
ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
企业云安全实践论坛

如何解决海量 DDoS 攻击的问题

网宿科技　　欧怀谷

目录

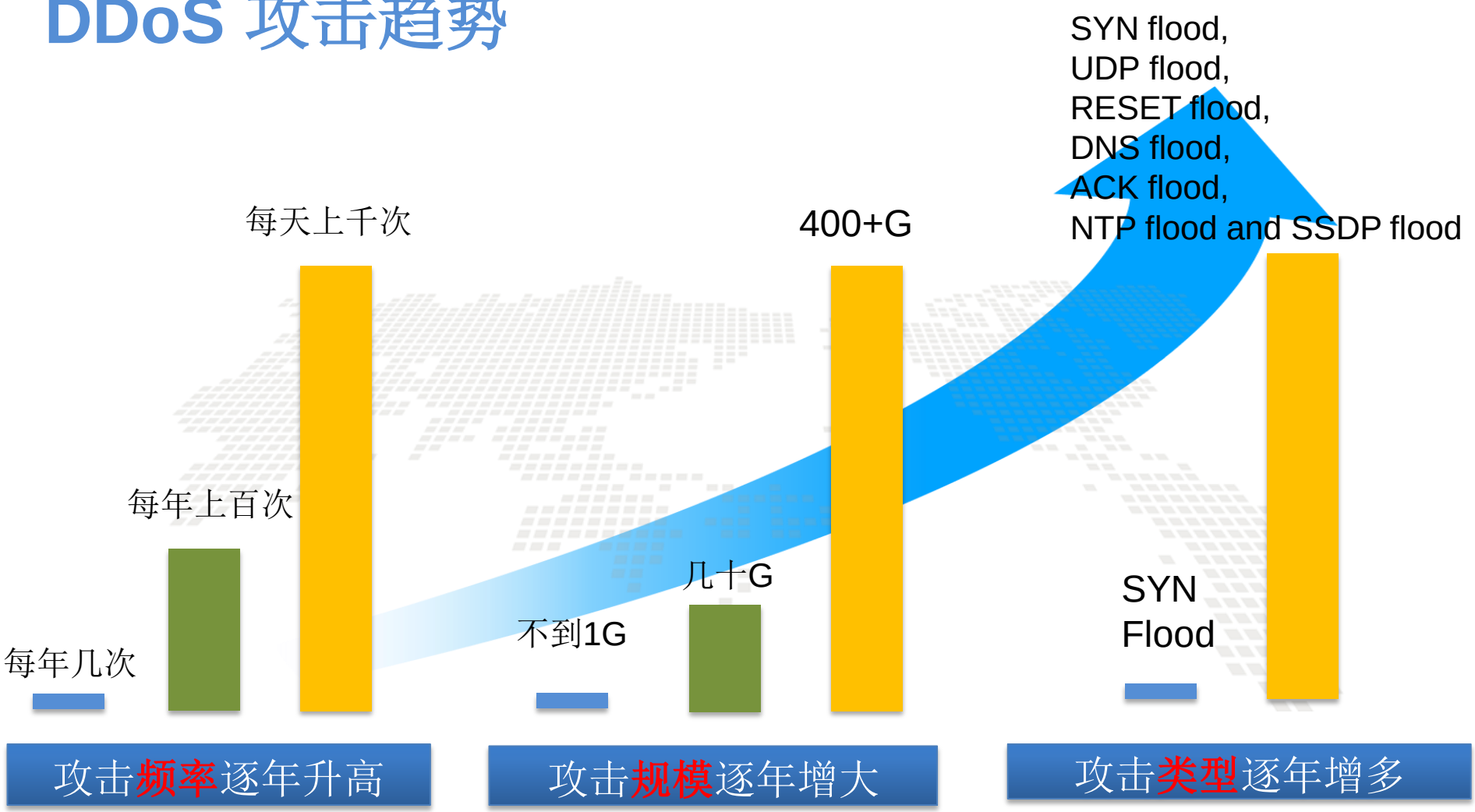
DDoS 发展趋势

行业现状

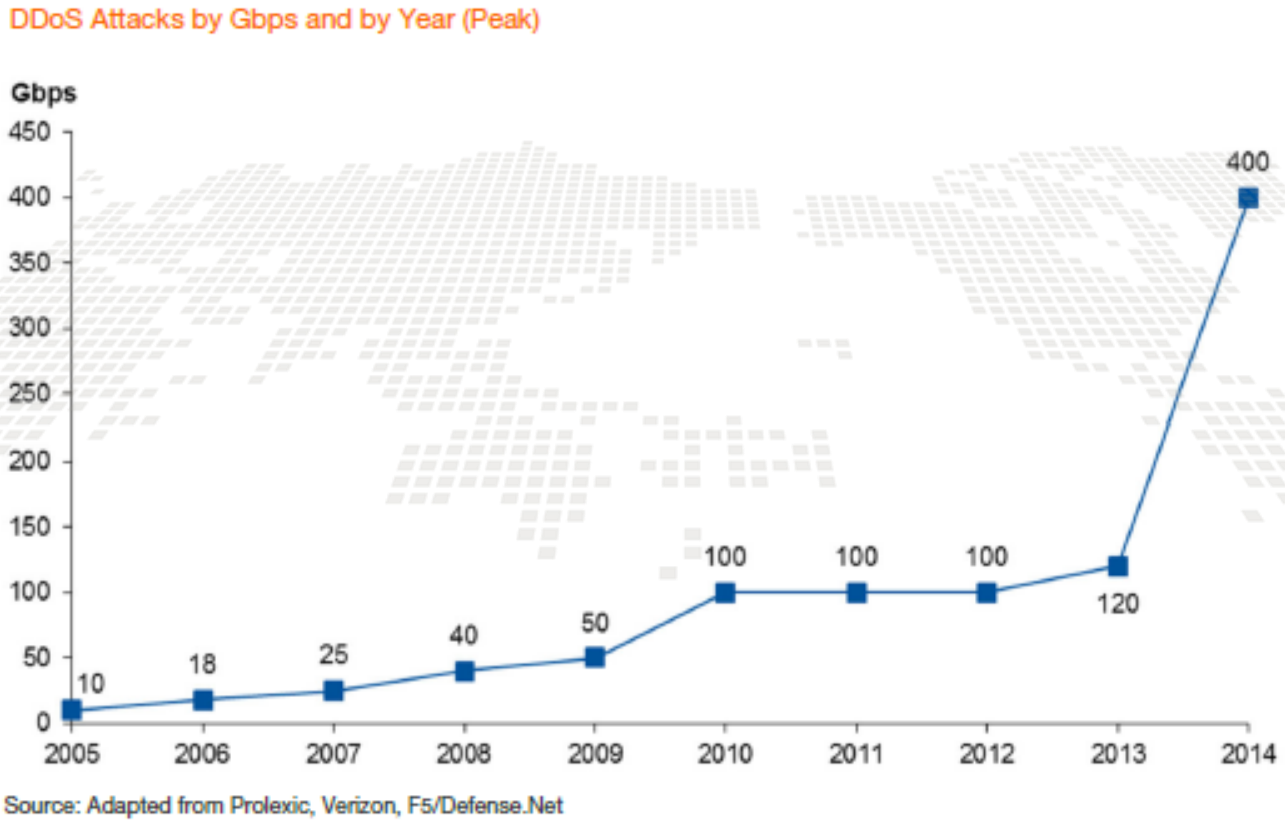
网宿抗 D 方案

DDoS 发展趋势

DDoS 攻击趋势


每天上千次
每年上百次
每年几次
400+G
几十G
不到1G
SYN flood,
UDP flood,
RESET flood,
DNS flood,
ACK flood,
NTP flood and SSDP flood
SYN
Flood
攻击频率逐年升高
攻击规模逐年增大
攻击类型逐年增多

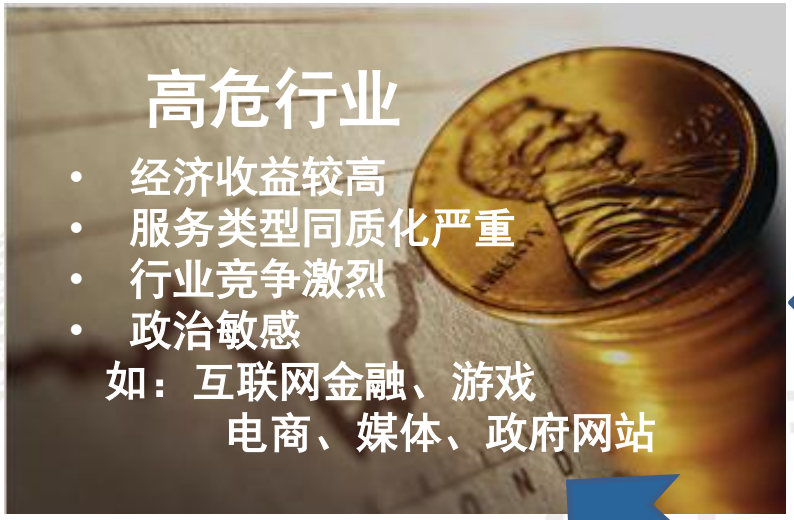
DDoS 攻击规模



From：Garnter

行业现状

DDoS 产业的三方



高危行业

- 经济收益较高
- 服务类型同质化严重
- 行业竞争激烈
- 政治敏感

如：互联网金融、游戏
电商、媒体、政府网站

选择

防护

防护方

- **防护能力：**防护峰值、防护种类、运营
- **解决方案：**传统设备、云清洗方案
- **提供方：**运营商、设备厂商、服务提供商
- **付费方式：**每设备、按次、按天、按流量大小

攻击

对抗

攻击方

- **工具：**LOIC，HIOC、XOIC、Darkddoser……
- **种类：**SYN flood,UDP flood, RESET flood, DNS flood, ACK flood, NTP flood and SSDP flood
- **目的：**炫技、黑产、恶性行业竞争、政治因素……

传统硬件抗 D 产品

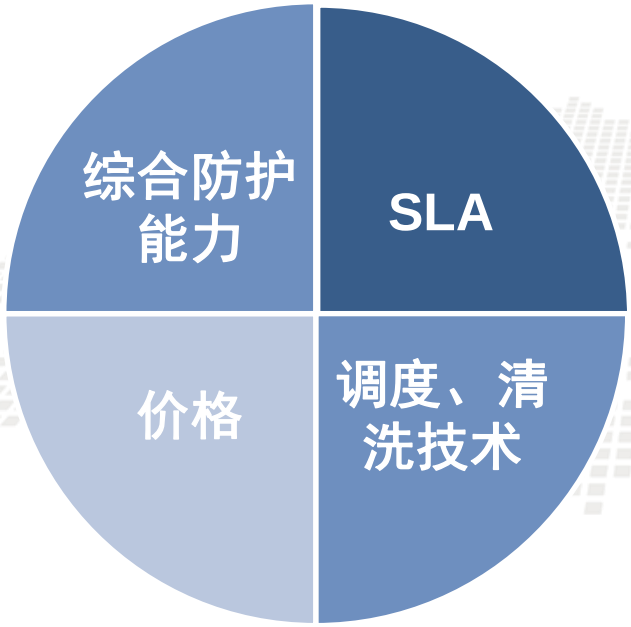
助力

* 攻防积累深厚
* 产品成熟度高
* 市场接受度好
* CPE端占有率高

挑战

* 成本高
* 升级、扩张性差
* 运维管理复杂
* 无法应对突发大规模攻击

云DDoS清洗



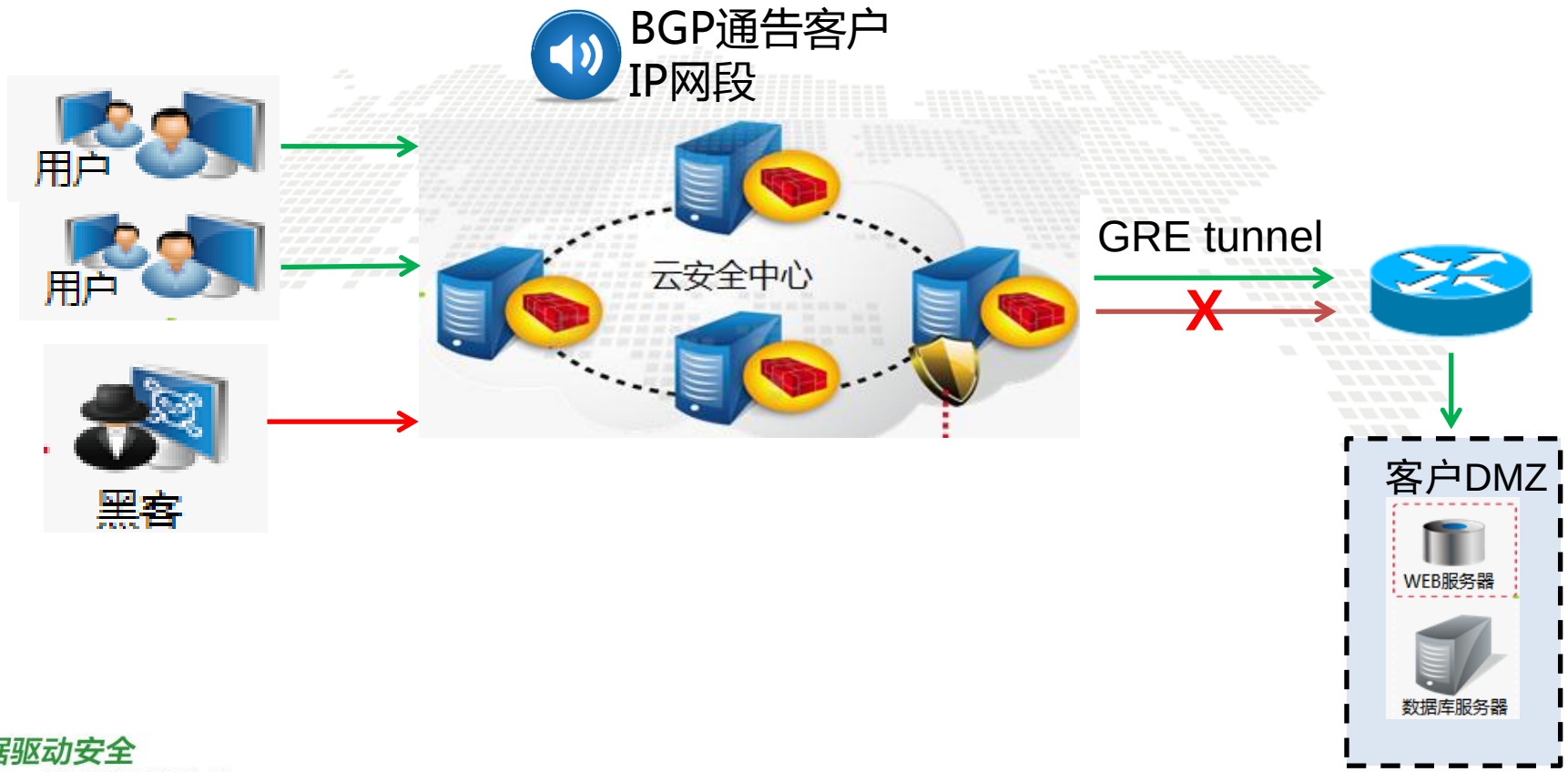
- 按需付费
- 无限扩展
- 免费升级
- 零运维、零改造
- 大数据分析

云安全 Anti-DDoS技术方案1

BGP Anycast

- Asymmetric routing
- Source IP 可见
- BGP依赖

- 国外广泛使用，国内尚无商用
- 针对各类应用均可防护

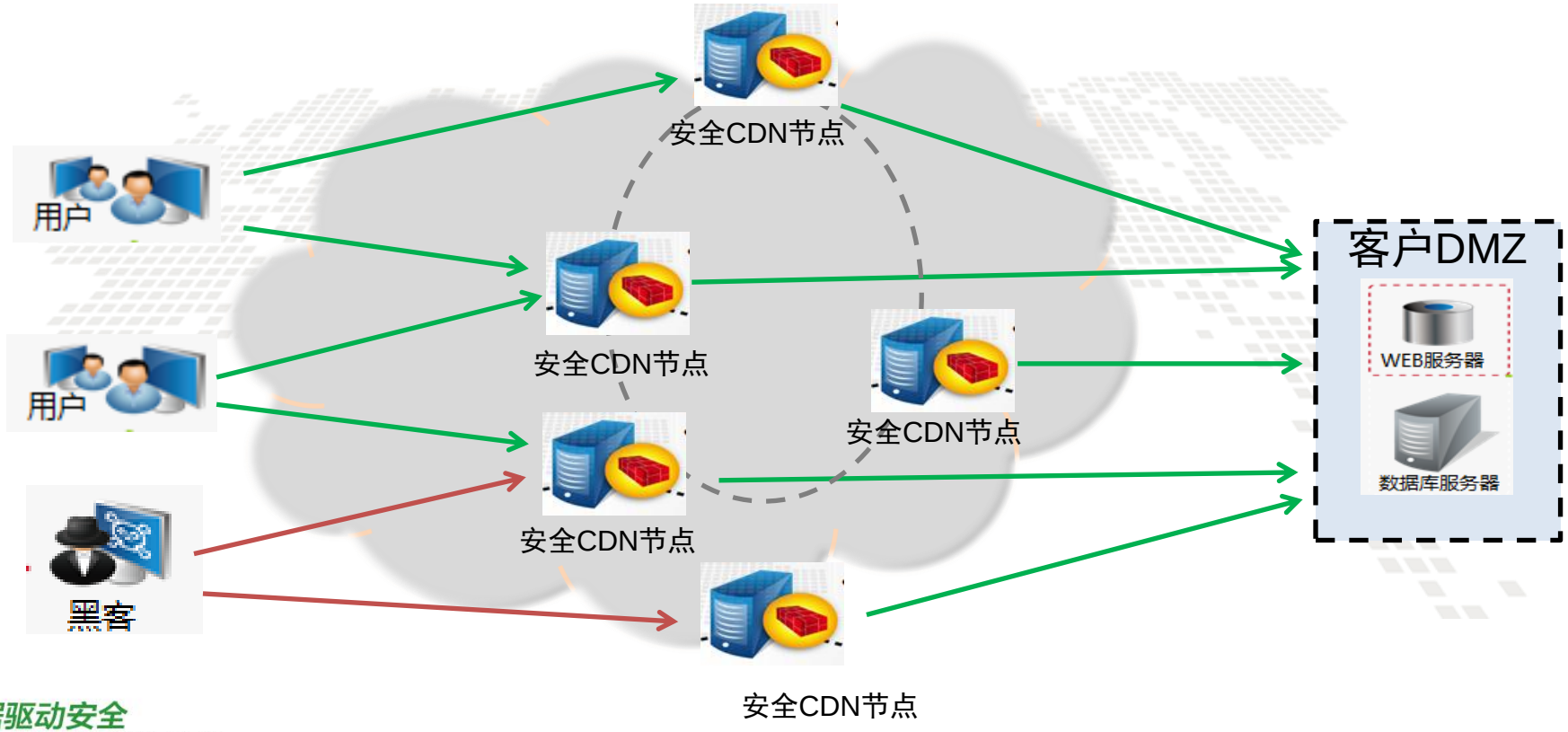


云安全Anti-DDoS技术方案2

Secure CDN

- DNS调度
- 不受带宽资源、ISP限制
- CDN加速
- 源IP不可见

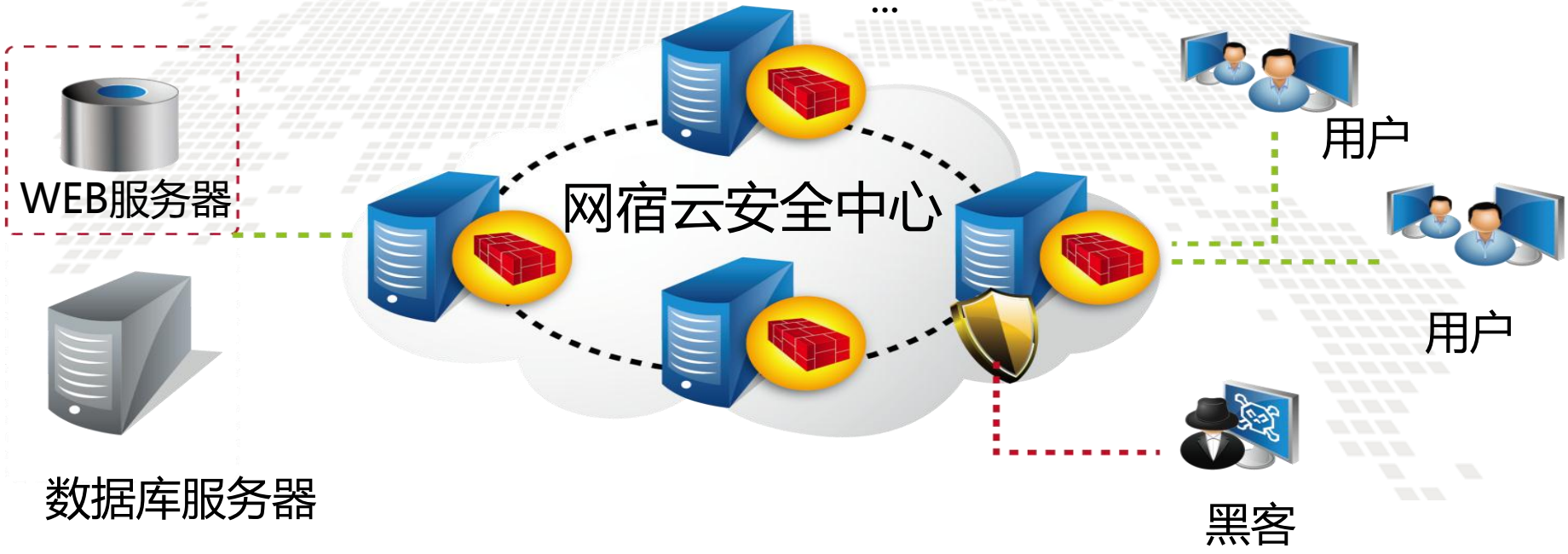
- 可适用于中国的网络环境
- 仅针对WEB应用有效
- 疏堵结合，分而治之



网宿抗D方案

网宿云安全: 提供一站式安全服务

- Anti-DDoS
- DNS 安全
- WAF
- ...



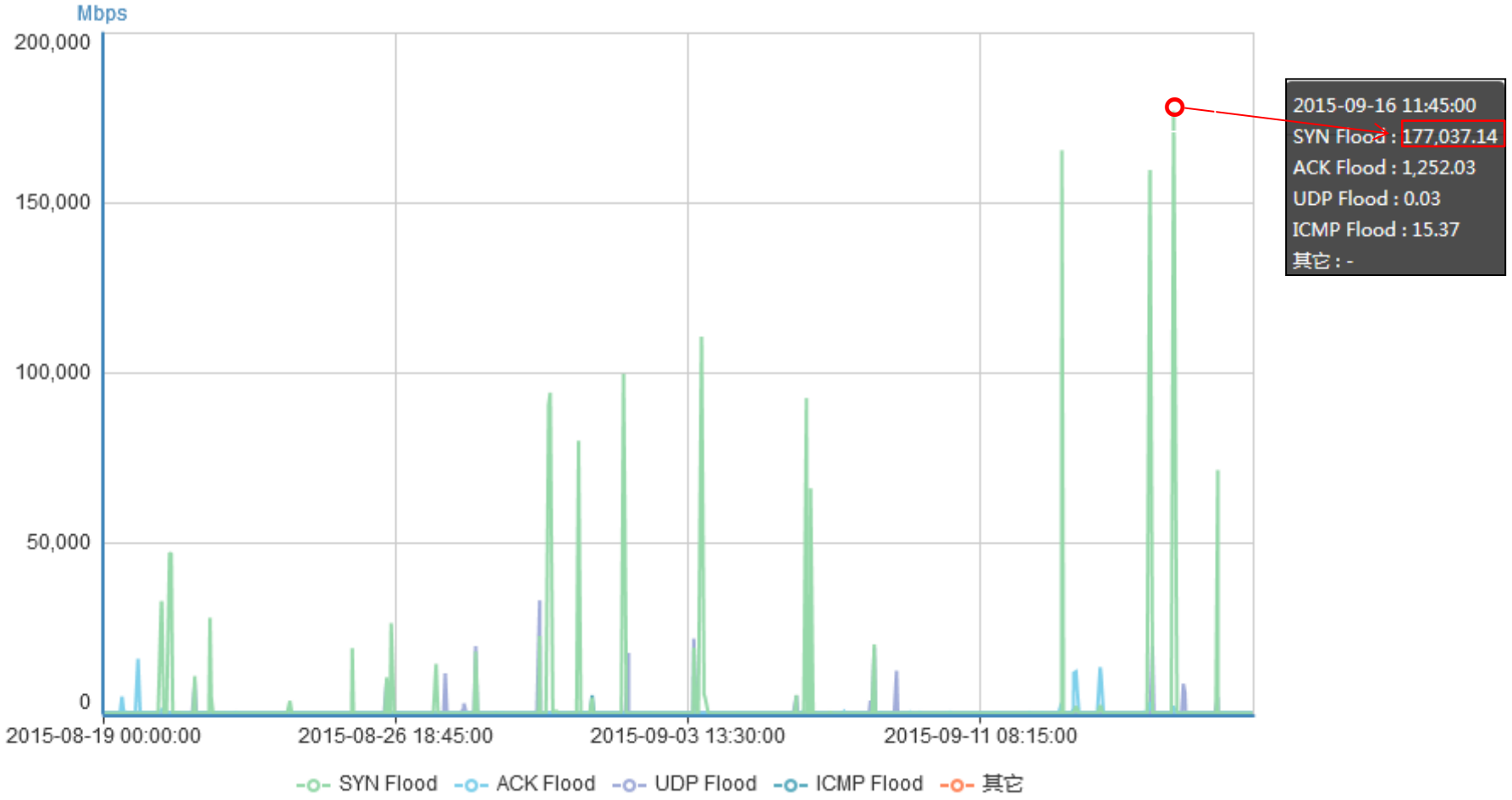
- **产品**

1. WSS ——安全加速服务
2. DMS ——DDoS流量清洗服务

- **技术**

1. DNS调度：利用DNS实现均衡，并加强DNS自身防护能力
2. DDoS清洗：4层负载均衡之前构建DDoS防护系统
3. 应用层防护：在4层与7层均实现HTTP Flood防护

网宿云安全平台数据



数据来源：
网宿云安全平台

ISC 2015 中国互联网安全大会

360互联网安全中心

THANK YOU

网宿科技 ChinaNetCenter