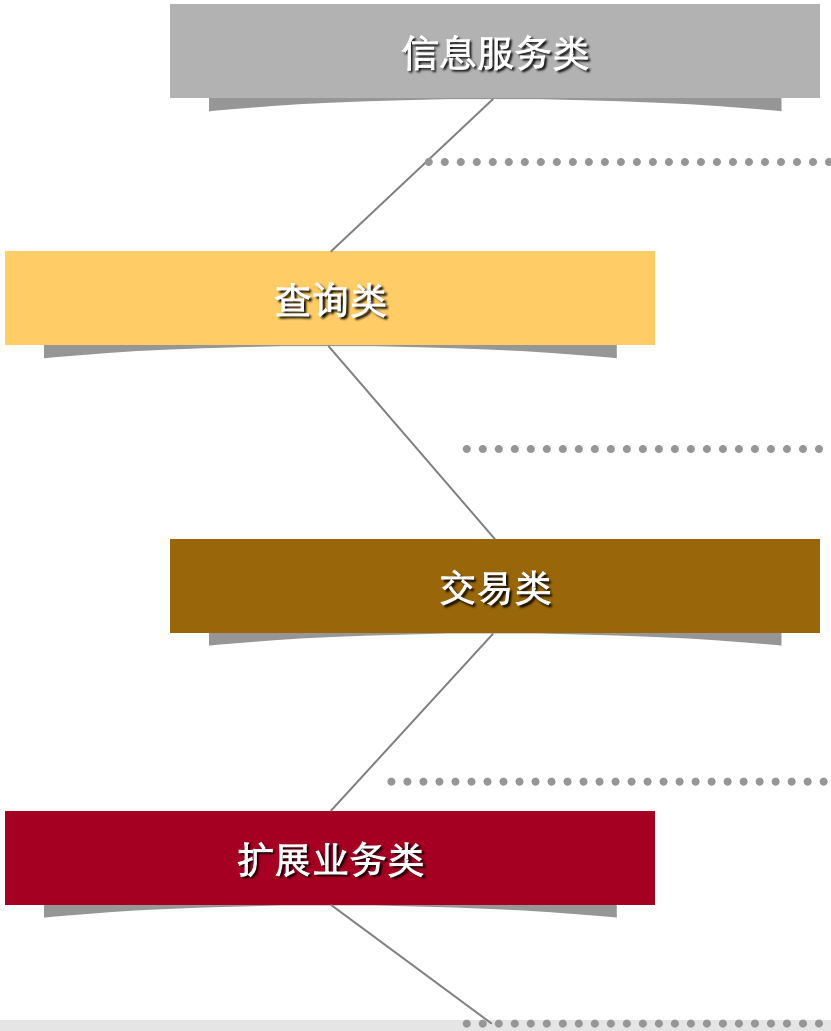
体验、安全、可信
—华为网银安全解决方案

www.huawei.com

HUAWEI

目录

网银当前业务介绍



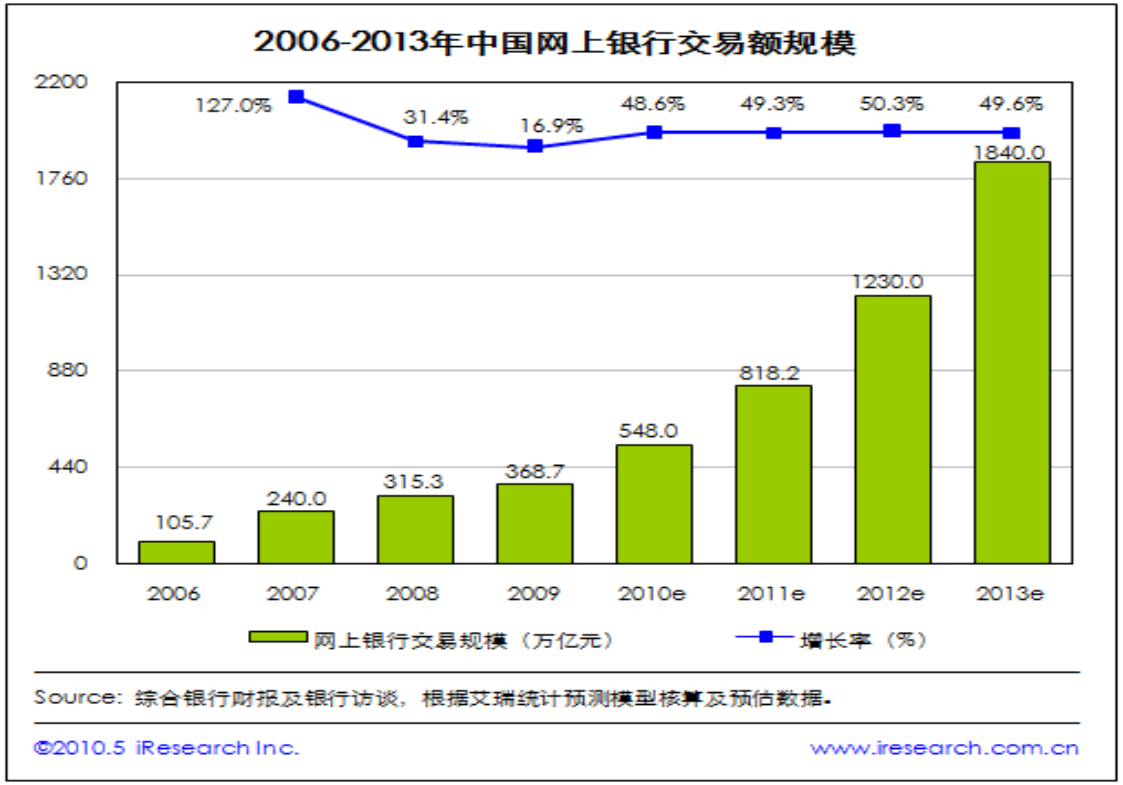
- 银行基本信息发布、银行业务品种的介绍、银行储蓄网点、自动柜员机 ATM网点和特约商户的分布情况

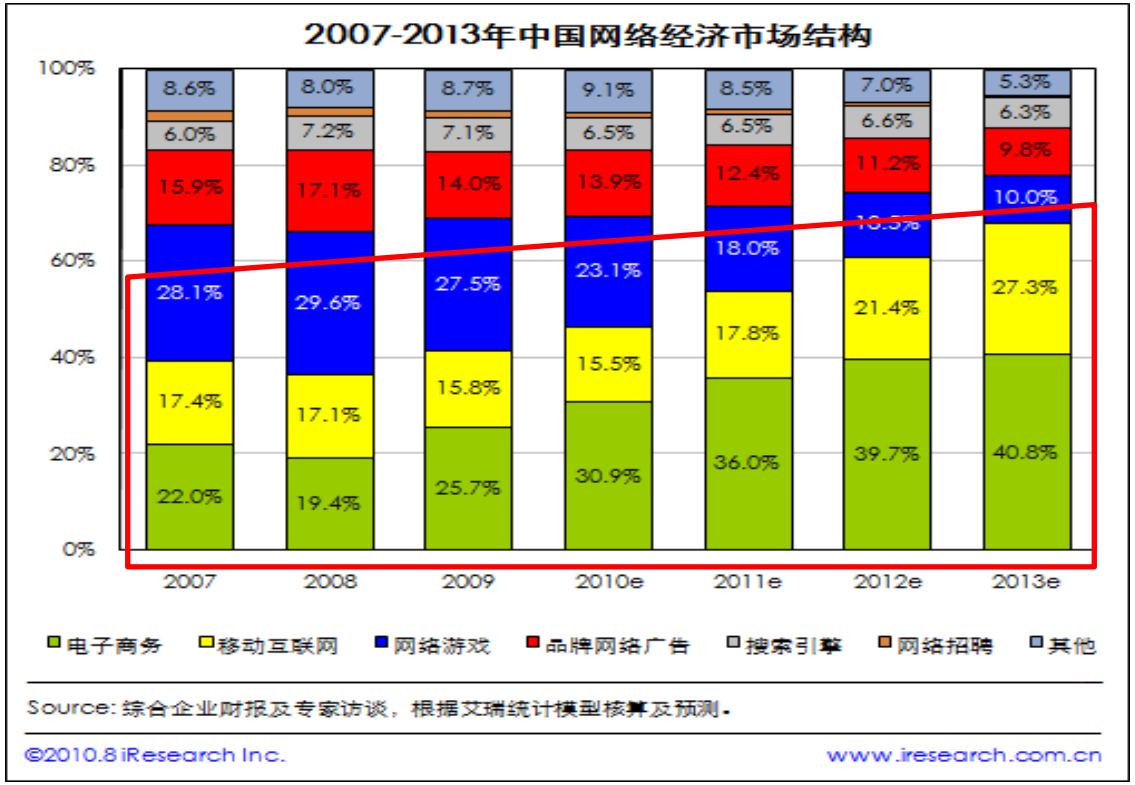
- 个人综合帐户余额查询、个人综合帐户交易历史查询
- 企业综合帐户余额查询、企业综合帐户交易历史查询、支票情况查询、企业受信额度查询、企业往来信用证查询
- 客户贷款帐户资料查询、汇兑状态查询、利率查询

- 网上转帐（即实现网上银行签约帐户之间的转帐）、网间转帐（即客户可将网上银行帐户的款项转入综合业务网络其它帐户）
- 代收和代付费业务（比如从活期或信用卡帐户代扣代缴日常水费、电费、煤气费、电话费和公用事业付费等）
- 个人小额抵押贷款、个人外汇买卖、企业外汇买卖、换兑等

- 企业银行服务、中间业务如证券交易、网上购物和网上支付、移动电子交易等，与Call Center和CRM结合提供个性化金融服务

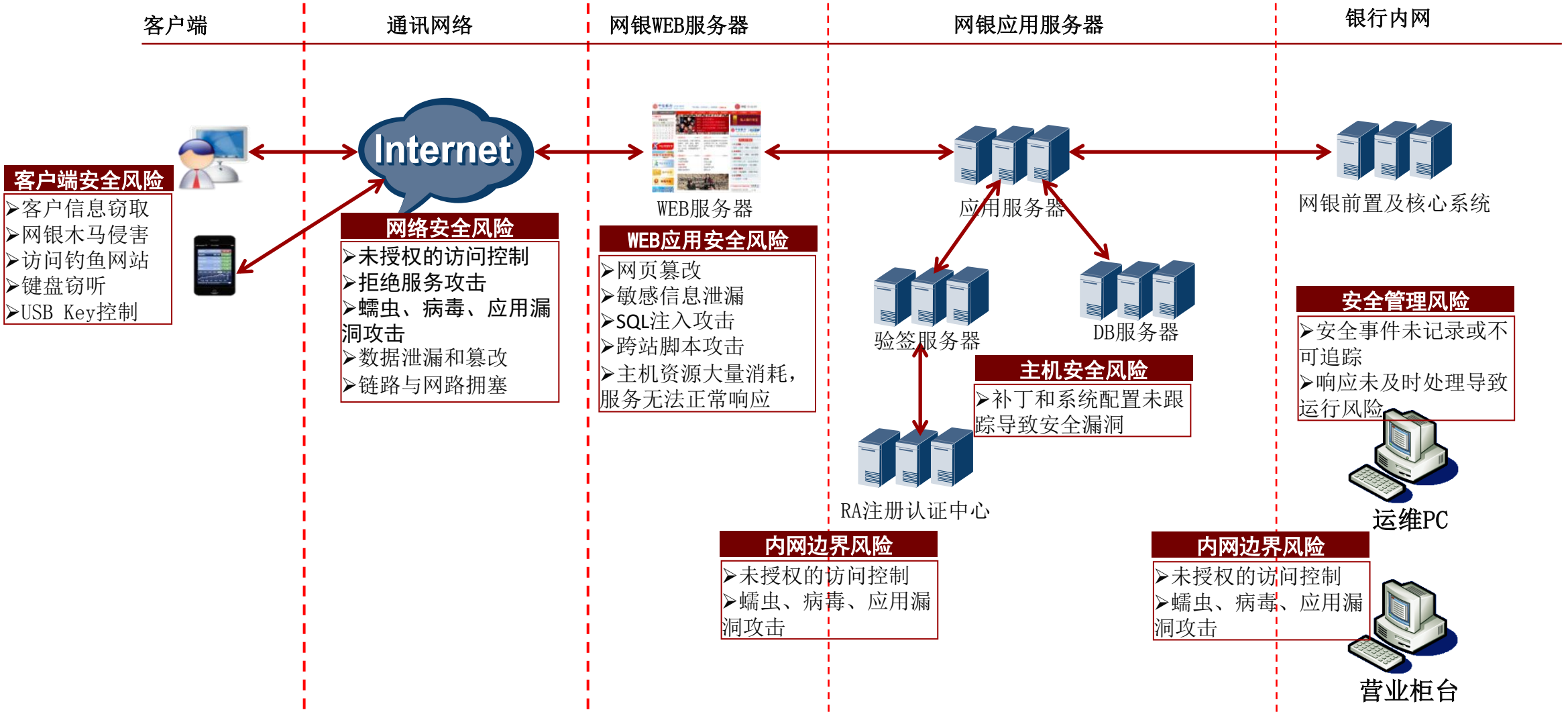
网银业务发展趋势





- 互联网和电子商务的发展给网银带来了新的挑战与机遇
- 手机网银、移动支付和钓鱼网站的防护成为网银安全新的课题

网银面对的安全威胁与挑战



目录

网银安全建设目标

端到端安全目标

- 为远程用户提供安全的会话、并发与时间控制
- 对用户从边界外发送和接收信息进行强身份认证和访问控制
- 为密码提供生命周期保护
- 接收方、发送者和攻击者信息可追查、防抵赖
- 提供服务与资源，阻止非法用户访问用户隐私
- 数据传输过程的防修改、防伪造

系统边界安全目标

- 物理与逻辑边界保护
- 边界系统与网络可用性保障
- 边界安全行为的可检测、审计与响应

本地计算安全目标

- 服务器可用性保障
- 应用和数据的机密性、完整性
- 内部与外部攻击行为审计
- 管理员操作审计
- 审计数据的保护
- 补丁与系统加固跟踪与评估
- 系统连续性和失效恢复保障

网络通信基础设施安全目标

- 局域/广域网网络通信可用性保障
- 网络上传输数据的机密性、完整性保护
- 重要业务流量（如用户流量、网络设施控制流量）免受影响
- 确保保护机制不会干扰骨干网和封闭网络的无缝操作

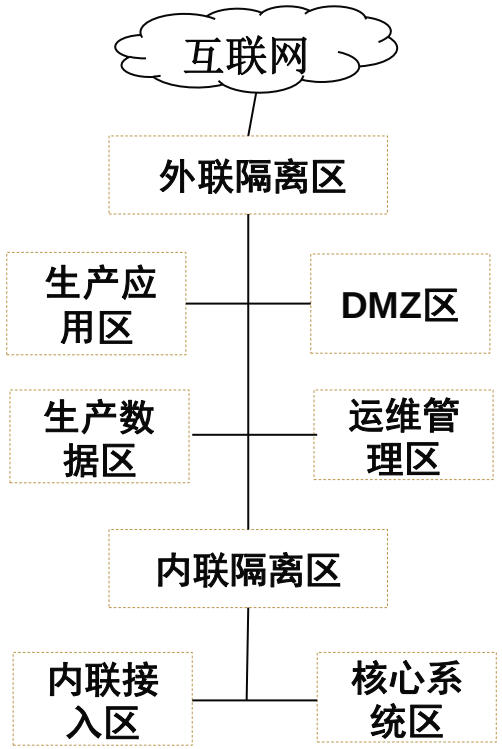
支撑性基础设施安全目标

- 密钥与证书的提供和识别
- 入侵与违规事件的检测、分析、响应与报告机制

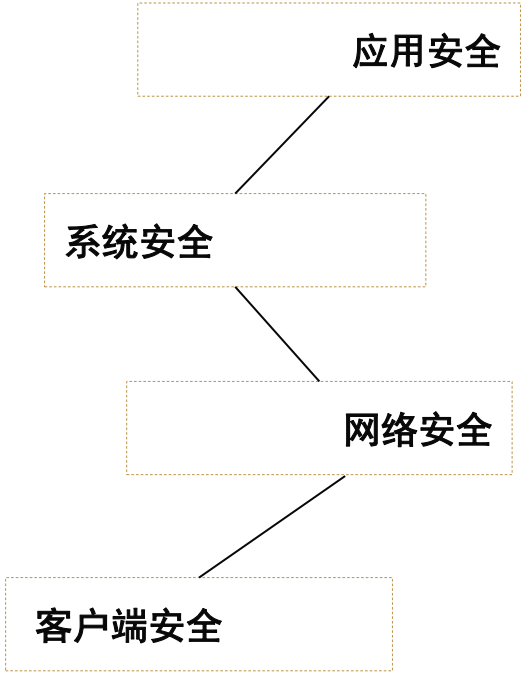
网银系统和数据的完整性、可用性、可追查性、保密性和抗抵赖性

华为网银安全解决方案设计思路

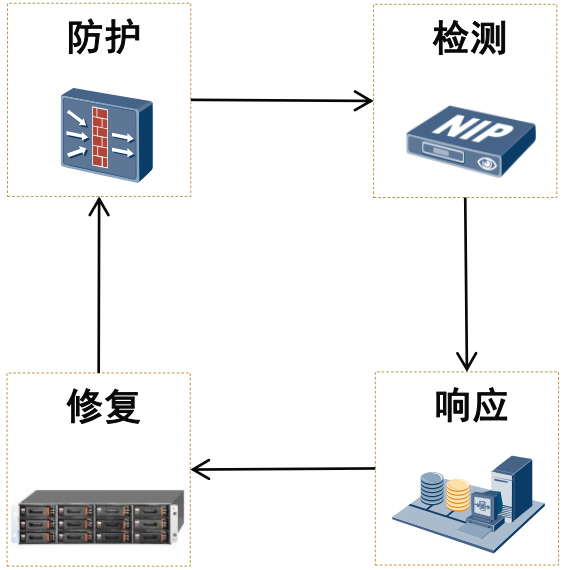
合理的IT逻辑架构



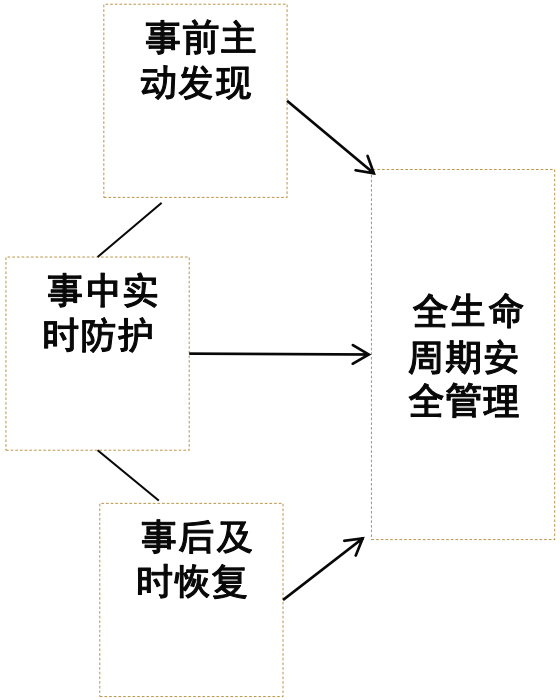
端到端的安全防护



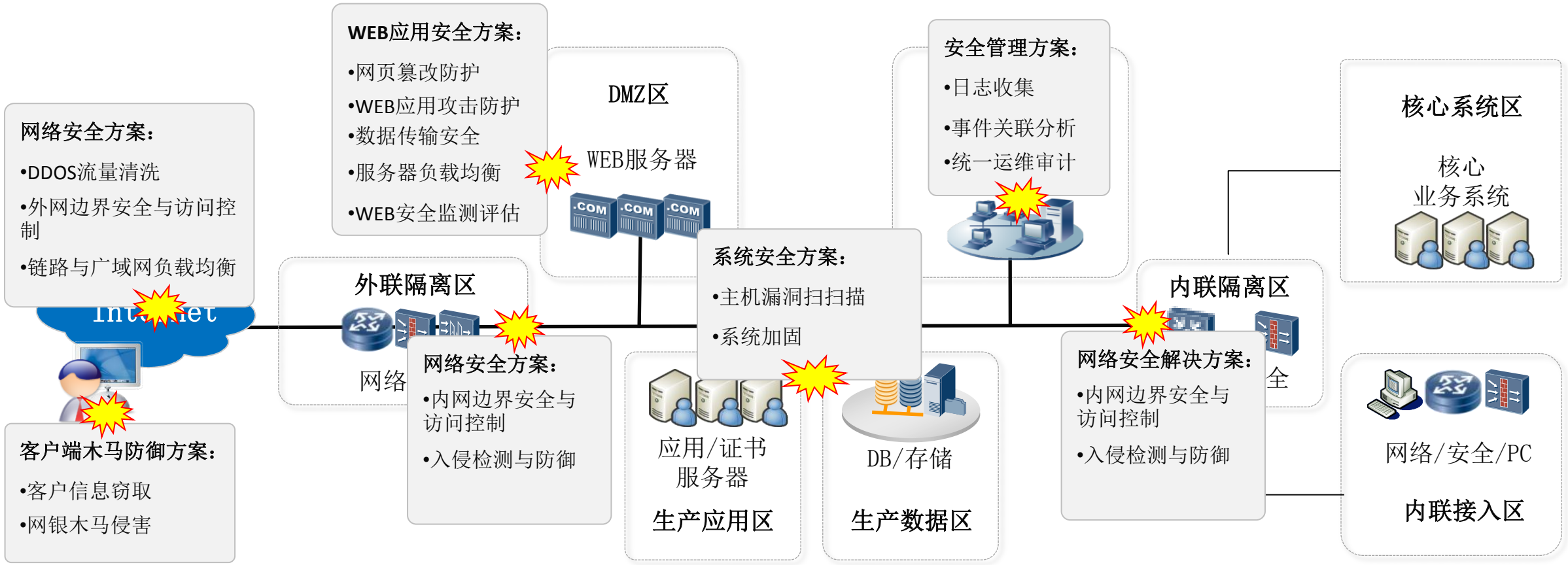
动态的安全闭环



全生命周期的安全管理



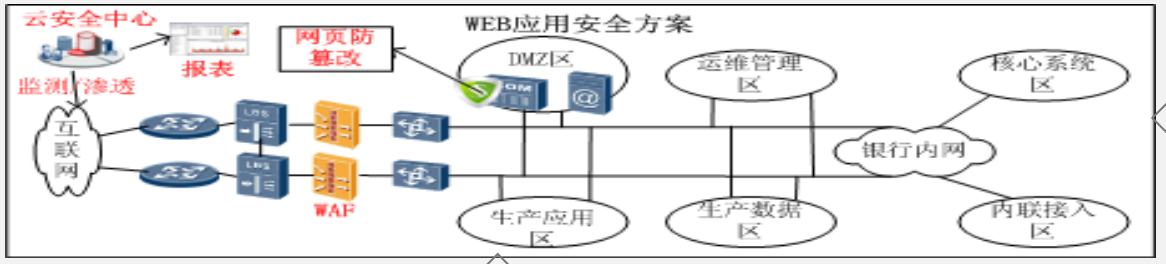
华为网银IT逻辑架构设计



合理的网银IT逻辑架构是网银安全的前提和基本保证

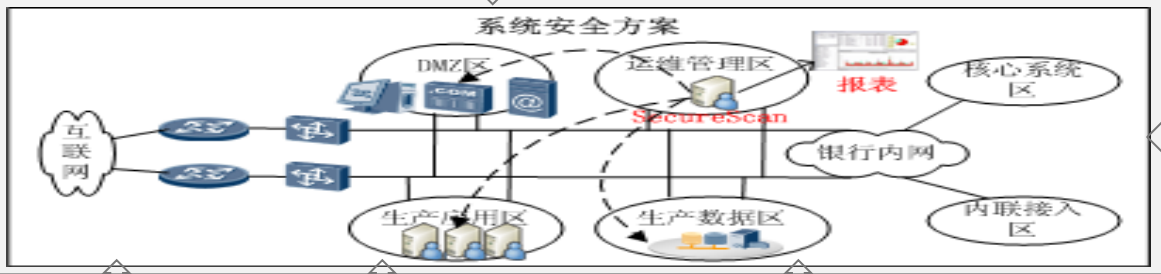
华为网银安全解决方案整体框架

WEB应用安全



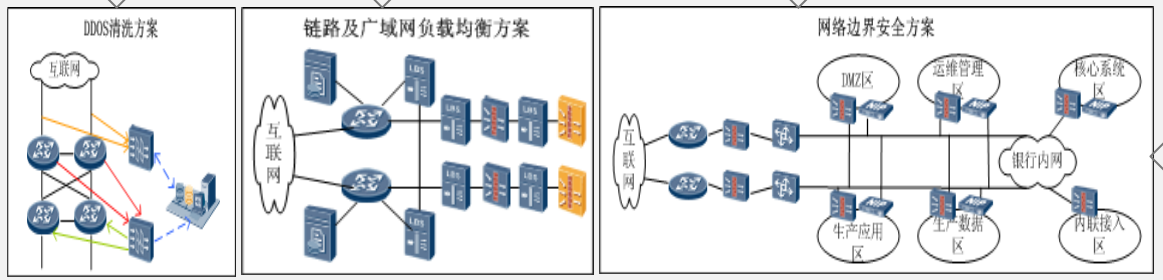
- 网页篡改防护
- WEB应用攻击防护
- 服务器负载均衡
- WEB安全监测评估
- 数据传输安全

系统安全



- 主机漏洞扫描与加固
- 主机安全威胁及时感知

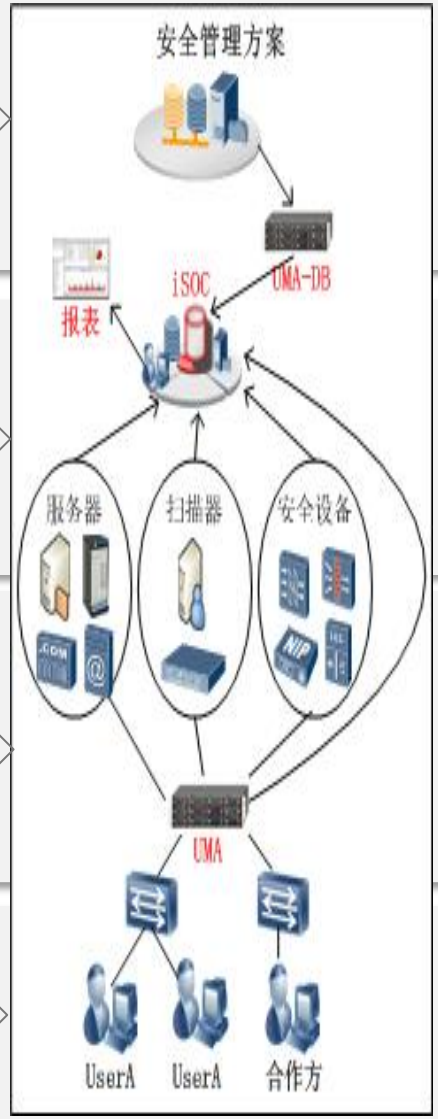
网络安全



- DDOS流量清洗
- 内外网边界安全与访问控制
- 入侵检测与防御
- 链路与广域网负载均衡

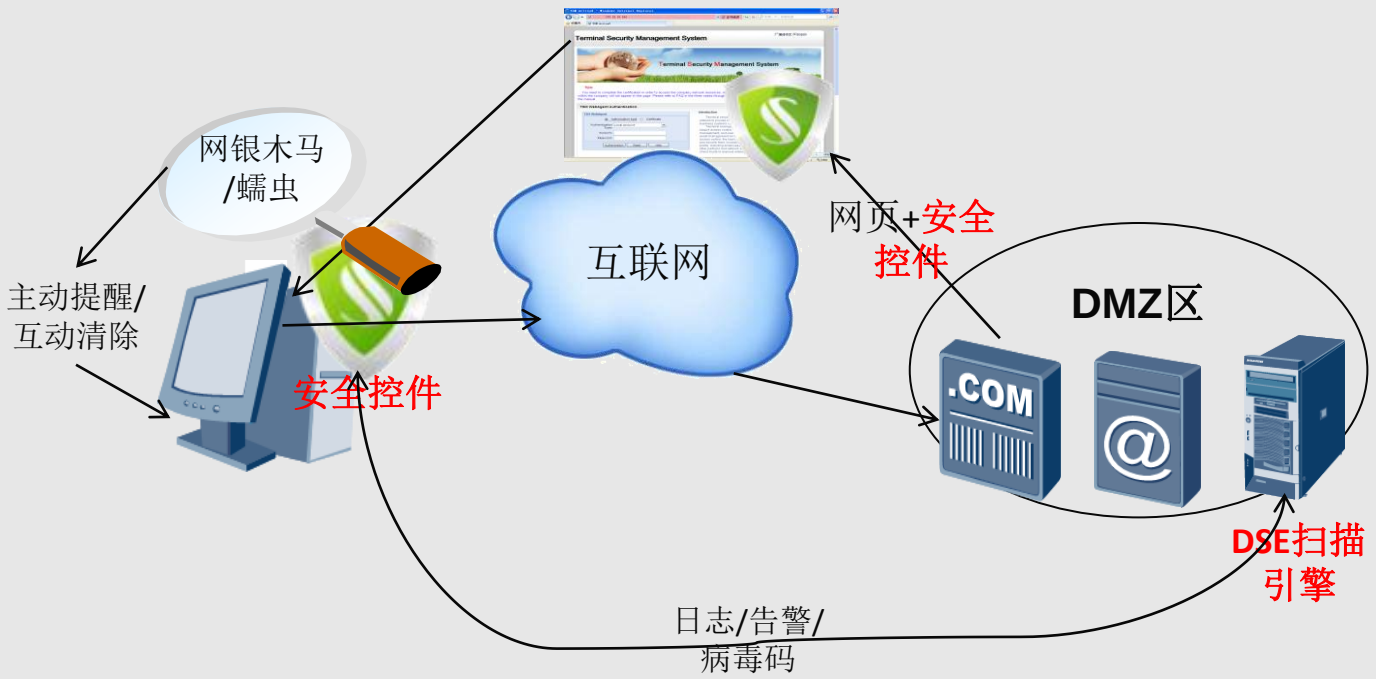
客户端安全

- 客户信息窃取
- 网银木马侵害



客户端安全—木马防御方案

客户端安全控件木马病毒查杀



方案及其特点

方案

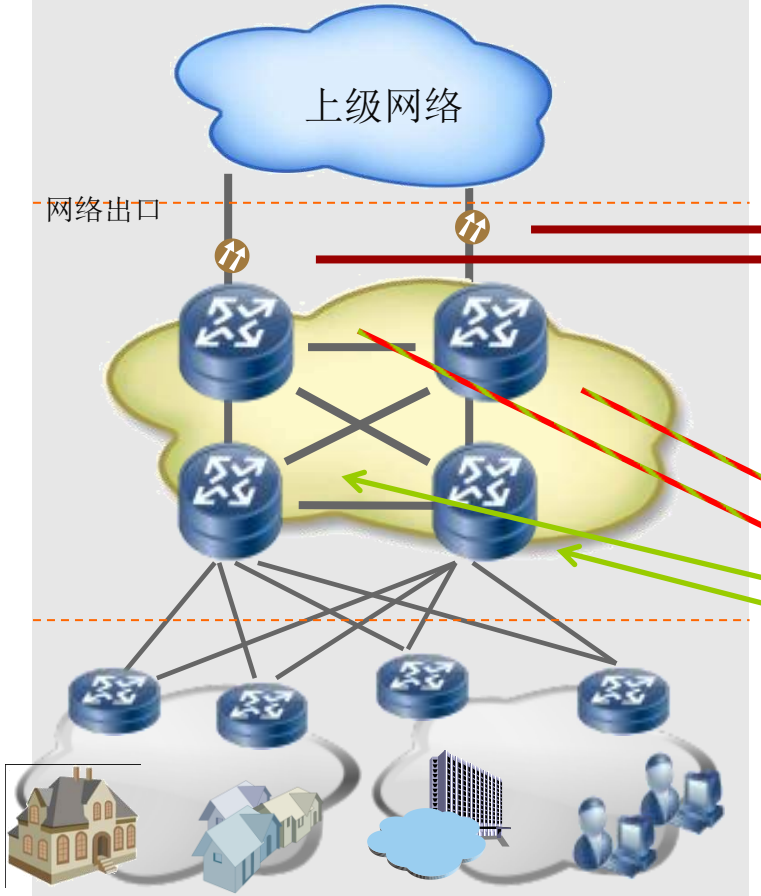
- 安全控件随网银登陆页面自动下发；
- 安全控件将扫描登陆环境，包括木马、僵尸、蠕虫、恶意程序或者其他病毒，清除网银使用的客户端环境，保障网银客户账号使用安全。
- 检测到木马病毒，即主动提醒客户，并互动清除
- 安全控件从DSE下载新的病毒码，将日志和告警信息上送DSE引擎

特点

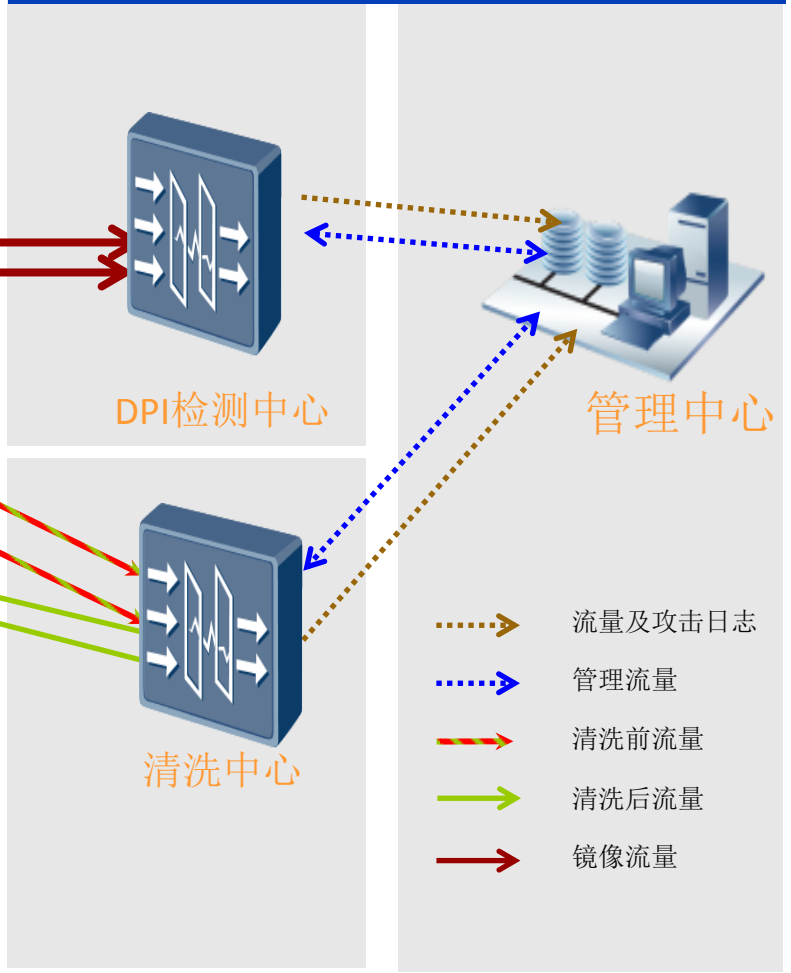
- 主动提醒、互动清除
- 网银木马病毒及时更新；
- 安全状况，网银中心实时掌控

网络安全— DDOS清洗方案

用户网络



旁路DPI检测动态引流清洗



方案及其特点

方案

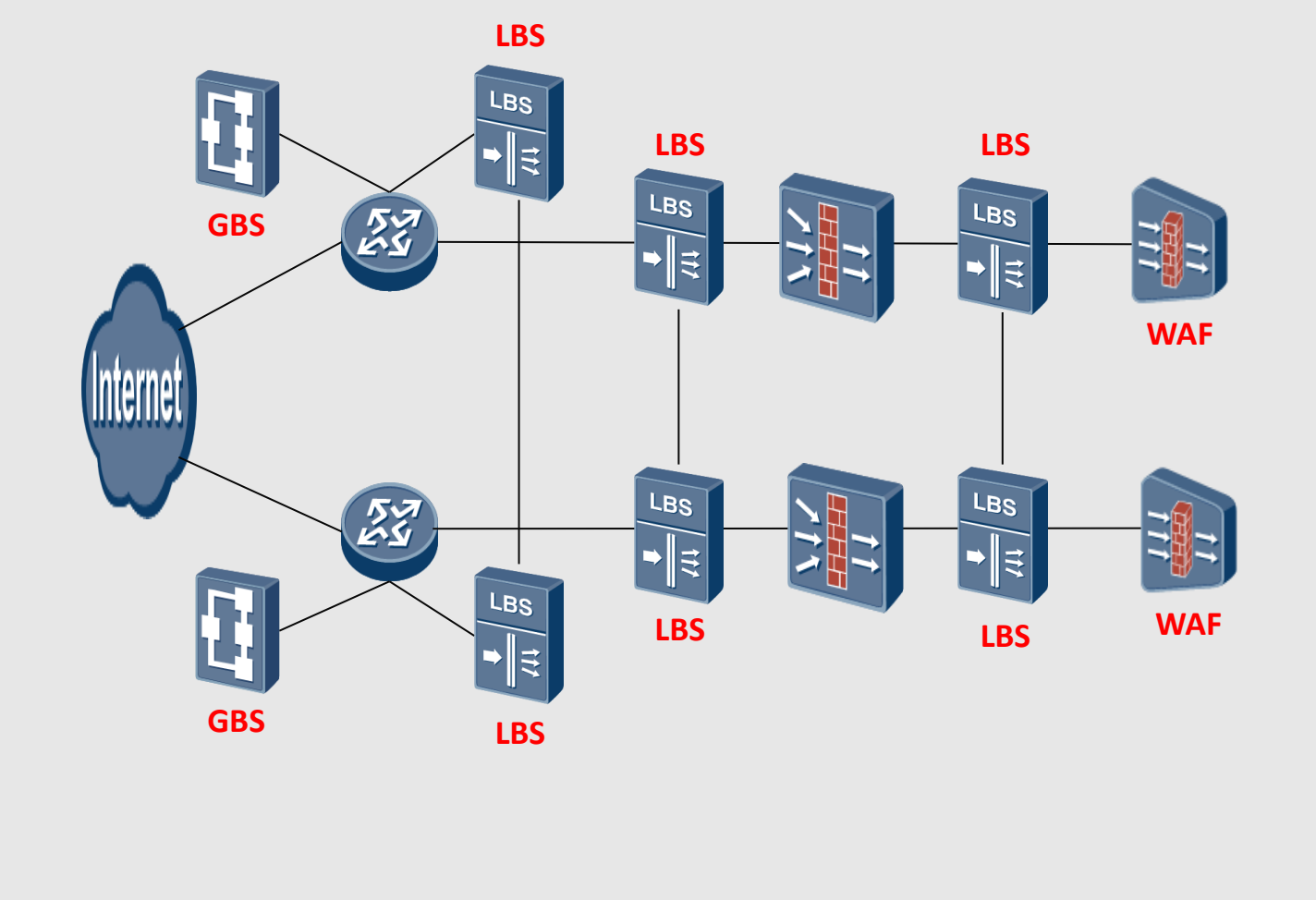
- 旁路部署DPI流量分析设备，全网流量检测异常后，自动下发引流策略到核心路由，将异常流量引入清洗设备进行清洗
- 管理中心可查看报表、攻击事件、清洗情况等
- 检测设备可部署在清洗设备上方，实现全流量检测；
- 检测设备可部署在清洗设备下方，实现小范围精确检测，节约成本

特点

- 旁路部署，不影响正常业务；
- 异常流量深度检测，DDOS攻击精确检测
- 攻击情况可视查看，及时响应

网络安全—链路及广域网负载均衡方案

链路及广域网负载均衡



方案及其特点

方案

- **GBS：** 广域网负载均衡，实现多中心分担网银业务，保证网银服务可用性；

- **LBS：**
- 链路负载均衡，实现多链路负载分担，保证链路传输免受故障影响；
- 防火墙负载均衡，保证边界安全防护高效、及时处理
- WEB应用防火墙负载均衡，保证WEB应用安全高效、及时处理

- **WAF：** WEB服务器负载分担、WEB应用安全防护，WEB服务优化

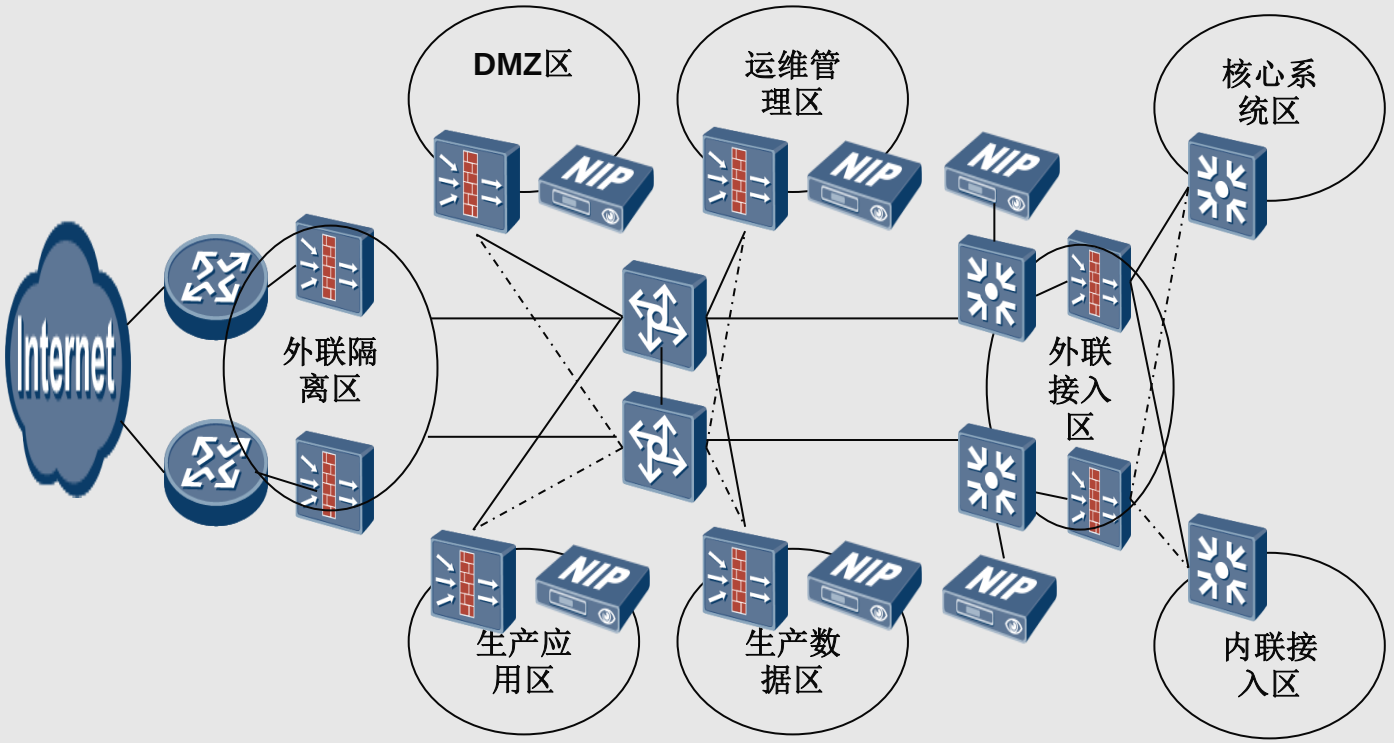
特点

- 多中心、多链路全面的网络流量分担；

- 安全处理多设备分担，降低网络延迟

网络安全—网络边界安全方案

内外网边界安全防护



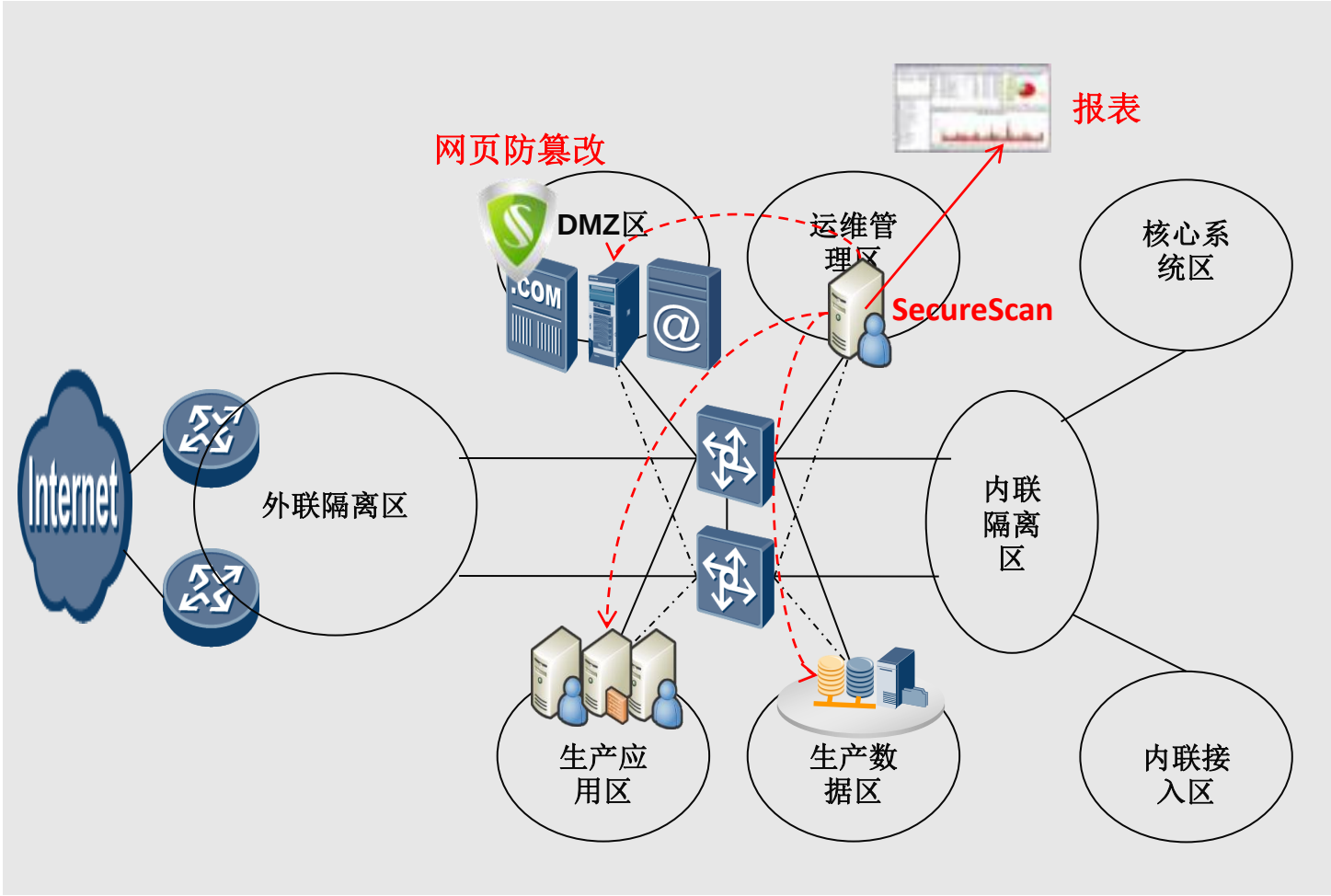
方案及其特点

方案

- 内部系统IP免受外部感知
- 各类区域FW边界安全防护，免受非法访问
- 各类区域IPS入侵防护，网络异常流量、安全风险及时感知；
- 安全域间防护，过滤非业务流量

系统安全—主机安全方案

主机安全防护



方案及其特点

方案

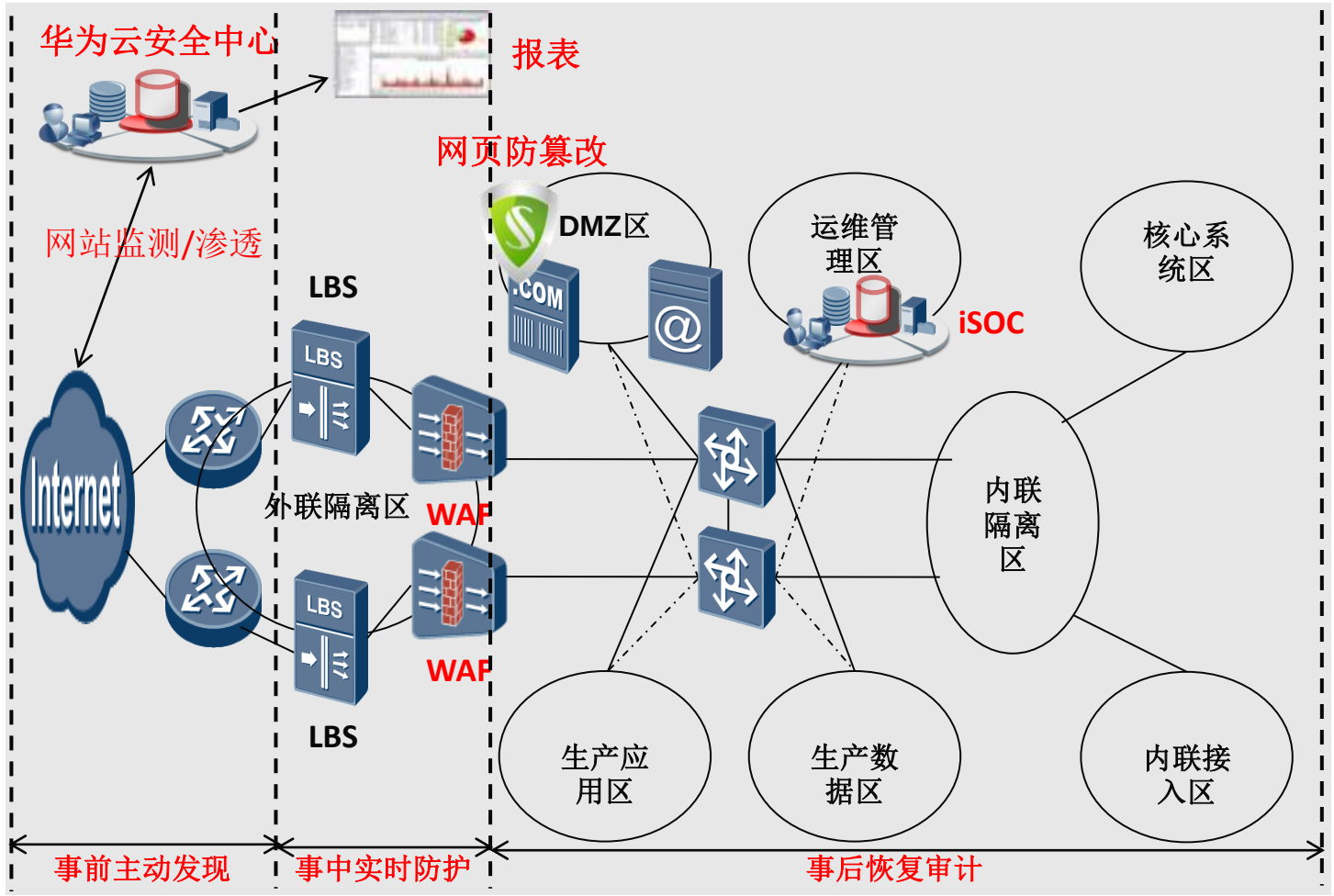
- **SecureScan：** 对网银各类服务器漏洞进行即时安全扫描；
- **包括：** WEB服务器漏洞扫描、数据库漏洞扫描、应用服务器漏洞扫描
- **协议和端口漏洞扫描：** 对各类服务器的端口和协议进行扫描

特点

- 功能全面的内网服务器系统漏洞安全管理；
- 漏洞复现技术：复现漏洞被利用的场景，呈现漏洞造成的危害程度；
- 华为云中心的安全能力支撑，提供更及时的扫描能力升级

WEB应用安全—WEB应用安全方案

WEB应用安全防护



方案及其特点

方案

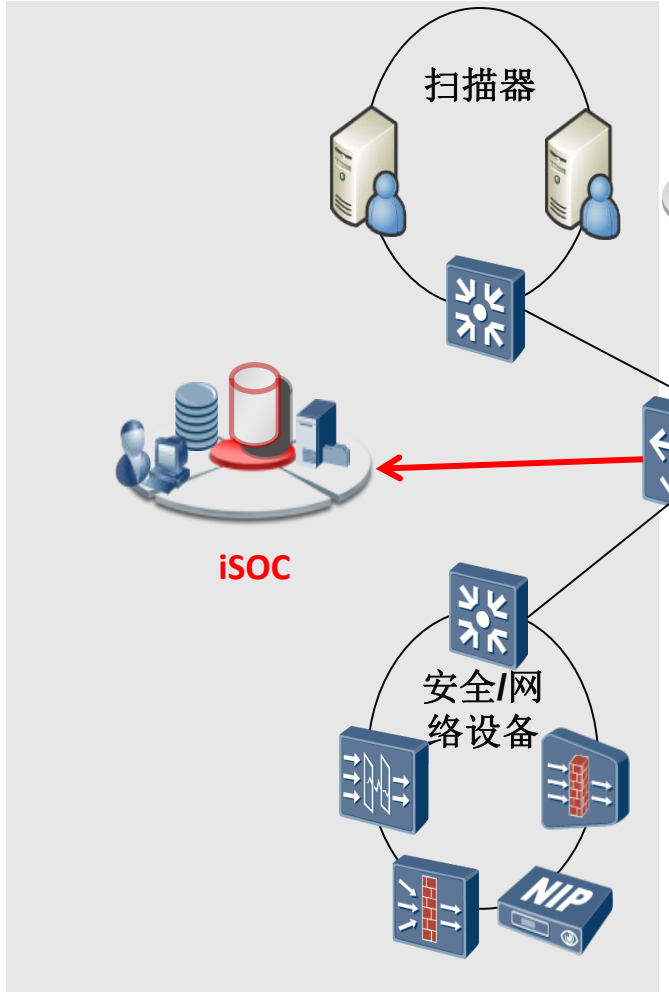
- **华为云安全中心：** 对网银网站进行页面解析、状态监控、渗透测试、漏洞扫描，并将监测情况以可视化报表展示；
- **WAF：** 用户与服务器双向流量检测，实时阻断WEB应用攻击与异常流量
- **网页防篡改：** 网页篡改驱动层检测，最快速度修复网页
- **iSOC：** WEB应用攻击和检测都有日志记录与告警，事后可追查与回溯

特点

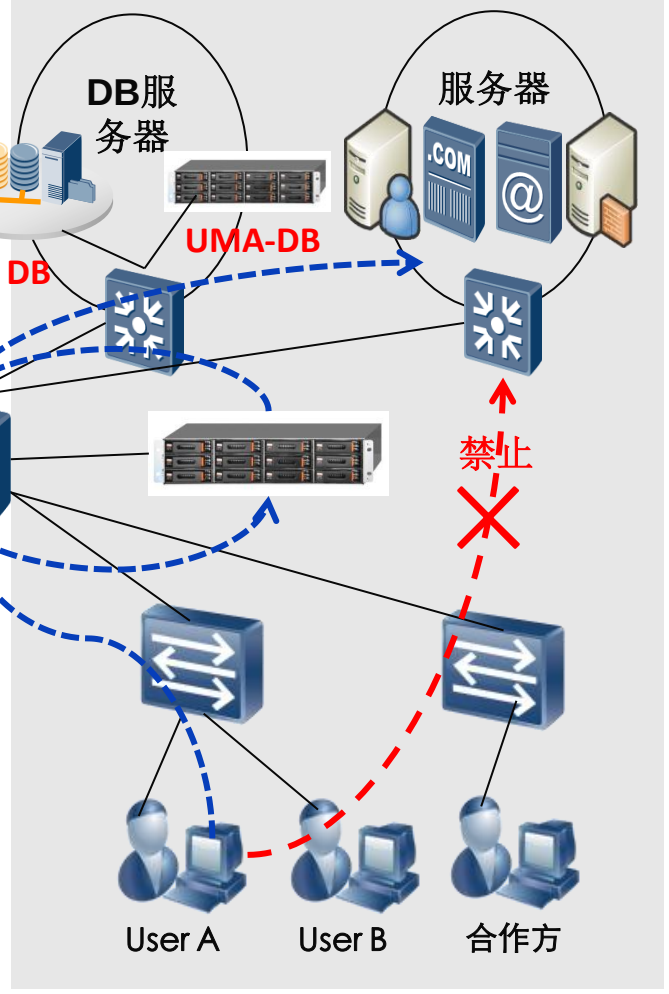
- 事前、事中、事后全生命周期安全管理与防护；
- 产品+服务多种手段解决WEB安全问题

安全管理解决方案

iSOC安全管控中心



UMA统一运维审计



方案及其特点

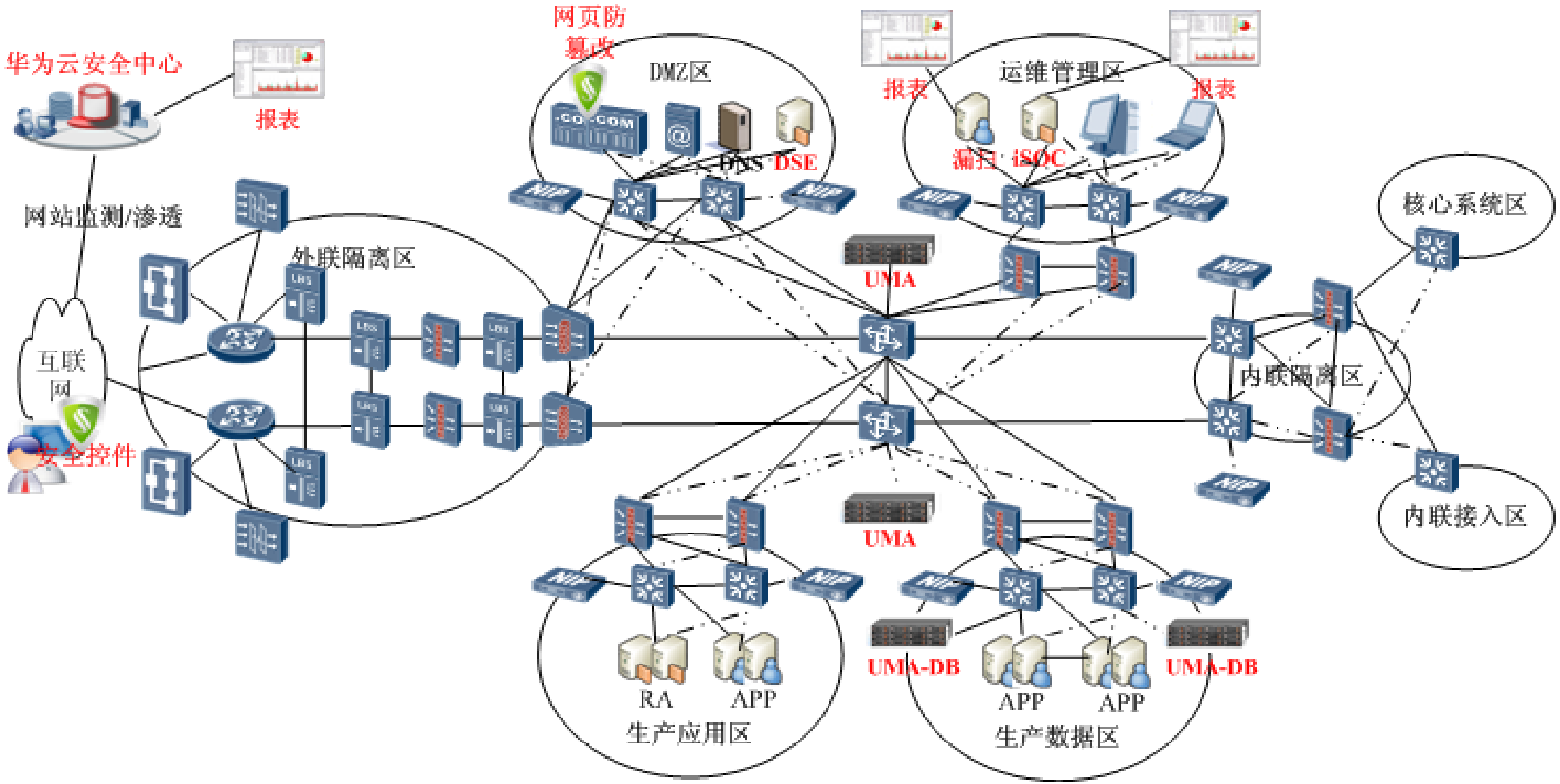
方案

- **iSOC：** 安全事件采集，关联分析，安全状况可视化展示；
- **UMA-DB：** 数据库操作日志采集、监测
- **UMA：** 为核心业务系统提供统一维护操作入口，实现单点登录

特点

- **全方位的安全管理：** 事前日志采集、事中关联分析，协助安全管理、事后追溯审计；
- **统一运维入口：** 服务器、网络、安全设备统一运维入口，单点登录，有效监控运维管理
- **运维集中管理：** 账号集中管理，权限严格控制，杜绝越权访问，实现命令级的控制

华为网银安全解决方案全景图



华为网银安全解决方案可销售安全产品清单

方案名	设备型号	备注
客户端安全解决方案	安全控件	终端安全扫描引擎，在网页中嵌入
	DSE	WEB安全动态检测引擎，在DMZ区部署
异常流量清洗解决方案	**ADI**	DDOS检测设备
	ADD	DDOS清洗设备
	ATIC	安全策略服务器
链路及广域网负载均衡解决方案	**F5-BIG-LB-1600/3600/3900 (加GTM license)**	广域网负载均衡器，多中心场景使用
	F5-BIG-LB-1600/3600/3900	链路负载均衡器，覆盖链路负载均衡、安全设备负载均衡

华为网银安全解决方案可销售安全产品清单

方案名	设备型号	备注
网络边界安全解决方案	**USG2000/USG5000系列防火墙**	覆盖外联隔离区、内联隔离区、服务器区间隔离
	NIP2000/NIP5000	服务器区域边界
主机安全解决方案	**SecureScan**	漏洞扫描器
WEB应用安全解决方案	**Netscaler MPX7500** **F5-BIGIP-ASM-3900** **明御 WAF-1000A** **天清汉马 WAG1010**	攻击报文事中拦截
	iGuard网页防篡改系统标准版V3.0 **InforGuard网页防篡改V5**	网页事后恢复
	iSOC	事后审计追溯
安全管理解决方案	**VSM**	可以覆盖交换机、安全设备管理
	iSOC	DDOS清洗设备
	UMA100/UMA200	覆盖主机系统、数据库系统、网络设备和应用系统
	UMA-DB	使用UMA-DB企业版

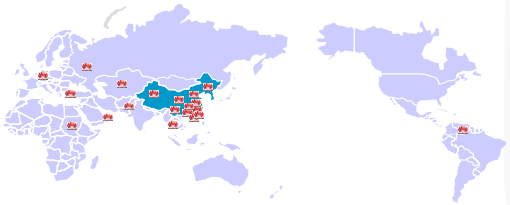
目录

世界级的安全能力中心

•和世界顶级运营商联手，拥有遍布全球的蜜网系统，能够及时搜集恶意样本并进行分析

•拥有近200人的专家团队及装备自动化分析平台的协议分析、安全攻防、恶意代码、URL分类安全实验室

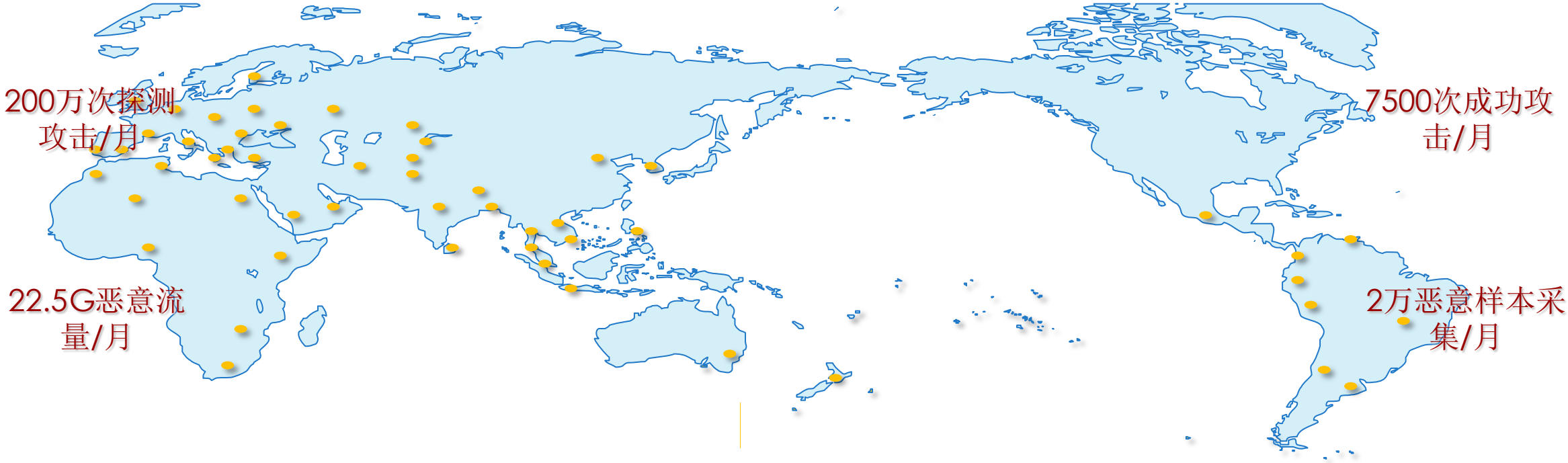
雄厚基础



•和SIG共享现网流量超过8000G的安全样本获取系统、分析系统和策略下发系统

•硕果累累，DPI协议识别数已达全球第一；URL分类支持的数量达到业界一流水平；累计申请专利超过100项。

全球动态蜜网系统

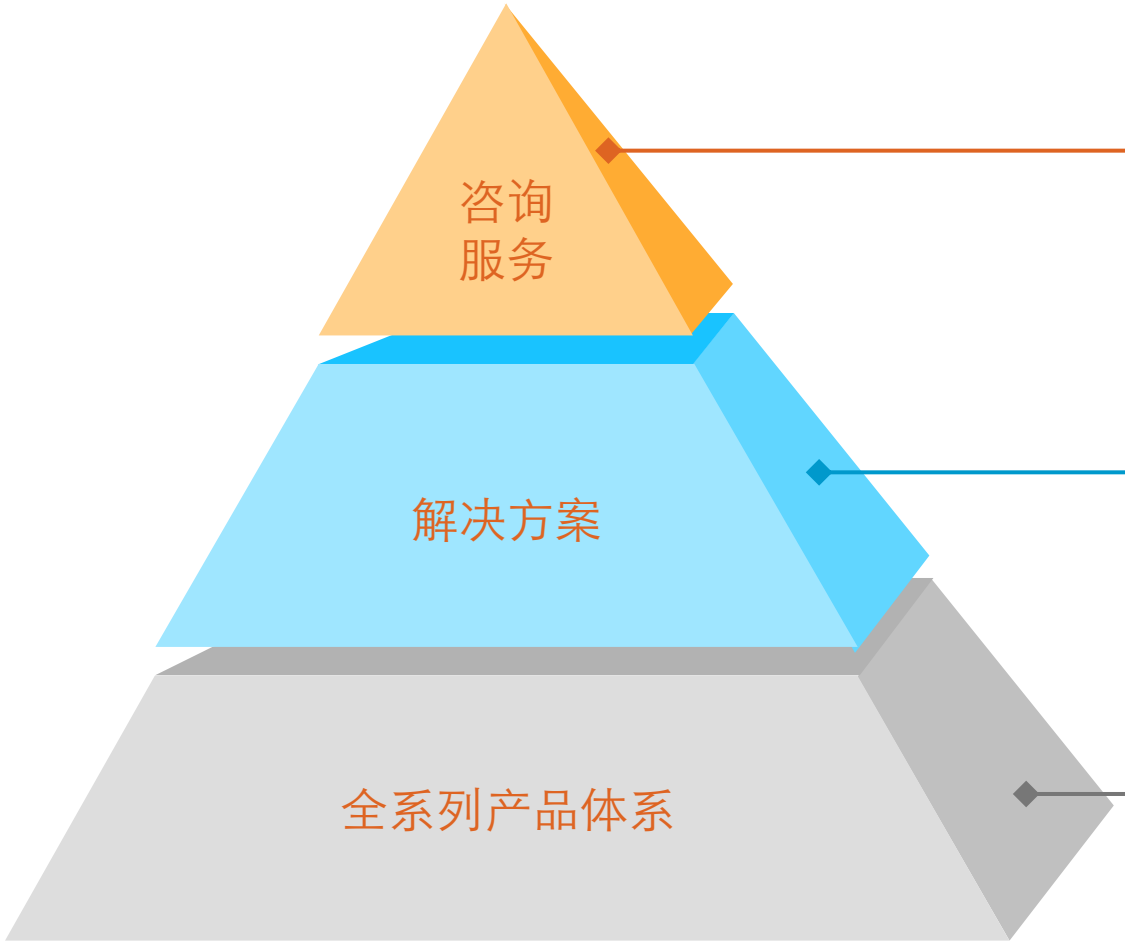


- 在全球多个国家建有蜜罐系统，形成覆盖全球的蜜网
  - 实时捕获蠕虫、病毒等恶意代码样本
  - 分析黑客攻击手法与后门工具
  - 统计全球DDOS攻击特征与数据

云安全感知全球威胁

- **云安全帮助您实时掌握全球安全威胁变化**
  - 用户可获得最专业的安全感知能力
  - 以全球的案例经验支撑安全建设

金字塔架构的产品和服务体系

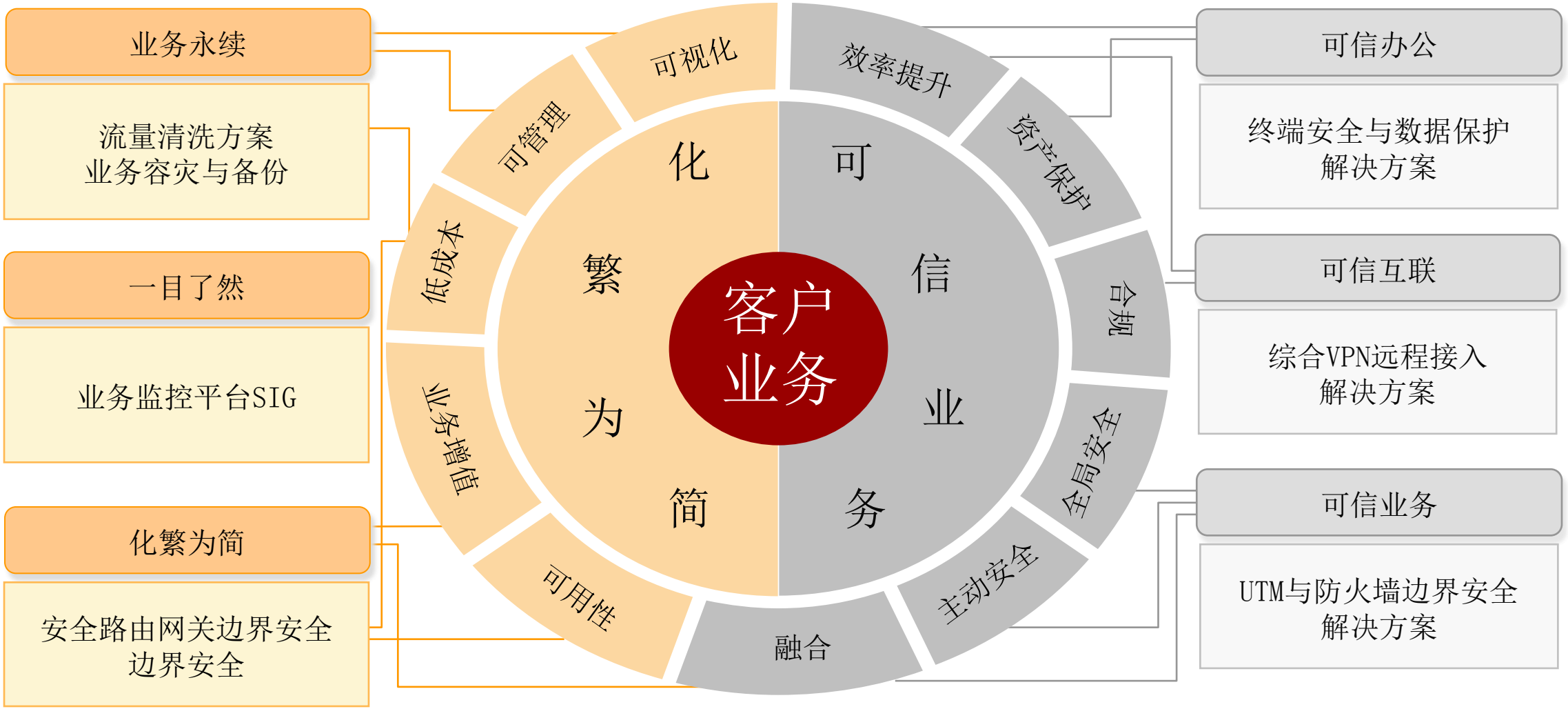


提供风险评估、等级保护、IT内控、SOX、容灾备份等全范围的安全存储高端咨询服务

提供覆盖政府、运营商、金融、能源、交通，SP、教育、医疗、企业等端到端的解决方案

提供覆盖高、中、低端全系列安全、存储软硬件产品

以客户为核心的安全理念-成就业务价值



华为安全产品全景图

云安全

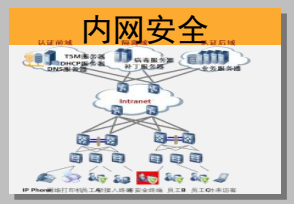
安全能力

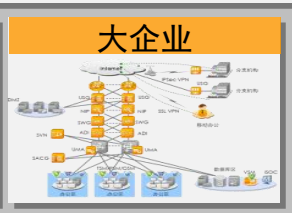
垃圾邮件库	恶意代码库	僵尸网络库
URL分类库	蠕虫病毒库	入侵/漏洞库

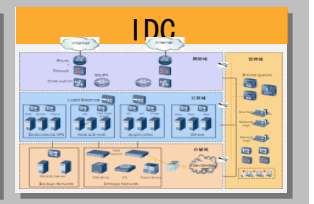
安全服务

安全应急响应	安全咨询服务	安全加固服务
安全升级服务	安全信誉评估	安全管理服务

安全方案



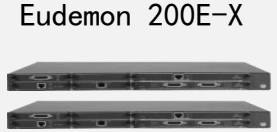




安全管理

应用安全

网关产品



目录

中国光大银行数据中心AntiDDOS项目

面临挑战：

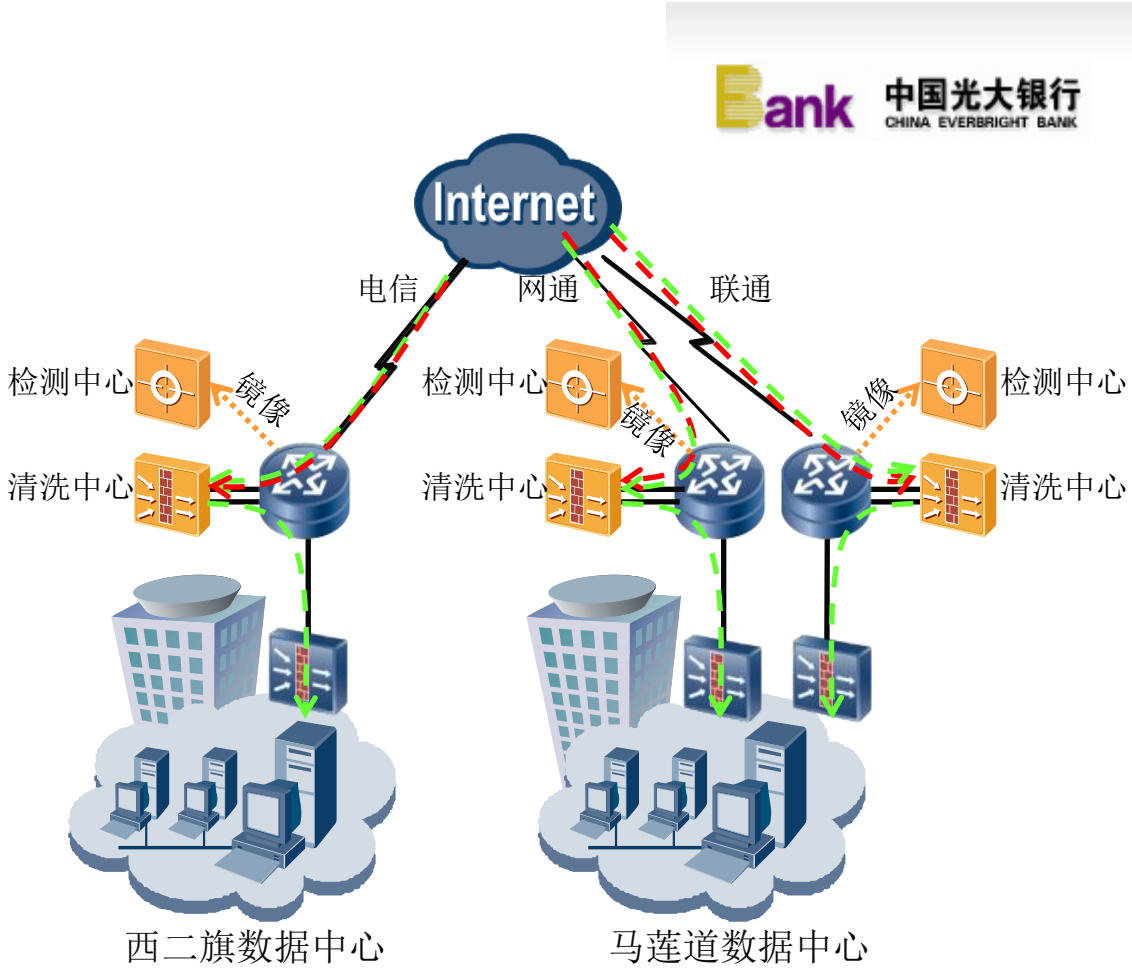
- 光大银行门户网站和网上银行经常遭到来自互联网的DoS/DDoS攻击，严重影响到了对外业务的正常开展。

华为解决方案：

- 采用SIG旁路检测＋USG联动清洗的专业抗DDoS系统，部署在光大银行数据中心的三条互联网出口处，对来自外部的各种DoS/DDoS攻击进行实时检测、联动、引流、清洗。

客户价值：

- 依托国内最大的“网络及应用攻防实验室”和遍布全球的蜜网监控系统，华为专业抗DDoS解决方案可以为光大银行数据中心提供从网络层到应用层的全面抗DoS/DDoS攻击防护，并且通过模拟交叉攻击测试，在所有参测厂商中一举胜出！



大连百年人寿保险公司网络安全项目

面临挑战：

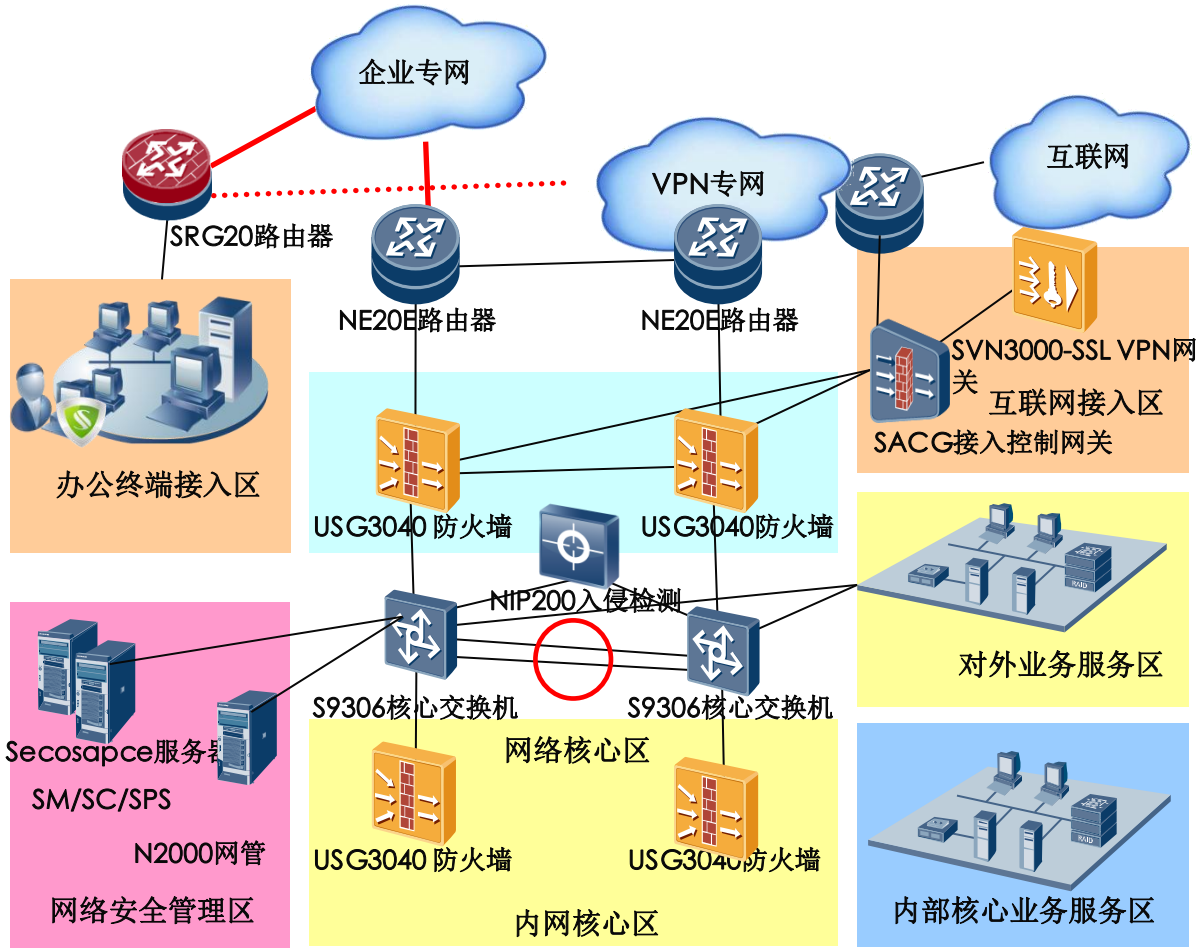
- 百年人寿计划09年中旬完成3至5个分公司建设，3至5年内完成全国省级分公司，部分地市级分公司的布点。网络安全问题不容忽视。

- **华为解决方案：**

- 核心网络区与内网核心区部署两台华为USG3040防火墙；
- 核心机房采用华为防火墙与入侵检测NIP设备联动，保护网络出口安全；
- 在互联网接入区采用华为SVN VPN设备，方便应对出差人员多样的VPN接入需求分别支持IPSEC与SSL接入；
- 分支机构选择集路由、交换、防火墙等功能于一身的SRG路由安全网关产品，为百年人寿提供高安全、高可靠多功能一体化的解决方案；
- 在办公终端接入区域，采用华为TSM终端安全管理系统保证内网用户的安全接入，管理人员通过网络安全管理区的策略服务器实现对办公终端集中管控，提高整网安全防护水平；

客户价值：

- 内网安全防护体系的建设使得用户在信息化建设后免受病毒、黑客等的攻击和干扰，并且有力保障了文档资料的安全，从而为银行系统正常的业务开展提供了内网安全平台。。



中国哈尔滨市商业银行内网安全项目

面临挑战：

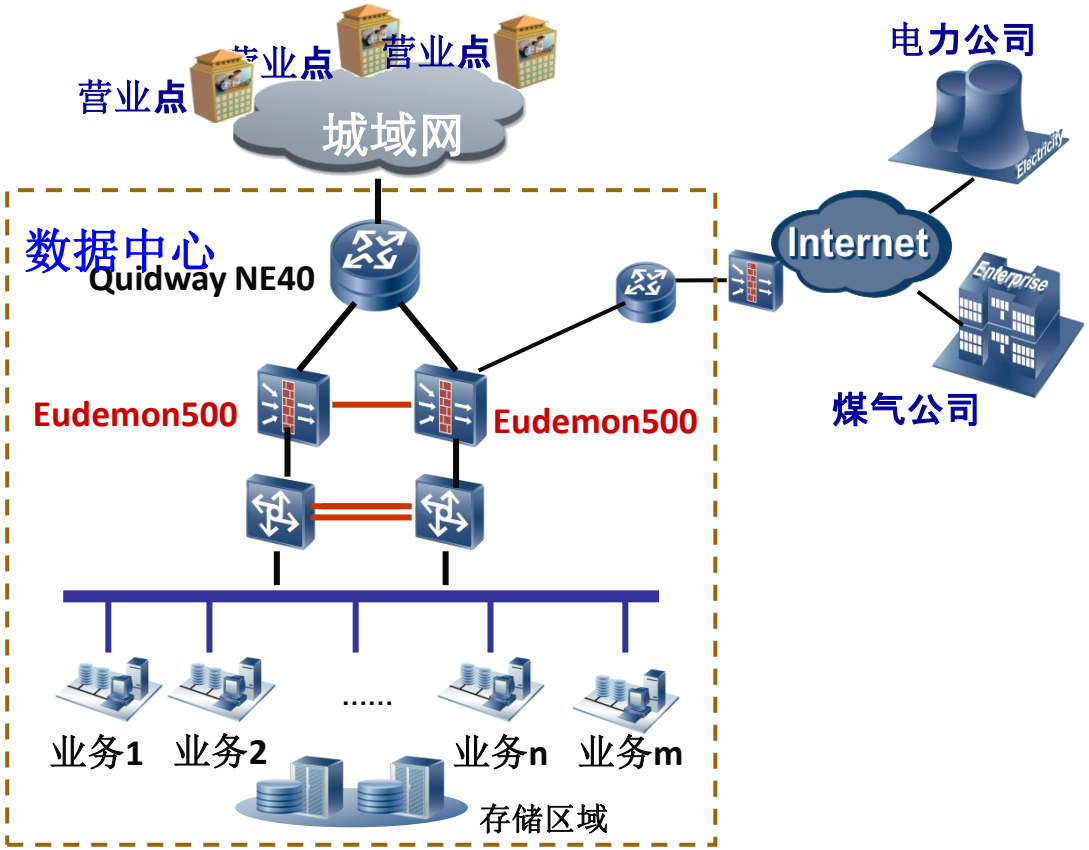
- 成立于97年的哈市商业银行，立足地方，经过10发展已经成长为东北地区盈利第一的地方银行。当前业务除了主营储蓄、贷款、票据业务外，还全面发展了中间业务。这些丰富的业务对哈商行数据中心提出了很高的网络安全和业务安全。

华为解决方案：

- 华为IDC安全防御方案通过两台Eudemon500千兆防火墙构筑银行数据中心的网络安全闸门。

客户价值：

- 最大限度地保证银行数据中心的网络安全，是核心业务连续性最有效的保障。



中国兴业银行内网终端安全项目

面临挑战：

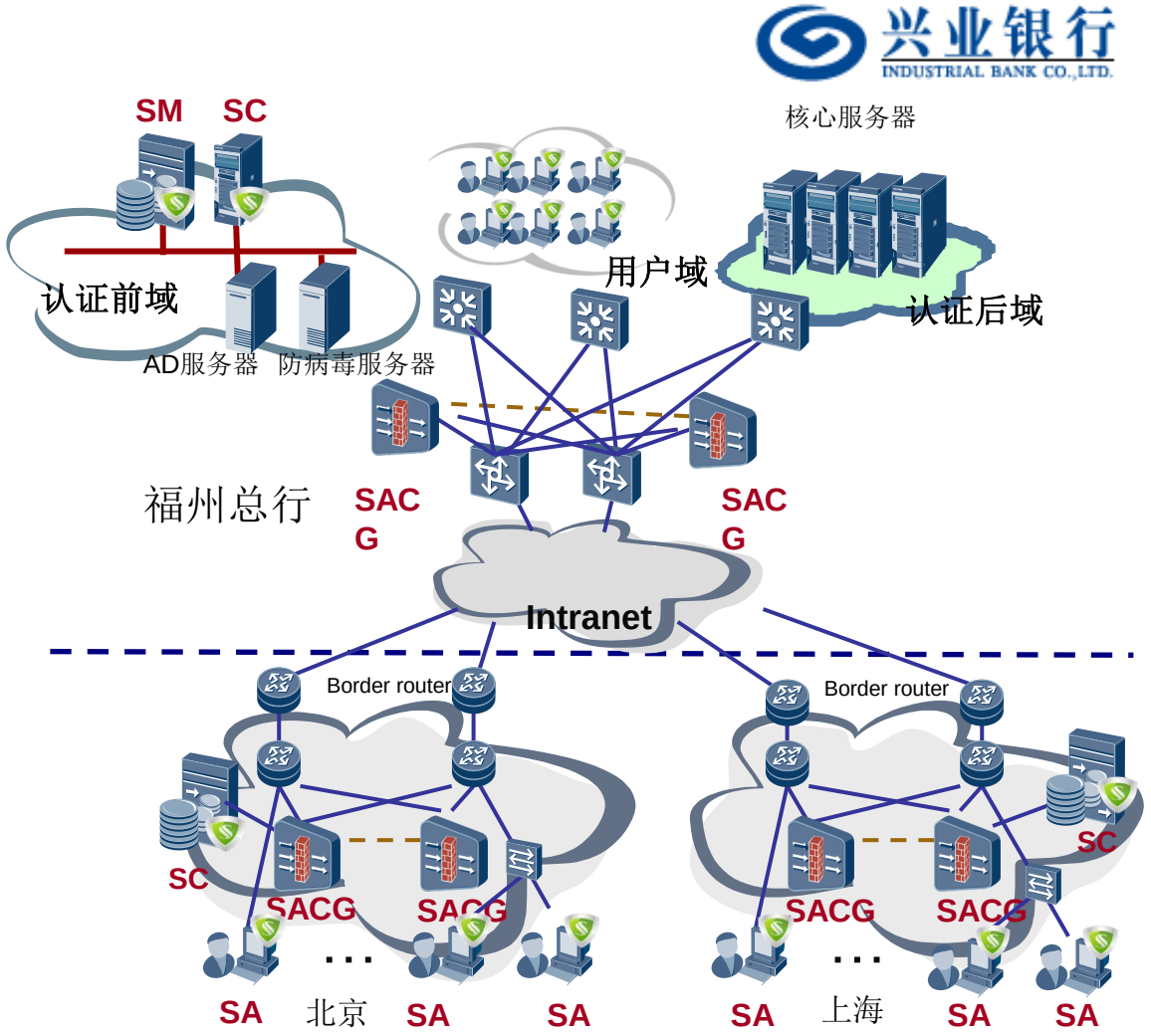
- 在当前复杂的网络环境下，重要机密信息保护、终端系统安全访问控制、及时更新和安装防病毒系统、人员活动跟踪和审计记录等安全管理急需进一步加强，需要以技术手段预防和消除有可能出现的信息安全风险

华为解决方案：

- Secospace系统通过网络和系统两个层面来搭建终端安全管理平台，将现有终端的补丁管理、软件分发、防病毒、资产管理、信息安全、权限控制等相关技术进行有机的整合，实现合法的、安全的终端接入，避免非法的、不安全的终端接入或把终端的安全问题带给其它终端、业务系统。
- 采用分布式部署方案，全国35个地市和地区，共4100个终端。

客户价值：

- 内网安全防护体系的建设使得用户在信息化建设后免受病毒、黑客等的攻击和干扰，并且有力保障了文档资料的安全，从而为银行系统正常的业务开展提供了内网安全平台。。



中国英大人寿移动办公远程接入项目

面临挑战：

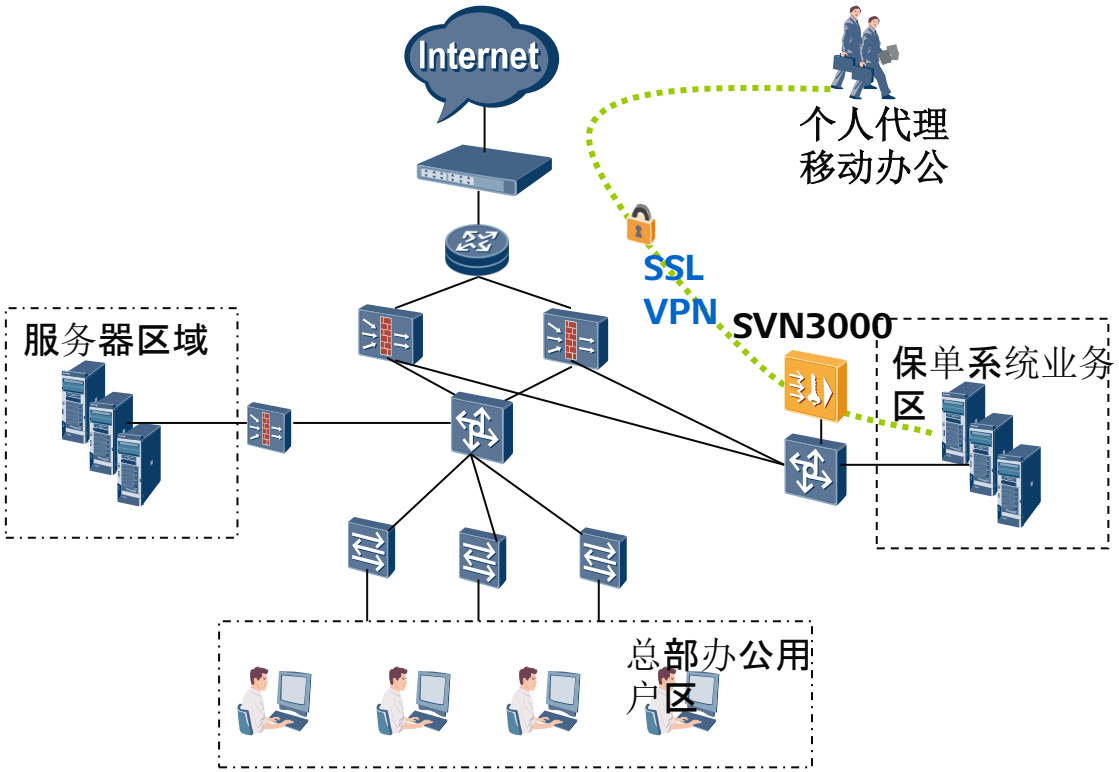
- 英大人寿全国20个省的个人保险代理经常需要移动办公，远程登录保单系统进行业务查询，全国代理同时在线用户连接数约1000~2000，后续有扩充需求。用户希望在投资有限的情况下能满足20个省的VPN系统相对独立、分级管理：总部设立系统管理员。20个省各自设立相应的二级管理员，只能管理该省的VPN系统和用户

华为解决方案：

- 华为SVN3000运用虚拟网关技术，给20个省各配置一个虚拟网关，实现各省SSL VPN系统的独立访问。为每个省设立一个虚拟网关管理员，采用USBkey＋数字证书 强认证方式，对他所属的虚拟网关进行配置管理，包括用户管理、资源管理、虚拟网关的安全策略管理等。
- 在总部设立系统管理员，管理设备系统及所有的虚拟网关管理员。

客户价值：

- 通过华为SVN3000为移动办公人员提供在公网传输业务的数据加密，高安全性、高性能的办公环境，提高了工作效率。虚拟网关技术，大大节省用户投资，满足多省VPN相对独立管理的需求。SVN3000集群技术满足用户未来业务扩容需求。



卢森堡工行远程安全接入项目

客户面临的挑战

●随着业务的扩展，出差、移动办公人员日益增多，亟需远程安全接入银行内部网络

●远程接入的用户认证需要采用物理媒介，避免因用户密码泄露导致安全事故

●需要对远程接入用户进行权限限制，根据用户身份授权访问内部网络资源

华为解决方案

●在银行网络出口部署Eudemon200E-X安全网关提供远程安全接入服务，两台安全网关做双机热备，保障了业务的连续性和可靠性

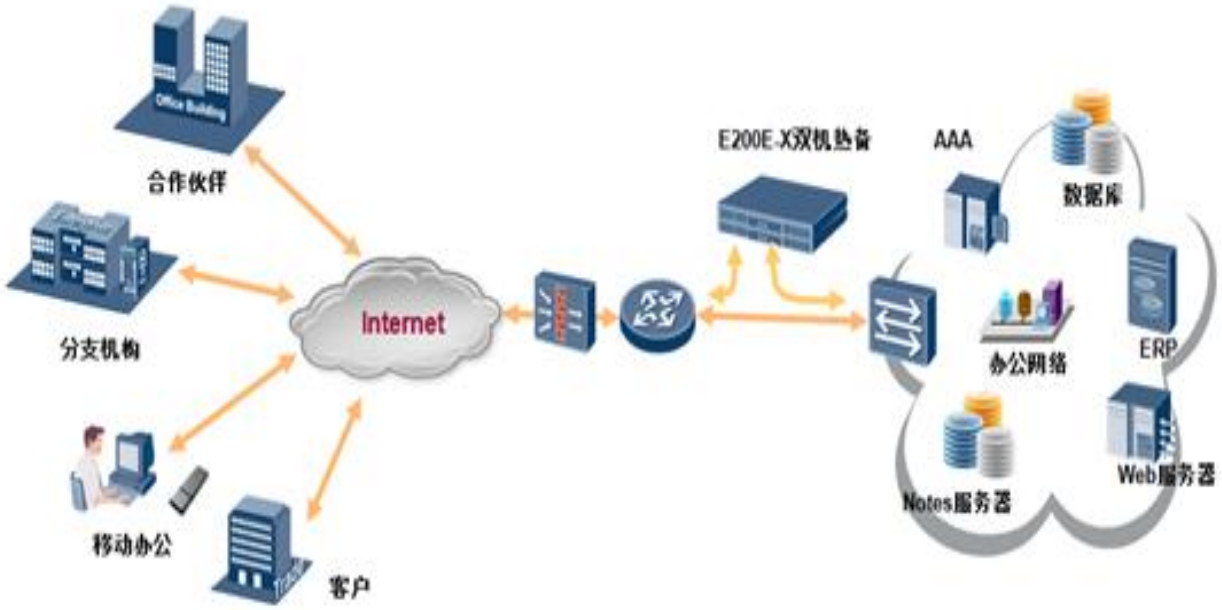
●用户认证采用USB Key数字证书+用户密码双因素认证，有效地降低由于密码失窃引入的安全风险，保证认证的可靠性

●对不同访问者开放的不同应用软件、数据资源，严格控制用户访问权限

客户价值

●Eudemon200E-X IPSec/SSL VPN一体化网关满足了移动办公远程安全接入内部网络的需求，双因素、物理媒介的认证方式保证了认证的可靠性，严格的权限访问控制机制满足了信息资产管理的安全需求

ICBC
中国工商银行



Thank you

www.huawei.com