Network Automation for Intrusion Detection System

HEPiX Fall 2017 Workshop at KEK, Tsukuba, Japan

Adam Krajewski
adam.krajewski@cern.ch | akrajews@Brocade.com

October 2017
Introduction
Introduction

- Building new Intrusion Detection System (IDS) for CERN
  - Design considerations

- Partnership with Brocade
  - CERN openlab phase V collaboration (from 2015)
  - Leverage Brocade hardware and software
  - Acquisition by Extreme Networks in progress

- Follow-up of HEPiX Fall 2016 talk
  - SDN-enabled Intrusion Detection System
  - https://indico.cern.ch/event/531810/contributions/2324770/
IDS at CERN

Overview

• 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
  • Inspired by Berkeley Lab [1]

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

Requirements

- 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

- ... and generally: maintainability + flexibility + programmability
Previously...
Architecture

Brief reminder of previous architecture

OpenDaylight
open-source SDN controller

OpenFlow
open protocol to program the hardware

Brocade Flow Optimizer
SDN application delivered by Brocade capable of monitoring and controlling network flows

OpenDaylight

Brocade MLXe
high-performance router

LAG

IDS 1

IDS 2

IDS 3

IDS x

PCAP

BRO

MIRRORED TRAFFIC
Limitations

Issues encountered

• Challenging configuration of symmetrical load-balancing
  • Limited use case documentation

• OpenFlow limitations
  • Traffic shunting not supported with OpenFlow
    • Matching on TCP flags not available in OpenFlow 1.3
    • Workaround with OpenFlow and User-Defined Access List is not scalable
  • Limited support on LAGs (Link Aggregation Groups)
    • Need to deploy OpenFlow rules on each physical interface separately
    • Complex configuration = complex maintenance

• MLXe form factor
  • 1U preferable
Design evolution
Brocade SLX

New product family

• Brocade SLX – a new product family [2]

• New hardware architecture
  • High performance
  • Data center focused

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

Adam Krajewski - Network Automation - HEPIX Fall 2017
Network automation

From OpenFlow-based SDN to network automation

Initial SDN paradigm: decouple control from forwarding and implement with software
- Open architecture, open principles
- Implement any feature with open protocols
- OpenFlow as key enabler
- Challenging to deploy and maintain (non-uniform vendor support)

Network automation
- Follow the main SDN principle: control networks with software
- Leverage proprietary hardware features through open APIs
  - REST APIs, NetConf, even OpenFlow
- Automation principles taken from DevOps
  - Use open, programmable & extensible tools
  - IF-THIS-THEN-THAT (IFTTT) approach through reusable modules and workflows
Network automation

Ecosystem

Configuration management

Device drivers

- Brocade’s PySwitchLib
- Juniper’s PyEZ
- ...
StackStorm / Brocade Workflow Composer (BWC)

The workhorse

• 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: Brocade Workflow Composer (BWC) [3]
  • https://bwc-docs.brocade.com/
Brocade Flow Optimizer (BFO)

The brain

• SDN application provided by Brocade [4]

• 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 Brocade Workflow Composer
**BWC + BFO**

*Network automation suite*

- **BWC** as the configuration workhorse
  - How to do?
  - Abstracting CLI manipulation
  - Python + modularity = flexibility

- **BFO** as the brain behind
  - What to do?
  - Applying actions on traffic flows coming to the IDS system

---

**Network Automation**

- **BWC**
- **BFO**
Currently...
Toolbox

Hardware

Brocade SLX 9540

High-end data center switch

Software

Brocade Workflow Composer (BWC)

Automated device configuration

Brocade Flow Optimizer (BFO)

Traffic flow visibility and actions

Bro Network Monitor System

Traffic sniffing platform

Adam Krajewski - Network Automation - HEPIX Fall 2017
Setup

Scientific Networks

CERN Campus Network

Public Internet

LHC Network

Setup

CERN Campus Network

Public Internet

LHC Network

Aggregate mirrored traffic

SLX 9540

Load balance

Network Automation

BWC

BFO

Configure

Monitor

Servers running Bro

Adam Krajewski - Network Automation - HEPiX Fall 2017
Traffic shunting

1. A bulk data transfer is mirrored
2. One of the servers receives it
3. BFO matches the traffic flow against safe traffic patterns
4. BFO uses BWC to configure the device to block data packets and allow TCP control flags through
5. The traffic is shunted

Adam Krajewski - Network Automation - HEPIX Fall 2017
**Selective mirroring**

1. Suspicious traffic is mirrored
2. One of the servers receives it
3. Bro detects suspicious traffic
4. Bro triggers selective mirroring mechanism
5. BFO uses BWC to configure the device
6. Suspicious traffic is mirrored to the dedicated packet capturing server
Conclusions
Current status and future 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
  • Other potential use cases

• Promising perspective of production deployment in 2018
References


[2] Brocade SLX

[3] Brocade Workflow Composer

Network Automation for Intrusion Detection System

HEPiX Fall 2017 Workshop at KEK, Tsukuba, Japan

Adam Krajewski
adam.krajewski@cern.ch | akrajews@Brocade.com

October 2017