# 广东省灭火救援指挥中心升级改造项目-智能化系统集成服务完善优化子项目需求

# 目　录

# 第一章 项目概述

## 1.1. 项目概述

### 1.1.1. 项目背景

近年来，随着国家对网络安全的高度重视，国家也对于安全提出了相关政策法规及技术标准，包括《网络安全法》，《网络安全等级保护基本要求》，《关键信息基础设施网络安全保护基本要求》等，且针对网络安全运营者提出不同的建设要求。同时《消防救援队伍信息化发展规划》（2019-2022）也明确强调，要重点以数据安全和应用安全为核心，采用先进的技术理念，开展各级各资产的安全防护体系建设，提升 “身份要认证，访问要授权，数据可管控，攻击可阻断，行为可溯源，态势能感知”的信息化安全保障体系。

### 1.1.2. 建设目标

本次项目目标是建设安全防护设施、流量溯源监控系统，网络准入系统与网络管理系统。从而提高总队在政务外网及应急指挥调度网的安全防护、访问控制能力、网络防病毒能力、安全威胁探测能力与网络管理能力，满足等保 2.0 三级要求。增强总队、总队直属单位及支队在政务外网及应急指挥调度网的网络流量朔源取证分析能力。实现总队在政务外网的网络准入管理。加强政务外网与应急指挥调度网的网络信息化管理能力。最终达到全省网络安全运行联网监控的目标。

### 1.1.3. 建设内容

本次项目网络系统由总队统一立项建设，部署分总队与支队两级部署，包含网络安全防护能力建设、流量溯源及安全运营平台建设、网络准入系统建设与网络管理系统建设，通过总队、支队两级联动，实现全省网络安全监控预警，具体建设内容如下：

**（1）网络安全防护能力建设**

总队部署防毒墙与防火墙基础网络安全防护设备，补全总队基础防护能力；

建设 3 台下一代防火墙设备，部署在应急指挥调度网外联部局、支队与直属单位链路之间，负责补全应急指挥调度网安全防护能力；

建设 2 台防毒墙设备，部署在政务外网与应急指挥调度网，串联在网络出口与上级单位链路之间，加强总队网络防病毒防御能力；

在政务外网与应急指挥调度网入网终端与服务器中部署终端安全系统应用，为关键业务设备与终端提供病毒与入侵攻击等威胁防御能力，防御病毒的感染与传播，解决现有总队终端防护能力薄弱问题。

**（2）流量溯源及安全运营平台建设**

在总队搭建流量溯源及安全运营平台，在支队部署流量探针模块，通过流量分析、态势感知等技术，针对全省政务外网与应急指挥调度网网络安全进行实时监控预警，并根据流量分析溯源攻击行为与违规行为。

在总队内网建设 1 套流量溯源及安全运营平台，政务外网出口路由器与应急指挥调度网核心处旁挂 1 台流量探针，流量探针采集网络核心的镜像流量，汇总采集流量上传平台分析；

各支队及总队直属单位，在政务外网与应急指挥调度网核心处旁挂 1 台流量探针；

**（3）网络准入系统建设**

在总队政务外网网络内网部署 1 套网络准入控制系统，实现对接入的总队政务外网终端进行入网控制，阻断非法的、未申报的 IP 地址终端接入。

**（4）网络管理系统建设**

在总队政务外网与应急指挥调度网各部署 1 套网络管理系统，对接部局、总队（含直属单位）、各支队以及大队/站各网络节点，实现实时网络状态监控，集中管理维护与集中故障管理处置，使网络安全稳定的持续运行。

## 1.1.4. 总投资及资金来源

本项目建设总投资为 XXX 万元。

# 第二章 项目现状及需求分析

## 2.1. 现状描述

### 2.1.1. 网络现状

省消防救援总队主要的信息化应用部署在电子政务外网以及应急指挥调度网。相关网络划分为：政务外网、应急指挥调度网、互联网，网络示意图如下：

总体网络拓扑（政务外网、应急指挥调度网、互联网等）

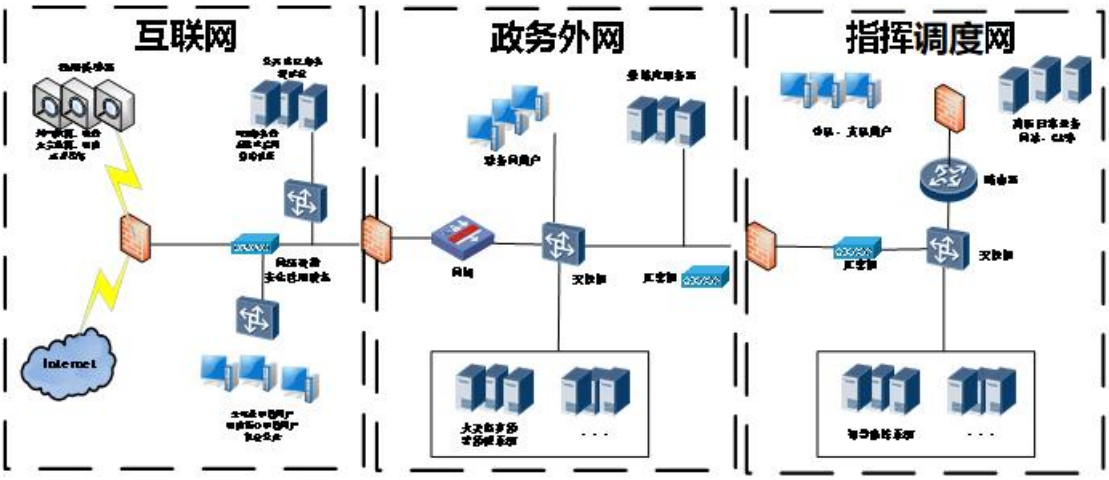


图 2- 1 总体网络示意图

广东省消防救援总队政务外网接入网按安全域功能划分，可以分为政务网外联边界区、业务服务区、核心交换区、专网边界接入区和楼层办公区。

广东省省消防救援总队政务外网拓扑图如下图所示：

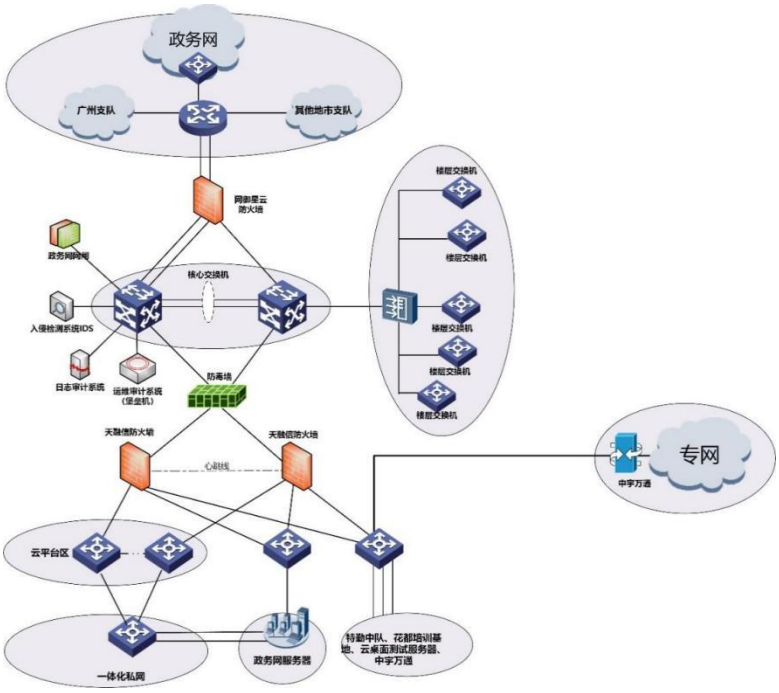
政务网
广州支队
其他地市支队
网御星云
防火墙
政务网防火墙
核心交换机
入侵检测系统IDS
日志审计系统
运维审计系统
(堡垒机)
防毒墙
天融信防火墙
天融信防火墙
心跳线
楼层交换机
楼层交换机
堆叠交换机
楼层交换机
楼层交换机
专网
中宇万通
云平台区
一体化私网
政务网服务器
特勤中队、花都培训基地、云桌面测试服务器、中宇万通

图 2- 2 政务外网拓扑图

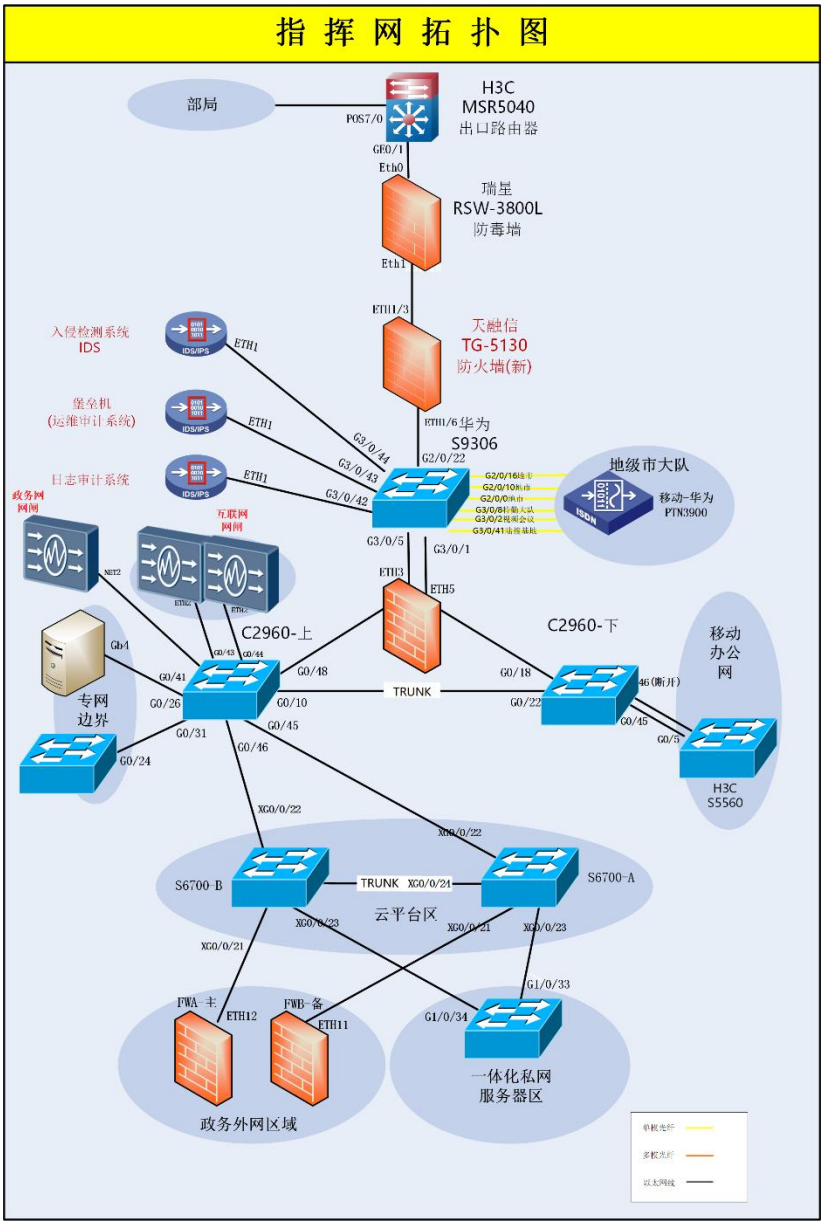


图 2-3 指挥网拓扑图

## 2.1.2. 存在问题

### 2.1.2.1. 缺乏网络安全防护能力

总队政务外网及应急指挥调度网的安全防护基本处于“裸奔”状态，网络中用户可以较容易实现私有网络搭建、实现跨网络连接，无法按照传统的网线和交换机端口来保证网络边界的完整，网络边界很有可能因为有线、无线网络设备的

连出，造成网络边界的被破坏，造成有不明终端穿越网络边界接入。因此中间缺乏防火墙、安全威胁探测等安全设备。在 2021 年护网行动中，共发现病毒 3000 余起事件，网络中传播病毒无法从关键节点处进行拦截，政务外网、应急指挥调度网的网络出口缺少相关的防病毒类的隔离设备，同时缺乏终端防护设备。

#### 2.1.2.2. 缺乏网络安全流量溯源与分析手段

**网络层面**：当前消防总队在网络监控方面缺乏网络异常流量采集和分析能力，无法在网络设备层面获取到流量数据，无法解决网络 NAT 地址转换溯源问题，导致在业务网络变更、网络故障、异常访问等网络异常中缺乏感知及告警能力。

**安全层面**：当前网络中，安全设备各自防护容易导致割裂的安全防御，无法协同作战，提供有效的整体安全防护，甚至导致安全运维复杂化。基于割裂的安全防御所产生的安全现状数据也将成为一座座安全孤岛，难以协同共享，导致碎片化的安全认知，只能看见碎片化的局部安全，无法形成统一的整体可视。

#### 2.1.2.3. 缺乏网络准入控制管理手段

网络资产台帐不清晰。总队至支队政务外网全网终端台账信息不全，终端数目众多且物理位置分散，无法实时对全网终端接入的终端类型及数量、IP/MAC 地址、接入位置等信息进行实时有效的统计及展示，不利于对终端资产进行有效管理和制定安全管理策略。

接入终端身份不明确，行为无管控。全省消防政务外网入网终端对应人员的身份信息真实性、合法性无法精确获取，人员随意使用任意终端都可以正常接入网络进行资源访问，同时对非法终端或用户没有强制有效的技术手段进行阻断隔离。

#### 2.1.2.4. 缺乏对各层级网络管理与监控手段

目前总队经过多年的信息化建设，各种不同的应用和业务系统都在网络上运行，对网络的依赖越来越大，总队政务外网和应急指挥调度网已经是由多个厂家

设备组网的庞大数据网络，现有管理手段已经无法满足政务外网（部局-省政数局-总队-支队）、应急指挥调度网（部局-总队-支队-大队/站）各层级的网络管理与监控需求。无法实现整个网络的集中管理维护、集中故障管理与性能监测，当出现网络性能下降、网络断开的情况时，消防战士及维护人员无法及时做出判断，并采取有效措施加以解决，严重影响总队各项业务工作的开展。

## 2.1.3. 需求分析

### 2.1.3.1. 总队政务外网安全防护能力建设需求

在总队政务外网出口路由器部署 1 台防病毒墙，串联在部局与总队网络链路之间，通过增加设备保证网络边界完整性，对病毒木马等流量进行安全防护的拦截。传统防御方式的主旨是将攻击者拒之门外，然而，随着攻击手段的多样化、隐蔽化、复杂化，传统的防御方式往往疲于应对。为了改变网络空间攻守力量不对称性，弥补传统防御方式的不足，快速感知威胁，延缓攻击，保护资产安全，通过下一代防火墙集成防病毒，WAF 等能力，进行实时动态防御。

### 2.1.3.2. 总队应急指挥调度网安全防护能力需求

总队应急指挥调度网按照等级保护定级指南，建设相关安全防护、安全审计能力。需在网络出口侧部署入侵检测与防御能力，对应用协议、异常行为、恶意文件的检测和防护；需在安全管理区域部署运维审计与管理平台对运维人员操作关键基础设施设备的行为进行记录，部署日志审计平台针对接入总队应急指挥调度网的网络设备日志、安全能力日志进行统一收集、集中分析、集中存储，满足安全审计要求；需在安全管理区域部署主机安全及管理系统，加强终端与防病毒、高级威胁防护能力，终端安全统一管理能力。

### 2.1.3.3. 全省流量溯源及安全运营平台建设需求

目前总队的政务外网的安全管理无法对应急指挥调度的总队直属单位、支队

的网络、总队级局域网区域的全面监测进行流量分析，无法实现对核心业务数据的长期实时安全监测分析能力。需建设流量溯源及安全运营平台，建立全省消防全流量安全分析及溯源取证机制。

**总队需求：**

需在总队政务外网部署 1 套流量溯源安全感知平台，在政务外网及应急指挥调度网网络出口部署 1 套流量探针和，探针实现对总队出口进行监测进行采集和流量分析；流量溯源安全感知平台通过接收并分析所有流量综合探针的告警日志，实现安全事件实时预警、事件关联分析、事件处置闭环、全网安全态势可视化。

**总队直属单位及支队需求：**

需在 3 个直属单位及 21 个地市支队政务外网及应急指挥调度网网络出口各部署 1 台网络分流器和流量溯源探针，实现对该支队的出口流量的镜像采集，并转发至安全运营平台进行网络流量安全分析。

### 2.1.3.4. 总队网络准入系统建设需求

目前总队至支队政务外网全网终端台账信息，全省消防政务外网入网终端身份不明确，行为无管控，总队政务外网缺乏 IP 资源高效流程管理，需通过网络准入控制系统，杜绝非授权终端接入。

**总队需求：**

需在总队政务外网网络内网部署 1 套网络准入控制系统，实现对接入的总队政务外网终端进行入网控制，阻断非法的、未申报的 IP 地址终端接入。

### 2.1.3.5. 网络管理系统建设需求

目前总队管理手段已经无法满足政务外网（部局-省政数局-总队-支队）、应急指挥调度网（部局-总队-支队-大队/站）各层级的网络管理与监控需求。无法实现整个网络的集中管理维护、集中故障管理与性能监测，当出现网络性能下降、网络断开的情况时，消防战士及维护人员无法及时做出判断，无法采取有效

措施加以解决，严重影响总队各项业务工作的开展。

**总队政务外网需求：**

需在总队政务外网部署一套网络管理系统，实现政务外网（部局-省政数局-总队-支队）各层级的集中管理维护、集中故障管理与性能监测，掌握全网及关键告警、性能状态等信息，及时发现异常状态并针对对应的指标监控进行处理，从而保证网络的正常运行。

**总队应急指挥调度网需求：**

需在总队政务外网部署一套网络管理系统，实现应急指挥调度网（部局-总队-支队-大队/站）各层级的集中管理维护、集中故障管理与性能监测，掌握全网及关键告警、性能状态等信息，及时发现异常状态并针对对应的指标监控进行处理，从而保证网络的正常运行。

### 2.1.4. 非功能需求分析

#### 2.1.4.1. 可靠性需求

在日常运行中，需要通过 7×24 小时不间断的系统性维护服务，确保平台具有良好的安全性和可靠性，同时结合备份恢复、入侵监测、防火墙等工作，共同构建起多层次，全方位的安全保障体系。另外，同时通过日常维护使系统具备一定的容错性，避免由于误操作或其他原因导致的系统错误。

#### 2.1.4.2. 易用性需求

在技术的使用和产品的选择方面要考虑其技术的成熟性，同时，在产品方面要考虑适用和实用，保证技术、性能满足网站建设需要。所提供的系统设计方案具有大量成功的实施案例，方案稳定成熟，有丰富的经验可以借鉴，能够确保用户在最短的时间内达到应用需求，并充分降低后期维护的影响。

#### 2.1.4.3. 响应速度需求

响应时间指标包括页面响应时间和数据响应时间。页面响应时间为用户点击操作页面后的反应，页面反应时间不超过 3 秒。数据响应时间为用户点击后的到结果的时间，包括服务器反应和数据传输到客户端，普通页面不超过 3 秒，跨年历史数据最大不超过 10 秒。系统的年可用率≥99.9%，由于偶发性故障而发生自动热启动的平均次数＜2 次/年。常规数据分析响应时间＜3 秒，历史数据分析响应时间＜5 秒。

### 2.1.5. 安全需求分析

#### 2.1.5.1. 业务保障安全需求

信息安全是本项目得以顺利实施的前提。本项目的安全体系应实现如下具体安全目标：

表 2- 6 安全体系具体安全目标

| 安全目标 | 描述 |
| --- | --- |
| 数据安全性 | 本项目应不包含涉密数据，对于消防工程指挥等敏感数据基于软件应用涉及加强数据管控，数据的共享交换存在的安全风险需要结合省消防救援总队的行政管理手段予以解决 |
| 身份真实性 | 能对通讯实体身份的真实性进行鉴别 |
| 信息机密性 | 保证机密信息不会泄露给非授权的人或实体 |
| 信息完整性 | 保证数据的一致性，能够防止数据被非授权用户或实体建立、修改和破坏 |
| 服务可用性 | 保证合法用户对信息和资源的使用不会被不正当地拒绝 |
| 不可否认性 | 建立有效的责任机制，防止实体否认其行为 |
| 系统可控性 | 能够控制使用资源的人或实体的使用方式 |
| 系统易用性 | 在满足安全要求的条件下，系统应当操作简单、维护方便 |
| 可审查性 | 对出现的网络安全问题提供调查的依据和手段 |

#### 2.1.5.2. 信息安全合规性要求

本项目在系统安全方面的设计，需按照按国家标准《信息安全技术　网络安全等级保护基本要求》（GB/T22239-2019）进行安全系统设计，按照《信息系统

安全等级保护定级指南》（GB/T22240）的要求确定信息系统安全保护等级。

# 第三章 建设方案

## 3.1. 建设思路

为进一步增强全省网络安全防范能力，构建“重防范、强溯查”的安全网络办公环境，建设完善的网络监控系统体系，网络监控系统作用于网络安全防范，主要实现防范网络入侵、病毒传播等安全防护，监控全省网络运行状况，对接入设备进行准入管理，发生安全事件后的溯源定位。

## 3.2. 总队安全防护建设

### 3.2.1. 政务外网-提高威胁防护能力

#### 3.2.1.1. 系统概述

本次项目在总队政务外网建设安全防护设施，为总队政务外网提供高级威胁检测、威胁情报应用、攻击模型自动化分析、重点保护对象分析、网络脆弱性分析、动态样本分析能力，加强网络的基本安全能力。

#### 3.2.1.2. 系统功能

通过部署具有安全威胁防护功能的防病毒墙，利用其特征检测、流检测和基于沙箱检测技术的文件检测，能发现网络攻击并且能够针对有效分析场景和 APT 攻击进行进一步分析与研判。

**特征检测**

在丰富、全面的特征检测规则库的基础上，利用特征匹配能力，优化规则库，对攻击进行有效性判定，确保事件准确性，提升有效性检测能力。对病毒、木马、蠕虫、僵尸网络、缓冲区溢出攻击、拒绝服务攻击、扫描探测、欺骗劫持、SQL 注入、XSS 攻击、网站挂马、隐蔽信道、AET 逃逸、C&C 行为等各种威胁的全面有效检测，针对僵木蠕类攻击、Web 攻击等热点攻击手段的攻击特征进行进一步

优化，确保有效的检测能力。

**恶意代码检测**

采用检测方法，多种核心检测技术手段：二进制检查、堆喷检测、ROP 利用检测、敏感 API 检测、堆栈检测、Shellcode 检查、沙箱检查等，可以检测出 APT 攻击的核心步骤。可实现包括对：未知恶意代码检查、嵌套式攻击检测、木马蠕虫病毒识别、隐秘通道检测等多类型未知漏洞（0-day）利用行为的检测。同时，通过 TAR-AIO 威胁分析平台进行威胁分析，有效发现 APT 攻击。

**取证与研判分析**

为了应对网络安全事件处置过程中的分析研判诉求，支持采用攻击事件完整流量存储能力。可通过上报事件进行分析研判，不仅具备原始流量文件下载的能力，还能够对原始流量进行解析，支持研判分析可视化呈现，协助收集尽可能多的信息或证据。

**联动处置**

可通过标准 Restful API 接口，支持与网络边界防护网关设备、终端等进行联动实现处置动作。利用自身的威胁检测与威胁分析能力，发现攻击行为，通过联动响应策略，对发现的攻击源或被保护的目标主机进行相应的处置动作，实现自动或手动的联动处置，实现安全事件快速闭环。

**可视化威胁感知**

通过攻击者视角、被攻击者视角、样本视角、事件视角等多维线索聚合，深度挖掘可疑关联，提供攻击者、被攻击者双向的威胁分析起点，在攻击面与被攻击面之间寻找深度隐藏的线索关联。

**集中管理与分析能力**

针对各类日志的不同特性，进行针对性的有效分析，按照有效分析场景进行针对性的可视化呈现。包括 WEB 攻击、暴力破解、脆弱口令等，产品还将根据实际情况进行进一步扩展，增加更多的分析模型与可视化呈现。

### 3.2.1.3. 部署防病毒墙

在总队的政务外网二级网出口路由前部署一台防病毒设备，启动病毒防护策

略。病毒防护策略用于组织针对各种协议的病毒防护，这些协议包括 HTTP、FTP、SMTP、 POP 和 IMAP，用户可以根据实际的网络环境和场应用组织适当的病毒防护策略，以达到高效合理的应用系统资源和更加有效的病毒防护效果。同时应对的不同需求使用三个病毒策略模板，分别为标准病毒防护模板、WEB 病毒防护模板和标准病毒检测模板，分别做不同的应对。

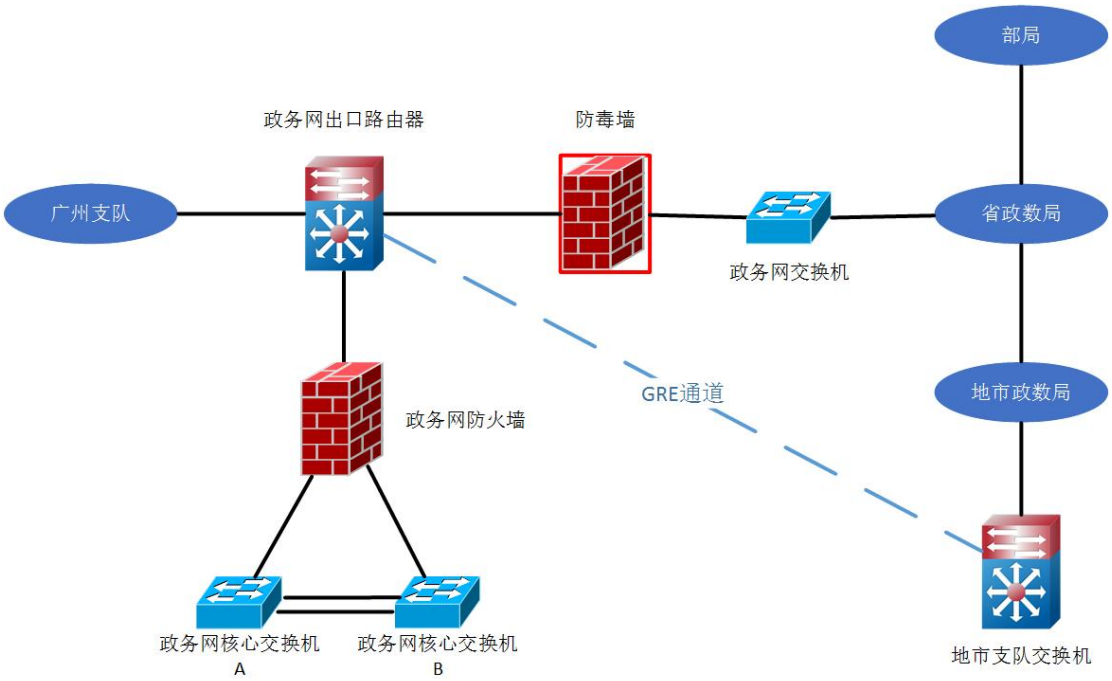


图 4- 1 防病毒墙部署示意图

### 3.2.1.4. 部署终端安全管理系统

总体来讲，终端计算机具有点数多、覆盖面大、难管理等特点，加之信息安全人员人手有限，终端分布环境复杂，威胁风险事件较多，使信息安全人员对终端安全工作处于被动状态。在终端安全方面，一旦出现病毒感染、恶意破坏传播、数据丢失等事件，将会给造成严重损失，后果不堪设想。现由于各部门及员工对计算机的合规使用、对终端安全以及病毒防范的意识和能力参差不齐，已严重影响到计算机信息系统安全性。正因如此，全方位做好信息系统的终端安全防护工作。因此本方案将针对终端建设一套终端安全系统，以确保的日常办公安全、稳定、高效运行。

终端安全系统为C/S部署、B/S管理方式，终端安全系统部署无需对网络进行调整或对网络设备进行配置，系统控制中心采用旁路方式接入内部网络，在办公环境所有主机上（包括物理PC终端、虚拟机、物理服务器、云主机）安装系统客户端代理，被管理主机能连通控制中心即可。管理员通过B/S管理中心对全网已安装客户端代理的主机进行策略设定下发、监控管理、安全审计等操作，客户端代理则负责策略接收、任务执行、日志上报等事项，以便整体保障终端安全性。

通过终端安全系统的全面部署应用，提供全网终端病毒、木马、入侵攻击等威胁防御能力，通过人工智能SAVE引擎、全网信誉库、云查引擎、行为分析等技术，全面应对威胁，有效防御新型未知病毒的感染与传播，解决现有信息系统安全问题，构建百分百多维度威胁防御体系。

## 3.2.2. 应急指挥调度网-增强安全防护能力

### 3.2.2.1. 系统概述

依据应急指挥调度网现状与实际需要，依据国家相关政策法规要求，建设目标是：落实《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）对三级系统的安全保护要求，并基于现代信息系统安全保障理论，采用现代信安全保护技术，按照一定规则和体系化的信息安全防护策略进行的整体设计。参照应急指挥调度网已有的安全能力，安全建设需补充覆盖以下内容：

### 3.2.2.2. 部署汇聚防火墙

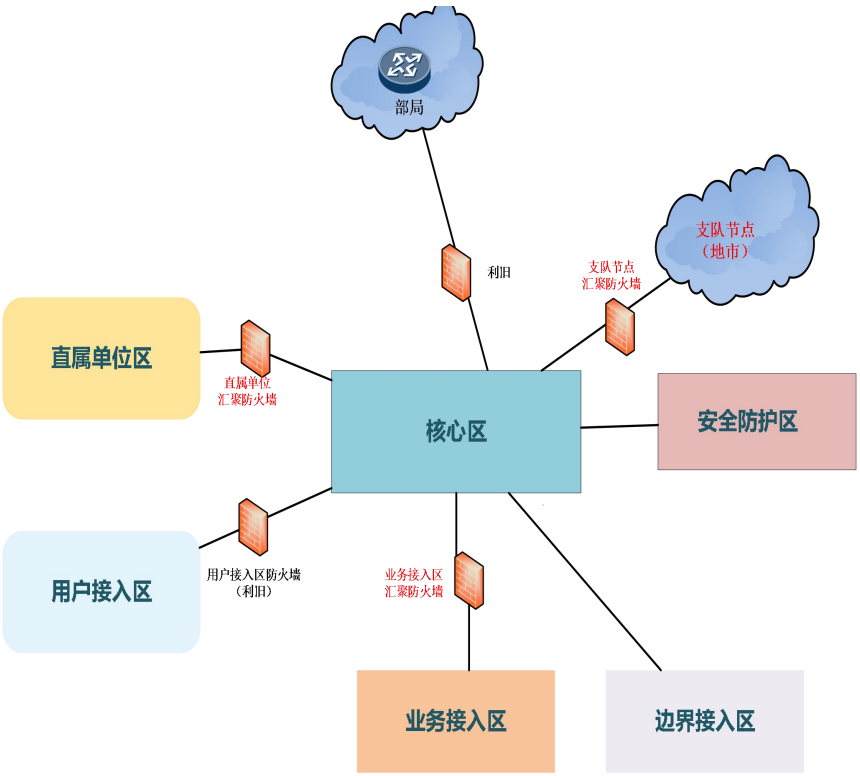


图 13 网络防火墙部署设计

核心区与地市支队的区域部署一台汇聚防火墙，提高总队应急应急指挥调度网出口的访问控制能力。

核心区连接直属单位区架设专属的汇聚防火墙，作为直属单位与总队之间的安全防护。

核心区和业务接入区之间部署汇聚防火墙，用于保护重要的业务系统安全。

核心区和用户接入区之间通过利旧部署防火墙，用于防护用户区域的安全，同时还可以起到用户访问控制的限制能力。

#### 3.2.2.3. 部署防病毒墙

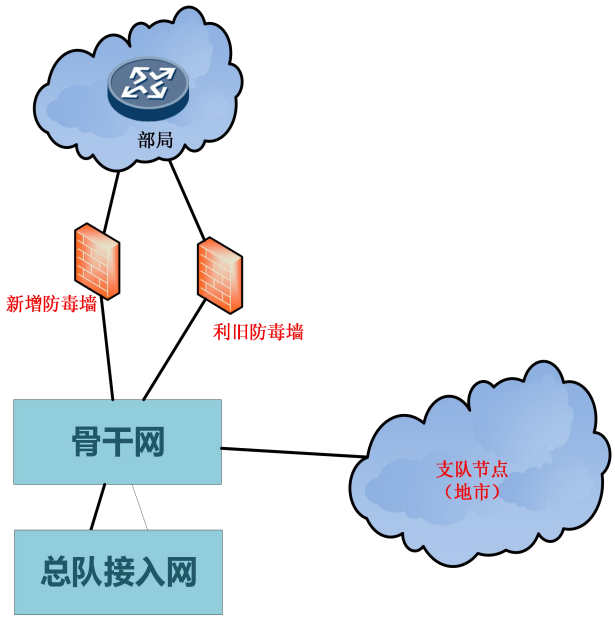


图 14 网络防毒墙部署设计

在新增应急指挥调度网与部局互联新增防毒墙，同时在原指挥调度网的骨干网与部局互联利旧原网络中的防毒墙，组成主备双链路同时防护，提高全省应急指挥调度网的网络防病毒能力。

#### 3.2.2.4. 升级改造原有病毒库

对总队原有的网御星云防病毒系统病毒库上进行升级改造，增加 windows 系统端防病毒授权、linux 服务器端杀毒软件授权，提升防病毒、漏洞扫描补丁、杀毒等防护能力，病毒库有效时长为期三年，不限有效次数。

## 3.3. 全省流量溯源及安全运营平台建设

### 3.3.1. 系统概述

本次项目通过建设全省流量溯源及安全运营平台，建立全省消防全流量分析取证机制，实现全流量原始数据包存储、全量数据检索、应用元数据解折、攻击回溯取证和数据安全分析的目的。

### 3.3.2. 系统功能

通过分光器和镜像方式采集网络核心出口流量，不改变物理网络拓扑的情况下，通过收集、汇总与分析各网络层级的网络流量，业务延迟、协议占比，让运维人员充分了解整体网络安全运行情况。同时，通过 TCP 会话回溯，避免花费大量精力还原故障现场，能够迅速响应，将业务影响降至最小，增强消防总队对网络安全预警与安全事件管理能力。

#### 3.3.2.1. 网络流量采集

通过传统的镜像、分光等网络引流技进行网络流量采集，网络流量不再成为运维人员的黑盒子，对网络流量采集进行完整采集。同时，采集设备支持全局以及单实例分发流量，采集包速，CPU，内存等资源消耗强控制，确保对系统零入侵，保障业务网络正常运行。

#### 3.3.2.2. 安全实时分析

系统支持大规模数据的处理速度。数据处理量级不低于 10 万 EPS。预置海量威胁检测模型和安全分析模型，扫描探查检测类模型、渗透攻击检测类模型、获取权限检测类模型、命令控制检测类模型、资产破坏类检测模型。自定义规则模型、统计模型、情报模型、关联模型等安全分析场景。

#### 3.3.2.3. 异常访问行为分析

系统需支持实时监测异常日志信息，通过规则模型、统计模型、机器学习模型和无监督的聚类分析。及时发现用户、系统或设备存在的可疑行为。利用网络分析的方法，关联用户和行为，通过多维态势可视化系统实时展现行为威胁状况。

#### 3.3.2.4. 深度感知分析

系统支持多维度的信息和多源数据进行整合、关联、智能分析和预测，基于攻击意图、攻击策略、攻击方法、攻击次数、攻击时间、处置状态等影响因子构建资产评级模型，基于海量安全告警分析内网资产中潜在的失陷资产。

#### 3.3.2.5. 潜伏威胁检测

系统支持对网络数据包、文件元数据、终端日志、威胁情报、沙箱报告、漏洞知识库等进行智能分析，重建攻击全路径，洞悉发动攻击的人员、目标、时间、地点和手段，发现高级潜伏威胁。

#### 3.3.2.6. 多维态势感知

系统支持可视化模块，从多个维度全面展现安全态势，便于研判安全事件。支持监测外部对内部攻击、内部跨安全域横向攻击、内部外连攻击等多种威胁方向，从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示安全态势的可视化呈现。

#### 3.3.2.7. 攻击追踪溯源

系统支持基于资产安全告警和攻击者的追踪溯源功能，实现对安全告警事件和攻击者的追踪与取证，并提供溯源报表的一键智能下载。能够对告警事件实现闭环式溯源，并提供对告警事件原始日志的查询服务。提供攻击者追踪溯源大屏，基于大数据关联分析技术，聚合展现疑似黑客组织 IP 组、攻击引发告警类型以及类似攻击行为手段，可基于时间轴动态查看攻击行为取证列表，实现对攻击者的精准追踪溯源。提供资产威胁溯源可视化分析大屏，为安全运维人员聚合呈现资产被攻击行为、影响资产范围、告警取证信息等，支持针对网内任意资产查询并呈现被访问趋势、被攻击趋势、被攻击手段、资产健康状态，资产评分等信息。

#### 3.3.2.8. 安全事件调查取证

系统支持通过搜索、聚合、关联等调查取证手段，提供攻击事件数据包、攻击者设备指纹等举证信息。支持基于源、目的、事件名、攻击意图等多种聚合调查方式，从不同维度聚合统计安全事件。可以关联资产信息、威胁情报、弱点详情、安全事件、处置方式等多维数据进行调查取证。

### 3.3.3. 部署流量溯源及安全运营平台

在总队部署全省流量溯源及安全运营平台（含 1 台硬件流量探针+1 套平台），分别旁挂在核心交换机和二级网出口路由器上，使用镜像口分别对总队内网与省-市间流量进行监控。通过流量采集、分析技术能实时的监控分析网络运行情况，及时发现网络及应用系统的异常行为，并提供强大的网络分析功能，保障网络安全高效持续运行。安全运营平台对接总队三网融合平台，对其网络安全情况进行统一监控。

在支队部署流量探针，旁挂在支队出口路由器上，使用镜像口对支队上联流量进行监控，并把采集信息传送至总队流量溯源及安全运营平台进行网络流量全况分析并且展示。

通过全流量分析、多维度的有效数据采集和智能分析能力，实时监控安全事件态势、横向威胁和外连风险等，让管理员可以清楚的感知全网安全情况，从而辅助决策。

通过全省流量溯源及安全运营平台，每季度出具一份季度分析报告，为总体提供数据支撑和决策分析。

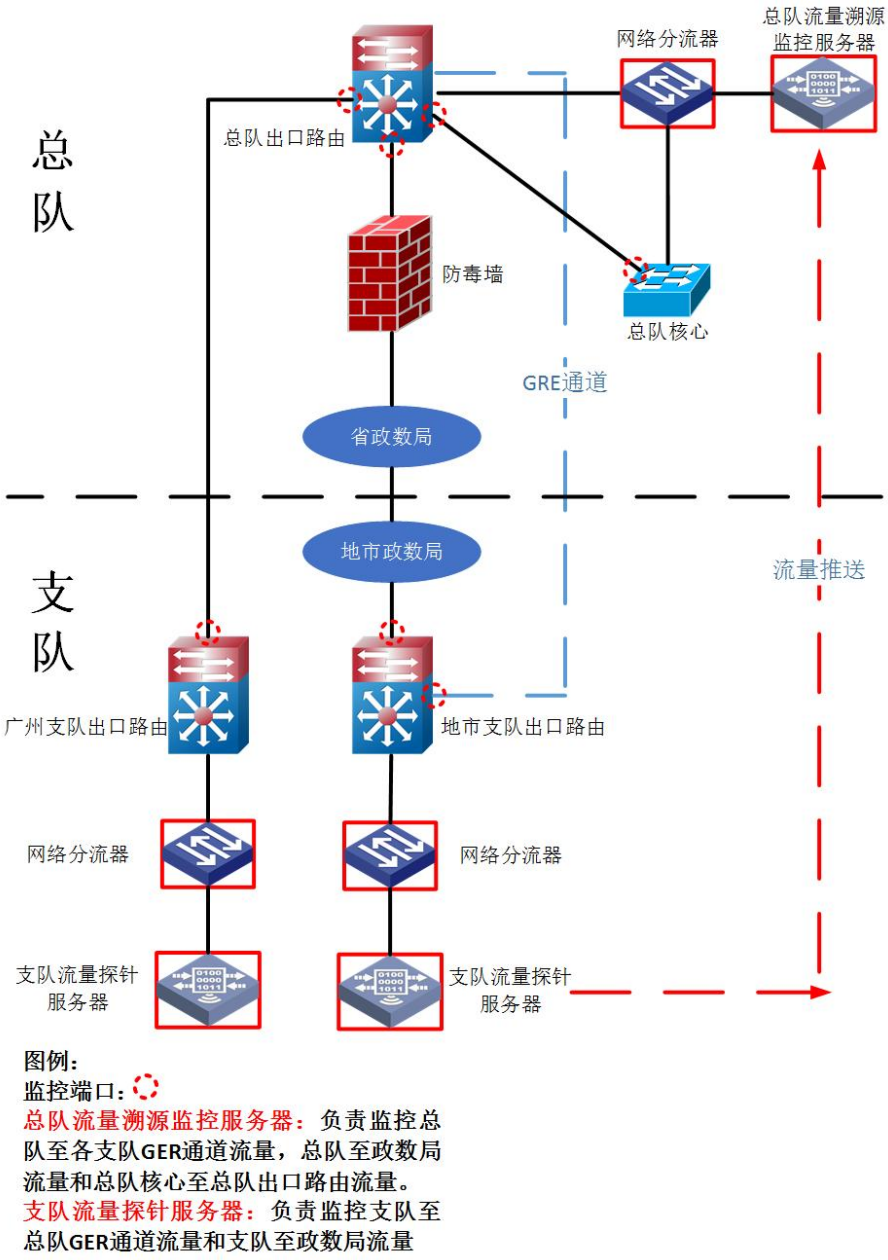


图 4- 3 流量溯源监控系统部署示意图

搭建完全省流量溯源及安全运营平台建设部署后，针对总队出口路由器 NAT 前流量及 NAT 流量采集到流量探针进行关联分析，可以快速定位攻击源真实内网 IP。

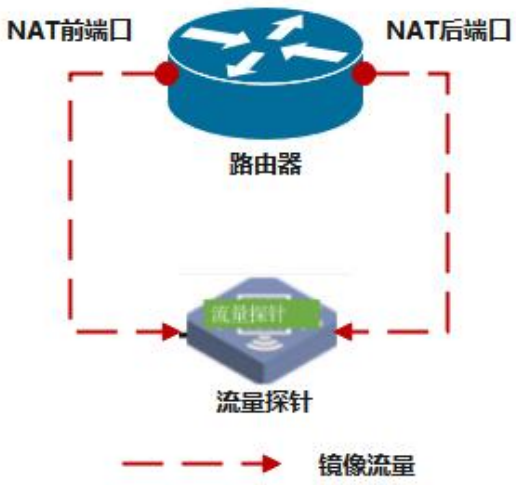


图 4- 4 溯源流程示意图

同时网络流量分析系统软件包含以下功能：

**一是网络流量采集**。通过的镜像、分光等网络引流技进行网络流量采集需求，对需要网络流量采集进行完整采集。同时，采集设备需支持全局以及单实例分发流量，采集包速，CPU，内存等资源消耗强控制，确保对系统零入侵，保障业务网络正常运行。**二是细粒度流量分发**。网络性能、系统安全是业务稳定发展的基础，而各部门出于运维监控的需求，分别在网络中部署复杂多样的网络探针，这对网络总体性能造成了一定影响。**三是多维度流量可视化**。提供多维度、多视角的流量统计，资源拓扑清晰展示资源层级和连通性关系，流量拓扑图提供更直观化流量关系的展示。**四是全网全时流量分析**。支持实时流量分析，及离线数据的回溯；对常见网络流量特征类型进行提取并直观展示。**五是性能可量化**。支持多维度、数据化、证据链、可视化展现网络中的性能指标，实现对异常网络事件的量化功能，为故障排查提供性能支撑。

## 3.4. 网络准入控制系统建设

### 3.4.1. 系统概述

本次项目在总队建设网络准入，把安全充分融合到内网的终端接入控制流程管理中，对任何人、设备、资源均零信任，都要进行层次化、流程化的验证，以终端接入网络为起点到再到访问资源全路径、全方位、高效、安全的节节把控，进行周期性验证的循环，以保障接入终端/人的安全可信，且在整个流程信息进行审记录，形成各类台账报表。

### 3.4.2. 系统功能

通过在总队网络准入控制系统建设，对总队政务外网内部的网络架构将实现规范化、可靠化以及高效化，接入流程和网内安全的制度化，各部门人员在受到统一管理的同时做到规范入网：

#### 3.4.2.1. 全面安全保障

网络准入控制系统一方面能减小实施及安全系统管理难度，通过一系列的安全规划、认证和安全检查、IP 状态审计，能够规范消防政务外网安全管理，树立安全意识，从制度和思想上建立起一条内网信息安全的防线，覆盖从网络安全、系统安全、应用安全、管理安全的多个层面。

#### 3.4.2.2. 安全管理策略落实

准入系统部署成功后，实现原定制的安全管理策略，百分百的落实到每台入网终端，如原内网终端安装杀毒软件等安全策略，在每台终端入网前强制要求进行检查及修复，保证每台入网终端都符合内部定制的安全基线方可入网，终端管理系统的部署使得管理员可以有效的要求和加固用户主机，简化安全管理的工作量。

#### 3.4.2.3. 终端入网管理

系统成功部署后，实时对全网终端接入进行监控，对全网接入终端进行统计及自动根终端类型分类统计（例如：PC、特殊 IP 设备、交换机、移动终端等），结合网络准入控制与网络交换联动，形成网络拓扑、交换机面板展示，实现从全局（网络拓扑）---局部（具体交换机面板）---终端详情（终端 IP/MAC 及类型等信息）来展示以接入终端为中心的相关联信息。

#### 3.4.2.4. 规范网络边界

对内网网中网环境、HUB 设备进行扫描，形成的网中网、HUB、移动终端的单独展示实时列表，并提供对应网络环境或设备的详细网络位置，配合报警机制，能第一时间把违规信息发送给管理员，进而规范网络边界，消除网络盲点。

### 3.4.3. 部署网络准入控制系统

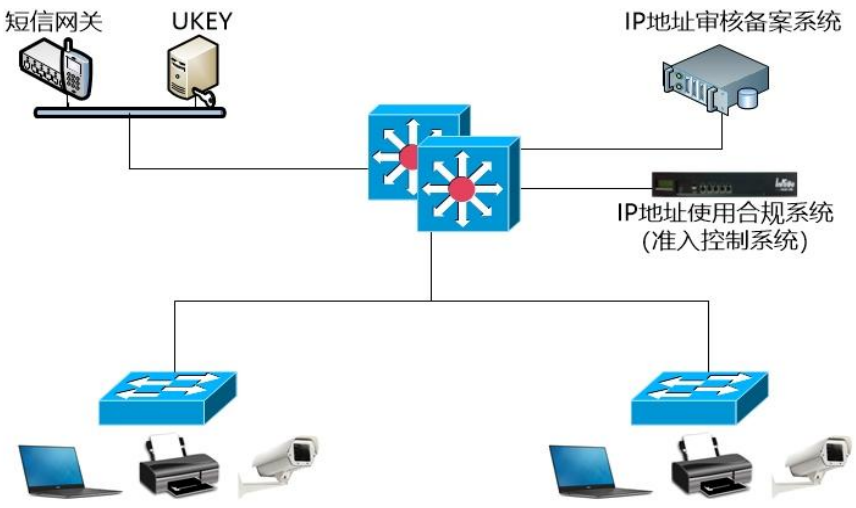


图 4- 5 网络准入控制系统示意图

在总队部署一套网络准入控制系统，对接入的总队政务外网终端进行入网控制。该系统与 IP 地址审核备案系统联动，阻断非法的、未申报的 IP 地址终端接入。对全网 IP 地址上线使用情况进行实时统计。IP 地址审核系统只需网络可达

即可，网络准入控制系统部署要按网络环境进行适配，旁路部署在核心交换机。网络准入控制系统功能如下：

一是设备发现识别。通过在二层网络进行被动监听终端报文、网络准入控制系统使用 SNMP、SSH 等网管协议与交换机联动获取终端信息、镜像流量分析等多种技术手段实现二层网络、三层网络下终端接入实时发现。 同时结合网络扫描、SNMP 尝试等设备特征指纹获取技术，获取到每台 IP 设备的唯一身份标识指纹，从而对设备进行识别（例如：PC、打印机、摄像头等类型）和网络位置定位。

二是终端准入管理。准入控制从管控的严格度上可划分三个级别：端口级（当终端未经准入授权，不能访问任何网络资源）、网关级（只有终端进行跨网段访问才触发准入控制）、网桥级（只有终端访问数据通过准入系统时才能触发准入控制）。

◆端口级准入控制技术有：802.1x、虚拟网关、ARP

◆网关级准入控制技术有：策略由、流量镜像

◆网桥级准入控制技术有：透明网桥

常用的准入有 802.1X、虚拟网关、流量镜像等，但每种准入技术都有自身技术优势和不足。

新终端入网后，会被强制断网并重定向到入网引导流程，通过准入系统行终端安全状态的核实（也可直接通过直接对终端进行拒绝入网或入网而无法再走比对终端安全状态流程），IP 终端合规后才能接入网络，如安装了杀毒软件等要求项，准入系统则自动对入网终端发行，否则会要求安装客户端提示页面。

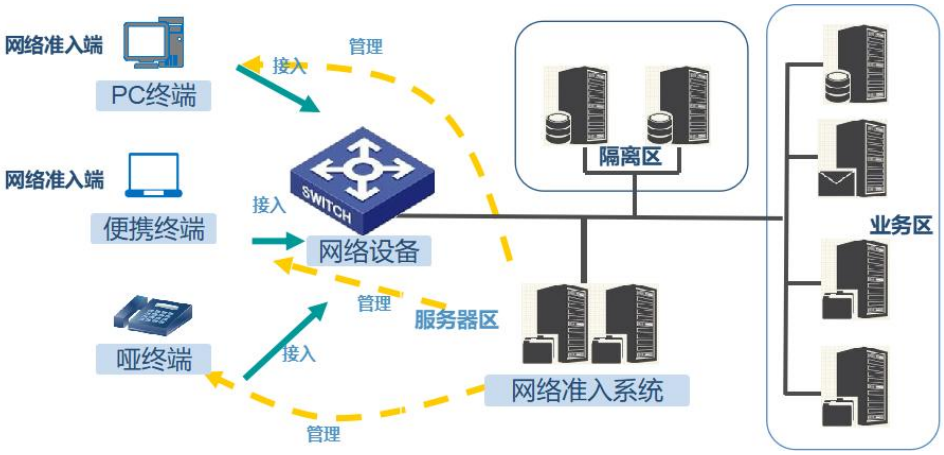

图 4- 6 网络准入控制系统部署示意图

## 3.5. 网络管理系统建设

### 3.5.1. 系统概述

本次项目在总队的政务外网、应急指挥调度网分别建设一套网络管理系统，全方位的监控整个网络各层级的运行情况，实现整个网络的集中管理维护、集中故障管理与性能监测，使消防员及运维人员可以根据网络的运行状态及监控告警，及时发现网络问题，进行设备故障定位和分析，排查网络隐患并及时调整。

### 3.5.2. 系统功能

#### 3.5.2.1. 网络设备管理

网络设备管理支持将网络设备（交换机、路由器、防火墙、WLAN 设备等）接入。对已接入的设备提供告警、拓扑、性能等基本管理功能，并通过对设备进行可视化监控。运维人员通过网络设备详情概览，监控网络设备基本信息，掌握网络设备运行状态。主动监控设备性能指标和告警信息，助力运维人员提前发现网络问题，进行设备故障定位和分析。

#### 3.5.2.2. 配置文件管理

配置文件管理帮助运维人员及时了解网络的配置变更情况，能快速恢复配置文件，避免设备遇到故障而导致设备配置丢失，提高业务运行的安全性和可靠性。设备配置文件被损坏，或由于其他需要，设备配置被修改时，配置文件管理的恢复功能可将已备份的配置文件及上传的配置文件恢复到设备上，快速恢复业务。同时还支持查看配置变更，获取配置变更信息，帮助及时了解网络的配置变更情况。

#### 3.5.2.3. 网络质量检测管理

配置文件管理支持通过 NQA 协议主动在网络设备之间发送诊断报文，测量线路上的丢包率、时延等关键性能指标，从而实现网络质量评估，为网络故障诊断和性能优化提供依据。

#### 3.5.2.4. 终端资源管理

通过终端资源管理，及时掌握终端接入情况，对终端进行统一管理，快速进行故障排查，包括终端 MAC、终端 IP、接入设备名称和端口等。运维人员可以快速查看设备和端口的运行状态、性能指标、告警，进行终端网络故障排查，有效支撑故障协查和故障分责的运维需要。

#### 3.5.2.5. 网络流量分析

网络流量分析可以实时监控全网流量，提供多维度流量分析，帮助及时发现网络中异常流量、了解网络带宽的使用情况。可以从接口、应用、协议等维度展示网络流量状态，为网络宽带规划提供数据支持。以实时监控全网流量，实现网络应用可视、可控，帮助快速定位网络异常，提高网络运维效率。

### 3.5.3. 部署网络管理系统

在总队政务外网部署一套网络管理系统，旁挂在政务外网核心交换机上，分别对总队-省政数局-部局政务外网与总队内网-省政数局-支队之间的网络状况进行监控。

在应急指挥调度网部署一套网络管理系统，旁挂在应急指挥调度网核心交换机上，分别对总队内网-部局与总队-支队-大队/站之间的网络状况进行监控。

对接部局、总队与支队关键核心网络设备，根据网络中已对接设备在线信息提供告警、拓扑、性能等基本，让网络运维人员及时发现并处置相关故障，以保障网络系统能够正常、高效运行。

# 第四章 设备清单

## 4.1. 设备清单

详见设备清单。

| 广东省灭火救援指挥中心升级改造项目-智能化系统集成服务完善优化子项目设备清单 | | | | | |
|---|---|---|---|---|---|
| **序号** | **设备名称** | **配置参数要求** | **数量** | **单位** | **备注** |
| **1.1 应急指挥网-总队安全防护建设** | | | | | |
| 1 | 汇聚防火墙 | 1、配置：双电源，前后风道，千兆电口≥14 个，万兆光口≥12 个，40GE 接口≥2 个；<br>2、性能：吞吐量≥25Gbps，最大并发连接数≥1000 万，每秒新建连接数≥40 万；<br>3、功能：具备访问控制、入侵防御、防病毒、带宽管理、加密流量检测、应用识别、安全虚拟化、流量探针、安全策略调优等能力。<br>4、服务：三年原厂质保服务。 | 3 | 台 | |

| | | | | | |
|---|---|---|---|---|---|
| 2 | 防病毒墙 | 1、配置：冗余电源，千兆电口≥5 个，万兆光口≥2 个；<br>2、性能：三层吞吐量≥40Gbps、防病毒吞吐量≥8Gbps、最大并发连接数≥400 万、每秒新建连接数≥26 万；<br>3、功能：支持漏洞扫描、支撑与漏洞扫描设备联动、支持 IPv4 和 IPv6 双栈协议下的病毒扫描与防护、支持基于策略的病毒扫描与防护、支持多接口可旁路的病毒文件传输监听检测方式、支持隔离病毒源地址、支持恶意地址主动屏蔽、支持快速扫描、全面扫描模式等；4、服务：三年原厂质保服务。 | 1 | 台 | |
| 3 | 数据库审计系统 | 1、配置：冗余电源；千兆电口≥8 个、千兆 SFP 接口≥4 个、千兆多模光模块≥4 个，内存≥32G，硬盘≥2*4T，硬盘扩展槽≥2 个，默认支持 RAID1；<br>2、性能：系统吞吐量≥4Gbps；<br>3、功能：（1）支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache 数据库审计；（2）支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为进行审计；（3）支持审计 HTTP 和 HTTPS 协议的 URL、访问模式、cookie、页面内容、Post 内容；（4）可审计记录 FTP、邮件、HTTP、HTTPS、SCP、SFTP 等方式传输的文件（包括文本、Word、Excel 等格式），并且可对审计到的文件进行查询和下载。 | 1 | 台 | |

| | | | | | |
|---|---|---|---|---|---|
| | | 4、服务：包含不少于 60 个被审计数据库服务数的授权，不低于三年原厂质保服务。 | | | |
| 4 | 网络准入控制系统 | 1、配置：冗余电源；10/100/1000M 自适应电口≥6 个，千兆 SFP 接口≥4 个、千兆多模光模块≥4 个，网络接口扩展槽位≥2 个；<br>2、性能：整机最大吞吐量≥28Gbps，最大支持管理≥5000 个终端设备；<br>3、功能：（1）支持多种准入控制技术（802.1X、EVG、DHCP、ARP、SNMP、端口镜像、策略路由、透明网桥），并且支持至少四种以上准入技术的复用；（2）支持系统内置账号认证、Radius 认证、AD 域账号认证、LDAP 账号认证、证书认证、短信认证、OAuth 认证、动态令牌认证等多种身份认证方式，并且支持多种认证方式组合使用；（3）支持终端入网的安全基线检查功能，包含 SP 补丁检查、系统补丁检查、系统时间检查、计算机名规范检查、防病毒软 | 1 | 台 | |

| | | | | | |
|---|---|---|---|---|---|
| | | 件检查（支持软件版本检查）、IP/MAC 绑定检查、Windows 防火墙检查、操作系统版本检查；（4）支持实时监测哑终端指纹信息的变化，当哑终端指纹信息变化时，可及时对其进行告警或阻断。<br>4、服务：提供不少于 200 个终端设备的准入控制授权，不低于三年原厂质保服务。 | | | |
| 5 | 升级运维审计系统（堡垒机）双因子认证模块 | 现有设备型号：网御星云 LA-OS-36ZO-M-GA<br>主要参数：100 个主机授权；硬盘容量 2TB,配置 10 个双因素认证专用动态口令卡；字符协议：1000 个；图形协议：300 个。<br>本项目增加双因子认证模块。（1）支持内置 USB-KEY 认证、动态口令认证、国密动态口令认证、手机令牌认证;(2)可集成其它外部认证协议:WindowsAD、RADIUS、LDAP、短信、北京 CA、吉大正元等第三方认证。 | 1 | 项 | 现有设备 |

| | | | | | |
|---|---|---|---|---|---|
| 6 | 升级下一代防火墙特征库和防病毒疫苗 | 现有设备型号：网御星云 Power V 6000-NF22A0-DZGA<br>主要参数：产品配置入侵防御和防病毒模块，配置特征库和防病毒疫苗；最大整机吞吐量：3Gbps，每秒新建连接数：1.2 万，最大并发连接数：200 万；一年内提供无限次数升级。 | 1 | 项 | 现有设备 |
| 7 | 升级防病毒系统病毒库 | 现有设备型号：瑞星企业终端安全管理系统软件<br>主要参数：产品提供 1 个管理平台，包含 1 个管理中心、1 个数据中心、1 个业务中心、1 个安装部署升级中心、1 个漏洞补丁分发中心。提供 500 个 windows 系统端防病毒授权，内置防病毒模块和漏洞扫描补丁分发模块，10 个 for linux 服务器端杀毒软件授权，提供防病毒模块；一年内提供无限次数升级。 | 1 | 项 | 现有设备 |
| 8 | 升级入侵检测系统特征库 | 现有设备型号：网御星云 TD3000-GS35A0-GA<br>主要参数：吞吐量：1.8G；最大并发 TCP 会话数：150 万；每秒新建连接数：6 万；配备特征库，对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解、拒绝服务、缓冲区溢出、欺骗劫持、僵尸网络、Xpath、网页木马、钓鱼网站、Webshell、数据库攻击、网络设备攻击、0day 攻击、可疑行为等常见攻击具有高精度的检测能力；全面兼容 CVE、BugTraq 等国际标准漏洞库；一年内提供无限次数升级。 | 1 | 项 | 现有设备 |

| | | | | | |
|---|---|---|---|---|---|
| 9 | 日常维护终端管理平台 | 现有设备型号：网御星云 ISM -DISC<br>主要参数：当安全基线策略不满足要求时，可以通过准入控制或主机防火墙控制功能限制用户网络访问，并给出修复提示；终端可设置上网黑白名单，即只能访问的网站和禁止访问的网站，也可控制终端通过 http 代理上网，规范上网行为；对终端移动存储设备进行加密管理，做到 U 盘专网专用，防止涉密信息泄漏；终端授权：300 个； | 1 | 项 | 现有设备 |
| 10 | 日常维护日志审计系统 | 现有设备型号：网御星云 Leadsec-RS-5ZO-GA<br>主要参数：存储容量 2TB；日志处理性能(平均)3000EPS；130 个日志源授权。 | 1 | 项 | 现有设备 |
| a1 | 应急指挥网-安全防护建设小计： | | | | |
| 1.2 应急指挥网-全省流量溯源及安全运营平台建设 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 1 | 流量溯源安全感知系统 | 1、配置：CPU：不低于 2 颗物理 CPU、单颗 10 核，内存 256G，DDR4，2 块 500GSSD 固态硬盘组成 RAID1，12*4TB 硬盘组成 RAID50,冗余双电源，2*GE 电口，4 个千兆光口，4*USB3.0 接口，2*USB2.0 接口，1*DB9 Console 接口，外置 1*VGA 接口；<br>2、功能：（1）内置分布式非关系型数据库和传统关系型数据库，提供弹性扩展能力和数据高可靠冗余存储。提供资产分析与管理、安全事件管理、关联分析、标准脆弱性管理（内置漏扫调度和配置核查调度功能）、风险评估、情报管理、首页、标准的报表模块、标准的响应管理模块、基础态势大屏呈现页面（资产态势、脆弱性态势、攻击态势）、权限管理、知识管理、系统自身管理；（2）系统能够自动进行网络拓扑发现，自动描绘网络中资产节点之间网络连接关系。配置 1 个本地日志采集器，配置 1000 管理节点授权；<br>3、服务：提供 3 年硬件维保及同代软件版本升级服务。确保 180 天以上存储数据。 | 1 | 套 | |

| | | | | | |
|---|---|---|---|---|---|
| 2 | 流量溯源探针 | 1、配置：冗余电源；千兆电口≥6 个（含 1 个带外管理口）、SFP 插槽≥2 个，千兆多模光模块≥2 个、2 个万兆 SFP+插槽、2 个接口扩展槽位、1 个 RJ45 Console 口、2 个 USB 口；CF 卡≥2G，内存≥16G，硬盘≥2T；<br>2、性能：实际网络环境处理能力≥1Gbps，每秒新建连接数≥2 万，最大并发连接数≥300 万；<br>3、功能：（1）全面的攻击检测能力，可检测常见的 Web 攻击、缓冲溢出攻击、安全漏洞攻击、安全扫描攻击、拒绝服务攻击、木马后门攻击、蠕虫病毒攻击、穷举探测攻击、CGI 攻击等；（2）具备 HTTP 协议攻击行为告警特征信息双向提取能力，提取内容包括攻击请求特征和完整的响应信息；（3）系统需具备全面的流量统计能力，可以支持实时统计当前网络中的总流量、Web 应用流量、数据库应用流量、邮件应用流量、P2P 应用流量，并按照流量趋势图的形式进行可视化展现；（4）系统需具备自动发现用户网络资产的能力，可自动上报网络中的存活资产，并支持获取内网资产的暴露面信息和资产指纹信息；<br>4、服务：提供三年专用规则引擎授权，三年原厂质保服务。 | 25 | 台 | |
| a2 | 应急指挥网-溯源平台建设小计： | | | | |
| A | 应急指挥网安全防护建设合计(a1+a2)： | | | | |

| 2.1 政务外网-总队安全防护建设 | | | | | |
|---|---|---|---|---|---|
| 1 | 防病毒墙 | 1、配置：冗余电源，千兆电口≥6 个，万兆≥2 个；<br>2、性能：三层吞吐量≥40Gbps、防病毒吞吐量≥3.5Gbps；应用层吞吐量≥12G，最大并发连接数≥400 万、每秒新建连接数≥26 万；<br>3、功能：提供 L2-L7 层各类威胁的检测和防护。<br>4、服务：三年原厂质保服务。 | 1 | 套 | |
| 2 | 网络准入控制系统 | 1、配置：冗余电源，6 个 1000MBASE-T 接口，1 个接口卡；<br>2、性能：每秒事务数（TPS)≥5000（次/秒）；最大吞吐量≥2Gbps，最大并发连接数≥4000（条）；<br>3、功能：支持在 IPv4 和 IPv6 双栈环境下的终端准入控制、重定向、认证、安检、修复等。<br>4、服务：提供不少于 200 个终端设备的准入控制授权，不低于三年原厂质保服务。 | 1 | 套 | |

| | | | | | |
|---|---|---|---|---|---|
| 3 | 升级入侵检测系统特征库 | 现有设备型号：网御星云 TD3000-GS35A0-GA<br>主要参数：吞吐量：1.8G；最大并发 TCP 会话数：150 万；每秒新建连接数：6 万；配备特征库，对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解、拒绝服务、缓冲区溢出、欺骗劫持、僵尸网络、Xpath、网页木马、钓鱼网站、Webshell、数据库攻击、网络设备攻击、0day 攻击、可疑行为等常见攻击具有高精度的检测能力；全面兼容 CVE、BugTraq 等国际标准漏洞库；一年内提供无限次数升级。 | 1 | 项 | 现有设备 |
| 4 | 升级运维审计系统（堡垒机）双因子认证模块 | 现有设备型号：网御星云 LA-OS-36Z0-M-GA<br>主要参数：100 个主机授权；硬盘容量 2TB,配置 10 个双因素认证专用动态口令卡；字符协议：1000 个；图形协议：300 个。<br>本项目增加双因子认证模块。（1）支持内置 USB-KEY 认证、动态口令认证、国密动态口令认证、手机令牌认证;(2)可集成其它外部认证协议:WindowsAD、RADIUS、LDAP、短信、北京 CA、吉大正元等第三方认证。 | 1 | 项 | 现有设备 |
| 5 | 升级防毒墙病毒库 | 现有设备型号：瑞星防毒墙 RSW-3800LS<br>主要参数：最大吞吐：7Gbps；HTTP 杀毒吞吐：≥750Mbps；FTP 杀毒吞吐：≥650Mbps；SMTP 杀毒吞吐：≥600Mbps；POP3 杀毒吞吐：≥600Mbps；最大 | 1 | 项 | 现有设备 |

| | | | | | |
|---|---|---|---|---|---|
| | | 并发数：2,000,000；新增并发数：42,000。一年内提供无限次数升级。 | | | |
| 6 | 升级漏洞扫描系统 | 现有设备型号：网神 SecVSS3600 漏洞扫描系统 S1500-U010P<br>主要参数：百兆，并行扫描能力≥40 台，256 个地址授权，可同时建立 5 个任务，含 WEB 应用扫描模块。一年内提供无限次数升级。 | 1 | 项 | 现有设备 |
| 7 | 日常维护日志审计系统 | 现有设备型号：网御星云 Leadsec-RS-5ZO-GA<br>主要参数：存储容量 2TB；日志处理性能(平均) 3000EPS；130 个日志源授权。 | 1 | 项 | 现有设备 |
| 8 | 日常维护终端管理平台 | 现有型号：网御星云 ISM -DISC<br>主要设备参数：当安全基线策略不满足要求时，可以通过准入控制或主机防火墙控制功能限制用户网络访问，并给出修复提示；终端可设置上网黑白名单，即只能访问的网站和禁止访问的网站，也可控制终端通过 http 代理上网，规范上网行为；对终端移动存储设备进行加密管理，做到 U 盘专网专用，防止涉密信息泄漏；终端授权：300 个。 | 1 | 项 | 现有设备 |

| | | | | | |
|---|---|---|---|---|---|
| 9 | 日常维护数据库安全审计系统 | 现有设备型号：网神 SecFox 安全审计系统<br>主要参数：吞吐量≥1600Mbps；峰值处理能力（条/秒）≥9000；端口数：4*10/100/1000 自适应电口。 | 1 | 项 | 现有设备 |
| b1 | 政务外网-安全防护建设小计： | | | | |
| **2.2 政务外网-全省流量溯源及安全运营平台建设** | | | | | |
| 1 | 流量溯源安全感知平台部署一体机 | 1、配置：数据存储容量单台≥72T,总容量≥216T，确保 180 天以上存储数据；内存单台设备≥256GB/台，总内存≥768GB；单台不低于 6 个千兆电口、2 个万兆光口，总接口数不低于 18 个千兆电口、6 个万兆光口；配备 SFP+万兆多模光模*12 块，速率≥10Gb/s，双 LC 接口；<br>2、性能：支持≥20Gbps 流量处理分析；<br>3、服务：提供三年的设备质保服务。 | 1 | 套 | |

| | | | | | |
|---|---|---|---|---|---|
| 2 | 流量溯源安全感知平台软件 | 1、性能：流量处理能力≥21Gbps，日志处理能力（EPS 每秒）≥36000。<br>2、功能：<br>（1）业务风险检出更精准：采集多源数据，结合机器学习、行为分析、关联分析等技术，有效发现高级威胁与异常行为；通过算法模型迭代、灰度运营优化、流量双向检测，大幅提升检出率，并降低误报率；（2）事件闭环更快速、更高效：具备全网资产可视化盘点，并对资产进行漏洞扫描，发现安全漏洞，并且攻击行为全过程溯源举证，看清威胁影响面，深度溯源攻击入口点，从根源分析安全风险。提供 SOAR 可编排的自动化响应策略，真正实现无人值守主动防御提供网络安全管理、实时攻击分析、溯源追踪、报告等功能；（3）支持 15 级自定义支队管理权限，支队管理员具备独立的管理页面，只能管理和查看所属支队的业务和终端资产的安全信息且具备完整的功能展示；（4）可视区域基于数据中心、总队、支队等按照风险等级（优秀、良、中、差）来展示数据中心的情况。支持对数据中心正常反问的趋势和攻击者监视和分析威胁的说明；（5）支持不同安全视角展示 16 个独立的大屏展示功能，包括但不限于全网安全态势感知大屏、支队安全态势大屏、安全事件态势大屏、安全重保态势大屏、资产态势大屏等<br>3、服务：提供三年的设备软件升级授权服务，包含特征库升级。 | 1 | 套 | |

| | | | | | |
|---|---|---|---|---|---|
| 3 | 总队流量溯源探针 | 1、配置：内存≥8G，硬盘容量≥256G；千兆电口≥6 个，2 千兆光口 SFP≥2 个；<br>2、性能：网络层吞吐量≥1.5Gbps；<br>3、功能：（1）、具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息功能；（2）具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；（3）、支持 SQL 注入、XSS 攻击等网站攻击检测;（4）支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤；（5）支持 Database 漏洞攻击等服务漏洞攻击检测。支持 Application 漏洞攻击等客户端漏洞攻击检测。支持 FTP、IMAP、MS Sql 等协议暴力破解检测；（6）支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，支持 ICMP、UDP、SYN 等协议外发异常流量检测。（8）支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名等僵尸网络行为检测。（9）支持 5 种类型日志传输模式，适应不同应用场景需求。支持传输协议（10）内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。（11 支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。 | 1 | 套 | |

| | | | | | |
|---|---|---|---|---|---|
| | | 4、服务：提供三年的设备软件特征库升级服务。 | | | |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 直属单位及珠三角地区支队流量溯源探针 | 1、配置：内存≥8G，硬盘容量≥64G；千兆电口≥6 个，2 千兆光口 SFP≥2 个；<br>2、性能：网络层吞吐量≥1Gbps；<br>3、功能： (1)、具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息功能；(2)具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；(3)、支持 SQL 注入、XSS 攻击等网站攻击检测;(4)支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤；(5)支持 Database 漏洞攻击等服务漏洞攻击检测。支持 Application 漏洞攻击等客户端漏洞攻击检测。支持 FTP、IMAP、MS Sql 等协议暴力破解检测；(6)支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，支持 ICMP、UDP、SYN 等协议外发异常流量检测。（8）支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名等僵尸网络行为检测。（9）支持 5 种类型日志传输模式，适应不同应用场景需求。支持传输协议（10）内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。（11 支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。 | 11 | 套 | |

| | | | | | |
|---|---|---|---|---|---|
| | | 4、服务：提供三年的设备软件特征库升级服务。 | | | |

| | | | | | |
|---|---|---|---|---|---|
| 5 | 支队流量溯源探针（非珠三角地区支队） | 1、配置：内存≥8G，硬盘容量≥64G；千兆电口≥6 个，2 千兆光口 SFP≥2 个；<br>2、性能：网络层吞吐量≥500Mbps；<br>3、功能：(1)、具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息功能；(2)具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；(3)、支持 SQL 注入、XSS 攻击等网站攻击检测;(4)支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤；(5)支持 Database 漏洞攻击等服务漏洞攻击检测。支持 Application 漏洞攻击等客户端漏洞攻击检测。支持 FTP、IMAP、MS Sql 等协议暴力破解检测；(6)支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，支持 ICMP、UDP、SYN 等协议外发异常流量检测。（8）支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名等僵尸网络行为检测。（9）支持 5 种类型日志传输模式，适应不同应用场景需求。支持传输协议（10）内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。（11 支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。 | 13 | 套 | |

| | | | | | |
|---|---|---|---|---|---|
| | | 4、服务：提供三年的设备软件特征库升级服务。 | | | |
| b2 | 全省流量溯源及安全运营平台建设合计: | | | | |
| **2.3 政务外网-网络管理系统建设** | | | | | |
| 1 | 网管平台软件 | 功能：Windows 中文版；Web 界面，永久授权。<br>拓扑、网络/设备/资源/链路管理、故障监控、性能监控、告警、日志、网管工具、监控扩展、图表、多用户。 | 1 | 套 | |

| | | | | | |
|---|---|---|---|---|---|
| 2 | 网管平台服务器 | 机架服务器；处理器配置不低于 2 颗 10Core/2.2GHz CPU；内存不低于 64GB；硬盘规格不低于 2*1200GB；支持 Raid，实配 Raid 卡+电容，不少于 4 个 GE 网口，配置双电源冗余； | 1 | 台 | |
| 3 | 网络设备许可 | 网络管理设备许可。 | 50 | 套 | |
| b3 | 政务外网-网络管理系统建设合计： | | | | |
| B | 政务外网安全防护建设合计（b1+b2+b3）： | | | | |
| **3 项目集成** | | | | | |
| C | 项目集成费用，包含系统联动及系统部署时现场所需要的线材、网络流量分流器等 | | 1 | 项 | |
| **4 第三方服务** | | | | | |
| 1 | 网络等级保护 2.0 三级 | 本次建设系统进行网络等级保护 2.0 三级评测（含建设方案差距评审） | 1 | 项 | |
| 2 | 商用密码应用安全性评估 | 取费参考《广州市政府投资信息化项目（建设类）方案编写规范》的设计咨询费进行计算。 | 1 | 项 | |

| | | | | | |
|---|---|---|---|---|---|
| 3 | 验收功能测评 | 取费参考《广州市政府投资信息化项目（建设类）方案编写规范》的设计咨询费进行计算。 | 1 | 项 | |
| 4 | 项目监理服务 | 取费参考《广州市政府投资信息化项目（建设类）方案编写规范》的设计咨询费进行计算。 | 1 | 项 | |
| D | 第三方服务小计: | | | | |
| **总计(A+B+C+D)：** | | | | | |