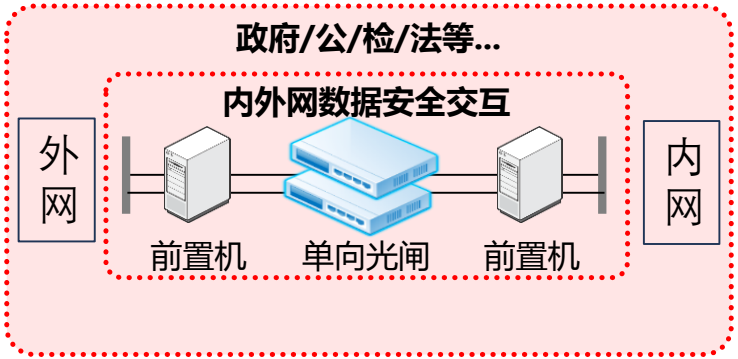
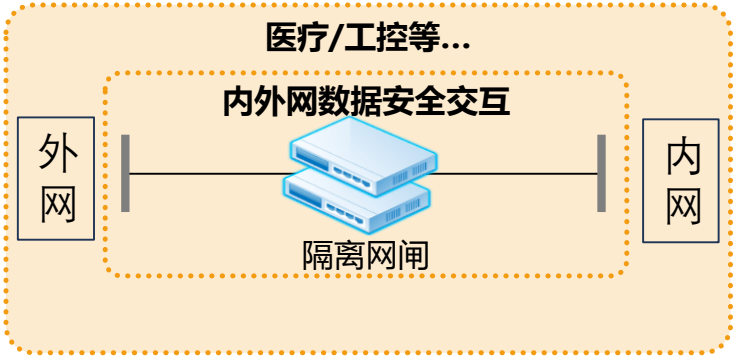
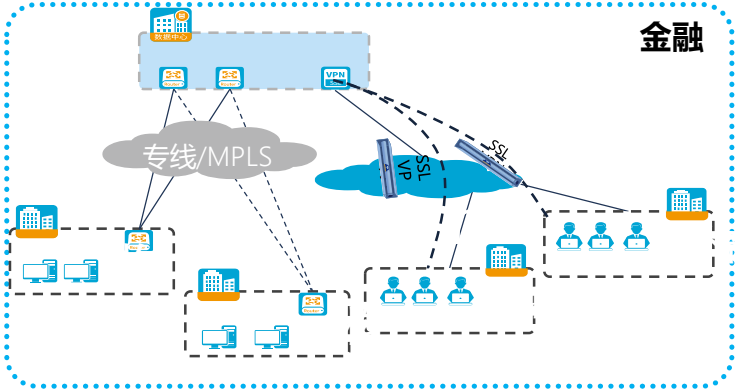
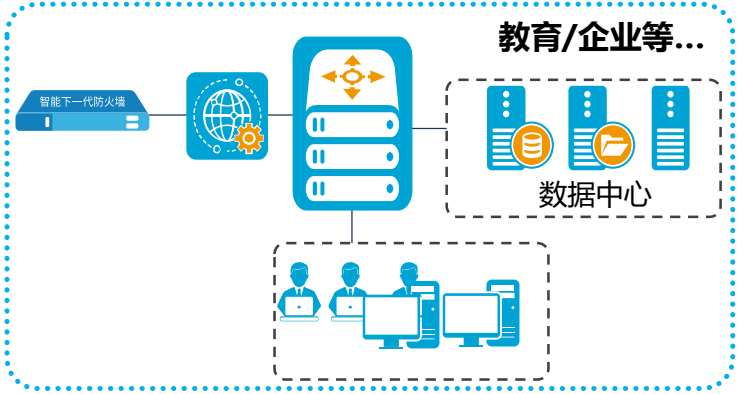

作品提交模板
(提交时请删除此标记)
Hillstone
山 石 网 科
Hillstone
山 石 网 科
方案名称：通用IT架构下的方案融合
个人信息：石浩-重庆银拓信息技术有限责任公司

# 背景介绍—通用IT架构下的方案融合




……？

100个客户有100种环境，方案怎么融合？如何给客户介绍公司的整体解决方案？如何根据客户环境给予最好的解决方案？
如何融合公司产品？如何制作一个大多数场景都适合的通用解决方案？
如何提升效率及方案能力？

# 需求分析—方案融合

- 场景化下的方案通点：

**行业细分及交付困难**

在场景化模式下，针对每个行业，甚至于行业内继续在细分，针对行业的解决方案大同小异，但是在解决的同时也需要深入调研，尤其是前期交流，不熟悉具体情况下，没有参考物。

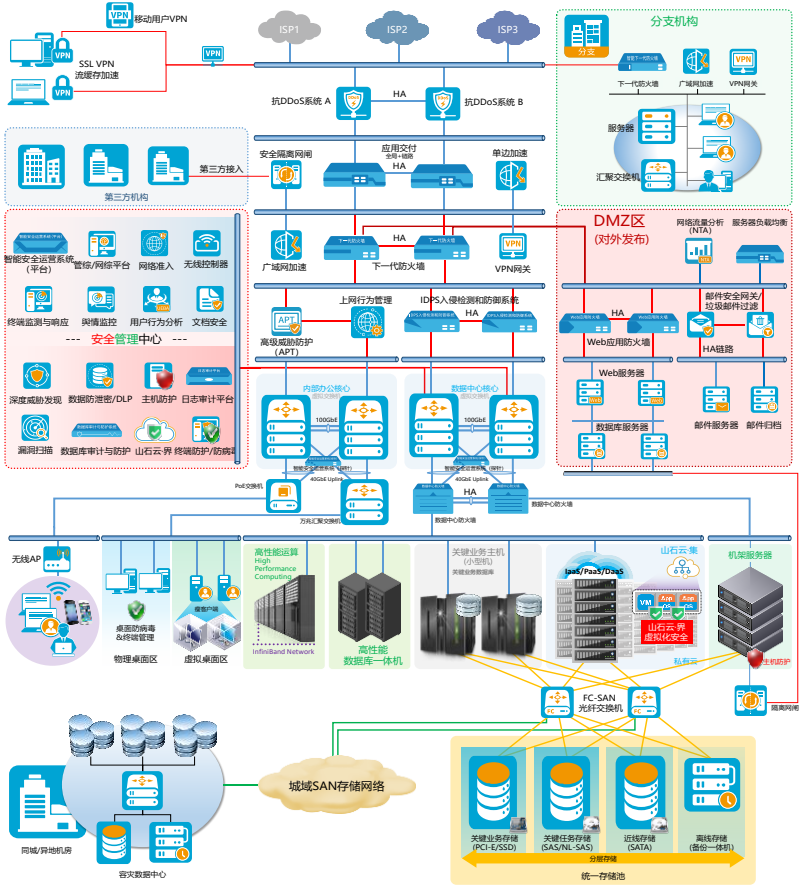
**方案重合性太高**

在大多数情况下，解决方案都是经过一个模板、上个类似方案修改而成，针对每个行业、每个客户的解决方案看似不同，其实殊途同归。

**方案延展、扩展性**

针对客户方案，很多时候都只考虑到当下客户需求而进行，多数解决方案的扩展性较差，只满足当下需求，而延展性也局限于本行业内，无法适用于其它行业、客户。

# 解决方案—通用IT架构下的融合方案




拓扑以下一代IT架构为详解，进行制作山石网科图标拓扑。

边界部分：多出口模式，外部通过VPN拨入，移动办公即为SSL VPN，第三方接入通过隔离网闸到边界安全，VPN有缓存、加速设备，同时保证解密后的流量能够通过安全设备过滤，应用交付做智能DNS、链路负载；出口第一部分为双机抗DDoS，在第一步拦截公网的DDoS攻击，然后通过下一代防火墙进行控制，外网部分通过APT到行为管理；内网部分则通过IPS到达核心。

DMZ：主要为Web、邮件等对外系统，针对不同场景使用不同的Server，而WAF、邮件安全则可以替换为其它安全设备，针对不同场景下使用；内部数据需要到后端数据中心进行数据同步时，通过网闸；

核心：内外网同时使用交换机虚拟化技术，二虚一的模式，同时使用探针收集内部核心流量，内外网隔离。

安全管理中心：囊括了态势感知、桌面、终端安全、文档安全、准入、无线控制器、舆情监控、行为分析、DLP、主机加固、虚拟化安全、数据库审计与防护、日志审计、漏扫、主机加固等管理加固类产品，此区域进行统一的管理、分析、监控。

数据中心：针对物理、私有云管控、安全加固，其中数据中心到核心流量保证都通过数据中心防火墙，可提升管理、流量审计控制的便携性。

容灾备份：备份通过Lan Free备份至备份一体机，同时通过SAN网络传至同城/异地备份中心。

P.S由于拓扑结构为纵向，此处展示为图片，原拓扑以对象文件的形式左图，双击即可。

# 优势价值—提升通用IT架构下的解决能力

整体方案优势：

- ❑ 满足相关法律法规，如等级保护2.0、网络安全法
- ❑ 保证信息安全事前可防御、事后可溯源
- ❑ 流量走向、数据存储、容错率、可靠性都能够保障
- ❑ 结构明朗、可操作性强、不同于场景化模式，但能兼容场景化模式

- ➢ 提升对于不熟悉客户环境下的前期交流
- ➢ 方案拓扑、产品融合能力提升
- ➢ 解决方案扩展性更高
- ➢ 减少场景化模式下的方案能力不足
- ➢ 不同场景下进行不同方案的快速输出
- ➢ 精准定位客户需求