云清之道

构建AntiDDoS生态共同体

Email: alan.qian@huawei.com
WeChat: AlanQianChina

AGENDA

IDCC

I DDOS战争二十年

II DDOS的世界是平的

III 几个重要趋势

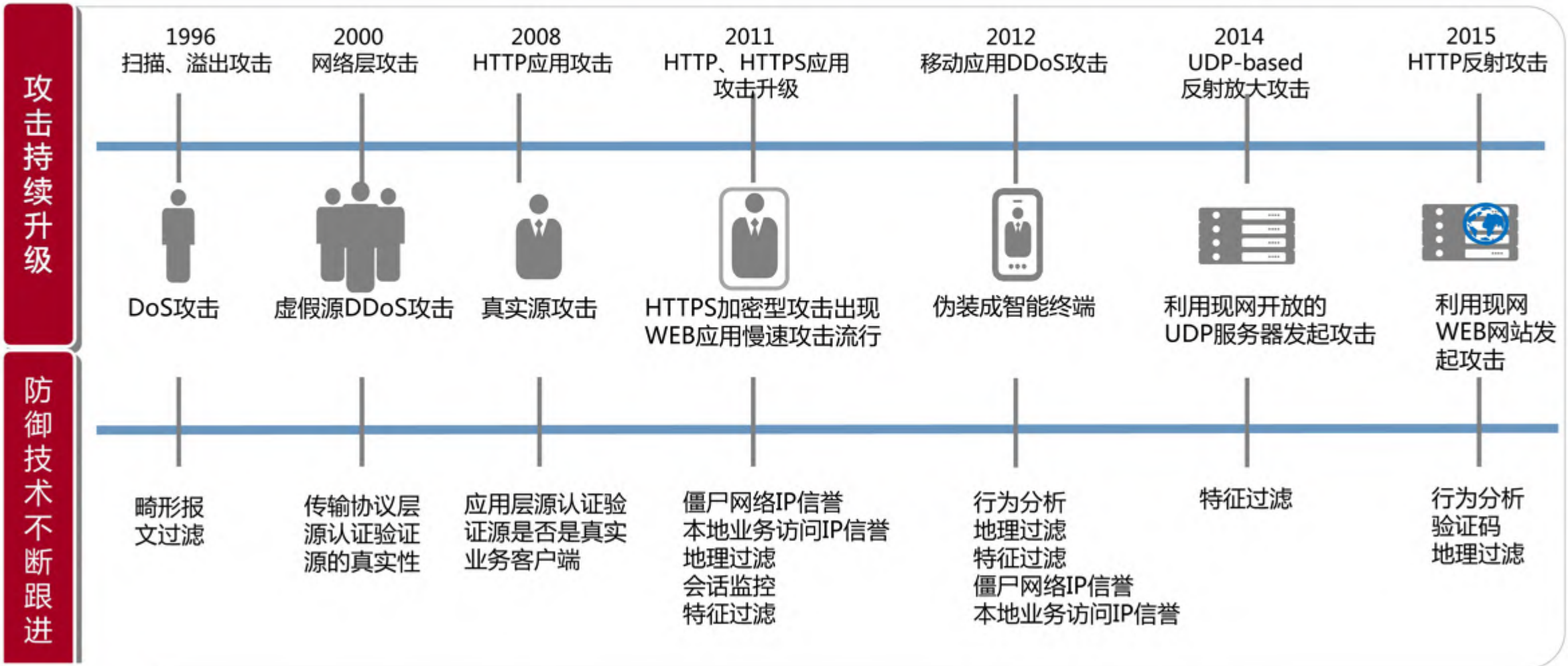
IV 数据中心面临的主要DDOS威胁

V DDOS防御要点

VI 云清联盟及运营考虑

DDoS战争二十年

IDCC



DDoS的世界是平的，捡根稻草就可以杀人

IDCC

Network Services	Legacy Protocols	P2P Networks	Game Servers	Botnets
DNS	CharGen	BitTorrent	Quake 3	ZeroXS
SNMP	QOTD	Kad	Steam	Sality
NTP				Zeus
NetBios				
SSDP				

NTP服务器分布图

DNS服务器分布图

DDoS的世界是平的，捡根稻草就可以杀人

IDCC

攻击类型	放大倍数	被利用的脆弱命令
NTP amplification attack	556.9	monlist query
DNS amplification attack	28 to 54	Text query
SSDP amplification attack	30.8	SEARCH request
Chargen amplification attack	358.8	Character generation request
SNMP amplification attack	6.3	GetBulk request
NetBIOS amplification attack	3.8	Name resolution
QOTD amplification attack	140.3	Quote request
Quake Network Protocol amplification attack	63.9	Server info exchange
Steam Protocol amplification attack	5.5	Server info exchange
BitTorrent amplification attack	3.8	File search
Kad amplification attack	16.3	Peer list exchange

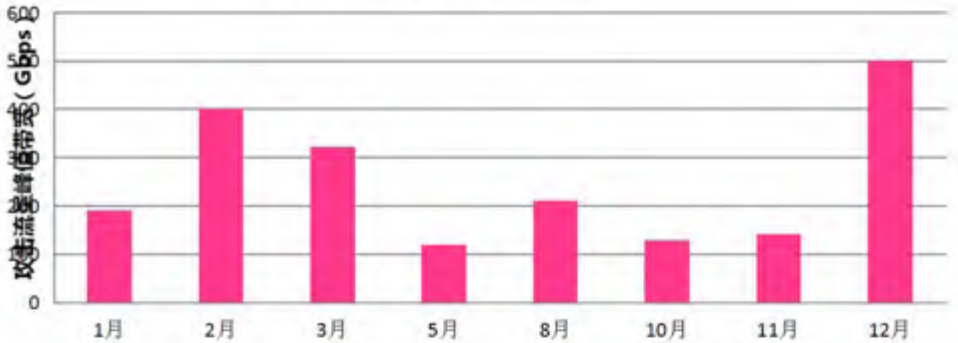
几个重要趋势

1. DDoS攻击向全球化、大流量发展，管道拥塞频发

云和互联网的发展导致DDoS迅速全球化，直接危及链路和在线业务可用性。

超百G攻击频发，直接危及Tier-2/3 运营商/ISP的管道可用性，链路资费昂贵，运营成本增高。

2014年超百G攻击频发



Source:华为云安全中心、Arbor

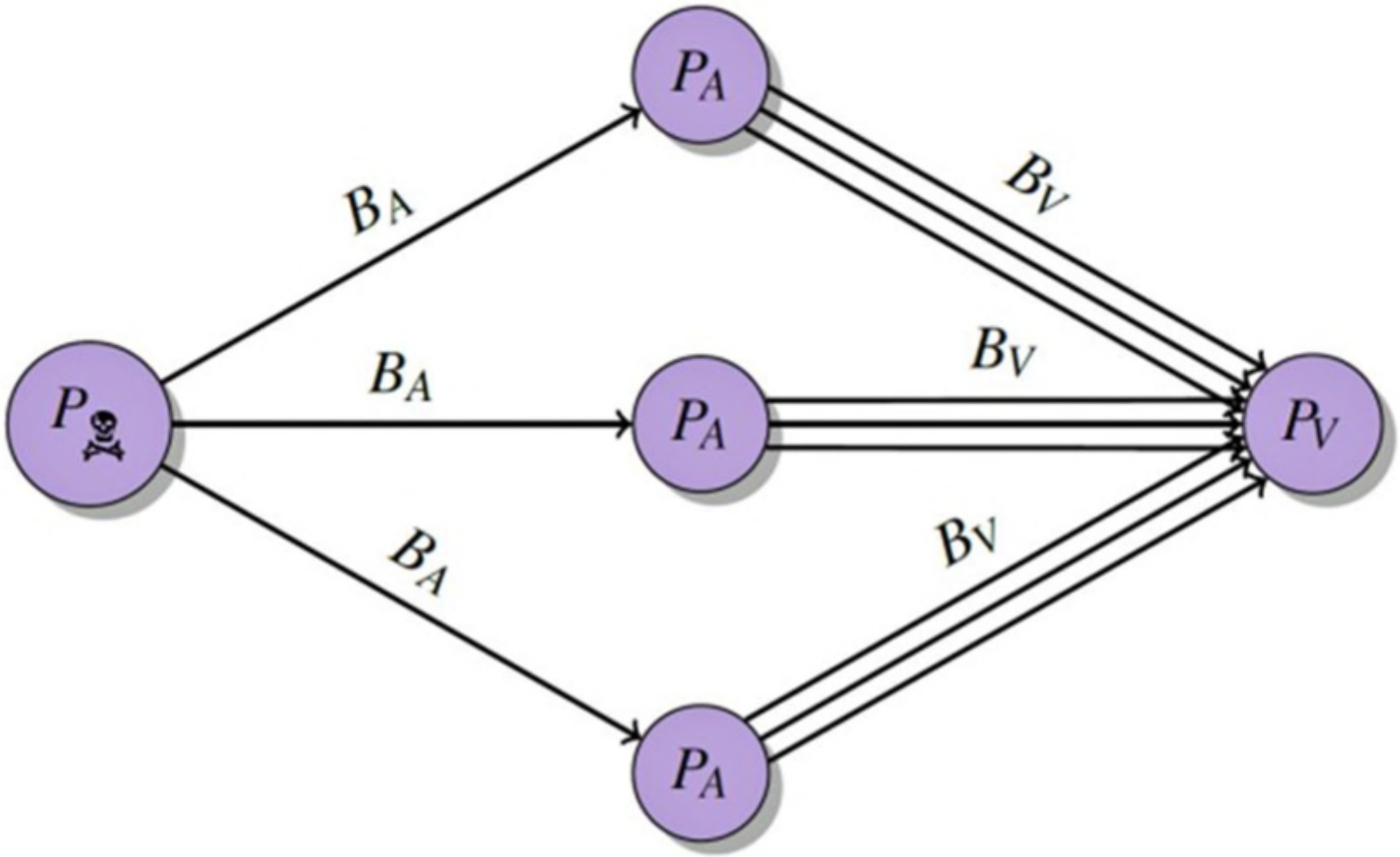
攻击事件1

2013年3月，Spamhaus遭受300G攻击，欧洲多国运营商管道拥塞，互联网访问缓慢。

攻击事件2

2014年12月，阿里云主机遭受500G攻击，其DC出口带宽只有300G，链路拥塞。如不及时处理，阿里云业务会全面瘫痪。

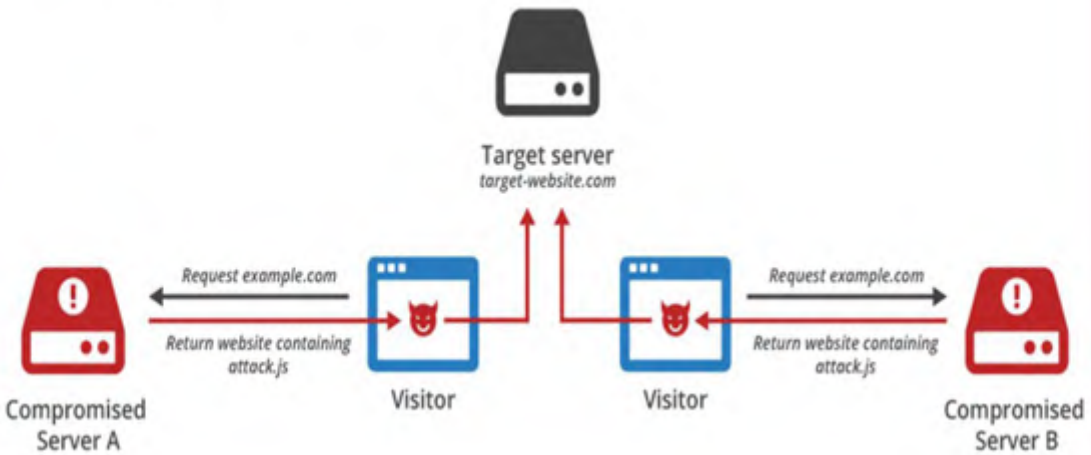
2. 2016年，利用P2P网络发起UDP反射放大攻击会成为趋势



IDCC

3. HTTP反射攻击势必崛起

JavaScript-based DDoS



攻击要素：可嵌入JavaScript的海量访问的社交网站
攻击危害： JavaScript定义的URI决定服务器资源消耗程度
防御手段：地理过滤、重定向验证码

WordPress pingback DDoS

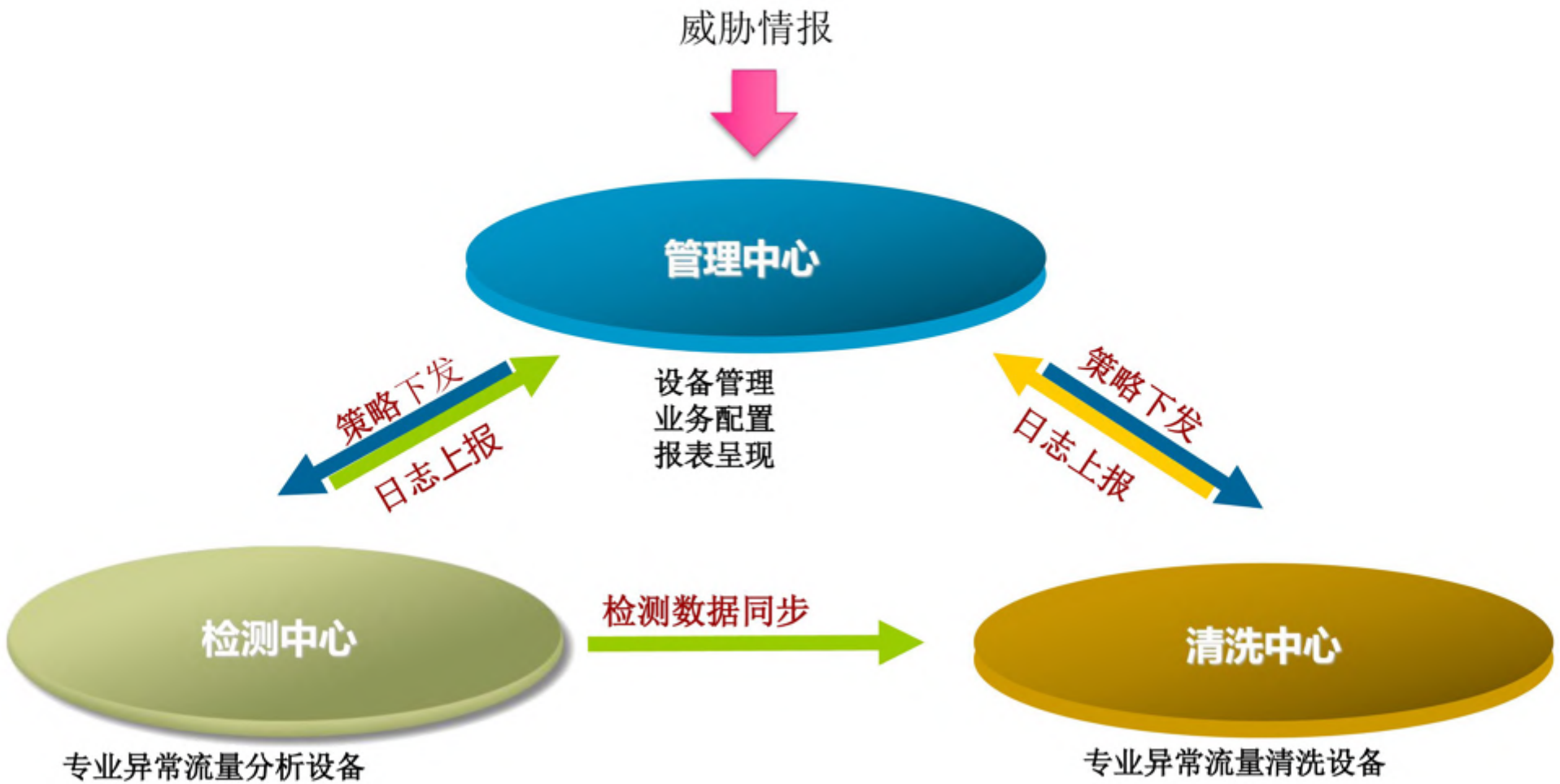
攻击要素：开放pingback服务的wordpress类网站
攻击危害： pingback脚本定义的URI决定服务器资源消耗程度
防御手段：地理过滤、行为分析

IDC面临的主要DDoS威胁

IDCC

攻击大类	攻击小类	攻击威胁
大流量DDoS攻击	SYN Flood	TCP会话
	UDP Flood, 包括UDP-based 反射放大攻击, 例如DNS反射放大攻击, NTP反射放大攻击	带宽
	ICMP Flood	带宽
HTTP 攻击	HTTP Get Flood	处理性能
	Slow Post Attack	HTTP会话
	Slow Header Attack	HTTP会话
	TCP重传	上行链路带宽
DNS攻击	DNS Query Flood(DNS Nxdomain floods)	处理性能

DDoS防御三要素：“云”－“查”－“杀”



Anit-DDoS防御架构要点

IDCC

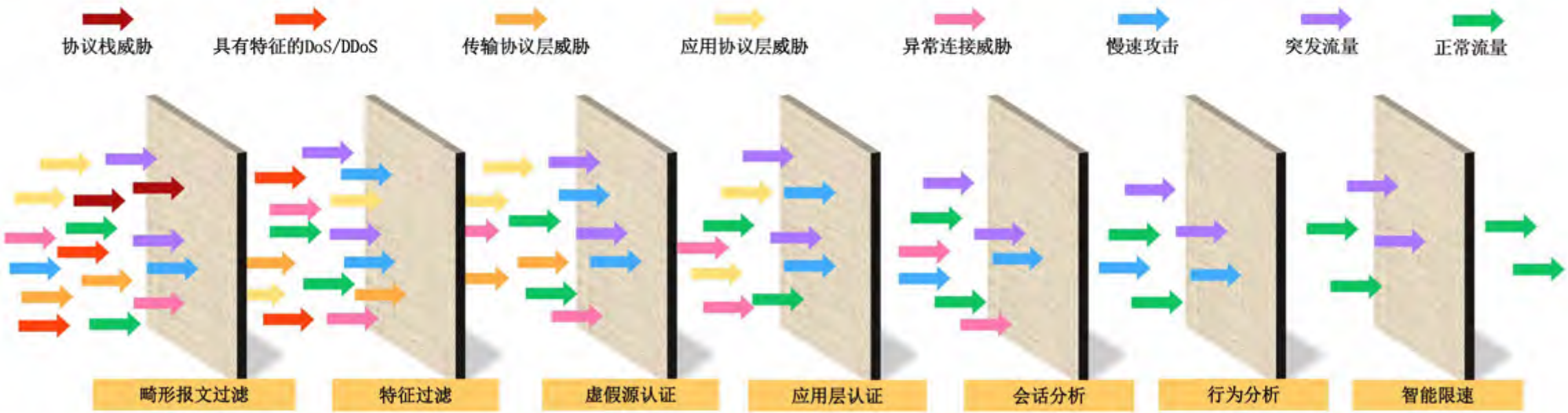
如何提升In-bound 应用层DDoS攻击防御能力，同时确保防御不影响正常业务访问？	核心技术
僵尸网络IP信誉、僵尸工具特征库提供全球数据收集、共享	智能云中心
DDoS僵尸网络发起的应用层攻击，如IMDDOS、YOyoDDoS、Darkness、BlackEnergy	源认证、IP信誉、地理过滤、指纹技术
自发僵尸网络攻击，如Anonymous号召发起的，利用LOIC、HOIC攻击的例子	僵尸工具特征库 地理过滤
慢速DDoS攻击，如Slowloris、Pyloris	IP信誉、地理过滤 会话监控+行为分析
加密应用DDoS攻击 移动应用DDoS攻击 新兴应用DDoS攻击	IP信誉 地理过滤 指纹技术 僵尸工具特征库

Anti-DDoS检测技术

IDCC

	逐流检测方案		逐包检测方案	
防护能力	大流量DDoS攻击 会话资源耗尽型DDoS攻击	☹	大流量DDoS攻击 会话资源耗尽型DDoS攻击 应用层DDoS攻击	☺
响应时间	分钟级（通常2~3分钟以上） (1. 路由器/交换机采样流量，汇总后发送; 2. Netflow流分析设备汇总Netflow流，判断是否有异常)	☹	2~3秒	☺
对现网路由器或交换机要求	需要现网交换机或路由器支持流采样及发送Netflow信息	☹	对现网路由器，交换机无特殊要求	☺
检测精度	无法检测出一些应用层慢攻击，如果用来给客户提供DDoS专业服务，可能导致投诉	☹	检测精确，能检测出各种类型攻击，包括大流量攻击和应用层慢攻击，可以用来给客户提供防DDoS增值服务	☺
每G流量成本	相对低 (基于流采样, 不是逐包加测,一般采样比1000:1, 大流量场景>200Gbps，较逐包方案成本低)	☺	相对高 (每个报文都要检测，大流量场景>200Gbps，成本较逐流检测方案高)	☹
检测性能扩展性	好 (不需要线性扩容 1. 部署Netflow流分析设备后，如果后续流量增长在Netflow流分析设备性能之内，不需要库容检测中心 2. 当现网流量超过已有的Netflow流分析设备性能后，需要扩容Netflow流分析设备)	☺	需要根据实际流量增长线性扩容 (逐包检测，现网流量增长，检测性能/接口数需要同步增长)	☹

清洗中心：层层过滤的手术刀式清洗机制



- 第一步，畸形报文过滤：过滤利用协议栈漏洞的畸形报文攻击、特殊控制报文过滤；
- 第二步，特征过滤：首先基于报文内容特征的静态匹配过滤，主要针对没有连接状态的攻击进行防范，如*UDP Flood*、*UDP*类反射放大攻击（包括*DNS*反射放大，*NTP*反射放大等），*ICMP Flood*；然后基于黑白名单静态过滤；
- 第三步，虚假源认证：用于防范虚假源发起的*SYN Flood*；
- 第四步，应用层源认证：用于防范虚假源或僵尸工具的*DNS Query Flood*、*DNS Reply Flood*、*HTTP get/post Flood*、*HTTPS Flood*、*SIP Flood*；
- 第五步，会话分析：基于会话检查可防范ACK Flood、*FIN/RST Flood*、*TCP*连接耗尽攻击、*TCP*异常会话攻击（socktress、重传攻击、空连接攻击）、*DNS Cache Poisoning*、*SSL-DoS/SSL-DDoS*、 *HTTP slow headers/post attack* ；
- 第六步，行为分析：僵尸网络发起的攻击流量和用户访问业务流量行为上存在很大差异，用户访问业务流量具有突发性，访问资源比较分散；而僵尸网络攻击因属于僵尸工具攻击，流量最大特征是访问频率恒定，访问资源固定。可基于行为分析防范CC攻击、TCP慢速攻击、真实源发起的TCP Flood。
- 第七步，智能限速：经过上述层层过滤后，如果流量还很大，超过服务器的实际带宽，则采用流量整形使到达服务器的流量处于服务器的安全带宽范围内，包括源限速和目的IP限速。

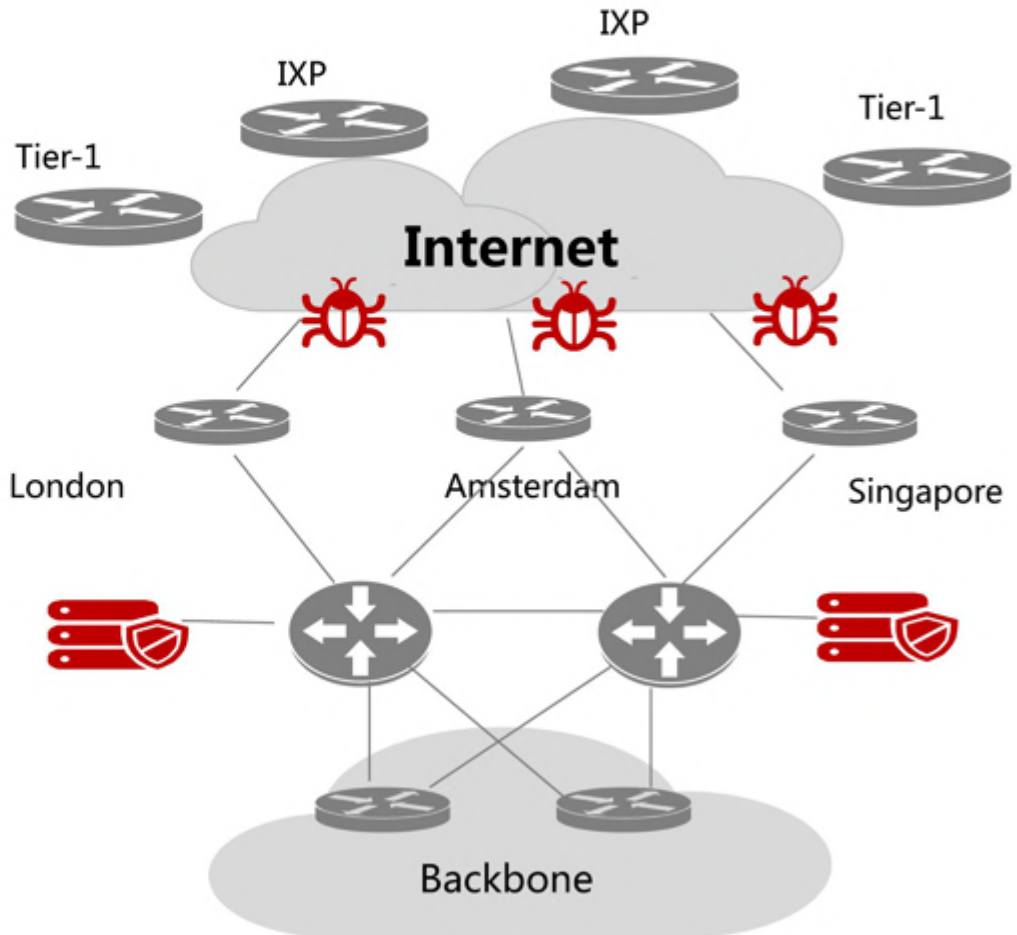
运营层面的考虑

IDCC

本地清洗方案无法解决上游管道拥塞

90%以上运营商在寻找云端的网流量清洁方案

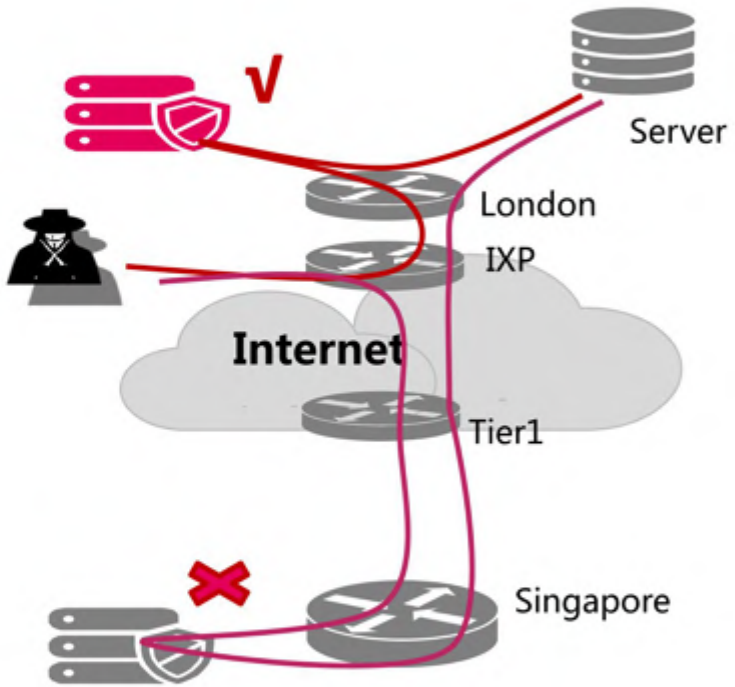
运营层面的考虑

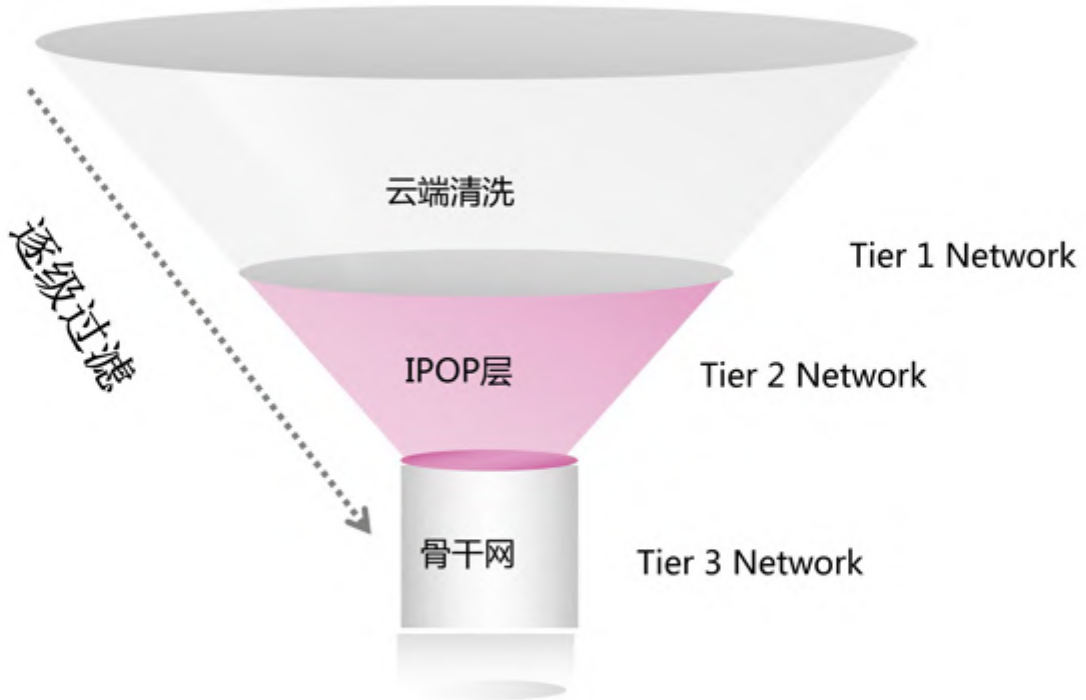


上游互联网到IPOP链路充斥攻击流量，
大量垃圾流量挤占昂贵的链路带宽

IGW部署的on-premise防御系统无法
保护IGW上行链路带宽

云清联盟的设计初衷



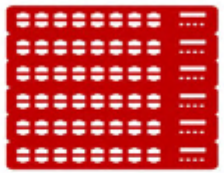


全球性大流量DDoS攻击，导致流经管道沿途受害，近源云清洗，才能真正确保链路可用性。

云清联盟的构成

IDCC

全球**TOP50**为主的运营商



数据中心服务提供商
全球性或者区域性

安全设备提供商）
领先的抗D能力

MSSP（安全服务提供商）
全球性或者区域性
7×24的应急响应专家团队

安全运营中心SOC平台
7×24的应急响应专家团队

云清联盟的核心组件

IDCC

云SOC(安全运营中心)

云SOC与盟员间的云信令通信，根据客户IPOP位置、SLA、商务成本等因素，提前建立好GRE隧道，选择有足够清洗资源的Scrubbing Center（清洗中心）清洗

清洗中心（Scrubbing Center）

全球化部署在互联网交换中心等位置，提供高性能清洗能力，通过Anycast快速引流并阻断攻击，回注清洁流量

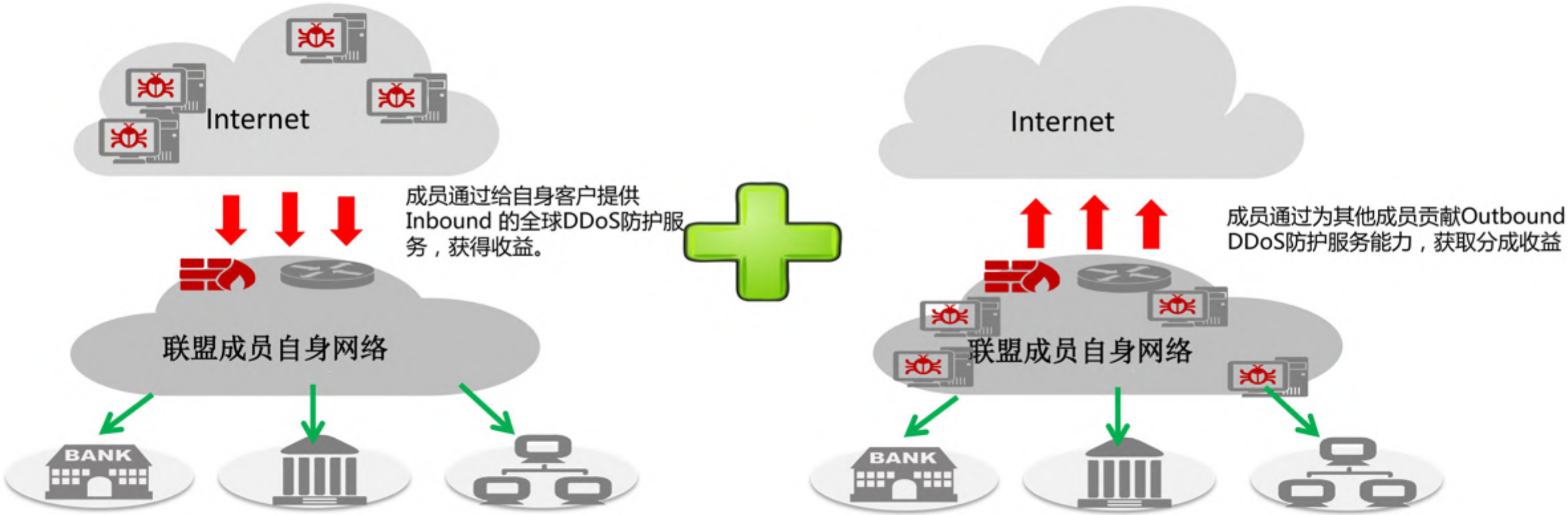
应急响应中心（Emergency Response Center ）

华为和云清联盟成员在全球各主要区域部署的7x24应急响应专家团队

云清联盟的全球布局

① 某成员通过本地on-premise DDoS系统清洗防御带宽范围内攻击过滤和应用型攻击，并及时发现大流量攻击；
② 在发现大流量攻击时发送云信令到云SOC；
③ 云SOC通知相应的云清洗联盟成员，启动近源防护。

运营方式：联盟成员利益分析



云清联盟规模构想

IDCC

全球4大洲，计划**10+**清洗中心

大数据**智能**调度，**近源**清洗

联盟成员所获得的价值

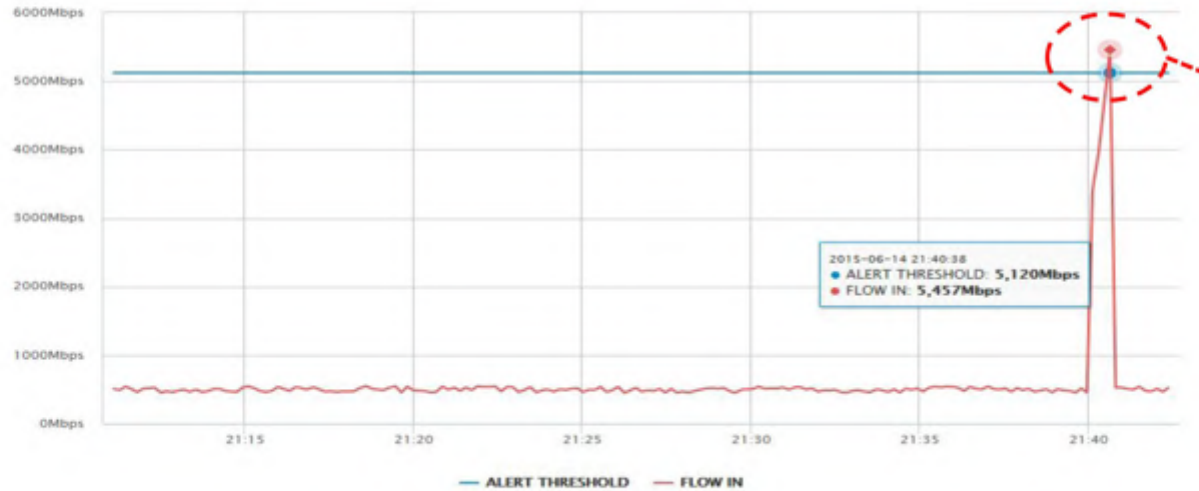
IDCC

- 短期价值：
  - 获得为自己的客户提供面向全球的DDoS云清洗服务能力
  - 通过为其他成员提供清洗服务获得收益
  - 提升自己在全球DDoS防护领域的品牌价值和影响力
- 长期价值：
  - 及时获得全球DDoS攻击态势的网络攻击数据和趋势分析
  - 联盟成员借助大平台将自身安全服务能力推向更多最终客户
  - 联盟成员安全服务能力的持续提升

云清洗工作流程-1

第一步：在云清洗管理平台为客户选择清洗服务提供商

云清洗工作流程-2



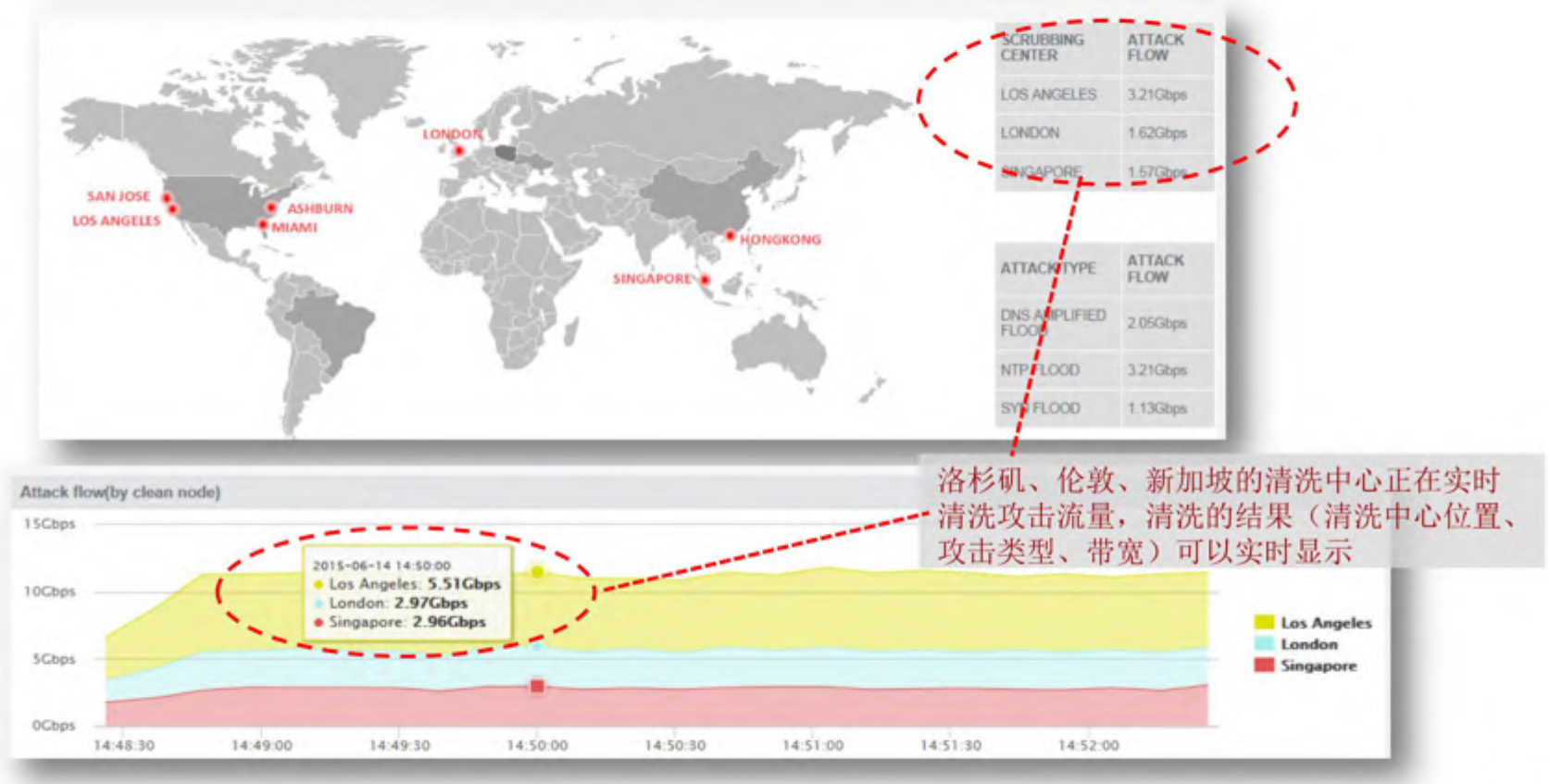
入网流量达到5.457Gbps，超过配置的阈值5Gbps，判断已发生大流量DDoS攻击.

华为云清洗管理平台上报攻击事件

Event ID	Start time	Customer	IP/Mask	Alert threshold	Country	Attack type	Action
42	2015/6/14 21:40:38	demouser	207.192.151.0/24	5G	ALL	SYN FLOOD, DNS AMPLIFIED FLOOD, NTP FLOOD	CLEAN

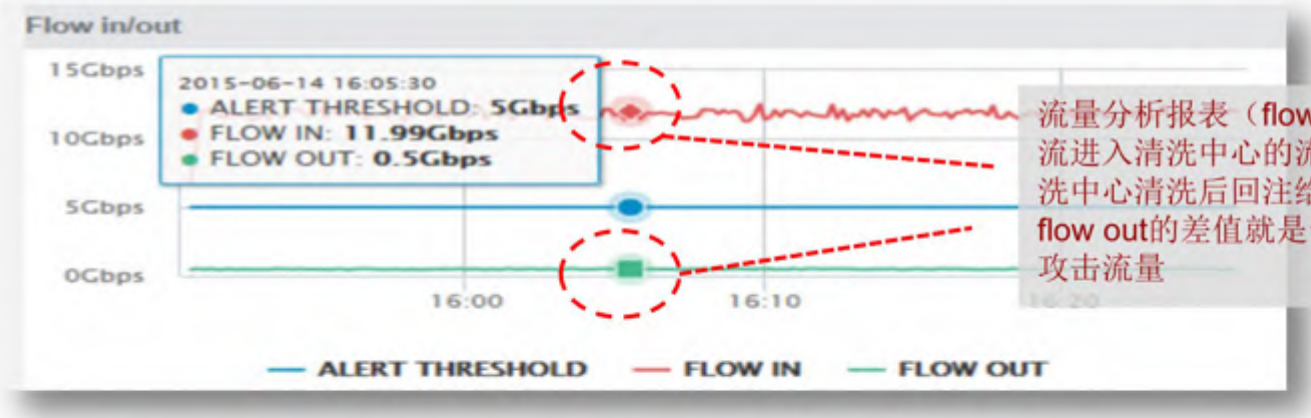
第二步：客户本地检测设备检测到超大流量DDoS攻击（超过阈值）

云清洗工作流程-3

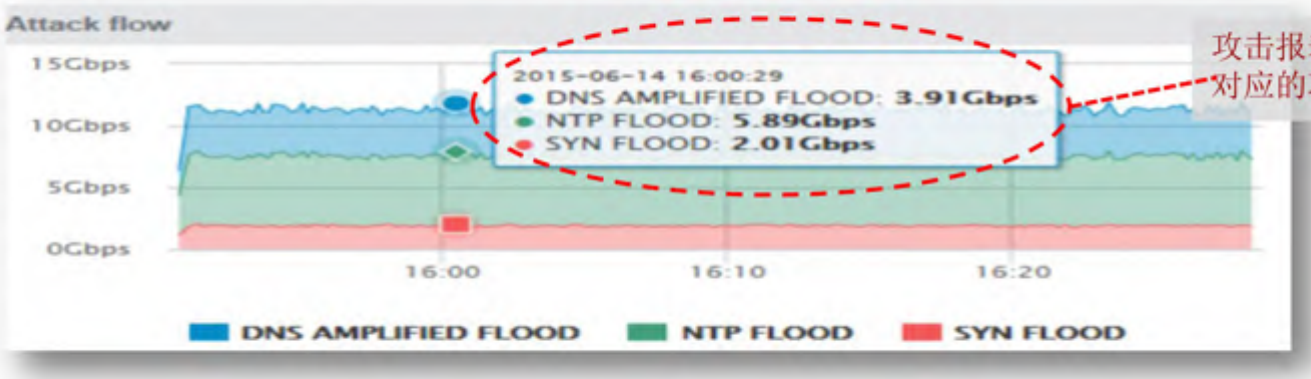


第三步：云清洗管理平台调度全球云清洗中心针对该用户的攻击流量启动云清洗

云清洗工作流程-4



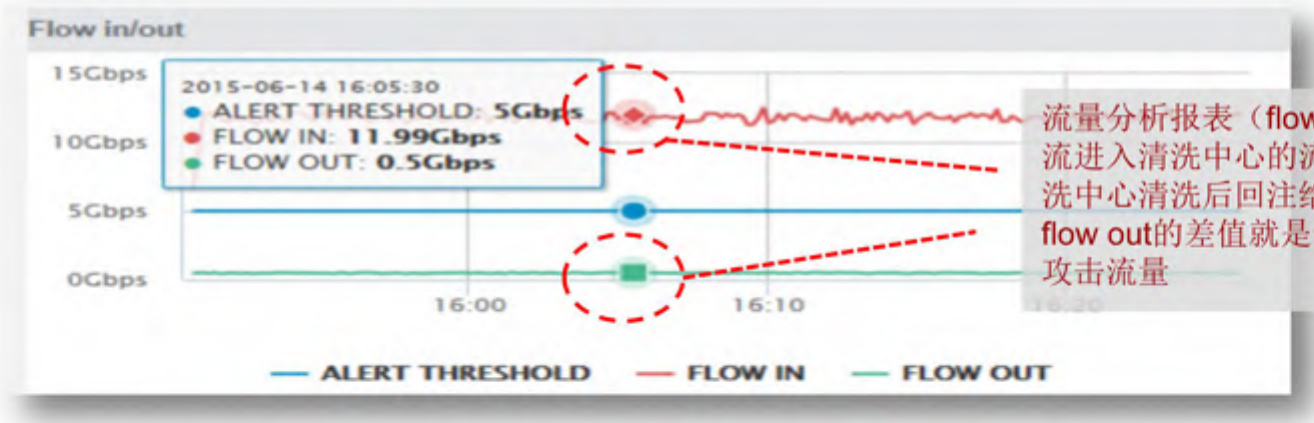
流量分析报表（flow in/out）：Flow in代表引流进入清洗中心的流量，flow out代表经过清洗中心清洗后回注给客户网络的流量，flow in-flow out的差值就是云清洗中心清洗掉的DDoS攻击流量



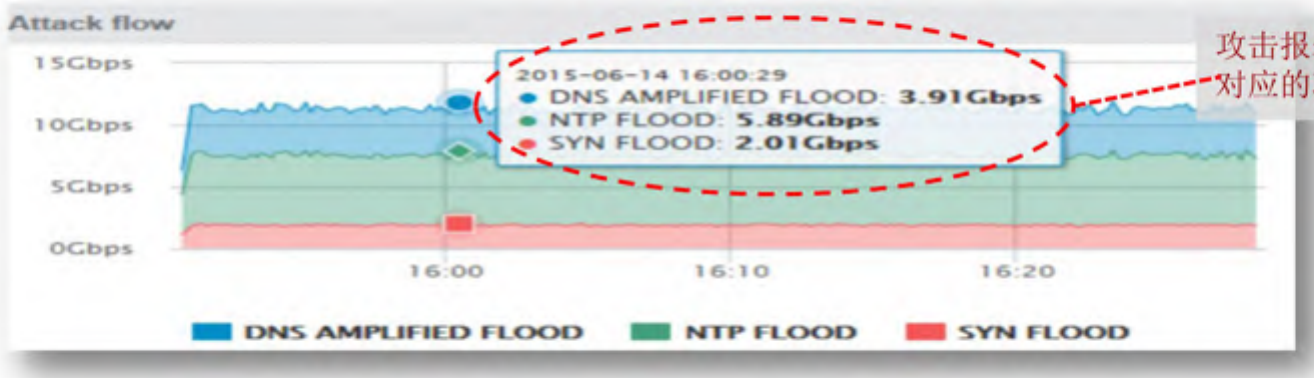
攻击报表：实时呈现攻击类型及对应的攻击带宽

第四步：云清洗管理平台查看攻击报表

云清洗工作流程-5



流量分析报表（flow in/out）：Flow in代表引流进入清洗中心的流量，flow out代表经过清洗中心清洗后回注给客户网络的流量，flow in-flow out的差值就是云清洗中心清洗掉的DDoS攻击流量



攻击报表：实时呈现攻击类型及对应的攻击带宽

第四步：云清洗管理平台查看攻击报表

客户化Portal，所见即所得

IDCC

用户对安全现状了如指掌

实时攻击数据在线呈现

- 实时反馈用户防御数据
- 请求响应情况
- 攻击详细数据

Thank you!