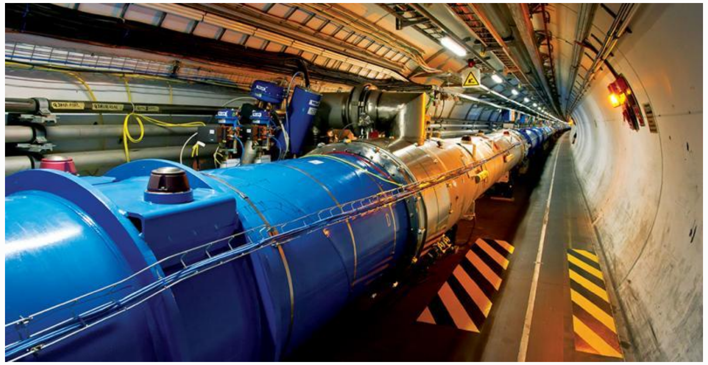
# Intrusion Detection System with Network Automation

Adam Krajewski

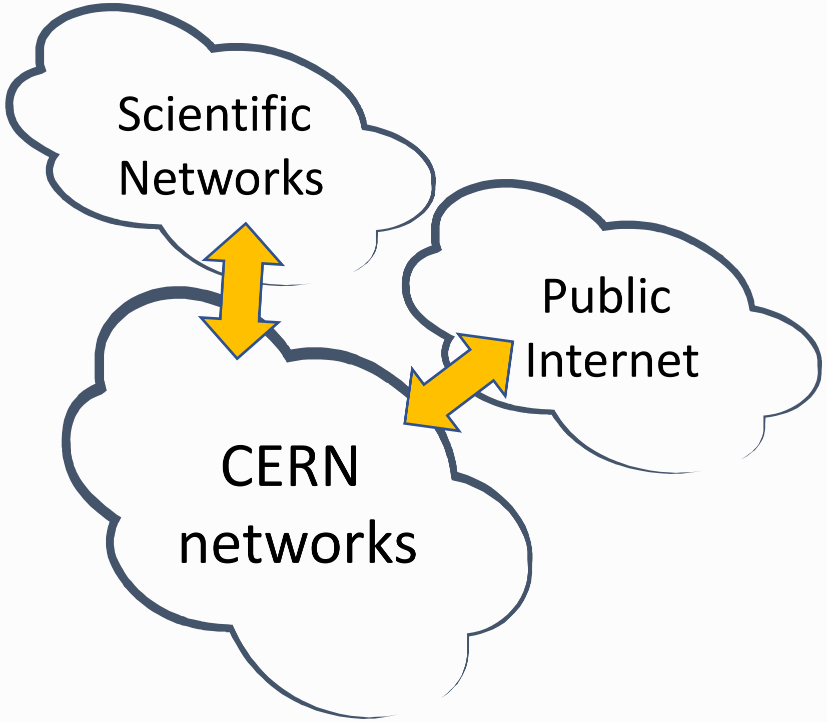
Stefan Stancu

June 2018

# Introduction



- The volume of traffic entering and leaving CERN is growing continuously
  - Connections to scientific networks and the Internet
- Precise traffic analysis and monitoring is crucial for network security
  - Cyber security threats can be detected and mitigated
- In need of a scalable and extensible Intrusion Detection System
- General design principles:
  - Analyse traffic at network boundaries
  - Aggregate and load-balance the traffic across a set of servers
  - Leverage advanced features of networking hardware



# Requirements

- Symmetrical load-balancing
  - For a given flow, both directions are forwarded to the same IDS server

CORE FUNCTIONALITY

- Traffic shunting
  - Offloading the IDS system by blocking data packets of trusted traffic
- Selective mirroring
  - Forwarding suspicious traffic flows to dedicated packet capturing servers

ADDITIONAL DYNAMIC FEATURES

- … and generally: maintainability + flexibility + programmability

# Toolbox

## Hardware

**Extreme Networks SLX 9540**

*High-end*
*data center switch*

## Software

**StackStorm**

*Automated*
*device configuration*

**Bro**

*Traffic sniffing platform*

# ExtremeRouting SLX

- SLX – a whole product family
  - Data center focused
  - High performance

- State-of-the-art features
  - Automation-ready
  - REST API
  - Virtual Machine hosting
  - … and more!

SLX 9850

SLX 9540

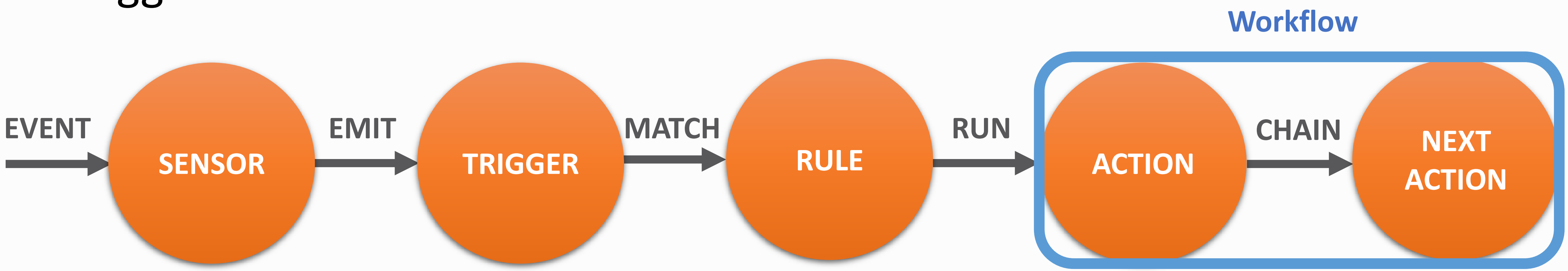
SLX 9240

SLX 9140

# StackStorm

- Platform for integration and automation across IT services and tools
  - Python-based & open-source

- Trigger-based workflow execution



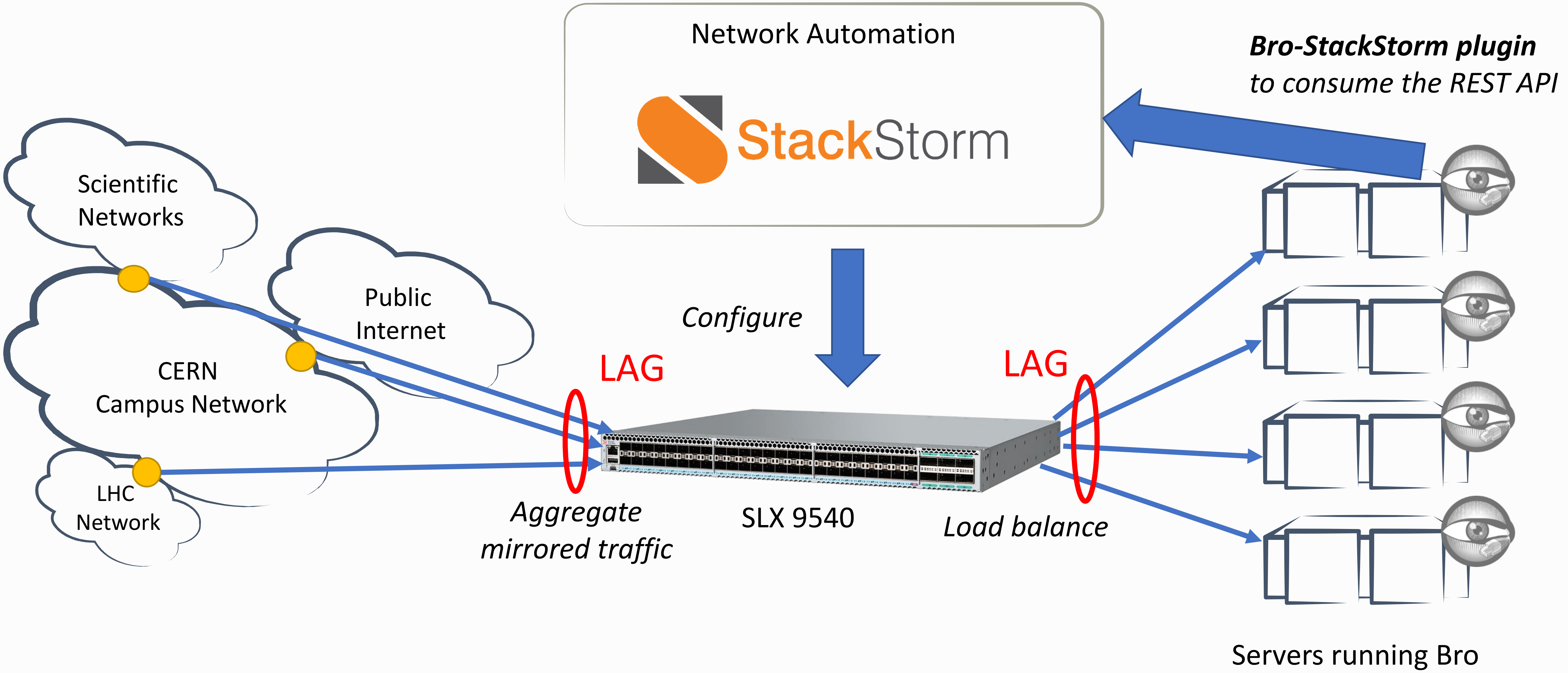
- Offers REST API and container-based deployment

# Bro

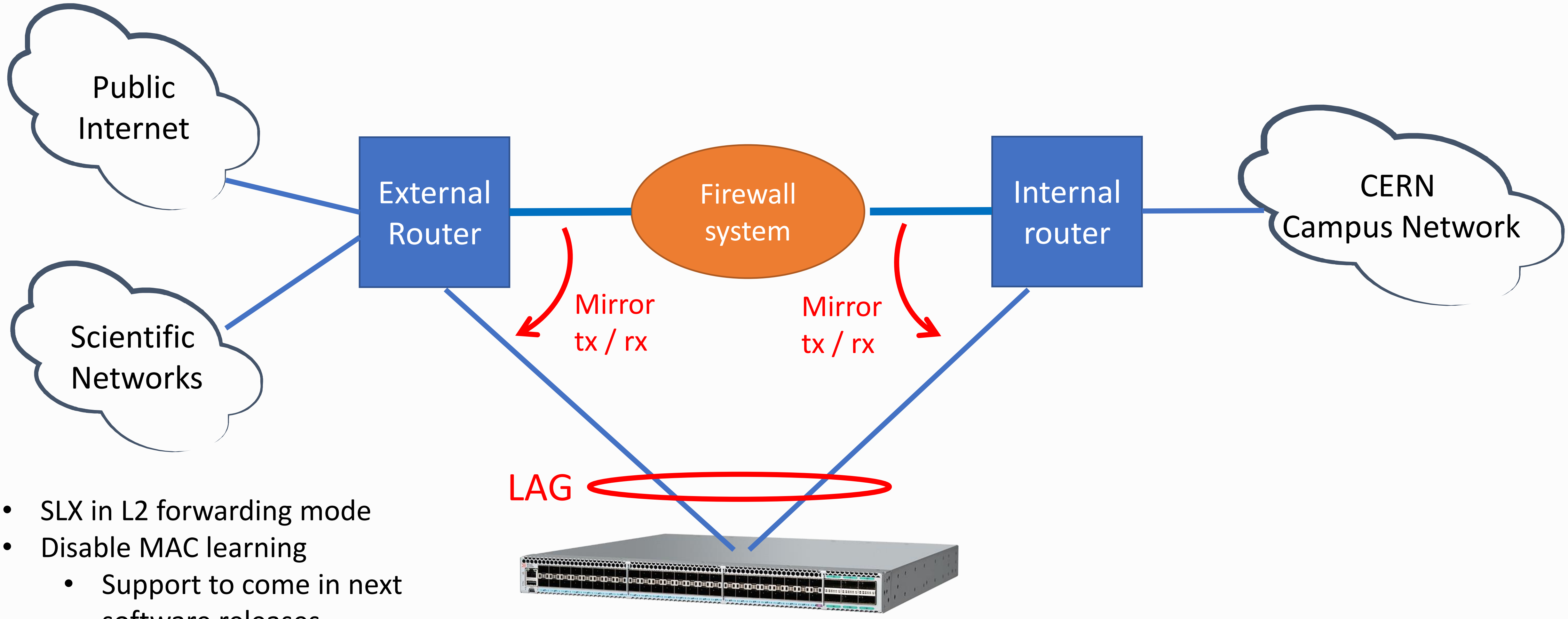
- The Bro Network Security Monitor
  - Open source
- Comprehensive traffic analysis platform
  - Event-based model for Deep Packet Inspection (DPI)
  - Option for calling user-provided code when an event occurs
    - Bro scripts
  - Flexible, **scalable** & extensible
    - Cluster mode
    - Plugins

```
event connection_established(c: connection) {
    # Handle TCP connection e.g. log
}
```

# Setup


Network Automation
StackStorm
Bro-StackStorm plugin
to consume the REST API
Scientific Networks
Public Internet
CERN Campus Network
LHC Network
Configure
LAG
LAG
Aggregate mirrored traffic
SLX 9540
Load balance
Servers running Bro

# Delivering traffic to IDS



- SLX in L2 forwarding mode
- Disable MAC learning
    - Support to come in next software releases

# Delivering traffic to IDS - configuration

- SLX

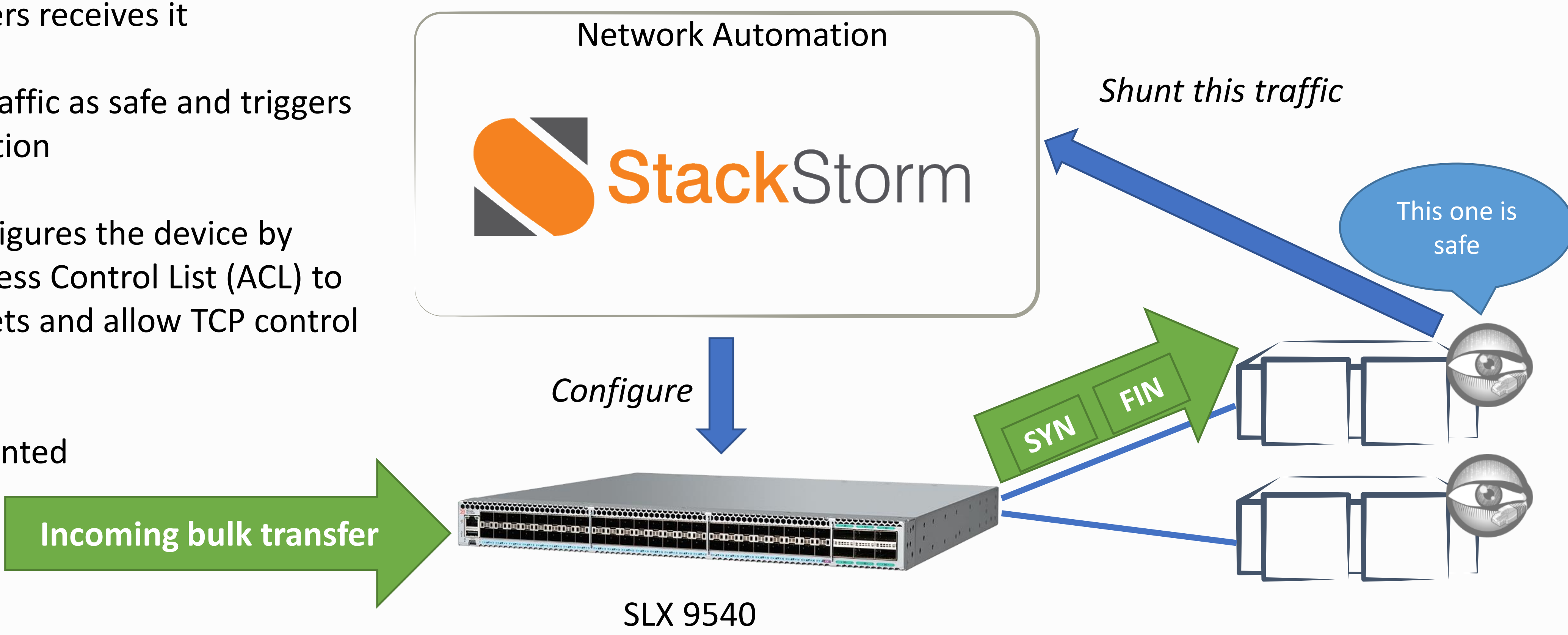
```
interface Port-channel 1
 description Ingress LAG
 switchport
 switchport mode access
 switchport access vlan 4
 no shutdown
!

interface Port-channel 20
 description Egress LAG
 switchport
 switchport mode access
 switchport access vlan 4
 no shutdown
!

interface Ethernet 0/3
 description Mirror In #1
 channel-group 1 mode on type standard
 no shutdown
!
! Symmetrical load-balancing of IP flows
no load-balance hash ethernet sa-mac
no load-balance hash ethernet da-mac
no load-balance hash ethernet vlan
no load-balance hash ethernet etype
```

- Mirror source (MLX)

```
! Mirror destination (100G)
mirror ethernet 13/2

! Mirror source (LAG of 10G links)
lag "4" dynamic id 4
 ports ethernet 1/4 to 1/5 ethernet 2/4 to 2/5 ethernet 3/4 to 3/5
 primary-port 1/4
 deploy

! Mirror port by port
interface ethernet 1/4
   mon ethernet 13/2 both
   exit
interface ethernet 1/5
   mon ethernet 13/2 both
   exit
interface ethernet 11/2
   mon ethernet 13/2 both
   exit
interface ethernet 2/4
   mon ethernet 13/2 both
   exit

! Continued for other LAG ports
```

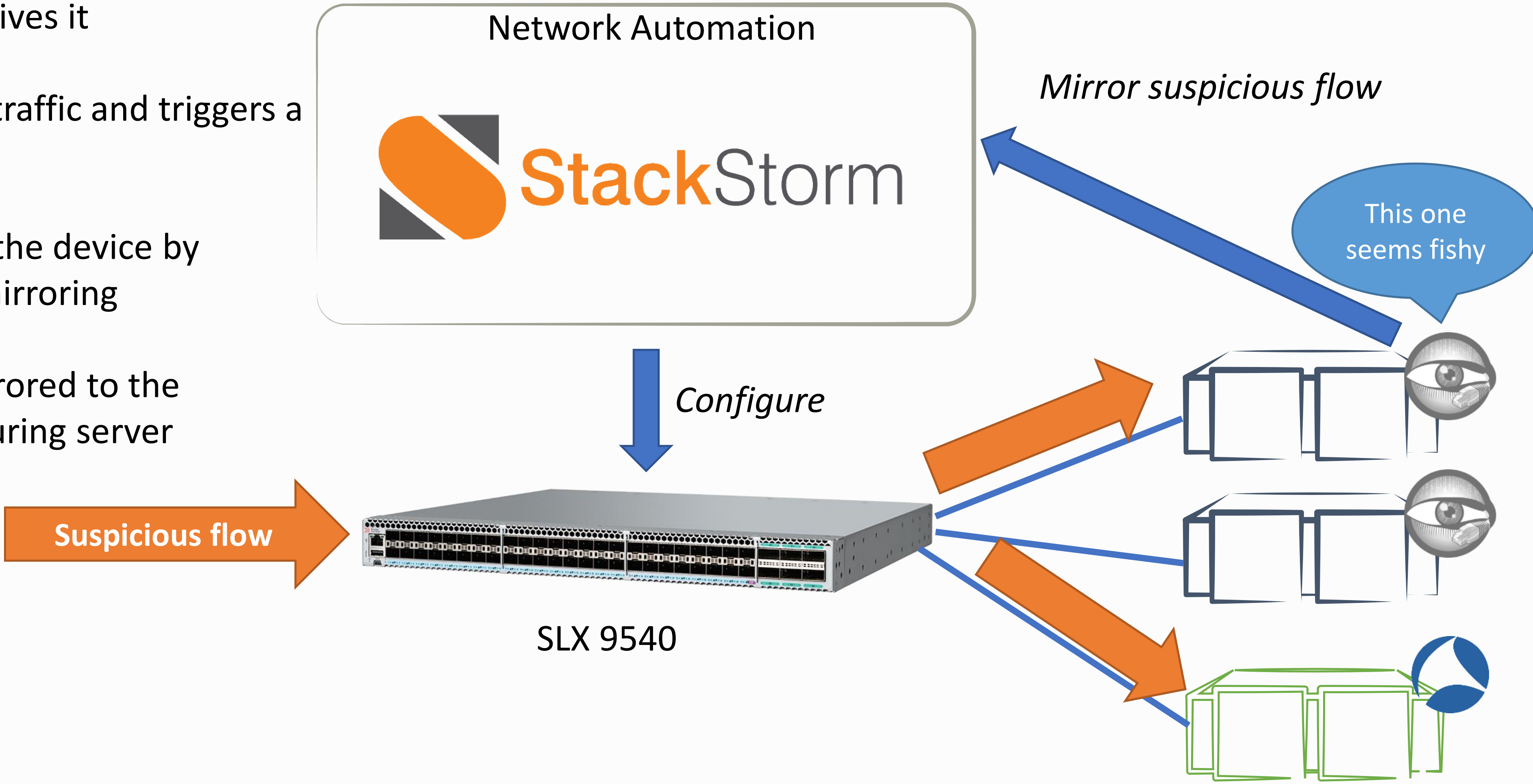
# Traffic shunting

1. A bulk data transfer is mirrored
2. One of the servers receives it
3. Bro marks the traffic as safe and triggers a StackStorm action
4. StackStorm configures the device by installing an Access Control List (ACL) to block data packets and allow TCP control flags through
5. The traffic is shunted



# Selective mirroring

1. Suspicious traffic is mirrored
2. One of the servers receives it
3. Bro detects suspicious traffic and triggers a StackStorm action
4. StackStorm configures the device by setting up ACL-based mirroring
5. Suspicious traffic is mirrored to the dedicated  packet capturing server



# Bro-StackStorm plugin

- Bro plugins allow to extend the system without re-compiling it
- Possibility of accessing StackStorm services directly in Bro scripts
    - Developed within CERN openlab collaboration with Extreme Networks

```
event connection_established(c: connection) {

    when (local result = StackStorm::shunt_traffic(c)) {

        if (result$success) {
           print “Successfully shunted TCP!”;
        } else {
           print fmt(“Error while shunting the traffic: %s”, result$error);
        }

  }
}
```

# Summary

- Prototype deployed in CERN Computer Centre
  - Sanity testing completed
  - Happy with the results

- Software development almost finished
  - StackStorm actions
  - Bro-Stackstorm plugin

- Investigating how to efficiently deploy and manage StackStorm
  - Possibly use containers

- Production deployment foreseen this year
  - Handling 160G of traffic

# Discussion?