Capítulo 2

Zero Trust Architecture para Dispositivos de Internet das Coisas e Redes de Próxima Geração: Ferramentas, Tendências e Desafios

Guilherme N. N. Barbosa (UFF), Martin Andreoni (TII),
Diogo M. F. Mattos (UFF)

Abstract

The exponential growth of connected devices and the complexity of emerging networking infrastructures increase digital security risks. The vulnerability of resource-constrained devices and the obsolescence of perimeter models hinder the adequate protection of data and services. This chapter surveys the adoption of Zero Trust Architecture (ZTA) as a solution to ensure continuous authentication, microsegmentation, and dynamic access policies in heterogeneous networks. The approach combines theoretical exposure with practical activities using the OpenZiti platform to implement services in a ZTA environment. The chapter discusses fundamentals of the architecture, identifies its main components, discusses the configuration of secure tunnels, and critically reflects on the challenges and opportunities of ZTA in next-generation networks. The chapter also explores real-world use cases in enterprise environments and federated networks.

Resumo

O crescimento exponencial de dispositivos conectados e a complexidade das infraestruturas de rede emergentes aumentam os riscos à segurança digital. A vulnerabilidade de dispositivos com recursos limitados e a obsolescência dos modelos perimetrais dificultam a proteção adequada de dados e serviços. Este capítulo examina a adoção da Arquitetura de Confiança Zero (Zero Trust Architecture - ZTA) como solução para garantir autenticação contínua, microsegmentação e políticas dinâmicas de acesso em redes heterogêneas. A abordagem combina exposição teórica com atividades práticas utilizando a plataforma OpenZiti para implementar serviços em um ambiente baseado em ZTA. O capítulo discute os fundamentos da arquitetura, identifica seus principais componentes, aborda a configuração de túneis seguros e propõe uma reflexão crítica sobre os desafios e as oportunidades da ZTA em redes de próxima geração. Também são explorados casos de uso reais em ambientes corporativos e redes federadas.

Este capítulo foi realizado com recursos do CNPq, CAPES, RNP e FAPERJ. Ferramentas de Inteligência Artificial Generativa, incluindo ChatGPT, Grammarly e Llama3.1, foram empregadas na revisão textual deste trabalho.

2.1. Introdução

A evolução das redes de computadores, impulsionada por tecnologias como Redes Definidas por *Software* (*Software Defined Networking* - SDN), Virtualização de Funções de Rede (*Network Function Virtualization* - NFV) e computação em nuvem, redefiniu o conceito de segurança, anteriormente centrado em perímetros físicos e esquemas tradicionais de autenticação e autorização. A virtualização e a descentralização tornaram obsoletas as abordagens baseadas em perímetro, impondo desafios mais complexos diante do acesso remoto e dinâmico de usuários [Jose Diaz Rivera et al., 2024]. Com a implementação da quinta geração (5G) dos sistemas de comunicação móvel, teve início uma nova era caracterizada por conectividade mais fluida, adaptável e de baixa latência. Essa transformação exigiu o fortalecimento das infraestruturas de rede, visando maior robustez e eficiência para suportar aplicações críticas com requisitos rigorosos de desempenho. Dentre os setores que mais se beneficiam dessa evolução destacam-se os veículos autônomos, a telecirurgia, as aplicações com drones e os sistemas de comunicação máquina a máquina (*Machine to Machine* - M2M), fundamentais no contexto da Internet das Coisas (*Internet of Things* - IoT), que já integra a infraestrutura digital conectando bilhões de dispositivos e promovendo avanços em áreas como saúde, mobilidade urbana e cidades inteligentes [Cunha Neto et al., 2024].

Projeções indicam que, até 2030, haverá cerca de 29 bilhões de dispositivos conectados à Internet [Gebresilassie et al., 2025]. Diante desse crescimento, torna-se imperativo o fortalecimento dos mecanismos de segurança, dado que esses dispositivos tendem a possuírem capacidades limitadas de proteção e se tornam vetores potenciais de ataques [Chen et al., 2023]. Tais vulnerabilidades expõem dados sensíveis a riscos crescentes, em um cenário regulado por legislações como a Lei Geral de Proteção de Dados (LGPD), no Brasil, e a *General Data Protection Regulation* (GDPR), na Europa. Embora amplamente difundida, a IoT impõe desafios crescentes, como privacidade, interoperabilidade, desempenho, regulamentação e confiança [Gebresilassie et al., 2025]. A heterogeneidade e distribuição dos dispositivos ampliam a superfície de ataque e dificultam a aplicação de soluções clássicas, como *firewalls* e sistemas de detecção de intrusão (*Intrusion Detection Systems* - IDS), sobretudo quando esses dispositivos compartilham redes locais com ativos críticos. Ademais, suas limitações computacionais frequentemente levam fabricantes a suprimir funcionalidades de segurança. A isso somam-se práticas como o uso corporativo de dispositivos pessoais (*Bring Your Own Device* – BYOD), o crescimento do teletrabalho e o uso de tecnologias de código aberto, ampliando os riscos e exigindo arquiteturas que tratem todos os dispositivos como potenciais ameaças.

Nesse cenário desafiador, o número de ciberataques tem aumentado significativamente em frequência e gravidade. Destacam-se os ataques de negação de serviço distribuído (*Distributed Denial of Service* - DDoS), viabilizados pela mobilização de bilhões de dispositivos comprometidos em redes *botnet*. Segundo relatório da Checkpoint[1], no primeiro trimestre de 2025, os ciberataques semanais aumentaram 47% em relação ao mesmo período de 2024. O Departamento de Ciência, Inovação e Tecnologia do Reino

[1]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`.

Unido[2] relata que 43% das empresas e 30% das instituições de caridade sofreram incidentes de segurança no último ano. Paralelamente, Grandes Modelos de Linguagem (*Large Language Models* - LLMs) e Modelos Compactos (*Small Large-Language Models* - SLMs) se tornaram alvos de exploração, dada sua integração em diversas aplicações cotidianas e sua integração a agentes autônomos de inteligência artificial. Técnicas adversariais vêm sendo desenvolvidas para explorar vulnerabilidades, inclusive por meio de transferência de ataques entre modelos abertos e fechados, explorando similaridades arquiteturais e de dados de treinamento [Kumar et al., 2024]. Outra ameaça emergente é a injeção de *prompt* (*prompt injection*), capaz de subverter instruções de forma maliciosa. Para mitigar esses riscos, são empregados mecanismos de segurança conhecidos como *guardrails*, embora estes ainda apresentem limitações diante de ataques sofisticados [de Oliveira et al., 2025].

Apesar da evolução tecnológica, muitas organizações ainda operam com modelos tradicionais de segurança centrados em perímetros físicos, com mecanismos centralizados de autenticação e controle de acesso. Essa abordagem baseia-se na premissa de confiança implícita, assumindo que dispositivos conectados à rede corporativa são confiáveis e que os serviços da rede são confiáveis. Contudo, esse modelo apresenta sérias limitações frente a ataques internos e à mobilidade crescente de usuários. A adoção de dispositivos móveis, a migração para a nuvem e a incorporação de dispositivos IoT romperam as fronteiras tradicionais, inviabilizando a segmentação baseada em localização física. A diversidade de dispositivos amplia a superfície de ataque e dificulta a aplicação de políticas uniformes. A visibilidade limitada sobre comportamentos e atividades, principalmente na rede interna, compromete a detecção de ameaças e a resposta a incidentes, exigindo modelos de proteção mais dinâmicos, contextuais e granulares.

Esse cenário evidencia a necessidade urgente de reformulação das estratégias de cibersegurança, com ênfase em novas tecnologias e práticas organizacionais. Tais estratégias devem incluir o fortalecimento de políticas, adoção novas arquiteturas e investimento contínuo na capacitação de profissionais, com foco na proteção de ativos estratégicos, privacidade e infraestrutura crítica [AlDaajeh e Alrabaee, 2024]. Ainda que campanhas de conscientização sejam relevantes, elas não são suficientes para induzir mudanças comportamentais duradouras [van Steen, 2025]. Com o avanço das regulamentações e estratégias nacionais, cresce a exigência por estruturas robustas de segurança e alinhamento com melhores práticas internacionais [Srinivas et al., 2019].

O *National Institute of Standards and Technology* (NIST) propôs a Arquitetura de Confiança Zero (*Zero Trust Architecture* - ZTA) como um novo paradigma de segurança [Sheikh et al., 2021, Zivi e Doerr, 2022]. A ZTA busca eliminar a confiança implícita por meio de autenticação contínua e validação rigorosa de cada tentativa de acesso. A arquitetura assume que qualquer segmento da rede pode ser comprometido, exigindo que cada solicitação seja autenticada, avaliada e autorizada dinamicamente [Zivi e Doerr, 2022]. Seus princípios fundamentais incluem autenticação robusta, controle de acesso baseado em políticas, verificação contínua e segmentação granular dos recursos. Adicionalmente, o conceito de Perímetro Definido por *Software* (*Software Defined Perimeter* -

[2]Disponível em: `https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025`.

SDP) e a microsegmentação são estratégias recomendadas pelo NIST [Syed et al., 2022].

A Arquitetura de Confiança Zero [Stafford, 2020] aprimora a segurança ao aplicar monitoramento contínuo, políticas rigorosas e autenticação contextual em toda a infraestrutura de Tecnologia da Informação e Comunicação (TIC). A Rede de Confiança Zero (*Zero Trust Networking* - ZTN) protege o tráfego de rede por meio de criptografia e segmentação, restringindo as comunicações a fluxos autorizados e seguros. Este capítulo aborda os fundamentos da ZTA e apresenta uma atividade prática de implantação de serviços utilizando a plataforma OpenZiti. O objetivo central do capítulo é contextualizar a arquitetura de confiança zero no aprimoramento da segurança de dispositivos IoT e redes de próxima geração, como redes além do 5G (*beyond 5G* - B5G) e 6G [Andreoni et al., 2022]. São discutidos os componentes essenciais da arquitetura, bem como os principais desafios de sua implementação. O capítulo adota uma abordagem técnico-prática, guiando os participantes na construção de um ambiente funcional baseado em ZTA com OpenZiti. Sua relevância está atrelada ao crescimento da IoT, à intensificação de ameaças de dia zero (*Zero Day Threats*) e à adoção do modelo BYOD [Anderson et al., 2022].

O restante do capítulo está organizado da seguinte forma. A Seção 2.2 apresenta a Arquitetura de Confiança Zero. Os principais componentes, soluções comerciais, taxonomia de aplicações e comparações entre modelos são discutidos na Seção 2.3. A Seção 2.4 descreve a implementação da ZTA, abordando técnicas e aspectos práticos. A Seção 2.5 traz um exemplo de aplicação da ZTA com a infraestrutura OpenZiti. Casos de uso reais são apresentados na Seção 2.6, e a Seção 2.7 explora projetos atuais de pesquisa e desenvolvimento. Desafios e tendências futuras são tratados na Seção 2.8, enquanto a Seção 2.9 conclui o capítulo.

2.2. Arquitetura de Confiança Zero (*Zero Trust Architecture*)

O conceito de (*Zero Trust*) representa uma mudança de paradigma na cibersegurança, afastando-se da lógica tradicional de confiança implícita (“confiar, mas verificar”) para o princípio de confiança por transação (“nunca confiar, sempre verificar”). Embora esse conceito tenha se popularizado a partir de 2020, com a publicação do arcabouço definido pelo NIST, sua ideia central remonta às discussões sobre a desperimetrização iniciadas pelo Jericho Forum em 2004. Esse grupo criticava a dependência de perímetros de rede seguros e discutia os desafios de manter simultaneamente os protocolos de segurança tradicionais e a disponibilidade dos serviços [Nace, 2020]. A formalização do modelo, no entanto, foi realizada por John Kindervag, então analista da Forrester Research, em seu relatório de 2010 intitulado "*No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*" [Kindervag et al., 2010]. Essencialmente, *Zero Trust* visa a eliminação da confiança implícita em qualquer parte da rede, independentemente de sua localização. Diferentemente dos modelos tradicionais, que assumem confiabilidade dentro do perímetro corporativo, o *Zero Trust* considera todo tráfego como potencialmente malicioso até que sua legitimidade seja verificada. Isso implica a verificação contínua de identidade, controle rigoroso de acesso, proteção persistente dos recursos e monitoramento detalhado de todas as atividades na rede. O conceito evoluiu ao ser integrado a arquiteturas como o *Secure Access Service Edge* (SASE) [Yiliyaer e Kim, 2022] e consolidado em políticas públicas, como a Ordem Executiva 14028 dos Estados Unidos, publicada em maio de 2021, que estabeleceu o *Zero Trust* como base para a modernização

da cibersegurança federal norte-americana [Alnoaimi e Alomary, 2025].

O Arquitetura de Confiança Zero (*Zero Trust Architecture* – ZTA), proposta pelo *National Institute of Standards and Technology* (NIST) [Stafford, 2020], constitui um paradigma baseado na premissa de que nenhuma entidade, seja usuário, dispositivo ou rede, deve ser implicitamente confiável. Essa abordagem adota um mecanismo de defesa com foco em **usuários, ativos e recursos individuais**, implementando verificações contínuas de identidade e autenticidade como critério para concessão de acesso. A transição do modelo de segurança atual, centrado em perímetros, para o modelo baseado em confiança zero é complexa, exigindo especialmente a reavaliação dos processos relacionados à segurança [Chen et al., 2023]. A autenticação e a autorização contínuas a cada solicitação aumentam a complexidade e requerem sistemas robustos de gerenciamento de identidade. Outro aspecto é a necessidade de todos os dispositivos manterem um nível mínimo de segurança, que deve ser monitorado e atualizado continuamente. A criptografia exerce papel essencial ao garantir a confidencialidade das comunicações, enquanto a microsegmentação permite dividir a rede em blocos menores, nos quais é possível aplicar políticas específicas. Essa estratégia não apenas limita os movimentos laterais de agentes maliciosos dentro da rede, mas também facilita o isolamento rápido de ameaças detectadas, especialmente em cenários envolvendo ataques do tipo *ransomware*. *Ransomware* é um tipo de *software* malicioso que, ao infectar um sistema, criptografa dados críticos e exige o pagamento de um resgate para restaurar o acesso. Esse tipo de ataque explora vulnerabilidades em dispositivos, aplicações ou credenciais, propagando-se rapidamente dentro das redes corporativas, especialmente quando há confiança implícita entre os elementos da infraestrutura. A ascensão e a popularização de *ransomware* nos últimos anos se devem à combinação de fatores como a ampliação da superfície de ataque, a interconectividade dos sistemas, o uso extensivo de dispositivos pessoais e o acesso remoto a ambientes sensíveis. Nesse contexto, a arquitetura tradicional baseada em perímetro se mostra insuficiente, pois assume confiabilidade interna e dificulta o isolamento de ameaças. A abordagem de confiança zero (*Zero Trust*), ao eliminar pressupostos de confiança e exigir autenticação e autorização contínuas para cada interação, torna-se essencial para conter movimentos laterais, limitar o escopo de comprometimento e viabilizar respostas rápidas e segmentadas a ataques de *ransomware*.

Os princípios que norteiam uma arquitetura de confiança zero são dinâmicos e adaptáveis, evoluindo conforme as ameaças cibernéticas se transformam, devendo ser agnósticos de tecnologias. São classificados como [Stafford, 2020]:

- **Todas as fontes de dados e serviços de computação são considerados recursos.** Uma rede pode incluir diversas classes de dispositivos. Uma organização pode optar por classificar dispositivos pessoais como recursos da empresa, caso estes tenham acesso a ativos corporativos.
- **Todas as comunicações são protegidas, independentemente da localização da rede.** Estar em uma rede corporativa não implica automaticamente confiança. Requisições de acesso, seja de dentro ou fora da infraestrutura, devem seguir os mesmos requisitos de segurança.
- **O acesso a recursos corporativos individuais é concedido por sessão.** A confi-

ança no solicitante é avaliada antes da concessão. O acesso deve ser concedido com o mínimo de privilégios necessários para a tarefa. Isso pode significar que o acesso foi concedido recentemente para a transação específica e não necessariamente imediatamente antes de iniciar a sessão ou transação. No entanto, a autenticação e autorização para um recurso não garantem automaticamente o acesso a outro recurso.

- **O acesso aos recursos é determinado por uma política dinâmica, podendo incluir outros atributos comportamentais e ambientais.** Uma organização protege seus recursos ao defini-los, identificando os membros envolvidos e estabelecendo os níveis de acesso necessários. No modelo de confiança zero, a identidade do usuário abrange a conta, os atributos associados e os artefatos utilizados para autenticação. O estado do dispositivo considera fatores como *software* instalado, localização geográfica, histórico de comportamento e credenciais. As políticas de acesso são baseadas em atributos do usuário, das propriedades do ativo e do ambiente, incluindo variáveis como localização e horário. As regras de acesso são alinhadas aos processos de negócios e ao nível de risco, adotando o princípio do menor privilégio para restringir visibilidade e acessibilidade de forma precisa e proporcional às necessidades operacionais.

- **A organização monitora e mede a integridade e a postura de segurança de todos os ativos próprios e associados.** Nenhum ativo é confiável por padrão. A segurança dos ativos é avaliada pela empresa durante o processamento de solicitações de acesso. Na implementação de uma arquitetura de confiança zero, torna-se essencial a adoção de um sistema contínuo de diagnóstico e mitigação (CDM) para monitorar dispositivos e aplicações, garantindo a aplicação de correções sempre que necessário. Ativos comprometidos, com vulnerabilidades conhecidas ou não gerenciados pela organização, podem ser submetidos a restrições severas, incluindo a negação de acesso a recursos corporativos. Essa abordagem também se estende a dispositivos pessoais, que podem ter acesso limitado a recursos específicos. Um sistema robusto de monitoramento e geração de relatórios é fundamental para fornecer informações precisas sobre o estado dos ativos da organização, permitindo ações proativas e baseadas em dados.

- **Toda autenticação e autorização de recursos são dinâmicas e rigorosamente aplicadas antes que o acesso seja permitido.** Um ciclo contínuo para acesso, avaliação de ameaças e adaptação constante da confiança na comunicação. Entidades que adotam a arquitetura de confiança zero devem implementar sistemas de gerenciamento de identidade, credenciais e ativos (ICAM), além de autenticação multifator (*Multi-Factor Authentication* - MFA) para acesso aos ativos. O monitoramento contínuo com reautenticação e reautorização ocorre em todas as transações, conforme definido pela política, visando equilibrar segurança, disponibilidade, usabilidade e custo.

- **Coleta do máximo de informações possível sobre o estado atual dos ativos, infraestrutura de rede e comunicações, utilizadas para aprimorar a segurança.** Uma organização deve coletar dados relacionados ao comportamento de segurança

dos ativos, como tráfego de rede e solicitações de acesso. Em seguida, processá-los e utilizar as percepções obtidas para aprimorar a criação e a aplicação de políticas de segurança. Esses dados podem ser usados para fornecer um contexto mais robusto nas avaliações de solicitações de acesso realizadas pelos usuários.

2.3. Principais Componentes da Arquitetura de Confiança Zero

O modelo de confiança zero é estruturado em diversos componentes lógicos, projetados para garantir que nenhuma entidade, interna ou externa, seja confiável por padrão. A interação entre esses componentes ocorre em um plano de controle dedicado, enquanto os dados das aplicações trafegam separadamente no plano de dados. Entre os principais componentes destacam-se o *Policy Decision Point* (PDP) e *Policy Enforcement Point* (PEP). O PDP é subdividido em dois elementos lógicos: o *Policy Engine (PE)* e o*Policy Administrator (PA)*. O *Policy Engine* é responsável por avaliar as políticas e determinar as decisões de acesso com base em atributos como identidade, contexto e regras predefinidas. Já o *Policy Administrator* implementa essas decisões, gerenciando as configurações de controle de acesso e aplicando as políticas nos componentes do plano de dados. Essa separação clara entre os planos de controle e de dados é essencial para garantir um gerenciamento seguro e eficiente dos recursos [Stafford, 2020]. Outro componente importante é o Algoritmo de Confiança (*Trust Algorithm* - TA), sendo esse utilizado para conceder ou negar acesso a um ativo. O TA recebe entradas de várias fontes, incluindo banco de dados de políticas, informações observáveis sobre os assuntos, padrões históricos de comportamento dos usuários, fontes de inteligência de ameaças e outros metadados. Essas entradas são categorizadas para avaliar a solicitação de acesso com base em critérios pré-definidos ou uma pontuação de confiança. Existem variações no TA, como a avaliação baseada em critérios versus a baseada em pontuação e a consideração singular versus contextual das solicitações [Stafford, 2020].

- ***Policy Decision Point* (PDP)** é o componente responsável por decidir se o acesso a um recurso deve ser permitido ou negado, além de estabelecer ou encerrar a comunicação entre uma entidade (usuário, dispositivo ou serviço) e o recurso solicitado [Teerakanok et al., 2021]. Em sua estrutura, o PDP é dividido em dois elementos lógicos: o **Policy Engine (PE)** e o **Policy Administrator (PA)**, que atuam para tomada de decisão e gestão de comunicação, respectivamente.

- ***Policy Engine* (PE)** é o componente central responsável pela decisão final de conceder, negar, revogar ou restringir o acesso de uma entidade a um determinado recurso. Para determinar sua decisão, este mecanismo utiliza um algoritmo que processa um conjunto de regras (políticas de segurança) baseado no princípio do privilégio mínimo. As entradas para esse algoritmo incluem as políticas pré-definidas e dados de fontes externas, como sistemas de Diagnóstico e Mitigação Contínuos (CDM), serviços de inteligência (*Threat Intelligence*) e registros de atividades. Operando em conjunto com o componente o *Policy Administrator*, o *Policy Engine* verifica explicitamente cada solicitação, toma a decisão, registra-a como aprovada ou negada, e o *Policy Administrator* executa a decisão [Stafford, 2020, Hussain et al., 2024].

- ***Policy Administrator* (PA)** é o componente responsável por estabelecer e encerrar a comunicação entre uma entidade e um recurso, atuando sob as decisões do *Policy Engine*. Quando uma sessão é autorizada, o PA gera *tokens* de autenticação ou credenciais específicas para a sessão e configura o *Policy Enforcement Point* (PEP) para iniciar a comunicação. Inversamente, caso a sessão seja negada ou uma autorização prévia seja revogada, o PA comunica o PEP para encerrar a conexão. Essa interação, que ocorre no plano de controle, assegura que o acesso aos recursos seja controlado de forma dinâmica, garantindo que todas as conexões sejam devidamente autorizadas e monitoradas. Embora algumas implementações possam unificar o PA e o PE, eles são conceitualmente definidos como componentes lógicos distintos [Stafford, 2020].

- ***Policy Enforcement Point* (PEP)** é responsável por habilitar, monitorar e, eventualmente, encerrar a conexão entre uma entidade e um recurso. Sua comunicação é feita com o *Policy Administrator* para encaminhar requisições e receber atualizações das políticas a serem aplicadas. Embora constitua um componente lógico em uma arquitetura de confiança zero (ZTA), o PEP pode ser implementado de maneira dividida, com um agente no lado do cliente e um *gateway* no lado do recurso. Esse mecanismo realiza o gerenciamento dinâmico do acesso e, caso detecte qualquer atividade suspeita durante a conexão, o PEP, por intermédio do PA, sinaliza o término imediato da sessão. Dessa forma, garante-se um controle de acesso seguro, contínuo e responsivo, sendo que a zona de confiança que contém o recurso corporativo situa-se após do PEP.

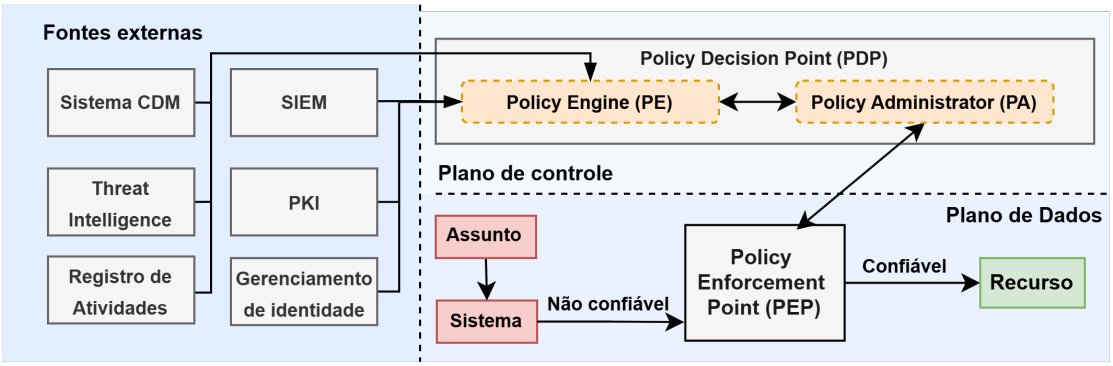


Figura 2.1. Componentes principais do modelo Zero Trust. Fontes externas como sistemas CDM, SIEM, *threat intelligence*, PKI, gerenciamento de identidade e registros de atividades fornecem informações ao *Policy Engine* (PE), que compõe, junto ao *Policy Administrator* (PA), o *Policy Decision Point* (PDP). O PE avalia as condições de acesso com base nas políticas definidas. O *Policy Enforcement Point* (PEP) aplica essas decisões, classificando o acesso do sistema como confiável ou não confiável. Apenas acessos considerados confiáveis são autorizados a interagir com o recurso no plano de dados.

Além dos componentes principais dos planos de dados e controle, outras fontes de dados podem ser utilizadas para fornecer regras de entrada e tomar decisões de acesso [Abdalla et al., 2024], tais como:

- **Sistema Contínuo de Diagnóstico e Mitigação (CDM)** desempenha um papel fundamental ao coletar informações atualizadas sobre o estado atual dos ativos. Sua principal função é implementar atualizações críticas em configurações e componentes de *software*, avaliando se os ativos estão executando componentes adequadamente, verificando a integridade dos componentes de *software* e identificar quaisquer componentes não autorizados, sinalizando possíveis vulnerabilidades.

- ***Threat intelligence feed(s)*** fornecem informações valiosas de diversas fontes, tanto internas quanto externas, auxiliando o PDP de confiança zero a tomar decisões de acesso informadas. Esses *feeds* atualizam constantemente o PDP sobre ameaças emergentes, vulnerabilidades recém-descobertas, relatórios de *malware* e ataques recentes a outros ativos. Ao aproveitar essa inteligência, o PDP pode identificar rapidamente riscos potenciais e impedir o acesso de fontes suspeitas.

- **Logs de rede e de atividades** atuam como um repositório de dados, coletando informações detalhadas sobre o tráfego de rede, acessos e eventos do sistema. Esses dados, atualizados em tempo quase real, alimentam sistemas de detecção e resposta a incidentes, permitindo a identificação rápida de ameaças e a tomada de decisões para a proteção da rede.

- ***Security Information and Event Management* (SIEM)** realiza a coleta, análise e o armazenamento de dados de eventos de toda a infraestrutura. Seu principal objetivo é fornecer uma visão completa da segurança da rede, agilizando a detecção de atividades suspeitas, incidentes cibernéticos e violações de políticas. Geralmente esses sistemas utilizam técnicas de correlação e análise comportamental, acelerando a identificação de ameaças.

- ***Public Key Infrastructure* (PKI)** é um conjunto de tecnologias, políticas e procedimentos utilizados para gerenciar o ciclo de vida de certificados digitais e chaves criptográficas. Baseia-se em criptografia assimétrica e depende de Autoridades Certificadoras (CAs) para a emissão, validação e revogação de certificados, sendo fundamental para aplicações como autenticação, assinatura digital e comunicação segura.

Enquanto o *Policy Engine* (PE) funciona como o cérebro, o *Trust Algorithm* constitui o processo utilizado pelo PE para conceder ou negar acesso a um recurso solicitado. Essa concessão baseia-se na análise de um conjunto de informações compiladas de múltiplas fontes, dentre as quais se destacam: a requisição de acesso, os base de entidades, base de ativos (abrangendo dispositivos como BYOD), as políticas de acesso, os registros de segurança e de tráfego de rede, bem como os dados de sistemas de inteligência de ameaças [Teerakanok et al., 2021]. A Figura 2.2 apresenta o processo de como as entradas podem ser categorizadas para serem utilizadas pelo *Trust Algorithm* [Stafford, 2020, Hussain et al., 2024]:

- **Requisição de acesso** refere-se ao processo pelo qual um indivíduo ou sistema explicitamente solicita acesso a um recurso específico. Essa requisição inclui principalmente informações sobre o recurso solicitado, mas também considera diversos

atributos de quem realiza a solicitação, tais como versão do sistema operacional, *software* utilizado, por exemplo, se o aplicativo está em uma lista de aplicações autorizadas, e nível de atualização de segurança. Dependendo desses fatores e do nível de segurança do ativo solicitado, o acesso pode ser restrito ou negado.

- **Base de entidades** é um repositório que contém as credenciais de todos as entidades (humanos e aplicações) e suas informações associadas, como atributos e privilégios. Este banco de dados detalha "quem" está solicitando acesso, incluindo identidades lógicas e resultados de autenticações. Atributos como hora e geolocalização são usados para avaliar a confiança. É crucial que os privilégios sejam atribuídos individualmente e não apenas por função. Todas essas informações são codificadas e armazenadas em um sistema de gerenciamento de identidade e banco de dados de políticas, sustentando a avaliação contínua da confiança em cada solicitação.

- **Base de ativos** é um repositório, ou sistema de inventário, que armazena o *status* dos ativos de uma organização (físicos, virtuais ou BYOD). Ele compara esse *status* registrado com o *status* observável de um ativo que faz uma requisição, incluindo informações como versão do sistema operacional, *softwares* e sua integridade, localização e nível de atualização. Com base nessa comparação, o acesso a outros ativos pode ser restrito ou negado.

- **Políticas de acesso** complementam a base de entidades, definindo os requisitos mínimos para acessar os recursos. As políticas podem incluir níveis de garantia como localização da autenticação multifatorial, por exemplo, negar acesso de endereços IP estrangeiros, confidencialidade dos dados e solicitações de configuração. Esses requisitos devem ser desenvolvidos tanto pelo custodiante dos dados quanto pelos responsáveis pelos processos de negócios que utilizam os dados.

- ***Threat Intelligence e Logs*** são as informações como assinaturas de ataques recém-descobertos ou *malware* operando na Internet, fornecidas por fontes internas ou externas.

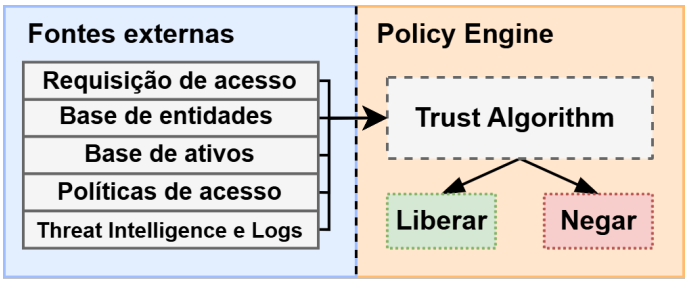


Figura 2.2. Funcionamento do *Policy Engine* a partir de fontes externas e como o algoritmo de confiança (*Trust Algorithm*) recebe dados de diversas fontes, como requisições de acesso, bases de entidades e ativos, políticas de acesso e informações de ameaças com *logs*. Com base nos dados, o algoritmo decide se a solicitação deve ser liberada ou negada.

2.3.1. Arquiteturas Alternativas e Componentes Inovadores

A evolução da *Zero Trust Architecture* (ZTA) exige a exploração de modelos e componentes alternativos que possam complementar ou até mesmo substituir a estrutura clássica formada pelo *Policy Engine* (PE), *Policy Administrator* (PA) e *Policy Enforcement Point* (PEP). Em ambientes altamente dinâmicos, móveis ou distribuídos, como sistemas industriais, redes táticas ou infraestruturas multi-cloud, os mecanismos tradicionais podem não oferecer a agilidade, visibilidade ou adaptabilidade necessárias. Nesse contexto, arquiteturas como *Single Packet Authorization* (SPA), *Software Defined Perimeter* (SDP) e modelos endógenos emergem como alternativas promissoras para estender os princípios de confiança mínima e verificação contínua da ZTA a novos domínios operacionais [Gupta et al., 2024, Dhiman et al., 2024, Gambo e Almulhem, 2025].

Uma abordagem recente e com destaque é o uso de *Single Packet Authorization* (SPA), um mecanismo de controle de acesso que se baseia na aceitação de um único pacote autenticado e criptografado como gatilho para liberar o acesso a um serviço ou porta protegida. Diferente de *firewalls* tradicionais, que estão sempre escutando, o SPA oculta completamente os serviços até que um pacote válido seja recebido, tornando os alvos efetivamente invisíveis a *scanners* ou sondas externas [Gupta et al., 2024]. Quando aplicado à ZTA, o SPA pode operar como uma extensão do PEP, adicionando uma camada de invisibilidade e controle extremamente granular sobre quais pacotes são considerados para avaliação. Isso é particularmente útil em ambientes industriais e militares, em que a redução da superfície de ataque é crítica.

Outra arquitetura complementar relevante é o *Software Defined Perimeter* (SDP), que pode ser interpretado como uma VPN de nova geração associada a políticas dinâmicas, identidade forte e microsegmentação. O SDP define quem pode ver e acessar recursos com base na verificação contextual de identidade, comportamento do dispositivo e localização, além de manter uma superfície de ataque mínima. A visibilidade é tratada como privilégio e não como pressuposto. Em ZTA, o SDP pode atuar como camada de controle entre o usuário e os recursos, aplicando autenticação mútua e verificação contínua antes de conceder acesso a qualquer *endpoint* [He et al., 2022, Nahar et al., 2024]. Essa abordagem é altamente compatível com redes 6G e IoT, em que os limites físicos de rede são efêmeros e os perímetros precisam ser definidos logicamente.

Propostas recentes de arquiteturas *endógenas* definem sistemas projetados para monitorar continuamente a si mesmos e adaptar seu comportamento com base em padrões históricos e aprendizado contínuo. Essas arquiteturas se inspiram em sistemas imunes artificiais, computação auto-defensiva e comportamentos emergentes adaptativos. Elas podem, por exemplo, identificar variações estatísticas no comportamento de processos ou fluxos de rede e ajustar automaticamente as políticas de acesso, a configuração de isolamento ou o nível de confiança atribuído a determinados dispositivos [Gambo e Almulhem, 2025]. A ZTA pode incorporar tais mecanismos como uma camada adicional de análise comportamental local, aumentando sua capacidade de resposta autônoma a ameaças em tempo real.

A adoção dessas arquiteturas alternativas e componentes não substitui diretamente a ZTA tradicional, mas a complementa. A combinação de técnicas como SPA para ocultação de superfície de ataque, SDP para controle baseado em identidade e arquiteturas

Tabela 2.1. Comparativo entre arquiteturas aplicadas à Zero Trust.

Modelo	Princípio Central	Aplicação em ZTA	Benefícios principais
Single Packet Authorization (SPA)	Liberação condicional via pacote criptografado	Acesso sigiloso a serviços e portas; invisibilidade por padrão	Superfície de ataque reduzida; difícil detecção por atacantes
Software Defined Perimeter (SDP)	Identidade como perímetro e controle de visibilidade	Camada de controle de acesso entre dispositivos e serviços	Microsegmentação; negação por padrão; controle granular
Arquitetura Endógena	Adaptação autônoma e auto-monitoramento	Reforço de políticas com base em análise comportamental interna	Detecção precoce de desvios; resposta adaptativa sem intervenção externa

endógenas para inteligência contextual posiciona a segurança como um sistema dinâmico e proativo. À medida que ambientes computacionais tornam-se mais heterogêneos, autônomos e distribuídos, a integração dessas abordagens será essencial para garantir a escalabilidade, resiliência e adaptabilidade dos mecanismos de controle de acesso.

2.3.2. Soluções Comerciais

Por se tratar de um paradigma crucial para a cibersegurança, diversas empresas já desenvolveram abordagens para implementação da arquitetura de confiança zero. Em 2009, o Google, através da solução **BeyondCorp**[3] começou uma iniciativa interna para permitir que os funcionários trabalhassem em redes não confiáveis sem o uso de uma Rede Virtual Privada (*Virtal Private Network* - VPN). Isso ocorreu após uma ação conhecida como Operação Aurora [Tankard, 2011]. Nesse incidente, os invasores obtiveram acesso à rede interna do Google, visando fontes de propriedade intelectual. Eles então usaram o sistema comprometido como um "ponto de partida" para se movimentar lateralmente dentro da rede. Consequentemente, o principal objetivo do Google era reduzir a confiança implícita que usuários e dispositivos haviam desenvolvido com base em sua presença física ou eletrônica na rede corporativa [Hosney et al., 2022]. Assim, todo acesso a sistemas internos só é liberado após três requisitos simultâneos: (i) autenticação do usuário, (ii) verificação do estado do dispositivo e (iii) criptografia de ponta a ponta. Esse processo garante que a experiência de uso seja idêntica para quem está na rede corporativa ou fora dela. Para reforçar essa lógica, o Google mantém uma "rede sem privilégios", isolada em endereços privados, que se comporta como se fosse externa. Dentro desse ambiente, listas de controle de acesso estritamente gerenciadas definem, dispositivo a dispositivo, quais recursos cada um pode alcançar, assegurando segmentação e mínimo privilégio [Kang et al., 2023].

Considerando centros de dados (*data centers*), organizações utilizam cada vez mais soluções de Rede Definida por *Software* (SDN), tais como o **VMware NSX**[4]. Esta plataforma permite a implementação de microssegmentação de forma granular, ao oferecer um modelo de segurança distribuída que atua diretamente no hipervisor. As políticas

[3]Disponível em `https://cloud.google.com/beyondcorp?hl=pt_br`.

[4]Disponível em `https://www.vmware.com/docs/vmware-zero-trust-evolution`.

de controle são aplicadas diretamente na interface virtual de cada máquina virtual, o que garante um nível elevado de isolamento entre cargas de trabalho. A microssegmentação é realizada por meio da definição de zonas de segurança lógicas entre diferentes aplicações, independentemente da sua localização física ou da estrutura de rede. As regras de segurança podem ser configuradas com base em múltiplos atributos, como identidade da VM, tipo de aplicação, sistema operacional ou regras de afinidade, dispensando a dependência exclusiva de endereços IP ou segmentações tradicionais. Com isso, é possível restringir a comunicação entre sistemas apenas ao que for estritamente necessário para o funcionamento das aplicações, reduzindo significativamente a superfície de ataque. Além disso, a capacidade de limitar interações desnecessárias entre cargas de trabalho contribui para dificultar o movimento lateral de ameaças em ambientes comprometidos, o que reforça a adoção de princípios alinhados ao modelo de confiança zero.

Para atender aos princípios da confiança zero no contexto de identidade, o **Microsoft Entra**[5] funciona como uma família de produtos de gerência de identidade e controle de acesso. Ele permite que as organizações não utilizem a confiança implícita, tratando cada identidade como um potencial ponto de violação. A solução implementa um arcabouço que verifica explicitamente todas as identidades, valida as condições de acesso, confirma permissões e monitora continuamente atividades suspeitas, garantindo que apenas usuários e dispositivos autenticados e autorizados acessem os recursos de rede de forma segura. Ainda nesse contexto, o **Okta** é um serviço de Gerenciamento de Identidade e Acesso (*Identity and Access Management* - IAM) que funciona como um intermediário para autenticação de usuários em diversas aplicações e sistemas de uma organização. Sua arquitetura é baseada em nuvem e seu objetivo é centralizar o controle de acesso. No processo de login de um serviço integrado, o Okta redireciona o usuário para sua própria plataforma para a validação das credenciais de acesso. A plataforma então utiliza protocolos padrão da indústria para confirmar a identidade do usuário, podendo aplicar requisitos como *Single Sign-On* (SSO), que permite o uso de um único login para múltiplos serviços, ou Autenticação Multifator (MFA), que exige uma segunda forma de comprovação de identidade. Após a validação, o Okta informa ao aplicativo que o usuário está autorizado, permitindo o acesso com base nas políticas que a organização configurou previamente.

O **Zscaler Zero Trust Exchange**[6] é uma plataforma em nuvem desenvolvida para implementar os princípios da arquitetura de confiança zero, com foco em segurança e conectividade. Em vez de permitir que usuários ou dispositivos acessem diretamente a rede corporativa, o Zscaler cria conexões seguras e verificadas entre usuários autenticados e as aplicações específicas que eles estão autorizados a acessar, sem que a rede como um todo seja exposta. Essa solução baseia-se em quatro pilares: identidade, dispositivo, contexto e política. A plataforma verifica a identidade do usuário, dispositivo por meio de integrações com provedores de identidade externos. Uma vez validada a identidade, o destino da conexão é avaliado para que, em seguida, sejam determinados os riscos baseados no contexto, considerando fatores como comportamento do usuário, postura

[5]Disponível em `https://learn.microsoft.com/pt-br/entra/fundamentals/what-is-entra`.

[6]Disponível em `https://www.zscaler.com/br/products-and-solutions/zero-trust-exchange-zte`.

do dispositivo, destino entre outros. Atendendo a todos os requisitos, as políticas são aplicadas por sessão e por solicitação.

O **Prisma Access** é uma plataforma de segurança em nuvem da Palo Alto[7] com objetivo de proteger o acesso a aplicações e *Software as a Service* (SaaS). Seu funcionamento baseia-se na consolidação de múltiplas funções de segurança e rede, gerenciado de forma centralizada. Após o usuário se conectar, a plataforma realiza uma verificação de confiança contínua com base no comportamento, com o objetivo de reduzir a superfície de ataque. Todo o tráfego, seja para aplicações de Internet, SaaS ou privadas, é protegido por meio de uma inspeção de segurança. A abordagem de *Zero Trust* é aplicada através do "ZTNA Connector"para segmentar usuários e redes através de um túnel seguro, garantindo que o acesso seja concedido apenas aos recursos estritamente necessários, seguindo o princípio de privilégio mínimo. A visibilidade é mantida por meio de uma política de prevenção de perda de dados (*Data Loss Prevention* - DLP) única para proteger tanto o acesso quanto os dados em toda a empresa.

2.3.3. Taxonomia de Aplicações, Tecnologias e Requisitos da ZTA

A adoção da *Zero Trust Architecture* (ZTA) vem se consolidando como uma resposta estratégica aos desafios de segurança em ambientes cada vez mais distribuídos, móveis e heterogêneos. Gambo *et al.* apresentam uma taxonomia abrangente que sistematiza os principais elementos que compõem uma arquitetura ZTA moderna e busca organizar o conhecimento existente em torno de quatro eixos fundamentais: os domínios de aplicação da ZTA, as tecnologias habilitadoras, os mecanismos de controle de acesso e os requisitos funcionais e não funcionais para sua implementação eficaz [Gambo e Almulhem, 2025].

Os domínios de aplicação identificados abrangem contextos como *Internet das Coisas* (*Internet of Things* - IoT), redes móveis emergentes (5G e 6G), ambientes *multi-cloud* e sistemas industriais (*Industrial Control Systems* - ICS/SCADA). Cada um desses cenários impõe exigências específicas de autenticação, controle de acesso e resiliência. Por exemplo, em sistemas IoT, a comunicação entre sensores deve ser autenticada continuamente em redes potencialmente maliciosas, já em redes 6G, a escalabilidade e a latência de decisões são aspectos críticos.

Gambo *et al.* apontam as tecnologias habilitadoras da ZTA como sendo autenticação contínua e multifatorial, microsegmentação, sensoriamento contextual, criptografia ponta-a-ponta, integração com *blockchain* para auditoria imutável e o uso de inteligência artificial para análise comportamental e adaptação de políticas de segurança. Essas tecnologias tendem a operar de forma coordenada para permitir decisões de acesso granulares e dinâmicas, rompendo com o paradigma de confiança estática baseada em perímetro.

Quanto aos mecanismos de controle de acesso, a taxonomia reconhece os modelos Controle de Acesso Baseado em Papéis (*Role-Based Access Control* - RBAC), Controle de Acesso Baseado em Atributos (*Attribute-Based Access Control* - ABAC) e Controle de Acesso Baseado em Políticas (*Policy-Based Access Control* - PBAC). O RBAC baseia-se na associação de usuários a papéis predefinidos, oferecendo simplicidade e facilidade de administração, mas apresenta limitações em ambientes dinâmicos por sua rigidez e falta

[7]Disponível em `https://www.paloaltonetworks.com/resources/datasheets/prisma-access`.

de contexto. O ABAC supera essas limitações ao permitir decisões com base em múltiplos atributos, como identidade, dispositivo, localização e horáriom promovendo maior flexibilidade e granularidade. No entanto, sua gestão pode se tornar complexa à medida que o número de atributos e regras cresce. Por sua vez, o PBAC formaliza o controle de acesso por meio de políticas explícitas, escritas em linguagens declarativas, facilitando auditoria, modularidade e integração com rotinas automatizadas [Oliveira et al., 2024]. Apesar disso, requer automações especializadas e conhecimento técnico mais avançado. No contexto de ZTA, ABAC e PBAC são mais alinhados aos princípios de verificação contínua e privilégio mínimo, sendo preferidos em implementações que exigem adaptabilidade e governança refinada sobre decisões de acesso. Embora o RBAC continue amplamente utilizado, ele é limitado em cenários dinâmicos. O ABAC, por sua vez, permite decisões mais refinadas ao considerar atributos de usuários, dispositivos e contexto. O PBAC é apontado como o mais aderente à filosofia *Zero Trust*, por sua capacidade de representar regras contextuais explícitas e adaptativas. A Tabela 2.2 compara as características dos diferentes modelos de controle de acesso para a aplicação em ZTA e a Tabela 2.3 apresenta exemplos de categorias e elementos da taxonomia [Gambo e Almulhem, 2025].

A taxonomia proposta enfatiza a importância de requisitos funcionais como autenticação contínua, monitoramento, resposta adaptativa e controle de acesso granular. Em paralelo, destaca requisitos não funcionais, tais como escalabilidade, interoperabilidade, resiliência, desempenho e compatibilidade com sistemas legados. A articulação desses requisitos com os demais eixos da taxonomia permite uma avaliação mais holística da maturidade de uma implementação ZTA.

A definição clara dos requisitos funcionais e não funcionais é essencial para orientar o projeto, a implementação e a avaliação de arquiteturas baseadas em *Zero Trust*. Os requisitos funcionais estabelecem os mecanismos fundamentais necessários para assegurar os princípios centrais da ZTA, como autenticação contínua, controle de acesso dinâmico e resposta adaptativa a ameaças. Já os requisitos não funcionais dizem respeito a qualidades do sistema que garantem sua viabilidade prática em ambientes reais, incluindo aspectos como escalabilidade, interoperabilidade e resiliência. A Tabela 2.4 resume os principais requisitos identificados na literatura técnica, com destaque para sua aplicabilidade em ambientes distribuídos, híbridos e dinâmicos.

De modo geral, a taxonomia de Gambo *et al.* oferece uma base sólida para compreender os fundamentos estruturantes da ZTA, permitindo seu desdobramento prático em diferentes domínios tecnológicos. Ao estabelecer relações explícitas entre aplicação, tecnologia e controle, ela contribui para a consolidação da ZTA como um paradigma capaz de responder aos desafios contemporâneos de segurança cibernética.

2.3.4. Comparação entre Modelos Convencionais de Segurança e Arquitetura de Confiança Zero

A evolução das arquiteturas de segurança em redes corporativas acompanha o aumento da complexidade e da dispersão dos ativos digitais. O modelo perimetral, ou castelo-e-fosso (*castle-and-moat*), historicamente predominante, assume confiança implícita nos elementos internos da rede, protegendo-os com firewalls, VPNs e segmentações físicas. Esse paradigma, no entanto, revela-se inadequado frente à popularização

Tabela 2.2. Comparação entre modelos de controle de acesso em diferentes domínios de aplicação.

Critério	Modelo	Descrição
Base de decisão	RBAC	Baseado em papéis atribuídos a usuários; permissões são estáticas e definidas por função
	ABAC	Baseado em múltiplos atributos de usuário, recurso e ambiente; permite decisões dinâmicas
	PBAC	Baseado em políticas declarativas codificadas; permite regras contextuais e sofisticadas
Flexibilidade	RBAC	Baixa; difícil adaptação a mudanças contextuais ou dinâmicas de acesso
	ABAC	Alta; incorpora atributos contextuais e ambientais para decisões mais precisas
	PBAC	Muito alta; políticas podem ser alteradas, versionadas e auditadas conforme necessidade
Adequação a IoT	RBAC	Limitada; requer definição prévia de papéis em ambientes com grande variabilidade
	ABAC	Alta; considera o estado do dispositivo, localização e outros atributos contextuais
	PBAC	Alta; possibilita definição de políticas específicas para dispositivos com base em risco
Aplicação em Nuvem	RBAC	Ampla adoção em sistemas IaaS, mas com limitações em granularidade
	ABAC	Amplo suporte; útil para ambientes com múltiplos *tenants* e requisitos dinâmicos
	PBAC	Ideal; permite governança e automação via "*policy-as-code*"
Redes Críticas	RBAC	Limitada; pouco adaptável a eventos de segurança em tempo real
	ABAC	Boa; permite decisões com base em atributos de missão e contexto operacional
	PBAC	Excelente; oferece rastreabilidade, controle de conformidade e resposta automatizada
Outras ferramentas	RBAC	Active Directory, FreeIPA
	ABAC	AWS IAM, XACML
	PBAC	Open Policy Agent (OPA), Rego, Keycloak Authorization Services

Tabela 2.3. Exemplos de categorias e elementos na taxonomia de ZTA.

Categoria	Elemento	Descrição
Domínio de Aplicação	IoT	Autenticação contínua entre sensores em rede maliciosa
Tecnologia Habilitadora	*Blockchain*	Auditoria imutável e controle distribuído
Mecanismo de Controle	ABAC	Acesso baseado em atributos de usuários e contexto
Requisito Funcional	Autenticação Contínua	Verificação periódica de identidade e postura do dispositivo
Requisito Não Funcional	Escalabilidade	Suporte eficiente a milhares de dispositivos simultâneos

de ambientes multi-*cloud*, à ampliação do trabalho remoto e à sofisticação dos ataques. Nesse cenário, a *Zero Trust Architecture* (ZTA) emerge como resposta, pautada no princípio de que nenhuma entidade (interna ou externa) deve ser considerada confiável por

Tabela 2.4. Requisitos funcionais e não funcionais para a implementação eficaz de uma arquitetura *Zero Trust*.

Tipo	Requisito	Descrição
Funcional	Autenticação Contínua	Verificação permanente da identidade e do estado dos dispositivos antes e durante a sessão
	Controle de Acesso Granular	Definição de permissões com base em atributos dinâmicos de usuário, recurso e contexto
	Monitoramento e Auditoria	Registro e análise contínua de eventos para detectar comportamentos anômalos e violações
	Resposta Adaptativa	Capacidade de reagir automaticamente a eventos de segurança, como revogação de acesso ou isolamento de sessão
Não Funcional	Escalabilidade	Suporte a um grande número de usuários, dispositivos e sessões simultâneas com desempenho aceitável
	Interoperabilidade	Integração com sistemas legados, múltiplos domínios e soluções heterogêneas
	Baixa Latência	Tempo de resposta reduzido para autenticação, autorização e troca de políticas
	Resiliência	Tolerância a falhas e ataques, com mecanismos de recuperação rápida e redundância

padrão [Gupta et al., 2024, Dhiman et al., 2024].

A distinção fundamental entre os dois modelos reside na forma de atribuição de confiança. No modelo tradicional, qualquer entidade inserida na rede passa a ser confiável automaticamente. Em contraste, a ZTA aplica validações contínuas, baseadas em múltiplos fatores como identidade, contexto, estado do dispositivo e comportamento recente. Enquanto o controle de acesso no modelo perimetral é centralizado em dispositivos de borda, na ZTA ele é distribuído, com autenticação e autorização aplicadas em cada tentativa de acesso [Gambo e Almulhem, 2025].

Outro ponto crítico é a gestão da sessão. No modelo legado, a autenticação inicial costuma garantir acesso prolongado, sem revalidação. Na ZTA, as sessões são curtas, monitoradas continuamente e revogadas dinamicamente diante de alterações contextuais ou comportamento anômalo. A detecção de ameaças também difere: enquanto o modelo tradicional se apoia na inspeção em pontos fixos da rede, a ZTA emprega telemetria contínua, análise comportamental e mecanismos automatizados para identificar desvios em tempo real.

A gestão de identidades e dispositivos reforça a maturidade exigida pela ZTA. No modelo tradicional, a autenticação é pontual e generaliza a confiança. Na ZTA, exige-se autenticação multifator, avaliação da postura do dispositivo e validação contextual alinhada às políticas definidas. Essa abordagem mostra-se eficaz para cenários modernos, como acesso remoto, ambientes BYOD (*bring your own device*), infraestrutura em nuvem e sistemas industriais conectados [Gupta et al., 2024, Dhiman et al., 2024].

A Tabela 2.5 resume as diferenças fundamentais entre os modelos. Em suma, a transição do modelo perimetral para o paradigma *Zero Trust* não representa apenas uma atualização tecnológica, mas uma mudança profunda de mentalidade, centrada em verificação contínua, privilégio mínimo e visibilidade completa.

Tabela 2.5. Comparação entre modelo de segurança perimetral e *Zero Trust Architecture* (ZTA).

Critério	Modelo Perimetral	Zero Trust Architecture (ZTA)
Princípio de confiança	Confiança implícita dentro da rede	Nenhuma confiança por padrão; verificação contínua
Local do controle de acesso	Na borda da rede (ex: firewalls)	Distribuído; aplicado em cada solicitação de acesso
Gestão da sessão	Sessões persistentes após login	Sessões curtas, monitoradas e revogáveis dinamicamente
Detecção de ameaças	Inspeção de tráfego na borda	Análise comportamental e telemetria contínua
Identidade e dispositivos	Autenticação pontual com baixa contextualização	Autenticação multifator e avaliação da postura do dispositivo

2.3.5. Confiança Zero em Redes 6G e Ambientes Inteligentes

A evolução para a sexta geração de redes móveis (6G) introduz uma nova era de conectividade hiperconvergente, densamente distribuída e intensiva em dados. Diferentemente das gerações anteriores, a 6G está intrinsecamente associada à integração de ambientes inteligentes (*smart environments*), como cidades autônomas, sistemas industriais avançados, veículos conectados e dispositivos de realidade imersiva. Nesse cenário, a superfície de ataque cresce exponencialmente, enquanto os modelos tradicionais de segurança, centrados em perímetros rígidos, tornam-se obsoletos. A arquitetura *Zero Trust* (ZTA) emerge como um paradigma fundamental para prover segurança contínua, contextual e verificável em redes 6G, operando com base no princípio de "nunca confiar, sempre verificar" [Nahar et al., 2024, Gupta et al., 2024].

As aplicações de ZTA em redes 6G cobrem desde o isolamento de *network slices* até a imposição de políticas dinâmicas de acesso em ambientes altamente distribuídos. Com a virtualização e a segmentação lógica de redes, cada fatia (*slice*) pode representar um domínio de missão crítica, como saúde, transporte ou manufatura. A ZTA, aplicada a esse contexto, assegura que cada entidade (dispositivo, usuário ou serviço) seja autenticada continuamente e que o acesso a qualquer recurso seja mediado por políticas contextuais. Essa arquitetura é particularmente eficaz em cenários que demandam latência ultrabaixa e alta confiabilidade, como controle de veículos autônomos, automação fabril e operações remotas de saúde [He et al., 2022].

A inteligência artificial (IA) torna-se uma aliada estratégica na implementação de motores de decisão em ZTA (*Zero Trust Decision Engines*). Com a coleta contínua de dados de contexto, comportamento de dispositivos, modelos de aprendizado de máquina podem inferir pontuações de risco e ajustar permissões dinamicamente. Técnicas como aprendizado federado, aprendizado por reforço e redes neurais leves permitem processar dados na borda, respeitando restrições de latência e privacidade. No entanto, esses mecanismos enfrentam desafios relevantes, como a redução de falsos positivos, a transparência das decisões automatizadas e a mitigação de viés em conjuntos de dados. Ainda assim, os *Zero Trust Decision Engines* baseados em IA representam um avanço essencial na direção de políticas adaptativas e autônomas.

A segmentação de redes densas, com bilhões de dispositivos interconectados, re-

Tabela 2.6. Integração entre componentes da ZTA, inteligência artificial e elementos da arquitetura 6G.

Componente ZTA	Uso de IA	Aplicação em Redes 6G
Motor de decisão	Análise comportamental e risco adaptativo	Controle de acesso dinâmico em *network slices*
Monitoramento contínuo	Aprendizado federado e detecção de anomalias	Supervisão de dispositivos em ambientes inteligentes
Segmentação lógica	Classificação automática de dispositivos	Microsegmentação em redes densas e móveis
Controle de políticas	Ajuste automatizado com base em contexto e ameaça	Orquestração em múltiplos domínios 6G

quer mecanismos refinados de microsegmentação e isolamento dinâmico. A ZTA fornece meios para classificar dispositivos por atributos de identidade, função, criticidade e confiabilidade, permitindo que comunicações ocorram apenas entre entidades autorizadas dentro de segmentos lógicos. Essa segmentação pode ser adaptada em tempo real com base em mudanças de topologia, comportamento suspeito ou modificações de contexto. Ambientes inteligentes com sensores, atuadores, câmeras, veículos e nós de computação de borda se beneficiam da capacidade da ZTA de orquestrar políticas em múltiplos domínios administrativos, com visibilidade e controle unificados.

A integração entre componentes da ZTA e as redes 6G é explicitada na Tebala 2.6. Apesar das vantagens promissoras, o uso de ZTA em redes 6G impõe desafios substanciais. A escalabilidade de mecanismos de autenticação e verificação contínua em ambientes massivos ainda requer avanços significativos. A latência na aplicação de decisões de acesso baseadas em IA precisa ser rigorosamente controlada para não comprometer requisitos de tempo real. Adicionalmente, a interoperabilidade entre diferentes domínios administrativos e fornecedores de rede ainda é uma barreira à aplicação prática de ZTA em escala global. Entre as direções futuras, destaca-se a incorporação de *blockchain* para auditoria distribuída, o uso de identidade descentralizada para autenticação federada, e a formalização de políticas como código para validação automática e verificabilidade.

A integração entre a *Zero Trust Architecture* (ZTA) e tecnologias *blockchain* surge como uma estratégia promissora para reforçar os pilares de segurança, auditabilidade e descentralização em ambientes distribuídos. Enquanto a ZTA opera sob o princípio da verificação contínua e do privilégio mínimo, *blockchain* fornece uma base imutável, confiável e auditável para registro e execução de políticas de acesso. A união dessas abordagens é particularmente relevante em contextos como Internet das Coisas (IoT), redes federadas, sistemas multi-organizacionais e infraestruturas críticas, nos quais a confiança entre entidades não pode ser presumida e a necessidade de visibilidade é essencial [Gupta et al., 2024, Pooja e Chandrakala, 2024].

No âmbito da ZTA, os componentes centrais do controle de acesso, *Policy Enforcement Point* (PEP), *Policy Decision Point* (PDP) e *Policy Administrator* (PA), dependem da correta autenticação, autorização e avaliação de contexto para decidir sobre a permissão de acesso a recursos sensíveis. A introdução da *blockchain* permite descentralizar parte dessas decisões, registrando regras e auditorias em contratos inteligentes. Com isso, é possível automatizar a aplicação de políticas de forma verificável e garantir que modifi-

cações nos critérios de acesso sejam historicamente rastreáveis. O uso de *blockchain* com suporte a contratos inteligentes, como Ethereum e Hyperledger Fabric, permite modelar regras de acesso granulares com base em atributos de identidade, localização, horário ou nível de sensibilidade do recurso [Tuler De Oliveira et al., 2022, He et al., 2022].

A tecnologia *blockchain* pode atuar como repositório confiável para identidades digitais descentralizadas (DID), *tokens* de acesso e eventos de auditoria [de Oliveira et al., 2024]. Em um sistema tradicional, essas informações ficariam armazenadas em servidores centrais, sujeitos a comprometimentos internos ou externos. Com a descentralização, cada entidade pode controlar sua identidade por meio de chaves criptográficas, enquanto a verificação de permissões ocorre por meio de consenso ou validação distribuída. Tal abordagem é compatível com mecanismos de controle de acesso acesso fino (*fine-grained*) como o ABAC (*Attribute-Based Access Control*), permitindo que decisões sejam tomadas com base em múltiplos atributos dinâmicos registrados na rede *blockchain* [Nahar et al., 2024].

Esse controle de acesso fino pode ser ampliado com contratos inteligentes que integram políticas contextuais complexas, como restrições geoespaciais (*geofencing*), análise de tempo de acesso, associação a grupos temporários ou níveis de risco atribuídos por algoritmos de aprendizado de máquina [Tuler De Oliveira et al., 2022]. Em arquiteturas ZTA integradas com *blockchain*, a decisão de acesso não depende apenas da verificação tradicional em um servidor central, mas da avaliação distribuída de múltiplos fatores, com evidência criptográfica e transparência.

A aplicação prática dessa integração já aparece em sistemas de saúde, consórcios industriais e ambientes acadêmicos, nos quais dados sensíveis precisam ser compartilhados entre instituições com diferentes níveis de autoridade e protótipos de redes B5G e 6G. Em plataformas de telemedicina, por exemplo, é possível garantir que apenas profissionais devidamente autenticados e com atributos específicos (ex: especialidade, vínculo institucional, jurisdição) acessem prontuários protegidos, sendo cada requisição registrada em *blockchain* para futura auditoria. Similarmente, em colaborações científicas, o uso de ZTA com *blockchain* permite que permissões de leitura, modificação e reuso de *datasets* sejam atribuídas de forma condicional, auditável e reversível [de Oliveira et al., 2024].

Contudo, a latência natural de redes *blockchain* pode ser um entrave para decisões em tempo real. Soluções como o uso de infraestruturas de *blockchain* permissionadas, uso de canais privados e mecanismos de cache podem mitigar esse impacto. A complexidade da governança das políticas e da atualização dos contratos inteligentes exige mecanismos robustos de versionamento, autenticação de administradores e validação formal de regras. Apesar dessas limitações, a sinergia entre ZTA e *blockchain* representa um avanço notável na construção de ecossistemas seguros, confiáveis e interoperáveis para redes 6G. Ao permitir um controle de acesso fino com rastreabilidade total, essas tecnologias reforçam os princípios de segurança por *design*, transparência e descentralização, fundamentais para os cenários modernos de computação em nuvem, IoT e cooperação federada entre organizações.

2.4. Implementação da Arquitetura de Confiança Zero

Existem múltiplas possibilidades para a implementação de uma arquitetura de confiança zero, que se diferenciam pelos componentes empregados e pela origem das políticas adotadas. Todas as abordagens contemplam os princípios descritos anteriormente, embora um ou dois deles possam assumir papel preponderante na formulação das políticas. Para obter uma solução abrangente, recomenda-se integrar elementos das três abordagens: governança de identidade aprimorada, microssegmentação lógica e segmentação baseada em rede [Stafford, 2020].

Na abordagem de **Governança de Identidade Aprimorada**, a identidade e os atributos são a base para a formulação de políticas de acesso. Cada solicitação a recursos corporativos é avaliada com base nos privilégios concedidos a uma dada identidade e fatores complementares, como o tipo de dispositivo, o estado e a rede, ajustam o nível de confiança resultante, podendo, por exemplo, restringir o acesso a subconjuntos de dados ou impor verificações adicionais. Embora o acesso à rede seja liberado a todos os ativos por padrão, o acesso a recursos críticos permanece condicionado à validação da identidade e a infraestrutura deve monitorar continuamente movimentações laterais ou tentativas de negação de serviço para conter ameaças internas. Dispositivos IoT, por exemplo, operam em condições de alta exposição, o que facilita a ação de invasores em busca de informações para viabilizar seus ataques. Para neutralizar essa ameaça, a auditoria regular da rede se torna uma solução crucial. Esse processo é um dos pilares da governança de identidade, garantindo a eficácia das políticas de autenticação e autorização e fortalecendo a segurança como um todo [Rizvi et al., 2023].

Alguns trabalhos avaliam o uso de Identidade Descentralizada para cenários *Zero Trust* em que diferentes domínios precisam compartilhar recursos com segurança. Em vez de depender de um servidor central, cada participante gera seu próprio identificador descentralizado (DID) e recebe credenciais verificáveis, guardadas em uma cadeia de blocos que funciona como registro imutável de confiança. Com isso, o controle da identidade passa a ser do utilizador (*Self-Sovereign Identity*); os atributos só são revelados quando necessário, e a autenticação/autorização é realizada com provas criptográficas que não expõem dados sensíveis [Bernabé Murcia et al., 2025]. O ciclo de vida da identidade consiste em cinco estágios essenciais [Aboukadri et al., 2024]: Provisionamento, Autenticação, Autorização, Manutenção e Desprovisionamento.

- **Provisionamento** envolve a geração de um identificador distinto, a criação de credenciais e a documentação do perfil de atributos do sujeito. Esses atributos podem incluir elementos como localização geográfica, endereço de e-mail ou características específicas de contexto.

- **Autenticação** consiste na confirmação que um dado usuário é realmente quem diz ser. Existem diversos tipos de autenticação, como baseadas em senhas, dois fatores, biométricas, federada ou *token*. Um dos requisitos para implementação da arquitetura de confiança zero, é que este processo seja feito de forma contínua.

- **Autorização** consiste em conceder ou negar permissões a um usuário, grupo de usuários ou uma entidade (como um serviço ou aplicação) para realizar ações espe-

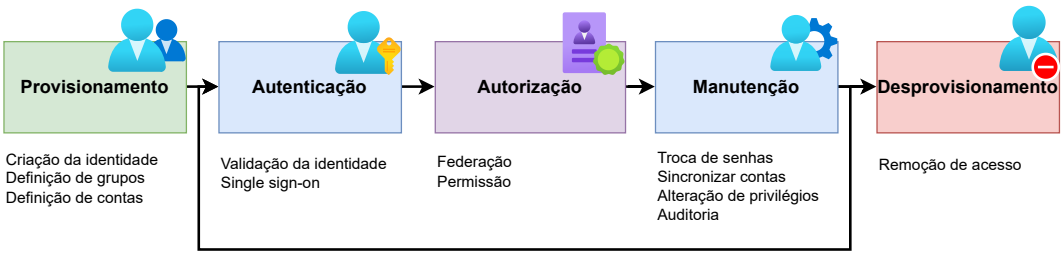


Figura 2.3. Ciclo de gerenciamento de identidade e acesso. O fluxo incia-se com o Provisionamento (criação de identidade e contas), seguido pela Autenticação (validação da identidade), Autorização (definição de permissões), Manutenção (atualização de senhas, sincronização e auditoria), e termina com o Desprovisionamento (remoção de acesso). Esse processo garante a segurança e o controle adequado sobre o acesso dos usuários ao longo de seu ciclo de vida no sistema.

cíficas. Nesse sentido, a autorização determina **o** que um usuário ou entidade pode fazer após a autenticação.

- **Manutenção** consiste no processo que lida com o fato de que as identidades são dinâmicas e podem sofrer alterações ao longo do tempo, seja devido à evolução das características do usuário ou a mudanças nas demandas de negócios, o que pode levar a transformações na identidade.

A **micro-segmentação** por sua vez, é uma abordagem de segurança que divide a rede em segmentos isolados e granulares, permitindo a aplicação de políticas de segurança específicas para cada carga de trabalho (*workload*). Por reduzir significativamente a superfície de ataque, esse conceito além de restringir o tráfego **leste-oeste** (movimentação lateral), também impõe controles sobre o tráfego **norte-sul**, limitando o tráfego entre usuários, aplicações e servidores. Essa granularidade não apenas eleva o nível de segurança, mas também aumenta a precisão de ferramentas de monitoramento, como as de detecção de anomalias, que operam com mais eficácia em ambientes menores e mais homogêneos. Impulsionada pelo avanço das Redes Definidas por *Software* (SDN) e dos centros de dados definidos por *software* (*Software Defined Data Centers* - SDDC), a micro-segmentação tornou-se peça-chave para conciliar segurança e flexibilidade [Mujib e Sari, 2020]. Em arquiteturas tradicionais, a segurança é concentrada em *firewalls* de borda. Contudo, uma vez que um atacante ultrapassa essa barreira de perímetro, ele ganha liberdade para se movimentar lateralmente pela rede interna e escalar o ataque. A micro-segmentação soluciona essa vulnerabilidade ao este para dentro do data center, controlando o tráfego leste-oeste, ou seja, a comunicação entre os componentes internos da infraestrutura [Mämmelä et al., 2016]. O modelo de serviços de uma rede micro-segmentada pode ser visualizado na Figura 2.4, sendo um componente lógico fundamental na arquitetura de segurança de confiança zero, baseando-se no princípio do “privilégio mínimo"para conceder acesso apenas quando estritamente necessário [Sheikh et al., 2021]. Essa abordagem consiste em dividir a rede em pequenas zonas isoladas, criando perímetros de segurança em torno de recursos e aplicações onde cada zona exige autorização específica para acesso. Dessa forma, a micro-segmentação permite implementar de

maneira granular e eficaz os tradicionais mecanismos de segurança, como Autenticação, Autorização e Auditoria, garantindo que apenas usuários e sistemas autenticados possam se comunicar.

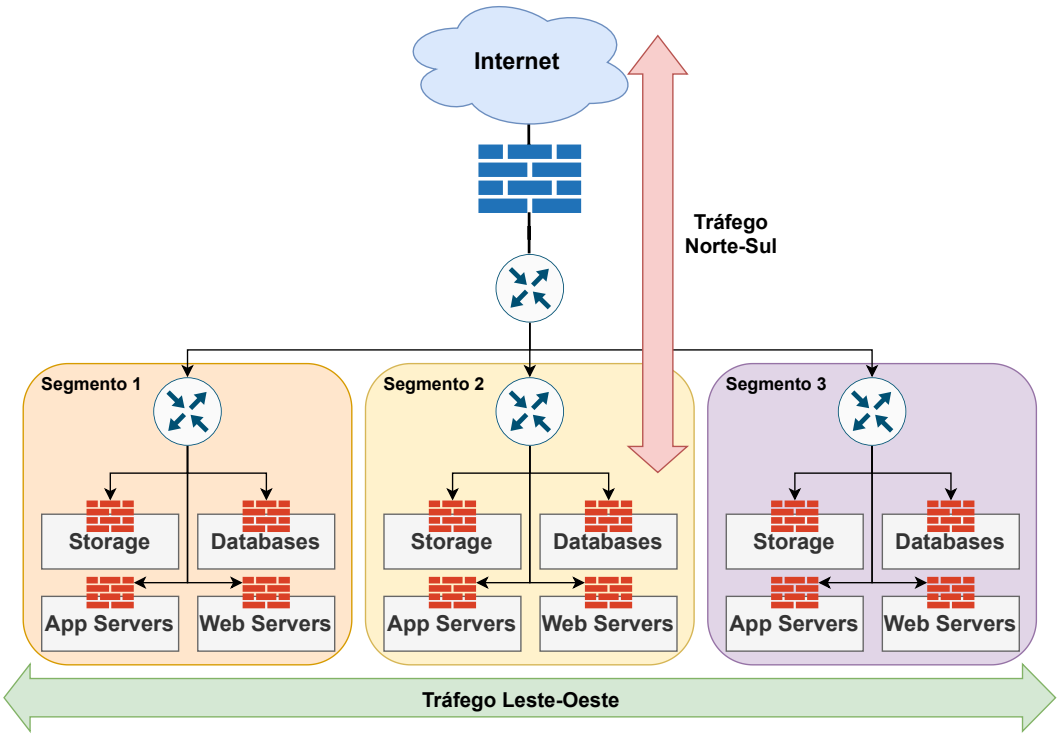


Figura 2.4. Ilustração de uma arquitetura de rede micro-segmentada, destacando a separação entre diferentes segmentos. Cada segmento é composto por componentes, como servidores de armazenamento (Storage), bancos de dados (Databases), servidores de aplicação (App Servers) e servidores web (Web Servers). Os segmentos são protegidos por *firewalls*, que controlam e limitam o tráfego interno (leste-oeste) entre os componentes do data center, bem como o tráfego externo (norte-sul) entre a rede interna e a internet. Essa abordagem de micro-segmentação visa aumentar a segurança ao isolar os diferentes segmentos e restringir a movimentação lateral de possíveis ameaças dentro da rede.

Para cargas de trabalho em contêineres, que são efêmeras e distribuídas por natureza, a micro-segmentação é crucial. Avanços foram feitos no suporte à micro-segmentação para esses ambientes, impulsionados em grande parte pela tecnologia eBPF (***extended Berkeley Packet Filter***) [Chang e Mukherjee, 2024]. O eBPF permite a execução de programas em um ambiente restrito dentro do *kernel* do Linux, fornecendo controle sobre o tráfego de rede e as chamadas de sistema, sem a necessidade de alterações no código da aplicação. Soluções de segurança nativas da nuvem aproveitam o eBPF para implementar a micro-segmentação, detre elas:

- **Cilium** utiliza o eBPF para criar políticas de rede independentes nas camadas 3 e 4 e segurança nas camadas 4 a 7 da pilha TCP/IP [Koukis et al., 2024]. O Cilium

estabelece uma **identidade estática** para cada carga de trabalho com base em seus metadados (como labels do Kubernetes), em vez de depender de endereços IP, que são variáveis em ambientes de contêineres. Com essa identidade, o Cilium impõe políticas de segurança diretamente no kernel, controlando quais serviços podem se comunicar entre si [Chang e Mukherjee, 2024].

- **Calico**, assim como o Cilium, é uma solução para contêineres que utiliza o kernel Linux e o protocolo BGP para criar uma rede de alto desempenho. Uma das suas principais características é o gerenciamento de endereços IP (IPAM) e aplicação de políticas de segurança granulares. Por padrão, o Calico emprega tunelamento de sobreposição (*overlay*) IP-em-IP [Nagendra e Hemavathy, 2023].

- **Flannel** é um plugin CNI *(Container Network Interface)* que simplifica a comunicação em rede orquestração de contêineres como o Kubernetes. O objetivo também é criar uma rede virtual sobre a infraestrutura (*overlay*), utilizando por padrão o encapsulamento VXLAN, mas também suporta alternativas como IPIP, host-gw e UDP [Koukis et al., 2024]. Para o gerenciamento da rede, o Flannel implementa um agente binário, o **flanneld**, na forma de um DaemonSet. Esse componente é responsável por alocar uma sub-rede de IP única para cada host, garantindo que não haja conflitos de endereço. A distribuição da configuração de rede e o roteamento do tráfego são coordenados através de um armazenamento central de chave-valor, como o etcd [Nagendra e Hemavathy, 2023].

Nesse sentido, a micros-segmentação substitui o modelo de segurança de confiança implícita pelo de acesso explícito, baseado em identidade e contexto. Ao criar zonas de controle menores, é possível aplicar políticas de segurança precisas, coletar métricas detalhadas e isolar incidentes rapidamente, o que limita o impacto de ameaças como o *ransomware*.

A última abordagem para a implementação da arquitetura de confiança zero consiste em considerar as redes não apenas como canais de comunicação, mas como elementos estratégicos no gerenciamento distribuído de dados. Essa perspectiva abrange atividades como acesso, processamento, transferência e armazenamento de informações diretamente na rede, reforçando seu papel central na arquitetura e na segurança das operações. Espera-se, portanto, que as estruturas de segurança de próxima geração, baseadas nesse modelo, garantam a proteção dos dados ao longo de todo o seu ciclo de vida [Ramezanpour e Jagannath, 2022]. Essa abordagem pode ser viabilizada por meio de uma rede *overlay*, geralmente operando na camada 7, mas que também pode ser configurada em níveis inferiores da pilha OSI. Tais soluções são frequentemente denominadas *Software Defined Perimeter* (SDP) e, em muitos casos, integram conceitos de *Software Defined Network* (SDN) e *Intent Based Network* (IBN) [Stafford, 2020]. Além de redefinir o papel das redes, o SDP atua como um mecanismo de segurança capaz de lidar com aspectos críticos como autenticação, controle de acesso granular e auditoria detalhada. Ele garante que apenas usuários autorizados tenham acesso aos recursos da rede, alinhando-se aos princípios fundamentais da confiança zero [Shen e Shen, 2024]. Utilizando políticas dinâmicas, o SDP estabelece túneis de comunicação seguros e isolados, ocultando a infraestrutura da rede e limitando o acesso exclusivamente aos recursos necessários, como

servidores e aplicações. Essa estratégia não apenas reforça a segurança, como também reduz a superfície de ataque, tornando a infraestrutura mais resiliente e adequada às complexidades inerentes das redes de próxima geração. Quando implementado na camada de aplicação. Existem algumas variações para iniciar a implementação [Stafford, 2020], podendo destar as baseadas em **Agente/*Gateway***, **Enclave** e **Portal**.

Na implementação baseada em **agente e *gateway***, o *Policy Enforcement Point* (PEP) é dividido em dois componentes: o agente, instalado no dispositivo (como um laptop), e o *gateway*, posicionado antes do recurso que se deseja o acesso, como uma aplicação ou banco de dados, por exemplo. O agente é responsável por interceptar e redirecionar o tráfego de rede do usuário para o *gateway* apropriado. Por sua vez, o *gateway* funciona como um *proxy* reverso, garantindo que toda a comunicação com o recurso passe obrigatoriamente por ele. O processo tem início quando uma entidade (usuário ou aplicação) tenta acessar um recurso corporativo. A solicitação é capturada pelo agente no dispositivo e enviada ao *Policy Administrator* (PA), um componente do plano de controle da arquitetura. Este por sua vez consulta o *Policy Engine* (PE), que avalia se o acesso cumpre as regras de segurança vigentes. Caso a solicitação seja aprovada, o PA instrui o agente e o *gateway* a estabelecerem um canal de comunicação seguro e direto. Para isso, são configurados parâmetros como endereços IP, portas, *tokens* de sessão e outros elementos de segurança que asseguram a confidencialidade e a integridade. Com o canal estabelecido, os dados trafegam criptografados diretamente entre o agente e o *gateway*, operando exclusivamente no plano de dados. A conexão é encerrada automaticamente ao final da sessão ou caso ocorra um evento de segurança detectado pelo PA, como a expiração do tempo de uso ou uma falha de reautenticação. Este modelo é ideal para organizações que gerenciam seus próprios dispositivos e não permitem o uso de aparelhos pessoais (BYOD). É também altamente eficaz em ambientes com recursos discretos que exigem comunicações estritamente controladas, representando uma implementação clássica do modelo cliente-servidor [Stafford, 2020]. A Figura 2.5 apresenta o fluxo dessa implementação.

A implementação baseada em **Enclave**, ilustrada na Figura 2.6, é uma variação do modelo agente/gateway. Nesse caso, o *gateway* encontra-se na fronteira de um enclave de recursos, dispensando a integração ponto a ponto. Por outro lado, forma-se uma zona implícita de confiança entre o *gateway* e os recursos, suprimindo as informações contextuais mais granulares oferecidas pelo primeiro modelo [Alevizos et al., 2022]. Este modelo pode ser útil para organizações que utilizam microsserviços baseados em nuvem para um único processo de negócios na qual toda a nuvem privada está localizada atrás de um *gateway* [Stafford, 2020]. Como desvantagem é que o *gateway* protege um conjunto de recursos, podendo não ser capaz de proteger cada recurso individualmente. Isso pode permitir que entidades acessem recursos aos quais não têm privilégios de acesso, caracterizando assim uma possível falha.

O modelo baseado em Portal, não requer a instalação de agentes nos dispositivos, sendo todas as solicitações de acesso encaminhadas a um portal [Tsai et al., 2024], conforme Figura 2.7. O principal benefício desse modelo em relação aos outros, reside no fato de não ser necessário a instalação de nenhum componente, sendo mais flexível em casos que se adote políticas de BYOD. No entanto, informações limitadas podem ser inferidas a partir dos dispositivos que solicitam acesso. Este modelo só consegue escanear e

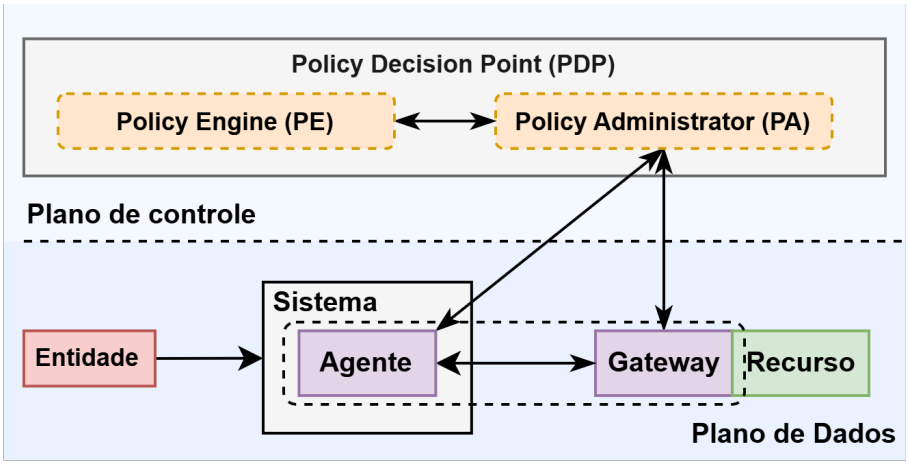


Figura 2.5. Arquitetura baseada no modelo agente-gateway. Esse modelo está dividido em dois planos: o Plano de Controle, onde se encontra o Ponto de Decisão de Política (PDP), composto pelo Policy Engine (PE) e pelo Policy Administrator (PA); e o Plano de Dados, que contém o Sistema, formado por um Agente e um Gateway, além do Recurso a ser acessado. A Entidade realiza uma solicitação, que é avaliada pelo Agente e encaminhada ao Gateway. As decisões de controle são tomadas com base nas políticas definidas no PDP.

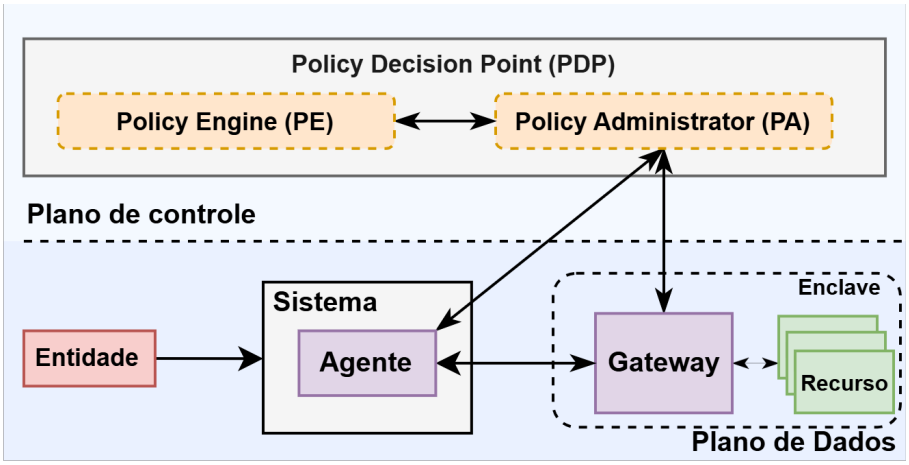


Figura 2.6. Arquitetura de controle de acesso com enclave de recursos. O Plano de Controle, onde atua o Ponto de Decisão de Política (PDP), composto pelo Policy Engine (PE) e pelo Policy Administrator (PA), e o Plano de Dados, onde a Entidade interage com o Sistema. O Sistema contém um Agente que se comunica com o Gateway, localizado em um Enclave junto aos Recursos protegidos. O PA aplica as decisões do PE, controlando o acesso por meio do Gateway conforme as políticas previamente definidas.

analisar ativos e dispositivos quando eles se conectam ao portal PEP e pode não ser capaz de monitorá-los continuamente em busca de atividades suspeitas, vulnerabilidades não corrigidas e configurações apropriadas [Stafford, 2020]. Um ponto de atenção, é o fato do portal se tornar um potencial alvo de ataques DDoS. Um único ponto de falha, pode interromper todos os serviços da organização. Nesse sentido, é mandatório que o portal seja bem provisionado para fornecer disponibilidade contra um ataque DoS ou interrupção da rede.

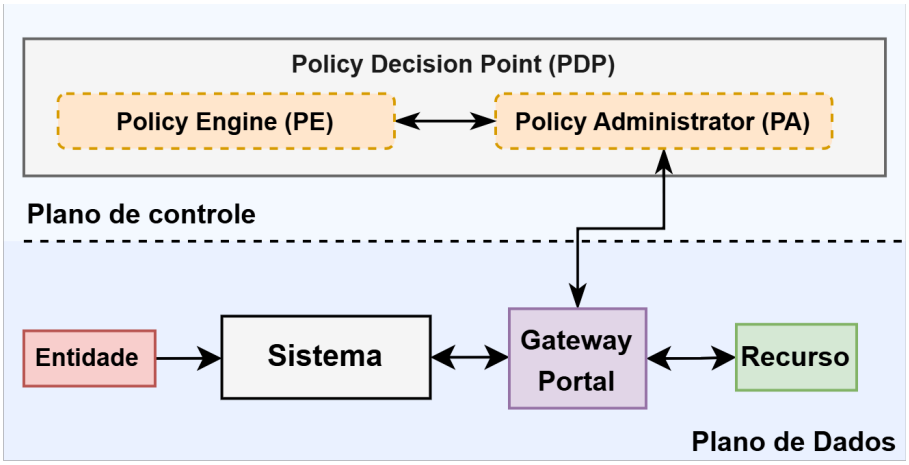


Figura 2.7. Arquitetura de controle de acesso baseado em portal. O Policy Decision Point (PDP), composto pelo Policy Engine (PE) e pelo Policy Administrator (PA), toma decisões com base em políticas definidas. A Entidade realiza uma solicitação ao Sistema, que interage com o Gateway Portal. O acesso ao Recurso é autorizado ou negado conforme as instruções do PA, que aplica decisões do PE.

Um dos principais desafios na implementação desse paradigma pelas organizações encontra-se na dificuldade de criar processos e políticas que atendam aos requisitos da arquitetura de confiança zero. Para que a implementação seja eficaz, todos os recursos que se deseja proteger precisam estar previamente mapeados o que exige um grande esforço dependendo do tamanho da organização. Outro aspecto desafiador na implementação é o gerenciamento de identidades. Em modelos tradicionais, esse gerenciamento enfrenta um problema central: dependência de uma terceira parte confiável. Esses sistemas foram desenvolvidos para facilitar a administração das bases de usuários pelas empresas, mas acabam limitando o poder dos próprios indivíduos sobre seus dados. Os usuários muitas vezes não sabem quais informações estão sendo coletadas, como são utilizadas ou com quem são compartilhadas. Esse desequilíbrio compromete a privacidade, a segurança e a autonomia digital das pessoas. Nesse contexto, a Identidade Autossoberana (*Self-Sovereign Identity* - SSI) surge como uma abordagem alternativa [Satybaldy et al., 2024]. Baseada em tecnologias descentralizadas, como *blockchain*, a SSI permite que os próprios usuários gerenciem suas identidades digitais. Ao inverter a lógica tradicional, a SSI devolve aos indivíduos a posse e o controle de suas informações, promovendo um ambiente digital mais seguro, transparente e centrado no usuário.

Mukta *et al.* propõem uma arquitetura de controle de acesso descentralizada e orientada por princípios de confiança zero, que integra identidades autossoberanas (*Self-Sovereign Identity* - SSI), identificadores descentralizados (*Decentralized Identifier* - DID), e controle de acesso baseado em capacidades (CapBAC). A proposta visa resolver as limitações de modelos tradicionais de controle de acesso, como a centralização da gestão de identidades e a ausência de verificação contínua de confiança, especialmente em ambientes dinâmicos e distribuídos. Com SSI e DIDs, os usuários mantêm controle direto sobre suas identidades e podem comprovar atributos sem revelar informações desnecessárias, enquanto o uso de CapBAC permite a delegação de acessos de forma segura, rastreável e com granularidade [Mukta et al., 2025].

2.5. Plataforma OpenZiti para Arquitetura de Confiança Zero: Exemplo Prático

OpenZiti[8] é um projeto de código aberto que permite incorporar redes de confiança zero diretamente em aplicações. Sua principal proposta consiste na simplificação da gestão de redes, ao elevar a identidade do usuário ou da aplicação, em vez do endereço IP, ao papel central da infraestrutura de rede. Essa abordagem permite reduzir complexidades inerentes das redes, como IPs estáticos, sub-redes, NAT e firewalls, que frequentemente se tornam obstáculos, pois necessitam de conhecimento especializado. A arquitetura do OpenZiti é composta por um controlador, roteadores de borda (*edge routers*) e roteadores *fabric* (*fabric routers*), que trabalham em conjunto para formar a estrutura de confiança zero. O projeto oferece SDKs que permitem a integração direta em aplicações, além de disponibilizar aplicativos de tunelamento que estendem o acesso a aplicações que não podem ser modificadas para incorporar os SDKs. Os principais componentes do OpenZiti a nível de aplicação:

- **Controlador Ziti** (*Ziti Controller*) funciona como o componente central, responsável pelo plano de controle da rede. É o primeiro elemento a ser configurado e iniciado, pois armazena e gerencia todas as informações de configuração dos roteadores, serviços, políticas e identidades. Uma das funções do controlador é a capacidade de estabelecer e atualizar dinamicamente as rotas para os serviços em nome dos clientes e roteadores, adaptando-se a mudanças na topologia da rede ou otimizando para maior eficiência.

- **Roteador de borda** (*edge router)* é o principal ponto de entrada e saída de tráfego para clientes, como aplicações com SDKs ou *tunnelers*, permitindo que acessem ou disponibilizem serviços de forma segura. Cada roteador possui identidade criptográfica própria e é previamente registrado no *controller*, e, quando designado como Edge Router, passa a autenticar, criptografar e autorizar todo o tráfego conforme políticas definidas, além de participar do roteamento interno, interceptar fluxos TCP/UDP provenientes de interfaces LAN ou WAN, e encaminhar tráfego para hosts sem *tunnelers*.

Esses são os principais componentes necessários para estabelecer uma rede com aplicações baseadas no modelo de confiança zero. Uma vez implementados, passa-se à próxima etapa: a configuração lógica do ambiente, para a qual é necessário compreender os conceitos de Identidades, Serviços e Políticas[9]. As **Identidades** representam *endpoints* individuais com a capacidade de estabelecer conexões. A segurança dessas interações é garantida através de autenticação mútua, empregando certificados X.509. Cada identidade é intrinsecamente vinculada ao seu certificado, tipicamente por meio da sua impressão digital. Ao iniciar uma conexão, o cliente na borda apresenta seu certificado. A infraestrutura de rede, então, realiza a validação do certificado. Este processo não apenas autentica a identidade, confirmando sua veracidade, mas também a autoriza, definindo os limites de

[8]Disponível em `https://openziti.io/`.

[9]Disponível em `https://openziti.io/docs/learn/introduction/components`.

seus privilégios. Somente após essa validação e autorização, os serviços específicos para os quais a identidade possui permissão são disponibilizados.

O **Serviço** é a unidade lógica que encapsula qualquer recurso acessível por clientes, definido por uma identidade, caracterizada por um nome e/ou certificado, ao invés de depender de conceitos de infraestrutura como DNS ou endereços IP; esse modelo proporciona um *namespace* praticamente ilimitado para identificação e abstrai do usuário final a complexidade do encaminhamento, pois o serviço apenas declara o roteador de borda a utilizar para a saída do tráfego da rede, podendo esse roteador coincidir ou não com o de entrada: se forem distintos, a própria rede realiza o roteamento interno necessário, de modo que basta ao usuário referir-se ao serviço para que todo o restante seja tratado automaticamente.

As **Políticas** definem as regras que controlam como identidades, serviços e roteadores de borda interagem entre si. Para que uma identidade possa acessar um determinado serviço, é necessário que haja uma associação explícita entre ambos. Como todo o tráfego destinado a um serviço é encaminhado por meio de um ou mais roteadores de borda, tanto a identidade quanto o serviço precisam ter permissão para utilizar o mesmo roteador, ou um conjunto comum de roteadores, garantindo, assim, que a comunicação ocorra de forma segura e controlada. Na plataforma OpenZiti existem as seguintes políticas:

- As **Políticas de Serviço** (*Service Policies*) definem a relação entre identidades e serviços dentro do OpenZiti. Nesse sentido, pode ser composta por um conjunto de serviços (aplicações) e um grupo de identidades. Quando um serviço é adicionado a uma Política de Serviço, todas as identidades associadas àquela política passam a ter acesso a esse serviço. Da mesma forma, ao incluir uma identidade em uma Política de Serviço, essa identidade adquire permissão para acessar os serviços definidos na política. Essas políticas são ainda responsáveis por determinar quais identidades podem acessar (*dial*) um serviço quanto quais podem fornecer ou hospedar (*bind*) esse serviço. No entanto, cada Política de Serviço pode permitir apenas um desses tipos de acesso por vez ou *dial* ou *bind*, nunca ambos simultaneamente.
- As **Políticas de Roteador de Borda** (*Edge Router Policies*) são responsáveis pelo mapeamento entre identidades e roteadores de borda. Cada política pode ser composta por um grupo de roteadores de borda e um grupo de identidades. Ao adicionar um roteador a uma Política de Roteador de Borda, todas as identidades associadas a essa política passam a ter acesso ao roteador em questão. Da mesma forma, ao incluir uma identidade em uma Política de Roteador de Borda, essa identidade adquire permissão para acessar os roteadores definidos na política.
- As **Políticas de roteador de borda de serviço** (*Service Edge Router Policie*s) atuam para mapear grupos de serviços existentes com um ou mais roteadores de borda. Ao adicionar um roteador de borda a esta classe de política, concederá os serviços associados a essa mesma política, ao roteador de borda e vice versa.

Para atender à diversidade de necessidades organizacionais e possibilitar uma transição gradual para o modelo de confiança zero, o OpenZiti oferece três modelos distintos de acesso:

- ***Zero Trust Application Access* (ZTAA)** é o modelo mais abrangente, como foco na segurança das comunicações entre aplicações. É projetado para simplificar implementações em ambientes multi-cloud , eliminando a confiança implícita na rede subjacente, incluindo a rede do host.

- ***Zero Trust Host Access* (ZTHA)** é o modelo que foca em proteger as comunicações a nível de *host*. A integração com soluções legadas ou existentes é viabilizada por meio do OpenZiti Tunneler, que encapsula aplicações tradicionais sem exigir modificações em seu código. Essa abordagem elimina a necessidade de confiar na rede subjacente, ao mesmo tempo em que garante que os firewalls — tanto de rede quanto do sistema operacional — operem em modo de negação por padrão, permitindo apenas o tráfego explicitamente autorizado. No entanto, neste modelo, apenas a rede do host é considerada uma zona de rede confiável.

- ***Zero Trust Network Access* (ZTNA)** tem como objetivo proteger o acesso a aplicações e serviços dentro de uma zona de rede segura. Seu funcionamento ocorre utilizando um OpenZiti Router. Embora o *firewall* de rede opere em modo de negação por padrão, os *firewalls* do sistema operacional ainda requerem regras de porta de entrada por serviço. Esse modelo permite o acesso de confiança zero em dispositivos que não podem instalar um OpenZiti Tunneler. Isso o torna especialmente adequado para organizações que estão no início de sua jornada rumo à confiança zero, mas que já enfrentam demandas urgentes por segurança reforçada e controle de acesso granular.

Com os conceitos previamente explorados, é possível iniciar a implementação da infraestrutura OpenZiti. No presente exemplo prático, é abordada a configuração utilizando o modelo ZTNA. Para isso, foram provisionados servidores em nuvens públicas utilizado o sistema operacional Debian 12, que desempenharão as funções de controlador e roteador de borda.

2.5.1. Configuração do Controlador

O primeiro passo consiste em instalar o binário do controlador OpenZiti, conforme o Código Fonte 2.1. Uma vez instalados é necessário configurar o arquivo com variáveis de ambiente boostrap.env e incluir as informações conforme o Código Fonte 2.2. É importante ressaltar que as configurações dos registros de DNS e regras de *firewall* dos servidores já estejam previamente criados.

Código Fonte 2.1. Instalação do controlador OpenZiti.

```
1 # Instalação do Controlador OpenZiti
2 apt update && apt upgrade -y
3 curl -sS https://get.openziti.io/install.bash | sudo bash -s
   ↪ openziti-controller
4 vim /opt/openziti/etc/controller/bootstrap.env
```

Código Fonte 2.2. Configuração do bootstrap do Controlador OpenZiti.

```
# the controller's permanent FQDN (required)
ZITI_CTRL_ADVERTISED_ADDRESS='controller.zetin.uff.br'

# the controller's advertised and listening port (default: 1280)
ZITI_CTRL_ADVERTISED_PORT='1280'

# name of the default user (default: admin)
ZITI_USER='admin'

# password will be scrubbed from this file after
# creating default admin during database initialization
ZITI_PWD='PASSWORD'

# additional arguments to: ziti create config controller
ZITI_BOOTSTRAP_CONFIG_ARGS=''
```

Para configurar as variáveis de ambiente do controlador é necessário gerar o arquivo completo e iniciar o serviço. O Código Fonte 2.3 apresenta os comandos para executar essas tarefas.

Código Fonte 2.3. Inicialização do Controlador OpenZiti.

```
/opt/openziti/etc/controller/bootstrap.bash
systemctl enable --now ziti-controller.service
```

Inicializado o controlador, todo o gerenciamento pode ser realizado por meio da interface de linha de comando (*Command-Line Interface* - CLI). No entanto, também é possível instalar uma interface gráfica, que torna o processo de administração mais intuitivo e acessível. O Código Fonte 2.4 apresenta os comandos necessários para execução desta tarefa.

Código Fonte 2.4. Configuração da interface gráfica.

```
mkdir -p /var/lib/ziti-controller/
wget https://github.com/openziti/ziti-console/releases/latest/download
 ↪  /ziti-console.zip
unzip -d /var/lib/ziti-controller/zac ./ziti-console.zip
```

Após a instalação, é necessário adicionar o caminho para o código no arquivo de configuração. Edite o arquivo `/var/lib/ziti-controller/config.yml` e adicione as seguintes linhas ao final do bloco `web` como ilustrado no Código Fonte 2.5. Com o controlador e a interface gráfica configurados, é possível realizar a autenticação na plataforma e iniciar todo processo de configuração de identidades, serviços e do roteadores de borda, conforme ilustrado na Figura 2.8.

Código Fonte 2.5. Arquivo de configuração da interface gráfica.

```
      - binding: zac
        options:
          location: /var/lib/ziti-controller/zac
          indexFile: index.html
```

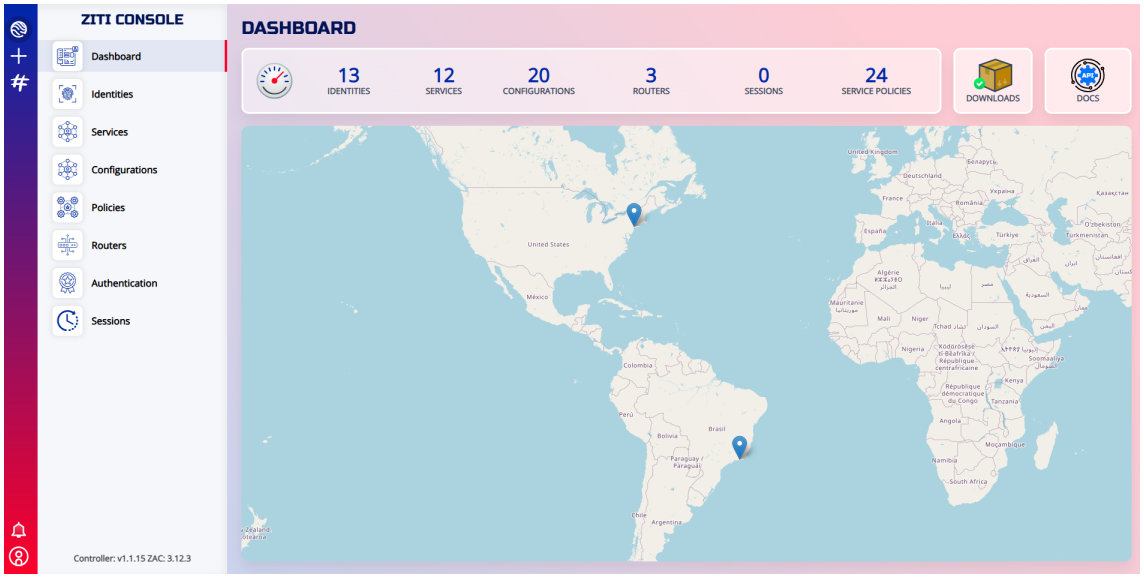


Figura 2.8. Tela inicial de gerenciamento da plataforma OpenZiti.

2.5.2. Configuração do Roteador de Borda

Esta etapa consiste na configuração de, no mínimo, um roteador de borda. Vale ressaltar que, dependendo da estratégia de implementação adotada, pode ser necessário configurar múltiplos roteadores, a fim de atender a requisitos específicos, como localização geográfica ou segmentação por serviços. Neste exemplo, será configurado um único roteador de borda em um servidor Linux Debian 12. Porém, é necessário criar logicamente o roteador para obter seu *token* de autenticação. A Figura 2.9 ilustra o processo para se criar o roteador. Uma vez concluída esta tarefa, é possível obter o *token* no formato jwt conforme Figura 2.10

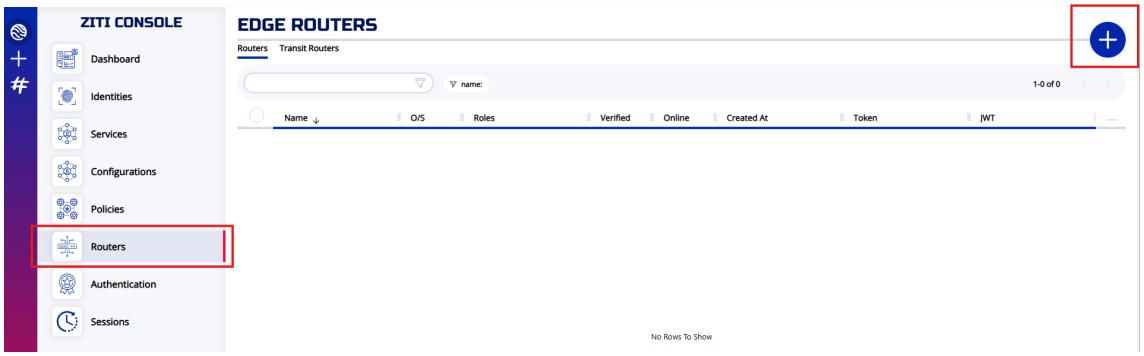


Figura 2.9. Configuração do roteador de borda.

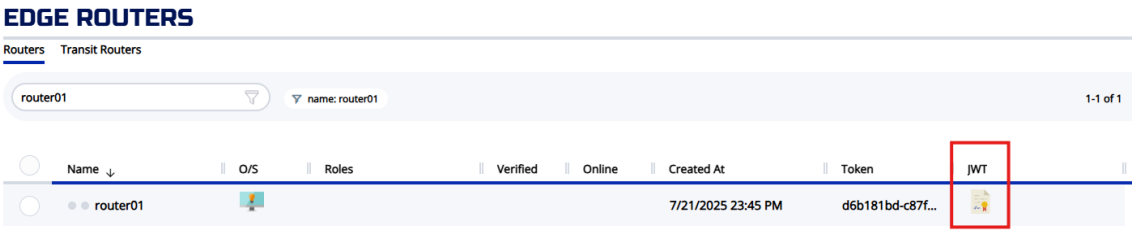


Figura 2.10. Obtenção do token para *enroll*.

Após a configuração lógica, é inicia-se a implementação do roteador de borda. Esse processo é semelhante ao da configuração do controlador, conforme ilustrado no Código Fonte 2.6. Um ponto de atenção fundamental é o uso do *token* gerado durante a etapa de configuração lógica. Esse *token* deve ser atribuído à variável ZITI_ENROLL_TOKEN e só pode ser utilizado uma única vez. Por isso, é essencial garantir que ele seja corretamente aplicado no momento do provisionamento, evitando erros ou a necessidade de gerar um novo *token*. Após configurado, é possível iniciar o serviço do roteador conforme o Código Fonte 2.7.

Código Fonte 2.6. Instalação do Roteador de Borda OpenZiti.

```
# Instalação do Controlador OpenZiti
apt update && apt upgrade -y
curl -sS https://get.openziti.io/install.bash | sudo bash -s
 ↪  openziti-router
vim /opt/openziti/etc/router/bootstrap.env

#Edite o arquivo boostrap.env e insira as seguintes informações

# the controller's DNS name (required)
ZITI_CTRL_ADVERTISED_ADDRESS='FQDN'

# the controller's port (default: 1280)
ZITI_CTRL_ADVERTISED_PORT='1280'

# this router's DNS name or IP address (default: localhost)
ZITI_ROUTER_ADVERTISED_ADDRESS='router01.zetin.uff.br'

# this router's port (default: 3022), if <= 1024,
# then grant the NET_BIND_SERVICE ambient capability in
# /etc/systemd/system/ziti-router.service.d/override.conf
ZITI_ROUTER_PORT='3022'

# token will be scrubbed from this file after enrollment
ZITI_ENROLL_TOKEN='TOKEN'

```

Código Fonte 2.7. Inicialização do roteador de borda OpenZiti.

```
/opt/openziti/etc/router/bootstrap.bash
systemctl enable --now ziti-router.service
```

2.5.3. Configuração das Identidades

A próxima etapa consiste na criação das identidades. A identidade é uma peça fundamental do OpenZiti, uma vez que é utilizada tanto pelos clientes (que realizam o *dial*) quanto pelos servidores (que hospedam as aplicações). Nesse exemplo, serão criadas duas identidades, Servidor1 e Cliente1, conforme Figura 2.11.

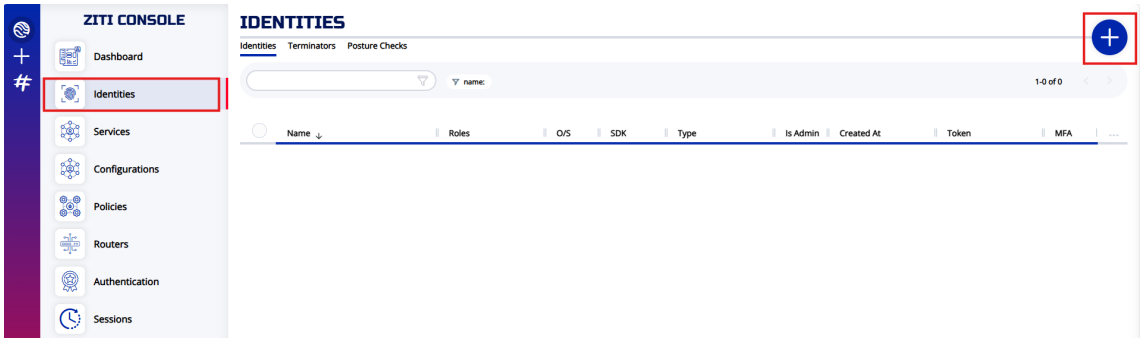


Figura 2.11. Criação de identidades no OpenZiti.

Ambas as identidades devem ser salvas conforme Figura 2.12 para serem configuradas nos respectivos ambientes.

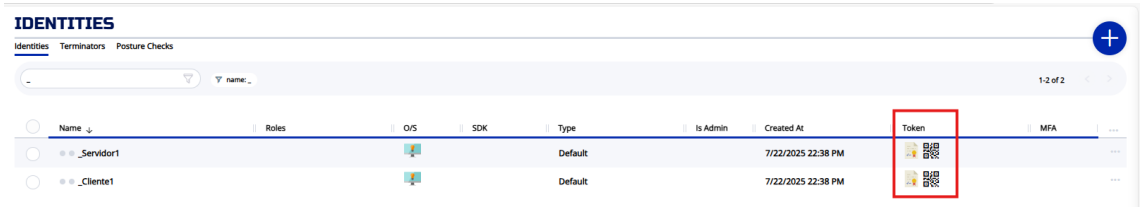
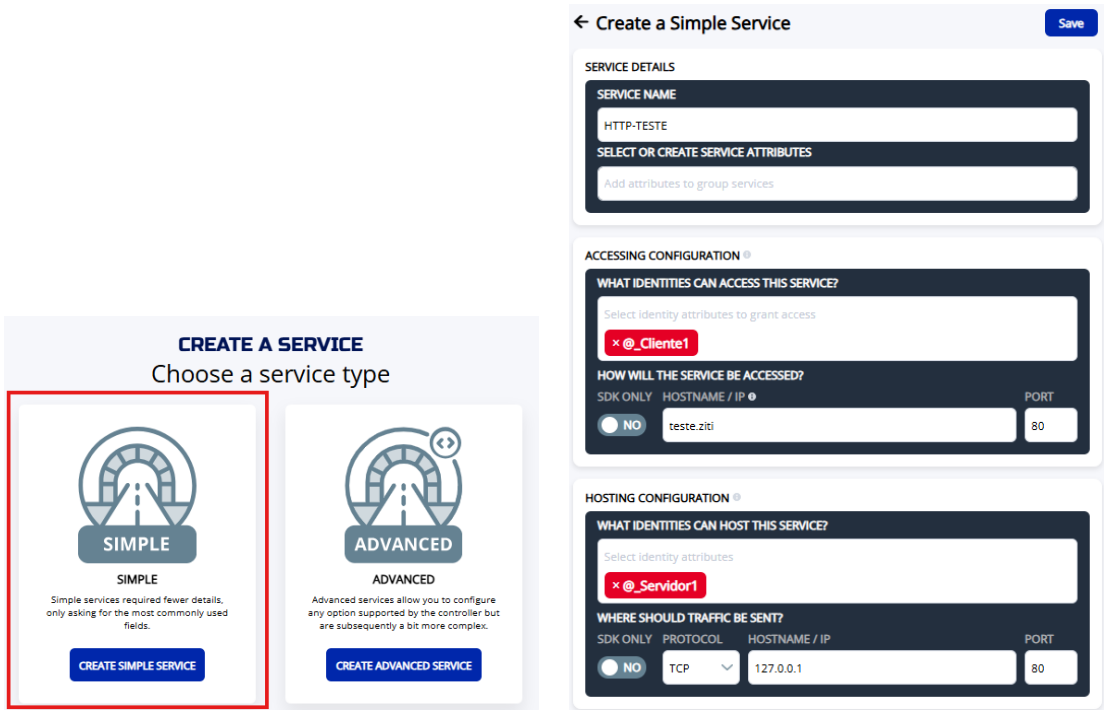


Figura 2.12. Identidades do servidor e cliente.

2.5.4. Configuração dos Serviços

Os serviços podem ser configurados através do CREATE SIMPLE SERVICE ilustrado pela Figura 2.13(a) acessado através do menu **Services**. Com está configuração, as **políticas de serviços** também serão criadas, tornando o processo mais intuitivo. O serviço depende de duas configurações essenciais para operar corretamente. A primeira é o acesso, que define quais identidades tem permissão para usá-lo, conforme Figura 2.13(b).Esta configuração é utilizada pelo cliente, indicando qual será o hostname e porta que serão interceptados para encaminhamento ao host que hospeda o serviço. A outra configuração é relacionado ao host, também ilustrado na Figura 2.13(b). Nessa configuração, o hostname ou IP deverão ser preenchidos com base em como o host consegue

se comunicar com a aplicação. Neste exemplo, como a aplicação é executada localmente, basta inserir o endereço IP da interface do host.

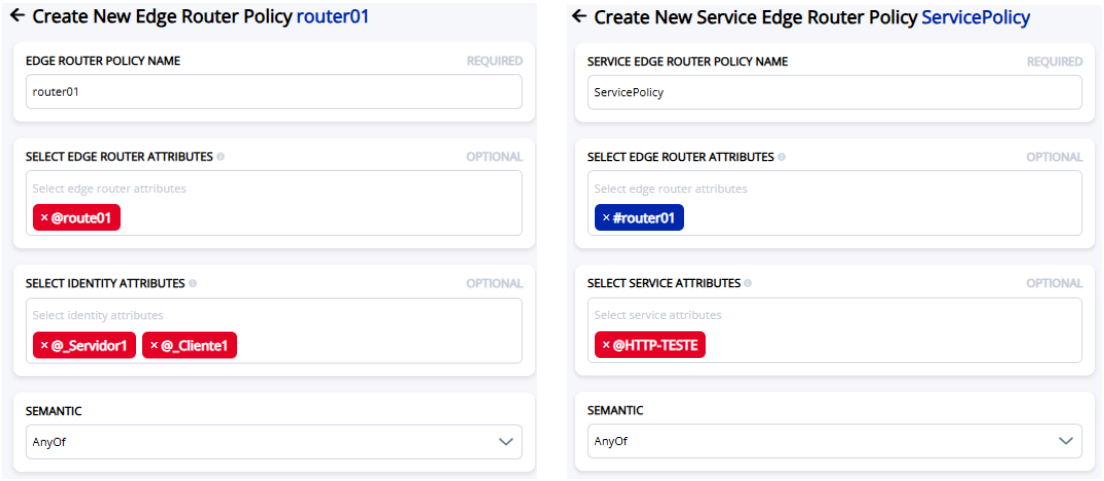


(a) Modos disponíveis para criação de um serviço. (b) Configuração de atributos de um serviço.

Figura 2.13. Criação de um serviço básico dentro do controlador OpenZiti.A Figura 2.13(a) ilustra os modos para criar os serviços, sendo eles o Simples e Avançado. A Figura 2.13(b) apresenta as configurações necessárias para mapear os atributos de acesso e hospedagem do serviços.

2.5.5. Configuração das Políticas

A última etapa da configuração no controlador OpenZiti consiste na criação das políticas do roteador de borda. Elas definem quais identidades (usuários, dispositivos, serviços) estão autorizadas a se conectar a determinados *edge routers* da rede Ziti. Essa definição é essencial, pois, para que uma identidade possa utilizar ou oferecer um serviço, é necessário que se conecte à rede por meio de um roteador autorizado. Para isso, acesse o menu *Policies* e, em seguida, ***Router Policies***. Após clicar no símbolo +, uma janela será exibida para o preenchimento dos dados, conforme a Figura 2.14(a). Neste momento, serão selecionados os atributos que compõem a política do *router01*. Neste exemplo, as identidades *Servidor1* e *Cliente1* terão permissão para acessar o roteador de borda *router01*. Com isso, o tráfego entre cliente e servidor, necessário para acessar ou hospedar um serviço, será encaminhado por esse roteador. A última política a ser configurada é ***Service Router Policies***, que determina quais roteadores podem hospedar e acessar serviços específicos, permitindo controlar e otimizar o caminho do tráfego com base em critérios como proximidade geográfica, desempenho ou disponibilidade.



(a) Política do roteador de borda.

(b) Política de serviço do roteador de borda.

Figura 2.14. Configuração das políticas do OpenZiti. A Figura 2.14(a) ilustra a configuração para criar as políticas do roteador de borda, relacionando quais identidades podem se conectar a um determinado roteador. Enquanto a Figura 2.14(b) relaciona quais serviços podem se associar a um roteador.

2.5.6. Configuração do Cliente

O OpenZiti oferece suporte à configuração de clientes em diversas plataformas. No caso do Windows, é necessário instalar o Ziti Desktop Edge, disponível no site oficial. Após a instalação, a identidade gerada deverá ser importada por meio da interface gráfica do aplicativo. Neste exemplo, foi utilizada uma identidade no formato .jwt, com o nome Cliente1. Uma vez autenticado, o aplicativo passa a interceptar e redirecionar o tráfego de rede para os serviços definidos na configuração, garantindo um acesso seguro e direto, sem a necessidade de VPNs tradicionais. Todo o acesso

2.5.7. Indicadores e Métricas Práticas

A adoção de uma Arquitetura de Confiança Zero (ZTA) impõe desafios operacionais e de desempenho, especialmente em ambientes de produção com restrições de recursos ou requisitos de latência. Para garantir sua viabilidade técnica e justificar sua implantação, é fundamental o uso de métricas objetivas que permitam comparar diferentes implementações, otimizar componentes críticos e avaliar sua resiliência. Indicadores funcionais estão relacionados à eficácia dos mecanismos centrais de controle e verificação da ZTA:

- **Tempo de Autenticação (T_{auth}).** Tempo médio entre a solicitação de acesso e a validação de identidade e dispositivo.
- **Latência de Autorização (T_{policy}).** Tempo de resposta do mecanismo de *enforcement* de políticas (Policy Decision/Enforcement Points).
- **Taxa de Acesso Permitido / Negado.** Razão entre decisões de permissão e bloqueio, útil para calibrar políticas e evitar falsos positivos.

- **Tempo de Detecção de Comportamento Anômalo (T_{anom}).** Tempo entre o início de uma atividade suspeita e sua detecção pelo mecanismo de monitoramento.

A aplicação da ZTA em dispositivos IoT e redes de borda exige atenção especial ao consumo de recursos locais:

- **Uso Médio de CPU (%CPU).** Percentual médio de utilização do processador durante sessões autenticadas.
- **Consumo de Memória (MB).** Memória média ocupada pelos agentes de confiança e mecanismos de autorização locais.
- **Overhead de Tráfego (ΔBW).** Aumento percentual no tráfego de rede causado por trocas de autenticação, verificação de contexto e atualizações de políticas.

A capacidade da arquitetura em manter sua funcionalidade frente a falhas ou ataques é avaliada por métricas de disponibilidade e recuperação:

- **Tempo Médio de Recuperação (MTTR).** Tempo necessário para restaurar o controle de acesso após falha ou comprometimento de um componente.
- **Taxa de Falsos Positivos/Negativos.** Incidência de decisões incorretas de bloqueio ou permissão frente a atividades legítimas ou maliciosas.
- **Disponibilidade dos Serviços de Autorização.** Percentual de tempo em que os mecanismos de autorização estão acessíveis e operacionais.

Essas métricas permitem uma abordagem baseada em evidência para decisões de projeto e ajuste de ZTA, suportando a definição de SLAs (Service Level Agreements), auditoria de conformidade e benchmarking entre soluções concorrentes. A sistematização de tais indicadores deve fazer parte de um processo contínuo de avaliação e melhoria da postura de segurança.

2.6. Estudos de Caso em Ambientes Reais

No setor corporativo, a adoção de ZTA vem sendo impulsionada pela necessidade de proteger acessos remotos, dados sensíveis e aplicações em nuvem contra acesso não autorizado e movimento lateral. Um exemplo recorrente é o uso de autenticação federada integrada a controles baseados em atributos (ABAC), em que políticas de acesso são definidas não apenas pela função do usuário, mas também por seu local de origem, horário, tipo de dispositivo e postura de segurança. Empresas que migraram para ambientes SaaS têm utilizado motores de decisão contextual e segmentação de acesso por carga de trabalho. Mecanismos de telemetria contínua são empregados para ajustar dinamicamente permissões, bloquear sessões anômalas e mitigar ataques de elevação de privilégio [Gupta et al., 2024, He et al., 2022].

Tabela 2.7. Estudos de caso com aplicação de *Zero Trust Architecture*

Domínio	Cenário de Aplicação	Técnicas ZTA Empregadas	Benefícios Observados
Corporativo	Acesso remoto e SaaS com verificação de contexto	ABAC, autenticação federada, avaliação de postura de dispositivo	Redução de superfícies de ataque, controle granular, conformidade regulatória
Rede federada	Compartilhamento de dados entre universidades e centros médicos	Identidade auto-soberana, *blockchain*, contratos inteligentes	Controle fine-grained, rastreabilidade, interoperabilidade entre domínios
Infraestrutura crítica	Segmentação de redes industriais e proteção de UAVs	Segmentação lógica, autenticação contínua, controle baseado em atributos	Resiliência a ataques, disponibilidade operacional, detecção de anomalias

Um segundo estudo relevante refere-se à aplicação de ZTA em redes federadas para colaboração científica. Ambientes como consórcios de pesquisa médica, universidades interligadas e plataformas de compartilhamento de dados sensíveis exigem um modelo de confiança distribuída. Nestes casos, a arquitetura *Zero Trust* é complementada pelo uso de *blockchain* e identidade digital auto-soberana (SSI), permitindo que múltiplas instituições compartilhem dados e recursos sem depender de uma autoridade centralizada [Tuler De Oliveira et al., 2022, de Oliveira et al., 2024, Pooja e Chandrakala, 2024]. Contratos inteligentes são utilizados para registrar e auditar acessos, enquanto decisões baseadas em atributos controlam permissões granulares. A rastreabilidade e a transparência se tornam elementos fundamentais para garantir confiança inter-organizacional, especialmente quando há exigências regulatórias como GDPR ou LGPD.

Em contextos de infraestrutura crítica, como redes de energia, hospitais, sistemas industriais (ICS/SCADA) e operações militares, os desafios de segurança são amplificados por fatores como conectividade intermitente, requisitos de tempo real e criticidade operacional. Nestes domínios, a ZTA é aplicada para segmentar logicamente redes industriais, autenticar continuamente sensores e atuadores, e aplicar políticas condicionais baseadas em localização, tempo e comportamento do dispositivo. Em sistemas de controle de tráfego aéreo e redes de UAVs, por exemplo, a ZTA tem sido usada para isolar domínios operacionais, aplicar autenticação baseada em certificados e monitorar desvios em rotinas de comunicação [Nahar et al., 2024, Dhiman et al., 2024, Gambo e Almulhem, 2025]. A resiliência a ataques persistentes é obtida por meio de microsegmentação combinada com motores de decisão assistidos por IA e detecção de anomalias.

Esses estudos de caso demonstram que a adoção da ZTA é viável e benéfica em diversos cenários, embora apresente desafios específicos conforme o domínio. Em ambientes corporativos, os ganhos em controle de acesso e visibilidade são evidentes, mas exigem integração com ferramentas modernas de identidade e autenticação. Em redes federadas, a descentralização da confiança amplia a escalabilidade da colaboração, mas impõe desafios de padronização e interoperabilidade. Já em infraestruturas críticas, a aplicação de ZTA exige compatibilidade com protocolos legados, operação em tempo real e alta confiabilidade.

A maturidade das soluções ZTA aplicadas a esses cenários ainda está em evolução. A integração com inteligência artificial para decisões de acesso adaptativas, a auditoria

baseada em *blockchain* e a aplicação de modelos de reputação estão entre os próximos passos para fortalecer a resiliência desses ambientes. O desenvolvimento de plataformas que ofereçam ZTA como serviço e ferramentas *open source* como OpenZiti favorecem a democratização dessa arquitetura em organizações de diferentes portes. À medida que surgem novas ameaças e regulamentações, a capacidade de adaptar e observar o comportamento da rede em tempo real será um diferencial estratégico na aplicação prática da *Zero Trust Architecture*.

2.6.1. Zero Trust em Ambientes Críticos: UAVs e IoBT

Ambientes críticos como operações militares, sistemas de defesa cibernética e redes de sensores táticos exigem altos níveis de confiabilidade, disponibilidade e segurança. A *Internet of Battlefield Things* (IoBT) e os veículos aéreos não tripulados (*Unmanned Aerial Vehicles* - UAVs) representam elementos essenciais nesses contextos, sendo amplamente utilizados para reconhecimento, vigilância, entrega de cargas e apoio à decisão. Contudo, essas plataformas estão expostas a ciberataques altamente sofisticados, tornando o modelo tradicional de segurança baseado em perímetro insuficiente. A *Zero Trust Architecture* (ZTA) se destaca como abordagem promissora para garantir segurança adaptativa e contínua nesses cenários, eliminando suposições implícitas de confiança em redes críticas e operando com base em verificação constante, privilégio mínimo e segmentação dinâmica [Alquwayzani e Albuali, 2024, Gupta et al., 2024].

No contexto militar, UAVs são utilizados para missões de *Intelligence, Surveillance and Reconnaissance* (ISR), frequentemente operando em redes sem infraestrutura fixa e com dispositivos móveis, intermitentes e heterogêneos. A ZTA permite isolar logicamente diferentes funções embarcadas, restringindo comunicações apenas ao necessário e aplicando autenticação contínua entre os módulos de controle, navegação, *payload* e telemetria. A segmentação fina possibilita impedir, por exemplo, que falhas em módulos de visão comprometam os canais de comando. Além disso, mecanismos como ABAC (controle baseado em atributos) ou PBAC (controle baseado em políticas) permitem decisões contextuais baseadas na missão, horário, tipo de sensor ou localização geográfica. Assim, apenas entidades que cumpram múltiplos critérios verificados em tempo real podem acessar fluxos críticos de controle, mitigando ataques como *hijacking*, *spoofing* e manipulação de carga útil [Alquwayzani e Albuali, 2024].

A IoBT estende esses desafios à escala de batalhões inteiros. Soldados, veículos, sensores, UAVs e dispositivos de comunicação formam redes móveis e intermitentes que devem ser gerenciadas de forma segura e adaptativa. A ZTA fornece as bases para criar domínios de confiança efêmeros e descentralizados. Microsegmentação dinâmica baseada em função e localização permite isolar fluxos de comando e controle dos fluxos de monitoramento ambiental. A aplicação de *machine learning* embarcado, combinada à telemetria contínua, permite detectar comportamentos anômalos e adaptar permissões automaticamente. Isso é viável mesmo em redes degradadas, por meio de modelos leves de aprendizado e uso de evidências parciais para classificação de risco [He et al., 2022].

Tecnologias de controle como SDN (*Software Defined Networking*) e a integração com redes 5G/6G aumentam a flexibilidade da orquestração de políticas em tempo real. Exemplos de frameworks operacionais como o TENA (*Test and Training Enabling Ar-*

Tabela 2.8. Comparação entre o uso da ZTA em domínios críticos e em domínios empresariais.

Critério	Domínios Críticos (UAVs, IoBT, Defesa)	Domínios Empresariais
Ambiente Operacional	Hostil, degradado, com conectividade intermitente e requisitos de missão	Controlado, com infraestrutura confiável e conectividade estável
Tipo de Dispositivo	Sensores embarcados, UAVs, dispositivos móveis militares	Estações de trabalho, servidores, laptops e dispositivos móveis corporativos
Requisitos de Segurança	Autenticação contínua, integridade de missão, controle sob ataque, operação sob falha	Conformidade regulatória, proteção de dados, disponibilidade de serviços
Topologia de Rede	Redes mesh dinâmicas, MANETs, infraestrutura distribuída e efêmera	Redes estáticas, híbridas ou em nuvem com perímetros conhecidos
Modelos de Controle de Acesso	ABAC/PBAC com verificação contextual e restrições baseadas em missão e localização	RBAC ou ABAC baseado em políticas organizacionais e funções fixas
Desafios Técnicos	Restrições energéticas, latência, confiabilidade da telemetria, interoperabilidade militar	Legado, resistência à mudança, integração com sistemas existentes
Automação e IA	Detecção autônoma de ameaças, análise embarcada e resposta local adaptativa	SIEM, automação de políticas, análise de logs e resposta centralizada
Padrões e Referências	DoD ZTA Reference Architecture, TENA, STIGs	NIST SP 800-207, ISO/IEC 27001, CIS Controls

chitecture) e a *DoD Zero Trust Reference Architecture* reforçam a viabilidade de soluções ZTA modulares e interoperáveis em contextos de defesa [Gupta et al., 2024].

Além dos ganhos operacionais, a ZTA em ambientes críticos enfrenta desafios técnicos significativos. A limitação de energia e processamento embarcado impõe restrições à aplicação de criptografia forte e algoritmos de aprendizado. A confiabilidade da coleta de contexto (*telemetria*) em ambientes hostis também é um fator limitante, já que sensores podem ser corrompidos ou operarem com latência. Em operações multinacionais, a interoperabilidade de políticas de acesso *Zero Trust* ainda requer padronizações robustas. Como caminhos futuros, propõe-se a adoção de inteligência federada para decisões de acesso distribuídas, bem como a integração de criptografia pós-quântica com autenticação contínua e verificação de integridade resiliente.

A aplicação de *Zero Trust* em UAVs e redes IoBT representa um avanço fundamental para a segurança de infraestruturas críticas e ambientes militares. A segmentação lógica, a verificação contextual e a capacidade de resposta adaptativa posicionam a ZTA como o novo paradigma para redes táticas confiáveis em tempos de guerra cibernética. A Tabela 2.8 apresenta uma comparação entre a aplicação da arquitetura *Zero Trust* em domínios críticos, como defesa e IoBT, e em contextos empresariais convencionais, destacando as diferenças em requisitos operacionais, tecnologias utilizadas, desafios e padrões de referência.

2.6.2. Colaboração Científica Descentralizada

A adoção de práticas colaborativas em ciência tem ampliado a complexidade dos ecossistemas de pesquisa, impondo novos requisitos à proteção de dados sensíveis. Em

ambientes compostos por múltiplas instituições e diferentes domínios de confiança, a *Zero Trust Architecture* (ZTA) emerge como alternativa robusta para assegurar confidencialidade, rastreabilidade e controle granular de acesso em atividades como revisão por pares e intercâmbio de dados experimentais. Soluções convencionais de revisão e compartilhamento operam com suposições de confiança implícita e autenticação insuficiente, o que expõe manuscritos e dados inéditos a riscos de vazamento, uso indevido e conflitos de interesse. A ausência de padronização entre instituições e jurisdições distintas agrava esse cenário, dificultando a harmonização das políticas de acesso [Pooja e Chandrakala, 2024].

Pooja e Chandrakala propõem um modelo baseado na combinação de ZTA, *blockchain* e contratos inteligentes para mitigar essas fragilidades [Pooja e Chandrakala, 2024]. As políticas de acesso consideram atributos contextuais, como afiliação, histórico de atuação e janela temporal de acesso, sendo avaliadas automaticamente por contratos inteligentes. O acesso a documentos é concedido apenas se a pontuação de confiança do revisor atingir o limiar mínimo, e os dados são protegidos com chaves derivadas temporalmente (HKDF), limitando sua exposição.

No compartilhamento de dados sob múltiplas restrições, como os clínicos ou envolvendo seres humanos, o sistema verifica se o requisitante atende aos critérios definidos por todos os controladores envolvidos. A decisão é tomada com base em interpolação de Lagrange entre políticas divergentes, permitindo decisões consensuais, auditáveis e flexíveis. Essa abordagem reduz o fenômeno de *data lock-in* e incentiva a reutilização responsável [Pooja e Chandrakala, 2024]. A arquitetura proposta é compatível com sistemas federados, como o *Federated Research Data Infrastructure* e com tecnologias como o *Hyperledger Fabric*. Sua integração reforça princípios como auditabilidade, exposição mínima de dados e responsabilização. O modelo permite ainda o uso de avaliações dos autores sobre os revisores, incorporando critérios reputacionais aos ciclos de seleção.

2.7. Projetos de Pesquisa e Desenvolvimento

Em um cenário cada vez mais dinâmico e conectado, o modelo de confiança zero está redefinindo a segurança cibernética, especialmente no contexto da Internet das Coisas (IoT) e das redes de próxima geração. Nesse sentido, abordagens de segurança proativa e adaptável tornam-se imperativas. Diversos projetos e iniciativas têm como objetivo expandir os horizontes desse modelo, explorando sua aplicação em áreas como saúde, redes 5G, privacidade e outros campos emergentes. O projeto NextSec propõe uma arquitetura para segurança em sistemas de próxima geração, para conectividade dispositivos IoT e pessoas, além de possibilitar comunicações máquina-a-máquina e fornecer recursos computacionais e de armazenamento com baixa latência. Os sistemas são essenciais para aplicações críticas como veículos autônomos e telecirurgia[10]. O projeto *Proactive End-to-End Zero Trust-Based Security Intelligence for Resilient Non-cooperative 5G Networks* visa desenvolver uma solução de segurança de ponta a ponta para aprimorar comunicações militares e de missão crítica através de redes 5G não confiáveis utilizando o princípio *Zero Trust*. O projeto também inclui o desenvolvimento de um currículo para treinamento em segurança 5G e a promoção da diversidade na pesquisa e desenvolvimento nesta área [11].

[10]Disponível em `https://www.nsf.gov/awardsearch/showAward?AWD_ID=2148374`.
[11]Disponível em `https://www.nsf.gov/awardsearch/showAward?AWD_ID=2226232`.

Por sua vez, o projeto *Zero-trust and Traceable Data Infrastructure for Health IoT Data Storage and Sharing* tem por objetivo desenvolver um ecossistema de compartilhamento de dados rastreável e de confiança zero onde a propriedade e o controle dos dados são devolvidos aos indivíduos que geram os dados. Nesse sentido, os proprietários dos dados poderão definir a política de acesso e compartilhamento que serão aplicados no modelo de confiança zero, ou seja, sem depender de coordenadores ou infraestrutura centrais[12].

O projeto Zero Trust X (ZTX) é uma iniciativa do Departamento de Defesa dos EUA para desenvolver uma solução de segurança de ponta a ponta, chamada *Zero Trust Chain* (ZTC), para o uso seguro e confiável de redes 5G em operações militares. Dada a defasagem dos EUA na fabricação de equipamentos de rede 5G e as vulnerabilidades de segurança das redes comerciais, o ZTX propõe um *software* que integra monitoramento de ameaças via Open-RAN (O-RAN) e 5G core, complementado por aprimoramentos de segurança nos dispositivos. Essa abordagem permite que as equipes militares compartilhem informações de forma segura em redes 5G de alto desempenho, mas potencialmente não confiáveis, detectando entidades maliciosas em tempo real e protegendo o tráfego do DoD, sem a necessidade de grandes modificações nas redes 5G existentes[13]

2.8. Desafios e Tendências Futuras

A *Zero Trust Architecture* (ZTA) consolida-se como um novo paradigma de segurança cibernética, desafiando o modelo perimetral tradicional ao adotar o princípio de "nunca confiar, sempre verificar". Embora sua adoção venha crescendo em diversos setores, desde redes corporativas até ambientes militares e infraestruturas críticas, a implementação prática da ZTA ainda encontra uma série de barreiras técnicas, operacionais e organizacionais. Esta seção discute os principais desafios que limitam a difusão ampla e eficaz da ZTA e aponta direções futuras promissoras para sua evolução.

2.8.1. Desafios de Implementação

A implementação eficaz da arquitetura de confiança zero enfrenta diversos desafios. A falta de padrões de comunicação entre dispositivos, arcabouços e plataformas utilizados podem são significativos [Bertino, 2021]. A necessidade de combinar grandes volumes de dados heterogêneos de várias fontes pode ser complexa e demorada. A micro-segmentação é crucial, porém enfrenta dificuldades em redes extensas devido à complexidade dos fluxos de trabalho e à tradução desafiadora de requisitos de acesso em políticas de controle de acesso aplicáveis tanto em nível de rede quanto de aplicativo. Os principais desafios na implementação da arquitetura de confiança zero incluem [Syed et al., 2022, Stafford, 2020]: (i) a integração com infraestruturas existentes, que demanda adaptação e migração complexas de sistemas legados; (ii) o gerenciamento robusto de identidades para autenticação e autorização contínuas também é essencial; (iii) a necessidade de monitoramento contínuo, requerendo tecnologias avançadas para detecção de ameaças em tempo real; e (iv) a adaptação é outra necessidade, permitindo que a arquitetura de confiança zero atenda às especificidades variadas de diferentes ambientes e casos de uso. A dificuldade de padronização e interoperabilidade entre soluções de diferentes

[12]Disponível em `https://www.nsf.gov/awardsearch/showAward?AWD_ID=2312973`.
[13]Disponível em `https://www.nsf.gov/awardsearch/showAward?AWD_ID=2515378`.

fornecedores, o que pode levar ao aprisionamento tecnológico, a ausência de formatos de dados comuns para troca de informações entre componentes de segurança; a necessidade de evitar interrupções na experiência dos usuários durante o processo de migração e a complexidade de definir níveis apropriados de confiança e classificar os recursos adequadamente podem ser obstáculos significativos nesta jornada. Além disso, lidar com dispositivos não gerenciados, como os oriundos de políticas BYOD, implica riscos adicionais devido à ausência de controle direto da organização. Outro ponto crítico é o aprimoramento contínuo do algoritmo de confiança, que deve incorporar informações de múltiplas fontes, como credenciais, localização, comportamento de rede e inteligência de ameaças, exigindo constante calibragem para evitar falsos positivos e negativos [Teerakanok et al., 2021].

A implementação da ZTA representa um paradigma de transformação profunda na forma como as organizações protegem seus ativos, usuários e dados. Um dos principais obstáculos é o **custo**, já que os investimentos necessários para modernizar infraestruturas legadas, adquirir novas ferramentas e treinar equipes podem ser substanciais. Embora os orçamentos destinados para aprimoramento da cibersegurança estejam crescendo, as restrições orçamentárias continuam sendo uma preocupação crítica. Um desafio recorrente são as **lacunas tecnológica**s. Muitas organizações ainda não dispõem de soluções adequadas para implementar políticas de acesso dinâmico, autenticação ou segmentação de rede baseada em identidade. A complexidade para integração entre sistemas legados e novas tecnologias também contribui para esse cenário, tornando difícil a orquestração de uma arquitetura coerente e segura. Outro aspecto importante são os **obstáculos regulatórios e legais**, como a necessidade de atender a exigências de privacidade e proteção de dados impostas por diferentes jurisdições. Isso exige atenção cuidadosa para garantir que as práticas de segurança estejam em conformidade com regulamentações como GDPR ou LGPD, dependendo do setor e da localização da empresa. Esse contexto regulatório pode tornar a implementação mais lenta e burocrática. A **escassez de profissionais qualificados** é outro fator que compromete o avanço dessas iniciativas. A demanda por especialistas em identidade, governança de acesso e segurança baseada em risco supera a oferta disponível no mercado, o que dificulta a formação de equipes capacitadas para conduzir o processo de adoção desse modelo. Esse déficit é especialmente crítico em organizações menores ou em setores que estejam iniciando sua jornada em infraestrutura digital.

Há ainda desafios de conscientização e adesão organizacional. Muitas vezes, os líderes ou equipes não compreendem completamente os benefícios desse modelo ou resistem à sua adoção por receio de impactos negativos. Diante desses desafios, é fundamental que as organizações adotem uma abordagem estratégica, baseada nas necessidades e com planejamento estruturado.

2.8.2. Desafios de Evolução da Arquitetura e Tendências Futuras

Um dos maiores obstáculos enfrentados na evolução e aplicação de ZTA em larga escala está relacionado à escalabilidade. Em arquiteturas que envolvem milhares ou milhões de dispositivos, como em ambientes IoT, redes 6G ou sistemas federados, o gerenciamento eficiente de identidades, políticas de acesso e contexto dinâmico torna-se uma tarefa complexa [Gambo e Almulhem, 2025]. A manutenção de políticas de acesso

granulares, associadas a múltiplos atributos, exige estruturas de governança robustas, sincronização entre domínios e mecanismos de distribuição de contexto em tempo real.

O desempenho também constitui um gargalo relevante. O modelo ZTA impõe verificações contínuas de identidade, postura do dispositivo, localização e tempo de acesso a cada solicitação. Esse processo, se não otimizado, pode introduzir latência excessiva e sobrecarga em sistemas sensíveis ao tempo, como controle industrial, comunicações táticas e serviços médicos [He et al., 2022, Barbosa et al., 2025]. Estratégias como cache de decisões de acesso, balanceamento entre política e contexto e uso de mecanismos locais de decisão vêm sendo exploradas para mitigar esse impacto.

A interoperabilidade entre domínios administrativos distintos representa outro desafio. A ausência de padronizações amplamente adotadas para troca de contexto, formatos de políticas e autenticação federada dificulta a integração de ZTA em ambientes colaborativos, como redes interinstitucionais, cadeias logísticas globais ou consórcios científicos [de Oliveira et al., 2024]. Embora existam iniciativas como o NIST SP 800-207 e modelos baseados em ABAC e PBAC, a heterogeneidade dos ecossistemas e a resistência a alterações estruturais dificultam a adesão ampla. Soluções emergentes têm buscado mitigar essas barreiras por meio da padronização de políticas e identidades. Um exemplo é a abordagem *Policy as Code*, cuja implementação mais conhecida é o *Open Policy Agent* (OPA)[14] em conjunto com a linguagem Rego, que permite expressar políticas de acesso de forma auditável, versionável e portável entre sistemas heterogêneos. No âmbito da padronização internacional, o grupo IETF propôs o *Security Automation and Continuous Monitoring* (SACM), voltado à automação do monitoramento e da verificação contínua de postura de segurança em redes federadas [Cam-Winget e Lorenzin, 2017]. Adicionalmente, frameworks de identidade federada baseados em *Identificadores Descentralizados* (DIDs) e *Credenciais Verificáveis* (VCs), como os definidos pelo W3C[15] e aplicados em sistemas como Trustbloc[16] ou Trust Over IP[17], oferecem mecanismos compatíveis com os princípios da ZTA ao eliminar dependência de autoridades centrais e permitir verificações criptográficas baseadas em contexto [de Oliveira et al., 2024]. A combinação dessas tecnologias possibilita a criação de ambientes ZTA interoperáveis, auditáveis e alinhados com requisitos de conformidade regulatória em múltiplos domínios.

A coleta, verificação e sincronização de informações contextuais, como comportamento de segurança do *endpoint*, geolocalização, horário e análise comportamental, é uma tarefa crítica e propensa a erros. A confiabilidade das fontes de contexto e a integridade dos dados coletados são determinantes para a eficácia das decisões de acesso [Gupta et al., 2024]. A presença de falsos positivos ou contextos desatualizados pode levar a decisões de bloqueio indevido, impactando a disponibilidade do sistema e a experiência do usuário.

Paralelamente, novos vetores de ataque como manipulação de IA, ataques à cadeia de suprimentos de *software*, exfiltração lateral em ambientes segmentados e exploração de vulnerabilidades em ferramentas de autenticação desafiam a resiliência das soluções

[14]Disponível em `https://www.openpolicyagent.org/`.
[15]Disponível em `https://www.w3.org/TR/did-core/`.
[16]Disponível em `https://trustbloc.readthedocs.io/`.
[17]Disponível em `https://trustoverip.org/`.

ZTA [Nahar et al., 2024]. O modelo *Zero Trust*, ao depender fortemente da identidade e da verificação contextual, torna-se sensível à qualidade e integridade dos sinais de confiança.

Diversas tendências futuras vêm sendo apontadas como complementares à consolidação da ZTA. Uma delas é a construção de arquiteturas *Zero Trust* autoadaptativas, baseadas em inteligência artificial embarcada, modelos de aprendizado contínuo e análise comportamental em tempo real. Tais sistemas serão capazes de ajustar políticas dinamicamente de acordo com padrões emergentes e variações do ambiente [He et al., 2022, Dhiman et al., 2024]. Modelos híbridos que combinam aprendizado supervisionado, não supervisionado e por reforço, aliados a computação de borda (*edge computing*), são promissores nesse cenário.

A integração de criptografia pós-quântica (*Post-Quantum Cryptography* - PQC) com identidade auto-soberana (*Self-Sovereign Identity* - SSI) representa outra fronteira. Sistemas baseados em *blockchain*, DID e contratos inteligentes permitirão registros auditáveis de decisões de acesso, confiança descentralizada e independência de autoridades centralizadas [Tuler De Oliveira et al., 2022, de Oliveira et al., 2024]. Essa abordagem oferece proteção de longo prazo e resistência a futuras quebras criptográficas, sendo particularmente relevante em ambientes regulados e de missão crítica.

A orquestração multidomínio e a computação federada também são tendências promissoras. Com a proliferação de computação em borda (*edge computing*) e redes 6G, a ZTA será exigida a operar em ambientes de baixa latência, alta mobilidade e autonomia local [Nahar et al., 2024]. Modelos federados de decisão, descentralização da verificação de identidade e sincronização segura de contexto são requisitos-chave para a efetividade da segurança nesse cenário.

No campo da observabilidade, destaca-se a segurança auditável e verificável. A instrumentação de sistemas ZTA com registros de atividades (*logs*) imutáveis, trilhas criptográficas e telemetria contínua permitirá não apenas detectar violações, mas também fornecer garantias formais de conformidade e accountability [Gupta et al., 2024, de Oliveira et al., 2024]. Isso reforça a transparência e viabiliza auditorias automatizadas, fundamentais para ambientes regulados.

O avanço de modelos como ZTA-as-a-Service também expressivo. Nesse novo modelo de serviço, componentes como motor de decisão, controle de acesso e contexto são oferecidos via APIs sob demanda. Essa tendência acelera a adoção de ZTA por organizações menores e possibilita a customização de políticas por perfil de risco e vertical de aplicação. Em paralelo, padrões técnicos estão em constante evolução, com contribuições do NIST, IETF, ETSI e IEEE propondo modelos referenciais, protocolos interoperáveis e linguagens declarativas de política.

2.9. Considerações Finais

O aumento da conectividade digital, impulsionado pela expansão de ambientes distribuídos e pela adoção de dispositivos heterogêneos, tem acentuado a fragilidade dos modelos tradicionais de segurança. Essa realidade, fundamenta a necessidade de repensar os mecanismos de proteção baseados em perímetro, cuja eficácia se torna limitada diante da fluidez das fronteiras organizacionais. A Arquitetura de Confiança Zero (*Zero Trust*

Tabela 2.9. Desafios e tendências emergentes na implementação de ZTA.

Desafio	Descrição	Tendência/Abordagem Promissora
Escalabilidade	Gestão de políticas e contexto em larga escala	Modelos federados e aprendizado distribuído
Performance	Verificação contínua introduz latência	Decisão local assistida por IA, caching adaptativo
Interoperabilidade	Incompatibilidade entre domínios e legados	Padrões abertos, autenticação federada, ABAC
Contexto	Confiabilidade e sincronização do ambiente	Telemetria contínua, validação cruzada, edge intelligence
Ameaças emergentes	Ataques à cadeia de suprimentos e exploração de IA	Certificação formal de componentes, observabilidade criptográfica

Architecture - ZTA) surge, nesse cenário, como uma abordagem orientada a minimizar a superfície de ataque por meio de validação contínua, microsegmentação e controle contextualizado de acesso. A proposta central do capítulo consistiu em apresentar os fundamentos teóricos, os componentes estruturais e as implicações práticas da ZTA, com foco especial na aplicação em redes de próxima geração, sistemas embarcados e ambientes corporativos descentralizados.

O capítulo percorreu os principais pilares da arquitetura, com ênfase nos modelos de autenticação adaptativa, nos mecanismos de autorização baseados em atributos e na importância da visibilidade contínua sobre o comportamento das entidades. A plataforma OpenZiti foi utilizada como referência de código aberto para demonstrar a viabilidade técnica da implementação de redes seguras baseadas em ZTA, evidenciando os ganhos em termos de resiliência, auditabilidade e governança distribuída. A análise foi complementada por uma taxonomia detalhada de aplicações, tecnologias e requisitos funcionais, permitindo sistematizar as diversas camadas envolvidas na adoção do modelo. A comparação entre a abordagem perimetral e a ZTA evidenciou a disrupção conceitual entre confiar implicitamente na infraestrutura e condicionar o acesso a fatores dinâmicos e verificáveis. Esses elementos sustentam a adoção crescente da ZTA como fundamento para arquiteturas resilientes em cenários como IoT, redes 5G/6G e ambientes BYOD.

Além dos benefícios imediatos, a ZTA também se projeta para cenários futuros marcados pela ascensão da computação quântica e pela obsolescência de algoritmos criptográficos tradicionais. A recente seleção de algoritmos resistentes à computação quântica pelo NIST reforça a necessidade de adaptação proativa das estratégias de segurança. A integração da ZTA com tecnologias emergentes, como criptografia pós-quântica e inteligência artificial aplicada à segurança adaptativa, aponta para um horizonte em que as organizações poderão responder automaticamente a ameaças complexas com alta precisão. Assim, perspectivas futuras para a evolução da ZTA envolvem desafios importantes, tais como escalabilidade técnica, maturidade organizacional e interoperabilidade interorganizacional. Para assegurar a viabilidade operacional desse modelo em larga escala, é necessária a adoção coordenada de ferramentas avançadas, como aprendizado federado, auditoria imutável em plataformas *blockchain* permissionadas e modelos descentralizados

de gestão de identidades auto-soberanas (SSI). O fortalecimento dessas práticas permitirá que a ZTA avance para além de um modelo conceitual, tornando-se um padrão normativo de segurança aplicável a ecossistemas digitais complexos.

A consolidação efetiva da ZTA depende de esforços colaborativos que envolvam diferentes setores da indústria, academia e governo. É mandatório o desenvolvimento de padrões técnicos unificados, políticas consistentes de segurança digital e novas soluções que promovam a delegação segura de confiança entre múltiplas partes. Dessa forma, a ZTA poderá estabelecer-se como um pilar fundamental na construção de infraestruturas digitais robustas, seguras e preparadas para enfrentar os desafios tecnológicos emergentes das próximas décadas.

Referências

[Abdalla et al., 2024] Abdalla, A. S., Moore, J., Adhikari, N. e Marojevic, V. (2024). Ztran: Prototyping zero trust security xapps for open radio access network deployments. *IEEE Wireless Communications*, 31(2):66–73.

[Aboukadri et al., 2024] Aboukadri, S., Ouaddah, A. e Mezrioui, A. (2024). Machine learning in identity and access management systems: Survey and deep dive. *Computers & Security*, p. 103729.

[AlDaajeh e Alrabaee, 2024] AlDaajeh, S. e Alrabaee, S. (2024). Strategic cybersecurity. *Computers & Security*, 141:103845.

[Alevizos et al., 2022] Alevizos, L., Ta, V. T. e Hashem Eiza, M. (2022). Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Security and privacy*, 5(1):e191.

[Alnoaimi e Alomary, 2025] Alnoaimi, S. e Alomary, A. (2025). Zero trust security: A comprehensive comparative analysis of zero trust maturity models. Em *2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*, p. 1–8.

[Alquwayzani e Albuali, 2024] Alquwayzani, A. A. e Albuali, A. A. (2024). A systematic literature review of zero trust architecture for military uav security systems. *IEEE Access*, 12:176033–176056.

[Anderson et al., 2022] Anderson, J., Huang, Q., Cheng, L. e Hu, H. (2022). Byoz: Protecting byod through zero trust network security. Em *2022 IEEE International Conference on Networking, Architecture and Storage (NAS)*, p. 1–8. IEEE.

[Andreoni et al., 2022] Andreoni, M., Barbosa, G. N. N. e Mattos, D. M. F. (2022). New barriers on 6G networking: An exploratory study on the security, privacy and opportunities for aerial networks. Em *2022 1st International Conference on 6G Networking (6GNet)*, p. 1–6.

[Barbosa et al., 2025] Barbosa, G. N. N., Andreoni, M. e Mattos, D. M. F. (2025). Leveraging zero trust for enhanced security and connectivity in ad-hoc mesh networks. Em *2025 12th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, p. 229–237.

[Bernabé Murcia et al., 2025] Bernabé Murcia, J. M., Cánovas, E., García-Rodríguez, J., M. Zarca, A. e Skarmeta, A. (2025). Decentralised identity management solution for zero-trust multi-domain computing continuum frameworks. *Future Generation Computer Systems*, 162:107479.

[Bertino, 2021] Bertino, E. (2021). Zero trust architecture: Does it help? *IEEE Security & Privacy*, 19(05):95–96.

[Cam-Winget e Lorenzin, 2017] Cam-Winget, N. e Lorenzin, L. (2017). Security Automation and Continuous Monitoring (SACM) Requirements. RFC 1654, RFC Editor.

[Chang e Mukherjee, 2024] Chang, H. e Mukherjee, S. (2024). Zeta: Transparent zero-trust security add-on for rdma. Em *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications*, p. 1041–1050.

[Chen et al., 2023] Chen, X., Feng, W., Ge, N. e Zhang, Y. (2023). Zero trust architecture for 6G security. *IEEE Network*, p. 1–1.

[Cunha Neto et al., 2024] Cunha Neto, H. N., Hribar, J., Dusparic, I., Fernandes, N. C. e Mattos, D. M. (2024). FedSBS: Federated-learning participant-selection method for intrusion detection systems. *Computer Networks*, 244:110351.

[de Oliveira et al., 2024] de Oliveira, N. R., dos Santos, Y. d. R., Barbosa, G. N. N., Reis, L. H. A., Mendes, A. C. R., de Oliveira, M. T., de Medeiros, D. S. V. e Mattos, D. M. F. (2024). Distributed data security in digital health: Self-sovereign identity, access control, and blockchain-based log records. Em *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, p. 558–565.

[de Oliveira et al., 2025] de Oliveira, N. R., Silva, J. V. V., de Medeiros, G. N. N. B. D. S. V. e Mattos, D. M. F. (2025). Incorporação de modelos de linguagem em larga escala em dispositivos móveis: Otimização, personalização e desafios. *Jornada de Atualização em Informática 2025; SBC; Maceio*, p. 147–196.

[Dhiman et al., 2024] Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U. e Hamid, Y. (2024). A review and comparative analysis of relevant approaches of zero trust network model. *Sensors*, 24(4).

[Gambo e Almulhem, 2025] Gambo, M. L. e Almulhem, A. (2025). Zero trust architecture: A systematic literature review.

[Gebresilassie et al., 2025] Gebresilassie, S. K., Rafferty, J., Abu-Tair, M., Ali, A., Chen, L. e Cui, Z. (2025). Shield: Secure holistic iot environment with ledger-based defense. *Internet of Things*, 30:101473.

[Gupta et al., 2024] Gupta, A., Gupta, P., Pandey, U. P., Kushwaha, P., Lohani, B. P. e Bhati, K. (2024). ZTSA: Zero trust security architecture a comprehensive survey. Em *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, p. 378–383.

[He et al., 2022] He, Y., Huang, D., Chen, L., Ni, Y. e Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, 2022(1):6476274.

[Hosney et al., 2022] Hosney, E. S., Halim, I. T. A. e Yousef, A. H. (2022). An artificial intelligence approach for deploying zero trust architecture (ZTA). Em *2022 5th International Conference on Computing and Informatics (ICCI)*, p. 343–350.

[Hussain et al., 2024] Hussain, M., Pal, S., Jadidi, Z., Foo, E. e Kanhere, S. (2024). Federated zero trust architecture using artificial intelligence. *IEEE Wireless Communications*, 31(2):30–35.

[Jose Diaz Rivera et al., 2024] Jose Diaz Rivera, J., Muhammad, A. e Song, W.-C. (2024). Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication. *IEEE Open Journal of the Communications Society*, 5:2792–2814.

[Kang et al., 2023] Kang, H., Liu, G., Wang, Q., Meng, L. e Liu, J. (2023). Theory and application of zero trust security: A brief survey. *Entropy*, 25(12).

[Kindervag et al., 2010] Kindervag, J., Balaouras, S. et al. (2010). No more chewy centers: Introducing the zero trust model of information security. *Forrester Research*, 3(1):1–16.

[Koukis et al., 2024] Koukis, G., Skaperas, S., Kapetanidou, I. A., Mamatas, L. e Tsaoussidis, V. (2024). Evaluating cni plugins features and tradeoffs for edge cloud applications. Em *2024 IEEE Symposium on Computers and Communications (ISCC)*, p. 1–6.

[Kumar et al., 2024] Kumar, S. S., Cummings, M. e Stimpson, A. (2024). Strengthening llm trust boundaries: a survey of prompt injection attacks. Em *2024 IEEE 4th International Conference on Human-Machine Systems (ICHMS)*, p. 1–6.

[Mämmelä et al., 2016] Mämmelä, O., Hiltunen, J., Suomalainen, J., Ahola, K., Mannersalo, P. e Vehkaperä, J. (2016). Towards micro-segmentation in 5G network security. Em *European Conference on Networks and Communications (EuCNC 2016) Workshop on Network Management, Quality of Service and Security for 5G Networks*.

[Mujib e Sari, 2020] Mujib, M. e Sari, R. F. (2020). Performance evaluation of data center network with network micro-segmentation. Em *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, p. 27–32. IEEE.

[Mukta et al., 2025] Mukta, R., Pal, S., Chowdhury, K., Hitchens, M., young Paik, H. e Kanhere, S. S. (2025). Zero trust driven access control delegation using blockchain. *Blockchain: Research and Applications*, p. 100319.

[Nace, 2020] Nace, L. (2020). Securing trajectory based operations through a zero trust framework in the nas. Em *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*, p. 1B1–1–1B1–8.

[Nagendra e Hemavathy, 2023] Nagendra, T. e Hemavathy, R. (2023). Unlocking kubernetes networking efficiency: Exploring data processing units for offloading and enhancing container network interfaces. Em *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)*, p. 1–7.

[Nahar et al., 2024] Nahar, N., Andersson, K., Schelén, O. e Saguna, S. (2024). A survey on zero trust architecture: Applications and challenges of 6G networks. *IEEE Access*, 12:94753–94764.

[Oliveira et al., 2024] Oliveira, N. R. d., Santos, Y. d. R. d., Mendes, A. C. R., Barbosa, G. N. N., Oliveira, M. T. d., Valle, R., Medeiros, D. S. V. e Mattos, D. M. F. (2024). Storage standards and solutions, data storage, sharing, and structuring in digital health: A brazilian case study. *Information*, 15(1).

[Pooja e Chandrakala, 2024] Pooja, S. e Chandrakala, C. B. (2024). Secure reviewing and data sharing in scientific collaboration: Leveraging blockchain and zero trust architecture. *IEEE Access*, 12:92386–92399.

[Ramezanpour e Jagannath, 2022] Ramezanpour, K. e Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of o-ran. *Computer Networks*, 217:109358.

[Rizvi et al., 2023] Rizvi, S., Zwerling, T., Thompson, B., Faiola, S., Campbell, S., Fisanick, S. e Hutnick, C. (2023). A modular framework for auditing iot devices and networks. *Computers & Security*, 132:103327.

[Satybaldy et al., 2024] Satybaldy, A., Ferdous, M. S. e Nowostawski, M. (2024). A taxonomy of challenges for self-sovereign identity systems. *IEEE Access*, 12:16151–16177.

[Sheikh et al., 2021] Sheikh, N., Pawar, M. e Lawrence, V. (2021). Zero trust using network micro segmentation. Em *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, p. 1–6.

[Shen e Shen, 2024] Shen, Q. e Shen, Y. (2024). Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach. *Computers & Security*, 136:103537.

[Srinivas et al., 2019] Srinivas, J., Das, A. K. e Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92:178–188.

[Stafford, 2020] Stafford, V. (2020). Zero trust architecture. *NIST special publication*, 800:207.

[Syed et al., 2022] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z. e Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE Access*, 10:57143–57179.

[Tankard, 2011] Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security*, 2011(8):16–19.

[Teerakanok et al., 2021] Teerakanok, S., Uehara, T. e Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. *Security and Communication Networks*, 2021(1):9947347.

[Tsai et al., 2024] Tsai, M., Lee, S. e Shieh, S. W. (2024). Strategy for implementing of zero trust architecture. *IEEE Transactions on Reliability*, 73(1):93–100.

[Tuler De Oliveira et al., 2022] Tuler De Oliveira, M., Reis, L. H. A., Verginadis, Y., Mattos, D. M. F. e Olabarriaga, S. D. (2022). Smartaccess: Attribute-based access control system for medical records based on smart contracts. *IEEE Access*, 10:117836–117854.

[van Steen, 2025] van Steen, T. (2025). Developing a behavioural cybersecurity strategy: A five-step approach for organisations. *Computer Standards & Interfaces*, 92:103939.

[Yiliyaer e Kim, 2022] Yiliyaer, S. e Kim, Y. (2022). Secure access service edge: A zero trust based framework for accessing data securely. Em *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, p. 0586–0591.

[Zivi e Doerr, 2022] Zivi, A. e Doerr, C. (2022). Adding zero trust in BYOD environments through network inspection. Em *2022 IEEE Conference on Communications and Network Security (CNS)*, p. 1–6.