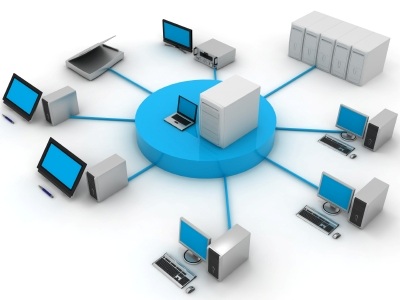
|  |  |
| --- | --- |
| Desenho de bandeira  Descrição gerada automaticamente com confiança média | Universidade da Beira Interior  Licenciatura em Engenharia Informática  **UC: Administração de Sistemas Em Rede** |



Trabalho realizado por:

Manuel Carvalho, nº43760

Bruno Monteiro, nº43994

Alexandre Monteiro, nº44149

Manuel Magalhães, nº44604

**Índice**

[**Introdução** 3](#_Toc103532356)

[**Estrutura da Rede** 4](#_Toc103532357)

[**Equipamentos Utilizados e Respetivas Configurações** 5](#_Toc103532358)

[ **HTTP-DEBIAN-1** 6](#_Toc103532359)

[ **HTTP-DEBIAN-2** 8](#_Toc103532360)

[ **NAS-OMV** 9](#_Toc103532361)

[ **DNS** 10](#_Toc103532362)

[ **DNS2** 10](#_Toc103532363)

[ **R1 (Configuração Firewall)** 11](#_Toc103532364)

[ **VPN** 11](#_Toc103532365)

[ **R1 e Configuração NAT** 15](#_Toc103532366)

[ **NTP** 20](#_Toc103532367)

[**Conclusão** 21](#_Toc103532368)

# **Introdução**

- Foi nos proposto no âmbito da unidade curricular de Administração de Sistemas em Rede, a realização de um trabalho prático que consiste na criação de um pequeno ecosssistema de uma rede na aplicação GNS3.

- A nossa rede possui todos as funcionalidades, quer obrigatória quer facultativa. Todas as configurações dos equipamentos presentes na rede serão explícitos nas secções seguintes.

# **Estrutura da Rede**

Diagrama

Descrição gerada automaticamente

# **Equipamentos Utilizados e Respetivas Configurações**

* **Routers**
* **Switches**
* **Cloud**
* **Computadores**
* **Servidores**
* **HTTP-DEBIAN-1**

- Configuração da interface de rede do servidor **HTTP**

nano /etc/network/interfaces (comentou-se a última linha do file)

clear

rm /etc/network/interfaces.d/50-cloud-init

touch /etc/network/interfaces.d/10-ens4

nano /etc/network/interfaces.d/10-ens4 (adicionou-se a configuração em baixo)

clear

systemctl restart networking

auto ens4

iface ens4 inet static

address 192.168.8.7

netmask 255.255.255.240

gateway 192.168.8.1

up echo nameserver 192.168.8.8 > /etc/resolv.conf

systemctl restart networking

**-** Configuração do serviço **nginx** para permitir o estabelecimento dos sites a criar e respetivas

configurações de forma a a ser possível o acesso ao conteúdo do website (foram estabelicídas difererentes portas para cada um dos sites, www.empresa => porta 80 / www.empresa.com => porta 8080)

mkdir /var/www/html/www.empresa

mkdir /var/www/html/www.empresa.com

(adicionou-se os respetivos ficheiros html para os dois *sites*)

nano /var/www/html/www.empresa/index.html

nano /var/www/html/www.empresa.com/index.html

chown -R www-data:www-data /var/www/html/www.empresa

chown -R www-data:www-data /var/www/html/www.empresa.com

nano /etc/nginx/sites-available/www.empresa.conf

Conteúdo do /etc/nginx/sites-available/www.empresa.conf:

www.empresa

server{

listen 80;

listen [::]:80;

root /var/www/html/www.empresa;

index index.html index.htm;

server\_name www.empresa;

location / {

try\_files $uri $uri/ =404;

}

}

nano /etc/nginx/sites-available/www.empresa.com.conf

Conteúdo do /etc/nginx/sites-available/www.empresa.com.conf

www.empresa.com

server {

listen 80;

listen [::]:80;

root /var/www/html/www.empresa.com;

index index.html index.htm;

server\_name www.empresa.com;

location / {

try\_files $uri $uri/ =404;

}

}

ln -s /etc/nginx/sites-available/www.empresa.conf /etc/nginx/sites-enabled/

ln -s /etc/nginx/sites-available/www.empresa.com.conf /etc/nginx/sites-enabled/

(efetuou-se uma remoção dos ficheiros default que se encontram no nginx)

(criou-se um ficheiro “port.conf” para se possibilitar **ip forwarding** para que o site www.empresa fosse apenas acedido pela porta 8080)

/etc/nginx/sites-available/port.conf <- serve para abrir a porta 8080

server {

listen 80;

server\_name www.empresa;

location /{

proxy\_set\_header X-Forwarded-For $remote\_addr;

proxy\_set\_header Host $http\_host;

proxy\_pass "http://127.0.0.1:8080";

}

}

/etc/init.d/nginx restart => (para que as configurações efetuadas no serviço **nginx** sejam implementadas)

* **HTTP-DEBIAN-2**

- Configuração da interface de rede do servidor **HTTP**

nano /etc/network/interfaces (comentou-se a última linha do file)

clear

rm /etc/network/interfaces.d/50-cloud-init

touch /etc/network/interfaces.d/10-ens4

nano /etc/network/interfaces.d/10-ens4 (adicionou-se a configuração em baixo)

clear

systemctl restart networking

auto ens4

iface ens4 inet static

address 8.8.8.2

netmask 255.255.255.240

gateway 8.8.8.1

up echo nameserver 8.8.8.8 > /etc/resolv.conf

systemctl restart networking

mkdir /var/www/html/www.sysadmintools.net

(criou-se o ficheiro html respetivo para o site)

nano /var/www/html/www.sysadmintools.net/index.html

chown -R www-data:www-data /var/www/html/www.sysadmintools.net

ln -s /etc/nginx/sites-available/www.sysadmintools.net.conf /etc/nginx/sites-enabled/

(removeu-se os ficheiros default do **nginx**)

/etc/init.d/nginx restart => (para que as configurações efetuadas no serviço **nginx** sejam implementadas)

* **NAS-OMV**

1. **Cliente HTTP-DEBIAN-1**

(instalar NFS FileSystem)

sudo apt update

sudo apt install nfs-common

mkdir /var/backups/websites/

mount -t 192.168.8.6:/EmpresaSharedFolder /var/backups/websites/

(criar um script para efetuar operações de backup)

nano /usr/local/bin/make\_backup.sh

(conteúdo do script)

TEMP=$(mktemp -d)

DATE=$(date +%A)

mount /var/backups/websites

tar cpzvf "$TEMP/$DATE".tgz /var/www/

cp "$TEMP/$DATE".tgz /var/backups/websites

crontab -e

(conteúdo no crontab file)

00 04 \* \* \* /usr/local/bin/make\_backup.sh

1. **Cliente ADMIN-UBUNTU**

(colocar no navegador o IP do servidor NAS e efetuar as alterações que sejam pretendidas => aceder à página do openmediavault**)**

2. Servidor NAS-OMV

(seguir passos de instalação default de um NAS Server => utilização do openmediavault)

* **DNS**

nano /etc/hosts

192.168.8.7 www.empresa

192.168.8.7 www.empresa.com

nano /etc/dnsmasq.conf

no-resolv

server=8.8.8.8

listen-address=::1,127.0.0.1,192.168.8.8

sudo systemctl start dnsmasq => para iniciar o **servidor de DNS**

* **DNS2**

nano /etc/hosts

8.8.8.2 www.sysadmintools.net

nano /etc/dnsmasq.conf

no-resolv

server=8.8.4.4

listen-address=::1,127.0.0.1,8.8.8.8

sudo systemctl start dnsmasq => para iniciar o **servidor de DNS**

* **R1 (Configuração Firewall)**

access-list 103 deny tcp any host 192.168.8.7 eq 8080

access-list 103 permit ip any any

ip access-group 103 in <- entradas de fora do router

(não permite passar tráfego de e para a porta 8080)

(visualização de logs de bloqueios no router)

show logging

* **VPN**

1. **Servidor**

(instalação do **OpenVPN** para serviços de VPN)

wget https://raw.githubusercontent.com/angristan/openvpn-install/master/openvpn-install.sh -O openvpn-install.sh

sudo bash openvpn-install.sh

1. **Cliente**

sudo su

wget -O - https://swupdate.openvpn.net/repos/repo-public.gpg|apt-key add -

echo “deb http://build.openvpn.net/debian/openvpn/stable xenial main” > /etc/apt/sources.list.d/openvpn-aptrepo.list

apt-get update && apt-get install openvpn

openvpn Vpn.ovpn

(as configurações do serviço **VPN** encontram-se nos trechos de comandos seguintes colocados no file **vpnopn**)

client

proto udp

explicit-exit-notify

remote 192.168.8.9 1194

dev tun

script-security 2

up /etc/openvpn/update-resolv-conf

down /etc/openvpn/update-resolv-conf

resolv-retry infinite

nobind

persist-key

persist-tun

remote-cert-tls server

verify-x509-name server\_2eIXRgMUEtkScEjJ name

auth SHA256

auth-nocache

cipher AES-128-GCM

tls-client

tls-version-min 1.2

tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256

ignore-unknown-option block-outside-dns

setenv opt block-outside-dns # Prevent Windows 10 DNS leak

verb 3

<ca>

-----BEGIN CERTIFICATE-----

MIIB1zCCAX2gAwIBAgIUcIziAz2pBF1hp/4nJaCoUfNhY9MwCgYIKoZIzj0EAwIw

HjEcMBoGA1UEAwwTY25fQkhOVmJ4OVJtZDJOTUZqdTAeFw0yMjA1MTMyMDQzNDJa

Fw0zMjA1MTAyMDQzNDJaMB4xHDAaBgNVBAMME2NuX0JITlZieDlSbWQyTk1GanUw

WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATXB6KuacxZqAI5563IHwxjbkDle+3l

7ej4oP0gwoXgkAybAtZgrz1RWKuiEAPLoxpMEwc8ZnGtVYzfb4/wPUuho4GYMIGV

MB0GA1UdDgQWBBQTrEPNouSyTbrHz68rRFlLSmttKDBZBgNVHSMEUjBQgBQTrEPN

ouSyTbrHz68rRFlLSmttKKEipCAwHjEcMBoGA1UEAwwTY25fQkhOVmJ4OVJtZDJO

TUZqdYIUcIziAz2pBF1hp/4nJaCoUfNhY9MwDAYDVR0TBAUwAwEB/zALBgNVHQ8E

BAMCAQYwCgYIKoZIzj0EAwIDSAAwRQIhANeYY61JMMSNpNF/r07L8uEpaXGPZUoz

mGxN4mqWKbArAiAIF9jKExx407ZR2EFvtHojRbhw1usquYoOBaQ2G/CGnA==

-----END CERTIFICATE-----

</ca>

<cert>

-----BEGIN CERTIFICATE-----

MIIB1jCCAXugAwIBAgIQQ5NJb1Xt8cohXTPAv3/i5TAKBggqhkjOPQQDAjAeMRww

GgYDVQQDDBNjbl9CSE5WYng5Um1kMk5NRmp1MB4XDTIyMDUxMzIwNDQxMVoXDTI0

MDgxNTIwNDQxMVowDjEMMAoGA1UEAwwDVlBOMFkwEwYHKoZIzj0CAQYIKoZIzj0D

AQcDQgAE4lugWxf1JX4IOyvz4QimYwqLkHXxfvoEpymlyU4WvqLVR/Zx7Up6w90T

QQQqHXPw+l326t7N285OPpVcaHknPKOBqjCBpzAJBgNVHRMEAjAAMB0GA1UdDgQW

BBT/EFRG8tZe+/wvMgyz2rYTfdw7UzBZBgNVHSMEUjBQgBQTrEPNouSyTbrHz68r

RFlLSmttKKEipCAwHjEcMBoGA1UEAwwTY25fQkhOVmJ4OVJtZDJOTUZqdYIUcIzi

Az2pBF1hp/4nJaCoUfNhY9MwEwYDVR0lBAwwCgYIKwYBBQUHAwIwCwYDVR0PBAQD

AgeAMAoGCCqGSM49BAMCA0kAMEYCIQCIhTs70+xbKJSPmmD5TDGXUJ/Om3mhB/SB

4x/aSXeGZQIhAKmq0CW+sB/avL8iaY7Ld83d/GvrAWjCNMDuuX6908XC

-----END CERTIFICATE-----

</cert>

<key>

-----BEGIN PRIVATE KEY-----

MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgjAeMen6IiM0DKRXB

cm8MVFZLyDw2p79mg+8ap0nKFtGhRANCAATiW6BbF/Ulfgg7K/PhCKZjCouQdfF+

+gSnKaXJTha+otVH9nHtSnrD3RNBBCodc/D6Xfbq3s3bzk4+lVxoeSc8

-----END PRIVATE KEY-----

</key>

<tls-crypt>

-----BEGIN OpenVPN Static key V1-----

c722137af69db9a0ab0ec2e824c9c983

a821205c2f8e346807f9bdef275aa6cc

802599c11edeaeec2db6d7bb813e1a1c

e96961d8eef2a58d4211bc9d0db7ee99

6be737c23eb9019676d57dfa6948c5f3

0c851d7ac5c6cc948ff232153845d256

2aef472a96da8686d222daaf9362ec83

56618eeead011afad0f56e692744ba09

b6233909c9d424ab014753e6335dacdf

ab9f9302538b4ed02f4b54b155d89301

39013749956ca5c0a1ac2e6c8c99b246

9c5960ebc79dfad97e95be12d5ced4ab

3e75b8e45fe8b566d4124481c8cb2791

3ccfb00181dc46801883bce6d175189d

aa08e7c2555a9484ac768059ba16b429

01cb11fdf5db710356228bf96b2fc41c

-----END OpenVPN Static key V1-----

</tls-crypt>

* **R1 e Configuração NAT**

Current configuration : 3642 bytes

!

version 15.9

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Router

!

boot-start-marker

boot-end-marker

!

!

!

no aaa new-model

!

!

!

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

!

!

!

!

!

no ip icmp rate-limit unreachable

!

!

!

!

!

!

no ip domain lookup

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

interface GigabitEthernet0/0

ip address 192.168.8.1 255.255.255.240

ip nat inside

ip virtual-reassembly in

duplex auto

speed auto

media-type rj45

!

interface GigabitEthernet0/1

ip address 8.8.8.1 255.255.255.240

ip access-group 103 in

ip nat inside

ip virtual-reassembly in

duplex auto

speed auto

media-type rj45

!

interface GigabitEthernet0/2

no ip address

shutdown

duplex auto

speed auto

media-type rj45

!

interface GigabitEthernet0/3

ip address dhcp

ip access-group 103 in

ip nat outside

ip virtual-reassembly in

duplex auto

speed auto

media-type rj45

!

ip forward-protocol nd

!

!

no ip http server

ip nat pool REDEMARELA 192.168.1.20 192.168.1.125 netmask 255.255.255.0

ip nat pool REDAZUL 10.0.0.20 10.0.0.125 netmask 255.255.255.0

ip nat inside source list 1 pool REDEMARELA overload

ip nat inside source list 2 pool REDAZUL overload

!

ipv6 ioam timestamp

!

!

access-list 1 permit 192.168.8.0 0.0.0.15

access-list 2 permit 8.8.8.0 0.0.0.15

access-list 103 deny tcp any host 192.168.8.7 eq 8080 log

access-list 103 permit ip any any

!

control-plane

!

banner exec ^C

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* IOSv is strictly limited to use for evaluation, demonstration and IOS \*

\* education. IOSv is provided as-is and is not supported by Cisco's \*

\* Technical Advisory Center. Any use or disclosure, in whole or in part, \*

\* of the IOSv Software or Documentation to any third party for any \*

\* purposes is expressly prohibited except as otherwise authorized by \*

\* Cisco in writing. \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*^C

banner incoming ^C

\* IOSv is strictly limited to use for evaluation, demonstration and IOS \*

\* education. IOSv is provided as-is and is not supported by Cisco's \*

\* Technical Advisory Center. Any use or disclosure, in whole or in part, \*

\* of the IOSv Software or Documentation to any third party for any \*

\* purposes is expressly prohibited except as otherwise authorized by \*

\* Cisco in writing. \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*^C

banner login ^C

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* IOSv is strictly limited to use for evaluation, demonstration and IOS \*

\* education. IOSv is provided as-is and is not supported by Cisco's \*

\* Technical Advisory Center. Any use or disclosure, in whole or in part, \*

\* of the IOSv Software or Documentation to any third party for any \*

\* purposes is expressly prohibited except as otherwise authorized by \*

\* Cisco in writing. \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*^C

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

line vty 0 4

login

transport input none

!

no scheduler allocate

!

end

* **NTP**

(instalar serviço **NTP**) => sudo apt install ntp

1. **Servidor**

nano /etc/ntp.conf

driftfile /var/lib/ntp/ntp.drift

server 0.pool.ntp.org

server 1.pool.ntp.org

server 2.pool.ntp.org

server 3.pool.ntp.org

restrict 192.168.8.0 mask 255.255.255.240 nomodify notrap

restrict 127.0.0.1

timectl set-ntp on

systemctl restart ntp

watch ntpq -p <- ver a sincronização ao vivo

1. **Cliente**

nano /etc/hosts

192.168.8.5 ntp-host

nano /etc/ntp.conf

driftfile /var/lib/ntp/ntp.drift

server 192.168.8.5

restrict 127.0.0.1

timedatectl set-ntp on

systemctl restart ntp

watch ntpq -p <- ver a sincronização ao vivo

(setup do clock **NTP**)

# **Conclusão**

**-** Com este trabalho foi possível aprender sobre a virtualização e uso do GNS3 sendo este um ambiente mais realista do comportamento de uma rede.

- Para além disso conseguimos desenvolver novas capacidades de desenvolvimento de uma rede.