ICS 13.310
A 91

GA

中华人民共和国公共安全行业标准

GA/T XXXX.3—XXXX

公安视频图像信息系统安全技术要求 第3部分：安全交互

Security technical requirements for video and image information system for public security—Part 3: Security interaction

（报批稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国公安部　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

GA/T XXXX《公安视频图像信息系统安全技术要求》分为4个部分：

——第 1 部分：通用要求；

——第 2 部分：前端设备；

——第 3 部分：安全交互；

——第 4 部分：安全管理平台。

本文件是 GA/T XXXX的第3部分。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由公安部科技信息化局提出。

本文件由全国安全防范报警系统标准化技术委员会（SAC/TC100）归口。

本文件起草单位： 苏州科达科技股份有限公司、杭州熙菱信息技术有限公司、公安部第一研究所、视频图像信息智能分析与共享应用技术国家工程试验室、公安部安全与警用电子产品质量检测中心、北京市公安局、浙江宇视科技有限公司、金鹏电子信息机器有限公司、深信服科技股份有限公司、杭州迪普科技股份有限公司、山东华软金盾软件股份有限公司、拓尔思天行网安信息技术有限责任公司、锚丁科技（北京）有限责任公司。

本文件主要起草人： 杨学军、张震宇、周群、王建勇、栗红梅、吴园、赖齐、吴参毅、韩煜、魏一、仇俊杰、邓永茂、鲁大军。

本文件于202x年首次发布。

公安视频图像信息系统安全技术要求

第3部分：安全交互

1. 范围

本文件规定了公安视频传输网的上下级主干网络间、主干网与接入网间，以及公安视频传输网与其他网络互联的安全交互系统架构、安全等级划分、安全策略、设备性能要求。

本文件适用于公安视频图像信息系统安全交互系统的规划设计、开发研制、部署实施、检测验收和运行维护。

2. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB 35114—2017 公共安全视频监控联网信息安全技术要求

GA/T 1400（所有部分）公安视频图像信息应用系统

GA/T XXXX.1—XXXX 公安视频图像信息系统安全技术要求 第1部分：通用要求

GA/T XXXX.2—XXXX 公安视频图像信息系统安全技术要求 第2部分 前端设备

3. 术语和定义、缩略语

3.1. 术语和定义

GB/T 22239、GB/T 28181、GB 35114—2017、GA/T 1400.4、GA/T XXXX.1—XXXX界定的术语和定义适用于本文件。

3.2. 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

DDoS：分布式拒绝服务（Distributed Denial of Service）

FTP：文件传输协议（File Transfer Protocol ）

ID：身份标识（Identity Document）

IP：因特网协议（Internet Protocal）

JDBC：Java数据库连接（Java Database Connectivity ）

MAC：媒体访问控制（Media Access Control）

SNMP:简单网络管理协议（Simple Network Management Protocol）

Syslog:系统记录（Syslog）

TCP/IP：网络通讯协议（Transmission Control Protocol/Internet Protocol）

4. 安全交互系统架构

4.1 安全交互体系

4.1.1 安全交互系统分为横向边界安全交互系统和纵向安全防护系统，结构框图见图1。

4.1.2 横向边界安全交互系统包括视频交换链路和数据交换链路，其中视频交换链路应采用符合GB/T 28181、GB 35114—2017视频联网协议和公安移动信息网专用协议的隔离交换；数据交换链路应采用符合GA/T 1400等协议和其它通用数据的隔离交换。

4.1.3 纵向安全防护系统是在视频资源接入时以及上下级的公安视频图像信息系统之间建立的安全防护系统，用于视频资源接入和上下级之间的纵向连接。纵向安全防护系统不隔离路由，上下级系统之间应用路由可达。纵向连接应采用符合GB/T 28181及GB 35114—2017视频联网协议、GA/T 1400视图库协议和其他必要的远程访问、运维和安全服务的交互。

4.1.4 公安视频传输网与公安信息网之间进行视频和数据交换时，应满足公安信息网边界接入的相关规定。

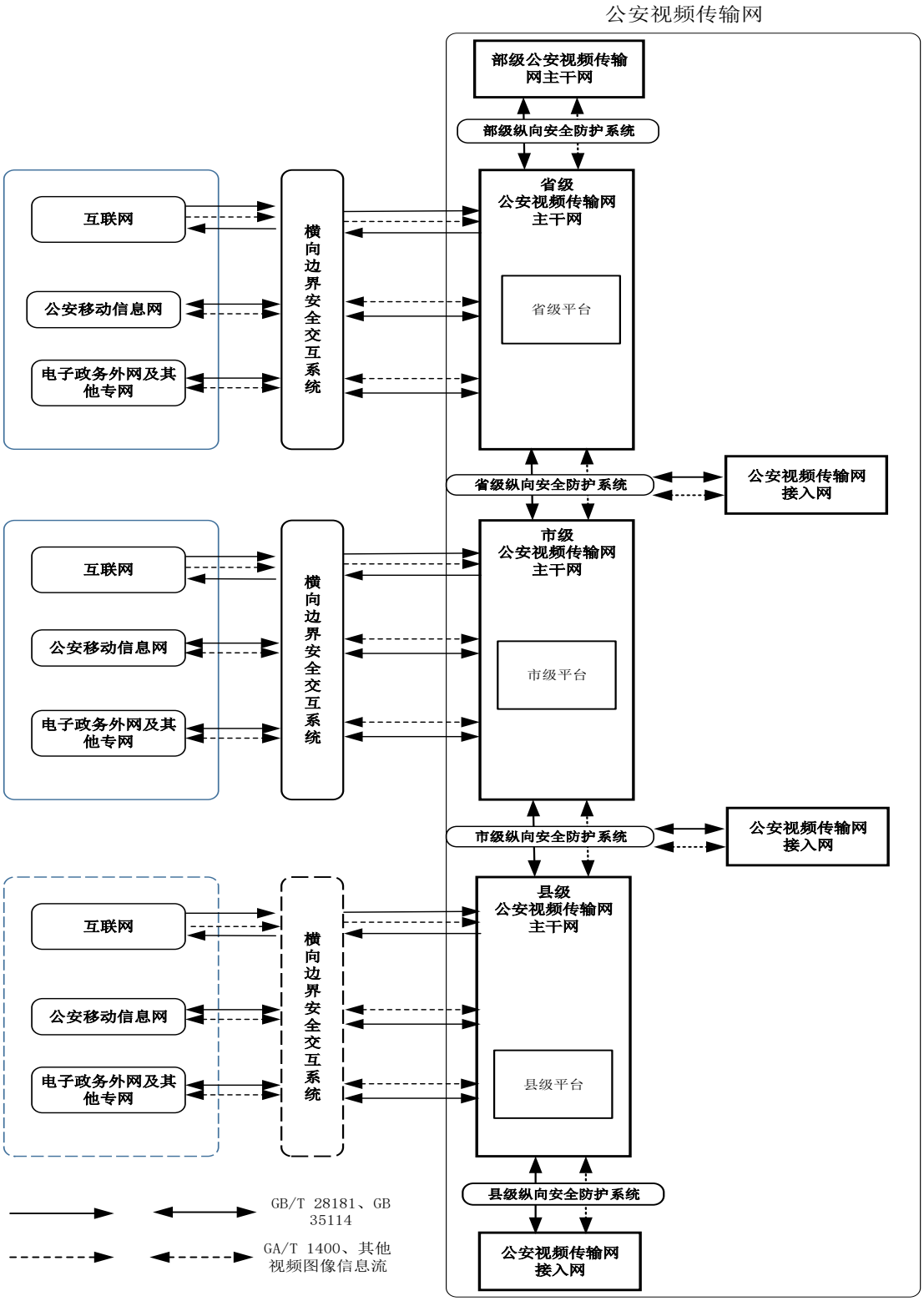

图 1　安全交互体系结构框图

4.2　横向边界安全交互系统功能架构

4.2.1　功能架构

横向边界安全交互系统功能架构见图2，共包含五个安全域：路由接入区、边界保护区、应用服务区、安全隔离区和安全监测与管理区，每个安全区域实现不同的安全功能。

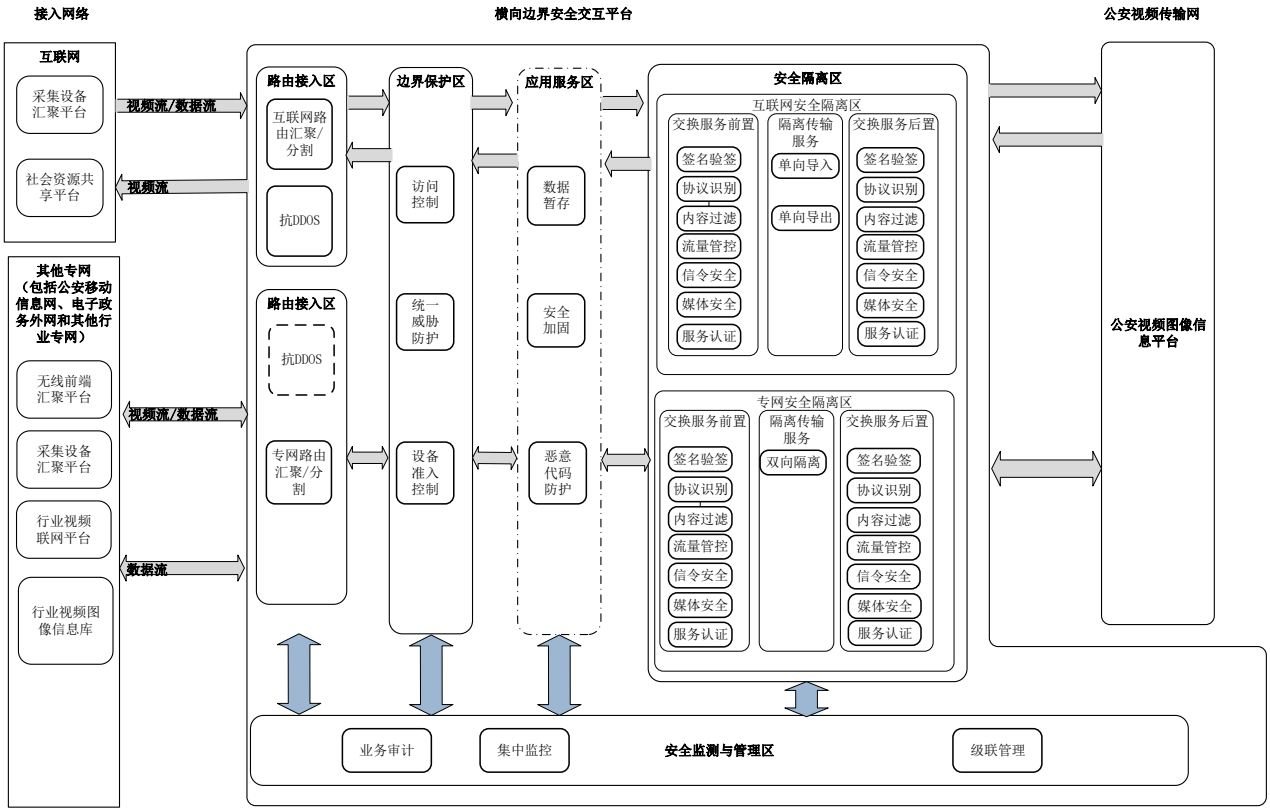

图 2 横向边界安全交互系统功能架构图

4.2.2 路由接入区

路由接入区将各外部链路与横向边界安全交互系统连接。实现路由访问控制，将来自不同接入对象或不同外部链路的数据流或视频流按照不同的安全策略加以区分。

4.2.3 边界保护区

边界保护区主要实现对横向边界安全交互系统的边界保护，支持的主要安全功能为：实现访问控制、设备准入和统一威胁防护，包括网络入侵防护和网络恶意代码防护等安全能力。

4.2.4 应用服务区

应用服务区主要处理各类与应用相关的操作，是对外信息发布、信息采集和数据交换的中间区域，支持应用代理、数据暂存、安全加固、恶意代码防护等功能。在视频交换链路中，一般不强制要求建立应用服务区。

4.2.5 安全隔离区

安全隔离区实现公安视频传输网与互联网、其他专网的安全隔离与信息交换，主要包括：

a) 针对互联网视频接入和视频共享，安全隔离区提供单向导入、单向导出、签名验签、协议识别、内容过滤、流量管控、服务认证、信令安全、媒体安全等安全能力。其中，视频流都采用单向传输的方式；

b) 针对互联网数据单向导入和单向导出，安全隔离区提供单向导入、单向导出、签名验签、格式检查、内容过滤、流量管控、服务认证等安全能力。其中，数据流都采用单向传输的方式；
c) 针对其他专网视频交换，安全隔离区提供双向隔离、签名验签、协议识别、内容过滤、流量管控、服务认证、信令安全、媒体安全等安全能力；
d) 针对其他专网数据交换，安全隔离区提供双向隔离、签名验签、协议识别、格式检查、内容过滤、流量管控、服务认证等安全能力。

4.2.6 安全监测与管理区

安全监测与管理区实现横向边界安全交互系统的业务审计、集中监管与级联上报等。支持以下主要安全功能：

a) 对各个安全组件的日志和交换业务日志进行采集；
b) 对横向边界安全交互系统的资产信息、安全基线、运行状态、配置管理、策略管理进行集中监管；
c) 向上级系统级联上报本级系统的数据。

4.3 纵向安全防护系统功能架构

4.3.1 功能架构

纵向安全防护系统包含安全防护区和安全监测与管理区，系统功能架构见图3。

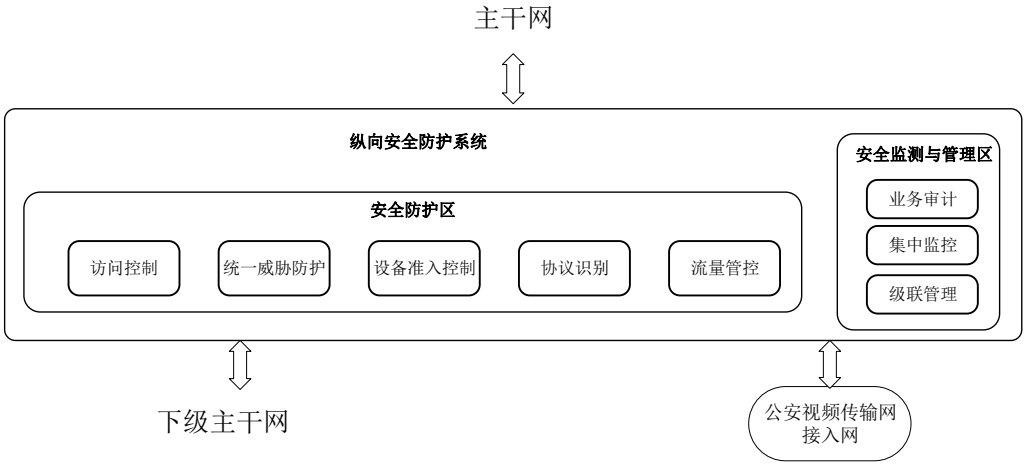

图 3 纵向安全防护系统功能架构图

4.3.2 安全防护区

安全防护区支持有线前端设备、无线前端设备、下级公安视频图像信息系统与上级公安视频图像信息系统进行可控的信息交换，支持以下主要安全功能：

a) 对有线前端设备，安全防护区提供设备准入、访问控制、统一威胁防护、协议识别和流量管控等安全能力，支持符合 GB/T 28181、GB 35114—2017 的视频流和符合 GA/T 1400 及其他必要的远程访问、运维和安全服务协议的数据流双向交换；
b) 对无线前端设备，安全防护区提供设备准入、访问控制、统一威胁防护、协议识别和流量管控等安全能力。支持符合 GB/T 28181、GB 35114—2017 的视频流和符合 GA/T 1400 及其他必要的远程访问、运维和安全服务协议的数据流双向交换；

c) 对下级公安视频图像信息系统，安全防护区提供设备准入、访问控制、统一威胁防护、协议识别和流量管控等安全能力,应支持符合 GB/T 28181、GB 35114—2017 的视频流和符合 GA/T 1400 和其他必要的远程访问、运维和安全服务协议的数据流双向交换。

4.3.3 安全监测与管理区

安全监测与管理区实现纵向安全防护系统的业务审计、集中监管与级联上报等,可以与横向边界安全交互系统共用，支持以下主要安全功能：

a) 支持对各个安全组件的日志和交换业务日志进行采集；
b) 支持对纵向安全防护系统的资产信息、安全基线、运行状态、配置管理、策略管理进行集中监管；
c) 支持向上级系统级联上报本级系统的数据。

4.4 无线视频前端的安全交互原则

4.4.1 无线视频前端的接入分为互联网接入和专网接入两种模式。

4.4.2 无线视频前端的互联网接入模式应由横向边界安全交互系统提供接入安全交互隔离。

4.4.3 无线视频前端应采用运营商VPDN或无线专网链路接入模式,应由纵向安全防护系统提供安全交互接入。在接入公安视频传输网时，宜采用基于GB 35114—2017的设备认证并符合GB 35114—2017的C级规定。

5. 安全等级划分

5.1 横向边界安全交互系统安全等级

5.1.1 横向边界安全交互系统的视频交换链路的安全等级由低到高分为基本级、增强I级、增强II级。每个等级的安全策略如下：

a) 基本级：应采用IP/MAC地址绑定、设备指纹等设备认证准入控制、防DDOS攻击、访问控制、统一威胁防护、安全加固、恶意代码防护、签名验签、协议识别、内容过滤、流量管控、服务认证、业务审计、集中监控、级联管理、双向隔离或单向导入、单向导出等安全策略；
b) 增强I级：在基本级基础上增加基于GB 35114—2017 的设备认证准入控制、针对控制信令的内容过滤安全策略；
c) 增强II级：在基本级基础上增加基于GB 35114—2017的设备认证准入控制、针对控制信令的内容过滤安全策略、针对媒体流的内容过滤安全策略。

5.1.2 横向边界安全交互系统的数据交换链路不区分安全等级，应采用设备证书、IP/MAC地址绑定等设备认证准入控制、防DDOS攻击、访问控制、统一威胁防护、安全加固、恶意代码防护、签名验签、协议识别、格式检查、内容过滤、流量管控、服务认证、业务审计、集中监控、级联管理、双向隔离或者单向导入、单向导出等安全策略。

5.2 纵向安全防护系统安全等级

纵向安全防护系统的安全等级由低到高分为基本级、增强I级、增强II级。每个等级的安全策略如下：

a) 基本级：应采用IP/MAC地址绑定、设备指纹等设备认证方式、访问控制、统一威胁防护、流量管控、协议识别、内容过滤等安全策略；
b) 增强I级：在基本级基础上增加基于GB 35114—2017的设备认证、针对控制信令的内容过滤安全策略；

c） 增强II级：在基本级基础上增加基于GB 35114—2017的设备认证、针对控制信令的内容过滤安全策略、针对媒体流的内容过滤安全策略。

5.3 安全等级选择原则

横向边界安全交互系统的安全等级和纵向安全防护系统的安全等级应符合下列规定：

a） 横向边界安全交互系统安全等级要求：
- 县(区、市）级根据需求可选择基本级；
- 地、市级（含）以上应不低于增强I级；
- 省级（含）以上宜采用增强II级；

b） 纵向安全防护系统安全等级要求：
- 县（区、市）级应不低于基本级；
- 地、市（含）以上应不低于增强I级；
- 省级（含）以上宜采用增强II级。

6. 安全策略

6.1 访问控制

应支持通过防护规则实现网络访问控制。对不符合防护规则的访问，系统应进行拦截并发出告警。

6.2 设备准入控制

6.2.1 横向边界应支持对外部接入设备的准入控制，并应满足下列要求：

a） 应支持对具有唯一性标识的设备进行认证；

b） 应支持对具有数字证书的设备进行认证；

c） 应支持设备注册，注册信息应包括设备IP/MAC、设备ID、设备属性等信息；

d） 宜支持采集外部接入设备的硬件信息、操作系统补丁状态、病毒库、进程、注册表、账户等信息，为信任评估提供实时准确的设备环境信息；

e） 宜通过基于安全模块的环境完整性度量技术，感知外部接入设备运行环境和状态。

6.2.2 纵向防护应支持对外部接入设备的准入控制，认证方式应符合GA/T XXXX.2—XXXX的规定。

6.3 统一威胁防护

应支持通过检测、阻断、限流、审计报警等防御手段，对蠕虫、后门、木马、间谍软件、Web攻击、拒绝服务等攻击形式进行有效防御。

6.4 安全加固

应支持通过打补丁、安装脚本、调整配置等方式增强系统的健壮性，防范或阻断恶意攻击，提升系统安全性。

6.5 恶意代码防护

应支持通过恶意代码检测引擎和恶意代码库的技术融合，对恶意代码进行高效检测和防御。

6.6 签名验签

签名验签应满足以下要求：

a） 支持签名验证，确保交换数据的真实性、完整性和不可抵赖性；

b） 支持对无签名或签名验证不通过的数据进行拦截丢弃，并进行日志报警。

6.7 协议识别

支持对指定协议的信令和数据流数据基于安全策略进行格式检查，对不符合格式的信令和数据流数据进行拦截丢弃，并进行日志报警。

6.8 内容过滤

内容过滤应满足以下要求：

a) 支持对指定协议的信令和数据流数据基于安全策略进行内容过滤，对含有敏感信息的信令和数据流数据进行拦截丢弃，并进行日志报警；
b) 支持对文本文件基于安全策略进行内容过滤，对含有敏感信息的文件进行拦截丢弃，并进行日志报警；
c) 支持对数据库内格式化数据基于安全策略进行内容过滤，对含有敏感信息的数据库数据进行拦截丢弃，并进行日志报警；
d) 支持对API请求/响应报文数据基于安全策略进行内容过滤，对含有敏感信息的API报文数据进行拦截丢弃，并进行日志报警。

6.9 流量管控

支持对视频和数据流量进行监测，以规则或统计基线判定异常并实施控制。

6.10 服务认证

服务认证应满足以下要求：

a) 支持通过鉴权方式对服务调用方进行身份认证，认证凭证包括数字证书、口令密码、动态令牌、Token等；
b) 支持对服务调用方进行权限控制，确保最小授权；
c) 支持对服务提供注册、编目、查询、变更、注销等功能。

6.11 信令安全

支持采用信令签名或信令加密等技术保证信令协议自身安全，抵御信令被篡改、夹带、窃听等安全风险。

6.12 媒体安全

支持采用媒体流签名或媒体流加密等技术保证媒体流自身安全，抵御媒体流被篡改、夹带、窃听等安全风险。

6.13 单向导入

单向导入应满足以下要求：

a) 支持数据物理单向传输，确保无任何反向通道；
b) 支持对导入数据传输过程记录日志。

6.14 单向导出

单向导出应满足以下要求：

a) 支持数据物理单向传输，确保无任何反向通道；
b) 支持对导出数据传输过程记录日志。

6.15 双向隔离

双向隔离应满足以下要求：

a) 支持根据事先定义安全策略对协议头剥离，支持根据事先定义安全策略对协议头进行再生；
b) 支持通过协议隔离方式断开内部TCP/IP连接，并在数据摆渡过程中不同时连接两侧主机；
c) 支持对数据摆渡传输过程记录日志。

6.16 业务审计

业务审计应满足以下要求：
a) 支持以syslog、JDBC、FTP、API接口等方式采集业务日志数据；
b) 支持对采集到的日志数据进行范式化、标准化处理；
c) 支持将采集到的所有安全组件日志向相关系统进行报送。

6.17 集中监控

集中监控应满足以下要求：
a) 支持边界安全交互系统资产管理，实现信息注册、资产维护、知识管理、漏洞管理等功能；
b) 支持对边界安全交互系统内核心关键设备运行状态进行检测和展现；支持对业务运行状态进行统计；支持依据业务审批信息设置业务监控报警阈值；支持流量和流速异常告警、违规业务告警和应用访问异常告警等业务监控报警功能；
c) 支持边界安全交互系统策略管理，实现安全策略配置下发、策略变更、策略删除、策略查询等功能；
d) 支持边界安全交互系统的安全反制，安全反制能够持续改进安全策略，实现动态安全防御，反制手段包括阻断非合规访问、阻断后续访问等；
e) 支持边界安全交互系统的服务配置管理，支持使用通用数据交换、接口服务、指定协议等交换服务接口申请服务对象，并审核申请合规性；支持通过审核服务的发布、变更和注销等功能。

6.18 级联管理

应支持边界安全交互系统级联管理，实现数据报送、审批、通报等功能。

7. 设备性能要求

7.1 横向边界安全交互系统视频交换链路性能应符合表1的规定。

表1 横向边界安全交互系统视频交换链路性能表

性能项	指标		
	基本级	增强Ⅰ级	增强Ⅱ级
传输时延/路	≤200ms	≤300ms	≤400ms
视频数据流吞吐量	≥200Mbps		
并发路数	≥50 路（按每路 4Mb/s 计算）		
每秒新建会话数	≥500 个		

7.2 横向边界安全交互系统数据交换链路性能应符合表2的规定。

表2　横向边界安全交互系统数据交换链路性能表

应用层吞吐量	≥400Mbps；
数据库同步速率	≥5000 条/s
FTP 并发同步速率	≥400Mbps
消息同步速率	≥3000 个/s
API 服务注册数	≥100 个
API 并发数	≥1000
传输时延	≤100ms

7.3 纵向安全防护系统性能应符合表3的规定。

表3　纵向安全防护系统性能表

性能项	指标		
	基本级	增强 I 级	增强 II 级
传输时延/路	≤100ms	≤200ms	≤300ms
视频数据流吞吐量	≥1000Mbps		
并发路数	≥250 路（按每路 4Mb/s 计算）		
每秒新建会话数	≥500 个		

7.4 边界集中监测与管理性能应符合表4的规定。

表4　边界集中监测与管理系统性能表

性能项	指标
日志采集速率	≥800EPS
级联上报延时	≤10s