广电IPTV业务安全分析

上海分公司　　彭超

目录

广电IPTV背景概述-电视盒子时代

- 百花争放，百家争鸣

电视盒子-IPTV业务的延伸

IPTV即交互式网络电视，是一种利用宽带网，集互联网、多媒体、通讯等技术于一体，向家庭用户提供包括数字电视在内的多种交互式服务---摘自百度百科

电视盒子是一个小型的计算终端设备，只要简单的通过HDMI或色差线等技术将其与传统电视连接，就能在传统电视上实现网页浏览、网络视频播放、应用程序安装，甚至能将你手机、平板中的照片和视频投射到家中的大屏幕电视当中---摘自百度百科

盒子的世界你懂吗？

互联网电视盒子

早在12年年底小米盒子试水互联网电视盒子领域，但不到一周就夭折

广电总局介入，小米盒子虽然已经和持有牌照的华数合作，但其还可连接腾讯视频、搜狐视频等互联网视频

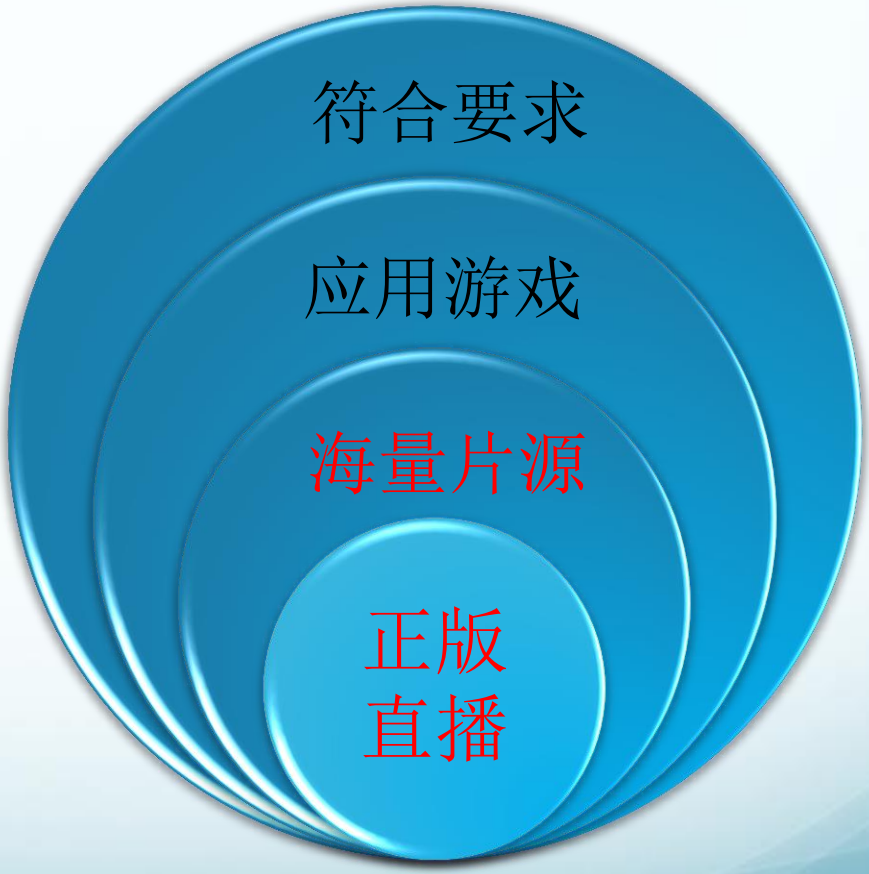
广电总局早在2011年底颁发《持有互联网电视牌照机构运营管理要求》

互联网盒子生死劫

1、 禁止电视盒子中载有任何视频应用客户端
2、 取消互联网电视盒子中直接提供的电视台节目时移和回看功能
3、 要求视频网站下架TV版应用
4、 针对视频聚合类应用进行整顿

那么问题来啦！
中国盒子哪家强？

广电盒子应运而生



安全与合规

事件：

XXX数字

广电总

《广播

《广播

广电等

〔2011〕

（GDJ

广播电视相关信息系统安全等级保护定级指南

安全播出重大事故界定标准及上报单位

事件类型		停播类型	停播时长			上报单位
			重保期的重点时段	日常重点时段/重保期	日常	
干扰插播	直插	省级及以上：全台性停播	≥15 秒钟	≥30 秒钟	≥1 分钟	逐级报总局
		省级及以上：上星广播节目停播（不含付费节目）	≥15 秒钟	≥30 秒钟	≥3 分钟	逐级报总局
		省级及以上：上星付费广播节目停播	≥30 秒钟	≥1 分钟	≥5 分钟	逐级报总局
	有插	其他广播节目停播	≥1 分钟	≥5 分钟	≥10 分钟	逐级报省局（总局直属报总局）
		地市级：全台性停播	≥1 分钟	≥5 分钟	≥10 分钟	逐级报省局
		地市级：部分节目停播	≥5 分钟	≥10 分钟	≥30 分钟	逐级报省局
	无同插	县级：全台性停播	≥5 分钟	≥10 分钟	≥30 分钟	逐级报省局
		县级：部分节目停播	≥10 分钟	≥30 分钟	≥1 小时	逐级报省局

广电IPTV业务安全分析

- 电视盒子背后的故事

呈现给我们的是这样的

IPTV业务系统组成

媒体生产、“正确的内”容推送

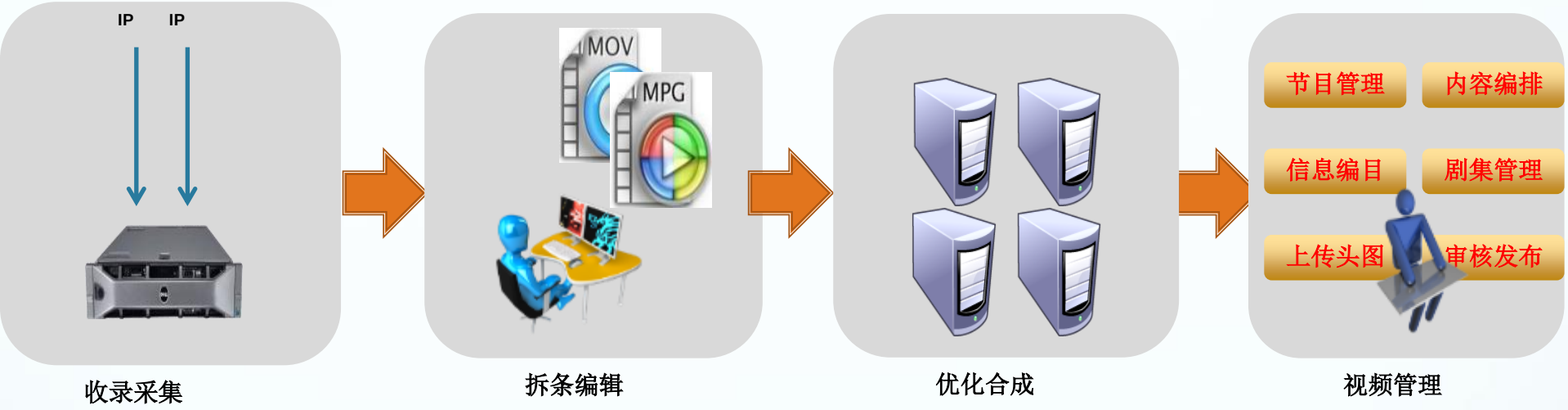
面向用户并为其提供服务

信号接收、无损传输、数据处理

媒体数据及视频分发中心

内容生产系统

内容生产系统


IP
IP
MOV
MPG
节目管理
内容编排
信息编目
剧集管理
上传头图
审核发布
收录采集
拆条编辑
优化合成
视频管理


IP收录控
IP收录控

威胁分析

1、IP收录可靠性
完整性

2、采集介质-U盘 编辑电脑主机
病毒传播？后门控制？

3、内容审核后-篡改风险
审核通过视频修改？篡改？
非法审核？

4、内容推送-位置
推送到不合理位置或复制推送

播控平台系统

面临的威胁

1、EPG管理
非法内容推送、恶意广告推送

2、付费管理
银行接口安全，支付安全

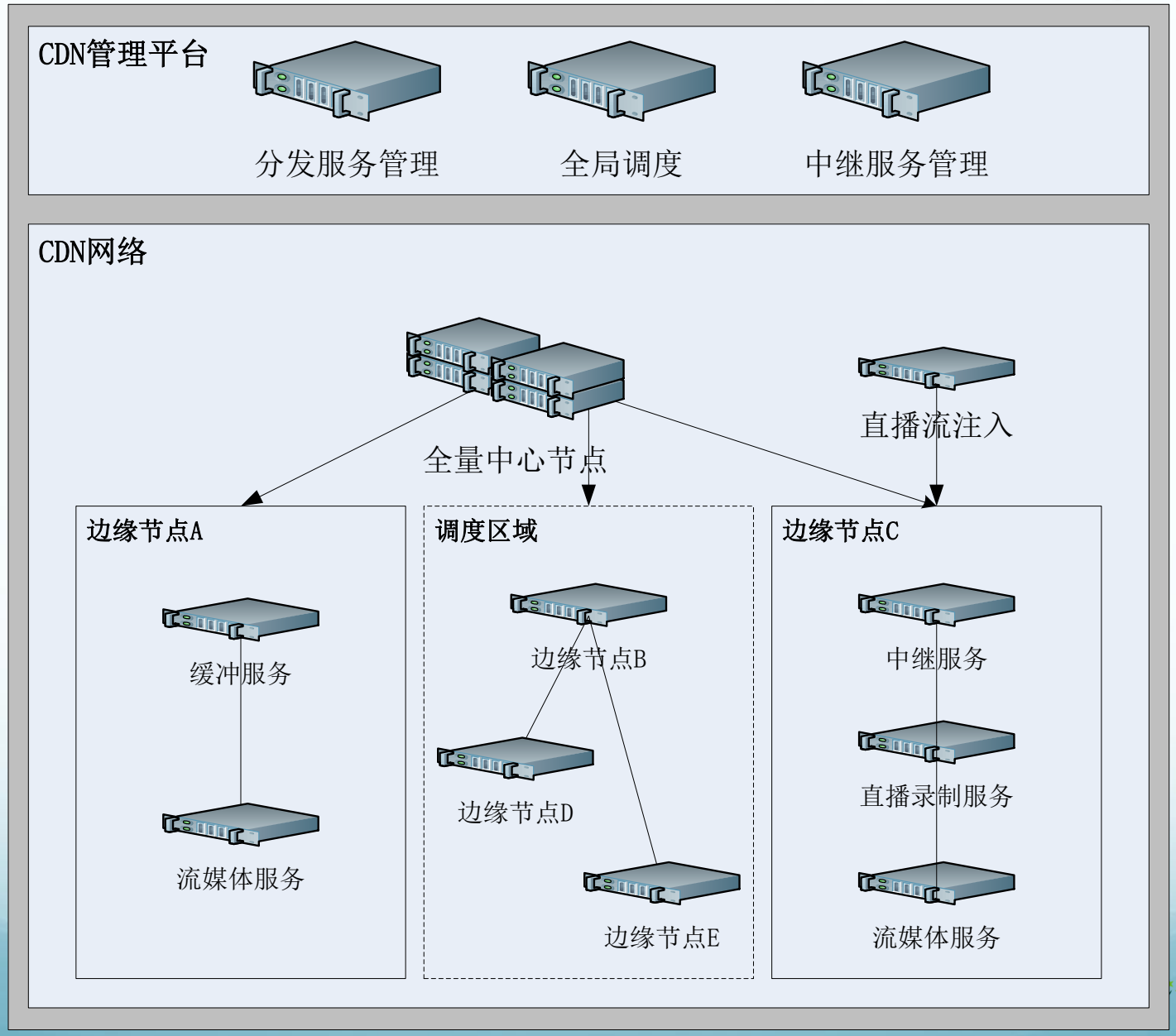
3、盒子终端
用户遥控操作安全
反接扫描

4、安全认证
唯一绑定？特征码篡改

5、用户信息
账号密码泄露？

6、应用安全
第三方应用安装或更新

CDN分发系统


CDN管理平台
分发服务管理
全局调度
中继服务管理
CDN网络
全量中心节点
直播流注入
边缘节点A
缓冲服务
流媒体服务
调度区域
边缘节点B
边缘节点D
边缘节点E
边缘节点C
中继服务
直播录制服务
流媒体服务

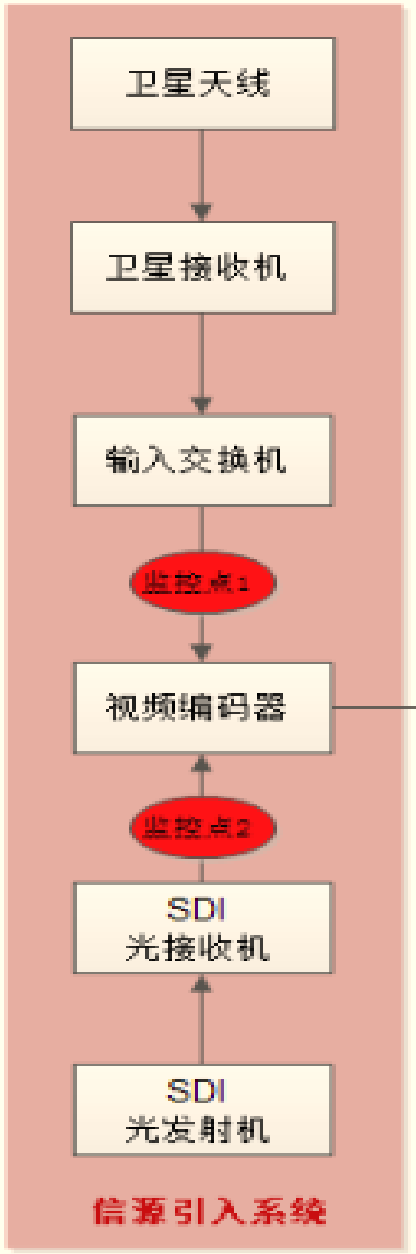
CDN-威胁分析

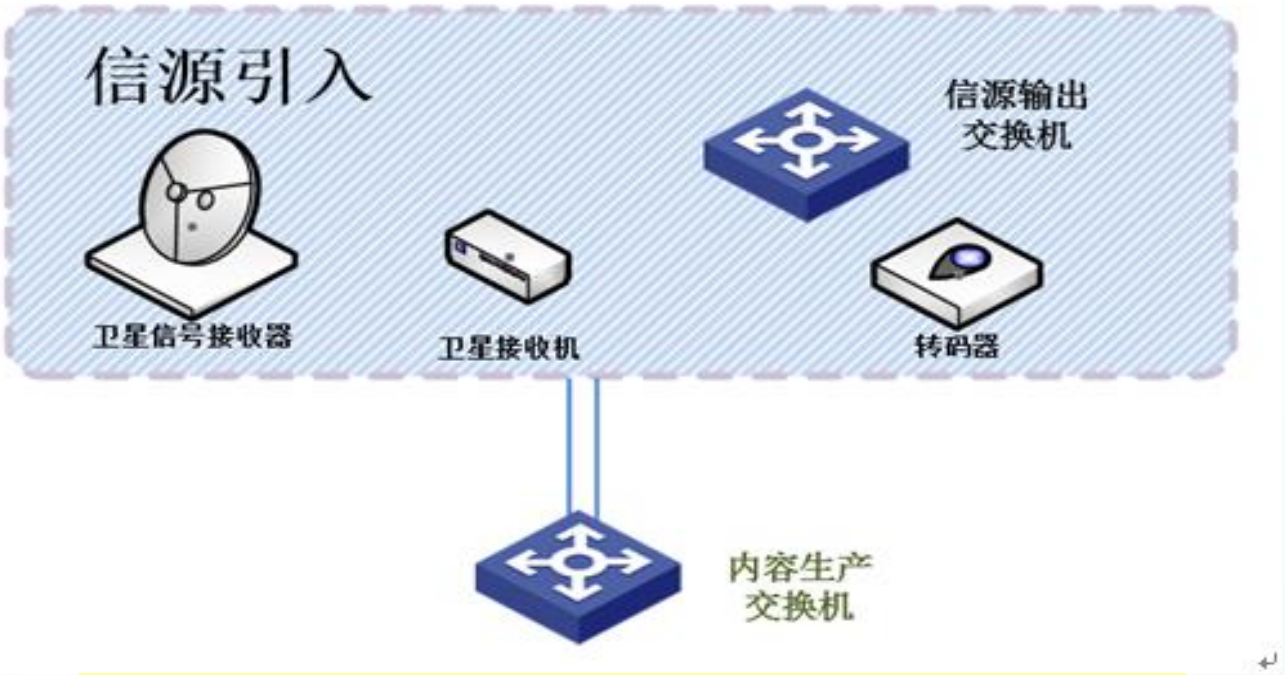
1、CDN管理平台
授权访问安全，系统漏洞安全

2、视频同步
与内容生产、信源引入同步安全

3、系统主机安全配置，弱口令

信源引入系统





资产类型	资产名称	应用说明
转码器	高清编码卡SDI	卫生健康 国学
转码器	高清编码卡SDI	暂无
转码器	高清编码卡SDI	浙江卫视高清 CCTV14
转码器	高清编码卡SDI	暂无
转码器	高清编码卡SDI	暂无
转码器	备份标清编码卡SDI	暂无
转码器	备份标清编码卡SDI	暂无
转码器	转码器网管系统	管理服务器

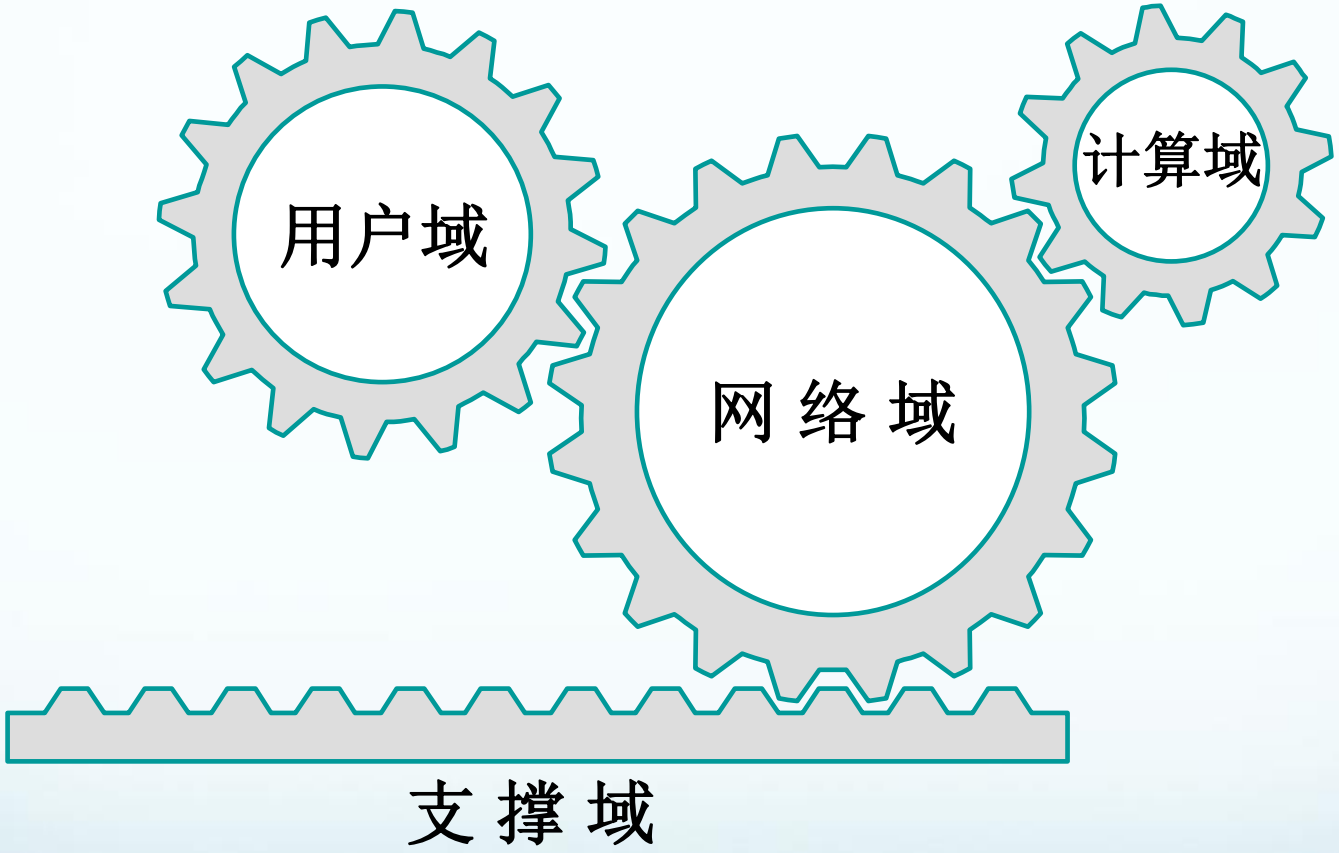
信号干扰

通过发射电磁波
对某些信号波段进行干扰

广电IPTV防护思路

- 安全域模型

安全域四要素



计算域设计

业务功能

- 依据IPTV信息系统的业务功能

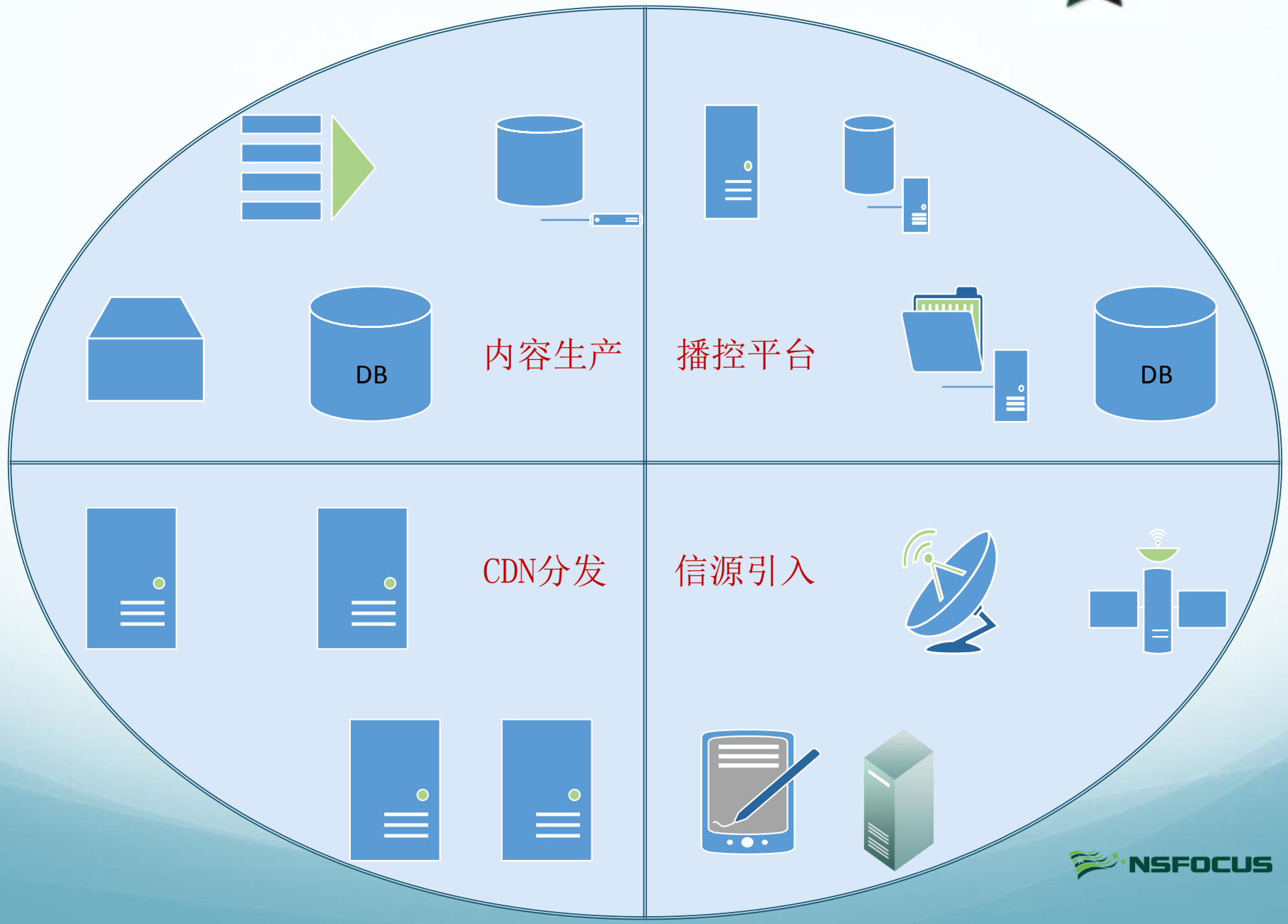
业务结构

- 依据IPTV信息系统应用结构和信息处理活动

服务对象

- 依据IPTV业务服务对象和接入方式

安全划分-计算域



用户域设计

安全划分-用户域

办公终端

业务编辑

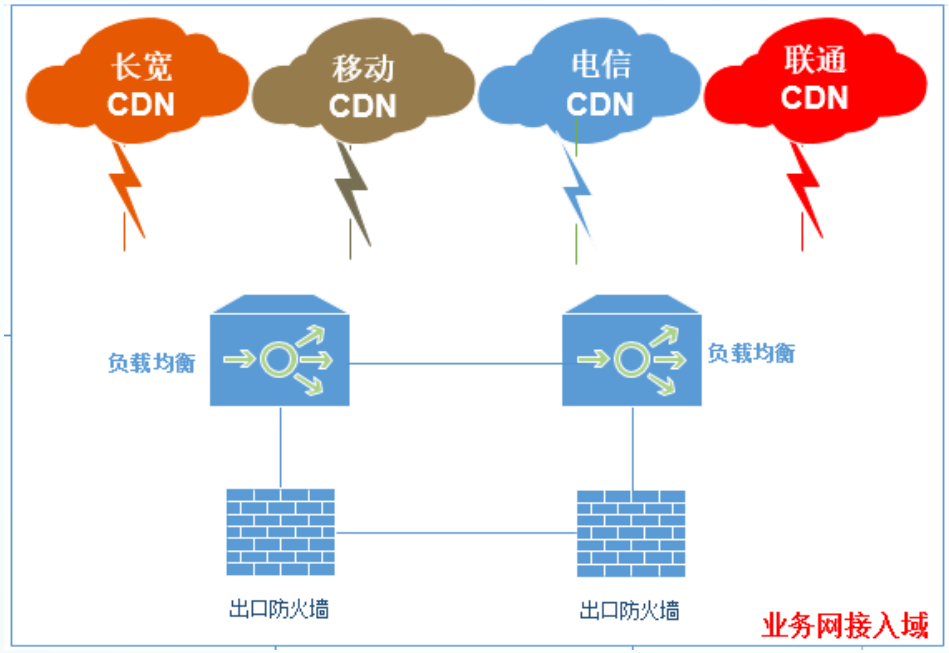
用户访问

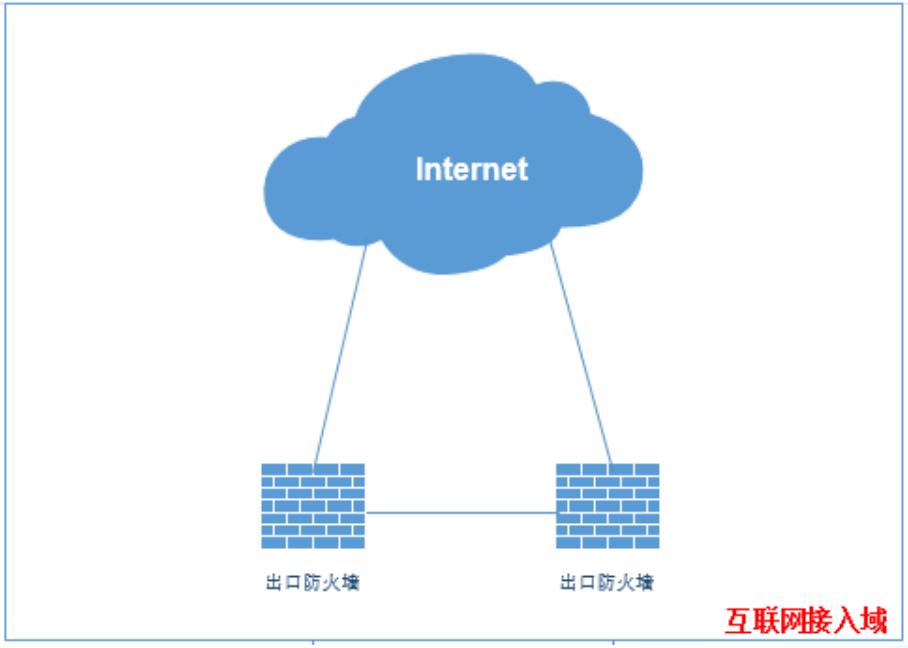
网络域设计

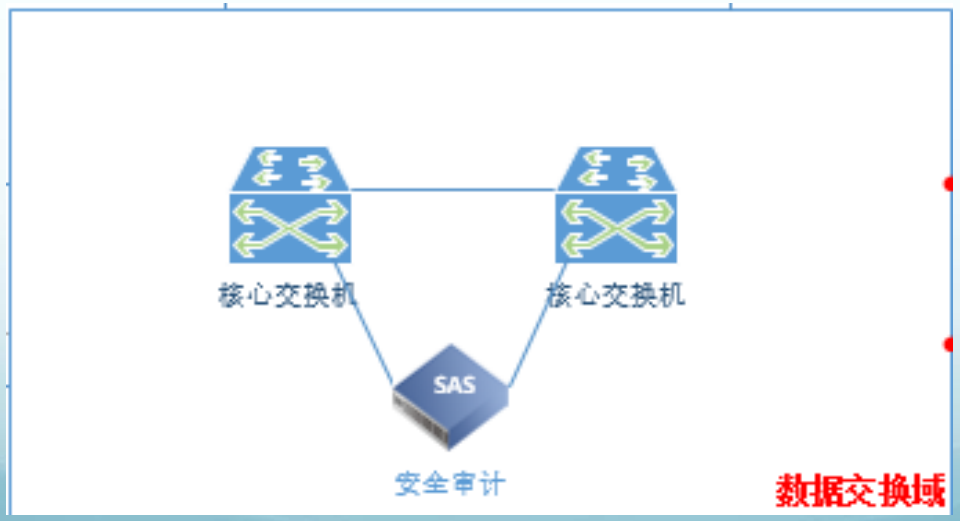
从业务数据流、管理数据流和数据处理活动的安全需求考虑

从网络的互联情况和网络IT要素的逻辑分布考虑

安全划分-网络域


长宽
CDN
移动
CDN
电信
CDN
联通
CDN
负载均衡
负载均衡
出口防火墙
出口防火墙
业务网接入域


Internet
出口防火墙
出口防火墙
互联网接入域


核心交换机
核心交换机
SAS
安全审计
数据交换域

支撑域设计

从承担信息系统的支撑功能考虑

- 控制功能
- 管理功能

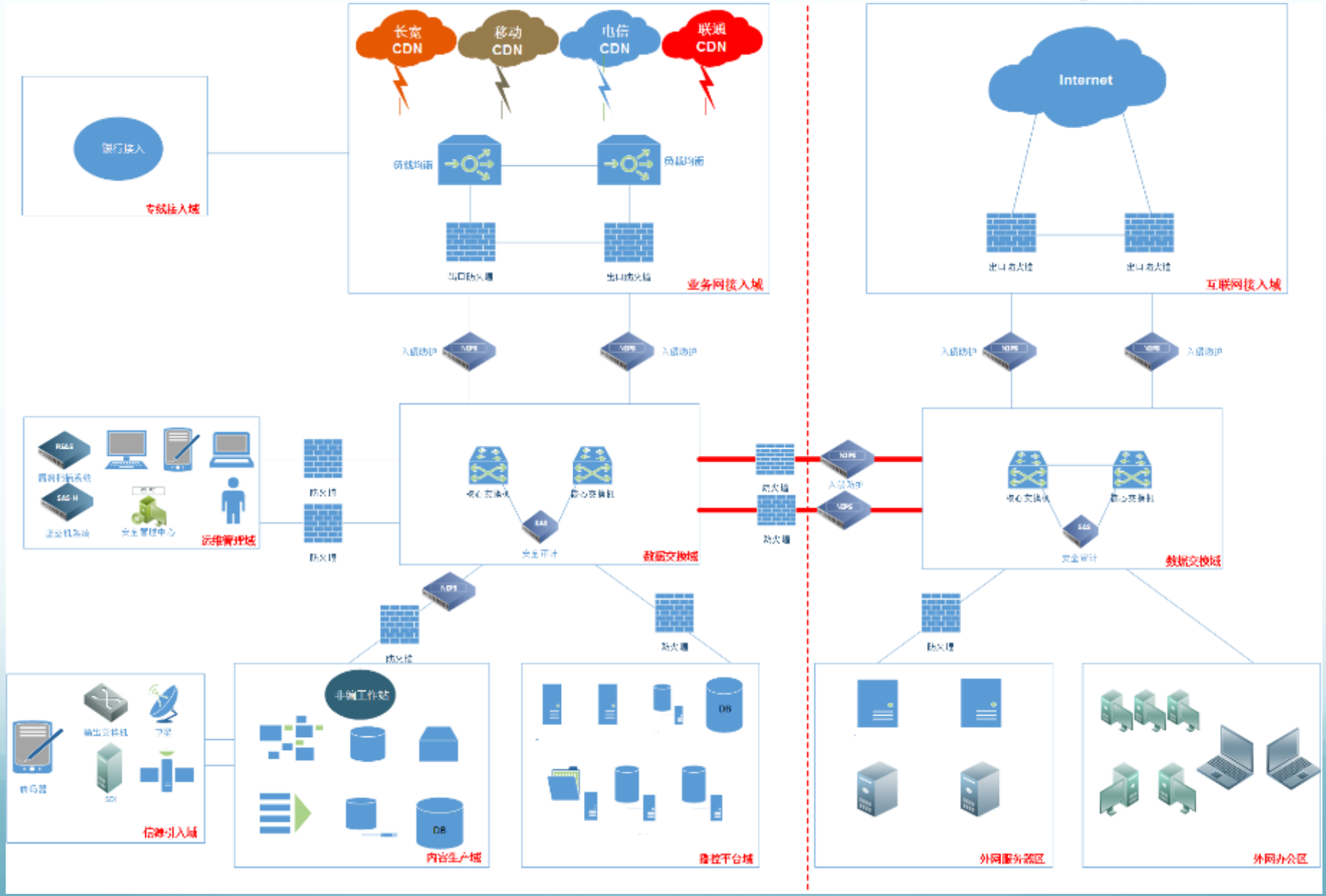
从合规性考虑

- 等级保护62号令
- SOX法令

安全划分-支撑域

运维审计监控平台
统一安全管理平台
系统安全评估平台

整体架构


长宽 CDN
移动 CDN
电信 CDN
联通 CDN
银行接入
专线接入域
负载均衡
负载均衡
出口防火墙
出口防火墙
业务网接入域
Internet
出口防火墙
出口防火墙
互联网接入域
入侵防护
入侵防护
入侵防护
入侵防护
防火墙
防火墙
核心交换机
核心交换机
安全审计
数据交换域
防火墙
防火墙
核心交换机
核心交换机
安全审计
数据交换域
防火墙
防火墙
防火墙
防火墙
非编工作站
DB
DB
内容生产域
监控平台域
外网服务器区
外网办公区
运维管理域
信源引入域

安全策略设计


对病毒蠕虫传播进行控制
满足业务和管理数据通信
满足萨班斯法案IT内控要求
防火墙策略
VLAN间策略
运维审计策略

业务数据流分析

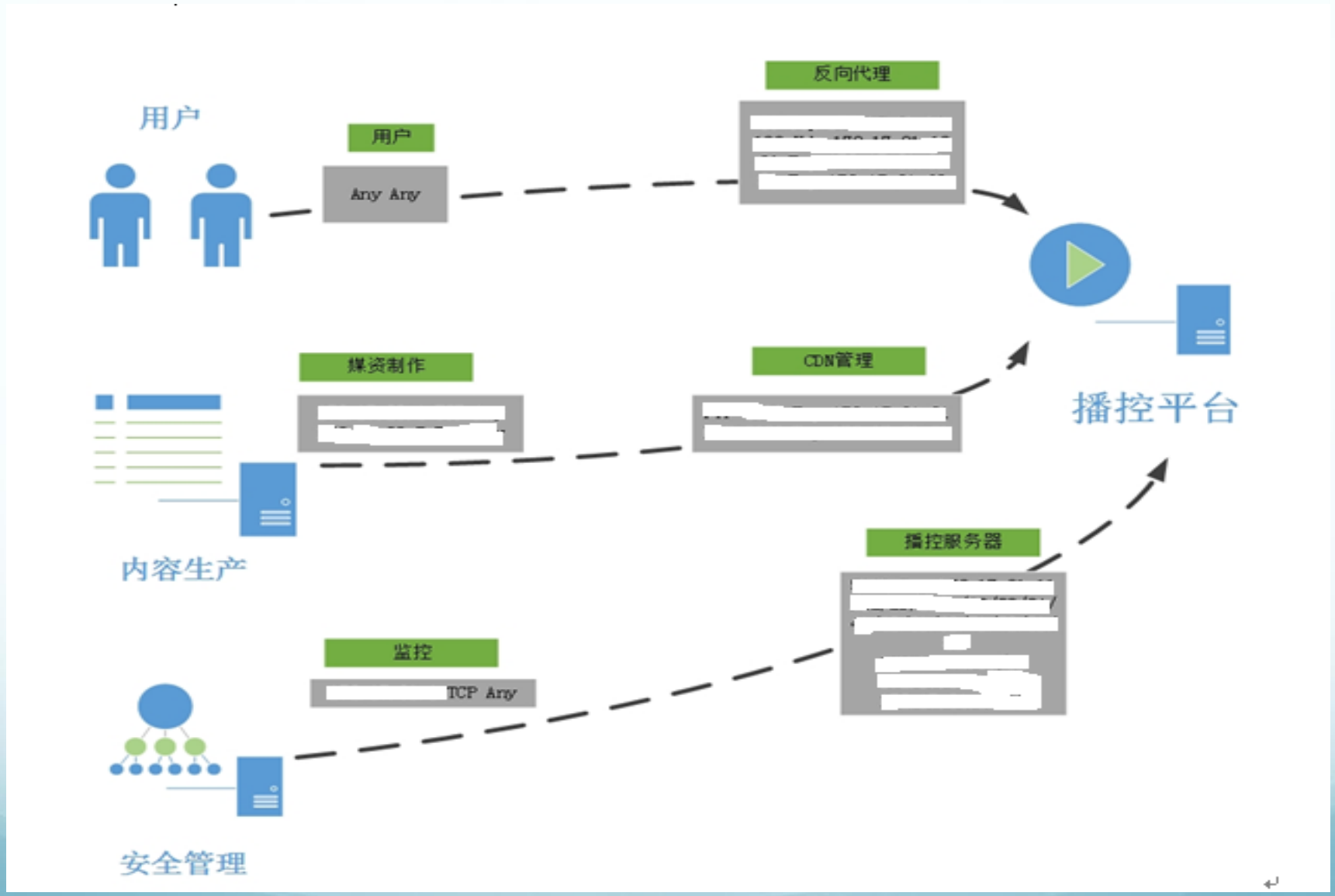
按顺序填写业务数据流的基本信息，请统计现网系统数据流情况。

1. 安全域：根据安全域划分结构图进行安全域名称填写，如内容生产域。
2. 业务类型：相应服务器业务名称。
3. IP地址：相应物理资产的IP地址，如果多个IP，请用分号隔开
4. 协议：相应业务系统使用到的协议，如UDP、TCP。
5. 端口：相应业务系统协议使用到的端口，如23、36。
6. 方向：—>（从左到右）、<—（从右到左）。
7. 功能说明：对该数据流功能、作用简要说明。

业务数据流分析

安全域	业务系统	IP地址	协议	端口	方向	端口	协议	IP地址	业务系统	安全域	功能说明
用户	用户	any	—	any			tcp		反向代理	互联网接入	用户数据请求
							udp				
							tcp				
							tcp				
							tcp		全局调度	中心CDN	
									主机负载		
							tcp		反向代理	播控平台	
							udp				
							tcp				
							tcp				
内容生产	媒资制作系统		TCP	any			TCP		CDN管理		传输视频

业务数据流分析-举例



安全策略实现-举例

1. 互联网出口的区域划分

互联网出口防火墙连接核心交换区域的核心交换机。

防火墙区域	说明
区域 A	连接负载均衡设备
区域 B	连接了核心交换机

2. 出口防火墙的访问控制策略：

1）禁止所有 IP 的病毒、蠕虫可能利用的端口 TCP:135、137、139、445、5554、9996；UDP:1434、137、139。

2）区域间的访问策略为只开放允许的和正常的访问，默认策略为禁止。

- 区域 A 对区域 B 的访问；

策略说明	允许用户通过互联网数据请求			
策略设置	源地址	目的地址	协议	条件
	Any	a.b.c.d	TCP（端口）	允许

- 区域 B 对区域 A 的访问

策略说明	XXXXXXX			
策略设置	源地址	目的地址	协议	条件
	X.X.X.X（监控服务器）	X.X.X.X	TCP（端口）ICMP	允许

策略说明	堡垒机管理中心 xxxxx			
策略设置	源地址	目的地址	协议	条件
	X.X.X.X（堡垒机）X.X.X.X（备用主机）	X.X.X.X	TCP（端口）ICMP	允许

其余全部拒绝。

2. 出口防火墙的访问控制策略：

1）禁止所有 IP 的病毒、蠕虫可能利用的端口 TCP:135、137、139、445、5554、9996；UDP:1434、137、139。

2）区域间的访问策略为只开放允许的和正常的访问，默认策略为禁止。

- 区域 A 对区域 B 的访问；

（1）VLAN 间的访问策略总览

	VLAN14	VLAN31	VLAN32	VLAN33	VLAN34
VLAN14		允许	允许	允许	允许
VLAN31	允许		允许	允许	允许
VLAN32	允许	允许		允许	允许
VLAN33	允许	允许	允许		允许
VLAN34	允许	拒绝	拒绝	允许	

结束语

三同步

黑名单、白名单

最小权限

安全运维

安全管理

谢谢