Instituto Superior de Engenharia do Porto

Sprint 2 - ASIST

Grupo 28

Tiago Marques – 1201276

Eduardo Silva – 1201371

Pedro Alves – 1201381

Pedro Rocha – 1201382

dezembro, 2022

Índice de Conteúdos

Índice de Figuras

Índice de Tabelas

US2 e US3 (3.2.4 - 4 e 3.2.4 - 5) – Como administrador do sistema quero que apenas os clientes da rede interna do DEI possam aceder à solução. Os clientes devem ser definidos pela simples alteração de um ficheiro de texto.

Para a realização das funcionalidades acima mencionadas, foi necessária a criação de uma firewall, para podermos definir que endereços podiam, ou não, aceder à solução. Para a realização da mesma, o principal comando usado foi o *"iptables"*.

Como a nossa solução está hospedada numa VM do DEI, apenas os clientes da rede interna (via VPN) conseguiam aceder à solução, mas, mesmo assim, foi feito o bloqueio (DROP) de todos os *IPs* externos com a *flag* -A (a *flag* -A adiciona a "regra" ao fim da lista, tendo em conta que mal o *IP* cumpra com alguma "regra" ele é aceite ou rejeitado de imediato, não verificando as outras regras, por esse motivo este bloqueio total tem de ser feito no fim). Após isto fizemos o *"ACCEPT"* de todos os *IPs* da rede do DEI, com a *flag* -I (a *flag* -I, quando não definida a posição para a regra ser inserida, insere no topo da lista). Para efeitos de teste bloqueamos também o *IP* de um elemento do grupo, para haver a verificação de que as regras estavam a ser bem definidas, tal como se pode ver nas seguintes imagens:

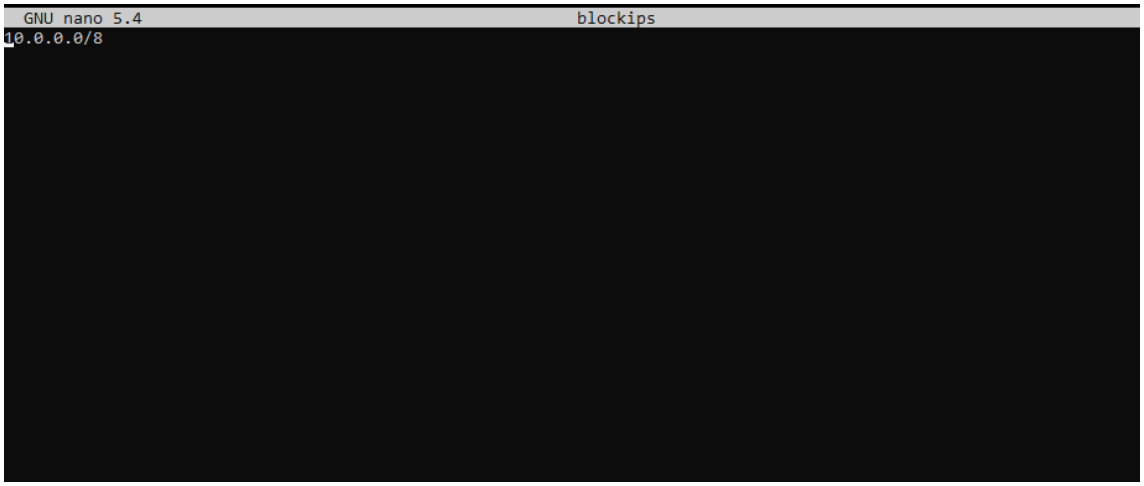

Figura 1 – Permissão de acesso à solução pelos utilizadores da rede do DEI

Como se pode reparar, os *IPs* a ser aceites mencionados em cima (neste caso a rede do DEI) foram definidos num ficheiro de texto.

Depois de inseridos no ficheiro de texto, fizemos um script em que são lidas todas as linhas do ficheiro definido e é feita a definição das regras de acesso, sendo que no fim do script é sempre bloqueado o *IP* de teste do elemento do grupo e todos os *IPs* externos.

```
  GNU nano 5.4                          iptraffic.sh *
#!/bin/bash
input="/home/blockips"
while IFS= read -r line
do
  iptables -I INPUT -p tcp --dport 80 -s $line -j ACCEPT
  iptables -I INPUT -p tcp --dport 22 -s $line -j ACCEPT
done < "$input"

iptables -I INPUT -p tcp --dport 80 -s 10.8.42.94 -j DROP
iptables -I INPUT -p tcp --dport 22 -s 10.8.42.94 -j DROP
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 22 -j DROP
```

Figura 2 – Script para restringir acesso à solução

Na resolução destas funcionalidades apenas bloqueamos o acesso a solução via HTML (*port*: 80) e via SSH (*port*: 22).

```
C:\Users\edusi>ipconfig

Windows IP Configuration


PPP adapter VPN Isep:

   Connection-specific DNS Suffix  . : dei.isep.ipp.pt
   IPv4 Address. . . . . . . . . . . : 10.8.42.94
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : Home
   IPv4 Address. . . . . . . . . . . : 192.168.1.140
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254
```

Figura 3 – Endereço IPv4 a ser bloqueado para efeitos de teste

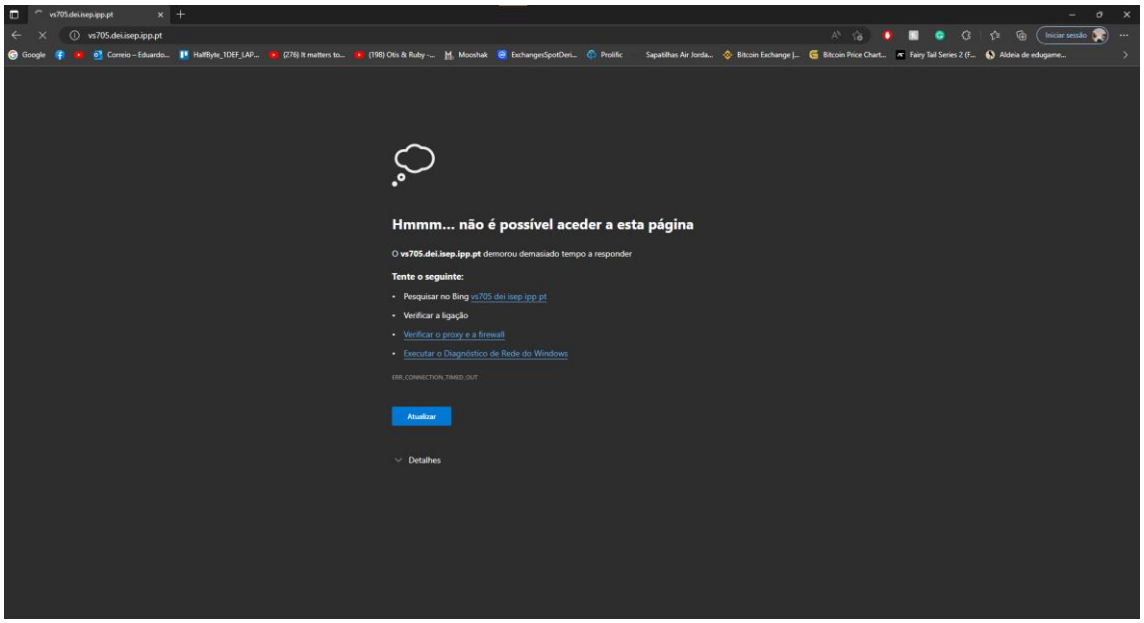

Figura 4 – Bloqueio bem-sucedido

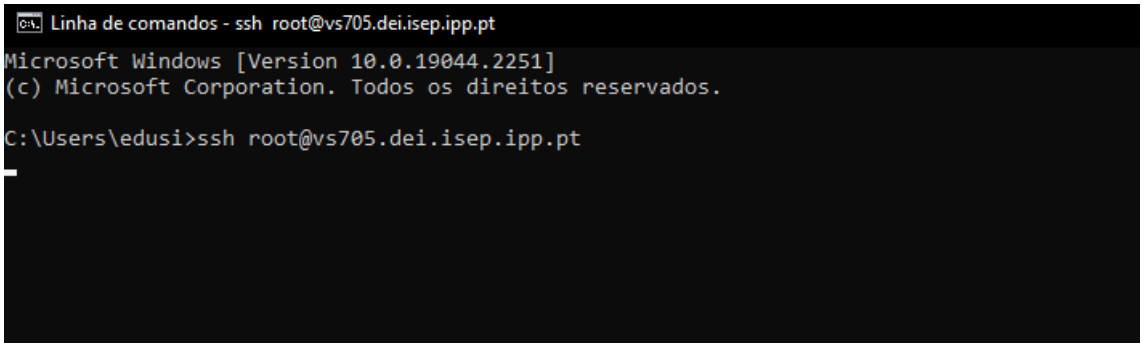

Figura 5 – Impossibilidade de aceder à VM via SSH

Nas três imagens acima listadas, podemos comprovar que o endereço de *IP* bloqueado para teste perde o acesso tanto ao *website* (porta 80) como à conexão via SSH (porta 22).

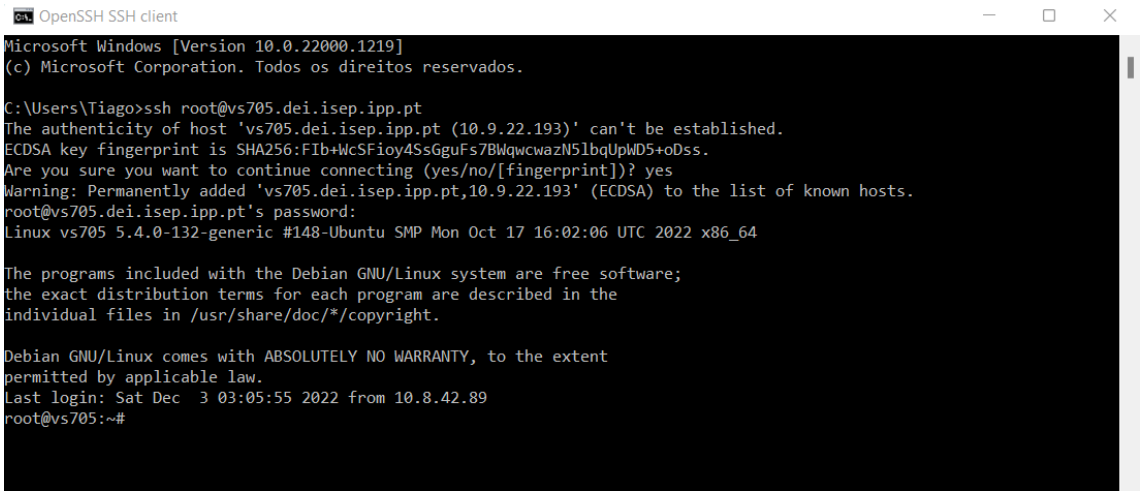

Figura 6 - Acesso à VM via SSH permitido

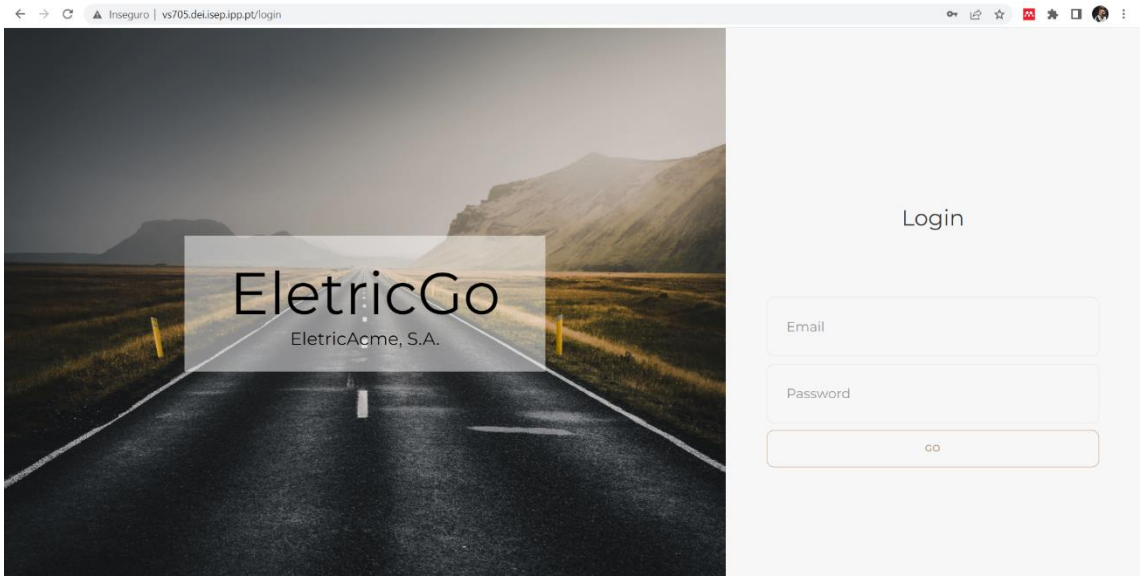

Figura 7 – Utilizador com permissão de acesso ao website

Já nas imagens acima, estando num utilizador normal da rede VPN do DEI, o acesso ao SSH é permitido tal como ao *website*.

US4 (3.2.4-6) - Como administrador quero identificar e quantificar os riscos envolvidos na solução preconizada

Com a finalidade de analisar a probabilidade de um determinado cenário ocorrer e o impacto do mesmo, é elaborada a Matriz de Risco. A cada célula da tabela está associado uma probabilidade e um impacto estimado.

		Impacto (Severidade)			
		Catastrófico (4)	Crítico (3)	Moderado (2)	Marginal (1)
PROBABILIDADE	Frequente (5)	20	15	10	5
	Provável (4)	16	12	8	4
	Ocasional (3)	12	9	6	3
	Remoto (2)	8	6	4	2
	Improvável (1)	4	3	2	1

Figura 8 - Matriz de Avaliação de Risco

A cada célula está associada a cor referente ao risco que apresenta, consoante a seguinte tabela.

Legenda (risco)	
15 - 20	Alto
10 - 14	Sério
5 - 9	Médio
1 - 4	Baixo

Figura 9 - Legenda (risco)

Na tabela seguinte, os riscos estão identificados, fundamentados e classificados.

Risco	**Fundamentação**	**Classificação**
Ataques *DDoS* e *DoS*	Probabilidade improvável e impacto catastrófico	4
Falha de alimentação elétrica	Probabilidade remoto e impacto marginal	6
Falha de conexão à Internet	Probabilidade ocasional e impacto crítico, uma vez que é perdida a conexão à base de dados, deixamos de poder fazer *requests* à mesma, não conseguindo assim fazer a interligação de módulos	9

Falha Servidores do *DEI*	Os diferentes módulos do projeto são serviços significantes, e p.e., o módulo de logística e o SPA necessitam do módulo de Gestão de Armazéns para o seu funcionamento, ou seja, relativamente à probabilidade é ocasional e ao impacto catastrófico	12
Falha de segurança	Com o desenvolvimento da funcionalidade 3.2.4 – 5, que permite a definição da permissão ou não do acesso à VM de clientes, através da alteração de um ficheiro de texto (manipulação de informação sensível), criou-se uma exposição a uma possível falha de segurança, uma vez que existe partilha de componentes administrativas, ou seja, probabilidade frequente e impacto catastrófico	20

Tabela 1 - Análise de Riscos

US5 (3.2.4-7) - Como administrador do sistema quero que seja definido o MBCO (Minimum Business Continuity Objective) a propor aos stakeholders

Definição do MBCO

O MBCO (Minimum Business Continuity Objective) corresponde à definição de um nível de serviços mínimo que deve se manter operacional se ocorrer um acidente, emergência ou desastre, para que a empresa consiga prosseguir com as suas atividades vitais.

Enquadramento com o negócio

Neste caso, como a EletricGo é uma empresa especializada em entregas, ao definir o MBCO, teremos de garantir que a EletricGo possa continuar a efetuar e gerir as entregas.

Análise do MBCO

Considerando o que foi mencionado anteriormente, os serviços que devem se manter operacionais são:

- Informação dos utilizadores, para que nenhuma informação relacionada com os utilizadores registados na aplicação seja perdida e, assim, para que os possam continuar a utilizar a aplicação;
- Gestão das entregas (Criar, Listar, Atualizar e Eliminar) a fim de que as principais atividades da EletricGo possam ser realizadas normalmente, assumindo que a base de dados que contém a informação relativa às entregas esteja funcional também.

Com estes dois serviços assegurados, a empresa pode continuar com as suas principais atividades mesmo que ocorra algum acontecimento inesperado.