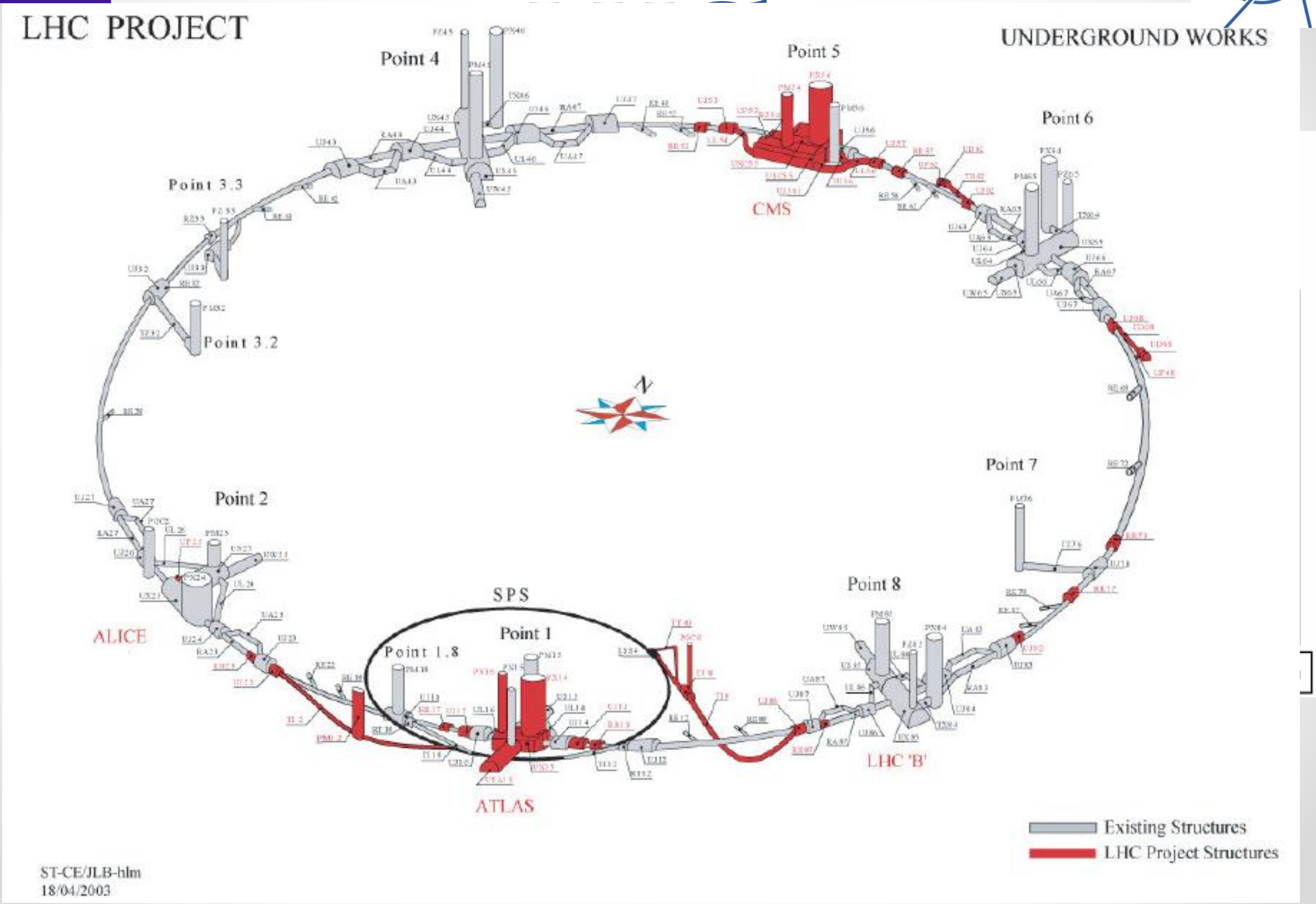
IT Security for the LHCb experiment

3rd Control System Cyber-Security Workshop (CS)2/HEP ICALEPCS – Grenoble

Enrico Bonaccorsi, (CERN) enrico.bonaccorsi@cern.ch
Loic Brarda, (CERN) loic.brarda@cern.ch
Mohamed Chebbi, (CERN) mohamed.chebbi@cern.ch
Niko Neufeld, (CERN) niko.neufeld@cern.ch
Enrico Papi, (CERN) enrico.papi@cern.ch

Outline

- LHCb intro
- IT Security – several point of view
  - Security risks
  - Physical and host local security approach.
  - Protected perimeter
  - Network security implementation
- Central Log System
- Data Security
- Log and data analysis


LHC PROJECT
UNDERGROUND WORKS
Point 4
Point 5
Point 6
Point 3.3
Point 3.2
Point 2
Point 7
Point 8
Point 1
Point 1.8
SPS
CMS
ALICE
ATLAS
LHC 'B'
N
Existing Structures
LHC Project Structures
ST-CE/JLB-hlm
18/04/2003

IT Security several point of view

- Physical Security
- Local Security
- Network Local Security
- Network Security
- Data Security

- Local and Remote Access
- High Availability
- Preemptive measures
- External connectivity
- Management of Application and Operating Systems
- Industrial security

Security risks

- Interruption in Data Acquisition
- Unauthorized modification/destruction to data and systems
- Unauthorized disclosure of data
- Denial of service

Security risks (2)

- Users Behavior
  - Theft of authentication credentials
  - Lack of awareness, caralessness or negligence
  - Unfair and fraudulent behavior
  - Human errors
- Attack and misconfiguration
  - Virus – Malware – Trojan – Backdoor – Rootkits - Worm – Hiding in encrypted sessions - etc
  - Sabotage
  - Unauthorized access
  - Information
  - Human errors
- Environmental
  - Theft of devices that contain data
  - Destructive events (earthquakes, fire, flood, etc)
    - Intentional, accidental, due to negligence
  - Human errors

Security Policy

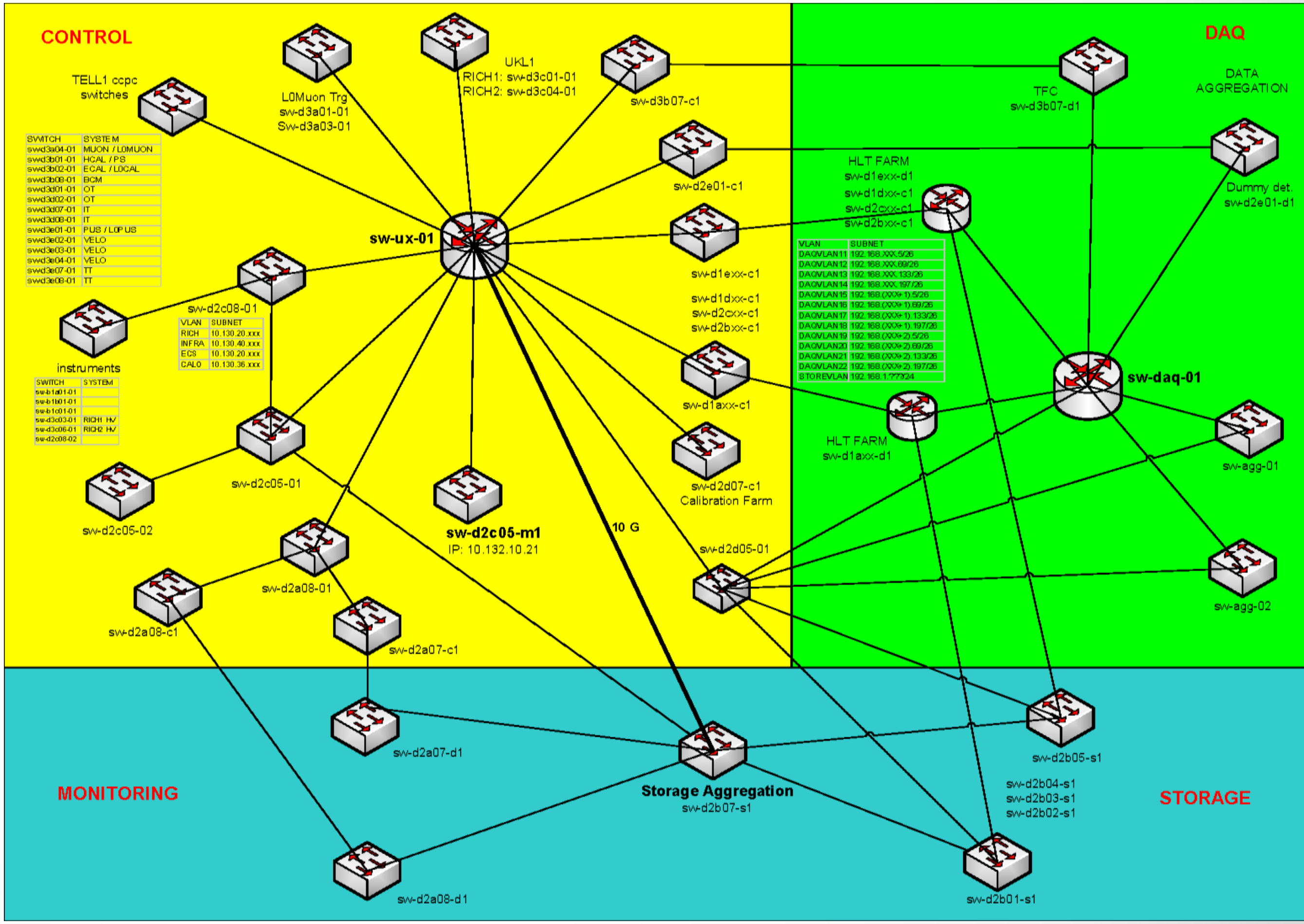
- Security policies have been produced following the CERN CNIC recommendations:
  - https://edms.cern.ch/file/1062503/2/Security_Baseline_for_File_Hosting.pdf
  - https://edms.cern.ch/file/1062500/2/Security_Baseline_for_Servers.pdf
  - https://edms.cern.ch/file/1062502/2/Security_Baseline_for_Web_Hosting.pdf

Physical and host local security approach

- Physical:
  - Authorization required to access Point 8
  - Biometric required to access the underground area
- Local
  - Private personal account for each LHCb user
    - Few shared account are still in use
  - PAM/Domain Policies used to restrict access to critical servers between LHCb groups
  - IPMI access protected by router ACL
  - Applications centrally managed by Quattor/System Center Deployment Services
  - No internet routing allowed except for few gateway server
  - Only WEB access granted through an HTTP proxy

Inner networks

- Traffic isolation using VLANs, 802.1q, Layer2 filtering and ACL
- LCG and TN accessible only from few hosts
- No internet connectivity
- Only LHCb laptop allowed



SWITCH	SYSTEM
swd3a04-01	MUON / L0MUON
swd3b01-01	HCAL / PS
swd3b02-01	ECAL / L0CAL
swd3b08-01	BCM
swd3d01-01	OT
swd3d02-01	OT
swd3d07-01	IT
swd3d08-01	IT
swd3e01-01	PUS / L0PUS
swd3e02-01	VELO
swd3e03-01	VELO
swd3e04-01	VELO
swd3e07-01	TT
swd3e08-01	TT

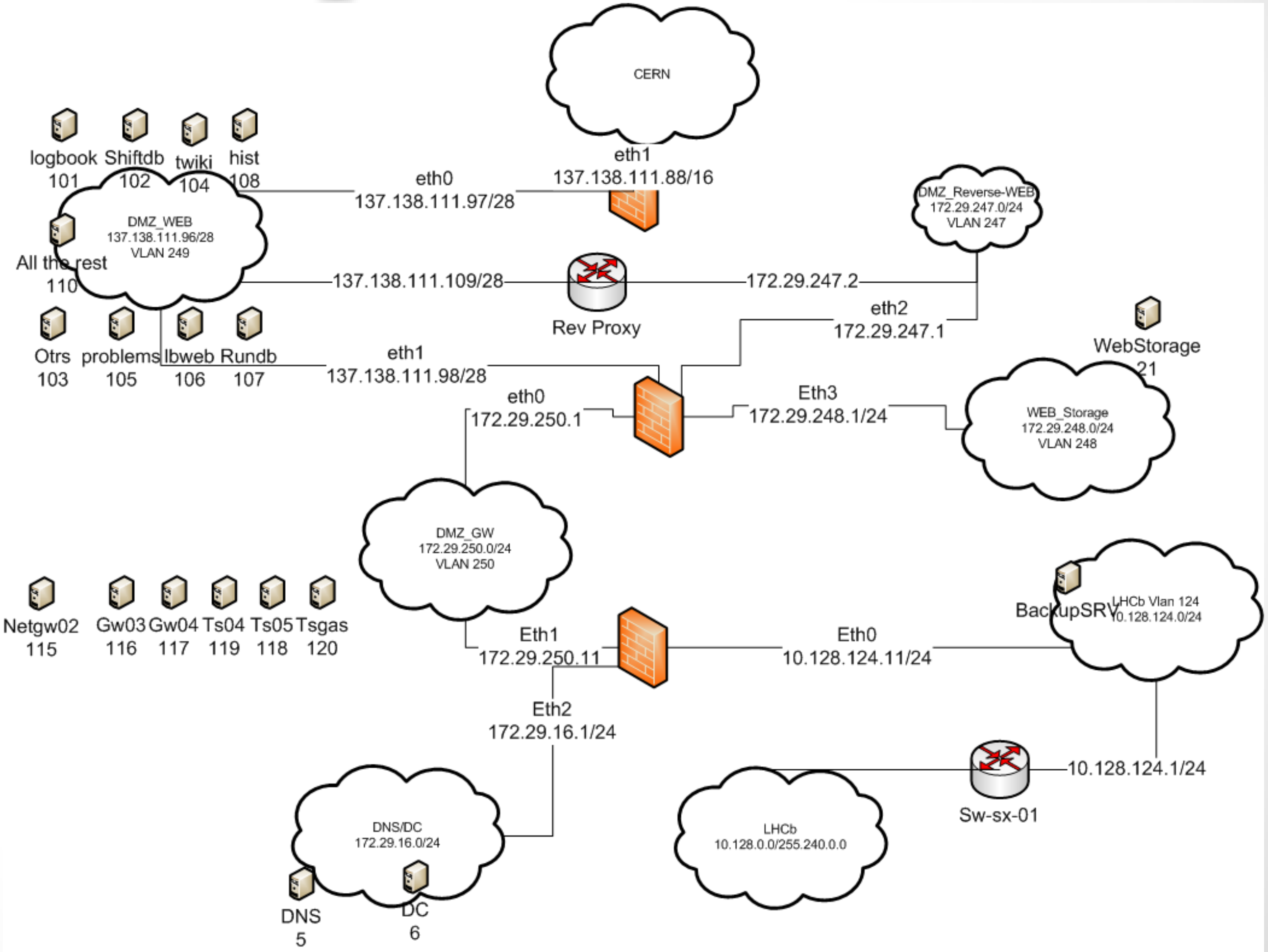
VLAN	SUBNET
RICH	10.130.20.xxx
INFRA	10.130.40.xxx
ECS	10.130.20.xxx
CALO	10.130.36.xxx

SWITCH	SYSTEM
sw-b1a01-01	
sw-b1b01-01	
sw-b1c01-01	
sw-d3c03-01	RICH1 HV
sw-d3c06-01	RICH2 HV
sw-d2c08-02	

VLAN	SUBNET
DAQVLAN11	192.168.XXX.5/26
DAQVLAN12	192.168.XXX.69/26
DAQVLAN13	192.168.XXX.133/26
DAQVLAN14	192.168.XXX.197/26
DAQVLAN15	192.168.(XXX+1).5/26
DAQVLAN16	192.168.(XXX+1).69/26
DAQVLAN17	192.168.(XXX+1).133/26
DAQVLAN18	192.168.(XXX+1).197/26
DAQVLAN19	192.168.(XXX+2).5/26
DAQVLAN20	192.168.(XXX+2).69/26
DAQVLAN21	192.168.(XXX+2).133/26
DAQVLAN22	192.168.(XXX+2).197/26
STOREVLAN	192.168.1.???/24

Network Security implementation

- General public and log in services/ Terminal services
  - RDP windows remote desktops
  - SSH gateways
  - NX linux remote desktops
  - Web services
- Network segmentation and trusted zones
  - level of trust based on three tiers the sensitivity of the data being processed
- Anomaly & Intrusion detection



Central Log System

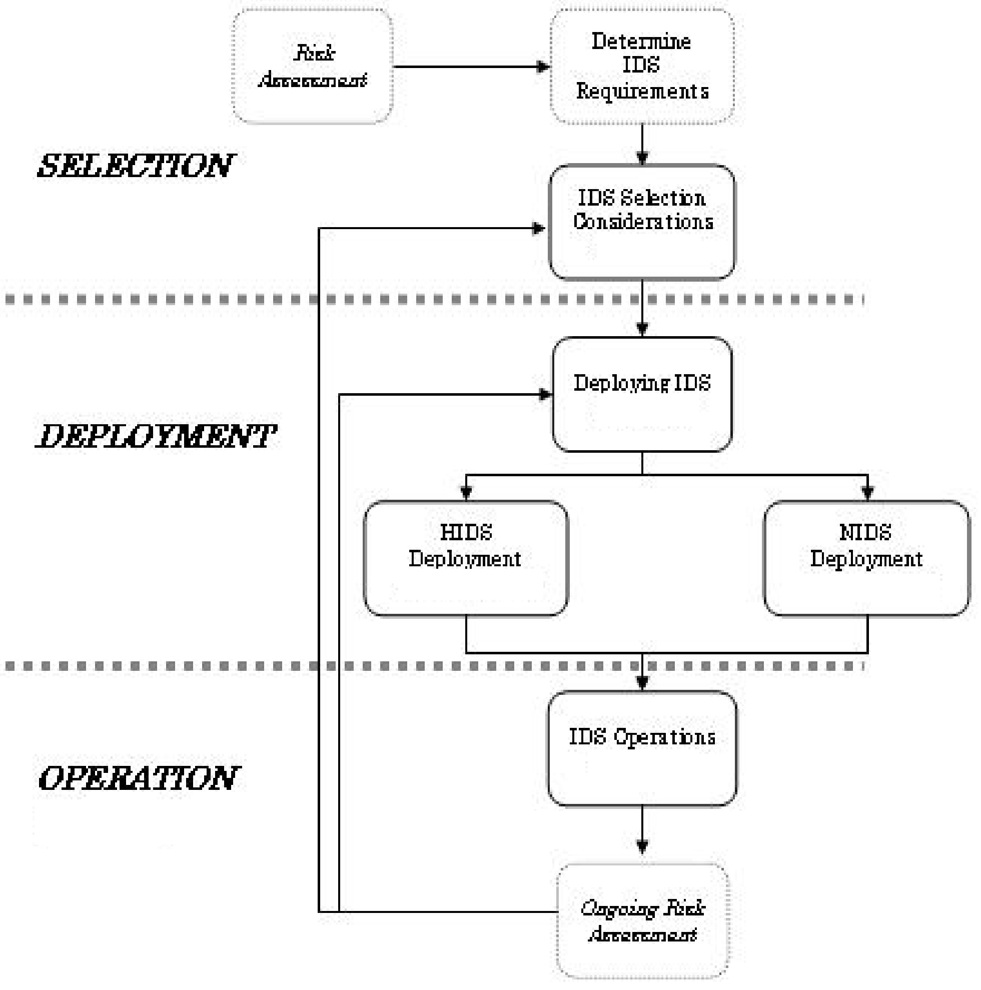
- All the windows and Linux servers send their logs to a clustered log server
- High Availability granted by
    - Active/Active two node cluster system
    - Raid 1 on each cluster node for the local disk
    - Filesystem replica over network between nodes
    - Backup on CASTOR
- Logs exported to the users by NFS

Data Security

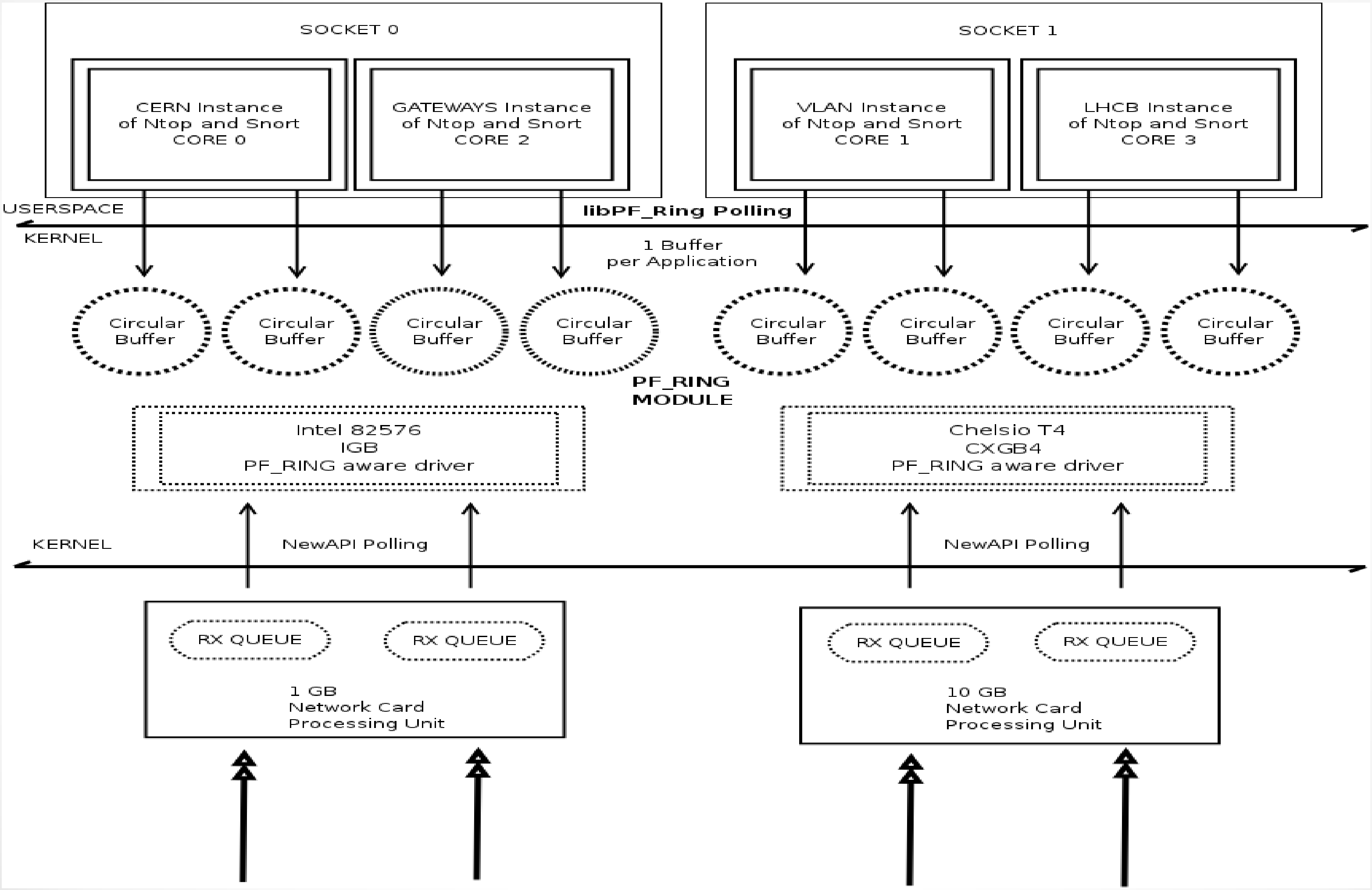
- Shared filesystem
  - served by a cluster of five nodes on redundant hardware
  - High Availability granted by Cluster of NFS/SMB servers that export the filesystem to the entire experiment
  - Data protection:
    - Short term based on different storage raid set using RSYNC for immediate user access (file deleted by mistake by the user, etc)
    - Long Term based on tape using CASTOR for… ever? ☺
    - Backup sent to CASTOR and stored on type
- Servers and Control PCs
  - High availability granted by RAID 1
    - SW RAID used when HW raid is not available
  - Daily Backup based on Tivoli (Thanks to IT dep.)

Network Intrusion/Anomaly Detection System

- Boundary networks traffic mirrored and analyzed
- ISO/IEC 18043:2006(E) Selection, deployment and operations of intrusion detection system
- Snort for NIDS
- NTOP for Anomaly Detection



Performance


SOCKET 0
CERN Instance of Ntop and Snort CORE 0
GATEWAYS Instance of Ntop and Snort CORE 2
SOCKET 1
VLAN Instance of Ntop and Snort CORE 1
LHCB Instance of Ntop and Snort CORE 3
USERSPACE
KERNEL
libPF_Ring Polling
1 Buffer per Application
Circular Buffer
Circular Buffer
Circular Buffer
Circular Buffer
Circular Buffer
Circular Buffer
Circular Buffer
Circular Buffer
PF_RING MODULE
Intel 82576 IGB PF_RING aware driver
Chelsio T4 CXGB4 PF_RING aware driver
KERNEL
NewAPI Polling
NewAPI Polling
RX QUEUE
RX QUEUE
1 GB Network Card Processing Unit
RX QUEUE
RX QUEUE
10 GB Network Card Processing Unit

Questions?

Backup slide

Snort Log data Analysis

Raw logs generated:

- Ntop – Suspiciuous (Syslog)
- Ntop – Others (pcap)
- Snort > Barnyard > Alerts (Syslog)
- Snort – Packets (pcap)

Barnyhard to offload output processing

Parsing

Visual – Links Graphs

Correlation to crosscheck to exclude false positives

Centralized Analysis console is not strictly necessary