紫光集团 | H3C
核心企业 | 数字化解决方案领导者

洪起说等保

2.0

洪起说等保 2.0

新华三集团

北京总部
北京市朝阳区广顺南大街8号院 利星行中心1号楼
邮编:100102

杭州总部
杭州市滨江区长河路466号
邮编:310052

www.h3c.com

CN-173X30-20190702-BR-HZ-V1.0

作者简介

洪起 中原人士

资深安全工程师

公元2015年，新华三参与等保标准编制工作

公元2017年，洪起全程配合公安部参与等保2.0标准的编制工作

洪起 潜心研究各类邪(hei)派(ke)招式，并搜罗玄铁金石铸造神器一件

横眉冷指，剑气如霜

四方宵小望风而遁

与江湖各邪门妖派的交锋中从不失手

洪起为六部督查、地州衙门、钱庄票号、铁匠私塾等名门正派宣讲化解之术，至今未歇

导言

网络安全等级保护已经进入2.0时代，等级保护制度已被打造成新时期国家网络安全的基本国策和基本制度。应急、恢复、预警、监测、综合考核等重点措施全部纳入等保制度并实施，对重要基础设施、重要系统以及“云、物、移、大、工控”纳入等保监管，将互联网企业纳入等级保护管理。

等保2.0与网络安全法的关系：等保2.0标准是国内非涉密信息系统的安全集成标准，网络安全法是作为法律、中国信息安全的基本法。网络安全法中明确提到信息安全建设要遵照等级保护标准。

网络安全法从立法到配套法律法规的确定完善，到市场上反映出来一定的效果是需要过程的。这个过程在于执法是否落实到位，规定的标准是否真的符合业务安全痛点。目前来看市场上大部分单位都以合规性建设为主，事实上我认为网络安全法考虑的非常全面，从立法角度来看，如果一步一步按照法律落实好，是一部非常健全的体系，做好了并不只是能达到合规这个价值层面，而是会使业务的风险管控、网络安全能力会上升到一个新的高度。

等保2.0与等保1.0的不同：从名称上来看，原信息安全等保标准叫做信息安全等级保护制度，现在2.0叫做网络安全等级保护制度。这意味着，等级保护上升到了网络空间安全的层面。这个名称的改变意味着等级保护的对象全面升级：之前保护的对象是计算机信息系统，而现在上升到网络空间安全了，除了包含之前的计算机信息系统，还包含网络安全基础设施、云、移动互联网、物联网、工业控制系统、大数据安全等对象。

目录 CONTENTS

第一回 等保2.0简介

前言

随着网络技术的快速发展，等级保护1.0标准已经不适用于诸如云计算、物联网、移动互联、工业控制系统、大数据系统等新型的网络互联系统，使得这些系统在安全防护上没有可遵循的安全基础标准。因此，公安部牵头组织了等级保护标准的研究修订工作，经过多方面的努力，已经在2017年10月形成新标准的报批稿，并于2018年7月征求了专家意见再次调整。新的标准名称由原来的《信息安全技术　信息系统安全等级保护基本要求》变更为《信息安全技术　网络安全等级保护基本要求》（我们简称等保2.0），与《中华人民共和国网络安全法》保持一致。作为数字化解决方案领导者的新华三，全程配合公安部参与了等保2.0标准的编制工作。

目前新的标准已经发布，为了使大家能够更好的理解新的标准，紫光旗下新华三集团（以下简称“新华三”）安全攻防团队推出“洪起说等保2.0”，希望能对大家有所帮助。

等保2.0标准的编制过程

阶段1	■ 信息安全技术 网络安全等级保护基本要求 第1部分 通用安全要求 ■ 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 ■ 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 ■ 信息安全技术 网络安全等级保护基本要求 第4部分 物联网安全扩展要求 ■ 信息安全技术 网络安全等级保护基本要求 第5部分 工业控制系统安全扩展要求
阶段2	■ 五个部分合并为：信息安全技术 网络安全等级保护基本要求
阶段3	■ 再次调整分类结构，体现一个中心、三重防御；强化可信计算

等级保护新标准最初包含5个部分，在编制过程中总共经历了两次大的变化，第一次是2017年8月根据网信办和公安部的意见将5个分册进行了合并，形成一个标准，并在2017年10月参加信安标委WG5工作组在研标准推进会，介绍合并后的标准送审稿，征求127家成员单位意见，修订完成报批稿；第二次大的变化是2018年7月根据沈昌祥院士的意见再次调整分类结构和强化可信计算，充分体现一个中心，三重防御的思想并强化可信计算安全技术要求的使用。

等保2.0的保护对象

等级保护对象由原来的“信息系统”改为“等级保护对象（网络和信息系统）”，安全等级保护对象包括基础信息网络（广电网、电信网等）、信息系统（采用传统技术的系统）、云计算平台、大数据平台、移动互联、物联网和工业控制系统等。新版安全要求在原有通用安全要求的基础上新增安全扩展要求，安全扩展要求主要针对云计算、移动互联、物联网和工业控制系统提出了特殊安全要求。

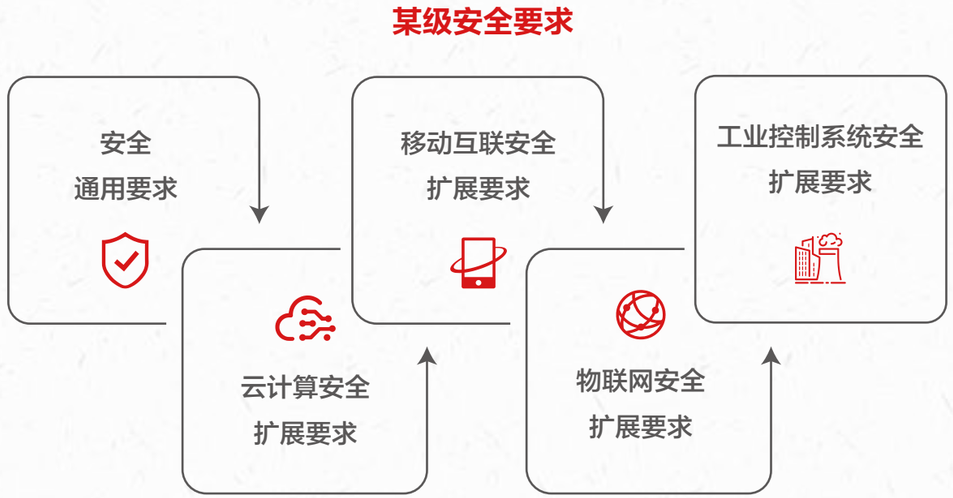
等保2.0标准的章节结构

等保2.0由10个章节8个附录，其中第6、7、8、9、10章为五个安全等级的安全要求章节，8个附录分别为：安全要求的选择和使用、关于等级保护对象整体安全保护能力的要求、等级保护安全框架和关键技术使用要求、云计算应用场景说明、移动互联应用场景说明、物联网应用场景说明、工业控制系统应用场景说明和大数据应用场景说明。

等保2.0标准的章节结构

调整后每一级的安全要求均包括安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求这几个部分。

安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，必须根据安全保护等级实现相应级别的安全通用要求；安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景实现安全扩展要求。



等保2.0标准的控制措施分类结构

■ 等保2.0的控制措施分为技术要求和管理要求两部分：

技术要求“从面到点”提出安全要求，“安全物理环境”主要对机房设施提出要求，“安全通信网络”和“安全区域边界”主要对网络整体提出要求，“安全计算环境”主要对构成节点（包括业务应用和数据）提出要求，“安全管理中心”主要对系统管理、集中管控等提出要求。

管理要求“从元素到活动”提出安全要求，“安全管理制度”、“安全管理机构”和“安全管理人员”主要提出了管理不可缺少的制度、机构和人员三要素，“安全建设管理”及“安全运维管理”主要提出了建设过程和运维过程的安全活动管理要求。

总结

■ 标准名称：

由信息安全等级保护基本要求改为网络安全等级保护基本要求；

■ 保护对象：

由信息系统改为等级保护对象；

■ 章节结构：

分为10个章节8个附录，标准要求包括1个通用4个扩展；

■ 控制措施：

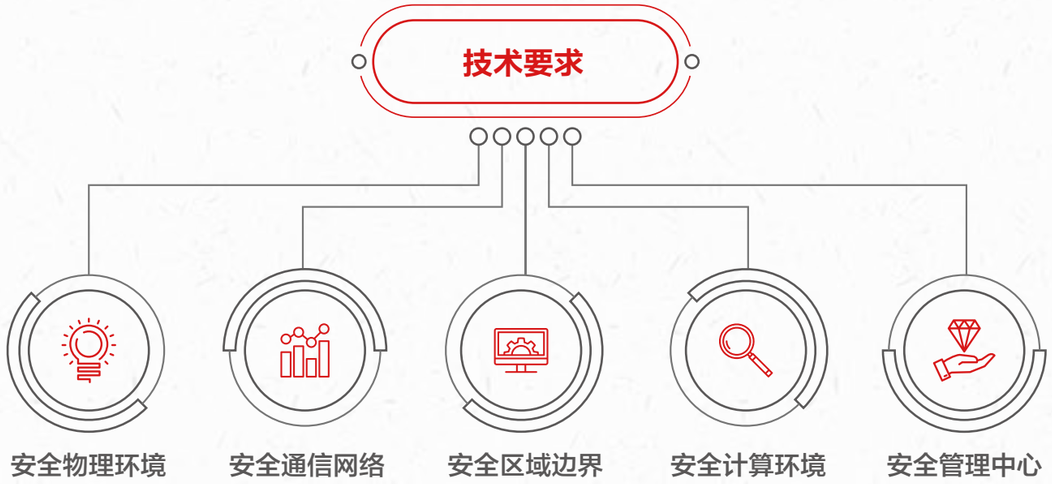
技术要求包括物理环境、通信网络、区域边界、计算环境和管理中心；管理要求包括管理制度、管理机构、管理人员、建设管理和运维管理

第二回

安全通用技术要求

本回内容概述

安全通用要求中的技术要求包括安全物理环境、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五个部分。



安全物理环境

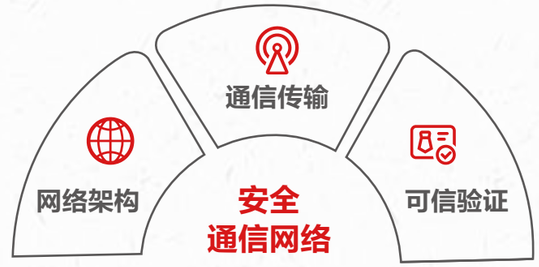
安全物理环境保护要求可概括为：

防震防风防被盗，水火雷电莫小瞧，

合理控制温湿度，电磁屏蔽门禁牢。

这里主要提出对网络机房的物理安全防护，包括机房场地应具有抗震、抗风、抗雨能力；具有防水防潮、防火防雷、防静电、防盗窃和防破坏能力；保障稳定安全的电力供应，同时将温湿度控制在合理范围之内，实施电磁屏蔽措施并配置电子门禁系统控制鉴别来访人员。

安全通信网络



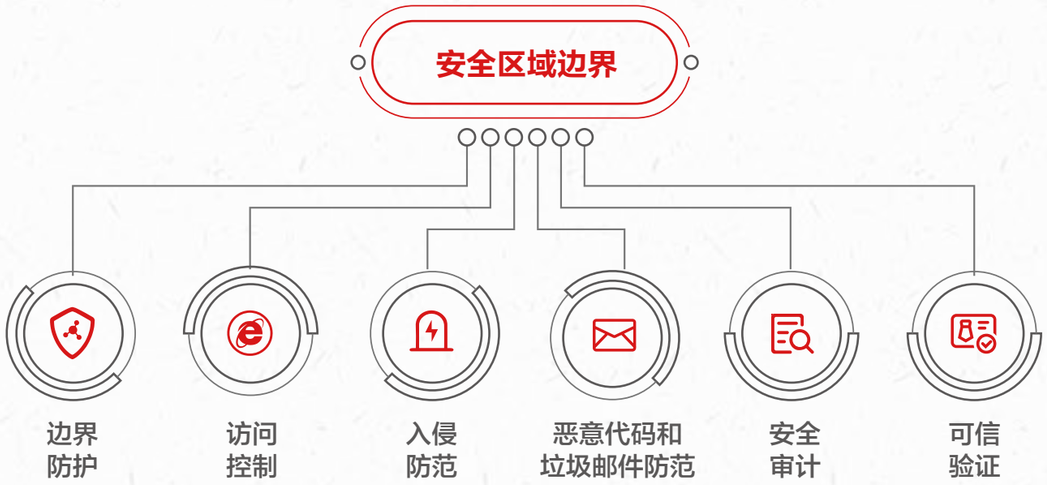
安全通信网络包括网络架构、通信传输和可信验证三个部分。

等保2.0中的网络架构对应等保1.0中的结构安全，主要对网络设备的业务处理能力、网络带宽、网络区域的划分和隔离以及通信线路、关键设备的可用性等提出了要求。H3C SecPath M9000系列是新华三推出的新一代高性能多业务安全网关，全面支持攻击防范、抗DDoS、访问控制、安全域划分等功能，并采用领先的多核全分布式架构，满足网络高可靠性需求。

通信传输对应等保1.0中的通信完整性和通信保密性，要求采用校验技术和密码技术保证通信过程中数据的完整性和保密性，防止通信过程中的数据遭到破坏或泄露；

可信验证为等保2.0新增的建议条款，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，并在应用程序的关键执行环节进行动态可信验证，在检测到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；为了实现可信验证技术，可在关键处理组件芯片上集成硬件电路来检测未经授权的固件修改。新华三可信计算系统是针对网络设备的一套可信解决方案，可满足等保2.0可信验证提出的建议。

安全区域边界



边界防护对应1.0中的边界完整性检查，在原有限制非授权接入及非授权外联行为的基础上，要求跨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，同时增加了无线网络接入使用的限制；

访问控制要求在网络边界或区域间设置访问控制白名单规则，并最小化优化配置访问控制列表，访问控制规则基于五元组控制数据包的进出，同时能够根据会话状态信息控制数据包进出，除此之外，还要求实现基于应用协议和应用内容的访问控制。

H3C 全系列防火墙配合H3C EAD桌面终端安全产品可满足等保2.0对边界防护及访问控制提出的安全要求。

入侵防范要求在关键节点处设置安全检测机制，同时检测和限制来自外部网络和内部发起的网络攻击，并分析和记录网络攻击行为；

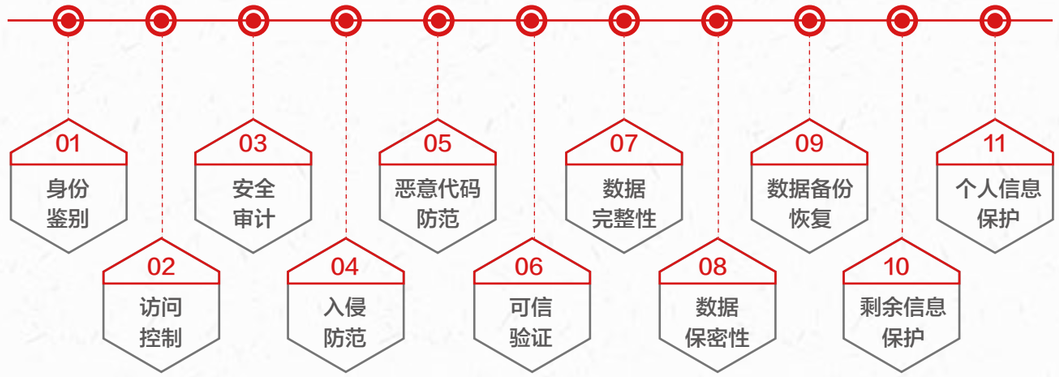
恶意代码和垃圾邮件防范要求在关键节点处部署恶意代码和垃圾邮件防护机制的同时，保持恶意代码库、垃圾邮件库的及时升级和更新；

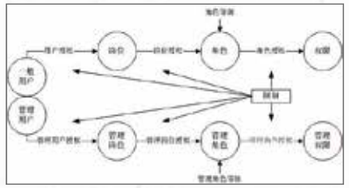
H3C SecPath IPS是业界唯一集成漏洞库、专业病毒库、应用协议库的IPS产品，可满足等保2.0对入侵防范及恶意代码防范要求。

安全审计要求在网络边界、重要网络节点进行，审计要覆盖到每个用户、重要的用户行为及重要安全事件，审计记录应能完整记录事件的必要元素或字段，并对审计记录进行保护，定期备份，避免遭到破坏，对于远程访问用户行为、访问互联网的用户行为等应提供单独审计和分析的能力；H3C SecCenter 安全管理中心集综合日志、网络设备、安全设备、业务应用审计于一体，可满足等保2.0对安全审计提出的要求。

可信验证与安全通信网络中的要求一致，这里不再赘述。

安全计算环境





身份鉴别　　访问控制　　安全审计

身份鉴别要求登录用户身份标识唯一，设置密码复杂度策略和密码周期，通过登录失败阈值设置限制非法登录次数，通过设置会话超时时间结束非活动会话，采用加密等方式进行远程管理，防止鉴别信息被窃听，并要求采用组合鉴别技术对用户进行身份鉴别；

除了组合鉴别技术需要额外使用密码技术产品之外，其它要求均可通过设备或服务器自身的安全策略配置实现。

访问控制用户账户权限分配，默认账户口令修改，多余、过期账户的删除和停用，避免共享账户及设置最小权限，配置细粒度访问控制规则（主体为用户级或进程级，客体为文件、数据库表级）并设置安全标记控制主体和客体的资源访问；

安全标记保护需要引入强制访问控制模型，目前对于windows系统由相应的操作系统加固软件实现，linux系统可通过Selinux来实现，其它自主访问控制要求均可通过系统用户、组权限设定及防火墙的访问控制规则实现。

安全审计要求覆盖到每个用户、重要的用户行为及重要安全事件，审计记录应能完整记录事件的必要元素或字段，对审计记录进行保护，定期备份，避免遭到破坏，并对审计进程进行保护，防止未经授权的中断；

新华三云智- SecCenter CSAP网络安全态势感知平台可完全满足安全审计提出的要求。

入侵防范

恶意代码防范

可信验证

入侵防范要求最小化安装所需的组件和应用程序，关闭不需要的服务、默认共享和高危端口，对通过网络管理的管理终端进行限制，对于人机接口输入或通过通信接口输入的内容要进行有效性检验，过滤非法输入，及时检测发现和修补系统漏洞，并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。

恶意代码防范要求采用防恶意代码产品、技术或通过可信验证机制及时识别并有效阻断入侵和病毒行为。

配置防火墙访问控制规则或部署堡垒机产品并部署H3C SecPath IPS可满足等保2.0对入侵防范和恶意代码防范提出的要求。

可信验证的要求与应对措施与安全通信网络中所说的内容一致，这里不再赘述。

数据完整性

数据保密性

数据备份和恢复

剩余信息保护

个人信息保护

数据完整性和数据保密性要求保障数据在传输和存储过程中不被非法破坏、修改，同时保护数据避免非授权访问，数据完整性保护主要通过校验技术或密码技术来实现，数据保密性主要通过密码技术在数据传输或存储过程中对数据进行加密来实现。

数据备份和恢复要求重要数据本地备份的同时利用通信网络进行实时异地备份，并提供重要数据处理系统的热冗余来保障系统的高可用性。

剩余信息保护要求鉴别信息、敏感数据的存储空间被释放或重新分配前得到完全清除，比如不准许使用系统的“记住密码”等功能，敏感数据存储空间重新分配时要保证其不能通过技术手段恢复已删除的数据。

个人信息保护要求仅采集和保存业务必需的用户个人信息，不准许非授权访问和非法使用用户个人信息。

安全管理中心

安全管理中心为等保2.0新增的控制措施，至此，我们所讲过的通用技术要求已经能充分体现等保2.0“一个中心，三重防御”的思想。所谓“一个中心，三重防御”指的就是建立以**“安全管理中心”**为核心的整体安全保障体系，**“安全通信网络”**主要对网络整体的安全防护提出安全要求 **“安全区域边界”**主要对网络边界和区域边界提出安全防护要求；**“安全计算环境”**主要对构成节点（包括业务应用和数据）提出安全防护要求。

安全管理中心包括系统管理、审计管理、安全管理和集中管控这四部分内容。

安全管理中心中的系统管理要求对系统管理员进行身份鉴别，对其操作方式进行限定，并对其操作行为进行审计，对安全管理中心系统资源和运行的配置、控制和管理应由系统管理员完成，其它用户不能授予以上权限。

审计管理要求对审计管理员进行身份鉴别，对其操作方式进行限定，并对其操作行为进行审计，对审计记录的分析、处理、存储、管理和查询等由审计管理员完成，其它用户不能授予以上权限。

安全管理要求对安全管理员进行身份鉴别，对其操作方式进行限定，并对其操作行为进行审计，安全管理中心的安全策略应由安全管理员进行配置，其它用户不具备配置操作权限。

系统管理员、审计管理员与安全管理员各司其职，这就是我们常说的三权分立思想。

集中管控要求对安全设备或安全组件进行管控时，应划分出特定的管理区域并建立安全的传输路径，对链路、设备和服务器等运行状况进行集中监测，对审计数据进行汇总和集中分析，对安全策略、恶意代码、补丁升级等事项进行集中管理，同时能对网络中发生的各类安全事件进行识别、报警和分析。

总结

■ 安全物理环境：

主要对网络机房在选址、设计、建设、使用时提出安全要求；

■ 安全通信网络：

主要对网络架构设计、通信传输保护和可信验证提出安全要求或建议；

■ 安全区域边界：

主要对边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计和可信验证提出安全要求或建议；

■ 安全计算环境：

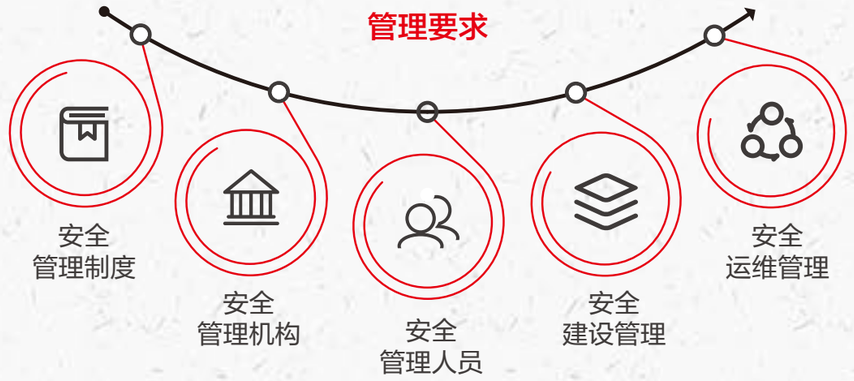
主要对构成节点（包括业务应用和数据）提出要求；

■ 安全管理中心：

安全管理中心主要对系统管理、审计管理、安全管理和集中管控提出要求；

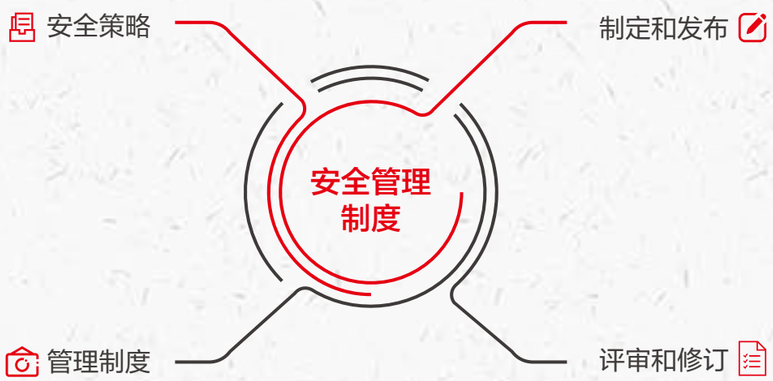
第三回 安全通用管理要求

本回内容概述



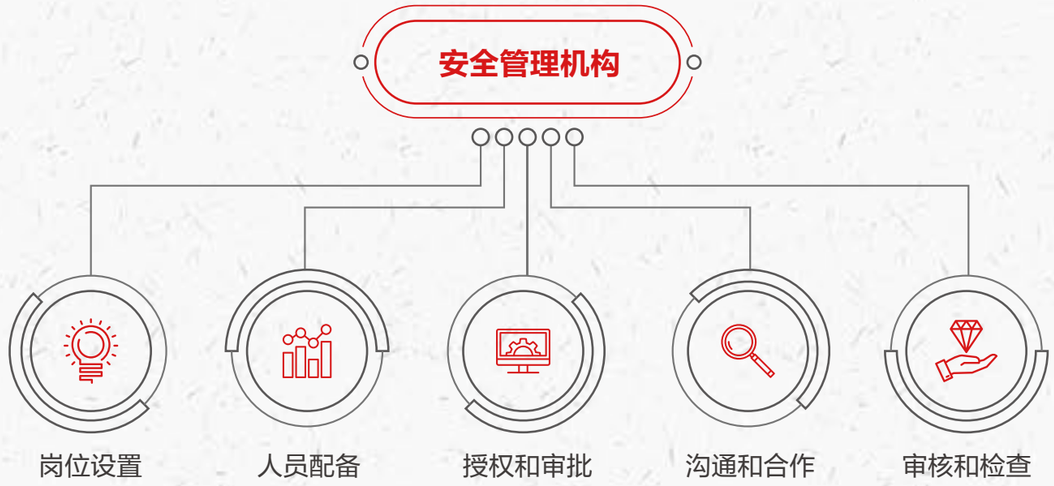
安全管理要求包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理这五个部分的内容。

安全管理制度



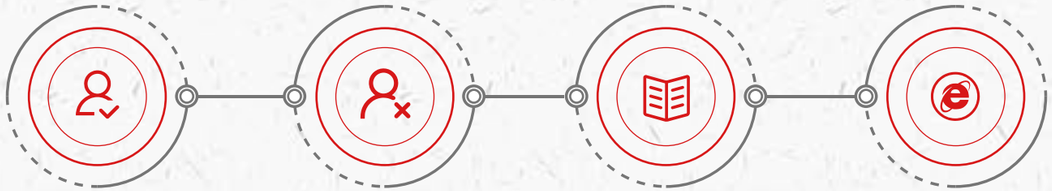
安全管理制度包括安全策略、管理制度、制定和发布、评审和修订。要求制定制定网络安全工作的总体方针和安全策略，并对安全管理活动建立安全管理制度，同时对管理操作建立操作规程，通过表单记录安全管理活动，形成由安全策略、管理制度、操作规程记录表单等构成的全面的安全管理制度体系。安全管理制度的制定由专门的部门或人员负责，并通过正式有效的方式发布，并进行版本控制。定期对安全管理制度的合理性和实用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

安全管理机构



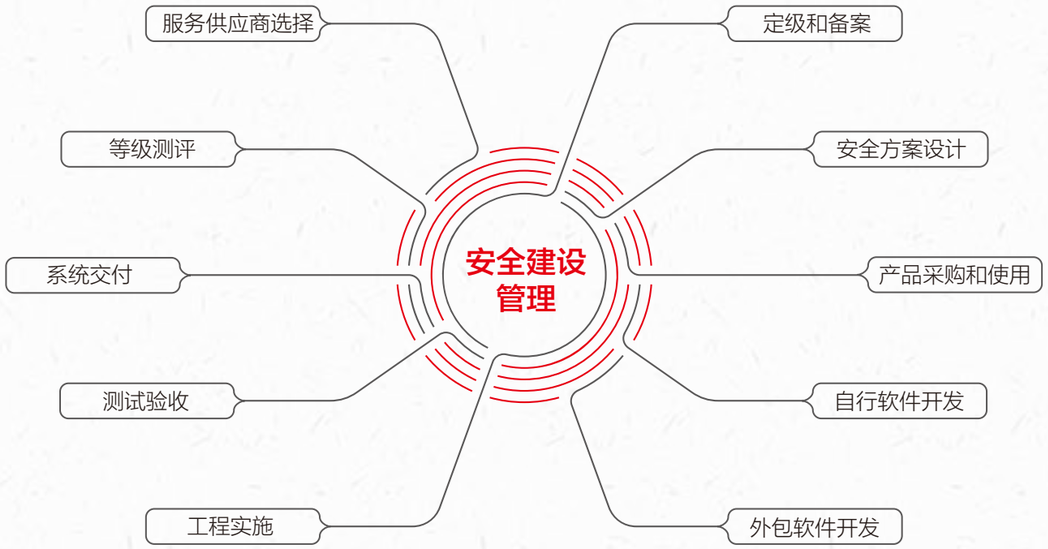
安全管理机构包括岗位设置、人员配备、授权和审批、沟通和合作、审核和检查这五部分内容。要求安全管理工作得到足够的重视，成立网络安全工作委员会或领导小组，最高领导由单位主管领导担任或授权，设立网络安全管理工作的职能部门并定义专人专岗。配置一定数量的系统管理员、审计管理员和安全管理员，且安全管理员不可兼任。根据各个部门和岗位的职责明确授权审批事项、对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，重要活动逐级审批。应加强沟通合作机制，包括组织机构内部和网络安全管理部门之间、网络安全职能部门、各供应商、业界专家及安全组织，共同协作处理网络安全问题，并建立外联单位联系列表。此外，还要建立审核检查机制，定期进行常规安全检查和全面安全检查，常规检查内容包括系统日常运行、系统漏洞和数据备份等情况；全面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。所有的检查活动过程应通过表格形式记录汇总安全检查结果形成安全检查报告，并对检查结果进行通报。

安全管理人员



安全管理人员包括人员录用、人员离岗、安全意识教育和培训、外部人员访问管理这几部分内容。要求指定或授权专门的部门或人员负责人员的录用，对被录用人员的身份、安全背景、专业资格等进行审查和技能考核，并与被录用人员签署保密协议，关键岗位人员应签署岗位责任协议；人员离岗时及时终止其所有访问权限，办理严格的调离手续，并承诺调离后的保密义务后方可离岗；应对各类人员进行安全意识教育和岗位技能培训，告知其相关的安全责任和惩戒措施，对不同的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并定期进行技能考核；外部人员物理访问受控区域前应提出书面申请，批准后由专人全程陪同，并登记备案，外部人员接入受控网络访问系统前也应提出书面申请，批准后由专人开设账户、分配权限，并登记备案，外部人员离场时应及时清除其所有访问权限，所有获得系统访问权限的外部人员均应签署保密协议，不准许进行非授权操作、复制和泄露任何敏感信息。

安全建设管理



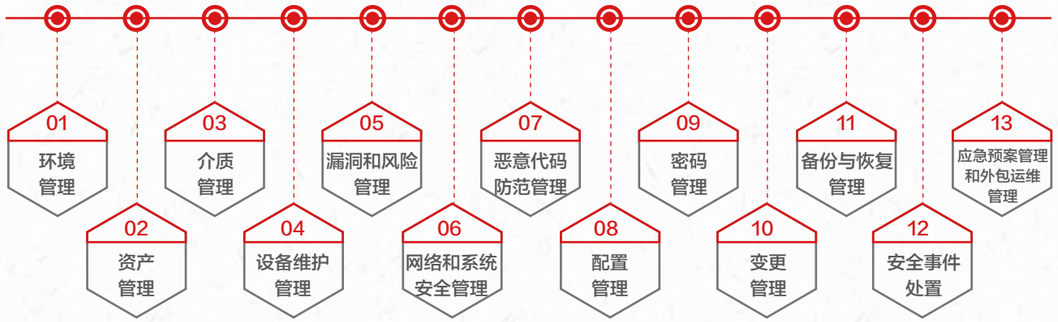
安全建设管理包括定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择这几部分内容。

定级和备案要求书面说明保护对象的安全保护等级及确定等级的方法和理由，定级结果应经过有关部门和有关安全技术专家的论证和审定，并经过相关部门的批准后，将备案材料报主管部门和相应的公安机关备案；安全方案设计应首先根据安全保护等级选择基本安全措施，进行风险分析并调整安全措施，根据等级保护对象的安全保护等级及与其它级别保护对象的关系进行安全整体规划和安全方案设计，同时组织相关部门和有关安全专家对安全整体规划进行论证和审定；

网络安全产品采购和使用确保符合国家的有关规定，密码产品与服务应符合国家密码管理主管部门的要求，并预先对产品进行选型测试，确定产品候选范围并定期审定和更新候选产品名单；制定软件开发管理制度和代码编写规范，并要求开发人员遵照执行，开发过程中进行严格的版本控制，全面的安全测试，并对开发活动进行控制、监视和审查，软件安装前应进行恶意代码检测；对于外包软件开发，应保证开发单位提供软件设计文档和使用指南，软件交付前检测其中可能存在的恶意代码，要求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。

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，制定安全实施方案并通过第三方工程监理控制实施过程；制定测试验收方案作为验收依据，形成验收报告；制定交付清单对所交接的设备、软件和文档等进行清点，组织相关人员进行技能培训并提供建设过程文档和运行维护文档；应定期或重大变更时或级别发生变化时进行等级测评，发现不符合相应等级保护标准要求的及时整改；服务供应商的选择应符合国家的有关规定，与之签订相关协议，明确各方需履行的网络安全相关义务，并定期对供应商提供的服务进行监督、评审。

安全运维管理



环境管理主要是机房环境的安全管理，包括出入管理、机房辅助设施、机房管理制度、来访人员管理等；资产管理要求编制保存资产清单，根据资产价值选择管理措施，依据资产重要程度进行标识并对分类与标识方法做出规定；介质管理要求介质在存放与传输过程中进行控制和保护；设备维护管理要求指定专门的部门或人员，并建立对应的管理制度，设备带离机房或办公地点应经过审批并加密重要数据，设备报废或重用前应完全清除存储介质数据，并确保无法被恢复重用；漏洞和风险管理要求及时识别、发现并修补安全漏洞和隐患，并定期开展安全测评，采取措施应对测评报告中发现的安全问题；网络和系统安全管理对包括管理员角色和权限的划分、账户及安全策略的控制和规定、日志记录和分析、各项运维活动的规程和审批等做了要求；恶意代码防范管理要求全员提高恶意代码防范意识，并定期验证防范恶意代码攻击技术措施的有效性；配置管理要求记录保存基本配置的同时将配置信息的改变纳入变更范畴实施变更控制，并及时更新基本配置信息库；密码管理遵循密码相关国家标准和行业标准，使用国家密码管理主管部门认证核准的密码技术和产品；变更管理要求明确变更需求并制定变更方案，建立变更的申报和审批程序，同时要建立中止变更并从失败变更中恢复的程序，明确

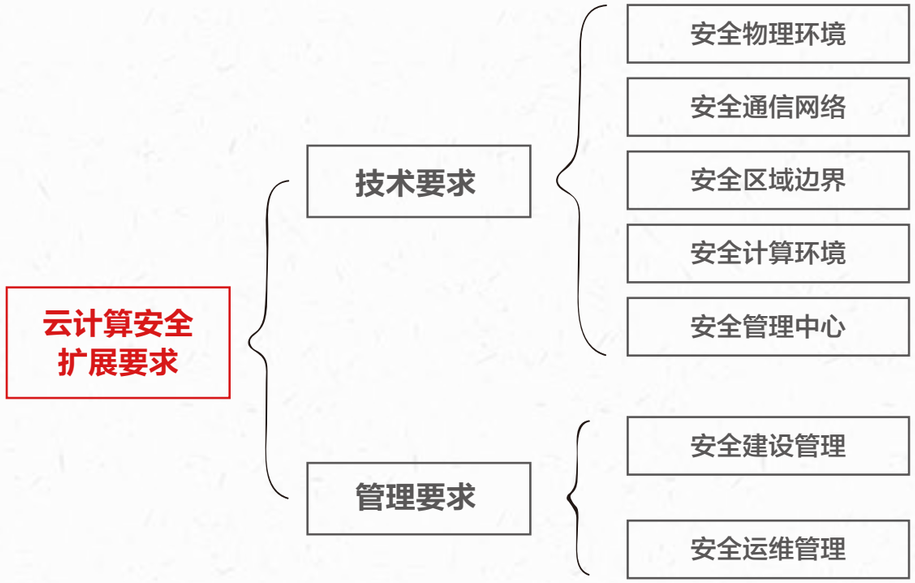
过程方法及人员职责，必要时对恢复过程进行演练；备份与恢复管理要求定期备份重要业务、系统及数据，规定备份方式、频度、存储介质、保存期等，并制定数据备份策略和恢复策略、备份程序和恢复程序等；安全事件处置要求及时向安全管理部门报告安全弱点和可疑事件，制定安全事件报告和处置管理制度，并在事件报告和响应处理过程中分析原因、收集证据、记录处理过程、总结经验教训，重大事件应采用不同的处理程序和报告程序；应急预案管理包括规定应急预案框架、制定应急预案、应急预案培训和演练、应急预案重新评估和修订完善等要求；外包运维管理对服务商的选择、相关协议的签订、服务商的工作能力以及对服务商的安全要求等方面提出了要求。

总结

在网络安全工作过程中，技术只是基础，更重要的是人的参与，是管理策略和管理手段的参与，安全管理在整个网络安全工作过程中是非常重要的，因此，我们不能一味的重视安全防护技术措施的部署而忽略安全管理体系的建设。

第四回 云计算安全扩展要求

本回内容概述

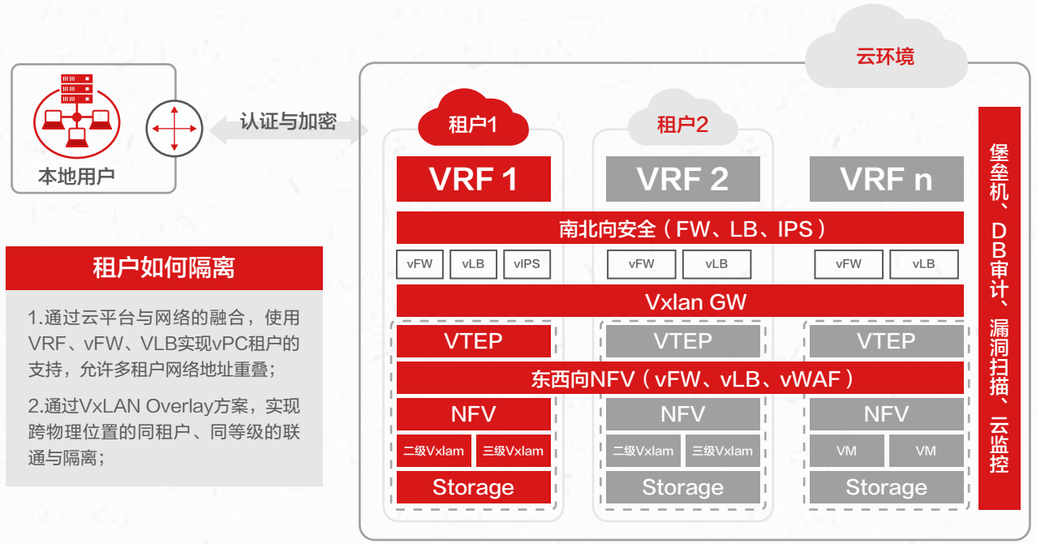


云计算安全扩展要求是在安全通用要求的基础上针对云计算的特点提出特殊保护要求。也就是说，在云计算环境中为了满足等保2.0的保准要求，既要满足安全通用要求，也要满足针对云计算提出的特殊保护要求。云计算安全扩展要求也分为技术要求和管理要求两大类。

安全物理环境

云计算安全扩展要求安全物理环境中的基础设施位置要求云计算基础设施位于中国境内。这是对提供云计算服务的云服务商提出的要求，由于在云计算环境中，数据的实际存储位置往往是不受客户控制的，客户的数据可能存储在境外数据中心，这就改变了数据和业务的司法管辖关系，需要注意的是，有些国家的政府可能依据本国法律要求云服务商提供可以访问这些数据中心的途径，甚至要求云服务商提供位于他国数据中心的数据。这使得客户的业务和数据隐私安全不能得到有效的保障。

安全通信网络之网络架构



租户如何隔离

1.通过云平台与网络的融合，使用VRF、vFW、VLB实现vPC租户的支持，允许多租户网络地址重叠；

2.通过VxLAN Overlay方案，实现跨物理位置的同租户、同等级的联通与隔离；

■ **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；**

解读：云计算环境中云服务商提供的云平台与客户的业务系统是需要分别单独定级的，那么云计算平台的等级保护等级必然不能低于其承载的客户业务系统的安全保护等级。

■ **应实现不同云服务客户虚拟网络之间的隔离；**

解读：除私有云外，整个云计算平台是由多个客户共享的，因此云服务商提供的云计算平台应具备隔离不同客户系统的能力，使得客户的虚拟网络在逻辑上实现独享。

■ **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；**

解读：云服务商在保证云计算平台达到相应等级的安全防护水平外，还应将相应的安全防护机制提供给客户。

■ **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；**

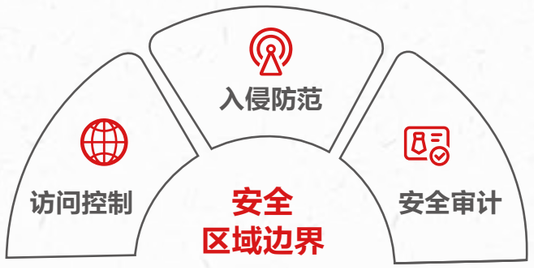
解读：客户的业务系统也是根据其对应的安全保护级别来部署安全防护措施，因此云计算平台应将相应的安全能力提供给客户，使用户可以根据需求进行自主选择、部署、配置。

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。

解读：这里是对云计算平台的兼容性提出的要求，有些客户可能根据其特殊的安全需求，需要引入云平台提供的安全防护之外的安全技术或产品，云计算平台应提供相应的开放接口供产品或服务的接入。

新华三安全云平台通过虚拟专有云（VPC）实现不同客户网络之间的逻辑隔离，通过安全资源池进行南北向安全防护，通过安全服务链提供东西向安全防护，可以各种虚拟化安全防护技术，完全满足等保2.0对云计算环境下网络架构安全的要求。

安全区域边界



访问控制

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问控制机制，设置访问控制规则。

解读：虚拟化网络边界的访问控制一般是通过虚拟防火墙来实现，不同等级的网络区域可以通过部署防火墙/虚拟防火墙，或者通过相应的跨网数据交换产品来实现。

入侵防范

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；

解读：这里是要求检测云服务客户对外发起的攻击行为，一般是通过入侵检测/防御系统来实现检测。

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；

解读：这里是要求检测外部网络对云计算环境发起的攻击行为，一般是通过入侵检测/防御系统来实现检测。

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；

解读：与传统网络南北向防护不同的是，云计算环境中东西向流量较多，而且也是安全防护的重点，云平台要具备东西向流量检测的能力，甚至是虚拟机与宿主机之间的流量检测能力。

d) 应在检测到网络攻击行为、异常流量情况时进行告警。

安全审计

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。

解读：在云计算环境中，云服务客户可以对自己的资产进行管理操作，而云服务商可以对云平台上的所有资产进行管理操作，当然也包括云服务客户的资产，这就需要云平台能分别对云服务商和云服务客户的重要操作进行审计和记录，使各方对自己的操作行为负责，同时，为保证云服务客户的有效权益，云平台也应提供相应的机制，使得云服务商在对客户系统和数据进行操作时，客户也能审计到云服务商的操作行为。

安全计算环境

安全计算环境，包括身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份恢复和剩余信息保护这几部分内容。

身份鉴别和访问控制

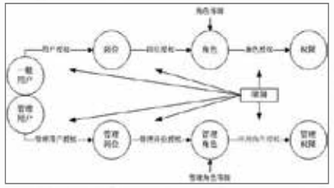
■ 身份鉴别

云安全计算环境中的身份鉴别要求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。

解读：

云计算平台要对管理终端身份的合法性进行验证，管理终端也要对所管理设备身份的合法性进行验证

■ 访问控制



▷ 应保证当虚拟机迁移时，访问控制策略随其迁移；

解读：

弹性扩展是云计算比较鲜明的特点，由于业务的需要，经常会涉及到虚拟机的新增、删除以及迁移等情况，这就需要虚拟机迁移后，云平台能够感知迁移的目标物理机，并通过策略下发等方式保持针对该虚拟机的访问控制策略不变，也就是访问控制策略随虚拟机的迁移而迁移。

▷ 应允许云服务客户设置不同虚拟机之间的访问控制策略。

解读：

这是对云平台提出的安全能力要求，云平台给云服务客户提供安全资源，并将所提供安全资源的管理权限一并分配给客户。

入侵防范及镜像和快照保护

■ 入侵防范

▷ 应能检测虚拟机之间的资源隔离失效，并进行告警；

▷ 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；

▷ 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。

解读：

这里是对云平台及相关组件提出的要求，虚拟机资源包括CPU、内存和磁盘等资源，云平台或相关组件能检测这些资源之间的隔离措施是否有效，同时检测虚拟机的使用及恶意代码在虚拟机之间的蔓延情况，发现异常情况时及时进行告警并处置。

■ 镜像和快照保护

镜像和快照保护是云计算环境特有的安全控制措施，其安全要求及解读如下：

▷ 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；

解读：

这里要求对重要业务系统提供安全的操作系统，生成加固过的虚拟机镜像，如关闭不必要的端口、服务，且进行了安全配置的加固。

▷ 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；

解读：

这里要求对生成的镜像或快照文件进行完整性校验，并具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。

▷ 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。

解读：

这里要求对虚拟机镜像或快照中的敏感资源采用加密、访问控制等技术手段进行保护，防止非法访问。

数据完整性和保密性

■ 数据完整性

数据完整性和保密性要求包括：

▷ 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；

▷ 应确保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；

▷ 应使用校验码或密码技术确保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；

▷ 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。

■ 数据保密性

解读：

这里首先对客户数据及用户个人信息存储的地理位置做了要求，必须存储于中国境内，如需出境应遵循国家相关规定，目前我们国家正规化出台个人信息出境安全评估办法，保障数据跨境流动中的个人信息安全；其次对云服务商管理客户数据的权限进行了限定，保障了云服务客户对自己业务数据的所有权；最后要求通过校验码、密码技术来保证数据在传输和使用过程中的完整性和保密性。

数据备份和恢复

■ 数据备份和恢复

数据备份和恢复要求如下：

▷ 云服务客户应在本地保存其业务数据的备份；

解读：

云计算服务虽然具备较高的可靠性，然而客户没有对自己业务和数据的实际控制权，为保证业务数据安全，重要业务数据必须本地备份。

▷ 应提供查询云服务客户数据及备份存储位置的能力；

解读：

这是对云计算平台提出的要求，考虑到云计算环境下，数据的物理存储位置较为模糊，云平台应提供查询数据及备份存储位置的能力。

▷ 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；

解读：

云平台自身也要提供客户数据备份功能，且备份的数据不能在同一物理服务器

▷ 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。

解读：

这条要求目的是使客户摆脱对某一云服务商的依赖，要求云平台统一标准和接口，使客户业务和数据能够在不同云服务商之间或者云平台和本地灵活迁移，有效保护云服务客户的权益

剩余信息保护

■ 剩余信息保护

剩余信息保护要求包括：

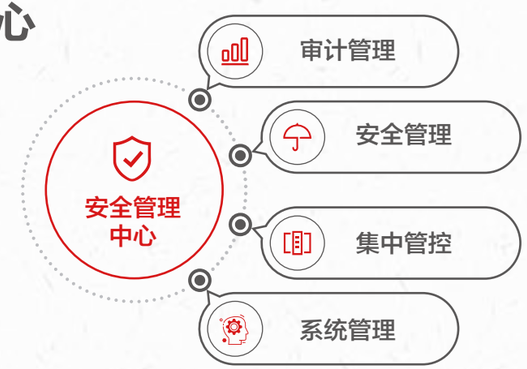
▷ 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；

▷ 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。

解读：

在云计算环境中，存储客户数据的存储介质由云服务商控制，客户不能直接管理和控制存储介质，当客户退出云计算服务或删除某个虚拟机时，云服务商应完全清除客户数据，包括备份数据和运行过程中产生的客户相关的数据，进行介质清理，不可清理的介质应物理销毁，保障客户数据的隐私安全。

安全管理中心



■ 集中管控：

▷ 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；

解读：

云计算环境的多客户、多业务的特点，决定了其资源的分配及策略的调整需集中进行自动化调度与分配，以减轻运维人员的负担。

▷ 应保证云计算平台管理流量与云服务客户业务流量分离；

解读：

这里要求对云计算平台上的资源进行带外管理，通过独立于客户业务网络之外的专用管理通道对云计算平台上的资源进行管理，以使云平台的管理流量与客户的业务流量分离。

▷ 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；

解读：

这里是对云计算平台、综合审计系统或相关组件提出的要求，由于审计数据包含了网络运行过程中的所有关键信息，因此要求云服务商与云服务客户分别各自收集，并实现各自的集中审计，最大限度的保护审计数据中的敏感信息不会遭到泄漏。

▷ 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。

解读：

云服务商和云服务客户各自负责各自控制资源的运行状况集中监测。

H3C SecCenter是业界管理功能最强大的软硬件一体化安全管理中心，基于先进的深度挖掘及分析技术，集安全事件收集、分析、响应等功能为一体，解决了网络与安全设备相互孤立、网络安全状况不直观、安全事件响应慢、网络故障定位困难等问题，能对各类网络、安全产品进行统一管理，提供超过1000种网络安全状况与政策符合性审计报告，使IT及安全管理员脱离繁琐的管理工作。

安全建设管理

■ 云服务商选择

- 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；
- 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；
- 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；
- 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；
- 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。

解读：

合规的云服务商是指通过权威机构安全审查的云服务商，客户在将业务部署或迁移至云计算平台之前，应对云服务商的资质进行审核，并确保其云平台的安全保护级别不低于客户业务系统的安全保护级别；同时由于目前缺乏有效的机制、标准或工具来对云服务商的各项数据与业务相关的安全责任进行检查和约束，所以客户要与云服务商签署服务水平协议、保密协议等，明晰云服务商的安全职责、行为准则以及违约责任等。

■ 供应链管理

- 应确保供应商的选择符合国家有关规定；
- 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；
- 应将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。

解读：

云计算环境是一个较为复杂的环境，涉及许多厂商的产品和组件，因此云服务商在对其云平台进行开发和相关产品和组件的采购时，要充分考虑安全需求，对产品和供应商的相关资质进行审核，对供应商提出相应的安全要求，确保供应商采取了必要的安全措施，云服务商还应要求供应商提供其产品和组件安全事件信息或安全威胁信息以及有关安全措施的文档信息，并及时传达到云服务客户，供应关系变更时，云服务商应将变更信息、变更带来的风险评估及采取的风险控制及时告知客户。

安全运维管理

云计算环境管理：

安全运维中的云计算环境管理要求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。

总结

■ 本回要点如下：

云计算基础设施要位于中国境内；

云计算平台应能为客户提供逻辑独享的网络；

云计算平台应为客户提供按需使用的安全能力；

云计算平台自身进行安全审计的同时，也要为客户提供云服务商对其资产进行管理操作审计的能力。

因云计算环境具备弹性灵活等特点，会涉及很多虚拟机新增、删除、迁移等情况，云平台应提供安全策略自动化部署和跟随迁移的能力；

东西向流量的识别和防护是云计算环境特有的需求。

■ 通过安全管理中心对云计算环境中的资源进行集中管控；

云服务客户选择合规的云服务商提供的服务，云服务商选择符合国家有关规定的供应商提供的产品和组件。

关于云计算环境的定级：

在云计算环境中，应将云服务商的云计算平台、云服务客户的业务系统分别单独作为等级保护的定级对象；对于大型云计算平台，应将大型的云计算基础设施和有关辅助设施划分为不同的定级对象（比如大型云计算平台的计费系统可单独作为一个定级对象）。

■ 结束语：

等保2.0云计算安全扩展要求中的安全管理中心、安全建设管理和安全运维管理，云计算安全扩展要求中的内容需要大家注意的是，**云计算安全扩展要求是满足通用安全要求的基础上，针对云计算的特点提出特殊保护要求。**

注：关于物联网、移动互联和工业控制系统安全的相关解读，小编提醒您关注“新华三大安全”《洪起说等保2.0》系列解读连载。

第五回 等保2.0解决方案

等级保护设计思路

■ 一个中心三重防护

■ 安全通信网络层面

双链路设备冗余	网络架构	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。
HTTPS VPN	通信传输	应采用密码技术保证通信过程中数据的保密性。
可信计算	可信验证	在应用程序的关键执行环节进行动态可信验证。

■ 安全区域边界层面

AC NGFW	边界防护	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。
NGFW DLP	访问控制	应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
沙箱反垃圾邮件系统	入侵防范	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。
ACG流量探针	安全审计	应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
可信计算	可信验证	在应用程序的关键执行环节进行动态可信验。

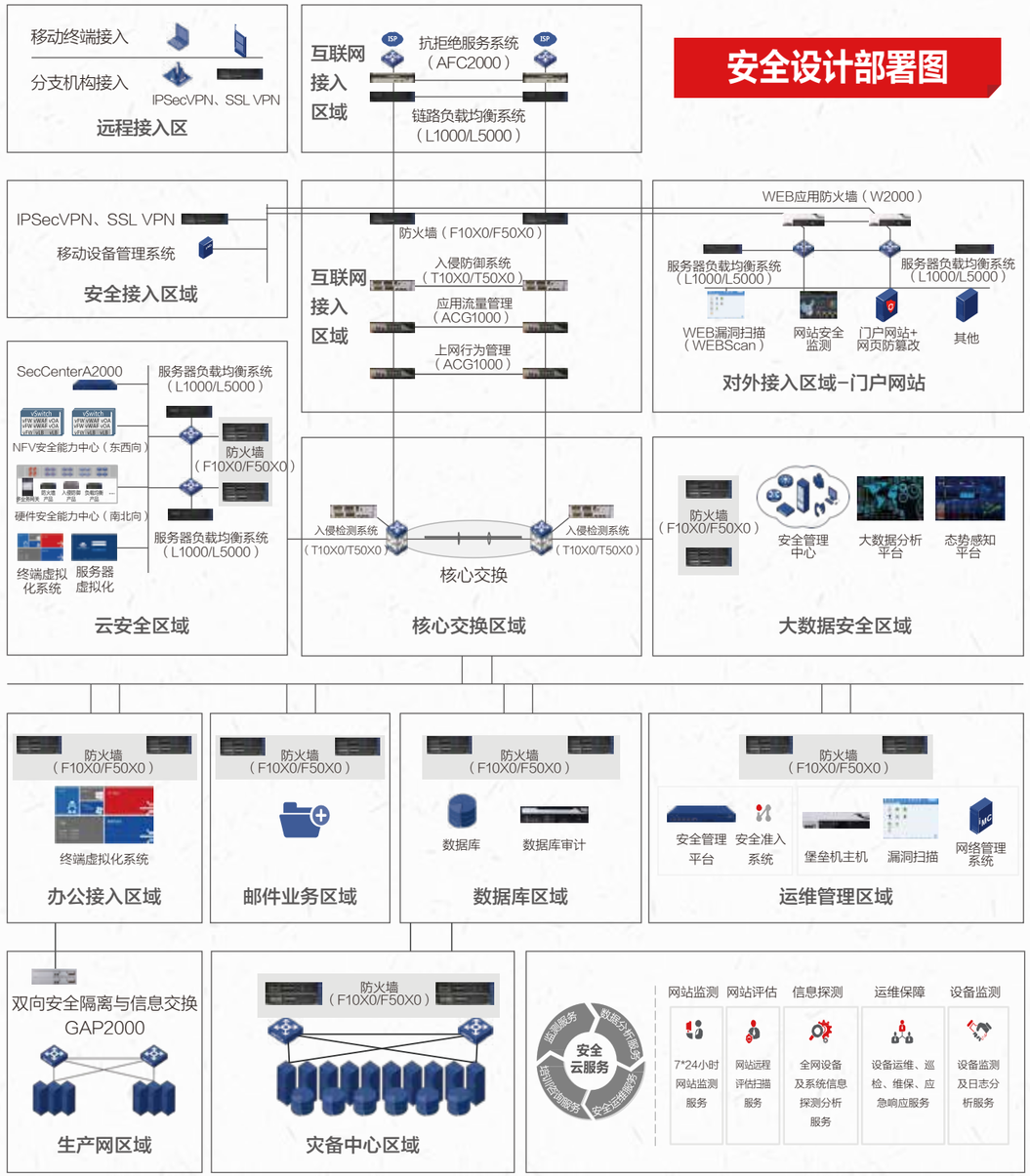
■ 安全计算环境层面

堡垒机	身份鉴别	应采用免受恶意代码攻击的技术措施或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。
主机加固	访问控制	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。
终端防病毒 沙箱	恶意代码防范	应采用免受恶意代码攻击的技术措施或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。
VPN加密机	数据保密性	应采用密码技术保证重要数据在传输/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。
数据实时备份 业务高可用架构	数据备份恢复	应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

■ 安全管理中心层面

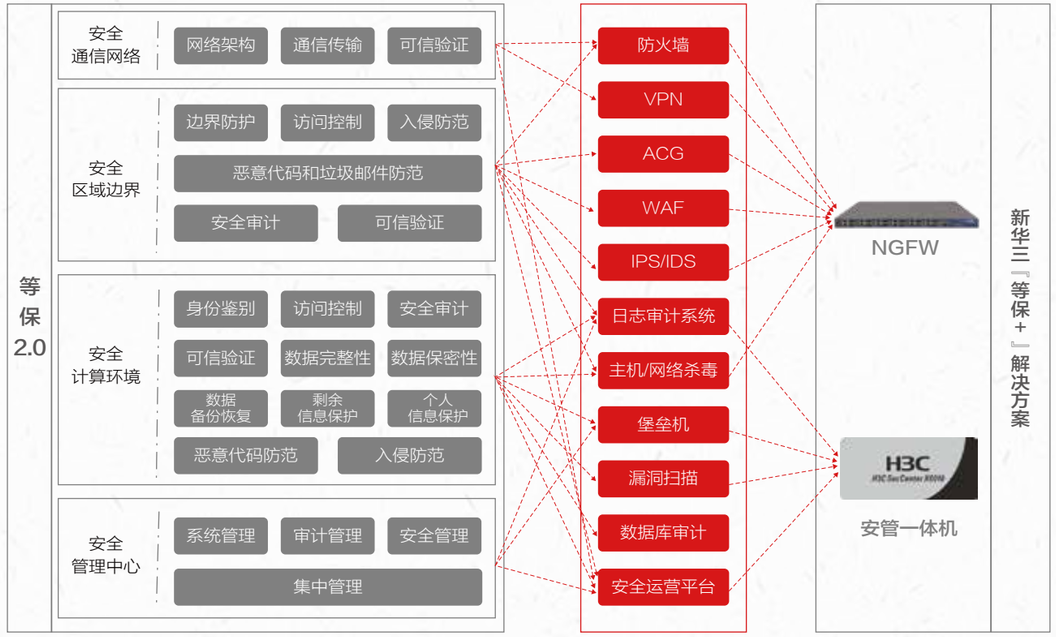
安全设备 纳管	安全管理	应通过安全管理员对系统中的安全策略进行配置。
安全管理区建设 FW	集中管控	划分单独的安全管理区域，并建立安全的信息传输路径。
SOC 日志审计系统	集中管控	应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； 审计记录留存时间符合法律要求。
主机加固 态势感知系统	集中管控	应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；并对各类安全事件进行识别、报警和分析。

新华三等保2.0方案设计

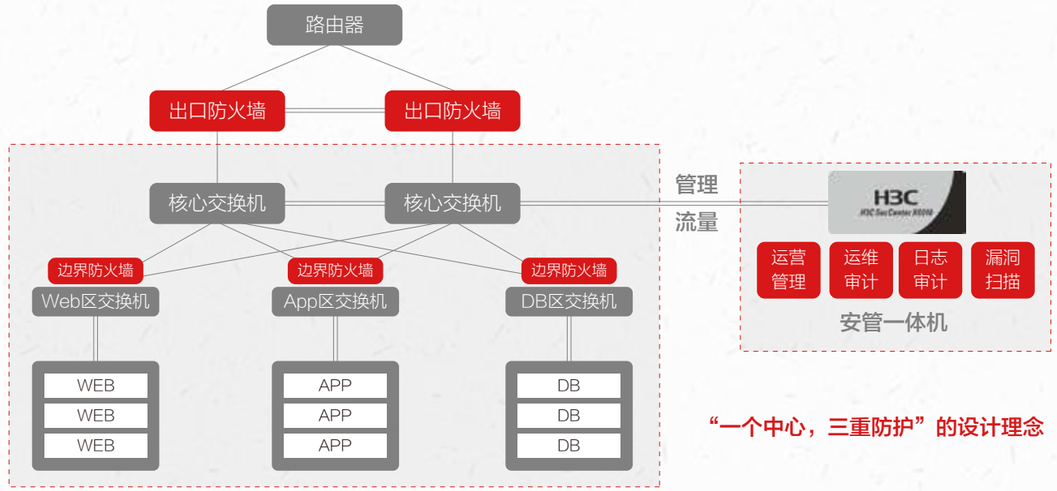


安全产品（服务）目录

新华三“等保+”解决方案



“等保+”解决方案架构



“一个中心，三重防护”的设计理念

H3C SecCenter X6010 安管一体机

等保2.0全景适用

- 等保2.0全景适用，高效合规，快速拿证
- 为客户建立信息安全技术体系、管理体系、运维体系

云网覆盖 资质完备

- 云+网+端 三位一体完全防护
- 资质完整，值得信赖

运营管理 按需扩展

- 构建多态化“安全管理中心”
- 前瞻设计，按需扩展

部署简单 维护方便

- 精简部署，快捷交付
- 涵盖等保主要要求，节约成本

新华三等保2.0扩展场景解决方案

等保2.0：云计算安全扩展要求

要求	云计算安全扩展要求	等保二级	等保三级
技术要求	安全物理环境	1	1
	安全通信网络	3	5
	安全区域网络	7	8
	安全计算环境	11	19
	安全管理中心	0	4
管理要求	安全管理制度	0	0
	安全管理机构	0	0
	安全管理人员	0	0
	安全建设管理	6	8
	安全运维管理	1	1
	云计算安全扩展要求	29	46

云计算安全扩展要求章节针对于计算的特点提出特殊保护要求。对于计算环境主要增加的内容包括“基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”和“云计算环境管理”等方面。

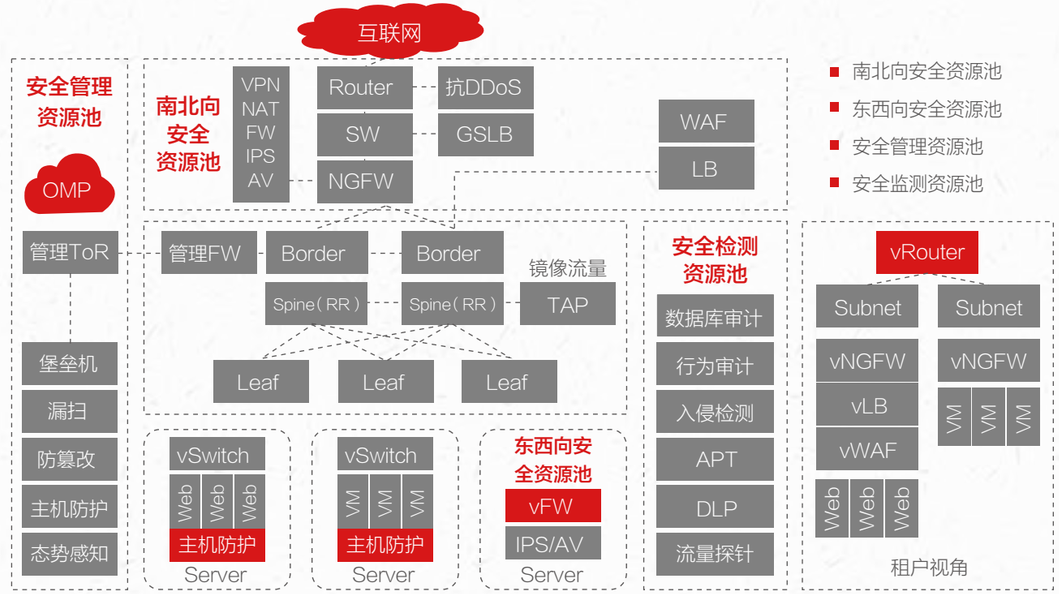
- 云计算平台的等级保护，等保二级需参考135项通用要求+29项云计算安全扩展要求；等保三级需参考211项通用要求+46项云计算安全扩展要求

- 对于政务云而言，不仅要参考等保2.0标准，也要参考GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》、GW0013—2017《政务云安全要求》

云安全合规能力需求

构建“云安全商店”，覆盖云基础设施安全、平台服务安全、应用服务安全以及场景化运维、运营管理，充分适配云等保要求，为云平台和租户提供一体化安全方案

云计算等保方案



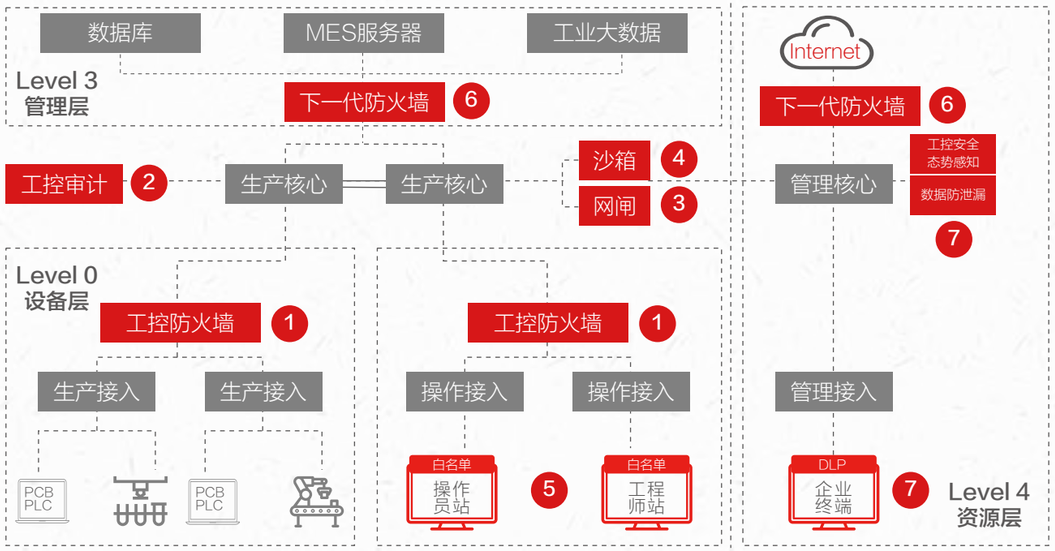
等保2.0：工控安全扩展要求

要求	工控系统安全扩展要求	等保二级	等保三级
技术要求	安全物理环境	2	2
	安全通信网络	4	4
	安全区域网络	5	8
	安全计算环境	2	5
	安全管理中心	0	4
管理要求	安全管理制度	0	0
	安全管理机构	0	0
	安全管理人员	0	0
	安全建设管理	2	2
	安全运维管理	0	0
	工控系统安全扩展要求	15	21

工业控制系统安全扩展要求章节针对工业控制系统的特点提出特殊保护要求。对工业控制系统主要增加的内容包括“室外控制设备防护”、“工业控制系统网络架构安全”、“拨号使用控制”、“无线使用控制”和“控制设备安全”等方面。

- 涉及工控系统建设的等保对象，等保二级需参考135项通用要求+15项工控系统安全扩展要求；等保三级需参考211项通用要求+21项工控系统安全扩展要求。

工控系统等保方案



1. 在设备层和控制层边界部署能够识别工控协议的工业控制防火墙
2. 在设备层和控制层边界部署能够识别工控协议的工业审计平台
3. 通过网闸进行生产环境与管理环境的物理隔离
4. 通过沙箱对生产和管理之间传输的文件进行未知威胁识别，防止类似“震网”
5. 在操作站上面安装主机白名单，形成授信环境
6. 在标准IT环境中防火墙边界防护
7. 在企业办公或资源终端部署数据防泄漏，防止图纸泄露

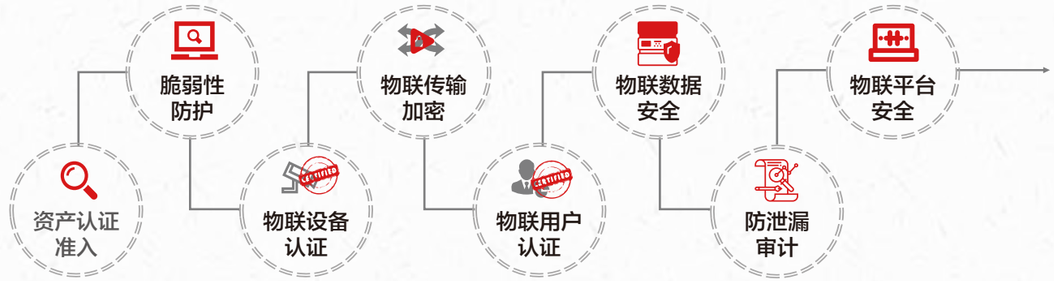
等保2.0：物联网安全扩展要求

要求	物联网安全扩展要求	等保二级	等保三级
技术要求	安全物理环境	2	4
	安全通信网络	0	0
	安全区域网络	3	3
	安全计算环境	0	10
	安全管理中心	0	0
管理要求	安全管理制度	0	0
	安全管理机构	0	0
	安全管理人员	0	0
	安全建设管理	0	0
	安全运维管理	2	3
	物联网安全扩展要求	7	20

物联网安全扩展要求章节针对物联网的特点提出特殊保护要求。对物联网环境主要增加的内容包括“感知节点的物理防护”、“感知节点设备安全”、“感知网关节点设备安全”、“感知节点的管理”和“数据融合处理”等方面。

- 涉及物联网建设的等保对象，等保二级需参考135项通用要求+7项物联网安全扩展要求；等保三级需参考211项通用要求+20项物联网安全扩展要求

物联网安全能力架构



物联前端安全

资产准入、设备指纹、设备认证、弱口令防护、漏洞检测…

物联传输安全

物联设备认证，物联传输加密，流量异常审计，链路质量监测…

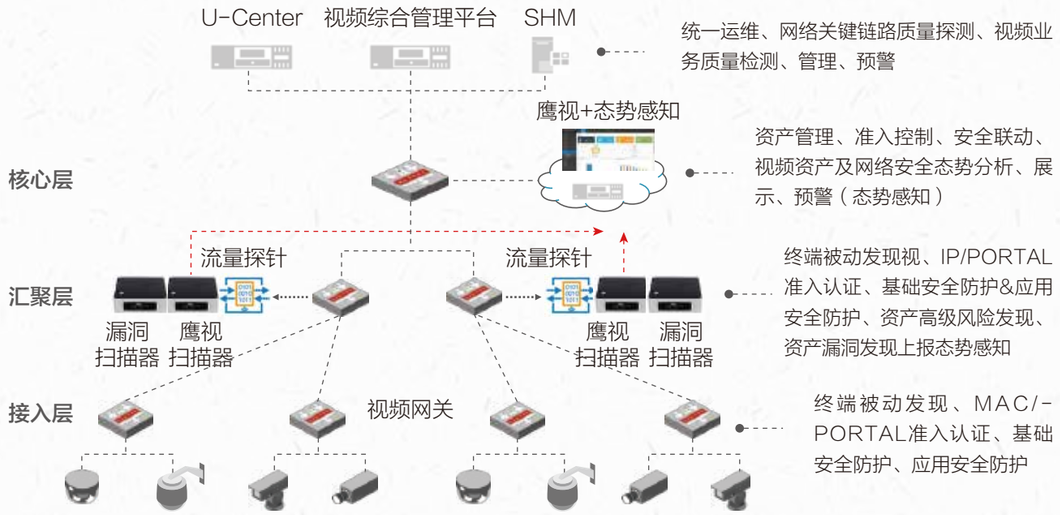
物联应用安全

物联用户认证，物联应用数据安全…

物联共享安全

物联数据防泄漏，用户行为审计，物联终端防泄漏…

物联网（视频）网络等保方案



等保2.0：移动互联扩展要求

要求	移动互联安全扩展要求	等保二级	等保三级
技术要求	安全物理环境	1	1
	安全通信网络	0	0
	安全区域网络	7	8
	安全计算环境	2	5
	安全管理中心	0	0
管理要求	安全管理制度	0	0
	安全管理机构	0	0
	安全管理人员	0	0
	安全建设管理	4	4
	安全运维管理	0	1
	移动互联安全扩展要求	14	19

移动互联安全扩展要求章节针对移动互联的特点提出特殊保护要求。对移动互联环境主要增加的内容包括“无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”和“移动应用软件开发”等方面。

- 涉及移动互联建设的等保对象，等保二级需参考135项通用要求+14项移动互联安全扩展要求；等保三级需参考211项通用要求+19项移动互联安全扩展要求。

移动互联网络安全能力架构

IPv6是移动互联的基础。IPv6报文结构中引入的新字段、IPv6协议族中引入的新协议可能存在漏洞，被利用发起DoS、嗅探、地址欺骗等攻击。

扩展头攻击

风险：

扩展头无限制，易受DoS攻击，消耗资源

措施：

可在防火墙上限制扩展头的数量和同一类型扩展头实例数目

分片攻击

风险：

- 利用首包逃避防火墙安全检测
- 产生大量分片，消耗资源

措施：

设备上设置合理的分片长度、数量

ICMPv6攻击

风险：

DDoS攻击

- 反射攻击

措施：

- 防火墙配置ACL白名单
- 关闭ICMPv6重定向

组播安全

风险：

- 冒充组播源，攻击组播成员
- 发送大量无效组播报告，浪费组播转发资源

措施：

进行MLD报文发送者认证

路由协议攻击

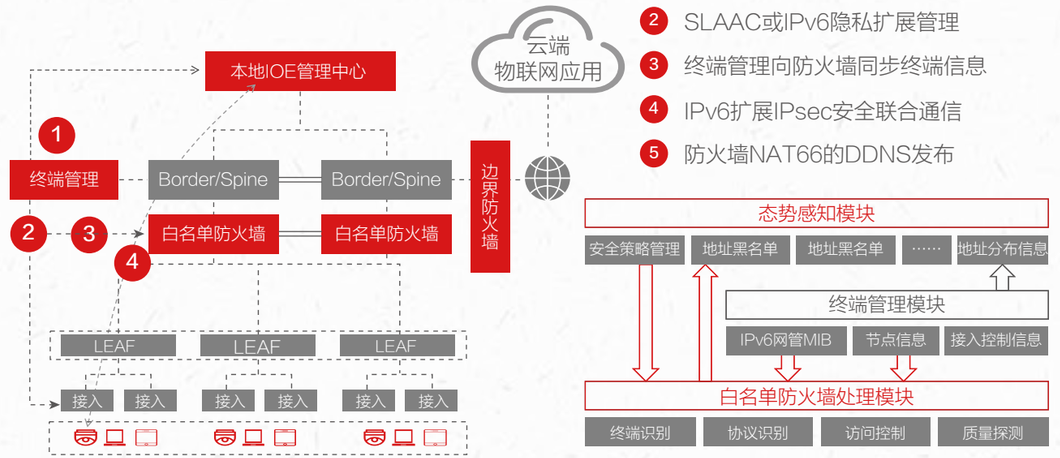
风险：

- 路由欺骗
- 非法路由获取

措施：

- 部署端到端的IPsec
- 禁止非法路由接入网络

移动互联网络等保方案



新华三等保2.0全景架构

第六回 新华三专业安全服务

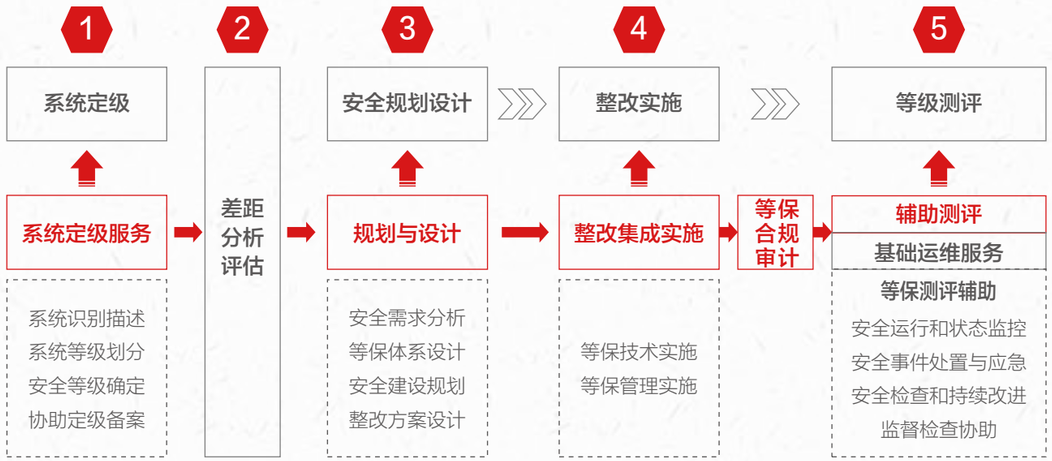
新华三安全服务概述

新华三安全服务团队具有网络安全、云安全、移动安全、大数据安全、工控安全、可信计算及物联网安全服务能力，为客户提供顾问式、管家式的安全服务，可提供的安全服务分5大类28个细分服务，涵盖风险评估、规划设计、工程实施、运行维护、知识传递五大过程，依据国家法规及行业标准结合云安全、安全设备、主机、网络、存储、数据库等专业技术提供一体化服务，凭借丰富的安全咨询和技术实践经验，帮助客户规划安全架构、评估风险态势、建设安全开发体系、防护加固体系和运维应急体系，满足监管合规要求，有效保障客户关键系统安全高可用性。

A、风险评估	B、规划设计	C、工程实施	D、运行维护	E、知识传递
安全评估类 A1:安全风险评估 A2:等保差距分析	**视划设计类** B1:安全战略规划 B2:管理体系设计 B3:等保体系设计 B4:云安全架构设计	**整改加固类** C1:安全加固 C2:等保整改	**平台运维类** D1:网站安全监测 D2:安全通告 **驻场协维类** D3:基础协维 D4:高级协维 **应急保障类** D5:应急响应 D6:重大时刻保障 **安全巡检类** D7:漏洞扫描 D8:基线检测 D9:日志分析 D10:安全策略维护	**安全培训类** E1:安全产品培训 E2:安全技术培训 E3:安全意识培训 E4:安全管理培训 E5:攻防演练培训 E6:定制化培训
安全检测类 A3:APP安全检测 A4:渗透测试 A5:代码审计	**合规咨询类** B5:等保合规咨询 B6:开发安全咨询 B7:ISO27001咨询 B8:云安全合规咨询			

安全等级保护服务解决方案

新华三安全等级保护服务解决方案根据国家、地方、行业的等级保护相关政策和标准要求，结合客户信息系统具体情况，为客户提供等级保护合规咨询服务。通过等级保护差距分析，协助客户发现信息系统的安全现状与需要达到的安全等级或目标的差异，配合客户完成信息系统的定级、备案和整改等工作，加强和完善客户在管理和技术方面的安全保障能力，为客户建立信息安全技术体系、管理体系、运维体系，帮助客户达到国家等级保护要求，获得等级保护认证证书。



信息安全等级保护是我国信息安全保障的基本制度、基本策略、基本方针，开展信息安全等级保护工作是信息安全保障工作中国家意志的体现，具有国家法律和政策的强制性。新华三长期深度参与、密切跟踪国家等级保护相关政策，参与等保标准编写,具备各种安全服务资质和专家资源，同多家测评机构签署战略协议深度合作，积累了丰富的经验。新华三安全等级保护服务解决方案主要包括以下工作内容:

定级备案:
依据法规标准,协助客户进行安全保护等级确定和指导备案表填写;

差距分析:
从安全技术和安全管理两个层面,对客户信息系统进行差距评估;

体系设计:
协助客户完成安全防护体系、管理体系、运维体系的设计规划;

安全整改:
根据整改设计方案,协助客户进行技术和管理整改,满足等保要求;

心协助测评:
测评机构测评期间,协助客户完成等保测评。

通过新华三安全等级保护服务，可是使客户信息系统建设和运营满足国家网络安全等级保护政策要求，了解当前目前整体安全风险分布状态和安全管理制度漏洞，提升安全技术防护水平和管理水平，提高客户安全保障能力，保障业务系统稳定运行。

安全体检服务解决方案

新华三安全体检服务参字ISO 27001、网络安全等级保护等国内外安全标准，依托专业的安全服务团队，通过资料收集、调查问卷、人员访谈、现场查勘、漏洞扫描、控制台审计、渗透测试、风险分析等方法，对用户网络、主机、终端、数据和应用系统等安全漏洞、安全风险隐患进行探测、分析、识别、控制、消除，可有效发现网络和应用系统面临的脆弱性、威胁和风险，帮助用户了解当前信息系统和网络面临的安全风险，并为客户提供风险规避建议及根据客户需求提供整改方案，规划安全体系建设。

第一阶段		第二阶段	第三阶段
管理现状评估	技术现状评估	安全规划设计	安全加固
信息安全管理架构分析 通过调研访谈、文件调查等方式，对安全组织架构进行分析，明确各部门及人员分工及职责，识别不足。 **安全管理制度文档缺失分析** 安全管理体系文件搜集，参照27001、等保等标准，鉴别制度流程表单缺失齐全情况。 **安全管理体系执行情况分析** 跟踪管理体系落地情况，对于无法落地的文件进行跟踪、反馈并完善。	**渗透测试** 模拟黑客渗透方式发现应用系统风险。 **网络架构评估** 从安全域划分、安全策略、边界防护等角度分析网络架构风险。 **代码审计** 分析核心系统源代码风险。 **漏扫、基线、日志分析** 审计日记、分析主机、设备、数据库等潜在的漏洞、基线配置等安全风险。	**整改加固方案** 针对发现的管理风险、技术风险，提出整改加固方案。 **安全规划方案** 结合信息安全现状，输出未来三年的信息安全规划方案，指导未来三年的信息安全建设。	**管理体系完善** 补充完善三、四级文件缺失的流程表单；更新管理体系文件。 **技术体系加固** 提供加固方案、协助加固主机系统、数据库、中间件等漏洞，负责对漏洞加固结果的验证。 **合规加固** 根据相关合规要求，对系统进行合规加固。

新华三安全体检服务可以帮助客户梳理信息安全合规需求，了解和掌握自身安全风险，制定或调整企业信息安全策略，指导信息安全建设和投入，为组织的信息安全规划方案提供依据，提高员工的信息安全意识，提升用户信息安全管理能力和防护水平，降低客户威胁事件发生的可能性及其造成的影响，将风险降低到可接受的水平。

全面的安全服务资质

新华三是唯一具备等级保护建设能力资质的国内综合类网络安全厂商，国家信息安全漏洞库CNNVD一级支撑单位，国家信息安全漏洞共享平台CNVD技术组单位。

新华三具备安全工程类一级、信息安全应急处理一级、信息安全风险评估一级服务资质，CMMI5、ISO9001/TL9000质量体系证书，信息安全管理体系(ISO27001)和信息技术服务管理体系(ISO20000)等资质证书。

微软MAPP计划

CMMI5

CVE

ITSS成员单位

新华三安全专业服务优势

新华三具备丰富的行业实战经验、全面的安全服务资质、强大的安全服务团队以及成熟的服务交付流程，为客户提供基于行业最佳实践的安全专业服务，保障客户业务的持续稳定运营。

丰富的行业实战经验

新华三在安全领域拥有超过10多年的服务案例积累，结合自身云计算、大数据和大互联的优势，提供最契合客户业务的服务体验。曾为北京奥运会、上海世博会、世界互联网大会、十九大、APEC峰会、杭州G20等重大活动提供安全保障，具备丰富的行业实战经验。并且在“心脏滴血”漏洞、勒索病毒等重大漏洞爆发的时候，表现出色，获得用户的一致好评。

强大的安全服务团队

新华三服务团队采用总部安全服务专家+区域安全服务工程师的模式，拥有超过100名安全服务专家及工程师，多人拥有CISP、CISSP、CISA、ITIL、ISO27001、H3CIE、CCIE、计算机信息系统集成项目经理、PMP认证等证书。

成熟的服务交付流程

新华三坚持以总部专家对项目进行交付，并在7大区（杭州、北京、合肥、成都、沈阳、广州、郑州）域设置安全服务人员，总部专家保证了项目的交付质量，区域服务工程也能够对用户的需求进行及时响应。

并且，新华三通过交付管理平台对安全服务交付的每一个环节，进行严格的把控，保证服务交付质量，以客户满意度为最终目标，为客户提供更高标准的服务。

结束篇

新华三信息安全技术有限公司介绍

新华三信息安全技术有限公司

新华三信息安全技术有限公司（简称新华三信息安全）是新华三集团的全资子公司，成立于2017年3月，位于安徽省合肥市高新区，为国内信息安全领域的领导企业，致力于为国家信息安全提供领先的信息安全产品与解决方案、专业的信息安全服务和优质的信息安全人才培养体系，为数字经济发展构筑主动防御、智能免疫的大安全体系。目前公司拥有近千名员工，其中55%以上为研发人员，70%以上拥有研究生学历，大安全专利授权总量超过1000件，90%以上为发明专利。

新华三信息安全可提供300多款安全产品，并在云安全、态势感知、高性能综合业务网关等前沿领域处于业界领先地位。作为国内率先推出全系列Sec　blade安全插卡和IPS产品的厂家，引领了网络安全的新时代。基于全球信息安全的最新发展趋势，新华三信息安全在业界明确提出从被动防御向主动防御发展的战略，为业界指明了发展方向。

基于十多年的信息安全实践经验，新华三信息安全全力满足各大行业在新IT与新经济时代的安全需求，广泛服务于政府、金融、企业、教育、运营商等各大行业，成功保障公安部、铁道部、工商银行、平安保险、中国互联网络信息中心、南方航空、南京大学等行业客户及G20杭州峰会、乌镇互联网大会等重大国事会议活动的信息安全。

新华三信息安全合肥创新体验中心于2017年12月6日正式启用，位于合肥市高新创业园二期J1-A栋23层，总面积近1000平方米，主要有序厅、解决方案区、案例展示区、综合实力区、攻防实验室等多个展示区域，通过高清屏幕、实物展示以及最新发布的态势感知实际场景演示等多种手段，对新华三的信息安全旗舰产品及解决方案进行全面展示，集中展现了新华三信息安全的整体实力。

态势感知展区

硬件展区

解决方案展区

高级威胁分析中心展区