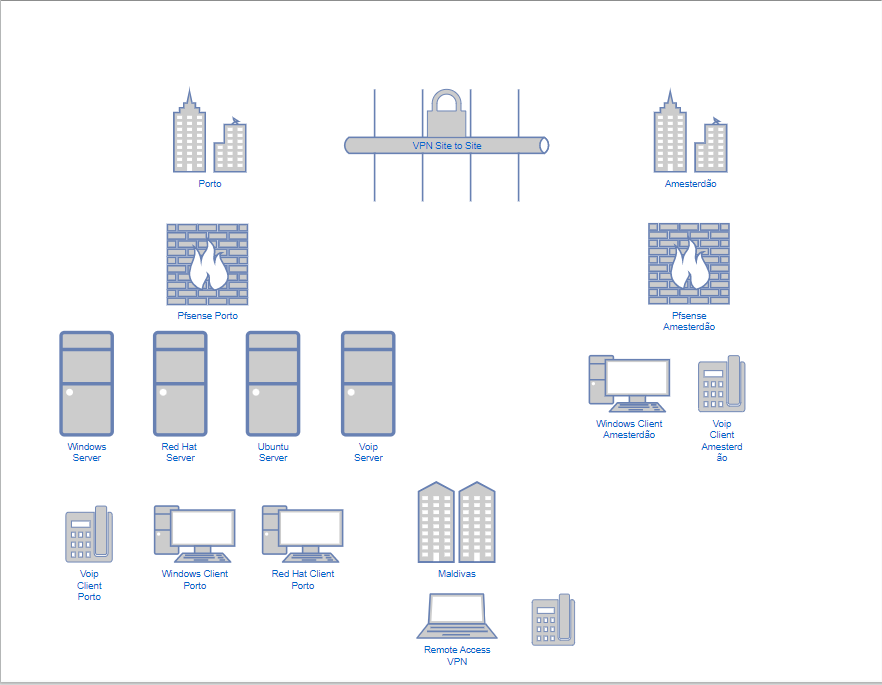
PROJETO UFCD 9191

1. Objetivos do projeto:
   1. Projetar e aplicar todos os conhecimentos adquiridos ao nível de redes e segurança;
   2. Projetar e aplicar todos os conhecimentos adquiridos ao nível de sistemas Linux e Microsoft, Kali entre outros.
2. Topologia de Rede:

No que concerne à parte de servidores e serviços pede-se que sejam instalados e configurados de acordo com o seguinte diagrama:



Kali linux

**Endereçamento:**

**Domínio:** citeforma.pt

**Rede Porto**: 192.168.60.0/24

Red Hat Server:192.168.60.2 (6-253)

Windows Server: 192.168.60.1(6-253)

Ubuntu Server: 192.168.60.3

VOIP Server: 192.168.60.4

Windows Client Porto e Red Hat Client Porto: DHCP

PfSense Porto: 192.168.60.254

**Rede Amesterdão:** 172.15.3.0/24

Pfsense Amesterdão: 172.15.3.254

Windows Cliente Amesterdão: DHCP(2-253)

1. Considerações iniciais e instruções:
   1. Cada aluno projeta e configura a topologia apresentada de acordo com as diretrizes definidas nos pontos seguintes.
   2. Qualquer situação omissa que não tenha sido mencionada neste enunciado, deve ser colocada ao formador, para posteriormente ser esclarecida/comunicada a todos os alunos.
   3. As tecnologias/diretrizes mencionadas neste enunciado são de implementação obrigatória, no entanto poderão ser implementadas mais tecnologias ou melhorias por forma a valorizar o trabalho. Melhorias essas que devem ser refletidas na apresentação e devidamente fundamentadas.
   4. Deve ser efetuada no final uma apresentação de **15** minutos sobre o trabalho efetuado.
      1. O formador irá solicitar/formular questões sobre o trabalho aos formandos.
2. **Serviços abordados**
3. DNS
4. DHCP
5. Postfix
6. Squid Proxy
7. Openfire
8. SSH
9. VPN
10. Remote Access VPN
11. VOIP
12. OpenVAS
13. Nessus

**DHCP E DNS**

**Ações a desenvolver:**

Instalar e configurar o servidor de DHCP E DNS na máquina de Red Hat Server e Windows Server.

Serviço ativo e bem configurado.

Estes dois serviços é para estarem obrigatoriamente a trabalhar nas duas máquinas e caso uma vá abaixo por qualquer motivo é a outra que fornece os serviços (failover).

Deve ser feito um script em python conforme feito em aula para confirmar que estão ambas a trabalhar em failover. Esse script deve ser configurado para passar a ser um serviço da máquina.

Criar registos de DNS para os diferentes serviços.

**POSTFIX**

**Ações a desenvolver aquando da instalação deste serviço:**

Este serviço é para ser instalado no Ubuntu Server.

Criar uma conta de email para cada utilizador.

Serviço ativo e pronto a fazer troca de emails entre utilizadores.

Todos as máquinas cliente devem ter a aplicação do Thunderbird para efetuar troca de emails entre utilizadores.

**SSH**

**Ações a desenvolver aquando da instalação deste serviço:**

Aceder de uma forma segura de uma máquina para outra.

Serviço ativo e configurado.

Instalar o PUTTY/MobaXterm em todas as máquinas Windows.

Mudar a porta do SSH para a 22006.

**OPENFIRE**

**Ações a desenvolver aquando da instalação deste serviço:**

Criar uma base de dados em MariaDB e integrar com a Active Directory para utilizar os utilizadores que estão alojados no Windows Server.

Mudar a porta do serviço para 8888 e 8889.

Serviço ativo e bem configurado.

Os clientes devem ter a aplicação Spark instalada e configurada para trocarem mensagens entre eles.

**Servidor VOIP**

**Ações a desenvolver aquando da configuração desta máquina:**

Deve instalar e configurar o serviço asterisk. Criar três extensões telefónicas (201,202,203).

Instalar a aplicação do zoiper na máquina Red Hat Client e o 3CX phone nas máquinas Windows.

**Kali Linux**

**Ações a desenvolver aquando da configuração desta máquina:**

Deve ser instalado nesta máquina o OpenVAS e o Nessus para serem elaborados relatórios sobre as vulnerabilidades existentes na infraestrutura da empresa para ser corrigidas posteriormente.

**PfSense Porto**

**Ações a desenvolver aquando da configuração desta máquina:**

Devem ser configuradas de maneira a aceder com o Administrator do Windows Server.

Os acessos terão que ser feitos obrigatoriamente por HTTPS, através da criação de um certificado.

Deve ser feita uma ligação VPN Site to Site para a rede de Amesterdão.

Deverá ser criada uma rota estática para a rede de Amesterdão para garantir que a zona tem Internet.

Deve ser feito port forwarding para a vossa máquina física e ou telemóvel.

**PfSense Amesterdão**

**Ações a desenvolver aquando da configuração desta máquina:**

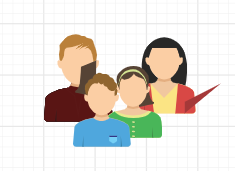
Deve ser feita uma ligação VPN Site to Site para a rede do Porto.

**SQUID PROXY:**

**Ações a desenvolver aquando da instalação deste serviço:**

O Squid e o Squid Guard devem estar instalados na PfSense do Porto.

Os **sites bloqueados** são: citeforma.pt, cisco.com, lpi.org.



**Utilizadores:**

-Roger

-Alex

-Sara

-Margarida

-Francisca

**Organizational Units (OU’s)**

Técnicos (Roger e Alex)

Suporte (Sara, Margarida e Francisca)

**NOTAS:**

Todas as máquinas devem estar no domínio inclusive a Pfsense.

Os utilizadores são criados no Windows Server.

Todos os serviços devem ser acedidos pelo nome do domínio e não por IP’s.

Todos os clientes e servidores só devem ter uma placa LAN.

As versões do Ubuntu Server deve ser a versão 20.04 ou superior.

A versão dos Windows Server deve ser a 2022.

As versões dos Windows Client devem ser a 10 pro.

1. Cotações:

|  |  |
| --- | --- |
| ***Tarefa*** | ***Valorização*** |
| DHCP e DNS | 1 valor |
| SSH | 1 valor |
| Openfire | 3 valores |
| VPN Site to Site | 3 valores |
| Remote Access VPN | 4 valores |
| Email | 3 valores |
| Squid | 1 valor |
| VOIP | 2 valores |
| Kali | 2 valores |
| Total | 20,00 Valores |

1. Data de Entrega:
   1. Até ao dia 08/03/2023.