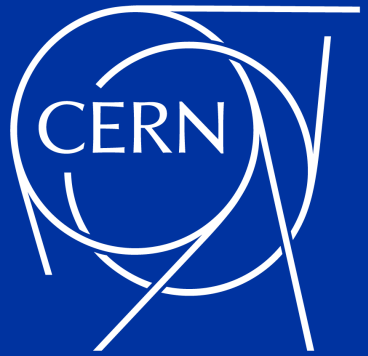


CERN Networking Mirroring and Distribution Setup for Zeek

CERN, Zeek Workshop - 25 March 2026

Edoardo Martelli, Stefan Stancu, Liviu Valsan

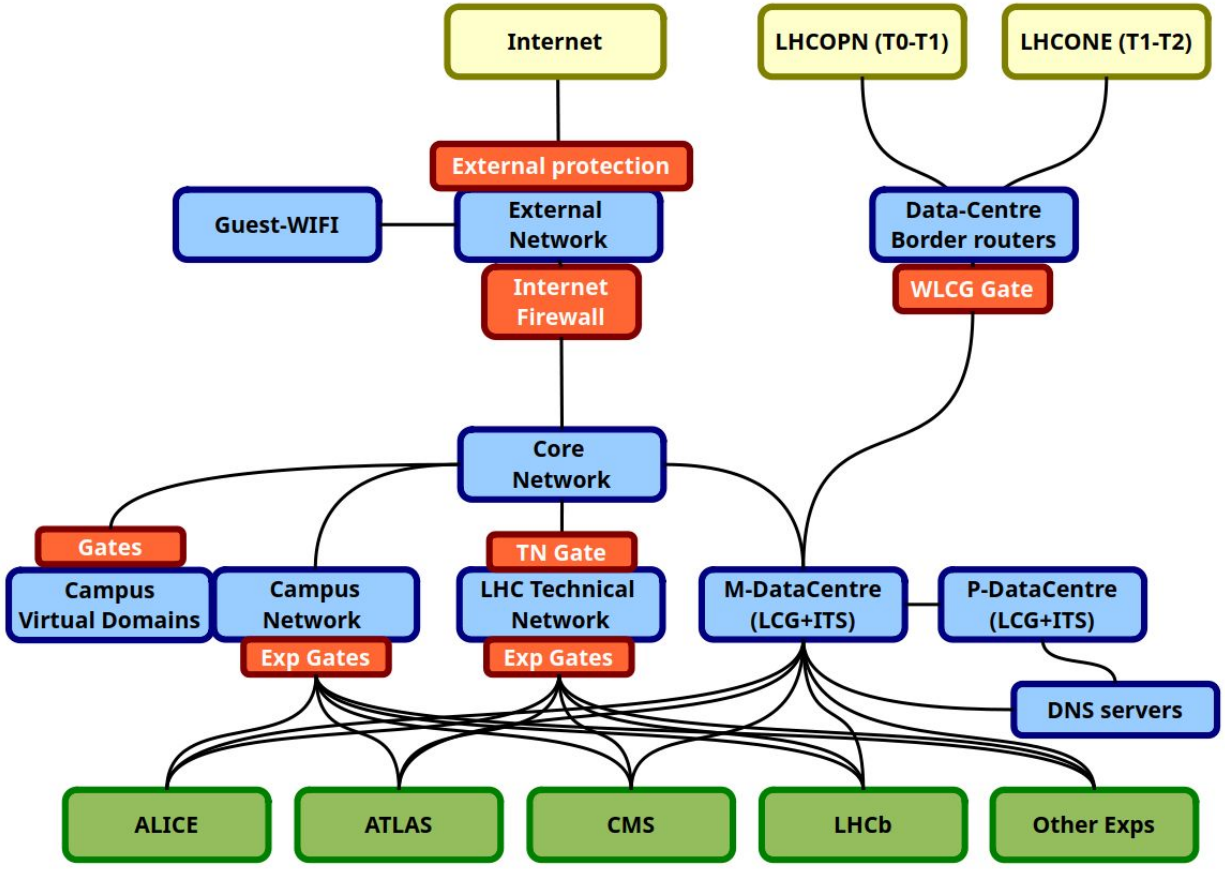
scope

Traffic at critical points is mirrored to the Zeek installation of the CERN Security Team for traffic inspection

Critical points:

- Internet firewall
- Gate at Accelerator network (AKA Technical Network, TN)
- CERN DNS servers
- Guest WIFI

CERN network domains



Not CERN

Managed by IT-CS

Policies by Security Team

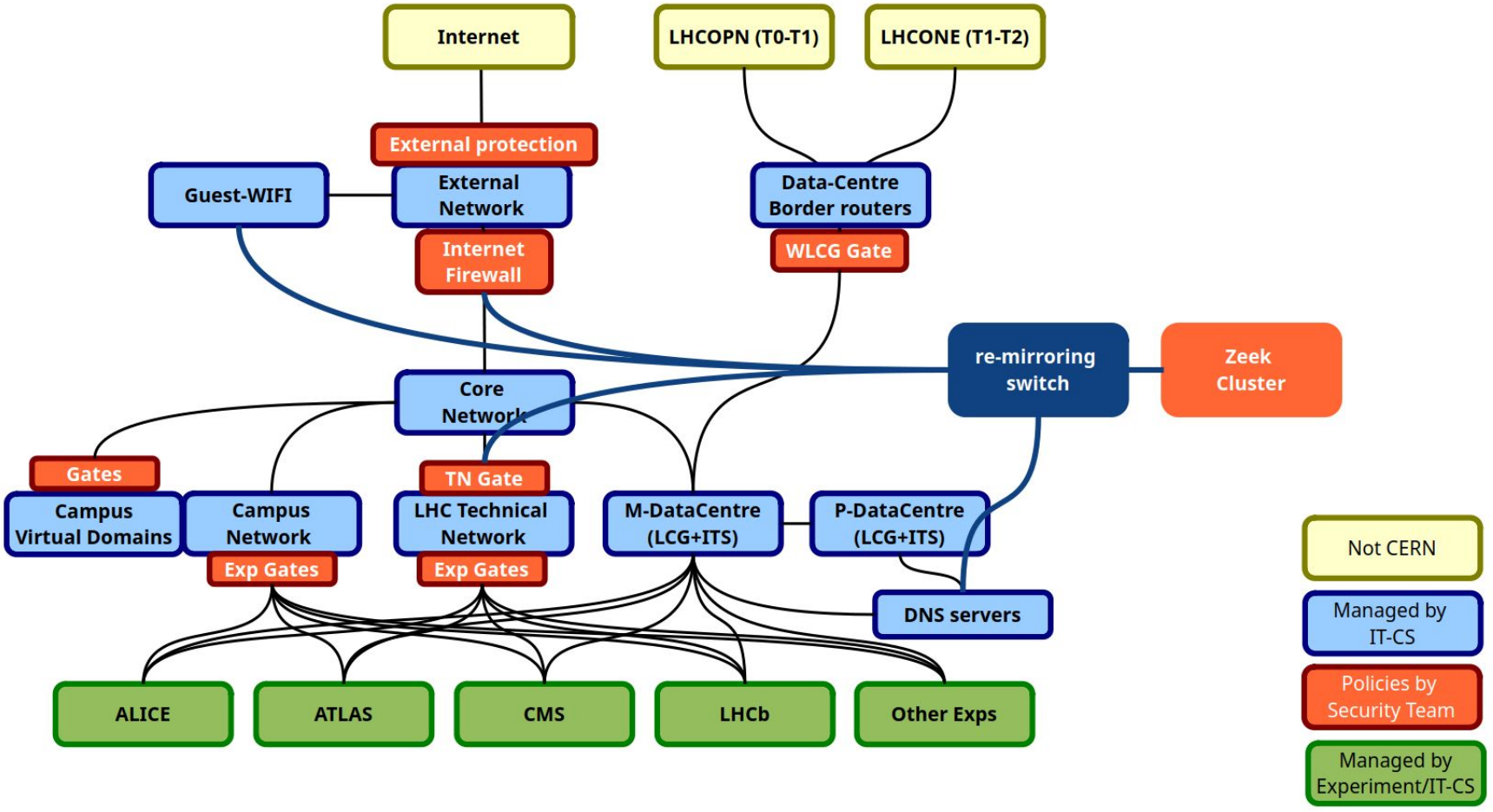
Managed by Experiment/IT-CS

traffic mirroring

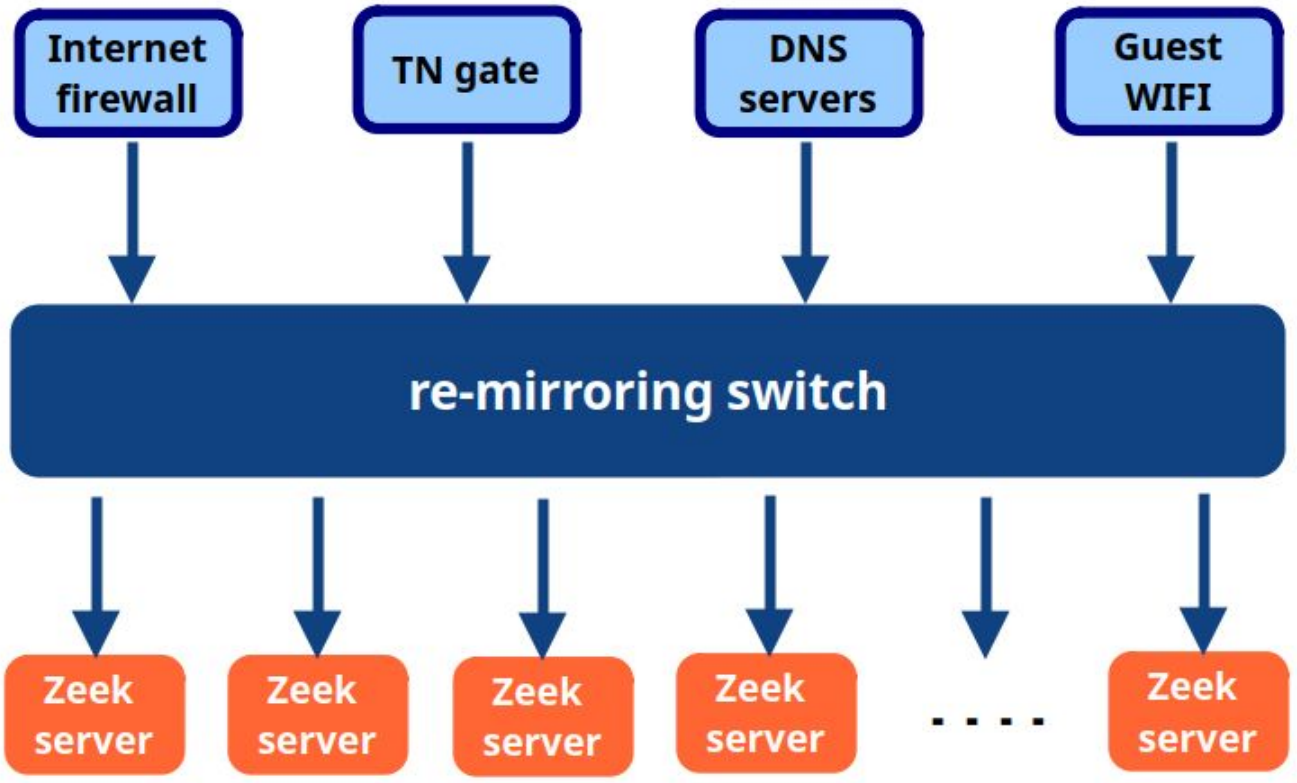
- switches and routers at critical network gateways mirror traffic of relevant interfaces

- a central switch capable of Passive Monitoring receives all the mirrors and re-mirror them again to a cluster of Zeek servers

mirroring points



setup


Internet firewall
TN gate
DNS servers
Guest WIFI
re-mirroring switch
Zeek server
Zeek server
Zeek server
Zeek server
Zeek server

implementation

Passive Monitoring

- **Passive Monitoring** allows Junos devices to capture, analyze, and forward network traffic to monitoring tools without participating in the network traffic themselves

- **Symmetric Hashing** is the capability of keeping the packets of the two directions of an IP flow mirrored out together to the same output interface

- Ref: Juniper Passive Monitoring

- We use a Juniper QFX10008

Juniper config

```
# input ports policy-route all the traffic to a dedicated routing instance (VRF)
set interfaces et-0/0/0 description "----> IN: mirror from LCG firewall"
set interfaces et-0/0/0 enable
set interfaces et-0/0/0 passive-monitor-mode
set interfaces et-0/0/0 mtu 9216
set interfaces et-0/0/0 unit 0 family inet6 mtu 9000
set interfaces et-0/0/0 unit 0 family inet6 filter input FF-PMON6-ET-0-0-0
set interfaces et-0/0/0 unit 0 family inet mtu 9000
set interfaces et-0/0/0 unit 0 family inet filter input FF-PMON-ET-0-0-0

# each port needs its own policy configuration
set firewall family inet6 filter FF-PMON6-ET-0-0-0 term T10 from interface et-0/0/0.0
set firewall family inet6 filter FF-PMON6-ET-0-0-0 term T10 then routing-instance PMON
set firewall family inet filter FF-PMON-ET-0-0-0 term T10 from interface et-0/0/0.0
set firewall family inet filter FF-PMON-ET-0-0-0 term T10 then routing-instance PMON

# VRF with a static route pointing to a virtual address
set routing-instances PMON instance-type virtual-router
set routing-instances PMON routing-options rib PMON.inet6.0 static route ::0/0 next-hop fd01::1
set routing-instances PMON routing-options rib PMON.inet.0 static route 0.0.0.0/0 next-hop 10.1.1.1
set routing-instances PMON interface ae0.0
```

Juniper config (2)

```
# output ports aggregated in a LAG
set interfaces xe-0/0/24 description "----> OUT: Zeek Node 9"
set interfaces xe-0/0/24 enable
set interfaces xe-0/0/24 ether-options 802.3adae0

# output LAG with a static definition of the MAC address of the default-gateway
set interfaces ae0 description "----> OUT: IDS servers"
set interfaces ae0 mtu 9216
set interfaces ae0 aggregated-ether-options link-speed mixed
set interfaces ae0 unit 0 family inet6 mtu 9000
set interfaces ae0 unit 0 family inet6 address fd01::2/64ndp fd01::1 mac 00:12:34:56:78:9a
set interfaces ae0 unit 0 family inet mtu 9000
set interfaces ae0 unit 0 family inet address 10.1.1.2/24 arp 10.1.1.1 mac 00:12:34:56:78:9a


# enable symmetric-hashing
set forwarding-options enhanced-hash-key inet6 no-incoming-port
set forwarding-options enhanced-hash-key inet no-incoming-port
# remove vlan-ids; workaround for switches not correctly removing them
set forwarding-options enhanced-hash-key layer2 no-vlan-id
```

alternative setup

- an alternate way of doing the mirroring can be implemented by using a vlan with two LAG interfaces, one for input and one for output, configured with

  ```
  switch-options no-mac-learning
  ```

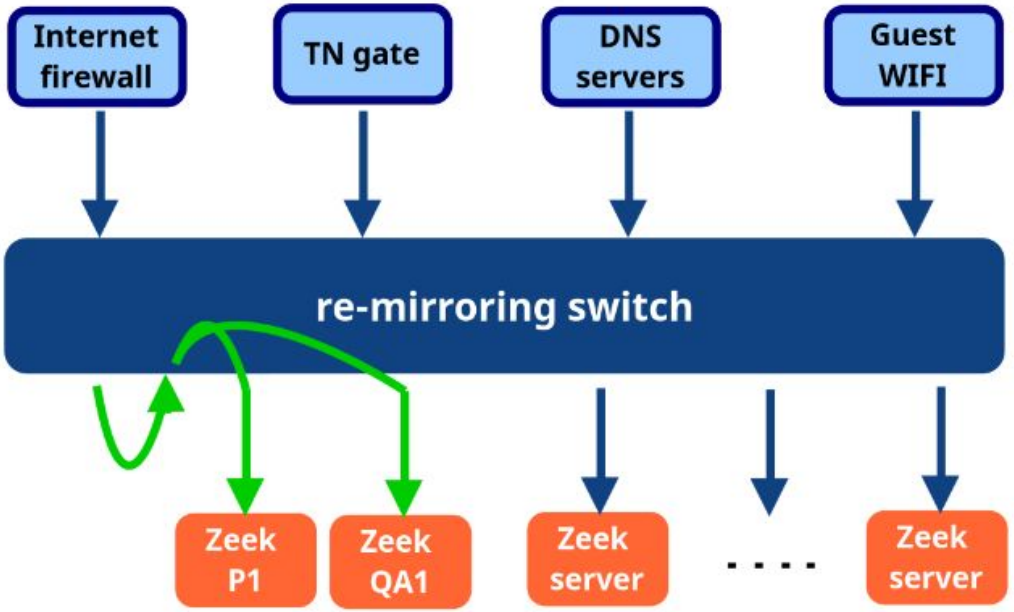
  to keep flooding traffic to the output LAG interface

- not implemented because at the time all the ports in the same LAG had to have the same speed. Now Juniper supports

  ```
  aggregated-ether-options link-speed mixed
  ```

QA re-re-mirroring

- three Zeek servers are paired with a forth one for QA
- the forth server (QA) receives the same copy of traffic as the third server (production) in the group



QA mirroring - config

```
# physical loop: xe-2/0/22 receives a portion of the traffic and send it to xe-2/0/23
set interfaces xe-2/0/22 description "----> OUT: cable to xe-2/0/23 for QA1 multiple copies"
set interfaces xe-2/0/22 ether-options 802.3ad ae0
set interfaces xe-2/0/23 description "----> IN-QA1: cable from xe-2/0/22 for QA1 multiple copies"
set interfaces xe-2/0/23 mtu 9216
set interfaces xe-2/0/23 unit 0 family ethernet-switching interface-mode access
set interfaces xe-2/0/23 unit 0 family ethernet-switching vlan members 11

# port xe-2/0/23.0 is mirrored into a VLAN (QA1-MIRROR-OUT VLAN10)
set forwarding-options analyzer QA1-MIRROR input ingress interface xe-2/0/23.0
set forwarding-options analyzer QA1-MIRROR output vlan QA1-MIRROR-OUT no-tag

# vlan definition (more in the next page)
set vlans QA1-MIRROR-OUT vlan-id 10

# two Zeek servers get the same traffic because they both belong to VLAN10 QA1-MIRROR-OUT
set interfaces xe-2/0/0 description "----> OUT-QA1: Zeek node 3"
set interfaces xe-2/0/0 mtu 9216
set interfaces xe-2/0/0 unit 0 family ethernet-switching interface-mode access
set interfaces xe-2/0/0 unit 0 family ethernet-switching vlan members 10
set interfaces xe-2/0/1 description "----> OUT-QA1: Zeek node 4"
set interfaces xe-2/0/1 mtu 9216
set interfaces xe-2/0/1 unit 0 family ethernet-switching interface-mode access
set interfaces xe-2/0/1 unit 0 family ethernet-switching vlan members 10
```

QA mirroring - config (2)

```
# vlan definitions
set vlans QA1-MIRROR-OUT description "----> destination vlan for QA1 mirror"
set vlans QA1-MIRROR-OUT vlan-id 10
set vlans QA1-MIRROR-OUT switch-options no-mac-learning
# the interface receiving the first mirror is in a vlan alone
set vlans QA1-MIRROR-DUMP description "----> dump vlan for QA1 mirror"
set vlans QA1-MIRROR-DUMP vlan-id 11
set vlans QA1-MIRROR-DUMP switch-options no-mac-learning
```

conclusion

conclusions

- it works: the switch allows passive-monitoring and it is able to keep the two directions of each flow on the same output port

- it scales: the switch can connect as many sources and destination as available physical ports

Questions?

edoardo.martelli@cern.ch