Universidade Federal do Rio Grande do Norte – UFRN

Departamento de Engenharia de Computação e Automação – DCA

Curso de Engenharia de Computação

Teophilo Vitor de Carvalho Clemente

Do VPN ao Zero Trust: Um Guia de Boas Práticas para Adoção do ZTNA em Redes Corporativas

Natal – RN

Dezembro de 2025

Teophilo Vitor de Carvalho Clemente

Do VPN ao Zero Trust: Um Guia de Boas Práticas para Adoção do ZTNA em Redes Corporativas

Trabalho de Conclusão de Curso de Engenharia de Computação da Universidade Federal do Rio Grande do Norte, apresentado como requisito parcial para a obtenção do grau de Bacharel em Engenharia de Computação

Orientador: Carlos Manuel Dias Viegas

Universidade Federal do Rio Grande do Norte – UFRN

Departamento de Engenharia de Computação e Automação – DCA

Curso de Engenharia de Computação

Natal – RN

Dezembro de 2025

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Central Zila Mamede

Clemente, Teóphilo Vitor de Carvalho.
Do VPN ao Zero Trust: um guia de boas práticas para adoção do ZTNA em redes corporativas / Teóphilo Vitor de Carvalho Clemente. - 2025.
54 f.: il.

Trabalho de Conclusão de Curso - TCC (graduação) - Universidade Federal do Rio Grande do Norte, Centro de Tecnologia, Curso de Engenharia de Computação, Natal, RN, 2025.
Orientação: Prof. Dr. Carlos Manuel Dias Viegas.

1. Zero Trust - TCC. 2. ZTNA - TCC. 3. VPN - TCC. 4. Cibersegurança - TCC. 5. Microssegmentação - TCC. 6. Acesso remoto seguro - TCC. I. Viegas, Carlos Manuel Dias. II. Título.

RN/UF/BCZM CDU 004

Elaborado por Jackeline dos Santos Pinheiro da Silva Maia Cavalcanti - CRB-15/317

Teophilo Vitor de Carvalho Clemente

Do VPN ao Zero Trust: Um Guia de Boas Práticas para Adoção do ZTNA em Redes Corporativas

Trabalho de Conclusão de Curso de Engenharia de Computação da Universidade Federal do Rio Grande do Norte, apresentado como requisito parcial para a obtenção do grau de Bacharel em Engenharia de Computação

Orientador: Carlos Manuel Dias Viegas

Trabalho aprovado. Natal – RN, 01 de Dezembro de 2025:

Prof. Dr. Carlos Manuel Dias Viegas - Orientador
UFRN

Prof. Dr. Ivanovitch Medeiros Dantas da Silva - Examinador Interno
UFRN

Prof. Dr. Eduardo de Lucena Falcão - Examinador Interno
UFRN

Natal – RN
Dezembro de 2025

A Deus que iluminou o meu caminho durante esta jornada. Aos meus pais, pela força, dedicação, carinho e amor que sempre me deram, tornando cada etapa da vida mais significativa e leve. À minha família, por oferecer amor, apoio incondicional e palavras de encorajamento nos momentos mais desafiadores. Aos amigos, pela presença que trouxe leveza, motivação e alegria durante esta trajetória. Ao meu orientador, pela paciência, pela disponibilidade constante e pela generosidade em compartilhar seus conhecimentos comigo, me auxiliando na condução deste trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo dom da vida e por ter iluminado e guiado meus caminhos até aqui, sua presença e força me sustentaram ao longo desta jornada.

Aos meus pais, Francisco e Francisca que foram fontes incessantes de carinho, amor, atenção e força durante esta caminhada. Mesmo distantes, cada mensagem, cada ligação ao final da noite (todos os dias desde que vim morar em Natal), cada oração me fortalecia nesta conquista e aliviava um pouco da saudade.

À minha namorada, Eduarda, que me acolheu a cada dia, principalmente nos mais difíceis, apoiando-me e motivando-me a ser melhor. Obrigado por vibrar comigo à cada conquista.

Aos amigos que adquiri até aqui, que nos momentos de conversa, de estudos coletivos e de descontração tornaram essa caminhada mais leve e contribuíram para o meu aprendizado.

À Universidade Federal do Rio Grande do Norte (UFRN), pela excelente formação que recebi ao longo da minha jornada acadêmica. À Escola de Ciência e Tecnologia (ECT), onde cursei o primeiro ciclo da minha formação universitária e obtive as bases sólidas da engenharia. Ao Departamento de Computação e Automação (DCA), onde cursei o segundo ciclo e adentrei na área da Engenharia de Computação e fui moldado como profissional.

Aos professores que me acompanharam até aqui, preocupados não somente com o repasse de conhecimento a nível profissional, mas também com o incentivo ao desenvolvimento de um pensamento investigativo e crítico. A eles minha gratidão, especialmente ao meu orientador professor Carlos Viegas, que não mediu esforços para me apoiar e orientar ao longo deste trabalho.

Por fim, agradeço a todos, que de alguma forma, contribuíram para a realização deste trabalho e conclusão deste sonho.

"Eu tentei 99 vezes e falhei, mas na centésima tentativa eu consegui,
nunca desista de seus objetivos mesmo que esses pareçam impossíveis,
a próxima tentativa pode ser a vitoriosa."
(Albert Einstein)

RESUMO

Este trabalho apresenta uma análise técnica da transição dos modelos tradicionais de acesso remoto baseados em VPNs (redes privadas virtuais) para arquiteturas fundamentadas no princípio de Zero Trust, com foco no Zero Trust Network Access (ZTNA). Por meio de uma revisão bibliográfica e documental das soluções e tecnologias envolvidas, são examinadas as limitações das VPNs frente ao crescimento da computação em nuvem, da mobilidade corporativa e das ameaças cibernéticas modernas. O estudo também descreve os fundamentos do Zero Trust, identifica vulnerabilidades recorrentes em firewalls e VPNs, analisa os principais componentes e conceitos do ecossistema ZTNA, tais como identidade como perímetro, políticas baseadas em contexto, autenticação multifatorial, microssegmentação e tecnologias correspondentes, comparando sua eficácia em relação aos modelos tradicionais. Como principal contribuição, apresenta-se um guia de boas práticas para a adoção de ZTNA, incluindo um roadmap de adoção, critérios técnicos de avaliação, indicadores de desempenho e recomendações de governança. Dessa forma, o estudo contribui para fomentar a pesquisa nesta área e incentiva a adoção do ZTNA, que representa uma evolução estratégica para as organizações que buscam elevar sua maturidade em segurança, reduzir superfícies de ataque e aprimorar a experiência do usuário em ambientes corporativos distribuídos.

Palavras-chaves: Zero Trust; ZTNA; VPN; Segurança da Informação; Cibersegurança; Microssegmentação, Redes Corporativas, Acesso Remoto Seguro.

ABSTRACT

This work presents a technical analysis of the transition from traditional remote access models based on VPNs (virtual private networks) to architectures based on the Zero Trust principle, focusing on Zero Trust Network Access (ZTNA). Through a bibliographic and documentary review of the solutions and technologies involved, the limitations of VPNs in the face of the growth of cloud computing, corporate mobility, and modern cyber threats are examined. The study also describes the fundamentals of Zero Trust, identifies recurring vulnerabilities in firewalls and VPNs, analyzes the main components and concepts of the ZTNA ecosystem, such as identity as a perimeter, context-based policies, multifactor authentication, microsegmentation, and corresponding technologies, comparing their effectiveness to traditional models. As a main contribution, a best practices guide for ZTNA adoption is presented, including an adoption roadmap, technical evaluation criteria, performance indicators, and governance recommendations. In this way, the study contributes to fostering research in this area and encourages the adoption of ZTNA, which represents a strategic evolution for organizations seeking to increase their security maturity, reduce attack surfaces, and improve the user experience in distributed corporate environments.

Keywords: Zero Trust; ZTNA; VPN; Information Security; Cybersecurity; Microsegmentation; Corporate Networks; Secure Remote Access.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACE	*Access Control Engine*
AH	*Authentication Header*
BYOD	*Bring Your Own Device*
C2M2	*Cybersecurity Capability Maturity Model*
CSF	*Cybersecurity Framework*
CASB	*Cloud Access Security Broker*
CISO	*Chief Information Security Officer*
DDoS	*Distributed Denial of Service*
DLP	*Data Loss Prevention*
DPI	*Deep Packet Inspection*
EDR	*Endpoint Detection and Response*
EPP	*Endpoint Protection Platforms*
ESP	*Encapsulating Security Payload*
GDPR	*General Data Protection Regulation*
IaaS	*Infrastructure as a Service*
IAM	*Identity and Access Management*
IDS	*Intrusion Detection Systems*
IKE	*Internet Key Exchange*
IPS	*Intrusion Prevention System*
IPSec	*Internet Protocol Security*
ISE	*Identity Services Engine*
LGPD	*Lei Geral de Proteção de Dados Pessoais*
MDM	*Mobile Device Management*

MFA	*Multifactor Authentication*
MTTD	*Mean Time to Detect*
MTTR	*Mean Time to Respond*
NAC	*Network Access Control*
NGFW	*Next-Generation Firewall*
NIST	*National Institute of Standards and Technology*
NPA	*Netskope Private Access*
PA	*Policy Administrator*
PaaS	*Platform as a Service*
PAM	*Privileged Access Management*
PDCA	*Plan-Do-Check-Act*
PDP	*Policy Decision Point*
PE	*Policy Engine*
PEP	*Policy Enforcement Point*
POC	*Proof of Concept*
RBAC	*Role-Based Access Control*
SaaS	*Software as a Service*
SASE	*Secure Access Service Edge*
SGSI	*Sistemas de Gestão de Segurança da Informação*
SIEM	*Security Information and Event Management*
SOAR	*Security Orchestration, Automation and Response*
SSL	*Secure Sockets Layer*
SSO	*Single Sign-On*
SWG	*Secure Web Gateway*
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*

XDR	*Extended Detection and Response*
ZIA	*Zscaler Internet Access*
ZPA	*Zscaler Private Access*
ZTA	*Zero Trust Architecture*
ZTNA	*Zero Trust Network Access*

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

A segurança da informação em redes corporativas tem se tornado um dos principais desafios no cenário tecnológico contemporâneo. A crescente digitalização das empresas, desde as mais tradicionais até as puramente tecnológicas, impulsionada pela onda da transformação digital e pelo aumento do trabalho remoto advindo da pandemia da COVID-19, trouxe inúmeros benefícios, mas também acarretou um significativo aumento na superfície de ataque das redes corporativas.

Em relação à pandemia da COVID-19, houve uma rápida migração nos modelos de negócio impondo às organizações uma mudança para o trabalho remoto, resultando em uma adoção massiva de redes privadas virtuais (VPNs) para manter a operação junto aos colaboradores. O estudo de Mirkovic, Feng e Li (2022) sobre os impactos do trabalho remoto pré e pós-pandemia destaca que esse cenário introduziu novos riscos à segurança e à privacidade, incluindo a implementação rápida de tecnologias sem treinamento adequado, o uso de dispositivos domésticos em ambientes compartilhados e a presença de usuários não confiáveis no local de trabalho remoto, elevando significativamente a superfície de ataque. De acordo com Mirkovic, Feng e Li (2022), o uso de VPNs chegou a crescer cinco vezes nas primeiras semanas de lockdowns e manteve-se em um patamar elevado mesmo após esse período, evidenciando a intensificação da dependência dessas soluções e a consequente ampliação da exposição a riscos de segurança.

Já no contexto da transformação digital e indústria 4.0 as empresas realizam um movimento comum para ambientes híbridos e multi-cloud e com isso as organizações corporativas passam a enfrentar uma complexidade de riscos ainda maior. Esse contexto ampliado permite que ameaças cibernéticas explorem diferentes pontos da infraestrutura, desde serviços em nuvem até os já mencionados dispositivos de funcionários conectados remotamente, facilitando ataques coordenados com uso de ransomware, malware e outras técnicas avançadas. Segundo o relatório da Check Point Research (2025), no primeiro trimestre de 2025 as organizações sofreram em média 1.925 ataques cibernéticos semanais, um aumento de 47% em relação ao mesmo período de 2024. No segundo trimestre do mesmo ano, esse número chegou a 1.984 ataques por semana, representando 21% de crescimento em comparação a 2024.

Em detrimento as práticas anteriores de acesso remoto, o conceito de Zero Trust, formulado por John Kindervag em 2010, rompe com a lógica perimetral ao adotar a premissa de “nunca confiar, sempre verificar”. Nesse modelo, cada acesso deve ser continuamente

autenticado, autorizado e validado de acordo com critérios como identidade, dispositivo, localização e risco associado (KINDERVAG; BALAOURAS; COIT, 2010). A aplicação prática desse paradigma, conhecida como Zero Trust Network Access (ZTNA), tem ganhado destaque como alternativa às VPNs tradicionais, ao oferecer controles granulares, redução da superfície de ataque e maior escalabilidade para redes corporativas (CISCO, 2024)

Desse modo, este trabalho busca explorar esse cenário de transição do modelo de confiança implícita para o modelo de confiança zero, discutindo o papel do ZTNA como evolução natural dos mecanismos de acesso remoto, tendo como objetivo criar um guia de boas práticas de como implantar o ZTNA em redes corporativas, incentivando assim sua adoção.

1.2 Justificativa

A crescente onda de ataques cibernéticos, como incidentes de ransomware, ataques a sistemas bancários e invasões explorando vulnerabilidades em VPNs, demonstram a necessidade urgente de repensar os modelos de segurança utilizados em empresas de diferentes portes. Estudos recentes de órgãos de referência, como o NIST SP 800-207 do National Institute of Standards and Technology, reforçam que o paradigma Zero Trust deve ser considerado uma diretriz estratégica para proteger ativos digitais em ambientes corporativos (ROSE et al., 2020).

Do ponto de vista acadêmico, este estudo contribui para consolidar o conhecimento sobre a arquitetura Zero Trust e sua aplicação prática em redes corporativas, oferecendo uma visão ampliada sobre o tema e sua importância no cenário da cibersegurança. Já sob a ótica prática, o trabalho tem relevância ao propor diretrizes aplicáveis a gestores de TI e equipes de cibersegurança, fornecendo recomendações de implementação que podem apoiar organizações na transição do modelo tradicional baseado em VPN para o modelo baseado em ZTNA.

Desse modo, a pesquisa justifica-se pelo ganho científico e pela sua aplicabilidade direta em empresas que buscam reduzir riscos cibernéticos e se adequar às demandas modernas de segurança.

1.3 Objetivo Geral

Este trabalho tem como objetivo geral desenvolver um guia de boas práticas para a adoção do Zero Trust Network Access (ZTNA) em redes corporativas, destacando suas vantagens em relação às Virtual Private Networks (VPNs) e apresentando recomendações que possam facilitar sua implementação no mundo corporativo.

1.4 Objetivos Específicos

- Revisar a literatura acadêmica e técnica sobre Zero Trust, ZTNA, VPN e tecnologias associadas.
- Identificar vulnerabilidades e limitações associadas ao uso de VPNs tradicionais em redes corporativas.
- Analisar os benefícios e desafios da adoção do ZTNA em comparação a modelos de segurança tradicionais.
- Elaborar diretrizes práticas que auxiliem organizações na implementação de ZTNA, considerando aspectos técnicos, organizacionais e de governança.
- Propor um roadmap de adoção de ZTNA adaptado ao contexto corporativo brasileiro.

1.5 Estrutura do Trabalho

A estrutura deste trabalho está organizada em cinco capítulos principais. O Capítulo 1 introduz a problemática pertinente ao tema, descrevendo o contexto, a justificativa, os objetivos e a relevância deste estudo. O Capítulo 2 apresenta a fundamentação teórica, abordando os conceitos fundamentais de segurança da informação em redes corporativas, as vulnerabilidades principais, as tecnologias tradicionais como VPNs e Firewalls e um detalhamento da evolução para o modelo Zero Trust e o ZTNA, com base em referências acadêmicas e de mercado. O Capítulo 3 descreve a metodologia adotada, caracterizada como pesquisa bibliográfica, exploratória e comparativa, explicitando as fontes consultadas e os critérios de seleção adotados. O Capítulo 4 apresenta os resultados obtidos, que consistem em um guia de boas práticas para adoção do ZTNA em redes corporativas, incluindo as recomendações de planejamento, implementação, gestão operacional, análise das soluções de mercado e um roadmap para adoção. Por fim, o Capítulo 5 apresenta a conclusão do estudo, retomando os objetivos, destacando as principais contribuições, limitações e sugestão de possíveis avanços para a pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, são apresentados os principais conceitos e tecnologias envolvidas na discussão sobre o ZTNA e sobre a segurança em redes corporativas. São abordados temas chave como o conceito de VPN e suas vulnerabilidades, firewalls, ZTA e ZTNA, como também modelos de implementação segura de uma rede zero trust e desafios existentes.

2.1 *Segurança da Informação em Redes Corporativas*

A segurança da informação, definida como a proteção de informação e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de prover confidencialidade, integridade e disponibilidade (NIST, 2024). A tríade anteriormente citada é conhecida como CIA, sendo um campo central dentro da ciência da computação e da gestão de tecnologia da informação, sendo peças centrais da segurança dos ativos digitais de uma organização (STALLINGS; BROWN, 2014).

A confidencialidade refere-se à proteção da informação contra acessos não autorizados, garantindo que apenas usuários devidamente autenticados possam acessar determinados dados ou sistemas. Isso é comumente implementado por meio de mecanismos de criptografia, autenticação multifator (MFA) e políticas de controle de acesso. A integridade garante que os dados permaneçam consistentes, completos e sem alterações indevidas durante o seu ciclo de vida. Técnicas como hashing, assinaturas digitais e controles de versão são utilizadas para preservar a integridade dos ativos. A disponibilidade, por sua vez, assegura que os sistemas e informações estejam acessíveis sempre que necessário, mesmo em situações adversas, como falhas de hardware, ataques distribuídos de negação de serviço (DDoS) ou desastres naturais.

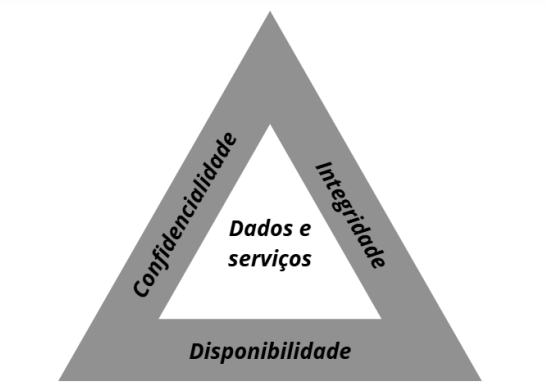

Figura 1 – *A* tríade de requisitos de segurança.

Fonte: Adaptado de Stallings e Brown (2014).

Por muitos anos, a segurança perimetral foi o principal alicerce da proteção das redes corporativas. Essa abordagem buscava proteger a infraestrutura a partir das fronteiras, utilizando recursos como firewalls e sistemas de detecção de intrusão (IDS). O modelo partia do pressuposto de que o tráfego interno era confiável, enquanto o externo deveria ser tratado como potencialmente perigoso. Essa lógica, embora eficiente em seu tempo, mostrou-se limitada diante de novos cenários de risco, como ameaças internas, a popularização do BYOD (Bring Your Own Device) e a expansão do acesso remoto.

Com o avanço da transformação digital e o crescimento da computação em nuvem, o modelo perimetral passou a ser ainda mais desafiado. Os ativos corporativos deixaram de estar concentrados apenas em data centers locais para se espalharem entre diferentes ambientes, serviços em nuvem como Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS), além de aplicações distribuídas e dispositivos móveis (RILEY; MACDONALD; ORANS, 2020). Essa descentralização reduziu a eficácia das defesas tradicionais baseadas exclusivamente na borda da rede, impulsionando as organizações a buscar estratégias mais flexíveis e adaptativas, entre elas o Zero Trust, que rompe com a ideia de confiança implícita no tráfego interno.

Um fator que acelerou essa mudança também foi a pandemia da COVID-19, que obrigou empresas a migrarem rapidamente para o trabalho remoto. Esse movimento resultou em uma adoção massiva de VPNs, mas também ampliou significativamente a superfície de ataque, uma vez que dispositivos pessoais passaram a ser utilizados para acessar redes corporativas. Estudos como o de Mirkovic, Feng e Li (2022) destacam que esse cenário introduziu riscos adicionais, incluindo a implementação apressada de tecnologias sem treinamento adequado, além da maior exposição a usuários não confiáveis nos ambientes domésticos.

Além disso, relatórios como o Verizon Data Breach Investigations Report (VERIZON, 2022) apontam que as principais causas de incidentes em redes corporativas continuam sendo ataques de engenharia social, ransomware e exploração de vulnerabilidades conhecidas. O mesmo relatório evidencia que mais de 80% das violações de segurança envolvem o uso de credenciais comprometidas, o que reforça a necessidade de evoluir para modelos que priorizem identidade e autenticação contínua como novos pilares de defesa.

A normatização também exerce papel central nesse contexto. A ISO/IEC 27001 estabelece diretrizes para a criação de Sistemas de Gestão de Segurança da Informação (SGSI), enquanto o NIST Cybersecurity Framework fornece práticas para identificação, proteção, detecção, resposta e recuperação diante de incidentes. Ambos os referenciais têm sido amplamente adotados por empresas que buscam alinhar a cibersegurança à governança corporativa e à mitigação de riscos.

Em suma, a segurança da informação em redes corporativas passou de um modelo

estático, baseado na proteção de perímetro, para um paradigma dinâmico e centrado em identidade, contexto e comportamento do usuário. Esse movimento marca a transição das soluções tradicionais, como VPNs, para arquiteturas mais avançadas, representadas pelo Zero Trust Network Access (ZTNA).

2.2 *Redes Privadas Virtuais (VPNs)*

Antes da ascensão de arquiteturas modernas como o Zero Trust Network Access (ZTNA), as empresas tradicionalmente se apoiaram redes privadas virtuais (VPNs) para prover comuninação "segura", as VPNs desempenharam um papel fundamental durante décadas, mas hoje são questionadas em relação à sua capacidade de responder adequadamente às novas dinâmicas de trabalho remoto, nuvem e mobilidade. As VPNs (Virtual Private Networks) surgiram como uma forma de estender a rede corporativa para locais externos, permitindo que usuários remotos acessem recursos internos com segurança. Seu funcionamento é baseado no tunelamento criptografado, que encapsula o tráfego entre o usuário e a rede da organização, utilizando protocolos como IPSec ou SSL/TLS (STALLINGS; BROWN, 2014).

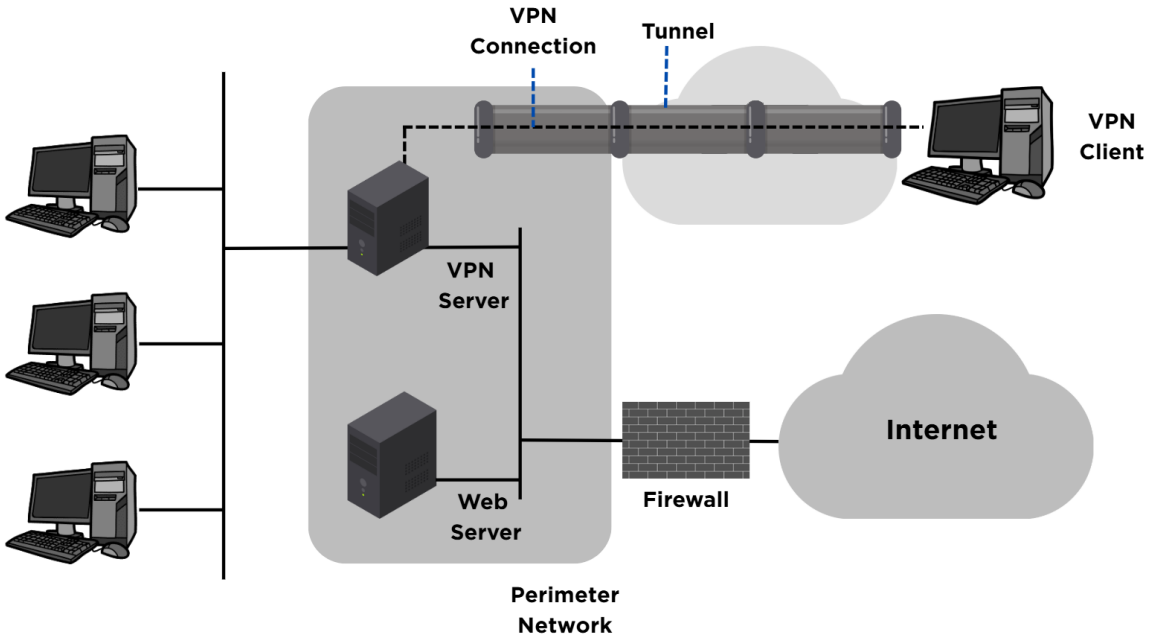

Figura 2 – *E*xemplo de arquitetura VPN de acesso remoto.

Fonte: PRÓPRIA, 2025.

2.2.1 IPSec (Internet Protocol Security)

O IPSec é um conjunto de protocolos desenvolvido pelo IETF para operar na camada de rede (Camada 3 do modelo OSI), fornecendo proteção direta aos pacotes IP.

Em uma VPN, o IPSec é amplamente utilizado para criar túneis criptografados entre dois dispositivos ou redes, permitindo o tráfego seguro de dados independentemente das aplicações utilizadas (FRANKEL, 2001).

O IPSec define dois modos principais de operação (THIRUVASAGAM; GEORGE, 2019):

- **Modo Transporte:** protege apenas o conteúdo do pacote IP, sendo usado em conexões diretas entre hosts.
- **Modo Túnel:** encapsula todo o pacote IP original dentro de outro pacote protegido, sendo o modo mais utilizado em VPNs site-to-site entre gateways ou roteadores.

Os principais componentes do IPSec são:

- **Authentication Header (AH):** garante integridade e autenticação dos pacotes.
- **Encapsulating Security Payload (ESP):** realiza criptografia e autenticação do conteúdo transmitido.

A troca de chaves é realizada por meio do protocolo IKE (Internet Key Exchange), que autentica os peers e estabelece os parâmetros de segurança da sessão. Estudos recentes demonstram que, apesar do elevado nível de segurança, o IPSec pode gerar sobrecarga de processamento e aumento de latência em redes com grande volume de tráfego (THIRUVASAGAM; GEORGE, 2019).

Devido a essas características, o IPSec é mais adequado para VPNs corporativas permanentes, como conexões entre filiais (site-to-site) ou entre firewalls e roteadores de borda, onde a estabilidade e o controle centralizado são mais importantes que a flexibilidade (NIST, 2020).

2.2.2 SSL/TLS (Secure Sockets Layer / Transport Layer Security))

O protocolo SSL/TLS, sucessor do SSL desenvolvido pela Netscape, opera na camada de transporte (Camada 4 do modelo OSI) e é amplamente utilizado em VPNs de acesso remoto (Remote Access VPNs). Diferentemente do IPSec, o SSL/TLS cria túneis entre o navegador ou cliente VPN e o servidor corporativo, garantindo a segurança dos dados transmitidos sobre a Internet (MEYER; SCHWENK, 2013).

O processo de handshake TLS autentica as partes envolvidas (via certificados digitais) e negocia os algoritmos criptográficos usados na sessão. Após essa fase, o tráfego entre o cliente e o servidor passa a ser criptografado e autenticado.

As VPNs SSL/TLS dividem-se em dois principais modelos (FORTINET, 2025):

- **SSL Portal VPN:** permite acesso seguro via navegador, sem necessidade de software adicional.
- **SSL Tunnel VPN:** estabelece um túnel completo, permitindo acesso a aplicações corporativas não baseadas em Web.

As VPNs baseadas em SSL/TLS costumam apresentar boa compatibilidade com diferentes dispositivos e ambientes, incluindo plataformas móveis e serviços em nuvem. Isso ocorre porque utilizam protocolos amplamente suportados e portas TCP comuns, como a 443, o que facilita sua operação mesmo em redes que possuem NAT ou regras de firewall mais restritivas. Entretanto, por funcionarem na camada de aplicação, sua proteção geralmente se limita ao tráfego das aplicações configuradas para uso da VPN. Já as soluções baseadas em IPSec operam na camada de rede, oferecendo cobertura para todo o tráfego IP gerado ou recebido pelo dispositivo.

Entre os benefícios da VPN estão a proteção contra interceptação de dados, a possibilidade de conectar escritórios remotos ou colaboradores em home office e a redução de custos em comparação com linhas privadas dedicadas. Contudo, esse modelo apresenta limitações significativas. Um dos maiores problemas está no conceito de "acesso total", visto que uma vez autenticado, o usuário geralmente ganha visibilidade para toda a rede corporativa que acessa, o que contraria os princípios modernos de privilégio mínimo. Além disso, ataques de força bruta contra credenciais, exploração de vulnerabilidades em appliances de VPN e configurações incorretas têm sido vetores frequentes de violações (CYBERSECURITY; (CISA), 2020).

2.3 *Firewalls*

Os firewalls são há anos a base da segurança de redes corporatias, atuando como mecanismos de filtragem de tráfego e controle de fronteira entre zonas de confiança. Esses dispositivos operam com base em regras estáticas relacionadas a endereços IP, portas e protocolos, implementando um modelo de perímetro que assume que usuários e dispositivos internos são confiáveis enquanto o tráfego externo é considerado hostil (STALLINGS; BROWN, 2014). Essa abordagem pressupõe que dispositivos e usuários internos são confiáveis, enquanto conexões externas representam riscos, o que resultou em arquiteturas de segurança baseadas em zonas de confiança.

A evolução das ameaças, no entanto, demonstrou que a inspeção superficial e o controle baseado em portas/protocolos eram insuficientes para redes modernas. Isso levou ao surgimento dos firewalls de segunda geração, capazes de realizar inspeção de estado (stateful inspection), rastreando o contexto das conexões e aumentando a precisão na análise de tráfego. Mais recentemente, os Next-Generation Firewalls (NGFWs) ampliaram

esse escopo ao acrescentar funcionalidades como inspeção profunda de pacotes (DPI), identificação de aplicações, controle por usuário e integração com sistemas de detecção e prevenção de intrusão (IDS/IPS), além de análises comportamentais baseadas em inteligência artificial (NETWORKS, 2025).

Os NGFWs representam um avanço significativo ao permitir que políticas sejam construídas não apenas com base em parâmetros técnicos da conexão, mas também com base em aplicações, usuários e perfis organizacionais. Essa abordagem aumenta a precisão na detecção de ameaças e reforça o princípio de defesa em profundidade.

Apesar de sua relevância, os firewalls apresentam limitações quando usados isoladamente. O modelo tradicional de perímetro pode criar "zonas amplas de confiança" internas, nas quais ameaças internas ou invasores pós-comprometimento podem se mover com relativa facilidade (KINDERVAG; BALAOURAS; COIT, 2010). Além disso, a relevância prática da gestão de vulnerabilidades pode ser observada em incidentes amplamente documentados, como aqueles envolvendo a exploração de falhas críticas em appliances de Firewall, como as falhas CVE-2018-13379 e CVE-2020-12812 em dispositivos Fortinet, amplamente utilizadas em ataques reais (CORPORATION, 2025).

Deste modo, no modelo Zero Trust, a função do firewall não é eliminada, mas transformada, este deixa de ser uma barreira única e passa a integrar uma malha de segurança distribuída, em que políticas são definidas de forma centralizada e aplicadas de maneira granular em múltiplos pontos da rede. O firewall recebe instruções de motores de decisão externa, como sistemas de identidade (IAM), avaliadores de postura e controladores ZTNA e assim aplica regras dinâmicas baseadas em identidade e contexto. Esse modelo reduz a dependência da topologia física e aumenta a capacidade de escalar ambientes híbridos e multi-cloud.

2.4 *Zero Trust Network Access (ZTNA)*

2.4.1 Origem e Definição

O conceito de Zero Trust surgiu formalmente em 2010, quando John Kindervag, então analista da Forrester Research, publicou um relatório questionando a efetividade do modelo de segurança baseado em perímetro. Kindervag, Balaouras e Coit (2010) argumentam que o paradigma de segurança tradicional, sustentado pela ideia de que tudo dentro da rede corporativa seria confiável, era falho por natureza. O autores propõem uma mudança conceitual fundamentada no princípio de "nunca confiar, sempre verificar" (never trust, always verify), segundo o qual todo usuário, dispositivo ou aplicação deve ser considerado potencialmente malicioso até que sua identidade seja devidamente autenticada, seu contexto analisado e suas ações monitoradas continuamente. Esse marco representou uma

ruptura com o modelo de segurança perimetral, historicamente dependente de mecanismos como firewalls e VPNs, que se mostraram insuficientes frente à crescente mobilidade e à descentralização dos ativos corporativos (BHUJBAL et al., 2024).

Durante a década de 2010, o modelo Zero Trust evoluiu de um conceito teórico para um paradigma estratégico de segurança cibernética amplamente reconhecido. O avanço da computação em nuvem, da virtualização e do trabalho remoto provocou uma expansão significativa dos perímetros de rede, tornando ineficaz a confiança baseada na localização (por exemplo, "estar dentro da LAN corporativa"). Nesse cenário, o Zero Trust passou a ser visto como uma abordagem que impõe autenticação, autorização e verificação contínuas em todas as comunicações, independentemente de origem ou destino. Conforme reforçam (BHUJBAL et al., 2024), o Zero Trust não apenas redefine a forma de controlar acessos, mas também introduz uma arquitetura centrada em identidade, que busca reduzir a superfície de ataque por meio de princípios como menor privilégio, microssegmentação e validação dinâmica de contexto.

A filosofia proposta por Kindervag encontra respaldo em diversas pesquisas acadêmicas recentes, que evidenciam sua aplicabilidade em diferentes domínios. As pesquisas de Liu, Tan e Liu (2024) destacam, por exemplo, a relevância do Zero Trust em ambientes de Internet das Coisas (IoT), nos quais a ausência de fronteiras físicas claras exige políticas de autenticação contínua e validação contextual. De modo semelhante Vaka (2021) observa que o Zero Trust oferece uma estrutura mais resiliente contra ataques internos e externos, uma vez que elimina a confiança implícita e promove uma segurança baseada em políticas verificáveis. Essa mudança conceitual tem permitido às organizações migrar de um modelo de defesa estática para um modelo dinâmico e adaptativo, mais alinhado às ameaças contemporâneas.

A evolução natural desse paradigma culminou na criação do Zero Trust Network Access (ZTNA), uma aplicação prática dos princípios de Zero Trust voltada ao controle de acesso à rede e às aplicações corporativas. De acordo com o Riley, MacDonald e Orans (2020), o ZTNA define um limite lógico de acesso baseado em identidade e contexto, ocultando os aplicativos corporativos da exposição pública e mediando o acesso por meio de um broker de confiança. Em outras palavras, o ZTNA substitui a lógica da VPN tradicional por um modelo mais granular e contextual, no qual o acesso é concedido de forma dinâmica, de acordo com as políticas estabelecidas e com o perfil de risco da sessão (BASHI; SENAN, 2025). Essa abordagem adota o princípio do menor privilégio, concedendo apenas as permissões estritamente necessárias e revogando-as automaticamente quando as condições de segurança não são atendidas.

Pesquisas recentes confirmam que o ZTNA se consolidou como um dos principais mecanismos técnicos de implementação da arquitetura Zero Trust. Bashi e Senan (2025) propõem um modelo de implantação que integra Policy Decision Point (PDP) e Policy

Enforcement Point (PEP), garantindo coerência nas políticas de acesso, autenticação contínua e monitoramento adaptativo. Já Qazi (2022) destaca que o uso de ZTNA amplia a visibilidade e o controle sobre o tráfego de rede, permitindo uma detecção proativa de anomalias e uma resposta automática a incidentes. Assim, o ZTNA representa não apenas uma tecnologia de acesso remoto, mas um pilar operacional da filosofia Zero Trust, oferecendo às organizações uma segurança mais granular, contextual e resistente a ameaças internas e externas.

2.4.2 Arquitetura Zero Trust (ZTA e ZTNA)

A arquitetura Zero Trust, segundo o NIST Special Publication 800-207 (ROSE et al., 2020), não é um produto único, mas sim um conjunto de princípios e componentes que podem ser combinados.

Os elementos centrais incluem:

- **Policy Decision Point (PDP):** responsável por avaliar solicitações de acesso com base em políticas de identidade, contexto, risco e conformidade, sendo constituído pelo Policy Engine (PE) e o Policy Administrator (PA).
- **Policy Enforcement Point (PEP):** aplica a decisão do PDP, sendo responsável habilitar, monitorar ou encerrar a conexão entre o usuário e o recurso.
- **Policy Engine (PE):** componente de lógica que avalia políticas as segurança e o fornece a decisão final da concessão do acesso a um recurso.
- **Policy Administrator (PA):** com base nas informações do Policy Engine envia instruções ao PEP sobre a ação de estabelecer ou interromper uma conexão.

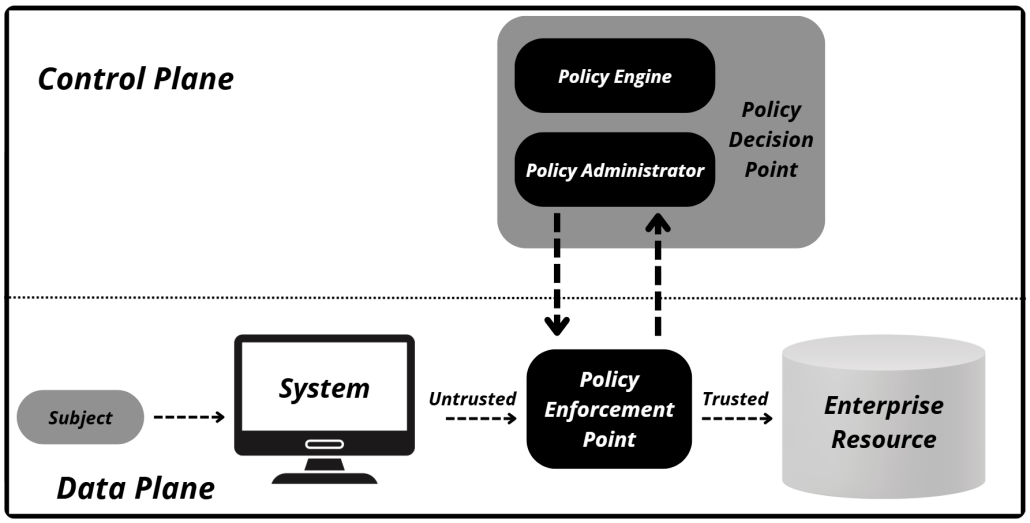

Figura 3 – *M*odelagem Zero Trust do NIST 800-207.

Fonte: Adaptado de Rose et al. (2020).

O PDP é o responsável por avaliar políticas de segurança e tomar decisões de autorização com base em critérios contextuais, como identidade, integridade do dispositivo, localização e comportamento do usuário. Já o PEP atua como o ponto de controle e execução, aplicando as decisões definidas pelo PDP nas tentativas de acesso aos recursos corporativos. Em ambientes corporativos modernos, frequentemente híbridos e distribuídos, com recursos espalhados entre data centers e provedores de nuvem, essa arquitetura possibilita que as políticas de acesso sejam aplicadas de forma uniforme, independentemente do local onde o recurso se encontra.

A partir deles é adotada uma autenticação contínua e adaptativa, um aspecto fundamental do modelo Zero Trust. Nesse tipo de autenticação, a verificação da identidade do usuário e das condições do dispositivo não ocorre apenas no momento inicial do login, mas é mantida durante toda a sessão, adaptando-se conforme o comportamento e o risco contextual, requerendo para isso integração com sistemas de identidade (IAM), ferramentas de monitoramento contínuo e mecanismos de autenticação adaptativa. Isso reduz a probabilidade de comprometimento de credenciais e dificulta a movimentação lateral de agentes maliciosos dentro da rede. Além disso, o monitoramento constante alimenta o PDP com dados comportamentais, permitindo o ajuste dinâmico de políticas e a resposta automática a eventos suspeitos.

Outro ponto chave da arquitetura é possibilidade da visão abrangente do tráfego, das requisições e dos padrões de acesso dos usuários, o que possibilita não apenas a detecção precoce de anomalias, mas também a auditoria e o cumprimento de normas regulatórias. Essa visibilidade é particularmente relevante em setores que lidam com informações sensíveis, como o financeiro, o governamental e o de saúde, onde a conformidade e a rastreabilidade são requisitos críticos.

O fluxo de funcionamento básico é o seguinte:

- O usuário solicita acesso a um recurso (aplicação).
- O sistema (Broker ZTNA) verifica quem é o usuário (identidade), em qual dispositivo está, a conformidade do dispositivo, em qual horário, qual geolocalização, demais filtros de acesso configurados e avalia qual risco envolve o pedido.
- O PDP avalia essas informações em tempo real.
- O PEP concede acesso apenas ao recurso específico solicitado, sem abrir toda a rede corporativa.

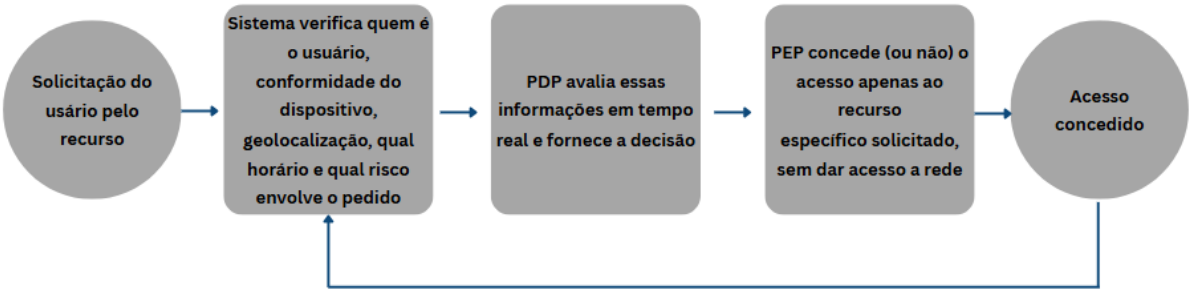

Figura 4 – *D*iagrama de fluxo do funcionamento da solução ZTNA.

Fonte: PRÓPRIA, 2025.

2.4.3 Princípios Fundamentais

O ZTNA se sustenta em alguns princípios-chave, definidos por (KINDERVAG; BALAOURAS; COIT, 2010) e reforçados por (ROSE et al., 2020):

- **Never Trust, Always Verify:** nunca confiar implicitamente em nada, mesmo que esteja "dentro" da rede.
- **Privilégio Mínimo:** conceder apenas os acessos necessários para a tarefa em questão.
- **Autenticação e Autorização Contínuas:** acesso não é permanente, deve ser validado dinamicamente a cada sessão.
- **Microssegmentação:** dividir a rede em pequenos blocos para isolar recursos críticos.
- **Visibilidade e Análise Contínua:** monitorar em tempo real usuários, dispositivos, tráfego e comportamentos.

Esses princípios diferenciam o ZTNA da VPN. Enquanto na VPN o usuário tem acesso amplo à rede, no ZTNA o acesso é sempre restrito, contextual e temporário.

2.4.4 Modelos de Implementação e Benefícios do ZTNA

Diversos fabricantes e organizações vem desenvolvendo arquiteturas baseadas no conceito de Zero Trust Network Access (ZTNA), cada uma com características e abordagens específicas. O Google BeyondCorp foi pioneiro na implementação em larga escala, eliminando a necessidade de VPNs internas e baseando o acesso em identidade, dispositivo e contexto. Essa arquitetura inovadora redefiniu o conceito de perímetro de segurança e se tornou uma das principais referências no desenvolvimento do modelo Zero Trust (WARD; BEYER, 2014). A figura a seguir ilustra a arquitetura do Google BeyondCorp.

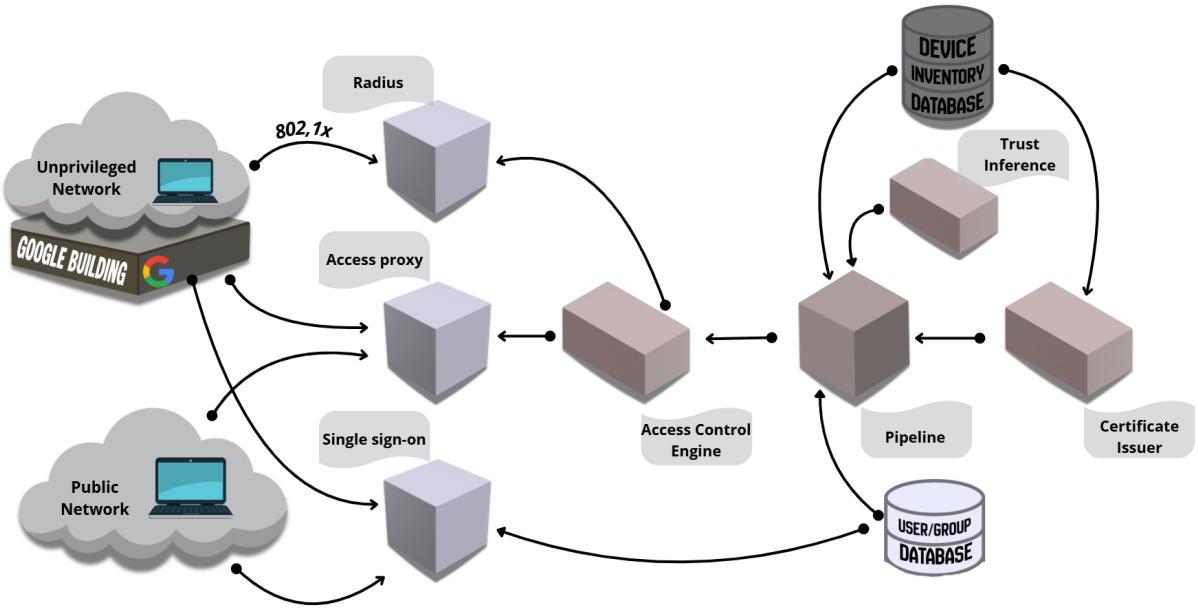

Figura 5 – *C*omponentes da arquitetura BeyondCorp.

Fonte: Adaptado de Google (2025).

Na tabela a seguir são evidenciados os componentes da arquitetura, sua função e um breve descritivo da atividade que desempenha dentro da arquitetura Zero Trust do Google.

Tabela 1 – Componentes do BeyondCorp e suas respectivas funções.

Component	**Função Principal**	**Descrição**
Device Inventory Database	Identificação e rastreamento de dispositivos.	Armazena informações sobre todos os dispositivos corporativos gerenciados. Cada dispositivo possui um certificado digital único vinculado ao seu registro no inventário, permitindo o rastreamento completo de seu ciclo de vida e garantindo que apenas dispositivos confiáveis acessem os recursos corporativos.
User/Group Database	Gestão de identidade e autenticação de usuários.	Mantém informações sobre usuários, cargos e grupos, integrando-se aos processos de RH. Atua em conjunto com o sistema SSO para autenticar e classificar usuários de acordo com suas funções.

Tabela 1 – Componentes do BeyondCorp e suas respectivas funções.

Componente	**Função Principal**	**Descrição**
Single Sign-On (SSO)	Autenticação centralizada de usuários.	Valida credenciais de primeiro e segundo fator, emitindo tokens temporários utilizados na autorização de acesso a recursos e aplicações corporativas.
Unprivileged Network	Segmentação e isolamento de tráfego interno.	Rede interna projetada sem confiança implícita, semelhante a uma rede externa. Todos os dispositivos precisam autenticar-se via 802.1x antes de obter acesso controlado.
RADIUS Server	Controle de acesso à rede e atribuição de VLANs.	Autentica dispositivos usando o protocolo 802.1x e os atribui dinamicamente a VLANs conforme seu status de gerenciamento e nível de confiança (gerenciado, convidado ou não reconhecido).
Access Proxy	Intermediação e proteção de acesso às aplicações.	Funciona como ponto único de entrada para aplicações internas e externas, aplicando criptografia, autenticação, controle de acesso, balanceamento de carga e proteção contra ataques de negação de serviço.
Access Control Engine (ACE)	Aplicação de políticas de autorização.	Avalia políticas de acesso com base na identidade do usuário, no estado e no nível de confiança do dispositivo. Fornece decisões de autorização contextuais e granulares.
Trust Inference	Avaliação dinâmica de confiabilidade.	Determina continuamente o nível de confiança de usuários e dispositivos com base em múltiplas fontes de dados, como certificados, inventário, contexto e comportamento.
Pipeline	Atualização contínua das políticas de acesso.	Agrega e distribui informações em tempo real (dispositivos, usuários, certificados e níveis de confiança) para manter o mecanismo de controle de acesso sempre atualizado.
Certificate Issuer	Emissão e gerenciamento de certificados de dispositivos.	Emite e gerencia certificados digitais exclusivos para dispositivos corporativos, vinculando-os aos registros do inventário para garantir a verificação da identidade do dispositivo.

A Microsoft também se destacou com o Zero Trust Framework, que adota a identidade como novo perímetro de segurança, utilizando integração com o Azure Active Directory, autenticação multifator (MFA) e o Microsoft Endpoint Manager para controle de dispositivos e políticas (CORPORATION, 2021). Já a Fortinet incorporou o ZTNA de forma nativa ao sistema operacional FortiOS, permitindo que seus firewalls atuem como ponto de aplicação de políticas granulares, centralizando autenticação, controle e monitoramento de sessões (FORTINET, 2022).

Outros provedores especializados, como Netskope e Zscaler, avançaram no modelo de ZTNA ao integrar inspeção de tráfego em tempo real e controle contextual de aplicações em nuvem, oferecendo soluções voltadas para ambientes distribuídos e híbridos (NETSKOPE, 2022) e (ZSCALER, 2025). Apesar das diferenças entre as arquiteturas, todos esses modelos seguem os mesmos princípios fundamentais do Zero Trust: identidade, contexto e microssegmentação, como base para controle adaptativo e acesso mínimo necessário.

A adoção do ZTNA traz benefícios amplamente reconhecidos na literatura. Entre eles, destaca-se a redução da superfície de ataque, já que os usuários não possuem visibilidade completa da rede, apenas dos recursos autorizados. Além disso, há uma mitigação de riscos associados a credenciais comprometidas, pois o acesso é continuamente e dinamicamente validado, impedindo movimentações laterais de invasores. O modelo também favorece a adequação à computação em nuvem e a mobilidade, sendo compatível com SaaS, IaaS e infraestruturas híbridas, e melhora a experiência do usuário ao substituir VPNs tradicionais por conexões mais leves e seguras. Desse modo, o ZTNA proporciona melhor governança e auditoria, permitindo rastreabilidade detalhada das ações e dos recursos acessados em tempo real.

2.5 *Normas, Regulamentações e Compliance*

A segurança da informação em redes corporativas não pode ser compreendida apenas sob o ponto de vista tecnológico. Ela depende igualmente da conformidade com normas, regulamentações e legislações nacionais e internacionais que orientam as organizações quanto às melhores práticas e aos requisitos mínimos para a proteção de dados e de infraestruturas críticas. Nesse cenário, tecnologias como ZTNA (Zero Trust Network Access), VPNs e firewalls de próxima geração desempenham papel essencial para garantir conformidade regulatória, ainda que apresentem desafios quanto à sua integração e operacionalização (ROSE et al., 2020).

2.5.1 Normas ISO/IEC 27000 e NIST SP 800-207

A ISO/IEC 27001 é amplamente reconhecida como a principal norma internacional para gestão da segurança da informação, oferecendo requisitos para o estabelecimento,

implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI) com base no ciclo PDCA (Plan-Do-Check-Act) (VANZOLINI, 2024). A certificação ISO/IEC 27001 está associada a ganhos significativos de desempenho, produtividade e reputação organizacional. Entretanto, os autores apontam desafios relacionados ao custo de implementação e à integração com outras normas.

A ISO/IEC 27002, norma complementar, detalha controles técnicos e operacionais aplicáveis a tecnologias de segurança. O Controle A.9 relaciona-se à autenticação multifatorial e à segmentação de usuários, princípios fundamentais do modelo Zero Trust. Já o Controle A.12 abrange a gestão de vulnerabilidades, monitoramento e uso de firewalls e sistemas como Intrusion Detection Systems (IDS) e Intrusion Prevention System (IPS) ((ISO); (IEC), 2022). A adoção dessas normas é frequentemente exigida em contratos corporativos e licitações públicas como diferencial competitivo.

O National Institute of Standards and Technology (NIST) tem papel central na definição de padrões de segurança nos Estados Unidos. A publicação NIST SP 800-207, intitulada Zero Trust Architecture, uma das principais referências deste trabalho, define os fundamentos do modelo Zero Trust, com ênfase em autenticação contínua, princípio do menor privilégio e visibilidade total sobre usuários, dispositivos e cargas de trabalho (ROSE et al., 2020).

2.5.2 LGPD e GDPR

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) estabelece um marco regulatório essencial para o tratamento de dados pessoais no Brasil, com foco em garantir a privacidade, a segurança e os direitos dos titulares. Inspirada na General Data Protection Regulation (GDPR) da União Europeia (UNION, 2016), a LGPD consolida princípios como a finalidade, necessidade, transparência, adequação e responsabilização, exigindo que organizações adotem medidas de governança e segurança da informação. O artigo 46 da LGPD determina a obrigatoriedade de medidas técnicas e administrativas que assegurem a proteção contra acessos não autorizados, destruição acidental ou ilícita e outras formas de tratamento inadequado. Já o artigo 50 incentiva a implementação de boas práticas e certificações como evidência de conformidade e comprometimento com a proteção de dados (BRASIL, 2018). Assim como a GDPR, a LGPD promove um ambiente regulatório que busca equilibrar o uso legítimo das informações com a preservação da privacidade individual e a transparência nas relações entre empresas, governos e cidadãos.

Apesar dos avanços, desafios persistem quanto à maturidade organizacional, à conscientização dos colaboradores e à integração da cultura de privacidade nas práticas empresariais. Nesse contexto, a efetividade da LGPD, assim como da GDPR, depende não apenas de conformidade legal, mas de uma mudança estrutural na forma como as

instituições tratam, armazenam e compartilham informações pessoais, sendo a adoção do modelo zero trust um método essencial para evitar vazamentos de informações.

2.5.3 Desafios de Compliance

Apesar da ampla normatização existente no campo da segurança cibernética, a conformidade regulatória em ambientes baseados no modelo Zero Trust ainda enfrenta desafios relevantes. Um dos principais obstáculos é a complexidade decorrente da multiplicidade de frameworks e diretrizes internacionais, como o NIST SP 800-207 (Zero Trust Architecture), a ISO/IEC 27001:2022 e ISO/IEC 27002:2022, que embora complementares, apresentam enfoques e métricas distintas em alguns casos. Essa fragmentação dificulta a implementação de um arcabouço unificado de segurança e pode gerar inconsistências entre políticas de acesso, autenticação e monitoramento contínuo. Além disso, observa-se uma defasagem regulatória frente à rápida evolução tecnológica que envolve o Zero Trust, especialmente diante da expansão de ambientes híbridos, da integração de IoT e da adoção crescente de arquiteturas de borda e microsserviços, contextos que exigem controles mais dinâmicos e contextualizados.

Outro desafio relevante refere-se à superficialidade das auditorias e avaliações de conformidade, muitas vezes voltadas apenas para a validação formal de políticas e não para a eficácia real dos mecanismos de segurança. Em diversas organizações, a adoção do Zero Trust ainda se limita à substituição de tecnologias legadas ou à implementação de autenticação multifatorial, sem o amadurecimento dos princípios fundamentais de verificação contínua, microssegmentação e avaliação contextual de risco. Nessa perspectiva, o compliance deve ser compreendido como parte integrante de uma estratégia de segurança adaptativa e resiliente, orientada não apenas ao atendimento de requisitos normativos, mas à melhoria contínua da postura de segurança e à redução de riscos. Assim, a conformidade no contexto ZTNA deve consolidar-se como um elemento operacional estratégico, sustentando a confiabilidade e a governança corporativa em ecossistemas distribuídos.

3 METODOLOGIA

Este capítulo apresenta a metodologia utilizada para o desenvolvimento deste trabalho, caracterizada por uma abordagem qualitativa, exploratória e bibliográfica, buscando compreender e comparar os modelos de segurança VPN (Virtual Private Network) e ZTNA (Zero Trust Network Access), com o intuito de propor um guia de boas práticas para adoção do modelo Zero Trust em redes corporativas.

3.1 *Tipo de Pesquisa e Abordagem*

A pesquisa é de natureza exploratória, pois busca aprofundar o entendimento sobre os conceitos, princípios e implicações da transição de modelos tradicionais de segurança (como VPNs e firewalls) para arquiteturas baseadas em Zero Trust. Segundo (MARCONI; LAKATOS, 2019), a pesquisa exploratória tem como finalidade proporcionar maior familiaridade com o problema, tornando-o mais explícito e passível de investigação científica.

Além disso, caracteriza-se como uma pesquisa bibliográfica, pois fundamenta-se em material já publicado, incluindo artigos científicos, livros, normas técnicas e relatórios institucionais. Tendo como base a análise de produções existentes, com o objetivo de extrair, comparar e consolidar informações relevantes sobre o tema estudado.

A abordagem empregada é qualitativa, centrada na análise interpretativa dos conceitos e práticas de segurança cibernética sob a ótica do modelo Zero Trust. Dessa forma, o estudo não visa mensurar desempenho técnico das soluções, mas sim analisar criticamente princípios, benefícios, riscos e boas práticas, com base na literatura científica e nas normas reconhecidas internacionalmente.

3.2 *Fontes, Coleta e Critérios de Seleção dos Dados*

Foram consideradas fontes de natureza acadêmica, técnica e normativa, conforme o recorte do tema. As fontes acadêmicas compreenderam artigos científicos de bases como IEEE, arXiv, MDPI e outros, com ênfase em publicações realizadas entre 2019 e 2025, período em que o conceito de Zero Trust Network Access consolidou-se como tendência global em segurança corporativa.

As fontes técnicas e institucionais incluíram relatórios e guias elaborados por entidades e fabricantes de referência no setor de cibersegurança, como o NIST, Forrester, Gartner, Cisco, Fortinet, Hillstone, Google, Microsoft e outros. Complementarmente, foram

consultados documentos normativos e padrões de segurança, como o NIST SP 800-207 (Zero Trust Architecture), ISO/IEC 27001 e 27002, Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) e o Regulamento Geral de Proteção de Dados (GDPR).

A pesquisa documental foi realizada por meio de consultas a bibliotecas digitais, portais institucionais e bases de dados especializadas, utilizando palavras como "Zero Trust", "ZTNA", "VPN vulnerabilities", "network security", "access control", "Zero Trust implementation" e "corporate cybersecurity". Para assegurar a qualidade e a validade das informações, foram aplicados critérios de seleção baseados em relevância, atualidade, aplicabilidade e confiabilidade das fontes, conforme demonstrado na tabela a seguir.

Tabela 2 – Critérios de seleção das fontes de pesquisa.

Critério	**Descrição**	**Exemplo de aplicação**
Relevância	Obras e artigos reconhecidos por órgãos científicos ou entidades de cibersegurança.	NIST, Forrester, Gartner, IEEE e outros.
Atualidade	Publicações preferencialmente dos últimos cinco anos (2019–2025).	Estudos recentes sobre ZTNA e tecnologias correlatas.
Aplicabilidade corporativa	Fontes com aplicabilidade prática em ambientes empresariais e políticas de segurança.	Guias e white papers da Fortinet, CheckPoint, Cisco, Google, Microsoft e outros.
Confiabilidade	Autores e instituições reconhecidos por rigor técnico e autoridade no tema.	ISO, NIST, Gartner e outros.

3.3 *Técnica de Análise dos Dados e Limitações do Estudo*

Os dados coletados foram tratados por meio de análise qualitativa e comparativa, com o objetivo de identificar padrões, lacunas e boas práticas entre os modelos VPN, ZTNA e tecnologias associadas.

A análise foi estruturada em quatro etapas:

- **Revisão conceitual:** levantamento das definições, princípios e fundamentos teóricos de cibersegurança, VPN, firewall, ZTA, ZTNA e tecnologias associadas.
- **Mapeamento de riscos:** identificação de vulnerabilidades documentadas e associadas a cada tecnologia.
- **Comparação entre modelos:** avaliação das diferenças arquiteturais, vantagens e limitações entre VPN e ZTNA.

- **Derivação de boas práticas:** elaboração de um guia de recomendações com base nos princípios do Zero Trust e nas diretrizes do NIST SP 800-207.

Como este trabalho adota uma abordagem teórica e bibliográfica, não inclui experimentação prática e nem medições quantitativas de desempenho. Assim, as conclusões baseiam-se na interpretação crítica da literatura técnica e acadêmica consultada, o que pode implicar limitações quanto à generalização dos resultados.

4 RESULTADOS E DISCUSSÕES

Este capítulo apresenta o resultado consolidado desta pesquisa e propõe um guia técnico de boas práticas para a adoção do Zero Trust Network Access (ZTNA) em redes corporativas, com base em normas internacionais, artigos científicos e relatórios de mercado e dos principais vendors da solução.

O propósito é demonstrar como a arquitetura Zero Trust pode substituir gradualmente os modelos tradicionais de segurança baseados em perímetro, especialmente as VPNs, promovendo um ambiente mais resiliente, escalável e conforme às exigências regulatórias atuais.

A partir da revisão bibliográfica e do estudo comparativo, foi possível desenvolver um conjunto de práticas técnicas, divididas em seis dimensões centrais: planejamento e estratégia, arquitetura e implementação, ecossistema tecnológico, gestão operacional, roadmap de adoção, seleção do fornecedor e discussão crítica dos resultados.

4.1 *Planejamento e Estratégia*

A adoção de uma arquitetura Zero Trust não deve ser encarada como um projeto exclusivamente técnico, mas como uma mudança estratégica e cultural dentro da organização. Antes da implementação, é fundamental estabelecer diretrizes de governança, avaliar a maturidade da segurança da informação e garantir o alinhamento entre a alta gestão, os objetivos de negócio e as exigências de compliance.

4.1.1 Avaliação de Maturidade Organizacional

A maturidade organizacional em segurança pode ser avaliada com base em frameworks reconhecidos como o Cybersecurity Capability Maturity Model (C2M2) (CYBERSECURITY; RESPONSE, 2022) e o NIST Cybersecurity Framework (CSF) (STANDARDS; TECHNOLOGY, 2024). Ambos têm como foco a adoção de práticas de gestão de segurança voltadas aos ativos e operações de tecnologia da informação, permitindo assim aprimorar as capacidades de segurança cibernética, avaliar o nível atual de maturidade e disseminar boas práticas. Esses modelos classificam o nível de maturidade em estágios que vão de Inicial a Otimizado (melhoria contínua).

Tabela 3 – Níveis de maturidade em segurança Zero Trust.

Nível	**Características principais**	**Riscos típicos**
Inicial	Controles reativos, ausência de padronização, políticas fragmentadas e foco apenas em correção de incidentes.	Falta de visibilidade, vulnerabilidades não identificadas, alto risco de ataques internos e externos.
Intermediário	Políticas formais, integração parcial entre sistemas, início de adoção de IAM e ferramentas de monitoramento.	Gaps entre políticas e execução real, inconsistências de configuração e exposição residual significativa.
Avançado	Monitoramento centralizado, IAM e MFA implementados, microssegmentação parcial, auditoria contínua.	Dependência tecnológica, aumento de custos operacionais e necessidade de processos mais maduros.
Otimizado	Cultura de segurança consolidada, automação com SOAR/XDR, políticas baseadas em contexto e revisões estruturadas.	Necessidade de revisão contínua das políticas devido à complexidade do ambiente e evolução das ameaças.

A partir dessa análise, a organização deve definir um plano de evolução de maturidade contínuo, priorizando controles essenciais como autenticação multifatorial, microsegmentação, gestão de identidade e monitoramento contínuo.

4.1.2 Escopo e Governança

A governança de segurança da informação constitui um dos pilares fundamentais para o sucesso da adoção do modelo Zero Trust. Mais do que um conjunto de diretrizes técnicas, a governança deve ser entendida como um mecanismo de coordenação estratégica, responsável por alinhar políticas de segurança, processos organizacionais e requisitos legais de proteção de dados.

A estrutura de governança deve ser formalizada por meio de uma Política Corporativa de Zero Trust, este documento deve definir princípios, papéis e responsabilidades institucionais. Essa política deve abranger:

- Identificação e classificação dos ativos críticos, incluindo aplicações, sistemas, dados sensíveis e usuários com privilégios administrativos;
- Mapeamento dos fluxos de informação entre ambientes on-premises, nuvem pública, privada e híbrida, permitindo a definição de controles de acesso adequados a cada contexto operacional;

- Estabelecimento de uma estrutura hierárquica de comando, composta por papéis como o Chief Information Security Officer (CISO), gestores de rede e infraestrutura, administradores de identidade e acesso (IAM) e auditores de compliance;
- Definição de mecanismos de auditoria e prestação de contas, assegurando que as decisões e ações relacionadas à segurança sejam rastreáveis e documentadas.

Uma governança efetiva pressupõe, ainda, integração entre as áreas técnicas, jurídicas e administrativas. Esse alinhamento é essencial para garantir que os controles técnicos implementados estejam em conformidade com as normas regulatórias vigentes, como a LGPD no caso do Brasil. Desse modo, é necessário instituir uma cultura organizacional voltada à responsabilidade compartilhada pela proteção de dados e continuidade dos negócios.

4.2 *Arquitetura e Implementação do ZTNA*

A implementação da arquitetura Zero Trust é condicionada a etapas e soluções complementares, o ZTNA assume que nenhum usuário ou dispositivo é confiável por padrão, exigindo autenticação e autorização a cada solicitação de acesso. Essa arquitetura combina tecnologias de identidade, contexto, visibilidade e controle, articuladas por meio de políticas dinâmicas.

4.2.1 Microssegmentação

A microssegmentação consiste na divisão lógica da rede corporativa em segmentos menores, independentes e controlados, nos quais são aplicadas políticas específicas de autenticação, autorização e monitoramento. Diferentemente da segmentação tradicional baseada em VLANs ou sub-redes, a microssegmentação adota uma abordagem baseada em identidade, contexto e risco, permitindo o controle de comunicação entre workloads, usuários e aplicações de forma granular e dinâmica.

O principal objetivo dessa técnica é restringir o movimento lateral de ameaças, ou seja, impedir que um atacante que obtenha acesso a uma parte da rede consiga explorar vulnerabilidades em outros sistemas ou serviços.

Boas práticas técnicas para implementação:

- **Segmentação baseada em identidade e contexto:** a associação de políticas deve ocorrer com base em atributos do usuário, do dispositivo e da aplicação, e não em endereços IP estáticos. Isso garante escalabilidade e compatibilidade com ambientes híbridos e multi-cloud;

- **Adoção de políticas "deny-all" por padrão:** toda comunicação interna deve ser bloqueada inicialmente, sendo permitidos apenas os fluxos explicitamente autorizados conforme a necessidade de negócio. Essa abordagem segue o princípio do menor privilégio (Least Privilege), central ao modelo Zero Trust;
- **Implementação de visibilidade leste-oeste:** diferentemente do tráfego norte-sul (entre usuários e a internet), o tráfego leste-oeste ocorre entre sistemas internos e é frequentemente explorado por atacantes após uma invasão inicial.

4.2.2 Identidade como Perímetro e Políticas Baseadas em Contexto

A identidade, seja de usuários, dispositivos, aplicações ou serviços torna-se um dos elementos centrais da avaliação, cada tentativa de acesso é tratada como potencialmente maliciosa, independentemente de sua origem interna ou externa, e deve ser continuamente validada. A avaliação da solicitação de acesso ocorre de forma contextual, considerando múltiplos parâmetros simultâneos, tais como:

- Credenciais e atributos de autenticação do usuário e da aplicação;
- Integridade, postura de segurança e conformidade do dispositivo utilizado;
- Localização geográfica, rede de origem e possíveis indicadores de risco;
- Horário e padrões históricos de comportamento do usuário;
- Sensibilidade e criticidade do recurso solicitado.

Essas variáveis alimentam mecanismos de decisão que operam com base em políticas dinâmicas. Nesse processo, um Policy Decision Point (PDP) analisa o nível de risco em tempo real e determina se o acesso deve ser concedido, negado ou se deve exigir verificações adicionais. Já o Policy Enforcement Point (PEP) executa a decisão, garantindo que somente requisições autenticadas, autorizadas e compatíveis com o contexto operacional sejam permitidas.

Com essa abordagem unificada de identidade e contexto, cada requisição é tratada como suspeita até que se prove segura, reforçando a segurança por meio de verificações contínuas e minimizando a superfície de ataque em arquiteturas ZTNA.

4.2.3 Autenticação Multifatorial (MFA) e Monitoramento Contínuo

A MFA aumenta a confiabilidade do processo de autenticação ao exigir múltiplas provas de identidade, como senha, token, biometria ou certificado digital, isso permite reduzir significativamente o risco de comprometimento de credenciais. Ao combinar fatores

distintos, a probabilidade de acesso não autorizado diminui mesmo quando um dos elementos é violado.

Complementarmente, o monitoramento contínuo garante a avaliação permanente e contextual das atividades na infraestrutura. Possibilitando correlacionar eventos em tempo real e com isso a execução de bloqueios de acesso, isolamento de ativos e aplicação de contramedidas, contribuindo diretamente para a redução do Mean Time to Respond (MTTR).

Recomendações de adoção:

- Tornar a MFA obrigatória, especialmente para contas com privilégios elevados;
- Implementar autenticação adaptativa baseada em contexto, considerando geolocalização, dispositivo, horário e nível de risco;
- Registrar e analisar logs de autenticação e acesso para auditoria e investigação;
- Correlacionar eventos de identidade, rede e uso de aplicações;
- Automatizar respostas a incidentes para mitigar rapidamente atividades suspeitas.

4.3 *Tecnologias que compõem o Ecossistema Zero Trust*

A efetividade de uma arquitetura Zero Trust depende não apenas dos princípios conceituais, mas também da integração entre múltiplas tecnologias de segurança, que juntas possibilitam a formação de um ecossistema ZTNA completo e responsivo. Essas tecnologias atuam de maneira orquestrada para assegurar autenticação, visibilidade, resposta a incidentes e proteção contínua de dados e usuários.

O ecossistema do ZTNA pode ser constituído por quatro camadas principais: controle de identidade, proteção de endpoints, visibilidade e resposta, e segurança em nuvem, as mesmas são apresentadas a seguir.

4.3.1 Controle de Identidade e Acesso

O gerenciamento de identidade é realizado por ferramentas de Identity and Access Management (IAM) que centralizam autenticações e autorizações, permitindo aplicar políticas baseadas em papéis e contexto. Essas soluções devem ser integradas a serviços de autenticação federada (como SAML, OAuth e OpenID Connect), garantindo interoperabilidade com aplicações locais e em nuvem.

Em junção o Single Sign-On (SSO) simplifica o processo de autenticação, reduzindo vetores de ataque por senhas fracas e melhorando a experiência do usuário. Adicionalmente,

o uso de Role-Based Access Control (RBAC) assegura que cada usuário possua acesso apenas aos recursos necessários para suas funções, conforme o princípio do menor privilégio. O controle de identidade também deve ser complementado por ferramentas de Privileged Access Management (PAM), que restringe e audita o uso de credenciais administrativas, eliminando riscos de abuso de privilégio.

4.3.2 Proteção e Monitoramento de Endpoints

Os endpoints: laptops, smartphones, servidores e dispositivos IoT, são pontos críticos na superfície de ataque, para garantir e avaliar o nível de segurança dos mesmos usa-se tecnologias de Endpoint Detection and Response (EDR) e Endpoint Protection Platforms (EPP), essas ferramentas realizam análise comportamental, bloqueiam processos suspeitos e isolam dispositivos comprometidos automaticamente. Ao serem integradas ao SIEM e ao NAC (Network Access Control), permitem ações como:

- Bloqueio de acesso de dispositivos não conformes;
- Quarentena automática de máquinas infectadas;
- Correlação de alertas para detecção de ataques coordenados.

Além disso, políticas de Bring Your Own Device (BYOD) devem ser controladas por soluções de Mobile Device Management (MDM), garantindo que apenas dispositivos registrados e compatíveis possam acessar os recursos corporativos.

4.3.3 Visibilidade e Análise Centralizada

O monitoramento unificado é garantido pela integração de Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) e Extended Detection and Response (XDR).

- O SIEM coleta e correlaciona logs de dispositivos, aplicações e redes, permitindo análises forenses e auditorias;
- O SOAR automatiza processos de resposta, reduzindo o tempo médio de contenção de incidentes;
- O XDR amplia o alcance da detecção ao integrar dados de endpoints, tráfego de rede e nuvem, utilizando técnicas de machine learning para identificação de ameaças complexas.

Boas práticas operacionais:

- Definir dashboards de monitoramento com indicadores de conformidade e risco;
- Correlacionar logs de autenticação, tráfego e aplicação e usá-los como base na criação de regras.
- Realizar revisões semanais ou diárias de alertas críticos, além de auditorias mensais sobre o funcionamento dos sistemas.

4.3.4 Segurança em Nuvem e Tráfego Web

Com a quantidade de sistemas e aplicações operados em nuvem, é essencial garantir o controle e a visibilidade do tráfego entre usuários, aplicações SaaS e ambientes híbridos.

O Cloud Access Security Broker (CASB) atua como intermediário entre o usuário e as aplicações em nuvem, aplicando políticas de segurança, criptografia e prevenção contra perda de dados (Data Loss Prevention – DLP). O Secure Web Gateway (SWG), por sua vez, monitora e filtra o tráfego HTTP/HTTPS, bloqueando sites maliciosos, downloads suspeitos e violações de política. Essas ferramentas integradas permitem a inspeção completa do tráfego de rede, independentemente da localização do usuário.

Essas soluções são frequentemente complementadas por arquiteturas de Secure SD-WAN (Secure Software Defined Wide Area Networking), que unem desempenho de conectividade e segurança, permitindo priorização de tráfego e inspeção profunda de pacotes (Deep Packet Inspection – DPI) sem perda significativa de performance.

4.4 *Gestão Operacional*

A fase de gestão operacional é contínua e visa manter o ambiente ZTNA eficiente, atualizado e resiliente. Essa etapa requer automação, métricas e conscientização organizacional.

4.4.1 Indicadores de Desempenho

Os indicadores de desempenho (KPIs) são fundamentais para medir a efetividade do modelo Zero Trust em uma organização, a partir deles é possível mensurar e aplicar melhorias na infraestrutura. Esses indicadores devem ser revisados periodicamente e reportados à governança de segurança como parte das auditorias internas, as metas sugeridas são baseadas em benchmarks dos principais fabricantes e devem ser alteradas para níveis melhores de acordo com o nível de maturidade da organização.

Tabela 4 – Indicadores de desempenho recomendados para ambientes Zero Trust.

Indicador	**Descrição**	**Meta sugerida**
MTTD (Mean Time to Detect)	Tempo médio para detecção de incidentes de segurança, considerando logs, alertas e telemetria correlacionada.	< 24 horas
MTTR (Mean Time to Respond)	Tempo médio necessário para resposta e recuperação após a identificação de um incidente.	< 48 horas
Taxa de conformidade de dispositivos	Percentual de endpoints que estão em conformidade com as políticas de segurança definidas (patches, antivírus, ERD ativo, configuração).	$\geq 95\%$
Taxa de cobertura de microsegmentação	Percentual de workloads, servidores e aplicações já protegidos por políticas de microsegmentação.	$\geq 90\%$
Taxa de detecção de ameaças	Percentual de ameaças detectadas pelas soluções de SIEM, EDR e sistemas de análise comportamental antes de impacto operacional.	$\geq 90\%$
Taxa de falsos positivos	Percentual de alertas incorretos gerados por ferramentas de segurança, como SIEM, EDR ou EPP.	$\leq 5\%$
Tempo de provisionamento IAM	Tempo médio necessário para ativar, ajustar ou revogar o acesso de um usuário autorizado no sistema de identidade.	≤ 15 minutos
SLA do Serviço ZTNA	Percentual de disponibilidade do serviço de acesso Zero Trust fornecido pela solução utilizada (on-premises ou cloud).	$\geq 99,9\%$

4.4.2 Roadmap de Adoção do ZTNA

A adoção do ZTNA deve seguir um processo incremental e controlado, com etapas bem definidas. O roadmap abaixo descreve a adoção em cinco fases principais, associando objetivos, atividades, desafios e resultados esperados.

Tabela 5 – Roadmap para adoção do ZTNA.

Fase	**Objetivo**	**Atividades Principais**	**Desafios**	**Resultados Esperados**
1. Planejamento Estratégico	Definir escopo e visão do modelo Zero Trust.	Mapeamento de ativos, análise de maturidade (NIST CSF/C2M2), definição de políticas iniciais de identidade e fluxos que serão migrados para ZTNA.	Inventário incompleto e falta de alinhamento entre áreas.	Escopo definido, requisitos claros e diretrizes iniciais estabelecidas.
2. Projeto Piloto	Validar o ZTNA em ambiente restrito.	Implantação de IAM/MFA, políticas contextuais, conectores ZTNA e microsegmentação inicial.	Compatibilidade com sistemas legados e ajustes de políticas.	Modelo validado, telemetria disponível e políticas ajustadas.
3. Expansão Operacional	Escalar o ZTNA para toda a organização.	Integração com SD-WAN, CASB, SWG e SIEM; expansão de microssegmentação; substituição gradual de VPN.	Complexidade de integração e custos de licenciamento.	Cobertura ampla de usuários/aplicações e redução da superfície de ataque.

Tabela 5 – Roadmap para adoção do ZTNA.

Fase	**Objetivo**	**Atividades Principais**	**Desafios**	**Resultados Esperados**
4. Operação Contínua	Manter estabilidade e eficácia da arquitetura.	Monitoramento de KPIs (MTTD/MTTR), revisão periódica de políticas, análise de eventos e ajustes contínuos.	Risco de políticas desatualizadas e novas ameaças.	Ambiente otimizado, seguro e alinhado às necessidades operacionais.
5. Governança e Evolução Zero Trust	Garantir atualização contínua do modelo ZTNA.	Auditorias (LGPD/ISO 27001), testes Red Team, atualização de agentes e políticas, revisão anual de riscos, mitigação de vendor lock-in.	Rápida evolução tecnológica e necessidade de governança madura.	Modelo Zero Trust evolutivo, aderente a normas e resiliente a novas ameaças.

O ciclo é iterativo, e cada fase deve ser revista periodicamente para incorporar novas tecnologias e requisitos regulatórios. Durante o processo, recomenda-se a adoção de princípios de governança adaptativa, baseados em revisões contínuas, auditorias anuais e atualização de políticas conforme evolução da infraestrutura e do cenário de ameaças.

4.5 *Implementações de ZTNA pelos Principais Vendors*

A aplicação prática dos princípios de Zero Trust Network Access (ZTNA) varia conforme a arquitetura e o portfólio tecnológico de cada fabricante. Embora todos se baseiem nos fundamentos estabelecidos pelo NIST SP 800-207 (ROSE et al., 2020), de autenticação contínua, controle contextual e microssegmentação, cada vendor adota estratégias distintas de integração, refletindo diferenças de foco entre infraestrutura, nuvem, endpoint ou aplicação.

4.5.1 Arquitetura e Modelo dos Principais Fabricantes

O quadro a seguir sintetiza a abordagem e arquitetura de alguns dos principais fornecedores de soluções ZTNA e seus respectivos diferenciais tecnológicos que auxiliam na tomada de decisão pela solução por parte de quem irá contratar o serviço.

Tabela 6 – Implementações de ZTNA pelos principais fornecedores.

Fabricante	**Arquitetura / Modelo**	**Principais Componentes**	**Diferenciais Técnicos**
Fortinet – FortiGate / FortiSASE / FortiClient	Arquitetura híbrida, combinando segurança de rede e endpoint.	FortiGate NGFW, FortiClient EMS, FortiAuthenticator, FortiAnalyzer, FortiSASE Cloud.	Integração nativa entre firewall, EDR e ZTNA; controle granular de acesso baseado em identidade; visibilidade unificada via FortiAnalyzer.
Hillstone Networks – Hillstone ZTNA Framework	Modelo centrado em rede, integrado ao sistema de prevenção de intrusão (NGFW).	Hillstone NGFW, Hillstone iSource e CloudEdge.	Integra ZTNA com IA comportamental; aplica políticas dinâmicas baseadas em contexto e risco; suporte a ambientes híbridos e multicloud.
Cisco – Cisco Secure Access / Duo / ISE	Arquitetura SASE (Secure Access Service Edge) native, com Zero Trust distribuído em identidade, rede e aplicação.	Cisco Secure Access, Cisco Duo MFA, ISE (Identity Services Engine), Umbrella (SWG/-CASB).	Forte ênfase em autenticação contínua e postura de dispositivo; integração com SD-WAN e Cloud Security; modelo adaptativo de confiança.

Tabela 6 – Implementações de ZTNA pelos principais fornecedores.

Fabricante	**Arquitetura / Modelo**	**Principais Componentes**	**Diferenciais Técnicos**
Netskope – Private Access / SASE Platform	Arquitetura cloud-native, 100% em nuvem, baseada em agentes de endpoint.	Netskope Private Access (NPA), Netskope Client, Cloud Exchange, Threat Labs.	Implementação leve e escalável de ZTNA; políticas contextuais; integração nativa com CASB, SWG e DLP.
Zscaler – ZPA / ZIA (Zero Trust Exchange)	Modelo Zero Trust Exchange, sem dependência de VPN ou gateway local.	Zscaler Private Access (ZPA), Zscaler Internet Access (ZIA).	Modelo totalmente em nuvem; isolamento de aplicações; autenticação contínua com visibilidade em tempo real e latência mínima.
Palo Alto Networks – Prisma Access / Cortex XDR	Arquitetura ZTNA 2.0, combinando acesso, análise e resposta.	Prisma Access, Cortex XDR, Cloud Identity Engine.	Abordagem centrada em identidade e comportamento; detecção automatizada via IA; integração total com SASE e SD-WAN.

A Fortinet aposta em um modelo híbrido de segurança unificada, onde o ZTNA é nativamente integrado ao firewall de próxima geração (NGFW). A política "identity-based access" é aplicada diretamente no FortiGate, associando usuários e dispositivos autenticados via FortiClient e FortiAuthenticator. Essa integração entre endpoint, gateway e nuvem é o diferencial da Fortinet, que reduz a necessidade de soluções externas para controle de identidade e microsegmentação.

A Hillstone Networks adota uma estratégia mais orientada à visibilidade comportamental e detecção inteligente, com o Hillstone iSource realizando análise de risco baseada em IA. Seu ZTNA se apoia fortemente na integração com soluções de Threat Intelligence, permitindo que as políticas de acesso sejam ajustadas dinamicamente conforme o comportamento dos usuários e dispositivos. O CloudEdge, por exemplo, estende esse controle

para ambientes multi-cloud.

A Cisco, por meio de sua arquitetura Secure Access, concentra-se na orquestração entre identidade, rede e nuvem. Ferramentas como o ISE (Identity Services Engine) implementam autenticação adaptativa e verificação de postura de dispositivo antes da concessão de acesso. O Umbrella, por sua vez, complementa o modelo com proteção de tráfego DNS, CASB e SWG. Essa abordagem torna a Cisco uma das soluções mais completas para ecossistemas corporativos complexos e distribuídos.

Netskope e Zscaler representam o modelo ZTNA 100% em nuvem (cloud-native), em que o acesso remoto é mediado por agentes instalados nos endpoints. No caso da Netskope Private Access (NPA), o controle é feito por meio de túneis criptografados dinâmicos que conectam usuários a aplicações específicas, sem expor a rede corporativa. Já o Zscaler Private Access (ZPA) opera em uma arquitetura de "Zero Trust Exchange", conectando usuários e aplicações diretamente via nuvem, o que reduz latência e aumenta a escalabilidade.

Palo Alto Networks, com sua plataforma Prisma Access, introduziu o conceito de ZTNA 2.0, que amplia o escopo do Zero Trust ao incluir análises de comportamento via IA e políticas baseadas em contexto em tempo real. O Cloud Identity Engine faz a mediação de identidade entre provedores diferentes, enquanto o Cortex XDR oferece detecção e resposta estendida, integrando acesso e monitoramento em um mesmo ecossistema.

4.5.2 Critérios Técnicos de Seleção

Ao comparar soluções comerciais, é recomendável utilizar uma matriz de critérios técnicos e funcionais, conforme o modelo baseado no Gartner (RILEY; MACDONALD; ORANS, 2020).

Tabela 7 – Critérios técnicos para avaliação de soluções ZTNA.

Critério	**Descrição**	**Indicadores recomendados**
Autenticação e Identidade	Suporte a IAM, SSO, MFA e autenticação adaptativa.	Protocolos SAML, OAuth 2.0, OpenID Connect.
Microsegmentação	Controle granular de acesso entre aplicações e usuários.	Políticas "deny-all" e segmentação lógica.
Monitoramento e Telemetria	Visibilidade completa de tráfego e eventos.	Integração com SIEM e logs de auditoria.

Tabela 7– Critérios técnicos para avaliação de soluções ZTNA.

Critério	**Descrição**	**Indicadores recomendados**
Escalabilidade	Capacidade de expansão e elasticidade em nuvem.	SLA 99,9%, balanceamento de carga.
Conformidade	Alinhamento a normas e regulações.	ISO/IEC 27001, NIST 800-207, LGPD.
Custo Total de Propriedade (TCO)	Custos diretos e indiretos (licenças, manutenção, suporte).	Pay-as-you-go, licenciamento por usuário.
Facilidade de Gestão	Interface centralizada e automação de políticas.	Console unificado, API aberta.
Integração com SASE	Compatibilidade com SD-WAN, CASB, SWG e DLP.	Arquitetura convergente SASE.

Com base nas boas práticas e nas tendências atuais de mercado, recomenda-se que as organizações iniciem sua jornada rumo ao Zero Trust Network Access (ZTNA) por meio de uma prova de conceito (PoC) focada em aplicações críticas e em um subconjunto representativo de usuários, permitindo avaliar desempenho, latência, requisitos de integração e eventuais impactos operacionais. É fundamental optar por soluções escaláveis e interoperáveis, evitando a dependência excessiva de um único fornecedor (vendor lock-in) e garantindo flexibilidade para evolução futura. A transição para o modelo Zero Trust deve ocorrer de forma gradual, começando pela implementação de mecanismos de autenticação robusta e microsegmentação, para depois avançar para monitoramento contínuo e automação de respostas.

Adicionalmente, a organização deve formalizar práticas de governança e estabelecer ciclos de revisão trimestral de políticas, assegurando aderência contínua aos princípios de Zero Trust e conformidade com normas e regulações aplicáveis. Dessa forma, a adoção do ZTNA deixa de ser tratada como um projeto isolado e passa a constituir um processo evolutivo da postura de segurança corporativa, integrando pessoas, processos e tecnologias em um ecossistema de confiança dinâmica, adaptativa e resiliente.

5 CONCLUSÃO

Este trabalho teve como objetivo principal analisar a transição dos modelos tradicionais baseados em VPN para arquiteturas fundamentadas no princípio de Zero Trust, propondo um guia de boas práticas para adoção do Zero Trust Network Access (ZTNA) em redes corporativas. A partir de uma revisão bibliográfica abrangente, de referenciais técnicos internacionais e da análise comparativa entre soluções de mercado, foi possível compreender as limitações dos modelos convencionais de segurança baseados em perímetro e evidenciar a necessidade de sistemas mais dinâmicos, contextuais e centrados em identidade para proteger ambientes corporativos modernos.

A pesquisa demonstrou que, embora as VPNs tenham desempenhado papel relevante durante décadas, especialmente em períodos como a pandemia de COVID-19, seu modelo de confiança implícita, aliado à falta de granularidade e dificuldade em escalar para ambientes distribuídos, tornou-se inadequada frente ao aumento de ataques cibernéticos avançados, à expansão de serviços em nuvem e à mobilidade dos colaboradores. Em contrapartida, o ZTNA apresenta uma abordagem mais robusta ao restringir o acesso a aplicações com base em identidade, contexto e postura de segurança, aplicando continuamente o princípio do menor privilégio e eliminando superfícies de ataque criadas por conexões sem restrições a rede.

O estudo promoveu uma revisão abrangente dos fundamentos que sustentam o modelo Zero Trust, com destaque para as contribuições teóricas de John Kindervag e para as diretrizes arquiteturais propostas pelo NIST SP 800-207. Também foram analisados os principais riscos associados ao uso de firewalls tradicionais e VPNs, incluindo vulnerabilidades críticas amplamente exploradas, que evidenciaram a fragilidade de modelos baseados em confiança implícita. Além disso, o trabalho examinou as tecnologias que compõem o ecossistema ZTNA, tais como IAM, MFA, microssegmentação, EPP, SD-WAN e outros, demonstrando como esses componentes se integram para formar uma arquitetura de segurança mais granular, contextual e orientada à identidade. Por fim, a elaboração do guia de boas práticas consolidou essas informações, oferecendo recomendações estruturadas para o planejamento, implementação, operação e otimização contínua da arquitetura Zero Trust, complementadas por indicadores de desempenho, critérios técnicos para seleção de fornecedores e um roadmap de adoção evolutiva.

Como principais contribuições acadêmicas e práticas, destaca-se que o trabalho fornece uma visão atualizada do estado da arte sobre Zero Trust e ZTNA, contextualizando sua adoção no cenário brasileiro e internacional, além de oferecendo um material orientativo aplicável a organizações de diferentes portes e níveis de maturidade. Os critérios técnicos

para avaliação de soluções, as tabelas comparativas, os riscos mapeados e o roadmap proposto servem como instrumentos para empresas que buscam iniciar ou aprimorar sua jornada em Zero Trust, auxiliando na tomada de decisão e reduzindo incertezas comuns nesse processo de transição.

Entretanto, este estudo também apresenta limitações. Em virtude da abordagem teórica, baseada em revisão bibliográfica e documental, impede a validação por meio de estudos de caso reais, experimentações laboratoriais ou testes comparativos entre soluções, que foram contornados pelos dados fornecidos pelos fabricantes. Além disso, o ritmo acelerado de evolução tecnológica faz com que arquiteturas de ZTNA sofram constantes atualizações, exigindo revisões frequentes para manutenção da aderência conceitual e técnica. Por fim, a análise de fornecedores, embora abrangente, poderia ser ampliada em pesquisas futuras com avaliação de desempenho a partir de testes das soluções comerciais, quando viável, seus custos e integração em ambientes corporativos reais.

Por fim, este estudo demonstrou que a adoção de ZTNA representa não apenas uma evolução tecnológica na área da cibersegurança, mas uma mudança estrutural na forma como as empresas encaram a segurança da informação. Ao substituir modelos baseados em perímetro por arquiteturas centradas em identidade, contexto e verificação contínua, as organizações ganham resiliência, visibilidade e capacidade de resposta, essenciais no cenário atual. Desse modo, a transição da VPN para o ZTNA, quando conduzida de forma estratégica e alinhada às melhores práticas, é uma etapa indispensável para fortalecer a postura de segurança corporativa em um cenário de ameaças cada vez mais sofisticadas e ambientes operacionais amplamente distribuídos.

REFERÊNCIAS

BASHI, Z. S. A.; SENAN, S. A comprehensive review of zero trust network architecture (ztna) and deployment frameworks. *International Journal on Perceptive and Cognitive Computing*, v. 11, n. 1, p. 148–153, 2025. Disponível em: https://journals.iium.edu.my/kict/index.php/IJPCC/article/view/494/327.

BHUJBAL, P. M. et al. Zero trust paradigm: Advancements, challenges, and future directions in cybersecurity. *International Journal of Intelligent Systems and Applications in Engineering*, 2024. Disponível em: https://ijisae.org/index.php/IJISAE/article/view/5105.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. 2018. Diário Oficial da União, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Check Point Research. *Q1 2025 Global Cyber Attack Report from Check Point Software: An Almost 50% Surge in Cyber Threats Worldwide, with a Rise of 126% in Ransomware Attacks*. 2025. Disponível em: https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/.

CISCO. *Verify Zero Trust Security Whitepaper*. 2024. Disponível em: https://www.cisco.com/c/en/us/support/docs/security-vpn/security-vpn/218443-verify-zero-trust-security-whitepaper.html. Atualizado 14 de Fevereiro de 2024; versão 2.0.

CORPORATION, M. *Zero Trust Guidance Center*. Redmond, WA: [s.n.], 2021. Microsoft Documentation Portal. Disponível em: https://learn.microsoft.com/en-us/security/zero-trust/.

CORPORATION, M. *CVE – Common Vulnerabilities and Exposures*. 2025. Disponível em: https://www.cve.org/.

CYBERSECURITY; (CISA), I. S. A. *Alert (AA20-107A): Exploitation of Pulse Secure VPN*. 2020. CISA Cybersecurity Alert. Disponível em: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-107a.

CYBERSECURITY, E. S. U.S. Department of Energy – Office of; RESPONSE, E. *Cybersecurity Capability Maturity Model (C2M2)*. 2022. Disponível em: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

FORTINET. *Zero Trust Network Access (ZTNA) with FortiOS*. Sunnyvale, CA: [s.n.], 2022. Fortinet White Paper. Disponível em: https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2022/fortinet-leads-evolution-converged-networking-security-new-fortios-innovations.

FORTINET. *What Is SSL VPN?* 2025. Fortinet Documentation Library. Disponível em: https://www.fortinet.com/resources/cyberglossary/ssl-vpn.

FRANKEL, S. E. *An Introduction to IPsec (Internet Protocol Security)*. 2001. NIST ITL Bulletin. Disponível em: https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2001-03.pdf.

Google. *BeyondCorp: A New Approach to Enterprise Security*. 2025. Disponível em: https://www.beyondcorp.com/.

(ISO), I. O. for S.; (IEC), I. E. C. *ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls*. 2022. ISO Standard. Disponível em: https://www.iso.org/standard/75652.html.

KINDERVAG, J.; BALAOURAS, S.; COIT, L. White Paper / Technical Report, *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*. 2010. Disponível em: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf. Atualizado em 17 setembro 2010.

LIU, C.; TAN, R.; LIU, Q. *Dissecting Zero Trust: Research Landscape and Its Implementation in IoT*. [S.l.]: SpringerOpen, 2024. 20 p. Disponível em: https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00212-0.

MARCONI, M. d. A.; LAKATOS, E. M. *Fundamentos de Metodologia Científica*. 9. ed. São Paulo: Atlas, 2019.

MEYER, C.; SCHWENK, J. *Lessons Learned From Previous SSL/TLS Attacks*. 2013. Cryptology ePrint Archive, Paper No. 2013/049. Disponível em: https://eprint.iacr.org/2013/049.pdf.

MIRKOVIC, J.; FENG, Y.; LI, J. *Measuring Changes in Regional Network Traffic Due to COVID-19 Stay-at-Home Measures*. 2022. Disponível em: https://arxiv.org/abs/2203.00742.

NETSKOPE. *ZTNA and SSE Architecture Overview*. Santa Clara, CA: [s.n.], 2022. Netskope White Paper. Disponível em: https://www.netskope.com/wp-content/uploads/2024/05/zero-trust-security-model-applied-to-netskope-intelligent-sse.pdf.

NETWORKS, P. A. *The History of Firewalls | Who Invented the Firewall?* 2025. Disponível em: https://www.paloaltonetworks.com/cyberpedia/history-of-firewalls.

NIST. *Guide to IPsec VPNs, NIST Special Publication 800-77, Revision 1*. 2020. NIST Special Publication 800-77, Revision 1. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf.

NIST. *Information Security — NIST Glossary*. 2024. Disponível em: https://csrc.nist.gov/glossary/term/information_security.

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.

RILEY, S.; MACDONALD, N.; ORANS, L. *Market Guide for Zero Trust Network Access*. 2020. Disponível em: https://www.gartner.com/en/documents/3986053.

ROSE, S. et al. Special Publication 800-207, *Zero Trust Architecture*. 2020. Disponível em: https://csrc.nist.gov/pubs/sp/800/207/final.

STALLINGS, W.; BROWN, L. *Segurança de Computadores: Princípios e Práticas*. 2. ed. Rio de Janeiro: Elsevier, 2014. ISBN 978-85-352-6449-4.

STANDARDS, N. I. of; TECHNOLOGY. *The NIST Cybersecurity Framework (CSF) 2.0*. 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

THIRUVASAGAM, P.; GEORGE, K. J. Ipsec: Performance analysis in ipv4 and ipv6. *Journal of ICT Standardization*, v. 7, n. 1, p. 59–76, 2019. Disponível em: https://journals.riverpublishers.com/index.php/JICTS/article/view/6407.

UNION, E. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. 2016. Official Journal of the European Union, L 119, p. 1–88. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

VAKA, P. R. Zero trust security model. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, v. 12, n. 6, p. 148–156, 2021. Disponível em: https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_12_ISSUE_6/IJARET_12_06_015.pdf.

VANZOLINI, F. C. A. *Sistema de Gestão de Segurança da Informação*. 2024. Site de notícias – Fundação Vanzolini. Disponível em: https://vanzolini.org.br/noticias/sistema-de-gestao-de-seguranca-da-informacao/.

VERIZON. *Data Breach Investigations Report (DBIR)*. 2022. Disponível em: https://www.verizon.com/business/resources/reports/2022-dbir-data-breach-investigations-report.pdf.

WARD, R.; BEYER, B. Beyondcorp: A new approach to enterprise security. *;login:*, USENIX Association, v. 39, n. 6, p. 6–11, 2014. Disponível em: https://www.usenix.org/system/files/login/articles/login_dec14_02_ward.pdf.

ZSCALER, I. *ZTNA: Redefining Secure Access for the Modern Era*. San Jose, CA: [s.n.], 2025. Zscaler White Paper. Disponível em: https://www.zscaler.com/resources/brochures/ztna-secure-access-for-modern-era.pdf.