华为云服务
– 云安全服务

HUAWEI

目录

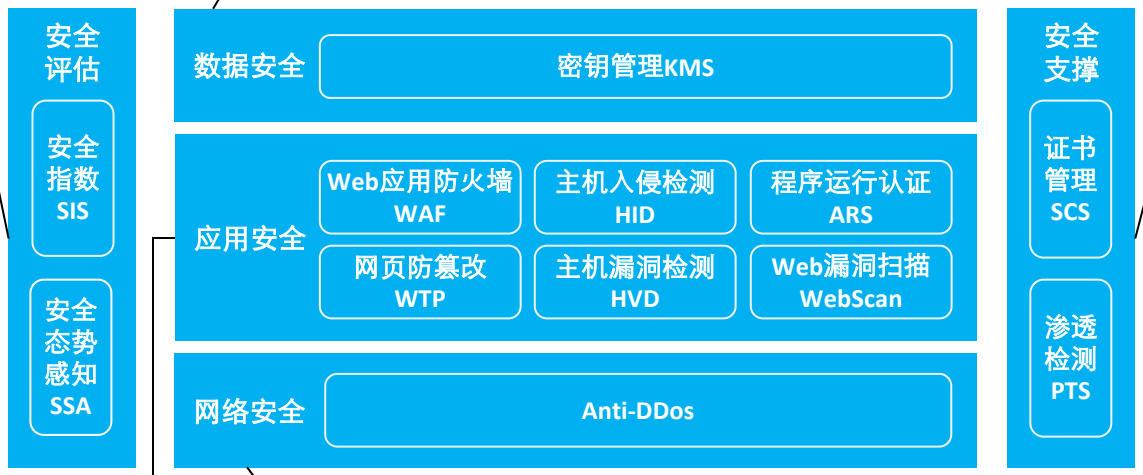
云计算安全问题与安全需求

- 数据与服务外包是云计算的特点，带来新的安全问题
  - 数据外包是指数据的产生、使用、存储、销毁等都在远端的云计算系统中，用户失去数据控制权，引发数据与隐私保护的安全问题
  - 服务外包是指应用服务部署在远端的云计算系统中，用户失去物理资源控制权，引发云应用的安全问题
- 机密性、完整性、可用性仍然是云计算的安全需求
  - 机密性要求云计算系统应能够有效保护用户数据
  - 完整性要求云计算系统应能够保证数据与服务不被伪造、篡改、删除
  - 可用性要求云计算系统在被攻击时的数据可用与应用可持续服务

云计算安全服务的核心目标

- 为用户在云上的数据与服务提供完整的安全解决方案，确保数据与服务的机密性、完整性与可用性是云安全服务的核心目标
  - 云安全服务为数据提供全生命周期保护
  - 云安全服务为应用提供运行环境（应用、系统、网络）保护
  - 云安全服务由一系列服务组成，每个服务既能独当一面，也能相互协作
  - 云安全服务能够分析和评估数据与服务的安全现状，为用户选择实施安全服务提供指导
- 云计算安全服务不提供云计算平台的安全保障

云计算安全服务的产品组成



数据安全

作为云安全服务的密码体系，为云计算环境下的用户数据应用、存储等提供机密性，完整性保障

安全评估

作为云安全服务的评估体系，为云计算平台与云技术应用提供科学、可用、实时的安全分析与安全评估能力，指导用户进行安全能力建设

安全支撑

作为云安全服务的有益补充，支撑系统的总体安全能力，让安全体系更加完善

网络安全

作为云安全服务的重要组成，实现网络隔离，应对网络攻击，保障网络安全

应用安全

作为云安全服务的重要组成，从操作系统与应用程序安全防护角度保障弹性云计算服务器及在其中运行的云计算应用的安全

云计算安全服务产品列表（1/3）

安全服务	所属类别	服务描述	主要功能	应用场景
Anti-DDos	网络安全	Anti-DDoS流量清洗服务（以下简称Anti-DDoS）是对IP地址进行DDoS（Distributed Denial of Service）攻击防护的一种网络安全服务	1. DDos攻击防护 2. 为单个IP地址提供监控记录 3. 为保护的IP地址拦截报告	1. 中小企业门户网站保护 2. 手游、页游、APP开发者及电子商务等初创公司的网站保护 3. 大中型企业出口安全防护
WAF	应用安全	Web应用防火墙是一种Web安全防护服务，通过对HTTP请求进行检测，实时拦截跨站脚本攻击、SQL注入攻击、漏洞入侵等黑客攻击，防止黑客利用应用程序漏洞入侵渗透，避免用户的数据泄露，保护弹性云服务器Web应用程序安全	1. Web攻击防护 2. 防护日志记录 3. 防护情况统计	1. 数据泄露防护 2. 网页篡改挂马防护 3. DDoS联合防护
HID		主机入侵检测用于检测弹性云服务器（ECS）是否遭受暴力破解攻击、是否存在异地登录、是否存在攻击弱点等，并基于检测结果提供安全分析报告。用户可根据报告加固ECS，提升安全性，降低安全风险	1. 暴力破解检测 2. 异地登录提醒 3. 弱口令检测 4. 数据库进程权限检测 5. 网页后门文件检测 6. 手动扫描 7. 安全检测报告	1. 主机系统安全配置优化与加固 2. 系统网络安全防护

云计算安全服务产品列表（2/3）

安全服务	所属类别	服务描述	主要功能	应用场景
HVD	应用安全	主机漏洞检测用于检测弹性云服务器（ECS）的是否存在安全漏洞，在漏洞被利用之前发现漏洞并修补漏洞，防患于未然，提高系统的安全性	1. 定期检测扫描弹性云服务器漏洞 2. 提供漏洞检测报告 3. 提供24小时内漏洞检测扫描结果	1. 运营网站上线前自测 2. 系统安全评估 3. 加固后评估
WTP		网页防篡改用于保护部署在弹性云服务器（ECS）上的Web站点，防止黑客、病毒等对站点目录中的网页、电子文档、图片、数据库等文件进行非法篡改和破坏，保障网站的安全性	1. Web站点文件保护 2. 告警信息记录 3. 防护详情统计	Web网站文件保护
ARS		程序运行认证服务是一个智能的进程管理服务，基于可定制的白名单机制，监视程序的执行，保障弹性云服务器的安全性	1. 本地进程信息列表 2. 设置进程状态 3. 查询历史进程信息	1. 云服务器进程监视 2. 云服务器进程状态标识
WebScan		Web漏洞扫描用于检测云服务器漏洞	1. 通用Web漏洞检测 2. 第三方软件漏洞检测 3. 指纹识别 4. 漏洞修复建议	Web弹性云服务器检测漏洞
KMS	数据安全	密钥管理服务是一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥安全	1. 管理用户主密钥 2. 创建、加密、解密数据加密密钥 3. 生成硬件真随机数	1. 用户个人数据加解密 2. 业务核心数据加解密 3. 关键信息资产加解密

云计算安全服务产品列表（3/3）

安全服务	所属类别	服务描述	主要功能	应用场景
SIS	安全评估	安全指数服务是一个评估用户云计算环境配置是否合理，安全措施是否足够，以及主被动安全概况，并为用户提供统一、直观、多维度的安全视图的安全服务	1. 安全等级评估 2. 主动、被动安全概况 3. 安全配置评估 4. 安全服务配置快速入口	用户云环境安全评估
SSA	安全评估	安全态势感知服务是一个基于大数据挖掘及机器学习技术，为用户全面智能分析安全态势状况，精准把握云服务器安全	1. 安全态势总览 2. 用户视角安全态势分析 3. 攻击者视角安全态势分析 4. 云平台全局态势 5. 实时安全情报搜集	云计算环境安全评估
SCS	安全支撑	证书管理服务是华为联合全球知名数字证书服务机构，为您提供的一站式安全套接层（SSL）证书和传输层安全（TLS）证书的全生命周期管理服务	1. 云端证书申请与管理 2. 集成云应用与证书服务	1. 企业应用可信认证 2. 企业网站可信认证 3. 应用数据传输保护
PTS	安全支撑	渗透测试服务是一个渗透测试服务单管理平台，用户可以通过该服务创建渗透测试服务单，平台以邮件形式将其传给第三方安全公司处理	1. 第三方测试机构推荐 2. 创建与管理服务单	基于第三方的增强系统安全渗透测试

华为公有云安全服务申请与使用

- 华为公有云提供统一安全服务管理平台
- 用户可根据自身的安全需求开通适合的安全服务
- 安全服务可单独使用，也可组合使用
- 安全运行日志可在“安全审计”（位于“管理与部署”分类）中查询
- 安全告警可根据用户需求通过短信、邮件等方式提供

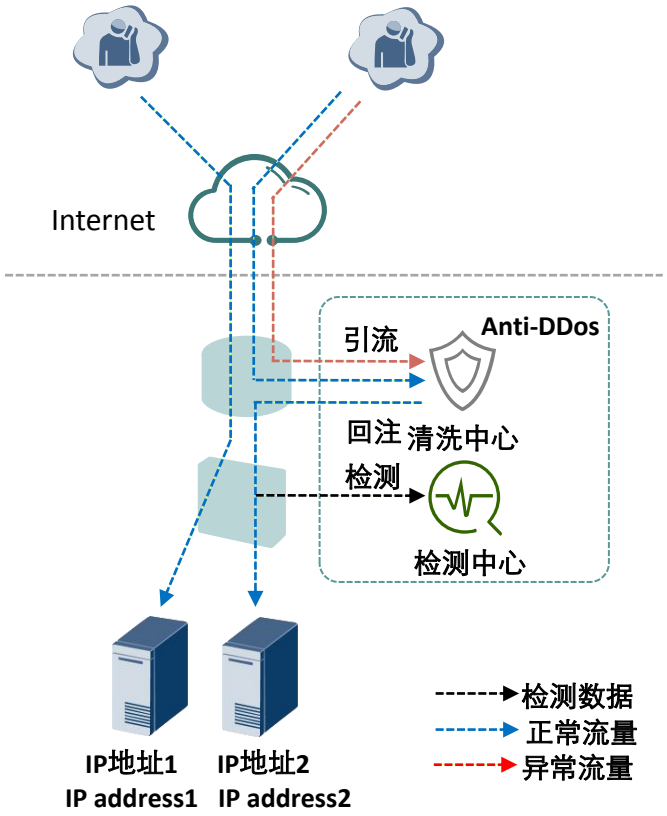
目录

1. 华为云安全服务基础
2. **华为主要云安全服务介绍**
   - Anti-DDos服务
   - Web应用防火墙服务
   - 安全态势感知服务
   - 密钥管理服务

云安全服务 — Anti-DDos

Anti-DDos为用户提供高可靠、高安全、按需使用、弹性扩展的DDoS攻击防范服务，保障用户弹性云服务器的可持续运行

部署架构与工作原理



Anti-DDoS设备部署在网络出入口

检测中心根据用户配置的安全策略，检测网络访问流量

当发生攻击时，将数据引流到清洗设备进行实时防御，清洗异常流量，转发正常流量

可防范的攻击类型

1. **抗流量型攻击：**SYN flood 、SYN-ACK flood、ACK flood、FIN/RST flood、UDP flood、IP Fragment flood、Stream flood等
2. **抗应用型攻击：**Web cc攻击、URL防护、Connection Flood、HTTPS Flood、HTTP Get Flood、HTTP Post Flood等

可防范的攻击规模

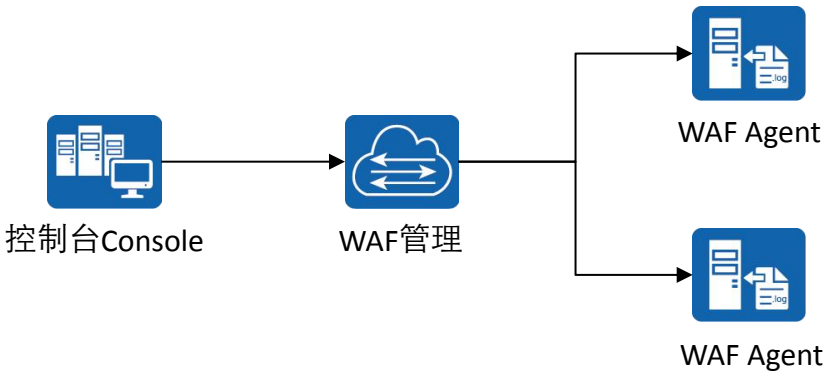
1. 防护能力≥2Gbps
2. 传输延迟≤30微秒
3. 每秒新建连接≥10万

注：华为云可根据业务要求不断提升服务的功能性能

云安全服务 — WAF

Web应用防火墙是通过执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护的应用安全服务

产品架构与工作原理



Agent代理部署在用户虚拟机中，实时监控L7的网络数据

Agent根据攻击特征库，过滤拦截网页木马，防止资源盗用

WAF管理接收Agent上报的工作信息

Console为用户提供可视化的WAF防护信息

关键特性

1. 防SQL注入、防XSS攻击：采用主动防御引擎，基于攻击特征库过滤用户输入，防止SQL注入，屏蔽恶意攻击
2. 防Webshell上传：深入分析POST内容，对上传数据进行比对，主动拦截网页木马
3. 防盗链：通过设置Cookie和校验Referer字段保障网站文件和流量资源的正常使用，防止非法盗用

主要参数

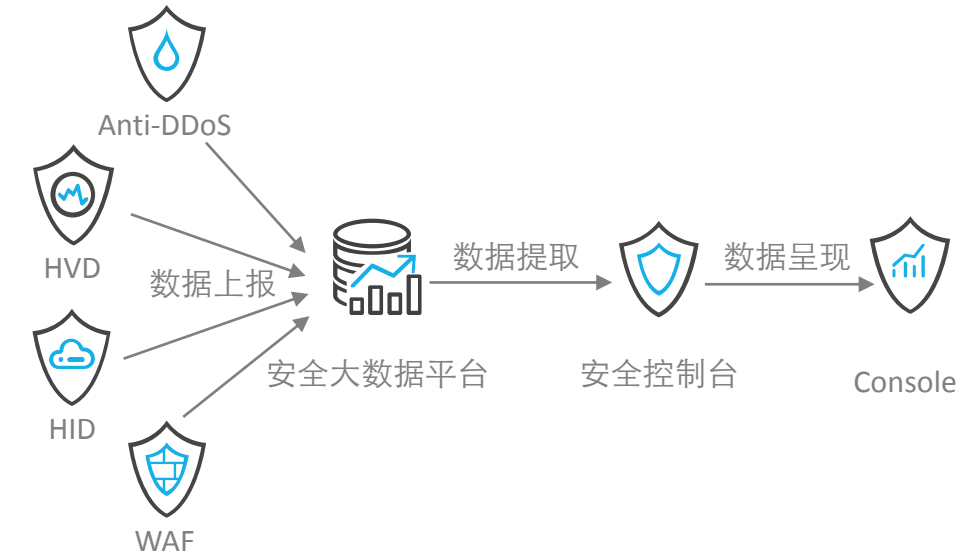
1. 支持的Web服务器类型：
   Windows：IIS6.0及后续版本
   Linux：Apache2及后续版本
2. 支持的HTTP/HTTPS协议解析

注：华为云可根据业务要求不断提升服务的功能性能

云安全服务 — SSA

安全态势感知服务能智能识别入侵手段和攻击手段，为用户提供专业的数据分析结果，帮助用户发现潜在的威胁

工作原理



安全大数据平台基于爬虫技术，从其它安全服务提取安全日志

安全大数据平台基于大数据技术，分析安全日志，形成安全报告

安全控制台基于Console提供的用户请求从大数据平台提取数据

Console为用户提供可视化的安全态势分析结构

服务特点

1. 基于大数据技术的可视化的安全评估与安全管理工具
2. 分别从用户视角和攻击者视角分析用户弹性云服务器面临的安全威胁、安全弱点，以及被攻击的情况
3. 通过采集安全情报，分析云平台面临的安全风险趋势，以便提前作出防范措施
4. 可指导用户的安全体系规划建设

注：安全态势感知的报表说明可参见相关用户手册

云安全服务 — KMS

密钥管理服务能够在云端为用户提供符合国家（地区）、行业标准规范的，高安全性的密钥产生、传输、使用、存储、销毁的全生命周期管理能力，让用户在云上便捷、安全、低成本的使用密钥

服务特点

1. 基于硬件加密码模块HSM进行密钥管理
2. 通过HSM生成真随机数TRNG（True Random Number Generator）与密钥
3. 采用多层密钥保护机制，每个用户都拥有自己的主密钥
4. 密钥的生成、传输、使用、存储、销毁都有专业的安全解决方案
5. 可与云计算的其它服务和用户的应用程序配合使用
6. 采用符合国家（地区）、行业要求的密码算法
7. 按需使用，按量计费

应用场景

1. 对象存储加密支持：与对象存储服务配合使用，应用于对象存储服务中对象的服务端加密
2. 云硬盘加密支持：与云硬盘配合使用，应用于云硬盘中的数据加密
3. 镜像服务加密支持：与镜像服务配合使用，应用于加密私有镜像的创建
4. 用户的应用加密支持：与用户的应用程序配合，为其加密能力提供密钥支持

缩略语（1/2）

缩写	全称	释义
Anti-DDoS	Anti Distributed Denial of Service	防御分布式拒绝服务
ACK Flood Attack	Acknowledgement Flood Attack	ACK 泛洪攻击
SYN Flood Attack	Synchronize Flood Attack	SYN 泛洪攻击
FIN/RST flood Attack	Finish/Reset Flood Attack	FIN/RST 泛洪攻击
CC Attack	Challenge Collapsar Attack	CC攻击
SIS	Security Index Service	安全指数服务
AES	Advanced Encryption Standard)	高级加密标准
CMK	Customer Master Key	用户主密钥
DEK	Data Encryption Key	数据加密密钥
HSM	Hardware Security Module	硬件安全模块
KEK	Key Encryption Key	密钥加密密钥
KMS	Key Management Service	密钥管理服务

缩略语（2/2）

缩写	全称	释义
HID	Host Intrusion Detection	主机入侵检测
PTS	Penetration Test Service	渗透测试服务
SCS	SSL（Secure Socket Layer） Certificate Service	证书管理服务
WAF	Web Application Firewall	Web应用防火墙
HVD	Host Vulnerability Detection	主机漏洞检测
ARS	Application Recognition Service	程序运行认证
APT	Advanced Persistent Threat	高级持续性威胁
SSA	Security Situation Awareness	安全态势感知
WTP	Web Tamper Protection	网页防篡改