SACC 2014中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2014
发现架构之美

腾讯云安全实践

-- 2014.9

大纲

- 自我介绍
- 腾讯云网络架构演进
- 腾讯云安全系统架构演进
- 云安全建设方向

自我介绍

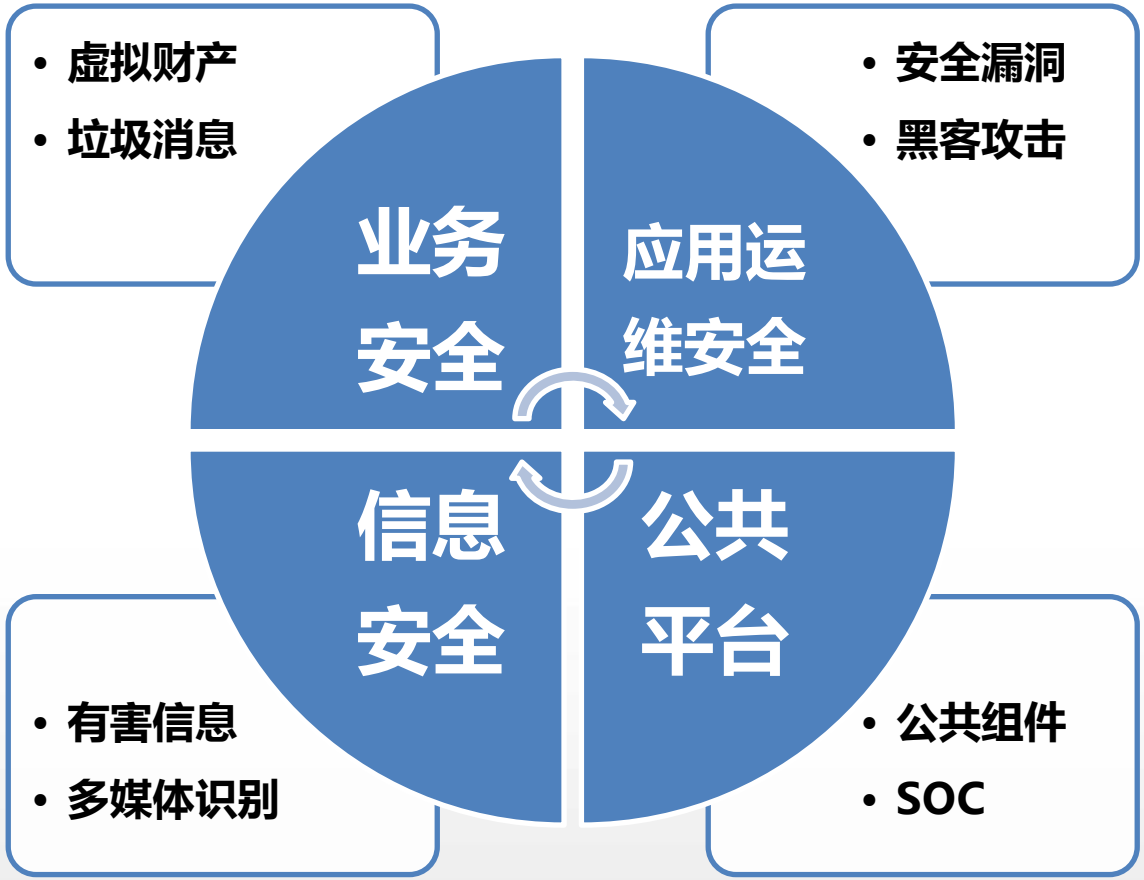
- bluezhou（周斌）
  - 2005年加入腾讯
  - SNG安全中心
  - 主要工作：QQ&Qzone业务安全、腾讯云安全

关于腾讯

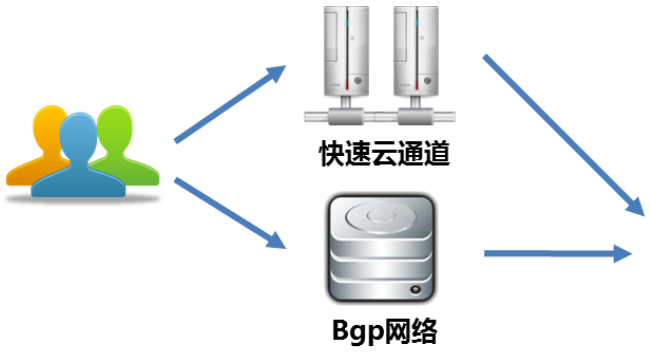
腾讯云

http://www.qcloud.com

腾讯的传统安全系统


• 虚拟财产
• 垃圾消息
• 安全漏洞
• 黑客攻击
业务安全
应用运维安全
信息安全
公共平台
• 有害信息
• 多媒体识别
• 公共组件
• SOC

腾讯云的架构



CVM
高性能，高稳定性云虚拟机

CEE
一体化web应用运行环境，弹性伸缩，中小开发者的利器

CBS
可靠弹性块存储,多种硬盘选型，丰富IO 策略

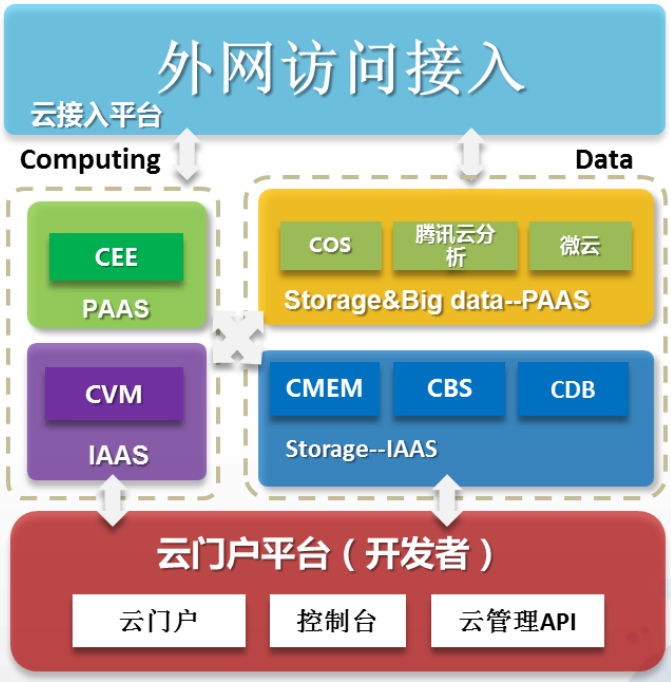
COS
泛网络，restful接口，对象存储服务

CMEM
兼容memcache协议，超高性价比分布式key-value缓存

腾讯云分析
海量分布式数据处理平台和数据市场

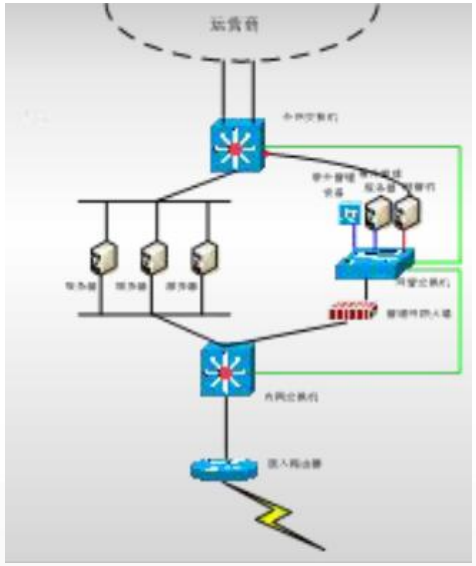
微云
社交个人存储，支持妙传，疾速访问，短连接分享

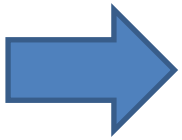
腾讯云服务整体解决方案

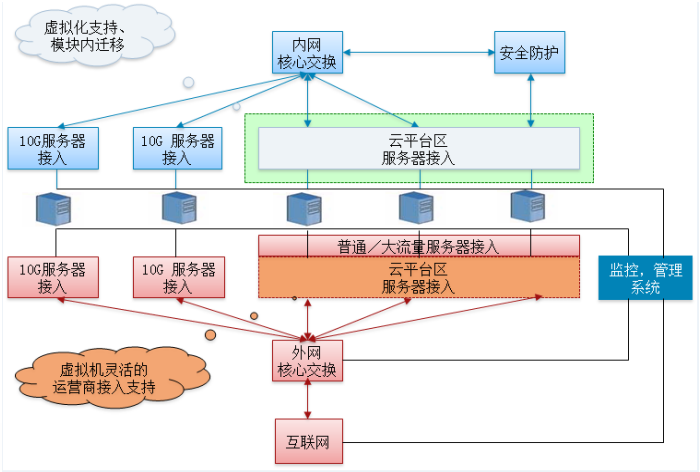


腾讯的网络架构演变

- long long ago…





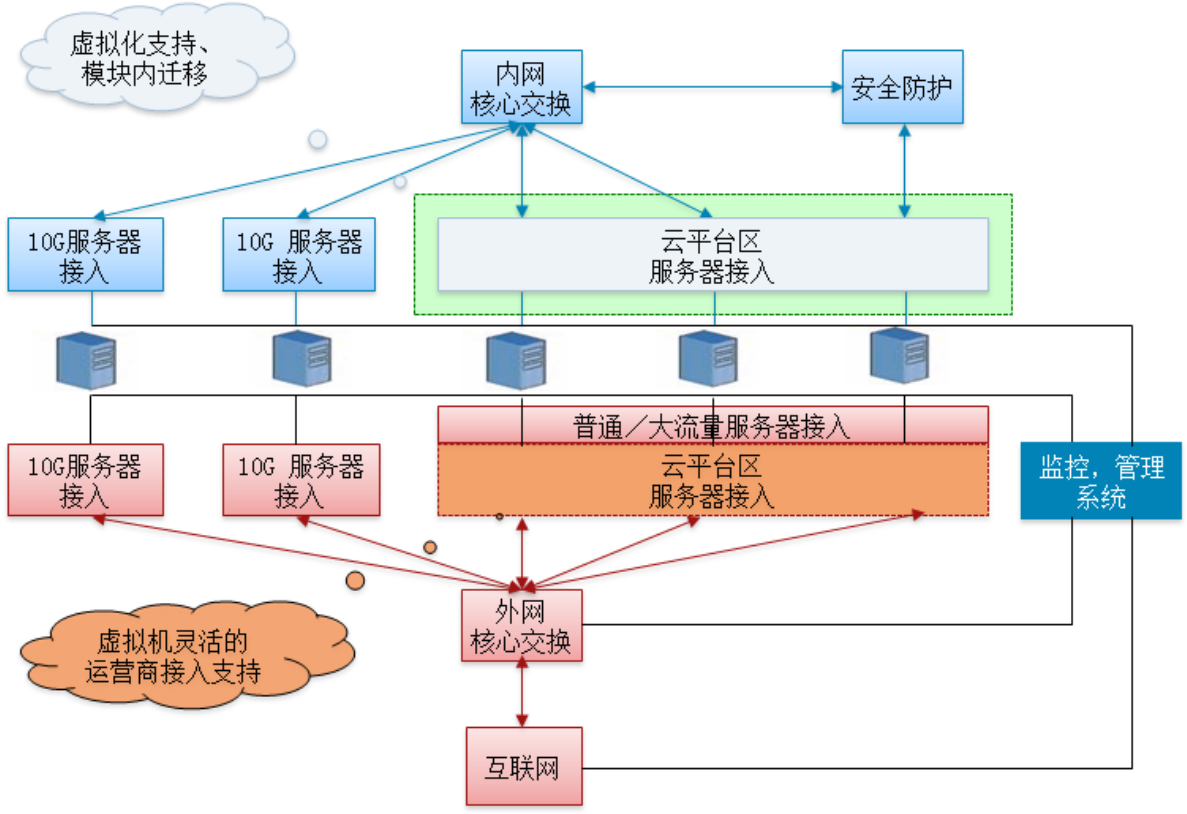


单IDC、同地模式

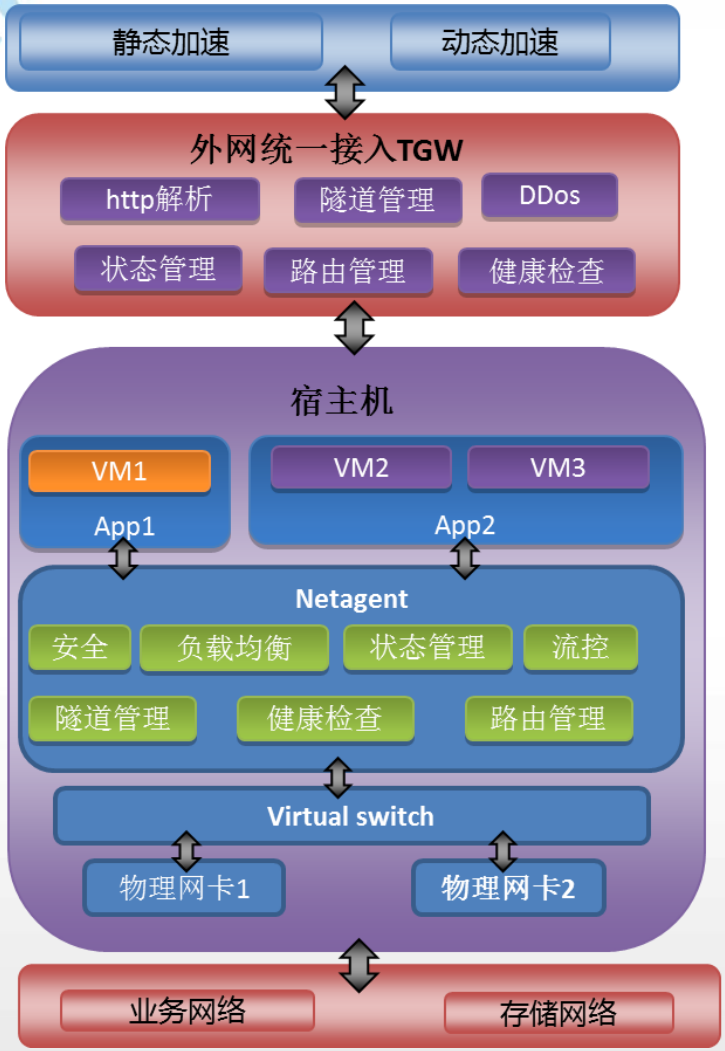
多IDC、异地分布模式

支持腾讯云的网络架构

- 云时代的基础网络



腾讯云网络架构



静态加速用图片等内容，动态加速智能选路，优化传输路径

TGW外网统一接入集群，外网IP和虚拟机解耦，四七层负载均衡，防御各种DDOS攻击

内网负载均衡，访问后端存储服务和自己搭建的服务

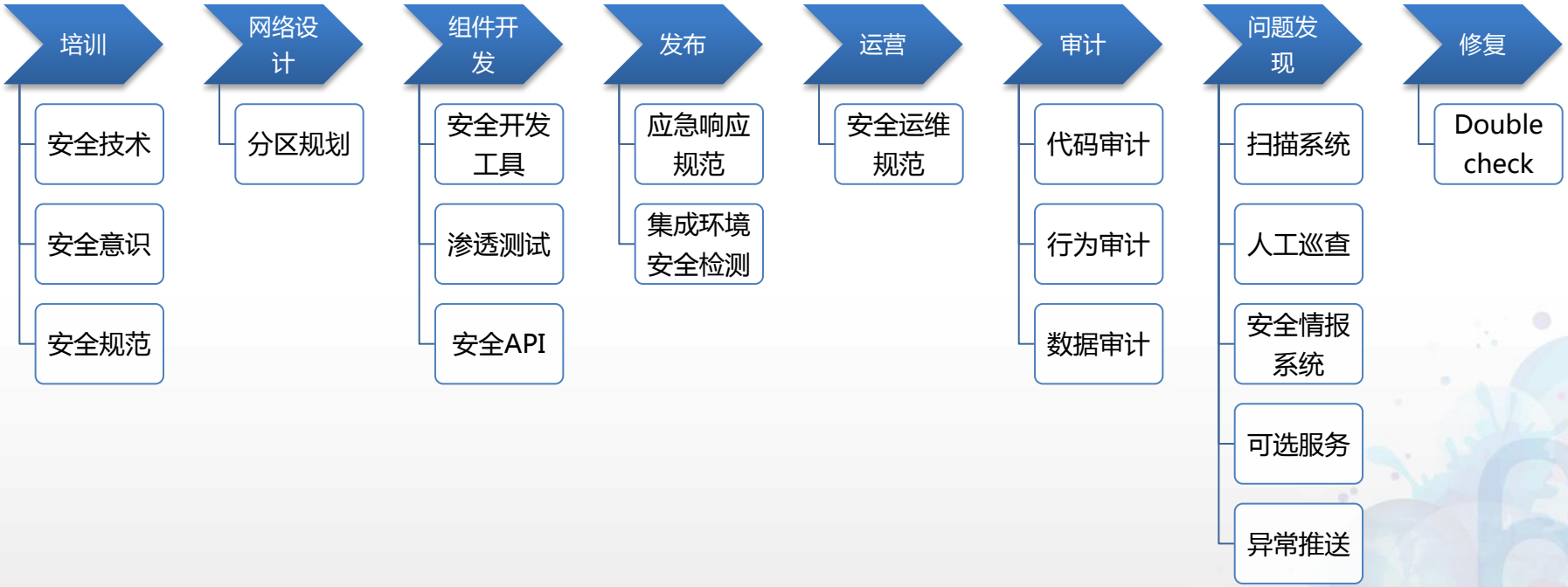
租户之间网络隔离，双向流量限制

VM之间带宽基于HTB的QoS控制

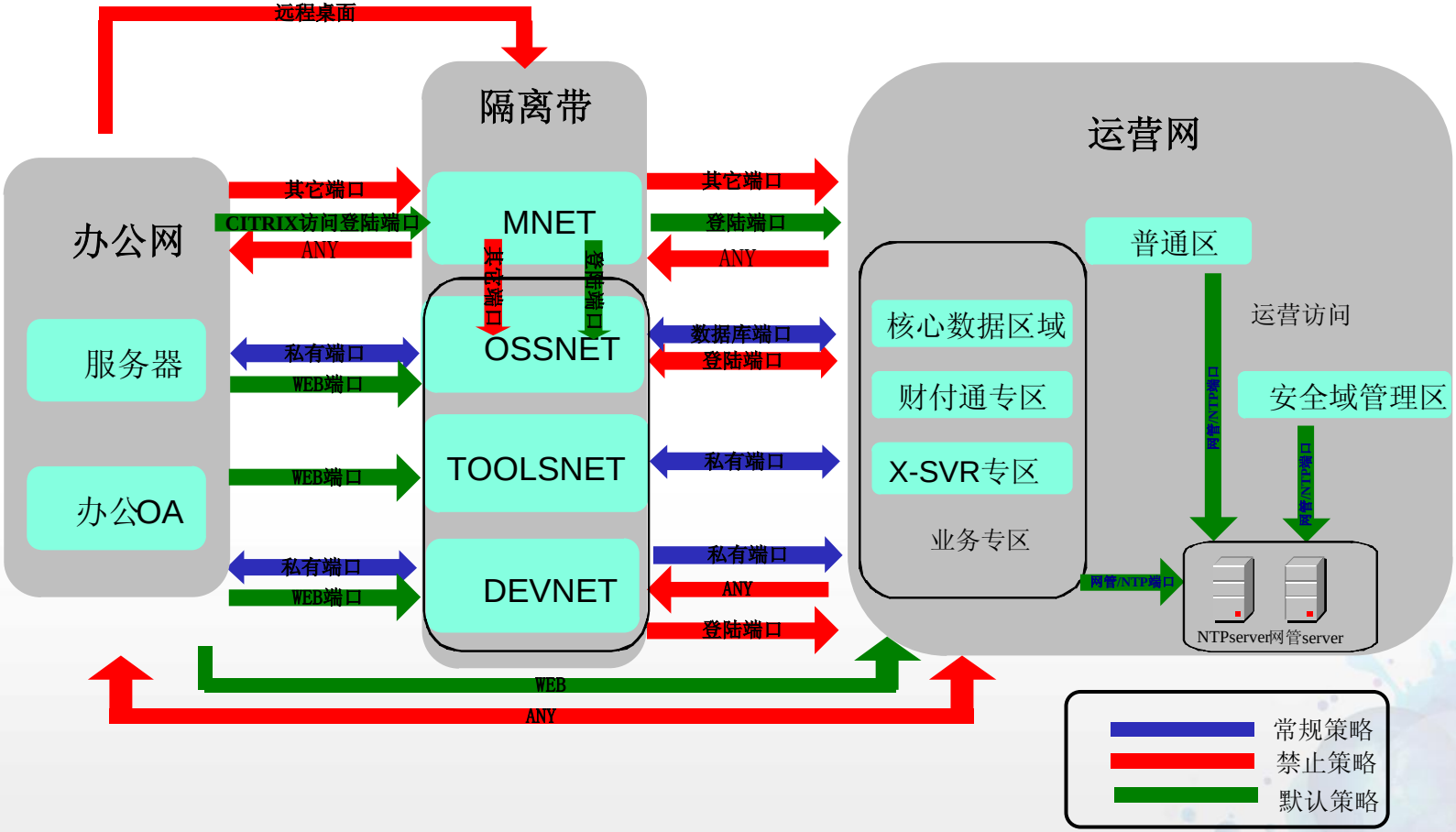
存储网络和业务网络分离，互为备份

腾讯云运营中的安全需求

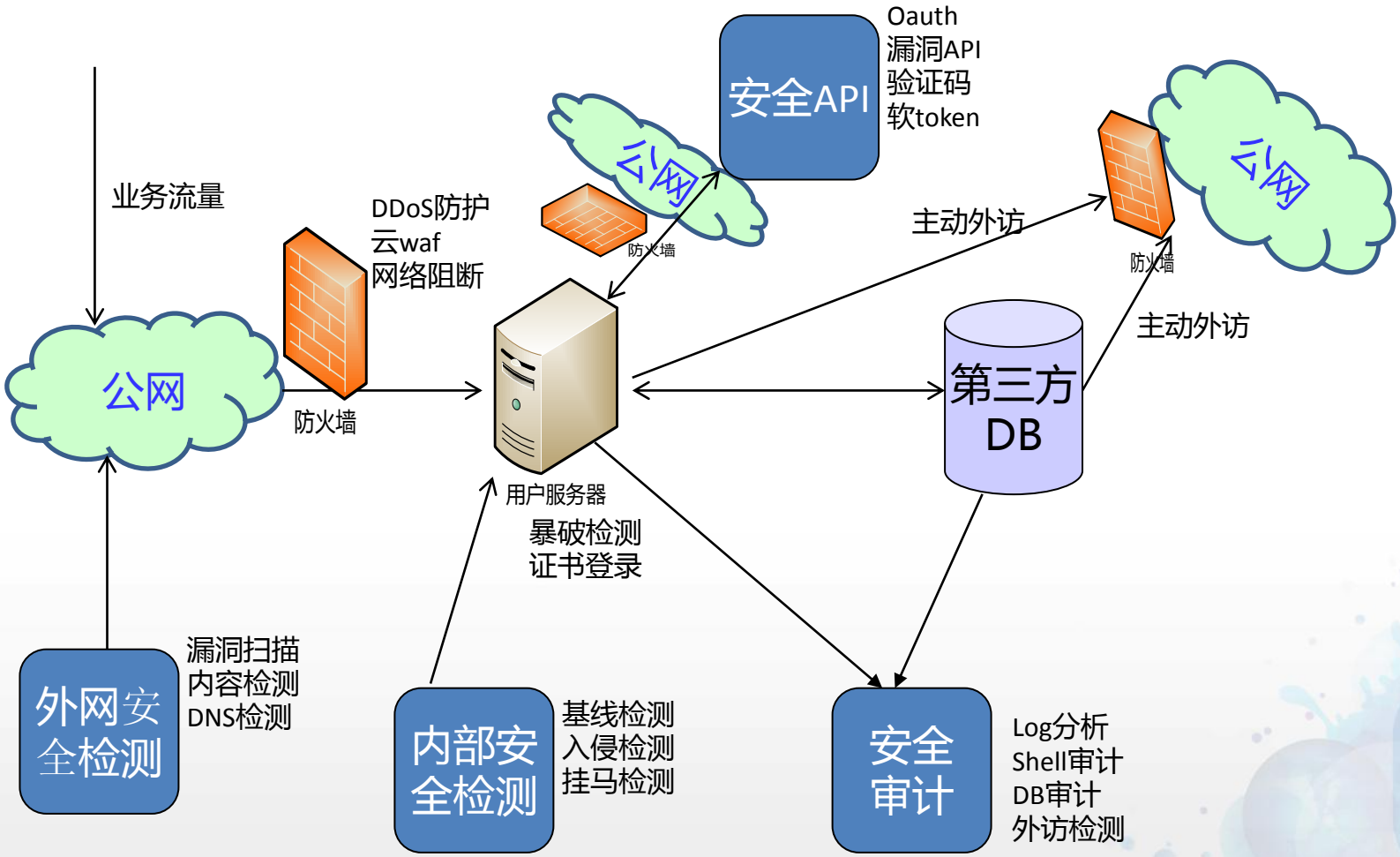
安全系统的要求：
有效隔离→安全防御→安全服务→内部审计



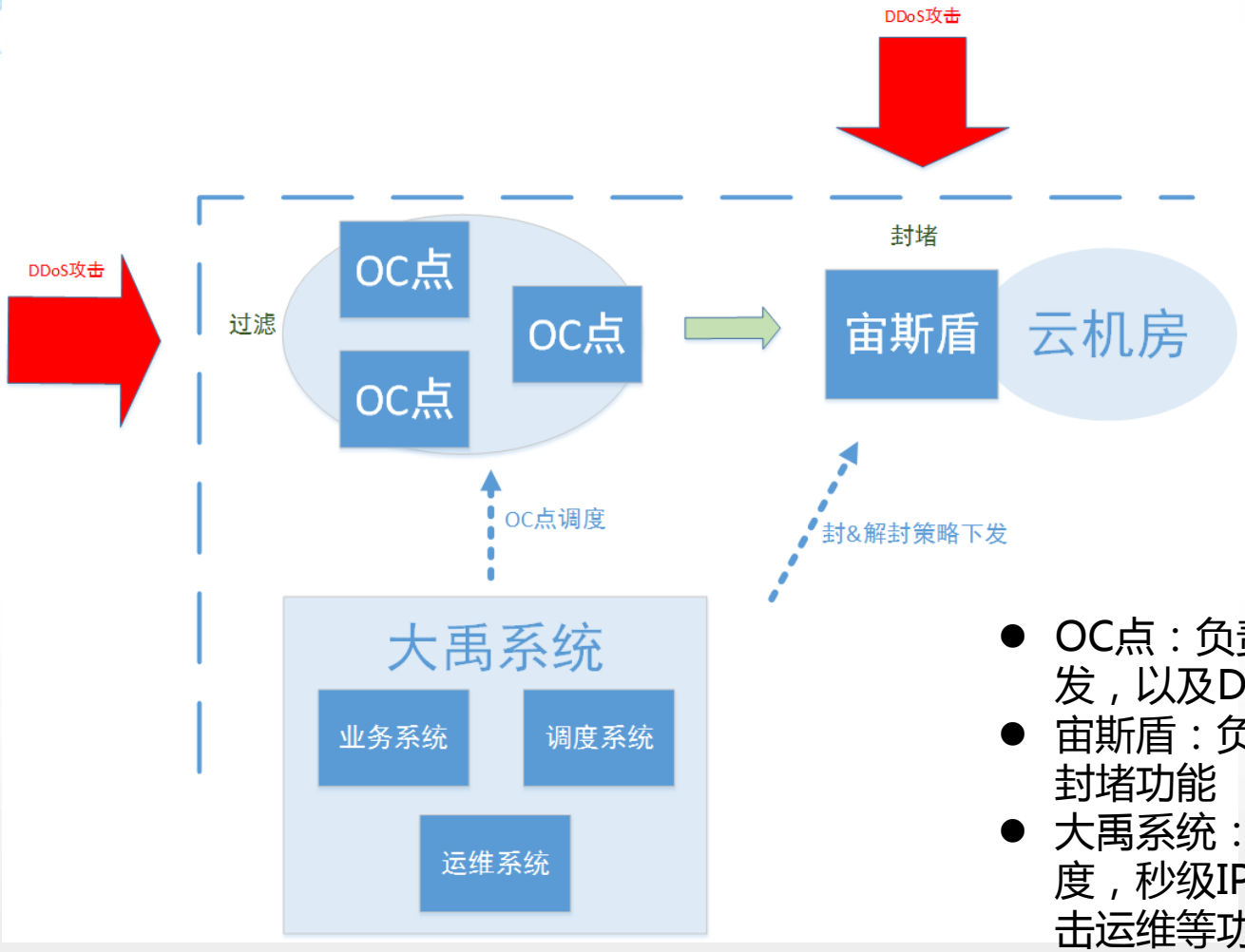
腾讯云的网络分区


远程桌面
隔离带
运营网
办公网
服务器
办公OA
其它端口
CITRIX访问登陆端口
ANY
私有端口
WEB端口
WEB端口
私有端口
WEB端口
MNET
OSSNET
TOOLSNET
DEVNET
其它端口
登陆端口
ANY
数据库端口
登陆端口
私有端口
私有端口
ANY
登陆端口
普通区
运营访问
核心数据区域
财付通专区
X-SVR专区
业务专区
安全域管理区
网管/NTP端口
网管/NTP端口
网管/NTP端口
NTPserver网管server
WEB
ANY
常规策略
禁止策略
默认策略

腾讯云安全系统架构


业务流量
DDoS防护
云waf
网络阻断
公网
防火墙
防火墙
云网
安全API
Oauth
漏洞API
验证码
软token
主动外访
防火墙
云网
主动外访
第三方
DB
用户服务器
暴破检测
证书登录
外网安全检测
漏洞扫描
内容检测
DNS检测
内部安全检测
基线检测
入侵检测
挂马检测
安全审计
Log分析
Shell审计
DB审计
外访检测

腾讯云安全DDoS防御系统—大禹

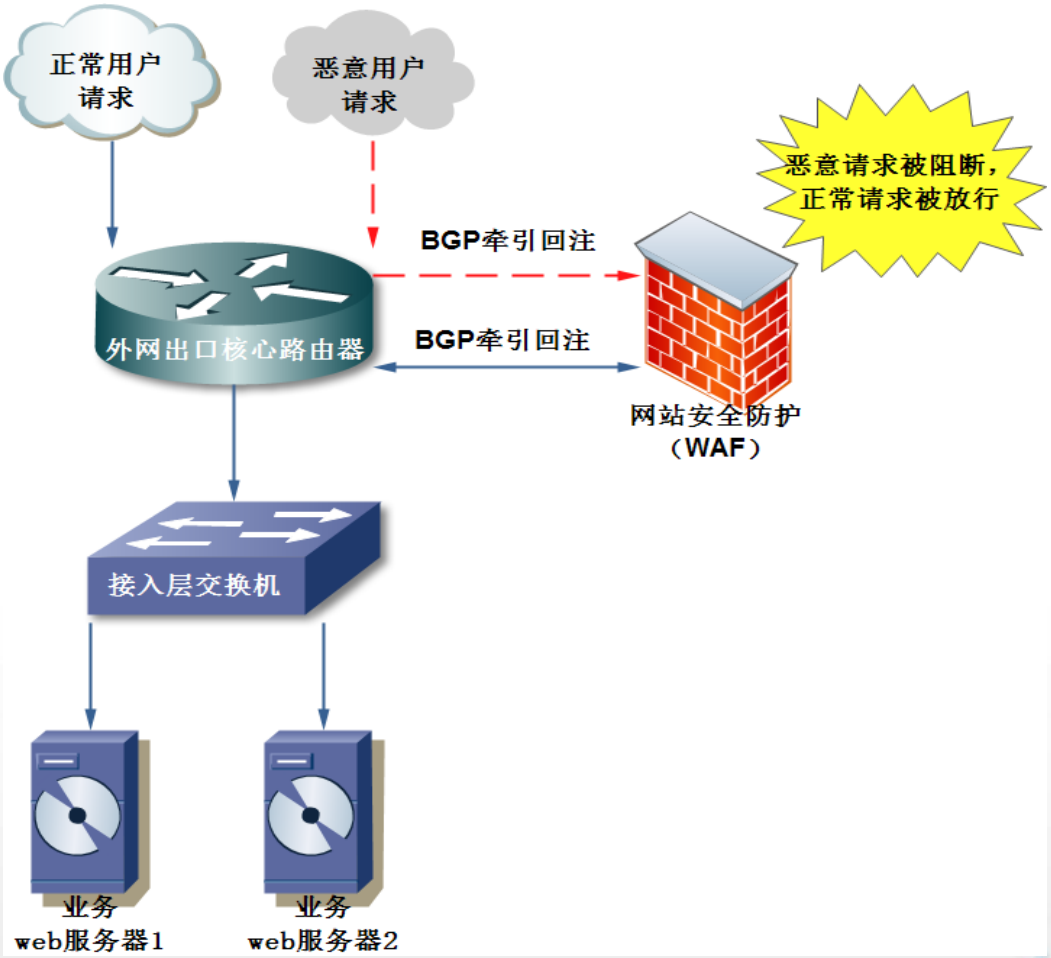


- OC点：负责用户业务接入、数据转发，以及DDoS攻击流量的过滤
- 宙斯盾：负责攻击流量拦截，和IP封堵功能
- 大禹系统：负责用户接入，流量调度，秒级IP封堵策略下发，DDoS攻击运维等功能

腾讯云安全DDoS防御系统—大禹

2014年累计防御攻击 2w+次，防御攻击时长 12w+分钟，最大单次攻击108G，清洗流量5T+

WAF


正常用户
请求
恶意用户
请求
恶意请求被阻断，
正常请求被放行
BGP牵引回注
外网出口核心路由器
BGP牵引回注
网站安全防护
（WAF）
接入层交换机
业务
web服务器1
业务
web服务器2

腾讯云的发布和运营

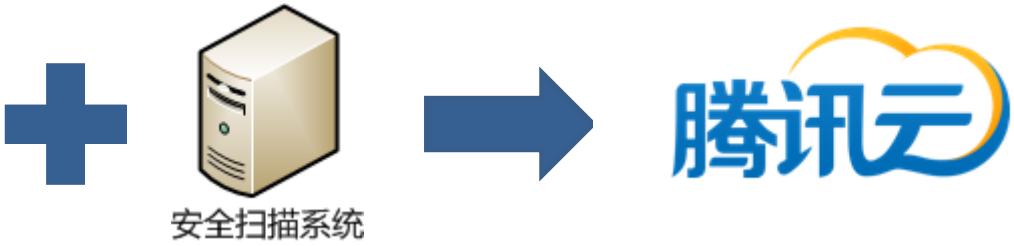
- 安全规范
  - 代码规范
  - 发布前安全检测
  - 应急安全准备
- 发布规范
  - 统一发布平台
  - 灰度发布
  - 现网观测
- 线上运营
  - 运维规范&连续性管理
  - 安全检测

重点：安全意识

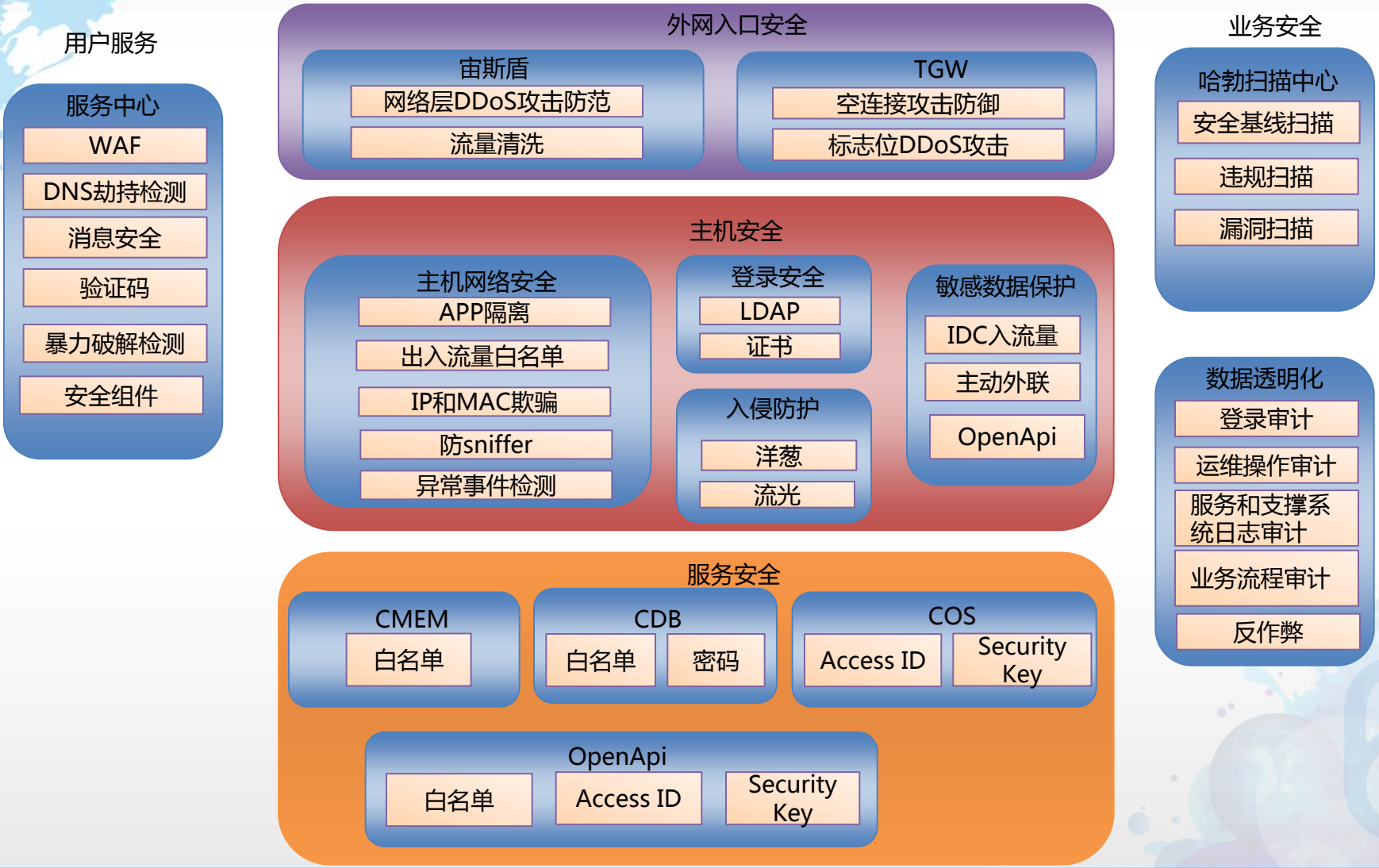
腾讯云的审计

腾讯云的安全问题发现&修复机制

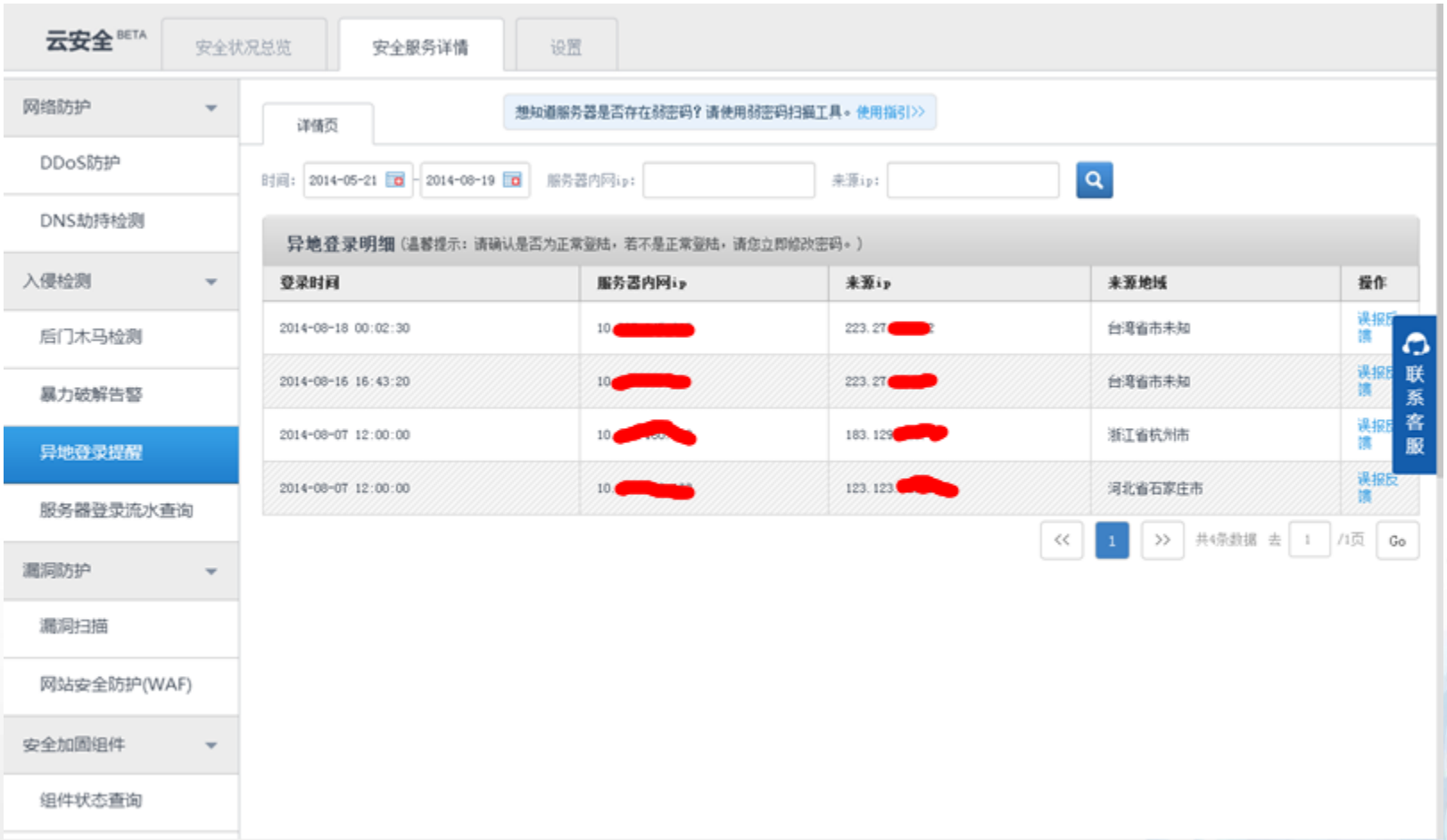
- TSRC



腾讯云安全功能框架


用户服务
服务中心
WAF
DNS劫持检测
消息安全
验证码
暴力破解检测
安全组件
外网入口安全
宙斯盾
网络层DDoS攻击防范
流量清洗
TGW
空连接攻击防御
标志位DDoS攻击
主机安全
主机网络安全
APP隔离
出入流量白名单
IP和MAC欺骗
防sniffer
异常事件检测
登录安全
LDAP
证书
入侵防护
洋葱
流光
敏感数据保护
IDC入流量
主动外联
OpenApi
服务安全
CMEM
白名单
CDB
白名单
密码
COS
Access ID
Security Key
OpenApi
白名单
Access ID
Security Key
业务安全
哈勃扫描中心
安全基线扫描
违规扫描
漏洞扫描
数据透明化
登录审计
运维操作审计
服务和支撑系统日志审计
业务流程审计
反作弊

腾讯云安全产品介绍


云安全 BETA
安全状况总览
安全服务详情
设置
网络防护
DDoS防护
DNS劫持检测
入侵检测
后门木马检测
暴力破解告警
异地登录提醒
服务器登录流水查询
漏洞防护
漏洞扫描
网站安全防护(WAF)
安全加固组件
组件状态查询
详情页
想知道服务器是否存在弱密码？请使用弱密码扫描工具。使用指引>>
时间：2014-05-21 - 2014-08-19
服务器内网ip：
来源ip：
异地登录明细（温馨提示：请确认是否为正常登陆，若不是正常登陆，请您立即修改密码。）
登录时间
服务器内网ip
来源ip
来源地域
操作
2014-08-18 00:02:30
台湾省市未知
2014-08-16 16:43:20
台湾省市未知
2014-08-07 12:00:00
浙江省杭州市
2014-08-07 12:00:00
河北省石家庄市
<< 1 >>
共4条数据 去 1 /1页 Go
联系客服

DNS劫持检测

1）Local DNS劫持监测

覆盖全国各主要城市Local DNS

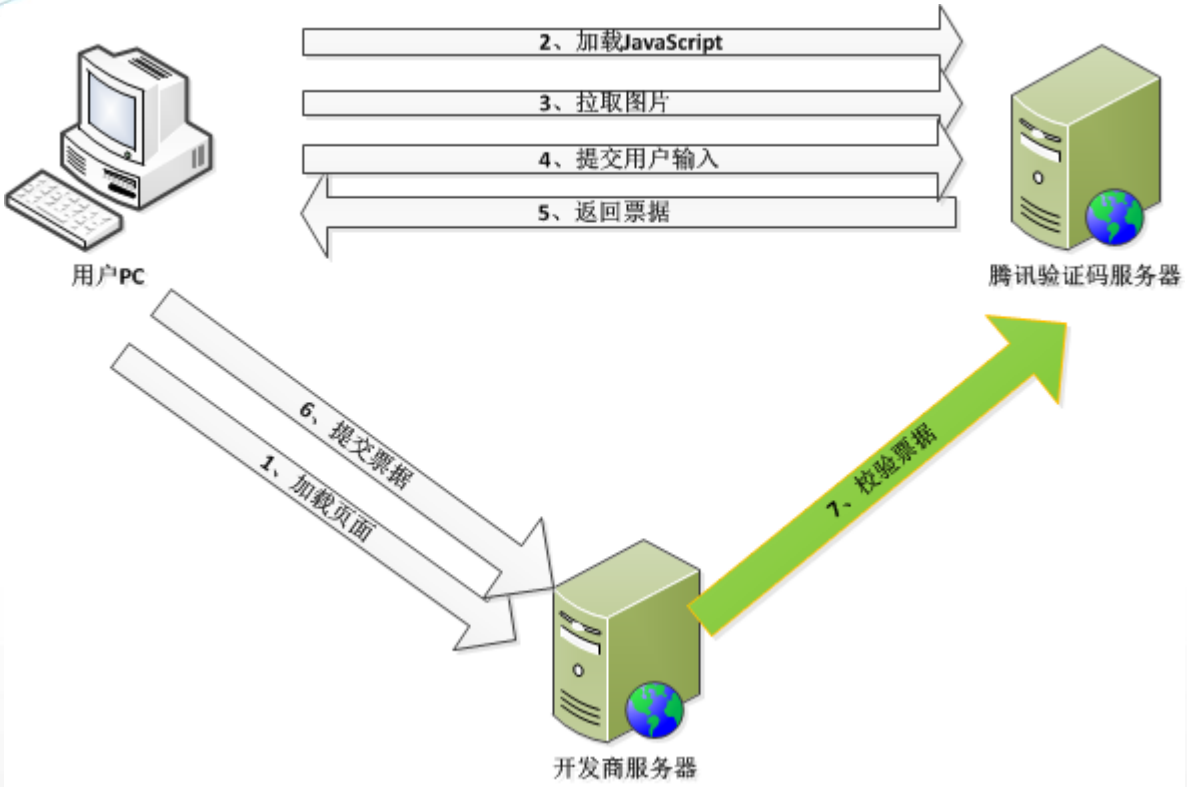
2）权威DNS篡改

权威DNS监测

报警子类型	覆盖用户数	细节
域名注册信息篡改告警	0	域名[redacted]注册信息发生变动，请关注(from:[redacted])
域名注册信息篡改告警	0	域名[redacted]注册信息发生变动，请关注(from:[redacted])
[单个域名在>2个LDNS的异常解析率大于5%]	11000	[DNS]系统发现,域名:[redacted]在2.5小时内，非故障类的解析异常比例超过5%的LDNS数为3，LDNS以及解析的详细信息为(TOP 2)，LDNS:[redacted](中国福建福州,移动,3499,7,2.05%)，解析信息：有风险：39%；
[单个域名在>2个LDNS的异常解析率大于5%]	11000	[DNS]系统发现,域名:[redacted]在2.5小时内，非故障类的解析异常比例超过5%的LDNS数为7，LDNS以及解析的详细信息为(TOP 2)，LDNS:[redacted](中国福建福州,移动,3499,7,2.05%)，解析信息：有风险：38.7%；

security.tencent.com

腾讯云安全API—验证码服务



安全便捷

稳定高效

接入简单

轻松维护

腾讯云安全防御效果

用户量

- 腾讯云安全服务开发者1w+

DDoS防护

- 2014年累计防护2w+次，最大攻击流量108G，平均防护生效时延<10s

漏洞防护

- 对使用了云安全漏洞扫描的业务，自动扫描，日均发现漏洞上千个
- 提供云waf功能，对恶意攻击进行透明过滤，时延毫秒级

违规发现

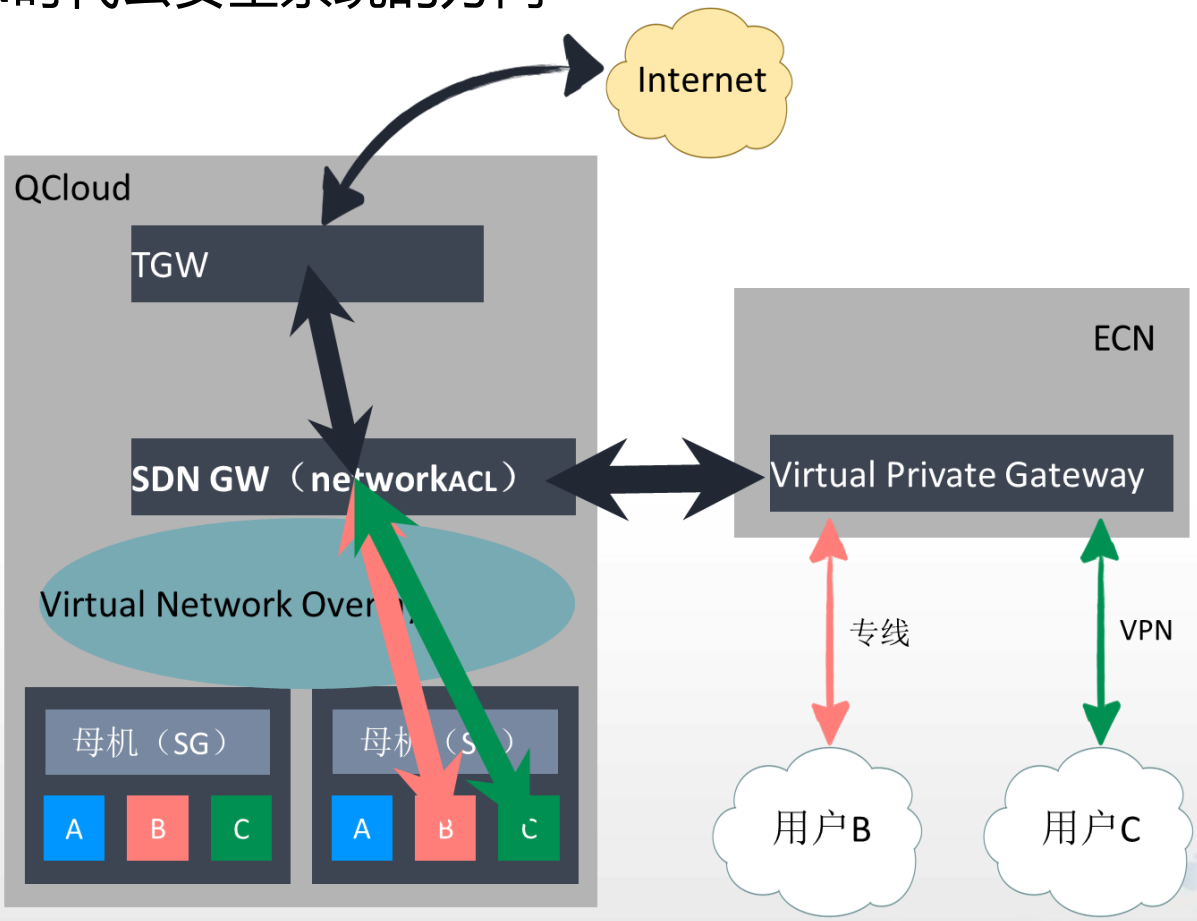
- 分钟级的违规发现能力

入侵检测

- 多渠道及时发现客户云服务器被入侵情况，日均发现数十起入侵事件
- 提供弱密码检测工具、证书登录等方式，帮助客户进行预防

腾讯云安全未来的方向思考

- SDN时代云安全系统的方向



Q&A

THANKS

SequeMedia 盛拓传媒 | IT168 www.it168.com | ChinaUnix | ITPUB

欢迎随时沟通

bblue@qq.com
bluezhou@tencent.com