方案名称：河南某企业安全服务方案

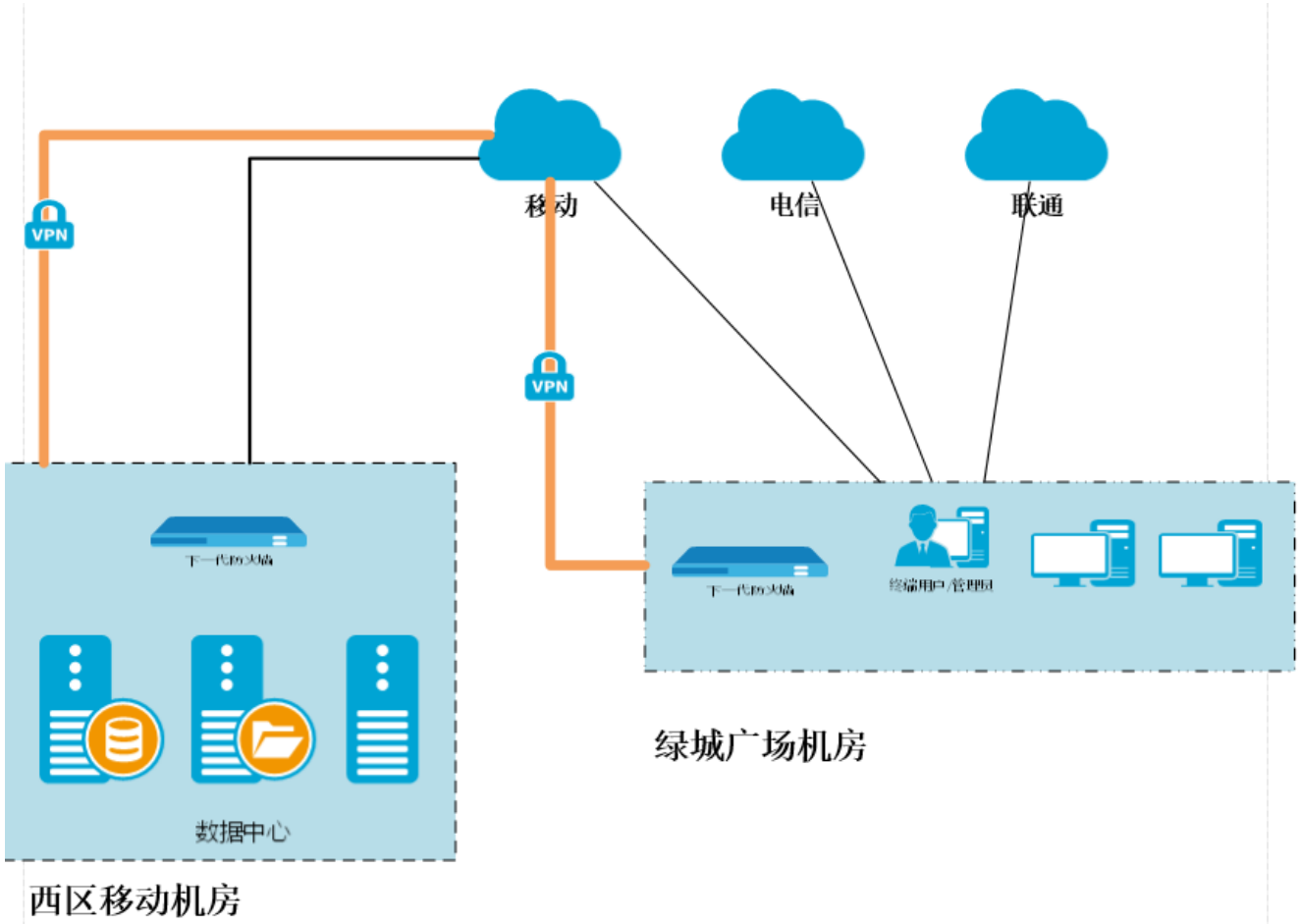
个人信息：魏经超-郑州华宜建计算机设备有限公司

项目背景

中国通信建设四局护网工作作为一项持续提升国家网络安全保障能力的手段之一，公安部自2016年起组织对互联网和关键信息基础设施等开展网络安全执法大检查，即“网络攻防演习行动”，从2016年至今已持续开展4年，规模不断扩大。2016年，公安部组织8支攻击队伍对民航、国家电网进行实战攻击；2017年，公安部组织18支攻击队伍对国家旅游局、北京市食药监局、中科院、央视网、中国人寿、北京市自来水公司、北京教育考试院、首汽租车、安贞医院、小米科技、网宿科技进行实战攻击；2018年，公安部组织41支攻击队伍对税务、电力、电信、银行、铁路、财政、广电、水利、教育、互联网、检察院、法院、石油、交通等16个行业29家单位共45个目标系统进行实战攻击；2020年，公安部组织110多家攻击队伍对金融、证券、电力、能源、通信、交通、航空等30多个重点行业118家单位130多个目标系统进行实战攻击。

本方案针对网络安全现状及2020中国通信建设四局行动总指挥规划要求，遵循保障原则及工作安排建立的一套适用于中国通信建设四局整体护网工作的全流程方案。

项目现状



当前业务系统部署在两个机房中，机房业务系统如下：

西区移动机房，3台4路服务器承载60余台虚拟机；

绿城广场机房， 1台物理机承载内网业务。

设计方案

序号	设备名称	设备简介	方式	类型	备注
1	WEB 应用防火墙	应用服务器区Web应用安全防护	现场 1台	安全产品	
2	日志审计	服务器、安全设备日志源信息收集，便于威胁回溯。	现场 1台	安全产品	
3	运维审计系统	对设备管理员进行身份鉴别、访问控制、操作审计	现场 1台	安全产品	
4	远程安全评估系统	山石商用漏洞扫描器，主机、web站点、数据库、中间件、网络设备等入网节点探测，发现非法入网节点及监控盲区，全局网络资产可视管理；安全漏洞、高风险服务、弱口令、网马暗链、远控后门等网络脆弱性扫描定位，高危流行漏洞针对性渗透测试；	现场 1台	安全产品	
5	内网威胁感知系统	办公内网的新型攻击行为和异常风险主机终端行为的分析和定位	现场 1台	安全产品	
6	安全态势感知系统	全息数据驱动的AI分析运营系统，由分析平台与丰富的探针共同构成，可为各行业客户提供网络威胁分析、态势呈现与溯源等功能，解决客户监控盲区，潜在安全隐患、运维低效等问题。智·源具备全息数据采集的能力，通过多种类型的数据探针采集数据，基于海量网络流量、威胁事件和终端日志等进行智能数据挖掘及分析，呈现全局网络安全及威胁态势。	现场 1套（含1个平台，1个探针）	安全产品	

优势

专家团队，定制化安全服务