

Case Study

OSSIM and Campus Party™

A high traffic, heterogenous network.

Telefonica and OSSIM harden the 2007 Campus Party™

For the first time 4Gigabit traffic has been analyzed using OSSIM in a real-world environment.

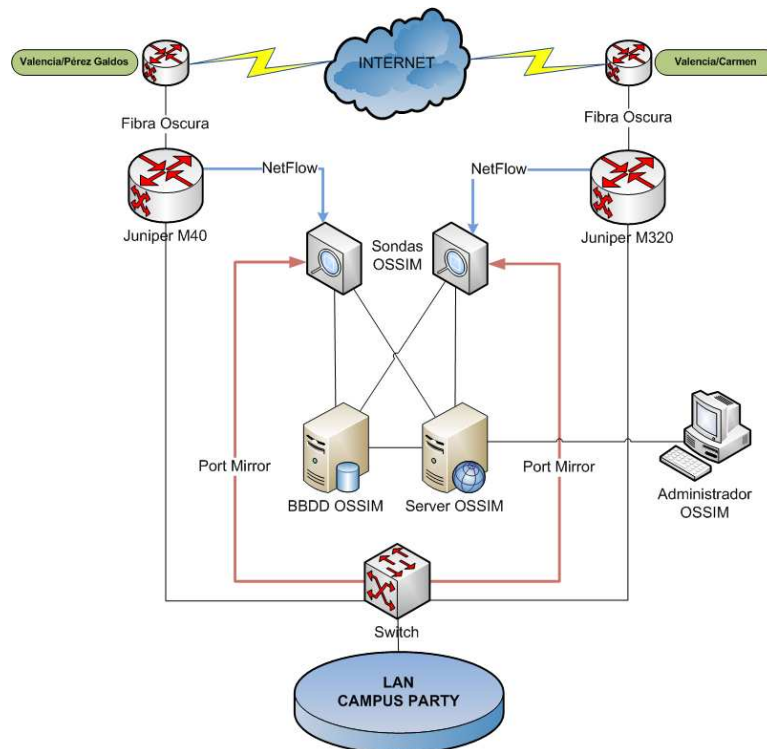
Madrid, October 30th 2007

Telefonica's Chief Operational Security Area has been put in charge of hardening the Campus Party™ at Valencia. For the first time ever a "high performance" security environment has been setup, since *proof was that previous editions had suffered attacks and sabotage attempts that affected the networks performance.*

For OSSIM, the security platform that groups more than 15 security elements such as network intrusion detection systems, anomaly detectors, vulnerability scanners, correlation engines and various realtime network and security detection and monitorization systems, having a sustained 4 Gigabit network traffic was also a new and interesting experience.

Deployment

A high availability installation was performed as shown on the graph below.



High traffic optimization

Various optimizations were accomplished in order to maximize the sensor's and database performance.

The kernels were compiled on 64 bits as was all the included software, *device polling* was disabled on network cards and a *ringbuffer* was put in place to maximize network capture performance.

Due to the very high network traffic, “ntop” was setup so it received its information via “netflow” from the routers, grabbing a representative amount of traffic for further analysis.

High volumen event correlation and data storage

In order to be prepared for an estimate of a hundred million events a day, two separate correlators were put in place so we could ensure high availability.

Storage was optimized for a hundred million simultaneous events inside the active table. A RAM “mirror” was created and data was injected simultaneously into RAM DB and stored on disk.

Fast Learning and Fine Tuning

One of the biggest challenges, since the project was limited to one week, was to quickly tune and adjust events and false positives, as well as getting the anomaly detectors to learn faster than usual.

The new real time event viewer came in very handy for this task, allowing for real time analysis of detected events

Anomaly detectors were adjusted to security-relevant ports using a high threshold, as an environment like the one Campus Party™ required.

Results

This supervision task, which managed to analyze the traffic at every moment, even at peak times, allowed to successfully detect and block both external attacks as well as internal network misuse.

José María Rodríguez, Technical Director at Campus Party™, concluded that the result had been very positive since “*it guaranteed network performance in such a challenging environment*” and confirmed that a similar system will be in place at future Campus Party™ editions.

“I would like to highlight the work of the security people from Telefonica. Now we are wondering how we could have done Campus Party™ without them”.

Upcoming editions will be held at different places in the world. The next one will be at Sao Paulo, Brasil, on February 2008.

For more information:

Chief Operational Security Area: Javier.Diaz-PalaciosSisternes@telefonica.es

OSSIM Security Platform : <http://www.ossim.net>