

COMO INSTALAR SUA PRÓPRIA REDE TOR: UM GUIA

HOW TO INSTALL YOUR OWN TOR NETWORK: A GUIDE

¹BARBIERI, B. ; ²SANTOS, J. S.

^{1e2}Departamento de SISTEMA DE INFORMAÇÃO –Faculdades Integradas de Ourinhos-FIO/FEMM

RESUMO

Inicialmente criada como uma rede governamental para pesquisa, design e análise de sistemas anônimos de comunicação, a rede TOR (The Onion Router) evoluiu para uso não governamental através do projeto Tor (Tor Project). Após as denúncias de espionagem de dados registradas, principalmente, em sites como o Wikileaks, vem à tona a questão “como garantir a confidencialidade dos dados”? O objetivo deste trabalho é apresentar montagem de uma rede Tor particular que garanta privacidade e confidencialidade na comunicação entre dois pontos.

Palavras-chave: TOR. Redes. Sistemas Anônimos de Comunicação.

ABSTRACT

Initially created as a governmental network for purposes of research, design and analysis into anonymous communication systems, the TOR (The Onion Router) network evolved for non-governmental use through The Tor Project. After the recorded allegations of data spying, primarily in websites like Wikileaks, the question comes up “how to ensure data confidentiality”? The goal of this research paper is to teach you how to assemble your own private Tor network as to ensure privacy and confidentiality in the communication between two points.

Keywords: TOR. Networks. Anonymous Communication Systems.

INTRODUÇÃO

Assunto cercado de mitificação e desconhecimento, a Segurança da informação é hoje um dos principais assuntos quanto se fala em Tecnologia da informação. Sites como o WikiLeaks, são responsáveis por difundir informação de como órgãos governamentais, têm, indevidamente, se apropriado de informações pessoais e empresariais ao redor do mundo. Tais notícias elevam a preocupação com a quebra do direito à privacidade.

A rede Tor, inicialmente criada para fins de pesquisa em comunicação anônima e privada, hoje é responsável por milhões de dólares em negócios ilegais, só nos Estados Unidos.

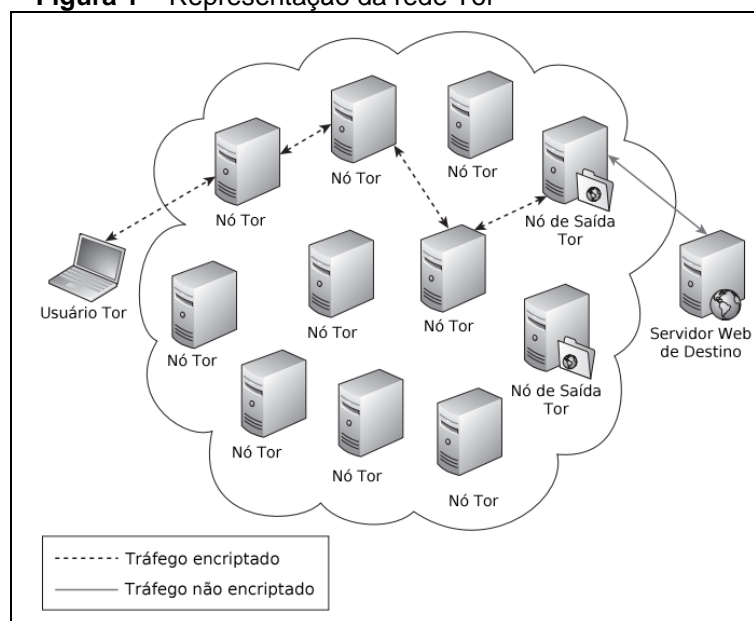
O objetivo deste é demonstrar a instalação de uma Rede Tor para uso particular, não público, como forma de se obter privacidade e confidencialidade na transmissão de dados utilizando o meio público chamado Internet. Tal prática é

muito utilizada por Cyberpunks (um tipo de hacker) extremamente preocupados em manter suas comunicações de dados fechadas ao acesso de terceiros.

A rede Tor é uma rede composta de túneis HTTPS, sobrejacentes à Internet, onde é fornecido um BIND (servidor DNS mais utilizado da Internet), geralmente na porta 9050 local para usar um servidor Proxy SOCKS5 (servidor que permite aplicações cliente-servidor transparentemente em um serviço de uma rede ao firewall) e apontados para o endereço local, com navegadores devidamente configurados para navegação, então os roteadores da rede Tor fazem o roteamento do endereço digitado de saída até seu destino, passando por vários nós da rede, fazendo que o usuário não tenha um IP fixo de saída, pois o Tor faz esse IP passar por várias camadas, redirecionando para diversos IP da rede, ficando assim o rastreamento do conteúdo difícil de ser localizado, e com conteúdos criptografados, o pacote chega ao seu destino com uma senha que só o destinatário tem acesso para desbloquear e abrir o conteúdo enviado.

Ligh et al. (2011, p. 2) definem Tor como “uma rede de computadores ao redor do mundo que envia requisições de forma criptografada do início da requisição até chegar na última máquina da rede, conhecida como o nó de saída. A partir desse ponto, a requisição é descriptografada e enviada ao servidor de destino. Nós de saída são usados especificamente como o último hop para o tráfego que sai da rede Tor e então como o primeiro hop para o tráfego que retorna”.

Figura 1 – Representação da rede Tor



Fonte: Adaptado de Ligh et al. (2011, p. 2)

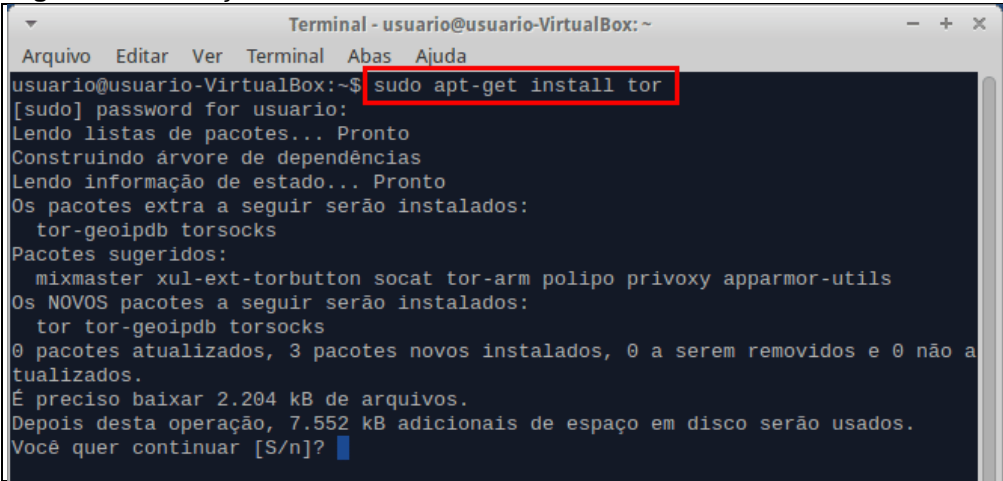
MATERIAL E MÉTODOS

1) Sistema Operacional

O sistema operacional utilizado para testes foi o Linux Xubuntu, instalado em máquina virtual VirtualBox, com recursos limitados. Para instalação em máquinas reais, recomenda-se utilizar a versão 13.04 da distribuição Ubuntu, sendo que a interface gráfica utilizada (ex: Gnome, Unity) pode ser de livre escolha.

2) Servidor Tor

Primeiramente, deve ser instalado o servidor Tor e configurado de modo a funcionar como um servidor privado, isto significa que outras pessoas utilizando programas de acesso à rede Tor não terão acesso a este servidor em particular. À denominação “servidor” entende-se que provê um serviço na rede, neste caso, o serviço é receber as requisições criptografadas de nosso cliente, outro software, descriptografá-las e direcioná-las ao destino. A versão do servidor Tor utilizada foi 2.3.25-13, é importante considerar que algumas configurações podem mudar ou não existir em outras versões.

Figura 2 – Instalação do Tor


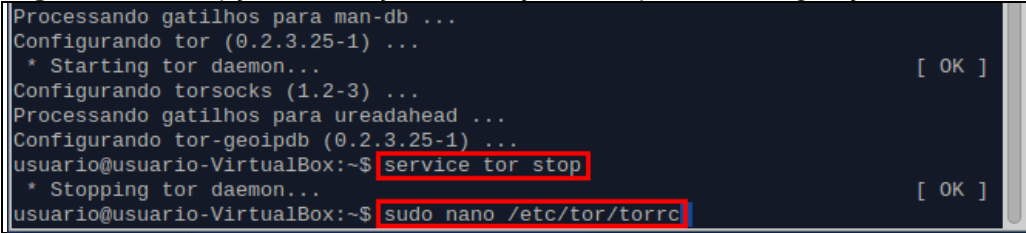
```

Terminal - usuario@usuario-VirtualBox: ~
Arquivo Editar Ver Terminal Abas Ajuda
usuario@usuario-VirtualBox:~$ sudo apt-get install tor
[sudo] password for usuario:
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os pacotes extra a seguir serão instalados:
  tor-geoipdb torsocks
Pacotes sugeridos:
  mixmaster xul-ext-torbutton socat tor-arm polipo privoxy apparmor-utils
Os NOVOS pacotes a seguir serão instalados:
  tor tor-geoipdb torsocks
0 pacotes atualizados, 3 pacotes novos instalados, 0 a serem removidos e 0 não a
tualizados.
É preciso baixar 2.204 kB de arquivos.
Depois desta operação, 7.552 kB adicionais de espaço em disco serão usados.
Você quer continuar [S/n]? █

```

Fonte: os autores

Após a instalação do servidor Tor, devemos parar o serviço em execução e abrirmos o arquivo de configuração para realizar as alterações necessárias.

Figura 3 – Interrupção do serviço Tor e edição do arquivo de configuração


```

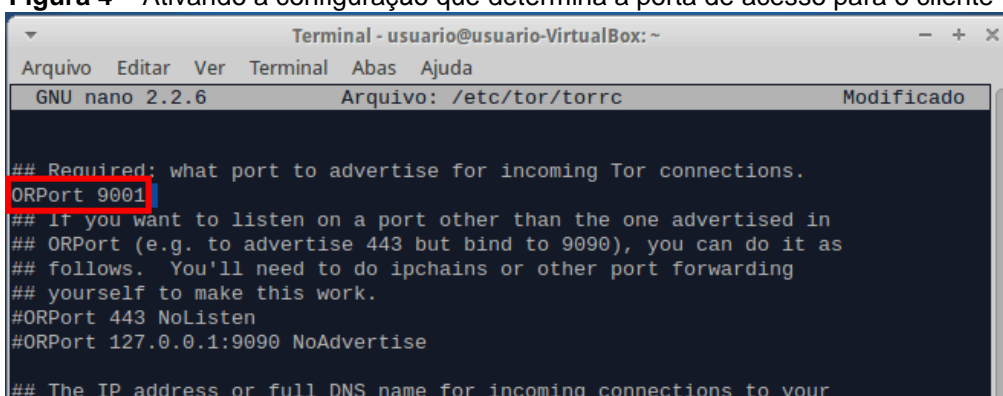
Processando gatilhos para man-db ...
Configurando tor (0.2.3.25-1) ...
* Starting tor daemon... [ OK ]
Configurando torsocks (1.2-3) ...
Processando gatilhos para ureadahead ...
Configurando tor-geoipdb (0.2.3.25-1) ...
usuario@usuario-VirtualBox:~$ service tor stop
* Stopping tor daemon... [ OK ]
usuario@usuario-VirtualBox:~$ sudo nano /etc/tor/torrc

```

Fonte: os autores

Com o arquivo de configuração aberto para edição, devemos adicionar algumas configurações ou apenas remover o caractere de comentário – no caso, é o caractere cerquilha (#) – para que a configuração existente seja utilizada, ao invés de ser ignorada.

Para configuração do servidor para uso privativo, as configurações devem estar como segue:

Figura 4 – Ativando a configuração que determina a porta de acesso para o cliente


```

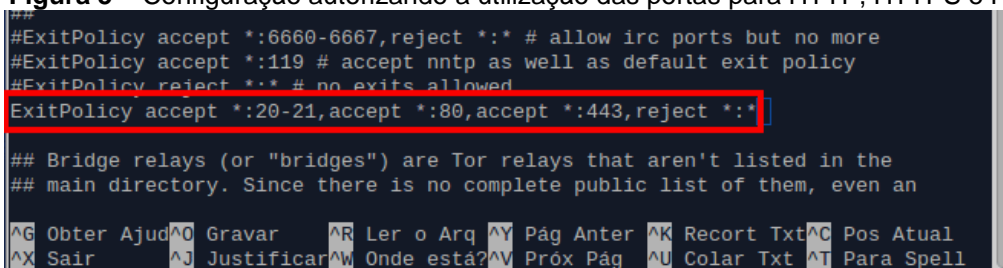
Terminal - usuario@usuario-VirtualBox: ~
Arquivo Editar Ver Terminal Abas Ajuda
GNU nano 2.2.6 Arquivo: /etc/tor/torrc Modificado

## Required: what port to advertise for incoming Tor connections.
ORPort 9001
## If you want to listen on a port other than the one advertised in
## ORPort (e.g. to advertise 443 but bind to 9090), you can do it as
## follows. You'll need to do ipchains or other port forwarding
## yourself to make this work.
#ORPort 443 NoListen
#ORPort 127.0.0.1:9090 NoAdvertise

## The IP address or full DNS name for incoming connections to your

```

Fonte: os autores

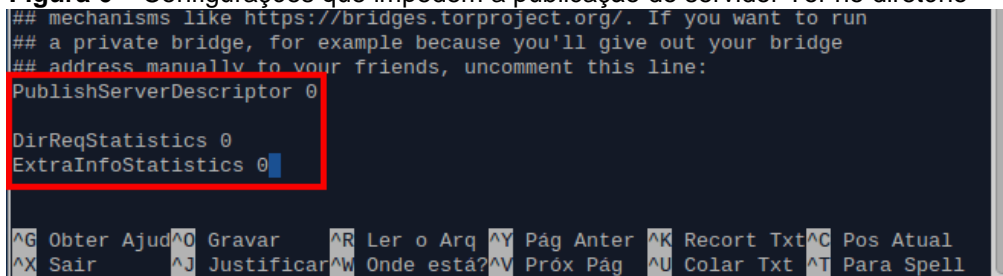
Figura 5 – Configuração autorizando a utilização das portas para HTTP, HTTPS e FTP


```

###
#ExitPolicy accept *:6660-6667,reject *:* # allow irc ports but no more
#ExitPolicy accept *:119 # accept nntp as well as default exit policy
#ExitPolicy reject *:* # no exits allowed
ExitPolicy accept *:20-21,accept *:80,accept *:443,reject *:*
## Bridge relays (or "bridges") are Tor relays that aren't listed in the
## main directory. Since there is no complete public list of them, even an
^G Obter Ajuda ^O Gravar ^R Ler o Arq ^Y Pág Anter ^K Recort Txt ^C Pos Atual
^X Sair ^J Justificar ^W Onde está? ^V Próx Pág ^U Colar Txt ^T Para Spell

```

Fonte: os autores

Figura 6 – Configurações que impedem a publicação do servidor Tor no diretório


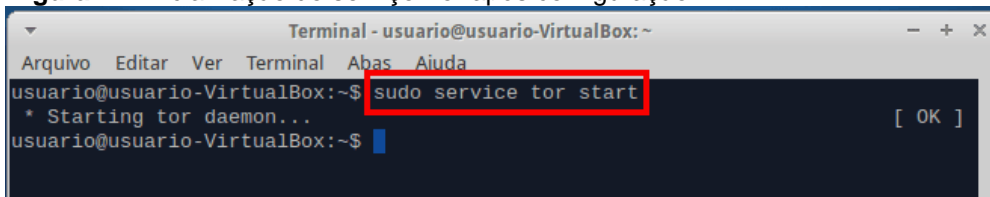
```

## mechanisms like https://bridges.torproject.org/. If you want to run
## a private bridge, for example because you'll give out your bridge
## address manually to your friends, uncomment this line:
PublishServerDescriptor 0
DirReqStatistics 0
ExtraInfoStatistics 0
^G Obter Ajuda ^O Gravar ^R Ler o Arq ^Y Pág Anter ^K Recort Txt ^C Pos Atual
^X Sair ^J Justificar ^W Onde está? ^V Próx Pág ^U Colar Txt ^T Para Spell

```

Fonte: os autores

A combinação das configurações acima serve para determinar a porta que o cliente deve utilizar para realizar o acesso através do servidor Tor, quais serviços podem ser utilizados através desse servidor – no caso apenas HTTP, HTTPS e FTP – e faz com que nosso servidor privado não seja publicado no diretório público, o que é feito por padrão, pelo fato do Tor ser um projeto de natureza colaborativa.

Figura 7 – Inicialização do serviço Tor após configuração

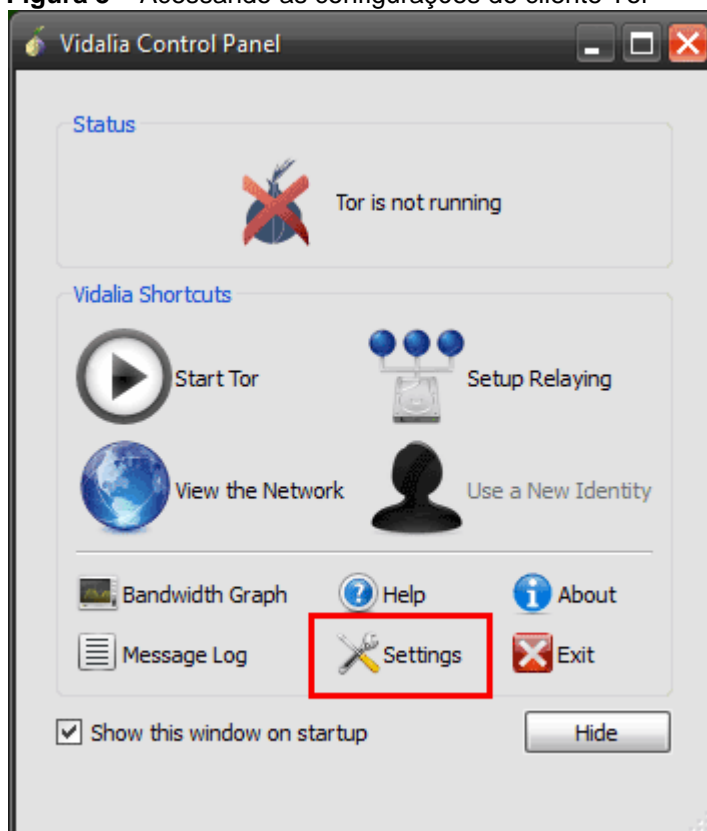
```
Terminal - usuario@usuario-VirtualBox: ~
Arquivo Editar Ver Terminal Abas Ajuda
usuario@usuario-VirtualBox:~$ sudo service tor start
* Starting tor daemon... [ OK ]
usuario@usuario-VirtualBox:~$
```

Fonte: os autores

Após a realização da configuração, o servidor Tor que estava parado deve ser iniciado novamente, para se tornar disponível para acesso.

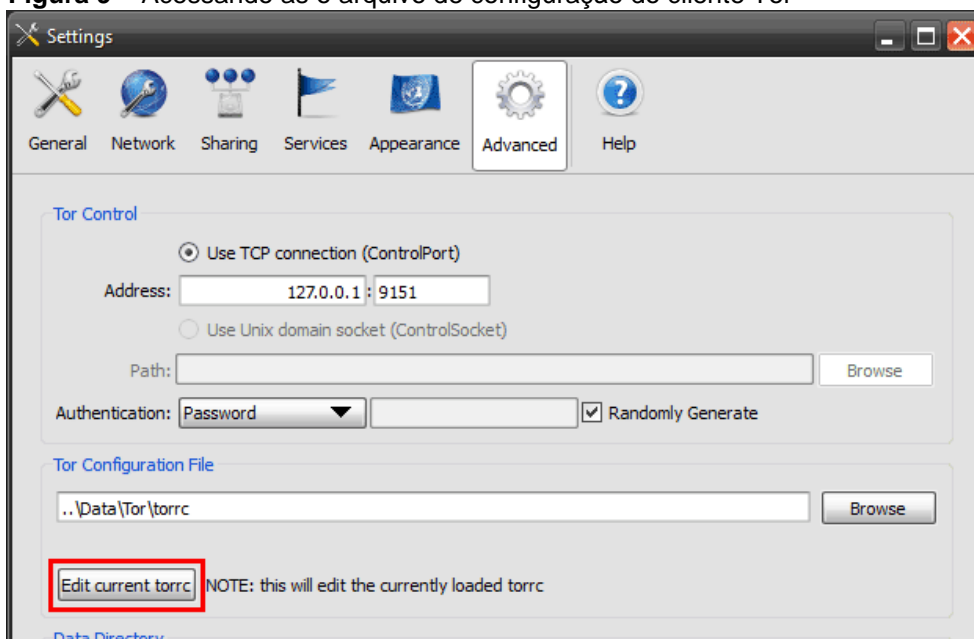
3) Cliente Tor

Para configuração do cliente Tor, foi utilizado o Tor Browser Bundle, aplicação que funciona sem a necessidade de instalação e é composta do navegador Mozilla Firefox modificado e configurado para a utilização da rede Tor.

Figura 8 – Acessando as configurações do cliente Tor

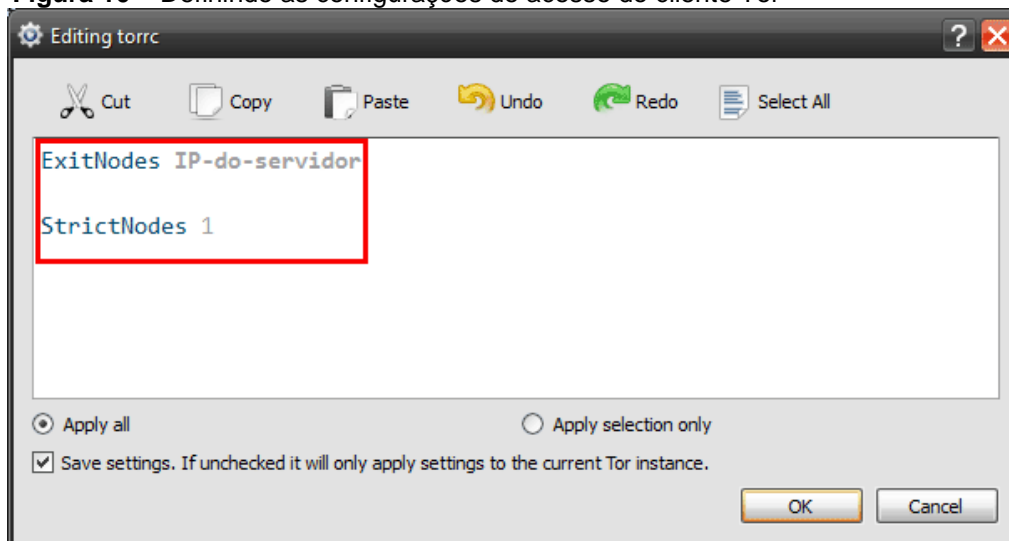
Fonte: os autores

Figura 9 – Acessando as o arquivo de configuração do cliente Tor



Fonte: os autores

Figura 10 – Definindo as configurações de acesso do cliente Tor



Fonte: os autores

No campo ExitNodes deve ser colocado o endereço IP do servidor Tor previamente configurado, isto fará com que a aplicação cliente, ou seja, o Tor Browser Bundle utilize nosso servidor, e apenas ele, como o nó de saída, que é o nó que envia uma requisição para o destinatário desejado, removendo a criptografia dos pacotes recebidos e os direcionando.

RESULTADOS E DISCUSSÃO

Utilizando uma distribuição Linux, como o Ubuntu, a instalação da rede Tor não apresenta grandes dificuldades, para que se tenha uma rede própria e privada é necessário instalar tanto o servidor, quanto o cliente, e não se devem utilizar outros nós na rede. Sendo possível transmitir dados entre dois pontos utilizando a estrutura pública da Internet como caminho, porém com confidencialidade.

CONCLUSÃO

A rede Tor permite uma navegação com privilégios de anonimato e criptografia, porém sempre há riscos de violação de informação quando se utilizam seus nós espalhados pela Internet. Montar uma rede Tor privativa, permite que se transmitam pacotes de rede com os mesmos privilégios, porém sem o risco de violação da informação.

Esse tipo de rede pode ser útil para utilização com acessos remotos que necessitem de privacidade.

REFERÊNCIAS

LIGH, M. H. et al. **Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code**. Indianapolis: Wiley Publishing, Inc., 2011.

PEREIRA, Leonardo. **Deep web**: saiba o que acontece na parte obscura da internet. Disponível em: <<http://olhardigital.uol.com.br/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120>>. Acesso em: 27 set. 2013.

STALLINGS, W. **Criptografia e segurança de redes**: Princípios e práticas. Tradução de Daniel Vieira. 4. ed. São Paulo: Pearson Prentice Hall, 2008.