网络安全保障

龚俭
东南大学计算机科学与工程学院
CERNET华东北地区网络中心
2017.5.5

安全威胁

- 给数据、系统、网络和内容的可用性带来负面影响的活动
- 故障
  - 由于硬件或软件问题引起的持续性系统和服务失效
- 意外
  - 由系统运行或环境所引起的临时性系统失效或服务降级
- 攻击
  - 攻击者发起的有意图的敌意活动

什么是网络安全保障

- 评估安全质量要考虑安全机制和保障机制两个方面
  - 安全机制决定安全水平
  - 保障机制决定安全机制的落实程度
- 校园网的安全管理
  - 安全策略规划
  - 基础设施建设
  - 网络安全保障：策略落实与设施使用

网络安全保障的目标

- 维护可用性
  - 基础设施的可用性
  - 服务的可用性
- 消除威胁
  - 基础设施与应用服务的安全性维护
  - 数据安全与隐私保护

网络安全保障的对象

- 直接责任对象
  - 校园网主干网设备
  - 网络中心的网络和服务器设备
  - *学校应用系统的服务器集群*
  - *学校级的应用系统*

- 间接责任对象
  - 学校下属单位的网络、服务器与应用系统

网络安全保障的内容

- 维持系统安全性
  - 漏洞修补与入侵检测
- 维持服务可用性
  - 故障监测、技术支持
- 维持数据安全性
  - （网络、主机、应用系统的）访问控制、安全审计、备份维护、篡改检测
- 感知安全态势
  - 网络管理、系统管理、安全监测
- 实施应急响应
  - 应急响应机制、应急响应设施、应急响应队伍

网络安全保障的形式

- 日常管理（根据安全策略落实责任）
  - 设施：检测、拦截、响应、加固
  - 队伍：管理、响应
- 威胁监测
  - 漏洞扫描、入侵检测、应用审计
- 应急响应
  - 阻断、清除、恢复、协同

CERNET华东北地区网络中心

- 直接责任对象
  - CERNET主干网接入设备
  - CERNET主干网运行管理与安全保障系统（部分）
  - 网络中心网络运行管理系统和安全保障系统
  - 江苏省计算机网络技术重点实验室
- 间接责任对象
  - 江苏省各入网单位

我们的网络安全保障目标

- 服务安全性
  - 邮件服务器和DNS服务器正常工作
  - 网管和网络安全保障系统正常工作，监测数据正常获取；
  - 重点实验室基础设施正常工作；
- 系统安全性
  - 网络中心内部所有的服务器系统没有漏洞和入侵；
- 数据安全性
  - 科研数据的访问控制；
  - 网站内容维护；
- 主干网安全保障
  - 主干网安全检测；
  - DDoS防御和僵尸网络追踪。

工作内容

- 维持系统安全性
  - 漏洞扫描、漏洞修补、入侵检测（HIDS）
- 维持服务可用性
  - 故障监测、DDoS监测、异常通信行为检测、异常路由检测
- 维持数据安全性
  - （网络、主机、应用系统的）访问控制、日志审计、备份维护、篡改检测
- 感知安全态势
  - 僵尸网络控制器监测、服务器发现、DDoS态势感知
- 实施应急响应
  - DDoS拦截、恶意活动跟踪与取证、NJCERT

设施建设

- 巡风系统-内部漏洞扫描
- 故障监测集成系统
- 网络安全保障系统
  - NBOS-网络行为观测与态势感知系统
  - Hydra/Monster-攻击阻断与样本/元数据采集系统
  - Chairs-分布式应急响应协同系统
  - IPCIS-IP综合信息平台与网络安全态势感知

巡风系统

- 由同程安全应急响应中心 (YSRC)在GitHub上开源的安全工具，采用Python编写。它在企业内网中使用指定漏洞插件巡航扫描系统，可通过扫描结果的搜索功能了解内部网络资产分布情况和漏洞检测结果。
  - 网络资产识别引擎会通过用户配置的IP范围定期自动地进行端口探测（支持调用MASSCAN），并进行指纹识别。
  - 漏洞检测引擎会根据用户指定的任务规则进行定期或者一次性的漏洞检测。

扫描统计结果


巡风
退出
搜索
任务
插件
统计
配置
148
收集记录总数
86
IP总数
负载：0%
扫描引擎
爬虫引擎
54
任务总数
54
插件总数
漏洞分类
总数：24
弱口令
14
网络资产信息变化
200
150
100
50
0
2017-03-02
2017-03-05
2017-03-08
2017-03-11
2017-03-14
2017-03-17
2017-03-20
2017-03-23
2017-03-26
2017-03-29
服务数量统计
服务类型
Web服务类型
20
15
10
5
0
ssh
telnet
mysql
mongodb
netbios
ftp
smb
rsync
mssql
rdp
pop3
smtp

插件检测结果

结果为累计数


巡风
搜索
任务
插件
统计
配置
当前页全选
当前页反选
结果集全选
结果集总数:2
.193.177:21
ftp
2017-03-21 10:39:10
Banner: 220 Welcome to the ftp service
.193.171:21
ftp
2017-03-21 10:39:10
Banner: 220 0G-9354 Network Management Card AOS v3.7.3 FTP server ready.


巡风
搜索
任务
插件
统计
配置
FTP弱口令 数量:1
2017-03-21
193.177:21
存在弱口令，账号：ftp，密码：123456

编号	节点名称	检测时间	检测IP总数	web服务器数	1类IP	2类IP	3类IP	4类IP	5类IP	6类IP	7类IP
1	清华大学	2017-04-24	356484	198598	7	142703	13725	37101	5062	3168	36523
2	天津大学	2017-04-19	34615	2592	0	1540	562	455	35	250	25515
3	河北师范	2017-04-20	21449	898	0	507	162	218	11	36	18297
4	太原理工	2017-04-20	14365	1108	0	577	264	248	19	52	10482
5	内蒙大学	2017-04-21	85696	334	0	199	60	66	9	71863	12523
6	东北大学	2017-04-19	23322	1610	0	782	219	588	21	923	15403
7	大连理工	2017-04-19	34638	5229	0	703	4282	230	14	86	26986
8	哈工大	2017-04-18	19227	864	0	495	196	138	35	157	15301
9	吉林大学	2017-04-20	11071	1496	0	919	239	302	36	145	6236
10	东南大学	2017-04-19	92626	14331	0	4575	7612	1985	159	1413	56906
11	山东大学	2017-04-19	56238	7409	0	2660	3253	1431	65	496	30707
12	青岛海洋	2017-04-18	213151	104654	4	71899	8141	21881	2729	1128	34049
15	浙江大学	2017-04-22	820004	526598	12	406058	28385	80827	11316	3929	46519
37	北京大学	2017-04-21	24010	2350	0	1249	476	586	39	156	13336
38	北京邮电	2017-04-21	32999	7380	0	3893	1652	1632	203	914	5201
合计			2721252	1081548	32	745003	115227	195340	25946	138292	784405

1类IP – 临时响应；

2类IP – 成功响应；

3类IP – 重定向；

4类IP – 客户端错误（网页不存在或要求认证）；

5类IP – 服务器错误；

6类IP – 响应TCP请求，但不响应HTTP请求；

7类IP – 不响应TCP请求和HTTP请求。

编号	节点名称	检测时间	检测IP总数	dns服务器数	可递归DNS	1类IP	2类IP	3类IP	4类IP	5类IP	6类IP
1	清华大学	2017-04-09	7209	1041	772	332	440	190	79	17	400
2	天津大学	2017-04-09	2298	206	157	59	98	41	8	9	1112
3	河北师范	2017-04-09	3708	67	24	14	10	32	11	4	3244
4	太原理工	2017-04-09	616	65	42	26	16	12	11	3	127
5	内蒙大学	2017-04-09	360	25	12	6	6	12	1	54	149
6	东北大学	2017-04-09	6900	6206	6177	24	6153	22	7	1	364
7	大连理工	2017-04-09	9176	8308	8225	17	8208	81	2	1	505
8	哈工大	2017-04-09	549	78	55	19	36	21	2	2	115
9	吉林大学	2017-04-09	1715	89	58	38	20	26	5	4	1061
10	东南大学	2017-04-09	5763	481	297	158	139	156	28	16	2432
11	山东大学	2017-04-09	2808	262	181	86	95	75	6	7	922
12	青岛海洋	2017-04-09	3255	1033	678	109	569	58	297	8	509
19	华中科技	2017-04-09	22367	193	111	44	67	59	23	4	20898
37	北京大学	2017-04-09	2814	699	139	83	56	551	9	3	675
38	北京邮电	2017-04-09	3482	1182	1038	149	889	117	27	461	268
合计			134130	34945	26864	3174	23690	2740	5851	854	49119

1类IP – 支持递归查询，支持TCP连接；

2类IP –支持递归查询，不支持TCP连接；

3类IP –不支持递归查询，支持TCP连接；

4类IP –不支持递归查询，不支持TCP连接；

5类IP –支持TCP连接，非DNS服务器；

6类IP – 不支持TCP连接，非DNS服务器。

编号	节点名称	检测时间	检测IP总数	mail服务器数	1类IP	2类IP	3类IP	4类IP
1	清华大学	2017-04-09	4997	377	0	376	1	2452
2	天津大学	2017-04-09	6984	38	0	38	0	6717
3	河北师范	2017-04-09	4229	21	0	21	0	4062
4	太原理工	2017-04-09	2732	16	0	16	0	2606
5	内蒙大学	2017-04-09	48365	7	0	7	0	48334
6	东北大学	2017-04-09	2015	35	0	35	0	1770
7	大连理工	2017-04-09	3506	29	0	29	0	3330
8	哈工大	2017-04-09	1943	29	0	29	0	1748
9	吉林大学	2017-04-09	931	23	0	23	0	753
10	东南大学	2017-04-10	1697	158	0	158	0	10
11	山东大学	2017-04-09	7368	96	0	94	2	6658
12	青岛海洋	2017-04-09	3521	234	1	233	0	1677
13	中科大	2017-04-09	8501	81	0	81	0	7908
37	北京大学	2017-04-09	2297	104	0	103	1	1524
38	北京邮电	2017-04-09	2364	122	0	122	0	1536
合计			243953	3969	9	3935	25	215874

1类IP – 只支持SMTP的Mail服务器，且能正确响应HELO；

2类IP –支持SMTP和ESMTP的Mail服务器，且能正确响应HELO；

3类IP –只支持SMTP的Mail服务器，但不能正确响应HELO；

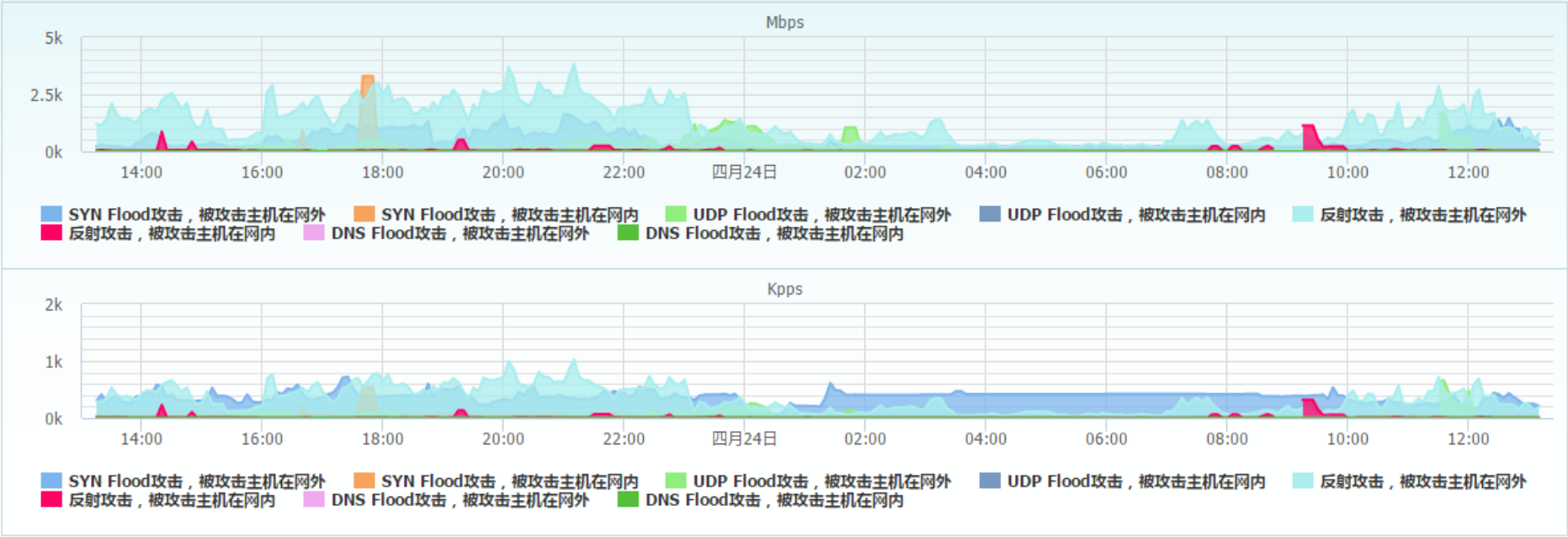
4类IP –非SMTP服务器。

网络行为观测系统

Network Behavior Observation System

首页 节点管理 热点分析 异常事件 DDoS攻击态势 IPDB 角色库维护 帮助

全网最近24小时DDoS流量



全网最近24小时对外DDoS攻击排名

被管网外攻击目标Top100 | 主节点参与攻击情况汇总 | 被管网内参与攻击Top100

排名	被攻击IP	归属	最大攻击强度(pps)	最大攻击强度(Kbps)	累计攻击报文数	累计攻击字节数	持续时间(秒)	网内攻击IP数	主节点参与攻击Top5	攻击类型
1	125.88.183.112	中国电信	216165	778488	1894476300	874697932800	15000	571	上海交大:31.65%， ...	反射攻击:100.0...
2	183.2.225.147	中国电信	250181	899408	1217711400	561030758400	70200	606	上海交大:31.48%， ...	反射攻击:100.0...
3	61.153.110.132	中国电信	133360	474912	1092669900	506479411200	20100	529	上海交大:36.71%， ...	反射攻击:100.0...
4	183.60.211.40	中国电信	150716	535008	1028148600	471673651200	78600	639	上海交大:32.13%， ...	反射攻击:100.0...
5	14.29.49.188	中国电信	195461	704808	990647700	458298163200	66600	597	上海交大:33.98%， ...	反射攻击:100.0...
6	116.211.143.119	中国电信	306660	168672	4998260400	394227609600	32400	972	广西大学:65.72%， ...	SYN Flood攻击...

网络行为观测系统

Network Behavior Observation System

2017.4.23的24小时统计

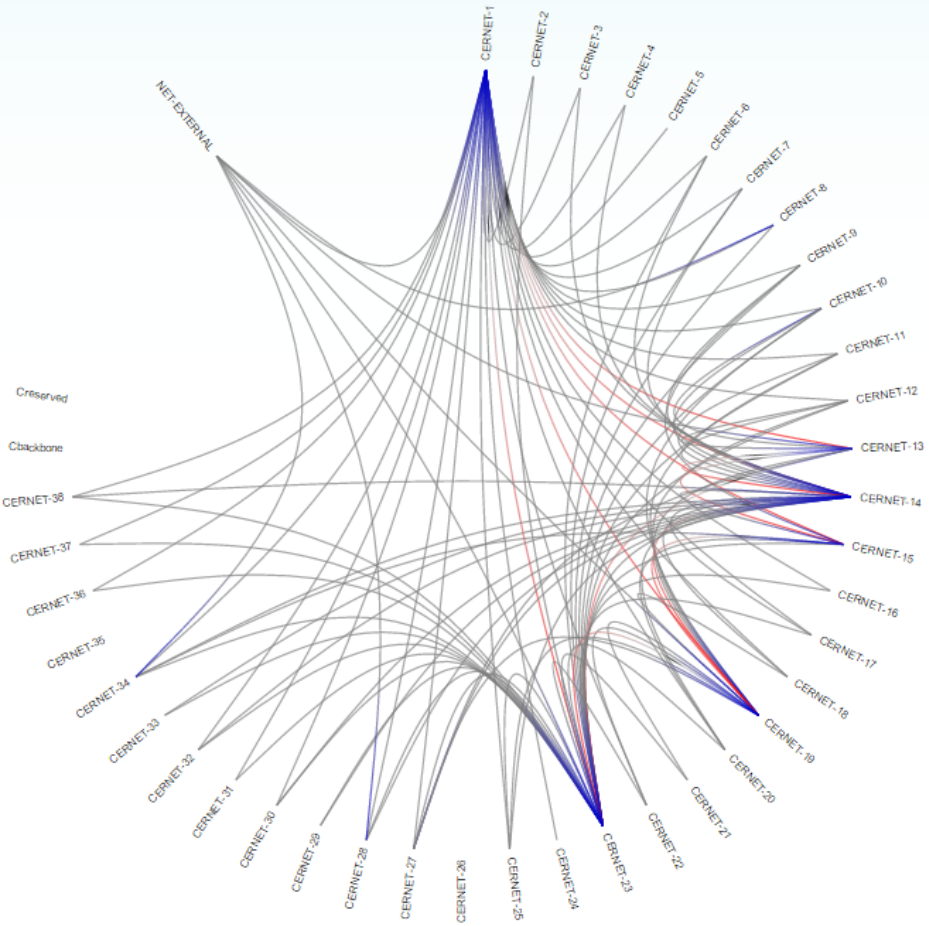
首页 节点管理 热点分析 异常事件 DDoS攻击态势 IPDB 角色库维护 帮助

未结束 24小时内 7天内 30天内 pkts: 10% 30% 50% 100% bytes: 10% 30% 50% 100%

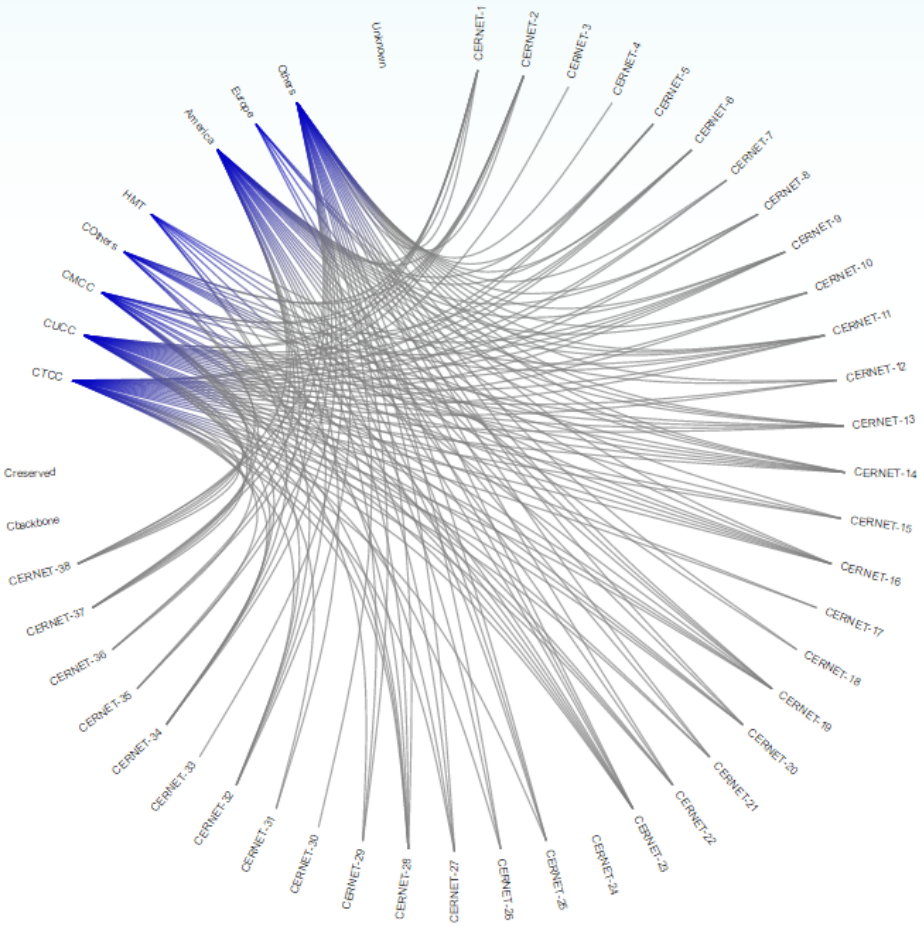
互相攻击，红/蓝长度-受到攻击总量的对比　　单向攻击，source(灰色)，target(蓝色)

网内受到攻击

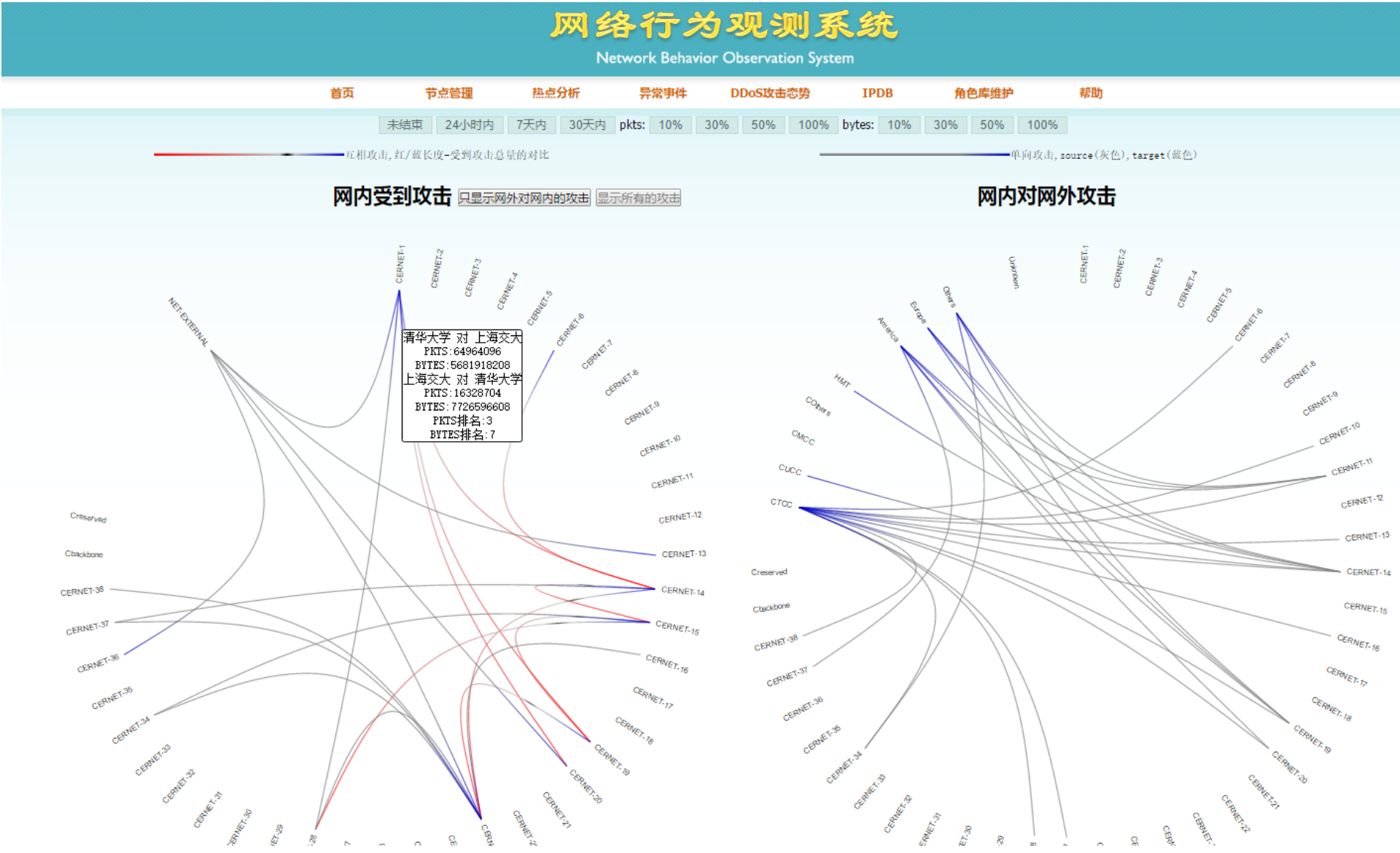
只显示网外对网内的攻击 显示所有的攻击



网内对网外攻击

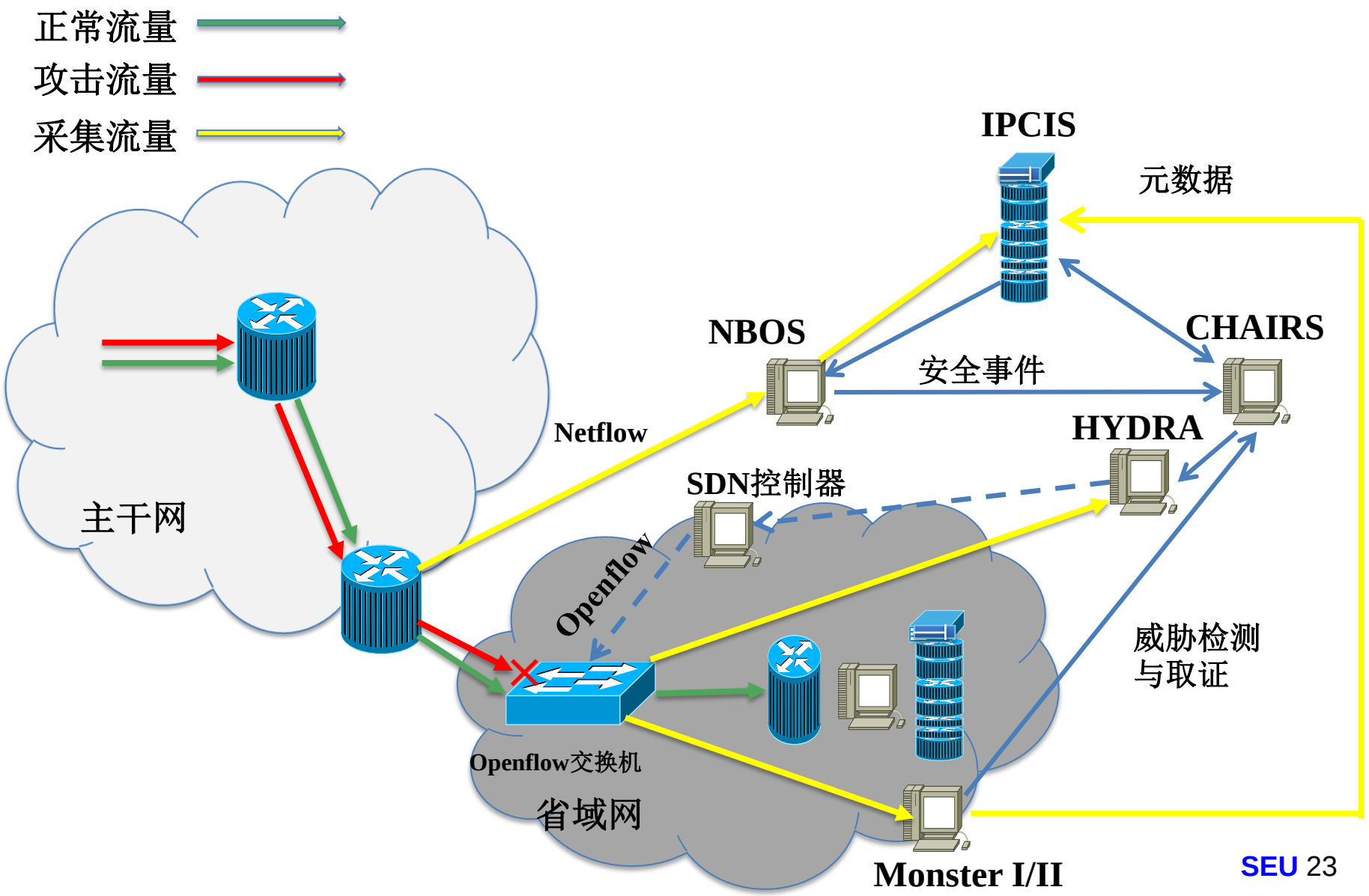


1-清华，13-合肥，14-上海，15-杭州，19-武汉，23-深圳



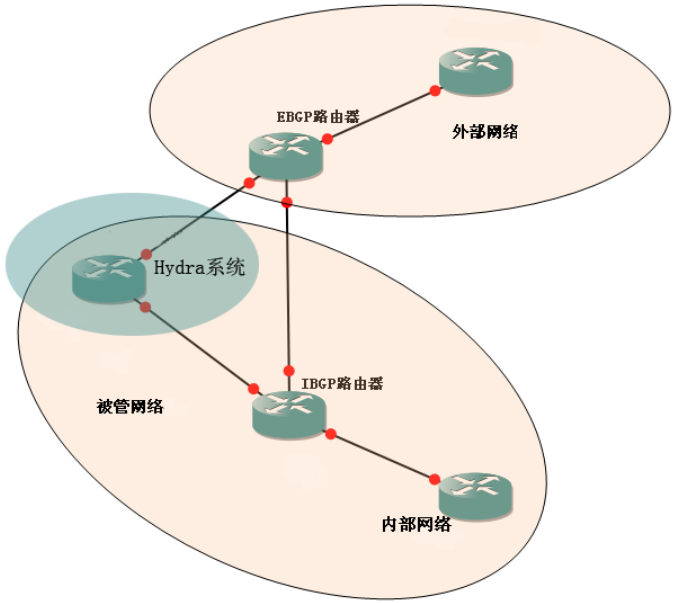
2017.4.24-2017.4.25：24小时之内前10%攻击强度的DDoS统计

网络安全保障系统总体架构

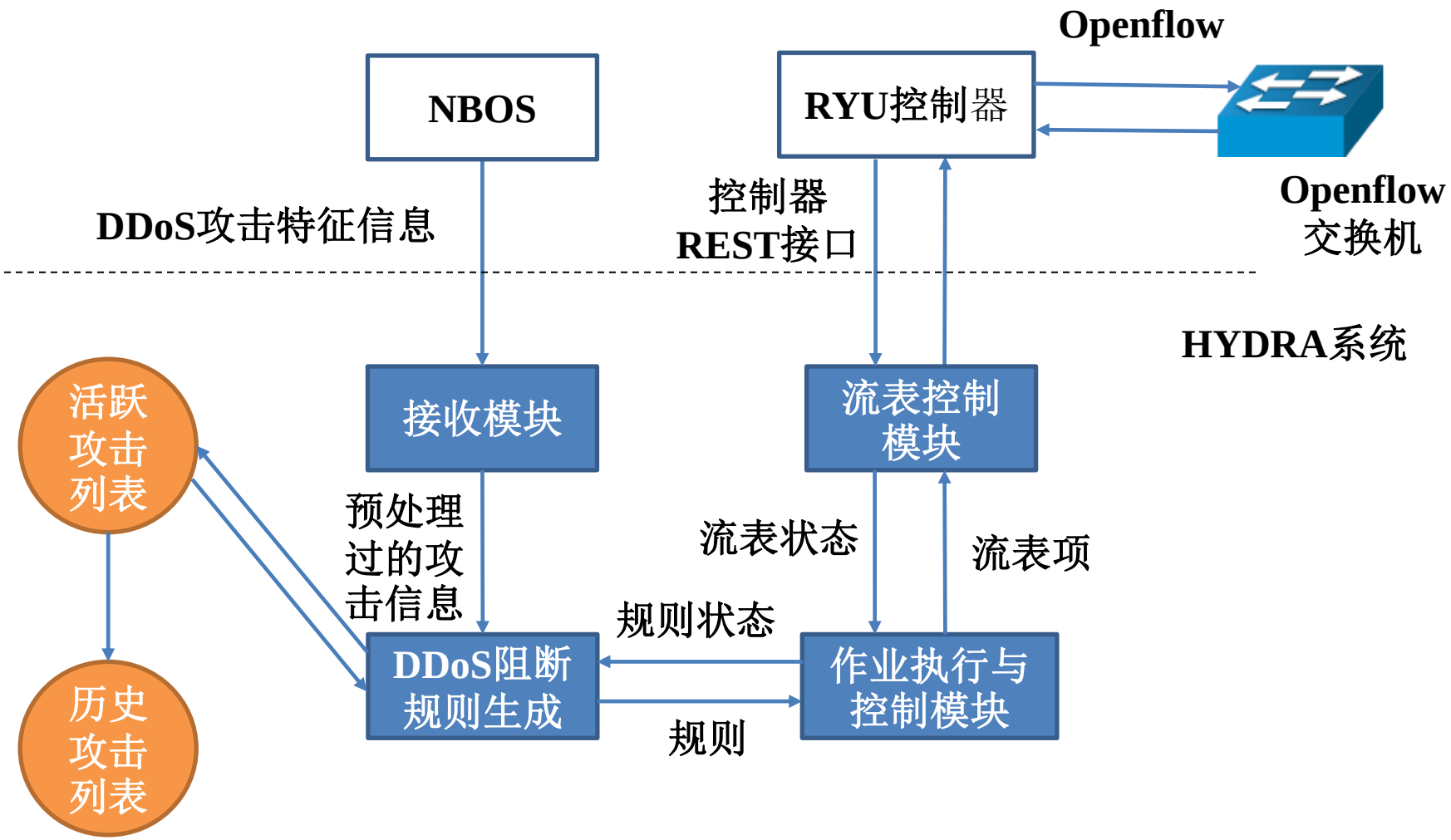


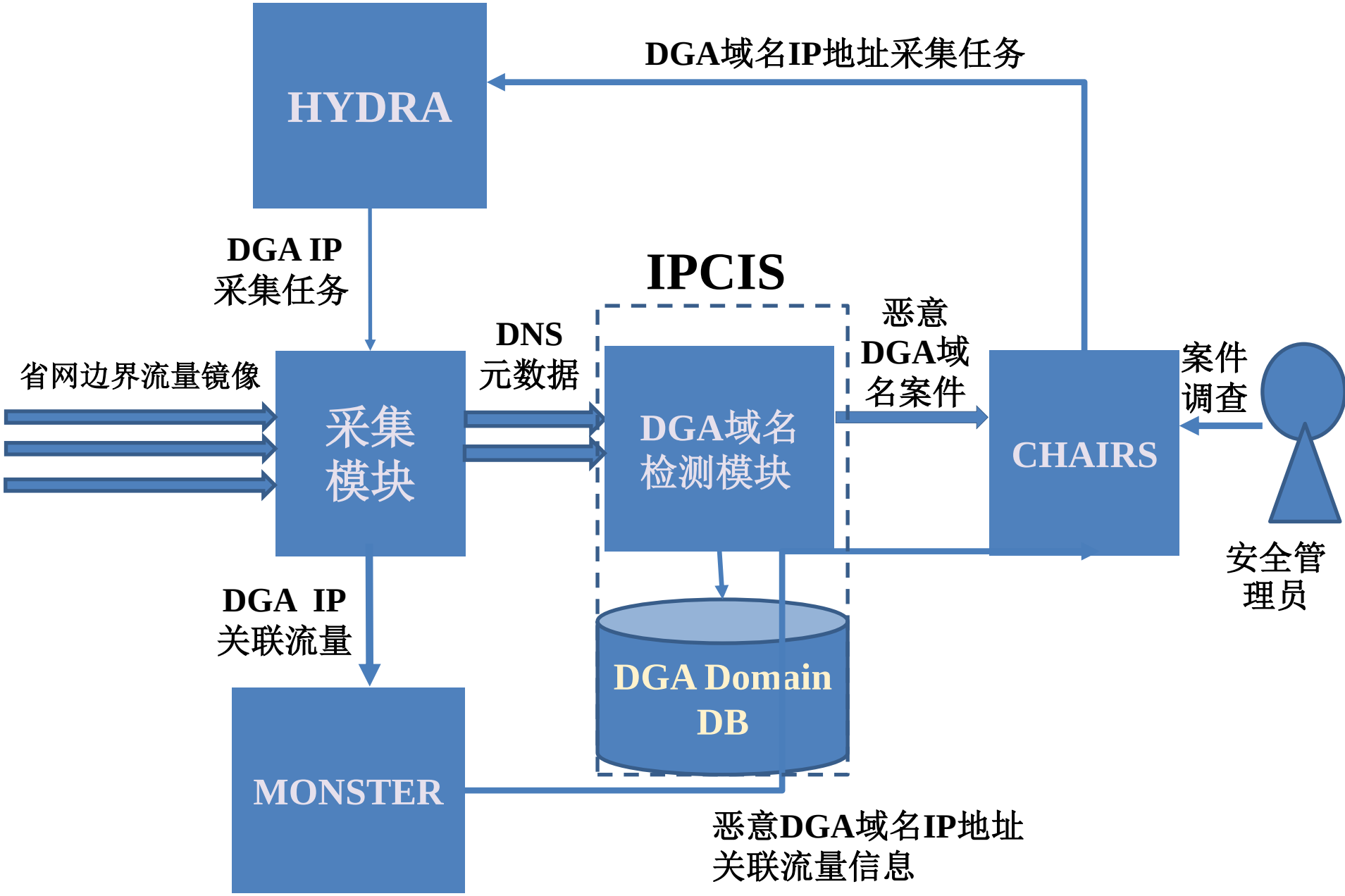
Hydra2.0系统

- **HYDRA1.0 (混合检测响应系统，HYbrid Detection Response Agent)系统是在国家科技支撑计划课题“新一代可信任互联网安全和网络服务”和211二期CERNET建设项目支持研制的网络安全事件应急响应系统。**
  - **Traffic diversion & Scrubbing**
  - **手工配置**
  - **GE环境**
- **Hydra2.0系统**
  - **基于SDN技术**
  - **Scrubbing & Intrusion detection & Sniffing**



DDoS防御控制模型


Openflow
NBOS
RYU控制器
DDoS攻击特征信息
控制器
REST接口
Openflow
交换机
HYDRA系统
活跃
攻击
列表
接收模块
流表控制
模块
预处理
过的攻
击信息
流表状态
流表项
规则状态
DDoS阻断
规则生成
作业执行与
控制模块
规则
历史
攻击
列表


HYDRA
DGA域名IP地址采集任务
DGA IP
采集任务
IPCIS
省网边界流量镜像
采集
模块
DNS
元数据
DGA域名
检测模块
恶意
DGA域
名案件
CHAIRS
案件
调查
安全管
理员
DGA IP
关联流量
DGA Domain
DB
MONSTER
恶意DGA域名IP地址
关联流量信息

混合检测响应系统

HYbrid Detection Response Agent

首页 作业管理 系统管理 响应管理 用户管理

作业列表

序号	作业名称	提交时间	类型	状态	操作
1	取证任务_-561	2017-03-22 00:18:06	自动响应	正在运行	
2	L1_DDoS响应_101.4.126.203	2017-03-21 22:26:34	自动响应	正在运行	
3	取证任务_-7558	2017-03-21 22:21:29	自动响应	正在运行	
4	取证任务_-9845	2017-03-21 21:43:23	自动响应	正在运行	
5	2017_3_21	2017-03-21 21:32:56	普通	停止	删除
6	取证任务_-1600	2017-03-21 21:21:33	自动响应	正在运行	
7	取证任务_-1644	2017-03-21 21:13:23	自动响应	正在运行	
8	取证任务_-2126	2017-03-21 21:05:22	自动响应	正在运行	
9	取证任务_-2952	2017-03-21 20:51:35	自动响应	正在运行	
10	L1_DDoS响应_101.4.126.203	2017-03-21 19:46:33	自动响应	正在运行	
11	取证任务_-7346	2017-03-21 19:38:21	自动响应	正在运行	
12	取证任务_-7356	2017-03-21 19:38:11	自动响应	正在运行	
13	取证任务_-7383	2017-03-21 19:37:44	自动响应	正在运行	
14	取证任务_-8006	2017-03-21 19:27:22	自动响应	正在运行	
15	L1_DDoS响应_101.4.126.203	2017-03-21 18:36:32	自动响应	正在运行	

Chairs的系统功能

- 案件的生命周期管理
  - 需要响应的安全事件定义为案件，并保存在案件库中。
  - 手工响应与自动响应结合
  - 案件的状态分为：正在跟踪、继续跟踪、误报、结束
  - 案件是响应过程记录和响应数据的综合数据组织
- 证据管理
  - 维护案件处理过程中收集到的各种数据证据
- 模板管理
  - 定义和维护响应模板

IP综合信息系统 IPCIS

首页 配置修改 进程监控 用户管理 日志查看 数据概况 使用手册 外部链接 返回登陆

当前域名数据库概况

非DGA域名概况

更新时间	非DGA二级域名总数	解析IP地址总数	DNS名字服务器总数	域名归属信息总数
2017-04-27 12:00:00	14,754,985	2,431,772	683,039	214,404

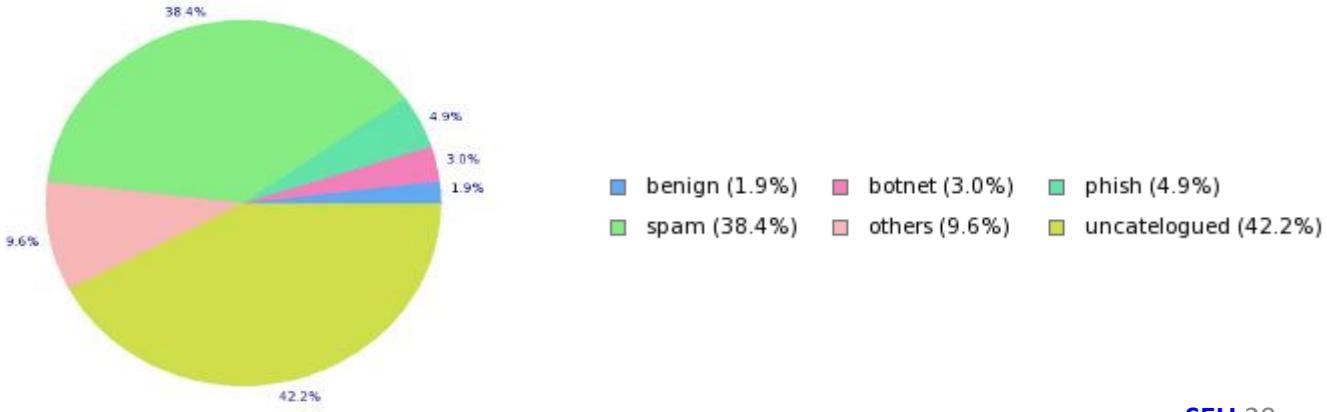
非DGA域名后缀分布概况

国家顶级域名数	通用顶级域名数	.cn下二级域名数	.edu.cn下三级域名数
213	22	601,489	7,530

DGA域名信息概况

当前活跃DGA二级域名总数	当前活跃DGA域名解析IP地址总数	当前活跃DGA域名DNS名字服务器总数
18,418	364,899	68,025

DGA二级域名服务类型信息概况



安全漏洞通告平台

- **ipdb.sec.edu-info.edu.cn**
- 发起人：网络信息安全工作组 (中国高等教育学会教育信息化分会)
- 管理
  - 学校的安全联系人：管理单位的域名、IP与联系人
  - 地区的联系人 (工作组 / 省厅)：管理该地区单位信息和单位联系人信息
- 应用
  - 对接工作组的其他系统
    - 漏洞报告平台 src.edu-info.edu.cn
    - 漏洞跟踪系统 vul.sec.edu-info.edu.cn
    - 微信公众号：教育网信安全发布 
  - 对接第三方系统
    - CNVD，360补天，漏洞盒子

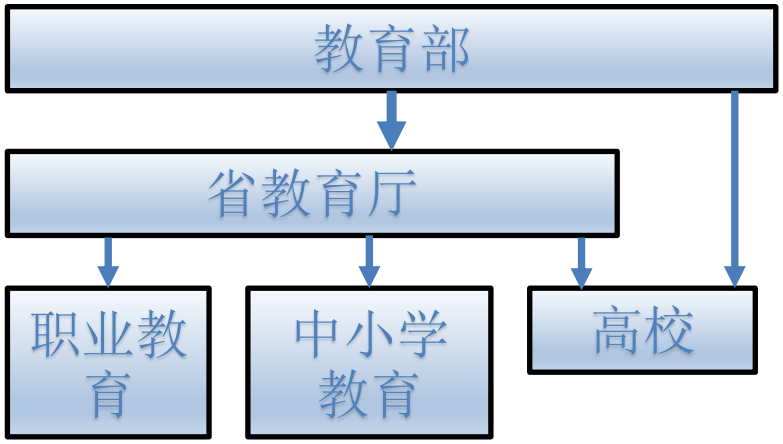
层次化管理结构

- 各类信息的接入
- 响应措施的落地
- 对单位不对个人
- 建立标准化的响应队伍

超级管理员

地区联系人

单位联系人



对接CNVD、漏洞盒子、360补天平台

- 根据邮件账号自动接收来自多个漏洞平台的漏洞通知

微信公众号：教育网信安全发布

- 手机实时推送安全漏洞信息
- 和IPDB注册邮箱绑定

IPDB基础数据库 — 规模

- 收录单位：3991所
  - 省教育厅： 31
  - 院校 ：3960
- 已注册单位 ： 927所
  - 省教育厅 ： 7
  - 院校 ：920
- 已注册联系人：1415人
- 已注册IP网段信息 ： 1784条
- 已注册二级域名信息：3004条

山东：59个单位98个联系人

安徽：48个单位59个联系人

江苏：14个单位23个联系人

中国高校网络信息安全工作组基础数据库 — 联系人

- 如何访问?
  - **http://ipdb.sec.edu-info.edu.cn**

- 如何加入?
  - 系统联系人：杨望 wyang@njnet.edu.cn
  - 地区联系人：
    - 山东：山东省教育厅 王淮；山东大学 万林，郭晓东
    - 安徽：中国科学技术大学 张焕杰
    - 江苏：东南大学 杨望
  - 详见： **http://ipdb.sec.edu-info.edu.cn/about**

小结

- 网络安全保障需要
  - 目标落实：直接责任、间接责任
  - 手段落实：工具、信息
  - 队伍落实：谁做什么

- 网络安全保障要形成纵深防御
  - 要扫好门前雪：层层拦截
  - 主干网：攻击拦截、网络安全态势感知
  - 校园网：僵尸主机处理、系统漏洞修补
  - **Crowdsourcing**：漏洞发现、技术支持

谢谢！