Redes Privadas Virtuais: O Uso do Radmin VPN Como Solução VPN para Pequenas Empresas

Gustavo de Araújo Cardoso[1], João Antonio Aparecido Cardoso[1], Luciano Bernardes de Paula[1]

[1]Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP)
Bragança Paulista – SP – Brasil

gustavo.cardoso90@gmail.com, joaocardoso87@hotmail.com, lbernardes@ifsp.edu.br

Abstract. *With globalization, companies have felt the need to link their branches over the Internet, and a possible solution could be the use of Virtual Private Networks VPN, enabling connections without the need to use dedicated links or costly infrastructure. In this work, a study of the various aspects involved in the use of VPN networks and a case study concerning the implementation of the Radmin VPN solution in an accounting office were carried out, where it was possible to identify the basic concepts of Virtual Private Networks, to provide knowledge of its main characteristics, and advantages and disadvantages of its use.*

Resumo. Com a globalização, empresas sentiram a necessidade de interligar suas filiais através da Internet, e uma possível solução pode ser o uso de Redes Privadas Virtuais VPN, permitindo conexões sem a necessidade do uso de enlaces dedicados ou infraestruturas custosas. Neste trabalho, um estudo dos diversos aspectos envolvidos na utilização de redes VPN e um estudo de caso referente a implantação da solução VPN Radmin em um escritório de contabilidade foram realizados, onde foi possível a identificação dos conceitos básicos das Redes Privadas Virtuais, de modo a propiciar o conhecimento de suas principais características, e vantagens e desvantagens de seu uso.

1. Introdução

Antes da popularização da Internet, grandes empresas utilizavam enlaces de dados oferecidos por empresas operadoras de telecomunicações para comunicação entre matrizes e filiais. Esses enlaces funcionavam através de circuitos dedicados oferecidos de acordo com as necessidades de comunicação e da infraestrutura disponível (FERREIRA, 2013). A sociedade tem passado por notórias mudanças, onde novas oportunidades de negócios e novas soluções e serviços surgiram, gerando também novas demandas de serviços e novas formas de trabalho, como o trabalho remoto feito de casa (home office) ou teletrabalho (OLIVEIRA, 2013).

Com isso, muitas empresas sentiram a necessidade de interligar computadores de diferentes localidades em uma rede corporativa para a troca de dados. Porém uma conexão segura e privada envolvendo escritórios ou fábricas localizadas, por vezes, em outras cidades, estados ou até mesmo em outros países, pode ser difícil ou quase impossível (SILVA, 2003). A infraestrutura necessária para uma conexão direta entre empresas distantes pode ser um problema operacional significante para as organizações, devido ao custo elevado de um enlace dedicado de internet e possíveis dificuldades geográficas para tal conexão (ABRINT, 2017). Uma solução, para este tipo de

problema, é o uso da infraestrutura aberta e distribuída da Internet para transmissão de dados, de modo privado, entre localidades diversas de uma empresa. Essa técnica é chamada *Virtual Private Network* (VPN) ou Rede Privada Virtual, e seu principal objetivo é permitir que uma infraestrutura de rede pública, como por exemplo a Internet, seja utilizada como *backbone* para a comunicação segura entre pontos distintos (FIGUEIREDO E GEUS, 2001).

Segundo Chin (1998), "o uso de Redes Privadas Virtuais representa uma alternativa interessante na racionalização dos custos de redes corporativas oferecendo confidencialidade e integridade no transporte de informações através de redes públicas". Por meio de conexões VPN usando a Internet, empresas podem se conectar e compartilhar dados importantes entre si, encurtando distâncias e agilizando a troca de informações, com custos relativamente baixos, e tornando possível uma gestão ou modelo de negócios mais dinâmico (GONÇALVES e SILVA, 2008).

Com isso, este trabalho pode ser justificado devido a necessidade de assimilarmos as principais características e o funcionamento básico de uma Rede Privada Virtual, uma vez que são conhecimentos de serviços cruciais para quem trabalha ou pretende trabalhar com redes de computadores. Por meio de um estudo de caso, pretende-se evidenciar como a solução Radmin VPN pode atender a demanda de pequenas empresas, e as vantagens e desvantagens desse tipo de conexão.

2. Redes Privadas Virtuais

As Redes Privadas Virtuais ou do inglês *Virtual Private Networks (*VPN), consistem em redes criadas sobre a rede de comunicação já existente. Elas têm carácter privado devido toda a informação ser transmitida de forma segura quer usando encriptação ou por recurso a encapsulamento do tráfego por outro protocolo, criando desta forma um túnel entre os dois extremos da comunicação (BRAGA, 2012). Através de uma conexão VPN, duas redes separadas fisicamente podem se comunicar como se fossem uma única rede (REZENDE, 2004). A Figura 1 apresenta um cenário de VPN, onde os dados transmitidos no link entre a matriz e as filiais são confidenciais.

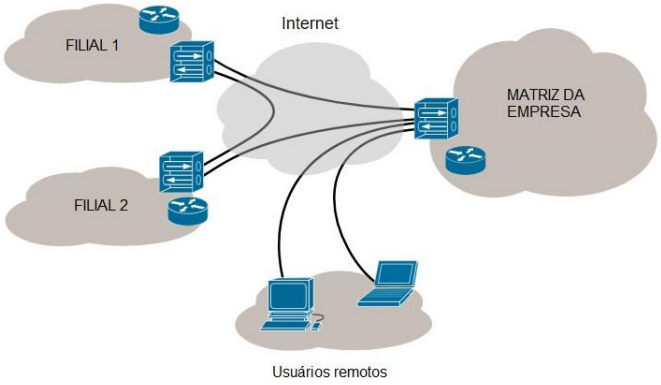

Figura1. Rede Privada Virtual - VPN. Wikipédia (2018)

Segundo Rezende (2004, p. 11), "para a realização dessa comunicação através de uma rede pública como a Internet, as VPN*s* se fundamentam em dois conceitos básicos, a criptografia e o tunelamento". De acordo com Miranda (2002), "existem vários tipos de implementação de VPN*s* e cada uma tem suas especificações próprias, assim como características que devem ter uma atenção especial na hora de

implementar". Dentre os vários tipos de VPN, destacam-se três principais aplicações ditas mais importantes, que são: intranet VPN, extranet VPN e acesso remoto VPN (CHIN; MIRANDA, 1998, 2002).

2.1 Acesso Remoto VPN

Acesso remoto é realizado por usuários móveis que se utilizam de um computador para conexão com a rede corporativa, partindo de suas residências, ou a partir de qualquer lugar através de redes *wireless* (ROSSI e FRANZIN, 2000). Uma VPN de acesso remoto pode ser usada para conectar empresas e colaboradores que estejam distantes fisicamente, e neste caso, torna-se necessário um *software* cliente de acesso remoto (SILVA, 2016). É importante uma autenticação rápida e eficiente que garanta a identidade do usuário remoto, e um gerenciamento centralizado desta rede, pois pode-se ter diversos usuários remotos conectados ao mesmo tempo, sendo necessário que todas as informações sobre os usuários, para efeitos de autenticação, estejam centralizadas num único lugar (MIRANDA, 2002).

Conforme pode ser analisado na Figura 2, o acesso remoto VPN possui uma grande aplicabilidade em ambientes cooperativos, onde os usuários remotos podem deixar de realizar ligações interurbanas, acessando os recursos da organização utilizando um túnel virtual criado através da Internet (REZENDE, 2004).

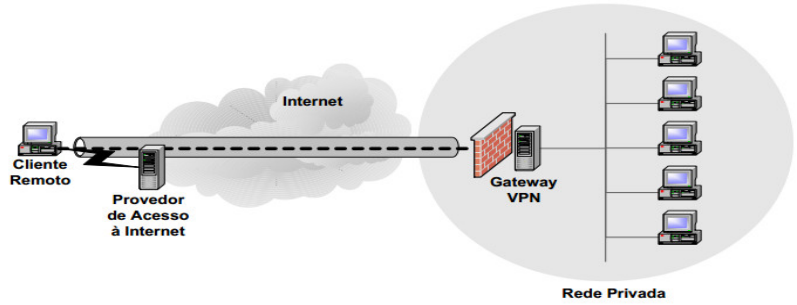

Figura 2. Acesso remoto VPN. Rezende (2004, p. 8).

Neste tipo de acesso, a segurança é muito importante, sendo necessário o uso de fortes sistemas de autenticação, uma vez que os recursos da organização são acessados diretamente pelos usuários remotos, o que torna difícil a implantação de medidas de segurança física (REZENDE e GEUS, 2002).

2.2 Vantagens e desvantagens do uso de VPNs

As redes virtuais privadas apresentam algumas vantagens e desvantagens em suas aplicações. Destaca-se como vantagens do uso de VPNs o baixo custo, pois as VPNs utilizam a Internet como conexão entre os diversos *gateways* e *hosts*, podendo diminuir o custo de implementação; sua escalabilidade e flexibilidade, pois as VPNs utilizam a rede pública para a comunicação entre matriz, filiais e parceiros comerciais, o que pode significar também maior flexibilidade com relação a usuários móveis e mudanças nas conexões; e a privacidade, pois simula uma conexão local, e a VPN pode ser utilizada como ferramenta para esconder a localização geográfica do cliente (PAULA, 2015).

Algumas desvantagens do uso de VPNs são em relação a velocidade da rede, pois quando o cliente VPN conecta-se com o servidor VPN, ele passa a atuar como se estivesse dentro de uma rede local (LAN), sendo necessária uma conexão de alta velocidade para garantir a interoperabilidade dos serviços requisitados através dessa

rede; quando ocorrem falhas e pacotes não são enviados, o *software* pode identificar essa situação como um ataque *hacker* e o túnel VPN é desfeito e refeito logo em seguida, porém com o mesmo problema acontecendo em *loop,* isso impossibilitará uma conexão estável; o cliente VPN pode ser uma porta de ataque das empresas, onde *hackers* podem atacar a máquina do cliente através do endereço IP original e então conectar-se diretamente ao servidor VPN, tendo acesso a dados sigilosos. Uma maneira de evitar esse tipo de ataque, seria configurando o cliente para aceitar somente conexões *IPSec*, o que impossibilitaria o *hacker* de realizar o primeiro ataque (PAULA, 2015).

3. Método e Objeto do Estudo

O método adotado para realização desse trabalho foi em um primeiro momento uma pesquisa bibliográfica com propósito de fundamentar a contextualizar o tema. Uma pesquisa exploratória foi realizada, pois tem por objetivo proporcionar maior familiaridade com o problema estudado (GIL, 2008). Com o intuito de compreender como funciona uma VPN e para atingir os objetivos definidos para esta pesquisa, foram consultadas diversas obras, como livros, artigos científicos, informativos especializados, dissertações, teses, e resultados de outras pesquisas sobre o tema escolhido.

Segundo Gil (2007), "um estudo de caso consiste no estudo profundo e exaustivo de um ou poucos objetos, de maneira que permita seu amplo e detalhado conhecimento". Por meio de um estudo de caso, esse trabalho buscou verificar e analisar se a implementação de ferramentas VPN pode contribuir para o sucesso das empresas. Este estudo de caso ocorreu em um escritório de contabilidade que atua há mais de 10 anos no mercado e está situado na cidade de Monte Verde - MG e que tem por finalidade atender a demanda fiscal e jurídica das empresas da região.

Com a crescente demanda de atendimento e a necessidade da obtenção de informações de forma dinâmica, os proprietários do escritório necessitavam de uma solução de acesso remoto que possibilitasse o acesso aos relatórios e aos documentos do escritório para seu uso durante reuniões e visitas a clientes, e para trabalho remoto.

Para atender essa necessidade, um *software* VPN foi implantado, possibilitando o acesso remoto ao servidor principal. Assim, o objeto de estudo desta pesquisa, foi a utilização de uma solução *freemium*[1] de VPN, chamada Radmin VPN, na rede local desse escritório, a fim de verificar se essa solução pode contribuir para a redução de custos de acesso remoto e atender a demanda de micro e pequenas empresas.

3.1 Local do Estudo de Caso

O escritório conta com 8 colaboradores e cada colaborador possui um computador *desktop* para uso pessoal. A empresa possui um servidor central de modelo Dell PowerEdge T130, no qual ficam as principais aplicações utilizadas. Os usuários usam os computadores no seu dia-a-dia para acesso a essas aplicações, que rodam localmente nesses computadores. Utilizando somente os bancos de dados das aplicações e pastas remotas que ficam no servidor central, onde arquivos como planilhas e documentos diversos são salvos em compartilhamentos de rede.

Os proprietários deste escritório de contabilidade solicitaram a configuração de uma solução VPN para o acesso remoto a este servidor central, com o propósito de

[1] É oferecido gratuitamente, mas usuários podem pagar para obterem recursos adicionais ou funcionalidades extras.

emitir relatórios, acessar as planilhas, consultar documentos, acessar serviços do servidor de *e-mail*, e para manutenção do servidor remotamente.

3.2 Problema

Algumas ferramentas de VPN foram testadas com o propósito de se verificar qual atendia melhor as necessidades da empresa. Soluções gratuitas como Open VPN, DynVPN, Hamachi, e Radmin VPN foram testadas, porém algumas dessas ferramentas possuem uma interface não tão simples e intuitiva, podendo ser mais complicadas e de difícil configuração. Além disso, alguns destes *softwares* apresentaram problemas como: intermitência na conexão, baixa velocidade, erros de compatibilidade de *drivers* com os sistemas operacionais do servidor ou da máquina cliente, entre outros problemas que foram encontrados durante os testes. Após diversos testes com diferentes soluções VPN, o técnico de informática do escritório utilizou a ferramenta Radmin VPN.

3.3 Radmin VPN

A solução Radmin VPN permite de modo simples a configuração de uma conexão segura entre computadores por meio da Internet, como se estivessem conectados por LAN. A parametrização da aplicação é feita de forma bastante simples, pois requer apenas a definição de um nome para a conexão e uma senha para a mesma. A ferramenta é um dos *softwares* de acesso remoto mais seguros e confiáveis atualmente, tanto governos quanto militares, especialistas em tecnologia e organizações financeiras confiam em seus recursos (RADMIN, 2018). Possui segurança com criptografia e suporte a redes de até 100Mbps, além de ser fácil de usar, pois conta com uma interface de configuração simples, tornando a tarefa de gestão da conexão VPN fácil tanto para profissionais de TI como para usuários amadores, conforme Figura 3.

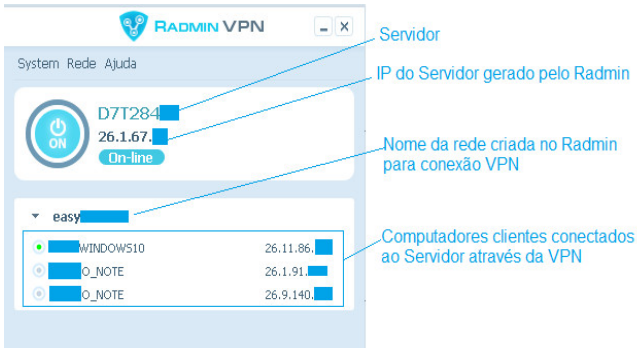

Figura 3. Interface do sistema Radmin VPN. Radmin VPN (2018).

Essa ferramenta foi instalada no servidor central, que conta com o sistema operacional Windows Server 2008 R2 64 bits, em um *notebook* que possui sistema operacional Windows 7 64 bits de uso dos colaboradores do escritório durante visitas aos clientes, deslocamentos, reuniões, ou em eventos em que a empresa necessita demonstrar seus serviços. Foi instalada também em mais dois computadores de uso pessoal dos administradores da empresa e do técnico de informática que presta serviços de suporte para o escritório, ambos com o sistema operacional Windows 10 64 bits.

A ferramenta Radmin VPN possui uma versão gratuita para até cinco computadores, o que pode atender a demanda de pequenas empresas como escritórios de contabilidade ou para usuários domésticos, pois é um *software freemium* e sua única restrição é o número de computadores utilizados ao mesmo tempo.

3.4 Segurança

A Segurança da Informação é sempre muito discutida, com o avanço da tecnologia e o desenvolvimento de novos dispositivos, maneiras de ataques e como se prevenir deles surgiram e surgem a todo instante. Segundo pesquisa realizada pela Kaspersky em 2013, 91% das empresas tiveram pelo menos um incidente de ameaça de segurança externa (KASPERSKY LAB, 2013).

Tendo em vista que o conceito de VPN é utilizar uma infraestrutura pública, o Radmin VPN utiliza a criptografia AES (*Advanced Encryption Standard)* de 256 bits, que é o padrão de criptografia adotado pelo governo norte-americano (NIST, 2001), e ficou famoso no Brasil na década passada por ser a "criptografia que nem o FBI conseguiu quebrar" no caso do banqueiro Daniel Dantas. Segundo a Famatech, desenvolvedora da ferramenta estudada, os recursos de segurança já vêm de fábrica, contando com criptografia AES256, e nunca foram encontradas vulnerabilidades nos 17 anos desde que o Radmin foi desenvolvido (RADMIN, 2018).

4. Resultados e Conclusões

Neste trabalho, por meio de uma revisão literária de diversas obras relacionadas às Redes Privadas Virtuais e de um estudo de caso, procurou-se evidenciar as principais características, funções, limitações, e vantagens e desvantagens do uso de VPNs em ambientes corporativos. Os objetivos gerais e específicos desta pesquisa foram atingidos, pois por meio dela, pode-se compreender o funcionamento básico desse tipo de conexão, e com o estudo de caso, foi possível constatar que as soluções de VPN podem contribuir nos negócios e reduzir custos. Para a utilização de uma VPN, é fundamental a escolha de soluções clientes e servidores que sejam compatíveis para se estabelecer uma conexão segura e confiável, e que os dispositivos usados no gerenciamento dessas conexões, possam garantir a segurança dos dados trafegados, assegurando a privacidade, integridade e autenticidade dos dados das organizações.

Neste estudo de caso, foram usadas soluções *free* de maneira a reduzir o custo da empresa, e ao mesmo tempo, fornecer uma solução prática, segura, e fácil de usar. Foram testados no mesmo ambiente outros *softwares* de VPN, tais como Hamachi, DynVPN, e Open VPN.

O Hamachi se mostrou também eficiente no quesito estabilidade e conexão, porém apresentou-se incompatibilidade de *drivers* com o sistema operacional Windows Server 2008 R2 64 bits, o que afastou essa opção. O DynVPN possibilita fácil configuração e compatibilidade de *drivers*, porém a conexão estabelecida se mostrou intermitente e lenta, apresentando instabilidade, com *pings* muito altos, causando lentidão demasiada no compartilhamento dos arquivos. O Open VPN, por sua vez, apresenta uma configuração mais técnica, demandando um conhecimento mais avançado sobre VPNs. O curto tempo de pesquisa disponível para que o técnico de informática do escritório pudesse aprender a configurar a ferramenta de forma adequada e segura, e a necessidade de uma rápida solução de acesso remoto, acabaram sendo fatores determinantes para a sua não escolha.

Então, a ferramenta Radmin VPN, que uniu a compatibilidade de *drivers* com diversos sistemas operacionais, a facilidade de configuração devido sua interface simples e intuitiva, segurança através de conexões criptografadas, velocidade e estabilidade de conexão, atendeu a demanda do escritório de forma satisfatória. A

parametrização do sistema requer apenas um nome e uma senha de acesso a serem definidos no servidor e nos computadores clientes para que a rede VPN se estabeleça.

Assim, o Radmin VPN pode contribuir para a redução de custos, para uma gestão de forma dinâmica, e no atendimento aos clientes das empresas. Para um melhor entendimento, no Quadro 1, são disponibilizados os requisitos de cada ferramenta conforme modelo para classificação de atributos de qualidade de software FURPS.

Software	Funcionalidade	Usabilidade	Confiabilidade	Desempenho	Suportabilidade
Radmin VPN	✓	✓	✓	✓	✓
Hamachi	✓	✓	✗	✓	✗
Dyn VPN	✓	✓	✗	✗	✓
Open VPN	✓	✗	✓	✓	✓

Quadro1. Classificação FURPS das ferramentas. Os autores (2018).

Devido à complexidade e amplitude do tema abordado, esse trabalho apenas tocou na superfície de seus conceitos para seu entendimento básico. Como sugestão para futuros trabalhos, é recomendável um estudo de caso fazendo um comparativo referente a implantação de outras soluções VPN em ambientes corporativos. Pode-se também, realizar levantamentos com relação ao percentual de recursos que as empresas podem economizar utilizando VPNs, estudos referentes a contribuição da VPN para o teletrabalho, comparativos referentes aos diversos tipos de soluções disponíveis no mercado, e estudos sobre as soluções VPN para dispositivos móveis.

5. Referências

ABRINT. **A Franquia na Banda Larga Fixa**: uma necessidade técnica. Disponível em: <http://telaviva.com.br/wp-content/uploads/2017/10/Franquia_estudo_tecnico_abrint.pdf >. Acesso em: 26 mai. 2018.

BRAGA, V. **Soluções *Open-source* para os Serviços de Fax e VPN numa Rede Empresarial**. 2012. 113f. Dissertação (Mestrado Engenharia Eletrotécnica e de Computadores). Faculdade de Engenharia da Universidade do Porto, FEUP - Departamento de Engenharia Informática, Porto, 2012.

CHIN, L. K. Rede Privada Virtual – VPN. Boletim bimestral sobre tecnologia de redes. **Rede Nacional de Ensino e Pesquisa (RNP),** v. 2, n. 8, nov. 1998.

FERREIRA, J. L. **Estudo de caso de soluções em VPN IPsec com servidores usando Software Livre**. 2013. 77f. Trabalho de Conclusão de Curso (Especialização em Teleinformática e Redes de Computadores). Universidade Tecnológica Federal do Paraná, Curitiba, 2013.

FIGUEIREDO, F.; GEUS, P. Acesso remoto em firewalls e topologia para gateways VPN. *In:* **Workshop em Segurança de Sistemas Computacionais**. p. 49-54, 2001.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

GIL, R. L. **Tipos de Pesquisa.** Universidade Federal de Pelotas. Pelotas, RS. 2009. Disponível em: <http://wp.ufpel.edu.br/ecb/files/2009/09/Tipos-de-Pesquisa.pdf>. Acesso em: 7 jun. 2018.

GONÇALVES, A. C.; SILVA, W. B. VPN**:** Uma Solução Segura e de baixo custo para Integração da Universidade Estadual de Goiás. **Webartigos**. 2008. Disponível em: <https://www.webartigos.com/artigos/vpn-uma-solucao-segura-e-de-baixo-custo-para-integracao-da-universidade-estadual-de-goias/12435>. Acesso em: 4 jun. 2018.

KASPERSKY LAB. *Global Corporate IT Security Risks*. Kaspersky Lab. p. 26. 2013.

LARMAN, C. **Utilizando UML e Padrões:** uma introdução à análise e ao projeto orientados a objetos e ao desenvolvimento iterativo. 3. ed. São Paulo: Artmed, 2007.

MIRANDA, I. C. **VPN - Virtual Private Network:** Rede Privada Virtual. Universidade Federal do Rio de Janeiro - UFRJ, Departamento de Engenharia Eletrônica e de Computação - DEL, Rio de Janeiro. 2002.

NAKAMURA, E. T. **Análise de Segurança do Acesso Remoto VPN**. Universidade Estadual de Campinas, Instituto de Computação. Campinas, SP: Unicamp. 2000.

NIST. ***Federal Information Processing Standard***, *publication* 197 (FIPS 197): *Announcing the advanced encryption standard* (AES). Washington D.C. 2001.

OLIVEIRA, J. F. N. As novas tecnologias da informação e da comunicação nas relações do trabalho: o teletrabalho. *In:* Congresso Internacional de Direito e Contemporaneidade, 2013, Santa Maria. **Anais**... Santa Maria: UFSM, 2013.

PAULA, D. **Vantagens e Desvantagens do uso de VPNs**. Seminário de Redes de Computadores, Universidade Federal do Rio de Janeiro - UFRJ, Departamento de Eletrônica da UFRJ, Rio de Janeiro. 2015.

RADMIN. *Radmin Software*. Disponível em: <http://www.radmin.com.br/>. Acesso em: 13 jun. 2018

REZENDE, E. R. S. **Segurança no acesso remoto VPN**. 2004. 127 f. Dissertação (Mestrado em mestrado em ciência da computação). Instituto de Computação – Unicamp, Campinas, SP, 2004.

REZENDE, E. R.; GEUS, P. Análise de segurança dos protocolos utilizados para acesso remoto VPN em plataformas Windows. **Anais...** IV Simpósio sobre Segurança em Informática, Universidade Estadual de Campinas, Instituto de Computação, 2002.

REZENDE, E.; GEUS, P. Uma solução segura e escalável para acesso remoto VPN. **SCIENTIA** – **Revista de Computação da Unisinos**, 15. jan./jun. de 2004.

ROSSI, M.; FRANZIN, O. **VPN -** ***Virtual Private Network*** **(Rede Privada Virtual)**. GPr Sistemas/ASP *Systems*. ago. 2000.

SILVA, C. Descubra por que usar uma VPN e veja como escolher a melhor. **Canaltech.** 2016. Disponível em: <https://canaltech.com.br/internet/descubra-por-que-usar-uma-vpn-e-veja-como-escolher-a-melhor/>. Acesso em: 24 mai. 2018.

SILVA, L. S. ***Virtual Private Network*** **- VPN**: Aprenda a construir Redes Privadas Virtuais em plataformas Linux e Windows. São Paulo (SP): Novatec, 2003.

VIRTUAL PRIVATE NETWORK. *In*: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=52175687>. Acesso em: 24 mai. 2018.