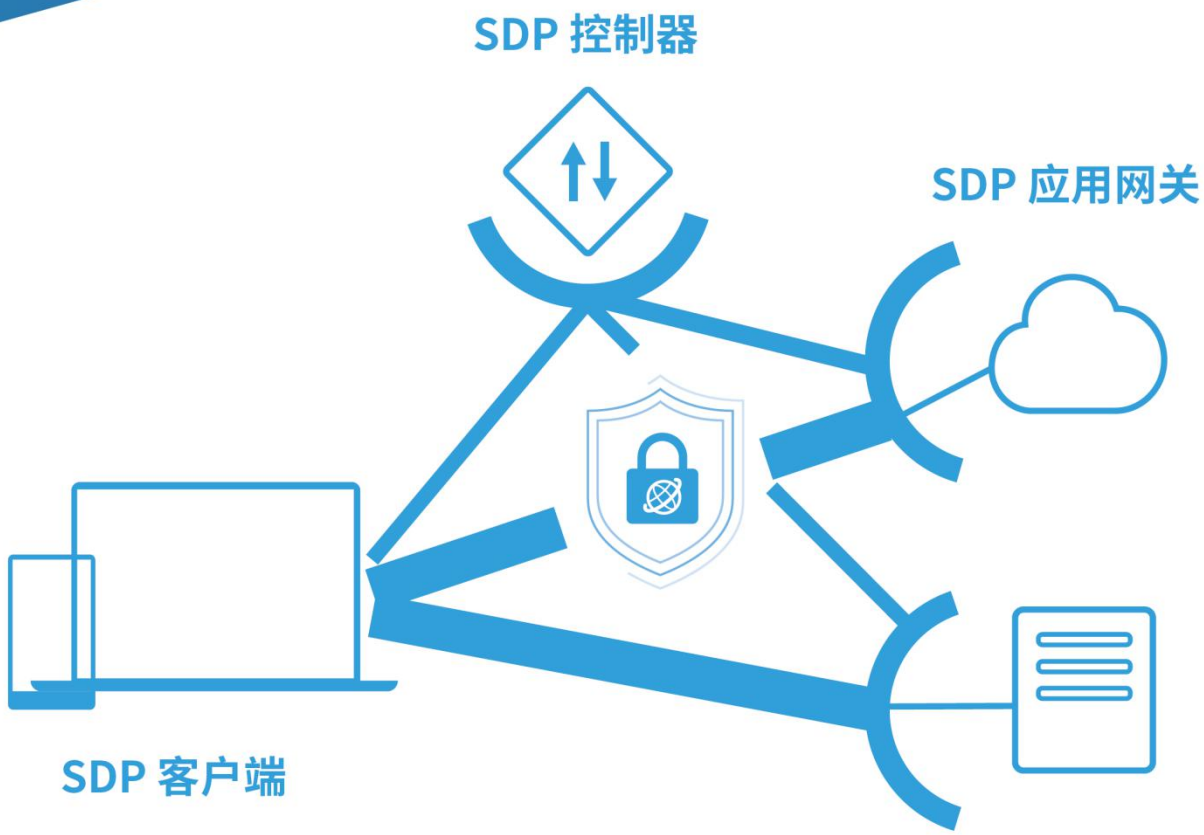
软件定义边界

SDP 实现等保 2.0 合规技术指南



CSA GCR GREATER CHINA REGION cloud security alliance ®

软件定义边界

SDP 实现等保 2.0 合规技术指南

白皮书

2020 年 4 月

编者信息

由云安全联盟大中华区（CSA GCR）组织SDP工作组专家对《SDP实现等保2.0合规技术指南》进行编写。

参与本文档编写的专家（排名不分先后）：

- **总编辑：**陈本峰（云深互联）
- **安全通用要求章节：**

  组长：卢艺（深信服） 组员：刘鹏（深信服）、鹿淑煜（三未信安）、潘盛合（顺丰）、刘洪森
- **云计算安全扩展要求章节：**

  组长：薛永刚（华为） 组员：秦益飞（易安联）、于继万（华为）、魏琳琳（国云科技）、杨洋
- **移动互联安全扩展要求章节：**

  组长：何国锋 组员：张全伟（吉大正元）、张泽洲（奇安信）、孙刚、赵锐
- **物联网安全扩展要求章节：**

  组长：余晓光（华为） 组员：张大海（三未信安）、高轶峰、马红杰、王安宇（OPPO）、杨喜龙
- **工控系统安全扩展要求章节：**

  组长：汪云林（天融信）组员：靳明星（易安联）、袁初成（缔安科技）、姚凯、于新宇（安几网安）
- **CSA GCR 研究助理：**朱晓璐、高健凯、廖飞

感谢以下单位对本文档的支持和贡献（按拼音排序）：

北京三未信安科技发展有限公司、北京天融信网络安全技术有限公司、长春吉大正元信息技术股份有限公司、国云科技股份有限公司、华为技术有限公司、江苏易安联网络技术有限公司、OPPO 广东移动通信有限公司、奇安信科技集团股份有限公司、上海安几科技有限公司、上海缔安科技股份有限公司、深信服科技股份有限公司、深圳顺丰泰森控股（集团）有限公司、深圳竹云科技有限公司、云深互联（北京）科技有限公司

序言

网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法，由公安部牵头的网络安全等级保护制度 2.0 标准于 2019 年 12 月 1 日实施，等保 2.0 将等保 1.0 的被动式传统防御思路转变为主动式防御，覆盖工业控制系统、云计算、大数据、物联网等新技术新应用，为落实信息系统安全工作提供了方向和依据。

云安全联盟提出的 SDP 软件定义边界是实施零信任安全架构的解决方案，SDP 将基于传统静态边界的被动防御转化为基于动态边界的主动防御，与等保 2.0 的防御思路非常吻合，成为满足等保 2.0 合规要求的优选解决方案。

CSA 大中华区 SDP 工作组的专家们对等保 2.0 做了深入解读，为读者们展示了如何通过 SDP 解决方案来满足企业的等保 2.0 合规要求，大家通过对这篇指南的学习也将在企业网络与信息安全保障能力提升方面受益。

李雨航 Yale Li

云安全联盟大中华区主席

目录

1 简介

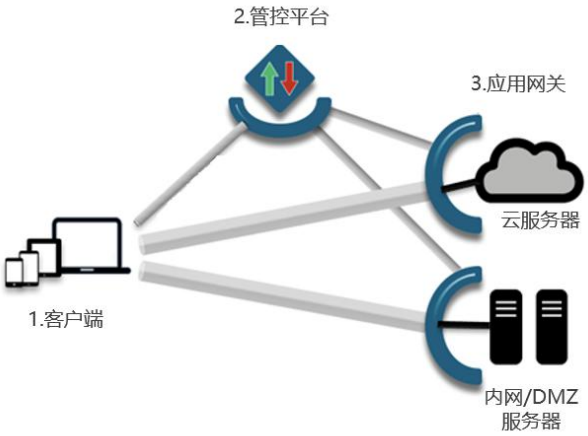
1.1 关于软件定义边界 SDP

传统企业网络安全架构通过建立一个固定的边界使内部网络与外部世界分离，这个边界包含一系列的防火墙策略来阻止外部用户的进入，但是允许内部用户对外的访问，即我们熟悉的“内网”。由于封锁了外部对于内部应用和设施的可见性和可访问性，传统的固定边界确保了内部服务对于外部威胁的安全。对于远程用户访问，最有效的办法也只是 VPN 接入。但是后期出现了各种各样的问题，云的租户不满足共用防火墙，希望得到更个性化的服务，传统防火墙和 VPN 不仅接入的体验、访问速度受限，更无法满足租户动态迁移、业务快速部署、策略随需生成、策略及时收回、策略路径可视等要求。另外，BYOD 和钓鱼攻击提供了对于内部网络的不可信访问，以及 SaaS 和 IaaS 正在改变边界的位置，企业网络架构中的固定的边界模型正在变得过时。

传统基于物理边界的安全模型已经不能满足云、移动、物联网时代的无处不在的连接需求以及日益严峻的企业内网渗透事故。公司企业纷纷将目光投向新一代的技术，比如基于零信任理念的软件定义边界，即 Software-Defined-Perimeter（SDP）安全技术架构。

SDP 方案是由国际云安全联盟 CSA 在 2014 年提出的一个零信任安全架构。在微软、Google 等国际互联网巨头公司内部都已经有成熟的应用。此后，Zscaler、思科、 赛门铁克、Akamai、Verizon 等知名公司都推出了 SDP 产品。软件定义边界（SDP）架构由客户端（Client）、管控平台（也称控制器，Controller）、

应用网关（Gateway）三个主要组件组成，如下图所示：



软件定义边界（SDP）架构

基于 SDP 安全架构方案可有效减少攻击面，缓解或者彻底消除威胁、风险和漏洞，从而帮助政府部门/企业能够集中资源于其他领域。关于 SDP 安全模型的详细描述以及应用实践，请参考 CSA 发布的 SDP 系列白皮书。下表列出了国际云安全联盟 CSA 统计的十二大安全威胁（来自《十二大网络安全威胁》白皮书），并分析 SDP 方案对于解决这些威胁的作用：

	安全威胁	SDP方案作用
1	数据泄露	SDP通过添加预验证和预授权层来减少公开暴露的主机的攻击面，实现服务器和网络的安全性的“最小访问权限”模型，从而有助于减少数据泄露的许多攻击方式。 剩余风险：数据泄露的几个其他攻击方式不适用于SDP，包括钓鱼、错误配置和终端保护。授权用户对授权资源的恶意访问将不会被SDP直接阻止。

2	弱身份、密码与访问管理	过去，VPN访问密码被盗往往会导致数据丢失。这是因为VPN通常允许用户对整个网络进行广泛的访问，从而成为弱身份、密码与访问管理中的薄弱环节。 相比之下，SDP不允许广泛的网络访问，并限制对这些主机的访问权限。这使得安全体系结构对弱身份、证书和访问管理有更大的弹性。SDP还可以在用户访问资源之前执行强认证。 剩余风险：政府部门/企业必须有一个积极的参与者来调整IAM流程，并确保访问策略被正确定义。过于宽泛的准入政策会带来潜在的风险。
3	不安全的界面和API	保护用户界面不被未授权用户访问是SDP的核心能力。使用SDP，未经授权的用户（即攻击者）无法访问UI，因此无法利用任何漏洞。 SDP还可以通过在用户设备上运行的进程来保护API。目前SDP部署的主要焦点一直是保护用户对服务器的访问。 剩余风险：服务器到服务器API调用在这个时候不是SDP的常见用例，因此API服务可能不会受到SDP系统的保护。

4	系统和应用程序漏洞	SDP显著减少攻击面，通过将系统和应用程序的漏洞隐藏起来，对于未授权用户不可见。 剩余风险：授权用户可以访问授权的资源，存在潜在的攻击可能性。其它安全系统如SIEM或IDS必须用来监控访问和网络活动（见下文的内部恶意人员威胁）。
5	账号劫持	基于会话cookie的帐户劫持被SDP完全消除。如果没有预先认证和预先授权，并且携带适当的SPA数据包，应用服务器会默认拒绝来自恶意终端的网络连接请求。因此，即使网络请求中携带被劫持的会话cookie，也不会被SDP网关准入。 剩余风险：钓鱼或密码窃取仍然是一个风险，但SDP可以通过执行强身份验证来减轻这种情况，并有基于诸如地理定位等属性来控制访问的策略。
6	内部恶意人员威胁	SDP将限制内部人员造成安全威胁的能力。适当配置的SDP系统将具有限制用户仅能访问执行业务功能所需的资源。因此，所有其他资源都将被隐藏。 剩余风险：SDP不阻止授权用户对授权资源的恶意访问。
7	高级持续威胁攻击	APTS本质上是复杂的、多方面的，不会被任何单一

	（APTS）	的安全防御所阻止。 SDP通过限制受感染终端寻找网络目标的能力，并且在整个政府部门/企业中实施多因子认证，有效减少攻击面，从而降低APT的存在可能性和传播。 剩余风险：预防和检测APTS需要多个安全系统和过程结合起来进行深入的防御。
8	数据丢失	SDP通过执行最小权限原则，并将网络资源对未授权用户隐藏起来，来减少数据丢失的可能性。SDP可以通过适当的DLP解决方案来增强。 剩余风险：SDP不阻止授权用户对授权资源的恶意访问。
9	尽职调查不足	SDP不适用
10	滥用和非法使用云服务	SDP并不直接适用，但SDP供应商的产品可能有能力检测和了解云服务使用状况。
11	DDoS拒绝服务	SDP架构中的单包授权（SPA）技术使得SDP控制器和网关对阻止DDoS攻击更有弹性。SPA与典型的TCP握手连接相比可花费更少的资源，使服务器能够大规模处理、丢弃恶意的网络请求数据包。与TCP相比，基于UDP的SPA进一步提高了服务器的可用性。

		剩余风险：虽然SPA显著降低了由无效SPA包所施加的计算负担，但它仍然是非零的，因此面向公众的SDP系统仍然可能受到大规模DDoS攻击的影响。
12	共享技术问题	SDP可以由云服务提供商使用，以确保管理员对硬件和虚拟化基础设施的访问管理。 剩余风险：云服务提供商除了SDP之外，还必须使用各种安全系统和流程。

1.2 关于等保 2.0

1.2.1 等级保护是国家信息安全管理的基本制度

随着政府、企事业单位信息化水平的不断提高，诸如泄密、黑客入侵等信息安全问题逐步凸现出来。近年来，国家层面越来越重视信息安全工作，确立了重要信息系统等级保护是国家信息安全管理的基本制度。

1994 年国务院发布了中华人民共和国国务院令（147 号）《中华人民共和国计算机信息系统安全保护条例》。自此，国家相关主管部门陆续发布了多项政策及标准，等级保护作为国家信息安全保障整改建设的标准，逐步进入落地阶段：

- 2003 年中办国办联合发布的中办发[2003]27 号文件—关于转发《国家信息化领导小组关于加强信息安全保障工作的意见》的通知；
- 2004 年公安部、保密局、国密办以及国信办联合发布的公通字[2004]66 号文件—《关于信息安全等级保护工作的实施意见》；

- 2005 年后公安部陆续发布了《信息系统安全等级保护实施指南》、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》和《信息系统安全等级保护测评指南》。
- 2007 年公安部、保密局、国密办和国信办联合发布的公通字[2007]43 号文件—《信息安全等级保护管理办法》。
- 2008 年《信息安全技术 信息系统安全等级保护基本要求》：明确对于各等级信息系统的安全保护基本要求。
- 2016 年 11 月，《网络安全法》正式发布，2017 年 6 月 1 日起开始施行。
- 2018 年 4 月，国家发布《全国医院信息化建设标准与规范(试行)》，此次《规范》中安全防护建设，对数据中心安全、终端安全、网络安全、容灾备份 4 个方面，19 个项目做了明确要求。
- 2019 年 5 月 13 日下午，国家标准新闻发布会在市场监管总局马甸办公区新闻发布厅召开，网络安全等级保护制度 2.0 标准正式发布，实施时间为 2019 年 12 月 1 日。

各政府、企事业单位都需要通过开展等级保护工作，推动等级保护整改建设实施，使得相关信息系统能够达到相应等级的基本保护和防护能力，从而满足上级部门的监管要求和政策法规的合规需求。

等保 2.0 一共分为五级，逐级安全要求增强，具体每一级内容如下：

信息系统的安全保护等级	内容
第一级：自主保护级	适用于一般的信息系统，其受到破坏后，会对公民、法人和其他组织的合法权益产生损害，但不损害国家安全、社会秩序和公共利益。

第二级：指导保护级	适用于一般的信息系统，其受到破坏后，会对社会秩序和公共利益造成轻微损害，但不损害国家安全。
第三级：监督保护级	适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成损害。
第四级：强制保护级	适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害。
第五级：专控保护级	适用于涉及国家安全、社会秩序和公共利益的重要信息系统的核心系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成特别严重损害。

1.2.2 等保合规建设过程中遇到的问题

由于信息安全保障工作的专业性和复杂性，各个单位在开展等级保护合规建设的过程中都不同程度遇到了诸多问题。据市场反馈，有近 60%的单位不了解等级保护建设工作如何开展，70%的单位不熟悉、不理解相关标准要求，大多数单位缺乏相关的知识和应对方案。

2 SDP 满足等保 2.0 安全通用要求

2.1 概述

随着信息系统的迭代速度加快，网络环境日趋复杂，传统的边界安全防护因为缺失灵活性无法适应复杂多变的攻击手段，因此现代网络安全体系建设应能够快速有效的部署访问策略，形成纵深边界安全防御和检测机制。等级保护 2.0 标准体系较 1.0 时代最大的变化，就是充分体现了“一个中心三重防御”的思想。一个中心指“安全管理中心”，三重防御指“安全计算环境，安全区域边界，安全网络通信”。从这一点上，等级保护 2.0 标准体系相比 1.0 时期的安全体系更注重整体动态的防御效果，强调事前预防、事中响应、事后审计。

软件定义边界（SDP）其本质是一套访问控制的策略体系，核心思想是构建以身份为中心，对网络传输进行的动态访问控制。它强调建立包括用户，设备，应用，系统等实体的统一身份标识，并基于最小化授权原则构筑访问。SDP 这种以网络为实施范围，以实体身份为抓手，最终实现对数据层面访问控制的安全体系很符合等级保护 2.0 标准体系中对三重防御体系，特别是“安全区域边界”和“安全网络通信”的要求。事实上，SDP 与等级保护 2.0 的总体思路是不谋而合的，这也体现了在安全挑战日新月异的大背景下，随着传统边界防护的瓦解，网络安全技术自身适应进化的一个过程。因此我们可以认为，借助 SDP，能够更加有效的解决等级保护的要求，构建全新的安全架构基石。

2.2 二级安全通用要求

2.2.1 安全通用要求（二级）概述

在国家等级保护 2.0 的二级要求中，明确了二级要求的保护能力即“能够防护免受来自外部小型组织的，拥有少量资源的威胁元发起的恶意攻击，一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和输出安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。”

由于二级要求是常见的相对基础层级的要求，在安全通用要求方面，主要针对多个领域，如物理安全，安全区域边界，安全计算环境，安全管理中心，安全管理制度，安全管理机构，安全管理人员和安全运维管理。通过对 SDP 的应用有效的提高安全管理效率，降低安全运维的成本与耗费，为真正的安全边界防护打开了起点。

等级保护的第二级别安全通用要求中由多个方面的技术要求，其中对于 SDP 帮助用户的满足的条目如下表所示：

要求项	要求子项	SDP适用情况
7.1.1安全物理环境	7.1.1.1--7.1.1.10	不适用
7.1.2 安全通信网络	7.1.2.1 网络架构	适用见2.2.2.1
	7.1.2.2 通信传输	适用见2.2.2.2
	7.1.2.3 可信验证	不适用
7.1.3安全区域边界	7.1.3.1 边界防护	适用见2.2.2.3
	7.1.3.2 访问控制	适用见2.2.2.4

	7.1.3.3 入侵防范	适用见2.2.2.5
	7.1.3.4 恶意代码防范	不适用
	7.1.3.5 安全审计	适用见2.2.2.6
	7.1.3.6 可信验证	不适用
7.1.4 安全计算环境	7.1.4.1 身份鉴别	适用见2.2.2.7
	7.1.4.2 访问控制	适用见2.2.2.8
	7.1.4.3 安全审计	适用见2.2.2.9
	7.1.4.4 入侵防范	适用见2.2.2.10
	7.1.4.5 恶意代码防范	不适用
	7.1.4.6 可信验证	不适用
	7.1.4.7 数据完整性	适用见2.2.2.11
	7.1.4.8 数据备份恢复	不适用
	7.1.4.9 剩余信息保护	不适用
	7.1.4.10个人信息保护	不适用
7.1.5 安全管理中心	7.1.5.1 系统管理	不适用
	7.1.5.2 审计管理	不适用
7.1.6 安全管理制度	7.1.6.1--7.1.6.4	不适用
7.1.7安全管理机构	7.1.7.1--7.1.7.4	不适用
7.1.8 安全管理人员	7.1.8.1--7.1.8.4	不适用
7.1.9 安全建设管理	7.1.9.1 --7.1.9.10	不适用
7.1.10 安全运维管理	7.1.10.1--7.1.10.14	不适用

2.2.2 对“7.1.2.1 网络架构”的适用策略

2.2.2.1. 本项要求包括:

a) 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。

b) 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。

2.2.2.2. SDP 的适用策略

针对第 a、b 条要求：SDP 提供应用层的边界防护，应用网关起到技术隔离作用。SDP 对于不同的网络分区支持发布特有的应用，由于 SDP 是通过 SDP 控制器来控制对应的连接访问，可以通过 SDP 的控制器来管理和控制对应的区域，同时对应的连接通过 SDP 客户端和 SDP 网关进行交互，大大提高了访问的可靠性和安全性。

对于安全边界的确定，SDP 有效的将其灵活性提高了，SDP 提供云平台和私有化部署，可以根据需要进行选择部署。SDP 实现的是边界防护，应用网关起到技术隔离作用，将应用服务器保护在网关后面，使外界扫描工具和攻击来源无法探测到服务器地址和端口。SDP 将原本固化的边界模糊化以减小攻击面。

2.2.3 对“7.1.2.2 通信传输”的适用策略

2.2.3.1 本项要求包括:

a) 应采用校验技术保证通信过程中数据的完整性。

2.2.3.2 SDP 的适用策略

针对第 a 条要求：“应采用校验技术保证通信过程中数据的完整性”，传输过程使用双向 TLS（mTLS）加密传输，防止被篡改，保障数据的完整性。

2.2.4 对“7.1.3.1 边界安全”的适用策略

2.2.4.1 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;

2.2.4.2 SDP 的适用策略

针对第 a 条要求：SDP 作为软件定义的边界安全隔离产品，可以有效地提供跨越边界的安全访问以及跨越边界数据流的受控接口。由于独特的 SDP 三组件关系，数据流仅能通过特定的客户端和网关，且经合法授权后，方可进入另外一个内部网络。

2.2.5 对“7.1.3.2 访问控制”的适用策略

2.2.5.1 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访问控制规则，默认情况下除允许通信外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，以允许

/拒绝数据包进出。

d） 应根据会话状态信息为进出数据或提供明确的允许/拒绝访问的能力。

2.2.5.2 SDP 的适用策略

对于访问控制来说，应根据具体情况部署 SDP 网关和控制器来保证对应的访问控制，SDP 的优势其实是对于请求验证的会话进行有效的验证和对应的访问控制。

因此，针对第 a 条要求：SDP 默认不信任任何网络、人、设备，均需进行验证，默认拒绝一切连接，只有验证合法的访问请求才被允许。并根据控制策略进行访问控制，仅对于验证合法用户，允许受控端口进行通信。即便合法的用户，也需要根据自己的权重分配账户和访问权限。

针对第 b 条要求：SDP 基于用户身份与授权进行精细化、颗粒度访问控制。

针对第 c 条：SDP 会对源地址、目的地址、源端口、目的端口和协议等进行检查，会基于上述信息进行访问控制，以允许符合条件的数据包通过，并拒绝不符合条件的数据包。

针对第 d 条要求：SDP 以身份化为基础，所有的访问请求都需要经过身份认证并植入会话状态信息，对所有访问流量会检测会话状态信息的合法性，仅允许携带合法会话状态信息的流量到达业务系统，拒绝非法访问。

对于其他的情况需要视情况而定对应的适用策略。

2.2.6 对“7.1.3.3 入侵防范”的适用策略

2.2.6.1 本项要求包括:

a）应在关键网络节点监视网络攻击行为

2.2.6.2 SDP 的适用策略

针对第 a 条要求：可以通过 SDP 控制器来监控所有对资源的访问日志以及异常行为，若对应的故障场景发生，则需要匹配对应的策略看是对应异常程度的严重程度，以帮助有效监控网络攻击行为。

对应的场景如果有变化，相应的策略需要调整。

2.2.7 对“7.1.3.5 安全审计”的适用策略

2.2.7.1 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。

2.2.7.2 SDP 的适用策略

SDP 的审计内容覆盖到每个终端用户，对于行为和重要事件进行记录。包括

日期、时间、事件等。并保存于管控平台，并进行定期备份，以防止未预期的删除、修改和覆盖等。

针对第 a、b 条要求：SDP 审计日志默认记录所有用户的所有访问日志，SDP 审计日志详细记录日期时间、用户、事件详情信息。

针对第 c 条要求：SDP 控制器上支持设置审计日志的保存时间，并且定期备份。

2.2.8 对“7.1.4.1 身份鉴别”的适用策略

2.2.8.1 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。

2.2.8.2 SDP 的适用策略

针对第 a 条要求：SDP 支持多因素认证，保证身份不易被冒用，并对密码复杂度有强制要求。

针对第 b 条要求：SDP 对登录认证有防爆破保护，以及连接超时自动注销保护。

针对第 c 条要求：SDP 对所有数据都使用双向 TLS（mTLS）加密传输，防止

数据在网络传输过程中被窃听，并且能防止中间人攻击。

2.2.9 对“7.1.4.2 访问控制”的适用策略

2.2.9.1 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。

2.2.9.2 SDP 的适用策略

SDP 属于访问控制类别产品，具备账号管理功能，能够分配账户访问与配置权限。即便合法的用户，也需要根据自己的角色确定账户和访问权限。

针对第 a、b 条要求：SDP 对所有的用户的访问连接都会进行授权校验。

针对第 c、d 条要求：SDP 控制器对账号会设置过期时间，对于长时间不登录的账号会禁止登录。

2.2.10 对“7.1.4.3 安全审计”的适用策略

2.2.10.1 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、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。

2.2.10.2 SDP 的适用策略

针对第 a、b 条要求：SDP 审计日志默认记录所有用户的所有访问日志，SDP 审计日志详细记录日期时间、用户、事件详情信息。

针对第 c 条要求：SDP 控制器上支持设置审计日志的保存时间，并且定期备份。

2.2.11 对“7.1.4.4 入侵防护”的适用策略

2.2.11.1 本项要求包括:

a) 应遵循最小安装的原则，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。

2.2.11.2 SDP 的适用策略

针对第 a、b 条要求：SDP 本身的特性就默认关闭所有端口，拒绝一切连接，

不存在共享和高危的端口，应用网关仅面向授权客户端开放访问权限，极大地控制了使用范围，减小了暴露面。通过客户端和控制器，可检测到入侵的行为，并在发生严重入侵事件时提供预警。

针对第 c 条要求：SDP 客户端在连接网关之前需要先去控制器进行身份和设备的验证，控制器可以对终端的接入方式或网络地址范围进行有效控制。

针对第 d 条要求：SDP 客户端和 SDP 网关之间使用特殊的通信协议以及加密(mTLS)的数据传输，以保证数据的正确性和有效性。

针对第 e 条要求：SDP 三组件（客户端、网关、控制器）支持自动更新和升级，保证可以及时修补漏洞。

2.2.12 对“7.1.4.7 数据完整性”的适用策略

2.2.12.1 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。

2.2.12.2 SDP 的适用策略

针对第 a 条要求：SDP 通过密码技术（mTLS 双向 TLS 加密）对网络传输进行数据加密，保障数据的完整性。

2.3 三级安全通用要求

2.3.1 安全通用要求（三级）概述

等保三级又被称为国家信息安全等级保护三级认证，是中国最权威的信息产品安全等级资格认证，由公安机关依据国家信息安全保护条例及相关制度规定，按照管理规范和技术标准，对各机构的信息系统安全等级保护状况进行认可及评定。其中三级是国家对非银行机构的最高级认证，属于“监管级别”，由国家信息安全监管部门进行监督、检查，认证需要测评内容涵盖等级保护安全技术要求 5 个层面和安全管理要求的 5 个层面，主要包含信息保护、安全审计、通信保密等在内的近 300 项要求，共涉及测评分类 73 类，要求十分严格。

等保三级中，通用安全要求项与 SDP 适用项如下表所示：

要求项	要求子项	SDP适用情况
8.1.1安全物理环境	8.1.1.1--8.1.1.10	不适用
8.1.2 安全通信网络	8.1.2.1 网络架构	适用见2.3.2.1
	8.1.2.2 通信传输	适用见2.3.2.2
	8.1.2.3 可信验证	不适用
8.1.3安全区域边界	8.1.3.1 边界防护	适用见2.3.2.3
	8.1.3.2 访问控制	适用见2.3.2.4
	8.1.3.3 入侵防范	适用见2.3.2.5
	8.1.3.4 恶意代码防范	不适用
	8.1.3.5 安全审计	适用见2.3.2.6
	8.1.3.6 可信验证	不适用

8.1.4 安全计算环境	8.1.4.1 身份鉴别	适用见2.3.2.7
	8.1.4.2 访问控制	适用见2.3.2.8
	8.1.4.3 安全审计	适用见2.3.2.9
	8.1.4.4 入侵防范	适用见2.3.2.10
	8.1.4.5 恶意代码防范	不适用
	8.1.4.6 可信验证	不适用
	8.1.4.7 数据完整性	适用见2.3.2.11
	8.1.4.8 数据保密性	适用见2.3.2.12
	8.1.4.9 数据备份恢复	不适用
	8.1.4.10 剩余信息保护	不适用
	8.1.4.10个人信息保护	不适用
8.1.5 安全管理中心	8.1.5.1 系统管理	不适用
	8.1.5.2 审计管理	不适用
	8.1.5.3 安全管理	不适用
	8.1.5.4 集中管控	适用见2.3.2.13
8.1.6 安全管理制度	8.1.6.1--8.1.6.4	不适用
8.1.7安全管理机构	8.1.7.1--8.1.7.4	不适用
8.1.8 安全管理人员	8.1.8.1--8.1.8.4	不适用
8.1.9 安全建设管理	8.1.9.1 --8.1.9.10	不适用
8.1.10 安全运维管理	8.1.10.1--8.1.10.14	不适用

2.3.2 对“8.1.2.1 网络架构”的适用策略

2.3.2.1 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。

2.3.2.2SDP 的适用策略

针对第 c、d 条要求：SDP 提供应用层的边界防护，应用网关起到技术隔离作用。SDP 的应用对于不同的网络分区有特别的应用，由于 SDP 是通过 SDP 控制器来控制对应的链接， 可以通过 SDP 的控制器来管理和控制对应的区域，同时对应的连接通过 SDP 客户端 和 SDP 网关进行交互，大大提高了访问的可靠性和安全性。

对于安全边界的确定，SDP 有效的将其灵活性提高了，SDP 提供云平台和私有化部署，可以根据需要进行选择部署。SDP 实现的是边界防护，应用网关起到技术隔离作用，将应用服务器保护在网关后面，使外界扫描工具和攻击来源无法探测到服务器地址和端口。SDP 将原本固化的边界模糊化以减小攻击面。

2.3.3 对“8.1.2.2 通信传输”的适用策略

2.3.3.1 本项要求包括:

a) 应采用校验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。

2.3.3.2SDP 的适用策略

针对第 a、b 条要求：SDP 组件之间的传输过程使用 mTLS 进行加密传输，防止被篡改，保障数据的完整性，同时也能防止被监听、窃取。mTLS 基于常见的密码学算法（如数字签名、散列、对称加密）。国际上使用 RSA、AES、SHA256 等通用算法来实现，而国内可以使用 SM2、SM3、SM4 等国密算法来实现。

2.3.4 对“8.1.3.1 边界防护”的适用策略

2.3.4.1 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。

2.3.4.2SDP 的适用策略

针对第 a 条要求：SDP 作为软件定义的边界安全隔离产品，可以有效地提供

跨越边界的安全访问以及跨越边界数据流的受控接口。由于独特的 SDP 三组件关系，数据流仅能通过特定的客户端和网关，且经合法授权后，方可进入另外一个内部网络。

针对第 b、c 条要求：SDP 秉承“先验证后连接”的原则，所有的终端设备首先要到 SDP 控制器上进行身份和设备的验证，才能被允许连接网关。当 SDP 网关部署在内部网络以及外部网络的边界上时，无论是外部的非授权设备私自联到内部网络，还是内部用户非授权联到外部网络，都可以被 SDP 网关阻止。

针对第 d 条要求：SDP 网关可以部署在无线网络以及企业资源所在网络的中间，只有通过 SDP 网关才能访问到企业的资源，对于非授权用户企业资源完全不可见，可以有效地防止非授权设备进入企业内部网络访问资源。

2.3.5 对“8.1.3.2 访问控制”的适用策略

2.3.5.1 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访问控制规则，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，以允许/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。

2.3.5.2 SDP 的适用策略

针对第 a 条要求：SDP 默认不信任任何网络、人、设备，均需进行验证，默认拒绝一切连接，只有验证合法的访问请求才被允许。并根据控制策略进行访问控制，仅对于验证合法用户，允许受控端口进行通信。即便合法的用户，也需要根据自己的权重分配账户和访问权限。

针对第 b 条要求：SDP 基于用户身份与授权进行精细化、颗粒度访问控制。

针对第 c 条：SDP 会对源地址、目的地址、源端口、目的端口和协议等进行检查，会基于上述信息进行访问控制，以允许符合条件的数据包通过，并拒绝不符合条件的数据包。

针对第 d 条要求：SDP 以身份化为基础，所以的访问请求都需要经过身份认证并植入会话状态信息，对所有访问流量会检测会话状态信息的合法性，仅允许携带合法会话状态信息的流量到达业务系统，拒绝非法访问。

针对第 e 条要求：SDP 以身份化为基础，对所有的访问，会检测应用协议及应用内容，包括 https、RDP 协议等检测，以对不同应用协议的访问进行不同的安全检查。

2.3.6 对“8.1.3.3 入侵防护”的适用策略

2.3.6.1 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。

2.3.6.2 SDP 的适用策略

针对第 a、b、c 条要求：SDP 网关部署在网络资源的关键位置，并且记录所有的资源访问日志，日志上传到 SDP 控制器，控制器对访问行为进行分析，发现并自动阻断网络攻击行为。

针对第 d 条要求：SDP 网关实时记录所有访问日志，日志内容包括源 IP 和端口、目标 IP 和端口，访问设备、访问时间等信息，同时对这些日志进行大数据智能分析并发出预警。

2.3.7 对“8.1.3.5 安全审计”的适用策略

2.3.7.1 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。

2.3.7.2 SDP 的适用策略

SDP 的审计内容覆盖到每个终端用户，对于行为和重要事件进行记录。包括日期、时间、事件等。并保存于管控平台，并进行定期备份，以防止未预期的删除、修改和覆盖等。

针对第 a、b 条要求：SDP 审计日志默认记录所有用户的所有访问日志，SDP 审计日志详细记录日期时间、用户、事件详情信息。

针对第 c 条要求：SDP 控制器上支持设置审计日志的保存时间，并且定期备份。

2.3.8 对“8.1.4.1 身份鉴别”的适用策略

2.3.8.1 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。

2.3.8.2 SDP 的适用策略

针对第 a 条要求：SDP 支持多因素认证，保证身份不易被冒用，并对密码复杂度有强制要求。

针对第 b 条要求：SDP 对登录认证有防爆破保护，以及连接超时自动注销保护。

针对第 c 条要求：SDP 对所有数据都使用双向 TLS（mTLS）加密传输，防止数据在网络传输过程中被窃听。

针对第 d 条要求：SDP 支持多因素认证，包括口令、短信、动态令牌、证书、UKey、生物特征等。这些鉴别技术可以采用密码技术来实现。

2.3.9 对“8.1.4.2 访问控制”的适用策略

2.3.9.1. 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) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

2.3.9.2SDP 的适用策略

SDP 属于访问控制类别产品，具备账号管理功能，能够分配账户访问与配置权限。即便合法的用户，也需要根据自己的角色确定账户和访问权限。

针对第 a，b 条要求：SDP 对所有的用户访问都会进行授权校验。

针对第 c、d 条要求：SDP 对账号会设置过期时间，对于长时间不登录的账号会禁止登录。

针对第 e 条要求：SDP 通过授权策略实现主体（用户）访问客体（业务系统）的访问控制。

针对第 f 条要求：SDP 的主体为用户，能实现用户级的的访问控制。同时支持进程级的安全检查，基于检查结果进行访问控制。同时客体为业务系统，并支持控制粒度细致到 URL 级别。

2.3.10 对“8.1.4.3 安全审计”的适用策略

2.3.10.1. 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、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。

d) 应对审计进程进行保护，防止未经授权的中断。

2.3.10.2 SDP 的适用策略

针对第 a、b 条要求：SDP 审计日志默认记录所有用户的所有访问日志，SDP 审计日志详细记录日期时间、用户、事件详情信息。

针对第 c 条要求：SDP 控制器上支持设置审计日志的保存时间，并且定期备份。

针对第 d 条要求：SDP 审计模块通过监控程序相互保护，在发生异常中断时会通过监控程序拉起。

2.3.11 对“8.1.4.4 入侵防护”的适用策略

2.3.11.1 本项要求包括：

a) 应遵循最小安装的原则，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。

2.3.11.2 SDP 的适用策略

针对第 a、b 条要求：SDP 本身的特性就默认关闭所有端口，拒绝一切连接，不存在共享和高危的端口，应用网关仅面向授权客户端开放访问权限，极大地控制了使用范围，减小了暴露面。通过客户端和控制器，可检测到入侵的行为，并在发生严重入侵事件时提供预警。

针对第 c 条要求：SDP 客户端在连接网关之前需要先去控制器进行身份和设备的验证，控制器可以对终端的接入方式或网络地址范围进行有效控制。

针对第 d 条要求：SDP 客户端和 SDP 网关之间使用特殊的通信协议以及加密(mTLS)的数据传输，以保证数据的正确性和有效性。

针对第 e 条要求：SDP 三组件（客户端、网关、控制器）支持自动更新和升级，保证可以及时修补漏洞。

针对第 f 条要求：SDP 会实时分析用户行为，发现异常入侵行为，并阻断和告警。

2.3.12 对“8.1.4.7 数据完整性”的适用策略

2.3.12.1 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。

2.3.12.2 SDP 的适用策略

针对第 a、b 条要求：SDP 通过密码技术对网络传输进行数据加密（mTLS，即双向 TLS），有效保障数据的完整性和保密性。

2.3.13 对“8.1.4.8 数据保密性”的适用策略

2.3.13.1 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；

2.3.13.2 SDP 的适用策略

针对第 a 条要求：SDP 通过密码技术对网络传输进行数据加密（mTLS，即双向 TLS），有效保障数据的完整性和保密性。

2.3.14 对“8.1.5.4 集中管控”的适用策略

2.3.14.1 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；

2.3.14.2 SDP 的适用策略

针对第 a 条要求：SDP 控制器对所有接入的 SDP 网关和 SDP 客户端进行集中管控，SDP 网关作为边界隔离设备，可以有效对网络资源进行分区域管理。

针对第 b 条要求：SDP 控制器和所有 SDP 网关和 SDP 客户端之间的通讯都基于双向 TLS（mTLS），保障信息传输的安全。

针对第 c 条要求：SDP 控制器实时监控所有接入的客户端、网关以及自身的服务器状态，并且可以在后台提供集中检测的用户界面。

针对第 d 条要求：SDP 控制器上支持设置审计日志的保存时间，并且定期备份。

针对第 f 条要求：SDP 审计日志会基于身份进行上下文分析，识别安全事件，并告警。

2.4 四级安全通用要求

2.4.1 安全通用要求（四级）概述

《信息安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

信息系统的安全保护等级分为以下五级，一至五级等级逐级增高，其中明确说明，等级保护四级要求：“适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成损害。”

因此对于等级保护四级中通用安全部分，其具体的要求项和 SDP 适用子项如下表所示：

要求项	要求子项	SDP适用情况
9.1.1安全物理环境	9.1.1.1--9.1.1.10	不适用
9.1.2 安全通信网络	9.1.2.1 网络架构	适用见2.4.2.1
	9.1.2.2 通信传输	适用见2.4.2.2
	9.1.2.3 可信验证	不适用
9.1.3安全区域边界	9.1.3.1 边界防护	适用见2.4.2.3
	9.1.3.2 访问控制	适用见2.4.2.4
	9.1.3.3 入侵防范	适用见2.4.2.5
	9.1.3.4 恶意代码防范	不适用
	9.1.3.5 安全审计	适用见2.4.2.6

	9.1.3.6 可信验证	不适用
9.1.4 安全计算环境	9.1.4.1 身份鉴别	适用见2.4.2.7
	9.1.4.2 访问控制	适用见2.4.2.8
	9.1.4.3 安全审计	适用见2.4.2.9
	9.1.4.4 入侵防范	适用见2.4.2.10
	9.1.4.5 恶意代码防范	不适用
	9.1.4.6 可信验证	不适用
	9.1.4.7 数据完整性	适用见2.4.2.11
	9.1.4.8 数据保密性	适用见2.4.2.12
	9.1.4.9 数据备份恢复	不适用
	9.1.4.10 剩余信息保护	不适用
	9.1.4.10个人信息保护	不适用
9.1.5 安全管理中心	9.1.5.1 系统管理	不适用
	9.1.5.2 审计管理	不适用
	9.1.5.3 安全管理	不适用
	9.1.5.4 集中管控	适用见2.4.2.13
9.1.6 安全管理制度	9.1.6.1--9.1.6.4	不适用
9.1.7安全管理机构	9.1.7.1--9.1.7.4	不适用
9.1.8 安全管理人员	9.1.8.1--9.1.8.4	不适用
9.1.9 安全建设管理	9.1.9.1 --9.1.9.10	不适用
9.1.10 安全运维管理	9.1.10.1--9.1.10.14	不适用

2.4.2 对“9.1.2.1 网络架构”的适用策略

2.4.2.1 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。

2.4.2.1 SDP 的适用策略

针对第 a、e 条要求：属于硬件和网络运营商能力范畴，SDP 不适用。

针对第 c、d 条要求：SDP 提供应用层的边界防护，应用网关起到技术隔离作用。SDP 的应用对于不同的网络分区有特别的应用，由于 SDP 是通过 SDP 控制器来控制对应的连接访问，可以通过 SDP 的控制器来管理和控制对应的区域，同时对应的连接通过 SDP 客户端 和网关进行交互，大大提高了访问的可靠性和安全性。

对于安全边界的确定，SDP 有效的将其灵活性提高了，SDP 提供云平台和私有化部署，可以根据需要进行选择部署。SDP 实现的是边界防护，应用网关起到

技术隔离作用，将应用服务器保护在网关后面，使外界扫描工具和攻击来源无法探测到服务器地址和端口。SDP 将原本固化的边界模糊化以减小攻击面。

针对第 f 条要求:“应按照业务服务的重要程度分配带宽，优先保障重要业务”，可通过 SDP 网关定义业务流量的带宽分配；当出现带宽瓶颈时，对非关键业务系统进行限速，优先保障关键业务系统的带宽。

2.4.3 对“9.1.2.2 通信传输”的适用策略

2.4.3.1 本项要求包括:

a) 应采用校验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。

2.4.3.2 SDP 的适用策略

针对第 a 条要求：“应采用校验技术保证通信过程中数据的完整性”，传输过程使用双向 TLS（mTLS）加密传输，防止被篡改，保障数据的完整性。

针对第 b 条要求：“应采用密码技术保证通信过程中数据的保密性”，传输过程使用双向 TLS（mTLS）加密传输，防止被监听、窃取。mTLS 基于常见的密码学算法（如数字签名、散列、对称加密）。国际上使用 RSA、AES、SHA256 等通用算法来实现，而国内可以使用 SM2、SM3、SM4 等国密算法来实现。

针对第 c 条要求：“应在通信前基于密码技术对通信的双方进行验证或认证”，SDP 的传输过程使用双向 mTLS 进行加密传输，采用基于密码技术的数字证书及

数字签名来进行双向身份认证；具体应用为，在建立 TLS 握手过程中要求终端提交用户数字证书，服务端检测终端用户证书的合法性，同时终端也检测服务器数字证书的合法性。

针对第 d 条要求："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"，需启用支持国家规定的密码算法和密钥管理标准的 SDP 软件或设备，同时对密码算法和密钥管理功能，应由国家密码管理部门认证通过的硬件密码模块提供。SDP 客户和网关建立加密通信，SDP 客户端内置支持国密算法的 Ukey 等硬件密码模块，SDP 网关内置符合国家商用密码算法要求的加密卡，密码运算使用加密卡内置加密算法，且使用加密卡进行密钥管理。

2.4.4 对"9.1.3.1 边界防护"的适用策略

2.4.4.1 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。

2.4.4.2 SDP 的适用策略

针对第 a 条要求：SDP 作为软件定义的边界安全隔离产品，可以有效地提供跨越边界的安全访问以及跨越边界数据流的受控接口。由于独特的 SDP 三组件关系，数据流仅能通过特定的客户端和网关，且经合法授权后，方可进入另外一个内部网络。

针对第 b、c 条要求：SDP 秉承“先验证后连接”的原则，所有的终端设备首先要到 SDP 控制器上进行身份和设备的验证，才能被允许连接网关。当 SDP 网关部署在内部网络以及外部网络的边界上时，无论是外部的非授权设备私自联到内部网络，还是内部用户非授权联到外部网络，都可以被 SDP 网关阻止。

针对第 d 条要求：SDP 网关可以部署在无线网络以及企业资源所在网络的中间，只有通过 SDP 网关才能访问到企业的资源，对于非授权用户企业资源完全不可见，可以有效地防止非授权设备进入企业内部网络访问资源。

针对 f 条要求：SDP 控制器对所有接入的设备进行终端环境检查、用户行为检查、身份认证，保证接入到网络的设备是身份可信、终端可信、行为可信。

2.4.5 对“9.1.3.2 访问控制”的适用策略

2.4.5.1 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访问控制规则，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，以允许/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。

2.4.5.2 SDP 的适用策略

针对第 a 条要求：SDP 默认不信任任何网络、人、设备，均需进行验证，默认拒绝一切连接，只有验证合法的访问请求才被允许。并根据控制策略进行访问控制，仅对于验证合法用户，允许受控端口进行通信。即便合法的用户，也需要根据自己的权重分配账户和访问权限。

针对第 b 条要求：SDP 基于用户身份与授权进行精细化、颗粒度访问控制。

针对第 c 条要求：SDP 会对源地址、目的地址、源端口、目的端口和协议等进行检查，会基于上述信息进行访问控制，以允许符合条件的数据包通过，并拒绝不符合条件的数据包。

针对第 d 条要求：SDP 以身份化为基础，所以的访问请求都需要经过身份认证并植入会话状态信息，对所有访问流量会检测会话状态信息的合法性，仅允许携带合法会话状态信息的流量到达业务系统，拒绝非法访问。

针对第 e 条要求：应在网络边界部署 SDP 代理软件或网关设备，按照所部署访问策略对通信协议进行转换或隔离。

2.4.6 对“9.1.3.3 入侵防护”的适用策略

2.4.6.1 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。

2.4.6.2 SDP 的适用策略

针对第 a、b、c 条要求：SDP 网关部署在网络资源的关键位置，并且记录所有的资源访问日志，日志上传到 SDP 控制器，控制器对访问行为进行分析，发现并自动阻断网络攻击行为。

针对第 d 条要求：SDP 网关实时记录所有访问日志，日志内容包括源 IP 和端口、目标 IP 和端口，访问设备、访问时间等信息，同时对这些日志进行大数据智能分析并发出预警。

2.4.7 对“9.1.3.5 安全审计”的适用策略

2.4.7.1 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。

d) 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。

2.4.7.2 SDP 的适用策略

针对第 a、b 条要求：SDP 审计日志默认记录所有用户的所有访问日志，SDP 审计日志详细记录日期时间、用户、事件详情信息。

针对第 c 条要求：SDP 控制器上支持设置审计日志的保存时间，并且定期备份。

针对第 d 条要求：SDP 网关部署在网络边界上，无论是远程访问的用户还是内网用户访问互联网都经过网关，网关可以对每个用户的行为做单独审计以及数据分析。

2.4.8 对“9.1.4.1 身份鉴别”的适用策略

2.4.8.1 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。

2.4.8.2 SDP 的适用策略

针对第 a 条要求：SDP 支持多因素认证，保证身份不易被冒用，并对密码复杂度有强制要求。

针对第 b 条：SDP 对登录认证有防爆破保护，以及连接超时自动注销保护。

针对第 c 条：SDP 对所有数据都使用双向 TLS（mTLS）加密传输，防止数据在网络传输过程中被窃听。

针对第 d 条：SDP 支持多因素认证，包括口令、短信、动态令牌、证书、UKey 等。

2.4.9 对“9.1.4.2 访问控制”的适用策略

2.4.9.1 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) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

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问。

2.4.9.2 SDP 的适用策略

针对第 a，b 条要求：SDP 属于访问控制类别产品，对所有的用户访问都会进行授权校验。

针对第 c,d 条：SDP 对账号会设置过期时间，对于长时间不登录的账号会禁止登录。

针对第 e 条：SDP 通过授权策略实现主体（用户）访问客体（业务系统）的访问控制。

针对第 f 条：SDP 的主体为用户，能实现用户级的的访问控制。同时支持进程级的安全检查，基于检查结果进行访问控制。同时客体为业务系统，并支持控制粒度细致到 url 级别。

针对第 g 条：应基于 SDP 的认证机制，对网络中的主体和客体定义基于身份的安全标记，并按照主体和客体的访问关系设置访问控制规则。

2.4.10 对“9.1.4.3 安全审计”的适用策略

2.4.10.1 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、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。

d) 应对审计进程进行保护，防止未经授权的中断。

2.4.10.2 SDP 的适用策略

针对第 a、b 条要求：SDP 审计日志默认记录所有用户的所有访问日志，SDP 审计日志详细记录日期时间、用户、事件详情信息。

针对第 c 条：SDP 控制器上支持设置审计日志的保存时间，并且定期备份。

针对第 d 条要求：SDP 审计模块通过监控程序相互保护，在发生异常中断时会通过监控程序拉起。

2.4.11 对“9.1.4.4 入侵防护”的适用策略

2.4.11.1 本项要求包括：

a) 应遵循最小安装的原则，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。

2.4.11.2 SDP 的适用策略

针对第 a、b 条要求：SDP 本身的特性就默认关闭所有端口，拒绝一切连接，不存在共享和高危的端口，应用网关仅面向授权客户端开放访问权限，极大地控制了使用范围，减小了暴露面。通过客户端和控制器，可检测到入侵的行为，并在发生严重入侵事件时提供预警。

针对第 c 条要求：SDP 客户端在连接网关之前需要先去控制器进行身份和设备的验证，控制器可以对终端的接入方式或网络地址范围进行有效控制。

针对第 d 条要求：SDP 客户端和 SDP 网关之间使用特殊的通信协议以及加密(mTLS)的数据传输，以保证数据的正确性和有效性。

针对第 e 条要求：SDP 三组件（客户端、网关、控制器）支持自动更新和升级，保证可以及时修补漏洞。

针对第 f 条要求：SDP 网关部署在重要节点上，会实时分析用户行为，发现异常入侵行为，并阻断和告警。

2.4.12 对“9.1.4.7 数据完整性”的适用策略

2.4.12.1 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。

c) 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

2.4.12.2 SDP 的适用策略

针对第 a 条要求：SDP 通过双向 TLS（mTLS）进行数据加密传输，mTLS 基于密码技术，可以有效保障数据的完整性。

针对第 c 条要求：在网络边界通过部署 SDP 网关，记录访问过程，并增加对访问过程的主体的基于密码学的数字签名机制，以满足可追溯的抗抵赖特性。

2.4.13 对“9.1.4.8 数据保密性”的适用策略

2.4.13.1 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。

2.4.13.2 SDP 的适用策略

针对第 a 条要求：SDP 通过双向 TLS（mTLS）进行数据加密传输。mTLS 基

于密码技术，可以有效保障数据的保密性。

2.4.14 对“9.1.5.4 集中管控”的适用策略

2.4.14.1 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。

2.4.14.2 SDP 的适用策略

针对第 a 条要求：SDP 控制器对所有接入的 SDP 网关和 SDP 客户端进行集中管控，SDP 网关作为边界隔离设备，可以有效对网络资源进行分区域管理。

针对第 b 条要求：SDP 控制器和所有 SDP 网关和 SDP 客户端之间的通讯都基于双向 TLS（mTLS），保障信息传输的安全。

针对第 c 条要求：SDP 控制器实时监控所有接入的客户端、网关以及自身的服务器状态，并且可以在后台提供集中检测的用户界面。

针对第 d 条要求：SDP 控制器上支持设置审计日志的保存时间，并且定期备

份。

针对第 f 条要求：SDP 审计日志会基于身份进行上下文分析，识别安全事件，并告警。

2.4.15 SDP 应用于等级保护（四级）的合规注意事项

SDP 应用于等级保护四级系统时，应注意参照相关的国家或行业标准来选择落地方案的产品和方案功能。等保条例依据《网络产品和服务安全审查办法（试行）》和《网络关键设备和网络安全专用产品目录》，要求第三级及以上网络的网络运营者应采用与其安全保护等级相适应的网络产品和服务，对重要部位使用的网络产品应通过专业机构的测评或认证。

SDP 在执行层面以密码技术作为支撑性技术，包括身份认证、授权管理、安全传输、安全审计等功能，其内部均采用了相应的密码技术。等保四级系统属于较高的安全等级系统，在上一节的分析中我们可以看到，在等保四级系统中，对密码技术的深入应用和合规要求相较其他级别更为突出和明确，因此在采用 SDP 构建四级系统时，需要重点关注密码技术对 SDP 安全能力的提升，并充分考虑密码国家标准或行业标准的约束。同时，绝大多数涉及国家安全、国计民生、社会公共利益或重要领域的核心业务，也会与关键基础设施的范围存在较大的重叠，在 2020 年生效的密码法作如下规定：

“第二十七条　法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测

评。”

在此文发表的时间段，还没有明确的关于密码应用安全性评估与等保测评的关系表述，但随着法律实施效果的显现，可以预见 SDP 在高安全等级网络中的应用会要求满足对应的密码测评要求。在等级保护四级以上系统中，应注意 SDP 所采用的密码算法，密钥管理和密码产品或模块应用的合规性。

此外，等级保护 2.0 标准体系中要求信息安全产品和密码产品与服务的采购使用应符合国家有关规定。因此，SDP 的实施者应当明确自己采购、使用或租用的产品的合规情况，以及外部网络服务提供者的相关资质，了解可能存在的安全风险。

需要特殊注意的是，在密码国家标准《GM/T0054-2018 信息系统密码应用基本要求》第 7.2.5 节中，等保四级系统相较三级系统的增加要求如下：

“应基于符合 GM/T0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。”

在 SDP 中常见的密码模块或密码产品包括但不限于：TPM 芯片、密码卡、密码机、VPN、安全网关、密码中间件、软件密码模块、密钥管理系统等。根据标准的要求，在四级系统中构建 SDP，应自查所采用的密码模块或密码产品是否满足三级以上的产品资质要求。

3 SDP 满足等保 2.0 云计算安全扩展要求

3.1 概述

在云计算环境中，由于计算、存储和网络等元素都被资源池化，虚拟机所在的物理位置和网络位置都可能频繁发生变化，因而造成了传统的网络安全防护手段无法有效应对云计算环境的情况。云计算环境中由于其资源规模决定了承载业务的种类和数量也非常庞大，多租户资源共享也决定了不能像已有的技术按照资源的物理位置、固定的网络访问接入以及静态的身份信任验证体系来架构云计算环境的安全。因此，在等保 2.0 的技术合规要求中，除了基本要求外，针对云计算还有单独的扩展要求。

除了在云计算环境内部，云的用户也与传统环境有着显著的不同。云的用户总是来自于云外，这意味着用户都是远程接入到云中来的，很难保证他们都有固定的网络地址，需要能够动态的赋予用户访问权限。

云环境本身和云的用户都存在很大的不确定性，使得安全通信网络成为了等级保护 2.0 中最具挑战性的部分之一。

软件定义边界（SDP）恰好给这种情况提供了一种行之有效的应对思路。与一般的先建立连接，然后进行鉴权的方式不同，SDP 要求首先进行身份鉴别，确定对应的访问权限和策略，然后才允许与相对应的服务建立连接。SDP 是以用户为中心的，而没有基于预设的发起方（IH）和接受方（AH）的地址，因而能够在内外部环境，尤其是网络地址和拓扑都持续发生变化的情况下，提供可靠的隔离和访问控制手段。CSA 提出采用以身份体系代替物理位置、网络区域的 SDP

零信任架构逐渐获得业界认可。

虽然 SDP 的具体实现方式不在本文的讨论范围之内，但是 SDP 控制器（Controller）和 SDP 网关（Gateway）的形态确实对其部署位置有较大的影响，而这又进而关系到 SDP 在什么层面上，实现了什么粒度的访问控制能力。因此，在叙述 SDP 在云计算环境中的适用策略之前，我们需要根据 SDP 网关的形态和部署位置，将 SDP 的在云计算环境下的部署分为以下几种方式。

- 内嵌式部署：SDP 网关以插件的形式部署在每个虚拟机上。这种部署方式下用户能够定义任意两台虚拟机之间的访问策略，从而实现虚机级别的细粒度隔离和访问控制。但这种部署方式需要将 Agent 内嵌到用户的系统中，并占用部分用户计算资源。
- 虚拟网元部署：SDP 网关作为单独的网元部署在云计算环境中。可以是虚拟化部署在每台宿主机上（可为不同宿主机上的虚机提供隔离和访问控制）或者每个租户私有网络内（可为不同租户间的虚机提供隔离和访问控制），取决于用户所需的访问策略需求。
- 物理网元部署：SDP 网关以单独形态部署在云边界。这种部署方式提供的隔离和访问控制粒度较粗，能够实现云内云外互访的访问策略需求。

用户可以根据实际环境需要，选择其中的一种方式或组合使用几种方式部署 SDP Gateway。

接下来的章节将分别介绍 SDP 在等级保护 2.0 中对第二、三、四级云计算安全扩展要求的适用情况和具体适用策略。

3.2 云计算安全扩展二级要求

等级保护 2.0 第二级要求中， SDP 能够帮助用户满足或部分满足的条目如下表所示。

要求项	要求子项	SDP适用情况
7.2.1 安全物理环境	7.2.1.1 基础设施位置	不适用
7.2.2 安全通信网络	7.2.2.1 网络架构	适用，见3.0
7.2.3 安全区域边界	7.2.3.1 访问控制	适用，见3.0
	7.2.3.2 入侵防范	适用，见3.0
	7.2.3.3 安全审计	适用，见3.0
7.2.4 安全计算环境	7.2.4.1 访问控制	适用，见3.0
	7.2.4.2 镜像和快照保护	不适用
	7.2.4.3 数据完整性和保密性	不适用
	7.2.4.4 数据备份恢复	不适用
	7.2.4.5 剩余信息保护	不适用
7.2.5 安全建设管理	7.2.5.1 云服务商选择	不适用
	7.2.5.2 供应链管理	不适用
7.2.6 安全运维管理	7.2.6.1 云计算环境管理	不适用

3.2.1 对“7.2.2.1 网络架构”的适用策略

3.2.1.1 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。

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。

3.2.1.2 SDP 的适用策略

可通过内嵌式或虚拟网元部署 SDP 网关满足:

采用内嵌式部署或虚拟网元部署（于每个租户私有网络内）的方式部署 SDP 网关，能够帮助满足 b)项的隔离的要求。SDP 控制器和网关保证用户设备的 SDP 客户端只能连接到有访问权限的对应云服务，不同客户的用户及其对应的云服务对其他云服务客户隐藏，“拒绝所有”的防火墙和强制的单包授权（SPA）机制能够实现不同业务的充分隔离。

SDP 架构强制要求所有的数据通信采用双向 TLS（mTLS）或 IPsec/IKE 机制保证云服务客户的用户与服务之间始终通过采用强加密隧道，保证通信传输安全，实现 c)中通信传输保护；通过控制器下发安全策略，可以细粒度配置用户的传输参数(如加密套件)。SDP 不实现静态的基于物理位置的安全边界保护，不实现传统意义上分区保护，取而代之的，是以用户为中心，动态定义应用访问的范围。传统的物理网络的边界已被打破，实现了更具弹性，动态变化的边界保护；SDP 在架构定义上，不强调入侵检测，入侵防范。“拒绝所有”的防火墙和强制的

单包授权（SPA）机制能有效防止入侵，且完善的日志和访问记录将记录入侵者留下的痕迹，攻击者入侵时被 SDP 丢弃的数据包也会提供可以被用于分析的证据和数据，用以改善防御和/或起诉攻击者。

3.2.2 对“7.2.3.1 访问控制”的适用策略

3.2.2.1 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。

3.2.2.2 SDP 的适用策略

可通过内嵌式、虚拟网元或物理网元部署 SDP 网关满足:

SDP 网关因实现代理的层次不同，可以实现网络层到应用层不同协议层级的访问控制。以 SDP 网关为边界，隐藏服务/服务器。SDP 提供严格的访问控制机制，用户和客户需要使用的云服务只有在向 SDP 控制器和网关环境中注册后才能访问，且用户只能通过确定的客户端才能访问有适当访问权限的服务。

3.2.3 对“7.2.3.2 入侵防范”的适用策略

3.2.3.1 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。

3.2.3.2 SDP 的适用策略

可通过内嵌式部署 SDP 网关部分满足：

用户及其使用的设备必须在 SDP 控制器注册，且在访问服务时经过严格验证。通过内嵌式部署 SDP 网关，可以帮助用户迅速检测虚拟机与宿主机、虚拟机与虚拟机之间不符合访问策略的异常访问行为，并提供攻击的具体记录，部分满足本项中的要求。

对于符合访问策略的网络攻击行为，SDP 需要结合行为日志大数据分析的软件，通过对用户行为的建模以及异常检测，发现攻击行为并且发出预警。

3.2.4 对“7.2.3.3 安全审计”的适用策略

3.2.4.1 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。

3.2.4.2 SDP 的适用策略

可通过内嵌式、虚拟网元部署 SDP 网关部分满足：

云服务商和云计算客户需要经过 SDP 网关实现云资源远程管理以及数据的操作，识别相关管理操作行为，以日志的方式保存到 SDP 控制器，满足 a)和 b)

项要求。

3.2.5 对“7.2.4.1 访问控制”的适用策略

3.2.5.1 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。

3.2.5.2 SDP 的适用策略

可通过内嵌式部署 SDP 网关满足:

虚拟机在迁移时，若其网络地址不发生变化，则原访问控制策略将仍然生效；若其网络地址发生变化，将重新触发到 SDP 控制器的认证，访问策略也将随之更新。云服务客户可以通过 SDP 控制器集中配置不同虚拟机之间的访问控制策略。

3.3 云计算安全扩展三级要求

等级保护 2.0 第三级要求中，SDP 能够帮助用户满足或部分满足的条目如下表所示。

要求项	要求子项	SDP适用情况
8.2.1 安全物理环境	8.2.1.1 基础设施位置	不适用
8.2.2 安全通信网络	8.2.2.1 网络架构	部分适用，见3.0
8.2.3 安全区域边界	8.2.3.1 访问控制	适用，见3.0
	8.2.3.2 入侵防范	适用，见3.0

	8.2.3.3 安全审计	适用，见3.0
8.2.4 安全计算环境	8.2.4.1 身份鉴别	适用，见3.0
	8.2.4.2 访问控制	适用，见3.0
	8.2.4.3 入侵防范	适用，见3.0
	8.2.4.4 镜像和快照保护	不适用
	8.2.4.5 数据完整性和保密性	不适用
	8.2.4.6 数据备份恢复	不适用
	8.2.4.7 剩余信息保护	不适用
8.2.5 安全管理中心	8.2.5.1 集中管控	部分适用，见3.0
8.2.6 安全建设管理	8.2.6.1 云服务商选择	不适用
	8.2.6.2 供应链管理	不适用
8.2.7 安全运维管理	8.2.7.1 云计算环境管理	不适用

3.3.1 对“8.2.2.1 网络架构”的适用策略

3.3.1.1 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。

3.3.1.2 SDP 的适用策略

可通过内嵌式或虚拟网元部署 SDP 网关部分满足：

采用内嵌式部署或虚拟网元部署（于每个租户私有网络内）的方式部署 SDP 网关，能够帮助满足 b)项的隔离的要求。SDP 控制器和网关保证用户设备的 SDP 客户端只能连接到有访问权限的对应云服务，不同客户的用户及其对应的云服务对其他云服务客户隐藏，“拒绝所有”的防火墙和强制的单包授权（SPA）机制能够实现不同业务的充分隔离。

SDP 架构强制要求所有的数据通信采用双向 TLS（mTLS）或 IPsec/IKE 机制保证云服务客户的用户与服务之间始终通过采用强加密隧道，保证通信传输安全，实现 c)中通信传输保护；通过控制器下发安全策略，可以细粒度配置用户的传输参数(如加密套件)。SDP 不实现静态的基于物理位置的安全边界保护，不实现传统意义上分区保护，取而代之的，是以用户为中心，动态定义应用访问的范围。传统的物理网络的边界已被打破，实现了更具弹性，动态变化的边界保护；SDP 在架构定义上，不强调入侵检测，入侵防范。“拒绝所有”的防火墙和强制的单包授权（SPA）机制能有效防止入侵，且完善的日志和访问记录将记录入侵者留下的痕迹，攻击者入侵时被 SDP 丢弃的数据包也会提供可以被用于分析的证据和数据，用以改善防御和/或起诉攻击者。

SDP 控制器实现安全控制中心功能，能够帮助满足 d）项的要求。它能够确定用户的客户端设备及云服务客户业务之间的对应关系，具备统一安全策略配置

管理能力。它能够支持云服务客户根据业务需求自主设置安全策略和访问方式，包括定义访问路径、选择安全组件、配置安全策略。同时，SDP 控制器，可以跟云平台配合，将 SDP 网关与业务实现自动网络编排。

a）和 e）项要求属于管理实践的范畴，不在 SDP 支持的范围之内，还需要结合其他措施实现本项的要求。

3.3.2 对“8.2.3.1 访问控制”的适用策略

3.3.2.1 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。

3.3.2.2 SDP 的适用策略

可通过内嵌式、虚拟网元或物理网元部署 SDP 网关满足:

SDP 网关因实现代理的层次不同，可以实现网络层到应用层不同协议层级的访问控制。以 SDP 网关为边界，隐藏服务/服务器。SDP 提供严格的访问控制机制，用户和客户需要使用的云服务只有在向 SDP 控制器和网关环境中注册后才能访问，且用户只能通过确定的客户端才能访问有适当访问权限的服务。

3.3.3 对“8.2.3.2 入侵防范”的适用策略

3.3.3.1 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。

3.3.3.2 SDP 的适用策略

可通过内嵌式部署 SDP 网关满足：

用户及其使用的设备必须在 SDP 控制器注册，且在访问服务时经过严格验证。通过内嵌式部署 SDP 网关，可以帮助用户迅速检测虚拟机与宿主机、虚拟机与虚拟机之间不符合访问策略的异常访问行为，并提供攻击的具体记录，部分满足本项中的要求。

对于符合访问策略的网络攻击行为，SDP 需要结合行为日志大数据分析的软件，通过对用户行为的建模以及异常检测，发现攻击行为并且发出预警。

3.3.4 对“8.2.3.3 安全审计”的适用策略

3.3.4.1 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。

3.3.4.2 SDP 的适用策略

可通过内嵌式、虚拟网元部署 SDP 网关部分满足：

云服务商和云计算客户需要经过 SDP 网关实现云资源远程管理以及数据的操作，识别相关管理操作行为，以日志的方式，保存到 SDP 控制器，满足 a）和 b）项要求。

3.3.5 对“8.2.4.1 身份鉴别”的适用策略

3.3.5.1 本项要求包括：

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。

3.3.5.2 SDP 的适用策略

可通过内嵌式、虚拟网元部署 SDP 网关满足：

SDP 保护云计算平台及其中的设备，对未经授权的远程管理终端不可见。采用任意一种部署方式，管理终端和云计算平台均需与 SDP 控制器进行身份认证，方能建立连接进行访问，即可满足本项要求。强制双向 TLS（mTLS）通信方式，而 mTLS 本身就是一个双向身份认证的机制，确保通信传输安全。

云计算平台可集成 SDP 控制器，并提供网关。

3.3.6 对“8.2.4.2 访问控制”的适用策略

3.3.6.1 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。

3.3.6.2 SDP 的适用策略

可通过内嵌式部署 SDP 网关满足:

虚拟机在迁移时，若其网络地址不发生变化，则原访问控制策略将仍然生效；若其网络地址发生变化，将重新触发到 SDP 控制器的认证，访问策略也将随之更新。云服务客户可以通过 SDP 控制器集中配置不同虚拟机之间的访问控制策略。

3.3.7 对“8.2.4.3 入侵防范”的适用策略

3.3.7.1 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。

3.3.7.2 SDP 的适用策略

可通过内嵌式部署 SDP 网关部分满足:

通过内嵌式部署 SDP 网关，可以帮助用户检测虚拟机与宿主机、虚拟机与

虚拟机之间不符合访问策略的异常访问行为，满足本项中 a)、b)的要求，满足本项中 c)的要求。

SDP 无法直接检测恶意代码的感染，但是感染恶意代码的虚机，要实现虚机之间的蔓延，需要触发相应的网络的请求。这类请求首先需要获得 SDP 控制器授权，虚机之间的直接访问，会被直接拒绝或者通过 SPA 机制，实现静默丢弃。这在很大程度上，可以阻止恶意代码在虚机间的蔓延。

SDP 客户端软件保证只有合法连接才能建立，并能够及时检测非法连接（资源隔离失效）和非法连接尝试（非授权新建虚拟机或者重新启用虚拟机），并进行记录和告警。

3.3.8 对“8.2.5.1 集中管控”的适用策略

3.3.8.1 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量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。

3.3.8.2 SDP 的适用策略

SDP 作为网络隔离和访问控制的手段，通过 SDP 控制器进行集中配置，因此可作为集中管控的一部分，部分满足本项中的相关要求。

云计算平台管理与云服务业务是两种不同的业务，由不同的业务服务/服务器提供。云计算平台管理流量和云服务业务流量分别从不同的用户端设备流向不同的目标服务/服务器，SDP 将目标服务/服务器隐藏，用户只能从确定的客户端设备才能发现对应的隐藏服务/服务器并发起访问；类似的，被隐藏的服务/服务器只会接受对应的用户从确定的客户端设备发起的连接。

3.4 云计算安全扩展四级要求

等级保护 2.0 第四级要求中， SDP 能够帮助用户满足或部分满足的条目如下表所示。

要求项	要求子项	SDP适用情况
9.2.1 安全物理环境	9.2.1.1 基础设施位置	不适用
9.2.2 安全通信网络	9.2.2.1 网络架构	适用，见0
9.2.3 安全区域边界	9.2.3.1 访问控制	适用，见0
	9.2.3.2 入侵防范	适用，见0
	9.2.3.3 安全审计	部分适用，见0
9.2.4 安全计算环境	9.2.4.1 身份鉴别	适用，见0
	9.2.4.2 访问控制	适用，见0
	9.2.4.3 入侵防范	适用，见0
	9.2.4.4 镜像和快照保护	不适用
	9.2.4.5 数据完整性和保密	不适用

	性	
	9.2.4.6 数据备份恢复	不适用
	9.2.4.7 剩余信息保护	不适用
9.2.5 安全管理中心	9.2.5.1 集中管控	适用，见0
9.2.6 安全建设管理	9.2.6.1 云服务商选择	不适用
	9.2.6.2 供应链管理	不适用
9.2.7 安全运维管理	9.2.7.1 云计算环境管理	不适用

3.4.1 对“9.2.2.1 网络架构”的适用策略

3.4.1.1 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。

3.4.1.2 SDP 的适用策略

可通过内嵌式或虚拟网元部署 SDP 网关部分满足：

采用内嵌式部署或虚拟网元部署（于每个租户私有网络内）的方式部署 SDP 网关，能够帮助满足 b)、f)两项的隔离和访问控制要求。

SDP 控制器和网关保证用户设备的 SDP 客户端只能连接到有访问权限的对应云服务，不同客户的用户及其对应的云服务对其他云服务客户隐藏，“拒绝所有”的防火墙和强制的单包授权（SPA）机制能够实现不同业务的充分隔离。

SDP 架构强制要求所有的数据通信采用双向 TLS（mTLS）或 IPsec/IKE 机制保证云服务客户的用户与服务之间始终通过采用强加密隧道，保证通信传输安全，实现 c)中通信传输保护；通过控制器下发安全策略，可以细粒度配置用户的传输参数(如加密套件)。SDP 不实现静态的基于物理位置的安全边界保护，不实现传统意义上分区保护，取而代之的，是以用户为中心，动态定义应用访问的范围。传统的物理网络的边界已被打破，实现了更具弹性，动态变化的边界保护；SDP 在架构定义上，不强调入侵检测，入侵防范。“拒绝所有”的防火墙和强制的单包授权（SPA）机制能有效防止入侵，且完善的日志和访问记录将记录入侵者留下的痕迹，攻击者入侵时被 SDP 丢弃的数据包也会提供可以被用于分析的证据和数据，用以改善防御和/或起诉攻击者。

SDP 控制器实现安全控制中心功能，能够帮助满足 d)项的要求。它能够确定用户的客户端设备及云服务客户业务之间的对应关系，具备统一安全策略配置

管理能力。它能够支持云服务客户根据业务需求自主设置安全策略和访问方式，包括定义访问路径、选择安全组件、配置安全策略。同时，SDP 控制器，可以跟云平台配合，将 SDP 网关与业务实现自动网络编排。

a）和 e）项要求属于管理实践的范畴，不在 SDP 支持的范围之内，还需要结合其他措施实现本项的要求。

3.4.2 对“9.2.3.1 访问控制”的适用策略

3.4.2.1 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。

3.4.2.2 SDP 的适用策略

可通过内嵌式、虚拟网元或物理网元部署 SDP 网关满足:

等级保护 2.0 中的第四级要求不同等级的网络必须物理隔离，因此，采用物理网元部署的 SDP 网关即可满足本项所有要求。

3.4.3 对“9.2.3.2 入侵防范”的适用策略

3.4.3.1 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。

3.4.3.2 SDP 的适用策略

可通过内嵌式部署 SDP 网关满足：

用户及其使用的设备必须在 SDP 控制器注册，且在访问服务时经过严格验证。通过内嵌式部署 SDP 网关，可以帮助用户迅速检测虚拟机与宿主机、虚拟机与虚拟机之间不符合访问策略的异常访问行为，并提供攻击的具体记录，部分满足本项中从 c)、d)的要求。

对于符合访问策略的网络攻击行为，SDP 需要结合行为日志大数据分析的软件，通过对用户行为的建模以及异常检测，发现攻击行为并且发出预警。

3.4.4 对“9.2.3.3 安全审计”的适用策略

3.4.4.1 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。

3.4.4.2 SDP 的适用策略

可通过内嵌式、虚拟网元部署 SDP 网关部分满足：

云服务商和云计算客户需要经过 SDP 网关实现云资源远程管理和数据的操

作，识别相关管理操作行为，以日志的方式，保存到 SDP 控制器，满足 a）和 b）项要求。

3.4.5 对“9.2.4.1 身份鉴别”的适用策略

3.4.5.1 本项要求包括:

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。

3.4.5.2 SDP 的适用策略

可通过内嵌式、虚拟网元或物理网元部署 SDP 网关满足:

SDP 保护云计算平台及其中的设备，对未经授权的远程管理终端不可见。采用任意一种部署方式，管理终端和云计算平台均需与 SDP 控制器进行身份认证，方能建立连接进行访问，即可满足本项要求。强制双向 TLS（mTLS）通信方式，而 mTLS 本身就是一个双向身份认证的机制，确保通信传输安全。

云计算平台可集成 SDP 控制器，并提供网关。

3.4.6 对“9.2.4.2 访问控制”的适用策略

3.4.6.1 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。

3.4.6.2 SDP 的适用策略

可通过内嵌式部署 SDP 网关满足：

虚拟机在迁移时，若其网络地址不发生变化，则原访问控制策略将仍然生效；若其网络地址发生变化，将重新触发到 SDP 控制器的认证，访问策略也将随之更新。云服务客户可以通过 SDP 控制器集中配置不同虚拟机之间的访问控制策略。

3.4.7 对“9.2.4.3 入侵防范”的适用策略

3.4.7.1 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。

3.4.7.2 SDP 的适用策略

可通过内嵌式部署 SDP 网关部分满足：

通过内嵌式部署 SDP 网关，可以帮助用户检测虚拟机与宿主机、虚拟机与虚拟机之间不符合访问策略的异常访问行为，满足本项中 a)、b)的要求，满足本项中 c)的要求。

SDP 无法直接检测恶意代码的感染，但是感染恶意代码的虚机，要实现虚机之间的蔓延，需要触发相应的网络的请求。这类请求首先需要获得 SDP 控制器授权，虚机之间的直接访问，会被直接拒绝或者通过 SPA 机制，实现静默丢弃。

这在很大程度上，可以阻止恶意代码在虚机间的蔓延。

SDP 客户端软件保证只有合法连接才能建立，并能够及时检测非法连接（资源隔离失效）和非法连接尝试（非授权新建虚拟机或者重新启用虚拟机），并进行记录和告警。

3.4.8 对“9.2.5.1 集中管控”的适用策略

3.4.8.1 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量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。

3.4.8.2 SDP 的适用策略

SDP 作为网络隔离和访问控制的手段，通过 SDP 控制器进行集中配置，因此可作为集中管控的一部分，部分满足本项中的相关要求。

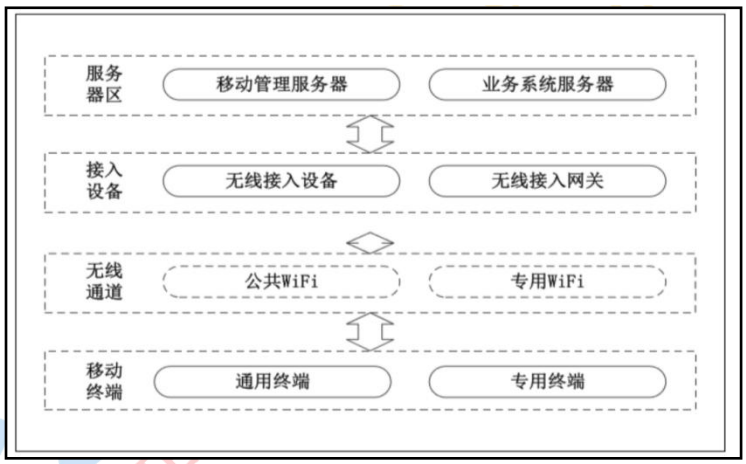
云计算平台管理与云服务业务是两种不同的业务，由不同的业务服务/服务器提供。云计算平台管理流量和云服务业务流量分别从不同的用户端设备流向不同的目标服务/服务器，SDP 将目标服务/服务器隐藏，用户只能从确定的客户端设备才能发现对应的隐藏服务/服务器并发起访问；类似的，被隐藏的服务/服务器只会接受对应的用户从确定的客户端设备发起的连接。

4 SDP 满足等保 2.0 移动互联安全扩展要求

4.1 概述

“等保 2.0”对移动互联应用场景进行了说明，指出采用移动互联技术的等级保护对象其移动互联部分由移动终端、移动应用和无线网络三部分组成，移动终端通过无线通道连接无线接入设备接入，无线接入网关通过访问控制策略限制移动终端的访问行为，后台的移动终端管理系统负责对移动终端的管理，包括向客户端软件发送移动设备管理、移动应用管理和移动内容管理策略等。

移动互联应用架构如下图所示：



图：移动互联应用架构

移动互联安全扩展要求是针对移动终端、移动应用和无线网络提出的特殊安全要求，它们与安全通用要求一起构成针对采用移动互联技术的等级保护对象的完整安全要求。移动互联安全扩展要求涉及的控制点包括无线接入点的物理位置、无线和有线网络之间的边界防护、无线和有线网络之间的访问控制、无线和

有线网络之间的入侵防范，移动终端管控、移动应用管控、移动应用软件采购、移动应用软件开发和配置管理。

软件定义边界（SDP）基于零信任安全理念，可以很好的保护跨网络的安全性。与一般的先建立连接，然后进行鉴权的方式不同，SDP 要求首先进行身份鉴别，确定对应的访问权限和策略，然后才允许与相对应的服务建立连接，无论是在固定网络和移动网络，都能提供可靠的隔离和访问控制。

在移动互联网扩展中，可以采用多种 SDP 部署方式。

- 内嵌式部署：SDP 功能以插件的形式部署在移动互联网终端和移动应用服务端。这种部署方式下用户能够定义任意两台设备之间的访问策略，从而实现终端级别的细粒度隔离和访问控制。但这种部署方式需要将 Agent 内嵌到用户的系统中，并占用部分用户计算资源。
- 应用侧网关部署：SDP 网关作为单独的网元部署在移动互联网环境中，部署在移动应用服务端前端位置。SDP 网关和移动互联网服务端通过可信网络连接。SDP 网关方式可以方便的实现应用侧的过渡，而不需要服务端更改。
- 移动互联网侧网关部署：SDP 网关作为单独的网元部署在移动互联网环境中，部署在移动互联网网络汇聚出口处。SDP 网关和移动终端通过一定的安全机制保障网络隔离和访问控制。汇聚网关模式可以支持未支持 SDP 的移动终端使用已经开启 SDP 的移动互联网应用服务。

用户可以根据实际环境需要，选择其中的一种方式或组合使用几种方式部署 SDP 网关。

SDP 对标移动互联安全扩展要求：

对标《GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求》中“7.3 移动互联安全扩展要求”部分内容、“8.3 移动互联安全扩展要求”部分内容、“9.3 移动互联安全扩展要求”部分内容，按照 SDP 标准规范描述，SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在后续章节详细阐述。

要求项	要求子项	SDP适用情况
7.3 移动互联安全扩展要求（二级）		
7.3.1 安全物理环境	7.3.1.1无线接入点的物理位置	不适用
7.3.2 安全区域边界	7.3.2.1 边界防护	适用
	7.3.2.2 访问控制	适用
	7.3.2.3 入侵防范	部分适用
7.3.3 安全计算环境	7.3.3.1 移动应用管控	不适用
7.3.4 安全建设管理	7.3.4.1 移动应用软件采购	不适用
	7.3.4.2 移动应用软件开发	不适用
8.3 移动互联安全扩展要求（三级）		
8.3.1 安全物理环境	8.3.1.1无线接入点的物理位置	不涉及
8.3.2 安全区域边界	8.3.2.1 边界防护	适用
	8.3.2.2 访问控制	适用
	8.3.2.3 入侵防范	部分适用，“无线接入设备的SSID广播、WPS等高

		风险功能"检测和禁止未覆盖
8.3.3 安全计算环境	8.3.3.1 移动终端管控	部分适用，“移动终端远程管控（如：远程锁定、远程擦除等）”未涵盖；
	8.3.3.2 移动应用管控	部分适用，“根据白名单控制应用软件安装、运行”未覆盖
8.3.4 安全建设管理	8.3.4.1 移动应用软件采购	部分适用，SDP组件验证要求严格，符合采购要求可通过验证。
	8.3.4.2 移动应用软件开发	部分适用，SDP组件验证要求严格，符合开发要求可通过验证。
8.3.5 安全运维管理	8.3.5.1配置管理	适用

4.2 移动互联安全扩展二级要求

等级保护 2.0 中第二级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在后续分节详细阐述。

要求项	要求子项	SDP 适用情况
7.3.1 安全物理环境	7.3.1.1 无线接入点的物理位置	不适用
7.3.2 安全区域边界	7.3.2.1 边界防护	适用，见 4.2.1
	7.3.2.2 访问控制	适用，见 4.2.2
	7.3.2.3 入侵防范	部分适用，见 4.2.3
7.3.3 安全计算环境	7.3.3.1 移动应用管控	部分适用，“根据白名单控制应用软件安装、运行”未覆盖，见 4.2.4
7.3.4 安全建设管理	7.3.4.1 移动应用软件采购	部分适用，SDP 组件验证要求严格，符合采购要求可通过验证，见 4.2.5
	7.3.4.2 移动应用软件开发	部分适用，见 4.2.6

4.2.1 对“7.3.2.1 边界防护”的适用策略

4.2.1.1 本项要求包括:

a) 应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

4.2.1.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能满足 a)访问和数据流通过无线接入网关设备的要求。无线终端作为 SDP 客户端，使用 SDP 网关作为无线接入网关。

4.2.2 对“7.3.2.2 访问控制”的适用策略

4.2.2.1 本项要求包括:

a) 无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符；

4.2.2.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能满足 a)的访问控制要求。

SDP 中每次会话都需要认证后连接，天然支持接入认证。根据等级保护 2.0 中要求，SDP 认证应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

4.2.3 对“7.3.2.3 入侵防范”的适用策略

4.2.3.1 本项要求包括:

a) 应能够检测到非授权无线接入设备和非授权移动终端的接入行为。

b) 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。

c) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。

d) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等;

e) 应禁止多个 AP 使用同一个认证密钥。

4.2.3.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能部分满足:

a）和 b)要求：由于 SDP 采用先认证后接入的方式，天然拒绝非授权连接，而非检测。可以拒绝非授权接入、网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。

c) 要求：SDP 不适用，依赖无线设备自身功能。

d）和 e)要求： SDP 不适用，属于管理范畴。

对于符合访问策略的网络攻击行为，SDP 需要结合用户行为日志大数据分析软件，发现异常行为并且发出预警。

4.2.4 对“7.3.3.1 移动应用管控”的适用策略

4.2.4.1 本项要求包括:

a) 应具有选择应用软件安装、运行的功能。

b) 应只允许可靠证书签名的应用软件安装和运行。

4.2.4.2 SDP 的适用策略:

SDP 本身不能提供相对应功能，可通过 SDP 插件或与 MAM（移动应用管控）或 MDM（移动设备管理）相关软件联动实现本项的要求。

4.2.5 对“7.3.4.1 移动应用软件采购”的适用策略

4.2.5.1 本项要求包括:

a) 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

b) 应保证移动终端安装、运行的应用软件由指定的开发者开发。

4.2.5.2 SDP 的适用策略:

SDP 本身不提供应用移动应用管控能力，但 SDP 软件采购时需要满足移动应用软件采购的要求，如需要合适的证书签名，或者可信的开发者开发。

4.2.6 对“7.3.4.2 移动应用软件开发”的适用策略

4.2.6.1 本项要求包括:

a) 应对移动业务应用软件开发者进行资格审查。

b) 应保证开发移动业务应用软件的签名证书合法性。

4.2.6.2 SDP 的适用策略:

SDP 本身不提供应移动应用软件开发控制，但应对移动业务应用软件开发者进行资格审查，应保证开发移动业务应用软件的签名证书合法性。

4.3 移动互联安全扩展三级要求

等级保护 2.0 中第三级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在后续分节详细阐述。

要求项	要求子项	SDP适用情况
8.3.1 安全物理环境	8.3.1.1无线接入点的物理位置	不适用
8.3.2 安全区域边界	8.3.2.1 边界防护	适用，见4.3.1
	8.3.2.2 访问控制	适用，见4.3.2
	8.3.2.3 入侵防范	部分适用，“无线接入设备的SSID广播、WPS等高风险功能”

		检测和禁止未覆盖，见4.3.3。
8.3.3 安全计算环境	8.3.3.1 移动终端管控	部分适用，“移动终端远程管控（如：远程锁定、远程擦除等）”未涵盖。
	8.3.3.2 移动应用管控	部分适用，“根据白名单控制应用软件安装、运行”未覆盖，见4.3.4
8.3.4 安全建设管理	8.3.4.1 移动应用软件采购	部分适用，SDP组件验证要求严格，符合采购要求可通过验证，见4.3.5。
	8.3.4.2 移动应用软件开发	部分适用，SDP组件验证要求严格，符合开发要求可通过验证。见4.3.6。
8.3.5 安全运维管理	8.3.5.1配置管理	适用，见4.3.7。

4.3.1 对“8.3.2.1 边界防护”的适用策略

4.3.1.1 本项要求包括：

a) 应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

4.3.1.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能满足 a)的边界防护要求。无线终端作为 SDP 客客户端，使用 SDP 网关作为无线接入网关。

4.3.2 对“8.3.2.2 访问控制”的适用策略

4.3.2.1 本项要求包括:

a) 无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

4.3.2.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能满足 a)的访问控制要求。

SDP 客户端中每次连接网关的会话都需要认证后连接，天然支持接入认证。SDP 默认采用多因子认证，认证方式支持认证服务器认证或国家密码管理机构批准的密码模块进行认证。

4.3.3 对“8.3.2.3 入侵防范”的适用策略

4.3.3.1 本项要求包括:

a) 应能够检测到非授权无线接入设备和非授权移动终端的接入行为。

b) 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。

c) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。

d) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。

e) 应禁止多个 AP 使用同一个认证密钥。

f) 应能够阻断非授权无线接入设备或非授权移动终端。

4.3.3.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能部分满足:

a）和 b)要求：由于 SDP 采用先认证后接入的方式，天然拒绝非授权连接，而非检测。

c)要求：SDP 不适用，依赖无线设备自身功能。

d）和 e)要求： SDP 不适用，属于管理范畴。

f) 要求： SDP 支持阻断非授权连接。

对于符合访问策略的网络攻击行为，SDP 需要结合用户行为日志大数据分析软件，发现异常行为并且发出预警。

4.3.4 对“8.3.3.2 移动应用管控”的适用策略

4.3.4.1 本项要求包括:

a) 应具有选择应用软件安装、运行的功能。

b) 应只允许指定证书签名的应用软件安装和运行。

c) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。

4.3.4.2 SDP 的适用策略:

SDP 本身不提供应用移动应用管控能力，但 SDP 插件需要满足移动应用管控要求，如需要合适的证书签名，加入到白名单中。

4.3.5 对“8.3.4.1 移动应用软件采购”的适用策略

4.3.5.1 本项要求包括:

a) 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

b) 应保证移动终端安装、运行的应用软件由指定的开发者开发。

4.3.5.2 SDP 的适用策略:

SDP 本身不提供应用移动应用管控能力，但 SDP 软件采购时需要满足移动应用软件采购的要求，如需要合适的证书签名，或者可信的开发者开发。

4.3.6 对“8.3.4.2 移动应用软件开发”适用策略

4.3.6.1 本项要求包括:

a) 应对移动业务应用软件开发者进行资格审查。

b) 应保证开发移动业务应用软件的签名证书合法性。

4.3.6.2 SDP 的适用策略:

SDP 本身不提供应用移动应用管控能力，但是 SDP 要求发起方进行身份验

证，即移动终端的应用软件在管控范围内，软件开发时需要满足移动应用软件开发的要求，如需要合适的证书签名，或者可信的开发者开发。

4.3.7 对“8.3.5.1 配置管理”的适用策略

4.3.7.1 本项要求包括:

a) 应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

4.3.7.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能满足，SDP 需要先认证后连接，因此必须要有终端配置管理和认证服务。

4.4 移动互联安全扩展四级要求

等级保护 2.0 中第四级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在后续分节详细阐述。

要求项	要求子项	SDP适用情况
9.3.1 安全物理环境	9.3.1.1无线接入点的物理位置	不适用
9.3.2 安全区域边界	9.3.2.1 边界防护	适用，见4.4.1

	9.3.2.2 访问控制	适用，见4.4.2
	9.3.2.3 入侵防范	部分适用，“无线接入设备的SSID广播、WPS等高风险功能”检测和禁止未覆盖，见4.4.3。
9.3.3 安全计算环境	9.3.3.1 移动终端管控	部分适用，“移动终端远程管控（如：远程锁定、远程擦除等）”未涵盖，见4.4.4。
	9.3.3.2 移动应用管控	部分适用，“根据白名单控制应用软件安装、运行”未覆盖，见4.4.5
9.3.4 安全建设管理	9.3.4.1 移动应用软件采购	部分适用，SDP组件验证要求严格，符合采购要求可通过验证，见4.4.6。
	9.3.4.2 移动应用软件开发	部分适用，SDP组件验证要求严格，符合开发要求可通过验证，见4.4.7。
9.3.5 安全运维管理	9.3.5.1配置管理	适用，见4.4.8

4.4.1 对“9.3.2.1 边界防护”适用策略

4.4.1.1 本项要求包括：

a） 应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设

备。

4.4.1.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能满足 a)的边界防护要求。无线终端作为 SDP 客客户端，使用 SDP 网关作为无线接入网关。

4.4.2 对“9.3.2.2 访问控制”的适用策略

4.4.2.1 本项要求包括:

a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

4.4.2.2 SDP 的适用策略:

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能满足 a)的访问控制要求。

SDP 客户端中每次连接网关的会话都需要认证后连接，天然支持接入认证。SDP 推荐采用多因子认证，认证方式支持适用认证服务器进行认证或国家密码管理机构批准的密码模块进行认证。

4.4.3 对“9.3.2.3 入侵防范”适用策略

4.4.3.1 本项要求包括:

a) 应能够检测到非授权无线接入设备和非授权移动终端的接入行为。

b) 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。

c) 应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态。

d) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。

e) 应禁止多个 AP 使用同一个认证密钥。

f) 应能够阻断非授权无线接入设备或非授权移动终端。

4.4.3.2 SDP 的适用策略：

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能部分满足：

a）和 b)要求：由于 SDP 采用先认证后接入的方式，天然拒绝非授权连接，而非检测。

c)要求：SDP 不适用，依赖无线设备自身功能。

d）和 e)要求： SDP 不适用，属于管理范畴。

f) 要求： SDP 支持阻断非授权连接。

对于符合访问策略的网络攻击行为，SDP 需要结合用户行为日志大数据分析软件，发现异常行为并且发出预警。

4.4.4 对“9.3.3.1 移动终端管控”适用策略

4.4.4.1 本项要求包括:

a) 应保证移动终端安装、注册并运行终端管理客户端软件。

b) 移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。

c) 应保证移动终端只用于处理指定业务。

4.4.4.2 SDP 的适用策略:

SDP 可以与移动设备管理软件（MDM）配合，保证移动终端安装了管理软件才可以访问网络，满足要求 a）。并且，通过在网络出口处部署 SDP 网关来实现移动端只能用于处理制定业务，满足要求 c）。

4.4.5 对“9.3.3.2 移动应用管控”适用策略

4.4.5.1 本项要求包括:

a) 应具有选择应用软件安装、运行的功能。

b) 应只允许指定证书签名的应用软件安装和运行。

c) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。

d) 应具有接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。

4.4.5.2 SDP 的适用策略:

SDP 本身不提供应用移动应用管控能力，但 SDP 插件需要满足移动应用管控要求，如需要合适的证书签名，加入到白名单中。

4.4.6 对“9.3.4.1 移动应用软件采购”适用策略

4.4.6.1 本项要求包括:

a) 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

b) 应保证移动终端安装、运行的应用软件由指定的开发者开发。

4.4.6.2 SDP 的适用策略:

SDP 本身不提供应用移动应用管控能力，但 SDP 软件采购时需要满足移动应用软件采购的要求，如需要合适的证书签名，或者可信的开发者开发。

4.4.7 对“9.3.4.2 移动应用软件开发”适用策略

4.4.7.1 本项要求包括:

a) 应对移动业务应用软件开发者进行资格审查。

b) 应保证开发移动业务应用软件的签名证书合法性。

4.4.7.2 SDP 的适用策略:

SDP 本身不提供应用移动应用管控能力，但是 SDP 要求发起方进行身份验证，即移动终端的应用软件在管控范围内，软件开发时需要满足移动应用软件开发的要求，如需要合适的证书签名，或者可信的开发者开发。

4.4.8 对“9.3.5.1 配置管理”适用策略

4.4.8.1 本项要求包括:

a）应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

4.4.8.2 SDP 的适用策略:

按照 SDP 标准规范，“SDP 组件”:

- SDP 控制器：SDP 控制器确定哪些 SDP 主机可以相互通信。SDP 控制器可以将信息中继到外部认证服务，例如认证，地理位置和/或身份服务器。
- SDP 连接发起主机（Initiating Host,即 IH）：SDP 连接发起主机（IH）与 SDP 控制器通信以请求它们可以连接的 SDP 连接接受方（AH）列表。在提供任何信息之前，控制器可以从 SDP 连接发起主机请求诸如硬件或软件清单之类的信息。

可通过内嵌式或应用侧 SDP 网关或移动侧 SDP 网关都能满足，SDP 需要先认证后连接，因此必须要有终端配置管理和认证服务。

移动终端作为 SDP 连接发起主机，在包括 SDP 控制器在内的移动接入平台，

管理平台内建立列表，进行设备识别。

5 SDP 满足等保 2.0 物联网安全扩展要求

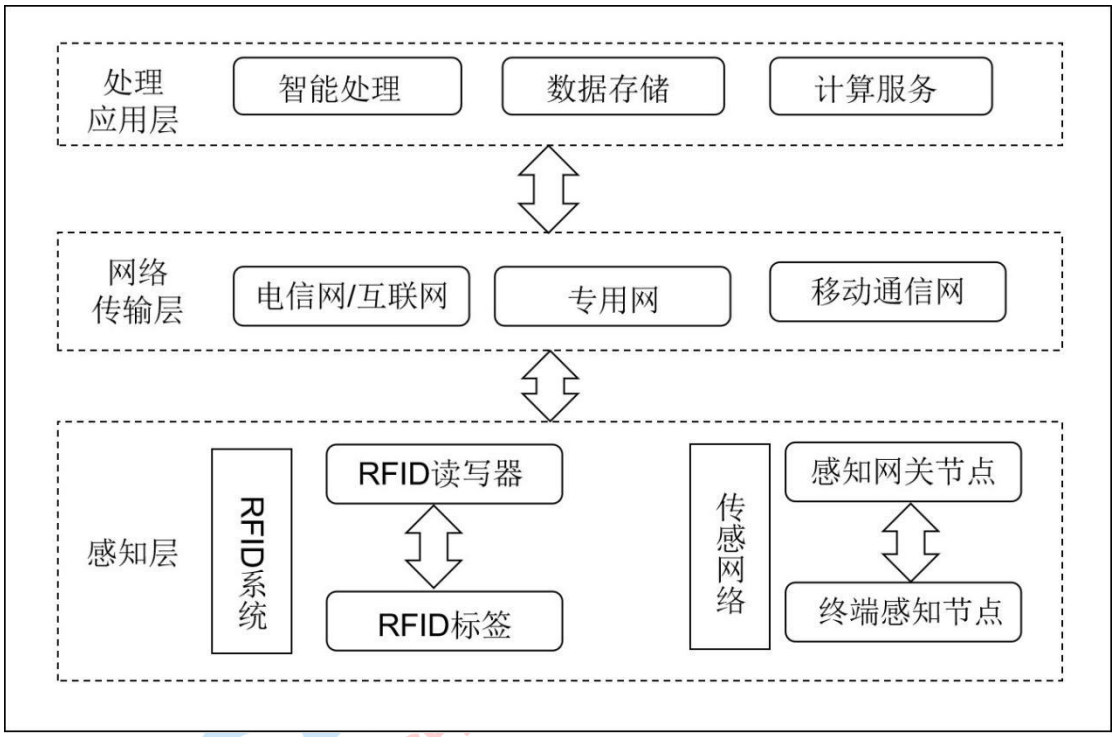
5.1 概述

物联网面临着错综复杂的安全风险。从管理角度看，物联网应用 涉及国家重要行业、关键基础设施，产业合作链条长、数据采集范围 广、业务场景多，各类应用场景的业务规模、责任主体、数据种类、 信息传播形态存在差异，为物联网安全管理带来挑战。从技术角度看， 物联网涉及通信网络、云计算、移动 APP、WEB 等技术，本身沿袭 了传统互联网的安全风险，加之物联网终端规模巨大、部署环境复杂， 传统安全问题的危害在物联网环境下会被急剧放大。

我国政府早在 2013 年就将安全能力建设纳入物联网发展规划。 近年来，随着物联网技术应用的不断成熟，物联网安全标准化得到进 一步重视，成为国家促进关键信息基础设施保护、行业应用安全可控 的重要抓手。值此物联网产业发展的关键时期，加快研制应用物联网 安全基础标准和关键技术标准，尤其是工业互联网、车联网、智能家 居等产业急需的物联网安全服务标准，已成为尤为紧迫的一项工作。

大量的新设备正在连接到互联网上。管理这些设备或从这些设备中提取信息抑或两者兼有的 后端应用程序的任务很关键，因为要充当私有或敏感数据的保管人。软件定义边界可用于隐藏这 些服务器及其在 Internet 上的交互，以最大限度地提高安全性和正常运行时间。

等级保护基本要求附录 F 中，描述了物联网应用场景。物联网从结构上可分为三个逻辑层，即感知层、网络传输层和处理应用层。其中感知层包括传感器节点和传感网网关节点，网络传输层包括将这些感知数据远距离传输到处理中心的网络，处理应用层包括对感知数据进行存储与智能处理的平台，并对业务应用终端提供服务。



图：物联网构成

下面将会对等保每一级别的物联网安全与 SDP 的适用策略方面进行详细描述。

5.2 物联网安全扩展二级要求

5.2.1 SDP 的适用情况

在物联网场景中，感知节点通常不是集中化部署在数据中心的，并且在能源、

交通等行业中感知节点往往还会在户外部署，进而通过有线或无线的方式与远程数据中心或云平台进行数据交互。分布式部署在数据中心外部的感知节点，及其与远程数据中心的通信渠道是物联网场景下的重要攻击面，攻击者有可能利用物理接触等手段对感知节点设备做深入的分析研究，从而发现其中可被利用的漏洞。还可以通过通信渠道将含有恶意代码的设备或攻击者的电脑连入远程数据中心。并且具有相同功能的感知节点设备的型号与配置通常区别不大，因此攻击者一旦掌握了某个感知节点设备的漏洞，便可能获得批量攻击整个物联网系统的能力，而这通常是攻击者对物联网系统的最终攻击目的。

对此，软件定义边界（SDP）将通过“零信任”框架，重构物联网系统的安全机制，并利用强化身份验证（多因素/逐步验证）、身份与设备的双向验证、网络微隔离、安全远程访问等技术手段实现增强物联网安全。物联网感知节点通常遵循“服务器-服务器”的 SDP 部署模式，但是由于物联网感知节点还分为感知层终端和感知层网关，因此从连接方式上可以进一步分为如下两种情况：

- 感知层终端-远程数据中心（服务器-服务器模式）：感知层终端设备与远程数据中心，均属于 SDP 部署模式中的“服务器”。服务器之间的连接都是加密的，无论底层网络或 IP 结构如何，SDP 模型要求服务器部署轻量级 SPA（单包授权）技术，即服务器之间首先通过 SPA 完成鉴权并建立加密连接，然后才进行正常通行，任何未授权的访问都不会得到服务器的回应。
- 感知层终端-感知层网关-远程数据中心的模式（客户端-网关-服务器模式）：这类连接方式通常是由于感知层终端计算或存储资源不够，或感知层终端设备需要更快速的实时响应，因此通过感知层网关设备提供边缘计算能力。此类连接方式要求感知层网关与感知层终端设备进行白名单机制的增强双向

设备验证（设备 ID/MAC/固件或 OS 内核完整性等多因素验证），同时感知层网关与远程数据中心均使用 SPA（单包授权）技术，确保感知层终端与感知层网关，以及感知层网关与远程数据中心进行通信前，应当首先完成授权验证，否则将不做任何响应。

等级保护 2.0 中第二级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在下个章节详细阐述。

等保要求项	等保要求子项	SDP适用情况
7.4.1 安全物理环境	7.4.1.1 感知节点设备物理防护	不适用
7.4.2 安全区域边界	7.4.2.1 接入控制	适用，见5.2.2
	7.4.2.2 入侵防范	适用，见5.2.3
7.4.3 安全运维管理	7.4.3.1 感知节点管理	部分适用，见5.2.4

5.2.2 对“7.4.2.1 接入控制”的适用策略

5.2.2.1 本项要求包括:

a）应保证只有授权的节点可以接入

5.2.2.2 SDP 的适用策略

- 对设备进行身份认证和验证
- 动态连接管理

5.2.3 对“7.4.2.2 入侵防范”的适用策略

5.2.3.1 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。

5.2.3.2 SDP 的适用策略:

- 对于未进行身份验证的请求不做回应，使设备在网络中被“隐藏”。
- 通过部署“DenyAll”SDP 网关（充当网络防火墙）可以确保未被认证和授权的访问无法进入内部网络。
- 通过检测“错误包”（非授权的请求等）识别可能存在的攻击行为。

5.2.4 对“7.4.3 安全运维管理”的适用策略

5.2.4.1 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、丢失和报废过程作出明确规定，并进行全程管理。

5.2.4.2 SDP 的适用策略:

要求 a）属于管理范畴，不属于 SDP 支持范围之内。

可通过 SDP 客户端的身份鉴别内置在感知节点设备、网关节点设备上，SDP 客户端支持各种已有身份认证体系，增强的身份验证方式，符合等保 2.0 要求。

感知节点设备、网关节点设备身份认证通过后，即可在安全管理系统上进行注册，在设备入库、存储、部署、携带、维修、丢失和报废全过程进行整体跟踪管理，从而满足 b）项要求。

5.3 物联网安全扩展三级要求

5.3.1 SDP 的适用情况

根据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》8.4 章节"物联网安全扩展要求"的描述，第三级的物联网安全扩展要求要求主要包括：安全物理环境、安全区域边界、安全计算环境、安全运维管理共四个部分。

根据附录 F （物联网应用场景说明）的描述：物联网通常从架构上可分为三个逻辑层，即感知层、网络传输层和处理应用层。对物联网的安全防护应包括感知层、网络传输层和处理应用层，由于网络传输层和处理应用层通常是由计算机设备构成，因此这两部分按照安全通用要求提出的要求进行保护，此标准的物联网安全扩展要求针对感知层提出特殊安全要求，与安全通用要求一起构成对物联网的完整安全要求。

其中感知层包括传感器节点和传感网网关节点，或 RFID 标签和 RFID 读写器，也包括这些感知设备及传感网网关、RFID 标签与阅读器之间的短距离通信（通常为无线）部分。

在感知层的各组件之中只有感知网关节点（例如 IoT 网关）具备底层计算系统，可以部署 SDP 功能模块。

等级保护 2.0 中第三级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在下个章节

详细阐述。

要求项-1	要求项-2	要求项-3	SDP适用情况
8.4 物联网安全扩展要求	8.4.1 安全物理环境	8.4.1.1 感知节点设备物理防护	不适用
	8.4.2 安全区域边界	8.4.2.1 接入控制	适用，见5.3.2
		8.4.2.2 入侵防范	适用，见5.3.3
	8.4.3 安全计算环境	8.4.3.1 感知节点设备安全	不适用
		8.4.3.2 网关节点设备安全	部分适用，见5.3.4
		8.4.3.3 抗数据重放	不适用
		8.4.3.4 数据融合处理	不适用
	8.4.4 安全运维管理	8.4.4.1 感知节点管理	不适用

5.3.2 对“8.4.2.1 接入控制“的适用策略

5.3.2.1 本项要求包括:

a) 应保证只有授权的感知节点可以接人。

5.3.2.2 SDP 的适用策略:

可以在物联网感知节点上部署 SDP 客户端，在物联网接入设备上部署 SDP 网关 ，因为 SDP 客户端连接前都需要经过 SDP 控制器认证和授权，因此只有授

权的感知节点可以接入。

5.3.3 对“8.4.2.2 入侵防范”的适用策略

5.3.3.1 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。

5.3.3.2 SDP 的适用策略:

假设指定感知节点连接在网关节点上，在网关节点和目标通信节点上都有部署 SDP 功能组件，在此情况下可通过 SDP 技术满足:

a)受限制的感知节点连接在网关节点上作为SDP架构中的连接发起主机IH，与目标通讯节点作为 SDP 架构中的连接接受主机 AH 建立 SDP 连接，同时 SDP 控制器发送安全策略，只允许受限感知节点去往允许的目标通讯节点进行通讯，从而实现此项控制要求。

b）受限制的网关节点作为 SDP 架构中的连接发起主机 IH，与目标通讯节点作为 SDP 架构中的连接接受主机 AH 建立 SDP 连接，同时 SDP 控制器发送安全策略，只允许受限网关节点去往允许的目标通讯节点进行通讯，从而满足此项控制要求。

5.3.4 对“8.4.3.2 网关节点设备安全”的适用策略

5.3.4.1 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秘钥进行在线更新。

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。

5.3.4.2 SDP 的适用策略:

假设指定网关节点和目标连接设备上都有部署 SDP 功能组件，在此情况下可通过 SDP 技术满足:

a) 如果网关节点和目标连接设备都部署了 SDP 功能组件且处于同一 SDP 环境中可以通过控制器实现标识和鉴别能力，从而满足此项要求。

b）在 SDP 架构中可以通过控制器进行授权指定允许的连接节点，并通过授权来限制伪造节点发送数据，从而满足此项要求。

e）和 f）授权用户终端上的 SDP 客户端在接入时需要到 SDP 控制器进行身份和设备的验证，在这个过程可以进行秘钥和关键配置参数的更新。

除此以外的其它要求不适用于 SDP 解决方案。

5.4 物联网安全扩展四级要求

5.4.1 SDP 的适用情况

等级保护 2.0 中第四级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在下个章节详细阐述。

要求项	要求子项	SDP适用情况
9.4.1 安全物理环境	9.4.1.1 感知节点设备物理安全	不适用
9.4.2 安全区域边界	9.4.2.1接入控制	适用，见5.4.2
	9.4.2.2 入侵防范	适用，见5.4.3
9.4.3 安全计算环境	9.4.3.1 感知节点设备安全	适用，见5.4.4
	9.4.3.2 网关节点设备安全	适用，见5.4.5
	9.4.3.3 抗数据重放	适用，见5.4.6
	9.4.3.4 数据融合处理	适用，见5.4.7
9.4.4 安全运维管理	9.4.4.1 感知节点管理	适用，见5.4.8

5.4.2 对“9.4.2.1 接入控制” 的适用策略

5.4.2.1 本项要求包括:

a) 应保证只有授权的感知节点可以接人。

5.4.2.2 SDP 的适用策略:

可以在物联网感知节点上部署 SDP 客户端，在物联网接入设备上部署 SDP 网关 ，因为 SDP 客户端连接前都需要经过 SDP 控制器认证和授权，因此只有授权的感知节点可以接入。

5.4.3 对“9.4.2.2 入侵防范”的适用策略

5.4.3.1 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。

5.4.3.2 SDP 的适用策略:

物联网感知节点设备，在接入网络时需要具有身份鉴别机制，采用访问控制机制，确保授权才允许接入。

边界防护：SDP 作为边界隔离产品，不会存在边界设备提供的受控接口进行通信的可能。由于独特的三组件关系，仅能通过特定的客户端，且经合法授权后，方可连入到内部网络。

入侵防范：SDP 本身的特性就不存在共享和高危的端口，应用网关仅面向客

户端开放访问权限，极大的控制了使用范围。通过客户端和管控平台，可检测到入侵的行为，并在发生严重入侵事件时提供预警。

访问控制：SDP 默认不信任任何网络、人、设备，均需进行验证，默认拒绝一切连接，只有验证合法的访问请求才被允许。并根据控制策略进行访问控制，仅对于验证合法用户，允许受控端口进行通信。即便合法的用户，也需要根据自己的权重分配账户和访问权限。

身份鉴别： 客户端支持各种已有身份认证体系，增强的身份验证方式，符合等保 2.0 要求。

5.4.4 对“9.4.3.1 感知节点设备安全” 的适用策略

5.4.4.1 本项要求包括:

a）应保证只有授的用户可以对感知节点设备的软件用进行配置或变更。

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（包括路曲节点）进行身份标识和鉴别的能力。

5.4.4.2 SDP 的适用策略:

物联网感知节点通常处于网络边缘，弱终端负责数据采集，强终端会涉及到一些边缘计算，安全计算环境首先要保证设备的安全。身份标识和鉴别是基本要求，通过可信 ID，确保资产不会被替换和伪造。SDP 可以提供身份和访问管理。

5.4.5 对“9.4.3.2 网关节点设备安全” 的适用策略

5.4.5.1 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点所发送的数的能力。

c）授衩用户应能够在设备使用过程中对关踺密钥进行在线更新。

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。

5.4.5.2 SDP 的适用策略:

物联网网关节点主要用于和弱终端的连接，需要对与其连接的设备合法性进行判断。设备的密钥和配置参数的更新，相当于有安全基线的要求，同时需要支持授权用户的在线更新。

5.4.6 对“9.4.3.3 抗数据重放” 的适用策略

5.4.6.1 本项要求包栝:

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忤改，避免数据的修改重放攻击。

5.4.6.2 SDP 的适用策略:

数据新鲜性是指对所接收的历史数据或超出时限的数据能够进行识别。物联网数据使用有可用性、完整性、保密性的要求，以避免数据重放攻击。SDP 拒绝

无效的数据包（可能来自未经授权的用户），所以它们可以防止和未经授权的用户或设备建立 TCP 连接，以避免数据重放攻击。

5.4.7 对“9.4.3.4 数据融合处理”的适用策略

5.4.7.1 本项要求包括:

a）应对来自传感网的数行数据融合处理，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。

5.4.7.2 SDP 的适用策略:

对于数据融合处理有两种方案，不同终端厂商设计时按照行业标准，使用通用协议加私有协议方式，为平台提供数据。或者平台自己能够支持多种协议的数据融合。

5.4.8 对“9.4.4.1 感知节点管理”的适用策略

5.4.8.1 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）对感知节点设备网关节点设备人厍、存储，部署，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脸查工具和检查维护记录等。

5.4.8.2 SDP 适用策略:

物联网感知节点设备，部署位置广泛环境恶劣，会因日久年深导致设备不可用。对运维管理提出要求是定期巡视设备并进行记录和维护，并对设备的入库、部署到报废的全生命周期进行管理。此外对运维的保密性管理也提出了要求。

软件定义边界可用于隐藏这些服务器及其在 Internet 上的交互，以最大限度地提高安全性和正常运行时间。

可信验证：SDP 通过客户端进行可信验证，在检测到可信异常后进行报警，并将审计记录反馈至管控平台。

安全审计：SDP 的审计内容覆盖到每个终端用户，对于行为和重要事件进行记录。包括日期、时间、事件等。并保存于管控平台，并进行定期备份，以防止未预期的删除、修改和覆盖等。

审计管理：所有的审计操作，审计管理员均需要进行身份验证。只在特定界面进行安全审计操作，并对所有操作行为进行记录。支持审计记录分析，分析结果可进行再处理。

6 SDP 满足等保 2.0 工业控制系统安全扩展要求

6.1 概述

工业控制系统涉及应用层、控制层和实时操作层，与传统的信息系统不同，其具有实时性、集成性、稳定性、高可用性和人机互操作性要求，工业控制系统网络组件涉及传统网络系统组件如OS、网络及网络设备、数据库等，同时包括工业控制专用设备或系统，如SCADA、PLC、DCS等，系统投入运营后不会轻易变更（如一般工业控制系统使用生命周期至少25年），因此随着运营年限增长各系统的漏洞、缺陷越来越多，易被病毒、恶意代码攻击，造成工业控制系统风险。另外由于工业控制系统稳定性要求，安全防护措施实施均要求对环境及业务零影响，传统的安全防护措施不太适用于工业控制系统防护，因此安全防护措施不足。

随着国家提出的工业互联网发展的战略，传统封闭式工业控制系统网络逐步走向外网、互联网，网络安全面临更大的挑战。

软件定义边界（SDP）的功能与技术在工业控制系统中有较好的应用环境，是工业控制系统（特别是工业互联网）安全加强的轻量级可选技术，包括SDP实现工业控制网络中的白名单机制（如应用白单名、设备白单名、用户白单名），可有效提升对网络安全管理；通过先认证再连接，实现对接入用户与设备安全管理；通过基于用户策略安全防护，实现用户身份鉴别、资源授权等安全；通过加密实现对工业系统指令与数据安全传输等等。

根据SDP 指南，SDP的部署可以分为以下几种方式。

- 客户端—网关模型：一个或多个服务器位于 SDP 连接接受主机（AH）后面，SDP 连接接受主机（AH） 充当客户端和受保护服务器之间的网关。这种模式将受保护的服务器与未经授权的用户隔离开，同时减轻了常见的横向移动攻击风险。
- 客户端—服务器模型：这种情况下，受保护的服务器将直接运行可接受连接主机（AH） 的软件， 而无需通过运行该软件的服务器前面的网关，从而建立了客户端和服务器之间的直接联系。
- 服务器—服务器模型：这种模式可以保护提供REST、SOAP、RPC等服务或 API的服务器免受网络上未经授权的主机的攻击
- 客户端-服务器-客户端模型：使用此模式，受保护的服务器将需要配备网关或轻量级SPA协议。受保护服务器所在的网络不需要限制入向（inbound）连接。服务器上的网关(执行点)使用SPA来防止内部和外部未经授权的连接。

结合在工业控制系统环境网络特殊情况，推荐SDP部署如下：

- 实时生产控制区与非实时生产控制区：实时生产控制区与非实时生产控制区部署SDP，利用先认证再连接对所有访问实时生产控制区、非实时生产控制区资源实现的接入准入；采用基于用户策略防护针对操作人员、运维人员、临时运维人员等进行严格授权与控制。
- 管理信息区：在管理信息区部署SDP，实现对网络关键资源安全保护，降低病毒、木马等安全威胁，同时，针对外部网络的远程接入、临接接入及访问等提供资源隐身、访问控制、传输加密、身份鉴别、资源授权

等功能。

- 工业互联网：工业互联网为全新的工业控制系统网络，可与SDP安全架构进行整合，利用SDP的准入、授权、动态、隐身、加密等安全功能与特性、实现对工业互联网实时控制系统、非实时控制系统、信息管理系统等提供多方位的安全保护，为工业互联网应用提供安全支撑。

6.2 工业控制系统安全扩展一级要求

等级保护 2.0 工业控制系统扩展要求第一级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足安全要求如下表所示。详细的适用说明将在下列章节详细阐述。

要求项	要求子项	SDP适用情况
6.5.1 安全物理环境	6.5.1.1 室外控制设备物理防护	不适用
6.5.2 安全通信网络	6.5.2.1 网络架构	适用，见6.2.1
6.5.3 安全区域边界	6.5.3.1 访问控制	适用，见6.2.2
	6.5.3.2 无线使用控制	适用，见6.2.3
6.5.4 安全计算环境	6.5.4.1 控制设备安全	不适用

6.2.1 对“5.5.2.1 网络架构”的适用策略

6.2.1.1 本项要求包括:

a) 工业控制系统与企业其他系统之间应划分两个区域，区域间应采用单向的技术隔离手段 b) 工业控制系统内部应根据业务特点划分为不同的安全区域，安全域之间应采用技术隔离手段。

6.2.1.2 SDP 的适用策略:

实时生产控制区与非实时生产控制区、管理信息区部署 SDP 可满足 a)。

在实时生产控制区与非实时生产控制区之间安全区域部署 SDP，可实现基于业务需求的技术隔离，可按网络、资源、应用、用户等进行技术隔离访问控制，可满足 b)要求。

6.2.2 对“6.5.3.1 访问控制”的适用策略

6.2.2.1 本项要求包括:

a) 应在工业控制系统与企业其它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。

6.2.2.2 SDP 的适用策略:

管理信息区部署 SDP 可实现对所有网络访问控制细粒度管理，可对 e-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务进行禁止。可满足 a)要求。

6.2.3 对“6.5.3.2 无线使用控制”的适用策略

6.2.3.1 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。

6.2.3.2 SDP 的适用策略:

通过管理信息区部署部署 SDP，利用先认证再连接、零信任等机制，实现无线用户、设备唯一性标识和鉴别，实现对网络资源的安全授权和使用，通过隧道加密，提升传输加密，满足 a)、b)要求。

6.3 工业控制系统安全扩展二级要求

第二级工业控制系统信息安全保护环境的设计目标是在第一级工业控制系统信息安全保护环境的基础上，增加系统安全审计等安全功能，并实施以用户为基本粒度的自主访问控制，使系统具有更强的自主安全保护能力。等级保护 2.0 中第二级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在下一章节详细阐述。

要求项	要求子项	SDP适用情况
7.5.1 安全物理环境	7.5.1.1 室外控制设备物理防护	不适用

7.5.2 安全通信网络	7.5.2.1 网络架构	适用，见6.3.1
	7.5.2.2 通讯传输	适用，见6.3.2
7.5.3 安全区域边界	7.5.3.1 访问控制	适用，见6.3.3
	7.5.3.2 拨号使用控制	适用，见6.3.4
	7.5.3.3 无线使用控制	适用，见6.3.5
7.5.4 安全计算环境	7.5.4.1 控制设备安全	不适用
7.5.5 安全建设管理	7.5.5.1 产品采购和使用	不适用
	7.5.5.2 外包软件开发	不适用

6.3.1 对“7.5.2.1 网络架构”的适用策略

6.3.1.1 本项要求包括:

a) 工业控制系统与企业其他系统之间应划分两个区域，区域间应采用单向的技术隔离手段。

b) 工业控制系统内部应根据业务特点划分为不同的安全区域，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。

6.3.1.2 SDP 的适用策略

实时生产控制区与非实时生产控制区、管理信息区、工业互联网部署 SDP 可满足:

在实时生产控制区与非实时生产控制区之间安全区域部署 SDP 网关，可实现基于业务需求的技术隔离，可按网络、资源、应用、用户等进行技术隔离访问控制，可满足 b)要求。在管理信息区内部部署 SDP，可满足 b)要求。

在工业互联网中，因需要跨越互联网，传统网闸措施不被推荐使用，因此，SDP 更适用于工业互联网的安全保护，部署 SDP 可满足 a)、b)、c)要求。

6.3.2 对“7.5.2.2 通讯传输”的适用策略

6.3.2.1 本项要求包括:

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措施。

6.3.2.2 SDP 的适用策略:

管理信息区、工业互联网部署 SDP 可满足:

部署 SDP 实现传输加密、身份零信任管理、访问控制等功能，满足等级保护 2.0 中工业安全扩展通信传输要求。可满足该要求。

6.3.3 对“7.5.3.1 访问控制”的适用策略

6.3.3.1 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。

6.3.3.2 SDP 的适用策略:

管理信息区、工业互联网部署 SDP，实现对所有网络访问控制细粒度管理，可对 e-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务进行禁止；满足 a)要求。

6.3.4 对“7.5.3.2 拨号使用控制”的适用策略

6.3.4.1 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量，并采取用户身份鉴别和访问控制等措施。

6.3.4.2 SDP 的适用策略:

实时生产控制区与非实时生产控制区、管理信息区、工业互联网部署 SDP 可满足:

通过 SDP 实现对远程拨号终端准入与用户零信任，访问传输加密以及访问资源按需授权，满足 a)要求。

6.3.5 对“7.5.3.2 无线使用控制”的适用策略

6.3.5.1 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。

6.3.5.2 SDP 的适用策略:

管理信息区、工业互联网部署 SDP 可满足:

通过部署 SDP，利用先认证再连接、零信任等机制，实现无线用户、设备唯一性标识和鉴别，实现对网络资源的安全授权和使用，通过隧道加密，提升传输加密，满足 a)、b)要求。

6.4 工业控制系统安全扩展三级要求

等级保护 2.0 工控安全扩展第三级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在下个章节详细阐述。

要求项	要求子项	SDP 适用情况
8.5.1 安全物理环境	8.5.1.1 室外控制设备物理防护	不适用

8.5.2 安全通信网络	8.5.2.1 网络架构	适用，见 6.4.1
	8.5.2.2 通信传输	适用，见 6.4.2
8.5.3 安全区域边界	8.5.3.1 访问控制	适用，见 6.4.3
	8.5.3.2 拨号使用控制	部分适用，见 6.4.4
	8.5.3.3 无线使用控制	适用，见 6.4.5
8.5.4 安全计算环境	8.5.4.1 控制设备安全	适用，见 6.4.6
8.5.5 安全建设管理	8.5.5.1 产品采购和使用	不适用
	8.5.5.2 外包软件开发	不适用

6.4.1 对“8.5.2.1 网络架构”的适用策略

6.4.1.1 本项要求包括:

a）工业控制系统与企业其他系统之间应划分两个区域，区域间应采用单向的技术隔离手段。

b）工业控制系统内部应根据业务特点划分为不同的安全区域，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。

6.4.1.2 SDP 的适用策略:

实时生产控制区与非实时生产控制区、管理信息区、工业互联网部署 SDP 可满足:

在实时生产控制区与非实时生产控制区之间安全区域部署 SDP 网关，可实现基于业务需求的技术隔离，可按网络、资源、应用、用户等进行技术隔离访问控制，可满足 b)要求。在管理信息区内部部署 SDP，可满足 b)要求。

在工业互联网中，因需要跨越互联网，传统网闸措施不被推荐使用，因此，SDP 更适用于工业互联网的安全保护，部署 SDP 可满足 a)、b)、c)要求。

6.4.2 对“8.5.2.2 通信传输”的适用策略

6.4.2.1 本项要求包括:

a）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信证技术手段实现身份认证、访问控制和数据加密传输。

6.4.2.2 SDP 的适用策略:

管理信息区、工业互联网部署 SDP 可满足:

部署 SDP 实现传输加密、身份零信任管理、访问控制等功能，满足等级保护 2.0 中工业安全扩展通信传输要求。可满足 a)要求。

6.4.3 对“8.5.3.1 访问控制”的适用策略

6.4.3.1 本项要求包括:

a）应在工业控制系统与企业其它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。

6.4.3.2 SDP 的适用策略

管理信息区、工业互联网部署 SDP 可满足：

管理信息区、工业互联网部署 SDP，实现对所有网络访问控制细粒度管理，可对 e-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务进行禁止；满足 a)要求。

6.4.4 对“8.5.3.2 拨号使用控制”的适用策略

6.4.4.1 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量，并采取用户身份鉴别和访顺控制等措施。

b) 拨号服务器和客户端应使用安全加固的操作系统，并采取数字证书认证，传输加密访问控制等措施。

6.4.4.2 SDP 的适用策略：

实时生产控制区与非实时生产控制区、管理信息区、工业互联网部署 SDP 可满足：

通过 SDP 实现对远程拨号终端准入与用户零信任，访问传输加密以及访问资源按需授权，满足 a)要求，部分满足 b)要求。

6.4.5 对“8.5.3.3 无线使用控制”的适用策略

6.4.5.1 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。

6.4.5.2 SDP 的适用策略:

管理信息区、工业互联网部署 SDP 可满足:

通过部署 SDP，利用先认证再连接、零信任等机制，实现无线用户、设备唯一性标识和鉴别，实现对网络资源的安全授权和使用，通过隧道加密，提升传输加密，满足 a)、b)、c)要求。

6.4.6 对“8.5.4.1 控制设备安全”的适用策略

6.4.6.1 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，应由基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测试，避免控制设备固件中存在恶意代码程序。

6.4.6.2 SDP 的适用策略:

实时生产控制区与非实时生产控制区、管理信息区、工业互联网部署 SDP 可满足:

通过部署 SDP，可实现内部应用准入、身份鉴别和访问控制，同时实现基于用户行为的安全审计，满足 a)要求。

6.5 工业控制系统安全扩展四级要求

等级保护 2.0 第四级要求中，规定了多个方面的具体技术要求。其中 SDP 能够帮助用户满足或部分满足的条目如下表所示。详细的适用说明将在下个章节详细阐述。

要求项	要求子项	SDP适用情况
9.5.1 安全物理环境	9.5.1.1 感知节点设备物理防护	不适用

9.5.2安全通信网络	9.5.2.1 网络架构	部分适用，见6.5.1
	9.5.2.2 通信传输	适用，见6.5.2
9.5.3 安全区域边界	9.5.3.1 访问控制	适用，见6.5.3
	9.5.3.2 拨号使用控制	适用，见6.5.4
	9.5.3.3 无线使用控制	部分适用，见6.5.5
9.5.4 安全计算环境	9.5.4.1 控制设备安全	部分适用，见6.5.6
9.5.5 安全建设管理	9.5.1.1 产品采购和使用	不适用
	9.5.1.2 外包软件开发	不适用

6.5.1 对“9.5.2.1 网络架构”的适用策略

6.5.1.1 本项要求包括:

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向安全隔离。

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。

6.5.1.2 SDP 的适用策略:

a) SDP 只能实现连接的控制，连接一旦建立，无法控制数据的通讯方向。

b) 安全域之间的隔离，依赖 a 项提供的设备，SDP 无法满足。

c) 内嵌式部署或者 SDP 网关可以进行分层组网，分层控制，可以满足该项

需求

6.5.2 对“9.5.2.2 通信传输”的适用策略

6.5.2.1 本项要求包括:

a）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传输。

6.5.2.2 SDP 的适用策略

可通过“内嵌式”或“网关式”部署 SDP 满足。

SDP 可以跨广域网部署，且通过 TLS 进行加密通讯，通过部署 SDP，结合适当的 IAM（Identity and Access Management 身份识别与访问管理）可以实现对网络访问控制细粒度管理，满足 a 项要求。

6.5.3 对“9.5.3.1 访问控制”的适用策略

6.5.3.1 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。

6.5.3.2 SDP 的适用策略:

可通过“内嵌式”或“网关式”部署 SDP 满足。

SDP 本身就可以实现针对不同的应用（主要是通过端口来判断）进行不同的访问控制策略，针对不同的应用进行白名单管理，满足 a 项要求。

防护机制失效通知依赖 SDP 设备本身的功能实现，尤其适用于网关式部署，通过在网关上部署相应的安全检测机制，进行预警和报警。

6.5.4 对“9.5.3.2 拨号使用控制”的适用策略

6.5.4.1 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量，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问服务。

6.5.4.2 SDP 的适用策略:

可通过“内嵌式”或“网关式”部署 SDP 满足。

通过 SDP 实现对设备准入与用户零信任，访问控制以及访问资源按需授权，满足 a)、b)、c)要求。但是 SDP 只能进行访问的控制，具体的控制，例如用户数量，身份鉴别等，需要结合拨号服务器进行二次控制。

6.5.5 对“9.5.3.3 无线使用控制”的适用策略

6.5.5.1 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。

6.5.5.2 SDP 的适用策略

可通过“内嵌式”或“网关式”部署 SDP 进行部分满足。通过 SDP 内部集成 IAM 功能，可以满足 a）b)要求。SDP 通讯本身就是加密的，可满足 c）项要求。针对 d）项需要部署专门的无线检测设备进行检测，SDP 无法满足。

6.5.6 对“9.5.4.1 控制设备安全”的适用策略

6.5.6.1 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。

6.5.6.2 SDP 的适用策略

b）c）项为管理要求，SDP 无法满足。d) e)项可以通过 SDP 客户端进行辅助实现。

7 总结

本白皮书对 SDP 的基本原理、等保 2.0 的发展背景及要求、SDP 与等保 2.0 的关系、SDP 满足等保 2.0 的二级、三级、四级安全通用要求、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、工业控制系统安全扩展要求等做了详细的阐述和说明。力求将 SDP 与等保 2.0 的每一项具体要求进行对比说明，方便本书的读者对 SDP 如何满足等保 2.0 的具体细节有更清晰的指导。

基于零信任理念的软件定义边界（SDP）技术不仅能够帮助企业做好网络安全建设，同时也能够满足等保 2.0 中的多项安全要求，除了在通用安全方面，还在诸如云计算、移动互联、物联网、工业控制等新兴领域方面发挥着巨大的作用。在边界防护、入侵防范、通信传输、身份鉴别、数据保密等方面，可以帮助企业

进一步收窄业务系统暴露面，保障业务系统的边界安全，是更符合新时代网络安全发展趋势的安全解决方案。

在网络安全已经上升到国家战略层面的今天，以等保 2.0 为代表的国家标准正在发挥越来越重要的作用。而如何将这些标准做到“落地实施”，则需要依托于所有的网络安全从业人员和厂商的共同努力。而这其中，以软件定义边界 SDP 为代表的新一代网络完全架构，正在颠覆传统的企业网络安全体系，将在今后企业网络安全建设和发展过程中发挥举足轻重的作用。