UserStory 650. – Realizado por António Sousa – 1060694

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

R: Por forma a permitir apenas o acesso à aplicação por parte dos clientes da rede interna, é necessário bloquear todo o acesso ao servidor e permitir apenas a gama de IP's da rede do DEI no porto onde a aplicação corre, que no caso será o porto 4000. Para se efetuar este bloqueio, faremos uso do comando *iptables*, que é uma interface de configuração num sistema de controlo de tráfego integrado no kernel do Linux denomiado d*e Netfilter*.

Comecemos primeiro por definir a política por defeito para *DROP* na cadeia *INPUT*. Isto significa que a ação a tomar quando um pacote de dados provém da rede e se destina ao próprio nó, é descartar o pacote, caso este não corresponda a nenhuma outra regra da cadeia.

Suponhamos que a rede interna do DEI, via cabo ou VPN, atribui a seguinte gama de IP's.

Gama de IP's rede DEI: **192.168.43.0/24**

Porto da aplicação: **4000**

Protocolo da aplicação**: TCP**

1. **# definir a política da cadeia por defeito para DROP**
   iptables -P INPUT DROP

Em seguida, é necessário configurar uma regra que permita a entrada de pacotes para a gama de ip's estabelecida, Porto e Protocolo da aplicação

2. **# definir permissão de entrada para gama, porto e protocolo**
   iptables -A INPUT -s 192.168.43.0/24 -p tcp –dport 4000 -j ACCEPT

Ainda é necessário bloquear todo o acesso não autorizado no porto 4000. Para isso, executamos a seguinte configuração:

3. **# bloquear acesso não autorizado no porto 4000**
   iptables -A INPUT -p tcp –dport 4000 -j DROP

Após a execução dos comandos acima, e por forma a persistir num ficheiro toda a configuração após um *reboot*, é necessário executar o seguinte comando:

4. **# persistir a configuração, inclusive gravar a configuração num ficheiro de texto**
   iptables-save | tee /etc/iptables/rules.v4

No comando acima, fazemos uso do comando 'tee' para ler do standard input e escrever simultaneamente para o standard output e para o ficheiro também, o resultado proveniente do comando iptables-save.

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

Desta forma, é possível voltar a carregar toda a configuração gravada no ficheiro da seguinte forma.

5. **# carregar toda a configuração do iptables a partir de um ficheiro**
   iptables-restore < /etc/iptables/rules.v4

É ainda possível, no caso de se pretender efetuar a configuração para uma outra gama de IP's, alterar diretamente o ficheiro de configuração previamente gravado (/etc/iptables/rules.v4), e executar novamente o comando do passo 5.