

ICS

点击此处添加中国标准文献分类号

SZDB/Z

深圳市标准化指导性技术文件

SZDB/Z XXXXX—XXXX

移动警务云终端建设规范

点击此处添加标准英文译名

点击此处添加与国际标准一致性程度的标识

(征求意见稿)

2018-01-10

XXXX - XX - XX 发布

XXXX - XX - XX 实施

深圳市市场监督管理局 发布

目 次

前言 VIII

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 系统组成 2

6 技术规范 3

前 言

本文件按照GB/T 1.1-2009给出的规则起草。

本文件由深圳市公安局视频警察支队提出。

本文件由深圳市公安局安全技术防范管理办公室归口。

本文件起草单位：。

本文件主要起草人：。

警务云终端建设规范

1 范围

本文件规定了警务云终端的网络建设规范、硬件通用规范、云平台建设规范、APP应用开发规范、终端管理规范。

本文件适用于深圳市公共安全领域的移动智能化应用。军队、公检司法、金融、海关等领域移动智能化应用可参照执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 4793.1-2007 测量、控制和实验室用电气设备的安全要求 第1部分：通用要求

GB/T 9813.1 计算机通用规范 第1部分：台式微型计算机

GB 31241-2014 便携式电子产品用锂离子电池和电池组安全要求

GA/T 818-2009 警用便携式治安管理信息采集终端通用技术要求

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1 双系统终端

同时运行“互联网系统”和“安全系统”的移动智能终端。应符合以下要求：

- a) 底层隔离：双系统从底层实施隔离，分别实施安全加固、功能裁剪及禁止 ROOT、刷机等措施；
- b) 运行隔离：两个系统独立运行、独立控制，互不交换数据，一键秒级切换；
- c) 存储隔离：两个系统的系统数据、应用数据、用户数据完整隔离；
- d) 通讯隔离：“互联网系统”可访问互联网，给用户自用；“安全系统”仅能访问公安无线虚拟专网，专用于警务工作，不存储业务数据；
- e) 双在线：任意系统使用移动数据网络，或互联网系统通过 wifi 接入互联网时，两个系统的网络通讯可同时在线。

3.2 公安信息网

是指公安机关开展工作使用的内部专用计算机网络，不得传输、处理、存储涉及国家秘密的信息。

3.3 公安无线虚拟专网

是基于运营商无线网络，利用 L2TP 隧道技术为警务工作构建的与公众互联网隔离的虚拟专用网络。用户使用移动终端通过无线 VPDN/VPN 网络安全地访问用户内网资源。

3.4 缩略语

下列缩略语适用于本文件。

AAA: 认证、授权、审计 (Authentication Authorization Accounting)

APP: 应用软件 (Application)

CDMA 2000: 码分多址接入 (Code Division Multiple Access 2000)

CDMA-IS95: CDMA 移动站—针对双模宽带蜂窝系统的与基站兼容的标准 (CDMA Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System)

CHAP: 握手认证协议 (Challenge-Handshake Authentication Protocol)

CPU: 中央处理器 (Central Processing Unit)

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

FDD: 频分复用 (Frequency Division Duplex)

GSM: 全球移动通信系统 (Global System for Mobile Communication)

GW: 网关 (GateWay)

IMEI: 国际移动设备身份码 (International Mobile Equipment Identity)

IMSI: 国际移动用户识别码 (International Mobile Subscriber Identification Number)

IP: 互联网协议 (Internet Protocol)

IPSec: IP 安全协议 (IP security)

L2TP: 第2层隧道协议 (Layer 2 Tunneling Protocol)

MEID: 移动设备识别码 (Mobile Equipment Identifier)

NFC: 近场通信 (Near Field Communication)

PE: 运营商网络侧边缘设备 (Provider Edge)

PPTP: 点对点隧道协议 (Point to Point Tunneling Protocol)

QoS: 服务质量 (Quality of Service)

RUIM: 可移动用户识别模块 (Removable User Identity Module)

SIM: 客户识别模块 (Subscriber Identification Module)

TCP/IP: 传输控制协议/因特网互联协议 (Transmission Control Protocol/Internet Protocol)

TD-SCDMA: 时分同步的码分多址 (Time Division-Synchronous Code Division Multiple Access)

TDD: 测试驱动开发 (Test-Driven Development)

TF/SD: 快闪存储器卡 (Trans-flash Card/Secure Digital Memory Card)

UDP: 用户数据报协议 (User Datagram Protocol)

UIM: 用户识别模块 (User Identify Module)

uRPF: 单播反向路由查找 (Unicast Reverser Path Forwarding)

USB: 通用串行总线 (Universal Serial Bus)

USIM: 全球用户标识模块 (Universal Subscriber Identity Module)

VPDN: 虚拟拨号专用网络 (Virtual Private Dialed Network)

VPN: 虚拟专用网络 (Virtual Private Network)

WCDMA: 宽带码分多址 (Wideband Code Division Multiple Access)

WiFi: 无线网络 (Wireless Fidelity)

WLAN: 无线局域网 (Wireless Local Area Network)

4 系统组成

4.1 概述

警务云终端是一部定制双系统移动终端。通过公安无线虚拟专网和警务云平台，警务云终端实现在公安无线虚拟专网内与警务云平台交互，并由警务云平台通过安全边界与公安信息网交换数据。

4.2 警务云终端架构图

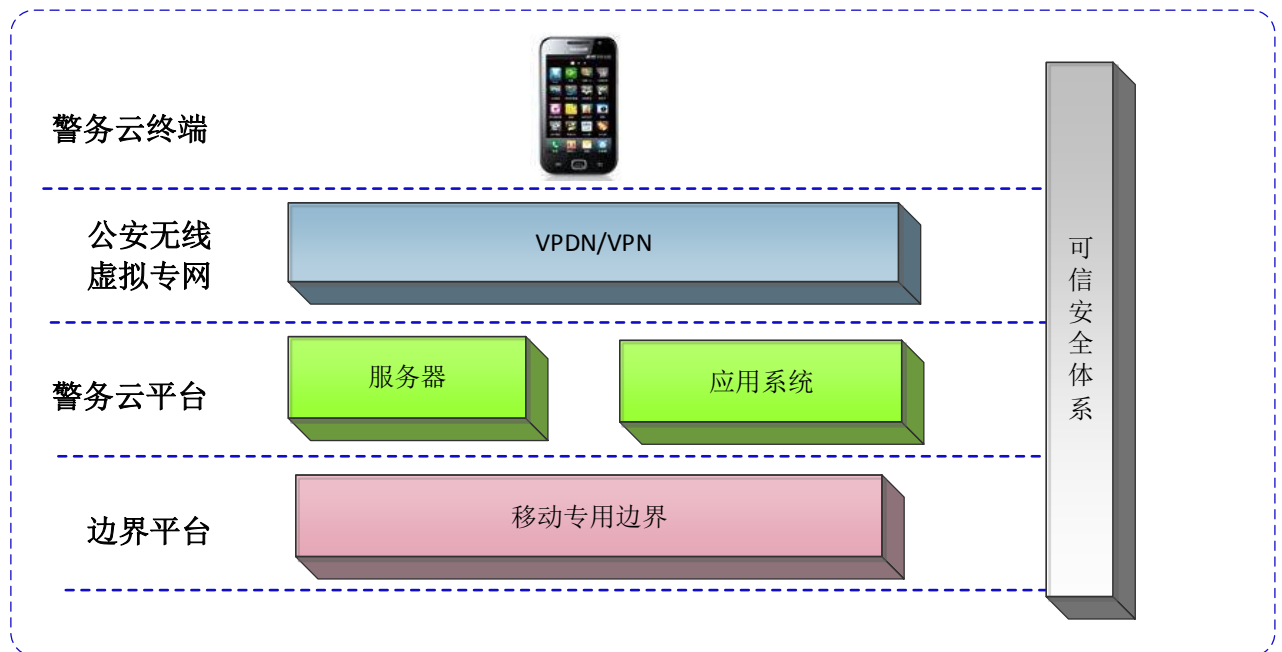


图1 警务云终端架构图

5 技术规范

5.1 网络建设规范

5.1.1 公安无线虚拟专网应承载在通信运营商移动网络和专线链路上，通过 L2TP、PPTP 等标准隧道协议建立加密通信，其中密码加密算法符合 CHAP，数据加密算法符合 IPSec，与互联网隔离。

5.1.2 移动终端在无线侧通过运营商蜂窝移动数据网络空中加密方式接入，且有线部分通过运营商专线接入，与互联网隔离，保障网络的安全可靠性。

5.1.3 在业务路由器上（如 PE）应实现基于物理端口的 QoS 等级标记，防止伪造 QoS 等级的攻击。

5.1.4 在业务接入控制点，应采用并发连接数控制技术，控制单个用户同时发起的信令、TCP 或者 UDP 连接的数量，阻止对信令服务器和网关发起的 DDoS 攻击。

5.1.5 在网络边缘应采用 uRPF 技术阻止可能发起的伪地址攻击。

5.1.6 通信运营商的 VPDN/VPN 系统应通过国家信息安全测评，满足信息系统安全保障级二级或以上。

5.2 硬件通用规范

5.2.1 基本要求

5.2.1.1 设备应具有工信部颁发的有效的《电信设备进网许可证》。

5.2.1.2 设备应为国产品牌智能机型。

5.2.1.3 设备应支持互联网系统和安全系统同时运行。

5.2.2 外观要求

外观应符合下列要求：

- a) 产品表面不应有明显的凹痕、破损、划痕、变形和污染等；
- b) 表面涂镀层应均匀，无起泡、龟裂、脱落和磨损现象；
- c) 金属零部件无锈蚀及其他机械损伤；
- d) 设备面板上所有标明按键功能的文字、符号应清晰、正确，易于识别。

5.2.3 标志要求

标志应符合下列要求：

- a) 在供电电源端子附近应标出电源的额定供电电压及使用电池的型号和连接极性；
- b) 开关的通断、按键的功能、各种连接的电缆以及备选件的安装均应表示清晰、明确；
- c) 需用文字表示的，应中文标出；
- d) 需用图形表示的符号应符合GB 4793.1-2007中5.1的规定；
- e) 在正常使用的情况下，标志应能长期保持清晰和牢固。

5.2.4 硬件要求

硬件应符合下列要求：

- a) 5.0 英寸或以上（电容屏、多点触控），分辨率为 1280 像素×720 像素或以上；
- b) CPU 主频 1.2GHz 四核或以上，内存容量应不少于 4G，存储容量应不少于 64G；
- c) 硬件接口应包括：
 - 1) 两个或以上外接 SIM 卡和 UIM 卡接口；
 - 2) 电源/USB 接口；
 - 3) TF/SD 卡；
 - 4) 蓝牙；
 - 5) NFC。
- d) 双摄像头（前后），前置摄像头 500 万像素或以上，后置摄像头 1300 万像素或以上；带 LED 补光灯。

5.2.5 设备软件要求

设备软件应符合下列要求：

- a) 操作系统：应使用经过安全加固的双系统软件，包括互联网系统和安全系统，两个系统同时运行，切换时间不应超过 3 秒；
- b) 应用系统：安全系统应预装终端设备管理软件、接入认证安全客户端软件等必要的应用程序；
- c) 安全系统不应预装与公安业务无关的应用软件。

5.2.6 通信要求

通信应符合下列要求：

- a) 具备移动数据通信功能，支持 4G 并向下兼容 3G、2G，数据符合 TCP/IP 协议和相关标准规定；
- b) 支持公安无线虚拟专网通过边界接入平台安全接入公安信息网，并支持在移动数据网络之间根

据信号情况自动切换，支持全国漫游接入；

- c) 支持互联网系统和安全系统分别同时接入互联网和公安无线虚拟专网，且互相隔离。

5.2.7 功能要求

功能应符合下列要求：

- a) 应具备全球定位系统（GPS、北斗等）定位及基站定位功能，卫星定位精度应在 15 米以内；
b) 设备应符合 GA/T 818-2009 中 4.1 条的要求。

5.2.8 性能要求

性能应符合下列要求：

- a) 视频帧率应不低于 25 帧/s；
b) 电池应符合 GB 31241-2014 的规定。电池连续工作时间应不小于 6h，待机时间应不小于 30 h；
c) 屏幕亮度不低于 350 cd/m²，对比度应不低于 500:1。

5.2.9 可靠性要求

可靠性应符合下列要求：

- a) 设备的可靠性应符合 GB/T 9813.1 的规定。设备的平均无故障工作时间（MTBF）不小于 5000h；
b) 应具备直流电源供电，在电压标称值±5%范围变化内，受试样品应能正常工作；
c) 电源极反接时不损坏终端能力；
d) 具备电源保护措施功能。

5.2.10 安全性要求

5.2.10.1 电气安全性要求

5.2.10.1.1 抗电强度

应符合 GB 4943.1-2011 中 5.2 的相关规定。

5.2.10.1.2 绝缘电阻

设备的电源插头或电源引入端与外壳裸露金属部件之间的绝缘电阻，常规环境条件下应不小于 100MΩ，在湿热条件下应不小于 5MΩ。

5.2.10.1.3 泄漏电流

设备的泄漏电流应不大于 5mA（AC、峰值）。

5.2.10.2 信息安全要求

5.2.10.2.1 应符合 GB/T 9813.1-2016 中的 4.4 的相关规定，设备接入公安无线虚拟专网应遵循相应技术规范。

5.2.10.2.2 身份鉴别管理要求

身份鉴别鉴定管理应符合以下要求：

- a) 应支持指纹或人脸等生物识别技术进行开机身份认证；
b) 在安全系统中应支持基于 TF 加密卡（含内置安全芯片）和 SIM/RUIM/USIM 卡相绑定的设备认证；

- c) 应支持密码长度、复杂度、更换周期、最大解锁错误次数的管理；
- d) 应实现终端系统弱口令检测与告警。

5.2.10.2.3 安全隔离要求

安全隔离应符合以下要求：

- a) 警务云终端安装有相互隔离的两个系统，两个系统没有主次，是并列关系，分为互联网系统和安全系统；
- b) 支持双系统隔离的终端，各系统所使用的存储区域应隔离；
- c) 确保联系人、短信等的隔离存储；
- d) 双系统隔离，通话、短信应能选择在安全系统接收；
- e) 互联网系统只能访问互联网，安全系统只能访问公安无线虚拟专网，应可检测并阻断安全系统访问互联网的行为；
- f) 应具备相应安全技术措施限制通过互联网系统对安全系统的渗透。

5.2.10.2.4 访问控制要求

访问控制应符合以下要求：

- a) 应限制对操作系统、应用软件等重要配置和敏感数据的访问权限；
- b) 安全系统中WLAN、蓝牙应通过移动终端管理平台进行授权网络连接和数据通信；
- c) 应确保安全系统仅能运行移动终端管理平台授权的应用。

5.2.10.2.5 数据安全要求

数据安全应符合以下要求：

- a) 应确保安全系统中的敏感数据加密存储；
- b) 应确保安全系统访问公安无线虚拟专网指定应用的数据加密传输；
- c) 应保证用户数据不被未授权用户查阅或修改。

5.2.10.2.6 外设控制要求

外设控制应符合以下要求：

- a) 应提供定位、录音、拍照和摄像等功能受控机制；
- b) 应提供互联网系统与安全系统切换受控机制；
- c) 应支持对I/O 接口屏蔽功能，防止非授权移动设备使用；
- d) 扩展卡槽或外置设备仅能读取指定的TF加密卡；
- e) 应具备wifi热点扫描功能。

5.2.10.2.7 TF 加密卡（含内置安全芯片）要求

TF加密卡（含内置安全芯片）应符合以下要求：

- a) 设备应安装TF加密卡（含内置安全芯片）套件，包括安全芯片、安全卡和安全加固软件；
- b) TF加密卡数据加解密、数字签名和验证、消息摘要和完整性检验等服务，应支持国产商用密码算法SM1、SM2、SM3及SM4，符合密码标准要求，配合安全平台完成数据加解密运算、数字签名验签、密钥交换和加解密、摘要值生成和完整性校验等；
- c) TF加密卡应划分多个证书容器，支持多证书认证；
- d) TF加密卡基于口令对用户进行认证，具有防暴力破解功能；
- e) TF加密卡存储容量应不小于4G，加密速度应不低于4 Mbps。

5.2.10.2.8 安全审计要求

安全审计应符合以下要求：

- a) 应能获取安全事件的审计日志；
- b) 应能获取用户操作的审计日志；
- c) 应支持向统一管理平台报送安全审计日志。

5.3 云平台建设规范

5.3.1 概述

移动警务云平台是支撑公安移动应用和移动互联网应用运行和管理的基本技术支撑系统，以及与其配套的标准和运维管理体系。

5.3.2 移动警务云平台的功能

移动警务云平台主要有以下功能：

- a) 为移动应用安全、稳定运行提供最基础的运行支撑服务，为移动应用用户提供通用便利支撑服务；
- b) 为移动应用全生命周期规范管理提供技术支撑服务，构建移动应用良好的管理、评价、共享、支撑机制；
- c) 构建开放的移动应用生态架构，促进移动应用健康、有序、繁荣发展。

5.3.3 移动警务云平台的构成

移动警务云平台由应用管理支撑系统和应用运行支撑系统构成。

5.3.4 应用管理支撑系统

5.3.4.1 总则

应用管理支撑系统分为开发管理和应用管理两部分。开发管理功能由应用开发资源服务子系统承担。应用管理功能由移动应用管理及发布子系统、移动互联网应用管理及发布子系统和应用部署监测子系统承担。

5.3.4.2 系统功能

系统功能应包括以下内容：

- a) 应用开发资源服务子系统：对应用开发者提供开发资源上传、检索、下载和知识库服务；
- b) 公安移动应用管理及发布子系统：提供行业移动应用的注册、审核、发布、撤销等全生命周期管理功能；提供对本地移动应用及其使用情况的汇聚功能，并按照统一标准开放接口，供应用部署监测子系统自动采集；
- c) 移动互联网应用管理及发布子系统：提供移动互联网应用的注册、检测、审核、发布、撤销等全生命周期管理功能；提供对移动互联网应用及其使用情况的汇聚功能，并按照统一标准开放接口，供应用部署监测子系统自动采集；
- d) 应用部署监测子系统：按照统一标准接口，定期从移动互联网应用管理及发布子系统和移动应用管理及发布子系统中采集移动应用及其使用情况，并具备统计分析功能。

5.3.5 应用运行支撑系统

5.3.5.1 总则

应用运行支撑系统包括统一认证授权子系统、移动信息资源服务子系统、应用监测评估子系统和实名认证子系统。

5.3.5.2 系统功能

系统功能应包括以下内容：

- a) 统一认证授权子系统：实现用户统一身份认证、应用访问授权、单点登录等功能；
- b) 移动信息资源服务子系统：实现统一的数据资源标准接口及数据授权访问；
- c) 应用监测评估子系统：实现行为审计、业务分析与综合评估等功能；
- d) 实名认证子系统：实现移动互联网用户实名认证功能。

5.4 APP 应用开发规范

5.4.1 总则

警务云平台应结合公安信息网业务系统和公安基层需求，基于警务云终端快速开发、集成各类警用功能：

- a) 实现警用微信：构建基于云架构的社交化应用平台，提供消息推送、警用微信、专网微博等功能，可创建、加入群组，发起交流或群聊，满足用户内部会商、沟通协同等需要；
- b) 扩展警务应用。

5.4.2 APP 应用开发要求

APP应用开发应符合以下基本要求：

- a) 用户授权访问控制：应对用户进行基于角色的授权和访问控制。用户的信息访问授权应遵循“最小权限原则”和“特权分散原则”；
- b) 系统权限访问控制：应按照“最小权限原则”限定终端系统权限访问，不得申请开放本应用不需要的终端系统权限（如启用定位功能、打开摄像头、读取通讯录等）；
- c) 日志管理与安全审计：应按照统一要求，对用户登录/退出、关键数据操作等行为记录日志。应用日志应保留用户身份信息，满足历史信息可倒查要求，并按照规范提交集中管控中心；
- d) 应用数据加密存储：移动应用应按照规定对重要数据进行加密存储；
- e) 资源访问接口要求：应遵循资源提供方的技术接口及管理规范。

5.4.3 前端应用开发标准

开发者应定义前端开发规则，在警务云终端 APP 运行的应用应遵守规则，应能帮助后台统计和管理应用。

5.4.4 后台应用开发标准

- a) 应用基本信息注册：每个新发布的应用，应在移动应用支撑平台中配置相关的应用信息；
- b) 应用日志信息注册：对于应用的每次访问，移动应用支撑平台应记录具体的操作内容、操作人、操作时间，便于在“使用排名”轻应用中统计数据 and 排查请求的有效性；
- c) 系统服务：基于公安信息网向独立应用提供的基于平台的接口；
- d) 消息服务：每个需要消息推送的应用，应配置对应的服务号，通过服务号把消息推送出去；对于服务号的配置，通过管理平台统一创建；
- e) 日志服务：提供查询自身应用的日志信息接口。

5.4.5 应用开发入住流程

应用开发入住流程应包括以下内容：

- a) 成为开发者；

- b) 申请应用；
- c) 提交审核；
- d) 开发测试；
- e) 应用上线。

5.5 终端管理规范

5.5.1 总体要求

终端管理总体要求应包括以下内容：

- a) 统一账号及登录验证，严格授权访问，实现单点登录等；
- b) 详细记录操作日志，汇聚业务采集数据，深化数据挖掘分析；
- c) 制定完善的研发、运维、使用、安保、共享等管理制度，并实现电子化、自动化监测和控制；
- d) 安全管理服务应对通信网络、区域边界、计算环境的保护部件进行标记管理、策略管理、授权管理。

5.5.2 终端安全管理

终端安全管理应包括以下措施：

- a) 生物识别。应通过指纹或人脸的识别认证，才可解锁进入系统；
- b) 安全系统。应禁止 ROOT 或刷机，预装公安定制版双系统，安全系统仅能接入公安无线虚拟专网，互联网系统只能接入互联网；
- c) 终端不存储数据。所有数据应存放在云端，终端仅缓存组织架构信息，不存储业务数据；终端丢失后，安全系统应有数据自动删除机制。
- d) 数字证书。对需与公安信息网交换数据且可能涉及公安工作秘密的警务应用，应强制实施数字证书认证，建立专用通信路径；
- e) 移动终端管理管控。定制研发并在安全系统预装移动终端管理工具，提供警务应用安全沙箱和加密通讯隧道，实施终端认证和访问控制，实现远程监控、远程擦除、预警锁定、手机找回、禁止运行非可信程序等；
- f) 应确保连续输入 10 次错误的认证信息，自动删除本机存储的工作信息。

5.5.3 专网安全管理

专网分为终端侧、运营商侧和公安机关侧三段链路。

- a) 终端安全系统侧应限制唯一网络接入点，仅限接入公安无线虚拟专网，不可接入互联网或其他网络；
- b) 运营商侧由 AAA（认证、授权、审计）服务器对终端进行域名、手机号码、IMSI 捆绑鉴权认证；
- c) 公安自建 AAA（认证、授权、审计）服务器对终端进行严格的域名、手机号、IMSI、用户名、密令、终端串码（MEID、IMEI）、IP 地址共七项信息关联验证，并在 L2TP 网络服务器部署应用层防火墙和访问控制策略，实现安全保障。

5.5.4 计算安全管理

计算安全管理应包括以下内容：

- a) 用户身份鉴别。采用如指纹、人脸、数字证书等，强化对服务器、终端用户等节点的身份认证；
- b) 强制访问控制。基于安全管理员对业务系统主客体实施统一标记，进行细粒度授权，用户执行业务操作时进行强制访问控制，为业务提供可控、安全的应用运行环境；
- c) 可信互联路径。通过对系统用户的强身份鉴别，在其与用户之间建立一条可信的通信路径；该路径的初始化只能由该系统用户完成，从而确保路径无法被篡改和旁路，保证用户身份认证过程的可信性；

- d) 数据完整性保护。对于可执行程序，确保在通过防篡改检查后才能被操作系统执行；对于业务数据，采用可信的校验机制，保证数据传输、存储过程中的完整性；
- e) 恶意代码防护。从恶意代码的特性、运行的角度防范运行，实现主动防御机制，保障工作站、服务器、边界所存储和传输的数据安全性。

5.5.5 边界安全管理

边界安全管理应包括以下内容：

- a) 边界访问控制。采用防火墙部件等的访问控制策略，对进出安全边界的数据信息进行控制，阻止非授权访问；采用安全隔离交换部件进行强隔离，进行安全数据交换；
 - b) 边界包过滤。通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出边界；
 - c) 边界安全审计。进入和流出信息流进行安全检查，禁止违反系统安全策略的信息流经过边界；实施严格、精细的安全边界日志审计，做到“记录留在边界”、入口有详细日志；
 - d) 边界完整性保护。发现和阻断违规外联，控制节点接入，实时发现并阻断入侵行为。
-