# From Kali and a Couple of VMs to NextGen Home Lab

"An Approach to Practice and Develop your Skills"

Bashar Shamma
@1337bash

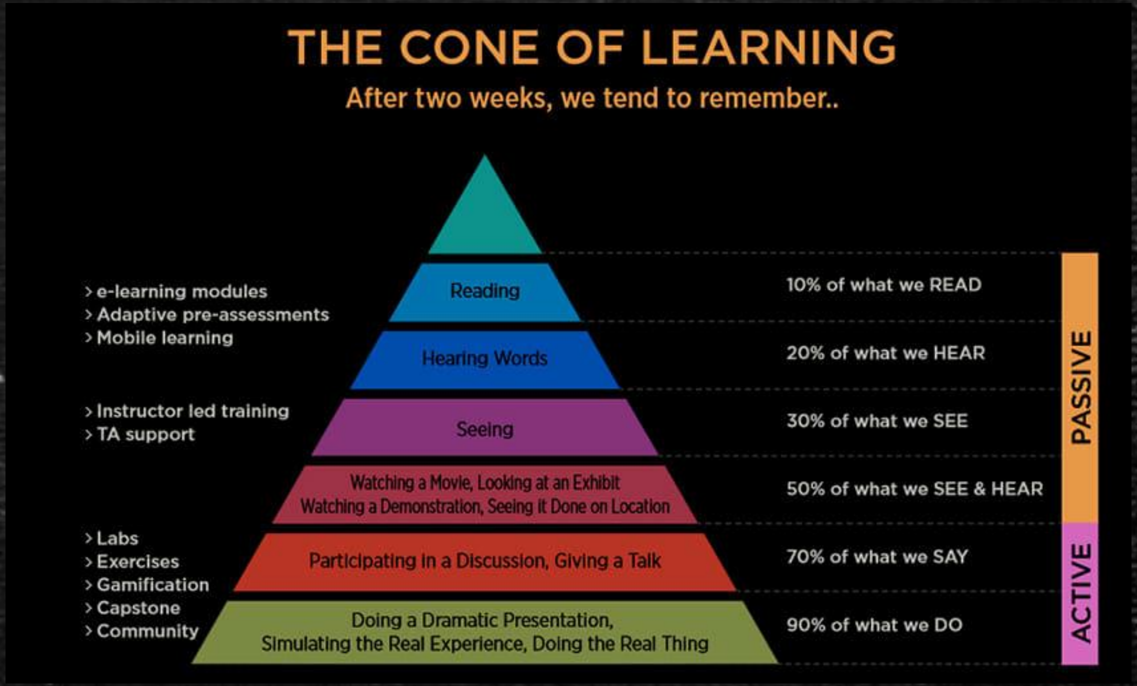
# Who Am I?

- Blue Team at a Fortune 100
- MS from UH
- GIAC x4
- @1337bash.

”SUCCESS IS A JOURNEY NOT A DESTINATION.”

# The Rationality of a Home Lab

- We learn by doing
  - A place to experiment
- Access to technologies beyond what’s available at work
- Separate network from home network



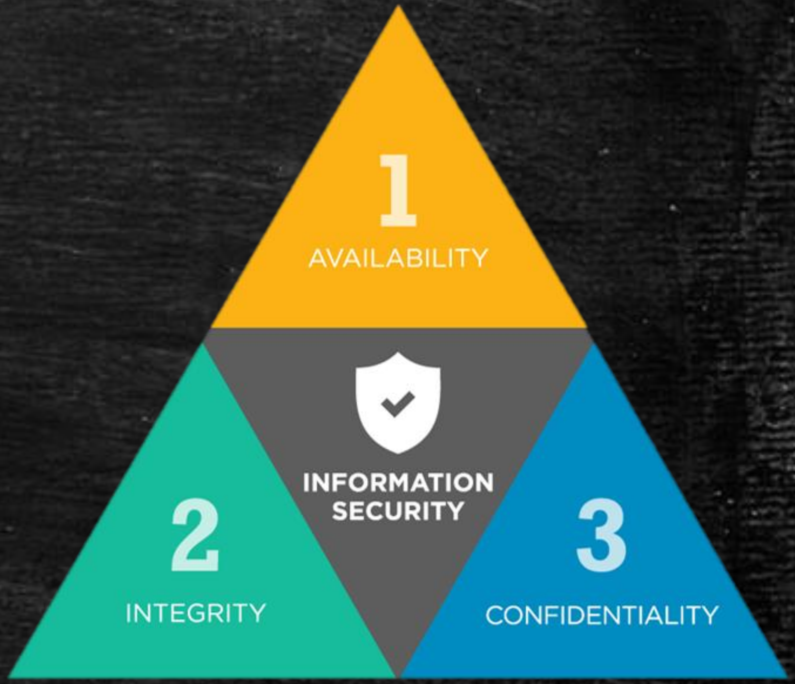
THE CONE OF LEARNING

After two weeks, we tend to remember..

› e-learning modules
› Adaptive pre-assessments
› Mobile learning
› Instructor led training
› TA support
› Labs
› Exercises
› Gamification
› Capstone
› Community
Reading
Hearing Words
Seeing
Watching a Movie, Looking at an Exhibit
Watching a Demonstration, Seeing it Done on Location
Participating in a Discussion, Giving a Talk
Doing a Dramatic Presentation,
Simulating the Real Experience, Doing the Real Thing
10% of what we READ
20% of what we HEAR
30% of what we SEE
50% of what we SEE & HEAR
70% of what we SAY
90% of what we DO
PASSIVE
ACTIVE

# NextGen HomeLab

- Enterprise in a box
  - Fictional Company/Enterprise.
  - The whole infrastructure virtualized on one server
- Learn the Foundation:
  - Networking.
    - Firewalls, vLans, Routing
  - Virtualization.
  - Active directory.
  - Linux and Windows Administration.
  - Business operations. (understanding the A in CIA)

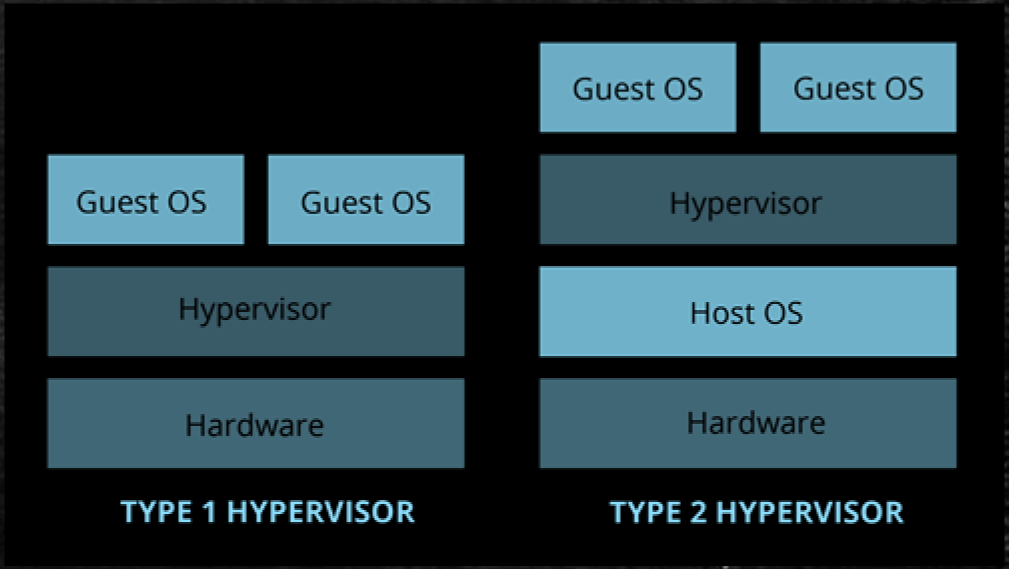


# Hardware

- The concept is scalable.
- Recommend dedicated machine with 32+ GB RAM
- SSD or NVMe Hard Drive.
- Deploy resource intensive VMs first .Drop after provisioning
  - Avg of 1 vCPU+ 0.5-1 GB RAM per VM for idle VMs.
- Primary Resource Consumers: VM that is actively working at all time.
  - SIEM
  - Packet Capture

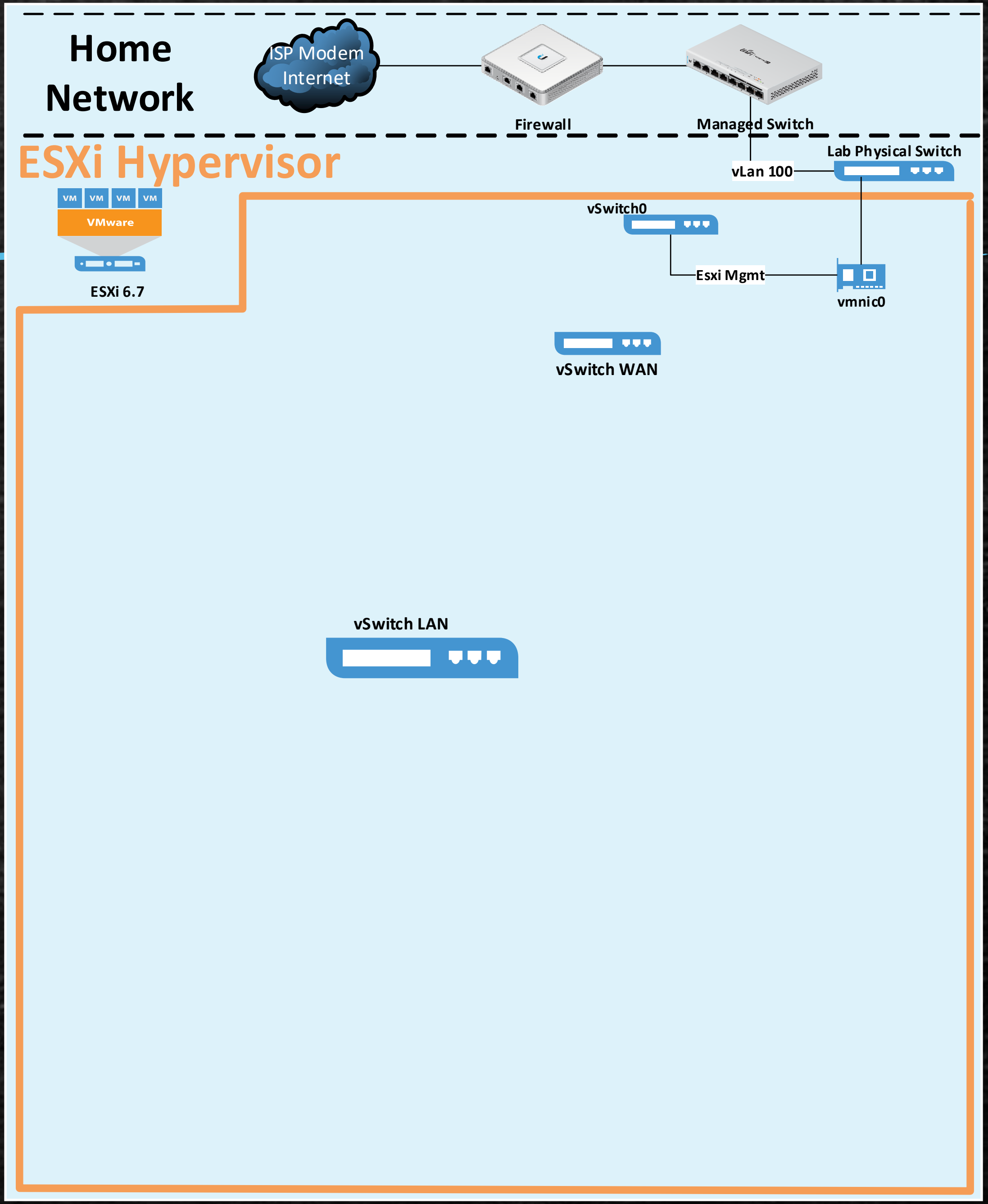
# Virtualization

- Type 1
  - VMware
    - Free ESXi → Max 8 vCPU per VM and a max of 2 CPUs in a physical ESXi host
    - vSphere/vCenter VMUG Advantage → $200/yr
  - Open Source
    - Proxmox
    - Xen
    - KVM
- Type 2
  - Commercial: VMware Workstation/Fusion
  - Free and Open Source: VirtualBox



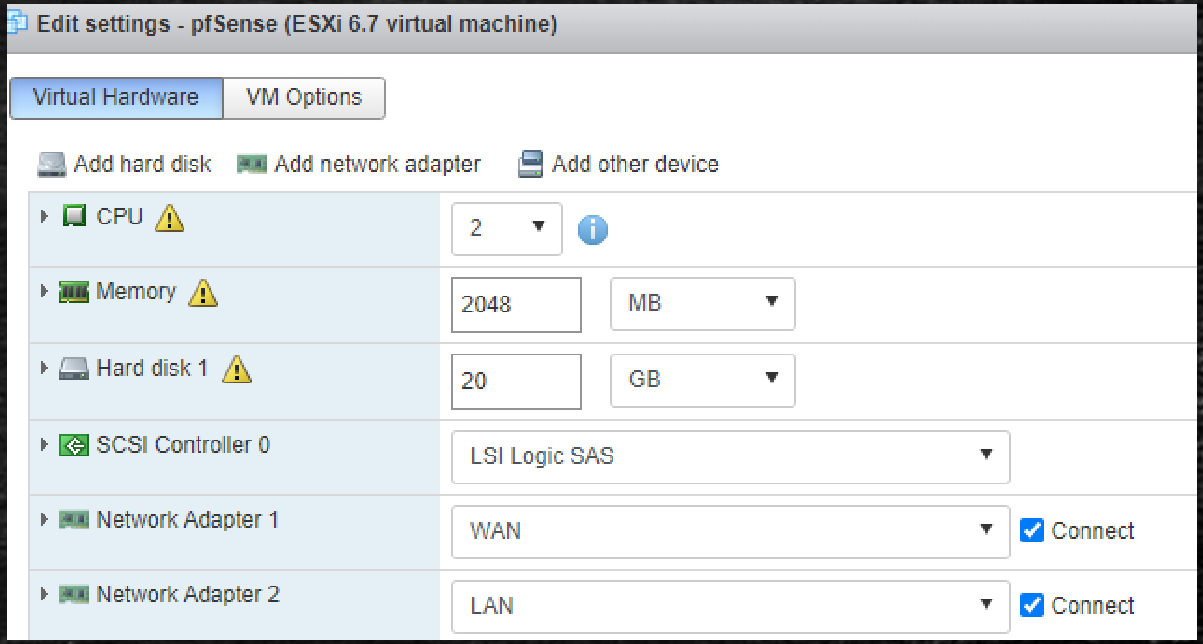
# Building the NextGen Home Lab

1. Separate Home Network
2. Build Hypervisor
3. Add vSwitches
4. Deploy pfSense



# pfSense

- pfSense: Open Source Firewall
- Packages: Proxy, VPN, IDS.
- Deploy pfSense Firewall as a VM and attach 2 vNICs WAN and LAN.



Edit settings - pfSense (ESXi 6.7 virtual machine)

CPU: 2

Memory: 2048 MB

Hard disk 1: 20 GB

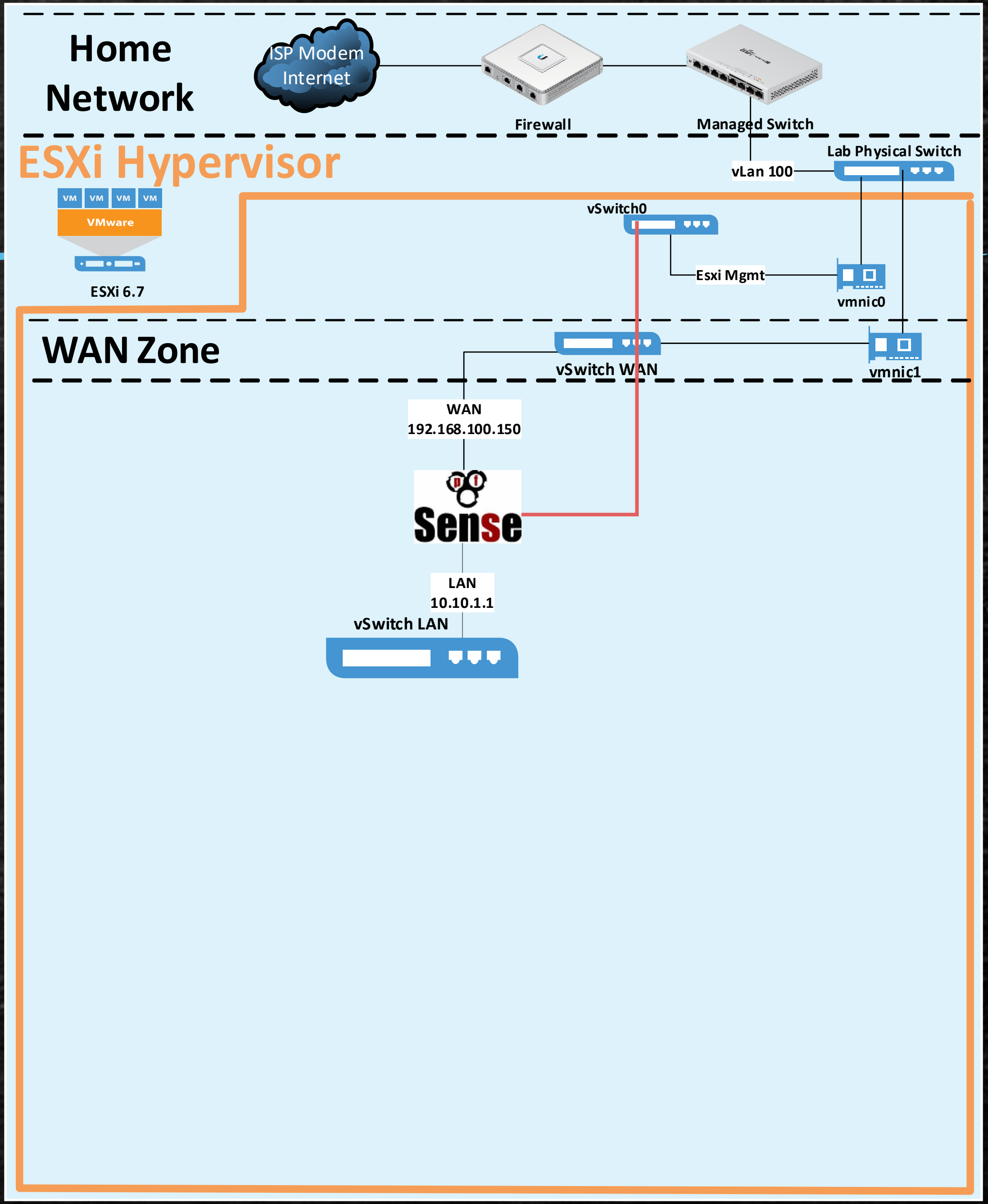
SCSI Controller 0: LSI Logic SAS

Network Adapter 1: WAN ☑ Connect

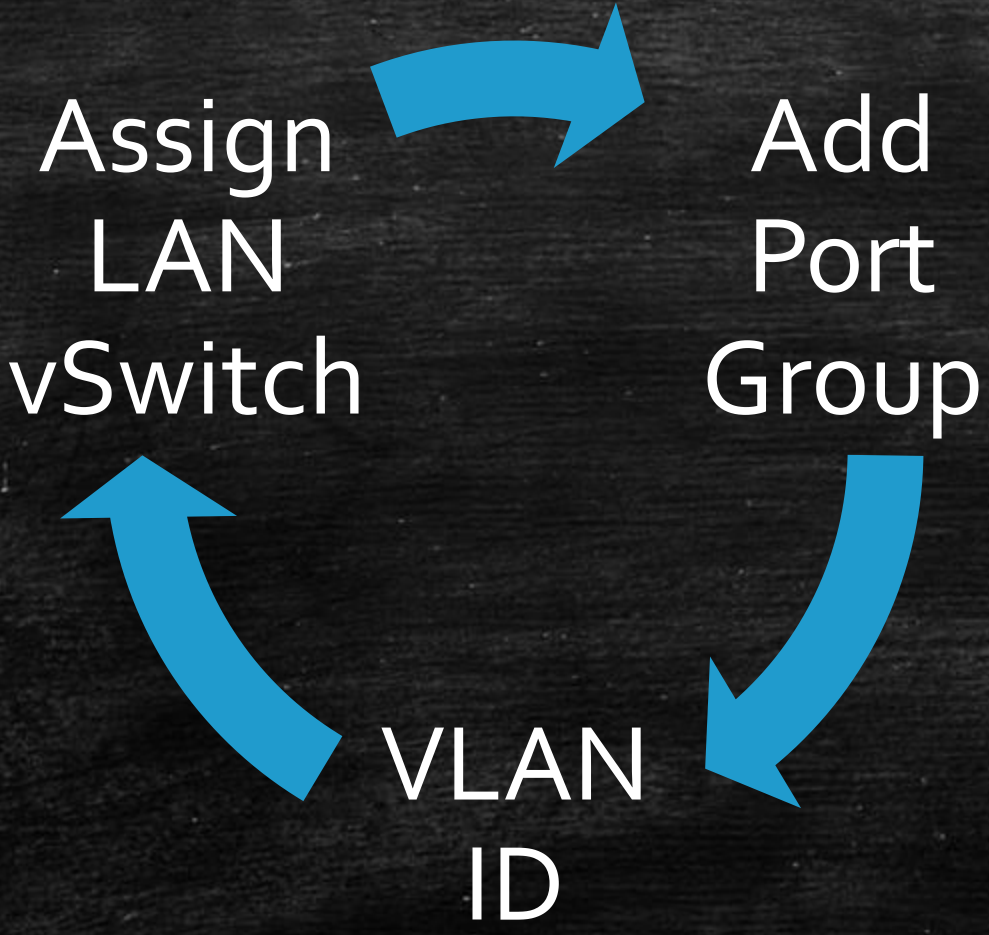
Network Adapter 2: LAN ☑ Connect

# Building the NextGen Home Lab

1. Separate Home Network
2. Build Hypervisor
3. Add vSwitches
4. Deploy pfSense
5. Configure VLANS



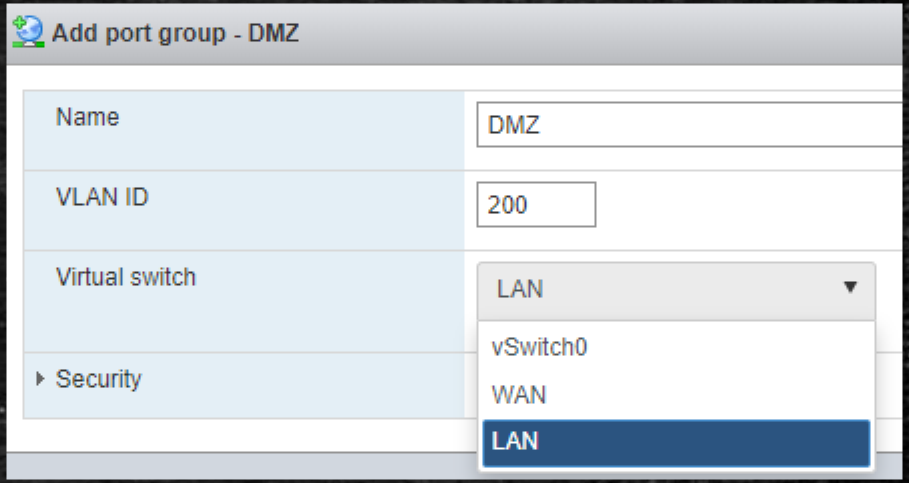
# Configure VLANs - ESXi



Assign LAN vSwitch

Add Port Group

VLAN ID



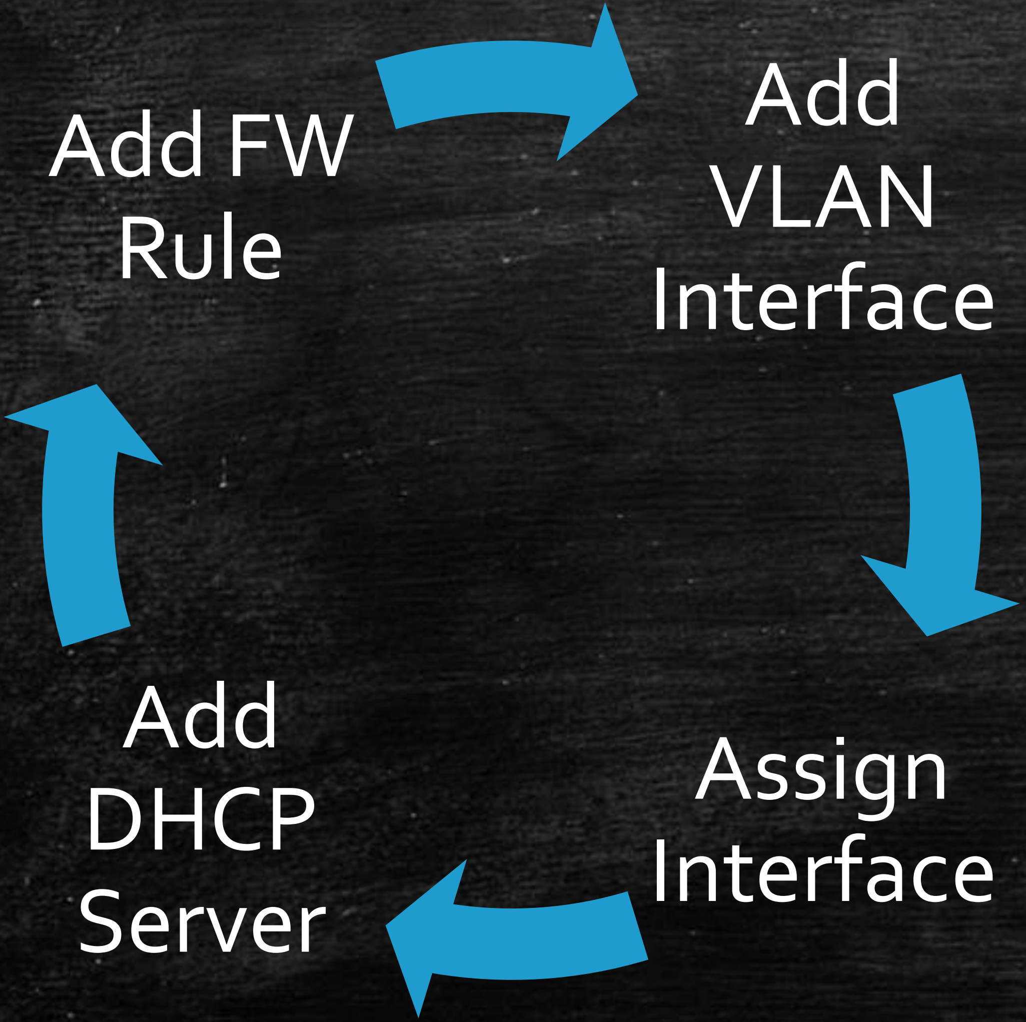
Add port group - DMZ

Name: DMZ

VLAN ID: 200

Virtual switch: LAN

# Configure VLANs - pfSense

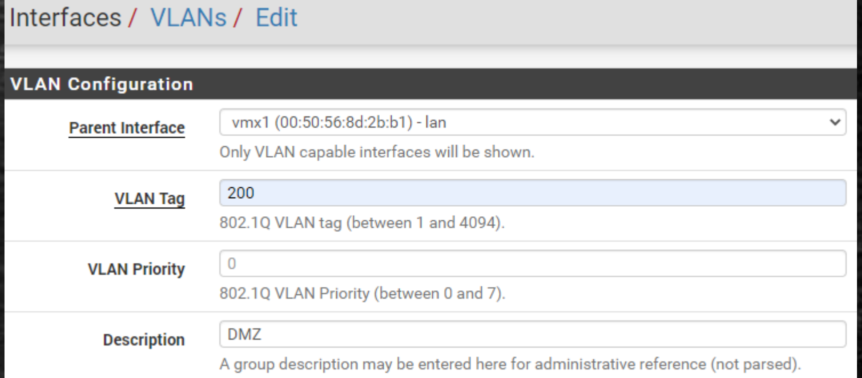


Add VLAN Interface

Assign Interface

Add DHCP Server

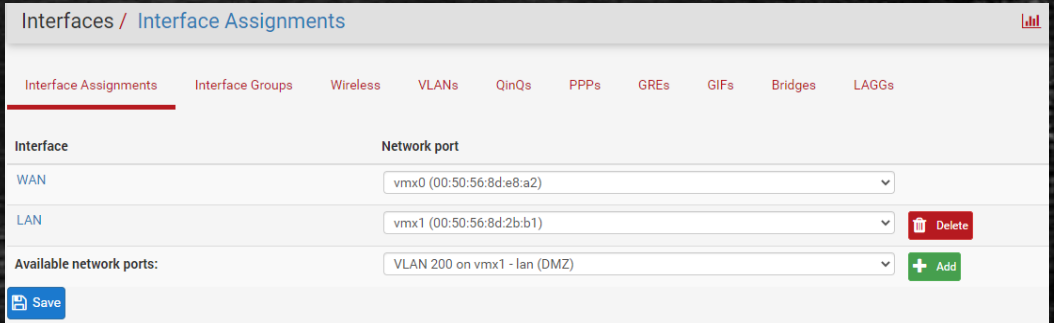
Add FW Rule



Interfaces / VLANs / Edit

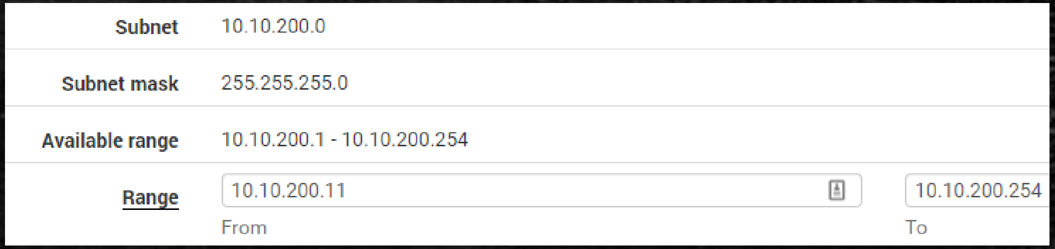
**VLAN Configuration**

| | |
|---|---|
| Parent Interface | vmx1 (00:50:56:8d:2b:b1) - lan<br>Only VLAN capable interfaces will be shown. |
| VLAN Tag | 200<br>802.1Q VLAN tag (between 1 and 4094). |
| VLAN Priority | 0<br>802.1Q VLAN Priority (between 0 and 7). |
| Description | DMZ<br>A group description may be entered here for administrative reference (not parsed). |



Interfaces / Interface Assignments

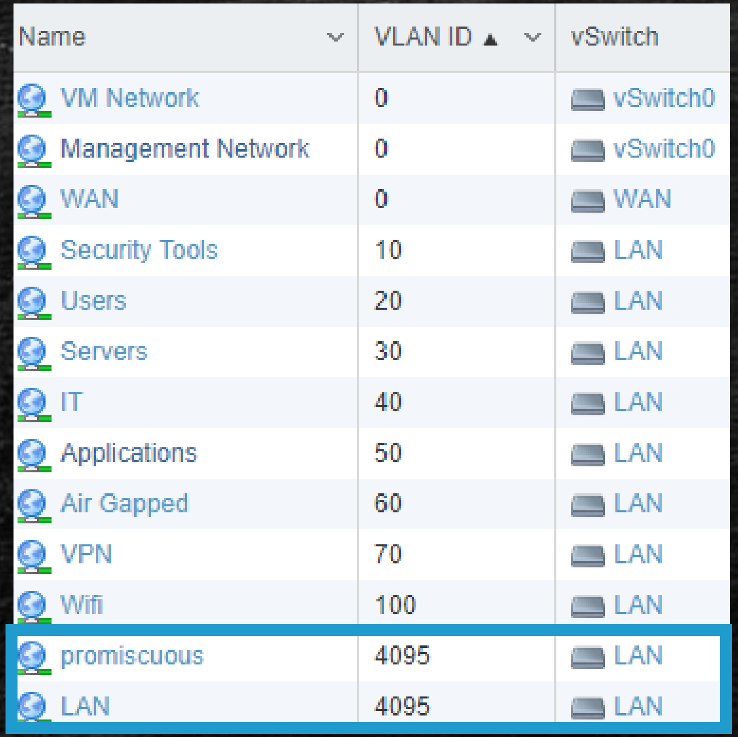
| Interface | Network port |
|---|---|
| WAN | vmx0 (00:50:56:8d:e8:a2) |
| LAN | vmx1 (00:50:56:8d:2b:b1) Delete |
| Available network ports: | VLAN 200 on vmx1 - lan (DMZ) Add |



| | |
|---|---|
| Subnet | 10.10.200.0 |
| Subnet mask | 255.255.255.0 |
| Available range | 10.10.200.1 - 10.10.200.254 |
| Range | 10.10.200.11 From<br>10.10.200.254 To |

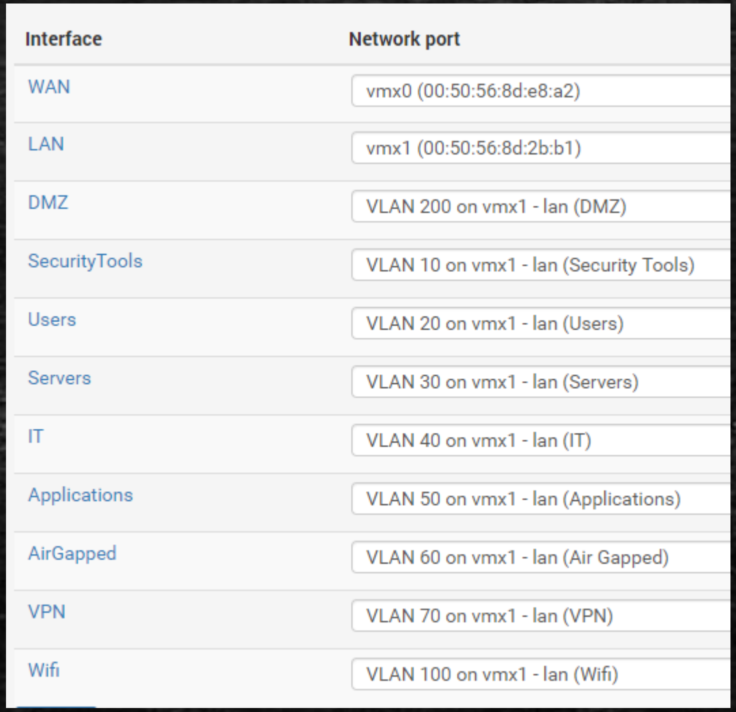
# VLANS

## ESXi



| Name | VLAN ID ▲ | vSwitch |
|---|---|---|
| VM Network | 0 | vSwitch0 |
| Management Network | 0 | vSwitch0 |
| WAN | 0 | WAN |
| Security Tools | 10 | LAN |
| Users | 20 | LAN |
| Servers | 30 | LAN |
| IT | 40 | LAN |
| Applications | 50 | LAN |
| Air Gapped | 60 | LAN |
| VPN | 70 | LAN |
| Wifi | 100 | LAN |
| promiscuous | 4095 | LAN |
| LAN | 4095 | LAN |

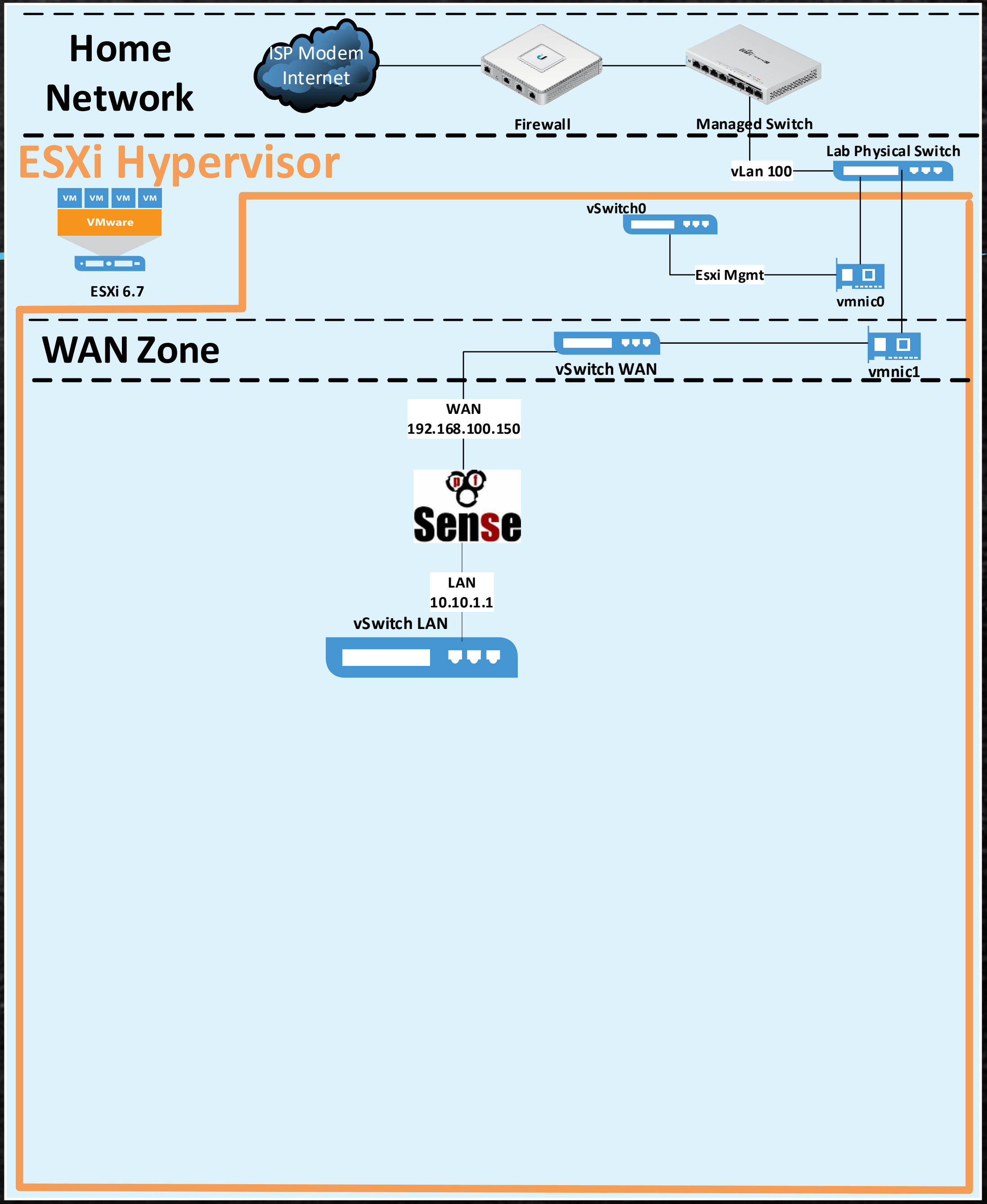
## pfSense



| Interface | Network port |
|---|---|
| WAN | vmx0 (00:50:56:8d:e8:a2) |
| LAN | vmx1 (00:50:56:8d:2b:b1) |
| DMZ | VLAN 200 on vmx1 - lan (DMZ) |
| SecurityTools | VLAN 10 on vmx1 - lan (Security Tools) |
| Users | VLAN 20 on vmx1 - lan (Users) |
| Servers | VLAN 30 on vmx1 - lan (Servers) |
| IT | VLAN 40 on vmx1 - lan (IT) |
| Applications | VLAN 50 on vmx1 - lan (Applications) |
| AirGapped | VLAN 60 on vmx1 - lan (Air Gapped) |
| VPN | VLAN 70 on vmx1 - lan (VPN) |
| Wifi | VLAN 100 on vmx1 - lan (Wifi) |

# Building the NextGen Home Lab

1. Separate Home Network
2. Build Hypervisor
3. Add vSwitches
4. Deploy pfSense
5. Configure VLANS
6. Build the Enterprise



# Core Servers & Enterprise Applications

## Servers

- Microsoft Free Trials
  - Windows 2012/2016/2019 as AD/DC – create a domain and make it a DNS server.
  - MSSQL Servers
  - SharePoint

  https://www.microsoft.com/en-us/evalcenter/try

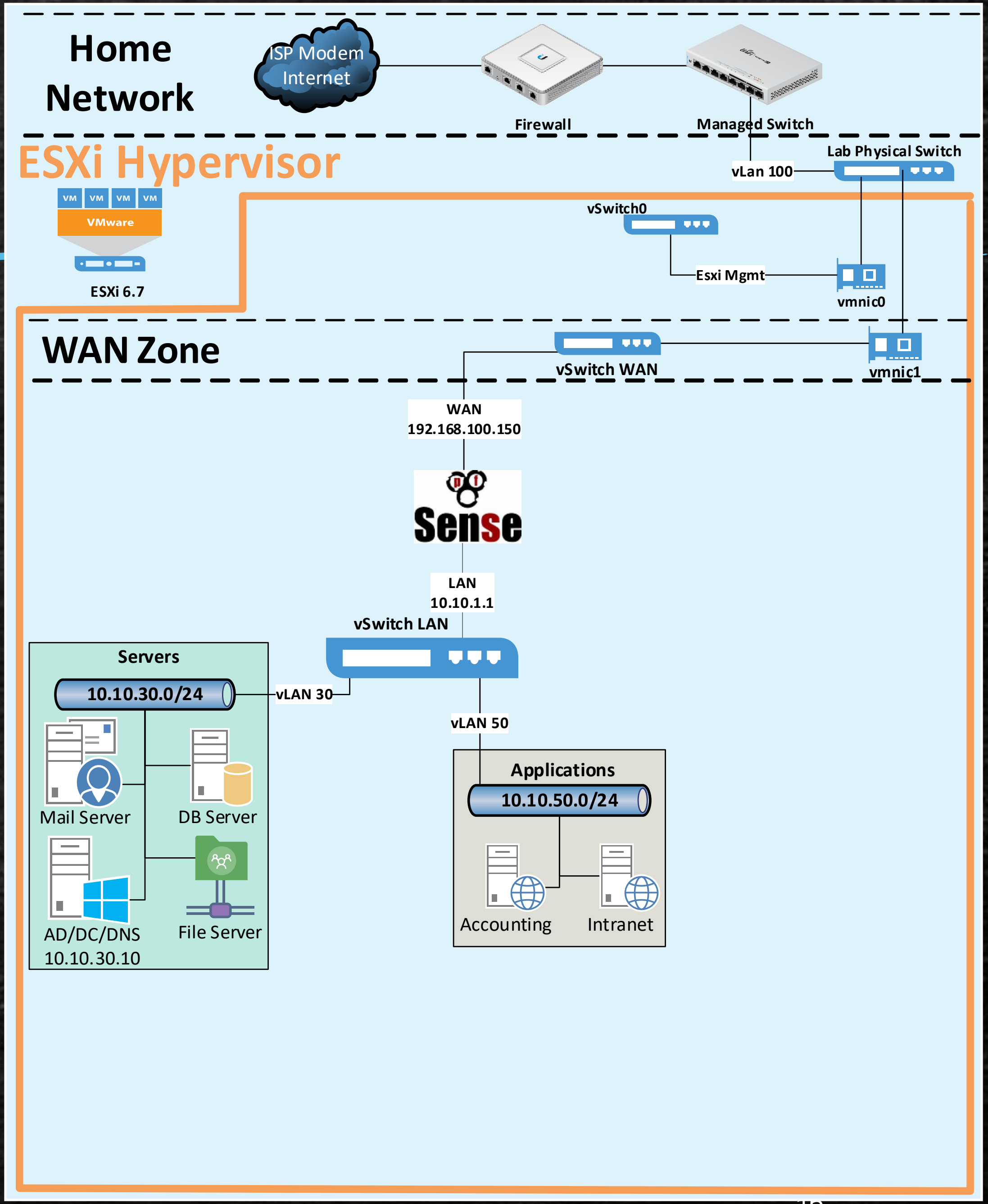
- Open Source
  - Email Server: Mail-in-a-Box/hMailServer
    - https://mailinabox.email/
    - https://www.hmailserver.com/
  - File Server: FreeNAS
    - https://www.freenas.org/

## Applications

- Intranet
  - Open Source Wiki or WordPress Projects
- Accounting/ERP? LedgerSMB
  - https://ledgersmb.org/
- Health Care? OpenEMR
  - https://www.open-emr.org/
- Vuln Servers
  - Metasploitable 2 or 3.
    - https://sourceforge.net/projects/metasploitable/
  - OWASP WebGoat
    - https://owasp.org/www-project-webgoat/

# Security Implication

- Open Company wide?
- Ports used by Core Servers
  - Active Directory
  - Databases
  - File Servers
    - Files Permissions.
- Management ports SSH RDP
- Default Configuration



# Enterprise Users & IT Admins

## Users

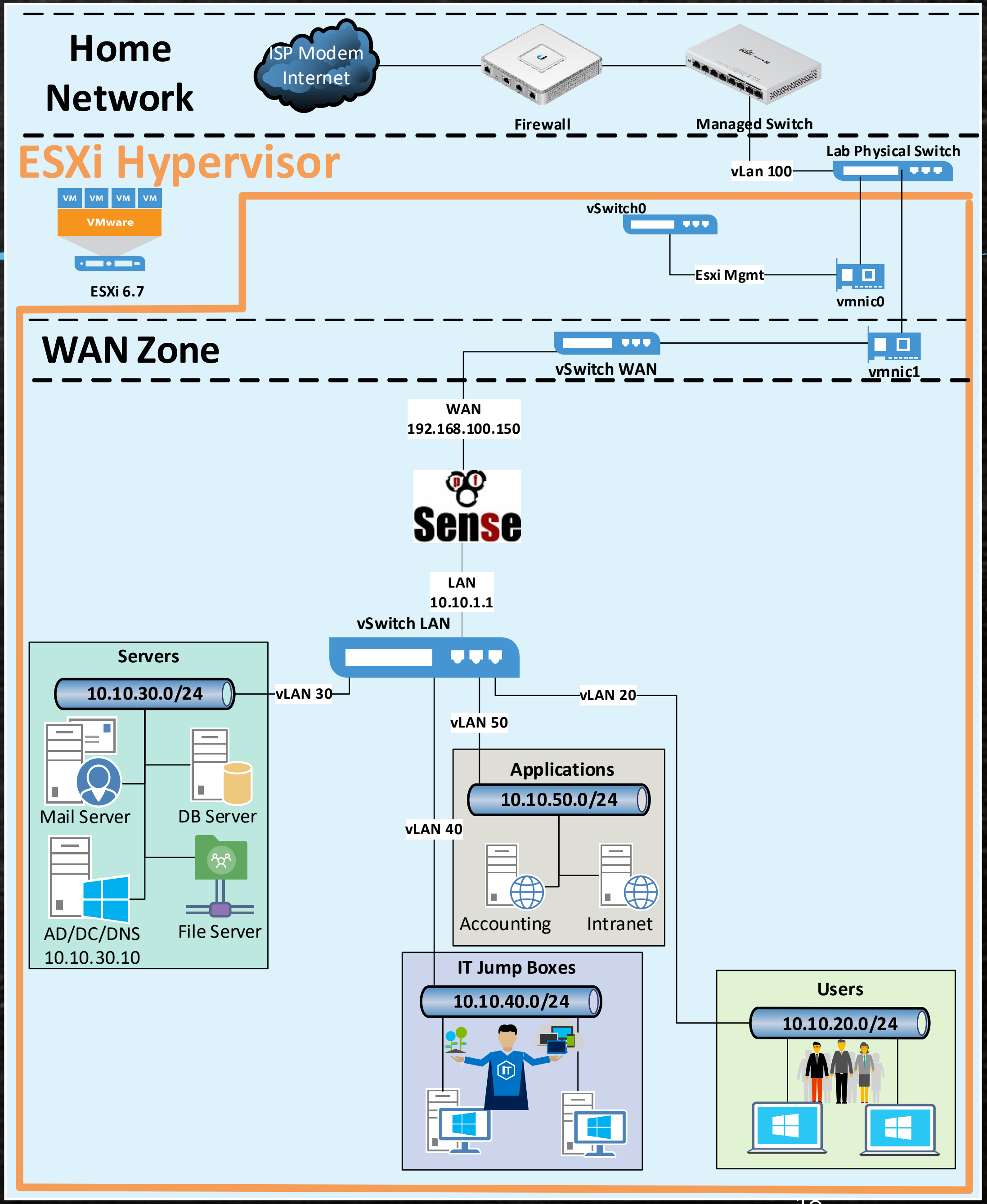
- Simulating employees
- Use Win10 as workstation/laptop
- AD object generator
  - https://www.secframe.com/badblood
- Scripts to generate traffic and user activity
  - https://github.com/ReconInfoSec/web-traffic-generator
  - https://github.com/ubeeri/Invoke-UserSimulator
  - https://github.com/cmu-sei/ghosts

## IT Admins

- Manage the infrastructure
- Subnet to access servers
- Remote Desktop Services (RDS)
- ManageEngine Desktop Central https://archives.manageengine.com/desktop-central/

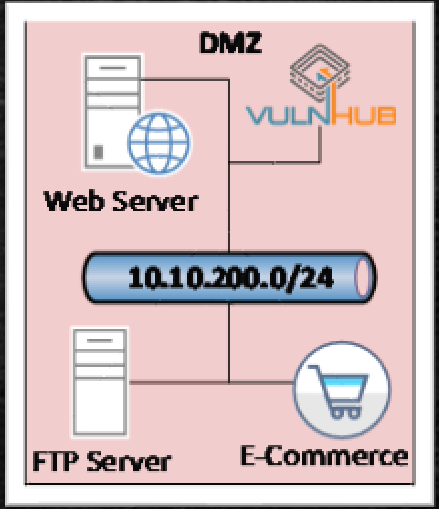
# Security Implication

- Jump box
- Dual-homed or firewall rules
- Which one makes it harder/easier for an attacker?
- Hardening



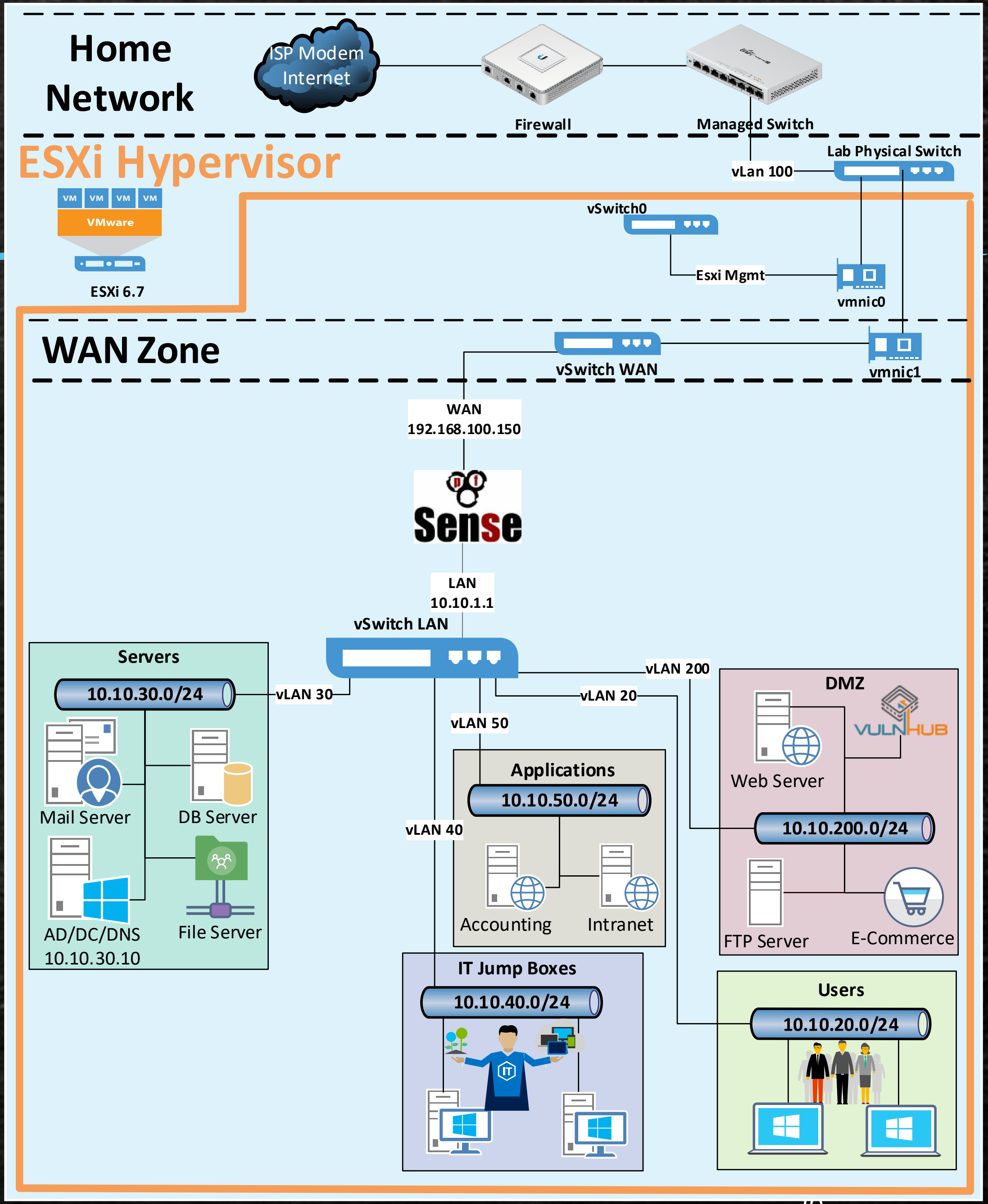
# DMZ

- Emulating Internet Presence
- Vulnerable WordPress as Our Enterprise Main Website.
  - WPScan Vulnerability Database: https://wpvulndb.com/
- OWASP Juice Shop
  - https://github.com/bkimminich/juice-shop
- FTP Servers to exchange files with our customers
  - Anonymous Authentication, Brute force, Exploit.
- Citrix Netscaler or F5 Big IP
  - 30 days tried from after signing up Vendor Site
- VulnHub VMs
  - https://www.vulnhub.com/



# Securing DMZ

- Keep internal network safe.
- Another firewall?
- Creds to manage.
- Where does a Database live?



# Optional

## Air Gapped

- Highly Vulnerable
- How would you isolate?
- How would you protect/detect

## VPN

- pfSense Built-in
- Remote Workforce
- Share environment with other researchers

## Guest WiFi

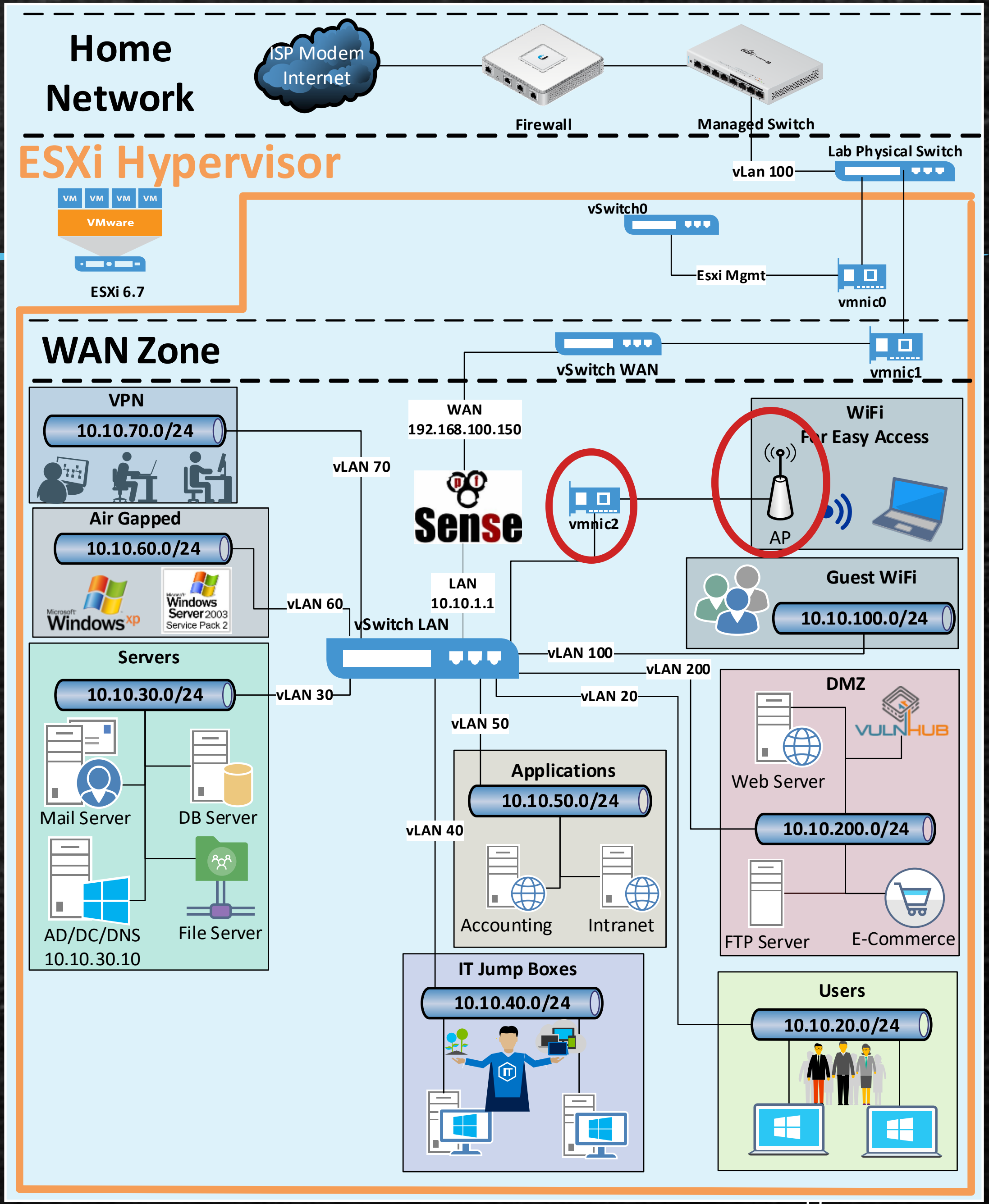
- Would your Enterprise have visitors?
- pfSense Captive Portal

## Home WiFi

- Connect directly to the Enterprise network on LAN
- Requires another physical NIC

# Wifi

- Router as AP
- Required another physical NIC
- Test Wifi Attacks

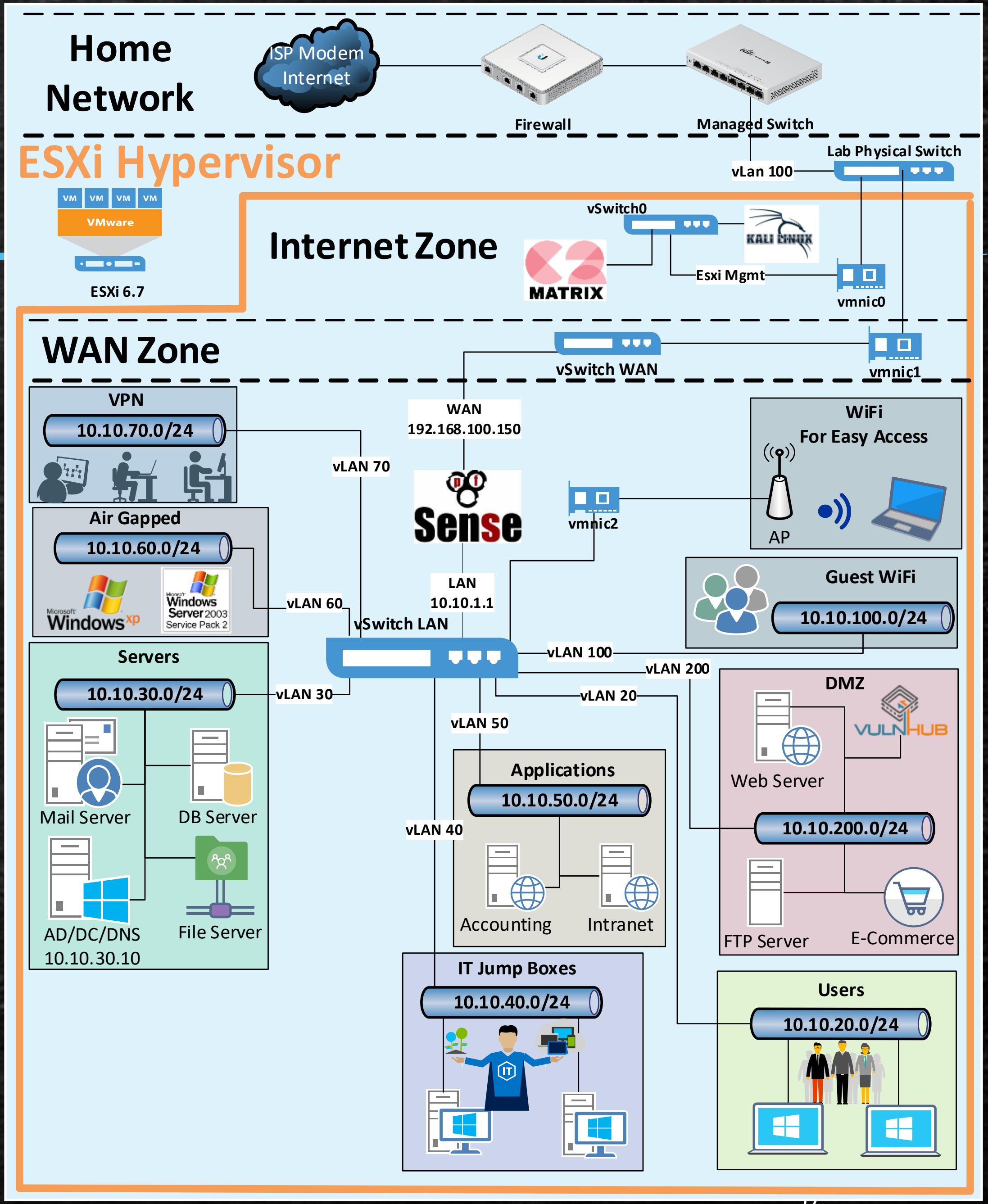


# Internet & Attacker Zone

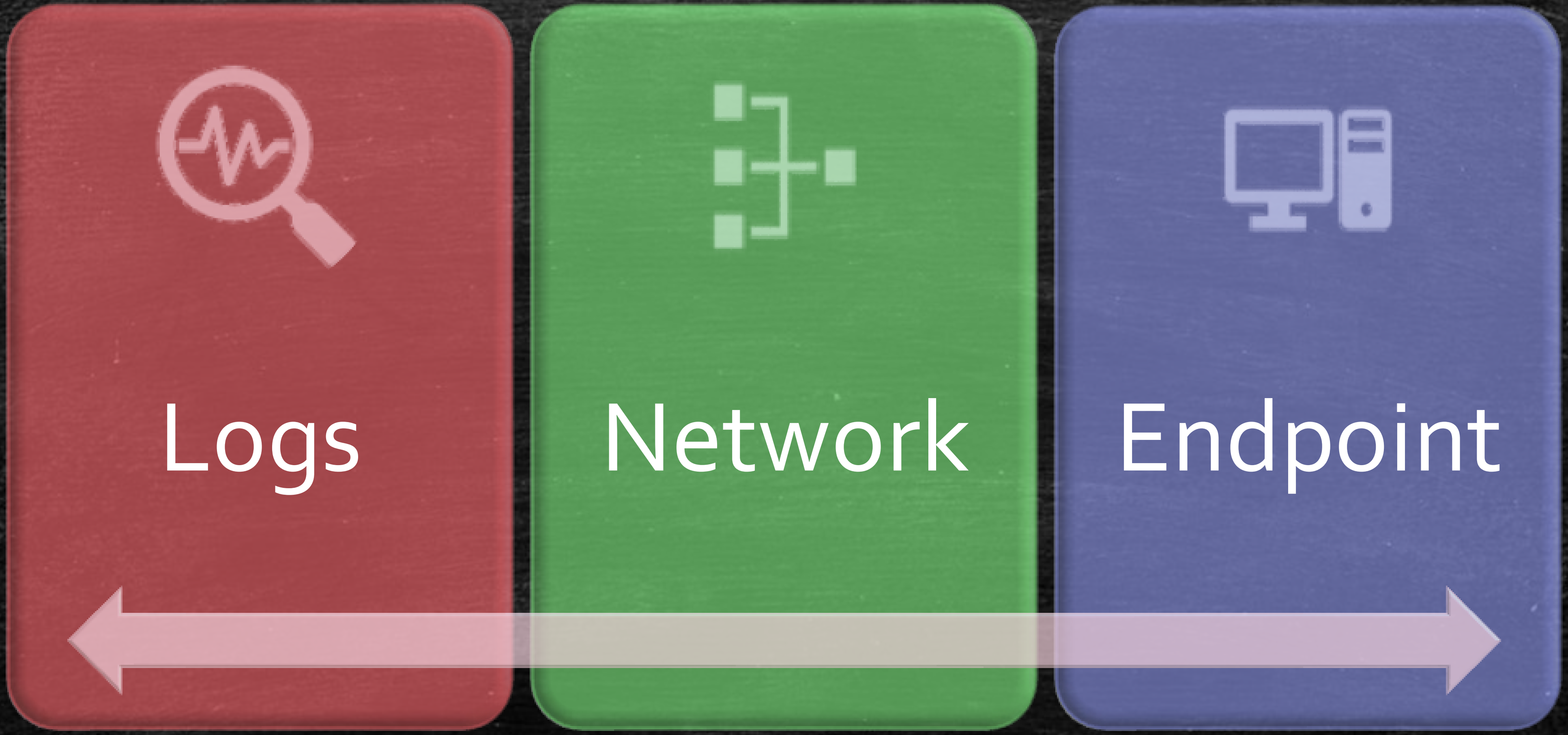
- Kali Linux
  - https://www.kali.org/
- Commando VM
  - https://github.com/fireeye/commando-vm
- Slingshot C2 Matrix Edition
  - https://www.sans.org/blog/introducing-slingshot-c2-matrix-edition/

# Red Team

- Compromise DMZ
- Move Laterally
- Start from the users network?



# Enterprise Visibility Simplified



Logs

Network

Endpoint

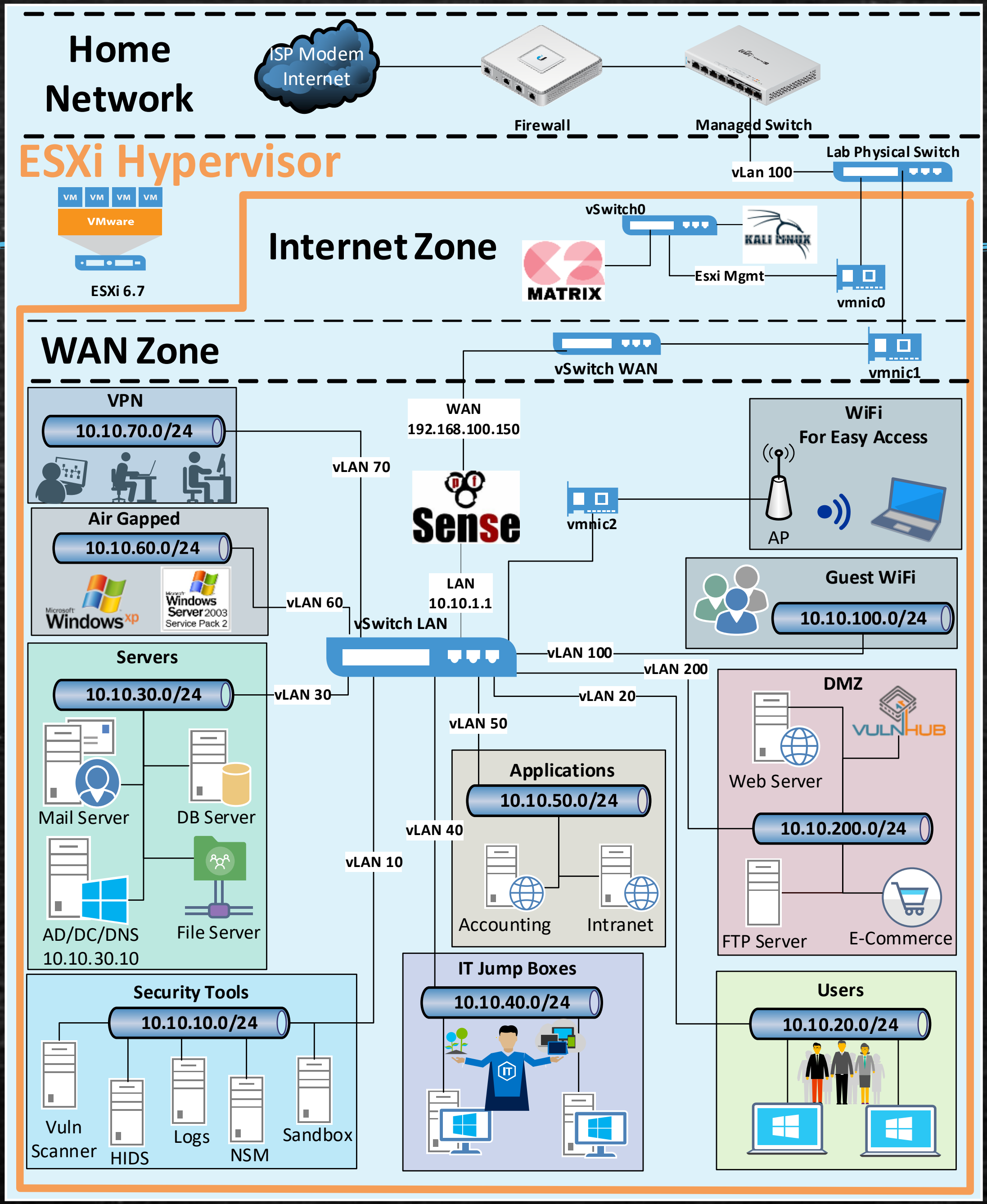
# Blue Team

- NSM/NIDS
  - Promiscuous VLAN
  - Zeek: https://zeek.org/
  - Suricata: https://suricata-ids.org/
  - SecurityOnion: https://securityonion.net/
  - Moloch: https://molo.ch/
- HIDS/Endpoint Logs
  - Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
  - Kolide Fleet/Osquery: https://www.kolide.com/fleet/
  - Wazuh/OSSEC: https://wazuh.com/
- SIEM
  - Open Source
    - Elastic Stack: https://www.elastic.co/elastic-stack
    - HELK: https://github.com/Cyb3rWardog/HELK
    - SOF-ELK: https://github.com/philhagen/sof-elk
    - GrayLog Open Source: https://www.graylog.org/
  - Free Commercial
    - Splunk ( Free Up to 500 mb a day) https://www.splunk.com/

# Additional Security Tools

- Vuln Scanner
  - OpenVAS: https://www.openvas.org/
  - Nessus Essentials (up to 16 IP addresses per scanner): https://www.tenable.com/products/nessus/nessus-essentials
- Sandbox
  - Cuckoo's Sandbox: https://cuckoosandbox.org/
- Honeypots
  - T-Pot: https://github.com/dtag-dev-sec/tpotce
  - Thinkst Canary: https://canary.tools/

# Scenario


Home Network
ISP Modem Internet
Firewall
Managed Switch
ESXi Hypervisor
VM VM VM VM
VMware
ESXi 6.7
vLan 100
Lab Physical Switch
Internet Zone
vSwitch0
KALI LINUX
MATRIX
Esxi Mgmt
vmnic0
WAN Zone
vSwitch WAN
vmnic1
VPN
10.10.70.0/24
vLAN 70
WAN
192.168.100.150
Sense
vmnic2
WiFi
For Easy Access
AP
Air Gapped
10.10.60.0/24
Windows xp
Windows Server 2003 Service Pack 2
vLAN 60
LAN
10.10.1.1
vSwitch LAN
Guest WiFi
10.10.100.0/24
vLAN 100
vLAN 200
Servers
10.10.30.0/24
vLAN 30
vLAN 20
DMZ
VULNHUB
vLAN 50
Mail Server
DB Server
Applications
10.10.50.0/24
Web Server
vLAN 40
10.10.200.0/24
vLAN 10
AD/DC/DNS
10.10.30.10
File Server
Accounting
Intranet
FTP Server
E-Commerce
Security Tools
10.10.10.0/24
IT Jump Boxes
10.10.40.0/24
Users
10.10.20.0/24
Vuln Scanner
HIDS
Logs
NSM
Sandbox

Thank You!

Questions? @1337bash