Connect Beyond the Network

# Extreme Flow Optimizer

*Openlab Technical Workshop 2018*

Adam Krajewski

adam.krajewski@cern.ch | akrajews@extremenetworks.com

January 2018

# Project overview (1)

- Initially collaboration between CERN and Brocade
  - Started in June 2015 as a 2-year project
  - Fellow recruited and strongly integrated with Brocade’s software development team
  - Initial goal:
    - Get expertise in the Brocade Flow Optimizer (BFO), a Software Defined Networking application
    - Enhance and generalize the BFO software architecture
- Evolution of 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) automation**
      - Firewall load-balancing
      - Advanced policy-based routing engine
    - Implement necessary features
  - Enhance BFO software architecture

# Project overview (2)

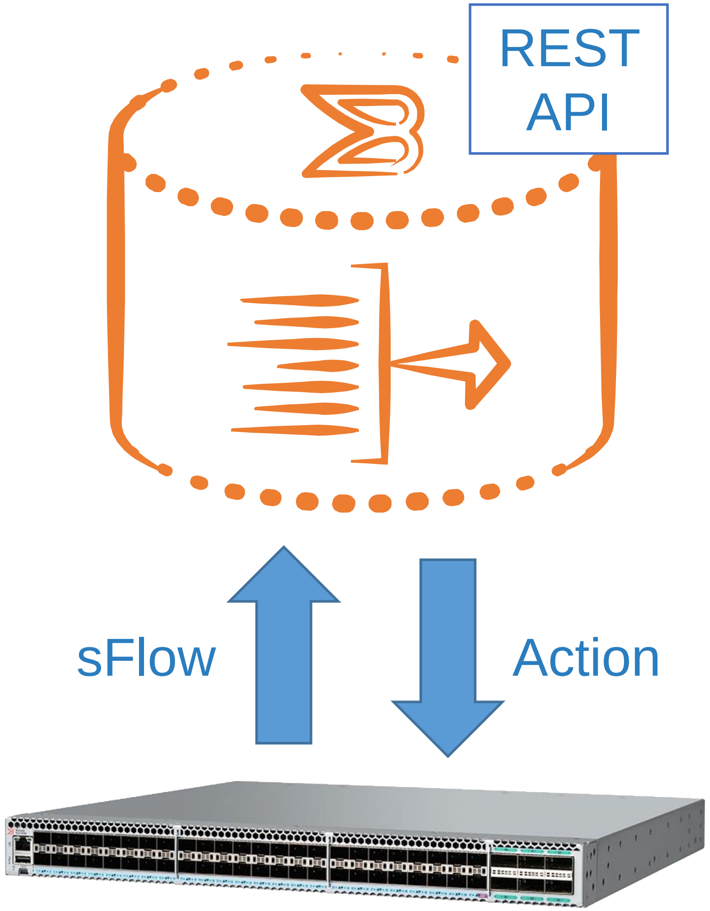
Extreme
Connect Beyond the Network

- Project continuation
  - Brocade acquired by Broadcom; Data Center BU acquired by Extreme Networks
  - Successful project handover and extension for the 3rd year of openlab phase V
  - **Brocade** Flow Optimizer becomes **Extreme** Flow Optimizer (EFO)

- Current goals:
  - Primary focus on the Intrusion Detection System use case
  - Switch SDN focus from OpenFlow to more generic network automation
    - Programmatically leverage proprietary hardware features through open-source platforms
    - Use StackStorm / Extreme Workflow Composer
  - Continue capitalizing on the acquired expertise
    - Further contributions to commercial software development

# Extreme Flow Optimizer (EFO)

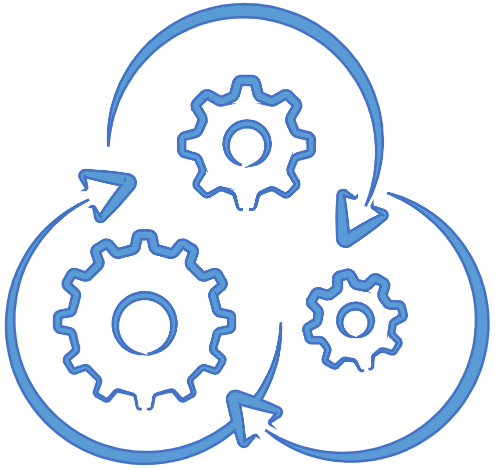
- Software Defined Networking application
- Monitoring large traffic flows and organizing them in a controlled manner
  - Traffic visibility through sFlow
  - Dynamic flow management through OpenFlow or CLI
    - Dropping, redirecting, mirroring, metering… and much more!
  - REST API for northbound integrations
    - Bro plugin developed within the openlab collaboration
- Integration with StackStorm



# StackStorm / Extreme Workflow Composer (EWC)

- Platform for integration and automation across IT services and tools
  - Python-based & open-source
  - https://stackstorm.com/
- Trigger-based workflow execution
  - Sensors listening to events (e.g. syslog)
  - Events translated to Triggers
  - Rules matching Triggers to Actions
  - Workflows grouping Actions together
- Enterprise edition: **Extreme Workflow Composer (EWC)**

StackStorm



Extreme Workflow Composer

# Product contributions

- More than 2 years of regular software development effort
  - Full-stack (frontend + backend) developer
  - Reporting to technical managers and product managers
  - Providing occasional technical expertise for customers in Switzerland

- Commercial feature ownerships (design, development, SQA):
  - Bro Integration
  - Palo Alto Networks Integration
  - Arbitrary Bitmask Support for IPv4
  - IP Blacklisting

- Strategic feature involvement:
  - Application tuning for better scalability
  - StackStorm orchestration for Docker

- Now putting more focus on StackStorm
  - Docker integration
  - EFO integration

# IDS at CERN

- The volume of traffic entering and leaving CERN is growing continuously

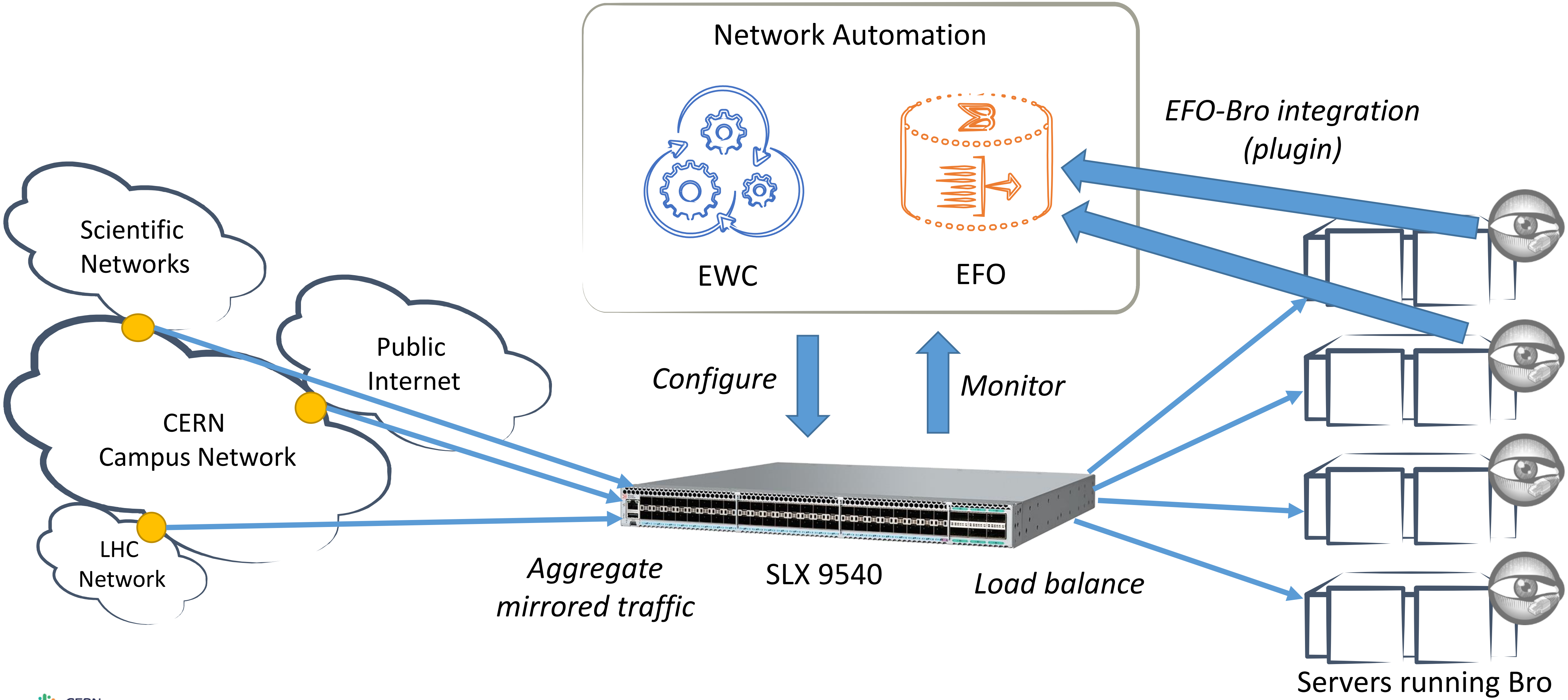
- Precise traffic analysis and monitoring is crucial for network security
  - Cyber security threats can be detected and mitigated

- Building a scalable and extensible IDS system at CERN

- General design principles:
  - Mirror traffic at network boundaries
  - Aggregate and load-balance the traffic across a set of servers
  - Programmatically leverage advanced features of networking hardware

- Advanced features:
  - Symmetrical load-balancing
    - For a given flow, both directions are forwarded to the same IDS server
  - Traffic shunting
    - Offloading the IDS system by blocking data packets of trusted traffic
  - Selective mirroring:
    - Forwarding suspicious traffic flows to dedicated packet capturing servers

# Setup


Network Automation
EWC
EFO
EFO-Bro integration (plugin)
Scientific Networks
Public Internet
CERN Campus Network
LHC Network
Configure
Monitor
Aggregate mirrored traffic
SLX 9540
Load balance
Servers running Bro

# IDS - status and plans

- Proof-of-concept prototype deployed in CERN Computer Centre

- Functional testing continues to ensure the requirements are met

- Continued software development
  - Implementing missing features for the IDS use case

- Production deployment planned for 2018

CERN openlab

Extreme

Connect Beyond the Network

# Extreme Flow Optimizer

*Questions?*

Adam Krajewski

adam.krajewski@cern.ch | akrajews@extremenetworks.com

January 2018