5G+安全云办公白皮书

中国联通

深信服科技

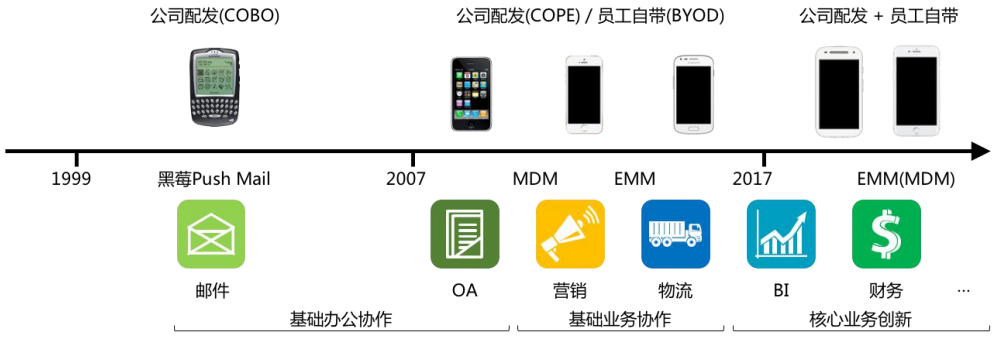
2019 年 5 月

目录

1.引言

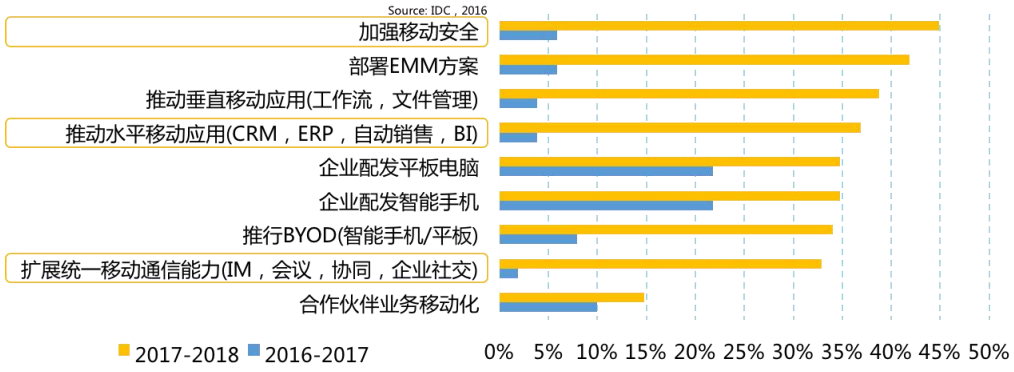
1.1. 移动化办公趋势

1999 年黑莓推出了 Push Mail 移动邮件办公，受到了企业的极大欢迎，因为邮件的移动化，能够有效的提升企业的效率。2007 年之后智能手机的普及，移动化更进一步，移动化从邮件延伸到了 OA、营销、统一通信等基础协作类应用。随着移动互联网和智能手机的发展进步，移动办公进入了优化阶段，从最开始的基础办公协作、基础业务协作，到核心业务创新。



企业移动化阶段与趋势

据咨询机构 IDC 统计，政企用户在 2017-2018 年的规划向核心业务的移动化延伸，例如 CRM、ERP、自动销售系统、BI 系统等；另外，部分政企用户还处在基础业务协作阶段，投资建设 IM、会议、协同、企业社交等应用。在此同时，移动安全的建设投入最大，可见政企用户认为安全问题是企业移动化的前提。



政企用户移动化建设规划统计

1.2. 移动化办公的安全挑战

传统的政企用户移动化办公采用 WLAN 网络或 3G/4G 接入，在终端管理与接入网络安全上存在如下挑战：

1. WLAN 网络接入安全挑战

无线网络的发展与普及正在改变企业网的架构，从 802.11a 到如今的 802.11ac，传输速率及调制方式均有大幅的提升，但企业网对网络安全及业务管控的要求均是现有无线技术所欠缺的。相对于有线网络来说，无线网络只是依靠电波来传送与接收，入侵者可以通过高灵敏的接收设备来进行破坏与入侵。传统无线采用 PSK 认证方式存在严重的安全缺陷，各种破解手段众多，对于企业而言，可能造成内部资源信息的泄露。同时，一旦接入企业无线局域网，黑客通过简单的方法即可获得此网中站点的 MAC 地址，然后利用这些 MAC 伪装地址进行更进一步的欺骗攻击。

2. 3G/4G 网络接入安全挑战

相比 WLAN 网络，3G/4G 网络拥有更高的安全性，通过与 VPN 的配合，能够满足政企用户的日常移动办公需求，但随着政企用户业务需求的复杂度逐步提升，产生了大量的语音、视频、数据采集等场景，对高带宽与实时性提出了跟高的要求。4G 网络理论值可达每秒 100M，但实际上当用户共享使用以及受到实际的网络覆盖影响时，实际访问速率均受影响，无法承载高带宽、实时性的移动化接入业务。

3. 移动接入终端安全风险

政企用户业务移动化时终端也会带来诸多泄密风险，如设备丢失，USB 拷贝，微信 QQ 分享，明文传输被监听，中间人攻击，入侵窃取服务器机密文件等等，防不胜防。可以说，数据泄密问题也是移动办公建设的拦路虎。

1.3. 5G 带来移动办公新体验

5G 作为下一代移动技术，可实现 10Gbps 的吞吐率、1ms 的端到端时延，支持每平方公里 100 万连接，在 500km/h 时速下依然可以正常连接，另外还有网络

切片，边缘计算，毫米波等众多特性，这些性能的提升和新的特性，必将解锁全新的应用，让网络的实用场景更加广阔，而这些应用是在 4G 时代不可能或者不实用的。

1. 更安全的移动办公

利用 5G 网络实现终端到边缘云端及远端的端到端互联，通过 VPN 及其他技术进行数据的加密，解决了移动办公的安全问题，能够加速政企客户的关键业务的移动化部署。

2. 更丰富的移动场景

5G 网络解决了带宽与实时性的问题，无论是固定场所办公大楼的终端办公，还是移动场景的远程接入办公，无论是日常办公还是高带宽的视频、数据采集场景，均可利用 5G 网络接入。

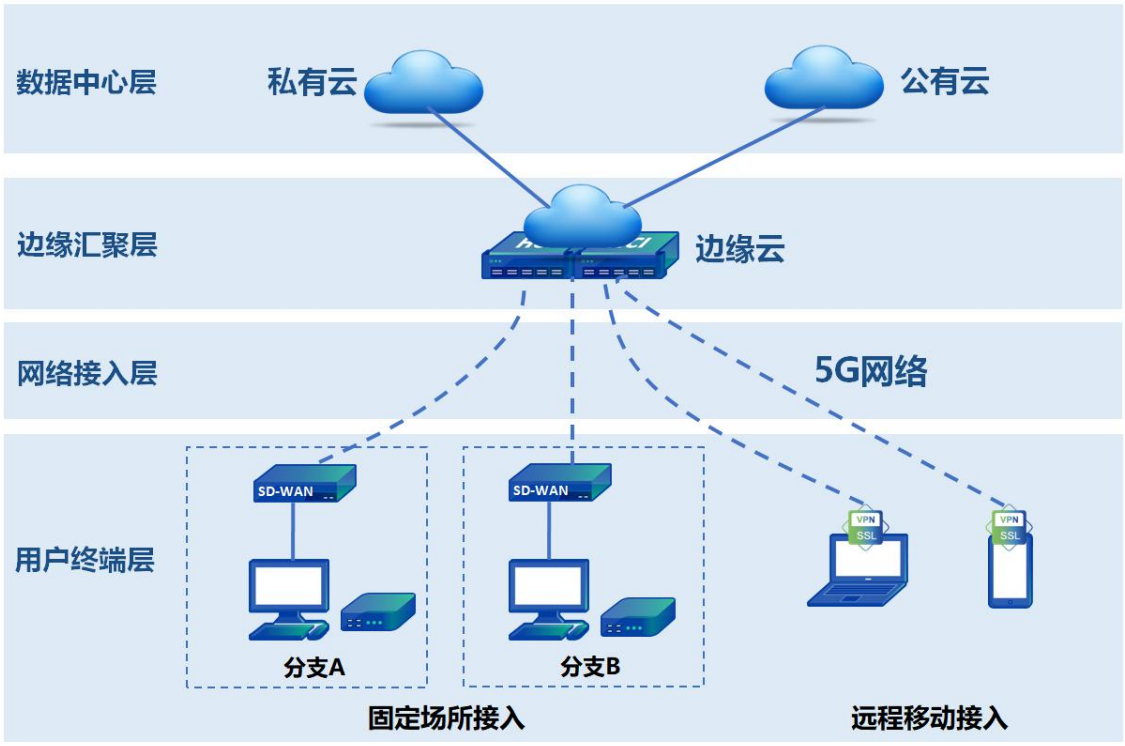
3. 更简洁的终端设计

利用 5G 网络的边缘云设计，可以将终端的计算工作量上移至边缘云节点，终端可采用极简的设计，既可以降低终端的复杂度减轻运维工作量，同时通过边缘云端丰富的策略保障了数据的安全性，降低了数据泄密的风险。

2.5G+云办公的整体架构

2.1. 5G+云办公的整体架构

5G+云办公利用 5G 网络接入技术，提供从终端到接入网络、边缘云的端到端解决方案，能够满足政企用户多场景的移动办公需求。5G+云办公的整体架构如下：



一、 用户终端层：

分为固定场所接入与远程移动接入两个场景：

1) 固定场所接入：采用基于 5G 场景的桌面云为分支提供办公解决方案，在分支端只需要部署 5G 桌面云终端即可，在边缘云部署桌面云服务器，通过 5G 网络提供的高速带宽满足桌面云的实时访问需求；
2) 远程移动接入：当用户端采用笔记本、平板电脑、手机等远程接入时，在边缘云部署移动安全管理平台 EMM，为终端提供一站式安全接入与管理解决方案，解决移动终端的安全接入问题；

二、网络接入层：

当政企用户有多个分支时，需要实现分支间的互联，或分支与云端的互联时，可以采用基于 5G 的 SD-WAN 解决方案提供高速的安全互联通道。

三、边缘汇聚层：

在边缘汇聚层部署边缘化，融合了桌面云资源池与移动安全管理平台 EMM，同时能够提供虚拟的资源池承载政企用户的移动办公应用。

使用边缘云服务降低终端与云端的响应时间，为用户提供高速、低延迟的接入服务，满足视频、高并发、实时业务的移动办公需求。

四、数据中心层

当政企用户使用了私有云或公有云服务时，边缘云的移动办公应用还可以通过SD-WAN与私有云或公有云进行互联互通，构建混合型的云数据中心架构。

2.2. 端到端的数据加密

2.2.1. SSL 协议加密传输

SSL VPN依托于内嵌在各种浏览器当中SSL协议（RFC2246）。它是一种安全可靠的协议，包括以下三个协议：

握手协议：客户和服务器之间相互鉴别-协商加密算法和密钥-它提供连接安全性，有三个特点身份鉴别，至少对一方实现鉴别，也可以是双向鉴别协商得到的共享密钥是安全的，中间人不能够知道协商过程是可靠的；

记录协议：SSL记录协议建立在可靠的传输协议（如TCP）之上它提供连接安全性，有两个特点保密性，使用了对称加密算法完整性，使用HMAC算法用来封装高层的协议；

警告协议：这个协议用于每时示在什么时候发生了错误或两个主机之间的会话在什么时候终止。

通过SSL协议将IP层以上的数据都通过SSL协议进行封装为5G+云办公提供端到端的数据加密通道。

2.2.2. 支持国产商用密码标准

数据加密是信息安全体系中重要的安全保障环节，随着科技的不断发展，常用的商业密码算法（如DES,RSA,MD5等）已确认可被破解。密码技术存在短板，安全设备就形同虚设，只有采用相对安全的密码算法，才实现真正的网络安全。因此，国家密码管理局出台了新的密码算法（SM1，SM2，SM3，SM4）并要求相关单位

选用国产商用密码标准。5G+云办公支持常见的国际通用商用密码算法，同时也支持国密局规定的国产商用密码标准，全面保障用户的业务安全。

2.2.3. 量子加密技术

量子通信加密技术本身并不是一种密码算法，而是利用量子物理，特别是量子纠缠的神奇特点来实现传统的加密算法的密钥协商（分发），简称量子密钥分发（Quantum Key Distribution，QKD）。由于这种特点，QKD 主要的应用是不断给用户更新密钥，而不能像公钥密码体制那样进行数字签名和用户身份认证。通信双方在进行保密通信之前，可以依靠 QKD 系统来“分发”这次加密算法所使用的密钥。由于量子纠缠状态的“不可测性”这一基本物理定律的保障，使得人们从理论上得到了安全性保障，即如果有人企图“偷听”密钥的传递，那么处于纠缠态的量子对就会发生坍塌，从而让通信双方得知此次密钥的传递发生了问题，于是可以再次协商、再次传递…。

利用量子密钥作为会话密钥可增强加密通信数据的机密性，5G+云办公可支持将量子加密技术作为可选的数据加密技术以进一步提升 5G 数据传输的安全性。

2.2.4. 硬加密技术

单一的软认证方式易被窃取，为了进一步提高身份认证的安全性，基于 5G 的安全云办公支持硬件特性的加密认证技术，可以利用硬件特征码、USBKey、动态令牌认证等方式进行硬件加密。

硬件特征码加密通过终端的硬件特征码绑定实现硬件终端的唯一标识。通过获取客户端的不可改变的硬件信息，如 CPU、硬盘、网卡等信息生成数字证书，并对证书和用户进行绑定实现用户身份的唯一性控制。

基于数字证书的 USB KEY 认证，将 CA 中心生成的数字证书颁发给 USB KEY，并为该 USB KEY 设置 PIN 码。通过硬件存储数字证书+PIN 码的方式保证

提供用户高安全的认证方式。同时客户端无需安装驱动即可使用 USB KEY 进行登录认证，大大提高了客户端使用的易用性。

动态令牌认证也是技术领先的一种硬件的双因素身份认证体系，内嵌特殊运算芯片，以事件同步的技术手段，通过符合国际安全认可的 OATH 动态口令演算标准，使用 HMAC-SHA1 算法产生 6 位动态数字进行一次一密的方式认证。由于实际上的安全问题都和密码有关，盗窃和破解密码是最常见的口令攻击手段，因此动态令牌很好的解决了以上问题，为用户的使用提供了极高的安全性保证。

3.用户终端层

3.1. 固定办公场所接入

在 5G 出现之前，政企用户的信息化建设几乎还是采用传统 PC 的办公模式为主，而传统 PC 属于独立计算模式，操作系统、应用程序及数据都与每台硬件设备紧密关联，即各组件绑定于每台用户 PC 上，只要其中一个环节出现问题，桌面将无法正常使用。所以长期以来，新桌面上线、软件的安装与管理、安全补丁的复杂部署、系统升级的版本冲突等问题已然成为桌面 PC 面临的最大挑战。同时随着 PC 需求量不断增加，桌面管理复杂度将呈指数级增长，并引发更多的终端安全隐患，这就需要投入巨大的精力及成本加以解决。

桌面云的出现解决了 PC 终端管理的问题，但由于带宽的限制，桌面云还需要在局域网场景下部署，政企用户获得桌面云的成本较高、运维压力较大，影响了用户的使用体验与业务效率的提升。

5G 出现后将改变这一局面，在用户端仅需部署桌面云瘦终端即可，后端服务器可以部署在边缘云节点，用户可以快速获取桌面云服务而摆脱繁重的运维工作量。

3.1.1. 5G 场景的桌面云架构

5G 场景的桌面云架构仅需要 5G 云终端、部署在边缘云的桌面云资源池（预装桌面虚拟化、服务器虚拟化、存储虚拟化等软件平台）两种硬件，即可完成 5G 架构下桌面云的搭建。

其中桌面云资源池出厂预集成了服务器虚拟化、存储虚拟化、桌面虚拟化（控制器）等软件平台，用户无需复杂的安装调试过程，将桌面云资源池开机之后，只需要按照向导式配置界面执行几个操作步骤，即可完成桌面云部署上线，非常方便快速。

5G 云终端既可以通过交换机级联后通过连接 5G CPE 的方式与边缘云互联，在未来也可以内置 5G 模组支持 5G 云终端与桌面云资源池的直接互联。

3.1.2. 简单易用的 5G 云桌面

5G 云终端支持如下特性简化用户的使用：

一、单点登录与一体化关机

采用单点登录技术，将云终端认证、操作系统认证合二为一，在通过 VDC 云终端严格认证之后，无需再次进行虚拟应用和虚拟桌面的认证，让用户从开机到进入云桌面，全程只有 1 次登录动作。同时可实现联动关机，用户只需点击 1 次云桌面“关机”按钮，终端与桌面将一体化关闭，保留与原有 PC 一样的使用体验。

二、图形化 Web 控制台

通过形象、简洁的单一图形化 Web 控制台进行云桌面服务器和虚拟机的统一管控，IT 管理员可以快速配置整个桌面云环境，降低 IT 管理复杂度与成本，并对

所有关键组件（包括 CPU、内存、存储和网络）提供全面、清晰的性能监控。

三、用户自助恢复快照

允许桌面云的最终用户在桌面导航条上查看自己桌面的快照信息，并选择需要恢复的时间点，将该桌面恢复到某个时间点的状态。从而在桌面发生崩溃、重要数据发生丢失、系统中毒无法恢复，例如 WannaCry 等情况下，无需管理员介入即可自助完成系统重置到用户选择的时间点。

四、在线消息推送

在办公期间，企业经常需要给一些员工发送相关通知，而大多时间采用发邮件或通讯工具的方式，由于员工使用邮件和通信工具的习惯问题，经常会有大量员工未及时查看通知内容，相关工作受到影响。

为了方便公司对员工进行消息推送，桌面云具备在线消息推送功能，可对所有用户或者选定的用户进行消息统一推送，在使用最频繁的办公设备上增加消息推送后，可极大地提高了消息传递的时效性和覆盖率。

3.1.3. 极致体验的 5G 云桌面

在 5G 网络环境中，结合桌面云的应用优化协议，能够给用户提供极致的访问体验。

一、SRAP 高效交付

云桌面需要通过网络交付给前端设备，其中最重要的组成部分就是桌面交付协议。为实现云桌面的高效交付，为虚拟桌面及远程应用程序设计并研制了 SRAP 协议，采用高效流压缩、智能数据缓存、动态图像优化等多项优化技术，相对 RDP 协议提升 6 倍传输效率，最大程度保障用户桌面体验。

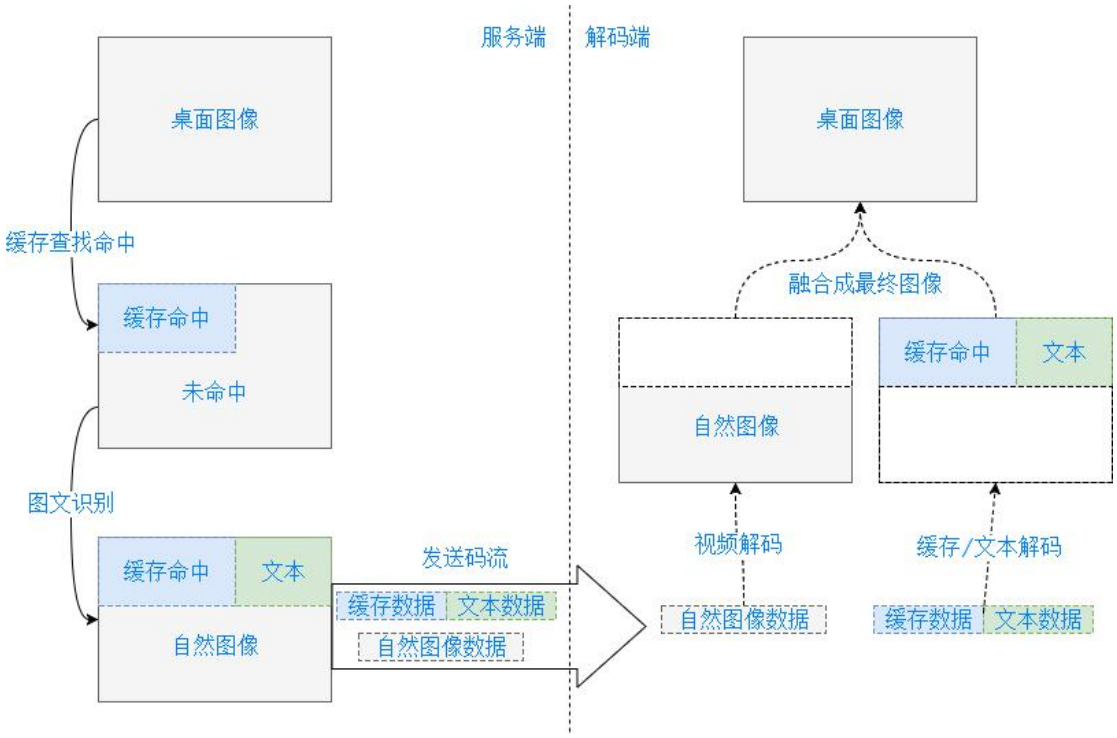
二、HEDC（High Efficiency Desktop Coding）

远程桌面传输的目的在于以较低的流量传输服务端画面到客户端，因此需要设计针对桌面图像（其由计算机产生，往往内容干净、重复模式多，有别于视频图像）的压缩算法。在 5G 场景下通过高效能桌面编码方案（HEDC，High Efficiency Desktop Coding），来削减桌面内容传输所需的带宽，改善用户的使用体验。

HEDC 编码方案如下图所示，基本思路如下：

1. 先用缓存去除当前画面中与历史信息相同的部分（冗余数据）；
2. 然后对未缓存命中的区域进行图文识别，分类为文本和自然图像两类；
3. 文本图像使用无损压缩算法，自然图像部分分离出来并使用视频编码技术进行压缩；
4. 最后把编码后的数据发送出去，其中自然图片部分是独立的视频码流。

HEDC 解码过程则是解出码流中的各个部分的数据然后还原成桌面图像。由于自然图像数据是封装为视频码流进行发送，因此可调用第三方视频解码库甚至硬件解码器进行解码。



基于 HEDC 在办公场景缓存命中率高达高达 95%，各场景对带宽需求如下：

虚拟机使用细化场景	所需带宽 (kbps)	
	下行	上行
静默	7	7

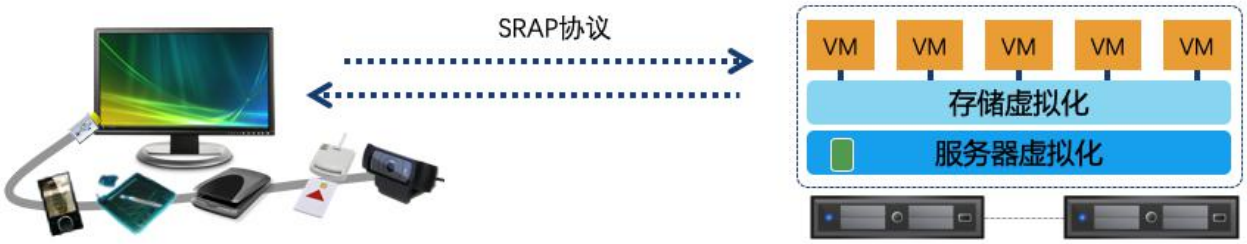
（桌面静止，用户无操作）		
office 打字 （输入中文字符频率 180 字/min）	95	10
PDF 浏览 （图文，滚动频率 0.6s/次）	150	10
PPT 播放 （图文，滚动频率 0.6s/次）	820	20
画图窗口拖动 （图片，300*400 窗口大小）	100	20
图片浏览 （1080P 图片，快速播放）	700	20
门户网站 （图文，有动图；滚动频率 0.6s/次）	860	55
OA 网站 （图文，无动图；滚动频率 0.6s/次）	450	20
视频播放 （QQ 影音，1080P 全屏播放）	4000	50

二、视频重定向与硬件解码

传统桌面虚拟化方案在播放高清视频时主要采用服务器解码和播放，然后将变化中的图像按帧传输给前端显示设备，但这种方式对服务器性能要求高，且非常占用带宽资源，往往效果不好。在 5G 场景下通过视频重定向与硬件解码技术，将视频文件重定向到瘦终端上，并利用 ARM 视频芯片实现解码播放，不仅大幅提升视频播放流畅度，更有效降低服务器资源消耗，提升虚拟机部署密度。

3.1.4. 广泛兼容的 5G 云桌面

桌面外围设备简称“外设”，是指连在桌面终端侧外围的硬件设备。对数据和信息起着传输、转送和存储的作用，是桌面云系统中的重要组成部分。如下图所示



✓ U盘、USB摄像头、扫描仪
✓ 证件阅读器、打印机、扫描仪
✓ 串口、并口等

市面上的外设各式各样，特别是 USB 外设，一种接口能兼容众多的外设，这也是 USB 协议的优势；如果从外设使用的接口类型来分，主要分为如下几种：

- USB 口；
- 串口；
- 并口；

如果从外设提供的功能来分，则种类繁多，如：U 盘、移动硬盘、摄像头、智能卡读卡器、UKey、加密狗、打印机、扫描仪、高拍仪、USB 耳机、指纹仪、证件阅读器等设备，而且有些设备还兼有多种功能。

外设技术是“外设重定向技术”的简称；是指在桌面云场景下，把终端侧的外围设备，通过桌面协议映射到虚拟机中，并能通过虚拟机使用这些外围设备的技术。同一款外设，如 U 盘、证件阅读器等外设使用通用 usb 重定向技术，像 usb 摄像头、串口、并口会有特定的重定向技术。

通过外设技术，允许将外设连接到终端上，外设驱动安装于服务器上，然后可以如本地桌面一样使用各种外设。通过总线映射技术在终端与云桌面之间构建一条专用的外设隧道，用于传输各类外设调用指令，完美兼容扫描枪、扫描仪、摄像头、密码小键盘、二代身份证读卡器、手写板、打印机映射、USB-key 等常见外设。

3.1.5. 显卡虚拟的 5G 云桌面

如果桌面云涉及到专业 3D 软件、视频监控、W10 等高端应用场景，普通的服务器就无法保障效果，甚至无法兼容这些软件，这时需要显卡虚拟化技术。

GPU 虚拟化的发展，经历了从软件共享 GPU 到 GPU 透传，再到硬件 GPU 虚拟化的演进。

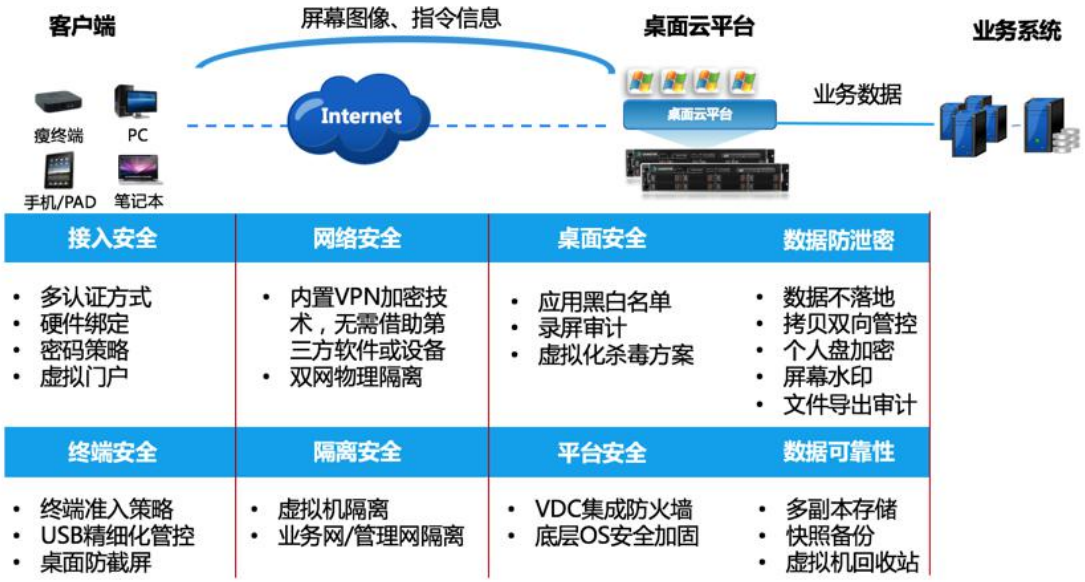
GPU 直通（pass-through）：显卡直通方案是通过 vfio 技术把显卡的 GPU 核透传给单个虚拟机使用，该技术将物理 GPU 核心 1:1 的映射到虚拟机中，给虚拟机呈现一个在功能和性能上都和物理 GPU 一致的设备。显卡直通的方案同样对 GPU 无硬件虚拟化的要求，因此普通显卡也能使用。但是这种方案要求每个虚拟机配置物理显卡核心，以英伟达的显卡为例，核心数较高的 M10 每张卡也仅仅只有 4 个物理核心，因此单台服务器能支持的 3D 用户数量非常有限，整体成本很高，当前体验也是最好的。

GPU 虚拟化（vGPU）：GPU 硬件虚拟化就是将显卡进行切片，并将这些切片分配给虚拟机使用。支持显卡硬件虚拟化的显卡可以根据需要切分成不同规格的时间片，因此可以分配给多台虚拟机使用。以英伟达 Tesla M60 为例，单个显卡最多可以虚拟化出 32 个 vGPU，支持 32 个用户同时使用。M10/M60 显卡可以根据不同场景和负载的需求，虚拟出不同规格的 vGPU，并能支持 3D 虚拟机在 3D 服务器之间迁移，这些都是新一代显卡虚拟化比较突出的特色功能。

5G 云桌面支持多种不同的显卡切分类型，管理员在设置虚拟机的时候可以根据用户的需求灵活的分配显卡资源，显卡的切片最小范围为一个物理核心，不同的物理核心可以做不同的切片。在 vGPU 模式下，整个集群中的 GPU 资源会做为一个资源池灵活的调度给最终用户使用，用户关机后会自动释放授权和硬件资源到资源池。

3.1.6. 安全可控的 5G 云桌面

根据桌面云面临的安全威胁和挑战，桌面云的数据安全安全解决方案如下图所示：



✓ **终端安全与接入安全**

- 接入终端操作系统安全、接入终端合法性校验。
- 通过用户名密码认证、U-Key 认证、硬件特征码认证、第三方认证服务（LDAP、Radius、CAS）认证、动态口令等多种认证方式、组合认证方式对接入桌面云的用户进行认证。
- 通过外设精细化控制，限制可用的外设品类、型号。

✓ **网络&隔离安全**

- 通过物理网络隔离、数据中心防火墙、传输加密、边界安全网关联动等手段，防范网络安全威胁。
- 内置 VPN 数据传输加密技术。
- 通过分布式防火墙限制东西向数据流动。

✓ **虚拟化安全**

- 引入 Hypervisor 层 WAF，提高 Hypervisor 抗攻击能力。
- 依据平台分层机制，保证虚拟化各层隔离安全。

✓ **虚拟机及桌面安全**

- 通过引入杀毒软件、应用控制、网络访问控制、虚拟机行为监控、软件分发、映射控制等保证虚拟机运行安全。

✓ **数据安全**

- 引入分布式虚拟存储技术，使用双副本方式实现数据安全存储。
- 通过桌面安全水印防止用户拍照导致数据外泄。
- 提供个人数据加密、数据访问控制、虚拟机数据传输控制保证用户数据安全。

✓ **管理安全**

- 从管理员账号、密码、权限、日志等方面提供日常运维管理的安全措施。

3.2. 远程移动办公接入

当政企用户通过自有笔记本电脑、手机，打印机，会议终端等设备远程接入网络时，可通过移动安全管理平台 EMM 提供各种安全和移动 APP 集成特性，将政企用户 IT 基础设施与 5G 移动网络和移动终端集成，将政企用户 IT 应用延伸到移动设备上，用以提升企业业务效率、提高员工工作满意度、降低企业成本。

移动安全管理平台 EMM 支持端到端的移动安全方案，保护政企用户 IT 数据在移动业务流中存储、传输的安全，降低因数据泄露而对业务造成的经济、法律、品牌等方面的风险。

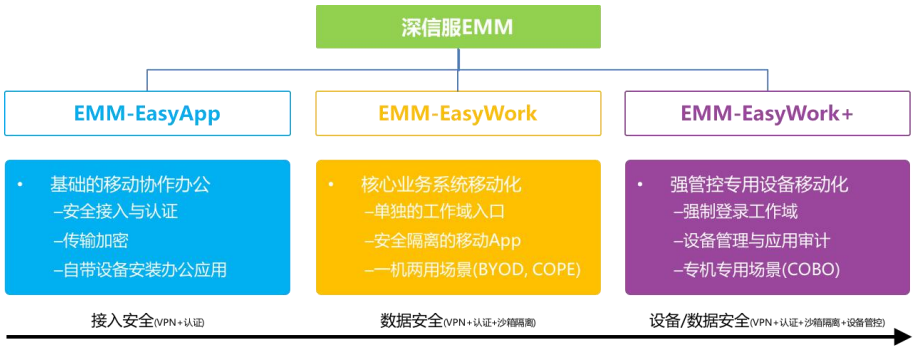
移动安全管理平台 EMM 还可以减少政企用户 IT 和动化安全保护实施门槛，通过高兼容性和易用性设计，支持员工主流的智能手机，免开发支持移动业务 App 的安全封装，并且提供一站式的移动应用商店服务，加速企业移动业务 App 上线之后的全员覆盖。

移动安全管理平台 EMM 在提供安全保护的同时，提供 App 高用户体验，不改变员工的移动应用使用习惯，保证员工的满意度，提升企业应用的使用率，真正的落地政企用户业务移动化，最终提升政企用户业务的效率，并为政企用户未来利用移动化进行业务创新打下基础。

3.2.1. 5G 场景的 EMM 架构

5G 场景的移动安全管理平台 EMM 架构上包含移动终端、统一认证与安全接入、自动化封装服务、企业应用商店、移动设备管控五个逻辑组件，其中自动化封装服务、企业应用商店、移动设备管理合称为移动数据安全管理平台，该平台可部署在边缘云节点。移动数据安全管理平台与企业应用服务器和认证服务器对接，完成移动 App 与企业 IT 基础设施的集成。

移动安全管理平台 EMM 包含 EMM-EasyApp、EMM-EasyWork、EMM-EasyWork+三个子方案，满足不同客户不同移动化阶段的需求。



EMM-EasyApp

EasyApp 支持移动办公应用 VPN 安全接入。移动 App 通过轻量级 SDK 集成或自动封装，快速支持 VPN 接入，保护数据传输安全；移动应用服务器部署在内网，系统信息和漏洞被隐藏，有效降低恶意攻击和入侵的安全风险。加固后的安全应用可以安装在员工手机上(BYOD)和企业配发设备上(COPE)，快速满足移动邮件、移动 OA 等基本的移动办公需求。

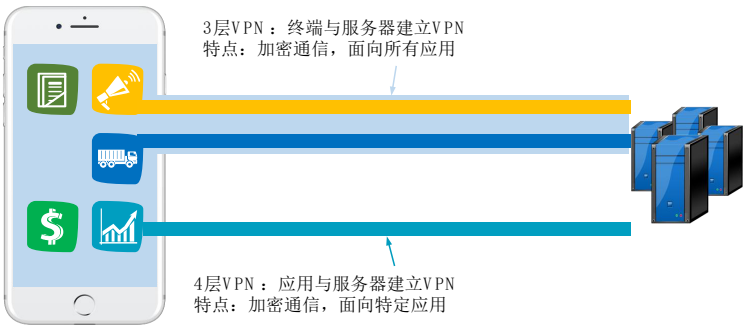
EMM-EasyWork

EasyWork 支持安全工作域数据安全。提供统一的移动工作域，内置安全邮件客户端、安全相册等基础应用，企业可通过自动封装加固，快速新增安全应用，如移动 CRM、移动 ERP 等。安全应用完全与个人域隔离，防止 USB 拷贝、社交共享、剪切板、截屏等手段泄密，满足企业使用员工设备(BYOD)或企业配发设备(COPE)进行核心业务移动化需求。

EMM-EasyWork+

EasyWork+支持移动数据安全与设备严管控制。设备开机强制进入安全工作域，用户只能使用工作域中的应用，如移动展业、移动营销等应用，防止使用个人应用影响效率。在应用安全隔离的基础上，对外设和网络连接进行严格控制，并支持多种安全合规审计，更进一步降低数据泄密风险，满足企业使用配发设备(COBO)进行强管控的核心业务移动化需求。

移动安全管理平台 EMM 采用 SSL VPN 技术进行加密，支持 3 层 VPN 和 4 层 VPN 接入。3 层 VPN 支持承载多个移动 App 的数据加密传输，4 层 VPN 支持一个移动 App 的数据加密传输。



3.2.2. SSL 传输加密

移动安全管理平台 EMM 的移动应用采用安全的 SSL 加密协议，保证移动 App 在传输中的安全。SSL 协议具备良好的安全性和网络穿透性，广泛适用于各个行业的安全传输加密。

3.2.3. 移动安全工作域

移动安全管理平台 EMM 向员工提供移动应用安全工作域，是移动应用的统一入口，所有的移动应用均可以快捷的访问，减少员工需要区分个人应用和工作应用造成的不便，提升应用体验。

完美支持一机两用模式，政企用户数据在个人设备上被完全隔离，能够防止个人设备病毒木马的恶意攻击，以及员工的有意无意泄密。员工离职或者设备丢失之后，可以远程擦除设备上的企业数据，保证政企用户的数据安全。同时，政企用户应用不会对个人的应用造成影响，完全保护员工个人应用的隐私，使得员工工作和生活两不误。

对于政企用户的核心生产系统，会配置专用的移动设备来支撑业务，这些设备仅能用作业务，不能用于个人用途，例如微信/QQ 聊天，或者存储个人文件或照片等。这种专用设备必须被企业有效管理，保证设备本身和设备上企业数据的安全。同时，专用设备可以被管理员进行全生命周期的设备管理，包括 Android 系统的基础功能管控、数据通道管控、应用使用管控等等。

3.2.4. 设备可信准入

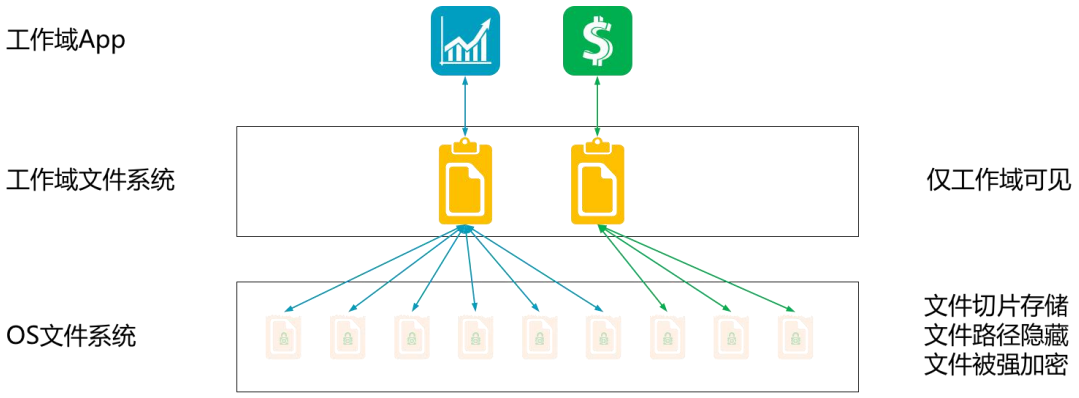
移动安全管理平台 EMM 支持多种身份认证方式，例如本地数据库认证、Radius 认证、LDAP/AD 认证、CA 认证、硬件特征码认证、手势认证等，满足客户不同的认证需求。

3.2.5. 移动安全隔离技术

采用创新的沙箱隔离技术，将工作域中的应用与个人域完全隔离，包括剪切板、文件系统、文件分享、网络传输等等，有效的防止个人域病毒木马攻击的同时，阻止员工恶意泄密的行为，保护政企用户的敏感数据的安全。

一、文件加密隔离技术

EMM 创建了一个完整的虚拟文件系统，这个文件系统只能被工作域中的 App 和服务访问。工作域中的 App 访问文件系统时，会调用工作域中的文件 API，之后工作域文件系统会调用个人域操作系统的文件系统，写入数据后进行强加密，或者解密后读取文件信息。



安全域文件在操作系统中存储时，采用分片存储的方式，而且文件路径对个人用户隐藏，即使黑客获取了分片文件，也很难合并成完整的文件，而且文件经过了高强度加密，进一步保证了文件的安全性。

二、剪切板隔离技术

EMM 安全域的剪切板与个人域也是隔离的，在企业移动 App 中拷贝的数据只能拷贝到其他企业移动 App 中，无法拷贝到个人域的应用中，防止员工将敏感信息有意或者无意泄露到互联网中，造成企业不可控的损失。

三、文件分享隔离技术

在移动社交网络发达的今天，在移动设备上进行文件信息分享非常方便，已经形成一种习惯。但是文件分享会对企业信息造成安全威胁，因此 EMM 方案提供移动应用分享隔离的方案。企业 App 中的文件只能在安全工作域内进行分享，而无法分享到微信、QQ、百度云盘等互联网应用中去。

四、防截屏技术

员工使用手机截屏功能能够获取移动办公应用的敏感信息，因此 EMM 方案提供企业应用防截屏的功能，防止员工截取企业敏感信息进行泄密。

3.2.6. 移动设备管理管理

移动设备管理解决方案支持对移动设备进行管理，包括设备注册、设备擦除、用户关联、策略关联、状态监测等功能，帮助管理员管理轻松管理海量设备，降低运维成本。

3.2.7. 应用安全封装

管理员在 EMM 后台上传 APK、IPA 文件之后，填写应用信息，选择需要封装的安全特性，即可提交 EMM 平台封装。

一、支持 iOS/Android 主流版本

采用系统底层技术进行安全代码的自动封装，支持 iOS 和 Android 的主流版本，兼容性具备天然的优势，覆盖员工使用的移动设备的各种机型和各种版本，避免因为版本不兼容造成的 IT 运维成本。应用封装之前，管理员获取 Android 或者 iOS 企业应用，上传到 EMM 平台。

二、安全策略封装

EMM 方案支持双域隔离应用的安全封装，封装之后，企业 App 具备安全隔离的功能，使得企业 App 快速获得移动应用数据安全的能力，包括剪切板隔离、分享隔离、文件隔离等。

3.2.8. 应用商店管理

支持一站式的企业应用商店服务，移动应用进行安全封装之后，即可通过应用商店后台进行统一的发布，员工即可在 EMM 客户端中应用商店进行应用的下载或者更新。

4.网络接入层

4.1. SD-WAN 组网

4.1.1. 5G 场景的 SD-WAN 定义

Software-Defined Wide Area Network（SD-WAN），即软件定义广域网络，是将 SDN 技术应用到广域网场景中所形成的一种服务。这种服务用于连接广阔地

理范围的企业网络、数据中心、互联网应用及云服务，旨在帮助用户降低广域网的开支和提高网络连接灵活性。SD-WAN 具备如下特征：

一、支持按照应用和网络质量实时动态选路

网络作为业务访问的必备通道，网络体验是越来越得到重视，而过去对这部分业务体验的管理比较粗放，当网络中断或拥塞时业务开展等都会受到影响。为了保证网络可用性，政企用户会在分支、总部、数据中心等购置多条物理传输链路。传统 VPN 只能使用静态配置将特定业务固定在指定链路上，也不支持对链路质量进行实时监测，很容易造成优质链路资源的浪费或过于拥塞导致体验不佳，也极易造成链路使用不均衡。

SD-WAN 最重要的特征是在 UNDERLAY 物理网络上并发构建 OVERLAY 多通道线路，并实时监测各线路 QOE（丢包、时延、抖动等参数），并以此为依据，进行智能化、精细化流量调度。需要支持识别客户业务，并能调整业务优先级，将重要业务手动指定到优质链路，或自动识别优质链路资源。当链路中断时，能在 1 秒内切换到备援链路；当链路实时网络质量不足以保证特定应用的体验时，可自动切换到其他可满足性能要求的链路，这些均为 SD-WAN 智能选路的最低基本要求。

二、支持网络传输独立性和传输资源虚拟化

随着 5G 宽带质量的不断提升，使用 5G 网络取代或部分取代专线已是大势所趋。SD-WAN 的物理网络可能是专线、互联网宽带，也可能是 3G/4G LTE 或 5G 网络。

为了充分和合理利用这些传输资源，SD-WAN 产品必须要支持将多条线路虚拟成一个大资源池，就像 CPU、存储资源虚拟池化一样，可以支持带宽的叠加和按需调度。

三、支持设备即插即用的易部署

SD-WAN 设备支持设备即插即用的零接触自动配置方式的易部署，设备配置全在中心端进行预配，分支设备在分支正确插上网线后，不需要本地做复杂配置，设备即可连上集中管理设备自动下载指定配置和策略来执行。

四、支持通过集中管理、AutoVPN 等简化管理

当分支规模比较庞大时，对多设备的管理和可视将变得至关重要。如果没有一个统一的集中管理系统，对网络管理员将是一种灾难，通过集中管理产品，只需配置统一模板，几分钟内就可以下发到所有分支，保证了配置的一致性。

同时对全网虚拟隧道的管理和可视也非常重要，管理员需要知道带宽资源被哪些应用、哪些分支所耗费、哪些分支存在故障和告警，以便进一步做故障排除。

4.1.2. SD-WAN 的主要功能

SD-WAN 的主要功能如下：

一、易部署

采用了邮件开局方式，支持在总部端提前配置好分支基础网络、总部接入等信息，将配置加密存储在 URL 链接中发送给分支管理员。通过分支管理员手动点击该链接，配置将自动完成，实施的分支管理员即使没有任何 IT 经验，也可在邮件内容的指导下轻松完成上架部署。

二、应用选路与流控

应用选路和流控是 SD-WAN 的核心功能之一，能实现带宽的最大化利用，以及在不增加带宽成本的同时提升应用传输质量。

1) 指定线路

指定线路功能就是指定应用（服务）优先转发的分支线路，同时能调整指定线路的优先级顺序。在进行数据转发时，优先使用排序靠前的线路进行转发，当前面线路故障时，切换到下一顺位的线路转发数据。

使用选定的线路进行数据包转发时，会优先选择对端相同的运营商线路作为接收端，如果没有在 BBC 中配置运营商信息，则默认选择相同编号的线路作为接收端。当选定的线路都故障时，从未选中运营商线路和跨运营商线路中按照高质量选路方法选择一条最优线路进行数据转发。

2) 高质量选路

选择“优先使用质量最好线路”的负载模式会根据各个线路的实时质量状况（丢包、延时、抖动），选择最优的可转发线路进行数据转发。

根据实时的线路质量状况，可以把不同的质量状况做一个转换，转换成同一标准，此时就可以对不同线路进行质量排序（权值越小，质量越优）。

权值算法为：权值 = 抖动（ms） * x + 丢包率 * y + 延时（ms）

高质量选路除了考虑线路权值之外，同时也将线路对当前服务优先级的剩余带宽作为选路依据，当线路无法承载当前优先级的应用时，该线路不会被选中。因此高质量选路会选择对当前服务优先级有可用带宽，同时权值最小的线路作为转发线路。另外，当选定线路都无法承载当前服务优先级的数据时，会从未选中运营商和跨运营商线路中选择质量最优线路对该连接进行数据转发。通过多重选择来保证被选中的传输线路质量稳定可靠。

3) 按剩余带宽负载

按剩余带宽负载可以更公平的使用所有外网线路。当连接建立时，获取所有选定线路对于当前应用的可用带宽大小，再生成一个小于总可用带宽大小的随机数，判断该随机数落在哪条线路区间，确定从哪条线路进行发包。

例如：线路 1 剩余 1M 带宽，线路 2 剩余 1M 带宽，线路 3 剩余 2M 带宽，此时生成一个 4M 以内的随机数，如果随机数小于 1M，此时选择线路 1 进行发包，如果随机数大于 1M 小于 2M，此时从线路 2 进行发包，其他的选择线路 3 进行发包，通过随机分配的发包比例为测试最优值。

同高质量选路一样，当选定的线路无法承载当前服务优先级流量时，该线路不会被选中。当所有选定的线路都无法承载当前服务优先级流量时，将从未选中运营商线路和跨运营商线路中按照高质量选路方法选择一条线路进行数据包转发。

通过以上逻辑，每次选路都会按照当前剩余带宽来计算和分配，带宽利用比例均衡。而且还会考虑带宽质量，选路质量稳定可靠。

4) 带宽叠加

选择带宽叠加负载模式，将一条连接的流量负载到多条线路中，达到单连接的最大带宽利用率。此时客户需配置可用于负载的线路的质量阈值，只有在阈值内的线路才可以做为负载线路。如果没有线路符合条件时，会从未选中运营商和跨运营商线路中选择质量最优线路对该连接进行数据转发。

包负载当前有两种负载模式，当设置了片段长度时，每线路发送一个片段后会切换到下一线路进行数据转发。当没有设置片段长度时，每线路会发送到该线路开始拥塞后才切换到下一条线路进行数据转发。当所有线路都拥塞时，不管是否设置片段长度，此时都会将数据包分配到最不拥塞的线路上，减少丢包的数量。

5) 应用流控

在应用选路的基础上加上流控功能，则可以进一步确保核心业务稳定传输，动态保障应用的传输质量。流控技术是在令牌桶方案的基础进行了大量优化，并加入了用户公平调度算法。当前支持用户自定义应用（五元组，可满足大部分内网应用需求，后续会加入应用识别算法，用户直接选择应用即可），并提供 5 种应用优先级选择。当带宽不足时，根据应用优先顺序，高优先级应用会得到优先传输的机会。而低优先级的应用则会因为抢占不到带宽而被切换到其他次优线路上。当相同优先级的应用同时竞争，用户公平调度算法则会根据算法模型给予各应用、用户较公平的数据传输机会。

4.2. 切片网络特性

网络切片就是将运营商的物理网络划分为多个虚拟网络，每一个虚拟网络根据不同的服务需求，比如时延、带宽、安全性和可靠性等来划分，以灵活的应对不同的网络应用场景，具体来说可以分为三类场景：

1) eMBB(Enhanced Mobile Broadband)增强型移动宽带：实现10Gbps的传输速率，适合三维立体视频、超高清晰度视频、云工作、云娱乐、增强现实等；

2) eMTC(Massive Machine Type Communication)大规模机器类通信：实现每平方公里百万设备连接，适合物联网、智慧家庭、智慧城市、智能楼宇等；

3) uRLLC(Ultra-reliable and Low Latency Communication)超高可靠与低延迟的通信：实现超高可靠超低时延通信场景，适合无人驾驶、远程医疗、智能工厂、紧急任务应用等。

在5G+云办公场景下，通过5G切片网络特性，可根据业务应用要求和实时链路质量检测为基础的SD-WAN智能路径控制，可以保证将客户的关键业务跑在最优质的切片上，保证其使用体验。

5.边缘汇聚层

5.1. 构建边缘云的最佳技术

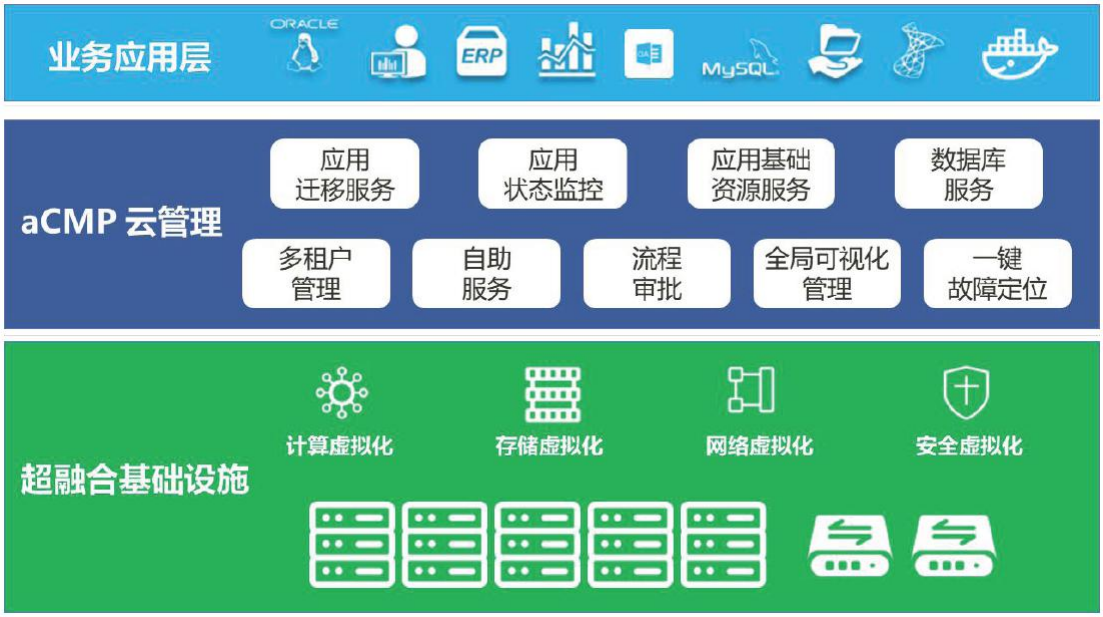
传统的云数据中心建设中，通常而言都是三层网络结构，这三层称之为接入层（Access Layer）、汇聚层（Aggregation Layer）和核心层（Core Layer）。接入层交换机一般会连接服务器，汇聚层交换机连接接入层的交换机，并且一般都会提供其他的服务，比如说防火墙，流量监测等等。一般而言汇聚层是 L2 和 L3 网络的分界点，汇聚交换机以下是 L2 网络，以上是 L3 网络。核心层交换机一般为数据中心进出数据包提供高速转发，并同时为数据中心内的多个汇聚交换机之间的通信提供转发。

随着业务的增长，传统的三层架构只能通过增加物理设备来满足业务发展，此时，数据中心架构的可扩展性成为制约业务发展的关键要素。同时随着数据中心设备增多，系统的故障点也会增加，导致整个平台可靠性下降。最后大量物理设备导致采购和项目上线周期变长。

近年来随着云计算的发展，计算、存储和网络资源纷纷被池化，软件定义的思想开始重构传统数据中心的建设。采用超融合架构构建数据中心逐渐成为数据中心新建的主流，基于超融合架构，只需采用 X86 服务器和交换机两种设备就可以在 5G 网络的城域网边缘构建边缘节点，用于承载云办公的各种业务。通过计算虚拟化提供统一的计算资源池，每一台 X86 服务器作为一个节点，基于分布式的架构，只需要三台服务器或者一体机就可以构建资源池，并且后续该资源池可以根据需要按需扩容；通过存储虚拟化可以构建统一的存储池，通过 SSD 分层和数据条带化来提供高性能，并且采用副本和仲裁为数据提供高可用；通过网络虚拟化来提供所画即所得的网络可编辑性，使得网络拓扑的变更更加简单便捷，基于 vXlan 构建虚拟机东西向流量的承载通道。除此之外，通过各种容错机制来保证系统的可靠性和业务的稳定性，采用模块化、标准化的资源池，提供最好的灵活性来应对边缘云的各种变化。

5.2. 基于超融合的边缘云架构

随着数据与业务的集中，传统的云数据中心的硬件架构已经无法满足业务的快速上线和灵活的业务部署。基于超融合的边缘云架构通过“云管平台 + 超融合架构”方案，基于分布式云数据中心架构，通过软件定义的方式实现全新的 IT 基础架构，通过服务器虚拟化将所有 X86 的计算资源池化、通过网络虚拟化构建出适合虚拟机迁移的大二层环境、最后通过存储虚拟化实现存储空间的融合。基于 VDC 实现多组织/多业务共享资源，按需服务，通过云管平台实现多个数据中心资源的统一管理，同时提供完整的安全和灾备方案。



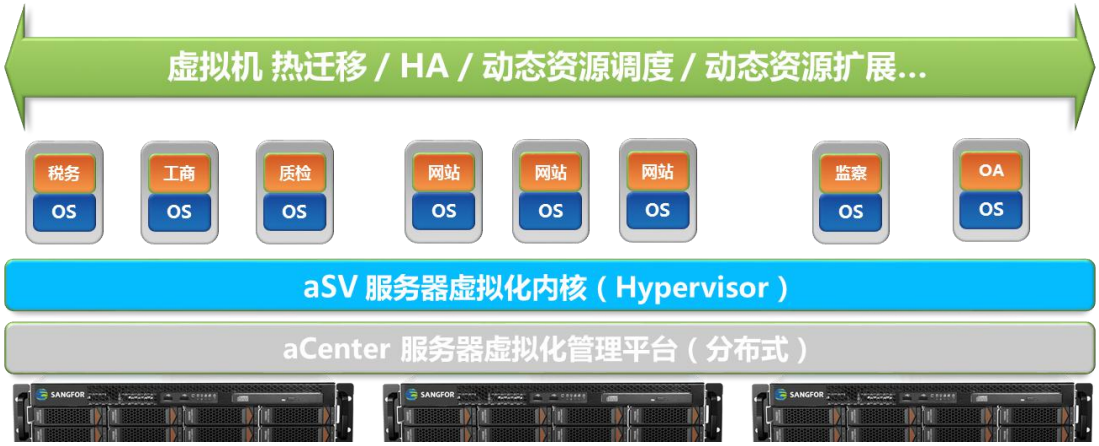
5.3. 边缘云的关键技术

边缘云的关键技术如下：

一、服务器虚拟化技术

服务器是云计算平台的核心，其承担着云计算平台的“计算”功能。对于云计算平台上的服务器，通常都是将相同或者相似类型的服务器组合在一起，作为资源分配的母体，即所谓的服务器资源池。在这个服务器资源池上，再通过安装虚拟化软件，使得其计算资源能以一种云主机的方式被不同的应用和不同用户使用。

边缘云虚拟化平台作为介于硬件和操作系统之间的软件层，采用裸金属架构的 X86 虚拟化技术，实现对服务器物理资源的抽象，将 CPU、内存、I/O 等服务器物理资源转化为一组可统一管理、调度和分配的逻辑资源，并基于这些逻辑资源在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境，实现更高的资源利用率，同时满足应用更加灵活的资源动态分配需求，譬如提供热迁移、HA 等高可用特性，实现更低的运营成本、更高的灵活性和更快速的业务响应速度，如下图所示：



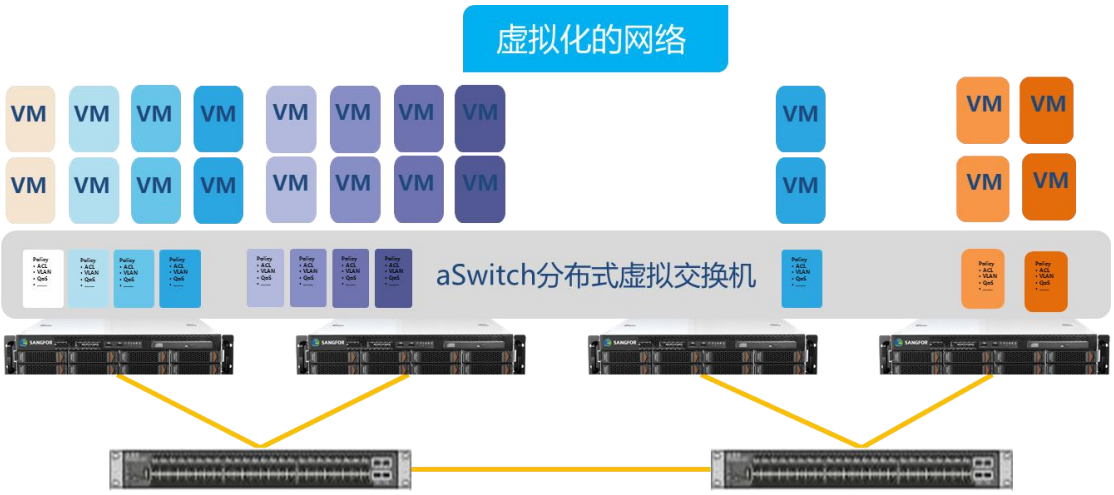
二、存储虚拟化技术

边缘云采用分布式存储技术构建统一的存储资源池，可以形成可横向扩展（Scale-out）的云计算基础架构。在业务应用区部署分布式存储方案，运行在这种架构上的云主机不仅能够象传统层次架构那样支持 vMotion、DRS、快照等，而且数据不再经过一个复杂的网络传递，性能得到显著提高。由于不再需要集中共享存储设备，整个云平台基础架构得以扁平化，大大简化了 IT 运维和管理。利用分布式存储技术构建云平台存储资源池，有效利用服务器资源，降低能源消耗，帮助实现 IT 环境的节能减排。

分布式存储的逻辑架构如上图所示。这种架构的基本单元是部署了虚拟化系统的 x86 标准服务器。在提供虚拟计算资源的同时，服务器上的空闲磁盘空间被组织起来形成一个统一的虚拟共享存储：虚拟存储系统。虚拟化存储在功能上与独立共享存储完全一致；同时由于存储与计算完全融合在一个硬件平台上，无需象以往那样购买连接计算服务器和存储设备的专用 SAN 网络设备（FC SAN 或者 iSCSI SAN）。

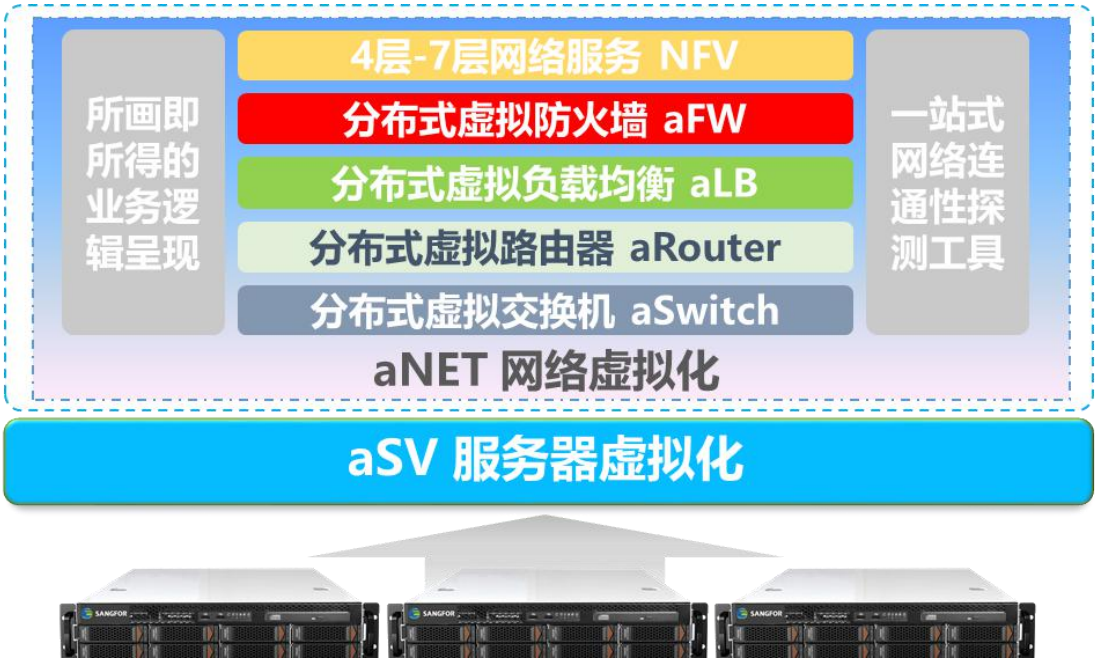
三、网络虚拟化技术

服务器虚拟化技术的出现使得计算服务提供不再以主机为基础，而是以云主机为单位来提供，同时为了满足同一物理服务器内云主机之间的数据交换需求，服务器内部引入了网络功能部件虚拟交换机 vSwitch（Virtual Switch），如下图所示，虚拟交换机提供了云主机之间、云主机与外部网络之间的通讯能力。



网络虚拟化 aNet，通过提供全新的网络运营方式，解决了传统硬件网络的众多管理和运维难题，并且帮助数据中心操作员将敏捷性和经济性提高若干数量级。

网络虚拟化 aNet 方案通过和服务器虚拟化 aSV 相结合，在虚拟机和物理网络之间，提供了一整套完整的逻辑网络设备、连接和服务，包括分布式虚拟交换机 aSwitch、虚拟路由器 aRouter、虚拟下一代防火墙 vNGAF、虚拟应用交付 vAD、虚拟 vSSL VPN、虚拟广域网优化 vWOC 等虚拟网络、安全设备；然后，还可以支持 VXLAN 等增强网络协议，实现和物理网络的无缝对接，简化网络的配置管理；此外，还可以通过虚拟化管理平台，实现网络拓扑部署、网络故障探测等网络管理功能。



从而，aNet 虚拟网络可以快速完成不同应用系统的网络部署，网络配置的自动化调整，网络故障排查等工作，提升网络的管理运维效率，提升网络就绪、扩展速度，降低数据中心物理网络的建设成本。

5.4. 边缘云管理技术

边缘云管理平台将超融合架构构建的虚拟化的全资源池，和第三方的虚拟化平台构建的资源池，通过流程化、自动化的方式，实现资源即服务的交付方式，交付给最终的业务部门或者业务使用者，并实现平台自动化的运维。

边缘云管理平台可以实现对第三方虚拟化管理，比如 Vmware 的 vCenter 等。管理平台采用分布式架构设计，即边缘云管理平台架构集群中，每个节点都可提供相应的管理服务，任何单一节点故障都不会引起整个平台的管理中断。并且平台可提供分级分权的管理，针对不同的平台用户，可以各自使用和管理平台管理分配给的对应资源，并且针对每种资源对象，可以部署更加精细化的权限管理和控制，极大了满足了边缘云平台，构建云化 IT 架构中，多租户使用 IT 资源的灵活性。

6.数据中心层

在数据中心层，随着政企用户业务数字化转型，政企用户可能搭建了自有的私有云或使用了部分公有云服务，边缘云与私有云或公有云的多云互联成为了 5G 安全办公需要解决的问题。

SD-WAN 将多个物理 WAN 链路组合到一个逻辑网络中，并提供流量优先级，以加速应用程序到本地和基于云的应用程序的性能。使用网络抽象，SD-WAN 通过使组织能够利用 Internet 来满足不断增长的带宽需求，从而提高分支连接的经济性。

利用 SD-WAN 的应用识别和流量控制功能，可以更好地支持边缘云对私有云或公有云的安全访问。IT 专业人员可以为每个应用程序和云环境设置特定的业务策略指标，并由 SD-WAN 平台强制执行。他们必须根据可以容忍的延迟程度，对

关键任务应用程序进行优先级排序。例如，它可以为低延迟流量(如统一通信、语音、视频、办公效率应用程序和一般电子邮件)设置不同的策略配置文件。

为了提高安全性，它可以设置关于应该通过哪些 WAN 链接的流量的策略，例如，私有 MPLS 与公共 Internet。SD-WAN 平台提供了关于流量源和目的地的可见性，可用于黑名单来阻止和白名单来加速。他们还可以隔离可疑的交通流。应用程序或平台级别的加密和微分割也可以用来提高安全性。

为响应客户需求，SD-WAN 供应商提高了识别和路由基于云的流量的能力，以加快与本地站点之间的流量。在多云之间部署 SD-WAN 可带来如下价值：

一、降低网络传输资源的资金投入（CAPEX）

通过使用互联网宽带，取代/部分取代了专线资源，而且带宽更大，多条链路的可用性也优于单条专线，当分支众多的情况下，对链路资源的资金投入可节省50%以上。

二、降低部署阶段和运维阶段的管理投入（OPEX）

通过在上架阶段即插即用的易部署方案和运维阶段在集中管理平台对全网的可视可控，大幅降低了客户的管理投入，增强了管理效率，也降低了对分支网络维护人员的能力要求。

三、保障业务访问的体验和安全

通过在分支部署多条链路，并根据业务应用要求和实时链路质量检测为基础的 SD-WAN 智能路径控制，可以保证将客户的关键业务跑在最优质的链路上，保证其使用体验，低优先级业务走较差的链路，充分利用链路资源；通过 NFV 等方式集成安全解决方案，又保证了分支的防护和业务访问的安全性。

7.5G 云办公的几种典型场景

7.1. 固定办公场景

固定办公场景一般有办公室，办公大厅，公共场所便民服务厅等，具体办公场景的不同，对于终端的需求也有差异。

在办公室场景下，网络连接终端需求相对简单，没有特殊的要求，只需要满简单易用，安全可靠即可。比如网速稳定，连接数量满足要求，网络连接安全等基本的连接特性。

在办公大厅的场景下，比如政务大厅，银行大厅，医院大厅等，这里的特色是网络设备的数量终端，需要支持大连接的设备，并且安装的环境也有一些特殊性，比如在建筑墙壁或者屋顶等，在相对长时间内有灰尘进入风险。

在公共便民服务亭场景下，因为空间限制，不能配备良好的环境，对网络终端的需求相对较高，如高温，高寒，灰尘等环境，需要设备可以在严酷环境下工作持续工作，保持长时间的稳定性可靠性。

不同的场景中接入网络的设备不同，对网络带宽的需求也不同，所以终端提供的网络接入能力也可根据所连终端的需求而不同。

固定办公场景中，网络接入终端可选择支持三频（2.4GHz, 5GHz, 60GHz）无线网络中一种或几种，支持有线方式接入，满足用户的多样化需求。终端本身支持加密，网络走专有切片网络，服务云端对终端的接入进行认证及信息解密。这样不管是用户设备支持哪种网络都可以接入，并且网络安全稳定可靠，不管是用于日常办公，还是文件传输，高清视频会议等场景，都能完美支持。设备移动方便，只需要接电源即可开启工作，网络信息配置支持远程配置，省去用户繁琐维护工作。

7.2. 移动办公场景

移动办公环境一般有单人内部办公，单人对外业务，团队对外服务等。

对于个人办公，方便与安全是首位的，因为用户需要多次地对设备进行操作，因此，一键式，统一式是设备操作的原则。终端上尽量少的案件，不同功能切换，动作选择等尽量统一化。还有就是要小巧便捷，工作时间长等。

对于单人对外业务办理的场景，以手提式办公箱形式，集成多种办公设备，设备间以最小连接，指定方式原则形成独立网络环境，无线方式的加密专网连接，在安全，稳定，可靠性方面提供充分的保障。对连接的数量要求不高，也不需要支持长时间工作，只需要保证网络本身的使用体验即可，如足够的带宽，超低的时延，网络数据安全传输等。

对于团队对外服务类，比如政务服务车。办公终端，用户信息读取，采集，信息展示，实时视频互动等需要接入网络，车载网络设备需要支持大量的网络连接，且支持大容量的传输，同时保障信息的安全，网络的稳定可靠。

专家顾问：张涌，迟永生，冯毅，施晓光，张瑜

编写组成员：

中国联通：胡宝命，孟宇，沙婷婷，朱叶，刘海涛，袁月

深信服：封华进 黄航 李全友 周巍 林国强 张武健