

## **Projeto Redes de Dados**

Bruno Alexandre Lopes Ferreira - 2211024

Ricardo Bento Santos - 2212946

Trabalho de Projeto da unidade curricular de Rede de Dados

Leiria, junho 2023



# Índice

<b>1.</b>	<b>Introdução.....</b>	<b>1</b>
<b>2.</b>	<b>Packet Tracer.....</b>	<b>2</b>
<b>3.</b>	<b>Deteção Ciberataques .....</b>	<b>Erro! Marcador não definido.</b>
<b>4.</b>	<b>Conclusão .....</b>	<b>Erro! Marcador não definido.</b>

# **1. Introdução**

Este relatório tem como propósito explicar detalhadamente todas as decisões tomadas na implementação do ambiente descrito no enunciado e no algoritmos de deep learning de cibersegurança.

## 2. Packet Tracer

De modo a implementar a sede e as suas filiais utilizando o menor número de endereços possíveis, optamos por endereçar primeiro as redes locais, começando pela de maior dimensão até à de menor. (Vendas > Recursos Humanos > Administração)

**Vendas - 32 PCs** ->  $2^6$  -> 6 bits ->  $32-6 = /26$  -> **255.255.255.192**

**Recursos Humanos - 20 PCs** ->  $2^5$  -> 5 bits ->  $32-5 = /27$  -> **255.255.255.224**

**Administração - 10 PCs** ->  $2^4$  -> 4 ->  $32-4 = /28$  -> **255.255.255.240**

### Sede – Rede Vendas

10.10.0.0

10.10.0.1 | fa0/0.10 Router Sede Internet

10.10.0.62 | fa0/0.10 Router Sede Vendas

10.10.0.63

### Filial 1 – Rede Vendas

10.10.0.64

10.10.0.65 | fa0/0.10 Router F.1 Internet

10.10.0.126 | fa0/0.10 Router F.1 Vendas

10.10.0.127

### Filial 2 – Rede Vendas

10.10.0.128

10.10.0.129 | fa0/0.10 Router F.2 Internet

10.10.0.19 | fa0/0.10 Router F.2 Vendas

10.10.0.191

### Sede - Recursos Humanos

10.10.0.192

10.10.0.193 | fa0/0.20 Router Sede Internet

10.10.0.222 | fa0/0.20 Router Sede Vendas

10.10.0.223

### **Filial 1 - Recursos Humanos**

10.10.0.224

10.10.0.225 | fa0/0.20 Router F.1 Internet

10.10.0.254 | fa0/0.20 Router F.1 Vendas

10.10.0.255

### **Filial 2 - Recursos Humanos**

10.10.1.0

10.10.1.1 | fa0/0.20 Router F.2 Internet

10.10.1.30 | fa0/0.20 Router F.2 Vendas

10.10.1.31

### **Sede - Administração**

10.10.1.32

10.10.1.33 | fa0/0.30 Router Sede Internet

10.10.1.46 | fa0/0.30 Router Sede Vendas

10.10.1.47

### **Filial 1 - Administração**

10.10.1.48

10.10.1.49 | fa0/0.30 Router F.1 Internet

10.10.1.62 | fa0/0.30 Router F.1 Vendas

10.10.1.63

### **Filial 2 – Administração**

10.10.1.64

10.10.1.65 | fa0/0.30 Router F.2 Internet

10.10.1.78 | fa0/0.30 Router F.2 Vendas

10.10.1.79

De modo ao Router Internet da Sede e as suas Filiais ter uma interface para conexão externa foram adicionados os seguintes ip's:

10.10.1.80 (/30)

10.10.1.81	se0/0/0.1	Router F.1 Internet
10.10.1.82	se0/1/0.1	Router Sede Internet

10.10.0.82

10.10.1.84 (/30)

10.10.1.85	se0/0/0.1	Router F.2 Internet
10.10.1.86	se0/1/0.2	Router Sede Internet

10.10.0.87

Por último foi feito o endereçamento da conexão com a ISP do Router Internet da Sede e dos servidores situados na Sede:

10.10.1.88 (/29)

10.10.1.89	fa0/0	Server Ficheiros
10.10.1.90	fa0/0	Server Página Web
10.10.1.91	fa0/0	Router Sede Internet
10.10.1.92	fa0/0	Server DNS

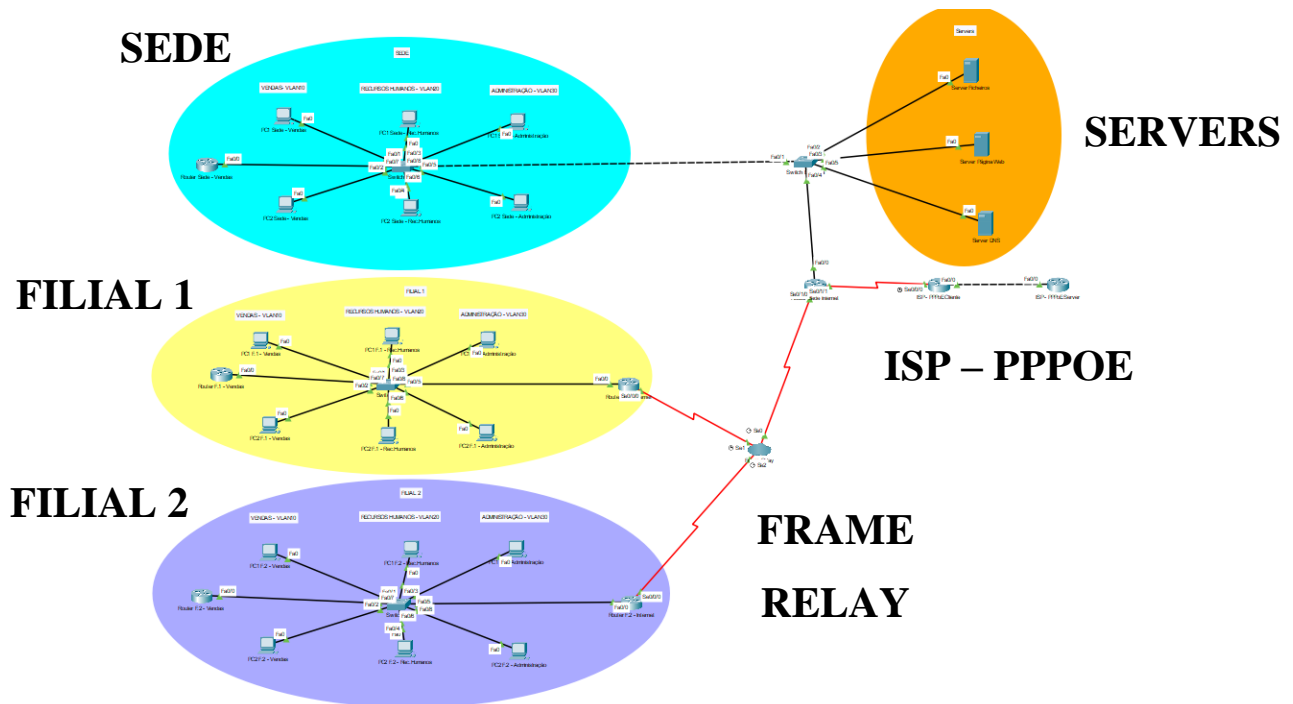
10.10.1.95

10.10.1.96 (/29)

10.10.1.97	se0/1/1	Router Sede Internet
10.10.1.98	se0/0/0	Router PPoE Cliente
(pool) 10.10.1.99-101	fa0/0	Router PPoE Cliente
10.10.1.102	fa0/0	Router PPoE Server

10.10.1.103

De acordo com o endereçamento esta foi a topologia que optamos:



De modo a implementar o parâmetro “As configurações IP de toda a empresa devem ser obtidas por DHCP alojado no router das Vendas”, optamos por implementar um Router Vendas em cada uma das localizações, responsável por atribuir ip’s localmente aos pc’s de cada rede local através de DHCP. Já os ip’s das interfaces dos routers vendas e internet são configurados estaticamente e manualmente.

Os servidores implementados foram:

- Ficheiros (impossível comunicar para fora da Sede e Filiais)
- Página Web
- DNS (para poder aceder à página)

Também foi implementado acesso aos routers locais por ssh apenas para a rede local da administração, assim como redes vendas apenas conseguem comunicar com a própria, tanto num contexto local ou remoto (Layer 2 e Layer 3).

Para haver conectividade entre os locais remotos da empresa foi implementado a tecnologia Frame Relay e nos routers internet das filiais e da sede foi usado o protocolo de roteamento OSPF.



Por último o router internet da sede responsável pela comunicação com a ISP, faz a tradução de endereços internos para “10.10.1.97” através do NAT. E a conexão com a ISP é feita por PPPoE.

## Configuração Router Vendas (Sede e Filiais)

- Como se pode ver pela figura, a topologia adotada localmente tanto para a Sede com as Filiais, é a ligação dos pc's a switch com as respetivas vlans em cada interface (Trunk em interfaces que ligadas aos routers)

- Vendas – vlan 10

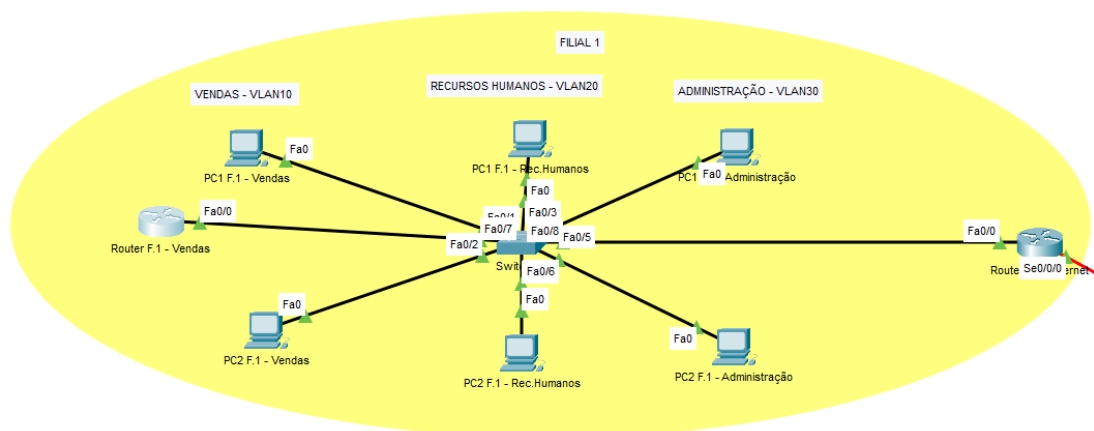
- Recursos Humanos – vlan 20

- Administração – vlan 30

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	10	--	000C.CF38.A0E5
FastEthernet0/2	Up	10	--	0004.9AAC.69E3
FastEthernet0/3	Up	20	--	0060.7001.5E40
FastEthernet0/4	Up	20	--	00D0.FF92.CB77
FastEthernet0/5	Up	30	--	0060.5C9D.9D31
FastEthernet0/6	Up	30	--	0005.5EA0.0656
FastEthernet0/7	Up	--	--	000C.CF36.6320
FastEthernet0/8	Up	--	--	0001.422E.B161

- De modo a obterem ip's foram criadas pools no router vendas para cada uma das redes. (default gateway = ip sub-interface router internet)
- E foram excluidos os ip's usados nas sub-interfaces tanto do router vendas (próprio DHCP) como no router internet

```
ip dhcp pool VENDAS-POOL
network 10.10.0.64 255.255.255.192
default-router 10.10.0.65
dns-server 10.10.1.92
ip dhcp pool REC_HUMANOS-POOL
network 10.10.0.224 255.255.255.224
default-router 10.10.0.225
dns-server 10.10.1.92
ip dhcp pool ADMINISTRACAO
network 10.10.1.48 255.255.255.240
default-router 10.10.1.49
dns-server 10.10.1.92
ip dhcp excluded-address 10.10.0.65
ip dhcp excluded-address 10.10.0.126
ip dhcp excluded-address 10.10.0.225
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.1.49
ip dhcp excluded-address 10.10.1.62
```

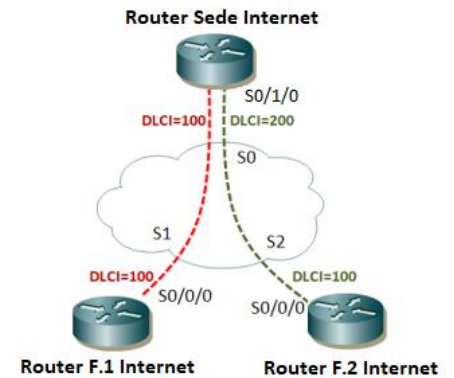


## Configuração Frame Relay

- A imagem representa a configuração da cloud:

Frame Relay

Serial0	Sede-F1	<->	Serial0	Sede-F1
Port	Sublink		Port	Sublink
1	Serial0		Serial1	F1-Sede
2	Serial0		Serial2	F2-Sede



- Na interface se0/1/0 do Router Internet Sede foi ativado a encapsulação frame-relay, definido os ip's nas sub-interfaces e associada a interface do frame-relay na respetiva sub-interface.
- O mesmo foi feito nos routers internet das filiais

```
interface Serial0/1/0
no ip address
encapsulation frame-relay
!
interface Serial0/1/0.1 point-to-point
ip address 10.10.1.82 255.255.255.252
frame-relay interface-dlci 100
ip nat inside
clock rate 2000000
!
interface Serial0/1/0.2 point-to-point
ip address 10.10.1.86 255.255.255.252
frame-relay interface-dlci 200
ip nat inside
clock rate 2000000
!
```

```
interface Serial0/0/0
no ip address
encapsulation frame-relay
!
interface Serial0/0/0.1 point-to-point
ip address 10.10.1.81 255.255.255.252
frame-relay interface-dlci 100
clock rate 2000000
!
```

```
interface Serial0/0/0
no ip address
encapsulation frame-relay
!
interface Serial0/0/0.1 point-to-point
ip address 10.10.1.85 255.255.255.252
frame-relay interface-dlci 100
clock rate 2000000
!
```

## Configuração NAT Router Internet Sedes

- De modo a traduzir os ip's internos quando necessitam de fazer comunicações externas através da ISP, foi configurado o router para trocar os ip's para o do NAT:

```
access-list 1 deny host 10.10.1.89
access-list 1 permit 10.10.0.0 0.0.1.255
access-list 1 deny any
```

```
ip nat inside source list 1 interface Serial0/1/1 overload
```

- Para cada interface do router conectada à rede local ser traduzia foi usado o comando "ip nat inside" em cada uma delas.

- Exemplo comunicação PC1 Vendas Sede para ISP:

```
Router-Internet-Sede#show ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
icmp 10.10.1.97:1       10.10.0.2:1       10.10.1.102:1     10.10.1.102:1
```

- A ACL usada no NAT era suposto bloquear o ip do servidor de ficheiros de ser traduzido, mas como a tradução ocorre mais rápido não funcionou, então bloqueamos com outra ACL a comunicação com ISP do servidor de ficheiros.

```
access-list 102 deny ip any host 10.10.1.89
access-list 102 permit ip any any
```

- A conexão estabelecida com o Router Cliente PPPoE ISP, foi feita através de ligação serial PPP c/ CHAP, com a seguintes configurações:

```
interface Serial0/1/1
ip address 10.10.1.97 255.255.255.248
encapsulation ppp
ppp authentication chap
ip access-group 102 in
ip nat outside
!

interface Serial0/0/0
ip address 10.10.1.98 255.255.255.248
encapsulation ppp
ppp authentication chap
clock rate 2000000
.
```

## Configuração Protocolo Roteamento – OSPF

- Para todos os routers internet, de modo a evitar o uso de rotas estáticas foi implementado o protocolo OSPF. Devido a haver poucas redes foi considerado uma área 0 para todo o ambiente, sendo que em cada router foi introduzido os comandos:
  - network – para as redes de cada interface (ou sub-interface)
  - passive-interface – para a rede local (p.e Router Internet F.1 – passive-interface fa0/0.10 ...) e ISP (caso da sede)
  - router-id – foi dado o maior ao Router Internet Sede de modo a ser o DR

- Exemplo Router Internet F.1:

```
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
passive-interface FastEthernet0/0
passive-interface FastEthernet0/0.3
passive-interface FastEthernet0/0.10
passive-interface FastEthernet0/0.20
network 10.10.0.64 0.0.0.63 area 0
network 10.10.0.224 0.0.0.31 area 0
network 10.10.1.48 0.0.0.15 area 0
network 10.10.1.80 0.0.0.3 area 0
!
```

## Configuração PPPoE ISP

- De modo a implementar o PPPoE optamos por cria-la na conexão ISP, com um Router Cliente PPPoE ISP e Router Server PPPoE ISP, a conexão entre estes routers é feita com recurso ao PPPoE.
- No cliente foi configurado o Dialer para receber ip da pool do server, este foi associado à interface que está conectada ao server e criado uma rota para encaminhar todo o tráfego pelo Dialer.

```

interface Dialer1
  dialer pool 1
  ip address negotiated
  mtu 1492
  encapsulation ppp
  ppp chap hostname PPPoE-Cliente
  ppp chap password cisco
!

ip route 0.0.0.0 0.0.0.0 Dialer1

interface FastEthernet0/0
  no ip address
  pppoe enable
  pppoe-client dial-pool-number 1
  duplex auto
  speed auto
!
```

- No server foi criado uma pool com os endereços a dar ao cliente, depois foi criado a virtual-template 1 onde foi adicionado a pool, a interface e o metodo de encapsulamento ppp com chap e por último, associado a virtual-template ao bba-group pppoe e definido o ip à respetiva interface e associado o group pppoe (também foi definido username e password, iguais às criadas no cliente)

```

bba-group pppoe global
  virtual-template 1
!
interface Virtual-Template1
  peer default ip address pool client-pool
  ip unnumbered FastEthernet0/0
  encapsulation ppp
  ppp authentication chap
!

interface FastEthernet0/0
  ip address 10.10.1.102 255.255.255.248
  pppoe enable group global
  duplex auto
  speed auto
!

ip local pool client-pool 10.10.1.99 10.10.1.101
```

- Para complementar a configuração feita de modo a poder comunicar com os pc's da sede e filiais foram adicionadas as seguintes rotas (para o router cliente e internet sede)

```

ip route 10.10.1.97 255.255.255.255 10.10.1.99
ip route 10.10.1.98 255.255.255.255 10.10.1.99

PPPoE-Cliente#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	10.10.1.98	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Virtual-Access1	unassigned	YES	unset	up	up
Virtual-Access2	unassigned	YES	manual	up	up
Dialer1	10.10.1.99	YES	IPCP	up	up
Vlan1	unassigned	YES	unset	administratively down	down

## Configuração Servidor Página Web

- De modo a mostrar a página web da empresa foi criado um servidor DNS para traduzir o ip do servidor página web para o url. (apenas https permitido)

HTTP ☐ On ☒ Off

HTTPS ☒ On ☐ Off

No.	Name	Type	Detail
0	empresa.pt	A Record	10.10.1.90

No.	Name	Type	Detail
0	empresa.pt	A Record	10.10.1.90

File Manager

	File Name	Edit	Delete
1	cscoptlogo177x111.jpg		(delete)
2	index.html	(edit)	(delete)


PC1 Sede - Administração

Physical Config **Desktop** Programming Attributes

Web Browser

< > URL  Go Stop

Página Empresa



## Configuração ACL's Redes

- Como foi dito no enunciado, redes locais apenas conseguem comunicar entre si, p.e vendas com vendas, administração com administração... De modo a complementar esta ideia, achamos por bem, implemeta-la para além do contexto local, ou seja, a rede vendas apenas consegue comunicar com rede vendas mesmo que seja com outra filial ou a sede.
- Para isso estabelecemos ACL's (nos routers internte) que bloqueiam o tentativas de comunicação entre redes diferentes localmente e remotamente.
- P.e Filial 1:

```
interface FastEthernet0/0.3
 encapsulation dot1Q 30
 ip address 10.10.1.49 255.255.255.240
 ip access-group PROIBIR_ADMIN in
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.0.65 255.255.255.192
 ip access-group PROIBIR_SSH_VENDAS in
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.10.0.225 255.255.255.224
 ip access-group PROIBIR_SSH_RECHUMANOS in
!
```

**Nota:** Encontram-se entradas para conectividade SSH, o que irá ser explicado a seguir.

```
ip access-list extended PROIBIR_SSH_RECHUMANOS
deny tcp 10.10.0.224 0.0.0.31 host 10.10.0.225 eq 22
deny tcp 10.10.0.224 0.0.0.31 host 10.10.0.65 eq 22
deny tcp 10.10.0.224 0.0.0.31 host 10.10.1.49 eq 22
deny ip 10.10.0.224 0.0.0.31 10.10.0.64 0.0.0.63
deny ip 10.10.0.224 0.0.0.31 10.10.1.48 0.0.0.15
deny ip 10.10.0.224 0.0.0.31 10.10.0.0 0.0.0.63
deny ip 10.10.0.224 0.0.0.31 10.10.0.128 0.0.0.63
deny ip 10.10.0.224 0.0.0.31 10.10.1.32 0.0.0.15
deny ip 10.10.0.224 0.0.0.31 10.10.1.64 0.0.0.15
permit ip any any

ip access-list extended PROIBIR_SSH_VENDAS
deny tcp 10.10.0.64 0.0.0.63 host 10.10.0.65 eq 22
deny tcp 10.10.0.64 0.0.0.63 host 10.10.1.49 eq 22
deny tcp 10.10.0.64 0.0.0.63 host 10.10.0.225 eq 22
deny ip 10.10.0.64 0.0.0.63 10.10.0.224 0.0.0.31
deny ip 10.10.0.64 0.0.0.63 10.10.1.48 0.0.0.15
deny ip 10.10.0.64 0.0.0.63 10.10.0.192 0.0.0.31
deny ip 10.10.0.64 0.0.0.63 10.10.1.0 0.0.0.31
deny ip 10.10.0.64 0.0.0.63 10.10.1.32 0.0.0.15
deny ip 10.10.0.64 0.0.0.63 10.10.1.64 0.0.0.15
permit ip any any

ip access-list extended PROIBIR_ADMIN
deny ip 10.10.1.48 0.0.0.15 10.10.0.64 0.0.0.63
deny ip 10.10.1.48 0.0.0.15 10.10.0.224 0.0.0.31
deny ip 10.10.1.48 0.0.0.15 10.10.0.0 0.0.0.63
deny ip 10.10.1.48 0.0.0.15 10.10.0.128 0.0.0.63
deny ip 10.10.1.48 0.0.0.15 10.10.0.192 0.0.0.31
deny ip 10.10.1.48 0.0.0.15 10.10.1.0 0.0.0.31
permit ip any any
```

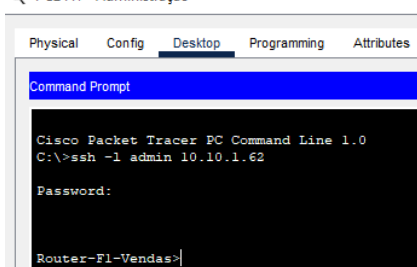
## Configuração SSH – Administração

- Para complementar o projeto, achamos que seria realista a rede de administração ter acesso por ssh aos routers, ou seja, ao router vendas e internet, tanto na sede como nas filiais.
- Para isso foi configurado o ssh nos routers, e depois estabelecido ACL's para apenas permitir os administradores.
- Ex: Filial 1 Router Vendas (Router Internet pode ser vista pelas imagens anteriores)

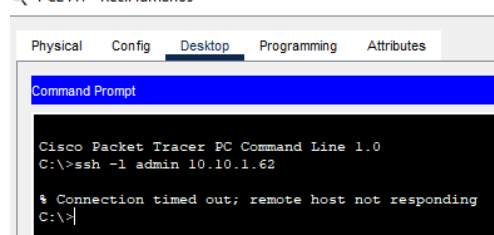
```
ip domain name admin
crypto key generate rsa ; 1024
enable password cisco
username admin password admin
ip ssh version 2
line vty 0 15
transport input ssh
login local
```

```
ip access-list extended PROIBIR_SSH_RECHUMANOS
deny tcp 10.10.0.224 0.0.0.31 host 10.10.0.254 eq 22
deny tcp 10.10.0.64 0.0.0.63 host 10.10.0.254 eq 22
permit ip any any
ip access-list extended PROIBIR_SSH_VENDAS
deny tcp 10.10.0.64 0.0.0.63 host 10.10.0.126 eq 22
deny tcp 10.10.0.224 0.0.0.31 host 10.10.0.126 eq 22
permit ip any any
ip access-list extended PROIBIR_SSH_VENDAS_RECH
deny tcp 10.10.0.64 0.0.0.63 host 10.10.1.62 eq 22
deny tcp 10.10.0.224 0.0.0.31 host 10.10.1.62 eq 22
permit ip any any
```

PC2 F.1 - Administração



PC2 F.1 - Rec.Humanos



### 3. Detecção Ciberataques

Com o material fornecido, implementamos o algoritmo para datasets diferentes com cerca de 50 mil imagens (com a distribuição 80% teste e 20% validação indicada):

- Bruno – 50106 entradas:
  - 74% Malignos
  - 26% Benignos
- Ricardo – 49992 entradas:
  - 55% Malignos
  - 45% Benignos

De modo a automatizar a divisão das imagens criadas pelo algoritmo que lê o ficheiro excel, mudamos o código para que, consoante o número de imagens criadas tanto para malignos ou benignos as divida para testes ou implementação:

1. Obtêm-se o número de imagens da validação para benignos e malignos
2. Criado variáveis de contagem do número de imagens criadas para benignos e malignos (percent\_benignos e percent\_maligno)
3. Durante o loop de cada linha é verificado qual o tipo de tráfego, se o número de imagens criadas para aquele tipo de tráfego é menor que as imagens necessárias para a validação cria na pasta validação, se maior passa para a pasta do teste.
4. Por último, é adicionado ao caminho da imagem o seu nome

```
num_validacao_benigno = round(c_B * 0.20)
num_validacao_maligno = round(c_M * 0.20)
```

```
if M_M[index] == 0:
    percent_benigno += 1
    if (percent_benigno <= num_validacao_benigno):
        meupath2 += "D:\\RD-PROJETO\\testesCiberataques\\Scripts\\data\\validacao\\" + str(M_M[index])
    elif (percent_benigno <= num_benignos):
        meupath2 += "D:\\RD-PROJETO\\testesCiberataques\\Scripts\\data\\treino\\" + str(M_M[index])
elif M_M[index] == 1:
    percent_maligno += 1
    if (percent_maligno <= num_validacao_maligno):
        meupath2 += "D:\\RD-PROJETO\\testesCiberataques\\Scripts\\data\\validacao\\" + str(M_M[index])
    elif (percent_maligno <= num_malignos):
        meupath2 += "D:\\RD-PROJETO\\testesCiberataques\\Scripts\\data\\treino\\" + str(M_M[index])

meupath2 += "\\" + str(M_M[index]) + "_" + str(index) + ".jpg"
```



Após serem criadas as imagens, é executado o algoritmo de deep learning. Ambos experimentamos várias combinações das variáveis **neurónios**, **bach size**, **numero epoch's** e **validation\_split** de modo a obter o mais próximo dos 100%.

### Valores máximos:

- **Bruno – 96% treino e validação**

```
Epoch 1/40
1065/1065 - 87s - loss: 0.3666 - accuracy: 0.8684 - val_loss: 0.3426 - val_accuracy: 0.8842 - 87s/epoch - 81ms/step
Epoch 2/40
1065/1065 - 65s - loss: 0.2283 - accuracy: 0.9193 - val_loss: 0.2063 - val_accuracy: 0.9341 - 65s/epoch - 61ms/step

Epoch 39/40
1065/1065 - 52s - loss: 0.1328 - accuracy: 0.9605 - val_loss: 0.1445 - val_accuracy: 0.9601 - 52s/epoch - 49ms/step
Epoch 40/40
1065/1065 - 52s - loss: 0.1331 - accuracy: 0.9602 - val_loss: 0.1390 - val_accuracy: 0.9611 - 52s/epoch - 49ms/step
```

```
num_classes = 2
N_Epoch = 40
N_Neuronio = 100
batch_size = 32
img_height = 1000
img_width = 11

train_ds = tf.keras.utils.image_dataset_from_directory(
    "D:\\RD-PROJETO\\testesCiberataques\\Scripts\\data\\treino",
    validation_split=0.20,
    subset="training",
    seed=123,
    image_size=(img_height, img_width),
    batch_size=batch_size)

val_ds = tf.keras.utils.image_dataset_from_directory(
    'D:\\RD-PROJETO\\testesCiberataques\\Scripts\\data\\validacao',
    validation_split=0.20,
    subset="validation",
    seed=123,
    image_size=(img_height, img_width),
    batch_size=batch_size)
```

- **Ricardo – 92% treino e validação**

```
Epoch 1/200
684/684 - 79s - loss: 0.5826 - accuracy: 0.8124 - val_loss: 0.3555 - val_accuracy: 0.8500 - 79s/epoch - 116ms/step
Epoch 2/200
684/684 - 75s - loss: 0.3410 - accuracy: 0.8709 - val_loss: 0.2636 - val_accuracy: 0.9132 - 75s/epoch - 110ms/step
Epoch 39/200
684/684 - 74s - loss: 0.2096 - accuracy: 0.9269 - val_loss: 0.1902 - val_accuracy: 0.9469 - 74s/epoch - 108ms/step
Epoch 40/200
684/684 - 74s - loss: 0.2079 - accuracy: 0.9260 - val_loss: 0.1929 - val_accuracy: 0.9448 - 74s/epoch - 108ms/step
```

```
num_classes = 2
N_Epoch = 200
N_Neuronio = 150
batch_size = 50
img_height = 1000
img_width = 11
```

```
train_ds = tf.keras.utils.image_dataset_from_directory(
    "C:\\RD-PROJETO\\testesCiberataques\\env\\Scripts\\data\\train",
    validation_split=0.3,
    subset="training",
    seed=123,
    image_size=(img_height, img_width),
    batch_size=batch_size)

val_ds = tf.keras.utils.image_dataset_from_directory(
    'C:\\RD-PROJETO\\testesCiberataques\\env\\Scripts\\data\\validation',
    validation_split=0.3,
    subset="validation",
    seed=123,
    image_size=(img_height, img_width),
    batch_size=batch_size)
```



