Customer

Industry

Research & Education

Challenges

- *Quick troubleshooting in vast decentralized network environment*
- *Fast detection of security incidents such as attempts to crack passwords*
- *Detection of large-scale security incidents*
- *A lot of VLANs, public and private subnet mix in every department*
- *Network under reorganization and modernization*

Deployed products

- *Flowmon Collector*
- *Flowmon Probes*
- *Flowmon ADS*

Benefits of the solution

- *Full IPv4/6 traffic visibility*
- *Automatic detection of attacks on network services*
- *Evidence of misuse in university network*
- *Higher visibility in complex network with easier modernization process and change management*

Contact

www.pw.edu.pl

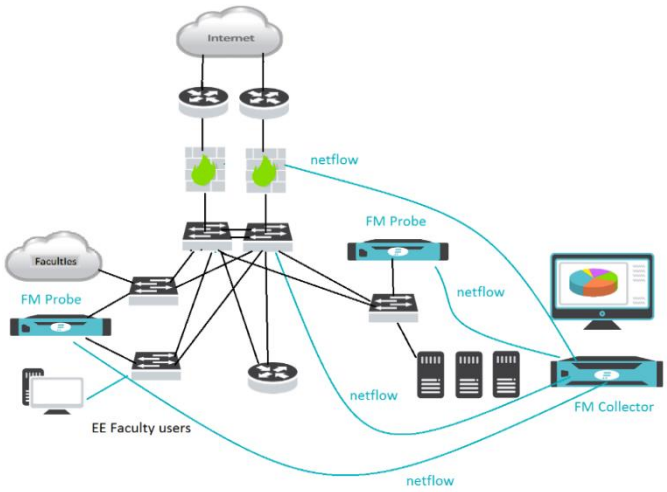
Warsaw University of Technology

Warsaw University of Technology was established in 1826. Now with over 37 thousand students it is the best technical university in Poland and one of the best universities in Central Europe. Currently, there are almost 2 600 academic teachers and nearly 2 200 non-academic employees. Warsaw University of Technology comprises 148 buildings with 320 laboratories and IT facilities with 5 200 computers.

Customer situation

Warsaw University of Technology has an extensive campus with many remote locations throughout Warsaw. The core network is based on 10 Gbps infrastructure. As many research projects are conducted, every department has several private subnets with public connectivity. This situation brings problems with overall network traffic visibility and detection, and localization of security incidents.

Deployment of the Flowmon solution



Flowmon solution was implemented in one department in the main campus and can monitor the network traffic of several university departments at the same time. The monitoring solution, employing both Probes and a Collector, is based on virtual appliances. NetFlow information is collected from several distribution switches, allowing a way to monitor communication between users and servers as well as the traffic between departments and the Internet, and through the VPN. Therefore, full visibility into routed traffic is ensured. The Collector stores the flow data for a desired period of time, provides visualization, analysis and reports. It is the central point where the Flowmon ADS (based on network behavior analysis) module is installed for automatic detection of security threats and performance incidents.

Customer review

Grzegorz Świątek, Vice-rector for IT at Warsaw University of Technology, summarizes the Flowmon solution deployment:

"Flowmon can analyze all generated flows and can report network attacks and potentially dangerous events. It also brings visibility of unwanted network communication and safety rules violations. The solution is a very helpful tool to keep all the traffic in our complex network under control."