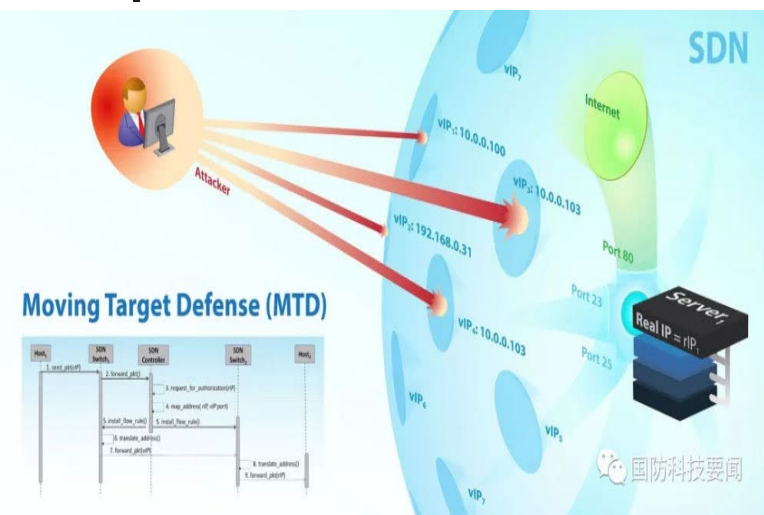




声 明

- 本PPT是电子工业出版社出版的教材《计算机网络安全原理》配套教学PPT（部分内容的深度和广度在教材的基础上有所扩展），作者：吴礼发
 - 本PPT可能直接或间接采用了网上资源、公开学术报告中的部分PPT页面、图片、文字，引用时我们力求在该PPT的备注栏或标题栏中注明出处，如果有疏漏之处，敬请谅解。同时对被引用资源或报告的作者表示诚挚的谢意！
 - 本PPT可免费使用、修改，使用时请保留此页。
-

第十五章 网络安全新技术





内容提纲

1

SDN安全

2

零信任安全

3

移动目标防御

4

网络空间拟态防御





问题分析

- 现有网络存在的问题：
 - 互联网流量急剧上升，对电信运营商提出了巨大挑战。为满足不断增长变化的用户需求，虚拟化与大数据等新型应用技术在网络服务器上进行越来越多的网络配置和数据传输等操作，**传统网络的层次结构和封闭的网络设备**已经不能够满足其日益增长的高可靠性、灵活性和扩展性方面的需求





软件定义网络

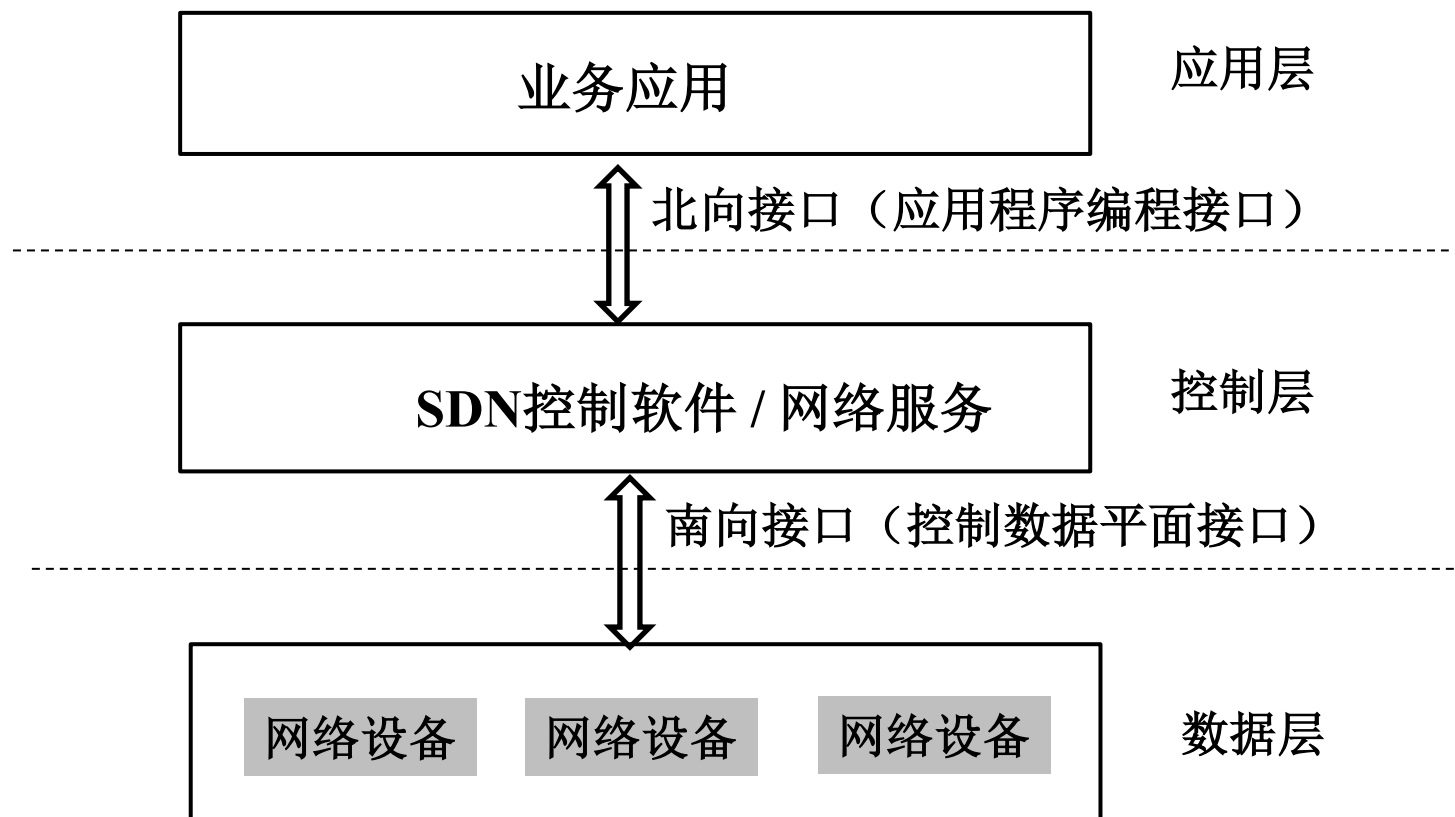
■ SDN的提出

- 斯坦福大学的Clean Slate研究组于2006年提出了“软件定义网络（Software-Defined Network, SDN）”这一新型网络创新架构
- 核心思想：将传统网络中的网络管理控制从网络数据转发层中分离出来，即将控制平面和数据平面分离，用集中统一的软件管理底层硬件，让网络交换设备成为单一的数据转发设备，控制则由逻辑上的集中控制器完成，实现网络管理控制的逻辑中心化和可编程化。

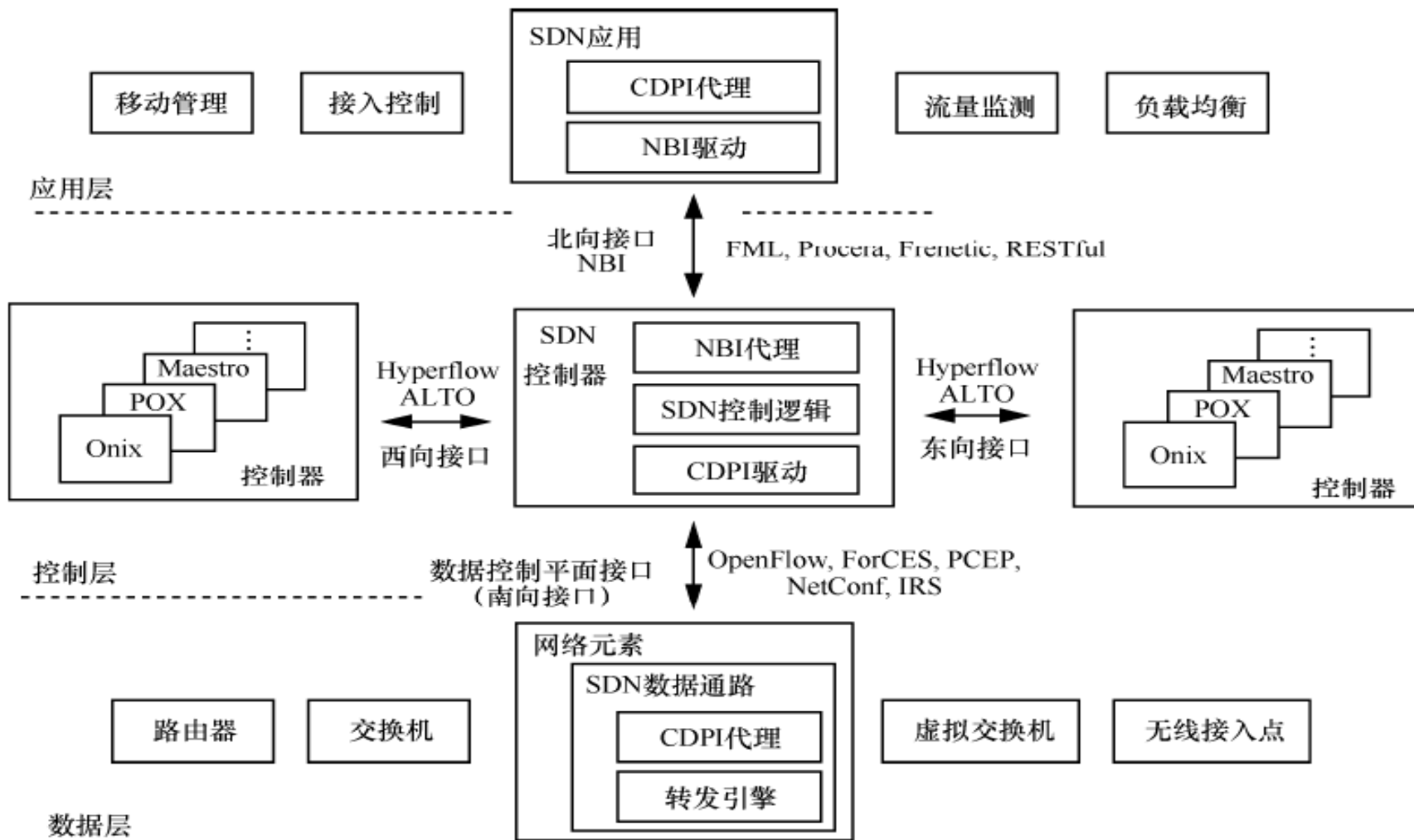


SDN体系结构

- SDN架构包含应用层、控制层和数据层三个层次



ONF SDN架构





NFV体系结构

虚拟网络功能（VNF）

虚拟网络功能1

虚拟网络功能2

...

虚拟网络功能n

NFV管理与编排

编排工具

NFV基础设施（NFVI）

虚拟计算

虚拟存储

虚拟网络

虚拟化层

计算硬件

存储硬件

网络硬件

虚拟网络
功能管理

虚拟基础
设施管理



OpenFlow

- OpenFlow作为ONF推出的SDN南向接口上控制器与数据层中的交换机之间的通信协议，已成为事实上的标准

协议版本	主要特点
OpenFlow 1.0	单表、IPv4
OpenFlow 1.1	多级流表、组表、MPLS、VLAN
OpenFlow 1.2	多控制器、IPv6
OpenFlow 1.3	Meter 表、版本协商能力
OpenFlow 1.4	流表同步、协议消息完善
OpenFlow 1.5	数据包类型识别流程（以太网数据包、PPP 数据包） egress Table



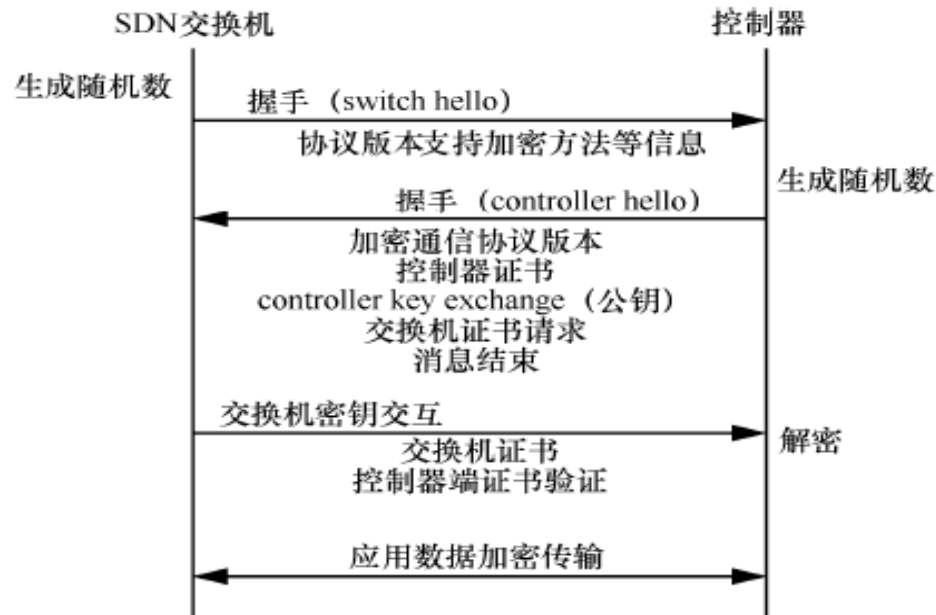
OpenFlow

- OpenFlow交换机进行数据转发的依据是流表（Flow Table）
 - 每个流表项都由3部分组成：用于数据包匹配的**包头域**（Header Fields），用于统计匹配数据包个数的**计数器**（Counters），用于展示匹配的数据包如何处理的操作（Actions）
 - 操作：必备：**转发**（forward）、**丢弃**（drop），可选：**排队**（enqueue）、**修改域**（modify field）



OpenFlow

- 控制器与交换机之间建立TLS连接的基本工作过程，OpenFlow 1.3 将TLS 设置为可选项，增加了SDN 的安全风险





SDN安全-应用层安全

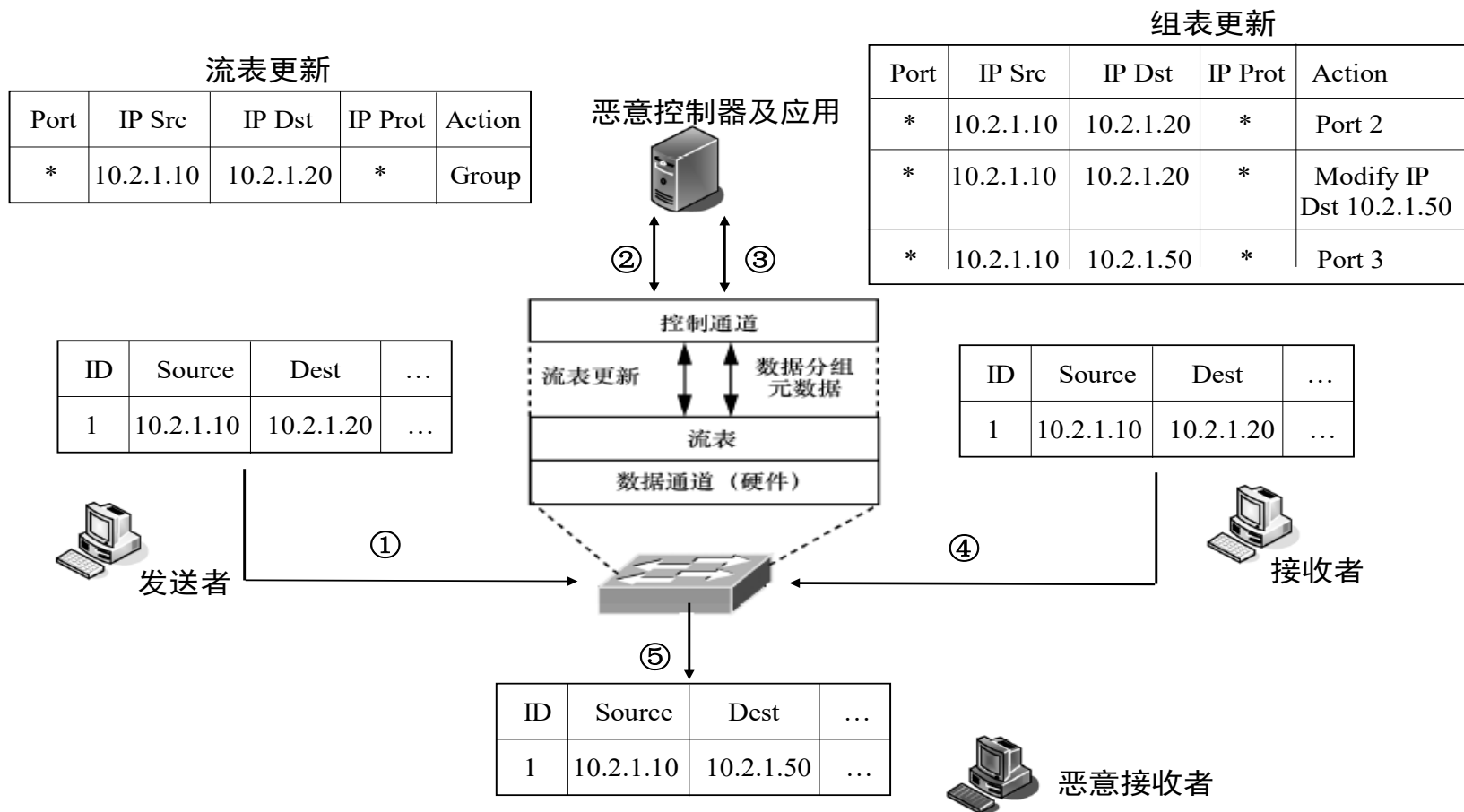
■ 应用层安全

- 威胁来自于两个方面：恶意应用造成的威胁，普通应用相互干扰或是运行出错等原因造成的威胁
- 包括：各类SDN 应用程序的恶意代码威胁；SDN 应用程序自身漏洞（BUG）及配置缺陷威胁；SDN 应用程序受到外部恶意攻击威胁；SDN 应用程序角色认证及访问权限威胁等



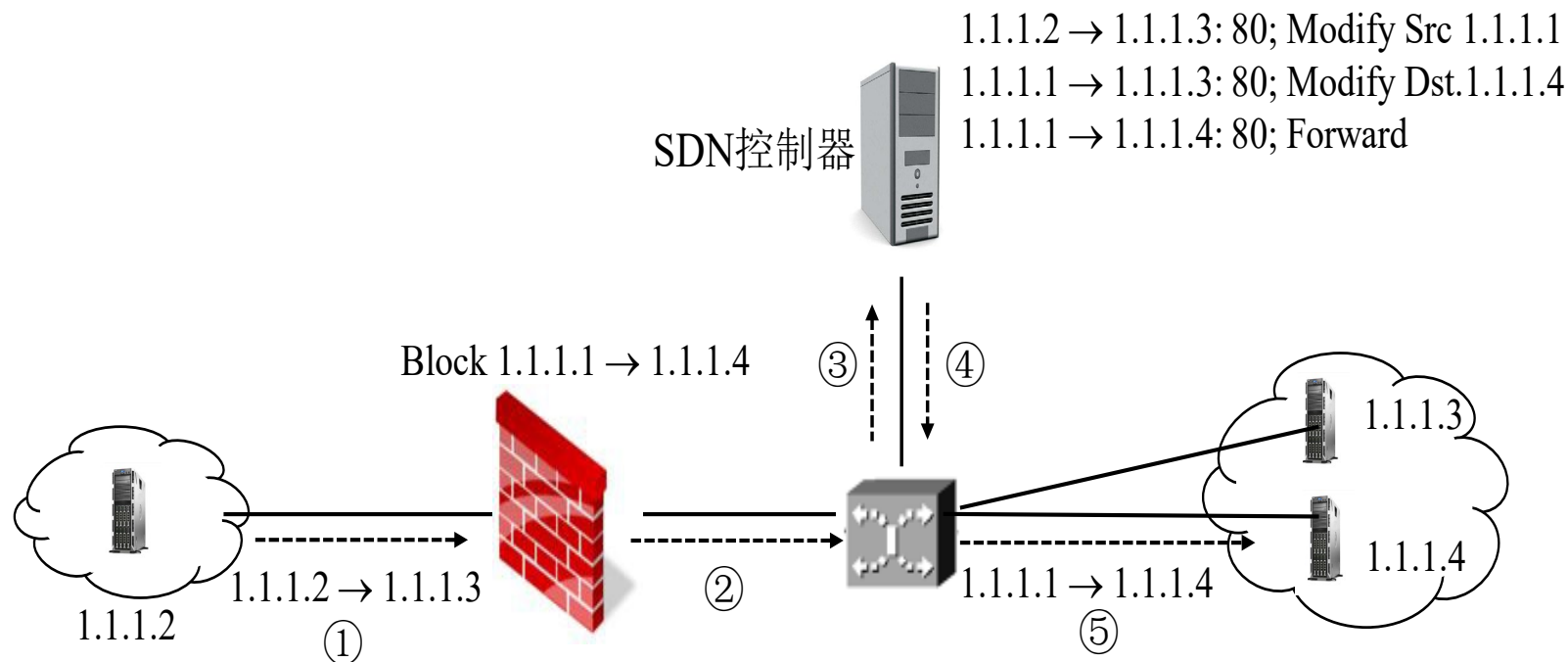
SDN安全-应用层安全

SDN恶意应用程序攻击场景示例



SDN安全-应用层安全

SDN应用程序配置冲突示例





SDN安全-北向接口安全

- 北向接口安全问题与应用层安全问题具有一定相似性，主要集中在非法访问权限、身份授权认证、数据泄露、数据篡改及程序漏洞等





SDN安全-控制层安全

- 控制器是核心，安全非常重要
- 控制器面临的安全威胁主要包括拒绝服务攻击和非法接入等





SDN安全-南向接口安全

- OpenFlow 协议中可能涉及的安全问题包括：
 - 控制器与交换机之间缺少数据加密措施
 - 控制器与交换机通信缺乏认证机制
- 主要原因：考虑到性能，**没有启用TLS**





SDN安全-数据层安全

- 数据层安全威胁，主要存在于数据层交换设备上。与传统设备类似，数据层交换设备的安全问题并非SDN特有，主要的安全威胁有拒绝服务攻击、非法设备接入和病毒感染传播



SDN安全研究

SDN 安全问题	安全问题类型	影响层面	问题描述及难点
授权认证问题	未经授权的控制器访问	C、S、D	1) 缺乏有效的信任评估和信任管理机制
	未经身份认证的应用	A、N、C	2) 验证网络设备是否安全的技术和验证应用程序是否安全的技术并不相同
数据安全问题	数据泄露	D	1) 侧信道攻击探测流规则
	数据篡改	C、S、D	2) 分组处理时序分析发现转发策略 3) 恶意修改流规则
恶意应用问题	虚假规则注入	A、N、C、D	1) 由非法用户或设备产生，如伪造的流规则等
	控制器劫持	C、S	2) 恶意应用程序可以轻易地被开发，已授权的合法应用程序也可能被篡改，并应用于控制器上 3) SDN 控制器受到最严重的威胁、故障或恶意的控制器可使整个 SDN 受到威胁
拒绝服务攻击	控制器泛洪攻击	C	1) 逻辑中心化控制器计算资源及交换机流表资源有限性 2) 资源管理机制不完善，无法区分攻击者与正常用户，提供不同服务质量
	控制/数据通路泛洪攻击	C、S、D	
	交换机流表泛洪攻击	D	
配置问题	缺少 TLS 机制	C、S、D	1) 不同控制器、不同应用程序间缺乏有效、安全流规则同步方案，无法避免相互竞争、彼此冲突和覆盖情况
	策略/流规则合法性及一致性	A、N、C	2) 缺少安全配置机制
系统级安全问题	架构缺陷	A、N、C、S、D	1) 系统架构无法从设计角度达到完美
	系统漏洞	A、N、C、S、D	2) 系统实现时无法避免引入系统漏洞，并为攻击者所利用
	缺少状态可视化	A、C	3) 系统无法对网络状态（安全、连接状态）可视化

表中A、N、C、S、D 分别表示应用层、北向接口、控制层、南向接口和数据层

SDN安全研究

SDN 安全问题	相关研究	研究目标	研究内容	涉及层面
授权认证	安全分布式控制， 拜占庭弹性 SDN	提高控制层对授权认证方面安全问题弹性	分布式签名算法设计	C、S
	弹性认证	提高 SDN 架构弹性	拜占庭式冗余设计	C、S
	PermOF	权限设置	控制器分层设计	C
	OperationCheckpoint	权限系统设置	接口检测系统设计	A、N
	AuthFlow	控制器行为检测	基于证书的认证系统	A、N、C
	FortNOX	授权接入控制	复合认证检测系统	A、C、S、D
		授权认证综合架构		A、N、C、S、D
数据安全	SE-Floodlight	架构组件间安全通信	认证及安全约束技术	A、N、C、S
恶意应用	ROSEMARY	复合安全功能内核	应用隔离及弹性策略	A、C
	LegoSDN	提高控制器弹性	容错机制	A、C
拒绝服务 攻击	Avant-Guard	数据平面代理	连接迁移、执行触发	C、S、D
	FloodGuard	控制器分析模块	流量迁移，主动流规则分析	A、C、S、D
	CPRcovery	冗余备份设计	主从控制器无缝切换	C、S
	Delegate Network Security	管理协议扩展	Iden++协议	S、D
	VAVE	DoS 伴随攻击 IP/MAC 欺骗	基于 SDN 的源地址认证	C、D
配置问题	NICE	检测网络内部冲突	网络行为建模 模型检查	A、C、S
	FlowChecker			
	Flover			
	Anteater			
	VeriFlow	实时策略检查	实时冲突检测解决算法	A、C、S、D
	NetPhumbe			
	FlowGuard			
	Frenetic	语义识别检测	高级语言冲突判断	A、N、C、S
	Flow-Based Policy			
	Splendid Isolation、VeriCon	形式化验证方法	形式化工具建模分析	N、C、S
	Verificare、Machine-verified SDN			
系统级安全	Debugger for SDN	简化 SDN 调试	SDN 原型网络调试器	A、S
	OFHIP、Secure-SDMN	提升 SDN 移动安全性	扩展安全加强版通信协议	S
	FRESCO、CMD	提升系统整体安全型	模块组合、拟态防御	A、N、C、S、D



内容提纲

1

SDN安全

2

零信任安全

3

移动目标防御

4

网络空间拟态防御

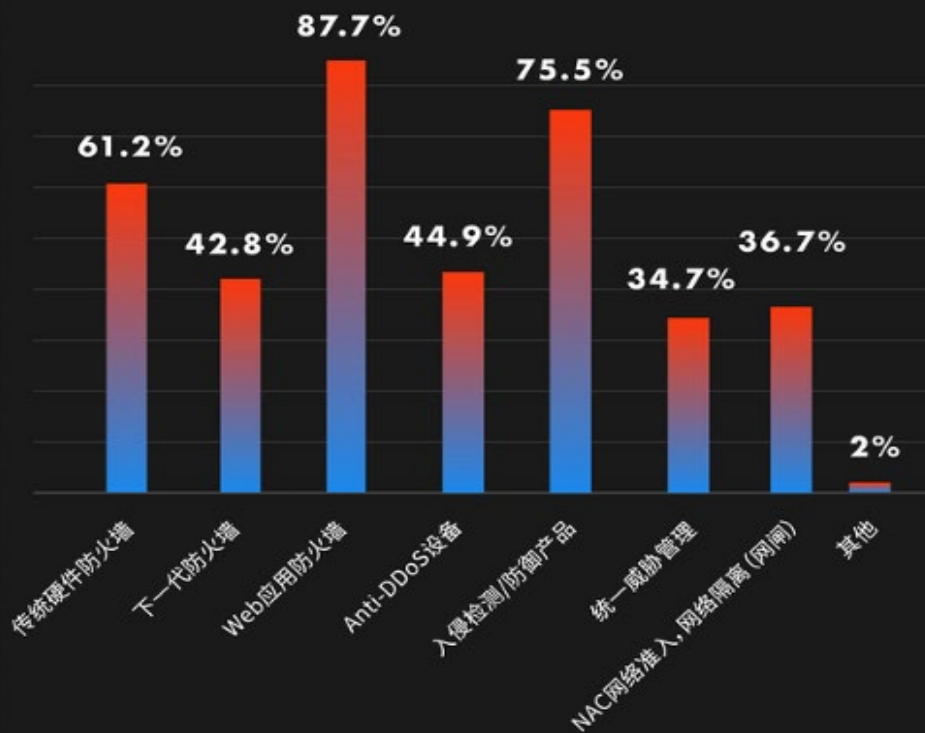


边界防护

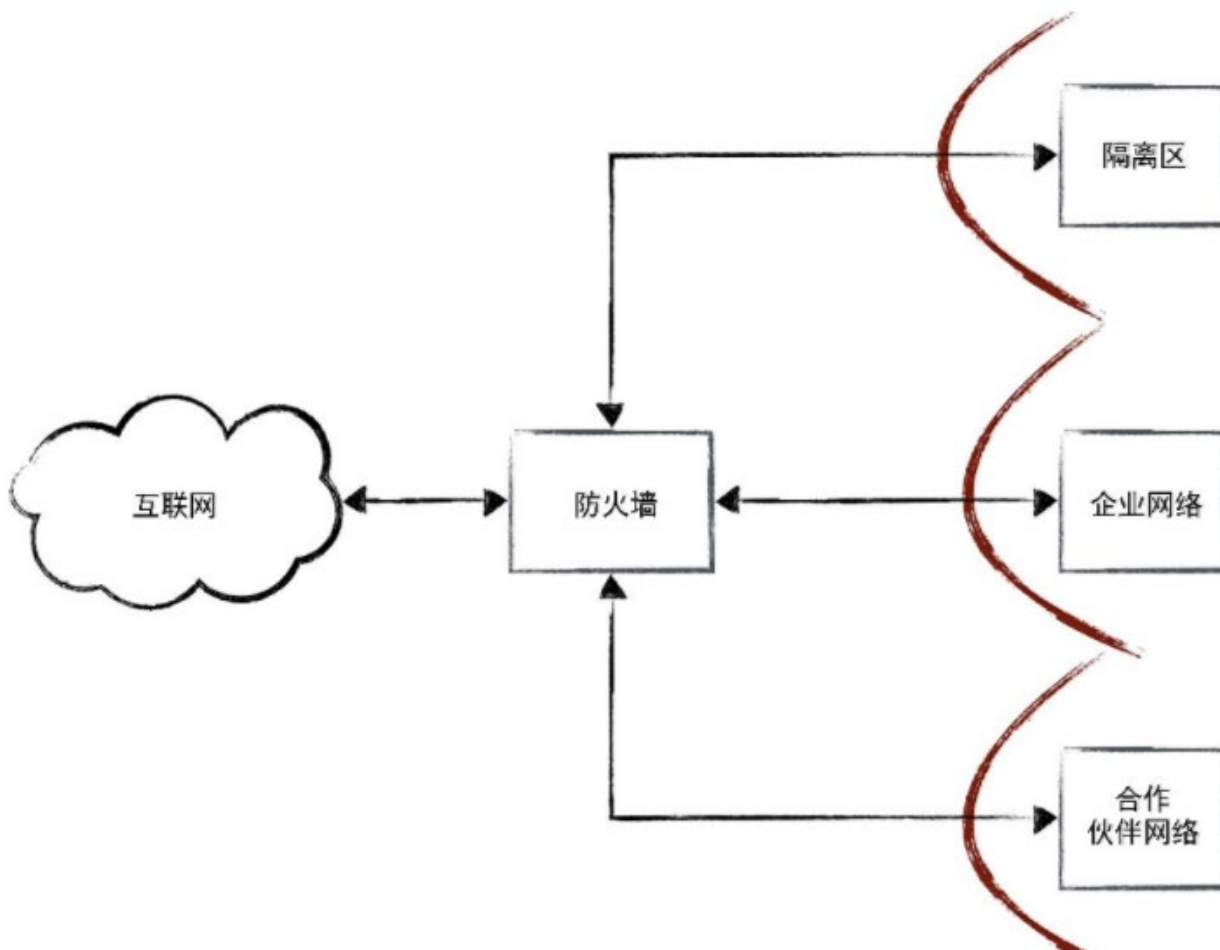
FreeBuf企业安全系列之

2020国内WAF 产品研究报告

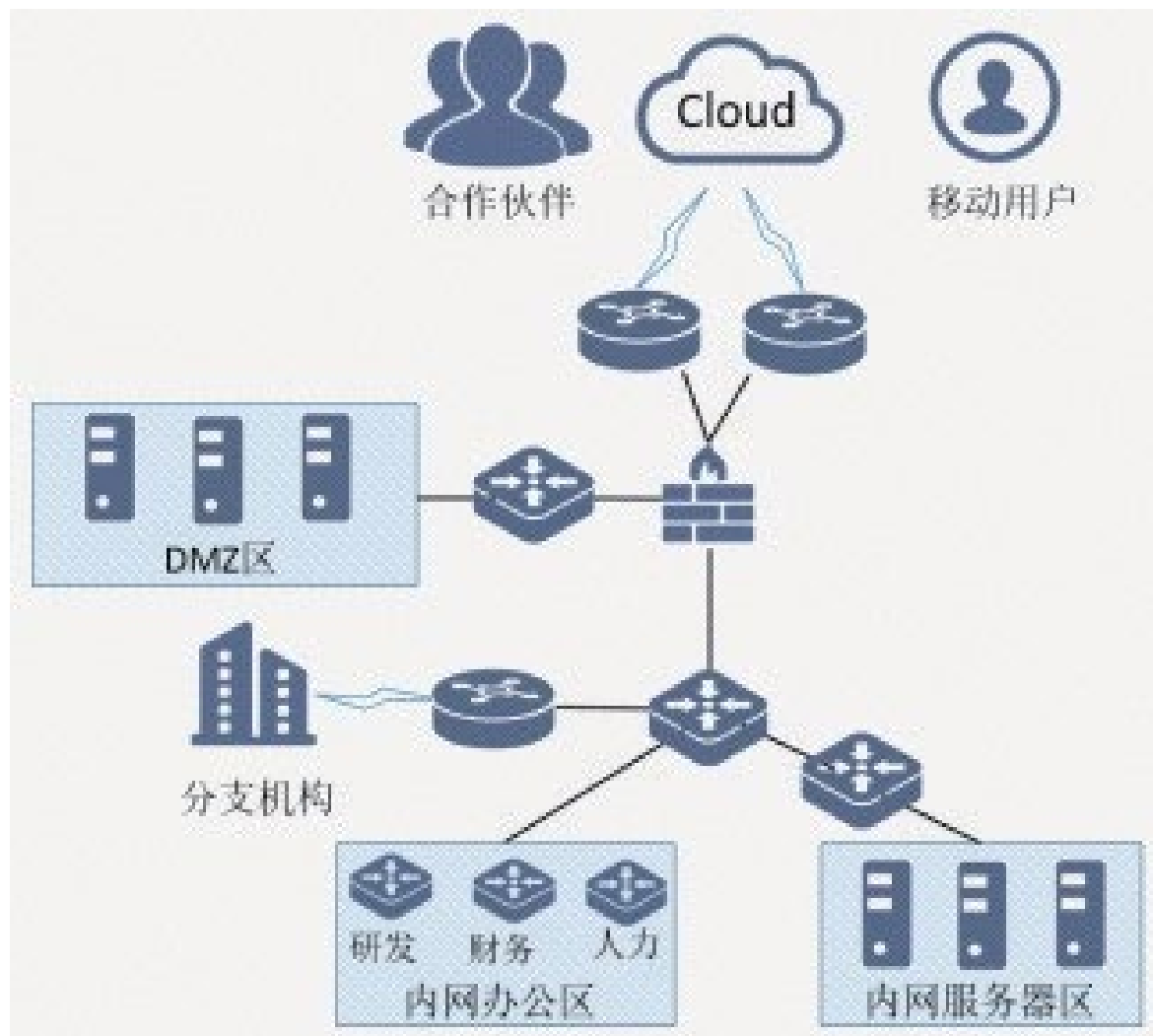
企业部署的边界防护设备



边界防护



边界防护





边界防护

■ 问题：

- 边界防护建立在“网络内部的系统和网络流量是可信的”这一假设上，缺乏网络内部的流量检查。
- 新的网络应用和计算模式，如云计算、移动设备、物联网，已无法满足“网络有明确的边界”这一条件，使得传统的、基于网络边界的安全防护模式逐渐失去了防护能力。
- 分区部署使得主机部署缺乏物理及逻辑上的灵活性。
- 边界防护设备一旦被突破，整个网络处于危险之中。



边界防护

- 突破边界不可避免

- 在Kill Chain攻击框架发布近10年后，ATT&CK框架进一步丰富了攻击分析和场景，包含了黑客渗透过程中利用具体的各种技术。在这些攻击技术和手段面前，传统的安全设备堆叠已经失守，如各种Webshell的混淆、加密流量、社会工程对于终端的渗透，基本都可以穿透所有的传统安全产品下堆叠出的安全架构和系统



边界防护

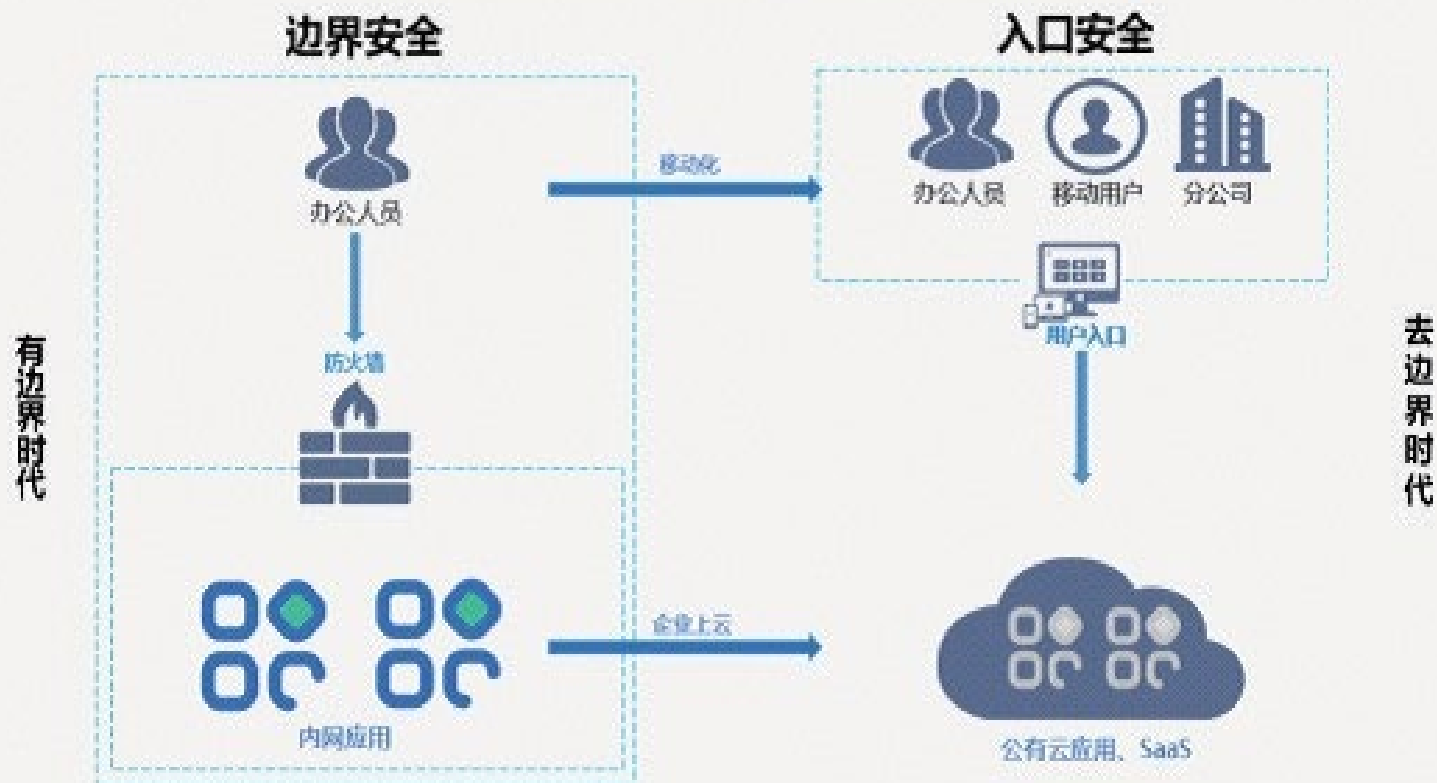
- 突破边界不可避免，且难以发现
 - FireEye 的M-Trends 2020 Reports中，发现攻击者隐藏或者驻留时间的中位数为56天。近几年的威胁检测时间都在不断缩短，主要是由于对于内部威胁发现较早，极大减少了中位数，但外部威胁的驻留时间还有141天，近5个月之久

GLOBAL MEDIAN DWELL TIME BY YEAR

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019
All	416	243	229	205	146	99	101	78	56
Internal Detection	—	—	—	—	56	80	57.5	50.5	30
External Notification	—	—	—	—	320	107	186	184	141

边界防护

去边界化时代，
传统边界安全不再适用，需要新安全体系：入口安全





零信任

- “**零信任**（Zero Trust）”这一术语是指一种不断发展的网络安全范式（paradigm），它将防御从静态的、基于网络边界的防护转移到关注用户、资产和资源。
 - 由Jon Kindervag在Forrester的一次报告中提出
 - 零信任假定不存在仅仅基于物理或网络位置（即局域网与互联网）就授予资产或用户账户的**隐含信任**（Implicit Trust）。





零信任

■ 零信任的理解

- “零信任”不是“不信任”，也不是“默认不信任”，更接近的说法是“从零开始建立信任”。“零信任”中的“零”是“**尽可能小**”的意思，而非“无或没有”之类的绝对概念。
- **不是“先验证，然后信任”，而是“永远不要信任，永远要验证”**



零信任

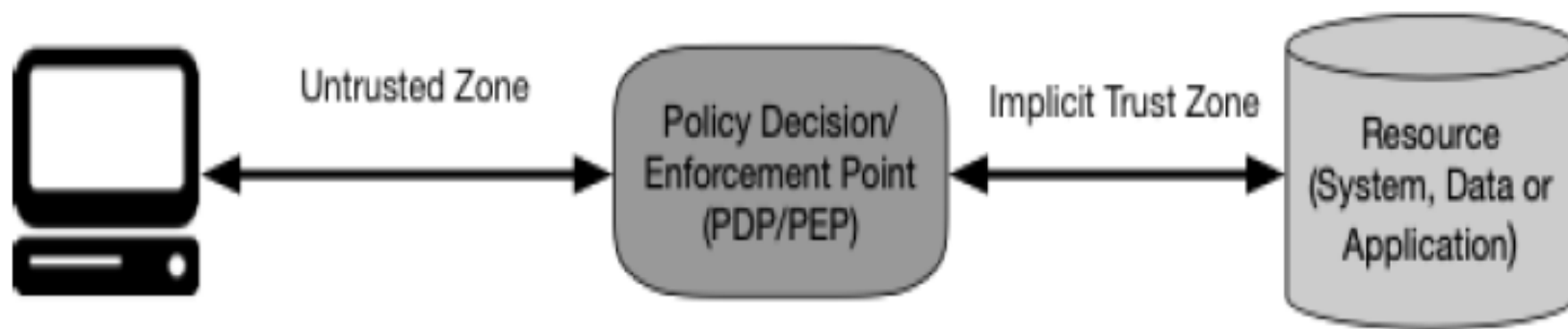
■ 零信任的理解



零信任

■ 零信任的理解

- NIST在2019年9月发布的“零信任架构（Zero Trust Architecture, ZTA）”标准草案中，将“零信任”解释为“**零隐含信任**（Zero Implied Trust）”



零信任

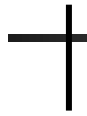


2020年NIST.SP.800-207-draft2

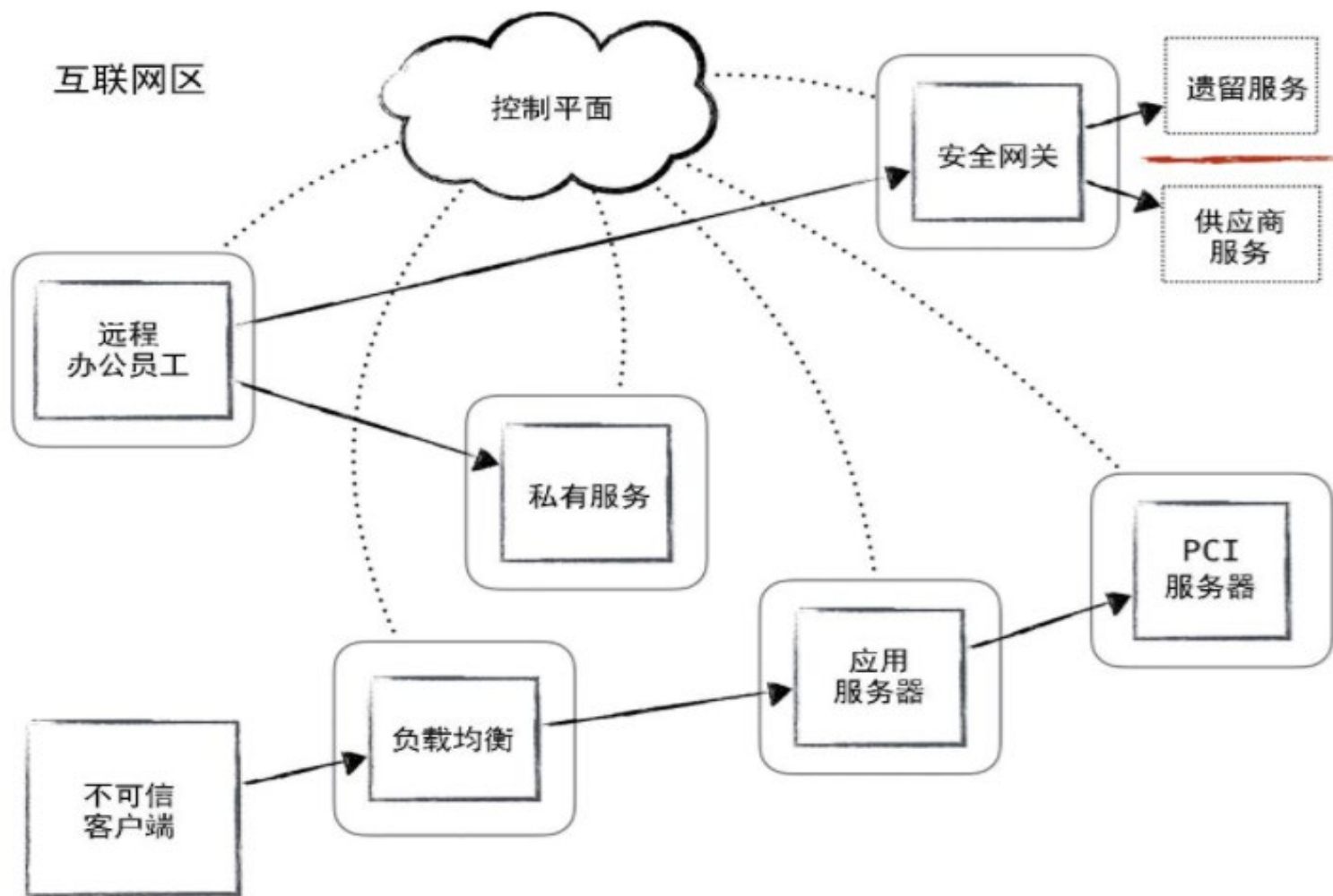
- 2018年中央部委、国家机关、中大型企业开始探索实践零信任安全架构
- 2017年微软推出了零信任安全解决方案，业界大厂开始大力跟进
- 2013年CSA提出了基于零信任的SDP解决方案
- 2011-2017年，Google Beyondcorp实施落地
- 2010年约翰.金德维格提出零信任理论



零信任

- 零信任安全有5个基本假定：
 - ① 网络无时无刻不处于危险的环境中。
 - ② 网络中自始至终存在外部或内部威胁。
 - ③ 网络的位置不足以决定网络的可信程度。“可信”内网中的主机面临的安全威胁与互联网上的主机别无二致。
 - ④ 所有设备、用户和网络流量都应当经过认证和授权。
 - ⑤ 安全策略必须是动态的，并基于尽可能多的数据源计算而来。
- 

零信任架构





NIST零信任架构

- 美国国家标准和技术研究所（NIST）在2019年9月发布了“零信任架构（Zero Trust Architecture）”标准草案（NIST.SP.800-207-draft），并于2020年2月发布了修订版NIST.SP.800-207-draft2
 - 美军方是重要推手：美国国防信息系统局（DISA）和国防部（DoD）公布的“BlackCore（黑核）”项目
 - 背景讨论





NIST零信任架构

■ 基本原则或宗旨（tenets）

- ① 所有数据源和计算服务都被视为资源
- ② 无论网络位置如何，所有通信都应是安全的
- ③ 对单个企业资源的访问是基于每个连接进行授权的
- ④ 对资源的访问由策略决定，包括客户身份、应用和请求资产的可观察状态，也可能包括其他行为属性





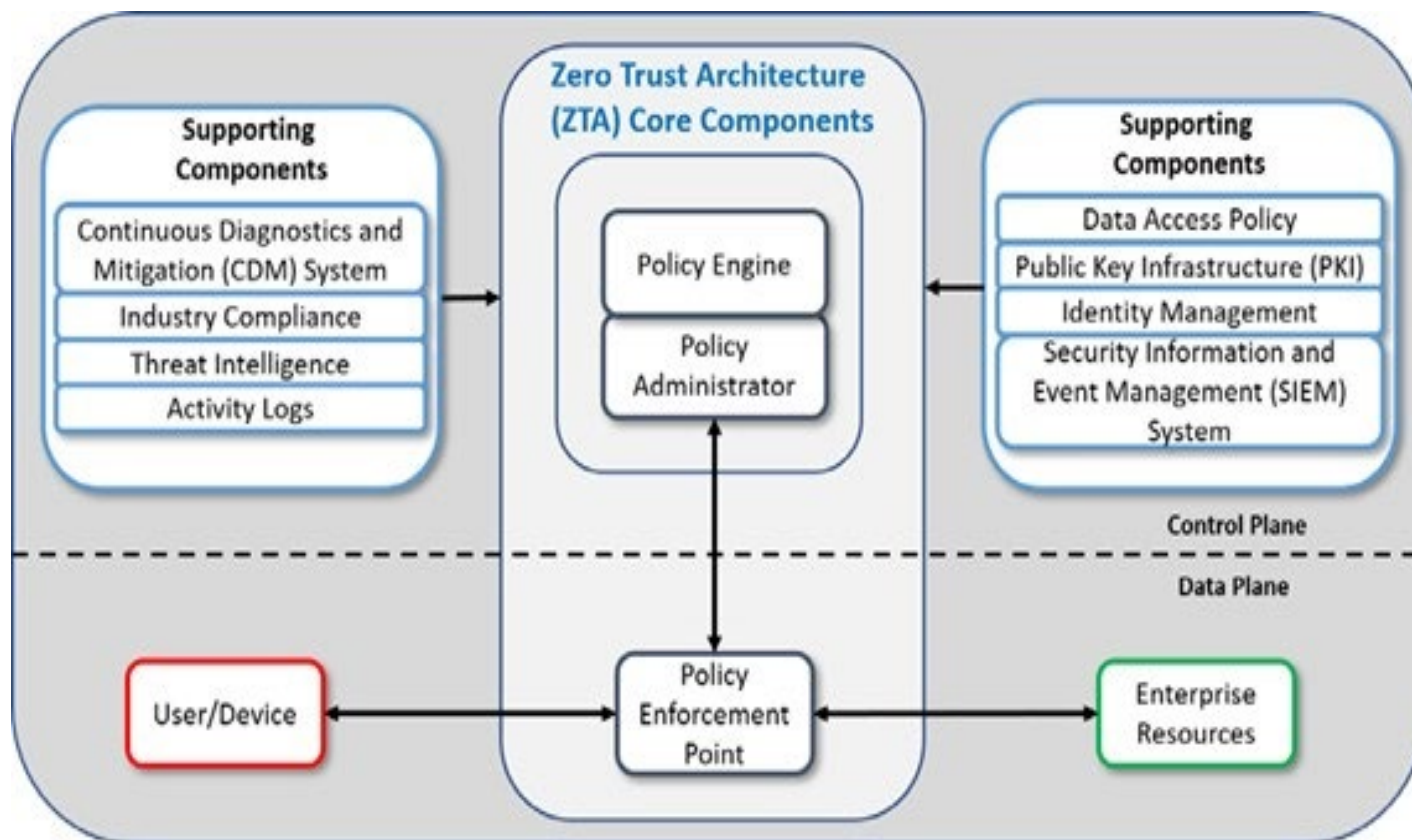
NIST零信任架构

- 基本原则或宗旨（tenets）

- ⑤ 企业确保所有自己拥有的和相关联的系统处于尽可能最安全的状态，并监视系统以确保它们保持尽可能最安全的状态
- ⑥ 在允许访问之前，所有资源的身份认证和授权都是动态的，并且必须严格地实施
- ⑦ 企业尽可能收集有关网络基础架构和通信的状态信息，并利用这些信息改善其安全形势（posture）

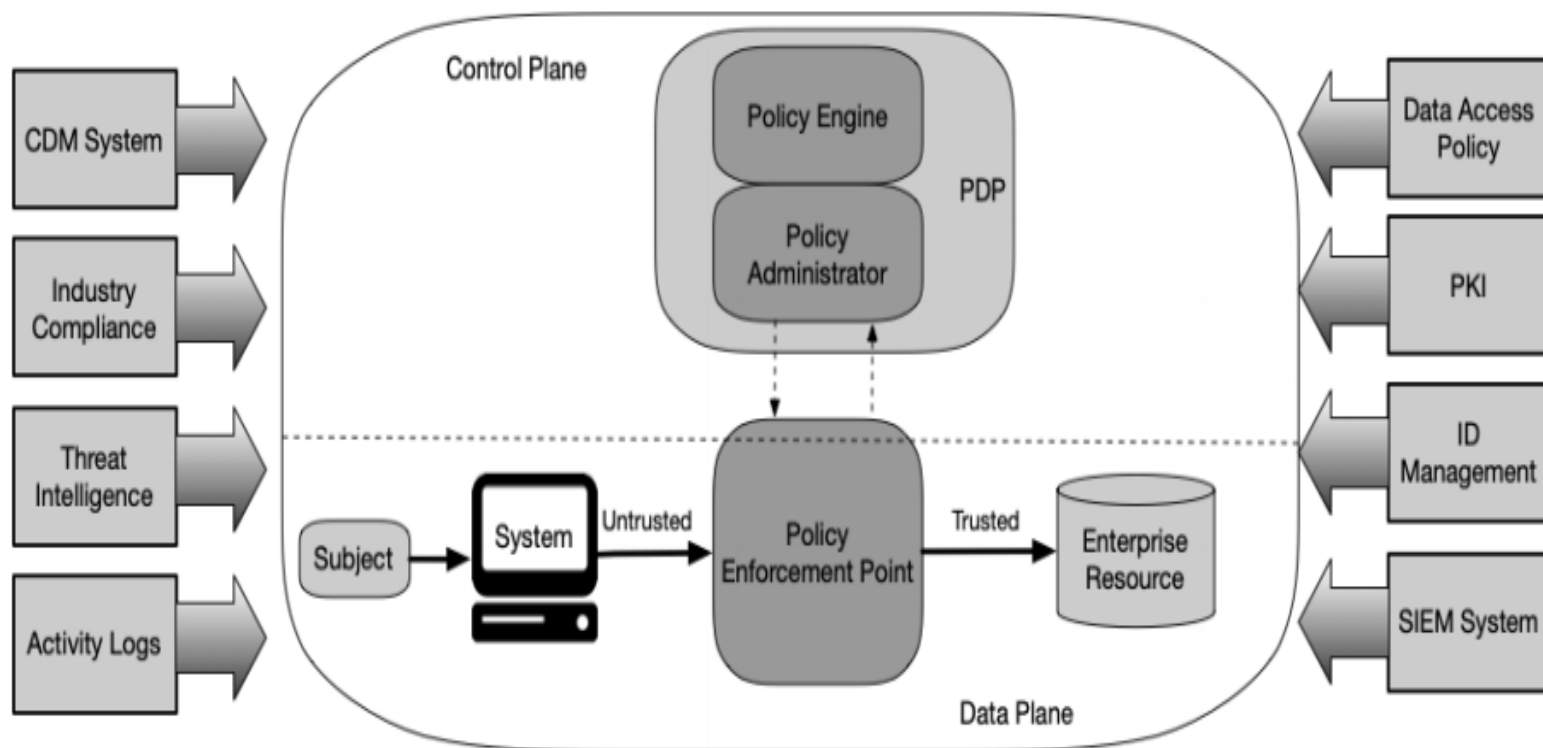
NIST零信任架构

■ ZTA（零信任架构）高层级架构



NIST零信任架构

■ ZTA架构中的核心逻辑组件





NIST零信任架构

- ZTA逻辑组件使用单独的控制平面进行通信，而应用数据在数据平面上进行通信





核心部件

- **策略判定点（PDP）** 被分解为两个逻辑组件：策略引擎（PE）和策略管理器（PA）。
 - PE负责最终决定是否授予访问主体对资源（客体）的访问权限
 - PA负责建立或关闭主体与资源之间的连接（是逻辑连接，而非物理连接）





核心部件

- **策略执行点（PEP）** 负责启用、监视并最终终止主体和企业资源之间的连接。
 - PEP是ZTA中的单个逻辑组件，但也可能分为两个不同的组件：客户端（例如，用户便携式电脑上的代理）和资源端（例如，在资源之前控制访问的网关组件）或充当连接门卫（gatekeeper）的单个门户组件。在PEP之外是前面介绍的托管企业资源的隐含信任区域



其它组件

- **持续诊断和缓解（CDM）系统**
 - 收集企业资产（assets）的状态信息，并负责
对配置和软件组件进行更新或升级
- **行业合规系统（ICS）**
 - 确保企业遵守与其相关的任何监管制度（如
FISMA，健康或财经行业信息安全要求等）





其它组件

- 威胁情报源 (TIF)

- 提供内部或外部来源的安全情报，帮助策略引擎做出访问决策

- 数据访问策略 (DAP)

- 一组有关访问企业资源的属性、规则和策略。
这组规则可以在策略引擎中编码，也可以由PE动态生成)





其它组件

- **企业公钥基础设施 (PKI)**
 - 企业PKI负责生成由企业颁发给资源、参与者和应用程序的证书，并将其记录在案
- **身份管理系统 (IDMS)**
 - 负责创建、存储和管理企业用户账户和身份记录，包含必要的用户信息。该系统通常利用其他系统（如PKI）来处理与用户账户相关联的工作



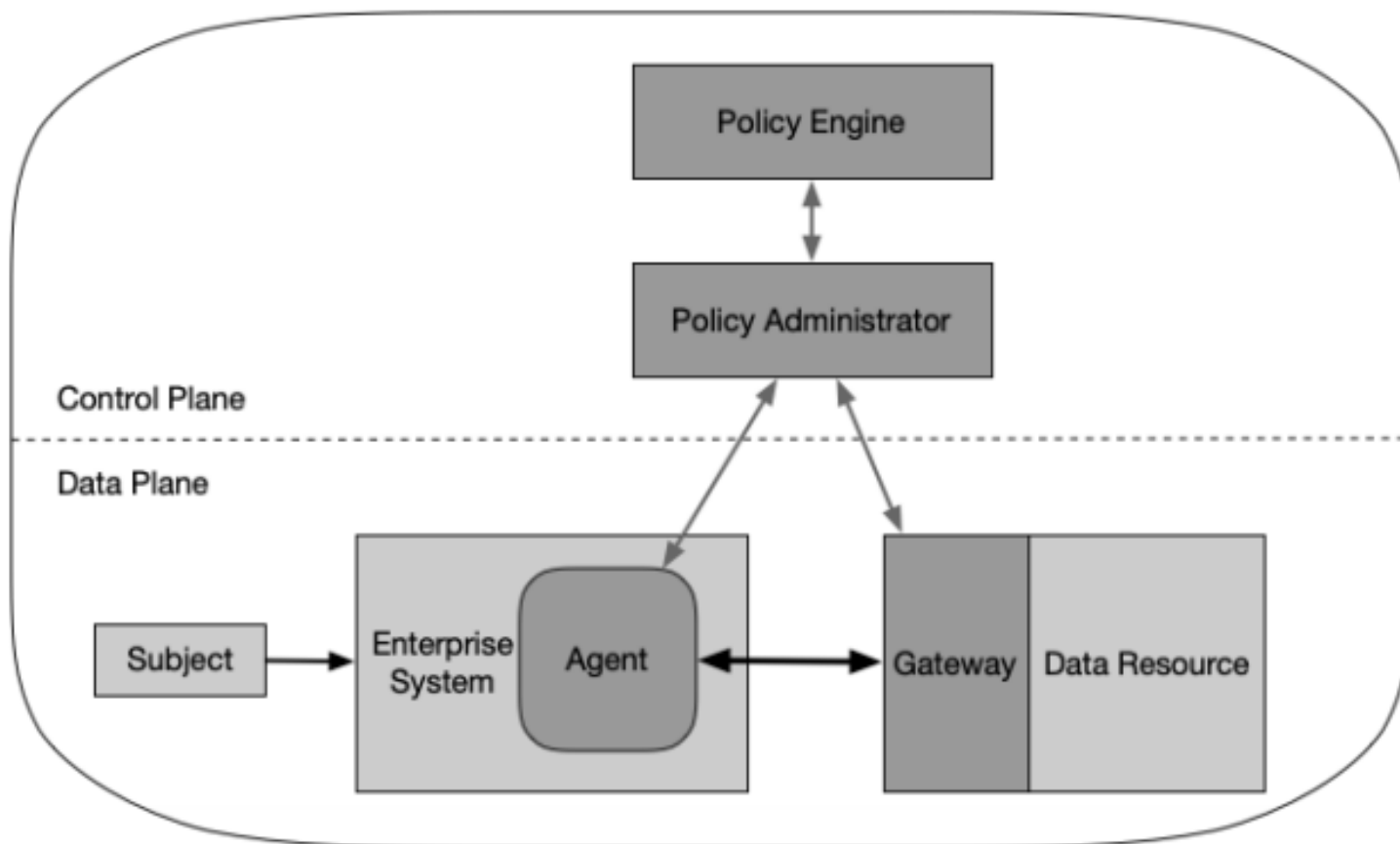
其它组件

- **网络和系统活动日志（NSAL）系统**
 - 聚合了资产日志、网络流量、资源访问操作和其他事件。这些事件提供关于企业信息系统安全态势的实时（或接近实时）反馈
- **安全信息和事件管理（SIEM）系统**
 - 收集以安全为中心的信息以供后续分析。分析结果将用于完善安全策略，并预警对企业资产发起的可能攻击



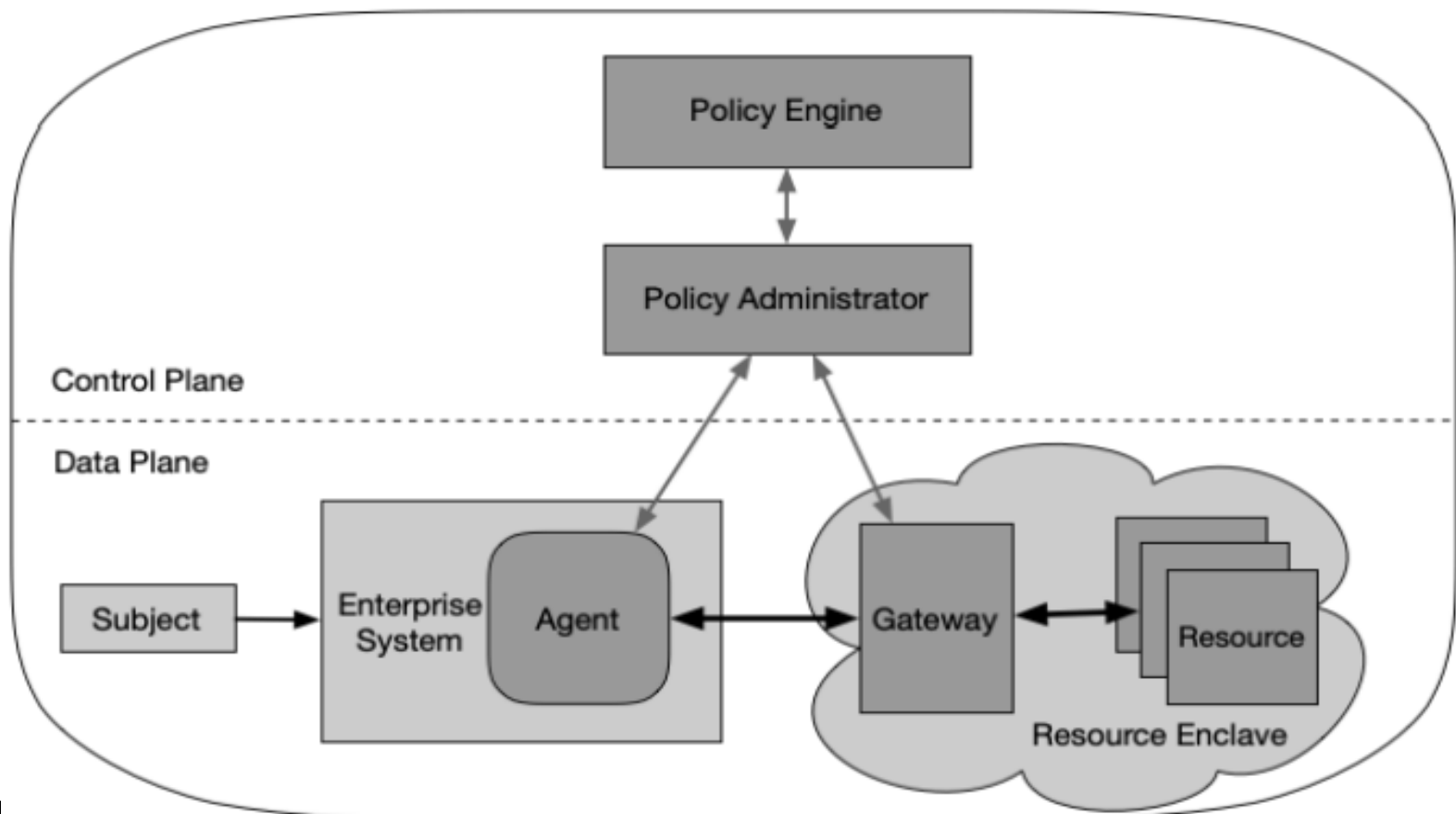
NIST零信任架构

■ 基于设备代理/网关的部署模型



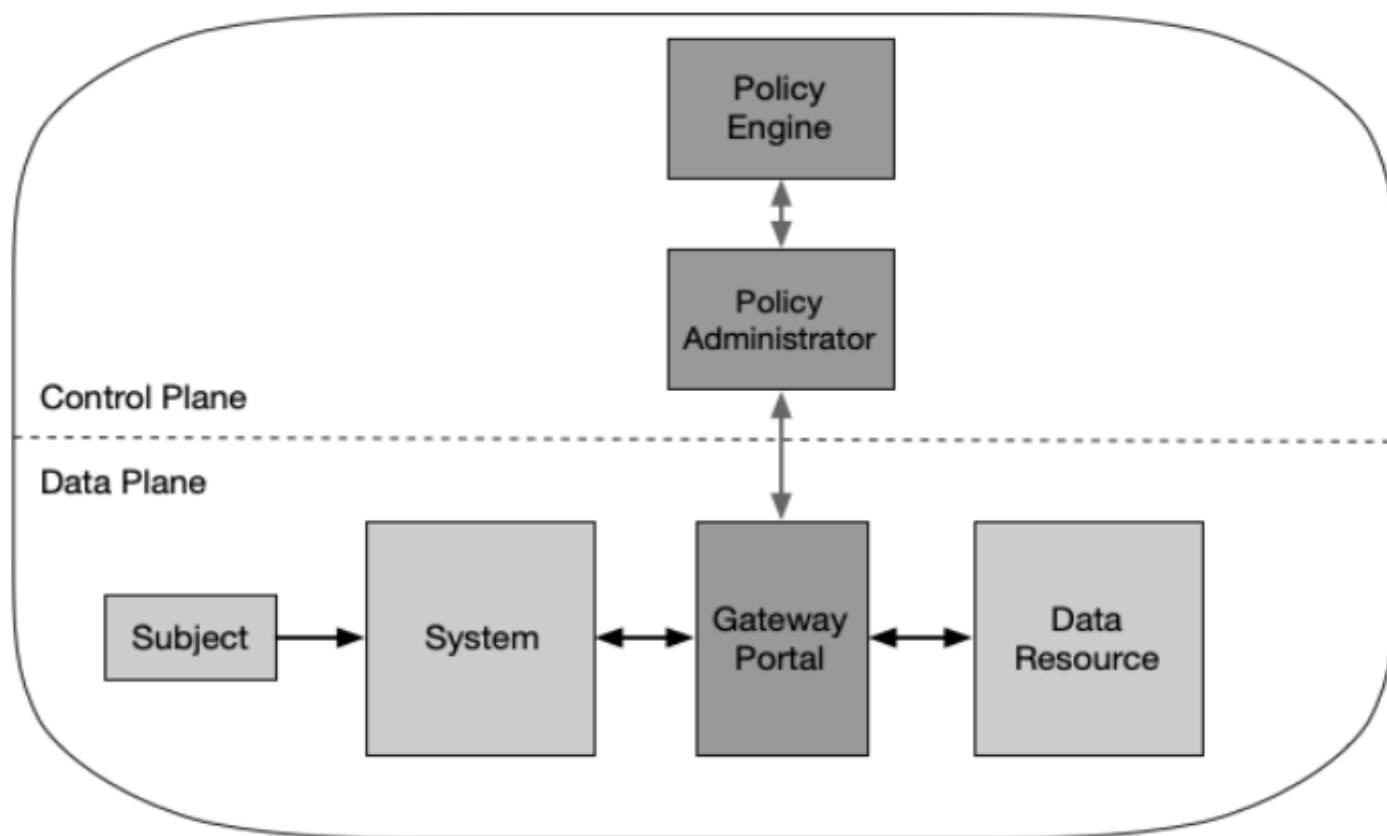
NIST零信任架构

■ 飞地部署模型



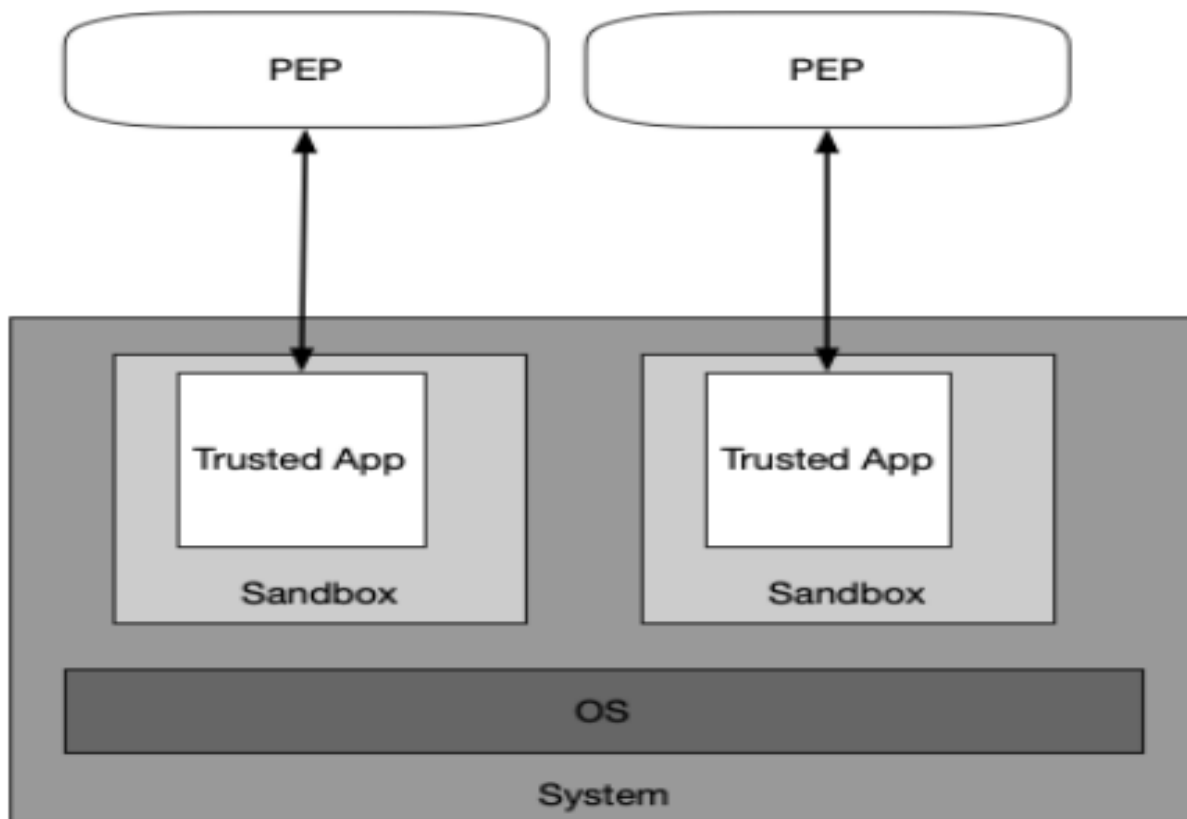
NIST零信任架构

■ 基于资源门户的部署模型



NIST零信任架构

- 设备应用沙箱模型





信任算法

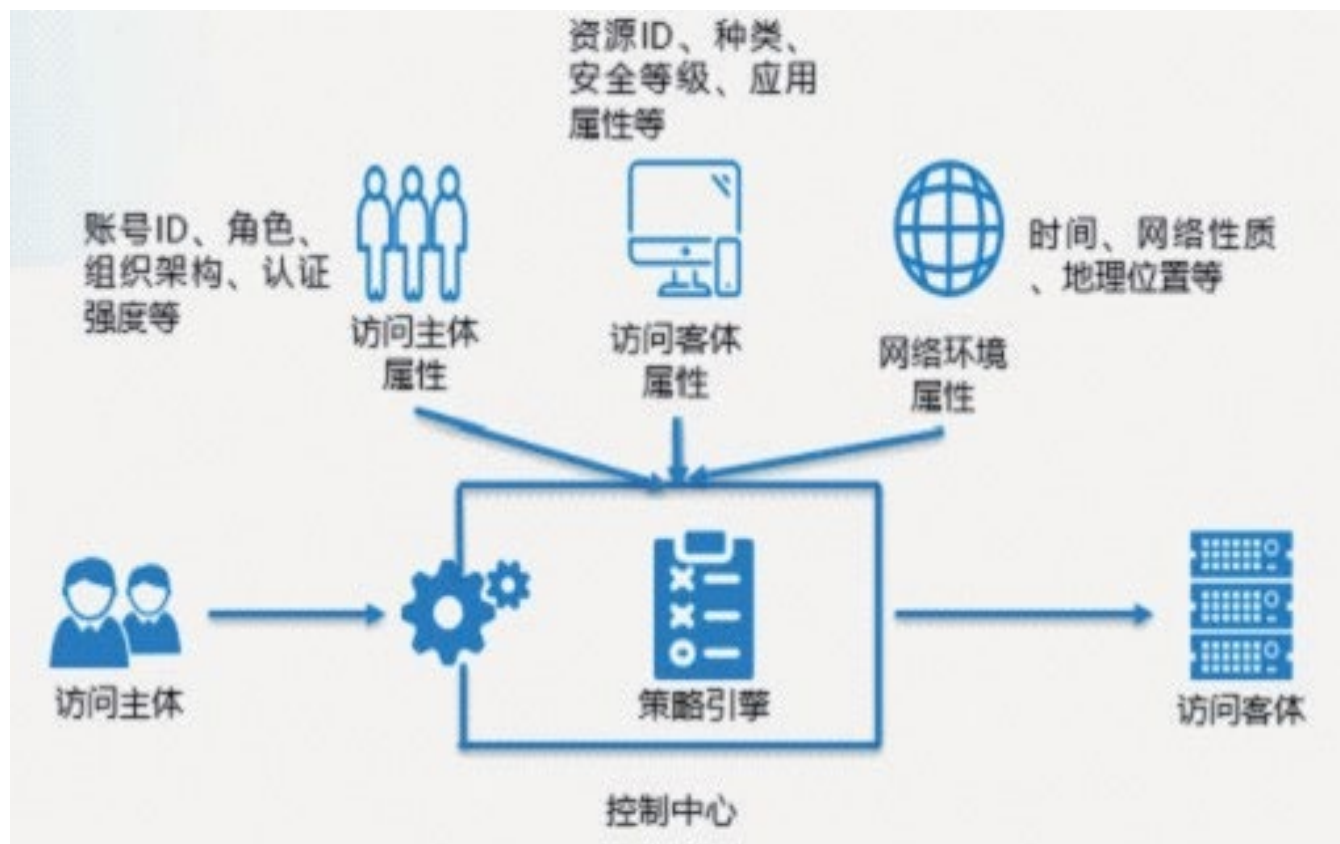
■ 动态评估信任等级

- ZTA中，不再给网络参与者定义和分配基于二元决策的策略，而是持续监视参与者的网络活动，并据此持续更新其信任评分，然后使用这个评分作为授权策略判定的依据之一。客户端以不可信的方式开始访问会话请求，并在访问过程中通过各种机制不断积累信任，直到积累的信任足够获得系统的访问权限。



信任算法

■ 基于属性的动态权限控制





零信任-进一步讨论

- 从继承和演进的角度看，零信任的核心之意是精细化和动态化。即将过去的相对粗颗粒度的、静态的防御机制，从最早的网络级，到后来的子网级或业务网络级，然后再到应用级，再到应用中的**操作级**，再往后到达**数据级**。这个发展的过程，就是一个越来越细粒度、越来越动态的过程，而且要**以信任体系**为支撑





零信任-进一步讨论

- 现代企业环境正在不可避免地云环境迁移，而零信任的特性非常适合云环境部署。零信任关于网络不可信、不受控的假设，特别适合云基础设施。特别是在使用商业云时，如果云基础设施本身受到威胁，则零信任架构可提供保护，避免敌手在我们的虚拟网络中扎根





零信任-进一步讨论

- 为配合NIST之前发布的《零信任架构》标准草案，NIST下属单位NCCoE于2020年3月发布了《实现零信任架构》（草案）项目说明书，征求公开评论。该项目说明书瞄准的是零信任架构的落地实践，期望实现安全性与用户体验的兼得。



奇安信零信任架构

奇安信零信任解决方案概念图

奇安信
新一代网络安全

1.以身份为中心

- ✓ 为网络中的人、设备、应用都赋予逻辑身份。
- ✓ 以身份为访问的主体进行权限设置和判定；而非以网络位置为访问控制的依据。

2.业务安全访问

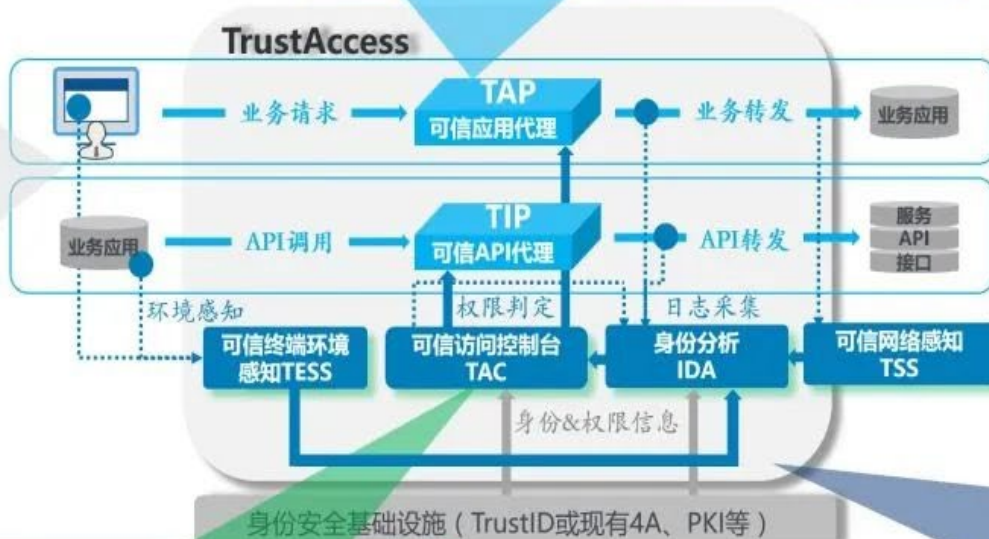
- ✓ 所有的访问都应该被加密和强制访问控制。
- ✓ 通过可信应用代理为用户访问业务应用进行保护。
- ✓ 通过可信API代理为应用和服务之间的API调用进行保护。

3.动态访问控制

- ✓ 所有访问权限不是静态的，而是动态调整的。
- ✓ 根据主体属性、客体属性、环境属性实现动态的、风险感知的可信访问控制。

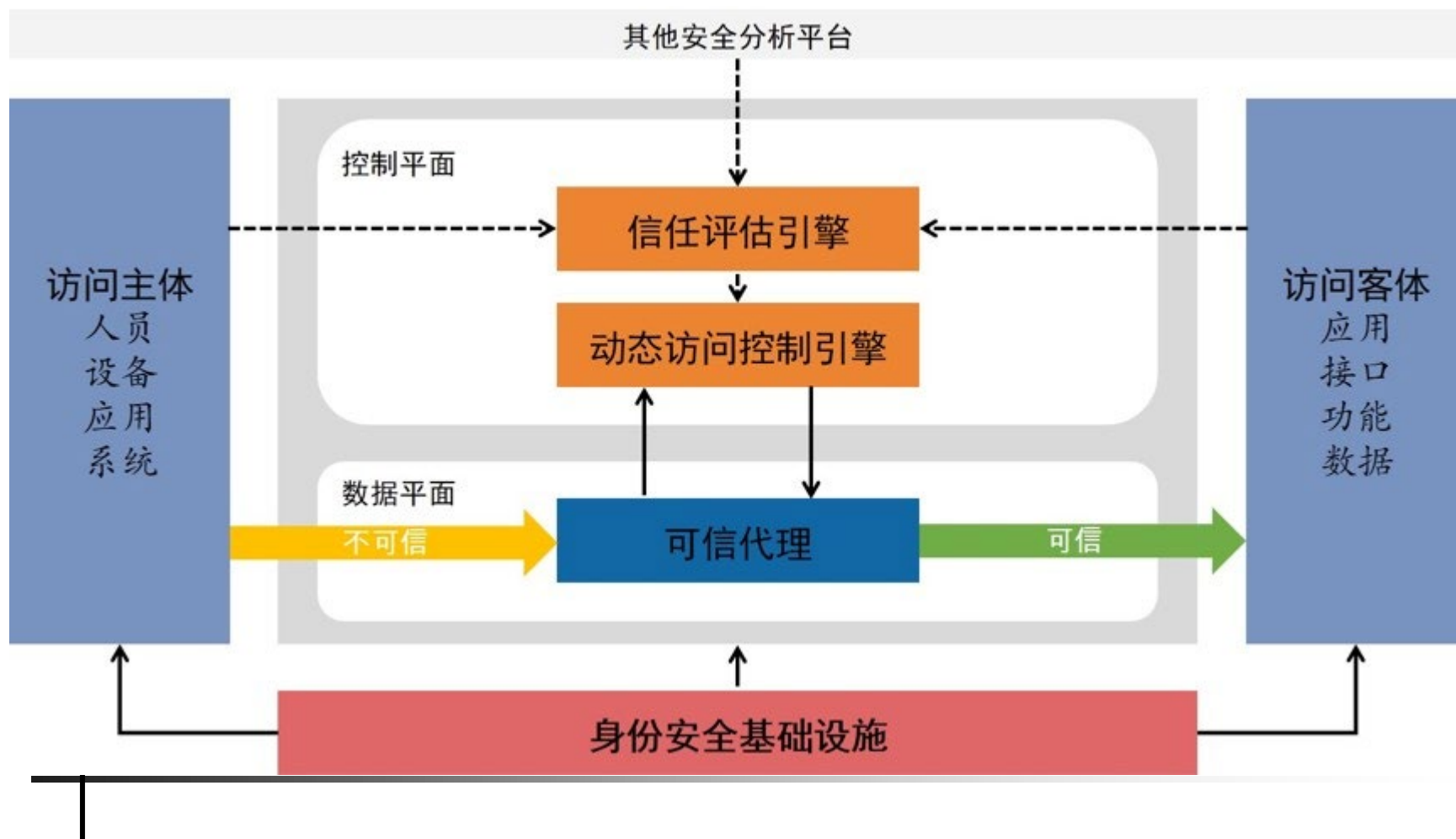
4.持续风险度量

- ✓ 持续的风险和信任度量支持动态访问控制。
- ✓ 可信环境感知对终端环境风险进行度量。
- ✓ 身份分析对身份及访问流量风险进行度量；并对外部风险输入进行关联分析



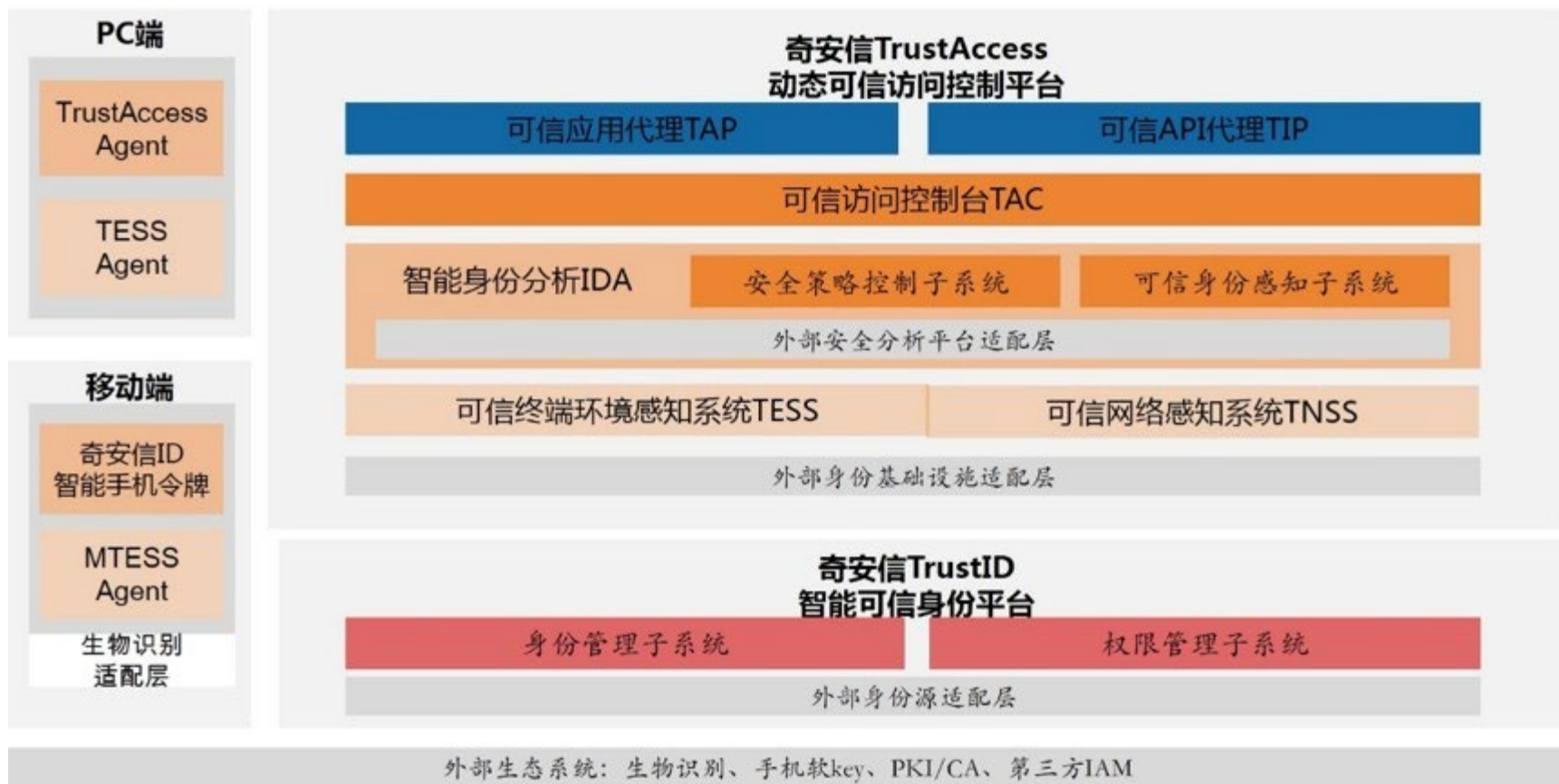
奇安信零信任架构

■ 核心架构组件



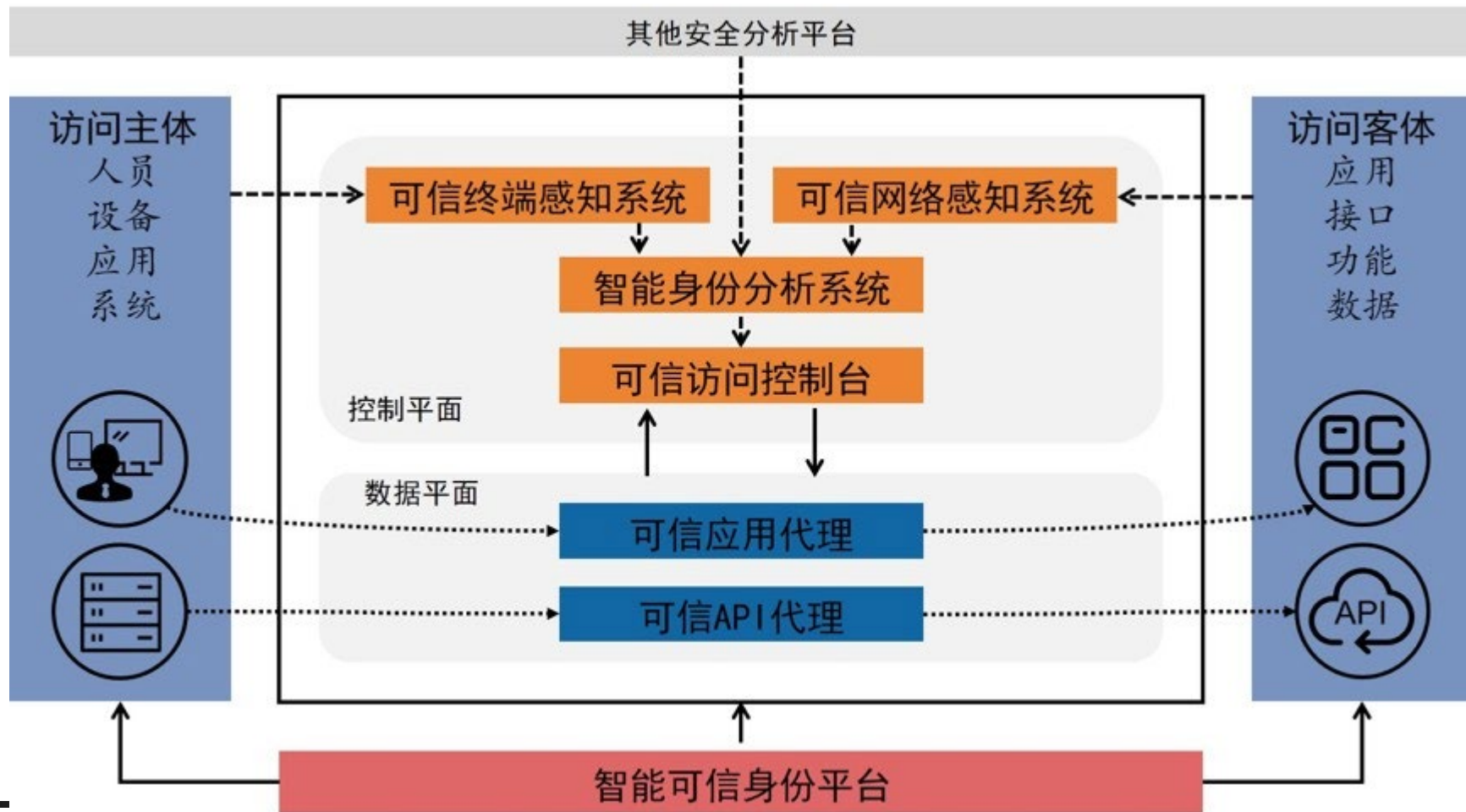
奇安信零信任架构

■ 产品解决方案



奇安信零信任架构

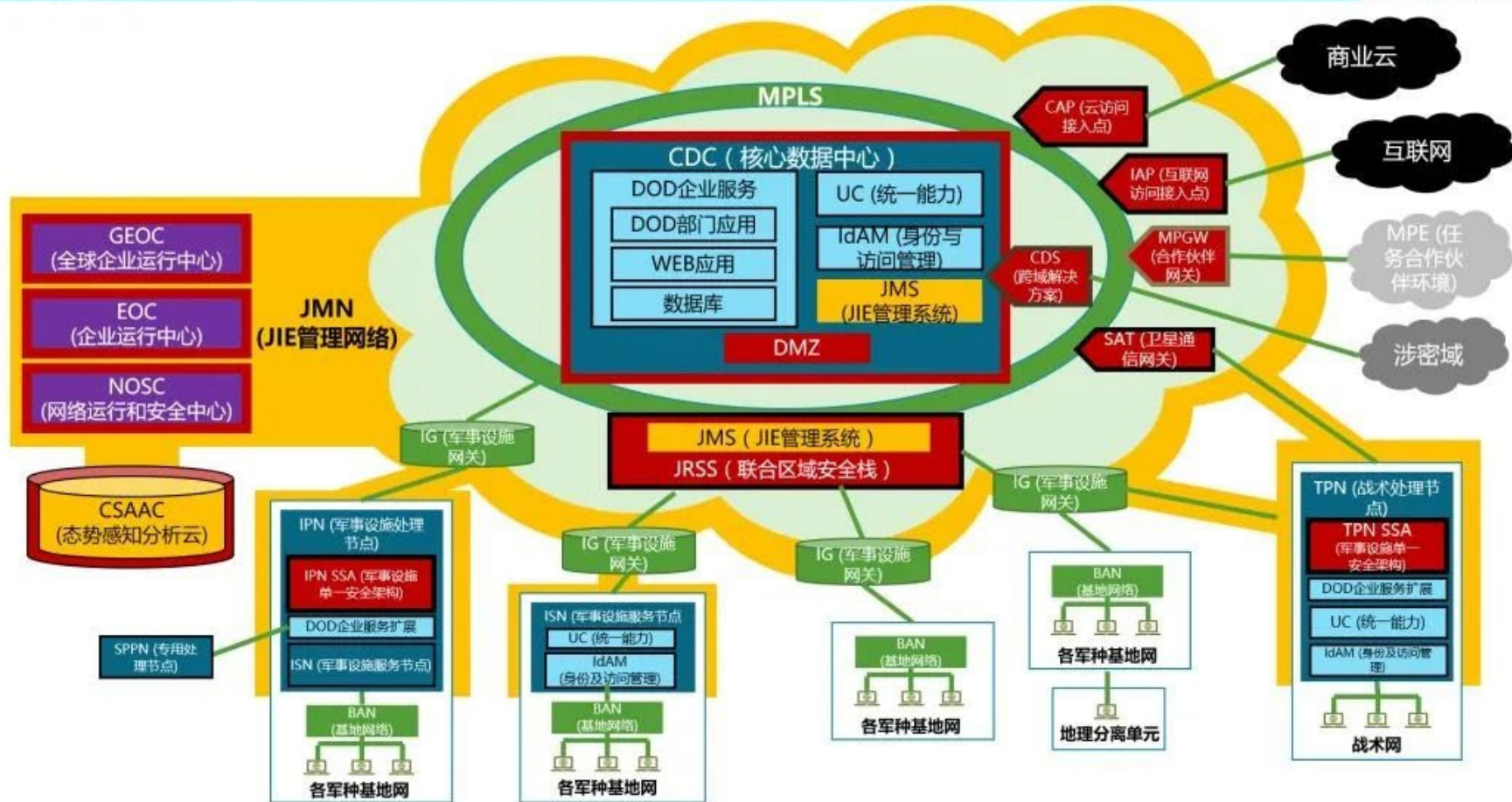
■ 解决方案与参考架构的关系



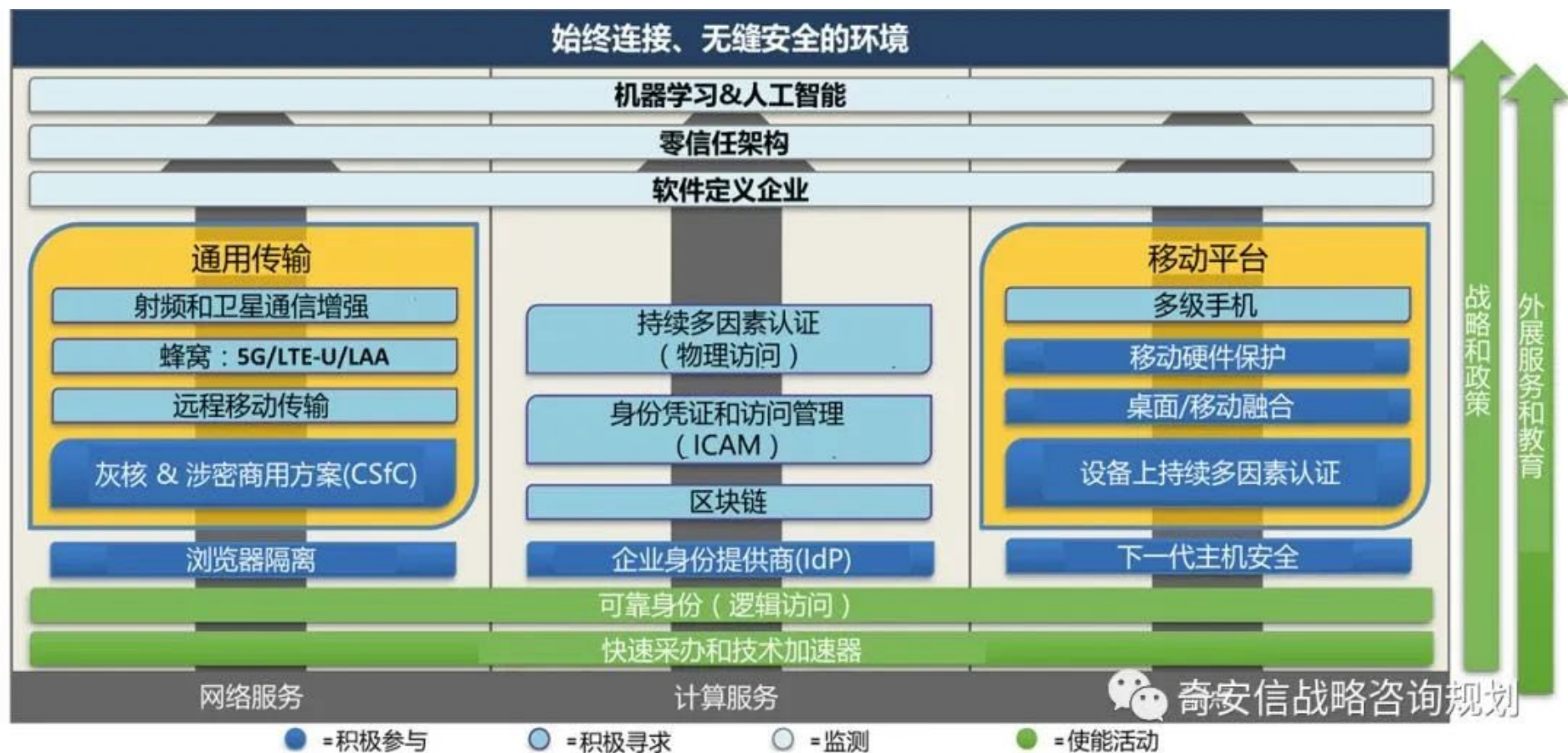
美军联合信息环境（JIE）架构

JIE框架

奇安信
新一代网络安全领军者

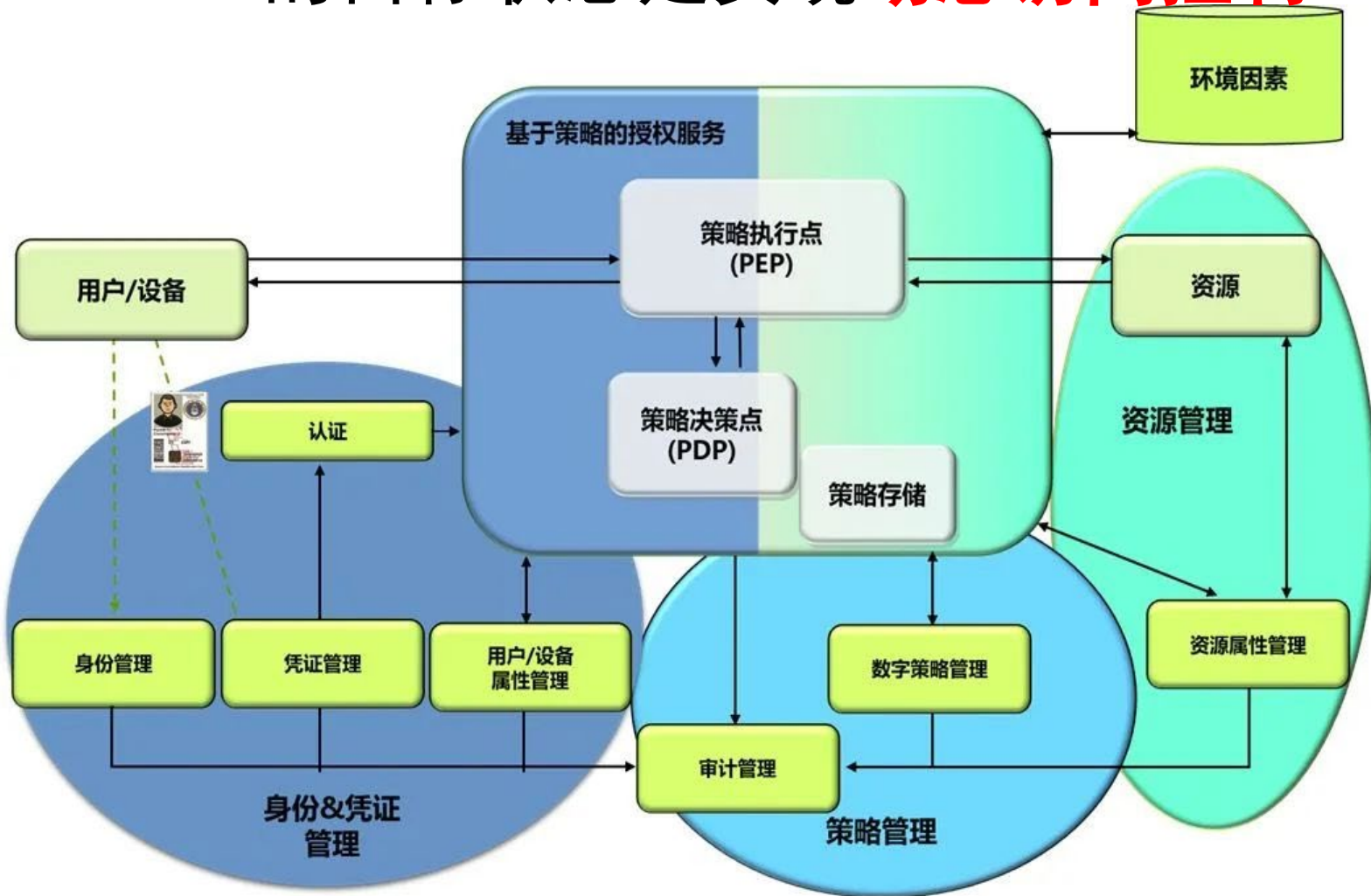


美国国防信息系统局技术路线图

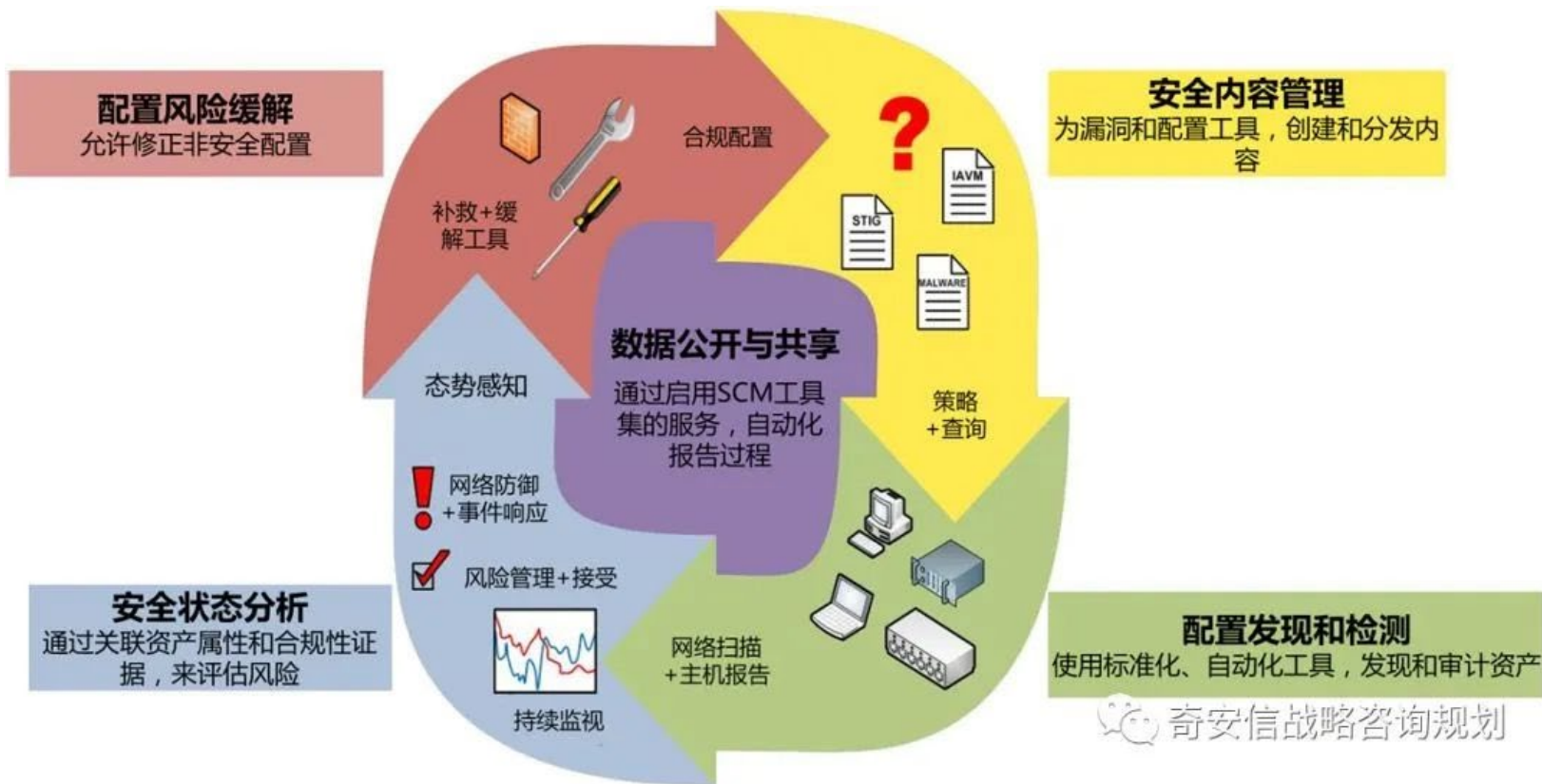


身份和访问管理 (IdAM)

- IdAM的目标状态是实现**动态访问控制**



美DoD的安全配置管理SCM



零信任与VPN

新冠终结VPN？打造零信任网络的五个步骤

安全牛 2020-03-17

[点击蓝字关注我们](#)





零信任实践

■ 应用场景

- **场景1：员工访问公司资源。** 员工希望从任何工作地点轻松、安全地访问公司资源。此场景将演示一种特定的用户体验，其中员工尝试使用企业管理的设备访问企业服务，如企业内部网、考勤系统和其他人力资源系统。该资源的相关访问请求将由本项目中实现的ZTA解决方案动态和实时地提供





零信任实践

■ 应用场景

- **场景2：员工访问互联网资源。** 员工正在尝试访问公共internet以完成某些任务。此场景将演示一种特定的用户体验，其中员工尝试使用企业管理的设备在internet上访问基于web的服务。虽然基于web的服务不是由企业拥有和管理的，但是该项目中实现的ZTA解决方案仍然会动态和实时地提供对该资源的相关访问请求。该解决方案将允许员工在任何位置访问，也就是说，员工可以使用企业管理设备在企业内部网、分支办公室或公共互联网内连接时访问互联网



零信任实践

■ 应用场景

- **场景3：承包商访问公司和互联网资源。** 承包商试图访问某些公司资源和互联网。此场景将演示一个特定的用户体验，其中受雇提供特定服务的承包商，试图访问某些公司资源和internet以执行组织的计划服务。公司资源可以是本地或云中的，承包商将能够在本地或从公共互联网访问公司资源。承包商试图访问的资源的相关网络访问请求，将由本项目中实施的ZTA解决方案动态和实时地提供。





零信任实践

■ 应用场景

- **场景4：企业内的服务器间通信。**企业服务通常有不同的服务器相互通信。例如，web服务器与应用服务器通信。应用服务器与数据库通信以将数据检索回web服务器。此场景将演示企业内服务器间交互的示例，其中包括场内、云中或在本地和云中服务器之间的服务器。本项目中实施的ZTA解决方案，将动态和实时地提供相互交互的指定服务器之间的关联网络通信。





零信任实践

■ 应用场景

- **场景5：与业务伙伴的跨企业协作。**两个企业可以在资源共享的项目上协作。在这种情况下，本项目中实现的ZTA解决方案将使一个企业的用户能够安全地访问另一个企业的特定资源，反之亦然。例如，企业A用户将能够从企业B访问特定的应用程序，而企业B用户将能够从企业A访问特定的数据库。





零信任实践

■ 应用场景

- **场景6：利用公司资源建立信心水平。** 企业有监控系统、安全信息和事件管理（SIEM）系统以及其他资源，这些资源可以向策略引擎提供数据，从而为访问企业资源创建更细粒度的信任级别，并促进基于信任级别的严格访问。在这种情况下，ZTA解决方案将这些监控和SIEM系统与策略引擎集成，以生成更精确的置信水平计算。





零信任实践

对于考虑采用零信任安全模型的组织，以下是一些有助于确保成功的最佳实践：

选择架构或技术之前，请确保您具有正确的策略。零信任是以数据为中心的，因此，重要的是考虑数据的位置，需要访问的人以及可以使用哪种方法来保护数据。Forrester 建议将数据分为三类-公开，内部和机密-每个“数据块”都应当有自己的微边界。

从小处着手以获得经验。为企业实施零信任架构的规模和范围可能是巨大的。例如，谷歌花了七年时间才完成BeyondCorp项目的实施。

考虑用户体验。零信任框架不必也不应该破坏员工的正常工作流程/体验，即使他们（及其设备）正受到访问权限验证的审查。零信任的部分认证和授权流程应当尽量“透明化”，在用户根本觉察不到的后台进行。

对用户和设备身份验证实施强有力的措施。零信任的根基是，在没有验证获得完全授权之前，没有任何人或任何设备可以信赖。因此，基于强身份、严格的身份验证和非永久权限的企业范围的IAM系统是零信任框架的关键构建块。

将零信任框架纳入数字化转型项目。为零信任网络重新设计工作流程时，还可以借此机会完成企业安全模型的转型。





零信任实践

■ 五个步骤

建立零信任框架并不一定意味着一整套的技术转型。企业可以采用循序渐进的方法，以受控的迭代方式进行，从而帮助确保最佳结果，同时对用户和操作的干扰降到最低。

1 定义保护面

零信任体系中，你的关注重点不是攻击面而是保护面。所谓保护面就是对公司最有价值的关键数据、应用程序、资产和服务（DAAS）。保护面的实例包括信用卡信息、受保护的健康信息（PHI）、个人身份信息（PII）、知识产权（IP）、应用程序（现成的或定制的软件）、SCADA控件、销售点终端、医疗设备、制造资产和IoT设备等资产以及DNS、DHCP和Active Directory等服务。

定义保护面后，你可以实施紧密的控制，使用简洁、精确和可理解的策略声明来创建一个微边界（或分隔的微边界）。





零信任实践

■ 五个步骤

2 映射交易流

流量在网络中的移动方式决定了其保护方式。因此，您需要获得有关DAAS相互依赖关系的上下文信息。记录特定资源的交互方式可以帮你确定合适的安全控制并提供有价值的上下文，以确保在提供最佳网络安全防护的同时，对用户和业务运营的干扰降到最低。

3 构建零信任IT网络架构

零信任度网络是完全自定义的，并没有唯一的标准和设计参考。总的原则是，零信任体系架构应当围绕保护面（资产、数据、应用和服务等）构建。一旦定义了保护面并根据业务需求映射了业务流程，就可以从下一代防火墙开始设计零信任架构。下一代防火墙可以充当分段网关，在保护面周围创建一个微边界。使用分段网关，您可以强制执行附加的检查和访问控制层，一直延伸到第7层，管控任何尝试访问保护面内部资源的访问。





零信任实践

■ 五个步骤

4 创建零信任安全策略

完成零信任网络架构的构建后，你将需要创建零信任策略来确定访问规则，你需要知道您的用户是谁，他们需要访问哪些应用程序，为什么他们需要访问，他们倾向于如何连接到这些应用程序，以及可以使用哪些控件来保护该访问。

通过实施这种精细粒度的策略，可以确保仅允许合法应用或者流量的进行通讯。

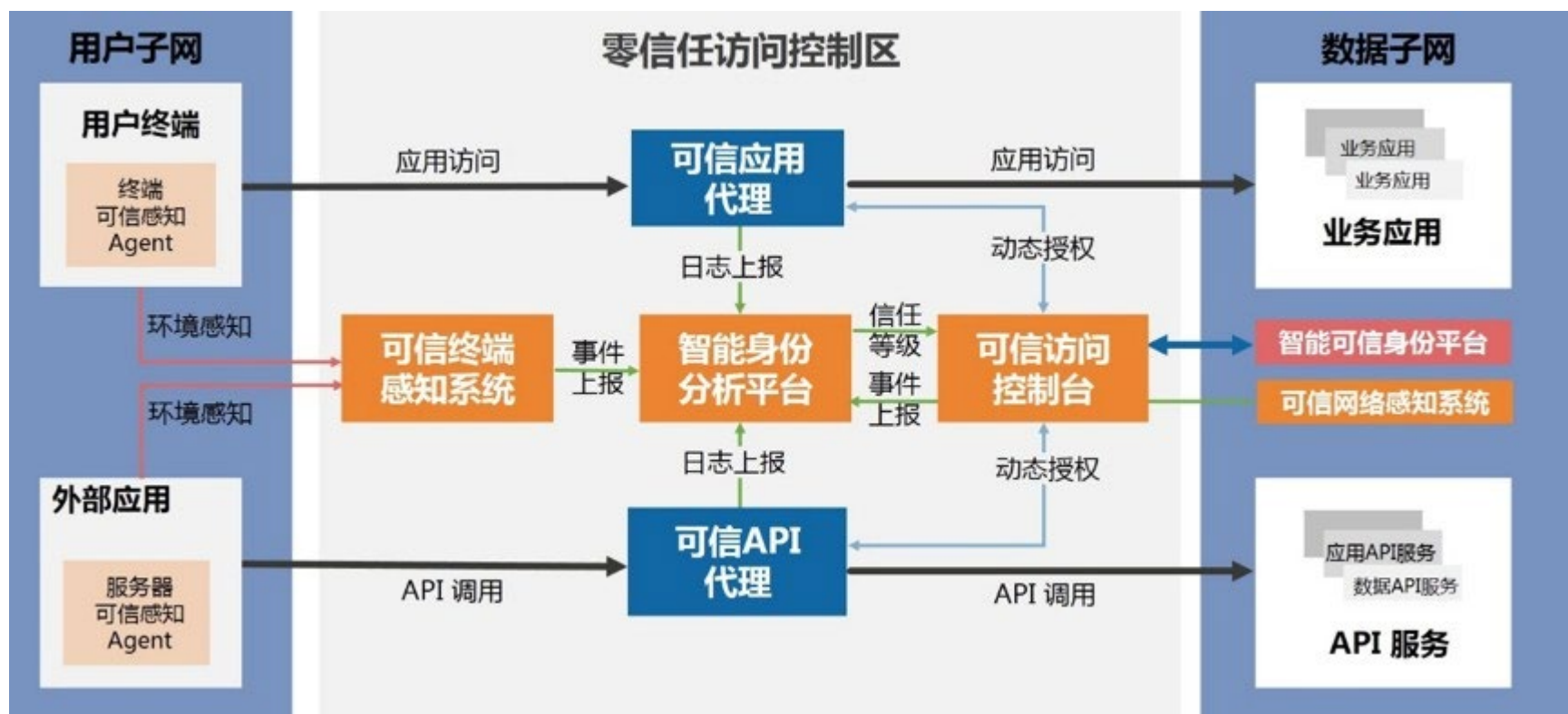
5 监控和维护零信任网络

这最后一步包括检查内部和外部的所有日志，侧重于零信任的运维方面。由于零信任是一个反复迭代的过程，因此检查和记录所有流量将提供宝贵的见解，以了解如何随着时间的推移持续改进零信任网络。



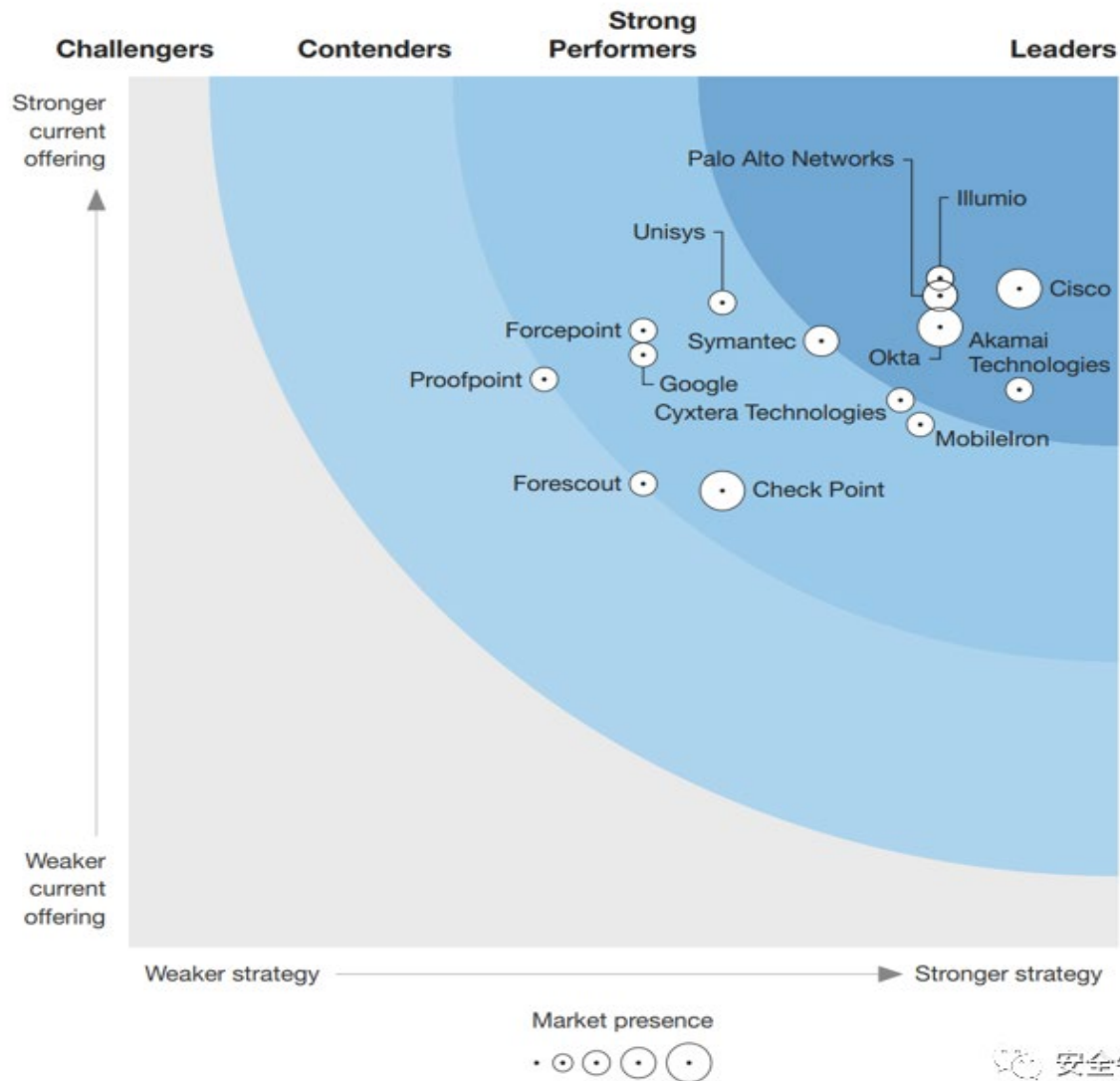
零信任实践

■ 典型场景



零信任厂商

Forrester 2019年
四季度市场报告





零信任厂商

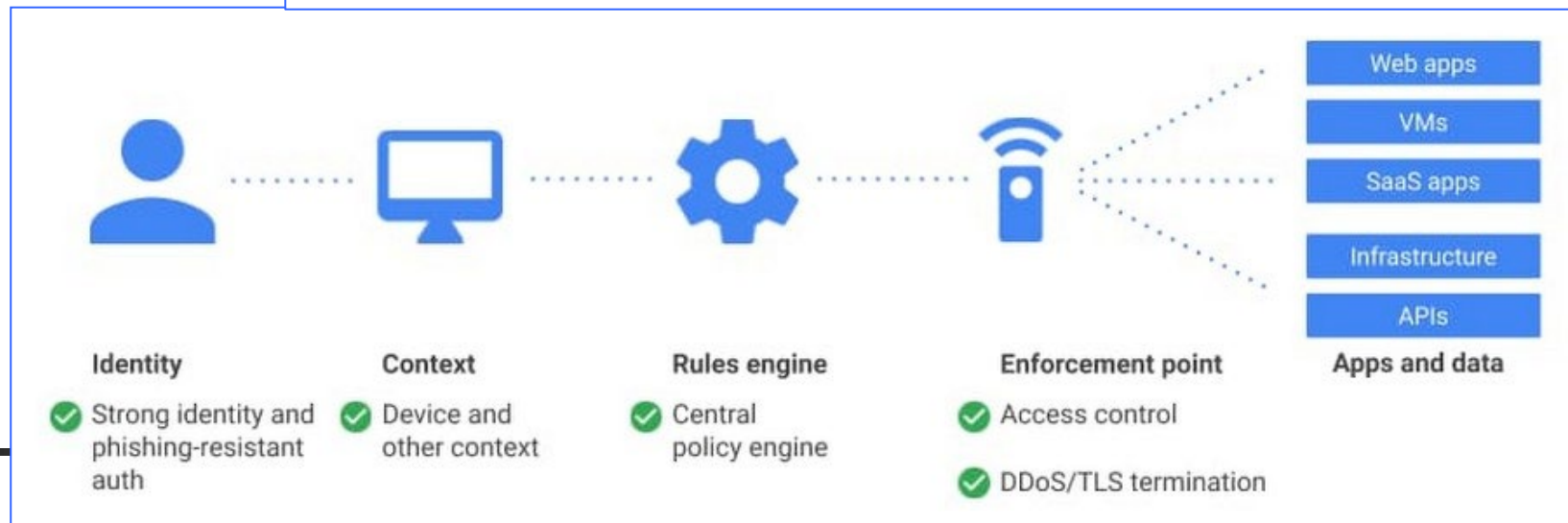
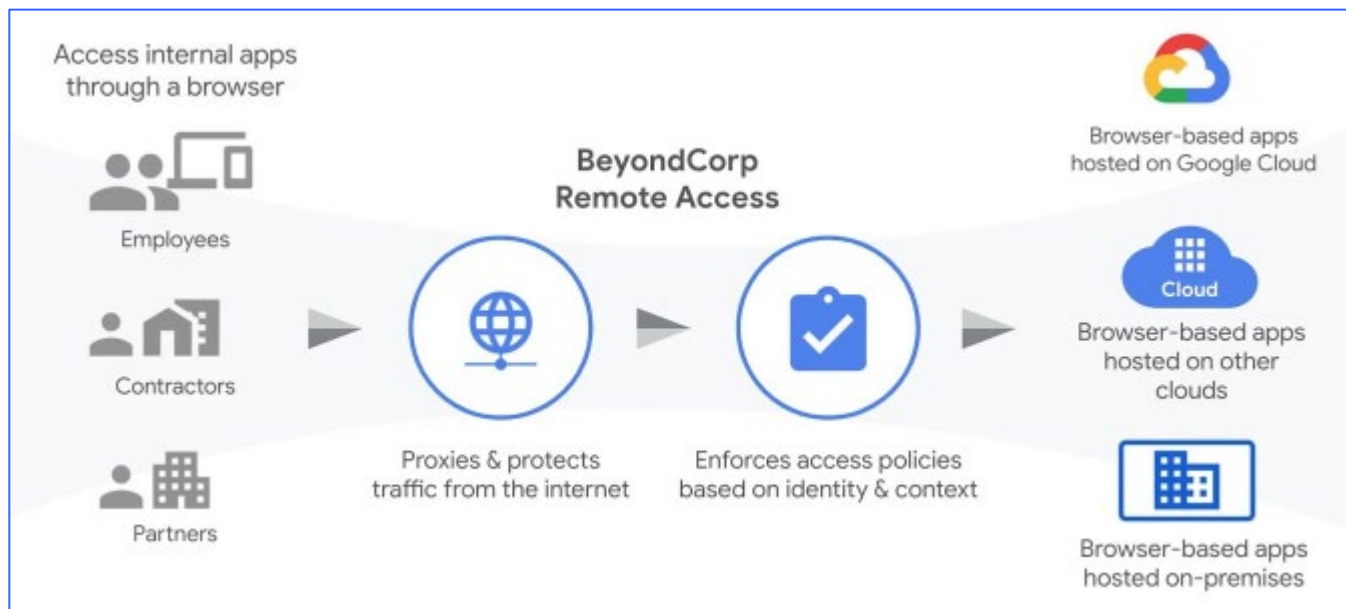
Table 1. Representative Vendors of ZTNA as a Service

Vendor	Product or Service Name
Akamai	Enterprise Application Access
Cato Networks	Cato Cloud
Cisco	Duo Beyond (acquisition by Cisco)
CloudDeep Technology (China only)	DeepCloud SDP
Cloudflare	Cloudflare Access
InstaSafe	Secure Access
Meta Networks	Network as a Service Platform
New Edge	Secure Application Network
Okta	Okta Identity Cloud (Acquired ScaleFT)
Perimeter 81	Software Defined Perimeter
SAIFE	Continuum
Symantec	Luminate Secure Access Cloud (acquisition by Symantec)
Verizon	Vidder Precision Access (acquisition)
Zscaler	Private Access
Source: Gartner (April 2019)	

2020奇安信-Gartner
零信任白皮书

零信任厂商

经过近十年的内部实践，2020年4月Google的BeyondCorp终于正式对外开放使用





零信任架构部署小结

- 短期来看，企业部署零信任架构面临的困难依然较多，特别是在已有的网络中实现零信任
 - 建立8种数据源并非易事
 - 对企业业务的深度了解
 - 管理成本和建设成本较高





内容提纲

1

SDN安全

2

零信任安全

3

移动目标防御

4

网络空间拟态防御





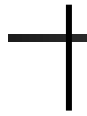
问题分析

- 网络系统的静态性、确定性和同构性，使得在网络攻防博弈中攻击者往往是优势的一方，网络安全存在“易攻难守”的局面





问题分析

- 这种被动劣势无法依靠现有防御方法来弥补，主要表现在以下4个方面：
 - 由于人的认知有限性，常用的代码检查机制或漏洞挖掘方法难以保证发现、排除所有的漏洞或者后门
 - 补丁下发通常明显滞后于攻击者对安全漏洞的利用，这一时间差为网络攻击提供了生存空间
 - 攻击特征不断地在快速变化
 - 未知攻击检测还没有有效解决方案
- 

- 移动目标防御（Moving Target Defense, MTD）
 - 2010年5月，美国网络与信息技术研发计划（NITRD）发布了《网络安全游戏规则的研究与发展建议》，2011年12月美国国家科学技术委员会（NSTC）发布了《可信网络空间：联邦网络空间安全研发战略规划》
 - 含义：移动目标是可在多个维度上移动降低攻击优势并增加弹性的系统
-

- 移动目标防御（Moving Target Defense, MTD）
 - 移动目标防御则是指防御者从多个系统维度持续地变换系统中的各种属性，从而增加攻击者的不确定性、复杂性和不可预测性，减小攻击者的机会窗口，并增加攻击者探测和攻击的成本





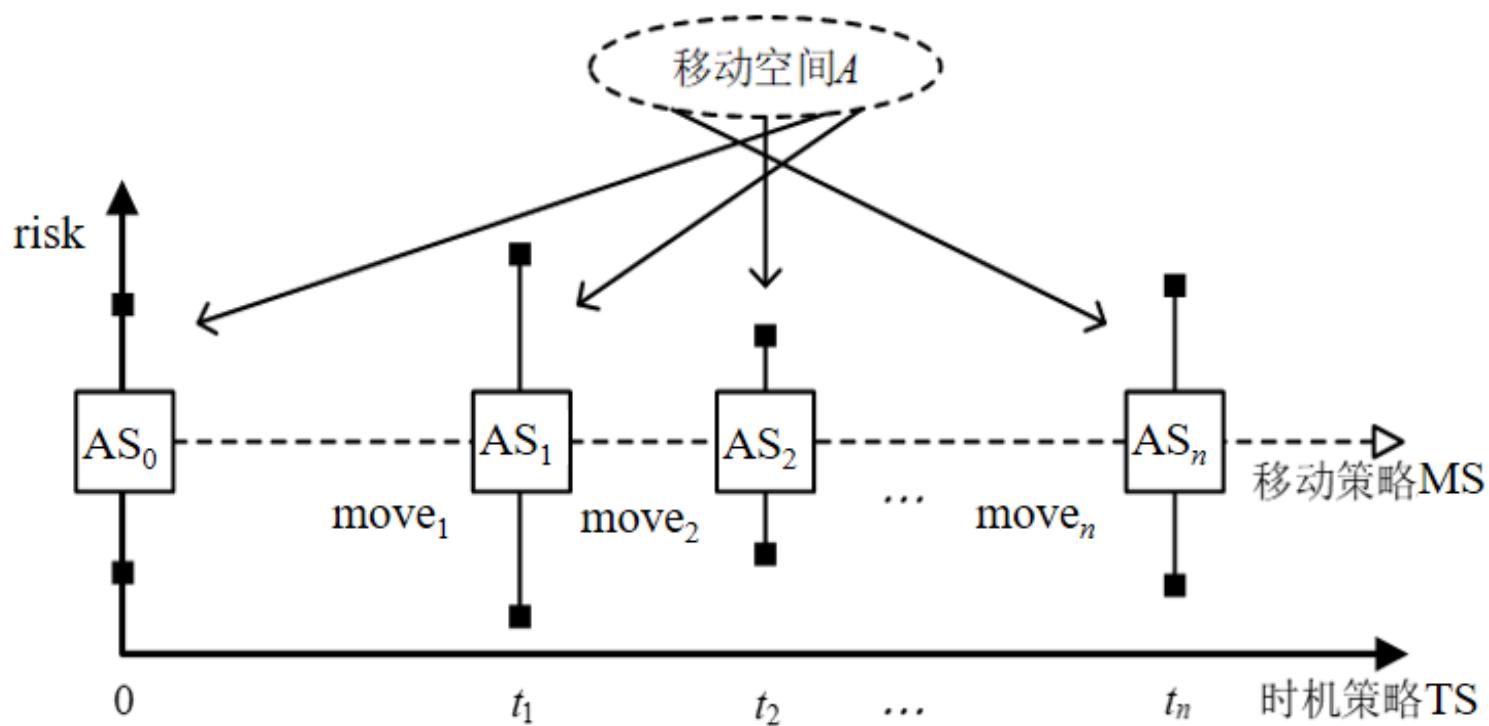
MTD攻击面

- 移动目标防御（Moving Target Defense, MTD）
 - 除了移动目标和移动目标防御外，MTD还涉及另外两个重要概念：**攻击面**（Attack Surface, AS）**和攻击面变换**（Attack Surface Shifting, ASS）



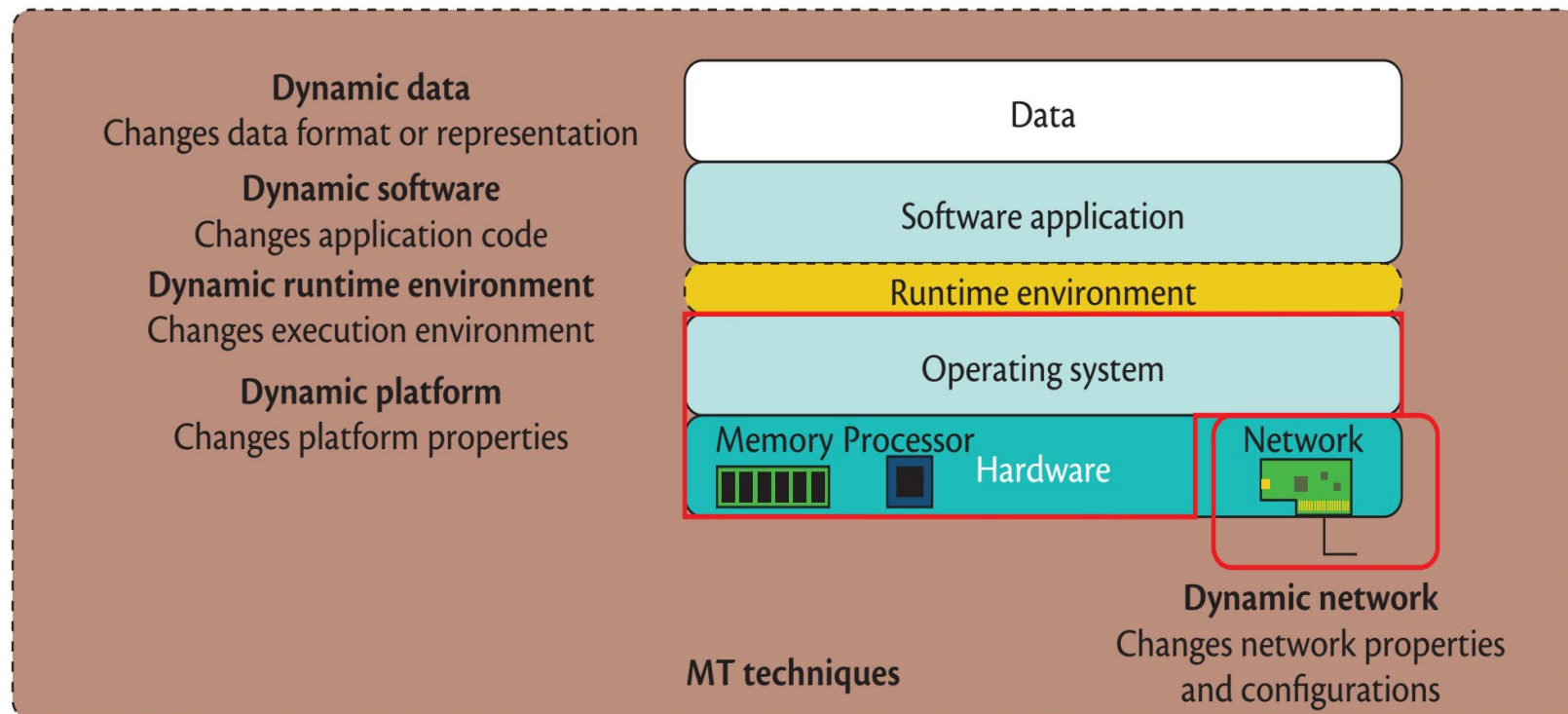
MTD攻击面

■ 攻击面变换



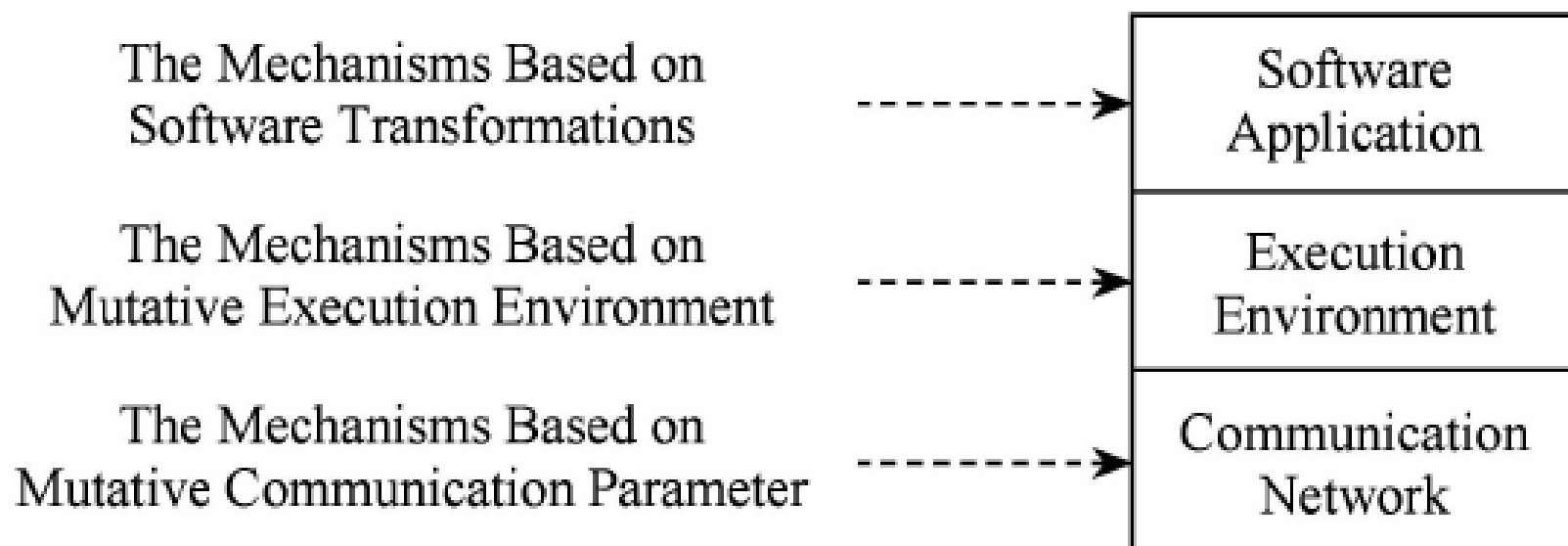
MTD关键技术

■ Lincoln实验室



移动目标防御技术研究进展

蔡桂林^{1,2} 王宝生¹ 王天佐¹ 罗跃斌¹ 王小峰¹ 崔新武²



CCS 2014 MTD Workshop

Pre-Conference Workshops (November 3, 2014)

Workshop Chairs

Cliff Wang
Army Research Office, USA



Dijiang Huang
Arizona State University, USA



You may contact the chairs at: ccs14workshopchairs@googlegroups.com

• Moving Target Defense (MTD)

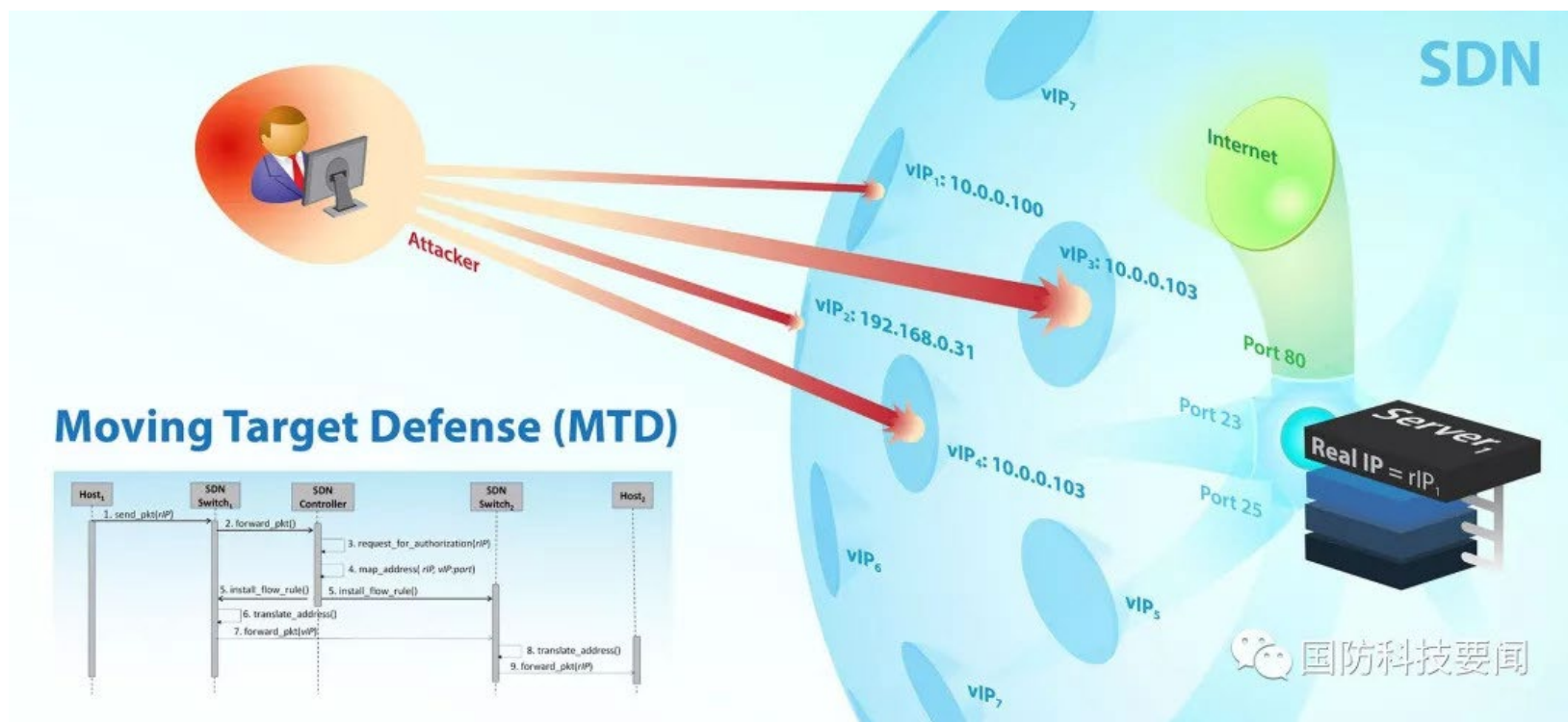
The static nature of current computing systems has made them easy to attack and harder to defend. Adversaries have an asymmetric advantage in that they have the time to study a system, identify its vulnerabilities, and choose the time and place of attack to gain the maximum benefit. The idea of moving-target defense (MTD) is to impose the same asymmetric disadvantage on the attacker by making systems dynamic and harder to predict. This workshop will bring together researchers from academia, government, and industry to report on the latest research efforts on moving-target defense, and to have productive discussion and constructive debate on this topic.

基于SDN的MTD

美陆军研究实验室开发移动目标防御技术

2018-09-12 20:00

作者：张彩 来源：国防科技要闻



国防科技要闻



基于SDN的MTD

美陆军研究实验室开发移动目标防御技术

2018-09-12 20:00

作者：张彩 来源：国防科技要闻

基于“软件定义网络”的MTD

主动防御手段需要不断改变IP地址，因此部署主动防御和安全系统会产生一定的成本。研究人员通过利用“软件定义网络”的技术，使计算机在保持真实IP地址不变的情况下，通过频繁改变虚拟IP地址将真实地址与网络隔离，可以在一定程度上降低成本。“软件定义网络”技术通过将网络中的各个设备的网络控制转移到集中控制器上，提供对网络策略的动态管理。SDN控制器可定义网络配置，在可变条件下使网络操作更可靠、反应更迅速。

由于目标系统的IP地址一直在改变，所以为了发现目标系统的漏洞，黑客必须花费时间、计算能力等更多的资源。据韩国光州科学技术研究所的Hyuk Lim教授介绍，这种主动防御手段可在攻击者进入目标系统之前采取防御措施。

基于SDN的MTD

《北京交通大学》 2018年

通过基于软件定义的网络（SDN）的移动目标防御（MTD）机制保护云数据中心网络

Gelato, Tadele Degefa

【摘要】：云计算作为一种新技术，其在过去十年中经历了十分快速且显著的发展，现在已经关系到了每个人的生活。在云计算的研究过程中，研究人员们提出了许多有关云计算的新的概念，比如“多租户”，这是网络中按需访问的一个可配置计算资源的共享池，它可以以最少的管理工作和更低的成本来快速提供和发布资源，这也使许多公司和组织将其传统的数据中心迁移到云中。此外，由于云计算具有诸多突出的特性，比如允许多用户间共享和外包资源的虚拟化，可扩展性，灵活性，敏捷性以及通过优化高效的计算以降低运营复杂性等，这同样也吸引了许多组织将其数据从传统数据中心转移到云中，依靠它来解决多个用户的访问需求，并且提高了资源利用率以适应快速变化的业务需求。然而，在传统数据中心迁移到云的过程中，我们会遇到各种安全问题，这些问题随着最新引入的云计算的概念也得到了升级，并且会导致确保云数据中心网络的安全变得更加困难。事实上，由于云本身的大规模性，直接访问云基础架构的移动设备的出现，以及个人和组织数据会实时添加到云等特性，它们都会进一步扩大云的漏洞，使服务可靠性，可用性和性能更容易受到敌手恶意活动的影响。此外，还存在一系列其他的问题，包括当前网络配置的静态性质、云操作与底层转发基础结构的紧密耦合，以及作为主要通信媒介的网络依赖关系等。而对于云的访问机制，当前也缺乏一种协调和弹性的防御机制。这些问题也进一步加剧了云计算会面临的安全风险，使云更容易被伪装为合法用户的敌手访问。为了解决这些安全问题，研究人员进行了广泛的研究工作，并且提出了许多不同的防御技术和解决方案，包括内置安全功能的新型硬件，高安全性的网络协议，防火墙，入侵检测系统（IDS）和入侵防御系统（IPS），以及昂贵的恶意软件检测工具，如防病毒程序和渗透测试工具。虽然多年来这些防御方法在复杂性和规模上都有显著的增长，但攻击者仍然能够有效地突破基于检测的安全防御措施，从而给出极具价值的且不对称的时间来执行目标系统的探查工作，以此来研究并确定云数据中心网络中的潜在漏洞。SDN的发明使得人们能够通过(?)转发设备的功能(即数据平面)与控制平面分离，以实现动态和灵活的数据中心网络。而为建立动态且主动的安全防御机制，研究人员提出了(?)云计算安全保护机制转变的新的创新方法。基于这种全新的SDN方法，研究人员提出一种新型博弈转换安全防御方法，我们称之为基于SDN的MTD。基于SDN的MTD机制对云计算数据中心网络可利用的方面进行了一些优化调整，



内容提纲

1

SDN安全

2

零信任安全

3

移动目标防御

4

网络空间拟态防御





第1卷 第4期
2016年10月

信息安全学报
Journal of Cyber Security

Vol. 1 No. 4
Oct., 2016

网络空间拟态防御研究

邬江兴

国家数字交换系统工程技术研究中心 郑州 中国 450001

摘要 本文扼要分析了网络安全不平衡现状及本源问题,重点阐述了动态异构冗余架构以及如何利用不可信软硬件构件组成高可靠、高安全等级信息系统的原理与方法,概略的给出了拟态防御的基本概念。最后,介绍了拟态防御原理验证系统的测试评估情况和初步结论。



网络空间拟态防御

- 网络空间拟态防御（Cyber Mimic Defense, CMD）是由中国工程院院士邬江兴团队提出的一种主动防御理论，主要用于应对网络空间中不同领域相关应用层次上基于未知漏洞、后门、病毒或木马等未知威胁。
- 借鉴生物界基于拟态现象（Mimic Phenomenon, MP）的伪装防御原理，在可靠性领域非相似余度（dissimilar redundancy）架构基础上导入多维动态重构机制



CDM原理

■ 两个公理

- **公理1**：“给定功能和性能条件下，往往存在多种实现算法”
- **公理2**：“人人都存在这样或那样的缺点，但极少出现在独立完成同样任务时，多数人在同一个地方、同一时间、犯完全一样错误的情形”





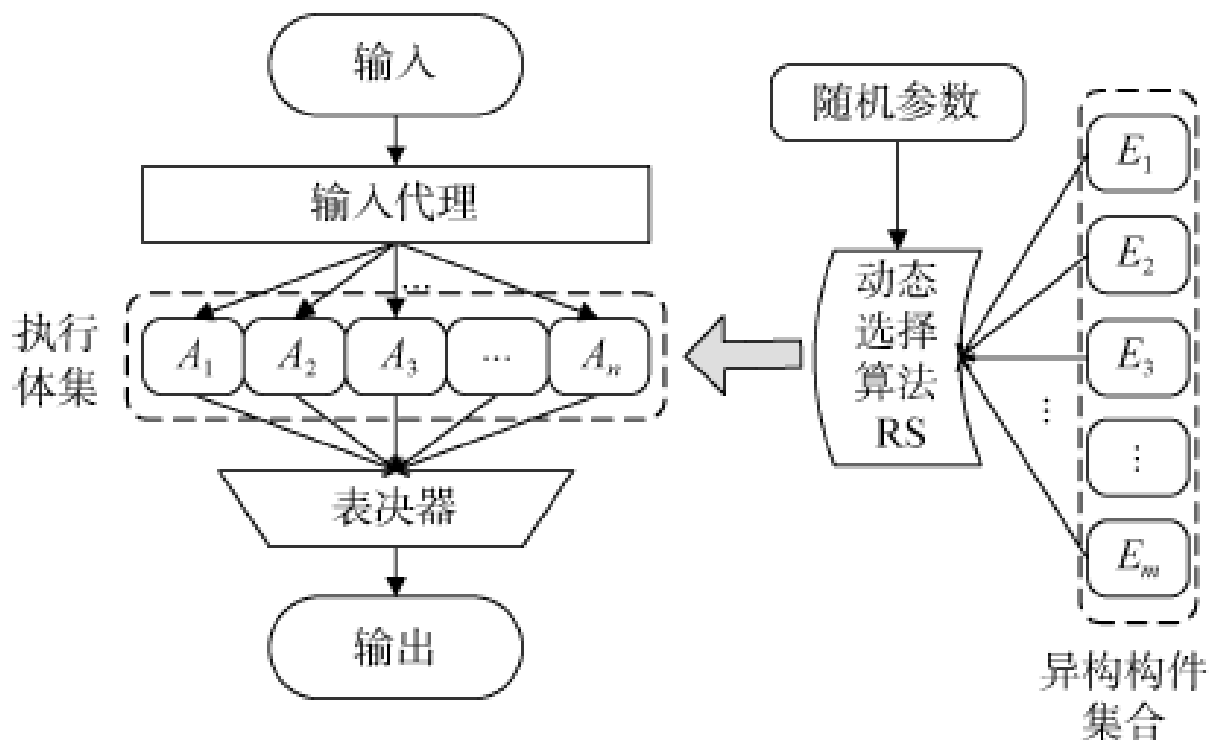
CDM原理

- 基于公理，CMD通过**异构性、多样或多元性**改变目标系统的相似性、单一性，以动态性、随机性改变目标系统的静态性、确定性，以**异构冗余多模裁决机制**识别和屏蔽未知缺陷与未明威胁，以**高可靠性架构**增强目标系统服务功能的柔韧性或弹性，以**系统的可视不确定**属性防御或拒止针对目标系统的不确定性威胁



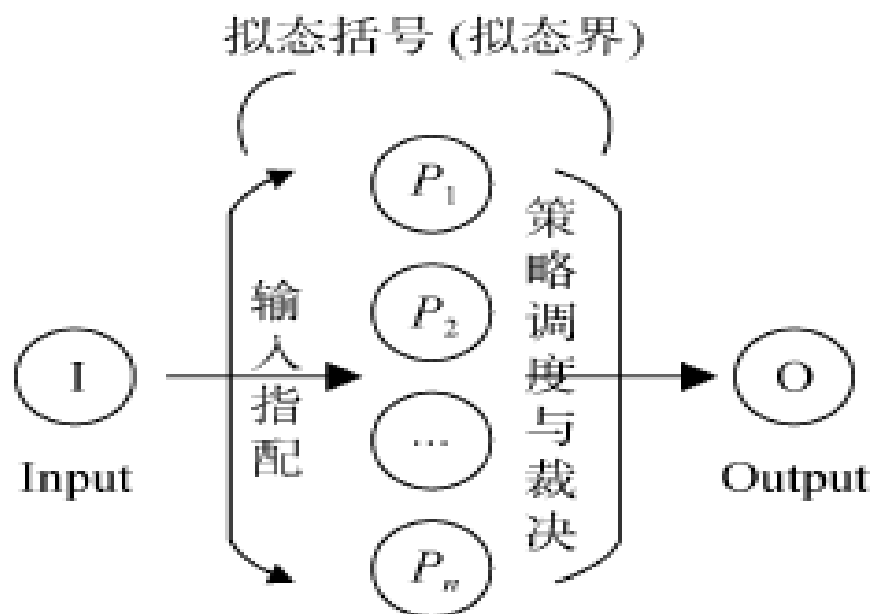
CDM的DHR架构

- CMD给出的原理性方法：动态异构冗余（Dynamic Heterogeneous Redundancy, DHR）架构



CDM的DHR架构

- CMD给出的原理性方法：动态异构冗余（Dynamic Heterogeneous Redundancy, DHR）架构



拟态界外的安全问题不属于拟态防御的范围



CMD安全等级

- 拟态防御的三个等级：
 - 完全屏蔽级
 - 不可维持级
 - 难以重现级



拟态防御理论与技术要点

拟态防御理论与技术要点(8122)



2019 西湖论剑·网络安全大会
2019 WEST LAKE CYBERSECURITY CONFERENCE

- ◆ 针对一个前提：防范未知漏洞后门等不确定威胁
- ◆ 基于一个公理：相对正确公理
- ◆ 依据一个发现：熵不减系统能稳定抵抗未知攻击
- ◆ 借鉴二种理论：可靠性理论与自动控制理论
- ◆ 发明一种构造：动态异构冗余构造（IT领域创新使能技术）
- ◆ 导入一类机制：拟态伪装机制
- ◆ 形成一个效应：测不准效应
- ◆ 获得一类功能：内生安全功能
- ◆ 达到一种效果：融合现有安全技术可指数量级提升防御增益
- ◆ 实现二个目标：归一化处理传统/非传统安全问题---- 获得广义鲁棒控制属性

在不依赖攻击者先验知识和行为特征信息情况下

将网络空间不确定安全威胁问题

归一化为可靠性与鲁棒控制理论和技术能够解决的问题

2019 西湖论剑·网络安全大会

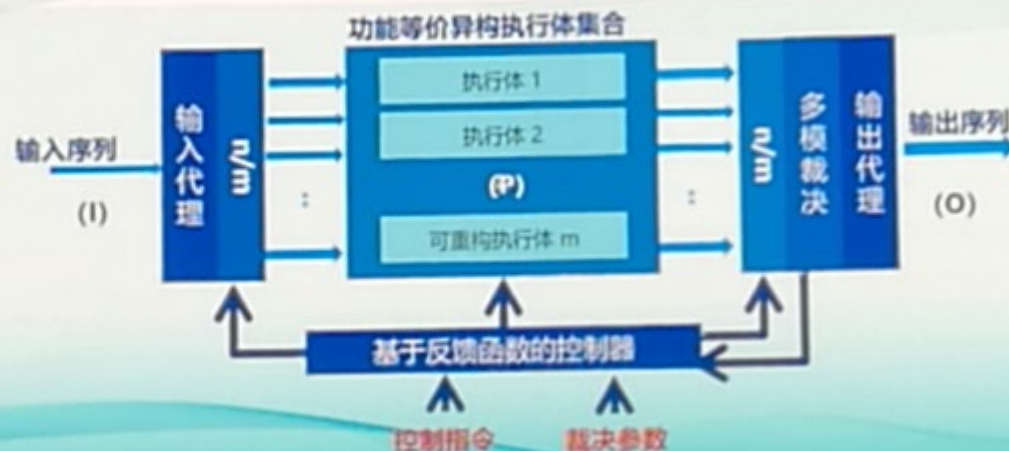
拟态防御理论与技术要点

拟态防御理论要点(8122)

发明一种构造：
动态异构冗余构造

导入一类机制：
拟态伪装机制

获得一种构造性功能：
内生安全功能



指数量级的提升了攻击门槛

任何利用个性化漏洞后门等攻击在机理上无效

任何试错或盲攻击都将导致当前防御场景改变

任何协同攻击即使成功也很难稳定维持和重复再现

拟态防御理论与技术要点

可量化设计、可验证度量的安全性能

- 差模漏洞后门的可利用概率
- 共模漏洞后门的可利用概率
- 控制环路漏洞的可利用概率
- 拟态构造功能的可靠性概率
- 拟态构造功能的可用性概率
- 拟态构造服务的可信性概率

借助可靠性验证理论和注入测试方法可定量检定

全球迄今尚没有一种ICT/CPS/IT产品

可以用“**白盒实验**”进行安全性测试与度量

颠覆基于目标对象软硬件漏洞后门等暗功能的攻击理论和方法

抵消技术和市场先行者在网安领域的战略优势

改变网络空间游戏规则

2019 西湖论剑·网络安全大会

拟态设备

系列化产品样机—已完成，体系化的现网示范应用已完成



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY EXPERIENCE



路由交换系统



Web服务器系统



防火墙/网关



域名服务系统



工业控制处理机



文件存储系统

工信部试点部署 (2018.1~)



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY EXPERIENCE

景安网络 拟态
路由器

景安网络 Cert中心 拟态
web服务

拟态
防御

河南联通 拟态
景安网络 域名服务


景安网络 拟态
防火墙

2018年1月 起，全球首次线上部署系列化的拟态构造设备

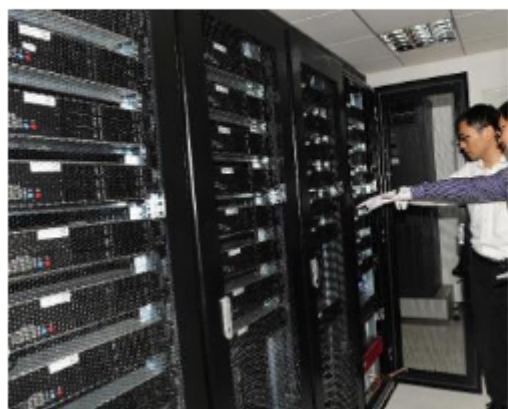
体系化的提供具有内生安全属性的可信的网络服务功能

2019 西湖论剑·网络安全大会

拟态计算机

拟态计算机  编辑词条

 添加义项 |  同义词 |  收藏 |  分享



拟态计算机堪称“变形金刚”。目前所用一般的计算机“结构固定不变、靠软件编程计算”，而拟态计算机的结构动态可变，“靠变结构、软硬件结合计算”。针对用户不同的应用需求，拟态计算机可通过改变自身结构**提高效能**。测试表明，拟态计算机典型应用的能效，比一般计算机可提升十几倍到上百倍，高效能特点显著。2013年9月，中国成功研制世界首台结构动态可变的拟态计算机。

2013年9月21日，这项名为“新概念高效能计算机体系结构及系统研究开发”项目，在上海通过了国家863计划项目验收专家组的验收，这是计算机发展史上的一条新道路，在不久的将来将会投入商业运用。相对于普通的计算机而言，拟态计算机的运行效能要高出几十甚至一百倍。拟态计算机的长处不在于单纯的速度，而是整体效能和效率的提高。



拟态路由器

拟态路由器是基于拟态防御机理研制的首款网络基础设施设备，可提供“高可靠、高可信、高可用”三位一体的广义鲁棒性服务，是支撑网络强国战略和构建安全可信基础设施的核心设备，是扭转网络基础设施易攻难守颓势的抓手级设备。

拟态架构的引入不影响路由器的基本功能和性能，能应对拟态界内未知漏洞后门病毒木马等不确定威胁，安全性由架构内生机制决定，不依赖其他防御手段，斩断攻击链各个环节，极大提高攻击难度和攻击代价，能自然融合其他防御技术，并获得超非线性防御效果。

拟态路由器



核心路由器



汇聚路由器



接入路由器

拟态 Web 服务器

软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2017, 28(4): 883-897 [doi: 10.13328/j.cnki.jos.005192]
©中国科学院软件研究所版权所有.

E-mail: jos@iscas.ac.cn
<http://www.jos.org.cn>
Tel: +86-10-62562563

拟态防御 Web 服务器设计与实现^{*}

全青¹, 张铮¹, 张为华², 鄢江兴³

¹(数学工程与先进计算国家重点实验室, 河南 郑州 450001)

²(复旦大学 并行处理研究所, 上海 201203)

³(国家数字交换系统工程技术研究中心, 河南 郑州 450002)

通讯作者: 张铮, E-mail: ponyzhang@126.com



摘 要: Web 服务器系统作为重要的服务承载和提供平台, 面临的安全问题日益严重. 已有的防御技术主要基于已知攻击方法或漏洞信息进行防御, 导致难以很好地应对未知攻击的威胁, 从而难以全面防护 Web 服务器系统的安全. 首先提出了攻击链模型, 对已有技术的问题和不足进行了深入的分析. 在此基础上, 提出了基于“动态异构冗余”结构的拟态防御模型, 并描述了拟态防御模型的防御原理和特点. 基于拟态防御模型构建了拟态防御 Web 服务器, 介绍了其架构, 分析了拟态原理在 Web 服务器上的实现. 安全性和性能测试结果显示, 拟态防御 Web 服务器能够在较小开销的前提下防御测试中的全部攻击类型. 说明拟态防御 Web 服务器能够有效地提升系统安全性, 验证了拟态防御技术的有效性和可行性. 最后讨论了拟态防御技术今后的研究前景和挑战.





拟态域名服务器

域名服务系统（DNS）是网络空间各类业务服务的“查号台”，用于实现网络域名到IP地址的翻译转换。域名服务是一种网络应用层资源的寻址服务，是其他网络应用服务的基础。攻击者可以基于域名协议及相关服务或防护系统的脆弱性，利用通信协议和软硬件的未知漏洞后门，通过篡改域名缓存数据或协议报文等技术手段实现域名劫持，冒名顶替包括政府、金融、公安、电子商务等网站在内的任何网站，实施虚假信息发布、木马病毒无感植入和机密数据窃取等恶意攻击。

拟态域名服务器以遏制域名解析服务漏洞后门的可利用性、建立内生安全防御机制、大幅提高攻击者的攻击难度和代价为出发点，可以在不改变现有域名协议和地址解析设施的基础上，通过拟态防御设备的增量部署，能够有效防御针对域名系统的域名投毒、域名劫持攻击等各种已知和未知域名攻击，能够提供安全可靠的域名解析服务。





拟态防火墙

防火墙是设置于网络关口的传统安全设备，为网络各类业务应用提供“安检准入”服务。防火墙是一种由软件和硬件设备组合而成的、部署在内部网与外部网之间、专用网与公共网之间的网络安全系统。防火墙是网络边界的第一道防线，也是众多网络安全产品中应用最为广泛的一种。通过部署防火墙产品，可以保护内部网免受非法用户的侵入，它能允许管理员“同意”的人和数据进入你的网络，同时将“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。防火墙对数据流进行过滤与控制时，其自身的协议栈或者支撑系统可能存在健壮性漏洞、未知漏洞、后门等有可能被高水平黑客利用，出现“防火墙不防火”的境况。

针对防火墙产品在web管理层面、数据流处理层面可能存在的漏洞后门，运用拟态防御技术，以动态异构冗余架构（DHR）为指导，对传统防火墙架构进行改造后，可以在管理、数据层面增加网络攻击者的攻击难度，有效防御“安检准入”中的内鬼侵扰，提供切实可信的准入控制保障。





MTD参考书

Jiangxing Wu

Cyberspace Mimic Defense

Generalized Robust Control and
Endogenous Security

 Springer



MTD与CMD

- 各方观点不一
- 局限性探讨





本章小结





进一步讨论

- 控制与数据平面分离思想的优缺点
 - SDN
 - 零信任
- 边界防护还有未来吗？
 - 边界在消失？
 - 无处不在的动态防御代表未来？
- 被动防护与主动防御





作业

