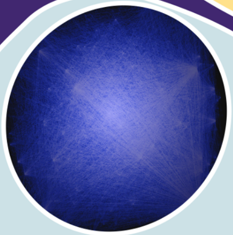
Large Graph Visualization
of millions of connections in the CERN Control System Network Traffic

Luigi Gallerani - CERN
ICALEPCS 2015
MCEC Melbourne

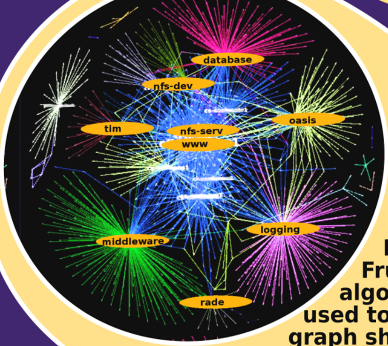
Abstract

More than 60 million IP packets are routed, every hour, between the CERN General Purpose Network and the Control System Network (Tech Net) Around 6000 hosts are involved.
In order to improve the security of the accelerator control system, we want to define firewall and routing rules and to understand the network host and ports relations. Using large graph visualization and clustering algorithms, we created comprehensible graphs of the recorded traffic on routers, reducing the complexity of the problem and showing the real network communication and dependencies. Traffic analysis combined with statistics offer a new approach for firewall rules definition.



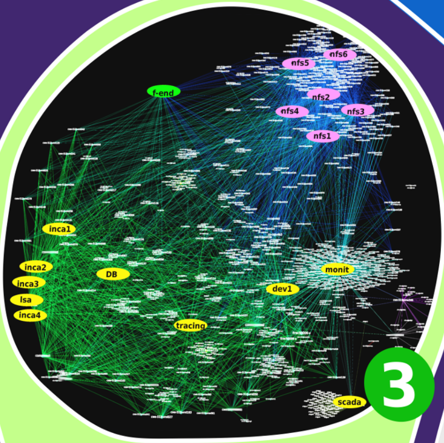
1

One hour of traffic plotted. 60 million connections with random host position gives only an idea of the complexity



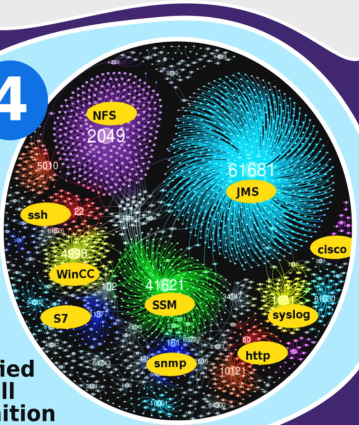
2

Reingold Fruchterman algorithm is used to cluster the graph showing the highly connected hosts. Above, the steps required to compute the full graph



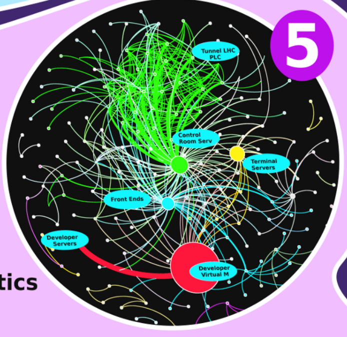
3

Each clusters of machines, identified in the previous step, is re-computed at maximum resolution. Full network dependencies of accelerator developer machines are shown in this graph



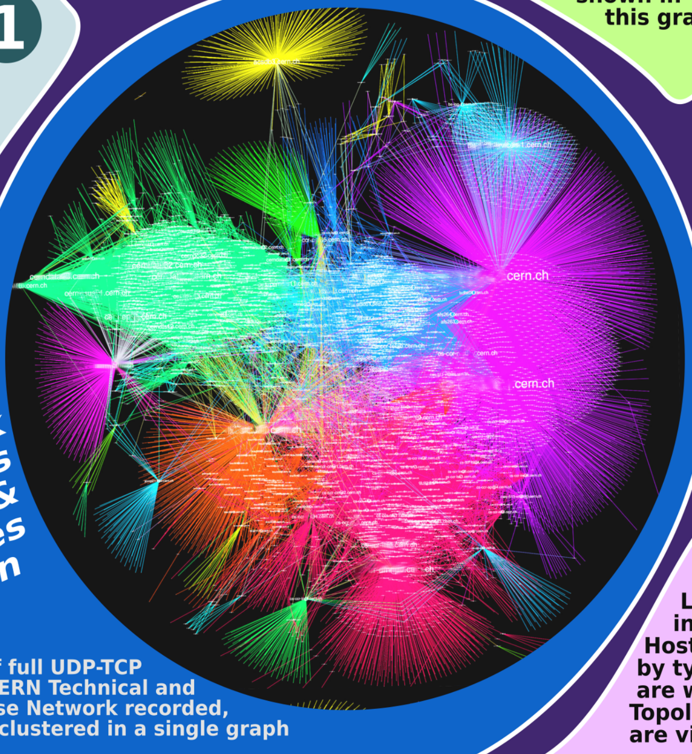
4

Clustering process is now applied to the ports. In this way services are identified and firewall rules definition becomes easier



5

Recorded traffic is combined with the LAN database information. Hosts are grouped by type and edges are weighted. Topology and statistics are visible together



Large graph analysis of network dependencies for routing & firewall rules definition

1 hour of full UDP-TCP traffic between CERN Technical and General Purpose Network recorded, mapped and clustered in a single graph