GVTech Solutions

Júlia Carlini Dornelas 2024145810

Leiria, *Novembro* de *2025*

Resumo

Este projeto visa a conceção e implementação de uma infraestrutura virtualizada completa, segura e resiliente, utilizando hipervisores de tipo 1 e tipo 2 . A solução inclui a configuração de redes segmentadas (LAN e DMZ), armazenamento partilhado via TrueNAS, políticas de firewall com OPNsense, e mecanismos de backup e alta disponibilidade. O ambiente simula uma infraestrutura empresarial real, permitindo a validação de conceitos de virtualização, segurança e gestão de redes.

Palavras-chave: (Virtualização, Segurança, Redes, Hipervisores, Armazenamento, Backup)

1. Introdução

Este projeto tem como principal objetivo a **implementação de uma infraestrutura virtualizada completa**, capaz de demonstrar as capacidades, a segurança e a robustez dos sistemas de virtualização modernos. Através deste projeto, pretende-se criar um **ambiente de testes empresarial simulado**, que permita explorar funcionalidades avançadas de virtualização, gestão de redes, armazenamento e políticas de segurança.

Para alcançar este objetivo, o projeto envolve:

- **Criação de um ambiente virtualizado híbrido**, utilizando hipervisores de tipo 1 (bare-metal) e tipo 2 (hosted), permitindo a execução de múltiplas máquinas virtuais (VMs) com diferentes sistemas operativos (Windows, Linux e outros). Esta diversidade possibilita avaliar a interoperabilidade e a gestão de recursos entre diferentes plataformas.
- **Implementação de um sistema de armazenamento partilhado**, garantindo que as VMs possam aceder de forma centralizada a dados críticos, promovendo redundância e integridade da informação.
- **Desenvolvimento de mecanismos de backup e recuperação**, assegurando que os dados e configurações das VMs possam ser restaurados rapidamente em caso de falha, simulando boas práticas de continuidade de negócio.
- **Configuração de uma topologia de rede segura e funcional**, com segmentação adequada, políticas de firewall, roteamento interno e acesso controlado à Internet, de modo a simular as necessidades de conectividade de uma empresa real.
- **Demonstração prática da comunicação entre VMs e hosts**, validando a interconexão, o desempenho, a disponibilidade e a resiliência da infraestrutura implementada.

Os resultados esperados incluem:

1. Uma **topologia de rede completa**, documentada e funcional, que assegure comunicação eficiente e segura entre todos os elementos da infraestrutura.
2. A configuração de hipervisores e VMs de diferentes sistemas operativos, permitindo testar a compatibilidade, gestão de recursos e administração centralizada.
3. A implementação de **armazenamento partilhado e políticas de backup**, promovendo alta disponibilidade, redundância de dados e segurança da informação.

4. Uma **demonstração operacional** do ambiente, evidenciando a interligação entre hosts, VMs e sistemas de armazenamento, bem como a robustez da solução perante falhas simuladas.

Este projeto, assim, pretende não apenas **reproduzir as condições de um ambiente empresarial real**, mas também servir como uma ferramenta de análise, experimentação e aprendizagem sobre **virtualização, gestão de recursos e segurança em sistemas informáticos**.

2. Planeamento

Esta secção apresenta o planeamento técnico do projeto, incluindo a caracterização da entidade fictícia, a definição da topologia da rede e a infraestrutura de virtualização a implementar. O objetivo é garantir uma estrutura organizada, escalável e adequada às necessidades académicas da unidade curricular.

2.1. Características da entidade

Número de utilizadores (hosts):

A entidade fictícia opera numa pequena infraestrutura composta por:

- 2 hosts físicos, cada um com funções de hipervisor:
  - PC1 – Hypervisor Tipo 1 (VMware ESXi)
  - PC2 – Hypervisor Tipo 2 (Windows + VMware)

Organização da Rede:

A rede encontra-se estruturada de forma simples e funcional:

Rede LAN (10.10.10.0/24)
Segmento principal onde se encontram:

- Os dois hosts físicos
- Máquinas virtuais internas
- Serviço de armazenamento (TrueNAS)
- Gestão centralizada das VMs

Rede DMZ (20.20.20.0/24)
Criada através do OPNsense para isolamento de serviços futuros que possam necessitar de acesso externo.
Atualmente não aloja o TrueNAS, garantindo boas práticas de segurança e alinhamento com os requisitos.

Serviços de Rede:

Os principais serviços previstos no âmbito deste projeto são:

- OPNsense – Firewall e router interno
- TrueNAS – Serviço de armazenamento para partilhas e backups
- Máquinas virtuais de teste (Windows/Linux) para apoio à gestão e ensaios laboratoriais

Outros:

- Acesso à Internet efetuado através de NAT no router/OPNsense
- A DMZ está preparada para futuras expansões (ex.: servidor web, FTP, etc.)

2.2. Diagrama lógico da rede

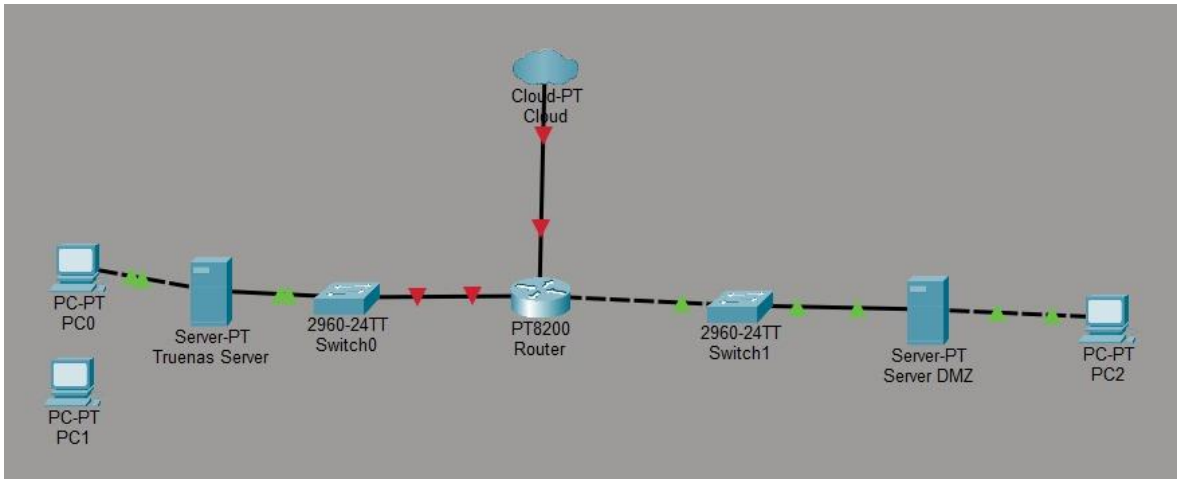

Figura 1 – Diagrama Lógico da Rede

Descrição

O diagrama lógico representa a organização conceptual da rede, segmentando os diferentes domínios operacionais (LAN e DMZ) e a forma como estes comunicam através da firewall OPNsense.

A LAN funciona como o núcleo interno onde se encontram os hosts, VMs e serviços essenciais. A DMZ encontra-se separada por firewall e disponível para alojar serviços expostos ao exterior, embora nesta fase não esteja a ser utilizada.

Endereçamento IP

Rede	**Máquinas**	**IP**
LAN: 10.10.10.0/24	Gateway: (OPNsense LAN)	10.10.10.1
	TrueNAS:	10.10.10.x
	Hosts físicos:	10.10.10.x
	VMs internas:	10.10.10.x
DMZ: 20.20.20.0/24	Gateway: (OPNsense DMZ)	20.20.20.1

Tabela 1 - Endereçamento IP

2.3. Diagrama físico da rede

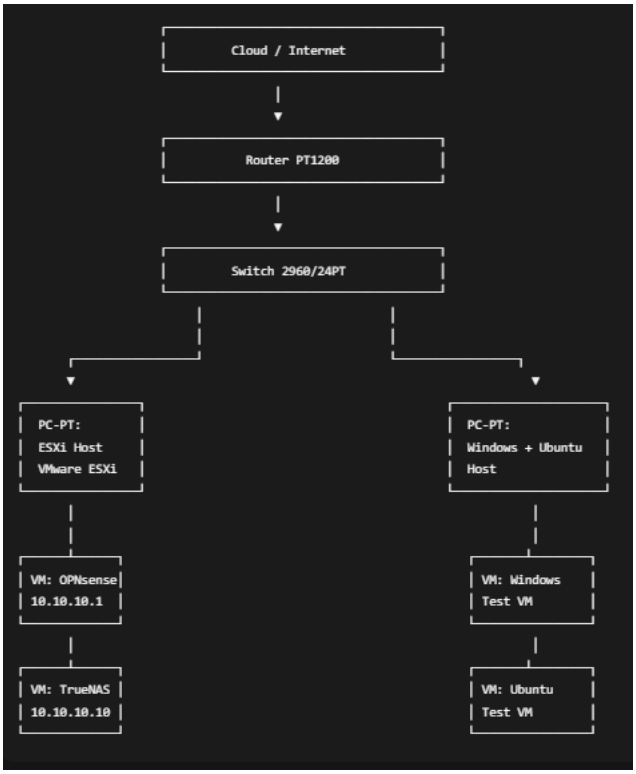

Imagem 2 – Diagrama Físico da Rede

Descrição

O diagrama físico apresenta as ligações reais entre os dois hosts e o router, demonstrando como a infraestrutura está concentrada:

Todos os hosts estão ligados fisicamente ao router/switch doméstico, recebendo acesso à Internet e comunicação interna.

Outros

- Cada host utiliza placas de rede físicas dedicadas para ligação à LAN
- A configuração física é mínima, privilegiando a virtualização para segmentação lógica

2.4. Diagrama de Rede Virtualizada

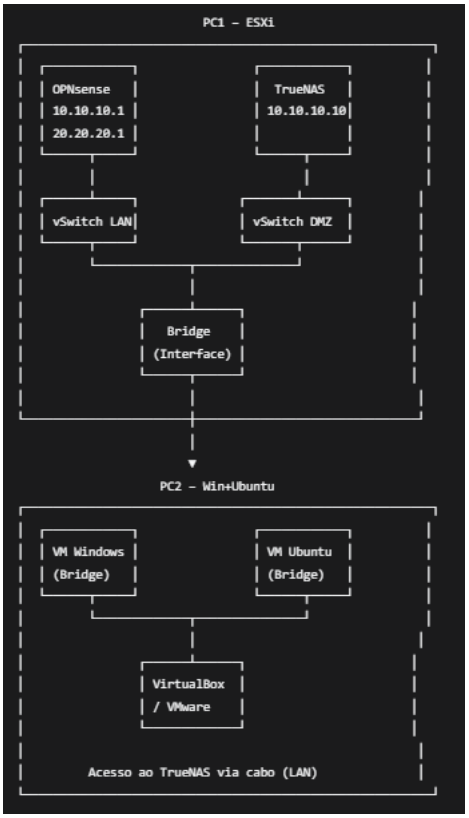

Imagem 3 – Diagrama de Rede Virtualizada

Descrição da Solução Virtual

O ambiente virtual está distribuído da seguinte forma:

PC1 – VMware ESXi (Hypervisor Tipo 1)

Máquinas virtuais:

- **OPNsense**
    - Interfaces virtuais:
        - LAN (10.10.10.1)
        - DMZ (20.20.20.1)

- **TrueNAS**
    - Interface virtual na LAN
    - Servidor interno de armazenamento

Switches Virtuais:

- vSwitch LAN
- vSwitch DMZ
- Bridge para interface física do PC1

PC2 – Hypervisor Tipo 2 (Windows + VirtualBox)

Máquinas virtuais:

- VMs Windows/Linux de teste
- Ligação NAT ou Bridge dependendo da necessidade
- Acesso ao TrueNAS pela LAN

PC3 – Hypervisor Tipo 2 (Ubuntu + VirtualBox)

Máquinas virtuais:

- VMs Linux para administração e testes
- Ligação Bridge à LAN
- Acesso ao TrueNAS para partilha ou backup.

Outros

- A rede virtualizada permite isolar VMs, criar redes internas e simular cenários reais
- Todos os ambientes virtuais comunicam via LAN e recorrem ao armazenamento do TrueNAS quando necessário

3. Pratica

4.1 Dimensionamento das VMs

Cada máquina virtual foi dimensionada de acordo com a sua função, tendo em conta as limitações de hardware disponíveis

VM	Função	CPU	RAM	Disco
OPNsense	Firewall	2 vCPU	2 GB	20 GB
TreNAS	Storage	4 vCPU	8 GB	100 GB
VM Linux	Testes	2 vCPU	2 GB	30 GB
VM Windows	Testes	2 vCPU	4 GB	50 GB

4.2 Ordem de ligar/Desligar das VMs

Arranque:

1. Hosts físicos
2. ESXi / VirtualBox
3. OPNsense
4. TrueNAS
5. VMs interna.

Encerramento: ordem inversa.

4.3 Implementação por Host

PC1 – ESXi

- Hypervisor tipo 1
- Aloja OPNsense e TrueNAS
- Switches virtuais LAN e DMZ

PC2 – Windows + Ubuntu + VirtualBox

- VMs de teste
- Rede em Bridge / NAT
- Vms
- Acesso ao storage

4.4 Hardware Físico

O ambiente foi implementado com recursos limitados, o que condicionou algumas funcionalidades avançadas.

Exemplo:

CPU: Intel i5 / Ryzen 5

RAM: 16 GB

Disco: 500 GB

Limitações: impossibilidade de HA real

4.5 Serviços implementados

Serviço	VM	IP	Função
OPNsense	VM	10.10.10.1	Firewall / Router
TrueNAS	VM	10.10.10.10	Storage
Linux VM	VM	DHCP	Testes

4. Conclusões

O **planeamento apresentado** estabelece uma base sólida para a implementação de um ambiente virtualizado **robusto, seguro e eficiente**, permitindo que todos os componentes da infraestrutura funcionem de forma integrada e coordenada.

Conclui-se que a **virtualização representa uma solução estratégica** para a otimização de recursos, possibilitando a centralização da gestão, a simplificação da manutenção e a melhoria do desempenho geral da infraestrutura. A utilização combinada de **hipervisores tipo 1 e tipo 2**, juntamente com **armazenamento partilhado, snapshots e mecanismos de backup**, proporciona **alta disponibilidade, redundância e segurança**.

A proposta assegura ainda **escalabilidade e flexibilidade**, permitindo expandir ou ajustar o ambiente virtual conforme as necessidades futuras. A **segmentação de redes, políticas de firewall e gestão de permissões diferenciadas** reforçam a proteção dos dados e serviços, simulando práticas reais de gestão de infraestruturas empresariais.

O **próximo passo** consistirá na implementação prática do ambiente, seguindo o planeamento definido, mas com **adaptação aos recursos disponíveis** e monitorização constante da infraestrutura. Esta fase permitirá validar a comunicação entre máquinas virtuais, a eficácia das políticas de segurança, a redundância e a performance do sistema, garantindo a consolidação dos conhecimentos teóricos em contexto aplicado.