FACULDADE DE CIÊNCIAS DO TOCANTINS

2021
Outubro e Novembro
Ed. 31 Vol. 1. Págs. 314-332

JNT-FACIT BUSINESS AND TECHNOLOGY JOURNAL - ISSN: 2526-4281 QUALIS B1

A IMPORTANCIA DA VPN (VIRTUAL PRIVATE NETWORK) DURANTE A PANDEMIA COVID-19: UMA REVISÃO DE LITERATURA

THE IMPORTANCE OF VPN (VIRTUAL PRIVATE NETWORK) DURING THE COVID-19 PANDEMIC: A LITERATURE REVIEW

Matheus Carvalho LEAL
Centro Universitário Instituto Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: matheus.car.leal@gmail.com

Marcelo Renato do Carmo PEREIRA FILHO
Centro Universitário Instituto Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: mrenato18@hotmail.com

RESUMO

VPN é a sigla da palavra rede virtual privada, do Inglês Virtual Private Network. A VPN é definida como uma rede de dados privada a fim de criar pontes de ligação entre diversos dispositivos através de uma rede pública: a internet, protegendo e criptografando todas as informações trocadas, proporcionando segurança e garantindo a privacidade dos dados transportados, evitando que seus dados fiquem visíveis para pessoas não autorizadas. A principal motivação para se fazer o uso da VPN é a redução de custos e a garantia de uma comunicação segura. Atualmente a VPN tem sido uma grande aliada das empresas durante a pandemia da covid-19, pois permite que os colaboradores trabalhem de home office através de uma rede segura para troca de dados. Partindo disso as empresas com filiais ou escritórios podem ter uma interligação e se unificar em uma só rede facilitando as comunicações coorporativas.

Palavras-chave: VPN. Redes. Segurança de dados.

ABSTRACT

VPN is the acronym for the word virtual private network, from English Virtual Private Network. VPN is defined as a private data network in order to create bridges of connection between various devices through a public network: the internet, protecting and encrypting all information exchanged, providing security and ensuring the privacy of transported data, preventing your data from are visible to unauthorized persons. The main motivation for using VPN is to reduce costs and ensure secure communication. Currently, VPN has been a great ally of companies during the covid-19 pandemic, as it allows employees to work from their home office through a secure network for data exchange. Based on this, companies with branches or offices can have an interconnection and unify in a single network, facilitating corporate communications.

Keywords: VPN. Networks, Data security.

INTRODUÇÃO

A tecnologia e as redes de computadores nas últimas décadas vêm sendo essenciais nos ambientes coorporativos facilitando a realização de tarefas do cotidiano e dinamizando o serviço dos funcionários nas empresas. O ambiente coorporativo pode ser caracterizado pela conectividade entre as empresas, e com o avanço da tecnologia, foram criadas inúmeras formas de fazer conexão entre as maquinas, visto que atualmente a troca de dados através da internet cada vez se faz mais necessária às atividades humanas.

Quando houve o surgimento das redes de computadores, não existia uma preocupação tão grande em relação à segurança dos dados como hoje. Naquela época, era difícil imaginar que atualmente praticamente tudo funcionária com o auxílio de maquinas [Santini 2005]. Com o aumento significativo da rede mundial de computadores, a comunicação e tráfego de dados passa a ter um papel essencial para a dinamização das mais diversas relações, tanto pessoais quanto trabalhistas.

Poucas situações no mundo mexem com o direito de ir e vir das pessoas, obrigando-as a ficar em isolamento domiciliar ou social, esse caso aconteceu em março de 2020, colocando o principal estado do país em quarentena inicialmente por 30 dias. Tudo isso devido à doença infecciosa Covid-19, que surgiu em Wuhan, China (SARS-CoV2) no final de 2019, se espalhou rapidamente para todas as províncias chinesas e, em 1 de março de 2020, para 58 outros países (LI ET AL., 2020).

Para tentar evitar a propagação do coronavírus o governo teve que pôr em pratica as medidas sanitárias como a quarentena e isolamento social visto que até então não se tinha muitas informações sobre o covid-19. Com o decreto da pandemia mundial, as pessoas foram aconselhadas a ficar em suas residências, empresas e comércios foram fechados. Diante desta situação atípica, governo e empresas se viram obrigadas mudar a forma de trabalho de seus colaboradores para respeitar as medidas restritivas e evitar a propagação do vírus.

Mediante a atual situação, à medida que as empresas adotaram para continuar em funcionamento foi o home office, pois permite que as pessoas possam trabalhar a distância recebendo e transmitindo informações, acessar arquivos relacionados à atividade laboral com rapidez e segurança mesmo fora da empresa. O trabalho remoto proporciona uma

comodidade maior, porém uma das grandes preocupações era a respeito da segurança dos dados durante a comunicação entre a rede coorporativa e a rede doméstica.

Com o home office, as empresas necessitam de soluções tecnológicas e um ambiente seguro para fazer essa ponte entre empresa e filial/colaboradores, e para isso o uso de VPNs é o mais indicado, pois, oferece diversas vantagens como redução do tempo, diminuição dos custos fixos de escritório e segurança durante o tráfego dos dados entre as redes de computadores domésticas e coorporativas.

De acordo com Souza (2009, p.21) "uma rede de computadores é um conjunto de equipamentos interligados de maneira a trocarem informações e compartilharem recursos", como arquivos, impressoras e softwares. Uma rede de computadores oferece conectividade entre um conjunto de componentes, porém, o seu grande diferencial é a capacidade de transportar mais de um tipo de dado (PETERSON; DAVIE, 2003).

As redes privadas virtuais (VPN) são elementos significantes dentro de uma empresa, e seu principal objetivo é utilizar uma rede de dados pública como a Internet para facilitar a comunicação no ambiente coorporativo. A facilidade da troca de informações oferecidas pela VPN permite uma redução de custo com infraestrutura e equipamentos, possibilitando uma comunicação segura sobre uma rede pública em diversos equipamentos de uma forma mais rápida e dinâmica.

Segundo Queirz (1998). VPN (virtual private network) surgiu da necessidade de interligar redes ou sub-redes privados a partir de outra rede para suporte de canais de comunicação seguro e mais barato. É um tipo de rede que permite a comunicação a longa distância, com menos custo, comparando com links dedicados e garante a privacidade de informação transmitida até ao seu destino, através da criptografia, protocolo de túnel.

Tendo em vista que a VPN tem como principal função estabelecer uma conexão entre 2 ou mais pontos através de uma rede pública não confiável, esse trabalho tem como objetivo geral fornecer informações a respeito dos benefícios do uso da VPN em empresas mantendo a confidencialidade e a integridade dos dados transportados. Os objetivos específicos são:

- Revisar a literatura que engloba a rede VPN;
- Distinguir os tipos de protocolos utilizados para criação da VPN;
- Escrever sobre a segurança de dados, redução de custo e otimização da comunicação entre os servidores das empresas;

- Discutir sobre o uso de VPN durante o home office durante a pandemia covid-19.

MATERIAIS E MÉTODOS

A análise bibliográfica foi guiada na revisão de literatura através de artigos científicos nacionais e internacionais publicados entre os anos 1998 a 2021 nas diferentes bases de dados: Google Acadêmico e Scielo.

Os critérios utilizados para inclusão dos artigos da revisão foram os que apresentaram ideias consistentes sobre a utilização dos protocolos da VPN, Bem como o compartilhamento de dados de forma segura, otimizada e de baixo custo para as empresas.

REFERENCIAL TEÓRICO

O acesso remoto VPN tem como intuito resolver problemas de conexão dos usuários que ainda não possuem um acesso direto com a internet, e isso é possível através da utilização de provedores de acesso. Outra grande vantagem do uso da VPN tanto para a empresa quanto para os usuários é a facilidade de acesso dos funcionários que trabalham em home office ou que fazem viagens e precisam de um ponto de conexão diferente a cada momento. A interligação de rede das empresas com seus clientes permite o acesso direto ao banco de dados, através de uma conexão segura e sigilosa entre os parceiros que fazem uso da mesma rede, atendendo as necessidades da empresa.

Ao criar uma conexão VPN, deve ocorrer a conexão de pessoas remotas autorizadas pela empresa e fornecer uma interconexão de redes geograficamente distantes, possibilitando o acesso das filiais com a empresa matriz. Essa conexão será feita através de um processo chamado tunelamento, onde os dados vão trafegar de uma extremidade a outra da conexão de uma forma segura. A segurança das informações passadas pelo túnel é garantida através da criptografia e formação de um novo pacote de dados visíveis apenas em dois pontos, o de partida e o de chegada.

Segundo cabini et all (2012), com a rede pode-se fazer circular informação, em qualquer lugar com menos custo e em tempo reduzido, com isso as organizações viverão uma grande vantagem, principalmente aquelas que tem muitas filiais.

Com a instalação da VPN na máquina, é realizada uma configuração por meio de um arquivo que contém as referências necessárias para fazer o tunelamento da conexão.

Após essa configuração, esse arquivo será processado através de um software mediante as chaves de acesso. Concluído esse processo, a rede estará habilitada para iniciar o protocolo de segurança (IPSec). O funcionamento da VPN se dá pela conexão em um provedor de internet e através dessa conexão dar instaurar um tunelamento com a rede remota.

Tipos de VPN

As redes privadas virtuais (VPN) podem ser classificadas referente à sua topologia e segurança.

Intranet

Segundo Rossi e Franzin (2000):

> Uma Intranet é utilizada para conectar sites que geralmente possuem uma infraestrutura completa de rede local, podendo, ou não, ter seus próprios servidores e aplicativos locais. Tais sites têm em comum a necessidade de compartilhar recursos que estejam distribuídos, como bases de dados e aplicativos, ou mesmo de troca de informações, como no caso de e-mail. A Intranet pode ser entendida como um conjunto de redes locais de uma corporação, geograficamente distribuídas e interconectadas através de uma rede pública de comunicação. Esse tipo de conexão também pode ser chamado de LAN-to-LAN ou Site-to-Site (ROSSI E FRANZIN, 2000).

Extranet

De acordo com Miranda (2002):

> Uma Extranet VPN será implementada para modelos informacionais que exijam dados em tempo hábil, correspondendo a cadeia de negócios existentes, como exemplo uma empresa que necessita ter os dados de seus sócios, fornecedores, clientes entre outros, dessa maneira é necessária uma solução aberta, para garantir a interoperabilidade com as várias soluções que as empresas envolvidas possam ter em suas redes privadas. Uma oura observação relevante é considerar o controle de tráfego, o que minimiza o efeito gargalo existente nos nós entre as redes e ainda garante uma resposta rápida para aplicações mais trabalhosas. (MIRANDA, 2002).

Argumentando sobre Acesso Remoto VPN Miranda (2002) diz que:

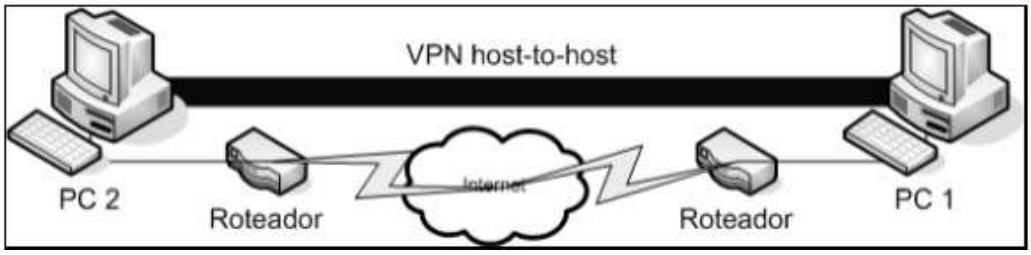
> Uma VPN de acesso remoto conecta uma empresa a seus empregados que estejam distantes fisicamente da rede. Neste caso torna-se necessário um software cliente de acesso remoto. Quanto aos requisitos básicos, o mais importante é a garantia de QoS (Quality of Service), isto porque,

> geralmente quando se acessa remotamente de um laptop, você está limitado à velocidade do modem. Outro item não menos importante é uma autenticação rápida e eficiente, que garanta a identidade do usuário remoto. E por último, um fator importante, é a necessidade de um gerenciamento centralizado desta rede, já que ao mesmo tempo, pode-se ter muitos usuários remotos logados, o que torna necessário que todas as informações sobre os usuários, para efeitos de autenticação, por exemplo, estejam centralizadas num único lugar (MIRANDA, 2002).

Existem três tipos de configurações de uma conexão VPN, sendo elas:

Host-Host: configuração onde existe um túnel entre os dois hosts, para que os dois pontos de acesso possam ter uma comunicação através da rede pública.

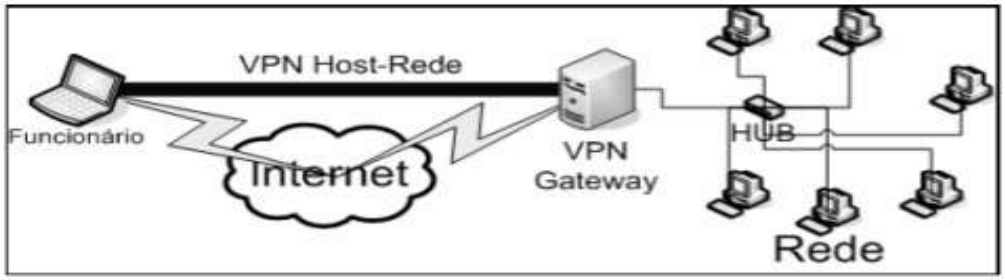
Figura 1. Representação de VPN Host-host



Fonte: Gendorf (2006).

Host-Rede: Configuração onde a conexão é estabelecida através de um host e uma rede privada.

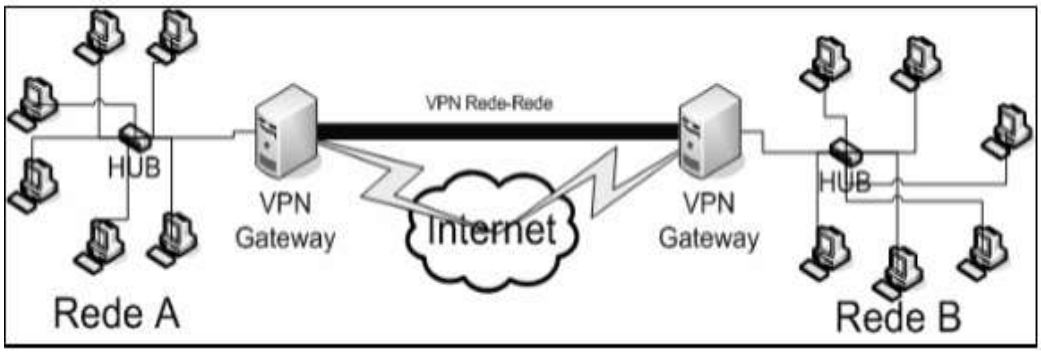
Figura 2. representação de VPN Host-rede.



Fonte: Gendorf (2006).

Rede-rede: Configuração onde a conexão é feita entre duas redes diferentes.

Figura 3. Representação de VPN Host-rede.



Fonte: Gendorf (2006).

Vantagens da VPN

Segundo Monteiro et al (2000), A utilização da VPN tem muitas vantagens em relação às outras opções, como por exemplo, linhas dedicadas. Para a sua construção existe um custo a pagar e a maior parte desse custo são declarações do desempenho na comunicação. Dentre as vantagens da VPN, estão:

- Redução de gastos, pois é utilizado uma rede pública para interligar dois pontos distantes através do acesso remoto.
- A otimização da comunicação, facilitando a troca de dados de uma forma rápida e simplificada.
- A segurança durante o transporte de dados, já que os mesmos são criptografados.
- Acessibilidade, pois a rede poder usada em toda parte geográfica que tenha acesso a internet.

Funções da Rede VPN

Segundo Rossi et al (2000), A VPN, sendo uma implementação segura apresenta algumas funções básicas para garantir a privacidade, integridade e autenticação das corporações envolvidas na comunicação:

- Privacidade – Como o meio de comunicação usado é público, fica fácil desviar os dados. É necessário garantir que os dados que estão a circular

sejam totalmente privados, de forma que mesmo se elas foram roubadas não sejam entendidas.

- Integridade – Possuem um mecanismo que detecta alterações de pacotes. No momento em que os dados forem recebidos, deve-se garantir na totalidade que ninguém, além do receptor/emissor possa alterar ou reencaminhar.
- Autenticação – Acesso apenas de pessoas autorizadas durante a troca de dados para evitar que as informações sejam roubadas. Os dados de uma VPN só vão reconhecer o outro VPN, se essas conexões tiverem autorização para a comunicação entre elas.

Segurança da rede VPN

Para garantir o funcionamento seguro de uma VPN, algumas técnicas podem ser utilizadas, como:

- **Modo túnel criptografado:** Segundo Miranda (2002), tanto os dados quanto o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de saída e de chegada.
- **Modo túnel não criptografado:** Segundo Chin (1998), o tunelamento não criptografado trabalha com o cabeçalho de pacotes e dados em um novo empacotamento e transmissão de acordo com um novo endereço de IP, o cabeçalho e os dados serão mantidos tais como foram geridos, porém tal processo leva a quebra da integridade, o que colocaria em risco a segurança dos dados.
- **Modo transporte:** Nesse modelo somente os dados é que passariam pelo processo de criptografia, surgindo mudanças no tamanho dos pacotes enviados e recebidos. Em uma análise mais detalhada o procedimento emprega segurança adequada para implementações em que os dados tenham seu trafego exclusivamente entre dois nós da rede (comunicação entre as máquinas).
- **Modo transmissão:** De acordo com Rossi e Franzin (2000), somente os dados são criptografados, não havendo mudança no tamanho dos pacotes. Geralmente são soluções proprietárias, desenvolvidas por fabricantes.

Matheus Carvalho LEAL; Marcelo Renato do Carmo PEREIRA FILHO. A IMPORTANCIA DA VPN (VIRTUAL PRIVATE NETWORK) DURANTE A PANDEMIA COVID-19: UMA REVISÃO DE LITERATURA. Facit Business And Technology Journal. QUALIS B1. ISSN: 2526-4281 http://revistas.faculdadefacit.edu.br/index.php/JNT. Out/Nov - 2021. Ed. 31; V. 1. Págs. 314-332.

Elementos de uma conexão VPN

- **Tunelamento:** Se refere ao modo que as informações trafegam pela rede túnel tem como ideia principal enviar os dados entre uma extremidade e outra, criptografando as informações trocadas e depois encapsulando o pacote de dados original dentro de um pacote novo;
- **Autenticação das Extremidades:** Se refere a garantia de privacidade, onde somete os usuários autenticados participam da transmissão de dados. Essa autenticação é realizada através de protocolos certificados que implementam algoritmos de hash como MD5, garantindo assim privacidade e integridades s mensagens trocadas na rede;
- **Transporte Subjacente:** Se refere a utilização da infraestrutura da internet e do protocolo TCP/IP para comunicação entre as redes para transmitir os pacotes de VPN, possibilitando a instalação e transmissão desses pacotes em qualquer parte da rede.

Protocolos

A Virtual Private Network (VPN) ou Rede Privada Virtual é uma das formas usadas pra unir diferentes redes de uma empresa, onde se utiliza para isso um meio público (geralmente a internet) para trafegar os dados entre elas. A sua característica principal é criar túneis de comunicação entre as redes, de forma que os dados trafeguem criptografados por estes túneis, aumentando a segurança na transmissão e recepção dos dados. Os protocolos da VPN têm a função de abrir, gerenciar e comunicar as funções dos tuneis virtuais.

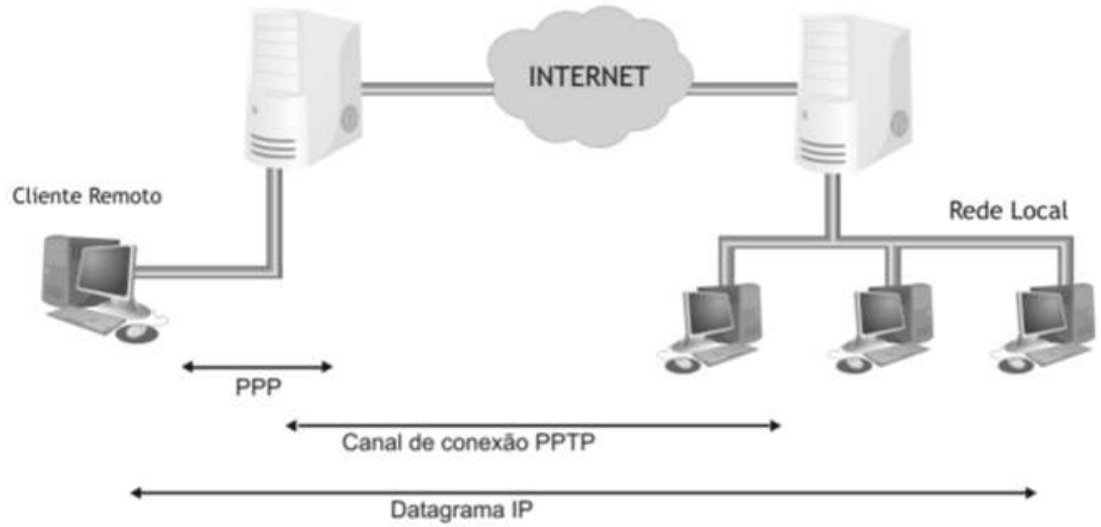
Alguns dos principais protocolos utilizados nos túneis virtuais são: PPTP (Point-to-Point Tunneling Protocol); L2TP (Layer 2 Tunneling Protocol); IPSEC (Internet Protocol Security). A escolha do protocolo será responsável pela conexão, trafego das informações e criptografia entre as maquina (hosts) da rede privada.

Point-to-Point Tunneling Protocol (PPTP) – O tunelamento ponto – a – ponto foi um dos primeiros protocolos de VPN a ser criado e surgiu para facilitar o acesso de computadores remotos a uma rede privada. É um protocolo da camada II da camada de enlace (TCP/IP). Ele é incorporado no Windows a partir do NT 4.0 e em clientes do

Windows 95 através de um patch. Agrega as funcionalidades do Point-to-Point Protocol (PPP) [Simpson 1994] para que o acesso remoto faça um túnel virtual até o destino. O PPTP encapsula pacotes PPP utilizando uma versão modificada do protocolo Generic Routing Encapsulation (GRE) [Farinacci et al. 2000]. Permitindo ao PPTP [Hamzeh et al. 1999] flexibilidade em lidar com outros tipos de protocolos como IPX, NetBEUI etc. O protocolo se baseia nos mecanismos de autenticação do PPP, os protocolos CHAP [Simpson 1996], MS-CHAP [Zorn 2000] e o inseguro PAP [Lloyd and Simpson 1992].

Os itens envolvidos em uma conexão PPTP são: cliente, servidor PPP e o servidor de rede.

Figura 4. Conexão PPTP



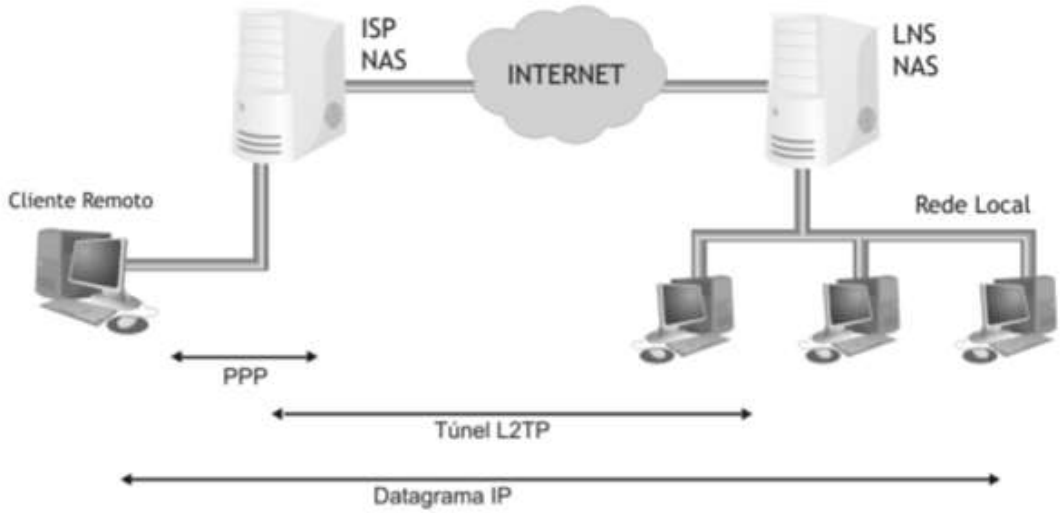
Fonte: Borges (2021).

Layer Two Tunneling Protocol (L2TP)

Buscando se criar um padrão de protocolos de tunelamento, o IETF uniu as melhores característica dos protocolos PPTP e o L2F, oferecendo assim uma maior flexibilidade do IP com a privacidade do Frame Relay permitido que o envio dos serviços sejam feitos nas terminações dos túneis. O L2TP tem a função de realizar o encapsulamento de pacotes PPP fazendo o uso de mecanismos de autenticação PPP. Esse protocolo também tem a função de prover a autenticação e suporte do túnel para que suas extremidades sejam autenticadas.

Criado para suportar dois modelos de tunelamento: Compulsório (criado automaticamente e iniciado pelo servidor de acesso a rede sob a conexão discada) e voluntario (iniciado pelo computador remoto, sendo mais flexível para usuários em transito que podem discar para qualquer provedor de acesso, como o provedor não participa da criação dos tuneis, este pode percorrer vários servidores sem precisar de uma configuração explicita), o funcionamento é baseado em um concentrador de acessos L2TP localizado no ISP, troca mensagens PPP com o servidor de rede L2TP para criação dos túneis. O L2TP passa os pacotes através do túnel virtual entre as extremidades da conexão. Os quadros enviados pelos usuários ao serem aceitos pelo ISP, são encapsulados em pacotes L2TP e encaminhados pelo túnel.

Figura 5. Conexão L2TP.



Fonte: Borges (2021).

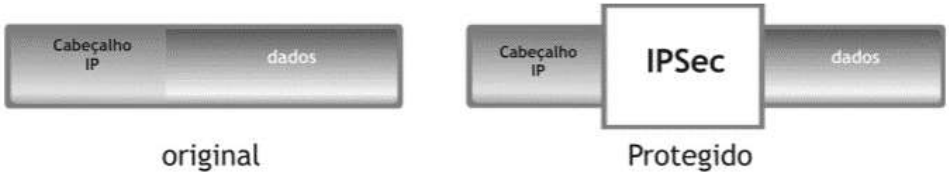
IP Security (IPSec)

No ano de 1995 devido as carências de segurança no protocolo IP, o IPSsec foi criado como uma alternativa para suprir essas carências de segurança. Esse conjunto de protocolos fornecem serviços de autenticação, controle de acesso, integridade e confidencialidade permitindo assim que um sistema se comunique com outro de forma rápida e transparente.

O IPSec pode funcionar de duas maneiras diferentes:

Modo Transporte: Há uma transmissão imediata dos dados protegidos entre as máquinas (hosts). Toda autenticação é realizada no payload e usada em clientes que fazem o uso do IPSec.

Figura 6. IPSec modo transporte.



Fonte: Borges (2021).

Modo Túnel: Os dados originais são encapsulados em um novo pacote criptografado (incluindo o cabeçalho original) e enviado para outro gateway, que desencapsula os dados e o encaminha ao seu destino final.

Figura 7. IPSec modo túnel

Fonte: Borges (2021).

O IPSec possui as características:

- Authentication Header (AH) - Sua principal função é garantir a integridade dos dados presentes no pacote incluindo a parte não alterável do cabeçalho, no entanto, tal função não garante a confidencialidade dos dados;
- Encapsulation Security Payload (ESP) - Miranda (2002) o conceitua como uma função que garante integridade, autenticidade e criptografia a área dos dados do pacote, sendo uma opção adequada para a implementação de um protocolo que cumpre as três vertentes de uma VPN segura, ou seja, integridade, confidencialidade e autenticidade.

Uso da VPN no Home Office

Com o surgimento da nova doença Covid-19/coronavírus, a maioria das empresas tiveram que encerrar ou reduzir suas atividades laborais devido as medidas restritivas para evitar a propagação do vírus. O novo cenário exigiu que as empresas tivessem que se reinventar e se adaptar à nova realidade e adotar o modo de trabalho home office.

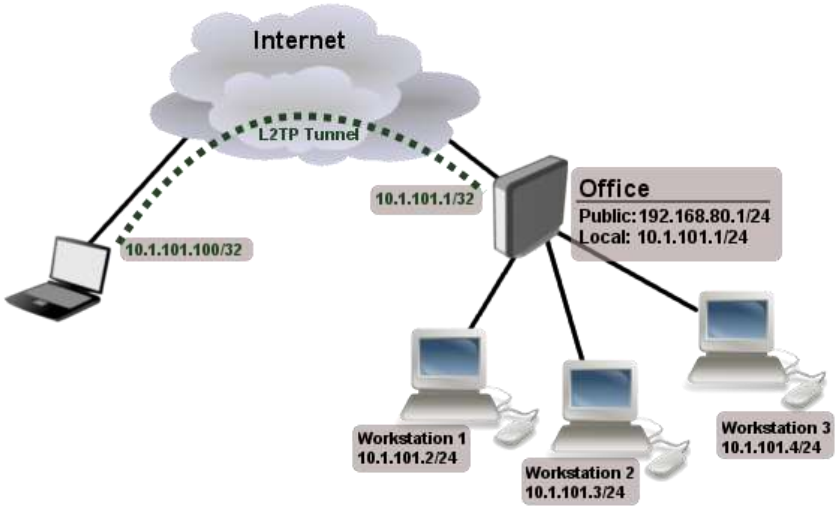
Inúmeros desafios surgiram tanto para as empresas quanto para as equipes de TI (tecnologia da informação), pois tiveram que se adaptar a várias mudanças na sua infraestrutura sem um planejamento prévio para conseguir se manter no mercado e atender a nova demanda em um curto período de tempo.

O teletrabalho é todo trabalho realizado à distância, ou seja, fora do local de trabalho, com uso de computadores, telefonia fixa e/ou celular e toda tecnologia que permita trabalhar em qualquer lugar, receber e transmitir informações, arquivos, imagens ou som relacionados à atividade laboral. A tecnologia foi criada para a melhoria da qualidade de vida do ser humano, e com sua evolução, a ideia de trabalho remoto se tornou uma realidade, chamado home office.

Virtual Private Network (VPN) é um recurso de cibersegurança que permite o tráfego de dados na internet seja feito de forma privada. Através da VPN todos dados enviados e recebidos são criptografados, de modo que terceiros não sejam capazes de acessá-los. A VPN atua como um firewall que protege o computador, criando um "túnel" exclusivo para que os dados trafeguem pela rede. A empresa precisa fornecer a VPN para que, mesmo de casa, o trabalhador e os dados estejam seguros.

Na prática do "home office" a VPN é primordial para que os colaboradores acessem os serviços de rede e as informações sensíveis da empresa normalmente, de onde quer que eles estejam. A única ferramenta que eles precisam para isso é o seu dispositivo (notebook corporativo) e de uma conexão com a Internet. Ou seja, orientando a sua equipe corretamente e implementando a ferramenta de cibersegurança adequada, é possível manter a produtividade da equipe, proteger os dados da empresa e evitar a propagação do Corona Vírus.

Figura 8. Terminal Service.



Fonte: https://wiki.mikrotik.com/wiki/Manual:Interface/L2TP.

Com toda a parte da VPN criada e configurada pelo Administrador de redes da empresa como demonstra na figura a cima, O cliente precisa configurar o acesso no terminal service ter acesso aos dados e comunicar com a Empresa.

Configuração da VPN utilizando o protocolo L2TP/IPSEC nos computadores dos colaboradores que estão em home office, os passos a seguir instrui o usuário de forma fácil e pratica a autenticar o acesso a VPN para ter acesso aos dados da empresa pelo túnel de conexão de forma segura e rápida.

- **Passo 1.** Acesse as configurações do Windows 10. Para isso, abra o menu Iniciar e clique em “Configurações”, na lateral esquerda;
- **Passo 2.** Na janela de configurações do sistema, clique em “Rede e Internet”;
- **Passo 3.** Agora, na barra lateral esquerda, clique em “VPN” e, à direita, selecione “Adicionar uma conexão VPN”;
- **Passo 4.** Entre com os dados da conexão VPN Passada pelo Administrador de Redes da sua Empresa (nome, endereço, usuário e senha) e, por fim, clique em “Salvar”;
- **Passo 5.** Agora, clique sobre o nome da VPN que você configurou para exibir as opções. Por lá, você pode se conectar ao servidor ou removê-lo.

Dessa forma passada pelo Administrador de Redes, você poderá configurar uma conexão VPN em seu computador ou tablet com Windows 10 e acessar redes privadas da sua Empresa.

DISCUSSÃO

VPN ideal permite que o usuário remoto trabalhe como se estivesse em uma estação de trabalho no escritório. Autenticação, transparência e facilidade de uso para o usuário remoto são fatores cruciais para este cenário. Nas redes de computadores, a segurança das informações tem novas conotações, os dados podem estar a ser utilizado remotamente e isso leva a uma nova forma de controlo.

Como essas redes de computadores geralmente são constituídos por hubs, roteadores, switches, terminais e servidores, onde cada um pode ter um nível diferente de implementação da segurança. Atualmente a circulação de informação nas redes é muito extensa, com a evolução tecnológica a utilização da internet vem sendo a prioridade para a tomada de decisão, definição dos negócios para a empresa. O uso da internet requer muita segurança, visto que por ali passa todos os dados que pode comprometer o futuro de uma empresa.

Pesquisas apontam que o trabalho remoto aumenta significativamente a produtividade dos colaboradores, e do ponto de vista da empresa, ocorre a redução dos custos organizacionais, como por exemplo, menor consumo de energia, água, e muitas vezes, redução das posições de trabalho dos funcionários, sendo possível diminuir o tamanho dos escritórios físicos, ou seja, é possível reduzir aluguéis ou a compra de locais mais enxutos (BLOOM, 2014).

Inicialmente quando surgiram as redes de computadores não havia uma preocupação tão grande quanto a segurança quanto hoje. Naquela época, era difícil imaginar que nos dias de hoje praticamente tudo funcionária com o auxílio de maquinas (Santini 2005). Com os avanços da tecnologia, obtemos diferentes formas de comunicação entre um local e outro independente da distância. Essas conexões permitem uma significativa redução de custos com infraestrutura e equipamentos e tempo.

Segundo Queirz (1998). VPN (virtual private network), surgiu da necessidade de interligar redes ou sub-redes privados a partir de outra rede para suporte de canais de comunicação seguro e mais barato. De acordo com Lima et al (2013), Uma VPN é

constituída para garantir a seus usuários segurança, integridade e confiabilidade no transporte de dados, sendo alternativa a links dedicados ou conexões exclusivas de redes. Dessa maneira, precisamos considerar alguns fatores para a sua constituição. O primeiro fator a ser levado em consideração ao criar-se uma VPN é o tipo de tunelamento, onde são desenvolvidos túneis blindados para a passagem de dados, e somente os usuários que detenham "autenticação" para trafegar na rede VPN tenha acesso aos dados enviados e recebidos nesse "túnel".

Uma das tecnologias largamente utilizadas pelas organizações para a conexão dos colaboradores para o trabalho remoto, a VPN (Virtual Private Network), em sua modalidade "Client to Site", cria um túnel de comunicação criptografado com a organização, que estende ao colaborador todos os recursos organizacionais, ferramentas e aplicações necessárias para a execução de suas atividades em qualquer lugar, além de oferecer a mesma segurança dos recursos de segurança da informação para o computador do colaborador remotamente (BAOMIN, NING & HONGQIANG, 2010).

De outro modo, a rede virtual privada (VPN) estende uma rede privada por uma rede pública e permite que os usuários enviem e recebam informações em redes públicas ou em pool, como se as suas manobras de computação estivessem diretamente associadas ao sistema enclausurado. Os aplicativos executados na VPN podem, portanto, se beneficiar da funcionalidade, segurança e gerenciamento da rede privada (JYOTHI & REDDY, 2018)

Segundo (Heyman, 2007) as conexões de rede privada virtual (VPN) estabelecem conexões seguras entre um usuário remoto e uma rede doméstica criptografando pacotes enviados pela Internet em vez de criar uma verdadeira rede privada. Sendo assim, pode-se afirmar que a utilização de VPNs tem colaborado diretamente no estabelecimento de conexões seguras entre redes, sem a necessidade de construção de infraestrutura adicional complexa, uma vez que, dependendo do cenário de uso, pode se tornar extremamente caro e problemática dependendo das características das redes comunicantes.

De acordo com Tyson (2007), a conexão virtual privat network vem como uma resposta aos usuários que buscam um preço acessível e uma rede eficaz para trafegar seus dados nas redes sem interferência de meios alheios. Este "usuário" está nas mais amplas esferas dos indivíduos que fazem uso da rede mundial de computadores, seja ele um usuário doméstico, assim como um usuário empresarial. A maioria das empresas têm instalações espalhadas por todo o país e até mesmo pelo mundo e todas precisam de uma

coisa: uma maneira de manter uma comunicação rápida, segura e confiável onde quer que seus escritórios estejam. Até recentemente, isso significou o uso de linhas dedicadas para manter uma rede de longa distância (TYSON, 2007).

A VPN deve dispor de ferramentas para permitir o acesso de clientes remotos autorizados aos recursos da rede corporativa e viabilizar a interconexão de redes geograficamente distantes, de forma a possibilitar acesso de filiais a matriz. Em geral, uma VPN, deve possibilitar o compartilhamento de dados e informações, além de garantir a privacidade e integridade dos dados que trafegam pela Internet.

CONCLUSÃO

A rede de computadores e vias de comunicação vem cada vez mais crescendo e se tornando presente na vida das pessoas, sendo uma ferramenta indispensável seja no ambiente de trabalho, escolar ou doméstico. Com essa nova era tecnológica onde tudo se revolve através de computadores/smartphones a segurança dos dados se tornou uma preocupação complexa.

Antigamente se fazia apenas o backup dos dados, mas com o avanço tecnológico outras soluções foram criadas para garantir a segurança durante o transporte dos dados durante a navegação na rede como a combinação de hardwares e softwares. É uma rede privada que possui inúmeras qualidades pois fornece uma intercomunicação segura garantida através dos tuneis e criptografia dos dados, gerando assim uma comunicação estável entre os usuários. Por possuir uma facilidade na comunicação e troca de dados entre locais distintos, as empresas cada vez mais vem aderindo a VPN no ambiente corporativo.

A VPN é uma vantagem para empresas que têm filiais ou ligações com outras empresas pois utiliza uma rede de dados privada e uma infraestrutura publica para transmissão de dados, mantendo assim uma confidencialidade e integridade durante a troca de informações de um lugar ao outro.

As redes privadas virtuais têm uma grande importância para as organizações, principalmente no aspecto econômico, como redução de custos, estabilidade e facilidade na comunicação.

Conforme vimos, a VPN é uma tecnologia muito útil no ambiente empresarial, que permite às pessoas acessarem documentos e conteúdos da empresa remotamente. Isso é

muito relevante, visto que a atual pandemia afastou os colaboradores dos escritórios e o home office virou o "novo normal". Portanto, a utilização da VPN em ambiente corporativo está se mostrando uma boa oportunidade para gestores que se preocupam com segurança, produtividade e redução de custos.

REFERÊNCIAS

BORGES, F. Fagundes, BA. Cunha, GN. VPN: **Protocolos e Segurança.** Universidade Catolica de Petropolis – UCP. 2021.

BLOOM, N. (2014). To raise productivity, let more employees work from home. **Harvard business review,** 92(1/2), 28-29

CABRINI F. H. et all. (2012). **Configuração de VPN Cisco**. 2012.

CARNEIRO, A. (2002). **Introdução à Segurança dos Sistemas de** informação. Lisboa: Editora de Informática, Ltda.

GENDOF, F. (2012). **Redes Virtuais Privadas em ambiente Cooperativo**. 2006. Obtido em:http://www.inf.ufsc.br/bosco.sobral/ensino/ine5630/material-cripto seg/slides.pdf.

GOMES, A. et all (2001). **Políticas de Segurança em redes de computadores.**

HEYMAN, Karen, 2007 "A new virtual private network for today's **mobile world." Computer** 40.12 (2007): 17-19. https://wiki.mikrotik.com/wiki/Manual:Interface/L2TP.

G1. (2019). Home office bateu recorde no Brasil em 2018. **IBGE.** G1.

LIMA, FS. SILVA, JA. MOURA, TR. Epaminonas, JM. Gonçalves, IR. VPN: Uma solução prática e economicamente viável. **Revista Tecnologias em Projeção** | v.4 | n.1. 2013.

LI, R., PEI, S., CHEN, B., SONG, Y., ZHANG, T., YANG, W., & SHAMAN, J. (2020). Substantial undocumented infection facilitates the rapid dissemination of novel coronavirus (SARS-CoV2). **Science,** 368(6490), 489-493.

MENEZES, G. M. (2004**). Viabilização de comunicação criptografia usando VPN com ADSL**.

PETERSON, L. L; DAVIE, B. S. (2003) **"Redes De Computadores".** 3. Ed. Rio De Janeiro: Elsevier.

SOUZA, Lindeberg Barros de. "Redes de Computadores": Guia Total. **Tecnologia, Aplicações e Projetos em Ambiente Corporativo**. 1. Ed. São Paulo. (2009).

SANTINI, S. (2005). We are sorry to inform you Computer, 38(12):128, 126–127.
SARLO, Lino, da Silva. **"Virtual Private Network**". Aprenda a construir rede privadas virtuais em plataformas linux e windows, Editora Novatec 2003.

SENA, J. C., GEUS, P. L., and AUGUSTO, A., Impactos da Transição e Utilização do IPv6 sobre a Segurança de Ambientes Computacionais. In: II WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS, maio 2002, Búzios. **Anais do 20o Simpósio Brasileiro de Redes de Computadores.** Búzios: SBRC'2002, 2002, pp.73-80.

SOUZA R. M. (2007). **Implantação de Ferramentas e Técnicas de segurança da Informação.**

OKANO, MT. SANTOS, HCL. HORONATO, WJ. VIANA, AM. URSINI, EL. **Impactos da pandemia Covid-19 em empresas de grande porte:** avaliação das mudanças na infraestrutura de tecnologia para o teletrabalho sob as óticas das teorias das capacidades dinâmicas e estrutura adaptativa. 2020. Preprint foi publicado em um jornal como um artigo. DOI do artigo publicado http://doi.org/10.33448/rsd-v9i9.7852.