华为 BYOD 移动办公安全

解决方案白皮书

华为技术有限公司

二〇一二年八月

商标声明

HUAWEI 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，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 背景介绍

自从iOS和Android为代表的智能手机和Pad推出以来，这些计算和表现能力远超前辈的强大智能终端快速统治了个人通信设备市场。全球知名调研机构IDC的数据显示，2011年全球智能手机出货量预计将达到4.72亿部，而2010年为3.05亿部。据IDC预计，这一数字有望在2015年末翻倍至9.82亿部。

如今很多员工更倾向于使用个人设备，如智能手机和平板电脑开展工作，这使得消费化趋势进一步发展。这一趋势也推动了越来越受企业青睐的“自带设备(BYOD)”计划。然而，从广义上来说，随着IT消费化的发展，即使是非常重要的业务应用也可在消费者界面显示，这一趋势比用户界面发展更为迅猛。

由于单独携带工作用设备和个人设备为用户带来的种种不便，越来越多的用户承认并支持“自带设备(BYOD)”策略。IT消费化为IT构成了巨大的压力，促使他们尽快建立BYOD策略。

来自IDC最新的调研报告显示，与2010年相比，企业移动化部署度过了探索期，已经处在加速阶段。其中受访的企业当中，83%的企业认为平板电脑成为企业未来业务不可分割的一部分；79%的企业高管期望企业支持其通过个人终端进行办公；75%的企业已经开放了BYOD政策；74%的企业认为BYOD成为趋势，不可阻挡；72%的企业认为BYOD能够提高企业效率。但是，在BYOD获得一片赞颂的同时，80%的企业表示BYOD将明显加重IT部门的工作量。

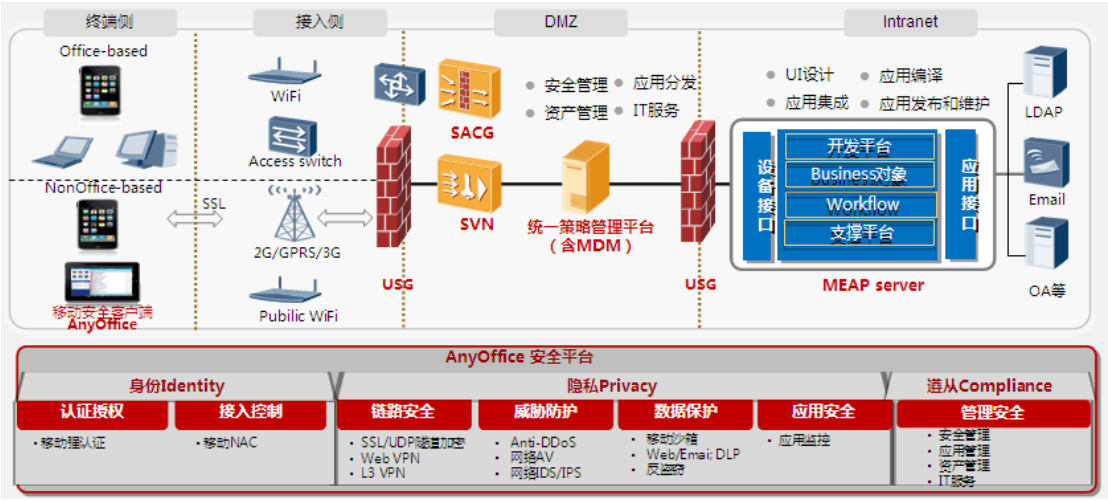
BYOD的移动化接入特性使得企业网络边界重新变得模糊。企业员工既可以通过3G在公共场所接入公司网络，也可以在企业园区通过Wi-Fi接入公司网络。BYOD设备用于办公的特点可以归纳为4A。Any Device——设备和操作系统的多样性；Any Time——随时访问公司网络；Any Location——任何可以接入移动互联网的场所；AnyOne——企业的任何成员。4A的特性使得目前的企业安全体系无法良好地应对，另外，当前不成熟的设备接入授权和管理能力也成为IT实施BYOD时增加工作量的原因。

2 方案概述

华为BYOD移动办公安全解决方案是针对当前BYOD移动办公的需求、特点和挑战，在保障移动办公人员顺畅、安全访问企业的同时，提供高效和良好的用户体验，实现了“安全”、“效率”和“体验”的完美融合。

华为公司凭借在网络通信领域和网络安全的技术积累和优势，在方案中融合了AnyOffice移动办公客户端、SVN2000/5000系列的SSL/IPSec一体化VPN硬件网关设备、SACG、兼具防火墙和UTM功能的USG2200/5100/5500设备、统一策略管理服务器以及移动企业应用平台（MEAP）。

图1 华为 BYOD 移动办公安全解决方案



其中，AnyOffice作为移动办公客户端运行在移动智能终端上；USG作为防火墙和UTM设备部署在企业网络的出入口处，负责攻击防范、网络流量的过滤和监控；SVN可以单臂挂接在出入口防火墙或者交换机上，也可以双臂挂接在防火墙和交换机之间；SACG作为内网用户接入的准入控制网关，旁挂在防火墙之后的交换机或路由器上，也可以透明直路方式串接在两个交换设备之间；而“统一策略管理服务器”和MEAP服务器则一般部署在企业内网的数据中心。

不同于机型统一的企业配机，BYOD设备往往具有机型多样、操作系统多样、版本多样的特点，因此，这些设备在认证、VPN接入、数据加密、MDM安全管控等方面的支持程度、实现技术也存在不同程度的差异。华为公司充分考虑了移动办公的特点、BYOD设备在移动办公应用中的特点，从身份（Identity)、隐私(Privacy)和遵从（Compliance）三个大方面提供了全面完善的端到端的解决方案。

在终端认证授权方面，本方案充分考虑了移动办公的特点，除传统的VPNDB本地认证、LDAP、Radius、SecurID、AD认证，还提供移动终端音频Key证书认证、移动终端硬件绑定的手段，既安全又便于用户操作。同时，基于企业用户的不同角色、设备归属精细控制用户访问企业内网资源的不同权限。

在链路安全方面，本方案基于企业在不同场景下的接入需求，提供了L3VPN、L4VPN、Web代理及L2TP over IPSec这几种不同的接入方式，通过AnyOffice和SVN网关的配合，完美解决了移动办公人员的企业内网安全接入问题，通过加密的VPN隧道，既保障用户的顺畅接入，又避免企业数据在传输过程中被非法窃听和篡改，使得用户像内网办公一样顺畅地访问内网服务器或办公PC。

在威胁防护方面，除了提供业界领先的DDoS攻击防护，还融合Symantec先进的入侵防御和反病毒技术，提供应用层的深度防护，充分确保进出企业的流量都是干净可信的。

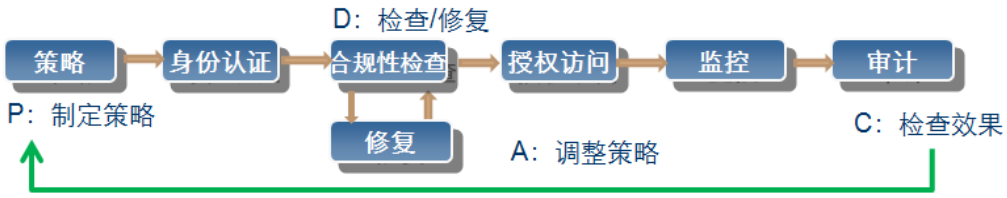
在数据保护方面，采用“安全沙箱”技术，将终端上的企业数据采用高强度加密算法保存，并且与个人数据隔离，从终端环节进一步遏制的企业数据泄密的可能性。

在应用安全和管理安全方面，方案支持各主流移动智能终端的各项通用MDM功能，包括应用管理、资产管理、安全管控、数据管理、设备管理等，同时，利用华为终端产品团队的优势，在华为手机、华为平板上提供更加强大和丰富的MDM控制能力。

2.1 Office-based 场景

用户在企业内网接入时，华为企业内网接入安全管理设计思路如下：

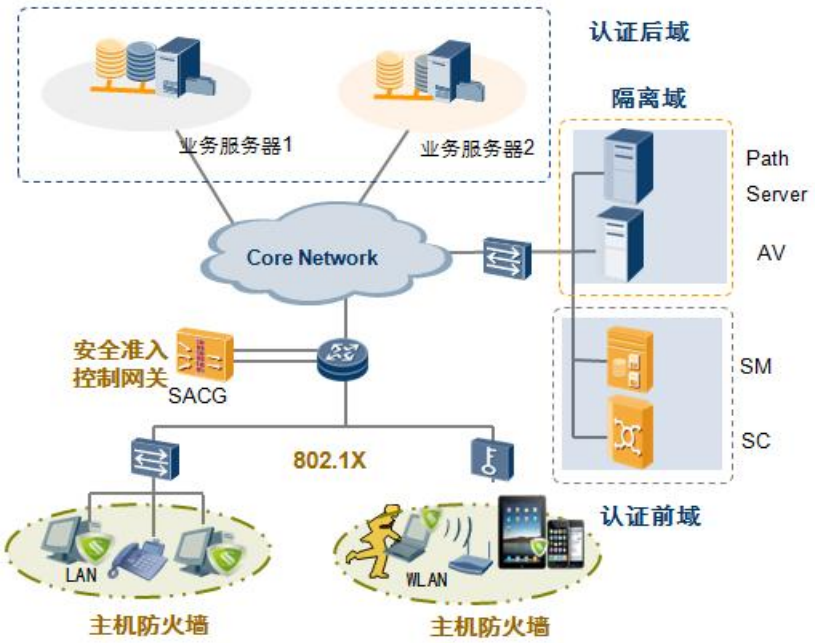
图2 华为内网安全接入设计思路



以安全策略为核心，用户在接入企业标准网络之前，第一步接受身份验证，认证通过后进行第二步强制合规性检查（包括安全状态诊断和系统配置检查），安全控制器依据检查结果作出仲裁，符合企业安全策略即可授权访问相应的网络资源；安全检查不合规的终端只能访问修复资源，完成必要的修复后才能接入网络。AnyOffice客户端对所有接入网络的终端进行持续的行为监控，及时对违规行为作出响应，并进行记录。整个流程形成Office-base环境安全保护的PDCA持续改进过程。

华为企业内网接入安全管理系统组成如下：

图3 华为内网安全接入系统组成



华为企业内网接入安全管理系统通过实施网络准入控制，能够有效的防范来自非法终端对网络业务资源的访问，防止信息泄密；通过准入控制设备(安全接入控制网关SACG、普通802.1X交换机、华为NAC接入控制网关、主机防火墙)，实现最小授权的访问控制，使得不同身份和角色的员工，只能访问特定授权的业务系统，保护企业的关键业务资源；采用终端安全状态与网络准入控制技术相结合，阻止不安全的终端以及不满足企业安全策略的终端接入网络，通过技术的手段强制实施企业的安全策略，来减少网络安全事件，增强对企业安全

制度的遵从；加强事后审计，记录和控制终端对网络的访问，控制网络应用程序的使用，敦促员工专注工作 ,减少企业在互联网访问的法律法规方面的风险 ,并且提供责任回溯的手段。

2.2 NonOffice-based 场景

用户外出进行移动办公时，通过AnyOffice连接SVN网关，提交帐号、密码或者客户端证书进行身份认证后，与SVN网关建立VPN加密隧道，并根据网关授予的权限访问企业的内网资源。

以收取邮件为例，完成在SVN网关上的认证和授权后，移动办公人员通过AnyOffice内置的安全邮件客户端收取新邮件 ,AnyOffice将邮件请求的应用层报文封装和加密 ,通过SSL隧道发送到SVN网关，SVN将报文解密、解封装后回注USG，由USG对报文明文内容做病毒检测、入侵检测和防护、DDoS应用层攻击的检测和防护，最后才将干净的流量送往企业内网。

相应地，当内网的邮件服务器返回响应报文给USG时，USG也会对报文做流量检测和过滤，然后将其发给SVN做VPN封装和加密，通过SSL隧道传输到AnyOffice的安全邮件客户端，客户端再将其解封装和解密，并用本地数据的加密算法存储在终端上。

3 方案关键组件

3.1 AnyOffice

AnyOffice客户端应用软件以one-agent的模式集成了安全邮件客户端、安全浏览器、移动终端管理（MDM）软件、L3VPN客户端、虚拟桌面等一系列自研应用，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。

同时，AnyOffice也是一个开放的平台，它支持当前流行的Android、iOS等各类智能终端操作系统，允许根据企业的实际需求增减第三方应用，也允许其他应用的开发厂商和SVN的安全SDK集成，从而成为具备加密传输、本地数据加密、数据隔离等能力的安全应用。

图4 AnyOffice 框架

在上述软件结构中，安全SDK是AnyOffice的一个关键部件，如下图所示，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（目前，支持的操作系统包括iOS、Android、Symbian、linux、BlackBerry），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、缓存清理接口以及数据隔离接口，方便各类自研及第三方的应用集成，使之具备数据加密传输、本地数据加密、缓存清理及数据隔离的能力。

所谓“数据隔离”是指用户在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，从企业角度看，这种手段既保证企业数据不被外泄，也防范个人数据中可能存在的企业违规信息（如新闻、娱乐信息）以及病毒、木马等非法程序在企业内部的传播和感染。从用户的角度看，用户个人数据都被隔离在“安全沙箱”之外，因此，不必担心BYOD设备中的个人数据会在移动办公的过程中流入企业内网而引起个人隐私的泄露。

另外，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。

图5 SDK 组件框架

目前，AnyOffice中的安全邮件客户端、安全浏览器、虚拟桌面均集成了安全SDK。

3.1.1 安全邮件客户端

邮件是企业移动办公的典型应用之一，AnyOffice默认内置的安全邮件客户端界面风格

与iOS自带的邮件客户端相近，符合移动终端用户的操作习惯，同时，由于安全邮件客户端自身具备L4VPN功能，不必在终端上安装和启用其它VPN拨号软件即可顺畅地接入企业邮件服务器。

安全邮件客户端支持SMTP、POP3、IMAP4等标准邮件收发协议。发送邮件时，该客户端构造的邮件应用层报文经过底层安全SDK的加密和封装，由SSL加密隧道发往SVN设备，SVN设备再将报文解封装、解密后，转发给企业内网的SMTP邮件服务器；接收邮件时，来自POP3或IMAP4邮件服务器的应答报文经过SVN设备的加密和封装，通过SSL加密隧道发给相应的移动终端，最后，通过安全SDK解封装和解密后上送邮件协议栈。

邮件在终端采用高强度加密算法加密存储，密钥不在终端保存，而是在AnyOffice成功登录网关后向网关请求获取，并且加密密钥会周期性变更，从而进一步提高终端数据的保密性和防破解能力。

企业管理员可根据员工的不同权限下发邮件控制策略，具体策略包括是否允许邮件转发、附件下载、附件上传、附件在线浏览。

另外，安全邮件客户端还针对移动办公的特点提供“邮件推送”功能，终端能在收到邮件推送消息时以铃声、振动等方式提醒用户，既为用户带来便利，又能确保邮件处理的及时性。

3.1.2 安全浏览器

随着各类企业应用的Web化（譬如，会议系统、考勤系统、文档查询系统等），通过浏览器访问企业内的各项应用的需求日益凸显出来，AnyOffice默认内置的安全浏览器支持HTTP、HTTPS等标准协议，同时，由于自身具备L4VPN功能，不必在终端上安装和启用其它VPN拨号软件即可顺畅地接入并访问企业网站。应用层HTTP或HTTPS报文的收发也都通过安全浏览器底层的安全SDK进行。

用户采用浏览器访问企业内网时，会在终端自动生成一些临时文件、Cookie、浏览历史记录，安全浏览器采用高强度加密算法自动加密这些文件和数据，并且在用户退出浏览器时清除这些访问痕迹。

企业管理员可根据员工的不同权限下发浏览控制策略，具体策略包括是否允许通过浏览器下载文件、上传文件、细粒度的企业内网URL访问权限控制。如果允许下载文件，那么，浏览器下载的文件也会被自动加密保存。

另外，安全浏览器还可根据终端屏幕分辨率自动调整Web页面的排版格式，确保给用户一个顺畅便利的访问体验。

3.1.3 虚拟桌面

不同于传统的PC访问PC的虚拟桌面软件，SVN推出的虚拟桌面软件支持Android和iOS这两种主流的移动智能操作系统，可以方便地集成到AnyOffice平台。

虚拟桌面特别适合使用PAD进行移动办公的用户，这些用户可通过虚拟桌面加密访问企业内网的办公PC、远程控制办公PC、运行PC上的各种软件。通过使用远程桌面协议，不需要在智能终端上安装各种办公软件，可以降低智能终端和内网服务器之间的数据流量，减少对智能终端上运算能力的需求。

同时，企业内部的任何数据均被保存在企业内网的PC或服务器上，无法通过虚拟桌面/虚拟应用拷贝到企业外部，从而达到企业数据对外隔离的效果。

3.2 SVN

SVN2000/5000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、数字证书认证、短信认证、终端硬件特征绑定及多种认证方式的组合认证。

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。

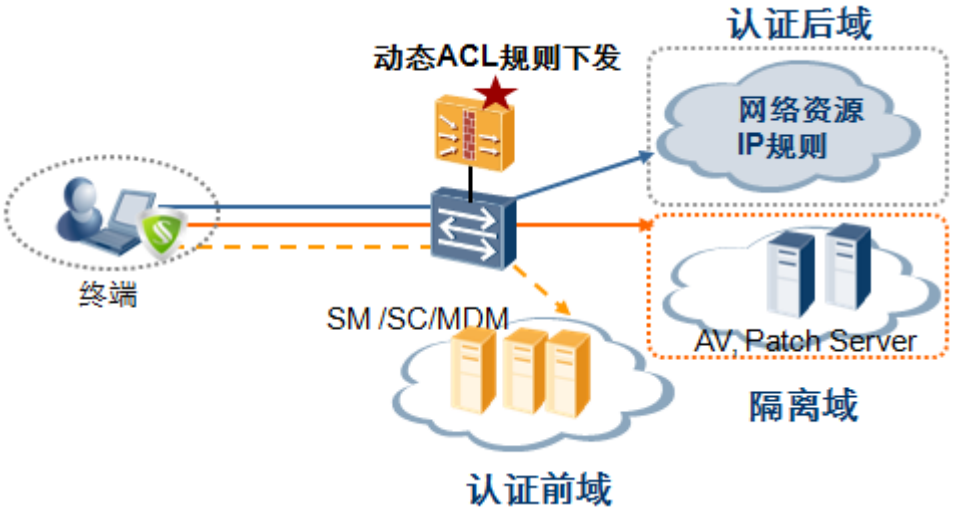
3.3 SACG

SACG是在华为电信级防火墙硬件平台上开发的专用的准入控制网关，通过基于角色的ACL规则（UCL）动态将用户关联到可以访问的认证后域，未通过身份认证和安全检查前，使用认证前域对应的ACL规则进行数据包的过滤，限制用户访问的网络资源。采用SACG接入控制方式可实现基于角色的网络访问权限控制;而且部署和实施简单，支持侧挂或直挂的方式，不改变现网拓扑结构。

SACG基于电信级的安全标准, 支持服务器资源池方式,SACG双机热备,并支持逃生通道,当SC与SACG以心跳异常时, SACG可自动根据业务优先或安全优先,开放或关闭所有网络权限控制.

SACG接入控制的流程如下：

图6 SACG 接入控制流程



1) 终端用户接入企业标准网络时,AnyOffice客户端会与SC建立一个SSL通道，用于保护AnyOffice客户端和SC之间的通信；

2) AnyOffice客户端与SC协商认证参数以及License控制信息；

3) 执行身份认证流程：AnyOffice客户端根据采用的身份认证类型（用户名+口令/AD域集成认证等），将用户名/口令信息上报至SC进行身份认证；

4)AnyOffice客户端向SC请求更新安全策略 ,获得最新的策略信息列表,执行安全策略检查,将结果上报SC；

5) SC收到安全认证的结果，判断是否符合策略规定的接入要求，如果满足，则与SACG联动，通过用户的身份属性匹配ACL规则,把对应的终端从认证前域切换到认证后域，实现最小授权访问的目的。

■ 安全管理平台SM

系统管理员通过登陆SM的WEB界面，可以完成终端用户管理、安全策略配置等业务管理工作，以及查询终端的安全状态和违规的历史记录和报表等。此外，作为管理平台，将管理其下的各个控制服务器SC的连接状态，向已经连接的各个SC控制节点发送实时指令，完成各种业务。

■ 控制服务器SC

SC主要负责完成如下几项业务：

- 与802.1X联动，当身份认证通过后，根据终端的安装状态，通知802.1X交换机开

放网络端口或者切换VLAN。

- 与SACG联动，当身份认证通过后，通过私有协议，根据终端的安全状态，对于安全检查不通过的终端，通知SACG切换到隔离域。对于安全检查通过的终端，通知SACG切换到认证后域。
- 作为与安全管理平台与AnyOffice交互的控制点，完成身份认证、安全策略下发、数据上报等任务。

3.4 USG

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DPI（深度包检测）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。

3.5 统一策略管理平台

3.5.1 统一策略管理流程

统一策略管理平台能够在整个组织内实施统一的安全策略、为各种用户提供优秀的经管体验、支持多种设备，符合安全和业务要求。平台能根据不同的用户角色、不同的设备类型、不同的场所、不同的时段、不同的区域采用不同的策略，确保对企业资源的安全访问，同时实现了与移动设备管理（MDM）的策略集成。提供涵盖整个组织的单一策略来源（有线网络、无线网络、远程网络、物理设备、虚拟设备），对移动设备有着最完善、最准确的管理，为用户和管理员提供了优良的体验、又不影响安全性、可见性和控制力。

统一策略管理流程如下：

图7 华为 BYOD 统一策略管理流程

管理员可以根据用户角色、设备类型、网络区域、时间段以及场所来配置不同的控制策略和安全策略，支持多种条件组合使用。例如：

图8 BYOD 统一策略执行应用场景

角色 \ 应用		核心应用	重要应用	受限应用	普通应用	一般应用	Internet
用户身份	高层领导	✓	✓	✓	✓	✓	✓
	普通员工	✗	✓	✓	✓	✓	✗
	合作伙伴	✗	✗	✓	✓	✓	✗
	访客	✗	✗	✗	✗	✗	✓
时间段	上班时间用户	✗	✓	✓	✓	✓	✗
	下班时间用户	✗	✗	✗	✓	✓	✓
网络区域	研发区	✗	✓	✓	✓	✓	✗
	市场部	✗	✓	✓	✓	✓	✓
设备类型	标配的Pad	✗	✗	✓	✓	✓	✓
	普通BYOD	✗	✗	✗	✗	✓	✓

注：✓表示安全策略执行通过后可以访问该业务资源；

✗ 表示没有权限访问该业务资源；

所有策略参数都可以实时下发立即生效、也可以由客户端定期请求更新。对于安全检查策略管理员可以根据应用场景配置不同的检查周期 ,监控类策略实时发现用户违规行为提醒用户并上报违规信息。系统提供趋势图、TopN图、饼图、柱状图等报表格式、预置常用报表模板，能免升级导入新的报表模板，按照模板提供基于策略、维度、范围、时段的组合展示。违规信息支持Syslog日志，可以与ISOC联动。系统的提供丰富的安全检查类策略、行为监控类策略、MDM管理策略，还提供用户自定义安全策略功能，对于一些特殊的安全检查，管理员可以利用系统提供的工具，自行开发出安全策略，对终端进行检查和管理。

3.5.2 MDM 管理

MDM是统一策略管理平台的一个核心组件 ,通过MDM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。MDM管理支持如下特性：

1) 资产管理和策略管理

在对BYOD设备执行MDM安全管控之前，首先要将用户的BYOD设备注册到企业的MDM管理平台、请员工签署相关协议，然后将MDM客户端安装到BYOD设备。之后，企业便可按双方的协议，从管理平台对移动终端进行状态查询、安全管控策略下发、应用分发

等操作了，管理员可据企业的实际情况和协议要求，通过MDM策略管理后台对终端进行“设备硬件硬件控制”、“越狱检测”、“远程锁定”、“GPS定位”、“远程擦除”、“应用一键配置”等操作。若员工需更换办公终端或离职，也可将终端从管理平台注销，脱离企业的MDM安全管控。

2) 设备硬件控制

MDM提供对移动终端设备摄像头/蓝牙/Wi-Fi/USB网络共享/GPS/VPN/蓝牙扫描/起热点功能/USB存储模式/麦克风/云服务和备份服务/截屏的控制能力，管理员可根据企业的实际情况下发策略，在员工使用AnyOffice接入企业内网期间，禁用这其中的部分或全部功能。

用户通过AnyOffice客户端登录SVN网关时，网关根据用户和设备信息下发相应的控制策略，AnyOffice根据这些策略进行控制。AnyOffice会把这些对系统硬件接口的修改记录下来，在用户在退出AnyOffice应用时，根据记录自动将这些配置恢复到登录前的状态，不影响用户在非办公期间对BYOD设备的使用体验。

3) “越狱”检测

越狱检测策略是网关在用户登录时下发给AnyOffice客户端的，如果检测到越狱，AnyOffice可根据策略的指示作出不同级别的响应：审计、提示、告警或断网。

4) 远程锁定/GPS定位/远程擦除

若终端丢失，员工可以自助管理Portal下发控制命令，对自己的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。在员工离职、更换办公终端等场景下，管理员也可通过管理后台给BYOD终端下发选择性数据擦除的指令，即仅仅擦除企业数据和卸载AnyOffice应用，而保留BYOD终端上所有的个人数据，这样既保证企业数据不外泄，又不破坏用户个人的数据和应用，用户完全可以继续正常的使用自己的个人终端。

5) 数据备份和恢复

备份通讯录、日历、邮件等关键数据到企业备份服务器，若终端丢失，可从备份服务器恢复到别的办公终端。

6) 应用一键配置

管理员还可通过MDM管理后台为所有员工的移动办公终端下发统一的应用配置，譬如，企业邮箱、VPN软件等的配置，这样既保证所有员工的办公软件的配置是安全的、一致的，也免去了每个员工分别去手工配置应用的麻烦。

7) 企业应用商店

提供企业应用的下载、升级、查询、搜索等功能。

8) 自助管理Portal

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。

3.6 MEAP

针对企业移动应用移植和发布的困难，本方案提供领先的企业移动应用平台MEAP（Mobile Enterprise Application Platform），实现企业应用的平滑迁移，提供一个简单的集成开发环境，支持HTML5/Native/Hybrid各种类型应用，一次开发，跨平台多次发布，可显著降低开发复杂度，为企业节约成本。

图9 方案关键功能列表

功能特性	
移动VPN	L3VPN支持Android4.0的API接口
	虚拟桌面支持鼠标模拟
	虚拟桌面支持远程唤醒
	安全SDK提供标准的webservice和http接口
	安全浏览器
应用发布	MEAP企业移动应用平台
	Push邮件客户端
	支持应用程序的发布功能
泛终端支持	支持iOS、Android、Win8 等主流移动操作系统
认证授权	移动终端硬件特征绑定
	针对L3VPN和安全SDK的客户端进行不同的授权
	针对移动用户进行分组授权
	针对公司配机和个人手机实施不同的安全策略
移动数据安全	数据备份、恢复
	数据远程擦除

	访问痕迹自动清除
	数据加密保存
One-Agent	安全浏览器、虚拟桌面、L3VPN、PushMail、MDM等功能客户端融合，具有统一的用户界面
客户端自保护	卸载保护
	服务常驻
移动终端管理	终端设备注册、注销
	终端设备绑定、取消绑定
	终端设备状态检查
	策略管理
	数据备份/恢复
	实现企业内部移动应用的管理门户
	提供用户自助管理页面：警报/锁定/擦除数据/定位等防盗窃功能
	终端设备定位管理
	提供移动终端设备信息的查询页面
	提供集中的移动终端设备的使用记录查询
	配套日志审计
分布式集群	SSL VPN会话同步
	配置同步
	license共享
	分布式集群
	智能选路
负载均衡	GSLB（Global Server Load Balance）全局负载均衡
	对内网服务器的负载均衡
网络无边界	内外网络感知和策略
	自动切换，VPN连接不间断
易用性	友好易用的用户界面

	易用直观的管理界面

图10 所支持的设备及平台

设备	平台版本
iPhone 3G/3Gs	iOS 3.1.3以上
iPhone 4/4s	iOS 4.0以上
iPad	iOS 3.2.2以上
Android	Android 2.2以上
Windows	XP,Vista,Windows 7
WindowsPhone	Windows Phone 8-即将推出

4 方案优势

4.1 Identity：统一的网络接入控制

■ 基于环境感知的网络接入控制

基于设备（What device）、角色（Who）、场所（Where）、时间（When）和接入方式（How）的环境感知，实现细粒度访问控制策略。管理员可通过统一策略管理平台，基于一个用户角色，多套策略模版，一次性配置和分发策略到移动客户端AnyOffice，AnyOffice基于环境感知，智能启动与设备环境适应的安全模块，联动SVN VPN网关、SACG安全接入控制网关或802.1X交换机，实现精确的网络访问控制。用户自由的从咖啡厅、机场远程接入，到出差至办事处，用户的远程会话可从SVN设备透明的切换到SACG设备，这个过程对用户完全透明，AnyOffice屏蔽一切复杂的网络连接，带给用户最简单、无缝的接入体验。

■ 统一策略管理

统一策略平台可保证单一策略来源，安全策略在全网范围保持一致性，轻松确保企业安全策略遵从。真正实现任何人、在任何地方、以任意授权设备（便携、智能手机或平板等物理设备，或虚拟设备）、通过任何网络（有线网络、无线网络、远程网络）自由、边界的访问公司内部资源。直观的管理界面简单、易用，提升管理员工作成效的同时，实现对移动设备的全面可见性和控制力。

4.2 Privacy：全面的数据安全和威胁防护

■ E2E（End to End，端到端）的数据防泄密

数据在设备侧: AnyOffice客户端开创性的通过沙箱技术，在同一台移动设备上创建了一个个人与企业分离的安全地带，轻松解决了个人和企业应用、数据混合带来的数据泄密和

病毒等风险，在个人需求和企业策略强制的冲突中实现平衡。当用户登陆AnyOffice工作台，所有的企业业务处理将在一个封闭的安全环境中，与个人应用隔离，在数据创建之初就确保存储在一个安全的隔离地带，并且加密保护；AnyOffice进程扮演着操作系统内核的角色，可监控企业应用的行为，个人应用不能访问企业应用，且阻断个人和企业应用之间的数据拷贝、剪切、粘贴等行为，并可根据策略阻止或使能应用的上传、下载等操作；在应用注销时，AnyOffice还能实现临时文件和数据的无痕化擦除，进一步减少数据泄密的风险。

数据在传输中: 在数据传输层面，SVN SSL VPN网关可提供L3/L4 VPN高强度加密传输，保证数据隐密性安全，防止数据的恶意嗅探和篡改。

数据在服务器侧: 移动设备因为体积小,丢失和盗窃的风险高，47%的受访企业表明有大量客户数据存储在移动设备上,每年因设备丢失和盗窃造成的数据泄密事件不胜枚举. 通过和管理后台联动，方案提供远程锁定、远程数据擦除、数据备份和恢复等反盗窃功能，以及GPS定位、自动报警等特性，确保在设备遗失情况下数据安全的万无一失。

■ 移动应用级安全

安全浏览器：随着企业各类应用的Web化（如会议系统、考勤系统、文档查询系统等），通过浏览器访问企业内的各项应用的需求日益增加。安全浏览器可根据终端屏幕分辨率自动调整Web页面的排版格式，确保给用户一个顺畅便利的访问体验。

同时，安全浏览器提供了关键的安全防护能力。首先是基于AnyOffice的沙箱安全模块，可隔离个人应用，并限制通过浏览器访问的企业B/S 应用的行为。安全浏览器具备L4VPN功能，不必在终端上安装和启用其它VPN拨号软件即可顺畅地接入并访问企业网站。

另外，安全浏览器支持无痕浏览功能，用户退出浏览器时可对临时文件、Cookie、浏览历史记录做无痕化清除访问痕迹。对于保存在本地的文件和数据也可提供高强度加密保护。

最后，安全浏览器还支持黑名单，可有效防止防止网络钓鱼和恶意软件风险

。

安全Pushmail：邮件是最早的移动办公应用。安全邮件客户端支持SMTP、POP3、IMAP4等标准协议收发邮件，并支持邮件实时推送，实现“及时经济”下的实时邮件处理。

同时，安全Pushmail可提供强大的安全特性，降低移动邮件引入的数据泄密和病毒风险。支持L4 VPN实现传输自动加密，防恶意窃取和篡改。邮件在终端采用高强度加密算法加密存储，密钥获取，本地不保存。另外，支持丰富的邮件安全控制策略，企业管理员可根据员工的不同权限下发，包括是否允许邮件转发、附件下载、附件上传、附件在线浏览等。

■ 电信级的网络侧移动威胁防护

在企业网络边界，针对以下三个场景，通过华为电信级高可靠USG系列防火墙，可提供网络侧的深度威胁防御能力。

来自Internet的移动平台威胁防护：DDoS防攻击与非法访问，防黑客跳板入侵，防病毒、木马传播，恶意邮件过滤。

来自Intranet的移动平台威胁防护：非法访问控制、内部员工恶意入侵、防病毒、木马传播。

移动办公终端内部信息安全管控：URL过滤非法访问控制、恶意Web页面访问控制、Web页面/邮件正文/附件关键字过滤。

4.3 Compliance：基于生命周期的移动设备管理

■ 获取

华为移动办公安全解决方案支持标配机和 BYOD 的资产发现和注册，进行密码的初始化，并提供移动设备使用承诺协议的自定义模板。

■ 部署

移动设备在接入企业网络时，IT 管理员都需要根据企业安全策略，华为移动办公方案支持对移动设备进行主机防火墙、VPN 和 WiFi 安全配置策略下发，以保证设备的安全合规性。

华为移动办公安全方案集成企业App Store，对企业移动App进行安全的远程分发、安装、配置，除此之外，企业可以根据用户角色定义App黑白名单策略，保证正确的人访问正确的应用和数据。最后，华为移动办公安全方案的应用签名验证特性，服务常驻防卸载功能保证授权的应用不被恶意的篡改和卸载，在移动终端上维持应用环境的完整性。

■ 运行

运行阶段重点关注数据和应用的安全性。华为移动办公安全方案支持密码策略、越狱检测与隔离、外设泄密通道(SIM 卡/摄像头/蓝牙/WIFI/USB/GPS/录音)的控制，保护在移动终端上使用的数据安全。移动设备容易丢失，为方案能够实施企业关键数据加密，远程备份/恢复/同步，远程锁定/数据擦除。除此之外，IT 管理员可以通过远程升级、打补丁的方式来增强应用的安全性。在管理后台，管理员可以审计查询所有移动办公设备列表，以及相应

的状态，例如设备型号，操作系统与版本等等，并可以输出资产审计报表。

降低 IT 支撑压力是移动办公方案的运作成功的一个重要因素，华为移动办公安全方案支持友好易用的自助 portal，员工可以完成注册、重置密码、挂失、锁定、数据备份与恢复、数据远程擦除等频繁使用的操作，有效的降低 IT 支撑人员压力。集中管理控制台除了支持上述功能之外，支持更加复杂的管理功能，例如消息推送，故障定位等；另外，管理 API 接口支持与企业现有 Helpdesk 集成，提升支撑服务效率。

■ 回收

员工离职或者设备丢失，为了防止数据泄漏，IT 管理员需要对遗留在设备上的应用进行卸载，对数据进行清除，最后注销此设备。对于企业标配设备，回收的设备可以重新注册绑定，并部署安全策略和应用。

■ 灵活的应用发布

MEAP第三方应用集成

移动设备和企业应用的复杂性，使得移动应用开发困难重重，华为提供集中的 MEAP 平台，将移动终端和企业应用集中适配对接，极具扩展性。华为 MEAP 平台，不仅支持 HTML5 和原生 Native 应用，而且支持以 Native 为容器，HTML5 为界面的混合 Hybrid 应用的开发部署。MEAP 集成开发环境，内置业务逻辑辅助设计模块，减少代码量，并且支持一次开发，跨多平台发布，降低开发难度，缩短应用上线时间。在设计开发阶段，企业可以在移动应用中内置丰富的安全特性，例如 SSL，SSO，MDM 安全特性联动。华为 MEAP 支持全生命周期的开发流程：设计、开发、测试、部署、维护，保证应用开发活动的连续高效。