IMPLEMENTAÇÃO DE VPNS SEGURAS COM ÊNFASE NA QUALIDADE[1]

Igor Cristiano Tibuski[2]

Marcos Mikalovicz[3]

Robson Hugo Henning[4]

RESUMO

A Internet vem crescendo consideravelmente desde sua criação em meados da década de 1980. Devido a este crescimento, surgiu a necessidade de garantir uma maior segurança na troca de dados entre pontos distintos. O meio garantido e de confiança é a criação de VPN, onde constitui de uma rede virtual que permite duas redes se conectarem de forma segura utilizando um canal público de comunicação, criando assim, um tunelamento que transmite os dados criptografados entre as redes. Este artigo retrata a implantação de três modos de VPN visando à agilidade na transmissão de dados.

Palavras Chave: Tunelamento, Criptografia, Protocolos.

ABSTRACT

The Internet has grown considerably since its inception in mid 1980. Due to this growth, the need arose to ensure greater security in the exchange of data between different points. The secured and trusted environment is the creation of VPN, which is a virtual network that allows two networks to connect securely using a public communication channel, thus creating a tunneling to transmit encrypted data between networks. This article depicts the implementation of three methods of targeting VPN agility in data transmission.

Key Words: Tunneling, Cryptography, Protocols.

---

[1] Trabalho desenvolvido para obtenção de conceito na disciplina de Trabalho de Conclusão de Curso, do Curso de Sistemas de Informação da Universidade do Contestado.

[2] Universidade do Contestado - Campus Mafra, Curso de Sistemas de Informação. Endereço: Rua Duque de Caxias, 366, Bairro Buenos Aires; Mafra SC; email:igor.ti91@gmail.com

[3] Universidade do Contestado - Campus Mafra, Curso de Sistemas de Informação. Endereço: Rua Tenente Ary Rauen, 98, Bairro Centro; Papanduva SC; email:marcosmikalovicz@msn.com

[4] Professor Orientador - Professor da Universidade do Contestado, UnC – Campus Mafra. Mestre em Ciência da Computação – Universidade Federal de Santa Catarina – UFSC, Brasil (2006)

INTRODUÇÃO

Quando surgiram as redes de computadores o principal objetivo era apenas conectar-se à outras máquinas, não havia tanta preocupação com a segurança de quem e quando os dados seriam acessados. Juntamente com a expansão e os avanços tecnológicos, obtivemos diversas formas de conectarmos uns aos outros. Para ligar objetos do dia-a-dia à Internet e às grandes bases de dados, é necessária uma combinação de um sistema eficiente de identificação e do uso de tecnologias sensoriais [BARCELLOS, 2013]. Uma forma segura de garantir a comunicação entre redes distintas é através da utilização de protocolos baseado em *Virtual Private Network* (VPN).

Em VPN, *Private* significa à forma de como os dados trafegam. São previamente criptografados para garantir total privacidade das informações na conexão. O termo *Virtual* indica que as máquinas conectadas à rede, não precisam estar no mesmo meio físico para funcionarem, podem assim, estar há quilômetros de distancia através de uma rede virtual. Ao abrir um portal VPN em seu equipamento, seja computador, tablet, smartphone ou navegar em um site VPN, o usuário trabalhará sob a proteção de VPN em sua série específica de computadores e redes [SILVA, 2013]. No artigo proposto, testamos a criação de túneis entre duas extremidades da conexão, sendo assim, os dados trafegam de uma ponta a outra de uma forma segura, prevalecendo à integridade dos dados originais.

DESENVOLVIMENTO

Definição de VPN

Virtual Private Network ou Rede Privada Virtual é constituída de uma rede privada que trabalha juntamente com a infraestrutura de uma rede pública como a Internet. A utilização da Internet em conexões privadas é uma ótima solução olhando através de custos e investimentos, porém, não em termos de privacidade, pois como é um meio público esses dados em trânsito podem ser lidos por qualquer pessoa conectada a rede, sendo totalmente inseguro. Dessa maneira a VPN surge como meio de incorporar a criptografia na comunicação entre os *hosts* da rede privada, assim, se os dados forem capturados durante a sua transmissão, dificilmente poderão ser decifrados sem os devidos meios de autenticação.

Os túneis virtuais habilitam o tráfego de dados criptografados pela Internet e esses dispositivos são capazes de decifrar esta criptografia formando uma rede virtual segura sobre

a Internet. Esses dispositivos de gerenciamento de VPN devem ser capazes de garantir a privacidade, integridade e a autenticidade dos dados. A VPN do tipo *Security* se utiliza de técnicas de criptografia para criar um canal de comunicação blindado. [OLIVEIRA; ABBOUD, 2013].

Figura 1. Exemplo de conexão VPN

A que se destina

A implantação de VPN é indicada nestes casos:

- Empresas que possuem filiais ou escritórios distantes entre si, onde cada escritório tenha uma intranet própria e haja a necessidade de se comunicar em forma de uma rede só.
- Funcionários, que trabalham em casa ou que estão em viagem e precisam acessar a rede do escritório de forma segura e rápida para utilizar recursos como se estivessem em seu local de trabalho.
- Empresas que queiram interligar sua rede com seus fornecedores ou clientes de uma forma mais direta, podendo ter acesso seguro as informações do Banco de Dados, por exemplo.
- Qualquer empresa ou pessoa que queira unir duas redes privadas, através de um meio público de uma maneira segura e confiável.

Elementos

Os principais elementos presentes em uma VPN são:

- **Autenticação:** Os dados são autenticados para assegurar que eles vieram de usuários validos, através da utilização de protocolos de autenticação, que geralmente são constituídos por algoritmos de *hash* como MD5. Desta forma, a integridade dos dados é garantida do inicio ao fim da transmissão.
- **Tunelamento:** É a forma de como os dados trafegam pela conexão VPN. O túnel certifica que os dados que estiverem trafegando pelo mesmo, permaneçam ininteligíveis para quem não fizer parte dele. Isso garante que se a informação for capturada, será muito difícil entendê-la, a menos que se descubra a chave previamente utilizada.
- **Transporte Subjacente:** O protocolo TCP/IP é a base da comunicação via Internet, devido a isso ele apresenta falhas de segurança. Isto faz com que os dispositivos VPN adicionem alguns cabeçalhos, o que possibilita a instalação destes em qualquer parte da rede.

Topologias

Existem três topologias em redes VPN:

- **Host-host:** É a comunicação entre dois microcomputadores separados fisicamente, podem estar ou não em uma mesma rede.
- **Host-gateway**: Conexão de um microcomputador a uma rede fisicamente distante.
- **Gateway-gateway:** Conexão entre duas redes VPN, porem possuem a característica de estar sempre conectados.

Protocolos

O protocolo de VPN é responsável pelo gerenciamento das conexões VPN, é ele quem define as configurações que serão utilizadas de acordo com seu modo de utilização. Por mais

que duas máquinas estejam conectadas à mesma rede, se não “falarem” a mesma língua, não há como estabelecer uma comunicação [MARTINS, 2012].

PPTP

Este protocolo é considerado simples e de fácil configuração, permite a transferência segura de dados baseadas em redes IP. Desenvolvido como uma extensão do protocolo Ponto a Ponto (PPP), o PPTP proporciona um nível maior de segurança e comunicação com multiprotocolos na Internet.

De forma geral, o protocolo PPTP utiliza o PPP para estabelecer a conexão entre o cliente PPTP e o servidor de acesso à rede (NAS - *Network Access Server* ou ISP - *Internet Service Provider*). Os dados encapsulados pelo cabeçalho PPP ganham um cabeçalho chamado GRE (*Generic Routing Encapsulation*) para o transporte dos dados. Após, ocorre à criação de uma conexão onde são estabelecidos os parâmetros de configuração da conexão entre os extremos do túnel. Dessa forma, é criado o túnel PPTP, possibilitando a criação da VPN.

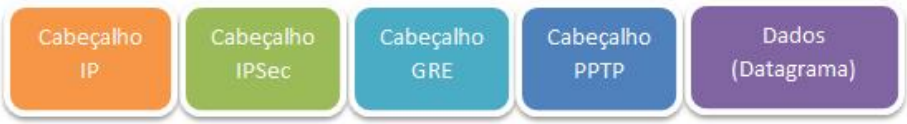

Figura 2. Conexão PPTP

Layer Two Tunneling Protocol (L2TP)

O L2TP oferece flexibilidade do protocolo IP com a privacidade do *Frame Relay* ou ATM, permitindo que os serviços de rede sejam enviados nas terminações de cada túnel. Além disso, permite que as extremidades do túnel sejam autenticadas para reforçar ainda mais sua segurança.

Originalmente, o L2TP foi desenvolvido para ser aplicado através de dois modos:

- **Voluntário:** Permite a inicialização através de um computador remoto, proporciona uma ótima aplicação para usuários em trânsito que necessitam discar de qualquer provedor, como o provedor não participa da criação do

túnel, pode-se percorrer vários servidores sem que haja uma previa configuração.

- **Compulsório:** Criado automaticamente pelo servidor de acesso, isso faz com que haja a necessidade que o servidor de acesso à rede seja pré-configurado para identificar qual a terminação necessária, com base na autenticação de usuários.

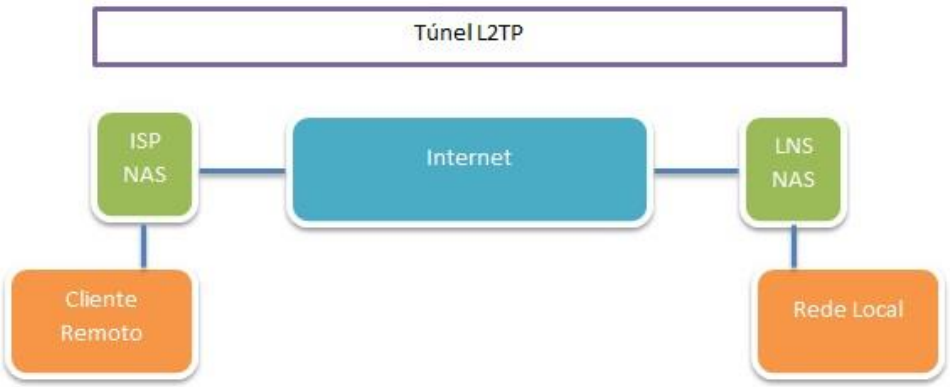

Figura 3. Conexão L2TP

Possui também, mecanismos de autenticação dentro do protocolo PPP, os protocolos PAP e CHAP. Porém, o L2TP não possui processos para gerenciamento de chaves criptográficas, sendo assim suscetível a ataques. Uma forma de assegurar ainda mais este protocolo, é a integração com o protocolo IPSec.

Ip Security (IPSEC)

Surgiu em meados de 1995 devido às falhas de seguranças encontradas no protocolo IP. Esse conjunto de protocolos fornece principalmente serviços de integridade, autenticação, controle de acesso e confidencialidade garantindo assim, uma maior estabilidade.

O IPSec pode trabalhar de duas formas diferentes:

- Modo transporte: É o modo nativo do IPSec, nele há transmissão direta dos dados devidamente protegidos entre os *hosts*. Toda a autenticação e cifragem são realizadas na mensagem *(payload)*, ou seja, ocorre na transmissão dos dados. Este modo é utilizado em comunicações host-a-host.

Figura 4. Estrutura do Pacote IPSec – Modo Transporte

- **Modo túnel:** O pacote original é encapsulado por inteiro em um novo pacote com a criptografia gerado pelo IPSec incluindo o cabeçalho original, após é enviado para o outro *gateway* IPSec que desencapsula e o encaminha ao destino (figura 5).

Figura 5. Estrutura do Pacote IPSec – Modo Túnel

Dentro do IPSec existe a *Security Association* (SA), uma biblioteca que contem todas as informações necessárias para aceitar as conexões entre as entidades do IPSec. Elas são criadas durante o processo de aceitação dos parâmetros da conexão, uma SA contem as informações na forma de algoritmos de criptografia, chaves secretas ou sequencias de números, funções *hash*, modo de funcionamento (túnel ou de transporte), porta de comunicação, entre outros.

Existem dois bancos de dados utilizados dentro do IPSec, o *Security Police Database* (SPD) e o *Security Association Database* (SAD). O SPD possui suas politicas de segurança submetidas nos pacotes. Essas politicas são definidas pelo administrador do sistema e serão utilizadas pela SA durante o processamento do pacote IP. O SAD faz com que os pacotes passem por regras, o pacote que aceitar pelo menos uma dessas regras sofrerá a ação determinada pelo administrador. Esta ação pode ser: recusar o pacote, aceitar o pacote e aplicar o IPSec sobre ele, ou deixa-lo entrar sem aplicar o IPSec.

O IPSec apresente três características gerais:

- ***Authentication Header* (AH):** O protocolo AH provê a autenticação e integridade dos dados, mas não a confidencialidade. Previne ataques do tipo *replay*, *spoofing e hijacking*. Insere um cabeçalho dentro do pacote, anexa um numero sequencial, que é zerado a cada nova associação segura e adiciona funções de *hash* ao AH.

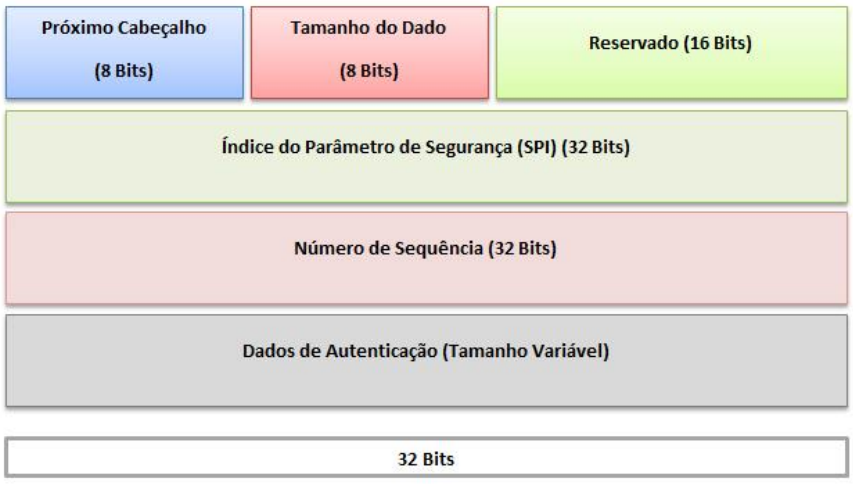

Figura 6. Campos do cabeçalho AH

- ***Encapsulation Security Payload* (ESP):** Com características do AH, este protocolo também fornece a confidencialidade dos dados. Ele adiciona um cabeçalho ESP logo após o anexo do cabeçalho AH e criptografa todos os dados com um algoritmo gerado durante o estabelecimento da aceitação da conexão (SA).

Figura 7. Pacote ESP

- **Gerenciamento de chaves:** Permite que uma chave de segurança seja gerada manualmente ou automaticamente pelo administrador e compartilhada com seus usuários. O protocolo principal é o *Internet Key Exchange Protocol* (IKE), que

combina com *Internet Security Association and Key Management Protocol* (ISAKMP), definindo assim como as chaves serão distribuídas.

OpenVPN

Consiste em um software livre e Open-Source que cria tuneis do tipo ponto-a-ponto ou server-to-multiclient criptografados. Permite que cada cliente utilize a autenticação pública com certificados digitais, fazendo isto através de assinaturas digitais e certificados de autoridade utilizando extensivamente a criptografia OpenSSL.

Todo pacote do OpenVPN consiste em apenas um binário tanto para conexões do lado do cliente quanto para conexões do lado do servidor. O método de autenticação com chaves secretas compartilhadas é o mais simples, e combinando com certificados ele se torna o mais robusto e rico recurso de autenticação.

Utilizando o protocolo UDP (padrão) ou TCP, consegue-se levar toda a comunicação somente por uma porta TCP/UDP, podendo trabalhar através de NAT para filtragem via firewall.

MATERIAIS E MÉTODOS

A metodologia utilizada para a implementação da arquitetura neste artigo foi à simulação e implantação de três protocolos VPN na topologia Servidor/Cliente a fim de obter as variações de velocidade/segurança de cada protocolo implementado.

Para criação do servidor foi instalada, a versão Windows Server 2008 R2 para a implementação das VPNS PPTP, L2TP (IPSec) e OpenVPN. As duas primeiras foram geradas a partir de serviços nativos na plataforma Windows, já a OpenVPN necessitou a instalação do Software Livre OpenVPN GUI.

As configurações técnicas utilizadas no servidor VPN foram:

- Processador AMD Phenom X4 920 2.80 Ghz;
- Memória RAM de 4GB;
- HD de 2 TB;
- Placa de rede on-board Fast Ethernet 100 Mbps;
- Placa de rede off-board Fast Ethernet 100 Mbps;

- Internet OI Velox de 10 Mbps de Download e 500 Kbps de Upload;

Figura 8. Teste velocidade original no Servidor

Na maquina cliente, temos Windows 7 Ultimate 64 Bits instalado. Todo processo de conexão foi feito através de configurações nativas no próprio Windows, apenas o protocolo OpenVPN precisou de Software especifico de conexão.

Foram utilizadas as seguintes configurações de hardware:

- Processador Core I5 2320 3.00 GHz;
- Memória RAM de 4 GB;
- HD de 500 GB;
- Placa de rede on-board Fast Ethernet 100 Mbps;
- Internet OI Velox de 5 Mbps e 500 Kbps de Upload;

Figura 9. Teste velocidade original no Cliente

Para a realização dos testes, foram utilizados três arquivos de formatos diferentes:

- Música em formato MP3 pesando 6,27 Mb;
- Arquivo Power Point pesando 8,95 Mb;
- Arquivo compactado (RAR) pesando 11 Mb;

Estes arquivos foram deixados em uma pasta compartilhada dentro do servidor VPN, após montar a topologia de cada VPN e realizar a conexão Cliente/Servidor, foi iniciado o download de cada arquivo cronometrando o tempo em três tentativas para se obter uma média de tempo, levando em consideração a instabilidade da conexão com a internet na região. Os valores obtidos de acordo com cada protocolo estão nas tabelas 1, 2 e 3.

A implantação da VPN PPTP é de fácil aplicação, após instalarmos o serviço necessário, foi criado um padrão de autenticação com usuário e senha onde o cliente faz a conexão e autentica para dar inicio a transmissão.

PPTP				
	Teste 1	**Teste 2**	**Teste 3**	**Média**
Música	01:45	02:14	01:44	01:54
Power Point	02:22	02:21	02:22	02:21
RAR	03:11	03:11	03:13	03:12

Tabela 1. Resultados com protocolo PPTP

A L2TP também foi instalada com serviços nativos do próprio Windows Server 2008 R2. Para assegurar ainda mais sua segurança foi aplicado também o protocolo IPSec, possibilitando assim, trabalhar com gerenciamento de chaves de segurança criada pelo administrador e compartilhada com o Cliente. Sendo assim, além de o Cliente ter que possuir um usuário e uma senha padrão, ele também precisara da chave de segurança para permitir a conexão, assegurando ainda mais o tunelamento.

L2TP (IPSec)				
	Teste 1	**Teste 2**	**Teste 3**	**Média**
Música	02:10	02:14	02:15	02:13
Power Point	02:45	02:44	02:47	02:45
RAR	03:25	03:28	03:26	03:26

Tabela 2. Resultados com protocolo L2TP (IPSec)

Já na OpenVPN, foi realizado o download do sistema de conexão OpenVPN GUI tanto no Servidor como no Cliente. O próprio site disponibiliza manuais para a devida implementação que é realizada em modo texto através de linhas de código, do modo de segurança, foi gerado um certificado digital e também compartilhada uma chave de segurança. A segurança ficou reforçada necessitando de certificado, chave e login na VPN para que a transmissão seja aceita.

OpenVPN				
	Teste 1	**Teste 2**	**Teste 3**	**Média**
Música	02:40	02:38	02:44	02:40
Power Point	03:10	03:12	03:09	03:10
RAR	04:00	04:05	04:06	04:03

Tabela 3. Resultados com protocolo OpenVPN

RESULTADOS OBTIDOS

Após a realização dos testes, ficou comprovado que a implantação das VPNs necessita de grande pesquisa e conhecimentos técnicos e científicos em redes e estrutura computacional. De modo geral, o protocolo PPTP foi mais rápido na troca de arquivos seguido por L2TP (IPSec) e por ultimo OpenVPN, conforme a tabela 4 a seguir:

Resultados			
	Música	**Power Point**	**RAR**
PPTP	01:54	02:21	03:12
L2TP (IPSec)	02:13	02:45	03:26
OpenVPN	02:40	03:10	04:03

Tabela 4. Resultados obtidos

Para uma analise mais concisa dos dados, levando em consideração a má qualidade da internet na região, previamente foi realizado três testes de conexão para que a velocidade inicial de cada teste seja a mais igual possível, possibilitando trabalhar com dados reais.

Para melhor interpretação dos resultados de tempo obtidos, foi gerado o gráfico da figura 10 que retrata de forma mais realista a diferença de tempo especificando cada protocolo e arquivo utilizado.

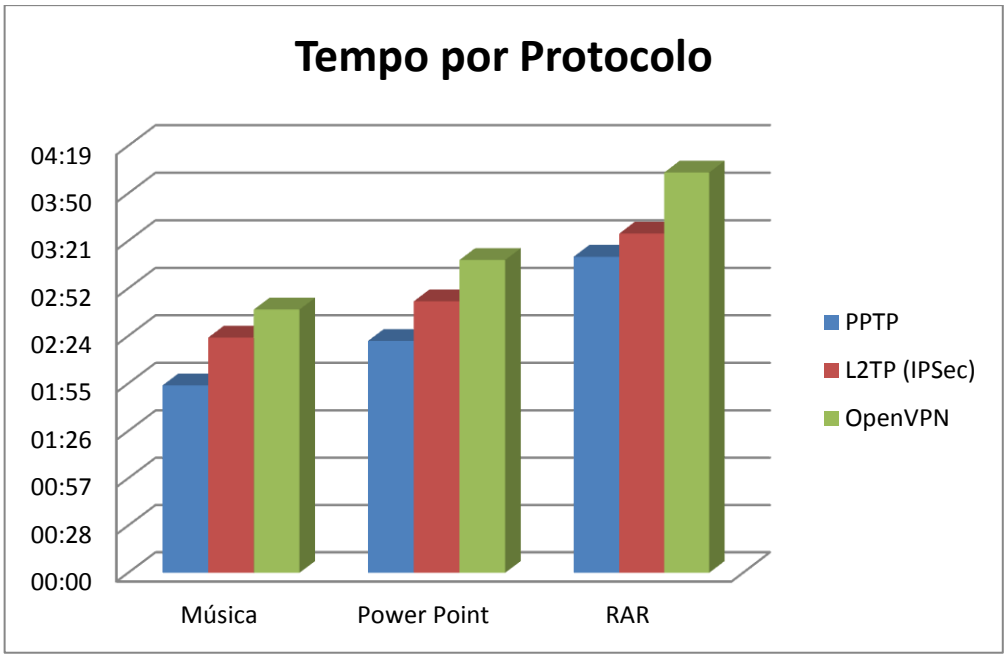

Figura 10. Gráfico de Tempo por Protocolo

CONCLUSÃO

Conclui-se que a implantação de servidores VPN em redes simples ou mais específicas é de grande eficácia, pois asseguram a transmissão dos dados sem que haja qualquer alteração de dados até a rede destino. Vimos que uma VPN depende também, muito do Upload do servidor, pois fechando o túnel a rede cliente fica totalmente dependente da rede do servidor, inclusive em questão de velocidade. Foi interessante implementar essas três topologias para entender como cada uma trabalha, e qual o impacto que elas causariam em seu uso.

Sobre os protocolos, todos eles apresentam segurança necessária para que se aplique a VPN, porém, o protocolo PPTP é inseguro apresentando somente um meio de autenticação básico que pode, por ventura, ser quebrado. Já os protocolos L2TP (IPSec) e OpenVPN foram mais eficazes com relação a segurança pois trabalham com uma criptografia mais avançada, onde fica mais difícil “roubar” esses dados durante a transmissão, sendo assim considerado topologias mais seguras.

No quesito velocidade, pode-se entender que quanto mais seguro for o protocolo VPN, menor será a sua velocidade de transmissão. Pois é necessário previamente criptografar os dados de acordo com a topologia, encaminhar o dado criptografado pela rede publica e também descriptografar no destino final para que se tenha um arquivo integro.

REFERÊNCIAS BIBLIOGRÁFICAS

OLIVEIRA, Carlos; ABBOUD, Ricardo. **Desafios da segurança cibernética nas subestações de energia elétrica**. Disponível em < http://www.osetoreletrico.com.br/web/a-revista/edicoes/1074-desafios-da-seguranca-cibernetica-nas-subestacoes-de-energia-eletrica.html/> Acessado em: 04/11/2014.

BARCELLOS, Marco. **Internet de Todas as Coisas: uma 'nova' internet para uma nova era**. Disponível em <http://canaltech.com.br/coluna/internet/Internet-de-Todas-as-Coisas-uma-nova-internet-para-uma-nova-era/> Acessado em: 04/11/2014.

SILVA, Thaís. **VPN e suas Utilidades**. Disponível em <http://blog.kaspersky.com.br/vpn-e-suas-utilidades/574/> Acessado em: 31/10/2014.

MARTINS, Elaine. **O que é TCP/IP?**. Disponível em <http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm> Acessado em: 31/10/2014.