卓越的互联网业务平台提供商

基于CDN云分发平台的DDoS攻击防护方案

武志鹏

SACC2012

网宿科技 ChinaNetCenter

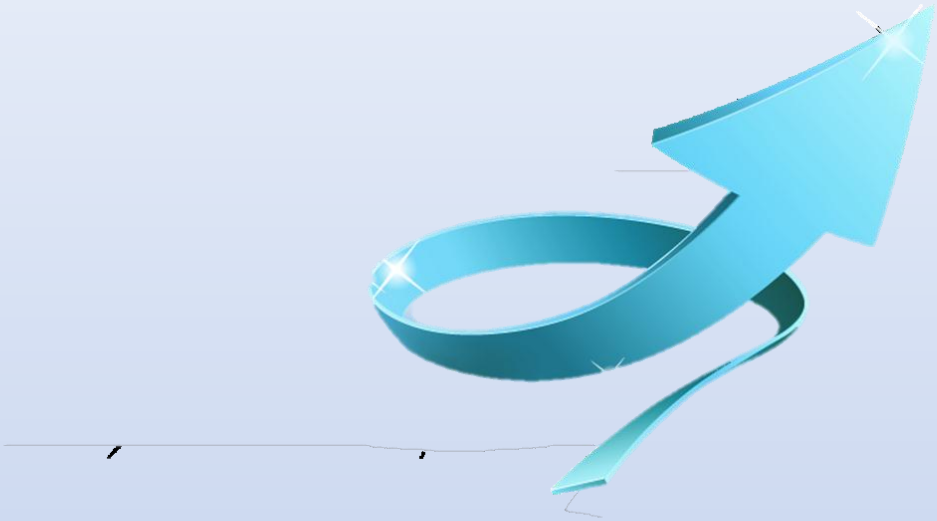
目录 Contents

网宿科技 ChinaNetCenter

DDos攻击

- DDoS攻击

  DDoS全名是Distributed Denial of Service (分布式拒绝服务),很多DoS攻击源一起攻击某台服务器就组成了DDoS攻击。



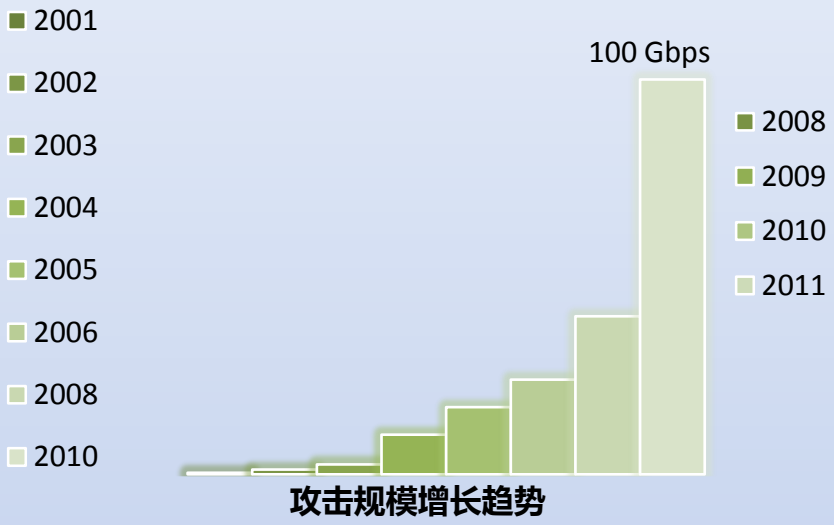
SACC2012

DDos攻击发展趋势

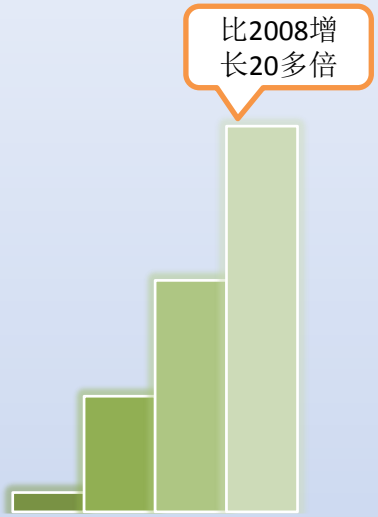
攻击规模倍数增长

攻击次数大幅增加

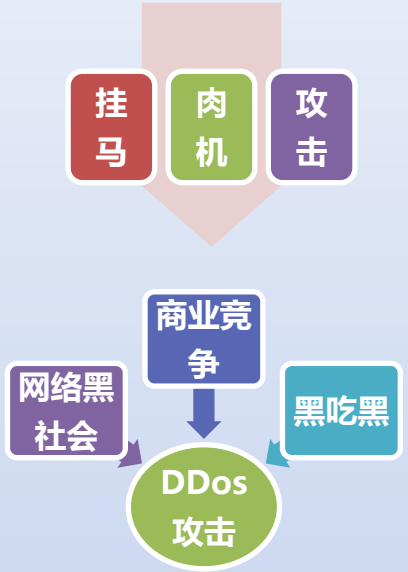
攻击形成产业链



攻击规模增长趋势



攻击次数增长趋势



网宿科技 ChinaNetCenter

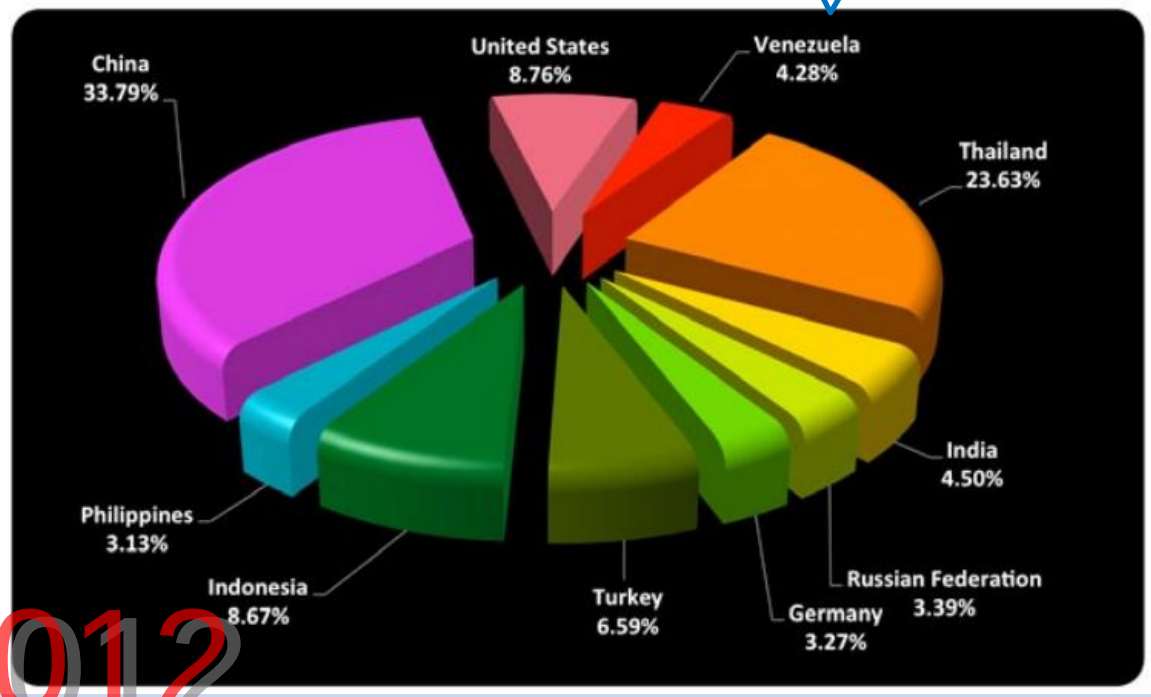
中国是最大的DDos攻击来源地

Akamai
2012 Q1

	Country	Q1 '12 % Traffic	Q4 '11 %
1	China	16%	13%
2	United States	11%	10%
3	Russia	7.0%	
4	Turkey	5.7%	
5	Taiwan	5.3%	
6	South Korea	4.3%	
7	Brazil	4.0%	
8	Romania	3.0%	
9	India	3.0%	
10	Germany	1.9%	
–	Other	39%	

Figure 1: Attack Traffic, Top Originating Cou

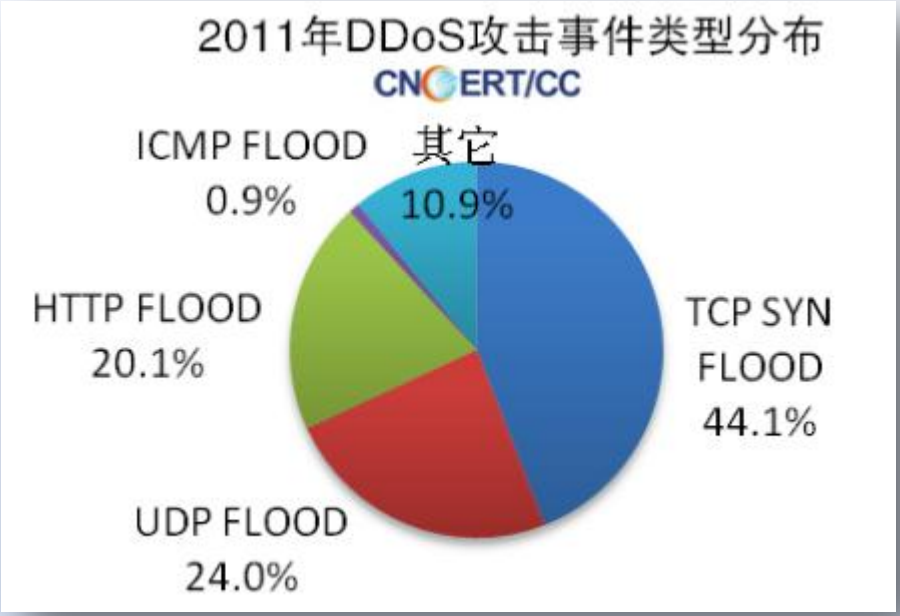
Prolexic
2012 Q2



SACC2012

网宿科技 ChinaNetCenter

中国DDos攻击频繁



- 我国境内日均发生攻击总流量超过1G的较大规模的DDoS攻击事件365起。
- 受攻击方恶意将流量转嫁给无辜者的情况屡见不鲜。2011年多家省部级政府网站都遭受过流量转嫁攻击，且这些流量转嫁事件多数是由游戏私服网站争斗引起。

摘自 国家互联网应急中心（CNCERT）《2011年中国互联网网络安全报告》

网宿科技 ChinaNetCenter

近年来一些DDos攻击事件

网宿科技 ChinaNetCenter

目录 Contents

DDos攻击防护方案思考

2

网宿科技 ChinaNetCenter

DDos攻击如何防御呢？

SACC2012

网宿科技 ChinaNetCenter

网宿DDoS攻击防护的思考

- 网宿拥有国内最大带宽容量的CDN平台，整体带宽储备量超过1500Gbps。
- 网宿通过多年的运营积累了丰富的DDos攻击防护经验，针对不同类型的攻击进行了针对性的防御，可以防御各种DDos攻击：SYN Flood、UDP Flood、ICMP Flood、HTTP GET/POST Flood、CC Flood、DNS Query Flood等。
- 在为客户网站提供安全保护的同时，也提供了CDN加速服务，提升用户体验，做到客户网站**“平”时“加速”，“攻”时“防护”**。
- 利用CDN多年数据分析经验积累，对攻击数据进行多角度的分析，以利于客户对攻击进行跟踪与后续处理。

目录 Contents

网宿DDos攻击防护方案概述 3

SACC2012

 | www.ChinaNetCenter.com

网宿科技 ChinaNetCenter

网宿DDoS攻击防护方案

方案动画演示

- 建立保护墙
- 攻击监测
- 调度、分散
- 逐个击破

网宿科技 ChinaNetCenter

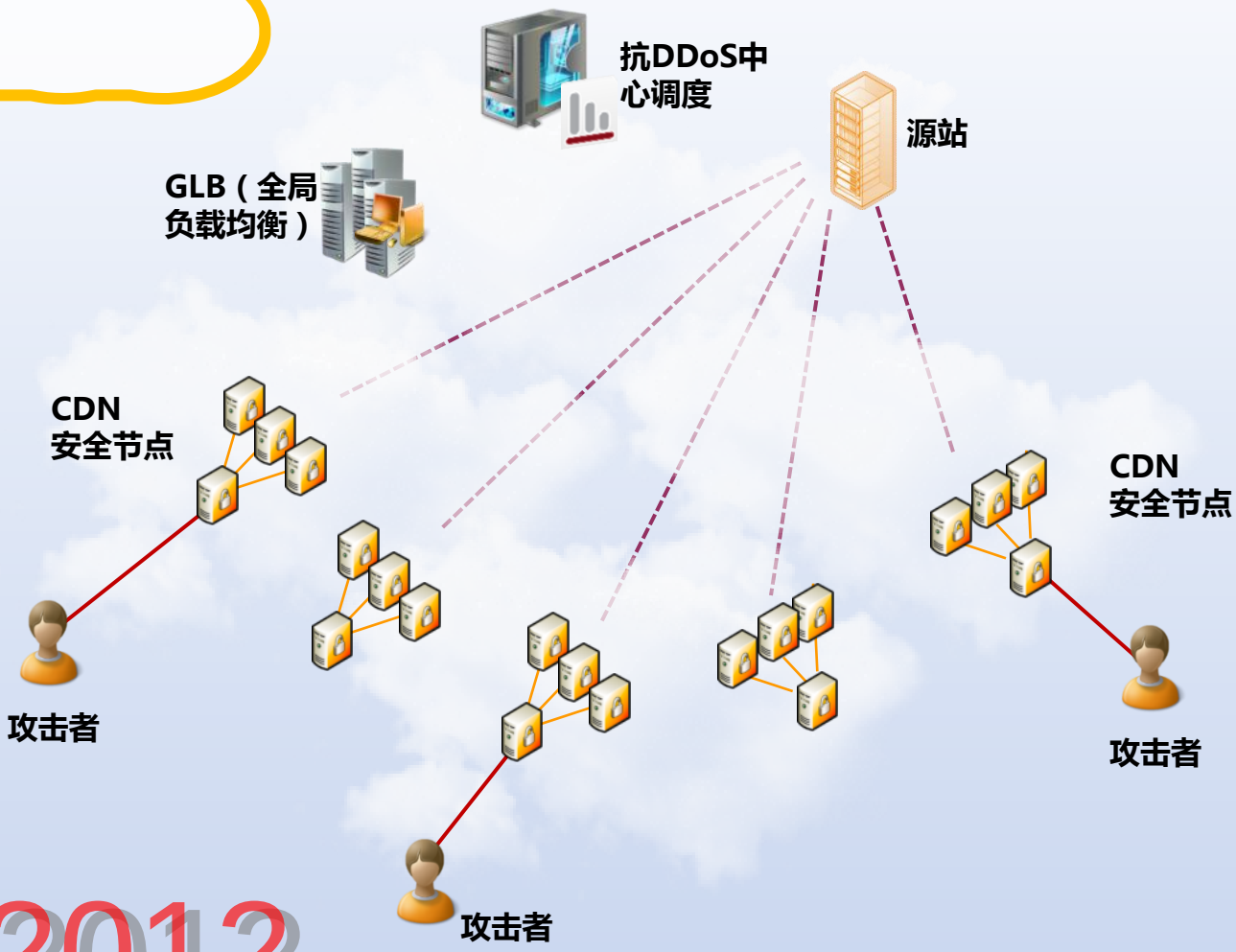
网宿科技DDos防护方案示意图

方案示意图

在客户源站外围建立**一道坚固的保护墙。**

CDN安全节点可抵御住绝大部分的攻击。

抗DDos调度中心，根据各个安全节点反馈的信息自动进行流量调度，保证每个安全节点所承受的攻击流量在它可承受的范围之内，尽量保证客户网站受攻击时访问的可用性。



网宿科技 ChinaNetCenter

目录 Contents

网宿DDos攻击防护方案功能介绍

4

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

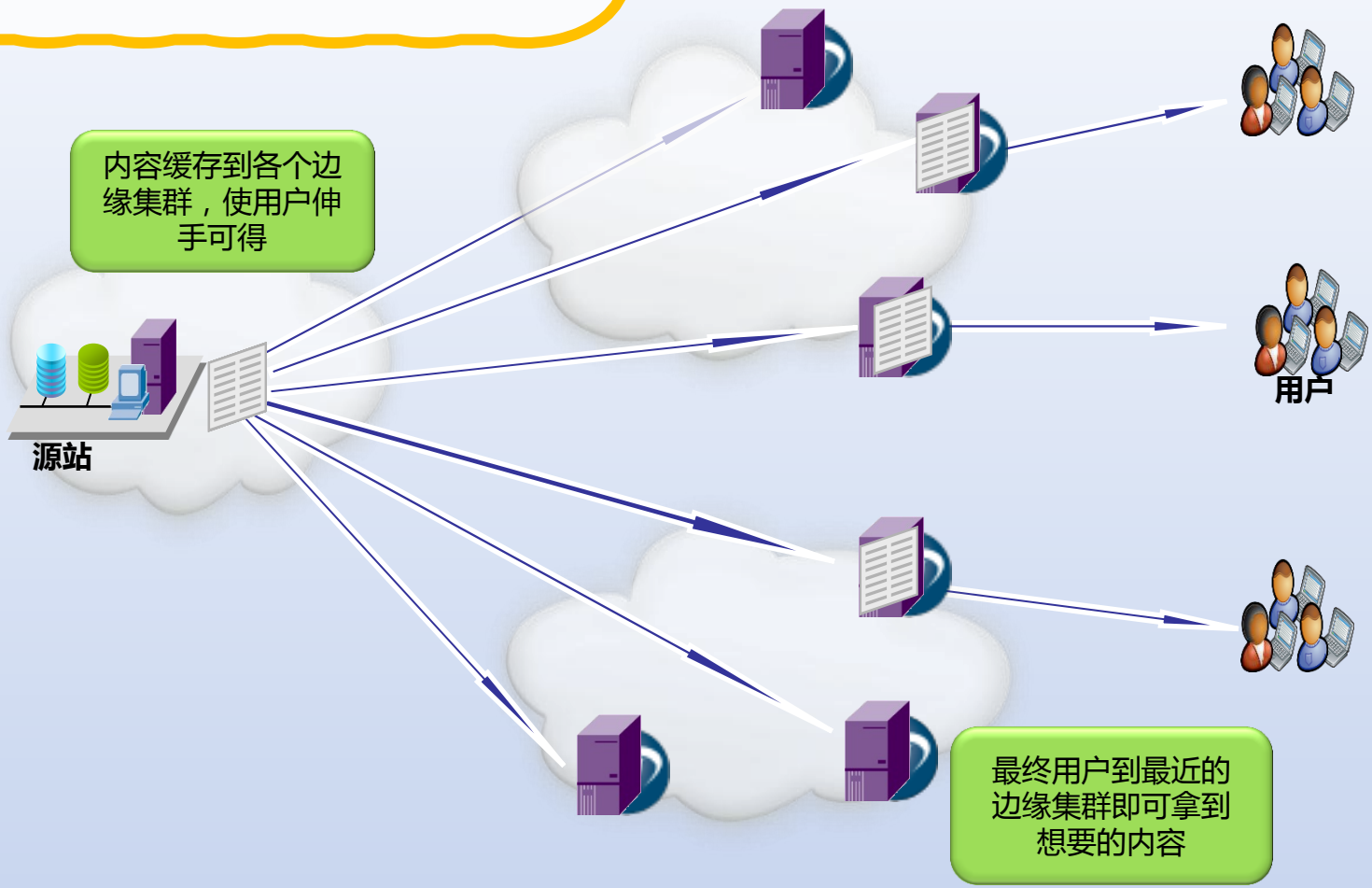
网宿CDN加速拥有强大的网络分发系统，可将客户网站的内容分发至网宿科技全网服务节点，并进行**智能调度**和**缓存**，使用户可**就近**取得所需内容，解决 Internet网络拥挤的状况，**提高用户访问网站的响应速度。**

SACC2012

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

CDN 加速功能



网宿科技 ChinaNetCenter

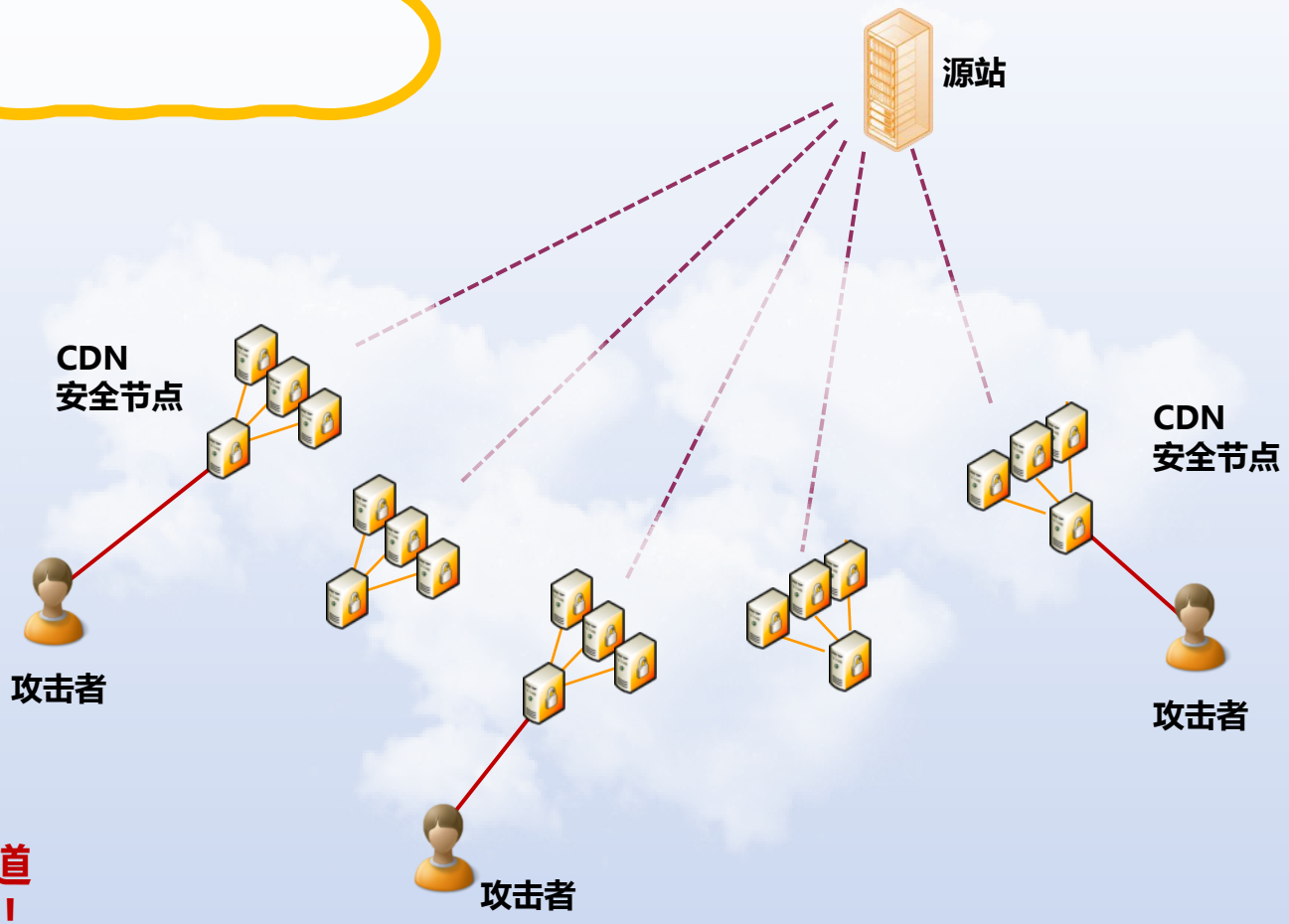
网宿科技DDos防护方案功能介绍

网宿DDos防护方案在客户源站外围建立一道坚固的保护墙，有效**隐藏了源站**。攻击者只能访问到CDN边缘安全节点，无法对客户源站进行直接攻击。保护墙除了**保护**源站不受到**DDos攻击**外，还**屏蔽了源站原有的其他安全漏洞**，消除了被攻击者利用其他漏洞攻击的隐患。

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

源站隐藏功能



攻击者不知道
源站在哪里！

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

抗SYN Flood攻击

当前最流行的DoS与DDos的方式之一，该攻击利用TCP协议缺陷，发送大量伪造的TCP连接请求，从而使得被攻击方资源耗尽。

SYN Flood攻击防范

传统的防范方案

收到传统的TCP SYN包并返回TCP SYN+ACK包时，根据SYN包计算一个cookie值，暂不分配数据区

根据cookie 值检验TCP ACK包的合法性。合法再分配专门的数据区进行处理未来的TCP连接

网宿的防范方案

网宿针对SYN攻击特征和协议栈低效的现状，在系统底层做了针对性的开发与性能优化，对SYN包做高效地响应和处理，使得防御SYN攻击的性能大幅提升。

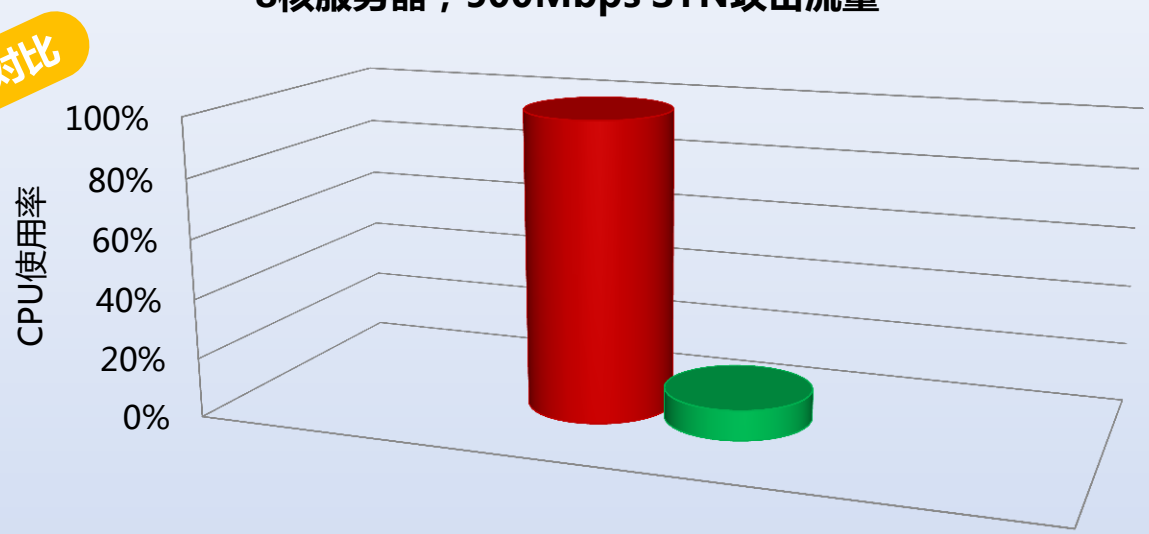
网宿抗SYN Flood性能是同等配置条件下传统SYN cookie的10倍以上！！

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

网宿抗SYN Flood攻击性能

抗攻击能力对比



	cpu使用率
syn cookie	100%
网宿方案	10%

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

抗UDP/ICMP Flood攻击

UDP/ICMP Flood攻击一般是带宽消耗型的攻击。

UDP/ICMP 攻击防范

由于主要提供的是Web服务，因此UDP/ICMP的数据包很少，网宿在系统底层针对这些类型包的请求设置一个阈值进行拦截，能够极大减轻机器的负载。

SACC2012

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

抗HTTP 攻击

HTTP Flood攻击是最为常见的DDos攻击之一。大量真实的HTTP请求，使得被攻击方资源耗尽。

HTTP 流量攻击攻击特征

特征　大量访问特定的静态URL，如网站首页

HTTP 流量攻击防护策略

策略1　CDN安全节点根据单位时间内同一IP的访问次数进行限制

策略2　CDN安全节点根据单位时间内的总访问流量进行限制

策略3　CDN安全平台根据单位时间内所有服务器的总访问流量进行限制

网宿科技DDos防护方案功能介绍

抗CC攻击

CC攻击是最为常见的DDos攻击之一。大量真实的HTTP请求，访问不存在的链接或者动态的URL，使得源站资源耗尽。

CC 攻击特征

特征1 大量访问不存在的URL，造成大量回源

特征2 大量访问动态的URL，造成大量回源

CC 攻击防护策略

策略1 CDN安全节点根据单位时间内同一IP的回源访问次数进行限制

策略2 CDN安全节点根据单位时间内的总回源访问流量进行限制

策略3 CDN安全平台根据单位时间内所有服务器的总回源访问量进行限制

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

抗DNS Query Flood 攻击

发送大量的域名解析请求，请求解析的域名可能是真实域名、随机生成或根本不存在的域名，从而使得被攻击方资源耗尽。

DNS 攻击防范策略

网宿使用**自主开发的GDNS**作为基础DNS，针对DNS Query Flood做了相应策略，单台服务器相比Bind抗攻击性能提升20倍以上，并通过集群化分布式的部署，使得整体系统具有很强的抗攻击能力。

网宿科技DDos防护方案功能介绍

网宿DDos防护方案对客户CDN加速及攻击进行详细的数据分析，为客户提供丰富的CDN加速报表及安全防护成果报表展示。

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

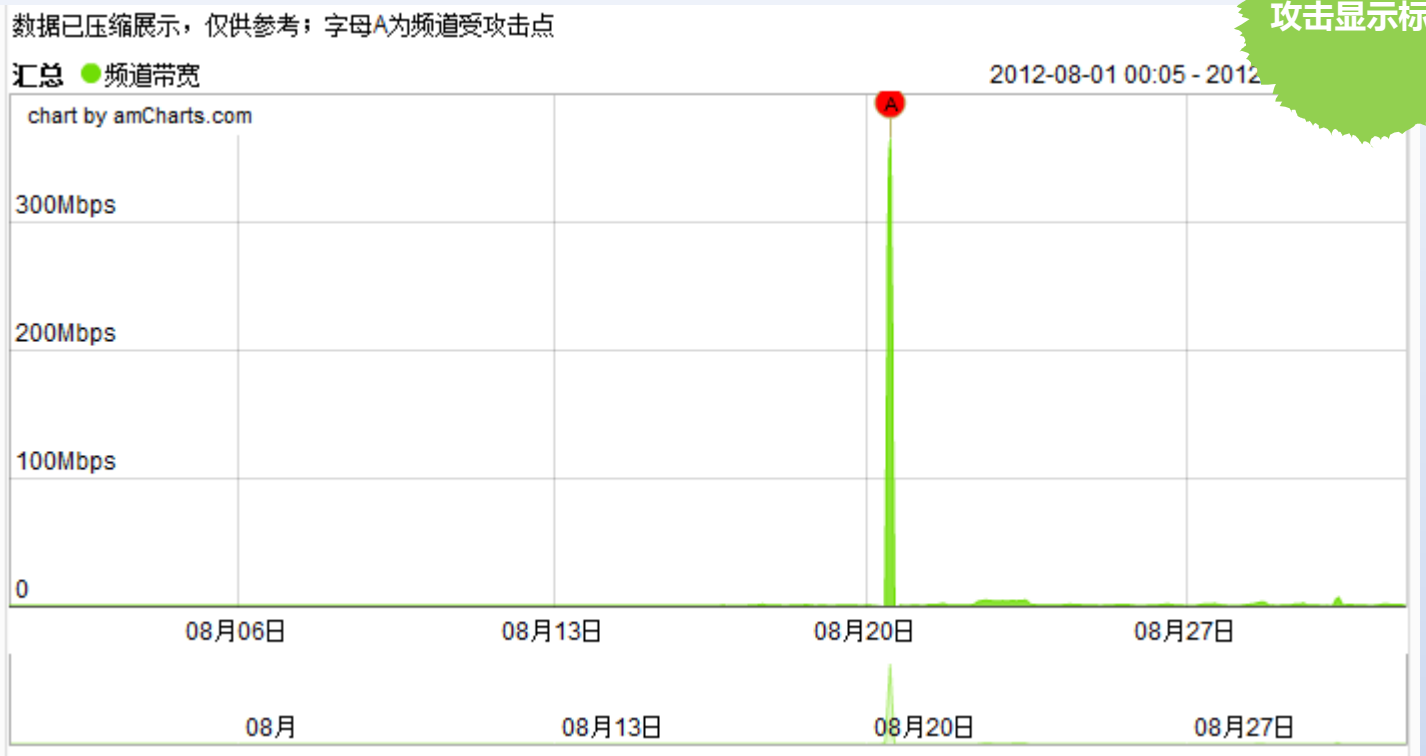
CDN加速报表

报表丰富
数据详尽

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

安全防护数据分析与展示



攻击显示标记

带宽攻击标记显示：

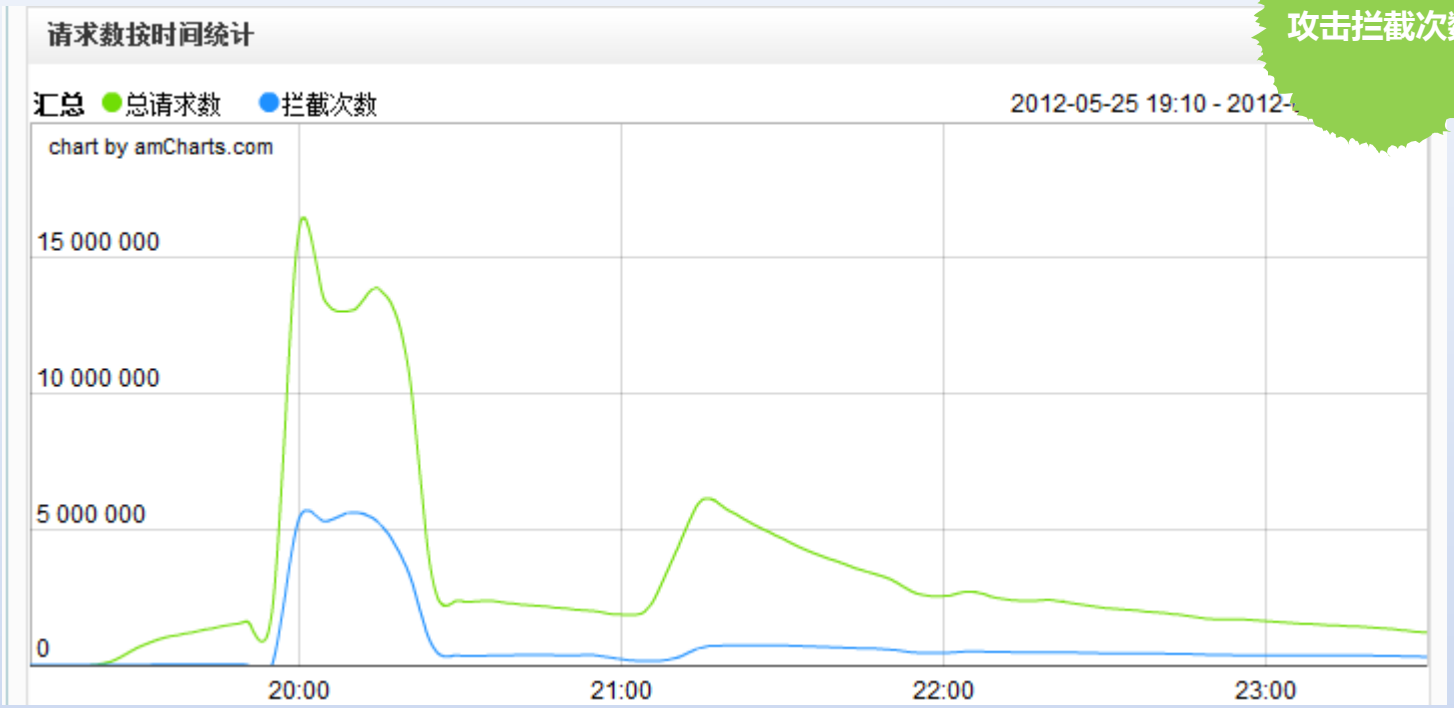
直观地了解某一定时间的攻击情况

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

安全防护数据分析与展示

攻击拦截次数



总请求次数与拦截次数的对比图：
直观地了解各个时段的安全防护状况

 | www.ChinaNetCenter.com

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

安全防护数据分析与展示

TOP100访客
安全拦截次数

TOP100访客按拦截次数排行

序号	IP	所在地	拦截次数
1	222.247.51.58	中国大陆湖南电信	226199
2	182.84.70.76	中国大陆江西电信	195880
3	115.221.233.48	中国大陆浙江电信	181403
4	61.131.218.95	中国大陆江西电信	169488
5	180.110.103.26	中国大陆江苏电信	152310
6	218.87.163.104	中国大陆江西电信	134384
7	124.193.57.188	中国大陆北京其它	128389
8	27.152.29.201	中国大陆福建电信	124656
9	218.87.107.10	中国大陆江西电信	107697
10	218.64.242.159	中国大陆江西电信	100991
11	117.40.252.172	中国大陆江西电信	99585
12	125.90.78.242	中国大陆广东电信	90658
13	219.159.186.12	中国大陆广西电信	90534
14	218.64.80.167	中国大陆江西电信	89715

TOP100访客拦截次数列表：

提供攻击访问最为强烈的IP列表，方便客户后续对攻击者的处理。

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

安全防护数据分析与展示

TOP100 URL
安全防护次数

TOP100 URL按拦截次数排行

序号	URL	拦截次数
1	http://www.[redacted]com/index.aspx	148456101
2	http://www.[redacted]com/	79282644
3	http://www.[redacted]com/wlManagerCenter/loginOn.aspx	50
4	http://www.[redacted]com/janhy.aspx	34
5	http://www.[redacted]com/wlManagerCenter/caselist.aspx	23
6	http://www.[redacted]com/site/BackSystem/KS.Split.asp	16
7	http://www.[redacted]com/site/BackSystem/index.asp	15
8	http://www.[redacted]com/site/BackSystem/Include/Label_Main.asp	13
9	http://www.[redacted]com/janhy.php	12
10	http://www.[redacted]com/janhy.asp	11
11	http://www.[redacted]com/site/backsystem/KS.Split.asp	8

TOP100 URL拦截列表：
提供攻击访问最多的URL列表，方便后续对被攻击URL做更进一步的防护处理。

网宿科技 ChinaNetCenter

网宿科技DDos防护方案功能介绍

实时监测攻击与报警

网宿DDos防护平台各个安全节点实时监测各种DDos攻击，并将详细的监测数据迅速报警到网宿科技24小时监控平台，24小时值班监控人员将迅速按照各种防攻击预案进行处理。另外，网宿DDos防护平台同时支持通过邮件与短信的方式将攻击报警通知到各相关人员，方便相关人员及时关注与介入处理。

网宿科技 ChinaNetCenter

目录 Contents

网宿DDos攻击防护方案案例

5

网宿科技 ChinaNetCenter

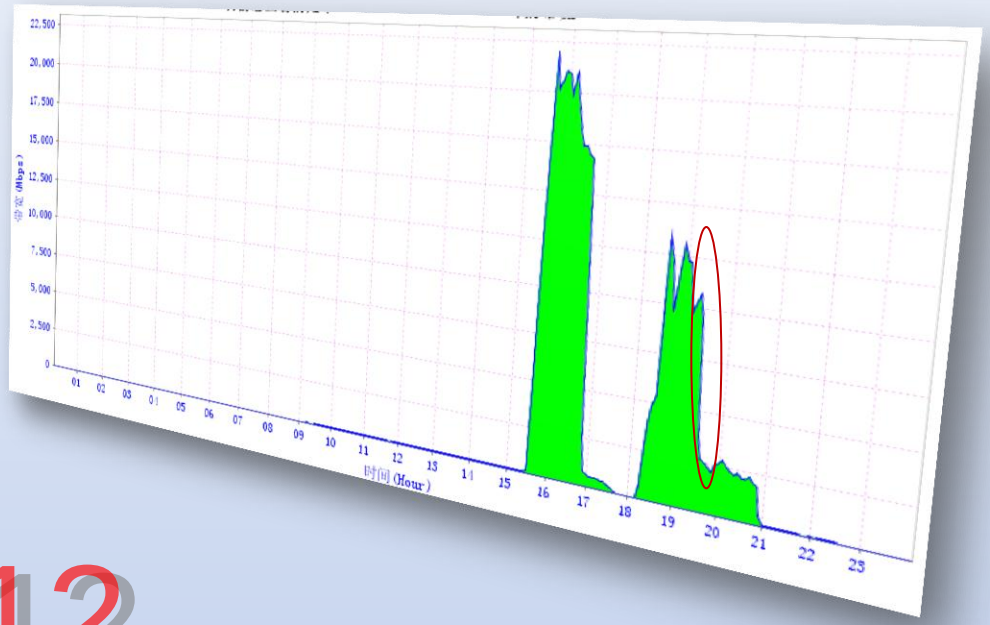
网宿抗DDoS攻击案例

某电子商城遭遇HTTP GET攻击

*2012年4月某电子商城 HTTP GET攻击，网宿成功抵御了**22Gbps**的HTTP GET攻击，攻击带宽约为该电子商城网站平常的**1100倍**(平常带宽约20Mbps)。*

- *19:30 网宿通过数据分析得到攻击特征。*
- *部署相应的安全防护策略，抵御异常请求，带宽降低为*
- *2.5Gbps。*

20:50攻击结束。



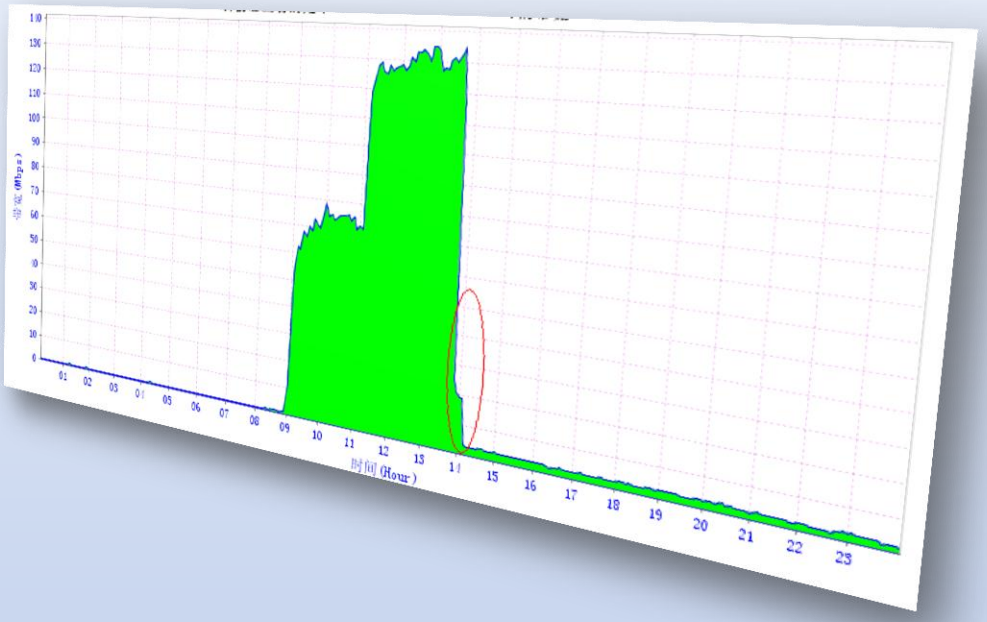
SACC2012

网宿科技 ChinaNetCenter

网宿抗DDoS攻击案例

某商业电讯网站遭遇CC攻击

2012年5月某商业电讯遭遇CC攻击，导致大量动态内容回源请求，最高回源动态请求量达140Mbps，经网宿数据分析后，部署相应的防护策略后，回源请求大大减小，源站压力骤降。

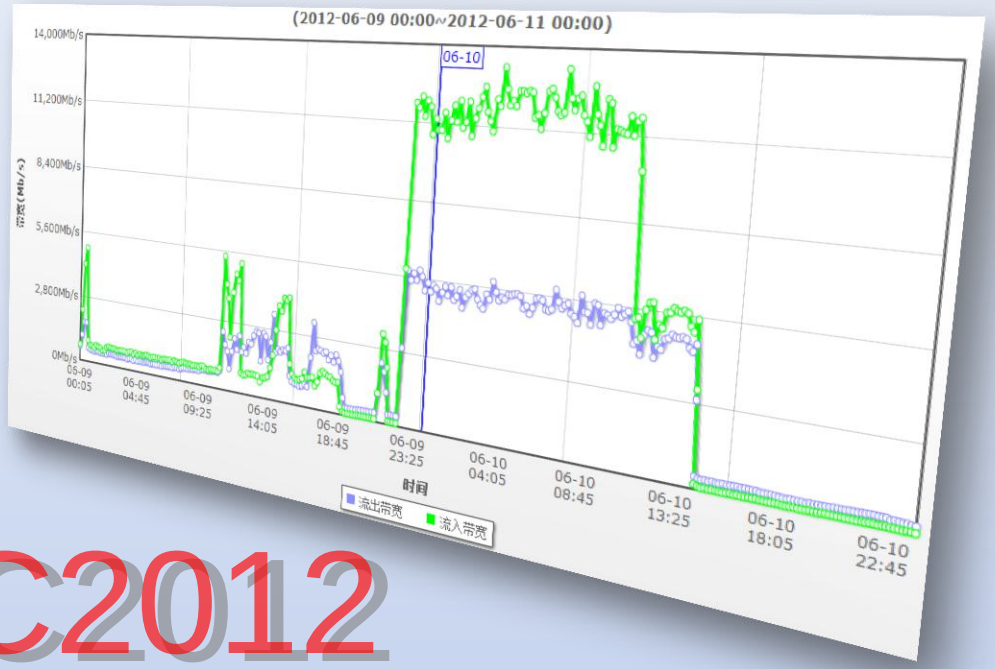


网宿科技 ChinaNetCenter

网宿抗DDoS攻击案例

某电子商务网站遭遇SYN Flood攻击

2012年6月某电子商务遭受多次SYN Flood 攻击，攻击时间持续较长，最大攻击量达到了 ***14Gbps***，*网宿成功抵御了攻击，保证了网站正常服务。*



SACC2012

网宿科技 ChinaNetCenter

网宿平台遭遇DDos攻击不完全记录

时间	攻击类型	攻击带宽
2011.9	**DNS Query Flood**	**>10Gbps**
2011.9	**SYN Flood**	**>15Gbps**
2011.11	**SYN Flood**	**>15Gbps**
2011.11	UDP Flood	>2Gbps
2011.12	DNS Query Flood	>8Gbps
2011.12	SYN/UDP/HTTP GET Flood	约3.6Gbps
2011.12	HTTP GET Flood	约2.3Gbps
2011.12	HTTP GET Flood	约1~2Gbps
2012.1	HTTP GET Flood	约7.5Gbps
2012.1	HTTP GET Flood	约7Gbps
2012.1	SYN/HTTP GET Flood	约4Gbps
2012.1	SYN/HTTP GET Flood	约2Gbps
2012.1	HTTP GET Flood	多次，1.1~1.5Gbps
2012.1	HTTP GET Flood	约2.75Gbps
2012.1	SYN/HTTP GET Flood	约5.5Gbps
2012.2	HTTP GET Flood	多次，3.7~4.5Gbps
2012.3	UDP/HTTP GET Flood	约5Gbps
2012.3	HTTP GET Flood	约2.25Gbps
2012.4	HTTP GET Flood	约2.7Gbps
2012.4	**HTTP GET Flood**	**约22Gbps**
2012.5	CC Flood	约140Mbps
2012.6	**SYN Flood**	**约14Gbps**

注：以上是从2011年9月到2012年6月的不完全统计攻击记录，除了CC Flood之外，均为1Gbps以上的。
其它攻击仅统计1Gbps以上的攻击，还有数十次1Gbps以下的攻击。

网宿科技 ChinaNetCenter

目录 Contents

网宿DDos攻击防护方案小结

6

SACC2012

 | www.ChinaNetCenter.com

网宿科技 ChinaNetCenter

网宿科技DDos防护方案小结

方案小结

- 首先，网宿DDos攻击防御方案充分利用CDN的特点，在客户源站**外围建立一道坚固的保护墙**，有效**隐藏客户源站**，避免源站受到攻击，**是对原有单一节点安全系统的有力补充。**
- 其次，网宿DDos攻击防御方案使用网宿全球负载均衡系统，该系统能够实时监测平台所有节点的服务状况，灵活调度流量，同时结合网宿抗DDoS调度系统，有效**分散攻击**，对故障进行及时切换，保障平台所有客户的可用性。
- 最后，网宿DDos攻击防御方案在**整个平台均部署了防攻击策略**，对不同类型攻击进行**针对性防御**。

网宿科技 ChinaNetCenter

THANK YOU!

感谢聆听！

SACC2012

 | www.ChinaNetCenter.com

网宿科技 ChinaNetCenter