

Relatório Projeto 3

LETI – REDSC 2023/2024

Data

Segunda-feira, 8 de janeiro de 2024

Autores

Alunos de Licenciatura em Engenharia de Telecomunicações e Informática pertencentes à turma 3DA:

Eduardo Pereira, 1211460

Raul Reis, 1211524

Introdução

Nest projeto será apresentada a formação de uma rede através do Kathara, um simulador de redes baseado em containers Docker. Ao longo deste projeto serão apresentados desafios como a distribuição de IPs, roteamento, utilização de servidores DNS, entre outros. Acreditamos que somos capazes de os superar a todos com os conhecimentos que detemos, sendo qualquer percalço resolvido rapidamente com pesquisa sobre o tema.

Preparação

1. Desenvolvimento remoto por tunnel do vscode

Para tornar mais fácil o desenvolvimento deste projeto, foi tomada a decisão de trabalhar na máquina virtual não por ssh ou diretamente no terminal da mesma, mas sim através da utilização da ferramenta de tunnel disponível no VSCode. Para tal foi necessário executar uns passos de preparação para o mesmo, presentes website oficial do Visual Studio <https://code.visualstudio.com/docs/remote/vscode-server>, no entanto irão ser apresentados os passos para a configuração do mesmo seguidamente.

Começando no computador que irá aceder ao tunnel, deve ser instalado o pack de extensões Remote Development no VSCode.

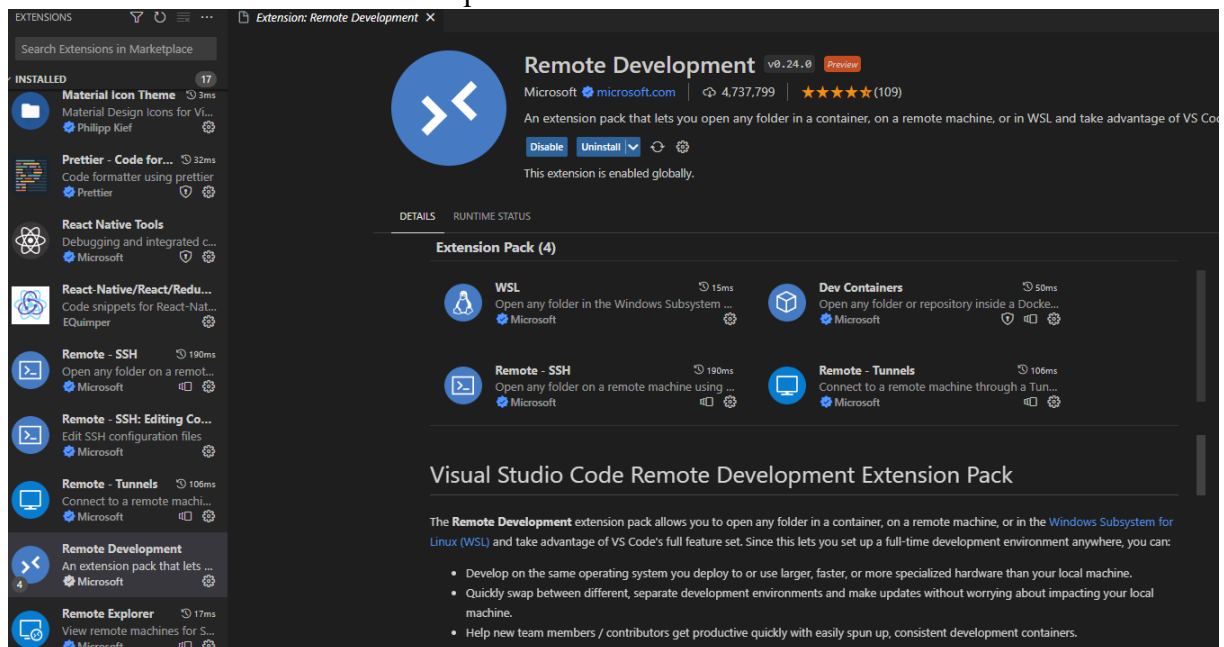


Figura 1 - Extensões VSCode

Esta extensão disponibiliza várias ferramentas que irão facilitar o acesso por tunnel, nomeadamente um menu presente do lado esquerdo do IDE que permite fácil acesso a todos os tunnels associados à conta github presente.

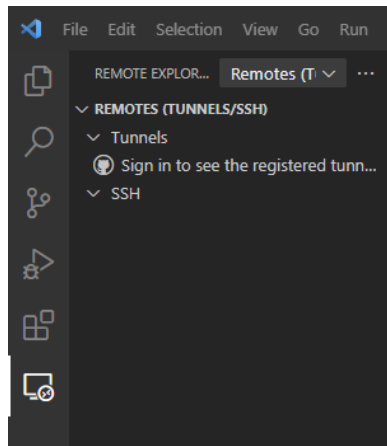


Figura 2 - Menu tunnels VSCode

Agora na máquina em que se pretende aceder via tunnel devemos instalar e extrair o CLI usando os comandos:

- `curl -Lk 'https://code.visualstudio.com/sha/download?build=stable&os=cli-alpine-x64' --output vscode_cli.tar.gz`
- `tar -xf vscode_cli.tar.gz`

Depois deve-se executar o comando `./code tunnel` para criar um tunnel, sendo depois escolhida a opção de “GitHubAccount”

```
redsc@redsc:~/tunnelConf$ curl -Lk 'https://code.visualstudio.com/sha/download?build=stable&os=cli-alpine-x64' --output
vscode_cli.tar.gz
redsc@redsc:~/tunnelConf$ tar -xf vscode_cli.tar.gz
redsc@redsc:~/tunnelConf$ ls
code  vscode_cli.tar.gz
redsc@redsc:~/tunnelConf$ ./code tunnel
*
* Visual Studio Code Server
*
* By using the software, you agree to
* the Visual Studio Code Server License Terms (https://aka.ms/vscode-server-license) and
* the Microsoft Privacy Statement (https://privacy.microsoft.com/en-US/privacystatement).
*
? How would you like to log in to Visual Studio Code? >
  Microsoft Account
  Github Account
```

Figura 3 - Seleção de tipo de conta

Sendo depois necessária confirmação

```
? How would you like to log in to Visual Studio Code? - Github Account
To grant access to the server, please log into https://github.com/login/device and use code [redacted]
```

Figura 4 - Confirmação de login

Seguidamente é atribuído um nome ao tunnel

```
*
? How would you like to log in to Visual Studio Code? - Github Account
To grant access to the server, please log into https://github.com/login/device and use code [redacted]
? What would you like to call this machine? (redsc) >
```

Figura 5 - Atribuir nome ao tunnel

E o tunnel está agora disponível para aceder remotamente

```
*
How would you like to log in to Visual Studio Code? · Github Account
To grant access to the server, please log into https://github.com/login/device and use code 82F1-5F37
What would you like to call this machine? · redsckathara
[2023-11-25 21:31:40] Creating tunnel with the name: redsckathara
[2023-11-25 21:31:41] Adopting existing tunnel (ID=ID { cluster: "uks1", id: "vvpt7755" })

Open this link in your browser https://vscode.dev/tunnel/redsckathara/home/redsc/tunnelConf
```

Figura 6 - Disponibilização do tunnel

No computador em que queremos aceder ao tunnel, é agora possível observar na janela de acesso remoto o tunnel que foi configurado, facilitando imensamente o desenvolvimento na máquina virtual.

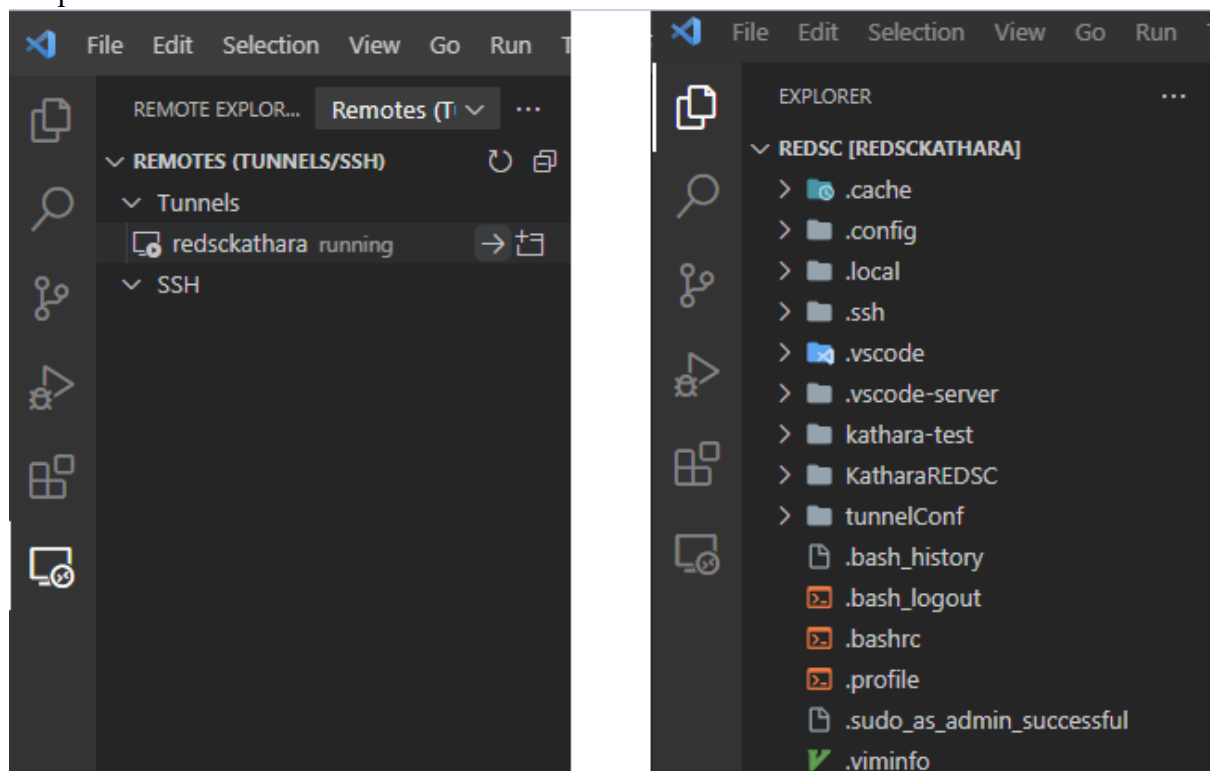


Figura 7 - Acesso ao tunnel

Cenário 1

1. Desenho da rede

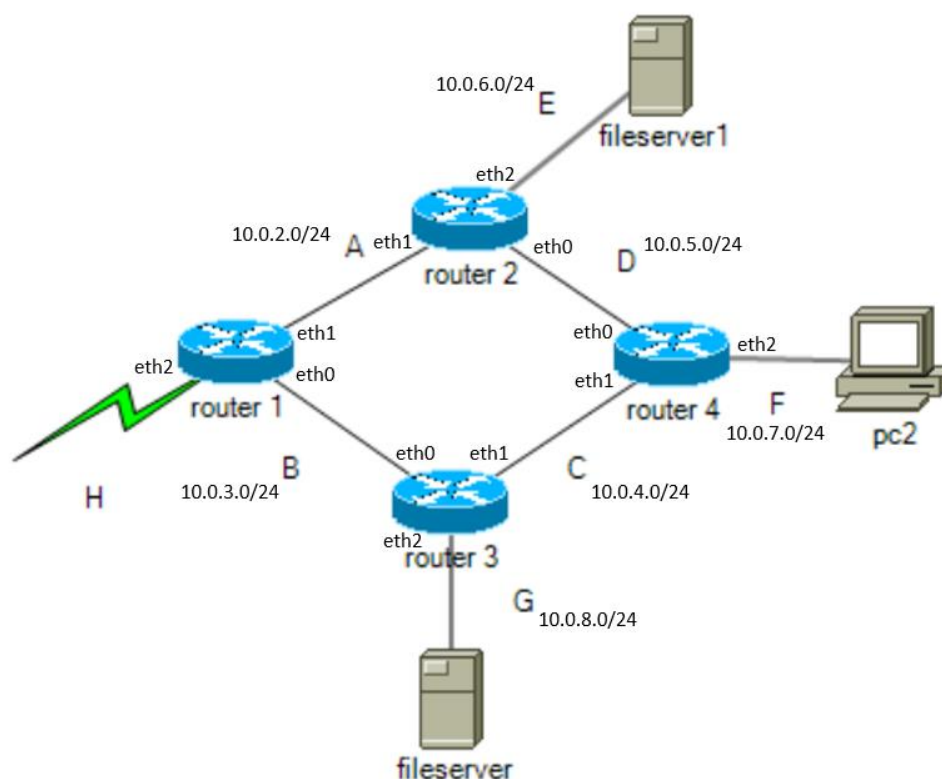


Figura 8 - Desenho da rede

A	B	C	D	E	F	G
10.0.2.0/24	10.0.3.0/24	10.0.4.0/24	10.0.5.0/24	10.0.6.0/24	10.0.7.0/24	10.0.8.0/24

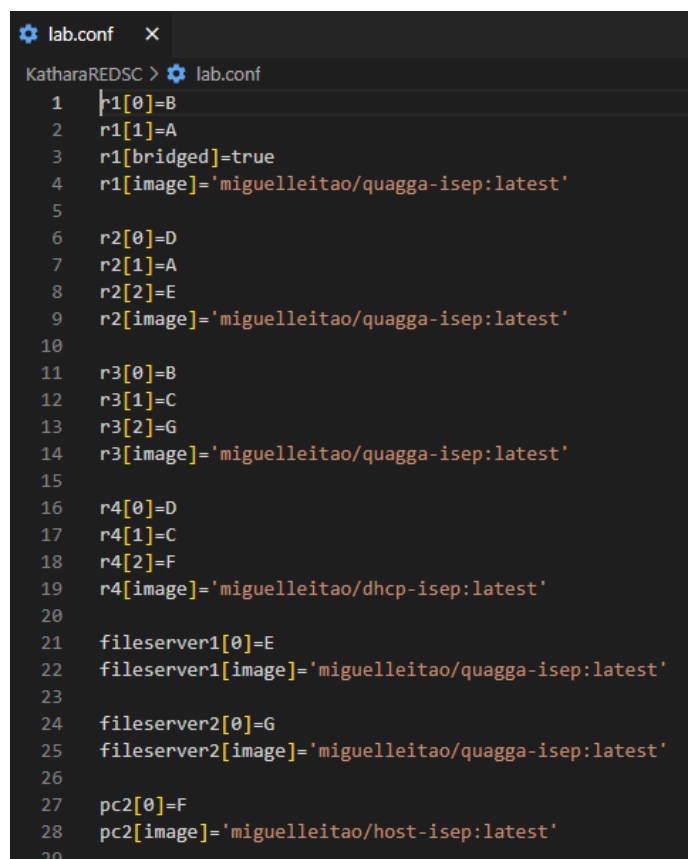
R1	R2	R3	R4	fileserver1	fileserver2
eth0 - 10.0.3.1	eth0 - 10.0.5.1	eth0 - 10.0.3.2	eth0 - 10.0.5.2	eth0 - 10.0.6.2	eth0 - 10.0.8.2
eth1 - 10.0.2.1	eth1 - 10.0.2.2	eth1 - 10.0.4.1	eth1 - 10.0.4.2	---	---
eth2 - *	eth2 - 10.0.6.1	eth2 - 10.0.8.1	eth2 - 10.0.7.1	---	---

Foi optada a utilização da gama **10.0.0.0/8** com sub-redes de **classe C** por questões de simplicidade, uma vez que no cenário apresentado o número de *hosts* disponibilizados pelas mesmas é mais que suficiente. O IP do **pc2** não está representado uma vez que foi especificado que a rede F deverá utilizar **DHCP**.

2. Configuração da rede no Kathara

A configuração da rede no Kathara foi relativamente simples, sendo apenas necessário criar o ficheiro “lab.conf”, que define quais as ligações presentes na rede, assim como pastas para cada

um dos dispositivos e ficheiros do tipo “.startup” para cada um dos mesmos, contento a configuração dos seus IPs estáticos.



```
lab.conf x
KatharaREDSC > lab.conf
1  r1[0]=B
2  r1[1]=A
3  r1[bridged]=true
4  r1[image]='miguelleitao/quagga-isep:latest'
5
6  r2[0]=D
7  r2[1]=A
8  r2[2]=E
9  r2[image]='miguelleitao/quagga-isep:latest'
10
11 r3[0]=B
12 r3[1]=C
13 r3[2]=G
14 r3[image]='miguelleitao/quagga-isep:latest'
15
16 r4[0]=D
17 r4[1]=C
18 r4[2]=F
19 r4[image]='miguelleitao/dhcp-isep:latest'
20
21 fileserver1[0]=E
22 fileserver1[image]='miguelleitao/quagga-isep:latest'
23
24 fileserver2[0]=G
25 fileserver2[image]='miguelleitao/quagga-isep:latest'
26
27 pc2[0]=F
28 pc2[image]='miguelleitao/host-isep:latest'
29
```

Figura 9 - Ficheiro "lab.conf"

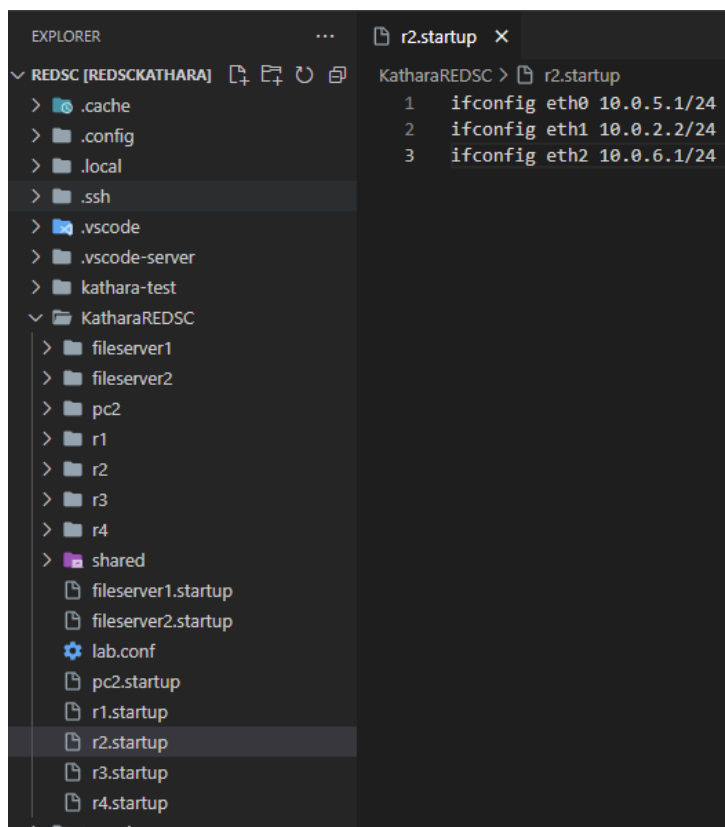


Figura 10 - Diretórios e ficheiros "startup" dos dispositivos

3. Roteamento dinâmico em RIP

Para que seja possível fazer mudanças de redes no futuro sem que ocorram problemas devido ao roteamento das mesmas, optou-se pela utilização do roteamento dinâmico em RIP (Routing Information Protocol).

Para tal foi necessário adicionar os ficheiros “*ripd.conf*” e “*daemons*” no diretório “*/etc/quagga/*” de todos os routers (r1-r4).

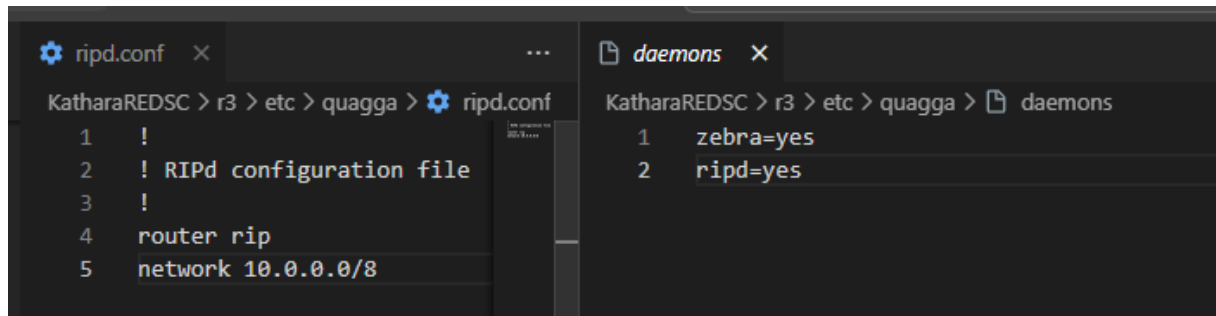


Figura 11 - Ficheiros configuração RIP

Também foi necessário adicionar a linha presente na Figura 12 todos os ficheiros “startup” dos routers para a definição de rotas ser executada automaticamente.

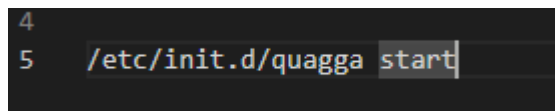


Figura 12 - Comando inicialização RIP

4. Webserver nos fileserver 1 & 2

Para a configuração dos *webserver*s foi utilizado o *apache2*, tendo a página disponibilizada o texto “FILESERVERX” em arte ASCII, onde X representa em qual dos servidores este se encontra.

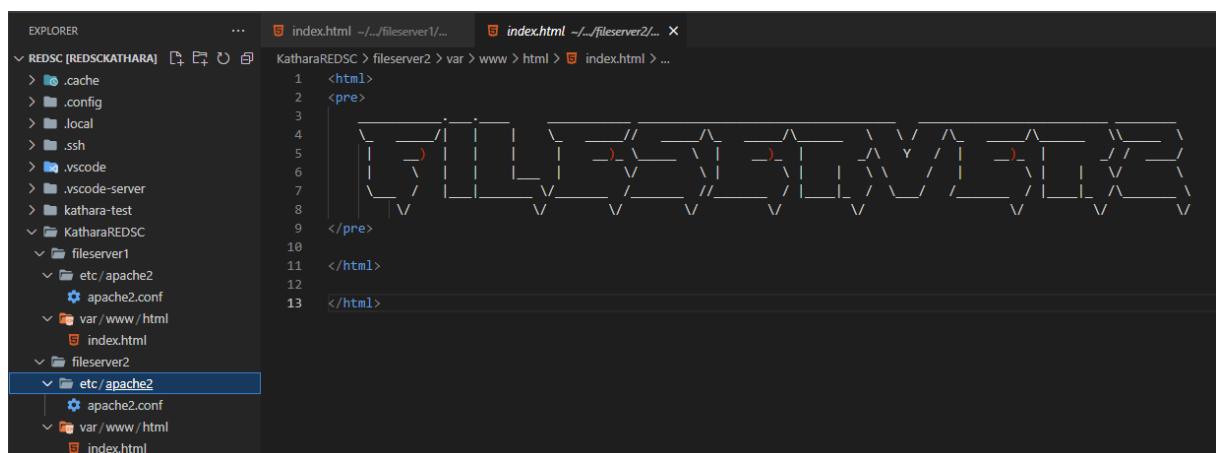


Figura 13 - Configuração Apache2

5. IP por DHCP ao PC2

Para atribuir o IP por DHCP ao “pc2” foi necessário, para além da configuração da imagem do router “r4” presente na **Figura 9**, adicionar o ficheiro e diretórios presentes na **Figura 14**.

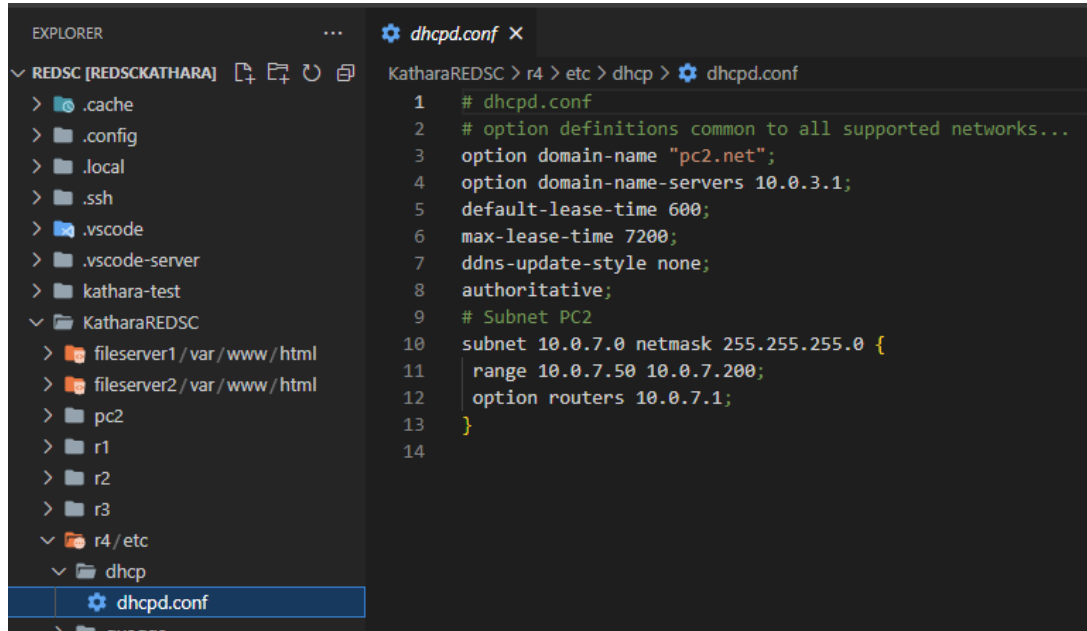


Figura 14 - Configuração DHCP no "r4"

Neste caso a configuração irá atribuir IPs por DHCP aos dispositivos presentes na rede 10.0.7.0/24 desde 10.0.7.50 até 10.0.7.200.

É ainda necessário especificar no ficheiro “startup” do “pc2” que o mesmo é um cliente DHCP, utilizando o comando presente na **Figura 15**.

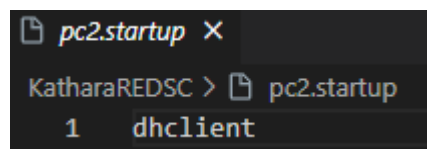


Figura 15 - Config DHCP “pc2”

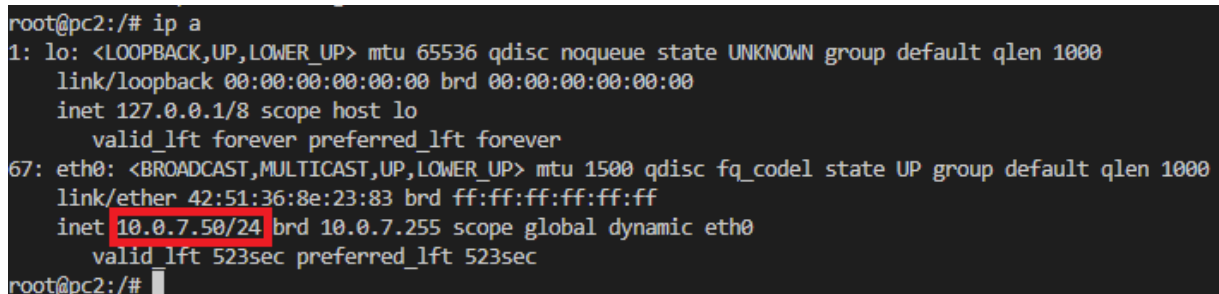


Figura 16 - IP atribuído por DHCP ao "pc2"

Cenário 2

1. Configuração de DNS

A configuração do DNS terá 3 partes, sendo as mesmas:

- **Configuração DNS externo** – permite aceder a servidores DNS fora da rede simulada (Ex: google);

Para a configuração do mesmo é adicionado o ficheiro `named.conf.options` a `r1`, estando presente no diretório e com as configurações demonstradas na

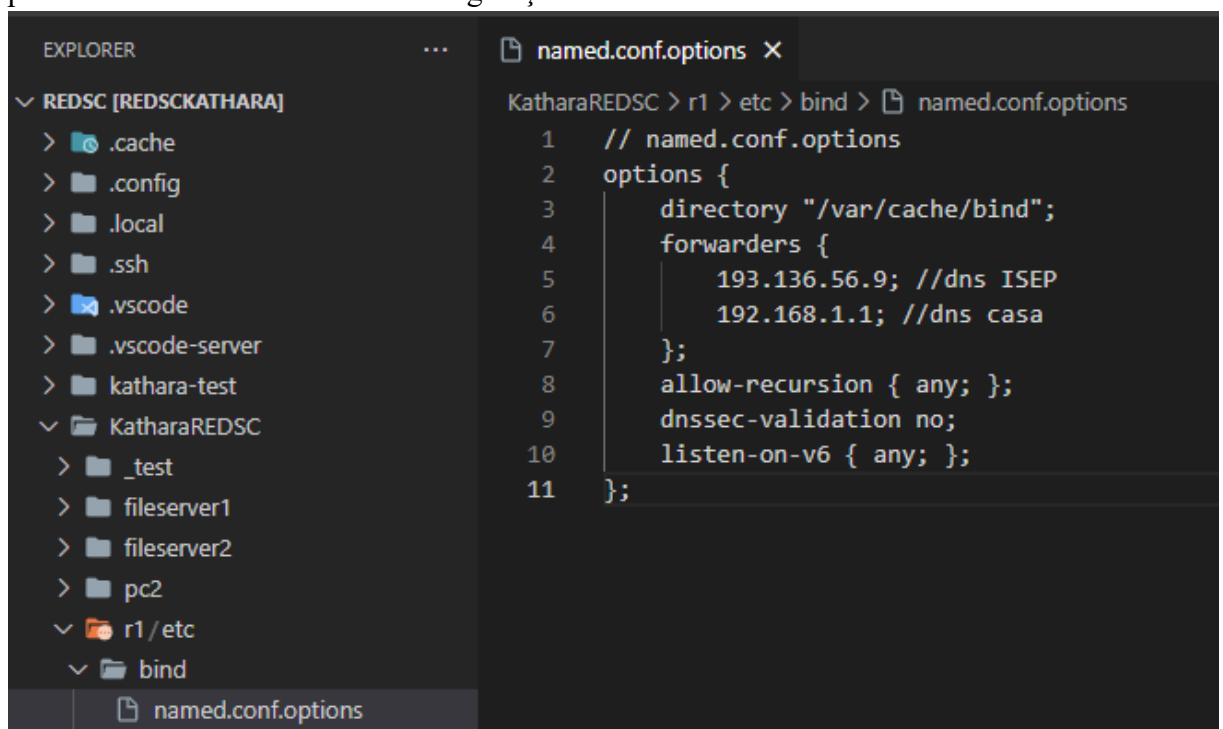


Figura 17 - Configuração DNS externo

É ainda necessário adicionar um comando ao startup do mesmo para este serviço ser ativado.

```
/etc/init.d/bind start
```

Figura 18 - Comando inicialização serviço DNS

- **Configuração DNS local** – permite a resolução de nomes para aceder a servidores presentes na rede;

Na configuração deste serviço irão ser adicionados 2 ficheiros, o “`named.conf.local`”, que irá indicar onde se encontrar informações sobre o DNS local, e o “`redsc.local.db`” que contém as informações do DNS local. As configurações dos mesmos podem ser observadas na *Figura 19* e na *Figura 20*.

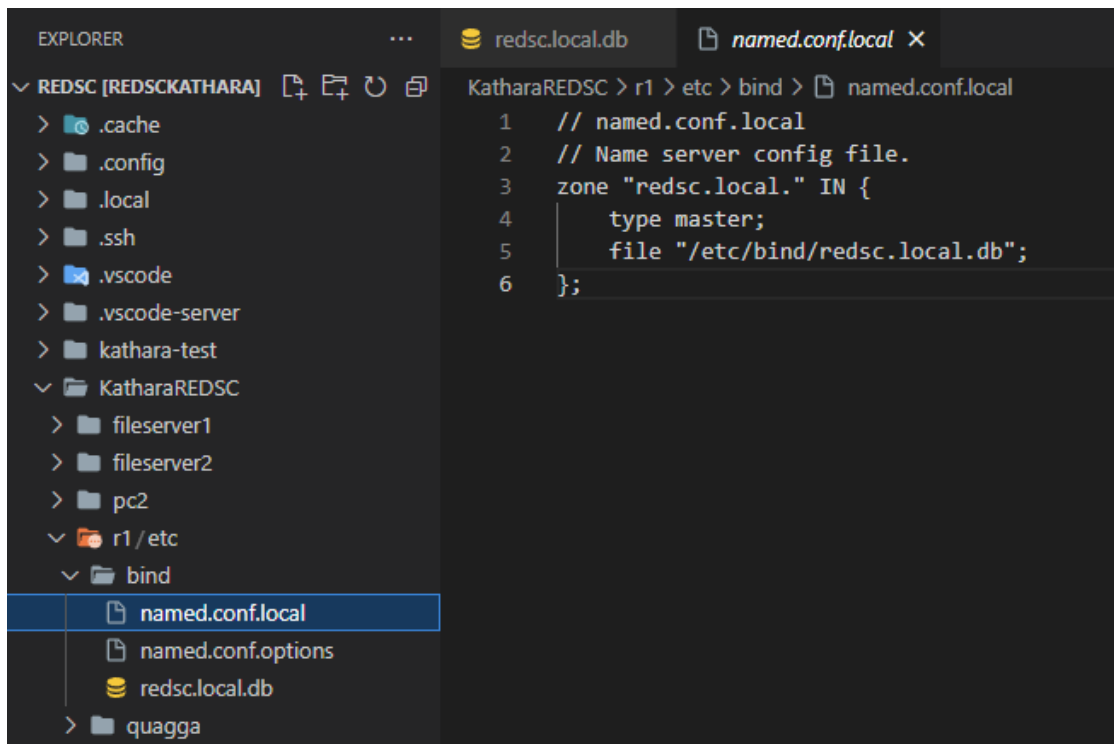


Figura 19 - Configuração "named.conf.local"

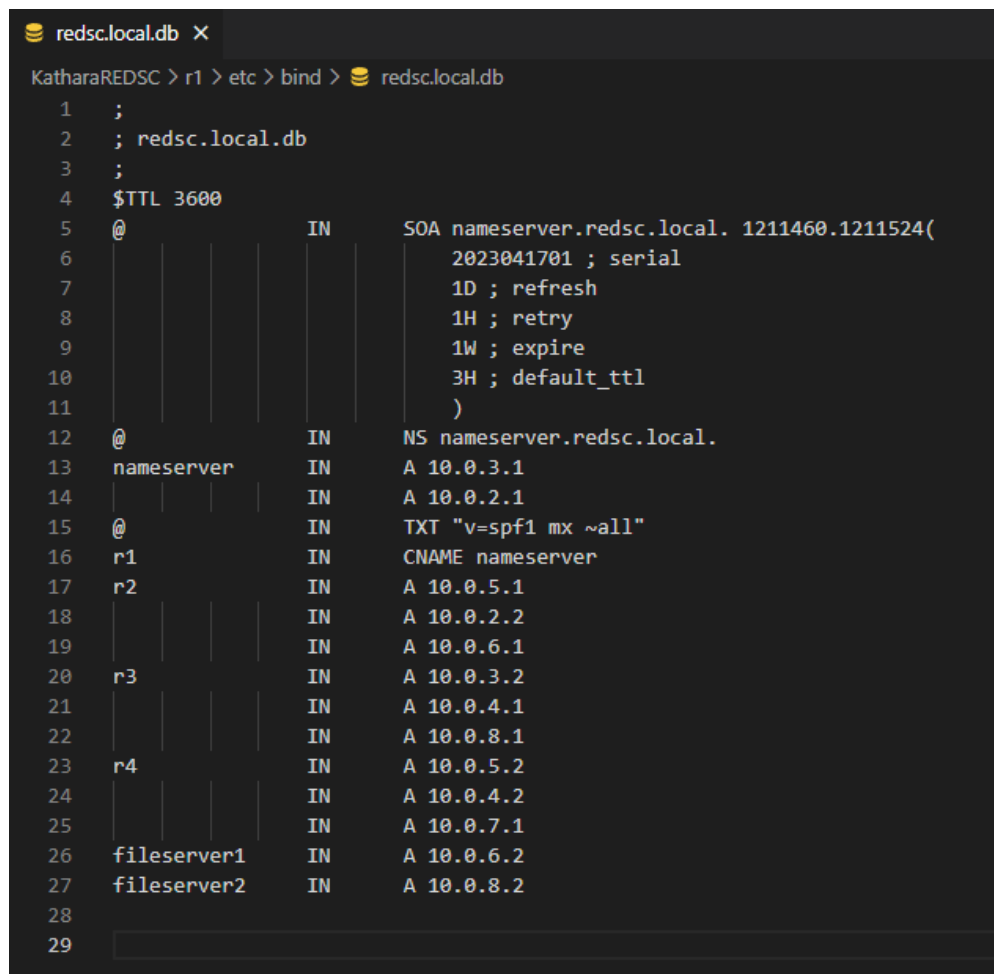


Figura 20 - Configuração "redsc.local.db"

- **Configuração do DNS reverso** – permite obter o nome do servidor através do IP;

Por fim, para a configuração do DNS reverso adiciona-se o segmento presente na **Figura 21** ao “*named.conf.local*”, criando o ficheiro “*rev.redsc_af.db*” (**Figura 22**)

```

8 // Reverse DNS resolution for Subnets
9 zone "0.10.in-addr.arpa" IN {
10     type master;
11     file "/etc/bind/rev.redsc_af.db";
12 };
13

```

Figura 21 - Config Reverse DNS

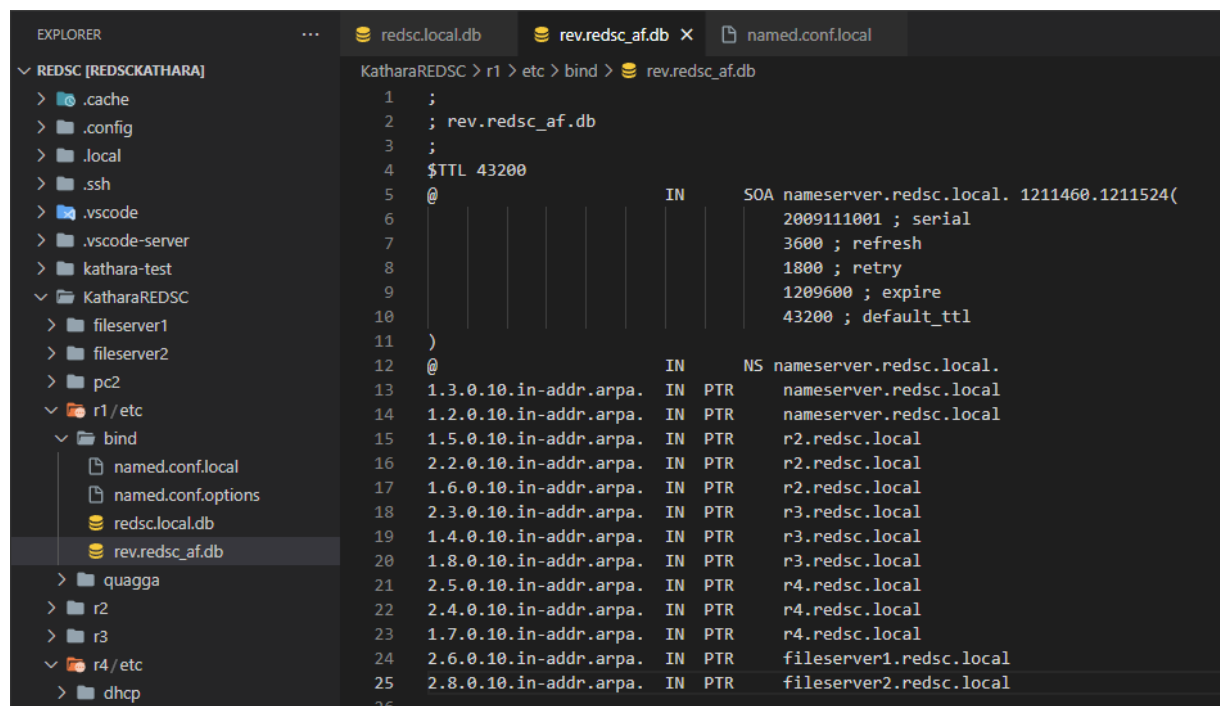


Figura 22 - Configuração de "rev.redsc_af.db"

NOTA: Para que o DNS local esteja disponível nos routers para além do “r1”, deve ser adicionado o ficheiro presente na **Figura 23**.

```

KatharaREDSC > r4 > etc > resolv.conf
1 nameserver 10.0.3.1
2 nameserver 10.0.2.1

```

Figura 23 - Ficheiro "resolv.conf"

Cenário 3

Neste cenário é pedido para ligarmos o router “R1” a uma firewall, neste caso será usado o *PfSense*, sendo depois expostas as páginas web presentes no fileServer1 e fileServer2 à web. Para tal, terão de ser feitas algumas mudanças nas configurações da placa de rede da máquina virtual onde o *kathara* se encontra a correr, assim como a introdução de uma nova máquina a correr *PfSense* com as suas específicas configurações.

1. Configurar máquinas virtuais

Depois de proceder à instalação do *PfSense* (tutorial presente em <https://docs.netgate.com/pfsense/en/latest/install/install-walkthrough.html>), devem ser mudadas as configurações da placa de rede tal como mostrado na **Figura 24**.

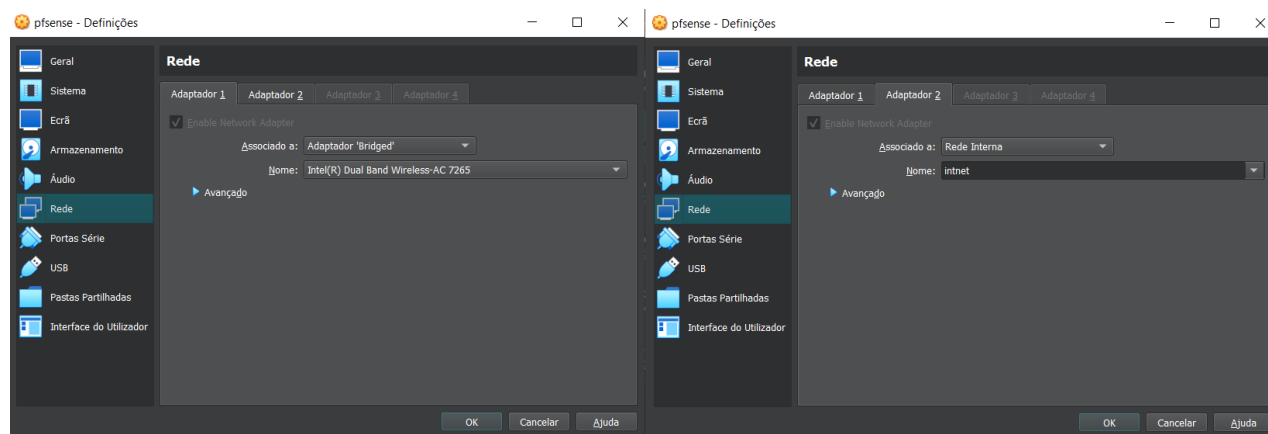


Figura 24 - Configuração placas de rede PfSense

Esta configuração permite o *pfsense* utilizar a rede a que o computador está ligado como WAN, e usar a rede interna da virtual Box como LAN.

Para que a máquina virtual esteja conectada à LAN do *PfSense* também devemos mudar as configurações da placa de rede tal como mostrado na **Figura 25**.

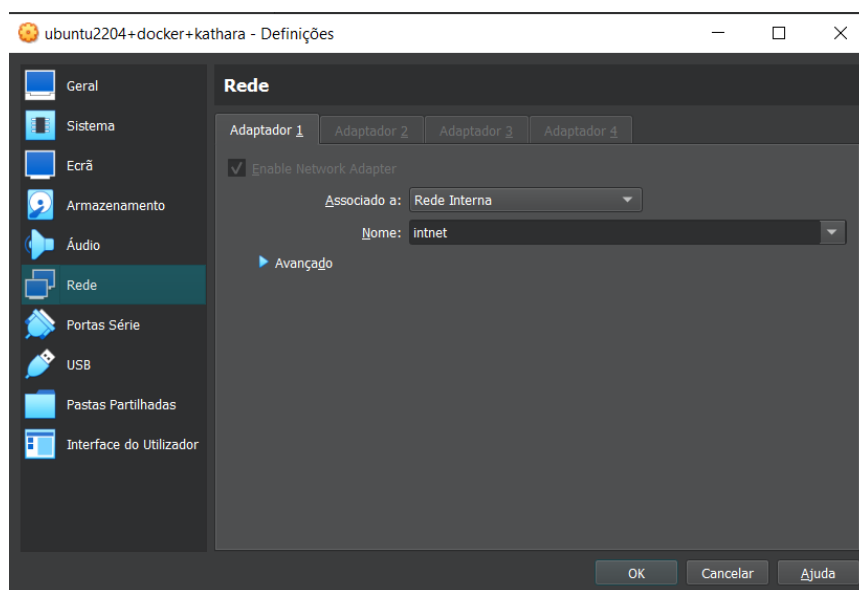


Figura 25 - Configuração placa de rede VM com Kathara

Por fim deve também ser configurada a rede LAN do PfSense, no nosso caso foi utilizada a rede 192.168.50.0/24, para evitar conflitos tanto com as redes de casa como as redes do ISEP, habilitando também DHCP para a mesma.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 1314bb560c7b03c67612

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.188/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Figura 26 - IPs Máquina PfSense

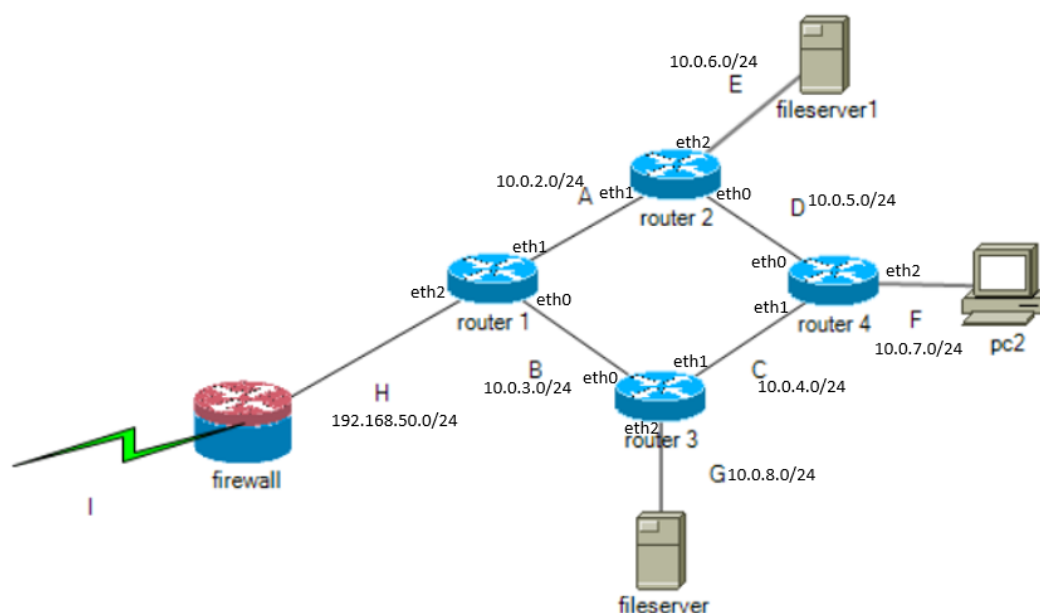


Figura 27 - Desenho rede com Firewall

A rede H representa a rede à qual a máquina virtual com a rede simulada está ligada, sendo que na verdade, sendo a mesma baseada em containers Docker, o router r1 que está em modo “bridge” tem, neste caso, o IP 172.17.0.3. É exatamente por esta razão que as mudanças feitas ao simulador no tópico seguinte são necessárias.

2. Configurar rede Kathara

Algumas mudanças também serão necessárias no ficheiro de “*lab.conf*” e “*r1.startup*”, para que seja possível exportar os servidores para a rede LAN do PfSense, estas mudanças estão presentes na **Figura 28** e **Figura 29**.

```
KatharaREDSC > r1.startup
1  ifconfig eth0 10.0.3.1/24
2  ifconfig eth1 10.0.2.1/24
3
4  iptables -t nat -A POSTROUTING -j MASQUERADE
5
6  iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 10.0.6.2:80 #PortForward FileServer1
7  iptables -t nat -A PREROUTING -p tcp --dport 81 -j DNAT --to-destination 10.0.8.2:80 #PortForward FileServer2
8
9  /etc/init.d/quagga start
10
11 /etc/init.d/bind start
```

Figura 28 - Port-Forward Webservers

```
r1[0]=B
r1[1]=A
r1[bridged]=true
r1[port]="80:80/tcp"
r1[port]="81:81/tcp"
r1[image]='miguelleitao/quagga-isep:latest'
```

Figura 29 - Port-forward para Docker

3. PortForward no PfSense

Para que seja possível aceder os webservers fora da rede interna gerida pelo PfSense será necessário configurar o port-forward na firewall. Para tal deve ser feito o login na página de configuração do PfSense num browser, usando o IP LAN do mesmo (neste exemplo 192.168.50.1) e utilizando as credenciais predefinidas “admin” e “pfsense” para *username* e *password*, respetivamente.

Seguidamente deve-se aceder às definições de firewall e adicionar uma nova regra com as definições presentes na **Figura 30**.

192.168.50.1/firewall_nat_edit.php?id=0 67%

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination ☐ Invert match. WAN address /
Type Address/mask

Destination port range Other 80 Other 80
From port Custom To port Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Single host 192.168.50.3
Type Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port Other 80
Port Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description Port Forward Fileserver1
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT Port Forward Fileserver1

Figura 30 - Configuração Port-Forward PfSense

Os parâmetros com a caixa vermelha indicam o seguinte:

- **Destination Port Range** – Indica a(s) porta(s) exteriores que devem obedecer a esta regra.
- **Redirect Target IP** – Ip da máquina para o qual o pedido vai ser redirecionado, neste exemplo refere-se ao IP da máquina que corre o kathara.
- **Redirect Target Port** – Porta a que se deve direccionar o pedido.

Devem ser criadas 2 regras uma, para o filerserver1 e outra para o fileserver2 (**Figura 31**)

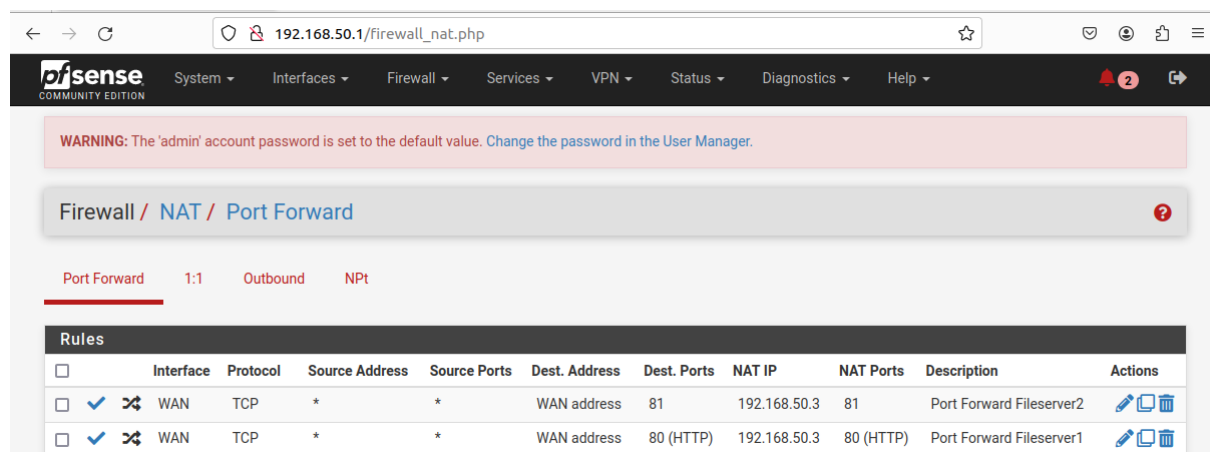


Figura 31 - Regras PortForward Fileservers

Finalmente devemos aceder à página de configuração do nosso router de casa para mapear as portas, disponibilizando estes servidores para a Web.

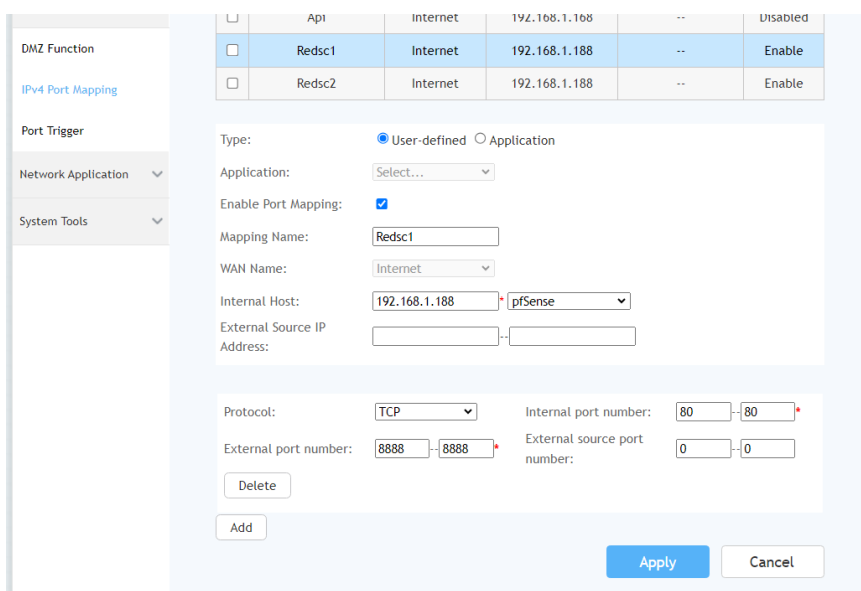


Figura 32 - Port-Forward Fileserver1 Router de casa

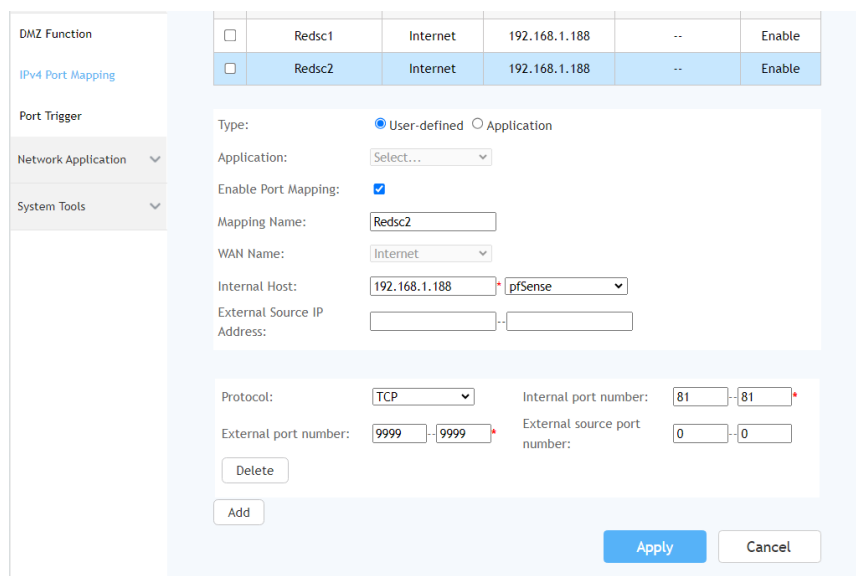


Figura 33 - Port-Forward Fileserver2 Router de casa

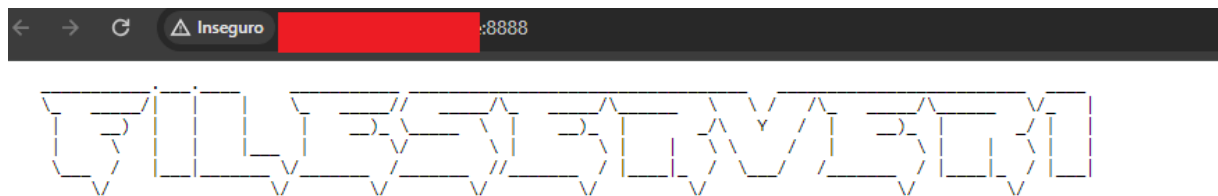


Figura 34 - Fileserver1 acedido externamente

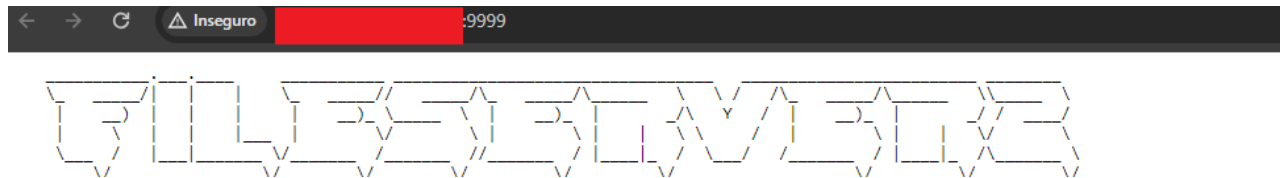


Figura 35 - Fileserver2 acedido externamente

4. Substituir o DNS server pelo fornecido pelo PfSense

Por fim também é requisitado usar o servidor DNS disponibilizado pelo *PfSense* na rede de *kathara*. Para tal devemos primeiramente aceder à página de configuração do mesmo em “*Services/DNS Resolver*” e adicionar os servidores DNS à escolha, tendo nós optado pelo da *cloudflare* e o do ISEP **Figura 36**.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / DNS Resolver

DNS Resolver Infrastructure Cache Speed									
Server	Zone	TTL	Ping	Var	RTT	RTO	Timeout A	Timeout AAAA	Timeout Other
1.1.1.1	.	78	23	13	75	75	0	0	0
193.136.56.9	.	849	21	4	50	50	0	0	0

DNS Resolver Infrastructure Cache Stats									
Server	Zone	eDNS	Lame Known	eDNS Version	Probe Delay	Lame DNSSEC	Lame Rec	Lame A	Lame Other
1.1.1.1	.	1		0	0	0	0	0	0
193.136.56.9	.	1		0	0	0	0	0	0

Figura 36 - Configuração DNS PfSense

Seguidamente, adicionar o IP do *PfSense* à lista presente no ficheiro “*named.conf.options*”.

```
r1.startup  named.conf.options X  lab.conf
KatharaREDSC > r1 > etc > bind > named.conf.options
1 // named.conf.options
2 options {
3     directory "/var/cache/bind";
4     forwarders {
5         193.136.56.9; //dns ISEP
6         192.168.1.1; //dns casa
7         192.168.50.1 //dns PfSense
8     };
9     allow-recursion { any; };
10    dnssec-validation no;
11    listen-on-v6 { any; };
12 };
```

Figura 37 - Configuração "named.conf.options"

Conclusão

Ao longo deste projeto fomos capazes de utilizar os conhecimentos adquiridos ao longo do semestre, assim como nos anos anteriores entre estes encontram-se conhecimentos de DNS, criação de redes, roteamento e roteamento de portas, containers Docker, entre outros.

Acreditamos ter sido capazes de cumprir todos os objetivos propostos com relativa facilidade, devido à nossa capacidade de resolução de problemas e procura de respostas desenvolvida ao longo dos anos.