日期：2012年5月31日星期四

Huawei Enterprise A Better Way

数据中心典型业务与分区设计

www.huawei.com/enterprise

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

目录

典型业务与分区设计

业务与分区概述

典型业务与分区设计

分区

分区定义

根据企业自身特点，依据业务系统的相关性、安全性、管理、规模等因素，对数据中心的服务器进行分区

分区组成

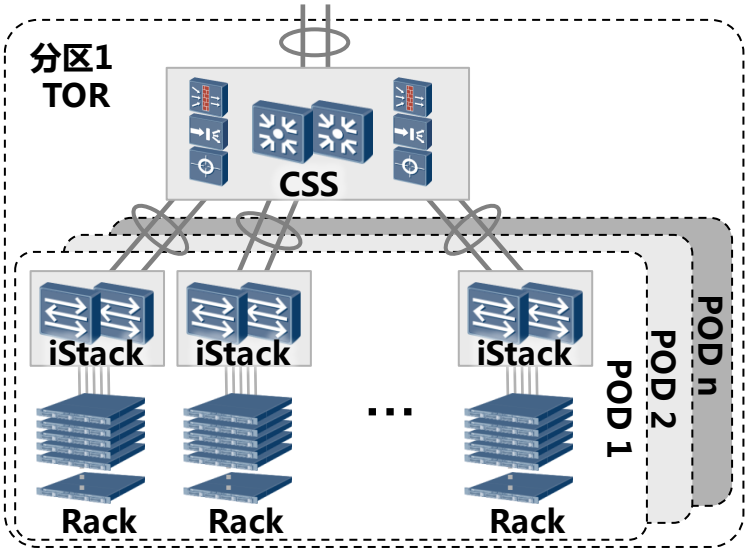
分区具备汇聚交换机，以及防火墙、负载均衡等业务设备

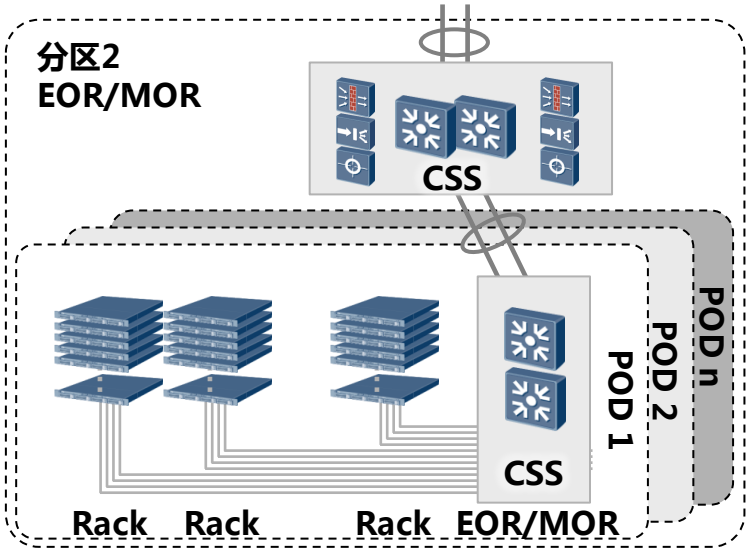
分区上行连接数据中心交换核心

如下是两种分区的示例，一个分区可由多个POD组成，采用TOR或者EOR的布局方式。

分区与业务关系

生产、办公、财务、ERP等业务，根据业务安全等级、业务关联度要求部署至不同分区





数据中心网络分区原则

安全性原则

按照安全等级不同，划分为不同分区

例如，为互联网用户，合作伙伴服务的服务器单独分区

信息敏感服务器单独分区

高可用布局原则

业务关联度高的服务器部署在同一个区域

业务关联度低的服务器拆分成多个区域

可用性要求高的业务拆分成两个对等区域。

容量适度原则

根据运维管理经验，控制单个区域内的服务数量，例如，500台以内

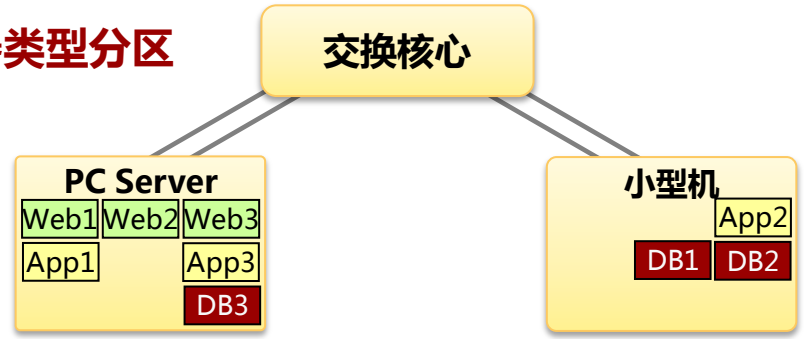
未来服务器数量增加、区域间流量增长后可考虑进一步拆分

独立运维管理原则

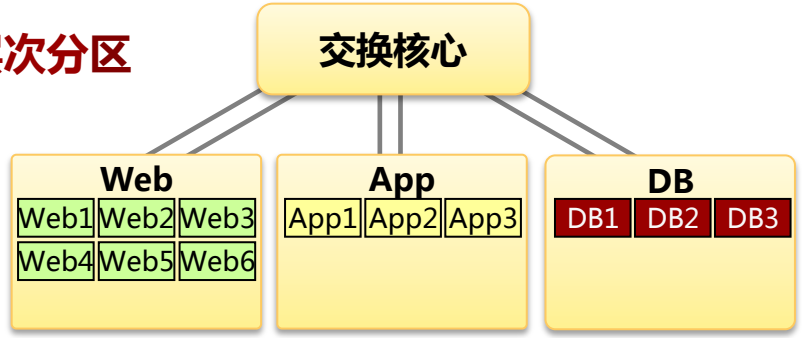
业务流量、安全控制、组网协议方面有特殊要求的服务器单独分区。

理论上的分区方式

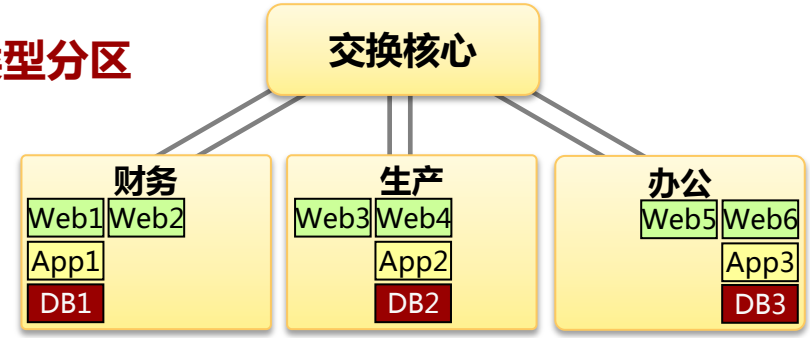
按服务器类型分区



按应用层次分区



按应用类型分区



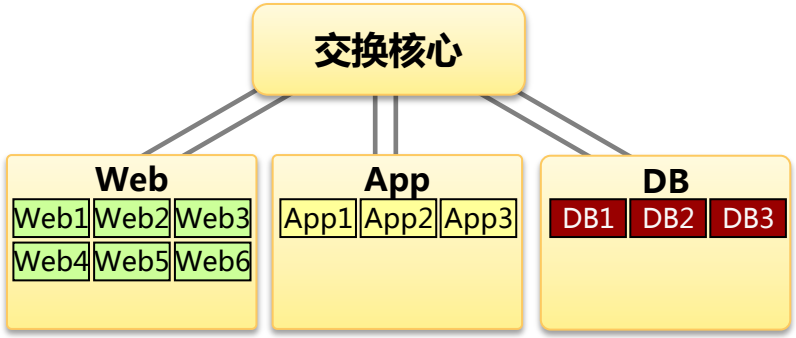
分区设计要点

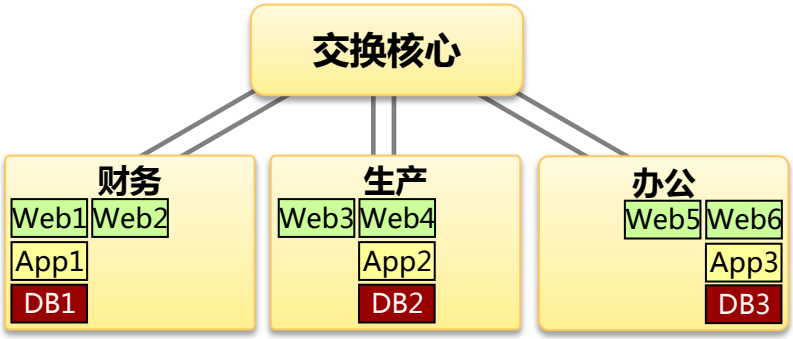
分区设计优先考虑综合布线及基础设施运维因素

可以按照服务器类型、业务应用层次、业务应用类型等方式划分，每种分区方式各有优缺点和适应范围

一个企业的数据中心，往往同时存在多种分区方式。根据业务的实际需要，多种模式混合使用

分区方式分析





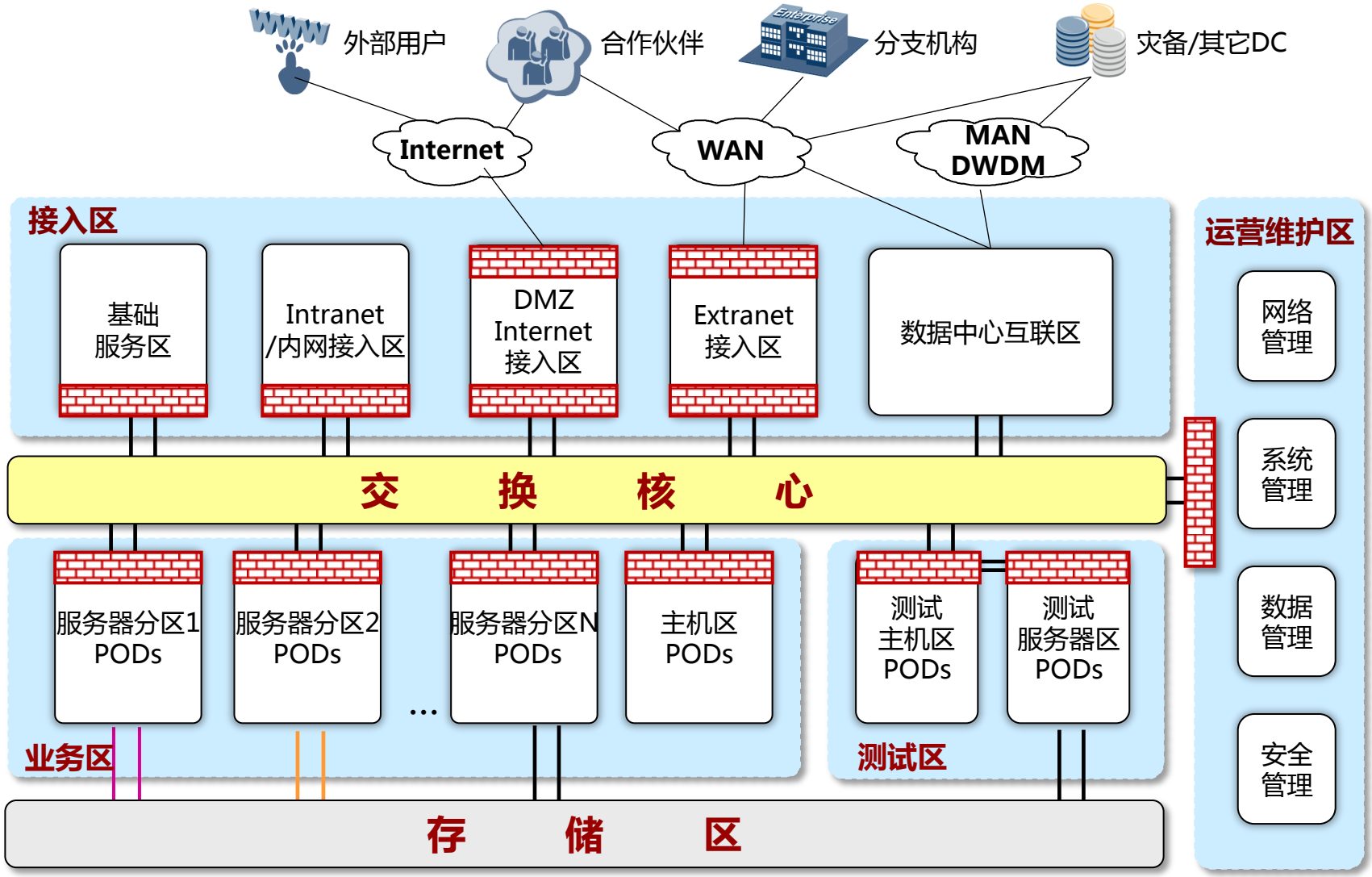
	模式A：按应用层次分区	模式B：按应用类型分区
部署说明	客户端到服务器的访问要经过三个区域 同一层服务器之间的互访不需要跨区域	客户端到服务器的访问只要经过一个区域 同一层服务器之间的互访需要跨区域
优点	每个区域只服务于应用逻辑中的一个层面（Web/App/DB) 应用层次之间物理分离	风险分散，一个区域内部故障或变更停机不会影响其他区域承载的业务 扩展性较强，当应用种类增加或者单个区域容量增加时，可以通过横向拆分扩容 可管理性强：便于故障定位和应急 低时延：同一应用各层服务器之间的流量在同一个区内
缺点	风险集中，一个区域内部故障或变更，会影响全部应用 扩展性较弱，服务器数量较多时，单个区域易达到容量上限 业务可管理性弱，不易进行故障定位和应急	应用层次之间无物理分离

分区部署要点

为了能够实现业务服务器的安全隔离、容量扩展和分类管理等需求，通常将业务区按应用层次、按应用类型两种模式细分。

两种模式各有优缺点，通常结合使用

数据中心典型分区


外部用户
合作伙伴
分支机构
灾备/其它DC
Internet
WAN
MAN
DWDM
接入区
基础
服务区
Intranet
/内网接入区
DMZ
Internet
接入区
Extranet
接入区
数据中心互联区
运营维护区
网络
管理
系统
管理
数据
管理
安全
管理
交 换 核 心
服务器分区1
PODs
服务器分区2
PODs
服务器分区N
PODs
主机区
PODs
测试
主机区
PODs
测试
服务器区
PODs
业务区
测试区
存 储 区

目录

典型业务与分区设计

业务与分区概述

典型业务与分区设计

服务器分区Server Farm

互联网分区 Internet

外联分区 Extranet

内部接入分区Intranet

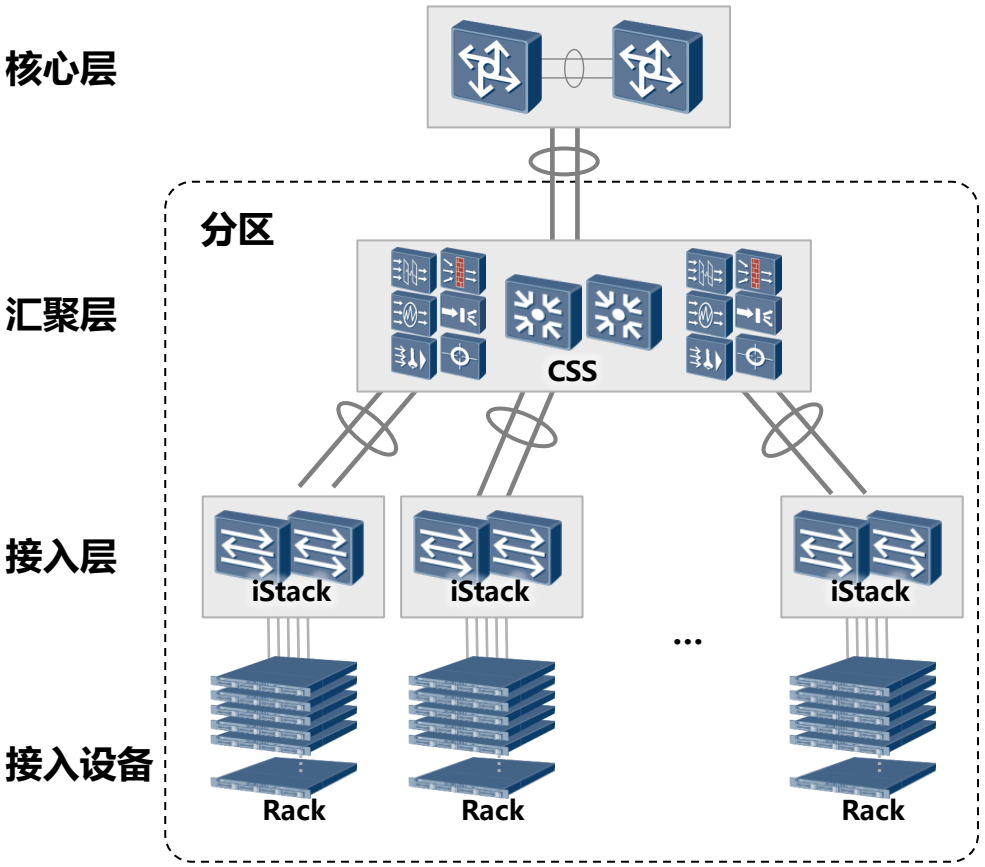
数据中心互联DCI

存储分区

管理分区

开发测试区

典型分区设计



目标

网络架构简单，易维护易部署，故障易隔离，容量易扩展，便于路由、流量、安全策略的配置

设计方法

层次化设计：每层功能清晰，架构稳定，易于扩展和易于维护

模块化设计：每个分区是一个模块，分区内部调整影响范围小，易于定位问题

冗余性设计：双节点适当冗余性提高可靠性

对称性设计：便于业务部署，拓扑直观，便于协议设计和分析

部署方式

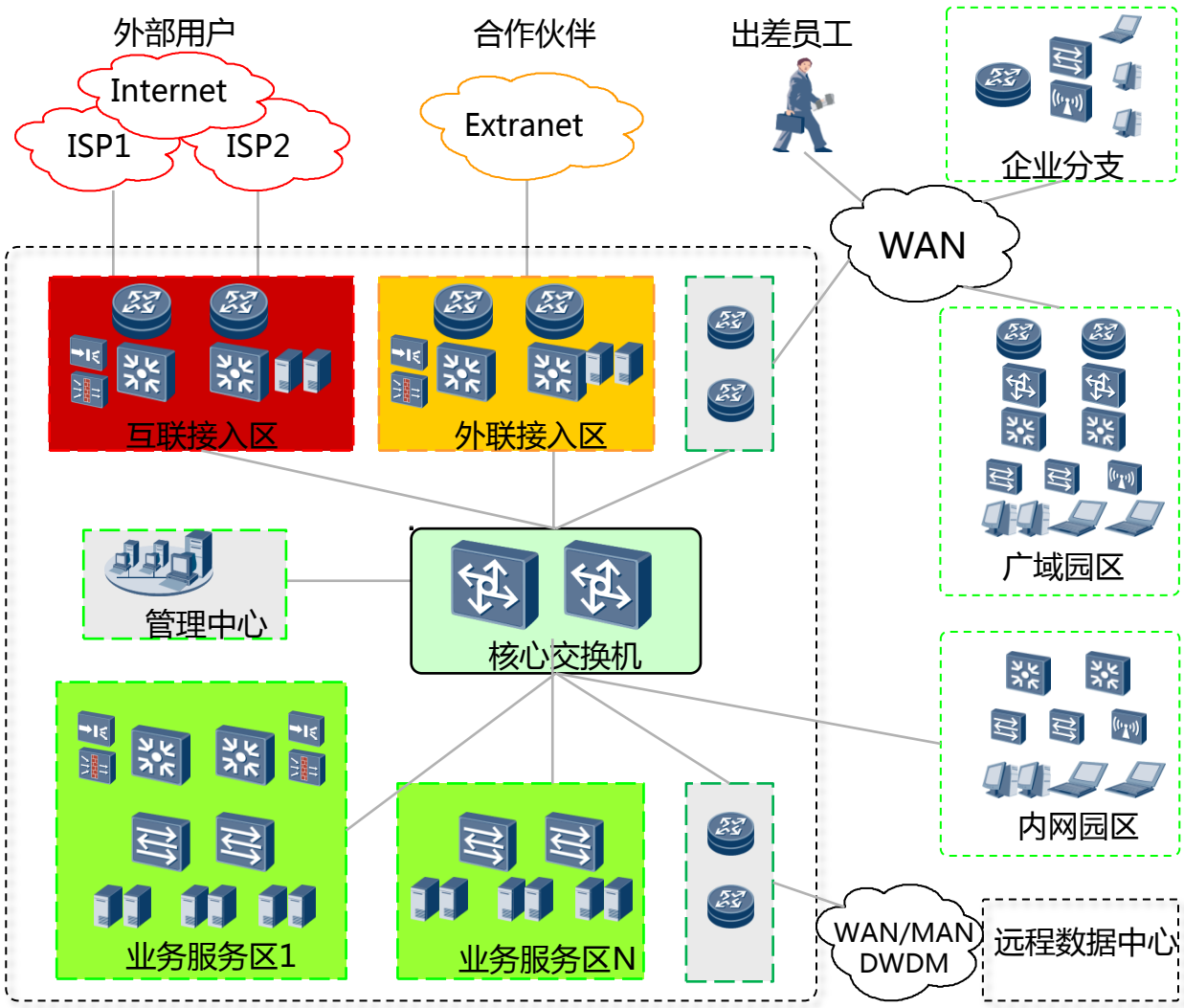
单层、EOR或TOR 2层星形结构

采用2层结构时部署跨设备捆绑或交换机集群技术，避免环路，STP 仍然部署，作为配置错误或误连等情况下的规避措施

采用旁挂功能模块的方式，提供防火墙等网络服务，高性能区域多采用机箱式防火墙

功能服务器区的物理布局设计建议:参考TIA942数据中心布局设计

数据中心分区安全设计



分区安全等级：

企业分支	高
广域园区	高
内网园区	高
出差员工	较高
合作伙伴	中
Internet用户	低

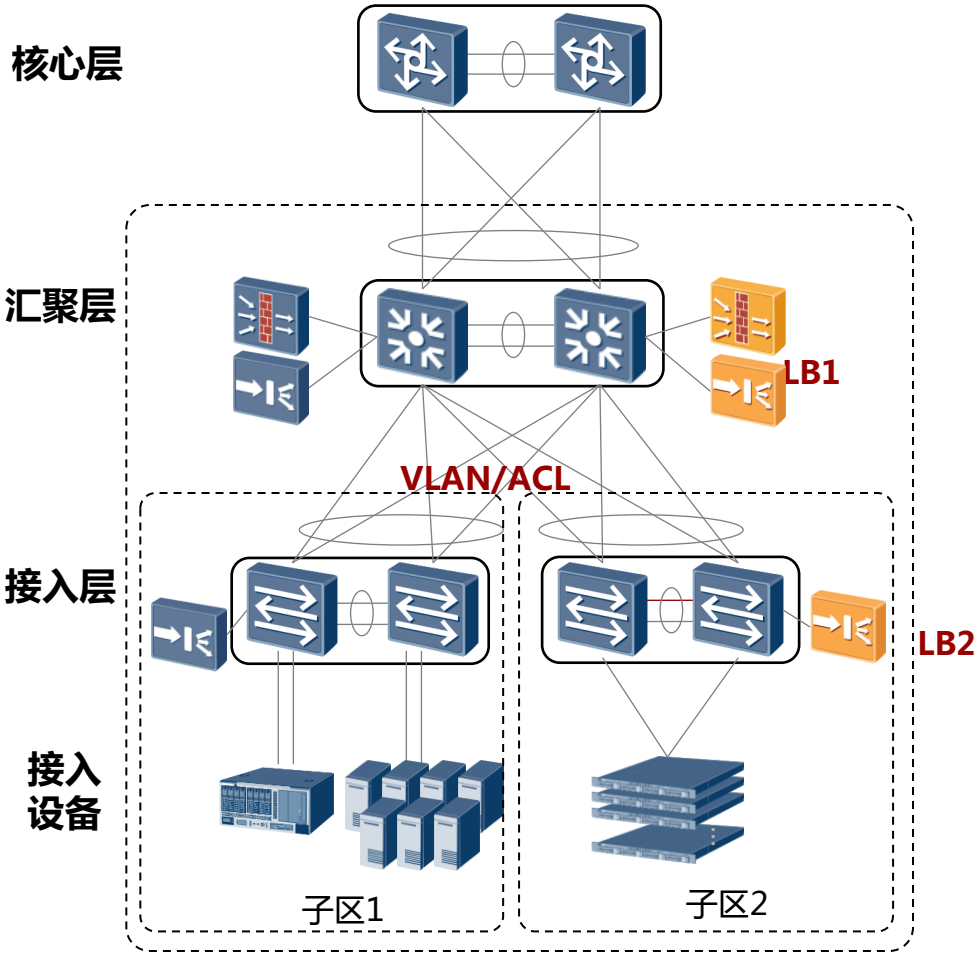
互联网客户最不可信，单独有互联业务区对应。

合作伙伴可信度居中，企业的中心仅开放部分业务给合作伙伴，部署Extranet Server区

企业分支和出差员工，根据访问方式的不同，给予不同的业务范围。

内部园区和广域园区都是企业的内部，可信度最高，根据不同部门和业务，访问数据中心的不同业务服务区。

服务器区设计



目标

服务器区提供各种类型服务器接入，并支持服务器的自身容错功能

部署防火墙确保服务器安全

部署负载均衡提升服务器的访问效率

方案

汇聚设备配置VLAN/ACL对分区内不同业务进行隔离。

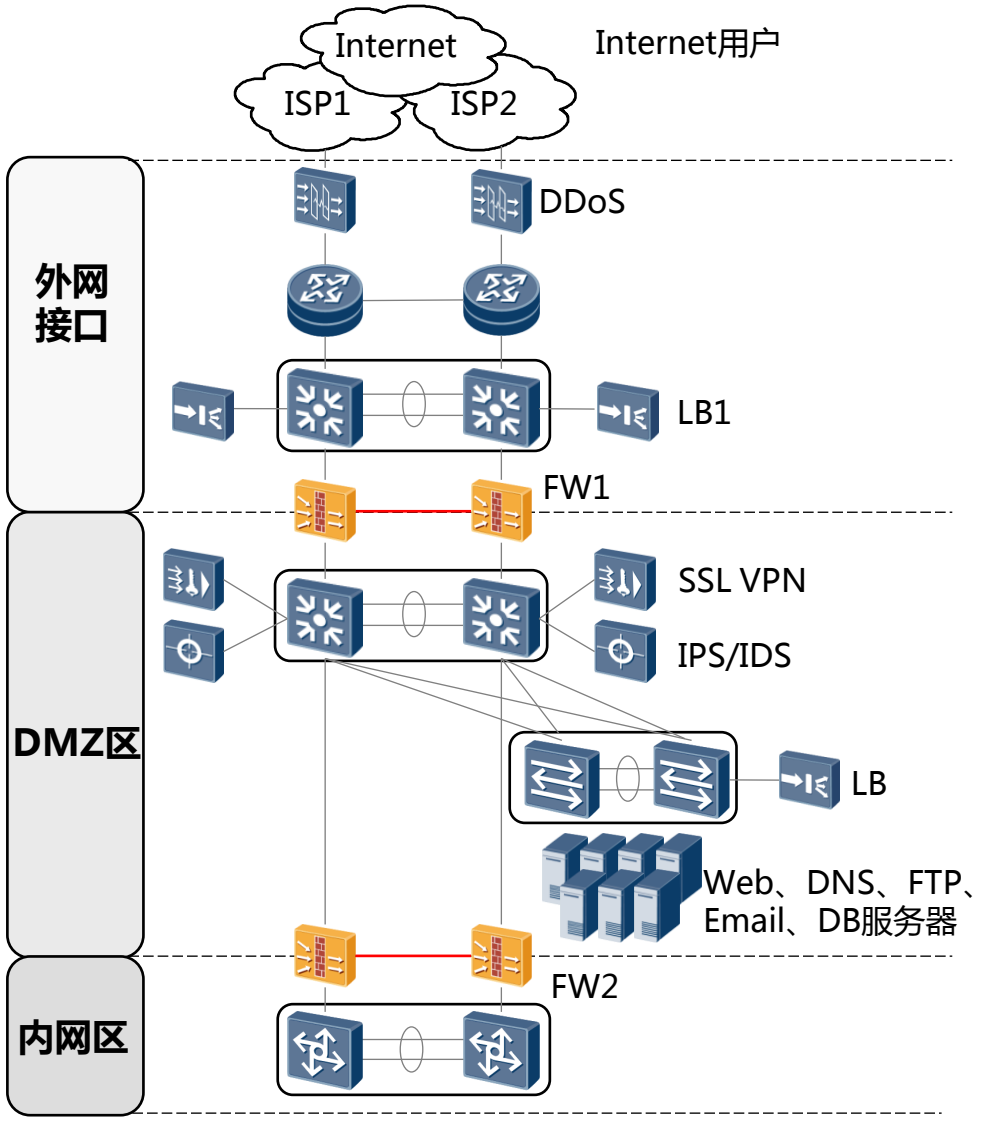
汇聚层采用旁挂方式，布署高性能防火墙，可以是框式设备或者防火墙集群。

LB1负责整 个分区内应用负载均衡。

LB2在子区内（可选），为区域内应用提供负载均衡。

可选配署NetStream,实现流量分析和管理。

互联网接入区设计



目标

部署丰富的安全控制机制，防范网络攻击等，实现Internet高风险区域客户的应用访问

部署LB，加快业务访问，提升体验

方案

DDoS 设备选择旁挂或串接方式，旁挂能够减少设备数量，消除单点故障，增强业务可靠性；DDoS 串接方式可采用镜像方式和分光器方式

防火墙1串行接入，双机热备部署，抗攻击能力强.对外网进行第一层隔离

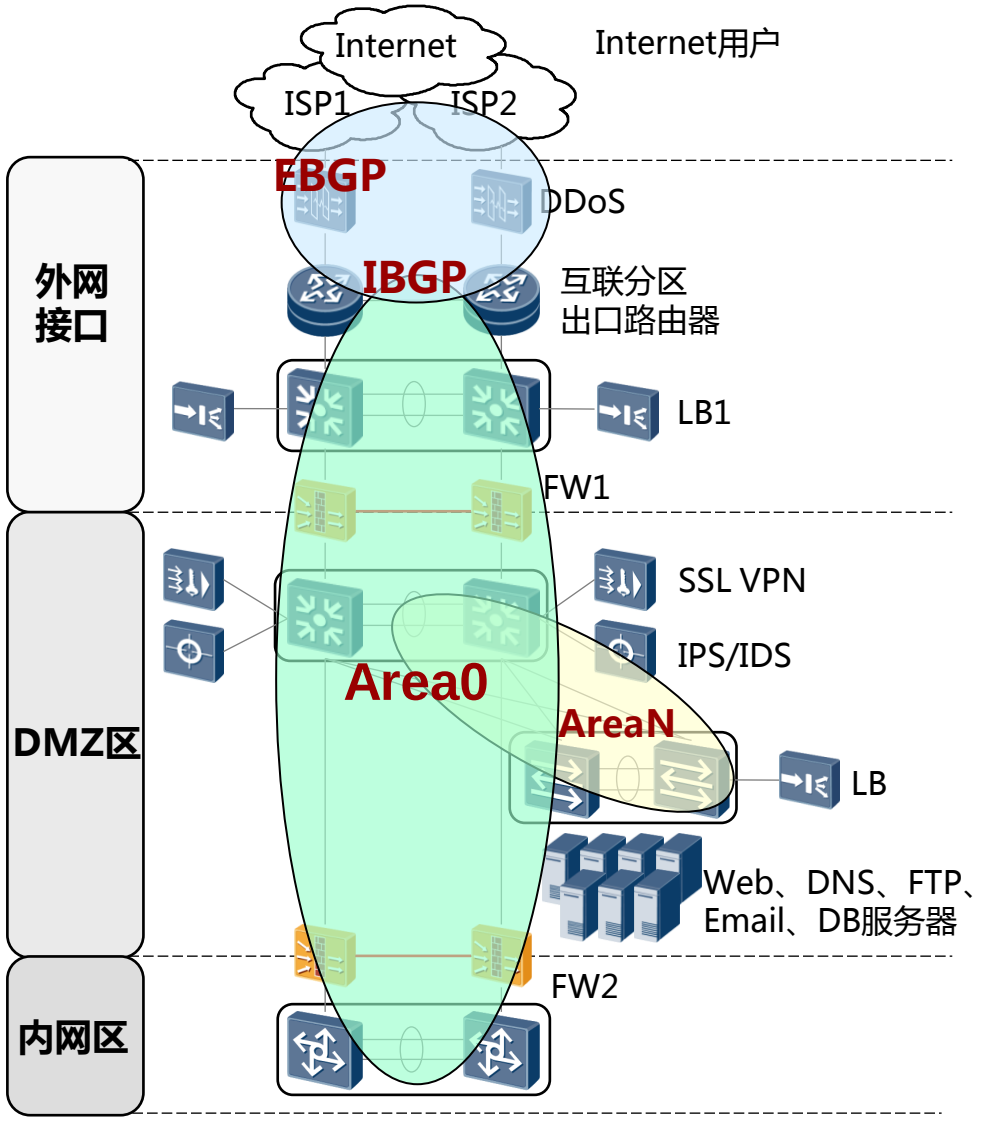
IDS/IPS设备接到防火墙内侧，既进行入侵检测，又可以避免误报。

SSL VPN 设备负责进行隧道终结

LB1 能实现全局负载均衡(可选);

防火墙2串行接入，双机热备部署，抗攻击能力强.对外网进行第二层隔离.提高安全性.同时将DMZ 与核心区隔离.

互联网分区路由设计（一）



场景

大型数据中心，互联网业务出口精确选择

方案

大型的数据中心出口路由器与运营商建立EBGP邻居

出口路由器部署IBGP，在IBGP上部署丰富的策略路由实现对互联网业务的精确选择

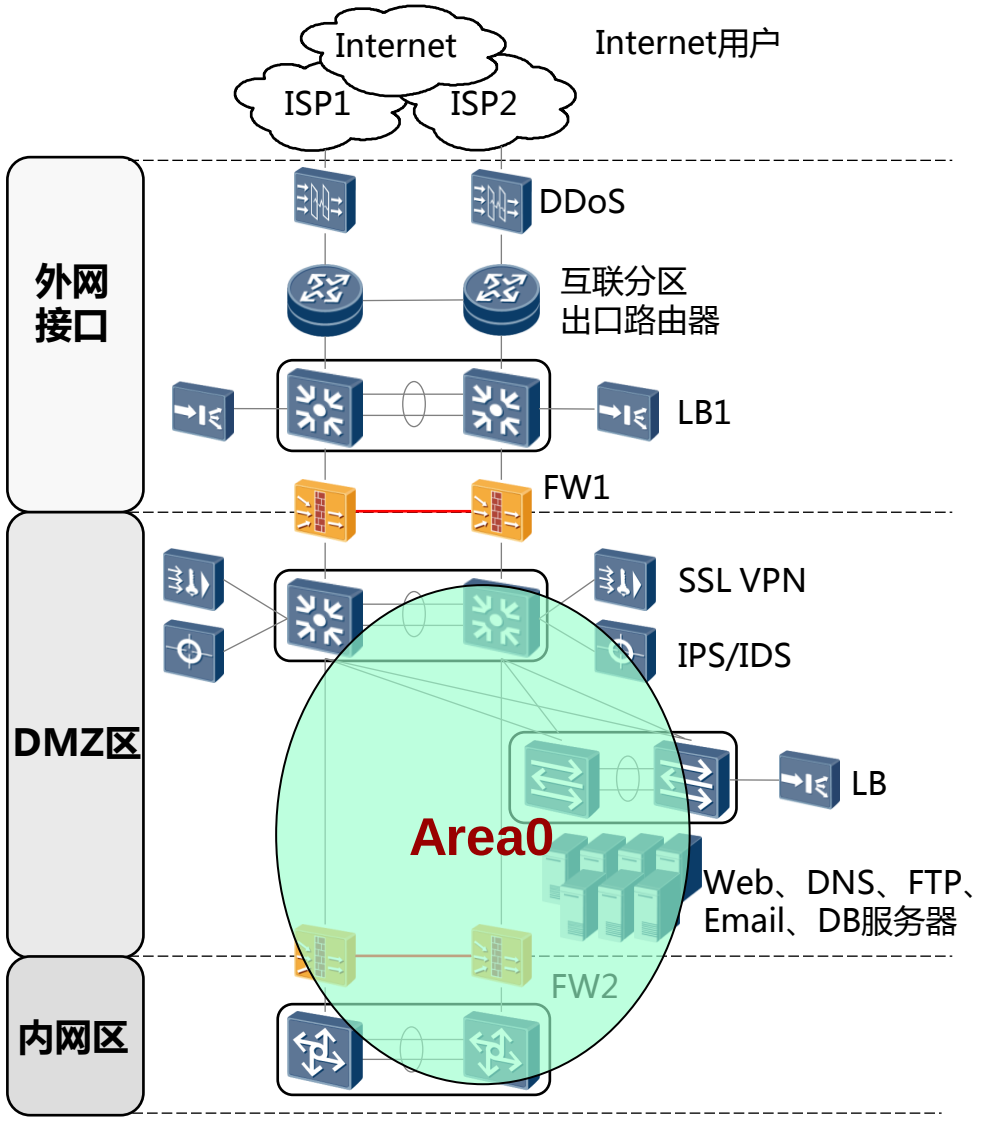
OSPF作为IGP协议，提供整网连通性

出口路由器内联接口配置OSPF

出口路由器向OSPF发布默认数由

这种路由设计适合DMZ为公网IP地址的情况，或者在LB上做NAT的情况

互联网分区路由设计（二）



场景

中小型数据中心，互联网业务出口精确选择

方案

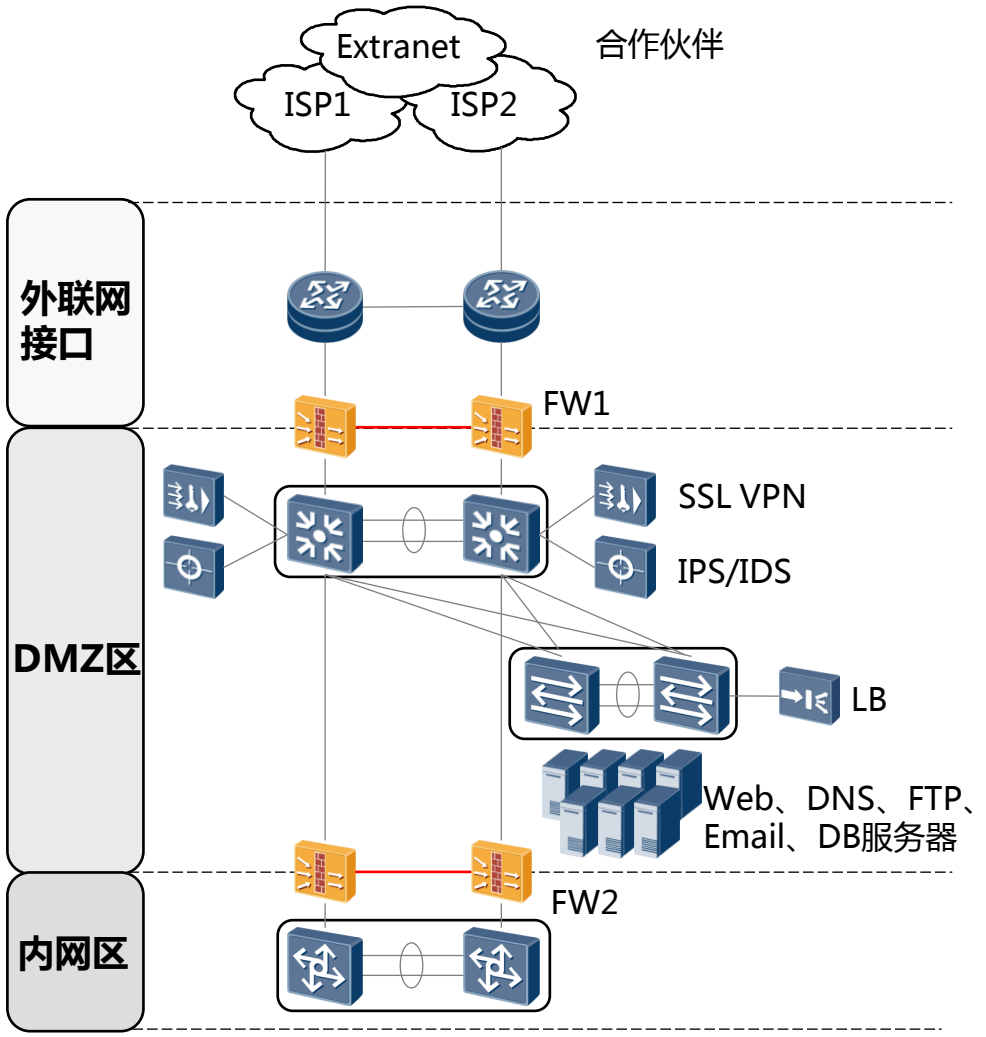
中小型的数据中心出口路由器与运营商使用静态路由

OSPF作为IGP协议，提供整网连通性

DMZ区域和内网接入区使用OSPF

FW1上做NAT，并且做为内外网分界，和FW1相连的设备：出口路由器和三层交换机需要配置静态路由

外联网出口区设计



目标

外联网出口提供企业与合作伙伴的业务系统连接，部署适当的安全策略，确保开放给合作伙伴的业务的安全访问

部署LB，加快业务访问，提升体验

部署要点

防火墙1串行接入，双机热备部署，抗攻击能力强.对外网进行第一层隔离

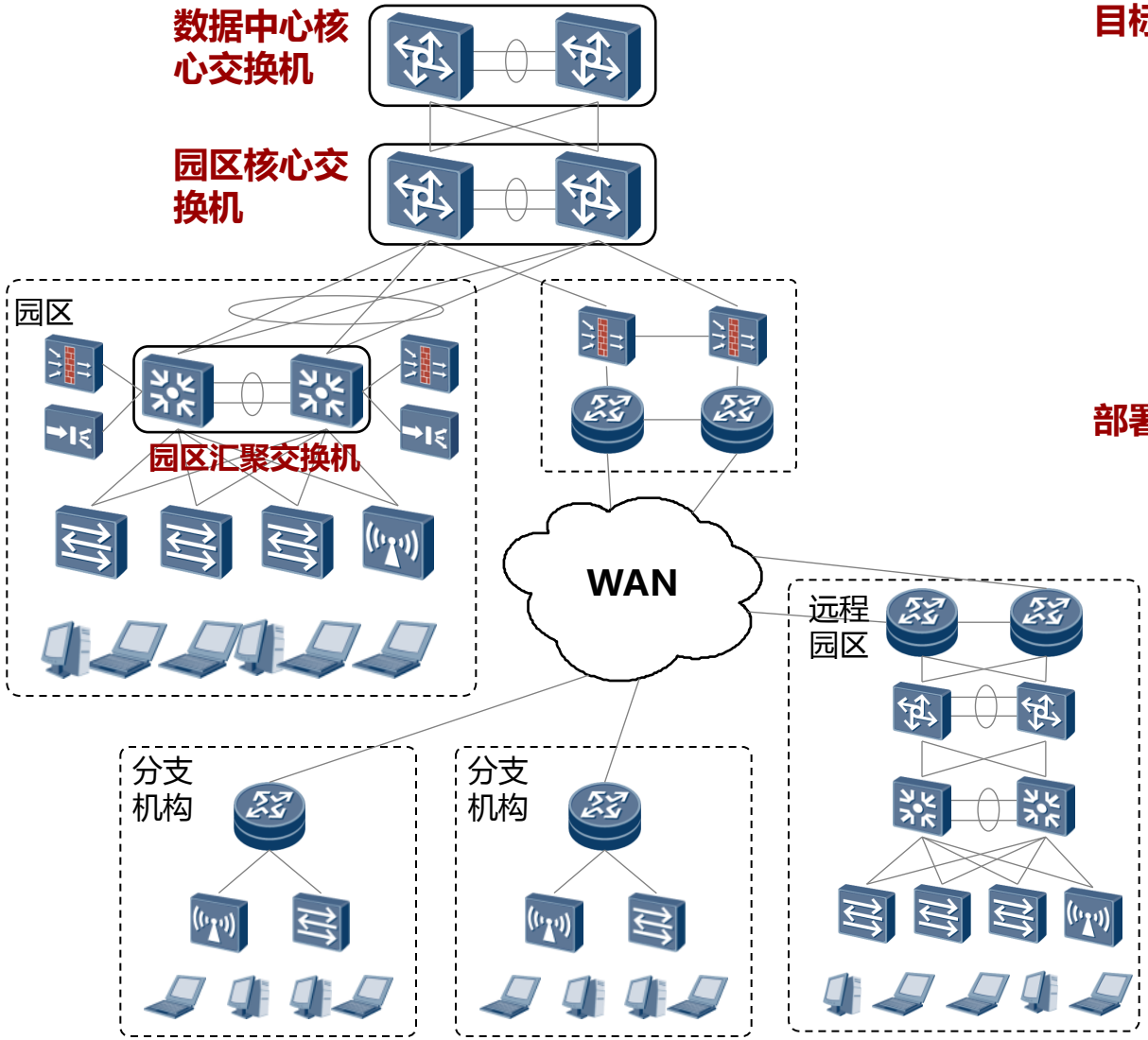
IDS/IPS设备接到防火墙内侧，既进行入侵检测，又可以避免误报。

SSL VPN 设备负责进行隧道终结

LB能实现全局负载均衡(可选);

防火墙2串行接入，双机热备部署，抗攻击能力强.对外网进行第二层隔离.提高安全性.同时将DMZ 与核心区隔离.

内网接入区设计



目标

内网接入区为内网用户提供接入数据中心的功能

本地园区网LAN接入数据中心，远程分支和远程园区通过WAN接入

使用防火墙解决内网用户非法访问问题。

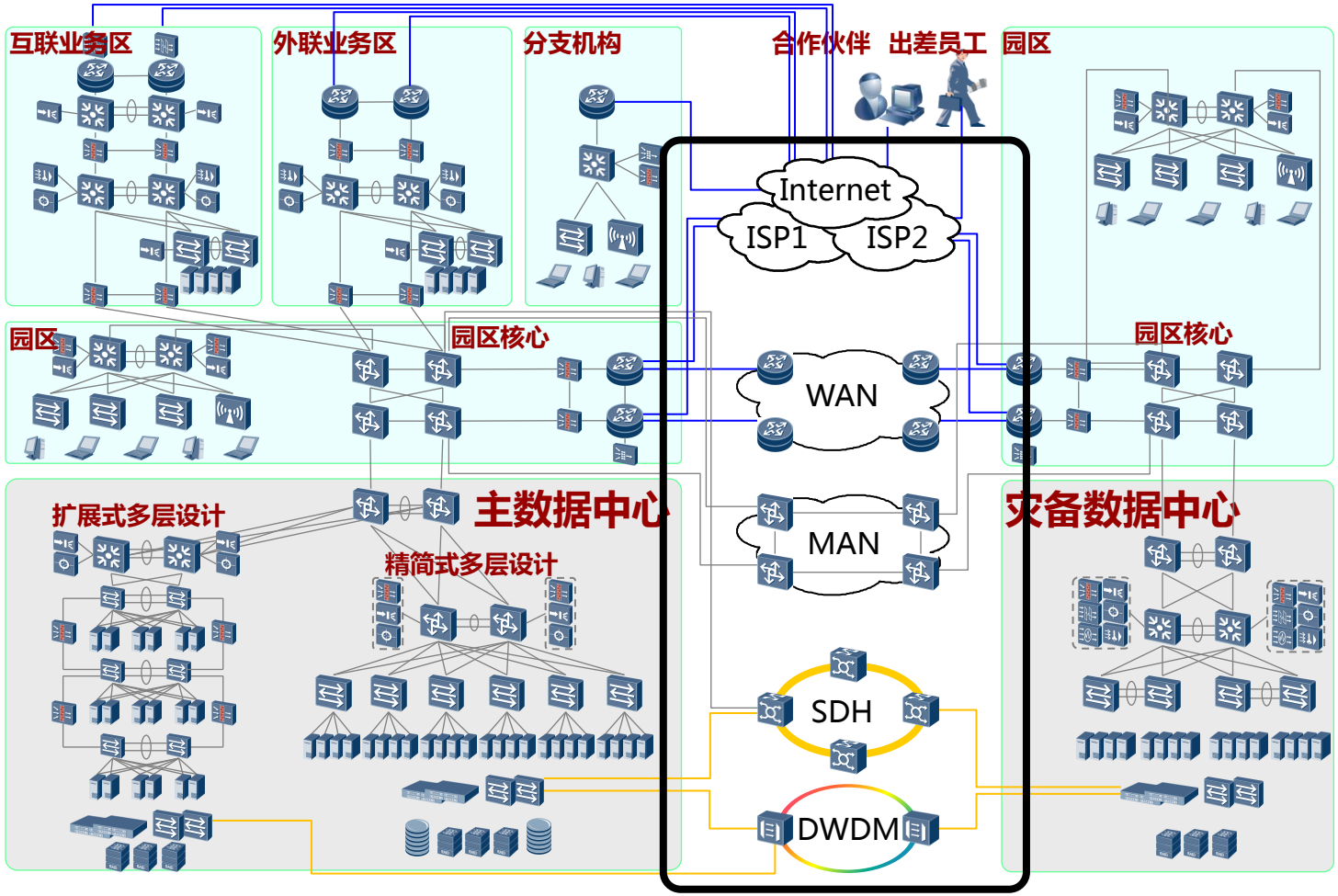
部署要点

防火墙可采用串接或者旁挂方式，双机热备部署，使核心区和内网用户隔离。抗攻击能力强

汇聚层旁挂LB，实现负载均衡和优化带宽管理.

低级别用户接入数据中心，可在园区的汇聚层适当部署防火墙

数据中心网络互联区域设计



目标

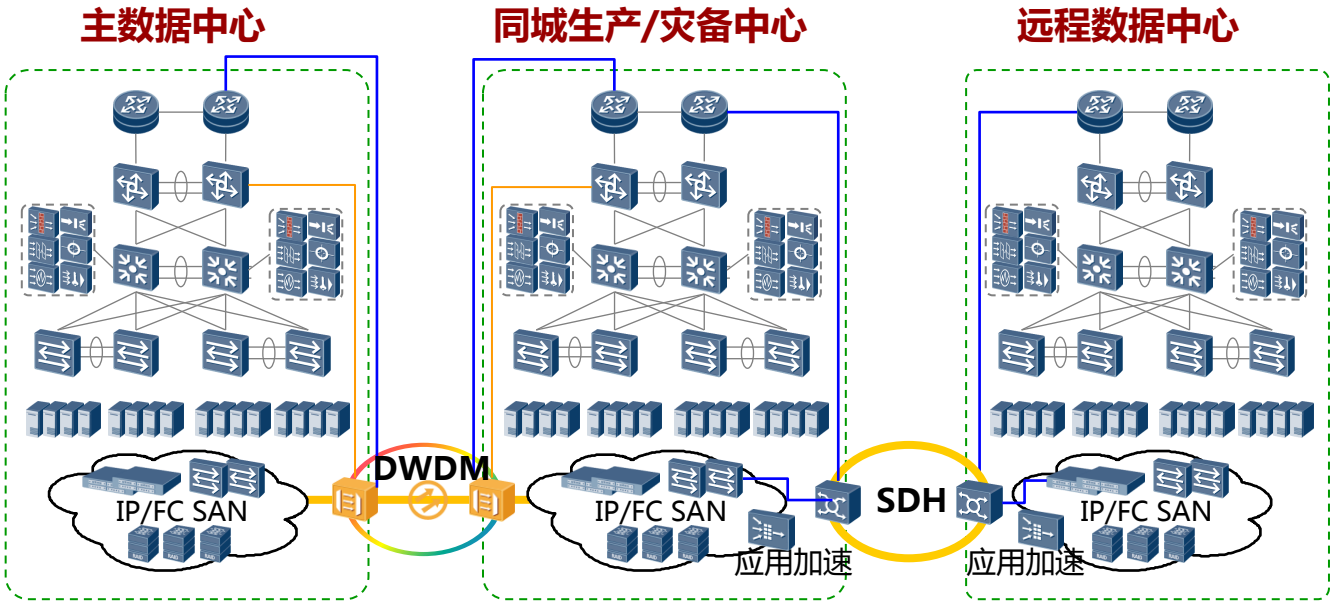
通过网络将跨不同地域的数据中心连接起来，实现数据中心之间资源的整合、池化和调度

可以多种互联方式结合

互联方式

- DWDM光纤互联
- SDH专线互联
- 城域承载网
- 自建WAN
- 租用运营商MPLS/IP网络
- Internet

数据中心互联区域设计：DWDW+SDH网络

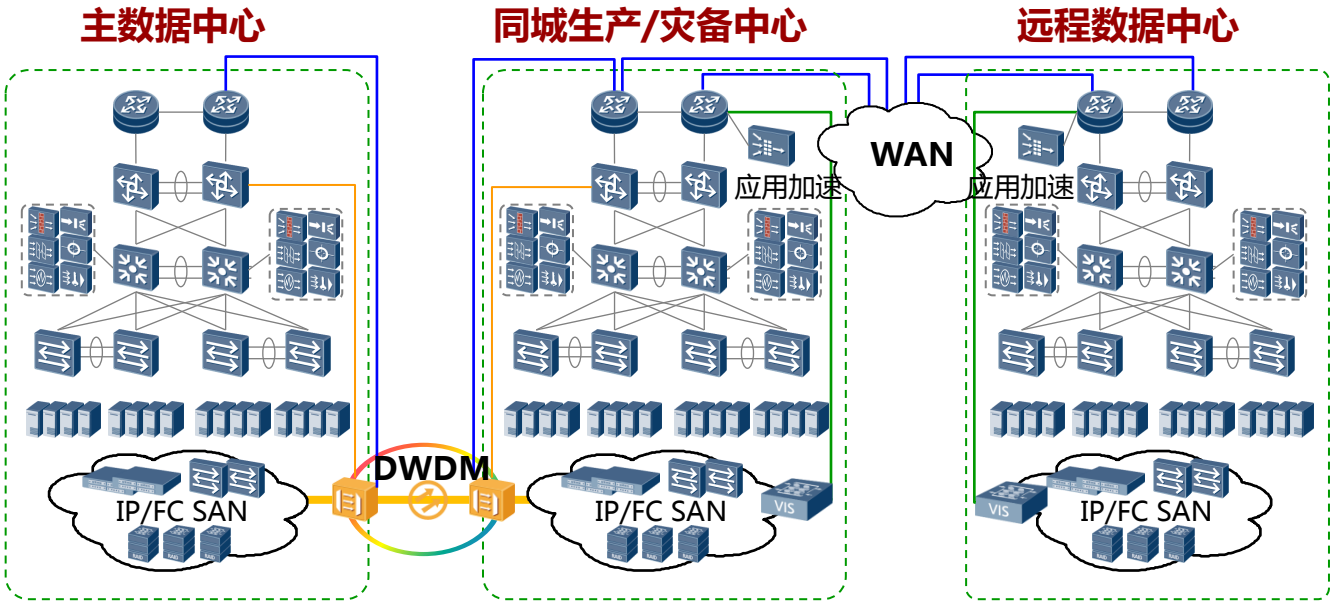


解决方案

OTN设备主要用于同城数据中心通过DWDM互联，可以承载IP，以太，FC存储等多业务

SDH设备用于数据中心与远程数据中心互联，可以选择在路由器上使用POS接口直接连接同城数据中心高可靠

数据中心互联区域设计：DWDW+WAN



解决方案

OTN设备主要用于同城数据中心通过DWDM互联，可以承载IP，以太，FC存储等多业务

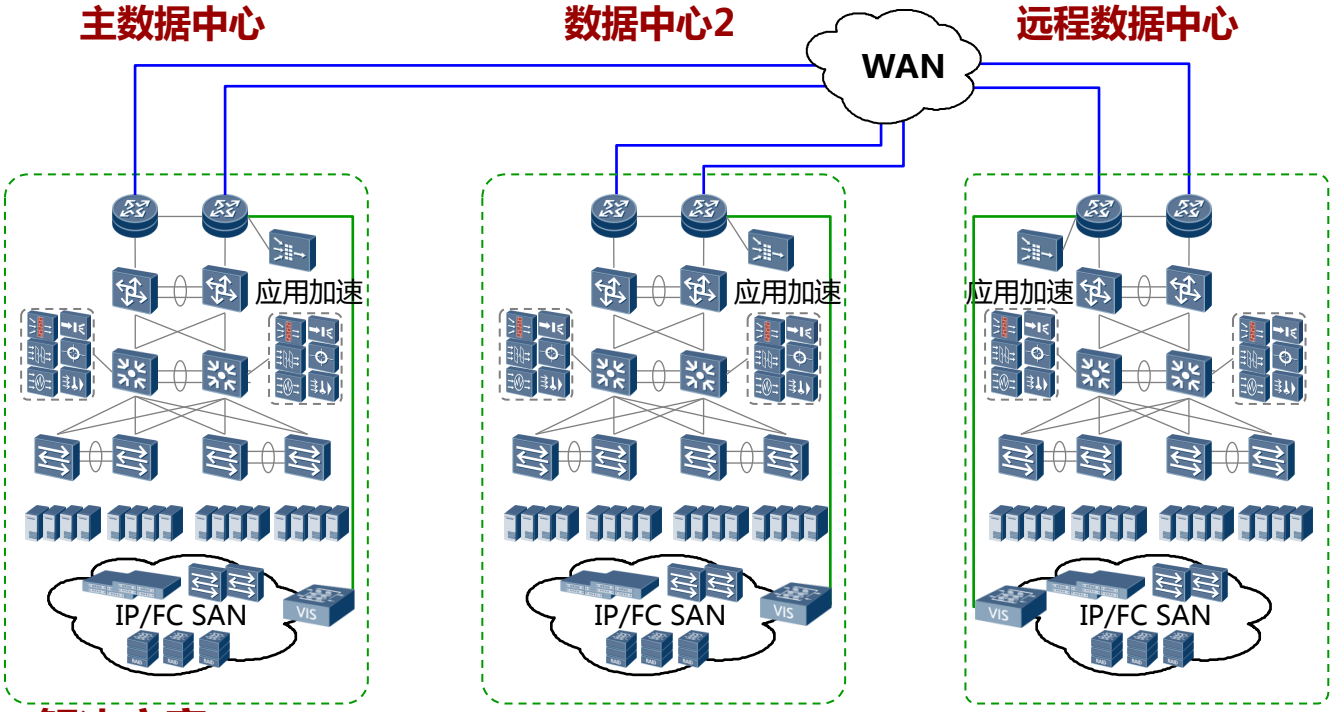
远程数据中心间通WAN连接

FC存储异步复制由中间设备转换(如VIS6000)

远程t同步复制通过服务器实现如（ NBU等 ）

路由器通过MPLS L3 VPN实现多业务隔离

数据中心互联区域设计：WAN



解决方案

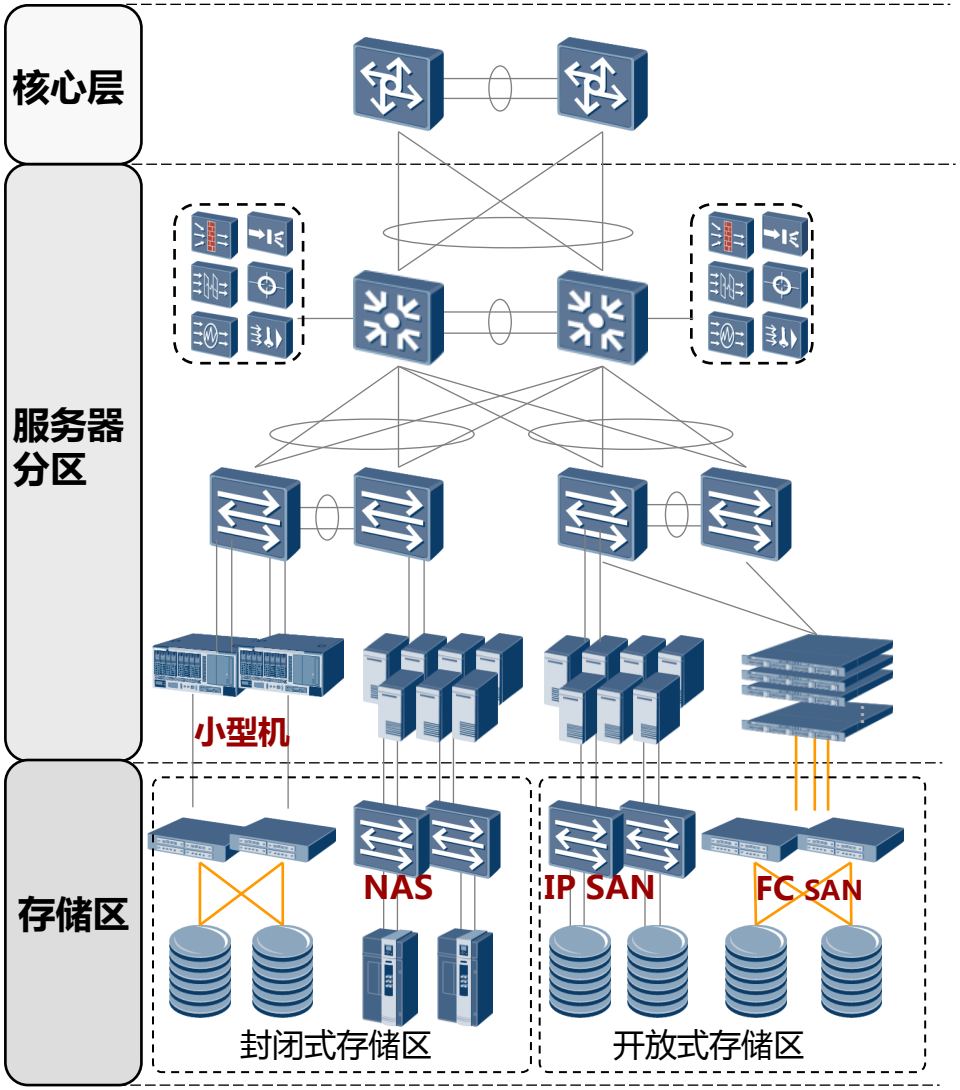
路据中心间通过专线连接

FC存储异步复制由中间设备转换(如VIS6000)

远程同步复制通过服务器实现（如NBU）

路由器通过MPLS L3 VPN实现多业务隔离

存储区设计



目标

数据中心普遍采用集中式存储管理模式。存储设备和服务器之间通过直接的高速网络联结，实现存储共享，备份，和容灾

部署要点

存储区依据服务器和操作系统的不同划分为封闭存储区和开放式存储区。

开放式存储区依据网络传输协议分为 NAS 和 SAN.

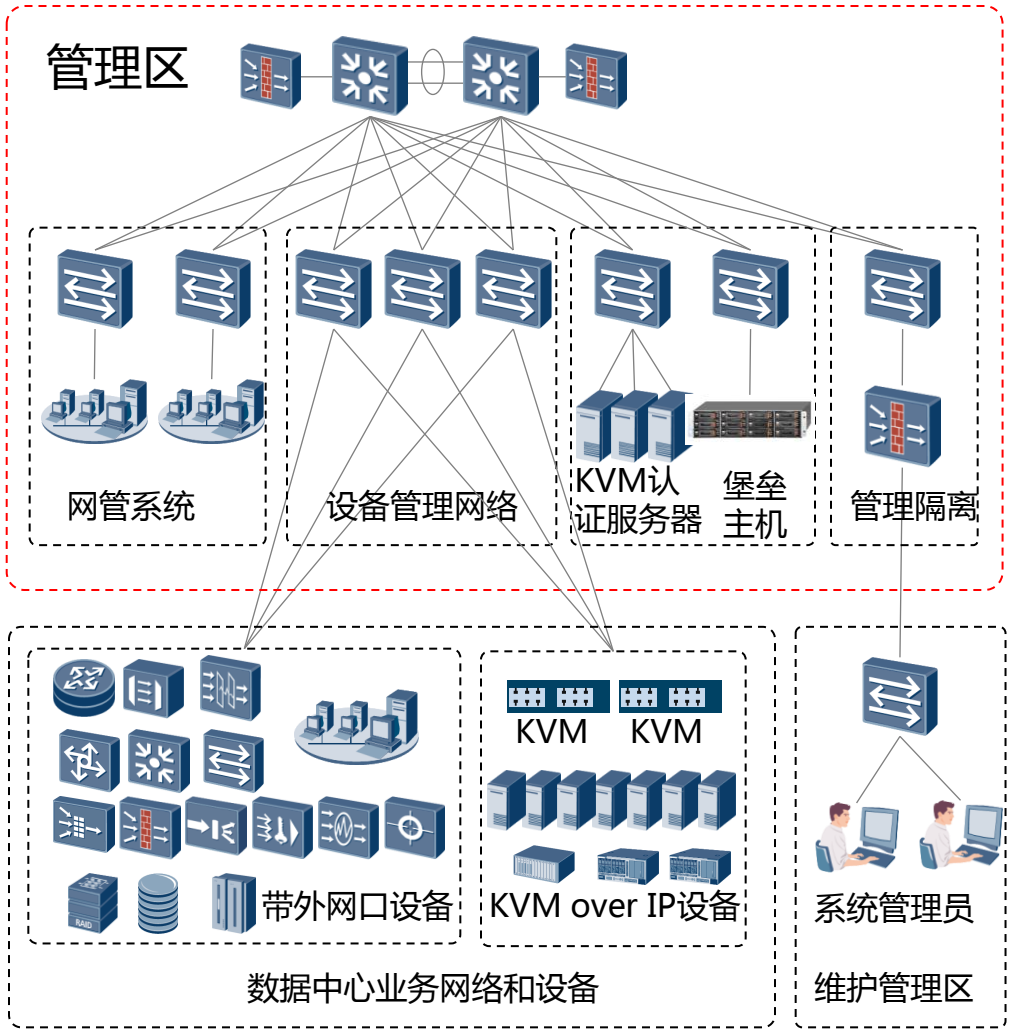
开放式存储区的集中存储池可以按服务等级分类。

IP存储区，可以通过目前运营商的MPLS VPN或者VPLS虚拟专线，实现主备两个数据中心之间的互通。

SAN存储区，可以采用裸光纤甚至DWDM，提供主备数据中心之间高速、低时延的互联互通，以满足存储数据的准实时备份需求。

.

管理区带外网络设计



目标

管理区负责数据中心的日常运维工作。管理网络分为带内网络和带外网络。

带外网络与数据中心的业务网络完全隔离，保证管理的可靠性，是优选方案。

管理区网络设备之间建议采用百兆互连

数据中心的管理建议使用带外网管。

部署要点

独立管理区域，网络设备可用带外网口，运行网管协议 实现网络管理、数据收集和实时监控 功能.

采用“堡垒主机”的方案， 通过KVM 转换器，客户端与服务器之间只传递键盘、鼠标和荧屏变化等交互信息，没有实际的业务数据流到客户端

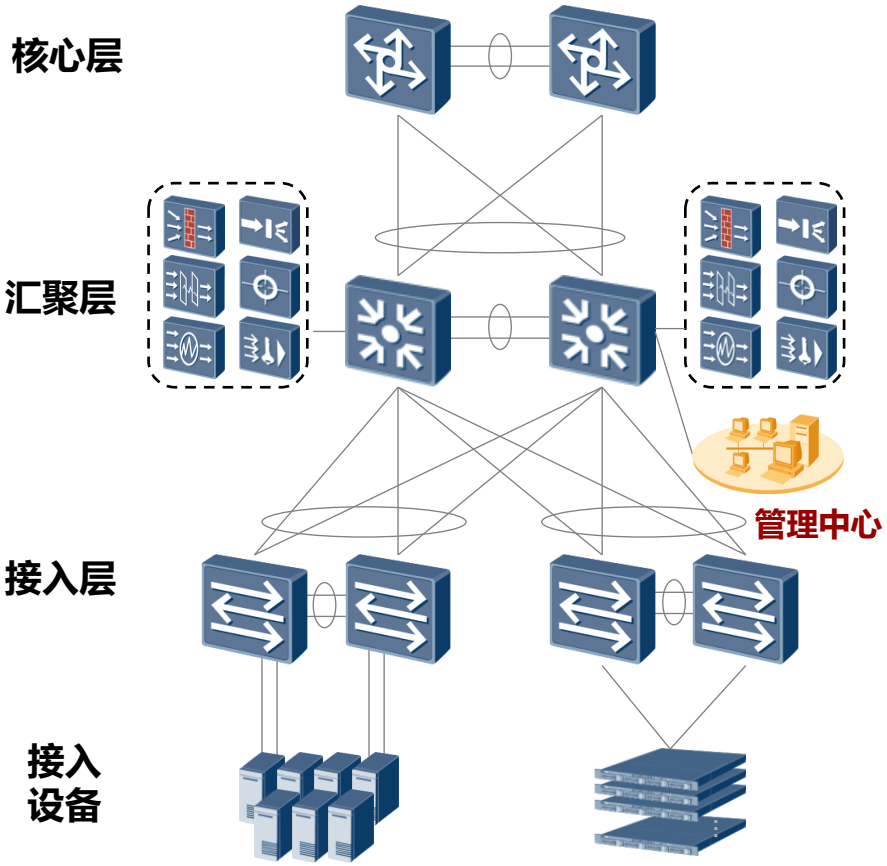
客户端看到的只是服务器上应用运行的显示映像，避免跨域传输实体数据，提升跨域访问安全性

系统管理员可远程控制服务器，实现无人机房管理

KVM 认证服务器根据管理员的分工不同，授予其不同的访问权限，从而限制其访问不同的设备.

汇聚层接入防火墙,抗攻击能力强

管理区带内网络设计



目标

带内网络是指网管系统利用现有业务网络进行管理、数据收集和实时监控等工作。

网管和业务不分离

部署要点

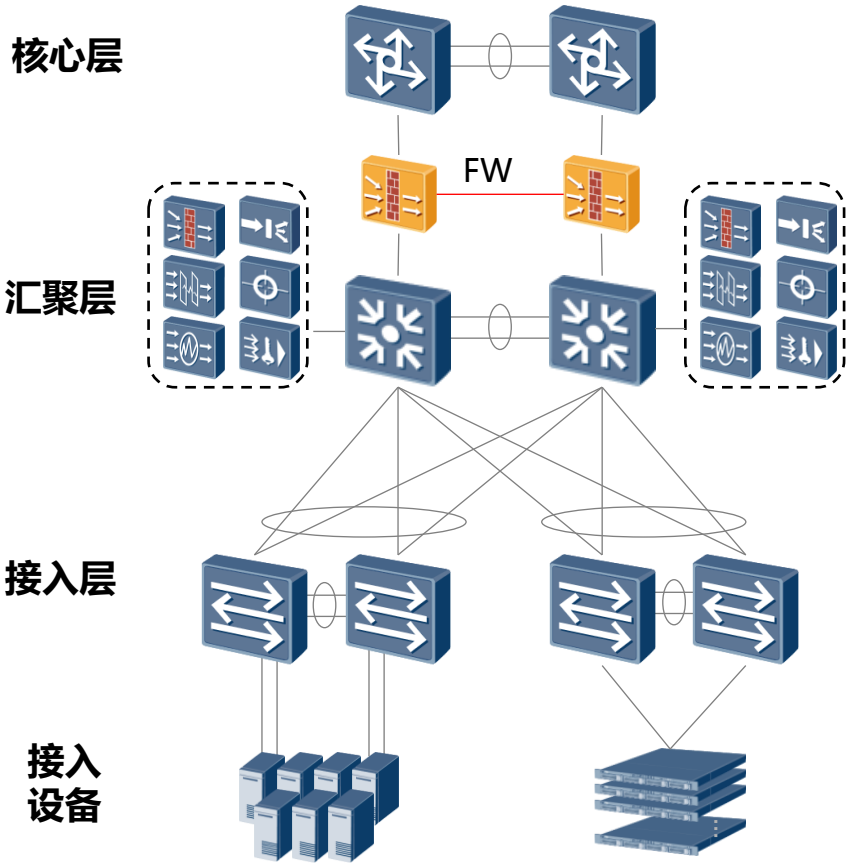
系统管理员使用RDP、VNC、Telnet、SSH、plsql、sqlplus、FTP、SFTP、Http、Https等传统手段管理服务器

不同的服务器运行不同的操作系统，管理手段不一，访问方式不同，运维复杂，工作量大。

网络管理与业务流量叠加在一起，增加了网络规划的难度。管理的可靠性和业务的持续稳定运行可能相互影响

带内管理虽然不需要增加KVM 等硬件设备，但网络规划难度大，运维复杂。

开发测试区设计



目标

测试区对新业务，组网和设备进行功能和性能的验证

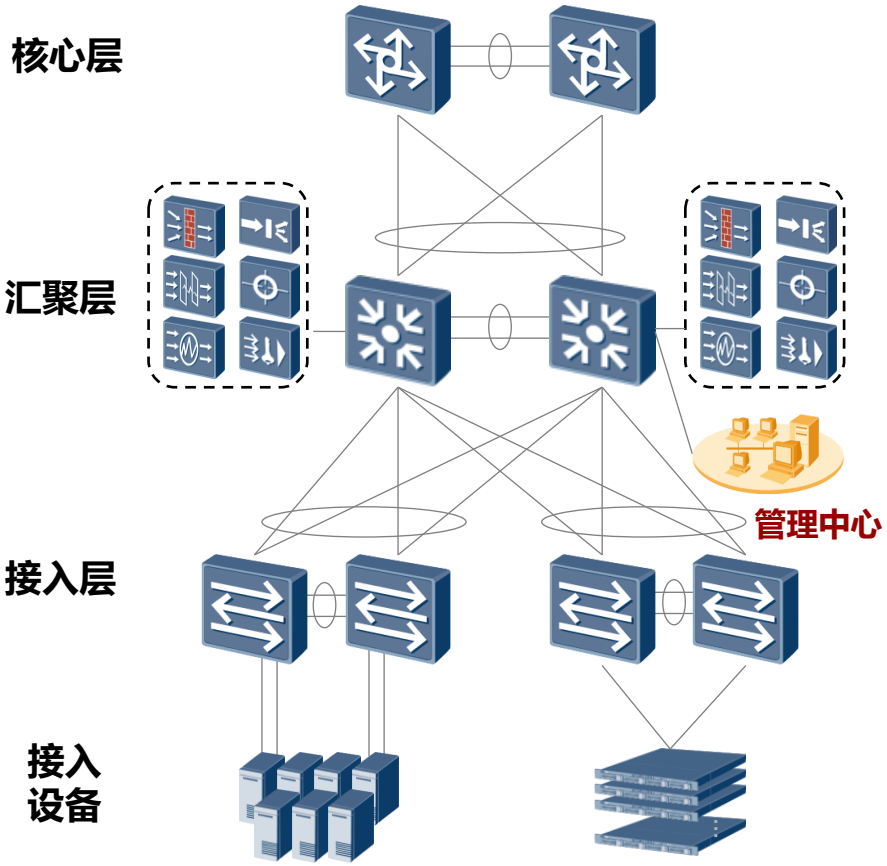
部署要点

防火墙采用串接方式，双机热备部署，使测试区和核心区隔离，抗攻击能力要求高。

测试区搭建二三层网络环境,并接入服务器,模拟现网进行业务功能验证.

汇聚层旁挂防火墙、负载均衡等各种业务设备，可调节验证网络性能.

管理区带内网络设计



目标

带内网络是指网管系统利用现有业务网络进行管理、数据收集和实时监控等工作。

网管和业务不分离

部署要点

系统管理员使用RDP、VNC、Telnet、SSH、plsql、sqlplus、FTP、SFTP、Http、Https等传统手段管理服务器

不同的服务器运行不同的操作系统，管理手段不一，访问方式不同，运维复杂，工作量大。

网络管理与业务流量叠加在一起，增加了网络规划的难度。管理的可靠性和业务的持续稳定运行可能相互影响

带内管理虽然不需要增加KVM 等硬件设备，但网络规划难度大，运维复杂。

Huawei Enterprise A Better Way