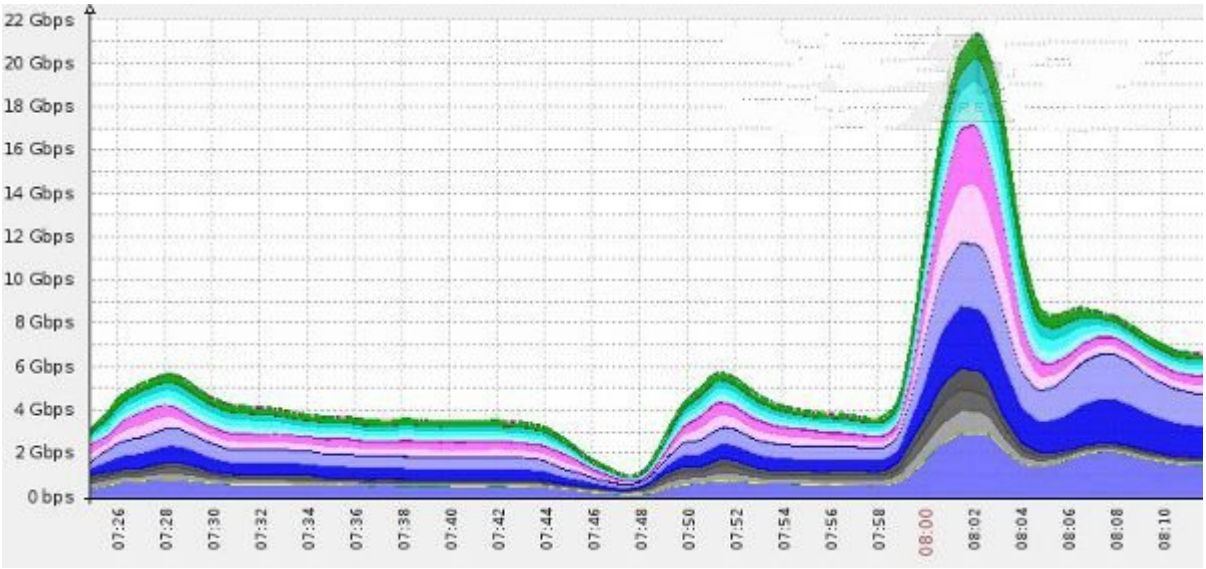
随着IT技术的发展,云计算开始进入到人们的视野,它是一种划时代的革命性产物,通过网络把大规模计算资源与存储资源进行有效整合,以可靠服务的形式提供给用户使用。其对信息技术产业的影响，已经从IT基础设施领域，扩展到了硬件和设备制造、软件开发平台、软件部署、软件销售、IT服务,几乎涵盖所有的IT硬件、软件、服务领域。

随着越来越多的公司开始使用虚拟化数据中心和云服务，企业基础设施出现了新的弱点。与此同时，云计算拒绝服务攻击也开始由原来利用大量数据流进行暴力式攻击转变为针对基础应用程序的技术性攻击。

近年来，DDOS攻击已经不单纯的是利用流量进行攻击，攻击者还尝试用DNS的漏洞和不正确的配置来进行攻击，如DNS反射攻击，根据Arbor Networks发布的2012年全球基础设施安全报告显示，41%的受害者的DNS基础设施遭到DDOS攻击。

DNS反射攻击是利用DNS协议的安全漏洞进行的攻击的拒绝访问攻击方式，攻击者利用僵尸网络向DNS服务器发送DNS请求，并将请求数据包的源地址设置为受害者。



大多数的(针对DDOS攻击的)网络对策方案无法使网络免受DDoS攻击，因为它们无法阻止通信的大量涌入，而且典型情况是，它们都不能区分好的内容和坏的内容。

传统的IPS、WAF之类根据特征来识别网络数据是有效的，但是对于内容合法而目的不良的攻击却束手无策。类似的，防火墙通常用一些简单的规则来拒绝或者允许协议、端口或IP地址。DDOS攻击可以很容易地绕过防火墙和IPS设备是因为它们被设计成在发送合法的通信流量。

DDOS攻击主要分类:

Volume Based

Attacks :大数据洪水攻击，此类别包括常见的ICMP洪水攻击、UDP洪水攻击和其他带有欺骗性的数据包洪水攻击。这种类型的攻击经常使用网络上常见的工具进行攻击。

Protocol Attacks：攻击者利用网络协议的缺陷攻击通信设备的服务资源，如负载均衡等。此类别包括SYN洪水攻击、Ping of Death攻击、分片包文攻击、Smurf攻击等。

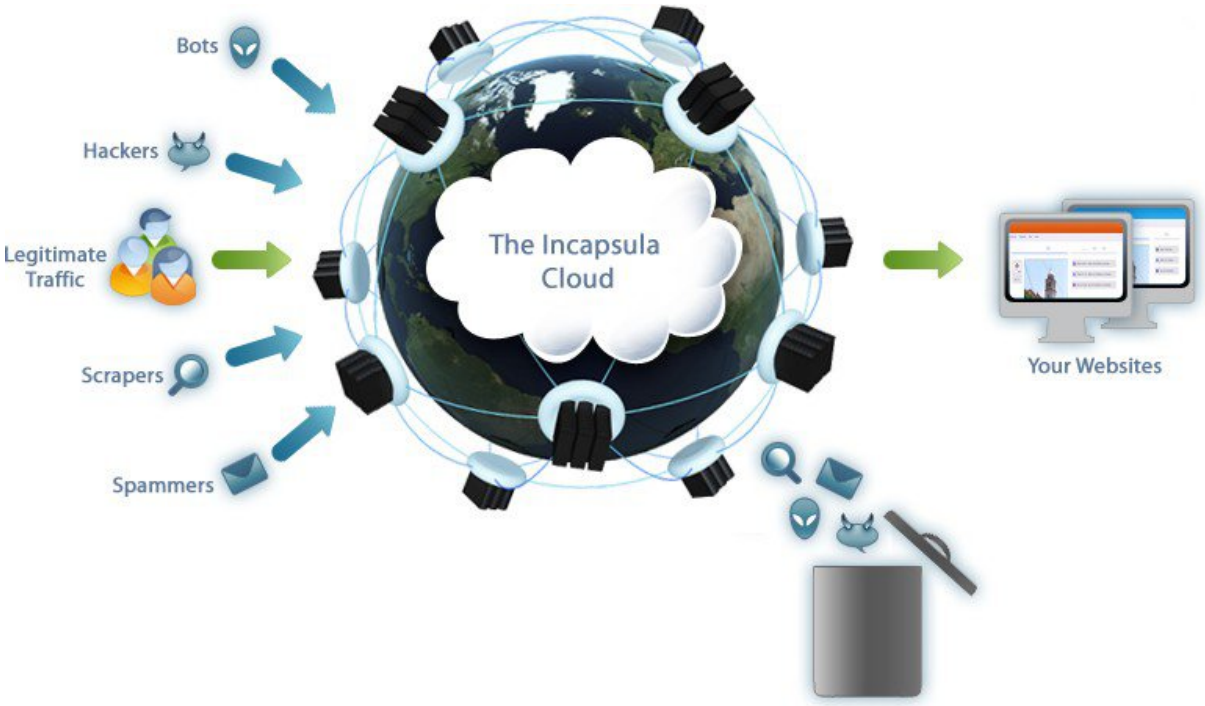
Application Layer (Layer 7)

Attacks：攻击者发送大量的数据包或利用服务器应用的漏洞等，饱和服务器的资源，造成DDOS攻击，该类漏洞往往不需要大量的肉鸡。应用层DDOS攻击的列子包括Slowloris、Apache、Windwos、OpenBSD等的漏洞。如ModSecurity
空指针间接引用远程拒绝服务漏洞(CVE-2013-2765)，攻击者可以利用该漏洞使Apache Web服务器崩溃。

基于云的DDOS缓解方案

由于云计算的带宽相比传统数据中心来说要大得多，所以DDOS攻击成本也相应增加，如去年维基解密遭到DDOS攻击，后迁移到云计算服务商CloudFlare上，这就让攻击维基解密变得十分困难，因为CloudFlare的服务器带宽都能达到10Gb/s，而之前的DDoS攻击的原理就是通过大量的访问请求导致服务器瘫痪。

大部分的DDOS商业解决方案提供了收集流量日志并基于相关阀值告警，另一种常见的DDOS检测方法是“分层过滤”，利用专用的设备和软件检测以及检测网络层和应用层不同类型的攻击，许多公司也利用开源软件来根据特征限制流量大小。



传统的DDOS攻击缓解方案是利用大量的网络带宽，并采用复杂的硬件，如防火墙、负载均衡等。也有很多人质疑，这种做法一方面是成本非常高，另一方面在很多情况下并没有什么好的效果。如市面上市面上2G硬防单价在10W左右。出于这个原因，很多公司都选择采用基于云计算的方式来防护DDOS攻击。

基于云计算的防护方法的另一个优点是减少设备和基础设施的投资（capex）以及其他硬件解决方案（opex），降低防护成本。

评估DDOS攻击缓解方案的关键标准

在众多的DDOS攻击缓解解决方案中选择一个适合自己的方法并不简单，如硬件方式、软件方式、基于云的解决方案等，为了简化选择过程，下面列举了一些在DDOS攻击防护方案中最重要的功能/标准供参考：

1：支持协议容量解决方案，提供细粒度的传输协议分析。

2：支持流量分析。

3：产品的灵活性：可以自定义策略和模式等。

4：产品的可扩展性

5：硬件的冗余功能的可用性

6：能提供详细的不同层次的报告和告警。

7：可靠性：DDOS是一个动态的威胁，没有固定的时间段，所以一定要能提供其产品的不断更新以及技术支持

8：双向流量监控：控制入站和出站流量

9：调查该产品的声誉和客户案例等。

如前所述，目前流行的DDOS攻击缓解方案是基于云的防护方式，公司Incapsula、Prolexic、Verisign、Juniper等都有提供这样现成的解决方案，能够实时监测和分析网络流量，当检测到DDOS攻击的时候，能够将恶意流量通过云架构进行缓解，进行流量清洗。

一个经典的案例是，今年5月的时候，美国MSSP

Prolexic宣布成功防护了史上最大的DNS反射DDoS攻击（DrDDoS），流量达167Gbps，目标是金融机构。Prolexic全球4个节点参与了防护，其中伦敦清洗中心承担了90Gbps的攻击。