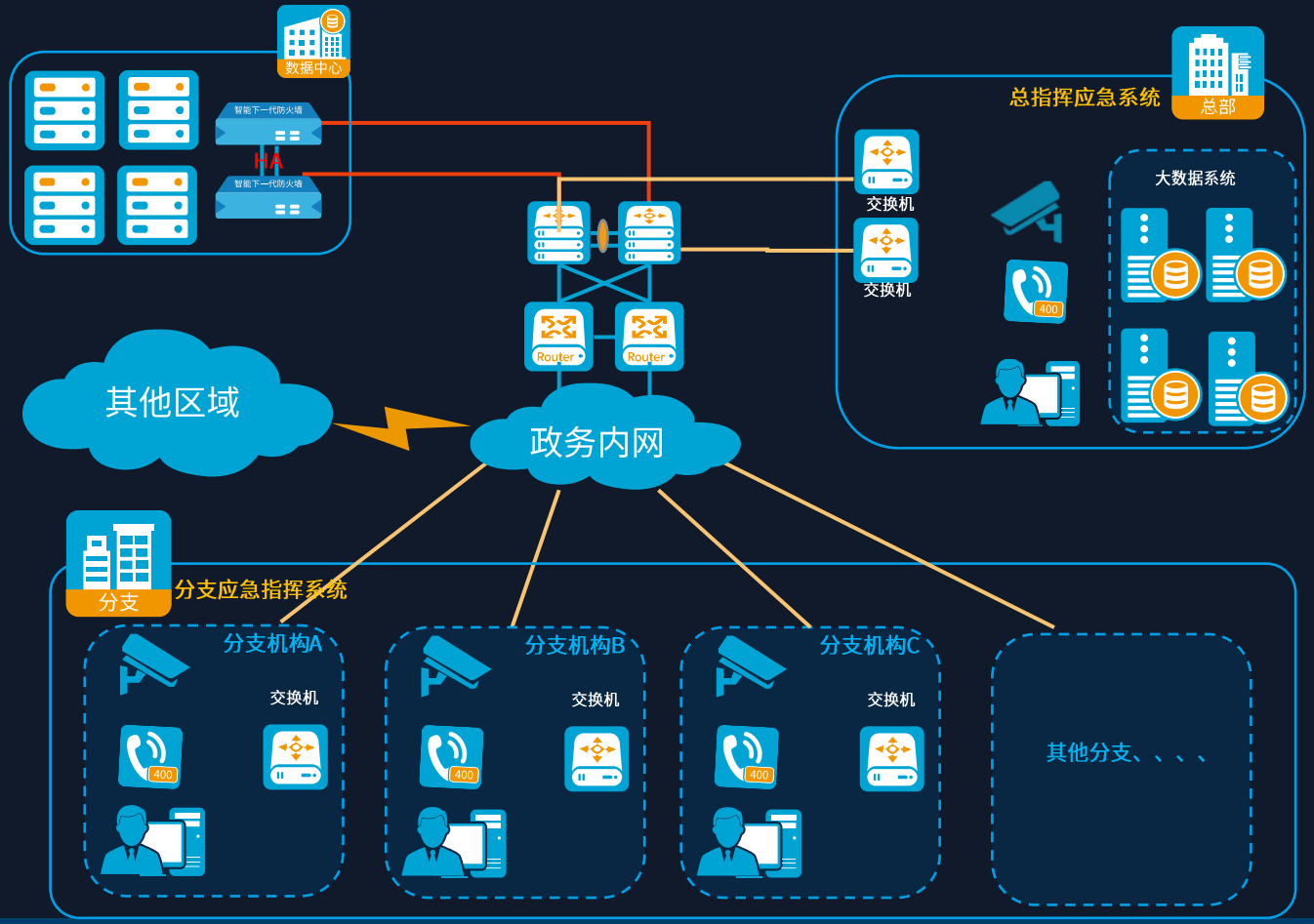
Hillstone 山石网科

某市应急指挥系统网络安全升级项目

彭海司-广州中科诺泰技术有限公司

背景介绍-市应急指挥系统网络现状



现状描述：
应急指挥系统部署于政务内网。市政府本部作为应急指挥中心，下属共有二十四分支，所有应急系统之间互联互通，应急大数据系统部署于本部，为指挥系统提供决策支持。

现指挥系统已运作多年，无论从网络可靠性，网络安全性还是从业务的稳定性都不足以支持现今的需求。

问题分析

IP地址不足

现今用于指挥系统的政务内网地址需要回收，每个分支只有一个政务内网IP。但分支应急指挥系统的话机、终端、语音网关、交换机、及新增的防火墙等，最少需要7个地址。而且需互联互通，不能通过NAT方法解决。

信息泄露风险

总部与分支之间网络通信使用无加密传输，指挥中心与分支经常需要传输一些机密文件及决策信息，总部的大数据平台存储着管理信息系统、地理信息系统、基础数据库。存在信息泄露的风险。

管理混乱

有的分支为后期自行组建并入应急指挥网络。管理权限及设备资产属于分支机构。并且设备品牌型号和软件版本不一致。出现故障时排查难度陡增。以及现今设备无统一管理平台和登录限制，存在防止误操作、滥操作、越权操作风险。

网络安全问题

指挥系统部署于政务内网，与政务其他系统互联互通，无安全隔离。终端电脑一旦感染病毒木马，将直接威胁到核心业务系统安全。并且指挥系统部分设备为外国产品，存在安全隐患。

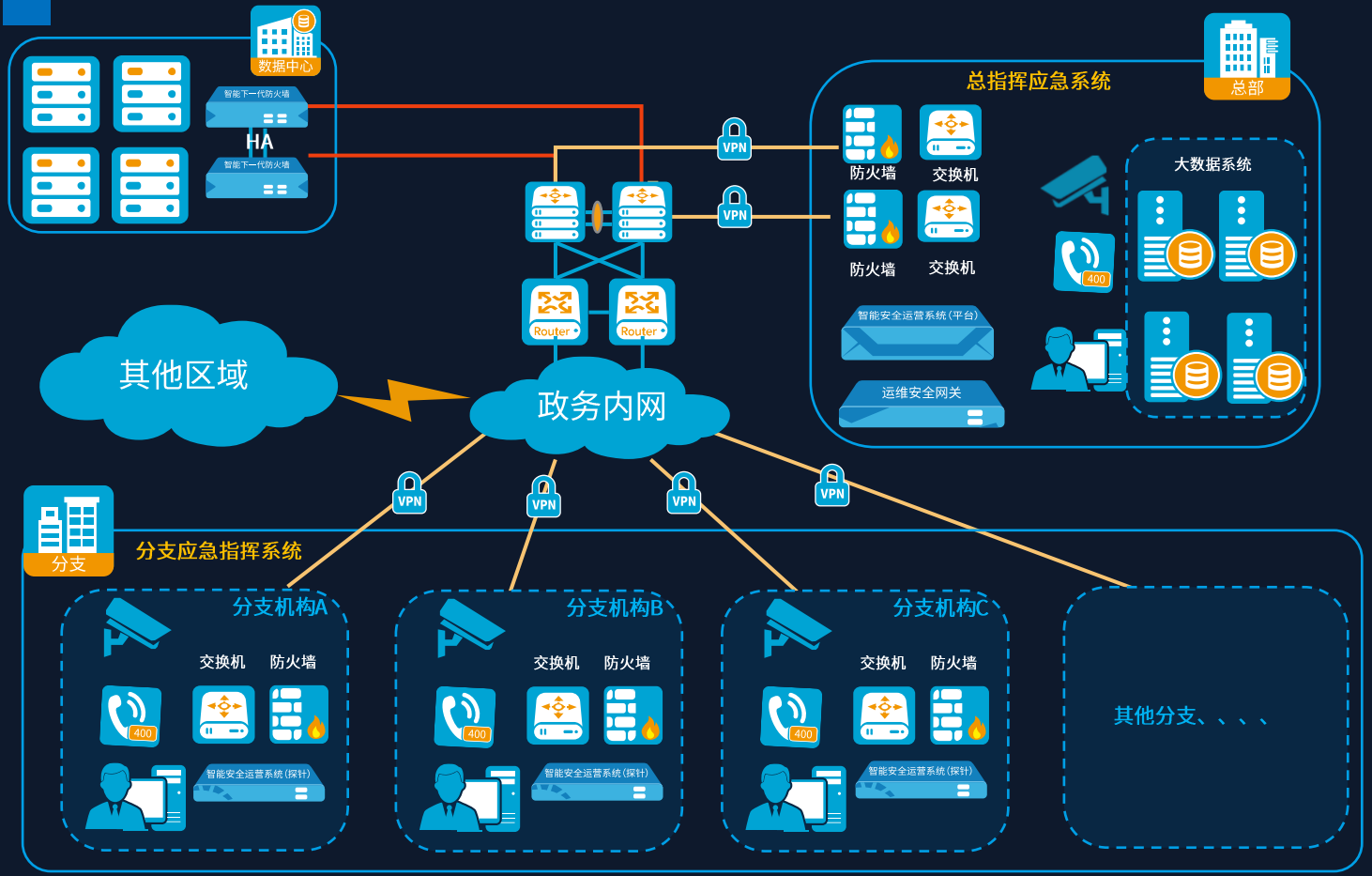
流量无管控

由于分支直接接入政务内网，分支与分支直接互联互通。分支之间的互访流量，总部市政府无法进行审计和回溯。不符合总部现今的管理规定。并且由于中间无流控设备及流控措施，没有对应急的视频流量做QOS。

不符合合规性

由于国家对网络安全的重视日益提高，颁布一系列针对行业及相关单位的安全要求，包括相关的等级保护、网络安全法、互联网信息服务管理办法。现今系统建设年限已久，无法符合监管部门的审计要求。

解决方案



Ipsec vpn

所有分支区域跟市政府创建ipsec vpn，解决政务内网ip地址不足问题。而且即互联互通又达到对指挥系统流量进行安全加密效果。

防火墙安全策略隔离

所有分支防火墙划分内外网安全域，做安全隔离，禁止分支应急指挥系统访问应急指挥系统之外的政务内网资源。禁止分支访问大数据系统，收紧分支的访问权限，并且防止内网病毒蔓延问题。

统一运维管理

通过应急系统的统一升级改造，将所有分支的管理权限上收市政府，统一纳管。摒除资产、品牌、版本、策略等混乱的情况。规范化运维管理，所有指挥系统相关网络设备只允许市政府本部运维安全网关管理。实现对核心资产的统一认证、统一授权、统一审计。

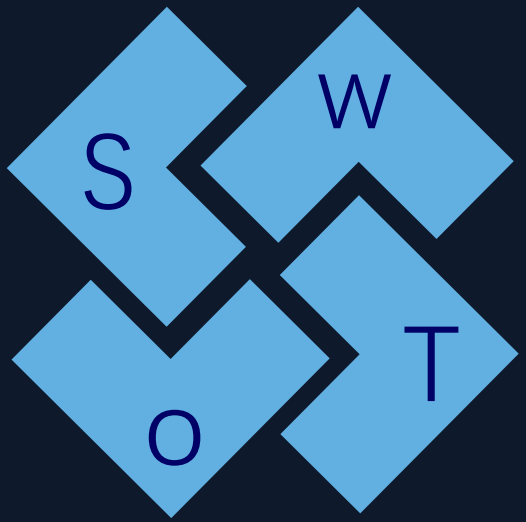
部署智能安全运营系统

通过把日记分发和流量镜像到智能安全运营系统探针。实现对网络威胁分析、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。并且解决行业的安全审计要求。

方案优势

解决用户需求

通过Ipsec vpn将分支与总部互联，解决应急指挥系统政务内网ip地址不足问题。分支直接互访必须进过总部，解决分支之间互访，总部无法控制并且无法审计回溯问题。



规范化统一管理

1、规范运维管理：统一访问入口，集中授权控制。
2、降低资产风险：防止误操作、滥操作、越权操作。
3、满足合规性要求：通过权限控制和审计记录，满足法律法规和IT运维要求。

加强安全防护

边界防火墙通过入侵防御和防病毒模块，可有效过滤病毒、木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁。通过区分安全域和访问控制，解决分支对政务内网系统无安全隔离，解决病毒木马肆意传播的安全隐患。

实时安全态势感知

采用总部部署智能安全系统平台，分支部署探针方式，并且分支之间互访需通过总部，对应急指挥系统的网络安全状态实时感知，加快网络管理人员对网络安全攻击的反应及处理，加强了对管理员对整体网络的安全管理。