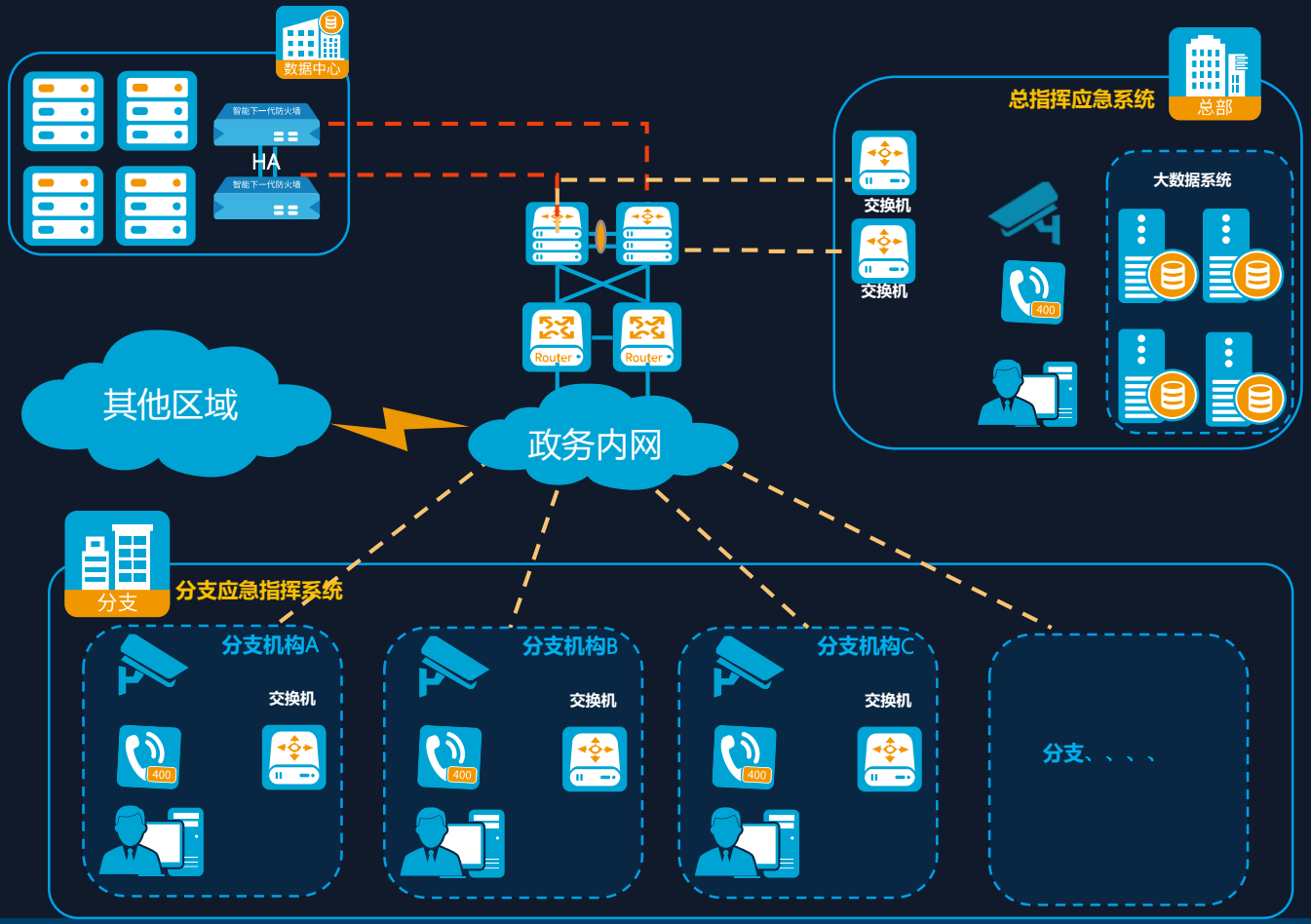
Hillstone
山 石 网 科

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



- 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，下属共有二十几个分支，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。

需求分析

IP地址资源不足

由于现今用于指挥系统的政务内网地址需要回收，每个分支能分配出来的政务地址只有一个。
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，加起来最少需要7个地址。

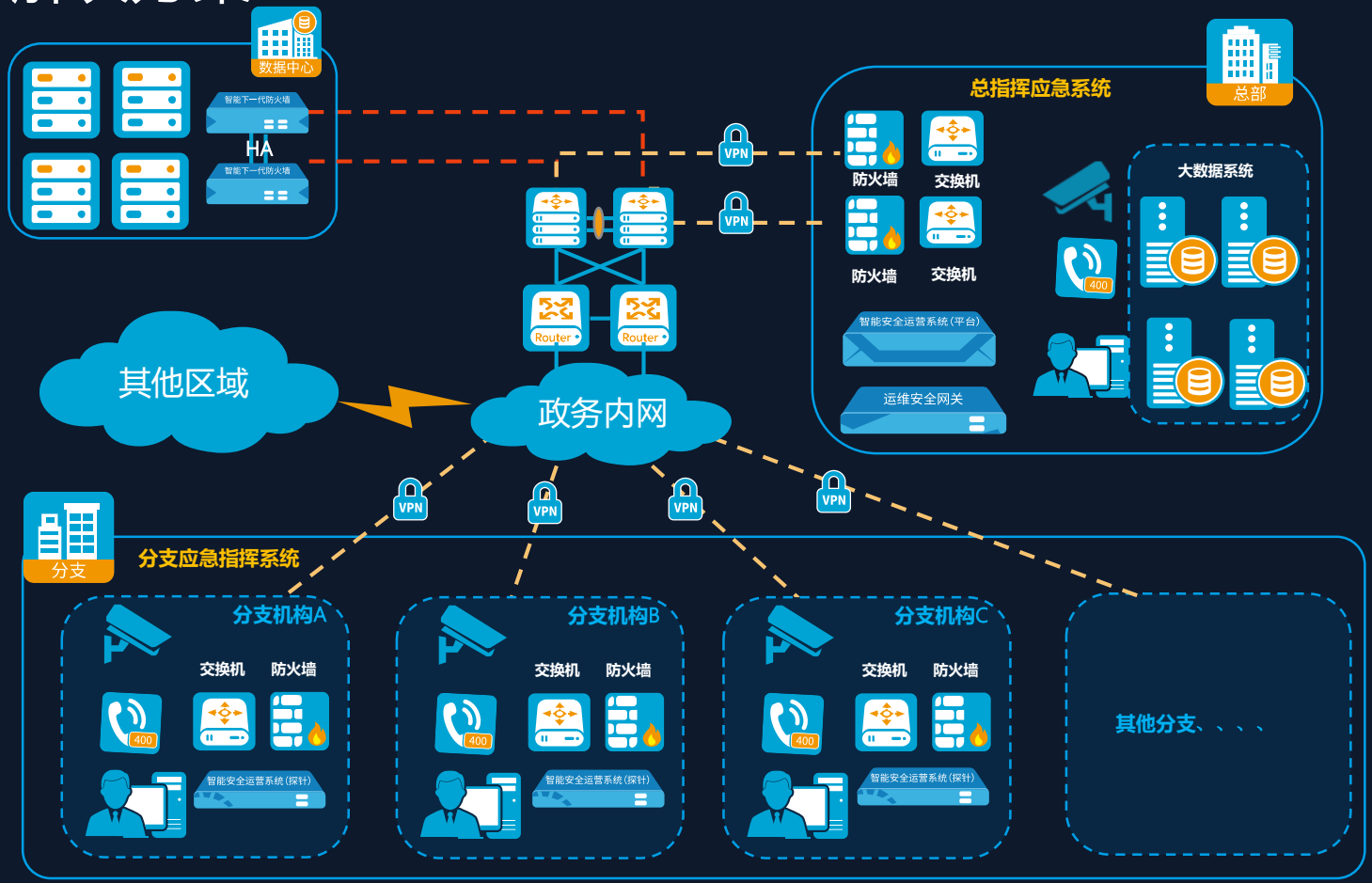
网络安全问题

现今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。

合规性要求

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。并且达到对指挥系统流量进行安全加密效果。

划分安全域
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。

统一运维管理
规范网络安全运维管理，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。

符合监管要求安全审计
分支应急指挥系统只能通过市政府才能互访。通过把日记分发和流量镜像到智能安全运营系统。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，分支直接互访必须进过总部。解决应急指挥系统政务内网ip地址不足问题，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。

全面威胁检测与防护

基于深度应用、协议检测和攻击原理分析的入侵防御技术，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，实现网络的L2-L7层网络安全防护。

满足行业合规性

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。

全景安全态势呈现

将关注视角定位于全局，以宏观尺度观察整体网络的安全趋势，提供一个以全局为视角的实时监控界面，在第一时间发现网络风险状况。利用Ai深度学习、大数据挖掘分析技术，以此发现潜在的高级威胁、还原攻击路径、提取证据信息。