# Medição do desempenho da rede TOR

Catarina Silva
2210440@myipleiria.pt
Gonçalo Vicente
2210510@myipleiria.pt

Departamento de Engenharia Informática
Instituto Politécnico Leiria-Escola Superior de Tecnologia e Gestão

## Resumo

A utilização de VPN em redes informáticas é uma questão amplamente discutida. Se, por um lado, podemos verificar uma maior segurança na rede, a verdade é que, o desempenho desta fica mais comprometido uma vez que existe uma maior quantidade de bytes que é necessário considerar, tendo em conta que o preço a pagar para a segurança reside numa quantidade elevada de *bytes*.

Neste documento, serão analisadas, com recursos a casos práticos, o desempenho que é possível obter com a utilização de VPN em detrimento da segurança ou se não se optar pelo seu uso privilegiando a velocidade.

## 1 Introdução

O presente trabalho é de cariz universitário e foi desenvolvido no âmbito da unidade curricular de Segurança em Redes de Computadores, inserida no Mestrado em Cibersegurança e Informática Forense e sob orientação do professor Mário Antunes, medindo o desempenho da rede TOR.

Ao longo deste documento, serão abordados o conceito de VPN, da rede TOR, bem como a explicação do setup utilizado. Numa outra secção, iremos enunciar os resultados obtidos com recursos a gráficos e tabelas, de forma a transformar a informação para uma forma mais visual e legível de entender.

No que diz respeito à VPN, este serviço consiste numa rede constituída por um conjunto de redes privadas interligadas por canais virtuais suportados noutras redes, normalmente públicas, como a rede de Internet. Um dos principais softwares utilizados neste trabalho é o browser Tor que visa garantir a anonimização da navegação. Para fazer a monitorização de todo o setup implementado, recorreu-se, utilizando uma máquina virtual Ubuntu, à ferramenta chronograf que pertence à InfluxDB.

Apesar de existirem vários artigos científicos relacionados com a rede Tor, encontrou-se muito pouca informação relativamente às velocidades associadas ao desempenho desta rede, transformando este trabalho num trabalho numa área onde ainda não existem estudos conhecidos, visto que os estudos existentes abordam maioritariamente anonimização da rede Tor, artigos de análises forenses relacionadas com a sua privacidade, as falhas que existem e sugestões de possíveis resoluções para as mesmas.

## 2 Desenvolvimento

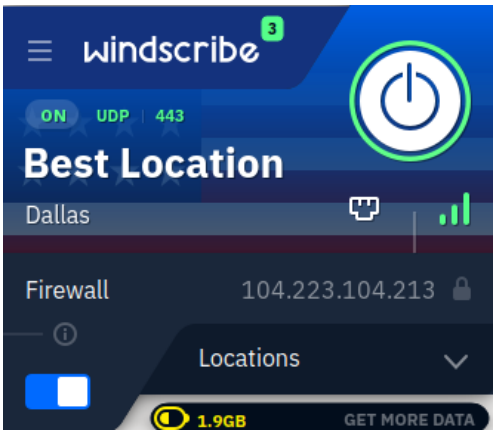
Nesta secção irão ser abordados temas como: VPN (*Virtual Private Networks*) e Rede Tor, de modo a sustentar e a contextualizar o trabalho que será realizado neste artigo. Iremos apresentar também o *setup* que foi criado para a realização das medições do desempenho da rede com VPN, sem VPN e da rede Tor com VPN.

### 2.1 VPN

Uma rede virtual privada (VPN) consiste numa rede constituída por um conjunto de redes privadas interligadas por canais virtuais suportados noutras redes, normalmente públicas como a rede de Internet. Por forma a garantir a segurança da comunicação aquando da utilização de uma VPN, são utilizadas técnicas para encriptação e autenticação.

Com o intuito de possibilitar a comunicação segura entre duas redes, ambas terão que acordar esquemas comuns para encriptação e autenticação, o que é feito por configuração adequada dos sistemas nos extremos do canal, sendo concentradores de VPN. **[1]**

Nosso trabalho, foi utilizada o serviço de VPN *Windscribe* numa máquina virtual Ubuntu Desktop 18.04 LTS. Para tal, foi necessário recorrer, através da *store* do *Windscribe*, fazer o download do respetivo package para o sistema operativo que se adequa ao trabalho. Seguidamente, foi necessário correr o comando "sudo dpkg -i <package que fizemos download>". Neste passo, encontra-se instalada a aplicação de VPN na máquina, sendo apenas necessário fazer login com uma conta criada para o efeito.

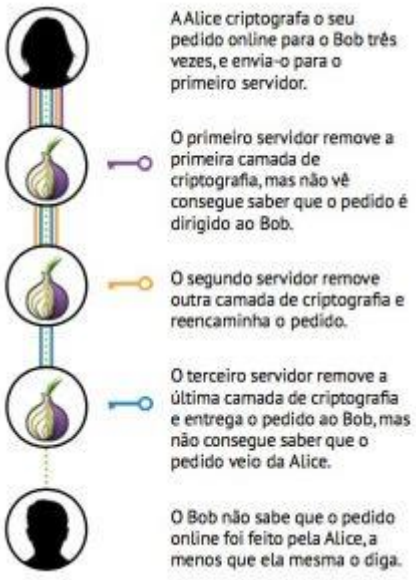



### 2.2 Rede Tor

É uma das redes mais utilizadas e conhecidas na *dark net*. Para conseguirmos utilizar esta rede é necessário recorrer à instalação de um *browser* específico, denominado de *Tor Browser*. O *Tor browser* é um *software* que visa garantir a anonimização da navegação. **[2]**

Para se entender o funcionamento da Rede Tor, apresentemos um exemplo ilustrativo: A Alice criptografa o seu pedido online para o Bob. Este é enviado para a primeira camada da Rede Tor para remover a primeira camada criptográfica sem se saber, ainda, o conteúdo do pedido. De seguida, o pedido é encaminhado para a segunda camada da Rede Tor para remover outra camada criptográfica do pedido, reencaminhando-o para a terceira e última camada da Rede Tor, removendo a última camada criptográfica do pedido, entregando-o a Bob. Bob recebeu o pedido, mas não sabe que este veio de Alice a menos que a mesma lhe diga.

Ou seja, a Rede Tor é constituída por três servidores criptográficos e quando um cliente faz um pedido, este é intercetado por esses mesmos servidores até chegar ao destino pretendido, sem nunca se saber o IP de origem, visto que durante a transmissão do pedido este adquire um dos IP's associados a um dos servidores, de forma aleatória, pelo qual passou. Na figura seguinte, é possível visualizar esta informação recorrendo à analogia entre a Alice e o Bob.



## 2.3 Setup utilizado

De forma a conseguirmos analisar algumas das diferenças existentes entre a utilização ou não de VPN no browser TOR, foi necessário recorrer à criação de um pequeno cenário prático para desenvolver a implementação a partir de tal.


Como foi dito na secção 2, recorreu-se à utilização de uma máquina virtualizada Linux com o sistema operativo Ubuntu 18.04 LTS, de memória RAM 4GB. Nesta máquina instalou-se o browser TOR na versão mais recente (0.4.5.9) e o browser Mozilla Firefox, versão 94.0, de forma a servir de base a todos os testes que foram necessários monitorizar.

Para nos auxiliar com as medições de monitorização de pacotes de rede, nomeadamente, a quantidade de *http requests*, a memória alocada, a memória utilizada (em %) e os bytes alocados através de *mallocs* e frees, recorreu-se ao software *chronograf*.

Este software foi escolhido após uma comparação com outro produto, também, da *influxDB*, sendo este o *telegraph*. Após uma análise entre os prós e os contras de cada *software*, conclui-se que, e tendo as necessidades deste trabalho, o *chronograf* era o mais adequado, uma vez que tinha uma implementação menos complexa e que permitia realizar a monitorização de rede em questão.

# 3 Resultados

No decorrer deste capítulo, iremos abordar os resultados obtidos através da realização de testes com recurso a medições da velocidade da navegação na rede entre os *browsers* Tor e Mozilla Firefox. Esses resultados, incluem ligações encapsuladas por VPN ou sem o recurso a esta tecnologia.

## 3.1Exemplos ilustrativos das medições realizadas

Ao longo do presente trabalho, foi necessário recorrer a um conjunto de casos práticos, de forma a que todas as medições efetuadas fossem o mais fidedignas possíveis. Assim, para ser possível efetuarmos sempre os mesmos acessos decidiu-se que se iria definir o acesso, primeiramente, através de uma pesquisa no navegador por ipleiria, seguidamente, selecionou-se o url do ipleiria.pt.

Após o website estar completamente carregado, voltou-se ao browser para pesquisar e, desta vez, por ead ipleiria. Inicialmente, abriu-se o link do ead 2019, porém voltou-se à pesquisa do navegador e procurou-se por ead 2021. Selecionou-se a opção de repor a password e de seguida fizemos login na plataforma. Já dentro da ead, abriu-se a disciplina de Segurança de Redes de Computadores onde se acedeu a um *link* para fazer o download do ISO do sistema operativo Ubuntu Server 18.04 Lts. Para deixar correr o download, abriu-se uma página relativa à entrega de um trabalho, anexou-se um ficheiro ao campo correspondente a essa ação e depois cancelou-se tanto a anexação do ficheiro como o download em questão.

Estes passos foram realizados nos 4 testes distintos que foram feitos, posteriormente, de forma a garantir que as ações executadas não se diferenciavam de teste para teste, garantindo assim a conformidade dos resultados.

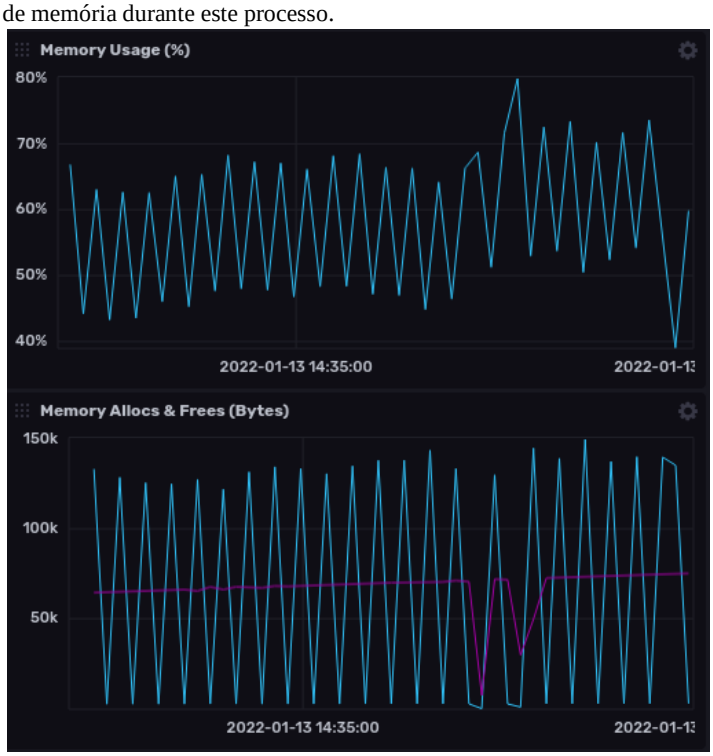
## 3.2 Gráficos obtidos dessas mesmas medições

Nos gráficos seguintes, podemos observar as medições efetuadas com recurso ao browser Tor e ao serviço de VPN descrito anteriormente. Através da sua análise, conseguiu-se observar diferentes tipos de valores associados a serviços de rede ou até mesmo ao gasto de memória pelo próprio sistema operativo.

### 3.2.1 Tor com VPN

O primeiro gráfico, referente ao "*Memory Usage (%)*", simboliza a percentagem de memória utilizada durante o processo das medições. Podemos observar a existência de grandes oscilações durante este período, estando estes valores compreendidos entre os 40% e 80% de memória utilizada.

Relativamente ao segundo gráfico, este representa a "*Memory Allocs & Frees (Bytes)*". Representado com a cor roxa, está os *allocs*, que representam a quantidade de *bytes* utilizados para processos de escrita. Com a cor azul, está representada a quantidade, em bytes, de libertações de memória durante este processo.




No próximo gráfico, é possível visualizar as "*Query request*", que simbolizam o tempo, em milissegundos, a que os *request* estiveram sujeitos. Existe algumas oscilações que podem ser atribuídas aos momentos em que não se estavam a realizar operações de leitura e escrita. Relativamente à "*Memory allocations (Bytes)*", é possível observar a alocação de memória em bytes durante o processo de medição. Mais uma vez, foram identificados dois grandes picos que são atribuídos a uma inexistência de pedidos ao servidor.

Nos blocos de gráficos seguintes, podemos observar o "*Request bytes"* que representa a quantidade de informação transmitida através de um pedido ao servidor. Com a linha azul é possível observar os pedidos que foram executados com sucesso, sendo marcados com o código HTTP 200, e com a linha roxa encontram-se marcados os pedidos com o código 499, que corresponde ao "*Client closed request*" que acontece quando o cliente fecha a conexão enquanto o servidor web *nginx* está a processar a solicitação.

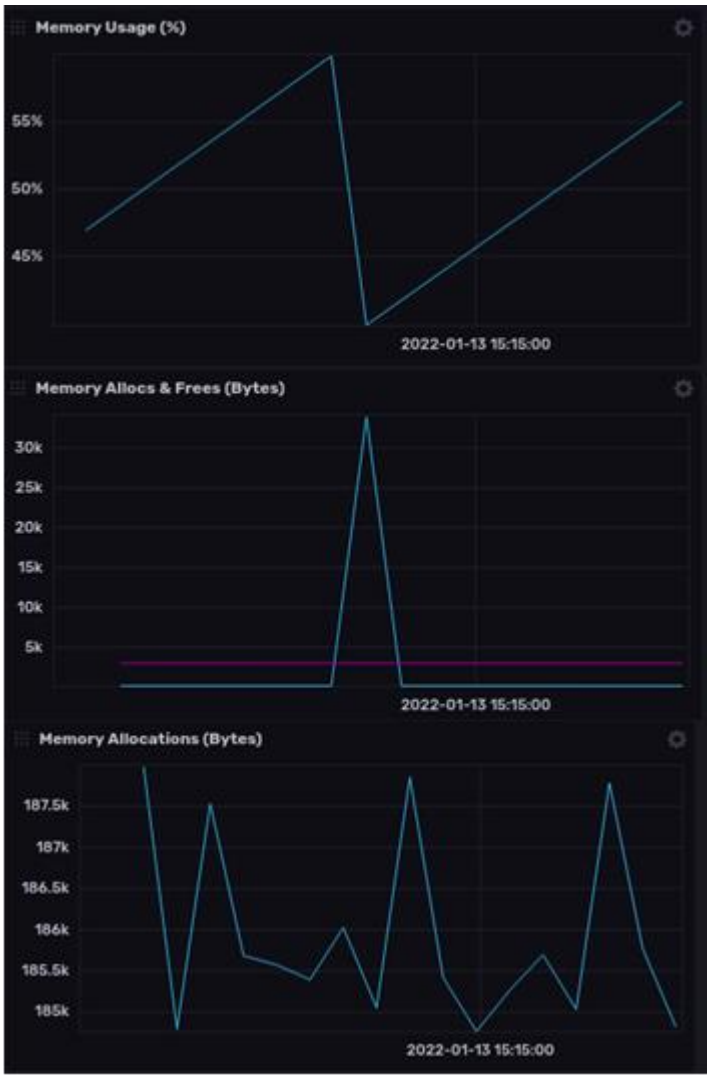
No segundo gráfico, encontram-se os "*Response bytes*", ou seja, os bytes associados às respostas do servidor. Com a linha azul encontram-se, mais uma vez, os códigos marcados com o código 200 e a roxo as respostas do servidor marcadas com o código 499, já explicados anteriormente.

Através de uma breve interpretação, podemos observar que estes gráficos apresentam um valor crescente durante o espaço temporal em análise, visto que existiu uma grande quantidade de pedidos ao servidor.


### 3.2.1 Mozilla Firefox com VPN

Para efeitos de comparação decidiu-se apresentar, igualmente, os gráficos referentes às medições realizadas no browser Mozilla Firefox com o serviço de VPN ligado.

A seleção dos gráficos para esta seção teve por base as claras diferenças entre este tipo de medição e a medição anterior, isto porque pela observação do gráfico seguinte conseguiu-se perceber que existiu uma menor utilização de memória, tendo valores compreendidos entre 42% e 60%, enquanto nas medições no browser Tor com VPN obteve-se valores compreendidos entre os 40% e 80%.




Esta discrepância de valores justifica-se, uma vez que o browser Tor já por si consome bastante recursos, uma vez que já possui uma VPN na sua arquitetura e assim, juntamente com um outro serviço de VPN exige ainda mais recursos computacionais do que o browser Mozilla Firefox, mesmo este estando a utilizar um serviço de VPN, tal como se pode observar em todos os gráficos referentes à memória utilizada.

## 3.3 Tabela com as medições de velocidade de navegação na rede

De forma a se conseguir obter dados para a realização do presente trabalho, foi necessário efetuar quatro tipo distintos de medições.

Como foi explicado na secção anterior, todos os testes realizados tiveram por base as mesmas operações. Assim, foram realizados testes recorrendo ao browser Tor, com e sem a utilização de uma ferramenta de VPN externa e ao browser Mozilla Firefox também utilizando o serviço de VPN numa primeira medição e numa segunda sem qualquer tipo de VPN incorporado.

No que diz respeito ao browser Tor com recurso ao serviço de VPN, os resultados obtidos podem ser observados na **Tabela 1**, localizada no canto inferior da página 4, começando, então, com o valor correspondente ao "*Query Request*". Nesta medição, o valor médio encontrado é 510 m, e representa o tempo, em milissegundos, a que os *requests* estiveram sujeitos. Relativamente ao campo "*Memory Allocation*" existiu um valor médio, no intervalo de tempo alvo de análise, de 4,45Mb, o que simboliza que foi alocado este valor durante a respetiva análise.

O próximo valor medido foi a "*Memory Usage"* que nos devolve, em percentagem, a memória utilizada pelo sistema operativo, tendo neste caso o valor de 58,57%.

No que diz respeito ao "*Memory Mallocs e Frees*", que representam a memória utilizada para processos de escrita ou para libertações de memória durante este processo, estes apresentam um valor médio igual de 68k.

Quanto ao "*Request bytes*" e "*Response bytes*", estes valores simbolizam a quantidade de informação transmitida através de um

pedido ao servidor e os bytes associados às respostas do servidor, respetivamente. Como se pode observar na tabela 1, a quantidade de *bytes* durante o processo de *request* (456k) é bastante inferior à apresentada no de *response* (1.23G), o que seria de esperar, tendo em conta que o servidor quando envia resposta tem que juntar mais informação ao pedido solicitado. Por fim, pode ainda observar-se que durante o tempo em estudo existiu um total de 1,03k de leituras.

De seguida foi efetuada uma outra análise no browser Tor, porém sem o recurso ao serviço de VPN *Windscribe*. Desta feita, não se registou qualquer valor durante o processo de "*Query Request"* não existindo qualquer tipo de pedidos à API do *InfluxDB.*

No que concerne à "*Memory Allocation*", pode observar-se um valor bastante menor que o anterior, registando 248k. Como não existiu uma alocação de memória bastante menor seria de esperar, tal como aconteceu, que a percentagem de memória utilizada também apresentasse um decréscimo, representando assim 47,41% de valor médio durante esta análise.

Analisando o campo "*Memory Mallocs e Frees*", é apresentando uma diferença substancial entre os *mallocs* e os processos de *free*, registando 3,27k e 34k, respetivamente. Tal como aconteceu na análise efetuada ao browser Tor com recurso a VPN, nos campos "*Request Bytes"* e "*Response Bytes*", são apresentados valores mais elevados no processo de "*Response*" (1,98G) do que no processo de "*Request*" (686k). Por fim, esta análise apresentou um número bastante inferior de leituras, sendo registado um valor médio de 63.49B.

Finalizados os testes no browser Tor, iniciou-se a análise do Mozilla Firefox. Durante o processo de medição com o recurso à VPN, foram registados diferentes valores.

Sobre o "*Query Request*" não existiu pedidos à API do *InfluxDB*, sendo registado o valor de 0 neste processo. Em relação à memória alocada, existiu uma alocação de 186k, registando assim um uso de 50,63% de memória.

No que diz respeito ao processo de *mallocs* e *frees*, existiu um valor superior nas operações de escrita (32,7k) do que nas libertações de memória (24k). Interpretando os valores de "*Request bytes*" e "*Response bytes*", existiu, tal como nas análises no Tor, um valor de *bytes* superior nas respostas do servidor (1,99 Gb) do que nos pedidos por parte do browser (709,4k).

Na Tabela 1, conseguimos, igualmente, observar os valores obtidos para o browser Mozilla Firefox sem recurso à utilização de VPN e com recurso à VPN.

Nas medições sem VPN, conseguiu-se perceber que os valores obtidos para as medições sem VPN no browser Tor e com VPN no browser Mozilla Firefox são, de certa forma, semelhantes, visto estarem em pé de igualdade nas condições da medição, pois o browser Tor só por si já apresenta uma VPN na sua constituição.

Quanto às medições com recurso à VPN, sobre a alocação de memória, foi registado um valor de 123,7k, representando 49,10% da utilização de memória.

Relativamente aos processos de *mallocs* e *frees*, foram registados os valores mais baixos de todas as análises efetuadas, 2,89k e 2,18k, respetivamente.

Observando os campos relativos ao *request* e *response bytes*, mais uma vez, verificou-se um maior número de *bytes* durante o processo de *response* (1,99G) do que no processo de *request* (751,9k). Todo este processo obrigou a um total de leituras de 30B.

**Tabela 1-** Medições obtidas através do software Chronograf.

| **Medições obtidas do *software*** | | | | |
|---|---|---|---|---|
| | Tor | | Mozilla Firefox | |
| | Sem VPN | Com VPN | Sem VPN | Com VPN |
| Query request | 0 | 510 m | 0 | 0 |
| Memory Allocation | 248 k | 4,45 M | 123,7k | 186 k |
| Memory Usage (%) | 47,41% | 58,57% | 49,10% | 50,63% |
| Memory Mallocs e Frees | 3,27 k / 34 k | 68 k / 68 k | 2,89 / 2,18k | 32,7k / 24 k |
| Total de leituras | 63,49 B | 1,03k | 30 B | 46 B |
| Request bytes | 686 K | 456 k | 751,9 k | 709,4 k |
| Response bytes | 1,98 G | 1,23 G | 1,99 G | 1,99G |

Tendo por base a análise da tabela anterior, iremos proceder à comparação entre os valores obtidos nos dois browsers.

Podemos, então, observar, em primeiro lugar, que existiu um número superior no browser Tor (510 m) face ao Mozilla Firefox (0) relativo ao *query request* à API do *InfluxDB*.

No que concerne à alocação e percentagem de memória utilizada, regista-se um valor bastante superior em ambos os parâmetros no browser Tor (4,45M e 58,57%) face ao Mozilla Firefox que apresenta como alocação de memória 186k e 50,63% de utilização de memória. Através da comparação da memória da máquina virtual utilizada, de 4GB, com as percentagens médias obtidas das medições, é possível aferir que na medição do browser Tor com VPN, a memória utilizada foi de 2,35 GB o que se pode aferir que foi mais de metade da RAM existente. O que seria de esperar, dadas as conclusões que se têm tirado ao longo da análise das medições, onde o browser Tor apresenta ineficiência no seu desempenho.

Analisando os valores de memória empregue em processos de escrita e libertação desta, existe um registo de 68k em ambos no Tor em comparação com 32,7k e 24k no Firefox. O que poderá indicar que como o browser Tor se torna ainda mais ineficiente do que já é, naturalmente, com a utilização de VPN, visto que os pedidos de escrita demoram mais tempo a ocorrer, devido a ter de existir uma verificação dos certificados que garantem a encriptação dos dados e garantir que existe a criação de um circuito aleatório para enviar a informação antes de carregar a resposta ao cliente.

Examinando a parte correspondeste ao *request* e *response bytes*, foi no browser da Mozilla que se registaram valores superiores (709,4k e 1,99G com VPN, face aos 456k e 1,23G registados pelo Tor, com VPN), porém não é uma diferença significativa, tendo em conta que o número de pedidos e de respostas foi o mesmo em todos os testes realizados.

Por último, e tendo em conta o total de leituras realizadas, foi no browser Tor que se registaram valores superiores (1,03k) contra 46B do Mozilla Firefox.

## 4 Conclusão

Com a realização deste trabalho podemos concluir que o browser Tor, nas suas versões mais recentes, se está a aproximar de uma estrutura semelhante ao Mozilla Firefox, visto que as medições sem VPN no browser Tor e com VPN no browser Mozilla Firefox são bastante semelhantes. O que indica que os parâmetros de navegação que estão a ser avaliados permitem resultados reais aquando dos testes realizados para a realização deste trabalho.

Assim sendo, é possível concluir, pela Tabela 1, que o browser Tor é mais oneroso para o sistema operativo que o Mozilla Firefox, quer com VPN, quer sem VPN, porém é o preço a pagar quando se pretende fazer uma navegação pela rede de forma segura e sem comprometimento da nossa verdadeira identidade.

De um modo geral, consideramos que o trabalho vai de encontro às expectativas que nos foram propostas aquando da apresentação dos temas em jogo e com isto conseguimos consolidar melhor os nossos conhecimentos face ao funcionamento da rede Tor e o efeito que um serviço de VPN poderá ter em questões de eficiência e rapidez.

## Referências

[1] E. Monteiro e F. Boavida, Engenharia de Redes Informáticas, Lisboa: FCA-Editora de Informática, 2011.

[2] M. Antunes e B. Rodrigues, Introdução à Cibersegurança- A Internet, Os Aspetos Legais e a Análise Digital Forense, Lisboa: FCA-Editora de informática, 2018.

[3] "Rede TOR," [Online]. Available: serverdo.in.

[4] "Security/Tor Uplift," 18 julho 2019. [Online]. Available: wiki.mozilla.org.