# Documento Detalhado de Funcionalidades e Processos

## Sumário



---

## PC1 – NAS (TrueNAS SCALE)

### 1.1. Função e Objetivos

O PC1 tem a função de armazenar e gerenciar os dados centralmente usando o sistema TrueNAS SCALE, que utiliza o ZFS para garantir integridade e oferecer funcionalidades como snapshots e compartilhamento via SMB/NFS.

### 1.2. Possibilidades de Implementação

Você pode instalar o TrueNAS SCALE diretamente na máquina física ou em uma máquina virtual (usando VirtualBox, VMware ou similar). Alternativamente, em uma configuração dual boot, o mesmo hardware pode ser usado para rodar o TrueNAS SCALE ou outro SO conforme necessidade (o grupo poderá testar a funcionalidade em ambiente real ou virtual).

### 1.3. Passo a Passo para Execução

#### Passo 1: Preparação do Ambiente

- **Verificação de Hardware:** Certifique-se de que o HD, memória e processador estão operacionais.
- **Rede:** Conecte o PC1 (físico ou VM) à rede interna (switch ou via conexão virtual).

#### Passo 2: Instalação do TrueNAS SCALE

- **Em Hardware Físico ou Dual Boot:**
    - Baixe a ISO do TrueNAS SCALE no site oficial.
    - Grave a ISO em um pendrive (use Rufus ou Etcher) e configure a BIOS para boot.
    - Siga o assistente de instalação e defina um IP fixo.
- **Em Máquina Virtual:**

    - Crie uma nova VM no VirtualBox ou VMware.
    - Aloca recursos mínimos (ex.: 2GB de RAM, 1 CPU, e espaço em disco compatível) e monte a ISO do TrueNAS SCALE.
    - Siga o assistente de instalação dentro da VM.

**Passo 3: Configuração Inicial**

- Acesse a interface web do TrueNAS SCALE (usando o navegador do Notebook ou outro dispositivo) inserindo o IP fixo definido.
- Configure a conta de administrador e ajuste as configurações de rede, se necessário.

**Passo 4: Criação do Pool de Armazenamento e Datasets**

- Na seção “Storage”, crie um pool utilizando o(s) disco(s) disponíveis.
- Crie datasets para organizar os dados e configure políticas de snapshots.

**Passo 5: Configuração dos Serviços de Compartilhamento**

- Ative os serviços SMB e/ou NFS.
- Crie compartilhamentos definindo permissões (usuários e grupos) conforme o uso esperado.

**Passo 6: Testes e Validação**

- Conecte-se ao compartilhamento via outro dispositivo (por exemplo, o Notebook).
- Transfira arquivos e verifique a integridade e o funcionamento dos snapshots.

**Passo 7: Documentação e Monitoramento**

- Documente IP, pools, datasets, compartilhamentos e configurações de segurança.
- Use as ferramentas integradas do TrueNAS SCALE para monitorar o desempenho e configurar alertas.

---

# PC2 – Firewall/IDS (OPNsense com Interface Cabeada e Wireless)

## 2.1. Função e Objetivos

O PC2 atua como a barreira de segurança da rede, utilizando o OPNsense para filtrar o tráfego, realizar NAT e monitorar possíveis intrusões (com módulos como Suricata). Ele dispõe de interfaces cabeada e wireless – sendo esta última útil para conectar dispositivos sem fio ou como WAN secundária.

## 2.2. Possibilidades de Implementação

- **Instalação Física:** O OPNsense é instalado diretamente no hardware.

- **Máquina Virtual:** Pode ser executado como uma VM usando plataformas como VMware ESXi ou VirtualBox (se a performance permitir).
- **Dual Boot:** Se o PC2 tiver outra função em outros momentos, pode ser configurado para dual boot com OPNsense e outro sistema.

## 2.3. Passo a Passo para Execução

**Passo 1: Preparação do Ambiente**

- Verifique que o hardware (processador, memória, HD) e a placa de rede wireless estão funcionando.
- Conecte o PC2 à rede interna através da interface cabeada.

**Passo 2: Instalação do OPNsense**

- **Em Hardware Físico ou Dual Boot:**
  - Baixe a ISO do OPNsense e grave-a em um pendrive.
  - Configure a BIOS para boot e instale o sistema, definindo as interfaces (cabeada e wireless).
- **Em Máquina Virtual:**
  - Crie uma VM com recursos mínimos (por exemplo, 1–2 GB de RAM, 1 CPU).
  - Monte a ISO do OPNsense e proceda com a instalação, configurando as interfaces virtuais.

**Passo 3: Configuração Inicial do OPNsense**

- Acesse a interface web do OPNsense via IP configurado na interface LAN.
- Configure a conta de administrador.
- Defina as interfaces:
  - **WAN:** Conectada ao roteador ou modem (pode ser obtida via DHCP ou IP fixo).
  - **LAN:** Conectada ao switch, defina um IP fixo (ex.: 192.168.1.1).

**Passo 4: Configuração da Interface Wireless**

- Verifique se a placa wireless é reconhecida pelo OPNsense.
- Ative a interface wireless, configure o SSID e defina o tipo de segurança (WPA2/WPA3).
- Atribua um IP para a interface wireless (por exemplo, 192.168.2.1) se ela atuar em rede separada ou para failover.

**Passo 5: Configuração das Regras de Firewall e IDS/IPS**

- Crie regras de firewall que permitam o tráfego da rede interna e bloqueiem acessos indesejados.
- Configure o NAT para que os dispositivos internos acessem a Internet apenas pelo firewall.
- Ative e configure o módulo IDS/IPS (ex.: Suricata) e defina as assinaturas e alertas desejados.

**Passo 6: Testes e Validação**

- Realize testes de conectividade (ping, traceroute) usando tanto as interfaces cabeada quanto wireless.
- Utilize ferramentas (como Nmap) para simular ataques e verificar se as regras estão bloqueando acessos não autorizados.
- Confirme que os logs do IDS estão sendo gerados e podem ser acessados via SSH.

**Passo 7: Documentação e Manutenção**

- Registre todas as configurações (IPs, regras de firewall, configurações do IDS, detalhes da interface wireless).
- Defina procedimentos de atualização e verificação periódica das assinaturas do IDS.

---

# PC3 – Backup, Logs e Monitoramento (Debian sem GUI)

## 3.1. Função e Objetivos

O PC3 é responsável por centralizar os backups, armazenar logs e monitorar os sistemas. Ele utiliza uma instalação do Debian sem interface gráfica, focada em tarefas de linha de comando e automação via scripts, sendo o acesso e gerenciamento feitos principalmente via SSH.

## 3.2. Possibilidades de Implementação

- **Instalação Física:** Instalar Debian diretamente no hardware.
- **Máquina Virtual:** Configurar uma VM com Debian em plataformas como VirtualBox ou VMware.
- **Dual Boot:** Se necessário, configurar dual boot para alternar entre Debian e outro sistema operacional.
- **Comunicação via SSH:** Fundamental para acesso remoto e gerenciamento, especialmente para membros do grupo.

## 3.3. Passo a Passo para Execução

**Passo 1: Instalação do Debian (Sem GUI)**

- **Em Hardware ou Dual Boot:**
  - Baixe a imagem do Debian (versão estável) e instale o sistema sem interface gráfica.
  - Configure um IP fixo e habilite o SSH (instale o OpenSSH Server).
- **Em Máquina Virtual:**
  - Crie uma VM com recursos mínimos (1–2 GB de RAM, 1 CPU).
  - Instale o Debian sem GUI e habilite o SSH.

**Passo 2: Configuração da Centralização de Logs**

Instale o rsyslog (caso não esteja instalado):
sudo apt update
sudo apt install rsyslog

- 
- Edite a configuração do rsyslog para permitir a recepção de logs remotos (modifique `/etc/rsyslog.conf` ou crie um arquivo em `/etc/rsyslog.d/`).
- Configure um diretório (ex.: `/var/log/centralizados/`) para armazenar os logs.

Reinicie o rsyslog:
sudo systemctl restart rsyslog

- 

**Passo 3: Implementação dos Scripts de Backup**

Instale o rsync:
sudo apt install rsync

- 

Crie um script de backup (por exemplo, `/usr/local/bin/backup_script.sh`):
#!/bin/bash
# Script de backup do NAS (PC1) para o PC3
rsync -avz /caminho/do/compartilhamento/ /backup/destino/

- 

Dê permissão de execução:
sudo chmod +x /usr/local/bin/backup_script.sh

- 

Configure o cron para executar o script (use `crontab -e`):
0 2 * * * /usr/local/bin/backup_script.sh

- 

**Passo 4: Instalação e Configuração da Ferramenta de Monitoramento**

Instale um agente de monitoramento (ex.: Zabbix Agent):
sudo apt install zabbix-agent

- 
- Configure o arquivo `/etc/zabbix/zabbix_agentd.conf` para apontar para o servidor de monitoramento (pode ser o próprio PC3 ou um servidor dedicado).

Reinicie o agente:
sudo systemctl restart zabbix-agent

- 

**Passo 5: Comunicação via SSH**

- **Acesso Remoto:**
  - Verifique que o SSH está ativo e configure a autenticação (pode ser por senha ou por chaves públicas).
  - Instrua os membros do grupo a usar clientes SSH (como PuTTY ou OpenSSH no Linux/Mac) para se conectar ao PC3 utilizando seu IP fixo.
- **Configuração de Firewall (no PC2):**
  - Certifique-se de que o PC3 só tem acesso à Internet e à rede interna através do firewall (PC2).
  - Configure regras que permitam o acesso SSH apenas a partir de endereços autorizados.

**Passo 6: Testes e Validação**

- **Backup:** Execute o script manualmente e verifique a cópia dos dados.
- **Logs:** Confirme que os logs dos demais dispositivos estão sendo armazenados em `/var/log/centralizados/`.
- **Monitoramento:** Verifique a interface do servidor de monitoramento e os alertas.
- **SSH:** Realize conexões SSH para garantir que o acesso remoto esteja funcionando.

**Passo 7: Documentação e Procedimentos de Manutenção**

- Registre as configurações de rede, os caminhos dos scripts, as configurações do rsyslog e do agente de monitoramento.
- Crie um manual básico para que qualquer membro do grupo possa atualizar ou ajustar as configurações conforme necessário.

---

# 4. Considerações de Virtualização / Dual Boot e Comunicação via SSH

## 4.1. Utilizando Máquinas Virtuais ou Dual Boot

- **Máquina Virtual:**
  - Crie VMs em softwares como VirtualBox ou VMware para cada função (NAS, Firewall/IDS e Backup/Logs).
  - Aloca recursos mínimos (RAM, CPU, disco) conforme as especificações recomendadas.
  - Configure a rede virtual para simular a topologia real, utilizando adaptadores em modo "bridge" ou "host-only" para comunicação com as demais VMs e com a rede do grupo.
- **Dual Boot:**
  - Em máquinas que suportem dual boot, instale o sistema operacional desejado (por exemplo, TrueNAS SCALE ou Debian) em partições separadas.

    - Utilize o boot manager para escolher qual SO iniciar conforme a função necessária no teste do projeto.

### 4.2. Comunicação via SSH

- **No PC3 e outros dispositivos baseados em Linux:**
    - Instale o OpenSSH Server para permitir conexões remotas.
    - Configure o arquivo `/etc/ssh/sshd_config` para melhorar a segurança (por exemplo, desabilitar login por senha e usar chaves públicas, se possível).
    - Compartilhe as chaves públicas com os membros do grupo para acesso seguro.
- **Testes:**

A partir de um computador (ou VM) em que o grupo trabalhe, abra uma conexão SSH usando:
ssh usuario@IP_do_PC3

    -
    - Verifique se a conexão é estabelecida e se o acesso aos serviços é permitido.

---

# Conclusão

Este documento fornece um guia completo e detalhado para configurar cada componente do projeto – NAS, Firewall/IDS e Backup/Logs – com a possibilidade de execução em máquinas físicas, virtuais ou via dual boot. A comunicação e gerenciamento via SSH garantem que os membros do grupo possam acessar e administrar os serviços remotamente, mesmo que apenas você possua as máquinas reais. Todas as etapas foram detalhadas para facilitar a implementação e a integração dos serviços, permitindo que o projeto seja executado de forma colaborativa e com flexibilidade.

Caso haja alguma dúvida ou seja necessário mais detalhes em alguma etapa, estarei à disposição para ajudar!