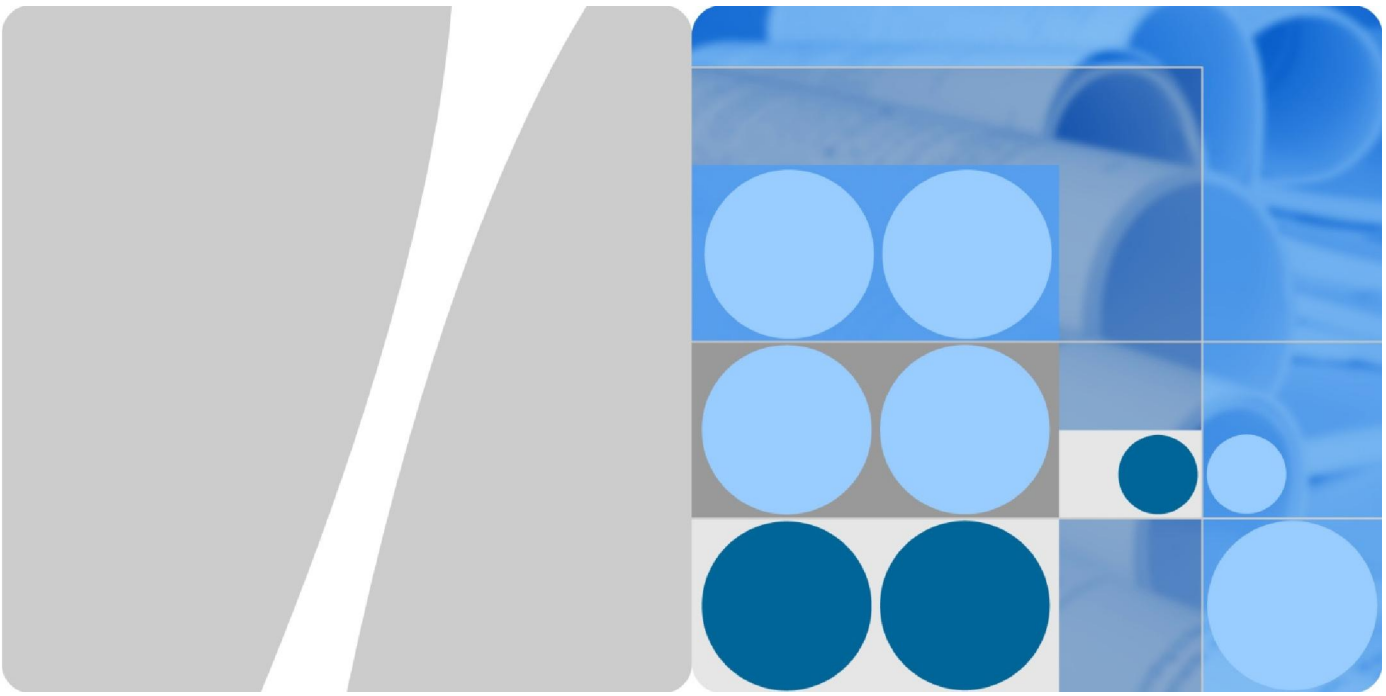


华为区域智慧隔离解决方案
销售指导书

华为技术有限公司

HUAWEI

商标声明

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

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 上市概述

华为智慧隔离解决方案通过领先的“安全沙箱”技术为不同区域的网络访问提供了安全的逻辑隔离方法，使用户能够在一台物理电脑上，同时建立多个逻辑隔离空间（互联网安全桌面、业务安全桌面、涉密区安全桌面），在每个安全桌面中进行不同的网络访问，安全桌面内的操作通过安全策略得到控制，安全桌面退出后数据自动清除。有效地阻止病毒、木马对企业内网的攻击；可靠地防止涉密区机密数据有意泄漏（外设、截屏、二次跳转）和无意泄漏（病毒、木马攻击、忘锁屏）。同时，华为智慧隔离解决方案提供了安全的跨区域文件传输方法，支持指纹级的文件审计，保证文件传输安全可控，提高工作效率。

华为智慧隔离解决方案包括SVN2000/5000系列产品，具体为SVN2230、SVN2260、SVN5530、SVN5560。

2 市场机会点分析

2.1 机会点概述

如果互联网访问终端与办公终端为同一台设备，办公终端存储的涉密及敏感信息存在被非法窃取或泄露的可能，特别是被木马控制的终端和开启远程操作的终端，都有可能在用户不知情的情况下被窃取信息。如何在同一台设备上安全的访问互联网和办公网成为一个重要需求，对安全要求较高的银行、证券、电力行业需求特别迫切。

银监会也多次发文，要求商业银行增强信息安全。在《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》（银监办发[2011]158号） 和《关于加强银行网站及网银系统安全防范工作的通知》（银监办发[2011]175号）中要求商业银行：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。《商业银行信息科技风险管理指引》（银监发[2009]19号）第二十四条规定：商业银行应根据信息安全级别，将网络划分为不同的逻辑安全域（以下简称为域）。应该对下列安全因素进行评估，并根据安全级别定义和评估结果实施有效的安全控制，如对每个域和整个网络进行物理或逻辑分区、实现网络内容过滤、逻辑访问控制、传输加密、网络监控、记录活动日志等。

证券行业期盼已久的“轻型营业部”试点即将推出，国内已有3家券商获准试点，3家券商为中信证券、国信证券和国泰君安证券。所谓轻型营业部，是指采用非现场交易模式的营业部。营业部通过减少后台人员、缩减面积、简化信息系统等“轻型化”后台设置降低运营成本，主要开设在空白低竞争区域，以增量客户交易佣金为主要收入。其营业面积、人员配置和运营成本都将远远低于传统的证券营业部，成本优势明显。

从目前市场拓展情况看，华为智慧隔离解决方案的市场机会点来自以下几个方面：

1）证券行业的轻型营业部：轻型营业部的员工需要使用一台设备访问互联网和证券办公网，互联网和证券办公网的安全隔离需求就产生了，带来了安全的市场机会。

2）银行的办公上网的安全隔离：银行的员工也存在着使用一台设备访问互联网和银行办公网，但

是要求两者互相隔离，避免病毒木马传播到办公网，避免银行敏感数据泄漏到互联网。

2.2 竞争格局

华为智慧隔离解决方案的市场目前主要集中在银行、证券、电力、大企业几个行业中，以上几个领域中主要竞争对手分布如下：

行业	主要竞争对手	竞争区域
银行/证券	深信服	中国
电力	深信服	中国
大企业	深信服	中国
其他	暂无	全球

具体竞争对手分析详见《华为智慧隔离解决方案竞争分析报告》。

3 解决方案销售整体策略

3.1 客户价值

华为智慧隔离解决方案的主要定位是：面向全球行业市场，重点行业：金融（银行/证券）、电力、大企业。华为智慧隔离解决方案为不同区域的网络访问提供了安全的逻辑隔离方法，使用户能够在一台物理电脑上，同时建立多个逻辑隔离空间（安全桌面），在每个安全桌面中进行不同的企业内部网络访问，保证了企业内部不同网络的有效隔离，保护了内部网络安全；智慧隔离解决方案也提供了安全的跨区域的文件传输方法，也支持指纹级的文件审计，保证文件传输安全可控。

3.2 版本迁移和生命周期

本版本是第一个解决方案发布版本，将于2016年12月31日停止销售，2017年12月31日停止生产，2019年12月31日停止服务。

3.3 解决方案亮点

- **完备的区域隔离，一机多用，降低投资成本**

  领先的安全沙箱：将内网和互联网安全隔离，有效防止病毒、木马对内网的攻击，配置只能运行的进程名单，防止员工运行于工作无关的应用，提高工作效率。

  专业的多实例技术：一个物理桌面内同时创建多个安全桌面，不同的安全桌面访问不同的业务，一机多用，大幅度降低投资成本

- **领先的数据防泄漏机制，数据安全无忧**

  完备的文件访问隔离：在安全桌面中只允许用户操作真实桌面指定的文件夹和目录，跨区域获取的数据文件重定向加密存储在虚拟空间中，退出安全桌面后无痕化清除。

  外设及网络访问控制：可以设置禁止安全桌面内访问终端外设及网络传输。

高强度透明加解密：在安全桌面内产生的数据都将被加密保存，采用强度最高的 AES256 加密算法，加密密钥动态生成，保存在 SVN 网关中，周期更新。

防截屏、防粘贴板拷贝：通过屏蔽截屏操作、虚拟化粘贴板等措施，防止机密数据泄漏。

- **专业的跨区域传输控制，数据传输无忧**

文件内容扫描：跨区域数据传输和安全桌面与真实桌面的数据导入导出都支持按关键字进行内容监控。

指纹级操作审计：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，回溯用户的非法操作。

- **部署便捷，用户体验好，降低管理成本**

便捷的部署：只需在网络区域边界部署 SVN 网关、客户端可自动安装，极低的部署成本和维护成本。

桌面自动启动：安全桌面可以设置开机自启动、退出安全桌面注销或者关闭计算机。

多桌面任意切换：用户可在终端屏幕上方浮动的导航条上进行多屏幕切换、操作方便

3.4 上市策略

- 目标市场

国内金融（银行/证券）、电力、大企业为主要目标市场。

海外大企业为主要目标市场。

- 上市节奏

SVN V200R002C00 版本将于 2012 年 12 月底可上市销售。

- 销售策略

引导客户关注我们的解决方案亮点（请参考第 3.3 章节）。

引导客户关注友商的不足（请参考《华为智慧隔离解决方案竞争分析报告》）。

注：SVN5530、SVN5560 已经标配了加密卡，不需要再单独配置。

- 销售限制

目前只能支持 Windows XP、2003、Win7 操作系统，其他操作系统暂不支持；如有客户需要支持新的操作系统，请与片区项目负责人联系。

3.5 License 策略

- License 销售策略

  华为智慧隔离解决方案可销售 SVN 硬件和软件 License。软件 License 包括 SSL VPN 并发用户数、安全桌面并发用户数、安全数传并发用户数三种。如果客户购买安全桌面并发用户数或安全数传并发用户数，则客户必须购买同等数量的 SSL VPN 并发用户数。客户购买的安全桌面并发用户数或安全数传并发用户数的数量可以小于但不能超过 SSL VPN 并发用户数的数量。

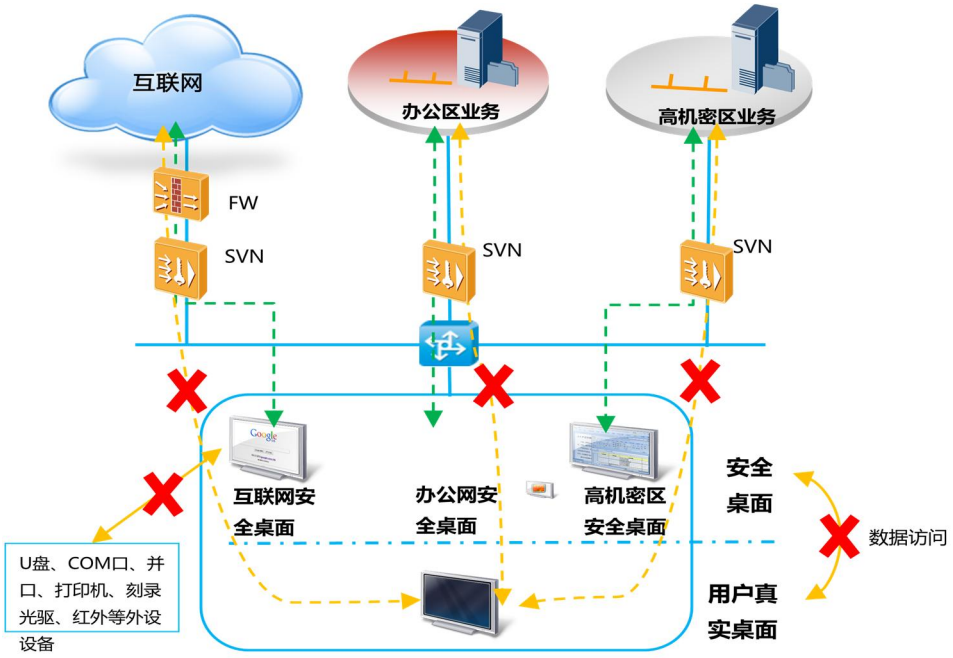
4 版本特性及解决方案

4.1 关键特性

解决方案关键特性简介：

名称	简介
安全桌面的接入控制	用户开启安全桌面登录安全接入网关，可提供多种丰富的认证方式。
终端安全检查	对接入终端设备的环境进行检查，包括操作系统、补丁、进程、端口、注册表等
病毒传播防范	在安全桌面中的病毒木马不能被扩散到真实桌面，防止了病毒木马的传播。
文件访问控制	真实桌面中数据文件和文档不能在安全桌面中可见，防止用户将真实桌面中的文件通过互联网安全桌面扩散传播。
防二次跳转	在安全桌面中禁止用户使用远程桌面跳转到其他电脑，防止数据泄密。
外设及网络访问控制	禁止用户通过打印、U 盘拷贝及网络文件传输等方式将机密数据带离安全桌面
防截屏、防粘贴板拷贝	禁止用户对屏幕进行截屏操作和粘贴拷贝，防止机密数据泄露。
安全数据传输	支持文件等数据在不同网络区域中安全传输
定制桌面背景	可对用户安全桌面的背景图片进行定制
单机多安全桌面，同时访问多个安全区域	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。安全桌面用户可在终端屏幕上方浮动的导航条上进行屏幕切换。
自我防护	防止用户对安全桌面客户端软件的非法卸载和强制关闭

4.2 解决方案介绍

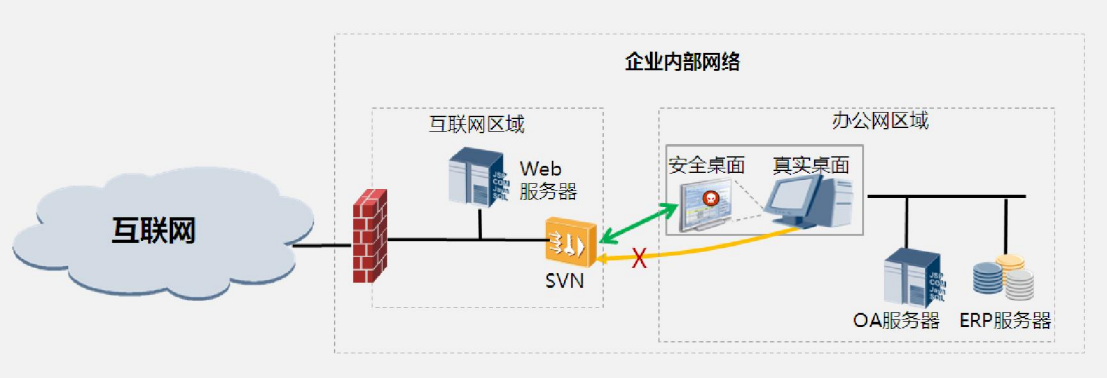


华为推出的智慧隔离安全解决方案弥补了网络区域隔离现状的不足，通过领先的“安全沙箱”技术为不同区域的网络访问提供了安全的逻辑隔离方法，使用户能够在一台物理电脑上，同时建立多个逻辑隔离空间（互联网安全桌面、业务安全桌面、涉密区安全桌面），在每个安全桌面中进行不同的网络访问，安全桌面内的操作通过安全策略得到控制，安全桌面退出后数据自动清除。有效地阻止病毒、木马对企业内网的攻击；可靠地防止涉密区机密数据有意泄漏（外设、截屏、二次跳转）和无意泄漏（病毒、木马攻击、忘锁屏）。同时，华为区域智慧隔离安全解决方案提供了安全的跨区域文件传输方法，支持指纹级的文件审计，保证文件传输安全可控，提高工作效率。

5 典型应用场景

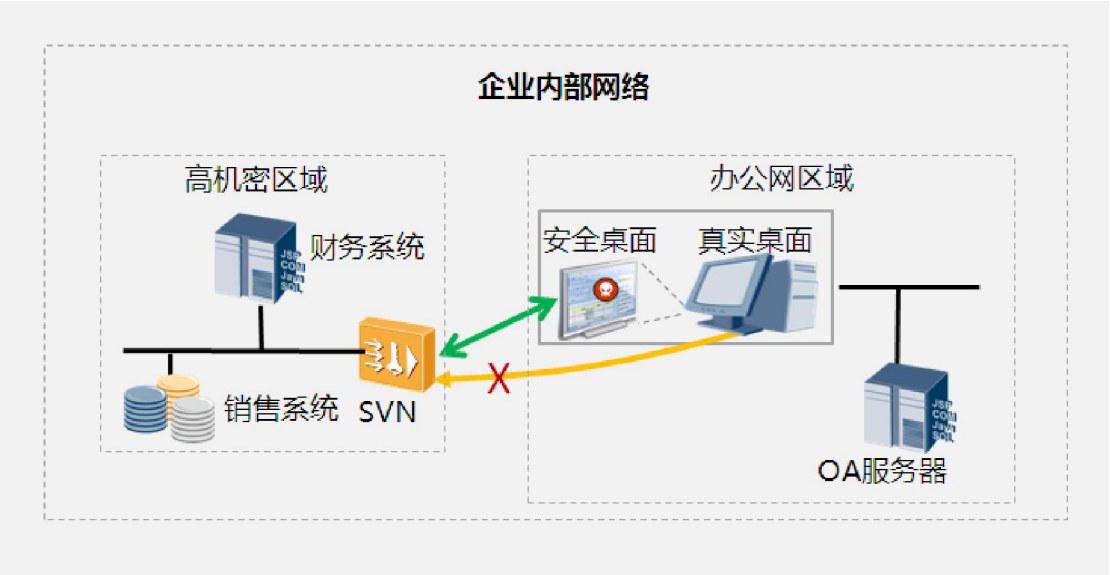
5.1 互联网安全访问场景

在企业的办公网和互联网边界部署SVN2000/5000系列网关，在用户的PC/笔记本终端上安装客户端软件，则用户就可以启动安全桌面，在安全桌面中访问互联网，保证来自互联网的内容仅仅在安全桌面空间中，木马病毒不能传播到其他办公网络设备上。用户也可以使用安全数传功能，将互联网的资源放到中转服务器上，通过管理员安全审核后，用户使用真实桌面再下载到本地，保证了来自互联网的内容经过安全审核后可以到达用户电脑，满足了业务需要。



5.2 高机密区安全访问

在企业的办公网和高机密网络区域之间部署SVN2000/5000系列网关，在用户的PC/笔记本终端上安装客户端软件，则用户就可以启动安全桌面，在安全桌面中访问高机密网络区域中的数据，保证来自高机密数据仅仅在安全桌面空间中，不能传播到其他办公网络设备上，数据传输也是经过高强度加密的。


企业内部网络
高机密区域
财务系统
销售系统
SVN
办公网区域
安全桌面
真实桌面
OA服务器

6 扩容升级和兼容性

6.1 升级能力

华为智慧隔离解决方案核心产品是SVN2000/5000，升级能力与SVN2000/5000产品保持一致。如果有特殊项目需求，请联系片区项目负责人。

6.2 扩容改造能力

华为智慧隔离解决方案核心产品是SVN2000/5000，扩容改造能力与SVN2000/5000产品保持一致，可以通过增加SVN设备数量来进行扩容。如果有特殊项目需求，请联系片区项目负责人。

6.3 兼容性

华为智慧隔离解决方案核心产品是SVN2000/5000，SVN2000/5000产品支持以下网管系统的管理：

- 华为公司网管平台 M2000
- 华为公司网管平台 I2000
- 华为公司网管平台 U2000
- 华为公司网管平台 VSM

7 交付与服务

7.1 备货预测

通过提前备货的措施，来有效缩短交付时间，如有紧急项目发货要求，请提前联系片区项目负责人。

7.2 交付时间

通过一系列措施提升低成本服务能力，缩短交付时间：

- 专业团队支撑规模开局，实现快速交付。
- 华为具有强大开发团队，能够快速实现的各种需求；具有全球各地技术支援工程师，随时支持各地项目交付。

8 注意事项

注意事项：

1. 贸易禁运和贸易管制国家（5+9 国家）禁止销售；
2. 政府涉密类业务禁止销售；
3. 国家与社会安全监控体系类项目管控销售；
4. 其他类项目和业务正常销售；

管控销售解释：

1. *要坚持被集成战略，不做直销，坚决不涉及内容解析，也不能集成和 OEM 内容解析产品。*
2. *要避免引导由中国政府直接/间接出资或优惠贷款。*
3. *在采取了规避相关法律及管制政策风险措施后（如在合同中明确了免责条款），基于商业原则和风险溢价原则，允许提供标准产品和部件。*