Scaling-out CERN's IDS System with Network Automation

Openlab Lightning Talk 2019

Author:

Andrea Lacava

andrea.lacava@cern.ch | thecave003@gmail.com

Supervisors:

Stefan Stancu

Edoardo Martelli

Openlab Collaborator:

Extreme Networks

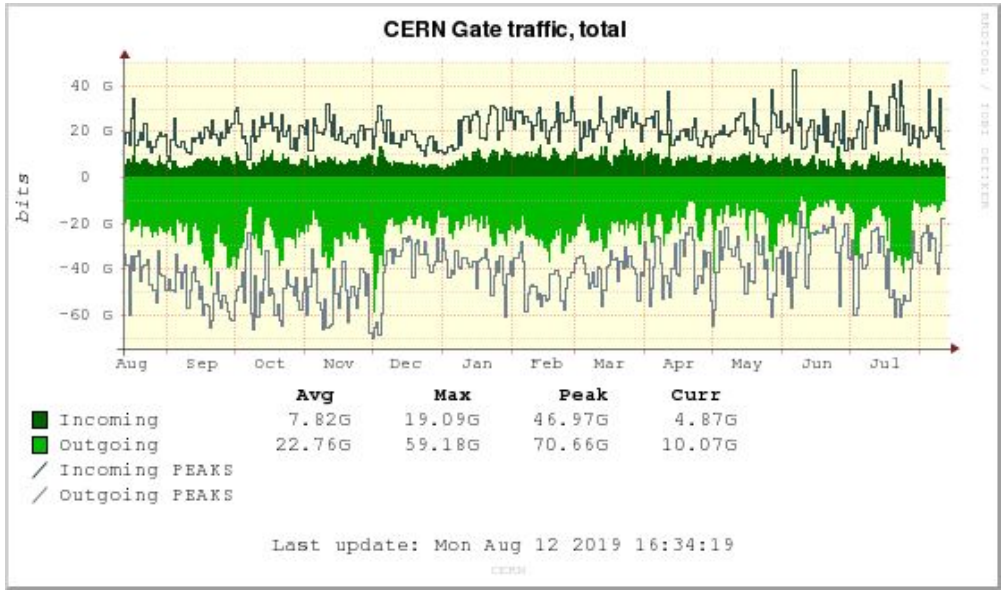
https://www.extremenetworks.com/

August 2019

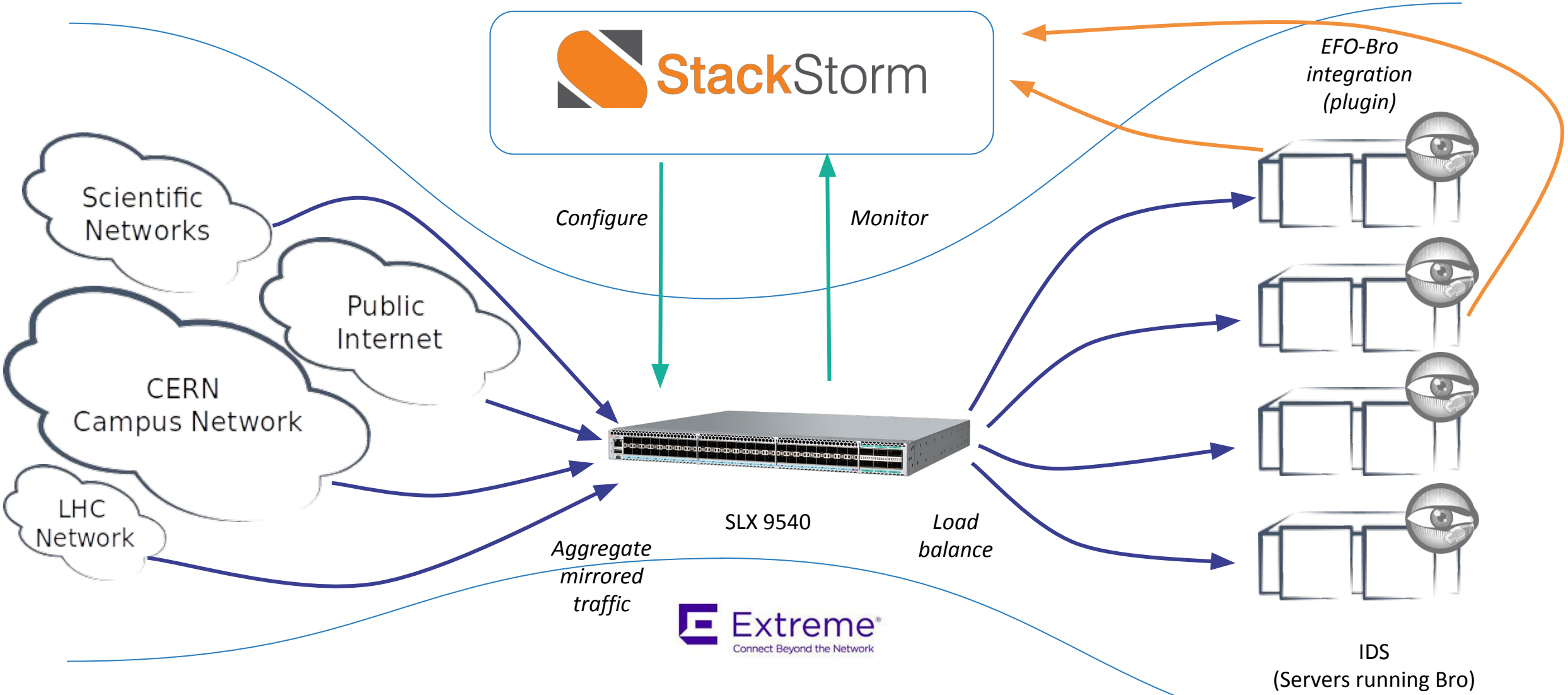
The problem: Keep CERN traffic safe

- The volume of traffic entering and leaving CERN is growing continuously
  - More than 100 Gbit/s incoming and outgoing traffic
  - More than 1 Million simultaneous connections

- Traffic needs to be inspected and analyzed in order to ensure security
  - We already have an Intrusion Detection System
  - Thanks to openlab project with Extreme Networks



Current setup – Limited scalability



StackStorm

aka "IFTTT for Ops"

- Event-driven automation engine
- Open source & Python friendly
- Enables *If This Then That* paradigm for (Dev)Ops
- Modular: users can develop their own Packs.

- ***Pack**: A set of **Rules** triggered by **Events** that runs **Actions***

if an IDS server needs maintenance — *then take it out from the network load balancer*

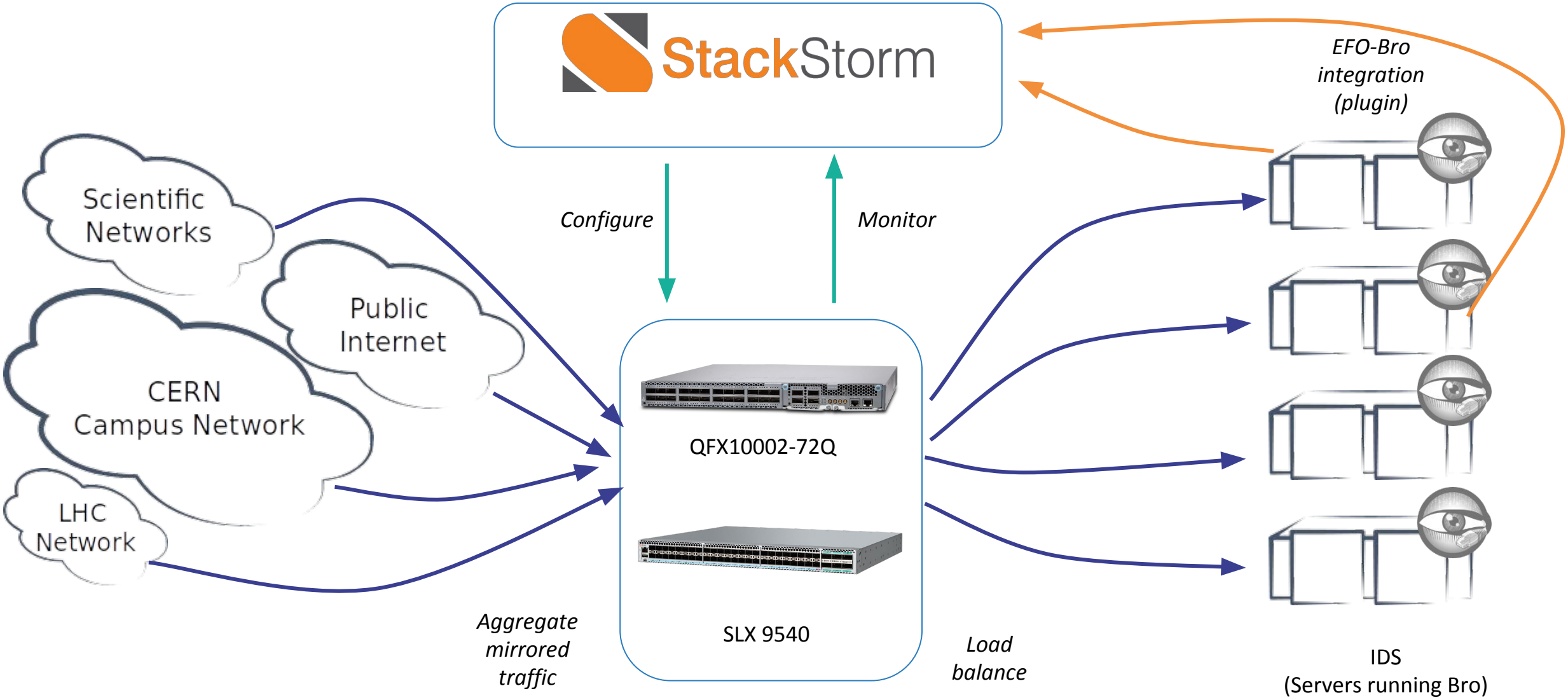
if a known traffic type saturates the IDS server — *then track only connection initiation and termination*

} Actions implemented in CERN IDS Pack

The solution

Multiple vendor support for IDS Stackstorm pack

New setup – scalable



My contribution

- Redesign of the existing Pack for the CERN IDS
  - Added abstraction layer for multiple vendor support
- Refactoring of the existing Actions code for the SLX platform
  - More than 1000 lines of code reviewed and adapted
- Implementation of the same Actions for the QFX platform
  - Also reported a *deployment related bug* in the StackStorm pack engine
- Fully functional prototype using the QFX platform
  - Production deployment foreseen for Q4 2019
- Made good pasta for more than 15 Openlab Students
  - *"Scalable and delicious" (cit.)*

Questions?

andrea.lacava@cern.ch | thecave003@gmail.com

thecave3.github.io/ | www.andrealacava.com