附件1：

达州市人民检察院检察工作网边界安全接入平台需求说明书

**目 录**

[第一章 项目概述 4](#_Toc4803)

[1.1 建设背景 4](#_Toc18325)

[1.2 建设目标 5](#_Toc23137)

[1.3 建设规模 6](#_Toc29093)

[1.4 建设内容 6](#_Toc21133)

[第二章 需求分析 7](#_Toc15020)

[2.1 现状分析 7](#_Toc9465)

[2.1.1 主机安全现状 7](#_Toc29828)

[2.1.2 网络安全现状 7](#_Toc14148)

[2.1.3 应用安全现状 7](#_Toc1229)

[2.2 业务需求 8](#_Toc7425)

[2.2.1 互联网接入需求 8](#_Toc19303)

[2.2.2 外部专网接入需求 8](#_Toc12001)

[2.3 应用需求 8](#_Toc32096)

[2.3.1 数据交换类 8](#_Toc6228)

[2.3.2 请求服务类 9](#_Toc8342)

[2.3.3 授权访问类 9](#_Toc30497)

[2.3.4 安全需求 9](#_Toc30072)

[第三章 系统建设内容 10](#_Toc17601)

[3.1 系统总体架构 10](#_Toc18286)

[3.2 总体建设内容 11](#_Toc16253)

[3.3 边界安全接入平台技术框架 12](#_Toc8700)

[3.4 网络安全技术建设方案 14](#_Toc31142)

[3.4.1 安全区域划分 14](#_Toc6053)

[3.4.2 接入设备技术要求 17](#_Toc10077)

[3.4.3 数据交换服务流程 18](#_Toc28936)

[3.4.4 接入平台性能要求 18](#_Toc18369)

[3.5 边界安全接入平台安全管理要求 19](#_Toc3542)

[3.5.1 建设管理要求 19](#_Toc27785)

[3.5.2 接入业务管理要求 19](#_Toc20113)

[3.5.3 运维管理 20](#_Toc15172)

[3.5.4 接入平台管理报表 20](#_Toc21817)

[3.6 系统配置及软硬件选型原则 20](#_Toc24032)

[3.7 网络安全系统软硬件配置清单 22](#_Toc7240)

# 项目概述

## 建设背景

随着检察机关科技强检战略深入实施，检察工作网作为检察机关的重要基础网络，已成为与其他党政机关、企事业等单位非涉密网络互联互通、数据共享和业务协同的重要支撑平台。但随着检察工作网覆盖范围、数据交换范围与用户群体的扩大，解决专网与专网之间、专网与互联网之间的边界链路安全问题，已成为加强检察机关与政法机关、行政执法部门资源共享，推动建设政法网络互联互通和信息资源共享平台的底板工程。

随着统一业务应用系统2.0在工作网的部署，今后检察机关业务主要在工作网进行开展，为进一步促进智慧检务的发展，需和外部非涉密网络之间进行数据和业务对接，工作网需和外部专网、互联网等进行互联互通。为此2018年7月13日，最高检下发了《智慧检务工程建设指导方案（2018-2020年）》（高检技〔2018〕59号），要求加快建设网络安全接入和交换平台。检察机关根据接入对象、接入链路、业务交换需求和应用场景，结合相关保密和安全要求，制定针对性的安全接入和交换方案，建设本级网络安全接入和交换平台。

2019年9月6日，最高检下发的《检察工作网边界安全接入平台建设管理规范》（高检技〔2019〕26号）要求，检察工作网需建设边界安全接入平台，明确了检察工作网边界安全接入平台的总体框架、技术要求和管理要求，为全国检察机关开展检察工作网边界安全接入平台建设和管理工作提供指导，保障检察机关与外部非涉密网络数据共享、业务协同安全稳定可靠运行，地市级院可以参照高检院管理规范和省院方案，做好本地边界安全接入平台建设，满足检察工作网与外部专网、互联网的数据交换和业务协同业务和移动办公等业务。

## 建设目标

本项目旨在落实最高人民检察院《最高人民检察院关于深化智慧检务建设的意见》、《关于加强新时代检察机关网络法治工作的意见》、《检察工作网安全保障系统建设指导意见》、《检察工作网边界安全接入平台建设管理规范》（高检技〔2019〕26号）要求及达州市人民检察院工作整体部署。以安全、可信、合规为目标，建设高效集约的检察工作网边界安全接入平台，具备完善的跨网交换安全能力，实现接入应用系统和设备的身份可信，保护数据安全共享，抵御网络恶意攻击满足机密性、完整性和可用性要求，确保跨网数据共享和业务协同的网络安全、主机安全、应用安全和数据安全。

## 建设规模

建设一条数据交换链路和一条视频交换链路连接外部专网（公安、法院等专网），建设一条数据交换链路连接互联网，建设一条视频交换链路连接移动专网，完善相应的网络安全和数据安全防护能力。

## 建设内容

建设3台接入交换机、2套数据安全交换系统、2套视频安全交换系统、1台网闸3台单向光闸、3台入侵检测、3台数据防泄漏、3台集控探针、1台集中监控系统、3台安全边界接入网关、3台接入防火墙。

# 需求分析

## 现状分析

### 主机安全现状

接入用户类型多，场所物理环境不安全、人员复杂、接入终端安全状态不可控，且接入后行为不可控，终端安全风险较大；其次，接入终端存在非法使用、非授权访问，甚至存在伪造终端接入，并有可能发展为木马、病毒的传播来源。

### 网络安全现状

接入链路复杂、缺乏针对数据传输机密性、完整性的保障机制，存在敏感数据被篡改外泄的风险，以及存在非法数据、病毒数据通过接入链路进入内部网络的风险。

### 应用安全现状

接入用户存在对应用的越权访问，信息泄密的风险；其次，与外部对象连接后应用系统暴露面扩大，安全风险增加，极易遭受黑客攻击、木马入侵、病毒传播、信息篡改和数据窃取等不同程度的安全威胁。

## 业务需求

### 互联网接入需求

互联网与检察工作网之间存在数据交换和业务协同需求，由于互联网安全级别低，互联网服务又需要与检察工作网进行信息交互，需要以服务请求方式实现互联网与互联网间的安全信息共享，边界安全接入平台需满足和互联网安全对接需求。

### 外部专网接入需求

外部专网包括政法专网、其它政府部门网络以及企事业单位的业务网络，由于检察业务存在和外部单位的数据交换和业务对接，因此检察工作网和外部网络之间存在数据共享交换和业务协同需求，边界安全接入平台需满足和外部专网安全互通需求。

## 应用需求

通过业务需求分析可知，边界接入业务在应用上主要有三大类：数据交换、请求服务和授权访问。

### 数据交换类

将数据交换类应用一方面要要实现将相关信息通过安全的接入方式采集到接入平台，另一方面要将采集到数据安全、稳定、可靠地交换到目标区域，以支撑内外网业务的开展。需实现如下功能：需支持各类B/S 应用的数据采集；需支持各类C/S 应用的数据采集；数据库同步、交换（包括异构数据库同步、交换）；文件数据交换。

### 请求服务类

特指外部的业务应用系统与内网业务系统之间，可以通过跨网络请求服务方式实现对接，必须采用标准消息格式和传输协议封装数据服务，实现数据查询服务、核查服务、批量对比服务、数据交换服务。

### 授权访问类

授权访问功能主要是指对于授权访问类终端通过安全接入链路访问内网资源时，对于不同的接入终端可实现基于资源、数字证书、IP 地址等多种类型访问权限的控制，保证内网资源不被越权访问，进而保护检察工作网业务的安全。

### 安全需求

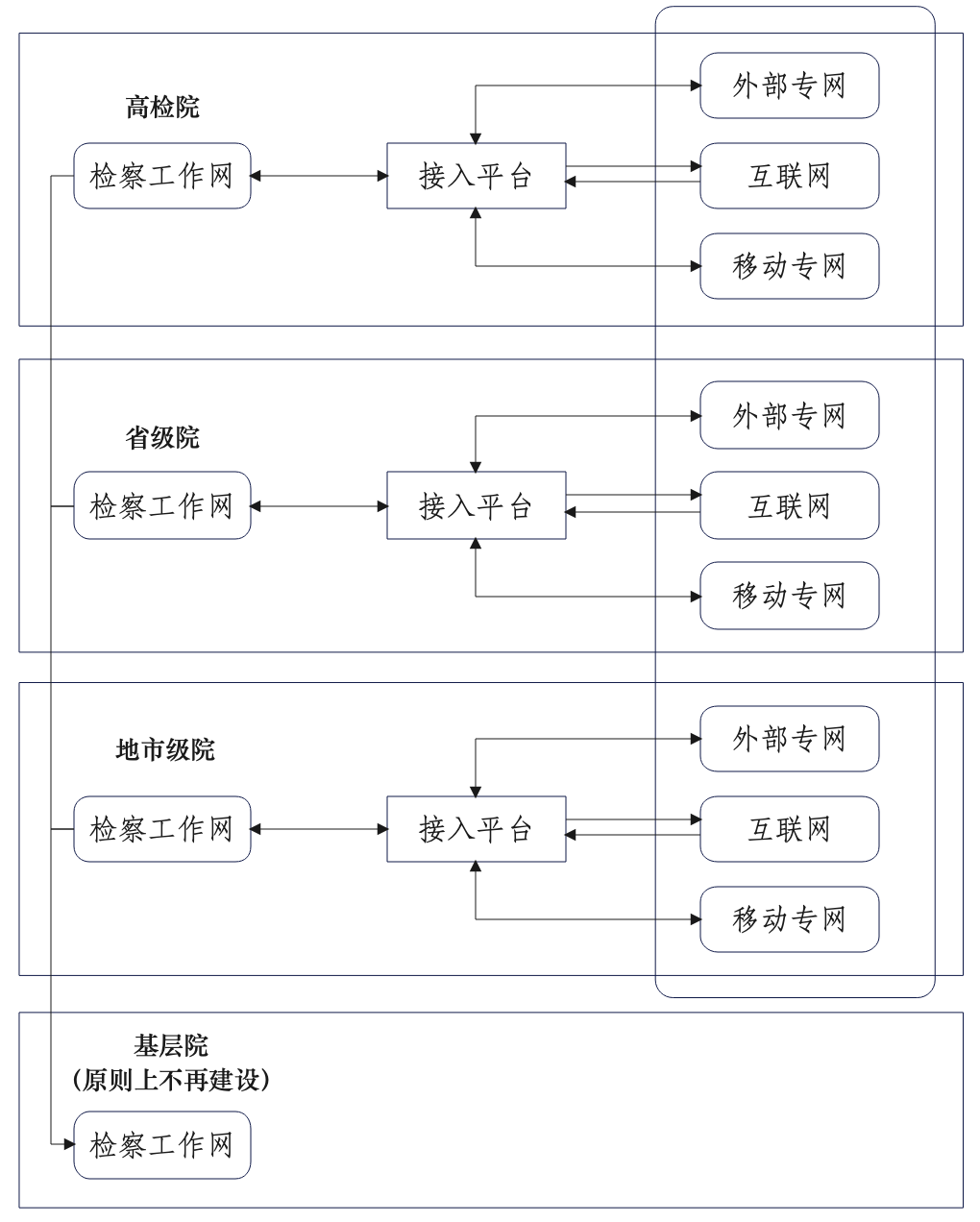
边界安全接入平台作为检察工作网边界接入统一的出入口，是检察工作网与外界各类接入业务的交通要道。在安全上存在各类风险，涉及接入终端、接入用户、外部/内部链路、网络层、信息传输、应用安全及平台主机等。

# 系统建设内容

## 系统总体架构

边界安全接入平台是检察工作网与外部网络进行数据交换的统一通道，通过该平台实现检察工作网与外部专网、互联网、移动专网等外部网络之间的数据安全交换。

边界安全接入平台在地市级检察院进行建设，基层检察院不再建设。各级接入平台负责本级管理范围内的所有边界接入业务。



## 总体建设内容

检察工作网边界安全接入平台是检察工作网与外部网络进行数据交换的统一通道，通过该平台实现检察工作网与外部专网、互联网等外部网络之间的数据安全交换。项目中，接入平台可划分为边界保护区、安全监测区、安全隔离区。对不同网络安全域提出如下技术要求：

**（1）边界保护区**

采部署国产化防火墙负责实现检察工作网边界安全接入平台安全防护区的访问控制策略,设置访问控制规则，保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信，对关键节点实现恶意代码进行检测和清除。

**（2）安全监测区**

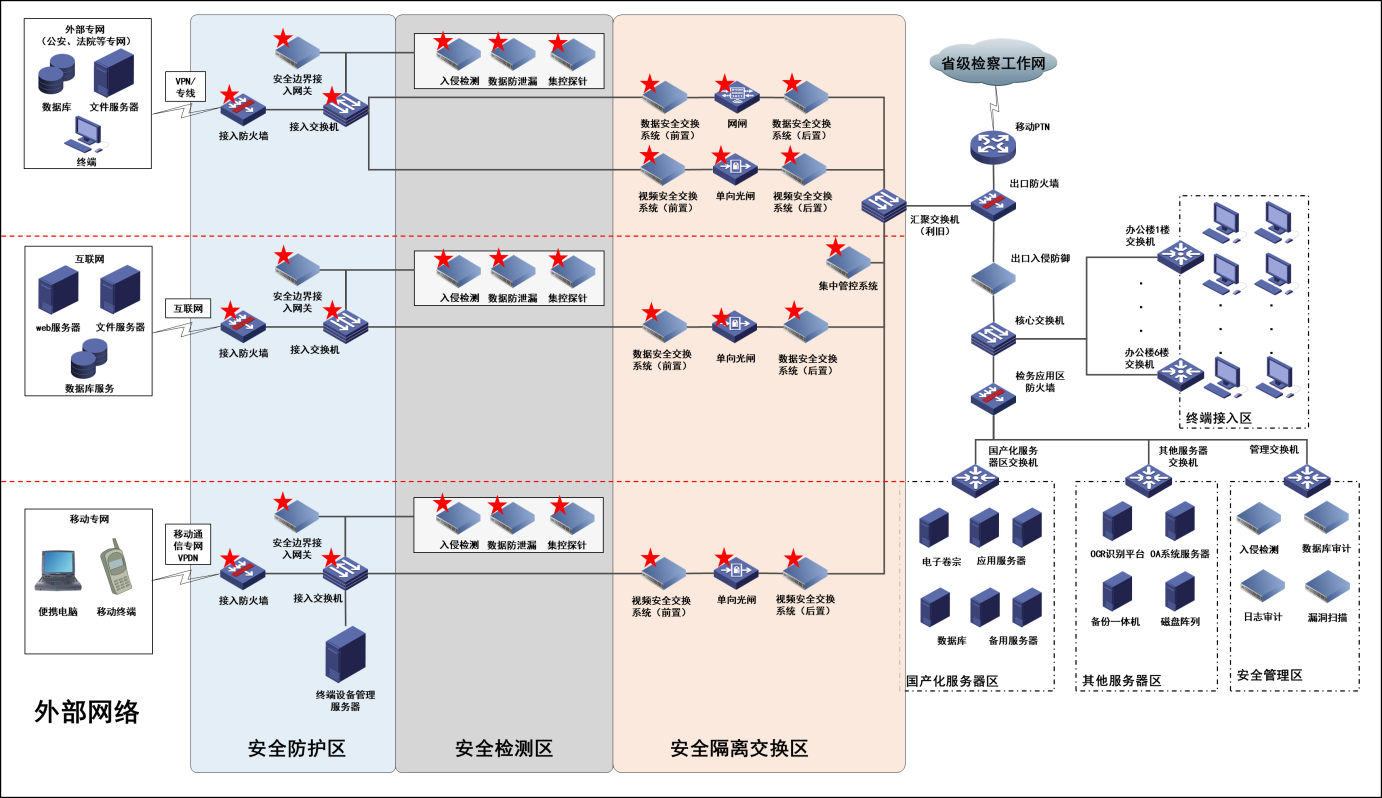
部署网络准入系统、日志审计和网络数据防泄漏设备。作为数据中心的集中安全监测区域，提供日志审计、网络数据防泄漏、恶意代码防范等安全服务，并实现工作网的安全管理。

**（3）安全隔离区**

安全隔离交换区域部署单向光闸、双向网闸、数据交换平台，用于外部专网与工作网间实现安全隔离，保证可靠、安全的的信息交换，提供安全浏览、数据库访问、文件交换、数据库同步、视频应用等多种服务。

## 边界安全接入平台技术框架

边界安全接入平台拓扑图如下所示：



边界安全接入平台拓扑图

1、边界安全接入平台是《检察工作网安全保障系统建设指导意见》(高检技[2018]62号)中跨网交换区的具体建设要求，应统一使用检察工作网安全保障系统中的网络信任基础设施区和安全管理区进行数字证书签发、安全管理等工作。

2、边界安全接入平台中的外部专网、互联网、移动专网接入可统一建设或者在统一规划的基础上按需分步建设。

3、市级院建设接入平台按上图进行建设。

## 网络安全技术建设方案

### 安全区域划分

接入平台可划分为安全管理区、安全防护区、安全检测区、安全隔离交换区。其中：

1、安全管理区：实现对接入平台的统一集中监控与审计。

2、安全防护区：实现接入平台与外部网络的网络隔离与防护。

3、安全检测区：实现对接入平台的综合安全检测和日志采集。

4、安全隔离交换区：实现外部网络对文件、数据库、音视频等数据的交换服务。

#### 安全管理区

该区域实现检察工作网中管理用户对接入平台进行运行状态监控、业务配置管理与集中日志审计。

1、运行监控

实时监控接入平台的运行状况，实现对安全事件信息的查询和统计、预警，及时生成报表。

2、业务配置管理

对接入平台内各个安全设备的配置信息进行集中管控。

3、安全审计

实现对网络、用户、业务应用系统、设备等的集中安全审计功能，以及对异常事件的追踪回溯。

#### 安全防护区

该区域实现对接入平台的边界保护。

该区域主要安全功能为：对接入设备实行准入控制;实现网络层安全访问控制、网络入侵防护、网络恶意代码防护、数据加密等。

#### 安全检测区

该区域采用物理机或虚拟化以旁路部署方式，实现对接入平台的日志采集与网络安全检测。

该区域主要安全功能为：基于网络流量，识别、发现网络中已知和未知威胁，防止数据泄露，发生数据泄露事件时，可以定位数据泄露的源头;采集接入平台中的所有设备日志信息，统一发送至安全管理区。

#### 安全隔离交换区

该区域实现外部网络对文件、数据库、音视频等数据的交换服务。该区域采用物理机或虚拟化部署两种方式，可以通过负载均衡和集群扩展的形式，确保服务的高可用性。

主要部署以下安全措施：

1、数据交换服务：部署数据交换服务系统，包括前置和后置服务，满足数据库、文件、音视频等资源交换。具体功能要求如下:

（1）API接口：支持API接口形式对外提供安全数据交换服务；

（2）文件交换：支持NFS、SMB、FTP 等多种文件传输协议，实现文件的安全交换；

（3）视频交换：支持符合国家标准的实时音视频协议传输；

（4）数据库同步：支持主流数据库的同步，支持异构数据库同步；

（5）执行预定义的访问控制策略；支持对传输数据类型检查及过滤；支持对数据内容进行识别和过滤；支持执行预定义的黑白名单策略；支持对交换的数据进行一致性和完整性校验；

（6）流量管控：应支持对应用请求信息进行流量控制，支持基于请求内容大小、请求速度、请求连接数和访问时段等参数进行流量控制。

2、安全隔离交换系统：部署安全隔离交换系统，阻断外部网络与检察工作网之间的所有直接网络连接，对网络协议进行剥离或转化，保证网络安全隔离与数据安全交换。支持不同网络之间的安全隔离；支持对网络流量的隔离和过滤防护，支持不同网络之间的单向及双向数据传输。

### 接入设备技术要求

接入设备包括外部专网接入设备、互联网接入设备和移动专网接入设备。

1、外部专网接入设备、互联网接入设备应通过 802.1x、设备证书、IP/MAC 绑定等技术实行准入控制；移动专网接入设备应采用数字证书、生物特征等双因子或多因子认证模式。

2、应实现接入设备与接入平台通信内容的机密性与完整性保护。

3、接入设备上安装的接入业务应用程序应完善自身的安全性和健壮性。

4、接入设备安全环境应满足网络安全等级保护三级要求。

5、移动专网接入设备应从终端应用、终端数据等方面进行安全增强，安装安全软件，支持国家商用密码加解密，并接受后台管控。

6、外部专网接入设备、移动专网接入设备不得与互联网应用在同一操作系统下混用，移动专网接入设备可探索采用单机双操作系统等方式实现与互联网应用在操作系统及以上级别的隔离。

### 数据交换服务流程

数据交换业务在经过安全防护区的安全防护措施之后，完成设备准入控制，并通过数据交换服务的前后置系统、安全隔离与交换系统与检察工作网完成数据交换。

数据交换时应采用细粒度、最小化授权原则进行访问控制，非授权的访问应被阻断。

### 接入平台性能要求

接入平台的性能应与数据交换的需求相匹配，满足业务应用的需要，并根据业务应用的发展变化对接入平台实施升级改造。

## 边界安全接入平台安全管理要求

### 建设管理要求

#### 审批备案要求

省级院、地市级院的接入平台建设方案应报高检院备案。地市级院接入平台建设方案应报省级院审批。

审批或备案时，建设接入平台的单位应填报《接入平台建设审批/备案表》，同时提交接入平台的技术方案和实施方案等材料。

接入平台发生重大变化时，应重新进行审批或备案

#### 安全性测评要求

接入平台应按照网络安全等级保护三级的要求进行建设。

建成后的接入平台应通过网络安全等级保护测评，由第三方测评机构出具正式测评报告。

接入平台可以单独测评，也可以在对检察工作网开展网络安全等级保护测评时将其一并纳入。

### 接入业务管理要求

经接入业务的主管部门审批后，由本级院信息化主管部门负责核实接入业务信息，制定技术方案实施接入并纳入日常运行监控管理。

接入业务通过审批后，本级院信息化主管部门应填报《接入业务信息备案表》，层报上级院信息化主管部门备案。

接入业务投入运行后，其业务内容应与备案信息一致。接入业务内容、方式、范围等发生变化时，应重新备案。

### 运维管理

本级院信息化主管部门负责本级接入平台的日常运行维护安全监测、应急响应等工作，纳入检察工作网安全保障系统统-运维，接入平台设备不得交与其他单位托管。

应建立安全事件紧急响应和处置工作机制，发生重大安全事件时应第一时间逐级上报，处置完成后应将处置情况逐级书面上报。可不定期请第三方机构进行渗透性测试，验证接入平台的安全性。

### 接入平台管理报表

本节对需要审批和备案的信息内容进行规范，包括《接入平台建设审批/备案表》和《接入业务信息备案表》。

## 选型原则

国产化：本项目设备均采用国产设备。

标准性：系统设计开发遵循国家标准、信息产业部有关软件行业的通用规范、通用的国际规范及各子系统间接口标准，保证各个模块之间可以无缝集成，并对外提供标准接口。

可扩展性：安全态势感知系统不仅要满足目前的要求，也要适应未来业务发展对提出的要求。平台设计要采用开放的技术，适应不断变化的数据采集范围和数据提供方式。

稳定性：系统设计充分考虑到可能部署的软硬件平台、用户可能使用的各类终端、各种可能的用户操作，使用面向对象语言丰富的异常处理机制，保证系统实现7×24小时稳定运行。

易维护性：系统采用先进的B/S的开发和应用模式，客户机无需安装任何客户程序，用户对系统的维护仅在服务器上进行，大大降低了维护工作量。支撑平台要提供简单易用的图形管理界面，方便管理人员对平台进行日常配置、维护和管理。

安全性：从系统安全、信息存储安全、信息传输安全、认证和授权的安全等多个方面考虑整体的安全性，构筑全面的安全体系，避免任何安全薄弱环节影响系统的全局安全性。平台要结合现有的安全信任体系，对数据传输、管理、发布、使用等不同环节，设计由外到内、由局部到全面、多层次的、纵深的、有效地部署和配置全面安全解决方案，以达到最佳的安全互补状态，保证系统受到可靠、安全的保护。

## 建设清单

在规划、建设、使用、维护整个信息系统的过程中，本方案将主要遵循统一规划、分步实施、立足现状、节省投资、科学规范、严格管理的原则进行安全体系的整体设计和实施，并充分考虑到先进性、现实性、持续性和可扩展性，符合等级保护要求，具体体现为：

1) 可控性：

采取相应的控制措施，保证检察工作网的边界可控，与其它网络、终端等链接和数据交换安全可控。

2) 可管理性

具有规范合理的检察工作网接入流程，针对检察工作网的用户、设备，具有相应的管理措施。

3) 可用性

应能满足市人民检察院的实际业务需求，技术方案具有可行性，安全管理措施具有可操作性。

4) 安全性

应保证接入和数据交换的安全，对终端、网络具备相应的保证与防攻击措施，确保信息不被非法获取。

5) 规范性

本次方案涉及的内容，应符合国家法律法规，以及相关政策，标准的规定。

具体如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备及软件名称** | **数量** | **单位** | **备注** |
| 1 | 接入交换机 | 3 | 台 |  |
| 2 | 数据安全交换系统 | 2 | 套 |  |
| 3 | 视频安全交换系统 | 2 | 套 |  |
| 4 | 网闸 | 1 | 台 |  |
| 5 | 单向光闸 | 3 | 台 |  |
| 6 | 入侵检测 | 3 | 台 |  |
| 7 | 数据防泄漏 | 3 | 台 |  |
| 8 | 集控探针 | 3 | 台 |  |
| 9 | 集中监控系统 | 1 | 台 |  |
| 10 | 安全边界接入网关 | 3 | 台 |  |
| 11 | 接入防火墙 | 3 | 台 |  |

# 硬件及相关设备

## 接入交换机（3台）

交换容量≥336Gbps/3.36Tbps，≥24个千兆电口，≥4个万兆光口，3年产品质保服务。

## 数据安全交换系统（2套）

1、包含前置及后置设备，前置：2U标准机架式硬件设备，吞吐量≥5Gbps，配备RJ45串口≥1个、USB口≥4个、千兆电口≥6个，双电源；后置：2U标准机架式硬件设备，吞吐量≥5Gbps，配备RJ45串口≥1个、USB口≥4个、千兆电口≥6个，双电源。

2、支持与单向光闸隔离设备采用API私密通讯，杜绝其他通用协议，如UDP直接传输数据。

3、文件同步类型支持本地FTP、本地SMB、本地NFS、本地SFTP、远程FTP等方式。

4、支持windows、Linux专用客户端方式的文件同步、支持文件特征、文件内容、文件名等各种过滤方式，支持图片内容过滤。

5、支持同步限速、同步间隔、配置任务优先级、监控目录清理。

6、默认支持Txt、AVI、Bak、Bat、BMP、BWF、Dll、Doc、Docx、Excel、Exe、MP3、PDF、PPT、PPTX、XML、Zip、WMA、Wps等文件特征过滤、具备文件特征智能识别功能，能针对新的特征文件进行系统自动学习和识别。

7、具备文件名和文件内容过滤，具备文件大小、文件病毒过滤。

8、支持各种数据库之间的异构同步，包括：不同数据库、一对多同步、多对一同步、自增字段同步、无主键表同步、异构同步、异构字段/表名同步、异构字段类型同步、大字段同步、大字段异构同步、条件过滤同步、异常恢复同步。

9、支持 BLOB、 CLOB、TEXT、IMAGE 等大字段的异构。

10、具备私有协议传输接口，支持 Webservice 接口混合数据传输支持 Webservice/form-data 协议 支持 Webservice 同步异步模式，支持短信息、结构化数据、非结构化数据、自定义数据及以上数据类型的混合数据同步交换。

11、支持唯一Token认证，只有经过认证的应用才能进行数据安全交互。

12、具备满足“GA/T 1788.3-2021 公安视频图像信息系统安全技术要求 第3部分:交互安全”标准的软件测试报告。

13、提供3年升级授权，远程支持服务，产品保修服务，硬件故障上门支持。

## 视频安全交换系统（2套）

1、包含前置及后置设备，前置：2U标准机架式硬件设备，吞吐量≥5Gbps，配备RJ45串口≥1个、USB口≥4个、千兆电口≥6个，双电源；后置：2U标准机架式硬件设备，吞吐量≥5Gbps，配备RJ45串口≥1个、USB口≥4个、千兆电口≥6个，双电源。

2、支持与单向光闸隔离设备采用API私密通讯，杜绝其他通用协议，如UDP直接传输数据。

3、支持海康、高新兴、海信、金鹏、贝尔、华三、科达、大华、佳都新泰、烽火等主流视频厂商协议深度解析。

4、支持解析视频交换过程的控制信令类型、格式和内容，对控制信令进行格式检查和内容过滤，仅允许符合格式要求的控制信令通过，对不符合格式的控制信令进行阻断和报警。

5、信令内容过滤应支持对SIP请求方法、源IP、视频编码等进行黑、白名单过滤。

6、支持基于SIP服务器域、SIP服务器ID等注册信息进行过滤。

7、支持视频插帧动作，可设置插帧频率。

8、支持DB33标准、GB28181标准、GB35114标准，支持RTSP协议。

9、支持视频信令，穿透正反两台光闸完成视频信令的交互，实现视频流的单向传输。

10、支持视频监控协议的负载和集群管理。

11、具备满足“GA/T 1788.3-2021 公安视频图像信息系统安全技术要求 第3部分:交互安全”标准的软件测试报告。

12、具备满足“GB 35114-2017 公共安全视频监控联网信息安全技术要求”标准的软件测试报告。

13、提供3年升级授权，远程支持服务，产品保修服务，硬件故障上门支持。

## 网闸（1台）

1、2U标准机架式硬件设备，冗余电源，内网：SATA硬盘≥4T，USB口≥2个，电管理口≥2个、千兆电口≥4个、千兆光口≥4个、接口扩展槽≥3个；外网：SATA硬盘≥4T，USB口≥2个，电管理口≥2个、千兆电口≥4个、千兆光口≥4个、接口扩展槽≥3个；吞吐量≥5.5Gbps，并发连接数≥210万。

2、设备支持代理及路由两种工作模式，管理员可依据实际网络状况进行相应的部署。

3、支持文件同步功能，支持覆盖、跳过、重命名同步策略，支持全量或者增量同步方式，支持对文件服务器IP对象、端口号、用户名、密码、路径、字符集等进行配置。

4、支持数据库同步功能，支持Oracle、SQLServer、Mysql、Sybase、DB2、Postgresql等多种主流国外数据库的同步和国产达梦数据库、人大金仓数据库的同步支持同构、异构数据库之间的同步，如Mysql同步至Oracle。

5、支持入侵检测功能，内置检测模板，同时可自定义模板、自定义规则，可通过授权扩展该模块。

6、支持可视化呈现，可统计网页业务、文件服务、通用服务、文件同步、数据库同步等业务数量，统计最近一天数据库同步、文件同步任务，圆环图展示内容审计信息，包括网页、邮件、文件、数据库、远程访问等内容。

7、支持对协议命令进行过滤（比如对网页浏览\_HTTP类型的OPTION、TRACE、GET、HEAD、DELETE、PUT、POST等命令字）；主要包括类型有网页浏览、邮件访问、文件访问、数据库访问、远程访问等。

8、支持威胁情报检测功能，内置IP、URL、域名、样本等情报库，可通过授权扩展该模块。

9、支持统一集中管理，实现实时监控管控设备状态，包括设备在线离线状态、设备名称、设备类型、设备IP地址、CPU使用率、内存使用率、CF卡/磁盘剩余空间、版本信息、流量信息等。

10、采取系统策略配置系统管理员、审计管理员和安全管理员三种角色分立的权限分配模式，用户只能维护操作本类基础管理角色的功能与操作，权限各不交叉。

11、支持报表任务功能,支持基于业务类型、文件名称、文件类型（html、pdf、word等）、时间（日报、周报、月报等）等进行新建报表任务。

12、支持报表配置自定义，报表封面LOGO、HTML报表封面LOGO、报表页眉LOGO等信息，便于项目统一管理。

13、支持web用户使用USBKEY认证。

14、产品提供3年产品系统升级授权、产品保修服务、远程支持服务。

## 单向光闸（3台）

1、2U标准机架式硬件设备，采用 “2+1”系统架构，内、外网处理单元+专用光隔离部件，物理上无任何反馈信号，保证软、硬件物理单向，内网：千兆电口≥6个，千兆光口≥4个，USB口≥2个，RJ45串口≥1个，RS232接口≥1个,RS485接口≥4个；外网：千兆电口≥6个，千兆光口≥4个，USB口≥2个，RJ45串口≥1个，RS232接口≥1个,RS485接口≥4个；带液晶显示屏。

2、吞吐量≥1300Mbps，并发连接数≥4万，系统延时≤0.5ms，文件传输≥100MB/s，数据库同步能力≥3000条/s，同时运行的任务数≥50。

3、支持统,主要包括文件同步、数据库同步、数据单向传输、邮件中继、防病毒功能，支持工业数据采集、转发、上报等功能。

4、支持主流数据库Oracle、SQL Server 、Sybase、 MYSQL、以及国产数据库(武汉达梦、人大金仓KINGBASE、神舟通用OSCAR、南大通用GBASE)的同步 ，且对数据库所在操作系统无要求。

5、支持SMB、FTP、SFTP、NFS等传输协议，支持用户端同步工具配合光闸使用，持LINUX、WINDOWS、UNIX等多种系统平台。

6、支持数据库的字段级同步，可以自由选择需要交换的数据表中字段，支持条件过滤，源端数据可以按照一定的特定条件进行交换，支持采用 WHERE语句编程。

7、支持本地/远程FTP、SMB、NFS等工作模式，支持强制访问控制，具备强制访问标志自定义、具备上传/下载安全等级分组、具备FTP命令黑白名单过滤。

8、支持Txt、AVI、Bak、Bat、BMP、BWF、Dll、Doc、Docx、Excel、Exe、MP3、PDF、PPT、PPTX、XML、Zip、WMA、Wps等文件特征过滤、具备文件特征智能识别功能，能针对新的特征文件进行系统自动学习和识别；具备文件名和文件内容过滤；具备文件大小、文件病毒过滤。

9、支持SMTP、POP3协议邮件中继。

10、具备本地访问控制功能，能对协议类型、源IP、本地IP、源端口、本地端口动作等进行限制。

11、支持设置冗余传输次数，传输次数范围 1-10，多次传输，降低数据丢失的风险。

12、支持与数据交换系统联动，支持视频信令、视频流分开独立设备传输。

13、日志存储时间大于180天；提供多种日志，条件查询，支持日志筛选、查看，并支持以log文本格式导出到本地；提供syslog与SNMP日志服务接口。

14、产品提供3年产品系统升级授权、产品保修服务、远程支持服务。

## 入侵检测（3台）

1、1U标准式机架硬件设备，含交流冗余电源，配备管理口≥1个、RJ45串口≥1个、千兆电口≥6个、千兆光口≥4个，扩展插槽位≥2个，硬盘≥4T。

2、采用国产化处理器和国产操作系统，CPU：内核≥8核、主频≥2.3GHz，内存≥32GB，满检速率≥9800Mbps，TCP并发连接数≥1000万。

3、系统应提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为10000种以上，获得CVE-Compatible兼容性认证。

4、系统支持手动添加非法IP、域名、到黑名单的功能。

5、支持基于SCADA等工控协议的相关漏洞攻击检测。

6、系统需提供至少五种以上内置规则模板，帮助用户快速上线。如DMZ区服务器、内网客户端、Web服务器、Windows服务器、UNIX服务器防护等规则模板，并可根据内置规则模板直接派生模板。

7、系统须支持IPv6/IPv4双协议栈功能，能同时辨识IPv4和IPv6通讯流量。支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略，为IPv6环境提供入侵检测。

8、系统应具备用户身份识别能力，支持基于用户身份进行策略配置、日志记录与查询；支持自动与手动获取用户信息列表并生成组织结构图。

9、系统应具备实时的日志归并功能，可以根据用户需要，按照告警事件的源/目的IP、事件类型等信息，对告警日志执行归并，有效抵御告警风暴。

10、系统应提供DoS/DDoS攻击检测能力，支持PING/UDP/SYN /ACK/DNS Request/DNS Reply Flooding，TCP/UDP PortScan，Ping Sweep，ARP Spoof，HTTP Get/HTTP Post Flood等常见的DoS/DDoS的攻击。

11、系统应提供服务器异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为。

12、系统应提供入侵行为特征的自定义接口，可根据用户需求定制相应的检测规则。

13、提供入侵检测功能模块，3年升级授权，远程支持服务，产品保修服务，硬件故障上门支持。

## 数据防泄漏（3台）

1、2U标准式机架硬件设备，含交流冗余电源，配备管理口≥1个、USB接口≥4个、千兆电口≥3个、千兆光口≥2个，扩展插槽位≥3个，硬盘≥4T。

2、网络流量处理性能≥500Mbps，邮件处理能力≥28万封/天，文件扫描识别能力≥24G/小时，数据库扫描识别能力≥240万条/小时，入库量≥5000条/秒。

3、支持旁路部署、串路部署、一体机部署、虚拟化云部署（软探针Agent）、代理部署（支持ICAP模式）。

4、具备内容识别功能，支持按正则表达式对文字内容进行识别，内置身份证、手机号、银行卡号、固定电话、邮件地址等正则表达式规则，方便策略引用。

5、支持关键词，多关键词组合形式的内容检测；支持关键词权重，至少命中次数，与或等复杂规则组合形式；支持忽略中文简繁体、英文大小写，恶意混淆等方式；支持英文、日韩语、或其他小语种的语言。

6、支持办公类、文本类、图片类、压缩包类、音视频类、源代码类、图纸类等常见文件类型识别 （如： doc、docx、xls、xlsx、ppt、pptx、rtf、pdf、txt、html、xml、rar、zip、tar、gzip、7z、iso 等常见的文档类型解析和内容提取）。

7、支持自定义格式文件类型的识别；支持上传文件自动生成/识别文件类型。

8、支持标准 HTTP（HTTPGET，HTTPPOST）、EMAIL（SMTP、POP3、IMAP、Exchange）、FTP（SMB1、SMB2）、OPC、modbus等协议识别。

9、支持OCR引擎，对网络外发的图片内容进行提取与识别（如：jpg、bmp、png、tiff、gif、dwg 等常见图片）。

10、支持伪装文件类型格式识别，如更改文件后缀仍可识别真实文件类型(如将“文件.doc”修改为“文件.dat”)。

11、支持数据库访问结果集审计，MySQL、Oracle、SQL Server、Postgresql、DB2、Sybase、Hbase；支持解析访问数据库返回的结果集，并依策略对敏感数据识别匹配。

12、支持文档溯源，文件记录MD5，根据MD5值可进行文件溯源查询。

13、支持选择不同的策略，对策略命中数据进行差异对比，以此进行策略设置调优。

14、提供3年产品升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

## 集控探针（3台）

1、1U标准式机架硬件设备，含交流冗余电源，配备RJ45串口≥1个、USB接口≥1个、千兆电口≥6个，内存≥16G，SSD硬盘≥512GB。

2、支持设备数据采集功能，数据采集性能≥4000条/s。

3、具有SNMP采集、SYSLOG收集、应用交换日志、交换日志统计、系统操作日志等功能。

4、系统可接收被管设备的SNMP trap信息，用于接收业务日志、设备运行信息等；支持SNMP V2和V3版本。

5、系统可接收被管设备的SYSLOG日志信息，用于接收操作日志、非标准格式日志等

6、系统支持接收被管设备基于Agent组件集成的运行信息数据，包括cpu利用率、内存利用率、磁盘利用率、接口流量等。

7、提供3年产品升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

## 集中监控系统（1台）

1、1U标准式机架硬件设备，含交流冗余电源，配备RJ45串口≥1个、USB接口≥1个、千兆电口≥6个，内存≥16G，SSD硬盘≥512GB。

2、具有业务侦测、设备自身管理、拓扑管理、日志管理等功能。

3、支持标准Syslog trap和Syslog端口自定义。

4、支持对内部链路管理，包括了对接入链路的新增、修改、删除、查看操作。

5、支持级联上报。

6、支持对业务类型、设备状态以及数据的统计进行直观查询。可在首页查看所有接入设备的在线离线状态。

7、支持被管设备资源池的监控功能，可实时提供目标设备的CPU、磁盘、内存、网络的详细使用情况（每个应用进程的消耗情况）。

8、提供3年产品升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

## 安全边界接入网关（3台）

1、1U标准式机架硬件设备，含交流单电源，配备RJ45串口≥1个、USB口≥2个、管理口≥2个、千兆电口≥6个、千兆光口≥4个，扩展插槽位≥2个，SATA硬盘≥4T、SSD硬盘≥128G。

2、HTTPS吞吐量≥2Gbps，最大并发连接数≥6000，每秒新建连接数≥10000，每秒新建用户数≥500，实配授权最大并发在线用户数≥500。

3、支持HA高可用、集群部署模式，以提高业务访问稳定性；客户端支持主流PC、移动端操作系统，包括Windows、MacOS、IOS、Android、Linux等；移动客户端支持Android, IOS SDK，并支持通过管理后台获得标准SDK、对接指导手册和demo样例。

4、支持网关集群的流量负载均衡，以提高网关响应速度，解决网络拥塞问题，达到高质量的网络访问效果。

5、支持客户端环境感知功能，支持客户端基础信息收集和上报，包括PC主机名/CPU/内存/操作系统/网卡/主板信息等信息，支持磁盘信息、进程信息、网络访问、补丁、终端软件等信息采集。

6、支持用户通过客户端及Web门户修改密码/PIN码，在管理员通过管理界面配置允许进行短信或邮件进行密码/PIN码更改后，用户自助在客户端通过验证可修改密码，以减轻管理员日常管理工作。

7、移动端支持导出终端认证日志，可通过协同工具发送给技术支持人员进行终端故障定位及排查。

8、 支持通过SDP模式代理C/S或通过非http/https类协议通信的应用，支持在代理通信中通过双向TLS加密传输。

9、支持账户自定义属性管理，可为组织提供个性化账户属性配置及管理，系统缺省提供默认账户属性，管理员可根据本组织需要进行自定义角色配置，以为不同角色进行授权。

10、支持对用户认证访问及风险情况进行概览展示，展示项包括但不限于：在线用户、终端等总览信息，用户风险情况统计排行、认证/授权情况TOP排行。

11、支持对所授权应用在WEB门户、电脑客户端、移动客户端分别进行展示配置，可配置特定应用仅通过电脑客户端展示，不展示在WEB门户及移动端。

12、支持为B/S应用上传国密证书，以支持国密加解密通信。

13、支持ABAC用户属性授权策略，支持根据用户自定义数据进行分类授权。

14、提供3年产品升级授权、远程支持服务、产品保修服务、硬件故障上门支持。

## 接入防火墙（3台）

1、1U标准机架式设备，采用国产化操作系统和国产化处理器，≥4个千兆电口（含≥1对bypass口），≥1个独立管理口，≥1个HA口，≥2个空闲接口扩展槽，≥8GB内存，≥1TB硬盘。

2、防火墙吞吐量≥12Gbps，防病毒吞吐量≥2Gbps，IPS吞吐量≥2.5Gbps，最大并发连接数≥300万，每秒新建连接数（HTTP）≥10万，提供IPSec VPN隧道数≥10000条，SSL VPN最大用户并发数≥6000个（配置≥8个SSL VPN用户数）。

3、支持入侵防御功能，具备多种协议和应用的攻击检测和防御，IPS特征库数量≥15000条。

4、支持防火墙策略命中次数统计及分析，统计首次命中及最近命中天数等细粒度分析，以及策略冗余检查，能够提升策略运维效率，防火墙支持策略助手功能，能够自动学习网络流量，自动生成防火墙策略。

5、支持热补丁升级功能，可在保证业务不中断的情况下，对设备当前系统版本进行升级维护。

6、产品具备开放性，提供丰富的RestAPI接口，具备与云管平台、SDN控制器、自动化运维管理等平台对接能力，实现自动化运维。

7、支持实现终端摄像头的识别和访问控制。

8、支持数据包路径检测能力，能够图形化的Debug展示数据包通过防火墙每个模块是否出现问题，如是否创建会话，是否匹配策略，是否进行流量管理等，便于图形化故障调试。

9、提供手机APP的监控通告服务，实现对防火墙的安全监控和威胁事件告警，且要求手机APP与所投产品为同一厂商。

10、支持VPN功能，提供IPSec VPN功能，提供SSL VPN页面定制功能特性，包括登录页面、交互信息、提示信息等定制功能。

11、支持全功能CLI（SSH、TELNET、CONSOLE等方式）命令配置，以方便快速进行脚本操作和故障调试，且CLI配置必须支持中文输入。支持配置文件备份到防火墙，备份数量≥10个；

12、支持WebUI开局安装向导，帮助用户按照指引的步骤完成防火墙设备的初始配置，包括系统时间、许可证等基本配置、路由模式的部署以及安全策略相关防护配置。

13、支持对NAT地址池中的地址进行有效性探测，在出现地址池地址不可用的时候自动排除，保障互联网业务安全稳定运行。

14、为保障所投设备日常使用的稳定性，要求所投产品通过《电磁兼容 试验和测量技术 浪涌（冲击）抗扰度实验》中所提及的测试标准。

15、所投产品具备国家网络与信息系统安全产品质量监督检验中心颁发的《信息技术产品安全测试证书》。

16、所投产品具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书(EAL4+)》。

17、配置3年应用识别、入侵防御、Web防护、威胁情报、病毒过滤功能模块，3年产品质保。