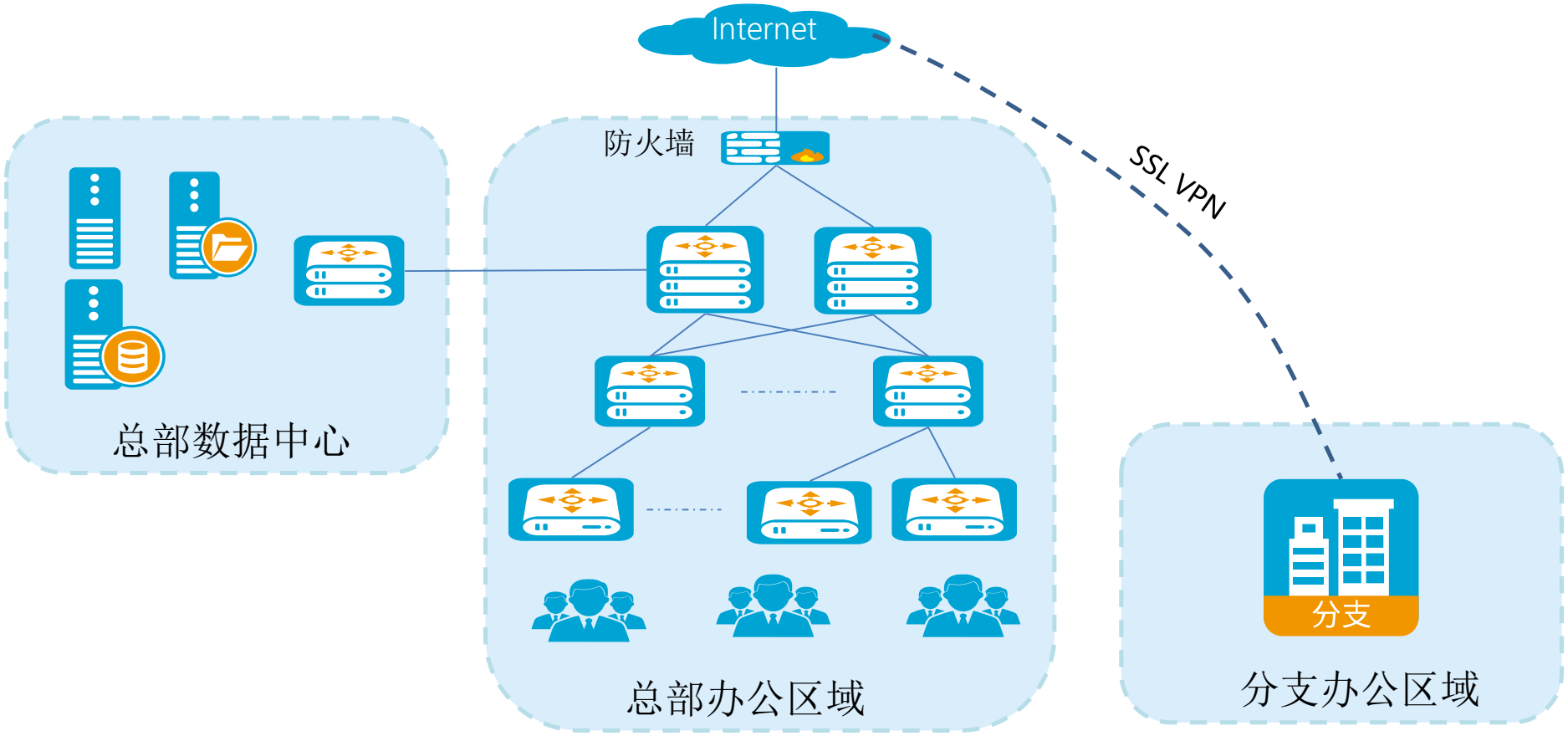
Hillstone
山石网科

Hillstone
山石网科

方案名称：企业网络安全防护解决方案

个人信息：刘飞-四川泰丰源信息工程有限公司

背景介绍—企业网络安全现状



总部

总部出口部署一台防火墙，并配置SSL VPN。规则库已经停止更新。

分支

分支通过SSL VPN访问总部数据中心。

需求分析—企业网络安全面临挑战

- 企业网络安全面临挑战：

边界安全

网络边界的模糊化以及黑客攻击的产业化使得网络安全事件相较以往成指数级的增加，新型安全事件如网站被篡改，被挂黑链，0 day漏洞利用，数据窃取，僵尸网络，勒索病毒以及一些未知威胁等等层出不穷。

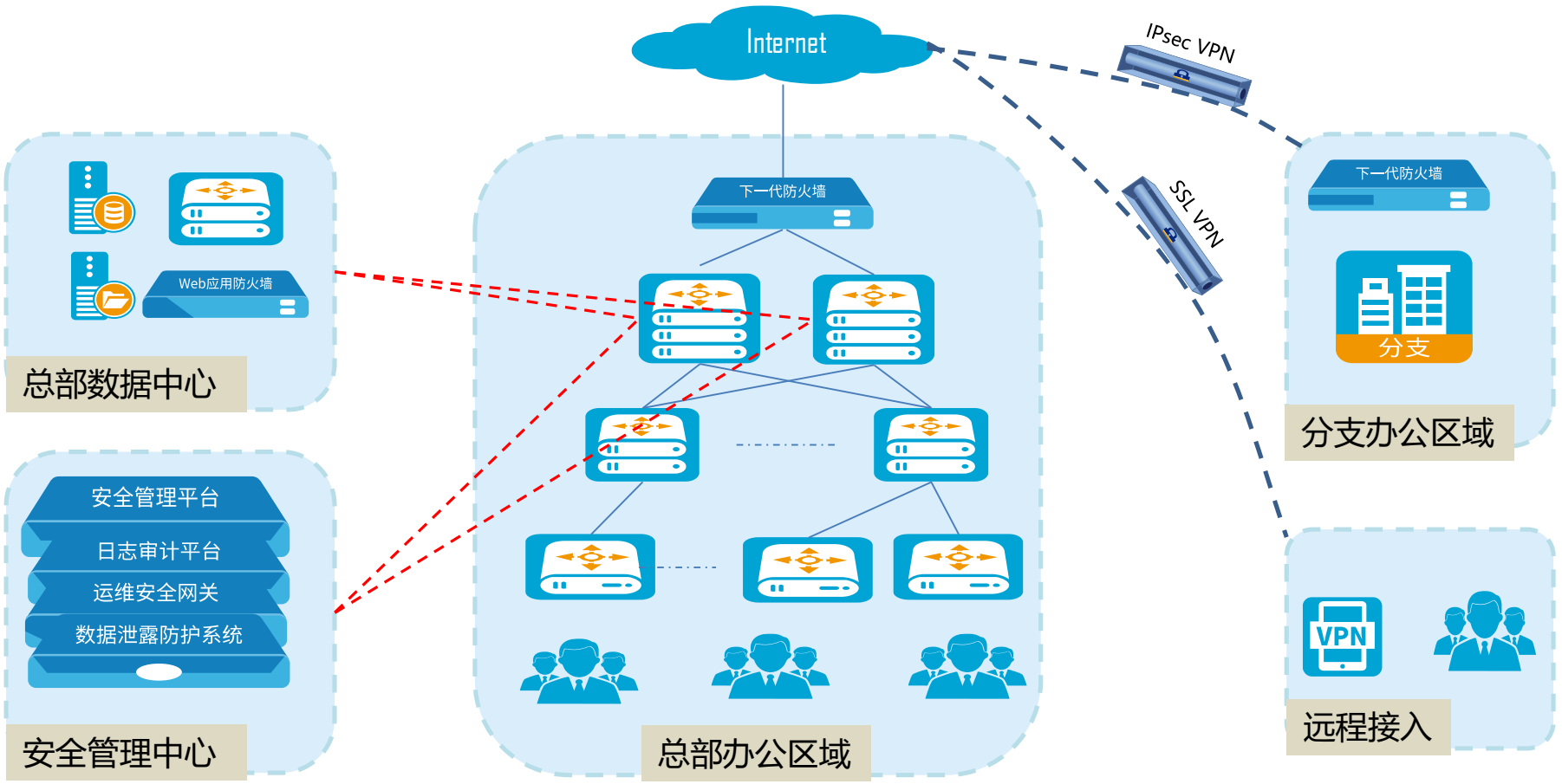
数据中心安全难以保障

数据中心区域区含了内部所有系统，存放了内部网络的所有数据，同时也最容易遭受攻击。据调查显示，服务器频频发生数据窃取、网页篡改、勒索病毒等危险事件。。

运维安全

传统的局部、碎片化的IT运维管理模式已经无法满足安全生产的实际需要。

解决方案-山石网科企业网络安全方案



数据中心

总部数据中心部署WEB防火墙
安全管理中心部署安全管理平台
安全管理中心部署日志审计
安全管理中心部署运维安全网关
安全管理中心部署数据泄露防护系统

总部办公

总部办公部署下一代防火墙
配置VPN功能

分支、远程接入

分支部署下一代防火墙
配置VPN。

优势价值—山石网科企业网络安全方案

边界安全

通过下一代防火墙做访问控制、入侵防范、恶意代码防范以及安全审计等安全防范。

分支互联、移动办公

通过IIPsec VPN和SSL VPN,保障分支机构和出差人员安全可靠的接入总部业务系统。

数据中心安全防护

通过启用防火墙、入侵防护、漏洞检测、敏感信息防泄漏、DoS/DDoS攻击防护、防病毒、防扫描、弱口令检查、防僵尸网络、web应用攻击保护、网站篡改保护等功能，可以实时发现数据中心业务系统区域隔离，避免因业务系统漏洞导致的入侵，防范病毒、蠕虫、僵尸网络等威胁内容在数据中心传播，防止口令密码被暴力破解，避免数据中心敏感信息被泄露，清洗数据中心异常流量，保护数据中心web应用安全，保障数据中心网络和业务安全运行。

运维安全

运维安全管理系统（堡垒机）以身份鉴别、访问控制、安全审计等监管要求为核心，基于"账号、认证、授权和审计"4A管理理念，采用三权分立和最小访问权限原则，实现精准的事前识别、精细的事中控制和精确的事后审计，帮助企业转变传统IT安全运维被动响应的模式，建立面向用户的集中、主动的运维安全管控模式，降低人为安全风险，满足合规要求，保障企业效益。