

XXX科技数据 中心改善方案

etonnet.com.cn

一通科技

设计目标

etonnet.com.cn

数据中心

网络架构

系统架构

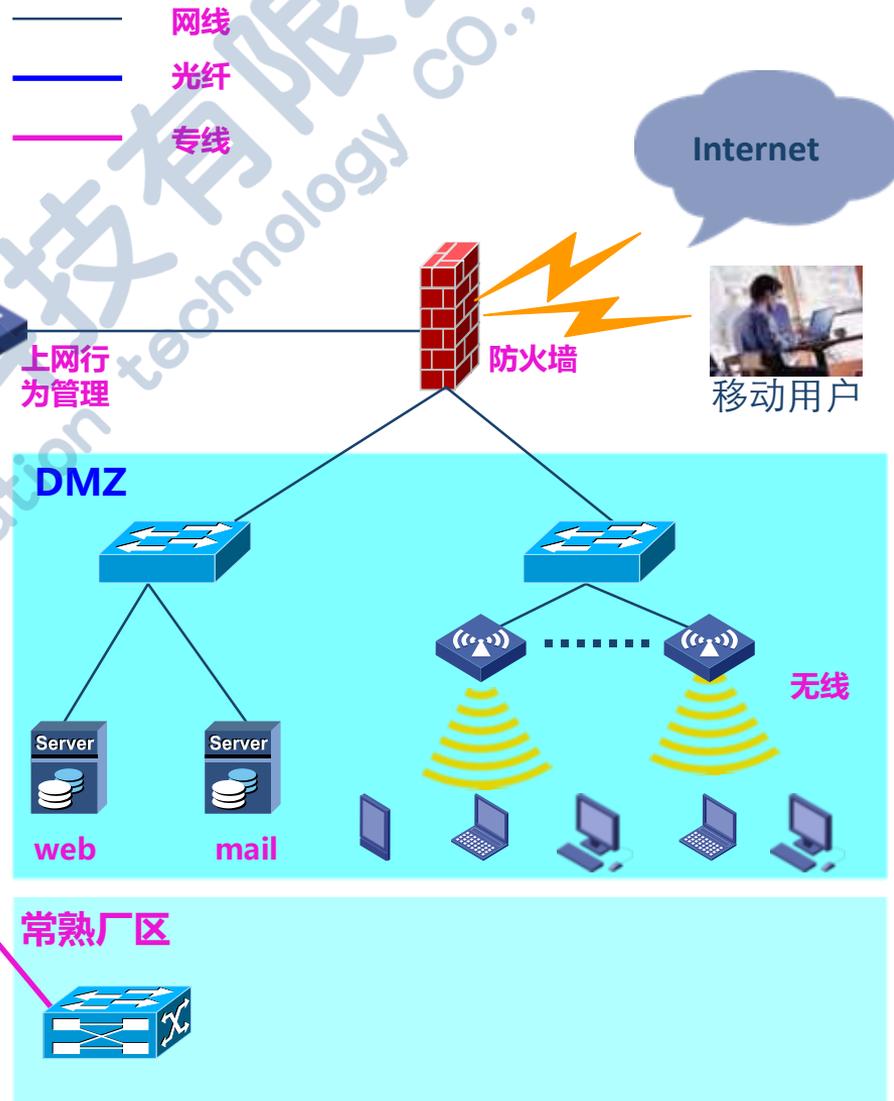
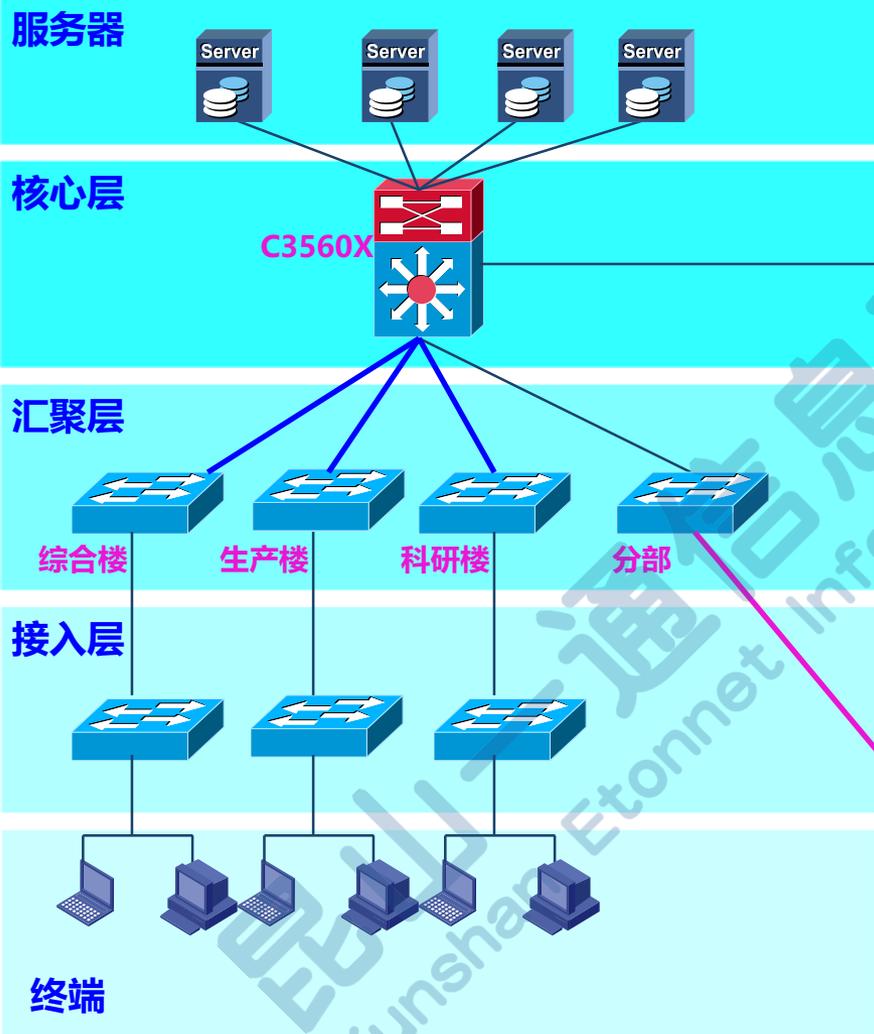
安全架构

基础架构

网络架构

etonnet.com.cn

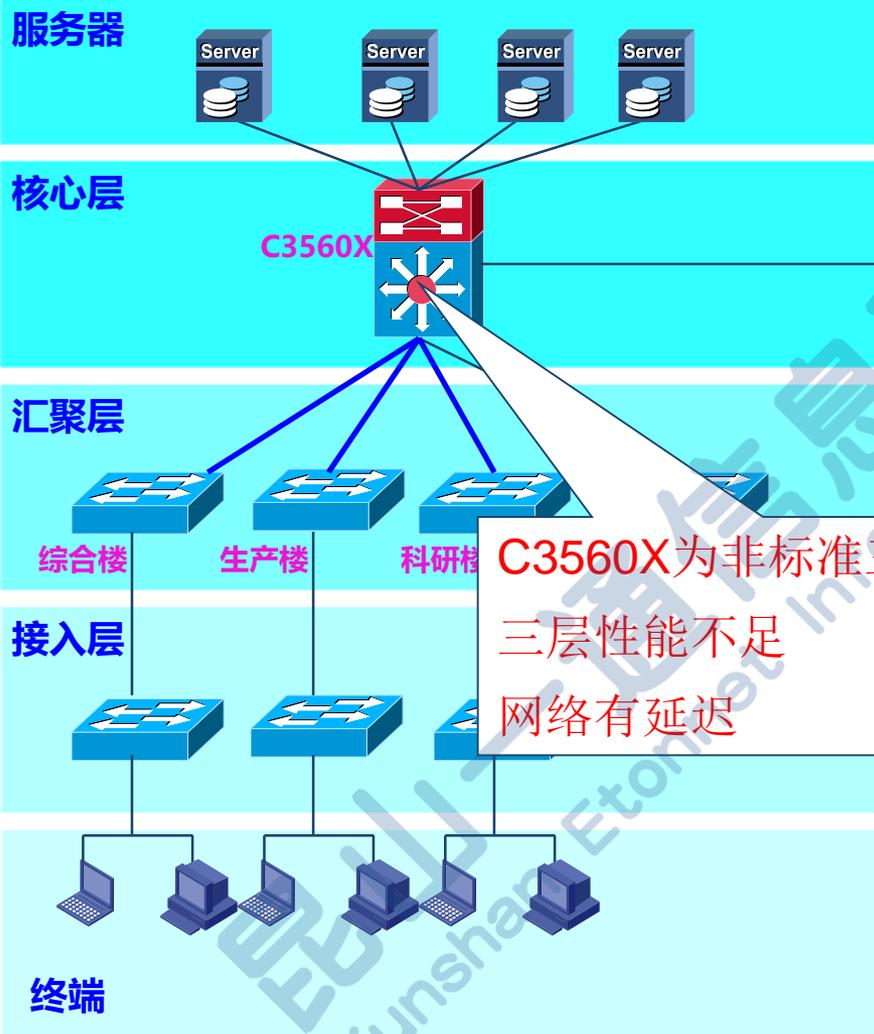
目前网络架构



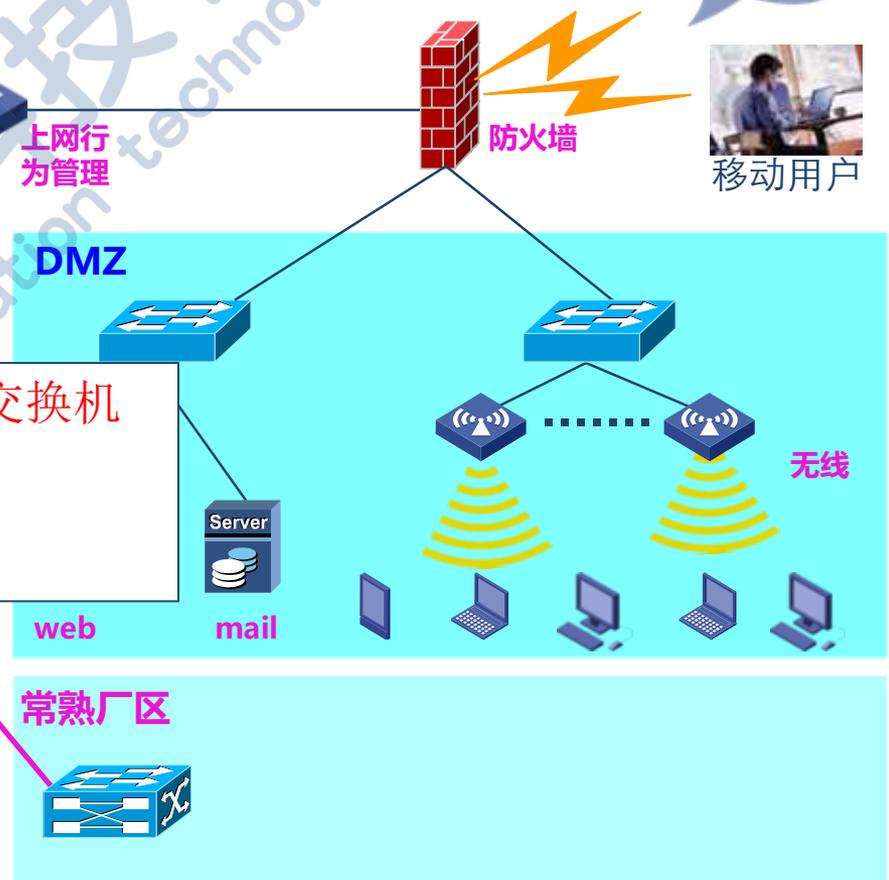
网络架构

etonnet.com.cn

问题一



- 网线
- 光纤
- 专线



网络架构

etonnet.com.cn

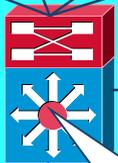
解决方案

服务器



核心层

C3850



汇聚层



接入层



终端



- 网线
- 光纤
- 专线

上网行为管理

防火墙

Internet



DMZ



web

mail

无线



常熟厂区



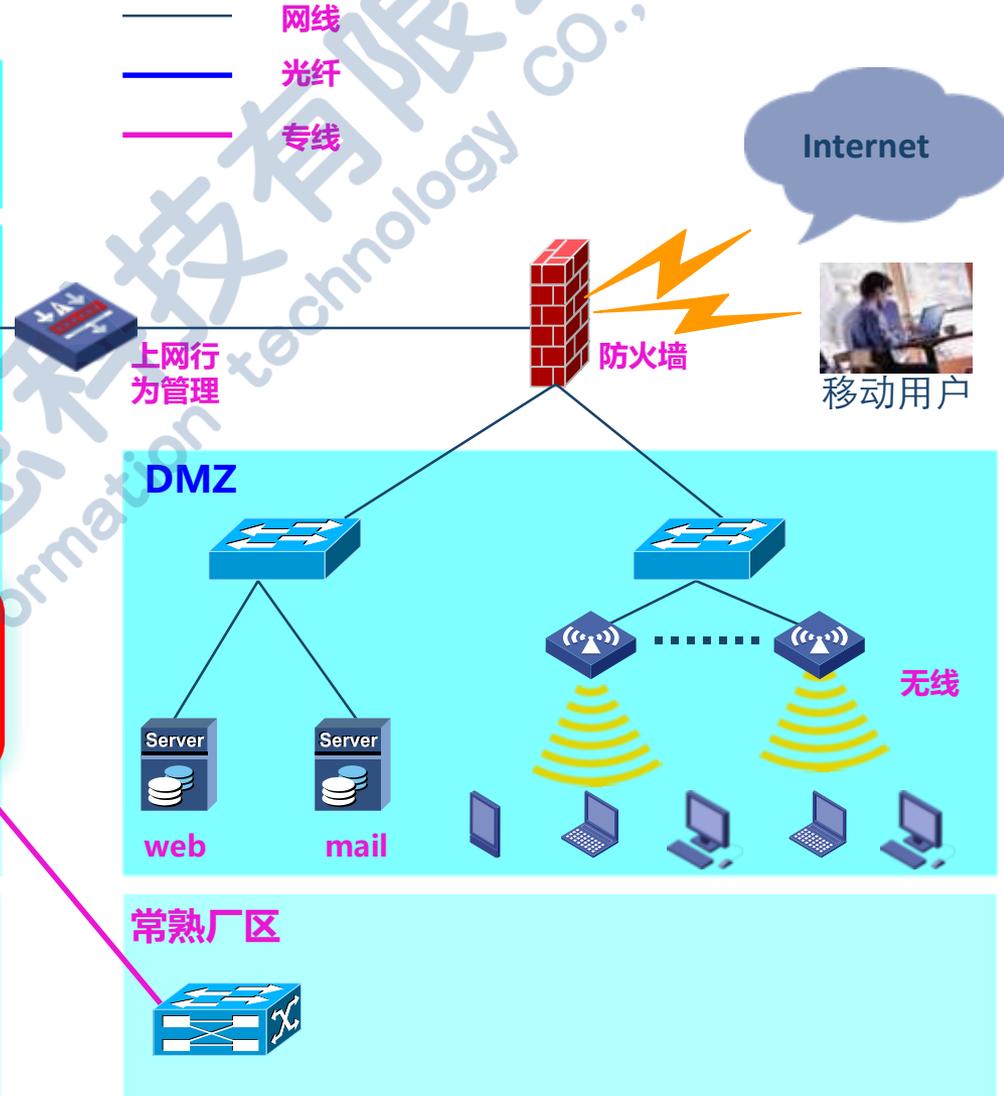
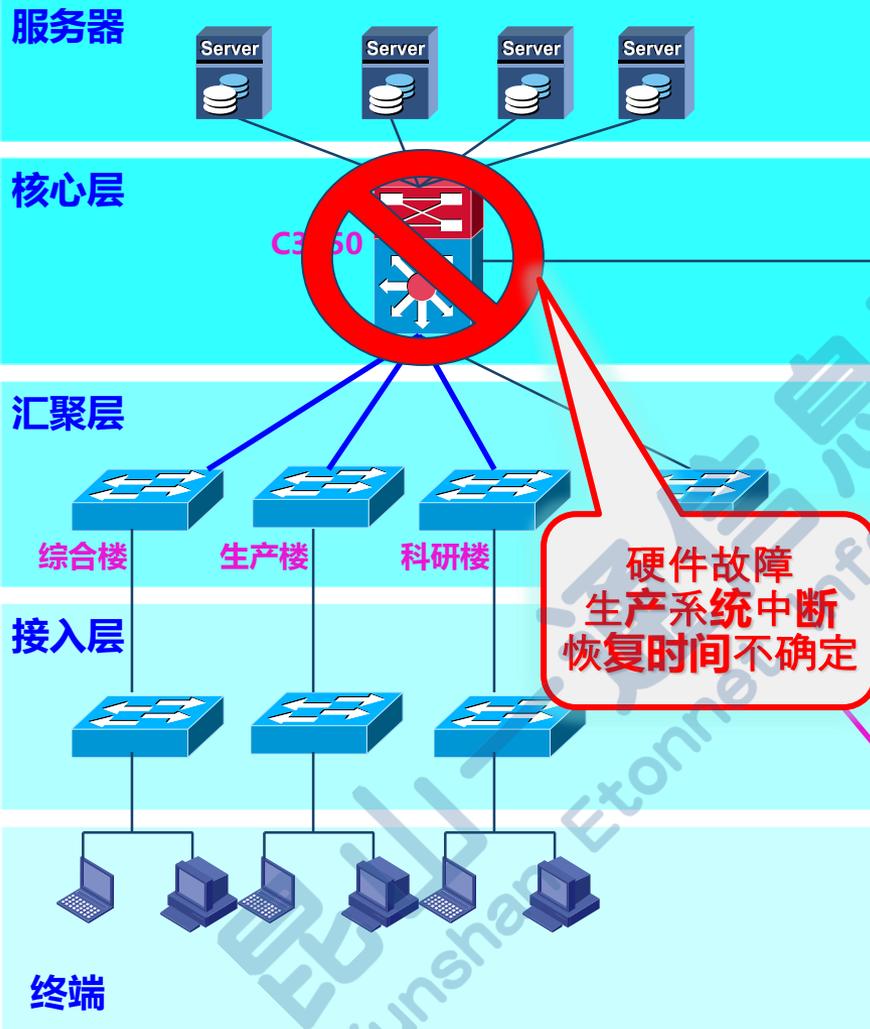
C3850 替换 C3560X

三层性能稳定
网络无延迟

网络架构

etonnet.com.cn

问题二



网络架构

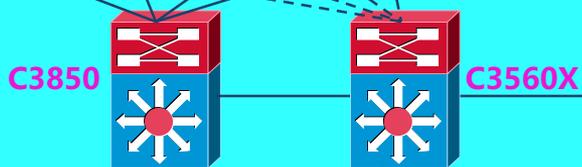
etonnet.com.cn

解决方案

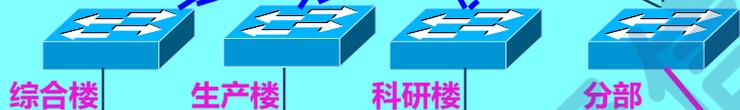
服务器



核心层



汇聚层



接入层



终端



—— 网线
—— 光纤
—— 专线



上网行为管理



防火墙



Internet



移动用户

采用Cisco HSRP原理
利旧双核心双链路
实现核心交换机HA



web



mail



无线

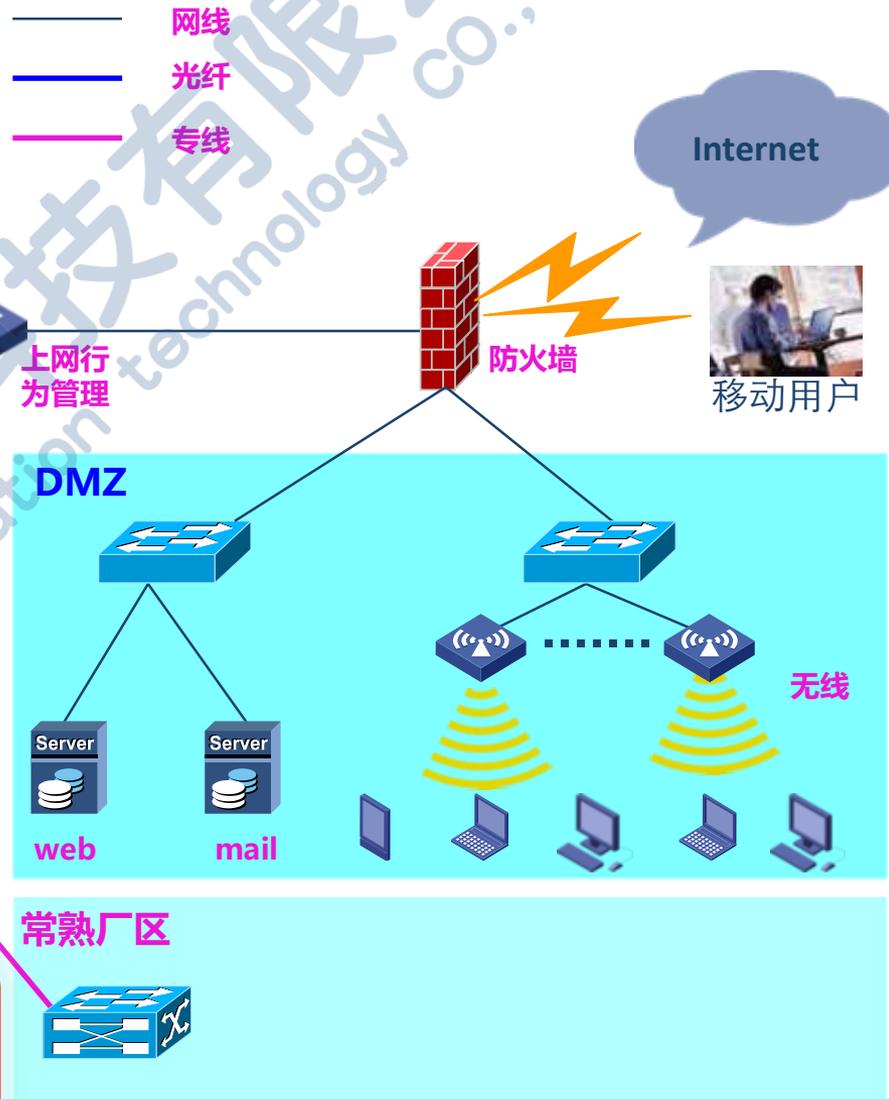
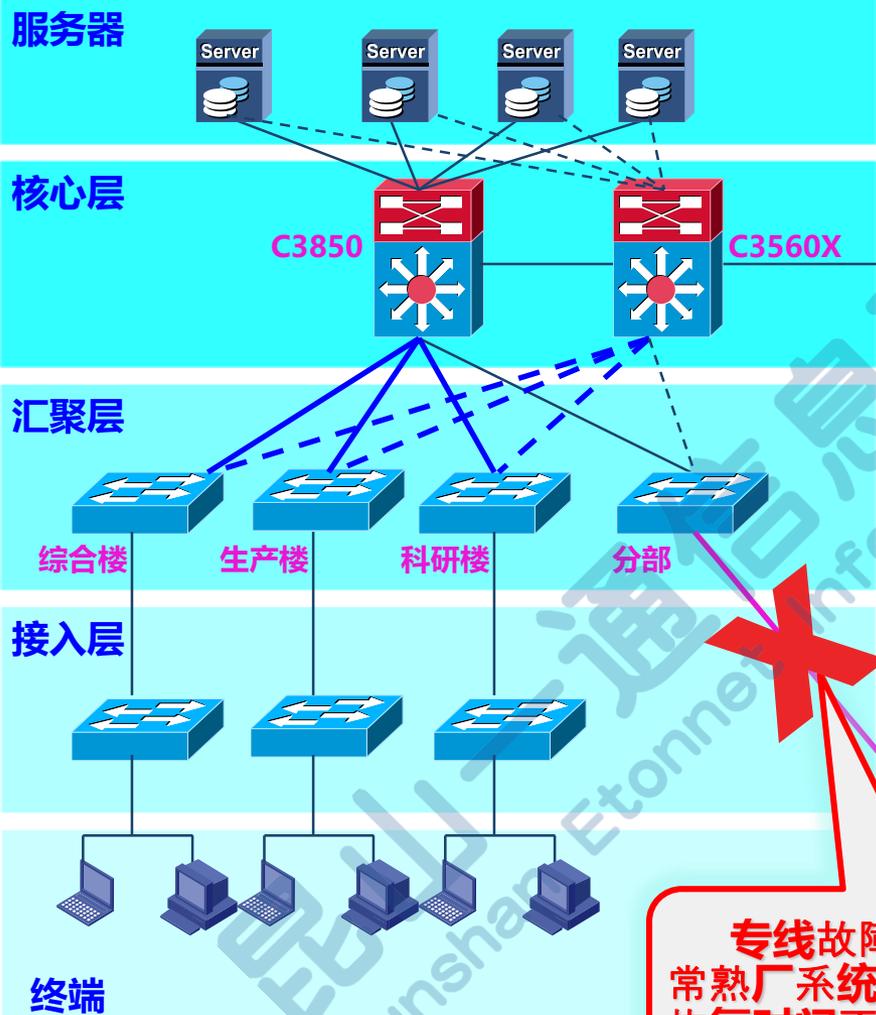
常熟厂区



网络架构

etonnet.com.cn

问题三



网络架构

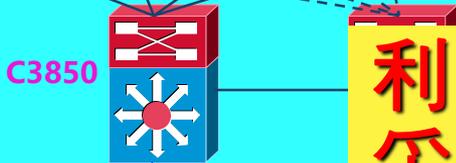
etonnet.com.cn

解决方案

服务器



核心层



汇聚层



接入层

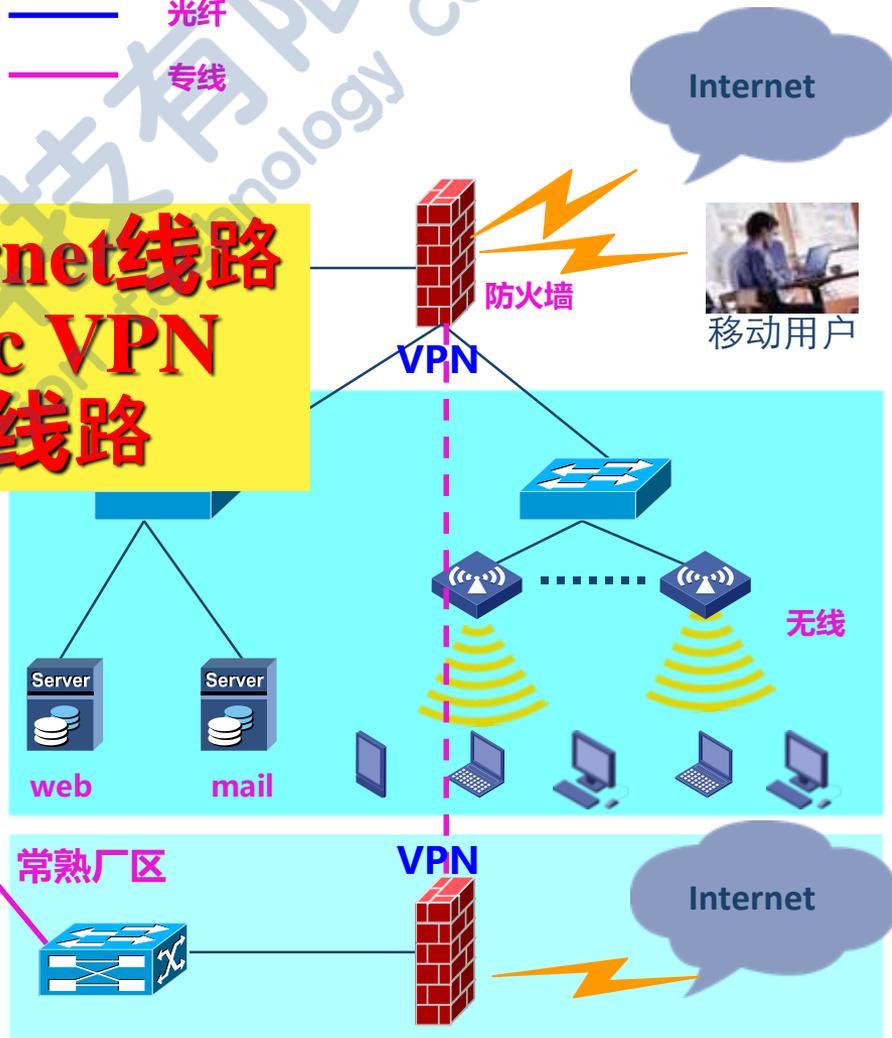


终端



利用Internet线路
采用IPSec VPN
建立备援线路

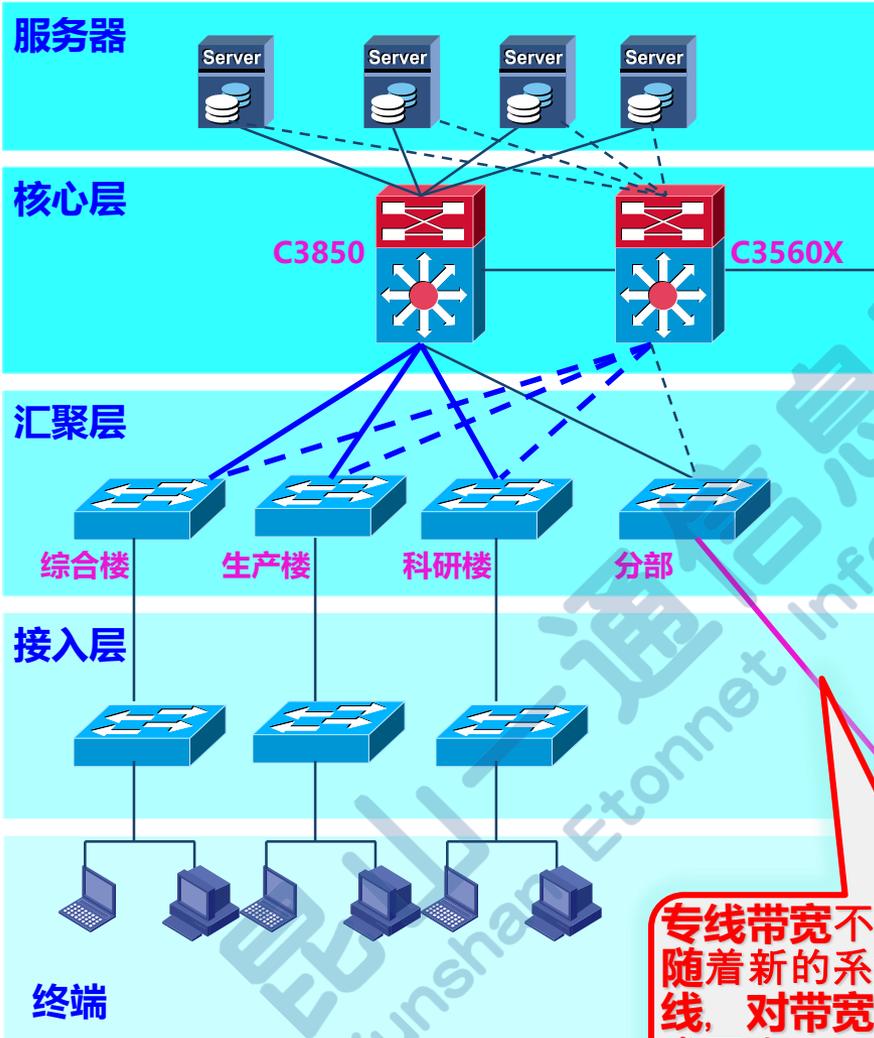
— 网线
— 光纤
— 专线



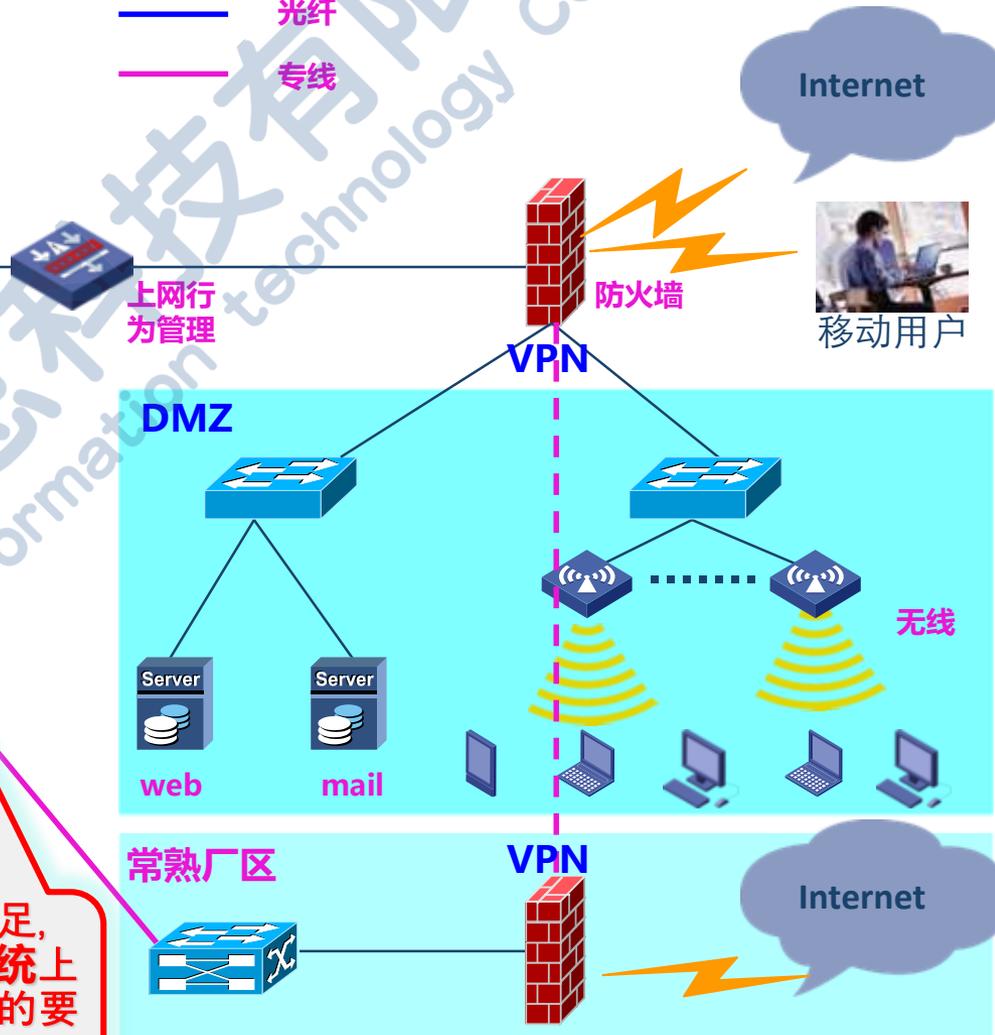
网络架构

etonnet.com.cn

问题四



- 网线
- 光纤
- 专线

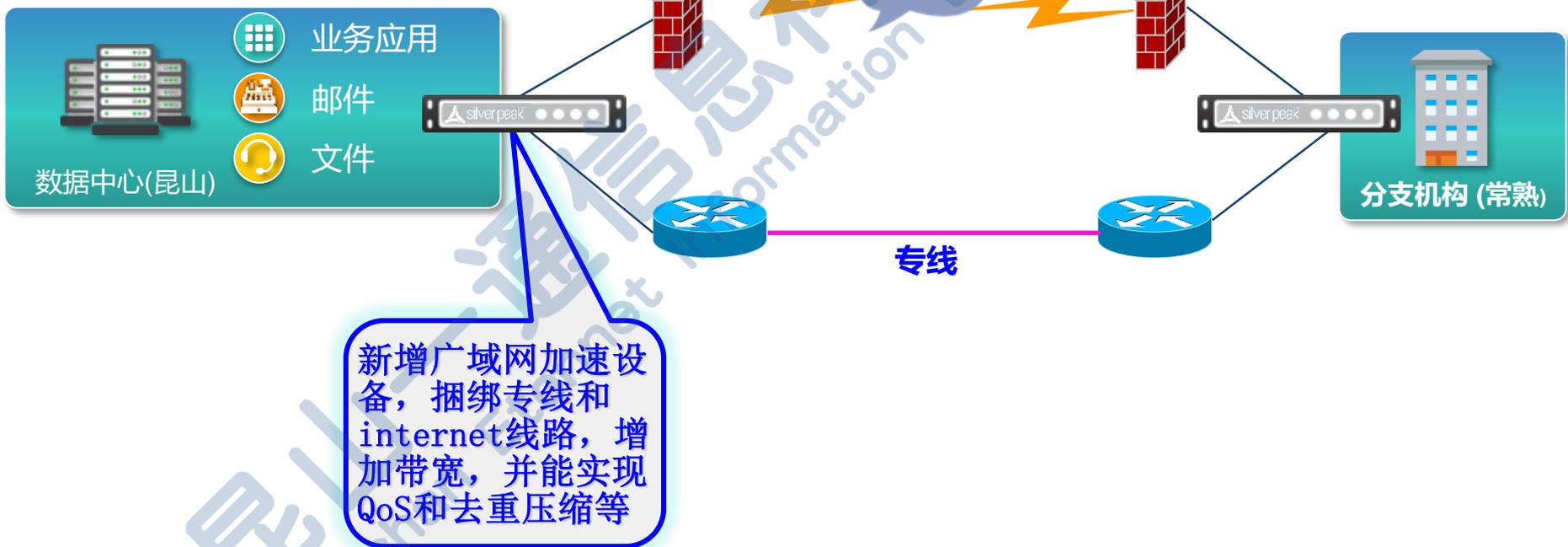


专线带宽不足，随着新的系统上线，对带宽的要求更高

网络架构

etonnet.com.cn

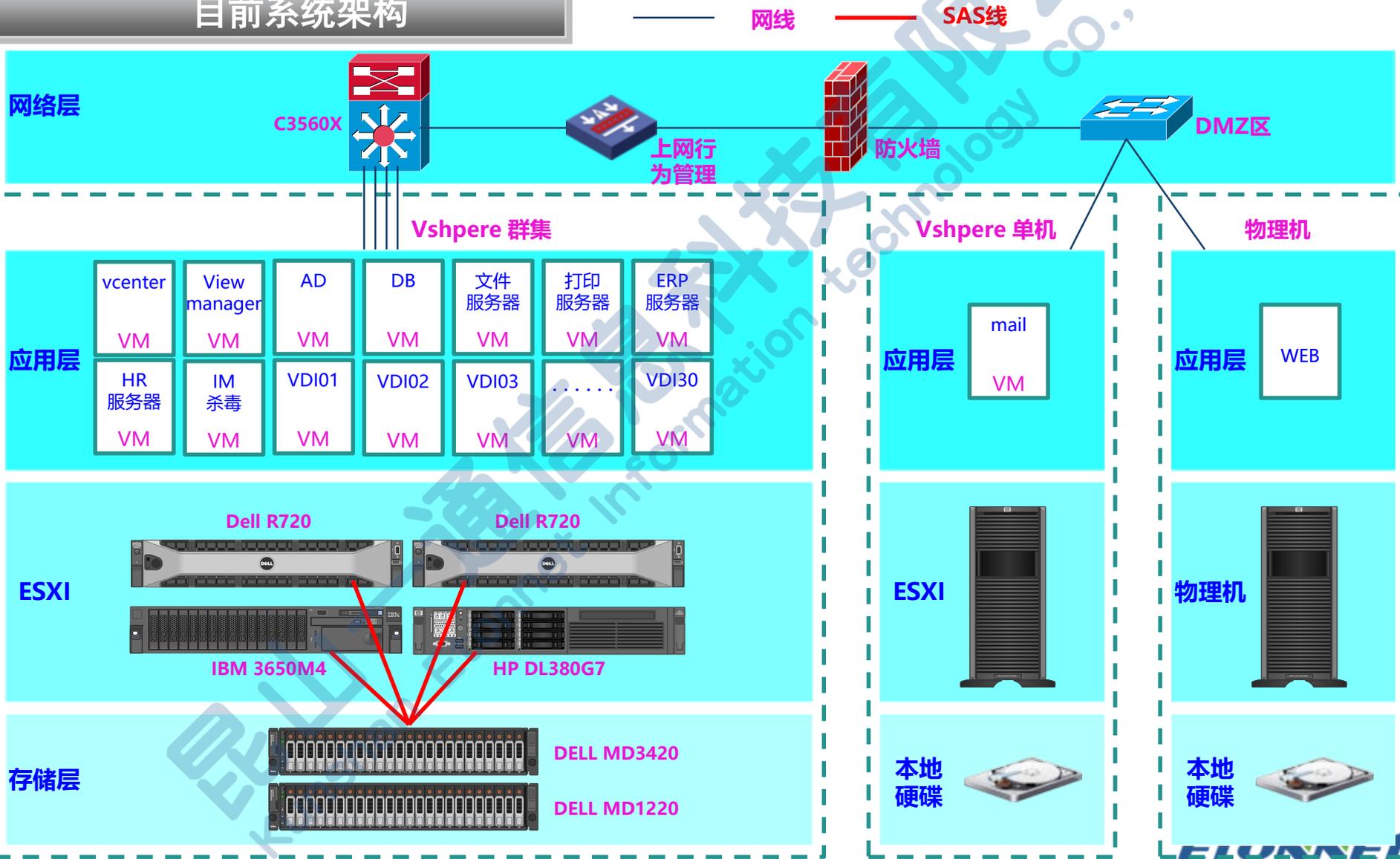
解决方案



系统架构

etonnet.com.cn

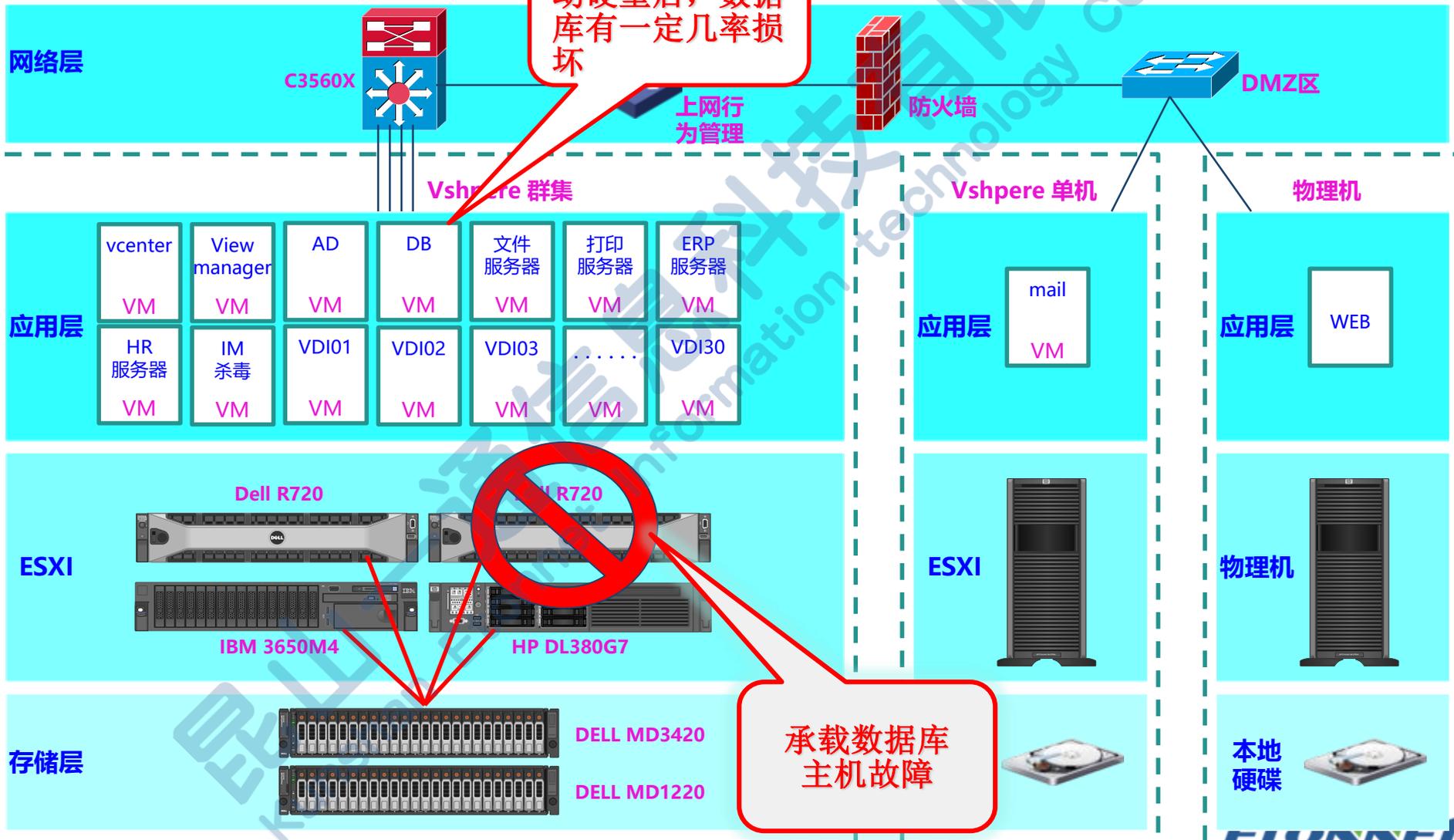
目前系统架构



系统架构

etonnet.com.cn

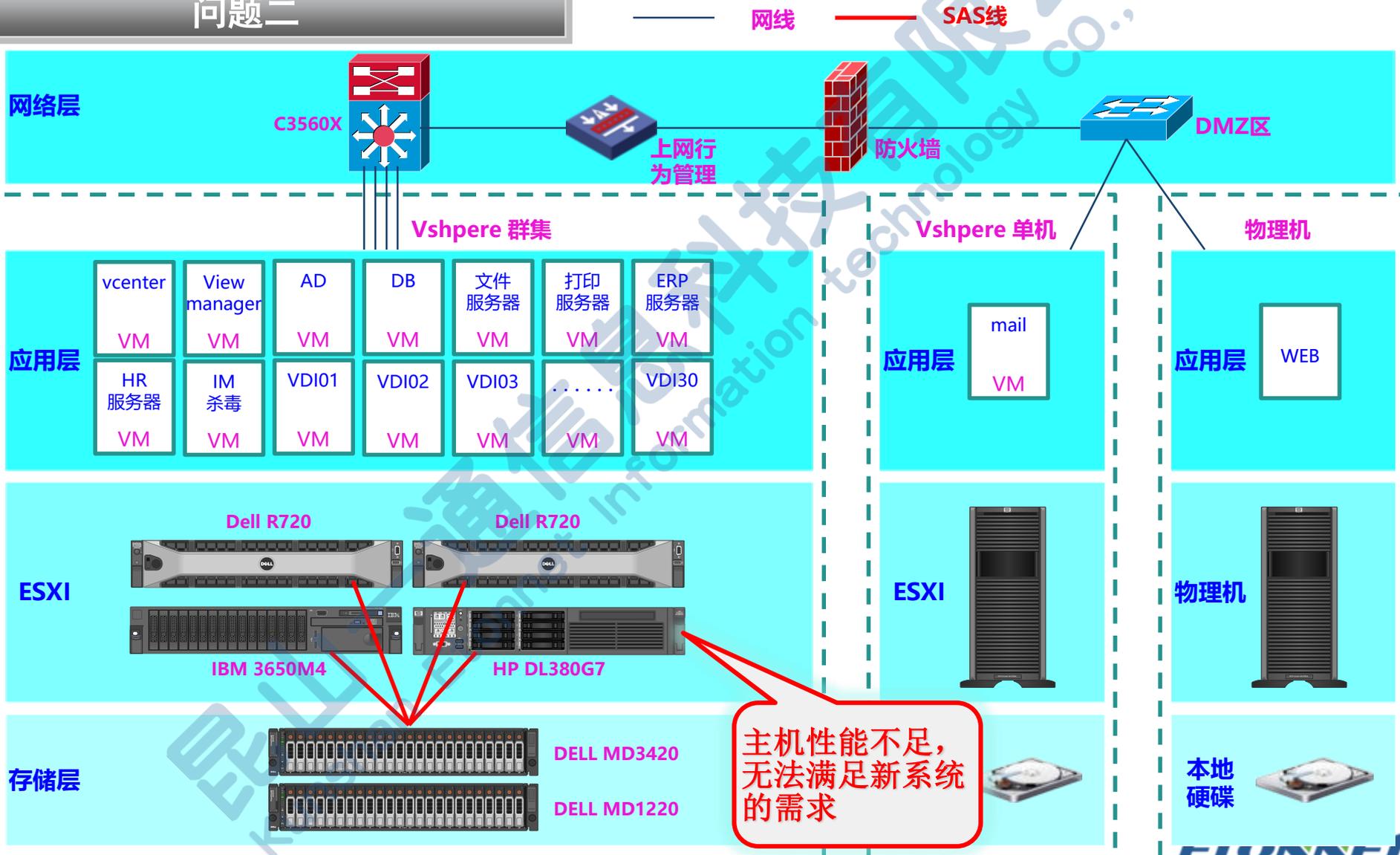
问题一



系统架构

etonnet.com.cn

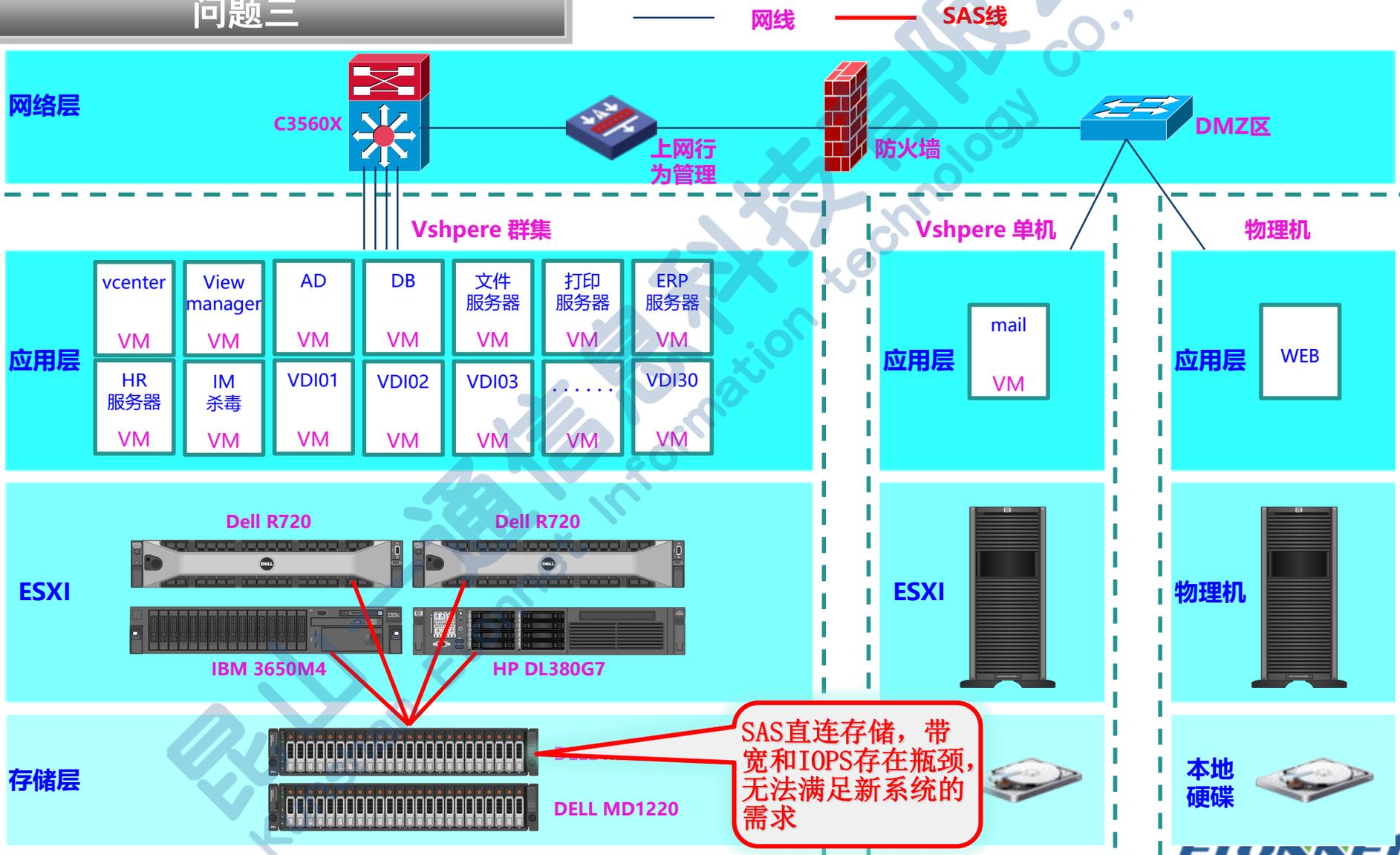
问题二



系统架构

etonnet.com.cn

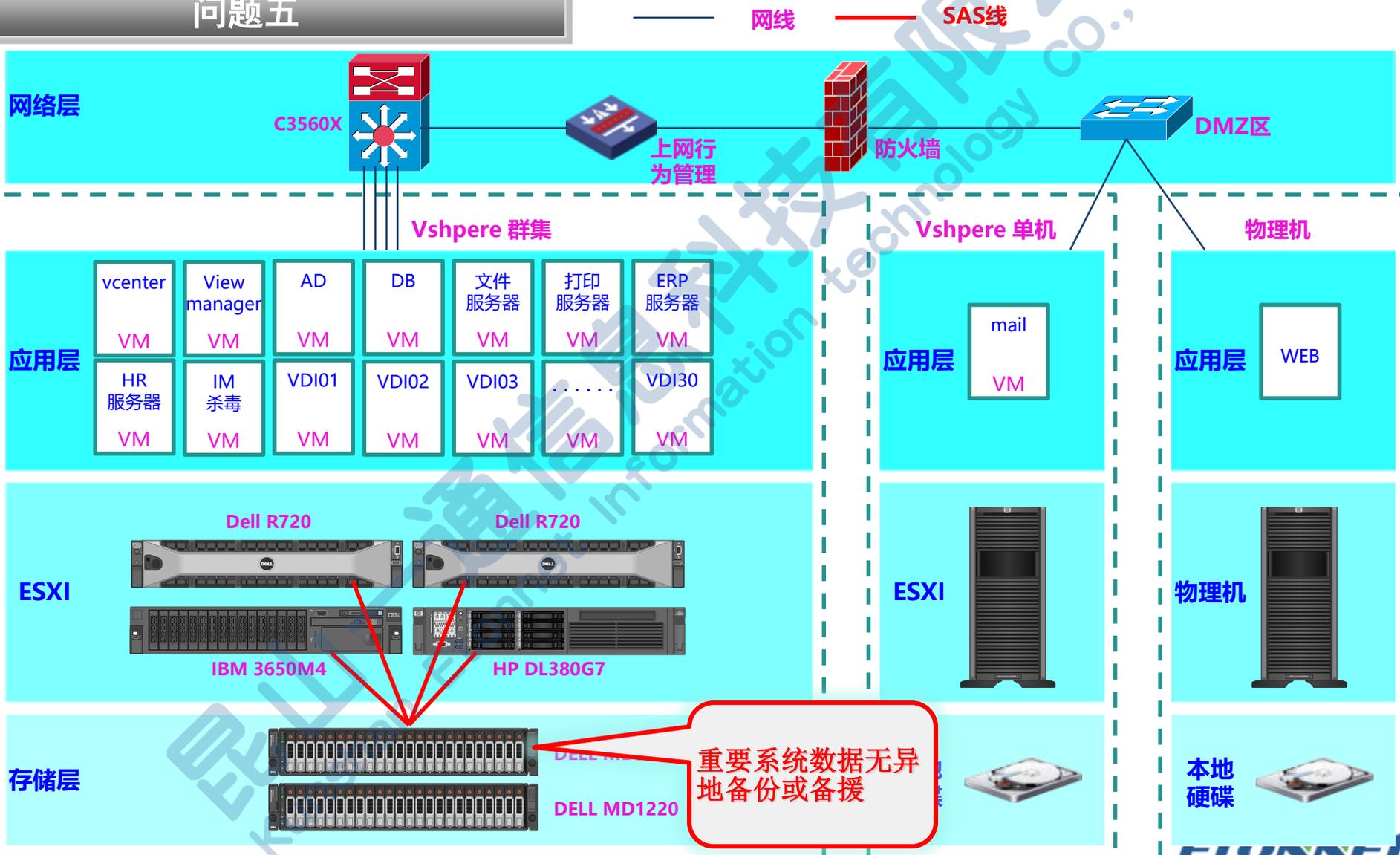
问题三



系统架构

etonnet.com.cn

问题五



重要系统数据无异地备份或备援

系统架构

etonnet.com.cn

解决方案

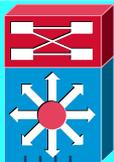
网线

SAS线

FC

网络层

C3560X



Vshpere 群集(旧)

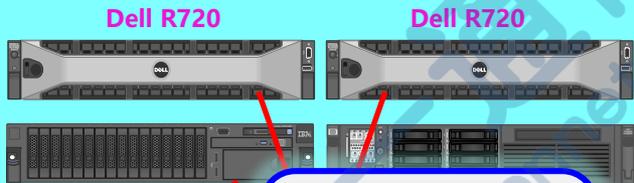
Vshpere 群集(新)

应用层

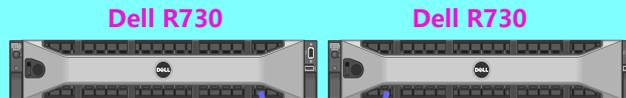


应用层

ESXI



ESXI



存储层



存储层



新增满足要求的主机和存储，建立新的vsphere群集

系统架构

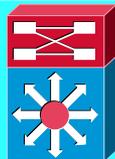
etonnnet.com.cn

解决方案

— 网线 — SAS线 — FC

网络层

C3560X



新建虚拟机作为ERP
前端应用系统，实
现数据和应用分离

Vshpere 群集(旧)

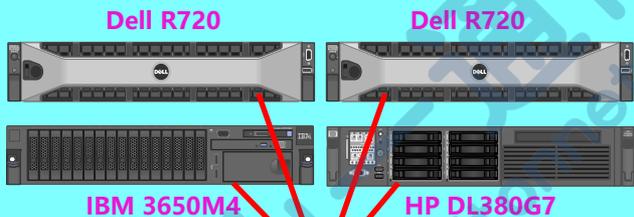
Vshpere 群集(新)



不同物理主机通过
RDM建立两台数据
库虚拟机，并建立
mscs群集



ESXI



ESXI



存储层



存储层



系统架构

etonnet.com.cn

解决方案

— 网线 — SAS线 — FC

网络层

C3560X



Vshpere 群集(旧)

Vshpere 群集(新)

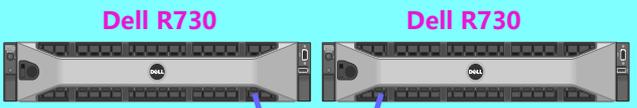
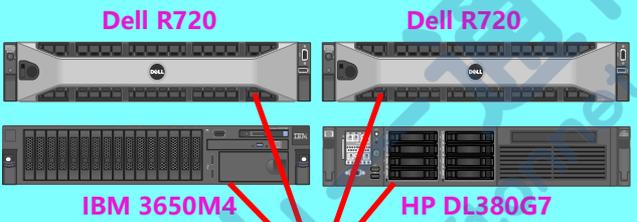


应用层

应用层

ESXI

ESXI



存储层

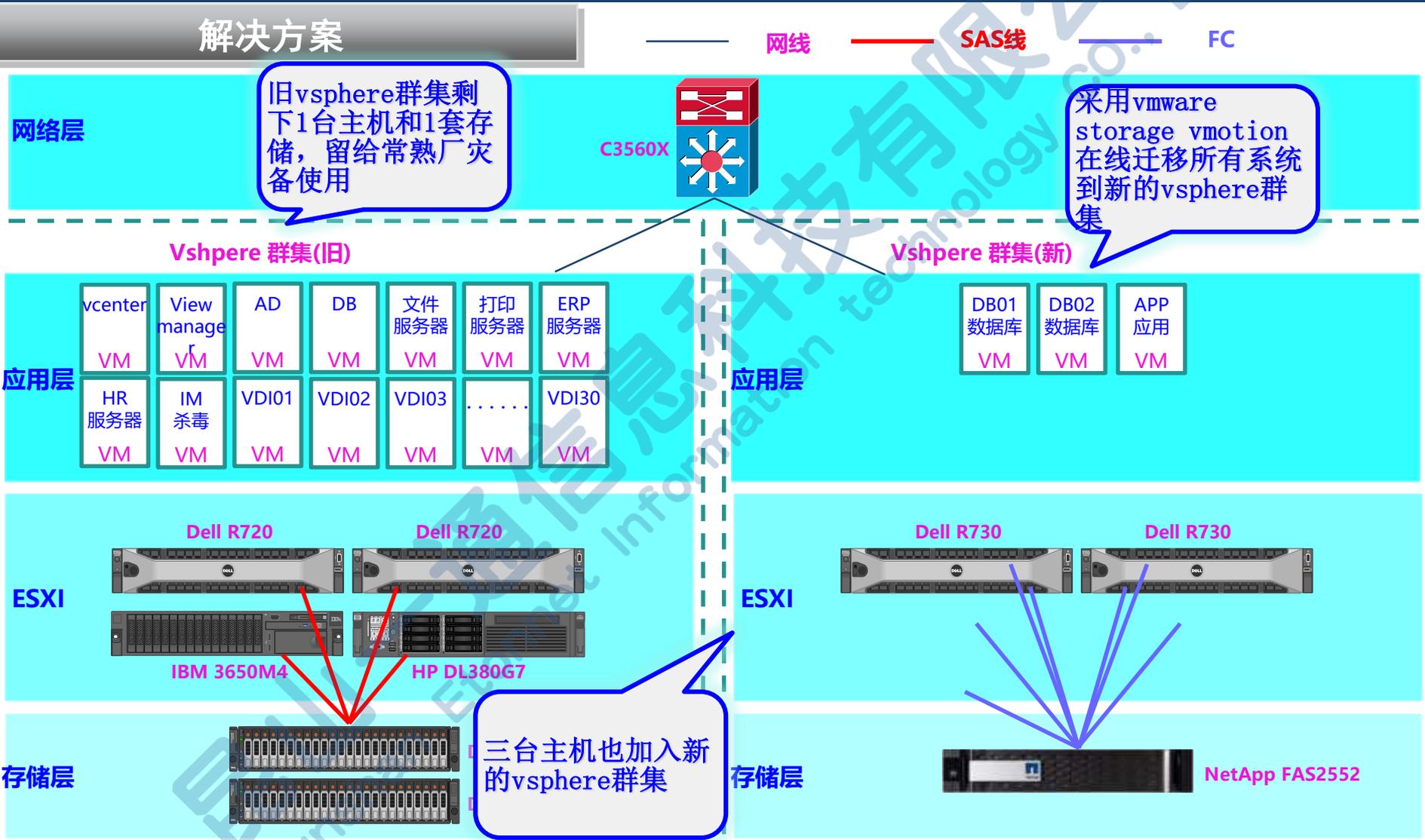
存储层



系统架构

etonnet.com.cn

解决方案



系统架构

etonnet.com.cn

解决方案

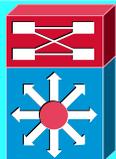
新vsphere群集完全替代旧vsphere群集运作

网线

SAS线

FC

C3560X



Vshpere 群集(旧)

Vshpere 群集(新)

应用层

应用层

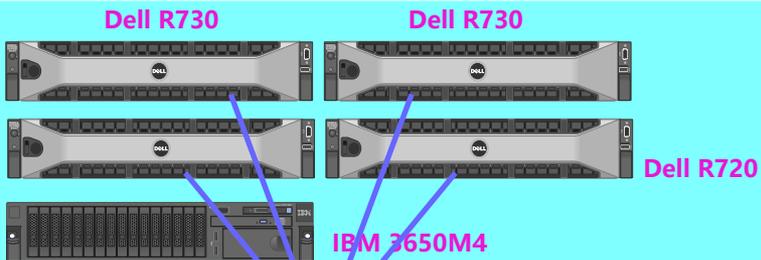


ESXI

ESXI



HP DL380G7



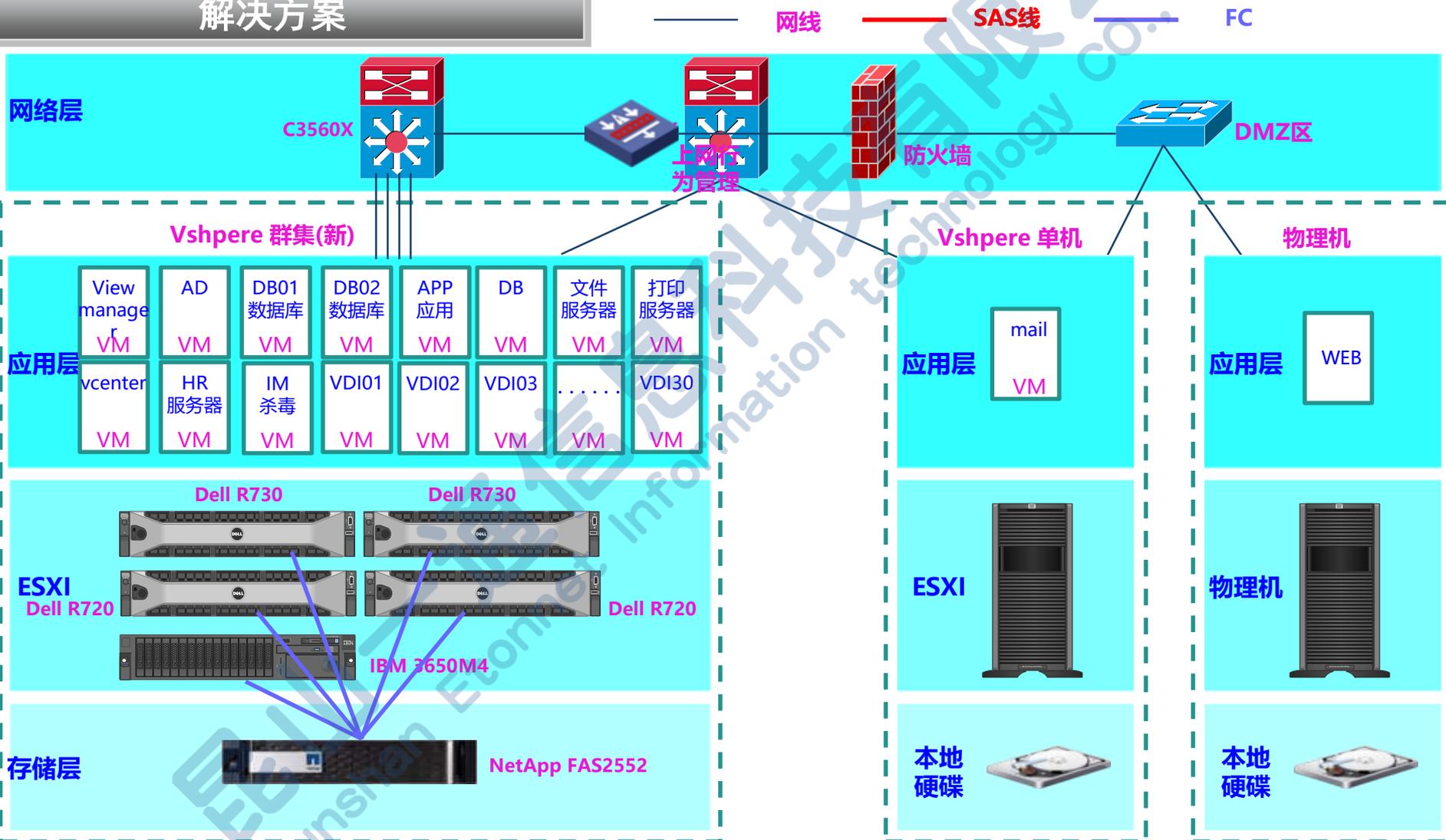
存储层

存储层



系统架构

解决方案



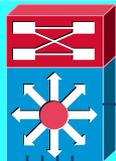
系统架构

etonnet.com.cn

解决方案

网络层

C3560X



DMZ区的mail通过 storage vmotion, WEB通过P to V 移到新vsphere群集

SAS线

防火墙

两台单机撤出

Vshpere 群集(新)

应用层



Dell R730

Dell R730

ESXI

Dell R720

Dell R720

IBM 3650M4

存储层



NetApp FAS2552

Vshpere 单机

应用层



ESXI



本地 硬碟



物理机

应用层



物理机



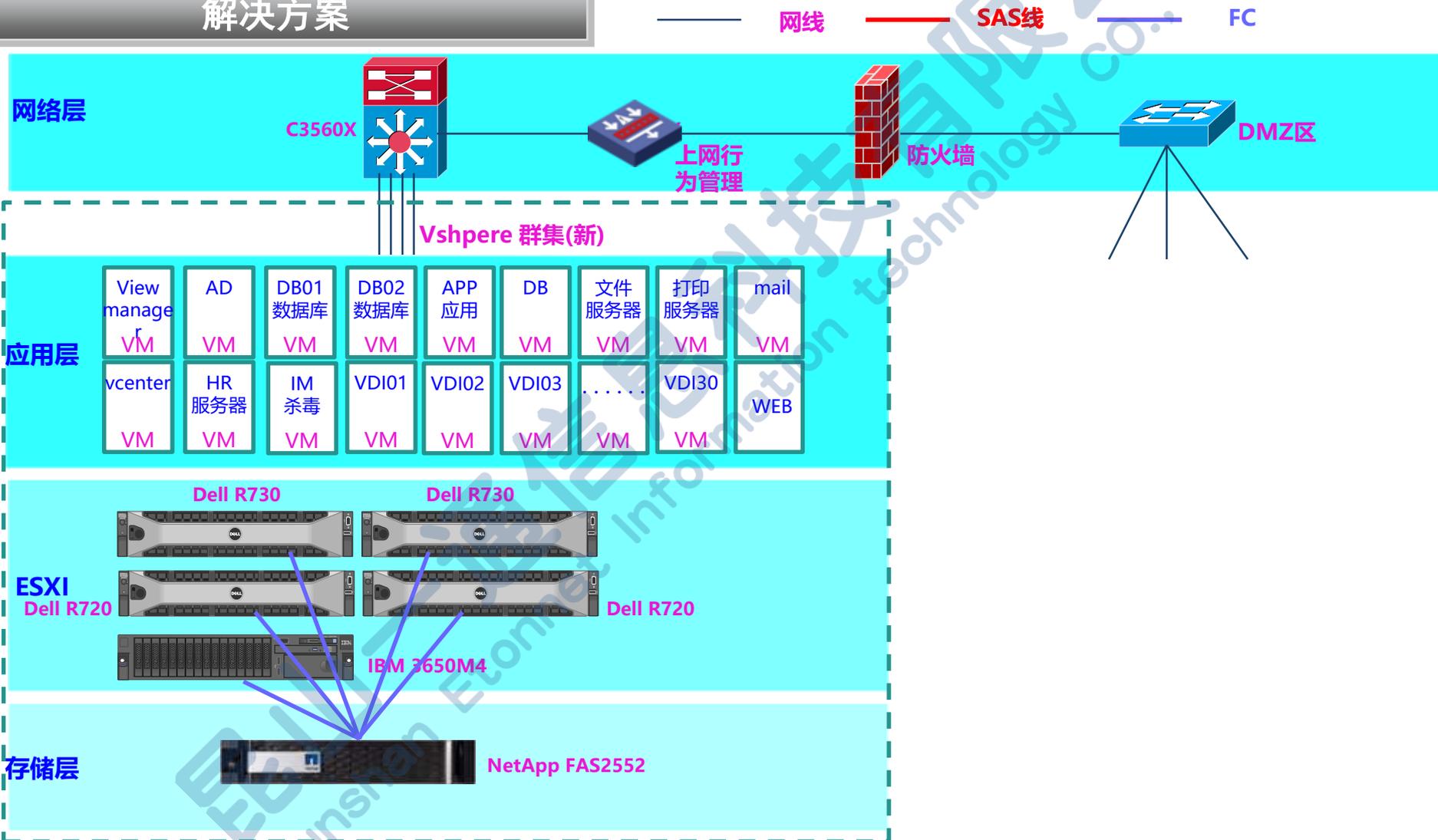
本地 硬碟



系统架构

etonnet.com.cn

解决方案

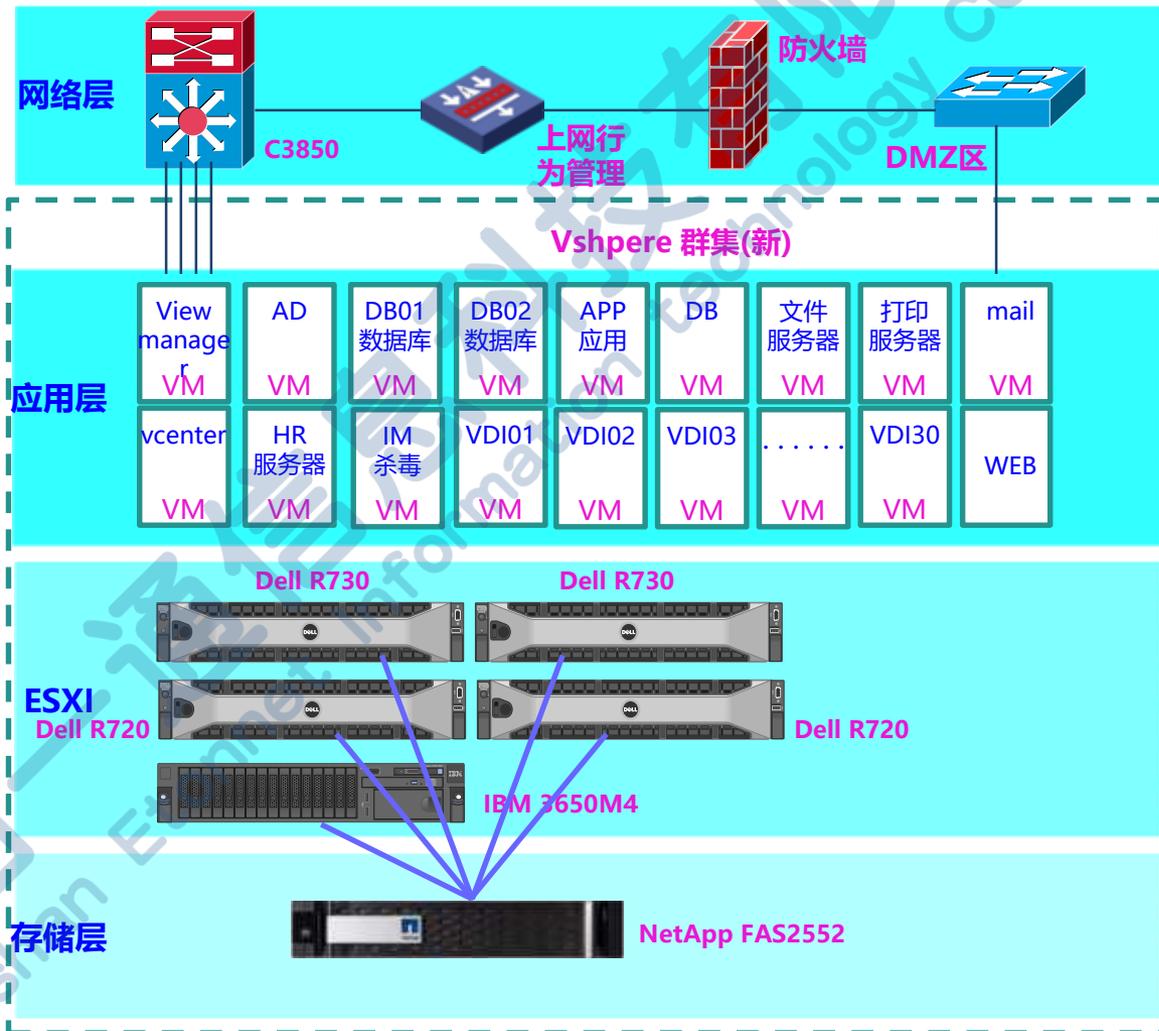


系统架构

etonnet.com.cn

解决方案

—— 网线 ——— SAS线 ——— FC



昆山厂

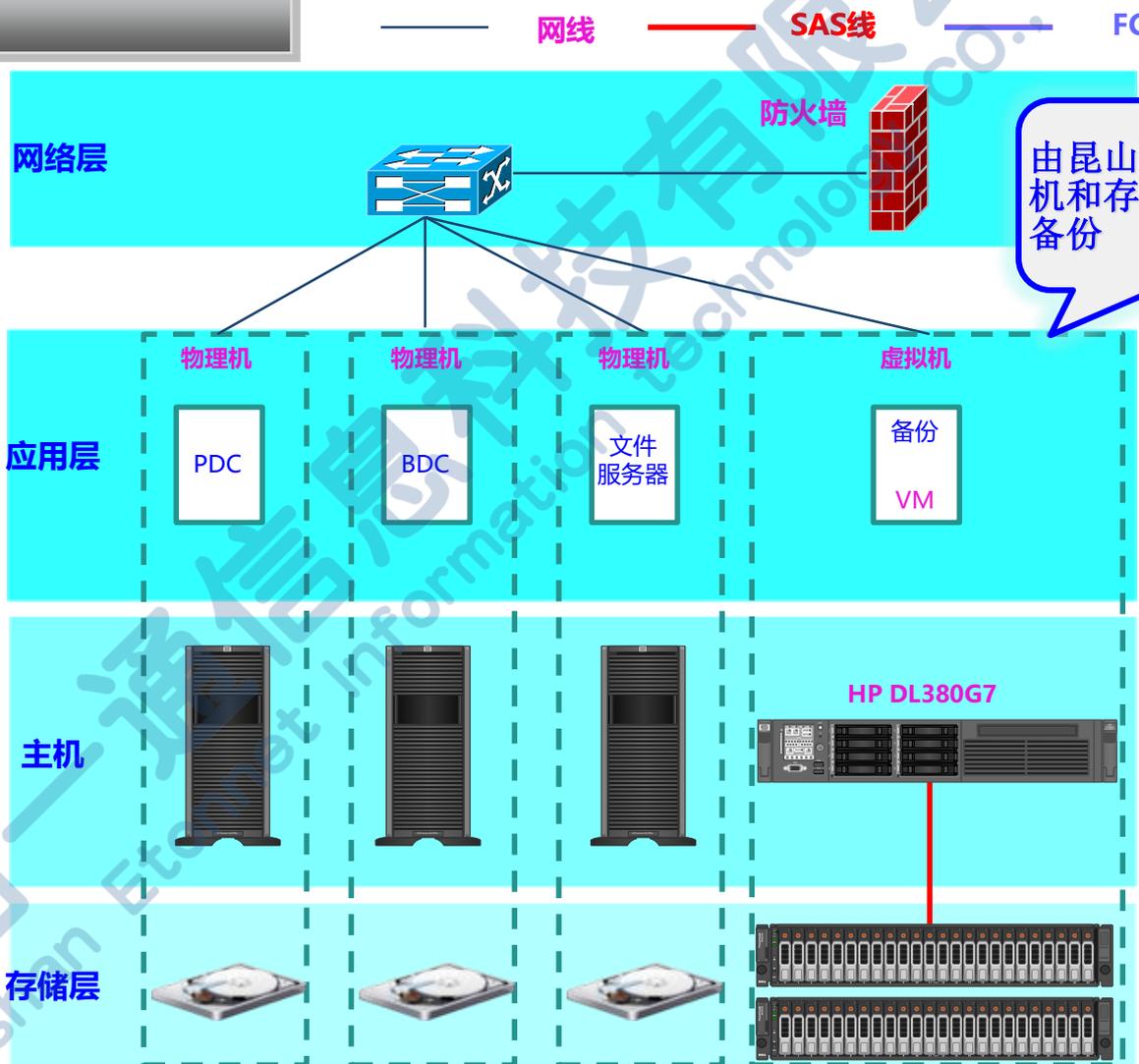
昆山 Etonnet Technology Co., Ltd.

系统架构

etonnet.com.cn

解决方案

常熟厂



防护痛点1—外来设备管控



如何避免**未经许可**的计算机设备连接内部网络

- 员工自行携带计算机设备
- 外来访客
- 研发/测试环境



如何确保IP的合理使用，避免IP冒用所造成的危害

- 误用他人IP，造成他人无法使用网络
- 冒用他人IP，企图隐藏身分
- 误用主机IP，造成服务中断
- 私自架设DHCP Server，造成网络异常



HELP

导入AD后的困扰

- 如何管理未加入AD的设备?
- 如何管理无法加入AD的设备?
- 使用者私自退域怎么办?
- 如何限制本机登入?
- 如何避免共享账号?

防护痛点4—终端合规检查



如何确保所有设备符合信息安全管理策略

- 是否已安装杀毒软件?
- 是否已安装所需之软件?
- 是否安装不当软件?
- 是否符合公司规定OS版本?
- 是否符合公司GPO套用规则?



是否拥有完整的IP使用记录

- WHO IS 192.168.0.1?
- 设备是什么?
- 使用者是谁?
- 位置在哪?

安全架构

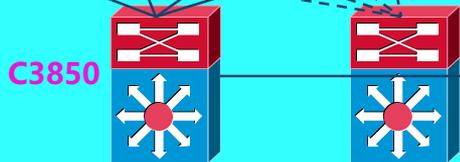
etonnet.com.cn

解决方案

服务器



核心层



Trunk



引入NAC设备，有效的保证内网的安全性

网络准入设备

汇聚层



接入层



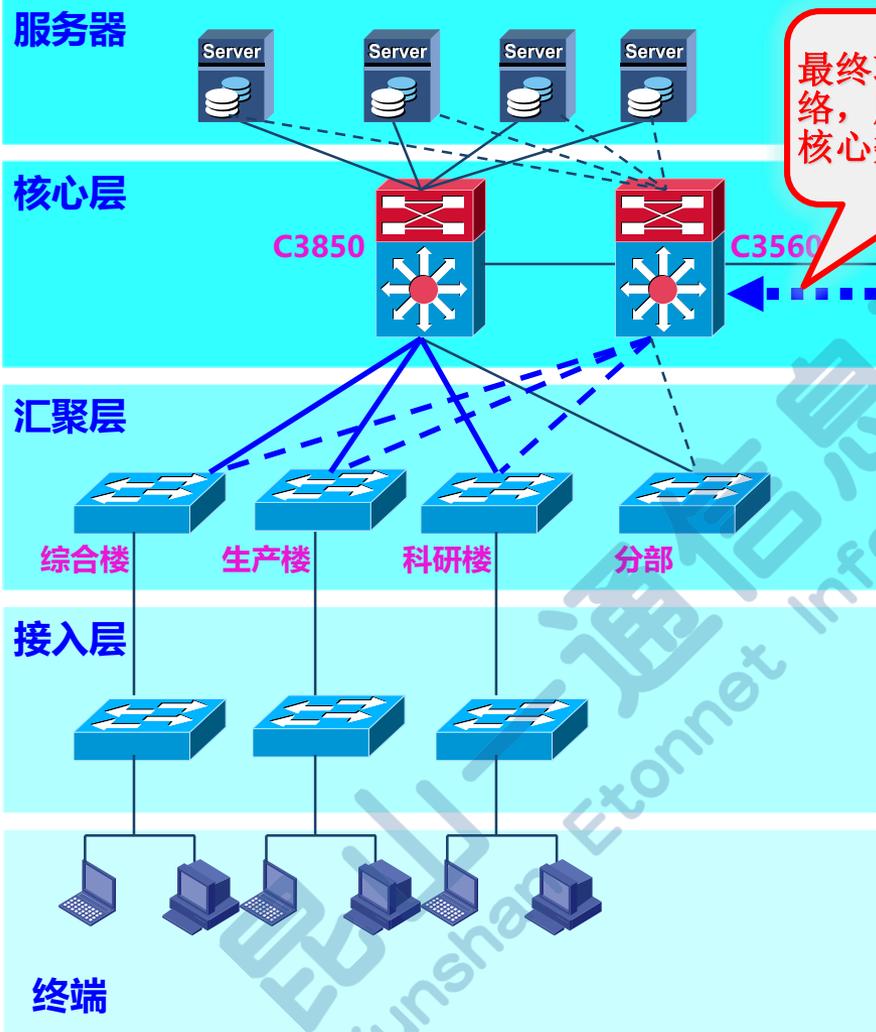
终端



安全架构

etonnet.com.cn

无线架构问题



最终攻击到内部网络，服务器，甚至核心数据



网线
光纤
专线

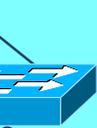
上网行为管理

DMZ

无线

DMZ区的系统因有对外开放端口，有可能被攻破

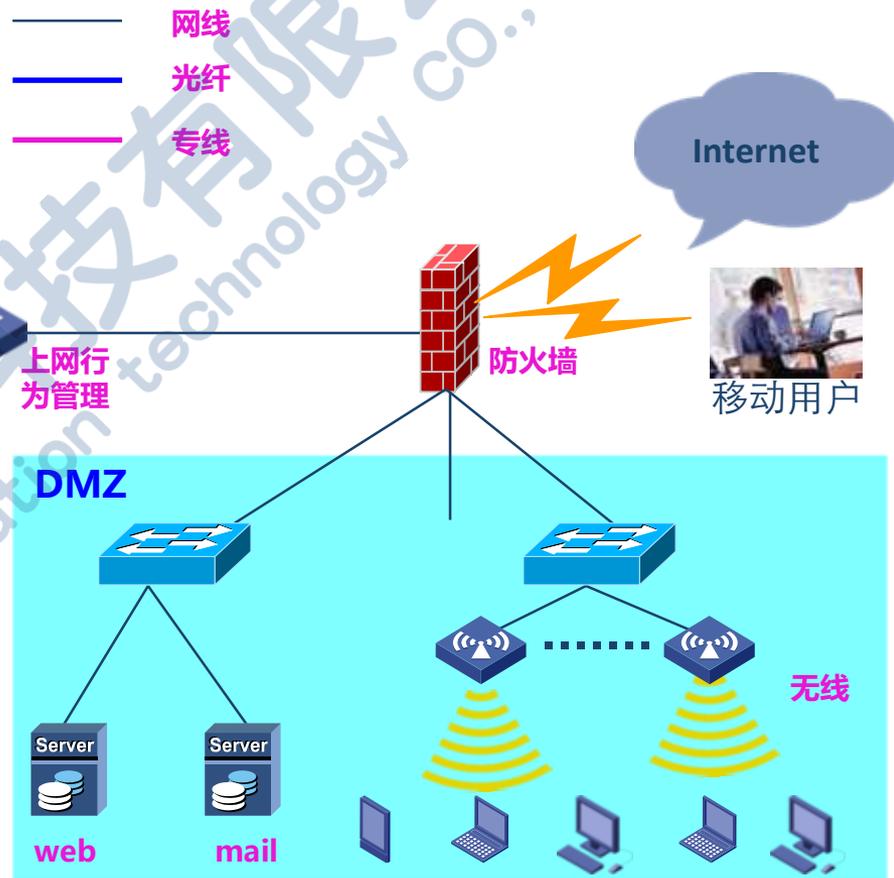
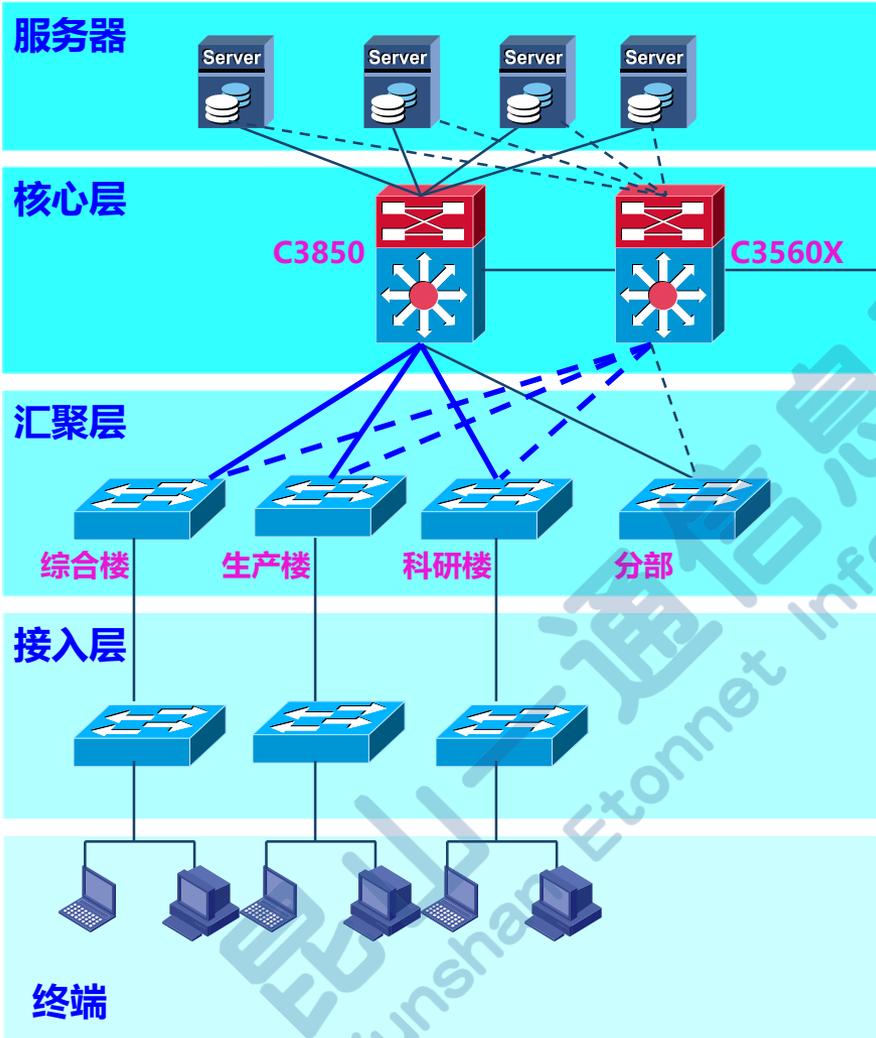
一旦被攻破，由此为跳板，进而攻击无线用户



安全架构

etonnet.com.cn

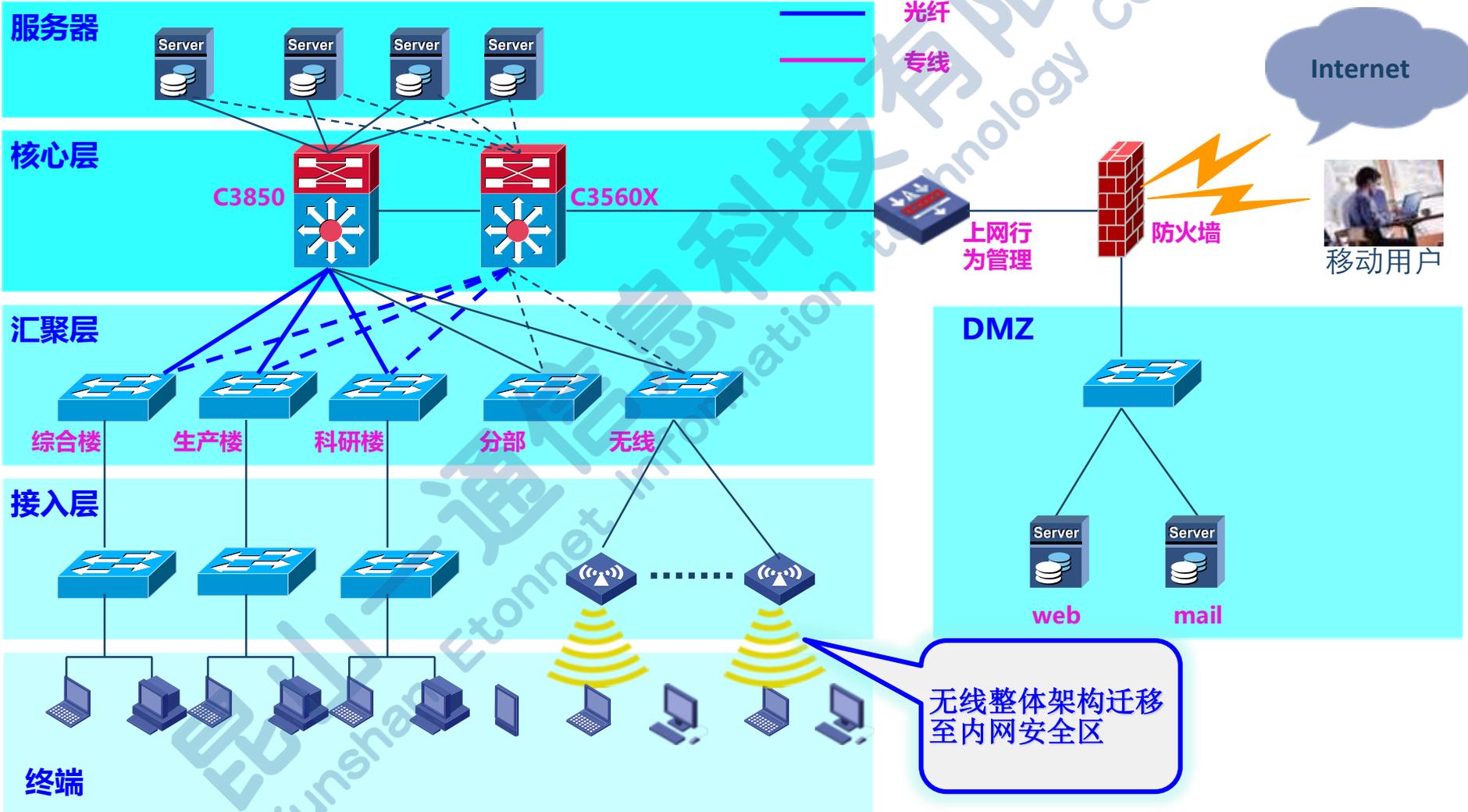
解决方案



安全架构

etonnet.com.cn

解决方案



缺乏IT运维管理平台

- 目前没有针对基础架构的性能和容量进行监控和管理的机制
- 所有的IT设备和系统的状况无法了解
- 只能做到有故障就处理，不能做到防患于未然
- 没有未来业务扩展和扩容的基本依据



建立IT运维管理平台

对象

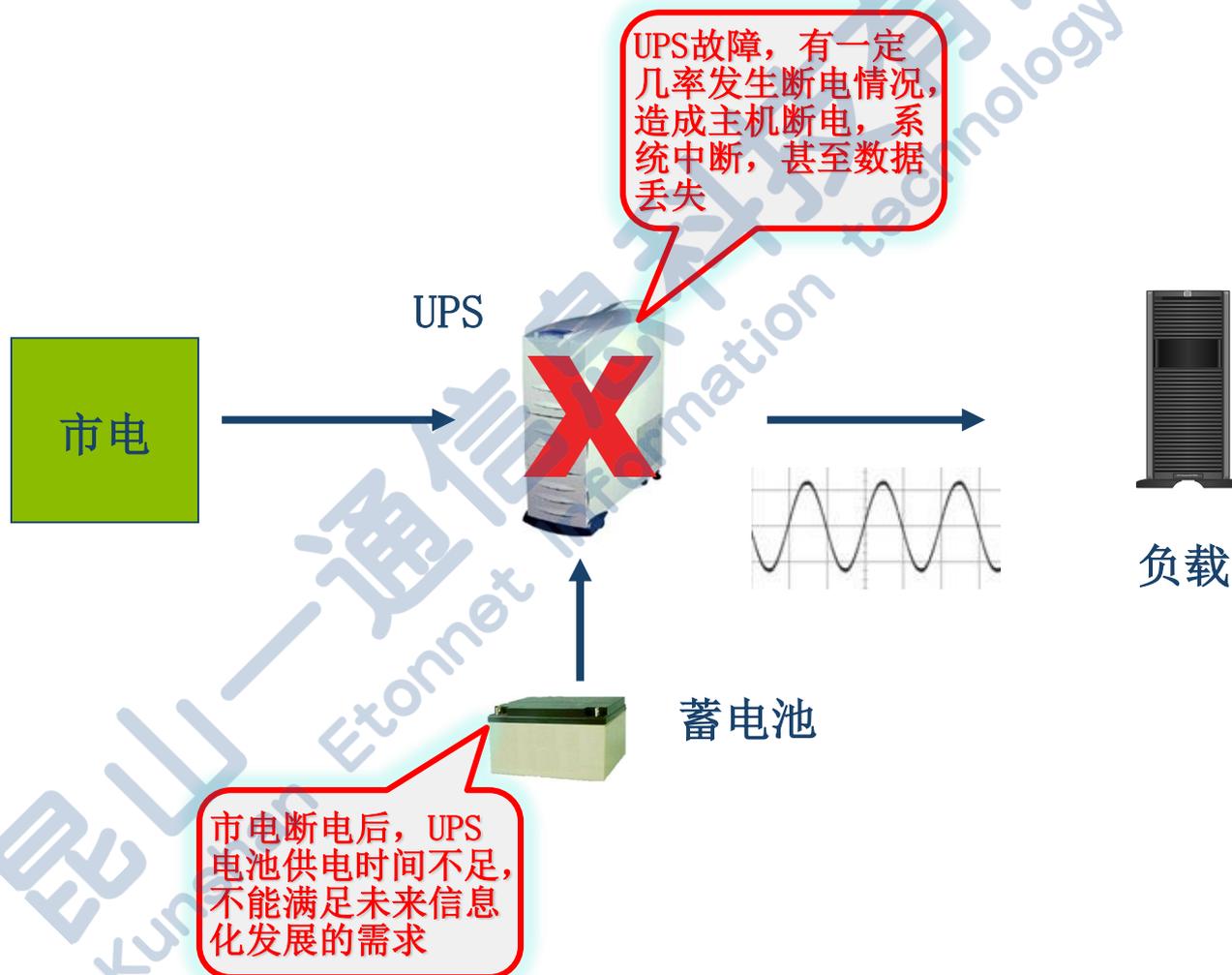
- ◆ 网络设备
 - 路由器
 - 交换机
 - 防火墙
 - 无线设备
- ◆ 计算机
 - 服务器
 - 桌面机
 - 域控制器
- ◆ 应用

内容

- ◆ 硬件和应用监控
- ◆ 性能监控
- ◆ 异常报警
- ◆ 历史记录查询
- ◆ 流量Top



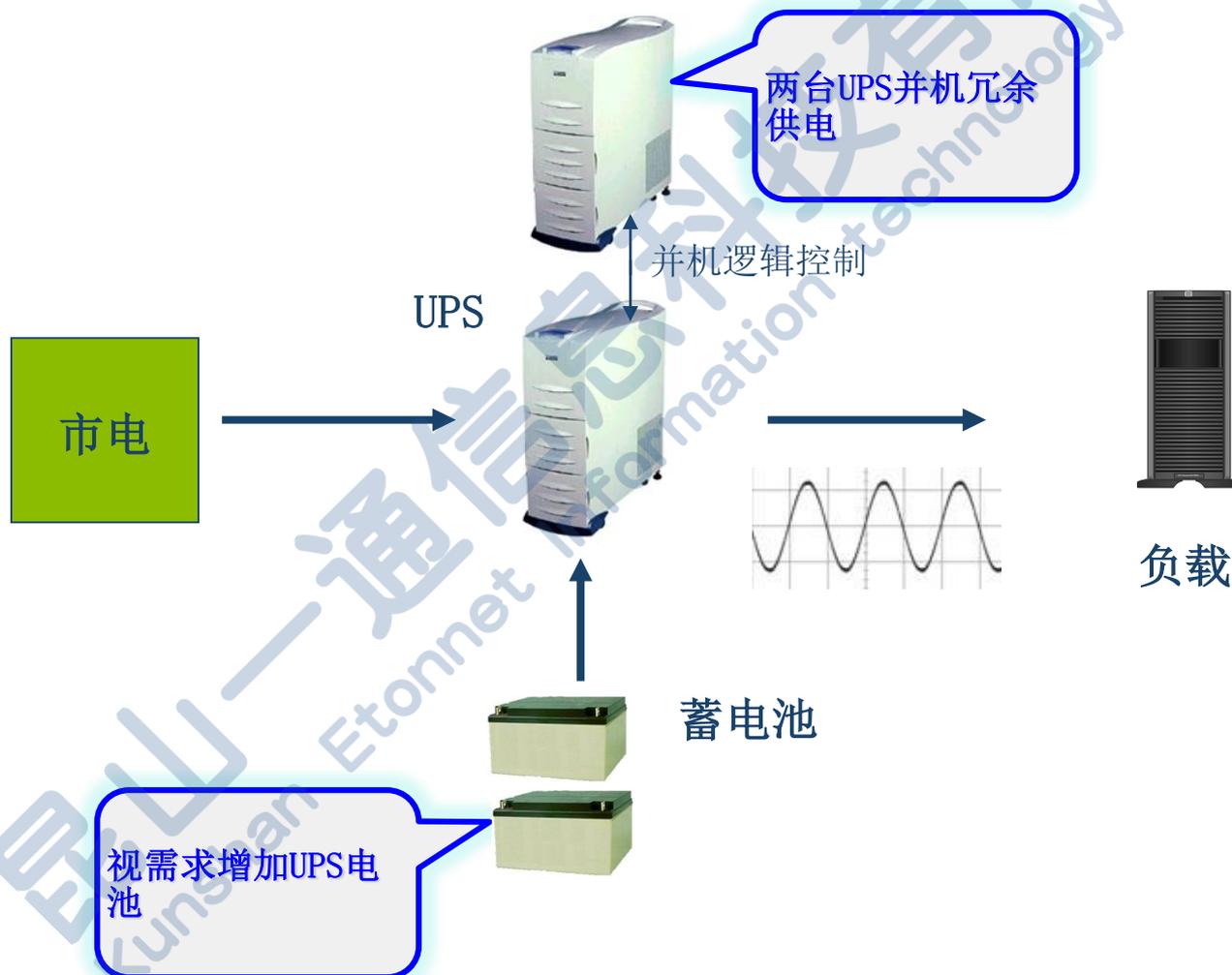
UPS问题



基础架构

etonnet.com.cn

解决方案



缺乏完善的机房环境监控机制

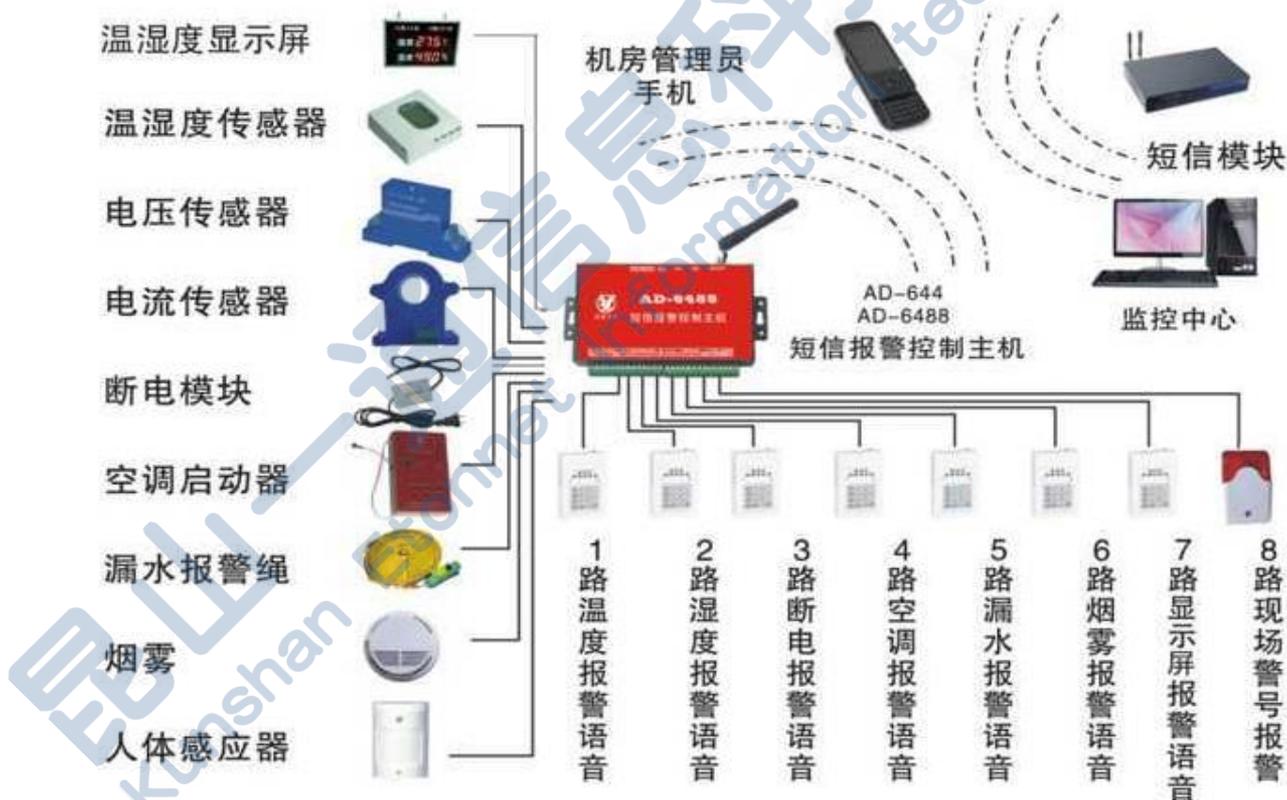
- UPS故障后，无法及时发现
- 缺少电力断电报警机制
- 缺少漏水检测机制
- 报警系统需完善，手机短信、电话语音、邮件等报警都需要建立
- 缺乏环境集中监控平台

昆山人通信信息科技有限公司
Kunshan Etonnet Information Technology Co., Ltd.

解决方案

建立完善的机房环境监控机制

监控整个机房内所有基础设施和设备的运行状态，通过相关实时监控数据了解机房内各设备的运行是否正常以及指定相应的设备冗余方案和维护机制





一通科技

Thank You !

etonnet.com.cn

一通科技-数据中心