解决方案实践

华为云办公安全

文档版本 1.0

发布日期 2022-11-10

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

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暗示的声明或保证。

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。

目 录

1 方案概述

应用场景

1. 普安场景实现一机多用
   - 场景描述

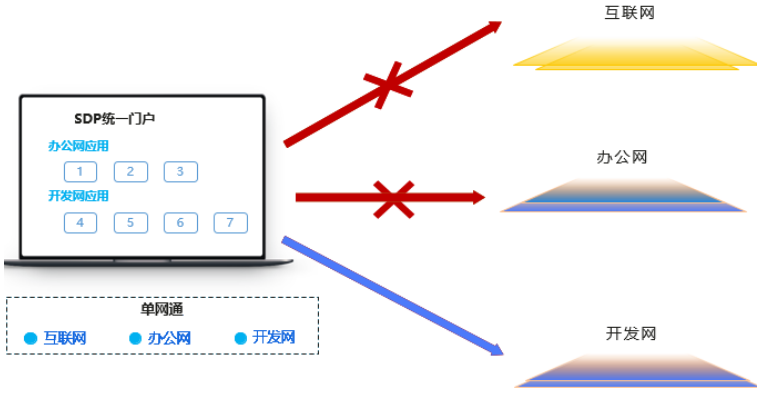
     终端需要连接多张网络，为实现网络隔离，连接每张网都需配置单独的终端或者VDI，投入成本和运维成本较高。

     疫情期间远程开发远程办公，核心代码和敏感数据存在泄露风险，VDI成本高，对出口带宽要求较高；
   - 解决方案

     单网通：终端用户在同一时间仅可访问单个网络；

     单台终端创建安全沙箱，沙箱之间及沙箱与本地数据隔离，沙箱通过安全网关访问相应的业务，并通过水印进行安全教育和泄密追溯；
   - 方案价值
     - 成本低：无需采购多台终端或VDI；
     - 体验好：用户只需操作单台终端，实现“一机多用”；
     - 高安全：数据隔离和通道隔离，同时实现业务的隐身；
     - 易运维：只需运维单台终端，运维工作大量缩减；

图 1-1 图示 1



2. 高安场景实现专机专用
   - 场景描述

     随着业务的需要，企业下发给员工配发设备，需要增强管控该类设备。

     - 专机私有化，员工私自下载软件。
     - 设备数据安全无法保障，违法外发。
     - 企业无法实时掌握配发设备使用情况，难以管理资产。
   - 解决方案

     配发设备专机专用，不允许私自下载软件及数据违法外发操作，提高设备使用效率
   - 方案价值

     i. 统一安全桌面，利用无法退出的特性实现专机专用和数据安全；
     ii. 其他：安全接入、安全桌面、应用商城、移动沙箱、安全水印
     iii. 专用配发pad开展移动业务

     图 1-2 图示 2

3. 移动应用场景实现应用隐藏
   - 场景描述

     - 客户将内部移动应用发布到钉钉、企业微信等软件上，需要将移动应用的服务端口独立开放到互联网，存在互联网暴露和被攻击风险；
     - 业务APP同样需要解决接入安全和数据防泄漏；
     - 行业监管加大对移动应用的安全检测力度，监管单位针对互联网暴露风险整改的意见
   - 解决方案

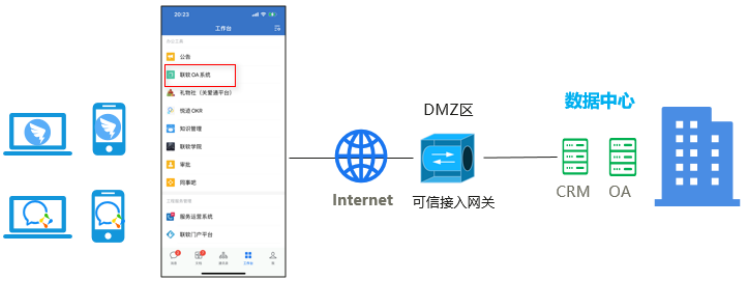
     在企业内网出口部署可信接入网关，将钉钉、企业微信上的移动应用URL代理到可信接入网关上，由可信接入网关统一转发到企业内网服务端；
   - 方案价值

     i. 安全：降低移动应用互联网暴露风险；

ii. 便捷：企业系统零改造；

iii. 成本：无需应用单独开发安全；

图 1-3 图示 3



4. 远程办公场景实现可信接入、网络隐藏

- 场景描述

  随着业务的发展，时代的进步，疫情的扩散，企业移动化办公，远程办公的需求逐渐增加，那么移动化办公、远程办公过程中，安全问题尤为突出。

  - 企业资产在互联网中暴露，容易被入侵。
  - 企业内部数据落地员工个人电脑，数据安全无法保证。
  - 由于移动化办公，终端与企业内业务应用互联通道处于互联网环境中，数据容易泄露

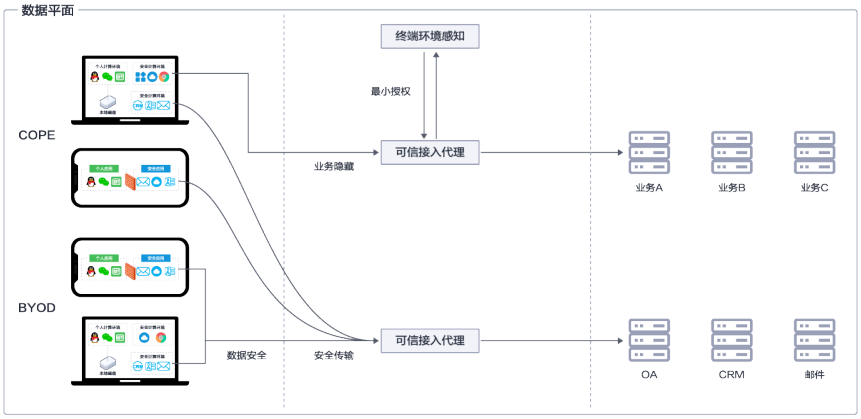
- 解决方案

  SPA敲门机制实现入口隐藏，应用级安全隧道保障传输安全，终端环境感知动态分配访问权限，应用统一门户及全生命周期管理，沙箱、水印等能力保障数据安全；

- 方案价值

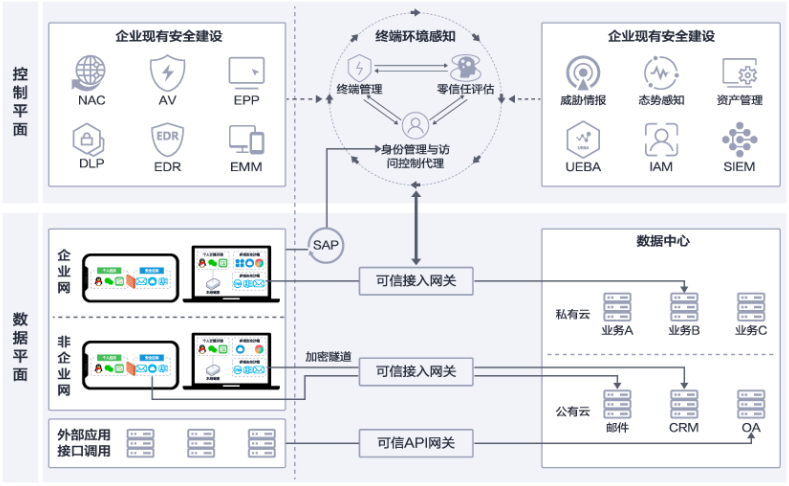
  - 业务应用隐藏在安全网关后面，互联网暴露面收敛
  - 应用统一管理和企业数据防泄漏
  - 身份认证、环境感知与动态授权，保证企业接入终端安全

图 1-4 图示 4



方案架构

图 1-5 架构图



架构描述：

1. 所有终端设备通过控制平面进行接入企业内部认证，通过终端标准化和身份认证进行信任评估，最小化授权访问
2. 所有企业业务隐藏在可信接入代理设备后，终端设备通过身份认证后访问可信接入代理设备，由可信接入设备进行代理访问企业业务
3. 终端设备与可信接入代理建立SSL应用级安全隧道，保护数据传输安全
4. 终端上设置沙箱，保证不同网络之间互相隔离，数据不落地，保护数据安全不泄露

方案优势

- 更安全
  - SPA机制“真隐藏”服务，暴露面收敛，天然抗攻击
  - 应用级加密隧道技术，避免内网全面暴露
  - 业内领先的安全沙箱、安全水印，防止企业数据外泄
  - 全面的环境感知能力和动态评分机制，提供持续可信访问
- 高效易用
  - 提供灵活、便捷的多因素认证方式
  - 支持SSO单点登录和手机扫码联动认证，无需反复认证
  - 统一门户，统一访问入口，规范用户访问行为
  - 部署简单、运维简单
  - 用户行为记录分析，提供丰富的决策依据
- 扩展性好
  - 微服务架构，按需灵活扩展模块
  - 标准API接口，轻松集成第三方系统；
  - 统一安全架构架构，可集成EPP、一个客户端实现内外网统一管理；

- 控制平面与数据平面分离，天然适配混合云网络

约束与限制

操作系统限制

- PC端操作系统：Win 7/10/11、Ubuntu、MAC OS支持3年内的版本（非Windows系统，部分功能不支持）；
- 移动端操作系统：Android、IOS、鸿蒙；

2 资源和成本规划

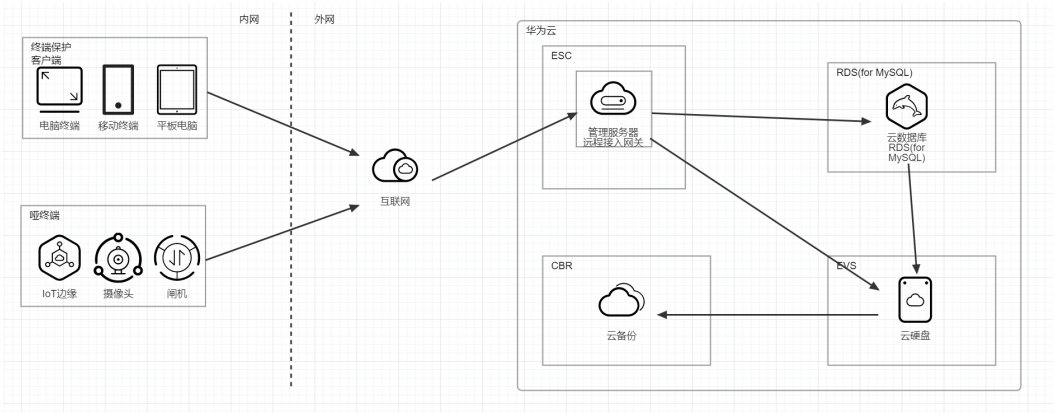
表 2-1 资源规格说明

产品名称	终端点数	华为云资源规格	数量
统一终端业务应用保护及数据管理平台	50-499	接入网关弹性云服务器 + 管理服务器弹性云服务器 通用计算增强型 C6s | 8核 | 16GB | 200G	1（如需负载，最少为2）
		云备份	1
		带宽	按需使用,5M
	500-199	接入网关弹性云服务器 + 管理服务器弹性云服务器 通用计算增强型 C6s | 16核 | 32GB | 500G	1（如需负载，最少为2）
		云数据库-MySQL 主备 8 vCPUs | 16 GB	1
		云硬盘 高IO | 500G	1
		云备份	1
		带宽	按需使用,5M
	2000-4999	接入网关弹性云服务器 通用计算增强型 C6s | 16核 | 32GB | 500G	1（如需负载，最少为2）
		管理服务器弹性云服务器 通用计算增强型 C6s | 16核 | 32GB | 500G	1（如需负载，最少为2）
		云数据库-MySQL 主备 8 vCPUs | 16 GB	1

产品名称	终端点数	华为云资源规格	数量
		云硬盘 高IO | 500G	1
		云备份	1
		带宽	按需使用,10M
	5000-9999	接入网关弹性云服务器 通用计算增强型 C6s | 16核 | 32GB | 500G	3
		管理服务器弹性云服务器 通用计算增强型 C6s | 16核 | 64GB | 500G	3
		云数据库-MySQL 主备 8 vCPUs | 16 GB	2
		云硬盘 高IO | 500G	2
		云备份	1
		带宽	按需使用,10M
	10000-20000	接入网关弹性云服务器 通用计算增强型 C6s | 16核 | 32GB | 500G	4
		管理服务器弹性云服务器 通用计算增强型 C6s | 16核 | 64GB | 500G	4
		云数据库-MySQL 主备 8 vCPUs | 16 GB	2
		云硬盘 高IO | 500G	2
		云备份	1
		带宽	按需使用,20M

架构图内容说明：

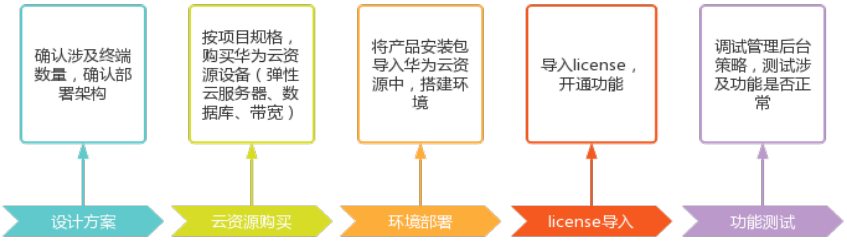
图 2-1 内容说明



3 操作流程

构建统一终端业务应用保护及数据管理平台流程图

图 3-1 流程图



4 实施步骤

4.1 搭建统一终端业务应用保护及数据管理平台系统环境

4.1.1 购买统一终端业务应用保护及数据管理平台产品 license

步骤1 选择任意浏览器访问华为云，登录账号：https://auth.huaweicloud.com/authui/login.html?locale=zh-cn&service=https%3A%2F%2Fmarketplace.huaweicloud.com%2F#/login

图 4-1 访问华为云

步骤2 购买统一终端业务应用保护及数据管理平台产品

登陆华为云后，选择云市场，选择安全，选择：“统一终端业务应用保护及数据管理平台”

选择购买规格、数量和购买方式（年或月），点击“立即购买”，确认订单信息，完成支付。

说明

当您购买产品服务后，会有联软工作人员第一时间联系您，帮您开通授权，请您耐心等待。

步骤3 购买华为云资源（弹性云服务器、数据库、公网IP、带宽）

根据企业项目涉及终端数量，对标云资源规格表，参考表内提供建议参数进行购买。

----结束

4.1.2 统一终端业务应用保护及数据管理平台系统部署在华为云环境中

步骤1 将统一终端业务应用保护及数据管理平台安装包导入到弹性云服务器中

步骤2 解压安装部署统一终端业务应用保护及数据管理平台安装包

步骤3 将已安装系统的弹性云服务器与数据库进行对接

步骤4 挂载公网IP

步骤5 检查系统组件运行情况

- Redis 进程： ps -ef |grep redis
- Tomcat 进程：ps -ef|grep tomcat
- 如没有redis进程，可通过service redis start 并在屏幕提示处输入yes 回车；
  启动redids 进程后，还需要把所有tomcat 进程停止后再启动以便连接redis;
  停止所有tomcat 的命令是 service emm-all-service stop
  启动所有tomcat 的命令是 service emm-all-service start
- 授权检查 进程：ps -ef|grep checklicense
  如没有授权检查相关进程，可通过 service checklicense start 进行启动

----结束

4.1.3 访问系统，导入 license，初始化配置

步骤1 访问系统

后台管理Web访问地址：**https://[ip]:7070/emm-manager/**

默认账号：

sysadmin/Leagsoftemm@1230 系统管理员

secadmin/ Leagsoftemm@1230 安全管理员

audit/ Leagsoftemm@1230 审计管理员

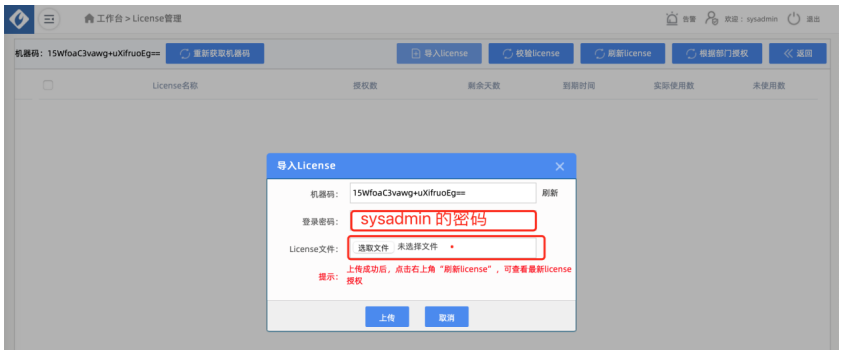
步骤2 导入license

第一次登陆系统需要导入license

图 4-2 导入 1

图 4-3 导入 2

图 4-4 导入 3



（授权是需要机器码）

步骤3 初始化配置

点击去设置

图 4-5 设置 1

1. 填充域名及访问端口
2. 点击添加区域，注册服务器列表

图 4-6 导设置 2

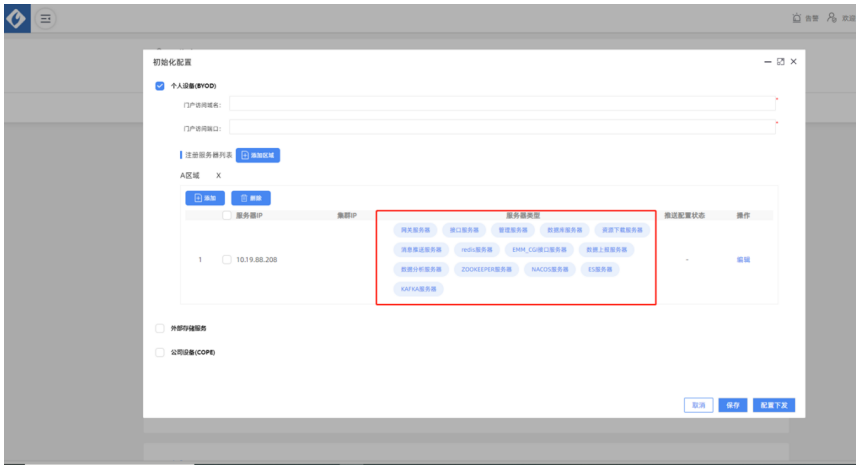
服务器IP处填写相关的服务器IP、集群IP处填写相关负载均衡IP

说明

如果内网和网关有多台服务器，则需要添加多条服务器IP项，若无集群IP则不填写集群IP项

3. 所有服务器配置完成之后点击右下角配置下发

图 4-7 设置 3



----结束

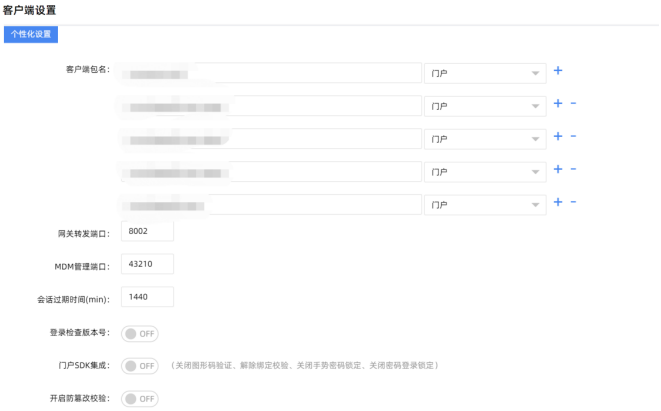
4.2 客户端设置

步骤1 配置基本参数

图 4-8 配置参数 1

图 4-9 配置参数 2

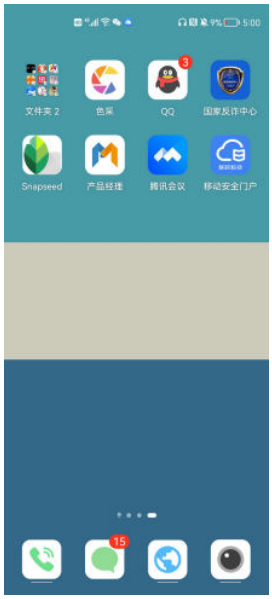
图 4-10 配置参数 3



步骤2 生成客户端，终端下载安装

图 4-11 PC 端

图 4-12 移动端



----结束

4.3 应用发布

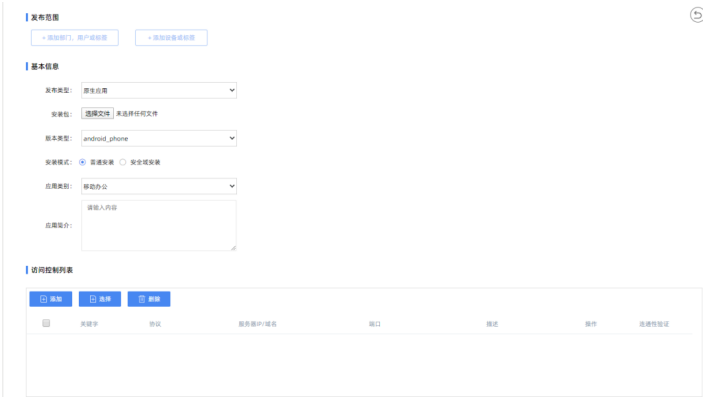
步骤1 使用拥有secadmin权限的账户登录管理后台。

步骤2 在工作台点击“快捷应用发布 > 添加应用”。

图 4-13 添加应用

步骤3 选择应用发布类型，填写下发范围,上传客户端安装包

图 4-14 传包



步骤4 点击“保存”，即可成功发布应用。

图 4-15 保存

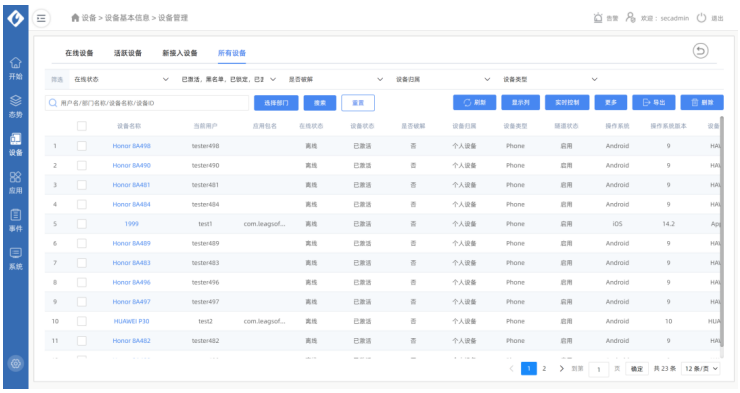
----结束

4.4 验证功能

步骤1 设备已安装客户端，并且进行设备注册

步骤2 打开系统后台，查看设备状态是否正常

图 4-16 查看设备状态

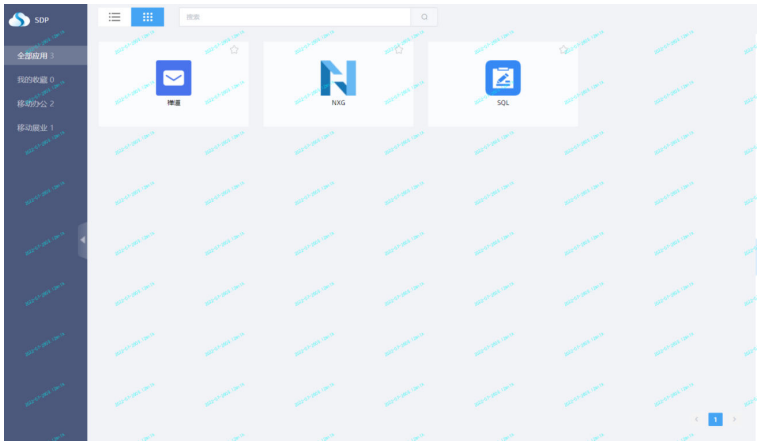


步骤3 设置功能项，下发设备，比如水印功能

图 4-17 设置功能项

步骤4 设备上检查功能是否实现

图 4-18 检查功能



----结束

5 修订记录

表 5-1 修订记录

发布日期	修订记录
2022-11-10	第一次撰写