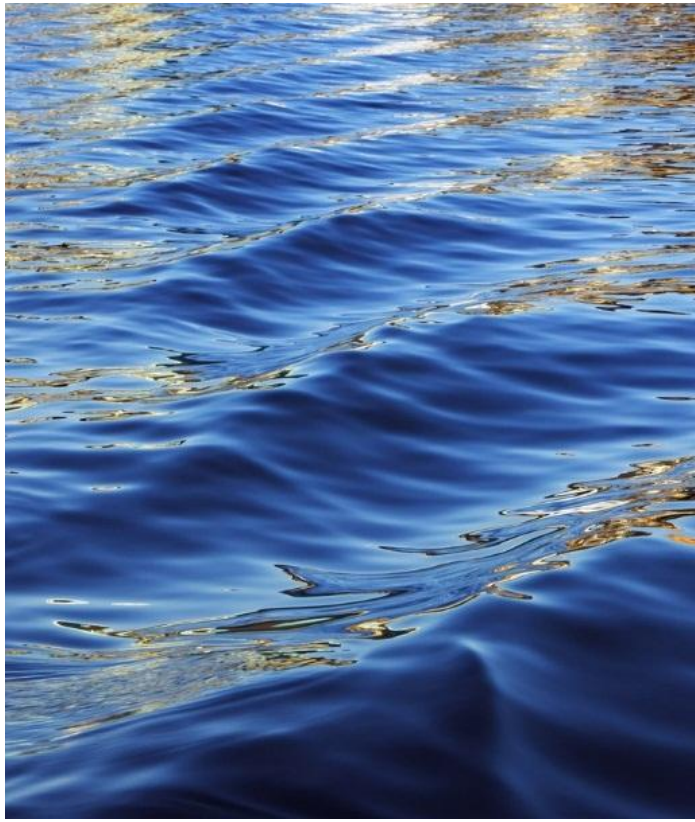
云计算安全等级保护关键保护关键问题探讨

国家信息中心
赵睿斌　博士



汇报提纲

近期信息安全热点事件分析

云等级保护能够提升云安全能力

“互联网+”时代的企业安全何去何从

面临太多不安全因素

木马
病毒
钓鱼链接

账号被盗
手机丢失
信息泄露

黑客攻击
信息窃取
信息篡改

虚拟社会
有害信息
政治危害
不良传播

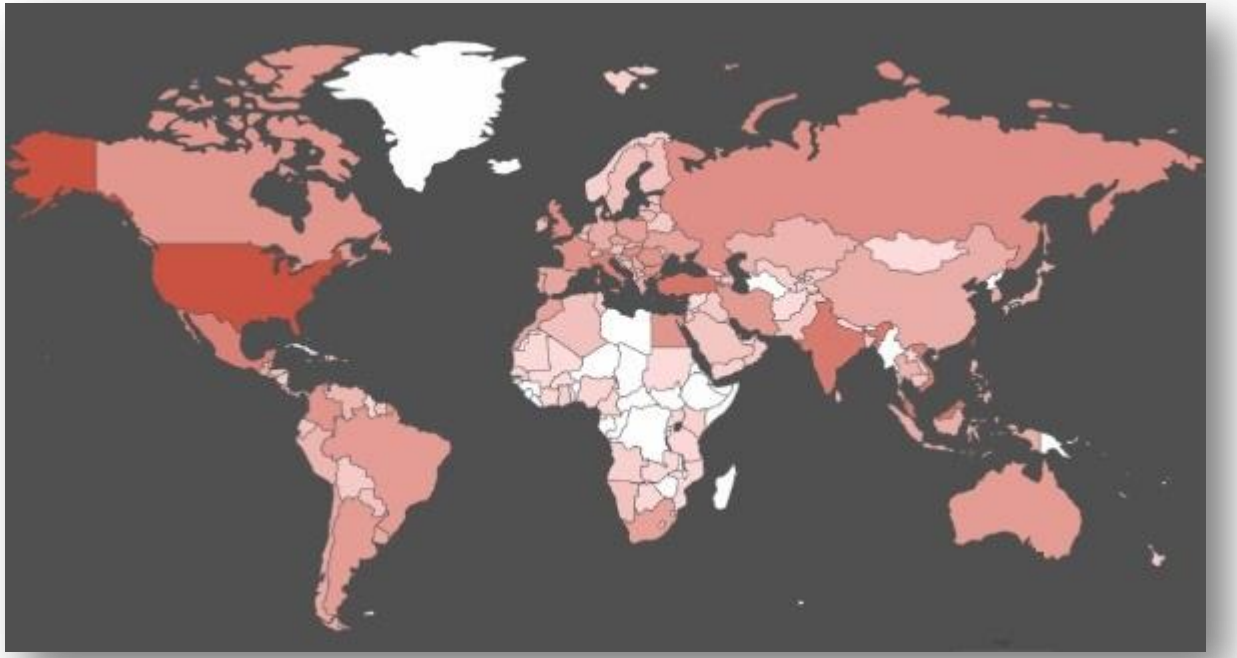
优酷被黑 1亿账户在暗网出售

几个月前，一个网络黑市商家兜售了10亿个被盗的中国网络巨头的用户账户。现在，CosmicDark上的一个黑市商家刚上架了一个用户数据库，该数据库包含了100,759,591个被盗的优酷用户账户。根据供应商的描述，该数据库中的数据是在2016年和今年年初在互联网上泄露的。CosmicDark上整个数据包的售价为300美元，截至目前数据库来源尚不清楚。数据包含电子邮件和可用MD5、SHA1散列解密的密码。就CosmicDark站点上作为样本的552个数据来看，常见的邮件地址后缀包括 @163.com 、 @qq.com 以及 @xiaonei.com。必须注意的是，这些作为样本提供的密码已经完全解密并在在互联网上公开。此外HaveIbeenpwned平台（该平台为访问者提供检查账户是否已被入侵的服务）也已证实了这次数据泄露事件。

NSA武器泄漏引发网络世界“核弹危机”

日前，据称是美国国家安全局（NSA）旗下的“方程式黑客组织”使用的部分网络武器被公开，其中包括可以远程攻破全球约70%Windows机器的漏洞利用工具。360安全卫士官方微博发布红色警报称，经紧急验证这些工具真实有效，360正密切监测和响应此次网络世界的重大灾难级危机。据了解，这些曝光的文件包含了多个Windows“神洞”的利用工具，不需要用户任何操作，只要联网就可以远程攻击，和多年前的冲击波、震荡波、Conficker等蠕虫一样可以瞬间血洗互联网。NSA武器公开将引发网络世界的腥风血雨。对个人用户来说，木马黑产很可能会改造NSA武器对普通网民发动攻击，制作出类似冲击波的蠕虫大规模传播，此次事件的影响不亚于一场核弹危机。对企业来说，国内大量高校、政府单位、国企以及互联网公司正在使用Windows服务器和办公电脑，漏洞涉及的系统组件也属于企业办公基础服务，如果没有及时应对，企业将面临着被不法分子轻易入侵渗透的风险。

全新物联网/Linux 恶意软件攻击数字视频录像机并组建僵尸网络



受漏洞影响的TVT Digital DVR设备分布图

Palo Alto Networks 威胁情报小组Unit 42近日发布报告宣称发现物联网/Linux僵尸网络Tsunami的最新变种并命名为Amnesia。Amnesia僵尸网络允许攻击者利用未修补的远程代码执行针对数字视频录像机(DVR)设备的漏洞攻击，2016年3月这一漏洞就被发现并公布，这些DVR设备由TVT Digital 生产并 通过70多家合作伙伴分销至全球。全球约有227000台设备受此漏洞影响，主要覆盖国家和地区包括：台湾、美国、以色列、土耳其和印度。Amnesia会探测其是否运行于VirtualBox、VMware或者QEMU虚机之上，一旦探测出这些运行环境Amnesia便会删除文件系统中的所有文件 ，从而卸载虚拟Linux系统，这不仅会影响到恶意软件分析沙箱的正常工作，还会影响到某些VPS和公有云中的QEMU Linux服务器。Amnesia通过远程代码执行对系统漏洞进行扫描、定位和攻击，攻击成功后Amnesia会实现对设备的全盘掌控。攻击者还会操纵Amnesia僵尸网络发动大规模的DDoS攻击，其猛烈程度如同2016年秋天我们见到的Mirai的僵尸网络攻击一样。

网络安全监督机构发现大型跨国网络攻击APT10

4月5日，对美国、日本、瑞典和其他欧洲国家公司通过IT服务商发起的大型网络攻击被曝光。该网络攻击由英国国家网络安全中心、普华永道和 BAE System 网络安全公司的合作发现。该攻击至少从2016年5月甚至可能早在2014年起，就试图获取托管服务商客户内部网络的访问权限。该攻击源自APT10，被命名为“Cloud Hopper” 。瑞典民事应急机构在声明中称其准确规模尚未可知，但据信涉及海量数据。该机构没有说明此网络攻击是否仍在进行。瑞典的高度数字化，以及大量服务外包给托管服务商的事实，意味着多家瑞典公司在该攻击的影响下会处于巨大的安全风险中。该机构称，这些攻击背后的黑客使用了大量资源来锁定其目标，并发送高端网络钓鱼邮件来感染计算机。据称，瑞典IP地址也被用于协同入侵和取回被盗数据，APT10的攻击尤其针对IT、通信、医疗保健、能源和研究机构等目标。

苹果手机用户注意 这个漏洞能在WiFi芯片上执行任意代码

苹果公司没给出多少细节，但你肯定不想漏掉本次最新iOS更新——10.3.1——因为它修复了一个非常讨厌的WiFi漏洞。苹果匆忙推出紧急更新是因为：“范围内的攻击者可能在WiFi芯片上执行任意代码。”——意味着恶意代码包可能赋予攻击者攻击平台。漏洞来源于谷歌Project Zero ，是个缓冲区溢出漏洞，可通过更好的输入验证解决。该漏洞影响 iPhone 5及以上版本，iPad 4代及更新机型，还有iPod touch 6代及更新版本。10.3.1更新仅在10.3放出后1周就发布了。虽然10.3摒除了32位设备，10.3.1却又包含了进来——暗示苹果对该漏洞的重视程度。

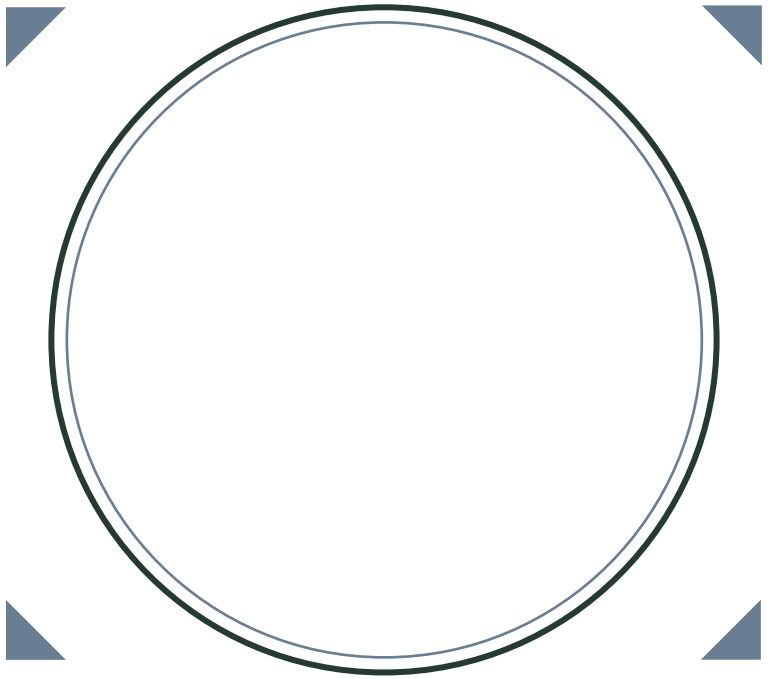
国内安全事件

2016.07 视频类

乐视视频网站7月19日发布声明称遭遇了自家有史以来最大一次DDoS攻击，峰值流量高达200G，致使大量用户无法正常访问。

2015.04 酒店类

七大知名品牌酒店被曝存在严重安全漏洞，房客开房信息一览无余，还可对酒店订单进行修改。



2015.02 金融类

国内四大比特币交易平台：火币网、OKcoin、比特币中国以及中国比特币先后遭到恶意DDoS攻击，导致平台登录困难。

2015.12 物流类

申通使用的某通用软件被曝存在13个安全漏洞，导致3万多客户信息被窃取，用于非法出售。

应用安全事件诱因

SQL注入

利用现有的应用程序，将恶意的SQL命令注入到后台数据库，得到一个存在安全漏洞的网上数据库。

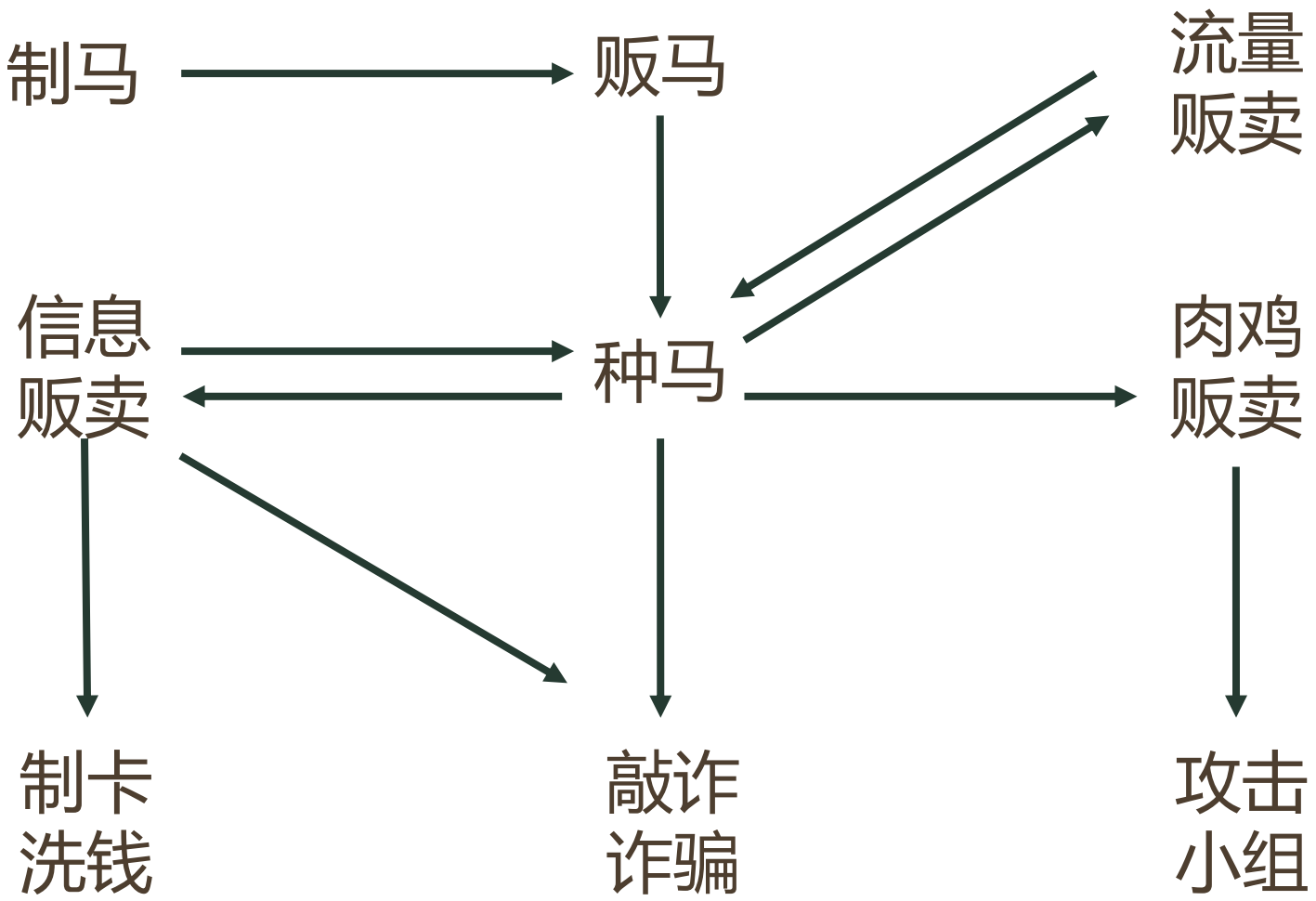
XSS攻击

跨站脚本攻击，利用网站漏洞从用户那里恶意盗取信息，用户在浏览网站、使用即时通讯软件、甚至在阅读电子邮件时，通常会点击其中的链接。攻击者通过在链接中插入恶意代码，就能够盗取用户信息。

黑客拖库

指网站遭到入侵后，黑客窃取其数据库。

黑色产业链日益猖獗



汇报提纲

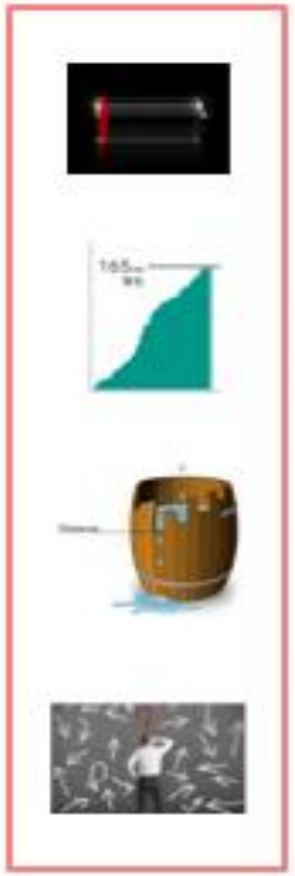
近期信息安全热点事件分析

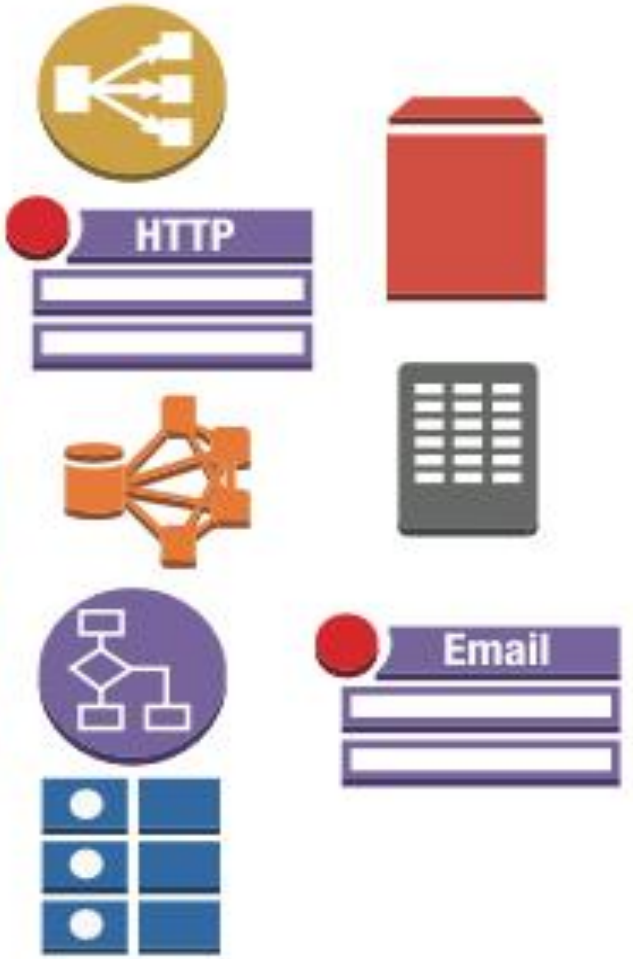
云等级保护能够提升云安全能力

“互联网+”时代的企业安全何去何从

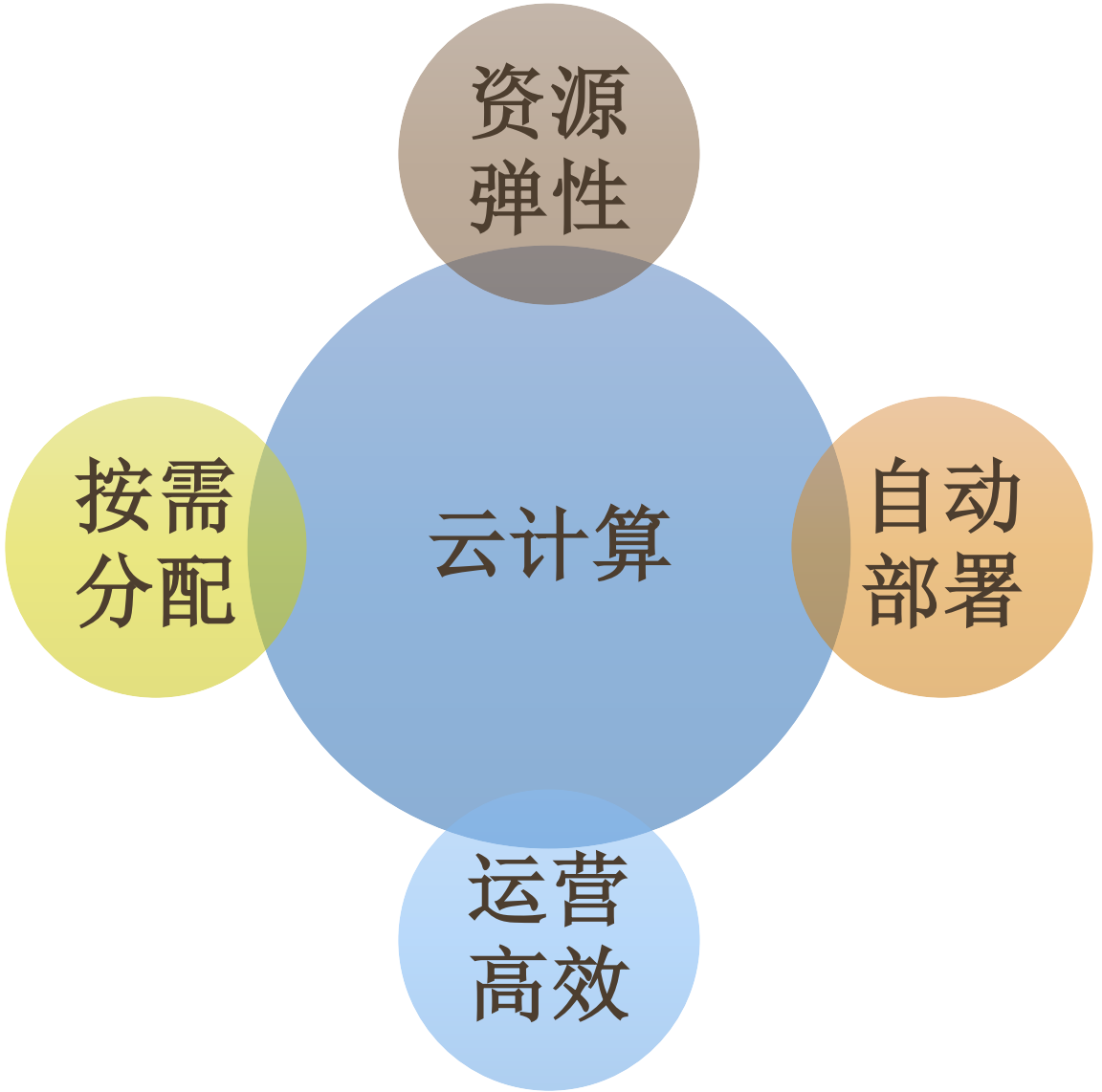
云平台在“互联网+”时代面临更多安全威胁

◆移动应用数量众多
◆管理难度大
◆通道复杂，云端混乱，资源浪费

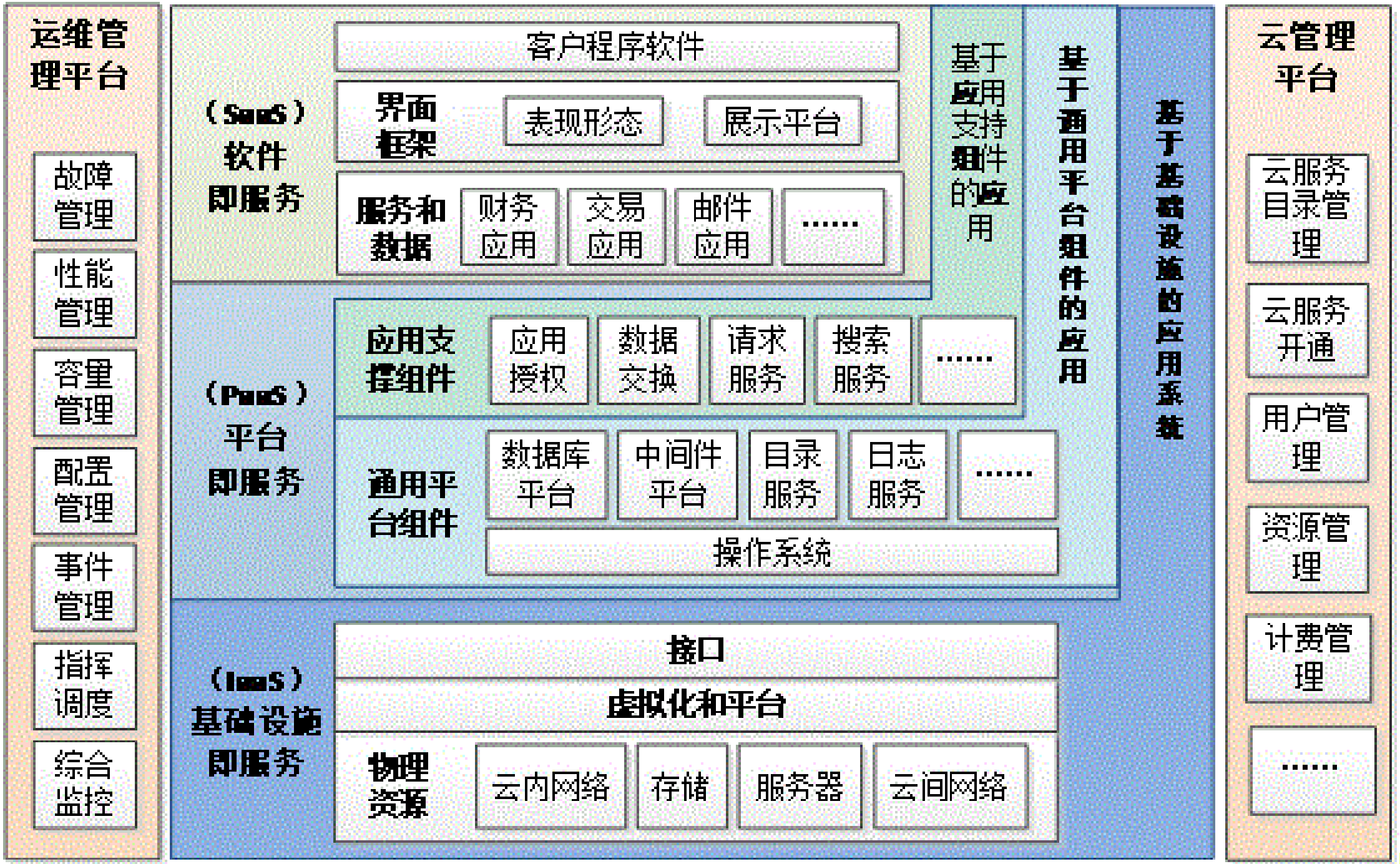




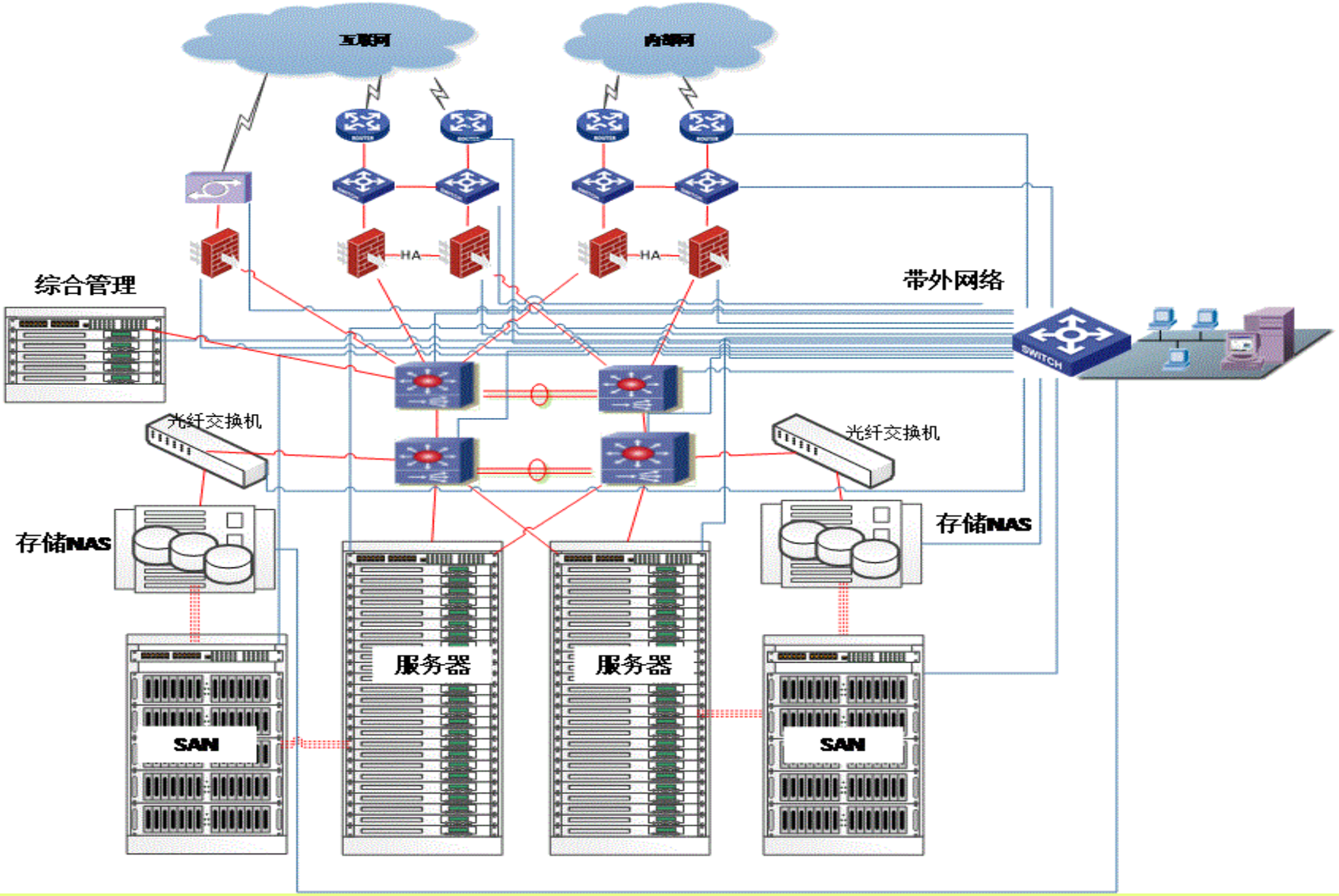
云计算四大特点



云计算系统逻辑结构

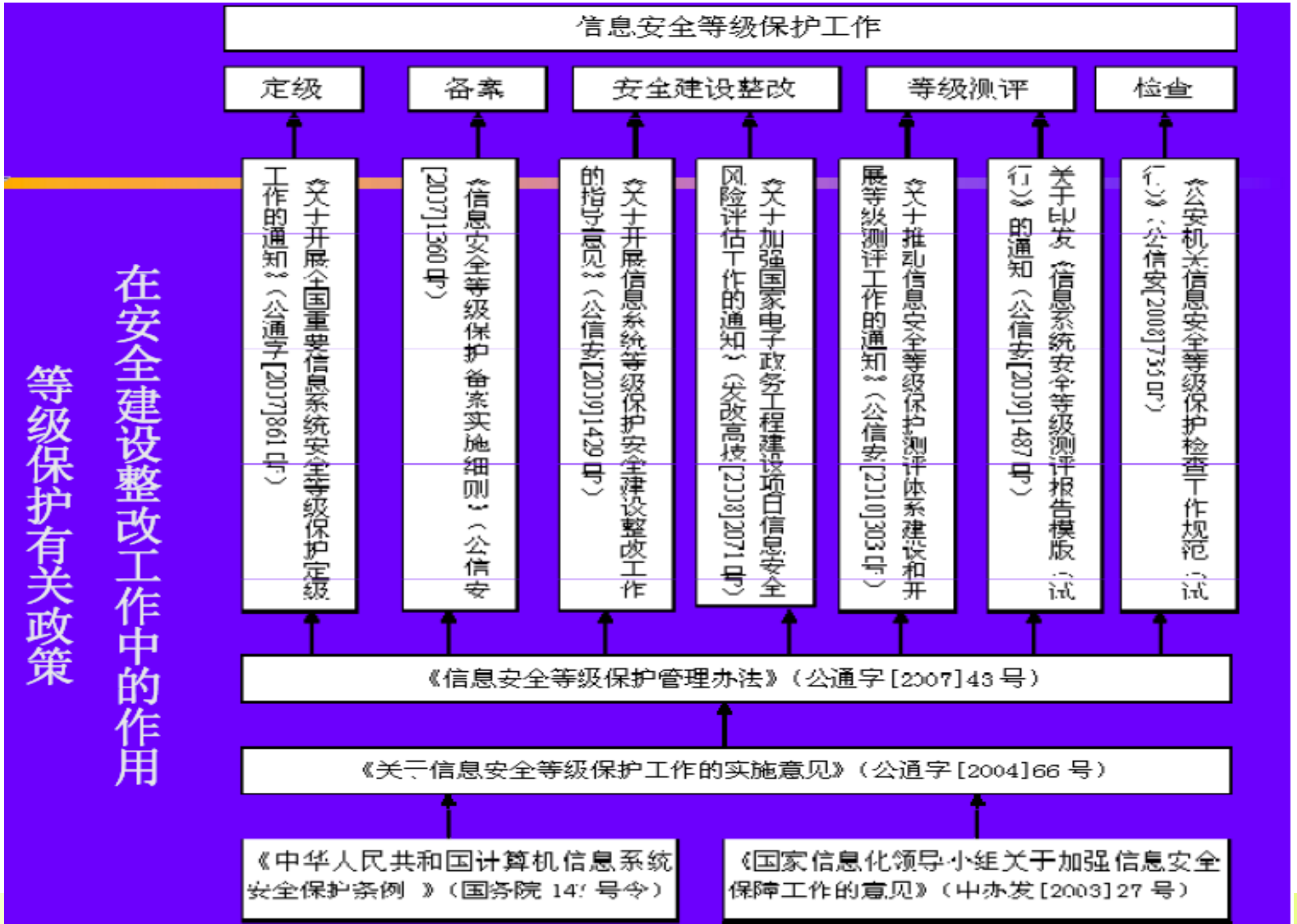

运维管理平台
故障管理
性能管理
容量管理
配置管理
事件管理
指挥调度
综合监控
（SaaS）软件即服务
客户程序软件
界面框架
表现形态
展示平台
服务和数据
财务应用
交易应用
邮件应用
……
基于应用支持组件的应用
（PaaS）平台即服务
应用支撑组件
应用授权
数据交换
请求服务
搜索服务
……
通用平台组件
数据库平台
中间件平台
目录服务
日志服务
……
操作系统
基于通用平台组件的应用
（IaaS）基础设施即服务
接口
虚拟化和平台
物理资源
云内网络
存储
服务器
云间网络
基于基础设施的应用系统
云管理平台
云服务目录管理
云服务开通
用户管理
资源管理
计费管理
……

云计算系统的典型架构


互联网
内部网
HA
HA
综合管理
带外网络
SWITCH
光纤交换机
光纤交换机
存储NAS
存储NAS
服务器
服务器
SAN
SAN

信息安全等级保护工作基础-法规政策

- 《中华人民共和国计算机信息系统安全保护条例 》（国务院147号令）
- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）
- 《关于信息安全等级保护工作的实施意见》（公通字[2004] 66号）
- 《信息安全等级保护管理办法》（公通字[2007]43号）
- 《信息安全等级保护备案实施细则》（公信安[2007] 1360号）
- 《公安机关信息安全等级保护检查工作规范（试行）》（公信安[2008]736号）
- 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）
- 《政府信息系统安全检查办法》（国办发[2009]28号）
- 《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）


信息安全等级保护工作
定级
备案
安全建设整改
等级测评
检查
《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字[2007]861号）
《信息安全等级保护备案实施细则》（公信安[2007]1360号）
《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）
《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2003]2071号）
《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）
关于印发《信息系统安全等级测评报告模版（试行）》的通知（公信安[2009]1487号）
《公安机关信息安全等级保护检查工作规范（试行）》（公信安[2008]736号）
《信息安全等级保护管理办法》（公通字[2007]43号）
《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）
《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）
《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）
在安全建设整改工作中的作用
等级保护有关政策

面向云特有技术/管理的安全问题

服务 | 架构 | 方案 | 设备 | 用户 | 安全措施 | 事件

关心的问题

- 虚拟化厂商没有把接口完全开放，在vSwtich网间流量方面的问题：如何控制南北流量问题和东西流量问题？如何做到云平台中的所有流量的监控?
- 虚拟机在迁移情况下如何做安全防护？
- 云计算信息系统的边界划分问题，如何做好云计算信息系统的边界划分？
- 桌面云中每个虚拟机在进行文件备份时，是如何实现增量备份的？
- 传统架构的安全防护和云计算环境下的安全防护的区别？
- 如何做好传统信息系统入云前的安全检查测试，入云后的安全防护？
- 云和服务器虚拟化的区别？
- 混合云中如何做好安全防护？
- 如何做好虚拟机的安全访问控制？
- 如何做好虚拟机间的安全隔离的？
- 如何防范虚拟机的逃逸？
- 如何能防止虚拟机的内存数据不被窃取？
- 是如何来实现虚拟机加固的？

云安全等级保护研究的意义、必要性

云计算威胁

云计算信息系统相较于传统信息系统，无论需要对抗的外部威胁还是对抗威胁的技术手段都发生较大的变化。

国内国际情况

国际和国内目前都没有一个完整的、广泛认可的云计算信息系统安全等级保护要求相关的安全标准。

云计算等保标准缺失

标准的缺失使得云计算信息系统安全等级保护制度的落实和推广无法全面实施，在一定程度上阻碍了云计算信息系统的安全建设和安全保障工作。

测评缺乏参考标准

权威的、系统的测评标准的缺失，测试评估结果在一定程度上得不到用户的认可，使得用户在建设、使用、维护云计算信息系统时，在租用云服务时，缺乏信心和必要的安全保障，从而在一定程度上限制了我国云计算产业的发展。

云安全等级保护标准研究的目的

标准编写目的

标准基于《信息安全等级保护云计算基本要求》，为云计算等级保护监督检查、测评工作参考依据，为系统建设、使用、维护提供参考。

基本要求

为评价云计算信息系统是否符合《信息安全等级保护云计算基本要求》提供获取证据的途径和方法。用以指导测评人员从信息安全等级保护的角度对云计算信息系统进行测试评估。

提供依据

为信息安全监管职能部门、信息安全测评服务机构、信息系统的主管部门及运营使用单位在进行针对云计算信息系统安全等级保护相关监督检查、测评评估等工作时，提供相关参考依据。

参考标准

为云计算信息系统的建设、使用、维护提供体系化的参考依据，为云服务用户提供必要的安全保障依据。

研究路径

- 实际应用环境调研
- 国内外相关成果研究

- 确定云计算环境安全检查与评估指标框架

- 云计算环境面临的威胁与风险分析

- 导出云计算环境安全保护基本要求

- 针对每项要求，结合保护对象、测试方法，给出测评指标项及判定标准

- 确定指标打分模型

- 汇总完成指标体系

- 业务试点及反馈

研究方式

云服务门户安全

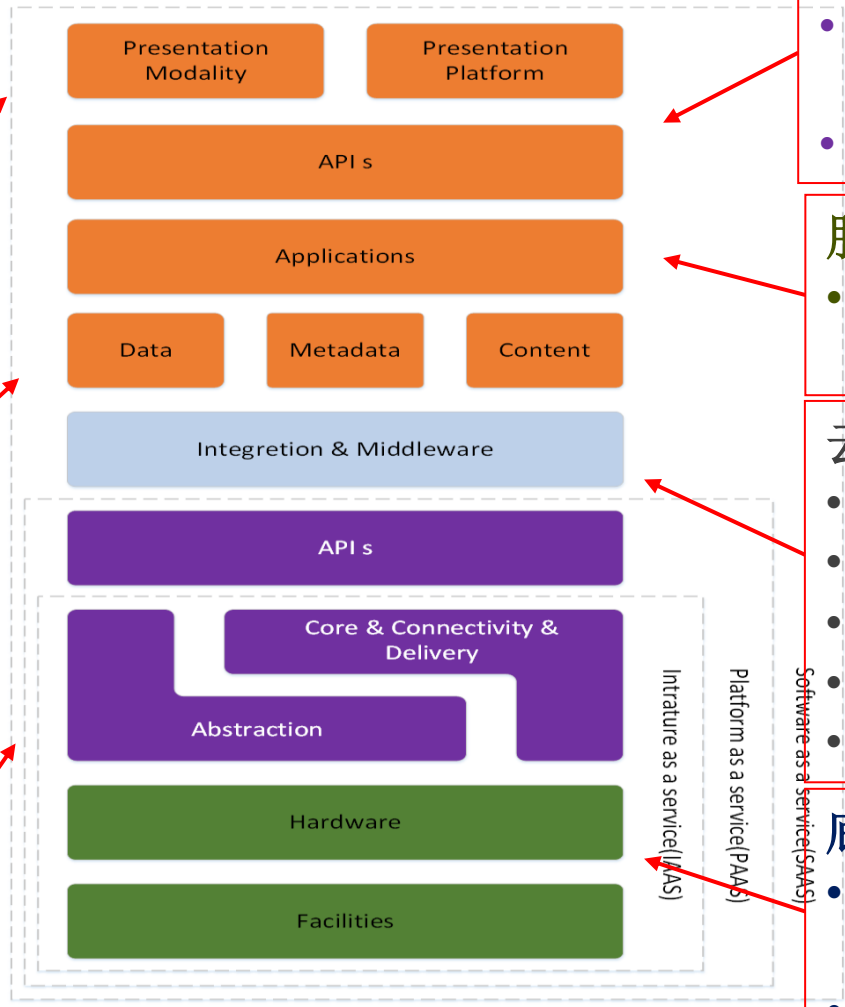
- 双向身份鉴别
- 传输加密
- 门户防DDOS攻击
- 门户防入侵
- 用户流量隔离(防流量渗入)

数据安全

- 数据隔离
- 数据完整性、保密性

虚拟化安全

- 虚拟机间的“溢出”监控与阻断
- 虚拟机流量识别
- 虚拟机迁移、操作日志审计
- 虚拟机内安全监控与用户行为审计、病毒过滤
- 虚拟化系统加固
- 虚拟机映像安全、数据安全



多租户隔离

- 多租户共享的情况下实现资源、环境、数据隔离
- 租户的身份认证、访问控制

服务水平协议管理

- 云服务内容、责任与权限、惩罚措施、服务能力监督

云管理平台安全

- 平台内部安全监控
- 管理行为审计
- 用户行为审计
- 云服务及接口安全
- 操作日志

底层数据备份等

- 多数据中心、多资源池的备份容灾
- 虚拟机备份与恢复
- 云存储备份与恢复

云安全等级保护标准编制思路

研究

通过对云计算信息系统安全保护结构的深入研究、云计算信息系统威胁与风险的分析、云计算信息系统安全保护的对象特征以及关键点的定位，对***《信息安全等级保护云计算基本要求》***中的要求项所应对的风险、作用的范围、作用的对象、可采用的措施及技术手段进行研究。

条款编制

以***《信息安全等级保护云计算基本要求》***的具体要求为测评项，逐条逐级规范化测试对象、测试方法、实施细则等内容，并给出结果判定依据。

云安全等级保护技术测评

数据安全与备份恢复测评部分包括数据完整性测评、数据保密性测评、备份与恢复测评。

应用安全测评部分包括安全审计测评、资源控制测评、接口安全测评。

主机安全测评部分包括访问控制测评、安全审计测评、剩余信息保护测评、入侵防范测评、恶意代码防范测评、资源控制测评、镜像与快照保护测评。

网络安全测评部分包括网络架构测评、访问控制测评、远程访问测评、入侵防范测评、安全审计测评、网络设备防护测评。

物理安全测评部分包括物理位置的选择测评。

云安全等级保护测评技术主要研究内容

物理安全测评内容

测评物理设备是否位于境内

应用安全测评内容

1、对云服务方、云租户各自控制部分进行审计和集中审计，并为数据审计汇集提供接口进行测评。

2、测评是否对应用系统运行进行监控，测评不同云租户应用系统与开发平台间是否隔离。

3、测评云服务对外接口安全性。

数据安全及备份恢复测评内容

1、测评虚拟机迁移过程的数据完整性、保密性。

2、测评云租户加密方案和解密方案，及数据备份方案。

3、测评云服务商是否提供云租户数据及备份存储位置，不同云租户审计数据是否隔离存放，以及是否能保证云租户业务数据迁移到其他云或本地。

云安全等级保护技术测评内容

网络安全测评内容

访问控制测评内容

1、测评虚拟机是否可非授权访问虚拟机。

2、测评访问控制设备、措施、管理模块和虚拟机迁移时策略是否随之迁移。

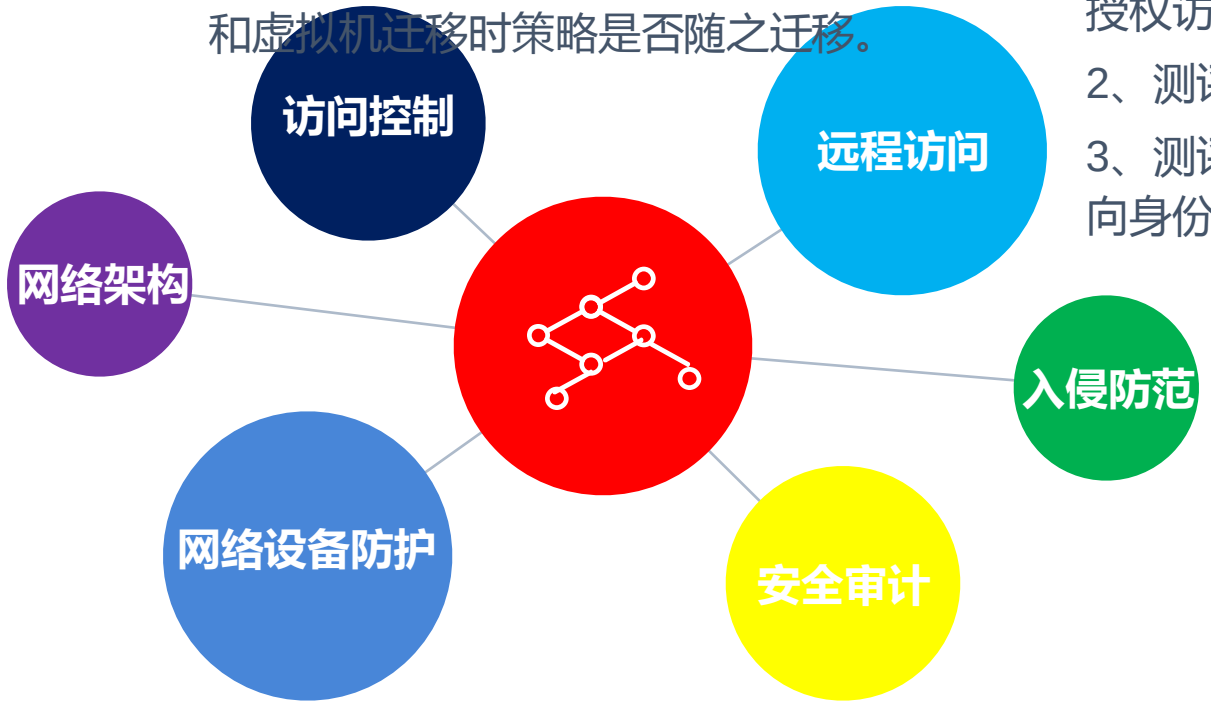
网络架构测评内容

1、测评虚拟化网络资源和网络拓扑是否实时更新。

2、测评广播时接受报文情况，测评流量是否可以识别，并对异常流量日志记录。

3、测评资源池划分、资源隔离。

4、测评是否开放接口允许第三方安全产品接入，及接口安全型。



远程访问测评内容

1、测评是否对远程连接监控，及非授权访问应对措施。

2、测评是否对特权命令审计

3、测评云平台和管理终端间是否双向身份验证。

入侵防范测评内容

1、测评对入侵行为的检测、防范和审计。测评入侵防范规则库的更新。

2、测评对互联网有害信息的检测。

网络设备防护测评内容

测评网络策略控制器和网络设备间双向身份验证机制。

安全审计测评内容

1、测评云租户、云服务方各自控制部分的审计数据的收集和集中审计。

2、测评是否提供审计数据汇集接口，可供第三方审计。

云安全等级保护技术测评内容

访问控制测评内容

1、测评是否设置专门运维终端。

2、测评云服务提供商对云租户数据库的权限。

3、测评管理员权限分离。

镜像和快照保护测评内容

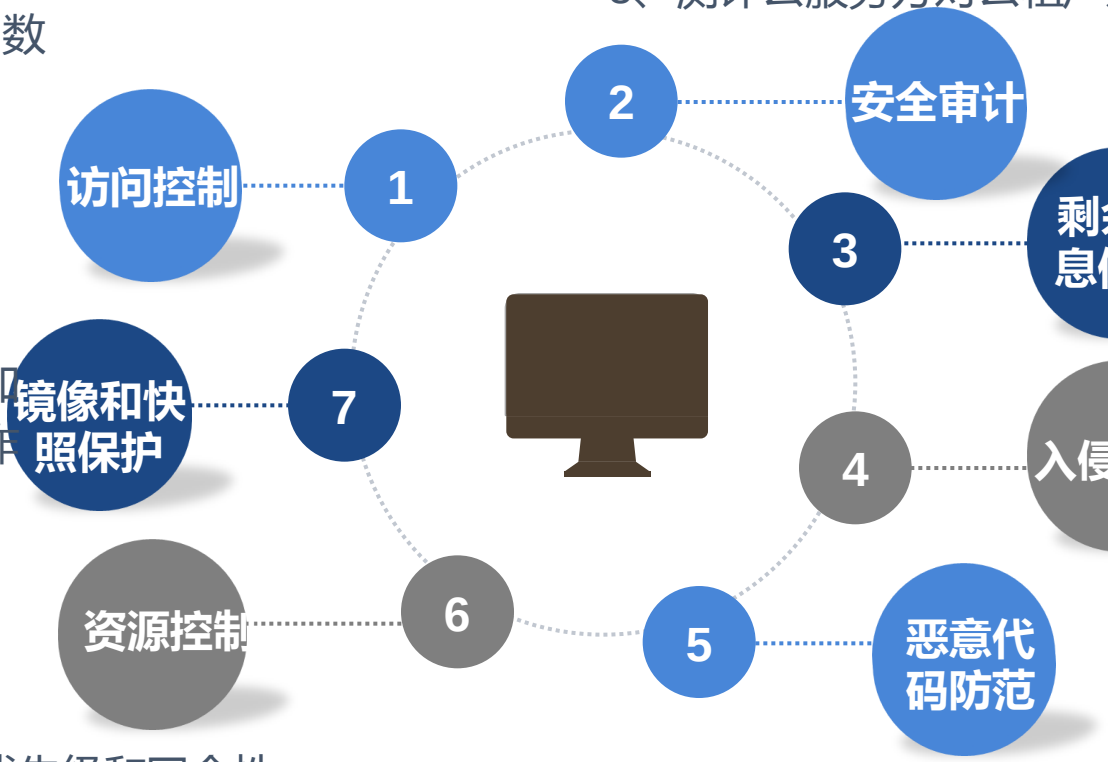
测评镜像快照的完整性校验、加密、和重要业务系统加固的操作系统镜像。

资源控制测评内容

测评资源的管理调度、分配、优先级和冗余性。

测评虚拟机网络接口带宽配置及监控方式。

测评是否部署监控信息汇集接口，并集中监控。



安全审计测评内容

1、测评云服务方和云租户各自控制部分数据的收集和集中审计。

2、测评是否提供接口，可控第三方审计。

3、测评云服务方对云租户系统数据的操作是否可被云租户审计。

剩余信息保护测评内容

测评空间回收时是否完全清除。

入侵防范测评内容

1、测评资源隔离与异常访问。

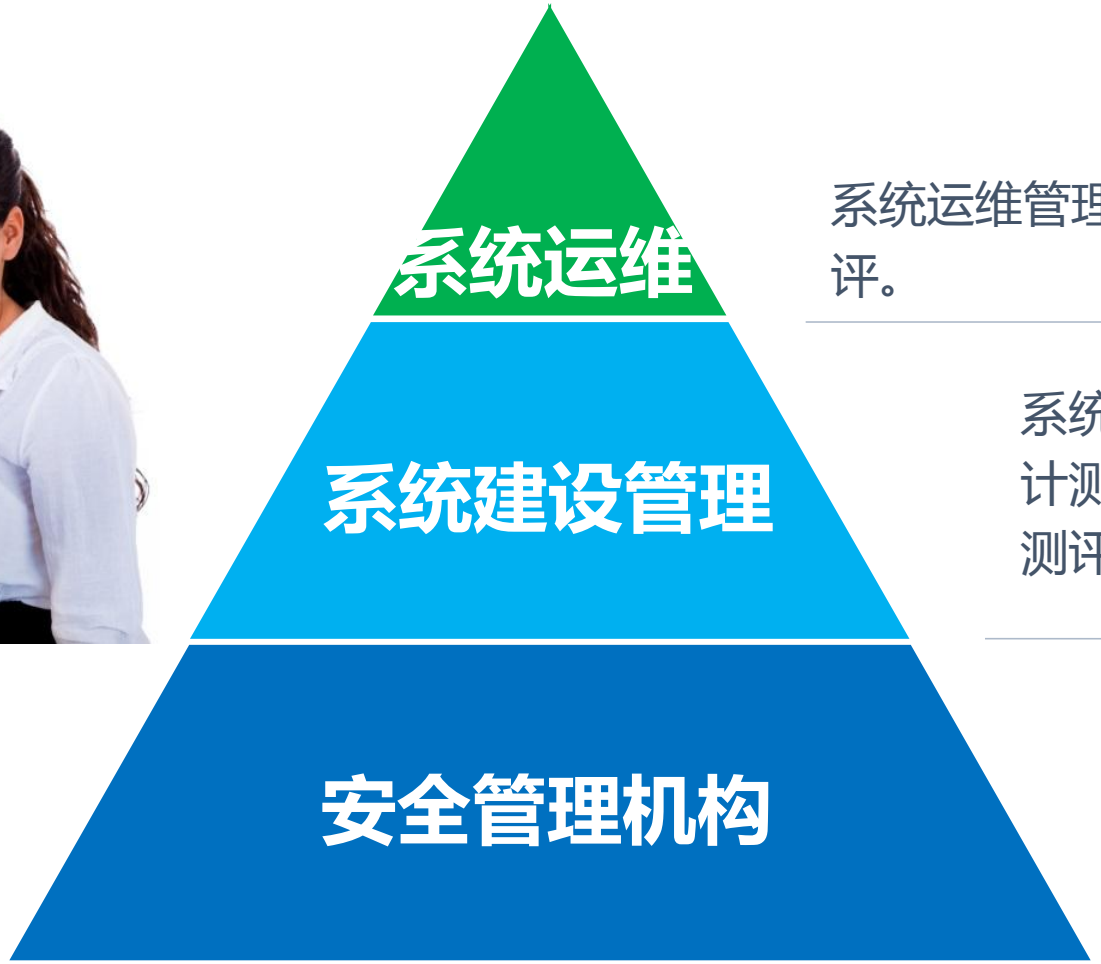
2、测评非授权新建或重启虚拟机。

3、测评虚拟机是否迁移至相同等级资源池。

恶意代码防范测评内容

测评恶意代码感染防范措施和虚拟机间蔓延防范措施。

云安全等级保护管理测评内容



系统运维管理测评部分包括监控和审计管理测评。

系统建设管理测评部分包括安全方案设计测评、测试验收测评、云服务商选择测评、供应链管理测评。

安全管理机构测评部分包括授权和审批测评。

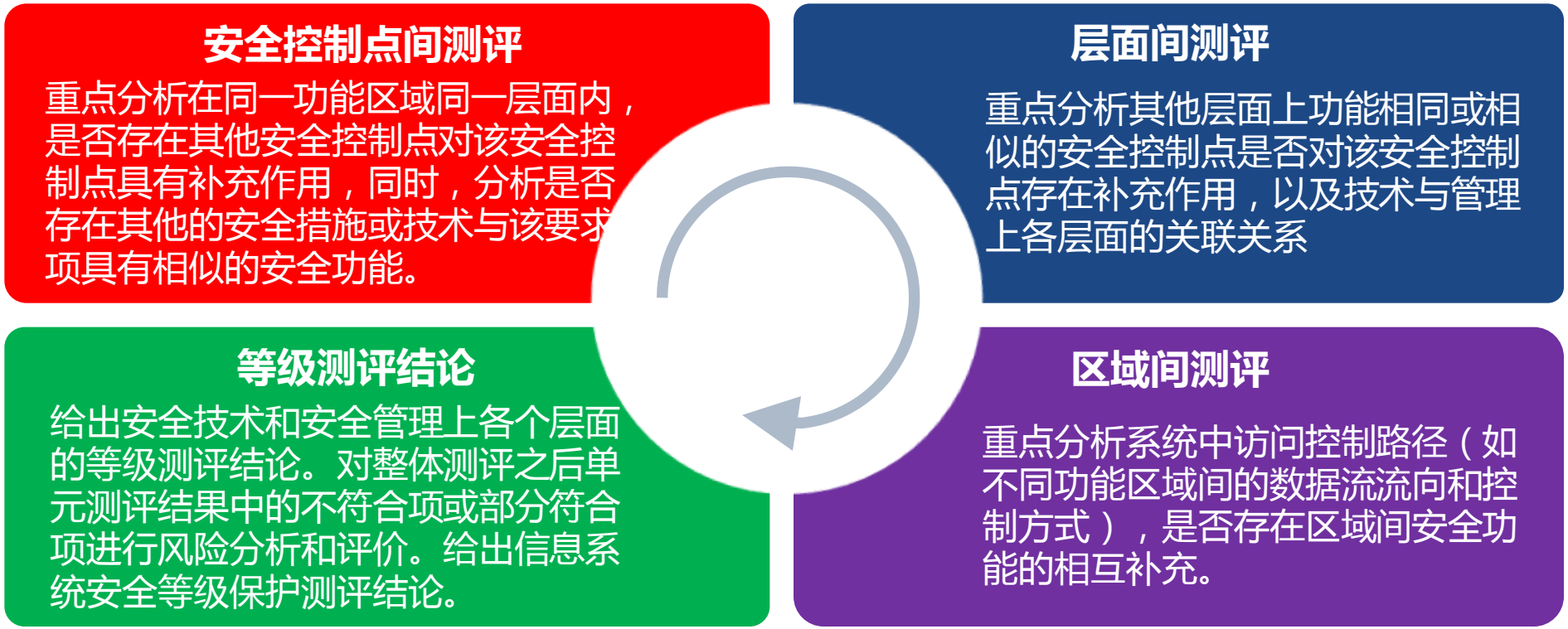
云安全等级保护单元测评

与传统信息系统相比新增保护对象

层面		云计算信息系统保护对象	传统信息系统保护对象
技术	物理安全	物理设备	机房及基础设施
	网络安全	传统网络设备、安全设备、网络结构、**虚拟化网络设备**	网络设备、安全设备、网络结构
	主机安全	传统主机、**宿主机、虚拟机、Hypervisor、云管理平台**	传统主机
	应用安全	业务应用系统	业务系统
	数据安全	管理数据**（包含虚拟机镜像文件）**、业务数据**（包括用户隐私）**、用户鉴别信息	管理数据、业务数据、用户鉴别信息
管理	安全管理机构	安全管理负责人、管理文档	安全管理负责人、管理文档
	系统建设管理	系统建设负责人、相关管理文档、服务合同、安全责任合同书或保密协议、**安全风险评估报告和风险预案。**	系统建设负责人、相关管理文档、服务合同、、安全责任合同书或保密协议
	系统运维管理	系统运维负责人、相关管理文档、**审计数据**	系统运维负责人、相关管理文档

云安全等级保护整体测评

整体测评主要分为安全控制点间测评、层面间测评、区域间测评三部分，最后得出等级测评结论。



云安全等级保护条款示例

3、测评对象

系统管理员,关键服务器、宿主机及虚拟机，关键数据库系统，云平台。

2、测评方法

访谈，检查，测试。

1、测评指标

见《云计算安全基本要求》 a)应根据云服务方和云租户的责任划分，收集各自控制的部分的审计数据；b) 应保证云服务方对云租户系统和数据的操作可被云租户审计；c) 应保证审计数据的真实性和完整性。

4、测评实施

a)应访谈系统管理员，是否采取措施划分云服务方和云租户的责任，收集各自控制的部分的审计数据；

b)应检查关键服务器、宿主机及虚拟机，关键数据库系统和云平台的安全审计策略，查看安全审计配置是否对云服务方和云租户的职责进行划分，收集各自控制的部分的审计数据；

c)应检查关键服务器、宿主机及虚拟机，关键数据库系统和云平台的安全审计策略，查看安全审计配置是否能够保证云服务方对云租户系统和数据的操作可被云租户审计；

d)应检查关键服务器、宿主机及虚拟机，关键数据库系统和云平台的安全审计策略，查看是否通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，是否实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等，查看是否采取措施能够保证审计数据的真实性和完整性。

5、结果判定

均为肯定，则信息系统符合本单元测评项要求。

研究成果

- ✓《云计算实际应用环境调研报告》
- ✓《云计算环境威胁与风险分析》
- ✓《云计算环境安全检查与评估指标体系》（中央网信办）
- ✓ 信息系统安全等级保护云计算相关标准（公安部）
- ✓《云计算环境安全评测业务管理体系》
- ✓《云计算环境安全评测业务服务流程体系》
- ✓《云计算环境安全评测工具整理》

研究成果

汇报提纲

近期信息安全热点事件分析

云等级保护能够提升云安全能力

“互联网+”时代的企业安全何去何从

终端安全 网络安全 应用安全

访问控制

实名注册
可信人员

安全协议
国密标准
杜绝攻击

安全通信协议

终端加密

本地加密
高强算法

云端加密

数据加密

APP防护

安全分级
远程擦除

身份证书
数字签名
密钥管理

权威CA系统

安全防护技术的思考

企业应该关注安全事件发展

➢01 可用性安全事件

指的是服务器无法正常访问或使用，危害在线业务的可用性。

DDoS攻击（包括流量攻击和应用攻击）会造成可用性安全事件。

➢02 应用安全事件

指的是服务器的数据或业务内容被盗取，业务信息、用户信息的安全无法得到保障。

网站存在漏洞，被黑客恶意利用，会造成业务安全事件。

DDoS攻击

DDoS攻击中文全称为分布式拒绝服务，是一种网络攻击手法，借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，其目的在于使目标服务器的带宽或计算资源耗尽，使服务暂时中断或停止，导致其对目标客户不可用。

01

流量攻击

流量攻击耗费的是服务器的带宽资源

这种攻击消耗网络带宽或使用大量数据包淹没一个或多个路由器、服务器和防火墙。流量攻击的普遍形式是大量看似合法的数据包被传送到特定目的地。为了使检测更加困难，这种攻击也常常使用源地址欺骗，并不停地变化。

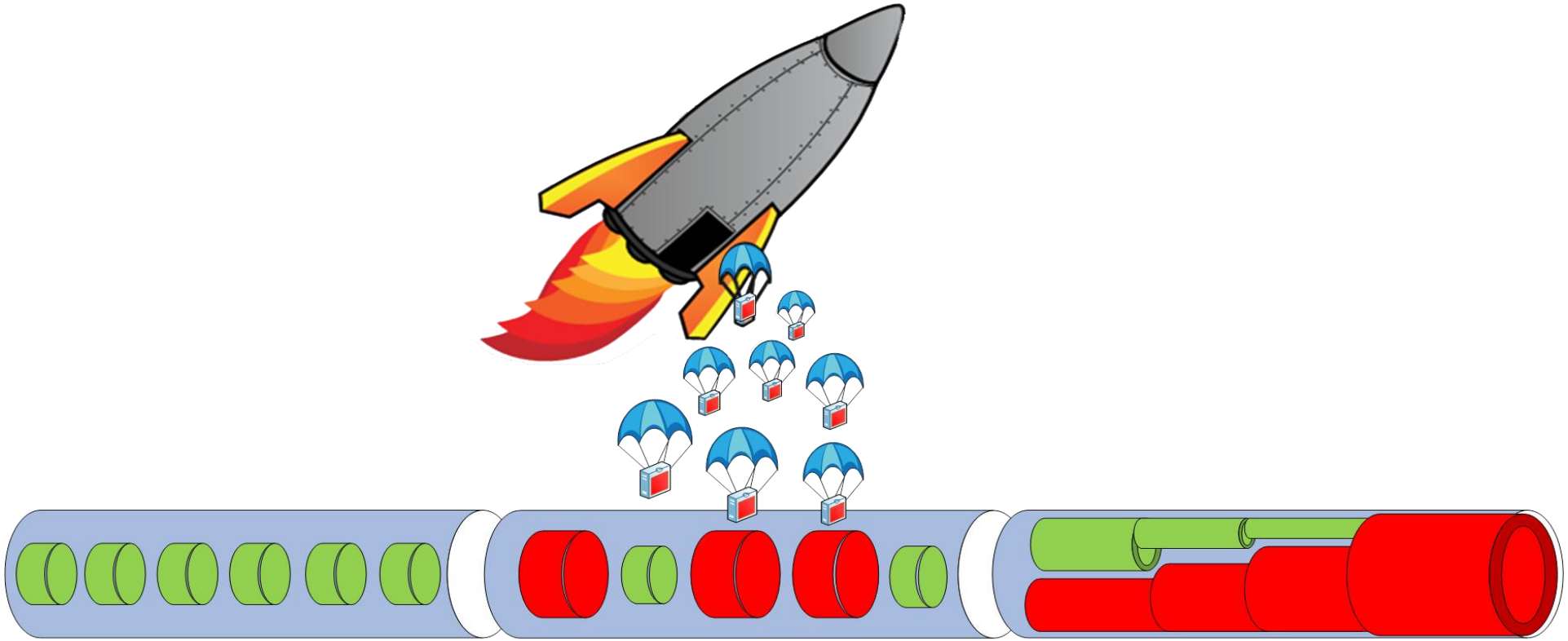
02

应用攻击

应用攻击消耗的是服务器的计算资源

利用TCP和HTTP等协议漏洞的行为来不断发送请求，占用服务器计算资源以阻止它们处理正常事务和请求。这种攻击从表面上看并不会有大的流量波动，但是用户会发现服务器的功能无法正常使用。

DDoS示意图



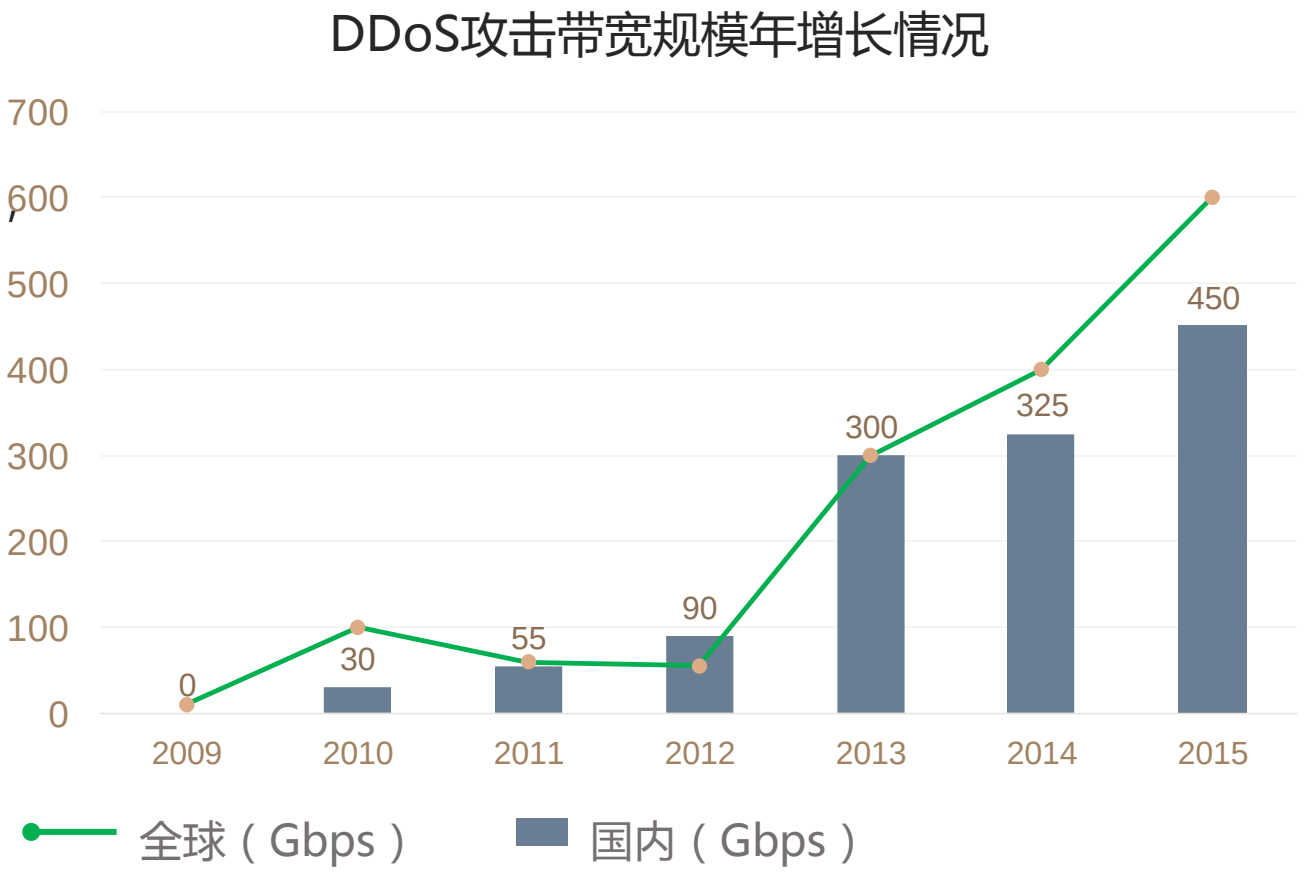
正常访问数据　　遭遇DDoS攻击带宽被侵占　　带宽被消耗殆尽

DDoS的发展

2013年起，反射攻击成为黑客攻击热门方式。经过DNS开放服务器反射将攻击流量轻松放大100倍，攻击规模越来越大。

2015年每个季度DDoS攻击发生频率比去年同期平均增长了超80%，每次DDoS攻击的持续时间接近21个小时，比去年同期提升了19%。

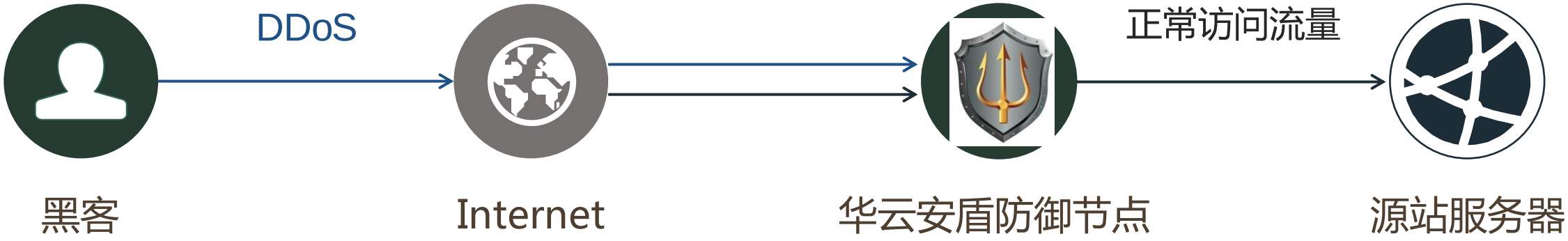
2016年的100G+超大规模流量攻击明显增多。华云安盾云安全在7月防御攻击流量最高峰值达到750Gbps。



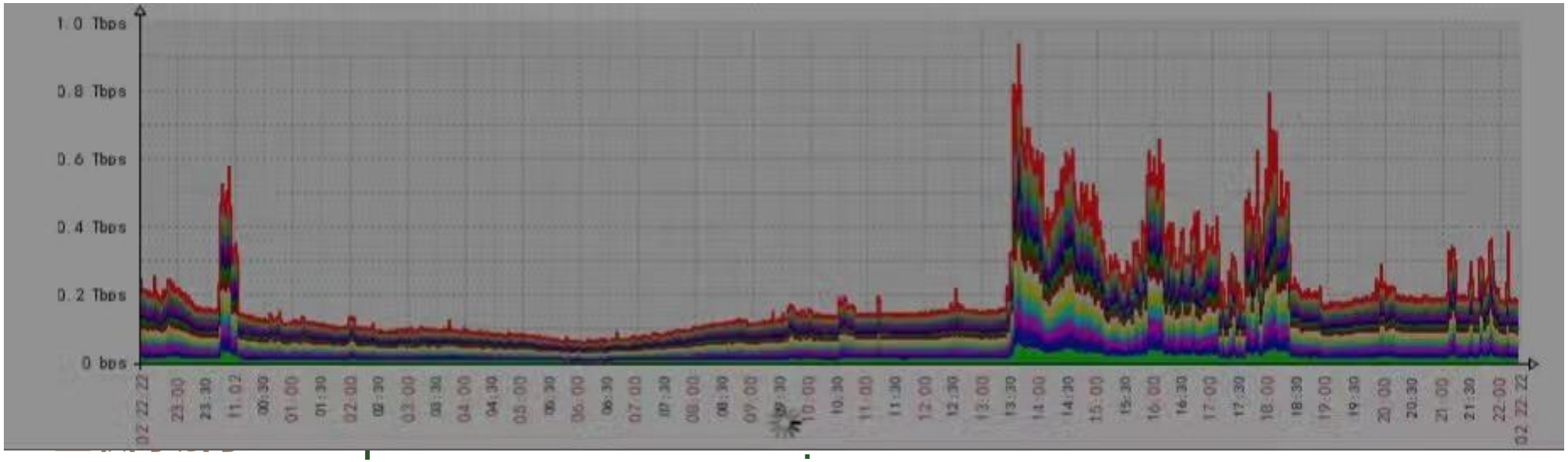
抗Ddos防御原理

DDoS如何防御？

华云安盾采用DNS解析的方式，使用户请求先经过华云安盾的防御节点，防御节点对于请求进行识别和过滤，正常访问流量牵引至源站服务器，恶意请求则清洗掉，从而实现DDoS防御。



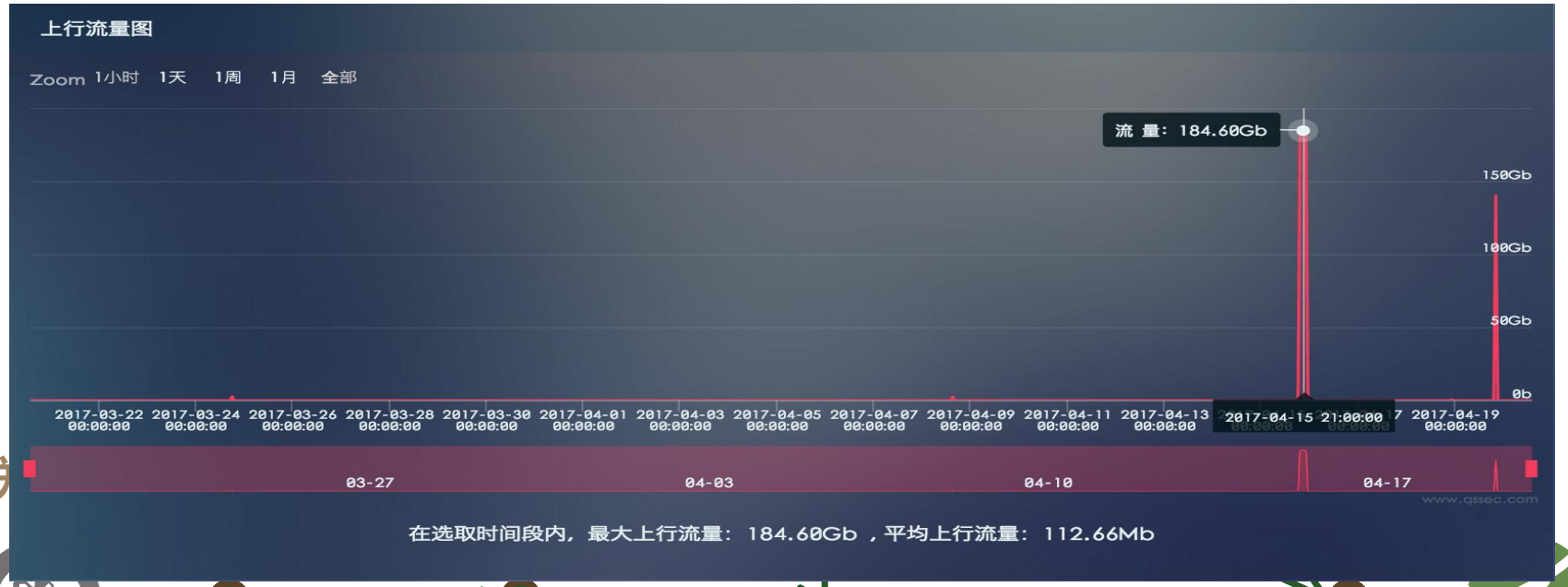
公有云抗DDoS业务

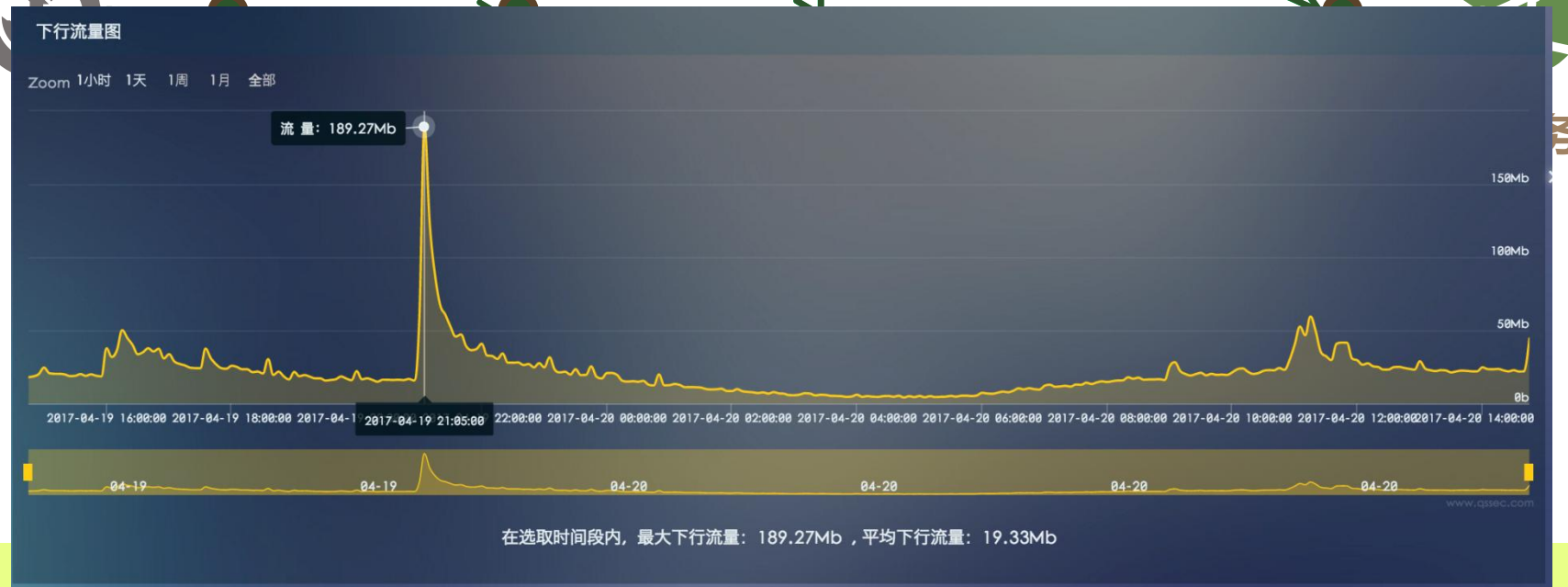


用
也

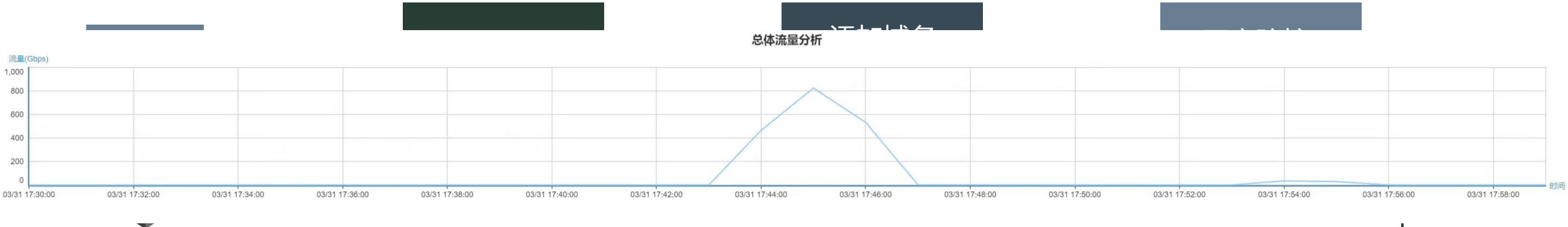
WAF（Web Application Firewall）应用

混合云安全防御机制


上行流量图
Zoom 1小时 1天 1周 1月 全部
流 量：184.60Gb
150Gb
100Gb
50Gb
0b
2017-03-22 00:00:00
2017-03-24 00:00:00
2017-03-26 00:00:00
2017-03-28 00:00:00
2017-03-30 00:00:00
2017-04-01 00:00:00
2017-04-03 00:00:00
2017-04-05 00:00:00
2017-04-07 00:00:00
2017-04-09 00:00:00
2017-04-11 00:00:00
2017-04-13 00:00:00
2017-04-15 21:00:00
2017-04-19 00:00:00
03-27
04-03
04-10
04-17
www.qssec.com
在选取时间段内，最大上行流量：184.60Gb ，平均上行流量：112.66Mb


下行流量图
Zoom 1小时 1天 1周 1月 全部
流 量：189.27Mb
150Mb
100Mb
50Mb
0b
2017-04-19 16:00:00
2017-04-19 18:00:00
2017-04-19 21:05:00
2017-04-20 00:00:00
2017-04-20 02:00:00
2017-04-20 04:00:00
2017-04-20 06:00:00
2017-04-20 08:00:00
2017-04-20 10:00:00
2017-04-20 12:00:00
2017-04-20 14:00:00
04-19
04-19
04-20
04-20
04-20
04-20
www.qssec.com
在选取时间段内，最大下行流量：189.27Mb ，平均下行流量：19.33Mb

防御开启



End

清洗攻击

DNS解析

修改域名DNS解析
指向华云安盾CNAME

我们需要的生活：简单、快乐、安全、便捷

娱乐

午餐

工作

清晨

谢谢

赵睿斌　博士
国家信息中心
zhrbdove@cei.gov.cn
15810196015