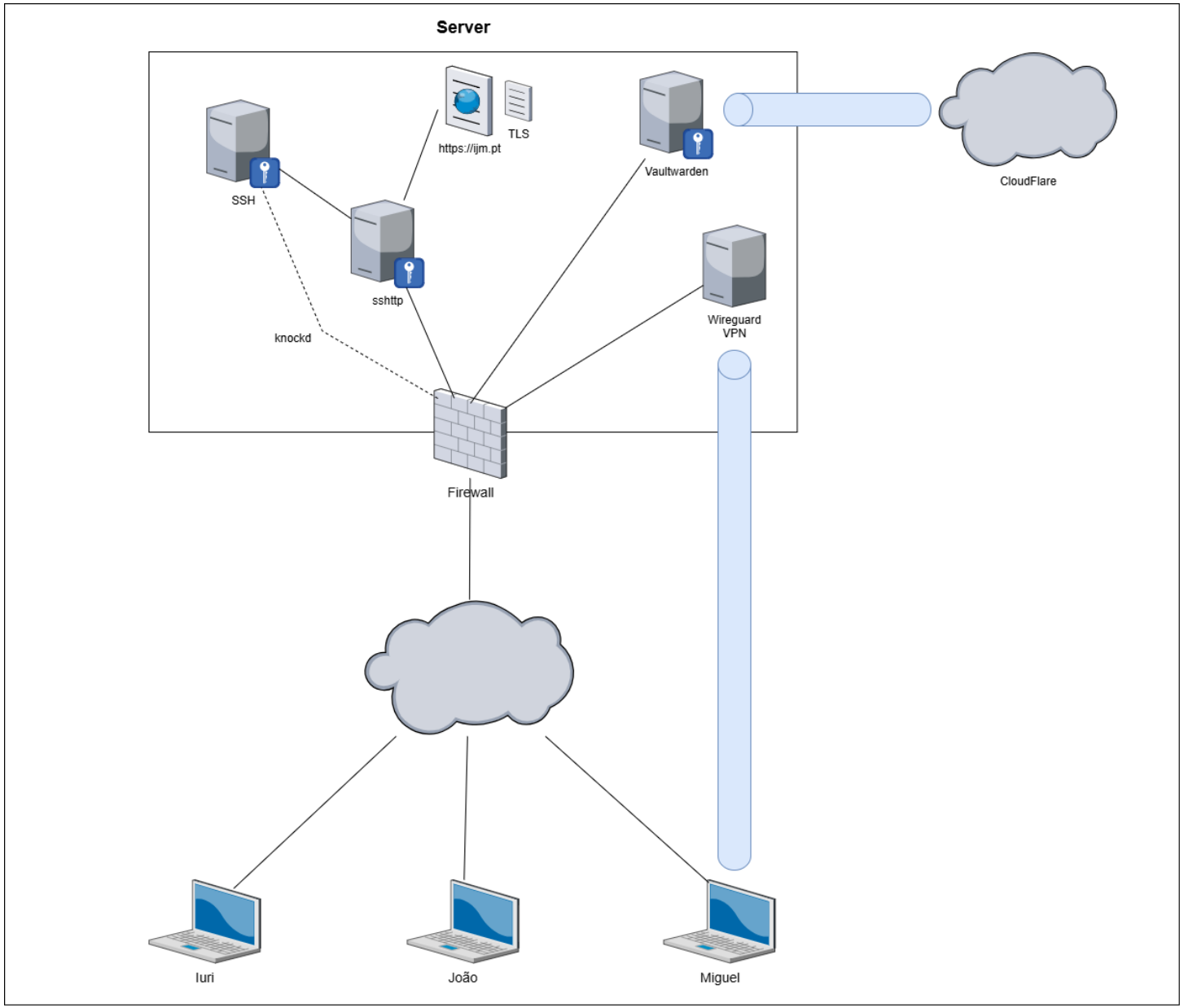
Segurança de Sistemas

Grupo D4

- Iuri Carrasqueiro (2222059)
- João Tendeiro (2222047)
- Miguel Lopes (2222397)

Índice

Esquema de rede



Criação do domínio e Implementação do Site

Obtenção gratuita de "ijm.pt" através do serviço dominios.pt

Serviço Web- **Apache2**

Criação de Certificado TLS

SSH

sshd:

- Chaves Assimétricas
- Não permite acesso root
- Portos 22
- Porto 22022: utilizado pelo sshttpd

Fail2ban:

- Bloqueio de IPs após 4 tentativas falhadas de troca de chaves via SSH
- Bloqueio temporário de 10 minutos

Firewall

Objetivo:

Proteger o servidor contra ataques filtrando tráfego de entrada e saída

Serviço IPTABLES:

Politica por omissão: Descarta pacotes que não atendem às regras definidas

Regras stateful e stateless

Limitação de pacotes ICMP, TCP e UDP

Logs todas as novas conexões de entrada

Firewall

Regras IN

- Ping
- SSH (22)
- HTTP(80)
- HTTPS(443)

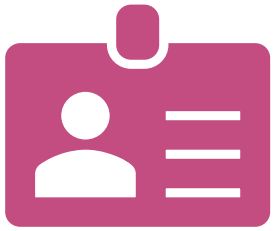
Regras OUT

- DNS(53)
- SSH(22)
- Whois(43)
- DNS over TLS(853)
- Git(9418)
- HTTP(80)
- Ping
- HTTPS(443)

SSHTTP

Objetivo:

Multiplexar HTTPS e SSH através de um único porto (443)



Identificação do Protocolo:

SSH: Encaminhado para a porto **22022**

HTTPS: Encaminhado para a porto **44044**

Port Knocking

- **Objetivo**: Abrir portos de forma dinâmica e segura
- Serviço Knockd
  - Abertura do porto 22:
    - Ø knock -v 192.168.20.150 22059 22047:udp 22397
  - Fechar porto 22:
    - Ø knock -v 192.168.20.150 22397 22047:udp 22059

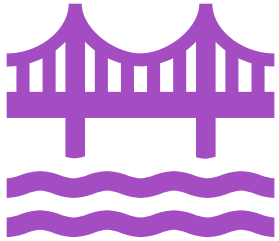
WireGuard

- **Objetivo**: Proporcionar acesso seguro à rede interna do servidor
- Serviço WireGuard
  - Porto 51820 UDP
  - Adiciona regras ao Iptables para permitir o funcionamento do serviço

Bitwarden

Objetivo:

Gerir senhas de forma segura



Serviço Bitwarden

Acesso ao serviço através de um túnel seguro criado via Cloudflare (porto 7844)

Questões