华为云 Stack 安全白皮书

文档版本 1.0

发布日期 2021-08-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

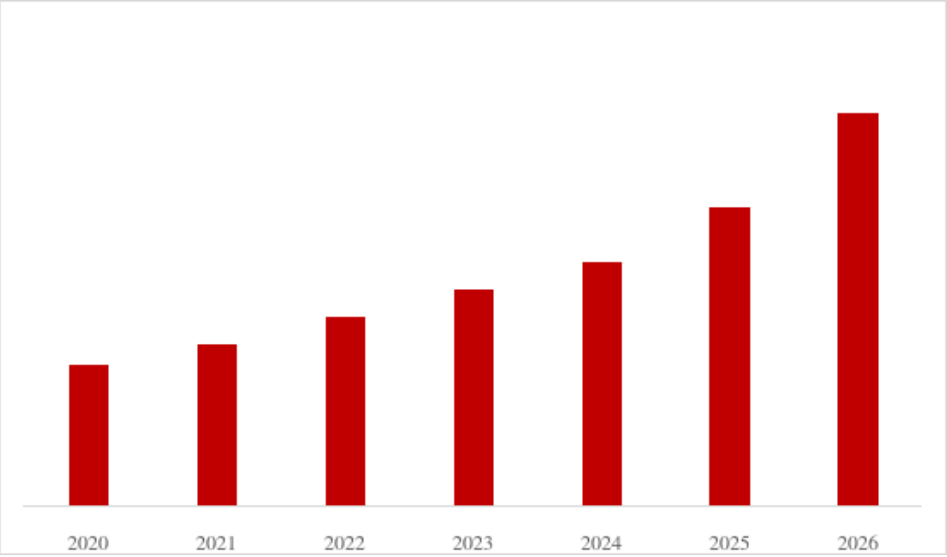
目 录

1 概述

1.1 混合云部署成为当下主流

随着云计算的普及，企业意识到云计算可以为其带来更灵活和更高效的企业管理模式。企业在云采用方面的经验越来越丰富，他们也逐渐发现其最有价值的数据应留存在企业内部，而不是全部托管至公有云上。因此，混合云的部署模式就成了很多企业的选择。

根据Mordor Intelligence发布的《混合云市场报告》显示，到2026年混合云的市场价值将达到1450亿美元，2020年-2026年混合云的复合年增长率预计为18.73%。可以推测，混合云将成为企业上云的主流模式。华为云Stack解决方案正是顺应此主流云部署模式下的产物。



SOURCE: Mordor Intelligence

经过华为云多年努力，利用在公有云和私有云领域的优势和专业知识为用户提供卓越的混合云管理解决方案。在国际知名调研机构Forrester发布的《The Forrester WaveTM: Hybrid Cloud Management Software In China,Q3 2021》报告中，将华为云定义为中国混合云管理市场的卓越表现者。

然而，客户普遍对混合云环境仍感到担忧。安全厂商Ermetic调研了超过300位信息安全主管，近80%的企业在过去18个月里至少经历过一次云数据泄露，43%的企业报告了超过10次。因此，云上层出不穷的安全与合规问题成为了客户选择使用混合云部署模式的主要顾虑。

1.2 华为云 Stack

华为云Stack解决方案是一套部署在客户本地数据中心的云基础设施，是华为云在客户数据中心的一种延伸，以一体化全栈方式交付完整的云服务平台，与华为云统一架构、统一服务、统一API。同时，华为云还可以提供统一安全运维运营服务，将华为云Stack运维面通过专线接入华为云运维中心，以降低客户的运维成本，保障运维安全。

华为云Stack为客户提供公有云服务体验：

- 华为云Stack为客户提供与华为云一致的基础架构，继承公有云大规模商用成熟架构，稳定可靠、开放兼容。
- 华为云Stack提供与华为云一致的API接口和管理工具，降低客户开发适配成本。
- 华为云Stack服务能力与华为云同步，云服务之间互相解耦，可根据业务场景按需部署、平滑扩展、快速同步华为云能力。
  - 提供完整的IaaS专属服务。
  - 按需搭配数据库、大数据服务、安全服务、中间件和应用服务。

华为云Stack为客户提供本地化部署和统一运维运营服务：

- 华为云Stack部署在客户数据中心，用户独享计算、存储、网络以及云服务等资源，通过物理隔离满足特定性能、业务应用和安全合规等要求。
- 客户可选用统一运营运维服务，选用本服务后，华为云Stack可通过专线接入华为云运维中心，由华为云专业运维团队统一运维，简化运维工作，降低运维成本，是政府、金融、以及大企业客户核心业务上云的优选途径。

华为云Stack为客户构建同构混合云，使其同时享有私有云和公有云的优势：

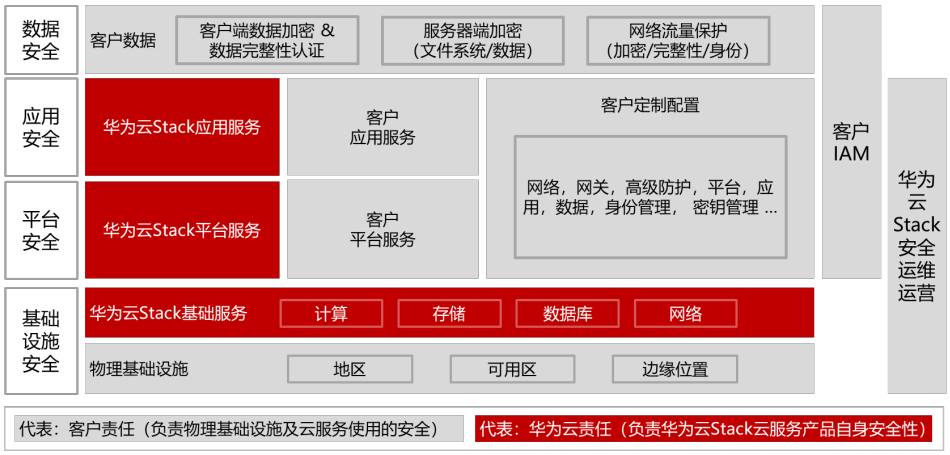
- 华为云Stack可通过虚拟专用网络（VPN）或云专线（DC）接入华为云，从而构建与华为云统一架构的混合云。可实现统一认证、SSO单点登录、不同云服务平台之间的跳转、跨云容灾备份，业务分层部署（例如分层存储架构）等场景。

华为云一直将提供“安全、可信的云服务/解决方案”作为其首要任务。为应对混合云场景下的常见风险，华为云Stack解决方案充分融入了公有云管理的云安全理念、世界领先的云安全实践、华为云常年积累的网络安全经验和优势以及在云安全领域的技术积累与运营实践，从华为云及客户责任共担模型出发，双方共同努力，创造安全的华为云Stack环境。

2 华为云 Stack 安全责任共担模型

华为云Stack是云计算的一种部署模型，其安全责任需要华为云与其客户共同分担，云服务客户也需要思考在华为云Stack环境中如何进行安全管理。客户在云安全管理方面的知识可能相对不够全面，或者原有的安全管理手段在华为云Stack环境中缺乏有效性。面对华为云Stack安全管理需求，客户可借助华为云Stack提供的服务及产品，提升自身在华为云Stack环境中的安全管理能力。

图 2-1 华为云 Stack 安全责任共担模型



华为云Stack安全责任共担模型，绿色部分为华为云责任，蓝色部分责任由客户承担。客户可向华为云购买统一运维运营服务，用以抵御外部攻击，满足合规要求。

华为云负责华为云Stack自身的安全，提供安全的云服务及产品；客户负责使用华为云Stack时内部的安全，安全地使用该解决方案。

数据安全：指华为云Stack中客户业务数据自身的安全管理，包括数据完整性认证、加密、访问控制等。

应用安全：指在华为云Stack中,支撑运维运营及客户业务等应用系统的安全管理，包括应用的设计、开发、发布、配置和使用等。

平台安全：指在华为云Stack中的微服务、管理、中间件等平台类的安全管理，包括平台的设计、开发、发布、配置和使用等。

基础设施安全：分为基础服务安全和物理基础设施的安全：

- 基础服务安全：指华为云Stack中包括的计算、网络、存储等方面的安全管理，包括云计算、云存储、云数据库等服务的底层管理（如虚拟化控制层）和使用管理（如虚拟主机），以及虚拟网络、负载均衡、安全网关、VPN、专线链路等。
- 物理基础设施安全：部署了华为云Stack的客户机房和环境的安全管理，以及物理服务器和网络设备等设施的管理。

华为云的主要责任是向客户提供安全可信的华为云Stack平台产品和交付，包括其中承载的基础服务、平台服务及应用服务，确保服务内置的安全功能。

客户的主要责任是运维运营部署华为云Stack的机房的物理基础设施，以及华为云Stack中的各项基础服务、平台服务和应用服务。同时，客户还负责构建物理层、基础设施层、平台层、应用层、数据层和IAM层的多维立体安全防护体系及其定制配置，保障其运维运营的安全，以及用户身份的有效管理。

2.1 华为云 Stack 中华为云的安全责任

华为云Stack作为解决方案及运维运营服务提供商，其安全责任在于提供安全的华为云Stack平台产品和交付，涵盖华为云Stack上的基础服务、平台服务、应用服务等，包括各项云服务的安全能力和性能。华为云Stack平台的安全设计和实施交付由华为云提供，华为云Stack确保提供给客户的平台安全设计和安全能力符合与客户签订的合同要求。华为云为其客户提供华为云Stack平台的安全运维运营服务，但需要客户向华为云购买并授权华为云提供该服务。

- 华为云将隐私保护视为华为云Stack解决方案的重中之重，将隐私保护理念融入到华为云Stack平台及云服务的开发设计之中，为客户提供稳定、可靠、安全、值得信赖及可持续的解决方案。在客户选择购买华为云Stack安全运维运营服务后，华为云将积极遵从隐私保护相关的法律法规要求，遵守服务边界，助力客户实现隐私合规。
- 华为云Stack的安全责任基于华为云作为云技术的研发者和云服务运维运营者的双重角色，首先务必保持从研发到运维运营的整个流程的云安全质量基线。华为云Stack一方面确保各项云技术的安全开发、配置和部署；同时采用适合云平台及云服务的漏洞管理机制，确保对云平台及云服务安全漏洞及时的应急响应，保证适合云平台及云服务运维运营周期的快速发布和不影响客户服务的持续部署，包括不断优化云平台及云产品默认安全配置、补丁装载前置于研发阶段和灵活简化安全补丁部署周期等措施。另外，华为云Stack的安全责任还表现在持续开发有强大市场竞争力并致力于为华为云Stack客户业务增值的云安全服务。
- 华为云Stack携手云安全商业合作伙伴向客户提供咨询服务，在虚拟网络、虚拟机（包括虚拟主机和访客虚拟机）的安全配置，系统和数据库安全补丁管理，虚拟网络的防火墙、API 网关和高级安全服务的定制配置，DoS/DDoS 攻击防范，客户安全事件的应急响应以及灾难恢复等方面协助客户。

2.2 华为云 Stack 中客户的安全责任

华为云Stack部署在客户机房中，客户承担物理基础设施、基础服务、平台服务、应用服务及客户数据的安全责任,以及安全策略配置、安全运维运营管理等。其安全责任包括但不限于如下安全活动：虚拟网络，虚拟主机和访客虚拟机等操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务、客户数据以及身份账号和密钥管理等方面的安全配置管理等。

- 客户使用哪些华为云Stack服务将最终决定客户的安全责任细节，具体到客户负责执行什么默认和定制的安全配置。对于华为云Stack的各项云服务，华为云Stack

只向客户提供执行特定安全任务所需的所有资源、功能和性能的华为云Stack平台产品及交付工作，而客户需负责各项可控资源的安全配置工作。

- 客户负责部署其虚拟网络的防火墙、网关和高级安全服务及其策略配置，客户空间的虚拟网络、虚拟主机和访客虚拟机等云服务所必需的安全配置和管理任务（包括更新和安全补丁），容器安全管理，大数据分析等平台服务的客户配置，以及其它各项客户购买的华为云Stack平台之上的云服务内部的安全配置等。客户也负责对其自行部署在华为云Stack平台之上的任何应用程序软件或实用程序进行安全管理。
- 在配置云服务时，客户负责在将各项安全配置部署到生产环境前做好充分测试，以免对其应用和业务造成负面影响。对大多数云服务的安全性而言，客户只需配置账户对资源的逻辑访问控制并妥当保管账户凭证。少数云服务则需要执行其他任务才能达到应有的安全性。例如使用数据库服务时，在华为云Stack上执行数据库整体安全配置的同时，客户还需设置用户账户和访问控制规则。各项监控管理服务和高级安全服务具有较多安全配置选项，客户可寻求华为云Stack和其合作伙伴的技术支持，以确保安全性。
- 无论使用哪一项华为云Stack平台上的服务，客户始终是其数据的所有者和控制者。客户负责各项具体的数据安全配置，对其保密性、完整性、可用性以及数据访问的身份验证和鉴权进行有效保障。作为数据安全的重中之重，即在使用身份认证和访问管理服务 (IAM) 和密钥管理服务 (KMS) 时，客户负责妥善保管其自行配置的服务登录账户、密码和密钥，并负责根据业界优秀实践执行密码密钥设定、更新和重设规则。客户负责设置个人账户和多因子验证 (MFA)，规范使用安全传输协议与华为云Stack资源通信，并且设置用户活动日志记录用于监测和审计。
- 客户对其自行部署于华为云Stack平台上、不属于华为云Stack提供的各项应用和服务的安全及隐私保护合规情况全权负责，并自行开展所服务行业的安全及隐私标准的合规评估。

3 华为云 Stack 如何应对混合云场景下的常见风险

云安全联盟（Cloud Security Alliance，简称CSA）于2020年7月发布了《Hybrid Clouds and its Associated Risks》。其中描述了混合云的概念和价值，突出了关键的应用场景，并指出了混合云场景下的常见安全风险。其风险分别为：

- 边界防护风险
- 数据泄露
- DDoS攻击
- 合规风险
- 定义不明确的SLAs
- 云技能集不一致
- 安全控制成熟度不一致
- 安全风险评估不足

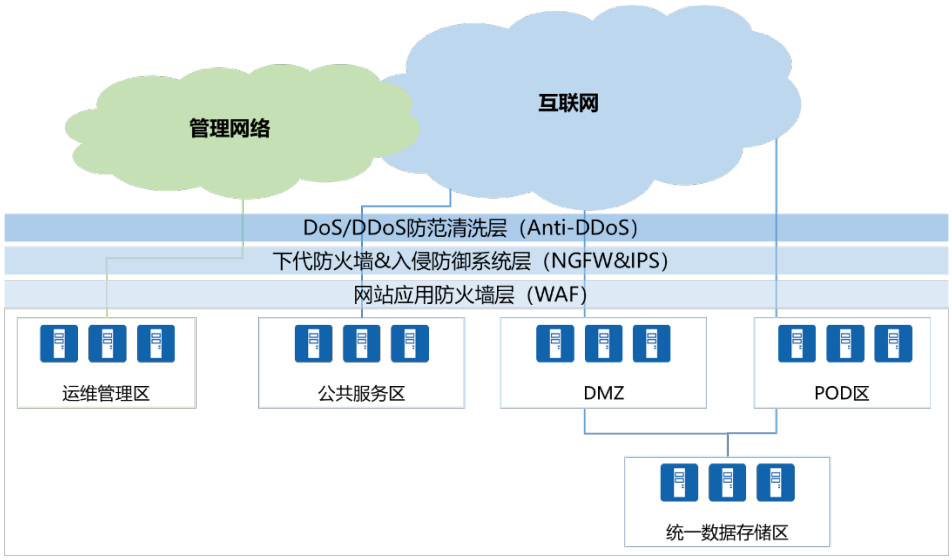
为了应对CSA提出的上述风险，华为云Stack解决方案从其逻辑架构设计、华为云Stack中承载的云服务和云产品等方面介绍了华为云部署和集成的安全功能和服务，以及客户可选择的安全功能和服务。

3.1 边界防护风险

当仅部署私有云时，应用程序的运行拥有清晰的网络边界和安全区域。但是，一旦它们从私有云迁移到公有云，原始的边界安全策略就可能会失效，从而影响应用程序的使用。发生这种情况的原因是不同种类的云使用的安全保护措施可能不在同一级别。此外，相应的管理职责也由一方变为多方。应用程序的弹性扩展也可能给安全带来挑战。混合云涉及的不同方（公共云与私有云/本地部署）之间实施的物理安全也可能存在差距[1]。

华为云Stack在设计阶段，就从功能架构上考虑解决方案在边界防护中的能力，能够有效应对常见的边界风险。华为云基于业界网络安全的优秀实践以及自身多年积累的丰富经验，对Stack平台进行了安全区域划分，安全区域内部的节点具有相同的安全等级。

图 3-1 华为云 Stack 平台安全域划分



华为云Stack根据业务功能和网络安全风险将其平台划分为多个安全区域，实现物理和逻辑控制并用的隔离手段，提供网络面对外部入侵时的自我保护和容错恢复能力。以下为华为云Stack五个重要的安全区域：

- DMZ 区：为客户部署了面向外网和用户的前置部件，如负载均衡器、代理服务器等，以及服务部件，如服务控制台、API 网关等。用户对DMZ区的访问行为不可信，所以华为云Stack为客户单独隔离DMZ区域。此区域部件面临极高安全风险，除部署了防火墙、防 DDoS 措施外，还部署了应用防火墙（WAF）及入侵检测设备（IPS）以保护基础网路、平台及应用。
- 公共服务区：该区域主要部署 IaaS/PaaS/SaaS 服务化组件如IaaS/PaaS/SaaS 服务控制部件，以及一些基础设施服务部件如补丁服务等。此区域内的部件根据业务需要由华为云Stack受限开放给用户。政务云管理员可以从内网区访问该区域进行操作和管理。
- 资源交付区（POD）：在此区域部署华为云Stack客户提供所需的基础设施资源，包括计算、存储、网络资源，如虚拟机、磁盘、虚拟网络。该区域还可以支撑对进出互联网的客户流量做 DDoS 防护及入侵检测与防御，保障客户业务安全。
- 数据存储区：此区域部署对象存储系统，提供对象存储服务。由于存储客户隐私数据，所以进行了分区隔离。在该区域边界由客户在安全组件上配置执行所需的访问控制规则，在任意客户空间访问该区域时不需要绕道 DMZ。但由于从外网访问安全风险高，所以必须通过DMZ的服务控制台或网关才能访问该区。
- 运维管理区：该区域主要部署操作运维部件，管理员可以通过此区域对其他区域进行统一的业务系统运维运营管理。当客户选择使用华为云提供的统一运维运营服务时，华为云运维人员将通过VPN接入该区域，再通过堡垒机访问被管理节点。

除此之外，华为云Stack还提供了丰富的网络边界防护服务供客户选用，以确保更好的应对风险。

1. **虚拟私有网络（VPN）**

   VPN用于在远端网络和华为云Stack VPC之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云上，为客户提供端到端的数据传输机密性保障。通过VPN在传统数据中心与VPC之间建立通信隧道，客户可方便地使用华为云的云服务器、块存储等资源，通过将应用程序转移到云中、启动额外的

Web服务器来增加网络的计算容量，实现了企业的混合云架构的同时，也降低了企业核心数据非法扩散的风险。

2. **弹性负载均衡服务（ELB）**

   ELB为其应用服务提供负载均衡能力，负责将访问流量自动分发到多个弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能，自动满足变化的流量需求。

3. **入侵防御（IPS）**

   IPS可通过预先设定的安全策略，对流经的每个报文进行深度检测（协议分析跟踪、特征匹配、流量统计分析、事件关联分析等），一旦发现隐藏于其中的网络攻击，可以针对网络攻击的威胁级别立即采取抵御措施，这些措施包括（按照处理力度）：向管理中心告警；丢弃该报文；切断此次应用会话；切断此次TCP连接。复用下一代防火墙能力，可以实现基于网络流量的IPS，帮助客户保护网络边界安全。

4. **边界防火墙服务（EdgeFW）**

   EdgeFW提供了严密的访问控制，对内、外部网络实施隔离，保护边界内部网络，对南北向边界提供高级安全保护，例如IPS、AV等，增强了传统边界防火墙所提供的保护。

5. **云防火墙（CFW）**

   CFW为客户虚拟机提供微隔离能力，并通过流量可视化以及基于业务属性标签的安全策略配置手段来降低安全运维复杂度。

6. **Web应用防火墙（WAF）**

   WAF可对Web应用层数据、HTTP进行完整的解析，对不同的编码方式做强制多重转换还原为攻击明文，把变形后的字符组合后再分析，能够较好地抵御来自Web层的组合攻击。同时，WAF提供专用的应用层规则，全面防护常见的Web攻击威胁，提高Web防护能力。从而避免源站被黑客恶意攻击和入侵，防止核心资产遭窃取，为网站业务提供安全保障。

7. **主机防护服务（HSS）**

   HSS是终端安全防护服务，提供主机入侵防御（HIDS）等安全功能保障弹性云主机的安全性。功能涉及恶意软件查杀、入侵检测、防火墙、日志审查、完整性监控和Web信誉等。

说明

1. 该风险描述来自于CSA发布的《Hybrid Clouds and its Associated Risks》。

3.2 数据泄露

在云环境中，用户的终端和云通过互联网进行连接。因此，由于人为错误或中间人攻击引起的未经授权访问均可能导致用户数据泄漏。此外，在运行混合云时，服务信息通常通过API与云进行交互。如果保护不当，也可能导致API接口被恶意攻击，以获得对混合云中数据的未经授权访问或配置修改，导致关键数据泄露或导致云/系统的中断[1]。

华为云高度重视客户的数据安全，把数据保护作为华为云安全策略的核心。华为云Stack始终遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为客户提供最切实有效的数据保护。

华为云Stack内置SSH传输协议，该协议是目前较可靠，专为远程登录会话和其他网络服务提供安全性保障的协议。利用SSH协议可以有效防止远程管理过程中的信息泄露

问题。透过SSH可以对所有传输的数据进行加密，并防止DNS欺骗和IP欺骗。除此之外，华为云Stack还提供了一系列云服务及解决方案供客户选择，帮助客户更好地预防数据泄露风险。

1. **统一身份认证服务（IAM）**

   华为云Stack集成了IAM统一身份认证服务，为客户提供了适合企业级组织结构的用户帐号管理服务，为企业用户分配不同的资源操作权限。用户通过IAM 的认证和鉴权后，以调用API的方式访问云资源。IAM可以按层次和细粒度授权，保证同一企业不同用户在使用云资源时得到有效管控，避免单个用户误操作等原因导致整个云服务的不可用，确保客户业务的持续性。

   IAM通过提供基于IP的ACL限制企业用户只在安全的网络环境下访问云资源，避免企业用户因接入不安全网络环境导致的数据泄露。

2. **数据加密服务（DEW）**

   客户可选用DEW服务对存储的数据进行加密。DEW负责对密钥全生命周期进行集中管理。在未授权的情况下，除客户外的任何人都无法获取密钥，对数据进行解密，确保了客户数据在华为云Stack上的安全。

3. **密钥管理服务（KMS）**

   客户可选用KMS服务，KMS为平台云服务、客户业务应用提供一种安全可靠、简单易用的密钥托管服务，其密钥安全由硬件安全模块 (HSM) 保护，帮助用户集中管理密钥生命周期安全。解决了云服务加密密钥安全创建、客户密钥统一管理的问题。

说明

1. 该风险描述来自于CSA发布的《Hybrid Clouds and its Associated Risks》。

3.3 DDoS 攻击

对于攻击者而言，对云环境发起资源攻击或应用层攻击可能花费的成本更低，并且对云环境的影响更为严重。DDoS攻击导致的直接后果就是网络流量拥堵，影响云服务质量，最终影响云服务提供商的声誉。在混合云环境中，DDoS攻击还可能造成混合云解决方案中组件之间“内部”通信的中断[1]。

华为云Stack为应对DDoS攻击，从平台设计上就考虑了以限制虚拟端口的方式抵御多方的大流量攻击。

华为云Stack通过限制虚拟端口的连接跟踪数来抵御来自云平台外部或平台内部其他虚拟机的大流量攻击，此类攻击会产生大量连接跟踪表项，如果不做限制，会耗尽连接跟踪表资源，导致不能接受新的连接请求，最终导致业务及管理流量中断。

除此之外，还为客户提供了Anti-DDoS流量清洗服务及两级云解决方案，从而可以实现及时的异常流量清洗，并提供为应对突发需求而进行的临时扩容。

1. **流量清洗（Anti-DDoS）**

   客户可将Anti-DDoS流量清洗设备部署在其数据中心网络出口区域。Anti-DDoS设备通过对互联网访问弹性云服务器、弹性负载均衡和裸金属服务器的业务流量进行实时监测，及时发现异常DDoS攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。

2. **两级云**

   客户可部署华为云Stack的两级云方案。该方案可以在本端华为云Stack资源不足时，通过对接对端的华为云Stack API Gateway的方式在对端华为云Stack上申请资源，而不需要对本端资源池做扩容，可以快速满足突发资源增长需求。

说明

1. 该风险描述来自于CSA发布的《Hybrid Clouds and its Associated Risks》。

3.4 合规风险

在混合云中，实现和维持一致的合规性是一个巨大的挑战。数据在本地和云端之间的流动增加了在混合模型中维护和遵守治理框架的难度。例如，公有云全球部署和存储的能力导致其需要符合所有数据所在国家和地区的法律法规或监管要求[1]。

华为云一贯高度重视客户的信任，并在此方面持续增加投入。而安全合规与标准遵从正是获得并维护客户信任的必由之路，同时也是防范“内鬼”破坏的重要手段。通过业界通用的安全合规与标准遵从的认证，既能提升华为云Stack的整体安全能力和业务水平，也能帮助客户减少对合规的担忧。

华为云建立了一个正式的、定期的审计计划，包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。

目前，华为云Stack的安全测评及认证有：

- ISO/IEC 27001
- CC[2] EAL2+
- 支持通过中国公安部信息安全等级保护三级
- 通过云测评《信息技术 云计算 参考架构》- 引领级测评
- ITSS云服务能力评估 - 私有云（1级）

客户可以在华为云信任中心申请下载最新的包含ISO27001在内的多种合规资质证书及报告，客户在下载此类资源之前需先同意华为云保密承诺函。

除此之外，华为云也为客户提供合规解决方案，从而可以更好的辅助客户实现华为云Stack环境的合规。

1. **华为云合规解决方案**

   除华为云Stack自身通过了各类网络安全及隐私保护相关的认证和鉴证外，华为云也致力于为客户提供合规解决方案。

   华为云依托自身安全能力与安全合规生态，为客户提供一站式的等保2.0安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保合规要求。华为云整合了其多年来研究的安全技术，为客户提供多场景的等保合规安全解决方案，满足多行业业务诉求。详情参见**“等保合规安全解决方案”**页面，同时该页面提供《等保合规2.0白皮书下载》的链接，客户可自行下载，提前针对等保需求进行自评估。

说明

1. 该风险描述来自于CSA发布的《Hybrid Clouds and its Associated Risks》。
2. CC：Common Criteria（CC）是国际标准化组织统一现有多种准则的结果，是目前最全面的评价准则。1996年6月，CC第一版发布；1998年5月，CC第二版发布；1999年 10月CC V2.1版发布，并且成为国际标准ISO/IEC 15408，我国于2001 年等同采用为GB/T 18336。CC的主要思想和框架都取自ITSEC和FC，并充分突出了“保护轮廓”概念。CC将评估过程划分为功能和保证两部分，评估等级分为EAL1、EAL2、EAL3、EAL4、EAL5、EAL6和EAL7共七个等级。每一级均需评估7个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估。

3.5 定义不明确的 SLAs

私有云的SLA可能没有使用公有云时的SLA清晰/严格。云服务提供商和客户本地环境的管理使用了不同的工具、API和SLA，这使得SLA的一致性变得难以实现。在这种情况下，企业需要意识到差异，以便设计和部署其应用程序以适应“正确的”Stack解决方案[1]。

华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。但是，客户也应确保其自身及其选定的其它服务提供商可按照合同及SLA约定提供相应服务。

说明

1. 该风险描述来自于CSA发布的《Hybrid Clouds and its Associated Risks》。

3.6 云技能集不一致

公有云和私有云可能需要单独的技能集，因为它们通常依赖于不同的平台来管理和监控云服务。此外，每个云都可能使用特定的管理配置和术语。考虑到云上的许多安全事件都需要被跟踪，通常被归因为不安全的或错误的配置，缺乏适当的云技能集和知识可能会为试图实施其云战略的企业造成可怕的后果。如果安全配置和控制未能在不同云中一致地应用，可能会产生安全风险。此外，从混合云系统管理的角度来看，企业需要协调不同的云技能集，对接不同的平台。对于用户来说，统一视图和易于使用的管理工具对于管理混合云、简化管理和提高管理效率至关重要。这就需要合适的云管理平台来集中管理混合云，为用户提供统一的管理、监控和审计能力[1]。

云技能集既包括华为云Stack解决方案所能提供的功能层面，也包括客户的管理人员专业技能层面。华为云Stack为客户提供统一云管理平台ManageOne，解决功能层面的问题；同时也为客户提供统一运营运维服务（如需），解决管理人员专业技能的问题。

1. **ManageOne云管理平台**

   华为云Stack中集成的ManageOne承担了云管理平台（CMP）的职责，通过自研和集成的方式，为客户提供对其企业私有云资源及企业租用的公有云资源进行统一管理的能力，包括客户自助服务界面，云服务管理和服务目录，计量，计算、存储和网络资源自动化配置，云服务和云资源的运维监控以及运营指挥分析等。

   - ManageOne提供云服务的统一接入、云服务管理、组织管理等能力，运营业务能力由云服务提供，从而实现云服务的统一运营管理。
   - ManageOne基于从南向对接系统中抽取的资源对象的告警、性能、拓扑等信息，对资源进行监控、统计、分析与预测，从而实现云数据中心资源的统一运维管理。
   - ManageOne提供对计算、存储、网络设备的运维监控能力，采集和监控告警、性能等数据，从而实现基础设施的统一运维管理。

   通过ManageOne云管理平台，可以帮助客户实现：

   - 统一云资源视图：从计算、存储、网络、数据库等资源类型的视角查看华为云Stack资源的信息和状态。
   - 统一性能监控：ManageOne运维面通过接入华为云Stack的云监控服务（CES），查询客户的性能监控数据，展示性能监控视图。

- 统一容量监控：ManageOne的容量监控支持监控华为云Stack，并统计华为云Stack账号在各区域的资源使用量。
- 统一大屏：ManageOne运维面的大屏支持展示华为云Stack各区域的概览数据。
- 统一报表：ManageOne运维面支持统计华为云Stack各区域的报表。

2. **统一运维运营服务**

   客户可按需选用华为云Stack的统一运维运营服务，该服务可以解决客户在使用混合云技术或多云技术时，多元业务带来的更大的成本压力和需要更快的相应修复的需求。同时，为客户提供了统一的运维平台，在帮助客户有效降低运维支出的同时，提供了更高质量的运维服务。

   华为云Stack的统一运维运营服务需要客户将运维面通过专线接入华为云运维中心，进行统一运维以降低运维成本。统一运维运营服务采取“1+4+4”安全体系保障统一运维运营服务的安全，实现运维运营服务可信、可控、透明。

说明

1. 该风险描述来自于CSA发布的《Hybrid Clouds and its Associated Risks》。

3.7 安全控制成熟度不一致

混合云环境中实施的安全控制的成熟度可能不一致。通常，公有云环境与典型的私有云相比，具有更高的安全控制成熟度，或更广泛的安全控制目录，主要是因为私有云没有公有云那么高级别的安全需求。针对混合云，应尽早识别这种风险，并由高级管理层审查。如果认为不可接受，必须在必要时审查和更新企业的安全控制目录，以便实施一套一致和标准化的成熟控制。这不仅将改善企业的安全状况，而且还可能降低组织的财务成本[1]。

当客户选择将部分云服务迁移上云，或者选择华为云的远程运维运营服务时，可能面临公有云的网络安全控制与其本地私有云的安全控制成熟度不一致的情况，因此建议客户选择以下服务用以统一管控华为云Stack环境下的安全控制。

1. **安全指数服务（SIS）**

   客户可选用SIS服务，SIS是关于云环境的一个安全评估服务，为客户提供统一、直观、多维度的安全视图。客户可以通过安全指数服务了解所使用云环境是否已合理配置，所采取的安全措施是否已经足够，以及主动安全、被动安全的概况。

2. **安全态势感知（SSA）**

   客户可选用SSA服务，该服务能够帮助客户理解并分析其安全态势，通过收集其他各服务授权的海量数据，对客户的安全态势进行多维度集中、简约化呈现，方便用户从大量的信息中发现有用的数据，预测将来有可能发生的安全事件，从而可以部署一致的安全控制措施。

说明

1. 该风险描述来自于CSA发布的《Hybrid Clouds and its Associated Risks》。

3.8 安全风险评估不足

由于不同的云服务提供商通常提供的基础架构不同，对混合云环境的安全风险评估可能具有一定的挑战性。例如，私有云可能由企业自行拥有和管理。因此，通常分别针对私有云和公有云环境执行风险评估，而不是作为一个整体进行全面的评估。客户通

常缺乏适用于混合环境的管理或技术工具，也可能无法对混合环境的IT基础架构和系统执行详细的风险检查，导致风险评估缺乏完整性并造成安全盲点[1]。

为实现混合环境下风险评估的全面性，华为云Stack为客户提供了云堡垒机服务、漏洞扫描服务、云审计服务以及云日志服务，从而对混合云环境下的安全漏洞进行全面扫描，提前识别并制定措施来缓解相应风险；另外，也可全面记录混合云环境下的操作记录，在风险发生后可以有效定位，从而防止其再次发生。

1. **云堡垒机服务（CBH）**

   客户可选用CBH服务，对各个VM的运维进行严格的访问控制与授权、对登录操作记录、审计、回溯。

2. **漏洞扫描服务（VSS）**

   客户可选用VSS，对网络设备、操作系统和数据库等平台部件进行扫描，找出有关网络的安全漏洞及被测系统的薄弱环节，并针对监测到的安全隐患给出相应的修补措施和安全建议，从而消减系统的脆弱性，避免黑客攻击行为，做到防患于未然。

3. **云审计服务（CTS）**

   客户可选用CTS审计服务，使用其各种云资源操作记录的收集、存储和查询功能，用以安全分析、合规审计、资源跟踪和问题定位等。

4. **云日志服务（LTS）**

   客户可选用LTS服务，LTS是一个可提供实时查询、转储等功能的服务；无需开发即可利用日志服务做实时决策分析，提升日志处理效率。

说明

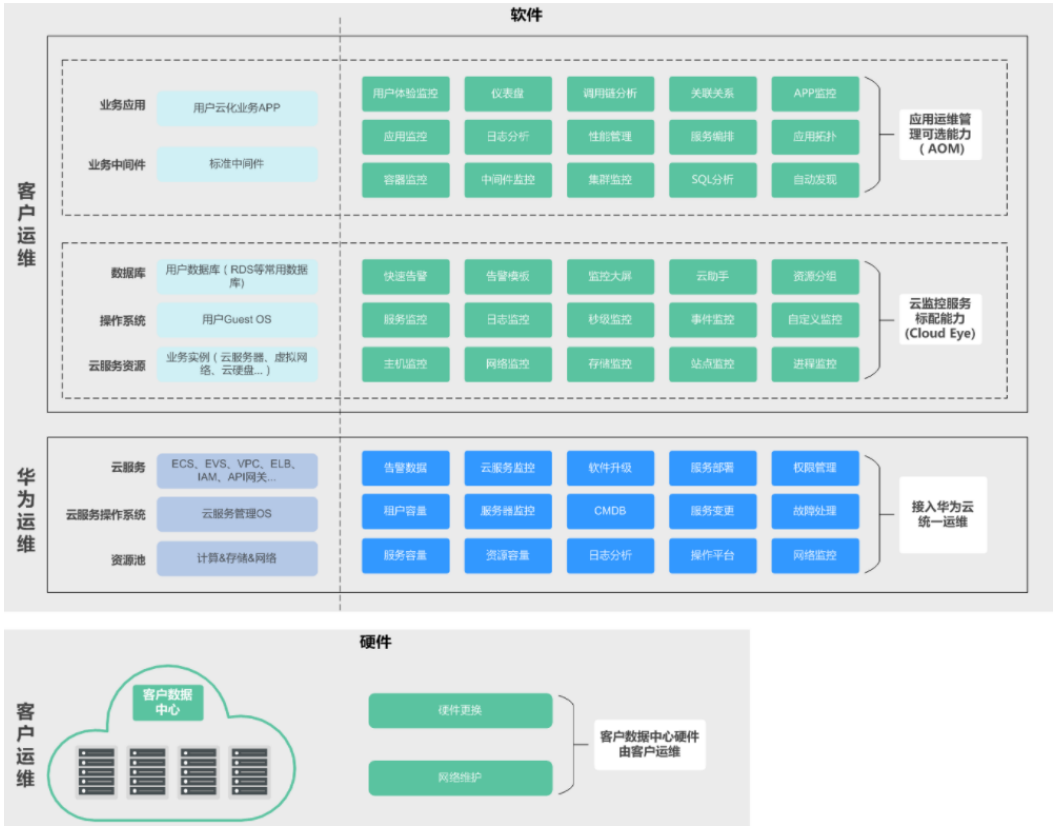
1. 该风险描述来自于CSA发布的《Hybrid Clouds and its Associated Risks》。

4 统一运维运营服务安全

华为云Stack客户可按需选择统一运维运营服务。华为云统一运维运营服务部署了多层数据保护机制，保障客户运维数据全生命周期的可靠和可用。

以下为客户选择华为云统一运维运营服务后的运维架构图。

图 4-1 华为云 Stack 统一运维运营架构图



华为云作为统一运维运营服务提供商，也从数据安全、IT安全、人员安全和物理安全制定了相关的策略和管控措施，确保客户运维数据的安全。

1. **数据安全**
   - 仅采集必须的运维数据

华为云Stack远程运维平台承诺仅采集必须的运维数据，包括：

获取的数据清单	数据用途	是否必选	业务面相关性	获取方式	获取周期
云服务清单和版本	了解各个云服务版本，用于指导升级和扩容	是	无	通过机机互联接口，通过Rest/HTTPS获取	最少3个月
云服务的资源信息、运行状态	了解云服务状态，用于升级前后的状态检查以及故障定位前后状态确认	是	无	通过机机互联接口，通过Rest/HTTPS获取	按需或定期均可
云服务性能信息	了解各个云服务负载情况以及容量情况，用于扩容建议和容量风险预警	否	无	通过机机互联接口，通过Kafka消息队列获取	最少3个月
云服务告警信息	了解各云服务的关键告警信息，用于故障定位和风险预警	否	无	被动接收云平台通过Kafka方式的转发告警	实时获取（现场技术支持） 最少3个月（远程技术支持）

- 运维数据全生命周期管理

  当客户选择使用华为云统一运维运营服务时，华为云Stack也部署了多层数据保护机制，保障客户数据的全生命周期的可靠和可用。

  - 有限采集：运维服务仅采集运维数据，不涉及任何客户的业务数据；
  - 安全传输：华为云技术支持中心对接客户VPC环境时，采用安全传输协议HTTPS，以防止数据在传输过程中发生泄露；
  - 可靠存储：运维数据仅在支持中心存储，客户的运维数据不会传出技术支持中心；
  - 管控使用：客户授予运维专家最小使用权限，可有效防护恶意人员的恶意操作；
  - 安全销毁：在客户销户时，华为云运维团队负责对历史数据进行安全擦除，防止数据被恢复；
  - 审计溯源：在提供统一运维运营服务过程中，数据的处理全程均进行了安全审计，确保可追溯取证。

2. **IT安全**

- 人机交互安全设计
  - 支持中心运维团队通过堡垒机接入支持中心，基于堡垒机账号认证授权审计，杜绝了身份管理风险。
  - 支持中心与客户机房侧、运维接入区与华为云Stack管理平面都用防火墙隔离，端口按需开放、禁止高危端口和协议，通信都采用HTTPS、SSH安全协议。客户对本侧的防火墙有完全的控制权，网络隔离保证无法从运维接入区进入客户数据平面，不能从网络侧触碰到客户区业务数据。
  - 支持中心与客户云之间采用VPN/专线/专网连接，采用加密隧道/专线及TLS传输加密技术保证数据传输安全。
  - 客户云对本侧堡垒机有完全的控制权，支持中心运维专家能看什么、执行哪些动作、什么时候接入都能通过堡垒机做最小授权（操作命令白名单）、最短时间授权（按工单操作时间窗），做过什么有审计可录像、可实时旁观。通过授权控制，可禁止技术支持中心运维人员直接登录计算、存储、网络节点，无法从虚拟化侧触碰客户数据。
- 人机交互安全设计
  - 支持中心侧发起推送的升级包都经过恶意代码检测并由华为云签名，软件在安全部署阶段会做验签，确保只有华为云验证通过的软件才能通过技术支持中心安装到客户云端。
  - 技术支持中心与客户云侧机机交互，都经过两侧防火墙，按需开启防火墙策略。
  - 支持中心与客户云之间采用VPN/专线/专网连接，采用加密隧道/专线及TLS传输加密技术保证数据传输安全。
  - 通道透明、可控：
    - 多协议透明封装及转发，通道端口归一；开放HTTPS通信端口，降低攻击面
    - API接口可白名单控制
    - 全量日志存储归档、可审计
    - 敏感数据脱敏

3. **人员安全**

   华为云始终落实网络安全上岗证、安全承诺、员工安全意识教育等措施，持续提升员工安全意识。

   - 网络安全意识教育
     - 日常网络安全意识教育由远程运维中心网络安全负责人组织开展；
     - 网络安全管理团队日常发送警示邮件，如网络安全规范、抵御恶意攻击的操作指导等。
   - 一线赋能
     - 远程运维中心网络安全赋能培训；
     - 运维工程师网络安全知识培训，确保覆盖率100%；
     - 远程运维中心关键岗位上岗证100%落实；

- 例行组织网络安全规范考试。

- 承诺书/保密协议
  - 远程运维中心所有员工及供应商均需签署网络安全遵从协议并遵从远程运维中心网络安全管理规定；
  - 所有远程运维中心员工及供应商都必须签署保密协议，承诺对客户及公司信息保密的约定。
- 员工调动流程
  - 所有离开远程运维中心的员工，包括离职或调离，必须获得所有相关签字确认，如生产电脑资产归还，接入客户网络用的账户删除。

4. **物理安全**

   华为云远程运维中心通过门禁管理系统、视频监控系统、独立区域、防火防断电等物理措施确保运维安全。

   - 独立办公区域
     - 远程运维中心与开放办公区隔离
     - 办公区分为多个不同等级的安全区域进行管理
   - 访问控制
     - 唯一的身份认证门禁卡
     - 根据工作需要赋予访问权限
     - 出入记录
     - 系统报告记录有关事件
   - 视频监控
     - 所有出入口视频摄像头
     - 视频保存在机房的硬盘录像服务器中
     - 只有IT和安全运营中心的人员可以调阅录像
   - 火灾检测和报警
     - 所有办公室和机房安装有消防系统
     - 机房、实验室和IT网络间安装惰性气体自动灭火系统
     - 24*7专职消防员
   - 不间断电源
     - 所有服务器和重要区域有永久电源，保证没有电力中断

5 安全服务及安全解决方案

华为云Stack拥有纵跨IaaS、PaaS和SaaS类多项供客户选择的云服务。致力于为华为云Stack客户业务赋能增值，为其安全保驾护航，华为云Stack还提供了相关的安全服务及安全解决方案供客户选择。

5.1 安全服务

5.1.1 网络安全

1. **虚拟私有云服务（VPC）**

   VPC为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。用户可以通过VPC方便地创建并管理自己的网络，通过配置DHCP执行安全快捷的网络变更；两个VPC可以通过对等连接功能互联；可以使用VPN将VPC与传统数据中心互联，实现应用向云上的平滑迁移。

   VPC提供了以下与客户网络安全强相关的网络功能：

   - 子网：子网是用来管理弹性云服务器网络平面的一个网络，可提供IP地址管理及DNS服务。同一个VPC的所有子网内的弹性云服务器默认均可以相互通信，处于不同VPC中的任意两台弹性云服务器默认禁止通信。
   - VPN：VPN用于在远端用户和VPC之间建立一条安全加密的通信管道，使远端用户通过VPN直接使用VPC中的业务资源。默认情况下，在VPC中的弹性云服务器无法与客户自己的数据中心或私有网络进行通信，如需通信，客户可启用VPN功能并配置VPN相关参数。
   - 云专线：云专线服务是在客户自营的内网本地数据中心与华为云Stack间建立连接的专线网络连接服务。客户可以利用云专线建立华为云Stack与客户的数据中心、办公室或主机托管区域的专线连接，降低网络时延，获得比互联网线路更快速、更安全的网络体验。

   VPC还提供了多项不同Open System Interconnection（OSI）层的网络安全防护功能，客户可以根据其网络安全需求定制配置。另外，VPC也提供了其他网络安全属性，例如IP和MAC绑定、防DHCP Server仿冒、防DoS/DDoS攻击，这些属性是在基础设施层实现的。

2. **安全组（SecurityGroup）**

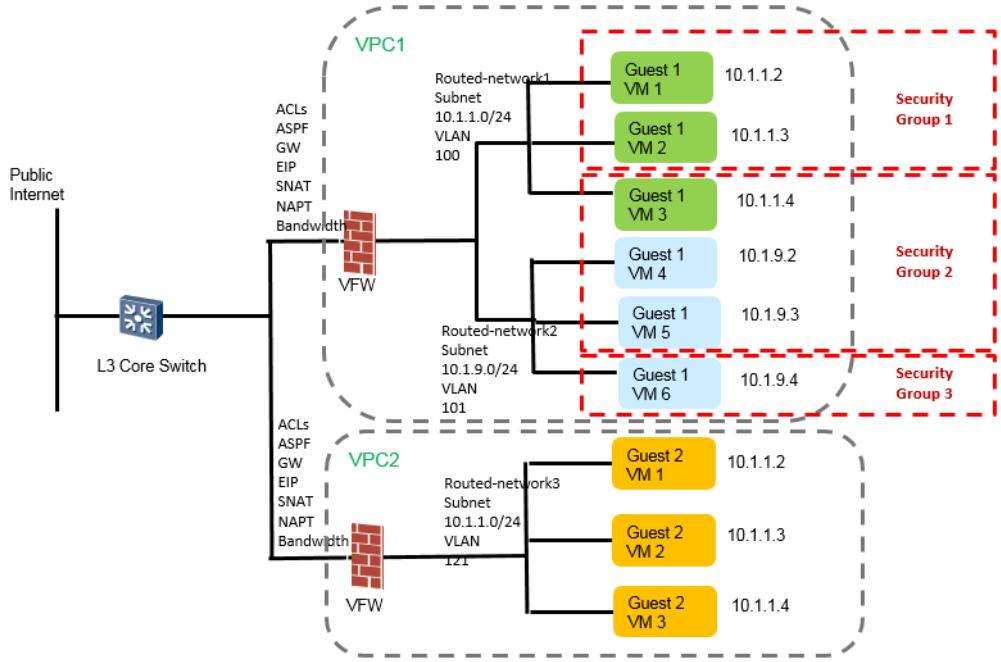
   虚拟机可以加入安全组，安全组用来实现组内和组间的访问控制，加强虚拟机的安全保护，实现VPC内部的网络隔离。安全组通过配置安全规则来控制云主机网络消息的流入流出，只允许授权的消息通过。

系统存在一个默认安全组(default)，当项目管理员创建虚机不指定安全组的时候，系统会自动分配默认的安全组。管理员可以创建自定义的安全组，可以在安全组中定义各种访问规则，当创建一个新的安全组时有以下几条默认规则：

- 允许IPv4出方向访问
- 不允许IPv4入方向访问
- 同一个安全组成员可以互相访问
- 不同安全组成员不可以互相访问

安全组默认的另一个规则是Drop，当报文在一个安全组内不能匹配任何规则时，此报文会被丢弃。

图 5-1 安全组原理图



3. **虚拟防火墙（VFW）**

   虚拟防火墙VFW，用于子网级别的安全防护。防火墙是一个或多个子网的访问控制策略，根据与子网关联的入站/出站规则，判断数据包是否允许流入/流出关联子网。规则匹配的顺序和配置顺序一致。VFW服务的功能如下：

   - 规则匹配域支持：源端口，源IP地址，目的端口，目的IP地址，协议
   - 可以调整规则的顺序
   - 协议支持：TCP，UDP，ICMP，ANY
   - 动作支持：Allow， Deny，Reject（仅Type1支持）
   - VFW支持与子网绑定，一个VFW支持和多个子网绑定，一个子网不能同时加入两个VFW
   - 支持入方向和出方向流量防护

4. **边界防火墙服务EdgeFW**

   边界防火墙EdgeFW，位于内、外部网络的边界处，是连接内网与外网的桥梁。边界防火墙服务提供了严密的访问控制，对内、外部网络实施隔离，保护边界内部网络，对南北向边界提供高级安全保护，例如IPS、AV等，增强了传统边界防火墙所提供的保护。

- 访问控制：支持用户自定义访问规则，策略组是对弹性公网IP的一组访问规则的集合。用户可以自行创建并定义策略组的访问规则或同弹性公网IP的绑定关系。当弹性公网IP与某个策略组绑定后，即受到该策略组的保护。
- 入侵阻断：超过3500+漏洞特征的攻击检测和防御。支持Web攻击识别和防护，如跨站脚本攻击、SQL注入攻击等。
- 网络防病毒：高性能病毒引擎，可防护500万种以上的病毒和木马。

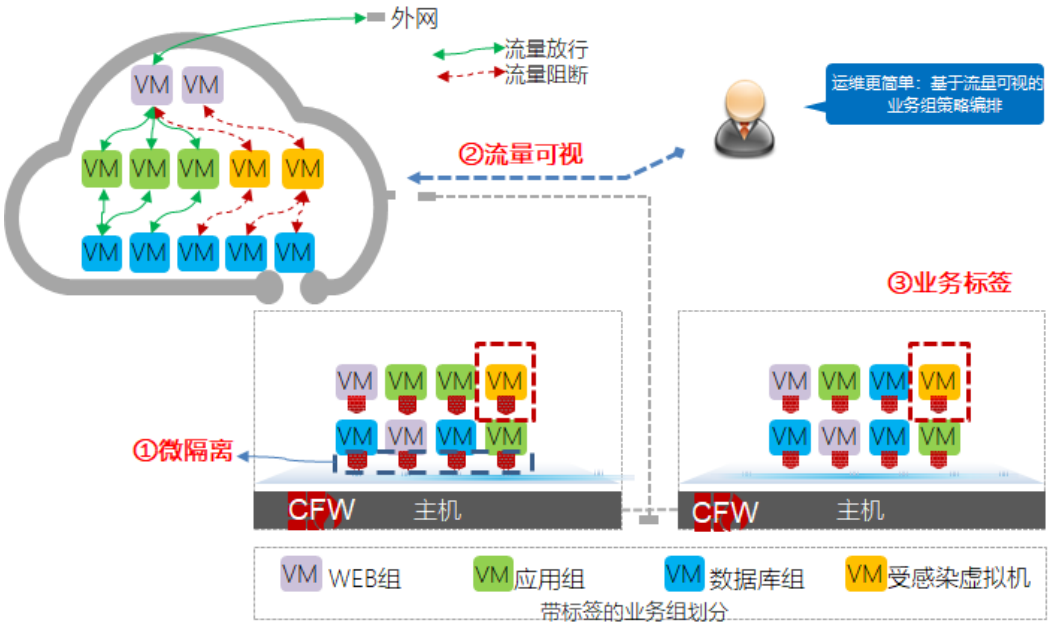
5. **云防火墙（CFW）**

   云防火墙CFW为客户虚拟机（VM）提供微隔离能力，并通过流量可视化、基于业务属性标签的安全策略配置手段来降低安全运维复杂度。CFW只能在Type I场境下使用，不支持Type II和Type III场景，云防火墙服务依赖分布式的IP Tables相关能力实现。

   功能特点：

   - 微隔离：提供VM到VM级细粒度的访问规则配置能力
   - 流量可视：基于拓扑图访问关系辅助用户定义策略
   - 业务标签：基于业务标签进行防护对象定义
   - 安全管理员可以使用云防火墙，为业务提供基于VM粒度的安全防护，基于业务标签来定义安全策略，使用流量可视功能辅助策略配置，从而简化运维复杂度，提升防护效果。

   图 5-2 CFW 逻辑功能视图



5.1.2 主机安全

1. **主机防护服务（HSS）**

   HSS是终端安全防护服务，提供主机入侵防御（HIDS）等安全功能以保障弹性云主机的安全性。功能涉及恶意软件查杀、入侵检测、防火墙、日志审查、完整性监控和 Web信誉等。

- 病毒引擎查杀：为了保证安全防护不对云环境造成影响，主机安全防护组件根植于云主机中，在安全组件的启动和查杀时，会通过管控中心对安全防护组件进行“排队”，避免启动风暴和查杀风暴。
- 云主机防火墙：基于云主机安全防护组件的模式，安全防护组件中的安全策略和云主机无缝绑定，无论云主机漂移至资源池中的任何宿主机均可保证云主机防护策略稳定有效，提供云主机对云主机的访问控制能力。同时可依据用户业务的需要，从IP、端口、协议、方向等方面制定云主机间的防火墙细粒度的访问控制策略，根据安全域的安全标准批量下发给云主机。
- 云主机入侵防御：安全防护组件中的入侵防御功能能够对外部向云主机发起的常见的拒绝服务攻击、缓冲区溢出攻击、木马后门攻击、WEB攻击等进行检测和防护。并针对云主机存在的系统、应用漏洞进行攻击点防护，防止外部对这些薄弱点进行定向攻击。
- 云主机加固：主机安全提供云主机加固功能，一键扫描云主机的安全配置情况及预置功能的安全状态，并提出安全整改意见，客户可使用主机安全组件自动修复这些安全缺陷，也可自行手动整改，保证客户内云主机安全基线一致。同时，对账号提供防暴力破解加固，杜绝任意来源的恶意暴力破解。
- 云主机webshell检测：由于某些云主机需要对外发布web业务，此时云主机暴露在外部环境下极易被植入网站后门或恶意webshell，从而导致网站被挂马、篡改等。因网站后门的潜伏期较长，对云主机系统影响较大，主机安全组件内置云主机webshell检测功能，采用云查杀引擎、启发式引擎、本地智能引擎等多种webshell扫描引擎，结合云端的webshell特征库，每天同步更新后门查杀规则，保证每一个后门第一时间暴露并被彻底查杀，保障网站安全。

5.1.3 应用安全

1. **网页防篡改服务（WTP）**

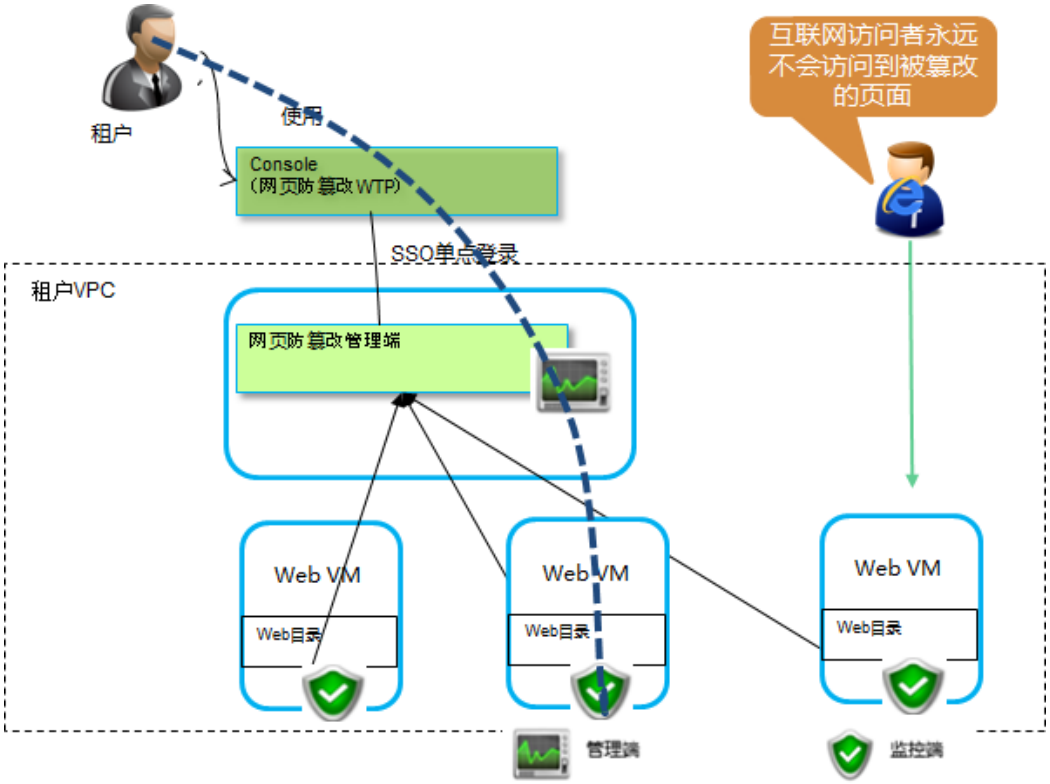
   WTP从系统底层驱动实现多种保护模式，防止静态和动态网站内容被非法篡改，保证网站内容的正确性。

   WTP提供如下功能：

   - 网页文件保护：通过web防攻击模块、防篡改模块（系统内核层的文件驱动），可对动态和静态网页文件进行完美的保护。按照用户配置的进程及路径访问规则，设置网站目录、文件的读写权限，限制文件目录的增、删、改操作行为，确保网页文件不被非法篡改。
   - 集中管理：通过监控端集中管理多台Web服务器，监测多主机实时状态，制定保护规则，接收Web服务器的报警和日志信息。控制Web服务器的启用、关闭、禁用等状态，并可对Web服务器的日志和报警情况做统计分析。
   - 实时报警：对非法篡改行为，系统会自动记录报警日志，并通过手机短信、电子邮件、syslog等多种方式通知管理员。能对网站攻击做到快速响应，及时应变。
   - 管理员权限分级：可对管理员及监控端分配不同的权限组合。
   - 日志审计：提供管理员行为日志，包括时间、事件、操作对象、行为、IP地址等详尽信息，方便区分正常更新过程和篡改攻击行为；支持保护日志查询审计功能；用户不能进行日志修改、删除操作，确保日志的准确性与完整性。
   - 站点文件保持：防篡改模块集成在Web服务器软件中，通过设定各种站点文件访问过滤规则，对多个站点文件或单个站点的文件夹进行保护。
   - 系统信息检测：管理控制端机器能记录所有监控端Web服务器的CPU、内存、硬盘等应用情况，方便管理员根据提供的硬件信息做升级和维护调整。

- 系统自我保护：网页防篡改系统能够实时地保护自己不被非法的删除、修改、卸载等，保证了即使服务器被非法入侵，也不能够对网站进行篡改，不能够对网站管理系统进行破坏。

图 5-3 网页防篡改逻辑原理图



客户申请网页防篡改服务后，会在客户的业务网络拉起承载防篡改管理端的虚拟机，即防篡改安全实例。在防篡改管理端下载相应的防护客户端，部署在需要防护的Web服务器上，配置需要防护的Web目录。在正常使用时，可以登录网页防篡改服务，通过单点登录的模式跳转到网页防篡改的客户端，配置使用。

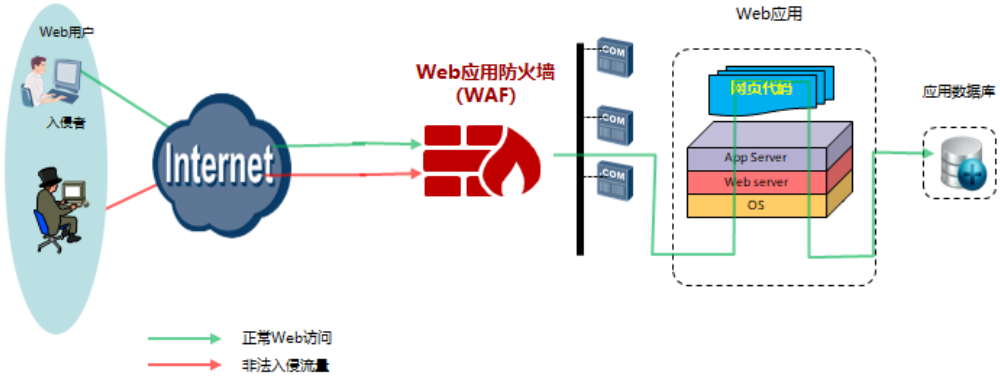
2. **Web应用防火墙（WAF）**

   WAF帮助用户解决面临的Web攻击（跨站脚本攻击、注入攻击、缓冲区溢出攻击、Cookie假冒、认证逃避、表单绕过、非法输入、强制访问）、页面篡改（隐藏变量篡改、页面防篡改）和CC攻击等安全问题。

   WAF的主要功能如下：

   - 防护Web通用攻击：如SQL注入、文件注入、命令注入、配置注入、LDAP注入、跨站脚本等，部署Web应用防护模块后自动屏蔽相应的Web攻击行为。
   - 协议规范性检查：通过HTTP协议规范性检查可以实现Web主动防御功能，如请求头长度限制、请求编码类型限制等，从而屏蔽大部分非法的未知攻击行为。
   - 抗Web扫描器扫描：Web应用防护模块能自动识别扫描器的扫描行为，并智能阻断如Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、WatchfireAppScan、N-Stealth、Acunetix Web Vulnerability Scanner等多种扫描器的扫描行为。

图 5-4 WAF 逻辑原理图



客户申请云WAF服务后，会在客户的业务网络拉起承载WAF的虚拟机，即WAF安全实例。WAF安全实例以反向代理的模式，防护对外提供服务的web服务器（具有EIP的服务器），从使用场景来说，客户申请云WAF服务后，与使用传统安全设备类似，需要登录通过SSO单点登录跳转到第三方的WAF管理平台，配置相应的策略，这部分的策略主要包括两个部分:

- 防护对象的配置：登录WAF服务Console，单点登录到WAF设备Console。在云WAF设备上配置防护的对象，同时需要在云WAF内配置VIP地址与回源IP之间的NAT转换。由于云WAF是反向代理的模式，需要在DNS处将对外服务域名对应的A记录修改为WAF的VIP地址；
- 安全策略的配置：登录WAF服务Console。SSO单点登录到WAF设备Console ,配置WAF使用的安全策略，查看报表、统计等。

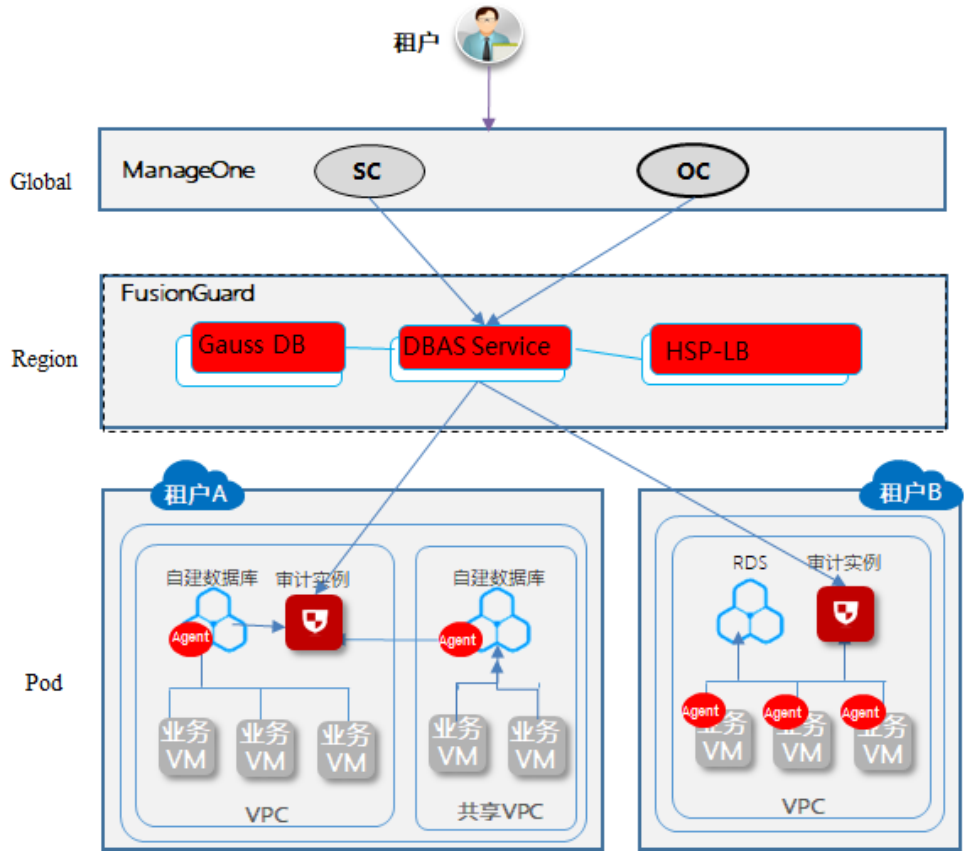
5.1.4 数据安全

1. **数据库审计服务（DBAS）**

   DBAS为用户提供基于ECS/BMS自建数据库、RDS数据库的用户行为发现审计、多维度分析、实时告警和报表等功能，保障云上数据库的安全，满足用户合规要求。

   数据库安全审计采用旁路部署模式，可在不影响用户业务的提前下支持对华为云Stack上的关系型数据库（RDS）、弹性云服务器（ECS）/裸金属服务器（BMS）的自建数据库进行灵活的审计。

图 5-5 数据库审计逻辑原理图



DBAS服务具有以下安全功能：

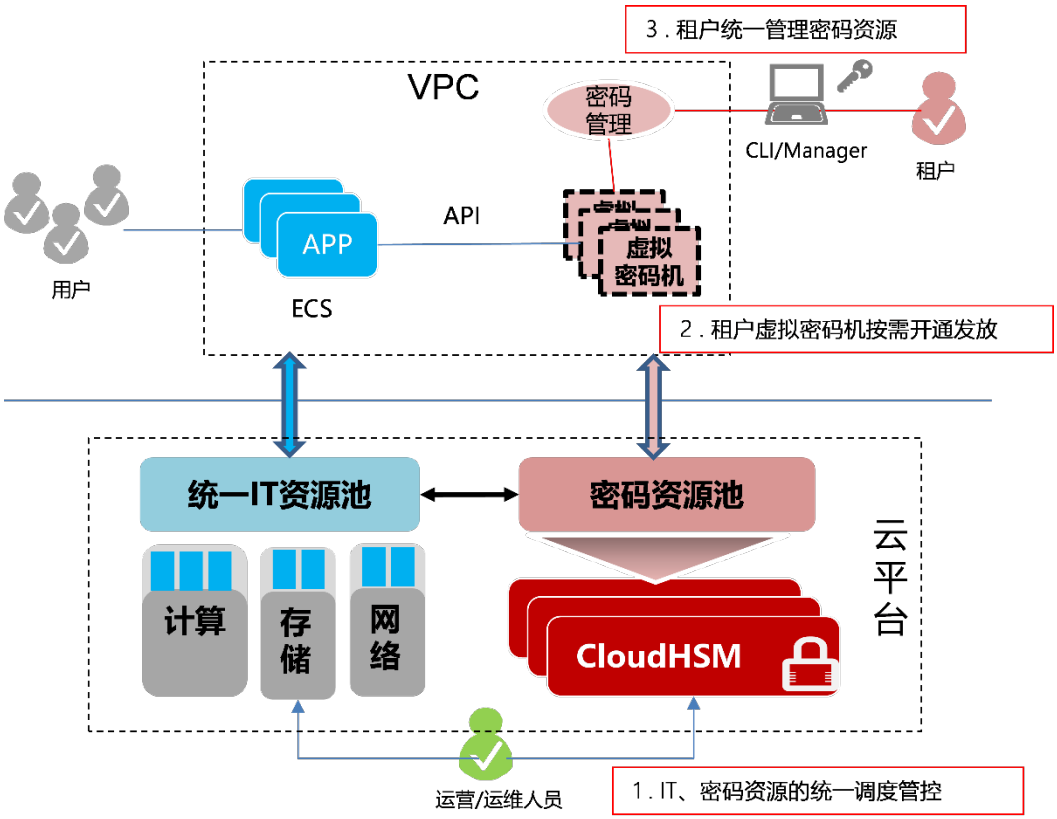
- 审计信息展示：
  - 对Oracle、MySQL、PostgreSQL、SQL Server、RDS等数据库的审计内容包括会话的终端信息、会话的主机信息、会话的其它信息、操作信息等。审计日志至少保留180天。
  - 支持从会话维度、语句类型纬度、风险纬度三个纬度进行导航展示，支持基于时间、客户端IP、目标数据库IP、客户端MAC、目标数据库MAC、操作类型、客户端端口、操作信息大小、返回状态、结果信息、客户端执行命令等详细信息内容。
  - 支持关联应用层和数据库层的访问操作、实现应用端用户身份行为识别。
- 审计报表：
  - 支持（系统级）多数据库聚合报表展现和单数据库综合性报表展现。
  - 支持基于总体概况、性能、会话、语句、风险多层面展现报表。
  - 支持报表定时推动功能，自定义推送周期推送报表文档。
  - 支持多种关联分析，对异常行为提供精细化报表，如会话（客户端和数据库用户）行为报表、风险操作风险分布情况分析报表、合规报表（满足数据安全标准，如Sarbanes-Oxley等）。

- 风险操作、攻击检测及告警：
  - 风险操作（操作类型、操作对象、风险等级等）告警。
  - 能够检测SQL注入（命令特征或风险等级）发现并告警。
  - 系统资源（CPU、内存和磁盘）阈值告警。
  - 支持自定义风险规则。
- 三权分立：
  - 支持系统、安全、审计管理员三员权限分离，并基于云IAM进行统一身份认证管理。
- 隐私数据保护：
  - 用户可以通过内置规则或自定义规则对审计平台（审计日志）存储和展示的敏感信息脱敏；严控个人数据收集、存储。
- 满足国内外合规及认证：
  - 国内：满足网安法、等保三级数据库审计需求，获得公安部《计算机信息系统安全专用产品销售许可证》。
  - 国际：满足Sarbanes-Oxley等国外法案，通过CSA STAR、ISO27001、ISO27017、ISO27018安全认证。

2. **数据加密服务（DEW）**

   DEW基于国家密码局认证的云服务器密码机（CloudHSM），构建虚拟化密码资源池，实现IT、密码资源统一调度管控，为用户按需提供虚拟密码机（VSM）的服务，支持政务、金融、公安等行业客户的云上密码服务及国密改造需求。解决了加密机入云、密码及IT资源统一调度、自动化管维的问题。

图 5-6 DEW 逻辑原理图



数据加密服务基于云加密机在云平台侧实现了虚拟化密码资源池的构建，并可统一调度管理密码资源，实现IT、密码资源的统一调度分配，支持对虚拟密码资源的配置、操作、漂移、升级等。客户在数据加密服务界面，可按需申请相应的VSM资源，服务自动化将VSM设备映射入客户VPC，同时管理员将所需的管理、备份Ukey发放给用户。用户持Ukey登录管理配置工具，远程初始化、配置VSM，并完成应用改造接入，实现应用对加密服务调用。客户可在服务界面进行VSM的申请、维护、关闭等，也可登录管理配置工具对名下所有密码设备、密钥进行统一管理和配置。

DEW服务具有以下功能：

- 密码资源池的统一调度：
  - 实现密码资源池管控系统，基于CloudHSM构建密码资源池
  - 支持对CloudHSM、VSM自动化配置、操作、漂移、升级等
  - 支持对密码资源池统一监管、分配、运维、告警处置等
  - 支持VSM集群集容量：>10240
- 客户按需动态开通VSM：
  - 支持客户自动化开通、配置、关闭VSM资源；
  - 支持客户VSM资源总览、性能查看、VSM资源查看等；
  - 单VSM加密性能规格：并发连接数64、256位SM2签名速度 ≥ 3200次/秒、 SM4加密/解密速度 ≥ 4000次/秒、 SM3杂凑计算性能≥ 4500次/秒

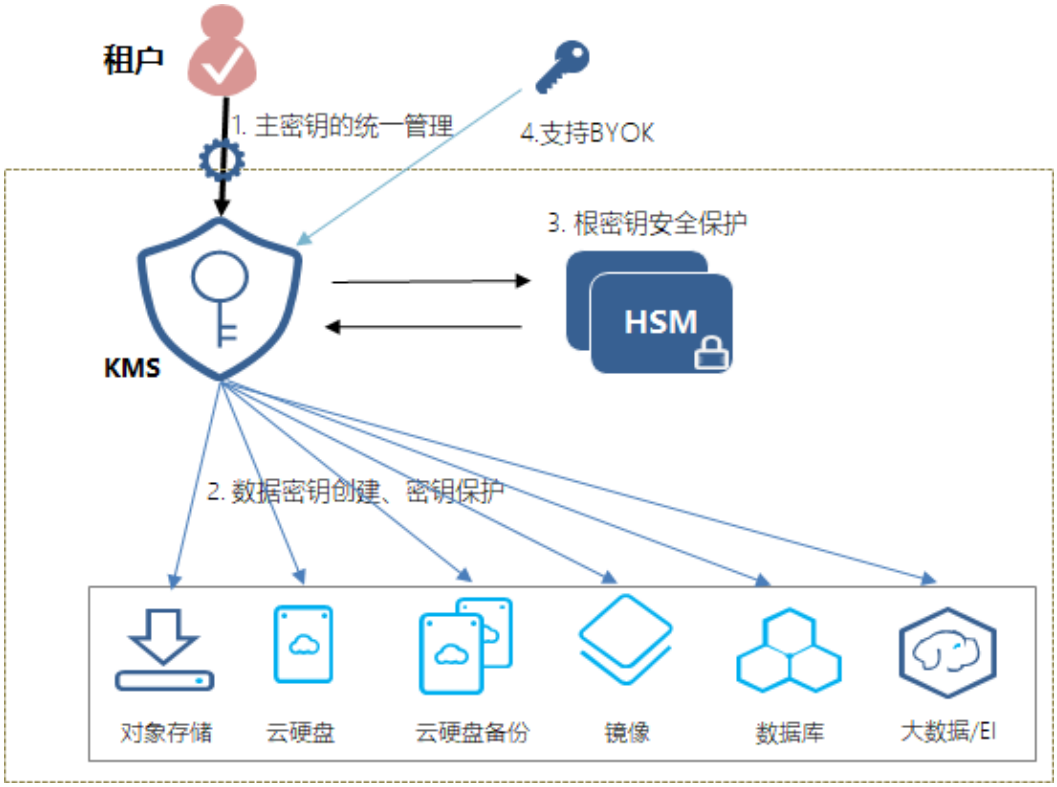
- 将VSM的安全接入客户VPC：通过网络映射，将VSM接入客户VPC，实现加密机的本地调用，保障VSM的使用、管理安全。
- 客户密码资源统一管理：支持客户统一管理名下的所有密码设备、密钥资源。

当前华为云Stack数据加密服务支持的云服务器密码机型号为兴唐通信SJJ1811、卫士通SJJ1744，设备均支持国密算法（SM2、SM3、SM4等），并获得国家密码局认证。

3. **密钥管理服务（KMS）**

KMS为平台云服务、客户业务应用提供一种安全可靠、简单易用的密钥托管服务，其密钥安全由硬件安全模块 (HSM) 保护，帮助用户集中管理密钥生命周期安全。解决了云服务加密密钥安全创建、客户密钥统一管理的问题，当前已支持OBS、DWS、DAYU服务集成加密功能。

图 5-7 KMS 逻辑功能图



用户可登录KMS系统，对客户主密钥进行全生命周期管理，包含创建、启用、禁用、删除、轮转、别名、修改用户主密钥等。对于集成了KMS加密的OBS服务，用户登录OBS服务时，可以选择“KMS 加密”加密文件，自动对上传文件加密并保存在云端，下载时自动解密。

KMS服务具有以下安全功能：

- 密钥生命周期管理：
  - 支持根密钥保护，基于硬件HSM根密钥保护
  - 支持客户创建、启用、禁用、删除、轮转、别名、修改用户主密钥
  - 支持各服务、应用创建、加密、解密数据密钥

- 支持AES 256、国密SM4两类对称密钥的创建和管理

– 云服务集成加密支持：

- 对象存储服务（OBS）集成：一键开通文件加密功能，对上传/下载OBS文件进行服务端加密/解密，1个文件1个密钥
- 智能数据湖运营平台（DAYU）集成：创建MRS Hive、MRS HBase、DWS、DLI、MySQL、SparkSQL、RDS等数据连接时，自动调用KMS创建数据密钥加密数据连接口令等
- 数据仓库服务（DWS）集成：服务创建数据表时，自动调用KMS创建数据密钥加密数据表

– 密钥安全管理：

- 密钥轮转：用户可按需对主密钥进行轮转（支持轮转周期7天-1095天）
- 密钥授权：支持按需密钥授权

– 自主密钥导入（BYOK）：用户根据KMS提供的API接口导入用户自己生成或获取到的用户主密钥。

– 小数据加密：少量数据（如口令、证书等）需要加解密时，可利用KMS在线工具完成。

当前KMS已与国内主流的加密厂商HSM设备型号适配：支持江南天安SJJ1310、三未信安SJJ1212。

5.1.5 安全管理

1. **安全指数服务（SIS）**

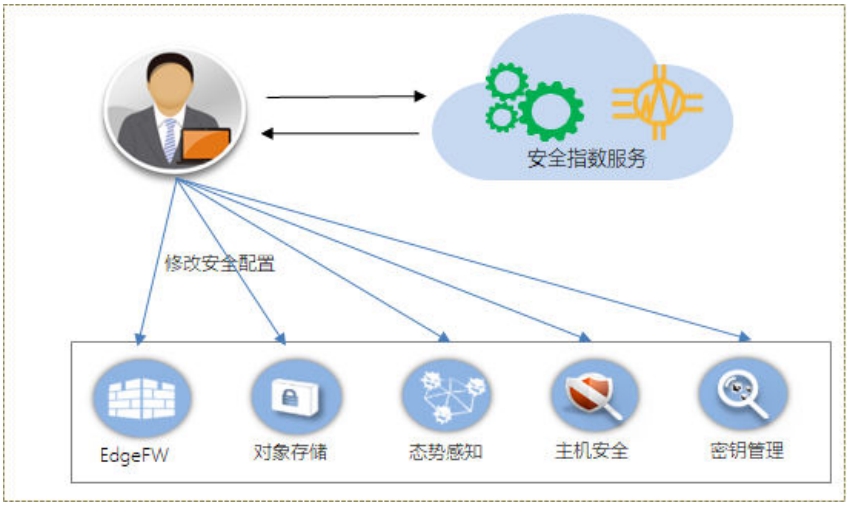
   安全指数服务SIS是关于云环境的一个安全评估服务，为用户提供统一、直观、多维度的安全视图。用户可以通过安全指数服务了解所使用云环境是否已合理配置，所采取的安全措施是否已经足够，以及主动安全、被动安全的概况。

   – 安全体检：从身份鉴别、访问控制、入侵防范、资源控制、备份恢复、数据安全几个维度对用户的云环境进行评估，根据最佳实践对不安全的配置提出修改建议，并提供快速修复的链接。

   – 合规报告：根据等级保护规范的技术要求，从安全计算环境、安全通信网络维度对用户的云环境进行检测，提供合规检测报告，辅助用户做等保评估。

   – 对云服务配置进行检查，依赖OBS、SSA、VPC、BMS、ELB、HSS、VDC、ECS、CSBS、CSDR、KMS、DEW、EdgeFW、CFW等服务。

图 5-8 安全指数逻辑原理图

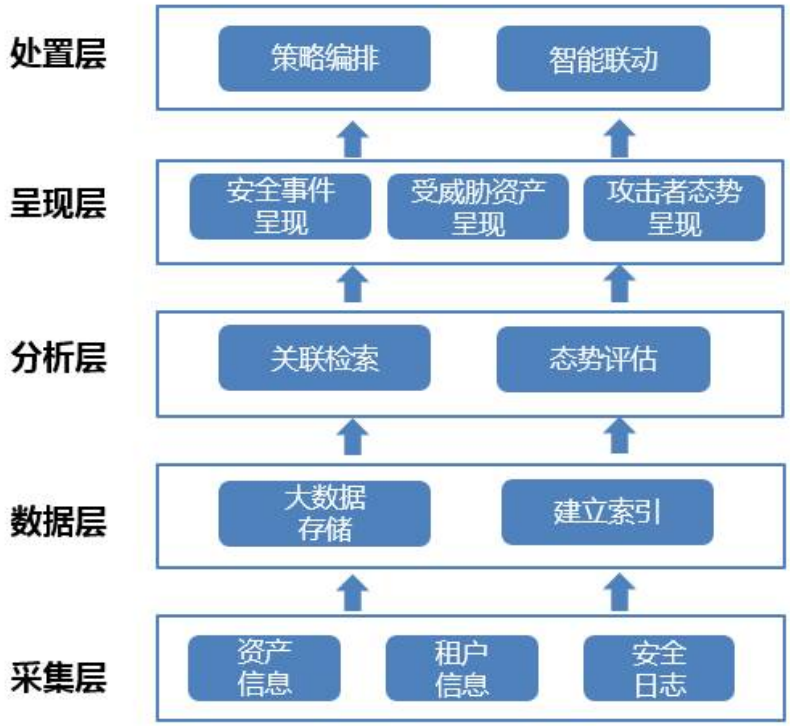


2. **安全态势感知（SSA）**

   安全态势感知服务SSA能够帮助用户理解并分析其安全态势，通过收集其他各服务授权的海量数据，对用户的安全态势进行多维度集中、简约化呈现，方便用户从大量的信息中发现有用的数据。同时，结合大数据挖掘和分析技术，提供全覆盖的从攻击者分析到全局分析的能力，帮助用户准确理解过去发生的每一件安全事件，以及预测将来有可能发生的安全事件。

   - 安全态势总览：按不同的维度统计用户每一天内的受攻击次数、发现弱点次数和感染病毒的次数，以及一周被攻击统计分布。
   - 用户安全态势：站在用户资产的角度，分别从威胁、弱点、主机病毒三个维度帮助用户理解其资产是否易受攻击、资产的受损程度和受损过程。
   - 攻击者态势：利用大数据技术分析攻击事件之间的关联，识别出不同攻击者的行为特征，从攻击者角度分析其攻击规模、攻击手段、活跃时间，帮助用户分析不同的攻击者以进行有针对的防范。
   - 安全联动处置：与云防火墙服务联动，对于受威胁资产进行一键隔离及一键恢复。

图 5-9 安全态势感知逻辑视图



安全态势感知服务使用其他安全服务作为数据源，依赖边界防火墙服务、及网络安全智能系统的流量探针（CIS）。同时依赖云防火墙服务进行安全联动处置。

3. **云堡垒机服务（CBH）**

   客户的各个VM的运维同样必须要有严格的访问控制与授权、并能够对登录操作记录、审计、回溯。传统堡垒机无法直接部署到云内客户的网络中，而虚拟化的云堡垒机可以灵活部署在客户网络中，对运维人员进行统一认证、单点登录、授权、操作审计等。

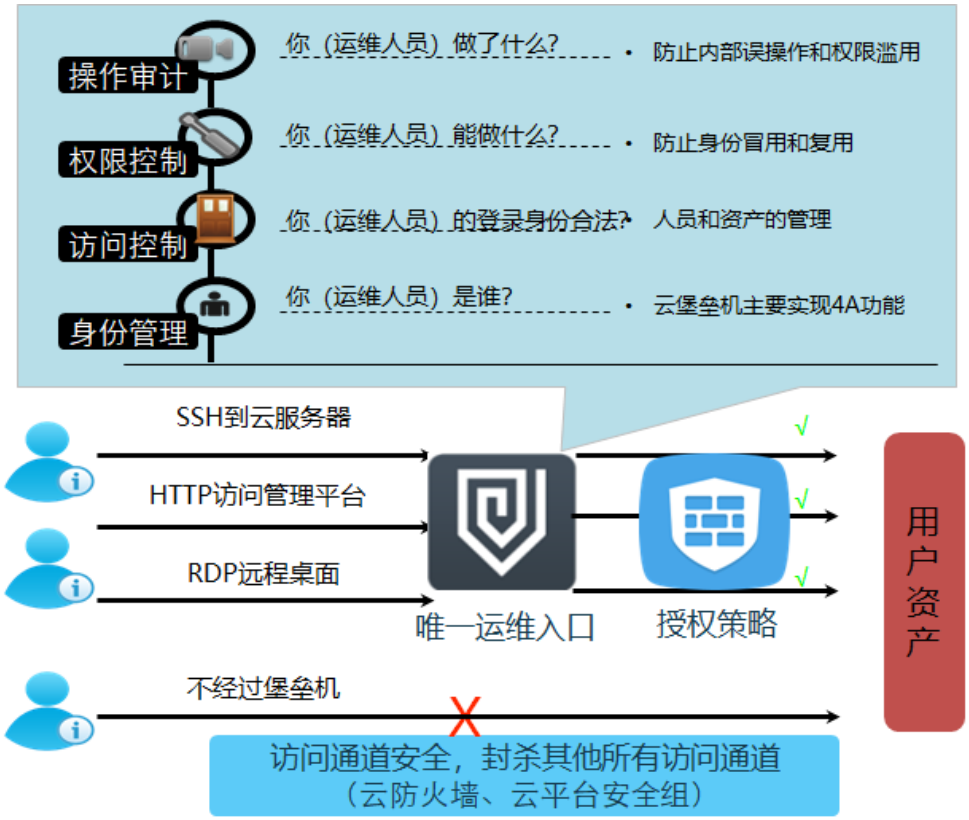
   CBH为客户VM提供账号管理、身份认证、自动改密、资源授权、实时阻断、同步监控、审计回放等能力，增强运维管理的安全性，具备强大的输入输出审计能力。

   云堡垒机服务提供如下功能：

   - 支持大部分运维途径的审计：云堡垒机服务实现了对以SSH、TELNET、FTP、SCP、SFTP、远程桌面RDP、VNC、HTTP、HTTPS、Oracle、MS SQL、DB2、Informix、MySQL等应用协议的集中管理与审计。
   - 实现运维人员、资产、权限的集中管理：部署云堡垒机后可以实现所有运维人员、云主机、安全设备、云数据库的集中管理。结合防火墙访问控制等措施可以确保云堡垒机是所有运维的唯一通道，确保所有运维人员的操作行为能够完整审计和控制。
   - 精细化的访问控制：云堡垒机将访问控制分成了运维授权、运维策略。（1）运维授权：是指运维用户和资产、应用之间的权限关系，即指定某个运维管理员可以管理哪些资产IP、账号。（2）运维策略：是可以给运维管理员可管理的资产实现更加精细化的控制，包括运维来源的IP范围、运维时间段的控制、特殊命令的审批、阻断等。

- 独具特色的审计分析能力：CBH可以完整记录运维管理员的运维过程，哪个账号通过哪个IP地址登陆了什么设备、在设备上面做了什么操作、目标设备的返回结果都会完整记录。

图 5-10 云堡垒机功能原理图



4. **漏洞扫描服务（VSS）**

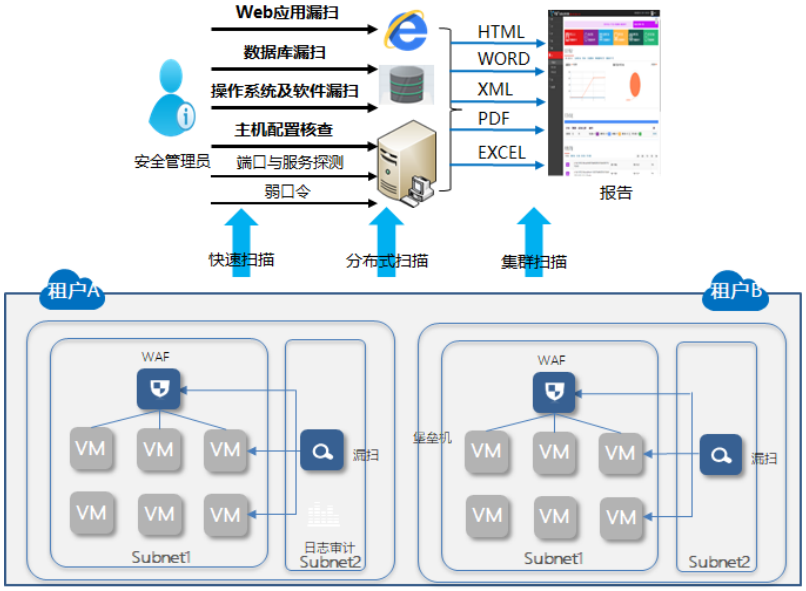
   VSS是一种主动的防范措施，能够对网络设备、操作系统和数据库等平台部件进行扫描，找出有关网络的安全漏洞及被测系统的薄弱环节，并针对监测到的安全隐患给出相应的修补措施和安全建议，从而消减系统的脆弱性，避免黑客攻击行为，做到防患于未然。

   VSS为客户VM提供Web、数据库、基线核查、操作系统、应用软件的安全检测为核心，弱口令、端口与服务探测为辅助的综合漏洞探测能力。

   VSS提供如下功能：

   - 分布式集群管理模块：漏洞扫描服务集成了Web扫描、系统扫描、基线核查、数据库扫描等。
   - 统计报告控制体系：统计报告控制体系致力于给客户更好的交互体验、更丰富的统计数据、更多维度的对比信息、更精致规范的报告内容。除了美观、大方、规范以外，统计报告内容同样支持用户自定义，极大程度上丰富了可用性与易用性。并且支持主流报告格式，包括：HTML、XML、PDF、WORD、EXCEL。

图 5-11 VSS 逻辑原理图



5.2 安全解决方案示例

5.2.1 政企大数据安全体系规划建设咨询服务

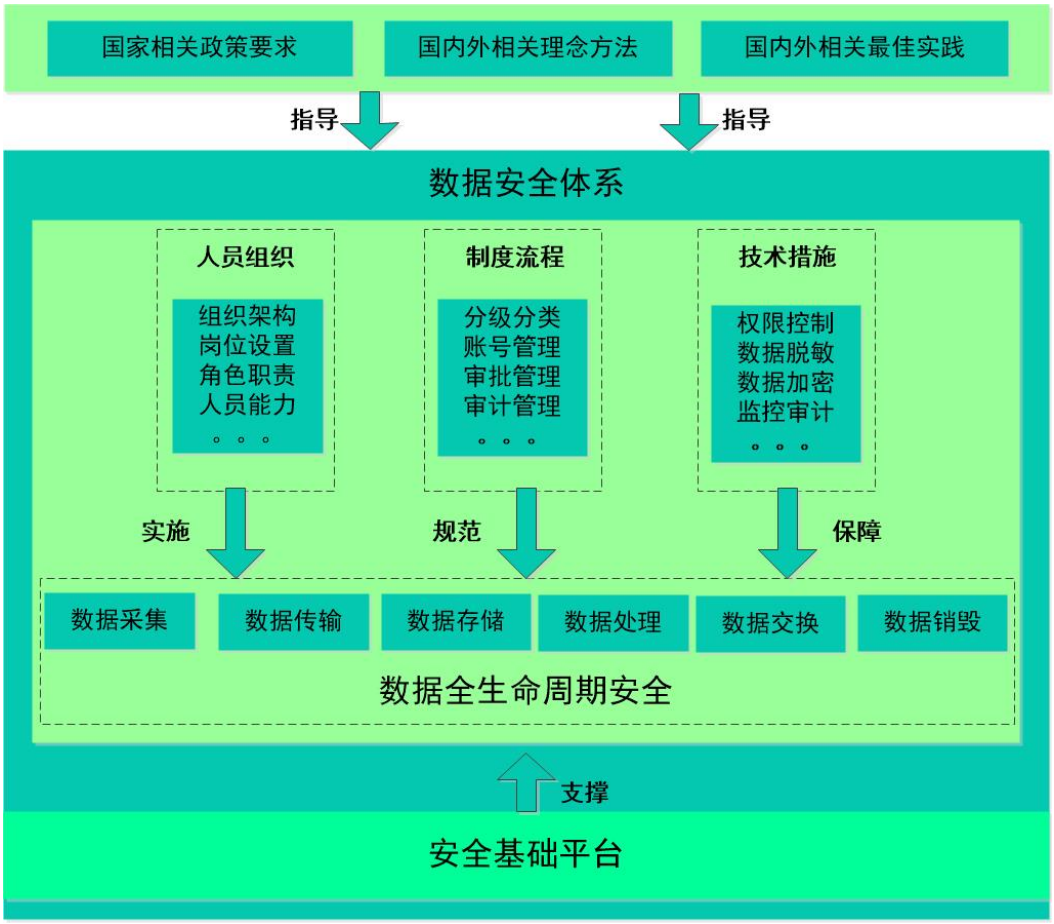
随着大数据发展，以及出于便民目的，政企大数据平台建设逐渐趋于流行，在此过程中，数据安全风险成为各大政企对于大数据安全平台的主要担忧。华为云为政企客户大数据平台提供数据安全体系规划建设咨询服务。

政企大数据安全体系规划建设咨询服务基于华为云Stack的主要安全能力，围绕“让大数据应用更安全”的愿景，覆盖数据安全防护、敏感信息管理、数据安全合规三大目标，实现对数据的保护。

1. **数据安全体系规划建设设计思路**

   政企大数据安全体系规划建设咨询服务以数据安全为核心，以数据的全生命周期为各个安全过程域，从组织人员建设、制度流程和技术措施三个维度对大数据中心的数据安全防护能力进行评估，进而全面了解目前的数据安全管理运行现状，并以此来规划设计切合政企未来大数据业务开展且可落地、可实施的数据安全保障体系，并同步编制配套相关的规章和标准，从而发挥安全对政企大数据业务健康发展的保障作用。

图 5-12 总体思路框架



2. **数据安全体系规划建设咨询服务交付内容**

   咨询服务交付具体分解为以下工作阶段，各阶段工作内容如下：

   - **调研评估阶段：**收集国家与政企建设相关的信息安全政策、法规和标准，以及国内外政务数据共享开放的最佳安全实践，提取价值内容，梳理和编制安全评估访谈问卷、现状调研表，对大数据中心、相关委办局和服务支撑单位进行调研评估，并汇总分析后形成对政企大数据中心的数据安全评估报告。
   - **规划设计阶段：**根据对政企大数据平台的数据安全现状评估结果，从政企开展数据共享开放业务的自身需求出发，规划设计适用于政企数据资源共享开放业务的数据安全防护体系。数据安全防护体系主要从政策标准、组织人员建设、制度流程和技术支撑等方面进行设计，并明确数据安全体系各部分的内容、所起的作用以及相互的关系。
   - **配套规章标准编制阶段：**根据数据安全体系规划的内容，编制政企数据安全方针政策、规章、标准体系和相关指南，规范和约束大数据平台的数据共享和开放工作，指导各级部门有效落实数据安全保障工作。

6 结语

随着云计算服务的不断发展，为了平衡其本地业务的稳定性和安全性以及新科技快速发展带来的新的机遇，越来越多的企业将其本地数据中心业务延伸至云上。随着新模式的出现，华为云也相应提供了华为云Stack来顺应企业的需求。面临复杂多变的网络环境及安全挑战，华为云遵从华为云Stack责任共担模型，依托华为特有的软硬件全栈技术优势，打造可信的解决方案，与客户共同构建华为云Stack环境的安全能力。

华为云以数据保护为核心，以安全工程为基石，提供满足全栈、全生命周期安全的产品和服务，以合规治理为城墙，对标全球化的权威标准与能力要求，实施完善的安全治理体系，让客户可以放心地使用华为云Stack解决方案，并在该解决方案上开展业务。在保障数据安全的同时，开放华为多年积累的AI及大数据处理能力，为客户创造价值，实现华为云和客户的双赢。籍此白皮书，将华为云Stack的安全设计理念以及华为云在安全领域的丰富实践和经验，分享给客户，分享给业界。也希望籍此，客户可以更加了解华为云Stack的安全能力，从而可以与华为云一道建立一个更加安全可信的华为云Stack环境。

参考资料：

[1]**https://cloudsecurityalliance.org/artifacts/hybrid-clouds-and-its-associated-risks**

[2]**https://www.mordorintelligence.com/industry-reports/hybrid-cloud-market**

[3]**https://www.forrester.com/report/The+Forrester+Wave+Hybrid+Cloud+Management+Software+In+China+Q3+2021/RES161519**