

ASIST

2019-2020

RELATÓRIO

SPRINT 1

Carlos Moreira – 1161882

José Pedro Oliveira – 1161842

Marco Pinheiro – 1170483

Pedro Barbosa – 1150486

Pedro Mendes – 1161871

Índice

[User stories 3](#_Toc24631321)

[Resolução 4](#_Toc24631322)

[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). 4](#_Toc24631323)

[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. 5](#_Toc24631324)

[a. Linux 5](#_Toc24631325)

[b. Windows 5](#_Toc24631326)

[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). 6](#_Toc24631327)

[a. Linux 6](#_Toc24631328)

[a. Windows 7](#_Toc24631329)

[4. Como administrador da infraestrutura quero impedir o IP spoofing na minha rede. 9](#_Toc24631330)

[a. Linux 9](#_Toc24631331)

[b. Windows 10](#_Toc24631332)

[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. 11](#_Toc24631333)

[6. Como administrador da infraestrutura quero que o acesso ao sistema seja inibido aos utilizadores listados em /etc/bad-guys. 11](#_Toc24631334)

[7. Como administrador da infraestrutura quero que as mensagens pré-login e pós-login bem sucedido sejam dinâmicas (por exemplo, “[Bom dia] | [Boa tarde] username”, etc.). 12](#_Toc24631335)

[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 13](#_Toc24631336)

# User stories

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).

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.

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 bem sucedido sejam dinâmicas (por exemplo, “[Bom dia] | [Boa tarde] username”, etc.).

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

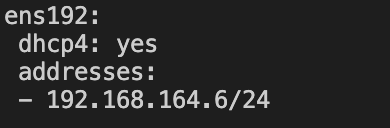
# Resolução

## 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).

* 1. Linux

sudo nano /etc/netplan/50-cloud-init.yaml

Adicionar as seguintes configurações:

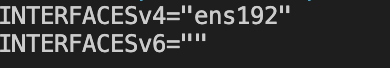


sudo netplan try

sudo netplan apply

sudo nano /etc/default/isc-dhcp-server

Adicionar as seguintes configurações:

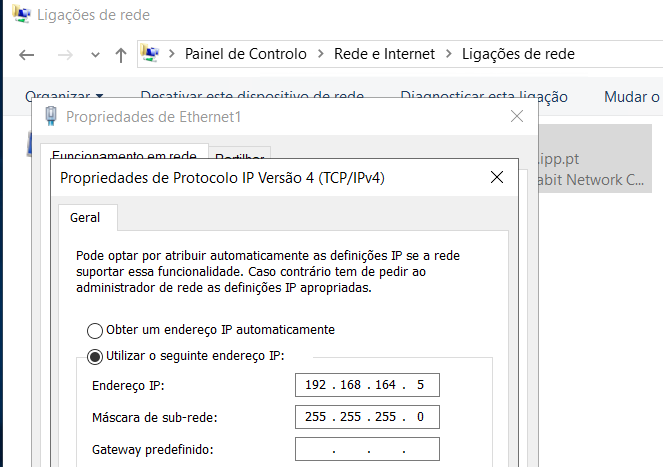


sudo service isc-dhcp-server start

* 1. Windows

Painel de Controlo\Rede e Internet\Ligações de rede

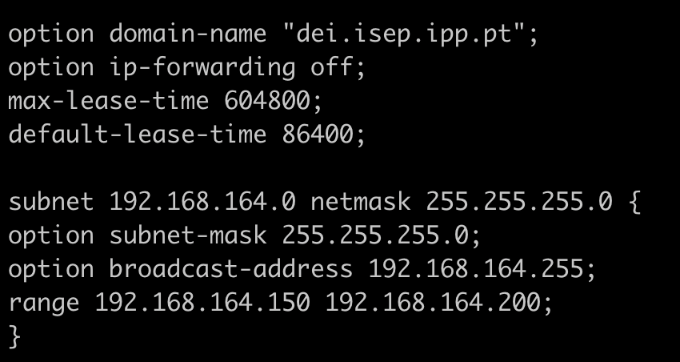
Adicionar as seguintes configurações à 2ª placa de rede (Ethernet1)



## 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.

### Linux

sudo nano -w /etc/dhcp/dhcpd.conf

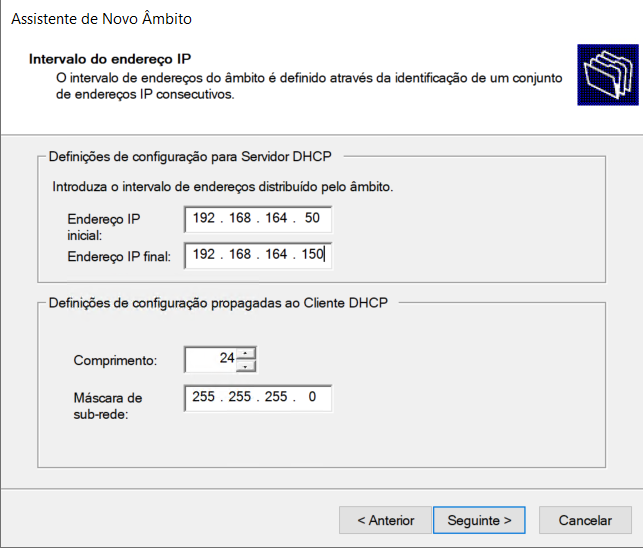


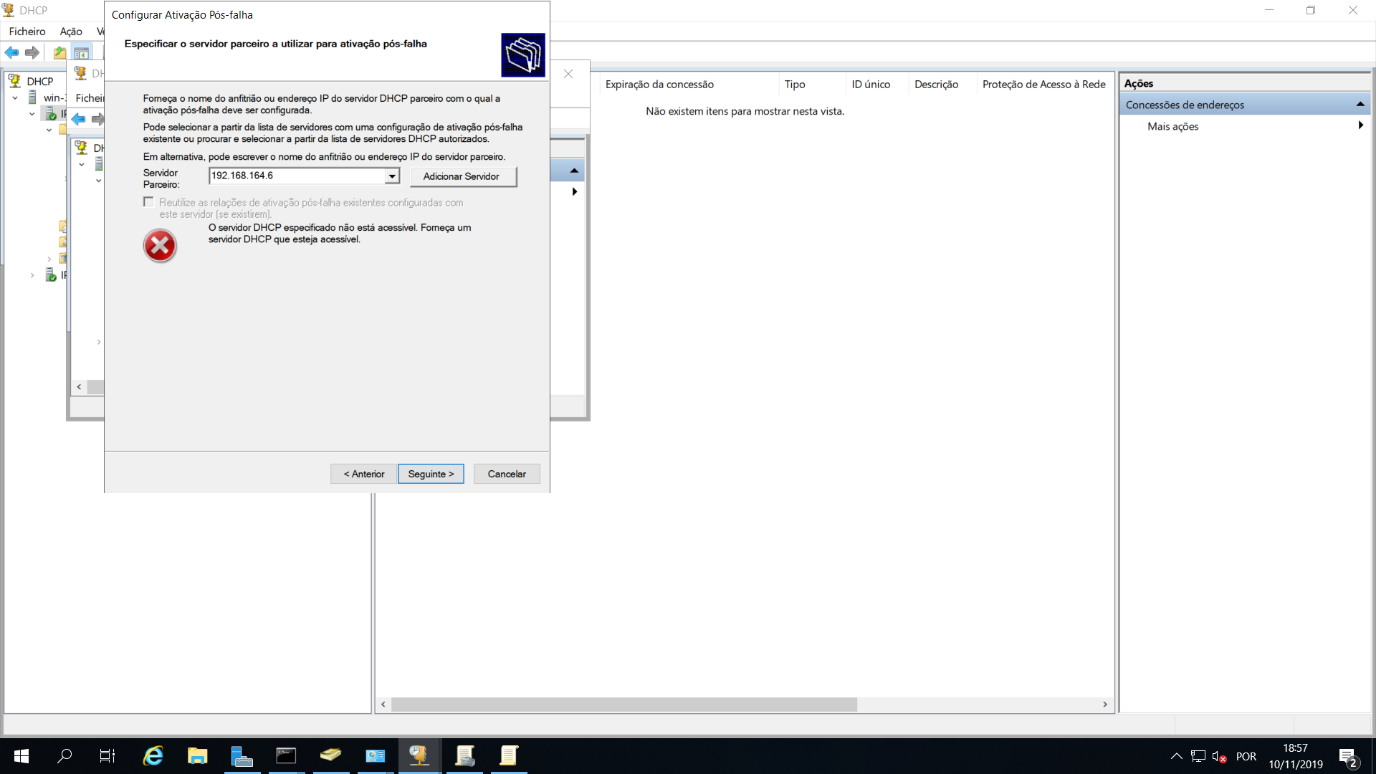
sudo systemctl restart isc-dhcp-server.service

### Windows

Para que os serviços funcionem em failover foi instalado um servidor dhcp, cujo ip é 192.168.164.5. Nesse servidor dhcp foi criado um âmbito cujo intervalo de ips é de 192.168.164.50 a 192.168.164.150.

Após configuração do ambito, tentamos configurar o failover, porém não é possivel essa configuração entre maquinas Windows e Linux, dado que têm configurações distintas para os âmbitos.





## 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).

### Linux

Criação de iptable com o nome chain-states:

sudo iptables -N chain-states

sudo iptables -A chain-states -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A chain-states -p udp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A chain-states -p icmp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A chain-states -j RETURN

Criação de iptable com o nome sprint\_b\_input\_chain:

sudo iptables -N sprint\_b\_input\_chain

Definição da iptable sprint\_b\_input\_chain para aceitar ligações HTTP (porta 80) através de protocolo TCP e UDP com o estado New e Established

sudo iptables -A sprint\_b\_input\_chain -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

sudo iptables -A sprint\_b\_input\_chain -p udp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

Definição da iptable sprint\_b\_input\_chain para aceitar ligações HTTPS (porta 443) através de protocolo TCP e UDP com o estado New e Established

sudo iptables -A sprint\_b\_input\_chain -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

sudo iptables -A sprint\_b\_input\_chain -p udp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

Definição da iptable sprint\_b\_input\_chain para aceitar ligações SSH (porta 22) através de protocolo TCP e UDP com o estado New e Established e negação de todas as outras ligações.

sudo iptables -A sprint\_b\_input\_chain -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

sudo iptables -A sprint\_b\_input\_chain -p udp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

sudo iptables -A sprint\_b\_input\_chain -j DROP

Criação de iptable com o nome sprint\_b\_output\_chain:

sudo iptables -N sprint\_b\_output\_chain

Definição da iptable sprint\_b\_output\_chain para aceitar ligações HTTP (porta 80) através de protocolo TCP e UDP com o estado New e Established. Estas ligações irão ser de saída.

sudo iptables -A sprint\_b\_output\_chain -p tcp --sport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

sudo iptables -A sprint\_b\_output\_chain -p udp --sport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

Definição da iptable sprint\_b\_output\_chain para aceitar ligações HTTPS (porta 443) através de protocolo TCP e UDP com o estado New e Established. Estas ligações irão ser de saída.

sudo iptables -A sprint\_b\_output\_chain -p tcp --sport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

sudo iptables -A sprint\_b\_output\_chain -p udp --sport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

Definição da iptable sprint\_b\_output\_chain para aceitar ligações SSH (porta 22) através de protocolo TCP e UDP com o estado New e Established. Estas ligações irão ser de saída mas apenas para elementos pertencentes ao grupo 1000, ou seja dos administradores. Todas as outras ligações de saída irão ser negadas.

sudo iptables -A sprint\_b\_output\_chain -p tcp --sport 22 -m owner --gid-owner 1000 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

sudo iptables -A sprint\_b\_output\_chain -p udp --sport 22 -m owner --gid-owner 1000 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

sudo iptables -A sprint\_b\_output\_chain -p tcp --sport 22 -m conntrack --ctstate NEW -j DROP

sudo iptables -A sprint\_b\_output\_chain -p udp --sport 22 -m conntrack --ctstate NEW -j DROP

Atribuição de iptables de entrada (INPUT) e saida (OUTPUT) de todas as chains criadas.

sudo iptables -A INPUT -j chain-states

sudo iptables -A OUTPUT -j chain-states

sudo iptables -A INPUT -j sprint\_b\_input\_chain

sudo iptables -A OUTPUT -j sprint\_b\_output\_chain

Todas as restantes configurações serão negadas.

sudo iptables -P INPUT DROP

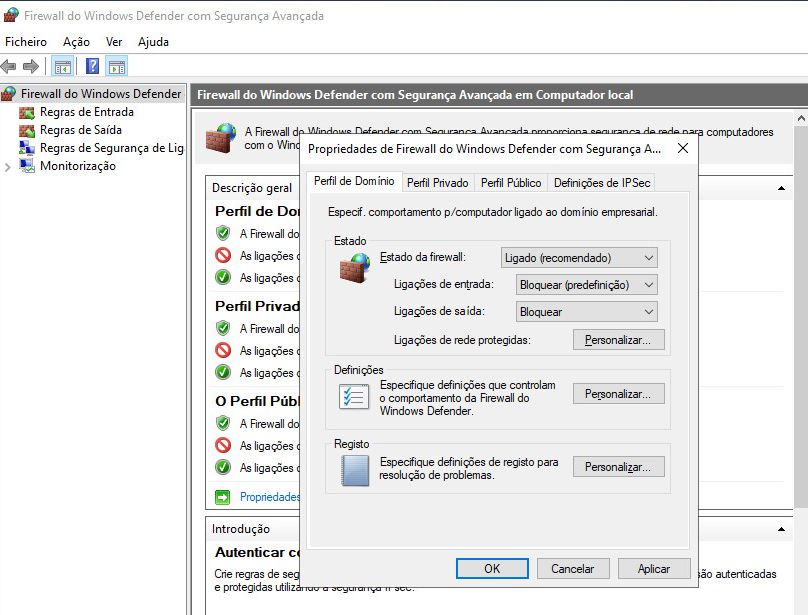
sudo iptables -P OUTPUT DROP

Relativamente às configurações SSH consideramos uma alternativa que nos pareceu mais simples. No ficheiro “/etc/ssh/sshd\_config” adicionar o comando:

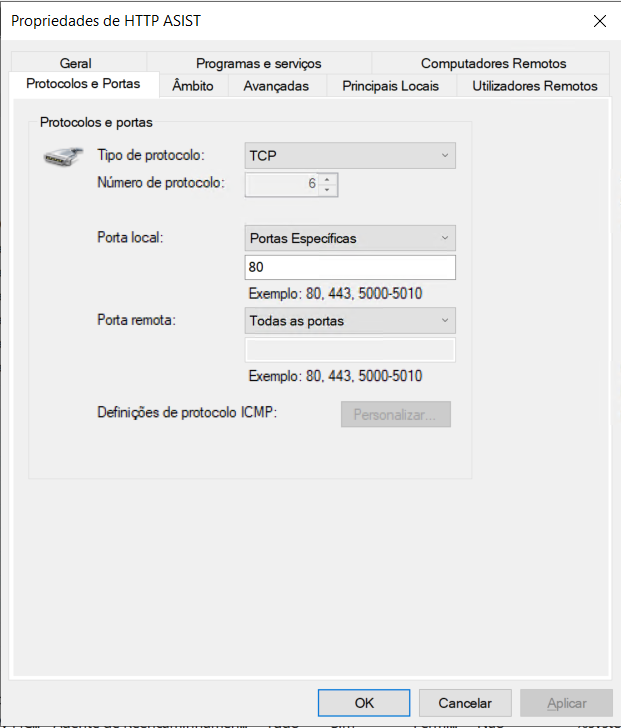
AllowGroups adm

### Windows

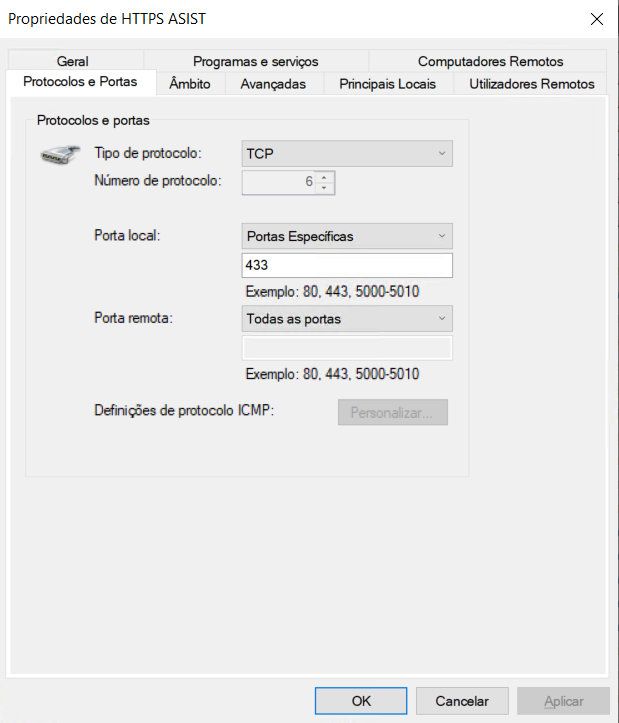
Para que a maquina esteja disponivel apenas para pedidos HTTP e HTTPS foi bloqueada a entrada e saida de todos os outros pedidos.



Para que estejam disponiveis pedidos em HTTP foi criada uma regra de entrada, abrindo a porta 80:

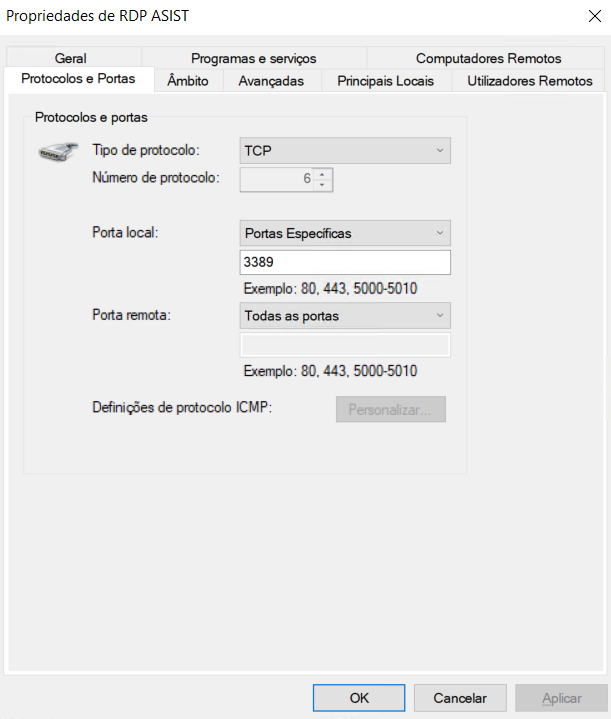


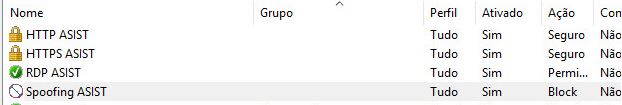
Para que estejam disponiveis pedidos em HTTPS foi criada uma regra de entrada, abrindo a porta 443:



Para que o acesso por RDP seja permitido aos administradores foi criada uma regra especificando a porta 3389.

**Nota:** Por definição esta regra já está configurada, no entanto, para melhor demonstração, foi criada de qualquer forma.





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

### Linux

A seguinte regra de iptable define que irão ser negados todos os endereços do range 10.9.\*.\* que não são provenientes da interface ens160:

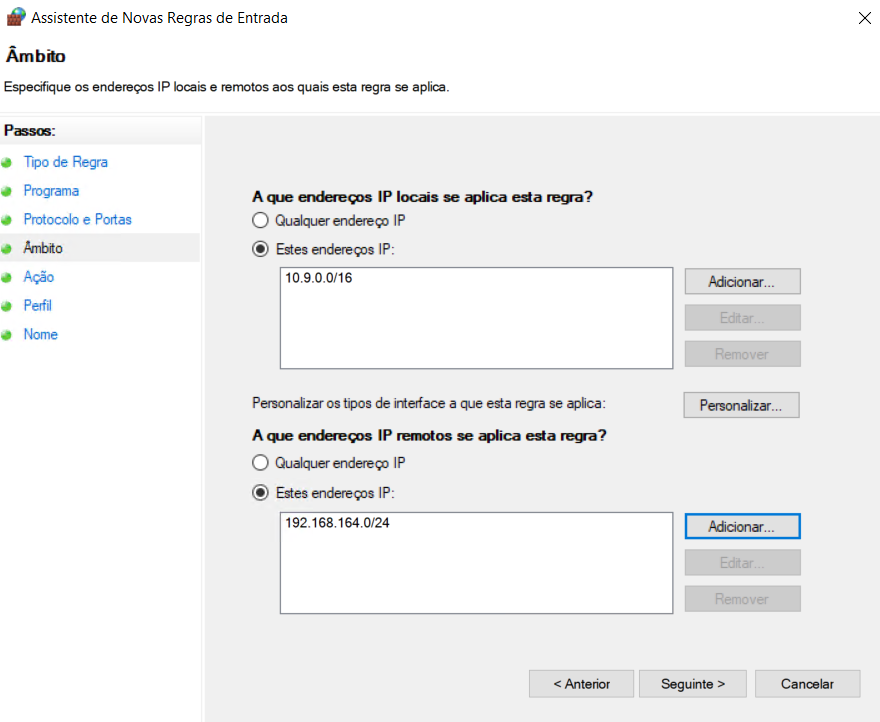
iptables -A INPUT -s 10.9.0.0/16 -i ! ens160 -j DROP

A seguinte regra de iptable regra diz para bloquear todos os endereços que não sejam 10.9.\*.\* vindos da interface ens160:

iptables -A INPUT ! -s 10.9.0.0/16 -i ens160 -j DROP

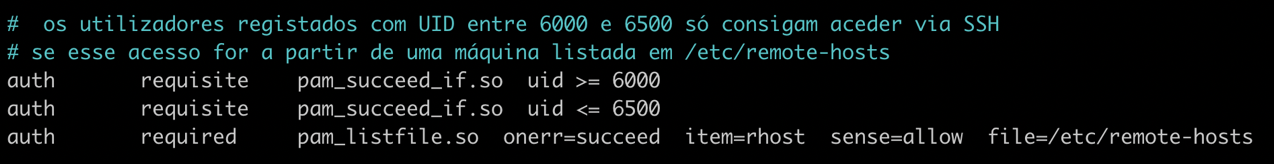
### Windows

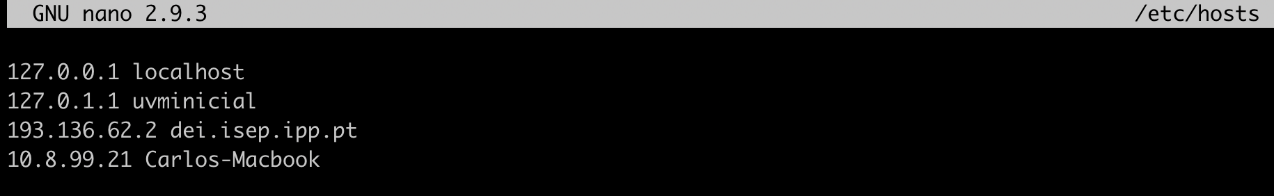
Para impedir o ip spoofing criou-se uma regra de entrada na firewall, especificando a gama de ips a qual se aplica a regra. O tipo de regra utilizada foi Personalizada de forma a ser especificada para qualquer tipo de protocolo.



## 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.

Adicionar ao ficheiro “/etc/pam.d/sshd” as linhas que irão definir o range de users permitidos e também apontar para o ficheiro “/etc/remote-hosts” de forma a verificar se se trata de um host permitido.



Criação de alias no ficheiro /etc/hosts

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

Nos ficheiros /etc/pam.d/login e /etc/pad.d/sshd necessário adicionar a linha seguinte, por forma a negar autenticação aos users que estejam no ficheiro bad-guys:

auth required pam\_listfile.so onerr=succeed item=user sense=deny file=/etc/bad-guys

Adicionar permissões ao ficheiro: chmod 600 /etc/bad-guys

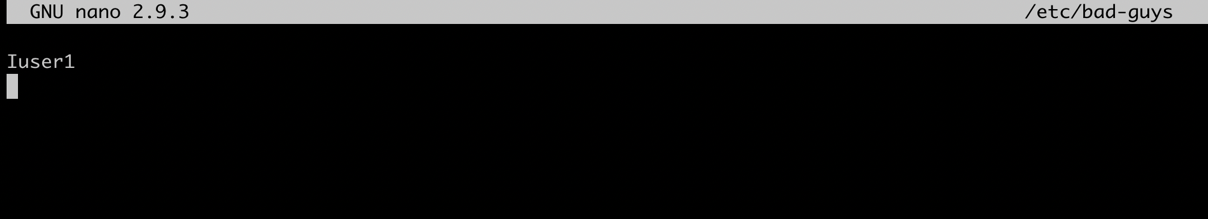


Figure 1 Configuração de ficheiro bad-guys

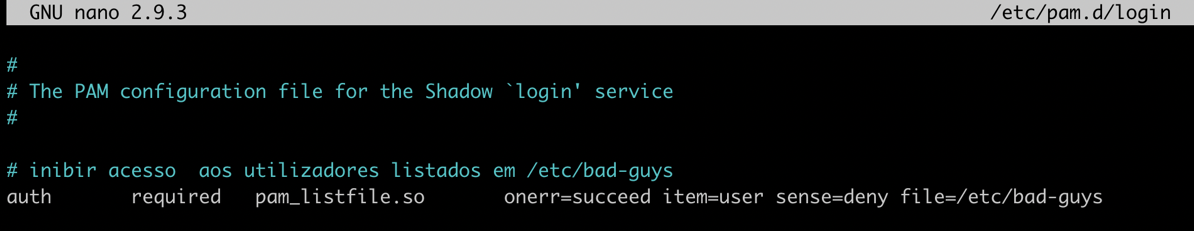


Figure 2 Configuração de ficheiro pam.d/login

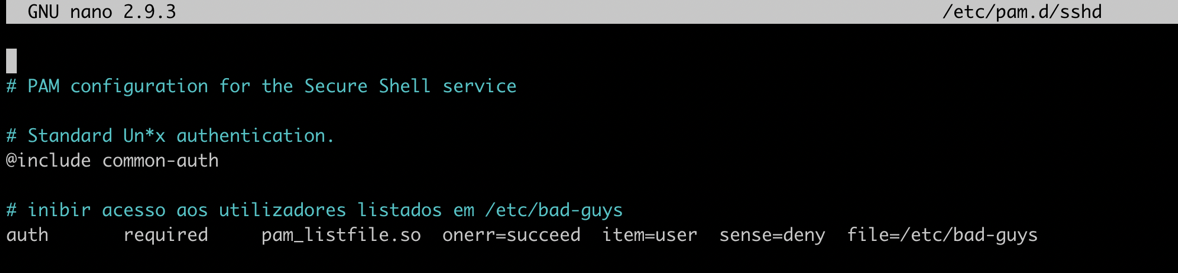


Figure 3 Configuração de ficheiro pam.d/sshd

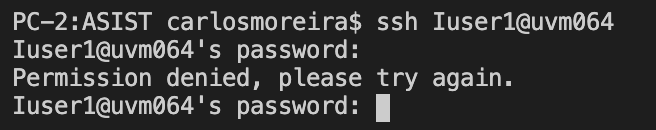


Figure 4 Exemplo de tentativa sem sucesso de login com user bloqueado



Figure 5 Consulta do ficheiro log auth.log

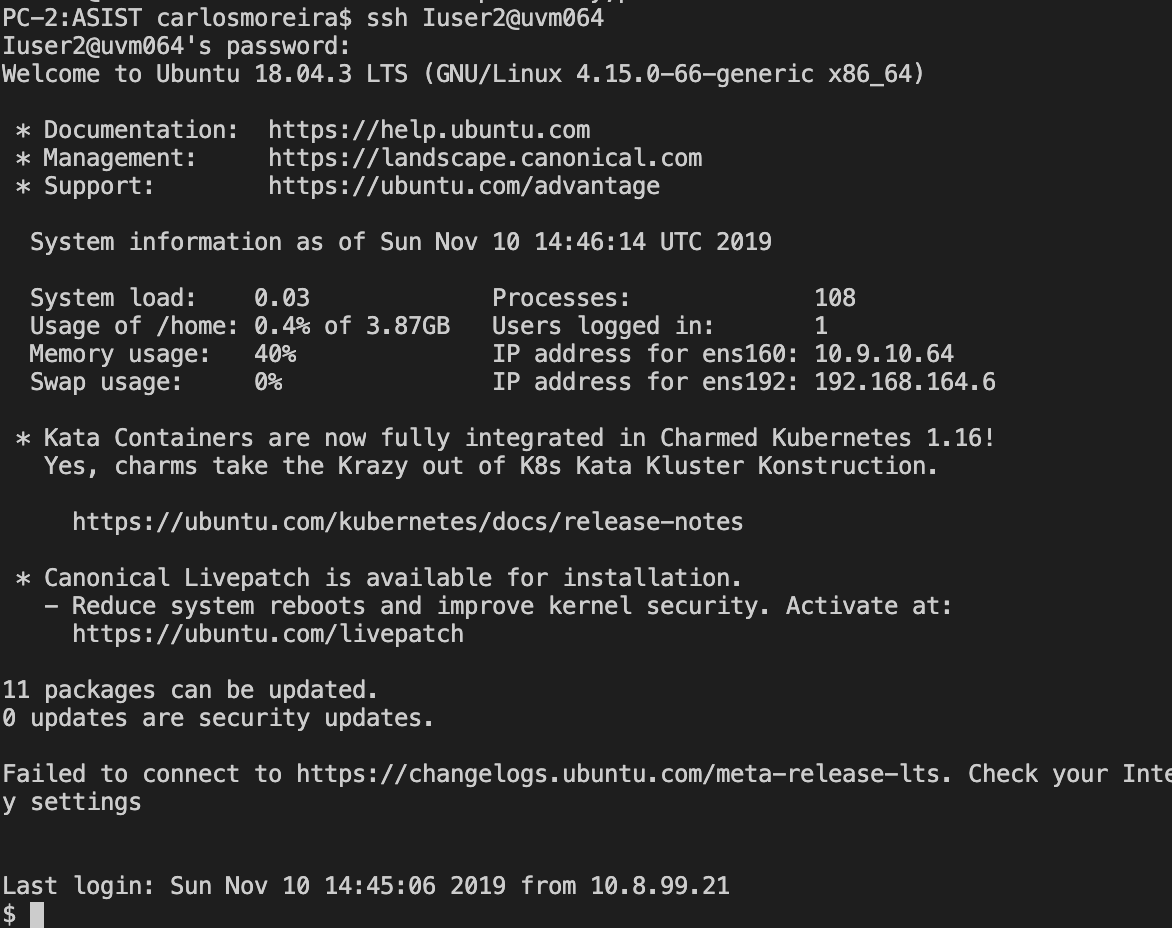


Figure 6 Exemplo de tentativa com sucesso de login com user permitido

## Como administrador da infraestrutura quero que as mensagens pré-login e pós-login bem sucedido sejam dinâmicas (por exemplo, “[Bom dia] | [Boa tarde] username”, etc.).

Adicionar a mensagem “Bem-Vindo a ASIST 2019/2020” no ficheiro /etc/issue:

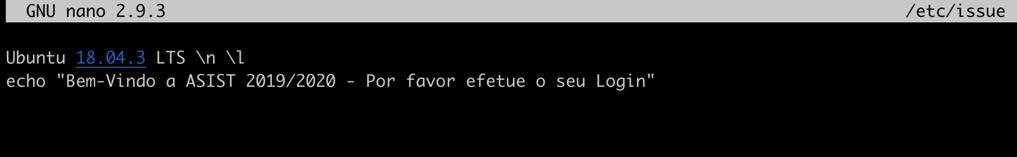
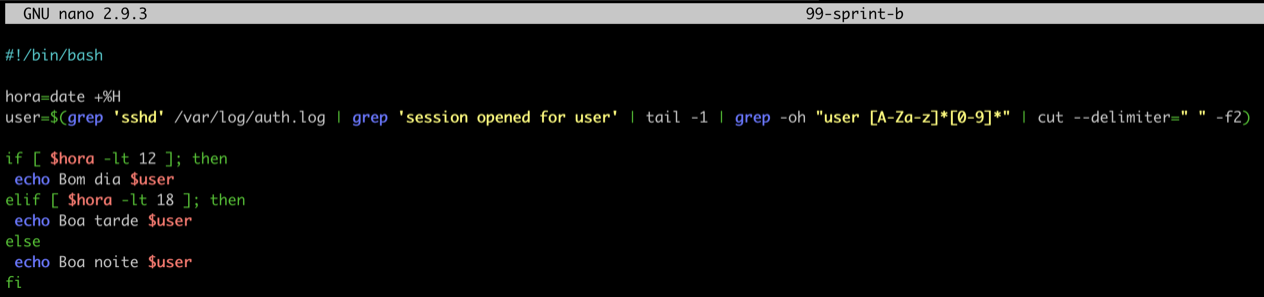




Figure 7 Mensagem de pré-login

Criação de um novo ficheiro na pasta “/etc/update-motd.d” com o nome “99-sprint-b”:



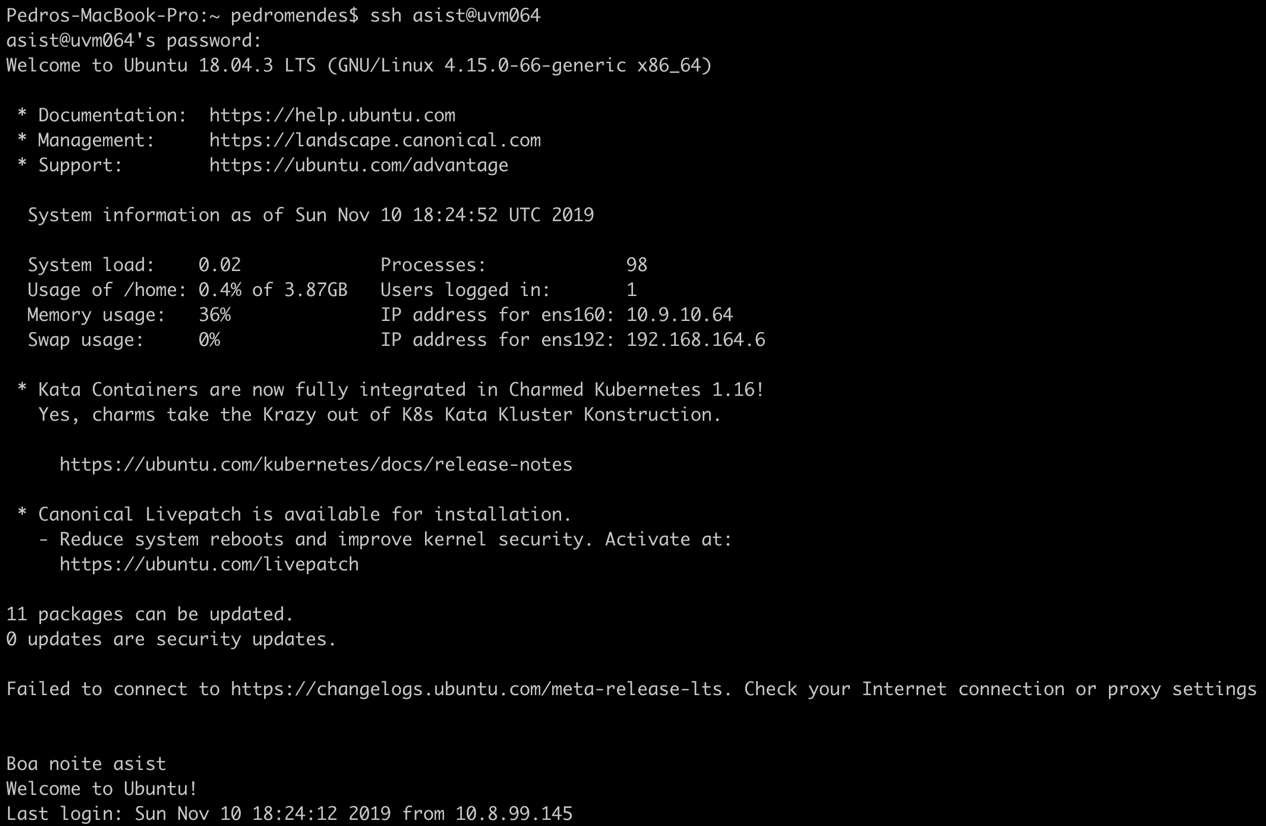


Figure 8 Exemplo de mensagem dinámica de login

## 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

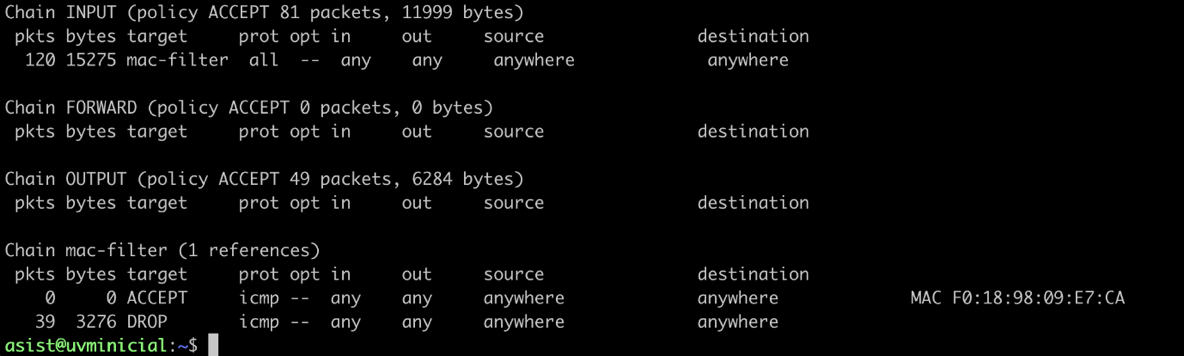
Adicionada linha as definições das iptables, onde se negam todos os pedidos icmp á excepção do mac address definido:

sudo iptables -N mac-filter

sudo iptables -A mac-filter -p icmp -m mac --mac-source F0:18:98:09:E7:CA -j ACCEPT

sudo iptables -A mac-filter -p icmp -m mac all -j DROP

sudo iptables -A INPUT -j mac-filter



Uma outra forma de configuração seria por IP, no entanto seria necessário configurar ips estáticos nas máquinas configuradas:

sudo iptables -I INPUT -p icmp -s ! 192.168.164.27 -j REJECT