CAICT 中国信通院　中国通信标准化协会 China Communications Standards Association

SASE成熟度能力要求标准解读

陈锐豪
中国信通院云大所云计算部工程师

2021 可信云大会
2021 TRUSTED CLOUD SUMMIT
数字裂变 可信发展

目录

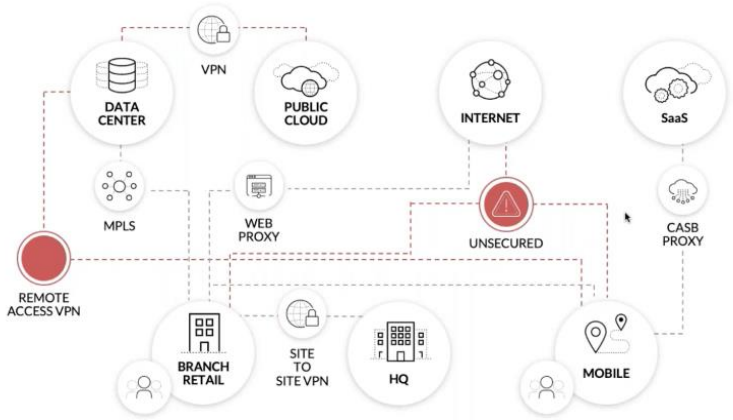
Part 1

什么是SASE

什么是SASE

企业需求发生变化

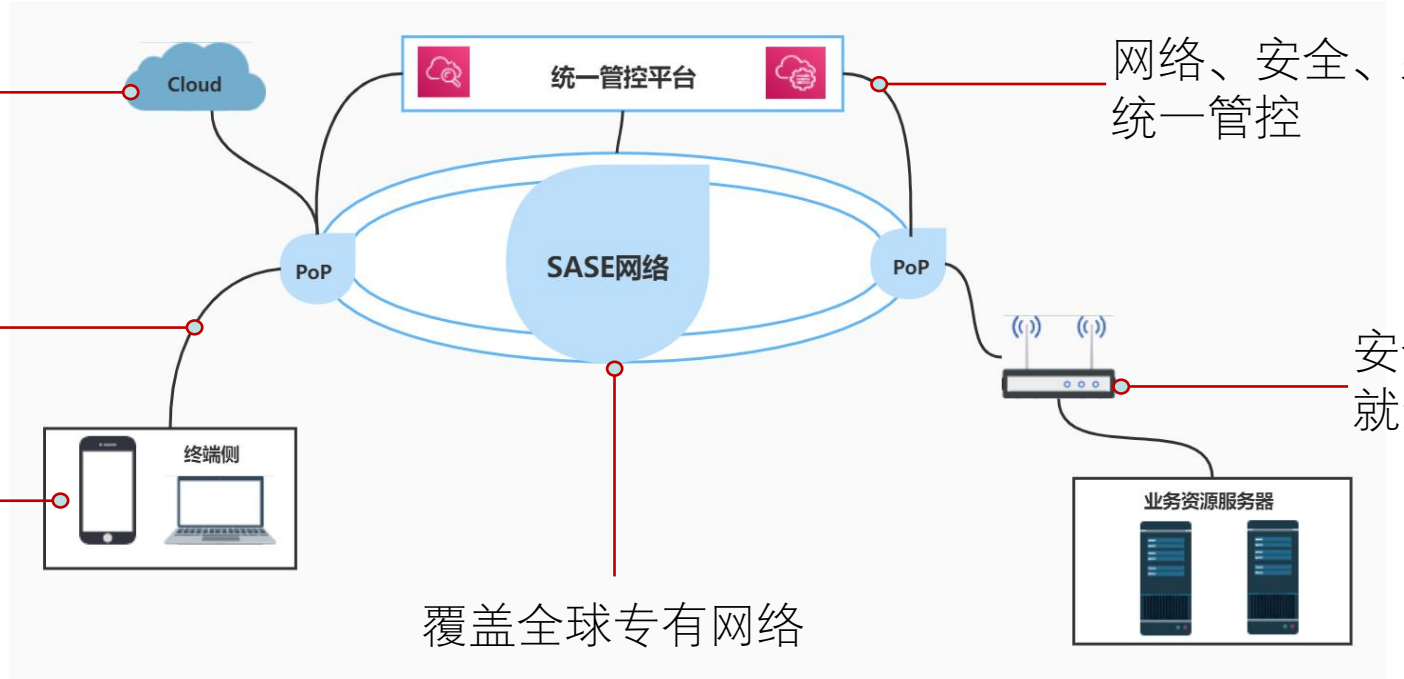
- 公有云流量增多：云平台应用，互联网流量增加；安全边界延伸
- 移动办公增多：移动端接入企业网络；移动就近响应；
- 分支功能增多：随着安全攻击与数据安全的重要性日益增加，分支包含多种安全防护能力。



技术理念不断革新

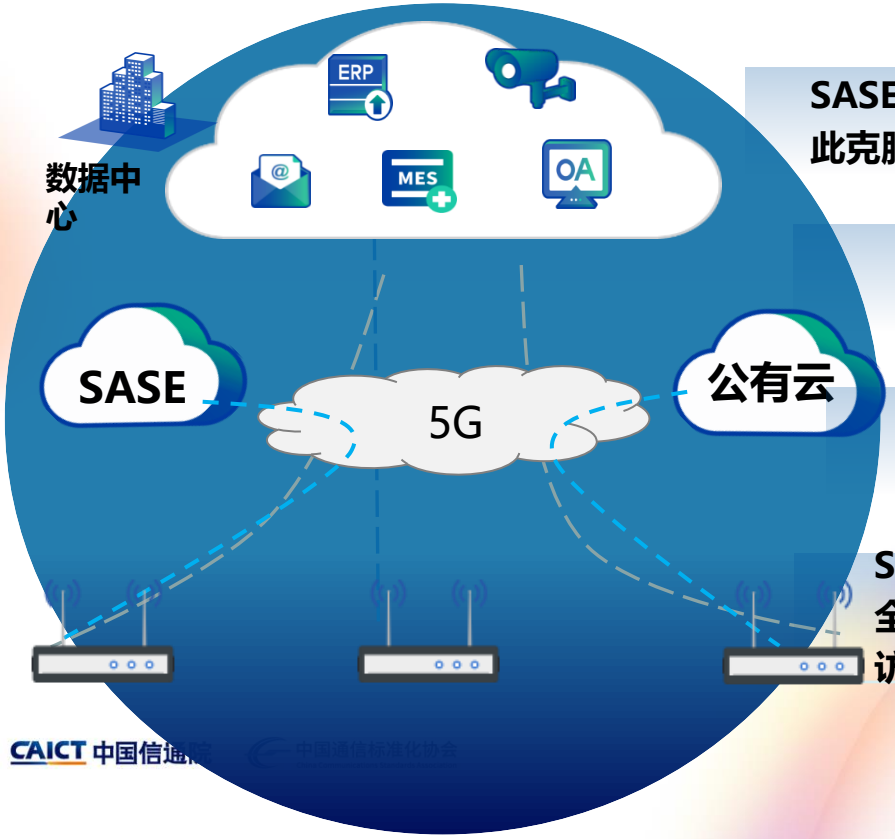
- SD-WAN功能不断完善：SD-WAN经过近年发展，从架构到技术已经趋于成熟。被大部分企业客户接受。
- 应用感知功能成熟：DPI等深度包解析技术成熟，用户对于业务的控制与感知需求从2-3层向4-7层上移。
- 安全理念革新：零信任安全、软件定义边界等新的安全理念逐渐被用户接受。

什么是SASE


多云的访问
Cloud
统一管控平台
网络、安全、身份、接入点
统一管控
PoP
SASE网络
PoP
安全的
就近接入
安全的
就近接入
企业终端
BYOD
外部人员
终端侧
业务资源服务器
覆盖全球专有网络

什么是SASE

SASE（Secure Access Service Edge），安全访问服务边缘，是一种Gartner模型，这种网络架构可将软件定义的广域网（SD-WAN）和安全性集成到云服务中，从而保证简化WAN部署、提高效率和安全性。



SASE包含了一个在自有服务专网上运行的网络连接服务，以此克服了连接过程中的的延迟问题

网络连接

SASE服务将使用没有特定硬件依赖关系的云原生架构，由软件定义和管理，不再依赖单一服务链

云原生架构

随着数据中心不再是网络中心，SASE将检查引擎带到附近的PoP点，更加符合边缘环境实际情况

分布式理念

SASE将广域网功能与全面的安全功能结合在一起，例如安全Web网关，云访问安全代理，防火墙即服务和零信任网络访问，以促进安全云和移动环境中的网络访问

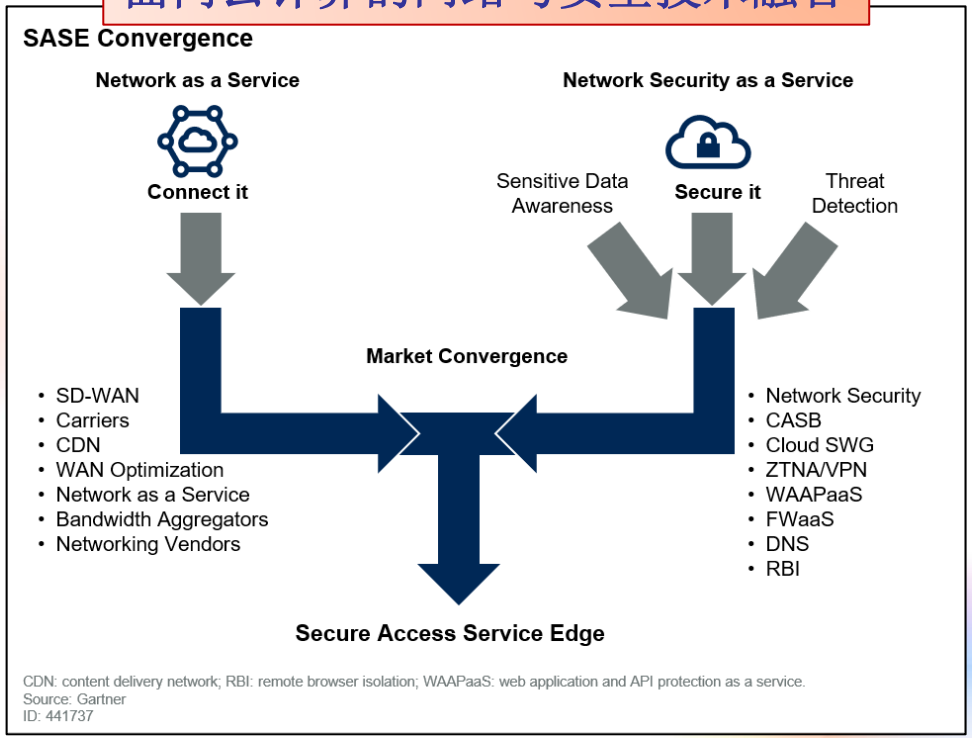
安全防护

Part 2

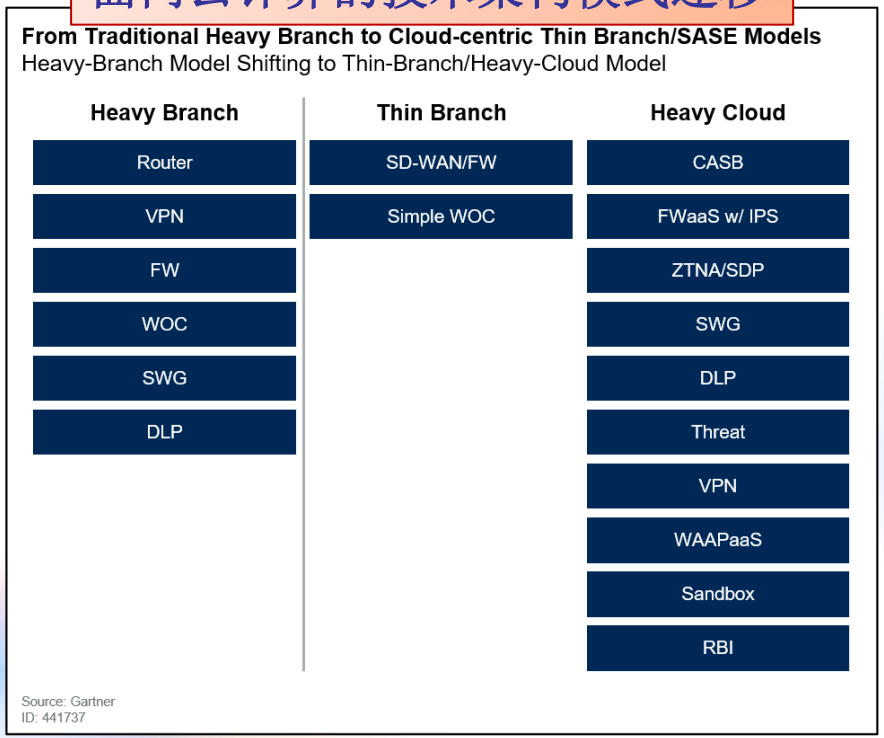
从技术特点看SASE

从技术特点看SASE

面向云计算的网络与安全技术融合



面向云计算的技术架构模式迁移



从技术特点看SASE

	传统安全	SASE安全
安全模型	重视边界安全	注重端到端的全链路安全性
身份管理	基于IP地址的身份管理	基于服务的身份管理
隔离粒度	独立操作系统	共享操作系统进程级隔离
威胁应对	被动	主动
漏洞修补方式	增量修补	重新部署全量修补

端到端全链路安全

- 端到端全链路安全涉及多段网络链路。
- 安全边界模糊，内网外网统一防护。

基于身份管理

- 所有访问控制基于身份执行。
- 一个身份登录IT架构内部所有资源。

分布式部署

- 依托POP点实现就近安全与网络响应。
- 实现多种云平台分布式部署。

Part 3

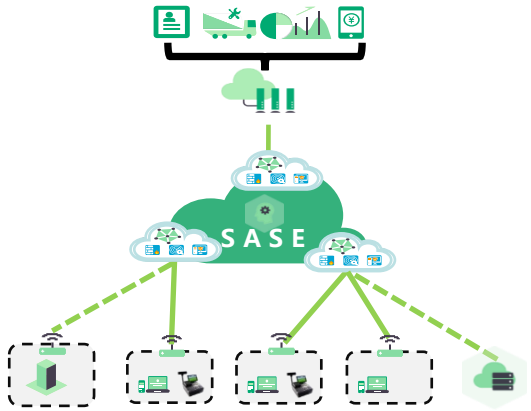
从应用场景看SASE

从应用场景看SASE

企业多分支机构远程访问

场景特点：多个分支机构分布在不同地理位置，存在大量访问私有机构资源需求。

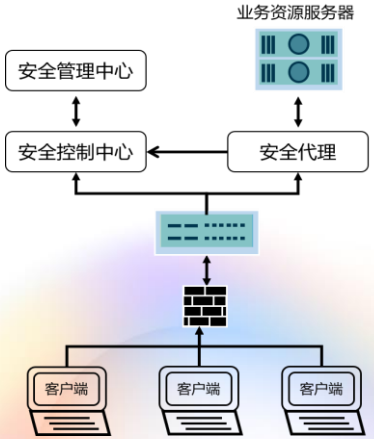
场景需求：
- ✓ 分支机构快速就近响应
- ✓ 私有资源访问限制
- ✓ 简化运维



第三方人员临时授权

场景特点：大量第三方人员接入需求。

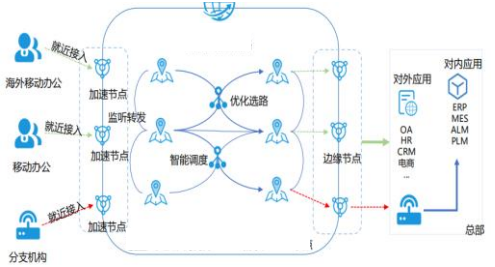
场景需求：
- ✓ 最小权限访问控制
- ✓ 动态身份评估



移动/居家办公

场景特点：不同移动终端移动接入，BYOD自带设备办公

场景需求：
- ✓ 就近接入
- ✓ 不同终端识别与管理



Part 5

SASE成熟度能力要求

SASE成熟度能力要求-工作汇报

多次标准研讨会打磨

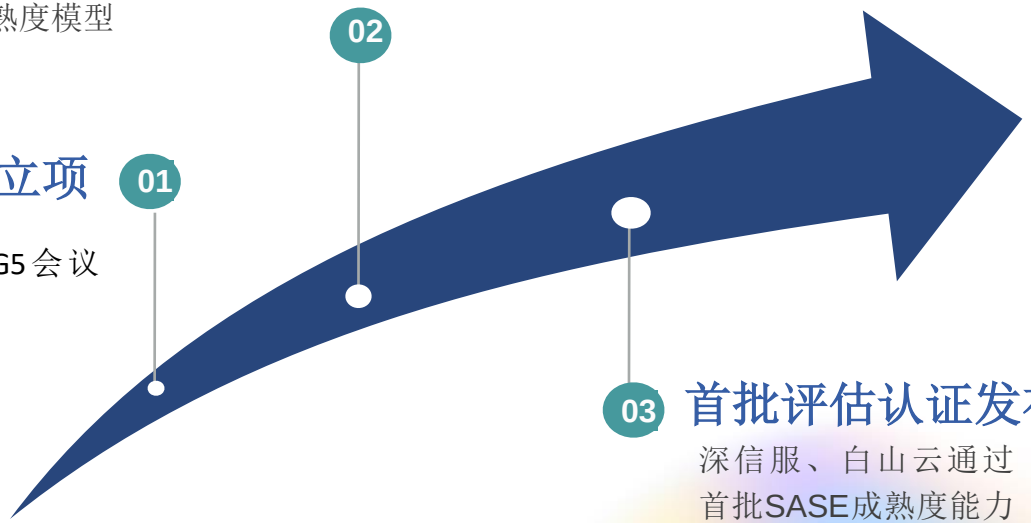
针对可信云SASE成熟度能力要求标准召开多次研讨会，企业专家深入探讨SASE成熟度模型

02

标协成功立项

01

2021年6月TC1WG5会议上成功立项



首批评估认证发布

03

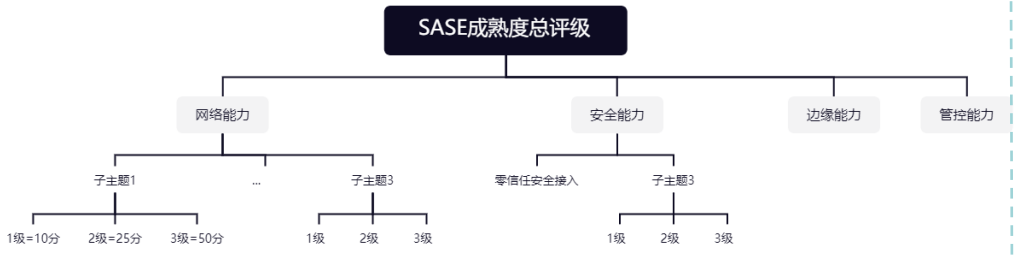
深信服、白山云通过首批SASE成熟度能力要求评估

多家企业共同参与标准标准制定与编写

中国信息通信研究院
深信服科技股份有限公司
贵州白山云科技有限公司
北京天融信网络安全技术有限公司
腾讯云计算(北京)有限责任公司
北京青云科技股份有限公司
阿里云计算有限公司
中移（苏州）软件技术有限公司
中国移动通信集团浙江有限公司
中国移动通信集团北京有限公司
新华三技术有限公司
中兴通讯股份有限公司
北京安天网络安全技术有限公司
杭州安恒信息技术股份有限公司
犀思云(苏州)云计算有限公司
北京奇虎科技有限公司
北京万维物联科技发展有限公司
北京贝思平云科技有限公司
中国电子系统技术有限公司
杭州网银互联科技股份有限公司
观脉科技(北京)有限公司
网宿科技股份有限公司
国家(杭州)新型互联网交换中心
上海缔安科技股份有限公司
启明星辰信息技术集团股份有限公司

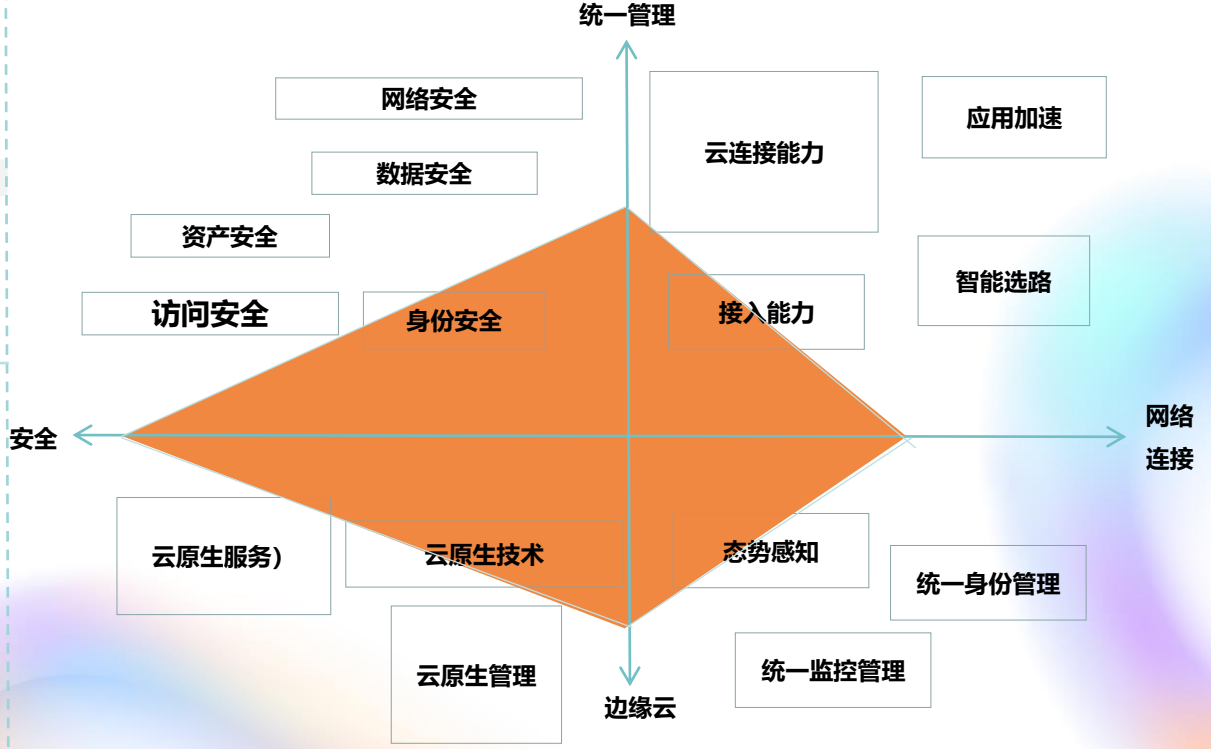
SASE成熟度能力要求-评级方法

SASE成熟度评级方法

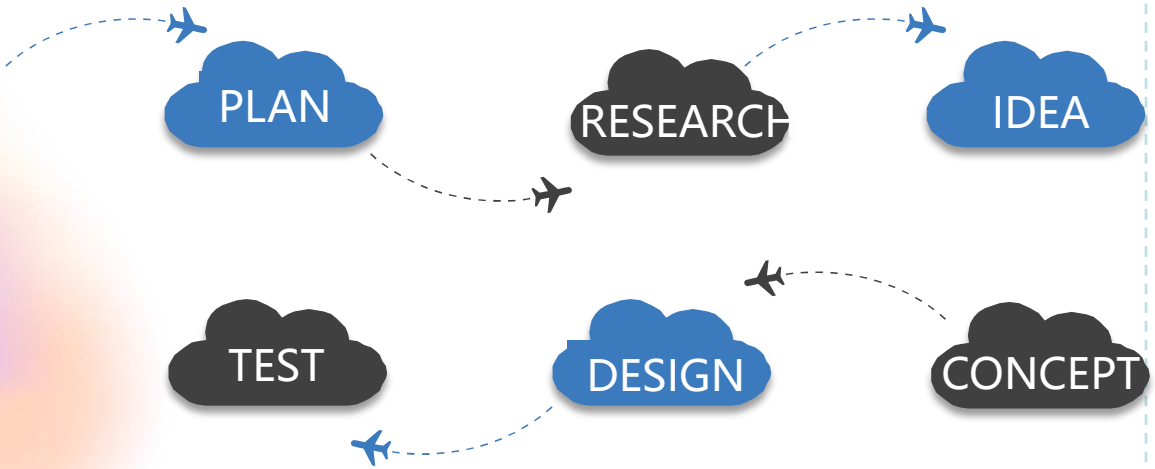


SASE成熟度能力要求

SASE成熟度能力象限



SASE成熟度能力要求-网络连接能力



网络冗余能力

——应支持链路层冗余，专有传输网络具有Overlay或Underlay的链路冗余。
——应支持接入层冗余，POP点间具备冗余迁移机制，单POP点故障后会自动迁移到其他可用POP点

多云连接能力

——应支持对1个主流公有云、私有云连接能力。
——应支持对2个及以上主流公有云、私有云连接能力。

网络接入能力

——应支持公网或专线的接入方式。
——应支持一种设备形态接入方式。
——应支持公网和专线的接入方式。
——应支持多种设备形态接入方式：硬件CPE、软件vCPE、客户端软件等。

流量QoS能力

——应支持针对流量的网络信息包括协议类型、源目的端口、IP地址进行分类。
——应支持基础QoS配置包括配置优先级、限速规则。
——应支持针对流量的应用类型与协议进行分类。
——应支持高级QoS配置包括流量整型、队列丢包机制。

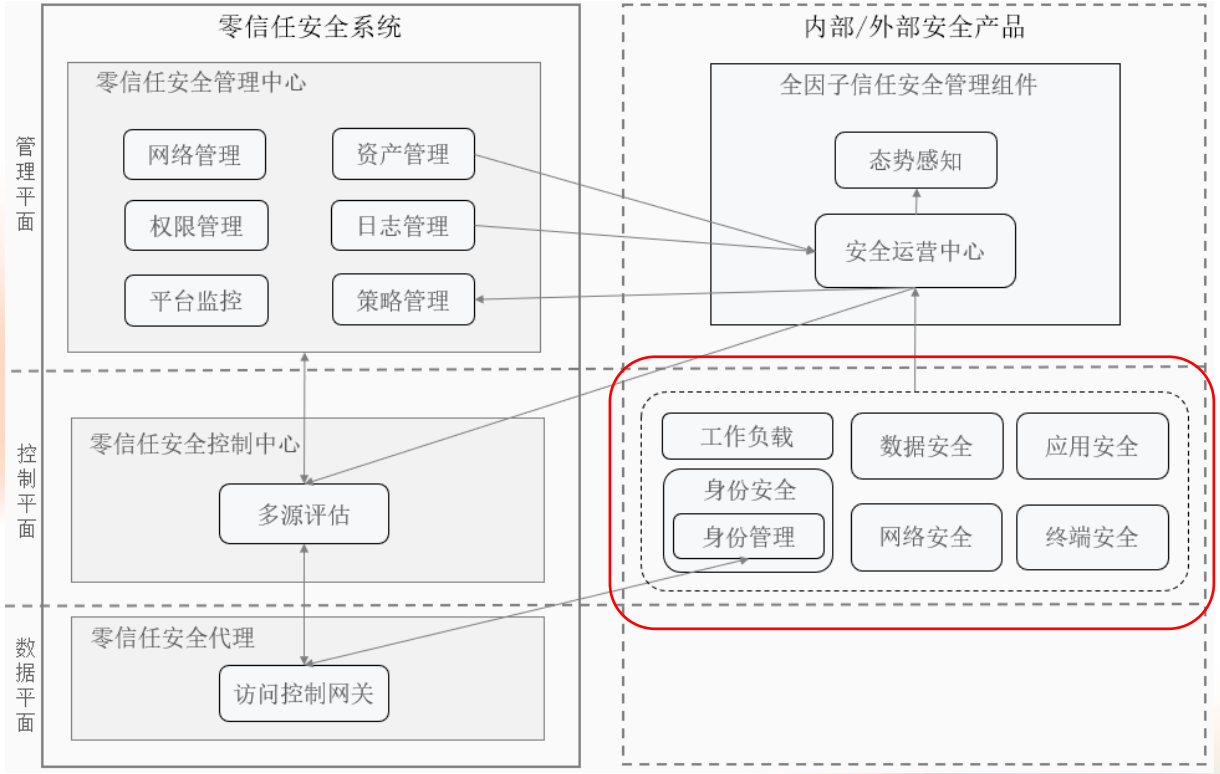
网络优化能力

——应支持根据流量网络信息包括IP地址、Mac地址、TCP/UDP协议进行选路能力。
——应支持手动切换流量线路能力。
——应支持基于用户域、五元组进行选路。

流量分析能力

——应支持网络识别能力，具备识别流量的TCP/UDP协议、源目IP地址、Mac地址、地域信息能力。
——应支持对采集的用户流量信息进行统计，生成报告并实时上传到统一管控平台或日志库能力。

SASE成熟度能力要求-安全能力



网络安全

——应支持由外部向IT架构发起的网络攻击和入侵防护。
——应支持对由IT架构向外部发起的网络攻击和入侵行为的阻断。
——应支持IT架构内部资源间的网络攻击和入侵防护。

应用安全

——应支持Web应用类资源的安全防护。
——应支持web攻击防护。
——应支持CC攻击、DDoS攻击防护。
——应支持应用常见安全漏洞扫描。

工作负载

——应支持主流的工作负载安全检测与防护，包括物理服务器、虚拟主机。
——应支持工作负载内主流的操作系统的安全检测与防护。
——应支持工作负载与终端间行为的检测与控制。

数据安全

——应支持数据防泄露：对IT架构中，以及由IT架构向外的数据传输和使用过程进行监测，及时发现数据泄露事件，对可能发生的泄露事件进行阻断，对已经发生的泄露事件进行追溯和追责。

SASE成熟度能力要求-边缘云能力

分布式能力

策略执行能力

- ✓ 边缘接入节点应支持自身数据转发的决策。
- ✓ 边缘节点应支持执行安全管控平台下发的安全策略。

边缘加速能力

- ✓ 应支持通过边缘侧针对延时要求敏感业务如进行访问加速能力：
  （1）支持实时音视频加速优化能力
  （2）支持图像、视频压缩优化加速能力
  （3）支持动态、缓存数据优化加速能力

分布式部署能力

- ✓ 应支持接入节点覆盖在主要地域（华东、华南、华北）
- ✓ 应支持在边缘接入节点部署安全与网络组件，在边缘侧即可实现安全检查能力。
- ✓ 应支持接入节点覆盖在主要城市（北京、上海、广州）
- ✓ 应支持边缘节点部署在公有云平台。
- ✓ 应支持接入节点覆盖国外主要地域（北美、南美、欧洲）

云原生能力

平台兼容能力

- ✓ 应支持在1种云平台与私有服务器进行部署，无平台限制。
- ✓ 应支持支持 B/S 或 C/S架构部署。
- ✓ 应支持客户端在1种终端平台（windows、mac、ios、android、linux）进行部署
- ✓ 应支持在2种以上云平台与私有服务器进行部署，无平台限制。
- ✓ 应支持客户端在2种以上终端平台（windows、mac、ios、android、linux）进行部署

弹性扩展能力

- ✓ 支持接入点弹性扩展，根据并发访问量动态调整接入点数量、网络、计算、存储、安全、身份资源。
- ✓ 支持网元弹性扩展，根据网络流量特征动态调整网元分布与数量。
- ✓ 支持服务级别弹性扩展，根据服务并发量动态调整服务资源。

多租户能力

- ✓ 应支持多租户提供服务能力
- ✓ 应支持租户账号管理，区分系统账号与租户账号。
- ✓ 应支持租户资源管理，租户查看与调用相应所属的设备与资源。
- ✓ 应支持租户网络隔离：应支持租户间网络非互通，其中租户的网络变化不影响其他租户。
- ✓ 应支持租户数据隔离，应支持租户间数据访问隔离，具备识别租户，建立数据库路由，执行对应数据库访问。

SASE成熟度能力要求-统一管控能力

平台通用能力

- ✓ 图形可视化
- ✓ 统一平台
- ✓ 多种终端访问

网络管理能力

- ✓ 全网监控
- ✓ 网络拓扑呈现
- ✓ 流量访问控制
- ✓ 自定义组网

安全管理能力

- ✓ 创建用户、用户组
- ✓ 多级授权管理
- ✓ 日志上报分析
- ✓ 安全态势可视化展示

配置管理能力

- ✓ 自定义配置模板
- ✓ 配置纠错
- ✓ 自动下发

运维管理能力

- ✓ 日志管理
- ✓ 告警管理
- ✓ 性能管理

资产管理能力

- ✓ 软硬件资产管理
- ✓ 自动发现网络中设备

API管理能力

- ✓ API接口功能
- ✓ 监控API使用情况
- ✓ API密钥

率先通过SASE成熟度能力评估厂商

TRUCS

SANGFOR 深信服科技

深信服科技股份有限公司

深信服云安全访问服务Sangfor Access

先进级

白山云科技 BAISHANCLOUD

贵州白山云科技股份有限公司

Baishan Canvas

先进级

THANKS!

2021
TRUSTED CLOUD
SUMMIT