**Uma imagem com texto

Descrição gerada automaticamente**

**Sprint B**

**Turma 3DI Professor Responsável**

**1190424-Beatriz Seixas Rui Filipe Marques, RFM**

**1190682- Jéssica Alves**

**1190967-Pedro Santos Unidade Curricular**

**1191460- Tiago Costa ASIST**

**Data de Entrega: 05/12/2020**

**Índice**

**1. Como administrador da infraestrutura quero que o servidor Windows e Linux forneçam endereços IP (na segunda placa de rede) da família 192.168.X.0/24 aos postos clientes, onde X é obtido por 100 + número\_do\_grupo (exemplo, para o grupo 99, X=199).3**

**2. Como administrador da infraestrutura quero que os serviços acima referidos funcionem em failover, com um deles a facultar endereços de 192.168.X.50 a 192.168.X.150 e o outro de 192.168.X.151 a 192.168.X.200**. **7**

**3. Como administrador da infraestrutura quero os servidores Windows e Linux estejam disponíveis apenas para pedidos HTTP e HTTPS. Tal não deve impedir o acesso por SSH ou RDP aos administradores (o grupo). 11**

**4. Como administrador da infraestrutura quero impedir o IP spoofing na minha rede. 13**

**5. Como administrador da infraestrutura quero que os utilizadores registados no Linux com UID entre 6000 e 6500 só consigam aceder via SSH se esse acesso for a partir de uma máquina listada em /etc/remote-hosts.19**

**6. Como administrador da infraestrutura quero que o acesso ao sistema seja inibido aos utilizadores listados em /etc/bad-guys.20**

**7. Como administrador da infraestrutura quero que as mensagens pré-login**

**e pós-login.21**

**8. Como administrador da infraestrutura quero que o servidor Linux responda e envie pedidos ICMP para teste de conectividade apenas e só aos computadores dos elementos do grupo.22**

**1 - Como administrador da infraestrutura quero que o servidor Windows e Linux**

**forneçam endereços IP (na segunda placa de rede) da família 192.168.X.0/24 aos**

**postos clientes, onde X é obtido por 100 + número\_do\_grupo (exemplo, para o**

**grupo 99, X=199); para o efeito devo alterar o endereço dessa placa assignado nas**

**aulas PL.**

O DHCP era necessário para este requisito, sendo assim foi instalado o servidor DHCP do ISC. Para isto foi utilizado o comando ‘sudo apt install isc-dhcp-server’.

De seguida foi configurada a interface secundária com o endereço que nos foi atribuído.

Uma imagem com texto

Descrição gerada automaticamente

De seguida foi configurado o ficheiro ‘/etc/dhcp/dhcpd.conf’ com a subnet da rede que será utilizada, incluindo o range, gateway, Broadcast e máscara.

A range da subnet vai permitir que o servidor DHCP funcione em fail over, conseguindo assim alcançar load balancing entre a máquina Windows e Linux. Estas têm 2 ranges diferentes para que ambas consigam atribuir endereços ip. Assim, no caso de uma das máquinas falhar, a outra pode continuar a atribuir endereços.

Uma imagem com texto

Descrição gerada automaticamente

O ficheiro ‘/etc/default/isc-dhcp-server’ foi também alterado para garantir que o servidor DHCP apenas usa a interface ens33.

Uma imagem com texto

Descrição gerada automaticamente

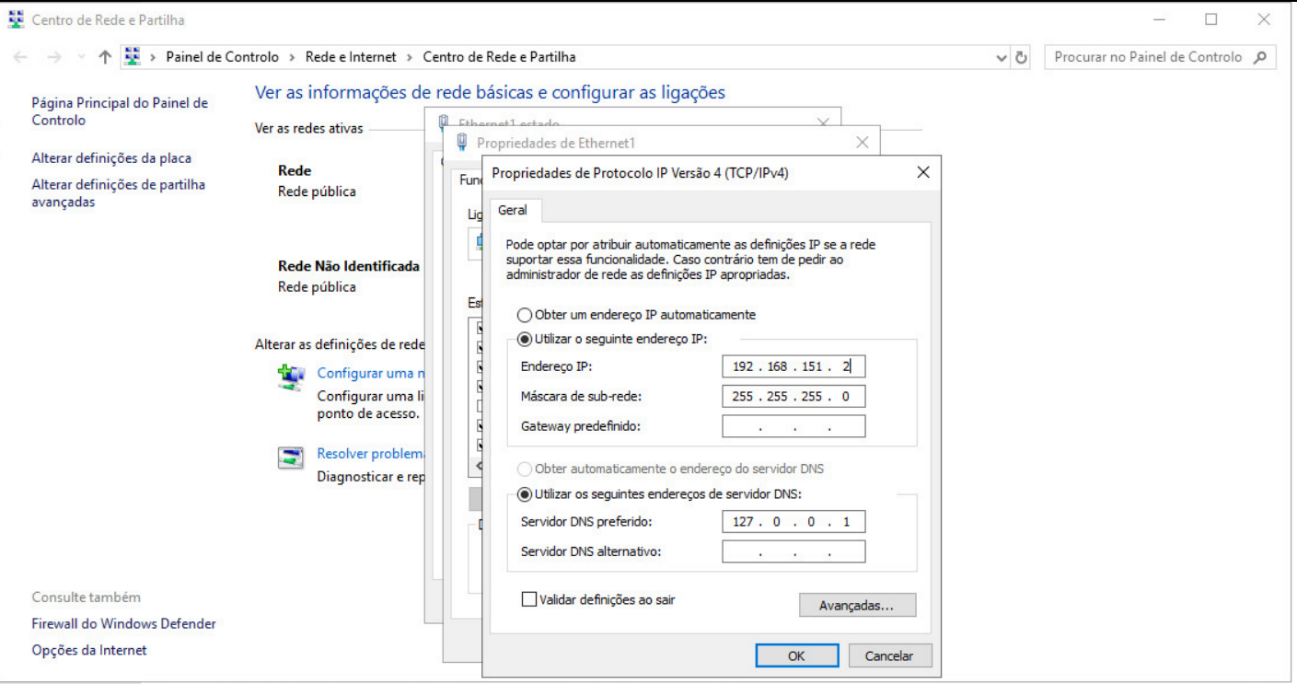
Inicia-se o serviço DHCP a partir do comando ‘sudo service isc-dhcp-server start’.

Em Windows, é necessário instalar a funcionalidade DHCP.

Uma imagem com texto

Descrição gerada automaticamente

De seguida atribuímos o IP estático ‘192.168.151.2’ para a interface de rede Ethernet1.



Por fim, foi efetuada a configuração do servidor DHCP, sendo alterado o range para 192.168.151.151 até 192.168.151.200.

**2. Como administrador da infraestrutura quero que os serviços acima referidos**

**funcionem em failover, com um deles a facultar endereços de 192.168.X.50 a**

**192.168.X.150 e o outro de 192.168.X.151 a 192.168.X.200.**

O DHCP era necessário para este requisito, sendo assim foi instalado o servidor DHCP do ISC. Para isto foi utilizado o comando ‘sudo apt install isc-dhcp-server’.

De seguida foi configurada a interface secundária com o endereço que nos foi atribuído.

Uma imagem com texto

Descrição gerada automaticamente

De seguida foi configurado o ficheiro ‘/etc/dhcp/dhcpd.conf’ com a subnet da rede que será utilizada, incluindo o range, gateway, Broadcast e máscara.

A range da subnet vai permitir que o servidor DHCP funcione em fail over, conseguindo assim alcançar load balancing entre a máquina Windows e Linux. Estas têm 2 ranges diferentes para que ambas consigam atribuir endereços ip. Assim, no caso de uma das máquinas falhar, a outra pode continuar a atribuir endereços.

Uma imagem com texto

Descrição gerada automaticamente

O ficheiro ‘/etc/default/isc-dhcp-server’ foi também alterado para garantir que o servidor DHCP apenas usa a interface ens33.

Uma imagem com texto

Descrição gerada automaticamente

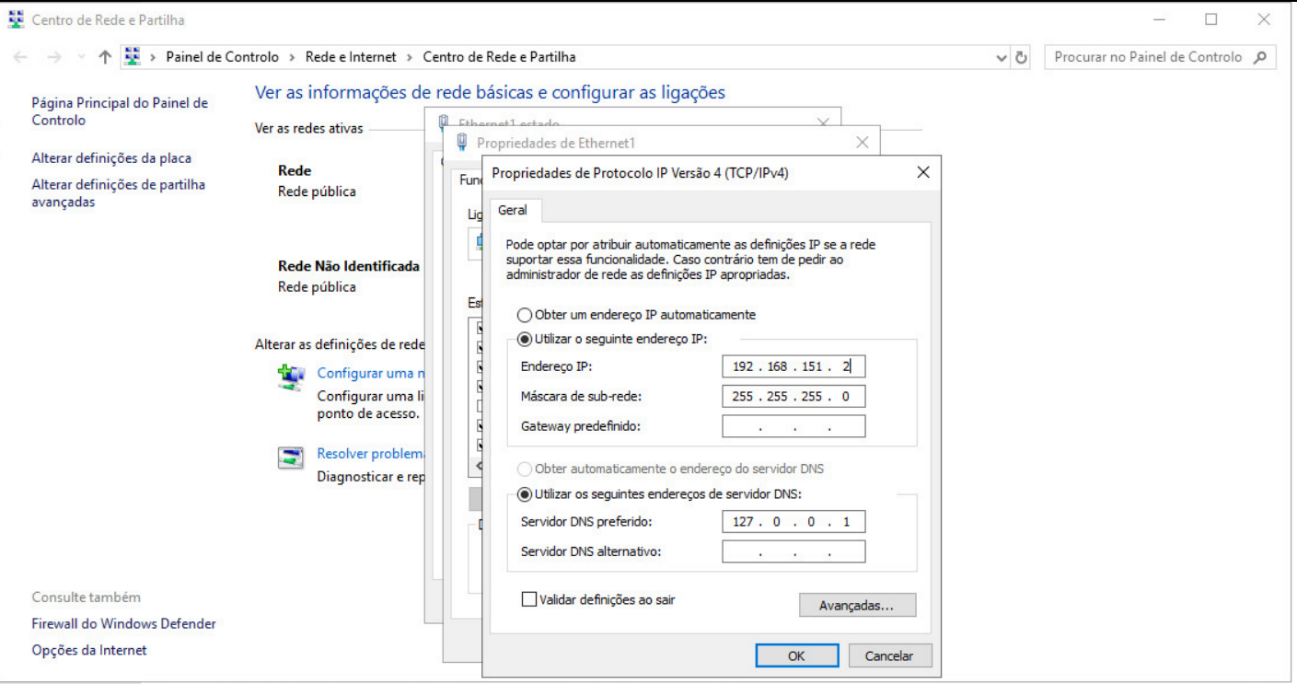
Inicia-se o serviço DHCP a partir do comando ‘sudo service isc-dhcp-server start’.

Em Windows, é necessário instalar a funcionalidade DHCP.

Uma imagem com texto

Descrição gerada automaticamente

De seguida atribuímos o IP estático ‘192.168.151.2’ para a interface de rede Ethernet1.



Por fim, foi efetuada a configuração do servidor DHCP, sendo alterado o range para 192.168.151.151 até 192.168.151.200.

Uma imagem com texto

Descrição gerada automaticamente

**3. Como administrador da infraestrutura quero os servidores Windows e Linux estejam**

**disponíveis apenas para pedidos HTTP e HTTPS. Tal não deve impedir o acesso**

**por SSH ou RDP aos administradores (o grupo).**

**4. Como administrador da infraestrutura quero impedir o IP spoofing na minha rede.**

**5. Como administrador da infraestrutura quero que os utilizadores registados no Linux com UID entre 6000 e 6500 só consigam aceder via SSH se esse acesso for a partir de uma máquina listada em /etc/remote-hosts.**

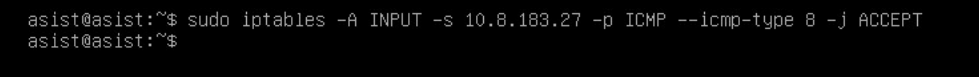
**6. Como administrador da infraestrutura quero que o acesso ao sistema seja inibido aos utilizadores listados em /etc/bad-guys.**

**7. Como administrador da infraestrutura quero que as mensagens pré-login e pós-login.**

**8. Como administrador da infraestrutura quero que o servidor Linux responda e envie pedidos ICMP para teste de conectividade apenas e só aos computadores dos elementos do grupo.**

Começamos por instalar o IpTables executandos os comandos: ‘sudo apt-get update’ e ‘apt-get install iptables’.

Após verificar que o iptables estava no estado vazio inicial, utilizamos o comando ‘iptables -A INPUT -s XX.X.XXX.XXX -p ICMP --icmp-type 8 -j ACCEPT’ para adicionar o endereço ip da máquina atual, onde XXX representa o endereço IP.



Posteriormente foi utilizado o comando ‘iptables -A INPUT -p ICMP –icm-type 8 -j DROP’ para não permitir quaisquer pedidos ICMP do tipo 8 recebidos de outros endereços IP.

Uma imagem com texto

Descrição gerada automaticamente

Para verificar as alterações do IpTables, utilizamos o comando ‘iptables -L -n -v’

Uma imagem com texto

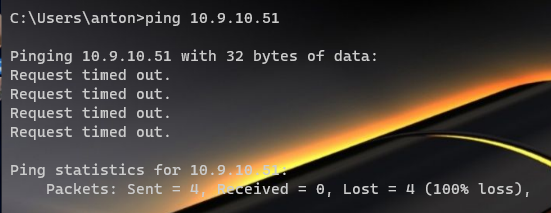
Descrição gerada automaticamente

Para verificar, foi efetuado um teste ping com a máquina cujo servidor continha o endereço IP.

Uma imagem com texto

Descrição gerada automaticamente

Após, outro teste com uma máquina cujo servidor não continha o endereço IP.



**IDs do Grupo\_051:**