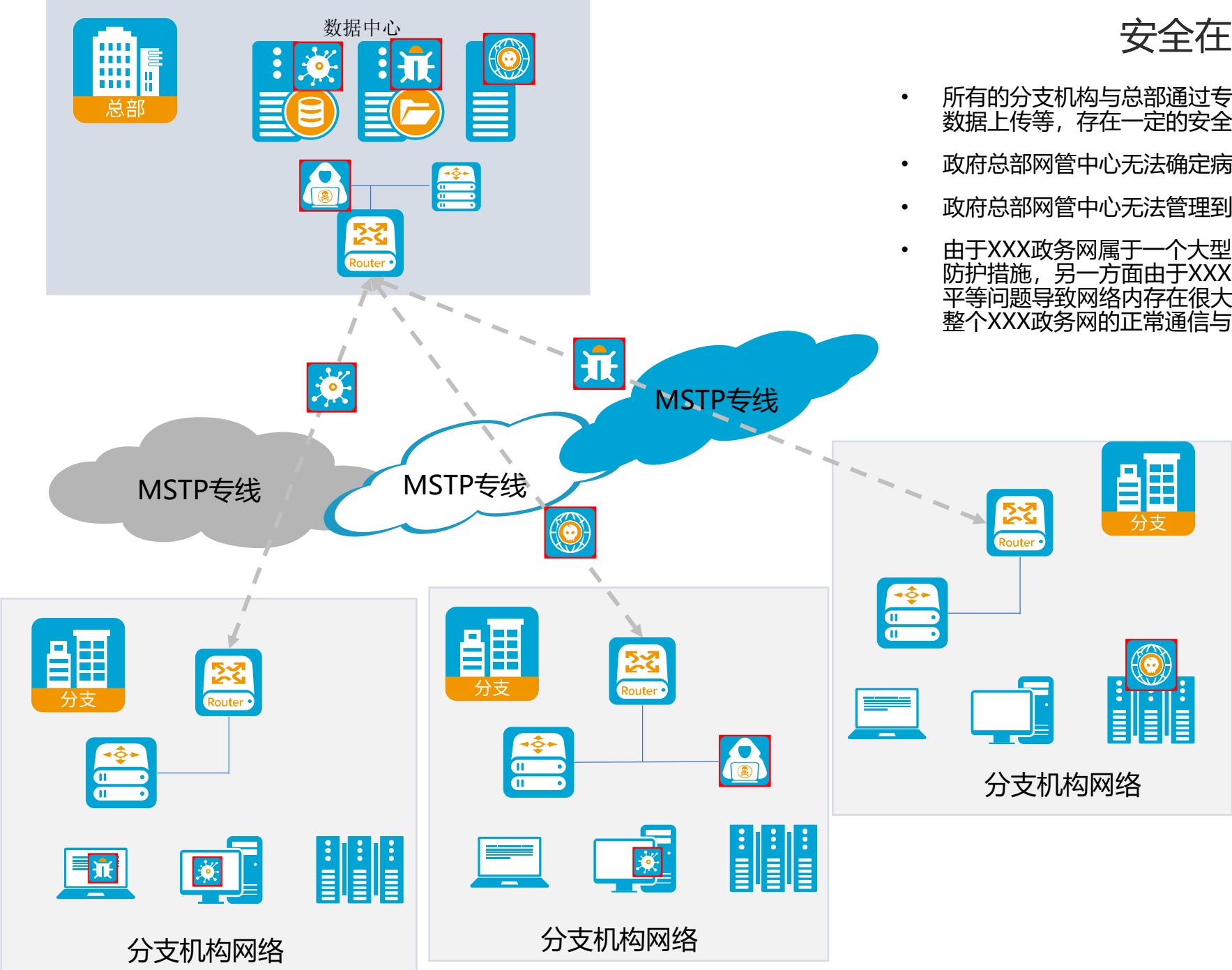


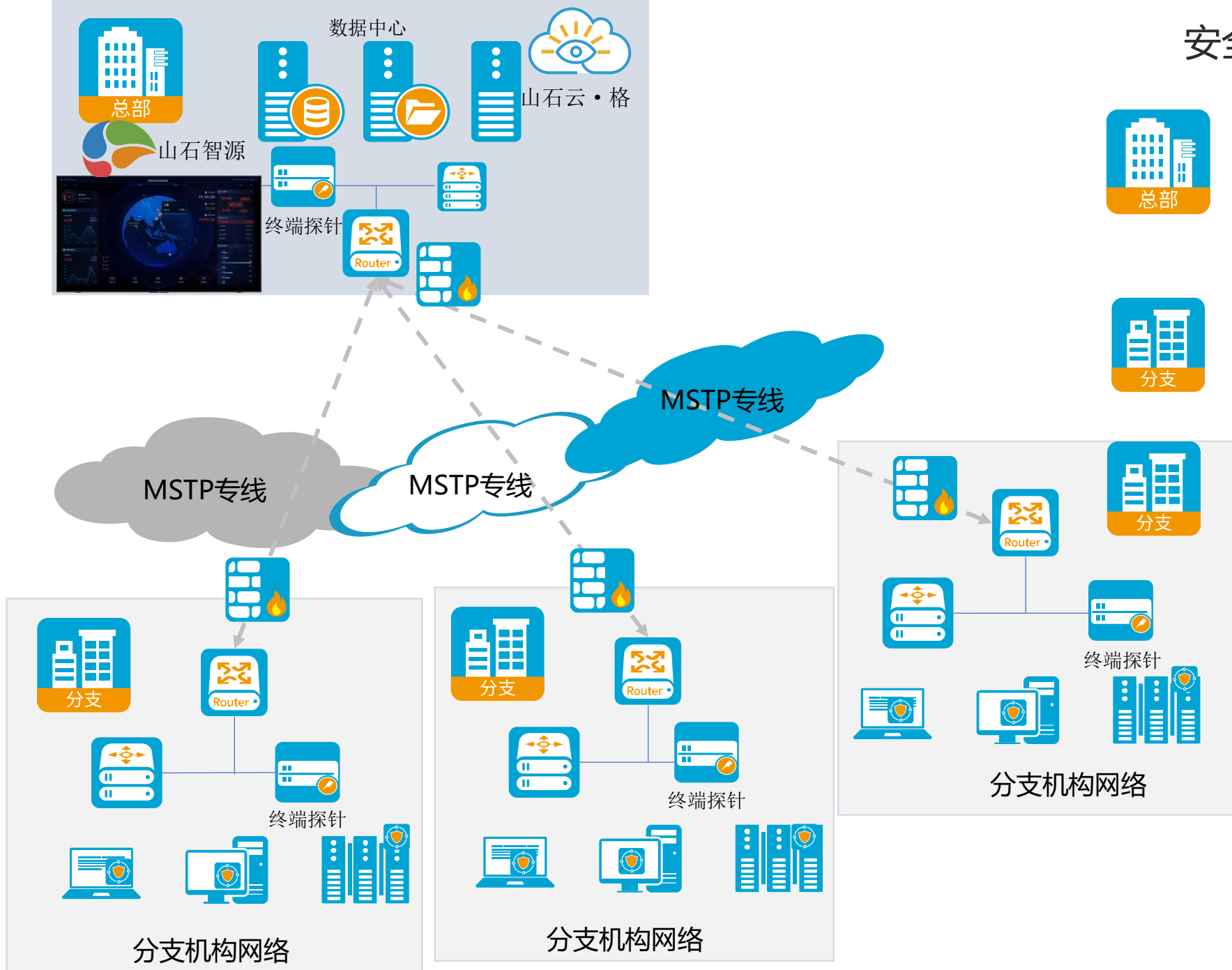
安全在线监控需求分析

- 所有的分支机构与总部通过专线连接，通过专线与总部进行资源共享，数据上传等，存在一定的安全风险隐患。
- 政府总部网管中心无法确定病毒源，无法查看整网的安全健康状况。
- 政府总部网管中心无法管理到分支机构。
- 由于XXX政务网属于一个大型的局域网，且网络内部没有很好的安全防护措施，另一方面由于XXX属政务的网络较大，下级管理人员IT水平等问题导致网络内存在很大安全隐患，一旦大面积暴发，将会影响整个XXX政务网的正常通信与业务系统运行



如图所示：总部会被攻击及传染所有类型的病毒及恶意代码，然后数据中心会攻击、感染所有上联的分支机构中的设备

安全在线监控治理解决方案



- 部署：山石智源（态势感知）及相关探针；
- 部署：数据库中心 山石云·格保护云环境；
- 部署：总部出口安全网关NGFW，开启入侵防护与病毒过滤功能



- 部署：山石智源-探针；
- 部署：终端安全产品；
- 部署：分支出口安全网关NGFW，开启入侵防护与病毒过滤功能，流量管控；



分支机构网络

安全在线监控治理方案价值

