

Documentación de Infraestructura

1. Topología de red:

La infraestructura está montada en un servidor físico con **Proxmox VE** y simulada parcialmente en **GNS3**.

La red se divide en dos entornos:

- Red insegura:

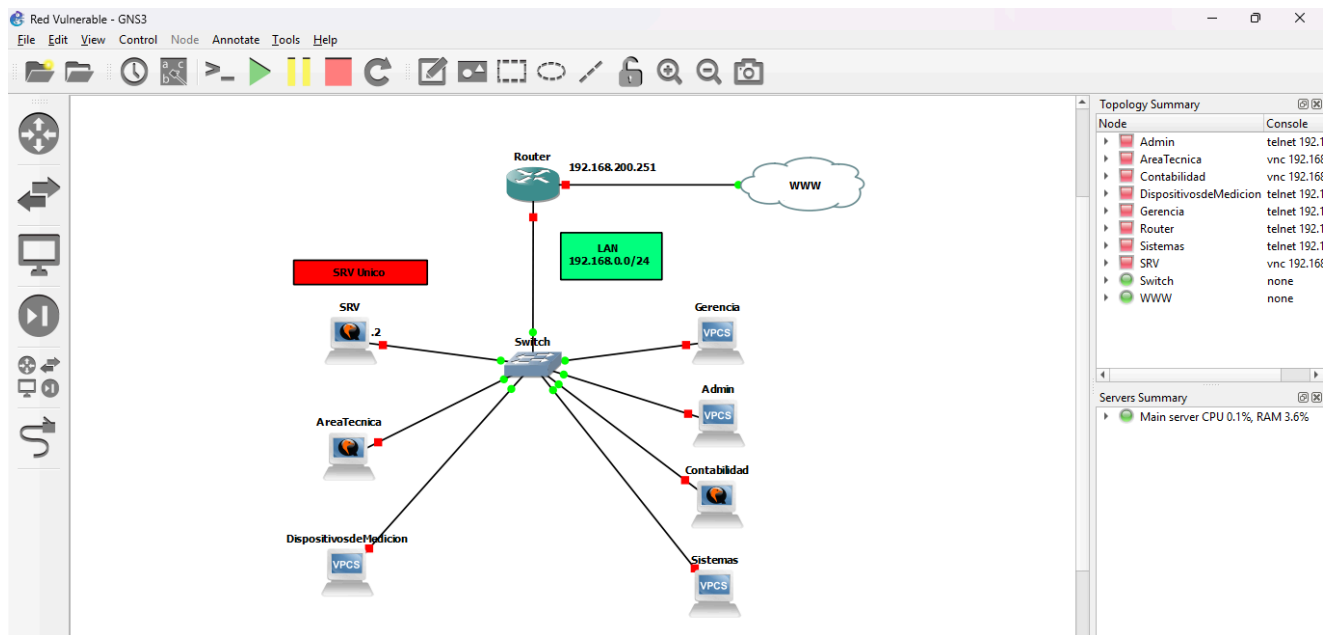
Expone servicios sin protección para pruebas de ataque.

Tabla de IPS (red insegura):

Heliópolis Red inicial.	
ISP	192.168.200.0/24
Router WAN	192.168.200.251
Router LAN	192.168.0.0/24
LAN	192.168.0.0/24 DHCP
SRV	192.168.0.2/24

Proxmox, GNS3, MikroTik, servidor en Ubuntu Server GUI ,Kali Linux.

El entorno virtualizado se implementó con un equipo físico con un Hipervisor llamado Proxmox en el cual se instaló GNS3 Server y a su vez el cliente se instaló en otra máquina la cual usamos para administrar la topología.



Topología insegura

- **Herramientas utilizadas:**
Nmap, Zenmap, Metasploit, Burp Suite, Nessus Essentials, Wireshark.
- **Topología y segmentación:**
Una única red, router, servidor unificado sin ninguna segmentación.
- **Configuración y evidencias:**

Configuración Proxmox:

- Red segura:

segmentada con VLANs, DMZ y firewalls.

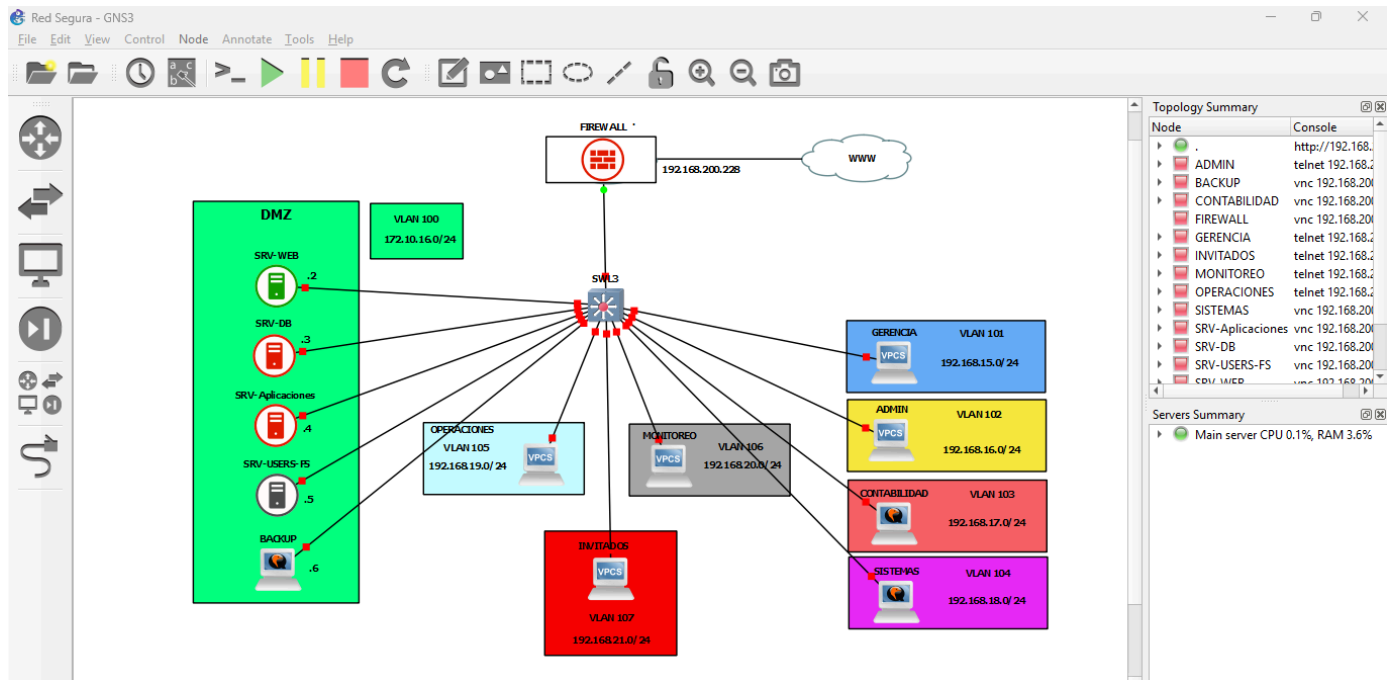
- **Tabla de IPS (red segura):**

Heliopolis Red Final.	
WAN	192.168.200.0/24
Firewall WAN	192.168.200.228
Firewall LAN	192.168.50.0/24
VLAN 100 DMZ	172.10.16.0/24
VLAN 101 Gerencia	192.168.15.0/24
VLAN 102 Admin	192.168.16.0/24
VLAN 103 Contabilidad	192.168.17.0/24
VLAN 104 Sistemas	192.168.18.0/24
VLAN 105 Operaciones	192.168.19.0/24
VLAN 106 Monitoreo	192.168.20.0/24
VLAN 107 Invitados	192.168.21.0/24

- **Configuración:**

Proxmox, GNS3, Pfsense, servidor en Ubuntu Server no GUI , Windows server, Windows 10, Kali Linux.

Para la implementación se usó el mismo servidor GNS3 para administrar las máquinas virtuales.



- **Herramientas utilizadas:**

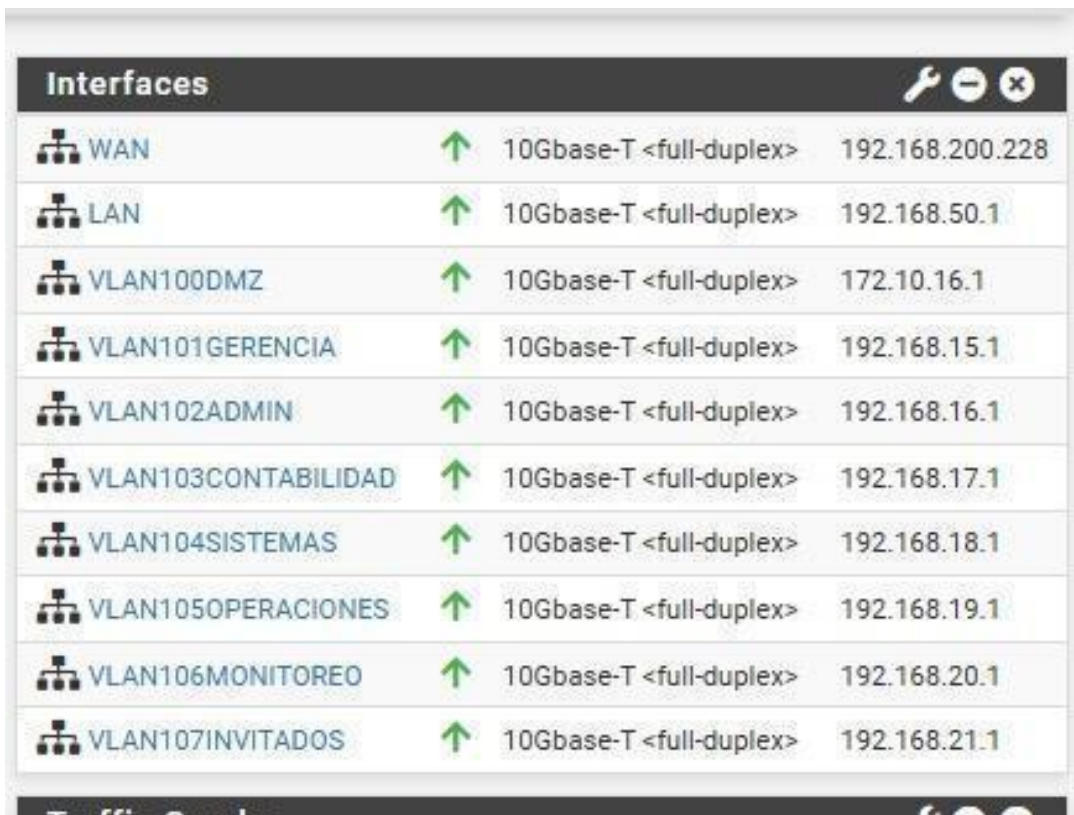
Nmap, Zenmap, Metasploit, Burp Suite, Nessus Essentials, Wireshark.

- **Topología y segmentación:**

Firewalls, Switch capa 3, Vlans, servidores independientes.

- **Configuración y evidencias:**

Configuración de VLANS en Firewall (pfSense):

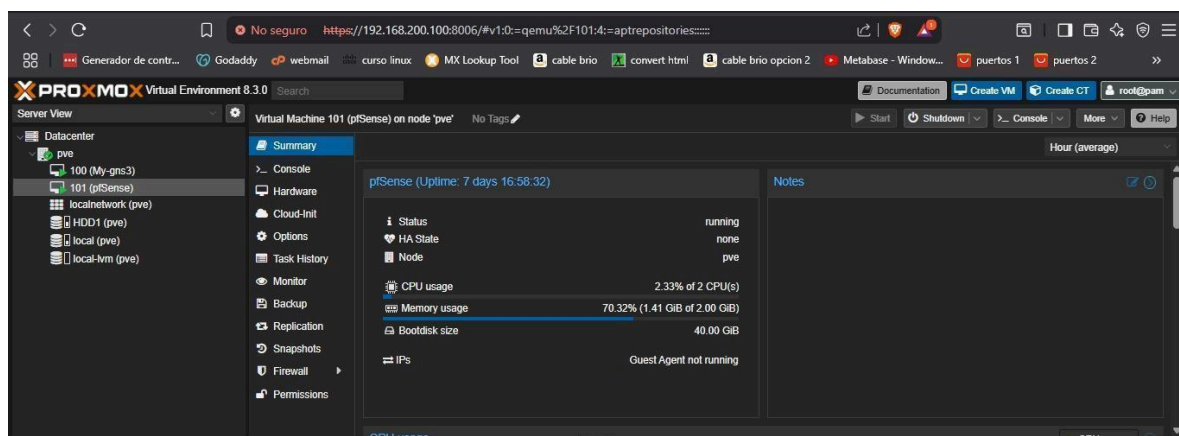


Interfaces			
WAN	↑	10Gbase-T <full-duplex>	192.168.200.228
LAN	↑	10Gbase-T <full-duplex>	192.168.50.1
VLAN100DMZ	↑	10Gbase-T <full-duplex>	172.10.16.1
VLAN101GERENCIA	↑	10Gbase-T <full-duplex>	192.168.15.1
VLAN102ADMIN	↑	10Gbase-T <full-duplex>	192.168.16.1
VLAN103CONTABILIDAD	↑	10Gbase-T <full-duplex>	192.168.17.1
VLAN104SISTEMAS	↑	10Gbase-T <full-duplex>	192.168.18.1
VLAN105OPERACIONES	↑	10Gbase-T <full-duplex>	192.168.19.1
VLAN106MONITOREO	↑	10Gbase-T <full-duplex>	192.168.20.1
VLAN107INVITADOS	↑	10Gbase-T <full-duplex>	192.168.21.1

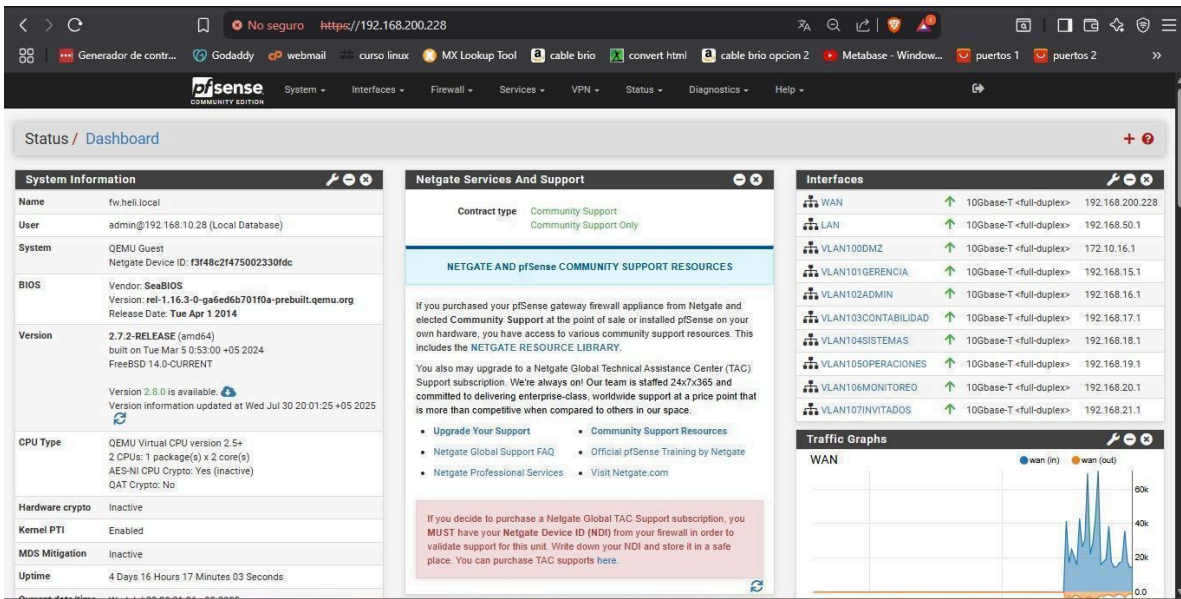
VLANs Firewall

En la anterior imagen se puede observar todas las interfaces de las VLAN ya configuradas con sus respectivas IPS.

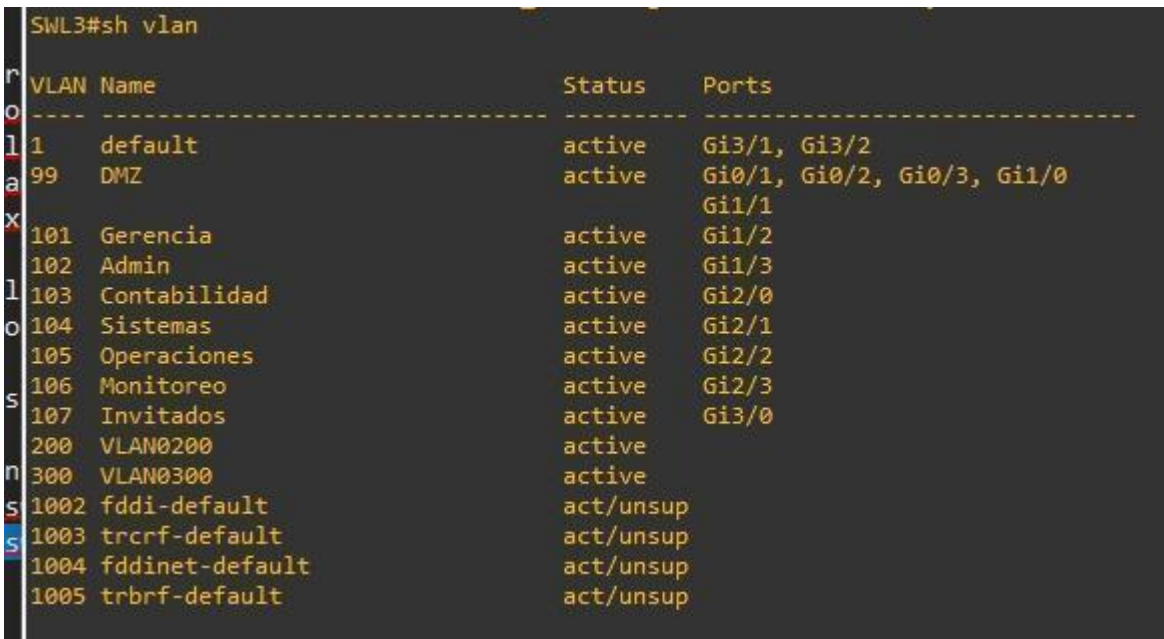
Configuración Proxmox:



Configuración Pfsense:



VLANS SWITCH:



En la anterior imagen podemos observar las interfaces asignadas a su respectiva VLAN.

5. Diseño de la Red Corporativa

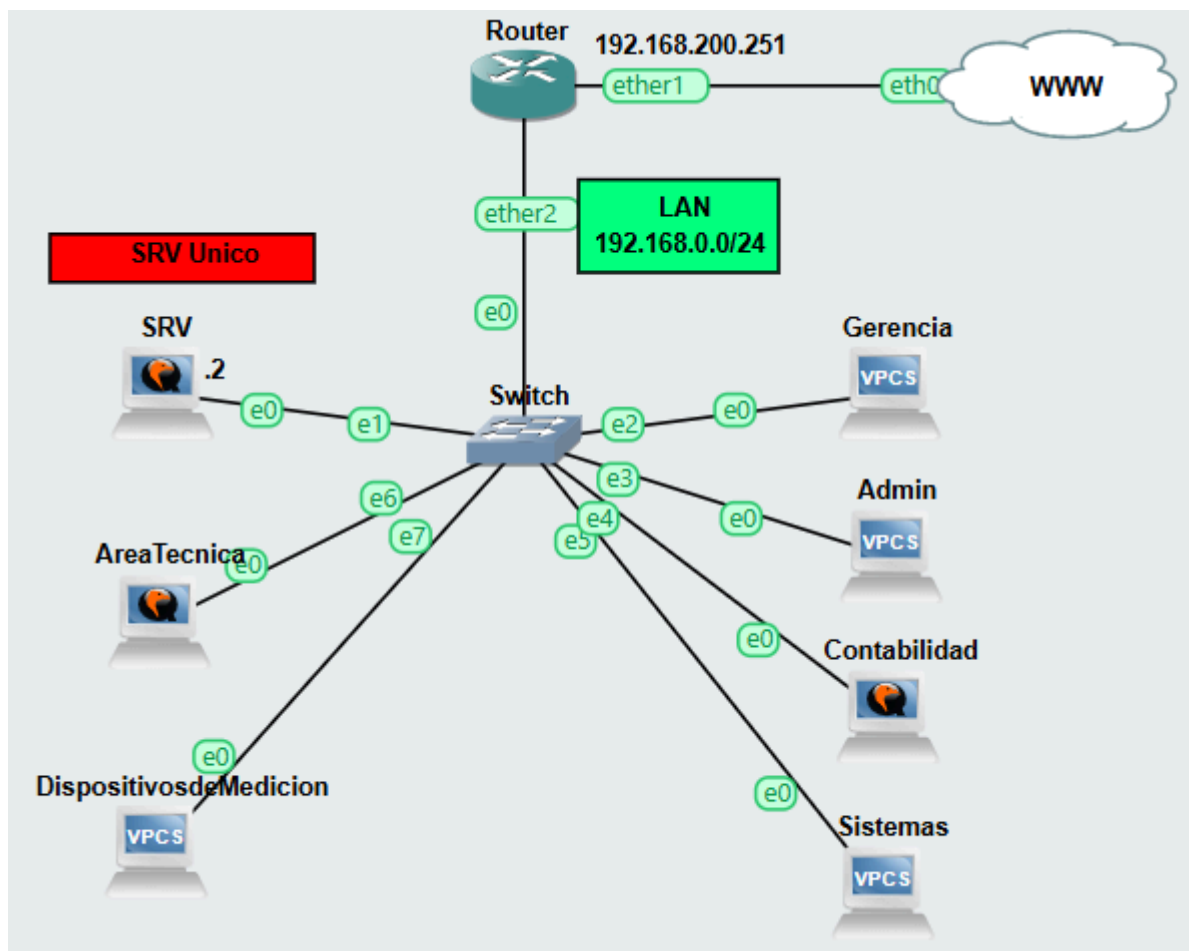
- Estructura simulada:

La empresa está dividida en 8 segmentos, los cuales son:

DMZ, Gerencia, administración, contabilidad, sistemas, operaciones, monitoreo, invitados.

- Topologías:

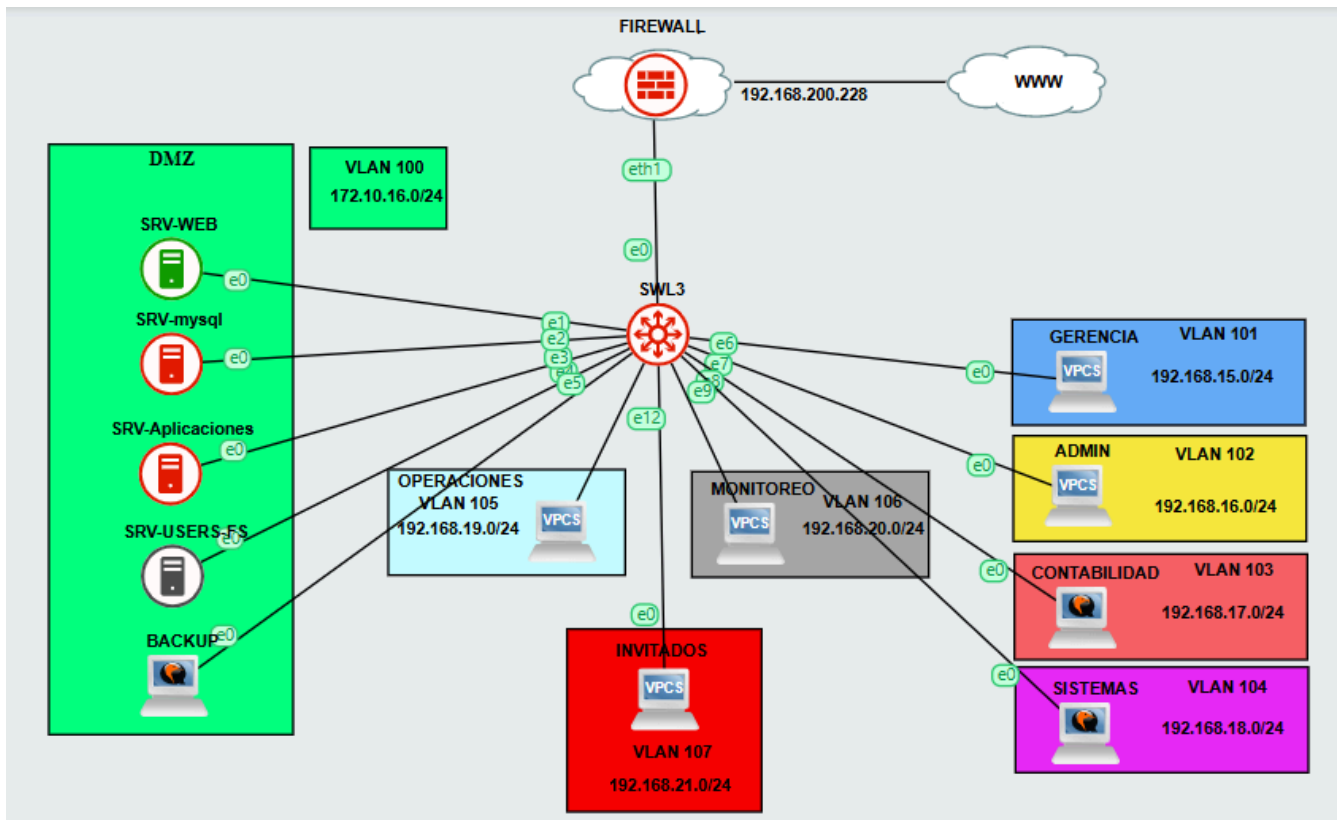
Red inicial:



Red insegura.

Como se puede ver en la topología inicial de la empresa, no había segmentación, tenían una red LAN general en la cual se le tenía una IP fija asignada únicamente al servidor, por lo tanto, con el hecho de que vulneren cualquier dispositivo tendrían fácil acceso a los demás sistemas de la red.

Red Final:



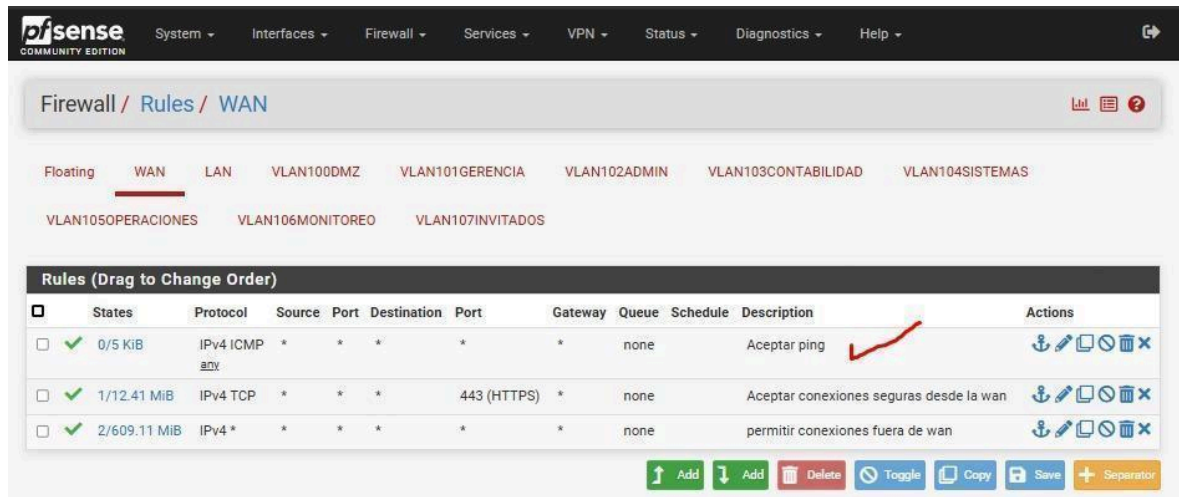
Red segura.

En esta red se puede observar que ya todo está segmentado por procesos con la ayuda de VLANs y se crea una parte (DMZ) donde se divide el único servidor que se tenía en 4 servidores diferentes para no tener todo centralizado y mitigar riesgos.

- Seguridad lógica:

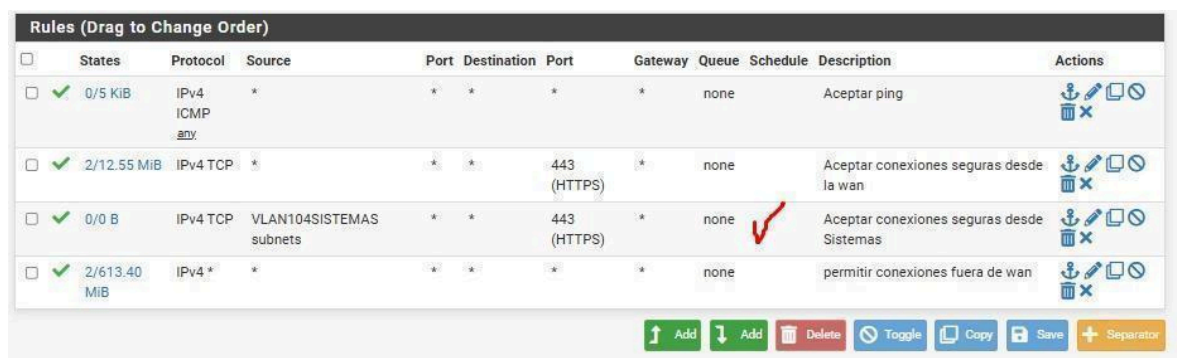
Políticas de ACLs (Access Control List), segmentación, roles y jerarquización.

- ❖ Que toda la red tenga comunicación a ICMP **Internet Control Message Protocol** (Protocolo de Mensajes de Control de Internet) “PING”.



Regla aceptar ping Pfsense.

- ❖ Que sólo la VLAN del área de SISTEMAS tenga acceso al puerto 443 (servicio HTTPS Hypertext Transfer Protocol Secure) del servidor web que está en el DMZ.















Regla acceso al puerto 443 (Area sistemas).








- ❖ Que todas las VLANS tengan acceso a internet ya que por defecto no tienen acceso a internet.

Firewall / Rules / VLAN104SISTEMAS

Floating WAN LAN VLAN100DMZ VLAN101GERENCIA VLAN102ADMIN VLAN103CONTABILIDAD **VLAN104SISTEMAS** VLAN105OPERACIONES VLAN106MONITOREO VLAN107INVITADOS

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/1.95 GiB	IPv4 *	VLAN104SISTEMAS subnets	*	*	*	*	none	✓	Permitir @ vlan 104 sistemas	   
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	none		aceptar ping	   
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	*	none		permitir trafico red fisica	   

















 Add
  Add
  Delete
  Toggle
  Copy
  Save
  Separator








Internet por defecto.

- ❖ Que los puertos 22 (protocolo SSH Secure Shell) de los DMZ únicamente respondan a la VLAN 104 de sistemas.

Floating WAN LAN **VLAN100DMZ** VLAN101GERENCIA VLAN102ADMIN VLAN103CONTABILIDAD VLAN104SISTEMAS VLAN105OPERACIONES VLAN106MONITOREO VLAN107INVITADOS

Rules (Drag to Change Order)













<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/14 KiB	IPv4 ICMP any	*	*	*	*	*	none		Aceptar Ping	   
<input type="checkbox"/>	✓ 0/3.82 GiB	IPv4 *	VLAN100DMZ subnets	*	*	*	*	none		Permitir @ vlan 100 DMZ	   
<input type="checkbox"/>	✓ 0/152 B	IPv4 *	*	*	*	*	*	none		Permitir desde fuera de la wan	   
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	VLAN104SISTEMAS subnets	*	VLAN100DMZ subnets	22 (SSH)	*	none	✓	Permitir SSH a Sistemas	   








 Add
  Add
  Delete
  Toggle
  Copy
  Save
  Separator

Permitir ssh a DMZ desde sistemas.

- ❖ Que el servidor de base datos únicamente responda al servidor web, de aplicaciones y a Sistemas.
















Floating	WAN	LAN	VLAN100DMZ	VLAN101GERENCIA	VLAN102ADMIN	VLAN103CONTABILIDAD	VLAN104SISTEMAS	VLAN105OPERACIONES	VLAN106MONITOREO	VLAN107INVITADOS
----------	-----	-----	------------	-----------------	--------------	---------------------	-----------------	--------------------	------------------	------------------








Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/14 KiB	IPv4 ICMP	*	*	*	*	none		Aceptar Ping	  
<input type="checkbox"/>	✓	0/3.82 GiB	IPv4 *	VLAN100DMZ subnets	*	*	*	none		Permitir @ vlan 100 DMZ	  
<input type="checkbox"/>	✓	0/152 B	IPv4 *	*	*	*	*	none		Permitir desde fuera de la wan	  
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	VLAN104SISTEMAS subnets	*	172.10.16.3	3306	*		Aceptar puerto DB a Sistemas	  

 Add
  Add
  Delete
  Toggle
  Copy
  Save
  Separator

Aceptar puerto DB a sistemas.

Floating	WAN	LAN	VLAN100DMZ	VLAN101GERENCIA	VLAN102ADMIN	VLAN103CONTABILIDAD	VLAN104SISTEMAS	VLAN105OPERACIONES	VLAN106MONITOREO	VLAN107INVITADOS
----------	-----	-----	------------	-----------------	--------------	---------------------	-----------------	--------------------	------------------	------------------

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/14 KiB	IPv4 ICMP	*	*	*	*	none		Aceptar Ping	  
<input type="checkbox"/>	✓	0/3.82 GiB	IPv4 *	VLAN100DMZ subnets	*	*	*	none		Permitir @ vlan 100 DMZ	  
<input type="checkbox"/>	✓	0/152 B	IPv4 *	*	*	*	*	none		Permitir desde fuera de la wan	  
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	VLAN104SISTEMAS subnets	*	172.10.16.3	3306	*		Aceptar puerto DB a Sistemas	  
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.10.16.2	*	172.10.16.3	3306	*		Permitir DB 3306 De SRV Web	  

 Add
  Add
  Delete
  Toggle
  Copy
  Save
  Separator

Permitir 3306 de servidor web.

Procedimiento de despliegue:

1. Preparar Proxmox e instalar todas las VMs necesarias.
2. Importar topología GNS3 y conectar con el bridge de Proxmox.
3. Configurar MikroTik como firewall de la red insegura.
4. Configurar pfSense como firewall de la red segura:
 - Crear VLANs.
 - Asignar interfaces y reglas.
5. Asignar IPs fijas a cada VM según su VLAN.
6. Levantar servicios (web, backend, base de datos, logs, backups).
7. Probar conectividad entre VLANs y con Internet.
8. Ejecutar pruebas de seguridad con Nessus y Wireshark.