

云原生网络安全开发应用

CODE FUTURE.

轻盈如薄纱，坚固若磐石

朱家睿

高级产品专家

1、云上安全运维困难和挑战

安全与业务的割裂

安全是纵深在整条业务架构中的必要因素，但与业务的割裂导致安全建设和运维成本高

计费模式的割裂

缺少安全效果计费

计费模式的不统一

部署形式的割裂

部署对架构入侵大

缺少混合云统一管理

安全能力的割裂

基础安全能力部分缺失

安全生态能力融合难

业务变革的安全挑战

业务边缘化的安全挑战

容器和硬件安全需求

传统网络安全方案 部署时遇到的挑战

用不了

因域名、DNS、端口、SNI等无法接入

没有域名、纯IP访问

不能修改DNS

非标端口

客户端不支持SNI

因资产规模、业务模型复杂等无法接入

多资产多端口

不能换IP

不希望改变网络架构

延迟不能增加

用不爽

接入后需要复杂配置、有扫描风险等

获取真实IP麻烦

防绕过额外增加配置

TLS1.0、弱算法风险

证书多处维护

接入效率低，链路复杂度增加

大带宽业务成本高

被攻击换IP手忙脚乱

运维复杂度大大增加

额外增加链路故障风险

2. 阿里云-原生网络安全方案

阿里云-原生网络安全方案

阿里云-原生安全帮助客户在现有业务架构基础上提供无缝部署、快速启用、按需付费的安全能力



亮点

最小化业务架构变化部署安全

一键启用

按需使用

客户价值

简化安全建设和运维，专注业务

建设安全能力，效果驱动付费

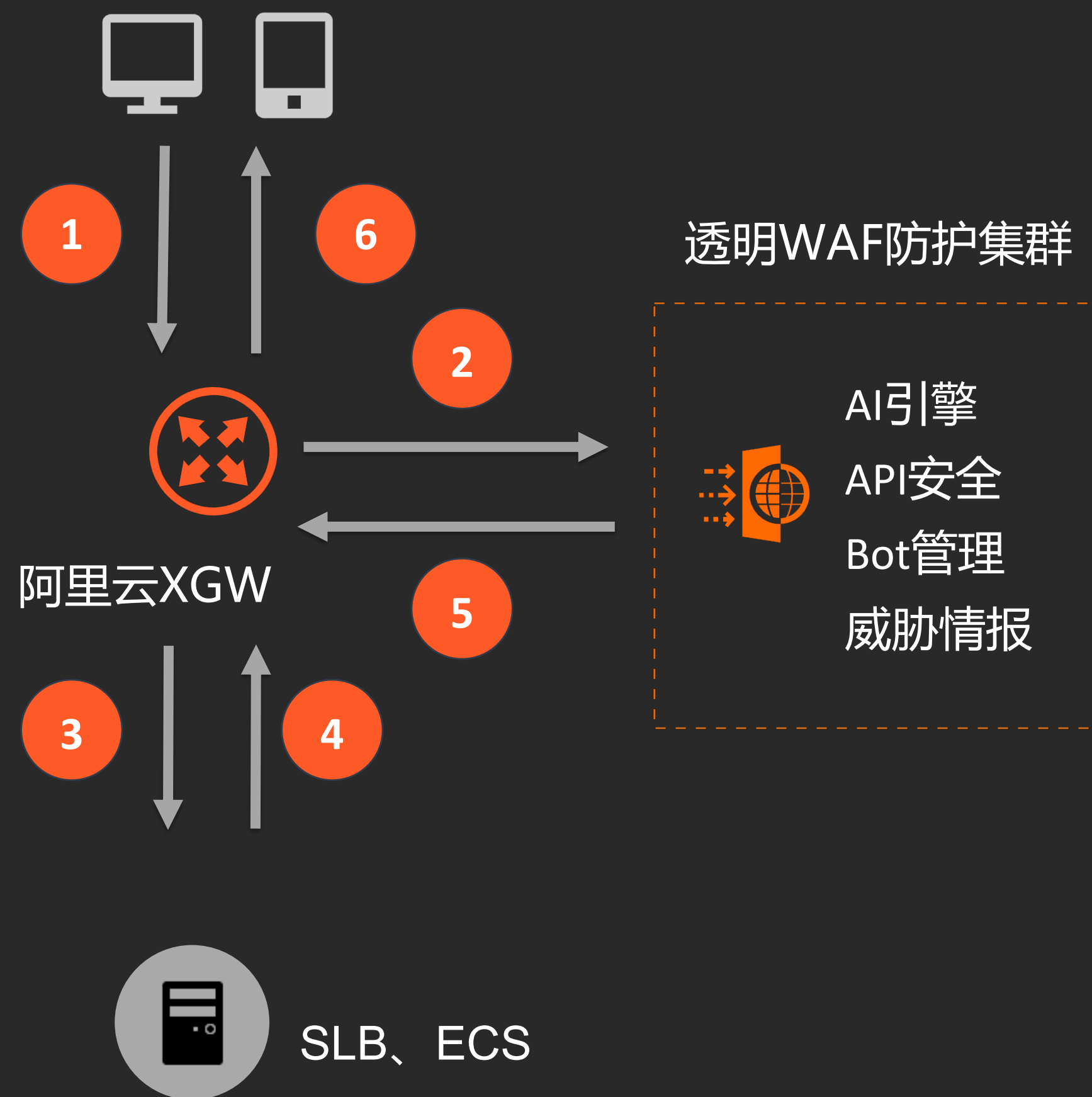
安全投入与业务发展阶段匹配

统一管理云上和云下安全能力

加速企业云化

原生透明WAF解决方案架构

透明WAF业务数据流向图



- 不需要修改DNS接入
- 任何端口都可以接入WAF
- 不需要更换IP
- 不需要兼容SNI
- 不需要修改客户端和服务端逻辑

- 通过XGW技术将去往SLB的公网IP流量先牵引到WAF集群
- 安全检测后，流量回注到SLB并修改IP，让SLB看到真实客户端IP
- 在七层SLB(开启HTTP/S协议)上的端口、证书、TLS等设置均自动同步到WAF、无需额外配置
- 按量计费、根据防护需求按需定制合适的防护策略,进一步降低用户接入成本

DDoS原生防护解决方案

全账号全资产

- 账号级防护，支持防御数百上千云资产
- 支持全类型云产品，包括ECS、VPC、EIP、SLB、WAF、NAT等

不改架构 不增延迟

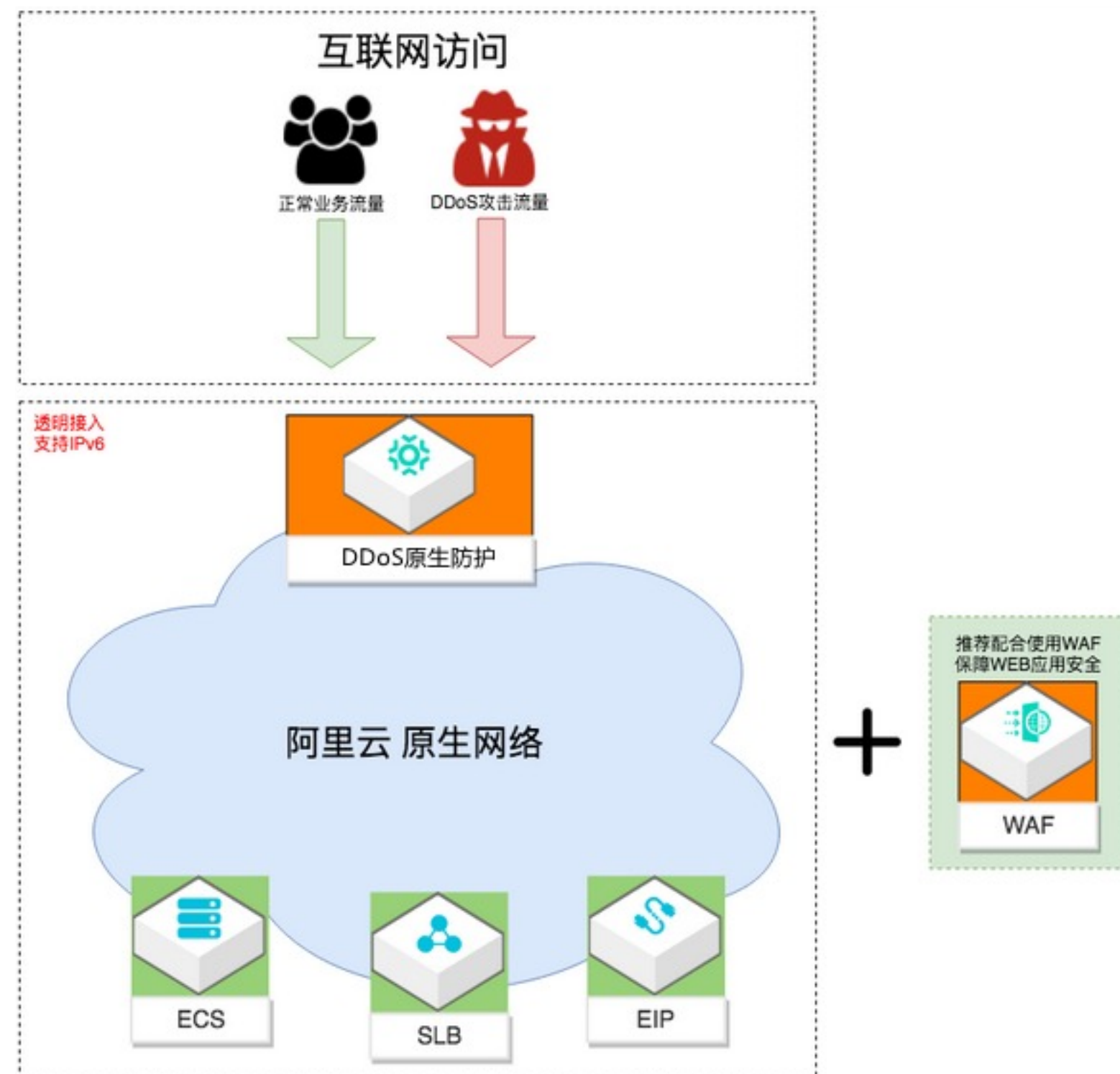
- 基于云原生，无需改变IP，一步完成
- 不增加延迟，不改变网络结构

费用可控

- 全力防护模式，不产生攻击后付费，无需升级弹性防护
- 部分开放按量计费模式

支持大型业务

- 适配所有业务规模，从100Mbps到1000Gbps，都可以合理成本接入



3、云原生网络安全产品介绍

透明WAF使用介绍

1.添加网站时，选择透明接入模式，完成相关授权

2.明确网站解析在哪个SLB实例和端口

3.勾选对应端口、点击保存即完成引流防护

4.七层SLB实例下，无需选择协议、上传证书、选择负载算法等，所有配置均从SLB自动同步

* 域名：

免登用户：1496796425594145，注意：这是云盾免登只读环境，所有操作均已记录日志，请注意数据安全！

请输入您的网站，例如：www.aliyun.com

支持一级域名（例如：test.com）和二级域名（例如：www.test.com），二者互不影响，请根据实际情况填写。

* 接入模式

Cname 接入

透明接入

new

透明接入：云上公网最佳接入方式，无需更改网站DNS解析及源站配置即可正常获取真实客户端IP。目前支持七层SLB实例(协议为HTTP或HTTPS)，支持区域为北京、深圳、上海、杭州、成都五个地区。

添加网站时，选择透明接入

1

2

3

添加域名信息

检查并确认

添加完成

<

SLB/ALB类型

选择需要防护的SLB实例

① 查看不到SLB实例？[点我了解](#)。支持SLB实例选择在端口级别，[了解更多](#) [查看可选范围](#) [C](#)

勾选对应要防护的端口进行引流

实例ID	IP地址	协议	证书	端口号 ?
SLB - lb-bp1exqozejikle0nhsxsf	47.99.88.208/华东1	HTTPS/HTTP	证书名称 szy.cn_2022年6月16日 证书ID 4065453 1	<input type="checkbox"/> 443 <input type="checkbox"/> 7800 <input type="checkbox"/> 4080
SLB - lb-bp1wlteo351f0tihce2e3	47.99.197.43/华东1	HTTPS/HTTP	证书名称 szy.cn_2022年6月16日 证书ID 4065453 1	<input type="checkbox"/> 443 <input type="checkbox"/> 7800 <input type="checkbox"/> 4080
SLB - lb-bp1tkrxh2ies0mgtwt679	47.98.198.122/华东1	--	--	--

下一步

取消

DDoS原生防护使用介绍

1.选择对应资产，一键启动防护

2.按需启用网络边界流量过滤

DDoS防护产品

资产中心

DDoS原生防护

实例管理

防护配置

防护分析Beta

DDoS高防

DDoS高防(新BGP)

DDoS高防(国际)

行业解决方案

游戏盾

DDoS防护选型

当攻击带宽不超过基础防护阈值时，免费为您清洗攻击流量。IP所在地域不同，所提供的默认基础防护阈值不同。

当攻击带宽超过弹性防护阈值，被攻击IP进入黑洞(当前解除黑洞时间： 300 分钟)状态。建议使用DDoS原生防护提升防护能力。[了解更多](#)

ECS 4SLBEIP (含NAT)其他

实例ID 请输入

IP/备注	状态	防护能力	清洗阈值
114.215.177.105 launch-advisor-20201126	正常	<div></div>	全力防御 BPS 300M PPS 70.00K
114.215.182.180 launch-advisor-20201126	正常	<div></div>	全力防御 BPS 300M PPS 70.00K
47.111.90.198 launch-advisor-20201113	黑洞中 解除黑洞	<div></div>	全力防御 BPS 60M PPS 12.00K
47.111.82.157 launch-advisor-20201113	黑洞中 推荐升级DDoS高防，避免被DDoS造成业务中断 了解更多	<div></div> <div>5.200G</div>	BPS 1200M PPS 900.00K
116.62.103.4 iZbp13vovt97rmw6uv8ty...	正常	<div></div> <div>5.200G</div>	BPS 1200M PPS 900.00K

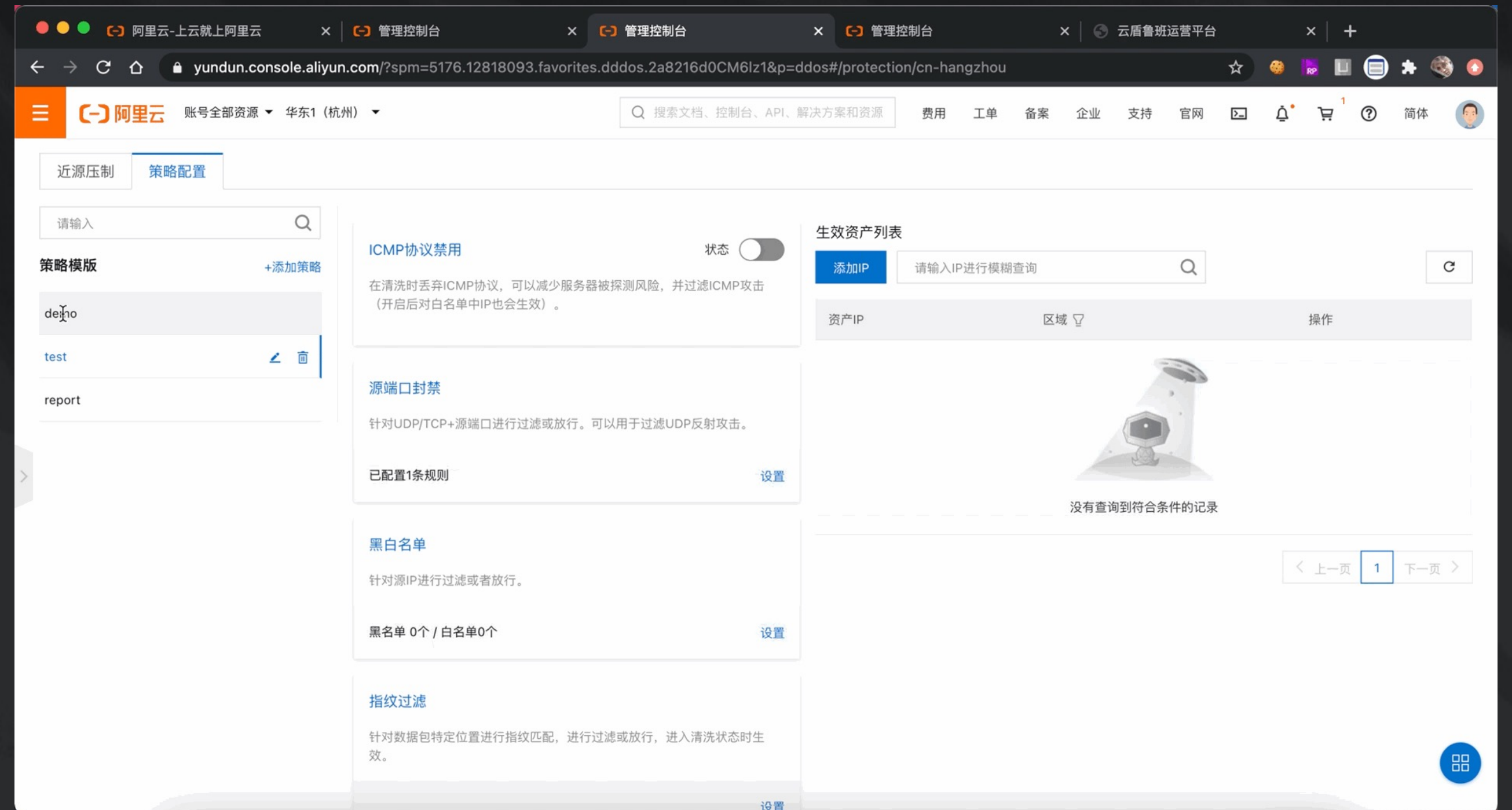
添加原生防护

< 上一页1/1下一页

DDoS原生防护使用介绍

1.选择对应资产，一键启动防护

2.按需启用网络边界流量过滤



4、典型场景

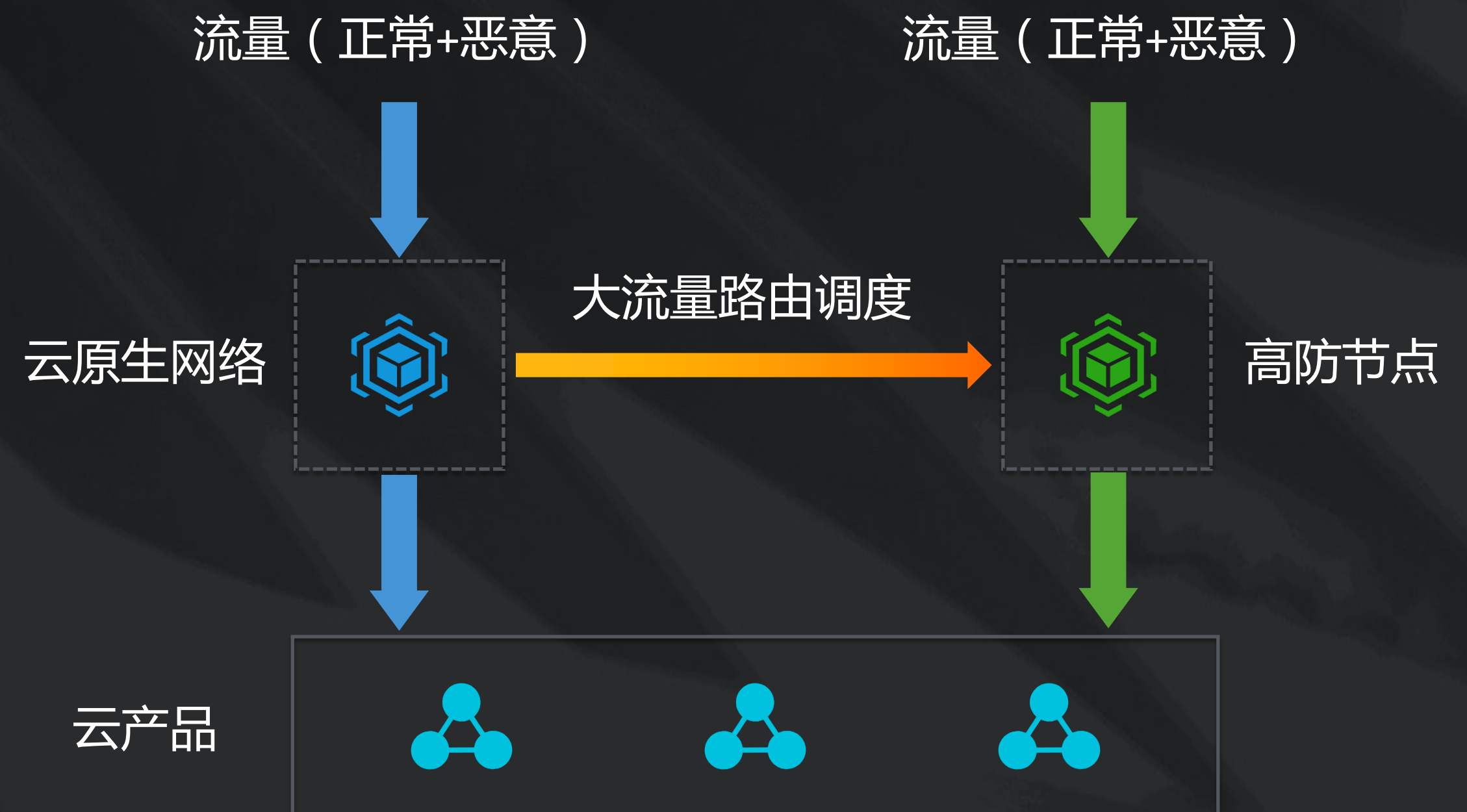
典型场景：游戏行业防御DDoS攻击

场景需求

1.多IP、多端口，不要通过代理模式接入

2.游戏上量快，尽量轻量化部署，多区域统一方案

3.对延迟和稳定性要求高，不要改变网络架构



防护调度：

采用路由代播技术，网络入口调度高防节点，对客户透明

典型场景：无法修改DNS一键启用WAF

场景需求

1. 不做DNS修改，接入WAF



业务流量走向：

业务流量走向不发生变化；

可提供全量请求日志与攻击防护日志；

安全防护：

流量进行分析bot流量与WEB攻击流量进行分析后，可进行观察、系统默认拦截，自定义拦截等；

提供AI智能防护，主动防御、全局流量限速、0Day默认防护等安全能；

Thanks_

CODE FUTURE_