

棱镜业务互联流量监测系统

FBA V3.0



产品咨询：13910518989 何先生



棱镜科技企业介绍

企业文化 Company Culture

企业精神

诚信务实 追求完美
坚持创新 持之以恒

企业文化

简单做人 高效做事
鼓励创新 迎难而上

经营理念

明德诚信 敬天爱人
和润于心 兼烛天下

企业愿景

成为智慧城市信息化领域一流
的产品、服务和解决方案提供商

公司简介

北京东方棱镜科技有限公司成立于2014年，是专业从事信息安全产品研发、生产和销售的公司，由一群多年在网络安全领域勤奋耕耘的资深人员创立。面对当前“群雄逐鹿”、“诸侯割据”但又缺乏创新的安全市场局面，APT攻击、数据泄密、病毒木马大行其道，安全事件防不胜防并且与日俱增，传统的“老三样”已经严重无法解决当前严峻的网络安全和信息安全难题，未发现和潜在的安全隐患是最危险的。我们选择了在蓝海中开拓，即使前方布满坎坷和荆棘也要勇于做信息安全行业的探路者，用全新的视角诠释网络安全和信息安全。

沈阳公司成立
成为中航工业提供商
2012年5月

北京公司成立
智慧城市解决方案提供商
2014年6月

2010年3月
阜新公司成立
立足工业控制网络安全

2013年8月
内蒙公司成立
成为边防安全提供商



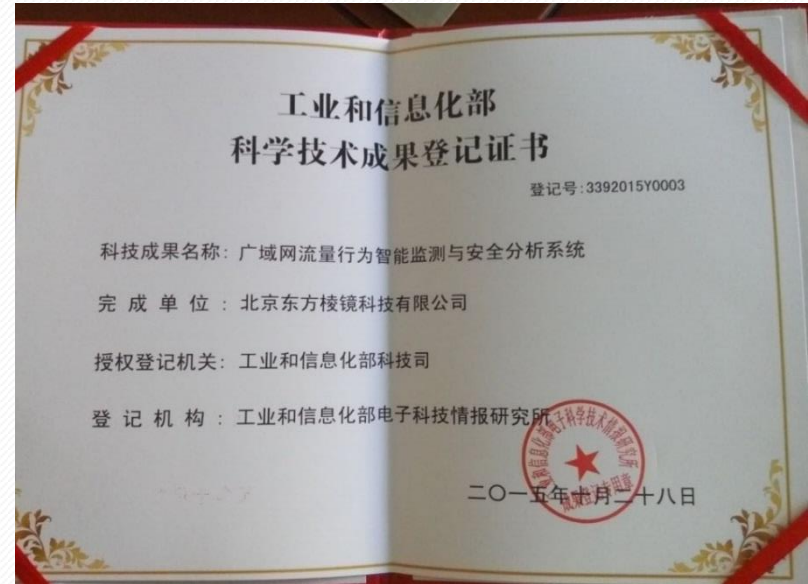
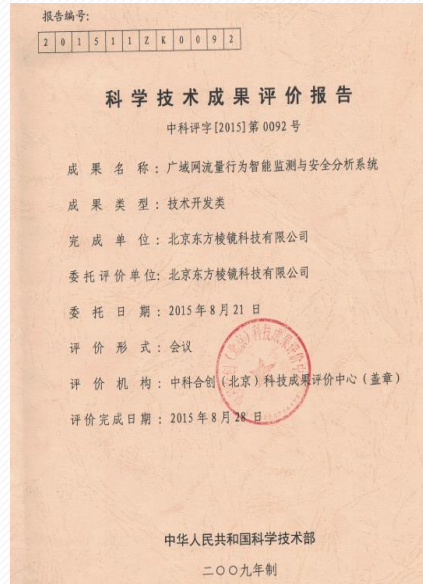
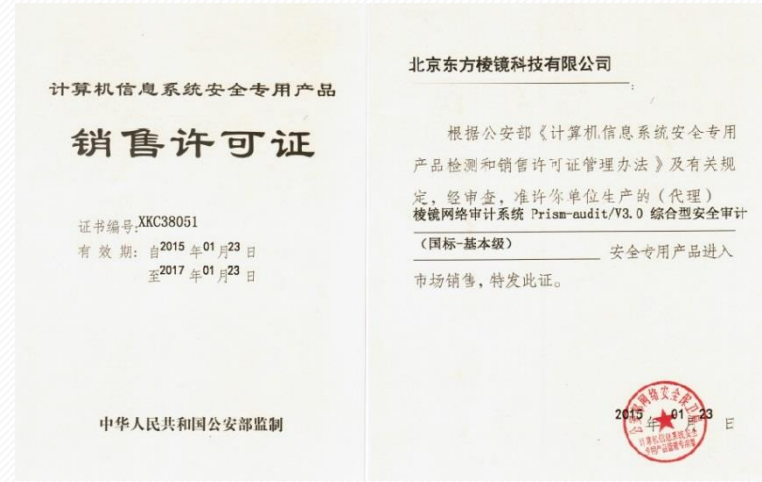
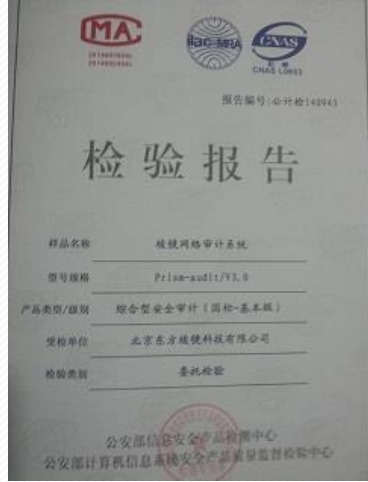


棱镜科技产品体系介绍





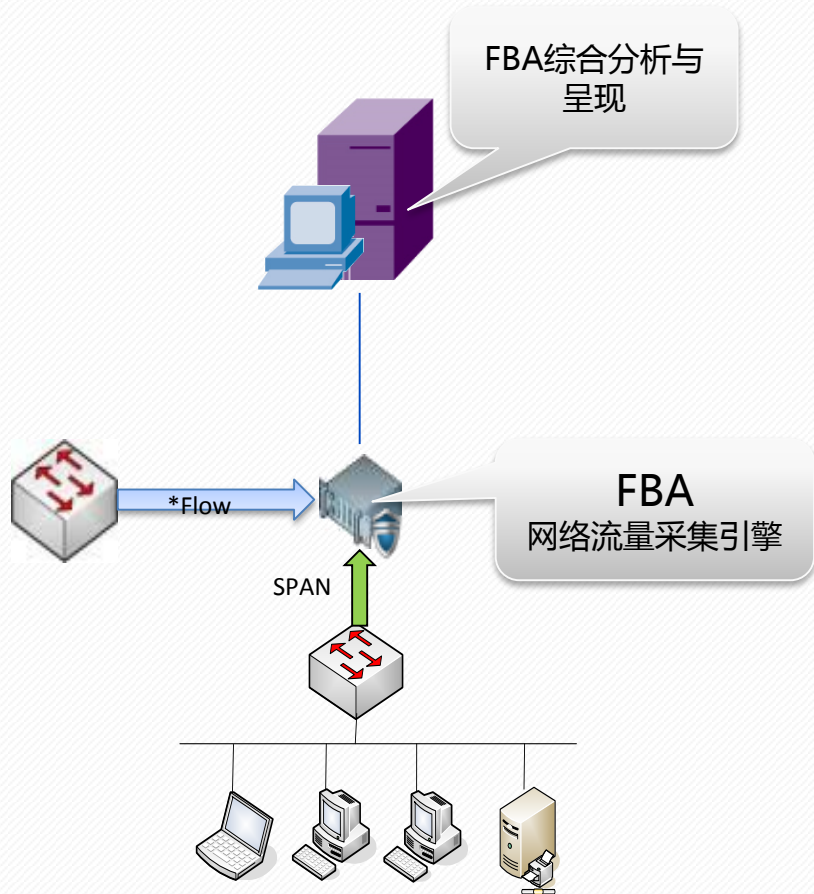
公司产品资质情况





FBA系统——先睹为快

面向连接的业务行为安全检测产品



是什么？

部署在网络安全域边界处，实现网络通讯流量的可视化与存储，进行通讯行为的秩序分析，以此发现安全风险（包括入侵和违规）

长什么样？

- ✓采集引擎为硬件盒子，千兆
- ✓可多路抓包，旁路镜像方式采集Flow
- ✓FBA综合分析及呈现为软件，也可提供软硬一体化设备



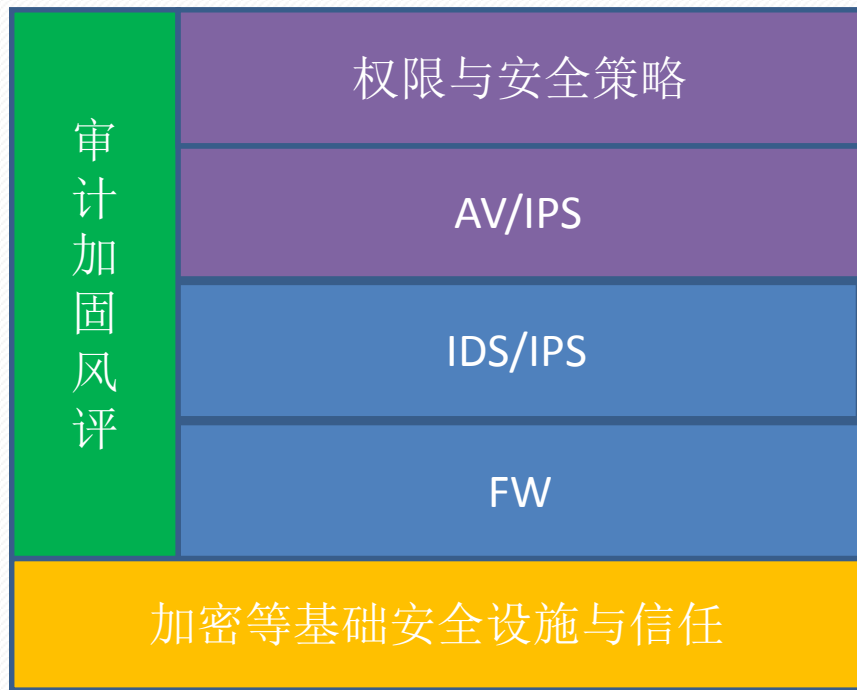
核心技术

- ✓创新的PcapStream流描述语言
——将网络流量转化成了设备间的互联事件
- ✓基于秩序的异常检测
——是基于互联行为的分析，而非基于特征的分析





以设备互联检测为基础的未知安全威胁监控利器



基于已知知识:

已知安全漏洞与缺陷
已知木马行为与特征
已知攻击行为
明文泄密
限定的权限

难以应对:

未知安全漏洞与缺陷
未知木马行为与特征
未知攻击行为
加密传输
社会工程
厂商后门

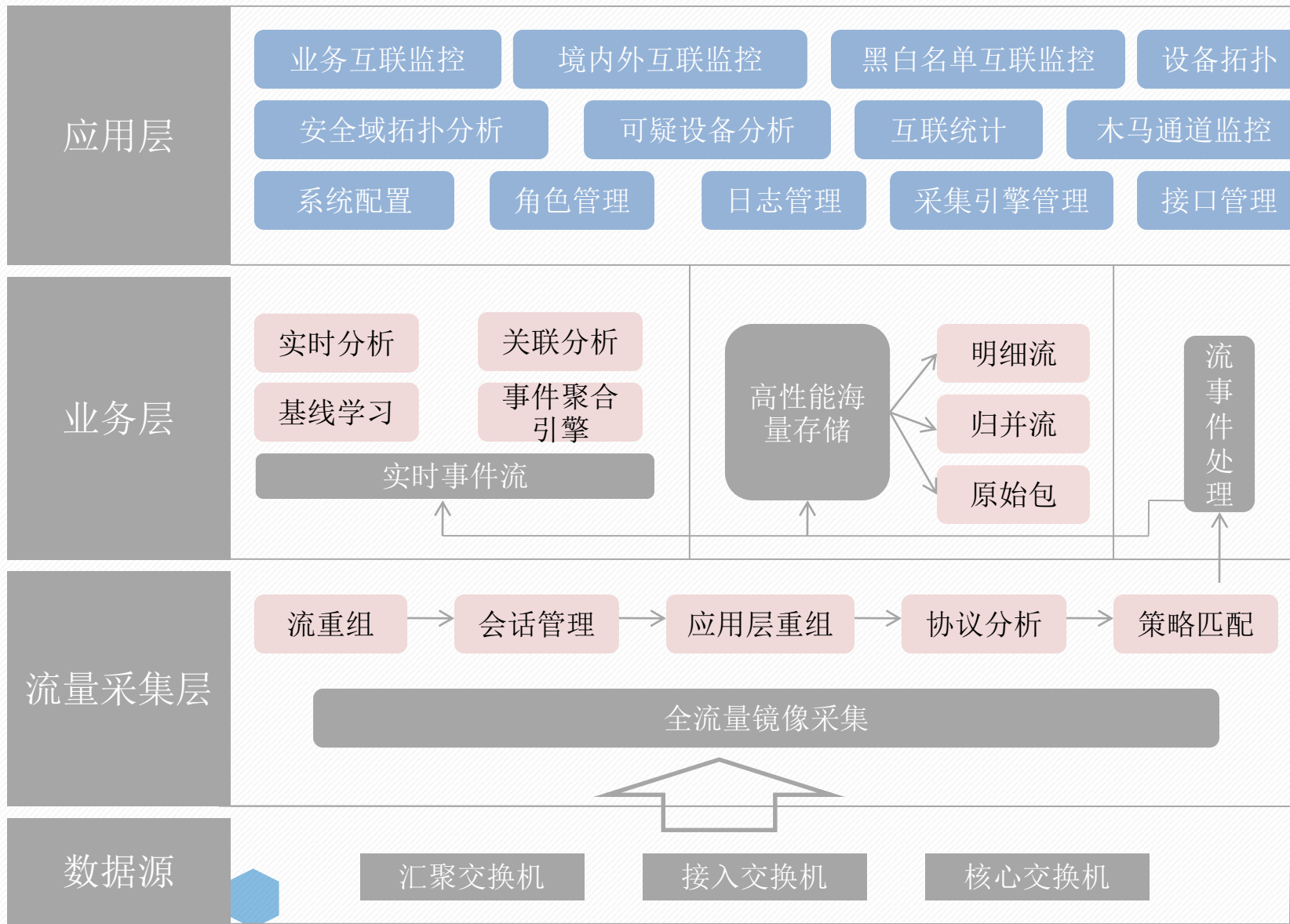
新安全形势下，传统安全产品已经**穷途末路**

然后所有客户却在迫切需要感知和预判威胁！



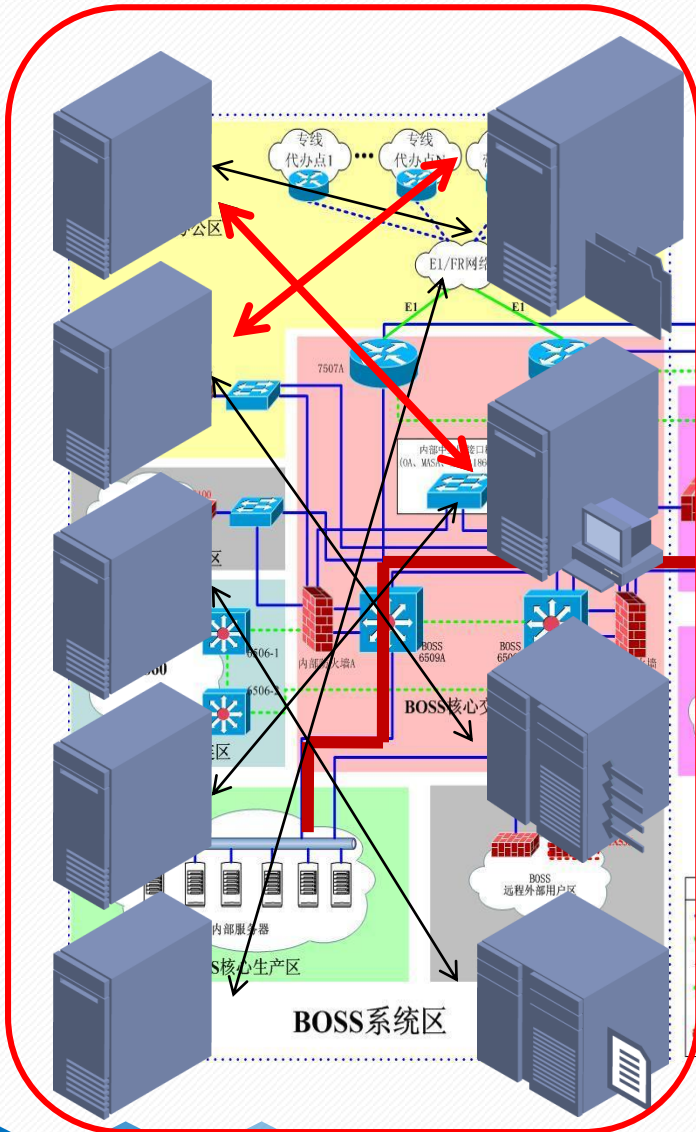


FBA系统功能架构



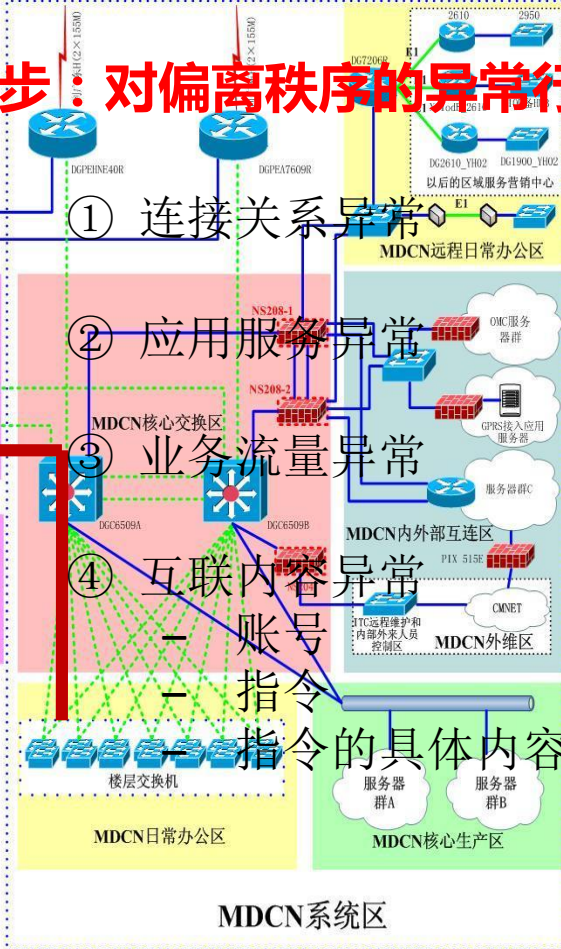


基于秩序安全的业务互联合规检测（关注七层协议）



第一步：建立设备间访问秩序基线

第二步：对偏离秩序的异常行为进行告警



① 连接关系异常

② 应用服务异常

③ 业务流量异常

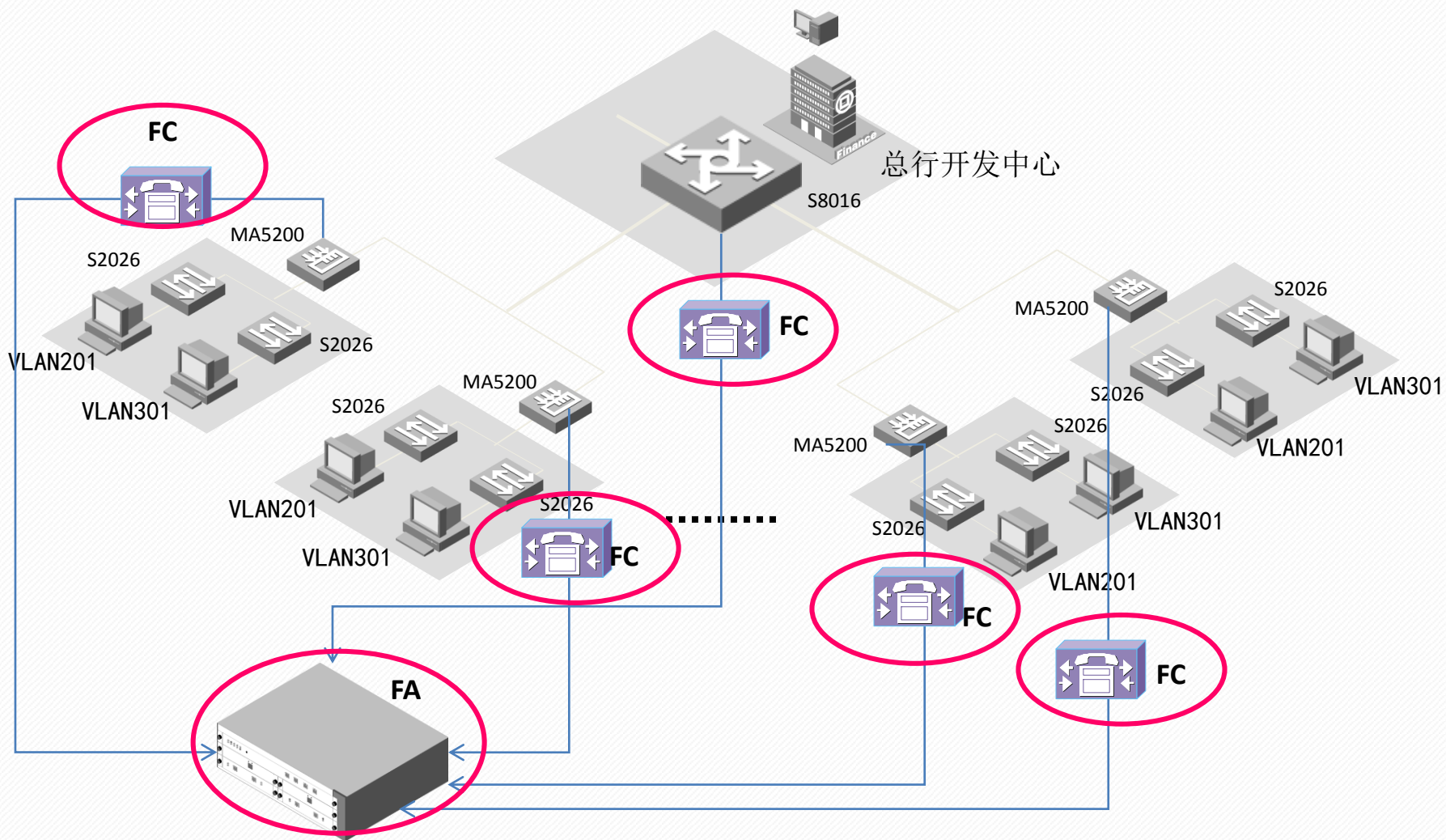
④ 互联内容异常

— 账号
— 指令
— 指令的具体内容等





支持多级级联部署

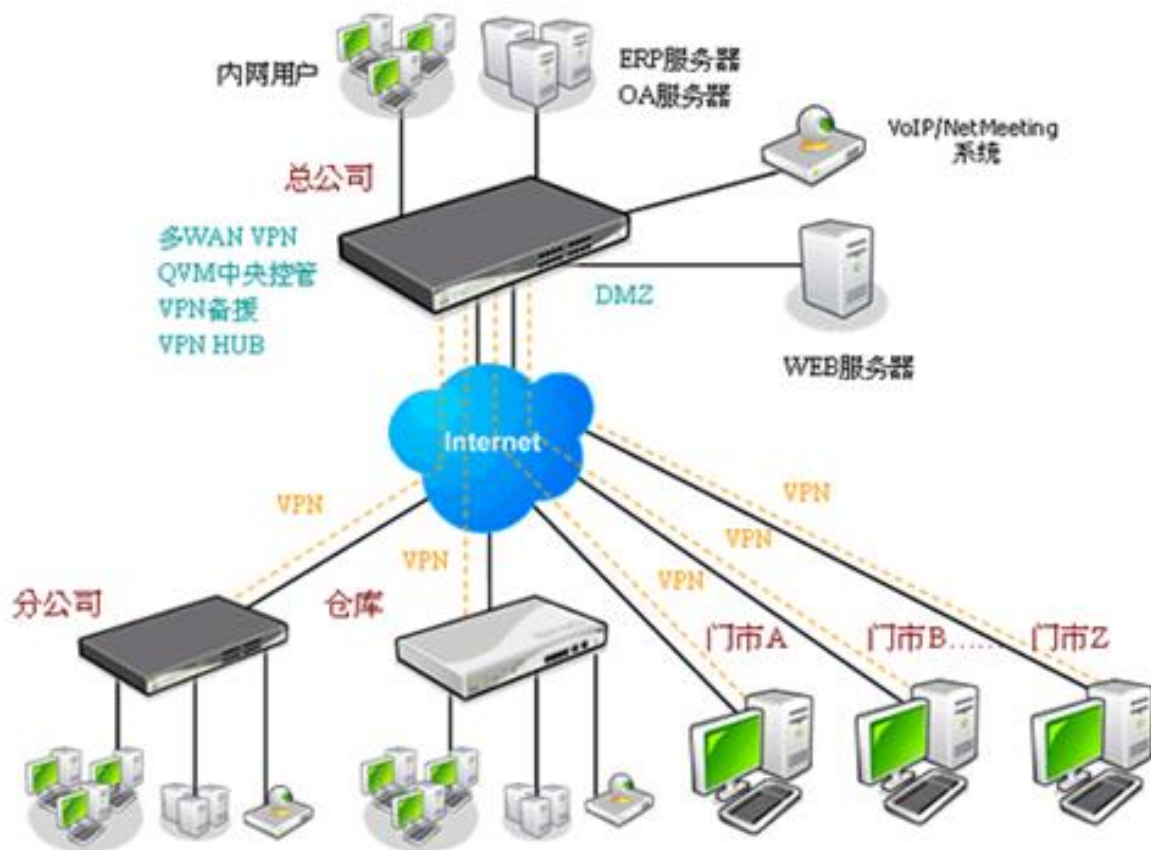


■ 集中展现分析、分布式采集数据的架构





IT运维管理价值

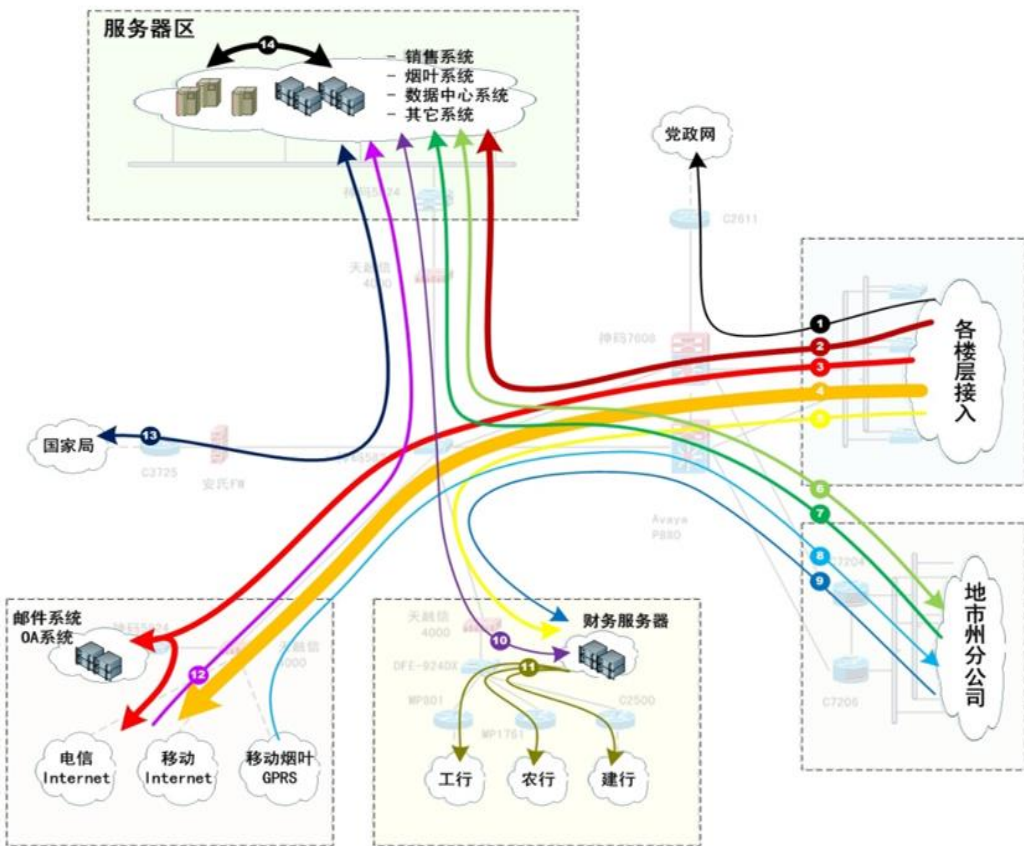


1. 哪些设备之间有互联关系?
2. 设备开放了哪些端口和服务?
3. 防火墙策略设置是否准确?
4. 设备之间互联频次如何?
5. 设备访问中断故障原因定位?
6. 哪些设备之间的访问是违规或异常访问?
7. 是否存在非法设备接入?
8. 是否存在境内/境外互联情况?
9. 是否存在可疑木马、可疑APT攻击情况?





IT业务系统运营价值



1. 业务系统软件是否存在设计隐患?
2. 全网业务流向最新状态如何?
3. 业务系统中访问频繁的页面功能有哪些?
4. 业务系统是否存在违规或非法访问?
5. 业务系统访问中断故障原因定位?
6. 业务系统访问流量趋势如何?
7. 业务系统访问负载均衡效果如何?
8. 是否存在境内/境外互联情况?
9. 是否存在可疑木马、可疑APT攻击情况?





棱镜科技产品特点和优势

一、产品功能简单易用

产品具有多项专利安全分析算法技术，整合了黑客攻防知识，集成了异常流量检测、入侵检测、应用协议识别、恶意IP地址库等知识库。使得安全管理深入浅出，体现软件“简单就是美”。

二、图形可视化

以可视化图形的方式展示异常业务流量和企业安全风险，帮助企业更轻松地发现潜在的恶意入侵和违规行为；

三、自动、定期提交安全分析报表。

以报表的方式自动、定期提交安全管理建议。

四、基于旁路的产品部署方式

不会影响客户网络中的业务运行，不会给客户带来任何业务风险。



产品咨询：13910518989 何先生

谢谢

THANKS !