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

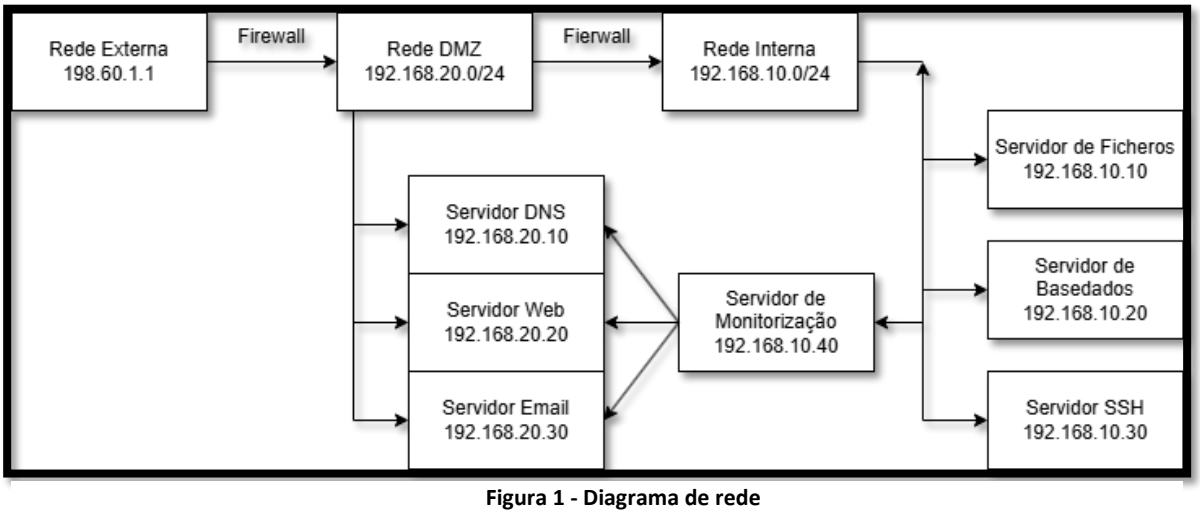

Figura 1 - Diagrama de rede

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.

3.2. 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.

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.