

## **Sprint 1 (Sprint B)**

**ASIST**

### **Turma 3DJ \_ Grupo 57**

1190903 \_ Miguel Gonçalves

1191018 \_ Rúben Rodrigues

1191042 \_ Rui Pinto

1191106 \_ Tomás Limbado

**Data: 5/12/2021**

## Índice

US1 .....	3
US2 .....	5
US3 .....	8
US4 .....	13
US5 .....	23
US6 .....	25
US7 .....	26
US8 .....	28

## US1

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

Linux:

Para a concretização deste requisito efetuou-se nano /etc/network/interfaces e alterou-se esse ficheiro conforme a imagem

```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens32
#allow-hotplug ens32
iface ens32 inet static
address 10.9.10.57
netmask 255.255.0.0
gateway 10.9.0.1
dns-nameservers 192.168.62.32 192.168.62.8

# This is an autoconfigured IPv6 interface
iface ens32 inet6 static
address fd1e:2bae:c6fd:1009::a:39
netmask 64
gateway fd1e:2bae:c6fd:1009::1
dns-nameservers fd1e:2bae:c6fd:62::32 fd1e:2bae:c6fd:62::8

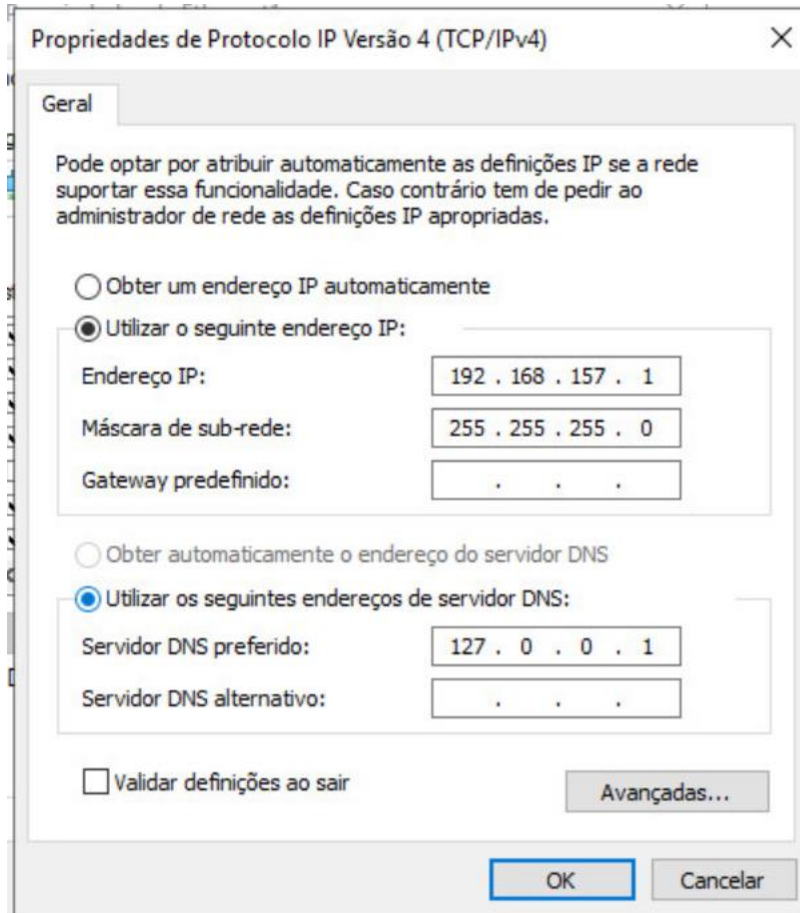
auto ens33
iface ens33 inet static
address 192.168.157.2
netmask 255.255.255.0
```

[ 31 linhas lidas ]

<b>^G</b> Ajuda	<b>^O</b> Gravar	<b>^W</b> Procurar	<b>^K</b> Cortar	<b>^T</b> Executar	<b>^C</b> Localização	<b>^M-U</b> Desfazer
<b>^X</b> Sair	<b>^R</b> Carregar	<b>^N</b> Substituir	<b>^U</b> Colar	<b>^J</b> Justificar	<b>^_</b> Ir p/ linha	<b>^M-E</b> Refazer

Windows:

Para a concretização deste requisito alterou-se o IP estático da segunda placa de rede tal como é possível verificar na imagem



## US2

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:

Para a realização deste requisito foi necessário utilizar DHCP, sendo assim foi instalado o servidor DHCP do ISC

```
root@asist:~# apt install isc-dhcp-server_
```

De seguida, é necessário também configurar o ficheiro /etc/dhcp/dhcpd.conf, para conter a subnet da rede que vamos utilizar, e de seguida especificar o range, a gateway (routers) e a sua máscara.

```
subnet 192.168.157.0 netmask 255.255.255.0 {  
    option subnet-mask 255.255.255.0;  
    range 192.168.157.151 192.168.157.200;  
    option routers 192.168.157.1;  
}
```

Garante-se também que o servidor DHCP apenas usa a interface ens33

nano /etc/default/isc-dhcp-server

```
GNU nano 5.4 /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""
```

Por fim inicia-se o servidor DHCP

```
root@asist:~# service isc-dhcp-server start
```

Windows:

Inicialmente é criado um servidor DHCP. Posteriormente é criado um âmbito de modo funcionar em failover utilizando o range de endereços solicitado

Assistente de Novo Âmbito

**Intervalo do endereço IP**

O intervalo de endereços do âmbito é definido através da identificação de um conjunto de endereços IP consecutivos.

Definições de configuração para Servidor DHCP

Introduza o intervalo de endereços distribuído pelo âmbito.

Endereço IP inicial: 192 . 168 . 157 . 50

Endereço IP final: 192 . 168 . 157 . 150

Definições de configuração propagadas ao Cliente DHCP

Comprimento: 24

Máscara de sub-rede: 255 . 255 . 255 . 0

< Anterior Seguinte > Cancelar

## US3

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:

De modo a permitir a solicitação no requisito foi efetuado

```
root@asist:~# apt install iptables-persistent
```

Criou-se um ficheiro com as seguintes regras

```
root@asist:~# nano /etc/init.d/rules.sh
```

```
GNU nano 5.4 /etc/init.d/rules.sh * M
#!/bin/bash
iptables -P INPUT DROP
iptables -F INPUT

iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT #http
iptables -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT #https
```

```
root@asist:~# cd /etc/init.d
root@asist:/etc/init.d# chmod +x rules.sh
root@asist:/etc/init.d# ./rules.sh
```

Foi ainda verificado que as regras tinham sido aplicadas

```
root@asist:/etc/init.d# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            tcp dpt:http ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:https ctstate NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

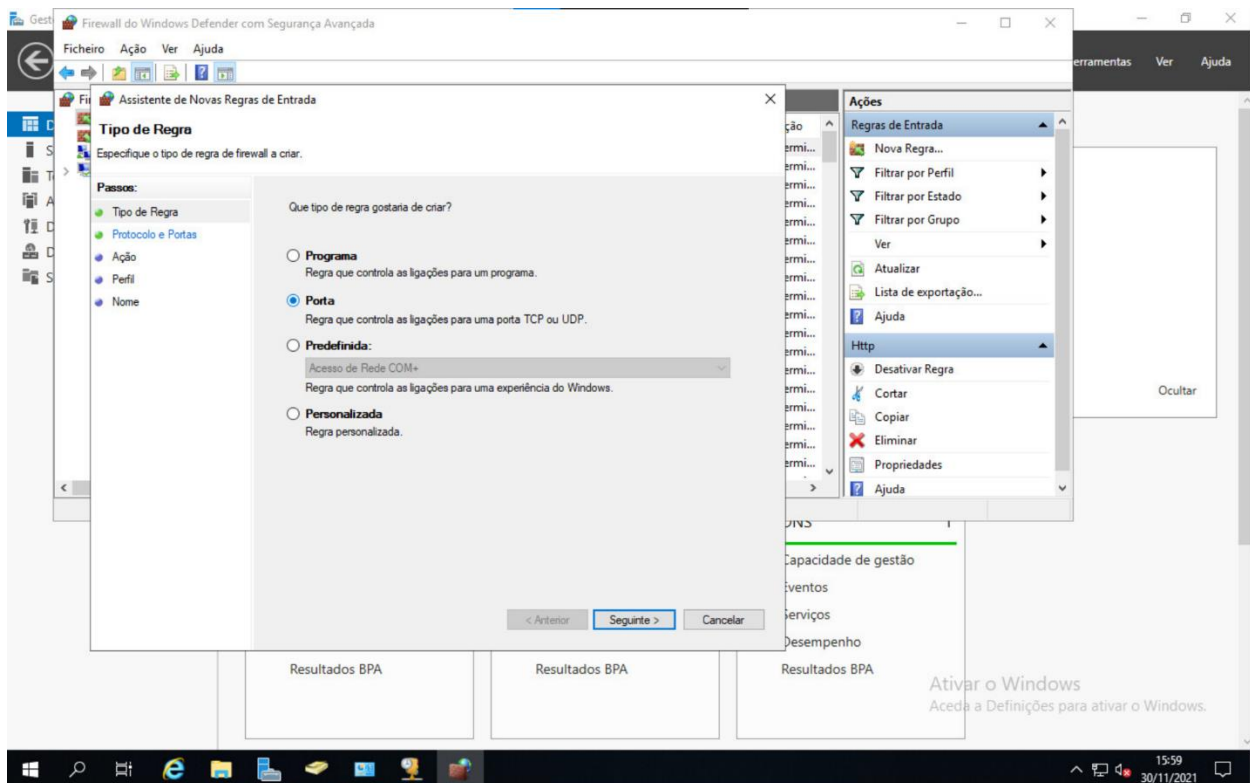
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

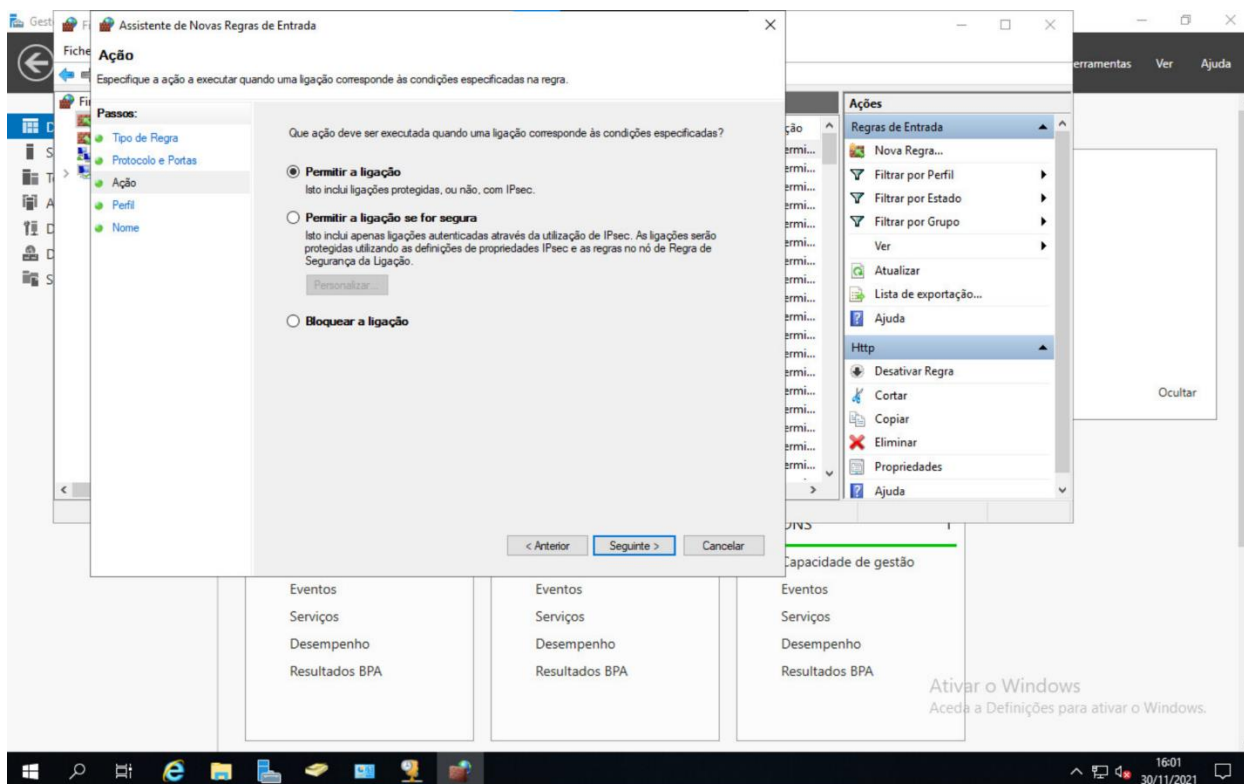
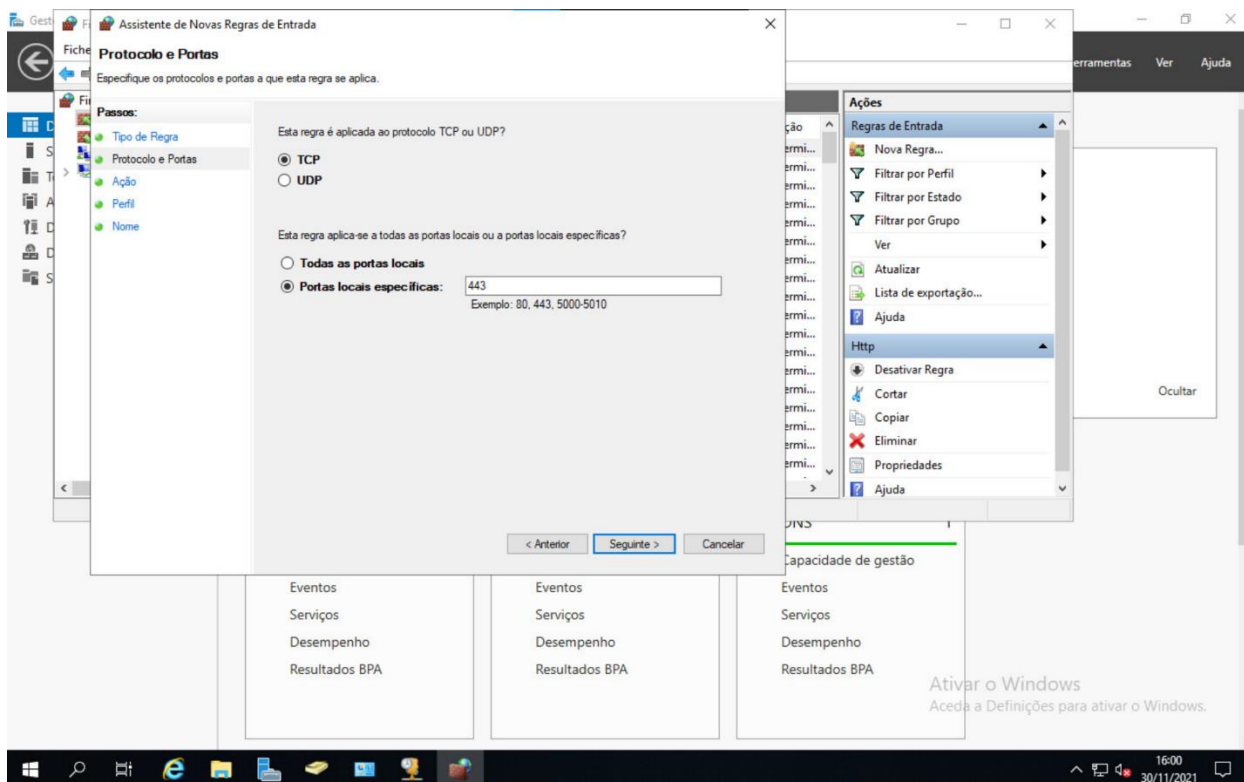
Como é possível verificar a policy para pedidos outbound é ACCEPT, logo não foi necessário criar regras para estes pedidos.

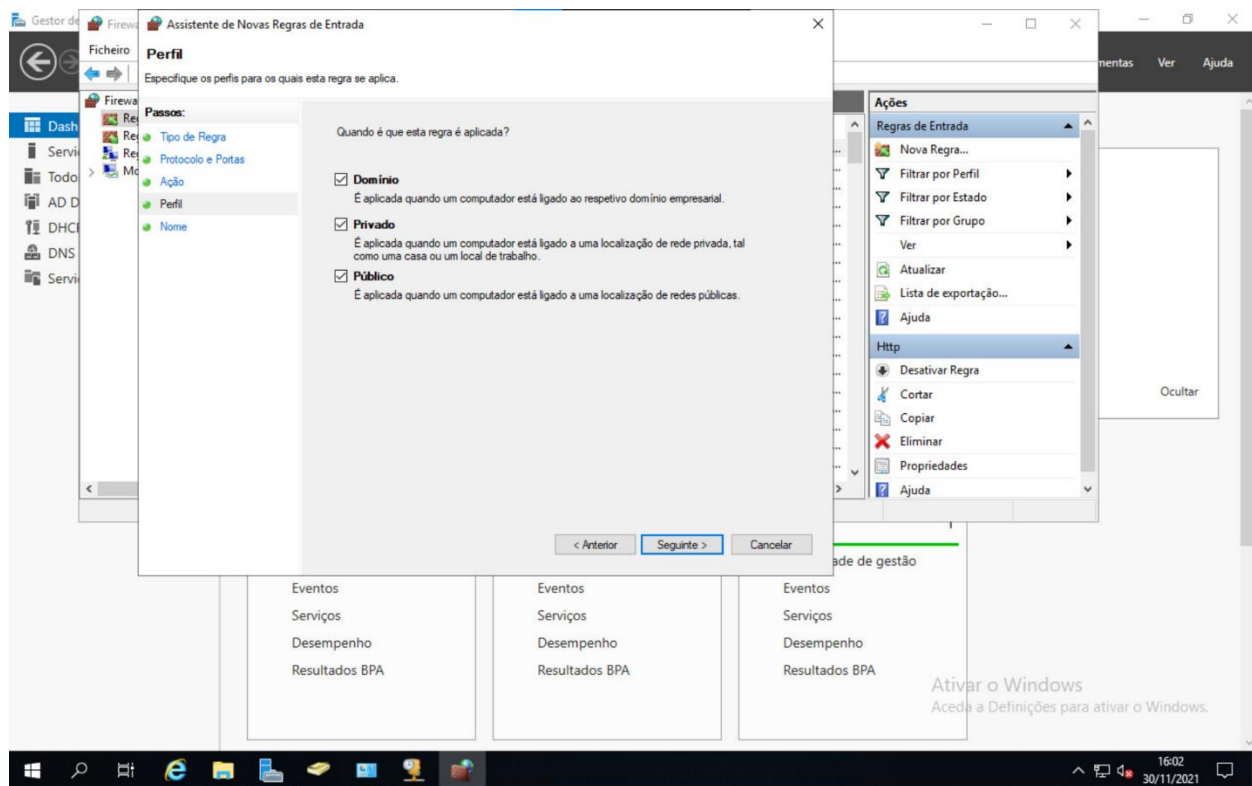


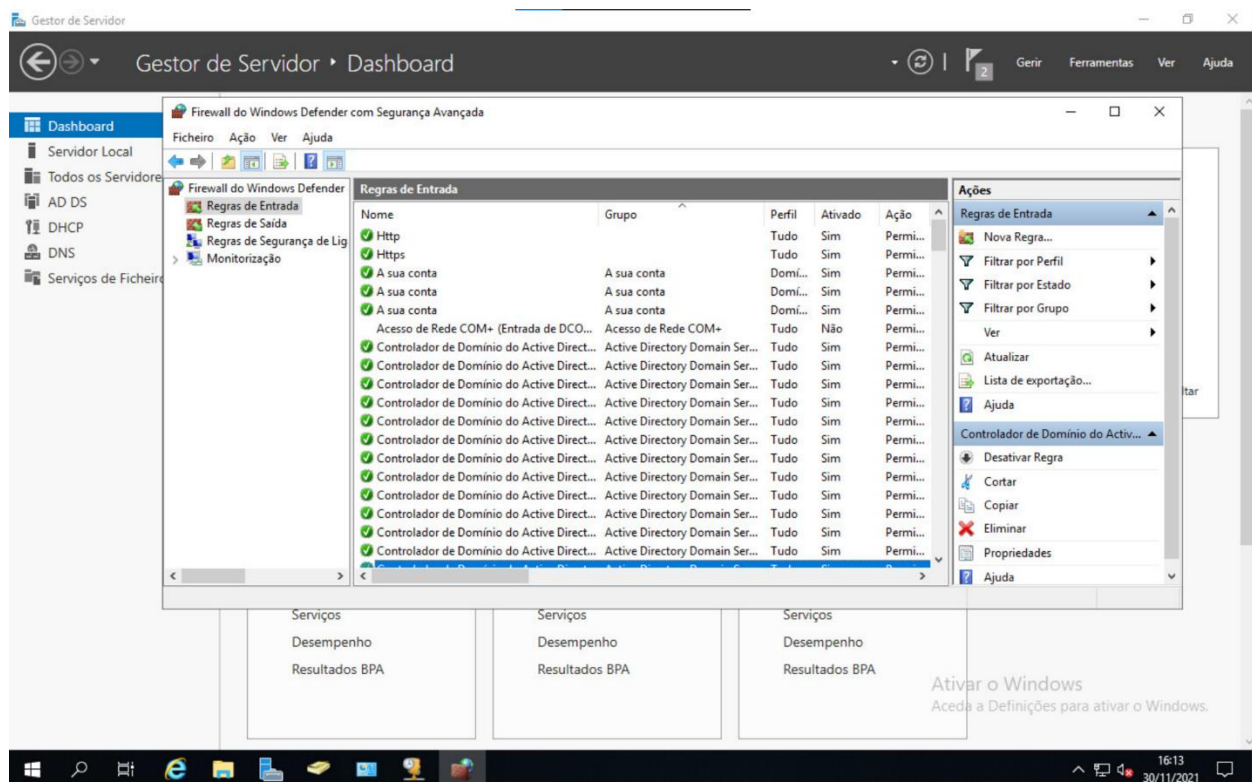
Windows:

Para cumprir o requisito configurou-se a firewall do Windows, para tal, acedeu-se às configurações avançadas da firewall do Windows e criou-se regras de entrada. Para tal seguiu-se os seguintes passos para as portas locais específicas (80 e 443), e permitiu-se sempre a ligação a essas portas









Não foram necessárias mais configurações pois no Windows o *Inbound Traffic* é rejeitado por omissão e no *Outbound traffic* só há block caso haja uma regra específica para tal, todas as por omissão estão em allow.

## US4

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

Linux:

Para a concretização do requisito, a restringiu-se a entrada de pacotes, manipulando a tabela filter, na built-in chain INPUT. Para tal criou-se o ficheiro /etc/stopIpSpoof.sh

```
GNU nano 5.4 /etc/stopIpSpoof.sh *
INTF1="ens32"
SV_IP="10.9.10.57/16"
INT_IP="192.168.157.2/24" #interface
INTF2="ens33"

#ens33 bloquear pacotes de ip que não o da rede que está ligada
iptables -A INPUT -i $INTF2 ! -s $INT_IP -j DROP

#ens32 aceitar os pacotes exceto os das redes privadas
iptables -A INPUT -i $INTF1 -s $INT_IP -j DROP

root@asist:~# chmod +x /etc/stopIpSpoof.sh
root@asist:~# ./stopIpSpoof.sh_
```

Ainda foi alterado o ficheiro seguinte colocando as linhas apresentadas na imagem

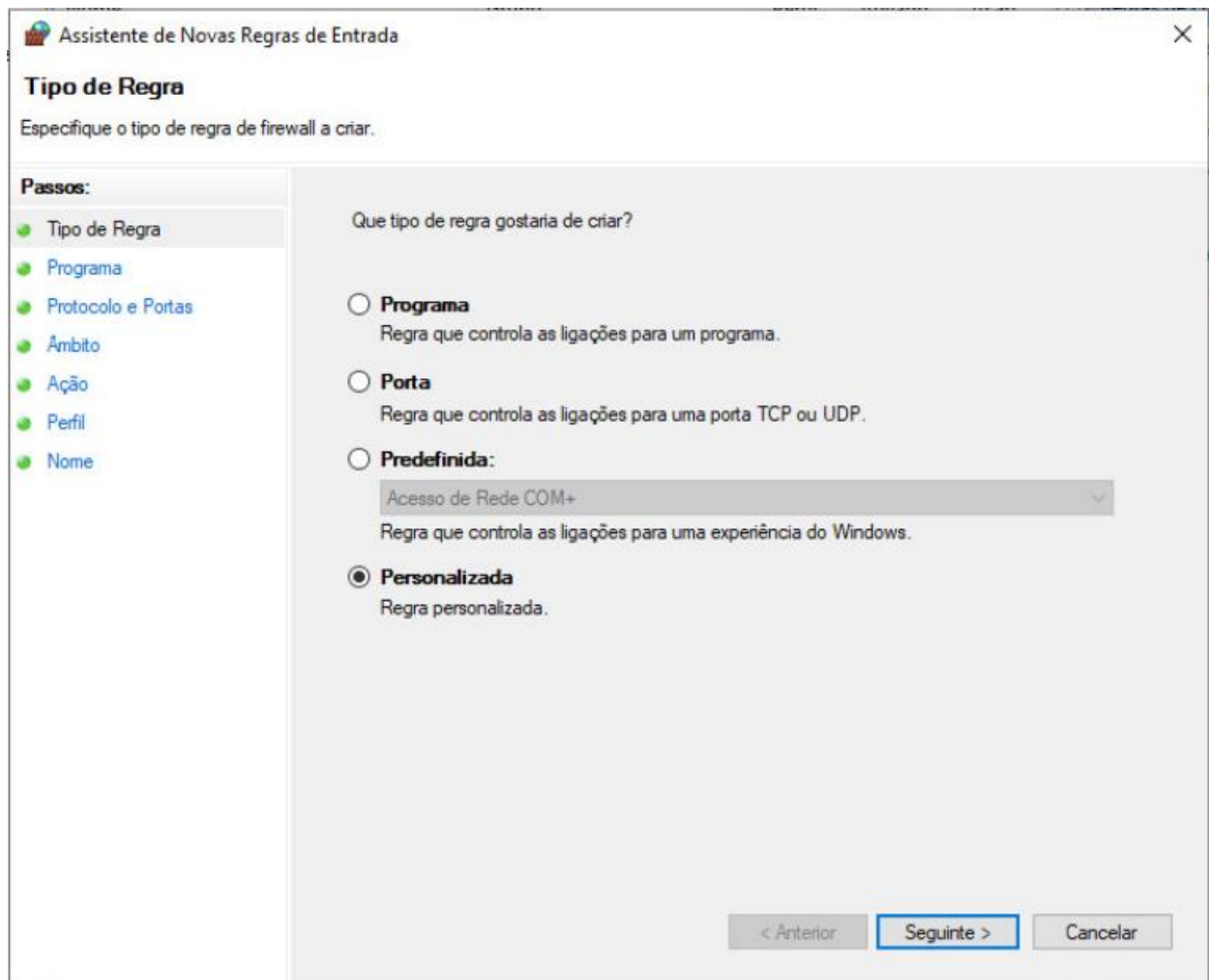
```
GNU nano 5.4 sysctl.conf *
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1
```

Windows:

Para impedir o IP Spoofing foram criadas novas regras de entrada na firewall do Windows, seguindo os seguintes passos



Assistente de Novas Regras de Entrada

## Programa

Especifique o caminho de programa completo e o nome executável do programa ao qual esta regra corresponde.

**Passos:**

- Tipo de Regra
- Programa**
- Protocolo e Portas
- Âmbito
- Ação
- Perfil
- Nome

Esta regra é aplicável a todos os programas ou a um programa específico?

☒ **Todos os programas**  
A regra é aplicável a todas as ligações no computador que correspondam a outras propriedades da regra.

☐ **Este caminho de programa:**

Procurar...

Exemplo: c:\path\program.exe  
%Program Files%\browser\browser.exe

**Serviços**  
Especificar os serviços a que esta regra se aplica.

Personalizar...

< Anterior   Seguinte >   Cancelar

Assistente de Novas Regras de Entrada

X

### Protocolo e Portas

Especifique os protocolos e portas a que esta regra se aplica.

**Passos:**

- Tipo de Regra
- Programa
- Protocolo e Portas**
- Âmbito
- Ação
- Perfil
- Nome

A que portas e protocolos se aplica esta regra?

Tipo de protocolo:

Qualquer

Número de protocolo:

0

Porta local:

Todas as portas

Exemplo: 80, 443, 5000-5010

Porta remota:

Todas as portas

Exemplo: 80, 443, 5000-5010

Definições de protocolo ICMP:

Personalizar...

< Anterior

Seguinte >

Cancelar



Assistente de Novas Regras de Entrada

**Âmbito**

Especifique os endereços IP locais e remotos aos quais esta regra se aplica.

**Passos:**

- Tipo de Regra
- Programa
- Protocolo e Portas
- Âmbito**
- Ação
- Perfil
- Nome

**A que endereços IP locais se aplica esta regra?**

☐ Qualquer endereço IP

☒ Estes endereços IP:

192.168.157.1

Adicionar...

Editar...

Remover

Personalizar os tipos de interface a que esta regra se aplica: Personalizar...

**A que endereços IP remotos se aplica esta regra?**

☐ Qualquer endereço IP

☒ Estes endereços IP:

10.9.11.57

Adicionar...


Editar...

Remover

< Anterior

Seguinte >

Cancelar

 Assistente de Novas Regras de Entrada X

### Ação

Especifique a ação a executar quando uma ligação corresponde às condições especificadas na regra.

**Passos:**

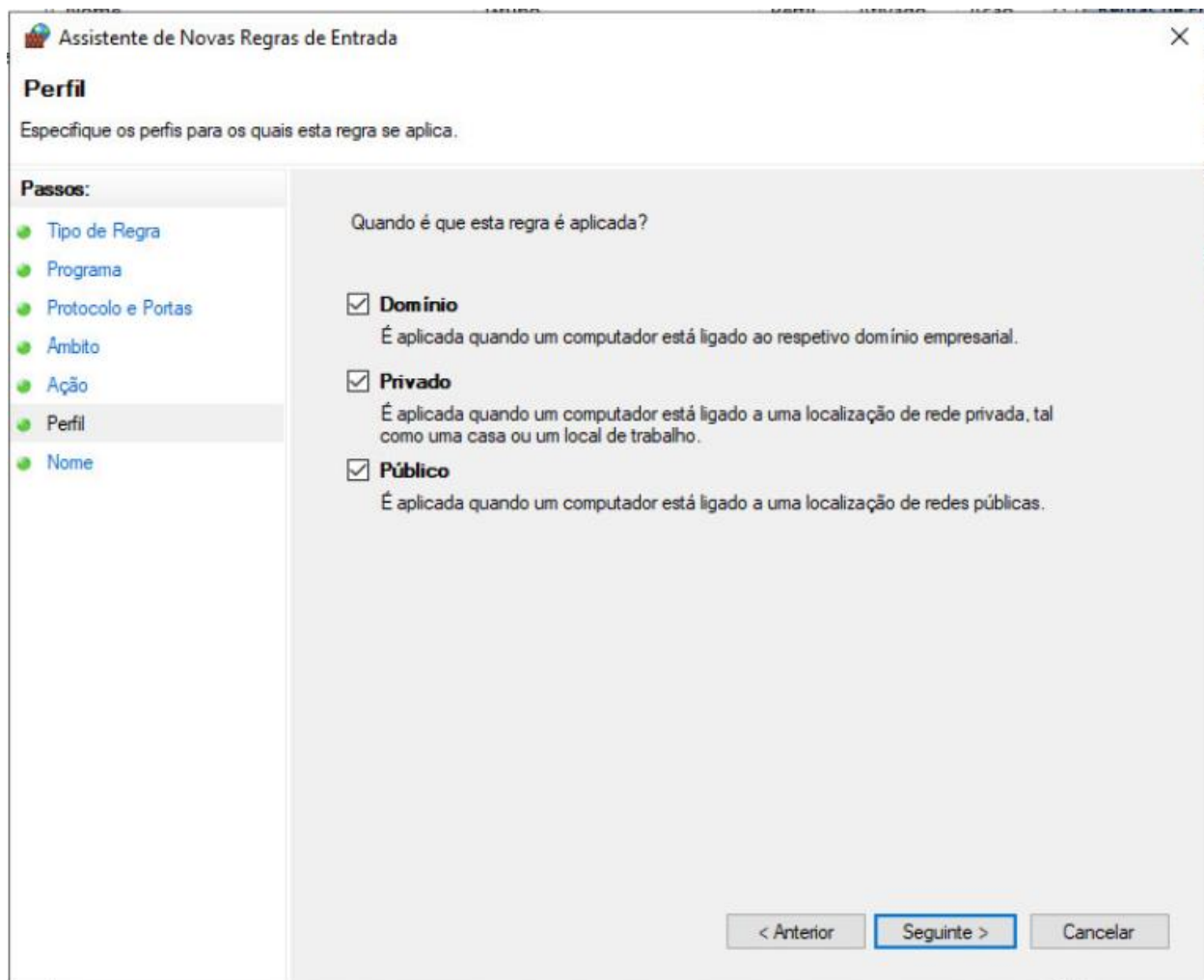
- Tipo de Regra
- Programa
- Protocolo e Portas
- Âmbito
- Ação**
- Perfil
- Nome


Que ação deve ser executada quando uma ligação corresponde às condições especificadas?

☐ **Permitir a ligação**  
Isto inclui ligações protegidas, ou não, com IPsec.

☐ **Permitir a ligação se for segura**  
Isto inclui apenas ligações autenticadas através da utilização de IPsec. As ligações serão protegidas utilizando as definições de propriedades IPsec e as regras no nó de Regra de Segurança da Ligação.

☒ **Bloquear a ligação**



 Assistente de Novas Regras de Entrada

**Nome**  
Especifique o nome e descrição desta regra.

**Passos:**

- Tipo de Regra
- Programa
- Protocolo e Portas
- Âmbito
- Ação
- Perfil
- Nome**

Nome:

Descrição (opcional):

< Anterior

Concluir

Cancelar

Foram efetuados os mesmos passos para a outra placa de rede

**Assistente de Novas Regras de Entrada**

**Âmbito**

Especifique os endereços IP locais e remotos aos quais esta regra se aplica.

**Passos:**

- Tipo de Regra
- Programa
- Protocolo e Portas
- Âmbito**
- Ação
- Perfil
- Nome

**A que endereços IP locais se aplica esta regra?**

☐ Qualquer endereço IP

☒ Estes endereços IP:

10.9.11.57

Adicionar...

Editar...

Remover

Personalizar os tipos de interface a que esta regra se aplica: Personalizar...

**A que endereços IP remotos se aplica esta regra?**

☐ Qualquer endereço IP

☒ Estes endereços IP:

192.168.157.1/24

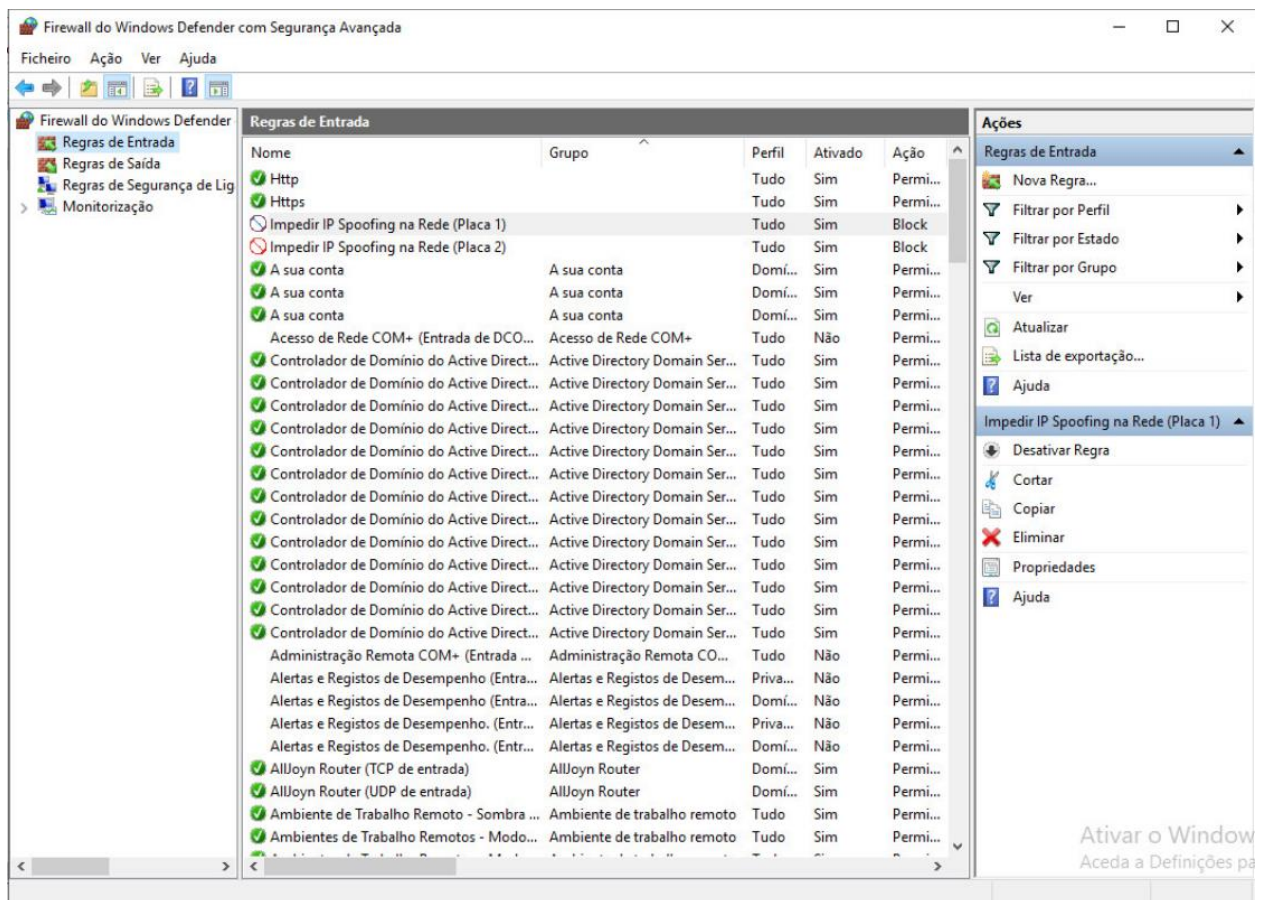
Adicionar...

Editar...

Remover

< Anterior   **Seguinte >**   Cancelar

Sendo assim criadas as regras de bloqueio

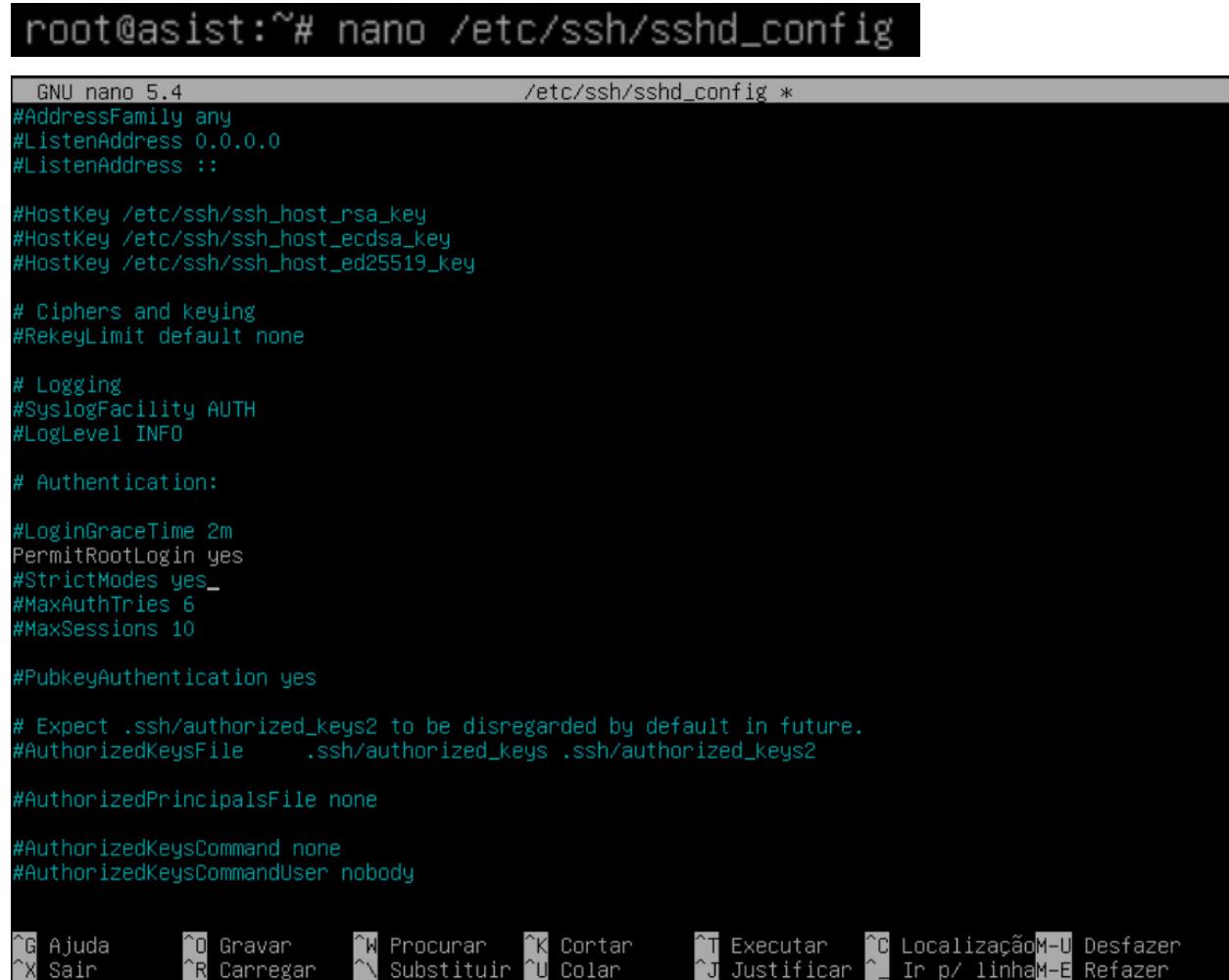


## US5

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`

De modo a cumprir o requisito alterou-se o seguinte ficheiro de modo a permitir o acesso via SSH à root

```
root@asist:~# nano /etc/ssh/sshd_config
```



```
GNU nano 5.4 /etc/ssh/sshd_config *
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes_
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

^G Ajuda      ^O Gravar    ^W Procurar  ^K Cortar    ^T Executar  ^C Localizaç
^X Sair      ^R Carregar  ^N Substituir ^U Colar     ^J Justificar ^_ Ir p/ linha
^M-U Desfazer
^M-E Refazer
```

Foram ainda realizadas mudanças ao nível do PAM, que corresponde ao conjunto de módulos que controla a autenticação dos utilizadores no sistema. Dessa forma, tivemos de alterar as configurações no ficheiro seguinte, acrescentando as duas últimas linhas da imagem

```
root@asist:~# nano /etc/pam.d/sshd

GNU nano 5.4 /etc/pam.d/sshd *
# Print the message of the day upon successful login.
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session optional pam_motd.so motd=/run/motd.dynamic
session optional pam_motd.so noupdate

# Print the status of the user's mailbox upon successful login.
session optional pam_mail.so standard noenv # [1]

# Set up user limits from /etc/security/limits.conf.
session required pam_limits.so

# Read environment variables from /etc/environment and
# /etc/security/pam_env.conf.
session required pam_env.so # [1]
# In Debian 4.0 (etch), locale-related environment variables were moved to
# /etc/default/locale, so read that as well.
session required pam_env.so user_readenv=1 envfile=/etc/default/locale

# SELinux needs to intervene at login time to ensure that the process starts
# in the proper default security context. Only sessions which are intended
# to run in the user's context should be run after this.
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so open

# Standard Unix password updating.
@include common-password

# autorizar acesso via SSH se os users tiverem UID entre 6000 e 6500
auth [success=ok default=ignore] pam_succeed_if.so debug quiet uid > 6000 uid < 6500
auth required pam_listfile.so onerr=fail item=rhost sense=allow file=/etc/remote-hosts
```



## US6

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

Para cumprir o requisito foram efetuadas mudanças ao nível do PAM, que corresponde ao conjunto de módulos que controla a autenticação dos utilizadores no sistema. Para tal, alterou-se o seguinte ficheiro acrescentando a segunda linha apresentada na imagem

```
root@asist:~# nano /etc/pam.d/common-auth
```

```
GNU nano 5.4 /etc/pam.d/common-auth
# inibir acesso aos users em /etc/bad-guys
auth required pam_listfile.so onerr=fail item=user sense=deny file=/etc/bad-guys

#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth [success=2 default=ignore] pam_unix.so nullok
auth [success=1 default=ignore] pam_ldap.so minimum_uid=1000 use_first_pass
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

## US7

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.)

Para a concretização do requisito foi alterado o seguinte ficheiro, acrescentando as mensagens apresentadas e obtendo -se o resultado apresentado para a mensagem pré-login

```
root@asist:~# nano /etc/issue
```

```
GNU nano 5.4 /etc/issue *
Bem-vindo
\nd
\nt
\ru users têm sessão iniciada.
```

```
Bem-vindo
Fri Dec 3 2021
23:33:33
0 users têm sessão iniciada.

asist login: _
```

Foi ainda alterado o seguinte ficheiro de modo a criar a mensagem pós-login

```
root@asist:~# nano /etc/profile
```

```
GNU nano 5.4 /etc/profile *
if [ "${PS1-}" ]; then
  if [ "${BASH-}" ] && [ "$BASH" != "/bin/sh" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='\h:\w\$ '
    if [ -f /etc/bash.bashrc ]; then
      . /etc/bash.bashrc
    fi
  else
    if [ "$(id -u)" -eq 0 ]; then
      PS1='# '
    else
      PS1='$ '
    fi
  fi
fi

if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi

h=$(date +%H)
if [ $h -lt 12 ]; then
  echo "Bom dia $USER !"
elif [ $h -lt 18 ]; then
  echo "Boa tarde $USER !"
else
  echo "Boa noite $USER !"
fi
```

```
Bem-vindo
Sat Dec 4 2021
19:15:13
0 users têm sessão iniciada.

asist login: root
Password:
Linux asist 5.10.0-8-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) 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: Sat Dec 4 19:12:52 WET 2021 on tty1
Boa noite root !
root@asist:~#
```

## US8

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

Para cumprir o requisito alteramos o ficheiro criado na US3 e acrescentaram-se as regras apresentadas de modo a que apenas aceite pacotes ICMP dos elementos do grupo

```
root@asist:~# nano /etc/init.d/rules.sh

GNU nano 5.4 /etc/init.d/rules.sh *
#!/bin/bash
iptables -P INPUT DROP
iptables -F INPUT

iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT #http
iptables -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT #https

#permite pedidos icmp do grupo
iptables -A -p icmp -s 10.8.181.195 --icmp-type echo-request -j ACCEPT #Tomas
iptables -A -p icmp -s 10.8.181.196 --icmp-type echo-request -j ACCEPT #Alex
iptables -A -p icmp -s 10.8.181.255 --icmp-type echo-request -j ACCEPT #Miguel
iptables -A -p icmp -s 10.8.181.156 --icmp-type echo-request -j ACCEPT #Rui

#deny all
iptables -A INPUT -p icmp -j DROP
```

Os IP's utilizados correspondem aos endereços do grupo na VPN do DEI:

Connection-specific DNS Suffix . : dei.isep.ipp.pt IPv4 Address. . . . . : 10.8.181.255 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . : 0.0.0.0	Miguel
Connection-specific DNS Suffix . : dei.isep.ipp.pt IPv4 Address. . . . . : 10.8.181.196 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . : 0.0.0.0	Rúben
Connection-specific DNS Suffix . : dei.isep.ipp.pt IPv4 Address. . . . . : 10.8.181.156 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . : 0.0.0.0	Rui
Connection-specific DNS Suffix . : dei.isep.ipp.pt IPv4 Address. . . . . : 10.8.181.195 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . : 0.0.0.0	Tomás