Network Monitoring On Large Networks

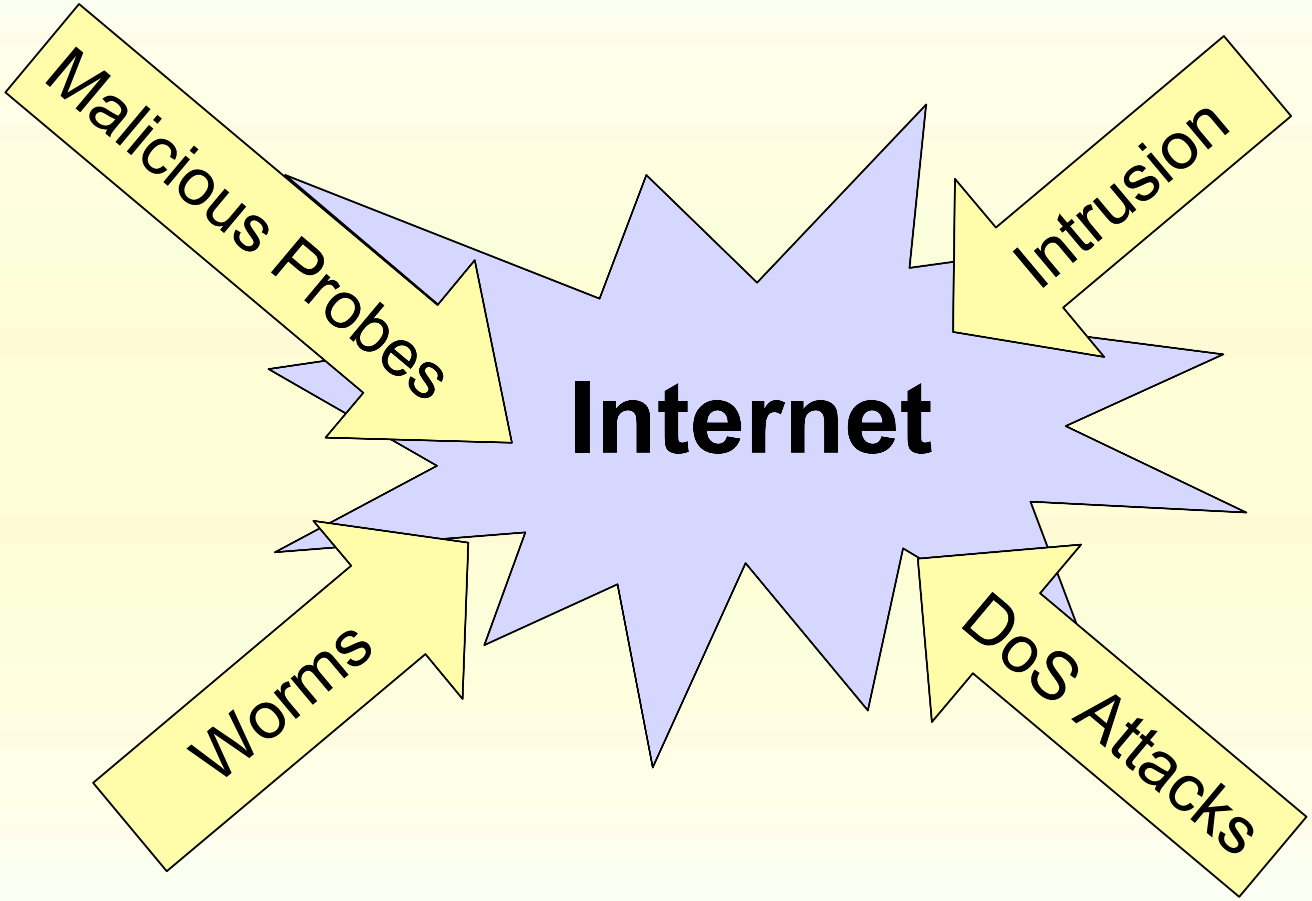
Yao Chuan Han (TWCERT/CC)

james@cert.org.tw

Overview

- Introduction
- Related Studies
  - SNMP-based Monitoring Tools
  - Packet-Sniffing Monitoring Tools
  - Flow-based Monitoring Tools
- The Proposed Mechanism
- Results
- Conclusion

Introduction



- Network security has become one of the most important issues on the Internet.

Real-time network traffic monitoring

- ❑ Provide the status and the patterns of network traffic.
- ❑ Provide the signs of abnormal traffic and potential problems.
- ❑ Detect the irregular activities.
- ❑ Identify the possible attack.
- ❑ Response the situation in time.
- ❑ Evidence of intrusions.

SNMP-based tools

- Collector:collect SNMP data.
- Grapher:generate HTML output containing traffic loading image.
- Provide a live and visual representation of network traffic and traffic trends in time-series data.
- Only provide information about levels and changes in traffic volume.
- Need more detailed data.

Packet-Sniffing tools

- Capture the traffic packets.
- Decode the packet header fields.
- Dig into the packet for more detailed information.
- Provide details on packet activity, but lack information on global network activities.
- Lack high-level management supporting.

Problems

- Timely analysis and storing large volume of data sometimes can be impractical.
- Breakdown: when traffic is too heavy to handle with.
- Tools: designed for detecting individual event, not monitoring overall network traffic condition.

Solutions

- ❑ Develop a new network monitoring method and build a practical system.
- ❑ Examine real time network utilization statistics.
- ❑ Look at traffic patterns.
- ❑ Perform early detection of worm propagation and DoS attacks.

Related Studies

- ❑ SNMP-based tools (MRTG)
- ❑ Packet-Sniffing tools (ntop)
- ❑ Packet-Sniffing tools (IPAudit)
- ❑ Flow-based tools (NetFlow)

SNMP-based tools (MRTG)

- MRTG:Multi Router Traffic Grapher
- Generate HTML page including traffic statistics images, provide a live and visual representation of network traffic.
- Keep all collected data to a log.
- Contain all data over last 2 years, logs does not grow unlimited.
- Monitor network traffic and other dynamic information.

Packet-Sniffing tools (ntop)

- Capture packets, and decode the packets to show network usage.
- Management: traffic measurement and monitoring, network optimization, network planning.
- Database support: long-standing network monitoring and problem backtracking.
- Reports: web mode, interactive command line mode.

Packet-Sniffing tools (IPAudit)

- Record the network activities on a network by host, protocal, and port.
- Listen to the network device in promiscuous mode.
- Monitoring intrusion detection, bandwidth consumption, and DoS attacks.
- IPAudit-Web: web based network reports.

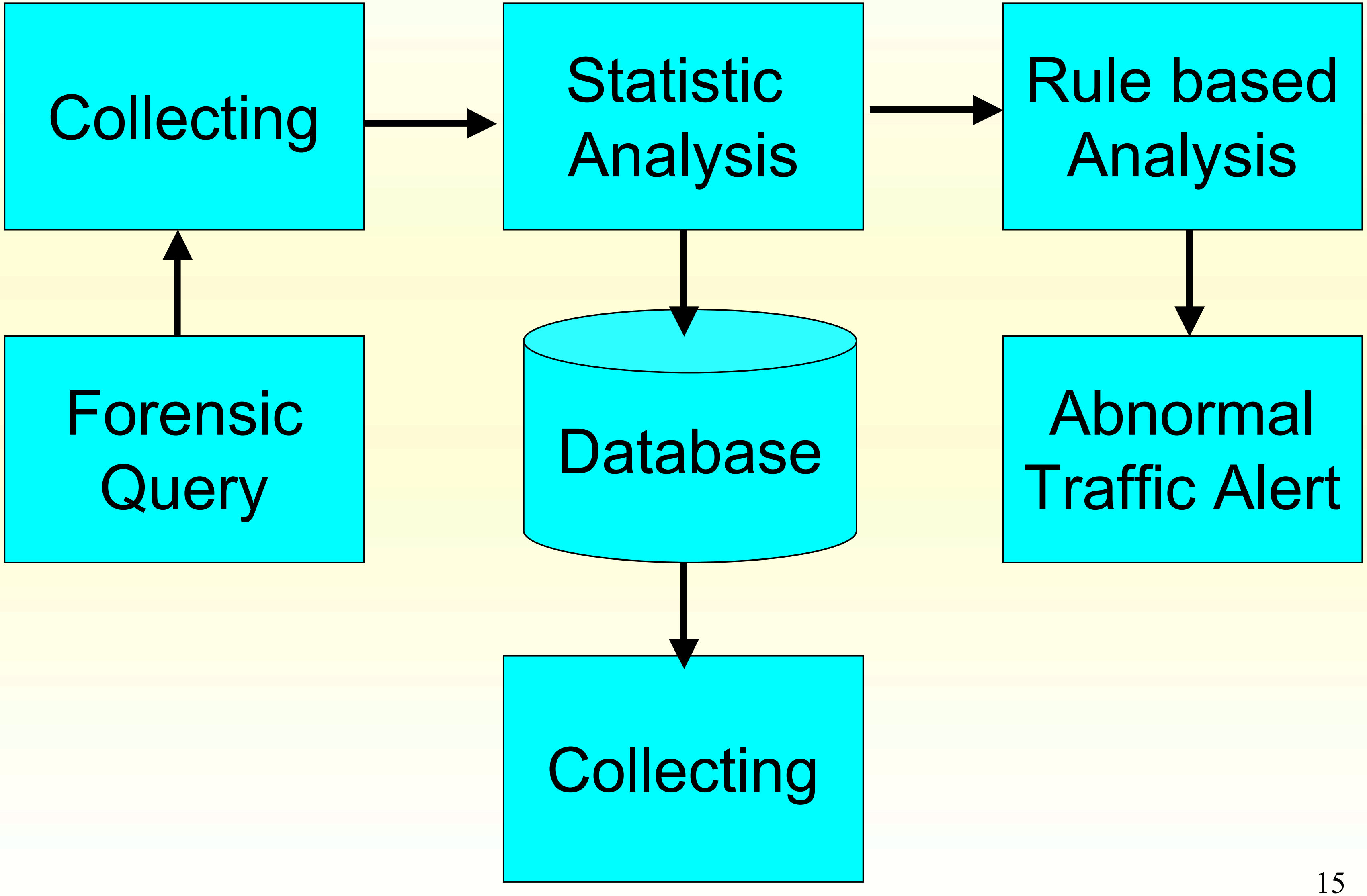
Flow-based tools (NetFlow)

- Network flow: a unidirectional sequence of packets between given source and destination network endpoints.
- NetFlow: provide the measurement for the flow-based network analysis.
- A unique flow: source/destination IP, source/destination port, layer 3 protocal type, type of service, input logical interface.

Flow Expired

- Idle for a specified time.
- Long-lived flows are expired. By default this is set at 30 minutes.
- The cache becomes full, and so heuristics are applied to age groups of flows to expire and export those flows.
- The TCP connection associated with the flow has reached its end (FIN) or has been reset (RST).

The Proposed Mechanism



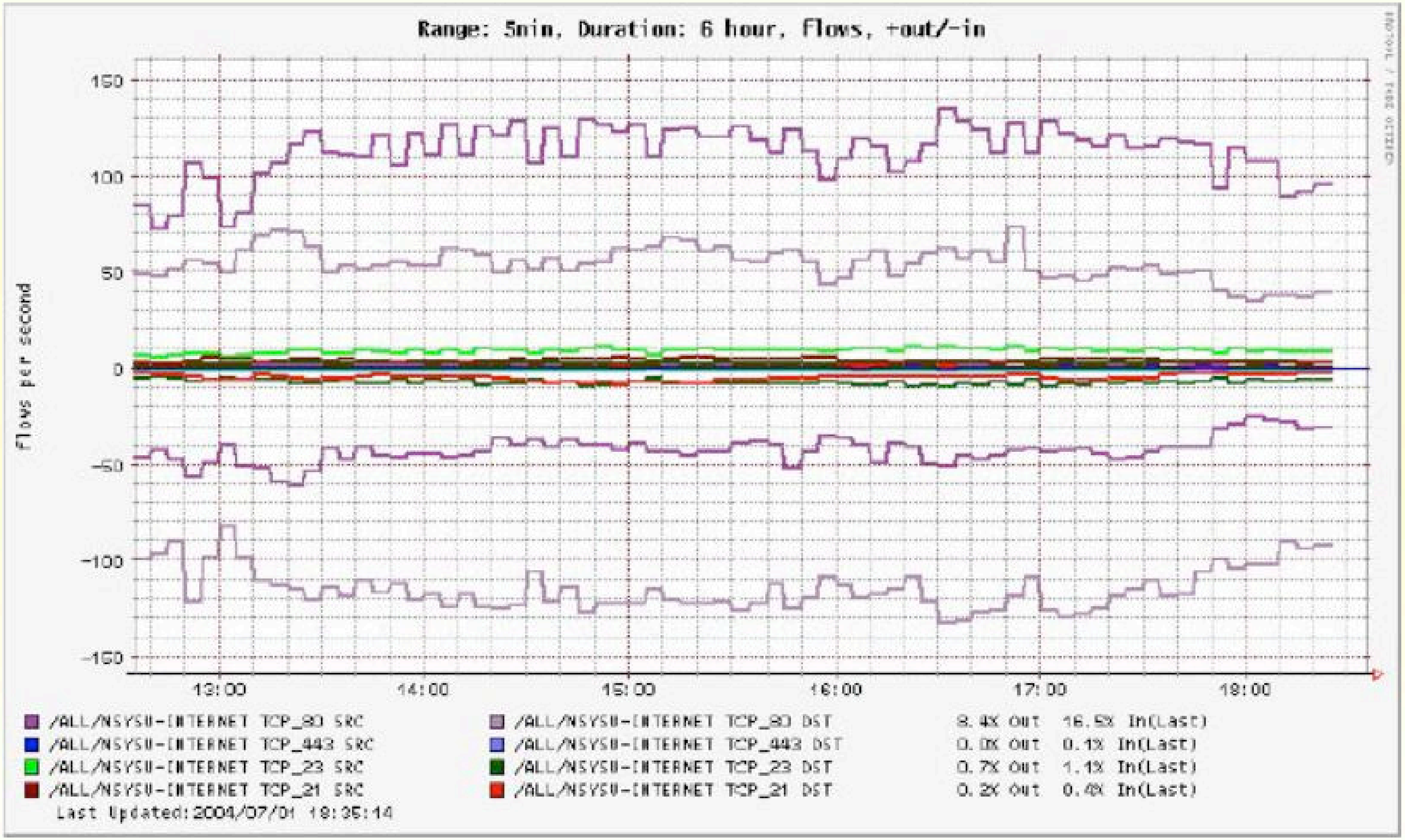
Collecting Module

- Capture the UDP Packets.
- Store the NetFlow Records.
- Rotate the records into the disk for further analysis.
- Records might occupy large space.
- Disk size should be carefully chosen.
- RAM Disk: accelerate the speed of the analysis.

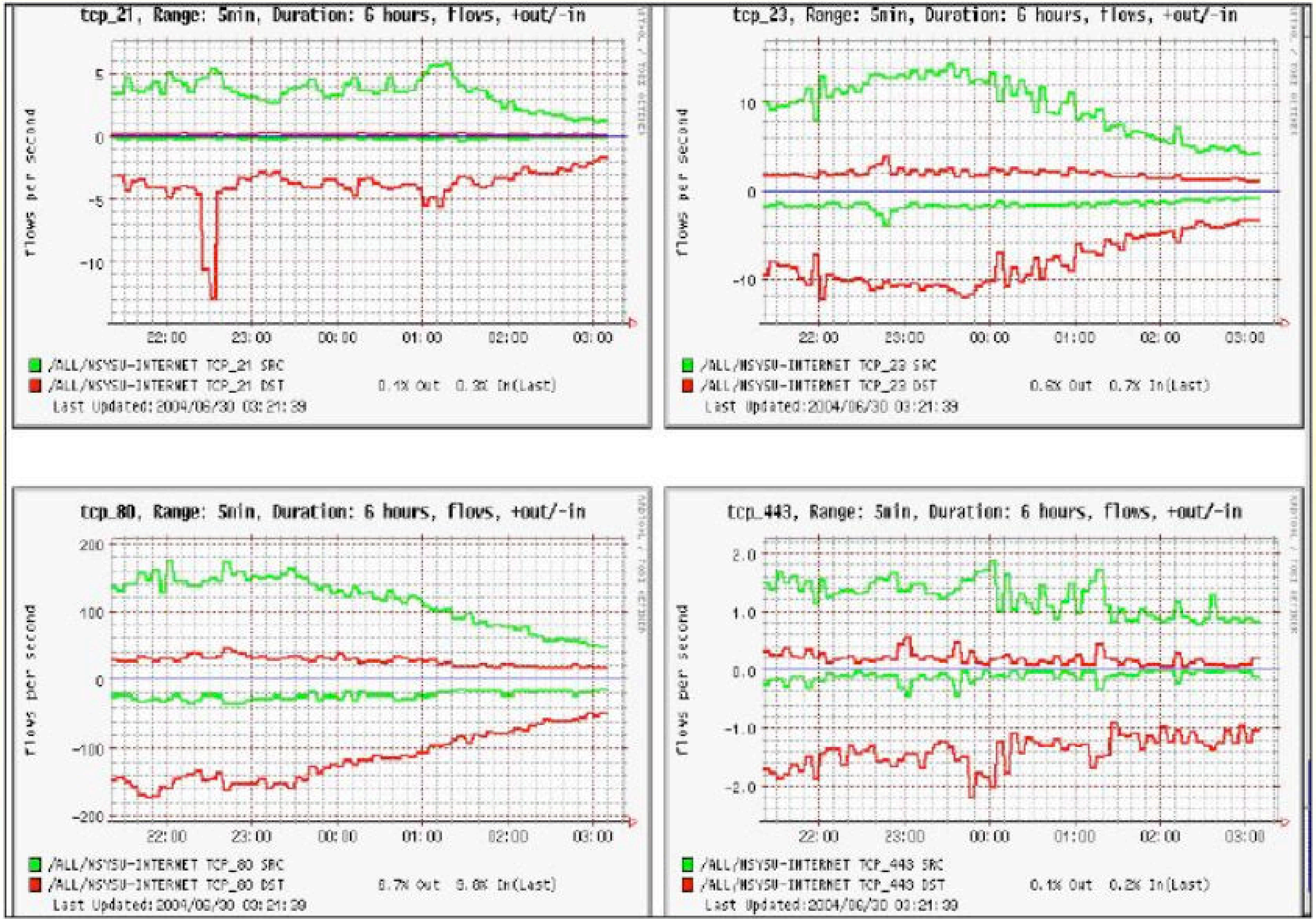
Statistic Analysis Module

- ❑ Examine each flow, maintain the counts of the attribute values.
- ❑ Summarize and store the statistics into the database.
- ❑ Information is shown in visual graph in web pages.
- ❑ Summarized information should be plotted into separate graphs.

Graph with aggregation



Graph without aggregation



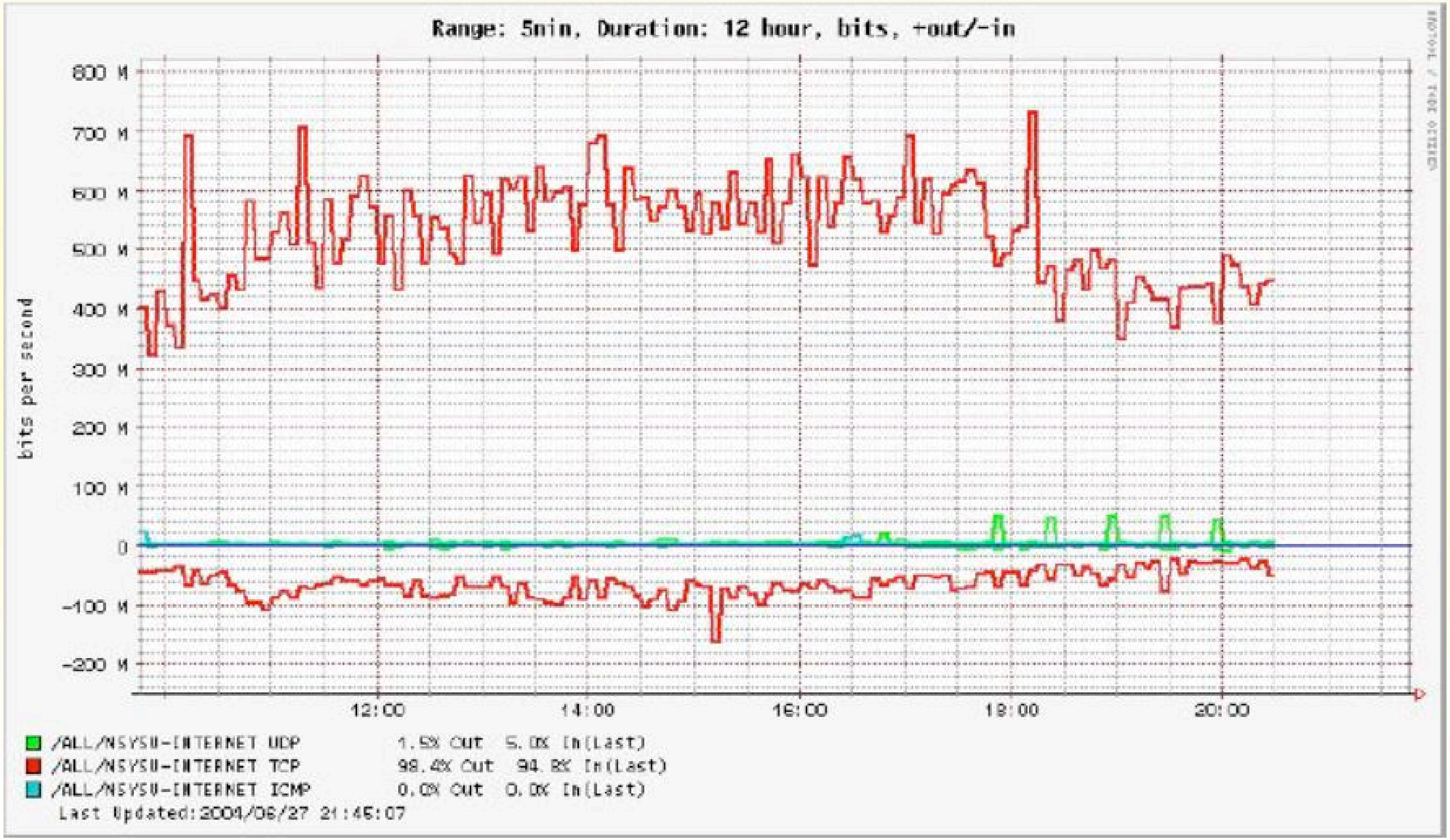
Rule Based Analysis Module

- ❑ Establish rules to alert the attacks.
- ❑ Attacks often have the patten.
- ❑ System will collect abnormal amount of the flows with this pattern.
- ❑ System needs to know the worm behavior prior to discover the worm activities.
- ❑ Establish the filtering rules.

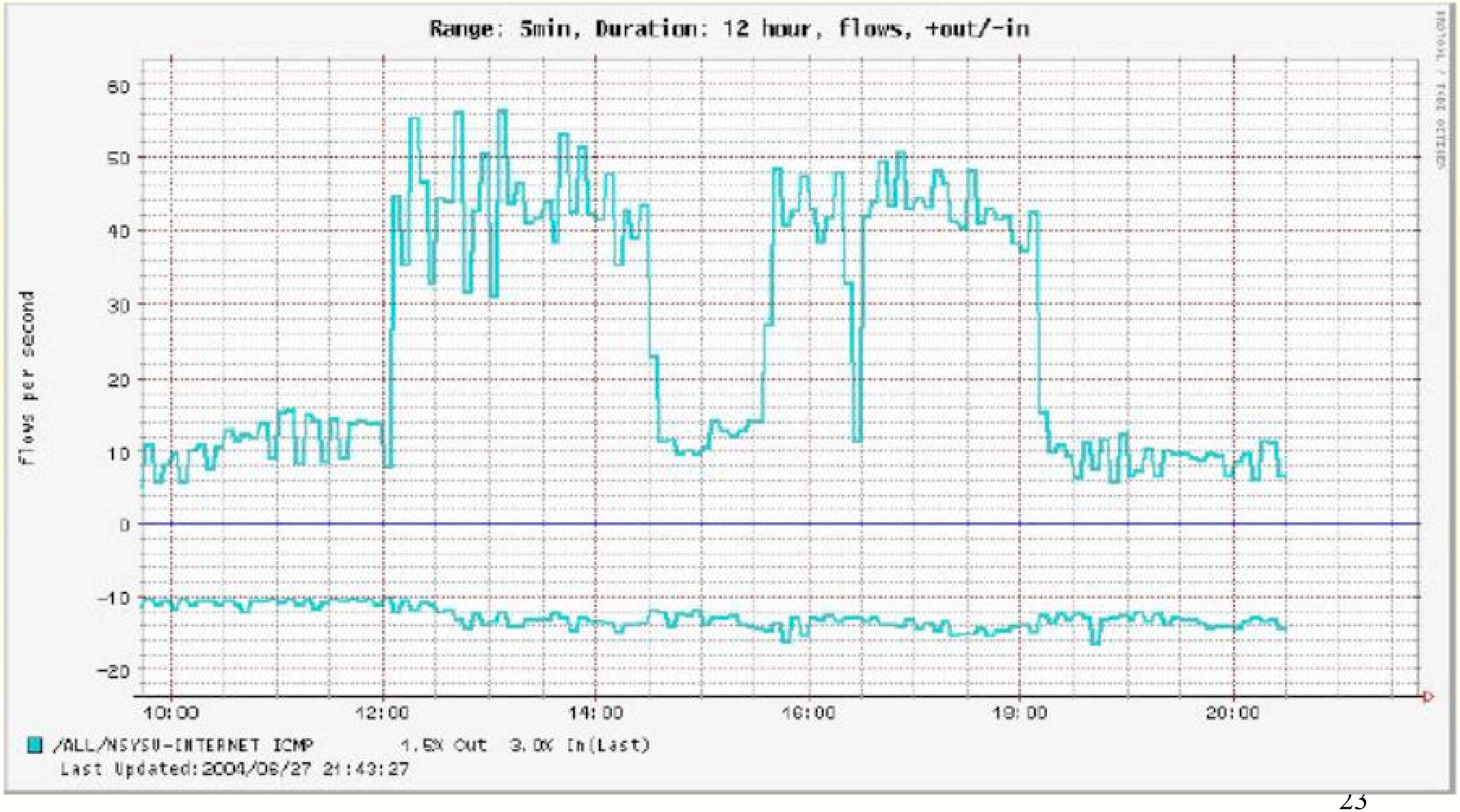
Results

- Results on Traffic Monitoring
  - Traffic volume of the IP protocols
  - Flow graph of the ICMP protocols
- Results on DoS Attacks Detection
  - Flow graphs of TCP port 22
  - Flow graphs of TCP port 44

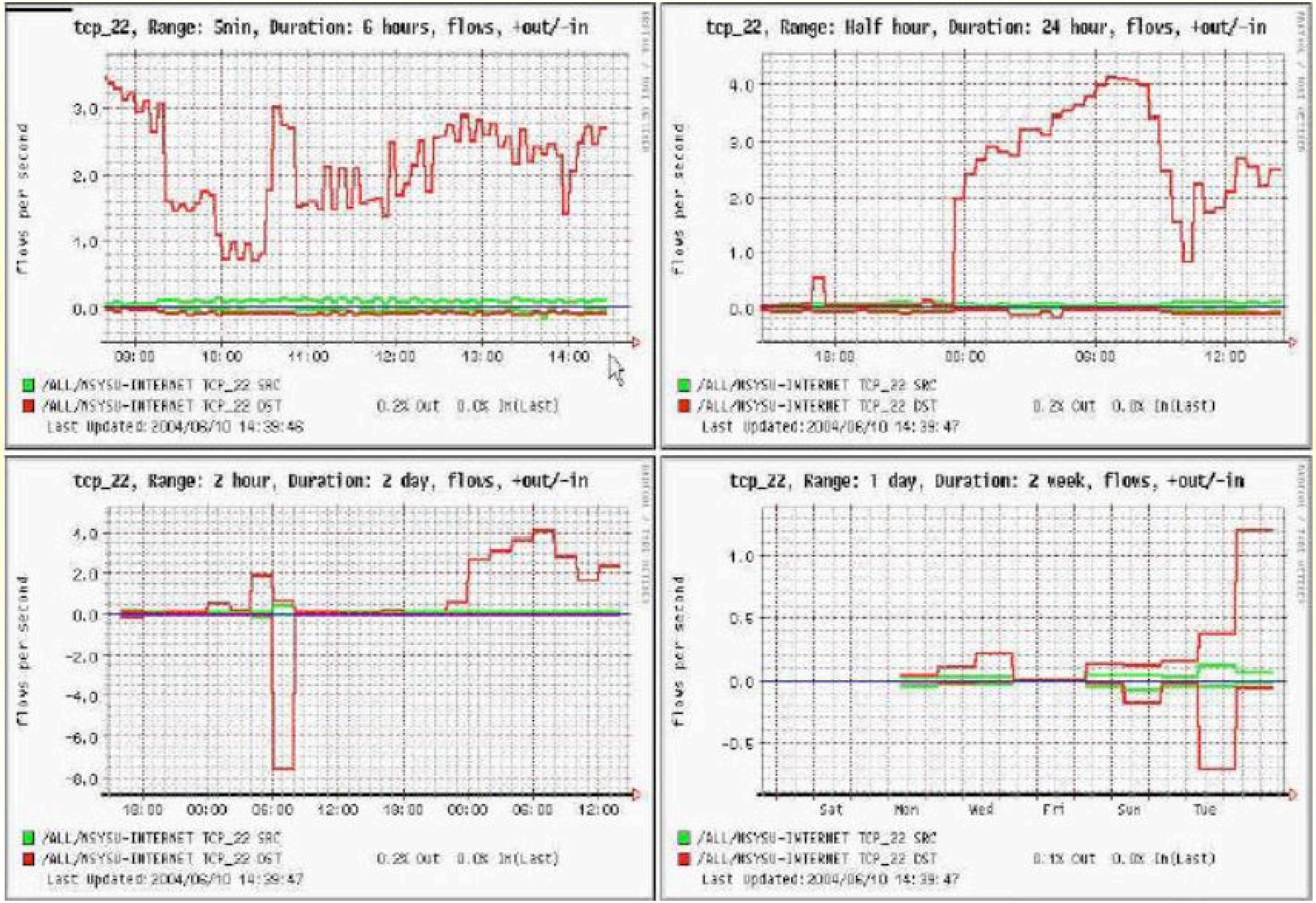
Traffic volume of the IP protocols



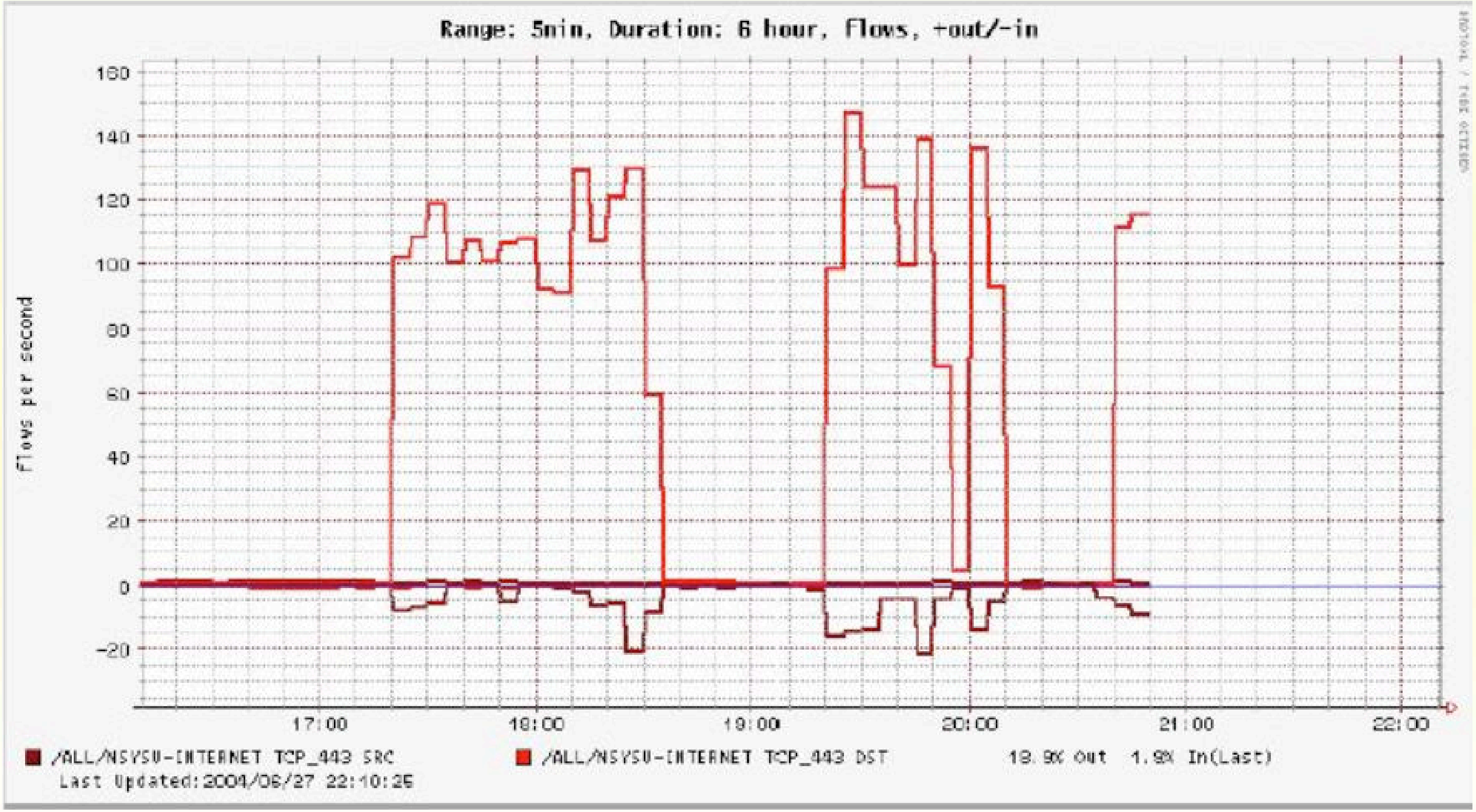
Flow graph of the ICMP protocol



Flow graphs of TCP port 22



Flow graphs of TCP port 44



Conclusion

- Shorten the management time in a large network.
- Find the malicious activities in progress as soon as possible.
- Monitor a large network in real-time.
- Separate flow graphs is easier to identify anomaly.
- Rule-based: filter well-known worm or DoS attacks.