CENTRO UNIVERSITÁRIO BRASILEIRO-UNIBRA
CURSO DE GRADUAÇÃO TECNOLÓGO EM REDES DE COMPUTADORES

GENILSON CARLOS DA SILVA NASCIMENTO
HYAGO FELIPE MORAIS DA SILVA
WESLEY COSTA DE FREITAS BEZERRA

REDES VIRTUAIS PRIVADAS NOS AMBIENTES CORPORATIVOS

RECIFE/2021

GENILSON CARLOS DA SILVA NASCIMENTO
HYAGO FELIPE MORAIS DA SILVA
WESLEY COSTA DE FREITAS BEZERRA

REDES VIRTUAIS PRIVADAS NOS AMBIENTES CORPORATIVOS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores. Professor(a) Orientador(a): Msc Ameliara Freire

RECIFE/2021

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 1745.

N244r Nascimento, Genilson Carlos da Silva

Redes virtuais privadas nos ambientes corporativos / Genilson Carlos da Silva Nascimento, Hyago Felipe Morais da Silva, Wesley Costa de Freitas Bezerra. Recife: O Autor, 2021.

35 p.

Orientador(a): Msc. Ameliara Freire Santos de Miranda.

Trabalho De Conclusão De Curso (Graduação) - Centro Universitário Brasileiro – Unibra. Tecnólogo em Redes de Computadores, 2021.

Inclui Referências.

1. VPN. 2. Conexão. 3. Criptografia. 4. Internet. 5. Segurança. 6. Dados. I. Silva, Hyago Felipe Morais da. II. Bezerra, Wesley Costa de Freitas. III. Centro Universitário Brasileiro - Unibra. IV. Título.

CDU: 004

Dedicamos este trabalho a todos que contribuíram direta ou indiretamente em nossa formação acadêmica.

AGRADECIMENTOS

Agradecemos primeiramente a Deus, por nos ter dado vida e capacidade de raciocínio para sempre buscar o conhecimento.

À nossa família que nos apoiou do início ao fim em todas as decisões tomadas por cada um de nós.

Ao nosso corpo docente por sempre nos prestar apoio em todas as dúvidas e questionamentos que houve durante o desenvolvimento do trabalho.

Abreviaturas

VPN – *Virtual Private Network*

TI – *Tecnologia da Informação*

SSL – *Secure Sockets Layer*

TLS – *Transport Layer Security*

PPTP – *Point-to-Point Tunneling Protocol*

L2TP – *Layer 2 Tunneling Protocol*

IPsec – *Internet Protocol Security*

MPLS – *Multi-Protocol Label Switching*

IP – *Internet Protocol*

SSH - *Secure Socket Shell*

DES - *Data Encryption Standard*

AES - *Advanced Encryption Standard*

RSA - *Rivest-Shamir-Adleman*

SAFER - *Secure and Fast Encryption Routine*

IDEA - *Internacional Encryption Algorithm*

Lista de Figuras

Sumário

REDES VIRTUAIS PRIVADAS NOS AMBIENTES CORPORATIVOS

Genilson Carlos da Silva Nascimento

Hyago Felipe Morais da Silva

Wesley Costa de Freitas Bezerra

Nome e sobrenome do(a) professor(a) orientador(a): Ameliara Freire

Resumo: Este trabalho tem como objetivo mostrar a definição de VPN assim como apresentar seu funcionamento, suas tipificações e seus benefícios. Apresentando exemplos de revisões bibliográficas, além de alternativas para o serviço, vantagens e desvantagens para um completo entendimento ao leitor. Porquanto, muitos colaborares utilizam VPN e não sabem o quão importante pode ser a ferramenta. Em detrimento disso, surge o interesse no desenvolvimento desta pesquisa no fito de conscientizar e trazer mais informações a respeito da Rede Virtual Privada que é a ferramenta que os colaboradores utilizam no âmbito corporativo. Por fim, será mostrado a relação entre VPN e segurança, e será apontado a exclusividade dos colaboradores autorizados em se conectar na rede da empresa, atendendo os pilares da segurança da informação.

Palavras-chave: VPN, Conexão, Criptografia, Internet, Segurança, Dados

Abstract: This work aims to show the definition of VPN along with its operation, types and benefits. Presenting examples of bibliographic reviews, as well as alternatives for the service, advantages and disadvantages for a complete understanding of the reader. Many employees use VPN and do not know how important the tool can be, with that came the interest in presenting this research, as a means of raising awareness and bringing more information to employees about the Virtual Private Network, a tool they use in the corporate sphere. Finally, the relationship between VPN and security will be shown, where in the conclusion it will be pointed out that only authorized employees can connect to the company's network, meeting the pillars of information security.

Keywords: VPN, Connection, Encryption, Internet, Security, Data

1. Introdução

Após o início da pandemia do covid-19 em março de 2020, pode-se perceber importantes mudanças nos hábitos sociais, visto que a necessidade de lavar as mãos com mais frequência, fazer a utilização de máscara, álcool em gel e evitar aglomerações para minimizar o contágio da doença, transformou-se o “novo normal” no cotidiano das pessoas.

Nesse ínterim, muitas empresas foram surpreendidas por não poder contar com seus colaboradores presencialmente, obrigando algumas a encerrarem suas atividades devido à crise econômica advinda desta situação inusitada.

Em decorrência disso, aquelas que conseguiram permanecer ativas buscaram a modalidade de trabalho de home office, assim, o setor de TI teve a responsabilidade de implementar uma infraestrutura para os seus funcionários acessarem os dados fora da empresa com segurança.

A segurança da informação é um desafio no dia a dia das empresas. Nesse processo, visa-se garantir a integridade dos documentos, seja no armazenamento ou ao compartilhar os arquivos de maneira eficiente. Esse fato tem deixado os profissionais de TI em alerta devido ao fato de que é a circulação de todas as informações da está acessível fora do local físico da empresa, pois o home office se tornou o modelo de trabalho mais utilizado.

Outrossim, a gestão corporativa necessitou implementar uma política que pudesse apresentar as diretrizes do serviço remoto aos colaboradores. Logo, foi necessário precaver além de tomar medidas tomadas em todas as tecnologias utilizadas, porque atualmente acontecem muitos ataques por via de engenharia social, além de possíveis arquivos maliciosos ingressarem na estação de trabalho do colaborador.

Portanto, os Analistas de Infraestrutura visam a implementação da VPN, uma rede virtual privada que usa a internet para conectar um ou vários computadores e manter os dados seguros nesse intermédio, Oliveira (2020). Pois, as redes virtuais privadas trabalham paralelas a rede pública, com a diferença de ter predefinida uma rota privada, garantindo a segurança dos dados (Tanenbaum, 2003).

As redes virtuais privadas têm outras vantagens, logo, ao implantar uma VPN, é executado um túnel entre as extremidades da conexão. Sendo assim, os dados trafegam de uma ponta até a outra.

Cabe destacar também que os benefícios para o uso de VPN são diversos, essencialmente no baixo custo e na comunicação segura. (Duarte, 2020).

Segundo Kaspersky (2021) criptografia em segurança virtual é a conversão de dados de um formato legível em um formato codificado. Consoante a isso, os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

Somado a isso, as VPN’s são imprescindíveis para os pilares de segurança da informação em virtude da criptografia embutida em seus túneis. Pois, de acordo com a OpenVPN (2021), empresa líder global em redes privadas e Cibersegurança, "uma Rede Privada Virtual (VPN) fornece à sua empresa uma conexão criptografada com segurança à sua rede pela Internet pública".

1.1 Objetivos

1.1.1 Objetivo Geral

Apresentar a VPN como uma boa alternativa para o intermédio ao tráfego de dados entre a empresa e seus colaboradores.

1.1.2 Objetivos específicos

- Analisar o que é VPN e seu funcionamento;
- Apresentar os tipos de aplicação da VPN;
- Citar as vantagens e desvantagens.

1.2 Justificativa

O trabalho tende a defender o uso da rede virtual privada para as corporações, mostrando o uso adequado e relatando a mesma como uma ótima opção, pois existem empresas que fazem a implementação do serviço sem estarem cientes dos riscos e de como usar de forma correta.

VPN pode ser uma solução para os dados trafegarem de forma segura, sendo um ótimo investimento quando implantada conscientemente de qual tipo mais adequado para a necessidade, segundo Duarte, (2020) VPN surgiu da necessidade

de se utilizar redes de comunicação não confiáveis para trafegar informações de forma segura.

Sendo a pesquisa voltada tanto para profissionais de TI que buscam entender um pouco mais o serviço, quanto para conscientizar os colaboradores sobre o uso da rede virtual privada, referenciando a importância dela no ambiente corporativo.

1.3 Metodologia

O trabalho foi realizado a partir da pesquisa bibliográfica.

2. Referencial Teórico

2.1 VPN: Definição e funcionamento

A sigla VPN significa Rede Virtual Privada, e é definida como uma ferramenta de tecnologia que é bastante utilizada por redes particulares, permitindo o colaborador utilizar seu dispositivo em uma rede desprotegida na internet com segurança, para enviar, receber e compartilhar dados na web (Kaspersky, 2021).

Segundo Oliveira (2020), é uma tecnologia de rede que utiliza a internet para conectar um grupo de computadores e manter a segurança dos dados que trafegam entre eles.

A VPN surgiu através da necessidade de segurança no compartilhamento de dados de uma rede com a outra sem serem interceptados por algum agente mal-intencionado, a sua maior função é fazer com que as redes continuem se comunicando com outras de forma protegida dentro da rede pública, Duarte (2020).

O seu funcionamento é semelhante à de um firewall, e à grosso modo é responsável pela proteção dos dados na internet assim como é o firewall com os dados do computador, podendo funcionar como acesso remoto ou *Site To Site*. Como por exemplo, quando se está usando uma VPN, o tráfego utiliza um túnel criptografado deixando a informação disponível apenas para você e o servidor VPN, Oliveira (2020).

Segundo Oliveira, 2020 há alguns tipos de uso mais comuns para VPN:

- Colaborador/funcionário: utiliza a VPN fornecida pela empresa quando está em casa ou viajando para acessar recursos na rede local;
- Fazer downloads: para evitar que alguma empresa o coloque na lista negra por estar baixando torrents, esse usuário utiliza VPN para se manter seguro enquanto usa as redes peer to peer;
- Para manter a privacidade: esse tipo de usuário sempre acha que estão lendo o que ele envia ou recebe. Por isso, para ter uma comunicação segura e criptografada, longe de olhos curiosos, este perfil utiliza conexão VPN;
- Viajante: serviços como Netflix e Amazon Prime disponibilizam um conteúdo distinto para cada país, de acordo com sua língua e costumes. Por isso, esse usuário viajante possui uma conexão VPN com o país de origem para ter acesso ao seu conteúdo preferido.

Mormente a isso, pelo método SSHA uma conexão VPN é feita da seguinte maneira: segundo Almeida (2020) a conexão entre o ambiente corporativo do escritório central e as localidades remotas é muito simples e se dá por meio da internet.

Atrelado a isso, o ponto de acesso remoto estabelece uma sessão via túnel SSH seguro com os controladores de rede e, após provisionado, forma um túnel seguro com o plano de dados, seja dos appliances físicos ou virtualizados. A partir deste momento, toda a comunicação é feita de forma segura e criptografada. Atualmente a plataforma permite dois modelos de topologia, centralizada e segregada (Almeida, 2020). A figura 1 apresenta o túnel criado pela VPN.

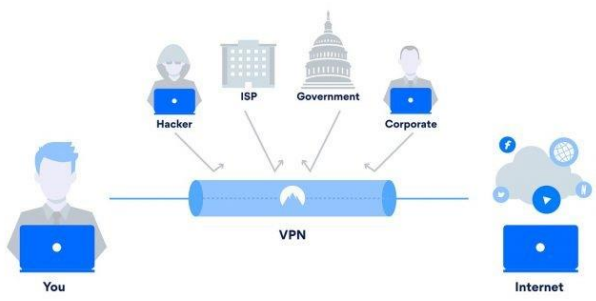

Figura 1. Túnel criado pela VPN Fonte: cybersecurity.att.com, 2019

Segundo Dias (2016) o tunelamento é uma técnica utilizada pela maioria das VPN’s (Redes Virtuais Privadas). Este é um processo que basicamente coloca cada pacote de informação enviado dentro de outro pacote, criando uma espécie de envoltório no mesmo.

2.2 Segurança

Segurança da informação é um assunto indispensável dentro de uma empresa e está dentro das vantagens pelo uso da VPN, pois a informação é o que tem de mais valioso dentro de uma corporação, sendo assim, esse conceito consiste em proteger a informação em si e não os ativos por onde ela irá trafegar ,e para tal deve seguir os três pilares confidencialidade, integridade e disponibilidade (Benetti, 2017).

As redes virtuais privadas, tem que o objetivo de manter o trafego seguro, mas para que ocorra é preciso que garanta Confidencialidade, Integridade e Autenticidade.

O primeiro ponto da confidencialidade é definido como todos os dados que trafegam que devem ser privados e criptografados. E, de acordo com Telium, 2020, a confidencialidade tem a ver com a privacidade dos dados da organização. Esse conceito se relaciona às ações tomadas para assegurar que informações confidenciais e críticas não sejam roubadas dos sistemas organizacionais por meio de ciberataques, espionagem, entre outras práticas.

Após isso, vem a integridade em que todos os dados devem seguir o seu curso predefinido, e que não tenham sucesso caso tentem re-encaminhar. Logo, citando Telium, 2020 "Integridade corresponde à preservação da precisão, consistência e confiabilidade das informações e sistemas pela empresa ao longo dos processos ou de seu ciclo de vida".

Por conseguinte, a disponibilidade visa garantir que apenas pessoas autorizadas tenham acesso aos dados, segundo Telium, 2020 "A disponibilidade está relacionada ao tempo e à acessibilidade_que se tem dos dados e sistemas da empresa, ou seja, se eles podem ser consultados a qualquer momento pelos colaboradores".

No que diz respeito a implementação correta da VPN, Goujon, (2012) diz que uma implementação correta dessa tecnologia permite assegurar a confidencialidade e a integridade das informações da empresa.

Segundo Furtado (2020) a tecnologia é uma ferramenta utilizada para manter a integridade dos documentos, armazenar e compartilhar arquivos de maneira eficiente, impedindo perdas, extravio ou violação de sigilo. Assim, o uso dessa tecnologia aliado a uma mudança na cultura e conscientização, possibilita que as atividades sejam realizadas rapidamente e com a devida segurança.

Na contemporaneidade, está mais comum as empresas de vários setores flexibilizarem a jornada de trabalho com a implementação do home office. Diante disso, é fundamental ter uma política específica que apresente as diretrizes do trabalho remoto de forma transparente para seus trabalhadores, assim como tomar cuidados a fim de garantir a segurança da informação e dos dados das empresas.

Outro fator importante é necessidade de a gestão corporativa verificar se as medidas estão sendo tomadas de forma correta, entendendo se os profissionais estão realmente se prevenindo de possíveis ataques cibernéticos. O ideal é que a empresa disponibilize dispositivos com sistemas e programas de proteção já instalados, como antivírus e firewall, tomando as devidas providências é possível dar continuidade ao trabalho tranquilamente e sem nenhum risco para o negócio (Furtado, 2020).

Segundo Andrade (2020) ao adotar o home office como uma modalidade de trabalho, as empresas e seus colaboradores devem ficar atentos a uma série de fatores que podem apresentar riscos para a segurança da informação daquela companhia e de seus clientes.

Neste momento é preciso refletir sobre os equipamentos utilizados pelos funcionários, seja ele da empresa ou pessoal, analisar com maior profundidade quais medidas podem ser tomadas para amenizar o risco dos ataques cibernéticos. Uma das preocupações que devem ser consideradas no home office é a exposição de informações a outras pessoas que convivem com o colaborador no mesmo ambiente, podendo ocorrer compartilhamento de dados sigilosos, havendo

possibilidade que a infraestrutura doméstica esteja precária, seja por uso dos equipamentos pessoais ou pela vulnerabilidade da internet residencial (Andrade, 2020).

Segundo Andrade (2020), VPN's (Virtual Private Network ou Rede Privada Virtual) são conexões que mantêm o tráfego de dados de forma segura e permitem o acesso a uma rede interna de uma empresa, mesmo trabalhando em casa. Com a adoção de VPN sendo recomendada por especialistas em segurança da informação, onde somente computadores e dispositivos que têm as credenciais necessárias recebem acesso a essas redes.

2.3 Criptografia

A criptografia é um conjunto de medidas que altera o pacote deixando a violação não autorizada, uma vez que cria uma chave privada que será usada para descriptografar o arquivo na outra ponta, sendo o modelo simétrico ou uma chave pública caso opte pela técnica assimétrica que usa chaves diferentes para criptografar e descriptografar (Pisa, 2012).

Esta tecnologia é utilizada há bastante tempo para evitar que terceiros subtraiam ou fraudem informações sigilosas. É importante conhecer quais são os tipos e as principais diferenças para entender como essas tecnologias conseguem proteger os dados (CryptoID, 2019).

DES

Segundo CryptoID (2019) Data Encryption Standard (DES) é uma das primeiras criptografias utilizadas e é considerada uma proteção básica de poucos bits (cerca de 56). O seu algoritmo é o mais difundido mundialmente e realiza 16 ciclos de codificação para proteger uma informação. A complexidade e o tamanho das chaves de criptografia são medidos em bits. Quando uma criptografia é feita com 128 bits, significa que 2128 é o número de chaves possíveis para decifrá-la. Atualmente, essa

quantidade de bits é considerada segura, mas quanto maior o número, mais elevada será a segurança.

No momento que um bloco é criptografado em bits, significa que um conjunto de informações passou pelo mesmo processo da chave, se tornando ilegível para terceiros. O DES pode ser decifrado com uma técnica de força bruta, por isso que os desenvolvedores precisam buscar alternativas de proteção mais complexas além do DES (CryptoID, 2019).

3DES

Segundo CryptoID (2019) o Triple DES foi originalmente desenvolvido para substituir o DES, já que os hackers aprenderam a superá-lo com relativa facilidade. Houve um tempo em que o 3DES era o padrão recomendado para segurança. Essa criptografia recebe esse nome pelo fato de trabalhar com três chaves de 56 bits cada, o que gera uma chave com o total de 168 bit. Especialistas no tema argumentam que uma chave de 112 bits é suficiente para proteger os dados.

DESX

Segundo CryptoID (2019) essa é outra variante do DES e trata-se de uma solução bastante simples do algoritmo, mas que aumenta exponencialmente a resistência contra-ataques de força bruta sem elevar a sua complexidade computacional. Adicionam-se 64 bits antes da encriptação, o que aumenta a proteção de 120 bits contra força bruta, essa tecnologia não é mais imune contra ataques mais sofisticados, como criptoanálises.

AES

Segundo CryptoID (2019) Advanced Encryption Standard (AES) — ou Padrão de Criptografia Avançada, em português — é o algoritmo padrão do governo dos Estados Unidos e de várias outras organizações. Ele é confiável e excepcionalmente

eficiente na sua forma em 128 bits, mas também é possível usar chaves e 192 e 256 bits para informações que precisam de proteção maior.

O AES é amplamente considerado imune a todos os ataques, exceto aos ataques de força bruta, que tentam decifrar o código em todas as combinações possíveis em 128, 192 e 256 bits, o que é imensamente difícil na atualidade.

Camellia

Segundo CryptoID (2019) desenvolvido em 2000, Camellia é uma criptografia que decifra blocos de informações. Trata-se de uma tecnologia com níveis de segurança bastante semelhantes ao AES, já que pode ser processada em 128, 192 e 256 bits.

Camellia pode ser implementada tanto em softwares quanto em hardwares, também sendo compatível com tecnologias mais econômicas de 8 bits até com processadores mais potentes de 32 bits (CryptoID, 2019).

RSA

Segundo CryptoID (2019) Rivest-Shamir-Adleman (RSA) foi um dos pioneiros em relação à criptografia de chave pública, seu nome é composto pelos sobrenomes de seus criadores, que também são fundadores da companhia RSA Data Security. Esse é considerado um dos algoritmos mais seguros do mercado, por essa razão também foi o primeiro a possibilitar a criptografia na assinatura digital. O RSA funciona da seguinte forma: ele cria duas chaves diferentes, uma pública e outra privada (que deve ser mantida em sigilo). Todas as mensagens podem ser cifradas pela pública, mas somente decifradas pela privada.

Hoje em dia essa tecnologia é utilizada em operações rotineiras, como por exemplo no envio de e-mails, compras online, assinatura digital, entre outras coisas (CryptoID, 2019).

Blowfish

Segundo CryptoID (2019) esse é outro algoritmo desenvolvido para substituir o DES. É uma cifra simétrica que divide as informações em blocos de 64 bits e criptografa cada um deles individualmente. O Blowfish é conhecido por sua velocidade de encriptação e efetividade em geral. Trata-se de uma tecnologia bastante segura, pois há estudiosos no assunto que afirmam que o código não pode ser quebrado.

É grátis e qualquer pessoa pode conseguir uma cópia do código-fonte, alterar e utilizá-lo em vários programas. O Blowfish é usado em plataformas de e-commerce para garantir segurança nos pagamentos e proteger senha de acesso dos usuários (CryptoID, 2019).

Twofish

Segundo CryptoID (2019) o Twofish é uma variação do Blowfish e consiste na cifração de blocos simétricos. A diferença é que ele é formado por blocos de 128 bits e chaves de até 256 bits. A tecnologia é considerada uma das mais rápidas de seu tipo e é ideal para prover segurança de softwares e hardwares. Seu código-fonte também é gratuito, podendo ser manipulado e utilizado por qualquer programador.

Há outra variação da mesma criptografia chamada Threefish, a diferença está nos tamanhos dos blocos que são de 256, 512 e 1024 bits, com chaves do mesmo tamanho (CryptoID, 2019).

SAFER

Segundo CryptoID (2019) SAFER (“mais seguro” em português) é uma sigla para Secure and Fast Encryption Routine. Consiste na criptografia de blocos em 64 bits, por isso é conhecido como *SAFER SK-64*.

No entanto, foram encontrados pontos fracos nesse código, que resultou no desenvolvimento de novas versões com diferentes tamanhos de chave, como a SK-40, SK-64 e a SK-128 bits (CryptoID, 2019).

IDEA

Segundo CryptoID (2019) o Internacional Encryption Algorithm (IDEA) é uma chave simétrica desenvolvida em 1991, que opera blocos de informações de 64 bits e usa chaves de 128 bits. O algoritmo em questão age de forma diferente, pois usa a confusão e difusão para cifrar o texto. Na prática, ele utiliza três grupos algébricos com operações misturadas, e é dessa forma que o IDEA consegue proteger as informações.

3. Tipos de VPN

As VPN's são identificadas em dois tipos, são elas: VPN de acesso remoto e Site a Site (Alhambra, 2020).

3.1 VPN de Acesso Remoto

Consiste em uma conexão segura e privada que acontece via internet, ela é útil no caso de um colaborador que está de home office ou em viagem e precisa entrar na rede privada da empresa, tendo acesso aos recursos necessários ao trabalho, como e-mail ou documentos corporativos (Alhambra, 2020).

Outro uso no caso dos usuários domésticos, geralmente ocorre quando precisam acessar sites restritos à sua região e utilizam a VPN para mascarar sua localidade, ou buscando melhorar a segurança da sua conexão (Alhambra, 2020).

Segundo Silva (2020) VPN de acesso remoto a um túnel protegido na internet, em que é possível acessar e-mails, documentos e sistemas corporativos em nuvem sem qualquer interceptação de administradores de redes diferentes. Abaixo, a figura 2 mostra a estrutura da VPN de acesso remoto.

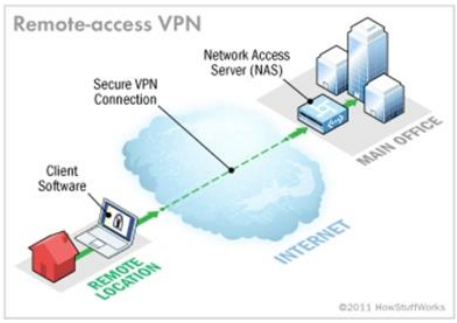

Figura 2 - VPN de Acesso Remoto Fonte: computer.howstuffworks.com, 2021

3.2 VPN Site a Site

Esse tipo de VPN também é conhecida como VPN roteador a roteador e é bastante utilizada no ambiente empresarial. muitas empresas executam a VPN site a site para conectar matriz a filial em diferentes locais geográficos (Alhambra, 2020).

Quando vários departamentos da mesma empresa na mesma região geográfica são conectados através dessa forma, isso é chamado de VPN via Intranet, conforme mostra na figura 3. Quando uma empresa utiliza este para conectar a outra empresa, é chamado de VPN via Extranet (figura 4).

Esse tipo cria uma conexão virtualizada entre as redes em empresas distantes, conectando através da Internet para manter uma comunicação segura e privada entre as empresas. A VPN site a site é baseada na conexão de roteador a roteador, um roteador atua como um emissor e outro como um receptor VPN. A conexão entre os dois só é permitida depois que uma autenticação é autorizada entre os aparelhos. (Alhambra, 2020).

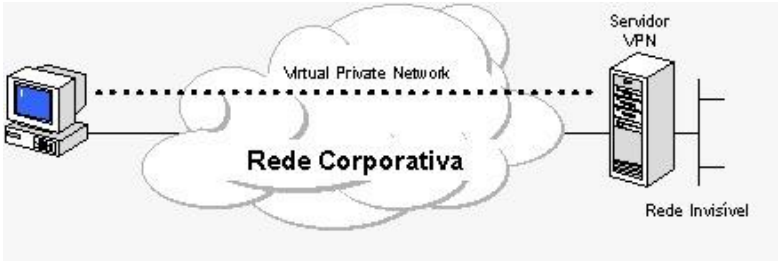

Figura 3 - Imagem Conexão intranet Fonte: gta.ufrj.br, 2016

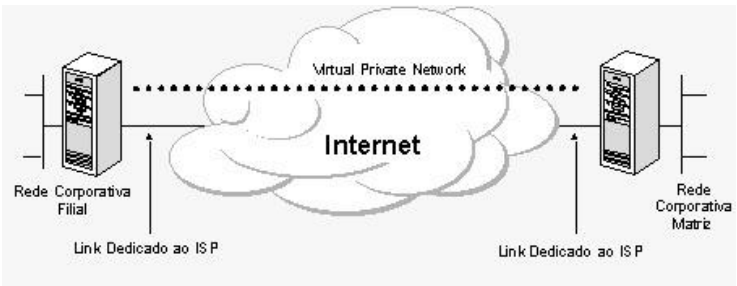

Figura 4 - Imagem conexão extranet Fonte: gta.ufrj.br, 2016

4. Protocolos VPN

4.1 IPSec

Como diz o nome, ele cuida da segurança da comunicação em uma rede IP, de maneira que autentica a sessão e usa criptografia para cada pacote durante uma conexão.

IPSec trabalha em dois modos emcapsulamento e transporte, apresentado na figura 5, sendo a principal diferença que o primeiro criptografa o pacote inteiro, enquanto ou ultimo apenas a mensagem do pacote. Segundo Jamhour (2009) é um protocolo de camada 3 projetado para suprir a falta de segurança de informações trafegando em rede pública.

Em suma, o IPSec protege os pacotes IP de dados privados, encapsulando em outros pacotes IP para serem transportados, conforme mostra na figura 6.

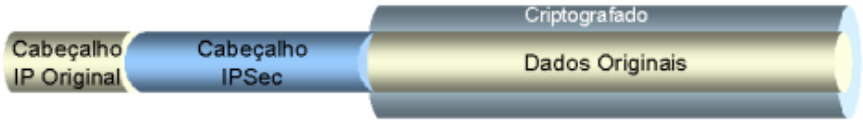

Figura 5 - IPSec Modo Transporte. Fonte: gta.ufrj.br

Figura 6 - IPSec Modo Túnel. Fonte: gta.ufrj.br

IPsec é transparente tanto para a os roteadores da Internet, que enxergam a mensagem como um datagrama comum com um cabeçalho IP roteável, quanto para os dispositivos na redes locais, que recebem e enviam pacotes descriptografados. Utilizando tês algoritimos de criptografias nesse processo AES128, HMAC-MD5 e HMAC-SHA1 (Cisco, 2002)

4.2 L2TP

Segundo Klusaite (2020) o Layer 2 Tunneling Protocol (“protocolo de tunelamento de camada 2”) não fornece nenhuma criptografia ou autenticação, é só um protocolo de tunelamento VPN que cria uma conexão entre você e o servidor VPN. Ele usa outras ferramentas IPSec para criptografar seu fluxo de dados e mantê-lo em privacidade e segurança. Este protocolo tem algumas vantagens, mas certos pontos fracos devem ser levados em conta.

L2TP é muito seguro pelo fato de não oferecer nenhuma ferramenta de criptografia em si mesmo, ele pode aceitar vários protocolos de criptografia diferentes,

ao invés de fornecer criptografia por conta própria, ele reuni várias criptografias diferentes (Klusaite, 2020).

Segundo Klusaite (2020) o Layer 2 Tunneling Protocol (“protocolo de tunelamento de camada 2”) não fornece nenhuma criptografia ou autenticação, é só um protocolo de tunelamento VPN que cria uma conexão entre você e o servidor VPN. Assim, utiliza outras ferramentas IPSec para criptografar seu fluxo de dados e mantê-lo em privacidade e segurança. Este protocolo tem algumas vantagens, mas certos pontos fracos devem ser levados em conta.

L2TP é muito seguro pelo fato de não oferecer nenhuma ferramenta de criptografia em si mesmo, ele pode aceitar vários protocolos de criptografia diferentes, ao invés de fornecer criptografia por conta própria, ele reuni várias criptografias diferentes (Klusaite, 2020).

Ademais, possui uma alta compatibilidade segundo Vpnmentor (2021) integrado em todo os dispositivos/sistemas operacionais modernos compatíveis com VPN.

4.3 PPTP

Segundo VpnMentor, (2021) desenvolvido por um consórcio fundado pela Microsoft Corporation, o encapsulamento ponto-a-ponto cria uma Rede Privada Virtual em redes discadas e tem sido o protocolo padrão para VPN’s desde a sua criação. O primeiro protocolo VPN a ser suportado pelo Windows, o PPTP fornece segurança através de uma variedade de métodos de autenticação, como o MS_CHAP v2, que é o mais comum do lote.

Segundo Alhambra (2020) o PPTP cria um encapsulamento e envolve o pacote de dados. Além disso, usa um protocolo ponto a ponto (PPP) para criptografar os dados entre a conexão. O PPTP é um dos protocolos VPN mais usados e está em uso desde o Windows 95. Além do Windows, o PPTP também é suportado no Mac e Linux.

Em situações normais, é utilizada uma criptografia de 128 bits, porém existem falhas graves a exemplo da possibilidade de uma autenticação MS-CHAP v2 não encapsulada, e mesmo que tenha sido uma falha corrigida, a conexão por PPTP é recomendada apenas quando a segurança não for a prioridade (vpnMentor, 2021).

Em contrapartida, ainda é bastante utilizado devido a sua boa compatibilidade, segundo VpnMentor (2021) todos os dispositivos e plataformas compatíveis com VPN tem o PPTP disponível como padrão, e uma vez que sua configuração é relativamente fácil, ele continua sendo a principal escolha tanto para provedores de VPN como para empresas.

4.4 SSL e TLS

SSL e TLS são tipos de protocolo que formam uma VPN em que o navegador atua como cliente e limita o acesso do colaborador a aplicativos específicos. Esses protocolos são mais usados por sites de compras online e provedores de serviços, segundo Augusto (2014), são protocolos de criptografia projetados para internet. Permitem a comunicação segura entre os lados cliente e servidor de uma aplicação web.

A conexão VPN por SSL permite um acesso remoto seguro por um navegador web , segundo Rosencrance, (2021) uma conexão SSL VPN usa criptografia ponta a ponta (E2EE) para proteger os dados transmitidos entre o software cliente do dispositivo de terminal e o servidor SSL VPN por meio do qual o cliente se conecta com segurança à Internet. As conexões E2EE são bastante confiáveis e tem compatibilidade com os navegadores modernos, descartando a necessidade de softwares clientes de terceiros (Rosencrance, 2021).

Segundo Microsoft, (2021) os protocolos TLS e SSL estão localizados entre a camada de protocolo do aplicativo e a camada TCP/IP, em que eles podem proteger e enviar dados do aplicativo para a camada de transporte. Como os protocolos

funcionam entre a camada de aplicativo e a camada de transporte, o TLS e o SSL podem dar suporte a vários protocolos de camada de aplicativo.

4.5 OpenVPN

Segundo Vpnmentor (2021) uma tecnologia de código aberto relativamente nova, o OpenVPN utiliza os protocolos SSLv3/TLSv1 e a biblioteca OpenSSL, juntamente com uma combinação de outras tecnologias, para fornecer aos usuários uma solução VPN confiável e forte. O protocolo é altamente configurável e funciona melhor em uma porta UDP, mas pode ser configurado para ser executado em qualquer outra porta também, tornando extremamente difícil para a Google e outros serviços similares bloqueá-lo.

O OpenVPN possui uma grande vantagem por sua segurança poder utilizar vários algoritmos de criptografia, tornando bastante confiável, segundo (Vpnmentor,2021) sua biblioteca OpenSSL suporta vários algoritmos criptográficos, tais como 3DES, AES, Camellia, Blowfish, CAST-128 e muitos outros. O padrão de criptografia utilizado é de blowfish 128 bits, é ideal, porém há falhas conhecidas (Vpnmentor, 2021).

Embora seja bastante popular entre os tipos de VPN e já utilizado como padrão em alguns serviços de VPN, não é suportado pelas plataformas e é obrigado que softwares de terceiros sejam utilizados (vpnmentor, 2021).

4.6 SSH

A comunicação SSH utiliza três métodos de criptografia e segungo Santana (2019) forma de manipulação de dados da qual o SSH se beneficia é o hash criptográfico. Funções de hash criptográfico são métodos para criar uma assinatura

ou resumo de um conjunto de informações. Seus principais atributos distintivos são que eles nunca devem ser revertidos, são praticamente impossíveis de influenciar e são praticamente únicos.

O protocolo tambem irá usar do método de chave simétrica, e segundo Santana (2019) a criptografia simétrica é uma única chave ou um par de chaves que são usados para criptografar e descriptografar uma mensagem. Essa chave é usada para criptografar toda a sessão de comunicação entre um cliente e um servidor.

Por fim, a criptografia assimétrica é usada pelo ssh, porém de uma maneira diferente da percepção geral, e segundo Gaino (2021) a criptografia assimétrica não é usada para criptografar toda a sessão SSH. Em vez disso, ela só é usada durante o algoritmo de troca de chaves de criptografia simétrica.

O SSH cria uma rota para transferir os dados, e garante que a rota seja criptografada. As conexões são criadas por um cliente SSH e os dados são transferidos de uma rede local para o servidor remoto através desta rota.

Segundo SSH Academy (2021) é um pacote de software que permite a administração segura do sistema e a transferência de arquivos em redes inseguras, ele é usado em quase todos os Data Centers e em todas as grandes empresas. A figura 7 a seguir mostra o funcionamento do SSH.

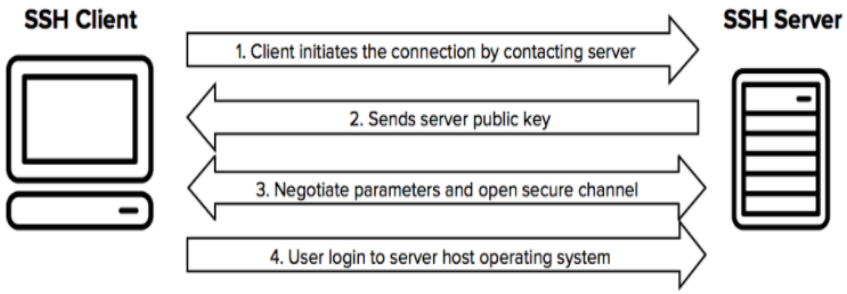

Figura 7 - Protocolo SSH Fonte: ssh.com/academy, 2021

5. VPN: Vantagens e desvantagens

5.1 Vantagens

Dentre as vantagens, a rede virtual privada pode trazer diferenças significativas em termos de custos, haja vista que algumas empresas tiveram cortes de custos imobiliários, pois estavam ultilizando as VPN's em serviço home office, por exemplo, segundo Silva, (2020) o home office pode ter se tornado mais comum em 2020, mas empresas que utilizam esse modelo de trabalho há mais tempo já comemoravam o corte de gastos.

Uma das maiores fabricantes de computadores do mundo, a Dell relatava em 2016 já economizar cerca de US$ 12 milhões por ano em custos imobiliários.

5.1.1 Mobilidade

Com toda a certeza a vantagem de ter possibilidade de trabalhar comos sistemas da empresa de qualquer lugar do mundo com conexão internet é inegavelmente uma grande vantagem proporcionada pela rede virtual privada Oliveira, (2020).

5.1.2 Possiblita o trabalho remoto

Segundo One (2019) ao ter uma rede VPN, aqueles que têm permissão à ela podem acessar de onde estiverem, não importa o dispositivo ou o lugar do mundo, desde que tenham acesso a internet. Isso pode ser interessante para quando os funcionários precisam trabalhar remotamente. Pois, com esse acesso irrestrito, fica desnecessário carregar notebooks da empresa ou anotar informações importantes quando estiverem à distância.

Com isso o trabalho se torna mais simples, possibilitando os colaboradores compartilhar e modificar arquivos com outros usuários de forma remota. A empresa ganha em economia, e não é obrigada a investir em equipamentos e outras tecnologias que consigam garantir segurança no acesso remoto e seus funcionários

podem usar os próprios dispositivos para trabalhar, seja dentro ou fora da empresa (One, 2019).

5.1.3 Privacidade

Segundo One (2019) o uso do servidor VPN faz com que o que circula na rede não seja acessado por quem não tem essa permissão. Assim, cada indivíduo tem acesso apenas ao que é do seu interesse para o trabalho e nada mais. Como consequência, todas as informações e dados que circulam dentro da rede da empresa acabam sendo mais confiáveis e úteis. Por isso, a privacidade de quem usa a rede e da empresa estará garantida, sem riscos de informações importantes vazarem.

5.2 Desvantagens

Caso seja adotada uma VPN gratuita ou de baixo custo, ela pode deixar brechas em pontos especificos da transmissão, podendo ocasionar uma interceptação.

5.2.1 Dependência da Internet

Segundo One (2019) o acesso remoto é algo muito útil para se trabalhar fora da empresa. Contudo, ao utilizar esse acesso pelo servidor VPN, é preciso sempre estar conectado à internet. Se a rede tem conexão instável, cai ou se está em lugar sem o acesso à rede, não será possível acessar o servidor VPN e seus dados armazenados nele.

5.2.2 Confiança no Servidor

Muitos servidores de VPN oferecem serviços gratuitos ou com preços baixos. É de fundamental importancia pesquisar sobre em quem vai confiar os dados da empresa e o atendimento que o provedor oferece. As VPNs são atualizadas constantemente, por isso é importante ter um suporte em que a empresa consiga facilmente entrar em contato para resolver os problemas que podem ocorrer (One, 2019).

6. Considerações Finais

No estudo realizado foram demonstrados a definição de rede virtual privada, o seu funcionamento, os demais tipos de conexões, as vantagens, desvantagens e protocolos destrinchados.

Como fora apresentado, a VPN traz diversos benefícios, no quesito segurança e não está apenas ligado ao software utilizado, aos tipos de hardwares, de tecnologia ou ao gerenciamento das redes, mas em todos esses elementos citados associa-se o comprometimento das partes envolvidas e uma política de segurança bem estruturada e aplicada.

Diante disso, foi visto que a VPN é uma ótima solução para as empresas que desejam implementar em sua infraestrutura, visto que permiti o acesso remoto dos colaboradores autorizados a se conectarem na rede de sua instituição.

Pode-se concluir que para adotar a VPN na rede é necessário possuir um bom link de internet, de preferência dedicado, escolher bem o tipo mais adequado para sua necessidade e obter um software que faça a comunicação de dados segura entre dois pontos.

7. Referências

TANENBAUM, Andrew S. Computer Networks: Fourth Edition. Prentice Hall, march. 2003.

O que é uma VPN. [S. l.], 2021. Disponível em: https://openvpn.net/what-is-a-vpn/. Acesso em: 30 out. 2021.

O QUE é Rede Virtual Privada (VPN) e vantagens na utilização por empresas. [S. l.], 2020. Disponível em: https://www.profissionaisti.com.br/o-que-e-rede-virtual-privada-vpn-e-vantagens-na-utilizacao-por-empresas/. Acesso em: 30 out. 2021.

O QUE é Rede Virtual Privada (VPN) e vantagens na utilização por empresas. [S. l.]: Aléx de Oliveira, 2020. Disponível em: https://administradores.com.br/artigos/o-que-%C3%A9-rede-virtual-privada-vpn-e-vantagens-na-utiliza%C3%A7%C3%A3o-por-empresas. Acesso em: 30 out. 2021.

VPN de acesso remoto: o que é, para que serve e os benefícios de usar uma. [S. l.]: Douglas da Silva, 2020. Disponível em: https://www.zendesk.com.br/blog/o-que-e-vpn-acesso-remoto/. Acesso em: 30 out. 2021.

COMO FUNCIONA uma VPN (rede privada virtual). [S. l.]: Jeff Tyson, Chris Pollette e Stephanie Crawford, 2021. Disponível em: https://computer.howstuffworks.com/vpn.htm#pt3. Acesso em: 30 out. 2021.

OS TIPOS de VPN e os seus protocolos. [S. l.]: Alhambraitbr, 2021. Disponível em: https://www.alhambrait.com.br/os-tipo-de-vpn-e-os-seus-protocolos/. Acesso em: 30 out. 2021.

IPSEC. [S. l.]: Edgard Jamhour, 2009. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/vpn_ipsec/ipsec.html. Acesso em: 30 out. 2021.

COMO UTILIZAR uma VPN para a segurança da informação. [S. l.]: André Goujon, 2012. Disponível em: https://www.welivesecurity.com/br/2012/09/11/como-utilizar-uma-vpn-para-a-seguranca-da-informacao/. Acesso em: 31 out. 2021.

SEGURANÇA: como funciona o Protocolo SSL/TLS. [S. l.], 2014. Disponível em: https://www.ecommercebrasil.com.br/artigos/seguranca-como-funciona-o-protocolo-ssltls/. Acesso em: 30 out. 2021.

SSH (Secure Shell) Home Page. [S. l.], 2021. Disponível em: https://www.ssh.com/academy/ssh. Acesso em: 30 out. 2021.

O QUE é criptografia?. Pedro Pisa, 2012. Disponível em: https://www.techtudo.com.br/noticias/2012/06/o-que-e-criptografia.ghtml. Acesso em: 31 out. 2021.

POR QUE a VPN pode ser indispensável para a sua empresa?. [S. l.]: Telium Networks, 2018. Disponível em: https://telium.com.br/blog/por-que-a-vpn-pode-ser-indispensavel-para-a-sua-empresa. Acesso em: 31 out. 2021.

PRECISA se adaptar ao home office durante a pandemia? Descubra como. [S. l.], 5 abr. 2020. Disponível em: https://www.correiobraziliense.com.br/app/noticia/eu-estudante/trabalho-e-formacao/2020/04/05/interna-trabalhoeformacao-2019,842584/precisa-se-adaptar-ao-home-office-durante-a-pandemia-descubra-como.shtml. Acesso em: 13 nov. 2021.

SEGURANÇA da Informação – Confidencialidade, Integridade e Disponibilidade (CID). [S. l.], 20 jul. 2015. Disponível em: https://www.profissionaisti.com.br/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid/. Acesso em: 13 nov. 2021.

CONFIDENCIALIDADE, integridade e disponibilidade: os três pilares da segurança da informação. [S. l.], 14 set. 2018. Disponível em: https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao. Acesso em: 13 nov. 2021.

PROTOCOLO TLS. [S. l.]: Microsoft, 12 ago. 2021. Disponível em: https://docs.microsoft.com/pt-br/windows-server/security/tls/transport-layer-security-protocol. Acesso em: 17 nov. 2021.

OS TIPOS de VPN e os seus protocolos. [S. l.]: Alhambraitbr, 1 jul. 2020. Disponível em: https://www.alhambrait.com.br/os-tipo-de-vpn-e-os-seus-protocolos/. Acesso em: 17 nov. 2021.

DESVANTAGENS de uma VPN. [S. l.], 21 jun. 2021. Disponível em: https://vpnoverview.com/pt/informacoes-sobre-vpn/desvantagens-vpn/. Acesso em: 18 nov. 2021.

QUAIS são os aplicativos para tunelamento. [S. l.], 22 nov. 2016. Disponível em: https://segurisoft.com.br/vpn/o-que-e-tunelamento-dados/. Acesso em: 22 nov. 2021.

SEGURANÇA da informação: 8 cuidados para o trabalho remoto. [S. l.], 23 jul. 2020. Disponível em: https://blog.convenia.com.br/seguranca-da-informacao/. Acesso em: 6 dez. 2021.

SEGURANÇA da informação e proteção de dados em home office. [S. l.], 23 maio 2020. Disponível em: https://digilandia.io/home-office/seguranca-da-informacao-no-trabalho-remoto/. Acesso em: 6 dez. 2021.

APÓS começo turbulento, empresas se adaptam ao home-office e planejam mantê-lo. [S. l.], 16 ago. 2021. Disponível em: https://www.cnnbrasil.com.br/business/apos-comeco-turbulento-empresas-se-adaptam-ao-home-office-e-planejam-mante-lo/. Acesso em: 6 dez. 2021.

O QUE é criptografia de ponta a ponta e por que você precisa dela. [S. l.], 18 set. 2020. Disponível em: https://www.kaspersky.com.br/blog/what-is-end-to-end-encryption/16041/. Acesso em: 6 dez. 2021.

SERVIDOR VPN: quais são os prós e contras de usar. [S. l.], 1 nov. 2019.

Disponível em: https://blog.hostone.com.br/servidor-vpn/. Acesso em: 6 dez. 2021.

OS TIPOS dos Melhores Protocolos VPN. [S. l.]: Laura Klusaite, 20 set. 2020. Disponível em: https://nordvpn.com/pt-br/blog/protocolos-vpn/. Acesso em: 6 dez. 2021.

SSL VPN (Secure Sockets Layer virtual private network). [S. l.]: Linda Rosencrance, 1 out. 2021. Disponível em: https://www.techtarget.com/searchsecurity/definition/SSL-VPN. Acesso em: 7 dez. 2021.

COMO FUNCIONA o SSH. [S. l.]: Ariane G., 6 jul. 2021. Disponível em: https://www.hostinger.com.br/tutoriais/como-funciona-o-ssh#Entendendo-diferentes-tecnicas-de-criptografia. Acesso em: 7 dez. 2021.

COMO O SSH estabelece uma comunicação segura. [S. l.]: Leonardo Santana, 6 nov. 2019. Disponível em: https://sempreupdate.com.br/como-o-ssh-estabelece-uma-comunicacao-segura/. Acesso em: 7 dez. 2021.

VPNS and VPN Technologies. [S. l.], 4 jan. 2002. Disponível em: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4. Acesso em: 8 dez. 2021.