REVISTA Interdisciplinar da Meta

# PROPOSTA DE IMPLEMENTAÇAO DE SERVIDOR VPN NA NUVEM

PROPOSAL FOR IMPLEMENTATION OF VPN SERVER IN THE CLOUD

Thiago Rodrigues Santana[1]
Alex Sanches Macedo[2]
Jéssica Cristiane Faustino Viana[3]

**RESUMO:** Com a crescente necessidade de se reduzir custos, as VPNs (Virtual Private Networks) já são realidade para a comunicação corporativa, porém, o uso da conexão criptografada da VPN pode ter diversos usos. A segurança na comunicação tornou-se cada vez mais importante, e para empresas, se torna interessante a utilização por conta da crescente necessidade de se reduzir custos. As VPNs surgem como alternativa para a comunicação corporativa. Esta pesquisa trouxe um modelo de implementação do serviço de VPN para pequenas empresas e pessoas comuns de modo a utilizar poucos recursos, porém que garantam a integridade da comunicação.
**Palavras-chave:** Open VPN, Criptografia, Nuvem.

**ABSTRACT:** With the growing need to reduce costs, VPNs (Virtual Private Networks) are already a reality for corporate communication, but the use of the VPN's encrypted connection can have several uses. Security in cost reporting has become increasingly important, and for companies, it becomes interesting to use the need to increase reduction. VPNs are an alternative for corporate communication. This research brought a small set of VPN service implementation for common companies in order to use resources, but that protect a communication communication model.
**Keywords:** Open VPN, Cryptography, Cloud.

## INTRODUÇÃO

Hoje, as redes computadores proporcionam uma infinidade de recursos e informações que são cada vez mais utilizadas. A segurança em uma rede é um dos principais fundamentos, existem vários algoritmos capazes de prover segurança em uma rede, como tambem existem diversas maneiras de se obter uma conexão segura, uma delas é a utilização do protocolo VPN que fornece criptografia dos dados. Esta tecnologia depende de um servidor onde os dados do cliente serão recebidos e enviados pela internet. Neste contexto, a adição da tecnologia de computação em nuvem traz alternativas interessantes para a utilização da VPN.

[1] Acadêmico do curso de Redes de Computadores da Faculdade de Tecnologia do Amapá – META.
[2] Graduado em Engenharia da Computação pela Universidade Federal do Pará (2013) e mestre em Engenharia Elétrica pela Universidade Federal do Pará (2022).
[3] Licenciada em Computação pelo Centro Universitário Claretiano; Tecnóloga em Sistemas para Internet pela Faculdade de Tecnologia do Amapá e Bacharel em Publicidade e Propaganda pela Estácio. Pós-graduada em Design Gráfico, UX e Multimídia, Ensino de Música e Docência no Ensino Superior. Docente da Faculdade de Tecnologia do Amapá – META. E-mail: jessicaviana@meta.edu.br

## REFERENCIAL TEÓRICO

VPN é a sigla para Virtual Private Network, ou, Rede Privada Virtual. “O termo Virtual entra, porque depende de uma conexão virtual, temporária, sem presença física no meio” (Silva, 2010). Esta tecnologia estabelece a criação de uma rede e a comunicação entre computadores que se conectam usando uma rede pública, porém, diferente das redes padrão, a VPN determina uma comunicação segura através da criptografia dos dados transmitidos. A VPN cria um túnel encriptado para que a sua máquina possa acessar à internet sem que o seu provedor consiga registrar as suas atividades.

Segundo Diógenes; Mauser (2013) a criptografia é ciência que tem como objetivo “misturar” as informações para que pessoas não tenham acesso a dados confidenciais, de forma que elas não possam lê-los ou alterá-los, ou seja, garantindo a integridade destes dados.

“Essa tecnologia é amplamente utilizada no ambiente corporativo, pois as vezes o colaborador está fora do ambiente físico da empresa, mas precisa conectar-se para na rede da mesma, e pode utilizar desta forma está tecnologia.” (MOSN, de Moraes. 2020, p. 20)

Basicamente, uma VPN permite acesso remoto a recursos de uma rede local, ainda que você não esteja fisicamente conectado nessa rede. Também serve para garantir proteção durante a troca de informações pela internet em redes públicas. Para Silva (2005, p. 22) “Vivemos hoje num ambiente globalizado, onde a liderança nos negócios está justamente na capacidade de se ultrapassar as fronteiras” Uma conexão VPN permitiria que as redes locais dos estabelecimentos se comuniquem de forma segura e eficiente, dispensando a necessidade de uma infraestrutura mais complexa.

Sob um ponto de vista de topologia, existem duas categorias principais de conexões VPN.

Client to Site (Accesso remoto) e Site to Site (Gateway para-Gateway).

A diferença entre elas é: a VPN cliente to Site é caracterizada por conexões pontuais de usuários remotos à rede (*single user*). Em contrapartida *VPNs Site to Site* tratam de conexões remotas entre redes, ou seja, atuam como uma extensão da rede, conectando redes entre si.

Uma VPN por si só é apenas uma maneira de melhorar sua segurança e acessar recursos numa rede na qual você não está fisicamente conectado. Porém, dependendo do uso, essa ferramenta pode transformar completamente cenários de trabalho. Instituições utilizam VPNs para a comunicação entre departamentos, uma vez que essas empresas implementam essas redes privadas através de redes públicas.

## MATERIAIS E MÉTODOS

- **OpenVPN**

"Um aplicativo livre para rede privada virtual com SSL, que chegou à classe dos softwares-padrão na versão 2.1, sendo útil, principalmente, em configurações de ambientes de larga escala" (Soest. 2011, p. 41).

Este software é muito útil para criação de soluções VPN para empresas e pessoas, pois ela possui recursos de implementação e administração simplificada e ainda conta com todos os recursos necessários para uma conexão privada como tunelamento e criptografia e é completamente transparente aos usuários.

> Quando configurado de forma correta, é um pacote repleto de funcionalidades para criar uma VPN de forma segura e o funcionamento desta comunicação requer duas instâncias, sendo servidor e cliente, que se comunicam entre si. Este software utiliza a biblioteca OpenSSL para promover a criptografia entre os canais de controle de dados, que ocorre nos protocolos UDP ou TCP, sendo que as camadas de segurança podem ser reforçadas por um sistema de antivírus ou firewall corporativo. MOSNA (2020)

- **OPENVPN SERVER**

O servidor VPN se comunica com a Internet para estabelecer o túnel. Seja um servidor tradicional, seja um servidor cloud, o OpenVPN Server recebe a chamado e, em seguida, prepara o ambiente de VPN para conexao.

- **OpenVPN Client**

Esta é a parte que possibilita ao cliente se comunicar com o servidor e, também, com os computadores participantes da chamada em VPN, independentemente do sistema operacional que cada um utilize.

- **Protocolo**

OpenVPN é um software código aberto para conexões VPN, utiliza o protocolo OpenVPN baseado no TCP e UDP que garante a entrega dos dados com segurança e velocidade através do túnel criptográfico estabelecido.

- **Segurança**

O conceito de VPN existe com a ideia de segurança dos dados transmitidos e das conexões. O OpenVPN utiliza a biblioteca OpenSSL criptografia. A autenticação entre os pontos da rede VPN é feita através de chaves secretas compartilhadas, e certificados digitais de segurança que podem sem combinadas. As versões mais atuais do software possibilitam autenticação com usuário e senha.

- **Tunelamento**

O protocolo OpenVPN utiliza a técnica de encapsulamento, onde os protocolos são encapsulados dentro de outro. Para enviar um datagrama pela VPN, primeiramente o pacote é encriptado e depois o encapsulamento é feito adicionando outro cabeçalho para ser enviado pela internet.

- **Ubuntu Server**

É distribuição do software de código aberto Linux focada para o funcionamento de servidores.
Este é o sistema operacional utilizado nesta pesquisa para rodar no servidor na nuvem .

- **Computação em Nuvem**

Este termo define-se como a utilização de recursos e serviços de computação como: gerenciamento de rede, armazenamento, servidores, softwares etc... através da internet. O nome “nuvem” vem da comum utilização da figura da nuvem para caracterizar a internet em fluxogramas.

A computação em nuvem pode ser categorizada da seguinte forma:

IAAS – Infraestrutura como serviço

PAAS – Plataforma como serviço

SAAS – Software como serviço

- **Nuvem Pública**

É um modelo de T.I. onde os recursos de computação baseados na nuvem são oferecidos por um provedor terceirizado.

- **Hospedagem na nuvem**

É a utilização de recursos de computação em nuvem para hospedagem de dados, serviços de gerenciamento e soluções de hardware. tem como característica a virtualização de recursos computacionais, e o usuário utiliza esses recursos para hospedar uma rede ou servidores, por exemplo.

- **Infraestrutura Convergente**

Trata-se de uma infraestrutura de T.I. que integra duas ou mais soluções de tecnologia combinadas com o objetivo de centralizar o gerenciamento dos recursos na rede. Esta é uma das principais características da nuvem publica, ela fornece benéficos importantes como: segurança dos dados, desempenho e baixo custo. Esta pesquisa utiliza a computação em nuvem para virtualizar um servidor VPN.

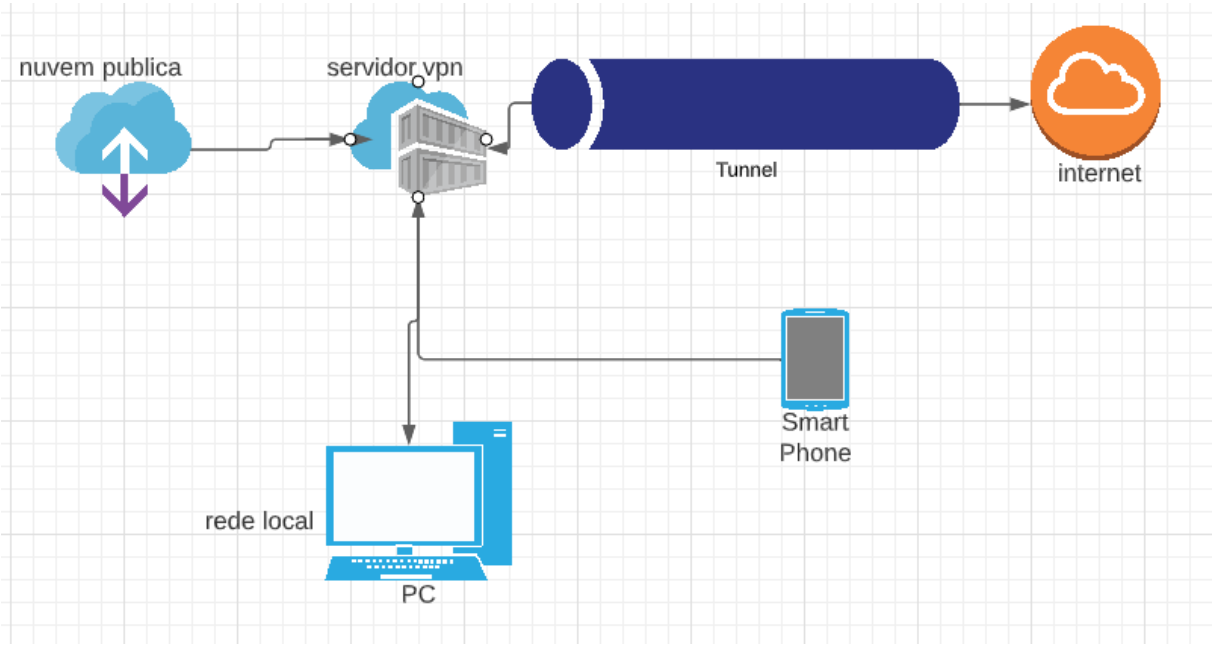
- **Azure**

É A nuvem publica da Microsoft utilizada neste estudo para hospedar o servidor VPN.

- **Topologia**

A figura 1 mostra a topologia da rede criada neste estudo. Todo o fluxo de dados da rede local é enviado para o servidor que envia o trafego criptografado pela internet

**Figura 1** – diagrama da topologia

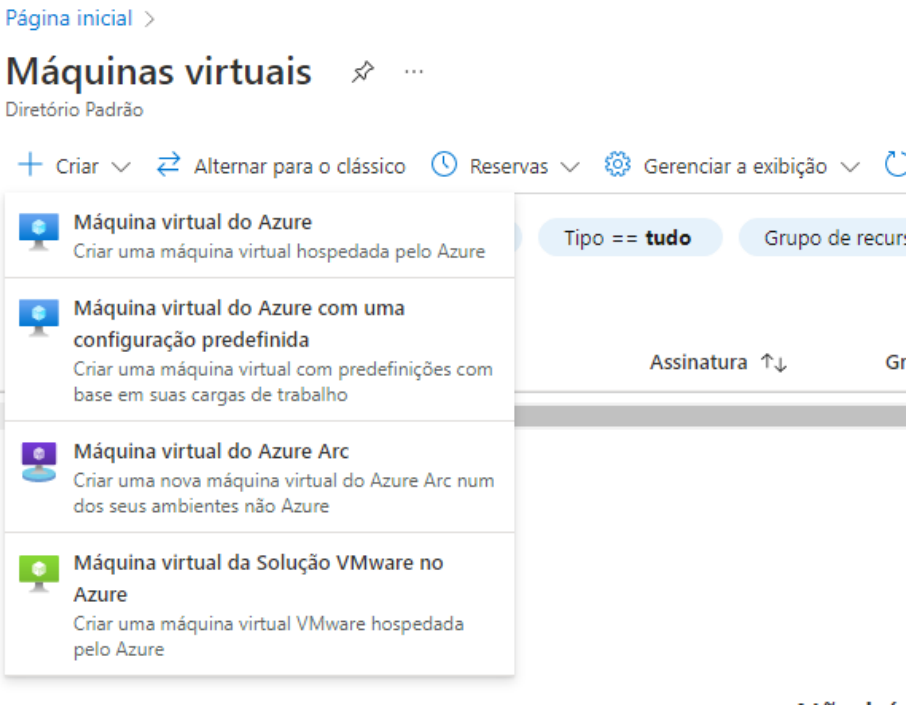



**Fonte:** autor

- **Criando uma Máquina Virtual com OpenVPN**

Utilizando a plataforma de nuvem publica Azure, na página inicial criou-se um recurso de serviço na plataforma, onde foi habilitado uma máquina virtual. A Figura 1 apresenta o menu do azure para criar recursos na nuvem.

**Figura 2** – criar máquina virtual no Azure




**Fonte:** Portal Azure

- **Configurando Máquina Virtual**

A figura 2 mostra as configurações básicas utilizadas para criação da VM.

**Figura 3** – Configurações da VM

| | |
|---|---|
| Assinatura | Azure subscription 1 |
| Grupo de recursos | (novo) VPNserver_group |
| Nome da máquina virtual | VPNserver |
| Região | Brazil South |
| Opções de disponibilidade | Nenhuma redundância infraestrutura necessária |
| Tipo de segurança | Padrão |
| Imagem | OpenVPN Access Server 2.8.5 – Gen1 |
| Tamanho | Standard D2as v4 (2 vcpus, 8 GiB memória) |
| Tipo de Autenticação | Chave pública de SSH |
| Nome de usuário | vpnuser |
| Nome do par de chaves | vpnkey |
| Azure Spot | Não |

**Fonte:** Portal Azure

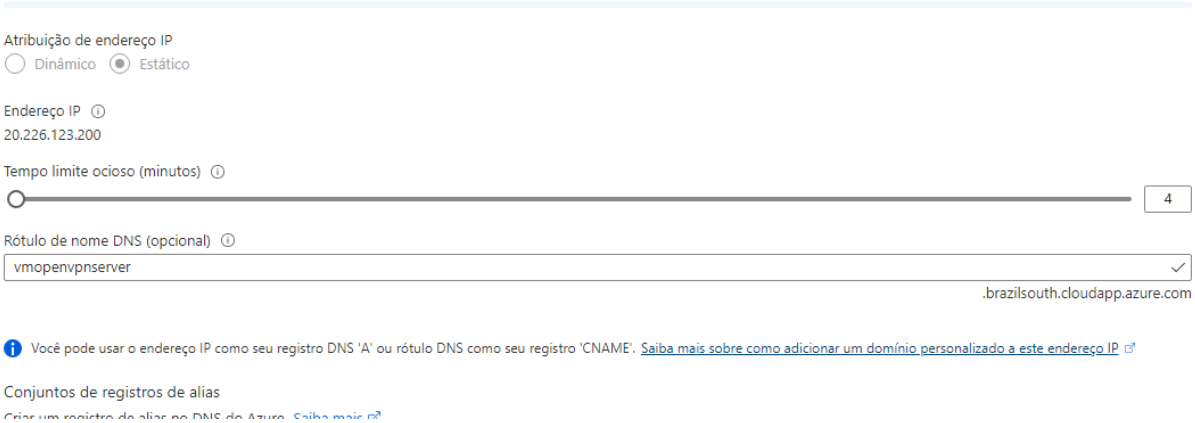
A escolha da região da máquina virtual é extremamente importante, pois este será o servidor VPN e a região onde ele está situado, isto implica diretamente na qualidade da conexão e o uso da VPN. Neste estudo, opta-se pela região do brasil, pois o intuito apenas propor a virtualização de servidor privado de VPN.

A nuvem publica Azure fornece na marketplace uma imagem pronta do software OpenVPN para a criação de máquinas virtuais que foi utilizada nesta pesquisa. Outas opções de configuração da máquina permaneceram os padrões da plataforma.

- **Definindo IP fixo**

Como padrão, o azure define um público para VM criada, e como utiliza-se autenticação com a vm via ssh, será necessário definir um ip fixo para esta autenticação e um rotulo DNS para facilitar a conexão ssh.

**Figura 4** – definindo IP fixo




**Fonte:** Portal Azure

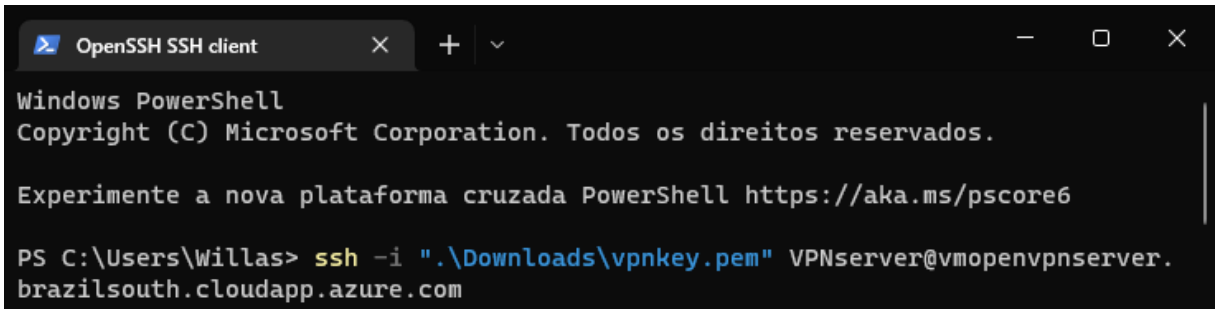
Também define um rotulo DNS para facilitar a conexão ssh.

- **Acessando a Máquina Virtual**

A figura 4 mostra como este acesso é feito via SSH no Windows Terminal. Primeiro SSH para indicar a conexão, depois o local da chave pública gerada e em seguida o usuário e o

IP da máquina, nesse caso também pode se utilizar o DNS configurado. Após aplicar o comando, já estou conectado ao servidor.

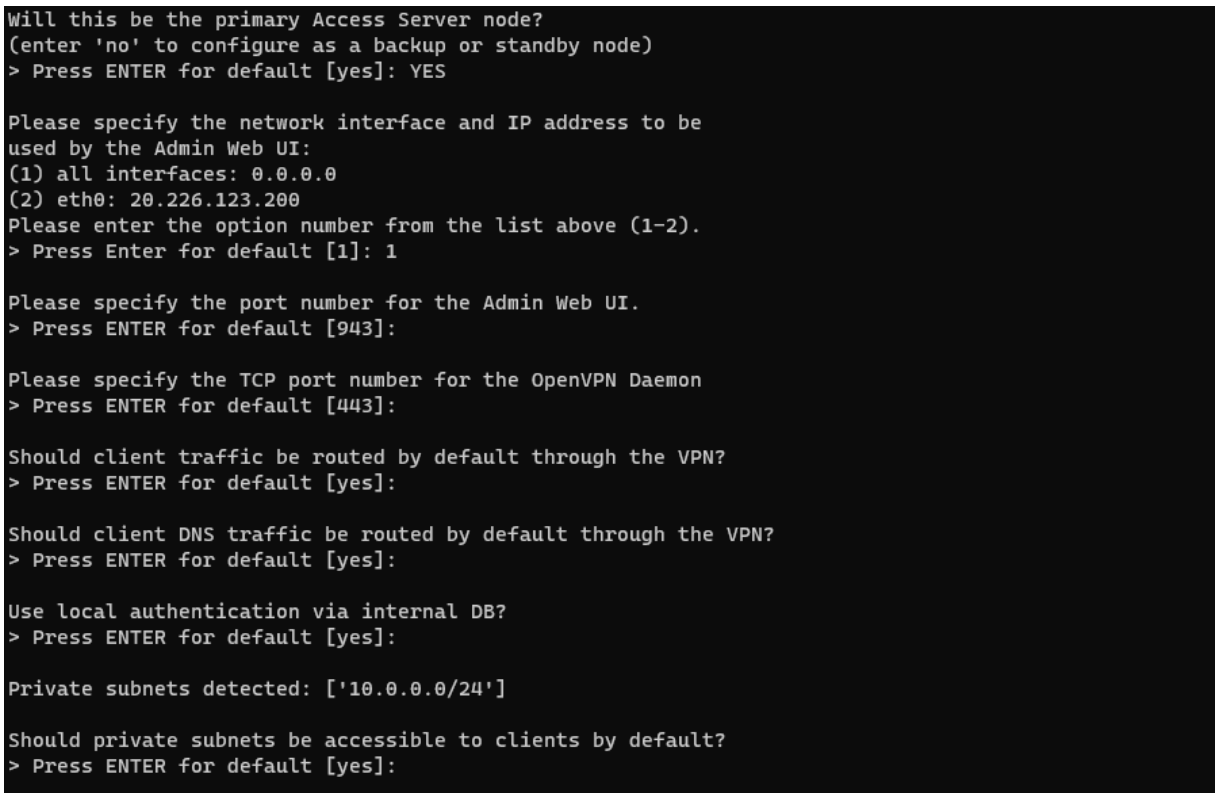
**Figura 5** – Acessando a VM




**Fonte:** Autor

Um script é executado na tela para as primeiras configurações do servidor. Primeiramente foi perguntado sobre as interfaces de rede a serem habilitadas, seleciona-se “1” para habilitar todas, as opções seguintes são definidas por padrão, apenas confirmo. Como mostra a figura 5.

**Figura 6** – Script Inicial do OpenVPN




**Fonte:** Autor

Agora é necessário definir uma senha para o usuário openVPN para seguir a configuração na web. Após isso, pode reiniciar a máquina para carregar as configurações que foram aplicadas.

**Figura 7** – Definição de Senha do Usuário

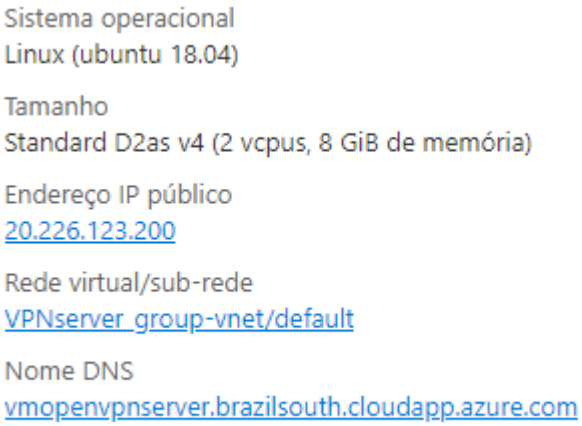
```
VPNserver@openvpnas2:~$ sudo passwd openvpn
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
VPNserver@openvpnas2:~$ sudo reboot
Connection to vmopenvpnserver.brazilsouth.cloudapp.azure.com closed by remote host.
Connection to vmopenvpnserver.brazilsouth.cloudapp.azure.com closed.
PS C:\Users\Willas>
```

**Fonte:** Autor

- **Acessando a Interface Web**

Para este passo utiliza-se o IP público ou endereço DNS da máquina virtual, seguido de "/admin" para poder fazer o login como administrador.

**Figura 8** – Informações da VM

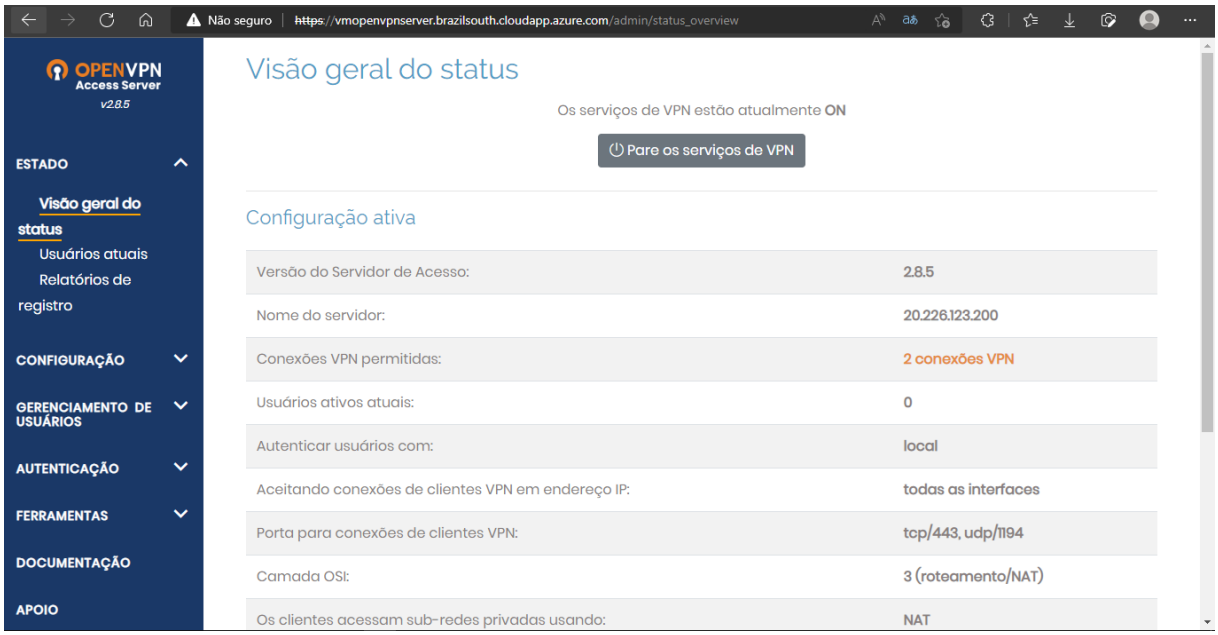



**Fonte:** Portal Azure

**Figura 9** – Tela de login


**Fonte:** Autor

**Figura 10** – Interface web do OpenVPN




**Fonte:** OpenVPN Access

As configurações padrão estão prontas para o uso, desde as configurações de máscara até roteamento do tráfego para o roteador VPN.

- **Autenticação Multifator**

O OpenVPN Server já vem com a funcionalidade para a autenticação com o google autenticador, basta habilitar no menu “autenticação” que entao será requisitado ao se conectar na VPN.

**Figura 11** – Autenticação multifator


**Fonte:** OpenVPN Access Server

A partir deste ponto, o servidor VPN já está funcionando.

- **Conectando cliente VPN**

Para conectar como cliente na VPN, retornamos a interface web do servidor para realizar o login de usuário e baixar o software cliente.

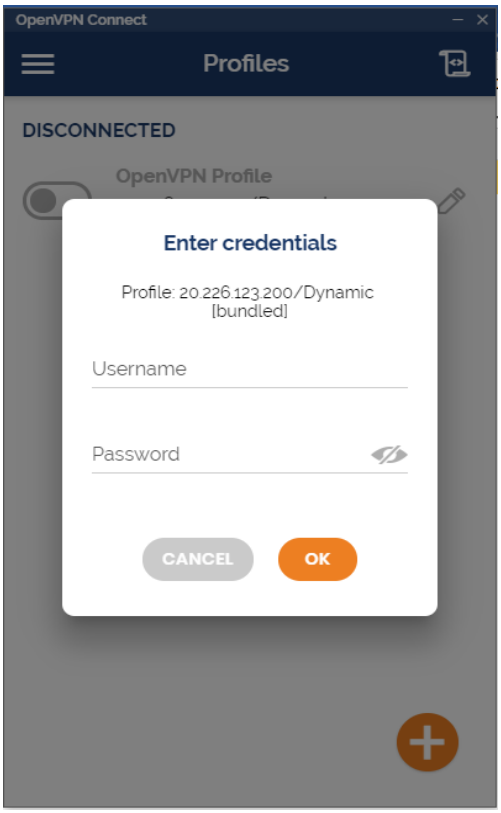
**Figura 12** – Download do software cliente


**Fonte:** OpenVPN access server

Assim pode-se baixar o software cliente multiplataforma para usar a VPN.

Com o software de acesso instalado, basta fazer o login na rede com as credenciais configuradas e habilitar a conexão com o servidor.

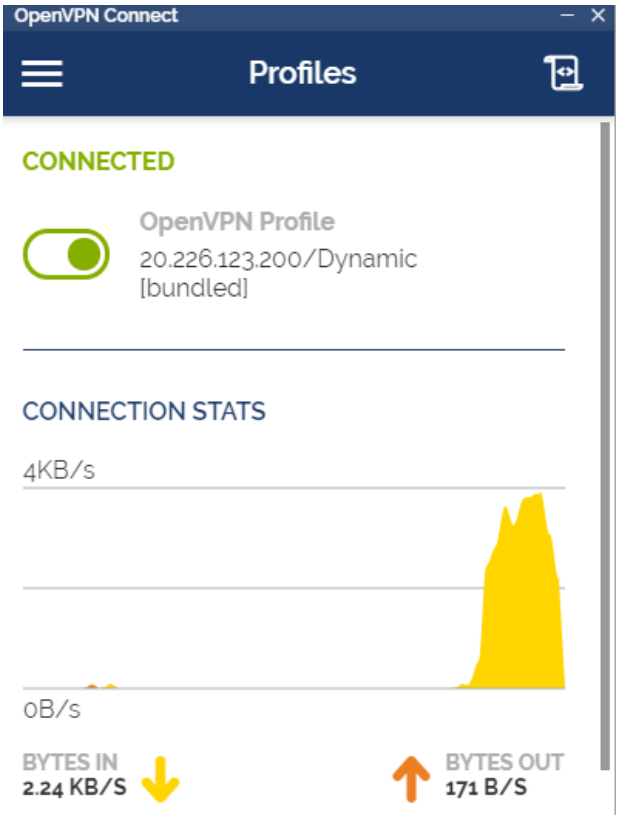
**Figura 13** – login




**Fonte:** OpenVPN connect

Agora já está conectado a VPN que que foi criada na nuvem, toda a comunicação do host com a internet está sendo mediada pelo servidor VPN. O servidor estabelece uma conexão segura através do túnel VPN por uma rede pública.

**Figura 14** – VPN conectada




**Fonte:** OpenVPN connect

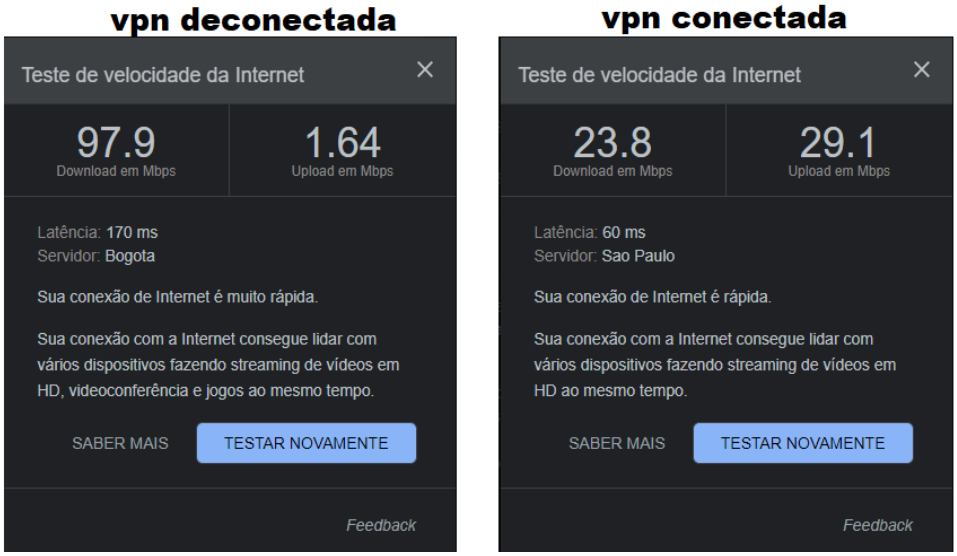
## ANÁLISE E DISCUSSÃO DOS RESULTADOS

A conexão das redes foi realizada com sucesso. Esta foi uma pesquisa para propor a utilização de uma VPN hospedada na nuvem para oferecer redução de custos e facilidade de acesso e configuração e conforme foi demostrado, pode ser realizada para fins tanto corporativos quanto para uso doméstico com segurança dos dados a serem transmitidos.

## ANÁLISE DA QUALIDADE DA CONEXÃO

Utilizando o teste de velocidade do google, estabelecendo um parâmetro para saber se a conexão com a VPN possui uma transmissão satisfatória sem perda na qualidade da conexão com a internet.  A figura 14 mostra um comparativo da velocidade antes e depois da conexão.

**Figura 15** – comparação da velocidade




**Fonte:** Google

## CONSIDERAÇÕES FINAIS

É possível concluir que a conexão com uma rede virtual privada abre muitas possibilidades para o uso.

Esta pesquisa demostrou que é possível criar e gerenciar um servidor VPN sem muitos recursos para que seu uso possa ser mais comum. Muitas pessoas utilizam VPNs de terceiros que podem expor o usuário a ameaças a privacidade da transmissão o dos seus dados. Com Este estudo é possível criar seu próprio servidor de rede privada para acesso remoto a rede, caso esteja longe ou para criptografia.

## REFERÊNCIAS BIBLIOGRÁFICAS

Algar Telecom. VPN: descubra por que ela é indispensável na sua empresa. Disponível em: https://blog.algartelecom.com.br/solucoes/vpn-descubra-por-que-ela-e-indispensavel-na-sua-empresa/. 2021

MOSNA, MORAES. Eduardo Mosna e Matheus de Moraes. Configuração de VPN site-to-site e client-to-site com OpenVPN e routerboard Microtik. Americana. 2020

SILVA, Lino Sarlo. Virtual Private Network . VPN: Aprenda a construir redes privadas virtuais em plataformas Linux e Windows. Edição 2. Novatec, 2005

SOEST, KUHNAST. Daniel Soest e Charly Kuhnast. Sem Necessidade de Mágica. Admin Magazine. 2011

PORTAL AZURE, 2022. Disponível em: https://portal.azure.com/ acesso em: 07/06/2022

GOOGLE, 2022. Disponivel em: https://www.google.com/ acesso em: 08/06/2022