引言

中大型企业上云时，通常选择按照业务线、项目或使用场景、生产测试环境来建立多账号体系。相对于单账号体系，多账号间的云资源默认隔离，便于不同产品/分支机构间进行独立的成本结算和运维管理，减少了单账号下过于宽泛的RAM权限带来的风险。

但同时，也会使安全管理变得较单账号体系复杂：

* 安全报表分析、资产盘点需要覆盖多个云账号，统计耗时耗力；
* 安全策略不得不在多个账号中进行重复配置，运维人员陷入“重复劳动”陷阱；
* 漏洞攻击、入侵、失陷等异常行为在影响多个账号时，应急处置手忙脚乱；
* 多个业务账号下，南北向与东西向流量缺乏统一视角，日志分析缺乏全局分析能力。

那么，从不同企业业务需求和组织架构出发  
云防火墙是怎样在阿里云上实现多账号统一安全纳管的呢？  
一起翻开这本“心法秘籍”来一探究竟

云墙“心法”一：集中用兵，打歼灭战

业务再多，防护也有“上帝视角”

云上的大、中型企业，业务类型千差万别，形成少则数十、多至数千的业务子账号，企业安全人员管理数千至十几万资产的统一防护，安全运维压力大。传统的网络防御架构下，防火墙的管理权限分属于不同业务部门，每个业务账号独立管理，缺乏统一视角，被动式入侵检测难逃“亡羊补牢”的尴尬。

* 互联网出入口管理：互联网出入口分散在不同账号中，进出流量夹杂大量攻击，针对EIP的攻击并发性强，而账号分属不同owner，防护碎片化；
* 攻击IP封禁：强对抗场景考验企业防御策略，对IP封禁策略、黑名单机制和主动外联行为发现的实时性有严苛要求；
* 蠕虫管理：一旦爆发强传染性蠕虫，云上防御需要实现组织统一管控，即时防御；
* 漏洞修复：在组织层级架构下，针对高危/中危漏洞认知水平、修复手段和漏洞防御理解力亟待拉齐；
* 误报率高：缺乏账号间关联关系学习，传统防火墙难以区分关联用户高频正常访问与暴力破解，入侵检测误报率高。

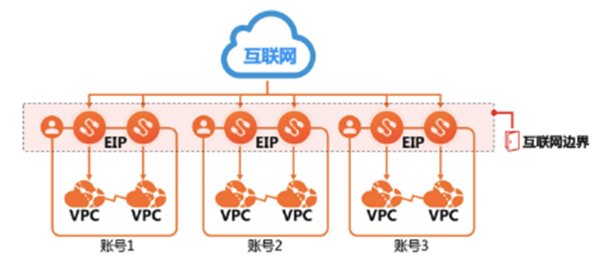


图 数千账号入侵防护亡羊补牢 vs 多业务账号统一入侵防护架构图

云防火墙公网资产自动安全纳管

通过阿里云·云防火墙的跨账号统一互联网边界资产管理能力，用户能够在一个控制台统一管理各个账号下的EIP资产，覆盖ECS、SLB和NAT资源。当受管账号发现新的网络资产时，会自动被云防火墙纳管，避免资产遗漏，网络防御无短板。

扫除业务间防护盲区

对于开启了防护的公网暴露资产，所有IPS规则即刻生效，多个账号下互联网边界统一安全防御，真正实现针对外部恶意入侵、攻击的单点告警和全业务象限协同拦截，降低由于管控疏漏导致的网络安全事件。

* 暴露面一键收敛：拨开复杂业务场景流量，依靠深度报文解析和海量历史日志的机器学习，实现边界暴露面的一键策略收敛，攻击水位下降90%；
* 大数据协同防御：依托图计算情报关联自生长，日均千万级的高质量精准情报实时拦截，协同构建多账号企业的动态网络安全边界，攻防和僵木蠕场景实现全球云网络视野的最早在野利用的可见可防；
* 虚拟补丁：为云上客户实现针对远程可利用漏洞（RCE）的跨账号虚拟化防御，拉齐应急响应能力。
* 白名单策略降低误报：基于账号间关联关系的流量学习，在企业账号间形成更高置信度的白名单策略，企业账号间互访实现0误报。

云墙“心法”二：力争主动，力避被动

跨业务环境统管，安全策略配置一次搞定

服务或资源隔离是减少系统间依赖，避免故障蔓延的重要手段。云上企业往往通过划分不同的VPC，将需要隔离的业务资源从网络层面分开。  
混合云架构下，对于不同的业务分支或环境属性，云账号支撑着更复杂的隔离与业务互访场景，如IDC与VPC间、VPN、专线等。复杂隔离访问需求带来的，是更为复杂的安全策略配置。

* 重复劳动：在不同的账号下搭建防火墙设备，在不同的区域中配置访问控制策略ACL，导致一条相同的策略需要多次配置；
* 策略冲突：对于不同的账号环境下的策略，缺乏统一管控，极易造成访问控制时的策略冲突等问题；
* 业务受阻：同一企业不同业务/环境间安全控制策略难以同步，严重时有可能影响业务（如：针对某类入侵，测试环境未设置阻断，而生产环境阻断未进行测试，防护规则与业务冲突，影响正常业务流量）。



图 多环境安全配置忙乱 vs 跨业务/开发-测试-生产环境策略配置统管

策略统管更高效

阿里云·云防火墙目前通过集成CEN服务，为企业跨账号以及跨VPC的流量互访，提供了统一的策略管控能力，帮助企业通过一个策略配置平台，实现不同账号和VPC间的访问控制策略统一管理，除了覆盖VPC间互访外，还能针对专线和云连接网CCN等混合云场景，实现一条策略，全局生效，单条策略下发耗时从原来的以天为单位缩短到以秒为单位，免去了多次配置同样策略所增加的工作量和风险，帮助企业更好的实现统一管控。

云墙“心法”三：精勤慎重，指挥若定

多地分公司统一安全报表分析与结算

组织架构一定程度上决定了云账号的结构，无论是集团-子公司运作模式，或是多分支机构运作模式，企业安全部门最大的难题就是对各个业务运行环境的统一安全感知能力，而其中，网络安全又是最重要的分析对象之一。企业在互联网侧总共暴露了多少网络端口，当前有多少个隔离域正在运行，规划的南北向和东西向隔离策略是否正常生效，有多少网络入侵事件每天在发生，全量的日志是否如规划被正确记录以满足审计的要求，是否有异常的流量正在发生，业务间的调用关系是否合理等，这些网络安全运维问题在一个账号下还相对可控，但一旦分散到多个云账号下，对于管理人员就成了灾难，流量数据的统一，网络日志的统一，攻击分析的统一，对于日常的安全运维，几乎都是“不可能的任务”。



图 多分支机构通过管理账号实现统一报表分析与结算

集中流量分析与报表统计

通过集中化的数据统计，网络安全运维人员只需要关注统一的数据平台，就能够实时掌握企业整体的网络安全运行态势、资产暴露情况、策略配置和效果、入侵防御数据，并且将不同账号环境下的日志数据自动化进行归集，在满足诸如等保2.0等合规要求的基础上，通过统一的分析，优化报表统计，使得结果更为准确，全面，也能更好的为后续优化工作提供数据基础。

用户声音

“云防火墙的集中管控能力帮助我们将云上多个业务账号和第三方测试账号进行了统一纳管，实现了一个控制台的防护可视化。这大大简化了日常的网络策略运维工作，提升了网络流量统一分析的效率和质量，非常好地满足了我们企业对于网络安全集中化管理的需求，并且为未来更精细化的网络策略管控铺平了道路。”——某大型金融企业信息安全负责人

云上多账号环境下的网络统一管理，是大型分支型企业网络安全防护的必经之路。无论是外企入华、国内企业出海，还是本土集团型企业规模化成长，云上统一网络安全管控与整体安全态势感知，都可以拉齐企业账号间安全水位，让安全防护无死角。