Uma imagem com texto

Descrição gerada automaticamente

TeSP de CiberSegurança e Redes Informáticas

Lourenço Eduardo Estêvão Pereira Índio – 2231606

Diogo Miguel Lucas Garcia - 2231620

ZhiJie Ruan - 2231605

Trabalho da Unidade Curricular de SRS

Leiria, novembro de 2024

# Lista de Imagens

[Figura 1 - Diagrama de rede 2](#_Toc187622817)

[Figura 2 – Netplan 8](#_Toc187622818)

[Figura 3 - Dorwarders 8](#_Toc187622819)

[Figura 4 - Zonas 9](#_Toc187622820)

[Figura 5 - Codigo de keys 9](#_Toc187622821)

[Figura 6 - ACL 10](#_Toc187622822)

[Figura 7 - Zonas 10](#_Toc187622823)

[Figura 8 - Netplan 12](#_Toc187622824)

[Figura 9 - Zonas 12](#_Toc187622825)

[Figura 10 - Netplan 14](#_Toc187622826)

[Figura 11 - Configuração de Apache 14](#_Toc187622827)

[Figura 12 - Netplan 15](#_Toc187622828)

[Figura 13 - Lista de Nomes e IP 16](#_Toc187622829)

[Figura 14 - Estado de email 16](#_Toc187622830)

[Figura 15 - login maps 17](#_Toc187622831)

[Figura 16 - Configuração de sokctes 18](#_Toc187622832)

[Figura 17 - Thunderbird 19](#_Toc187622833)

[Figura 18 – Thunderbird 19](#_Toc187622834)

[Figura 19 – Configs gerais do Nagios 21](#_Toc187622835)

[Figura 20 - Configuração web 21](#_Toc187622836)

[Figura 21 - Configuração web 22](#_Toc187622837)

[Figura 22 - Configuração web 22](#_Toc187622838)

[Figura 23 - Configuração web 23](#_Toc187622839)

[Figura 24 - Configuração web 23](#_Toc187622840)

# Lista de siglas e acrónimos

|  |  |
| --- | --- |
| ESTG | Escola Superior de Tecnologia e Gestão |
| IPLeiria | Instituto Politécnico de Leiria |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Índice

[Lista de Imagens ii](#_Toc181826583)

[Lista de siglas e acrónimos iv](#_Toc181826584)

[1. Introdução 1](#_Toc181826585)

[1.1. Objetivo do trabalho 1](#_Toc181826586)

[2. Caso de Estudo 2](#_Toc181826587)

[2.1. Empresa 2](#_Toc181826588)

[2.2. Diagrama de rede 2](#_Toc181826589)

[2.3. Serviço de Email 2](#_Toc181826590)

[2.4. Serviço de Monitorização 2](#_Toc181826591)

[2.5. Serviço de Acesso Remoto 3](#_Toc181826592)

[3. Serviços de Rede Seguros 5](#_Toc181826593)

[3.1. Serviço de nomes (DNS) 5](#_Toc181826594)

[3.1.1. Funcionalidade do DNS em uma Empresa 5](#_Toc181826595)

[3.1.2. BIND (Berkeley Internet Name Domain) 6](#_Toc181826596)

[3.1.3. Como é que isto reforça a segurança? 7](#_Toc181826597)

[3.2. Serviço Web (Apache2) 13](#_Toc181826598)

[3.2.1. Software Apache 13](#_Toc181826599)

[3.2.2. Virtual Hosts 13](#_Toc181826600)

[3.2.3. Segurança 13](#_Toc181826601)

[4. Conclusões 24](#_Toc181826602)

# Introdução

Neste relatório, apresenta-se a fase inicial do desenvolvimento de uma rede e serviços para uma empresa Este projeto visa estabelecer um ambiente seguro e eficiente, correspondendo às necessidades de uma empresa que lida com clientes, serviços, rede e servidores.

## Objetivo do trabalho

Este trabalho será realizado no âmbito da UC de SRS do curso CRI e tem por objetivo, desenvolver uma infraestrutura de rede e serviços segura e eficiente para a empresa uma determinada empresa. Deve permitir que a empresa ofereça suas soluções e plataformas com confiabilidade e segurança.

Serão configurados e implementados serviços essenciais que achamos essenciais como: Serviços de rede e conectividade para garantir uma comunicação segure entre utilizadores, serviços de acesso remoto para facilitar a gestão de maneira mais segura.

# Caso de Estudo

## Empresa

Nome: About

Domínio: about.pt

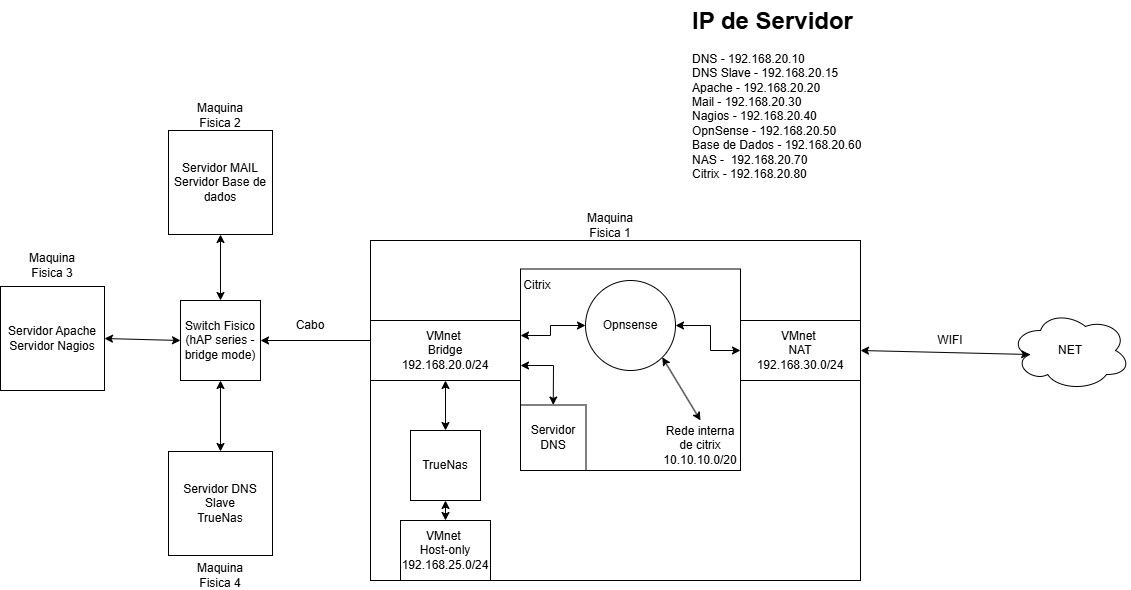
Funcionário: 50 pessoas

Figura - Diagrama de rede

## Diagrama de rede

## Serviço de Email

O serviço de email é essencial para a comunicação interna e externa de qualquer empresa, permite que os colaboradores enviem e recebam emails de forma segura, seja para comunicação interna ou para contato com clientes externos.

## Serviço de Monitorização

O serviço de monitorização é crucial para garantir a operação contínua e eficiente dos sistemas e serviços da empresa, permite que a equipe de TI acompanhe o desempenho, a disponibilidade e a integridade dos recursos de rede, detetando e respondendo rapidamente a possíveis problemas ou falhas que poderão acontecer.

Para implementar este serviço, iremos utilizar o NAGIOS, é um serviço popular e confiável para monitorizar a rede e servidores. O NAGIOS permite monitorizar vários aspetos dos sistemas bem como: disponibilidade de serviços, desempenho de recurso e até mesmo enviar alertas de possíveis problemas.

## Serviço de Acesso Remoto

O serviço de acesso remoto permite que os administradores gerenciem os servidores de forma segura, podendo os mesmos estar fora das instalações da empresa. Esse acesso é fundamental para realizar tarefas de manutenção, atualização e resposta a incidentes de forma rápida e eficiente.

O OpenSSH é um software de acesso remoto, devido à sua segurança e flexibilidade ele é amplamente utilizado para conexões seguras, permitindo o acesso a servidores via protocolo SSH (Secure Shell).

**Configurações de Segurança**:

* **Autenticação por Chave SSH**: A autenticação será feita através da chave SSH, que são mais seguras. Somente usuários com a chave privada irão conseguir ter acesso aos servidores.
* **Criptografia RSA**: Será utilizada a criptografia RSA para a geração das chaves, garantindo assim um nível de alta segurança.
* **Tamanho da Chave**: A chave será gerada com um tamanho de 4096 bits
* **Armazenamento da Chave Privada**: A chave privada será armazenada com segurança pelos administradores da rede, em dispositivos seguros e protegidos por senha, para evitar que seja acedida por terceiros.

**Quem vai utilizar?**

O acesso remoto será distribuído aos administradores do sistema responsáveis pela manutenção e monitorização dos servidores. Cada utilizador autorizado terá sua própria chave SSH, permitindo auditoria e controle de acesso.

# Serviços de Rede Seguros

## Serviço de nomes (DNS)

O serviço de nomes ou DNS (Domain Name System), é responsável pela resolução de nomes de domínio em endereços IP, permitindo que os utilizadores tenham acesso aos serviços e sites da empresa por meio de nomes em vez de endereços IP numéricos. Esse serviço é essencial para a navegação e comunicação em rede, tanto para acesso interno quanto externo.

### Funcionalidade do DNS em uma Empresa

Para uma empresa, o DNS é vital tanto para o **acesso interno quanto externo** aos serviços:

* **Acesso Interno**: Facilita a navegação dentro da rede corporativa, permitindo que funcionários acedam os recursos internos (como servidores de arquivos e intranet) usando nomes amigáveis em vez de endereços IP.

**Acesso Externo**: Permite que clientes e parceiros acedam serviços da empresa hospedados em servidores públicos (por exemplo, site da empresa, e-mail, e-commerce).

### BIND (Berkeley Internet Name Domain)

O BIND (Berkeley Internet Name Domain) é um software de DNS, pois é um dos mais populares e confiáveis para implementação de serviços DNS, com suporte para as principais funcionalidades de segurança e redundância. Algumas das principais funcionalidades que fazem do BIND uma escolha popular incluem:

1. **Suporte a Zonas Primárias e Secundárias**:
   * O BIND permite configurar **servidores DNS primários e secundários**, garantindo **redundância** e **disponibilidade**. Se o servidor DNS primário falhar, o secundário pode continuar respondendo às consultas.
2. **Segurança com DNSSEC**:
   * **DNSSEC** (DNS Security Extensions) é uma extensão de segurança que protege o DNS contra-ataques como envenenamento de cache e falsificação de dados, assegurando a **autenticidade e integridade das respostas DNS**.
3. **Controlo de Acesso com ACLs**:
   * O BIND permite definir **ACLs** (Access Control Lists) para controlar quem pode consultar, transferir zonas ou atualizar registros DNS. Isso ajuda a proteger o DNS contra acessos não autorizados e pode ser configurado para permitir apenas consultas de dispositivos internos, se necessário.
4. **Balanceamento de Carga e Alta Disponibilidade**:
   * Com o uso de **registros DNS de balanceamento de carga** (como registros de tipo *A* com múltiplos IPs), o BIND pode distribuir o tráfego entre vários servidores, proporcionando **distribuição de carga** e **melhor desempenho**.
5. **Log e Monitoramento**:
   * O BIND oferece recursos extensivos de **log** e **monitoramento**, permitindo que os administradores acompanhem as consultas DNS, identifiquem problemas, e ajustem a configuração para otimizar o desempenho e a segurança.
6. **Zonas e Registros:**
   * Zona de Forward (.com): Contém registros para os serviços e servidores acessíveis externamente.
   * Zona de Reverse (ex. 192.168.24.5): Permite a resolução reversa para identificar nomes a partir de endereços IP internos.

### Como é que isto reforça a segurança?

Globalmente, essas configurações reforçam a segurança do serviço DNS ao proteger a integridade, disponibilidade e controle de acesso.

### Configurações do DNS no Cenário

Configuração do Hostname:

Define o hostname como dns.aboutt.pt com o comando:

* sudo hostnamectl set-hostname dns.aboutt.pt

Atualiza o arquivo /etc/hosts para incluir:

* 127.0.1.1 dns.aboutt.pt

Configuração do Netplan:

Define a interface de rede ens33 com um IP estático 192.168.20.10/24 e um gateway padrão 192.168.20.2. Configura o servidor DNS primário como 192.168.20.2.

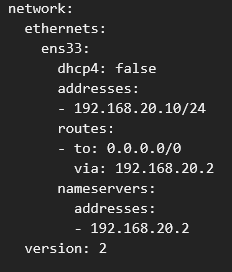


Figura – Netplan

Instalação do Bind:

Atualiza os pacotes e instala o Bind9:

* sudo apt-get update
* sudo apt-get install bind9

Configuração do Forwarding:

Edita o arquivo /etc/bind/named.conf.options para configurar os servidores DNS de encaminhamento:

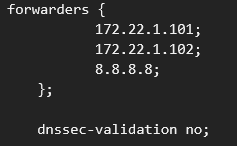


Figura - Dorwarders

Verifica a configuração e reinicia o serviço:

* named-checkconf /etc/bind/named.conf.options
* sudo service named restart

Configuração de Zonas DNS:

Define as zonas em /etc/bind/named.conf.local:

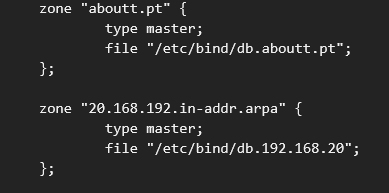


Figura - Zonas

Cria e configura os arquivos de zona direta (db.aboutt.pt) e reversa (db.192.168.20).

Assinatura DNSSEC:

Gera chaves ZSK e KSK com os comandos dnssec-keygen.

Inclui as chaves no arquivo de zona e assina a zona com:

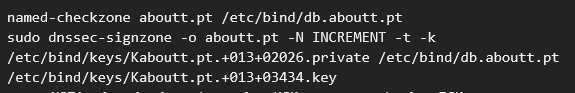


Figura - Codigo de keys

Restrição de Acesso:

Configura uma ACL no arquivo /etc/bind/named.conf.options para permitir consultas recursivas apenas de IPs específicos:

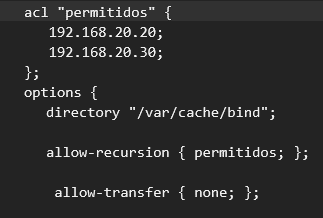


Figura - ACL

Configuração de Servidor Slave:

Adiciona permissões no DNS principal para transferências de zona para o IP do servidor slave (192.168.20.15):

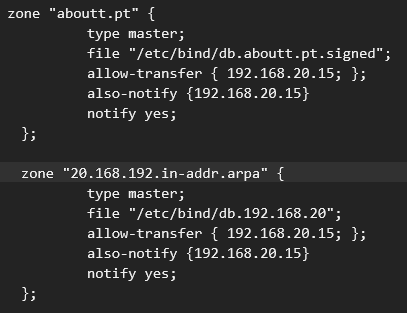


Figura - Zonas

Essas configurações abrangem desde a instalação e configuração básica do DNS até a implementação do DNSSEC e integração com um servidor slave.

### Configurações do DNS Slave no Cenário

1. Definir o hostname do servidor como dns2.aboutt.pt:  
   Use o comando abaixo para definir o hostname:

* sudo hostnamectl set-hostname dns2.aboutt.pt

1. Configurar o arquivo /etc/hosts:  
   Edite o arquivo e adicione a entrada abaixo:

* sudo nano /etc/hosts

No arquivo, adicione:

* 127.0.1.1 dns2.aboutt.pt

1. Reiniciar o servidor para aplicar as alterações:

* sudo reboot

1. Atualizar os pacotes do sistema:

* sudo apt-get update

1. Instalar o Bind9:

* sudo apt-get install bind9

1. Configurar a interface de rede com Netplan:  
   Edite o arquivo de configuração do Netplan com:

* sudo nano /etc/netplan/ 00-installer-config.yaml

Adicione as configurações abaixo:

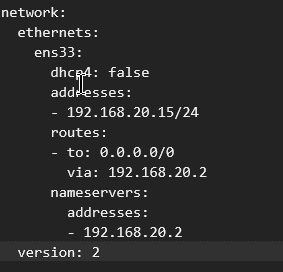


Figura - Netplan

Após salvar, aplique as configurações com:

* sudo netplan apply

1. Configurar as zonas DNS no arquivo do Bind9:  
   Edite o arquivo de configuração local do Bind9:

* sudo nano /etc/bind/named.conf.local

Adicione o conteúdo abaixo:

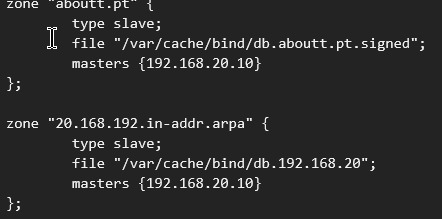


Figura - Zonas

1. Criar o diretório de cache para o Bind e definir permissões:  
   Crie o diretório e ajuste as permissões:

* sudo mkdir -p /var/cache/bind
* sudo chown bind:bind /var/cache/bind

1. Verificar a configuração do Bind9:  
   Execute o comando para validar o arquivo de configuração:

* sudo named-checkconf

1. Reiniciar o serviço Bind9:  
   Após validar a configuração, reinicie o serviço:

* sudo systemctl restart bind9

Com estas configurações, o servidor estará configurado como um DNS Slave sincronizando as zonas "aboutt.pt" e "20.168.192.in-addr.arpa" a partir do mestre no IP 192.168.20.10.

## Serviço Web (Apache2)

Um serviço web permite que pessoas acessem sites e aplicativos de uma empresa pelo navegador. É o que faz o site aparecer na tela quando alguém acede o endereço da empresa.

### Software Apache

Apache é um programa usado para configurar e gerenciar serviços web, permitindo a hospedagem de sites e aplicativos de maneira confiável e personalizável.

### Virtual Hosts

Com o Apache, é possível configurar múltiplos sites ou serviços na mesma máquina, cada um com suas próprias configurações, como endereços e permissões.

### Segurança

* **HTTPS**: Criptografa a comunicação entre o servidor e o usuário para garantir a segurança dos dados.
* **Autenticação Básica**: Restringe o acesso a certas áreas do site, exigindo que o usuário insira um nome de usuário e senha.
* **Forçar HTTPS**: Redireciona automaticamente todos os acessos para uma conexão segura, protegendo os dados durante o tráfego na rede.

### Configurações do Apache no Cenário

* **Configurações Principais:**

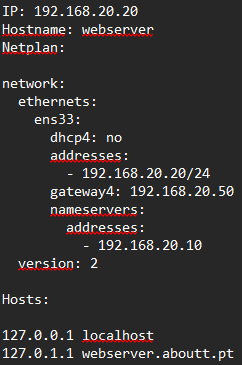


Figura - Netplan

* **Uma imagem com texto, captura de ecrã, Tipo de letra, design

  Descrição gerada automaticamenteAboutt.conf:**

Figura - Configuração de Apache

## Serviço de Email (PostFix)

O Postfix é um servidor de email open-source usado para enviar e receber mensagens via protocolo SMTP, sendo conhecido pela segurança e flexibilidade, permitindo configurações avançadas como autenticação, encriptação e filtragem de mensagens.

### Software PostFix

O Postfix é uma aplicação usada para configurar e gerenciar serviços de email, suportando envio e receção de mensagens através do protocolo SMTP.

### Segurança

* **TLS:** Protege a comunicação entre o cliente e o servidor de email através de encriptação.
* **Autenticação SMTP:** Garante que apenas utilizadores autorizados consigam enviar emails pelo servidor.

### Uma imagem com texto, captura de ecrã, software, Tipo de letra Descrição gerada automaticamenteConfigurações do PostFix no Cenário

Figura - Netplan

* Colocar endereço na VM Email

* No bind do dns colocamos o subdomínio no caso o mail com o respetivo domínio /etc/bind/db.aboutt.pt

Uma imagem com texto, captura de ecrã, Tipo de letra, software

Descrição gerada automaticamente

Figura - Lista de Nomes e IP

* Instalação do Postfix com os seguintes comandos:

Sudo apt-get update  
sudo apt-get install postfix

sudo systemctl status postfix

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

Figura - Estado de email

* No /etc/postfix/master.cf descomentamos o -o smtpd\_tls\_security\_level=encrypt para permitir ativar o TLS e torna lo obrigatório no novo porto "587" e tornar o serviço seguro.

### Configuração da Autenticação SASL no Postfix

A autenticação SASL é essencial para garantir que apenas utilizadores autorizados possam enviar mensagens através do servidor de email. Nesta configuração, o Postfix será integrado ao Dovecot para habilitar o SASL.

### Passos para Configurar a Autenticação SASL

**1. Ativar a Autenticação SASL:**

sudo postconf -e 'smtpd\_sasl\_auth\_enable = yes'

**2. Configurar o Tipo de Autenticação para o Postfix utilizar o Devecot como autenticação**:

sudo postconf -e 'smtpd\_sasl\_type = dovecot'

**3. Configurar o Socket de Comunicação:**

sudo postconf -e 'smtpd\_sasl\_path = private/auth'

**4. Configurar o Domínio Local**

sudo postconf -e 'smtpd\_sasl\_local\_domain = $myhostname'

**5. Configurar Restrições de Remetentes**

sudo postconf -e 'smtpd\_sender\_restrictions = reject\_sender\_login\_mismatch, permit\_sasl\_authenticated, reject'

1. **Impede Autenticação Anônima**

sudo postconf -e 'smtpd\_sasl\_security\_options = noanonymous'

1. **Editar o arquivo de mapeamento:**

sudo nano /etc/postfix/smtpd\_sender\_login\_maps

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

Figura - login maps

1. **O comando seguinte é importante para guardar o arquivo de mapeamento:**

sudo postmap /etc/postfix/smtpd\_sender\_login\_maps

### ****3. Configuração do Socket Dovecot para Postfix****

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

Figura - Configuração de sokctes

A configuração do Socket Dovecot para Postfix permite que o Postfix use o Dovecot para autenticar os utilizadores, assim apenas utilizadores autorizados poderão enviar emails pelo servidor.

### Configuração do Thunderbird

**Configuração do cliente de email com os seguintes detalhes:**

Servidor SMTP: 192.168.20.30 no porto 587 (STARTTLS) e posteriormente 465 (SSL/TLS).

Servidor POP3: 192.168.20.30 no porto 110.

**Alteração da Segurança:**

Trocamos a segurança da ligação do SMTP de STARTTLS para SSL/TLS no Thunderbird.  
Mudamos o porto do SMTP para 465, garantindo comunicação criptografada desde o início.

**Configuração do POP3**

Removeu-se a opção “Manter as mensagens no servidor” para economizar espaço no servidor.  
Configurou-se no Thunderbird para descarregar mensagens e apagá-las automaticamente do servidor após o download.

**Alguns Testes no Thunderbird:**

De Diogo para Lourenço:

Uma imagem com texto, captura de ecrã, software, Página web

Descrição gerada automaticamente

Figura - Thunderbird

De António para Diogo:

Uma imagem com captura de ecrã, software, texto, Ícone de computador

Descrição gerada automaticamente

Figura – Thunderbird

## Servidor de Monitorização (Nagios4)

O **Nagios 4** é uma ferramenta de código aberto para monitoramento de sistemas, redes e aplicações. Com uma interface web intuitiva, os administradores podem visualizar o status dos dispositivos e configurar parâmetros de monitoramento.

Entre suas características principais estão:

* **Monitoramento em tempo real**: Realiza verificações frequentes para detetar falhas ou problemas.
* **Alertas e notificações**: Envia notificações através de e-mail ou SMS quando há falhas.
* **Escalabilidade**: Suporta desde redes pequenas até grandes infraestruturas corporativas.
* **Interface web**: Permite monitorar e configurar o sistema através de uma interface intuitiva.
* **Extensibilidade**: Oferece suporte a plugins para monitorar uma ampla gama de serviços.

### Configurações do Nagios no Cenário

* **Configurações Principais:**

Uma imagem com texto, captura de ecrã, Tipo de letra, design

Descrição gerada automaticamente

Figura – Configs gerais do Nagios

* **apache.conf:**

Uma imagem com texto, captura de ecrã, Tipo de letra, design

Descrição gerada automaticamente

Figura - Configuração web

* **dns.cfg:**

**Uma imagem com texto, captura de ecrã, Tipo de letra, design

Descrição gerada automaticamente**

Figura - Configuração web

**mail.cfg:**

**Uma imagem com texto, captura de ecrã, menu, Tipo de letra

Descrição gerada automaticamente**

Figura - Configuração web

**mysql.cfg:**

**Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente**

Figura - Configuração web

**opnsense.cfg:**

**Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente**

Figura - Configuração web

# Conclusões

Este relatório apresenta a fase inicial do desenvolvimento de uma rede segura e eficiente para a empresa About, incluindo monitoramento com Nagios, acesso remoto com OpenSSH, DNS com BIND e servidor web com Apache. Essas configurações garantem comunicação segura, proteção de dados e confiabilidade dos serviços online, criando uma base sólida para o ambiente de TI da empresa.