

中立安全·赋能产业

Anycast弹性IP

全球视角下的公网加速与安全解决方案

UCloud优刻得 产品总监 冯业浩

Google Public DNS: 8.8.8.8

```
[root@10-50-78-94 ~]# ping -c 6 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=52 time=1.14 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=0.534 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=0.545 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=52 time=0.620 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=52 time=0.656 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=52 time=0.603 ms

--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 0.534/0.684/1.149/0.213 ms
```

```
[root@10-11-166-209 ~]# ping -c 6 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=0.724 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=1.15 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=0.738 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=0.594 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=0.744 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=53 time=0.535 ms

--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5003ms
rtt min/avg/max/mdev = 0.535/0.749/1.159/0.199 ms
```

```
[root@10-8-162-17 ~]# ping -c 6 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=4.55 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=4.21 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=4.20 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=4.20 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=4.21 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=53 time=4.17 ms

--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 4.170/4.261/4.557/0.143 ms
```

Google Public DNS: 8.8.8.8



Google Public DNS: 8.8.8.8



UCloud的AnycastEIP



全球加速



分布式服务



防DDoS攻击



全球高可用

AnycastEIP，利用UCloud的全球BGP宣告能力、覆盖全球的十余个海外节点以及节点间的专线资源，提供全球网络加速。

AnycastEIP能够实现IP传输的质量优化，实现多入口就近接入，减少公网延时抖动带来的影响，提升EIP的全球使用体验。

什么是Anycast?

	场景	报文复制	接收方
Unicast 单播	单个源向单个接收方进行通信	无需复制	单个接收方
Multicast 组播	单个源向若干接受方进行通信	复制多份	多个接收方，接收方由IGMP等组播协议进行管理
Broadcast 广播	单个源向其子网内所有资源进行通信	复制多份	多个接收方，接收方为子网内所有资源（无VLAN隔离情况下）
Anycast 任播	单个源向一组接收方进行通信，但实际接收方仍然是一个，由路由协议选择确定	无需复制	一组接收方。该组接受方向互联网宣告相同的地址，报文选择目标服务器是通过路由协议确定的。

- 第一期 洛杉矶、华盛顿、法兰克福、中国香港、新加坡、中国台北、东京 七个边缘接入点，基本覆盖全球核心区域
- 利用UCloud全球专线组成的骨干内网，业务流量可以调度到UCloud所有的海外节点



边缘POP点

AnycastEIP可以用来做什么？

01

全球服务加速

02

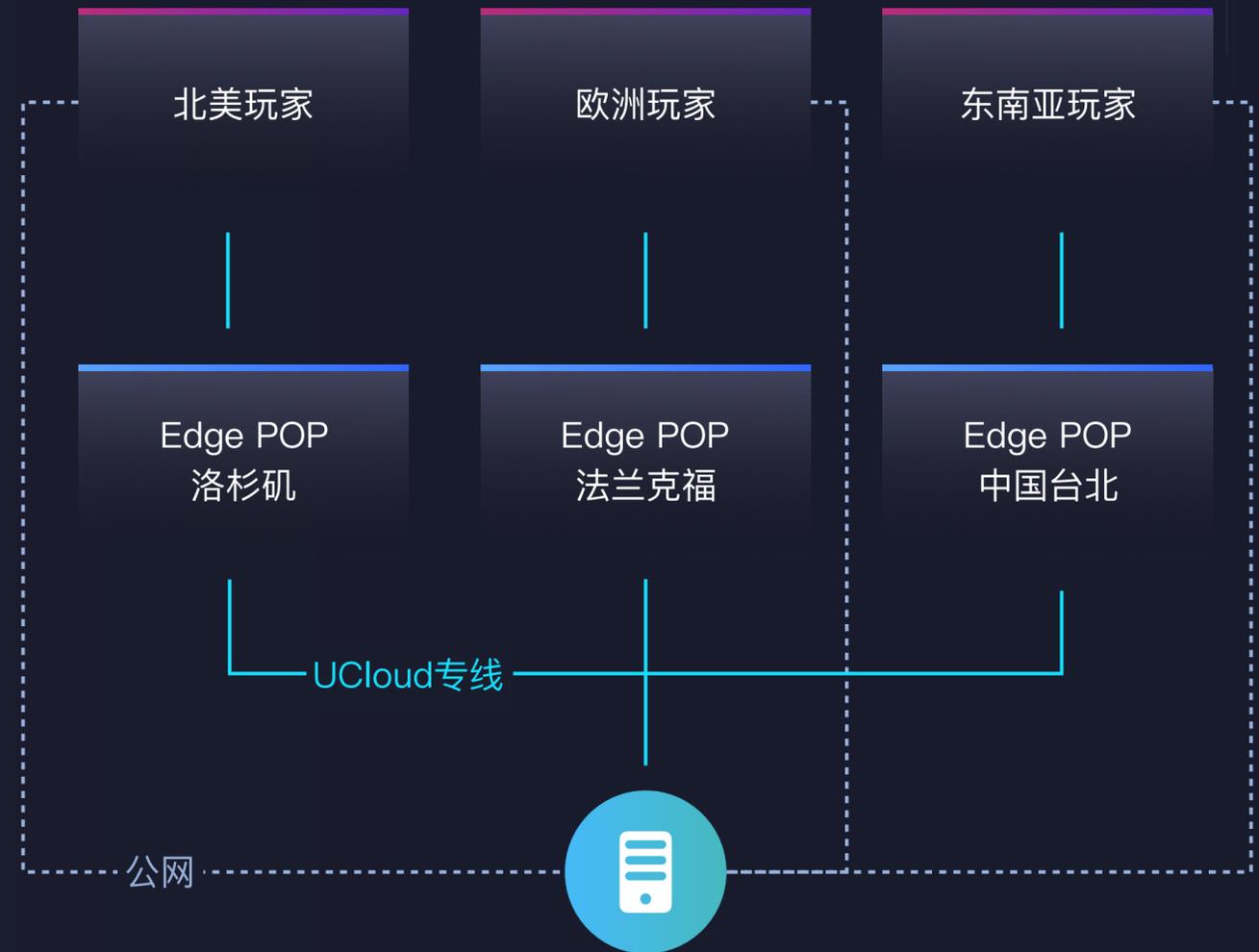
Global Public DNS

03

DDoS全球分布式清洗

全球加速服务

- 普通EIP：单点宣告，全球玩家需要通过公网才能访问。延时高，抖动大。
- AnycastEIP：用户通过UCloud全球的Edge POP就近接入UCloud骨干网，并通过UCloud专线完成传输，保证延时低、抖动小。



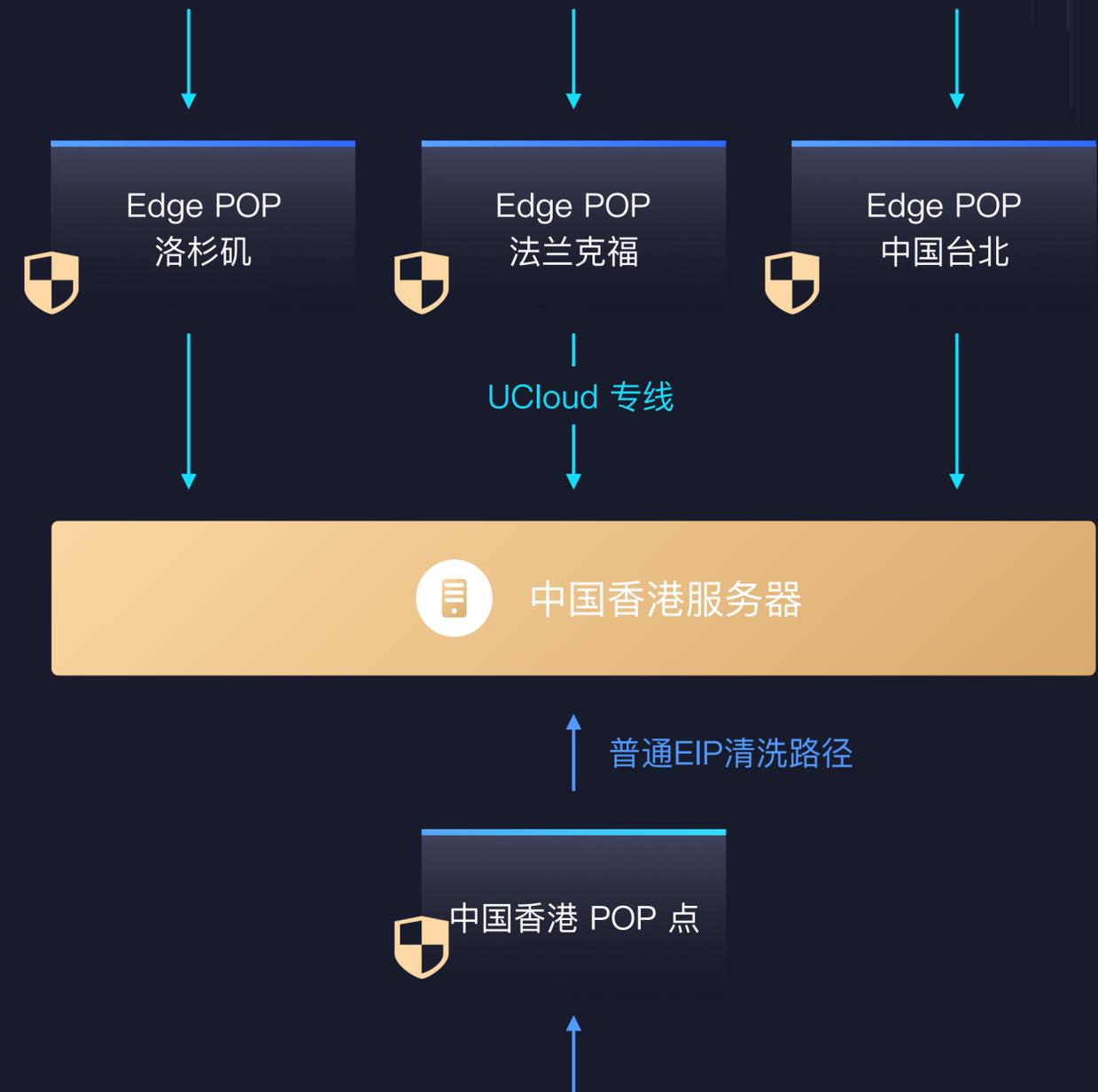
Global Public DNS

- 普通EIP：单点宣告，全球用户需要通过公网才能访问。延时高，抖动大。
- AnycastEIP：使用AnycastEIP，并在多个Edge POP的就近Region直接部署多个同样的服务，用户请求就近处理，达到类似8.8.8.8的效果。

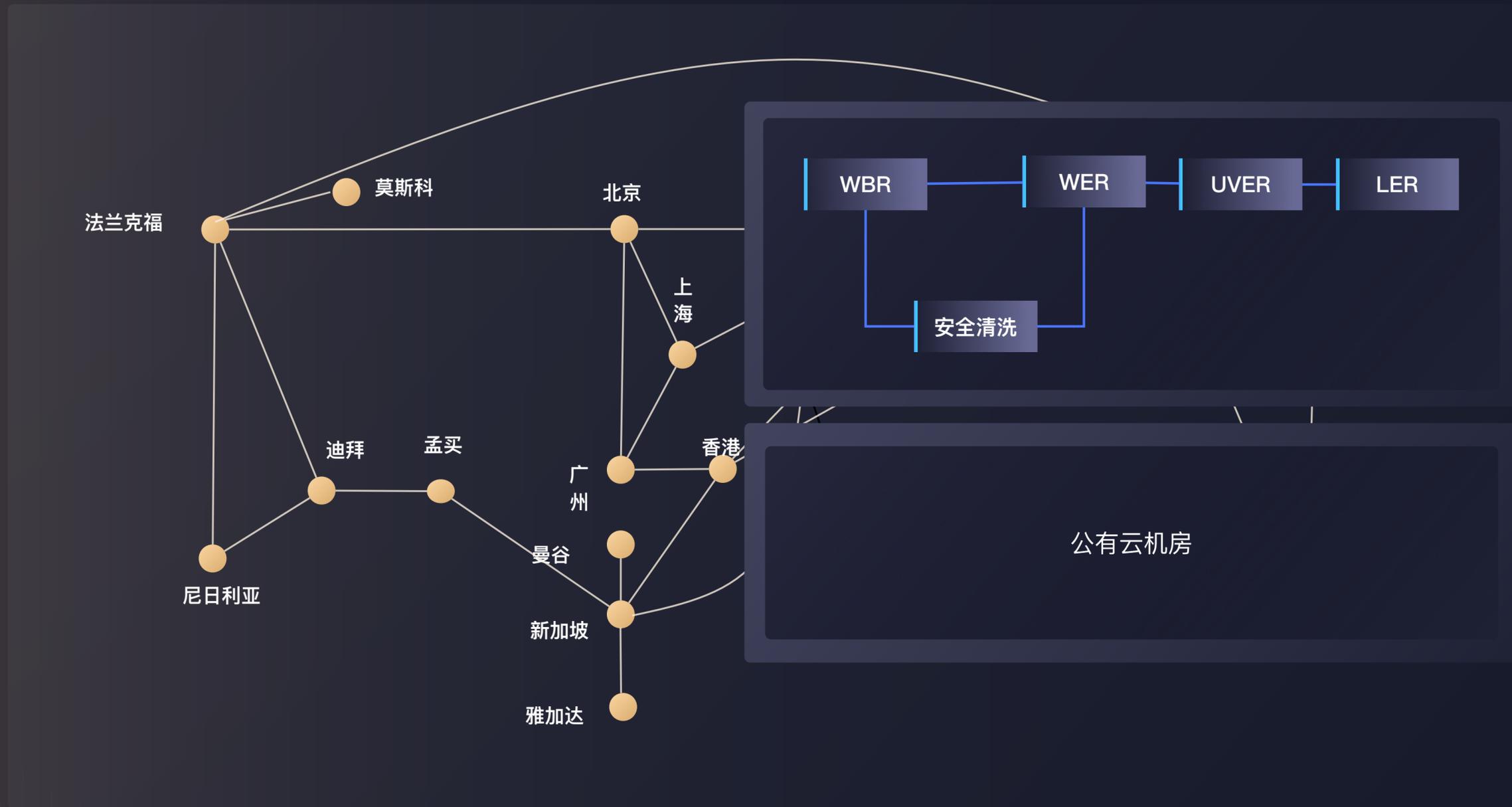


基于Anycast的全球分布式清洗

通过AnycastEIP，将攻击流量负载均衡到多个边缘POP点，并分别进行清洗，清洗后的流量可以通过UCloud专线送到源站。利用分布式清洗和专线回源，突破本地上联等物理限制，有效保证业务安全。

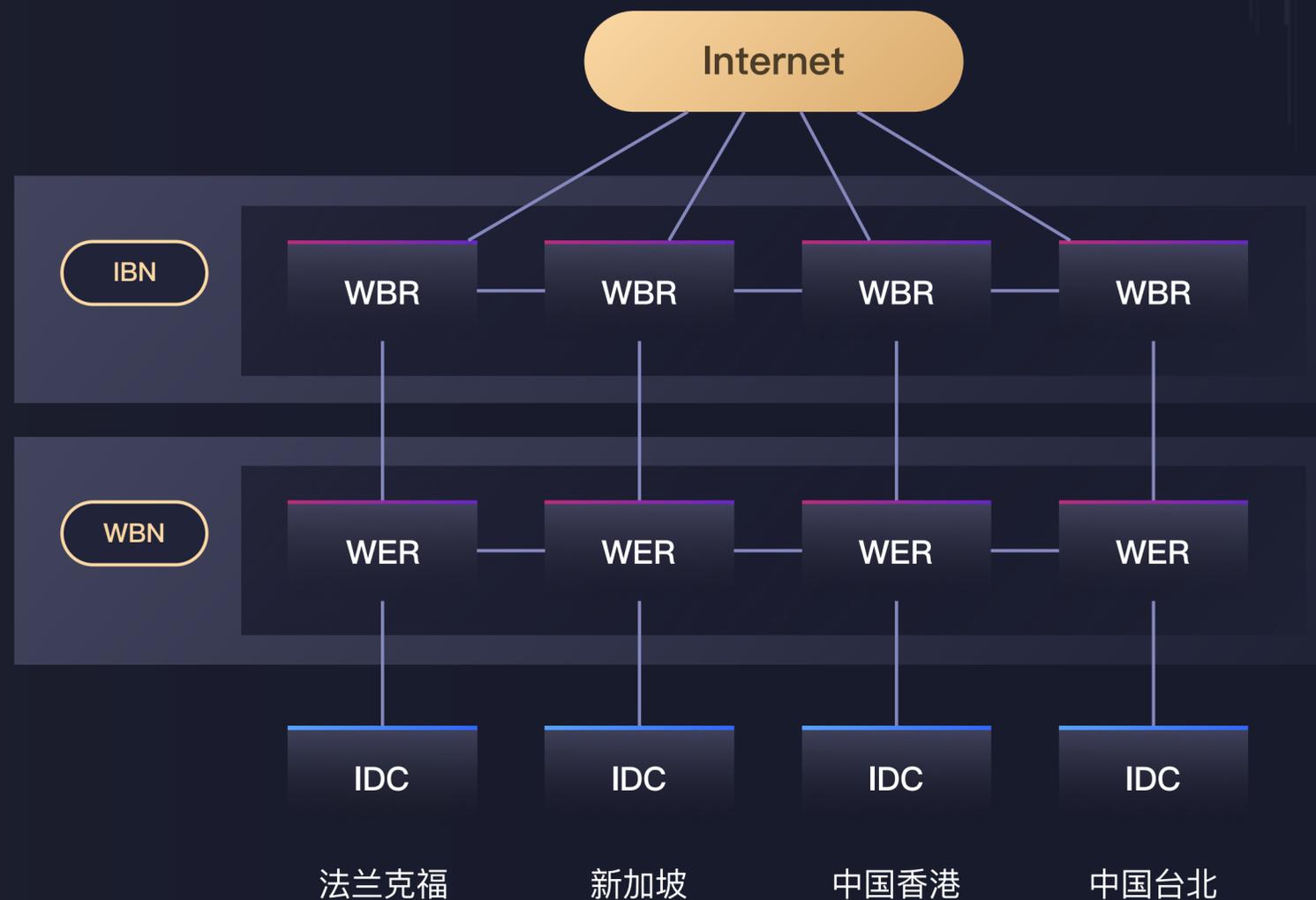


AnycastEIP之基础设施



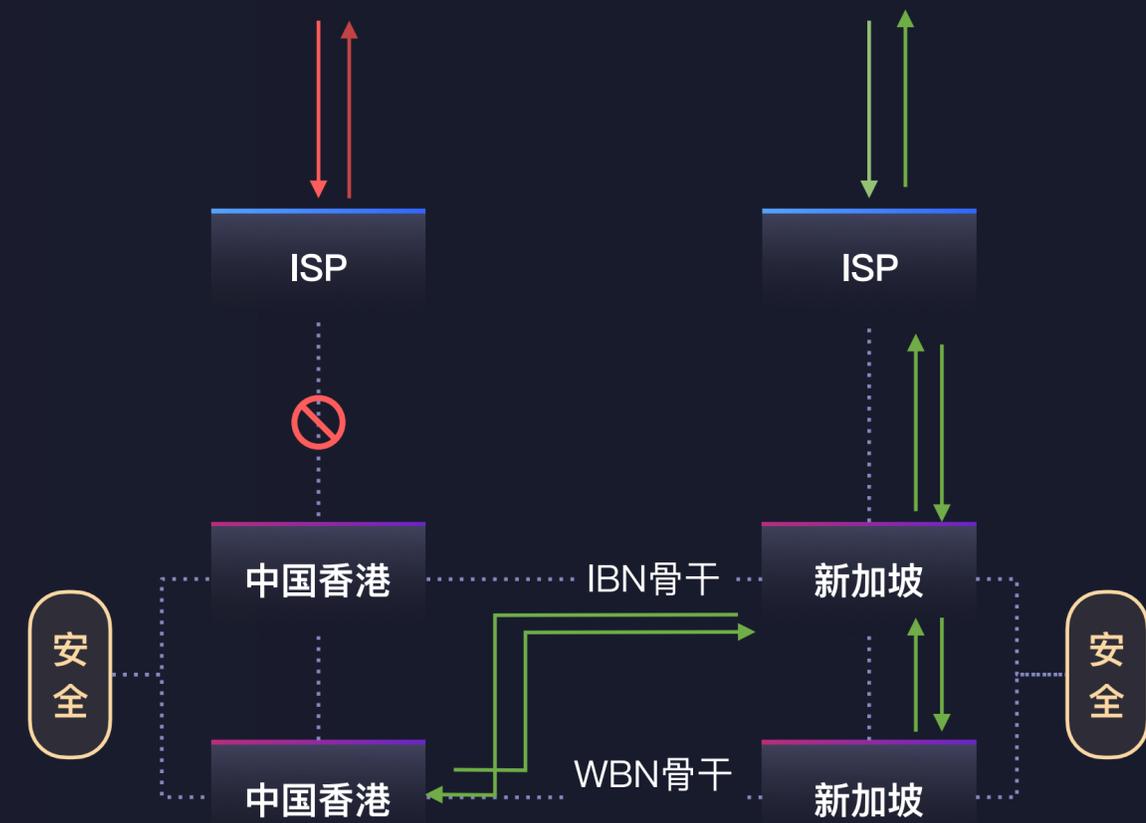
AnycastEIP之基础设施

- IBN网络：机房出口级别的容灾调度
- WBN网络：UCloud之间的公网互访加速
- LBN网络：高速通道的承载网



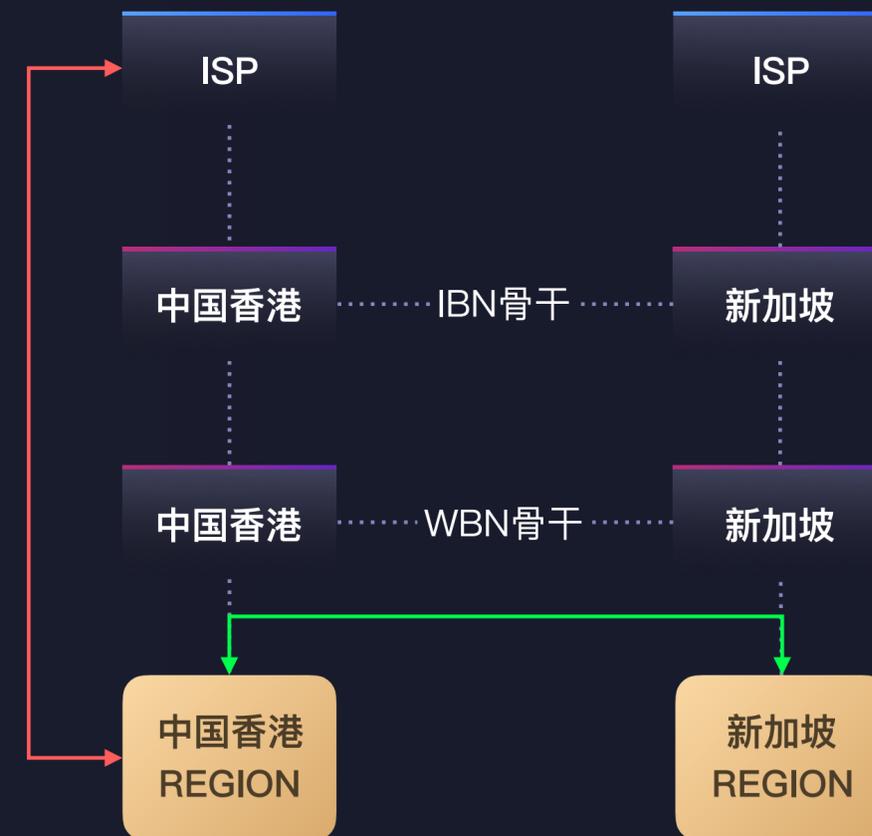
IBN网络：机房的出口容灾

如果海外单个机房的ISP运营商出口全断，则可以依靠IBN网络实现出口的切换，保证机房的出口安全。



WBN网络： UCloud的内部公网加速

如右图所示：正常的公网访问，将通过WBR/WBR路径直接上公网。而不同Region之间的UCloud公网IP的互访，则直接通过WBN网络互联。从而保证UCloud内部公网IP之间互访的质量。



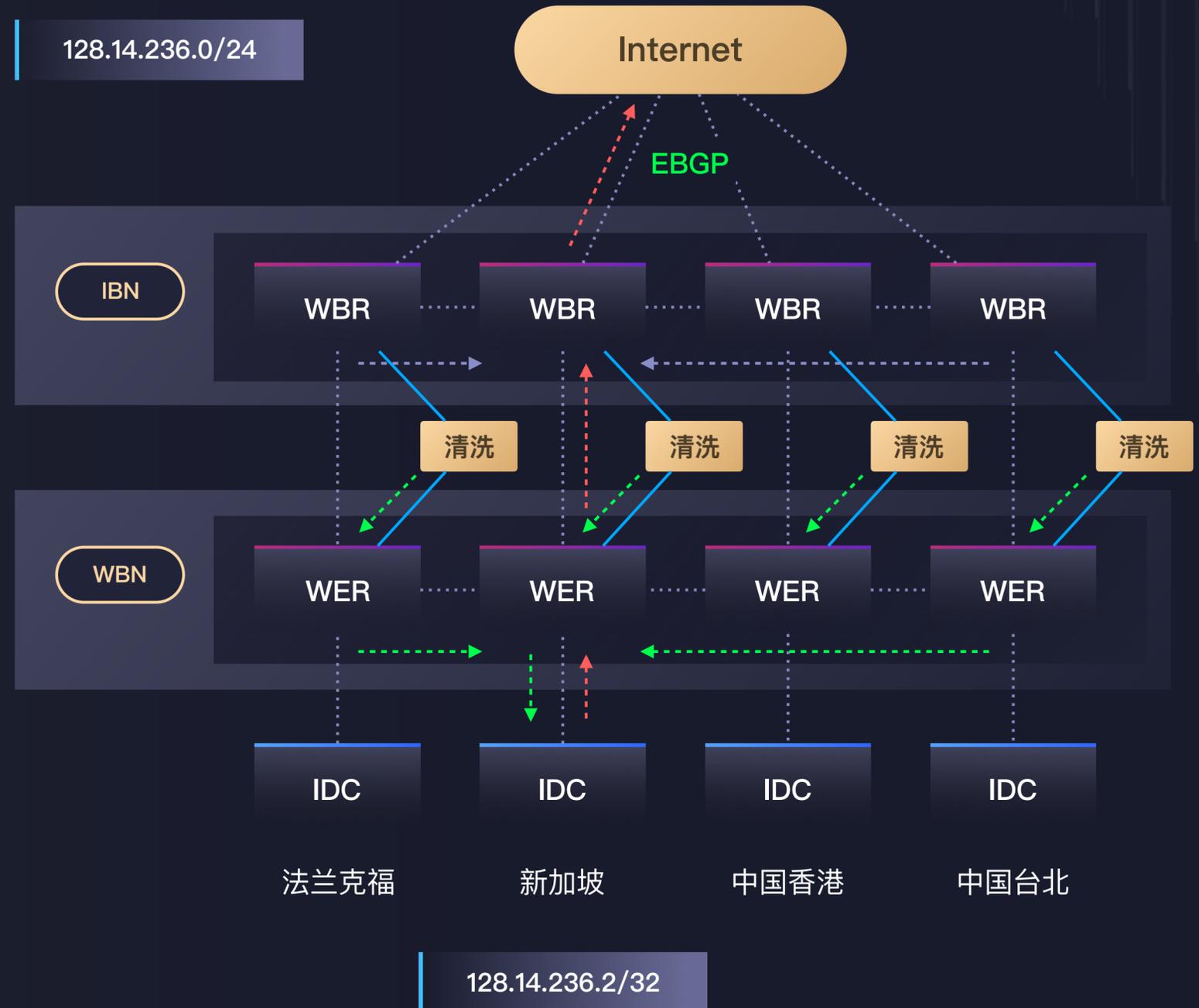
全球加速原理

流量出向:

源机房的核心通过默认路由出本地公网

入向流量:

- 跨机房回源: 公网路由通过BGP选路, 根据就近原则选择合适的机房入口流量回到各机房WBR, WBR通过IBN网络查询IBGP路由源机房的WBR并送到WER后完成回源。
- 本机房回源: 公网路由到本机房WBR后将流量送至WER, WER在将流量送至UVER
- DDoS回源: 当源站IP受到DDoS攻击时, 各anycast机房会进行分布式流量清洗, 清洗后的流量需要回注到WBN网络后送回源站



自研POP点安全分析与清洗系统

检测集群

- 基于DPDK开发，10Gbps线速
- 支持包量、流量、Syn/Fin/Rst/Ack/UDP/ICMP等协议检测

清洗集群

- 基于DPDK开发，10Gbps线速，单核达4M pps清洗能力
- 支持多种清洗算法
- 联动自动封堵



一个强大的本地清洗系统需要：

- 足够的公网上联带宽
- 强大的检测系统
- 强大的清洗系统

但是，不是每个地域，每个机房都可以满足以上条件。AnycastEIP利用

UCloud底层架构，可以实现

- 摆脱本地资源限制，全球统一的240Gbps清洗能力，保障客户业务安全
- 安全问题不再成为海外云计算选点的限制

AnycastEIP产品介绍

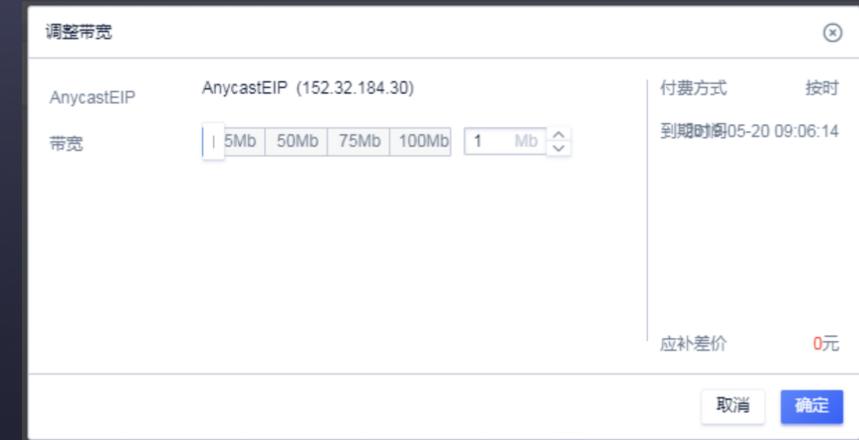
The screenshot displays the UCLLOUD console interface for managing AnycastEIP resources. The top navigation bar includes '全部产品', '默认项目', and '全球服务'. The main content area is titled '基础网络 UNet' and features a tabbed interface with 'AnycastEIP' selected. Below the tabs, there are buttons for '申请AnycastEIP', '释放', and '更多'. A table lists the resources with columns for '资源名称', 'IP地址', '资源ID', '业务组', '绑定资源数量', '带宽', '到期时间', and '操作'. Two resources are listed: 'may.he' and 'AnycastEIP'. The '操作' column for each resource contains '详情' and '绑定资源' buttons.

资源名称	IP地址	资源ID	业务组	绑定资源数量	带宽	到期时间	操作
may.he 修改名称及备注	152.32.184.43	anycasteip-mdezj5xg	Default	0	1Mb	2019-05-20 09:45:40	详情 绑定资源 ...
AnycastEIP 修改名称及备注	152.32.184.30	anycasteip-zfpwwayn	Default	1	1Mb	2019-05-20 09:06:14	详情 绑定资源 ...

AnycastEIP产品介绍



支持全球级别的统一带宽计费，支持带宽升降级。



支持绑定多个Region的uhost或者ulb，支持资源的健康检查。

Anycast全球清洗产品介绍

Anycast全球清洗

防护包管理 清洗详情 安全策略管理 使用记录

创建防护包

防护包ID	防护包名称	资源ID	AnycastEIP	状态	剩余时长 (s)	到期时间	自动续包	操作
usec_anycast-4fr3j11k	444444	usec_anycast-4fr3j11k		正常	3600	2019-06-14 17:21:05	关闭	开启自动续费 绑定AnycastEIP 历史资源
usec_anycast-hnsufrcg	333333	usec_anycast-hnsufrcg		正常	3600	2019-06-14 16:19:33	关闭	开启自动续费 绑定AnycastEIP 历史资源
usec_anycast-z42p5tih	new-test	usec_anycast-z42p5tih	106.75.189.54	已用尽	0	2019-06-14 14:24:55	关闭	重新购买 删除 历史资源
usec_anycast-exblo5bb	test_wu	usec_anycast-exblo5bb		正常	3600	2019-06-13 19:56:21	开启	关闭自动续费 绑定AnycastEIP 历史资源
usec_anycast-alv1vxew	123测试	usec_anycast-alv1vxew		正常	3600	2019-06-13 19:48:06	关闭	开启自动续费 绑定AnycastEIP 历史资源
usec_anycast-sbkl15c	xxx	usec_anycast-sbkl15c		正常	3600	2019-06-13 18:22:11	关闭	开启自动续费 绑定AnycastEIP 历史资源

Anycast全球清洗产品介绍

支持最高240G的全
球清洗能力

支持弹性清洗

支持区域黑洞

支持清洗策略的自
助调整

支持自助解封

Anycast存在的问题

● 次优化问题

由于公网环境异常复杂，Anycast大部分情况下带来的都是优化，少数情况下也可能带来恶化

● 单程加速问题

入向走UCloud专线，出向仍然走的是公网，只能带来单向的加速效果

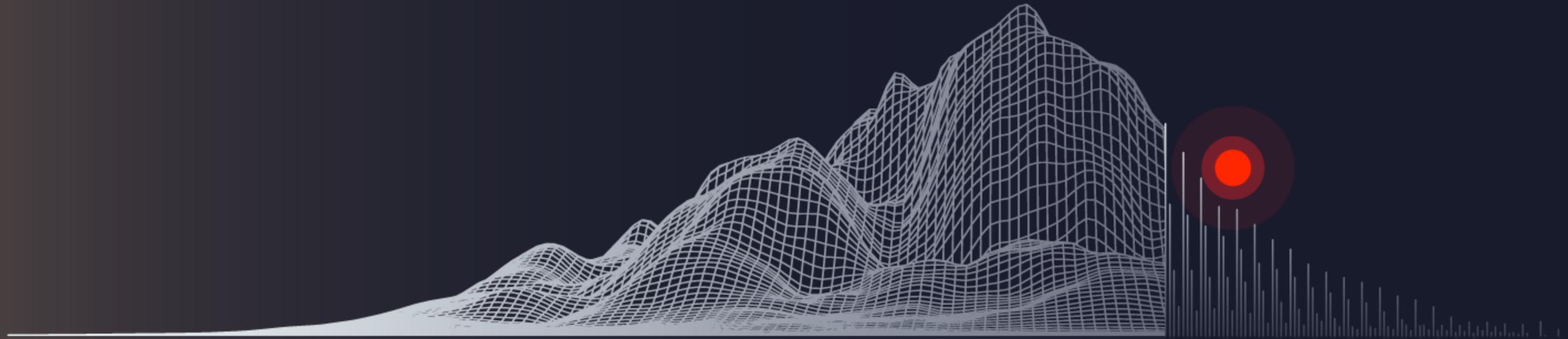
AnycastEIP后续产品规划

● Global ULB

全球Anycast加速的负载均衡，解决单向加速问题，实现全球高可用

● Global PathX

基于Anycast实现全球加速，解决单向加速问题。



THANKS