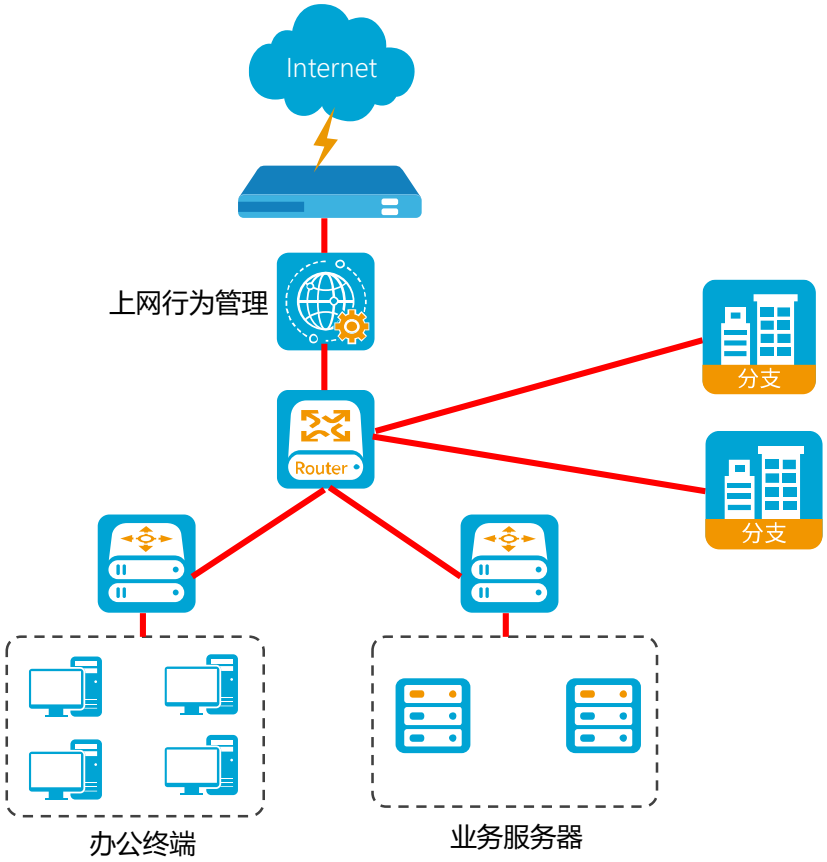

Hillstone
山 石 网 科
方案名称：企业网络安全解决方案
个人信息：张鑫-世纪华风科技有限公司

背景介绍—网络现状



当前网络现状描述

- 互联网出口采用防火墙连接一条线路，为电信ADSL 50M用于办公上互联网；
- 全网络核心为路由器，承担全网路由流量转发，并通过专线与分支进行互联；
- 有上网行为管理进行流量控制和上网行为控制；
- 接入交换机连接终端与业务服务器
- 2台服务器虚拟化后，提供虚机业务服务。

需求分析—网络问题

网络风险分析

问题分析：

1、网络设备使用时间较久，已经进入老化阶段，设备稳定性下降，性能无法满足；

2、缺少安全控制手段，网络入侵、病毒木马无法检测防护，安全风险无法控制；

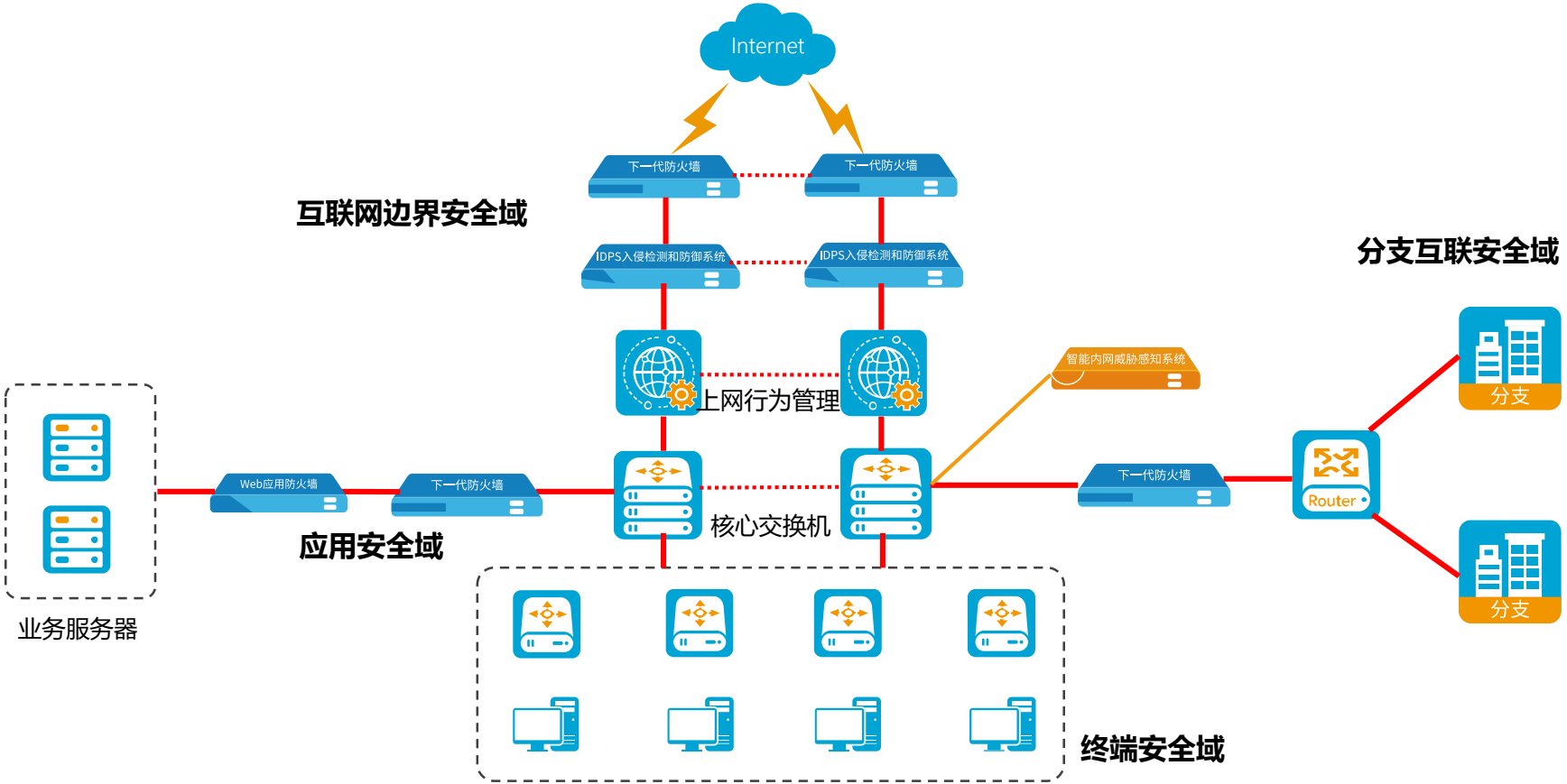
3、网络结构不合理，当前路由器做为网络核心，对网络扩展，网络调整改动十分麻烦；

4、分支专线网络接入没有安全检测和控制措施，入侵行为、木马病毒无法防护；

5、应用系统缺少网络控制措施，没有访问权限管理，应用系统缺少专业应用层防护手段，WEB攻击无法阻断，造成数据被篡改、窃取丢失等风险；

6、虚拟化平台内虚拟机东西向流量无法识别发现，虚拟机间存在随意的安全互访，易造成数据泄露，虚拟机被攻击后，无法进行网络隔离，缺乏威胁阻断措施。

解决方案—网络安全解决方案



方案介绍—解决方案介绍

- 将网络划分为四个安全域，分别为互联网边界安全域、应用安全域、终端安全域和分支互联安全域
- 互联网边界安全域： 1、增加一条其他运营商互联网ADSL链路

  2、出口冗余部署两台防火墙，实现链路负载、抗DDOS、NAT和VPN冷备份

  3、冗余部署两台IPS入侵防御系统，实现L2到L7层全面的网络入侵、木马病毒防护
- 应用安全域： 1、边界部署一台防火墙，实现端口级别访问控制，隔离不安全服务，封堵威胁行为

  2、部署一台WAF，对WEB应用进行安全防护

  3、Vmware虚拟化平台部署一套云格，实现虚拟机流量可视化、风险可视化，阻断安全威胁
- 分支互联安全域：1、在互联路由器后端串行部署一台防火墙，开启抗攻击、入侵防御、防病毒等功能
- 核心交换域：1、网络改造后，网络流量的中心为核心交换机

  2、旁路部署威胁感知系统，实现对高级威胁、未知威胁的检测发现并与防火墙实现联动防御