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

Lista de siglas e acrónimos

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

Índice

1. 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.

1.1. 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.

2. Caso de Estudo

2.1. Empresa

Nome: About

Domínio: about.pt

Funcionário: 50 pessoas

2.2. Diagrama de rede

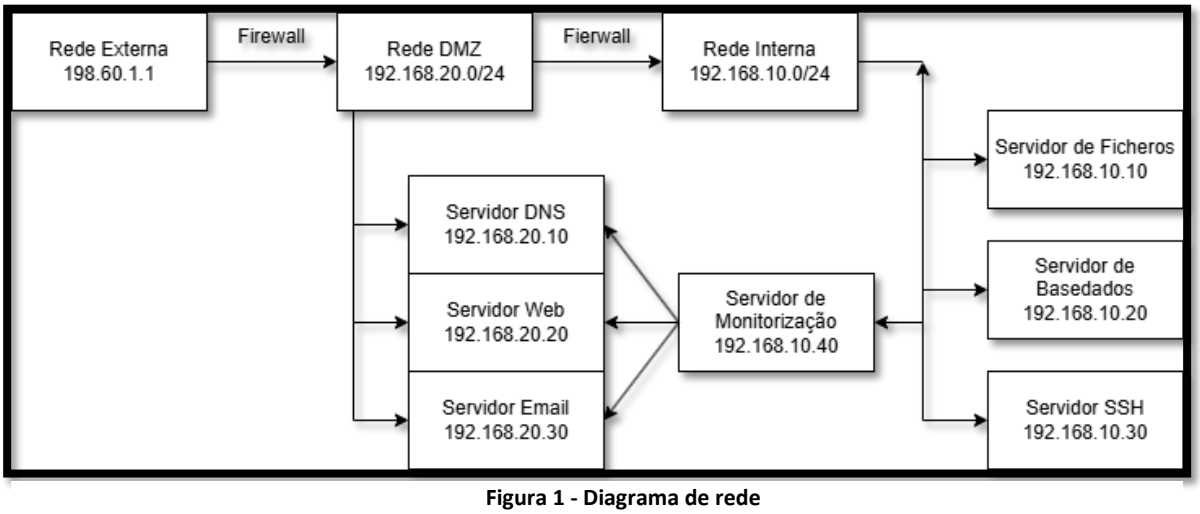


Figura 1 - Diagrama de rede

2.3. 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.

2.4. 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.

2.5. 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.

3. Serviços de Rede Seguros

3.1. 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.

3.1.1. 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).

3.1.2. 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.

3.1.3. 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.

3.1.4. 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.

```
network:
  ethernets:
    ens33:
      dhcp4: false
      addresses:
      - 192.168.20.10/24
      routes:
      - to: 0.0.0.0/0
        via: 192.168.20.2
      nameservers:
        addresses:
        - 192.168.20.2
  version: 2
```

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:

```
forwarders {
            172.22.1.101;
            172.22.1.102;
            8.8.8.8;
    };

    dnssec-validation no;
```

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:

```
zone "aboutt.pt" {
        type master;
        file "/etc/bind/db.aboutt.pt";
};

zone "20.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168.20";
};
```

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:

```
named-checkzone aboutt.pt /etc/bind/db.aboutt.pt
sudo dnssec-signzone -o aboutt.pt -N INCREMENT -t -k
/etc/bind/keys/Kaboutt.pt.+013+02026.private /etc/bind/db.aboutt.pt
/etc/bind/keys/Kaboutt.pt.+013+03434.key
```

Restrição de Acesso:

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

```
acl "permitidos" {
   192.168.20.20;
   192.168.20.30;
};
options {
   directory "/var/cache/bind";

   allow-recursion { permitidos; };

    allow-transfer { none; };
```

Configuração de Servidor Slave:

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

```
zone "aboutt.pt" {
        type master;
        file "/etc/bind/db.aboutt.pt.signed";
        allow-transfer { 192.168.20.15; };
        also-notify {192.168.20.15}
        notify yes;
};

zone "20.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168.20";
        allow-transfer { 192.168.20.15; };
        also-notify {192.168.20.15}
        notify yes;
};
```

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

3.1.5. 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
2. 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
3. Reiniciar o servidor para aplicar as alterações:
   - sudo reboot

4. Atualizar os pacotes do sistema:

    - sudo apt-get update

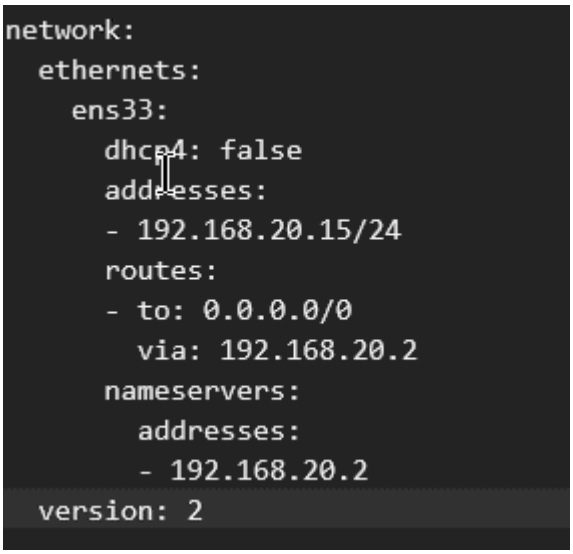
5. Instalar o Bind9:

    - sudo apt-get install bind9

6. 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:



   Após salvar, aplique as configurações com:

    - sudo netplan apply

7. 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:

```
zone "aboutt.pt" {
        type slave;
        file "/var/cache/bind/db.aboutt.pt.signed";
        masters {192.168.20.10}
};

zone "20.168.192.in-addr.arpa" {
        type slave;
        file "/var/cache/bind/db.192.168.20";
        masters {192.168.20.10}
};
```

8. 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

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

   - sudo named-checkconf

10. 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.

3.2. 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.

3.2.1. 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.

3.2.2. 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.

3.2.3. 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.

3.2.4. Configurações do Apache no Cenário

- **Netplan:**

```
network:
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.20.20/24
      gateway4: 192.168.20.2
      nameservers:
        addresses:
          - 192.168.20.10
  version: 2
```

- **Aboutt.conf:**

```
<VirtualHost *:80>
  ServerName www.aboutt.pt
  DocumentRoot /var/www/aboutt
</VirtualHost>

<VirtualHost *:443>
  ServerName www.aboutt.pt
  DocumentRoot /var/www/aboutt

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
  SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

</VirtualHost>

<Directory /var/www/aboutt>
  AllowOverride All
  Require all granted
</Directory>
```

3.3. 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.

3.3.1. 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.

3.3.1. 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.

3.3.2. Configurações do PostFix no Cenário

- Colocar endereço na VM Email

```
 GNU nano 6.2                                  /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: false
      addresses:
      - 192.168.20.30/24
      gateway4: 192.168.20.2
      nameservers:
        addresses:
          - 192.168.20.10
    ens37:
      dhcp4: true
  version: 2
```

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

```
 GNU nano 4.8                                                /etc/bind/db.aboutt.pt
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     dns.aboutt.pt. antonio.aboutt.pt. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      dns.aboutt.pt.
dns     IN      A       192.168.20.10
gateway IN      A       192.168.20.2
web     IN      A       192.168.20.20
mail    IN      A       192.168.20.30

$INCLUDE "/etc/bind/keys/Kaboutt.pt.+013+03434.key" #ZSKkey
$INCLUDE "/etc/bind/keys/Kaboutt.pt.+013+02026.key" #KSKkey
```

- Instalação do Postfix com os seguintes comandos:

  Sudo apt-get update

  sudo apt-get install postfix

  sudo systemctl status postfix

```
ubuntu@mail:~$ sudo systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
     Active: active (exited) since Mon 2024-11-25 13:22:32 UTC; 27min ago
       Docs: man:postfix(1)
    Process: 1688 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1688 (code=exited, status=0/SUCCESS)
        CPU: 2ms

nov 25 13:22:32 mail.aboutt.pt systemd[1]: Starting Postfix Mail Transport Agent...
nov 25 13:22:32 mail.aboutt.pt systemd[1]: Finished Postfix Mail Transport Agent.
ubuntu@mail:~$
```

- 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.

4. 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 servidora 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.