**NBOS系统功能简介**

NBOS系统（Network Behavior Observation System—NBOS）是一个使用B/S结构的、以流记录(Netflow等)为分析数据源的、精细化的网络运行管理和安全监测系统 。NBOS安装在网络的边界处，实时地提供面向不同时空粒度的网络运行状态和安全监测数据。NBOS的原型系统来自于一个国家科技支撑计划项目。在随后的CERNET主干网的升级过程中，重新设计和开发的NBOS\_S于2013年8-12月在CERNET的全部38个主节点成功安装，并一直正常稳定地运行到现在。在此过程中NBOS\_S有过2次全面升级，目前的版本是3.0。图1是正在运行的NBOS\_S3.0版南京主节点的首页。



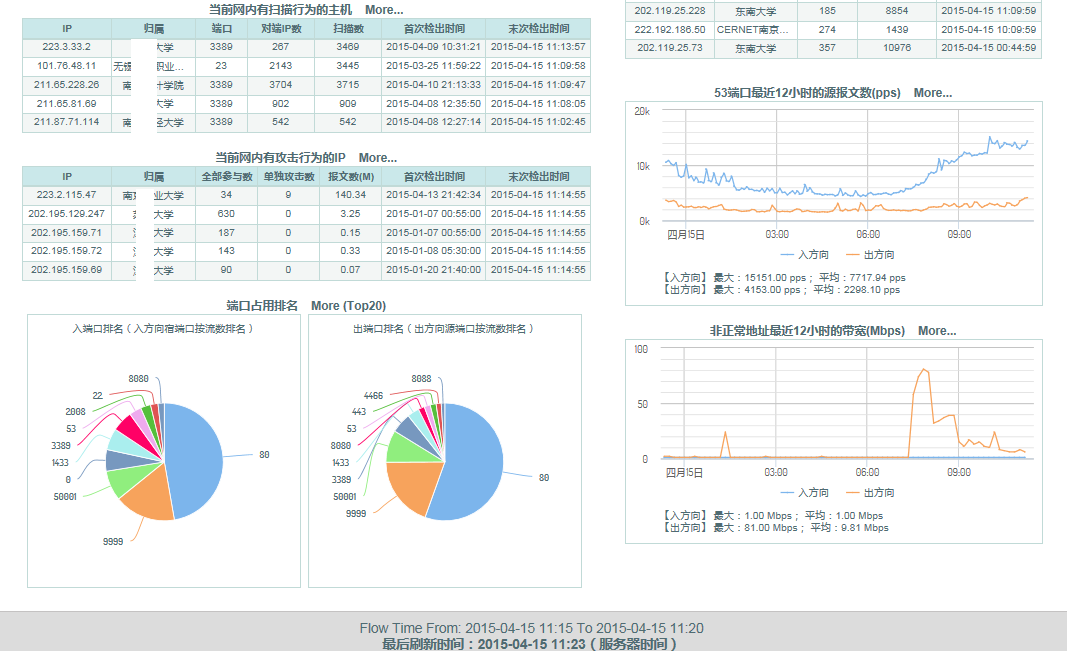


图1 NBOS（南京）驻地系统首页

CERNET南京主节点接入江苏境内的超过100个的高校和机构，覆盖6000个左右的C类地址空间。目前边界网络设备是华为公司的NE40路由器，它提供的NetstreamV9是NBOS的分析数据源。

NBOS\_S还是一个轻便高效的系统。在所有的CERNET主节点，NBOS均运行在一台双Intel CPU（E5-2609 0 @ 2.40GHz）+4G内存的普通刀片服务器上，在正常的情况下，可以处理1000万条左右的原始流记录/时间粒度（5分钟）。

下面分安全监测和网络管理2个方面分别简单地介绍一下它的主要功能。

### 安全监测方面

##### 一 DDOS攻击检测

这是NBOS最具特色的功能。目前可以检测出SYNFlood、TCP/UDPFlood、DNSFlood和反射式DDOS一共4种类型的攻击。对反射式攻击能准确地定位网内有攻击行为的主机。 对其它类型的部分攻击可以定位僵尸主机，并给出其参与攻击的情况。具体实例参见图2-图5。由于检测具有实时性，NBOS提供的这些信息有助于其他设备（如支持SDN的设备）对攻击流量进行过滤。通过对僵尸主机的跟踪，可以发现控制器，这是我们目前正在进行的研究工作。



图2 NBOS的DDOS检测主页面

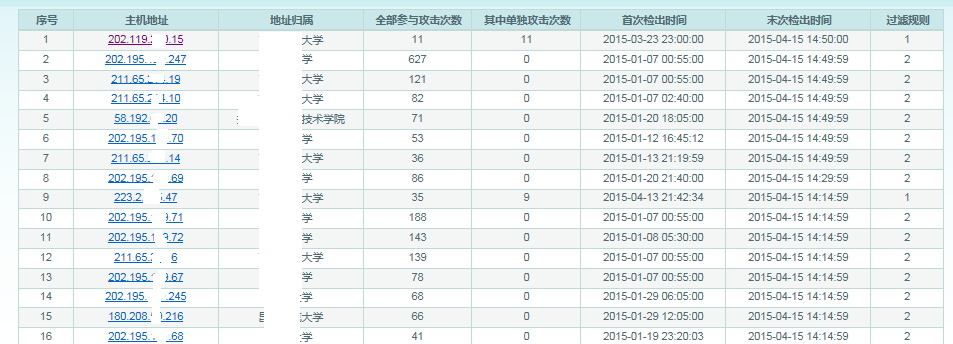


图3 参与攻击的网内主机情况



图4 网内僵尸主机202.119.\*.15参与攻击的情况



图5 反射攻击检测页面

##### 二 扫描检测

NBOS的扫描检测功能既可以观测到网外主机对网内主机危险端口的扫描现象，也可以发现网内主机的扫描行为，这些有扫描行为的网内IP，都是存在后门、且被安装了僵尸进程的主机。图6给出了NBOS观测到的网外主机对网内主机3389端口的扫描现象。图7是网内有扫描行为的主机的检测结果



图6 网外（国内）主机扫描网内主机3389端口的情况



图7 网内有扫描行为主机的检测结果

##### 三 网内WEB服务器安全检测

NBOS \_S在总控系统的支持下，有定位网内所有的WEB服务器，并对其流量进行监控并发现存在漏洞的功能。图8是这个功能的主页面，图9给出了图8中序号为53的202.119.\*.56主机的事件详情，图中的数据表明这台WEB服务器用3389和3306等危险端口与网外主机进行交互，这是一个典型的安全漏洞。图9是202.119.\*.56的首页。



图8 NBOS的WEB服务器异常检测主页面



图9 WEB服务器202.119.\*.56的异常检测详情



图10 WEB服务器202.119.\*.56的首页

### 网络管理方面

##### 一 精细化的占用带宽统计

带宽统计是最常规的网络管理功能，常规的SNMP网管只能提供面向链路的带宽占用情况， NBOS可以：

**1）分类显示带宽占用情况。**可以分别提供全网或网内的任何一个单位到教育网、国内其他运营商或国际的带宽占用情况，如图11所示。这是其他类型的网管所不能做到的。

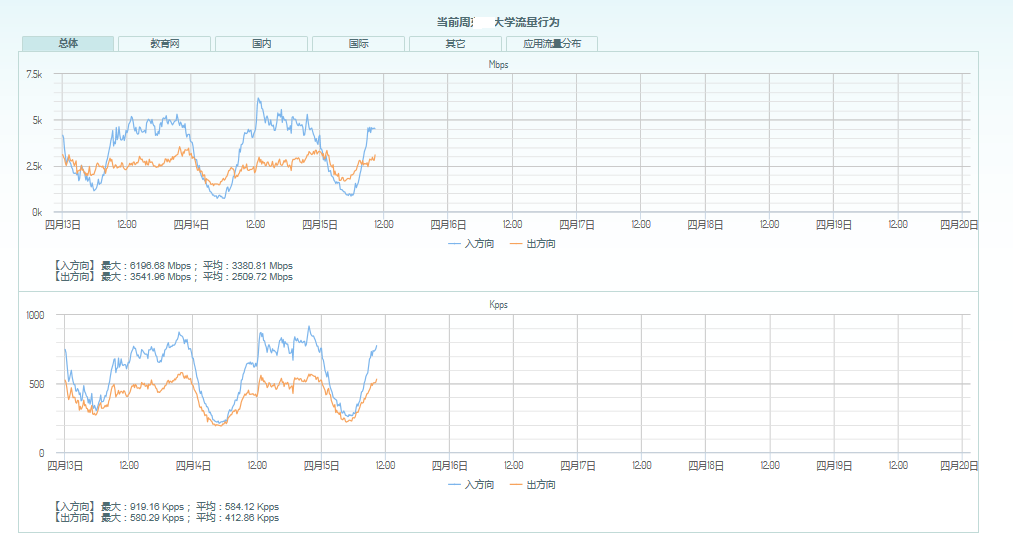


图11 NBOS可以对占用带宽情况进行分类显示

**2）流量中端口的占用带宽的情况**

实时的情况在首页中显示，参见图1(饼图)。历史情况有专门的查询页面。

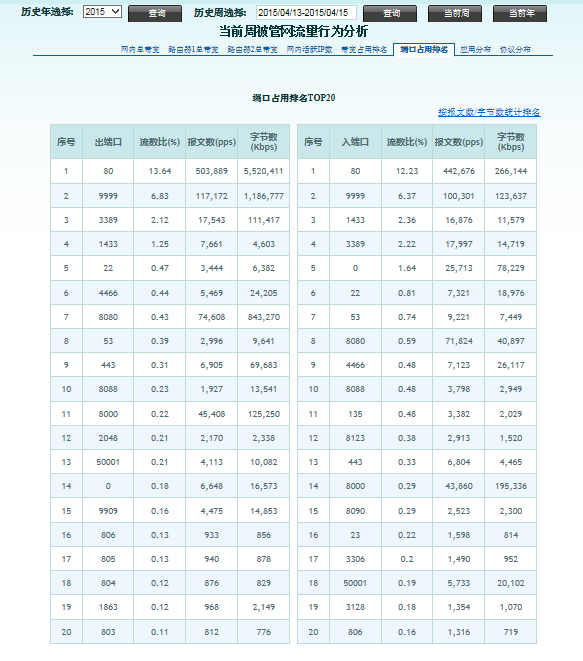


图12 按周统计带宽占用TOP20的端口

**3） 网内单位的带宽占用的排名情况**

当前情况在首页中，如图1，历史情况可按周查询

**4）单个IP的流量行为追踪。**

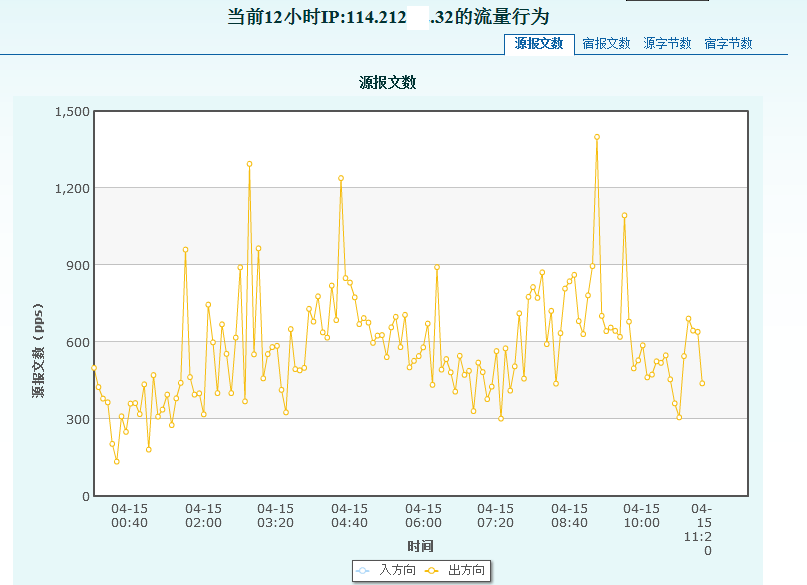


图13 IP114.212.\*.32当前12小时的流量情况



图14 该IP使用端口情况

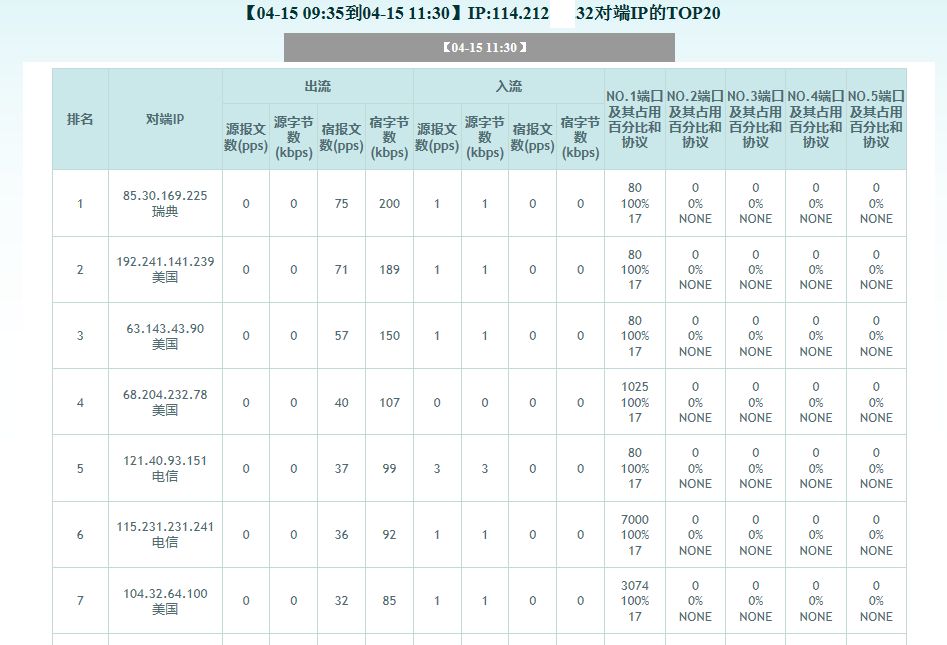


图15 该IP交互的对端情况

**5）端口流量行为追踪**

可以给出使用特定端口的IP和对端的情况

**6）网内单位流量行为监测**

可以给出网内特定单位最活跃的IP、端口以及交互的网外主机的地址情况

##### 二 流量热点数据

NBOS这部分的功能可以给出当前和以往网络中按流量、访问、端口和地址对等角度统计的热点数据。其中最具特点的是热点事件的检测，它可以检测出汇聚后的流量，图16是这个功能的主页面， 其中序号为12的事件表明网内有49台主机，同时向美国主机[54.240.227.0](http://202.112.25.167/NBOS_s/event2001_num_detail_select.php?selectip=54.240.227.0)（属于亚马逊公司数据中心）的443端口发送数据，这是HTTPS使用的端口，5分钟内的流量总和为638.9MB 。NBOS还可以进一步给出这个事件的详情，如图17所示，包括这49台主机的地址、归属和各自发送的流量等。



图16 NBOS检测出的到境外的大流量事件



图17 上图序号为12的事件中向美国主机[54.240.227.0](http://202.112.25.167/NBOS_s/event2001_num_detail_select.php?selectip=54.240.227.0)发送数据的网内主机