UCloud 云安全白皮书

中立 专业 安全 可信

UCloud 安全团队

2018 年 4 月

目录

1、序言 1
2、安全基因构造安全平台 1
2.1 专业的安全团队 1
2.2 审计与合规团队 2
2.3 员工背景调查和保密协议 2
2.4 全员安全培训 2
3、数据安全 3
3.1 数据上云安全传输 3
3.2 云中数据安全保护 3
3.3 数据下云安全擦除 4
3.4 数据所有权及用户隐私保护 4
4、基础安全 5
4.1 物理安全 5
4.2 网络安全 5
5、安全运营 7
5.1 流程安全 7
5.2 漏洞管理 8
5.3 云平台反入侵 8
5.4 事件管理与应急响应 8
6、客户业务安全服务——天罡安全解决方案 9
6.1 解决方案体系 9
6.2 解决方案架构 10
6.3 解决方案优势 11
6.4 解决方案核心产品及技术 11
7、安全合规性与审计 17
7.1 法律法规 17
7.2 云计算业务许可 18
7.3 云合规认证体系 18
7.4 合规咨询服务 19
8、云安全生态 20

1、序言

随着云计算行业的发展和成熟，越来越多的用户选择将业务放到云平台，云平台在承载大量用户和海量业务的同时，也肩负起更多的责任。UCloud 已为 5 万余家企业级客户提供服务，是国内领先的云计算服务平台。为保障用户业务的持续良好运行，保护用户数据的安全性和完整性，云平台的安全性一直是 UCloud 的重中之重。

近年来，安全性已成为云服务商的竞争门槛之一。网络信息安全作为 UCloud 的经营保障，是一项全员参与的重点活动，贯穿于 UCloud 组织及产品的整个生命周期。从基础设施的建立、产品的设计到业务运行连续性，从组织机构的设置和运作、人员的招聘和培训到日常办公，网络信息安全意识已经潜移默化的深入到 UCloud 每个人、每个环节。安全性是 UCloud 日常运营和灾备工作的核心，安全性更是逐步成为用户信赖 UCloud 的重要理由和依据。

2、安全基因构造安全平台

2.1 专业的安全团队

UCloud CEO 兼联合创始人季昕华，互联网行业资深安全专家，曾担任过腾讯安全负责人、盛大首席安全官，在他的带领下，UCloud 创立之初，就有着根深蒂固的安全基因，云平台架构设计就已经将安

全性作为重要因素。

UCloud 有着数十人组成的专职安全团队，秉承着专职、专业、专注的理念，汇集各方面的安全专家、安全专业人员。团队由研发、运维、运营构成，覆盖基础设施安全、网络安全、主机安全、应用安全、数据安全、运维安全、安全管理及安全服务，并有专职团队负责安全漏洞及安全事件的运营和处理，每个层次、每个环节都做到可控、可信、可靠。

2.2 审计与合规团队

UCloud 建立专业的合规团队，完成内部安全审计，保障公司、云平台、云产品符合国家和地区监管、获得国际认证认可，并且为客户提供合规咨询服务，帮助客户更顺利的完成监管和认证。

2.3 员工背景调查和保密协议

在员工入职前，UCloud 在国家及地区法律法规允许的情况下，通过一系列背景调查手段来确保入职的员工符合公司的行为准则、保密规定、商业道德和信息安全政策。背景调查的详细程度取决于岗位需求，可能涉及刑事、职业履历和信息安全等多个方面。员工入职的同时，均与劳动合同同步签署安全保密协议。

2.4 全员安全培训

任何一名进入 UCloud 的员工，都要先参加基础安全培训，包括网

络信息安全、员工保密责任、办公和上网安全、社会工程学防护、安全制度和法规等。安全团队还会组织有针对性的专业安全培训，包括代码安全、流程安全、安全漏洞分析等。

3、数据安全

3.1 数据上云安全传输

公有云用户选择 UCloud，将自身业务迁移部署到 UCloud 公有云时，UCloud 为用户提供相应的工具和技术手段，与用户现有的数据格式保持最大的兼容性，支持数据加密传输（如 HTTPS、SSH 等）。

UCloud 依托合作运营商提供的高质量网络链路，为用户提供专线接入服务，以专线方式连通用户本地业务到 UCloud 数据中心，具有线路独享、安全私密、延迟低、质量稳定等特性，以构建混合构架，满足原有业务转型、异地容灾、多区域业务扩展等复杂业务场景。

3.2 云中数据安全保护

公有云用户共享 UCloud 的底层硬件，UCloud 通过安全的架构设计，保证用户数据和业务之间严格的逻辑隔离，保证同一资源池用户数据互不可见，云主机根据帐号进行隔离，通过网络隔离的技术保证不同用户间的主机和数据互不可见，无法通过内网访问。

UCloud 使用分布式存储，文件被分割成许多数据片段分散存储在

不同的设备上，并且每个数据片段存储多个副本。数据可用性达99.9999%。UCloud 云主机可接入数据方舟，独家支持连续数据保护，支持 12 小时内任一秒、24 小时内任一整点时刻、3 天内任一零点时刻数据恢复，最大限度保护数据。

3.3 数据下云安全擦除

在客户要求删除数据或设备在弃置、转售前，UCloud 将通过高级清零操作彻底删除用户所有数据且无法复原，并对报废硬盘做消磁处理。

客户数据彻底删除的场景不包括 UCloud 为未及时续费用户的数据保留 7 天，以防止用户由于某些原因无法及时续费导致重要数据被删除。

3.4 数据所有权及用户隐私保护

作为独立的云计算厂商，承诺客户拥有数据的绝对所有权，保障数据的私密性，完整性和持久性。UCloud 严格依据国家法律法规及服务协议的约束，未经用户允许，不会将用户数据提供给第三方，不会将用户数据存储在国外数据中心或用于国外业务或数据分析，不会对外呈现用户个人信息等隐私数据。

4、基础安全

4.1 物理安全

1）安全的物理位置

UCloud 各数据中心机房均按照相关国际标准、国家及地方安全要求进行选址，自建或租赁数据中心均进行严格要求和管控。

2）基础设施安全

UCloud 数据中心机房采用双路供电，配备柴油发电机，主要设备均接入 UPS 供电。电力系统、空调系统均采取高可用性冗余配置。数据中心各区域均接入火灾自动检测装置，配备完善的灭火设备。

3）机房安全管理

UCloud 各数据中心机房 7*24 小时专人值守，来访需审批、登记和专人陪同。机房值班人员每日巡检，检查机房环境状态、设备运行状态。安排设备厂商定期进行设备巡检，维护和升级。

机房工作人员均需经过完善的培训，熟悉机房设备的操作，熟悉机房监控状态，熟悉机房管理和应急响应流程。针对消防、灾备及重要系统制定应急预案，安排机房人员定期演练，熟练应急响应流程。

4.2 网络安全

1）网络安全隔离

作为国内最早使用 SDN（Software Defined Network）技术的云计算厂商，UCloud 从创业伊始就把租户隔离作为云网络设计的第一原则。UCloud 利用 SDN 技术搭建 Overlay 网络，来解决多租户间隔离的问题。每个用户会被分配一个独立的网络 ID。只有隶属于同一用户、带有相同网络 ID 的数据包才会被允许互相访问。来自不同用户的报文则在 SDN 转发器处会被强行终结，从而确保用户数据不会被其它用户嗅探到。

2）VPC 私有网络

UCloud 所有可用区网络都是按照 VPC（Virtual Private Cloud）架构设计，用户可以快速搭建自定义的子网，各子网之间完全隔离（基于网络二层）。UCloud 推出的新一代 VPC 2.0 具有业界最灵活的自定义网段方式，还提供了业内首创的子网跨可用区能力，主机在可用区间迁移时，内网地址可保持不变，实现了更强的灾备能力。

3）DDoS 防护

近年来，DDoS（Distributed Denial of Service）攻击数量和规模均呈现迅速增长的趋势，影响范围也扩张到多个行业。云平台承载着诸多客户的业务，也成为 DDoS 的重灾区。

UCloud 拥有专业的 DDoS 网络安全防护团队，云平台接入专业的 DDoS 防护设备，可有效抵御 SYN FLOOD，UDP FLOOD 等常见攻击，保障云平台业务的正常运作。

为保障客户业务不受到 DDoS 攻击的影响，DDoS 网络安全防护团队将 10 年安全防护经验输出为高防服务 UADS，为客户提供专业的高级防护系统，具有国内最大 600Gbps，海外 1T 的攻击防护能力，详见 6.3 章节高防服务。

5、安全运营

5.1 流程安全

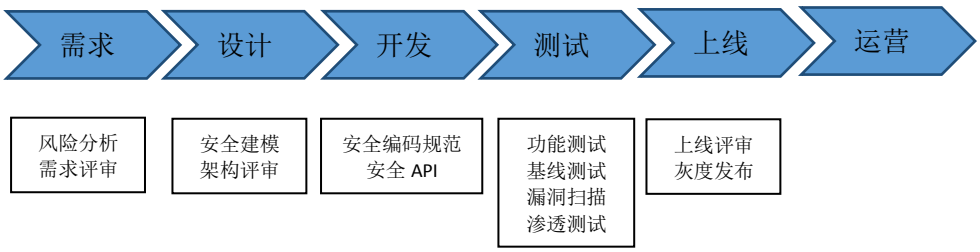

图 5-1 安全开发流程

为保证用户使用云平台及各云产品的安全性，UCloud 严控整个开发生命周期，将网络信息安全植入其中。UCloud 安全开发生命周期主要包括以下流程：

1）需求分析：对需求进行风险分析，并加入需求的安全评审。

2）架构设计：依据安全建模方法，对系统架构进行多层次的评审。

3）开发实现：对研发人员进行安全开发、代码安全等专业培训，规范研发人员遵守安全编码规范，提供和使用安全 API。

4）测试验收：由质量部门严格把关，进行功能测试、基线测试、安全漏洞扫描及渗透测试，及时发现和修复安全漏洞。

5）发布上线：采用灰度发布方式，上线后定期进行安全漏洞扫描。

6）安全运营：应用监控预警系统，建立完善的应急响应流程，完成问题的处理与跟踪。

5.2 漏洞管理

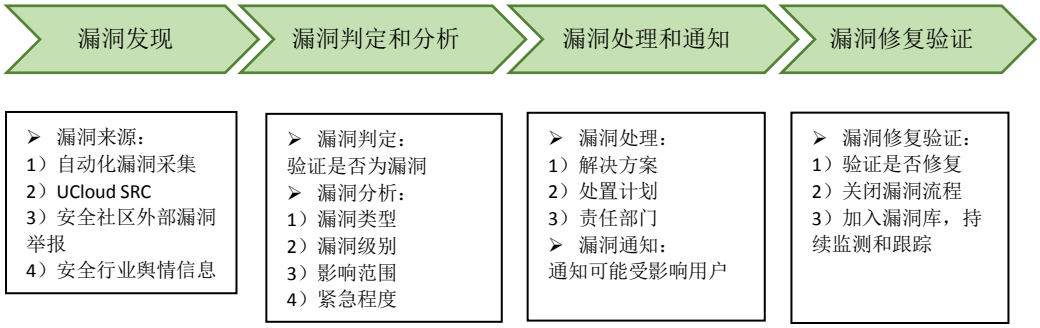

图 5-2 漏洞管理流程

UCloud 安全中心在漏洞管理和发现具备专职团队，漏洞管理团队的主要责任就是发现、跟踪、追查和修复安全漏洞。通过数字化的“漏洞分”运营，对每个真实的漏洞进行分类、严重程度排序和跟踪修复。UCloud 安全中心与各安全研究社区保持联系，受理外部漏洞举报。

5.3 云平台反入侵

UCloud 安全团队结合多年的反入侵经验，集合数名反入侵安全专家，围绕基础设施安全、网络安全、主机安全、应用安全、数据安全、运维安全、安全管理及安全服务等安全纬度，构造起多层次立体化的入侵防御和检测，确保平台安全不受入侵影响。

UCloud 平台上所有用户之间实施严格的网络隔离，某个用户遭到入侵后，不能通过云平台网络渗透入侵到其他用户。

5.4 事件管理与应急响应

客户在使用产品中遇到任何问题，均可以向技术支持反馈，UCloud 团队提供 7*24 小时技术支持，90 秒极速响应。UCloud 建立完善的安全管理制度，对安全事件进行分类分级，按照流程进行响应和处置。对于涉及到产品的事件均定义为运营质量事件，设置明确的事件处理机制和奖惩制度，保证极速响应、快速定位、专业解决，保障客户权益。

UCloud 时刻监控业界安全情报，发现有会影响商户或平台的安全事件(如业界发现高危漏洞等)会立刻启动应急流程确保客户及平台的安全。UCloud 服务可用性已在可信云网站进行阳光披露，水平一直处于业内第一梯队。UCloud 签署国内首批可信云保险，支持最高百倍赔偿。

6、客户业务安全服务——天罡安全解决方案

UCloud 整合自身安全技术能力及安全攻防经验积累，打造了多款丰富的安全产品&服务，为客户提供组合或单项的安全解决方案。

6.1 解决方案体系

UCloud 为客户提供纵深安全防护，涵盖了网络安全、主机安全、应用安全、数据安全、运维安全、安全管理及安全服务，提供 10 余款安全产品&服务满足客户的各类安全需求。

UCloud云安全体系		
等保咨询测评服务	SOS应急响应服务	安全服务
态势感知	威胁情报	安全管理
堡垒机		运维安全
SSL证书	数据库审计	数据安全
主机入侵检测		主机安全
Web漏洞检测	Web应用防火墙	应用安全
高防服务		网络安全
云平台基础设施安全		云平台安全

图 6-1 UCloud 云安全体系

6.2 解决方案架构

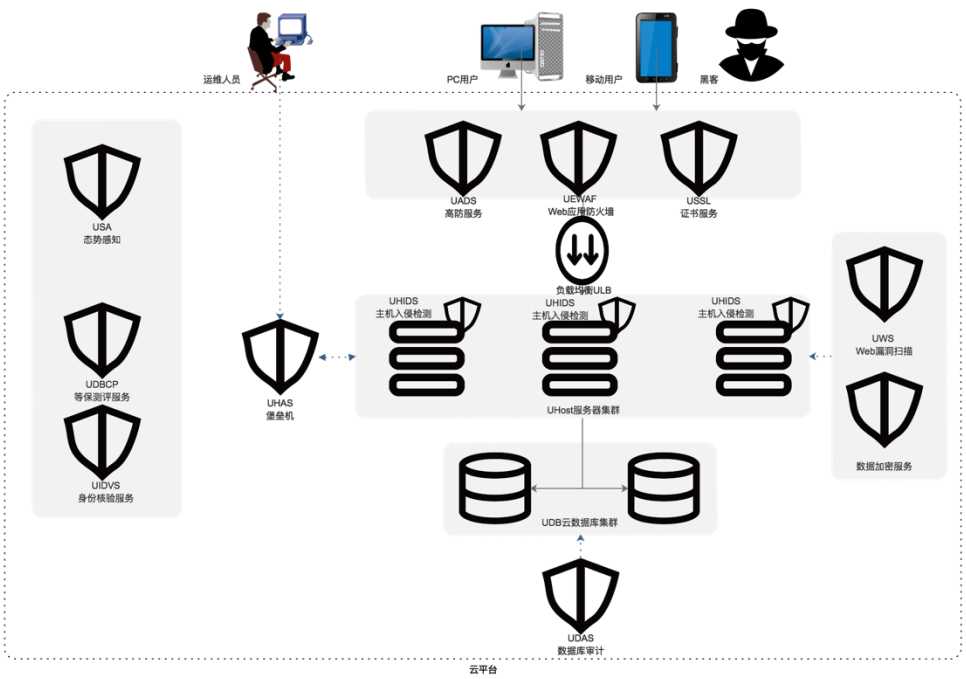

图 6-2 UCloud 云安全架构

UCloud 云安全方案与云平台深入融合，一方面充分利用云计算平台的优势进行安全架构建设，另一方面利用安全技术优势保护云平台的安全。

UCloud 云安全方案在充分理解攻击及业务架构的基础上，采用从深立体的防御体系，保障云平台业务的安全。

6.3 解决方案优势

1）方案灵活可剪裁。企业机构可以根据自身安全防护需求和成本预算选择适合自己的安全产品。

2）支持私有云、混合云架构。所有的安全产品均能够单独部署在客户的托管机器上。

3）持续优化和改进。相比于传统的安全解决方案，能够保持先进性，不落后于时代的发展。

4）部署简单方便。不影响现有业务，无需改动代码。

6.4 解决方案核心产品及技术

1）态势感知

态势感知为客户提供一站式的大数据安全平台，全方位展示客户云上资产的整体安全态势，一方面可以追溯已经发生的网络、主机、应用等安全事件，另一方面可以展示当下的安全整体状况，此外通过大数据等技术预测安全发展趋势，帮助客户建立一套完善的事前预判、事中防护、事后取证分析的大数据安全平台。

2）威胁情报

威胁情报采用 200+威胁情报源，千万级有效情报数据，洞悉 IP、域名、文件等的安全状态。缓解目前攻防对抗不对称的现状，共同抵御外部威胁。

3）Web 漏洞检测

Web 漏洞扫描（UCloud Web Scan）是用于检测 Web 网站漏洞的安全服务。可以准确、全面扫描 Web 网站程序中存在的漏洞，避免漏洞被黑客利用影响网站安全；与传统或开源的漏洞扫描产品相比具有抓取数据更全面、误报率更低、漏洞库更新及时且不影响业务等优势。

4）企业应用防火墙 UEWAF

企业应用防火墙（UCloud Enterprise Web Application Firewalls）是为企业提供的 web 应用防火墙，用于针对 web 网站的常见攻击进行监测和阻断。支持发现 SQL 注入、XSS 跨站等 web 攻击行为。可以为用户降低停机时间、篡改和数据失窃的风险，并隐藏源站，防止对源站的直接攻击。

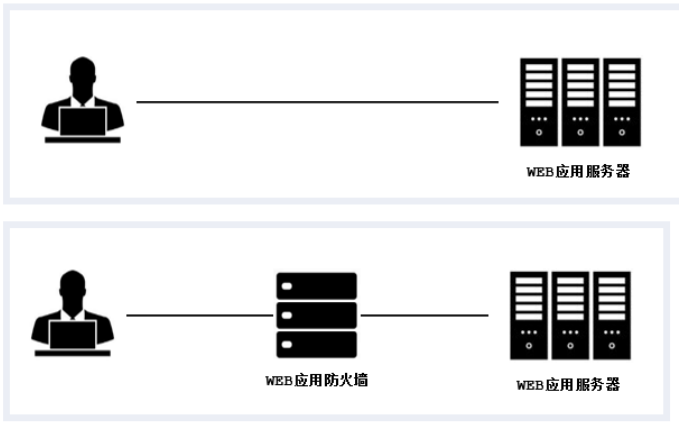

图 6-3 系统接入 UEWAF 前后对比

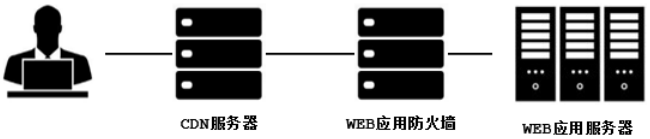

图 6-4 CDN 结合 UEWAF

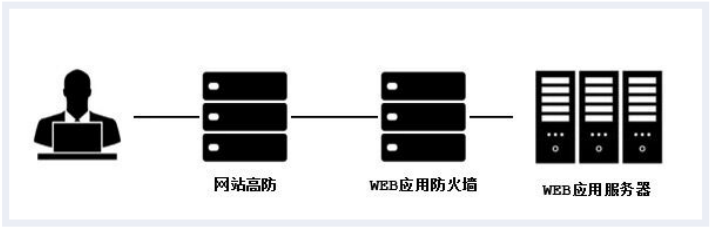

图 6-5 高防结合 UEWAF

5）SSL 证书管理 USSL

SSL 证书管理（UCloud SSL）为客户提供统一的 SSL 证书管理服务，客户可以方便的在云上完成证书申请、购买、审核、签发等证书流程，还可以统一管理自己已有证书。UCloud SSL 证书管理支持 keyless 的安全解决方案，也就是私钥证书无需上传，通过访问私钥服务器验证，使用更安全。

6）数据库审计

数据库审计对数据库的审计和事务日志进行审查，从而跟踪各种对数据库操作的行为。一般审计主要记录对数据库的操作、对数据库的改变、执行该项目操作的人以及其他的属性。这些数据库被记录到独立的平台中，并且具备较高的准确性和完整性。针对数据库活动或状态进行取证检查时，审计可以准确的反馈数据库的各种变化，对我们分析数据库的各类正常、异常、违规操作提供证据。

7）主机入侵检测

主机入侵检测是部署在云主机上的安全 Agent，集检测、修复、防御于一体，支持 UCloud 云主机和阿里云主机、腾讯云主机、私有云托管的服务器等。能够及时发现黑客的入侵行为，包括检测异地登录、暴力破解、后门木马、配置缺陷及高危漏洞等。

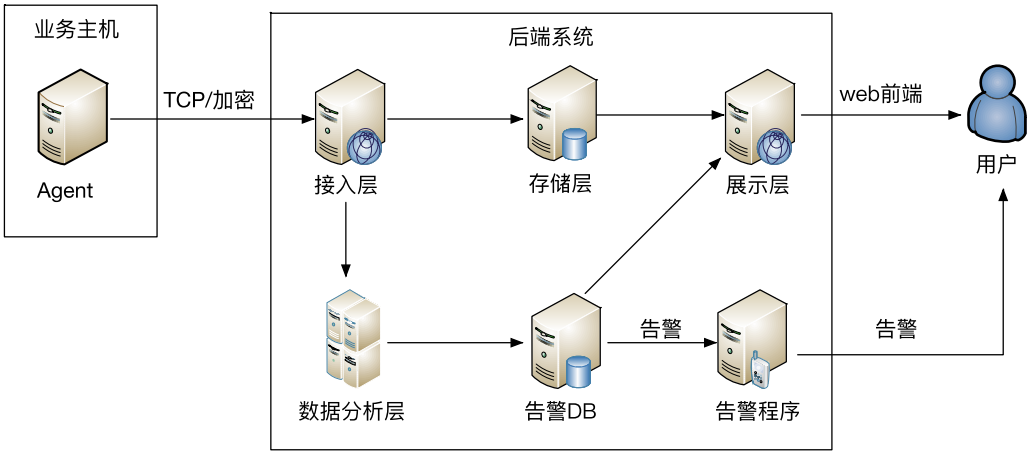

图 6-6 服务器安全管家应用示意图

8）堡垒机 UHAS

运维审计系统（UCloud Host Audit System），即俗称的堡垒机，拥有账户、认证、授权、审计功能，为用户提供集中式运维管理解决方案。运维人员可通过堡垒机远程访问云主机（UHost），记录所有对云主机的操作，方便遇到问题时的场景重现和责任追溯，提升企业内部运维风险控制水平。

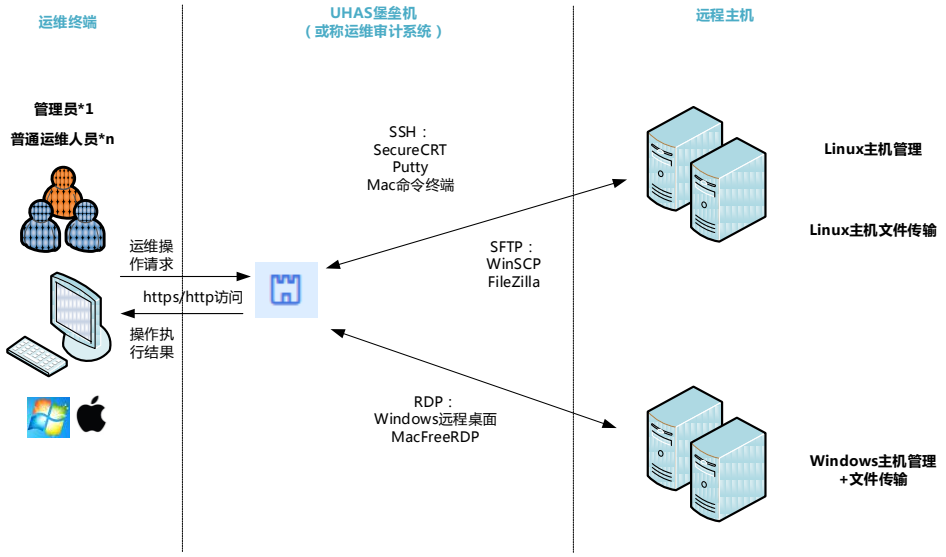

图 6-7 UCloud 堡垒机应用示意图

9）高防服务 UADS

高防（UCloud Anti DDoS）为已备案的域名或源站 IP（包括非 UCloud 的弹性外网 IP）提供 DDoS 攻击防护。当用户的域名或源站 IP（包括非 UCloud 的弹性外网 IP）在遭受大流量的 DDoS 攻击时，可以通过高防 IP 代理源站 IP 面向用户，隐藏源站 IP，将攻击流量引流到高防 IP 进行清洗，确保源站的稳定正常运行。

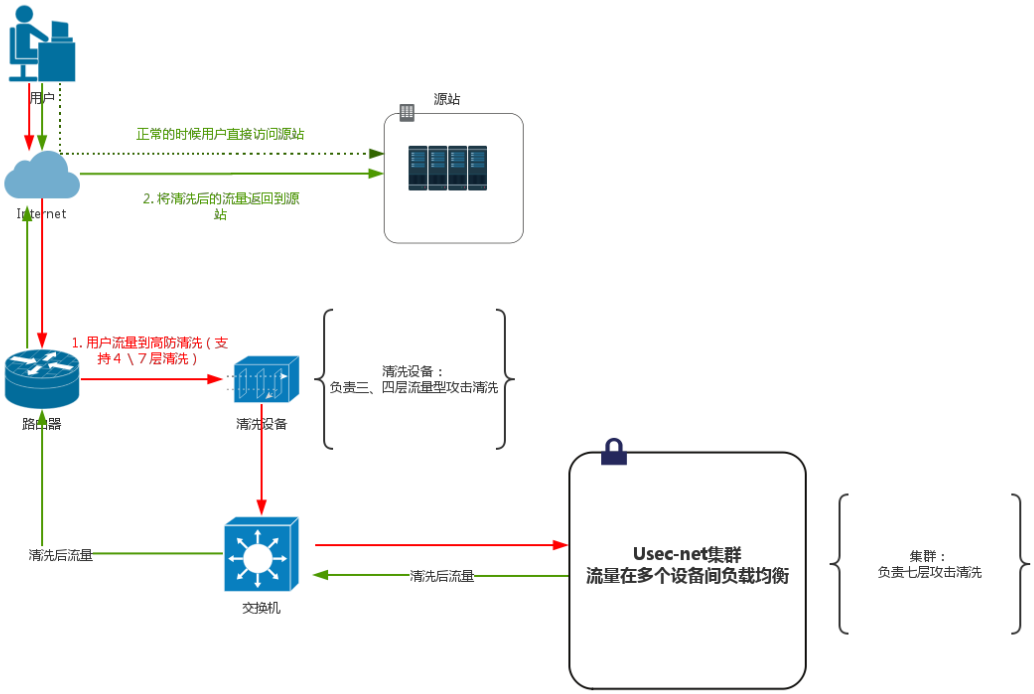

图 6-8 UCloud 高防服务架构示意图

10）等保咨询测评服务

等保咨询测评服务-UDBCP，主要包含两部分内容：等保咨询服务和等保测评服务，企业根据自身需求情况进行服务项目的选择。

（1）等级保护咨询服务

为企业的等级保护工作提供专业的建议，协助企业进行系统的定级、备案，采用技术手段和访谈调查方式发现企业安全现状与国家等级保护要求之间的差距，然后依照国家等级保护相关标准，完成等级保护建设整改方案设计。（注：企业依据所提供的等级保护建设整改方案进行安全建设整改）

（2）等级保护测评服务

根据国家网络安全等级保护的相关测评标准、规范等，对企业的待测评系统进行网络安全等级保护测评，并出具等级保护测评报告。

11）SOS 应急响应

UCloud 建立由多名安全攻防经验丰富的安全专家组成 SOS 应急响应团队，提供 7x24 小时的安全应急响应。安全专家团队时刻监控业界安全情报，发现有会影响商户或平台的安全事件(如出现高危漏洞等)会立刻启动应急流程确保商户或平台的安全。

7、安全合规性与审计

客户在使用云服务获得便利、提高效率的同时，也面临着数据安全和业务合规的挑战。UCloud 先客户所想，捍卫云平台安全，通过行业权威合规性认证，为客户营造安全的空间，让客户安心的将业务部署在安全可信的 UCloud 平台。UCloud 将根据国家法律法规要求、用户需求及云计算行业的发展，持续关注和完成更多的认证认可，向用户展现自身实力。

7.1 法律法规

UCloud 严格遵守国家法律法规和政策要求，遵循云计算行业及网络信息安全方面的标准和规范。尤其在 2017 年 6 月 1 日国家全面执行《网络安全法》，UCloud 在用户隐私信息保护、网络信息安全、知

识产权保护等方面更加高度重视，按照法律规定和公安部门要求执行，确保所提供的云平台及云产品符合国家法律法规要求。

7.2 云计算业务许可

UCloud 在拥有电信业务 IDC 牌照及 ISP 牌照的基础上，又率先获得工信部颁发的电信业务云计算牌照，拥有正式的云计算服务业务许可，客户可以放心使用通过国家许可的 UCloud 云服务。

7.3 云合规认证体系

图 7-1 UCloud 云合规认证体系

2014 年 7 月，UCloud 首批通过可信云服务认证，获得云主机、云数据库、云缓存及云分发服务认证。

2014 年 8 月，UCloud 云服务平台高分通过公安部等保三级测评。

2015 年 8 月，UCloud 首批通过数据中心联盟主导的大数据产品能力认证。

2016 年 7 月，UCloud 获得最新版本的 ISO/IEC 27001:2013 信息安全管理体系认证。

2016 年 8 月，UCloud 通过 CSA 和 BSI 联合推出的 CSA STAR 国际云安全认证。

2016 年 9 月，UCloud 作为国内首批试点，率先通过可信云安全认证，云服务做到可信、安全。

2016 年 9 月，UCloud 通过 ISO/IEC 20000:2011 信息技术服务管理体系认证。

2016 年 12 月，UCloud 通过工信部第一批 ITSS 云计算服务能力评估，并获得最优级别（增强级）的认证。

2017 年 4 月，UCloud 获得可信云颁发的云主机分级“五星+及五星”最高级别。

7.4 合规咨询服务

客户需要各类合规证明时（例如，客户自身需要完成等保测评），UCloud 可以为客户提供云平台已获得的证书、报告等相关证据，并尽可能的给予客户服务和协助，帮助客户更顺利的完成认证认可。

8、云安全生态

U 市场以 UCloud 云服务内容为基础，通过聚合第三方应用和服务，为企业提供一站式的中立服务平台。UCloud 将根据客户需求引入业内一流的安全设备厂商和安全服务厂商进入 U 市场，为客户提供更为人性化的安全保障，形成互利共赢的行业安全生态。