HEPiX Fall 2012 Workshop

Contribution ID: **4**

Type: **Presentation**

ZNeTS: log your network traffic !

Wednesday, 17 October 2012 09:25 (25 minutes)

ZNeTS is an acronym for "The Network Traffic Supervisor". It is a tool for monitoring and recording machines traffic during months.

ZNeTS is a network tool for network introspection and a response to the legal need, in France, to store one year traffic traces.

ZNeTS is very easy to deploy whatever the architecture of your network.

ZNeTS identifies compromised local machines (by virus, trojans, abusive or illegal usage, DNS or Mac spoofing, etc…).

ZNeTS graphical interface is intuitive and ergonomic. Integrated metrology features offer two levels of details. Alerts are simple and relevant.

Over the last 6 month, the tool has been successfully deployed as an appliance into all the IN2P3 laboratories (the french national research institute in physics) and we gave very positive feedbacks from the System administrators.

Summary

ZNeTS is a powerful and easy tool for monitoring LAN, parts of LAN and machines. It has been developed for the CNRS (the french national research institute).

The purpose is:
- The acquisition and conservation of inbound and outbound network flows (during many months or years… even on very high speed networks)
- Research and filter data, with an integrated search engine
- The detection of anomalies causing the generation of alert and optional email sending
- Metrology, with the calculation and visualization of hourly and daily statistics of the overall traffic and detailed traffic (for each subnet, and machine on the LAN).

ZNeTS is very easy to deploy. It was developed in C++ and includes a web server that implements HTTP/1.1 standard (RFC2616). Authentication by login / password or certificate-X509 is also possible.

The web interface based on the Dojo framework is particularly ergonomic and allows the interpretation and visualization of data. ZNeTS is suitable for all network architectures. It is able to acquire not only the data from NetFlow probe (netflow mode), but also directly from a physical interface (sniffer mode). It is able to decode most versions of NetFlow and IPFIX. It supports IPv4 and IPv6. Packages have been built for most Linux distributions.

ZNeTS is not just a collector. It uses optimized flows that are re-aggregated during a adjustable period of time (from 1 minute to 1 hour). ZNeTS may even send its flows to another collector (and then behaves as a NetflowV9 probe)

The graphical interface is intuitive and ergonomic. Metrology offers two levels of detail. Alerts are simple and relevant (based on counting algorithms). Access to the network flows is easy, the selection forms are pre-filled automatically after each interaction. 2 clicks on charts or on an alert report are enough to see the corresponding flows.

Primary author: Mr DESCOMBES, Thierry (CNRS IN2P3)

Presenter: Mr DESCOMBES, Thierry (CNRS IN2P3)

Session Classification: Security and Networking

Track Classification: Security & Networking