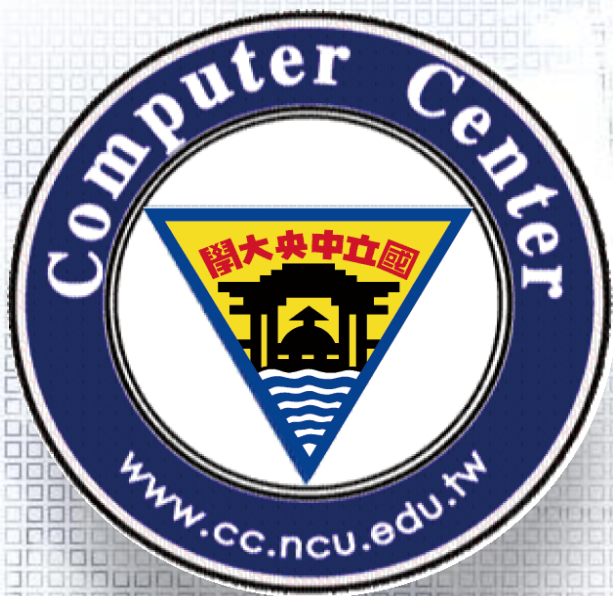




Cloud-based FDS 異常流量偵測系統

中央大學電算中心 楊素秋

Aug 22th 2014



報告大綱

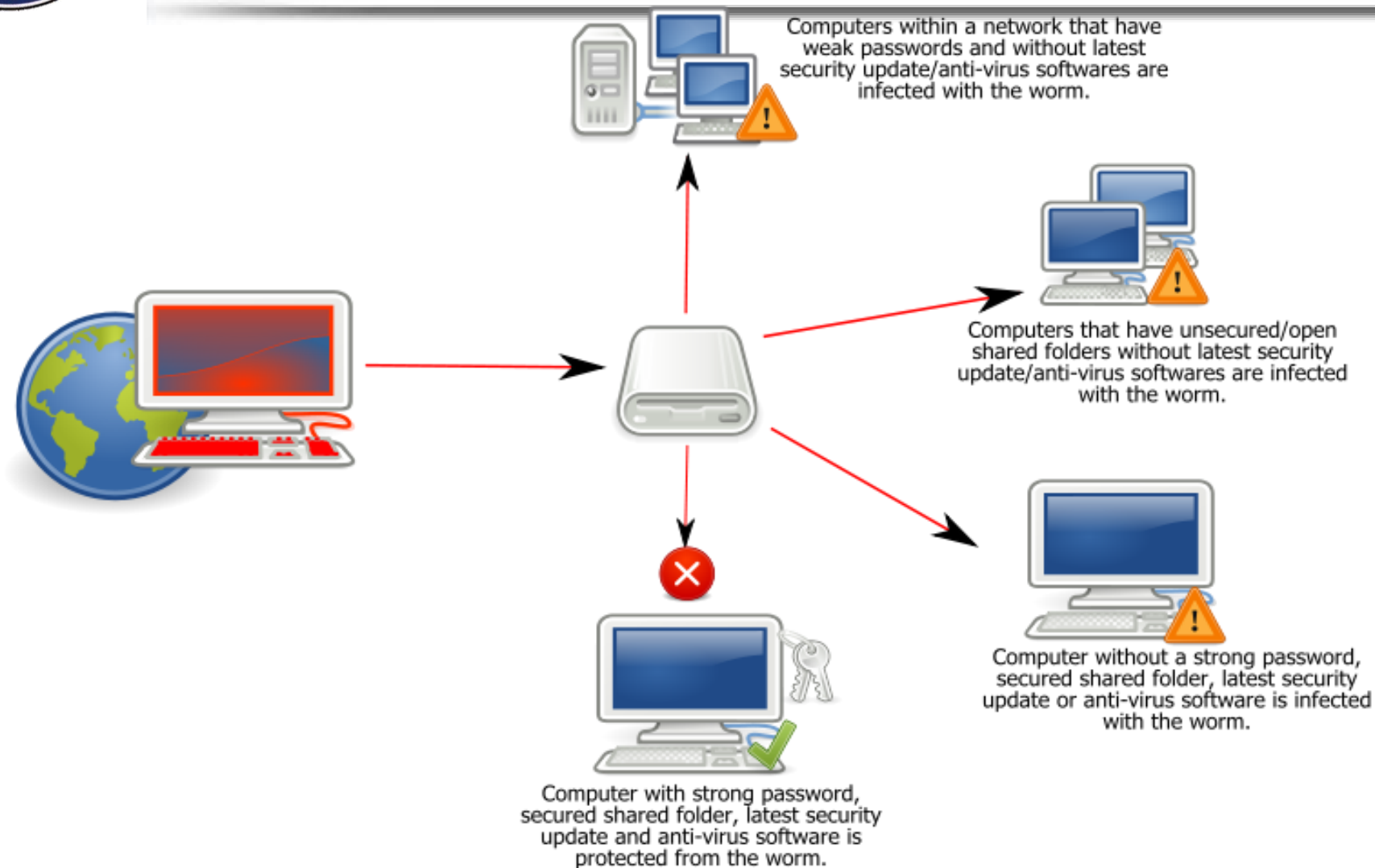
- ❑ 1. 網路危機
- ❑ 2. 網路異常流量偵測
- ❑ 3. Apache Hadoop (Cloud Computing)
 - Hadoop, Hadoop Mongo Connector
- ❑ 4. Cloud-based異常流量偵測
 - TopN, TopC, PortScan, UDP Flooding 流量
- ❑ 5. Pandora異常流量
- ❑ 6. Zone Protection
- ❑ 7. 結語



1. 網路危機

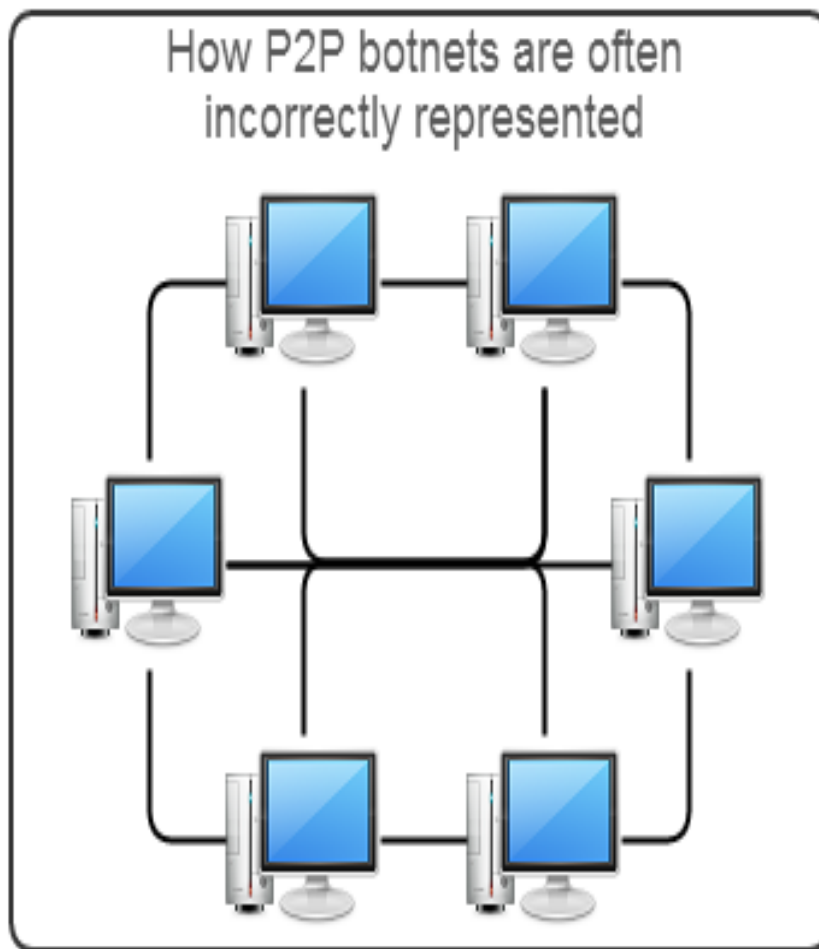
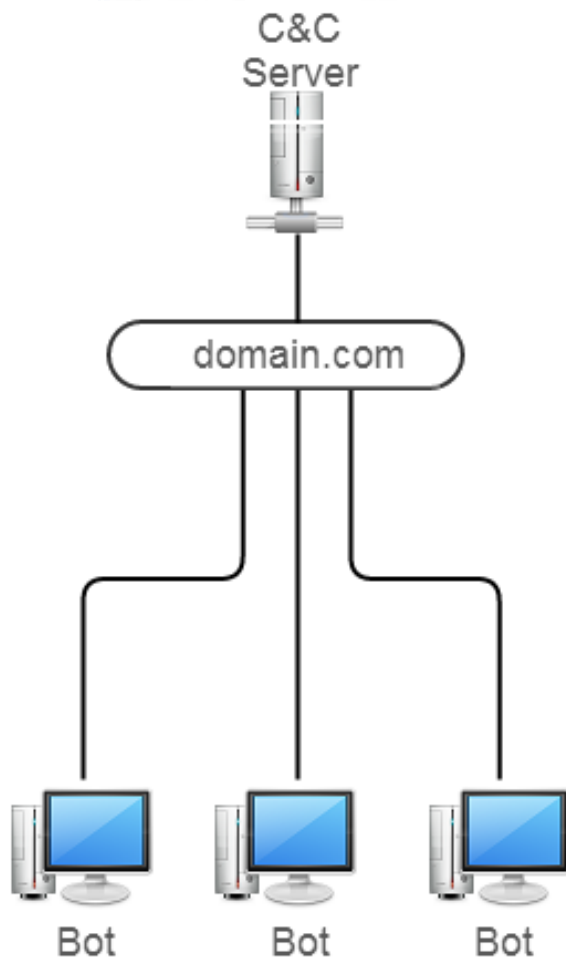
- 網路病毒 / 蠕蟲 / Botnet
 - 作業系統 弱點
 - 應用軟體 弱點
- 網路使用習慣
 - Unsecure password
 - Unsecure share folder
 - Without latest secure update
 - Without anti-virus software
- 社交工程
 - Virus mail
 - Clicking url
 - Unsecure software sharing

Worm: Win32 Conficker



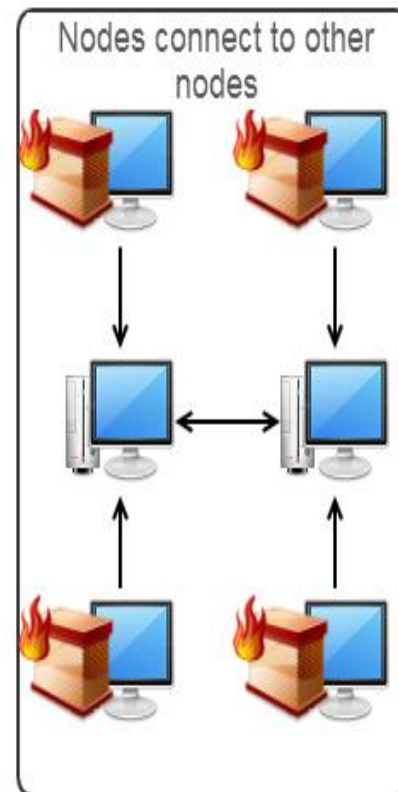
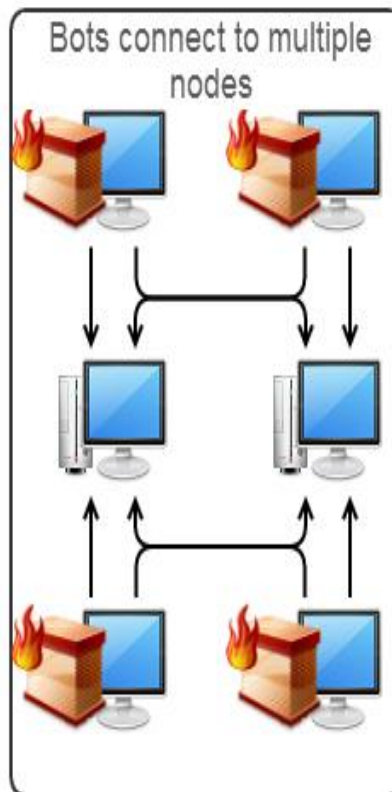
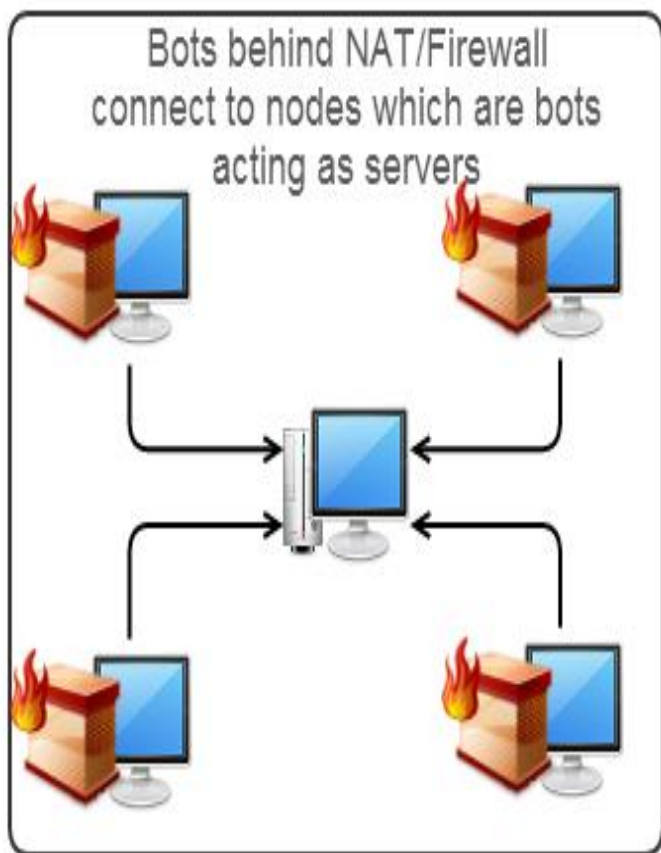
Botnet

“Peer-to-Peer Botnets for Beginners “ (轉載自 malwaretec.com)



Botnet

“Peer-to-Peer Botnets for Beginners “ (轉載自 malwaretec.com)





1. 網路危機

賽門鐵克：防毒軟體已死 改被動防守策略

【[聯合新聞網／記者楊又肇／報導](#)】 (2014/05/08)

賽門鐵克資訊安全部門資深副總Brian Dye 近期受訪表示

目前防毒軟體最多僅能阻擋一半以下的病毒攻擊

透過防毒軟體完全阻擋的時代已經消逝

未來將以減少因攻擊造成損失比例為目標



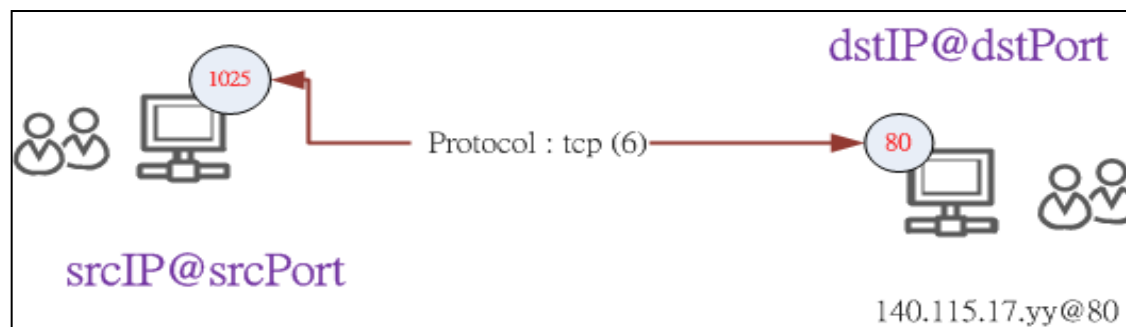


2. 網路異常流量偵測

- ☐ Spam email
- ☐ PortScan
 - worm/botnet spreading, password cracking
- ☐ DDoS Attack
 - Network service, bandwidth, sessions
- ☐ Flooding Traffic
 - Networking resource
 - tcp, udp, icmp



2. 網路異常流量偵測(cont.)

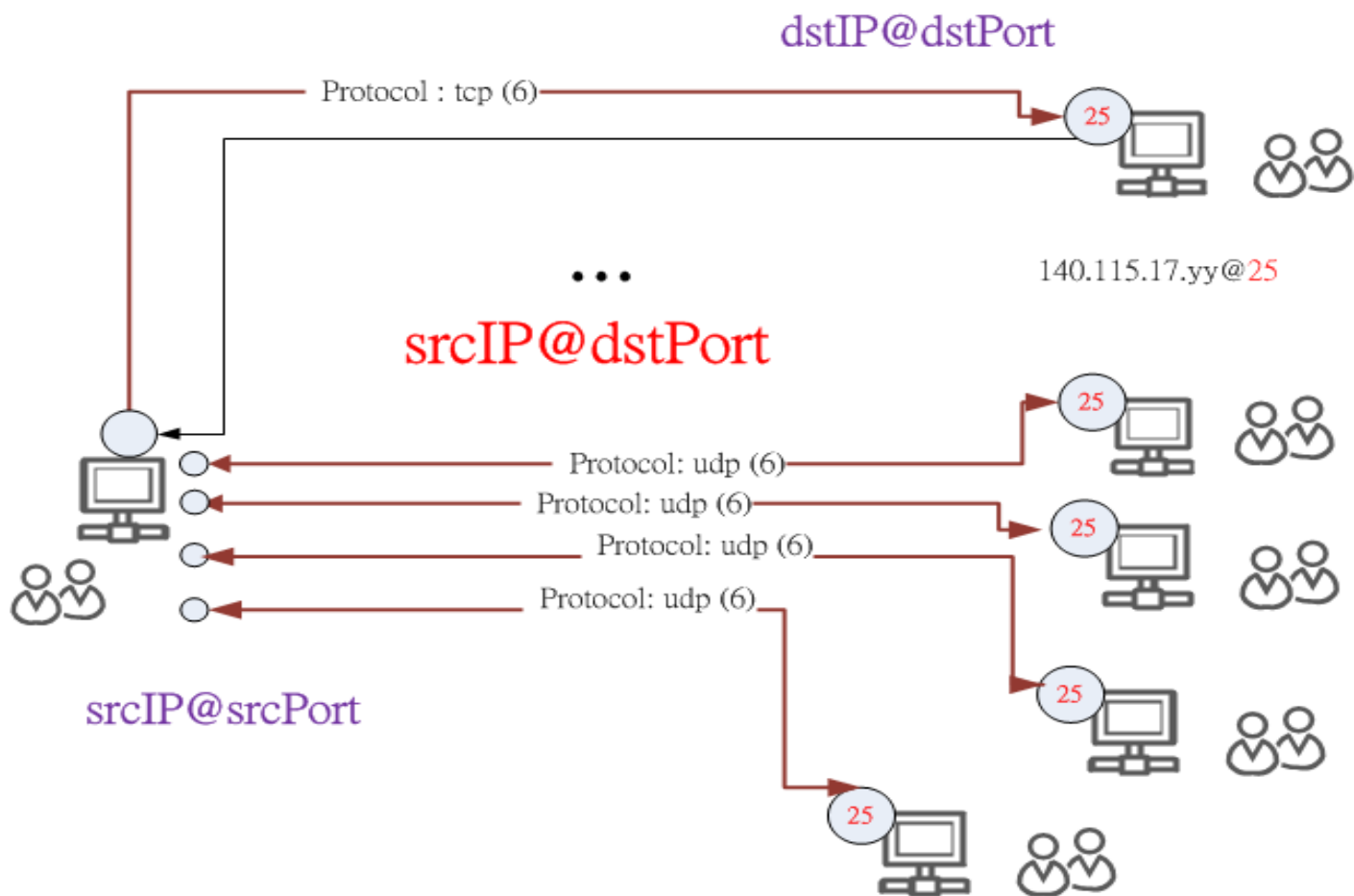


➤ NetFlow data

- 5-tuple record

-	srcIP	dstIP	prot	sPort	dPort	oct	pkt
-	-----						
-	96.244.49.242	140.135.230.123	6	3618	445	64	1
	96.244.49.242	140.135.59.95	6	3619	445	64	1
	96.244.49.242	140.135.148.61	6	3772	445	64	1

2. 網路異常流量偵測(cont.)





TANet 桃園區網 TopN 流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[伺服器機檢察系統\]](#) [\[NCU 伺服器機檢察系統\]](#) [\[NCU](#)

TopN 流量偵測

TopN 流量監測

TopN 流量排行

TopN 流量 (小時)

Top 連接數量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (小時)

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

UDP 流量排行

Udp 流量 (小時)

Udp 流量 (10分鐘)

UDP Flooding 流量監看

UDP Flooding 流量

TCP 異常流量偵測

密碼猜測 流量

Pandora 流量 (111.111.111.111)

Pscan 流量查詢

Keyword:

Q Search

Oid	Hostip	Cnt	Cnt_in	Cnt_out	Sum (B)	Psz_in	Psz_out	Sum_dur (Hour)
1	163.25.34.254@443	747393	230277	517116	10374	1122	230	5
2	210.60.0.2@443	665567	292393	373174	31881	1264	259	12
3	219.139.57.206@3389	651743	567717	84026	36687	1151	85	12
4	123.125.99.101@1433	569026	419218	149808	151	65	78	12
5	120.124.115.200@80	533173	162609	370564	3520	806	312	12
6	120.125.11.230@443	517474	277808	239666	17018	1038	585	8
7	163.25.34.254@80	499702	146854	352848	41868	1443	65	5
8	210.60.0.2@80	484763	205529	279234	29786	1425	68	12
9	182.93.14.100@3389	449407	449407	0	37721	1227	0	4
10	120.125.11.230@80	421661	243610	178051	47149	1453	71	8
11	210.59.42.253@443	413273	121818	291455	7906	1158	281	5
12	192.192.21.28@443	329103	160781	168322	10271	1216	182	5
13	192.192.21.27@443	312565	163196	149369	9375	1172	146	5
14	210.59.40.2@443	310826	101762	209064	9204	1275	119	4
15	192.83.196.115@0	306292	306292	0	27	75	0	12
16	192.192.21.23@443	303565	156309	147256	9855	1176	405	5

國立中央大學 電算中心



hadoop.tyc.edu.tw/Fdns x

hadoop.tyc.edu.tw/Fdns/

應用程式 雙連的網站 網管工具箱 網頁快取圖庫 Map Reduce Seco... download Invoice - Sample In... (Part 1) Configurin... Spring Hibernate Jazoon.com/histor... Text File to JPG file ... gotoalberto/mong... Hadoop 1.0 + Mo... ZK 其他書籤

您希望 Google Chrome 儲存密碼嗎? 儲存密碼

TANet 桃園區網 TopN 流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[伺服器主機檢查系統\]](#) [\[NCU 伺服器主機檢查系統\]](#)

INCUI TopN 流量偵測

TopN 流量監測

TopN 流量排行

TopN 流量 (小時)

Top 連接數量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (小時)

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

UDP 流量排行

Udp 流量 (小時)

Udp 流量 (10分鐘)

UDP Flooding 流量監看

UDP Flooding 流量

TCP 異常流量偵測

密碼猜測 流量

Pandora 流量 (111.111.111.111)

Pscan 流量查詢

Keyword: @25

Old	Hostip	Cnt	Cnt_in	Cnt_out	Sum (B)	Psiz_in	Psiz_out	Sum_dur (Hour)
31	120.125.120.115@25	190787	45847	144940	49	79	61	3
80	203.71.234.10@25	97508	3560	93948	12	85	54	2
120	140.115.71.94@25	75803	6353	69450	101	75	218	6
322	140.115.25.15@25	24738	119	24619	14	86	112	3
330	109.135.1.221@25	22813	6395	16418	1	46	46	1
371	184.22.136.101@25	16683	11028	5655	7	79	50	2

國立中央大學 電算中心



2. 網路異常流量偵測(cont.)

□ 桃園區網提供的異常偵測協助

➤ IPS資源應用量監看

- <http://kscore.tyc.edu.tw/Kscore>
 - CPU load : management / data plane
 - Session Rate, Temperature
 - Monitoring Session, Packet, Traffic of IPS

➤ Botnet 紀錄與自動通報

- DB: {id, conf, botIP, rule, **mgt**, **email**, created}
 - Extract email content
 - Query Mgt, Contact_Email (IP addr)
 - Automatically notification



2. 網路異常流量偵測(cont.)

□ 桃園區網提供的異常偵測協助 (cont.)

➤ Asoc 資安事件紀錄與自動通報

- 收TWCERT email, Extarct email content
- Query Mgt, Contact_Email , Automatically notification

➤ 異常流量偵測 / 監看

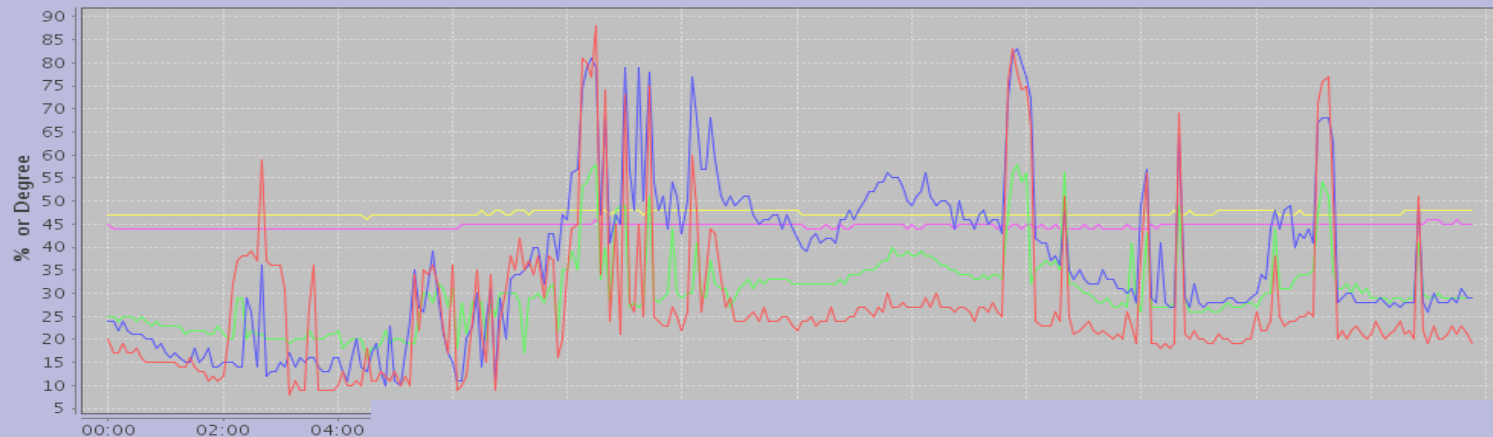
- <http://hadoop.tyc.edu.tw/Fdns>
 - TopN 流量, Top UDP 流量 (10-minute, hour, day)
 - » Udp Flooding
 - PortScan 流量
 - Top Connections , Top Packets
 - » Pandora 異常流量



IPS資源應用量監看

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-09-23)

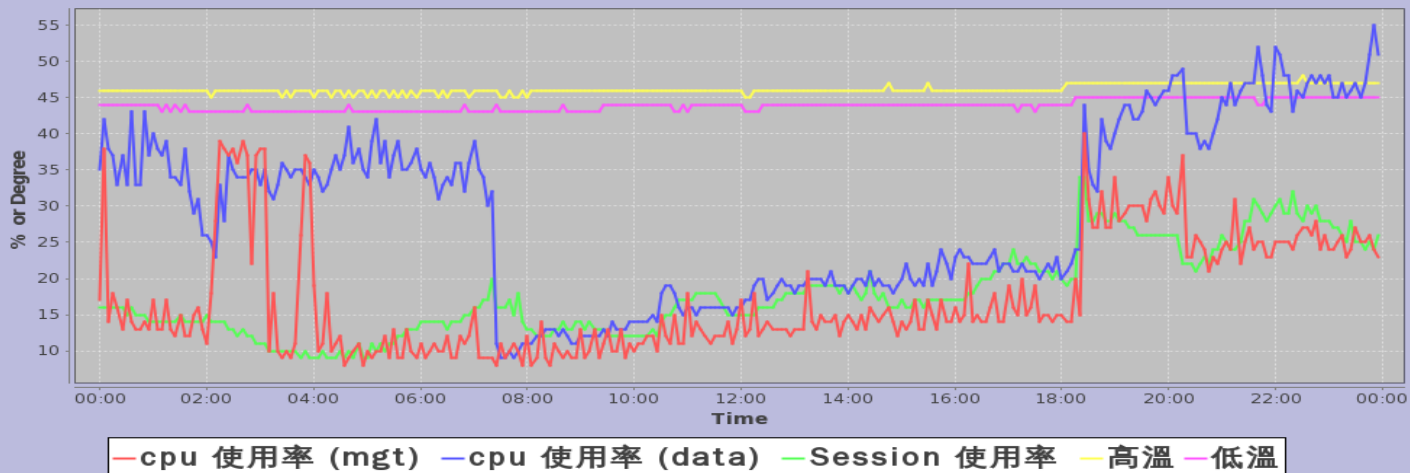
系統運作溫度 不可過高, Session使用率 不可過高



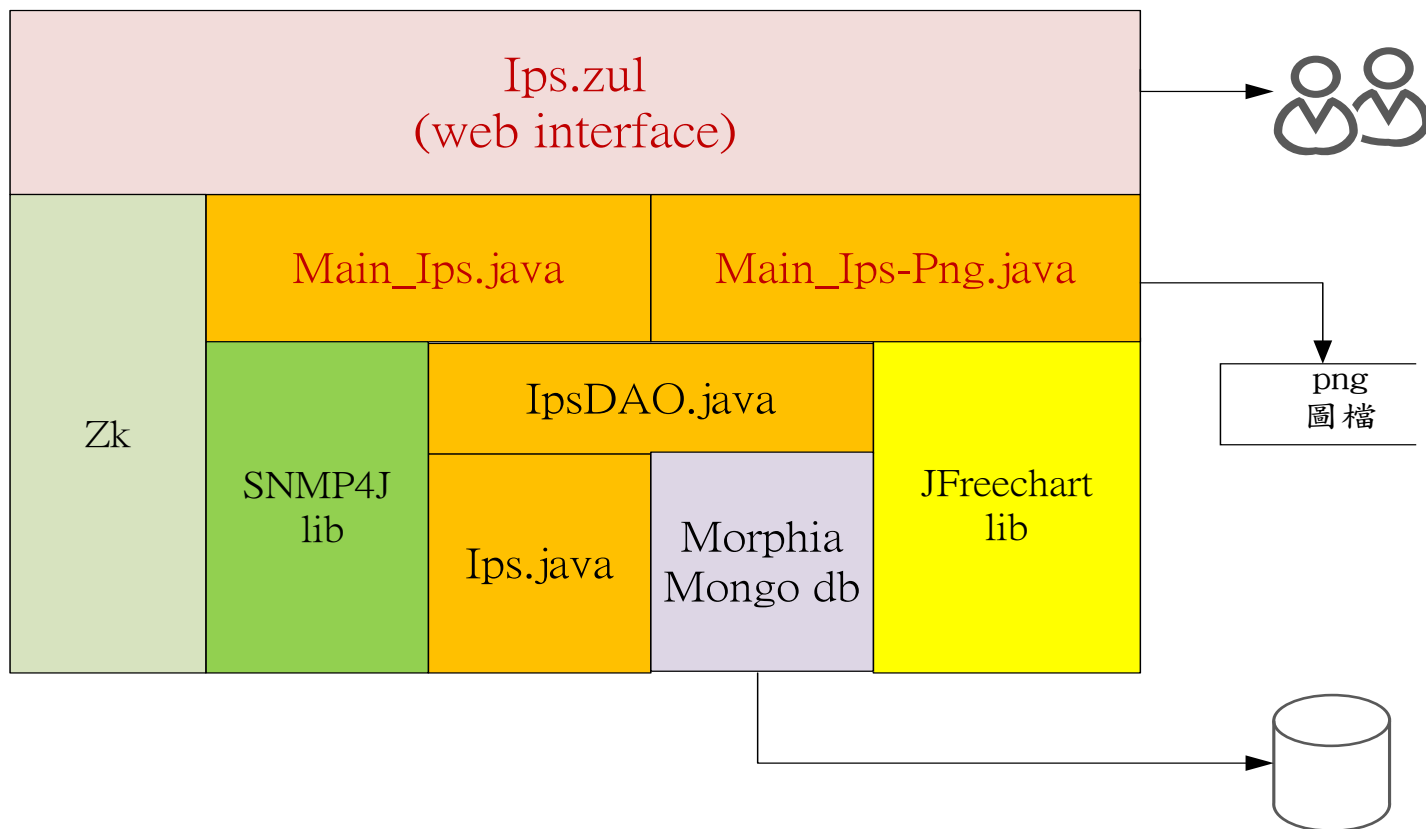
—cpu 使用率

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-10-27)

系統運作溫度 不可過高, Session使用率 不可過高



IPS資源應用量監看系統 架構



連網設備資源應用監看系統架構



Botnet 通告紀錄查詢 網頁

<http://kscore.tyc.edu.tw/Kscore/searchAsocMvc.zul>



臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器主機群
中央大學 伺服器主機群

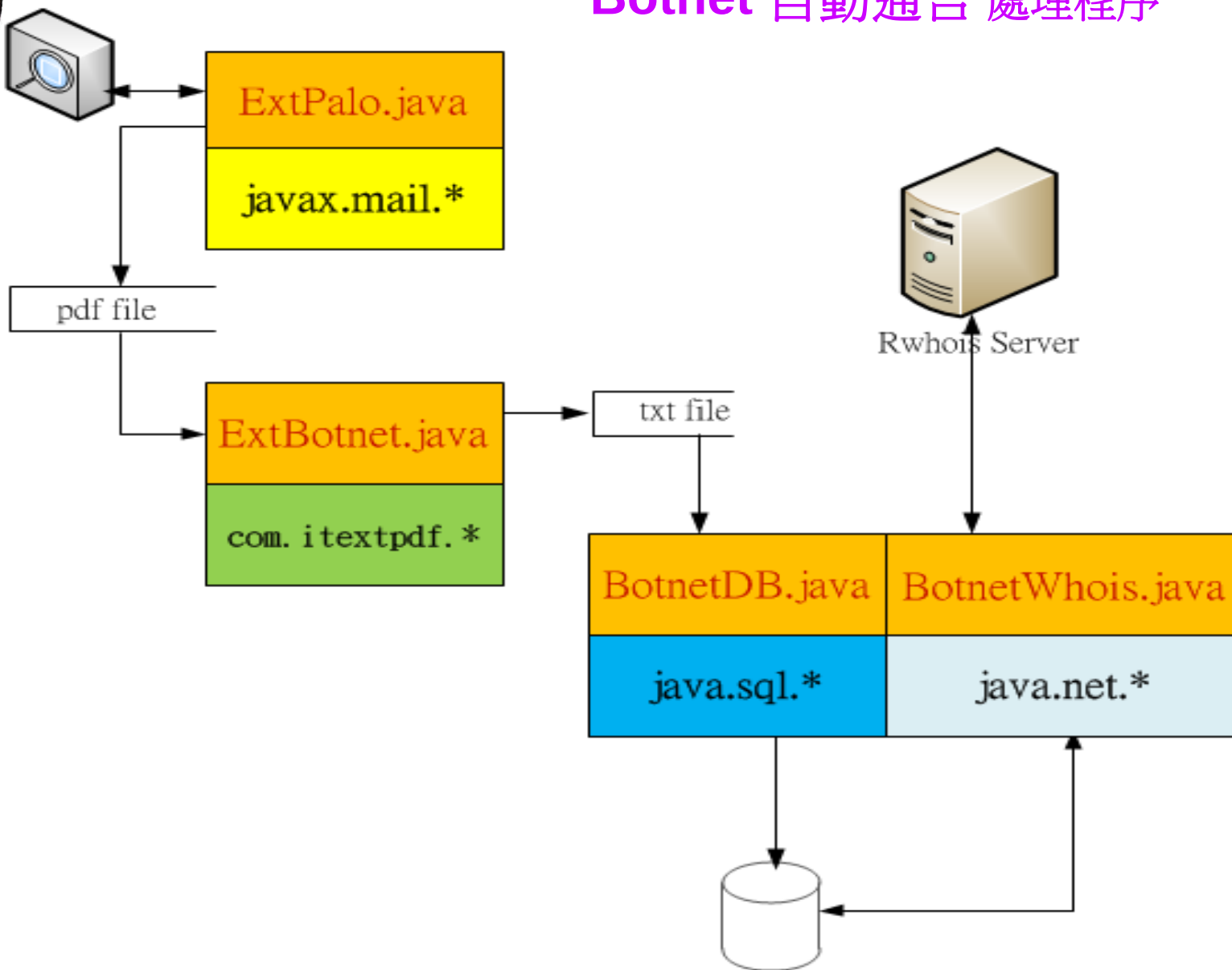
桃園區網 Botnet 通告紀錄查詢

Keyword:

Botnet_信度	Botnet IP	Botnet 判別依據	Botnet 管理者 Email	通告日期
4	140.115.20.48	vsys1 Repeatedly visited (54) the same malicious URL \secure-content-delivery.com\	hsuhm@cc.ncu.edu.tw,wangcy@cc.ncu.edu.tw	2013-10-24 00:00:00
4	140.115.43.92	vsys1 Repeatedly visited (24) the same malicious URL \secure-content-delivery.com\	gracelin@ncu.edu.tw,hhtsai@cc.ncu.edu.tw	2013-10-23 00:00:00
4	140.115.231.108	vsys1 Repeatedly visited (64) the same malicious URL \api.idown.org/api/update_server.php\	center9@cc.ncu.edu.tw	2013-10-23 00:00:00
4	120.124.62.204	vsys1 Repeatedly visited (30) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	tychiu@mail.vnu.edu.tw,cysung@mail.vnu.edu.tw	2013-10-23 00:00:00
4	140.115.230.9	vsys1 Repeatedly visited (32) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	center9@cc.ncu.edu.tw	2013-10-23 00:00:00
4	140.115.53.122	vsys1 Repeatedly visited (30) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	jjhuang@cc.ncu.edu.tw,wjwang@csie.ncu.edu.tw	2013-10-22 00:00:00
4	140.115.219.57	vsys1 Repeatedly visited (28) the same malicious URL \api.luckyleap.net\	center9@cc.ncu.edu.tw	2013-10-22 00:00:00
4	140.135.31.2	vsys1 Repeatedly visited (20) the same malicious URL \api.luckyleap.net\	yeh@cycu.edu.tw,wenhan@cycu.edu.tw,anpin	2013-10-22 00:00:00
4	140.115.66.145	vsys1 Repeatedly visited (22) the same malicious URL \api.webconnect.co/rs\	opcwl@ncu.edu.tw,tlyeh@cc.ncu.edu.tw,howa	2013-10-22 00:00:00
4	140.135.26.155	vsys1 Repeatedly visited (33) the same malicious URL \secure-content-delivery.com\	yeh@cycu.edu.tw,wenhan@cycu.edu.tw,anpin	2013-10-21 00:00:00
4	140.138.225.90	vsys1 Repeatedly visited (32) the same malicious URL \www.searchn.kr/ncs/intro_pnoc.php\	joejoe@saturn.yzu.edu.tw,c7ht@saturn.yzu.edu.tw	2013-10-21 00:00:00

國立中央大學 電算中心

Botnet 自動通告 處理程序





Asoc 資安通報紀錄查詢 網頁

163.25.251.55/Kscore/D/ x

163.25.251.55/Kscore/Demo.zul

應用程式 建議的網站 網管工具箱 網頁快訊圖庫 Map Reduce Seco... download Invoice - Sample In... (Part 1) Configurin... Spring Hibernate jazon.com/histor... Text File to JPG file ... 其他書籤

臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器主機群
中央大學 伺服器主機群

區網 Asoc Abuse紀錄查詢

Keyword:

Asoc_ID	IP	School	AbuseType	Date
AISAC-28522	192.192.250.155	開南大學資訊科技中心	對外攻擊	2013-10-23 11:16:31
AISAC-28283	140.135.198.35	中原大學電算中心	對外攻擊	2013-10-21 08:56:54
AISAC-28251	210.60.0.2	國立體育大學	殭屍電腦(Bot)	2013-10-21 08:26:22
ASOC-EWA-201310-0645	140.135.25.98	中原大學電算中心	對外攻擊	2013-10-17 16:02:10
AISAC-28124	192.83.181.124	國立體育大學	網頁置換	2013-10-16 22:26:26
AISAC-28110	192.192.250.94	開南大學資訊科技中心	對外攻擊	2013-10-16 17:36:05
AISAC-27968	140.115.71.237	中央大學電機	對外攻擊	2013-10-15 14:27:08
AISAC-27966	140.115.152.210	中央大學通訊	對外攻擊	2013-10-15 14:26:58
AISAC-27875	140.115.5.32	中央大學教職員宿舍	對外攻擊	2013-10-12 22:36:32
AISAC-27855	140.115.65.65	中央大學機械	對外攻擊	2013-10-11 11:56:30
AISAC-27789	140.115.185.82	總務處	對外攻擊	2013-10-08 15:26:05
AISAC-27641	210.60.0.2	國立體育大學	殭屍電腦(Bot)	2013-10-03 14:56:32
AISAC-27470	140.135.24.101	中原大學	對外攻擊	2013-09-28 13:46:17
AISAC-27339	120.124.129.31	健行科技大學	對外攻擊	2013-09-25 08:36:27
AISAC-27294	140.135.50.72	中原大學	殭屍電腦(Bot)	2013-09-24 13:53:05
AISAC-26791	140.135.56.124	中原大學	對外攻擊	2013-09-09 17:48:01
AISAC-26599	140.138.31.199	元智大學	殭屍電腦(Bot)	2013-09-05 10:27:26
AISAC-26458	140.115.65.65	中央大學機械	對外攻擊	2013-09-03 09:28:42
NTUSOC-EWA-201308-0094	120.124.74.210	萬能科技大學	可疑連線	2013-08-30 11:40:55
AISAC-26247	140.115.49.1	中央大學生資	對外攻擊	2013-08-27 15:57:33

國立中央大學 電算中心



臺灣學術網路 桃園區網中心

網路設備運作狀況

PaloAlto 5060 IPS
PaloAlto Sessions
區網機房 溫度/濕度
Cisco 6509 Router
網管交流圈地

運作狀況歷史紀錄

IPS 資源應用狀態查看
IPS Session 連接量查看
IPS 流量及封包量 MRTG

IPS 偵測資料/Asoc 資安通告

區網 Botnet 通告量分布圖
通告之 Botnet 紀錄查詢
區網 Asoc 資安事件量分布圖
Asoc 事件通告紀錄查詢
網路應用分布

連線狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連線狀態

異常流量查看

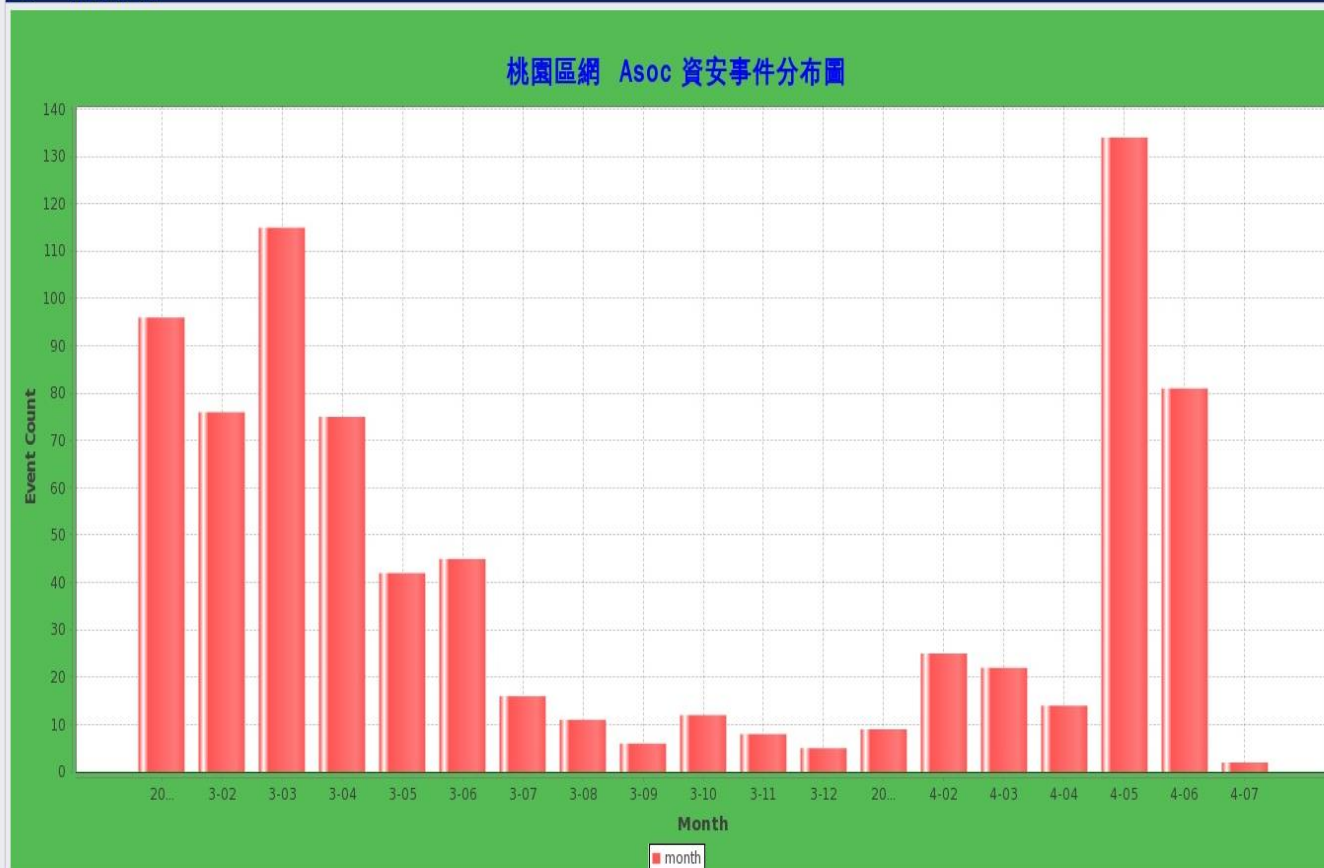
桃園區網 異常流量偵測系統
中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器主機群
中央大學 伺服器主機群

Service Usage Statistics

區網 Asoc 資安事件分布圖



國立中央大學 電算中心



3. Cloud Computing

- ❑ Hadoop
 - javac (compile)
 - java jar (execution)
- ❑ Hadoop + **Maven**
 - Input/output to text files
- ❑ **Hadoop + MongoDB + Maven**
 - Input/output to mongoDB **

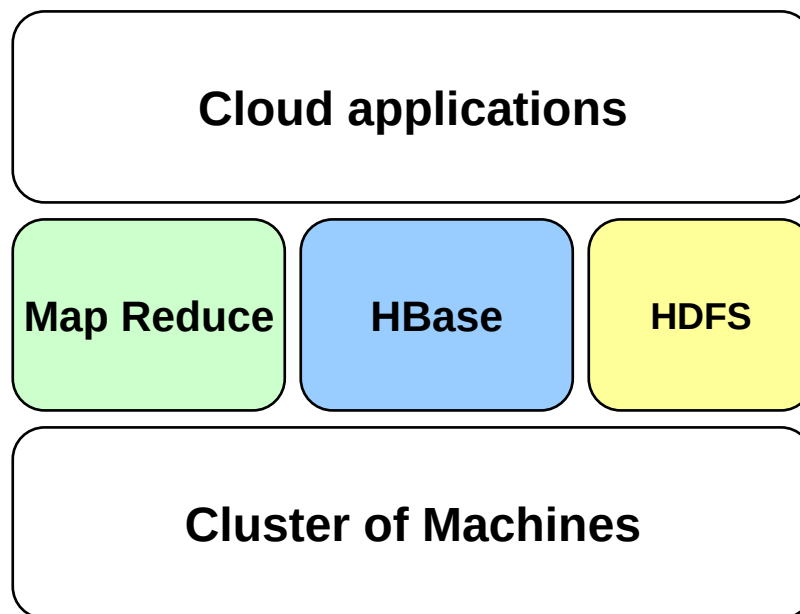


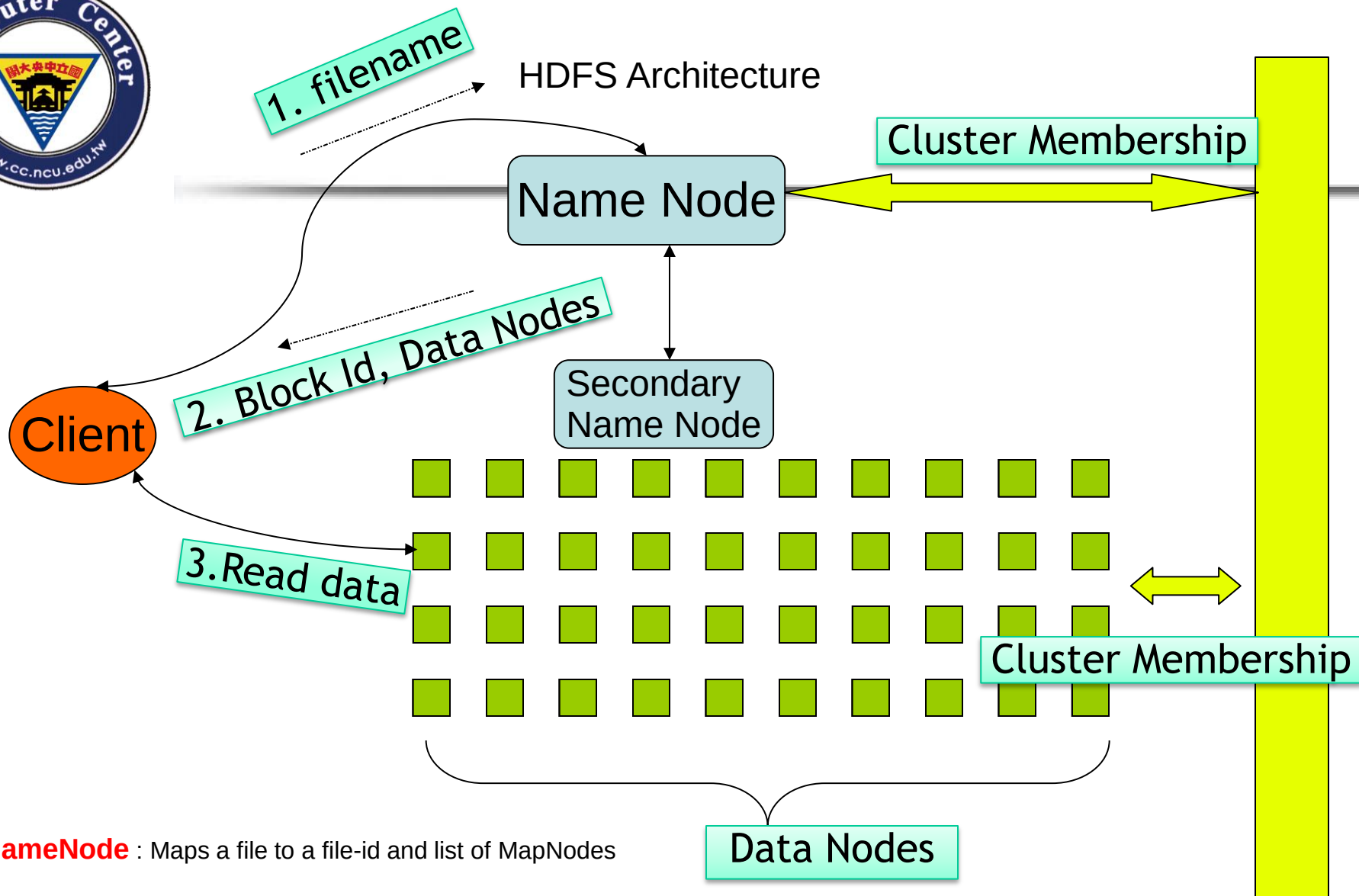
3. Cloud Computing (cont.)



- ☐ provides a framework for large scale parallel processing
 - distributed file system
 - map-reduce programming paradigm.

- ☐ **Open source project**
- ☐ Written by Java
- ☐ Runs on
 - **Linux**, Mac OS/X,
 - Windows, Solaris
 - Commodity hardware





NameNode : Maps a file to a file-id and list of MapNodes

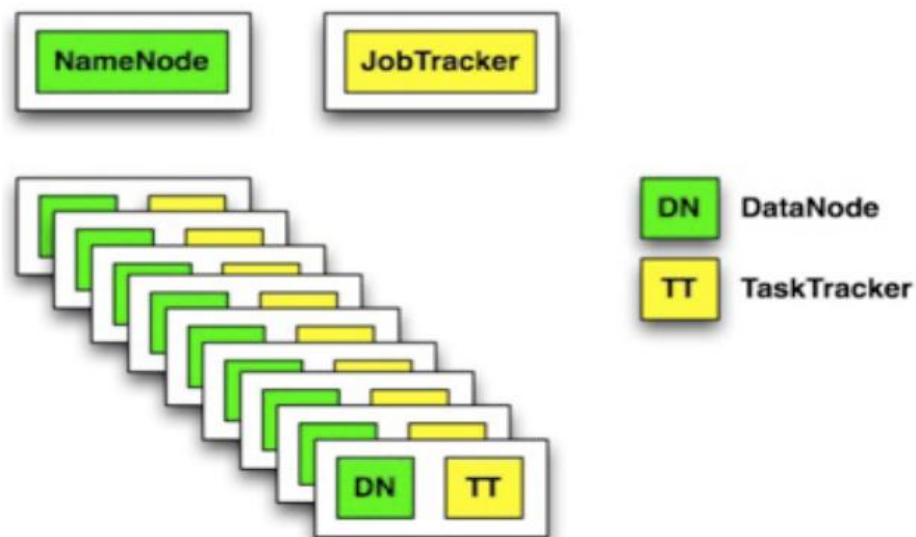
DataNode : Maps a block-id to a physical location on disk

SecondaryNameNode: Periodic merge of Transaction log



3. Cloud Computing (cont.)

- MapReduce framework consists of
 - master JobTracker
 - slave TaskTracker per cluster node.
- JobTracker is responsible for
 - **scheduling** the jobs' component tasks on the slaves
 - **monitoring** them and re-executing the failed tasks.
- TaskTrackers execute the tasks





3. Cloud Computing (cont.)

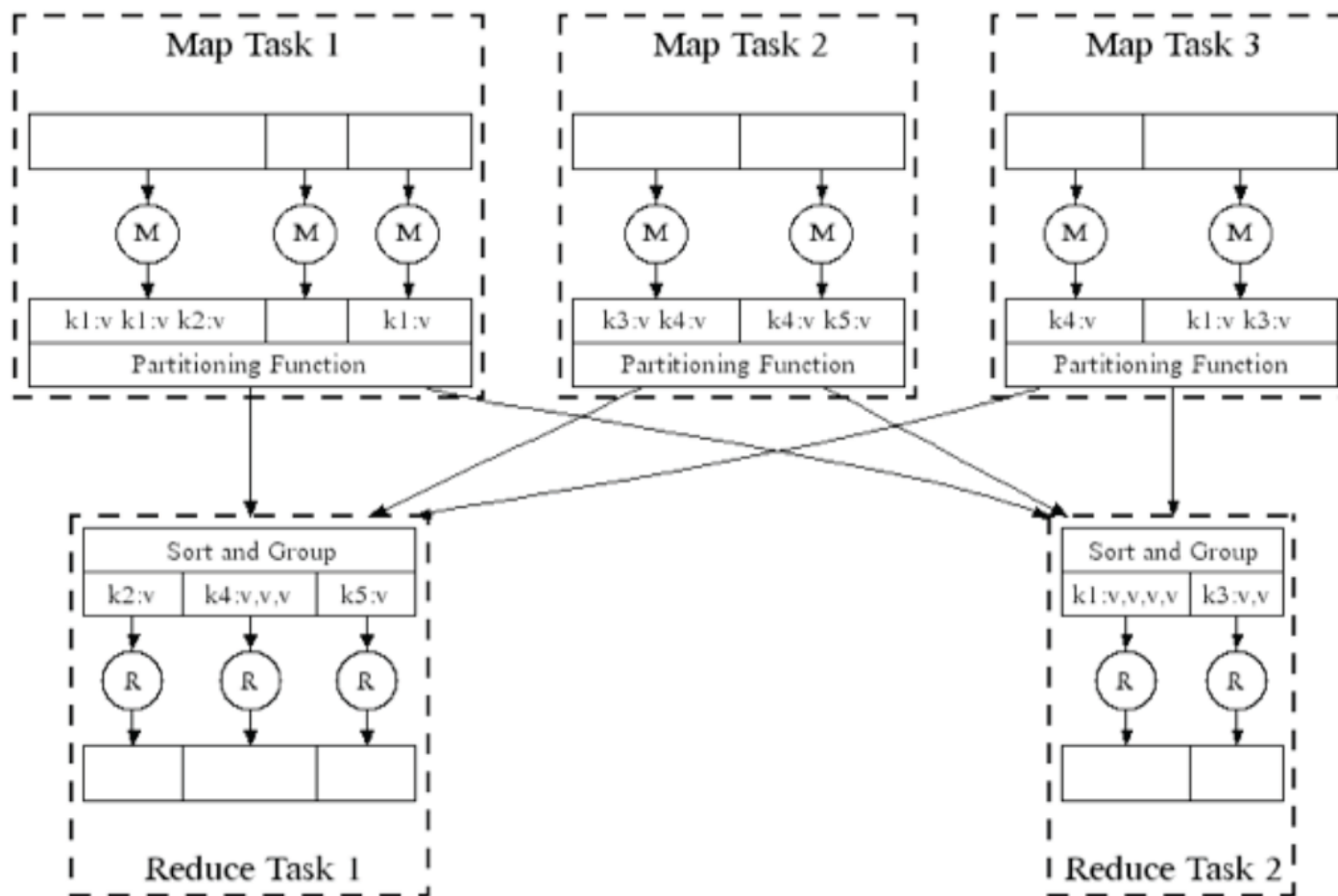
❑ Hadoop installation

- Hadoop tutorial
 - http://trac.nchc.org.tw/cloud/wiki/Hadoop_Lab1
- `cd /opt`
- `yum -y install openssh rsync`
 - `vim /etc/ssh/ssh_config`
 - `ssh-keygen -t rsa -f ~/.ssh/id_rsa -P ""`
 - `cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys`
- `wget http://apache.mesi.com.ar/hadoop/common/hadoop-1.2.1/hadoop-1.2.1.tar.gz`
- `tar zxvf hadoop-1.2.1.tar.gz`
- `mv hadoop-1.2.1 hadoop`
- `/opt/hadoop/conf`
 - `core-site.xml`, `hadoop-env.sh`, `mapred-site.xml`
- **`hadoop namenode -format`**
 - **`Hadoop dfsadmin -safemode leave`**
- `/opt/hadoop/bin`
 - `start-all.sh`, `stop-all.sh`



- **# /opt/hadoop/bin/start-all.sh**
 - starting **namenode**, logging to /opt/hadoop/logs/hadoop-yang-namenode-centos-2-31.out
 - 140.115.2.31: starting **datanode**, logging to /opt/hadoop/logs/hadoop-root-datanode-centos-2-31.out
 - 140.115.2.31: starting **secondarynamenode**, logging to /opt/hadoop/logs/hadoop-root-secondarynamenode-centos-2-31.out
 - starting **jobtracker**, logging to /opt/hadoop/logs/hadoop-yang-jobtracker-centos-2-31.out
 - 140.115.2.31: starting **tasktracker**, logging to /opt/hadoop/logs/hadoop-root-tasktracker-centos-2-31.out
- **# jps**
 - **28844 DataNode**
 - **28974 SecondaryNameNode**
 - **27588 NameNode**
 - **29193 TaskTracker**
 - **29272 Jps**
 - **27936 JobTracker**
 - **24521 Bootstrap**
- **# /opt/hadoop/bin/stop-all.sh**

Execution flow of a MapReduce





3. Cloud Computing (cont.)

□ Hadoop

➤ Mapreduce 程式

- Compile
 - **javac** -classpath /opt/hadoop/hadoop-core-1.0.1.jar:/opt/hadoop/hadoop-tools-1.0.1.jar -d flood_min flood_min.java
 - **jar** -cvf **flood_min.jar** -C flood_min/ .
- Execute
 - **hadoop jar** **flood_min.jar** flood_min input_dir output_dir

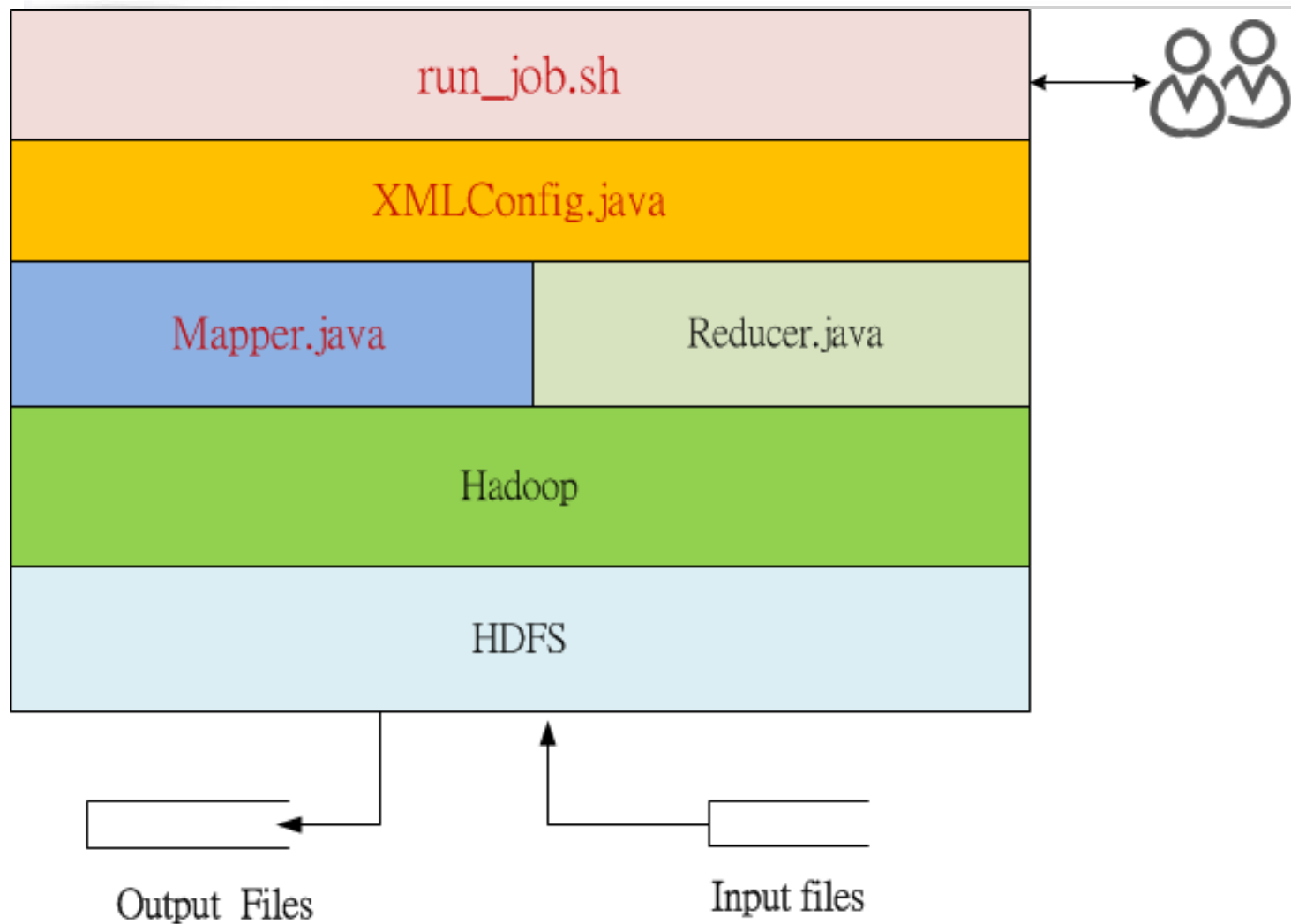


3. Cloud Computing (cont.)

□ Hadoop + Maven

➤ Mapreduce 程式

- Compile
 - mvn clean compile package
 - » target/project_name.war
- Execute
 - run_job.sh
 - » org.apache.hadoop.util.Tool;
 - » org.apache.hadoop.util.ToolRunner;





run_job.sh

```
#!/bin/sh
source /etc/profile
mday=`/bin/date '+%m%d'`
min=$(date --date='10 minute ago' +%H%M)

export HADOOP_HOME="/opt/hadoop"
JARNAME="tyrc_hadoop-1.0.jar"

HERE="$( cd "$( dirname "${BASH_SOURCE[0]}" )" && pwd )"

declare -a job_args
job_args=("jar" "$HERE/target/$JARNAME")

# INPUT SOURCE -
job_args=(${job_args[@]} "flood.flood_min")
job_args=(${job_args[@]} "flow_min")
job_args=(${job_args[@]} "output_flood")

$HADOOP_HOME/bin/hadoop "${job_args[@]}"

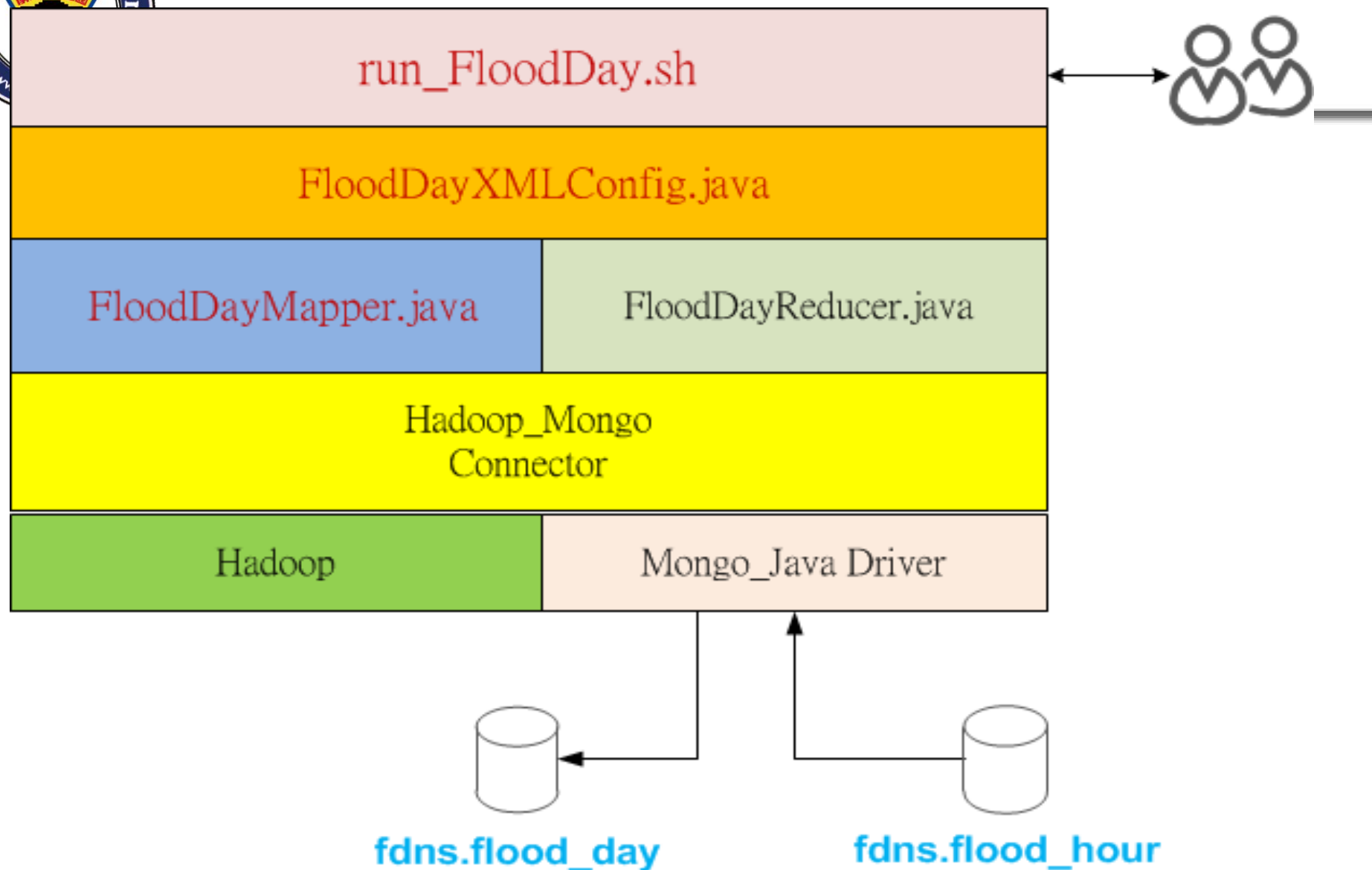
cd /home2/tyrc/Data/flood
hadoop fs -get output_flood/part-r-00000 $mday$min
```



3. Cloud Computing (cont.)

□ Hadoop + MongoDB + Maven

- Install Hadoop
- Install Hadoop Mongo Connector
 - lib
- Modify pom.xml
 - <resource>
 - <directory>\${basedir}/lib</directory>
 - </resource>
- run_job.sh





pom.xml

```
...  
<build>  
  <plugins>  
    <plugin>  
      <groupId>com.googlecode.addjars-maven-plugin</groupId>  
      <artifactId>addjars-maven-plugin</artifactId>  
      <version>1.0.5</version>  
      <executions>  
        <execution>  
          <goals>  
            <goal>add-jars</goal>  
          </goals>  
          <configuration>  
            <resources>  
              <resource>  
                <directory>${basedir}/lib</directory>  
              </resource>  
            </resources>  
          </configuration>  
        </execution>  
      </executions>  
    </plugin>  
  </plugins>  
</build>
```



FloodDayMapper.java

```
public class FloodDayMapper extends Mapper<Object, BSONObject, Text, Text > {
    @Override
    public void map(final Object pKey, final BSONObject pValue, final Context pContext)
        throws IOException, InterruptedException {
        final String hostip = (String) pValue.get("hostip");
        final long sum_in = ((Number) pValue.get("sum_in")).longValue();
        final long sum_out = ((Number) pValue.get("sum_out")).longValue();
        final int cnt_in = ((Number) pValue.get("cnt_in")).intValue();
        final int cnt_out = ((Number) pValue.get("cnt_out")).intValue();
        final long pkt_in = ((Number) pValue.get("pkt_in")).longValue();
        final long pkt_out = ((Number) pValue.get("pkt_out")).longValue();
        final int sum_dur = ((Number) pValue.get("sum_dur")).intValue();
        final String created = (String) pValue.get("created");
        if ( (sum_in >= (100000 * cur_hour) || sum_out >= (100000 * cur_hour) ) && created.contains(today) ) {
            String keyOut = hostip;
            String valueOut = String.valueOf(sum_in) + ":" + String.valueOf(sum_out) + ":" +
                String.valueOf(cnt_in) + ":" + String.valueOf(cnt_out) + ":" +
                String.valueOf(pkt_in) + ":" + String.valueOf(pkt_out) + ":" + String.valueOf(sum_dur);
            pContext.write(new Text(keyOut), new Text(valueOut));
        }
    }
}
```



FloodDayReducer.java

```
public class FloodDayReducer extends Reducer<Text, Text, Text, BSONWritable> {
    @Override
    public void reduce(final Text pKey, final Iterable<Text> pValues, final Context pContext)
        throws IOException, InterruptedException {
        for (final Text value : pValues) {
            String[] token = value.toString().split(":");
            sum_in += Long.parseLong(token[0]);
            sum_out += Long.parseLong(token[1]);
            cnt_in += Integer.parseInt(token[2]);
            cnt_out += Integer.parseInt(token[3]);
            pkt_in += Long.parseLong(token[4]);
            pkt_out += Long.parseLong(token[5]);
            sum_dur += Integer.parseInt(token[6]);
            if ( pkt_in > 0 ) psz_in = sum_in / pkt_in;
            if ( pkt_out > 0 ) psz_out = sum_out / pkt_out;
        }
        if ( sum_in >= (50000 * sum_dur) || sum_out >= (50000 * sum_dur) ) {
            BSONObject outDoc = BasicDBObjectBuilder.start()
                .add("sum_in", sum_in).add("sum_out", sum_out).add("cnt_in", cnt_in).add("cnt_out", cnt_out)
                .add("pkt_in", pkt_in).add("pkt_out", pkt_out).add("sum_dur", sum_dur)
                .add("psz_in", psz_in).add("psz_out", psz_out).add("created", today).get();
            BSONWritable pvalueOut = new BSONWritable(outDoc);
            pContext.write(pKey, pvalueOut);
        }
    }
}
```




FloodDayXMLConfig.java

```
package tyrc;
```

```
import com.mongodb.hadoop.util.MongoTool;  
import org.apache.hadoop.conf.*;  
import org.apache.hadoop.conf.Configuration;  
import org.apache.hadoop.util.ToolRunner;
```

```
public class FloodDayXMLConfig extends MongoTool {
```

```
    /*  
        static {  
            Configuration.addDefaultResource("src/examples/hadoop-local.xml");  
            Configuration.addDefaultResource("src/examples/mongo-defaults.xml");  
        }  
    */  
  
    public static void main(final String[] pArgs) throws Exception {  
        System.exit(ToolRunner.run(new FloodDayXMLConfig(), pArgs));  
    }  
}
```



run_mongo_job.sh

```
#!/bin/sh
cd /home2/tyrc/mongo_hadoop.
export HADOOP_HOME="/opt/hadoop"
INPUT_URI="mongodb://localhost:27017/fdns.flood_hour"
OUTPUT_URI="mongodb://localhost:27017/fdns.flood_day"
JARNAME="mongo_hadoop-1.0.jar"
HERE="$( cd "$( dirname "${BASH_SOURCE[0]}" )" && pwd )"
declare -a job_args
job_args=("jar" "$HERE/target/$JARNAME")
job_args=(${job_args[@]} "tyrc.FloodDayXMLConfig")
job_args=(${job_args[@]} "-D" "mongo.job.verbose=true")
job_args=(${job_args[@]} "-D" "mongo.job.input.format=com.mongodb.hadoop.MongoInputFormat")
job_args=(${job_args[@]} "-D" "mongo.input.uri=$INPUT_URI")
job_args=(${job_args[@]} "-D" "mongo.input.split_size=8")
job_args=(${job_args[@]} "-D" "mongo.job.mapper=tyrc.FloodDayMapper")
job_args=(${job_args[@]} "-D" "mongo.job.reducer=tyrc.FloodDayReducer")
job_args=(${job_args[@]} "-D" "mongo.job.output.key=org.apache.hadoop.io.Text")
job_args=(${job_args[@]} "-D" "mongo.job.output.value=com.mongodb.hadoop.io.BSONWritable")
job_args=(${job_args[@]} "-D" "mongo.job.mapper.output.key=org.apache.hadoop.io.Text")
job_args=(${job_args[@]} "-D" "mongo.job.mapper.output.value=org.apache.hadoop.io.Text")
job_args=(${job_args[@]} "-D" "mongo.output.uri=$OUTPUT_URI")
job_args=(${job_args[@]} "-D" "mongo.job.output.format=com.mongodb.hadoop.MongoOutputFormat")
echo "${job_args[@]}" "$1"
$HADOOP_HOME/bin/hadoop "${job_args[@]}" "$1"
```



4. Cloud-based 異常流量偵測

□ Cloud-based 異常流量偵測系統

➤ 桃園區網 FDNS (舊)

- TopN 流量排行, Top 連結 排行 (file)
- Top UDP 排行 (mysql DB)
- Kscore 異常監看 (mysql DB)

➤ 桃園區網 FDNS (新)

- <http://hadoop.tyc.edu.tw>
 - **Mongo DB Collections**
 - » flood_day, flood_hour
 - » TopN, Pscan, UdpN, TopC, TopP, pwCrack
 - **SEARCH 功能**



TopN 流量排行 查詢

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://163.25.255.31/Fdns/ 20140402.png (PNG Image, 1000 x... x) TopN 連結查看

163.25.255.31/Fdns/ Yahoo

Most Visited Getting Started

TAnet 桃園區網 異常流量監測

TopN 流量監測

- TopN 流量排行
- Top 連接數量排行
- UDP 流量排行

Pscan 異常偵測

- Pscan 異常流量排行
- Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

- Udp 流量 (10分鐘)
- Udp 流量 (小時)

UDP Flooding 流量監看

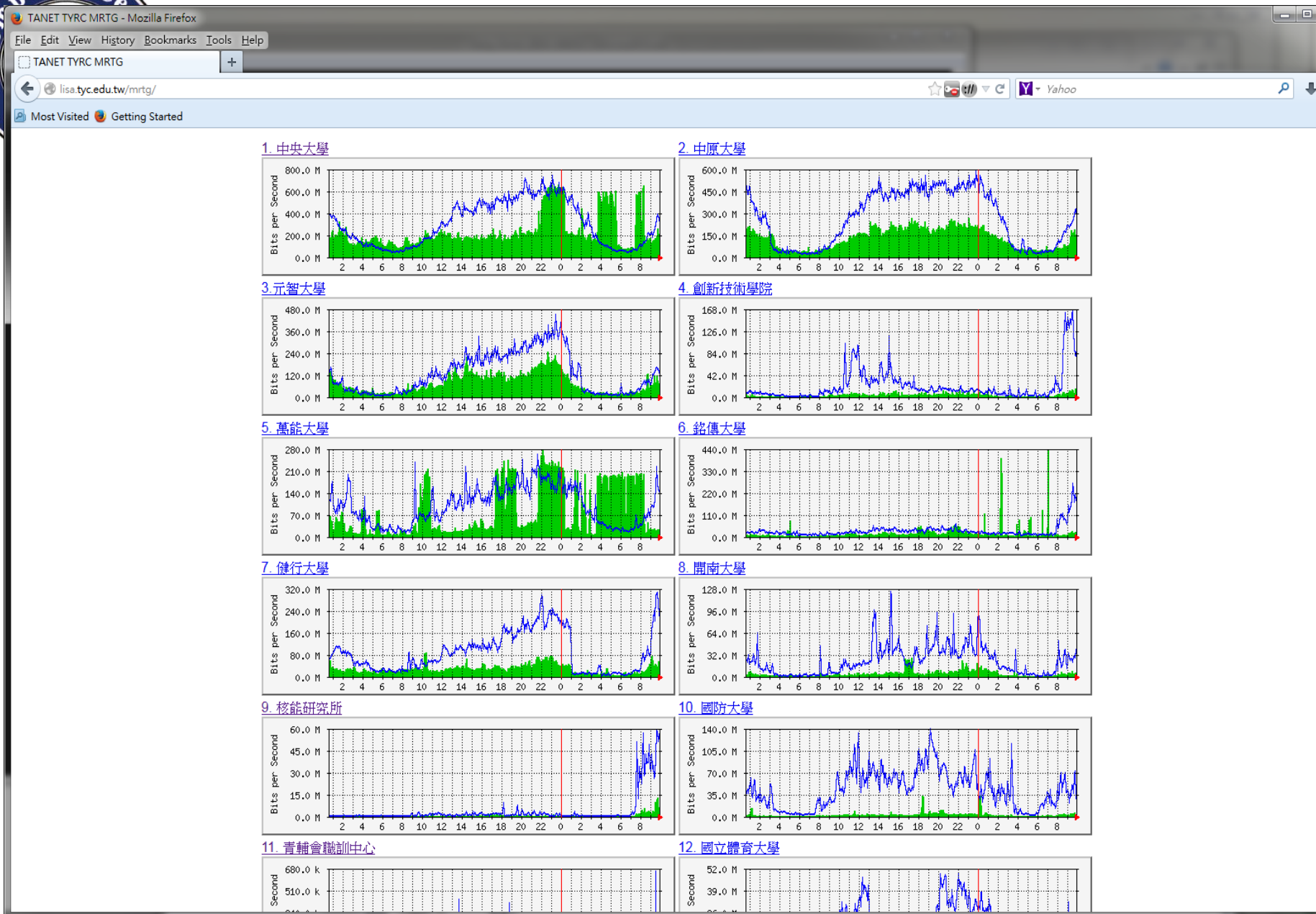
- UDP Flooding 異常流量

Tyrc TopN 流量排行

Keyword:

Oid	Hostip	Sum (MB)	Sum_in	Sum_out	Psiz_in	Psiz_out	Sum_dur (Hour)
1	202.169.175.79	391696	3343	388353	52	1482	17
2	202.169.173.204	356278	3323	352955	50	1482	17
3	202.169.175.80	353407	2890	350517	50	1482	17
4	202.169.173.207	351020	2551	348469	51	1482	17
5	202.169.173.205	346050	3054	342996	51	1482	17
6	202.169.173.210	342072	2871	339201	50	1481	17
7	202.169.175.77	338562	2330	336232	51	1481	17
8	202.169.175.81	335845	2561	333284	51	1479	17
9	202.169.173.209	324979	2661	322318	51	1481	17
10	202.169.173.208	321074	2855	318219	51	1482	17
11	202.169.175.78	316795	2356	314439	51	1482	17
12	202.169.173.211	313393	2689	310704	51	1480	17
13	202.169.173.206	312774	2346	310428	51	1479	17
14	202.169.175.76	309776	2201	307575	51	1479	17
15	140.115.17.45	273703	190	273513	49	1460	17
16	163.28.5.32	176386	3410	172976	53	1464	17
17	210.60.0.2	163829	155464	8365	1303	135	17
18	163.28.5.17	138713	3113	135600	58	1453	17
19	163.28.5.34	133038	2763	130275	57	1462	17
20	120.125.11.230	128768	115510	13258	1290	268	17

國立中央大學 電算中心





Udp Flooding 流量異常查詢

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://163.25.255.31/Fdns/

163.25.255.31/Fdns/

Most Visited Getting Started

 **TANet 桃園區網 TopN 流量監測**

TopN 流量監測

- TopN 流量排行
- Top 連接數量排行
- UDP 流量排行

Pscan 異常偵測

- Pscan 異常流量排行
- Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

- Udp 流量 (10分鐘)
- Udp 流量 (小時)

UDP Flooding 流量監看

- UDP Flooding 異常流量

UDP 流量排行

Keyword:

Oid	Hostip	Sum (MB)	Sum_in	Sum_out	Cnt_in	Cnt_out	Psiz_in	Psiz_out	Sum_dur (Hour)
1	192.186.208.165	177453	177453	0	506	0	1052	46	2
2	140.115.126.110	161350	0	161350	0	137	0	1052	2
3	162.212.252.47	154238	154238	0	349	0	1052	65	1
4	212.90.148.51	149669	149669	0	720	0	1052	332	2
5	120.124.40.98	129381	0	129381	23	657	137	1052	5
6	120.124.16.105	125480	0	125480	0	849	0	1054	5
7	198.251.80.166	94059	94059	0	154	0	1052	65	1
8	162.212.252.235	93630	93630	0	133	0	1052	65	1
9	198.251.80.221	53463	53463	0	128	0	1052	65	1
10	163.25.26.150	34036	55	33981	382	480	45	468	6
11	80.80.160.8	17597	17597	0	42	0	1052	46	1
12	96.45.82.133	17294	17294	0	31	0	1052	476	1
13	120.125.94.225	16998	5589	11409	41507	69354	581	985	9
14	140.135.13.130	15975	1106	14869	7993	7957	65	1059	10
15	140.135.9.120	15703	2861	12842	53648	52246	183	888	10

國立中央大學 電算中心

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://163.25.255.31/Fdns/

163.25.255.31/Fdns/ ☆ Yahoo

Most Visited Getting Started



TANet 桃園區網 TopN 流量監測

TopN 流量監測

TopN 流量排行

Top 連接數量排行

UDP 流量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

Udp 流量 (10分鐘)

Udp 流量 (小時)

UDP Flooding 流量監看

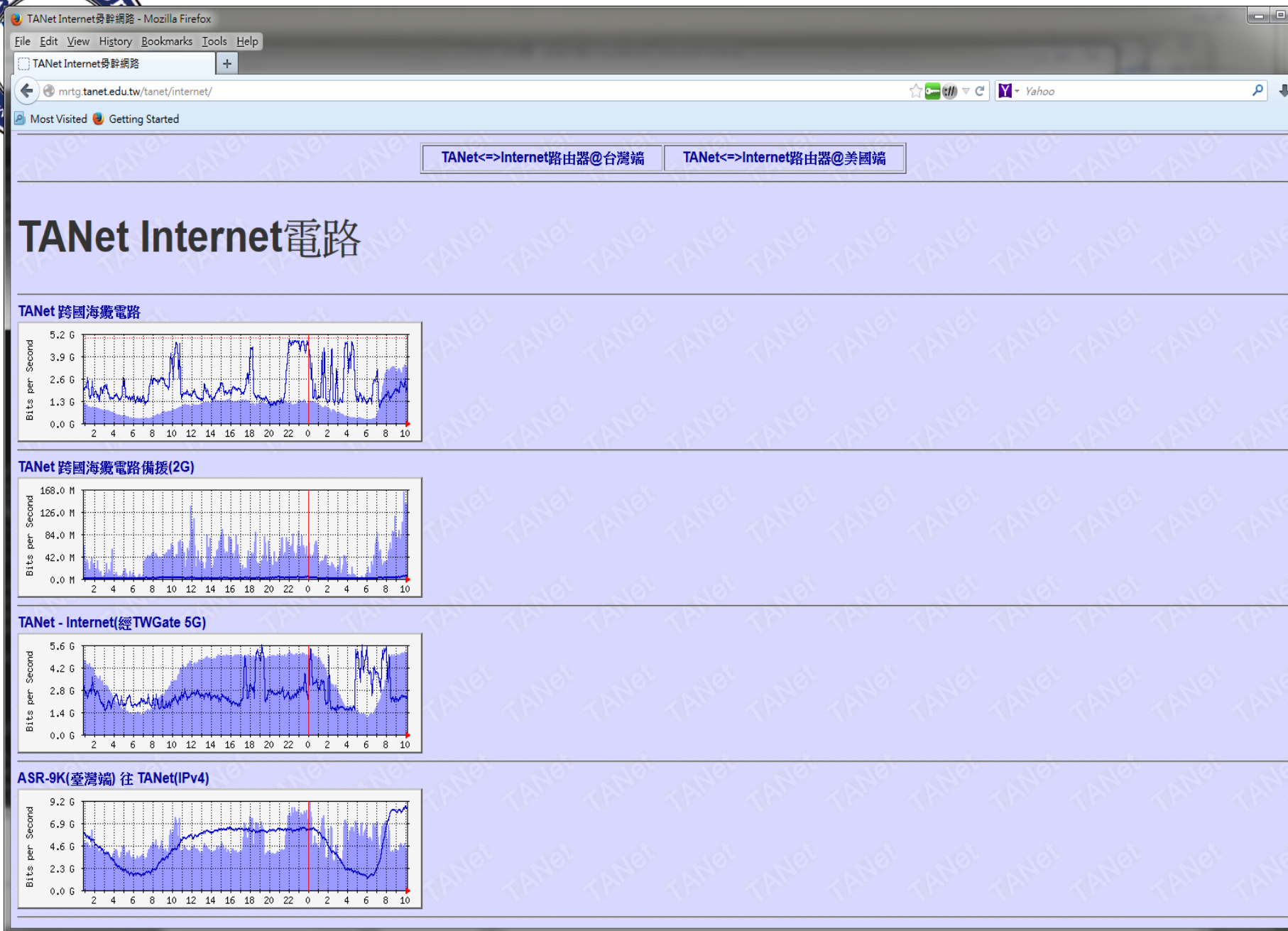
UDP Flooding 異常流量

UDP Flooding 偵測 (Kscore)

Keyword:

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
140.115.126.110@	0	18015	0	12	130	1052	04-21 08:20
140.115.126.110@	0	14150	0	17	115	1052	04-21 08:10
120.124.16.105@1	0	5381	0	51	214	1052	04-21 07:50
120.124.40.98@17	0	7465	0	58	49	1052	04-21 07:50
140.115.126.110@	0	12347	0	24	131	1052	04-21 07:50
120.124.40.98@17	0	6614	1	31	137	1052	04-21 07:40
140.115.126.110@	0	17309	0	10	137	1052	04-21 07:40
120.124.40.98@17	0	5134	1	37	137	1052	04-21 07:30
140.115.126.110@	0	29218	0	28	124	1052	04-21 07:30
120.124.40.98@17	0	6186	0	18	46	1052	04-21 07:20
120.124.16.105@1	0	6710	0	39	72	1052	04-21 07:00
120.124.40.98@17	0	5505	1	18	137	1052	04-21 07:00

國立中央大學 電算中心



File Edit View History Bookmarks Tools Help

http://hadoop...edu.tw/Fdns/ +

hadoop.tyc.edu.tw/Fdns/ Yahoo

Most Visited Getting Started

 **TANet 桃園區網 TopN 流量監測** [\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[伺服器主機檢客系統\]](#) [\[NCU 伺服器主機檢客系統\]](#) [\[NCU TopN 流量偵測\]](#)

TopN 流量偵測

TopN 流量監測

TopN 流量排行

TopN 流量 (小時)

Top 連接數量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (小時)

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

UDP 流量排行

Udp 流量 (小時)

Udp 流量 (10分鐘)

UDP Flooding 流量監看

UDP Flooding 流量

TCP 異常流量偵測

密碼猜測 流量

Pandora 流量 (111.111.111.111)

UDP 流量排行

Keyword:

Oid	Hostip	Sum (MB)	Sum_in	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Sum_dur (Hour)
1	198.50.130.224	115780	115780	0	698	0	1052	46	2
2	120.125.114.3	40861	0	40861	0	167	0	1052	2
3	198.50.130.227	30568	30568	0	217	0	1052	46	1
4	120.125.115.22	23639	0	23639	0	99	0	1052	1
5	37.187.40.140	23307	23307	0	84	0	1052	73	1
6	94.23.197.146	21779	21779	0	130	0	1052	46	1
7	176.31.228.8	20945	20710	235	3132	218	1480	73	3
8	162.218.53.138	18130	18130	0	72	0	1052	73	1
9	91.121.182.86	11018	11018	0	48	0	1052	73	1
10	163.25.20.177	7642	7311	331	64782	88381	1162	85	6
11	210.60.0.2	5412	3010	2402	79221	77813	419	337	7
12	162.218.53.228	5101	5101	0	17	0	1052	73	1
13	120.124.84.34	4174	3358	816	37616	42996	556	203	8
14	162.218.53.254	4036	4036	0	12	0	1052	73	1
15	37.187.199.115	3937	3937	0	21	0	1052	73	1
16	163.25.26.150	3443	0	3443	6	11	76	468	1
17	120.124.160.116	3337	2	3335	16	67	73	1493	2

國立中央大學 電算中心

Computer Center

File Edit View History Bookmarks Tools Help

http://hadoop....edu.tw/Fdns/

hadoop.tyc.edu.tw/Fdns/

Most Visited Getting Started



TANet 桃園區網 TopN 流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[伺服器主機檢查系統\]](#) [\[NCU 伺服器\]](#)

TopN 流量監測

TopN 流量排行

TopN 流量 (小時)

Top 連接數量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (小時)

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

UDP 流量排行

Udp 流量 (小時)

Udp 流量 (10分鐘)

UDP Flooding 流量監看

UDP Flooding 流量

TCP 異常流量偵測

密碼猜測 流量

Pandora 流量 (111.111.111.111)

Tyrc UDP 流量排行 (10分鐘)

Keyword: 120.125.114.3

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
120.125.114.3@17	0	3239	0	12	0	1052	05-07 04:10
120.125.114.3@17	0	4164	0	21	0	1052	05-07 04:00
120.125.114.3@17	0	7956	0	43	0	1052	05-07 03:50
120.125.114.3@17	0	3149	0	11	0	1052	05-07 03:40
120.125.114.3@17	0	2578	0	9	0	1052	05-07 03:30
120.125.114.3@17	0	4278	0	10	0	1052	05-07 03:20
120.125.114.3@17	0	2179	0	9	0	1052	05-07 02:30
120.125.114.3@17	0	1304	0	5	0	1052	05-07 02:20
120.125.114.3@17	0	3205	0	9	0	1052	05-07 01:40
120.125.114.3@17	0	3391	0	31	0	1052	05-06 23:30
120.125.114.3@17	0	5099	0	35	0	1052	05-06 23:20
120.125.114.3@17	0	4604	0	31	0	1052	05-06 23:10
120.125.114.3@17	0	4597	0	27	0	1052	05-06 23:00
120.125.114.3@17	0	6079	0	32	0	1052	05-06 22:50

國立中央大學 電算中心

2014/10/14

©2012 Computer Center, National Central University.

46



TANet 桃園區網 TopN 流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[伺服器主機檢察系統\]](#) [\[NCU 伺服器\]](#)

主機檢查系統 INCU TopN 流量偵測

TopN 流量監測

[TopN 流量排行](#)[TopN 流量 \(小時\)](#)[Top 連接數量排行](#)

Pscan 異常偵測

[Pscan 異常流量排行](#)[Pscan 異常流量 \(小時\)](#)[Pscan 異常流量 \(10分鐘\)](#)

UDP 詳細流量監看

[UDP 流量排行](#)[Udp 流量 \(小時\)](#)[Udp 流量 \(10分鐘\)](#)

UDP Flooding 流量監看

[UDP Flooding 流量](#)

TCP 異常流量偵測

[密碼猜測 流量](#)[Pandora 流量 \(111.111.111.111\)](#)

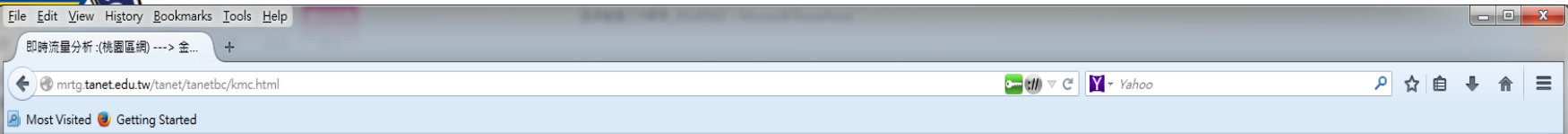
Tyrc UDP 流量排行 (10分鐘)

Keyword: 120.125.115.22

Q Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
120.125.115.22@17	0	2415	0	4	0	1052	05-07 06:10
120.125.115.22@17	0	2124	0	9	0	1052	05-07 05:10
120.125.115.22@17	0	4654	0	16	0	1052	05-07 05:00
120.125.115.22@17	0	1502	0	4	0	1052	05-07 04:30
120.125.115.22@17	0	2412	0	4	0	1052	05-07 04:10
120.125.115.22@17	0	5482	0	25	0	1052	05-07 03:50
120.125.115.22@17	0	4839	0	22	0	1052	05-07 03:40
120.125.115.22@17	0	4796	0	19	0	1052	05-07 03:20
120.125.115.22@17	0	3393	0	9	0	1052	05-07 02:30
120.125.115.22@17	0	2493	0	9	0	1052	05-07 02:20
120.125.115.22@17	0	3866	0	17	0	1052	05-07 01:40
120.125.115.22@17	0	2613	0	14	0	1052	05-06 23:30
120.125.115.22@17	0	1453	0	7	0	1052	05-06 23:20
120.125.115.22@17	0	860	0	4	0	1052	05-06 23:10
120.125.115.22@17	0	1454	0	6	0	1052	05-06 23:00

國立中央大學 電算中心



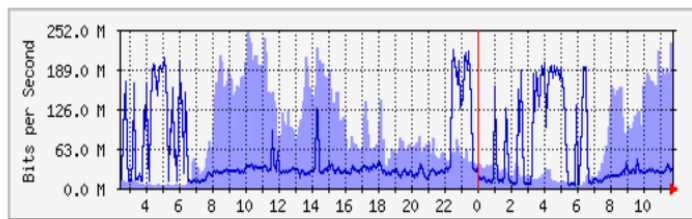
即時流量分析 :(桃園區網) ---> 金門縣網

Description: (桃園區網) ---> 金門縣網

Max Speed: 300 Mbps

上次統計更新時間: 2014 年 五 7 日 星期三 11:45

每日 圖表 (5 分鐘 平均)



最大

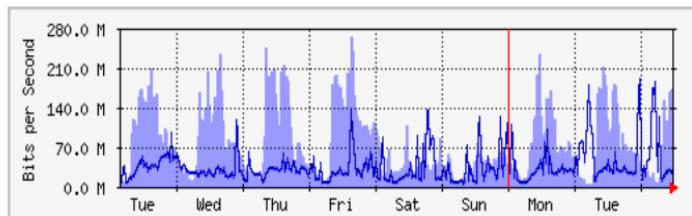
平均

目前

區網 ==> 縣網: 249.3 Mb/秒 (83.1%) 75.3 Mb/秒 (25.1%) 188.2 Mb/秒 (62.7%)

縣網 ==> 區網: 217.5 Mb/秒 (72.5%) 51.0 Mb/秒 (17.0%) 30.0 Mb/秒 (10.0%)

每週 圖表 (30 分鐘 平均)



最大

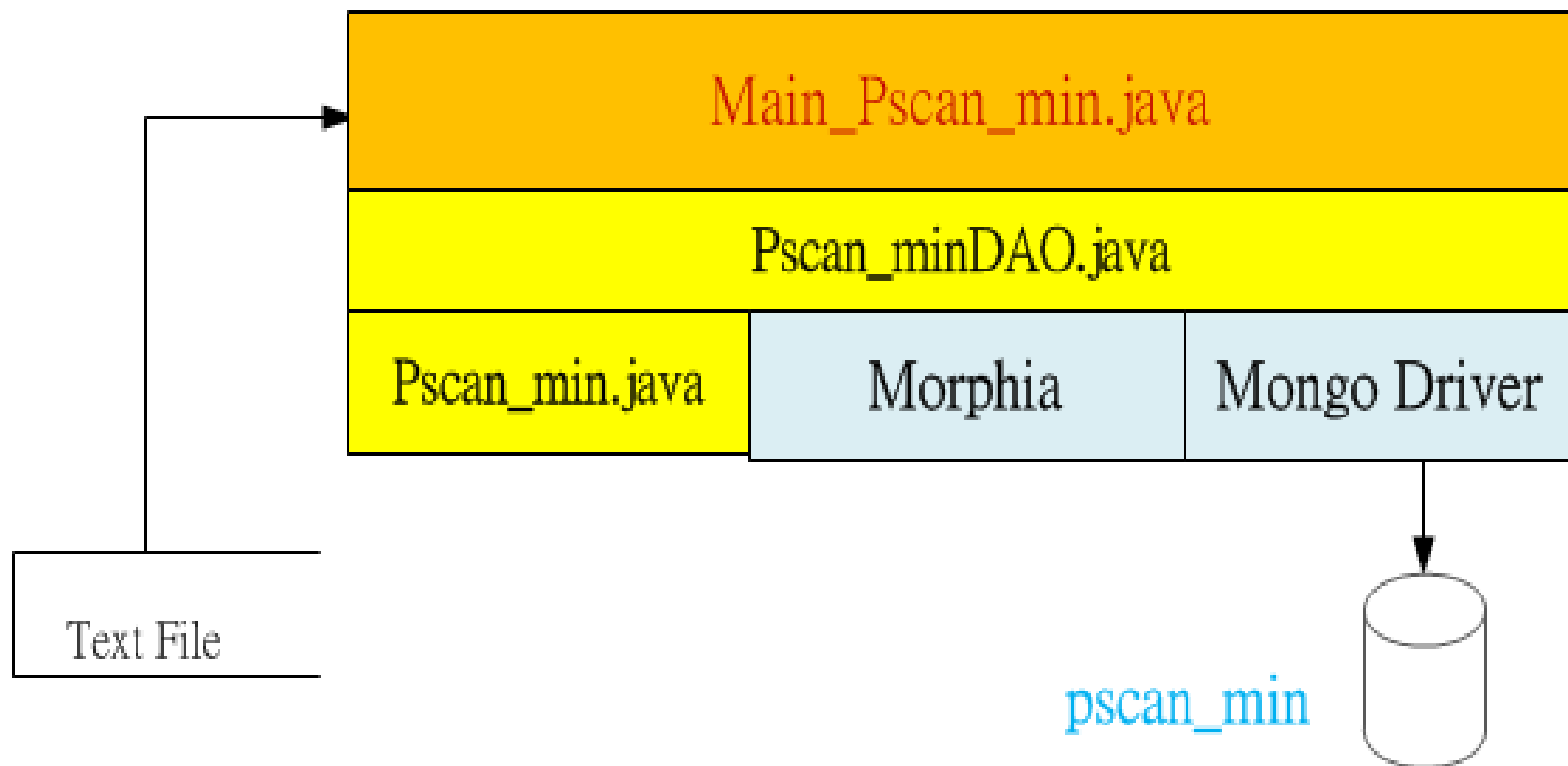
平均

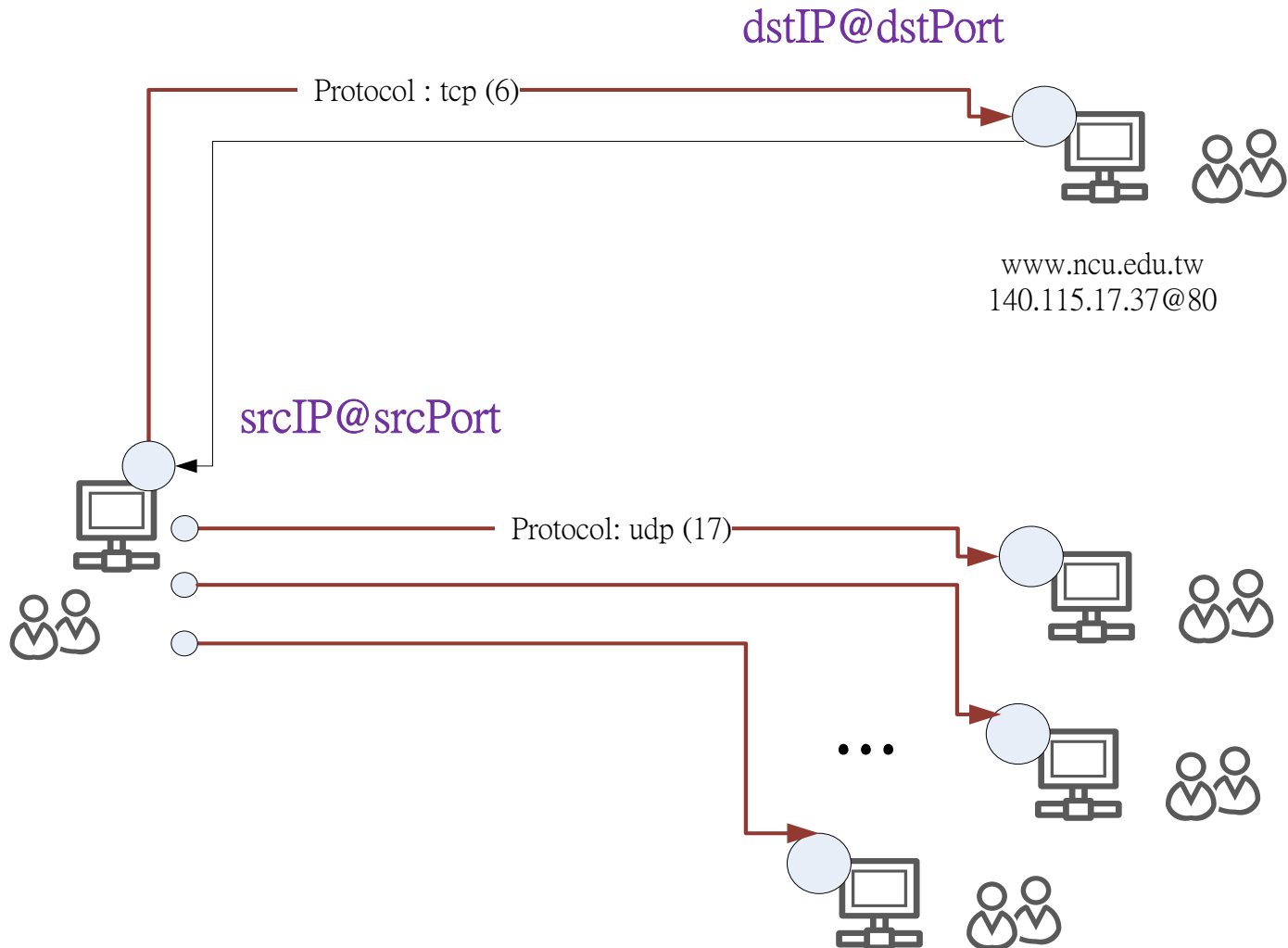
目前

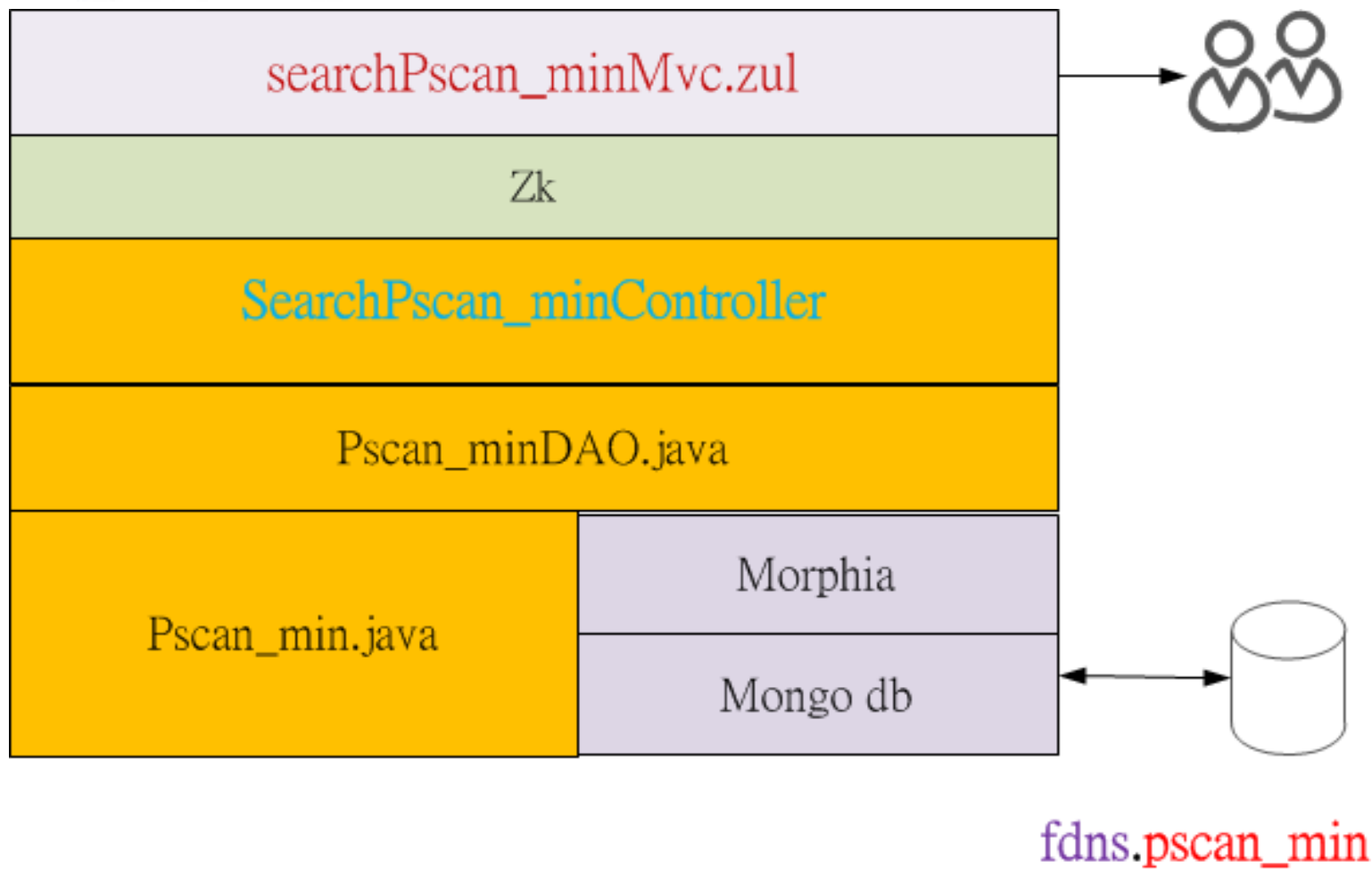
區網 ==> 縣網: 263.6 Mb/秒 (87.9%) 73.7 Mb/秒 (24.6%) 171.2 Mb/秒 (57.1%)



Fdns 架構 (Pscan_min 例)









TopN 流量監測

TopN 流量排行

Top 連接數量排行

UDP 流量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

Udp 流量 (10分鐘)

Udp 流量 (小時)

UDP Flooding 流量監看

UDP Flooding 異常流量

PortScan 流量 (per-10分鐘)

Keyword:

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
120.124.84.36@443	540	48	12056	17321	1171	122	04-22 15:00
120.124.84.36@80	2857	29	6114	10285	1401	80	04-22 15:00
120.125.11.202@443	794	202	16836	24421	1073	418	04-22 15:00
120.125.11.202@80	1807	56	12577	18376	1442	84	04-22 15:00
120.125.11.230@443	1286	503	47130	67390	915	366	04-22 15:00
120.125.11.230@80	4527	129	33772	47080	1438	86	04-22 15:00
120.125.120.115@25	3	3	10064	16762	81	50	04-22 15:00
163.25.155.5@443	192	18	3867	7555	1172	118	04-22 15:00
163.25.34.254@443	267	61	12619	25775	1048	189	04-22 15:00
163.25.34.254@80	1405	48	7880	17372	1389	68	04-22 15:00
163.25.34.50@443	549	625	6323	14408	872	795	04-22 15:00
163.25.34.50@80	6466	110	5336	13451	1493	54	04-22 15:00
163.30.178.45@443	120	13	4280	5322	1160	146	04-22 15:00

國立中央大學 電算中心



4. UDP Flooding 流量偵測

□ Target UDP Flooding

- appServ flooding (per-10-minute)
 - Output Packet Size $\sim$ 1500 B/pkt
 - Output flow count > 10000
- Bandwidth Flooding
 - Output Udp Traffic > 5 GB
- Resource Flooding
 - Output Packet Size < 80 B/pkt
 - Output flow count > 100000
- Connection Flooding
 - Output flow count > 100000
- Packet Flooding
 - Output packet count > 1000000



Mongo/Morphia 篩選規則例

(10-minute Udp Traffic)

```
public static List<Udp_min> getAllKscore() throws
UnknownHostException {
    // Datastore ds = getDatastore();
    Query<Udp_min> q= ds.createQuery(Udp_min.class);
    q.or(
        q.and(
            q.criteria("psz_out").greaterThan(1495),
            q.criteria("cnt_out").greaterThan(10000)
        ),
        q.and(
            q.criteria("cnt_out").greaterThan(10000),
            q.criteria("psz_in").lessThanOrEq(80),
            q.criteria("psz_out").lessThanOrEq(80)
        ),
        q.criteria("sum_out").greaterThan(5000),
        q.criteria("cnt_out").greaterThan(100000)
    );
    return q.asList();
}
```



TANet 桃園區網 異常流量監測

TopN 流量監測

- TopN 流量排行
- Top 連接數量排行
- UDP 流量排行

Pscan 異常偵測

- Pscan 異常流量排行
- Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

- Udp 流量 (10分鐘)
- Udp 流量 (小時)

UDP Flooding 流量監看

- UDP Flooding 異常流量

Tyrc UDP Flooding 偵測

Keyword: 163.30.154 Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
163.30.196.253@17	0	6	0	126270	46	50	04-13 20:20
163.30.196.253@17	0	9	0	181984	176	50	04-13 20:30
120.125.2.67@17	0	8993	0	20	245	600	04-13 21:20
163.25.26.150@17	12	6159	5	10	46	468	04-13 01:40
140.115.30.31@17	0	3175	0	300064	125	1304	04-13 02:00
140.115.30.31@17	0	3987	0	303333	64	1299	04-13 02:10
163.25.26.150@17	12	6364	7	8	46	468	04-13 02:10
140.115.30.31@17	0	1579	0	142819	70	1303	04-13 02:20
163.25.26.150@17	4	5572	31	31	46	468	04-13 02:50
163.25.26.150@17	1	5075	28	50	46	468	04-13 05:30
140.115.170.248@17	0	5165	0	71	426	468	04-13 12:10
120.125.2.67@17	0	6433	0	20	270	600	04-13 12:50
163.25.131.1@17	0	20193	0	12	70	1028	04-13 15:10
163.25.131.1@17	0	6214	0	16	64	1028	04-13 15:20
163.30.154.129@17	0	25	0	232940	69	108	04-13 17:50
163.30.196.253@17	0	21	0	202257	565	108	04-13 17:50
163.30.154.129@17	0	25	0	501966	97	50	04-13 18:20

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://163.25.255.31/Fdns/ 20140402.png (PNG Image, 1000 x... x) TopN 連結監看

163.25.255.31/Fdns/ ☆ Yahoo

Most Visited Getting Started



TANet 桃園區網 異常流量監測

TopN 流量監測

TopN 流量排行

Top 連接數量排行

UDP 流量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

Udp 流量 (10分鐘)

Udp 流量 (小時)

UDP Flooding 流量監看

UDP Flooding 異常流量

Tyrc UDP Flooding 偵測

Keyword: 163.30.154 Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
163.30.154.129@17	0	25	0	232940	69	108	04-13 17:50
163.30.154.129@17	0	25	0	501966	97	50	04-13 18:20
163.30.154.129@17	0	125	0	1151491	131	108	04-13 18:30
163.30.154.129@17	0	77	0	714677	1148	108	04-13 18:40
163.30.154.129@17	0	132	0	1214887	565	108	04-12 06:10
163.30.154.129@17	0	13	0	122804	565	108	04-12 06:20
163.30.154.129@17	0	37	0	341436	143	108	04-12 16:30
163.30.154.129@17	0	156	0	1433489	132	108	04-12 00:20

國立中央大學 電算中心



TANet 桃園區網 TopN 流量監測

[區網專線學校 MRTG 流量](#) · [區網 IPv6 MRTG 流量](#) · [區網 Links 連線狀態偵測](#) · [網管工具箱](#) · [區網伺服器主機檢查系統](#)

[INCL] 网络十指检索系统 [INCL TopN 流量预测]

TopN 流量監測

TopN 流量排行

Top 連接數量排行

UDP 流量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

Udp 流量 (小時)

Udp 流量 (10分鐘)

UDP Flooding 流量監看

UDP Flooding 流量

TCP 異常流量偵測

密碼猜測 流量

Pandora 流量 (111.111.111.111)

UDP Flooding 偵測 (Kscore)

Keyword:

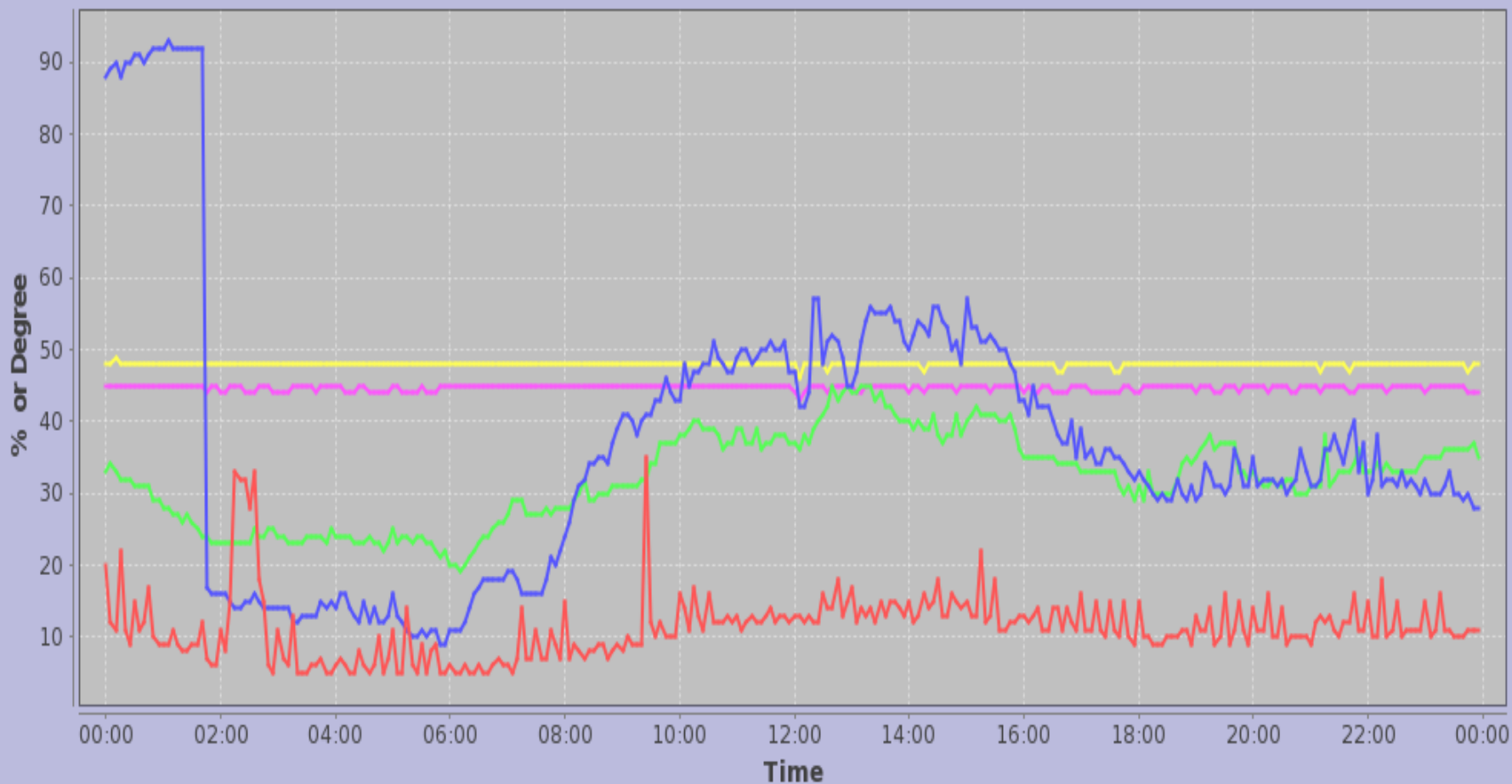
Q Search

Hostip	Sum_in(MB)	Sum_out	Cnt_in	Cnt_out	Psz_in	Psz_out	Created
120.125.85.166@17	0	1804	0	71219	0	1393	05-01 04:50
120.125.85.166@17	0	4685	0	81128	0	1376	05-01 04:40
120.125.85.166@17	0	3268	0	80847	0	1382	05-01 04:30
120.125.85.166@17	0	3255	0	76953	0	1381	05-01 04:10
120.125.85.166@17	0	2472	0	70559	0	1385	05-01 04:00
120.125.85.166@17	0	3354	0	79880	0	1381	05-01 03:50
120.125.85.166@17	0	295	0	49251	0	1500	05-01 03:40
140.115.8.220@17	0	4446	0	103938	0	1317	05-01 01:30
140.115.8.220@17	0	2327	0	111485	0	1325	05-01 01:20
140.115.8.220@17	0	2326	0	104407	0	1324	05-01 01:10
140.115.8.220@17	0	4434	0	98618	0	1317	05-01 01:00
140.115.8.220@17	0	2295	0	89948	0	1322	05-01 00:50
140.115.8.220@17	0	3309	0	90727	0	1319	05-01 00:40
140.115.8.220@17	0	4405	0	76696	0	1316	05-01 00:30
140.115.8.220@17	0	2328	0	94438	0	1323	05-01 00:20
140.115.8.220@17	0	2274	0	78074	0	1321	05-01 00:10

國立中央大學 電算中心

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2014-05-01)

系統運作溫度 不可過高, Sesssion使用率 不可過高



—cpu 使用率 (mgt) —cpu 使用率 (data) —Session 使用率 —高溫 —低溫



5. Pandora 異常流量

☐ KMPlayer 安裝

- 未 unmask “Pandora tv” 選項
- Malwarebytes starts blocking 111.111.111.111 about every 60 seconds.

☐ hook up with something called Pandora

- The player has added a directory,
 - Pandora TV
 - KMPlayerservice.exe

☐ Uninstall “Pandora tv”

Computer Center

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://hadoop.tyc.edu.tw/Fdns/index.zul

hadoop.tyc.edu.tw/Fdns/index.zul

Most Visited Getting Started



TANet 桃園區網 TopN 流量監測

[桃園區網 TopN 流量偵測] [中央大學 TopN 流量偵測] [桃園區網 Links 連線狀態偵測] [網管工具箱] [桃園區網問]

部主機檢査系統1

TopN 流量監測

TopN 流量排行

Top 連接數量排行

UDP 流量排行

Pscan 異常偵測

Pscan 異常流量排行

Pscan 異常流量 (10分鐘)

UDP 詳細流量監看

Udp 流量 (小時)

Udp 流量 (10分鐘)

UDP Flooding 流量監看

UDP Flooding 流量

密碼猜測 流量

Pandora 流量 (111.111.111.111)

Pandora 流量排行 (小時)

Keyword: 120.124 Search

Hostip	輸入量(MB)	輸出量	輸入連結量	輸出連結量	輸入封包長度	輸出封包長度	紀錄時間
120.124.4.53#111.111.1	0	42252	0	678	0	50	04-29 10:00
120.124.4.64#111.111.1	0	44328	0	707	0	50	04-29 10:00
120.124.46.3#111.111.1	0	42844	0	696	0	50	04-29 10:00
120.124.50.91#111.111	0	42536	0	696	0	50	04-29 10:00
120.124.84.34#111.111	0	85240	0	1410	0	50	04-29 10:00
120.124.84.35#111.111	0	49228	0	867	0	49	04-29 10:00
120.124.84.36#111.111	0	127964	0	2310	0	49	04-29 10:00
120.124.84.38#111.111	0	232848	0	4411	0	48	04-29 10:00
120.125.112.105#111.1	0	41664	0	638	0	48	04-29 10:00
120.125.112.161#111.1	0	39744	0	631	0	48	04-29 10:00
120.125.112.178#111.1	0	54436	0	780	0	50	04-29 10:00
120.125.112.79#111.11	0	44408	0	659	0	52	04-29 10:00
120.125.112.88#111.11	0	45888	0	714	0	48	04-29 10:00
120.125.114.27#111.11	0	43920	0	670	0	48	04-29 10:00

國立中央大學 電算中心



6. Zone Protection

□ 區網 IPS

- Protect Range 最大
- 精確 target 許多 worm, vulnerability, DDos attack
- Active block connection / drop packet

□ 區網 Traffic 特色

- Volume
- Dirty
- Creative attack behavior



6. Zone Protection (cont.)

☐ 維持 IPS 不被攻垮 (2014-06-19)

- CPU load (data plane)
- CPU load (management plane)
- Session rate

☐ Packets limitation

- SYN packets
- UDP Packets
- ICMP packets, ICMPv6 packets
- Other Packet



TANet 桃園區網 TopN 流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管\]](#)

工具箱 [\[伺服器機檢索系統\]](#) [\[MCU 伺服器機檢索系統\]](#) [\[MCU TopN 流量偵測\]](#)

TopN 流量

[TopN 流量排行](#)

[TopN 流量 \(小時\)](#)

UDP Flooding 流量監看

[UDP Flooding 流量](#)

UDP 詳細流量

[UDP 流量排行](#)

[Udp 流量 \(小時\)](#)

[Udp 流量 \(10分鐘\)](#)

Pscan 異常

[Pscan 異常流量排行](#)

[Pscan 異常流量 \(小時\)](#)

[Pscan 異常流量 \(10分鐘\)](#)

TopP 封包量

[TopP 封包量排行](#)

[TopP 封包量 \(小時\)](#)

[TopP 封包量 \(10分鐘\)](#)

TopC 連接量

[TopC 連接數量排行](#)

[TopC 連接量 \(小時\)](#)

[TopC 連接量 \(10分鐘\)](#)

TCP 異常流量偵測

UDP Flooding 偵測 (Kscore)

Keyword:

Search

Hostip	輸入量(MB)	輸出量	輸入連接數	輸出連接數	輸入封包大小	輸出封包大小	輸入封包量	輸出封包量Psz	紀錄時間
140.115.188.2	0	1034	6	422	65	1299	121	795766	07-16 09:10
140.115.188.2	8	1213	4	238	71	1306	115693	928771	07-16 08:50
140.115.158.1	0	16900	0	8	0	1052	0	16064811	07-16 08:30
140.115.158.1	0	21167	0	10	0	1052	0	20120867	07-16 08:10
163.25.122.24	0	1139	1	29	73	1478	2437	770488	07-16 08:10
140.115.158.1	0	21139	0	12	0	1051	0	20094999	07-16 07:50
140.115.158.1	0	21155	0	10	0	1052	0	20110249	07-16 07:40
140.115.158.1	0	14803	0	7	0	1052	0	14071996	07-16 07:20
140.115.158.1	0	21160	0	10	0	1052	0	20114087	07-16 07:00
140.115.158.1	0	21167	0	11	0	1051	0	20121205	07-16 06:40
140.115.158.1	0	21156	0	10	0	1052	0	20110528	07-16 06:20
140.115.158.1	0	19048	0	9	0	1052	0	18107332	07-16 06:00
140.115.158.1	0	21160	0	10	0	1052	0	20114631	07-16 05:40
140.115.158.1	0	19011	0	9	0	1052	0	18071951	07-16 05:20
140.115.158.1	0	21167	0	11	0	1051	0	20120796	07-16 05:00
140.115.158.1	0	21154	0	10	0	1052	0	20108956	07-16 04:40
188.165.239.1	0	5	3260	57181	48	45	5382	111938	07-16 04:30
163.25.122.24	1	1390	12	38	73	1476	14038	942052	07-16 04:20

國立中央大學 電算中心

File Edit View History Bookmarks Tools Help

PA-5060

https://192.192.227.33/#network:vsys1::network/network-profiles/zone-protection

Most Visited Getting Started

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

Commit Save

Help

Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
QoS
Network Profiles
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile

	Flood Protection					Reconnaissance Protection		
Name	SYN Flood	UDP Flood	ICMP Flood	ICMPv6 Flood	Other IP Flood	TCP Port Scan	UDP Port Scan	Host Sweep
☒ Flood_Protect	☒	☒	☒	☒	☒			

Zone Protection Profile

Name: Flood_Protect

Description:

Flood Protection

☒ SYN

Action: Random Early Drop

Alert (packets/sec): 100000

Activate (packets/sec): 180000

Maximum (packets/sec): 180000

☒ ICMP

Alert (packets/sec): 100000

Activate (packets/sec): 160000

Maximum (packets/sec): 160000

☒ ICMPv6

Alert (packets/sec): 100000

Activate (packets/sec): 160000

Maximum (packets/sec): 160000

☒ Other IP

Alert (packets/sec): 100000

Activate (packets/sec): 150000

Maximum (packets/sec): 150000

☒ UDP

Alert (packets/sec): 100000

Activate (packets/sec): 140000

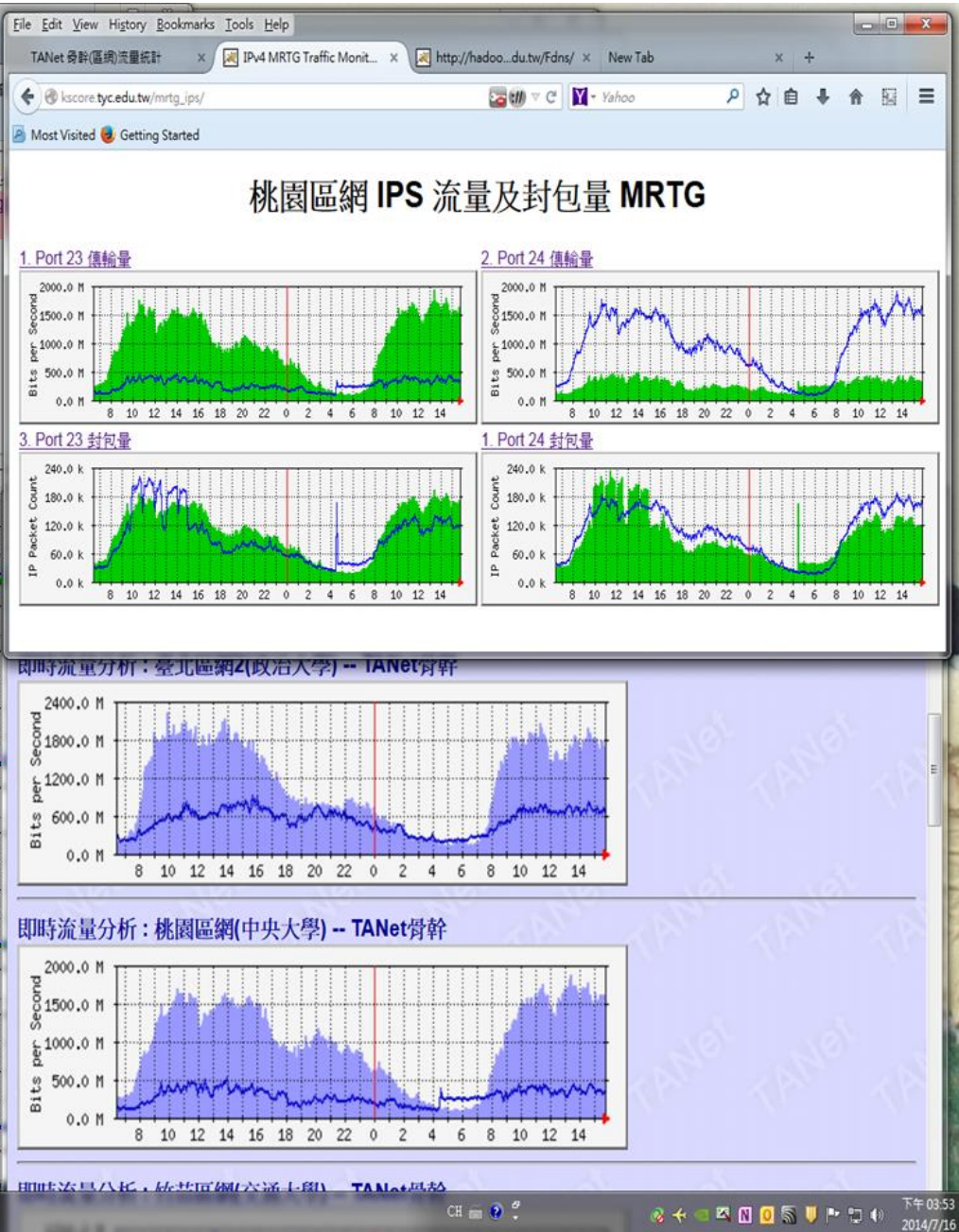
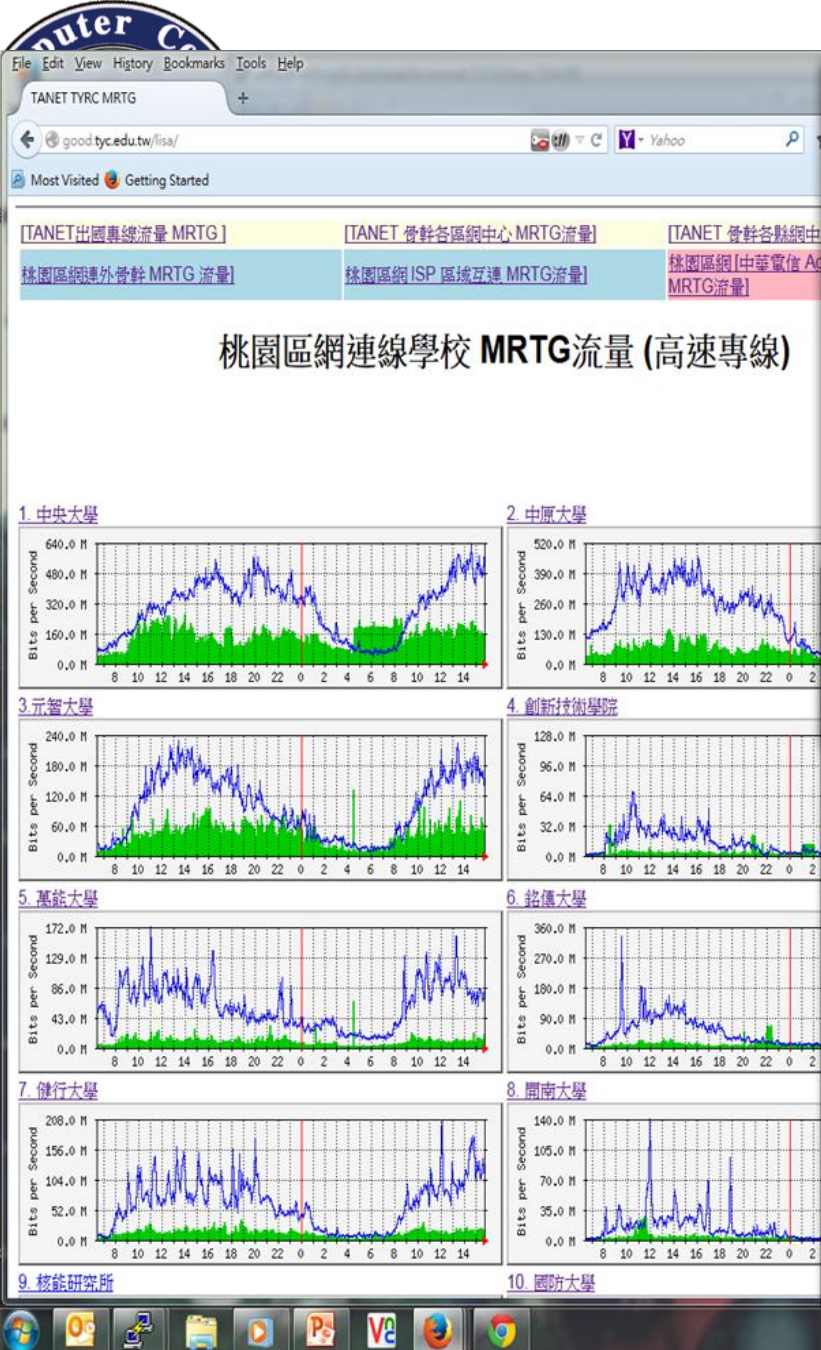
Maximum (packets/sec): 140000

OK Cancel

+ Add - Delete Clone

admin | Logout

Tasks Language Alarms





7. 結語

□ 校園網路（中央大學例）

- Resource 耗損
 - IPS/Router/Firewall Overload
- 連線速度超級慢
 - BW, Connections,
- 校內主機 大量 crack 成群主機 accounts

□ 區域聯防

- 連線 機關/學校
- 外部攻擊(非 tw. Domian)
 - 即時攔阻 Blocking, 自動開單 Notification





6. 結語 (cont.)

□ TANET 整體 布局

➤ TANET 出國連網 ***

- IPS/Router/Firewall Resource 耗損
- 連線速度超級慢
- 外部超量攻擊 攔阻 (非 tw. Domian)

➤ 主要 區網/縣網中心

- Mongo DB cluster
 - Shard_tyrc, shard_moe,
- Data Mining
 - 即時攔阻 Blocking, 自動開單 Notification



6. 結語 (cont.)

- Cloud-based FDS
 - 提供具體的flooding attack records
 - 參考 Netflow 原始紀錄
 - 調整 IPS protection 機制 之依據
- IPS protection
 - Vulnerability limitation
 - 不斷進化的攻擊 traffic
 - Packet limitation
 - Zone Protection



Computer Center, National Central University.



Thank You!