案例 1

中国移动政企客户分公司

主标题：某发动机制造企业 SD-WAN 工业专网安全解决方案

副标题：低成本易管理的云、网和安全一体化解决方案

引言：中国移动通信集团公司政企客户分公司（简称政企分公司），前身为中国移动总部集团客户部，成立于 2012 年 8 月，是中国移动通信集团公司下属经营集团客户市场的专业化分公司。

集团客户市场是当今全球信息通信行业发展的重要蓝海。截至 2014 年 1 月，中国移动集团客户数已超过 320 万家，覆盖了全国逾 40%的法人和产业活动单位，集团成员达 2.3 亿户，集团客户的整体收入已超过中国移动整体收入的 40%。开展集团客户市场的专业化运营，已经成为推动我国信息化事业持续健康发展的必然趋势。

按照中国移动的整体战略部署，政企分公司主要提供面向政府、大型企业等重要集团客户的销售和端到端服务；负责面向全国的集团客户产品整合和产品推广；统筹各方资源，组织协调跨省跨国业务的支撑和调度。

政企分公司将依托于中国移动在网络、客户、渠道、业务和产业链等方面的整体优势，紧密围绕“移动改变生活”的发展愿景，持续地提升面向各行各业的信息服务份额，做质量更好、服务更优、创新更强、价值更高、管理更有效的运

营商和现代服务企业。

一、项目概况

1. 项目背景

随着近几年工业互联网的发展，传统的工业网络正在向扁平化、IP 化演进，越来越多的工厂内设备接入工业专网，并通过互联网进行跨区域数据传输。同时企业上云已经成为共识，通过结合公有云与私有云，打造企业混合云成为未来一段时间内的大趋势。因此工业企业各机构、厂区以及云数据中心间面临不同于以往的网络互联和网络安全挑战。传统的网络设备和网管系统使用复杂、技术要求高，不能满足工业企业对网络的便捷有效管理需求。同时为保证网络安全，需要在网关处堆叠多种不同类型的安全设备，不但组网复杂，管理维护难度大，也自然造成设备采购和运维成本高。工业企业亟需一套成本较低且易于管理的云、网及安全一体化解决方案。

2. 项目简介

本项目将中国移动的 SD-WAN 产品用于某发动机制造企业的工厂外网络建设中，利用 SDN 与 NFV 技术，通过位于云端的集中管理平台解决运维管理难题，通过多功能一体化的安全网关降低设备采购成本。该发动机制造企业所面临的具体问题如下：

1、企业总部厂区目前在进行智慧工厂改造，厂区内生产设备逐步联入企业内网并将数据上传至 MES 系统，一些敏感设备数据存在跨区域传输需要。企业现有的跨区域传输手段是租用运营商的传输专线，因此没有建设接入互联网所必须的防火墙、入侵保护等安全防护措施，难以实现工厂内网与工厂外网的隔离，也就无法保证生产运营数据的安全存储和防止关键数据外泄。目前企业需要运用上述的安全措施在总部厂区，工程研究院和欧洲研发中心之间组建跨区域的工厂外网专网。

2、企业在智慧工厂改造过程中，组建企业内部私有云平台，将关键生产系统部署于私有云上，同时部分企业应用部署于公有云，但企业缺乏组建安全的混合云网络的手段。

3、企业管理人员缺乏统一的管理平台对网络和节点进行集中管控，无法及时对网络异常状态进行有效处理，无法对设备进行远程管理维护。

3. 项目目标

本项目即着眼于通过一套 SD-WAN 方案，解决上述该发动机制造企业所面临的网络和安全问题。

二、项目实施概况

1. 项目总体架构

该发动机制造企业通过部署基于 SDN/NFV 技术的 SD-WAN 网络实现工厂外网专网的组建，并保证专网安全。SD-WAN 网络由集中管理平台与安全网关组成，集中管理平台在中国移动的公有云端进行部署，可对整个网络进行统一管理；安全网关部署于企业内部，通过虚拟化的方式灵活承载网络功能，来提供企业工业专网所需的各种网络安全特性，同时安全网关支持通过 TD-LTE 网络进行数据传输。

该企业的 SD-WAN 工业专网解决方案如下图所示：

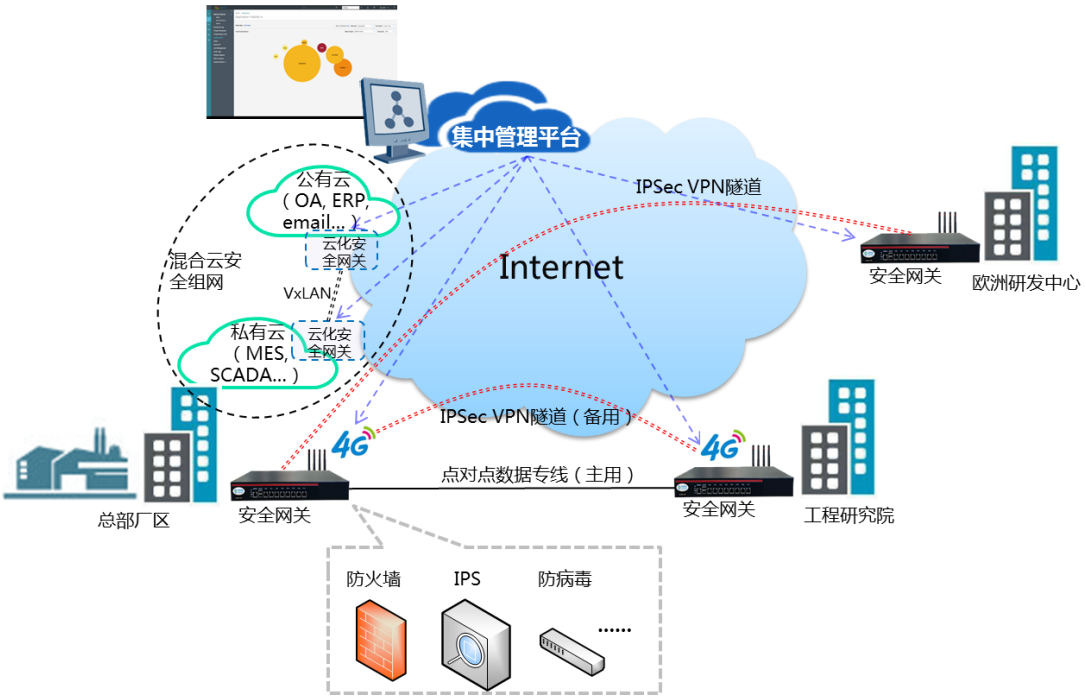

图 1　某发动机企业 SD-WAN 工业专网组网示意图

2. 项目主要内容

（1）网络互联

在该企业总部厂区与工程研究院之间各部署一台安全网关，通过安全网关在两点间部署主备两条数据链路进行数据传输，主用链路为一条点对点数据专线，该链路为企业专用，与 Internet 物理隔离。备用链路为使用安全网关建立的一条加密的 IPSec VPN 隧道，通过 TD-LTE 无线网络进行数据传输。基于 IPSec 的加密功能，可以保证数据的端到端安全传输。安全网关支持 TD-LTE 通信功能，在不额外增加物理链路的情况下，快速完成备用链路的部署。在主链路故障时，业务会自动切换至 TD-LTE 链路。

在该企业的欧洲研发中心中部署安全网关，并与总部厂区基于 Internet 建立加密的跨国 IPSec VPN 隧道，在原有互联网数据传输基础上保证数据的传输安全。

（2）网络安全

安全网关采用通用硬件架构，以虚拟化的方式构建网络功能。该企业通过安全网关的状态化防火墙功能，根据流量上下文对流量进行管理和控制,并对防火墙安全区域和安全等级进行划分。

安全网关支持 L3~L4 的防攻击功能，防 DoS/DDoS 攻击功能，支持防端口扫描功能，防止其它设备或者应用的恶意端口扫描。安全网关能实现主动入侵防御功能，通过本功能，防火墙可以识别并阻止 L7 的异常流量和攻击，提高网络可靠性。

安全网关支持防病毒功能，可以检测压缩包内的文件，并提供病毒阻断功能，防止带毒文件被下载到本地。支持对 HTTP、POP3、SMTP、IMAP 和 FTP 协议报文中的木马、病毒、广告程序、蠕虫和其他恶意程序的检测和阻挡；支持对 ZIP 或者 RAR 数据包的内容扫描功能，可以智能跳过指定大小的压缩包或者带密码的压缩包；检测到病毒之后，发送告警信息至平台。

安全网关通过 DPI 检测流量类型，对生产办公类数据精细化管理，并优先保障关键流量的传输。

（3）混合云安全组网

在该企业的公有云和私有云的虚拟机上分别云化部署安全网关，并通过网

关支持的 VxLAN 功能，打通公有云和私有云间的大二层网络，同时使用网关的安全功能保证混合云网络安全。

（4）网络管理

该企业网关人员通过集中管理平台对全网设备、网络功能、业务流量和安全态势进行统一管理，可视化管理方式使网络管理便捷高效。

三、下一步实施计划

下一步计划在该企业扩展 SD-WAN 的部署规模，使工业专网逐步覆盖企业所有厂区、办公区、服务网点等分支机构。

四、项目创新点和实施效果

1. 项目先进性及创新点

技术创新点：

（1）本项目中使用了基于 SDN 和 NFV 技术的 SD-WAN 安全网关，网关集网络与安全功能于一体，大大降低了企业组建安全的工业专网所需的网元数量，简化了网络拓扑结构，并降低硬件采购成本。

（2）通过部署于中国移动公有云端的集中管理平台对企业工业专网进行统一管理，一套平台即可实现对网络状态和安全态势的实时监控，并为企业节省了部署网管服务器的投资，同时可视化的操作方式大大降低了对网管人员的技术要求。

（3）通过云化部署网关软件，非常便捷的打通了企业云、网连接，同时利用网关的安全功能充分保障云安全。

商业模式创新点：

（1）融合网络与安全的一体化解决方案。

（2）以服务的形式向客户提供安全可靠的工厂外网络，客户通过月租费的形式支付费用，降低一次性投资。

可复制推广性：

本项目可面向工业行业内的所有企业，在工厂外网络的联网和安全领域进行复制推广。

2. 实施效果

本项目实施后完全达到了预期目标，解决了前述该发动机制造企业面临的三个主要网络和安全痛点。根据测算，本项目共帮助企业减少了 50%的网络和安全设备投资，降低了 70%的运维成本。