

Sprint 2

Administração de Sistemas

Turma 3DF _ Grupo 25
1200625 – Sérgio Lopes
1200628 – Tiago Freitas
1201386 – Rita Sobral
1202016 – Vasco Azevedo

Data: 04/12/2022

Índice

Índice de quadros, figuras, abreviaturas	3
User Story 2.....	4
User Story 3.....	7
User Story 4.....	10
User Story 5.....	12

Índice de quadros, figuras, abreviaturas

Tabela 1.....	10
Tabela 2 - Matriz de Risco	10
Tabela 3 - Legenda da Matriz de Risco	11
Figura 1 - ipConfig	4
Figura 2 - ipTables	4
Figura 3 - ipTables -L antes de editar	5
Figura 4 - ipTables -L após edição	5
Figura 5	6
Figura 6	6
Figura 7 - Lista ip	7
Figura 8 - ipTables -L antes de edição	7
Figura 9 - Desenvolvimento da US	8
Figura 10 - ipTables -L após edição	8
Figura 11	9
Figura 12	9

User Story 2

Como administrador do sistema quero que apenas os clientes da rede interna do DEI (cablada ou via VPN) possam aceder à solução.

No desenvolvimento desta User Story, temos em nossa posse a vm **Debian 11 Bullseye (base system)** - **All VNETs**. Sendo que devemos de controlar as tentativas de conexão à nossa vm, vamos definir regras da iptables que atuarão em cadeia de Input. Para tal, conectados á vpn do DEI vemos o ipconfig:

```
PPP adapter ISEP VPN:

Connection-specific DNS Suffix  . : dei.isep.ipp.pt
IPv4 Address. . . . .           : 10.8.43.147
Subnet Mask . . . . .           : 255.255.255.255
Default Gateway . . . . .       : 0.0.0.0
```

Figura 1 - ipConfig

Concluindo que todos os clientes da rede interna do DEI pertence a 10.8.0.0/16.

Visto que queremos permitir o acesso à nossa máquina aos clientes de rede interna do DEI e bloquear todas as restantes conexões, usando Accept e Drop à tabela filter iremos garantir este critério e para que as nossas alterações sejam guardadas usamos o comando sudo /sbin/iptables-save.

```
root@vs758:~# iptables -A INPUT -p tcp --dport 22 -s 10.9.22.246/16 -j ACCEPT
root@vs758:~# iptables -A INPUT -p tcp --dport 22 -s 10.8.0.0/16 -j ACCEPT
root@vs758:~# iptables -A INPUT -p tcp --dport 22 -j DROP
root@vs758:~# sudo /sbin/iptables-save
# Generated by iptables-save v1.8.7 on Sun Dec  4 12:27:37 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 10.9.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.8.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j DROP
COMMIT
# Completed on Sun Dec  4 12:27:37 2022
# Generated by iptables-save v1.8.7 on Sun Dec  4 12:27:37 2022
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 2222 -j DNAT --to-destination :22
COMMIT
# Completed on Sun Dec  4 12:27:37 2022
# Warning: iptables-legacy tables present, use iptables-legacy-save to see them
```

Figura 2 - iptables

Tendo que:

1. O primeiro comando garante que não somos bloqueados de aceder à solução via SSH (10.9.22.246/16);
2. De seguida permitimos o acesso aos clientes de rede interna do DEI (10.8.0.0/16);
3. Bloqueando por fim o acesso a todas outras conexões;

Para garantir o nosso desenvolvimento temos o iptables -L antes e depois das alterações e ainda o acesso á nossa solução com e sem vpn, respetivamente.

```
root@vs758:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@vs758:~#
```

Figura 3 - iptables -L antes de editar

```
root@vs758:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     tcp  --  10.9.0.0/16            anywhere            tcp dpt:ssh
ACCEPT     tcp  --  10.8.0.0/16            anywhere            tcp dpt:ssh
DROP       tcp  --  anywhere              anywhere            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@vs758:~#
```

Figura 4 - iptables -L após edição

Através da Figura 5 e da Figura 6 conseguimos constatar que só é possível aceder à solução através da rede do DEI.

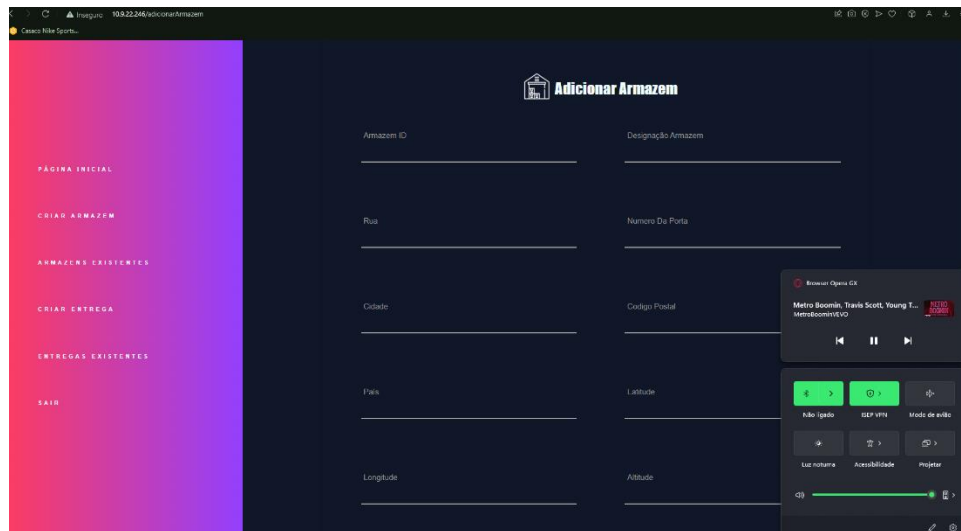


Figura 5

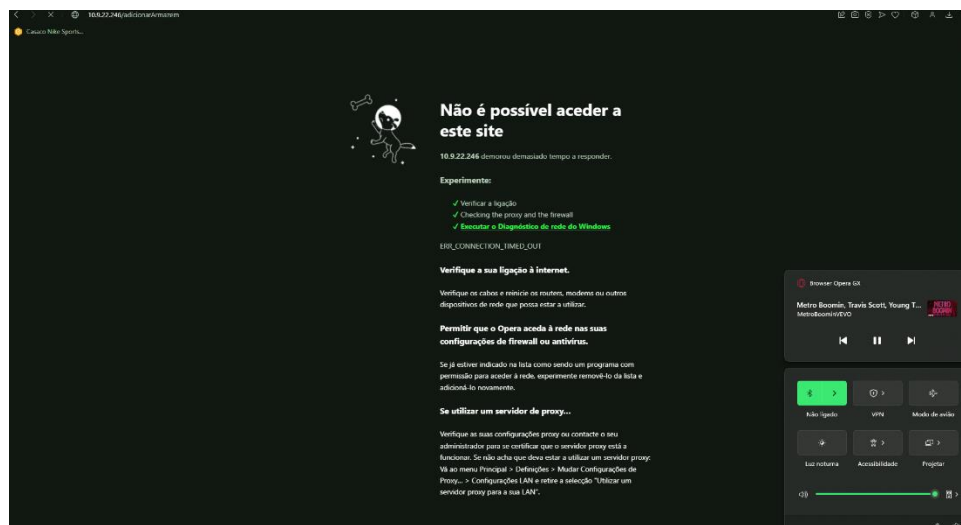


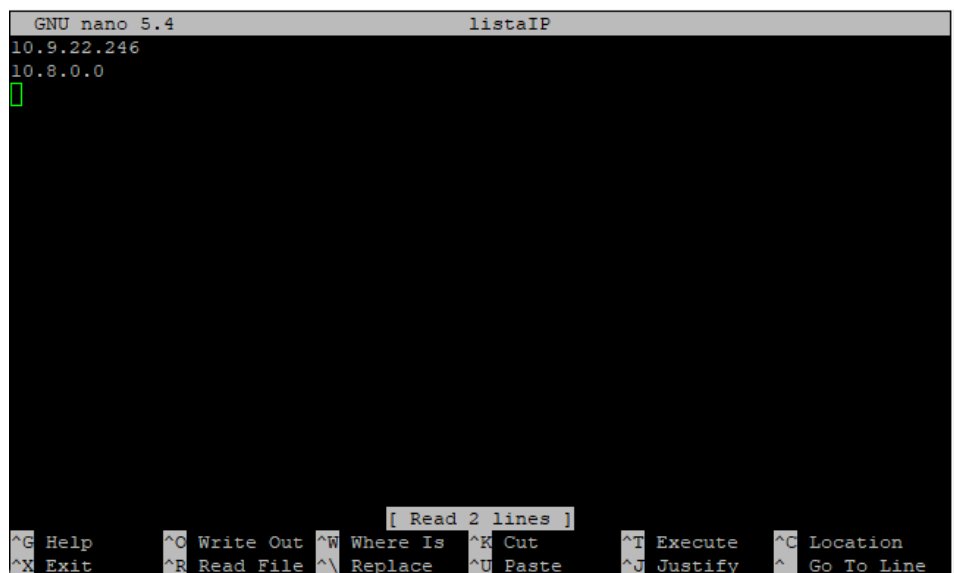
Figura 6

User Story 3

Como administrador do sistema quero que os clientes indicados na user story 2 possam ser definidos pela simples alteração de um ficheiro de texto.

O solicitado para o desenvolvimento desta User Story era que os clientes indicados na US anterior possam ser definidos pela simples alteração de um ficheiro texto.

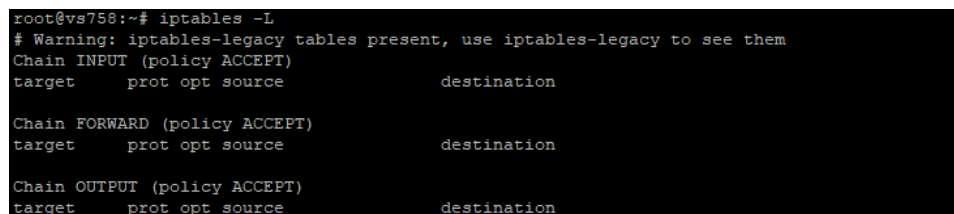
De modo a corresponder ao pedido, começamos com a criação de um ficheiro através do comando **cat > listaIP** onde é adicionado os dois IPs:



```
GNU nano 5.4 listaIP
10.9.22.246
10.8.0.0
[ Read 2 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^I Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

Figura 7 - Lista ip

Como comprovativo que a US3 está operacional, antes da execução dos comandos presentes na Figura 9, efetuamos o reset à vm de modo que o iptables não tivesse qualquer regra:



```
root@vs758:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Figura 8 - iptables -L antes de edição

Podemos então começar a executar a nossa US:

```
root@vs758:~# for IP in $(cat listaIP); do iptables -A INPUT -p tcp --dport 22 -s $IP/16 -j ACCEPT; done
root@vs758:~# sudo /sbin/iptables-save
# Generated by iptables-save v1.8.7 on Sun Dec  4 15:32:26 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 10.9.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.8.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
COMMIT
# Completed on Sun Dec  4 15:32:26 2022
# Generated by iptables-save v1.8.7 on Sun Dec  4 15:32:26 2022
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 2222 -j DNAT --to-destination :22
COMMIT
# Completed on Sun Dec  4 15:32:26 2022
# Warning: iptables-legacy tables present, use iptables-legacy-save to see them
root@vs758:~# iptables -A INPUT -p tcp --dport 22 -j DROP
root@vs758:~# sudo /sbin/iptables-save
# Generated by iptables-save v1.8.7 on Sun Dec  4 15:33:12 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 10.9.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.8.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j DROP
COMMIT
# Completed on Sun Dec  4 15:33:12 2022
# Generated by iptables-save v1.8.7 on Sun Dec  4 15:33:12 2022
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 2222 -j DNAT --to-destination :22
COMMIT
# Completed on Sun Dec  4 15:33:12 2022
# Warning: iptables-legacy tables present, use iptables-legacy-save to see them
```

Figura 9 - Desenvolvimento da US

1. **for IP in \$(cat listaIP); do iptables -A INPUT -p tcp --dport 22-s \$IP/16 -j ACCEPT; done** , permitimos o acesso aos clientes indicados no ficheiro de texto listaIP.
2. **iptables -A INPUT -p tcp --dport 22 -j DROP** , onde é negado o acesso a todas as outras ligações.

Não esquecendo da execução do comando **sudo /sbin/iptables-save** para que as alterações à tabela sejam guardadas

```
root@vs758:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:ssh
ACCEPT     tcp  --  10.9.0.0/16            anywhere             tcp dpt:ssh
ACCEPT     tcp  --  10.8.0.0/16            anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere               anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Figura 10 - iptables -L após edição

Nota:

Inicialmente pensamos que a forma de resolução desta US seria após a edição das iptables na US2, guardarmos as configurações da mesma para um ficheiro de texto, onde posteriormente bastava o comando **iptables-restore < /etc/sysconfig/iptables**, onde para tal criamos a diretoria e salvamos as regras:

```
root@vs758:~# mkdir /etc/sysconfig
root@vs758:~# iptables-save > /etc/sysconfig/iptables
```

Figura 11

```
root@vs758:~# Using username "root".
root@vs758.dei.isep.lpp.pt's password:
Linux vs758 5.4.0-132-generic #148-Ubuntu SMP Mon Oct 17 16:02:06 UTC 2022 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec  4 12:52:04 2022 from 10.8.43.175
root@vs758:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@vs758:~# iptables-restore < /etc/sysconfig/iptables
root@vs758:~# sudo /sbin/iptables-save
# Generated by iptables-save v1.8.7 on Sun Dec  4 12:58:30 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [25:2936]
-A INPUT -s 10.9.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.8.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j DROP
COMMIT
# Completed on Sun Dec  4 12:58:30 2022
# Generated by iptables-save v1.8.7 on Sun Dec  4 12:58:30 2022
*nat
:PREROUTING ACCEPT [6:522]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 2222 -j DNAT --to-destination :22
COMMIT
# Completed on Sun Dec  4 12:58:30 2022
# Warning: iptables-legacy tables present, use iptables-legacy-save to see them
root@vs758:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    tcp  --  10.9.0.0/16            anywhere            tcp dpt:ssh
ACCEPT    tcp  --  10.8.0.0/16            anywhere            tcp dpt:ssh
DROP      tcp  --  anywhere              anywhere            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@vs758:~#
```

Figura 12

Após alguma discussão entre os membros do grupo, concluímos que assim não seríamos capazes de alterar os ips e que esta não seria a resolução idealizada para responder ao pedido da US3.

User Story 4

Como administrador quero identificar e quantificar os riscos envolvidos na solução preconizada.

Módulo	Localização	Serviços Dependentes	Prioridade
MDA	MariaDB Server – DEI Cloud	MDL Planeamento	2
MDL	MongoDB Server – DEI Cloud	Planeamento	2
Visualização	Azure Web Apps	Todos	1

Tabela 1

Avaliação de Riscos

Para uma melhor perceção dos riscos envolvidos na solução preconizada, iremos utilizar uma matriz de risco, que auxilia na identificação de que riscos devem receber mais atenção. A matriz relaciona a probabilidade de acontecimento com o impacto resultante.

	Muito baixo	Baixo	Moderado	Elevado	Muito elevado
Muito provável (90%)					
Provável (70%)				(MDA e MDL) Falha da VM do DEI	
Ocasional (50%)				Falha de segurança Não possuir protocolo HTTPS no MDL e no planeamento	(Visualização) Falha do Azure Web Apps
Improvável (30%)				Falha na conexão à Internet	Ataques à VM do DEI
Muito improvável (10%)				Falha no fornecimento de eletricidade	

Tabela 2 - Matriz de Risco

Fonte: Própria

Tolerável
Indesejável
Intolerável

Tabela 3 - Legenda da Matriz de Risco

Depois de realizada a avaliação de riscos, verificamos que a maior vulnerabilidade é a utilização de VM's do DEI, pois existem múltiplas razões para que exista uma falha. Uma das soluções passaria pela transição para um serviço de Cloud pago, tendo sempre em conta a relação entre qualidade e preço. A falha das VM's do DEI e do Azure Web Apps seria intolerável pois colocaria o sistema inoperacional.

Os ataques às VM's do DEI e não possuir protocolo HTTPS no MDL e no planeamento são também um risco que temos de ter em conta, pois pode tornar o sistema inoperacional, sendo por este motivo intolerável que aconteça.

Como risco indesejável que temos de ter em conta é a falha na conexão à Internet, pois pode impedir a comunicação entre os módulos do sistema desenvolvido, tornando o sistema inoperacional. Já o risco tolerável identificado até ao momento foi a falha no fornecimento de eletricidade, pois é muito improvável de acontecer.

User Story 5

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

O MBCO (Minimum Business Continuity Objective) é, tal como o nome indica, os objetivos de continuidade de negócio mínimos, que serve para especificar o nível de capacidade mínimo aceitável solicitado imediatamente após a recuperação de uma atividade em particular, garantindo o funcionamento do sistema, tendo em consideração os períodos com maior tráfego.

Depois de uma análise sobre o sistema desenvolvido, definimos que existem módulos e componentes que se tornam fulcrais para o bom funcionamento do programa, de forma a garantir que é possível o uso do mesmo com fluidez. Sendo um destes módulos, o SPA, que é o que garante que o programa tem user interface de modo a permitir aos utilizadores utilizarem o programa, tendo um especial foco em criar (camiões, percursos, armazéns e entregas). Para isso, também os módulos MDA, bem como o MDL, tornam-se importantes para garantir que a criação e adição à base de dados é efetuada com sucesso, bem como o planeamento das rotas dos percursos dos camiões para as entregas nos armazéns, etc.

De modo que, módulos como de SGRAI, que permitem ter uma visualização gráfica do programa, tornam-se menos importantes e pouco ou nada têm impacto para o bom funcionamento do sistema, caso haja alguma rutura ou mau funcionamento do módulo.