UNIVERSIDADE PARAÍSO - UNIFAP

UNIDADE ACADÊMICA DE GRADUAÇÃO

CURSO DE SISTEMAS DE INFORMAÇÃO

ERINALDO FEITOSA DE SOUZA[1]; KLEBER SILVA[2]

IMPLEMENTAÇÃO DE SEGURANÇA EM UMA REDE ATRAVÉS DO USO DA REDE VIRTUAL PRIVADA (VPN)

Juazeiro do Norte-CE

2020

ERINALDO FEITOSA DE SOUZA[1]; KLEBER SILVA[2]

IMPLEMENTAÇÃO DE SEGURANÇA EM UMA REDE ATRAVÉS DO USO DA REDE VIRTUAL PRIVADA (VPN)

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação, pelo Curso de Sistemas de Informação da Universidade Paraíso – UNIFAP

Orientador: Prof. Me. Fabrício Carneiro da Costa

Juazeiro do norte - CE

2020

IMPLEMENTAÇÃO DE SEGURANÇA EM UMA REDE ATRAVÉS DO USO DA REDE VIRTUAL PRIVADA (VPN)

Erinaldo Feitosa de Souza[1], Kleber Silva[2],

Orientador; Fabrício Carneiro.

Resumo: O presente artigo pretende mostrar de uma forma funcional sobre que é uma Virtual Private Network (VPN), começando com um histórico sobre VPNs, a importância de sua utilização em uma empresa e em residências, como funciona, uma breve descrição dos protocolos que são utilizados, autenticação e integridade, serão apresentados também dois tipos de criptografia que uma VPN pode utilizar (vale lembrar que os tipos de criptografia apresentados são apenas alguns dos tipos de criptografia utilizados), aplicações VPN e os benefícios gerados a uma empresa.

Palavras-chave: VPN. Segurança da Informação. Criptografia.

Resumen: Este artículo pretende mostrar de manera funcional qué es una Red Privada Virtual (VPN), comenzando con una historia sobre las VPNs, la importancia de su uso en una empresa y en los hogares, cómo funciona, una breve descripción de los protocolos que se utilizan. , autenticación e integridad, también se presentarán dos tipos de encriptación que puede utilizar una VPN (recuerde que los tipos de encriptación presentados son solo algunos de los tipos de encriptación utilizados), las aplicaciones VPN y los beneficios que genera a una empresa.

Palabras clave: VPN. seguridad de la información. criptografía.

1. INTRODUÇÃO

A VPN trata-se de uma rede privada construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois ou mais computadores através da rede. Utiliza-se a infraestrutura da internet para conectar redes distantes e remotas. As redes VPN são muito utilizadas pelas grandes empresas, especialmente nas companhias em que funcionários trabalham remotamente. Segundo o Site (HMA. 2020. Disponível em: <https://www.hidemyass.com/pt-br/what-is-vpn>).

> VPN significa Virtual Private Network (rede virtual privada). Ela permite navegar na internet de maneira anônima e segura, de qualquer lugar. As VPNs protegem você através da criação de um túnel criptografado que conecta seu computador à internet, hotspots Wi-Fi e outras redes.

Com o avanço na área da tecnologia da informação, com a atual demanda no mercado de trabalho e com a necessidade das empresas se comunicarem e ter informações de forma cada vez mais rápida e confiável continua tornando a VPN uma idéia cada vez mais viável para empresas que dependem dessa comunicação. O universo de TI vem evoluindo cada vez mais ao passar dos anos, observa-se gigantes mudanças quando fazem comparações entre os antigos computadores e mainframes e as tecnologias contemporâneas. Tecnologia essa que vem crescendo e abastecendo o mercado consumidor.

Com o grande crescimento da Internet, e o constante aumento de sua área de abrangência, e a expectativa de melhorias na qualidade dos meios de comunicação associado a um grande aumento na velocidade de acesso, a internet passou a ser vista como um meio conveniente para as comunicações corporativas.

Conexões através de VPN têm um valor consideravelmente mais baixo que links dedicados principalmente quando se trata de longas distâncias. Com toda essa infraestrutura de conexão entre hosts da rede privada é uma ótima solução em termos de custos, e o ponto da segurança e privacidade é adicionado através de criptografia, ou seja, mesmo que as informações que passam por um sistema de

túnel VPN sejam capturadas não possam ser decifradas. Como já foi dito as tarifas de longa distância são os maiores custos deste tipo de conectividade. entre tanto outros custos incluem investimentos

Segundo o site (ALERTA SECURITY, Disponível em: <https://www.alertasecurity.com.br/por-dentro-da-cybercriminal-inc-sonicwall-expoe-novos-dados-de-ciberataques-e-comportamentos-de-agentes-de-ameacas-em-relatorio-mais-recente>).

> Para os cibe criminosos e agentes de ameaças, a linha de frente digital é um panorama sem lei de alvos e oportunidades. Apesar das melhores intenções de órgãos governamentais e de aplicação da lei e grupos de fiscalização, o panorama de ameaças cibernéticas moderno está mais ágil e evasivo do que nunca.

em Servidores de Acesso Remoto na matriz e pessoal especializado para configurar e manter os servidores.

Estes túneis habilitam o tráfego dos dados criptografados através da Internet e esses dispositivos, são capazes de entender os dados criptografados formando uma rede virtual segura sobre a rede Internet. Que tentam sempre atender esses 3 requisitos.

Privacidade dos dados: Mesmo se ocorrer uma interceptação de dados no meio do túnel não podem ser decodificados

Integridade dos dados: As informações são inalteráveis, ou seja, não podem sofrer mudança durante a transmissão.

Autenticidade: garantir que o dispositivo remoto o qual o túnel foi estabelecido é um dispositivo autorizado e não um equipamento qualquer.

A utilização da VPN tem o principal intuito a comunicação de dois computadores de maneira em que as informações trocadas por eles sejam protegidas, por meio da encriptação de dados.O uso de uma VPN ligada diretamente a uma rede doméstica pode ser exemplificada na navegação anônima que permite

acesso a conteúdo que não está disponível no seu país ou seja mesmo que a pessoa esteja no Brasil a máquina pode entender que ela está no Canadá através do seu IP.

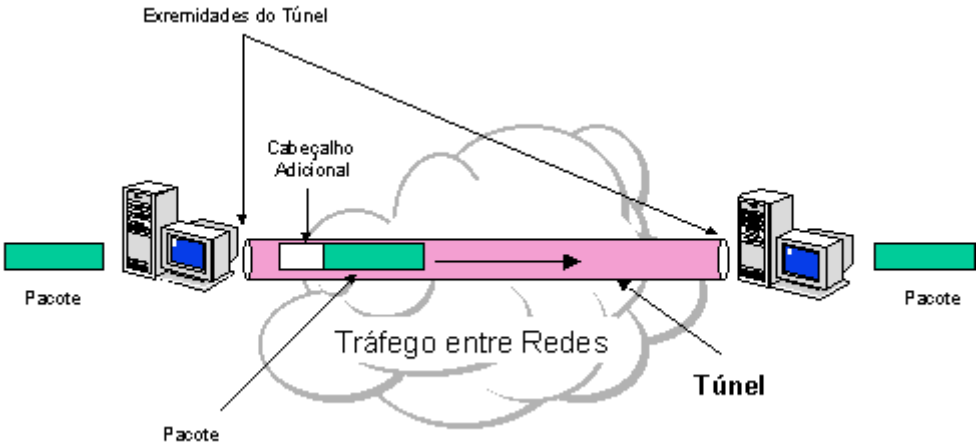

Figura 1 conexão VPN entre dois computadores

Figura disponível em https://memoria.rnp.br/newsgen/9811/vpn.html

2. OBJETIVO GERAL

O intuito do artigo é mostrar a necessidade da integração de uma VPN na transferência de dados sigilosos principalmente em sites de órgão públicos brasileiros, que raramente se faz conexões criptografadas, tornando os dados da sociedade a mercê de integridade e confidencialidade, mas também aos usuários de redes de internet em bares, cafés etc., que desejam realizar troca de informações (remetente-receptor) sem que terceiros saibam do que se trata. E assim implantar de forma pratica nos sistemas do governo, e de forma teórica e eficiente, por meio de comunicação em massa inclusive através de escolas, para que não apenas técnicos em TI, mas também a população (quanto mais souberem utilizá-la mais barata vai ser sua adesão e monitoramento) principalmente às crianças, aprendam e ensine que sobre a tecnologia deve-se ter cautela no que se acessa, sendo que as mesmas possuem mais facilidade no aprendizado.

Figura 2 Site da Sefaz sem certificado SSL

Figura disponível em https://www.sefaz.ce.gov.br

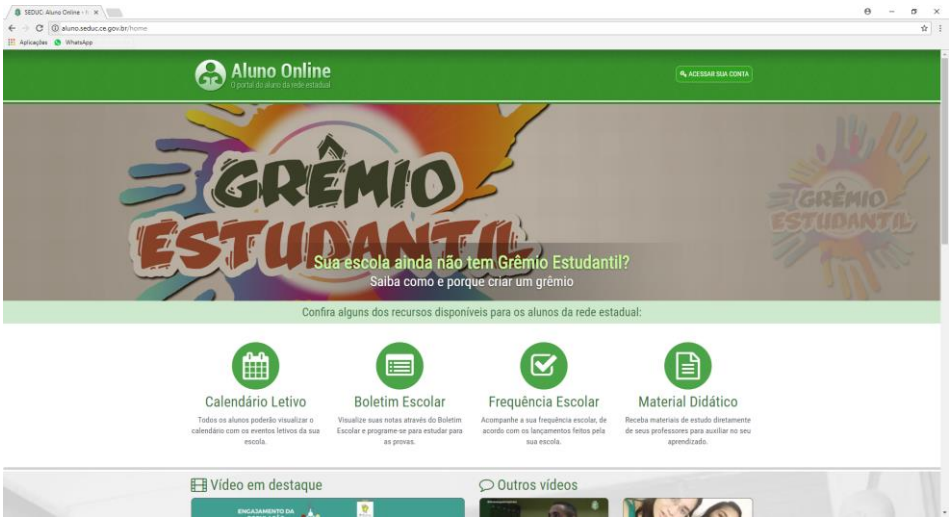

Figura 3 Site da Seduc/Aluno Online sem certificado SSL

Figura disponível em https://www.alunoonline.seduc.ce.gov.br

3. OBJETIVOS ESPECÍFICOS

- Conhecer como funciona uma rede virtual privada
- Tornar-se rotineiro o uso da VPN
- Analisar a necessidade dos locais de implementação
- Criar métodos de divulgação através de escolas e instituições de ensino técnico
- Adaptar sistemas a pessoas leigas para utilização da VPN como método de segurança

4. METODOLOGIA

A metodologia utilizada foi prioritariamente qualitativa, uma vez que se baseou na análise bibliográfica e documental na área de tecnologia, fornecendo dados tanto de livros e jornais como de sites e documentos na internet que normalmente são bem acessíveis. A escolha desse tipo de abordagem mostrou-se muito relevante para o estudo do tema já que ela fala de segurança na internet e justo lá onde deve ser encontrada. Abaixo está informado como ficará descrita a metodologia deste artigo representado pela

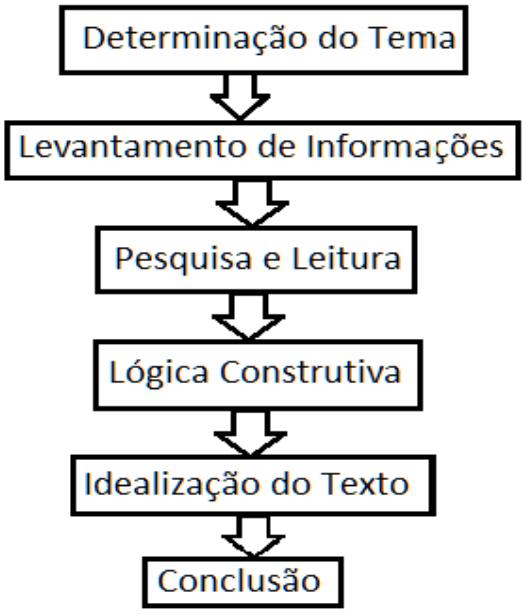

Figura 4

Metodologia deste artigo.

5. DESENVOLVIMENTO

Segundo a empresa de serviços de VPN (2020,“HideMyAss” disponível em: <https://www.hidemyass.com/>) considerada um serviço de VPN renomada pela Forbes e The Guardian “ a VPN é a ferramenta certa para todos que querem navegar na rede com segurança privacidade e nenhuma restrição.” De acordo com o ideal desta empresa, para preencher os requisitos de segurança deve-se ter em mente cinco pontos.

Usar uma VPN é como ter uma caixa postal na Internet: um endereço que permite que você não seja rastreado.

Em vez de fornecer seu endereço IP real, ao clicar em um website, seu computador fornece um dos nossos endereços.

Os dados de trafego são fornecidos ao servidor VPN e depois encaminhamos ao cliente, de forma instantânea e segura

O resultado? Parecerá que você está no local que nosso servidor estiver localizado, permitindo acessar a Internet como uma pessoa local, seja qual for sua localização.

E bisbilhoteiros e hackers online não poderão rastrear seu endereço real através de suas atividades, descobrindo quem você é e onde está.

Vantagens e desvantagem sobre o uso da VPN é um fato muito retrucado por quem já tem algum conhecimento sobre VPN já que a taxa de desvantagem fica quase que mínima em relação ao que ela traz de benefício, devido isso foi realizada uma pesquisa no fórum da Tecno Masters cujo reuniu fatos e os relacionou como vantagens e desvantagens da VPN:

Vantagens: “Segurança” – Acontece à criptografia e o anonimato na rede adicionando uma camada de segurança a mais em sua rede dificultando o monitoramento não autorizado pelo usuário em uma rede.

“Permite acessar conteúdo exclusivo por país” – Alguns serviços pela internet são permitidos apenas em seus países, devido este fato o uso da VPN possibilita o

acesso do mesmo, pois ao utilizar um Servidor VPN que está localizada noutro país os dados captados são do Servidor e não do Cliente.

“Libera acesso a sites/programas bloqueados na rede” – No caso de algumas empresas ou até mesmo em um país que sofre com censura é comum ser barrados vários conteúdos presentes na rede e através do uso da VPN é possível quebrar esse bloqueio.

Desvantagens: “Latência” – Com o uso da VPN geralmente seu tráfego vai ficar mais demorado digamos assim, pois como geralmente os Servidores VPN são requisitados para ficar em outro continente, devido a localização há um pequeno atraso na informação já que ela tem que trafegar o continente 2 vezes(Na requisição e na resposta).

“Crimes com uso de VPN” – É fato que a VPN traz segurança, porém essa segurança pode vir acometida de crimes já que dificulta a interceptação da mensagem ou de sua localização. Caso seja requisitado o serviço uma empresa de VPN ela guardará todas suas informações do que foi navegado e quando foi navegado para ter um controle para o caso de ocorrer um crime e o mesmo for denunciado, porém se o criminoso utilizar de meios próprios de VPN já traz alcança um patamar a mais dificuldade a mais para sua localização.

De acordo com os pontos descritos acima, fica decidido que para o estudo deste artigo é necessário utilizar os tipos de VPN que atendem a demanda, tais como Ponto a Ponto Empresarial quanto Ponto a Ponto para utilização de servidores de games, VPN para quem trabalha remotamente, ou VPN para as pessoas que querem navegar na rede de forma sigilosa e oculta

6. RESULTADOS

Ao final desta pesquisa de caso de estudos, e após o levantamento de dados bibliográficos analisados ficou bem claro que o uso de VPN é bem complexo, pois o que torna vantagens e necessidades para alguns setores, para outros se torna uma mera desvantagem, um exemplo poderíamos citar as empresas que necessitam de segurança na sua rede de intranet e internet, mais se deparam com o problema de

latência de trafego causando lentidão e vários processos da empresa. Já para os usuários domésticos e pequenas empresas o uso das VPN não trazem tantos transtornos, por não ser tão necessário e por não haver tanta necessidade de proteção dos dados, como também a falta de conhecimento sobre segurança de dados.

7. CONSIDERAÇÕES FINAIS

Neste trabalho cientifico foi mostrado como um dos principais problemas da informática, a segurança durante a troca de informações em rede, isto por ser um dos princípios dessa tecnologia, ao analisar os variados tipos de ataques é perceptível que grande parte dos internautas caem nessa armadilha muitas vezes sem perceber, porem para os realizadores e leitores desse artigo diminui-se as chances desse imprevisto.

Com o presente artigo tem como resultado a amostra de conhecimento dos realizadores em contribuir para a sociedade acadêmica na área, e internautas, ainda conta com o princípio de estudo, análise e solução de uma VPN como possível solução de meio mais seguro para a transição de dados. Com observações próprias, observar que usuários da rede mundial de computadores são vítimas de forma oculta, e detalhar neste trabalho como ocorre e oque deve-se fazer para solução do problema.

Com o objetivo detalhado na metodologia, mostra-se que o resultado esperado tem como previsões em primeira mão com divulgação em empresas, questão de meses após a divulgação, na segunda idéia sendo o ensino de crianças e adolescentes ao uso correto de tecnologia e uso da VPN espera-se resultados em dez anos, de imediato espera-se bons resultados, mas ao longo prazo é quase que inegável a excelência de resultados.

Como pesquisas futuras, iremos usar o Pentest para procurar por falhas numa VPN bem monitorada, usar recursos de dispositivos fixos e moveis para ter acesso à

localização do verdadeiro IP mesmo que esteja usando uma VPN, para evitar o sigilo de invasores.

Para a comunidade acadêmica este artigo disponibiliza outro meio de tornar a transmissão de dados mais segura que o conveniente, com os futuros trabalhos detalhados abrir portas de conhecimento de acadêmicos e outros para os diversos meios de pesquisas e modos de utilização de VPN, assim contribuindo de diversas formas para ouvintes e sociedade.

REFERÊNCIAS

JAMILSON BINE. **Estudo de segurança em dispositivos moveis.** Disponível em: <https://semanaacademica.org.br/system/files/artigos/jamilson_bine-estudo_de_seguranca_em_dispositivos_moveis.pdf> Acessado em 15 ago. 2020.

ALERTA SECURITY. **Os pilares da segurança da informação.** Disponível em: <https://www.alertasecurity.com.br/blog/31-base-capitulo-1-os-pilares-da-seguranca-da-informacao> Acessado em 15 ago. 2020.

Google Scholar. **Utilização da Virtual Privete Network (VPN).** Disponível em: <https://scholar.google.com.br/scholar?hl=ptBR&as_sdt=0%2C5&q=tcc+sobe+vpn&btnG=> Acessado em: 16 ago. 2020.

CISCO. **What is afire wall.** Disponívelem: <https://www.cisco.com/c/pt_br/products/security/firewalls/whatisafirewall.html> Acessado em 16 ago. 2020.

HMA. **Teste de VPN.** Disponível em: <https://www.hidemyass.com> Acessado em: 16 ago. 2020.

TECNOMASTER. **Vantagens e desvantagens de usar uma VPN.** Disponível em:<http://tecnomasters.com.br/computadoreseredes/vantagensedesvantagens-de-usar-uma-vpn/8748> Acessado em: 17 ago. 2020.

THE GUARDIAN. **VPN Internet Private Security.** Disponível em: <https://www.theguardian.com/technology/askjack/2012/may/17/vpn-internet-privacy-security> Acessado em 17 ago. 2020.

GABRIEL TORRES. **Livro de Hardware Curso Completo.** Volume - 4. 2001.

NEWS GEN. **conexão VPN entre dois computadores.** Disponível em: <https://memoria.rnp.br/newsgen/9811/vpn.html> Acessado em: 19 ago. 2020.

SEFAZ. **Site da Sefaz sem certificado SSL.** Disponível em:<https://www.sefaz.ce.gov.br> Acessado em: 20 ago. 2020.

SEDUC. **Site da Seduc/Aluno Online sem certificado SSL** Disponível em:<https://www.alunoonline.seduc.ce.gov.br> Acessado em 20 ago. 2020.