Brocade Flow Optimizer

› 08/12/2016

Openlab Technical Workshop 2016

Adam Krajewski
IT-CS-CE

Background image: Shutterstock

CERNopenlab

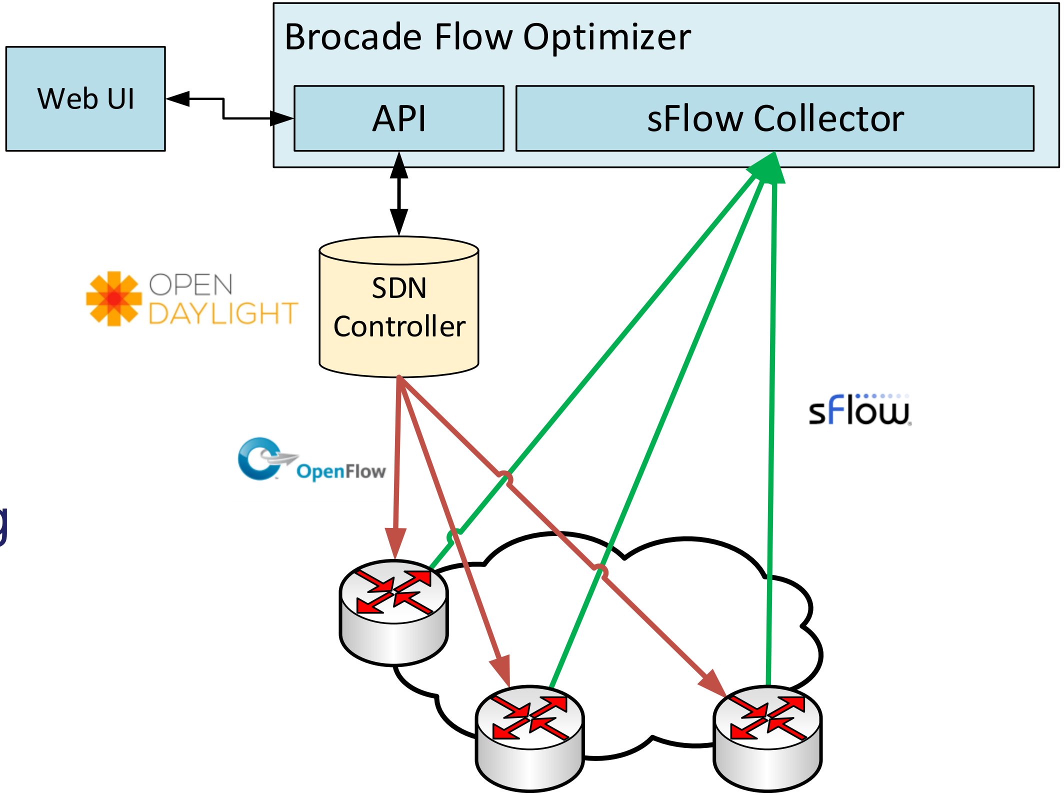
Agenda

- **Project recap**
  - Brocade Flow Optimizer software
  - Project goals
- **CERN contributions to BFO software**
- **SDN-enabled IDS at CERN**
- **Future plans**

Background image: Shutterstock

Brocade Flow Optimizer

- **SDN application developed by Brocade**
  - Provides insight into the network traffic and enables flow steering
  - Dynamic programming of network devices’ forwarding engines with OpenFlow
  - UI + REST API



Background image: Shutterstock

Project overview

- **Collaboration between CERN and Brocade**
  - Started in June 2015
  - Initial goal:
    - Enhance and generalize the Brocade Flow Optimizer (BFO) architecture
- **Current goals:**
  - Adapt BFO to build an intelligent network traffic steering system answering CERN's needs
    - Define use cases and requirements for them:
      - Intrusion Detection System (IDS) mirroring
      - Firewall load-balancing
      - Advanced policy-based routing engine
    - Implement necessary features
  - Enhance BFO software architecture

Background image: Shutterstock

CERN contributions to BFO

- **Fully integrated within Brocade's BFO development team**
  - Involvement in agile sprints
  - Daily stand-ups

- **CERN's contributions to BFO software releases**
  - ~40 JIRA issues resolved
  - 4 feature ownerships
    - Functional specification -> development -> SQA testing
  - Three official releases in 2016

- **IDS use case enabled by CERN's contribution**

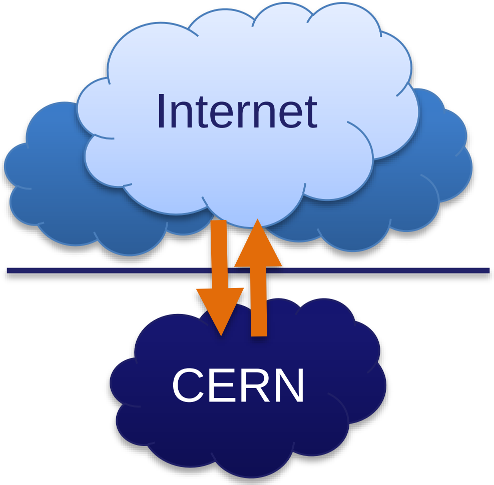
Background image: Shutterstock

IDS at CERN

- **CERN uses an Intrusion Detection System to scan the network traffic for possible security threats**

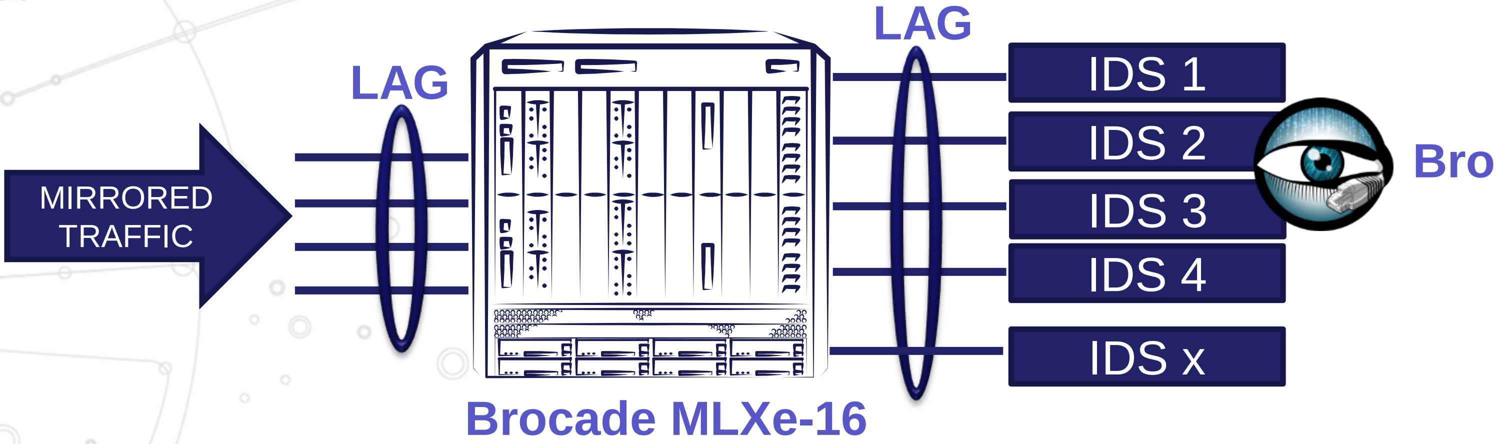
- **The current setup has limited scaling capabilities**
  - Traffic volume at the network boundaries grows continuously

- **A new setup is required**
  - Scale-out capabilities
  - Programmability to implement additional features



Background image: Shutterstock

Planned setup

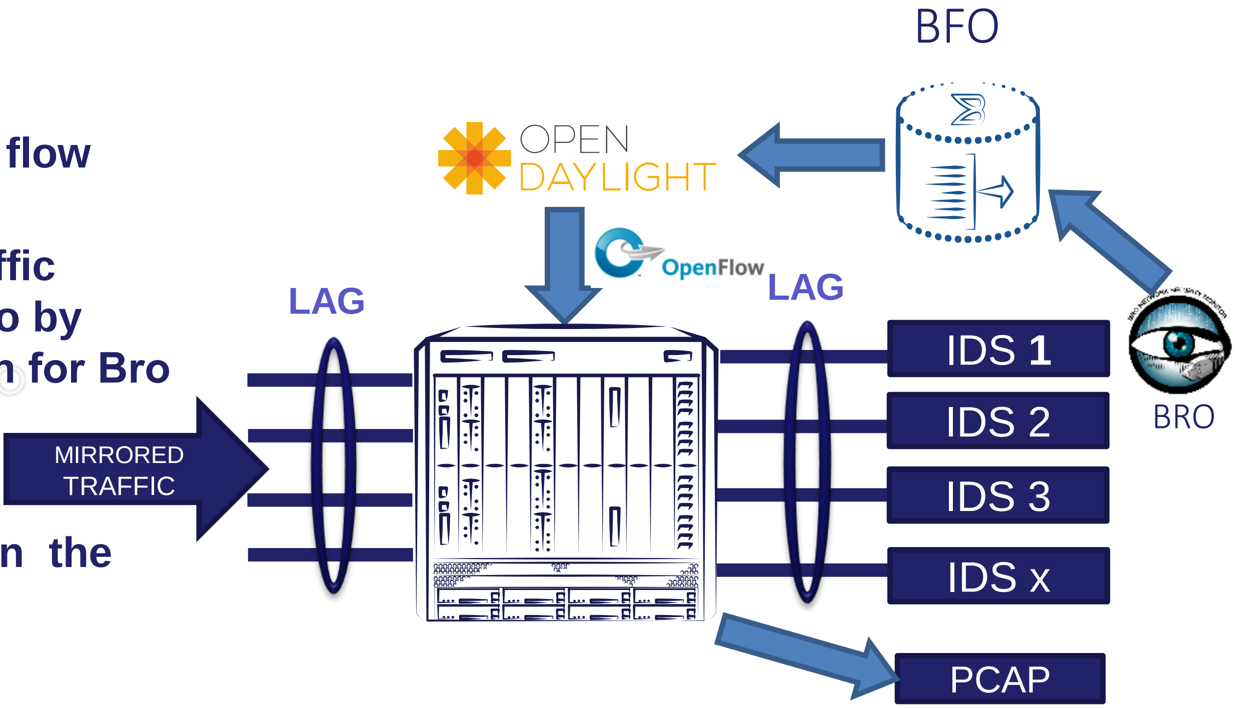


- **The traffic mirrored at the CERN firewall is distributed across a pool of 16 servers, each running the Bro open-source network monitor**
- **Required features:**
  - Symmetrical load-balancing
  - Traffic shunting - filtering out TCP data packets belonging to trusted flows
  - Selective mirroring – mirroring suspicious traffic to a dedicated server for detailed analysis
- **Leverage SDN concept – BFO playing a key role**

Background image: Shutterstock

Full setup and status

- Leverage BFO for dynamic flow programming
- Selective mirroring and traffic shunting triggered from Bro by leveraging the BFO's plugin for Bro



- Prototype setup deployed in the CERN Computer Centre
- Testing on-going
- Promising perspective of production deployment

Background image: Shutterstock

Future plans

- **Finalize IDS prototype validation and proceed with deployment**
- **OpenFlow-based load-balancing in the IDS setup**
  - Improve current static load-balancing with a flexible, software-based solution
- **Further enhancements to support other use cases**
- **Invest more effort into making the BFO architecture extensible**

Background image: Shutterstock