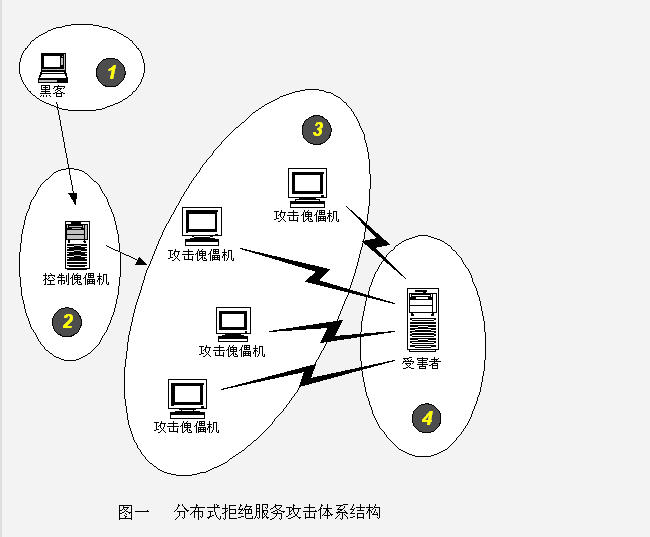
## DDOS攻击分析方法与分析

### DDOS 概论

DDOS 英语全名为Distributed Denial of Service 分布式拒绝攻击。是现在网络攻击中最经常使用也是最难以防御的一种网络攻击。其攻击原理与传统的DOS相似，都是利用合理的服务请求来占用过多的服务资源，从而使合法的用户无法得到服务响应。DDOS是传统的DOS的“增强版”。由传统的单台PC的攻击扩展为大量的PC（一般是黑客占领的傀儡机，也就是“肉鸡”）集群的攻击。其攻击效果和规模是传统的DOS所无法相比的，下图为DDOS攻击的示意图：



如上图：黑客控制者一般会通过“跳板”即图中的2 控制傀儡机来发送自己的攻击指令，而傀儡机接受到攻击指令以后会向受害者发起潮水般的攻击。淹没正常的服务请求，造成正常的服务无法进行。

### DDOS种类

DDOS的攻击方法很多，大体上可以分为三大类：

主要以消耗系统资源为主的攻击

这种代表者为 syn flood 和模拟正常用户访问请求反复查询数据库等大量消耗系统资源的攻击。消耗系统资源的攻击不需要很大的流量就能取得不错的攻击效果。例如SYN flood ，windows2000 系统当物理内存是4g的时候 核心内存只有不到300M，系统所有核心模块都要使用核心内存所以能给半连接队列用的核心内存非常少。Windows 2003 默认安装情况下，WEB SERVER的80端口每秒钟接收5000个SYN数据包一分钟后网站就打不开了。标准SYN数据包64字节 5000个等于 5000\*64 \*8(换算成bit)/1024=2500K也就是 2.5M带宽 ，如此小的带宽就可以让服务器的端口瘫痪，由于攻击包的源IP是伪造的很难追查到攻击源,，所以这种攻击非常多。

消耗网络资源的攻击

代表者有UDP flood ，ICMP flood ，smurf等。此类攻击主要是通过大量的伪造数据包，来淹没正常的数据请求，实现拒绝服务。此类攻击的数据包多为大包，而且伪造现象明显。值得指出的是 UDP flood 即可以消耗网络资源又能造成攻击主机的系统资源耗尽，这个和UDP的设计原理有关。当被攻击主机收到对自己没有开放UDP端口的请求的时候，会回送ICMP 端口不可达的信息，当大量的请求来临时，回送ICMP信息所消耗的资源越来越大，最好导致系统没有资源分配给正常的请求。

针对系统或者网络设备自身的bug 的攻击

代表者有比较有名的ping of death，land-based 和teardrop等。这类攻击大多设计精巧，利用系统自身的漏洞造成服务器或网络设备宕机或重启，从而无法提供正常的服务，此类攻击在现实中已经很少见到。

### DDOS攻击分析

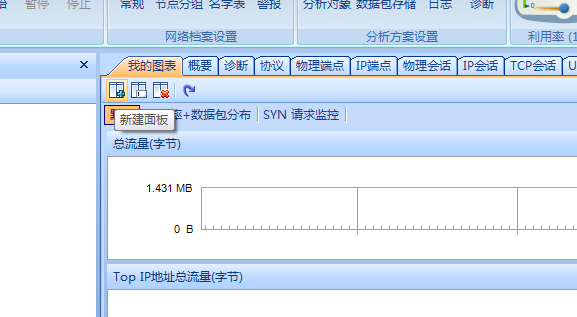
DDOS攻击造成的现实是比较明显的，例如网络带宽被大量的消耗，网络利用率接近100%，服务器的CPU和内存消耗很大，正常的服务响应很慢或完全无响应等。当客户遇到这种现象的时候第一个反应就是：我被攻击了。但究竟是什么攻击？怎么采取措施？我们建议采用抓包分析的方式来了解和分析。

使用抓包分析能够比较直观和准确的反应网络现状，了解攻击行为和方式。只有在对攻击有很清楚的认识后，我们才能采取有针对性的防御，这样的防御才是积极有效的。

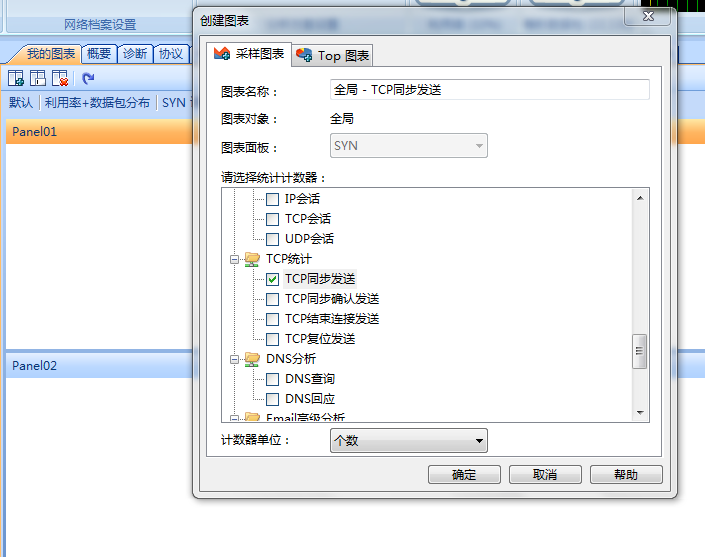
这里我们使用几种比较常见的DDOS攻击来分析

###### SYN flood。

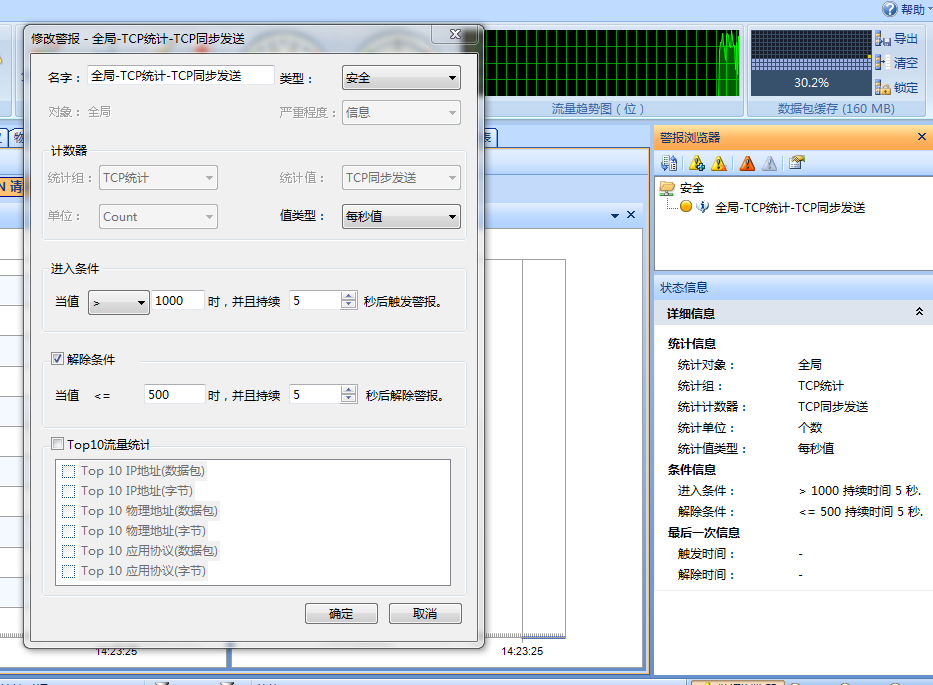
具体原理不再阐述，SYN Flood 攻击是一项比较容易实现 而且是比较难以防御的攻击。分析此种攻击前，我们先利用科来强大的图表自定义功能来设定自己的TCP参数，我指定了两个TCP请求监控表，如图：点击“我的图表”右上角的“新建面板”



我们选中TCP 同步发送，和TCP同步确认发送两个选项



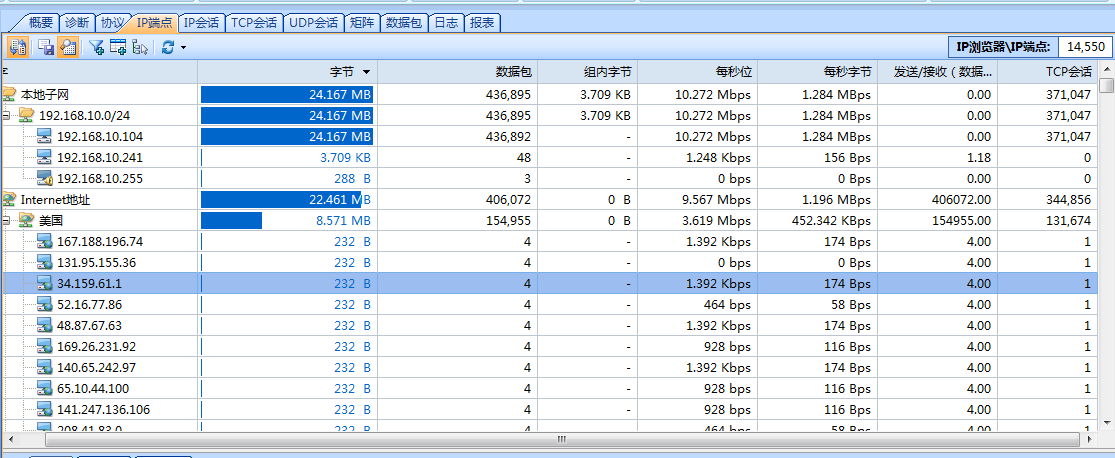
针对 SYN flood 我们还可以利用科来的告警提示来进行预防，如图我们设置告警：



我们设定当TCP SYN 请求超过1000 并持续了5秒后发出警报，档TCP SYN 每秒钟个数少于500持续5秒后解除报警。

然后将以前的DDOS 攻击数据包导入进行分析。

首先我们在端点视图会发现被攻击的端点的接受和发送数据包比例失调。接受大量数据包，但发送较少。而且流量较大，TCP会话很多。如图：

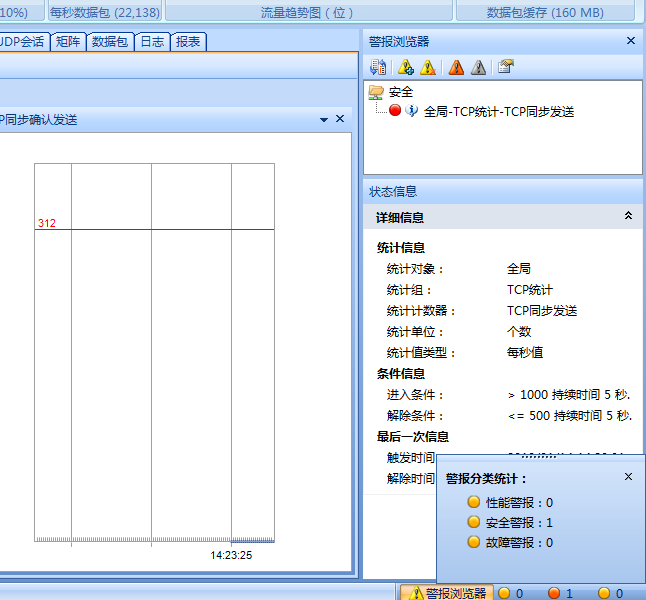


我们在图表中可以很直观的看到TCP同步和TCP同步确认的数据包。如图：

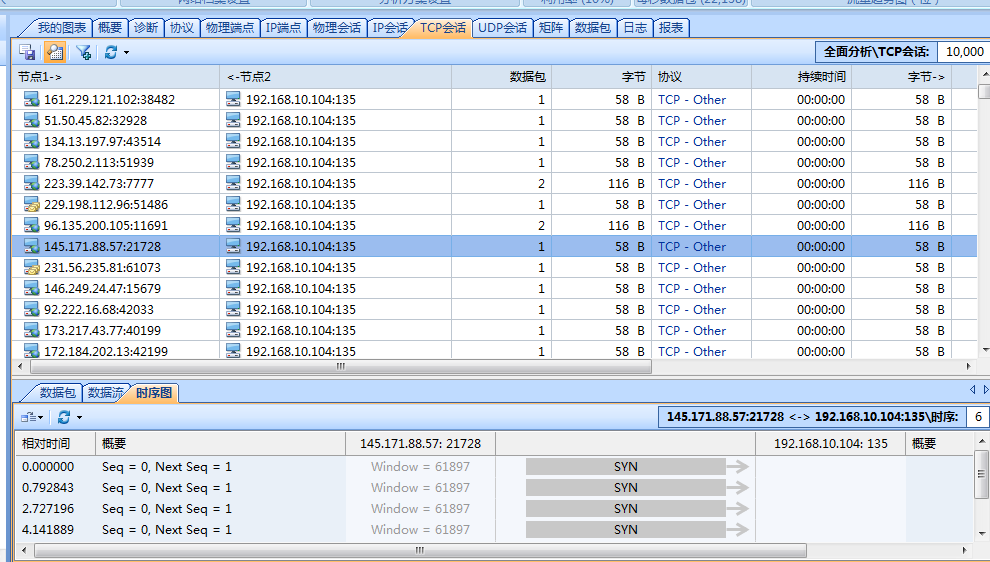


我们看到针对被攻击主机每秒的 SYN 请求接近20000个，而TCP 同步确认却几乎为0。

设置的TCP SYN 警报也已经产生告警 如图：

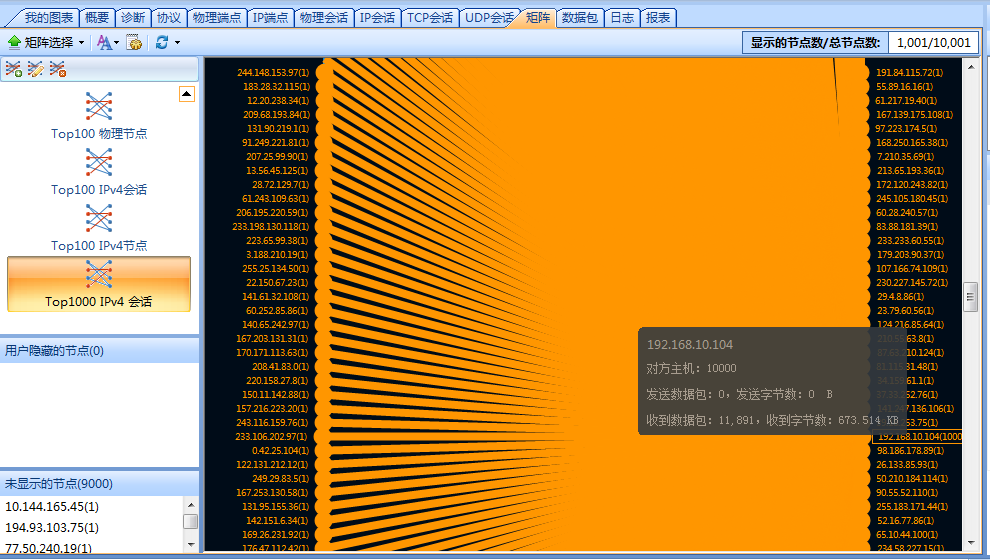


而通过其他传统的一些功能也能很清楚的了解网络中的SYN flood 攻击。我们可以查看TCP会话，如图：



我们看到 大量的互联网主机利用不同的端口在向192.168.10.104的135端口进行同步请求，TCP会话数在段几秒内到达几万。

增强型的矩阵视图也直观显示了针对被攻击主机的通信连接情况：远端主机超过10000，只接受收据包，没有发送。



数据包视图利用“解码字段”选项可以直观看到TCP SYN 值为1的数据包占了网络数据包的绝大部分如图：



通过以上丰富的图表和不同的界面的展现，我们就可以很快的了解是哪种DDOS攻击，从而采取应对的措施，减少损失。

防范SYN flood 攻击可以做以下几点措施：

边界路由过滤 RFC1918规定的一些不能在公网传输的私网地址段。

缩短路由器或FW上的SYN 超时时间，以及使用SYN代理技术

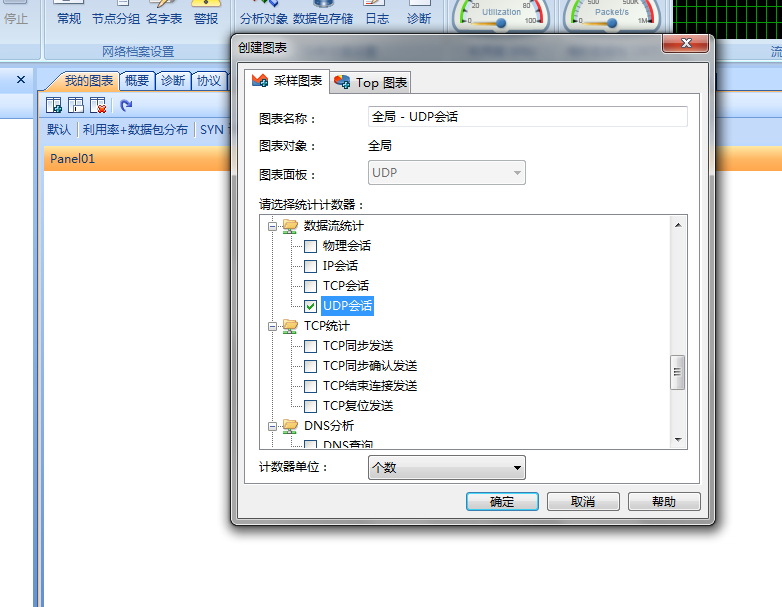
加固服务器TCP/IP的协议栈。增加最大半连接数，缩短SYN 超时时间，使用SYN cookies 技术等

使用防DDOS攻击的硬件设备或模块。

###### UDP flood

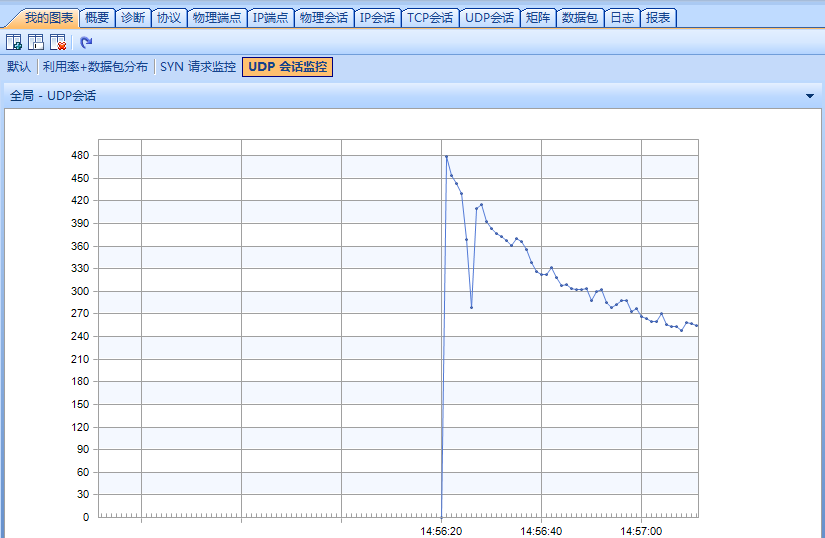
UDP Flood 是一种混合攻击，即能快速的消耗网络带宽，也可以消耗系统资源。

分析UDP flood 攻击之前我们可以利用图表功能设置对UDP会话的监控，如图：

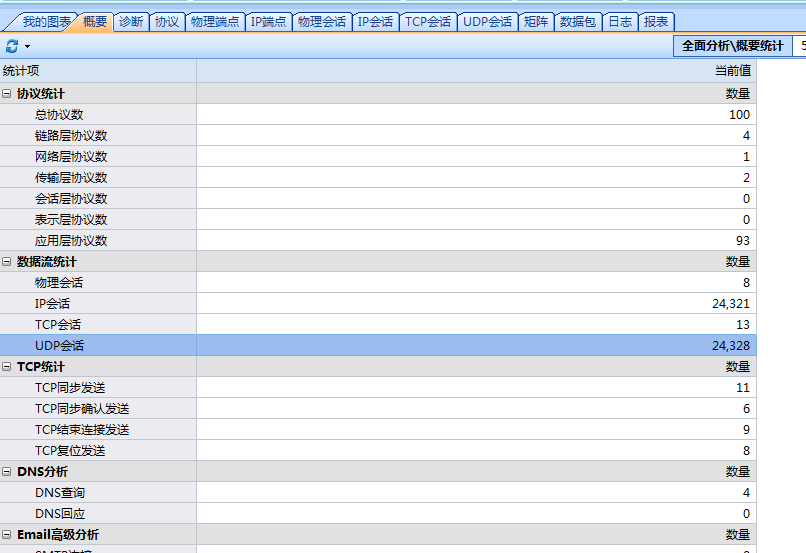


我们做好设置后，将UDP flood 数据包导入，进行分析。

首先我们在图表视图中看到UDP 会话的情况如图：



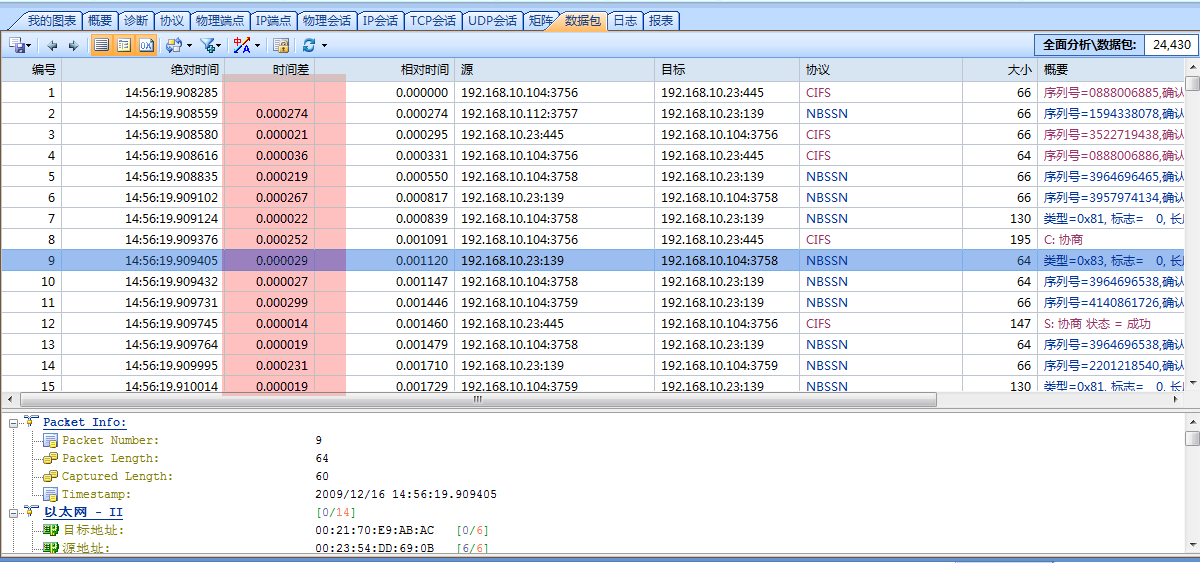
UDP 每秒钟会话数超过300，峰值能到480个，而服务器并未提供UDP服务。统计视图也可以看到UDP 会话数在40秒内就产生了24328个UDP会话，如图：



查看UDP 会话我们发现，大量的互联网随机IP 在向192.168.10.104的不同UDP端口进行访问。如图：



在数据包视图中我们可以看到 时间间隔很短的时间内发送大量的UDP 数据包。如图：



针对UDP flood 的攻击防护可以从以下几点来做：

增大网络带宽和服务器性能

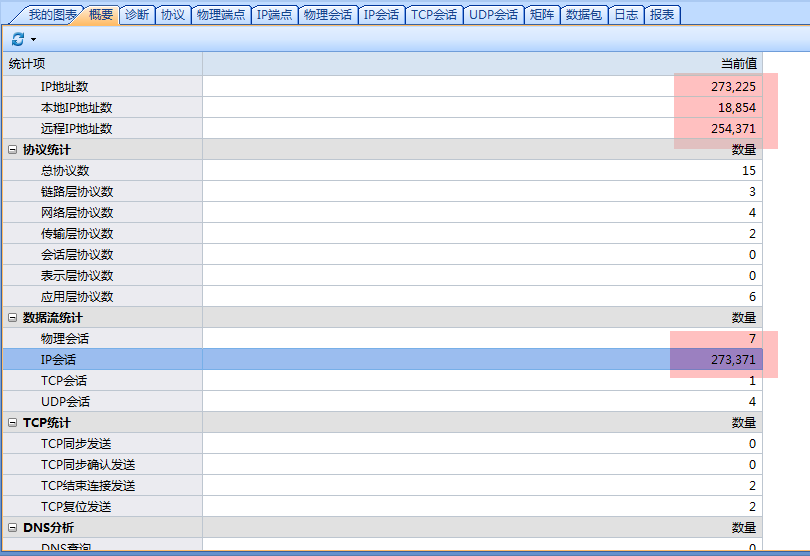
路由器和防火墙设置UDP会话限制。

利用SP的一些类似源地址过滤手段来丢弃没有回传路由的UDP请求。

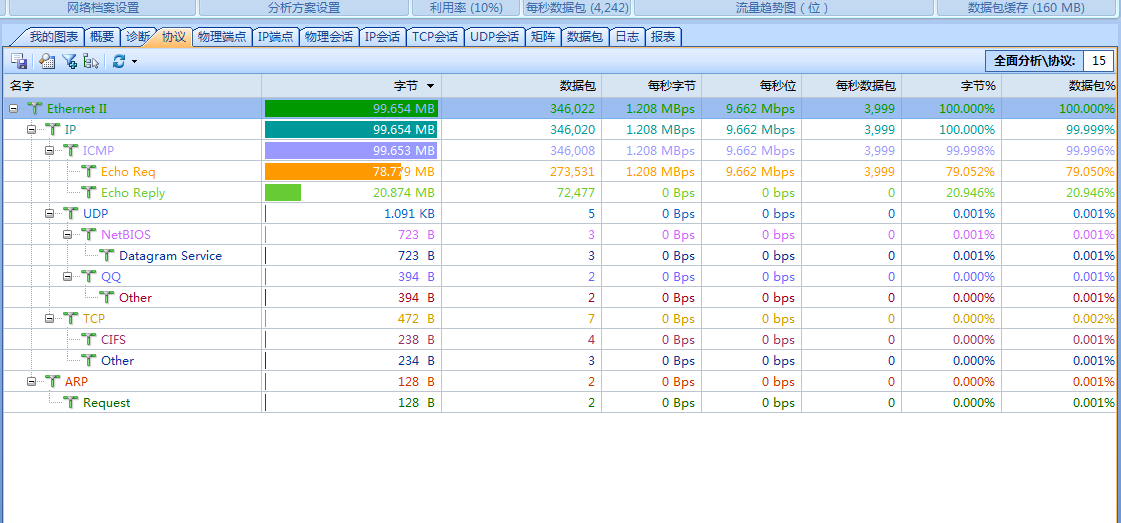
###### ICMP flood

ICMP flood 攻击主机发起大量的ICMP echo 来堵塞网络，淹没正常服务请求的一种攻击，主要是针对网络带宽进行攻击。

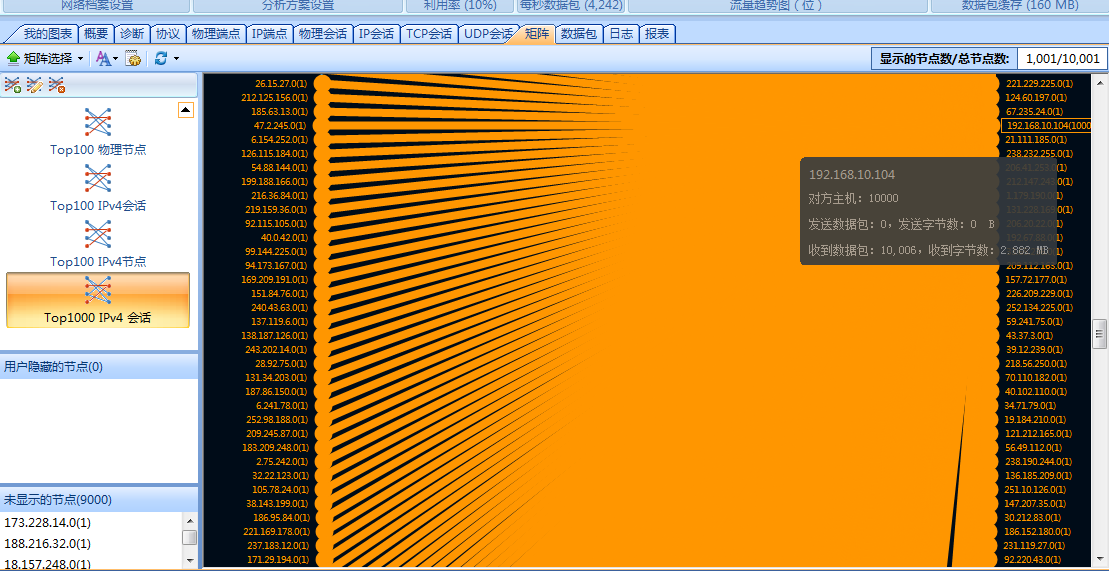
这种DDOS的特征比较明显，通过抓取攻击数据包可以很直观的了解其攻击现象，如图：首先我们可以看到概要视图中的IP会话数很多，远远超出TCP和UDP会话。



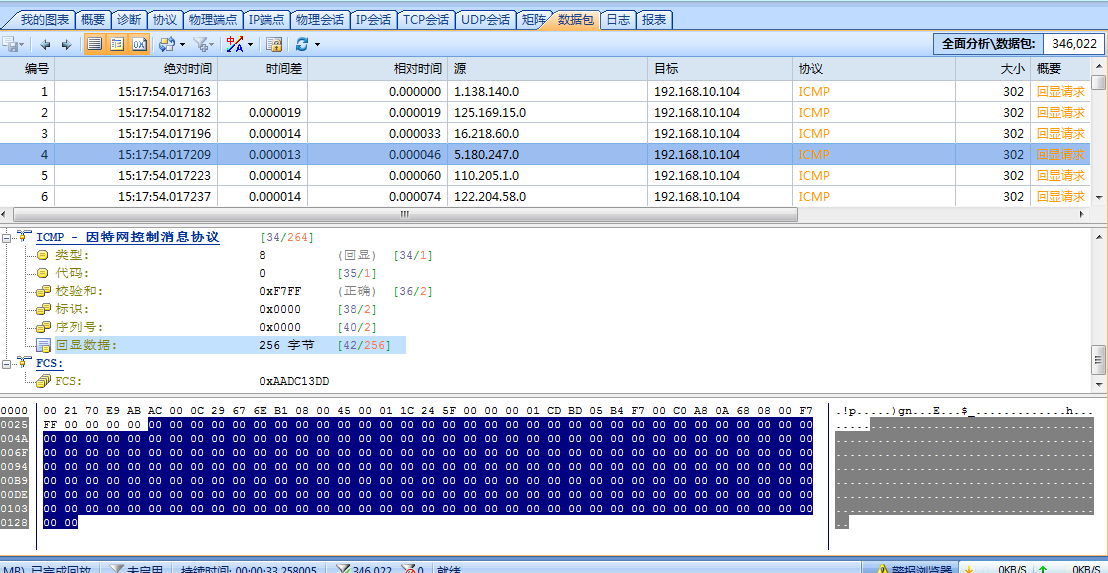
协议视图里我们看到ICMP echo 的协议流量过大，而echo replay 很少，比例失衡如图：



矩阵视图中 我们看到 被攻击IP的与上万（矩阵中对方主机默认最多10000,）IP进行通信。被攻击主机只有接受无发送。



数据包视图中我们看到大量的ICMP 数据包，而且有很明显的伪造填充和伪造现象，如图:

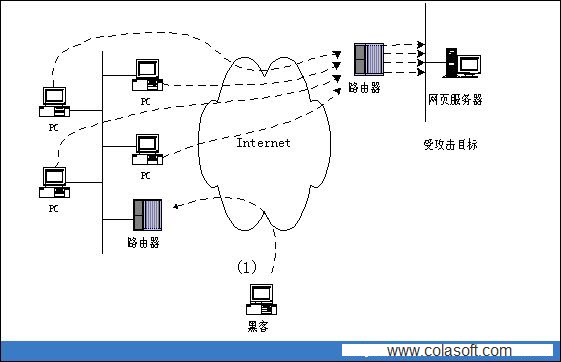


通过这几个简单的试图我们可以迅速的了解网络中发生的ICMP DDOS攻击。

ICMP DDOS的防御较为简单，可以在边界路由器或防火墙和服务器上面禁止使用ICMP协议。

###### Smurf 攻击

Smurf 攻击是一种设计很巧妙的DOS攻击，利用一些网络设备的配置或本身的一些漏洞进行杠杆式的DOS攻击，1台发起者就能产生数倍的流量，相当于流量放大器。攻击原理如下图：



该攻击向一个子网的广播地址发一个带有特定请求(如ICMP回应请求)的包，并且将源地址伪装成想要攻击的主机地址。子网上所有主机都回应广播包请求而向被攻击主机发包，使该主机受到攻击。子网内有多少台主机，流量就会被扩大几倍。

Smurf攻击中最明显的也是 ICMP 协议占了网络流量很大比例，而且源地址是多是子网IP。Smurf攻击防范也很简单，在子网路由器上面关闭对广播地址的ICMP转发。