Hillstone
山 石 网 科

方案名称：卫健委等保三级建设方案

个人信息：戴虓晨-苏州市永嘉信息科技有限公司

Hillstone
山 石 网 科

背景介绍—政府机构网络现状

- 内网主要提供HIS、LIS等系统应用，同时提供对外服务，比如门户网站、医疗保险等。
- 外网提供办公人员访问互联网。
- 通过电信专线与各社区卫生服务中心及社区医院互联。
- 通过电信专线与各社区卫生服务中心及社区医院互联。
- 网络安全建设较为薄弱，仅有深信服防火墙一套，以及天融信相关设备。服务器区域也无安全防护设备。内网整体无全面的防护手段，无法及时对各系统交互，人员访问，业务发布做访问控制，威胁监测等。安全威胁隐患较高。不能满足等级保护三级建设要求。

需求分析—政府机构面临挑战

- 等级保护制度建设前面临的威胁：

移动办公数据被窃听和篡改

随着医疗交流活动，医药体制改革，防控疫情活动的广泛开展。使得很多业务通过互联网平台被传递。而众所周知的互联网开放性，使得以明文的方式在网络中传递数据时，数据很容易遭到窃听、篡改和重放攻击。

不规范上网行为带来的风险

人员在过度使用互联网资源的同时，严重的降低了工作效率，同时访问互联网上的非法恶意网站，所产生的后果会直接影响到整个信息系统的安全。为此应当通过相应的技术手段和管理手段对上网活动进行有必要的控制和日志审计。

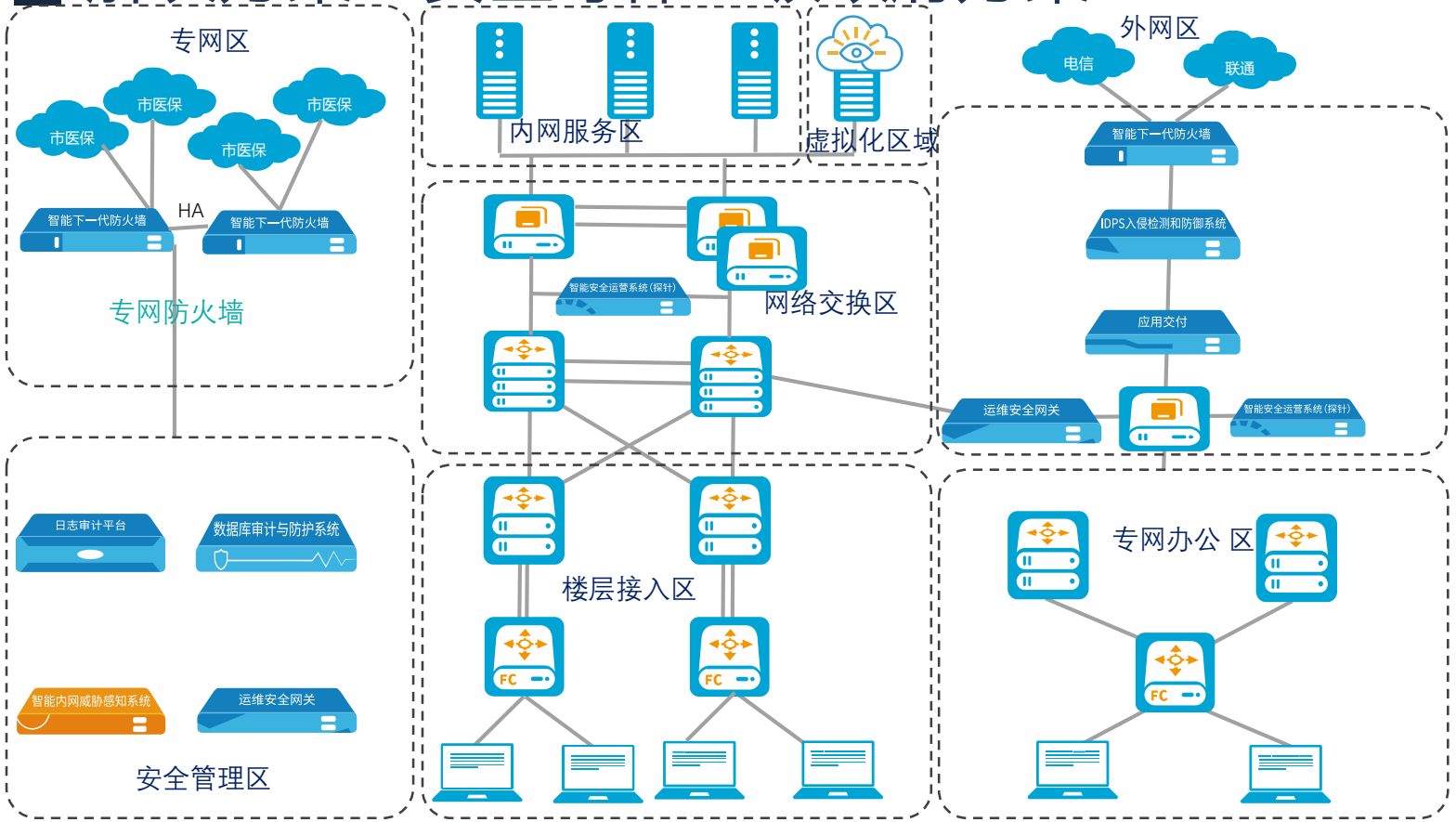
内外网数据交换带来的潜在威胁

内网运行着最重要的业务信息系统，其业务重要性程度要远远高于外网，但随着支付宝网上诊疗、网上咨询、移动办公等业务的开展，内网与外网的数据对接交换已成为必然，但与此同时外网的安全隐患，也会对内网造成冲击，包括病毒的传入、黑客的跳板攻击、黑客的临近攻击等。

互联网威胁

一些新业务的建设危险端口的暴露进一步对互联网出口的安全控制提出了要求，基于互联网的开放性，往往使得网络会面临众多的安全问题，包括互联网上蠕虫病毒的传播、互联网上黑客的渗透，内部职工对互联网资源的过的访问等。

解决方案—安全等保三级政府方案



部署说明（新增）

核心前置边界:
防火墙
入侵防御
负载均衡

专网边界:
防火墙（启用HA）

虚拟化区域:
云格（保护私有云内部东西向的流量）

运维管理区:
网络安全审计
运维管理系统
数据库审计系统
态势感知平台

优势价值—安全等保2.0助力政府

- 网络安全边界基础防护：通过将防火墙部署在不同安全域之间，使得防火墙成为不同网络或网络安全域之间信息的唯一出入口，能根据安全策略控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。
- 有效抵御种类攻击：利用IPS对缓冲区溢出、SQL注入、暴力破解、DDoS攻击、扫描探测、蠕虫病毒、木马后门等各类黑客攻击和恶意流量进行实时检测及报警，并通过与防火墙联动、TCP Killer、发送邮件、安全中心显示、运行用户自定义命令等方式进行动态防御。
- 提供上网访问行业的监管和审计功能：下一代防火墙的NAT、IPS、上网行为分析等功能，能够有效记录接入用户的网络日志和安全日志，可以帮助用户解决网络出口日志审计的困扰，并为用户提供了丰富便捷的日志查询功能，满足《网络安全法》及上级单位的监管要求。
- 降低数据安全风险：数据库静态审计代替繁琐的手工检查,预防安全事件的发生。依托其权威性的数据库安全规则库，自动完成对几百种不当的数据库不安全配置、潜在弱点、数据库用户弱口令、数据库软件补丁、数据库潜藏木马等等静态审计，通过静态审计，可以为后续的动态防护与审计的安全策略设置提供有力的依据。
- 节约带宽成本：应用交付AX系列支持专利技术的被动链路探测技术，解决链路利用率不均衡、单点故障、跨 ISP 访问效果差、链路资源浪费等问题,保障业务的稳定性。
- 精确定位攻击：智·源具备全息数据采集的能力，通过各种类型的数据探针采集数据，基于海量网络流量、威胁事件和终端日志等进行智能数据挖掘及分析，呈现全局网络安全及威胁态势。
- 加强云安全防护：虚拟化安全防护系统，深入到虚拟化内部，实现基于VM和VM组间的安全防护策略，通过虚拟交换机vSwitch固有的特性，将虚拟机间的流量牵引到虚拟防火墙的上，实施过滤，保障不同VM业务之间互访时的受控性和安全性。 同时基于用户、应用和威胁的角度，统一呈现虚拟化数据中心VM间的流量，进而进一步实现对VM间流量的控制和安全防护。

Thanks

Hillstone
山石网科

为您的安全竭尽全力！

400-828-6655

https://www.hillstonenet.com.cn