NSFOCUS

绿盟网站云清洗（云DDoS）服务

绿盟云 NSFOCUS CLOUD | cloud.nsfocus.com

ANONYMOUS，DDoS全球代言人

史上最大规模DDoS攻击（2014）

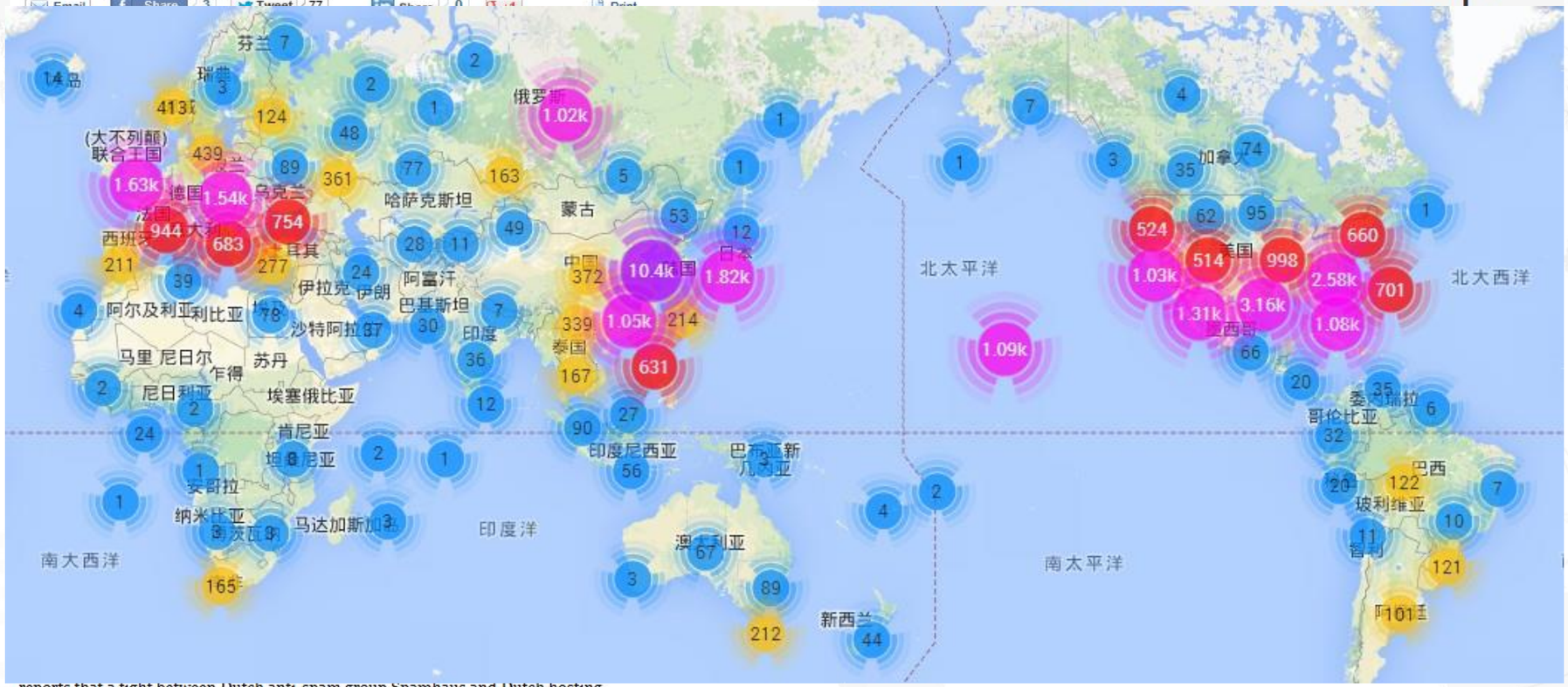
Spat between two Dutch companies sparks record-breaking 300Gbps DDoS attack

By Brad Reed | BGR News – Wed, Mar 27, 2013

reports that a fight between Dutch anti-spam group Spamhaus and Dutch hosting company Cyberbunker has resulted in the world's largest recorded distributed denial-of-service (DDoS) attack, which peaked at speeds of 300Gbps this week. The spat between the firms started when Spamhaus added Cyberbunker to its blacklist, which is designed to help email providers block alleged spammers. Shortly after Spamhaus blacklisted Cyberbunker, which says it on its website that it will host any data not related to child pornography or terrorism, the anti-spam group was hit by an enormous DDoS attack that is described by Akamai Networks chief architect Patrick Gilmore as "the largest publicly announced DDoS attack in the history of the Internet."

CLOUDFLARE

Technical Details Behind a 400Gbps



——放大倍数10倍以上的NTP服务器的分布

DDoS攻击就在我们身边

那段时间，我们哪儿也去不了

“乌云”“果壳”等公益网站

NSFOCUS

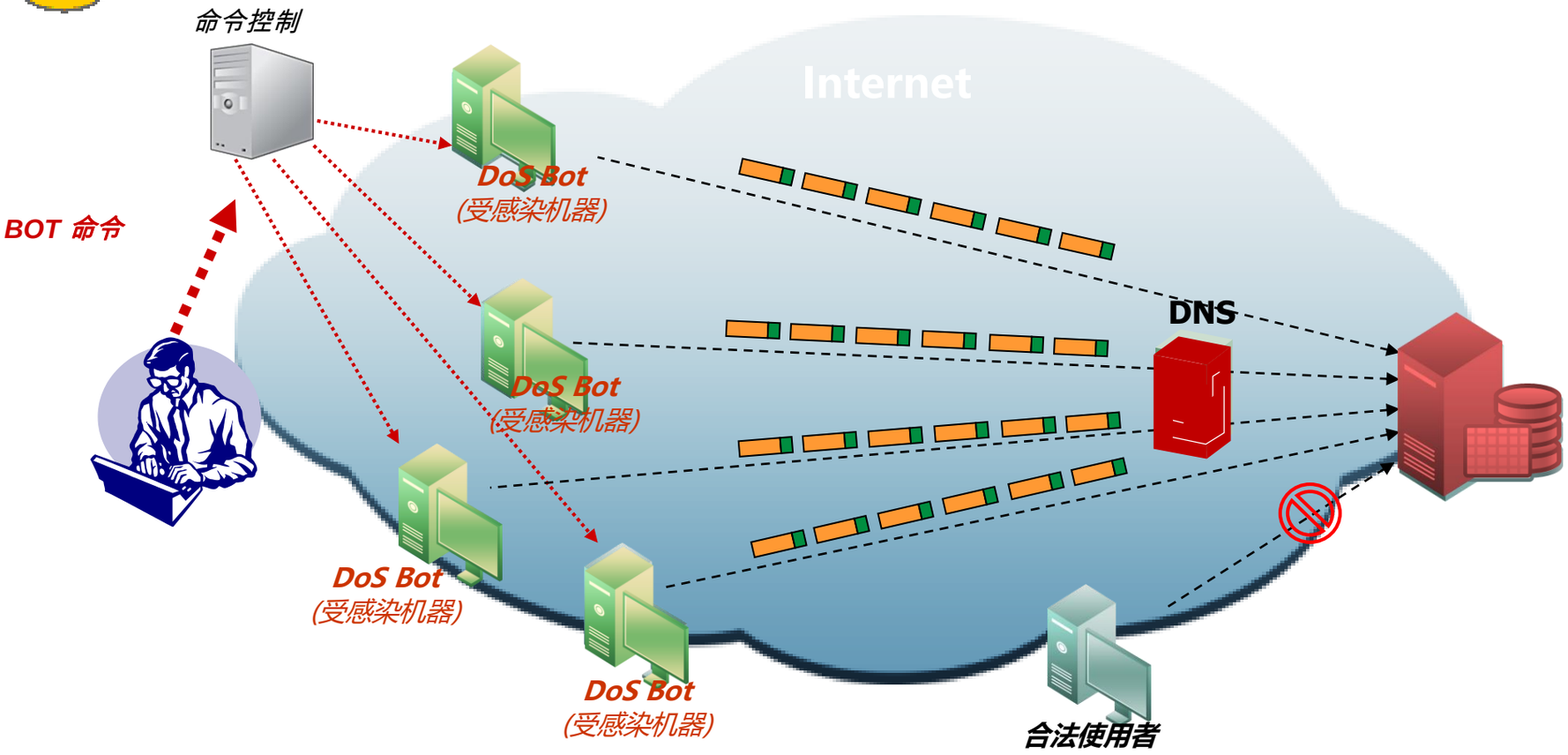
DoS

Denial of Service，拒绝服务。属于攻击早期形态，由于攻击者**带宽**、**CPU**等资源不足，较难形成威胁，如果是目标有明显漏洞，不需要僵尸网络，攻击成本较低

DDoS

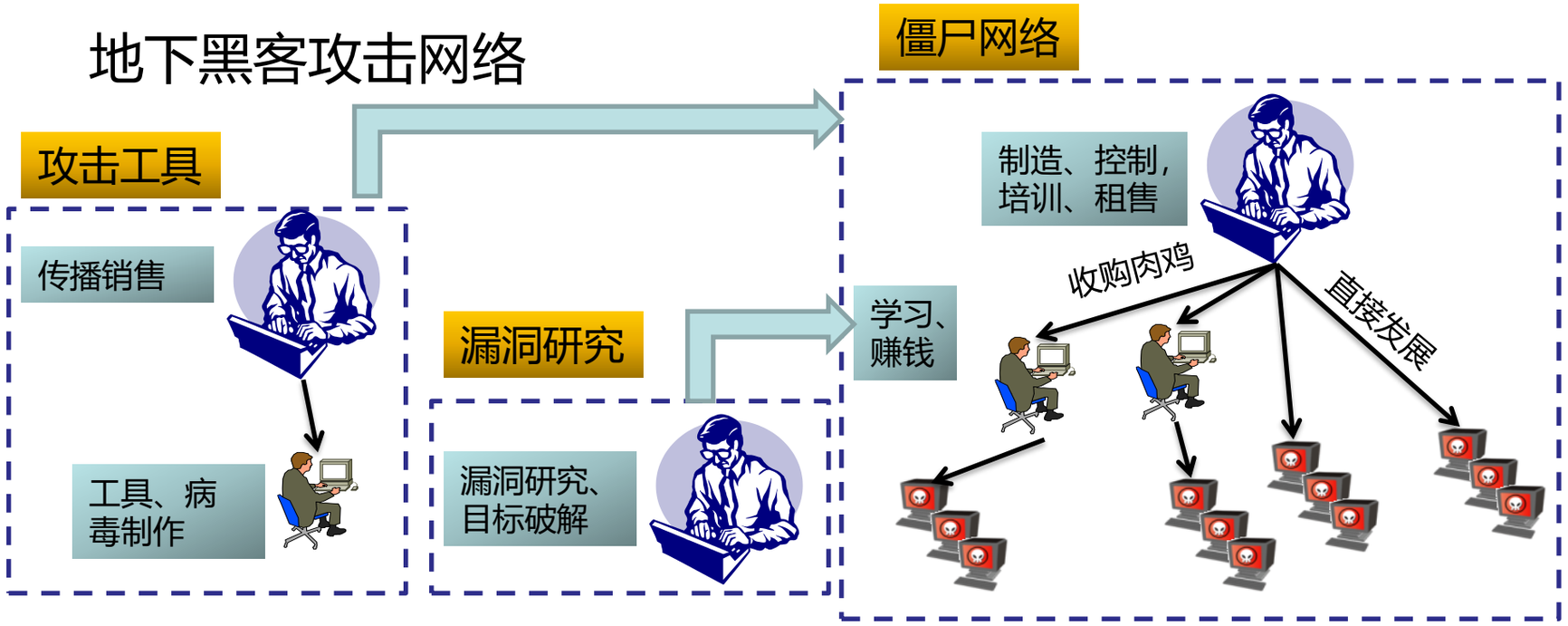
Distributed Denial of Service，**分布式**拒绝服务。当前主流攻击手段，主要消耗网络带宽、消耗主机资源、利用漏洞发起攻击

DDoS攻击过程



阻塞沿途带宽 **攻击基础网络设施** **瘫痪最终服务器**

DDoS攻击地下产业化



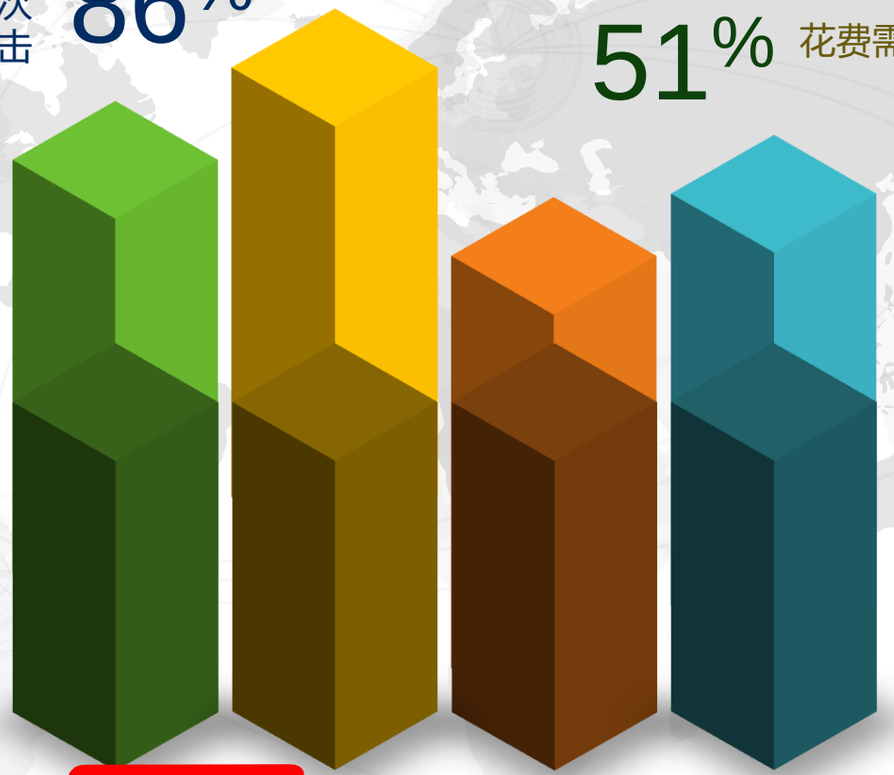
企业遭受DDoS持续威胁

其中86%的企业表示在2017年遭受不止一次DDoS攻击 **86%**

51% 花费需要3个小时以上发现被攻击

84%的企业在2017年遭受过DDoS攻击 **84%**

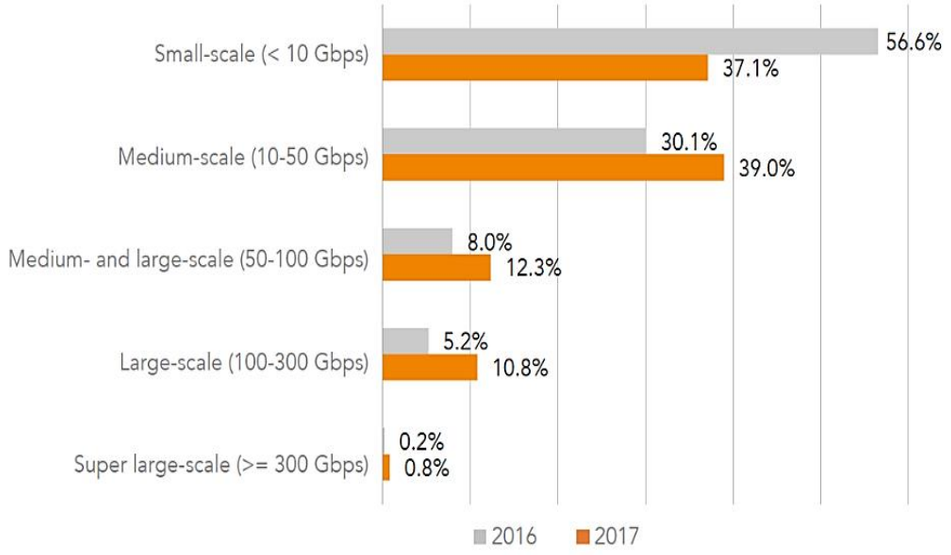
77%
由第三方发现



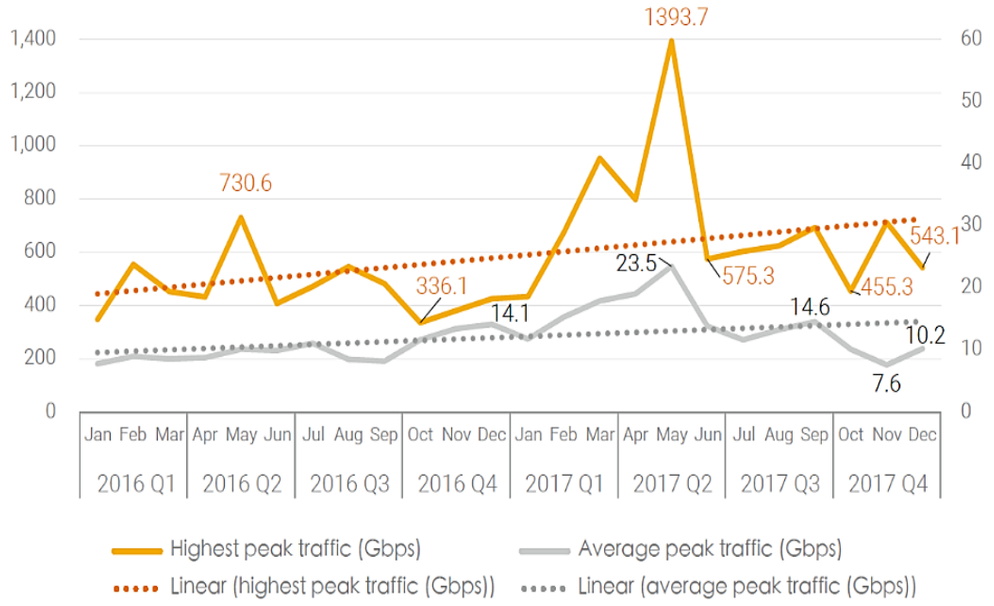
44% 平均攻击峰值造成盈利损失 $

DDoS攻击规模与日俱增

Proportions of DDoS attacks of various scales in 2017 and 2016



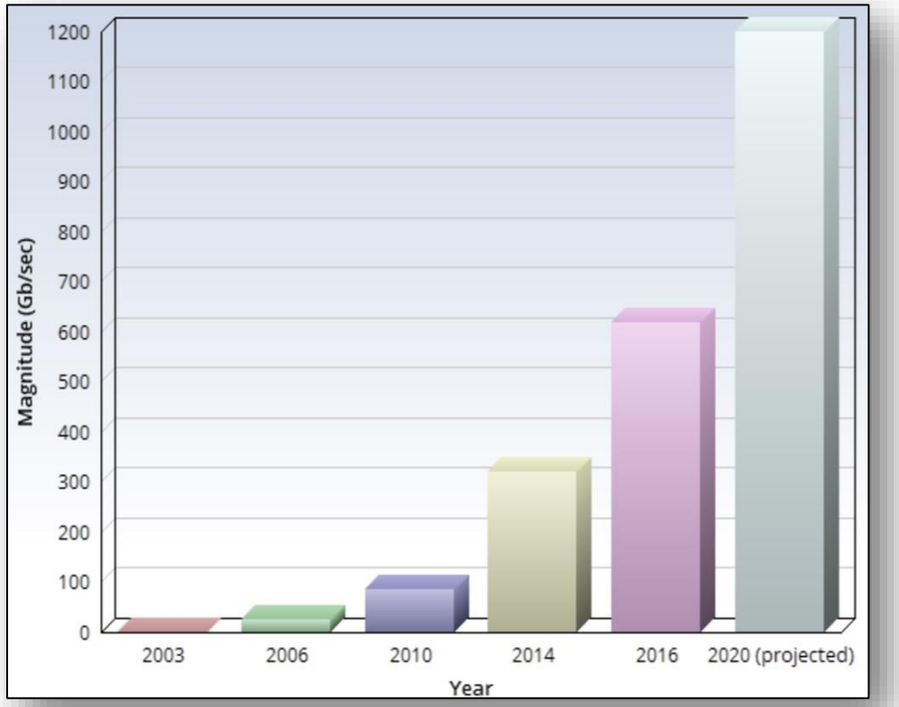
Monthly single-attack traffic peak and average attack peak (Gbps)



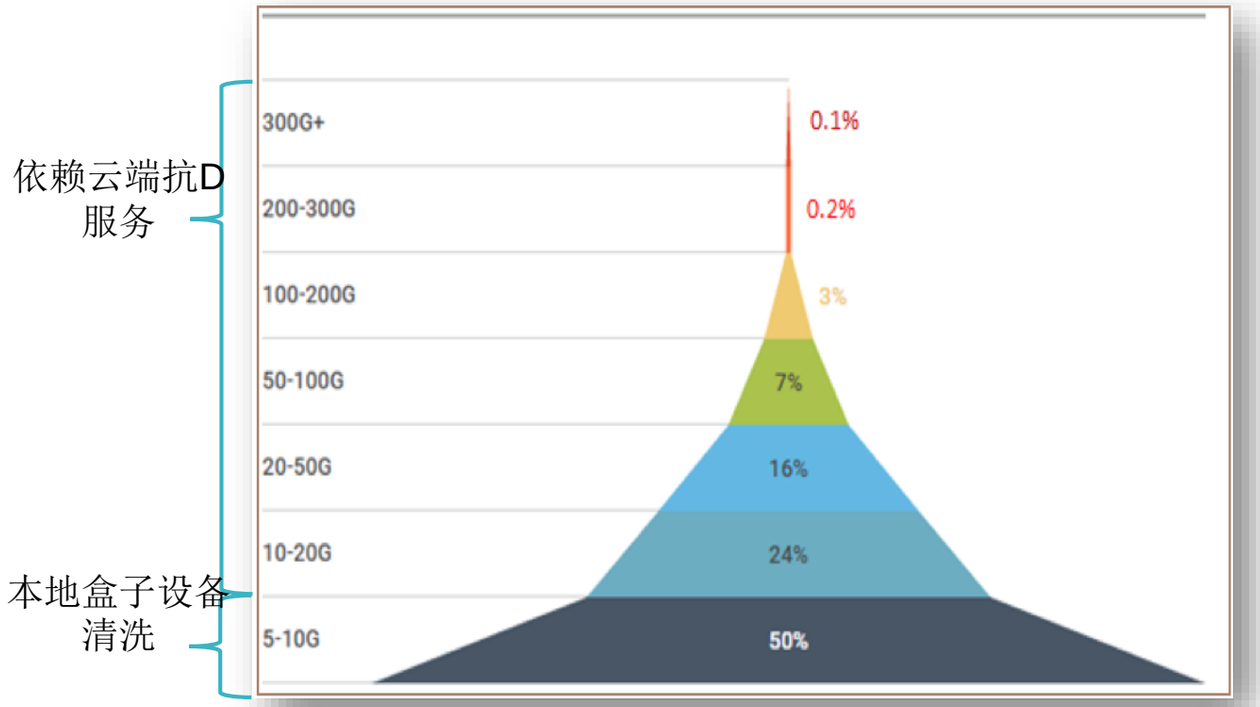
*NSFOCUS 2017 DDOS AND WEB APPLICATION ATTACK LANDSCAPE

为什么选择云抗D?

攻击规模超过本地清洗能力



- 攻击规模越来越大



- 几乎一半以上额攻击都超过了10Gbps

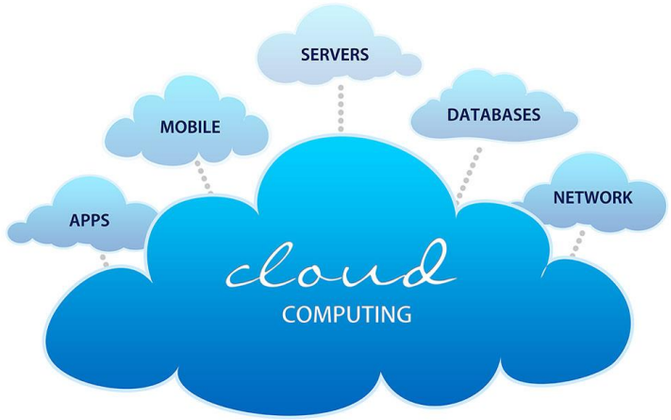
本地清洗能力已无法应对日渐增长的攻击规模！

NSFOCUS

为什么选择云抗D?

基于云计算的安全服务

- 能力:
  - 无需购买硬件、软件，云服务触手可及
  - 用多少，买多少
  - 按需弹性扩容
- 特征:
  - 按需清洗
  - 灵活的业务接入方式
  - 资源池共享
  - 快捷
  - 灵活计费

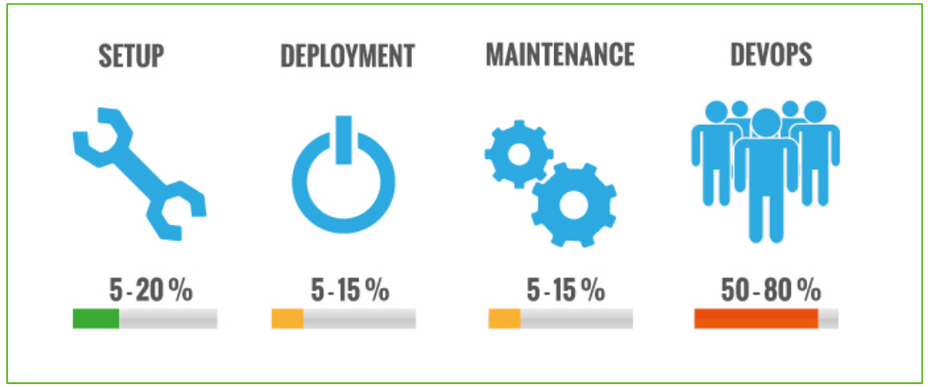


NSFOCUS

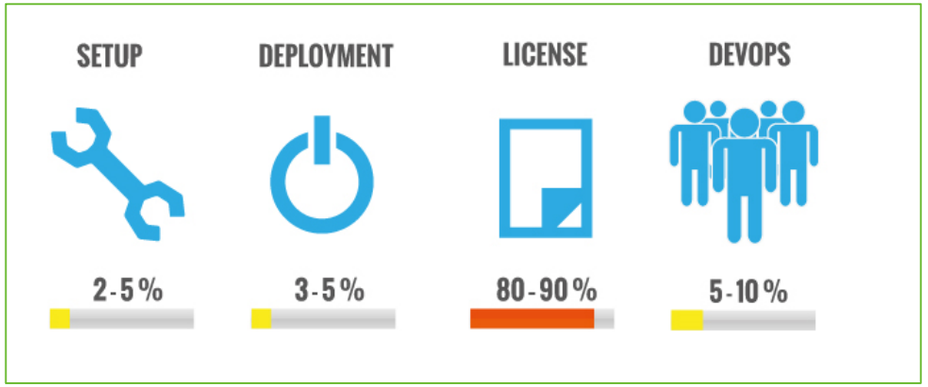
为什么选择云抗D?

本地清洗和云端清洗的开销对比

本地



云



- 云服务需要更少的资本投入，投入更贴合实际需求，开发和运营成本极低。

Source: *http://insights.wired.com/profiles/blogs/the-total-cost-of-ownership-in-house-vs-cloud-based-development#axzz4F8BVelpc*

NSFOCUS

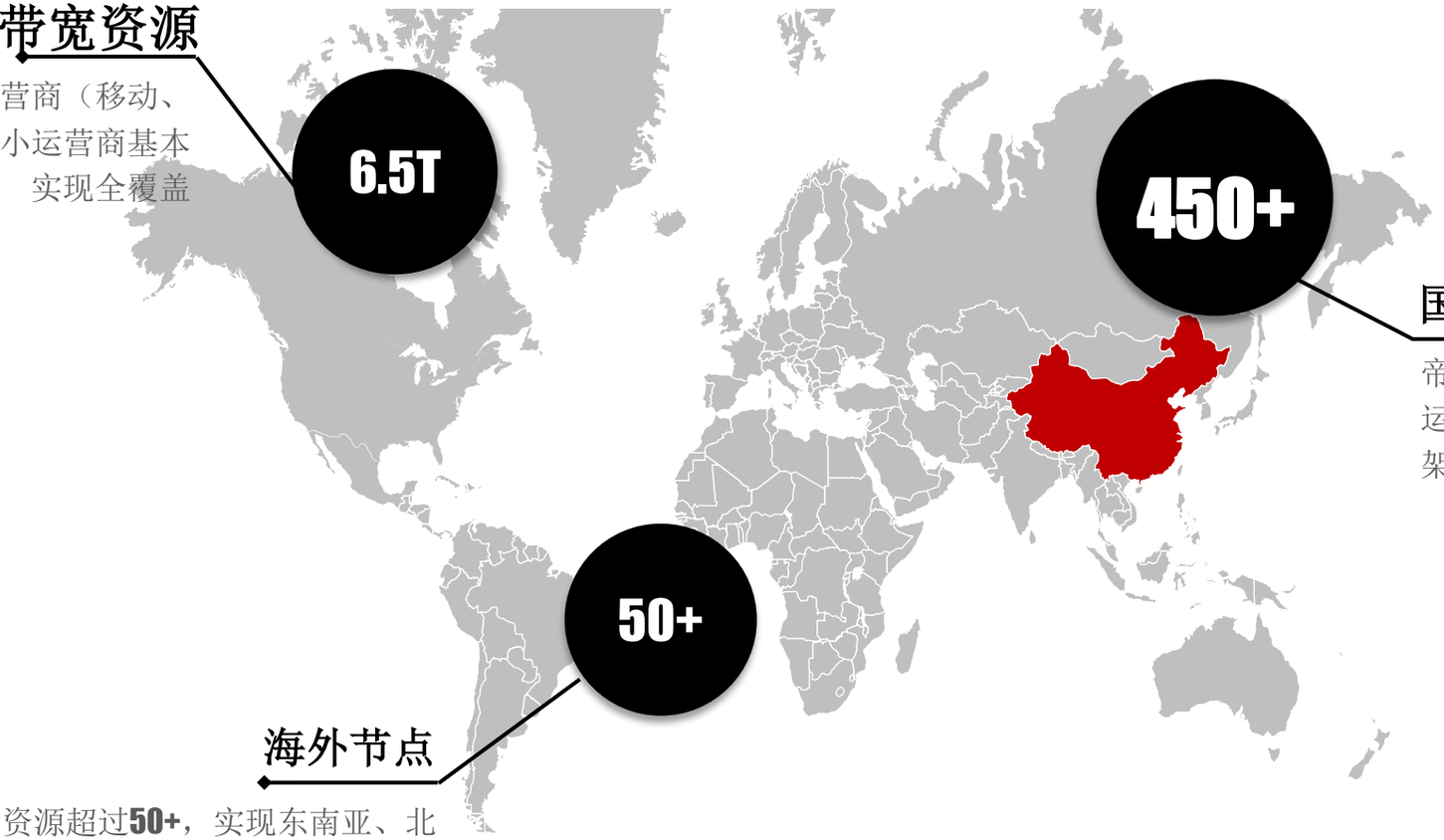
什么是绿盟云清洗

- 绿盟云清洗是绿盟采用业界领先的ADS防护产品，结合帝网丰富的CDN网络带宽资源构建的云端的DDoS防护服务。绿盟云清洗服务可以为公有云客户、CDN客户及传统web应用客户，提供从网络层到应用层的DDoS攻击防护。

CDN_节点与带宽资源

带宽资源

运营带宽达到**6.5T+**，三大运营商（移动、联通、电信）资源丰富，中小运营商基本实现全覆盖



国内节点

帝网科技国内节点数达到450+，实现了多运营商线路、跨区域的分布式、三级部署架构

海外节点

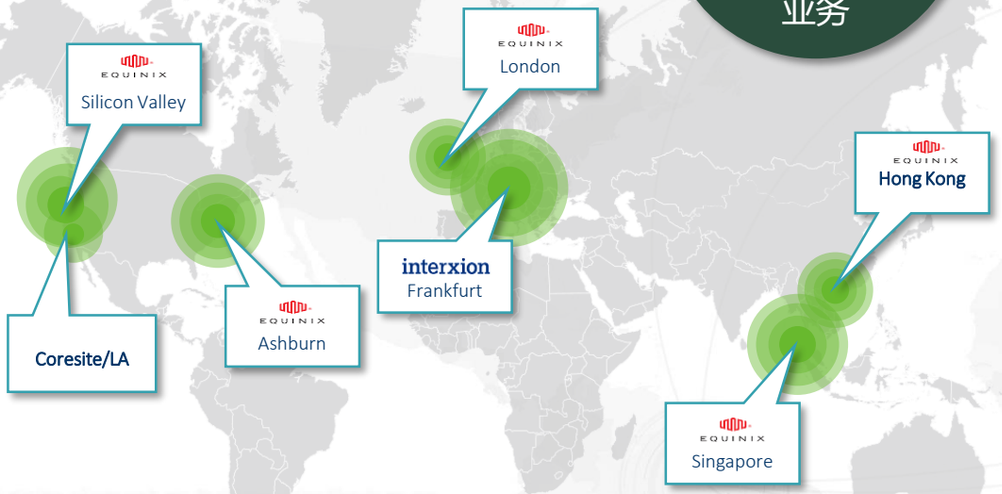
海外节点资源超过**50+**，实现东南亚、北美、欧洲等热点区域的全面覆盖，通过专线与国内直连，有效保障内容分发质量

NSFOCUS

绿盟云清洗中心

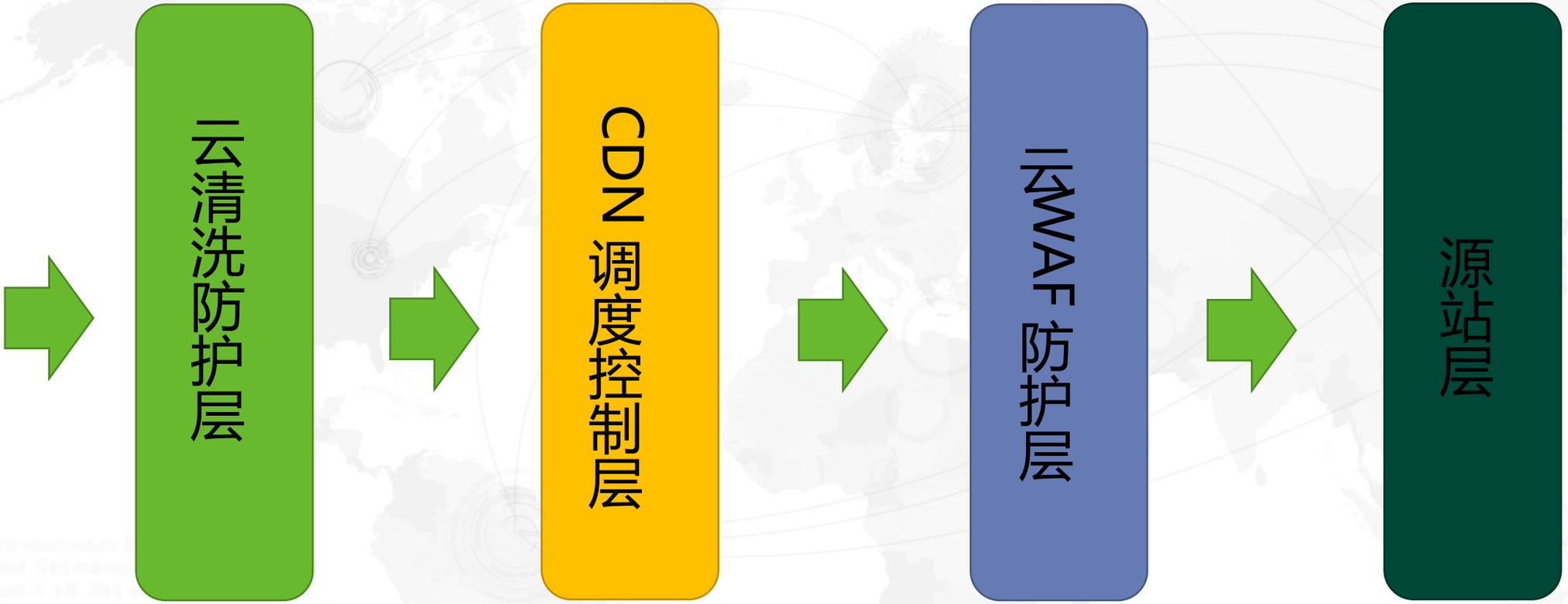
7
全球布局，
Tier1 运行商
承托Internet
业务

5
国内多线路
Tier1 运行商



- 世界各地均可轻松接入
- 清洗中心全球布局，保障延迟优化
- 国内多节点，多线路
- 国际1.5T，国内300G清洗能力

CDN安全业务体系架构

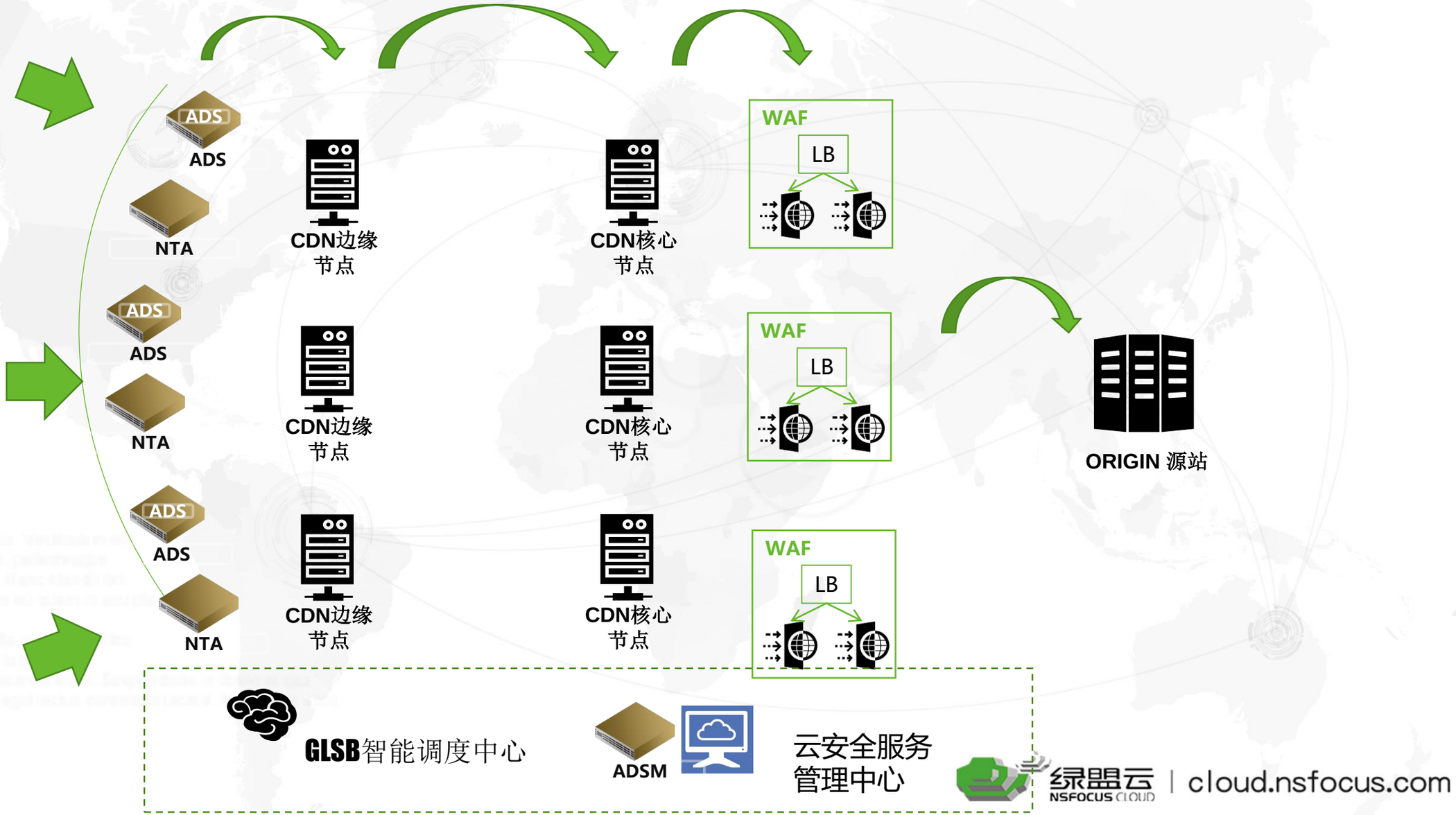


DDoS攻击防护

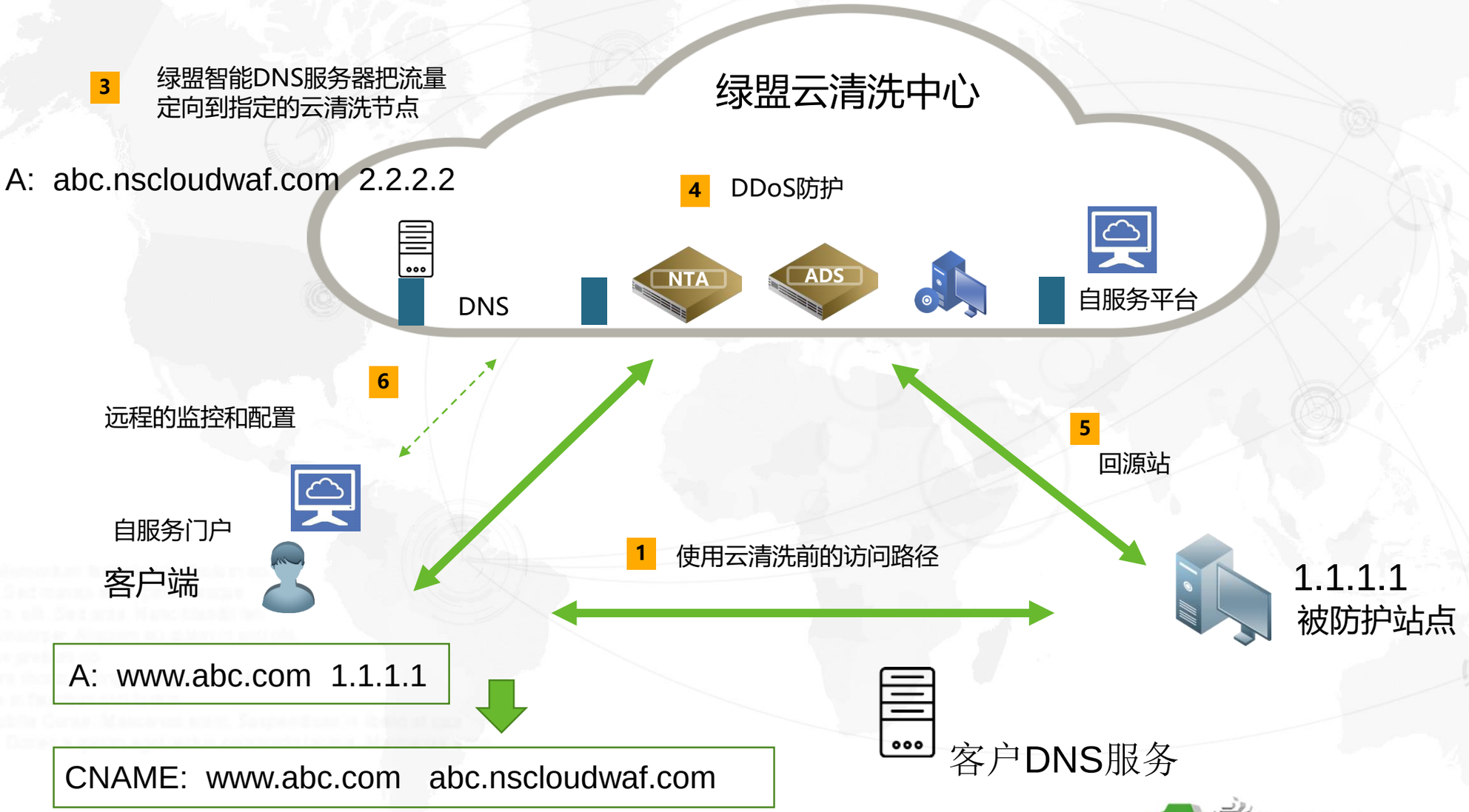
CDN流量调度

WEB应用防护

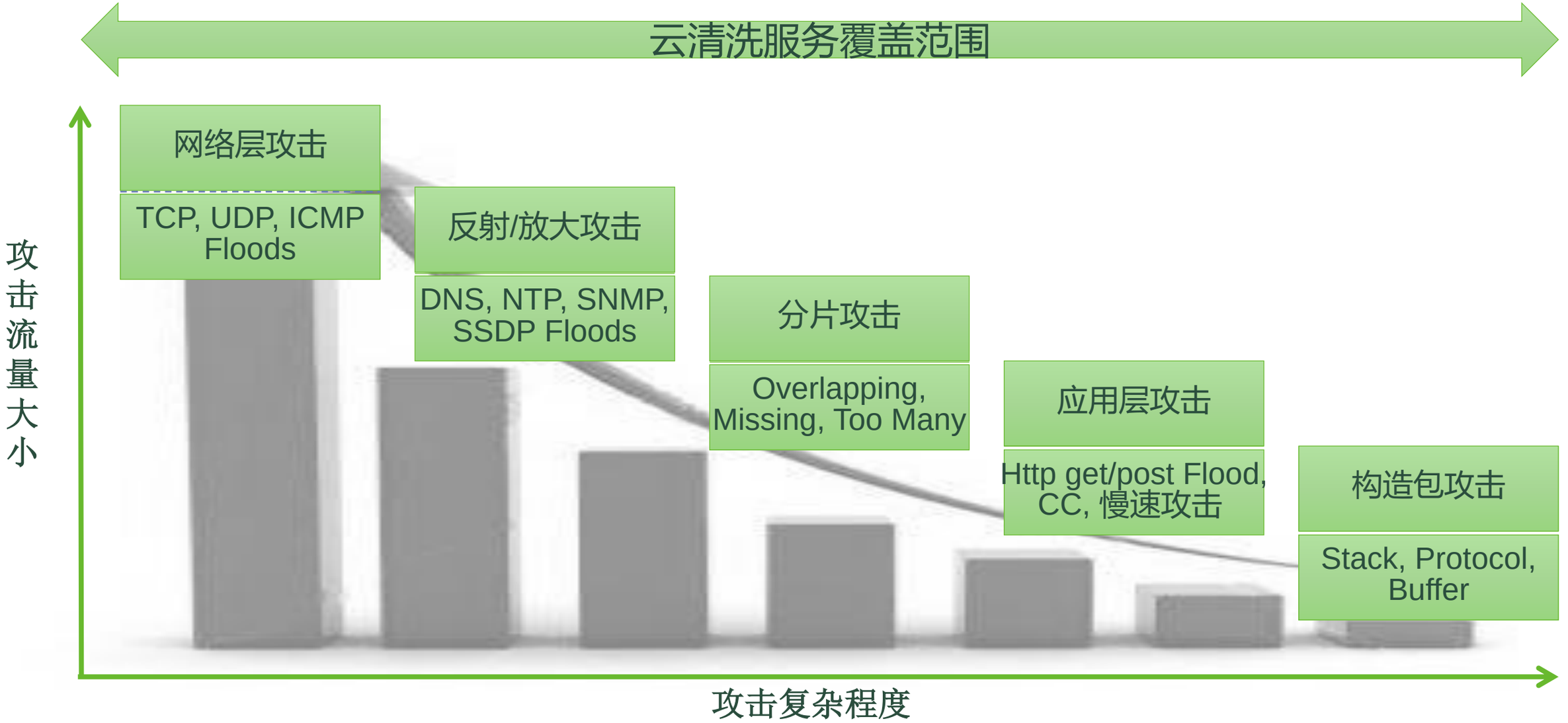
CDN安全业务部署架构



绿盟云清洗工作流

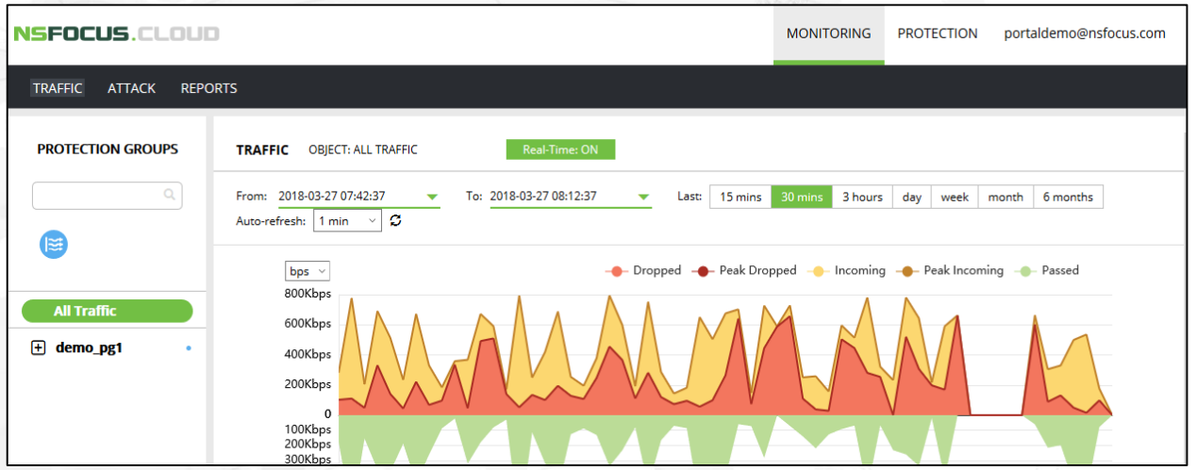

3
绿盟智能DNS服务器把流量
定向到指定的云清洗节点
绿盟云清洗中心
A: abc.nscloudwaf.com 2.2.2.2
4
DDoS防护
DNS
NTA
ADS
自服务平台
6
远程的监控和配置
5
回源站
自服务门户
客户端
1
使用云清洗前的访问路径
1.1.1.1
被防护站点
A: www.abc.com 1.1.1.1
CNAME: www.abc.com abc.nscloudwaf.com
客户DNS服务
2
改变DNS记录

云清洗服务防护规格


云清洗服务覆盖范围
网络层攻击
TCP, UDP, ICMP Floods
反射/放大攻击
DNS, NTP, SNMP, SSDP Floods
分片攻击
Overlapping, Missing, Too Many
应用层攻击
Http get/post Flood, CC, 慢速攻击
构造包攻击
Stack, Protocol, Buffer
攻击流量大小
攻击复杂程度

绿盟云清洗监控门户

- 助力客户运维监控和策略调整，满足多租户的安全能力销售业务需求
- 原始数据由绿盟云清洗中心的ADSM设备获取，及时、精准；
- 账号分层分级：用户账号，工程运维账号



优势

- 多租户
- 多重安全机制
- 客户自行控制清洗策略
- 实时监控及报表
- 溯源报告
- 支持白牌

产品亮点

24 x 7

全时服务，快速响应
24*7不间断支持

精准防护

方案核心由绿盟旗舰抗D设备保障，准确敏捷定位恶意流量，覆盖全协议层攻击

简洁易用

专属云清洗门户网站，清洗情况，丰富报表，流量分析唾手可得

云地合一

云清洗方案与绿盟本地ADS设备有机结合，无缝保障客户网络

云业务联动

与我们的数据中心伙伴合作，联动您在Amazon，Ali， Azure上的云业务

NSFOCUS

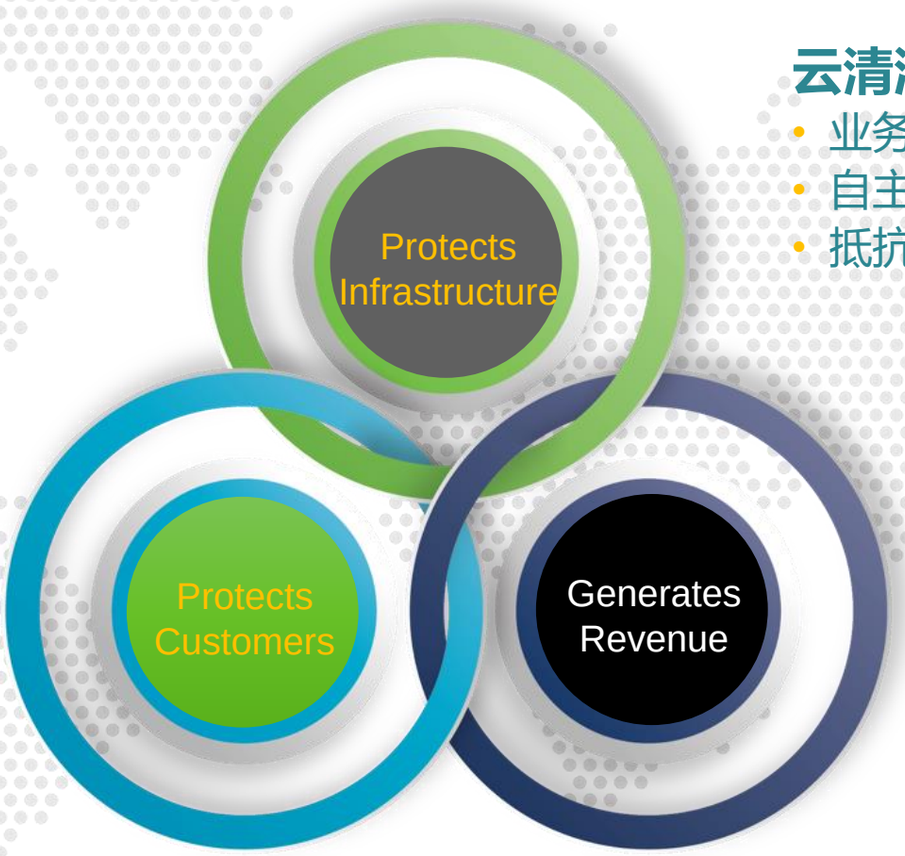
云清洗产品竞争分析

	绿盟云清洗服务	国内主要云清洗服务提供商
云清洗厂家	绿盟云清洗	阿里云盾、电信云堤、腾讯云，Ucloud，知道创宇，360，金山云，京东云等
最大防护容量	一期国内建设300G，国际1.5T，基础网络拥有6.5T规模	360、金山、京东、知道创宇、Ucloud 1-2T的防护；腾讯、电信、阿里 >5T的防护
流量牵引方式	BGP（海外）DNS（国内）	DNS，从牵引方式上讲，国内基本使用的是DNS的方式，各厂家的差异不大。
攻防能力	ADS+NTA产品是业内领先的专门的DDoS防护产品，有近20年的研发历史，众多国内外电信级的客户，从网络到应用层的防护，丰富的防护算法	基本上是采用第三方DDoS防护产品+自研方式，对防护产品不熟悉，自研产品缺少商用的检验，检测和防护的精准性不高。
运维值守	有多年经验的DDoS攻防专家团队	缺乏对DDoS安全攻防的运维团队
价格体系	价格定义为市场中等价格，防护效果好，但进入云清洗市场晚。	云堤和阿里价格偏高，也是我们主要的竞争对手。其他厂家价格和绿盟持平，有些小厂家价格低。
方案体系	云清洗+云WAF+CDN 云清洗+本地清洗	其他厂家只能提供部分的整体方案。
用户Portal	每用户可监控攻击事件、可调整攻防参数	没有或展示、配置攻击界面不全

WEB业务安全服务组合模式

	CDN	云清洗	云WAF	客户类型及客户需求
1	✓			CDN的用户，主要是提供网站加速功能，没有任何的安全防护措施。是需要转化的存量客户。
2	✓	✓		CDN的用户，有对DDoS防护的需求，如SYN Flood， UDP Flood，ACK Flood等，客户如游戏类网站，希望提供专业的DDoS高防
3	✓		✓	CDN的用户，有对WEB网站的防护需求，如Injection, XSS, CSRF, 暴力破解, Web Shell, 爬虫攻击，扫描攻击。客户为互联网、政府、企业的门户网站。
4	✓	✓	✓	CDN的用户，对DDoS攻击和WEB应用层面的攻击都比较重视，希望有全面的防护。客户如互联网金融，电子商务网站。
5		✓		非CDN的用户，只是要单向防护DDoS攻击，如为了防护竞争对手中的恶意攻击。
6			✓	非CDN的用户，对CDN的加速没有强烈的要求，但对网站的安全有诉求。如政府、教育系统的网站。
7		✓	✓	非CDN的用户，有比较严格的合规性的要求，而自己却没有能力购买和运维安全产品，希望购买DDoS和WAF类的安全服务。如政府、中小企业、初创公司等。

绿盟抗D解决方案体系



本地清洗 On-Premises Defenses

- 灵活，**turn-key**方案
- 快速响应，客户自控
- 网络层及应用层防护

云清洗 Cloud Defenses

- 业务提供商模式
- 自主清洗中心，全球布局
- 抵抗超大量级**DDoS**攻击

云地联动 Hybrid Defenses

- 联动方案
- 客户业务+互联网出口
- 最快响应

NSFOCUS

客户列表

MetTel

ISP
NAMR

HOST EUROPE
GoDaddy

Hosting
EMEA
Germany

maxihost

Hosting
LATAM Brazil

G·CORE LABS

Gaming Hosting
EMEA
Luxembourg

multiplay

Hosting
EMEA

Voip Unlimited

VoIP
EMEA

UCLOUD

Cloud Provider
APAC

Always On.
opus:interactive

Server
Choice

ALOO TELECOM

DDoS防护产品资质与荣誉

CDN及电信增值业务运营牌照

中华人民共和国
增值电信业务经营许可证

经营许可证编号：B1-20100055

根据《中华人民共和国电信条例》及国家有关规定，经审查，准许你公司按照本经营许可证（正文和附件）载明的内容经营增值电信业务，特颁发跨地区增值电信业务经营许可证。

公 司 名 称：上海帝联信息科技股份有限公司

法 定 代 表 人：康凯

注 册 资 本：人民 元

注 册 住 所：上海市普陀区中江路 879 弄 21 号楼 1 楼 101 室

业 务 种 类：（见附页）

业务覆盖范围：（见附页）
（服务项目）

签 发 人：

发 证 日 期：二〇一七 年 三 月十五日

有 效 期 至：二〇二一 年 九 月二十日

CDN运营牌照

2016年3月1日，《电信业务分类目录（2015年版）》正式实施，目录规定CDN运营资质

2017年1月22日，工信部发布了关于清理规范互联网网络接入服务市场的通知，
通知要求未按照承诺如期取得相应业务经营许可证的企业，从2018年1月1日起不得经营

2017年3月15日，帝联科技正式首批获颁CDN运营牌照

编号：B1-20100055

中国CDN行业TOP3

中国互联网企业TOP100

NSFOCUS

谢谢！

01

客户支持

电话咨询

010-68438880 转 5675

客服邮箱

help@nsfocus.com

02

市场合作

电话咨询

010-68438880 转 5068

联系邮箱

nscloud@nsfocus.com

绿盟云 NSFOCUS CLOUD | cloud.nsfocus.com