FS0001

证券轻型营业部解决方案

技术建议书

文档版本 V1.0

发布日期 2013-10-24

作者 樊玉轲、孙化刚

华为技术有限公司

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

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： 0755-28560000 4008302118

客户服务传真： 0755-28560111

目 录

1 文档说明

1.1 文档目的

本文从技术角度，对证券公司的轻型营业部ICT建设进行规划设计和建议，目的如下：

1） 对证券轻型营业部所需的主要ICT系统进行整体分析设计，明确客户总体需求，阐明设计思路，给出总体设计方案，界定轻型营业部建设所需的各个子系统；

2） 对轻型营业部建设所需的各个子系统进行细化设计，明确子系统功能、组网方案、关键指标、部署建议和设备选型。

1.2 文档范围及结构

本文分13章，各个章节的内容简要介绍如下：

第1章：文档介绍，包括文档的目的、文档范围和结构。

第2章：项目概述，包括项目行业背景、项目的客户背景、项目的范围。

第3章：客户项目需求分析，包括客户的业务需求和规划，以及业务对ICT的需求。

第4章：证券轻型营业部总体方案设计，包含逻辑架构、物理架构、接口描述和总体方案亮点。

第5章至第9章：证券轻型营业部各子系统方案设计，包含证券一体机、数据中心接入区、AnyOffice见证开户、桌面云、统一网管等；各个子系统描述主要包括：组网方案、安全&可靠性设计、部署方案、推荐配置、方案亮点等。

第10章：证券软件系统及互通测试介绍，包括合作伙伴的系统对接和客户POC测试等。

第11章：各子系统涉及的主要产品及特点。

第12章：华为证券轻型营业部方案的成功案例。

第13章：缩略语。

2 项目概述

2.1 轻型营业部建设趋势

2.1.1 行业背景

近年来，证券行业不景气，2012全年和2013上半年114家证券公司中有15家亏损，其他证券公司的利润均有不同程度下滑，各证券公司亟需业务创新和组织创新来实现扭亏为盈和增加利润。

1. **经纪业务无增值点，需要业务创新，而新型业务需要大量新型渠道来支撑**

股市行情低迷、交易量萎缩，竞争加剧，导致佣金率不断走低，甚至低于万分之八，证券公司经纪业务交易收入整体明显下降。公开数据显示，2012年证券公司代理买卖证券业务净收入同比缩水26.82%。因而以经纪佣金为主要收入来源的证券公司将面临较大的压力。所以证券公司大都积极开展投资理财等增值服务，这要求证券公司建设更多的分支和渠道以发展客户。

据证券公司调研资料显示，在一线城市，新设一家传统营业部的成本在500万～600万元，后期的运营成本一年需要300万~500万元，且新设营业部基本在3年后才能实现盈利。随着电子商务的推广和网络的普及，大部分投资者都由营业部现场交易转变为非现场交易（网上委托交易、电话委托、手机委托等），据统计，目前现场交易的比例已达到95%以上，因此投资巨大的现场交易设备、场地都出现过剩和闲置，带来持续的无价值的运营成本投入，加剧了营业部的亏损局面。

2. 由于监管原因，证券公司网点建设无自由度，网点覆盖区域集中且存在大量的空白区

证券公司综合治理结束后，证监会于2008年重启了证券公司分支机构的审批工作，营业部审批相对更加严格，对证券公司资质、营业部数量、信息系统建设和相对饱和地区都加以限制；但这些限制降低了证券行业的风险，但是随着市场的不景气，越来越制约证券公司的发展，不利于业务创新。

而实际全国存在大量证券服务空白区，为证券公司提供了广阔的发展空间。 截至2012年10月底，全行业共有证券公司分公司337家，证券营业部5385家，主要集中在全国一二线城市，且大部分地区的传统营业部已相对饱和。而随着我国经济的高速增长，三、四线城市居民的财富也快速积累，相应产生了新的金融服务需求。但目前全国2003个县级行政区（不含市辖区）中，有超过60%的区域无证券分支机构，相应的金融服务渠道尚未建立。这为证券公司的新建渠道和发展客户提供了广阔的空间，而新的网点分支不适合按传统营业部模式建设。

3. 监管层适应行业创新要求，对轻型营业部建设放行

以2012年5月7~8日在京召开的“证券公司创新发展研讨会”为里程碑，监管层为促进证券行业的创新发展，发布了证券公司创新发展11条措施，明确放宽营业部建设要求。此后监管层和相关组织逐步完善并发布了涉及营业部的行业规定和规范：

- 2012年12月3日，证券协会发布《证券公司证券营业部信息技术指引》，明确将证券营业部信息系统建建设模式从重到轻分为A、B、C三类，证券公司可自主选择不同模式。

类型	特点	修订重点
A型营业部	在营业场所内部署与现场交易服务相关的信息系统为客户提供现场交易服务；部署证券公司网上交易站点的证券营业部，或作为其他证券营业部网络通信汇聚节点且所连接的证券营业部中提供现场交易的证券营业部。	合理降低了有关 IT 系统建设和管理要求，继续指导此类型证券营业部信息系统建设和管理
B型营业部	在营业场所内未部署与现场交易服务相关的信息系统，但依托公司总部或其他证券营业部的信息系统为客户提供现场交易服务	给出了最低标准和原则性要求
C型营业部	在营业场所内未部署与现场交易服务相关的信息系统且不提供现场交易服务	给出了最低标准和原则性要求

- 2013年3月15日，证券协会发布《证券公司开立客户账户规范》，明确非现场开户的业务流程规范，包括见证开户和网上开户。

- 2013年3月15日，证监会发布《证券公司分支机构监管规定》，对证券公司设立分支机构不再

作数量和区域限制，对营业部规模也不再限制。

- 2013年3月25日，中国证券登记结算有限责任公司发布《证券账户非现场开户实施暂行办法》，为非现场开户铺平了道路。

监管层放松了营业部的审批限制，截止2013年9月，已有40多家证券公司申请了500多家轻型营业部，轻型营业部已成为证券公司低成本渠道扩展的最佳选择。

2.1.2 轻型营业部业务定位

1. 轻型营业部定义

轻型营业部是指与传统营业部相比营业面积小、人员配置简化、IT投入低，侧重营销和服务的新型营业部；轻型营业部主要为客户提供开户、投资咨询和理财等增值业务；轻型营业部内不再部署与现场交易服务相关的信息系统，基本不提供现场交易服务。前述B/C型营业部属于轻型营业部的范畴。

由于轻型营业部的营业面积、人员配置、建设投入都将远低于传统营业部，因此设立成本、维护成本、退出成本都极大地降低。

2. 轻型营业部业务定位

1) 轻型营业部作为营销和服务前哨，实现以客户为中心的渠道扩张

政策放开后，证券公司大多会在没有网点的省份增设轻型营业部，填补网点空白，进一步完善公司战略布局，实现业务渠道延伸。传统营业部定位是交易中心，而轻型营业部定位是销售门店；轻型营业部将不再以拉客户炒股为主业务，而是作为营销和服务前哨，主要提供开户、产品营销、投资咨询和财富管理等多种服务。

2) 轻型营业部后台集中作业，优化业务流程，降低营业部运营成本和运营风险

由于轻型营业部的人员等资源配置简化，业务流程也随之调整创新，营业部主要完成客户接洽、业务数据采集及产品及服务营销，业务流程审批和专家答疑等均由总部后台集中作业完成，通过轻型营业部的业务和技术整合，逐步打造高效的流程证券。随着轻型营业部的规模建设，证券公司将在营业部层面实施分类管理和差异化经营，将省级传统营业部或区域分公司升级为中心营业部，将县市级的营业部实行整合或降级，形成“中心营业部+轻型营业部”的布局，利于向流程证券演进。

轻型营业部不设现场交易大厅、不提供现场交易、仅提供开户和投资咨询等服务，类似地产中介门店，因而轻型营业部的经营面积比传统营业部小的多，在100平米左右。轻型营业部内主要包括柜台（负责开户与咨询等业务）、办公室和会议室等。轻型营业部内的工作人员也精简得多，一般固定编制3人左右。人员配置多以“3+n”方案，其中“3”是指负责人、柜台、综合岗，“n”是指若干营销人员，总人员基本在10人左右。营销人员可在营业部内进行投资咨询，也可在营业部外进行非现场开户。

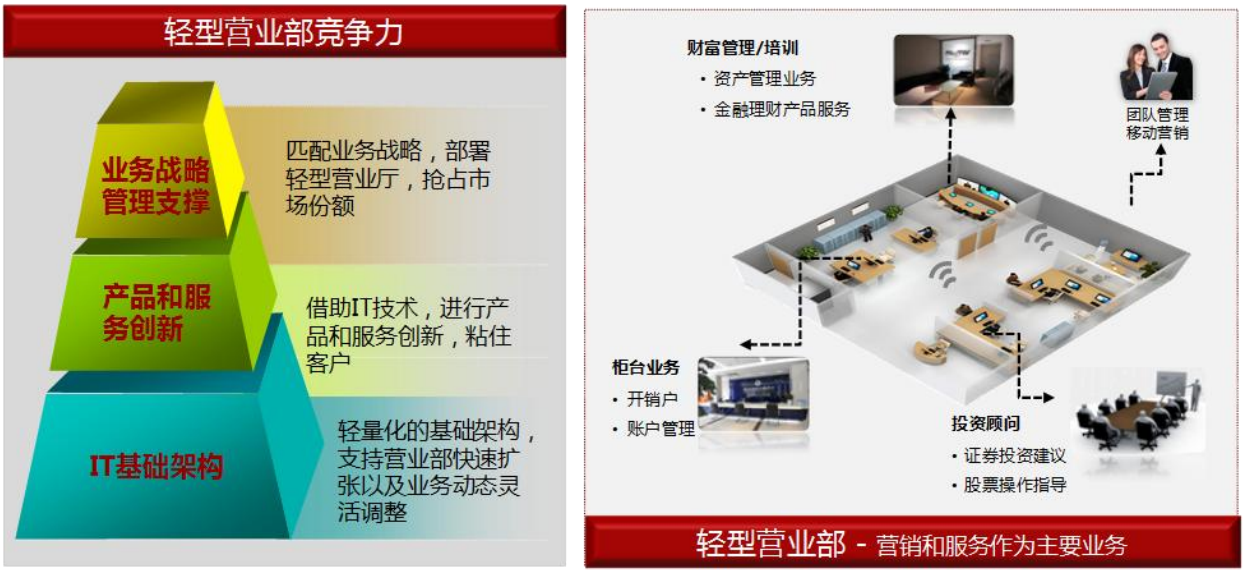

图1 营销和服务前哨

2.1.3 轻型营业部 IT 建设模式

1. 营业部IT轻量化、移动化

轻型营业部不设现场交易、行情等系统，对网络和设备的要求指标有所降低；轻型营业部相关的应用系统及服务器和存储等都部署在总部或区域中心，营业部终端主要通过应用客户端完成各类业务；因而营业部的IT设备主要为终端提供接入通道。

由于路途远和时间冲突，很多客户不便到营业部开户或办理业务，这就要求证券公司能够安排营销人员深入城镇或社区为客户服务。营销人员多使用轻便的智能终端，完成客户信息采集和业务办理。同时营业部内的营销人员也可以使用智能终端进行产品展示和股票推荐等业务。

2. 营业部远程集中管理

对于全国性证券公司，轻型营业部多实行“中心营业部+轻型营业部”的布局和分层管理模式，因而轻型营业部也多采用区域中心统一接入的方式；对于区域性或营业部扁平化管理证券公司，可以直接通过总部统一接入。

轻型营业部人员配置简化，一般不配备IT技术人员，且轻型营业部数量多、地域分散，难以由IT人员实施本地运维，因而需要通过总部/区域中心进行远程集中管理。

3. 营业部采用低成本的互联网VPN链路接入

轻型营业部不提供证券交易，对网络时延和可靠性要求比较低；由于专线的成本比较高，因而通过互联网建IPSEC VPN，实现数据安全传输成为主要的选择；同时见证开户等移动应用也多选择互联网SSL VPN接入，既安全又省成本。目前ADSL/3G等宽带接入网络可满足基本音视频应用需求。

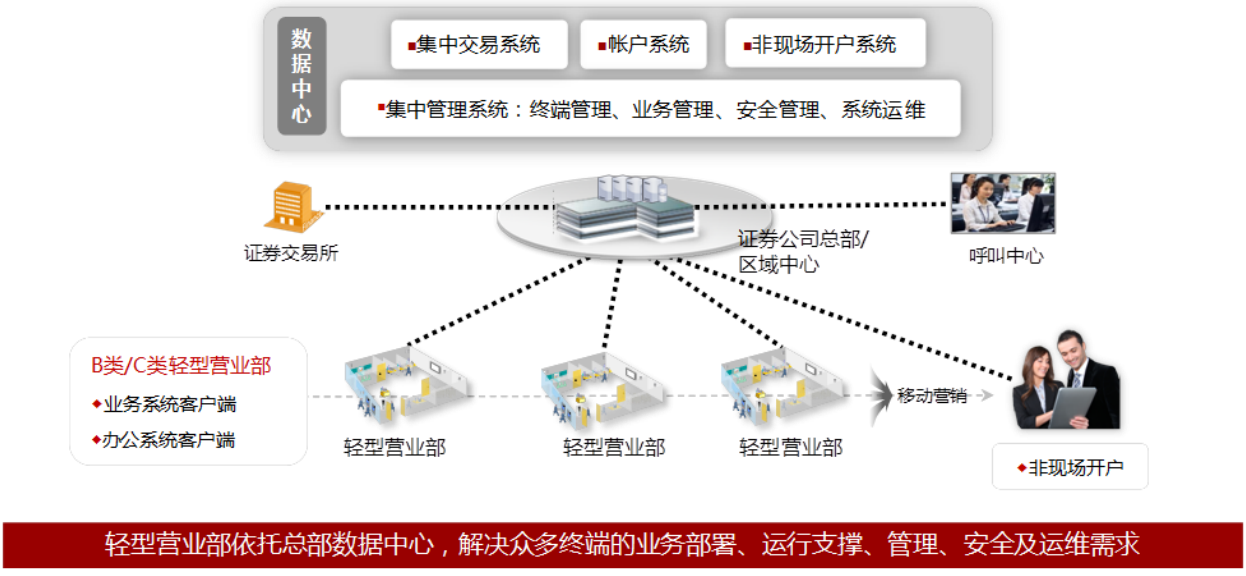

图2 IT 建设模式

2.2 项目背景

XX证券有限责任公司(以下简称"XX证券")经中国证监会批准于20XX年XX月XX日在XX成立，注册资本XX亿元人民币，现有正式员工XXXX人。

XX证券的经营范围包括：证券经纪、证券投资咨询、与证券交易、证券投资活动有关的财务顾问、证券承销与保荐、证券自营、证券资产管理、证券投资基金代销、融资融券。

为了抓住政策放开的机会，提高公司竞争力，对营业部空白区域覆盖，支持创新业务，实现差异化竞争。XX证券公司决定大力发展轻型营业部建设，拓展公司服务渠道，为客户供提供投资顾问、理财咨询等增值服务，提升公司整体竞争实力。

2.3 项目范围

按照XX证券公司对轻型营业部的设想，B类营业部面积在100-300平方米，C类营业部50~100平方米，主要功能是开户、投资者教育、产品发售、产品演示等。

为尽可能简化营业部技术维护工作量和降低运行维护成本，除了必要的网络设备和工作电脑外，其它的一般都尽量部署在总部或区域中心，轻型营业部必要的技术维护由总部或区域中心的专职IT维护人员负责，主要是远程维护。

XX证券公司涉及的软硬件信息系统主要有：

营业部软件系统：

- 账户管理系统、集中交易系统、融资融券系统、经纪业务管理系统、投顾理财系统、财务软件、OA办公等系统。其中集中交易和账户管理等系统均由XX公司提供。

营业部硬件设备：

- 终端外设：多易拍、二代证读卡器、打印机（针式）、打印机（激光）、密码键盘、拍照摄像头、复印机等。
- 基础网络硬件设备：小型机柜、交换机、防火墙、3G/专线/ADSL网络、PC机/TC终端、摄像监控系统等。

客户初步规划：

- 一期在南方分别规划建设XX个B类营业部和XX个C类营业部；后期向全国扩展，建设总规模达XXX个轻型营业部；
- 轻型营业部将全国范围内部署，前期通过南方中心接入，后期分南北方两中心分区域接入；
- 每个轻型营业部人数5~10人，大部分是营销人员，移动营销人员总数将达到XXX人，前期主要从事非现场开户业务；
- 公司员工PC机逐步进入换代周期，计划在总部及周边营业部试点桌面云，以加快桌面部署；初期规模为200人；

3 客户需求

3.1 需求概述

本章节重点介绍轻型营业部开展的业务，并阐述由于业务特点带来的ICT建设需求。

3.1.1 轻型营业部业务规划

证券轻型营业部的规划布局如下图，主要的业务包括：

图3 轻型营业部业务场景图

- **柜台及经纪业务**：柜员使用账户管理系统客户端完成客户开销户处理，并为客户提供密码修改、资料变更和查询等业务；并可根据客户委托进行股票买卖或撤单。
- **投资理财业务**：客户经理使用产品销售平台向客户展示并销售金融产品；投资顾问使用投资顾问平台为客户做出投资建议，辅助客户进行股票、基金等交易。
- **办公业务**：营业部员工需要访问公司发文，使用出差申请、报销等OA系统，完成日常办公操作；营业部员工也可使用会议系统参加总部的音视频会议或培训等，加强与总部的沟通。
- **上网业务**：轻型营业部员工及等待办理业务的客户可以上网查阅资料或浏览新闻等。
- **非现场业务**：客户经理（见证人）使用非现场开户系统，深入到社区或乡镇为客户现场办理开户，而不需要客户到营业部，服务范围大大提升，可以为证券公司争取到更多资源。

营业部内按角色和业务不同划分为不同的功能区域，各功能区域对业务开展和管理有如下要求：

1) **有线、无线局域网**：柜台、会议室主要用有线，营销区、客户区应支持WIFI；
2) **业务区域安全隔离**：各业务区域应进行安全隔离，避免越权互访；
3) **远程访问总部系统**：营业部仅部署业务客户端，业务系统服务器部署于总部或区域中心；
4) **设备集中放置**：营业部不设机房，设备放置于办公区或普通房间；

3.1.2 轻型营业部的 ICT 需求

综前所述，轻型营业部具有以下特点：

- **点小量大**，所以需要考虑低成本的快速部署，包括快速开局、桌面的快速投放；
- **营业部不设IT人员**，所以轻型营业部建设需要重点考虑集中远程管理问题；
- **互联网VPN链路接入，**因此需要解决桌面安全（含移动桌面）及数据中心安全接入问题；

轻型营业部的主要ICT需求：

1. **营业部一体机：降低网点的部署成本，实现网点集中远程管理**

轻型营业部的IT建设需要考虑桌面、网络、安全、视频监控、机房环境管理、UPS供电等多种需求。而轻型营业部建设的主要目的是低成本的渠道扩张，因此**如何降低网点设备的首次部署成本及长期运维成本**是关键。而原有营业部的采购模式是分散的、多厂家的采购，导致无法统一网管，而且初装成本很高，需要各厂家设备提前预集成、调测，因此需要一种新型的建设模式，不能在继续采用原有的设备分散采购模式，需要一体化的设备，实现集中管理和远程运维，最终实现按站点的运维管理。

2. **数据中心接入区：减小对传统营业部和原来网络的影响，实现统一安全可靠接入**

从1.1.2中，我们了解轻型营业部的建设不仅仅是网点的ICT的建设问题，还涉及到前后台流程的优化和配合，因此数据中心的改造和扩容也是需要重点考虑的。由于营业部数量多且使用语音和视频等大流量的办公业务，为了避免对传统营业部接入或网上证券接入造成影响，同时考虑互联网接入的安全要求，总部或区域中心的数据中心应该新建轻型营业部的专用接入区。

3. **营业部桌面：安全、快速部署、集中运维**

轻型营业部不再配置IT技术人员，营业部内工作人员办公终端的采购、部署、维护要求简单；桌面

的软件系统安装、维护等工作要求减少业务人员的参与；营业部运营初期人员变动也较大，如何保证信息安全也是一项重要工作；因而客户需要一种既安全、快捷、集中管理的桌面投放方式。

4. **非现场开户：安全、便捷、易管理**

为了更好完成开户数据采集、投资者教育等业务流程，以及向客户进行产品展示，客户经理需要屏幕比较大的PAD做为营销终端，同时PAD应能集成二代证读卡器和大容量电。当见证开户终端数量较大时，证券公司需要通过移动终端管理系统将这些终端进行有效资产管理，并避免非法终端接入公司网络和终端数据泄密。

3.2 一体化机柜需求

为支撑营业部的终端接入，并保证安全可靠，需要在营业部部署多种设备：

- **路由器**：广域网接入，实现与总部的总部的网络互通；
- **防火墙**：网络攻击防护，保障互联网接入安全；
- **上网行为管理网关**：保证上网合规，实现问题回溯和审计；
- **交换机**：局域网有线接入；
- **WLAN**：局域网无线接入，支撑室内移动办公；
- **UPS**：保证主要设备在停电时能继续支持业务办理完成；
- **小型机柜**：《证券营业部信息技术指引》要求营业部设备集中放置和管理；

轻型营业部不设机房，使用一体化机柜可将机柜、网络、安全等设备有机集成，可以解决多厂商选型困难、成本高、集中管理等问题，但仍需要重点考虑以下问题：

无IT人员，如何实现设备快速安装？

无IT人员，如何实现业务快速开通？

同时，为支撑营业部的业务开展，一体化机柜需要具有局域和广域网络接入、安全防护等能力，并具有高可靠性。有如下需求：

1. **VPN广域接入**：支持轻型营业部与数据中心通过IPSec VPN连接，对业务数据进行加密传输。
2. **3G广域接入**：支持通过3G接入数据中心，推荐使用联通WCDMA制式。
3. **路由自动切换**：营业部出口路由器支持路由自动倒换，无需人工干预。
4. **链路备份**：支持专线（E1、SDH）、ADSL、3G等接入；《证券营业部信息技术指引》要求营业部与总部数据中心至少两条链路。
5. **上网行为管理**：支持URL过滤和内容过滤，支持P2P、IM、炒股等软件的控制。
6. **UTM**：防火墙应具有UTM功能，可以对内外网攻击实现有效隔离。
7. **局域网接入**：支持有线和WLAN无线接入，支持按VLAN进行区域隔离。
8. **UPS需求**：满足在市电停电后，为机柜内设备和部分重要办公设备提供30分钟电源供应。

3.3 数据中心接入区需求

轻型营业部的批量建设给数据中心接入区带来了新挑战：

- ✧ 轻型营业部多通过互联网宽带接入，给数据中心带来安全隐患；
- ✧ 大量轻型营业部接入，原有数据中心接入区面临扩容压力；
- ✧ 全国范围的营业部按不同中心接入，以保证链路的可靠性；
- ✧ 见证开户等移动业务开展共享接入区，并需要E2E的安全保证；
- ✧ 营业部与接入区互联设备存在兼容性问题；
- ✧ 营业部与接入区设备应进行统一管理；

为了避免轻型营业部的接入对传统营业部接入和网上证券接入等产生不利的安全或性能影响，建议新建轻型营业部专用接入区，同时接入应具有以下能力：

1. 支持营业部的多种链路类型接入，如ADSL、专线（E1、SDH、MSTP等）；
2. 支持IPSec VPN和SSL VPN；
3. 支持设备冗余和链路备份；
4. 支持双中心接入区双活接入；
5. 有效防护来自广域网和内网的安全攻击，对内部网络实现有效安全保护；
6. 支持移动用户的安全接入；
7. 支持当网络出现拥塞时，优先保证时延敏感业务的服务质量，如经纪业务；

3.4 移动终端及管理需求

传统开户方式需要携带很大的设备箱(包) ，包括：便携机、摄像机、高拍仪、二代证读卡器、备用电源、3G卡及各种接口线等。一是作业工具多，设备携带和使用不方便；二是易遗漏或没电，影响业务开展；三是若终端缺乏管理，则存在较大安全问题：

- ✧ 移动设备缺乏有效管理，易导致安全隐患
- ✧ 终端外设随意连接、随意拷贝，易导致数据泄漏
- ✧ 终端丢失/被盗的问题，公司机密数据可能被窃取
- ✧ 终端应用安装随意，容易被木马等恶意程序入侵
- ✧ 公司应用不及时升级，导致业务出现问题

为保证见证开户的高效开展，并保证移动终端的有效管理，需满足以下需求：

1. 提供行业专用的非现场开户终端；
2. 移动终端数据加密传输；

3. 移动终端本地数据加密存储；
4. 支持终端通过SSL VPN连接总部；
5. 支持移动设备管理MDM，包括资产管理、应用管理、设备管理、安全管理等；

3.5 桌面快速投放需求

当前营业部终端存在核心数据管控不严，业务过程难审计，终端部署耗时且维护成本高等问题，具体表现如下：

- ✧ 数据分散各个营业部终端，如客户证件、资产信息、合同文本
- ✧ 证件扫描、信息填写、电子签名、合同打印等业务办理过程需可审计，可追溯
- ✧ 需逐台PC安装操作系统，系统打补丁、安装控件、插件、驱动等
- ✧ 硬件故障、新业务系统上线、病毒防护都需技术人员现场处理

为了实现轻型营业部的终端和桌面的快速部署、保证信息安全、降低维护成本，桌面云将是一种比较好的选择。桌面云需要满足客户的如下需求：

1. 瘦终端能满足OA办公、软件测试、营业厅不同场景下对性能和外设的支持；
2. 虚拟桌面站点可以接入互联网，允许进行互联网的浏览、文件上下载等常见操作；
3. 支持集中管理能力，如对操作系统镜像统一管理、软件补丁统一分发、TC终端统一管理；
4. 支持通过ADSL接入城域网使用桌面云；
5. 支持终端之间分别实施物理隔离或网络隔离，如办公终端与营业厅终端进行隔离；
6. 系统要支持安全架构设计，具有完善的安全防护能力；
7. 系统支持高可用性、动态迁移等可靠性设计；
8. 系统支持通过扩容存储与计算资源实现用户平滑扩容；

3.6 集中运维需求

轻型营业部IT轻量化，安排专职IT运维人员没有必要且成本高；轻型营业部分散，相对偏远，难以安排专职的IT运维人员负责多个营业部；且轻型营业部多批量采购和部署，规格统一，适合专人统一管理维护。因此主要通过远程方式实现对网络设备和安全设备的管理维护。网管系统应提供如功能：

1. 设备管理：包括路由器、防火墙、上网行为管理网关、交换机，UPS等L1设备；
2. 告警管理：支持短信或者Email方式通知；
3. 配置文件管理：支持配置文件备份、恢复、比较；
4. WLAN管理：支持可视化管理和向导式服务配置；

4 轻型营业部解决方案总体设计

4.1 遵循的标准和规范

证券轻型营业部解决方案遵循如下行业标准和技术标准：

- 《证券公司证券营业部信息技术指引》(2012.12.03)，证券营业部分类和建设标准
- 《证券公司开立客户账户规范》(2013.03.15)，非现场开户的流程规范
- 《证券公司分支机构监管规定》(2013.03.15)，分支机构设立、撤销等规定
- 《证券账户非现场开户实施暂行办法》(2013.03.25)，中登非现场开户规范
- 《中华人民共和国公安部第82号令》，规定了互联网服务提供者如何落实负责互联网安全保护技术措施，并保障互联网安全保护技术措施功能的正常发挥。

4.2 方案设计思路

以客户为本，依据客户的IT诉求，结合先进实用的IT技术，更好地满足客户轻型营业部的业务需求。方案设计主要基于以下考虑：

➢ **快部署**

证券一体机统一选型、标准化模块设计，载板运输支撑现场免安装调测，实现营业部IT设备的快速部署；U盘开局支持轻型营业部快速联网，业务快速开通，实现现场免IT人员。

通过桌面云实现桌面的快速投放。业务软件系统后台统一安装维护，TC上电即可用；虚拟机桌面发放在短时间内搞定。

➢ **高可靠**

轻型营业部与总部/区域中心之间网络采用双链路连接；支持路由器、上网行为网关、交换机等进行双机冗余配置，通过VRRP实现主备，或通过等价路由实现负载均衡。

接入区采用成熟的组网架构，通过防火墙、交换机、SVN等网络安全设备的冗余，保证接入区的安全可靠；同时与营业部提前调测，实现高兼容性。

➢ **易管理**

轻型营业部IT设备通过eSight统一网管实现远程集中维护，营业部做到无人值守；接入区设备与营业部使用一套网管，统一界面、节省成本；桌面云VDI物理与虚拟资源的统一管理，提高虚机维护效率，减少维护人员。

➢ **低成本**

标准化机柜，规模化采购降低成本；部署快速，节省成本；无机房设计，减少机房投入；远程集中维护，省维护人员，提升效率；桌面云使业务快速投放，减少等待成本；移动终端便捷高效，省时省成本。

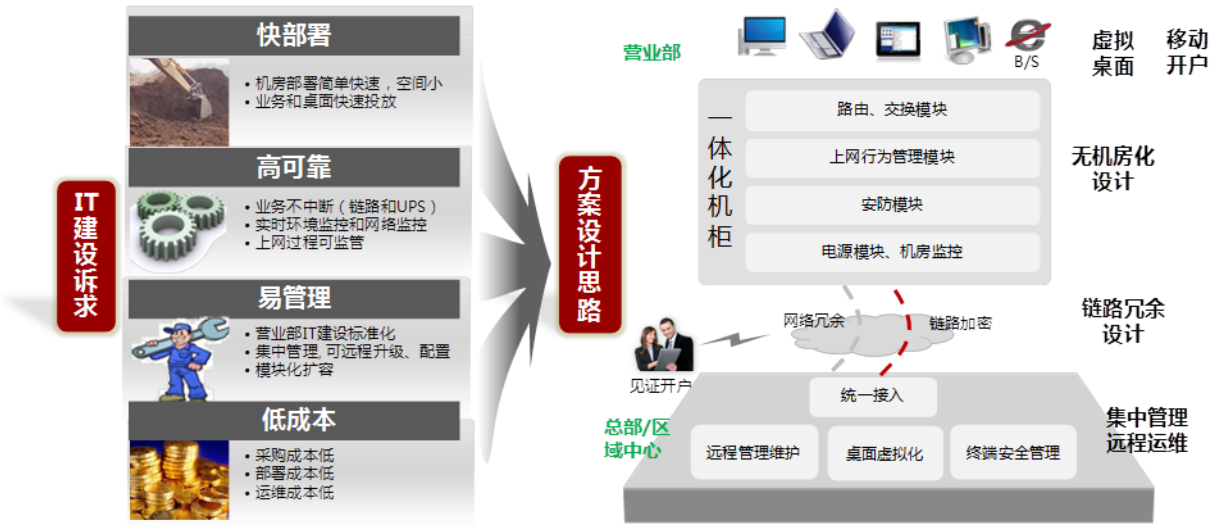

图4 轻型营业部设计思路

4.3 方案整体设计架构

4.3.1 总体逻辑架构

证券轻型营业部解决方案中主要包含了证券一体机、数据中心接入网络、AnyOffice、桌面云、网管、证券业务系统等子系统及相关终端。其中证券业务系统由合作伙伴提供，互联网使用运营商网络，其它子系统及TC和移动终端由华为提供，PC、笔记本等终端由客户另行采购。各子系统关系如下：

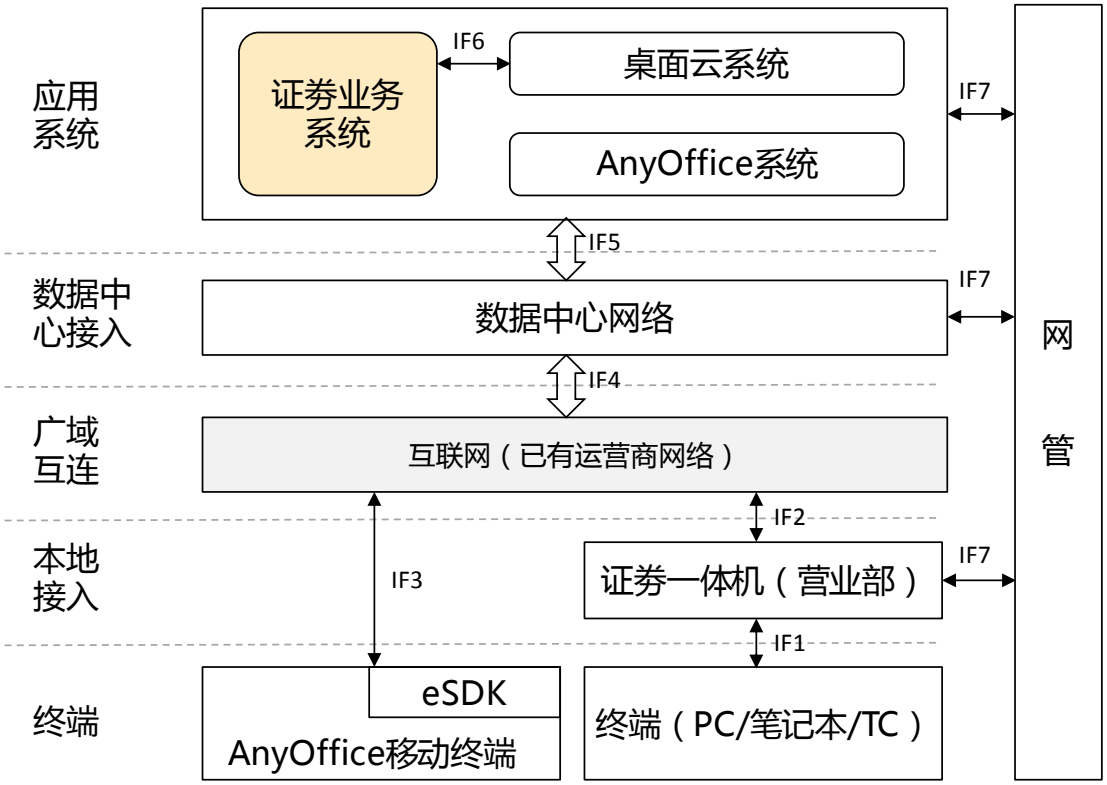

图5 轻型营业部方案逻辑架构

- **子系统简介**

证券一体机：支撑轻型营业部内的终端接入，通过互联网与数据中心实现VPN互联。华为提供；

数据中心网络：主要包括轻型营业部的统一接入区，并利用接入区和数据中心原有网络实现与其它系统互通。华为提供数据中心接入区方案；

桌面云系统：支撑轻型营业部桌面的快速投放，包括TC瘦终端和桌面云后台。华为提供；

AnyOffice系统：提供移动营销/移动办公的PAD终端；提供移动设备的安全管理；提供SDK供移动终端调用，实现通道建立和数据加解密等操作。华为提供；

网管系统：主要支撑轻型营业部、接入区、其它系统相关华为设备的管理。华为提供；

证券业务系统：包括渠道系统、核心系统、办公系统、管理决策系统等，实现证券公司的交易、帐户、资产等主业务，并支撑日常办公和管理。合作伙伴提供；

- **子系统间接口**

IF1：证券营业部内终端通过以太网有线和WIFI无线接入一体机；TC使用ICA/HTTPS协议与桌面云后台通讯；PC等终端使用HTTP等协议访问业务系统；

IF2：证券一体机利用ADSL、3G等宽带网络，通过PPP拨号接入互联网，并与数据中心接入区建立IPSec VPN；

IF3：移动终端通过3G网络PPP拨号接入互联网，并与接入区建立SSL VPN；合作伙伴可以使用安全eSDK将移动应用进行安全封装，实现SSL通道建立、关闭和数据加解密等操作；

IF4：数据中心接入区通过IP方式接入互联网，与轻型营业部间建立IPSec VPN，与移动终端建立SSL VPN；

IF5：数据中心接入区与桌面云、AnyOffice等系统通过IP通讯；

IF6：桌面云虚机通过IP协议与证券业务系统交互；

IF7：网管系统通过SNMP协议管理轻型营业部、接入区等系统相关设备；

4.3.2 总体物理架构

轻型营业部内部署证券一体机，实现营业部终端接入，支持有线和无线WIFI接入。数据接入区部署路由器、防火墙等设备，保证轻型营业部的安全可靠接入，并通过数据中心原有网络实现与桌面云后台、网管系统、AnyOffice的MDM服务器等子系统的通信。

为了轻型营业部的更可靠接入，避免因单数据中心接入区故障而导致的业务中断，证券公司在条件允许的情况下可考虑建立多个接入中心，轻型营业部通过多链路多中心接入，实现业务零中断。

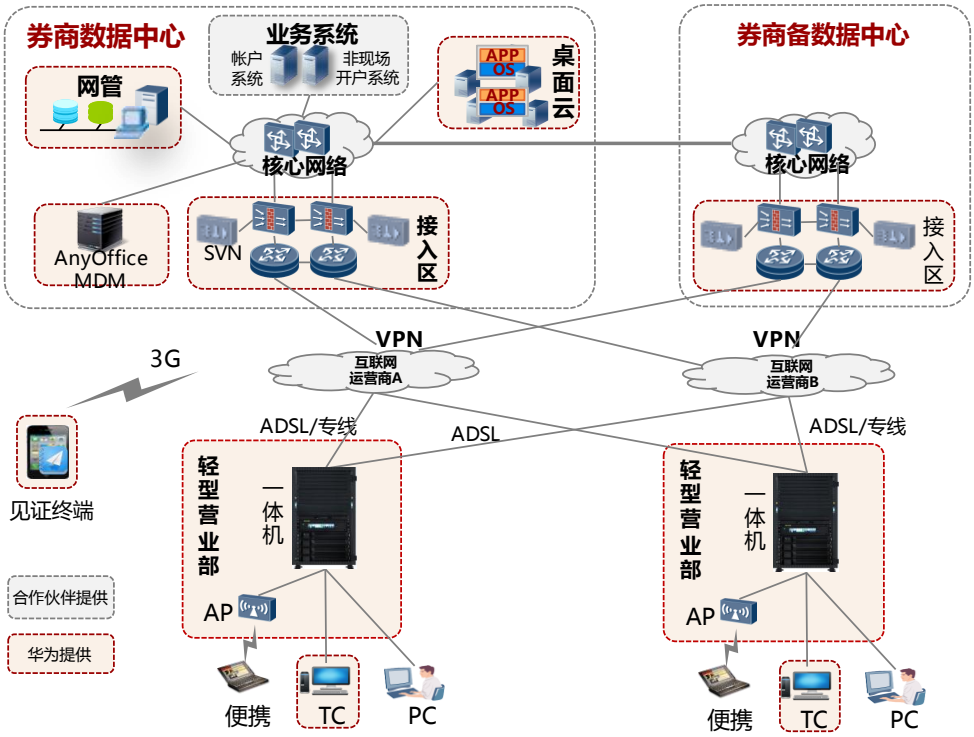

图6 轻型营业部方案物理架构

4.4 方案亮点

图7 解决方案价值

- **系列化的证券一体机，营业部部署时间从3个月缩短到1天**
  - **生产预安装**：生产线批量完成一体机所有设备的预安装和调测，保证发货前无问题；
  - **带板运输**：除电池外，按站点整体发货运输，减少现场组装工作，实现现场免调测；
  - **U盘开局**：非技术人员使用U盘完成组网配置，实现快速营业，部署效率提高70%以上；
- **eSight统一网管，实现集中监控，远程维护**

- **统一管理**：eSight支持华为能基、网络、安全、服务器、存储等设备的统一管理；
- **图形化操作**：eSight提供Web化网管，图形化操作，并支持部分第三方设备的管理；
- **“0”维护人员**：轻型营业部不配置IT人员，由总部集中管理轻型营业部和接入区等设备；

- **多层次防护，实现综合安全**
  - 终端：桌面云实现终端数据不落地；MDM提供移动终端的生命周期安全管理；
  - 营业部：AR内置防火墙，ASG上网行为管控、S27进行VLAN隔离；
  - 接入区内：实现内外网攻击防护，AR、SVN、USG等均支持高安全的国密算法；
- **方案整体设计，成本下降30%**
  - 标准化一体机，规模采购降低成本；机柜即机房，减少机房投入 ；
  - 营业部快速部署，节省成本；桌面云使桌面快速投放，减少等待成本；
  - 营业部远程集中维护，省维护人员，提升效率；桌面云集中维护，效率提升10倍；
  - 见证终端便捷高效，省时省成本；

5 证券一体机方案

5.1 证券一体机组成

华为证券一体机解决方案就是将路由器、交换机、上网行为管理网关、配电PDU、UPS等统一集成到行业机柜中，经过优化组合，提供预集成、标准化、具有可靠性的端到端轻型营业部组网的整体方案。如下图所示：

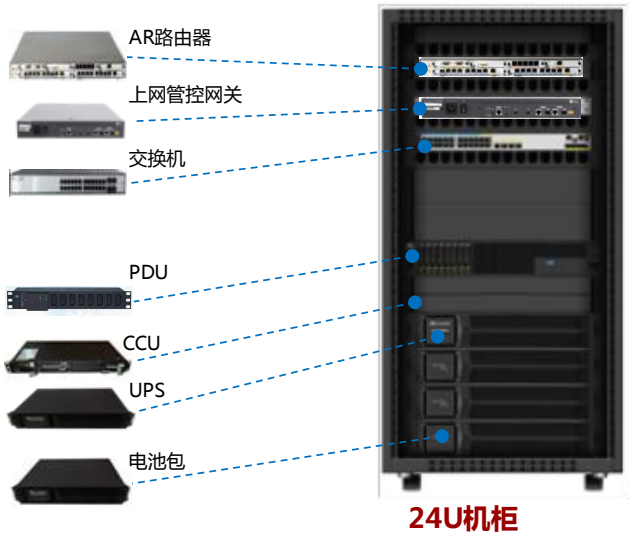

图8 证券一体机组成

硬件资源包括：

- 标准24U机柜：总装机柜，实现生产预安装
- 路由模块：支持多链路广域接入，内置防火墙
- 交换模块：支持局域网有线接入，无线通过扩展WIFI实现
- 上网行为管理模块：支持用户上网的管控和审计；
- 备电模块：包括UPS与电池包，支持停电不停业；
- 机柜监控模块：CCU及各类传感器，实现机柜小环境的监控；

软件资源包括：

- ASG Manager：ASG的远程日志保存和审计；
- 网络管理软件：轻型营业部L1/L2设备管理，集中部署

5.2 典型套餐设计

轻型营业部接入点数量通常规划为10~50个，营业部内主要开展开销户柜台业务、投资咨询、日常办公等，没有交易业务，本地不部署业务服务器。营业部网络可靠性要求较高，一般采用双链路备份，通过VPN网络连接到接入中心。

证券公司根据营业部的重要程度不同，分别定位为样板门店、中心门店、普通门店等类型，不同类型的营业部在投资成本、接入点数量、WIFI覆盖和可靠性有不同的要求，针对这些差异，我们提供三种典型套餐设计方案。由于批量生产成本低、交付周期短，建议客户优先选择这3种套餐。客户定制化的配置成本偏高，交付周期长。

5.2.1 简配型设计

普通门店这类轻型营业部，地段相对偏僻，面积30~50m^2，人员、业务量相对较少，对网络接入和可靠性要求比较低，针对此类营业部的组网设计如下：

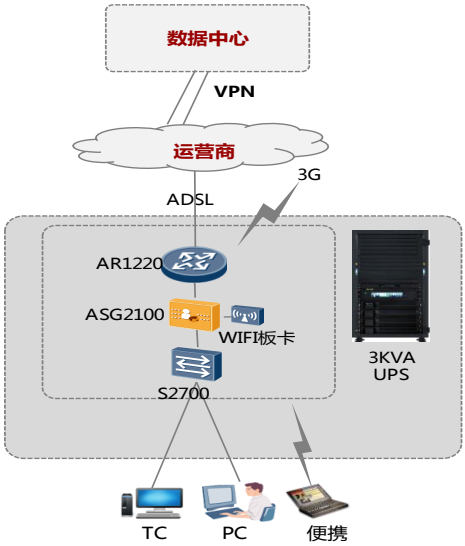

图9 简配型组网

此备选方案的特点：

- 设备无冗余；
- ADSL+3G双链路冗余；
- WIFI内置，覆盖面积可达50m^2；
- 机柜无CCU监控，标配3KVA UPS+1电池包，支持30分钟续电；
- 成本低，可支持10人办公；

5.2.2 标配型设计

重要的普通门店和部分中心门店这类轻型营业部，地位相对更重要，面积50~100m^2，人员、业务量相对较多，对网络接入和可靠性要求比较高，针对此类营业部的组网设计如下：

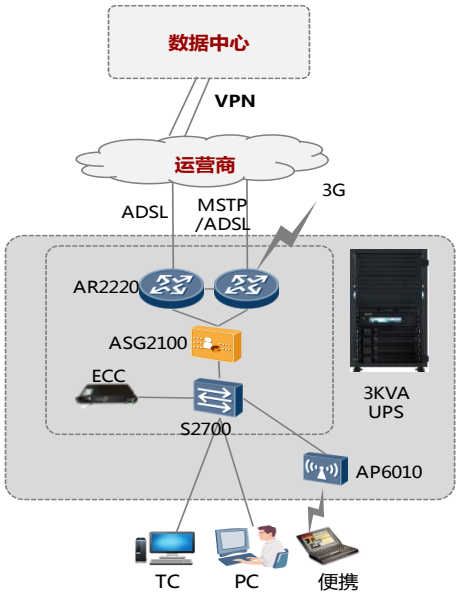

图10 标配型组网

此备选方案的特点：

- 广域接入路由器冗余，保证与总部网络连接不中断；
- 双ADSL+3G链路冗余；
- 独立WIFI瘦AP*2，覆盖面积超过100m^2；
- 机柜包含CCU监控，标配3KVA UPS+1电池包，支持30分钟续电；
- 可靠性适中，成本适中，可支持10-20人办公；

5.2.3 增强型设计

样板门店和部分中心门店这类轻型营业部，用于对外展示的窗口，供上级、同行和客户参观，地段

相对较好，面积100~150m^2，人员、业务量相对较多，多提供视频会议、远程专家等业务，对网络接入和可靠性要求更高，针对此类营业部的组网设计如下：

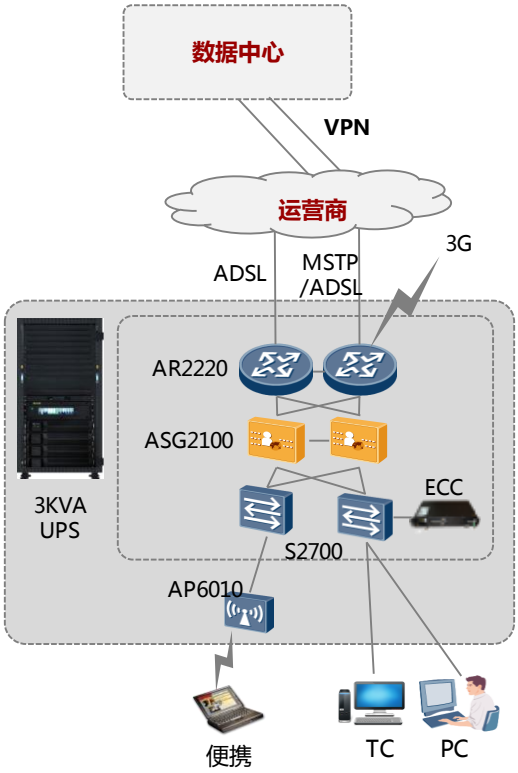

图11 增强型组网

此备选方案的特点：

- 主要网络设备均采用冗余配置；
- 专线+ADSL+3G链路冗余；
- 独立WIFI瘦AP*2，覆盖面积可达150m^2；
- 机柜包含CCU监控，标配3KVA UPS+2电池包，支持30分钟续电；
- 可靠性适高，成本较高，可支持>20人办公；

5.3 安全性设计

5.3.1 VPN 设计

除部分重要级别高的轻型营业部通过专线与总部互联外，其它轻型营业部多通过PON、ADSL等有线宽带或3G无线接入互联网，再与总部建VPN隧道，进行安全数据传输。VPN技术包括SSL VPN、IPSec VPN、GRE VPN等，对轻型营业部与总部间互联属于Site-to-Site应用，可选择使用IPSec VPN。IPSec支持站点间认证，可选择SHA-2等高安全性的加密算法，数据加密可选择3DES、AES等难破解的算法。对于安全性要求更高的证券公司，可以选择华为的国密SIC卡。

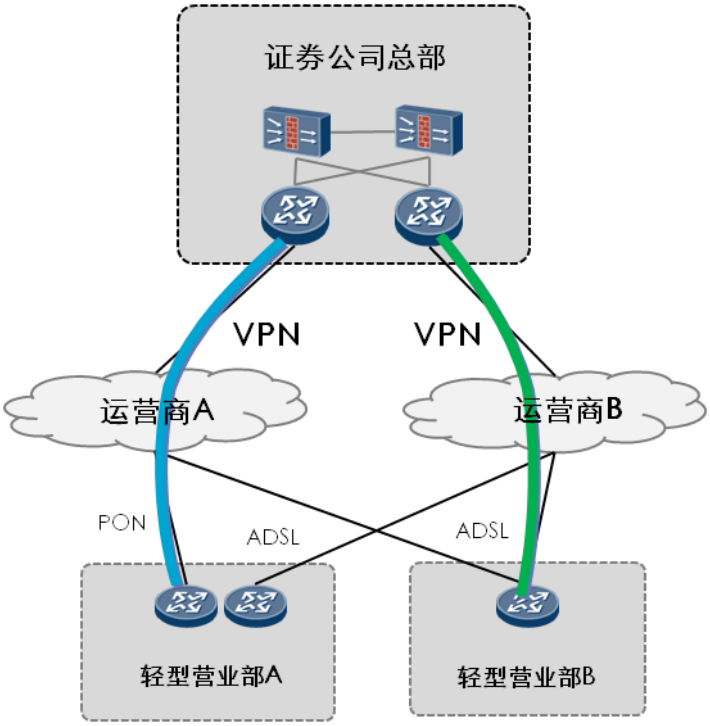

图12 VPN 组网

营业部广域地址：

- 若轻型营业部用PON接入，则可能使用固定IP，ADSL/3G等多使用PPP拨号动态获取IP，华为的IPSec VPN实现支持IKE方式协商，不必指定本地址，屏蔽配置差异。

营业部与总部动态路由：

- 若轻型营业部与总部间使用动态路由，则可使用GRE over IPSec方式，通过GRE隧道动态交换路由，避免当营业部数量较多时，在总部数据中心配置较多静态路由。GRE支持OSPF等协议。

5.3.2 广域防攻击设计

防攻击：

由于轻型营业部不部署服务器、不对外提供服务，来自外部的攻击相对少些；轻型营业部对成本比较敏感，而又不能不考虑攻击防护。AR的内置防火墙很好地解决了这一矛盾，AR内置防火墙具有以下功能，可满足轻型营业的需求：

- 支持安全域功能
- 支持包过滤防火墙
- 支持应用层包过滤ASPF(application specific packet filter)
- 支持黑白名单
- 支持攻击日志

- 支持DDOS、泛洪等攻击防范

防火墙双机热备：

AR通过HSB(Hot-Standby）协议，根据防火墙主备备份组的状态和事件通知（批量备份、实时备份、主备使能、独立运行）对防火墙Session表在主备设备间进行同步处理。在主设备故障时流量切换到备用设备，用户业务不中断，实现业务的高可靠性。

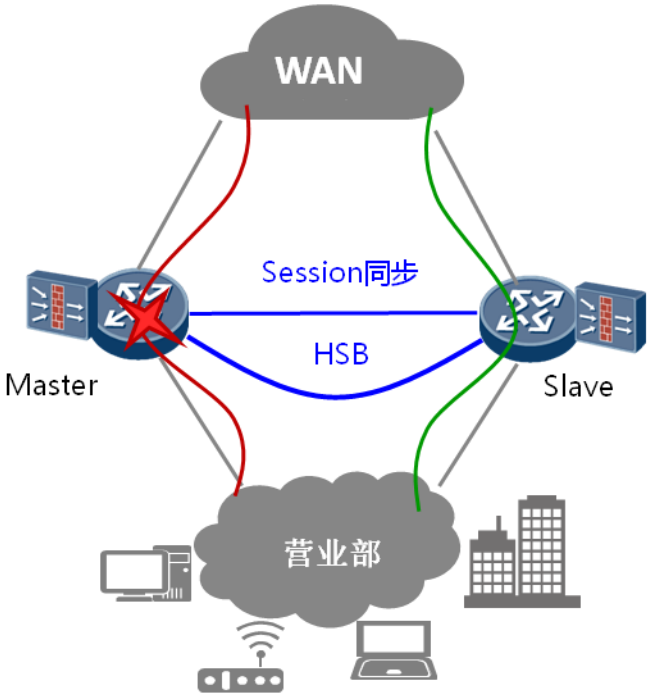

图13 防火墙双机热备

5.3.3 上网行为管理设计

轻型营业部内部员工上网可能带来的工作效率低下、带宽滥用、恶意软件感染、内部信息泄漏以及法律合规等问题，证券公司需要全面、有效的上网行为管理。

针对客户对上网行为管理的需求，我们采用华为的上网行为管理网关ASG2100实现上网行为的有效管控。ASG做为内网网关，集中实现有线和无线接入的出口流量管控，上行通过AR完成多种方式的广域接入。

ASG的上网行为管控日志需要保存到日志服务器，日志服务器与ASG管理软件ASG Manager共用同一服务器；ASG Manager服务器部署在总部，统一管理所有轻型营业部的ASG。服务器要求使用Windows 7/Windows 2003/Windows 2008操作系统。

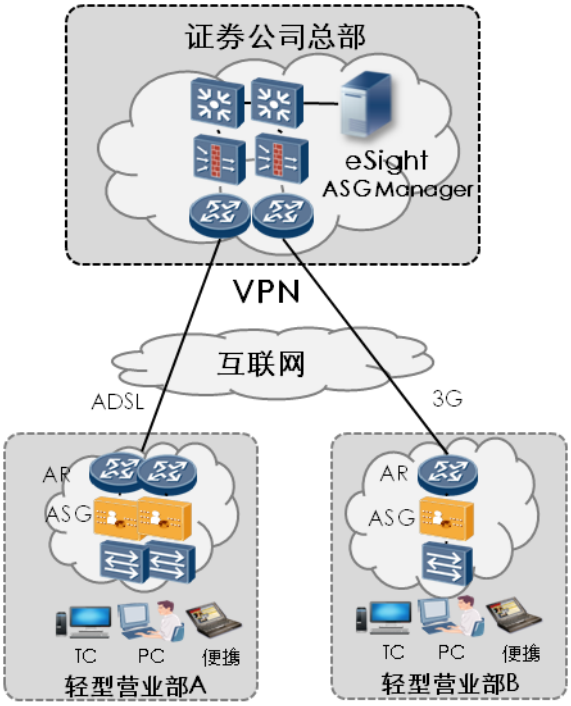

图14 ASG Manager 部署

上网行为管理功能包括：

- **管控上网行为**

根据不同部门（单位）、不同员工分配不同的互联网资源访问权限，杜绝越权访问和权限滥用；对上班时间从事办公无关的行为进行拦截或启用上网时间限制；杜绝上班时间无关网页、IM聊天、在线网页视频、BT等P2P下载、网络游戏等行为，确保工作效率；

针对内置预定义的应用协议分类和自定义的应用分类，做阻断或允许通过的策略配置。可以对股票行情和交易软件单独区分行情和交易，阻断交易进行，但对行情查看放行，确保证券行业的合规性。

- **防止带宽资源滥用**

基于时间段、用户/部门、应用/应用类型，为各部门划分和分配出口带宽。保证员工访问服务器区资源的带宽、保证领导和部分特别人员和部门的带宽、限制员工在上班时间使用办公无关的大流量应用；同时提供带宽保证措施，保证关键应用对外提供服务的带宽、保证内部重要人员的上网带宽；对P2P、在线网页视频、P2P视频等带宽滥用的应用进行封堵或限速，提高出口带宽利用率，保证正常上网需求，保证对外服务器的带宽，确保有限的带宽资源能最大限度的发挥作用。

- **全面WEB威胁防御**

自动过滤钓鱼、网马、恶意软件下载等恶意网站，检测威胁流量和病毒，确保用户安全上网；定位异常终端：检测ARP和IP欺骗、泛红攻击、端口和地址扫描等异常行为，并自动防御。

- **管控违规信息**

过滤不良网站和非法网站（反动、色情、暴力、博彩等）、过滤非法言论。包括过滤违法违规网页、过滤通过网页发布不良信息，管控不良言论，做到关键事件有据可查，快速配合相关部门的审查。

- **记录用户上网轨迹**

记录网络访问行为，满足公安部82号令要求； 行为日志审计和外发内容保存，满足企业定期检查最近网络访问日志的审计要求和监管要求。

- **上网行为和流量统计**

统计用户上网行为及时长、统计应用和用户流量，识别主要用户和主要应用及其变化趋势，为行为管理和带宽优化提供依据。

5.3.4 局域网隔离设计

根据轻型营业的业务区域划分和设备连接管理的需要，就终端和设备的在交换机上的接入端口分别划分到不同的VLAN，各VLAN之间进行隔离，除了设备管理外，一般不允许跨VLAN访问，可以防止普通的非法和越权访问。

对于WIFI无线接入，根据不同的用户使用不同的SSID，各SSID对应相应的区域VLAN，保证业务统一隔离。

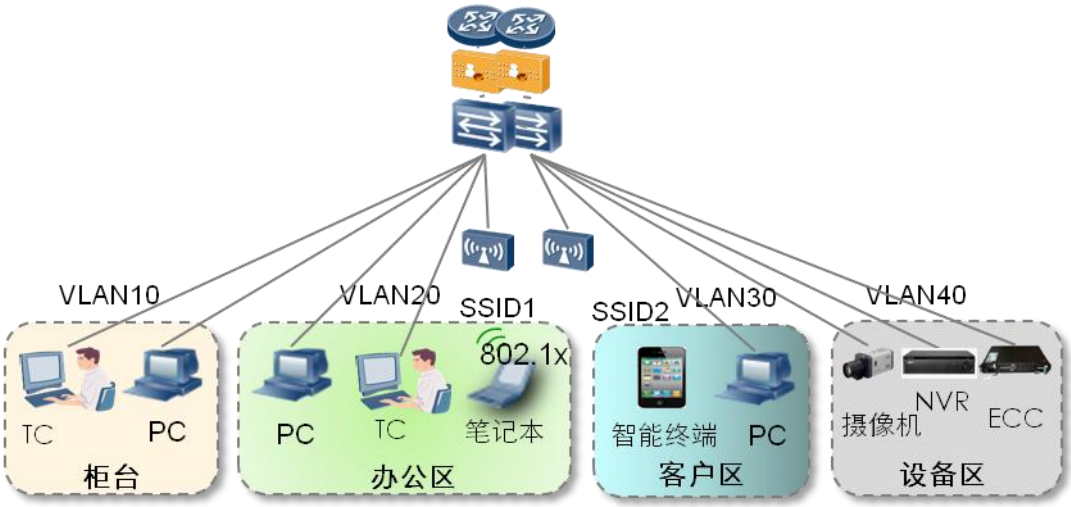

图15 局域网 VLAN 隔离

5.4 可靠性设计

5.4.1 冗余设计

1、链路冗余

经济型：采用ADSL+3G双链路冗余，其中ADSL下行带宽比较大，线路稳定性好，选作主链路，3G作为备用链路。AR路由器使用接口备份特性支此应用方式，当ADSL故障时，自动切换到3G链路；继而当ADSL恢复时，可回切到ADSL线路。同时为了避免线路不稳定频繁切换，可设备切换间隔。业务和上网使用同一链路。

标准型/增强型：采用2*ADSL+3G共3条链路冗余，其中一条质量较好的ADSL（如电信）+3G（如联通）做为与总部的业务通道，以接口备份方式工作；另一条ADSL（如联通）做为上网使用，当此ADSL故障时，临时借用业务通道，恢复后再自动回切。对业务而言，3条链路的优先级由高到低是电信ADSL

一联通3G一联通ADSL。

2、设备冗余

只有标准型和增强型组网支持设备冗余。

标准型：仅负责广域接入的主设备AR路由采用冗余。两个AR路由器间启用VRRP，以负载分担的方式工作，其中业务流量和上网流量分别路由到不同的AR。当ASG或交换机故障时，可以临时将设备或终端直接连接到AR上。

增强型：网络和安全设备全部冗余配置。AR路由器间启用VRRP，负载分担方式；ASG间启用HRP，主备方式工作；交换机独立配置，可统一划分VLAN，一个故障时将终端临时迁移到另一台交换机。

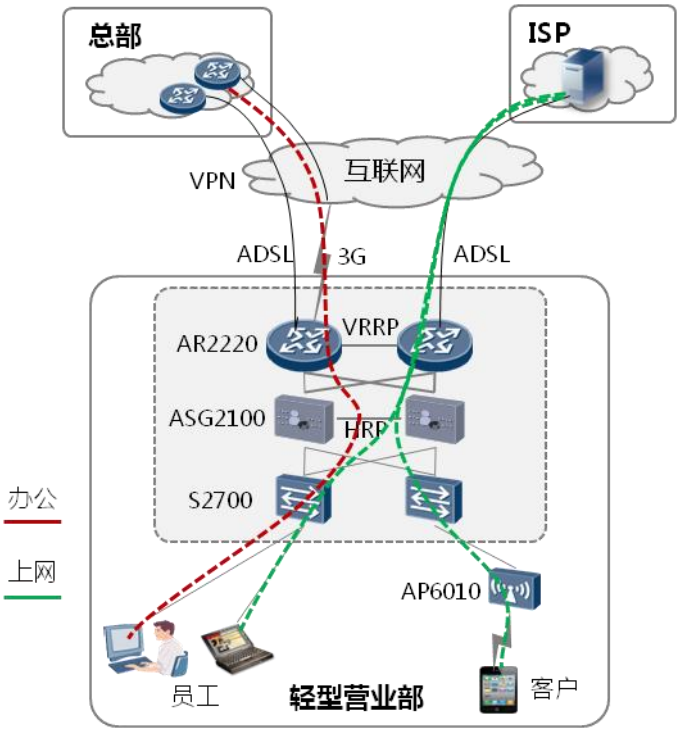

图16 设备及链路冗余

5.4.2 Qos 规划

轻型营业部人员较少，终端主要是普通的摄像机、PC、TC、便携机、移动终端等，不存大流量的设备；营业部内交换机S27支持全线速二层转发，而ASG三层转发可达300Mbps，可满足局域网内的转发性能要求。跨VLAN和交换机的转发由ASG完成。总体上讲营业部局域网转发基本不需要做QOS，主要在广域出口进行QOS调度，即在AR上进行QOS配置和调度。

轻型营业部广域上行流量可能有：柜台经纪、投资理财、办公、语音、视频、上网等，可采用CBQ调度策略，各业务的QOS优先级规划如下：

数据流	QOS优先级	CLASS	DSCP	备注
管理/控制流	高	EF	101110	低丢包率、低时延、高带宽
语音/视频流				
柜台经纪流	高	AF4	100010	带宽保证、低时延

投资理财流			100100	
办公流	一般	AF2	010010	
上网流	低	BE	000000	

5.5 路由规划

证券公司需要事先规划各个营业部的IP地址段，以利于路由规划和配置。

静态路由方式适合营业部数量少的情况，AR配置缺省路由，下一跳出口为营业部ADSL链路出口；营业部接入中心路由器配置到各个营业部网络的静态路由。

动态路由协议适合营业部数量多，采用静态路由配置起来比较繁琐的情况，动态路由协议通常采用RIP或OSPF，结合GRE over IPSec方式，与总部动态交换路由。

简配型组网，ADSL+3G链路采用接口备份，以主备方式工作，链路自动切换，路由规划简单。标准型和增强型组网相对复杂，分别考虑业务和上网数据流的路由规划。

5.5.1 业务路由规划

业务路由使用动态路由协议，如下图，其中ADSL+3G接口备份方式作为主链路，另一ADSL做为备链路。营业部与总部间运行OSPF协议，营业部分别学习到2条到业务系统（如帐户系统）的路由，由于主链路优先级高或COST值小，只有主链路路由加入到当前转发路由表中；当主链路ADSL和3G都故障，则再使用备用链路路由，主链路恢复正常后，则仍然根据路由优先级使用主链路路由。

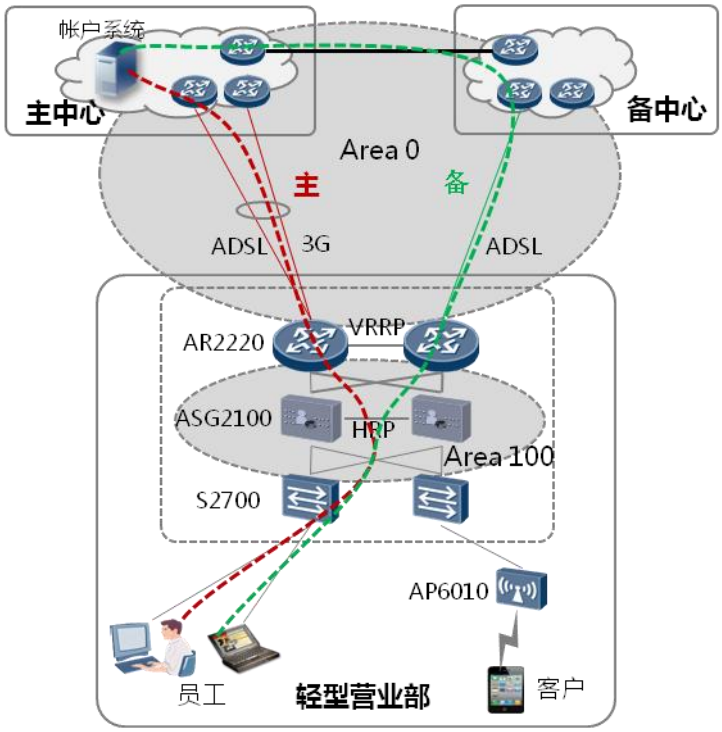

图17 业务路由

为保障路由的快速收敛和倒换，可使用NQA结合接口备份，OSPF的快速Hello，BFD for OSPF等

机制加快收敛速度。

5.5.2 上网路由规划

上网数据流不需要也没必要与公网交换路由，由于采用的是PPP拨号方式上网，只需增加一条缺省路由即可，其中左边路由器的ADSL+3G作为备用链路，配置缺省路由的优先级比右边主链路的低。ASG运行OSPF，会学习到公网的路由，优先采用高优先级的主链路路由。

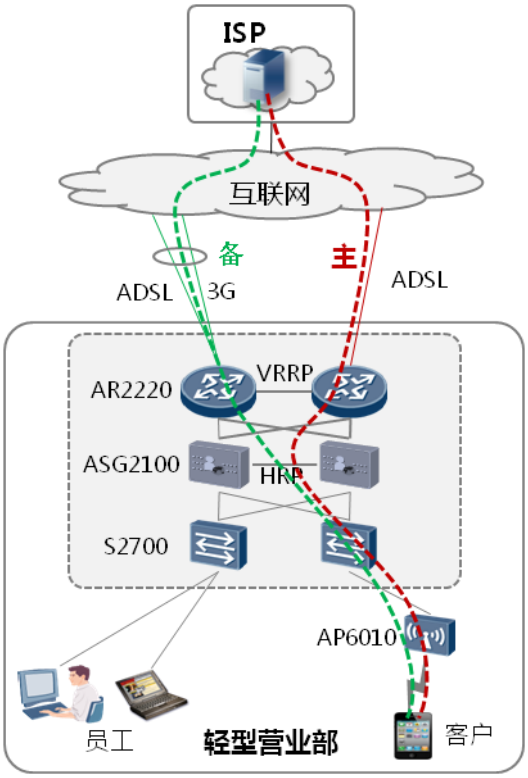

图18 上网路由

5.6 WIFI 无线接入设计

5.6.1 WIFI 组网设计

简配型轻型营业部组网中由ASG+WIFI板卡实现小面积的覆盖，由ASG既做AP又做AC功能，类似胖AP的方式。这里主要分析标准型和增强型组网的WIFI设计。

由于胖AP需要单个管理和配置，当数量大时，管理和维护的工作量会相当大，因而当前瘦AP+AC的方式逐渐普及。此方式可以对AP统一升级、统一配置，减少管理和配置工作量。我们根据轻型营业部的特点和部署数量推荐两种部署方式：

1、本地分布AC：轻型营业部各自的AR作为AC，分别管理营业部内的瘦AP；此方式适用于营业部建设数量少于**40**个的证券公司。

2、远程集中AC：在总部部署独立的AC6605，统一管理所有轻型营业部的瘦AP；此方式适用于营业部建设数量超过**40**个的证券公司；此方式管理效率更高、成本更低。

同时由于轻型营业部使用IPSec VPN接入总部，并使用安全性高的加密算法，因而可以保证到营业部与总部间业务数据的传输安全性，且而营业部的上网数据流都通过总部转接，对总部的压力会很大，因而采用WIFI数据流本地转发的方式。

如下图，对集中AC的方式，营业部AP与总部AC建立CAPWAP隧道，通过隧道传输各类控制数据，包括AP参数、配置等；而数据采用本地转发的方式，如上网流直接在营业部本地出口，经纪等业务流也在本AR通过IPSec VPN传送到总部。而分布AC的方式，通过对AR内置的AC实现对营业部内AP的管理。通过eSigth可以实现对集中AC和AR的统一管理。

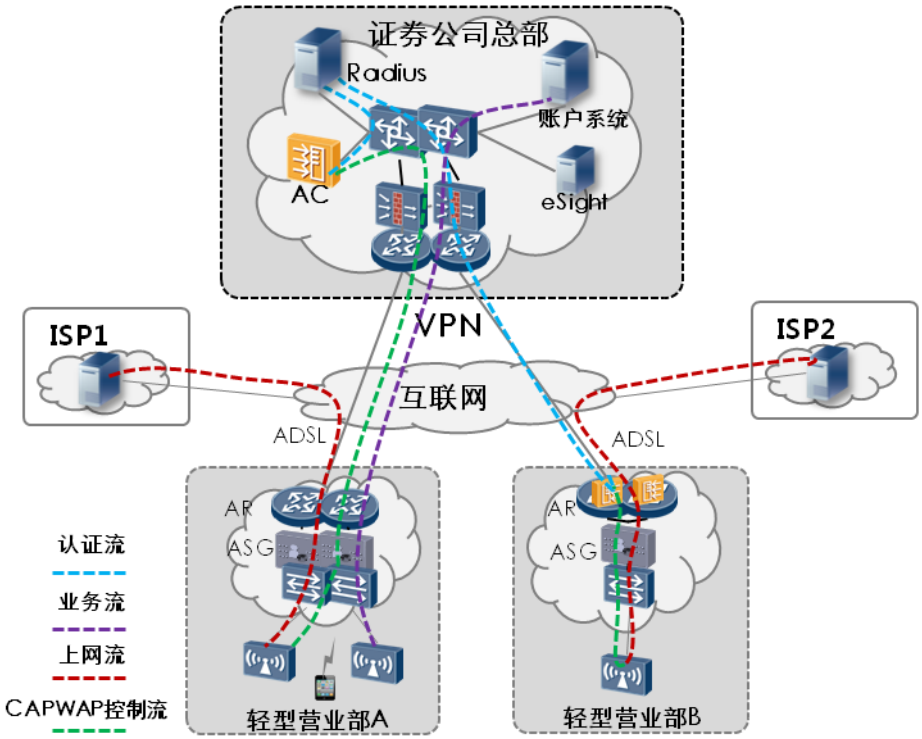

图19 WIFI 组网

5.6.2 WIFI 用户认证

华为WIFI网络产品支持无认证，本地密码认证和基于RADIUS的802.1X认证多种模式，同时通过华为专有的用户组控制策略，可以对不同的办公用户分配不同的访问权限；通过AC控制器与Radius服务器配合，实现对用户登陆设备台数和登陆时长的管理。

用户的认证策略

对于客户区的用户实现无认证模式接入WLAN网络，并通过DHCP动态方式获取IP；对于办公区的用户可通过RADIUS的802.1X认证模式接入办公网络，并通过静态或者动态方式获取IP。对于802.1X认证可以选择用户名/密码或者数字证书模式。

AC与Radius配合

在AC控制器上启动Radius的认证和计费功能，同时在Radius服务器上配置一个用户下面支持的max session数为1来实现一个用户只允许同时一台终端设备在线，如有其它终端想通过此用户名登陆，则会认证失败，通过AC控制器在总部的集中部署，可以实现跨AP的用户统一管理。同时可在Radius服务器上配置用户多长时间后需要重新启动认证，当时间到达后，AC控制器会自动让用户下线。

5.6.3 业务 SSID

SSID主要作用就是区分不同的业务类型或用户群体，无论是客户和员工的接入带宽划分，还是多业务数据传输的隔离，都需要合理划分VLAN，而在营业部WIFI网络中，SSID也需要和VLAN根据实际业务需要进行映射匹配，承担与VLAN相同的工作，可以说SSID就是VLAN在无线网络中的延伸。因此，在业务VLAN的规划中必须综合考虑VLAN与SSID的映射关系，常见映射关系有1:1、1:N、N:1、N:N四种。

单AP可以配置多个SSID，相当于将一个AP划分为多个VAP，每一个SSID对应一个VAP，AC针对VAP进行策略下发，VAP根据策略进行终端与业务管理。华为单频AP可支持16个SSID，双频AP可支持32个SSID。

在营业部无线网络中，按照无线业务，一般建议设置2个SSID，即员工办公和客户上网，客户或员工移动时，无线接入可在AP之间自动漫游切换，用户感觉不到掉网。SSID还可以根据实际业务需求来增加，不同区域的AP可设置不同的SSID来实现不同的业务承载。

华为AP6010产品可以支持802.11a/b/g/n，满足不同客户端接入需要；支持MIMO，成倍地提高无线信道容量、信道可靠性，降低误码率。支持802.11af标准的POE供电。

5.7 机柜设计

华为证券一体机呈现为一体化总装机柜，该总装机柜集成了机柜、UPS、配箱、PDU、电池、网络设备、安全设备等。

一体机统一选型，统一测试，统一发货；采用无机房化设计，免工勘；一体机出厂前即完成预装，现场只需简单安装电池包即可，满足轻型营业部快速部署的需求。一体机可根据用户需求灵活配置基本单元的种类及数量，在电力供应、通信端口上预留合理的余量，保障灵活、快速的实现平滑扩容。其中UPS标配3KVA，配置的电池可满足机柜内设备及外部少量设备至少30分钟备电。

机柜的前门、后门及侧板均可锁定，用提供的专用钥匙打开；机柜底部设有防鼠功能过线底板，支持上走线和下走线。

机柜的技术指标如下：

项目	规格描述
标准化	标准化机柜，符合 IEC60297-1 标准
尺寸	W×D×H：600mm *1100mm *1200mm
电源制式	单相交流输入，额定： 220V/230V/240V AC 50Hz（60Hz）
兼容性	全面支持第三方 IT 设备
气流组织	机柜前单开门，后双开门
快速部署	自带滚轮，调平支脚，可快速搬运安装
工作环境	温度 5~30℃，相对湿度 10~90%
防护等级	IP50 防尘/防水滴（风扇除外）
防雷等级	满足 C 级防雷等级
UPS	输入 165V~275V AC；

	输出 220/230/240±1%V AC； 输出额定功率：3kVA

机柜具有小环境监控能力，可以对开关门磁、温、湿、烟、水浸传感并可通过网管进行短信等方式告警，可以满足复杂环境下的应用。并支持UPS、电池的状态监控。

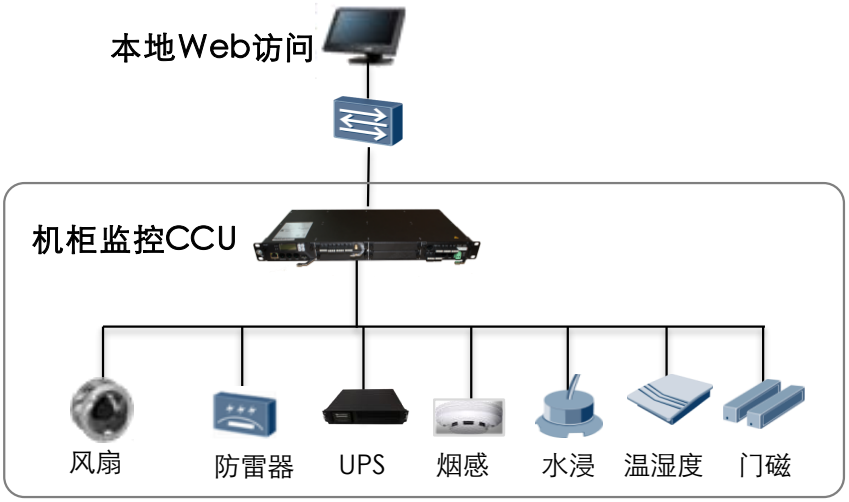

图20 CCU 监控

5.8 快速部署设计

证券轻型营业部解决方案支持轻型营业部L1&L2设备的快速、自动化的部署，运维方案的快速部署设计从三个方面来完成该项工作：软硬件预配置、U盘开局、远程配置。

5.8.1 软硬件预配置

一体机硬件预安装

1) 安装L1设备（UPS、PDU等）；

2) 安装路由器、交换机、ASG等L2设备；

3) 安装理线架、理线托盘、机柜假面板等附件；

4) 综合布线：包括信号线、电源线、接地线；

5) 机柜电池包不做预安装，而是在客户现场安装；

软件预安装

- 完成一体机内各设备的缺省软件的安装工作，软件预安装包括AR路由器、S2700交换机、ASG等缺省软件安装。

网络预配置

1) AR、ASG、交换机、网关等网络参数设置；

2) 局域网交换机VLAN划分；

3) 无线SSID设定；

业务系统预配置

- 通过业务系统预配置使得客户对机柜上电后，各设备即可正常工作，在远程连接接通后即可融入证券公司整体网络，开始正常工作。
- 业务系统预配置工作包括缺省的的防火墙策略、上网行为管理策略、QOS策略、视频监控业务系统的部署。

5.8.2 U 盘开局

U盘开局是指在一体机开局部署时，使用U盘中预先存储的配置文件、软件包等开局文件完成营业部网络的初始配置，打通营业部与总部的网络，再由总部通过网管或SSH等远程连接实现一体机内设备的详细配置，这样可以避免专业的IT技术人员到开局现场进行现场设备调测。营业部人员安装好机柜电池包，整机上电检查无问题再下电，再分别把U盘插到AR、ASG上，然后一体机上电，设备自动完成数据配置，实现网络连接配置、软件升级等操作。其中交换机与AR已经预先连线，通过AR可实现S27交换机的开局。

U盘开局协作流程如下：

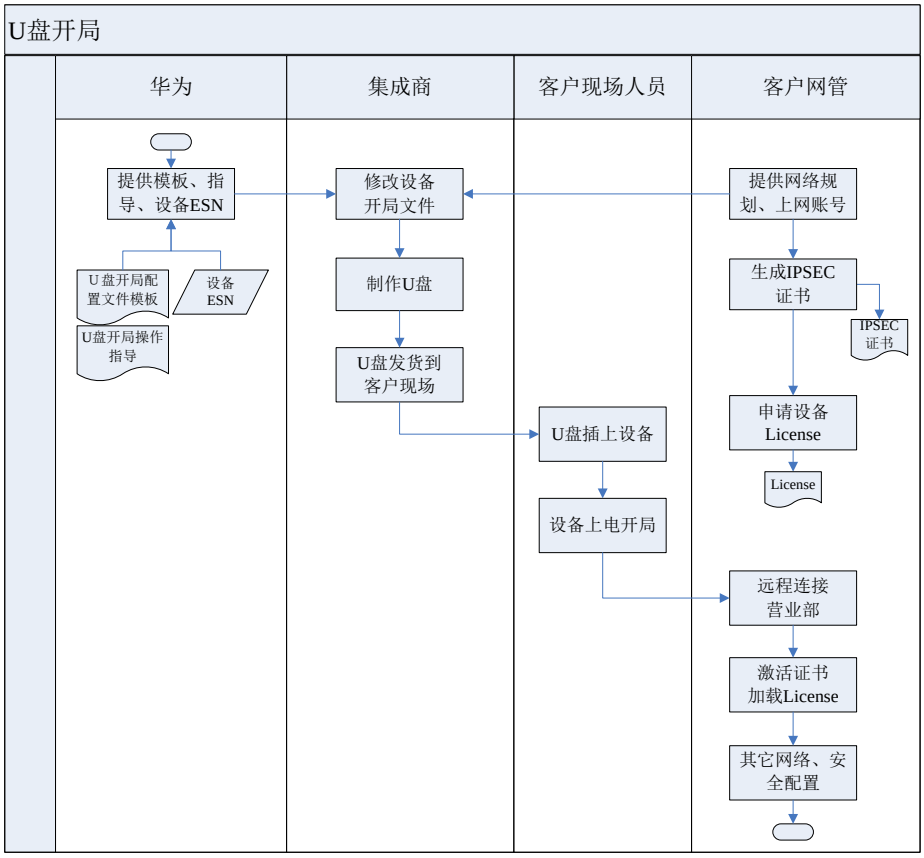

图21 U 盘开局界面

- **华为**

1）根据轻型营业部的特点和典型套餐配置，提供证券一体机的缺省配置模板，包括AR、ASG、交换机等的U盘开局索引和配置文件；其中AR负责完成交换机的开局；

2）为集成商和客户提供U盘开局指导文件；

3）根据具体项目为集成商提供营业部设备的ESN号，集成商根据ESN制作不同的U盘；

- **集成商**

1）依据客户提供的网络规划、上网账号等，修改U盘开局模板，生成客户化配置文件；为了避免AR的U盘混插，AR开局索引文件中指定对应AR的ESN号；

2）把U盘正确编号，分别把AR、ASG的开局文件拷到U盘中；

3）把U盘发货到对应的营业部现场；

- **客户现场人员**

1) 按U盘编号分别插入AR、ASG等设备；

2) 机柜整体上电，观察设备开局指示灯，绿灯常绿表明开局成功；开局成功后通知总部网管；

- **客户网管**

1) 为集成商提供网络规划和上网账号等信息；

2) 如果与营业部的IPSEC VPN使用证书认证，则需要制作证书；

3) 由于AR的AC功能、ASG的审计等功能需要软件License，需要到华为网站提供合同号、ESN等信息申请下载License；

4) 营业部现场人员U盘开局成功后，网管通过网管或SSH等方式连接到营业部；

5) 网管加载设备软件License，并激活IPSEC证书（如果有）；

6) 网管再完成营业部的其它网络和安全配置，营业部开局整体结束；

5.9 推荐配置清单

简配型配置清单：

序号	名称	型号	描述	推荐数量	选择性
1	路由器	AR1220		1	必选
1.1	AR 路由器	AR1220	AR1220,2GE WAN,8FE LAN,2 USB,2 SIC	1	必选
1.2	3G 接口卡	AR01SDGW1A	3G HSPA+7 接口卡-1*2	1	必选
	3G 延长线	ASMAM0001	3G 全向天线-垂直极化-不需要支架	1	
1.3	ADSL 接口板卡	AR0MSLA1XA01	1 端口 ADSL2+ ANNEX A/M WAN 接口模块	1	必选
2	交换机	S2726		1	必选
2.1	交换机	S2700-26TP-EI-AC	S2700-26TP-EI-AC 主机(24FE,2GECombo,交流供电)	1	必选
3	上网行为管理	ASG2100		1	必选
3.1	上网行为管理网	ASG2100-AC	ASG2100 标配 2GE 交流主机-含 4GE(RJ45)电接口板-含	1	必选

	关		HS 通用安全平台软件		
3.2	WIFI 扩展卡	SU1M0MAPWN00	WLAN 业务板-含 HS 通用安全平台软件	1	必选
3.3	软件 License	LIC-CFA-ASG2100	内容过滤与审计功能模块开关-含 HS 通用安全平台软件	1	必选
4	机柜	24U 标准机柜		1	必选
4.1	24U 标准机柜	DC3B24UCAB01	数据中心服务器机柜(24U,PDU,3KVA UPS),AC 220V*1)	1	必选
4.2	电池包	3K 专用	备电模块-UPS 电池包-96V-7Ah-3K 专用	1	必选
4.3	外接线缆	机柜接地线	电子电力线缆-450V/750V-黄/绿-62A（单位：米）	5	必选

标配型配置清单：

序号	名称	型号	描述	推荐数量	选择性
1	路由器	AR2220		2	必选
1.1	AR 路由器	AR2220	AR2220 路由器(百兆_RJ45*8,千兆_RJ45*1,单交流电源)	2	必选
1.2	3G 接口卡	AR01SDGW1A	3G HSPA+7 接口卡-1*2	1	必选
	3G 延长线	ASMAM0001	3G 全向天线-垂直极化-不需要支架	1	
1.3	ADSL 接口板卡	AR0MSLA1XA01	1 端口 ADSL2+ ANNEX A/M WAN 接口模块	2	必选
1.4	软件 License	LAR0DATAE03	AR2200 数据业务增值包	2	必选
		LAR0AC03	AR2200 无线控制器 license	2	
2	交换机	S2726		1	必选
2.1	交换机	S2700-26TP-EI-AC	S2700-26TP-EI-AC 主机(24FE,2GE Combo,交流供电)	1	必选
3	上网行为管理	ASG2100		1	必选
3.1	上网行为管理网关	ASG2100-AC	ASG2100 标配 2GE 交流主机-含 4GE(RJ45)电接口板-含 HS 通用安全平台软件	1	必选
3.2	软件 License	LIC-CFA-ASG2100	内容过滤与审计功能模块开关-含 HS 通用安全平台软件	1	必选
4	WLAN	AP6010		2	必选
4.1	WLAN AP	AP6010DN-AGN-CN	AP6010DN-AGN 组合配置(11n,室内普通型,2x2 双频,内置天线,含中式电源适配器)	2	必选
5	机柜	24U 标准机柜		1	必选
5.1	24U 标准机柜	DC3B24UCAB01	数据中心服务器机柜(24U,PDU,CCU,3KVA UPS,监控组件(烟雾,温湿度,液位传感器,门磁开关*2),AC 220V*1)	1	必选
5.2	电池包	3K 专用	备电模块-UPS 电池包-96V-7Ah-3K 专用	1	必选
5.3	外接线缆	机柜接地线	电子电力线缆-450V/750V-黄/绿-62A（单位：米）	5	必选

增强型配置清单：

序号	名称	型号	描述	推荐数量	选择性
1	路由器	AR2220		2	必选
1.1	AR 路由器	AR2220	AR2220 路由器(百兆_RJ45*8,千兆_RJ45*1,单交流电源)	2	必选
1.2	3G 接口卡	AR01SDGW1A	3G HSPA+7 接口卡-1*2	1	必选
	3G 延长线	ASMAM0001	3G 全向天线-垂直极化-不需要支架	1	
1.3	ADSL 接口板卡	AR0MSLA1XA01	1 端口 ADSL2+ ANNEX A/M WAN 接口模块	2	必选

1.4	软件 License	LAR0DATAE03	AR2200 数据业务增值包	2	必选
		LAR0AC03	AR2200 无线控制器 license	2	
2	交换机	S2726		2	必选
2.1	带 POE 交换机	S2700-26TP-PWR-EI	S2700-26TP-PWR-EI 主机(24 百兆 RJ45,2 千兆 Combo,PoE,双电源槽位,不含电源)	2	必选
2.2	交换机电源	W0PSA2500	交换机电源，250W 交流电源模块(灰色)	2	必选
3	上网行为管理	ASG2100		2	必选
3.1	上网行为管理网关	ASG2100-AC	ASG2100 标配 2GE 交流主机-含 4GE(RJ45)电接口板-含 HS 通用安全平台软件	2	必选
3.2	软件 License	LIC-CFA-ASG2100	内容过滤与审计功能模块开关-含 HS 通用安全平台软件	2	必选
4	WLAN	AP6010		2	必选
4.1	WLAN AP	AP6010DN-AGN-CN	AP6010DN-AGN 主机(11n,室内普通型,2x2 双频,内置天线,不含电源适配器)	2	必选
5	机柜	24U 标准机柜		1	必选
5.1	24U 标准机柜	DC3B24UCAB01	数据中心服务器机柜(24U,PDU,CCU,3KVA UPS,监控组件(烟雾,温湿度,液位传感器,门磁开关*2),AC 220V*1)	1	必选
5.2	电池包	3K 专用	备电模块-UPS 电池包-96V-7Ah-3K 专用	2	必选
5.3	外接线缆	机柜接地线	电子电力线缆-450V/750V-黄/绿-62A（单位：米）	5	必选

5.10 方案亮点

- 3种系列化套餐，满足不同成本、安全、体验需求
- 一体化设计，减少二次组装
- 傻瓜式电池包安装，不需要专业人员
- 带板运输，U盘开局，部署效率高70%
- 集中管理，无需专业IT人员
- 投入小，降低CAPEX

6 数据中心接入区方案

6.1 网络架构设计

原有传统营业部主要以专线方式通过公司安全接入区与总部数据中心互联。而轻型营业部多通过互联网宽带接入，如果仍从原接入区接入，会给数据中心带来安全隐患；大量的轻型营业部接入，也会对原有接入区造成扩容压力；同时，见证开户等移动业务的开展也需要改造接入区，并需要考虑移动E2E安全。从网络的改造难度、可靠性和安全性等方面考虑， 我们建议新建轻型营业部接入区。

新建的接入区需要支持轻型营业部的接入和扩容，并需要充分考虑互联网接入方式的安全性和可靠性，以及保证移动应用的安全接入。如下为轻型营业部的接入中心网络架构图：

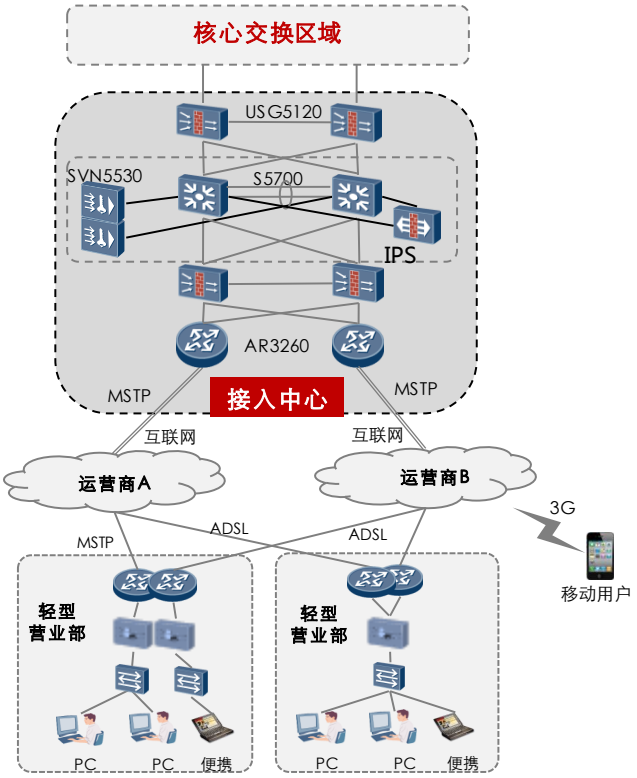

图22 轻型营业部接入区

证券公司已启动同城双中心、两地三中心的建设，实现数据中心接入网络的异地冗余备份，因而轻型营业部接入区则需要考虑双中心或多中心的建设。轻型营业部分别接入不同的接入中心，增强业务可靠性。双接入中心网络架构如图所示，多个接入中心的可借鉴双接入中心方案。

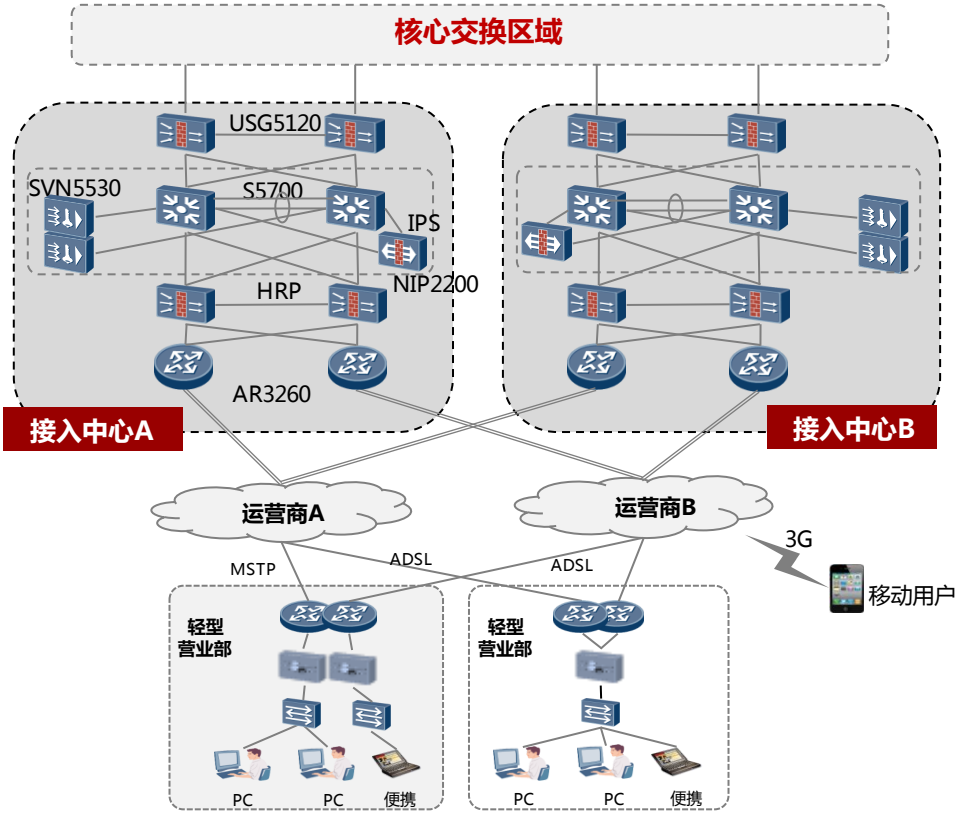

图23 双接入中心网络架构图

接入区AR路由器具有多种接口卡，可以支持MSTP专线、FE/GE方式接入运营商网络；同时路由器支持IPSec VPN、GRE等VPN，支持营业部与总部间的VPN通道。

6.2 安全设计

为了提高接入区的安全性，接入区采用两层防火墙的“三明治”架构，两层防火墙为间DMZ区。VPN、防火墙、IPS、SVN形成了比较全面的安全防护：

- VPN：AR路由器终结IPSec VPN，最多支持6000个IPSec隧道；AR同时支持最多1024个GRE隧道，支持多达1000个营业部采用GRE over IPSec隧道动态交换路由信息；
- 外层防火墙：可实现NAT、广域隔离、攻击防范等，对外网进行第一层隔离；
- 中间IPS：服务器漏洞防护、Web应用防护、恶意软件防护、DDoS防护等，既进行入侵检测，又可以避免误报；
- 内层防火墙：对外网进行第二层隔离，同时将DMZ 与内网核心区隔离，提高安全性；
- SVN：终结移动用户的SSL VPN，实现数据传输加解密；SVN设备旁挂在DMZ区交换机，不影响营业部链路的接入。

6.3 可靠性设计

数据中心接入区通过多种设计保证可靠性：

多链路冗余：AR路由器支持专线、以太网等多种接入方式；通过不同运营商分别接入，实现链路的冗余备份。

防火墙双机冗余：内层和外层防为墙分别采用VRRP双机主备冗余方式，既保障安全防护，又做到良好的可靠性。

交换机堆叠：DMZ区交换机通过堆叠虚拟成一台交换机，既使得管理配置方便，又保证可靠的数据交换。

SVN双机冗余：SVN支持VRRP双机主备冗余，通过HRP心跳线保证状态同步。

IPS设备：华为NIP设备支持双机冗余，客户根据需要配置。

客户可以根据需选择购置链路负载均衡和服务器均衡设备。

6.4 路由策略

本方案采用GRE+OSPF的路由方式，单接入中心、双接入中心及多接入中心配置方式类似，此处以双接入中心场景作为举例。

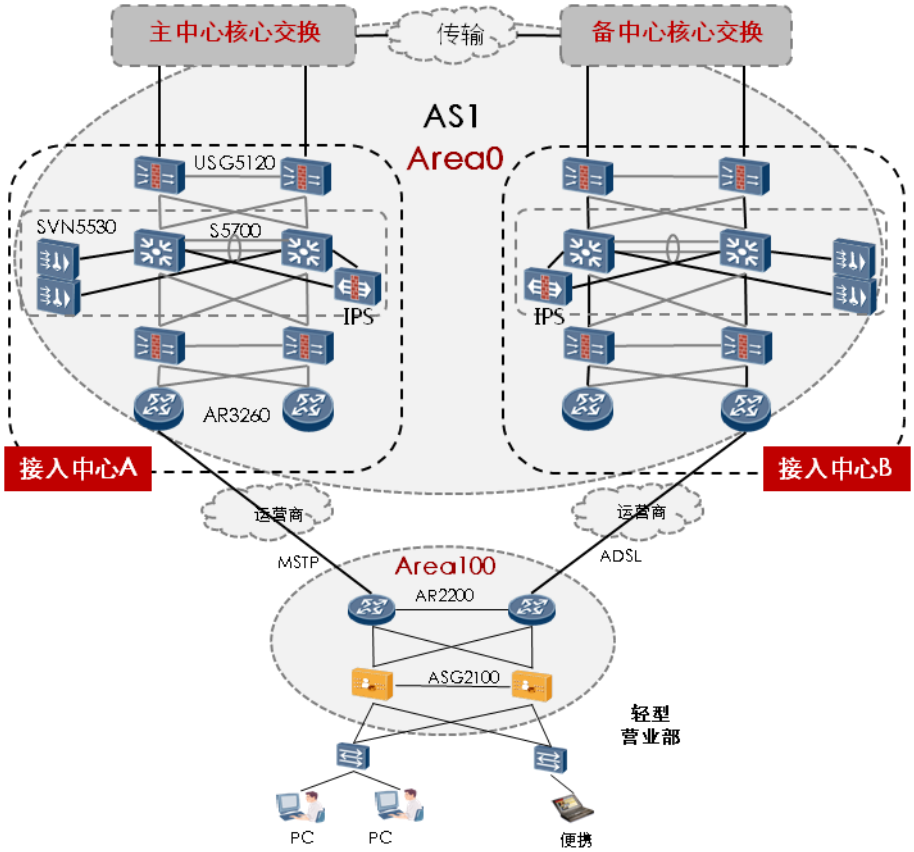

图24 路由规划

如图以营业部接入2个运营商链路作为案例，接入方式可以为ADSL、3G及各类专线，营业部公网IP可以为静态IP或者浮动IP地址类型。

建立主备链路通道，如果是安全性较高的专线，比如MSTP，可以不建立IPSEC VPN通道，对于ADSL及3G拨号链路在营业部端建立与总部的IPSEC VPN通道。在不同运营商之间进行链路传输，可能会影响传输质量，所以建议在营业部、接入中心同一家运营商之间建立IPSEC VPN通道，如图蓝色线示意在不同运营商异地建立备份链路，如果是单接入中心，则备份链路建立在接入中心另外一个路由器接口处，如此建立证券公司虚拟的局域网络。

根据证券公司规划的私网IP地址，在建立好的虚拟局域网络中，在IPSEC VPN及专线链路上，建立起主备GRE通道配置总部为OSPF骨干区域，每50~100个营业部为一个stub区域，营业部主线路COST值高于备链路，使用OSPF协议进行收敛，在营业部主链路上进行BFD探测，加速路由表的收敛。

6.5 Qos 规划

当网络出现拥塞时，优先保证对时延敏感业务。广域数据流的QoS优先级规划如下：

数据流	QOS优先级	CLASS	DSCP	备注
管理/控制流	高	EF	101110	低丢包率、低时延、高带宽
语音/视频流				
交易流	高	AF4	100010	带宽保证、低时延
经纪流			100100	

行情流	较高	AF3	011010	
办公流	一般	AF2	010010	
上网流	低	BE	000000	

调度策略：

1）采用CBQ调度策略，根据各类队列DSCP优先级转发；

2）采用WRED加权随机先期检测机制，预测网络的拥塞情况，提前丢弃非关键的数据包，防止TCP的全局同步问题。

6.6 移动终端接入设计

证券公司将逐步开展非现场开户等移动营销业务，让证券公司从业人员可以借助互联网通过标准的Web浏览器或者客户端软件随时随地安全访问证券公司内网资源。

SSL(Secure Socket Layer) VPN是以SSL/TLS协议为基础进行扩展的新型VPN，是互联网移动应用采用的主要VPN技术。SSL VPN不仅能够对IP通信进行保护，而且实现了更加细致的访问控制能力，大大增强了对内网的安全保护。同时，SSL VPN通信基于标准TCP/IP，因而不受NAT限制，能够穿越防火墙，使用户在任何地方都能够通过SSL VPN网关代理访问内网资源，使得远程接入更加安全、灵活简单。

SVN（Security Virtual Network）是华为公司面向金融等行业推出的一款一体化VPN网关设备。部署SVN，无需改变网络结构，可以直接单臂挂接到客户现有出入口防火墙或者路由器、交换机上，简单快捷。SVN基于华为专业的高可靠硬件平台和专用的实时操作系统，具备业界领先的系统安全性和可靠性，针对证券公司非现场开户的远程接入需求，提供了安全、便捷、高效、易管理的端到端远程接入解决方案。

华为的SVN设备通过与移动终端配合，在不安全的公共网络上构建安全的SSL隧道，满足大量智能移动终端用户的接入需求，同时保障数据的传输安全。在用户通过SVN的身份认证、终端安全检查等策略检查后，用户登录SVN网关，在公网上建立起和内部网络之间的加密隧道。用户所有的认证信息和应用数据都通过加密后在公网上传输，避免了数据被非法窃取和篡改的风险。不同的用户拥有不同的权限，根据访问控制策略对用户的访问行为进行控制，避免越权非法访问。

SVN方案提供的主要功能有：

- ✧ 对用户进行全面的身份认证、访问授权以及行为审计，充分保证用户身份的合法性，实现灵活细致的访问控制策略。
- ✧ 对远程用户与证券公司内网之间的传输数据进行强加密，保护敏感信息，杜绝信息泄露。
- ✧ 对广泛的远程访问业务提供支持，包括对Web资源、文件系统、多种C/S应用以及与应用无关的全IP层业务访问。
- ✧ 提供详细的日志功能，便于对用户/管理员的操作行为进行实时的审计与管理。

6.7 推荐配置清单

产品	型号	数量
路由器	AR3260	2
防火墙	USG5120	4
交换机	S5700	2
SSL 网关	SVN5530	2
IPS	NIP2200	1

6.8 方案亮点

- **与营业部预集成，交付快**：与证券一体机预集成测试，保证快速对接，不存在兼容性问题
- **无私有协议，自主可控**：支持开放的OSPF等协议，符合公开的RFC
- **低成本链路接入**：支持使用ADSL、3G等低成本线路通过互联网VPN接入
- **统一网管**：与营业部使用同一套网管，真证实现统一管理

7 AnyOffice 见证开户方案

7.1 方案概述

7.1.1 见证开户流程

见证开户是指由证券公司开户工作人员在公共场合面见客户并通过证券公司网络或单机版见证开户系统为客户开立账户。目前见证开户分为双人见证开户和视频见证开户。

双人见证开户模式是两名工作人员（如客户经理和见证人）与客户在公共场合约见，客户经理通过非现场开户系统辅助客户完成开户需要的资料录入及相关文件签署等环节，见证人在旁监督整个开户过程以符合规定；为了保证整个开户业务的开展，需要账户审核人员以及回访人员配合完成。由于要求见证人是证券公司签署劳动合同的正式员工，所以见证人数量并不太多，难以大规模进行双人见证开户；且见证人外出服务的客户少，综合成本高。

视频见证开户模式是证券公司委派一名客户经理面见客户，客户经理通过非现场开户系统辅助客户完成开户需要的资料录入及相关文件签署等环节，由公司统一组织的柜台人员以远程实时视频方式完成见证。见证人可以集中部署，少数人满足大量业务需求。

双人见证和视频见证的业务流程基本一致，主要差别是一个由见证人在本地见证，一个是见证柜员远程视频见证，参见下图：

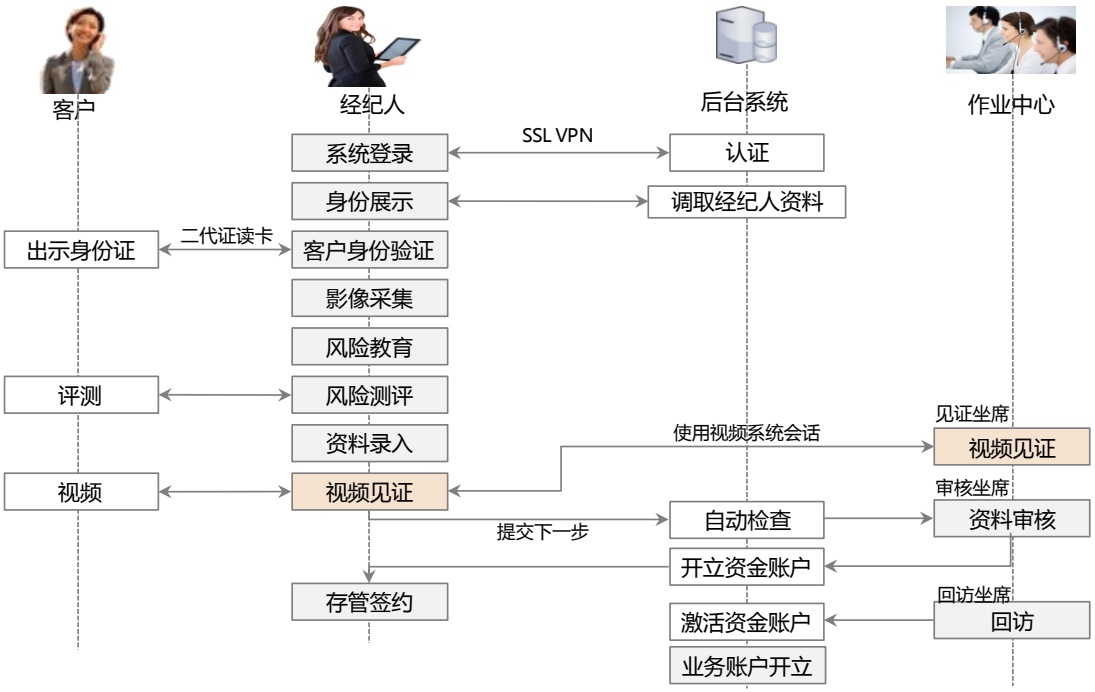

图25 见证开户

以上流程可由非现场开户系统软件进行配置：

1) **经纪人登陆**：通过员工（柜员）号登录非现场开户系统，便于查询统计以及考核；

2) **经纪人身份展示**：使用客户端查询工作人员信息并展示给客户(无需登陆证券协会网站)；

3) **客户身份验证**：通过二代证读卡器直接读取，辅助中登与公安联网校验；

4) **影像采集**：通过终端实时采集影像或图片并上传系统，可辅助中登的标准进行框选；

5) **风险教育**：系统可根据证券公司要求进行模板配置；

6) **风险测评**：系统可根据证券公司要求及开通的不同业务品种配置；

7) **资料录入**：使用客户端将客户其他信息（邮寄地址等）进行界面录入；

8) **视频见证**：远程见证人员通过系统与客户即时视频，确认客户身份信息和开户意愿；

9) **资料审核**：审核客户的资料及影像信息的真实性，生成客户代码，未激活资金账户；

10) **存管签约**，密码设置：客户选择证券公司现有存管银行签约的模式，并设置资金交易密码；

11) **业务账户开立**：客户选择存管签约扣费方式和密码设置，为客户开立股东等业务账户；

12) **回访**：客户在设置密码，存管签约后，即可对客户进行回访激活资金账户；

双人见证和视频见证都要求客户经理使用便捷的移动终端（如PAD）完成上述业务操作，提高开户效率，提升品牌；同时移动终端的安全管理也需要重点考虑。

7.1.2 见证开户方案

根据业务开户的业务需求，我们提出见证开户一体机+AnyOffice移动安全平台的解决方案。其中见

证开户一体机满足行业移动终端的需求，AnyOffice安全平台可以为终端提供移动工作台、SSL VPN安全接入、MDM移动设备生命周期安全管理等功能。非现场开户系统（含见证开户）由合作伙伴提供。

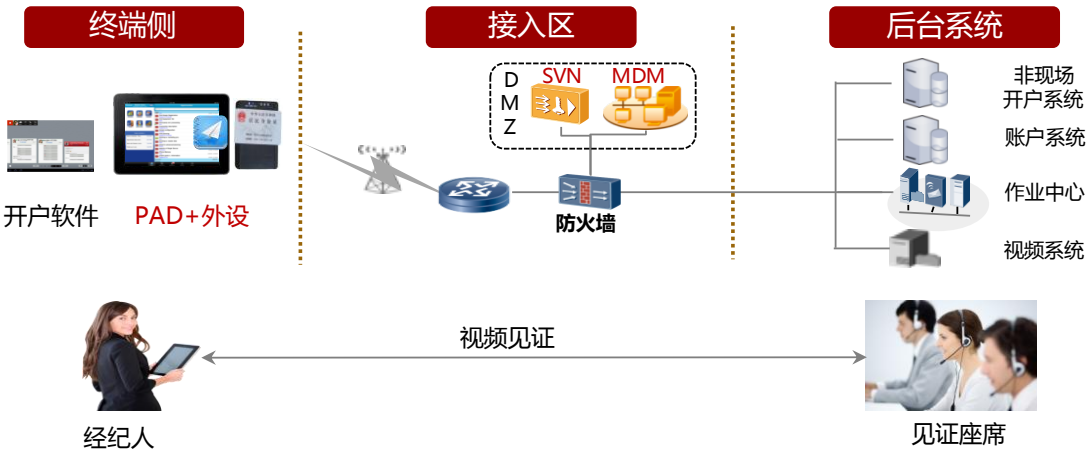

图26 见证开户方案

7.2 见证开户一体机

采用传统工具的见证开户将面临一些问题：

- 作业工具多，易遗忘或丢失，影响开展业务；
- 工具笨重，携带方便、使用效率低；
  - 携带笨重的设备箱(包)：便携机、摄像机、高拍仪、二代身份证读卡器、备用电源、3G卡及各种接口线等 ；
  - 便携机、摄像机续电时间短，没电错失很多机会；

根据行业需求和当前工具存在的问题，我们提出了见证开户一体机的解决方案。方案采用华为的MediaPAD10+行业定制背夹，可以为客户提供便携式、一体化的见证开户或移动营销的高效工具。

图27 见证开户一体机

见证开户一体机具有如下特点：

- **专业防护设计**：防水、防尘、防震；
- **二代身份证识别**：识别第二代居民身份证的真假，读取身份证上的用户信息，安全、高效；
- **大容量电池**：10000mAH大容量备用电池；
- **独特串口设计**：背夹独特的USB转串口设计，改变与PAD传统的蓝牙连接，解放PAD的蓝牙接口，可以使用空闲的蓝牙接口连接蓝牙打印机、POS机等设备；
- **预留接口**：预留USB、音频等接口，方便临时对接不常用外设

7.3 AnyOffice 移动安全平台

7.3.1 AnyOffice 平台介绍

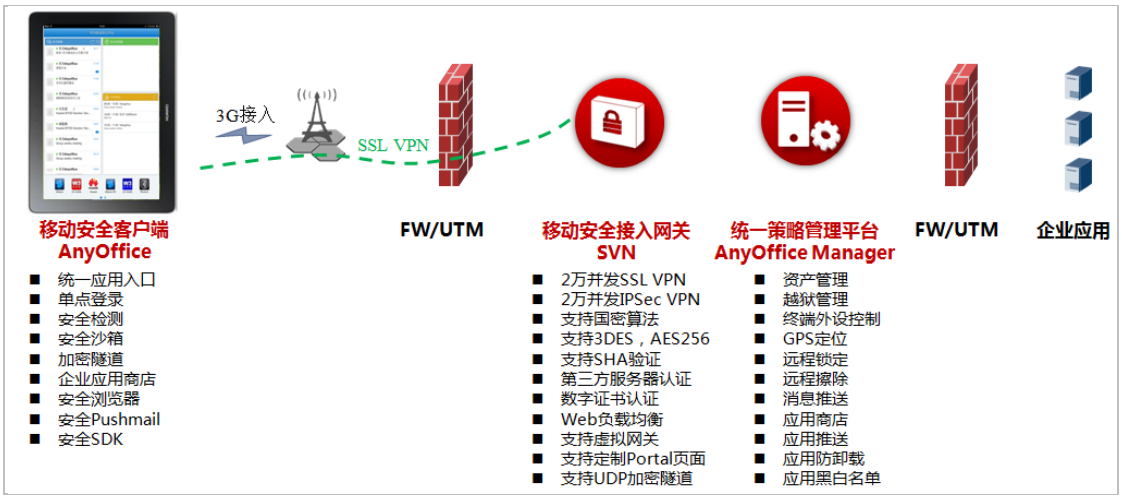

图28 AnyOffice 主要组件

华为AnyOffice移动安全平台解决方案包括移动安全客户端（AnyOffice客户端）、移动安全接入网关（SVN）、统一策略管理平台（AnyOffice Manager）共3个重要组件，它们协同提供终端管控、应用管理、数据安全等EMM（企业移动管理平台）基础平台功能。

1) **移动安全客户端**（AnyOffice客户端）

AnyOffice客户端作为移动终端上的企业应用统一接入平台，提供安全沙箱、SSL VPN等安全功能，并配合AnyOffice Manager，实现MDM、MAM、MCM等功能；AnyOffice客户端提供安全SDK，供第三方应用快速集成安全功能；

2) **移动安全接入网关**（SVN）

SVN是SSL/IPSec一体化VPN网关，支持2万规模并发VPN，支持口令、数字证书、短信、硬Key等多种认证方式，支持国密算法；

3) **统一策略管理平台**（AnyOffice Manager）

AnyOffice Manager作为AnyOffice移动安全平台方案的核心组件，与AnyOffice客户端协作，实现

MDM、MAM、MCM等功能。

7.3.2 移动安全客户端（AnyOffice 客户端）

图29 AnyOffice 客户端

AnyOffice移动安全客户端是基于沙箱的统一移动工作台，可满足移动办公的通用需求，保障企业员工安全、顺畅、高效地接入和访问企业内网。

AnyOffice移动安全客户端主要特性如下：

- **安全平台**：提供企业统一应用入口、单点登录、安全沙箱、VPN加密隧道等功能
- **终端管理**：配合AnyOffice Manager，提供MDM、MAM、MCM等功能
- **安全SDK**：应用集成只需1～2天，即具备移动沙箱及VPN等安全特性，加快发布

7.3.2.1 安全平台

1) 主流操作系统支持

AnyOffice是一个开放的平台，它支持当前流行的Android、iOS、Windows Phone7等各类智能终端操作系统。基于移动业务需求，推荐终端选配如下：

- **iOS**：身份、品牌的象征；建议使用于领导移动办公、大堂产品展示等场景；
- **Android**：扩展性强，易接外设、背夹；建议用于见证开户等移动营销场景；
- **Windows Phone7**：该类终端市场份额小，产业链不够成熟，暂不建议使用。

2) 企业统一应用入口

AnyOffice客户端提供企业应用统一入口，企业应用都在平台中展现，把企业应用和个人应用独立开来，企业应用图标支持分组布放，便于应用管理及查找，且提升企业形象。

3) 单点登录

AnyOffice平台支持单点登录特性，只需平台一次登录后，平台中的所有应用在启动时在后台静默登录，无需用户再重复输入登录信息，免除重复登录烦恼，增强用户体验效果。

4) 安全沙箱

图30 安全沙箱

AnyOffice 支持数据隔离功能，企业数据落地在安全沙箱中，用户个人数据都被隔离在安全沙箱之外；用户在AnyOffice内阅览和编辑的所有内容都不能拷贝到AnyOffice外部，也不能把AnyOffice外部的数据拷贝进来；这种手段既保证企业数据不被外泄，也避免了病毒、木马等非法程序在企业内部的传播和感染。

5) VPN加密隧道

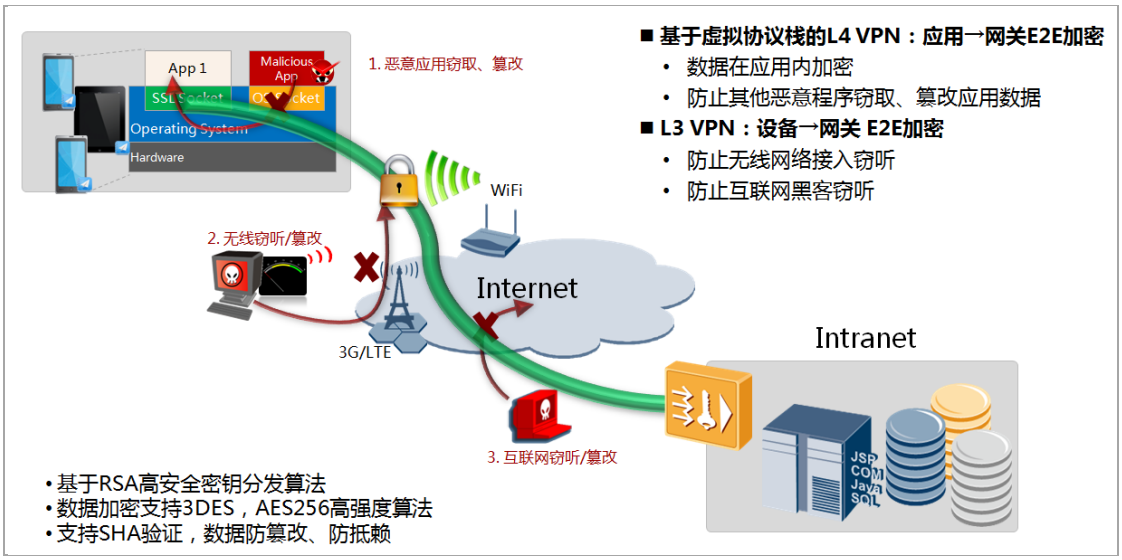

图31 VPN 加密隧道

SSL VPN加密隧道保证了终端应用到移动安全接入网关间的数据传输进行端到端加密，避免遭受途经网络可能存在的数据窃听、篡改等危害，AnyOffice平台支持3DES、AES256以及国密（SM1、SM2、

SM3）等高强度算法，充分保证企业数据安全。

6) 统一文档转换模块

AnyOffice内置的文档转换模块可以将Windows Office文档转换成移动终端系统可识别的格式，并呈现给用户，譬如，将PowerPoint格式转换为图片格式；也支持对ZIP、RAR压缩包的解压、PDF文档的解析和呈现、GIF等图片格式的呈现。

文档转换模块为安全浏览器和安全邮件客户端提供方便快捷的文件在线浏览能力，通过这个模块，用户可以用安全浏览器直接浏览公司文档，也可用安全邮件客户端打开邮件附件中的各类文档，而不必担心手机或平板不识别Office文档的问题，也不必安装第三方的文字处理软件。

7.3.2.2 终端管理

AnyOffice客户端配合AnyOffice Manager服务端，完成MDM（移动设备管理）、MAM（移动应用管理）、MCM（移动内容管理）等功能，具体功能介绍详见AnyOffice Manager章节描述。

7.3.2.3 安全 SDK

图32 安全 SDK 架构

安全SDK不是一个可独立工作的组件，而是一个软件开发包，它不对外公开源代码，但对外提供API供集成它的上层应用使用。

SDK通过华为公司的Dopra抽象层和各个具体的操作系统适配对接，屏蔽底层操作系统的差异，向上提供统一的本地加解密接口、兼容标准SOCKET的安全通信接口，方便各类自研及第三方的应用集成，只需1～2天，使第三方应用具备数据加密传输、移动沙箱等安全能力，加快应用发布速度，降低应用开发及维护成本。

7.3.3 移动安全接入网关（SVN）

SVN2000-M/SVN5000-M系列安全接入网关是华为公司面向运营商、政府、金融及其他行业推出的优秀的SSL/IPSec一体化VPN网关设备，它基于华为专业的高可靠硬件平台和专用的实时操作系统，具备业界领先的系统性能、安全性和可靠性。

SVN2000-M/SVN5000-M主要特性如下：

- 超大性能：SSL/IPSec一体化VPN网关，支持2万规模并发VPN
- 多种认证：支持口令、数字证书、短信、硬Key等多种认证方式
- 支持国密：支持国密SM1、SM2、SM3算法

SVN支持静态路由、OSPF、BGP、ISIS动态路由协议、策略路由和路由迭代，支持IPv4和IPv6双协议栈工作方式，也支持双机热备和物理链路备份。部署SVN安全接入网关，无需改变网络结构，可以直接单臂挂接到出入口防火墙或者路由器、交换机上，简单快捷。

SVN作为企业移动办公的安全接入网关，提供了丰富的认证手段和灵活的访问授权控制手段，企业或机构可以根据自身需求、认证体系的建设情况灵活选择认证方式，保护企业的原始投资，包括VPNDB本地认证*、LDAP/AD /Radius/SecurID认证*、终端硬件特征绑定*、数字证书认证、短信认证、及多种认证方式的组合认证（*标记的为使用AnyOffice客户端接入时支持的认证方式）。

在授权和访问控制上，SVN引入角色的概念，对不同的角色授予不同的资源访问权限，同时，通过配置访问控制策略，可以在用户访问已授权资源时增加额外的访问控制，包括基于URL、IP、端口的细粒度访问控制。

SVN具备强大的移动办公安全接入能力，提供Web代理技术供用户在各种终端类型上使用标准浏览器随时随地的安全访问内网的Web服务器、提供L3VPN供Android终端以网络扩展方式访问企业内网、提供安全SDK给各种移动应用集成使之具备L4VPN接入能力，同时，还支持标准L2TP over IPSec协议的接入。

另外，SVN通过虚拟网关为用户提供SSL VPN服务。SVN作为一个物理实体，可以通过虚拟技术将其虚拟为多个逻辑上的SSL VPN网关，以提供给多个企业或者一个企业的多个部门使用。比如，某个大型企业有多个部门，每个部门有各自的员工，部门间能够访问的资源和服务也各不相同，每个部门有自己的访问控制规则。在这种情况下，就可以为每个部门分配一个虚拟网关，每个虚拟网关都是独立可管理的，可以配置各自的用户、资源和ACL规则，形成独立的访问体系。而每个部门的感觉就像各自在使用一个独立的网关设备一样高效、安全。

7.3.4 统一策略管理平台（AnyOffice Manager）

统一策略管理平台（AnyOffice Manager）是AnyOffice移动安全平台方案的核心组件，涵盖MDM、MAM、MCM等3个领域内容，通过AnyOffice Manager的管理可以避免用户在移动终端上操作可能带来的安全隐患，防止移动终端不慎丢失后造成数据泄露。

AnyOffice Manager主要特性如下：

- MDM：支持资产管理、外设管控、终端丢失管理、证书自动化等功能
- MAM：支持应用管理、应用商店、应用策略等功能
- MCM：支持安全沙箱、安全Pushmail、安全浏览器、文件安全管理等功能

7.3.4.1 MDM (移动设备管理)

1) 资产管理

资产管理功能主要提供终端资产注册/注销和管理，具体功能如下：

- **自动资产注册**：设备接入内网时，自动将终端设备信息与用户账号信息上报后台系统进行注册；
- **Email/SMS推送邀请注册码**：设备注册时，可支持注册码确认功能，增强资产安全性保障；
- **多人共用设备**：支持多个账号绑定一个终端设备，实现多人共用设备功能；
- **资产注销**：管理员手工注销、用户自助注销；
- **绑定限制**：限制一个账户可以绑定的终端数量；
- **保密协议**：用户在设备上首次接入时弹出“保密协议”信息，用户阅读并确认才允许接入；
- **自动开户**：设备首次接入时，根据账户信息，自动授予用户归属群组对应的预置权限；
- **终端状态报表**：显示终端型号、归属用户、系统信息、已装应用列表和正在运行应用列表等。

2) 外设管控

外设管控功能主要提供终端设备能力和系统环境的策略管理，具体功能如下：

- **准入检查**：用户登录时启动准入检查，策略上可检查开机密码、锁屏密码、应用列表和应用版本等；
- **防截屏**：防止恶意软件截获应用界面，通过图片泄密；
- **越狱管理**：支持越狱设备监测，可对越狱设备采取审计、提示、警告和断网四种策略；
- **系统功能控制**：支持摄像头、蓝牙、Wi-Fi、GPS、便携式热点、录音、USB网络共享、SB存储模式、云服务、备份服务和VPN等功能特性控制。
- **密码策略**：选择图形密码或者文字密码，锁屏密码可采用图形密码；密码字母最少个数、最小密码长度、最大密码长度、密码有效期、密码数字最少个数、新输入的密码和旧密码是否相同、输错密码的最大次数（达到次数即启动设备擦除）；

3) 终端丢失管理（GPS定位/远程锁定/远程擦除）

图33 终端丢失管理

在终端丢失场景，管理员可在AnyOffice Manager管理后台对BYOD设备进行远程锁定和GPS定位，若确认无法找回，也可远程擦除终端上的数据。

若用户不希望管理员干涉，则可以登录自助管理Portal，在终端丢失时，通过GPS定位功能，在地

图上直观地查看终端的物理位置，并进行远程锁定、远程擦除操作。

同时，终端的SIM变更时，会根据配置策略实现自动锁定、自动定位、远程数据擦除、短信报警和自动通知功能。

4) 证书自动化

华为AnyOffice Manager管理平台与CFCA证书系统进行定制对接，通过使用CFCA证书系统提供的证书发放、更新、吊销、重发等定制接口进行证书自动化管理，屏蔽人工操作，提高证书管理效率和改善用户体验。CFCA系统为中国金融认证中心提供的证书颁发管理系统，由CA和RA两部分组成。RA提供了封装证书申请、注销、更新、补发等接口，移动设备管理平台通过RA的证书管理接口进行证书操作。

AnyOffice Manager管理平台在运行过程中，存在如下证书管理动作触发点：

- **资产注册**：AnyOffice Manager管理平台组建包含用户名、终端ID的DN，构成证书申请请求，向RA申请并下载软证书；
- **证书即将到期**：AnyOffice Manager管理平台组建包含用户名、终端ID的DN，构成证书更新请求，向RA更新并下载新有效期的证书；
- **资产注销**：AnyOffice Manager管理平台组建包含用户名、终端ID的DN，构成证书吊销请求，向RA注销用户移动设备的证书；
- **终端证书移除**：AnyOffice Manager管理平台组建包含用户名、终端ID的DN，构成证书补发请求，向RA补发并下载用户移动设备的证书；
- **资产重新注册**：AnyOffice Manager管理平台组建包含用户名、终端ID的DN，构成证书申请请求，向RA申请并下载软证书。

7.3.4.2 MAM(移动应用管理)

1) 应用管理

应用管理主要提供企业应用的管理功能，具体功能如下：

- **查看应用列表**：终端上可查询应用列表，每个应用信息包括名称、大小、ID、版本、应用程序数据；
- **基于分组的应用**：企业应用图标分组布放，增加使用便利性。

2) 应用商店

应用商店主要提供企业应用发布功能，具体功能如下：

- **企业应用商店**：后台提供企业应用签名/分发/强制安装/强制卸载/强制升级与版本管理；前台客户端提供应用手工安装/卸载/升级/搜索/分类查看功能；
- **应用使用权限控制**：控制企业内部不同角色人员的应用使用权限（譬如，企业领导的权限和普通员工权限的区分）；
- **应用一键配置**：邮件客户端配置（EAS、IMAP、SMTP、POP等）和浏览器的配置由安全接入网关负责统一下发，自动完成配置。

3) 应用策略

应用策略主要提供企业应用及第三方应用的策略控制，具体功能如下：

- **应用防卸载**：防止应用被用户卸载；
- **应用黑白名单**：如果黑名单生效，则列入黑名单的应用不能安装，安装了也不能运行； 如果白名单生效，则只有白名单的应用可以安装使用；
- **应用推送**：支持将移动应用主动推送至终端工作台。

7.3.4.3 MCM(移动内容管理)

1) 安全沙箱

AnyOffice平台支持安全沙箱功能，保证企业数据安全，具体见移动安全客户端（AnyOffice客户端）章节介绍。

2) 安全Pushmail

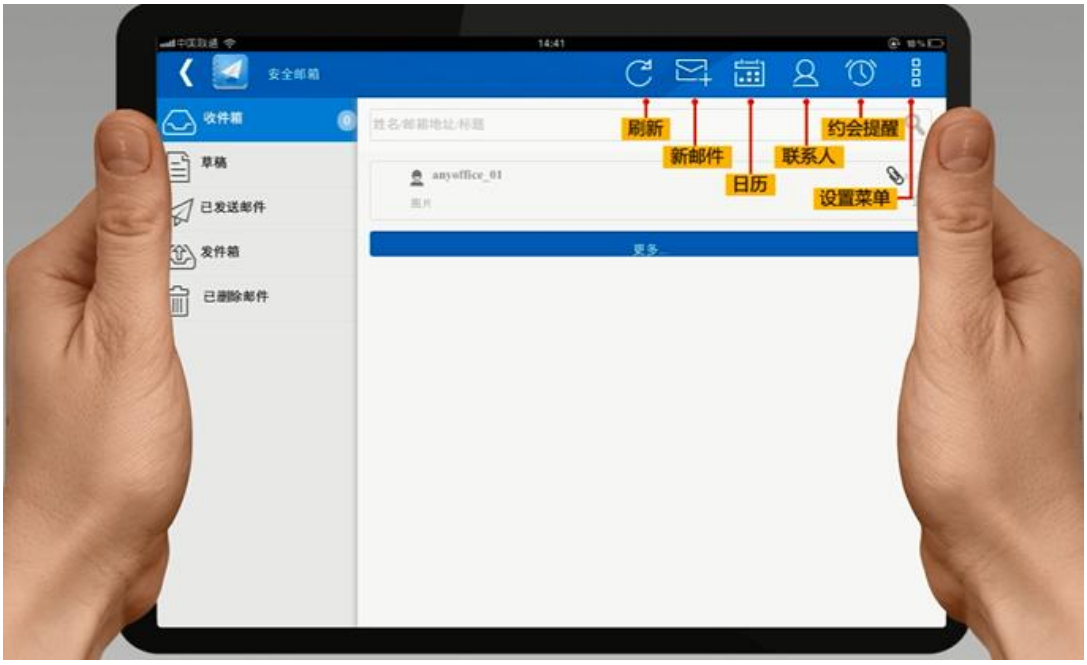

图34 安全 Pushmail

Pushmail客户端是支持DirectPush技术的邮件客户端。Pushmail的主要用途是为用户提供安全受控的即时邮件推送服务。Pushmail客户端通过移动VPN或内置的应用层隧道与企业移动接入网络建立加密隧道，在用户查看企业邮箱时提供安全通信防护，附件浏览和下载控制。

图35 邮件安全策略

针对于智能终端和Pad设备的操作特点，Pushmail客户端提供以下特性，为用户提供优质体验：

- 邮件协议
  - 支持SMTP、POP/POP3、IMAP4以及EWS、SOAP、HTTP和HTTPS等丰富的邮件协议。
- 邮箱功能
  - 对于单个邮件支持创建，打开，发送，接收，转发，删除，回复，标记和移动、搜索、订阅管理等功能；
  - 通过邮件配置自动获取功能简化用户配置，特定情况下实现了零配置；
  - 支持在线模式下，本地邮件操作同步到服务器；
  - 支持邮件实时推送和通知，并支持同步策略和通知方式的配置。
- 离线邮箱
  - 支持离线登录进入邮箱；
  - 支持离线阅读本地邮件和附件、查看联系人、查看日历/约会/会议；
  - 支持离线撰写邮件/约会的草稿。
- 邮件传输加密
  - 传输加密方式支持全系列的SSL/TLS协议；
  - 支持客户端/SVN间传输加密；
  - 支持客户端/邮件服务器间传输加密。
- 邮件附件在线浏览
  - 支持Office、 PDF和文本文件浏览；
  - 支持压缩文件浏览；
  - 支持图片文件浏览；
  - 支持日历格式附件的自动解析。
- 邮件加密保存
  - Pushmail对邮件正文和附件都进行加密保存，缓存的邮件支持周期性清理。
- 邮件策略控制
  - 支持邮件附件的访问、转发策略控制；

- 支持邮件内容转发策略控制；
- 支持离线登录邮箱的权限策略控制。
- 提供邮箱界面的自动超时锁定。

■ 日历

- 支持约会/会议的查询，提醒，添加，删除、修改以及同步功能。

■ 联系人

- 支持个人联系人的查询，增加，删除和修改以及同步；
- 支持企业联系人的查询；
- 支持自动缓存最近使用联系人清单；
- 在邮件处理过程中支持各种丰富的联系人详细信息的联想；

■ 邮件系统的认证授权

- 支持邮件服务器的独立登录或单点登录。

■ 优化极简风格的界面

- 支持收件人折叠和邮件头折叠等界面改进。

3) 安全浏览器

图36 安全浏览器

安全浏览器是基于浏览器内核的华为自研浏览器。安全浏览器的主要用途是为用户提供安全浏览企业Intranet网站内容的能力。

安全浏览器底层通过VPN或内置应用层隧道与企业移动接入网络建立加密隧道，在用户浏览企业Intranet网站时提供安全通信防护。

针对智能终端、平板等BYOD设备的屏幕尺寸和操作特点，安全浏览器提供以下功能，为用户提供优质体验。

- **BYOD设备WEB内容适配/页面重排**：安全浏览器根据终端屏幕尺寸，自动对下载的Web页面进行内容块重排处理，在BYOD设备上提供上下滑动浏览页面的功能；

- **流量精简**：根据流量精简策略，对于Web页面中的资源进行过滤和内容优化，精简流量；
- **个性化的书签授权和UI自定义**：支持用户自定义登录页面、资源书签（管理员授权/用户自定义）和应用框架；
- **数据保护**：支持离线资源、密码、下载的文件、访问历史、Cookies和临时文件的在线加解密能力；在退出浏览器时，可按照策略自动清理缓存和配置；
- **文档沙箱浏览**：支持Office、 PDF、文本、图片、压缩文件等办公所需文档格式的在线或离线安全浏览，实现公司数据与个人数据的隔离。
- **访问行为管控**：基于URL黑白名单的管控，并根据策略限制文件上传、下载和保存等行为；
- **支持权限提升**：为浏览器提供可信的权限提升，按照业务需求，通过调用摄像头、录音、放音、短信、电话、文件夹等，实现丰富的移动办公业务功能。

7.3.5 业务应用发布方案

业务应用发布分为应用集成、应用打包、应用发布、应用安装、应用使用和应用管理六大部分，内容和流程如下图所示：

1) **应用集成**：业务应用程序在基于安全SDK开发，集成。
2) **应用打包**：应用程序开发好后与相关的证书、配置文件一起打包为业务应用。
3) **应用发布**：业务应用发布到企业应用商店，供用户下载。
4) **应用安装**：初次使用用户先安装AnyOffice平台，然后注册、认证，最后在平台中通过商店链接下载应用程序，并安装。
5) **应用使用**：用户使用应用程序账号登录，合法认证后，办理相关的业务。
6) **应用管理**：后台管理员，远程管理用户、设备、审批等等信息。

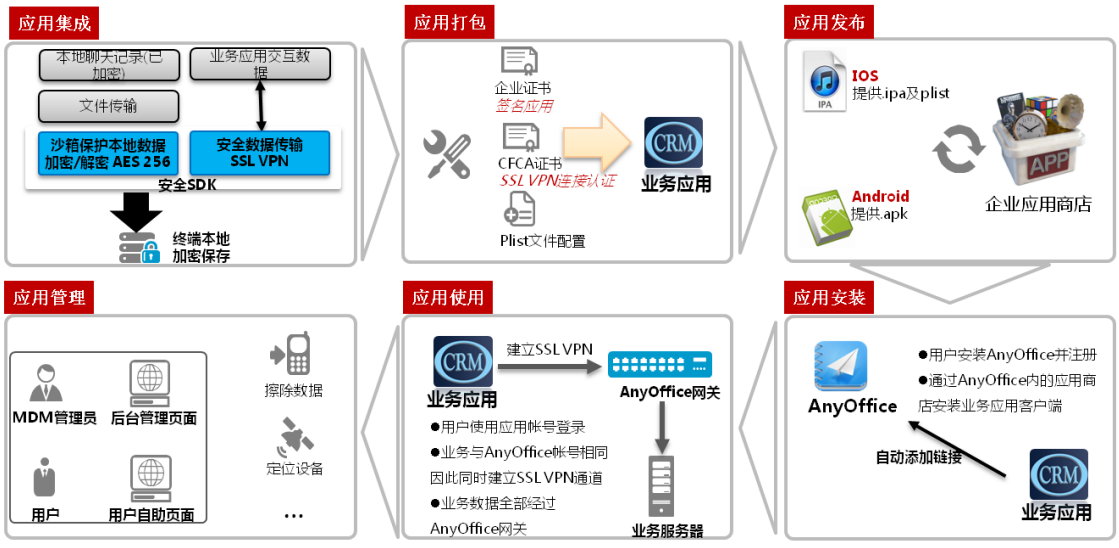

图37 业务应用发布

7.3.5.1 业务集成发布流程（开发者视角）

业务应用集成开发分为四个步骤：评估、应用集成、准备、发布，如下图：

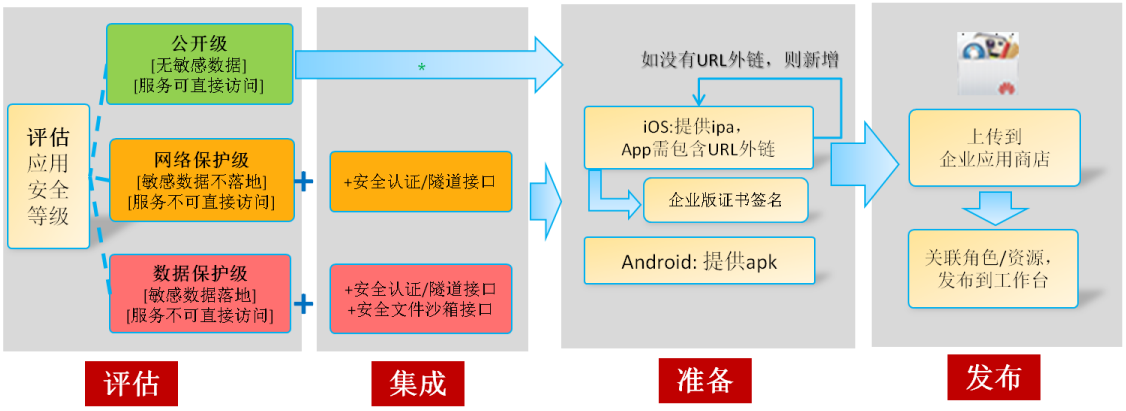

图38 业务应用集成开发

1) 评估：

在开发应用程序之前，先评估开发的应用的安全等级；一般分为三个级别：

- **公开级**，无敏感数据，服务可直接访问；比如：理财产品展示等；此级别无需进行数据的网络传输加密和本地加密。
- **网络保护级**，敏感数据不落地，服务不可直接访问；比如：大厅填单等；此级别只需进行数据的网络传输加密，保证传输安全。
- **数据保护级**，敏感数据落地，服务不可直接访问；比如：信用开业务等；此级别需要有本地数据做安全加密保护和网络传输加密保护。

评估完成应用的安全等级，我们根据需求，使用相关的安全策略，与AnyOffice平台SDK集成。

2) 集成：

应用完成评估后，根据三个级别完成相应的集成开发，下面就根据三个级别分别阐述具体的集成过程。

公开级：

- 在业务应用和移动数据器之间直接通过明文传输进行业务交互。

网络安全级：

- 业务应用集成安全SDK，基于用户名+密码或者CA证书认证建立SSL VPN通道，用于业务权限认证和数据传输。
- 业务应用通过SSL VPN把用户和密码传到后台服务器，后台应用服务器到认证服务进行认证并下发权限。
- 应用的业务流量均通过基于L4层的SSL VPN隧道与应用服务器进行业务交互。

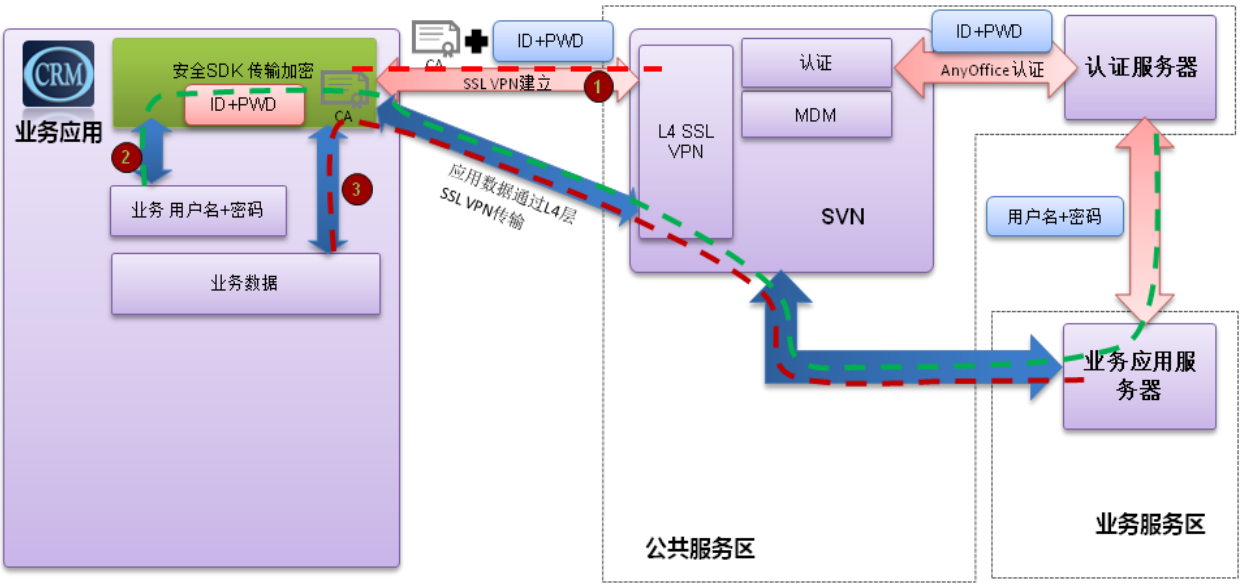

图39 网络安全级交互

数据安全级：

- 业务应用集成安全SDK，基于用户名+密码或者CA证书认证建立SSL VPN通道，用于业务权限认证和数据传输。
- 业务应用通过SSL VPN把用户和密码传到后台服务器，后台应用服务器到认证服务进行认证并下发权限。
- 应用的业务流量均通过基于L4层的SSL VPN隧道与应用服务器进行业务交互。
- 业务应用程序中有需要在本地落地的数据，通过安全SDK对数据进行加密存储。

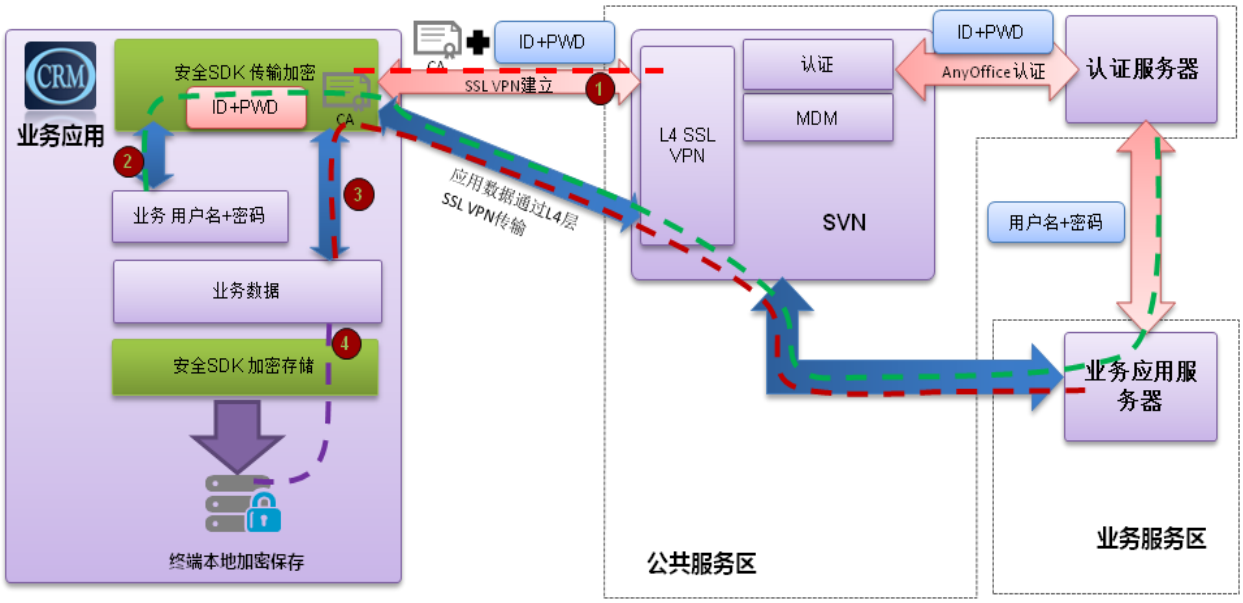

图40 数据安全级

3) 准备：

- 对于IOS需要通过企业版证书对应用进行签名，得到企业版应用安装包（ipa）格式；Andriod系统直接把应用程序打包生产apk格式。

4) 发布：

- 管理员上载企业版应用信息和安装包到应用商店，并设置下载权限。

7.3.5.2 业务应用工作流程（客户经理视角）

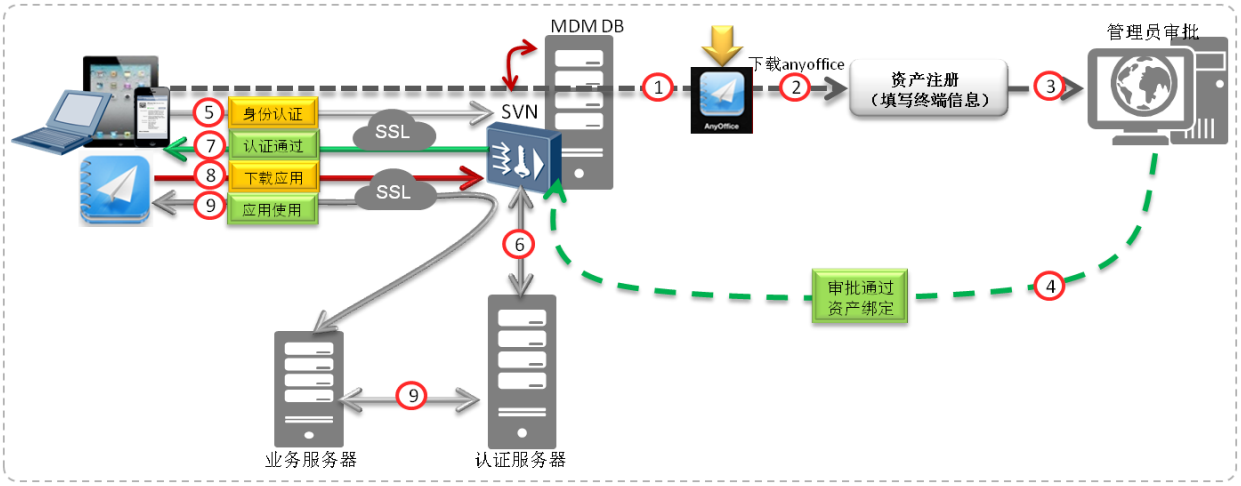

图41 业务应用工作流程

1) 使用者拿到初始的PAD，首先通过3G专线连接到内部网络，通过浏览器输入URL链接下载AnyOffice应用程序，并安装。

2) 根据AnyOffice的提示填写资产和个人相关信息，进行终端信息和个人信息绑定。

3) PAD资产和个人信息提交到管理员这边，资产管理员核实相关信息进行审批。

4) 资产管理员审批成功，并在后台完成个人相关证书、资产信息、用户的关联。

5) AnyOffice向SVN建立SSL连接，并将用户名密码传递给SVN进行认证。

6) SVN收到认证请求后，作为认证服务器的客户端，将用户信息发送到认证服务器验证。

7) 认证服务器验证用户信息并返回结果，SVN收到的认证响应，允许用户登录，并同时下发应用策略。

8) Anyoffice基于SVN的安全隧道访问应用商店，并从商店中下载应用，SVN从MDM DB

9) 服务器中获取应用，通过SSL隧道发送给移动终端。

10) 用户通过AnyOffice中应用链接打开应用程序，并向SVN建立SSL连接；然后，应用终端向业务服务器发起认证请求，业务服务器把相关的用户信息提交到认证服务器完成认证，登录成功后，进行应用访问或业务提交。

7.4 典型配置

见证开户一体机典型配置：

产品	型号	基本规格
华为 MediaPad 10 FHD	S10-101u	尺寸：10.1 寸 材质：镁铝合金 厚度：8.8mm 分辨率：1920*1200 操作系统：Android4.0 重量：580g 摄像头像素：前置 130 万，后置 800 万 3G 版本 RAM:1GB 内存:8GB 处理器：海思 K3V2 Cortex-A9 四核 1.2GHz
华为 MediaPad 10 Link	S10-201u	尺寸：10.1 寸（257.4mm*175.9mm*9.9mm） 材质：镁铝合金 厚度：9.9mm 分辨率：1280*800 操作系统：Android4.0 重量：640g 摄像头像素：前置 30 万，后置 320 万 3G 版 RAM:1G,内存:8GB 海思 K3V2 平台四核 1.2GHz
身份证&电池背夹	JR-3000	定制背充式二代身份证读卡器背夹

AnyOffice典型配置：

产品	描述	数量	备注
SSL 网关	SVN2230-M（500 人以下）	2	可与接入区 SVN 共用
	SVN2260-M（1000 人以下）	2	
	SVN5530-M（5000 人以下）	2	
MDM 服务器	IBMX3650M4（1.2TB）、Windows Server 2008、SQL Server 2008	2	可支持 20000 用户，双机可靠
软件 License	SSL VPN 并发用户数、虚拟网关、虚拟桌面、安全邮件等	—	根据实际需求选择

7.5 方案亮点

- **高效的开户终端：**MediaPAD一体化背夹，便携、插拔式设计，两倍续航，拍照补光，LOGO/UI可定制，实现高效开户；
- **统一用户体验**：移动终端符合IOS、Android等用户的使习惯，多平台体验一致；
- **业务零间断**：VPN网关对终端与虚拟IP的连接定时扫描，一旦连接中断，链路快速自动重连，重连时间可控制在4秒内；
- **公私数据隔离**：使用业界领先的沙箱技术，实现个人和企业的数据、应用的安全隔离，轻松解决个人和企业数据、应用混合带来的数据泄密和病毒感染等风险；

- **多维度防泄露**：MDM提供数据权限管理、外接端口管控，防截屏等数据管理功能，防止数据无意泄露；提供数据远程擦除、设备远程锁定/解锁以及GPS定位功能，确保在设备遗失、被盗窃等情况下数据万无一失；
- **应用更安全**：AnyOffice提供安全SDK功能,为客户定制自己的移动应用提供应用级数据加密接口，支持iOS，Android等主流操作系统，使移动应用更安全；

8 桌面云方案

8.1 总体方案介绍

轻型营业部部署桌面云可支持营业部的批量建设和业务快速投放，支持证券公司实现快速抢占市场和价值客户的目的。由于轻型营业部多通过互联网接入总部或区域中心，而互联网的网络QOS难以保证，可能存在时延和抖动，影响桌面云的体验。因而建议客户根据实际测试情况部署桌面云，以达到良好的桌面体验。

以下是桌面云的总体方案，终端接入利用营业部一体机和数据中心接入区之间建立的VPN通道：

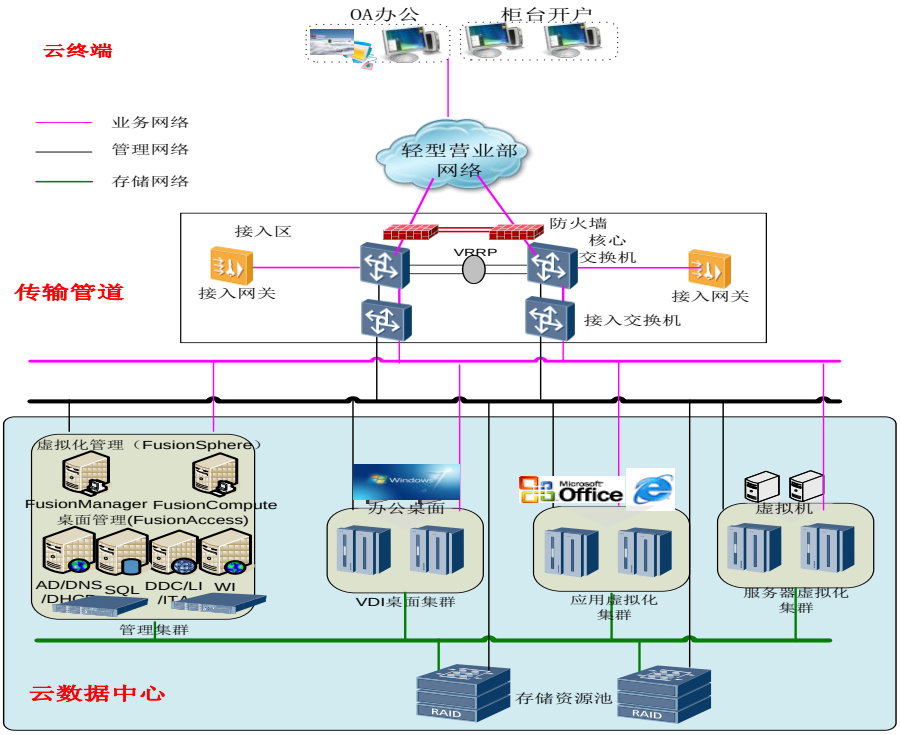

图42 桌面云总体方案

本项目为了实现高安全、高可靠、高性能、易远程集中运维、平滑扩容的目标，采用业界主流成熟的虚拟化技术，实现虚拟桌面、应用发布、服务器虚拟化等要求。本项目方案主要以下方面考虑：

资源池设计：根据本项目的需求，服务器上安装华为的虚拟化软件，将服务器池化。池化后VDI桌面、应用虚拟化、服务器虚拟化的服务器分别组成集群。池化后服务器上运行虚拟机便于管理、监控。虚拟机在集群里可以实现定制策略迁移、手动热迁移、故障热迁移。资源池的设计具有高可靠、平滑扩容特性。

桌面管理：华为虚拟桌面管理软件FusionAccess，提供高性能且可靠的桌面投送。

虚拟化管理：为了便于硬件设备（服务器、存储、交换机）、虚拟资源的集中管理，采用华为的虚拟化管理软件FusionSphere。FusionSphere采用B/S架构，可以远程统一管理本项目中VDI桌面、应用虚拟化、服务器虚拟化三个资源池。FusionSphere可管理、监控硬件资源、虚拟资源；支持虚拟机的快速部署、定制化策略调度。

- **计算资源池**

计算资源池为用户提供CPU、内存计算资源。在服务器上安装华为的虚拟化软件，可以在一台服务器上虚拟出多个台虚拟机，提供弹性规格的虚拟桌面。这几个资源池归属同一朵桌面云管理系统。

- **存储资源**

存储资源主要为虚拟桌面提供系统空间和数据空间、还有桌面云管理系统所需要的空间。这些存储都在主用存储上。主存储根据数据类型的不同，划分不同的数据LUN。这里的数据类型主要包括 管理数据、Windows系统数据、用户数据。

8.2 营业部日常办公

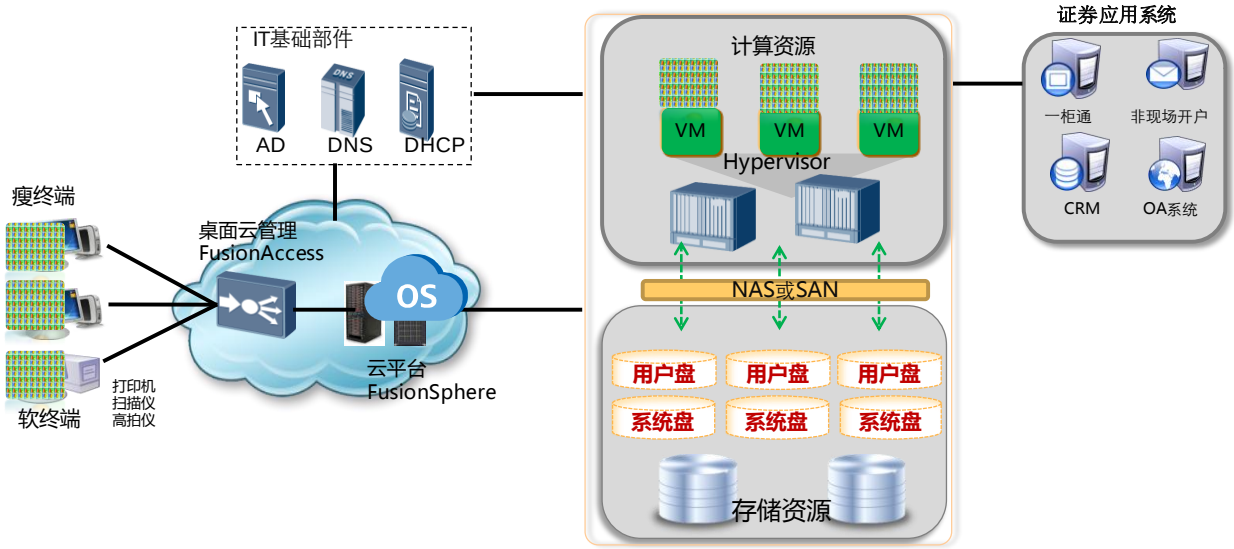

图43 营业部办公应用场景

营业部桌面云的特点和差异：

- ✧ 前台终端：为操作型岗位，大部分时间使用营业系统应用进行业务处理，有简单的数据存储、交换需求；
- ✧ 管理座席：为知识型岗位，除营业系统管理应用外，还有Office办公软件、多媒体播放有一定需求。
- ✧ 所需外设多：营业部终端需支持各种打印机、扫描仪外，还需支持SIM卡读写器、密码小键盘、摄像头、手写板等外设。

证券营业部桌面云解决方案针对营业部分布地域广泛，网络连接质量差异大的特点，改进了桌面云系统的调度和连接优化配置，可以有效的克服网络闪断，网络速率抖动等恶劣条件，保证证券营业部系

统的高质量服务。

华为桌面云可以支持营业部常见的日常办公软件，比如可使用office，IE，Adobe Reader等日常办公软件，浏览图片，播放flash，音频，视频流畅。

华为桌面云支持证券经纪业务系统，如一柜通。针对证券业务系统采用的B/S架构，华为桌面云虚拟桌面IE浏览器兼容所需插件（密码软键盘、图片处理等插件）的安装；TC兼容各类常用外设，可辅助完成业务流程需要的身份验证、采集影像、证件扫描等操作。

华为桌面云支持与企业已有的IT系统对接，充分利用已有的IT应用。比如利用已有的AD系统进行桌面云用户鉴权；在桌面云上使用已有的IT工作流；通过DHCP给虚拟桌面分配IP地址；通过企业的DNS来进行桌面云的域名解析等。

华为营业部桌面云解决方案的优势

营业部桌面云解决方案有如下优点：

- 利旧原有IT外设：无需采购新的IT外设，兼容常见接口外设，并可对于外设驱动统一部署和管理，保证即插即用的客户体验。
- 软件快速安装部署：运营软件通过云平台集中推送，做到大规模快速软件安装部署，便于证券公司统一新业务上线。
- 支持客户自助系统：支持客户自助系统在桌面云的部署，可免认证使用证券公司为客户提供的系统，办理许可的相关业务。

8.3 瘦终端外设接入

证券营业部桌面云解决方案提供即插即用的外设终端接入方案，并通过预置的具备广泛兼容性的驱动插件支持常见的串口、并口、USB口外设；支持多种类型的打印机、扫描仪、读卡器、评价器。极大的降低了企业客户部署的难度。

TC外设接口如下：

- 网口：1个（百兆）
- 并口：1个
- 串口：4个
- USB2.0接口：6个
- 键盘/鼠标：PS/2

支持如下外设接入：

- 打印机（USB、串口、并口及网络接入方式），例如：HP LaserJet P3015；四通OKI MICROLINE 6300FC。
- 身份证阅读器（USB方式接入），例如：CP IDMR02/TG。
- 手写板（USB方式接入），例如：汉王行业签字板ESP560，WACOM 签名数位板STU-500B。
- 华为USB KEY。

✧ 高拍仪，例如：多易拍 DE-300，多易拍AF526。

✧ 摄像头，例如：台电的TL-T838-NDE2S，Microsoft VX-1000，Logitech C310。

8.4 桌面安全

桌面接收、处理、存储应用系统的数据，这些数据是券商的关键信息资产，需要从终端设备接入、文档管理、数据传输及虚拟桌面系统几个层次全面保证信息资产的安全性。

用户名+域密码认证

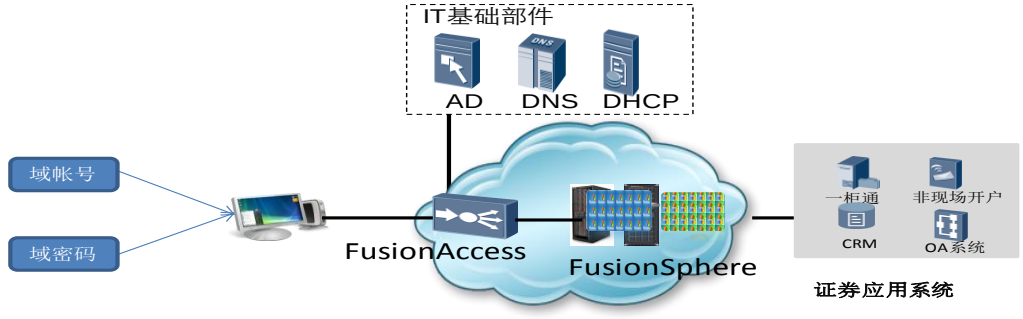

图44 安全接入认证示意图

华为的虚拟桌面可以根据AD域帐号+域密码方式进行认证，用户输入AD域帐号和密码后，AD服务器进行认证，认证成功后即可进入用户虚拟桌面。在虚拟机里可以锁屏，输入域密码解锁。

双因子认证

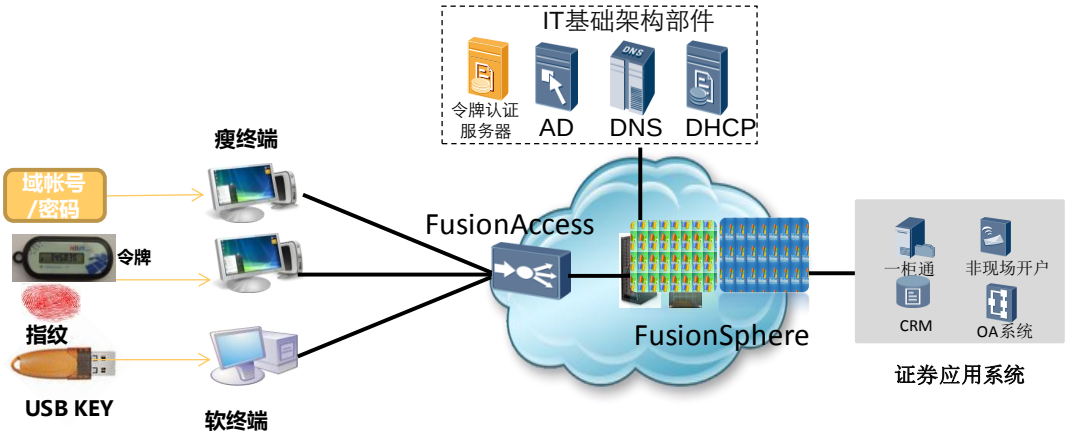

图45 双因子认证

桌面云支持令牌、指纹、USB KEY等双因子认证。其中令牌认证使用动态密码技术，每隔一段时间，令牌上的密码就会变化，避免了静态密码被摄像、偷窥的风险。令牌认证再结合AD域密码就可以实现双因子认证，增强安全性。令牌认证需要在桌面云系统增加令牌认证服务器。用户认证时需要输入用户域帐号、域密码、动态密码。

USB端口管控

FusionCloud具有丰富的外设映射策略，可以提供USB设备管理，能够区分USB鼠标/键盘和USB存储设备，针对USB存储设备，提供允许/禁止/只读控制能力。同时外设映射策略可以基于AD用户账号、

OU组进行配置。

瘦终端绑定虚拟机认证

为了进一步保证合法用户登录虚拟机，满足追溯到人的安全要求，可以限制用户只能在指定的地点上登录虚拟机。桌面云管理员可以在ITA Portal将瘦终端的MAC与用户的域帐号绑定。如果用户更换办公位、或更换瘦终端，需要通知管理员在ITA Portal重新更新MAC地址绑定关系。

数据加密方案

TC的认证接入采用HTTPS加密传输；桌面访问采用传输加密（ICA over SSL）等手段，保证业务运行和维护安全。

8.5 可靠性

桌面云平台通过在系统的各个层面采用相应的可靠性技术来保障业务提供的可用性，包括：

硬件可靠性

- 虚拟桌面系统中的硬件可靠性包括内存、硬盘、电源等多个层面的内容，提供BIOS内存自检和ECC纠错技术；
- 支持硬盘热插拔和RAID功能，提供硬盘在线故障检测和预警；
- 支持电源1+1冗余和热插拔；

网络路径全冗余

- 核心层交换设备通过使用交换机集群技术，保证对外与防火墙/NAT和对内汇聚交换机连接的冗余。
- 虚拟网络层通过采用多网卡绑定等技术避免单个网卡故障引发的业务中断。

管理节点冗余

虚拟桌面的管理软件均采用1+1备份的方式运行，当一个管理节点的软件出现故障的时候，系统自动切换到备用节点，保证整个系统不间断运行。

存储多路径

虚拟桌面系统中的每个计算节点与存储集群之间将至少会配置两个完全冗余的路径，从而提供卷的多路径访问功能，多条路径间的故障切换由软件自动提供，从而避免单点故障带来的存储访问问题。

存储数据的冗余备份

虚拟桌面的存储数据采用多种备份机制机制，以保证存储数据不丢失。当采用IP SAN作为存储设备时，在IP SAN高可靠性的基础之上，再提供2块热备盘做冗余备份，保证数据不丢失。

故障检测

华为虚拟桌面系统提供了一个故障信息收集和存储集群节点可用性度量的功能。通过在每个被监控的节点上运行探针程序，华为虚拟桌面系统可以收集它运行的机器的核心指标如CPU使用情况、基础网络流量和内存数据等，检测到诸如进程崩溃、管理和存储链路异常，节点宕机、系统资源过载等各种异常，使系统具备完善的故障检测能力。

虚拟机热迁移

提供虚拟机的自动迁移和手动迁移方案，当前计算节点出现故障或者计算节点负载过高时，可以通过虚拟机迁移把虚拟机迁移到正常的计算节点或者负载相对较低的计算节点上，保证虚拟桌面的不间断访问。

8.6 桌面云应用容灾

8.6.1 GSLB 业务冗余容灾

适用场景

GSLB业务冗余容灾方案适用于不需要用户数据备份、只需要业务容灾的场景，例如营业厅柜台、客服坐席、呼叫中心等场景。

方案组网及实现

GSLB业务冗余容灾是针对关键业务用户，在两个数据中心内分别为其分配桌面资源，由GSLB负责数据中心的选择，从而使得用户可以接入到不同数据中心桌面；GSLB将根据数据中心的运行状态以及用户所在的地址位置执行选择策略，从而实现用户接入桌面的自动负载均衡和容灾切换。方案组网如下图所示。

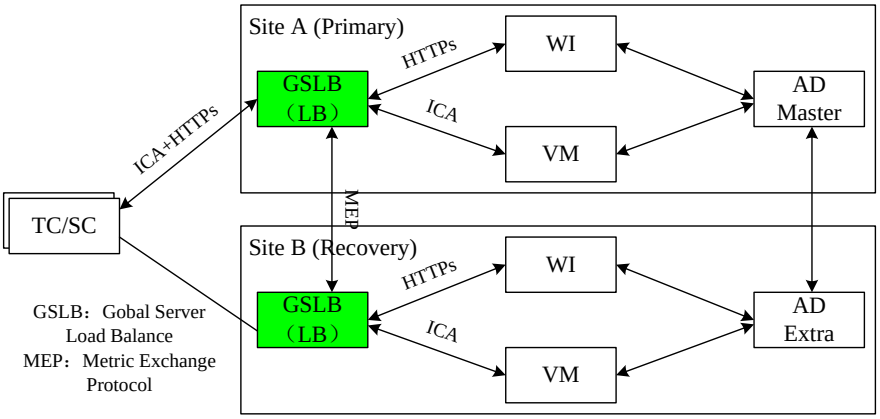

图46 GSLB 业务冗余容灾方案

业务冗余容灾流程如下：

（1）TC上设定默认的桌面业务入口域名，其主用、备用DNS地址分别为两个数据中心的GSLB IP地址，由GSLB负责域名解析。

（2）GSLB负责监控数据中心运行状态，正常情况下该域名将被解析至该用户主用数据中心入口IP地址，使得用户的访问请求路由至其主用桌面。

（3）GSLB上可以设置DNS解析策略，根据TC的源IP 进行DNS智能解析，如对于IP段为A的用户请求，其主用站点地址为A ，备用站点为B ；而对于IP 段为B的用户请求，其主用站点为B，备用站点为A，从而实现两个数据中心之间的负载均衡。

（4）为保证切换对用户无感知，两个数据中心VM用户名和密码完全相同。因此，建议采用统一

的AD域控制器，当用户修改密码时各个AD域控制器可以进行数据同步，其中AD域控制器布置在生产局，AD额外域控制器布置在容灾局，以保证在生产局AD域控制器故障时，容灾站点仍然可以接入业务。

（5）为了充分利用VM的利用率，一般采用POOL方式桌面组，用户与VM之间没有绑定关系。

灾难恢复流程如下：

（1）当TC检测到主用DNS（对应生产GSLB）故障后，将自动将DNS请求发送给备用DNS（对应容灾GSLB），并由备用DNS解析为用户备用桌面所在的入口IP地址，用户即可以使用备用数据中心桌面继续业务。

（2）在故障恢复后新的DNS请求将重新发送给主用DNS（对应生产GSLB），并由主用DNS将DNS请求解析为主用站点地址，从而恢复用户对于原主用桌面的使用。

8.6.2 GSLB+NAS 远程复制容灾

适用场景

GSLB+NAS远程复制容灾方案适用于既需要保证数据不丢失，又需要尽快恢复业务。例如OA办公，研发，应用虚拟化等场景。

方案组网及实现

对于办公桌面等业务可以直接使用NAS共享目录的方式，将NAS作为数据存储盘使用。在NAS服务器上为每个VM的用户分配帐号、密码、目录、硬盘配额（支持域鉴权），采用多NAS引擎时还可指定不同NAS IP地址；VM启动后将“NAS IP地址+共享目录”映射为网络硬盘进行访问。方案组网如下图所示。

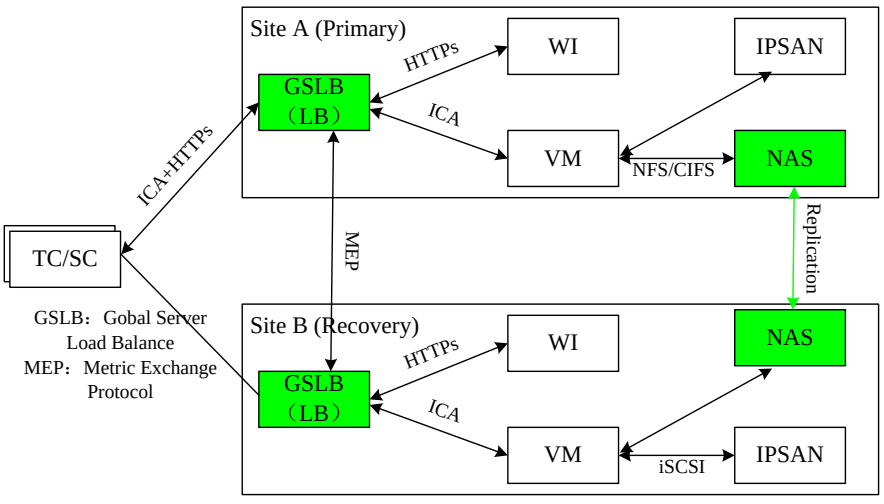

图47 GSLB+NAS 远程复制容灾方案

（1）TC上设定默认的桌面业务入口域名，其主用、备用DNS地址分别为两个数据中心的GSLB IP地址，由GSLB负责域名解析。正常情况用户的访问请求路由至其主用桌面VM。

（2）当TC检测到主用DNS（对应生产GSLB）故障后，将自动将DNS请求发送给备用DNS（对应容灾GSLB），并由备用DNS解析为用户备用桌面所在的入口IP地址，用户即可以使用备用数据中心桌面继续业务。

（3）对于办公桌面等业务可以直接使用NAS共享目录的方式，将NAS网络硬盘作为主存储，保存用户关键数据。本地NAS启用远程复制功能，将数据复制到异地容灾NAS。

（4）当生产中心发生灾难时，管理员需要将异地容灾NAS提升为主用NAS；当TC通过GSLB登录到备用VM时，备用VM启动后自动挂载容灾NAS上的共享目录作为网络硬盘使用。

8.7 运维管理

8.7.1 运维系统架构

华为桌面云运维服务管理，基于B/S架构，提供远程集中运维管理，全中文界面。华为运维管理参考ITIL标准，基于统一维护，可运营、可管理的理念，设计了符合虚拟化产品特点，易运维的管理系统。支持友好的WebUI维护界面，统一管理所有硬件资源与虚拟化资源，VDI桌面，提供基于定制化策略的自动化运维系统。

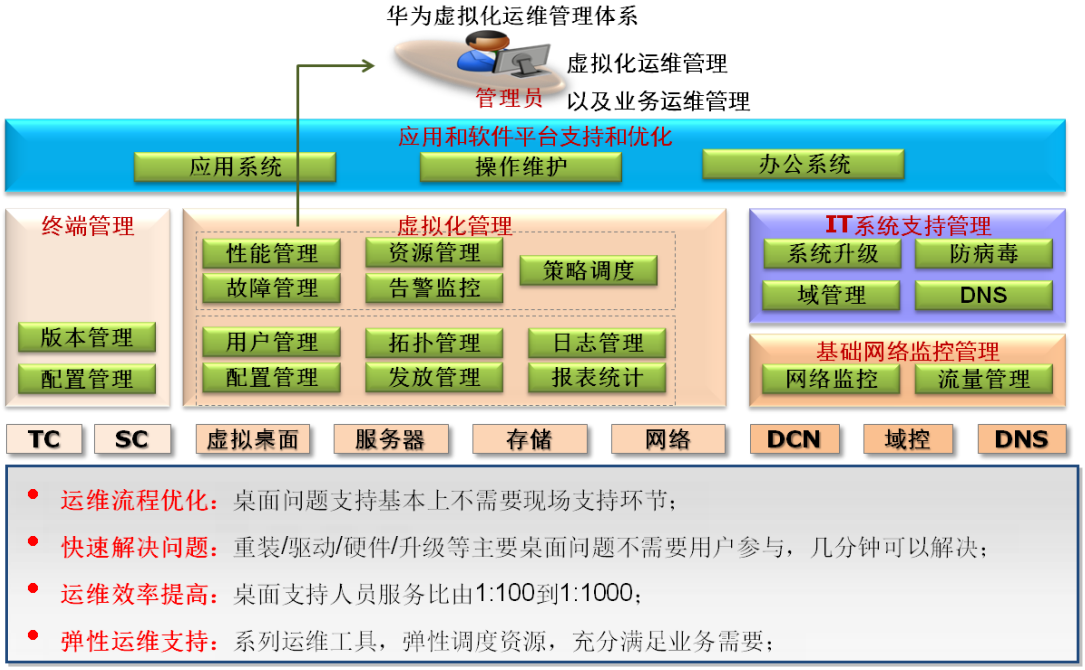

图48 运维系统架构

桌面云系统运维和维护管理主要由“FusionSphere运维管理系统”提供，“桌面云业务维护系统”提供部分辅助功能。运维系统基于Web架构，用户可通过IE、Firefox浏览器访问，无需安装本地客户端。

华为FusionAccess的统一资源发放WEB PORTAL，业务发放更灵活、更高效。强大的OM运维能力，支持用户分权分域管理，安全性高。管理员可通过Portal快速地进行业务发放、桌面管理、模板管理、权限管理、资源管理、监控管理、告警管理、拓扑管理、日志管理、任务管理、统计管理。

管理员登录支持SSL、数据加密、用户密码加密保存，确保用户数据安全。

桌面管理支持虚拟桌面生命周期管理、快照、使用快照创建虚拟机和恢复虚拟机。为用户数据提供备份功能。

拓扑管理能让管理员非常直观地看到系统的部署情况、运行情况。

告警管理支持告警转E-Mail、短信的即时通知，使用户及时了解系统。

日志管理支持操作日志、运行日志记录，便于审计和故障处理。FusionAccess支持集中日志，用户桌面日志、管理日志进行集中收集和分析；

统计管理支持灵活配置、报表统计分析。

桌面云系统支持软件HA，高可靠性，减少故障对系统和业务的影响。

支持系统配置自动备份，避免系统数据丢失。

支持动态节能，例如：虚拟机长时间未用则自动休眠、用户再次使用时自动恢复虚拟机使用；虚拟机自动调度包括定时迁移关闭启动虚拟机、将虚拟机集中运行在某些服务器并下电其他服务器。

8.7.2 虚拟桌面管理

虚拟桌面运营管理由FusionAccess提供，该系统基于Web架构，用户可通过IE、Firefox浏览器访问，无需安装本地客户端。并且支持管理员分级分域管理。

虚拟机发放

管理员可以Portal发放裸虚拟机，完整复制，链接克隆虚拟机。

支持虚拟机的单个发放或批量发放。批量发放可以发放给一批人，批量创建后的虚拟机有系统盘、用户盘，关联到AD域帐号。

虚拟机发放给用户即绑定用户，只有绑定用户才能访问虚拟机。支持发放时自动绑定、手动绑定。

一个虚拟机可以绑定给一个用户，也可以绑定给多个用户。多个虚拟机组成的资源池，可以共享绑定给多个用户。适用于多种用户场景，例如个人办公虚拟机则一一绑定，公用虚拟机则一对多或多对多绑定。

桌面管理应用于用户进行虚拟桌面的发放和维护场景。用户通过桌面管理主要完成以下三大维护管理模块：

虚拟机管理

该模块可完成虚拟机的启动/唤醒、重启、休眠、关闭、删除、解分配、以及高级功能（强制重启、强制关闭、追加用户、删除用户、虚拟机配置调整、链接克隆虚拟机一键还原、安全删除）等操作。

修改虚拟机可以修改虚拟机的业务类型、CPU、内存以及描述。

一键式还原针对链接克隆虚拟机，强制还原虚拟桌面系统到初始状态。

安全删除功能把虚拟机删除后，但磁盘空间不会立即可用，会在后台进行磁盘空间的清“0”处理，磁盘空间清“0”后会自动加入可用的存储资源池。

虚拟机模板和镜像管理

支持虚拟机模板的创建、修改、删除、查看。虚拟机模板参数包括：虚拟机规格（CPU、内存、系统磁盘大小）、镜像、虚拟机QoS（是否HA、服务质量级别）等。

虚拟机组管理

每个虚拟机都必须归属于某个虚拟机组。该模块可完成虚拟机组的创建、编辑、删除、添加虚拟机、更新链接克隆组软件以及一键式还原。

桌面组管理

每个虚拟桌面都必须归属于某个桌面组，该模块可完成桌面组的创建、编辑、删除、分配虚拟机、批量分配虚拟机以及一键式还原。

8.7.3 软件管理

软件系统包括：云平台系统软件、桌面接入系统软件、用户虚拟机软件。为了方便客户管理软件，软件系统具有如下特点：

软件预安装和预置

发货前，桌面接入系统及操作系统补丁，已预置在基础服务器镜像中，在现场可直接快速创建虚拟机。用户虚拟机支持将用户应用软件预置到虚拟机模板中，使用虚拟机模板安装虚拟机。

软件自动化批量安装

云平台软件：支持统一安装界面，一次性导入所有服务器的信息，多节点同时加载安装，安装效率高。

桌面接入系统软件：支持统一安装界面，便于安装管理。

用户虚拟机软件：通过虚拟机模板方式，创建虚拟机并安装应用软件，且支持批量创建虚拟机，大大减少了用户操作和操作难度。

升级、打补丁及回退自动化

云平台软件支持升级、打补丁有工具支撑，实现了自动化健康检查、分发软件、升级/打补丁、校验、回退。且支持静默升级，即升级/打补丁不影响业务。

用户虚拟机软件管理集中化

支持使用工具快速将用户数据从原来的物理机迁移到虚拟机、虚拟机间数据迁移。

用户虚拟机操作系统，通过补丁服务器打补丁，方便安全。

通过AD域控管理用户虚拟机的应用软件，具有准入控制、安全策略管理、员工行为管理、软件分发功能。

8.7.4 资源管理

FusionManager云管理平台，通过对各种物理资源、虚拟化资源数据统一建模，将资源以用户可见的资源池形式提供给上层应用。

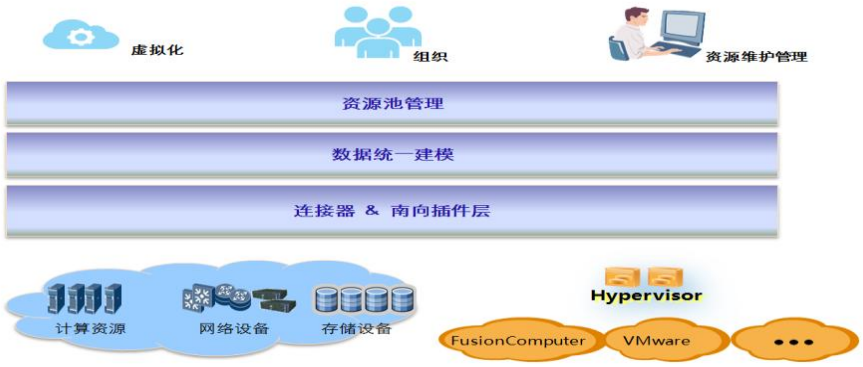

图49 统一资源管理模型

统一资源管理，支持发现其管辖范围内的物理设备（包括机框、服务器、存储设备、交换机）以及它们的组网关系。支持将这些物理设备进行池化管理，提供给应用管理模块使用。对于虚拟化一体机场景支持自动发现物理设备，基础设施虚拟化场景需要手工导入物理设备，对服务器、存储设备和交换机进行集中管理，对物理资源进行池化管理，给上层的业务发放屏蔽物理设备的差异。

虚拟化资源管理可以统一管理不同系统提供的不同的虚拟资源，包括虚拟机资源、虚拟网络资源、虚拟存储资源的管理等。

通过资源池管理，提高基础设施资源的利用率和灵活性，提供统一的虚拟化资源管理能力，对上层应用发放屏蔽差异；实现虚拟资源集中管理提升管理效率，降低运维成本。

采用南向插件机制，使FusionManager可以快速、便捷、可定制的实现不同硬件和虚拟化系统的对接。

- **物理资源管理**

对于华为自研的物理设备可自动发现；第三方厂家设备支持单条设备接入或批量设备接入。

服务器资源管理能够发现服务器的配置信息，可以实现服务器的监控，监控信息包括CPU占用率，内存占用率，网络流出、流入，磁盘I/O写入、读出，可以按周、月、年及自定义时段查询性能监控结果。服务器设备的维护能力：上电，下电，安全重启，安全下电，强制下电，进入维护模式，退出维护模式，一键式上电、下电所有服务器；

网络设备管理能够发现交换机的配置信息，显示交换机端口的连接状态，状态信息包括连接与否、发送、接收速率，发送、接收丢包率，发送、接收错误率。另外还可以对本系统的网络模式及网络配置进行管理。

存储设备管理能够发现存储设备，查看存储设备的配置信息，信息包括存储设备位置，产品型号，状态，管理IP地址，磁盘数量。可以查询存储设备的总容量和可用容量，以便用户知道是否要扩容存储设备。支持IP SAN、FC SAN、NAS、服务器本地存储。

资源集群管理，集群的创建、删除、扩容、减容，对集群进行性能监控，配置集群的资源调度策略，调度策略可以设置为手动和自动，实现虚拟机根据系统负荷在不同服务器上迁移。

- **虚拟资源管理**

虚拟化资源管理支持对计算虚拟化、网络虚拟化、存储虚拟化的管理。

虚拟机生命周期管理：业务管理员通过应用对虚拟机进行创建、销毁操作，对虚拟机的日常维护包括：启动、重启、迁移、关闭、修复、快照、虚拟机资源调整和监控；

虚拟化网络管理：虚拟网络管理负责管理系统的虚拟交换机及虚拟交换机分配的子网。虚拟网络对应的是DVS(分布式虚拟交换机)和PortGroup（端口组）。分布式虚拟交换机支持系统管理员对一至多台主机上的虚拟交换机的上行链路和虚拟端口进行配置与维护。对子网、VLAN和端口组的管理；可对端口组进行限速设置、上限带宽、优先级和DHCP隔离配置。

虚拟化存储管理：可以管理IP SAN、FusionStorage、FC SAN、NAS上的存储资源，以数据存储为单位分配给资源集群使用。数据存储是虚拟机卷所在的存储空间，其对应的物理概念是：SAN的存储资源池、FusionStorage的内部资源池。

可以向存储资源池中增加、删除数据存储，已经存在的数据存储可以进行扩容，支持多级存储。

8.7.5 智能调度管理

资源统一调度，支持设置集群资源的调度策略，根据管理员设置的调度策略。

根据应用场景，可以分为三种策略类型：组内自动伸缩策略、组间资源回收策略和时间计划策略。

组内自动伸缩策略

针对单独的应用而言，应用根据应用的当前负载动态的调整应用实际使用的资源，当一个应用资源负载较高时，自动添加虚拟机并且安装应用软件；当应用的资源负载很低时，自动释放相应的资源。

组间资源回收策略

当系统资源不足的情况下，系统可以根据组间设置的资源复用策略， 优先使优先级高的应用使用资源，使优先级低的应用释放资源，以供优先级高的应用使用。

时间计划策略

时间计划策略允许用户对于不同的应用实现资源的分时复用。用户可以设置计划策略，使得不同的应用分时段的使用系统资源，比如说白天让办公用户的虚拟机使用系统资源，到了晚间可以让一些公共的虚拟机占用资源。

节能降耗

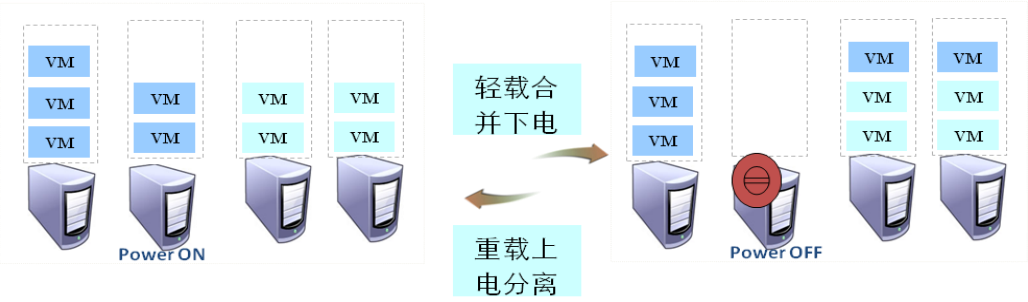

图50 智能节能调度策略

上图是的调整策略，可以实现节能降耗，实现轻载合并下电，重载分离上电。

✧ 系统负荷不大时，各VM占用CPU较低，部分VM关机了，可以将某些服务器上的虚拟机自动

迁移到其他节点，对这个服务器进行休眠或下电，实施系统节能策略。

- ✧ 系统重载时，再让部分物理机上电，并迁移VM到新物理机，保证用户感受。
- ✧ 系统需分析并选择合适的物理机上下电，减小迁移的VM数目。
- ✧ 为了快速响应，系统保证小部分物理机处理休眠态。

8.7.6 开放接口管理

支持通过ITA提供开放接口，客户通过调用接口实现自己的定制化需求，例如虚拟机管理、虚拟机磁盘管理、虚拟机关联、网络管理、告警、开户。

以下是基本的业务流程：

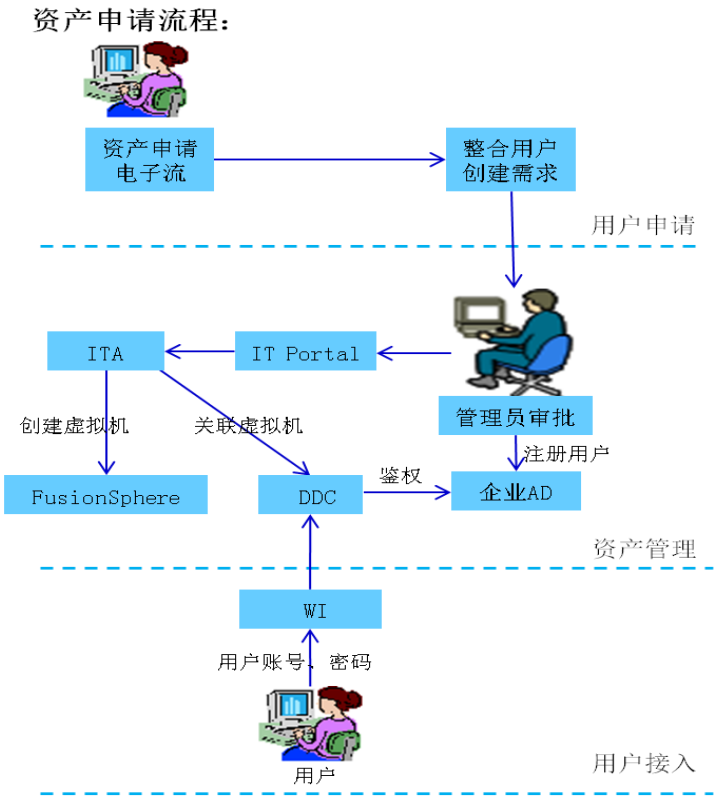

图51 自助请求流程

通过与ITA接口的对接，客户可以定制化开发自己的云计算IT资产管理系统，实现对员工域账号、虚拟桌面的完全对接，资产回收完全自动化。

以下是基本的业务流程：

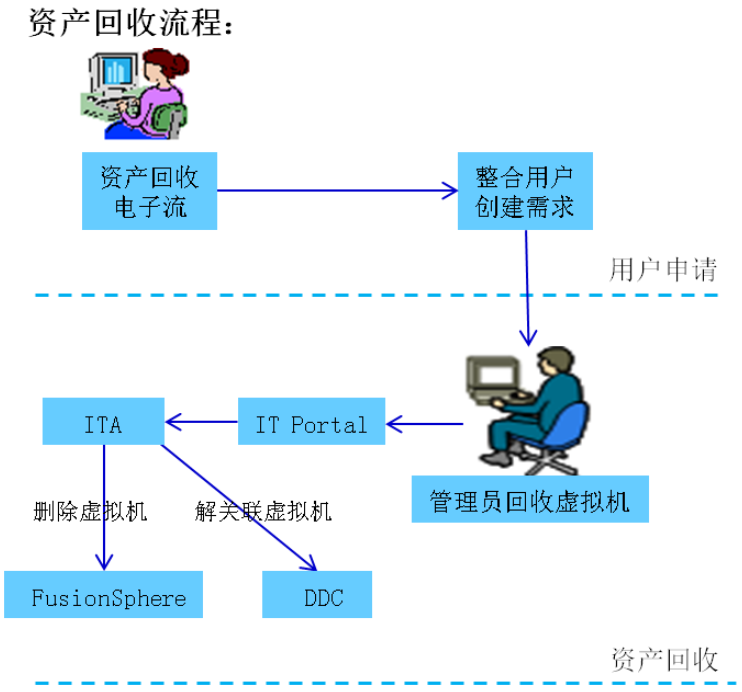

图52 资产回收流程

8.7.7 健康检查工具

健康检查工具是虚拟桌面平台为技术支持工程师和维护工程师提供的一套日常检查工具，并能输出各部件健康检查报告。方便技术支持工程师和维护工程师快速了解系统的健康状况。通过检查系统当前信息和运行状态，反映系统健康或亚健康状态，在开局、巡检、升级等维护场景中使用。

目前健康检查工具可以检测整机PDU健康状态，交换机健康状态，IPSAN健康状态：FusionSphere健康状态，FusionAccess健康状态。

图53 健康检查工具

8.7.8 TC 统一管理

华为的所有瘦终端都可通过统一的管理系统进行管理。它是一套基于Browser/Server 的管理系统，支持客户机的远程管理操作。同时，对于其他厂家的客户机，以及安装了Windows XP操作系统的PC，只要符合华为的通讯和界面规范，仍可实现联合管理。

桌面管理系统包含如下几个管理功能：

基本管理：

该模块是进行主要的客户机管理操作的模块，同时监测客户机运行状况和操作行为，对可能影响系统安全的问题进行警报处理。瘦客户端远程电源控制功能，包括瘦客户端的开机、关机、注销和远程唤醒等操作。

对瘦客户端各项性能进行监控，方便跟踪瘦客户端的运行状况，对突发状况进行及时的处理。同时，通过报表的分析统计，使用户对瘦客户端性能有全局的了解。

部署管理：

高级操作指南中的操作主要会涉及到这个模块，主要实现是部署、升级相关的操作。

公共管理：

通用的模块。包括对管理员权限的管理、管理员的操作日志和管理工具的基本配置。管理系统用户管理，提供用户建立、删除、审批新用户申请、角色管理、角色分配等通常的功能。

对管理员、瘦客户端的活动进行了记录和统计，以日志的形式进行存档和管理；使用户对系统操作情况有全局的了解。

作业管理：

对瘦客户端设备的管理操作进行调度，为一些繁琐重复长时间的管理操作建立作业，制定作业的执行策略，任务之间的依赖关系，帮助系统管理员完成无人值守的管理操作。

消息管理：

为管理员和瘦客户端用户提供一个实时消息交互通道，方便系统管理员与瘦客户端用户进行在线实时交流。

华为瘦终端统一管理软件有如下特色优势：

- 支持TC终端零配置，降低用户使用门槛

通过终端管理系统，统一能够对TC的配置信息进行下发，无需终端用户自行进行设置，降低用户使用门槛，也便于管理员统一管理。

- 支持TC自动升级和开机强制升级

能够对于已下电的TC，在其下次开机时会进行强制升级，保证所有的TC都能够升级到目标版本。

- TC用户的权限控制

TCM对TC的配置信息，可以根据用户类型不同，发放不同的权限让用户进行修改，这样可以区别对待不同的用户群体。

8.8 配置规划

8.8.1 带宽设计

营业部在城域网下部署，网络带宽受以下限制：

网点规模（并发用户）	每用户桌面带宽需求（平均）	网点网络接入带宽	建议接入方式
10	150-200kbps	1.5-2Mbps	专线/ADSL
20	150-200kbps	3-4Mbps	专线/ADSL
30	150-200kbps	4.5-6Mbps	专线/ADSL
50	150-200kbps	7.5-10Mbps	专线/ADSL

数据中心云平台对外带宽要求：为了让所有用户都能有较好的使用体验，除了考虑每个网点的网络接入方式及带宽外，还需要考虑数据中心云平台的对外接入带宽，要求该接入带宽是所有网点接入带宽需求总和。按每终端占用带宽150-200kbps计算，如虚拟桌面数量为400个，则总带宽要求为60-80Mbps。

8.8.2 推荐配置清单

说明：

不同种类的应用软件、应用软件使用方式（比如频繁度、同时使用人数）、以及虚拟机的配置等，都会影响使用体验。华为推荐的虚拟机配置密度，是典型应用场景下的的参考配置。为了获取更为准确的虚拟机密度配置，建议模拟实际应用环境，进行性能测试。

在实际使用过程中，如果出现由于应用负载变化等原因，导致用户体验变差情况。可以购买新主机、存储等资源进行扩容，降低虚拟机配置密度，来获取更良好的体验。

本期规划桌面配置规格与数量如下：

推荐场景	规格	数量
OA 办公	VCPU=2 MEM=2G 系统盘=40G，数据盘=80G 网络=共享 1G 系统盘 IOPS=17 数据盘 IOPS=3	500

- **服务器**

以证券公司研发办公应用场景为例，可选用重载100%并发比例。采用E6000 (2*E5-2630）刀片，虚拟机密度为达到37，计算服务器共需要14台，增加一台冗余服务器，则需要配置15台。

虚拟桌面管理（FusionAccess）与云管理(FusionSphere)服务器需要两台服务器，一共需要17台服务器。

每服务器内存条数=(虚拟机密度*虚拟内存+8G（底层虚拟化的消耗）)/内存条大小=*（37*4+8）/8=20根*。

备注：虚拟机密度的三种典型性能应用场景的说明，客户可根据实现情况选用。

【轻载虚拟机规格】

用户并行使用2个日常应用程序（Office/Outlook/IE等）的应用。适用于简单办公，营业厅、公用上网机、电子阅览室等轻量应用场景。

【中载虚拟机规格】

用户并行使用5个日常应用程序（Office/Notes/IE等）的应用。适用于普通办公，网管维护等应用场景。

【重载型虚拟机规格】

用户并行使用8个应用程序（例如OFFICE/ Notes /Visio/IE/ZIP/ Acrobat Reader），适用于研发办公应用的应用场景。

- **存储设备**

通过容量和IOPS两个维度计算存储设备配置，每个600G SAS硬盘的极限IOPS为200，有效IOPS=200/(1+3*70%)=64（RAID5的写惩罚是1：4。创建RAID5后，系统盘考虑70%写比例造成的写惩罚），RAID5只有一个校验盘。

下面公式中参数说明：

RAID组有效容量：RAID5的RAID组需要减去一块校验盘的容量。RAID6需要减去两块校验盘的容量。RAID10只有一半可用容量。实际多少块盘组RAID可根据实际要求更改。

热备盘率：下面公司中12块中包含一块热备盘，可根据实际要求更改。

存储配置计算过程如下：

- **容量维度**

总盘数=(总人数*每人数磁盘空间+管理节点容量)/（每盘标称容量*磁盘利用率/1.024^3）*RAID组有效容量*热备盘率）= *(500*40+1200)*/(600*0.95/1.024^3）**(7/6)*(24/22)*=52

- **IOPS维度**

总盘数=（(总人数*每人IOPS数+管理节点IOPS)*IO落盘率）/（每盘标称IOPS*IOPS利率/(1+3 *写比例)）*热备盘率=*(500*17+1000)* *21%/(200*60%/(1+3*70%))*(24/22) =57

结合容量和IOPS维度两个角度，使用RAID5的600G SAS盘建议配置57块。

- **网络设备**

接入交换机，建议配置：S5700-28C　2台。

- **接入网关**

结合用户数以及桌面云出口带宽，可以确定使用何种规格的负载均衡设备，目前使用MPX7500和MPX9500两种型号的Netscaler，具体的配置原则如下：

用户数小于2500，配置一对NetScaler MPX7500
用户数大于2500，小于5000，，配置一对NetScaler MPX9500，依次类推

- **配置清单**

设备类型	型号	单位	数量
资源服务器	E6000 服务器（2 路 6 核 CPU、72G 内存）	台	15
管理服务器	E6000 服务器（包括桌面会话管理 FusionAcess 和虚拟化管理 FusionSphere）	台	2
接入交换机	S5728	台	2
存储	S5500T（配置 135 块 600G SAS 硬盘）	套	2
云终端	CT3000	台	500
机柜	IDCU 机柜(4 路 16A 交流 220V 输入)	个	2
桌面云软件	桌面云企业增强版，每 10 用户。	个	50

8.9 方案亮点

- **桌面快速投放**（从>3个月到<1周）：应用后台统一分发，前台只保留TC，上电即用
- **兼容行业所需外设：** 兼容业务办理使用的高拍仪、身份证阅读器、手写板等外设
- **兼容主流证券经纪系统：** 可对接市场主流证券经纪业务系统，可兼容业务办理所需IE插件
- **全面的安全管控：** 终端与信息分离，USB设备控制访问、文档安全管理
- **桌面集中维护，效率提升10倍：** 100桌面/人到1000桌面/人，单人可以维护50个以上营业部
- **业务审计：** 提供实时录屏录像，支持轻型营业部见证开户

9 统一网管方案

通过eSight统一网管可以实现轻型营业部设备和WLAN的远程管理，并能对数据中心接入区设备等实现集中管理。eSight支持分级部署，可以在总部集中部署，也可以在总部和区域中心分布部署。

华为eSight统一网管，可以实现对AR路由器、Sx7交换机、ASG上网行为网关的直接管理，通过AR或AC6605实现对瘦AP6010的管理。

9.1 eSight 概述

eSight是华为面向企业市场推出的新一代IT统一运维系统，遵循ITIL规范，实现对企业资源、业务以及用户的统一管理，为企业和合作伙伴提供融合、开放的运维平台，实现以企业设备-业务-应用-用户为核心的企业立体化运维。

eSight提供丰富的openSDKs，可以快速管理其他厂家设备，快速集成到企业管理平台中。

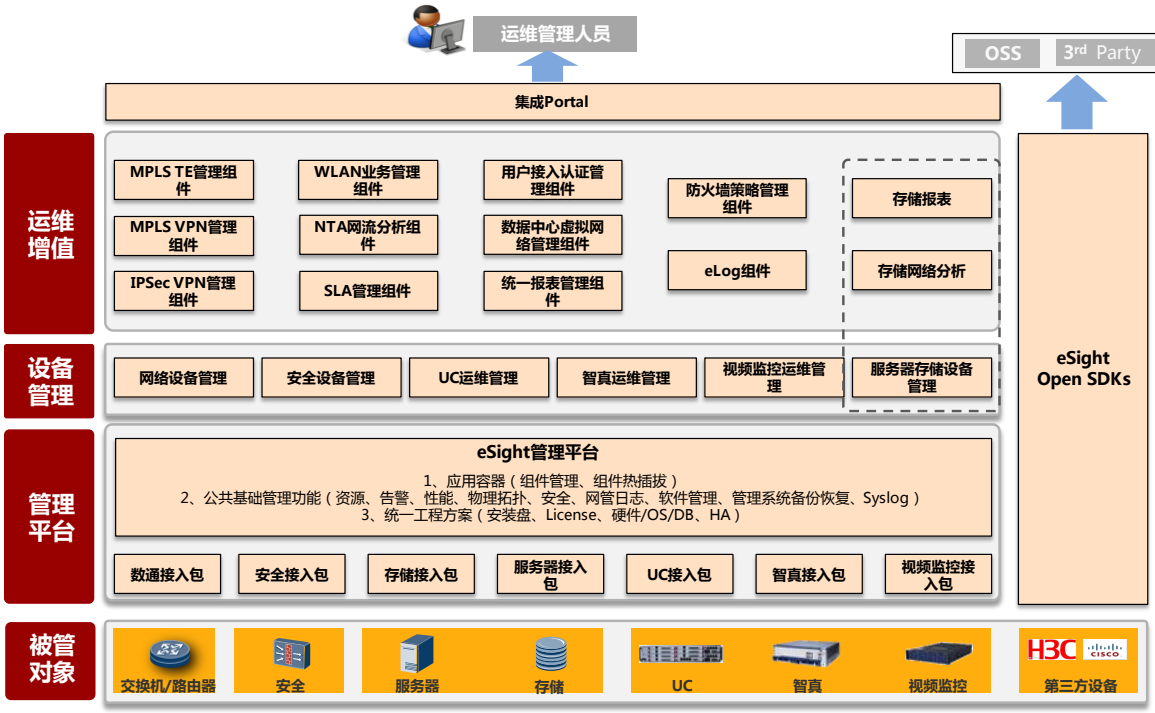

图54 eSight 组件

eSight提供了网络设备、安全设备、智真设备、监控设备、存储设备、服务器设备的统一管理平台，即可为单场景提供管理方案，更可为多种组网场景提供管理方案。

9.2 技术架构

- **Web化架构**

eSight作为B/S架构，拥有B/S架构的先天优势，它运行在客户端的浏览器之上，系统升级或维护时只需更新服务器端软件即可。具有如下优点：

✧ 具有分布性特点，可以随时随地进行查询、浏览等操作。

✧ 业务扩展简单方便，仅需要更新服务器，即可实现系统功能增强。

- **可集成性**

eSight系统使用Spring远程代理与Hessian、JSON结合，提供开放式服务集成总线。Hessian服务可以实现与其它Java系统的对接，JSON服务可以实现与多种语言系统对接。另外，eSight界面框架提供主菜单、系统菜单、用户菜单、Portal等多种扩展点，可实现与其它第三方系统的界面集成。

- **组件化**

eSight采用组件化的设计思路，并使用OSGI、Spring DM、Hessian、Birt等业界优秀的组件。

➢ 通过OSGI实现应用组件的动态插拔能力

➢ 使用Virgo整合Web服务与应用服务

➢ 使用Hessian、JSON提供开放的集成接口

- 通过使用扩展点机制提供灵活的扩展性及二次开发能力

eSight基于OSGI平台，其组件在运行时都处于一个java进程中，各组件可以以插件的形式独立启停（当依赖的组件状态满足要求时）。只有第三方系统、报表组件、智能配置工具会以独立进程的形式运行。

- **可独立修复组件**

eSight采用扩展点机制实现了功能的增量开发与网元版本适配包的增量开发，达到不用修改原有发布包代码即可增加新的功能或新的网元适配包。基于OSGI平台的模块化框架使得各业务组件都可做到独立升级、打补丁。

- **全面的安全防护**

eSight针对网络安全问题，针对企业运维特点，提供全面的安全防护方案。

网络安全：包括安全域划分、防火墙隔离、远程维护安全、入侵检测等安全方案，通过安全组网技术对OSS网络提供防护。

平台安全：包括系统加固、安全补丁、防病毒三类防护手段，通过提升操作系统、数据库的安全级别为eSight提供安全可靠的平台。

应用安全：包括传输安全、用户管理、会话管理、日志管理等方案。

9.3 主要管理功能

轻型营业部相关设备的管理主要关注eSight的拓扑管理、告警管理、WLAN管理等功能组件。

9.3.1 拓扑管理

eSight提供了物理拓扑树、自定义视图，从不同的角度为用户浏览视图的同时，为实时了解和监控整个网络的运行情况提供了便利。

- **拓扑图功能**

eSight以左树右图的方式组织整个视图，其中左导航树以树型直观的体现出网络结构的层次关系；右视图支持在背景图上将各对象显示在不同的坐标上，可直观了解对象部署位置。

用户可以设置主拓扑的背景图，eSight支持gif和jpg格式的图片。

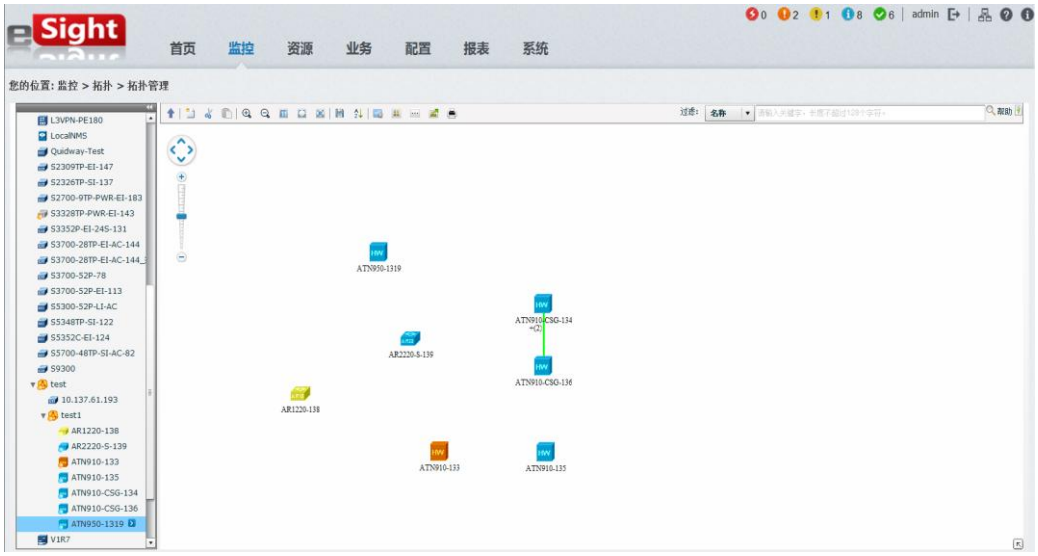

图55 eSight 页面布局

- **拓扑自动发现**

eSight提供拓扑自动发现功能，可以批量创建网元。

- **拓扑告警显示**

eSight拓扑告警支持使用不同的颜色或图标表示子网和网元状态的方式，实时的监控网元的告警状态。通过拓扑图上网元节点可以跳转到网元的当前告警，也可以在拓扑图界面显示选中网元的当前告警。

9.3.2 告警管理

eSight 告警分为4种告警级别： 紧急、重要、次要、提示。根据告警的确认和清除状态，告警分为4种状态：未确认未清除、未确认已清除、已确认未清除、已确认已清除。

当设备运行异常时，需要通过一系列流程处理设备故障，eSight告警上报和处理流程如下图所示：

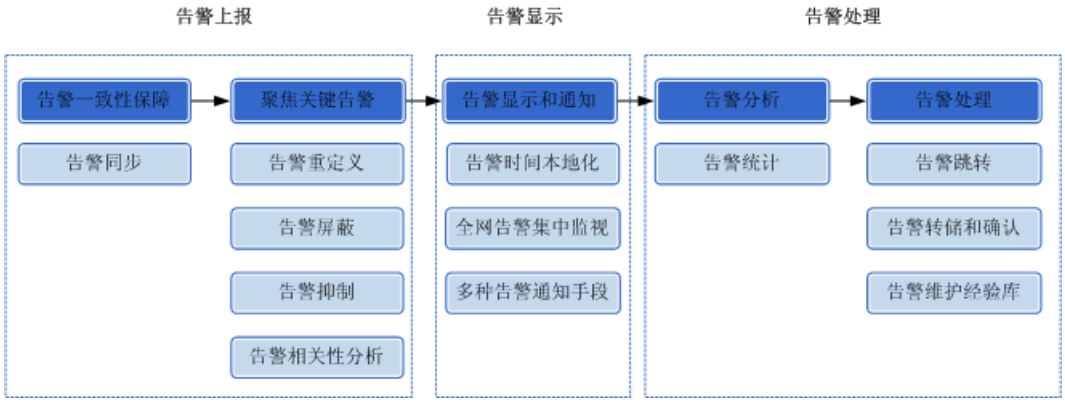

图56 eSight 告警上报和处理流程

- **告警上报**

告警同步：正常情况下，设备产生一条告警，在很短的时间内（一般不大于10秒）就会上报到eSight

并且在其告警列表中显示出来。当网管与网元通讯中断恢复后或者网管重新启动后，网元侧的告警未及时上报到网管，造成网管侧和网元侧的告警状态不一致，eSight通过手工和自动两种告警同步方式，保证网管侧真实地反映网元当前的运行状态。

告警重定义：eSight提供对网元侧的告警进行重定义功能，用户可以根据实际需要重新设置某些告警的告警级别信息。通过告警级别重定义，用户可以改变告警在eSight中显示的级别，突出用户关心的告警。

告警屏蔽：告警屏蔽功能可以对某些不重要的告警进行屏蔽，避免大量的冗余信息。

- **告警显示**

告警时间本地化：上报告警的设备可能和用户使用的网管不在同一时区，为了方　便用户准确的了解告警发生的时间，eSight会自动将告警的时间（设备时间）转换为网管的本地时间。

全网告警集中监视：eSight提供全网统一的告警板、告警浏览，告警查询模等手段，实时了解全网的运行状况。

多种告警通知手段：eSight提供多种告警通知手段，无论何时何地，都能及时通知维护人员定位问题，提高故障处理的实时有效性，如下图：

图57 eSight 告警通知手段

- **告警处理**

告警统计：eSight能按照用户所设的统计条件对告警信息进行统计。统计条件包括告警名称、告警级别、告警功能分类、告警发生时间、告警状态、告警源等，也可以是以上各项的组合。

告警跳转：eSight提供告警定位功能，从告警跳转到产生该条告警的拓扑对象（网元、网元面板），快速定位网络故障，提高定位效率。

告警转储和确认：eSight支持告警手工确认和自动确认功能。对与历史告警，支持手工转储和自动转储，自动转储还支持溢出转储和周期转储。

9.3.3 WLAN 管理

WLAN网络管理帮助用户快速完成无线网络部署，提供网络设备、非法AP等物理资源监控，实现故障的快速感知、定位及解决，同时通过无线相关报表及多形式分类资源统计，为用户日常运维及网络

调整提供了依据，极大提升网络管理效率。

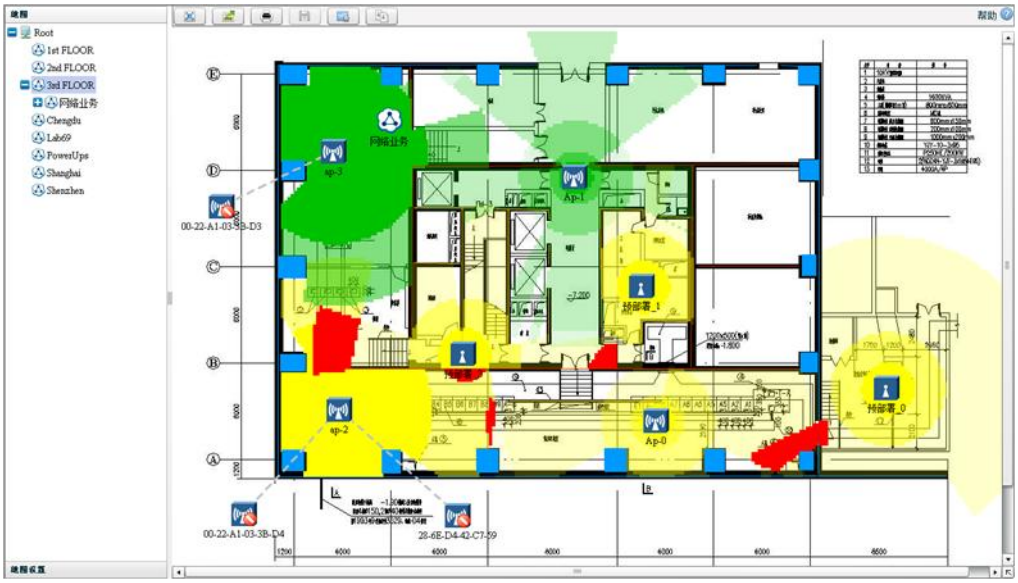

图58 WLAN 位置拓扑

- **网络部署**

网络安装完毕后，用户通过简洁向导式部署页面，首先指定AC参数配置，其次创建网元级配置模板，通过规化表单批量导入FIT AP列表，最终批量完成FIT AP部署，快速完成WLAN网络的部署。

- **网络监控**

用户可以通过网管物理拓扑，查看监控AC设备及链路状态；可以通过WLAN业务拓扑直观查看STA、FIT AP、AC接入关系；可以通过位置拓扑查看当前热点位置及射频信号覆盖范围并在视图上标识当前非法AP位置。

用户通过性能管理、告警管理及WLAN物理资源管理监控网络运行状况，并通过报表系统周期性给出WLAN相关报表，帮助用户实现轻松运维。

- **网络故障恢复**

当网络中的AP出现异常或在WLAN网络的调试过程中，用户可以通过网管远程批量恢复AP的出厂设置；在WLAN网络中AP升级完成后或在WLAN网络的调试过程中，用户可以通过网管远程批量重启AP；当网络中的AP出现硬件故障需要替换时，用户可以通过网管快速完成AP替换，AC复制故障AP上原有的配置至替换新替换的AP，快速保证AP替换后业务不变。

用户可以可通过AP PING上行设备IP（包括网关或服务器IP），根据测试结果，判断AP上行业务线路的通断情况；或通过AP下行PING用户IP地址，从而确认用户报障原因是用户关联问题还是上行业务不通。AP Ping受AP状态正常约束，所以提供AC的诊断，AC下行Ping，可诊断AC至AP链路通断。

9.3.4 配置文件定制

eSight提供了对设备的配置文件的管理功能，包括对设备配置文件的备份和恢复功能，以及在设备配置文件更新之后重启设备的功能。

对于非华为设备，eSight提供通过命令行管理设备配置文件的功能。由于各个厂商设备之间以及同

一家厂商的设备之间对设备配置文件的操作命令存在差异，自定义设备管理模块提供按照设备类型为维度对配置文件操作命令的定制功能。用户完成配置文件定制之后，在设备配置文件管理模块定制属于当前设备类型的设备的备份任务，网管就可以对设备的配置文件进行备份管理。

- ✧ 设备类型：要定制的配置文件命令的设备类型。
- ✧ 备份命令：备份设备配置文件的命令。
- ✧ 恢复命令：恢复设备配置文件的命令。
- ✧ 重启命令：重启设备的命令。

9.4 部署设计

eSight有多种版本，证券轻型营业部适用的主要是标准版和专业版。

版本	管理网元数	硬件配置	操作系统+数据库
标准版、专业版	0-200	CPU：1*双核 2G 以上 内存：4GB 或以上 硬盘：80GB	Windows Server 2008 R2 标准版（64 位）+ Mysql 5.5 或者 Windows Server 2008 R2 标准版（64 位）+ Microsoft SQL Server 2008 R2-标准版 或者 SUSE Linux 11 SP1（64 位） + Oracle 11g R2
	200-500	CPU：2*双核 2G 以上 内存：8GB 或以上 硬盘：250GB	
	500-2000	CPU：2*四核 2G 以上 内存：8GB 或以上 硬盘：320GB	
	2000-5000	CPU：2*四核 2G 以上 内存：16G 或以上 硬盘：600G	
专业版	5000-20000	CPU：4*四核 2G 以上 内存：32G 或以上 硬盘：1.2T	SUSE Linux 11 SP1（64 位）+ Oracle 11g R2
客户端要求：内存 1G 以上，Windows XP with SP3/Windows 7+IE9、IE8、Firefox3.6、Firefox12 以上			

基于eSight统一网管，我们分别提出“**总部-分支**”和“**总部-分部-分支**”两个场景的运维部署方案，客户可根据实际情况选择。

总部-分支场景部署，如下图所示：

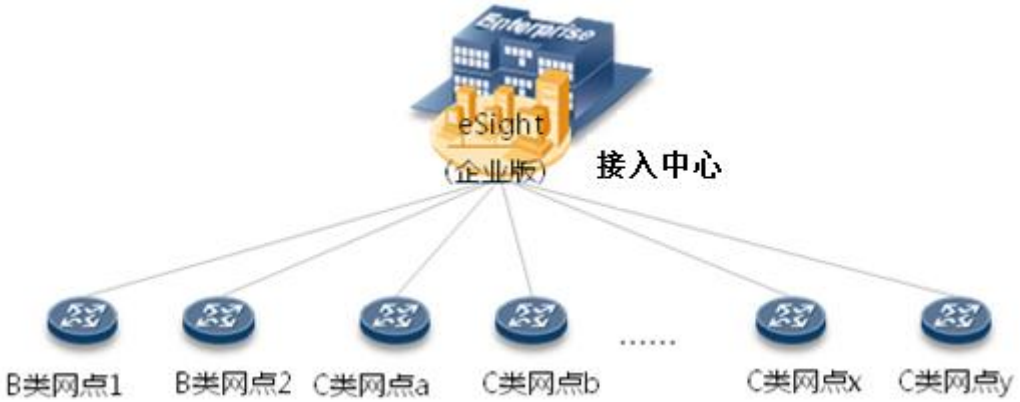

图59 接入中心—营业部运维场景

- ✧ 总部根据整网规模，部署eSight企业版/专业版。
- ✧ 分支设备的snmp trap target-host设置为总部网管地址。
- ✧ 总部网管对全网设备（包括分支设备）自动发现并进行集中远程管理。也可通过Telnet/SSH对分支设备进行管理。
- ✧ 总部安装部署IPSec VPN、WLAN等组件，实施增值业务管理。

总部-分部-分支场景部署，如下图所示：

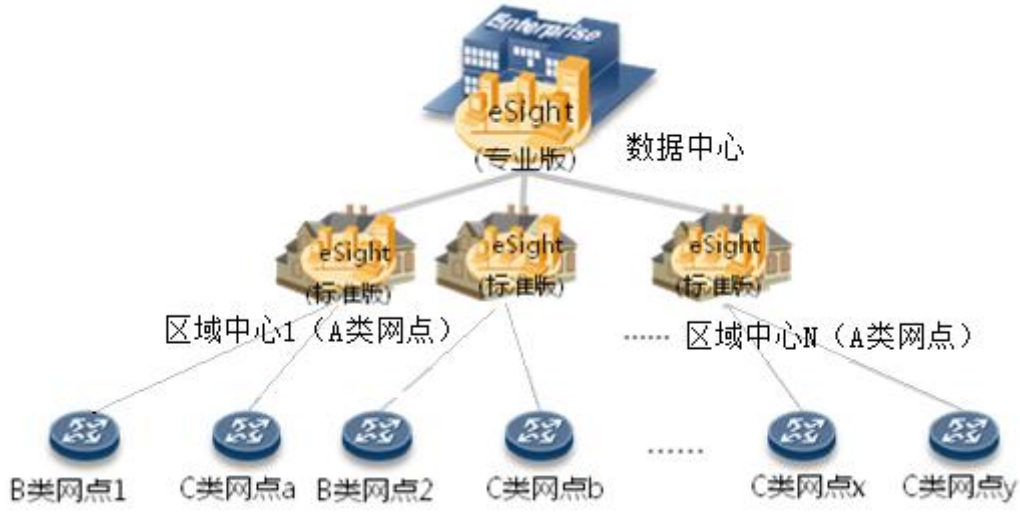

图60 数据中心-区域中心-营业部运维场景

总部部署eSight专业版，区域中心部署eSight标准版，两者形成二级网管结构。

分支设备的snmp trap target-host设置为总部网管地址。

区域中心对本地设备和下属分支设备自动发现并进行集中远程管理。也可通过Telnet/SSH对分支进行管理。

总部安装部署IPSec VPN、WLAN等组件，实施增值业务管理。

9.5 推荐配置清单

产品	型号	说明	数量
网管平台	V300R001	eSight 管理平台-标准版	1
组件及 License	V300R001	eSight 网络设备管理组件	1
		eSight 网络设备管理 License-每管理 100 设备	1
		eSight WLAN 业务管理组件	1
		eSight WLAN 业务管理 License-每管理 50AP	1
		eSight IPSec VPN 管理组件(含 60 节点)	1
		eSight MicroDC 管理组件	1

9.6 方案亮点

- 管理架构简单，管的准
  - 集中组件负责多个Micro DC分支站点的集中运维管理
  - 本地组件负责单个Micro DC站点的快速部署开局
- 完备的管理对象，管的多
  - 多MicroDC统一管理
  - IT与通信设施管理
  - 机房动环监控
- 高效的运维功能，管的好
  - 设备批量发现
  - 告警/事件/性能/报表
  - 分层拓扑/机架图/面板图
  - 智能告警联动

10 证券业务系统方案

轻型营业部各角色可能用到的业务系统如下图所示。传统营业使用时，多为本地胖客户端，而针对轻型营业部应用，多提供WEB客户端。另外，除了非现场开户系统是新开发外，其它各系统基本是沿用原有的系统。这些系统由合作伙伴提供，华为轻型营业部方案已与合作伙伴系统直接对接测试，且通过客户POC测试完成了与其他软件厂商的对接。

图61 证券业务系统

10.1 与合作伙伴对接测试

恒生电子股份有限公司 HUNDSUN TECHNOLOGIES INC.

恒生金融产品销售系统

该金融产品销售平台应当是集产品销售、登记托管、资金结算、市场拓展等多种功能于一体，方便一、二级市场投资者在同一个平台下完成所有金融产品（包括各类基金、保险、信托、银行理财产品、证券公司集合理财产品等）的投资购买，并能较好地提供多样化的金融产品综合服务；同时也为金融服务商组合理财产品快捷销售提供统一平台支持，为后续资产配置资产池、专业化产品设计做好准备。

版本：V1.0 sp1 pack3，http://www.hundsun.com/zqhy/924.htm

恒生统一账户管理系统

“统一账户管理系统”实现了客户账户、资金账户、交易产品账户（证券、期货、基金、融资融券等）统一开户、更改、管理；客户资料、影像、电子档案的采集和集中管理工作，实现了中登代理所有账户管理功能，设计了复核和回访保证账户的合规、长效，远程开户更是方便证券公司营销人员上门为客户服务。提高账户管理工作质量，确保做到客户信息真实、准确、完整；同时，有效整合客户信息，提高柜面人员工作效率。为证券公司提供一套全面的账户、档案、资料管理方案，满足不断发展的多业务需求。

版本：V2.0，http://www.hundsun.com/zqhy/563.htm

恒生离柜开户系统PAD版

恒生离柜开户系统支持网上开户和见证开户模式，网上开户由投资者自助登陆证券公司开户网站并提交开户申请；见证开户是由证券公司工作人员使用开户平台为投资者提交资料申请开户，支持视频见

证。

版本：V1.0，http://www.hundsun.com/zqhy/911.htm

金证新一代集中交易系统

金证新一代集中交易系统遵循“小核心、大外延”的设计理念，实现以客户、账户、资产为核心，以各种业务为外延。支持沪深AB股、开放式基金、代办股份转让、创业板、非交易所债券以及其他的沪深交易所全部业务，体现了以客户为中心的一站式证券服务的思想，证券公司通过金证新一代集中交易系统可以真正实现集中管理，集中交易、集中清算、统一服务。

版本：Win-spb5.2 Patch5.4.7.1(R)

金证非现场开户系统PAD版

金证非现场开户系统包括网上开户和见证开户系统，网上开户由投资者自助登陆证券公司开户网站并提交开户申请；见证开户是由证券公司工作人员使用开户平台为投资者提交资料申请开户，支持视频见证。

版本：V1.0

已发布的测试报告参见以下链接：

http://enterprise.huawei.com/cn/partners/open-lab/interoperability/test-list/index.htm

10.2 客户 POC 测试

长城证券，证券一体机：

对营业部常用的业务系统进行了连通性测试和性能测试，主要包括：柜台系统、远程非现场开户系统、新意结算系统、CRM、财务用友系统、办公OA系统、HR人力资源管理系统、短信管理系统、投资顾问平台、视频会议系统等。

东方证券，桌面云：

东方证券桌面云测试使用的软件如下，测试结果表明，业务软件兼容性不存在问题。

软件名称	厂商名称	版本号	应用场景描述
Office 2010 Sp1	微软	14.0.6029	办公
Adobe Reader 9	Adobe	9.4.0	办公
Adobe Flash Player	Adobe	10.1.85	办公
Lotus Notes	IBM	8.01 8.50	办公
综合办公平台	东方证券	--	OA 系统
风险投资调查系统	东方证券	--	内部系统
新总系统	东方证券	--	营业部
金仕达	东方证券	--	营业部
DSM	华为	--	文档安全
TSM	华为	--	终端安全
FlashFTP	--	3.4.1	文件传输
安全控件	东方证券	--	营业部
OCR 图像识别	东方证券	--	营业部
身份证阅读器	东方证券	--	营业部

同时，东方证券桌面云TC测试使用如下外设，测试结果表明，外设兼容性良好，可以正常使用上述业务系统完成业务操作。

设备名称	设备型号	接口类型	测试结果
票据打印机	OKI MICROLINE 6300FC	USB	Pass
激光打印机	HP LaserJet P3010 PCL6	USB	Pass
激光打印机	HP LaserJet Professional p1106	USB	Pass
手写板	WACOM 签名数位板 STU-500B	USB	Pass
身份证识别器	普天 CP IDMR02/TG	USB	Pass
高拍仪	良田 S300D	USB	Pass
高拍仪	多易拍 AF546	USB	Pass
摄像头	Logitech C200	USB	Pass
摄像头	天敏 LOMOONS	USB	Pass

11 方案主要产品介绍

11.1 证券一体机

华为MicroDC解决方案是根据云时代的集团企业“业务集中化、分支简单化”的趋势，助力客户更好的聚焦企业核心业务和流程，开发的简单快捷、无人值守的分支机构微数据中心。

MicroDC预集成机柜布线、供配电、动环监控等机房基础设施，整合计算、存储、网络安全、语音通信等ICT基础架构，提供以分支站点为视角的远程统一管理，搭建面向分支机构的开放软硬件平台。

小型分支机构场景典型配置（MicroDC3000L0　24U机柜加基础配置）预留扩展能力，可供灵活选配其他设备进行柜内扩展。当站点需求增加，设备增加时，MicroDC支持机柜扩展。

MicroDC3000L0可满足轻型营业部无机房化、快速部署等要求。

11.2 数据中心接入区

11.2.1 AC6605 无线接入控制器

AC6605是华为技术有限公司推出的无线接入控制器盒式设备；提供大容量、高性能、高可靠性、易安装、易维护的无线数据控制业务，具有组网灵活、绿色节能等优势。AC6605集成了千兆以太网交换机功能，实现有线无线一体化的接入方式。可灵活配置无线接入点的管理数量，具有良好的可扩展性。是配合Huawei技术领先级、性能增强级、经济适用级无线接入点，组建大中型规模的园区覆盖或企业办公网络、行业无线城域网覆盖、热点覆盖等应用环境的理想接入控制器。

AC6605产品有如下特点：

高性能

- 支持快速漫游（缓存PMK）
- 高达512 APs管理能力

高可靠

- AC设备间1+1双链路备份
- 上行链路LACP、MSTP 50ms保护
- 双电源接口，备份保护
- 风扇、电源热插拔，高温告警保护

强大的组网和业务能力

- 丰富接口：2个10GE光接口，4个GE Combo接口，24个GE电口。
- 业务强大：精细化QoS、丰富L2/L3功能、标准MIB接口。

保护投资

- 无缝适应WLAN 11b/g和11n
- 华为标准软件平台，和宽带城域设备无缝融合

11.2.2 S5700 系列交换机

Quidway® S5700系列全千兆企业网交换机（以下简称S5700），是华为公司为满足大带宽接入和以太网多业务汇聚而推出的新一代绿色节能的全千兆高性能以太网交换机。它基于新一代高性能硬件和华为公司统一的VRP®（Versatile Routing Platform）平台，具备大容量、高密度千兆端口，可提供万兆上行，充分满足客户对高密度千兆和万兆上行设备的需求，同时针对企业网用户的园区网接入、汇聚、IDC千兆接入以及千兆到桌面等多种应用场景，融合了可靠、安全、绿色环保等先进技术，采用简单便利的安装维护手段，帮助客户减轻网络规划、建设和维护的压力，助力企业搭建面向未来的IT网络。

S5700系列以太网交换机为盒式设备，机箱高度为1U，提供标准型（SI）和增强型（EI）两种产品版本。标准型支持二层和基本的三层功能，增强型支持复杂的路由协议和更为丰富的业务特性。

技术指标如下：

指标项目	指标要求
尺寸	1U 机架设备 ,满足工业标准机柜安装要求
网络接口及数量	100/1000M 自适应以太网口≥48 个，SFP（GE/10GE）光纤上联端口≥2 个
电源模块	内置模块化双电源
交换容量	背板交换容量≥256Gbps；端口交换容量≥176Gbps；包转发率≥132Mpps,
管理功能	须支持 SNMP V1/V2/V3、Telnet、RMON、SSHV2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理，支持 NQA ，支持基于 IPv6 的管理，支持群管理
特性	支持自动协商工作方式、自协商速率、链路聚合； 支持 Access、Trunk、Hybrid 和 QinQ 各种 VLAN； 支持静态、动态 MAC、静态、动态 ARP； 支持静态路由、RIP V1、V2、OSPF、IS-IS、BGP 等路由协议； 支持 DHCP Client/Server/Relayl，支持 DHCP snooping 支持 IPv6、QoS 调度

11.2.3 USG5100 系列防火墙

USG系列产品是华为为解决政府、企业、数据中心等机构的网络安全问题，而自主研发的统一安全网关。USG系列基于业界领先的软、硬件体系架构，以用户为核心的安全策略融合了IPS、AV、URL过滤，应用程序控制，邮件过滤等行业领先的专业安全技术，可精细化管理1000余种网络应用，支持IPv6协议，为用户提供强大、可扩展、持续的安全能力。

支持的功能特性如下：

IPS 入侵防御系统	支持（系统漏洞，未授权下载，欺骗软件，间谍/广告类软件，协议识别等）
AV 防病毒系统	支持（文件识别及筛选，高效病毒扫描，可检测 700 多万种病毒）
AS 反垃圾邮件系统	支持（本地黑、白名单，远程实时黑名单、内容过滤、关键字过滤、附件类型、大小、数量等）
URL 过滤系统	支持 6500 万网站识别（黑白名单过滤，远程分类过滤，自定义分类过滤、搜索引擎关键字过滤，恶意 URL 库与钓鱼网站识别）
应用管理	支持 1000+协议识别与管理，涵盖所有主流应用协议，如：QQ，网易泡泡，阿里旺旺，PPStream，PPLive，迅雷，电驴，同花顺，大智慧，MSN，GoogleTalk，Youtube，Facebook，BitTorrent，eMule，Skype 等等。
VPN	IPSec VPN / SSL VPN / MPLS VPN
DDoS 攻击防护	支持防范多种 DoS 和 DDoS 攻击，如 SYN Flood、ICMP Flood、UDP Flood 等
路由特性	IPv4：静态路由、RIP、OSPF、BGP、IS-IS
	IPv6：RIPng、OSPFv3、BGP4+、IPv6 IS-IS、IPv6RD、ACL6
部署及可靠性	支持透明、路由、混合等部署模式，支持主/主，主/备模式备份

扩展及I/O规格如下：

型号	USG5120	USG5150	USG5160
固定接口	2×GE（RJ45）+ 2×GE（combo）	4×GE（combo）	4×GE（combo）
扩展槽位	4×MIC+2×FIC+2×DFIC	4×MIC+2×FIC+4×DFIC	4×MIC+2×FIC+4×DFIC

重要性能指标如下

一级规格	**USG5100**		
	USG5120	USG5150	USG5160
FW 吞吐量	2G	4G	6G
每秒新建连接数	6 万	6 万	6 万
最大并发连接数	200 万	300 万	300 万

产品具有如下特点：

性能优异，稳定可靠

性能优异，实现海量业务处理，大容量NAT转换能力，轻松实现海量业务处理；

高密度接口，适应不同应用场景需求，为提前跨入万兆时代的您提供不同组网情况下的安全防护，方便您细化安全区域；

超长无故障运行时间，确保客户业务连续性：关键部件冗余配置，成熟的链路转换机制，支持内置Bypass插卡（USG5100支持），为您提供超长无故障硬件保障；商用10年+的超稳定软件平台，全球在线设备超过10万台，为您打造永续的办公环境；

专业安全，信心保障

业界领先反病毒引擎，提供99%高精准检出率：基于Symantec多年积累的反病毒技术，采用文件级内容扫描的AV引擎，结合全球领先的仿真环境虚拟执行技术，提供高达99%的精准检出率，多次荣膺国际评测组织好评；

专业IPS引擎，让【变形】无所遁形：传统的基于攻击代码的防护方式，因为攻击种类的频繁变形，需要维护更新庞大签名库，使得IPS引擎不堪重负，检测性能低下，误报漏报率较高。USG采用Symantec领先的漏洞防护技术，针对漏洞（而非攻击代码）提供“虚拟补丁”， 让各种攻击变形无所遁形；

完善的反垃圾邮件能力，保护企业邮件服务器安全；根据邮件正文、标题、关键字、附件属性来控制员工的邮件行为，避免邮件泄密和不安全因素的引入

专业团队实时更新，实现零日攻击防护：全球部署的蜜网系统和300+人的专业安全分析团队，持续追踪最新、最热门、最高危的系统漏洞和软件漏洞，以最快速的应对方案实现零日攻击防护，为您提供更安全的办公网络；

上网管理，高效工作

海量网站分类，营造绿色上网环境：6500万海量网站，130+内容分类，屏蔽挂马钓鱼等恶意网站，防范员工不当操作危害内网安全；隔离赌博色情等不良网站，营造绿色上网环境，规范员工上网行为、减少企业法律风险；

精细应用管理，创建高效办公网络：1000+种应用协议识别，基于时间、应用、用户、带宽、连接数的多方位调控手段，让P2P/IM/GAME/WEB网站随您掌控，可有效保障关键业务带宽，提升带宽利用率，提升员工工作效率；

丰富的报表：从用户、应用、流量、行为等多维度真实呈现用户上网行为，让您时刻掌握网络利用情况；

灵活配置，快速部署

以用户为核心的安全策略：基于用户的访问控制、限流、网络应用控制和内容安全、策略路由等技术，提供细粒度的控制权限，抛弃基于IP配置的复杂性，配置更加灵活、控制更加精准；

一体化策略设计：所有配置统一入口，在一个页面配置完所有策略，减少对象之间的跳转，简化配置步骤，避免漏配，提升上线速度；

专业配置向导：基于WEB界面的专业配置向导，采用人机对话方式引导管理员进行配置，全面提升管理员操作体验；

11.2.4 SVN5530 安全网关

SVN5530产品是华为公司最新推出的一款安全接入网关，采用可靠的硬件平台，安全的实时嵌入式操作系统，传承多年在通讯、网络领域的研发、设计能力，满足各种严苛的国际认证规范，为企业、政府、运营商提供了远程接入、移动办公的安全解决方案。

SVN产品主要功能为：

- 对用户进行全面的身份认证、访问授权以及行为审计，充分保证用户身份的合法性，实现灵活细致的访问控制策略。
- 对远程用户与证券公司内网之间的传输数据进行强加密，保护敏感信息，杜绝了有效信息的泄露。
- 对广泛的远程访问业务提供支持，包括对web资源、文件系统、多种C/S应用以及与应用无关的全IP层业务访问。
- 无需管理员大费周章地为用户安装、配置和维护客户端软件，用户只需要标准浏览器，就能实现访问，有效提高移动办公人员（如非现场开户办理人员）的工作效率。
- 提供详细的日志功能，便于对用户/管理员的操作行为进行实时的审计与管理。
- 高可靠性，SVN的双机热备技术支持抢占功能，这一点在互为备份流量分担的组网中特别重要，因为一旦设备故障所有流量都切换到一台设备上时，需要一个切实的机制能保证故障设备恢复时流量能平滑的切换回去，而支持抢占功能的双机热备技术能保证这种切换的平滑，从而保证了互为备份组网的可靠运行；支持OSPF+VRRP混合组网的方式。

SVN 5530关键技术规格如下表所示：

名称	简介
WEB 代理	支持通过标准浏览器访问内网 WEB 资源，实现对内网网站、Email 等 web 应用的代理。支持对页面所带的 URL 地址进行改写，包括对 HTML/SHTML/DHTML、Javascript、CSS、ActiveX、VBScript、OWA、XML、WML、FLASH、Java applet、PDF 等的改写。
SSL 最大并发用户数	12000
每秒新建 SSL 连接数	3000
云接入并发用户数	2500
文件共享	支持内网 CIFS（Windows）、NFS（Linux）文件系统，实现文件系统访问 Web 化。
端口转发	提供丰富的 C/S 应用支持。无需安装客户端软件，即可实现 Telnet、RDP、SSH、VNC、Notes、Email、FTP、Oracle 等的内网 TCP 应用。

名称	简介
网络扩展	支持基于 IP 的所有内网应用，实现内网的全网访问。通过配置隧道模式控制用户对内网、Internet 及本地局域网的访问权限，包括全通道、分离通道和客户自定义三种方式。
跨平台的安全 SDK	提供跨平台的安全 SDK 组件，和用户的各种应用实现无缝集成，使用户的应用能够安全访问业务资源。支持 Android、Windows、iOS(iPhone/iPad)、Linux、Symbian、Blackberry、Mac OS 等主流平台。
虚拟桌面	支持用户使用智能移动终端设备（iOS、Android 平台）通过虚拟桌面，访问内网的 PC 机/笔记本/虚拟机进行各种业务处理，仅仅传输操作界面、键盘、鼠标信息，保证了访问的安全性。
独立 CA 功能	内置独立 CA，提供证书颁发、撤消等管理功能
虚拟网关	每个虚拟网关可配置独立的用户、资源、管理员和访问策略。能够在企业的不同用户群组或不同的企业间形成完全隔离的访问体系。
安全桌面	用户通过安全桌面可以安全访问内网资源，对内网资源的数据操作均在安全桌面中进行，与本地桌面的数据隔离，安全桌面内的数据无法通过本地打印、本地文件拷贝、本地网络传输等方式转移至安全桌面外部，用户退出安全桌面后，所有访问痕迹被清除，防止了内网资源数据保留在用户设备上而造成泄密。
终端硬件绑定	将用户账号与终端设备绑定，使远程用户只能通过特定的终端接入企业，保证终端的安全可信。单台设备可支持十万条绑定策略，每个用户最多可以与五台 PC 绑定。
客户端安全检查	通过对客户终端个人防火墙、杀毒软件、操作系统版本及补丁、注册表、特定文件、特定端口、应用进程等相关状态的检测，并实施相应的权限控制，降低客户端非安全因素对内网造成的安全威胁。
安全浏览器	安全浏览器可以细粒度的控制用户访问，可以在用户退出浏览器时自动清除访问历史数据，避免隐私数据泄漏，做到无痕访问，帮助企业更好的保护商务机密数据。

11.2.5 NIP2000/5000 系列 IPS

NIP2000/5000系列作为业界领先的入侵检测/防御类产品，支持在IPv4&IPv6网络环境下提供虚拟补丁、Web应用防护、终端安全防护、网络应用管控、恶意软件控制、病毒防护以及Anti-DDos等安全功能。通过深入应用内容的分析和检测，实时阻断网络流量中隐藏的蠕虫、木马、间谍软件、DoS等攻击与恶意软件，并对各种P2P、IM等非关键业务进行有效管理。实现服务器/客户端保护、网络基础设施保护及网络性能的保护。

全面防护——场景全覆盖

- 提供最高达10G的IPS防护性能，全面覆盖用户各带宽场景；
- 支持对用户服务器、客户端、互联网出口、分支互联、数据中心等部署场景入侵防护；
- 提供服务器漏洞攻击防护、Web应用防护、恶意软件控制、病毒防护、应用管控、网络层DDoS防护、应用层DDoS防护、上网客户端攻击防护等功能，全面覆盖各种攻击场景；
- 强大的应用感知能力，识别应用1200+，全面覆盖用户业务带宽控制；

准确检测——“零”误报，有效降低维护成本

- 基于先进的漏洞特征检测技术，检测精准，“零”误报，确保用户业务正常运行。
- 签名库85%默认开启率，确保系统上线即实时防护；
- 签名库80%的默认阻断率，自动阻截关键威胁，确保用户安全无忧。

易于使用——“零”配置上线

- 零配置上线：设备上电接通即可正常工作，无需复杂的签名调校及网络参数调整；
- 丰富的策略模板：为各专门场景提供最简单的配置方式，便于客户实施定制化安全策略；
- 实时系统监控及安全趋势监控，数十种分析报表，轻松掌握安全状态。

产品主要规格：

型号	NIP2150	NIP2200	NIP5100	NIP5200	NIP5500
产品性能	低端千兆		中端千兆	高端千兆	万兆
扩展及 I/O					
专用管理口	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)
固定接口	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo) 2×10GE(SFP)
扩展槽位	3×FIC	3×FIC	3×FIC	3×FIC	2×FIC
扩展网络接口	BYPASS: 4×GE(RJ45) 2Line(LC/UPC) 接口： 8×GE(RJ45)、 8×GE(SFP)	BYPASS: 4×GE(RJ45) 2Line(LC/UPC) 接口： 8×GE(RJ45)、 8×GE(SFP)	BYPASS ： 4×GE(RJ45)、 2Line(LC/UPC) 接口： 8×GE(RJ45)、 8×GE(SFP)、 2×10GE、 2×10GE+8GE	BYPASS ： 4×GE(RJ45) 2Line(LC/UPC) 接口： 8×GE(RJ45)、 8×GE(SFP) 2×10GE、 2×10GE+8GE	BPASS： 4×GE(RJ45) 2Line(LC/UPC) 接口： 8×GE(RJ45)、 8×GE(SFP) 2×10GE
功能特性					
服务器防护	✧ 针对应用服务器提供全方位的安全防护，解决以下问题：系统漏洞攻击、服务漏洞攻击、暴力破解、SQL 注入、跨站脚本、病毒防护				
客户端防护	✧ 提供浏览器及其插件（Java、ActiveX 等）的安全防护； ✧ 提供对 PDF、Word、Flash、AVI 等常见文件的防护； ✧ 对操作系统漏洞、间谍/广告软件以及病毒等的检测防护；				

基础设施保护	✧ 畸形报文攻击防护、特殊报文控制、扫描类攻击防护、TCP/UDP 泛洪攻击防护； ✧ 应用层 DDoS 攻击防护：HTTP、HTTPs、DNS、SIP 等； ✧ 流量自学习：根据对客户正常流量的统计，设定流量型攻击的阈值；
应用管控	✧ 支持 1200+应用协议识别与管理，涵盖主流应用协议：P2P/IM/网络游戏/炒股软件/语音应用/在线视频/流媒体/Webmail/移动终端应用/远程登录等应用的识别及控制
报警及响应	✧ 实时警报、声音报警、Syslog、SNMP Trap、E-Mail、发送短信、第三方联动、IP 地址隔离、攻击报文抓取、实时阻断会话
设备管理	✧ 图形化界面配置、管理员分级管理、访问控制权限设置、设备集中管理； ✧ 引擎知识库定时升级、引擎知识库回滚、内网集中升级；
日志报表	✧ 设备状态监控、事件信息记录备份、日志查询及过滤、网络状况实时监控、报表制定生成
部署	✧ IPS 在线部署；IDS 旁路部署；部分接口在线，部分接口旁路的混合部署； ✧ 支持硬件 BYPASS 插卡、支持双机部署；

整机规格					
尺寸(W×D×H)mm	442×415×130.5	442×415×130.5	442×415×130.5	442×415×130.5	442×415×130.5
功率	300W	300W	300W	300W	300W
电源	AC:100～240V 50/60Hz 支持冗余			AC:100～240V 50/60Hz DC：-48～-60V 支持冗余	
工作环境	温度:0~40℃ 湿度:10%～85%不结露				
MTBF	12.67 年	12.67 年	12.67 年	12.67 年	12.67 年

11.3 AnyOffice

11.3.1 SVN 系列安全接入网关

SVN2000-M/SVN5000-M系列安全接入网关是华为公司面向运营商、企业、政府、行业推出的优秀的SSL/IPSec一体化VPN网关设备，它基于华为专业的高可靠硬件平台和专用的实时操作系统，具备业界领先的系统性能、安全性和可靠性。

SVN支持静态路由、OSPF、BGP、ISIS动态路由协议、策略路由和路由迭代，支持IPv4和IPv6双协议栈工作方式，也支持双机热备和物理链路备份。部署SVN安全接入网关，无需改变网络结构，可以直接单臂挂接到出入口防火墙或者路由器、交换机上，简单快捷。

SVN作为企业移动办公的安全接入网关，提供了丰富的认证手段和灵活的访问授权控制手段，企业或机构可以根据自身需求、认证体系的建设情况灵活选择认证方式，保护企业的原始投资，包括VPNDB本地认证*、LDAP/AD /Radius/SecurID认证*、终端硬件特征绑定*、数字证书认证、短信认证、及多种认证方式的组合认证（*标记的为使用AnyOffice客户端接入时支持的认证方式）。

在授权和访问控制上，SVN引入角色的概念，对不同的角色授予不同的资源访问权限，同时，通过配置访问控制策略，可以在用户访问已授权资源时增加额外的访问控制，包括基于URL、IP、端口的细粒度访问控制。

SVN具备强大的移动办公安全接入能力，提供Web代理技术供用户在各种终端类型上使用标准浏览器随时随地的安全访问内网的Web服务器、提供L3VPN供Android终端以网络扩展方式访问企业内网、提供安全SDK给各种移动应用集成使之具备L4VPN接入能力，同时，还支持标准L2TP over IPSec协议的接入。

另外，SVN通过虚拟网关为用户提供SSL VPN服务。SVN作为一个物理实体，可以通过虚拟技术将其虚拟为多个逻辑上的SSL VPN网关，以提供给多个企业或者一个企业的多个部门使用。比如，某个大型企业有多个部门，每个部门有各自的员工，部门间能够访问的资源和服务也各不相同，每个部门有自己的访问控制规则。在这种情况下，就可以为每个部门分配一个虚拟网关，每个虚拟网关都是独立可管理的，可以配置各自的用户、资源和ACL规则，形成独立的访问体系。而每个部门的感觉就像各自在使用一个独立的网关设备一样高效、安全。

11.3.2 USG 防火墙

USG2200/5100系列是华为公司针对中小型企业的需求推出的新一代产品。可广泛应用于中小企业、大型企业分支机构等。

USG2200/5100采用模块化设计，集安全、路由、交换、无线（WiFi、3G）等特性于一体，接口类型丰富，性能领先。能为中小企业、大型企业分支机构、SOHO办公类用户、以及网吧出口网关提供安全防护，并能提供集成的网络出口安全与互联解决方案，降低企业总所有成本，提升企业的效率，是中小型企业网络的理想安全防护设备。

USG5500系列产品是华为面向大中型企业和下一代数据中心推出的新一代电信级统一安全网关设备。可广泛应用于运营商、企业、政府、金融、能源、学校等领域的网络边界。

该系列产品采用全新的万兆多核硬件平台，面对企业海量业务处理零延迟，打造更高速的网络；融合Symantec先进的入侵防御和反病毒技术，全新演绎专业内容安全防御，营造更安全的网络；集成业界领先的SA（业务感知）识别技术，精细管理超千种应用程序，创建更高效的网络。为大型企业和数据中心打造“更高速、更高效、更安全”的高性价比网络体验。

USG系列产品在基本防火墙功能基础上还支持丰富的路由协议，可节省用户投资，降低组网成本；支持IPv4和IPv6双协议栈工作方式，提供完整的IPv6特性和IPv4网络向IPv6网络平滑迁移的解决方案；提供了完备的UTM（Unified Threat Management）功能，致力于内容安全防护、上网行为管理等方面，为用户提供全方位的安全防护。

11.3.3 MediaPad10

对于行业应用，目前推荐华为的MediaPAD10：

Android ICS4.0

CPU： 海思K3V2 Cortex-A9四核1.4GHz

屏幕： 10.1寸 ，IPS全视角屏

分辨率： 1920 x 1200 224PPI

存储： 2GRAM+16G ROM

摄像头： 后800W+前130W，AF/720P录像

网络： HSPA+ / HSPA / UMTS / GPRS / GSM，Wi-Fi 802.11b/g/n

视频解码： 1080P，支持所有主流音频格式播放

重量/电池： ~590g，6600mHA

尺寸： 257.4mm*175.9mm*8.8mm

11.4 桌面云

11.4.1 Tecal E6000 V2 服务器

E6000服务器具有如下特点：

- 散热好：

华为刀片散热架构先进：每个模块独享风道；刀片采用“对称布局”设计，相对“影子布局”，散热更均匀。

- 可靠性高：

架构可靠性高：背板采用无源背板；全冗余设计；所有模块（刀片/硬盘/交换/管理/风扇/电源）支持在线热插拔。

- 管理维护简单：

“免下架”维护：机箱上架后，终生“免下架”维护。机箱所有模块拔出后，只剩下免维护的无源背板和结构件。ZeroTouch零接触管理，所有管理维护操作都可以远程完成。

E6000硬件规格

系统	类别	描述
E6000	尺寸	8U 机架（HxWxD：353mm×447mm×810mm）

主机	刀片槽位	10
	交换机模块	6，可配置为 6 个 GE 交换模块或 4 个 GE 交换模块+ 2 个 FC 交换模块
	电源	6 个 110V/220V 80plus 电源
	风扇	9 个热插拔风扇模块
BH622 V2 刀片	CPU	采用 Intel 新一代四核或六核或八核 Intel Sandy Bridge-EP Xeon E5-2600 系列处理器，支持 130W、95W、80W 系列；
	内存	24 个 DDR3 内存插槽，最大支持 768G 内存；
	硬盘	2 个 2.5 英寸 SAS/SATAII/SSD 硬盘，支持内置 1.8T SAS 硬盘存储,2T SATA 硬盘存储或 600GSSD 硬盘存储； 支持 RAID0、1，512MB/1GB Raid Cache； 支持 BBU 电池保护（选配）；
	IO 扩展	板载 2 个 GE 接口； 支持扩展 2 个 PCIe 8x IO 接口；
管理	管理	支持单板管理模块 BMC 提供对服务器的智能监控功能，符合 IPMI2.0 标准 支持远程 KVM，虚拟媒体等功能

11.4.2 S5500T 存储

华为桌面云解决方案支持华为T系列S5500T存储，也可异构第三方主流存储设备。OceanStor S5500T存储为用户提供系统空间和数据空间，存储特点如下：

- 高性能、高扩展性

高速部件/高速总线：配备64位多核处理器以及高速大容量缓存，最高36GB/s的系统内部交换带宽，支持SAS2.0宽端口后端通道。

支持多种不同种类的硬盘：SAS/SATA/SSD。

支持最大2块I/O接口卡：最大12个IO接口（包括前端与后端接口）。支持4/8Gb FC、1/10G Ethernet与6Gb SAS2.0接口。

三重性能加速技术：依靠强大硬件支撑的固有性能，使用SmartCache技术持续监测系统热点数据并缓存至SSD盘片，最高可获得数倍的读性能提升；利用纯SSD将系统性能再次大幅提高。三重性能加速机制，稳固按需提升系统性能，全面降低整体拥有成本。

高镜像带宽：双控之间的Cache镜像采用专用高速8GB/s通道，消除双控间数据交换的瓶颈。

- 高可靠、高可用性

接口模块化热插拔设计： TurboModule技术使得I/O接口卡可在线热插拔而无需关闭存储控制器，对业务主机完全透明，实现真正的在线I/O扩容。

掉电数据保护：系统掉电后内置电池模组自动将Cache数据写入数据保险箱，保证数据不丢失。

硬盘预拷贝技术：提前发现即将故障的硬盘，主动迁移故障盘数据，规避系统降级的风险，有效降数据丢失的风险。

硬盘坏道修复技术：最大限度修复硬盘坏道，将硬盘故障率降低50%以上，延长硬盘的可使用周

期。

高级数据保护技术：利用HyperImage以及HostAgent实现针对应用系统数据的一致性快照，并能从快照中瞬间恢复数据；跨存储平台卷拷贝技术实现异构存储间的数据保护。远程复制技术实现数据异地备份容灾保护。

- 低总体拥有成本

统一的IO接口模块：本系列全线产品使用统一的IO模块，极大降低总体拥有成本。

24盘位高密设计：2U/4U高密度硬盘框（24块/框），平均1U空间最高可容纳12块硬盘（2.5英寸），相对于低密度盘框设计来讲，扩容成本降低60%。

易用的管理维护工具：通过ISM统一管理界面，5步即可完成基本配置。支持声音、灯光、手机短信、邮件等多种告警手段；一键式双控在线Firmware升级，有效地降低用户运维成本。

- 低功耗

硬盘节能技术：依据业务负载，实现硬盘智能休眠，可降低40%的能耗。

智能风扇调速技术：根据系统当前温度智能调节风扇转速，降低风扇功耗及噪音，(风扇占整机功耗15%左右)，增强设备环境适应能力。

CPU智能变频：根据业务压力智能调节CPU工作频率，在业务压力小时，降低CPU工作频率，大大降低系统功耗。

技术规格

型号	S5500T
硬件特性	
存储处理器	多核多处理器组
缓存	8GB 、16GB、32GB
控制器数	2
前端通道端口类型	8Gb FC、1/10GE(iSCSI)
后端通道端口类型	24Gb SAS 宽端口
板载 IO 端口数	8×8Gb 前端 FC 及 4×24Gb 后端 SAS 宽端口
最大 IO 模块数	2
最大硬盘数量	288
硬盘规格	SAS、SATA、SSD
软件特性	
RAID 支持	0,1,3,5,6,10,50
连接主机数量	512
Luns	2048
支持快照数量	1024
TurboBoost	支持
TurboModule	支持
其他功能软件	HyperImage（快照）、HyperCopy（LUN 拷贝）、HyperMirror（同步/异步远程复制）、HostAgent（主机端快照/复制管理模块）、UltraPath（多路径

	软件）、Diskguard（主机端数据保护软件）、SmartCache（TurboBoost 中的动态数据缓存技术）
操作系统兼容性	AIX、HP-UX、Solaris、Linux、Windows 等

11.4.3 S5700 交换机

Quidway® X7系列系列全千兆企业网交换机（以下简称X7系列），是华为公司为满足大带宽接入和以太网多业务汇聚而推出的新一代绿色节能的全千兆高性能以太网交换机。它基于新一代高性能硬件和华为公司统一的VRP®（Versatile Routing Platform）平台，具备大容量、高密度千兆端口，可提供万兆上行，充分满足客户对高密度千兆和万兆上行设备的需求，同时针对企业网用户的园区网接入、汇聚、IDC千兆接入以及千兆到桌面等多种应用场景，融合了可靠、安全、绿色环保等先进技术，采用简单便利的安装维护手段，帮助客户减轻网络规划、建设和维护的压力，助力企业搭建面向未来的IT网络。

X7系列系列以太网交换机为盒式设备，机箱高度为1U，提供标准型（SI）和增强型（EI）两种产品版本。标准型支持二层和基本的三层功能，增强型支持复杂的路由协议和更为丰富的业务特性。

技术指标如下：

指标项目	指标要求
尺寸	1U 机架设备 ,满足工业标准机柜安装要求
网络接口及数量	100/1000M 自适应以太网口≥48 个，SFP（GE/10GE）光纤上联端口≥2 个
电源模块	内置模块化双电源
交换容量	背板交换容量≥256Gbps；端口交换容量≥176Gbps；包转发率≥132Mpps,
管理功能	须支持 SNMP V1/V2/V3、Telnet、RMON、SSHV2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理，支持 NQA ，支持基于 IPv6 的管理，支持群管理
特性	支持自动协商工作方式、自协商速率、链路聚合； 支持 Access、Trunk、Hybrid 和 QinQ 各种 VLAN； 支持静态、动态 MAC、静态、动态 ARP； 支持静态路由、RIP V1、V2、OSPF、IS-IS、BGP 等路由协议； 支持 DHCP Client/Server/Relayl，支持 DHCP snooping 支持 IPv6、QoS 调度

11.5 eSight 统一网管

华为推出的eSight网管产品提供可视化管理、统一运维，降低运维成本。设备可视、流量可视、质量可视、业务可视，实现企业整体从网络-设备-质量-流量-业务多层体系内容可视，降低企业运维难度，提升企业员工网络应用体验；提供整体运维方案，统一部署，统一运维，实现不同组件间功能智能联动，

将复杂的企业管理运维有效融合，化繁为简。

eSight网管产品具有如下特色：

真正轻量级系统：基于B/S架构，可在便携机上安装，满足用户随时随地访问。

多设备管理：IP+IT设备统一管理和自定义管理能力，有效降低初次投资，解决后顾之忧。

统一的运维体验：基于统一的企业管理平台，提供完整的解决方案，功能间智能联动，提供相同的运维体验，降低IT人员学习成本

可视化的管理：可视化是管理的基础，提供多种视图多种图标，从不同层面以不同方式全面呈现网络状态和网络质量。

12 成功案例

12.1 长城证券

长城证券有限责任公司
GREAT WALL SECURITIES CO., LTD.

客户需求&挑战：

- ✧ 长城证券申请设立15个轻型营业部获批，要求营业部能快速部署和远程维护；
- ✧ 长城证券总部部署CheckPoint防火墙，用于实现营业部IPSEC VPN对接；

华为方案：

- ✧ MicroDC证券一体机简配版，并进行冗余增强；
- ✧ 通过一体化选型、模块化设计、生产预安装、带板运输、U盘开局等特性，实现轻型营业部的现场免IT人员、快速安装、快速配置；
- ✧ 通过链路和设备冗余提高可靠性；通过VPN、AR内置防火墙和ASG保证安全性；

- ✧ 使用华为AR路由器解决了其他厂商未能解决的CheckPoint防火墙对接问题；

客户价值：

- ✧ 轻型营业部一天内完成IT部署，实现营业部快速营业；加速长城证券战略部署；

12.2 东方证券

客户需求&挑战：

- ✧ 规划XXX个轻型营业部，要求桌面快速部署，减小对营业部人员的要求；
- ✧ 在加快部署的同时保证数据安全和系统管理维护效率；

华为方案：

- ✧ 数据中心部署华为FusionCloud 桌面云系统，
- ✧ 支持桌面快速发放，后台集中管理；应用软件后台统一部署；
- ✧ 数据在终端不落地，保证业务数据安全；
- ✧ 量身定制瘦终端，兼容高拍仪等多种外设；

客户价值：

- ✧ 桌面投放时间缩短到1周，终端维护效率提升10倍；
- ✧ 营业部快速构建、高效办公、简单运维；

12.3 中银国际证券

客户需求&挑战：

- ✧ 后续轻型营业部大量部署，关注大量桌面的启动风暴；
- ✧ 为了后续业务扩张，提前考虑存储和服务器的扩容能力及性能；
- ✧ 业务系统使用Windows、Linux等多种OS，要求云平台虚机都能支持；

华为方案：

- ✧ 部署华为FusionCloud 桌面云系统；
- ✧ 定时开关机机减小启动风暴对系统的冲击；并通过运维系统进行实时监控；同时保证人为风暴不对在线虚机产生影响；

- ✧ E6000高密度服务器+S5500T企业级IPSAN，提供高性能、良好的兼容性和扩展性；
- ✧ 云平台支持SUSE，Redhat，debian，ubuntu，fedora等常见的各种LINUX虚拟机

客户价值：

- ✧ 满足当前营业部的建设需求，又保证后期的扩展和兼容性需求；
- ✧ 实现高效的虚拟桌面生命周期管理；

12.4 宏源证券

客户需求&挑战：

- ✧ 非现场开户业务放开，宏源借此大范围挖掘客户，探索价值区域；
- ✧ 笔记本电脑笨重，携带和产品展示不便；

华为方案：

- ✧ MediaPAD10 FHD，支持业务高效开展；
- ✧ 6600mAH大容量电池，超长续航；
- ✧ 高清全视角大屏，前后摄像头，四核CPU，优秀体验；

客户价值：

- ✧ 营销队伍专业化配备，给客户印象深刻；
- ✧ 业务办理效率提高30%；

13 缩略语

缩写	全称	解释
AR G3	the Third-Generation Access Router	第三代接入路由器
ASG	Application Security Gateway	应用安全网关
NVR	Network Video Recorder	网络视频录像机
CCU	Cabinet Control Unit	机柜控制单元
SVN	Security Virtual Network	安全虚拟网络
USG	Unified Security Gateway	统一安全网关
NIP	Network Intelligent Protection	网络智能防护