有多面性的特点。比如从网络入侵检测的角度来看可以把 WAF 看成 运行在 HTTP 层上的 IDS 设备;从防火墙角度来看，WAF 是一种防火墙的功能模块;还有人把 WAF 看作“深度检测防火墙”的增强。

总体来说，Web 应用防火墙的具有以下四大个方面的功能：

审计功能：用来截获所有 HTTP 数据或者仅仅满足某些规则的会话。

访问控制功能：用来控制对 Web 应用的访问，既包括主动安全模式也包括被动安全模式。

架构/网络设计功能：当运行在反向代理模式，他们被用来分配职能，集中控制，虚拟基础结构等。

Web 应用加固功能：这些功能增强被保护 Web 应用的安全性，它不仅能够屏蔽 WEB 应用固有弱点，而且能够保护 WEB 应用编程错误导致的安全隐患。

1、事前主动防御，智能分析应用缺陷、屏蔽恶意请求、防范网页篡改、阻断应用攻击，全方位保护 WEB 应用。

2、事中智能响应，快速 P2DR 建模、模糊归纳和定位攻击，阻止风险扩散，消除“安全事故”于萌芽之中。

3、事后行为审计，深度挖掘访问行为、分析攻击数据、提升应用价值，为评估安全状况提供详尽报表。

4、面向客户的应用加速，提升系统性能，改善 WEB 访问体验。

5、面向过程的应用控制，细化访问行为，强化应用服务能力。

6、面向服务的负载均衡，扩展服务能力，适应业务规模的快速壮大。

5.3 设备拓扑示意

Web 应用防火墙部署在服务器区域前端，专门针对 web 应用进行防护，Web 应用防火墙应保证所有服务器流量从本设备经过检测后再放通给服务器。

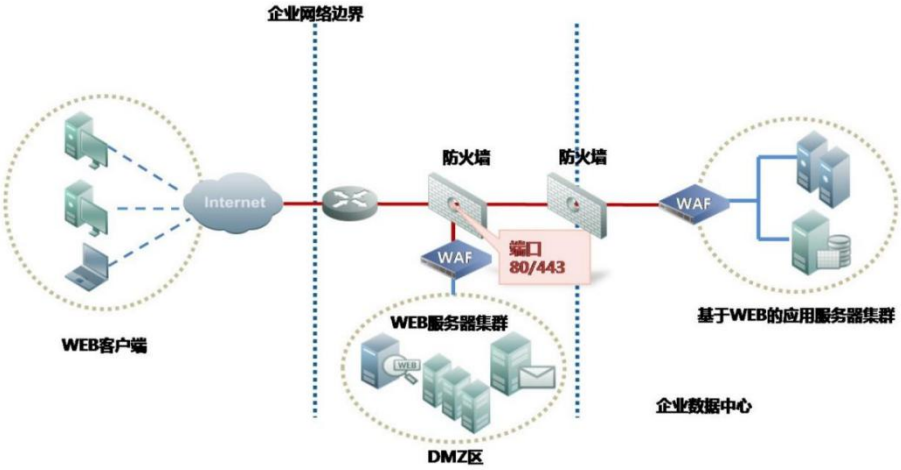

图 3.6 Web 应用防火墙设备部署方式

6、运维审计系统设备（堡垒机）

6.1 设备介绍

运维审计系统（堡垒机），即在一个特定的网络环境下，为了保障网络和数据不受来自外部和内部 用户的入侵和破坏，而运用各种技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动，以便集中报警、及时处理及审计定责。主要用于服务器、网络设备、安全设备等的权限分离和安全管控。

6.2 设备功能

其从功能上讲，它综合了核心系统运维和安全审计管控两大主干功能，从技术实现上讲，通过切断终端计算机对网络和服务器资源的

直接访问，而采用协议代理的方式，接管了终端计算机对网络和服务器的访问。

形象地说，终端计算机对目标的访问，均需要经过运维安全审计的翻译。运维安全审计扮演着看门者的工作，所有对网络设备和服务器的请求都要从这扇大门经过。因此运维安全审计能够拦截非法访问，和恶意攻击，对不合法命令进行命令阻断，过滤掉所有对目标设备的非法访问行为，并对内部人员误操作和非法操作进行审计监控，以便事后责任追踪。

安全审计作为企业信息安全建设不可缺少的组成部分，逐渐受到用户的关注，是企业安全体系中的 重要环节。同时，安全审计是事前预防、事中预警的有效风险控制手段，也是事后追溯的可靠证据来源。

单点登录功能：支持对 Windows、Linux、Unix、数据库、网络设备、安全设备等一系列授权账号进行密码的自动化周期更改，简化密码管理，让使用者无需记忆众多系统密码，即可实现自动登录目标设备，便捷安全。

账号管理：设备支持统一账户管理策略，能够实现对所有服务器、网络设备、安全设备等账号进行集中管理， 完成对账号整个生命周期的监控，并且可以对设备进行特殊角色设置如：审计巡检员、运维操作员、设备管理员等自定义设置，以满足审计需求。

身份认证：设备提供统一的认证接口，对用户进行认证，支持身份认证模式包括动态口令、静态密码、硬件 key 、生物特征等多种

认证方式，设备具有灵活的定制接口，可以与其他第三方认证服务器之间结合；安全的认证模式，有效提高了认证的安全性和可靠性。

访问控制：设备支持对不同用户进行不同策略的制定，细粒度的访问控制能够最大限度的保护用户资源的安全，严防非法、越权访问事件的发生。

操作审计：设备能够对字符串、图形、文件传输、数据库等全程操作行为审计：通过设备录像方式实时监控运维人员对操作系统、安全设备、网络设备、数据库等进行的各种操作，对违规行为进行事中控制。对终端指令信息能够进行精确搜索，进行录像精确定位。

6.3 设备拓扑示意

堡垒机部署的前提是必须切断用户直接访问资源的路径，建议堡垒机冗余部署，部署在网络安全管理区域，通过 VPN 访问，在交换机做策略限制，只允许堡垒机 IP 访问内网服务器，一般部署在所有用户都能访问资源的核心网络端口下。

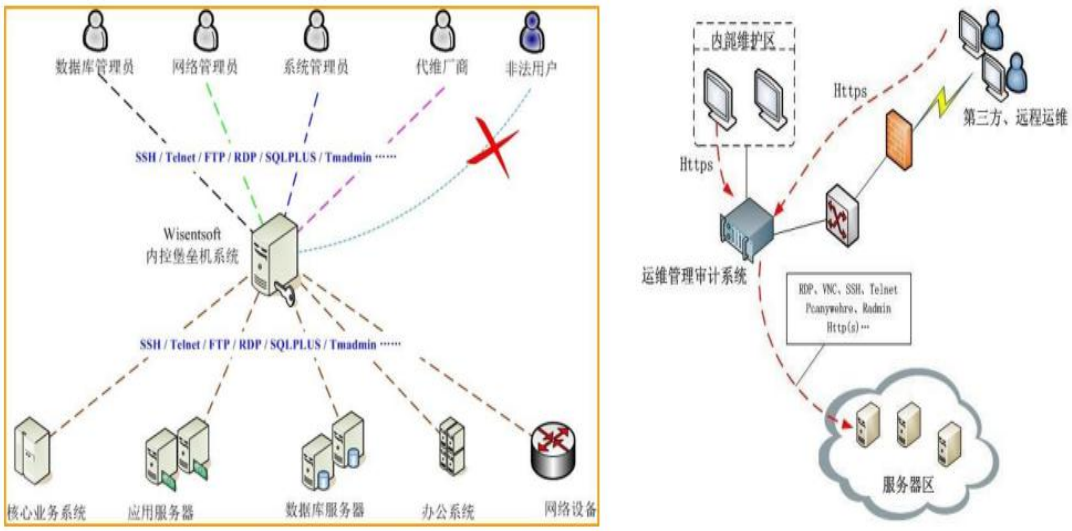

图 3.7 运维审计系统设备部署方式

7、上网行为管理设备

7.1 设备介绍

上网行为管理是指帮助互联网用户控制和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析。专用于防止非法信息恶意传播，避免国家机密、商业信息、科研成果泄漏的产品；并可实时监控、管理网络资源使用情况，提高整体工作效率。

7.2 设备功能

上网人员管理、邮件管理、网页发帖管理、上网应用管理、流量管理、行为分析。

7.3 设备拓扑示意

部署在网络出口边界，保证所有用户的流量在从出口到达互联网之前通过本设备检测后放行。

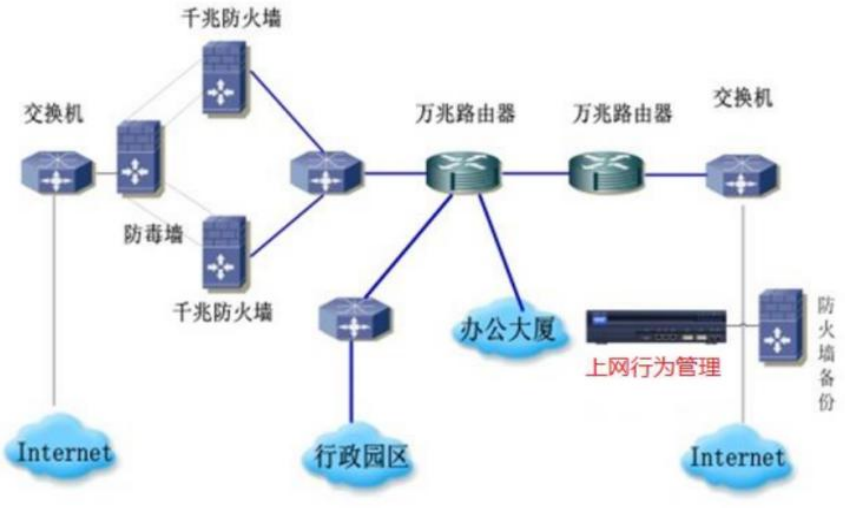

图 3.8 上网行为管理设备部署方式

8、虚拟专用网络设备（VPN）

8.1 设备介绍

VPN(virtual private network)虚拟专用网络。在公用网络上建立专用网络，采用国密算法进行加密通讯。在企业网络中有广泛应用。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN有多种分类方式，主要是按协议进行分类。 VPN的隧道协议主要有三种：PPTP、L2TP和IPSec。常用VPN类型有SSL VPN(以HTTPS为基础的VPN技术)和IPSec VPN(基于IPSec协 议的VPN技术，由IPSec协议提供隧道安全保障)。

8.2 设备功能

VPN属于远程访问技术，简单地说就是利用公用网络架设专用网络。

例如某公司员工出差到外地，他想访问企业内网的服务器资源，这种访问就属于远程访问。 让外地员工访问到内网资源，利用VPN的解决方法就是在内网中架设一台VPN服务器。外地员工在 当地连上互联网后，通过互联网连接VPN服务器，然后通过VPN服务器进入企业内网。为了保证数据安全，VPN服务器和客户机之间的通讯数据都进行了加密处理。有了数据加密，就可以认为数据是在一条 专用的数据链路上进行安全传输，就如同专门架设了一个专用网络一样，但实际上VPN使用的是互联网上的公用链路，因此VPN称为虚拟专用网络，其实质上就是利用加密技术在公网上封装出一个数据通讯隧道。

8.3 设备拓扑示意

部署在网络、应用、服务器前端。保证外网用户接入内网流量从该设备经过放通。

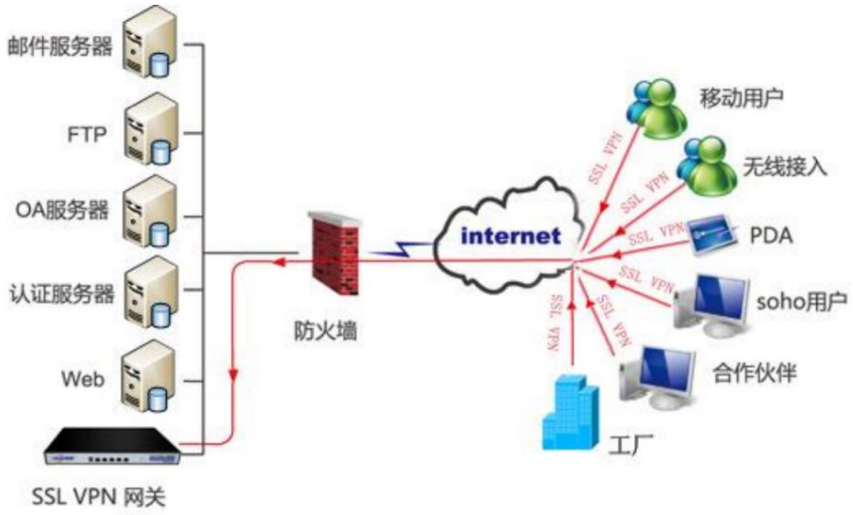

图 3.9 虚拟专用网络设备部署方式

9、防毒墙

9.1 设备介绍

考虑到防火墙、漏扫设备、入侵检测等设备面临诸如 SQLSlammer 等新的蠕虫病毒时，仍然显得力不从心，通过防毒墙在网络边缘进行病毒检测、拦截和清除功能，在不同的网络边缘分别布置不同性能的防毒墙保护网络安全。

9.2 设备功能

通过独立的检测机制，毁灭性病毒和蠕虫病毒进入网络前即在网络边缘进行全面扫描，可用于独立式边缘病毒扫描结构，同时，它也可以作为企业整体网络防病毒的一个组成部分，建立网络边缘（网关）、客户端和服务器三层病毒扫描架构的立体网络防病毒体系，对企业网络的入口提供了简单的"即插即忘"式的保护，能够抵御某些新型蠕虫的攻击，病毒在进入网络之前就会被拦截，避免了由于病毒入侵到服务器和工作站所引起的一系列的典型问题。在新病毒的传播中，硬件防毒墙能够有效防止网络攻击，且不会消耗大部分资源用于拦截病毒，

设备接入不需要改变整体网络结构。从而可实现内部网络无改动，病毒防护更有效。

9.3 设备拓扑示意

部署在应用、服务器前端，网络防火墙前后。保证用户上网下载等流量从该设备经过放通。

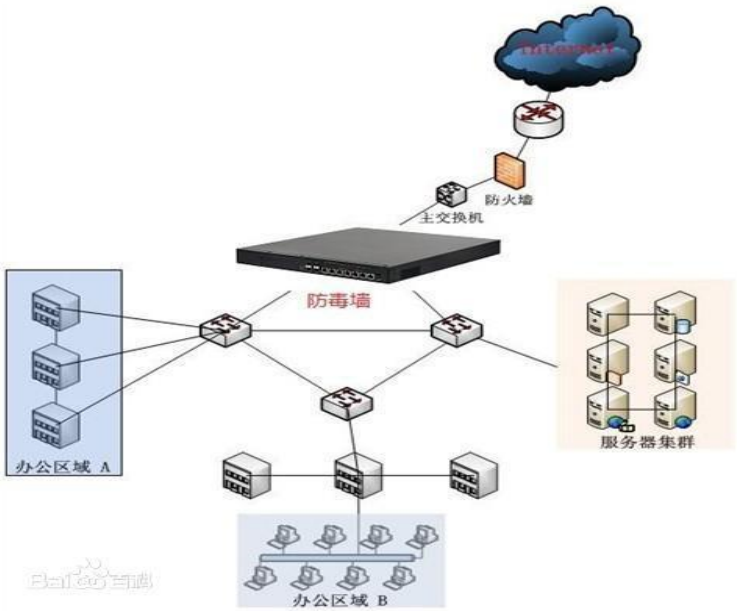

图 3.10 防毒墙设备部署方式

10、应用主机综合安全防护软件

10.1 软件介绍

该系统采用 C/S 与 B/S 的结合，通过 PC 端、客户端、浏览器即可实现对服务器端的安全管理与监控。系统跨平台支持 Windows 及 Linux 双操作系统，以操作系统内核加固技术、Web 访问控制技术作为核心防御体系，针对操作系统核心资源，如注册表、网络连接、系统文件、进程等进行有效防护，同时，采用 Web 访问控制技术有效抵御网络层攻击。

10.2 软件功能

安全防护：依托操作系统内核加固和 web 访问控制技术，有效监测与防护 CC 攻击、SQL 注入、XSS 跨站、漏洞利用、敏感词过滤、暴力破解、木马远程控制、网页篡改等黑客入侵行为；

风险监测：实时检测进程恶意创建、数据盗取、页面篡改等各类攻击动作，归并攻击日志，自动回溯攻击过程，发布安全预警信息，指导开展应急处置工作，实现事前预警、事中控制和事后追溯；

安全巡检：制定操作系统与业务应用安全基线规则，对主机系统和 web 应用进行恶意文件扫描、系统服务优化、账户安全检查、系统配置安全检查、计划任务和补丁扫描等巡检，以确定当前系统安全风险，提出安全运行和安全策略实施建议；

应急处置：研究主机防火墙技术，细粒度管理系统对外服务端口和运行应用情况，解决同级网络间、主机间的访问控制问题，避免安全事件的由点及面的扩散，当遇安全事件能够一键封闭服务端口、启停业务应用、处置病毒传播、终端不良信息扩散等；

安全态势展示：汇集全部单点防护探针监测数据，进行集中分析，可视化展示攻击源信息、攻击类型、攻击事件、风险状态、入侵事件等攻击行为，支撑威胁事件研判和指挥决策。

10.3 设备拓扑示意

软件部署分为云中心部署和Agent部署两个部分。

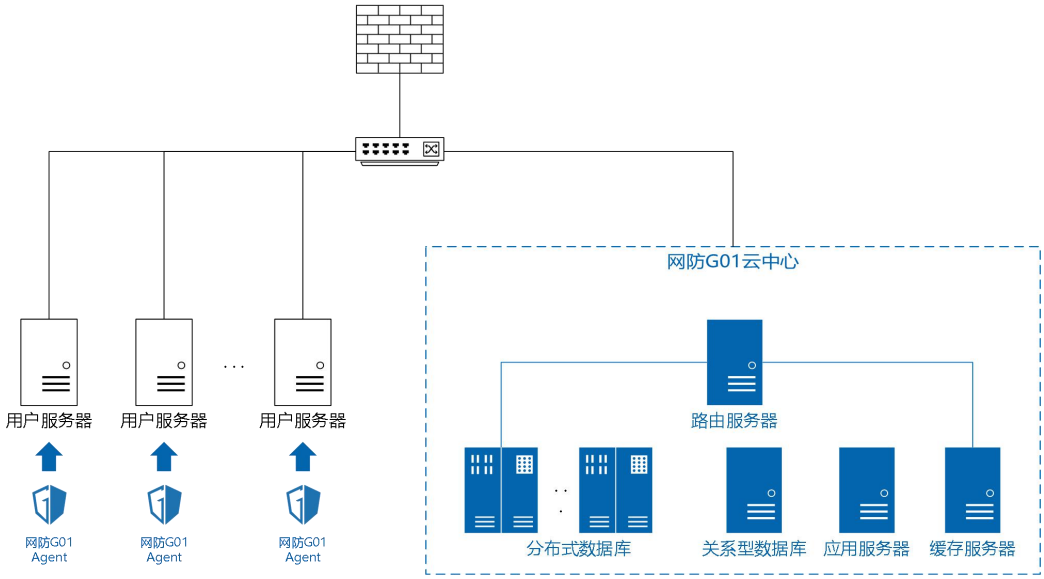

图 3.11 应用主机综合安全防护软件部署方式

11、数据库审计设备

11.1 软件介绍

数据库审计（简称 DBAudit）能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

11.2 软件功能

通过应用层访问和数据库操作请求进行多层业务关联审计，实现访问者信息的完全追溯，包括：操作发生的 URL、客户端的 IP、请求报文等信息，通过多层业务关联审计更精确地定位事件发生前后所有层面的访问及操作请求，使管理人员对用户的行为一目了然，真正做到数据库操作行为可监控,违规操作可追溯。

通过对不同数据库的 SQL 语义分析，提取出 SQL 中相关的要素（用

户、SQL 操作、表、字段、视图、索引、过程、函数、包等） 实时监控来自各个层面的所有数据库活动，包括来自应用系统发起的数据库操作请求、来自数据库客户端工具的操作请求以及通过远程登录服务器后的操作请求等 通过远程命令行执行的 SQL 命令也能够被审计与分析，并对违规的操作进行阻断系统不仅对数据库操作请求进行实时审计，而且还可对数据库返回结果进行完整的还原和审计，同时可以根据返回结果设置审计规则。

一旦发生安全事件，提供基于数据库对象的完全自定义审计查询及审计数据展现，彻底摆脱数据库的黑盒状态。

灵活的策略定制：根据登录用户、源 IP 地址、数据库对象（分为数据库用户、表、字段）、操作时间、SQL 操作命令、返回的记录数或受影响的行数、关联表数量、SQL 执行结果、SQL 执行时长、报文内容的灵活组合来定义客户所关心的重要事件和风险事件多形式的实时告警：当检测到可疑操作或违反审计规则的操作时，系统可以通过监 控中心告警、短信告警、邮件告警、Syslog 告警等方式通知数据库管理员。

对于客户关心的操作可以回放整个相关过程，让客户可以看到真实输入及屏幕显示内容。对于远程操作实现 对精细内容的检索，如执行删除表、文件命令、数据搜索等。

11.3 设备拓扑示意

一般部署在连接数据库服务器汇聚交换机镜像端口下，用于整体流量分析和日志审计分析。 不改变原有网络结构，不会对网络产生

任何影响。

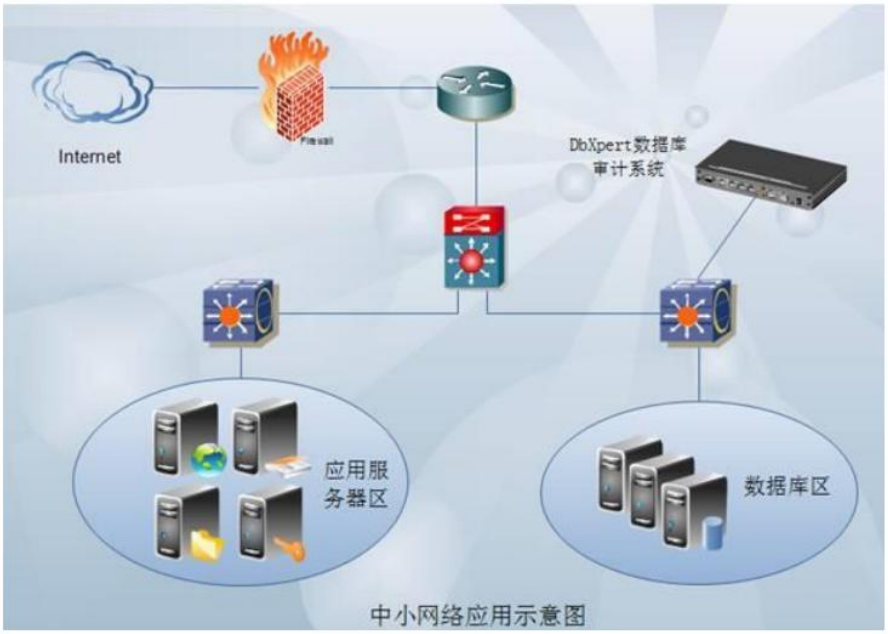

图 3.12 数据库审计设备部署方式

12、日志审计设备

12.1 软件介绍

日志审计系统是用于全面收集企业 IT 系统中常见的安全设备、网络设备、数据库、服务器、应用系统、主机等设备所产生的日志（包括运行、告警、操作、消息、状态等）并进行存储、监控、审计、分析、报警、响应和报告的系统。

12.2 软件功能

日志监控：提供日志监控能力，支持对采集器、采集器资产的实时状态进行监控，支持查看 CPU、磁盘、内存总量及当前使用情况；支持查看资产的概览信息及资产关联的事件分布；

日志采集：提供全面的日志采集能力：支持网络安全设备、网络设备、数据库、Windows/Linux 主机日志、Web 服务器日志、虚拟化

平台日志以及自定义等日志；

提供多种的数据源管理功能：支持数据源的信息展示与管理、采集器的信息展示与管理以及 Agent 的信息展示与管理；提供分布式外置采集器、Agent 等多种日志采集方式；支持 IPv4、IPv6 日志采集、分析以及检索查询；

日志存储：提供原始日志的存储，可自定义存储周期，支持 FTP 日志备份以及 NFS 网络文件共享存储等多种存储扩展方式

日志检索：提供丰富灵活的日志查询方式，支持全文、关键字、括弧、正则、模糊等检索；提供便捷的日志检索操作，支持保存检索、从已保存的检索导入见多条件等；

日志分析：提供便捷的日志分析操作，支持对日志进行分组、分组查询以及从叶子节点可直接查询分析日志；

日志转发：支持原始日志、范式化日志转发

日志事件告警：内置丰富的单源、多源事件关联分析规则，支持自定义事件规则，可按照日志、字段布尔逻辑关系等方式自定义规则；支持时间的查询、查询结果统计以及统计结果的展示等；支持对告警规则的自定义，可设置针对事件的各种筛选规则、告警等级等；

日志报表管理：支持丰富的内置报表以及灵活的自定义报表模式，支持编辑报表的目录接口、引用统计项、设置报表标题、展示页眉和页码、报表配置基本内容（名称、描述等）；支持实时报表、定时报表、周期性任务报表等方式；支持 html，pdf，word 格式的报表文件以及报表 logo 的灵活配置；

12.3 设备拓扑示意

日志审计系统一般为分布部署时，采集器可视用户需求部署在任何网络可达区域。

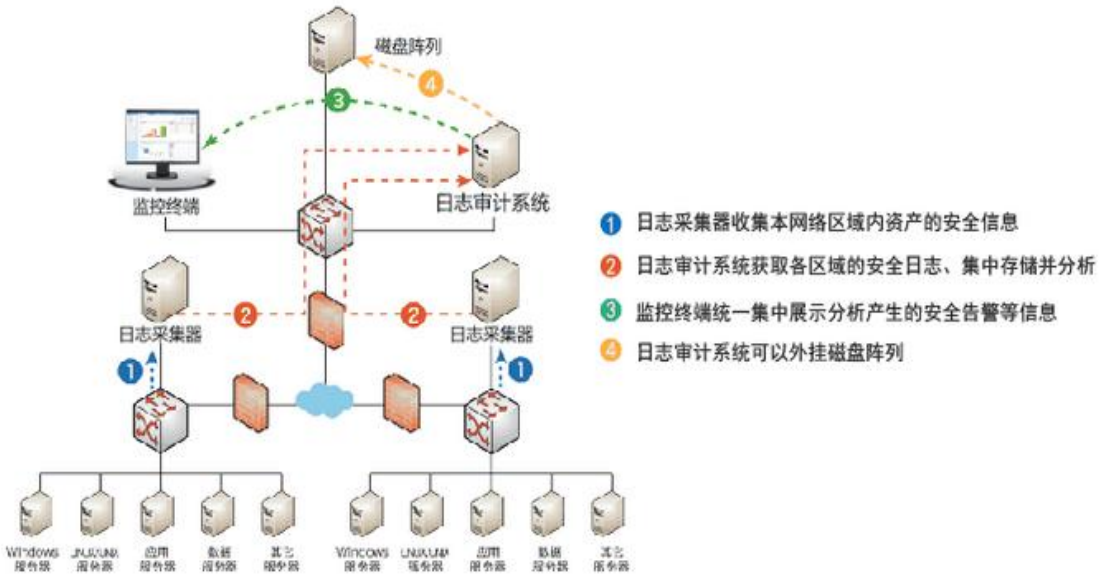

图 3.13 日志审计设备部署方式

13、服务器密码机

13.1 设备介绍

服务器密码机是符合国家密码管理局批准使用的高性能密码设备，通过旁路部署，实现密钥生成、签名验签、数据的加密、数据的解密等操作，为各类密码安全应用系统提供高速的、多任务并行处理的密码运算，是信息安全产业链中最基本的、最不可缺少的硬件密码设备。

13.2 设备功能

服务器密码机具有如下主要功能：

密钥存储：密码机内可安全存储各种类型的非对称密钥对、对称密钥；

密钥生成：密码机可提供各类型密钥对的生成功能；

非对称密码运算：密码机可提供基于 SM2、RSA、DSA、ECDSA、SM9、EdDSA 等算法的签名/验签、加密/解密、密钥协商等功能；

对称密码运算：密码机可提供基于 SM1、SM4、SM7、SSF33、DES/3DES、AES 等算法的加解密功能，算法模式支持 ECB/CBC/OFB/CFB/CTR/XTS/GCM/CCM 等；

消息鉴别码的产生及验证：密码机可提供基于 SM1、SM4、SM7、SSF33、DES/3DES、AES 等算法的 CBC-MAC、CMAC 的产生及验证；

杂凑密码运算：密码机可提供基于 SM3、SHA1、SHA2、MD5 等算法的杂凑运算功能；

消息认证码的产生：密码机可提供基于 SM3、SHA1/SHA2 等算法的 HMAC 的产生及验证；

随机数生成：密码机可提供基于双 WNG8 物理随机源的随机数生成功能。

13.3 设备拓扑示意

服务器密码机旁路部署通过 API 接口调用，支持单机、集群部署。集群部署可提高密码运算性能，增强设备冗余，集群中密码机故障时，可不影响业务系统正常运行。

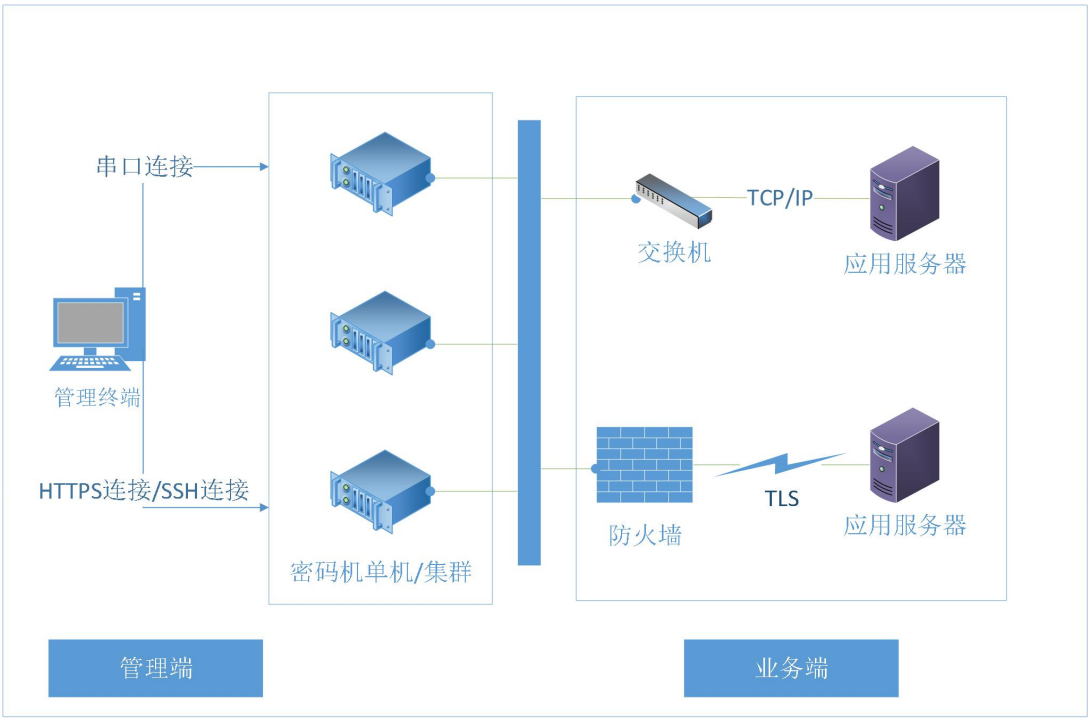

图 3.14 服务器密码机设备部署方式

14、密钥管理系统

14.1 设备介绍

密钥管理系统是符合国家密码管理局批准使用的高性能密码设备，通过旁路部署，实现密钥生成、签名验签、数据的加密、数据的解密等操作，支持包括对称密钥、非对称密钥、数字证书和认证令牌等多种加密对象的管理，简化密钥管理模型；同时，提供了基于用户组的密钥管理策略，使得加密变得更易于配置和管理，减少了密钥管理系统的维护成本，满足用户多应用多业务的密钥管理需求。

14.2 设备功能

密钥管理系统具有如下主要功能：

提供对称密钥、非对称密钥、数字证书等加密对象的状态管理和属性管理。完成对加密对象的生成、存储、激活、分发、更新、注销和销毁等全生命周期管理操作及加密属性的获取、添加、修改和删除

等操作。

安全密钥生成：密钥管理系统密钥采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的随机数，密钥生成后由 HSM 模块中的系统保护密钥加密后存储。

多种算法密钥管理：支持 SM4、AES、3DES 等对称算法密钥的生成与管理；支持 SM2、RSA、ECDSA 等非对称算法密钥的生成与管理；支持 HMAC-SM3、HMAC-SHA1 等密钥的生成与管理。

密钥安全下发：客户端业务系统密钥获取操作支持 SSL 数字证书、密钥用户名和口令及 wrapping key 等多种认证及加密方式，几种方式可灵活组合配置。保证敏感信息在经过网络传输过程中的安全性，避免接口通信信息泄露、中间人攻击、重放攻击等可能性。

丰富开发接口：支持 KMIP 和 REST 密钥管理接口，同时支持 GM/T 0018 密码设备应用接口规范、JCE、PKCS#11 和 REST 等密码运算标准接口。

安全密钥运算：对于应用系统的敏感数据加密和签名等密码运算操作，可指定密钥名称通过密钥管理系统完成密码运算，密钥管理系统中的密钥不会暴露在系统之外，保证密钥的安全性。

服务管理：可创建多个密钥管理服务和密码运算服务，并为每个服务指定自定义端口，是否开启白名单认证，是否启用 SSL 通信和是否认证客户端证书等灵活控制。

备份/恢复：支持对用户加密对象及系统配置等重要数据的备份/恢复机制，系统管理员可方便的在 Web 管理控制台完成系统备份操作，

可下载或配置自动导出到备份服务器进行妥善保存。

分布式部署：密钥管理系统既可以在一个数据中心独立部署，也可以同时部署在不同的数据中心，多个密钥管理系统之间可通过安全协议同步密钥数据，实现多节点共同协作。

安全简便的 Web 管理：通过密钥管理系统的 Web 管理控制台，系统管理员可以方便的管理系统和系统中的密钥保护策略，Web 管理为 Https 链接，有效保证系统安全。

支持的三方业务系统：支持多种类型及平台的业务系统透明数据加密及密钥管理，如下表所示：

数据库加密	MySQL、Oracle、SQLServer、DB2
大数据平台加密	Apache Hadoop
存储服务器加密	Windows&Linux 文件系统加密； Windows&Linux 磁盘加密； NAS、SAN、GPFS 网络文件系统加密； NetAPP 存储加密。
虚拟服务器加密	Vsphere、Openstack

14.3 设备拓扑示意

密钥管理系统旁路部署通过 API 接口调用，支持单机、集群部署。集群部署可提高密码运算性能，增强设备冗余，集群中密钥管理系统故障时，可不影响业务系统正常运行。

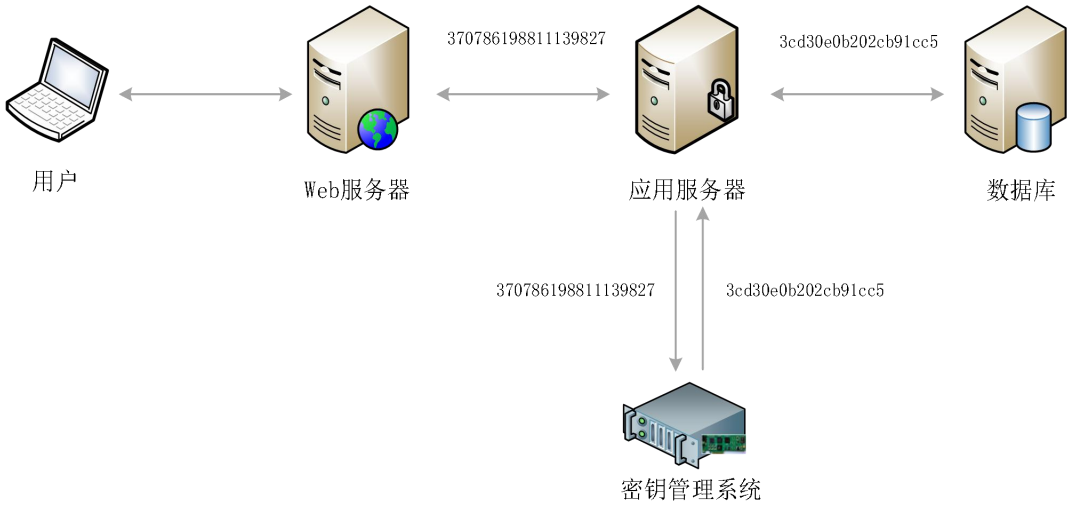

图 3.15 密钥管理系统部署方式

15、 签名验签系统

15.1 设备介绍

签名验签系统为网络交易使用者提供基于 PKI 体系架构和数字证书支持的电子签名解决方案。在电子政务活动中，为关键业务提供数据私密性保护、防篡改、抗抵赖的综合安全能力。可提供多种格式的数字签名验签功能（PKCS#1、PKCS#7 Attach/Detach、XML 等）；实现文件的签名验签功能；数字信封的加解密操作；数据和信息的完整性校验功能；提供证书有效性验证；

15.2 设备功能

签名验签系统具有如下主要功能：

多应用支持：签名验签系统可支持不同应用的证书及对应密钥的生成及存储；

多信任域支持：支持配置不同的证书信任域，证书验证策略支持配置不验证、根证书、CRL、OCSP 等多种验证策略；

数字签名/验证：签名验签系统可提供基于 SM2、RSA 等算法的

PKCS#1 签名/验证、PKCS#7 Attached 签名/验证、P7 Detached 签名/验证功能；签名格式符合 PKCS#7、GM/T0010 等标准中定义的数据类型；

数字信封加密和解密：签名验签系统可提供基于 SM2、RSA 等算法的数字信封加密、解密功能，数字信封格式符合 PKCS#7、GM/T0010 等标准中定义的数据类型；

带签名的数字信封加密和解密：签名验签系统可提供基于 SM2、RSA 等算法的带签名的数字信封加密、解密功能，数字信封格式符合 PKCS#7、GM/T0010 等标准中定义的数据类型。

15.3 设备拓扑示意

签名验签系统旁路部署通过 API 接口调用，支持单机、集群部署。集群部署可提高密码运算性能，增强设备冗余，集群中的签名验签系统故障时，可不影响业务系统正常运行。

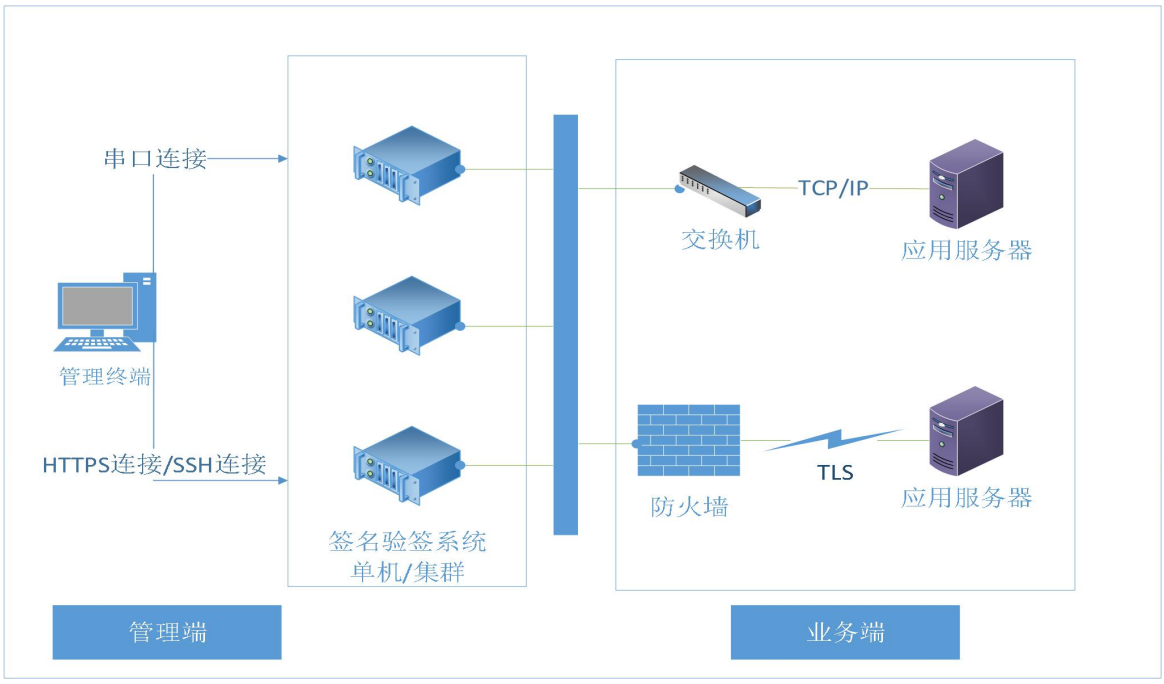

图 3.16 签名验签系统部署方式

16、 态势感知系统

16.1 设备介绍

态势感知系统通常是集合了防病毒软件、防火墙、入侵监测系统、安全审计系统等多个数据信息系统，将这些系统整合起来，对目前的整个网络威胁情况进行评估，以及预测未来的变化趋势。

16.2 设备功能

态势感知系统主要分为四个部分：数据采集、特征提取、态势评估、安全预警。

数据采集：就是对当前整个网络状态进行数据提取，包括网站安全日志、漏洞数据库、恶意代码数据库等多个数据进行统筹整理，一般各个厂家都会有自己对应的信息数据库。

特征提取：通过第一步收集了大量的数据之后，从这些数据中提取有用的数据进行相应的预处理工作，为后面接下来的工作做好数据准备。数据采集和特征提取都是整个网络安全态势感知系统的最底层，数据准备工作。

态势评估：态势评估主要是通过对关联事件进行数据融合处理，从时间、空间、协议等多个方面进行关联识别。简单来说，就是结合数据信息、对当前的时间进行危险评估、判断危险等级。

安全预警：在通过了上面的几个步骤提取了大量的网络状态数据之后，系统就会根据指定的标准对目前的网络状态以及未来的网络状态进行评估和预测，进而给出相应的分析报告和安全状态预警处理。

16.3 设备拓扑示意

部署在安全管理区组成独立的安全管理网络，不会影响用户业务网络和其他网段。

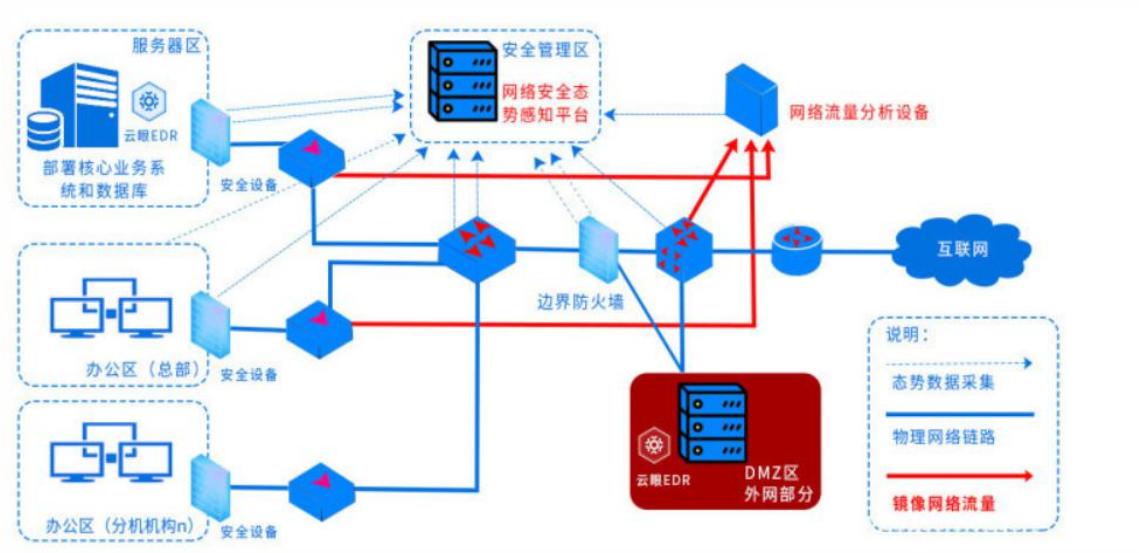

图 3.17 态势感知设备部署方式

17、 网管平台设备

17.1 设备介绍

网管平台(网络管理平台)设备是进行网络管理所需要的设备，其配置应满足网络管理的所有要求，网络管理系统设备包括各节点的网管单元以及网络管理中心的设备和相应的软件，可以在工业环境中对网络进行规划、控制和监视，可以确保网络的正常运行。

17.2 设备功能

集中化管理

多设备类型管理：服务器、存储、网络、WLAN、GPON、摄像头等多种设备类型统一管理。

一体化设备管理：设备信息、告警、关键 KPI、硬件部件等信息集成呈现。

统一平台按需构建：统一的资源管理、告警监控、性能监控和报表分析平台。

可视化监控

多维度监控：告警面板、性能分析、全网拓扑视图，实时感知设备故障。

场景化监控：场景化 DASHBOARD 和大屏监控，全方位掌握 ICT 系统状态。

E2E 故障监控：网络质量诊断、视频质量诊断技术等故障诊断工具。

智能化分析

自定义报表：拖曳式报表定义工具，所见即所得，无需二次开发。

开箱即用：固化运维经验，预置资源、告警、性能等常用报表，满足日常所需。

自助式数据分析：同比、环比、TopN、分类汇总统计等分析方法；柱状图、饼图、曲线图等丰富的图形展示。

17.3 设备拓扑示意

部署在安全管理区组成独立的安全管理网络，不会影响用户业务网络和其他网段。

图 3.18 网管平台设备部署方式

第四部分：高频漏洞预防与处置

依据近年来国家、部、省各类预警通报，本手册整理了常见的漏洞，供各单位举一反三，做好网络安全的加固，同时为相关问题的预防和处置提供参考。

1、XSS 漏洞处置方案

1.1 事件描述

跨站脚本攻击（XSS）对于反射和 DOM 的影响是中等的，而对于存储的 XSS，XSS 的 影响更为严重，譬如在受攻击者的 浏览器上执行远程代码，例如：窃 取凭证和会话或传递恶意软件等.

跨站脚本攻击（XSS）大致分为以下类型：

(1) 反射式 XSS：应用程序或 API 包括未经验证和未经转义的用户输入， 作为 HTML 输出的一部分。一个成功的攻击可以让攻击者在受害者 的浏览器中执行任意的 HTML 和 JavaScript。通常，用户将需要与指 向攻击者控制页面的某些恶意链接进行交互，例如恶意漏洞网站， 广告或类似内容。

(2) 存储式 XSS:应用或者 API 将未净化的用户输入存储下来了，并在后期在其他用户或者管理员的页面展示出来。存储型 XSS 一般被认为是高危或严重的风险。

(3) 基于 DOM 的 XSS：会动态的将攻击者可控的内容加入页面的 JavaScript 框架、单页面程序或 API 存在这种类型的漏洞。理想的 来说，你应该避免将攻击者可控的数据发送给不安全的 JavaScript API。

1.2 XSS 攻击分类与原理

XSS 攻击主要分为两大类：一类是来自内部的攻击、一类是来自

外部的攻击；内部的攻击主要是利用 web 程序自身的漏洞，提供特殊的字符串，从而使得跨站页面直接存在于被供给站点上，这个字符串被称之为跨站语句；这一类攻击所利用的漏洞非常类似于 SQL Injection 漏洞，都是由于 程序开发者没有对用户输入做充分的检查和过滤造成的；外部的攻击主要是指自己构造 XSS 跨站漏洞网页或者寻找非目标机以外的有跨站漏洞的网页；

XSS 常见的攻击手法：

(1)依赖跨站漏洞，需要在被攻击网站额页面种入脚本的手法，例如：cookie 盗取，通过 javascript 获取被攻击网站种下的 cookie，并发送给攻击者；ajax 信息盗取，通过 javaScript 发起 ajax 请求；

(2)不依赖跨站漏洞的手法，例如：单向 http 动作，通过 img.src 等方法发起跨站访问，冒充被攻击者执行特权操作，但是这种方式很难拿到服务器的返回值；双向的 http 动作，如果服务器产生一段动态的 script ，那么可以用 script.src 的方法访问并拿到服务器的返回值；

1.3 预防措施

在开发一个服务的功能点接口时，对用户输入的参数进行过滤，对输入到 HTML 的数据进行编码，也就是对用户提交的所有内容进行过滤，对 url 中的参数进行过滤，过滤掉会导致脚本执行的相关内容；然后对动态输出到页面的内容进行 html 编码，以防万一可进行黑名单方式过滤掉字符如：”、’、>、<、script、onerror、src、

javascript、onload、expression 等危险的字符词汇特征。建议在系统或者正式上线前，先在测试环境上线，做实验测试，等功能安全完善，发现没有其他问题后再上线正式环境，同时在各个安全设备都把该应用接口配置策略做防护监测。

1.4 应急准备

- ◆ 防火墙设备
- ◆ 应用主机综合安全防护软件
- ◆ 入侵检测系统

1.5 监测预警

主要通过部署的防火墙设备、应用主机综合安全防护软件与入侵检测系统进行检测防护，执行日常安全维护、作业计划检查、日常安全工单、安全预警公告、用户投诉等手段进行安全事件发现和检测。

1.6 事件处理

对于不同的攻击特征，应采取相应的处理措施，因此首先应该定位攻击的特征，保证后续处理措施的有效性：

1.6.1 攻击判断

现象一：查看流量是否存下恶意的 JS 代码

现象二：流量是否存在一些与业务无关的相关字符

1.6.2 处置

（1）定期扫描

定期扫描现在持有的网站，彻查可能存在的安全漏洞，对新出现的漏洞进行及时清理。

（2）过滤无用输入字符

在防火墙和入侵检测系统做测率过滤对一些无关业务的字符和一些危险的 js 代码做字符过滤和检测。

1.6.3 恢复

对存在漏洞的接口做防火墙策略或者代码层防护修补，修复完接口可恢复正常的业务应用。

1.7 事件上报

事件处理完成后，应形成安全事件的应急处理分析报告，上报给相关主管部门，具体上报机制参考《江苏省交通运输厅网络安全事件应急预案》。

2、SQL 漏洞处置方案

2.1 事件描述

数据库注入攻击（SQL 注入）即是指 web 应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在 web 应用程序中事先定义好的查询语句的结尾上添加额外的 SQL 语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

数据库注入攻击（SQL 注入）大致分为以下类型：

(1) 基于布尔的盲注::：因为web 的页面返回值都是 True 或者 False，所以布尔盲注就是注入后根据页面返回值来得到数据库信息的一种办法。

(2) 基于时间的盲注：当布尔型注入没有结果（页面显示正常）的时候，很难判断注入的代码是否被执行。基于时间的盲注便应运而生，所谓基于时间的盲注，根据 web 页面相应的时间差来判断该页面是否存在 SQL 注入点。

(3) 联合查询注入：使用联合查询进行注入的前提是要进行注入的页面必须有显示位。所谓联合查询注入即是使用 union 合并两个或多个 SELECT 语句的结果集,所以两个及以上的 select 必须有相同列、且各列的数据类型也都相同。联合查询注入可在链接最后添加 order by 9 基于随意数字的注入，根据页面的返回结果来判断站点中的字段数目。

(4) 基于错误信息的注入：此方法是在页面没有显示位，但是 echo mysql_error();函数输出了错误信息的时候方能使用。优点是注入速度快,缺点是语句较为复杂,而且只能用 limit 依次进行猜解。总体来说，报错注入其实是一种公式化的注入方法，主要用于在页面中没有显示位,但是用 echo mysql_error();输出了错误信息时使用。

2.2 SQL 攻击分类与原理

SQL 注入攻击是通过操作输入来修改 SQL 语句，用以达到执行代码对 WEB 服务器进行攻击的方法。简单的说就是在 post/getweb 表单、输入域名或页面请求的查询字符串中插入 SQL 命令，最终使 web 服务

器执行恶意命令的过程。可以通过一个例子简单说明 SQL 注入攻击。假设某网站页面显示时 URL 为 http://www.example.com?test=123，此时 URL 实际向服务器传递了值为 123 的变量 test，这表明当前页面是对数据库进行动态查询的结果。由此，可以在 URL 中插入恶意的 SQL 语句并进行执行。另外，在网站开发过程中，开发人员使用动态字符串构造 SQL 语句，用来创建所需的应用，这种情况下 SQL 语句在程序的执行过程中被动态的构造使用，可以根据不同的条件产生不同的 SQL 语句，比如需要根据不同的要求来查询数据库中的字段。这样的开发过程其实为 SQL 注入攻击留下了很多的可乘之机。

SQL 常见的攻击手法：

（1）数字型注入：

当输入的参数为整型时，如 ID、年龄、页码等，如果存在注入漏洞，则可以认为是数字型注入。这种数字型注入最多出现在 ASP、PHP 等弱类型语言中，弱类型语言会自动推导变量类型，例如，参数 id=8，PHP 会自动推导变量 id 的数据类型为 int 类型，那么 id=8 and 1=1，则会推导为 string 类型，这是弱类型语言的特性。而对于 Java、C#这类强类型语言，如果试图把一个字符串转换为 int 类型，则会抛出异常，无法继续执行。所以，强类型的语言很少存在数字型注入漏洞。

（2）字符型注入：

当输入参数为字符串时，称为字符型。数字型与字符型注入最大的区别在于：数字型不需要单引号闭合，而字符串类型一般要使用单

引号来闭合。

2.3 预防措施

在编写需要操作数据库的接口，对接口使用预编译的 sql 语句，sql 语句的语意不会发生改变。在参数输入过程中检查数据的输入类型比如用户在输入邮箱时，必须严格按照邮箱的格式；输入时间、日期时，必须严格按照时间、日期的格式等等，以防万一可进行黑名单方式过滤掉字符如：and、or、select、from、union、updatexml、where、order、 sleep、&、&&、|、||等词汇特征，在设置数据库时给数据库的权限分配尽量低权限。在系统或接口正式上线前，先在测试环境上线并做实验测试，等功能安全完善，发现没有其他问题后再上线正式环境，在上线正式环境后应在各个安全设备都把该应用接口配置策略做防护监测。

2.4 应急准备

- ◆ 防火墙设备
- ◆ 应用主机综合安全防护软件
- ◆ 入侵检测系统

2.5 监测预警

主要通过部署的防火墙设备、应用主机综合安全防护软件与入侵检测系统进行检测防护，执行日常安全维护、作业计划检查、日常安全工单、安全预警公告、用户投诉等手段进行安全事件发现和检测。

2.6 事件处理

对于不同的攻击特征，应采取相应的处理措施，因此首先应该定位攻击的特征，保证后续处理措施的有效性：

2.6.1 攻击判断

现象一：查看流量是否存下恶意的SQL语句代码

现象二：流量是否存在一些与业务无关的相关SQL命令字符

2.6.2 处置

（1）定期扫描

定期扫描现在持有的网站，彻查可能存在的安全漏洞，对新出现的漏洞进行及时清理。

（2）过滤无用输入字符

在防火墙和入侵检测系统做策略过滤对一些无关业务的字符和一些危险的SQL语句代码做字符过滤和检测。

2.6.3 恢复

对存在漏洞的接口做防火墙策略或者代码层防护修补，修复完接口可恢复正常的业务应用。

2.7 事件上报

事件处理完成后，应形成安全事件的应急处理分析报告，上报给相关主管部门，具体上报机制参考《江苏省交通运输厅网络安全事件应急预案》。

3、弱口令处置方案

3.1 事件描述

弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，由于这样的口令很容易被破解，从而使用户的互联网账号受到他人控制，因此不推荐用户使用。

弱口令一般分为两种：

（1）某些网站搭建好后会默认设置一些账号密码，由于管理员没有修改更正默认的密码导致的弱口令

（2）由于用户个人的原因导致的弱口令。

3.2 弱口令攻击分类与原理

弱口令攻漏洞与个人习惯相关与意识相关，为了避免忘记密码，使用一个非常容易记住的密码，或者是直接采用系统的默认密码等，需要加强相关的网络安全意识。

3.3 预防措施

在开发系统的登陆页面时，提示用户设置强密码，不允许用户设置只有数字和字符的密码，验证密码复杂度，不然提示密码设置失败密码过于简单，每过一个月用户登陆后强制弹窗提示用户修改密码。

3.4 应急准备

- ◆ 防火墙设备
- ◆ 应用主机综合安全防护软件
- ◆ 主机检测系统

3.5 监测预警

主要通过部署的防火墙设备、应用主机综合安全防护软件与主机检测系统进行检测防护，执行日常安全维护、作业计划检查、日常安全工单、安全预警公告、用户投诉等手段进行安全事件发现和检测。

3.6 事件处理

对于不通的系统和后台根据业务的权重来做相应的后续处理和一些管制方法。

3.6.1 攻击判断

现象一：出现大量的登陆后台或者端口服务的发包流量。

现象二：流量是否存在一些口令简单的发包。

3.6.2处置

（1）定期扫描

定期扫描现在持有的网站，对后台和端口服务的账号做检查查看是否有简单的密码，对新创建的账号密码进行检查检验是否为弱密码。

（2）监测口令数据包

对存在漏洞的接口做防火墙策略或者代码层防护修补，修复完接口可恢复正常的业务应用。

3.6.3 恢复

发现弱口令及时提醒相关管理员修改密码，然后对其服务器进行流量检测是否被利用传马等操作。

3.7 事件上报

事件处理完成后，应形成安全事件的应急处理分析报告，上报给相关主管部门，具体上报机制参考《江苏省交通运输厅网络安全事件应急预案》。

4、任意文件上传处置方案

4.1 事件描述

任意文件上传漏洞是指用户上传了一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。常见场景是 web 服务器允许用户上传图片或者普通文本文件保存，而用户绕过上传机制上

传恶意代码并执行从而控制服务器。显然这种漏洞是 getshell 最快最直接的方法之一，需要说明的是上传文件操作本身是没有问题的，问题在于文件上传到服务器后，服务器怎么处理和解释文件。

4.2 文件上传分类与原理

Web 应用程序通常会有文件上传的功能,例如在 BBS 发布图片,在个人网站发布 ZIP 压缩包,在办公平台发布 DOC 文件等,只要 Web 应用程序允许上传文件,就有可能存在文件上传漏洞。

大部分文件上传漏洞的产生是因为 Web 应用程序没有对上传文件的格式进行严格过滤,还有一部分是攻击者通过 Web 服务器的解析漏洞来突破 Web 应用程序的防护：

请求抓包上传 php 文件时，Content-Type 值是 application/octer-stream，上传 jpg 格式的文件时 Content-Type 值是 image/jpeg，可以修改文件类型进行绕过。在脚本文件开头补充图片对应的头部值，或在图片后写入写入脚本代码，将文件名后面直接加上%00.jpg，先绕过后缀上传，然后利用 burp 的 urldecode 功能，其实和/00 截断将 hex20 变成 00

4.3 预防措施

在开发需要上传文件的接口时，在判断文件类型时，可以结合使用 MIME Type、后缀检查等方式。在文件类型检查中，推荐白名单方式,黑名单的方式容易被其他方式手段绕过。此外，对于图片的处理，可以使用压缩函数或者 resize 函数，在处理图片的同时破坏图片中可能包含的 HTML 代码，或者在使用白名单的时候，使用分割字符串

(上传来的文件名)，使用″.″来分割，仅允许分割后，字符串只有两个，一个是文件名，一个是文件扩展名，在上传文件后不返回上传的文件路径，并随机数修改文件名，在条件允许的条件下将上传的图片重新保存为一个新的图片，将图片内容二次渲染把里面可能含有的的可执行代码删除，部署可以把网站服务器和文件服务器分开，但是要保证，文件服务器的安全级别很高，且保证上传文件是相对高的可靠，直接把上传的图片等文件存储在文件服务器，并在文件服务器把所有目录设置为可读可写不可执行，在系统或接口正式上线前，先在测试环境上线，做实验测试，等功能安全完善，发现没有其他问题后在上线正式环境，在上线正式环境后应在各个安全设备都把该应用接口配置策略做防护监测。

4.4 应急准备

- ◆ 防火墙设备
- ◆ 应用主机综合安全防护软件
- ◆ 入侵检测系统

4.5 监测预警

主要通过部署的防火墙设备、应用主机综合安全防护软件与入侵检测系统进行检测防护，执行日常安全维护、作业计划检查、日常安全工单、安全预警公告、用户投诉等手段进行安全事件发现和检测。

4.6 事件处理

验证木马是否上传成功对照流量的特征找到对应的相关文件上传点存放位置，查看相关位置是否存在恶意文件木马，根据文件是否存在危害来判断是否要做后续的排查工作。

4.6.1 攻击判断

现象一：查看流量看是否存在不符合上传点对应的后缀是否存在大量脏字符。

现象二：流量中是否存在一些和网站搭建相关的语言代码。

4.6.2 处置

（1）定期扫描

定期扫描现在持有的网站，对网站的上传点进行扫描查看是否存在绕过的可能性。

（2）过滤无用输入字符

在防火墙和入侵检测系统做策略过滤一些与业务无关的字符和一些危险的开发语言语句代码做字符过滤和对上传文件的后缀检测。

4.6.3 恢复

对存在漏洞的接口做防火墙策略或者代码层防护修补，修复完接口可恢复正常的业务应用。

4.7 事件上报

事件处理完成后，应形成安全事件的应急处理分析报告，上报给相关主管部门，具体上报机制参考《江苏省交通运输厅网络安全事件应急预案》。

5、未授权访问漏洞处置方案

5.1 事件描述

未授权访问可以理解为需要安全配置或权限认证的地址、授权页面存在缺陷，导致其他用户可以直接访问，从而引发重要权限可被操作、数据库、网站目录等敏感信息泄露。

目前主要存在未授权访问漏洞的有:NFS 服务,Samba 服务,LDAP，Rsync， FTP， GitLab， Jenkins， MongoDB， Redis， ZooKeeper，ElasticSearch，Memcache，CouchDB，Docker，Solr，Hadoop，Dubbo等

5.2 未授权访问分类与原理

Web 服务器会有很多的接口和端口服务，当开发网页的人员对代码编写的不够严格时就可能存在接口的未授权访问，未授权访问更多的时开发员的马虎导致的，使其对功能点接口的访问没有严格的把控用户的权限访问，导致某些功能没有在理想状态下被不法分子利用产生的漏洞，端口服务造成的未授权则是服务器的运维人员在对服务器管理没有合理给端口服务的配置文件设置好用户的访问权限或者把一些危险端口对外映射导致的未授权漏洞。

5.3 预防措施

在开发阶段对每一个接口做好应用访问权限控制，和对系统的访问控制权限，对各个系统和应用授权以及授权之后可以做的操作，对各个用户分配单独的应用权限功能，在系统或接口正式上线前，先在测试环境上线，做实验测试，等功能安全完善，发现没有其他问题后

再上线正式环境，在上线正式环境后应在各个安全设备都把该应用接口配置策略做防护监测。

5.4 应急准备

- ◆ 防火墙设备
- ◆ 应用主机综合安全防护软件
- ◆ 入侵检测系统

5.5 监测预警

主要通过部署的防火墙设备、入侵检测系统、应用主机综合安全防护软件与漏扫检测系统进行检测防护，执行日常安全维护、作业计划检查、日常安全工单、安全预警公告、用户投诉等手段进行安全事件发现和检测。

5.6 事件处理

验证未授权的系统是服务还是某个 API 接口,服务的未授权可能配置文件没有正确配置或者允许游客访问导致的该问题。再对服务器进行排查看是否有后门木马根据流量分析和漏扫检测进行检查后无问题修改配置文件禁止游客或空口令访问即可，框架 API 接口的为首可能是未对接口进行身份验证核查导致的。检查接口看接口是存在信息泄露还是命令执行，如是命令执行应对服务器进行后门木马检测可用流量分析和漏扫检测进行检查，后续对接口进行身份验证即可。

5.6.1 攻击判断

现象一：通过应用主机综合安全防护软件查看查看是否存在没有 cooKie 的情况下就查看一些功能的列表的流量。

现象二：查看 url 的目录路径是否是网上一些框架存在的信息泄露或未授权的页面地址。

5.6.2 处置

（1）定期扫描现在持有的网站，对服务进行扫描查看是否存在未授权可以访问的服务，通过扫描查看网站是否存在框架自带的未授权的框架文件。

（2）过滤危险目录。在防火墙和入侵检测系统做策略过滤一些无关业务的目录文件。

5.6.3 恢复

对存在漏洞的接口在代码层做身份验证，未授权的服务在配置文件修改为需身份验证访问，修复完接口可恢复正常的业务应用。

5.7　事件上报

事件处理完成后，应形成安全事件的应急处理分析报告，上报给相关主管部门，具体上报机制参考《江苏省交通运输厅网络安全事件应急预案》。

6、反序列化远程代码执行漏洞处置方案

6.1 事件描述

反序列化漏洞就是指黑客序列化一个包含恶意代码的实例对象（通常是 Runtime.exec 来执行后台命令），此时会得到对象的字节数据。然后字节数据通过接口发送到服务端（被攻击的服务器）。服务器在反序列化出对象的过程中（readObject 方法里面）就会触发触发恶意代码执行，从而达到攻击的目的。

6.2 反序列化远程代码执行漏洞分类与原理

程序应用对用户输入，即不可信数据做了反序列化处理，那么攻击者可以通过构造恶意输入，让反序列化产生非预期的对象，非预期的对象在产生过程中就有可能带来任意代码执行。

6.3 预防措施

在设计反序列化接口时严格控制接口参数的数据，不允许用户控制控制反序列化的数据参数，在系统或接口正式上线前，先在测试环境上线，做实验测试，等功能安全完善，发现没有其他问题后再上线正式环境，在上线正式环境后应在各个安全设备都把该应用接口配置策略做防护监测。

6.4 应急准备

安全保障

- ◆ 防火墙设备
- ◆ 应用主机综合安全防护软件
- ◆ 漏扫检测系统
- ◆ 入侵检测系统

6.5 监测预警

主要通过部署的防火墙设备、入侵检测系统、应用主机综合安全防护软件与漏扫检测系统进行检测防护，执行日常安全维护、作业计划检查、日常安全工单、安全预警公告、用户投诉等手段进行安全事件发现和检测。

6.6 事件处理

对数据包进行验证，查看该数据是否为真实成功的攻击，假如攻击成功，对攻击成功的服务器进行隔离禁止后续操作，对该服务器的所有流量进程查看，看是否对其他服务器进行一个内网攻击，对被攻击成功的服务器进行主机扫描查看是否被上传隐藏的木马程序，查看用户和任务计划查看是否存在攻击留有后续拿下服务器手段，清除完毕后，找到对应反序列话参数，进行修复。

6.6.1 攻击判断

现象一：通过应用主机综合安全防护软件查看查看数据宝里是否存在不属于业务的一些特殊参数。

现象二：查看传参中是否存在一些Java,Php,Python等编成语言的命令。

6.6.2 处置

1、定期扫描

定期扫描现在持有的网站，对服务进行扫描查看是否存在反序列话漏洞。

2、过滤危险字符

在防火墙和入侵检测系统做策略过滤一些无关业务的字符禁止用户传输代码命令在数据中。

6.6.3 恢复

对存在反序列话漏洞的参数做过滤验证不要把用户的输入或者是用户可控的参数直接放进反序列化的操作中去，参数的代码过滤严谨后恢复正常的业务应用。

6.7 事件上报

事件处理完成后，应形成安全事件的应急处理分析报告，上报给相关主管部门，具体上报机制参考《江苏省交通运输厅网络安全事件应急预案》。

7、信息泄露处置方案

7.1 事件描述

信息泄露包括的内容很广泛,很多漏洞都可以归为信息泄露类的漏洞，当网站泄露了敏感的用户或业务数据或者泄露了在理想状态下不是需要给用户知道的一些信息。

7.2 信息泄露分类与原理

由于后台人员的疏忽或者不当的设计，导致不应该被前端用户看到的数据被轻易的访问到。

比如：通过访问 url 下的目录，可以直接列出目录下的文件列表：输入错误的 url 参数后报错信息里面包含操作系统、中间件、开发语言的版本或其他信息：前端的源码（html,css,js）里面包含了敏感信息，比如后台登录地址、内网接口信息、甚至账号密码等：某个接口泄露了用户的个人信息等。

7.3 预防措施

在开发时写入 robots.txt, sitemap.xml 这些文件，这些文件列出特定目录不让爬虫爬取，配置好服务的配置文件禁止游客访问或者目录无权限访问，在系统或接口正式上线前，先在测试环境上线，做实验测试，等功能安全完善，发现没有其他问题后在上线正式环境，在上线正式环境后应在各个安全设备都把该应用接口配置策略做防护监测。

7.4 应急准备

- ◆ 防火墙设备
- ◆ 应用主机综合安全防护软件
- ◆ 漏扫检测系统

7.5 监测预警

主要通过部署的防火墙设备、应用主机综合安全防护软件与漏扫检测系统进行检测防护，执行日常安全维护、作业计划检查、日常安全工单、安全预警公告、用户投诉等手段进行安全事件发现和检测。

7.6 事件处理

对数据包进行验证，查看该数据里的内容是否真实泄露了内部或者用户信息。找到对应的数据接口或者目录文件，对数据接口进行加敏处理，对目录文件在配置文件中修改为禁止访问。

7.6.1 攻击判断

现象一：通过应用主机综合安全防护软件查看查看是否存在敏敏感信息。

现象二：查看url是否存在访问一些奇怪的文件做读取操作。

7.6.2 处置

1、定期扫描

定期扫描现在持有的网站，对服务进行扫描查看是否存有中间件配置不当导致的信息泄露。

2、监测特殊文件

在防火墙和入侵检测系统对一些不属于业务的文件做监测，防止攻击者扫描敏感文件。

7.6.3 恢复

对存在泄露用户的接口做用户验证，或者敏感数据加敏，对泄露的文件或目录在中间件的配置文件修改配置禁止目录和文件访问权限，修改过后恢复正常的业务应用。。

7.7 事件上报

事件处理完成后，应形成安全事件的应急处理分析报告，上报给相关主管部门，具体上报机制参考《江苏省交通运输厅网络安全事件应急预案》。

网络安全

畅游网络/安全从你我做起

江苏省交通运输厅科技处

江苏省交通通信信息中心

联合编制