Relatório de Projeto – Redes de Dados

Licenciatura em Engenharia Informática

Camila Reis da Silva 2212487

Gabriel Gouveia Marques 2212512

José Pedro Ribeiro Martins 2212947

Leiria, junho de 2023

Índice

1. Introdução

No âmbito da Unidade Curricular de Redes de Dados, inserida no 2º semestre do 2º ano da Licenciatura em Engenharia Informática da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, foi-nos proposta a realização de um projeto prático a fim de consolidar conhecimentos adquiridos em contexto de sala de aula, quer na vertente teórico-prática como na vertente prática laboratorial.

A elaboração deste projeto torna-se relevante na medida em que pretende facilitar a compreensão da articulação entre diferentes componentes e resolução de problemas - aplicando tanto competências genéricas na área das redes de dados como conhecimentos e técnicas específicos de comunicação em sistemas locais e distribuídos, recorrendo a planeamento e implementação de cenários de redes locais e a sua interligação através das redes públicas.

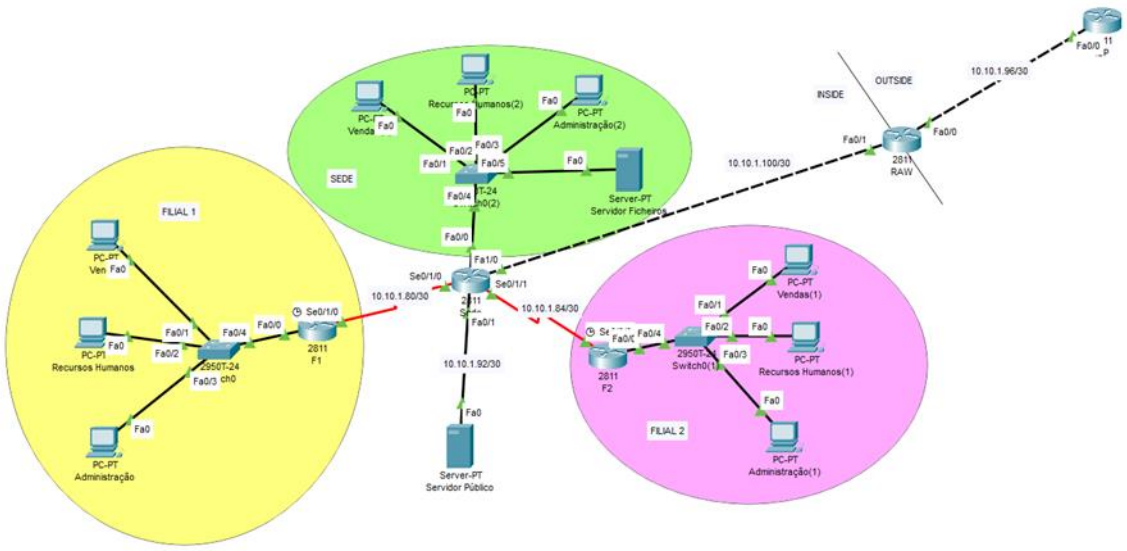
O projeto desenvolvido em todas as suas etapas tendo por base o cenário proposto no enunciado para este trabalho em questão, implicando a configuração de um cenário de redes relativo a uma empresa de Cibersegurança IoT e a simulação de deteção de ciberataques em redes IoT com recurso a utilização de redes neuronais artificiais.

A elaboração deste relatório pretende dar a conhecer o trabalho desenvolvido pelo grupo de estudantes autor do mesmo e as tarefas por ele desenvolvidas.

2. Caracterização do Cenário

O cenário desenvolvido é relativo a uma empresa de cibersegurança IoT composta por um total de 3 filiais: Sede, Filial 1 e Filial 2. Cada uma dessas 3 filiais possui 3 redes locais, nomeadamente Vendas, Recursos Humanos e Administração. A Sede possui ainda ligação a um Servidor Público para armazenamento do website e um Servidor de Ficheiros, interno à empresa e acedido apenas pelos hosts da mesma. No router da Sede temos também a ligação realizada com o exterior.

O router RAW representa um router fronteira, realizando ligação entre as redes internas da empresa e o exterior (internet). É nele onde são configuradas algumas das políticas de segurança e privacidade do cenário.



3. Caracterização de Rede e Serviços

O cenário projetado, tal como solicitado no enunciado, serviu-se da rede 10.10.0.0/23 para todas as necessidades de endereçamento.

De modo a salvaguardar a utilização do menor número de endereços possíveis recorreu-se ao subendereçamento da rede mencionada de modo a atender os requisitos: 2 filiais e 1 sede, cada uma com 3 redes locais Vendas (32 PCs em cada), Recursos Humanos (20 PCs em cada) e Administração (10 PCs em cada).

Para cada rede Vendas do cenário foi utilizada uma sub-rede /26, com 62 endereços disponíveis para hosts. Para cada rede Recursos Humanos foi utilizada uma sub-rede /27, com 30 endereços disponíveis para hosts. Para cada rede Administração foi utilizada uma sub-rede /28, com 14 endereços disponíveis para hosts. Para cada rede de interligação entre routers e servidores foi utilizada uma sub-rede /30, com 2 endereços disponíveis para hosts.

Sede

Equipamento	Interface	VLAN	IP	Máscara de rede	Default Gateway
PC VENDAS	Fa 0/1	10	10.10.0.0 - 10.10.0.63	255.255.255.192	10.10.0.62
PC RH	Fa 0/2	20	10.10.0.192 - 10.10.0.223	255.255.255.224	10.10.0.222
PC ADMIN	Fa 0/3	30	10.10.1.32 - 10.10.1.47	255.255.255.240	10.10.1.46
Router Sede	Fa 0/0.1 Fa 0/0.2 Fa0/0.3 Se0/1/0 Se0/1/1 Fa 0/1 Fa 1/0	10 20 30 N/A N/A N/A N/A	10.10.0.62 10.10.0.222 10.10.0.222 10.10.1.82 10.10.1.85 10.10.1.94 10.10.1.102	255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.252 255.255.255.252 255.255.255.252 255.255.255.252	N/A N/A N/A N/A N/A N/A N/A
Servidor Publico	Fa 0	N/A	10.10.1.93	255.255.255.252	10.10.1.94
Servidor de Ficheiros	Fa 0	N/A	10.10.1.89	255.255.255.252	10.10.1.90

Filial 1

Equipamento	Interface	VLAN	IP	Máscara de rede	Default Gateway
PC VENDAS	Fa 0/1	10	10.10.0.64 - 10.10.0.127	255.255.255.192	10.10.0.126
PC RH	Fa 0/2	20	10.10.0.224 - 10.10.0.255	255.255.255.224	10.10.0.254
PC ADMIN	Fa 0/3	30	10.10.1.48 - 10.10.1.63	255.255.255.240	10.10.1.62
Router F1	Fa 0/0.1 Fa 0/0.2 Fa0/0.3 Se 0/1/0	10 20 30 N/A	10.10.0.126 10.10.0.254 10.10.1.62 10.10.1.81	255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.252	N/A N/A N/A N/A

Filial 2

Equipamento	Interface	VLAN	IP	Máscara de rede	Default Gateway
PC VENDAS	Fa 0/1	10	10.10.0.128 - 10.10.0.191	255.255.255.192	10.10.0.190
PC RH	Fa 0/2	20	10.10.1.0 - 10.10.1.31	255.255.255.224	10.10.1.30
PC ADMIN	Fa 0/3	30	10.10.1.64 - 10.10.1.79	255.255.255.240	10.10.1.78
Router F2	Fa 0/0.1 Fa 0/0.2 Fa0/0.3 Se 0/0/0	10 20 30 N/A	10.10.0.190 10.10.1.30 10.10.1.78 10.10.1.86	255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.252	N/A N/A N/A N/A

Router RAW

Equipamento	Interface	IP	Máscara de rede
Router RAW	Fa 0/1 Fa 0/0	10.10.1.101 10.10.1.98	255.255.255.252 255.255.255.252

Router ISP

Equipamento	Interface	IP	Máscara de rede
Router ISP	Fa 0/0	10.10.0.1.97	255.255.255.252

Cada filial é composta por 3 VLANs representadas por computadores correspondentes às redes locais solicitadas, 1 switch onde se encontram conectadas estas redes, e um router conectado ao switch e de acesso ao exterior da rede.

De modo a hipoteticamente gerir recursos físicos a metodologia escolhida de ligação ao router

foi de router-on-a-stick, criando no mesmo subinterfaces relativas às VLANs.

De modo a garantir que não existe comunicação intra-filial entre as VLANs foram criadas extended ACLs de modo a controlar o tráfego em cada router.

FILIAL 1

```
Extended IP access list 101
    10 deny ip 10.10.0.64 0.0.0.63 10.10.0.224 0.0.0.31
    20 deny ip 10.10.0.64 0.0.0.63 10.10.1.48 0.0.0.15
    30 deny ip 10.10.0.224 0.0.0.31 10.10.0.64 0.0.0.63
    40 deny ip 10.10.0.224 0.0.0.31 10.10.1.48 0.0.0.15
    50 deny ip 10.10.1.48 0.0.0.15 10.10.0.64 0.0.0.63
    60 deny ip 10.10.1.48 0.0.0.15 10.10.0.224 0.0.0.31
    70 permit ip any any
```

FILIAL 2

```
Extended IP access list 101
    10 deny ip 10.10.0.128 0.0.0.63 10.10.1.0 0.0.0.31
    20 deny ip 10.10.0.128 0.0.0.63 10.10.1.64 0.0.0.15
    30 deny ip 10.10.1.0 0.0.0.31 10.10.0.128 0.0.0.63
    40 deny ip 10.10.1.0 0.0.0.31 10.10.1.64 0.0.0.15
    50 deny ip 10.10.1.64 0.0.0.15 10.10.0.128 0.0.0.63
    60 deny ip 10.10.1.64 0.0.0.15 10.10.1.0 0.0.0.31
    70 permit ip any any
```

A filial Sede, para além da configuração supramencionada, apresenta também ligação no router a um Servidor Público para alojamento da página web da empresa e uma quarta subinterface ligada a um servidor de ficheiros que só é acedido pelos computadores da empresa. Este controlo de acesso é também garantido com recurso a uma extended ACL, identificada como 102.

SEDE

```
Extended IP access list 101
    10 deny ip 10.10.0.0 0.0.0.63 10.10.0.192 0.0.0.31
    20 deny ip 10.10.0.0 0.0.0.63 10.10.1.32 0.0.0.15
    30 deny ip 10.10.0.192 0.0.0.31 10.10.0.0 0.0.0.63
    40 deny ip 10.10.0.192 0.0.0.31 10.10.1.32 0.0.0.15
    50 deny ip 10.10.1.32 0.0.0.15 10.10.0.0 0.0.0.63
    60 deny ip 10.10.1.32 0.0.0.15 10.10.0.192 0.0.0.31
    70 permit ip any any (6 match(es))
Extended IP access list 102
    10 permit ip any 10.10.0.0 0.0.1.255
    20 deny ip any any
```

A configuração de IP de toda a empresa foi obtida por recurso ao serviço DHCP, alojado em cada um dos routers Filial1, Filial2 e Sede. A configuração de IP dos servidores, no entanto, é

estática, de modo a garantir o acesso consistente aos mesmos. Por se tratar de uma empresa pequena, mas com muitos endereços disponíveis (garantido pela rede /23) não se definiu um lease time para a utilização dos endereços IP atribuídos. As pools definidas foram com base no subendereçamento calculado para cada subrede, sendo o default router o endereço atribuído às interfaces das respetivas redes.

DHCP SEDE

```
ip dhcp pool PoolVendas
 network 10.10.0.0 255.255.255.192
 default-router 10.10.0.62
 dns-server 8.8.8.8
ip dhcp pool PoolRH
 network 10.10.0.192 255.255.255.224
 default-router 10.10.0.222
 dns-server 8.8.8.8
ip dhcp pool PoolAdmin
 network 10.10.1.32 255.255.255.240
 default-router 10.10.1.46
 dns-server 8.8.8.8
!
```

DHCP F1

```
!
ip dhcp pool PoolVendas
 network 10.10.0.64 255.255.255.192
 default-router 10.10.0.126
 dns-server 8.8.8.8
ip dhcp pool PoolRH
 network 10.10.0.224 255.255.255.224
 default-router 10.10.0.254
 dns-server 8.8.8.8
ip dhcp pool PoolAdmin
 network 10.10.1.48 255.255.255.240
 default-router 10.10.1.62
 dns-server 8.8.8.8
!
```

DHCP F2

```
!
ip dhcp pool PoolVendas
 network 10.10.0.128 255.255.255.192
 default-router 10.10.0.190
 dns-server 8.8.8.8
ip dhcp pool PoolRH
 network 10.10.1.0 255.255.255.224
 default-router 10.10.1.30
 dns-server 8.8.8.8
ip dhcp pool PoolAdmin
 network 10.10.1.64 255.255.255.240
 default-router 10.10.1.78
 dns-server 8.8.8.8
!
```

De modo a garantir a comunicação entre as 3 filiais da empresa recorreu-se a encaminhamento dinâmico por EIGRP uma vez que este permite uma rápida convergência em caso de mudanças na topologia de rede, utilização eficiente da largura de banda, é compatível com a utilização de submáscaras de tamanho variável e, apesar de a empresa desenvolvida no cenário ser pequena, EIGRP apresenta grande escalabilidade, caso houvesse um aumento da empresa.

Na sede foi também definida uma rota estática "por omissão" de acesso à internet, que reenvia toda a comunicação da rede interna para o router RAW. No entanto, esta rota assegura apenas o acesso da empresa à internet, e não à própria empresa em caso de falha.

Não obstante, a informação de encaminhamento é importante ser enviada apenas para outros equipamentos que também façam ligação com outras redes. Assim sendo, de modo a evitar envio desnecessário de informação pela rede, foram definidas em todos os routers interfaces passivas, que apenas comunicam a sua topologia mas não recebem informação sobre topologia externa – uma vez que esta não é necessária, já que todas as necessidades de encaminhamento serão supridas neste caso pelos routers.

IP ROUTE SEDE

```
!
router eigrp 1
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 10.10.0.0 0.0.0.63
 network 10.10.0.192 0.0.0.31
 network 10.10.1.32 0.0.0.15
 network 10.10.1.80 0.0.0.3
 network 10.10.1.84 0.0.0.3
 network 10.10.1.92 0.0.0.3
 network 10.10.1.100 0.0.0.3
!
ip classless
ip route 10.10.0.0 255.255.254.0 10.10.1.101
!
```

IP ROUTE F1

```
!
router eigrp 1
 network 10.10.1.80 0.0.0.3
 network 10.10.0.64 0.0.0.63
 network 10.10.0.224 0.0.0.31
 network 10.10.1.48 0.0.0.15
!
```

IP ROUTE F2

```
!
router eigrp 1
 network 10.10.1.84 0.0.0.3
 network 10.10.0.128 0.0.0.63
 network 10.10.1.0 0.0.0.31
 network 10.10.1.64 0.0.0.15
!
```

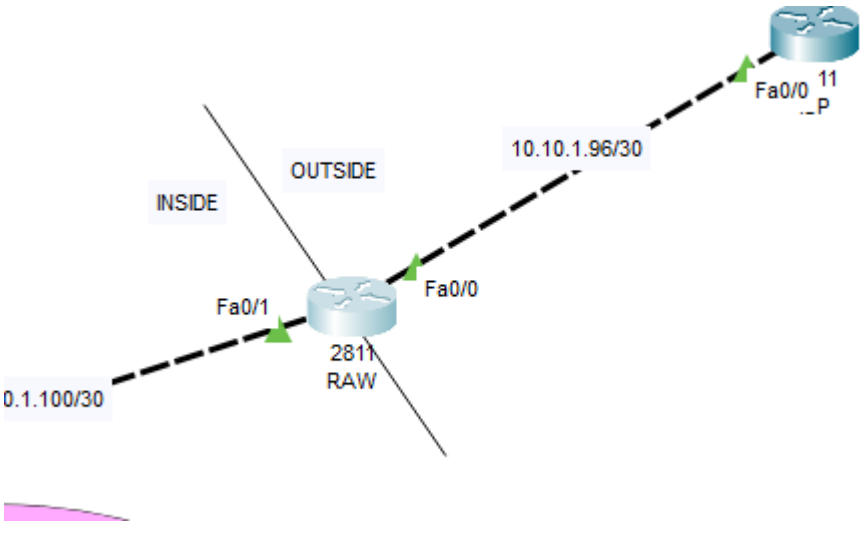
IP ROUTE RAW

```
!
router eigrp 1
 redistribute static
 network 10.10.1.100 0.0.0.3
!
```

De maneira a garantir a privacidade da rede foi aplicado o protocolo NAT, uma vez que o mesmo permite ocultar os endereços privados dos nossos dispositivos, substituindo-os por um endereço único público aquando da comunicação com a internet. Tal configuração foi realizada com recurso as um router de fronteira (RAW), que define o interior da rede (nat inside) na interface FastEthernet 0/1 e exterior da rede (nat outside) na interface FastEthernet 0/0. É neste router e nessas interfaces onde se encontram as configurações de tradução de endereços relativas à nossa empresa.

O método utilizado de modo as conseguir que todos os endereços privados da empresa fossem traduzidos para um único endereço público foi com implementação de PAT através do comando “nat overload”, que faz com que os hosts sejam diferenciados entre si através dos portos utilizados durante a comunicação, e não pelo IP em si.

NAT



```
!
ip nat inside source list 1 interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.1.97
!
ip flow-export version 9
!
!
access-list 1 permit 10.10.0.0 0.0.1.255
!
!
!
```

```
!
interface FastEthernet0/0
 ip address 10.10.1.98 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.10.1.101 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
```

O acesso a dispositivos de rede, por motivos de segurança, deve ser limitado apenas a utilizadores autorizados. Para evitar que qualquer host da empresa aceda às configurações de rede implementadas, o acesso é controlado por utilização de passwords encriptadas em todos os routers da empresa. Foram definidos também, por motivos legais, avisos apresentados aquando da tentativa de acesso aos routers.

```
FORBIDDEN ACCESS TO UNAUTHORIZED PERSONNEL

User Access Verification

Password:

Sede>enable
Password:
Sede#
```

```
service password-encryption
!
hostname Sede
!
!
!
enable secret 5 $1$mERr$yiuHj7Lm4U9ZRn8VNI6160
!
```

Foi-nos solicitada também a implementação do protocolo PPPoE como meio de ligação entre a empresa e o ISP. No entanto não fomos capazes de fazer essa implementação. Ao executar as configurações abaixo apresentadas deparámo-nos com problemas de conectividade, não tendo o cenário a responder como o esperado. Por esse motivo, tais configurações foram

eliminadas do ficheiro de Packet Tracer do trabalho, de maneira a apresentar um cenário funcional apesar de incompleto de acordo com os requisitos do enunciado.

```
bba-group pppoe EX
  virtual-template 1
!
interface Virtual-Template1
 peer default ip address pool PPPoE-Dialers
 ip unnumbered FastEthernet0/0
 encapsulation ppp
!
interface FastEthernet0/0
 no ip address
 pppoe enable group EX
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
interface FastEthernet0/0
 no ip address
 pppoe enable group ex
 pppoe-client dial-pool-number 1
 ip nat outside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.10.1.101 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface Dialer0
 dialer pool 1
 ip address negotiated
 mtu 1492
 encapsulation ppp
!
```

4. Simulação de deteção de ciberataques em redes IoT, utilizando redes neuronais artificiais

Uma rede neuronal artificial é um modelo computacional que se inspira no funcionamento do cérebro humano. É composta por neurónios interconectados que recebem entradas, realizam cálculos e geram saídas. Durante o treino, os pesos das conexões entre os neurónios são ajustados para minimizar o erro entre as saídas previstas e as saídas desejadas. Uma vez treinada, a rede neuronal pode ser utilizada para fazer previsões ou classificações em novos dados, com base nos padrões aprendidos durante o treino.

Normalmente, durante o treino de uma rede neuronal, é comum dividir os dados disponíveis em duas partes principais: um conjunto de treino e um conjunto de validação.

O conjunto de treino é utilizado para ajustar os pesos das conexões da rede neuronal, permitindo que esta aprenda a relação entre os dados de entrada e as saídas desejadas. Este conjunto contém exemplos de dados nos quais o modelo é treinado para realizar previsões ou classificações corretas.

Já o conjunto de validação é utilizado para avaliar o desempenho da rede neuronal em dados não vistos durante o treino. Ajuda a verificar se o modelo está a generalizar corretamente os padrões aprendidos, sendo uma medida importante para evitar o *overfitting* do modelo aos dados de treino que é quando o modelo apresenta resultados excelentes, mas quando verificado com dados novos demonstra mau desempenho.

A separação dos dados em conjuntos de treino e validação permite avaliar a capacidade da rede neuronal de generalizar para novos dados e ajustar os parâmetros do modelo com base no desempenho observado no conjunto de validação. Isto ajuda a garantir que a rede neuronal seja capaz de lidar com dados não vistos anteriormente e melhore o seu desempenho.

Um dos requisitos do trabalho é o treino de 3 modelos diferentes com base em datasets diferentes. Desta forma foram escolhidos vários ficheiros de origem de forma a gerar datasets que iriam ser usados para treinar os modelos.
Cada um dos datasets foi formatado para incluírem cerca de 100 000 linhas.

O dataset 1 é originado da junção de 2 datasets originais, o **CTU-IoT-Malware-Capture-1-1** e o **CTU-IoT-Malware-Capture-9-1**. De cada um destes foram selecionadas 50 mil linhas e foram concatenadas assim formando o dataset 1.

Originalmente os dados do dataset 1 apresentavam os seguintes resultados:

Benign	49939
(empty) Malicious PartOfAHorizontalPortScan	49167
(empty) Benign	834
Malicious C&C	55
Malicious C&C-FileDownload	5

Após uniformização da informação ficamos com o seguinte resultado:

Malicious	50061
Benign	49939
Total	100 000

O dataset 2 é originado de 1 dataset original, **CTU-IoT-Malware-Capture-43-1**. Deste foram selecionadas 100 000 mil linhas formando o dataset 2.

Originalmente os dados do dataset 2 apresentavam os seguintes resultados:

Malicious PartOfAHorizontalPortScan	56836
Benign	30006
Malicious Okiru	13116
Malicious C&C	29
Malicious C&C-FileDownload	13

Após uniformização da informação ficamos com o seguinte resultado:

Malicious	69994
Benign	30006
Total	100 000

O Dataset 3 é originado de 1 dataset original, o **CTU-IoT-Malware-Capture-1-1**. Deste foram selecionadas 100 mil linhas formando o dataset 3.

Originalmente os dados do dataset 3 apresentavam os seguintes resultados:

Malicious PartOfAHorizontalPortScan	55043
Benign	44957

Após uniformização da informação ficamos com o seguinte resultado:

Malicious	55043
Benign	44957
Total	100 000

Após a padronização dos três conjuntos de dados, cada um deles é processado individualmente por um programa em Python baseado no ficheiro "**Converte_Excel_to_JPG_RD_v01.ipynb**" fornecido na página da disciplina no Moodle da UC.

Foram realizadas diversas alterações ao programa para permitir que, de forma automática, os dados anteriores sejam removidos e a estrutura das pastas seja criada novamente toda vez que o programa for executado. Além disso, para acelerar o processo de armazenamento dos dados, o programa utiliza a biblioteca de multiprocessing.

Cada conjunto de dados é dividido na proporção de 80/20. Os 80% dos dados são utilizados para o treinamento do modelo, enquanto os 20% restantes são destinados à validação. Dentro de cada divisão de treino e validação, os dados são novamente divididos em duas pastas: "0" e "1". A pasta "0" representa os dados " **Benign**", ou seja, as comunicações inofensivas, enquanto a pasta "1" contém os dados "**Malicious**", ou seja, as comunicações categorizadas como ataques.
Feita a divisão correta dos datasets foi corrido o programa "**Deep Learning Cybersecurity with images RD v01.ipynb**" e tal como o programa base anterior fornecido na página do moodle da UC.

Neste programa foram realizadas algumas modificações, incluindo os parâmetros de treino e a forma como os dados são lidos. Uma vez que a separação dos dados em uma proporção de 80/20 já foi feita no programa anterior, substituímos a função "**tf.keras.utils.image_dataset_from_directory**" pela função "**train_datagen.flow_from_directory**", que permite ler diretamente os dados já separados. Finalmente foram trocados os parâmetros de treino para os seguintes:

num_classes	2
N_Epoch	10
N_Neuronio	64
batch_size	64
img_width	850
img_height	11

Após definidos os parâmetros de treino e a preparação dos datasets foram obtidos os seguintes resultados para cada dataset.

Dataset 1 - PartOfAHorizontalPortScan e C&C-FileDownload

```
Found 80000 images belonging to 2 classes.
Found 20000 images belonging to 2 classes.
Class names: ['0', '1']
image_batch.shape =  (64, 11, 850, 3)
labels_batch.shape =  (64,)
Epoch 1/10
1250/1250 - 514s - loss: 0.0340 - accuracy: 0.9963 - val_loss: 0.0020 - val_accuracy: 0.9995 - 514s/epoch - 412ms/step
Epoch 2/10
1250/1250 - 69s - loss: 0.0015 - accuracy: 0.9996 - val_loss: 9.8682e-04 - val_accuracy: 0.9998 - 69s/epoch - 55ms/step
Epoch 3/10
1250/1250 - 71s - loss: 6.3381e-04 - accuracy: 0.9998 - val_loss: 0.0011 - val_accuracy: 0.9997 - 71s/epoch - 56ms/step
Epoch 4/10
1250/1250 - 70s - loss: 2.5357e-04 - accuracy: 1.0000 - val_loss: 4.2097e-04 - val_accuracy: 0.9999 - 70s/epoch - 56ms/step
Epoch 5/10
1250/1250 - 75s - loss: 1.3547e-04 - accuracy: 1.0000 - val_loss: 2.7200e-04 - val_accuracy: 0.9999 - 75s/epoch - 60ms/step
Epoch 6/10
1250/1250 - 67s - loss: 5.2229e-05 - accuracy: 1.0000 - val_loss: 1.7943e-04 - val_accuracy: 0.9999 - 67s/epoch - 54ms/step
Epoch 7/10
1250/1250 - 70s - loss: 1.6046e-05 - accuracy: 1.0000 - val_loss: 1.9656e-04 - val_accuracy: 0.9999 - 70s/epoch - 56ms/step
Epoch 8/10
1250/1250 - 70s - loss: 1.0438e-05 - accuracy: 1.0000 - val_loss: 2.0582e-04 - val_accuracy: 0.9999 - 70s/epoch - 56ms/step
Epoch 9/10
1250/1250 - 67s - loss: 6.0483e-06 - accuracy: 1.0000 - val_loss: 1.6566e-04 - val_accuracy: 0.9999 - 67s/epoch - 54ms/step
Epoch 10/10
1250/1250 - 62s - loss: 3.1668e-06 - accuracy: 1.0000 - val_loss: 2.0274e-04 - val_accuracy: 0.9999 - 62s/epoch - 49ms/step
```

Dataset 2 - PartOfAHorizontalPortScan e Okiru

```
Found 80000 images belonging to 2 classes.
Found 20000 images belonging to 2 classes.
Class names: ['0', '1']
image_batch.shape =  (64, 11, 850, 3)
labels_batch.shape =  (64,)
Epoch 1/10
1250/1250 - 479s - loss: 0.0504 - accuracy: 0.9833 - val_loss: 0.0040 - val_accuracy: 0.9995 - 479s/epoch - 383ms/step
Epoch 2/10
1250/1250 - 58s - loss: 0.0025 - accuracy: 0.9997 - val_loss: 0.0025 - val_accuracy: 0.9996 - 58s/epoch - 46ms/step
Epoch 3/10
1250/1250 - 59s - loss: 0.0015 - accuracy: 0.9998 - val_loss: 0.0015 - val_accuracy: 0.9997 - 59s/epoch - 47ms/step
Epoch 4/10
1250/1250 - 59s - loss: 8.0595e-04 - accuracy: 0.9998 - val_loss: 8.8177e-04 - val_accuracy: 0.9998 - 59s/epoch - 47ms/step
Epoch 5/10
1250/1250 - 67s - loss: 3.1867e-04 - accuracy: 0.9999 - val_loss: 8.6265e-04 - val_accuracy: 0.9998 - 67s/epoch - 54ms/step
Epoch 6/10
1250/1250 - 64s - loss: 1.0099e-04 - accuracy: 1.0000 - val_loss: 9.8571e-04 - val_accuracy: 0.9998 - 64s/epoch - 51ms/step
Epoch 7/10
1250/1250 - 63s - loss: 3.6613e-05 - accuracy: 1.0000 - val_loss: 9.8398e-04 - val_accuracy: 0.9998 - 63s/epoch - 51ms/step
Epoch 8/10
1250/1250 - 61s - loss: 2.2430e-05 - accuracy: 1.0000 - val_loss: 9.5221e-04 - val_accuracy: 0.9998 - 61s/epoch - 49ms/step
Epoch 9/10
1250/1250 - 63s - loss: 1.3833e-05 - accuracy: 1.0000 - val_loss: 0.0012 - val_accuracy: 0.9998 - 63s/epoch - 50ms/step
Epoch 10/10
```

Dataset 3 – PartOfAHorizontalPortScan

```
Found 80000 images belonging to 2 classes.
Found 20000 images belonging to 2 classes.
Class names: ['0', '1']
image_batch.shape =  (64, 11, 850, 3)
labels_batch.shape =  (64,)
Epoch 1/10
1250/1250 - 478s - loss: 0.0993 - accuracy: 0.9711 - val_loss: 0.0103 - val_accuracy: 0.9981 - 478s/epoch - 382ms/step
Epoch 2/10
1250/1250 - 72s - loss: 0.0058 - accuracy: 0.9992 - val_loss: 0.0026 - val_accuracy: 0.9997 - 72s/epoch - 57ms/step
Epoch 3/10
1250/1250 - 74s - loss: 0.0018 - accuracy: 0.9998 - val_loss: 9.0693e-04 - val_accuracy: 0.9999 - 74s/epoch - 59ms/step
Epoch 4/10
1250/1250 - 64s - loss: 6.5221e-04 - accuracy: 0.9999 - val_loss: 4.0489e-04 - val_accuracy: 0.9999 - 64s/epoch - 51ms/step
Epoch 5/10
1250/1250 - 63s - loss: 2.3557e-04 - accuracy: 1.0000 - val_loss: 1.8249e-04 - val_accuracy: 1.0000 - 63s/epoch - 51ms/step
Epoch 6/10
1250/1250 - 66s - loss: 9.5780e-05 - accuracy: 1.0000 - val_loss: 1.0809e-04 - val_accuracy: 1.0000 - 66s/epoch - 52ms/step
Epoch 7/10
1250/1250 - 64s - loss: 4.8652e-05 - accuracy: 1.0000 - val_loss: 1.0654e-04 - val_accuracy: 1.0000 - 64s/epoch - 51ms/step
Epoch 8/10
1250/1250 - 65s - loss: 2.4789e-05 - accuracy: 1.0000 - val_loss: 4.2222e-05 - val_accuracy: 1.0000 - 65s/epoch - 52ms/step
Epoch 9/10
1250/1250 - 65s - loss: 1.2616e-05 - accuracy: 1.0000 - val_loss: 2.9278e-05 - val_accuracy: 1.0000 - 65s/epoch - 52ms/step
Epoch 10/10
1250/1250 - 64s - loss: 6.9082e-06 - accuracy: 1.0000 - val_loss: 1.5871e-05 - val_accuracy: 1.0000 - 64s/epoch - 51ms/step
```

5. Conclusão

Com a realização deste trabalho foi-nos possível cumprir os objetivos propostos na introdução – de aprofundar e melhor compreender de que maneira as diversas etapas de planeamento e configuração de redes e serviços interagem entre elas, as suas dependências, bem como o relacionamento e dependências entre a aplicação e implementação de diversos serviços de redes.

O desenho inicial do cenário foi uma etapa realizada com pouca dificuldade, sendo que se baseou maioritariamente nos cenários desenhados em contexto de sala de aulas mas aplicado ao contexto proposto pelo enunciado do projeto.

A implementação de diversas políticas e serviços, como NAT, apesar de a título individual não colocarem problemas, revelou-se mais trabalhosa, uma vez que ao contrário do já trabalho em aulas, exigiu uma maior interligação e conexão com outros serviços e políticas de modo a obter uma rede completa e completamente funcional.

A simulação de deteção de cibertaques com uso a redes neuronais artificiais provou-se um maior desafio, uma vez que foi um tema nunca antes abordado ao longo do semestre, e que exigiu maior esforço autónomo por parte do grupo para adquirir os conhecimentos suficientes para a implementação pedida.

Foi também sentida dificuldade nalguns protocolos com o PPPoE por se tratar de uma configuração também nunca abordada em contexto de sala de aula, exigindo também esforço da nossa parte no sentido de aquisição de novos conhecimentos. No entanto, e provavelmente por uma falha de capacidade de resolução de problemas, não fomos capazes de implementar esta funcionalidade de maneira satisfatória, obrigando a que a mesma fosse omitida do presente relatório.

O balanço retirado da realização do projeto é positivo, pois contribuiu para a consolidação de conhecimentos. Também positivo é o balanço da elaboração do presente relatório, uma vez que nos permitiu uma reflexão sobre o percurso deste trabalho, falhas a colmatar futuramente, e pontos a explorar.

Como sugestão, gostaríamos de reforçar a ideia de se abordarem os tópicos de futuros enunciados em contextos de aulas práticas-laboratoriais.

Bibliografia

- Moodle (ead.ipleiria.pt/2022-33)