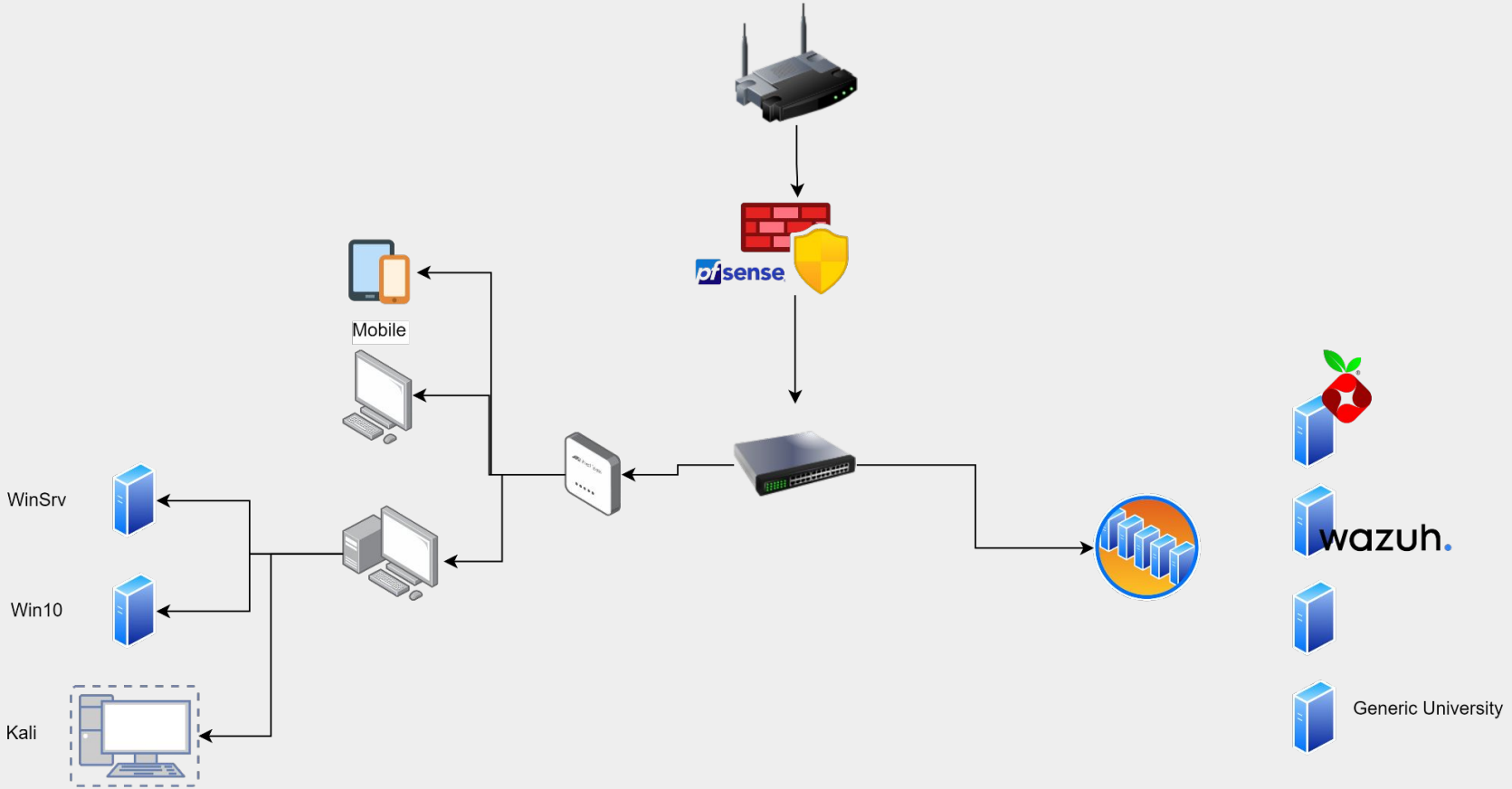
Building your (MY FIRST) home lab

Arturo Sustaita

#BugBites

Who Am I?

- Security Consultant - Penetration Tester
- Dad
- Coffee lover


pfsense
Mobile
WinSrv
Win10
Kali
wazuh.
Generic University

Fase 1

Objetivo original:

Virtualizar máquinas

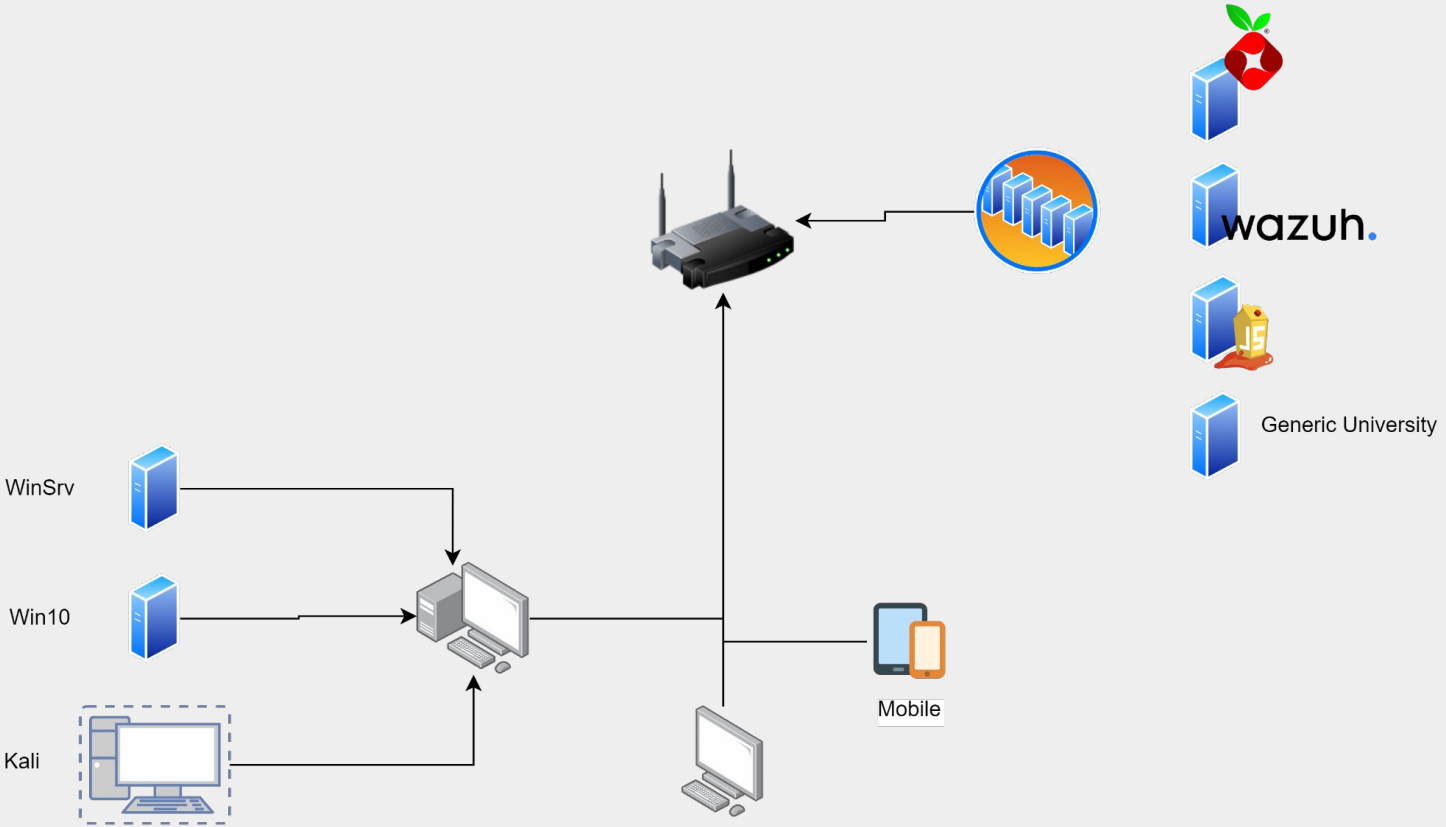
Recursos

- Appliance
- Modem

wazuh.

PROXMOX

Fase 1



- Modem restringido
- Disco Duro murió
- Electricidad*
- Sin monitoreo red inalámbrico

Exitos

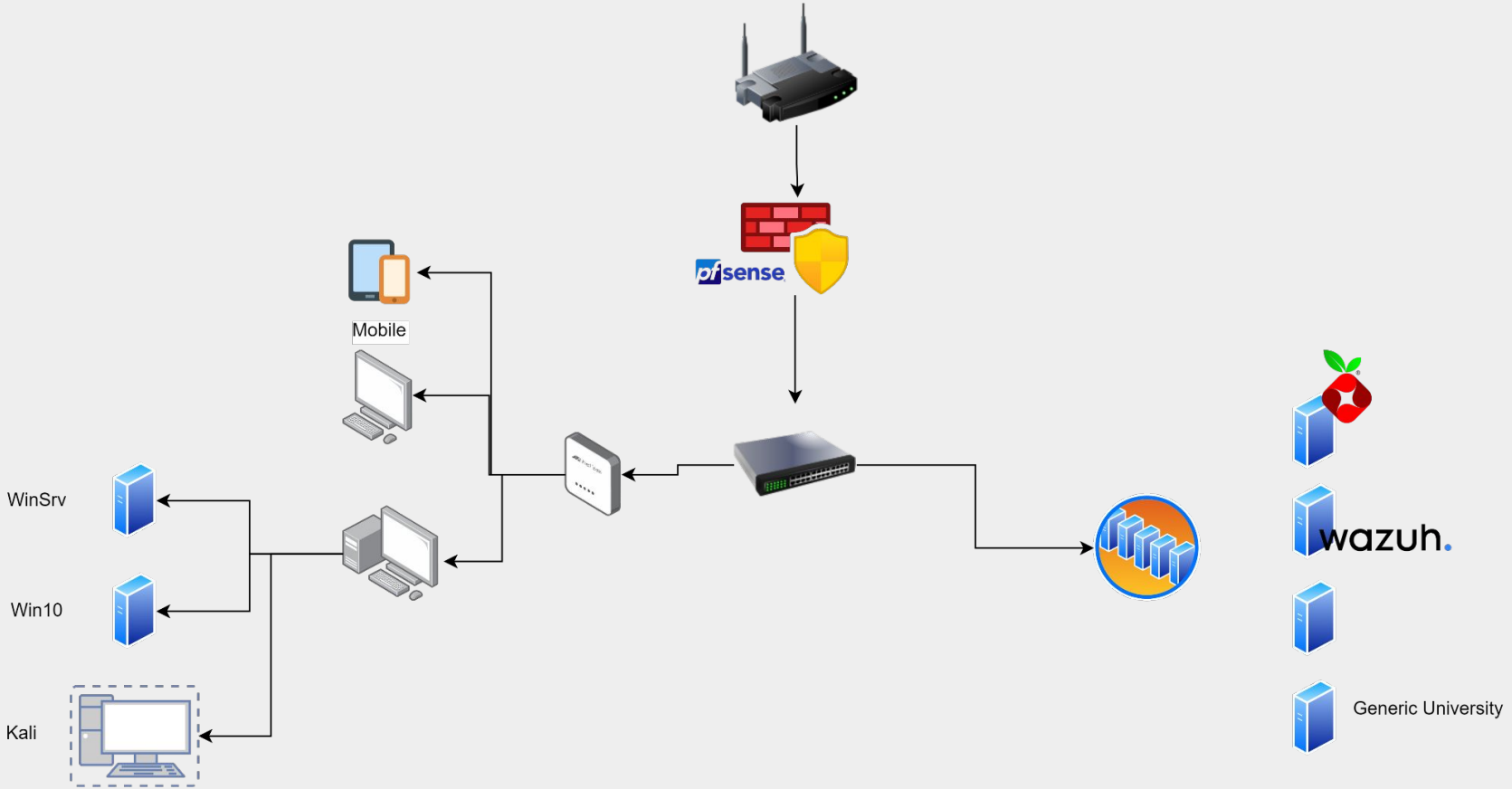
- Virtualización
- Integridad de archivos
- Monitoreo de eventos de Docker
- Análisis de vulnerabilidades
- Detección de malware

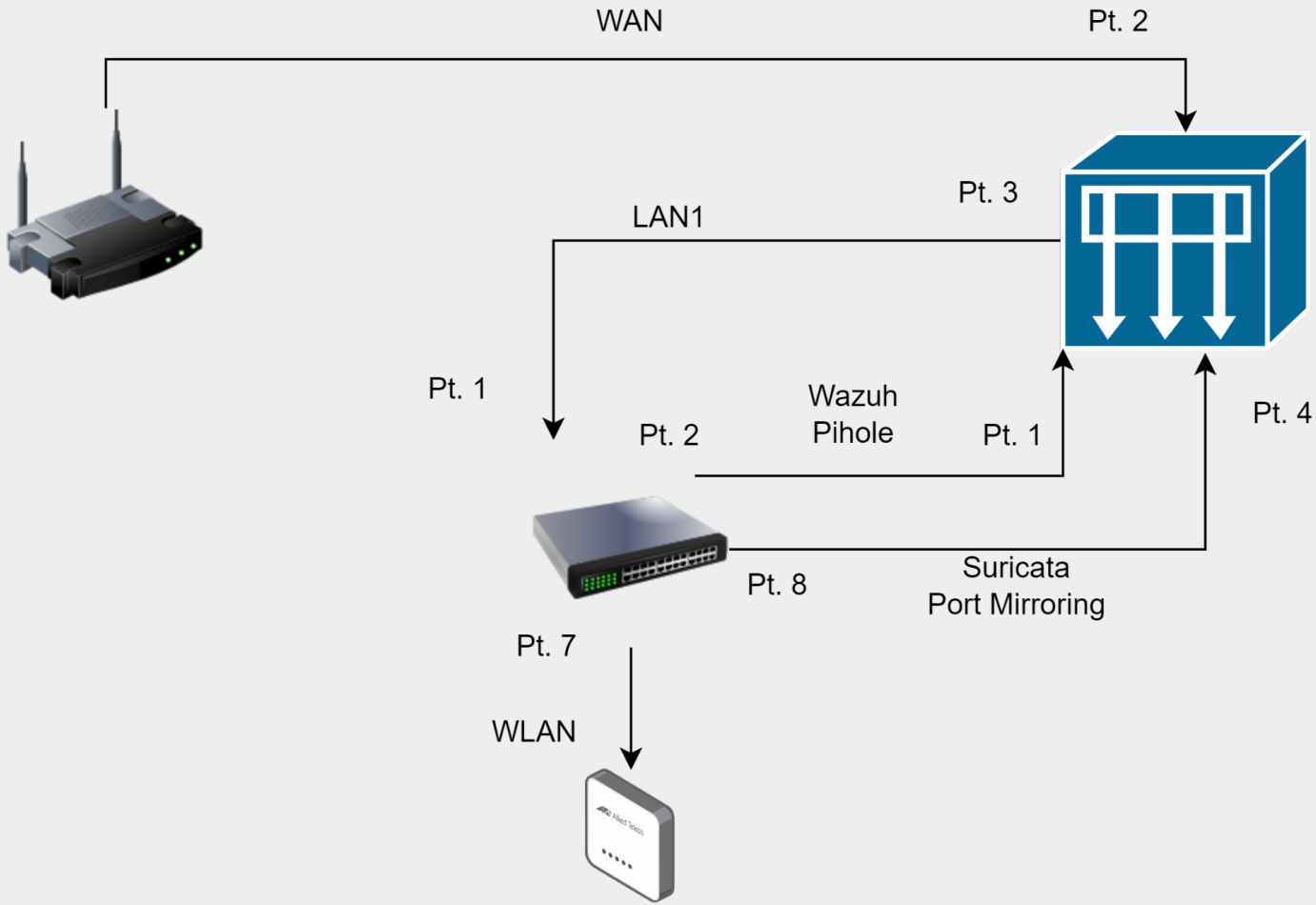
Fase 2

Retos

- Integrar Firewall PFSense
- Integrar dispositivos inalámbricos

Nuevas adquisiciones


pfsense
Mobile
WinSrv
Win10
Kali
wazuh.
Generic University

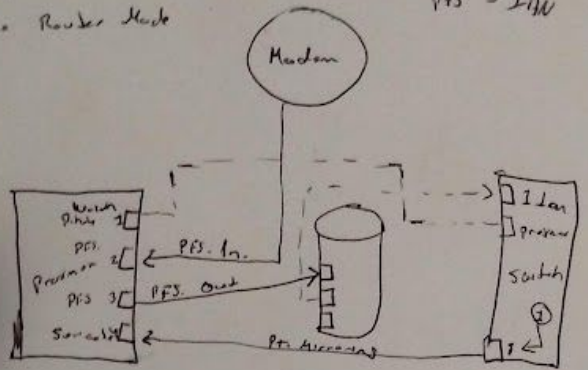

WAN
Pt. 2
Pt. 3
LAN1
Pt. 1
Wazuh
Pihole
Pt. 2
Pt. 1
Pt. 4
Pt. 8
Suricata
Port Mirroring
Pt. 7
WLAN

Op 1

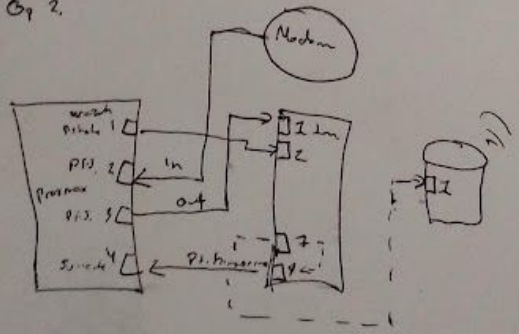
Bce Router Mode

p+2 - WAN

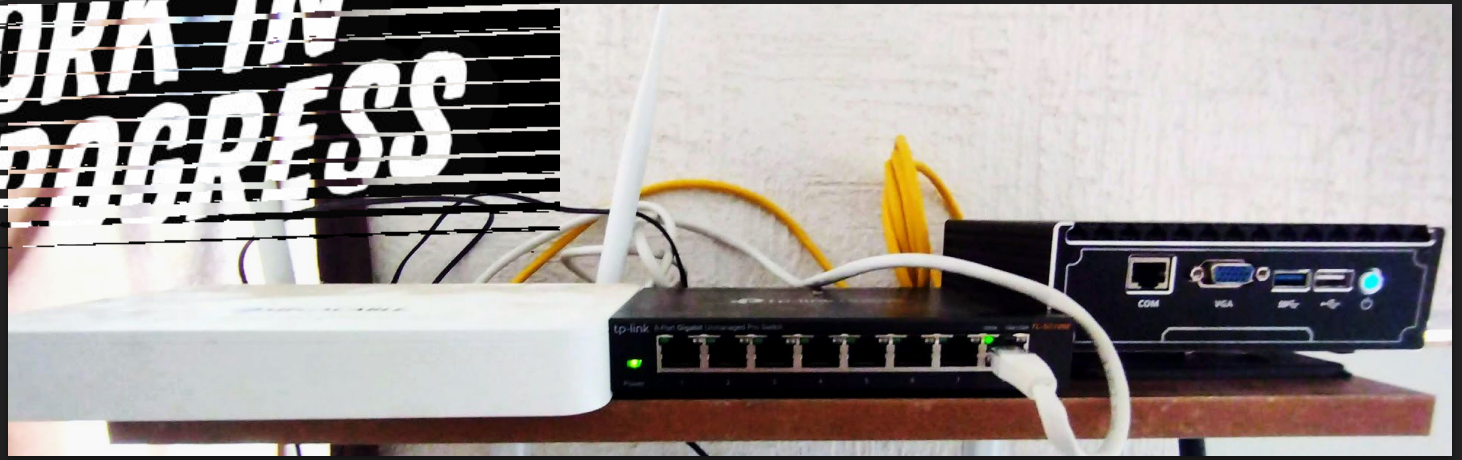
p+3 - LAN



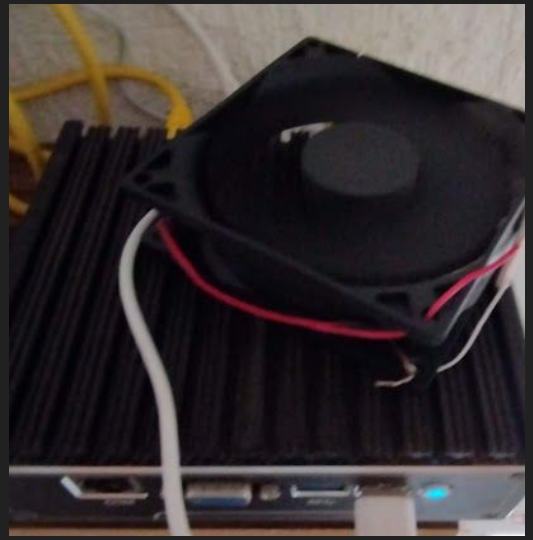
Op 2.

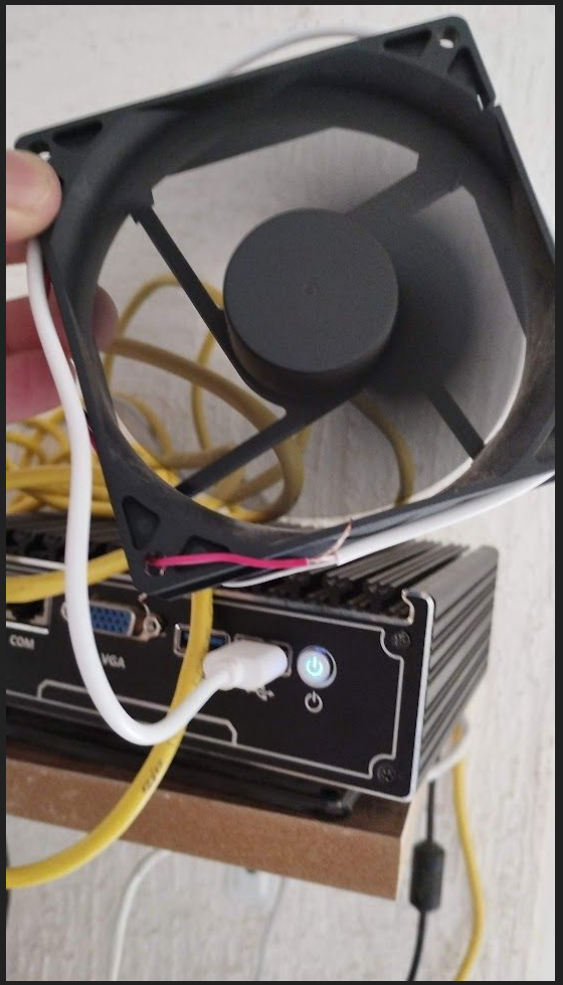


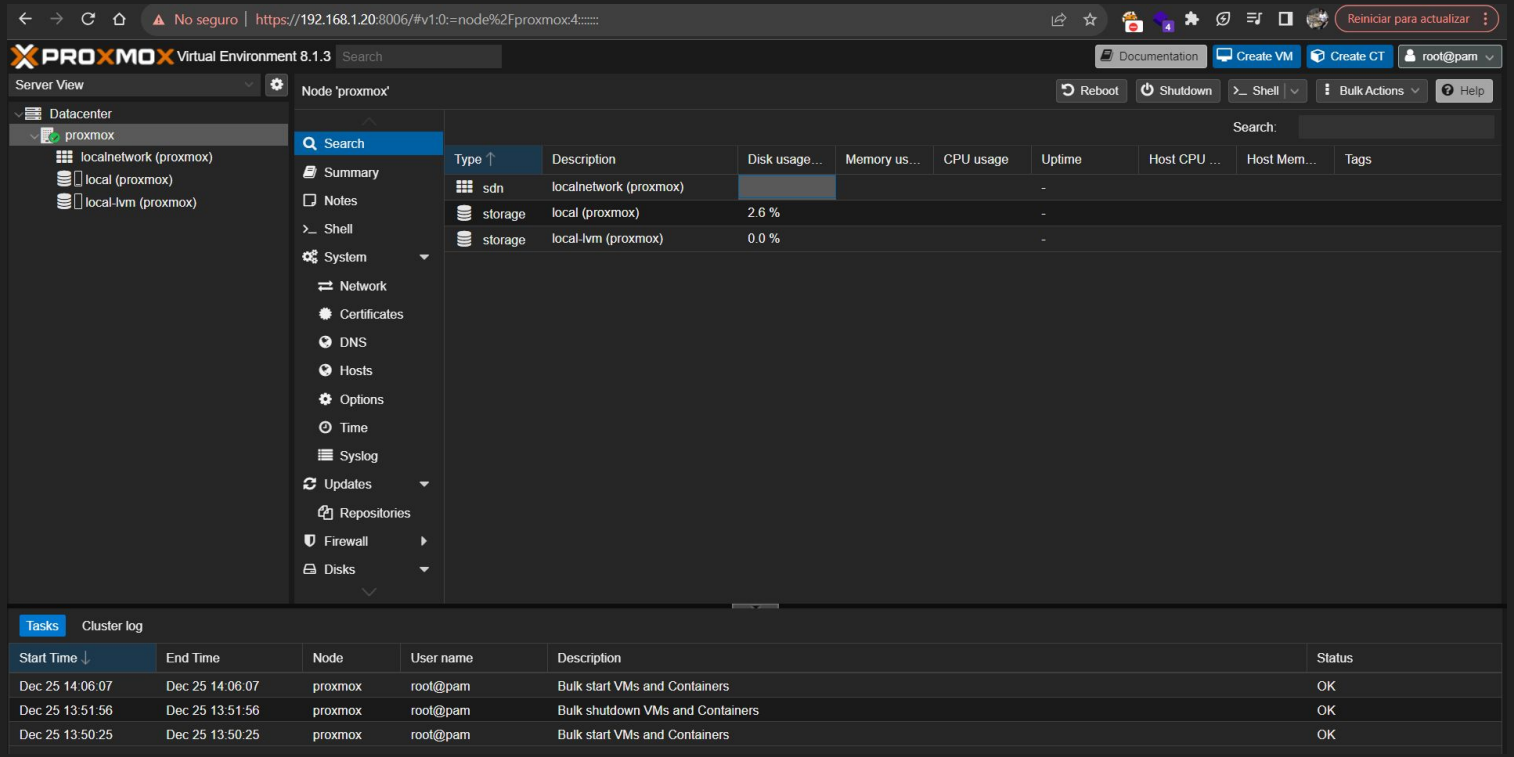
WORK IN PROGRESS

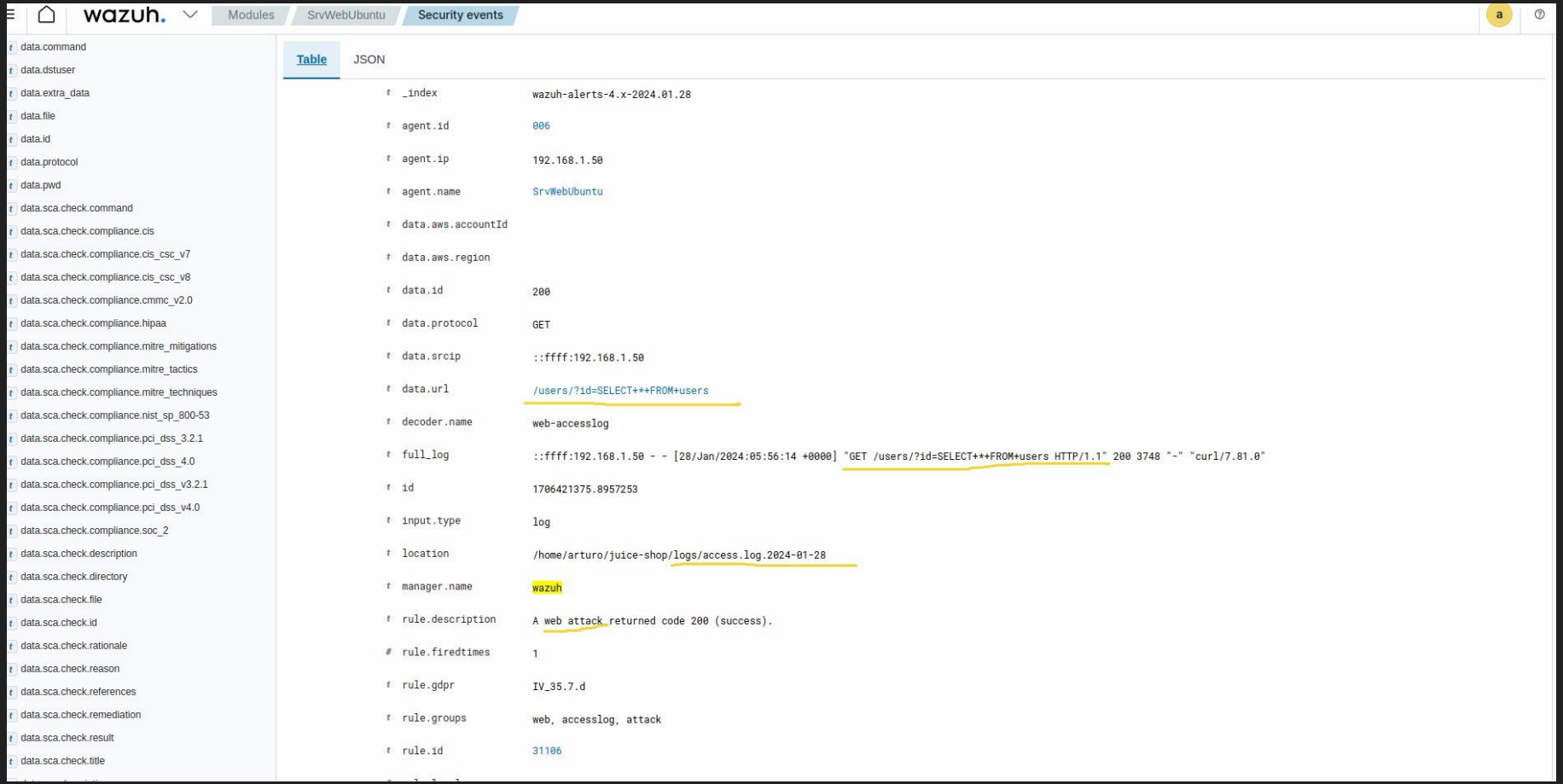


WORK IN PROGRESS




COM
VGA


No seguro | https://192.168.1.20:8006/#v1:0:=node%2Fproxmox:4::::::
Reiniciar para actualizar
PROXMOX Virtual Environment 8.1.3
Search
Documentation
Create VM
Create CT
root@pam
Server View
Datacenter
proxmox
localnetwork (proxmox)
local (proxmox)
local-lvm (proxmox)
Node 'proxmox'
Reboot
Shutdown
Shell
Bulk Actions
Help
Search
Summary
Notes
Shell
System
Network
Certificates
DNS
Hosts
Options
Time
Syslog
Updates
Repositories
Firewall
Disks
Search:
Type
Description
Disk usage...
Memory us...
CPU usage
Uptime
Host CPU ...
Host Mem...
Tags
sdn
localnetwork (proxmox)
storage
local (proxmox)
2.6 %
storage
local-lvm (proxmox)
0.0 %
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Dec 25 14:06:07
Dec 25 14:06:07
proxmox
root@pam
Bulk start VMs and Containers
OK
Dec 25 13:51:56
Dec 25 13:51:56
proxmox
root@pam
Bulk shutdown VMs and Containers
OK
Dec 25 13:50:25
Dec 25 13:50:25
proxmox
root@pam
Bulk start VMs and Containers
OK


wazuh.
Modules
SrvWebUbuntu
Security events
a
data.command
data.dstuser
data.extra_data
data.file
data.id
data.protocol
data.pwd
data.sca.check.command
data.sca.check.compliance.cis
data.sca.check.compliance.cis_csc_v7
data.sca.check.compliance.cis_csc_v8
data.sca.check.compliance.cmmc_v2.0
data.sca.check.compliance.hipaa
data.sca.check.compliance.mitre_mitigations
data.sca.check.compliance.mitre_tactics
data.sca.check.compliance.mitre_techniques
data.sca.check.compliance.nist_sp_800-53
data.sca.check.compliance.pci_dss_3.2.1
data.sca.check.compliance.pci_dss_4.0
data.sca.check.compliance.pci_dss_v3.2.1
data.sca.check.compliance.pci_dss_v4.0
data.sca.check.compliance.soc_2
data.sca.check.description
data.sca.check.directory
data.sca.check.file
data.sca.check.id
data.sca.check.rationale
data.sca.check.reason
data.sca.check.references
data.sca.check.remediation
data.sca.check.result
data.sca.check.title
Table
JSON
_index wazuh-alerts-4.x-2024.01.28
agent.id 006
agent.ip 192.168.1.50
agent.name SrvWebUbuntu
data.aws.accountId
data.aws.region
data.id 200
data.protocol GET
data.srcip ::ffff:192.168.1.50
data.url /users/?id=SELECT+*+FROM+users
decoder.name web-accesslog
full_log ::ffff:192.168.1.50 - - [28/Jan/2024:05:56:14 +0000] "GET /users/?id=SELECT+*+FROM+users HTTP/1.1" 200 3748 "-" "curl/7.81.0"
id 1706421375.8957253
input.type log
location /home/arturo/juice-shop/logs/access.log.2024-01-28
manager.name wazuh
rule.description A web attack returned code 200 (success).
rule.firedtimes 1
rule.gdpr IV_35.7.d
rule.groups web, accesslog, attack
rule.id 31106

Pi-hole

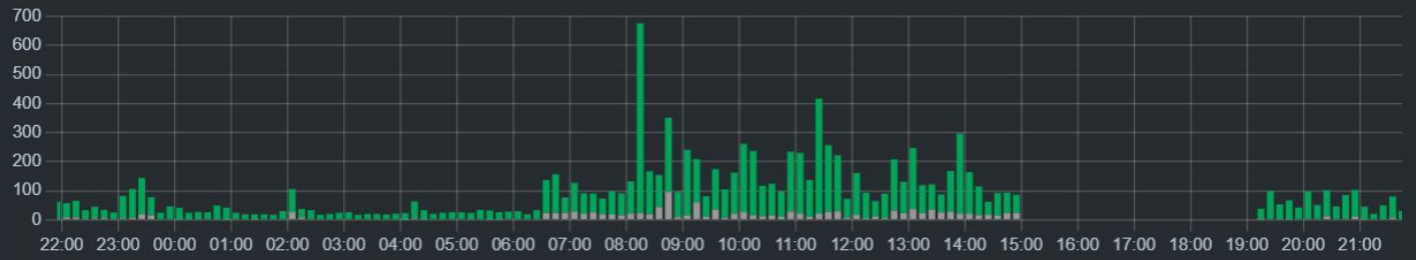
hostname: pihole

Status
Active
Load: 2.21 2.42 2.16
Memory usage: 12.7 %
Temp: 47.0 °C

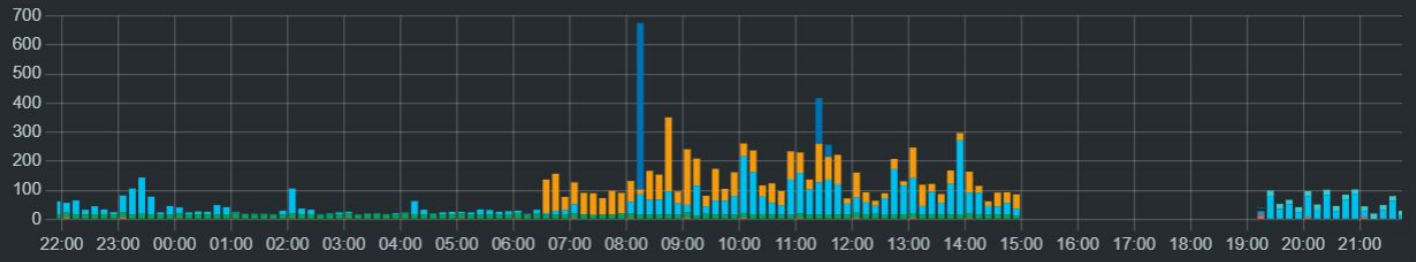
- Dashboard
- Query Log
- Long-term Data
- Groups
- Clients
- Domains
- Adlists
- Disable Blocking
- Local DNS
- Tools
- Settings
- Donate

Total queries	Queries Blocked	Percentage Blocked	Domains on Adlists
11,242	1,347	12%	172,482
8 active clients	List blocked queries	List all queries	Manage adlists

Total queries over last 24 hours



Client activity over last 24 hours



Retos

- Diseño de red
- Configuración PFSense
- Migrar dispositivos a la nueva red

Conclusiones

- Wazuh
- PFSense
- Pihole
- ~~Suricata~~
- Proxmox

Next steps

- Monitoreo de red inalámbrica
- VPN
- Smart Home
- Electricidad

Referencias

- https://www.youtube.com/@NetworkChuck
- https://documentation.wazuh.com/current/quickstart.html
- https://forum.proxmox.com/threads/start-and-stop-kvm-vm-from-command-line.580/
- https://forum.proxmox.com/threads/temporary-failure-in-name-resolution.133176/

Gracias

#BugBites