网易 DDoS 防护建设从 0 到 1

网易云 163yun.com × 网易易盾 dun·163·com

DDoS的现状和趋势

小结

1

2

3

4

About网易安全

网易DDoS防护建设

业务线纷繁复杂，带来巨大的安全挑战

1 100多款游戏产品

网易游戏
游 戏 热 爱 者




2 电商、教育、互娱、社交

电子商务


在线教育



互动娱乐


社交论坛


3 新闻、邮箱、硬件、金融

新闻门户

网络邮箱

智能硬件

互联网金融


4 云计算、大数据、人工智能等

云计算

网易云





大数据


网易大数据
Netease Big Data


网易猛犸
Netease Mammut


网易有数
Netease YouData

人工智能


网易安全团队

内容安全

业务安全

移动安全

网络安全

反垃圾

验证码 / 注册保护 / 登录保护 / 活动反作弊 / 风控 / 账号安全

应用加固 / 安全SDK / 渠道检测 / App漏洞扫描挖掘

DDoS防护 / 漏洞扫描 / Web应用防火墙 / 应急响应 / 态势感知 / DLP / 入侵检测

DDoS的现状和趋势

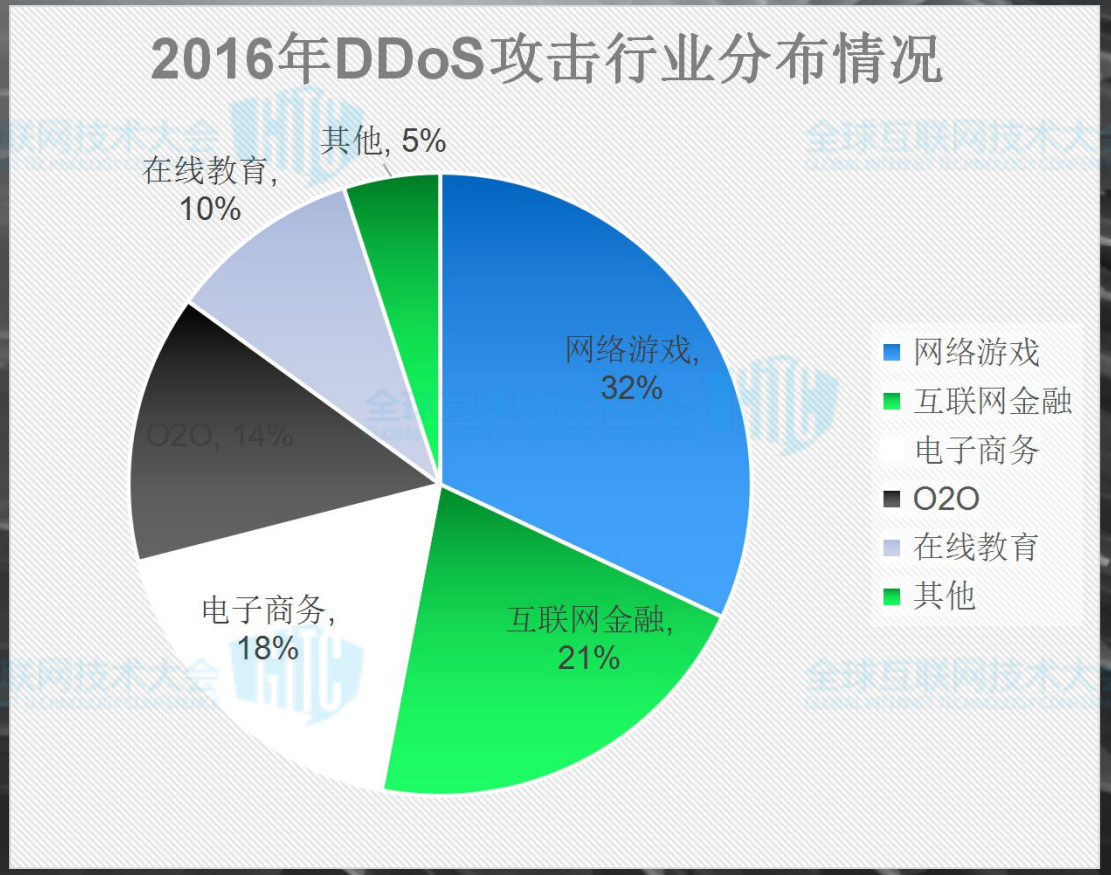
1 About网易安全

2 网易DDoS防护建设

3

4 小结

DDoS攻击趋势



注：数据来源说明（CNCERT/CC）

DDoS攻击趋势

攻击发起的全球化趋势

IoT设备被控制作为攻击源

应用层CC攻击仍然是防护的难点

有组织的黑客攻击

超过300G的大流量攻击越来越多

DDoS的现状和趋势

小结

1

2

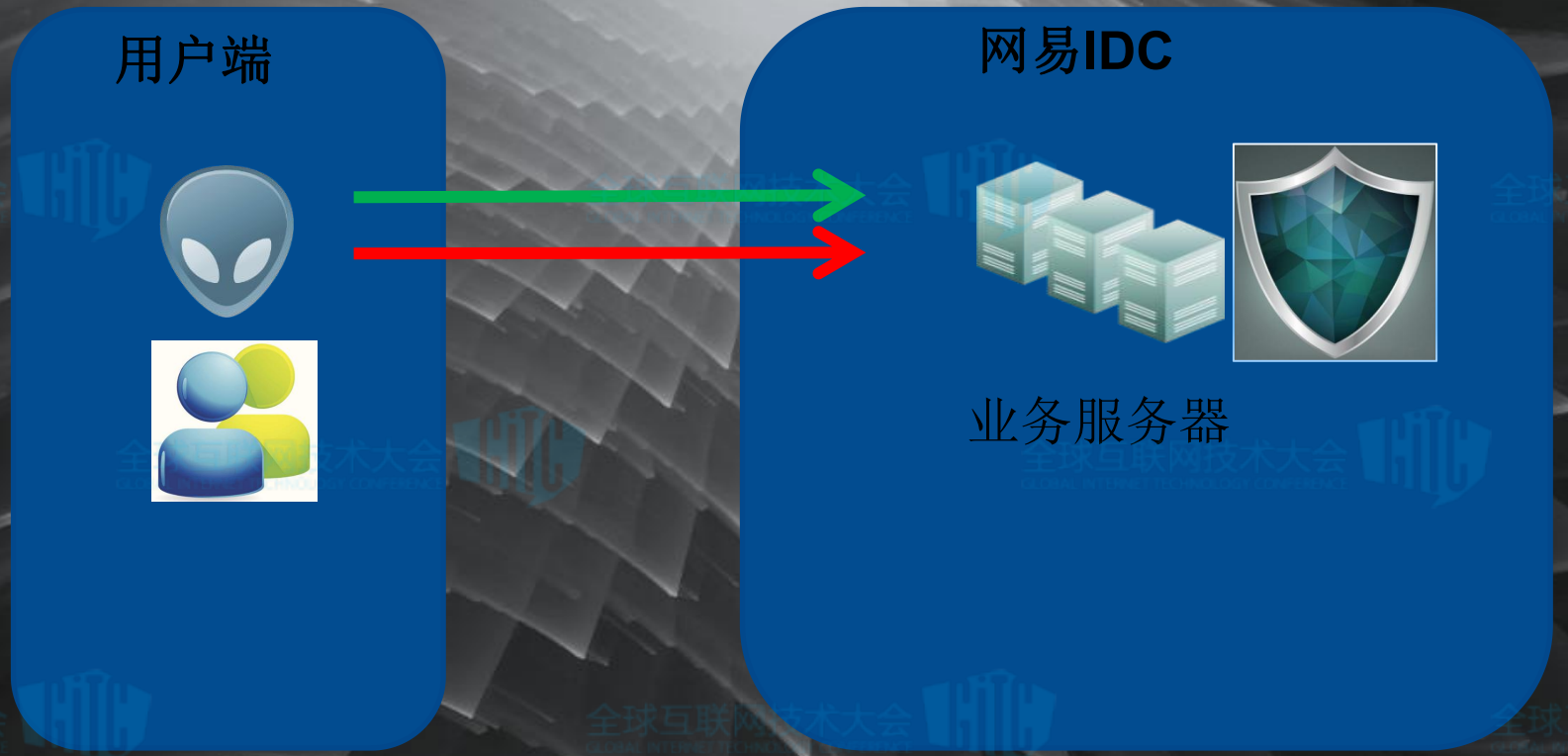
3

4

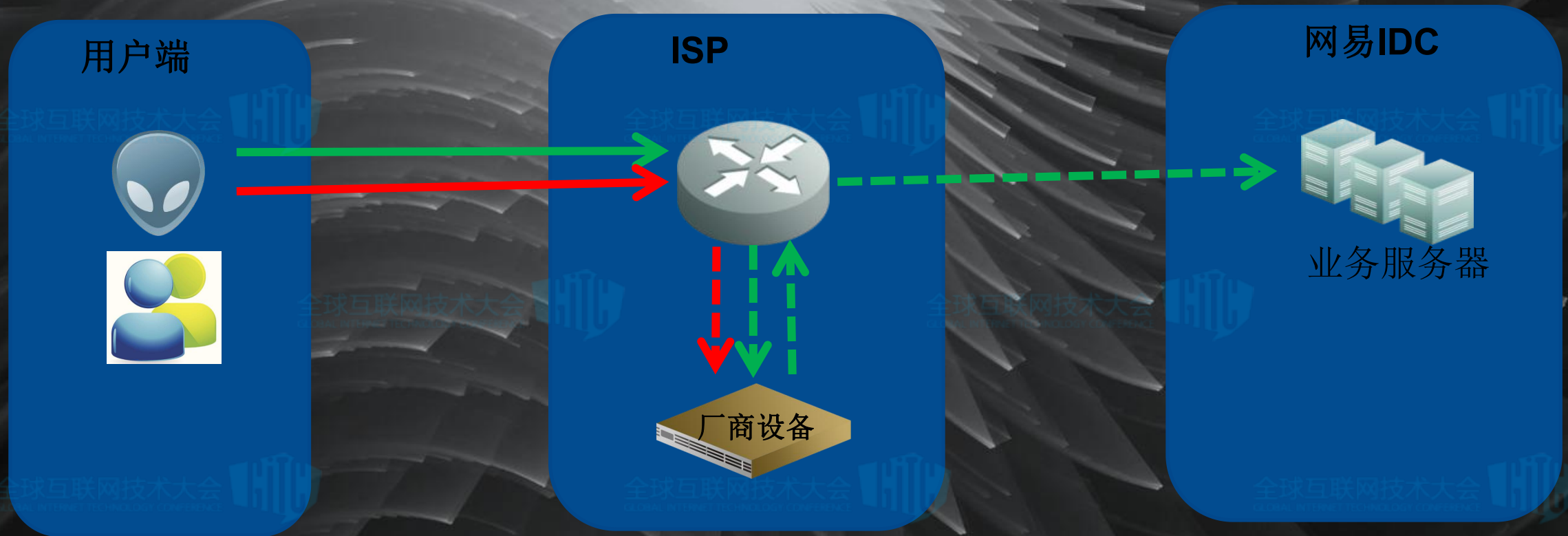
About网易安全

网易DDoS防护建设

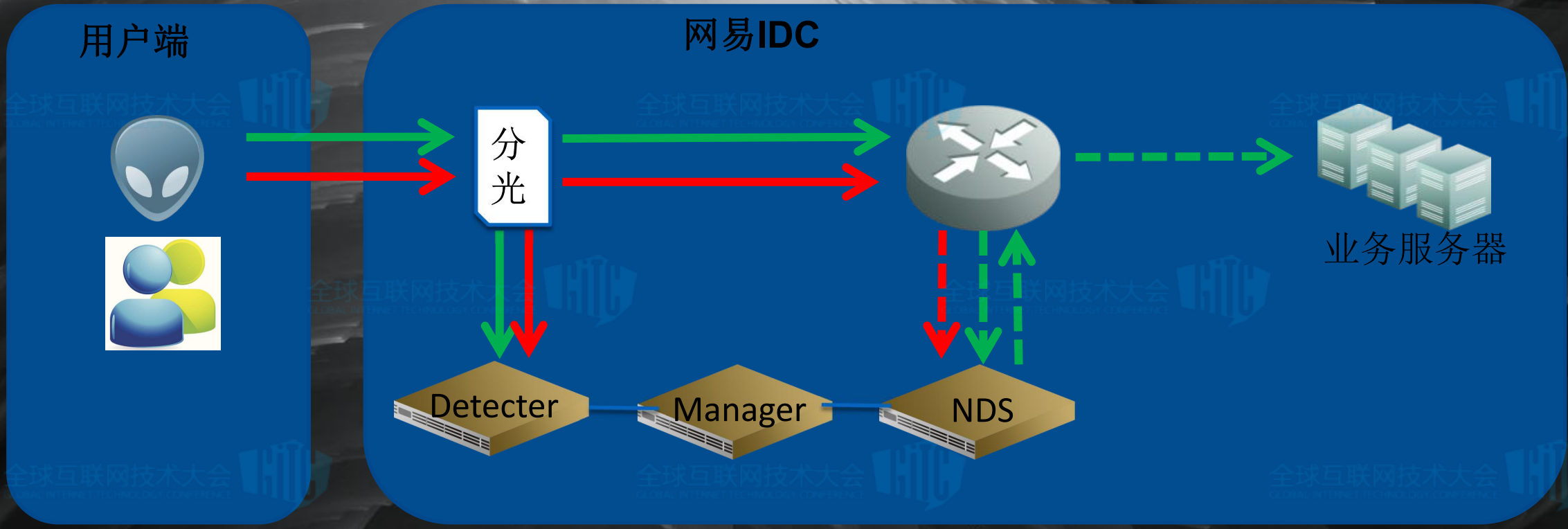
服务器加固和堆硬件



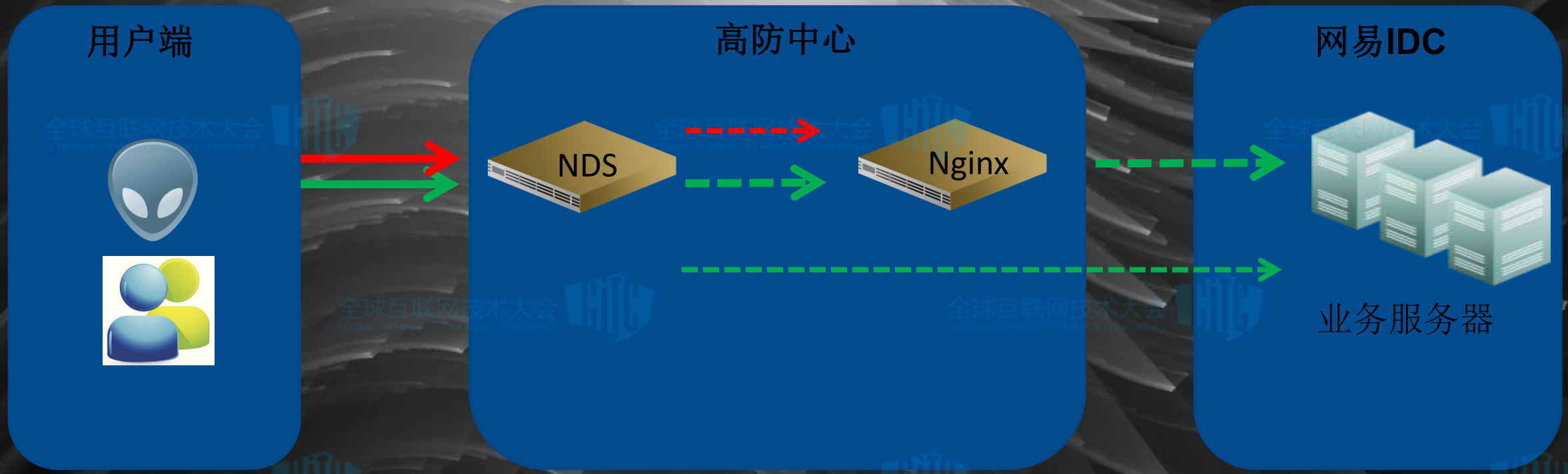
运营商侧设备清洗



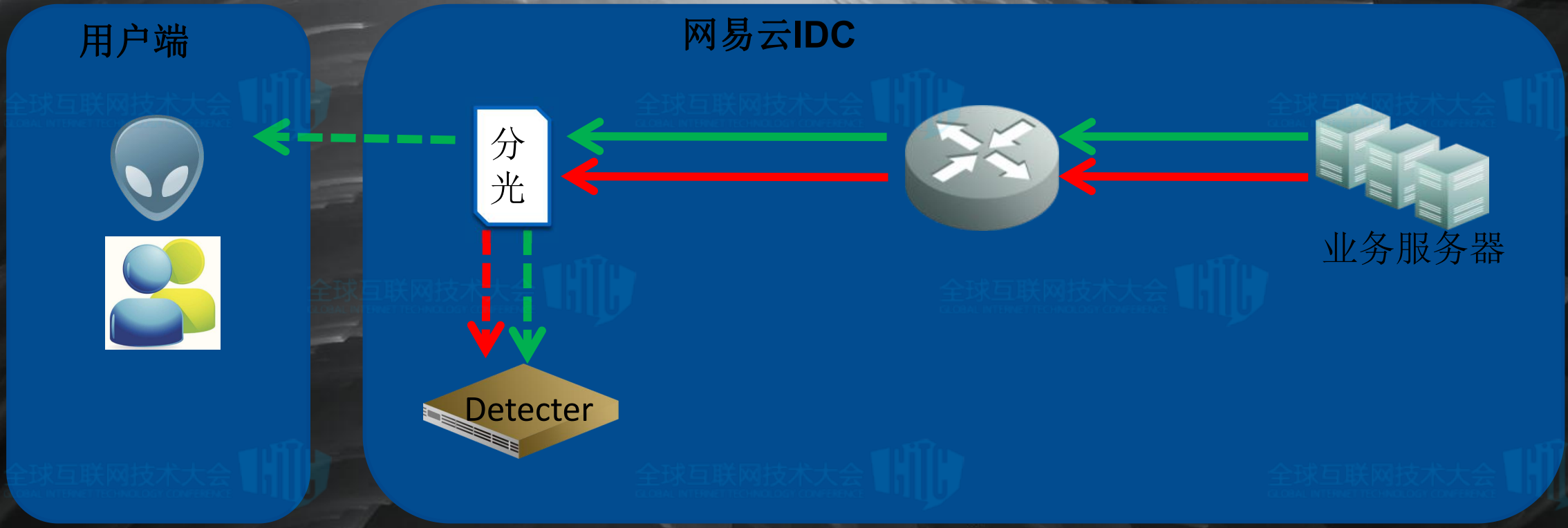
网易自研 NDS 抗D架构



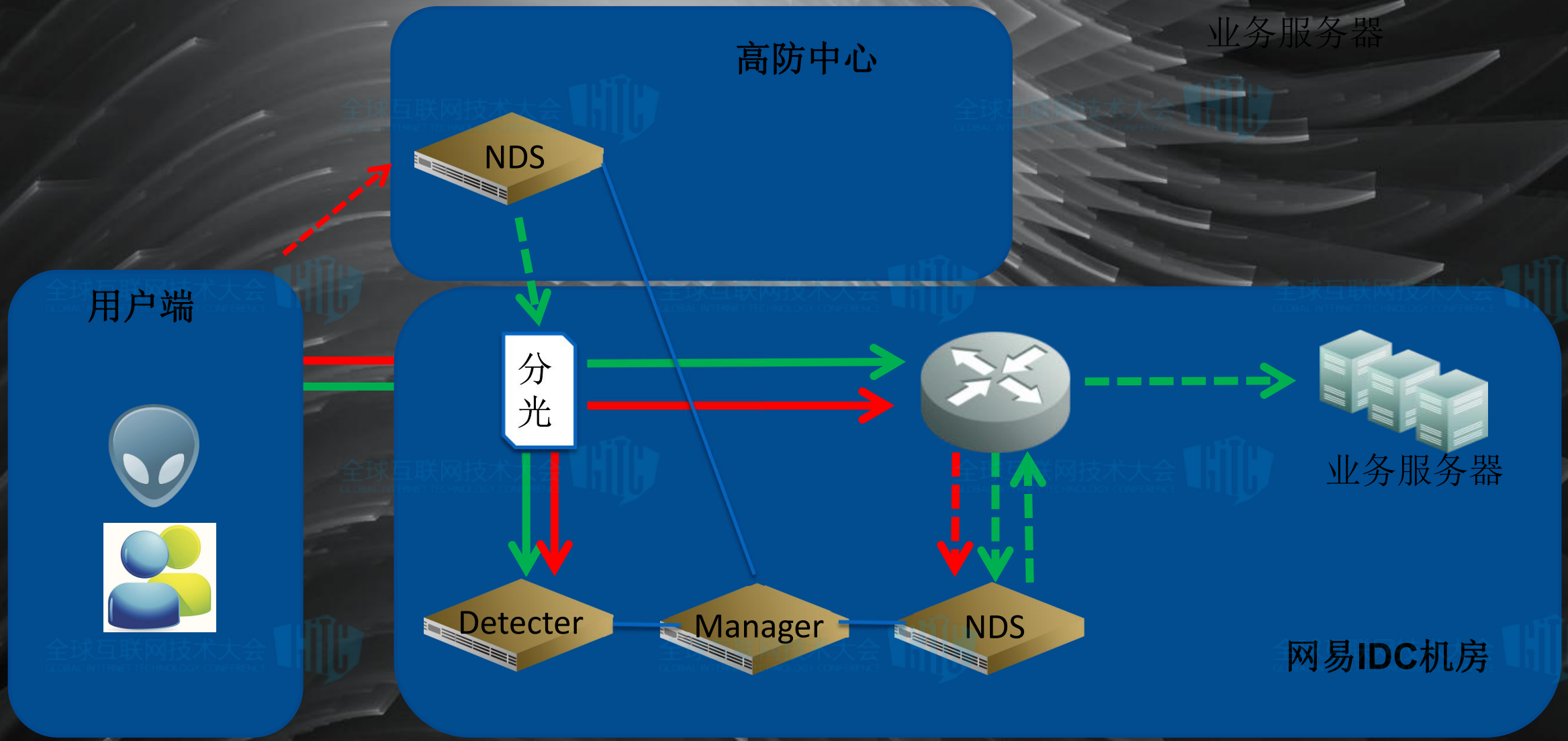
网易云易盾 DDoS 高防架构



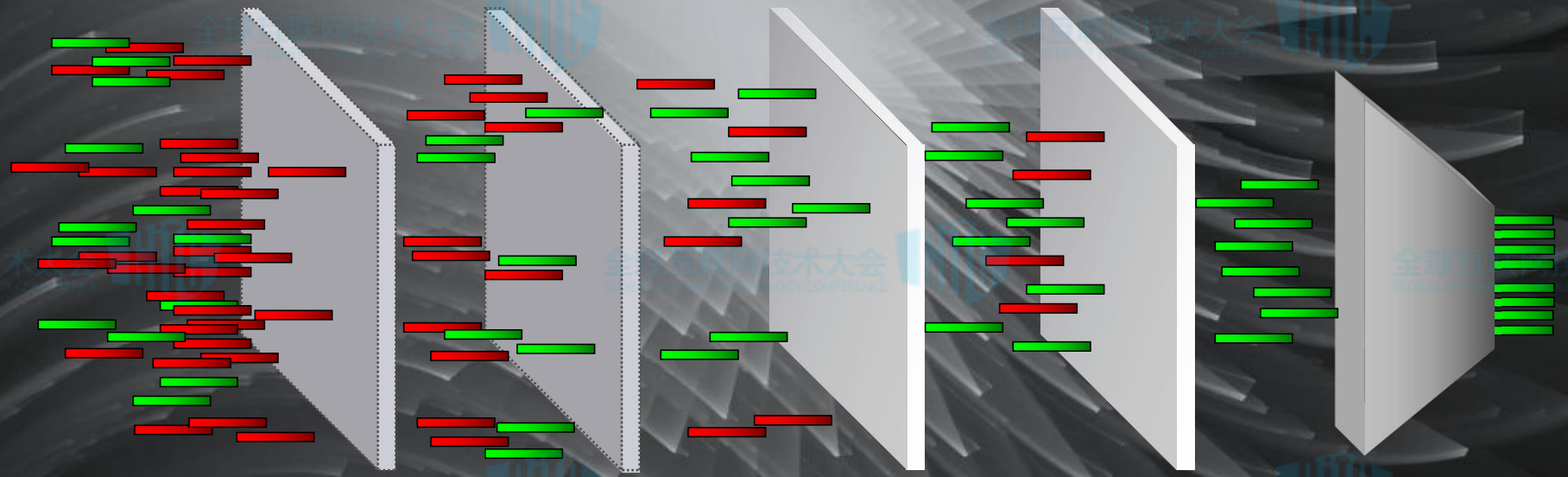
Outbound 流量检测



云端本地联动



多层次立体防护



静态/动态过滤
- 黑白名单
- ACL过滤
- TCP状态机验证
- 畸形包过滤

客户端真实性检测
- SYN Cookie验证
- RESET验证
- TCP反弹验证
- TTL验证

特征识别
- 网络层特征
- 传输层特征
- 应用层特征
- 自定义特征

应用层分析
- JS 反射
- HTTP 指纹校验
- 插件过滤
- 信誉库验证

限速
- 源IP限速
- 目的IP限速

IP 信誉库

- 通过各类僵尸网络挖掘技术、DDoS攻击防御时产生的黑名单等，形成C&C主机及肉鸡IP库
- 根据IP活跃时间评估僵尸网络主机活跃时间，将活跃的主机地址作为恶意流量过滤地址列表
- 共享IP信誉库
  - 网易云易盾反垃圾
  - 网易邮件反垃圾
  - 网易云易盾验证码
  - 网易云易盾反作弊
  - …

基于地理位置的压制

001.050.078.000	001.050.078.255	中国	宁夏	*	*	电信	基站
001.050.079.000	001.050.079.255	中国	宁夏	*	*	电信	基站
001.068.000.000	001.068.000.255	中国	山西	*	*	电信	基站
001.068.001.000	001.068.001.255	中国	山西	*	*	电信	基站

前2列分别是起始和终止IP地址，其余的从左往右依次是：

第3列：国家

第4列：省份/直辖市

第5列：城市

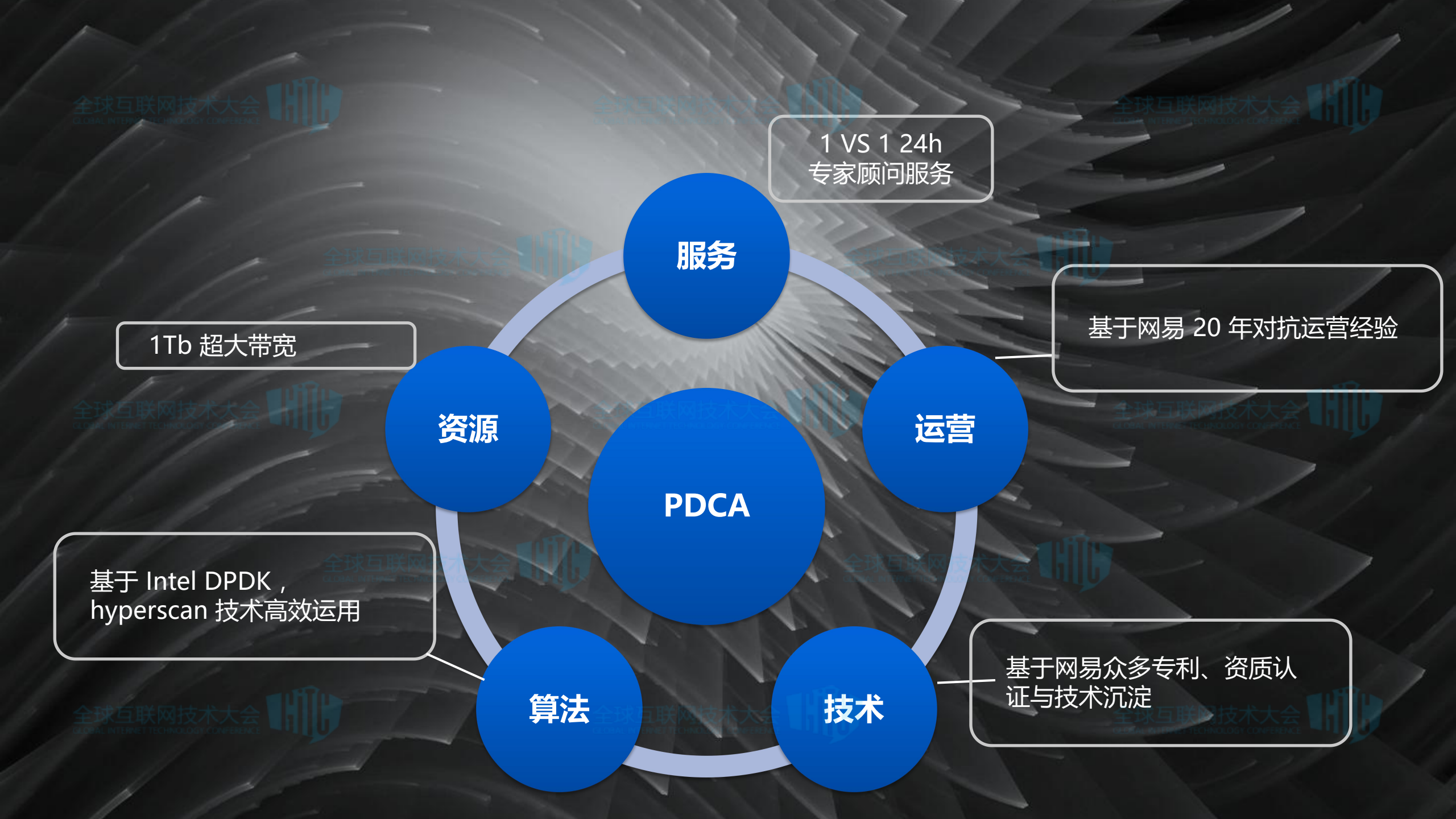
第6列：所有者（基站库中所有者与运营商一致）

第7列：运营商/线路

第8列：基站类型（普通基站/WIFI）

易盾抗D服务

全方位防护	超大防护带宽	全业务支持	快速接入	高安全性
• 全面支持SYN/ACK/ICMP/UDP/NTP/DNS/HTTP等各类Flood以及CC攻击等常见攻击类型的防护。	• 提供1T超大防护带宽，单IP防护能力最大可达数百G，超大带宽，才能从容应对超大流量攻击。	• 全面支持TCP/UDP/HTTP/HTTPS等协议，满足网络游戏各种类型的业务需求。	• “5分钟”即可完成业务切换，即使在被攻击中，也可快速接入，实现应急防护，最大限度减少损失。	• 基于网易20年的网络安全防护经验，尤其是在游戏领域独有的技术积累，保障业务的高安全性、高可靠性。


1 VS 1 24h
专家顾问服务
服务
1Tb 超大带宽
资源
基于网易 20 年对抗运营经验
运营
PDCA
基于 Intel DPDK，
hyperscan 技术高效运用
算法
技术
基于网易众多专利、资质认
证与技术沉淀

DDoS的现状和趋势

小结

1

2

3

4

About网易安全

网易DDoS防护建设

1到N

- DDoS威胁情报共享
  - 包括IP库，攻击特征，攻击工具
- Outbound攻击联防
  - 各个本地IDC机房共同封杀被攻击IP
- 与运营商联动

1到N

- 业务流量模型的智能学习
  - 使用用数据挖掘、机器学习和深度学习等手段，利用算法模型来解决不同场景下的业务流量模型
- 深层次DDoS攻击探测
  - 针对数据异常流量分析、应用层分析、主机识别、协议分析、指纹检测、连接跟踪、端口保护、流量控制等对数据包的多层深层次的攻击检测
- 基于多维度信誉库（IP，设备，指纹）的清洗策略
  - 基于网易大数据，建立针对用户IP、用户设备、用户指纹等多维度的信誉库，在DDoS防护时根据信誉进行区分
- 提供客户端SDK，增加人机识别功能
  - 提供Win，IOS，Android端SDK，采集用户鼠标键盘等操作轨迹，真假人机识别的对抗

Q & A