国家信息中心
State Information Center

国家电子政务外网管理中心
National E-Gov Network Administration Center

政务云安全技术要求及态势感知建设

邵国安

2017年6月13日

地址：北京市西城区三里河路58号　邮编：100045　电话：010-68527618 68557203　传真：010-68533919

习近平《在网络安全和信息化工作座谈会上的讲话》（2016年4月19日）

- 树立正确的网络安全观，**理念决定行动**
  - 网络安全是**整体**的而不是**割裂**的
  - 网络安全是**动态**的而不是**静态**的
  - 网络安全是**开放**的而不是**封闭**的
  - 网络安全是**相对**的而不是**绝对**的
  - 网络安全是**共同**的而不是**孤立**的

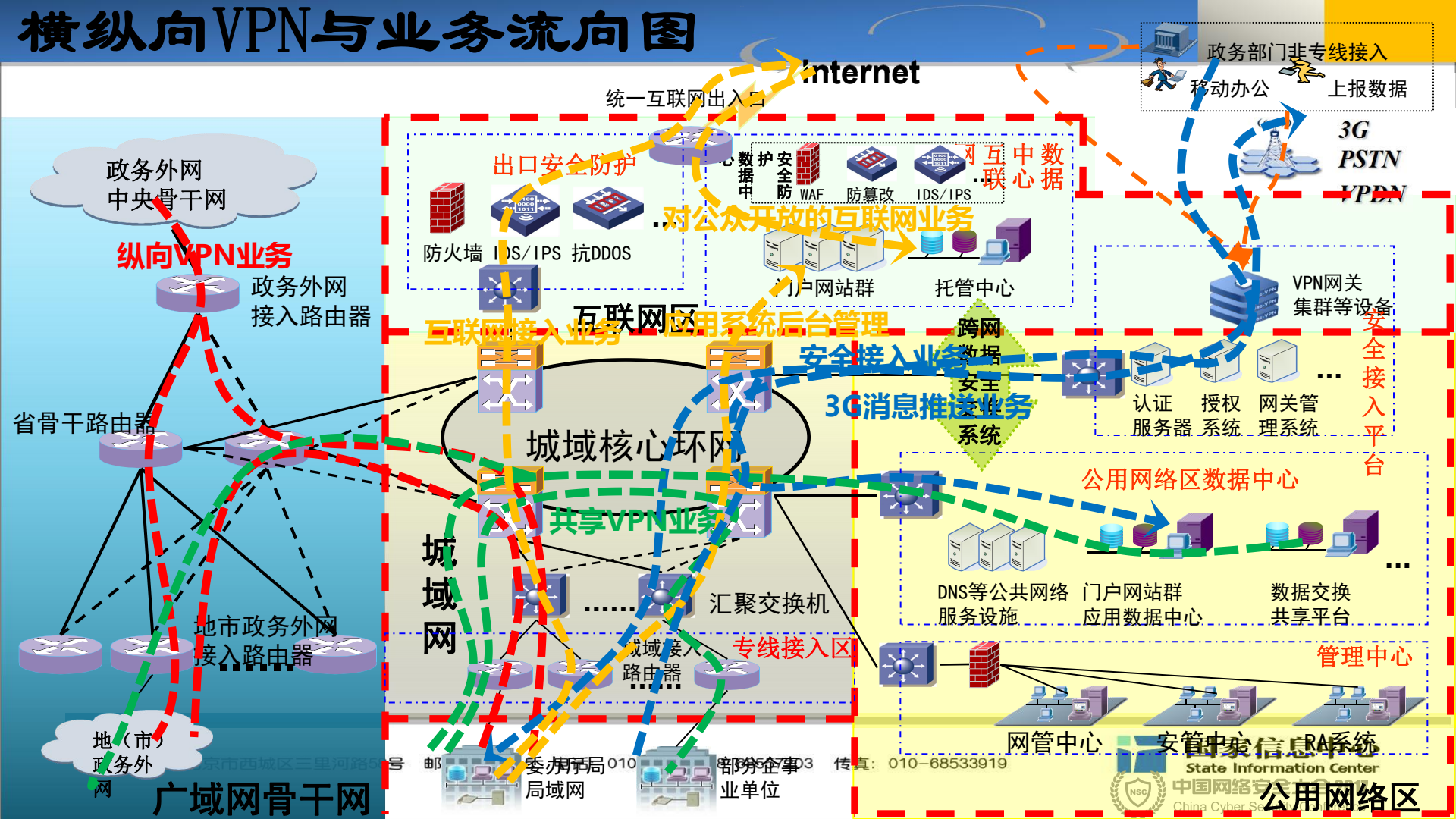
网络安全和信息化是相辅相成的。安全是发展的**前提**，发展是安全的**保障**，安全和发展要同步推进。

- **全天侯全方位**感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险
- 网络安全的本质在**对抗**，对抗的本质在攻防两端**能力**较量
- 大国网络安全**博弈**，不单是**技术**博弈，还是**理念**博弈、**话语权**博弈

政务外网现状（截至2016年12月）

- 在纵向覆盖方面，政务外网省、地市和区县三级覆盖率分别达到100%、97.3%和90%，已有24个省（区、市）和新疆生产建设兵团实现县级及乡镇的专线全覆盖
- 在横向接入方面，政务外网已连接了130个中央政务部门和相关单位，其中37个为业务应用发起部门，79个为业务应用参与部门。省以下接入政务部门数达24.4万个，接入终端超过280万台
- 据不完全统计，各地基于政务外网部署的行政审批、电子监察、应急平台、社会保障、文化共享、卫生医疗等业务应用系统总计超过5000项
- **全球最大的政务专网**
- 50%以上的省级政务外网实现的统一的互联网出口并集中管理

横纵向VPN与业务流向图



政务外网统一安全策略

- “2+N”业务逻辑划分：公共网络区、互联网区和N个专用网络区
- 统一的IP地址：国家、省、市、县广域网骨干网设备地址、共享服务器地址使用统一规划的地址
- 全网骨干网按等级保护第三级进行保护
- **统一的安全监测**：全网实现国家 、省二级或国家、省、地（市）三级安管系统互联，实现全网的安全事件监测与快速响应
- **统一的网络信任体系**：身份认证、授权管理、责任认定
- 可信的接入与互联：专线接入、网关+认证统一接入
- **逐步减少各级政务部门的互联网出口**，通过政务外网的互联网VPN统一出口，设立安全分析中心，统一管理、统一监控、统一分析与预警和应急处置和安全信息共享，（如IP地址库、全球黑名单库、案例库、知识库、事件库等）
- 跨区域（公共区与互联网区）的安全数据交换
- 局域网内的用户终端跨区域的安全访问

国家电子政务外网安全战略目标

- 设立国家政务外网安全信息共享与分析中心（eGov-ISAC)
  - 以国家、省级、地市级政务外网统一互联网出口的网际监控为抓手
  - 统一规范、统一管理、统一监控、统一分析与预警
  - 安全信息共享（如IP地址库、全球黑名单库、案例库、知识库、事件库等）
  - 安全监测、漏洞修复、威胁溯源、应急响应、态势感知和分析报告
  - 建立与国家信息安全主管部门（网信办、公安、安全、保密、军队）的信息安全通报、处置与联动机制
  - 建立与高校、研究机构、安全厂商、其他关键基础设施单位及第三方机构等信息安全安全共享、通报、处置与联动机制及情报共享平台
  - 制定相关信息安全共享、DNS部署指南、安全事件评估等相关标准、
  - 为国家的各关键行业建立信息共享与数据分析中心并形成国家的力量
- 建立我们国家新技术和攻防研发的平台和情报共享平台
- 成为国家重要的专业的信息安全支撑队伍

在政务信息化建设中的要求

- 边界安全
  - 与互联网的连接（ISP)、与移动运营商的VPDN连接、各局域网出口与政务外网的连接及其他专线的边界
  - 基于行为、攻击攻击、特征匹配、DNS监控、NAT及域名监控
- 网络安全
  - 各类安全防护设备的日志、安全策略及实时监测、网络流量的监测、网络行为审计
- 终端安全
  - 对各类终端的管理：操作系统、各类应用客户端、病毒补丁管理、DNS管理及访问控制
- 应用安全
  - 应用系统原代码管理、网络信任体系（身份认证、授权管理和责任认定）及系统补丁管理
- 数据安全
  - 数据加密、数据库审计，作为资产进行管理

安全运维应作为一个常态的服务

“常态甄别和缓解”（网络安全威胁）计划
CDM : Continuous Diagnostics and Mitigation

旨在提供工具和服务，使各级政府和机构得以加强网络安全，改善网络安全态势。

被称为---常态监控即是服务
(简称：CMaaS)
Continuous Monitoring as a Service

来源：国土安全部US-CERT
https://www.us-cert.gov/cdm

国家电子政务外网安全监测报告
安全事件分级分类（共八类）

类别	一级分类	二级分类
0	授权训练、演习、调查	授权的渗透测试、漏洞扫描、安全检查等
1	成功入侵	木马入侵、病毒入侵、后门入侵、 漏洞入侵、猜口令成功、网络攻击等
2	不成功的入侵行为企图	猜口令、SQL注入尝试等
3	拒绝服务攻击	短包、流量、DNS放大攻击等
4	违规行为	非法外联、安全策略不正确、误操作等人为事件
5	嗅探踩点	非授权漏洞扫描、常用服务探测等
6	可识别的异常	跨境数据传输、软件后门（尚未受控）、系统漏洞、不当使用、 信息破坏、设备设施故障、灾害性事件等
7	其他未知异常	0day、通过行为分析的各类异常情况

国家标准 政务云 标准

政务云安全要求

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919

《政务云安全要求》编写原则

- 在遵循国家标准的基础上，尤其是已发布的《信息安全技术 云计算服务安全指南》（GB/T 31167-2014)和《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014)标准
- 参照公安部正在组织制定的《第2部分 网络安全等级保护基本要求 云计算安全扩展要求（征求意见稿）》（GB/T 22239.2)
- 参照国际标准及美国NIST的相关标准
- 政务云安全要求，定位在各级政务部门使用云计算开展电子政务过程中，应遵循的安全要求
- 目标：结合电子政务外网，针对政务部门特殊的安全要求，具备可操作性、针对性强、提出本标准

定义

- **政务云：**用于承载各级**政务部门**开展公共服务、社会管理的业务信息系统和数据,并满足跨部门业务协同、数据共享与交换等的需要，提供IaaS、PaaS和SaaS服务的云计算服务。
- **电子政务：**是政府通过信息通信技术手段的密集性和战略性应用组织公共管理的方式，旨在提高效率、增强政府的透明度、改善财政约束、改进公共政策的质量和决策的科学性，属于政务部门社会管理、公众服务，业务协同的**内部**信息化过程，并开放相关数据
- **政务外网：**是政务部门信息化、办公协同、数据共享的需要，属于内部专网，其**专线**接入应该只限于政务部门

企业面临12大云计算安全威胁（2016年）

- 根据CSA（云安全联盟）列出
  - 数据泄露
  - 凭据或身份验证遭到攻击或破坏
  - 接口和API被黑客攻击
  - 利用系统漏洞
  - 账户被劫持
  - 来自企业内部的恶意人员
  - APT寄生虫
  - 永久性的数据丢失
  - 缺乏尽职调查
  - 云服务的滥用
  - DDOS攻击
  - 共享的危险

云计算参考架构

服务层

- 软件即服务SaaS
- 平台即服务PaaS
- 数据存储即服务DaaS
- 基础设施即服务IaaS

云运营中心

- 服务目录管理
- 服务水平管理
- 服务流程管理

服务管理

- 客户项目管理
- 生命周期管理
- 计费账单管理

业务管理

云基础架构平台

云中间件

- 企业数据总线
- 应用服务器
- 关系数据库
- NoSQL DB
- 分布式计算

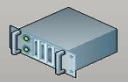
云操作系统

- 资源调度
- 存储管理
- 网络管理
- 系统管理
- 用户管理

资源池化

逻辑资源池
(计算资源、存储资源、网络资源)

物理设备

云安全中心

- 身份安全
- 网络安全
- 数据安全
- 内容安全
- 安全管理

数据中心
基础设施

CloudBase
模块化数据中心

CloudBase
集装箱数据中心

物理防火墙

集群管理

业务应用1

业务应用2

VM VM VM VM

VM VM VM VM

Hypervisor-KVM

Hypervisor-KVM

linux

linux

身份认证系统

主机监控审计

杀毒软件

远程管控

虚拟化层监控审计

三权分立

虚拟化入侵检测、入侵防御

虚拟防火墙

操作系统加固系统

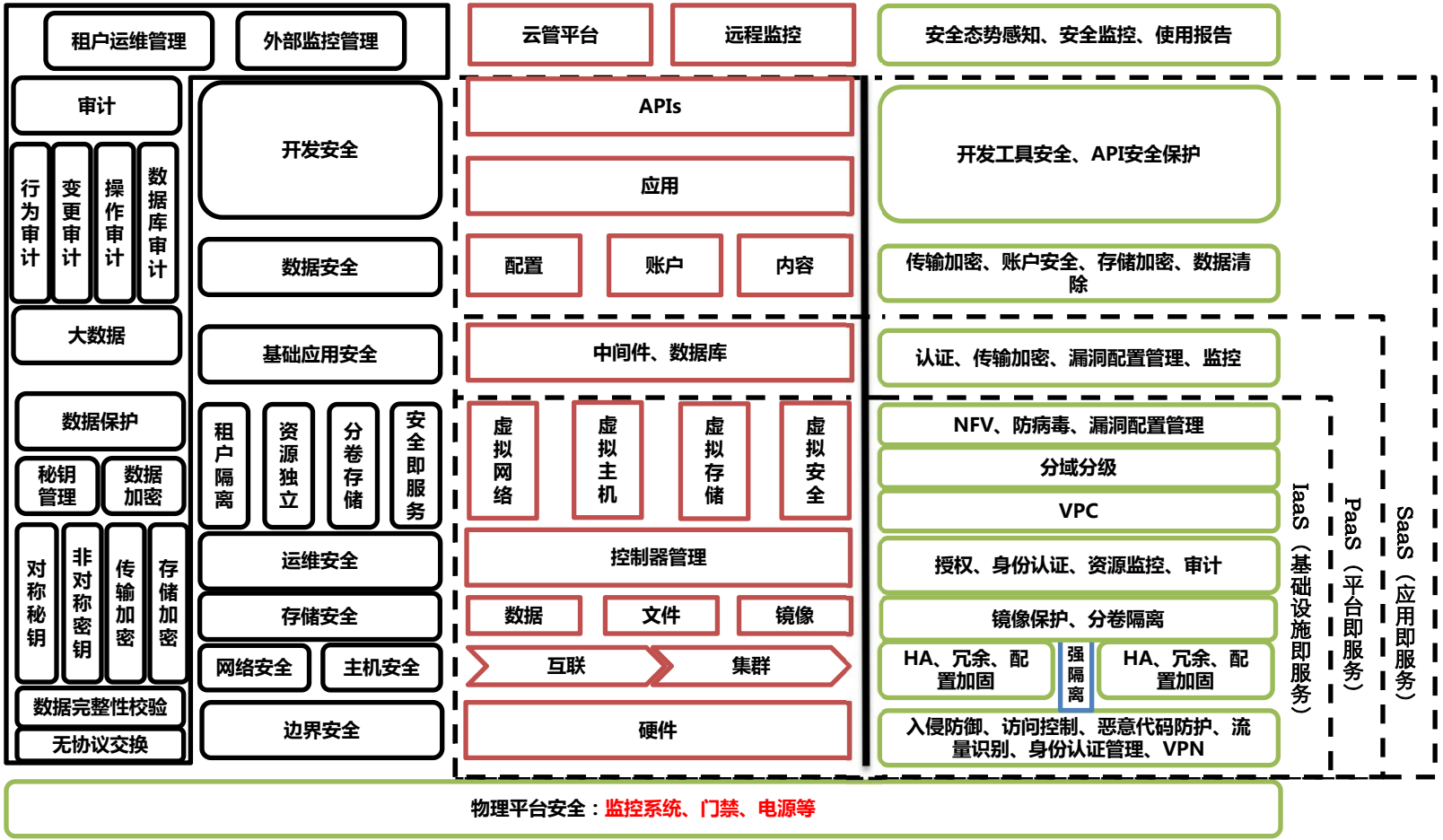
安全云管理平台

独立产品

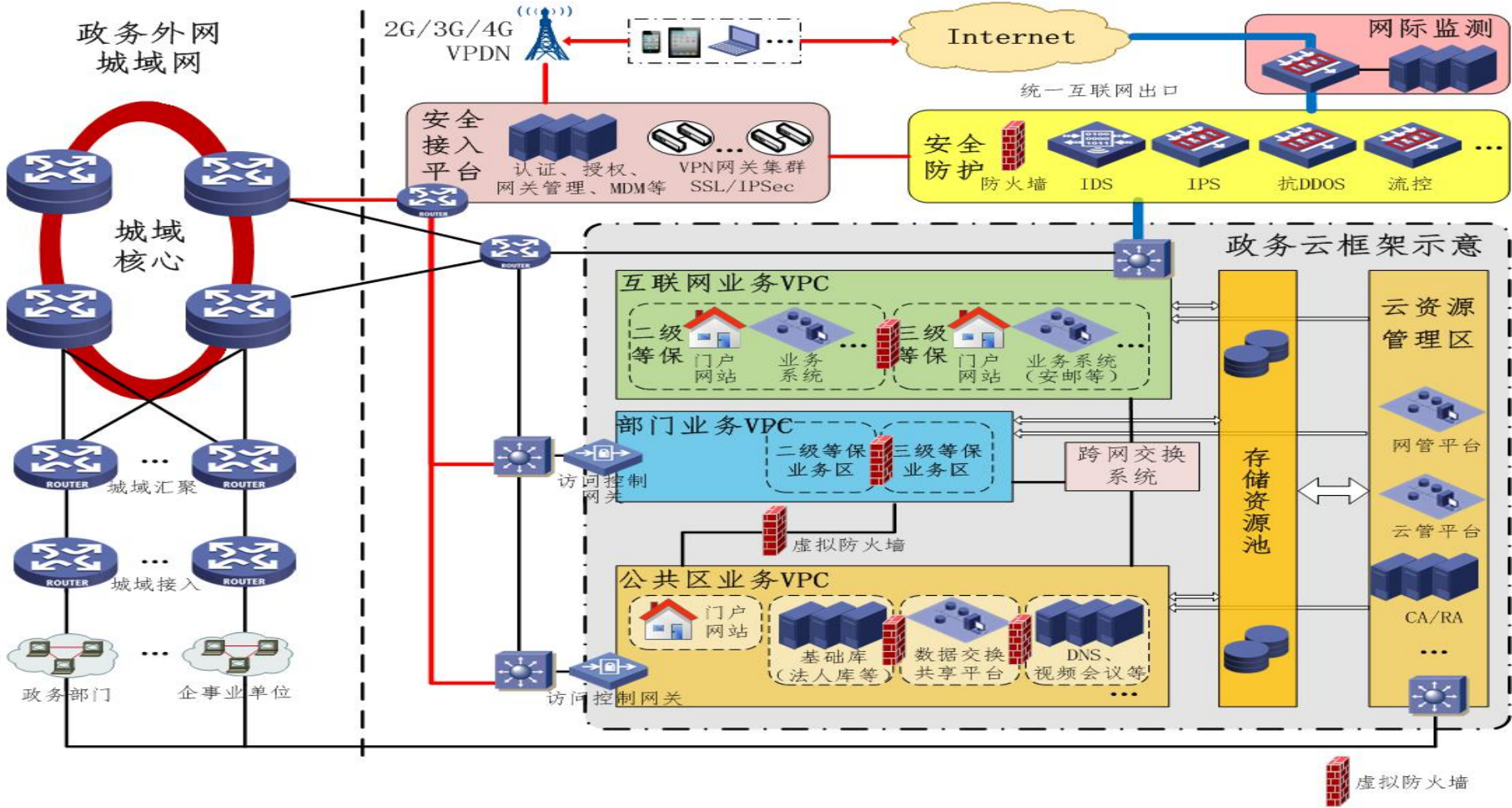
安全NAS

地址：北京市 ：010-68527618 68557203 传真：010-68533919

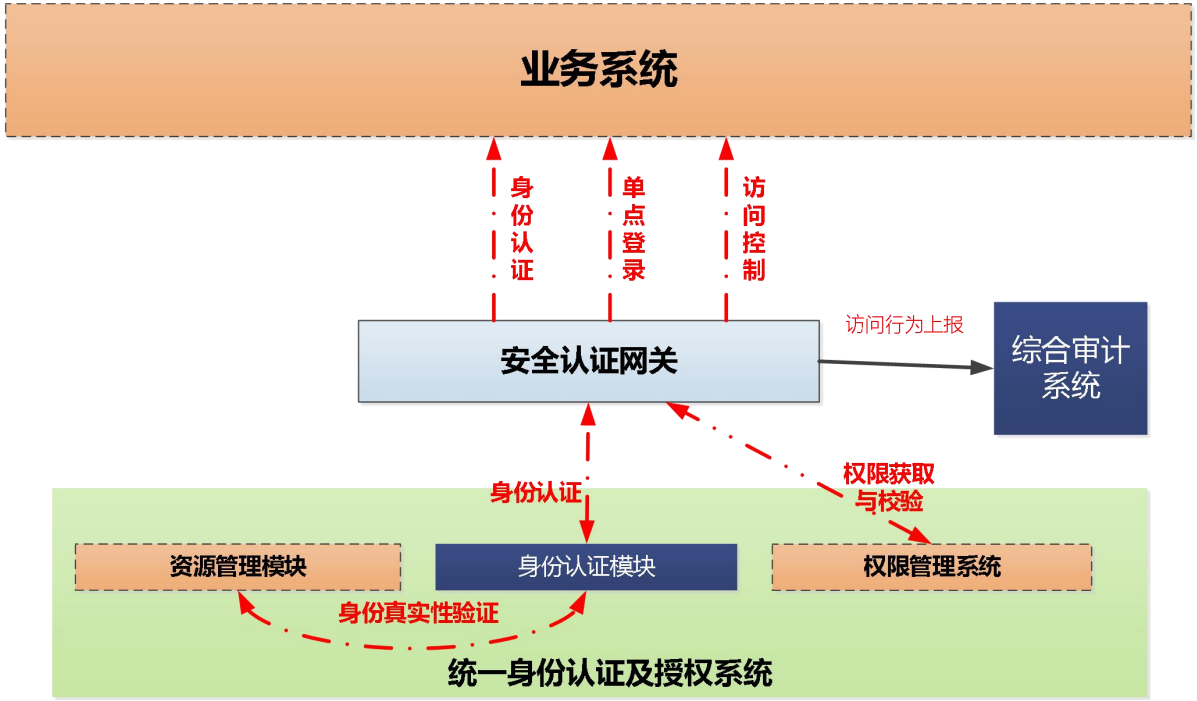
政务云安全框架图


租户运维管理
外部监控管理
审计
行为审计
变更审计
操作审计
数据库审计
大数据
数据保护
秘钥管理
数据加密
对称秘钥
非对称密钥
传输加密
存储加密
数据完整性校验
无协议交换
开发安全
数据安全
基础应用安全
租户隔离
资源独立
分卷存储
安全即服务
运维安全
存储安全
网络安全
主机安全
边界安全
云管平台
远程监控
APIs
应用
配置
账户
内容
中间件、数据库
虚拟网络
虚拟主机
虚拟存储
虚拟安全
控制器管理
数据
文件
镜像
互联
集群
硬件
安全态势感知、安全监控、使用报告
开发工具安全、API安全保护
传输加密、账户安全、存储加密、数据清除
认证、传输加密、漏洞配置管理、监控
NFV、防病毒、漏洞配置管理
分域分级
VPC
授权、身份认证、资源监控、审计
镜像保护、分卷隔离
HA、冗余、配置加固
强隔离
HA、冗余、配置加固
入侵防御、访问控制、恶意代码防护、流量识别、身份认证管理、VPN
IaaS（基础设施即服务）
PaaS（平台即服务）
SaaS（应用即服务）
物理平台安全：监控系统、门禁、电源等

政务云与政务外网、互联网的关系及要求



统一认证及授权管理



网络信任体系要求：

1、基于PKI的数据证书对身份地验证。

2、所有信息系统定级为三级，其访问系统均应通过数字证书

3、通过访问控制网关，访问信息系统时应基于身份、角色的访问控制并审计。

4、实现终端统一管理，当插入证书时，应立即断开互联网连接，并对相关文档加密存入本地硬盘。

5、责任认定，对访问人的行为、内容等进行审计。

6、支持云计算环境的瘦客户端模式或BYOD方式。

数据保护

- **镜像、副本、快照**—与应用系统读取数据实时、同步，防止存储块故障导致**数据损坏，**保证业务连续性。
- **备份**
  - RPO--灾难发生后，系统和数据必须恢复到的**时间点**要求
  - RTO--灾难发生后，信息系统或业务功能从停顿到必须**恢复的时间**要求
  - 同城系统备份—2个数据中心之间距离在50公里以内，信息系统能迅速恢复使用，如银行的二地3中心
  - 异地数据备份：与主用数据中心之间距离在500公里以外，一般只做数据同步
  - 数据备份策略：为了达到数据恢复和重建目标所确定的备份步骤和行为。通过确定备份时间、技术、介质和场外存放方式，以保证达到RPO 和RTO的要求

制定《政务云安全要求》（1）

- 政务业务应部署在**独立**的政务云上，**不得**部署在公有云上；
- 各级政务云基础设施应按其所承载的信息系统安全等级保护最高等级要求进行建设，一般情况下应**按第三级等级保护要求建设**和保护；
- 政务云上承载互联网门户网站及必须部署在互联网上信息系统的计算资源和网络资源从云计算核心层以下其计算和网络资源在物理上就应**分开部署**，根据系统预设的调度策略进行资源调度和迁移；
- 所有对云资源的操作必须通过云资源管理区，加强审计和控制；
- 云服务商应提供对各信息系统的核心或敏感数据进行**加密存储**的功能，应按照国家密码管理有关规定使用和管理政务云平台中所使用的密码设施，并按规定生成、使用和管理密钥；

制定《政务云安全要求》（2）

- 应对租户管理员**用户名密码**及政务云的管理数据单独加密存储，重点保护。其密钥的使用和管理应符合国家密码管理局的有关规定；
- 重要部门的信息系统在分地域部署云计算基础资源时，可将计算、网络和存储资源采用**分布式部署**方式部署在远端并进行统一管理；
- 要求业务流与管理流**分开**，应能区分运维管理人员、租户管理员、安全人员及公务人员访问业务和对各类资源的管理，并实施严格的访问控制策略；
- 明确**远程管理**责任，云服务商需要对计算资源进行远程管理时，应对所有远程维护和诊断活动进行审计，按照对所有远程维护和诊断会话的记录进行审查；

制定《政务云安全要求》（3）

- 云计算环境应具备基于行为的**实时检测**、策略控制、事件预警及安全事件及时处置的能力；
- 云服务商应**定期**向政务云管理单位提交各租户安全情况及资源使用率情况；
- 对**重点租户**的信息系统和数据应能重点进行安全保障，实时了解异常情况并预警；
- 政务云应具备**分级管理**和控制的能力，VPC内部信息系统之间的访问控制及数据使用等管理权限应开放给租户，云服务商应具备对资源使用情况实时监测、发现异常、预警和协助处置的能力

云计算建设过程中应关注的安全问题

- 自建自用（数据和物理位置、隐私/开放、边界化和自供/外包）
  - 在任何情况下，对信息系统和数据的可管理、可控制、可追溯
  - 在虚拟环境下做好信息系统的边界访问控制
  - 对云计算环境的综合管理系统和审计是关键
    - 对各类资源的实时调度时应有记录
    - 任何安全问题应实时告警
    - 对网络管理员、系统管理员、操作人员的行为审计
- 租用或托管时，作为信息系统和数据的拥有者
  - 对信息系统和数据的实时管理
  - 自主进行边界访问控制
  - 对数据的存储位置、使用情况和安全，应做到实时了解
  - 系统的运行报告、审计报告及应急措施等

云计算环境不同角色的安全需求

- 政务云管理部门
  - 负责政务云的安全监管、汇总租户的需求并核实
  - 对租户所使用的计算、网络和存储资源情况进行监督管理（如资源使用情况，TOP排名、明确使用、安全及管理责任）
  - 对云服务商提供的各类资源、远程运维等进行监督管理和审计
- 云服务客户（各政务部门）
  - 明确与云服务商的责任边界，属于租户责任的内部资源做到可管理、可追溯、可控制，要求云服务商开放相关API接口
  - 实时了解自身信息系统的使用情况、数据存储位置、使用及异常告警
  - 应实时了解操作系统、中间件和应用软件的漏洞情况及其他安全异常等
- 云服务提供方
  - 提供政务云边界安全及统一的安全接入平台服务
  - 提供政务云实时运行、各类资源使用和调度、政务云安全保障和开放第三方监控需要的API接口

政务云存在问题及思考

- 应用在集中、数据在集中，意味着风险也在集中
- 云计算环境的虚拟化引入，带来很多新的安全**挑战**，云管理部门、租户及云服务商之间的责、权、利及边界问题
- 安全**第三方监管**的引入，相关监管的接口规范
- 基于**对抗理念**下的主动安全防御、主动的漏洞扫描、全天候全方位的安全态势感知在云环境中如何实现？
- 云环境中**海量数据**下的管理及安全保障
- 多应用环境下的跨VPC**数据同步**问题及安全机制
- 基于**网络信任体系**下的应用保护尚未从理念上建立，今后的发展趋势？
- 政务云今后需要从**PaaS**和SaaS方向努力吗？如何模块化、结构化？

安全防御四大要素

- **威慑**：通过衡量并增加对手实施恶意网络空间活动的成本，降低收益，为潜在对手增加风险和不确定性，有效慑止恶意网络空间活动的能力。
- **防护**：组件、系统、用户和关键基础设施有效抵抗恶意网络空间活动并确保机密性、完整性、可用性和问责的能力。
- **检测**：有效检测甚至预测对手决策和活动的能力，因为绝对安全是不存在的，所以应假设系统无法抵抗恶意网络空间活动。
- **适应（弹性）**：防御者、防御和基础设施通过有效应对破坏，从破坏中恢复，在完全恢复的过程中持续操作以及适时调整以挫败未来类似活动，动态适应恶意网络空间活动的能力。

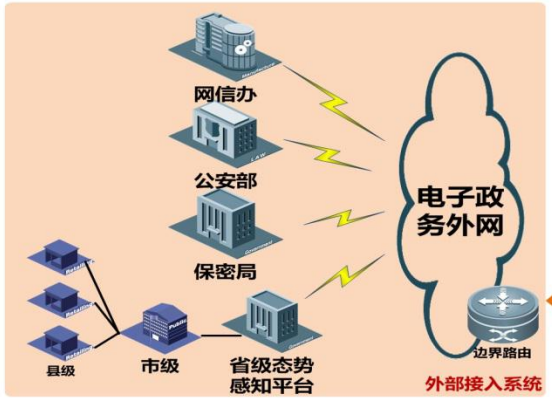
网络威慑

- **威慑**在某种意义上与洞察力相关。通过使潜在对手确信，如果它进行网络攻击，它将遭受无法承受的代价，以及通过降低潜在对手攻击成功的可能性，威慑才起作用。
  - **响应**：对危害国家安全的网络攻击立即做出响应
  - **拒止**：提高有效的防御能力，以保护国家关键基础设施免遭复杂攻击
  - **追查溯源**：情报和追查能力有助于揭露一个行为体的网络角色，确定攻击发起点、策略、技术和程序，确定攻击者的特征。
  - **弹性**：保护被攻击网络能继续运转，具备一定的弹性
- 主动检测、发现漏洞、缓解弱点、快速反应、信息共享

安全态势感知的建设

- 目标：**全天候天方位感知网络安全态势**
- 需求：实时发现网络异常、攻击目标，关联分析、迅速定位、及时预警处置并总结评估
- 态势感知三要素：有效数据获取、关联分析及图形化展示
- 建设要求：基于网络行为的实时的监测和控制
  - 应从网际监控、网络安全、终端管理、应用保障和数据安全五个维度
  - 注意不同监测系统的互补、交叉验证及特征库的及时更新
  - 全网事态的把握及情报共享
  - 在边界明确的情况下，实时做到网络行为的可控制、可管理和可追溯
  - 核心是保护应用系统和数据的安全
- 图形化展示要求：**领导能看懂决策、专业人员能处置及非专业人员也能懂**

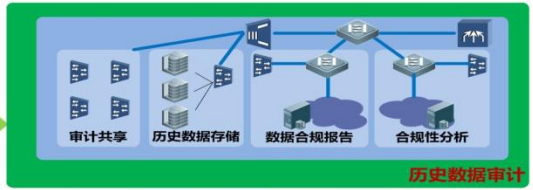
安全大数据综合分析与态势感知平台



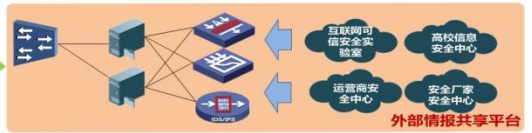
API

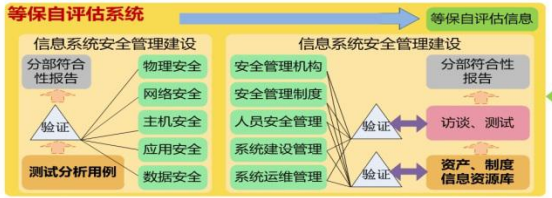
信息发布

数据接口



数据接口



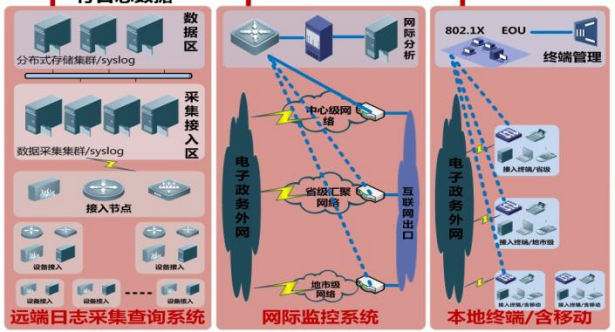


数据接口

远程设备运行日志数据

流量数据

状态策略数据



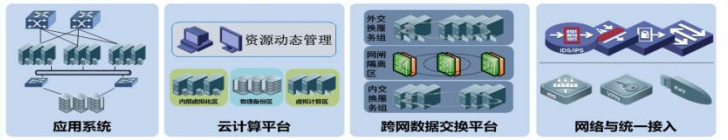
海量分类审计数据

符合性数据&反馈性数据

终端数据访问数据

网络安全实时状态数据

网络实时状态数据



Thank you 谢 謝

地址：北京市西城区三里河路58号　邮编：100045　电话：010-68527618 68557203　传真：010-68533919