

QUBES OS 4

A reasonably secure operating system

FIRST TC - 10 september 2018
Presented by Xavier BAHUON, CISSP at ACTION CYBER

Summary

- **What is Qubes OS ?**
- **How does it works ?**
- **Use case :**
 - Receipt of documents (HR, Marketing...)
 - Administrator IT
 - Pentesting Lab
- **And more...**
- **Gaps and roadmap !**

What is Qubes OS ?

- License GNU GPL v2



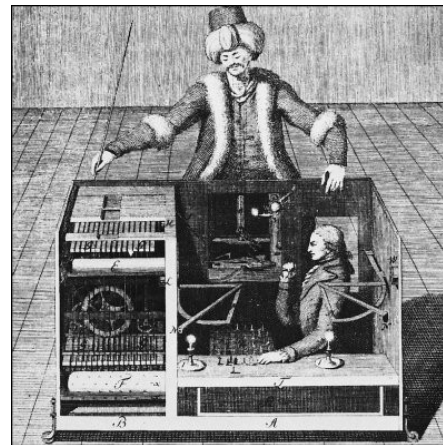
- Hypervisor “bare metal” : Xen OS



- Virtualize : Linux, Windows



- Approach :
Don't trust the hardware



What is Qubes OS ?

- Hardware Compatibility List

HARDWARE TYPE

- Laptop Devices
- Desktop, Workstation & Servers
- Motherboards
- + Add Your Device

MARKS & COLOURS

- yes**: feature is working correctly
- unknown**: a blank cell indicates we lack information
- partial**: some tweaking is needed, see remarks for more information
- no**: does not work or is not present

LIST COLUMNS

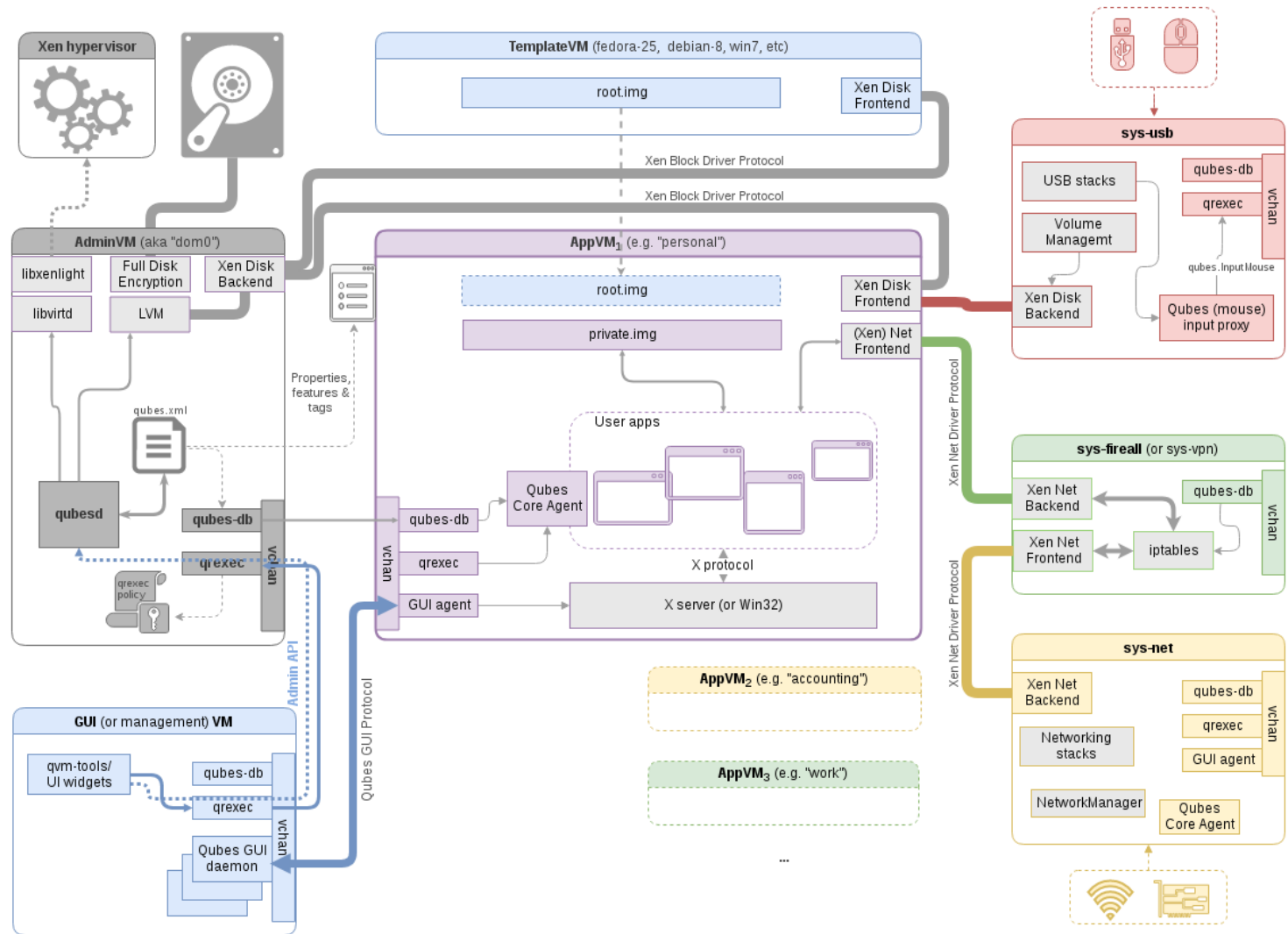
- Model**: Manufacturer and Devicename (Socket/CPU, Chipset/Southbridge, Graphics)
- BIOS**: Reported BIOS version
- HVM**: Intel VT-x or AMD-v technology (required for running HVM domains, such as Windows-based AppVMs)
- IOMMU**: Intel VT-d or AMD IOMMU technology (required for effective isolation of network VMs and PCI passthrough)
- SLAT**: Second Level Address Translation (SLAT): Intel VT-x support for Extended Page Tables (EPT) or AMD-V support for Rapid Virtualization Indexing (RVI).
- TPM**: TPM with proper BIOS support (required for Anti Evil Maid)
- Qubes**: Reported Qubes version (R=Release, rc=release candidate, B=Beta, i.e.: R1, R2B1, R2rc1)
- Kernel**: Reported dom0 kernel version (numbers in uname -r), can be selected during Installation and boot in Troubleshooting menu
- Remark**: Further Information field. Qubes, Kernel and this field is coloured in conjunction to reflect general machine compatibility
- Credit**: Name linked to report in qubes-users

LAPTOP DEVICES

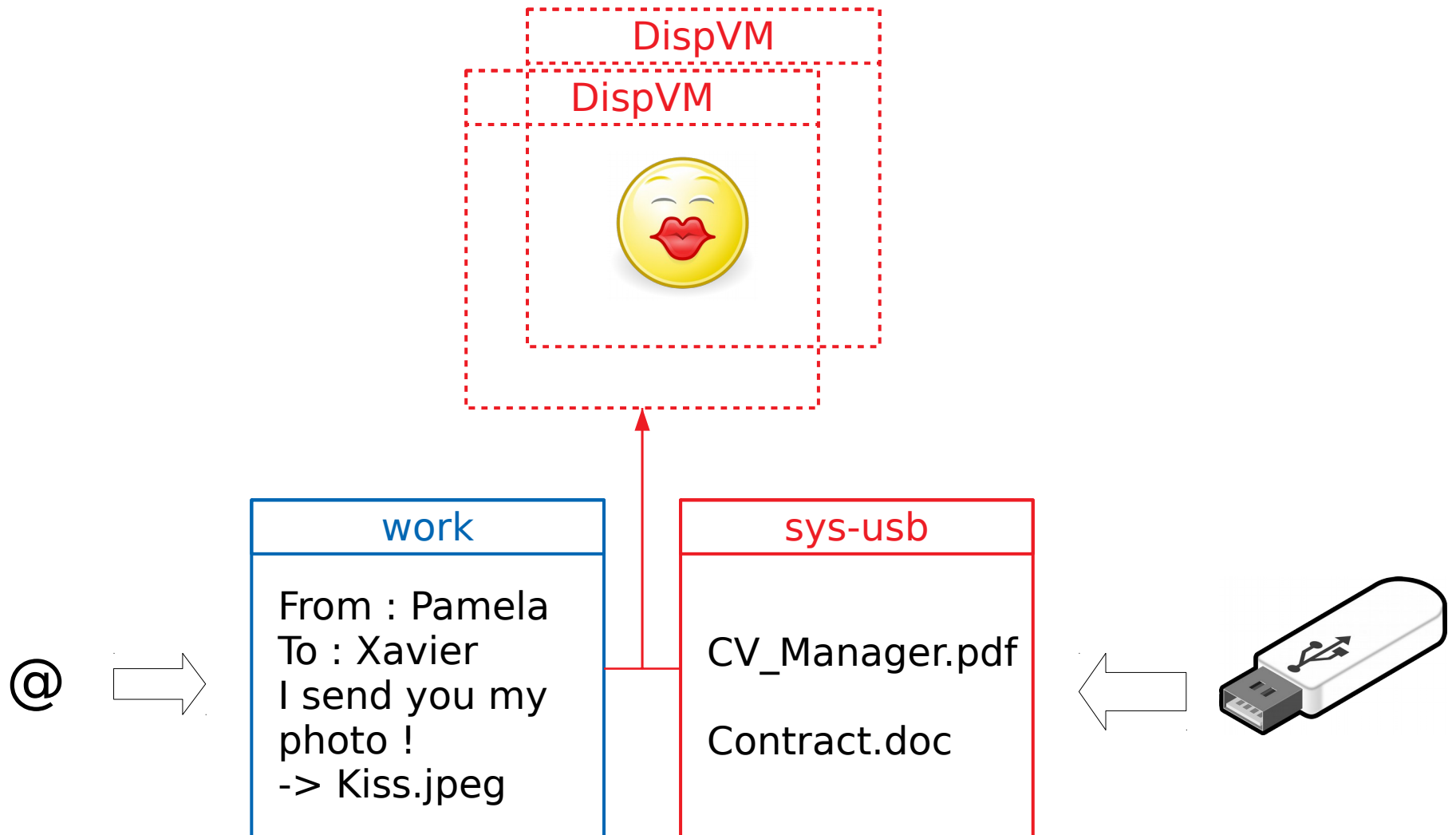
| Model | BIOS | HVM | IOMMU | SLAT | TPM | Qubes | Xen | Kernel | Remark | Credit |
|--|------------|-----|-------|---------|-----|-------|---------|-----------|---|---------------|
| ASUS N56VZ HM67 Express HD Graphics | N56VZ.216 | yes | no | unknown | | R2rc2 | 4.1.6.1 | 3.12.23-1 | Chipset does not support VT-d | Oleg Artemiev |
| ASUS X55A | | no | no | unknown | | R2B2 | | 3.7.6 | read more | Zrubi |
| ASUS X750JA I7-4700HQ HM86 HD Graphics 4600 | X750JB.208 | yes | yes | unknown | | R2 | 4.1.6.1 | 3.12.23-1 | Enable legacy CSM and disable secure boot in BIOS | HawKing |

How does it works ?

Architecture of QUBES OS

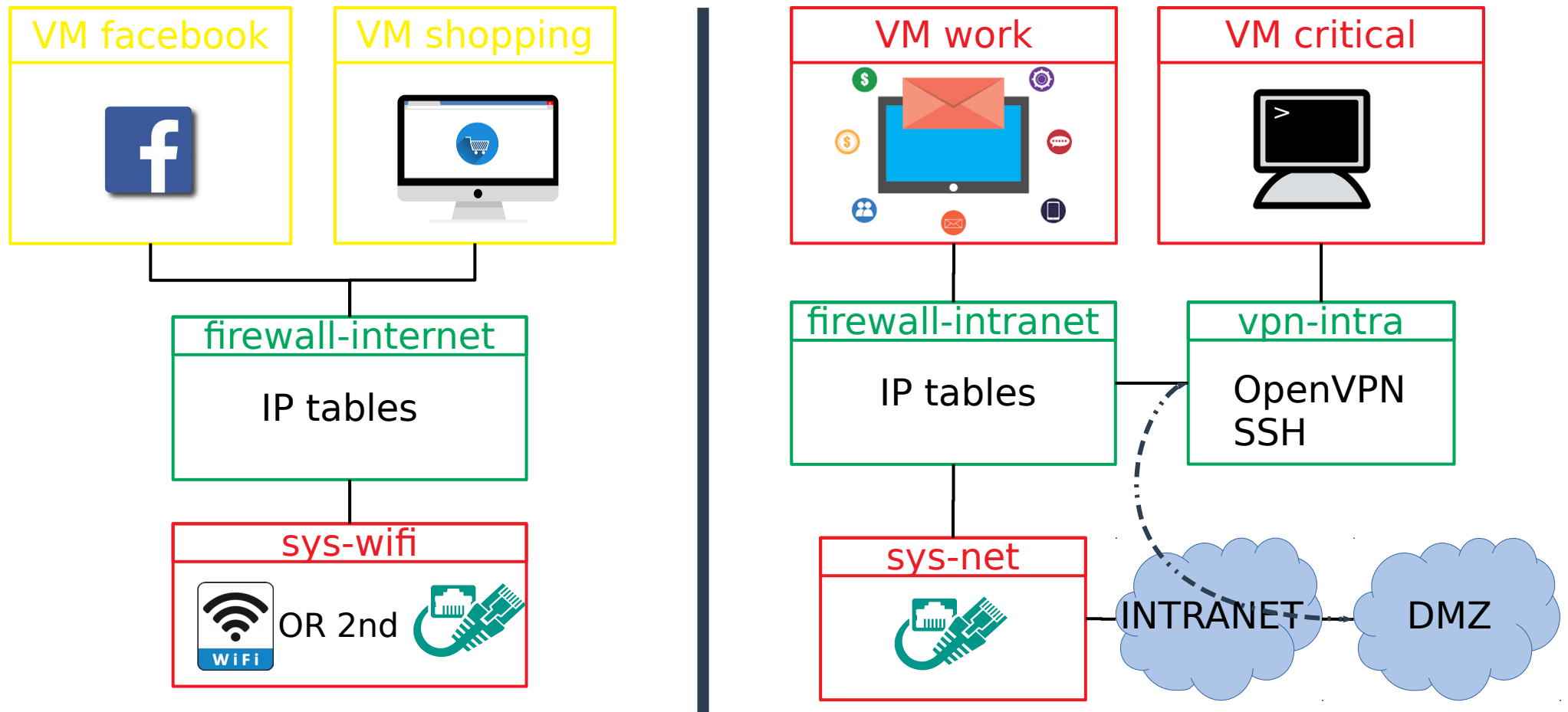


Use Case -> Receipt of documents (HR, Marketing...)

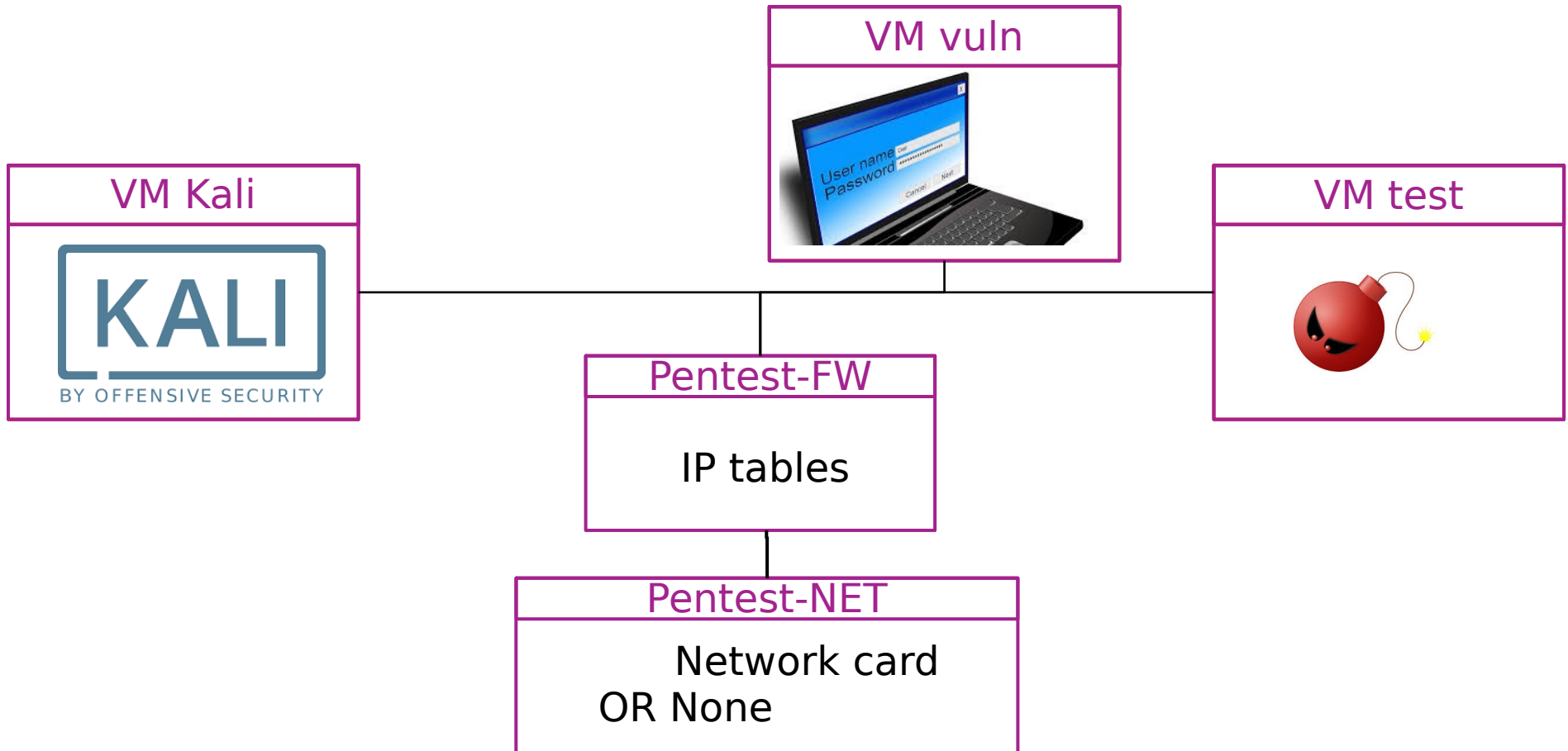


Use Case -> Administrator IT

Same machine but compartmentalization



Use Case -> Pentesting Lab



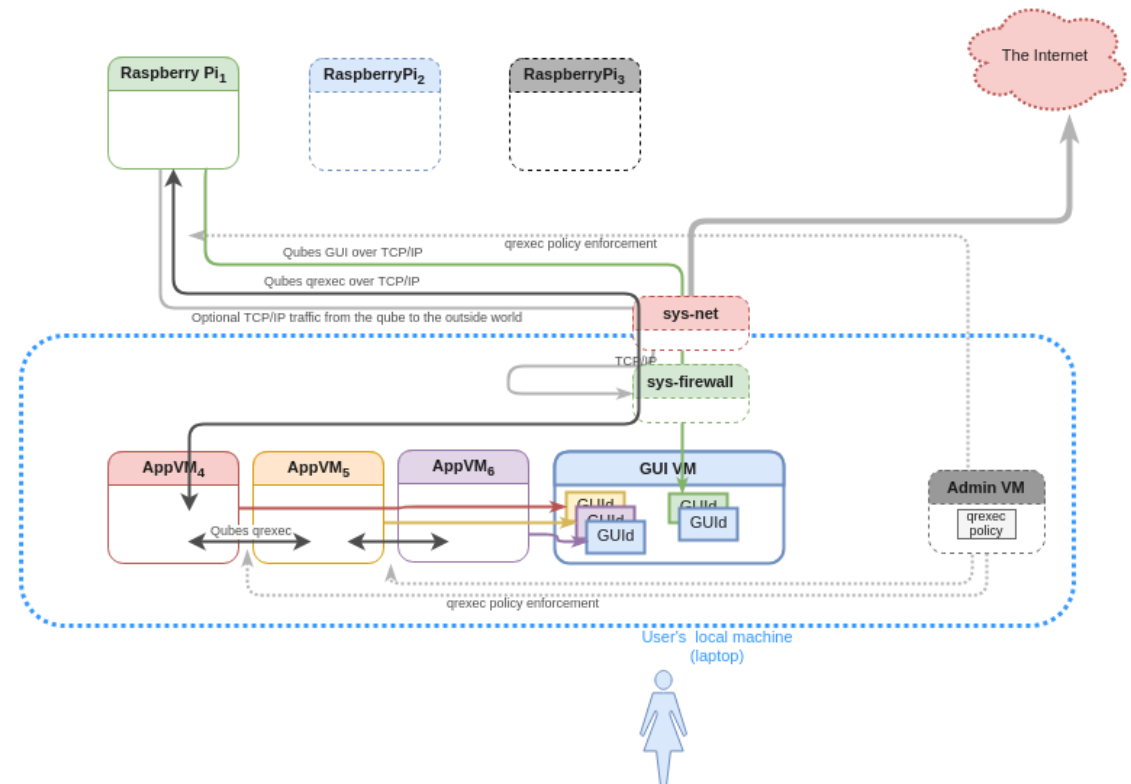
And more...

- **The Salt Deployment architecture**
- **Anonymization with Tor**

→ **www.qubes-os.org**

Gaps and roadmap !

- Air GAP
- Forensic lab
- GPU-passtru



Thank you for your attention

Questions ?