UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

Marcelino Francisco Gomes das Chagas

Comparação de VPN e ZTNA: Uma Análise de Segurança e Desempenho em Ambientes Corporativo

Recife

2024

Marcelino Francisco Gomes das Chagas

Comparação de VPN e ZTNA: Uma Análise de Segurança e Desempenho em Ambientes Corporativo

Monografia apresentada ao Curso de Bacharelado em Ciências da Computação da Universidade Federal Rural de Pernambuco, como requisito parcial para obtenção do título de Bacharel em Ciências da Computação.

Universidade Federal Rural de Pernambuco – UFRPE

Departamento de Computação

Curso de Bacharelado em Ciências da Computação

Orientador: Robson Wagner Albuquerque de Medeiros

Recife

2024

Dados Internacionais de Catalogação na Publicação
Sistema Integrado de Bibliotecas da UFRPE
Bibliotecário(a): Ana Catarina Macêdo – CRB-4 1781

C427c Chagas, Marcelino Francisco Gomes das.
Comparação de VPN e ZTNA : uma análise de segurança e desempenho em ambientes corporativo / Marcelino Francisco Gomes das Chagas. – Recife, 2024.
46 f.; il.

Orientador(a): Robson Wagner Albuquerque de Medeiros.

Trabalho de Conclusão de Curso (Graduação) – Universidade Federal Rural de Pernambuco, Bacharelado em Ciência da Computação, Recife, BR-PE, 2024.

Inclui referências e apêndice(s).

1. Tecnologia da informação. 2. Extranets (Redes de computação). 3. Sistemas de recuperação da informação - Segurança. 4. Computação em nuvem 5. Provedores de serviços da Internet . I. Medeiros, Robson Wagner Albuquerque de, orient. II. Título

CDD 004

MINISTÉRIO DA EDUCAÇÃO E DO DESPORTO
UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO (UFRPE)
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

http://www.bcc.ufrpe.br

FICHA DE APROVAÇÃO DO TRABALHO DE CONCLUSÃO DE CURSO

Trabalho defendido por **MARCELINO FRANCISCO GOMES DAS CHAGAS** às 14h do dia 30 de setembro de 2024, na Universidade Federal Rural de Pernambuco, em Recife, no Auditório do Departamento de Computação, como requisito para conclusão do curso de Bacharelado em Ciência da Computação da Universidade Federal Rural de Pernambuco, intitulado "**Comparação de VPN e ZTNA: Uma Análise de Segurança e Desempenho em Ambientes Corporativo**", orientado por Robson Wagner Albuquerque de Medeiros e aprovado pela seguinte banca examinadora:

Robson Wagner Albuquerque de Medeiros
DC/UFRPE

Fernando Antônio Aires Lins
DC/UFRPE

Em memória do meu querido irmão Rafael Chagas. Este trabalho é dedicado a você, que, mesmo não estando mais fisicamente ao meu lado, continua presente em meu coração e em minhas lembranças.

Agradecimentos

Primeiramente a Deus, que me deu forças em todos os momentos para seguir em frente com as batalhas.

À minha esposa, Edla Marcela, por estar sempre ao meu lado na nossa jornada de vida e por todo o incentivo e suporte na minha jornada acadêmica, me motivando a cada passo do caminho.

Aos meus pais, Marcilio Chagas e Judite Silva, por serem meu porto seguro em todos os desafios da minha vida.

Ao meu amigo, Edilson Alves, que esteve comigo desde o primeiro dia da graduação, dividindo momentos de descontração.

A todos os professores da UFRPE que contribuíram para minha formação acadêmica, especialmente aqueles que me guiaram ao longo do caminho.

A todos os funcionários da UFRPE, em especial à Sandra Xavier, por todo apoio durante a graduação.

“A segurança não é um produto, é um processo.”
(Bruce Schneier)

Resumo

O avanço tecnológico constante e a rápida expansão das infraestruturas em provedores de nuvem pública têm gerado desafios significativos para as empresas, especialmente no que diz respeito à segurança da informação. As tradicionais medidas de segurança, como as Redes Privadas Virtuais (VPNs), que criam um túnel seguro para a transmissão de dados entre o usuário e a rede corporativa, nem sempre são adequadas para proteger os dados em ambientes de nuvem, resultando em uma necessidade crescente de reavaliação das estratégias de proteção. A pandemia do COVID-19 intensificou ainda mais essa demanda, à medida que as organizações se viram forçadas a adotar práticas de trabalho remoto em larga escala. Nesse cenário, a confiança nos dados finais tornou-se uma preocupação crítica, especialmente diante das limitações das soluções tradicionais de VPN. Em resposta a esses desafios, a Arquitetura de Confiança Zero (ZTA) e o Acesso à Rede com Confiança Zero (ZTNA) emergem como abordagens promissoras. ZTNA é uma tecnologia baseada nos princípios da ZTA que redefine o controle de acesso à rede, eliminando a confiança implícita em qualquer usuário ou dispositivo, independentemente de sua localização, e exigindo verificação contínua para cada tentativa de acesso. Essa abordagem oferece uma segurança mais granular a nível de rede e controle de acesso, além de ser adaptável em ambientes on-premise e na nuvem, protegendo os dados em ambientes corporativos distribuídos e em constante evolução. O objetivo deste trabalho é realizar uma análise comparativa das tecnologias de rede VPN e ZTNA, com ênfase na avaliação de segurança e desempenho. Serão examinadas as características de segurança oferecidas por cada tecnologia, incluindo autenticação, controle de acesso e criptografia, bem como o impacto dessas tecnologias no desempenho da rede em termos de latência, largura de banda e tempo de resposta. Através desta análise, busca-se identificar as vantagens e desvantagens de cada abordagem tecnológica, oferecendo insights valiosos para profissionais de TI e organizações na seleção e implementação da solução mais adequada às suas necessidades de segurança e desempenho em ambientes corporativos modernos.

Palavras-chave: Acesso à rede de confiança zero, Rede privada virtual, Arquitetura de confiança zero.

Abstract

Constant technological advances and the rapid expansion of infrastructures in public cloud providers have created significant challenges for companies, especially with regard to information security. Traditional security measures, such as Virtual Private Networks (VPNs), which create a secure tunnel for data transmission between the user and the corporate network, are not always adequate to protect data in cloud environments, resulting in a growing need to re-evaluate protection strategies. The COVID-19 pandemic has further intensified this demand, as organizations have been forced to adopt remote working practices on a large scale. In this scenario, trust in the final data has become a critical concern, especially given the limitations of traditional VPN solutions. In response to these challenges, Zero Trust Architecture (ZTA) and Zero Trust Network Access (ZTNA) have emerged as promising approaches. ZTNA is a technology based on the principles of ZTA that redefines network access control by eliminating implicit trust in any user or device, regardless of their location, and requiring continuous verification for every access attempt. This approach offers more granular security at the network and access control level, and is adaptable in on-premise and cloud environments, protecting data in distributed and constantly evolving corporate environments. The aim of this work is to carry out a comparative analysis of VPN and ZTNA network technologies, with an emphasis on evaluating security and performance. The security features offered by each technology will be examined, including authentication, access control and encryption, as well as the impact of these technologies on network performance in terms of latency, bandwidth and response time. Through this analysis, we aim to identify the advantages and disadvantages of each technological approach, offering valuable insights for IT professionals and organizations in selecting and implementing the solution best suited to their security and performance needs in modern corporate environments.

Keywords: Zero Trust Network Access, Virtual Private Network, Zero Trust Architecture.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

UDP	User Datagram Protocol
TCP	Transmission Control Protocol
VPN	Virtual Private Network
SSO	Single Sign-On
IaaS	Infrastructure as a Service
ZTA	Zero Trust Architecture
ZTNA	Zero Trust Network Access
IPSec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
MFA	Multi-Factor Authentication
SSL	Secure Sockets Layer
TLS	Transport Layer Security
LAN	Local Area Network
WAN	Wide Area Network
BYOD	Bring Your Own Device
IP	Internet Protocol
QoS	Quality of Service
EC2	Elastic Compute Cloud

Sumário

1 Introdução

O coronavírus causou um impacto gigantesco no mundo, afetando diversas áreas, como saúde, ensino e outros serviços. A transição urgente dos negócios, que geralmente levaria meses ou até mesmo anos, foi necessária à medida que as empresas precisam mudar suas operações para o ambiente remoto em resposta às medidas de isolamento social. Além da questão da sobrevivência, muitas empresas tiveram que inovar e experimentar novas formas de trabalhar, atender clientes e oferecer seus serviços (Forbes, 2020).

Essa rápida transição para o trabalho remoto trouxe também um desafio crítico: garantir a segurança das informações e das conexões remotas.

Durante este período, houve um aumento significativo na demanda por serviços em nuvem, como a Infraestrutura como Serviço (IaaS), oferecida por grandes empresas como Amazon, Microsoft, Alibaba, Google e Huawei. De acordo com dados do Gartner, esse segmento cresceu aproximadamente 40,7% em 2020 em comparação com o ano anterior, totalizando cerca de US$ 64,3 bilhões em movimentação financeira. Essas empresas representam coletivamente cerca de 80% do mercado, resultando em um crescimento substancial para todas elas (Olhar Digital, 2021).

Com a transformação digital acelerando o uso de serviços na nuvem no mundo corporativo, a expansão de diferentes ambientes, como multi-cloud, híbrido, público e privado, para gerenciamento também tem resultado em um aumento das ameaças cibernéticas. Essas ameaças aproveitam-se desse cenário na nuvem, utilizando esses serviços para alavancar várias etapas da *kill chain*, como ataques orquestrados e planejados, que podem ser executados por meio de ransomware, malware e outros tipos de ameaças. Isso amplia o perímetro de segurança que o ambiente corporativo deve manter, tanto para a infraestrutura dos serviços quanto para a conexão dos colaboradores, que também precisa ser mantida segura. Mundialmente, em 2021, foram registrados mais de 50% de ataques por semana a redes empresariais em comparação a 2020 (Security Leaders, 2020).

Durante a transição para o trabalho remoto, impulsionada pela pandemia, muitas empresas adotaram soluções de VPN (Virtual Private Network) para permitir que seus colaboradores acessassem a rede corporativa de forma segura. No entanto, ao contrário do modelo de segurança Zero Trust (ZT), que não confia automaticamente em nenhum usuário ou dispositivo, seja ele interno ou externo à rede, o acesso no Zero Trust é sempre verificado e controlado de forma contínua.

Apesar do aumento das menções ao conceito de *ZT* Zero Trust nos dias atuais,

o conceito de segurança foi inicialmente apresentado pelo Jericho Forum, um grupo de Chief Information Security Officers (CISOs) sediado no Reino Unido. Eles observaram o avanço da computação móvel e dos ambientes de nuvem, percebendo que os métodos tradicionais de acesso e autorização de dispositivos estavam se tornando inadequados, o que ampliava significativamente o perímetro de segurança que precisavam proteger (ACT-IAC, 2019).

Nesse cenário, a comparação entre a VPN tradicional e abordagens mais modernas, como o ZTNA, torna-se essencial para determinar qual solução oferece maior eficácia na proteção e na eficiência das operações corporativas.

A partir desse contexto, este trabalho tem como objetivo analisar e comparar as soluções de VPN e ZTNA, com foco em seus aspectos de segurança e desempenho no ambiente corporativo, a fim de identificar qual delas oferece maior proteção e eficiência para as organizações no cenário atual.

1.1 Problema da Pesquisa

Este trabalho tem como principal objetivo responder ao problema de pesquisa definido a seguir:

- Qual das duas tecnologias, VPN (Virtual Private Network) ou ZTNA (Zero Trust Network Access), proporciona o melhor desempenho, além de oferecer as características mais robustas de autenticação e segurança ?

1.2 Justificativa

A pandemia e o isolamento social impuseram desafios significativos às empresas, destacando especialmente a necessidade de garantir acesso eficiente e seguro às redes corporativas, uma tarefa complexa para os engenheiros de infraestrutura e redes. A transição para o trabalho remoto aumentou a demanda por soluções que ofereçam um equilíbrio entre eficiência e segurança no tráfego de informações, tornando esses aspectos cruciais para a continuidade dos negócios.

Tanto empresas quanto órgãos públicos, diante da urgência gerada pela situação, optaram por adotar a tecnologia VPN (Virtual Private Network) para permitir uma conexão entre os dispositivos dos colaboradores e a infraestrutura, tanto em ambientes públicos quanto privados. De acordo com uma pesquisa da Atlas VPN, o uso de VPN aumentou em 124% no uso de VPN durante o período de 8 a 22 de março de 2020.(Security Org, 2023)

Com o rápido aumento e adoção das tecnologias de VPN para permitir o acesso a ambientes e serviços de órgãos públicos ou empresas privadas, também surge a preocupação com outro fator crucial: a segurança da informação. Pois empresas e órgãos públicos ao redor do mundo ainda operam em cenários de segurança que tradicionalmente confiam em firewalls como principal barreira de proteção dentro de um perímetro, contudo não se leva em consideração os demais meios de acesso ao ambiente da empresa, como por exemplo a rede doméstica ou pública de onde se conectam os dispositivos de colaboradores (QAZI, 2022).

Por outro lado, a abordagem de confiança zero (Zero Trust Architecture - ZTA) fundamenta-se no princípio de que nenhum recurso pode ser automaticamente considerado seguro e, portanto, deve ser protegido. Em um ambiente empresarial complexo, composto por uma infinidade de microserviços, a proteção eficaz de cada ponto de acesso torna-se crucial (QAZI, 2022).

A implementação da arquitetura ZTA fortalece a defesa de todos os pontos de acesso críticos, incluindo os dispositivos dos colaboradores utilizados para acessar os ambientes, mitigando ameaças potenciais ao ambiente empresarial.

1.3 Objetivos

1.3.1 Objetivo geral

Realizar uma análise comparativa entre tecnologias de rede VPN da OpenVPN (OpenVPN, 2023) e ZTNA da Cloudflare (Cloudflare ZTNA, 2024), avaliando aspectos como desempenho de rede, características mais robustas de autenticação e segurança.

1.3.2 Objetivos específicos

1. Desenvolver um ambiente de teste para a avaliação das soluções VPN e ZTNA.
2. Identificar as vantagens e desvantagens de cada solução, destacando suas diferenças fundamentais de forma clara e acessível.
3. Avaliar o desempenho das soluções VPN e ZTNA por meio da coleta de métricas de latência, largura de banda e tempo de resposta, a fim de mensurar o impacto das tecnologias de forma precisa e objetiva.
4. Examinar como o ZTNA representa uma evolução das soluções VPN, destacando suas vantagens em termos de segurança, flexibilidade e gerenciamento de acesso em ambientes corporativos modernos.

2 Fundamentação Teórica

Para um melhor entendimento deste trabalho, será apresentado o conceito sobre as tecnologias utilizadas. Na seção 2.1 é abordado acerca de VPN e suas características. Na seção 2.2 uma introdução do conceito de Zero Trust e suas características. Na seção 2.3 uma análise comparativa entre as duas tecnologias VPN e Zero Trust, vantagens e desvantagens.

2.1 Redes Privadas Virtuais (VPNs)

Virtual Private Network (VPN) é uma rede de comunicação privada que opera dentro de uma rede de comunicação pública, como a Internet. As VPNs são uma parte crucial do protocolo de segurança em camadas, uma vez que criptografam o tráfego de Internet, ocultando a identidade online do usuário, tornando-as essenciais para a proteção de dados pessoais e corporativos em ambientes de rede pública (OpenVPN, 2023).

Na Figura 1 temos o exemplo de uma infraestrutura empresarial, onde os colaboradores possuem acesso ao banco de dados localmente, através dos pontos de acesso descritos na imagem, seja via switch ou wireless access point. Caso fosse necessário acessar o banco de dados fora dessa rede, não seria possível.

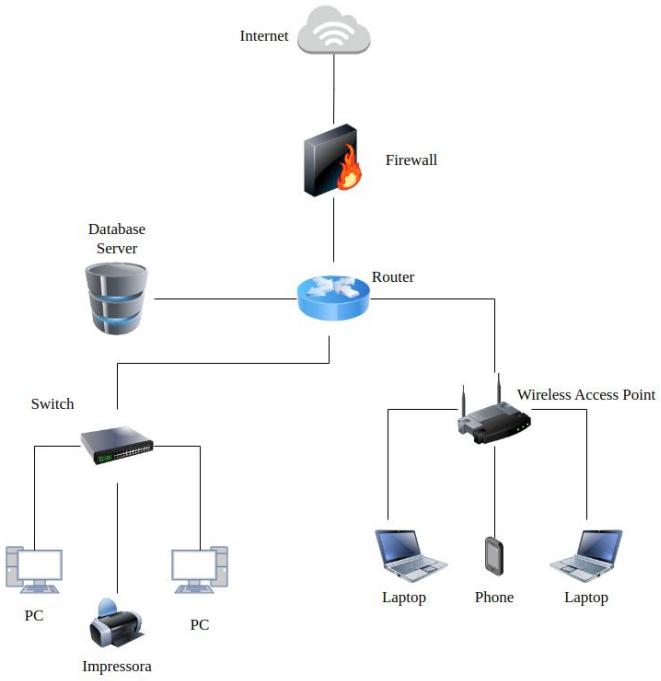

Figura 1 – Exemplo de Rede Empresarial

No cenário da Figura 2, o colaborador está trabalhando remotamente e precisa acessar a infraestrutura da empresa para realizar suas atividades. Nesse caso, ele utiliza uma solução de VPN para criar um túnel seguro até o ambiente da empresa, permitindo que ele acesse a infraestrutura da empresa de forma remota(OpenVPN, 2023).

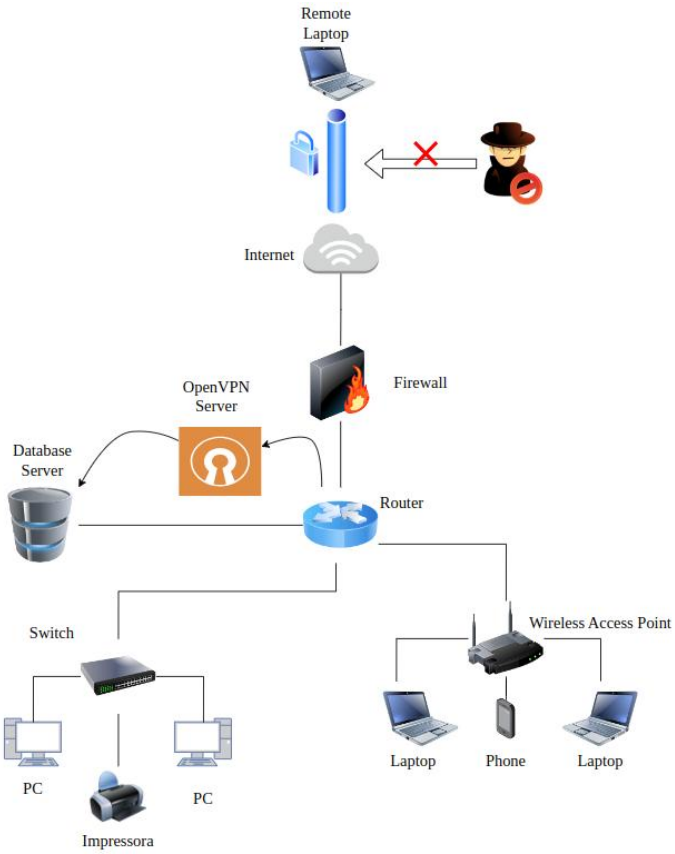

Figura 2 – Exemplo de Rede Empresarial com VPN

2.1.1 Tipos de VPN

Existem diversos tipos de soluções de VPN disponíveis no mercado. Neste trabalho, discutiremos brevemente algumas dessas soluções.

2.1.1.1 SSL (Secure Sockets Layer) VPN

Esse tipo de VPN utiliza uma camada de soquete seguro (SSL VPN), que garante aos usuários acesso à rede da organização, aos sistemas internos, às pastas compartilhadas e a outros serviços através de um navegador Web, sem a necessidade de instalar e configurar um software especializado no equipamento. As VPNs SSL oferecem uma conexão criptografada segura entre os dispositivos, independentemente do local de acesso à rede que o usuário está utilizando, seja em uma conexão de Internet pública ou em outra rede segura.

Com a segurança na camada de transporte TLS, todo o tráfego entre o navegador web e o servidor ou dispositivo SSL VPN é criptografado com o protocolo SSL VPN, garantindo uma maior segurança para o usuário. A SSL VPN prioriza o uso do protocolo criptográfico mais recente e atualizado instalado no equipamento, evitando o uso de protocolos desatualizados. Sempre que houver uma atualização do sistema operacional ou do navegador, a versão mais recente do protocolo será atualizada juntamente com ele (FORTINET SSL VPN, 2024).

1. **SSL Portal VPN**

   Neste tipo de SSL VPN, o usuário basicamente acessa um determinado endereço web e insere suas credenciais para iniciar uma conexão segura. Isso permite que o usuário tenha acesso aos serviços e aplicações da rede privada da empresa.

2. **SSL Tunnel VPN**

   A SSL Tunnel VPN, diferente do SSL Portal VPN, pode exigir aplicativos adicionais instalados no navegador do usuário (Add-ons), pois o túnel SSL VPN irá permitir acesso a serviços de rede com segurança, que não são apenas baseados na web por meio de um túnel que está sob SSL, onde determinados softwares ou redes exclusivas não podem ser acessados diretamente pela Internet.

2.1.1.2 Site-to-Site VPN

Uma VPN site-to-site é uma rede privada entre intranets, conectando várias redes LAN a uma WAN em uma organização. Isso permite que os usuários dessas redes seguras acessem recursos mutuamente. Esse tipo de VPN é comumente utilizado em empresas de grande porte, permitindo a conexão de diversos departamentos em várias regiões (Kaspersky, 2023).

1. **Intranet-based Site-to-Site**

   A VPN *intranet site-to-site* é utilizada para conectar várias redes (LAN) de uma mesma empresa, formando uma única rede (WAN) e combinando os recursos de cada escritório de forma segura.

2. **Extranet-based Site-to-Site**

   A VPN *extranet site-to-site* é utilizada para interligar duas ou mais empresas diferentes, visando compartilhar alguns recursos, mantendo alguns outros privados.

2.1.1.3 Remote Access VPN

Neste tipo de VPN, conhecido também como Cliente VPN, os usuários precisam ter um cliente VPN instalado e devidamente configurado em seus equipamentos. Após

a configuração, o funcionário terá acesso remoto à infraestrutura da empresa, podendo acessar serviços, softwares e outros recursos por meio de um túnel criptografado. E a partir deste tipo de VPN que iremos comparar com a solução de ZTNA.

2.1.2 Vantagens

O uso da tecnologia de VPN, traz consigo algumas vantagens, na utilização dessa tecnologia num ambiente corporativo:

1. A privacidade das informações é fortalecida com o uso de uma VPN, que traz consigo uma maior segurança através de diversos tipos de criptografia, os quais podem variar de acordo com a solução de VPN utilizada, evitando a interceptação de dados por parte de hackers.

2. Maior flexibilidade, pois permite que os usuários possam utilizar redes públicas ou privadas de qualquer local, para se comunicar com a infraestrutura da empresa, e assim acessar seus serviços.

3. Redução de custos ao optar por servidores de VPN em nuvem, em um ambiente corporativo, utilizar um servidor de VPN local implica custos adicionais, como expansão de banda para suportar mais conexões, despesas com manutenção e atualização de hardware, além da necessidade de garantir alta disponibilidade do servidor. com uma solução em nuvem, esses custos extras são evitados.

2.1.3 Desvantagem

Contudo podemos analisar algumas desvantagem que a tecnologia de VPN pode trazer a um ambiente corporativo:

1. Redução na velocidade de conexão, pois independente da velocidade de conexão do cliente, a velocidade de saída será determinada a partir do servidor de VPN.

2. A ausência de políticas rígidas de autenticação baseadas em identidade e contexto nas VPNs é uma desvantagem, pois o vazamento dessas credenciais pode conceder acessos não autorizados com mais facilidade. Isso torna mais difícil detectar comportamentos suspeitos na infraestrutura.

2.2 Zero Trust

O conceito de Zero Trust apesar de ser bastante popular nos dias atuais, começou a ganhar força entre 2009 e 2010, atraves de um analista da Forrest Research o

John Kindervag (Kindervag John, 2024).

O Zero Trust trata-se modelo de segurança que parte do principio de confiança zero, ou seja, nenhum usuário é confiável, onde é necessário uma verificação de identidade rigorosa para todos os usuários, que tentam acessar os recursos de uma rede privada, independentemente se os usuários estão dentro ou fora do perímetro da rede da empresa. A Figura 3 mostra que são exigidos uma ou mais meios de autenticação para que o usuário se conecte à rede corporativa, numa arquitetura Zero Trust. Esses meios de autenticação podem incluir sistemas de gerenciamento de identidade e acesso (IAM), o número de série do equipamento, aplicativos de segurança como autenticadores de múltiplos fatores (MFA), além de verificações de conformidade do dispositivo.

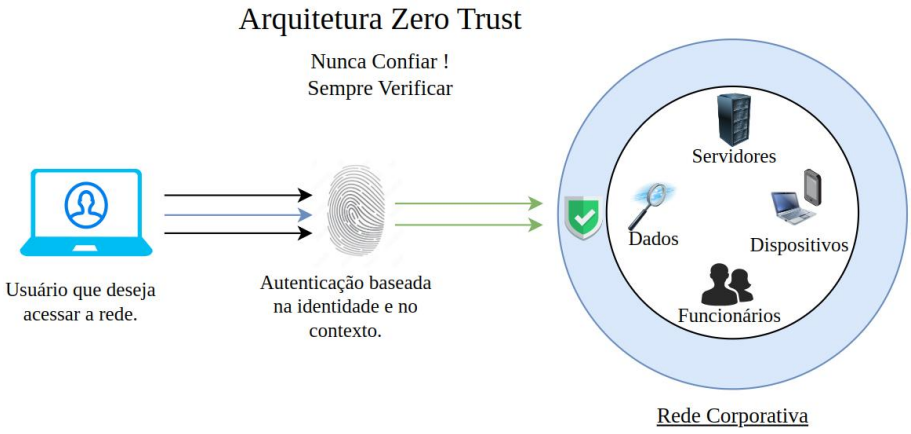

Figura 3 – Exemplo de Cenário Zero Trust

No modelo de Zero Trust, na parte de verificação de identidade, podem ser configurados um ou mais meios de verificação em conjunto, como tecnologias de IDP, dispositivos de MFA ou até mesmo contextos como endereço IP, validação de agentes instalados no equipamento, localização do acesso, número de série do equipamento, dentre diversos outros.

2.3 Comparação entre VPN e ZTNA

As tecnologias de ZTNA e VPN possuem o mesmo objetivo, que é o de proteger os dados e garantir uma comunicação segura no acesso remoto a redes e recursos corporativos. Contudo a tecnologia de VPN comparada ao ZTNA possuem diversas limitações (Check Point, 2024). Sendo elas:

1. Não possui um suporte adequado para dispositivos BYOD: Estes dispositivos podem não estar em conformidade com as políticas de segurança e não ter os endpoints devidamente instalados. Isso torna o equipamento não gerenciável,

permitindo que esses dispositivos acessem recursos corporativos, o que pode trazer malwares ou diversas outras ameaças cibernéticas para a rede corporativa.

2. Não oferece uma segurança adequada: Após a conexão, o usuário obtém acesso ao grupo de recursos ao qual está autorizado, o que ainda pode permitir que invasores se movam lateralmente dentro desse ambiente. Isso significa que, a partir do ponto de conexão, eles podem explorar vulnerabilidades presentes na rede corporativa, aumentando o risco de comprometimento de outros sistemas.

3. Não oferece um controle de acesso a nível de rede: após a conexão via VPN, o usuário obtém acesso excessivamente permissivo à rede corporativa, podendo acessar serviços e/ou aplicações. Mesmo sem as credenciais necessárias, ele consegue visualizar os serviços dentro da rede corporativa.

No ZTNA, cuja premissa é a de zero confiança, se utiliza-se o principio do menor privilégio, concedendo acesso ao mínimo de permissões possíveis para o usuários. Trazendo assim diversos benefícios, sendo eles:

1. Oferece uma gestão de acesso mais granular a nível de aplicativo. Ou seja, torna-se possível criar níveis de acesso desde o aplicativo até a consulta de ambiente, entre outros.

2. Com o ZTNA, toda a infraestrutura da empresa fica oculta. Em conjunto com os níveis de acesso concedidos ao usuário, isso permite que ele tenha acesso apenas ao que realmente precisa.

3. Em uma estrutura de ZTNA, a movimentação lateral na rede é dificultada, tornando ataques cibernéticos mais desafiadores devido às políticas de acesso do usuário-alvo.

4. Dependendo da solução de ZTNA adotada, ela fornece um controle de acesso rigoroso. Equipamentos que estejam na mesma rede não conseguem enxergar o host com ZTNA. Além disso, o controle de redes de máquinas virtuais, contêineres e outras soluções de rede instaladas no host não permite comunicação entre si, garantindo assim maior segurança.

3 Trabalhos Relacionados

As referências utilizadas na construção deste trabalho foram obtidas de fontes como o Periódicos CAPES, os sites de fabricantes da solução digital e o portal IEEE, utilizando termos como ZTNA (Zero Trust Network Access), VPN e Performance VPN.

(QAZI, 2022) discute a mudança das medidas tradicionais de segurança para a arquitetura de confiança zero (ZTA), destacando a importância de adaptar os princípios da ZTA às redes para proteger dados e ativos críticos, além de implementar soluções de software que garantam acesso remoto seguro. Este estudo é importante para a esta pesquisa, pois fornece uma base sobre como a ZTA pode substituir as VPNs tradicionais em um ambiente corporativo, tema central deste trabalho: a comparação entre VPN e ZTNA.

(ANTONIUK; PLECHAWSKA-WóJCIK, 2023) conduziram um estudo com o objetivo de verificar o desempenho da comunicação via Internet configurada com três protocolos VPN: Wireguard, OpenVPN e L2TP/IPSec. Para os testes de desempenho, foram utilizadas três ferramentas: o comando ping, Speedtest-cli e Iperf3. Este estudo foi utilizado como base para a escolha da metodologia e das ferramentas empregadas na análise de eficiência do ZTNA em comparação com a VPN no contexto corporativo, permitindo uma avaliação crítica das vantagens e desvantagens de cada solução em termos de desempenho.

(IORDACHE; DRAGOMIR; MARIAN, 2022) exploram a introdução da autenticação multifator (MFA) como uma maneira de aprimorar a cibersegurança em instituições públicas. Eles argumentam que a implementação do MFA, em conjunto com uma arquitetura de Confiança Zero (ZTA), proporcionaria uma abordagem mais granular à segurança de rede e de dados. Este trabalho destaca a importância da utilização de MFA como um componente complementar ao ZTNA, aumentando a segurança de acesso num ambiente corporativo.

(ESTRI JH; DEWIUMAR RUSYDI; RIADI IMAM, 2019) trata-se de um estudo que ressalta a eficácia da Cloudflare como uma solução de proteção contra ataques cibernéticos, como *DDOS* e outras ameaças. A Cloudflare não apenas otima a entrega de dados, mas também bloqueia ameaças e limita *bots*, resultando em uma melhoria significativa na velocidade e desempenho do site.

No trabalho (QU; LI; DANG, 2012), foi realizado um estudo de caso que analisa o desempenho da solução OpenVPN em dispositivos Android, considerando parâmetros como protocolo, criptografia e compactação. Os resultados indicam que a compactação de dados impacta a taxa de transferência, enquanto o tempo de ida e volta varia

conforme o protocolo de transporte utilizado.

O estado da arte atual demonstra que, embora a VPN tenha sido amplamente utilizada como solução de acesso remoto por muitos anos, suas limitações de segurança, como a possibilidade de movimentação lateral e o acesso amplo à rede, a tornam menos eficaz em cenários onde a granularidade e a segurança são prioritárias. Em contrapartida, o ZTNA surge como uma alternativa mais robusta, oferecendo um controle de acesso mais refinado e baseado em princípios de confiança zero, limitando os riscos associados ao acesso indevido. No entanto, questões de desempenho da solução do ZTNA ainda são áreas de interesse que exigem maior exploração.

Este trabalho busca realizar uma análise comparativa entre essas duas abordagens, VPN OpenVPN e ZTNA Cloudflare, com foco em suas implicações de segurança e desempenho em ambientes corporativos, visando preencher lacunas no entendimento de suas melhores aplicações.

4 Metodologia

A metodologia deste estudo envolve a criação de um ambiente de teste para a avaliação das soluções de VPN e ZTNA, utilizando a OpenVPN e a solução ZTNA da Cloudflare como foco. Serão configurados cenários nos quais as métricas de desempenho, como latência, largura de banda e quantidade de transferência de dados, serão coletadas para mensurar o impacto dessas tecnologias.

A análise também incluirá uma comparação das características de autenticação e segurança de cada solução, com o objetivo de identificar suas vantagens e desvantagens. Além disso, será apresentada a maneira como o ZTNA pode representar uma evolução em relação às VPNs tradicionais, destacando sua flexibilidade, segurança e gerenciamento de acesso em ambientes corporativos.

4.1 Experimento

Para a experimentação deste trabalho, visando uma análise comparativa entre a as tecnologias de OpenVPN (VPN) e Cloudflare (ZTNA), foi construído um cenário para teste para cada solução. As métricas selecionadas para a avaliação incluem largura de banda(bit rate), transferência de dados e latência.

1. **Largura de banda (bit rate)** é utilizado para avalia a capacidade de transmissão de dados em cada tecnologia.
2. **Transferência de Dados** é utilizado para mensurar a eficiência e a capacidade de cada solução em lidar com volume de tráfego.
3. **Latência** para determinar o tempo que os pacotes de dados levam para percorrer a rede, esse dado impacta diretamente a experiência do usuário.

Para obter as métricas necessárias, foi utilizada a ferramenta iPerf3 (Iperf3, 2024), que coleta informações sobre largura de banda e transferência de dados, essa ferramenta também foi utilizada no estudo (ANTONIUK; PLECHAWSKA-WóJCIK, 2023). Essa ferramenta foi aplicada em ambas as soluções: ZTNA e VPN. Além disso, a ferramenta Ping Monitor foi utilizada para medir a latência entre o dispositivo móvel e o servidor do ambiente corporativo. A OpenVPN Connect foi empregada para conectar tanto o dispositivo móvel quanto a solução desktop. Para o desktop, utilizou-se o Cloudflare WARP para se conectar ao ambiente, e no dispositivo móvel, o software 1.1.1.1 (Cloudflare Zero Trust).

4.1.1 Ambiente

Neste estudo, o ambiente foi construído utilizando a nuvem da AWS, especificamente o serviço EC2, para implementar ambas as soluções: OpenVPN e ZTNA da Cloudflare. Cenários foram configurados para refletir condições reais de uso em um ambiente corporativo.

4.1.2 OpenVPN (VPN)

Para a realização dos experimentos e testes necessários nesta seção do trabalho, foi utilizado o serviço de Elastic Compute Cloud (EC2) da Amazon Web Services (AWS). O EC2 possuí diversas características, contudo foi escolhido devido a sua flexibilidade e criação de IP pública (Elastic IP), para simular um ambiente corporativo. A Tabela 1 exibe as configurações da instância do OpenVPN Server criada na AWS:

Tabela 1 – Ambiente do OpenVPN Server

Região	**Arquitetura**	**Tipo**
N. Virgina (us-east-1)	x86_64	t2.micro

A instância de Application também foi criada na AWS via serviço EC2, representando uma máquina de onde será executado a ferramenta iPerf3, com as respectivas configurações descritas na Tabela 2:

Tabela 2 – Ambiente do Application Server

Região	**Arquitetura**	**Tipo**
N. Virgina (us-east-1)	x86_64	t2.micro

A Tabela 3 descreve as configurações do equipamento utilizado para simular o cliente OpenVPN (Desktop):

Tabela 3 – Configurações do Hardware

Memoria	**Processador**	**Sistema Operacional**
16,0 GB	AMD Ryzen 7 1700 2,50GHz	Windows 10

A Tabela 4 descreve as configurações do equipamento utilizado para rodar a aplicação OpenVPN Connect, que simula o cliente OpenVPN em um smartphone:

Tabela 4 – Configurações do Smartphone

Memoria	Processador	Sistema Operacional
12,0 GB	MediaTek Helio G88	Xiaomi HyperOS

A infraestrutura fornecida pela AWS, permitiu que os testes fossem conduzidos de forma eficiente. A Figura 4 descreve visualmente a composição dos dispositivos numa rede corporativa e como ocorre a sua respectiva comunicação entre eles:

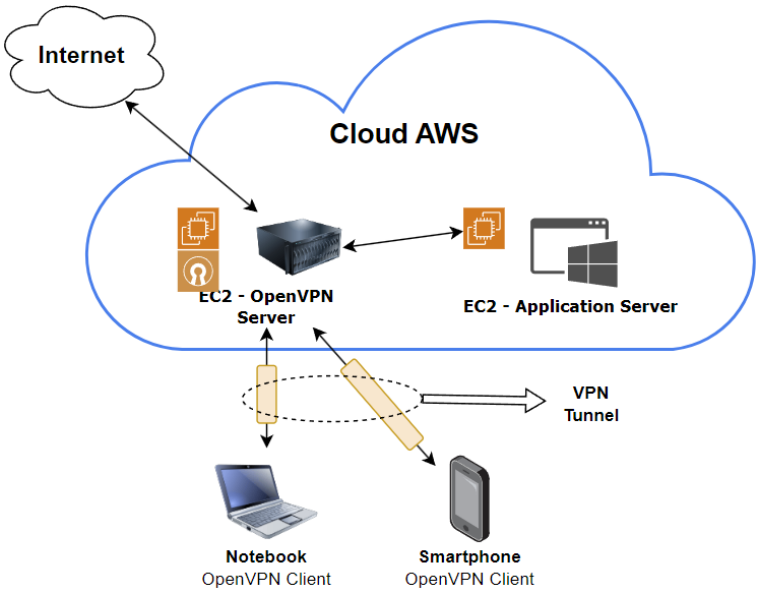

Figura 4 – Ambiente de Solução OpenVPN

4.1.3 Cloudflare (ZTNA)

Na solução da Cloudflare (ZTNA) para realização dos experimentos e testes necessários foi utilizado o ambiente gratuito da Cloudflare (Price ZT, 2024). Além disso, o serviço Elastic Compute Cloud (EC2) da Amazon Web Services (AWS) foi empregado devido à sua flexibilidade e à possibilidade de criação de IP público (Elastic IP),permitindo a simulação de um ambiente corporativo. Onde foi criada uma instância permitindo a utilização como tunnel de saida para a internet. A Tabela 5 descreve as configurações da instância EC2 do Tunnel Cloudflare.

Tabela 5 – Ambiente de Tunnel Cloudflare

Região	Arquitetura	Tipo
N. Virgina (us-east-1)	x86_64	t2.micro

A Tabela 6 apresenta as configurações da instância EC2 utilizada como Application Server:

Tabela 6 – Ambiente do Application Server

Região	**Arquitetura**	**Tipo**
N. Virgina (us-east-1)	x86_64	t2.micro

A Tabela 7 apresenta as configurações do hardware de desktop utilizado no nosso cenário para simular o cliente que usa a solução de ZTNA da Cloudflare para se comunicar com a rede corporativa.

Tabela 7 – Configurações do Hardware

Memoria	**Processador**	**Sistema Operacional**
16,0 GB	AMD Ryzen 7 1700 2,50GHz	Windows 10

A Tabela 8 apresenta as configurações do hardware de smartphone utilizado no nosso cenário para simular o cliente que usa a solução de ZTNA da Cloudflare para se comunicar com a rede corporativa:

Tabela 8 – Configurações do Smartphone

Memoria	**Processador**	**Sistema Operacional**
12,0 GB	MediaTek Helio G88	Xiaomi HyperOS

A infraestrutura fornecida pela Cloudflare permite a integração com diversas outras tecnologias de nuvens públicas, além de suportar a integração com várias soluções existentes no mercado.

A Figura 5 apresenta o cenário construído em conjunto com a infraestrutura da AWS, implementando a solução de ZTNA da Cloudflare, oferecendo uma visão do ambiente corporativo.

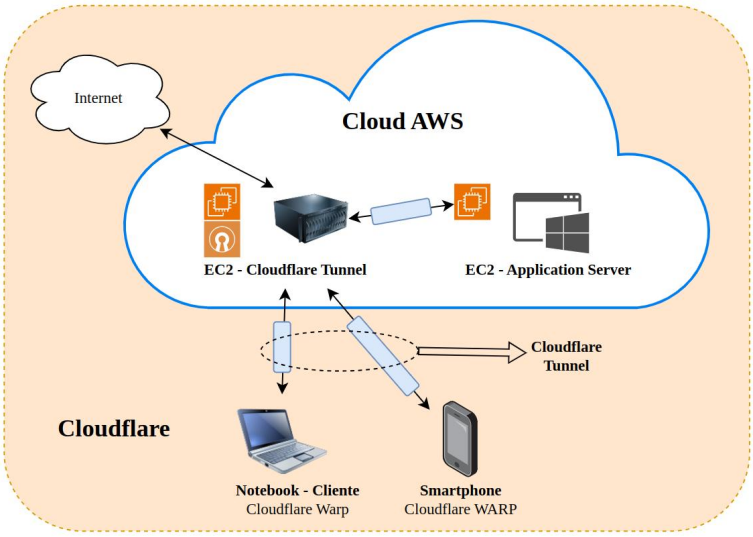

Figura 5 – Ambiente de Solução Cloudflare ZTNA

5 Resultados

Neste capítulo, apresentamos os resultados dos testes realizados no capítulo anterior, separados por cada solução: OpenVPN (VPN) e Cloudflare (ZTNA).

5.1 OpenVPN (VPN)

Na solução de OpenVPN, foi construído um cenário simulando um ambiente corporativo, conforme ilustrado na Figura 4, utilizando a infraestrutura da AWS. Para a realização do teste, utilizamos a ferramenta iPerf3, que é executada tanto no host com o cliente OpenVPN quanto no servidor de aplicação (Server Application).

Toda a execução desse teste ocorre através do túnel OpenVPN estabelecido entre o Cliente e Servidor de Aplicação, o que permite medir o desempenho da rede, fornecendo métricas como Bit Rate, Taxa de transferência, protocolos dentre outros parâmetros. Neste trabalho utilizamos as métricas de Transferência, Bit Rate e Protocolo. Transferência representa a quantidade total de dados transferidos entre o cliente e o servidor durante o teste. Bit Rate mostra a taxa de transferência de dados ao logon do tempo, refletindo assim a eficiência da conexão de rede durante o teste, permitindo avaliar a largura de banda disponível.

5.1.1 Cliente OpenVPN x Servidor de Aplicação

A Tabela 9 apresenta os resultados obtidos na máquina do cliente OpenVPN de teste, utilizando a ferramenta iPerf3 com o protocolo TCP. Neste teste, é possível observar a quantidade de dados transferidos por intervalo de tempo, o bit rate de cada intervalo e o protocolo utilizado. Todo ocorreu através da solução de OpenVPN.

Tabela 9 – Cliente OpenVPN X Servidor de Aplicação - TCP

Nome	**Intervalo (MBytes/seg)**	**Transferência**	**Bit Rate**	**Protocolo**
Desktop	0.00-1.01	1.62 MBytes	13.6 Mbits/sec	TCP
Desktop	1.01-2.02	2.25 MBytes	18.6 Mbits/sec	TCP
Desktop	2.02-3.00	2.12 MBytes	18.1 Mbits/sec	TCP
Desktop	3.00-4.02	2.38 MBytes	19.7 Mbits/sec	TCP
Desktop	4.02-5.00	2.25 MBytes	19.1 Mbits/sec	TCP
Desktop	5.00-6.01	2.25 MBytes	18.8 Mbits/sec	TCP
Desktop	6.01-7.01	2.25 MBytes	18.7 Mbits/sec	TCP
Desktop	7.01-8.02	2.25 MBytes	18.8 Mbits/sec	TCP
Desktop	8.02-9.01	2.25 MBytes	19.0 Mbits/sec	TCP
Desktop	9.01-10.04	2.12 MBytes	17.4 Mbits/sec	TCP

A Tabela 10 apresenta uma visão detalhada da quantidade de dados enviados e recebidos, a média de Bit Rate e o intervalo de tempo em megabytes por segundo (MB/s), obtidos pela ferramenta iPerf3, que estava sendo executada no cliente OpenVPN, através da conexão OpenVPN com o servidor de aplicação.

Tabela 10 – Cliente OpenVPN X Servidor de Aplicação - TCP

Status	**Intervalo (MBytes/seg)**	**Transferência (Soma)**	**Bit Rate (Média)**	**Protocolo**
Enviado	0.00-10.04	21.8 MBytes	18.2 Mbits/sec	TCP
Recebido	0.00-10.28	21.1 MBytes	17.2 Mbits/sec	TCP

Na Tabela 11 apresenta o resultado complemento do teste da ferramenta iPerf3 rodando no servidor de aplicação. Do servidor de aplicação para o cliente (Desktop) é possível observar a quantidade de dados transferidos por intervalo de tempo, o bit rate de cada intervalo e o protocolo utilizado. Todo ocorreu através da solução de OpenVPN.

Tabela 11 – Servidor de Aplicação X Cliente (Desktop) - TCP

Nome	**Intervalo (MBytes/seg)**	**Transferência**	**Bit Rate**	**Protocolo**
Servidor	0.00-1.01	384 KBytes	3.12 Mbits/sec	TCP
Servidor	1.01-2.01	2.25 MBytes	18.9 Mbits/sec	TCP
Servidor	2.01-3.01	2.12 MBytes	17.8 Mbits/sec	TCP
Servidor	3.01-4.01	2.38 MBytes	19.9 Mbits/sec	TCP
Servidor	4.01-5.01	2.25 MBytes	18.9 Mbits/sec	TCP
Servidor	5.01-6.01	2.25 MBytes	18.9 Mbits/sec	TCP
Servidor	6.01-7.01	2.25 MBytes	18.9 Mbits/sec	TCP
Servidor	7.01-8.01	2.25 MBytes	18.9 Mbits/sec	TCP
Servidor	8.01-9.01	2.12 MBytes	17.8 Mbits/sec	TCP
Servidor	10.01-10.28	640 KBytes	19.2 Mbits/sec	TCP

A Tabela 12 apresenta uma visão detalhada da quantidade de dados recebidos, a média de Bit Rate e o intervalo de tempo em megabytes por segundo (MB/s), obtidos pela ferramenta iPerf3, que estava sendo executada no Servidor de Aplicação, através da conexão OpenVPN com o cliente OpenVPN (Desktop).

Tabela 12 – Servidor de Aplicação X Cliente OpenVPN (Desktop)

Status	**Intervalo (MBytes/seg)**	**Transferência (Soma)**	**Bit Rate (Média)**	**Protocolo**
Recebido	0.00-10.20	21.1 MBytes	17.2 Mbits/sec	TCP

A Tabela 13 apresenta os resultados obtidos na máquina do cliente OpenVPN de teste, utilizando a ferramenta iPerf3 no protocolo UDP. No protocolo UDP não há garantia de que o pacote chegue corretamento ao destino (RFC 768 - UDP, 2024).

Neste teste, é possível observar a quantidade de dados transferidos por intervalo de tempo, o bit rate de cada intervalo e o protocolo utilizado. Todo ocorreu através da solução de OpenVPN.

Tabela 13 – Cliente OpenVPN (Desktop) X Servidor de Aplicação - UDP

Nome	Intervalo (MBytes/seg)	Transferência	Bit Rate	Protocolo
Desktop	0.00-1.01	126 KBytes	1.05 Mbits/sec	UDP
Desktop	1.01-2.02	128 KBytes	1.07 Mbits/sec	UDP
Desktop	2.02-3.00	131 KBytes	1.03 Mbits/sec	UDP
Desktop	3.00-4.02	126 KBytes	1.06 Mbits/sec	UDP
Desktop	4.02-5.00	129 KBytes	1.05 Mbits/sec	UDP
Desktop	5.00-6.01	128 KBytes	1.04 Mbits/sec	UDP
Desktop	6.01-7.01	129 KBytes	1.04 Mbits/sec	UDP
Desktop	7.01-8.02	127 KBytes	1.04 Mbits/sec	UDP
Desktop	8.02-9.01	127 KBytes	1.06 Mbits/sec	UDP
Desktop	9.01-10.03	131 KBytes	1.05 Mbits/sec	UDP

A Tabela 14 apresenta uma visão detalhada da quantidade de dados enviados, a média de Bit Rate e o intervalo de tempo em megabytes por segundo (MB/s), obtidos pela ferramenta iPerf3, que estava sendo executada no Servidor de Aplicação, através da conexão OpenVPN com o cliente OpenVPN (Desktop).

Tabela 14 – Servidor de Aplicação X Cliente OpenVPN (Desktop) - UDP

Nome	Intervalo	Transferência	Bit Rate	Protocolo
Servidor	0.00-1.01	384 KBytes	3.12 Mbits/sec	UDP
Servidor	1.01-2.01	2.25 MBytes	18.9 Mbits/sec	UDP
Servidor	2.01-3.01	2.12 MBytes	17.8 Mbits/sec	UDP
Servidor	3.01-4.01	2.38 MBytes	19.9 Mbits/sec	UDP
Servidor	4.01-5.01	2.25 MBytes	18.9 Mbits/sec	UDP
Servidor	5.01-6.01	2.25 MBytes	18.9 Mbits/sec	UDP
Servidor	6.01-7.01	2.25 MBytes	18.9 Mbits/sec	UDP
Servidor	7.01-8.01	2.25 MBytes	18.9 Mbits/sec	UDP
Servidor	8.01-9.01	2.12 MBytes	17.8 Mbits/sec	UDP
Servidor	8.01-9.01	2.12 MBytes	17.8 Mbits/sec	UDP
Servidor	10.01-10.28	640 KBytes	19.2 Mbits/sec	UDP

5.1.2 Cliente (Smartphone) x Servidor de Aplicação

Para avaliar o desempenho da rede via smartphone (Cliente) com as configurações 4, foi necessário o aplicativo OpenVPN Connect, para se conectar via VPN

OpenVPN.

Para realização do teste foi utilizado a aplicação Ping Monitor, onde foi obtido a latência da conexão e a qualidade de serviço (QoS). A Tabela 15 mostra um teste de 11 ping utilizando a aplicação Ping Monitor, via conexão OpenVPN.

Tabela 15 – Cliente OpenVPN (Smartphone) x Servidor de Aplicação

Horário	**Sequencia**	**Ping**
10:05:38 PM	1	108 ms
10:05:39 PM	2	108 ms
10:05:40 PM	3	107 ms
10:05:41 PM	4	109 ms
10:05:42 PM	5	108 ms
10:05:44 PM	6	108 ms
10:05:45 PM	7	108 ms
10:05:46 PM	8	108 ms
10:05:47 PM	9	108 ms
10:05:48 PM	10	108 ms
10:05:49 PM	11	107 ms

Assim, foi obtida uma média de ping de 108 ms na comunicação entre o dispositivo smartphone e o servidor de aplicação através da VPN OpenVPN.

5.1.3 Segurança

A solução de openvpn utiliza o protocolo de criptografia SSL (Secure Socket Layer), de forma à garantir que os dados compartilhados atraves da internet, permaneçam privados, da qual utiliza a criptografia AES-256 (OpenVPN - Whats is Openvpn, 2024). Além possuir diversos benefícios como:

1. Opção de escolha entre criptografia convencional baseada em chave estática ou criptografia de chave pública baseada em certificado.
2. A utilização de todos os recursos de criptografia, autenticação e certificação da biblioteca OpenSSL para proteger o tráfego da rede privada contra agentes mal-intencionados e provedores de Internet (ISPs) enquanto transita pela Internet.
3. Utilização dos recursos de autenticação, certificação e criptografia da biblioteca do OpenSSL dentre vários outros.

5.1.3.1 Controle de Acesso

A solução OpenVPN oferece suporte a controle de acesso, uma ferramenta essencial para a segurança. Isso permite gerenciar permissões de acesso para usuários ou grupos de usuários, restringindo seu acesso a determinados serviços ou servidores específicos (OpenVPN - Managing Access control, 2024). Os tipos de controle de acesso possuem três níveis: Global, Grupo e Usuário.

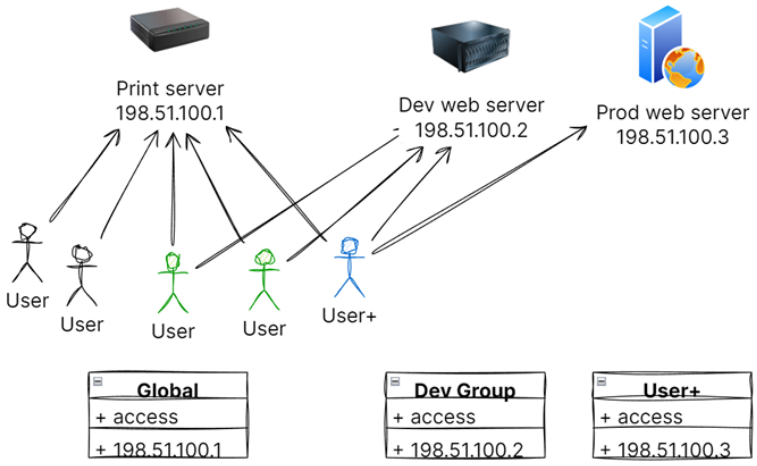

Figura 6 – Exemplo de Controle de Acesso OpenVPN

No entanto, o OpenVPN não realiza o controle de rede dos usuários, ou seja, ele não monitora nem impõe políticas específicas sobre o tráfego de rede gerado pelos usuários conectados ou que chega aos usuários.

A função do OpenVPN é essencialmente fornecer um canal seguro para a transmissão de dados, criptografando as comunicações entre o cliente e o servidor. Embora o OpenVPN se destaque na proteção dos dados em trânsito, para alcançar um nível de controle mais granular, como inspeção, filtragem, gerenciamento do tráfego de rede ou aplicação de políticas como QoS, é necessário integrar soluções complementares. Funcionalidades mais avançadas desse tipo são comumente encontradas em arquiteturas ZTNA.

5.2 Cloudflare (ZTNA)

Na solução de Clouflare ZTNA, foi construído um cenário simulando um ambiente corporativo, conforme ilustrado na Figura 5, utilizando a solução ZT gratuita da cloudflare, em conjunto com a infraestrutura da AWS. Para a realização do teste, foi utilizado a ferramenta iPerf3, que é executada tanto no host com o cliente ZTNA quanto no servidor de aplicação.

Toda a execução desse teste ocorre através da solução de ZTNA, da qual fornece a gestão de todo acesso e perímetro a todos dispositivos que ingressaram na

rede. E atráves da iPerf3 foi realizado a medição e desempenho da rede, fornecendo métricas como Bit Rate, Taxa de transferência, protocolos dentre outros parâmetros.

Neste trabalho foi utilizado as métricas de Transferência, Bit Rate e Protocolo. Sendo que a transferência representa a quantidade total de dados transferidos entre o cliente e o servidor durante o teste. Bit Rate mostra a taxa de transferência de dados ao logon do tempo, refletindo assim a eficiência da conexão de rede durante o teste, permitindo avaliar a largura de banda disponível.

5.2.1 Cliente ZTNA x Servidor de Aplicação

A tabela 16 apresenta o resultados obtidos na máquina do cliente ZTNA, utilizando a ferramenta iPerf3 com o protocolo TCP. Neste teste é possível observar a quantidade de dados transferidos por intervalo de tempo, o bit rate de cada intervalo e o protocolo utilizado. Todo o teste ocorreu através da ferramenta de ZTNA da cloudflare.

Tabela 16 – Cliente ZTNA (Desktop) X Servidor de Aplicação - TCP

Nome	**Intervalo (MBytes/seg)**	**Transferência**	**Bit Rate**	**Protocolo**
Desktop	0.00-1.01	4.00 MBytes	33.5 Mbits/sec	TCP
Desktop	1.01-2.02	4.12 MBytes	34.2 Mbits/sec	TCP
Desktop	2.02-3.00	4.12 MBytes	34.7 Mbits/sec	TCP
Desktop	3.00-4.02	3.75 MBytes	31.7 Mbits/sec	TCP
Desktop	4.02-5.00	4.50 MBytes	37.4 Mbits/sec	TCP
Desktop	5.00-6.01	5.25 MBytes	44.1 Mbits/sec	TCP
Desktop	6.01-7.01	4.75 MBytes	40.2 Mbits/sec	TCP
Desktop	7.01-8.02	5.25 MBytes	43.6 Mbits/sec	TCP
Desktop	8.02-9.01	4.00 MBytes	33.7 Mbits/sec	TCP
Desktop	9.01-10.04	4.50 MBytes	37.8 Mbits/sec	TCP

A Tabela 17 apresenta uma visão detalhada da quantidade de dados enviados e recebidos, a média de Bit Rate e o intervalo de tempo em megabytes por segundo (MB/s), obtidos pela ferramenta iPerf3, que foi executada a partir do cliente, através da conexão ZTNA com o servidor de aplicação.

Tabela 17 – Cliente ZTNA (Desktop) X Servidor de Aplicação - TCP

Status	Intervalo (MBytes/seg)	Transferência (Soma)	Bit Rate (Média)	Protocolo
Enviado	0.00-10.04	44.2 MBytes	37.1 Mbits/sec	TCP
Recebido	0.00-10.28	44.1 MBytes	36.6 Mbits/sec	TCP

A Tabela 18 apresenta os resultados obtidos na máquina do cliente ZTNA, utilizando a ferramenta iPerf3 no protocolo UDP. Nesse teste é possível observar a quantidade de dados transferidos por intervalo de tempo, o bit rate de cada intervalo e o protocolo utilizado. Todo o processo ocorreu através da solução de ZTNA.

Tabela 18 – Cliente ZTNA (Desktop) X Servidor de Aplicação - UDP

Nome	Intervalo (MBytes/seg)	Transferência	Bit Rate	Protocolo
Desktop	0.00-1.01	127 KBytes	1.03 Mbits/sec	UDP
Desktop	1.01-2.02	130 KBytes	1.05 Mbits/sec	UDP
Desktop	2.02-3.00	126 KBytes	1.04 Mbits/sec	UDP
Desktop	3.00-4.02	130 KBytes	1.06 Mbits/sec	UDP
Desktop	4.02-5.00	128 KBytes	1.05 Mbits/sec	UDP
Desktop	5.00-6.01	127 KBytes	1.05 Mbits/sec	UDP
Desktop	6.01-7.01	128 KBytes	1.05 Mbits/sec	UDP
Desktop	7.01-8.02	128 KBytes	1.05 Mbits/sec	UDP
Desktop	8.02-9.01	127 KBytes	1.05 Mbits/sec	UDP
Desktop	9.01-10.03	128 KBytes	1.06 Mbits/sec	UDP

Diferente do OpenVPN, no cloudflare ZTNA, todo acesso é criptografado de um para um, entre o dispositivo de um determinado usuário a um determinado servidor ou aplicação. Logo o ZTNA não expõe endereços de IP à rede, ou seja, toda a rede permanece invisível para os dispositivos conectados.

5.2.2 Cliente ZTNA (Smartphone) x Servidor de Aplicação

Para avaliar o desempenho da rede via smartphone (cliente) com as configurações 8, foi necessário o aplicativo 1.1.1.1(ZeroTrust), para se conectar a rede ZTNA.

Para realização do teste foi utilizado a aplicação Ping Monitor, onde foi obtido a latência da conexão e a qualidade de serviço (Qos). A Tabela 19 mostra um teste com 11 ping utilizando a aplicação Ping Monitor, via conexão ZTNA.

Tabela 19 – Cliente ZTNA (Smartphone) x Servidor de Aplicação

Horário	Sequencia	Ping
11:41:13 PM	1	127 ms
11:41:14 PM	2	111 ms
11:41:15 PM	3	133 ms
11:41:16 PM	4	122 ms
11:41:17 PM	5	120 ms
11:41:18 PM	6	113 ms
11:41:19 PM	7	113 ms
11:41:20 PM	8	114 ms
11:41:21 PM	9	120 ms
11:41:22 PM	10	111 ms
11:41:23 PM	11	126 ms

Assim, foi obtido uma média de ping de 120 ms na comunicação entre o dispositivo de smartphone e o servidor de aplicação através da VPN.

5.2.3 Segurança

A solução da ztna utiliza o protocolo de criptografia TLS, visando garantir uma maior segurança(Cloudflare ZTNA, 2024). A solução ZTNA possui diversos usos e benefícios tais como:

1. O ZTNA não expõe endereços IP à rede. Logo o resto da rede permanece invisível para os dispositivos conectados.
2. Diferente do openvpn o ztna possui fatores adicionais para controle de acesso, logo o usuário pode entrar em uma rede ou aplicativo, mas se o dispositivo não for confiável, o acesso será negado.
3. Possui integração com serviços de IdPs e plataformas de SSO.

5.2.3.1 Controle de Acesso

A solução Zero Trust oferece diversas opções para controle de acesso e segurança em ambientes corporativos. Diferentemente do OpenVPN, que fornece controle de acesso principalmente através de grupos, o Zero Trust inclui recursos como gateway seguro na web, acesso seguro a aplicativos SaaS, princípios de acesso mínimo, monitoramento de logs e acessos dos usuários, integração com soluções de IdP dentre

outros (ZTNA - Access control, 2024). A Figura 7 mostra o mecanismo de identidade, para acesso aos recursos da rede.

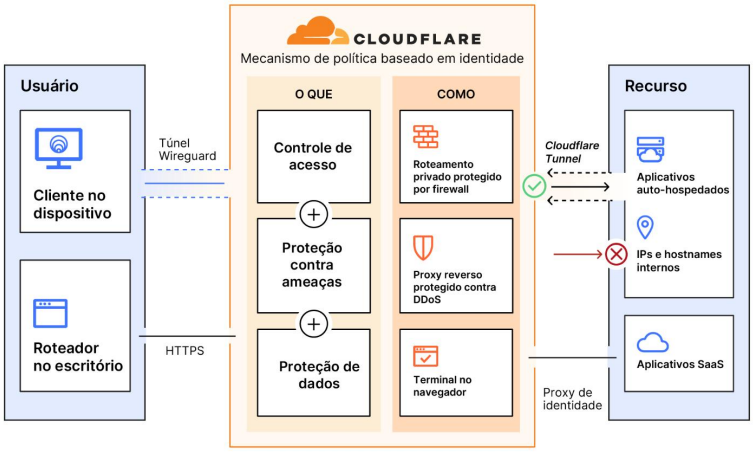

Figura 7 – Política Baseada em Identidade

Antes de acessar a rede ZTNA, é realizada uma verificação de identidade do usuário, que pode incluir múltiplas etapas, como a checagem do número de série da máquina, versão de aplicativos, ferramentas de segurança, entre outras. Além disso, no Cloudflare Access, é possível integrar com Multi-SSO para conceder acesso a diferentes grupos, usuários ou até mesmo aplicações. A lista de ferramentas de SSO que permitem integração inclui Active Directory, Keycloak, OneLogin, Okta, entre outras.

5.3 VPN x ZTNA

A Figura 8 mostra que a solução ZTNA possui um desempenho de transferência superior a solução OpenVPN, no teste realizado na ferramenta iPerf3 no protocolo TCP, de comunicação entre o desktop e o servidor de aplicação.

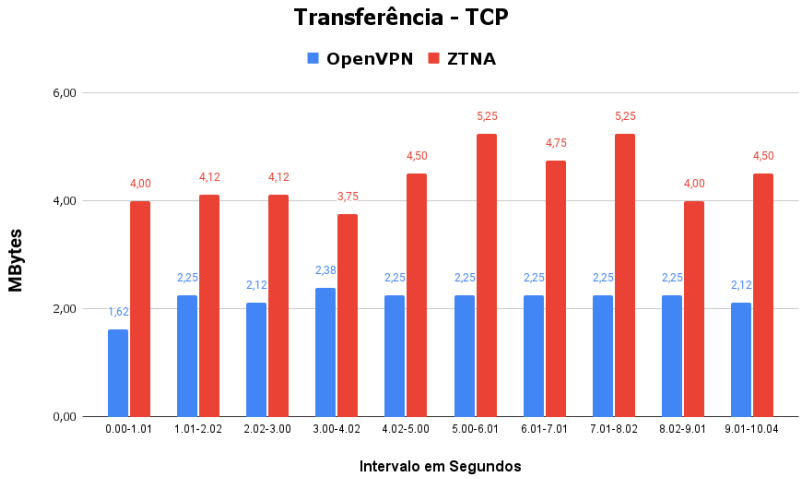

Figura 8 – Comparação de Transferência - TCP

Na Figura 9, mostra que a solução ZTNA, possui um desempenho de bit rate superior a solução OpenVPN, no teste realizado na ferramenta iPerf3 no protocolo TCP, de comunicação entre o desktop e o servidor de aplicação.

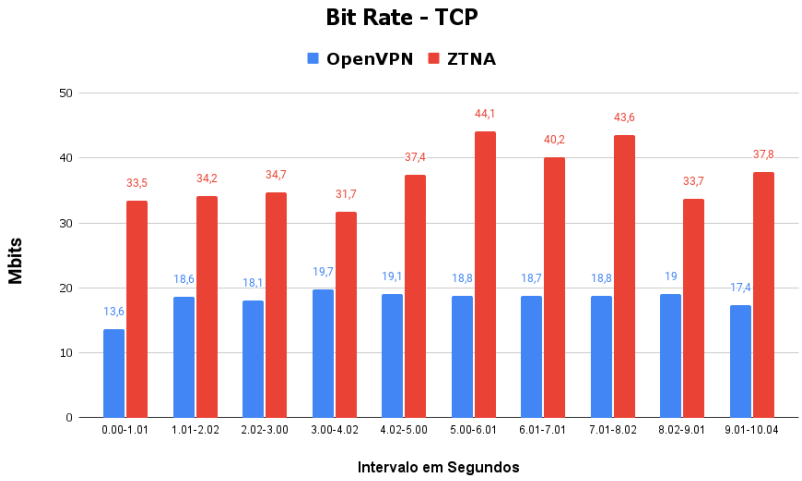

Figura 9 – Comparação de Bit Rate - TCP

Na figura 10 é possível observar que as duas soluções obtiveram resultados quase que semelhantes em transferência, utilizando a ferramenta iPerf3 no protocolo UDP, de comunicação entre o desktop e o servidor de aplicação.

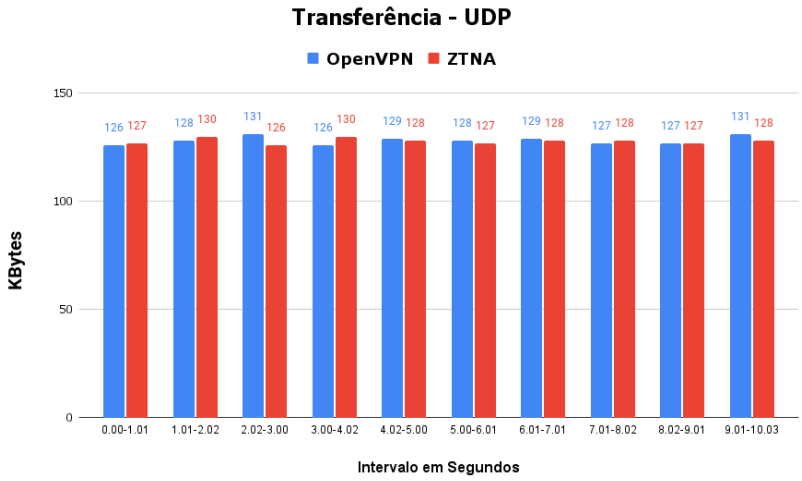

Figura 10 – Comparação de Transferência - UDP

Na figura 11 é possível observar que as duas soluções obtiveram resultados quase que semelhantes em bit rate, utilizando a ferramenta iPerf3 no protocolo UDP, de comunicação entre o desktop e o servidor de aplicação.

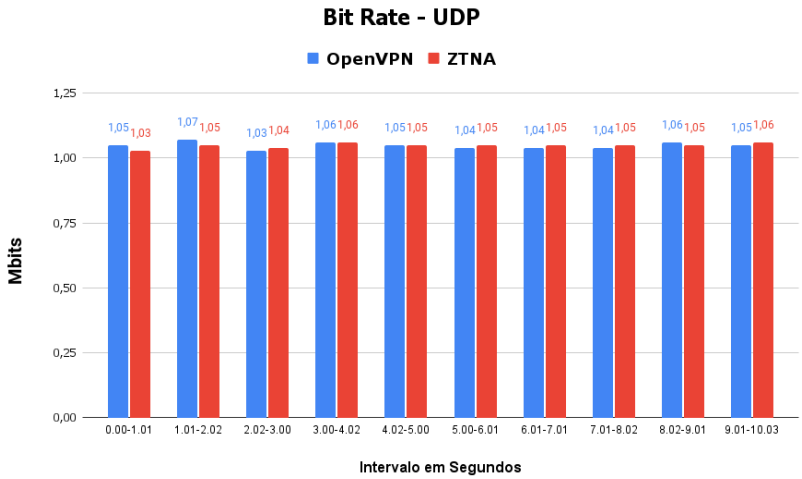

Figura 11 – Comparação de Bit Rate - UDP

Na figura 12 podemos observar que a solução OpenVPN apresentou uma latência melhor em comparação ao ZTNA no teste realizado em um smartphone. Foi utilizada a mesma ferramenta, o Ping Monitor, para ambos os cenários, tanto no OpenVPN quanto no ZTNA.

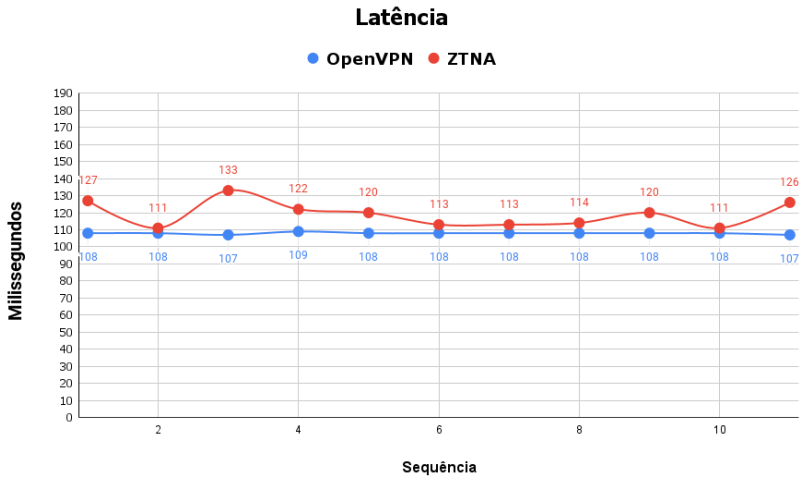

Figura 12 – Latência no Smartphone

O OpenVPN não possui controle sobre a rede LAN à qual o usuário está conectado para acessar o serviço. Se essa rede estiver configurada de maneira insegura, pode permitir que outros usuários dentro da mesma rede se comuniquem entre si, abrindo a possibilidade de ataques laterais contra o usuário que utiliza o OpenVPN.

Na figura 13, podemos observar que a máquina possui comunicação lateralmente, na rede LAN que a mesma está conectada.

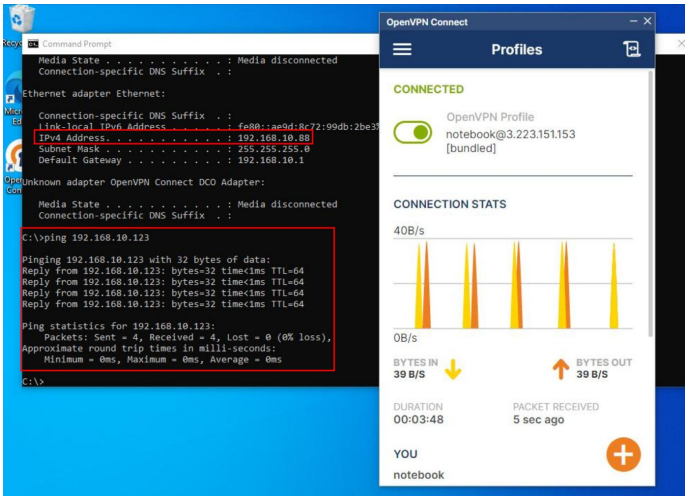

Figura 13 – Desktop possui comunicação com outro dispositivo na LAN

Na figura 14, é possível observar que, no ambiente construído, há comunicação entre os equipamentos na rede LAN, mesmo com a conexão VPN ativa. Isso demonstra a possibilidade de ataques laterais nessa rede, o que pode permitir que um invasor obtenha acesso ao túnel da VPN.

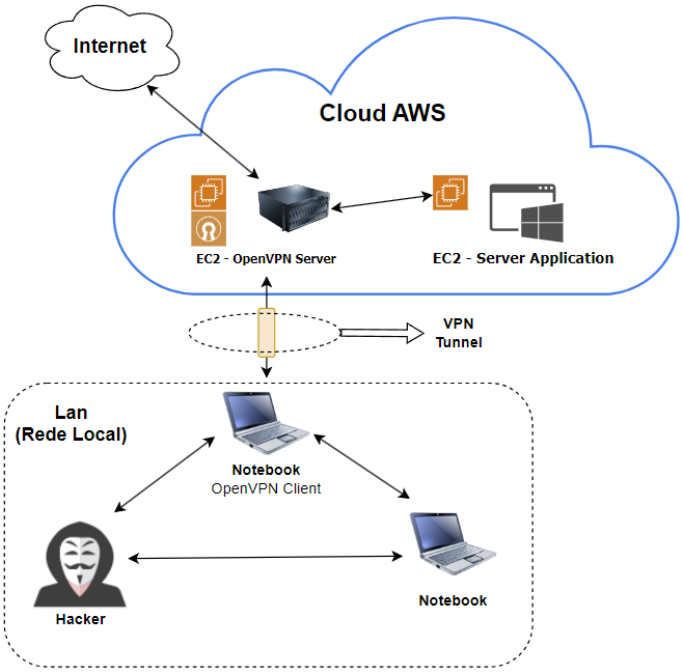

Figura 14 – Exemplo de LAN (Rede Local)

Diferentemente do OpenVPN, as políticas de acesso no ZTNA vão além dos grupos de usuários. Utilizando o princípio do menor privilégio, é possível conceder acesso apenas e especificamente a determinadas aplicações ou redes, evitando assim permissões desnecessárias a recursos que o usuário sequer utilizará.

A Figura 15, mostra que após o dispositivo ingressar na rede corporativa por meio da solução ZTNA. Assim que o dispositivo se conecta, o sistema inicia uma série de verificações de segurança, que incluem autenticação de identidade, validação de políticas de acesso e avaliação do estado do dispositivo. Uma vez que todas essas verificações são concluídas e o dispositivo é considerado seguro, todo o controle de acesso e a gestão da rede passam a ser administrados pela empresa. Isso significa que o acesso a recursos críticos é restrito com base em políticas de acesso dinâmicas, que levam em conta não apenas a identidade do usuário, mas também o contexto e o comportamento do dispositivo. Essa abordagem garante uma camada adicional de segurança, mitigando riscos associados a acessos não autorizados e garantindo que apenas dispositivos confiáveis tenham permissão para interagir com a infraestrutura corporativa.

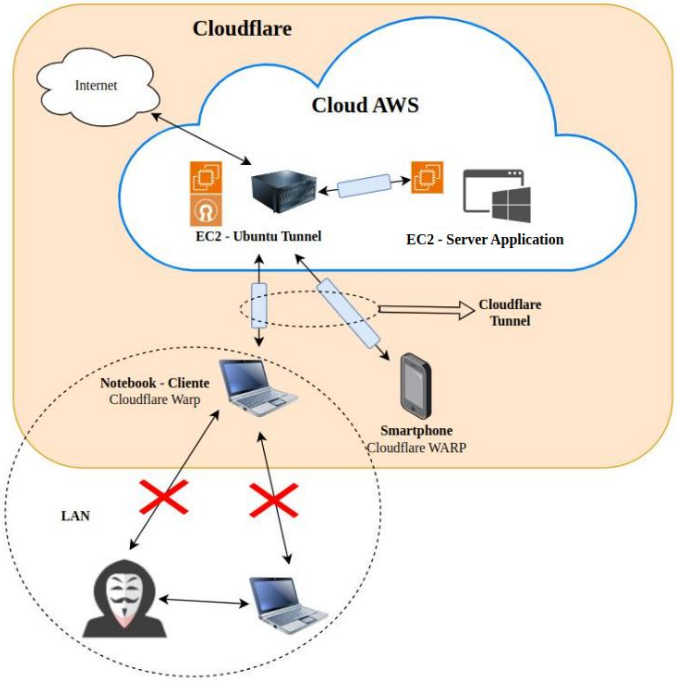

Figura 15 – Conectado no ZTNA

6 Conclusão

Este trabalho teve como objetivo realizar uma análise comparativa entre as tecnologias de OpenVPN e ZTNA aplicadas em um ambiente corporativo, focando nas vantagens de segurança de ambas. Foi construído um cenário semelhante para cada tecnologia, no qual o desempenho da rede foi analisado durante o uso de cada uma.

Os resultados obtidos foram analisados em conjunto com a comparação das vantagens e desvantagens de cada tecnologia. Os gráficos comparativos apresentados no capítulo anterior permitiram visualizar de forma clara o desempenho de cada solução em diferentes protocolos. Essa análise não apenas contribuiu para atingir o objetivo geral do trabalho, mas também para responder aos objetivos específicos estabelecidos.

Nos testes realizados, é possível observar um desempenho superior da solução de ZTNA em comparação com o OpenVPN, especialmente na comunicação entre o desktop e o servidor de aplicação onde executa o iPerf3. Isso ficou evidente após a relação dos testes com a ferramenta iPerf3, que mediu o bit rate por intervalo de tempo, para os protocolo TCP e UDP. Os gráficos 8 e 9 mostram que o ZTNA obteve um melhor desempenho em relação a *bit rate* e à transferência de dados. Nos gráficos é possível observar que a solução do ZTNA foi melhor em relação a OpenVPN em termos de largura de banda e transferência, isso contribui para uma melhor experiência do usuário. Além disso, o ZTNA oferece vantagens adicionais, como uma segurança aprimorada, graças à abordagem de ”confiança zero”, que reduz a superfície de ataque lateral na rede. Outras características incluem acesso granular e segmentação de rede, permitindo um controle mais preciso sobre o que cada usuário pode acessar, além de oferecer visibilidade e monitoramento detalhados sobre as ações de cada usuário.

Por outro lado, o OpenVPN apresentou um desempenho superior nos testes realizados em dispositivos móveis (smartphones) em comparação com o ZTNA. O gráfico 12 apresentado no capitulo anterior, mostra que a solução de VPN, obteve uma latência melhor em relação a solução ZTNA no dispositivo de smartphone. E essa diferença, impacta diretamente na experiência do usuário, ao utilizar a solução. O melhor desempenho do OpenVPN pode ser atribuído ao fato de que, nessa solução, o tráfego não precisa ser inspecionado por políticas granulares, resultando em uma conexão mais simples e direta.

A solução ZTNA representa uma evolução em relação às tradicionais soluções de VPN, sendo projetada para enfrentar as ameaças modernas, especialmente com a expansão dos ambientes de trabalho remoto, híbrido e o uso de dispositivos não geren-

ciados. Além disso, ela oferece uma capacidade de escalabilidade que pode melhorar a experiência do usuário.

A tecnologia de Zero Trust tem crescido a cada ano, e novas empresas, estão se destacando ao fornecer esse tipo de serviço. Como trabalho futuro, iremos avaliar soluções de ZTNA, comparando a abrangência de cada solução e as funcionalidades que elas oferecem em relação umas às outras.

Referências

ACT-IAC. *Zero Trust Cybersecurity Current Trends*. 2019. <https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf>. Acessado em: 18 de Abril 2024. Citado na página 13.

ANTONIUK, J.; PLECHAWSKA-WÓJCIK, M. Comparative analysis of vpn protocols. *Journal of Computer Sciences Institute*, v. 27, p. 138–144, 2023. ISSN 2544-0764. Citado 2 vezes nas páginas 21 e 23.

Check Point. *ZTNA x VPN*. 2024. <https://www.checkpoint.com/pt/cyber-hub/network-security/what-is-zero-trust-network-access-ztna/ztna-vs-vpn/#LimitationsofVPN>. Acessado em: 11 de Junho 2024. Citado na página 19.

Cloudflare ZTNA. *Whats is Zero Trust Network Access*. 2024. <https://www.cloudflare.com/learning/access-management/what-is-ztna/>. Acessado em: 30 de Junho 2024. Citado 2 vezes nas páginas 14 e 36.

ESTRI JH; DEWIUMAR RUSYDI; RIADI IMAM. *Implementation of Cloudflare Hosting for Speeds and Protection on The Website*. 2019. <https://eprints.uad.ac.id/15251/1/T2_1689048037_NASKAH_PUBLIKASI.pdf>. Acessado em: 11 de Maio 2024. Citado na página 21.

Forbes. *Qual o impacto da Covid-19 na 4ª Revolução Industrial?* 2020. <https://forbes.com.br/forbes-tech/2020/12/qual-o-impacto-da-covid-19-na-4a-revolucao-industrial/>. Acessado em: 18 de Abril 2024. Citado na página 12.

FORTINET SSL VPN. *O que é SSL VPN*. 2024. <https://www.fortinet.com/resources/cyberglossary/ssl-vpn>. Acessado em: 13 de Maio 2024. Citado na página 17.

IORDACHE, C. A.; DRAGOMIR, A. V.; MARIAN, C. V. Public institutions updated enhanced biometric security, zero trust architecture and multi-factor authentification. In: *2022 International Symposium on Electronics and Telecommunications (ISETC)*. [S.l.: s.n.], 2022. p. 1–4. Citado na página 21.

Iperf3. *Iperf3*. 2024. <https://iperf.fr/>. Acessado em: 30 de Junho 2024. Citado na página 23.

Kaspersky. *O que é uma VPN e como funciona?* 2023. <https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn>. Acessado em: 13 de Maio 2024. Citado na página 17.

Kindervag John. *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. 2024. <https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf>. Acessado em: 13 de Maio 2024. Citado na página 19.

Olhar Digital. *Com pandemia de coronavírus, mercado global de IaaS cresceu quase 50% em 2020*. 2021. <https://olhardigital.com.br/2021/06/30/pro/mercado-global-de-iaas-cresceu-quase-50-por-cento-em-2020/>. Acessado em: 18 de Abril 2024. Citado na página 12.

OpenVPN. *What Is A VPN?* 2023. <https://openvpn.net/what-is-a-vpn/>. Acessado em: 13 de Maio 2024. Citado 3 vezes nas páginas 14, 15 e 16.

OpenVPN - Managing Access control. *Managing Access control*. 2024. <https://openvpn.net/as-docs/access-control.html#>. Acessado em: 30 de Junho 2024. Citado na página 33.

OpenVPN - Whats is Openvpn. *Whats is Openvpn*. 2024. <https://openvpn.net/faq/what-is-openvpn/>. Acessado em: 30 de Junho 2024. Citado na página 32.

Price ZT. *Price ZT*. 2024. <https://www.cloudflare.com/pt-br/plans/zero-trust-services/>. Acessado em: 30 de Junho 2024. Citado na página 25.

QAZI, F. A. Study of zero trust architecture for applications and network security. In: *2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*. [S.l.: s.n.], 2022. p. 111–116. Citado 2 vezes nas páginas 14 e 21.

QU, J.; LI, T.; DANG, F. Performance evaluation and analysis of openvpn on android. In: *2012 Fourth International Conference on Computational and Information Sciences*. [S.l.: s.n.], 2012. p. 1088–1091. Citado na página 21.

RFC 768 - UDP. *RFC 768 - UDP*. 2024. <https://www.rfc-editor.org/rfc/rfc768>. Acessado em: 30 de Junho 2024. Citado na página 30.

Security Leaders. *Pandemia desafia CISO a reforçar segurança na nuvem*. 2020. <https://securityleaders.com.br/pandemia-desafia-ciso-a-reforcar-seguranca-na-nuvem/>. Acessado em: 18 de Abril 2024. Citado na página 12.

Security Org. *Increased Usage During COVID-19 Pandemic*. 2023. <https://www.security.org/vpn/statistics/>. Acessado em: 18 de Abril 2024. Citado na página 13.

ZTNA - Access control. *Control Access*. 2024. <https://www.cloudflare.com/products/zero-trust/zero-trust-network-access/>. Acessado em: 30 de Junho 2024. Citado na página 37.