HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

华为区域智慧隔离安全解决方案

技术交流版

enterprise.huawei.com
HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Content

HUAWEI

企业网络访问安全风险

泄密事件频发

手机用户信息被盗

2011年3月至8月，王某参与研发与维护某运营商计费经营系统，利用工作便利，多次侵入这家通信运营公司用户数据库盗取1394万手机用户个人信息并出售。

潜艇资料遭泄密

某所科研人员彭某收到了一封“国防科工委办公厅的中秋贺卡”，信手点开后，邮件中某境外机构特制的间谍程序被激活，彭某电脑中违规存储的潜艇隐身机密材料被从网上窃走

iPad2设计图遭泄露

iPad2后壳设计图遭代工企业员工主动泄密给山寨厂商，导致苹果iPad2还没上市，抢iPad2商机的山寨版不单抢先在苹果iPad2上市前推出山寨版iPad2保护套，甚至还在美国CES展上贩卖

企业网络访问安全风险

内网病毒爆发

国内某大型企业网络现状：

- 企业PC终端数量24万台
- 仅通过防火墙划分安全域
- 办公网终端同时访问互联网
- 每月病毒报警200万次，导致网络瘫痪，业务中断

解读：互联网访问终端与办公终端为同一台设备，导致病毒通过网站挂马、非法下载等方式在办公网传播，造成办公网病毒泛滥、终端被动泄密

传统隔离技术分析

完全物理隔离

部署两套独立的网络设备、布线及办公终端。安全性好，但成本高。

双网线隔离卡

终端加配隔离卡，实现单主机双硬盘网卡，两个硬盘网卡对应两套独立的网络设备。

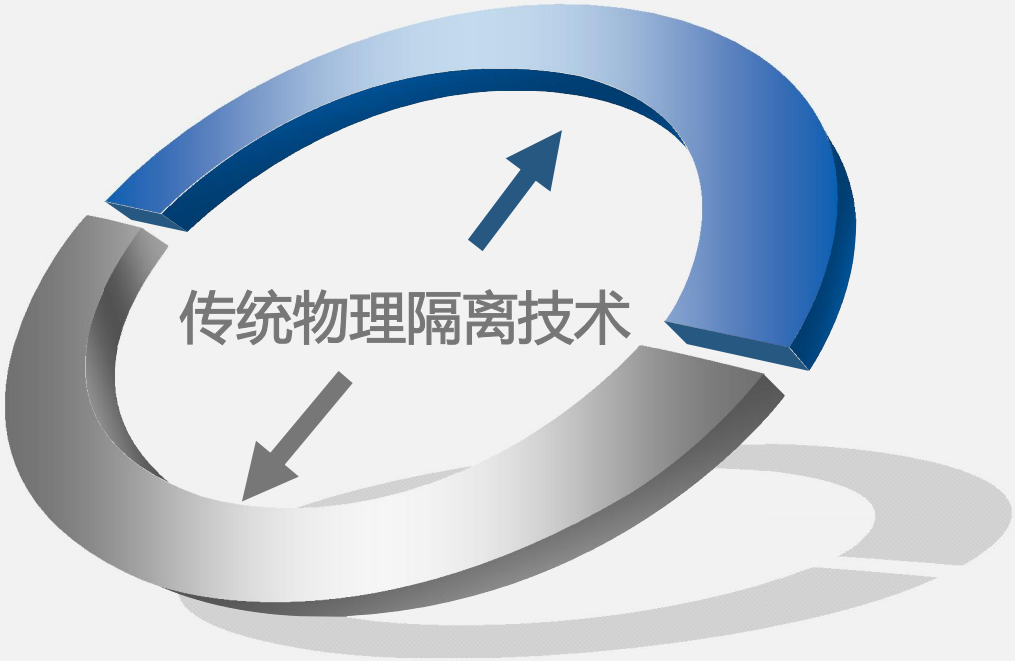
单网线隔离卡

基于单网线的隔离卡，加上网络选择器技术，将不同的电平信息传递到网络选择端。

物理隔离网闸

在应用层将将数据包进行分解或重组为静态数据，然后以“摆渡文件”的形式来传递原始数据。

传统物理隔离技术不足



- 物理隔离技术仅仅是一种被动的隔离开关，手段单一，没有与其他安全技术进行配合；
- 物理隔离不能做到安全状态检测，容易被非法人员利用而混入内部网络；
- 内部防范措施薄弱。由于内外网的存储介质都在本地，不能有效地防止内部人员的信息主动泄密行为，尤其是内部人员作案；
- 复核取证难度大。内部网络信息一旦泄露出去，无法进行复核、取证、确认信息泄露的行为人有相当的困难。

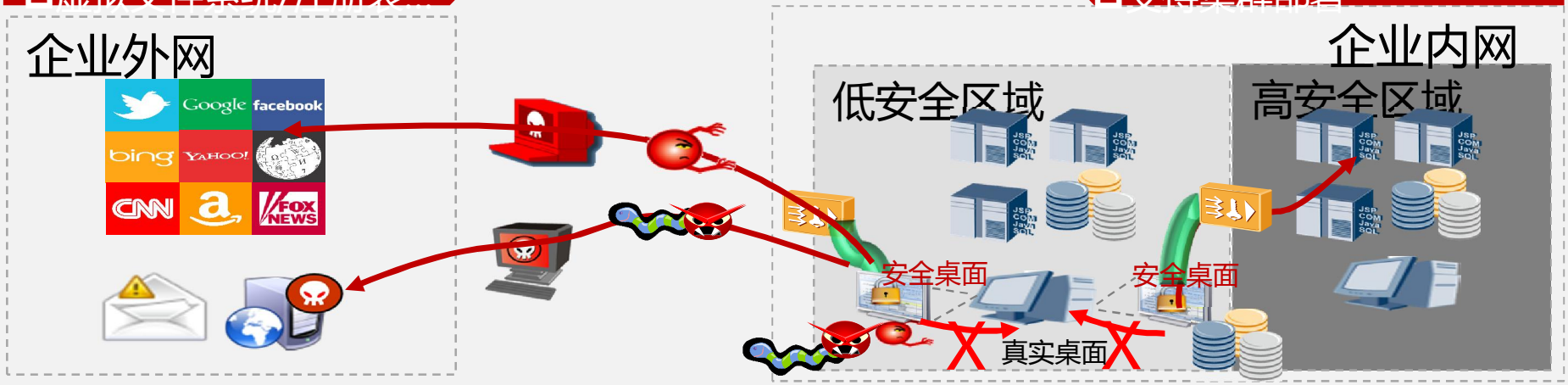
Content

HUAWEI

区域智慧隔离方案介绍

兼容桌面办公应用
- 可运行真实桌面应用
- 虚拟文件系统/注册表

部署不影响现有网络
- 接入网关旁路部署
- 支持集群部署



安全桌面客户端
- 基于安全沙箱技术
- 安全桌面与真实桌面隔离
- 兼容Windows操作系统

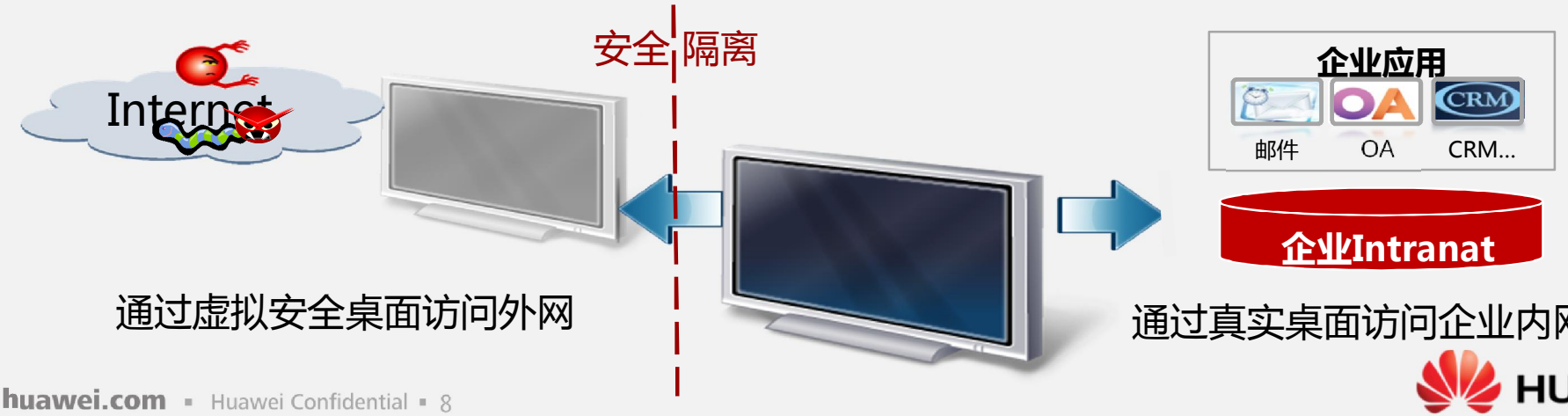
安全接入网关
- 身份认证
- VPN加解密
- 安全审计

区域智慧隔离方案中需要在不同安全区域边界部署安全接入网关， 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，终端通过**安全桌面**与安全接入网关之间的数据传输进行安全加密。

HUAWEI

什么是安全桌面

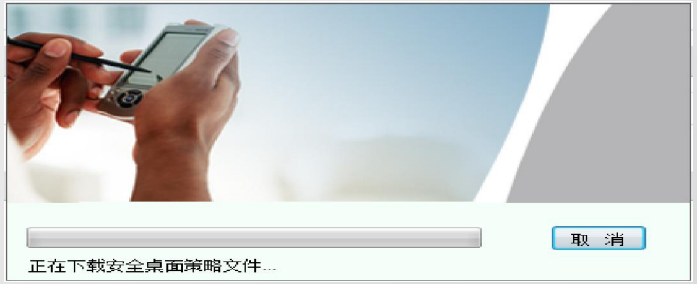
- 安全桌面生成现有操作系统的全新虚拟镜像，它具有真实Windows系统完全一样的功能。
- 进入虚拟系统后，所有操作都是在这个全新的独立的虚拟系统里面进行，可以独立安装运行软件,保存数据,拥有自己的独立桌面，不会对真正的系统产生任何影响。
- 当用户退出安全桌面时，之前在虚拟镜像系统里面所做的修改，全部都被还原。



安全桌面如何启动

一般用户登录操作系统只有一个桌面可以操作，即Windows默认桌面

1



SVN安全接入网关推送安全桌面客户端及策略文件到终端

3

用户登录SVN安全接入网关Portal页面

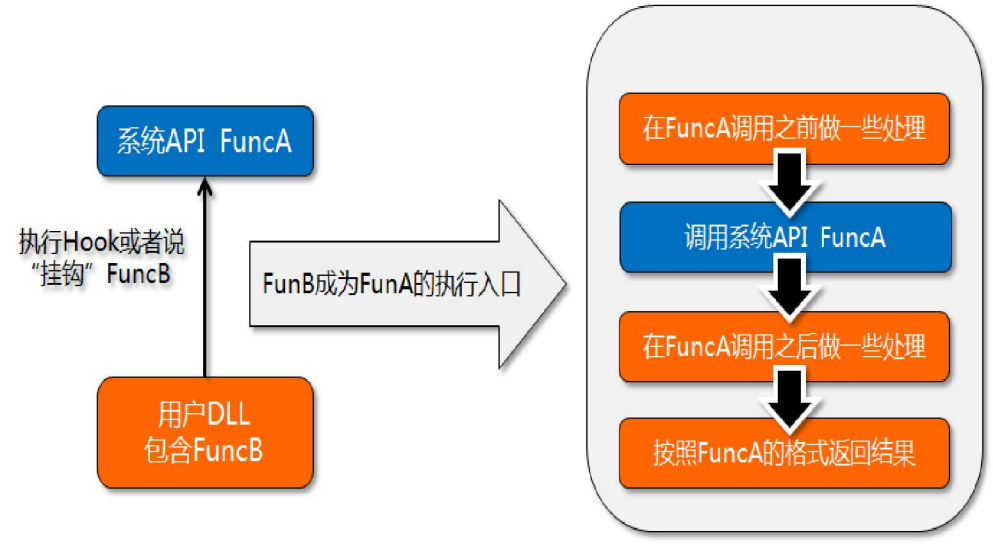
2

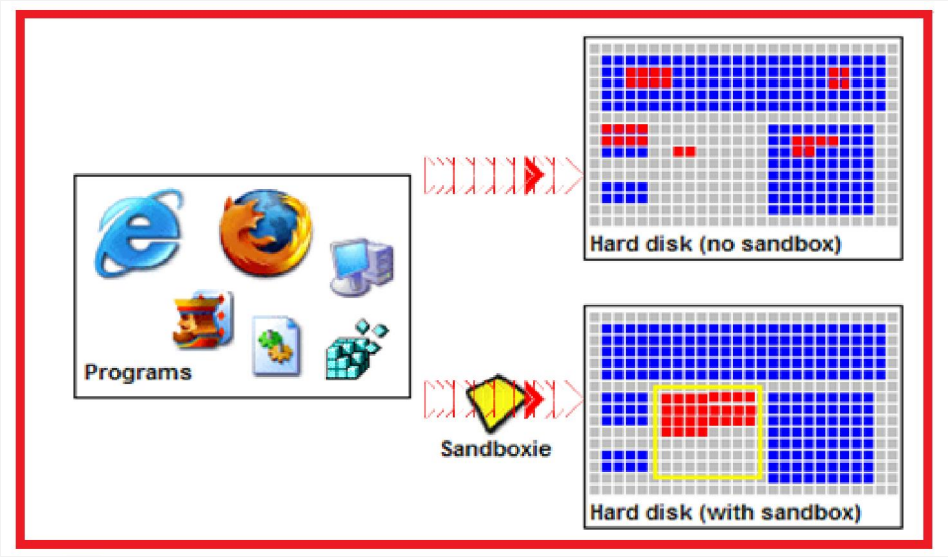
安全桌面启动并切换到前台，安全桌面与默认桌面数据隔离

4

HUAWEI

安全桌面关键技术——沙盒技术





安全沙盒对操作系统的文件读写、注册表项读写、程序运行、软件安装操作和COM实例创建的API进行了Hook。当上述操作发生时，通过沙盒技术，把程序生成和修改的文件（包括注册表和系统核心数据），重定向到自身文件夹中。通过加载自身的驱动来保护底层数据，属于驱动级别的保护。

沙盒技术是否安全?

2008年9月Chrome首次露面即公布了沙盒技术，其他主流浏览器开发商都在借鉴Google Chrome的安全标准，隔离来自其他操作系统的不可信任数据。

卡巴斯基安全部队2012应用沙盒2.0技术，分为安全桌面和安全浏览器两部分，针对应用程序和浏览器分别保护，将沙盒(Sandboxie)技术融入在了产品中，有效隔离病毒木马威胁

苹果要求明年3月起所有Mac软件采用沙盒技术

2011-11-07 15:06 来源：腾讯科技 作者：晁晖 RSS 复制链接 打印

核心提示：北京时间11月7日消息，据国外媒体报道，苹果通知软件开发商称，从明年3月1日起，向Mac App Store提交的软件必须采用“沙盒”（sandboxing）技术。

北京时间11月7日消息，据国外媒体报道，苹果通知软件开发商称，从明年3月1日起，向Mac App Store提交的软件必须采用“沙盒”（sandboxing）技术。

苹果要求软件采用沙盒技术可能会令部分开发商不满，但沙盒是一种更好的安全技术。尽管沙盒技术并不完美，但苹果的要求并不过分。

沙盒能隔离未经检验的代码修改活动，例如恶意件，有效地防止恶意件兴风作浪。

苹果在通知中称，“绝大多数Mac用户没有受到过恶意件的骚扰，我们在开发确保Mac用户继续不被骚扰的技术。从明年3月1日开始，所有向Mac App Store提交的软件都必须采用沙盒技术。通过限制软件可以使用的资源，在软件中采用沙盒技术是保护系统和用户安全的一个好途径，使恶意件更难危害用户的系统。”

Content

HUAWEI

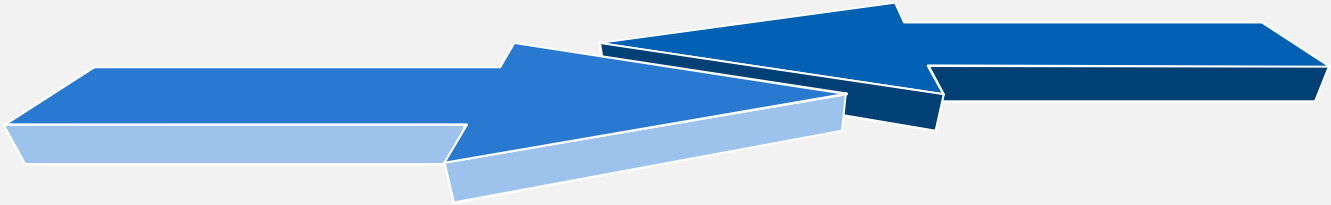
安全桌面应用场景

互联网病毒入侵防护

访问互联网时，常常会感染病毒、木马和间谍软件，严重时会造成计算机系统的崩溃。安全桌面内访问互联网，可以有效避免主机被感染

存储设备病毒入侵防护

移动存储设备，如U盘，很容易受病毒感染，直接在本机打开则很可能会导致本机也被感染。在安全桌面内打开，可以有效避免主机被感染



安全桌面是基于虚拟化技术的产品，利用虚拟化技术独有的隔离效果实现安全目的。

安全桌面除了可以隔离病毒以外，也可以用于隔离不同安全等级的网络。

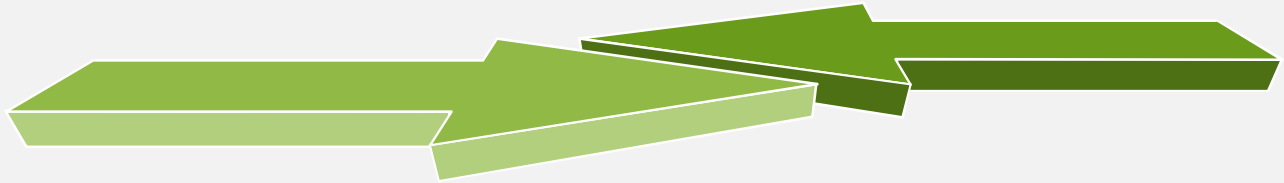
安全桌面应用场景

本机数据防泄密

互联网上充斥着各种木马程序和间谍软件，试图窃取用户本机隐私数据。安全桌面控制策略限制对本机数据的访问，任何试图窃取本机文件数据的行为都将被禁止。

高安全区域数据防泄密

用户通过低安全区域访问高安全区域，安全桌面控制策略限制机密网络内的数据转移到非安全的网络上来。管理者可以统一设置安全桌面的权限，分配其接入哪个级别的网络。



用户可以在同一台电脑上，通过不同的安全桌面，既可以访问机密内网也可以访问不安全的外网（互联网等）。不同安全桌面之间的文件传输是受控的（过滤或审批）

Content

HUAWEI

区域智慧隔离解决方案特点

HUAWEI

丰富的认证方式

主认证方式

- 本地用户认证（VPNDB）
- 外部用户认证（LDAP/AD/SecurID/Radius）

辅助认证方式

- 短信认证
- 图形码认证
- 终端标识码认证

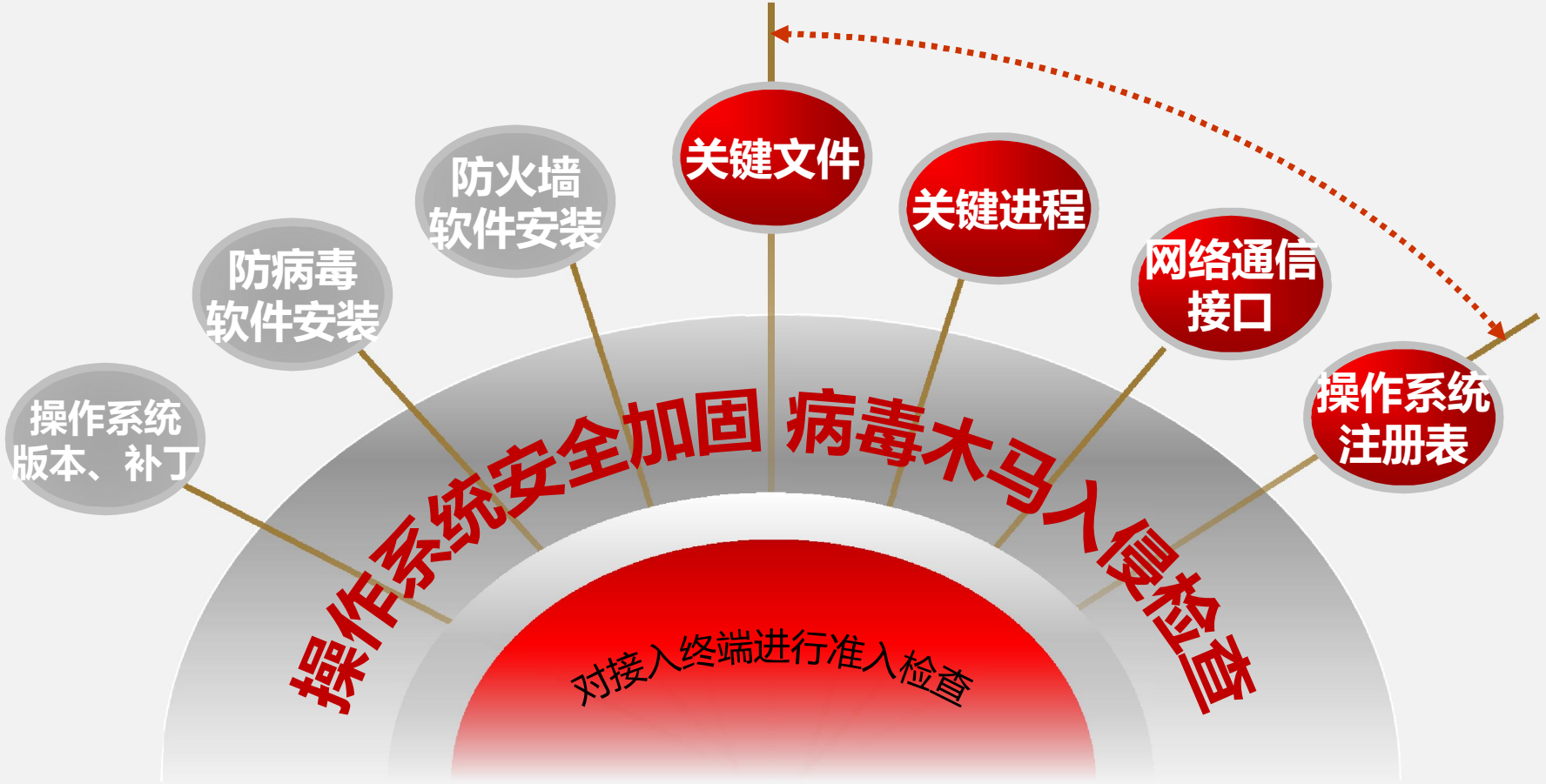
证书认证

- 证书匿名认证（只认证证书有效性）
- 证书挑战认证（双因素认证）——同时进行主认证和证书认证

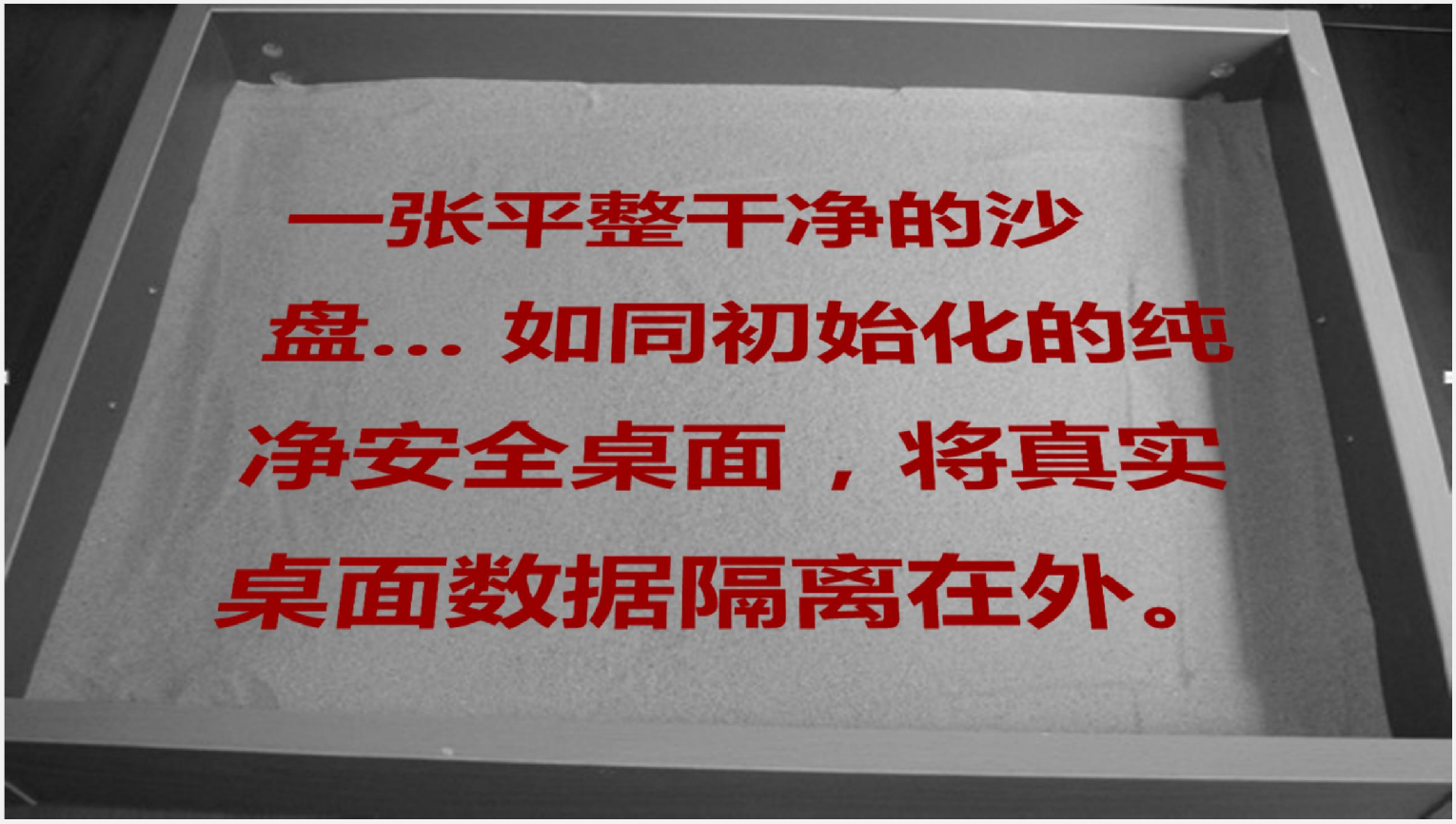
多级认证

- 最大支持三级主认证，三级认证均失败用户才会登录失败

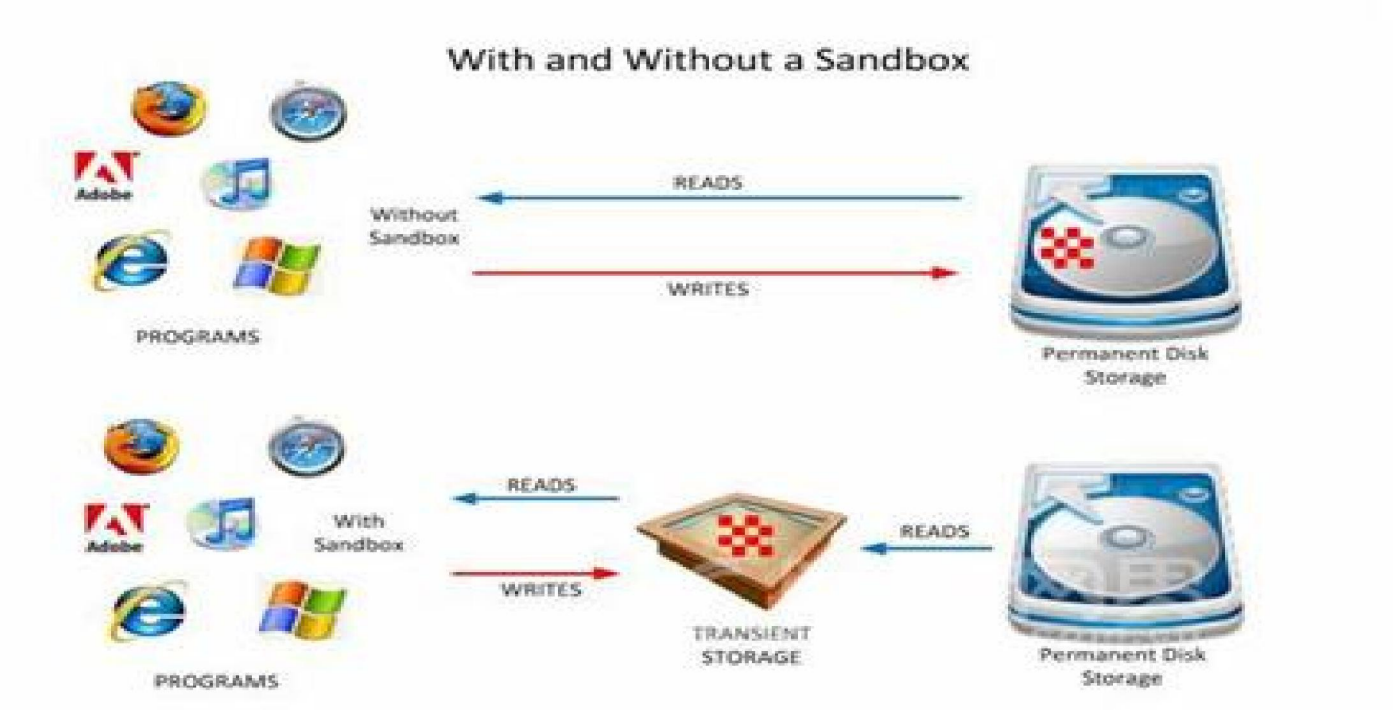
严格的接入控制策略


操作系统
版本、补丁
防病毒
软件安装
防火墙
软件安装
关键文件
关键进程
网络通信
接口
操作系统
注册表
操作系统安全加固 病毒木马入侵检查
对接入终端进行准入检查

纯净安全桌面启动



透明加解密虚拟空间



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（AES-256）保存在虚拟空间中，真实桌面下无法正常打开和运行

数据重定向隔离

使用安全桌面过程中，跨区域获取的数据文件重定向到虚拟空间中，退出安全桌面后，安全桌面内遗留的文件、对计算机终端做的任何修改都会被清除，用户终端将被还原成为启用安全桌面之前的状态。

外设及网络访问控制

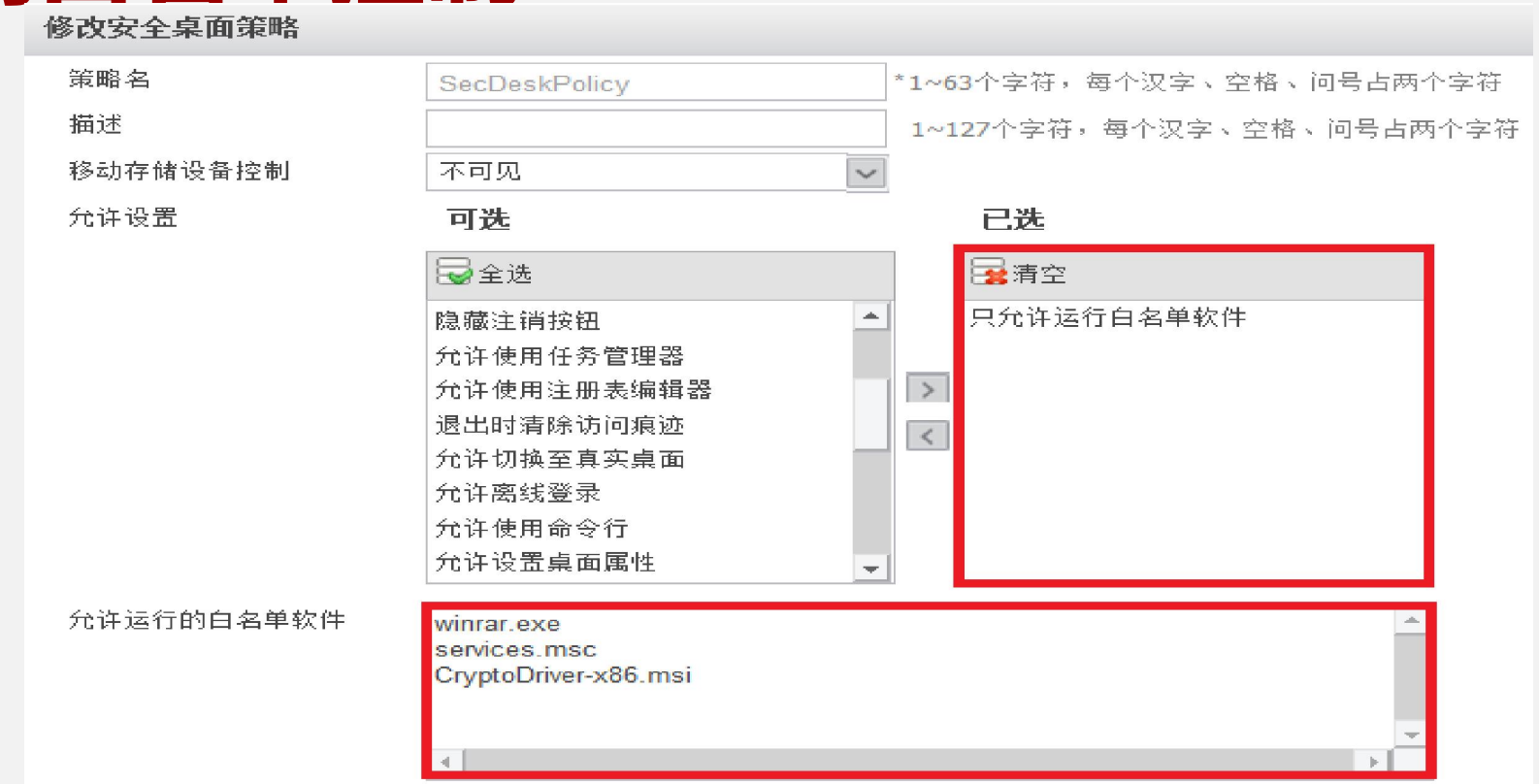
外设控制

- USB移动存储设备访问控制，可实现安全桌面内允许USB鼠标、USB KEY，禁止U盘
- 打印机使用控制，禁止/允许安全桌面内打印
- COM口使用控制，禁止/允许安全桌面内通过COM口发送、接收数据

网络访问控制

- 管理员设置安全桌面内访问控制列表，允许用户访问授权网络，为设置允许网段默认禁止
- 管理员设置安全桌面启动后，真实桌面访问控制列表，允许用户访问授权网络，为设置允许网段默认禁止

应用白名单控制



管理员设置安全桌面内应用程序白名单，未在白名单定义应用，将被禁止运行，防止数据越权访问或泄露。

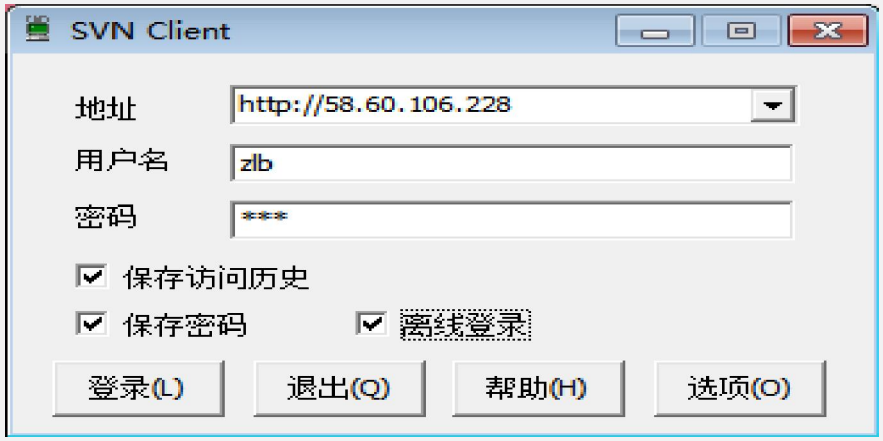
安全桌面保持

默认情况下，用户在安全桌面内所做的一切操作，在用户退出安全桌面之后都被清除，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。

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相同用户重新进入安全桌面后才能重新打开。

安全桌面离线模式

办公网用户在安全桌面下处理文件时，可能出现某项工作无法在工作时间内完成，希望将工作带回家完成。这时可以将安全桌面切换到离线模式登录，离线模式安全桌面对数据的隔离保护依然有效。



离线模式需要通过独立客户端软件登录，采用离线模式前需要通过在线模式首次登录网关一次，获取安全桌面策略文件及密钥材料

安全数据传输

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

操作习惯与真实桌面一致

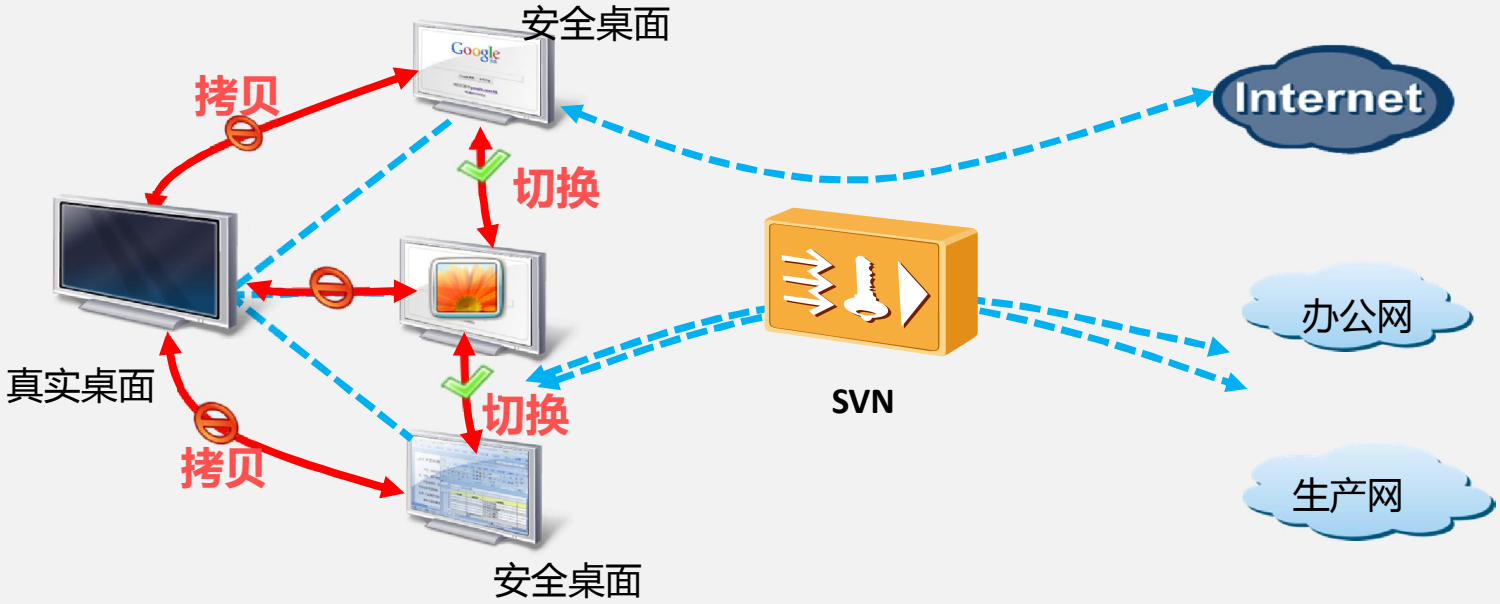
真实桌面

VS

安全桌面

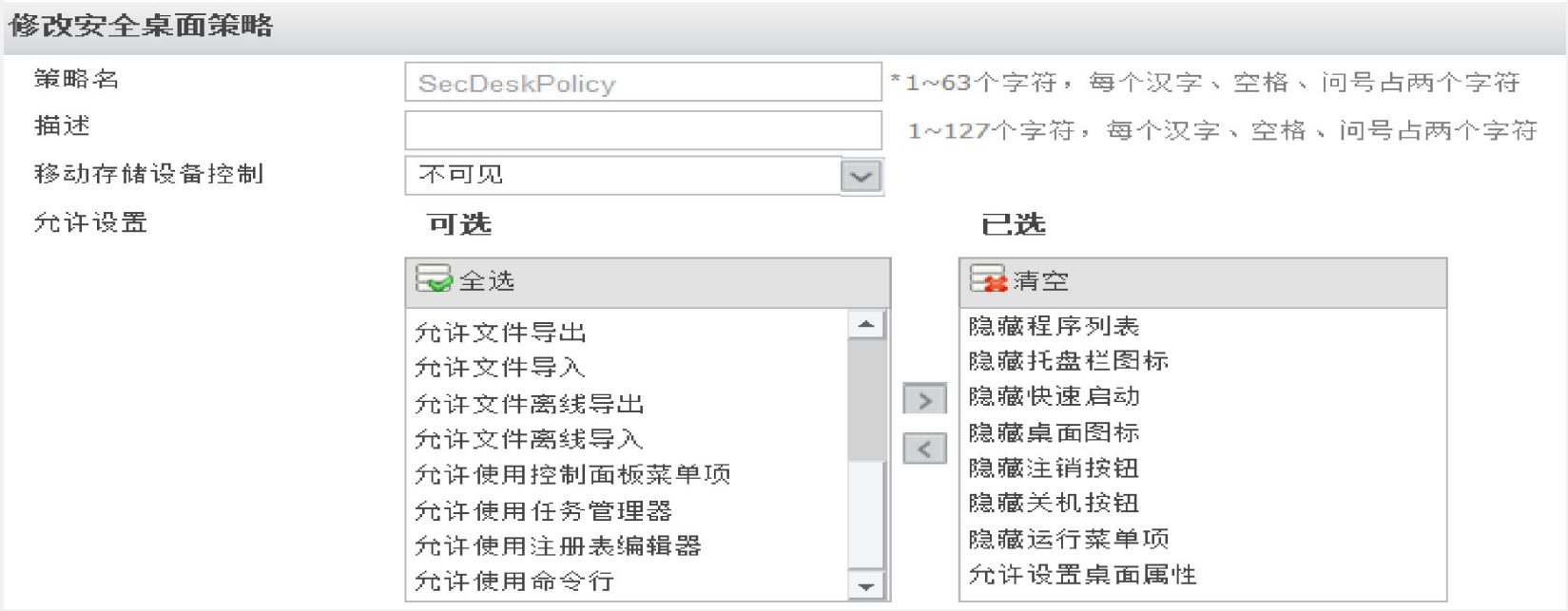
安全桌面内，操作性和原本的真实桌面是一致的，并且兼容真实桌面中的应用，所以用户可以在安全桌面内保持其原有的操作习惯，无需对终端操作人员进行培训

单机多安全桌面，桌面间任意切换



在超过两个业务区域隔离的情况下，例如办公网、业务网、互联网，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，每一个安全桌面可连接一个不同的业务区域。多安全桌面间可以任意切换。

安全桌面内背景、功能菜单自定义



管理员可设置安全桌面策略，在安全桌面内隐藏特定功能菜单项、按钮，允许或禁止安全桌面内设置桌面属性或使用命令行、注册表、控制面板、任务管理器等。

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY