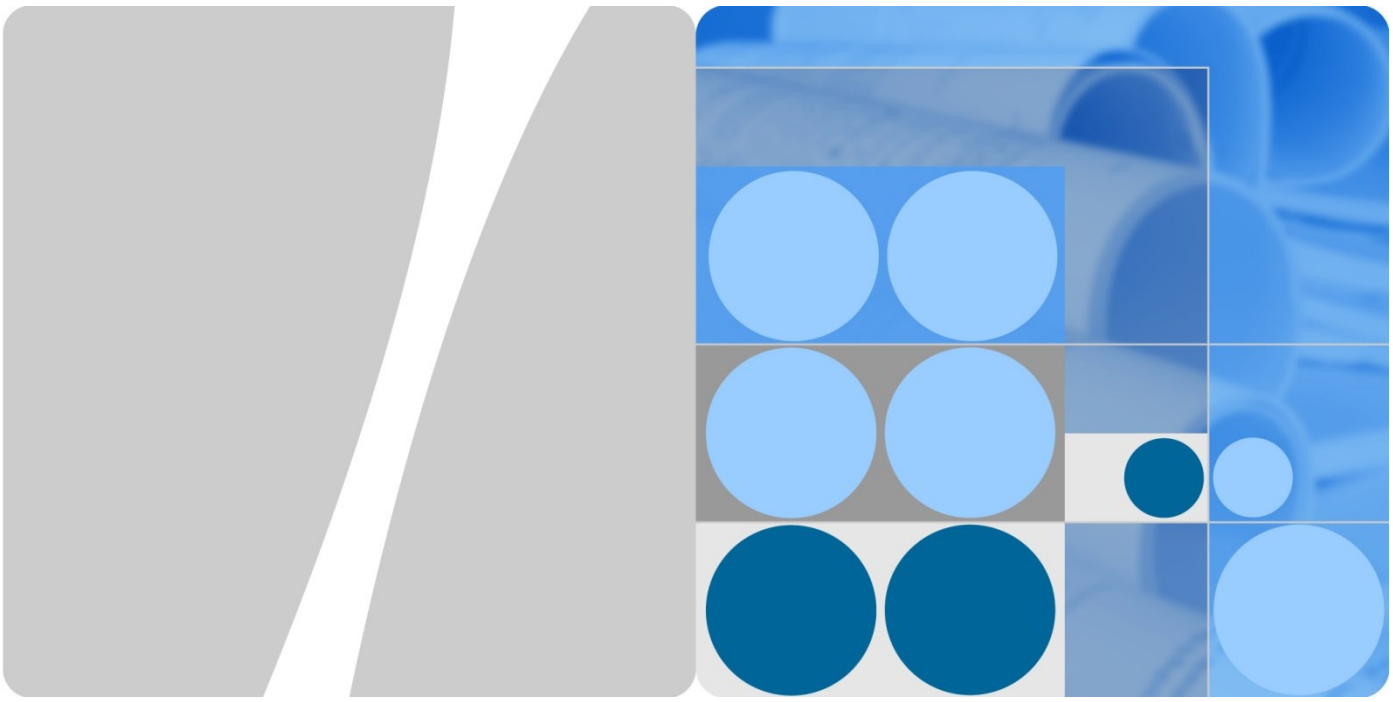


华为区域智慧隔离解决方案
技术白皮书

华为技术有限公司

商标声明

 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 概述

1.1 多业务区域共存的应用背景

在 IT 应用初期，许多行业网络部署时并未进行良好的规划，通常是先建立一张网络，然后各项业务陆陆续续从传统方式迁移到网络上，此时主要还是考虑各项业务的可用性，而忽略了业务在网络中的安全威胁，并未对各种不同业务在网络中进行分割。例如办公数据、生产数据网和安防监控数据可能一个网络中传输，或者公司内网数据和互联网访问数据在同一个网络中传输，而没有从物理或者逻辑上进行分隔。

随着 IT 化程度普及程度越来越高，以及各种网络安全泄密事件的传播，人们对网络安全重视程度逐步增强，一些政府和行业监管机构逐步出台针对网络的管理办法和规范，例如《信息安全等级保护管理办法》、《 计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》以及《关于银行业金融机构重要系统高可用性及信息安全管控风险提示的通知》、《关于加强银行网站及网银系统安全防范工作的通知》等。这些管理办法和规范要求加强敏感信息保护，积极采取技术手段，在物理安全、网络安全、系统安全、应用安全等不同层面，采取有效的网络隔离、终端控制、用户权限与密码管理、信息资源管理、系统日志分析、运行安全监控、操作审计、防病毒统一部署管理等措施，主动应对安全威胁，重点防范外部攻击，保障系统和数据安全。

1.2 多业务区域目前存在的问题

随着政府和行业监管政策以及企业 IT 部门制定的网络管理措施的实施，不同业务网络经过改造逐步实现了网络隔离，但在生产经营过程中，存在一些特殊部门、特殊岗位存在跨区访问的合理需求，在这些部门或岗位的终端上具备访问不同业务区域的能力，甚至可能要求能够同时访问两个不同的业务区域，由此带来了以下需要解决的问题：

1) 病毒和木马等跨区传播

当终端在一个业务区域中感染病毒或者木马程序，在其访问另外业务区域时，可能将

病毒或木马程序传播到另外一个业务区域。

2) 机密数据跨区泄露

当终端接入高密业务区域，并从网络中下载机密数据保存到本地后，在其接入低密业务区域的网络时，可能将本地的机密数据泄露出去。机密数据的泄露分为主动泄密和被动泄密两种方式。

3) 数据跨区传播的安全审计

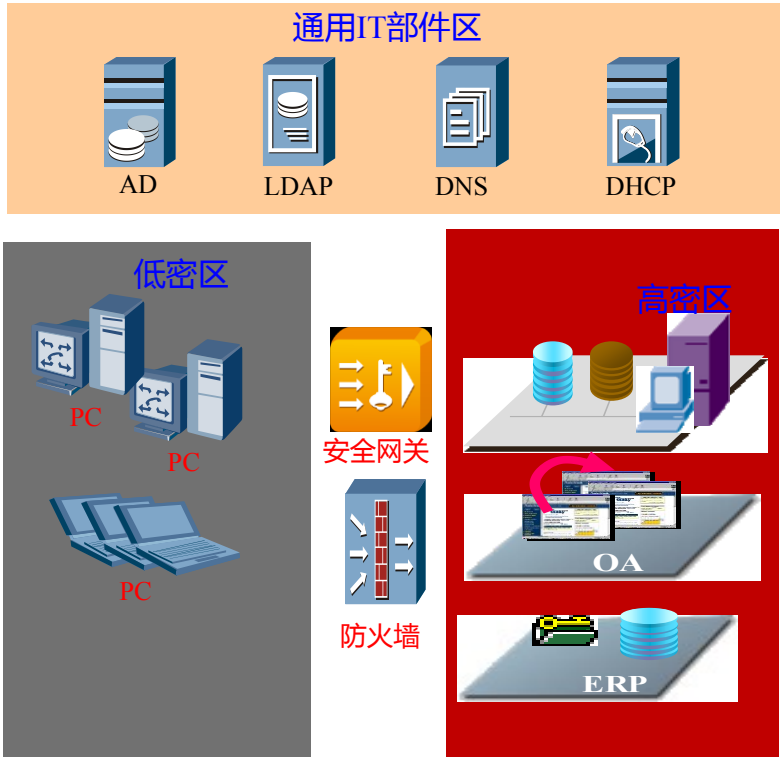
当关键数据通过终端中转在不同业务区域中传播时，网络中需要对关键数据的传播进行监控机制，IT管理员需要能够可视化地了解关键数据在区域间的传播。

2 解决方案介绍

2.1 解决方案整体说明

针对多业务区域隔离目前存在的问题，华为公司提供区域智慧隔离的安全解决方案。

2.1.1 整体架构方案



区域智慧隔离方案架构图

说明：低密区和高密区是相对的，安全等级要求高的区域被称之为“高密区”，而安全等级要求高的区域称之为“低密区”。一般而言，Internet 网络区域都是低密区，而办公网是高密区。

2.1.2 方案简介

智慧区域隔离方案中需要在不同业务区域之间部署安全接入网关， 所有跨区域访问的终端接受该安全接入网关的管理和控制，跨区域访问时，终端和安全接入网关之间的数据传输可进行安全加密。

当终端需要进行跨区域访问时，首先需登录安全接入网关，接受安全接入网关的接入认证。认证通过后，接入终端在本地系统的桌面中创建一个安全桌面，和本地真实桌面进行逻辑隔离。创建安全桌面后用户的使用体验如下：

桌面切换：用户在同一台终端上可使用两个工作桌面，一个是原有的桌面，我们称之为“真实桌面”，另一个为安全接入网关的客户端软件创建的工作桌面，我们称之为“安全桌面”。用户在终端上可以在两个桌面之间切换。在某些场景下，管理员在安全接入网关上配置策略，可能禁止用户在两个桌面间切换。

桌面内的操作：用户在安全桌面内可以进行文件操作、运行软件、访问网络等操作，所有的操作和在真实桌面内的操作形式相同。用户在进行正常的工作时几乎感知不到安全桌面和真实桌面的差异，只有在进行一些不合理的操作时会被禁止，例如可能在将机密数据保存到 U 盘、访问工作不相关的网络时受到禁止。

退出安全桌面：用户结束在安全桌面内的工作后，可退出安全桌面，退出后，用户在安全桌面内产生的数据、文件等信息在真实桌面内不可见。

通过安全接入网关在终端上创建的安全桌面，可实现本地真实桌面和本地业务区域连接，安全桌面和另外一个业务区域连接。通过这种实现方式，接入终端可同时连接两个业务区域，而两个业务区域的工作桌面又逻辑隔离，即满足了跨区域访问，又实现了区域逻辑隔离。

本章后续章节将对区域智慧隔离解决方案进行详细说明。

2.2 接入控制

2.2.1 用户认证

用户进行跨区域访问时，需要登录安全接入网关，接受用户认证。区域智慧隔离支持多种丰富的认证方式，包括

1) 本地用户名、密码认证
2) Radius认证

3) SecurID认证
4) LDAP认证
5) AD认证
6) 数字证书认证（UKey认证）
7) 短信密码辅助认证
8) 图形验证码辅助认证

2.2.2 终端认证

在用户登录时，安全接入网关除了对用户身份进行认证外，还可以对接入终端进行准入检查，可检查的内容包括：

1) 操作系统版本号、补丁
2) 防病毒软件
3) 防火墙软件
4) 关键文件
5) 网络通信端口
6) Windows系统注册表
7) 关键进程

只有满足安全接入网关定义的安全策略的终端才能够被允许接入。

2.3 病毒传播防范

病毒或木马程序一般通过在操作系统内安装病毒文件、感染系统内已有的文件、修改系统注册表，或者修改系统的配置文件等形式产生具体的破坏行为。安全接入网关客户端安全桌面通过文件操作重定向、注册表操作重定向等方式防范病毒在安全桌面与真实桌面之间传播。

在不允许真实桌面访问互联网、允许安全桌面内访问互联网的应用场景下，安全桌面的病毒防范功能将能够很好地防止用户访问互联网过程中无意感染的病毒或木马传染到真实桌面。在真实桌面已经感染病毒或木马的情况下，启动安全桌面后，病毒或木马有可能会感染安全桌面内的文件。这种情况下，需要通过终端接入认证功能进行规避，不允许带毒终端启用安全桌面。

2.3.1 文件操作重定向

在安全桌面内，原有的软件系统可以继续访问，但是原有的文件系统都会在安全桌面中进行虚拟化重定向，互联网的病毒软件，对文件、系统等的操作都会被进行重定向，因此进行的更改都不是对源文件进行更改，在安全桌面退出之后就会被自动清除掉。例如：在安全桌面内对一个 Word 文档修改后保存，用户切换到真实桌面后可发现原来的 Word 文档并没有被修改。

安全桌面内对整个文件系统都进行了重定向，所有在安全桌面中被运行过的文件或者被访问过的数据都将被重定向。网络上的木马软件如果想要对桌面内的任何软件进行挂马、注入，所有的影响都只能被限制在安全桌面中；网络上的病毒文件如果想要保存到在本机中的硬盘，也会被重定向到特定临时区域并被加密转换，不会影响到真实桌面。

2.3.2 注册表操作重定向

和文件操作重定向类似，在安全桌面内对注册表的操作也会被重定向，例如病毒或木马软件修改 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services 注册表，实际上是对一个虚拟化的注册表进行修改，而这些修改并不会影响真实桌面内的 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services 注册表。通过这种重定向虚拟化隔离的方式，可屏蔽病毒或木马软件对真实桌面的影响。

2.3.3 可执行文件控制

缺省情况下，可在安全桌面内执行真实桌面内安装的软件，但在一些强制安全策略下，管理员可配置一个应用程序白名单，只允许在安全桌面内执行白名单内的软件，其余不在白名单外的应用程序不运行运行。为了减少管理员的配置难度，系统默认的一些关键应用缺省添加在白名单内，例如 word、IE 等。

对于需要以单独进程运行的病毒软件，由于其程序不在白名单内，将不能在安全桌面内正常运行。在这种实现方式下，即可避免安全桌面内新增病毒程序运行，也可避免真实桌面内原有病毒程序在安全桌面内运行。

2.4 机密数据防泄露

在允许真实桌面访问低密区而安全桌面内访问高密区的场景下，需要防止数据从高密区泄漏到低密区。通过控制安全桌面内访问真实桌面的文件路径、进行注册表编辑控制、禁止终端外设访问、控制网络访问控制等多种方式防止机密数据泄漏。

在允许真实桌面访问高密区而安全桌面内访问低密区的场景下，需要防止将机密数据从真实桌面内转移到安全桌面导致机密数据泄漏。在这种场景下，区域智慧隔离方案通过控制安全桌面内能够访问真实桌面的文件路径防止病毒或木马将机密数据从真实桌面泄漏到安全桌面，不能防止用户主动将真实桌面内的数据拷贝到安全桌面。

2.4.1 文件访问控制

在已经发生的企业泄密案件中，有很大部分互联网泄密案隶属于被动泄密，即不是由企业用户主动盗取机密数据，而是由于计算机终端被入侵、被植入木马后门等恶意程序导致机密数据被非法盗取。

为了防止安全桌面内病毒或木马等软件在用户不知情的情况下将真实桌面内的机密数据复制到安全桌面，管理员可配置安全桌面内能够访问真实桌面文件路径，例如管理员可配置安全桌面内只能够访问 C 盘，那么安全桌面内的病毒软件将不能够将 C 盘外的文件拷贝到安全桌面内，从而避免机密数据跨区域泄漏。

2.4.2 文件重定向

当安全桌面和高密业务区域连接，而真实桌面和低密业务区域连接时，文件重定向功能可防止将安全桌面内的机密数据泄漏到真实桌面。

依赖于文件重定向功能，用户在安全桌面内将机密数据保存到磁盘的一个文件路径时，实际是保存在安全桌面内的一个虚拟化重定向的文件路径下，该路径对用户隐藏。当用户切换到真实桌面后，并不能在真实桌面的文件路径下访问到保存的机密数据。

2.4.3 外设禁用

当安全桌面内保存有机密数据时，如果不对终端的外设进行访问控制，恶意用户将有可能通过打印、U 盘拷贝等方式将机密数据带离安全桌面，为了防止此类行为发生，区域智慧隔离

方案提供配置选项，使得管理员可禁止安全桌面内访问终端外设。可进行访问控制的终端外部设备包括：

1) 打印机
2) USB存储设备
3) COM接口

2.4.4 网络访问控制

通过业务区域隔离组网，用户终端正常情况下只能访问一个业务区域。对于特殊岗位、特殊部门存在跨业务区域访问时，可通过登录安全接入网关启动安全桌面，在安全桌面内访问另外一个业务区域的网络。尽管如此，在安全桌面内能够访问的另外一个业务区域网络的权限也需要受控，从安全角度看，能够允许访问的网络应满足“最小开放”原则，即在满足正常工作需求的前提下，能够开放的访问权限越小越好。

区域智慧隔离解决方案提供安全桌面内网络访问控制的功能，管理员可在安全接入网关上配置允许安全桌面内访问的网段，并下发到接入终端上。接入终端上启动安全桌面后，根据管理员的策略对用户的网络访问行为进行管控，用户在安全桌面内只能够访问管理员开放的特定网段，任何访问未开放网络的行为都将被阻止。

2.4.5 透明加解密

在安全桌面中，所有被修改过的文件、安全桌面内产生的数据都将被加密保存，加密算法采用强度最高的 AES256，加密密钥动态生成，保存在安全接入网关中，并按周期进行更新。

安全桌面中对文件、配置数据等信息的加解密是自动完成，对于用户来说透明，即用户不用关心什么时候加密、什么时候解密、哪些信息需要加密等问题。例如从网络中下载的文件，在安全桌面内可以正常地打开、编辑、保存，但从真实桌面中看，这个文件是加密的，在真实桌面内不能打开，即使将该文件拷贝到其他终端上也无法获取文件存储的信息。

当安全桌面内访问互联网，并从互联网上感染了病毒和木马后，由于安全桌面对文件进行了透明加解密，导致加密后的病毒或木马在真实桌面内不能解密运行，从而避免了病毒或木马的运行和扩散感染。

2.4.6 防截屏

通过截屏（屏幕拷贝）的方式也可能导致关键信息的泄漏，区域智慧隔离解决方案考虑到这种风险，并提供了部分解决措施。

用户切换到安全桌面后，安全接入网关的客户端软件将屏蔽键盘上的“屏幕打印键”，禁止用户使用该按键进行屏幕拷贝；除次之外，安全接入网关的客户端软件还会对 windows 系统的截屏 API 函数进行管理，防止截屏软件进行屏幕拷贝。

除了对本机的直接截屏进行防范之外，区域智慧隔离解决方案还对一部分间接截屏进行防范。间接截屏方式包括以下几种：

1) 远程访问：

当安全桌面内存在机密数据时恶意用户可能通过远程访问机制（例如 mstsc ）登录到特定终端上，并启动安全桌面接入业务区域，此时恶意用户可能会尝试在发起远程连接的终端上对安全桌面内的机密数据进行截屏；当真实桌面和安全桌面同时存在，并且真实桌面内存在机密数据时，恶意用户也可能远程连接到真实桌面拷贝屏幕。

管理员可在安全接入网关上配置策略，限制远程连接后只能访问真实桌面或者只能访问安全桌面，通过不同的策略灵活应对上述两种不同场景。

2) 虚拟机环境：

恶意用户也可能通过在虚拟机环境中启动安全桌面并访问机密数据，然后在真实桌面对虚拟机进行屏幕拷贝，为了避免这种途径的数据泄露，智慧区域隔离的安全桌面禁止在虚拟机环境中启动。

3) 桌面共享：

恶意用户也可能在接入终端上启动安全桌面，然后将真实桌面通过网络共享给其他终端，并在其他终端上进行屏幕拷贝。这种情况下，不能简单通过防截屏功能防止机密数据泄露，管理员可配置一些复杂的安全策略避免数据泄露，例如禁止安全桌面内启动屏幕共享程序、禁止安全桌面和真实桌面切换、系统开机后自启动安全桌面。通过上述安全策略，系统开机后自动进入安全桌面，恶意用户将不能在真实桌面内启动屏幕共享程序，而进入安全桌面后恶意用户也无法启动屏幕共享程序。

2.4.7 防粘贴板拷贝

对于一些特别机密的关键数据，即使无法通过文件传播，无法通过屏幕拷贝传播，windows系统提供的粘贴板机制也需要认证对待。Windows 粘贴板机制允许在一个进程中拷贝数据，这些数据保存在系统粘贴板中，切换到另外一个进城后，可将系统粘贴板中的数据复制出来。

为了避免安全桌面和真实桌面间通过系统粘贴板传播数据，安全桌面虚拟化了一个粘贴板，和系统粘贴板进行了隔离。在安全桌面内拷贝的数据保存在虚拟化粘贴板内，只能复制到安全桌面内的进程中，无法复制到真实桌面内的进程中。

2.5 高效办公

区域智慧隔离解决方案除了考虑安全特性之外，对于跨区域的业务办公在满足安全性的基础上提供一些措施，以提高办公效率，包括安全桌面保持功能、离线模式、文件透传、安全桌面协作等特性。

2.5.1 安全桌面保持

默认情况下，用户在安全桌面内所做的一切操作，都被临时加密保存在磁盘上，在用户退出安全桌面之后，所有的临时文件都被清除，这种实现方式的安全性最高，但是影响办公效率，例如当用户在安全桌面内进行作业，当工作未完成但也不得不中断时（参加重要会议、下班等情况），此时保存在安全桌面内的工作成果如果不能保存将严重影响工作效率。

针对上述情况，管理员可配置“安全桌面保持”功能。启动安全桌面保持功能后，用户在安全桌面的工作成果，在退出安全桌面时，自动以高强度加密的方式保存在磁盘上。这些加密数据只有在重新进入安全桌面后才能重新打开。

安全桌面保持功能和用户帐号相关，用户 A 在终端上保持的安全桌面，将只有用户 A 才能够重新进入，即使另外一个用户 B 拥有合法的权限在相同终端上进入安全桌面，他所进入的也是另外一个安全桌面，而不能访问用户 A 的数据。

安全桌面保持功能保存的数据的安全性，依赖于高强度加密，区域智慧隔离解决方案充分考虑了加密的安全性，包括加密算法的选取、加密密钥的生成和管理、加密密钥的更新等各方面。

2.5.2 离线模式

离线模式是针对移动办公场景的一个重要功能，例如用户在公司启用安全桌面进行作业，下班后用户可能希望将未完成的作业带回家继续完成；或者用户使用无线网络接入公司网络，在安全桌面内办公，当用户失去网络连接后，用户可能希望能够继续办公。

区域智慧隔离解决方案中安全桌面提供离线模式，在离线模式下，用户可以在不连接安全接入网关的情况下启动安全桌面，并对安全桌面内保存的数据进行编辑保存。为了保证安全性，用户在离线情况下启动安全桌面也需要进行用户名、密码的认证。

2.5.3 文件透传

为了保证安全桌面内的机密数据泄漏到真实桌面，所以缺省情况下不允许将安全桌面内的文件保存到真实桌面。但在一些特殊情况下， 因为工作的需要非常有必要将安全桌面内的文件直接保存到本地真实桌面。

区域智慧隔离解决方案中安全桌面提供文件透穿功能，允许用户将安全桌面内的文件保存到真实桌面。但是该方式存在巨大的安全隐患，不建议管理员进行这样的配置，其安全隐患如下：

1) 安全桌面透传到真实桌面的文件未进行任何病毒检查，有可能将带毒的文件进行跨区域传播。
2) 安全桌面透传到真实桌面的文件未进行任何内容安全检查，管理员对用户透传的文件内容无法监控，无法审计。

2.5.4 安全文件传输

安全桌面提供的“文件透传”功能，可以在本地的真实桌面和安全桌面间快速传递文件，但其安全风险较大。区域智慧隔离解决方案推荐管理员选择“安全文件传输”方式在跨业务区域之间传递文件。

用户在安全桌面内编辑保存的数据文件，如果需要跨区域传递到另外一个业务区域， 用户可将该文件通过网络上传到一个特性的共享文件夹下。用户切换到真实桌面后可通过安全接入网关从共享文件夹下载所需的文件。

安全文件传输对于用户来说稍稍增加了复杂性，但是对于企业管理员来说极大了增强了安全性。首先管理员可配置用户所允许上传文件的共享文件夹、可配置用户所允许下载的共享文件夹、可配置用户上传下载文件格式、文件关键字监控等。

用户通过“安全文件传输”功能上传下载文件的操作都会被详细的记录，管理员可根据记录定期审计用户行为，回溯用户的非法操作。

2.5.5 安全桌面协作

当存在多用户协作场景时，通过安全桌面协作功能可支撑该工作方式。

默认情况下，用户起用安全桌面后，将和本地网络内的其他终端之间进行网络隔离，也就是说用户在安全桌面内无法访问到本地局域网内的其他用户终端。当一项工作需要多人完成时，该用户的工作成果无法传递给其他同事继续完成。通过“安全桌面协作”功能，可允许该用户在安全桌面内和另外一个用户的安全桌面进行网络通信，并且在网络中传递的工作成果以加密的方式保存避免网络窃密。

2.5.6 多安全桌面

在超过两个业务区域隔离的情况下，例如企业同时存在办公网、生产网、安防监控网等业务区域，如果存在同一个终端要求能够同时接入超过两个不同的业务区域时，可在终端上启动多个安全桌面，除本地桌面连接本地业务网络外，每一个安全桌面可连接一个不同的业务区域。

2.5.7 安装卸载

用户在安全桌面内办公，可能存在一些未知的应用程序，此时可在安全桌面内进行试安装、试运行。在安全桌面内运行测试，可在判断该程序确实无安全风险后，再将其安装到真实桌面中。由于安全桌面内提供文件重定向、注册表重定向等功能，可避免未知软件威胁到真实桌面内的安全。

2.6 易用性

2.6.1 桌面切换

用户在终端上启动多个工作桌面后，可在不同桌面之间切换。区域智慧隔离解决方案中用户可在终端屏幕上方浮动的导航条上进行屏幕切换。

3 方案亮点

3.1 方案优势

3.1.1 安全的区域隔离

华为区域智慧隔离解决方案通过综合运用文件/注册表/粘贴板重定向、透明加解密、防截屏、网络控制、外设控制等各种手段，可有效保障真实桌面与安全桌面之间的隔离，保障安全桌面与其它网络设备之间的隔离，保障安全桌面和外部设备之间的隔离。

华为区域智慧隔离解决方案对安全桌面内的数据使用 AES 256 高强度加密算法，并提供完整的加密密钥管理机制，通过安全的密钥管理、密码算法保障数据的高安全性。

3.1.2 专业的跨区域传输控制

对于必须的跨区文件数据传输，华为区域智慧隔离解决方案能够提供足够信赖的文件传输控制机制。管理员可配置策略，对跨区传输的文件内容进行扫描，禁止包含指定关键字的文件跨区传输；管理员也可配置审计策略，对所有跨区传输的数据文件提取指纹，用户文件的操作都会被详细的记录，管理员可根据记录定期审计用户行为，回溯用户的非授权操作。

3.1.3 部署便捷

华为区域智慧隔离解决方案之需在网络区域边界部署安全网关，即可提供多区域隔离功能。通过在一台安全网关上实现多个安全桌面区域之间的隔离，可实现上网安全桌面和办公安全桌面配套一体，简化网络部署节省部署成本。

对用户而言，安全桌面客户端可自动安装、自动升级 。客户端可提供多个安全桌面，用户可在多桌面之间自然顺畅地切换，有效节省操作步骤和时间，提高工作效率。