Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Moises Matias e Silva

SISTEMAS MULTINÍVEIS DE SEGURANÇA E REDES ZERO TRUST: IMPLEMENTANDO PROCESSOS, SISTEMAS E INFRAESTRUTURAS SEGURAS E POSSÍVEIS.

Americana, SP
2022

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Moises Matias e Silva

SISTEMAS MULTINÍVEIS DE SEGURANÇA E REDES ZERO TRUST: IMPLEMENTANDO PROCESSOS, SISTEMAS E INFRAESTRUTURAS SEGURAS E POSSÍVEIS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof.
Área de concentração: Segurança relacionada aos cartões de crédito.

Americana, SP.

2022

Moises Matias e Silva

SISTEMAS MULTINÍVEIS DE SEGURANÇA E REDES ZERO TRUST: IMPLEMENTANDO PROCESSOS, SISTEMAS E INFRAESTRUTURAS SEGURAS E POSSÍVEIS.

Trabalho de graduação apresentado como exigência parcial para obtenção do título de tecnólogo em curso superior de Tecnologia em segurança da Informação pelo centro Paula Souza – Fatec Faculdade de tecnologia de American- Ralph Biasi

Americana, 02 de Dezembro de 2022

Banca examinadora:

Profº Drº Henry Alves de Godoy (Presidente)

Doutorado

Fatec Americana

Profº Drº Rodrigo Rosalis da Silva (Membro)

Doutorado

Fatec Americana

Profº Esp. Evandro Santaclara

Especialista

Fatec Americana

AGRADECIMENTOS:

Seria difícil e talvez injusto, nomear todos um a um aqui, de modo a correr o risco de ser injusto e não citar devidamente todos aqueles que me incentivaram nesta jornada. Agradeço aos meus professores da Fatec Americana, em especial professores Rogério, Mariana, Elton, Maxwell Vitorino, Henri Alves Godoy, Juliana Beckendorf, onde através deles, pude entender a base de todos os processos do tema de segurança da informação, minha família pelo apoio e motivação para continuar neste processo de aprendizado. Aos amigos e colegas de trabalho que me ajudaram a refletir sobre decisões e escolhas ao longo deste ciclo de aprendizagem; Amigos esses como Ana Beatriz Juliani e Andrei Bonon, que me acompanharam em toda essa jornada, torcendo por mim, Joana Eduardo, uma amiga que ainda carrego com carinho e sempre senti o apoio dela, mesmo que a distância, aos meus amigos Diego Quadrado, Eduardo Christofoletti e Tarcísio Cardoso, que em momentos cruciais me ensinaram a crescer e me tornaram tanto uma pessoa mais forte um profissional mais competente. Muitos amigos que me apoiaram até aqui também merecem ser citados, entre eles Rafael, Bárbara, Matheus Antonio, Loghann, Pedro, Marcelo, Rafael, Paulo, Karla, Sidney, Mario, Ivan, Gabriel, Henrique, Arthur, Arthur e Felipe; Meus antigos e atuais chefes, pelas oportunidades e aprendizado que muito acrescentaram em minha vida e por fim, agradeço a Deus por me dar saúde e a força para chegar até a conclusão do curso tecnólogo de Segurança da Informação.

DEDICATÓRIA

Dedico este trabalho a todos os que me ajudaram ao longo desta jornada acadêmica. Ao meu pai, Elias Matias e Silva, pelo estímulo à tecnologia e aprendizado desde a minha mais tenra idade. A minha mãe, Vastí Rodrigues e Silva; linguista, que desde minha mais tenra idade também me cobriu de amor, carinho e ensinou o amor e prazer pelo aprender e a curiosidade. Aos meus avôs Moisés Teixeira e Silva e Vicente dos Santos Rodrigues, por me ensinarem desde cedo as responsabilidades e carinho para com a família, Minhas avós Jurema Teixeira e Silva e Miriam dos Santos Rodrigues, as quais me criaram com um amor gigante. Minhas tias Betânia, Dalete e Elisa, Meus tios Natanael, Washington, Ubiratan, Ely, Dario, Davi e Levi. Minhas irmãs Suzanne Rodrigues e Rebecca Benatti. Meus primos, Juliana, Jasón, Ezequiel, Josué, Josafá, Sarah, Azenate, Jonatas, Elias, Aline, Abigail, Davi, Davi Jetter, Dario Filho, Natalia e muitos outros primos; Meu orientador Henry Alves Godoy, que não só me ensinaram como em muito somaram em minha vida. A Minha Sobrinha Vivian, um tesouro na minha vida. Em especial também dedico este trabalho a todas as vítimas da pandemia de COVID-19, e aos profissionais de saúde infraestrutura, comunicação, segurança, saneamento e zeladoria, que mesmo sem muitas vezes podemos ver suas atuações, foram cruciais para que nosso mundo continuasse em pleno funcionamento, bem como suas estruturas. A todos eles, dedico o resultado de todo o esforço realizado ao longo deste percurso, e meu sincero agradecimento.

Em memória de Otácilio e Ubirajara. Hoje, vocês moram em meu coração.

RESUMO

A cada ano aumentam os gastos com segurança e as crescentes proporções de ataques e invasões a sistemas cibernéticos continuam aumentando junto aos orçamentos em busca de soluções.

As estratégias tradicionais de defesa baseadas em perímetro estão desatualizadas e propensas a falha, principalmente porque a maioria dos incidentes de segurança vem de pessoas de dentro da organização. Estes mesmos modelos, não abrangem também soluções nos campos relacionados a níveis de acessos devidamente definidos. O que resulta muitas vezes em exploração de ataques como a movimentação lateral.

As ameaças internas também possuem uma grande parcela destes incidentes. Incidentes, justamente relacionados a níveis de acesso indevidamente configurados e o mal gerenciamento de políticas de acesso.

Em uma época em que a vigilância em rede é onipresente, existe a dificuldade em saber em quem confiar. Podemos confiar que o tráfego de Internet próprio estará protegido contra intrusão e exploração para o roubo de dados? Não podemos fazer esta afirmativa com certezas absolutas. Mesmo provedores de serviços ou equipes locais e terceirizadas devem ser devidamente checadas e analisadas.

A suposição de que os sistemas e o tráfego em um datacenter podem ser totalmente confiáveis é falha. As redes modernas e os padrões de uso não são mais semelhantes aos que faziam sentido na defesa do perímetro há muitos anos. Como resultado, a movimentação livre em uma infraestrutura “segura” é frequentemente trivial, uma vez que um único host ou link foi comprometido, especialmente através de ataques laterais.

Neste sentido, as organizações estão hoje repensando sua mentalidade em relação à segurança da informação, mantendo uma mentalidade de segurança de dentro para fora, como sugere a arquitetura Zero Trust.

Atingir a confiança zero é muitas vezes percebido como caro e complexo. No entanto, o Zero Trust se baseia em sua arquitetura existente e não exige que necessariamente seja substituída a tecnologia e ativos tecnológicos que já fazem parte da sua infraestrutura.

Este TCC, tem o objetivo de apresentar sistemas de infraestruturas e arquiteturas de sistemas, baseados em modelos de segurança multinível em conjunto

com a arquitetura zero trust, mostrando também as possibilidades de sua implementação em diversos cenários, bem como suas vantagens e desvantagens. Através desta, também se busca a discussão sobre sua implementação em diversos cenários possíveis e mais próximos do mundo real, de modo a apresentar uma solução e aplicação prática e objetiva.

Palavras-Chave: Zero Trust; Arquitetura; Segurança, Redes.

ABSTRACT

Each year, security spending increases, and the growing proportions of attacks and intrusions into cybernetic systems continue to increase along with budgets in search of solutions.

Traditional perimeter-based defense strategies are outdated and prone to failure, especially since most security incidents come from insiders. These same models also do not cover solutions in fields related to duly defined access levels. Which often results in the exploitation of attacks such as lateral movement.

Insider threats also have a large share of these incidents. Incidents are precisely related to improperly configured access levels and poor management of access policies.

In an age where network surveillance is ubiquitous, there is challenging to know whom to trust. Can we trust that our Internet traffic will be protected from intrusion and exploitation for data theft? We cannot make this statement with absolute certainty. Even local and outsourced service providers or teams must be appropriately checked and analyzed.

The assumption that systems and traffic in a data center can be trusted entirely is flawed. Modern networks and usage patterns are different from what made sense in perimeter defense many years ago. As a result, roaming freely over a “secure” infrastructure is often trivial once a single host or link has been compromised, primarily through lateral attacks.

In this sense, organizations are now rethinking their mentality about information security, maintaining a security mentality from the inside out, as suggested by the Zero Trust architecture.

Achieving zero trust is often perceived as expensive and complex. However, Zero Trust builds on your existing architecture and does not necessarily require you to replace technology and technology assets that are already part of your infrastructure.

This TCC aims to present infrastructure systems and system architectures based on multilevel security models in conjunction with zero trust architecture, showing the possibilities of its implementation in different scenarios and its advantages and disadvantages. Through this, we also seek to discuss its implementation in different possible scenarios closer to the real world to present a practical and objective solution and application.

Keywords: Zero Trust; Architecture; Security, Networks.

LISTA DE ILUSTRAÇÕES:

SUMÁRIO:

1. INTRODUÇÃO:

A pandemia do Novo Coronavírus (COVID-19) mudou a rotina de muitas pessoas e organizações, os hábitos que antes da pandemia eram comuns pouco a pouco dão espaço para novos hábitos e o ritmo mudança causada pelo impacto dos eventos é inevitável. Em especial no caso das organizações, onde as mesmas se viram desafiadas diante de um novo paradigma temporal, as posições antes tomadas como inflexíveis, agora se viram diante da necessidade de mudar ou desistir. Diversas organizações, diante deste novo cenário não estavam preparadas e terminaram por encerrar suas atividades diante de uma mudança repentina onde o isolamento social, por muitos meses se tornou regra para a contenção da pandemia. Foram incontáveis o número de organizações que encerraram suas atividades, e os impactos econômicos causados pela pandemia do COVID-19 foram tão graves que os governos decidiram por se envolver diretamente em iniciativas para auxiliar e renovar a infraestrutura geral do país. Desde iniciativas como a CISA Americana (Cybersecurity and Infrastructure Security Agency) - Fundada em 2020, a iniciativas maiores em diversos países mundo afora.

Sabe-se também, que apesar das arquiteturas de segurança já estarem presentes desde ao menos 30 anos antes, bem como os riscos apresentados as organizações, a adoção de soluções de segurança de forma robusta e bem estruturada, ocorria a passos lentos. Causados mutas vezes pela inflexibilidade das organizações, falta de compreensão da importância da TI e a área de segurança, e o não investimento devido no setor de TI, ao não entender este como parte estratégica da organização.

Com essa mudança de paradigma social repentina, as possibilidades e realizações de ataques de cibersegurança também aumentaram vertiginosamente. Segundo a organização NETSCOUT de acordo com o relatório Threat Intelligence Report, apresentado em setembro de 2021 o número de ciberataques no Brasil aumentou 16,17% no primeiro semestre do ano citado — quando comparado ao mesmo período de 2020 [14].

O mesmo relatório da NETSCOUT, mostra que foram cerca de 5,4 milhões de ataques. O número representa um aumento de 11% em relação ao mesmo período

do ano anterior, com ritmo suficiente para superar o recorde de 2020. Ao compararmos o mesmo período [14].

Segundo Geraldo Guazzelli, diretor da NETSCOUT Brasil: "*Ataques e invasões relacionados à segurança cibernética seguem crescendo, colocando cada vez mais as empresas na defensiva e na busca de soluções e processos que as protejam efetivamente antes da ocorrência de um evento. Visibilidade total das redes e do tráfego IP tornaram-se fundamental nesta guerra diária*" [14].

Muitas organizações, ao tentar entender a segurança da informação de forma prática, focam em soluções a nível de usuário e ferramentas de monitoramento, esquecendo assim, da segurança a nível mais crítico, que é a implementação de arquiteturas e sistemas seguros nas mais diversas camadas da organização. Assim, por mais fortes e de alta tecnologia que as soluções implementadas possam ser e se apresentar, diante de uma infraestrutura e modelos que em seu cerne são inseguros, todas apresentarão brechas possíveis e eventualmente graves, que poderão e serão exploradas por um adversário.

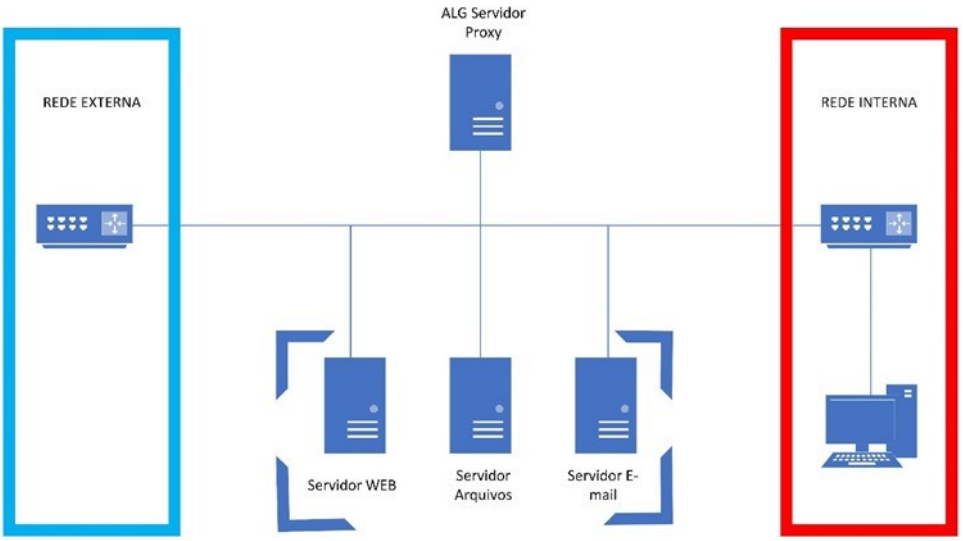
Do mesmo modo que não existem sistemas, processos e implementações de sistemas perfeitos e sem perdas; na segurança da informação, se entende que não existe a segurança completamente perfeita e a prova de falhas. Toda infraestrutura, processos e arquiteturas, bem como os sistemas que os acompanham, precisam ser constantemente revisados diante do tempo e época que se encontram. Deste modo, busca-se minimizar ao máximo possível as falhas e brechas que apresentem riscos a organização.

Este trabalho busca apresentar a conceitualização e implementação de sistemas com múltiplas camadas e níveis de segurança, em conjunto com a arquitetura zero trust (Tradução livre: Confiança zero ou mínima), que pode vir a ser uma alternativa viável e possível para uma organização em um modelo de evolução constante e atemporal. A implementação de sistemas, processos e infraestruturas com base nestes conceitos, pode apresentar uma solução viável e interessante em cenários diversos e reais de pequenas a grandes organizações (Os quais serão abordados também nos tópicos aqui descritos).

2. *DEFININDO OS PRINCÍPIOS DE ZERO TRUST:*

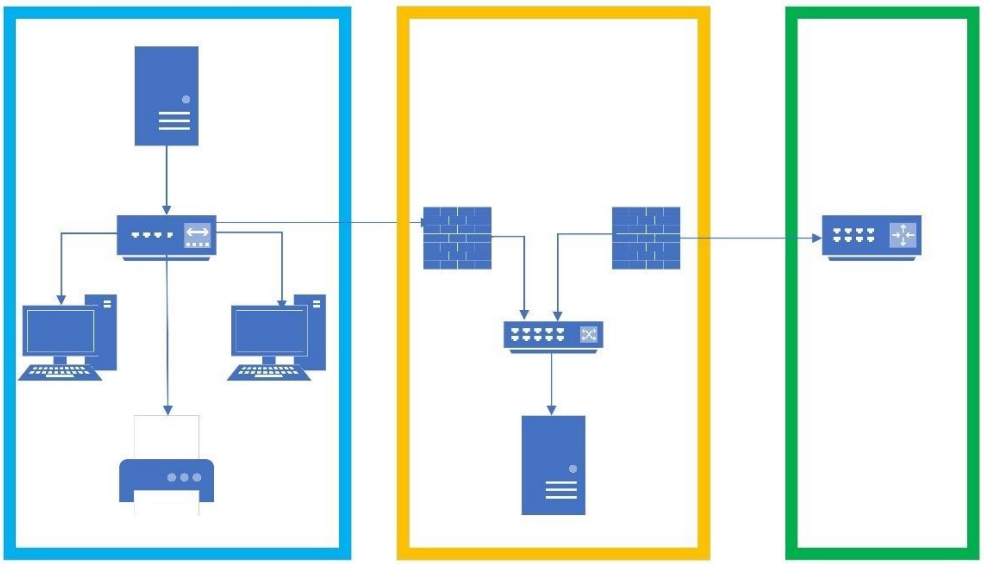
Originalmente, a arquitetura de segurança de rede tradicional, particiona a rede em outras diferentes, e cada rede em zonas delimitadas. Cada zona é contida por um ou mais firewalls que formam uma defesa de perímetro [8]. Dentro de cada zona, é concedido um nível de confiança e é permitido o acesso a recursos específicos. Este modelo oferece uma defesa em profundidade muito forte. Por exemplo, recursos considerados mais arriscados, como servidores da web que enfrentam a Internet pública, são colocados em uma zona de exclusão (muitas vezes chamada de “DMZ”), onde o tráfego pode ser rigidamente monitorado e controlado, como podemos observar a partir da figura 01, um modelo simples dessa segurança baseada em perímetro, e na figura 02, contendo uma arquitetura abrangente descrevendo outros ativos na rede.

Figura 01- Modelo simples de segurança Baseada em perímetro.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

Figura 02 – Modelo de arquitetura abrangente, baseada em perímetro.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

Entretanto, apesar de o modelo oferecer uma segurança forte, um problema inerente, está justamente em considerar a segurança do ponto de vista externo (De fora para dentro), não considerando ameaças internas, ou mesmo ativos (endpoints) comprometidos através de exploits “zero-day”, Ip-spoofing, adulteração de endereços MAC, entre outros modos de exploração, conforme podemos observar em exemplo na figura 03

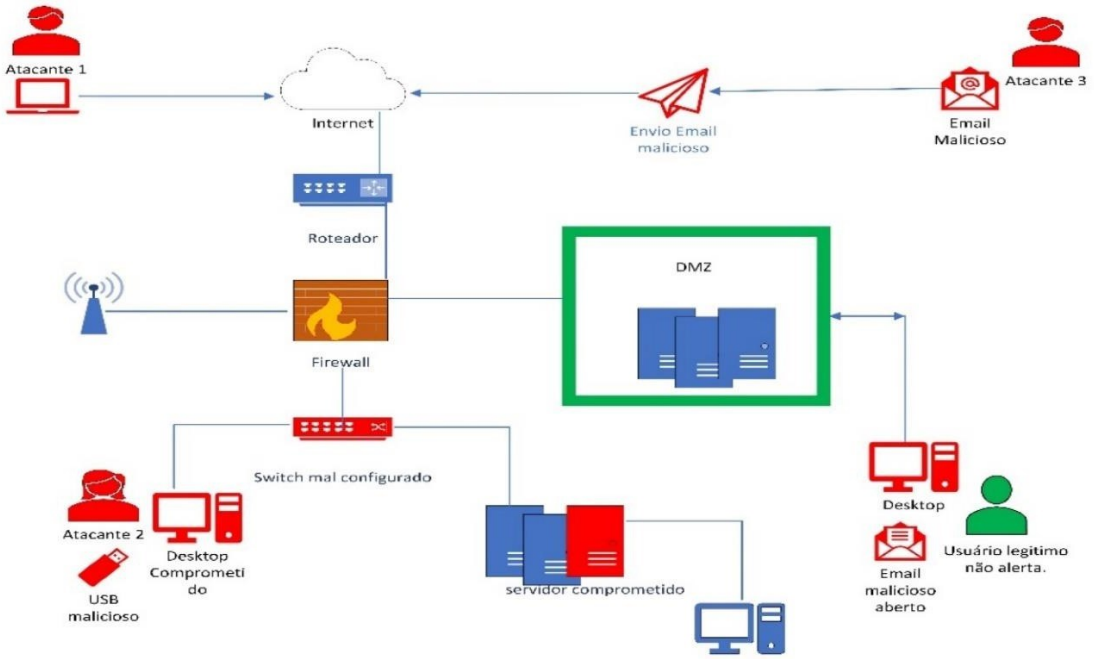


Figura 03: Cenário de possíveis ataques a uma rede com perímetro.

Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

A arquitetura de modelo zero trust, visa resolver os problemas inerentes em colocar a confiança em uma rede específica. Em vez disso, é possível proteger a comunicação e o acesso à rede de forma tão eficaz que a segurança física da camada de transporte pode ser razoavelmente desconsiderada. Claro que objetivos neste escopo são algo de uma confiança e consideração na infraestrutura como um todo, altamente elevados. Porém, com a criptografia atual, e sistemas de automação devidamente aplicados e configurados, essa visão é realmente alcançável.

Assim, em conjunto com um perímetro definido por software (Software Defined Network – SDN) e outra soluções integradas, é fornecido o acesso seguro e evita-se a perda de dados, independentemente de onde os usuários estejam, quais dispositivos estão sendo usados ou onde suas cargas de trabalho e dados estejam localizadas (ou seja, datacenters, nuvens públicas ou aplicativos SaaS).

Através dessa arquitetura de segurança, os acessos antes precisam ser devidamente autorizados, pois, é a organização que estabelecerá o acesso requisitado de acordo com as necessidades - e apenas o que precisam - para a sua função de trabalho.

O Zero Trust é um modelo de segurança de rede, baseado em um rigoroso processo de verificação de identidade. A estrutura estabelece que somente usuários e dispositivos autenticados e autorizados podem acessar aplicações e dados. O princípio maior da segurança baseada em Zero Trust, é que as vulnerabilidades geralmente aparecem quando as organizações confiam demais em indivíduos ou dispositivos. O modelo de Zero Trust sugere que nenhum usuário, mesmo se permitido na rede, deve ser confiável por padrão, porque eles podem ser comprometidos. A identidade e a autenticação do dispositivo são necessárias em toda a rede, e não apenas no perímetro e zonas de segurança estabelecidas como seguras. Ao limitar quais partes têm acesso privilegiado a cada segmento de uma rede, ou a cada máquina em uma organização segura, o número de oportunidades para um hacker obter acesso a conteúdo seguro é bastante reduzido e riscosmitigados.

O termo Zero Trust, foi criado originalmente por John Kindervag, analista da Forrester Research [23][26]. O termo foi mencionado pela primeira vez pelo seu autor em 2010, data de sua introdução [10]. Uma das descrições mais populares é dada em um relatório recente do Gartner que descreve o conceito de acesso à rede de confiança zero (ZTNA):

> *O novo modelo apresenta uma abordagem na qual um agente de confiança medeia conexões entre aplicativos e usuários. A ZTNA abstrai e centraliza os mecanismos de segurança para que os engenheiros e funcionários de segurança possam ser responsáveis por eles. O ZTNA começa com uma postura de negação padrão de confiança zero. Ele concede acesso com base na identidade, além de outros atributos e contexto (como hora / data, geolocalização e postura do dispositivo) e oferece adaptativamente a confiança apropriada necessária no momento. O resultado é um ambiente mais resiliente, com maior flexibilidade e melhor monitorização* [12].

A arquitetura, é baseada na premissa de que “nunca se deve confiar, sempre verificar”, inclusive em usuários internos a rede, pois o acesso de um ativo organizacional pode ser comprometido a requisição de acesso pode não ser legitima.

A ideia desta arquitetura é que seja projetada para proteger ambientes digitais modernos onde os acessos legítimos a aplicativos e cargas de trabalhos críticos podem vir de quaisquer lugares externos a organização. Sejam casas, cafeterias, escritórios entre outros.

A arquitetura Zero Trust exige uma visibilidade, imposição e controle consistentes que podem ser entregues diretamente no dispositivo ou através da nuvem, de acordo com a infraestrutura da organização a considerar.

Embora as redes de confiança zero estejam ganhando interesse nos setores governamentais, militares, industriais e econômicos; atualmente não há padrões definidos de como realizar sua arquitetura. Apesar disso, existem características e princípios que norteiam sua existência.

Uma rede de confiança zero é construída em cima de cinco pilares principais:

1. *A rede é sempre considerada hostil, seja ela interna ou externa.*
2. *As ameaças externas e internas existem na rede o tempo todo.*
3. *A localidade da rede não é suficiente para decidir a confiança em uma rede.*
4. *Cada dispositivo, usuário e fluxo de rede são autenticados e autorizados.*
5. *As políticas devem ser dinâmicas e calculadas a partir do maior número possível de fontes de dados disponíveis no momento da execução.* [8]

De acordo a publicação de referência NIST SP 800-207 (2020), existem componentes essenciais, que integram uma arquitetura Zero Trust. Abaixo, podemos ver alguns componentes que integram a estrutura lógica de uma arquitetura Zero Trust:

- **Mecanismo de política (PE):** Este componente é responsável pela decisãofinal de conceder acesso a um recurso para um determinado recurso. O PEusa a política da organização, bem como a entrada de fontes externas (por exemplo, sistemas CDM, serviços de inteligência de ameaças, descritos abaixo), como entrada para um algoritmo de confiança conceder, negar ou revogar acesso ao recurso. O PE é emparelhado com o componente do administrador de políticas. O mecanismo de política toma e registra a decisão (como aprovada ou negada), e o administrador de políticas executa a decisão.
- **Administrador de políticas (PA):** Este componente é responsável por estabelecer e/ou desligar o caminho de comunicação entre um assunto e um recurso (através de comandos aos PEPs relevantes). Isso geraria

qualquer autenticação específica de sessão e token de autenticação ou credencial usado por um cliente para acessar um recurso corporativo. Isso é intimamente ligado ao PE e depende de sua decisão de permitir ou negar uma sessão. Se a sessão é autorizada e o pedido autenticado, o PA configura o PEP para permitir que a sessão comece. Se a sessão for negada (ou uma aprovação prévia for revogado), o PA sinaliza para o PEP para desligar a conexão. Algumas implementações podem tratar o PE e o PA como um único serviço; aqui, ele é dividido em dois componentes lógicos. O PA se comunica com o PEP ao criar o caminho de comunicação. Esta comunicação é feita através do plano de controle.

- **Ponto de aplicação da política (PEP):** Este sistema é responsável por habilitar, monitorar, e eventualmente terminando as conexões entre um assunto e um recurso da organização. O PEP se comunica com o PA paraencaminhar solicitações e/ou receber atualizações de política de o PA. Esteé um único componente lógico no ZTA, mas pode ser dividido em dois diferentes componentes: o cliente (por exemplo, agente em um laptop) e o lado do recurso (por exemplo, gateway componente na frente do recurso que controla o acesso) ou um único componente do portal que atua como um gatekeeper para caminhos de comunicação. Além do PEP está a zona de confiança que hospeda o recurso da organização. Além dos componentes principais em uma organização implementando uma ZTA, várias fontes de dados fornecem entrada e regras de política usadas pelo mecanismo de política ao tomar decisões de acesso. Esses incluem fontesde dados locais, bem como fontes de dados externos (ou seja, não controlados pela organização ou criados por ela). Estes podem incluir:
- **Sistema de diagnóstico e mitigação contínuos (CDM):** Reúne informações sobre o estado atual do ativo da organização e aplica atualizações para configuração e software componentes. Um sistema CDMpode trabalhar em conjunto com um banco de dados de gerenciamento de configuração (CMDB) e fornecer ao mecanismo de política as informações sobre o recurso fazendo uma solicitação de acesso, como se ele está executando o sistema operacional (SO) apropriado e com as devidas correções, a integridade dos componentes de software aprovados pela organização ou presença de componentes não aprovados e se o ativo tem

quaisquer vulnerabilidades. Os sistemas CDM também são responsáveis por identificar e impor um subconjunto de políticas em dispositivos não pertencentes a organização, ativos na infraestrutura organização.

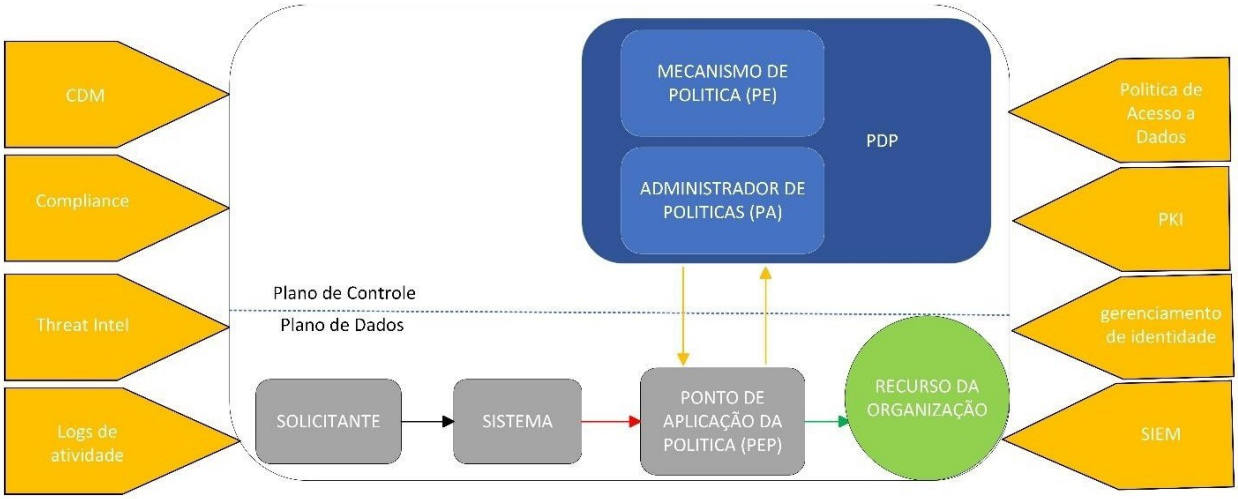
- **Sistema de conformidade da indústria:** Isso garante que a organização permaneça em conformidade com qualquer regime regulatório ao qual possa se enquadrar (por exemplo, FISMA, assistência médica ou financeira requisitos de segurança da informação da indústria). Isso inclui todas as regras de política que uma organização desenvolve para garantir a conformidade.
- **Feed(s) de inteligência de ameaças:** Fornece informações de fontesinternas ou externas que ajudam o mecanismo de política a tomar decisões de acesso. Estes podem ser vários serviços que obter dados de fontes internas e/ou externas múltiplas e fornecer informações sobre ataques ou vulnerabilidades recém-descobertas. Isso também inclui falhas recém-descobertas em software, malware recém-identificado e ataques relatados a outros ativos que a política mecanismo vai querer negar o acesso a partir de ativos da organização.
- **Logs de atividades de rede e sistema:** Este sistema agrega logs de ativos, tráfego de rede, ações de acesso a recursos e outros eventos que fornecem feedback em tempo real (ou quase em tempo real) sobre a postura de segurança dos sistemas de informações das organizações.
- **Políticas de acesso a dados:** são os atributos, regras e políticas sobre acesso a recursos da organização. Este conjunto de regras pode sercodificado (via interface de gerenciamento) ou gerada dinamicamente pelomecanismo de políticas. Essas políticas são o ponto de partida para autorizar o acesso a um recurso, pois fornecem os privilégios básicos de acesso para contas e aplicativos/serviços na organização. Essas políticas devem ser baseadas nos papéis da missão e necessidades da organização.
- **Infraestrutura de chave pública organizacional (PKI):** Este sistema é responsável por gerar e certificados de registro emitidos pela organização para recursos, assuntos, serviços e formulários. Isso também pode se a aplicar a uma PKI que não é construída sobre certificados X.509.
- **Sistema de gerenciamento de Identidade (ID):** É responsável por criar, armazenar e gerenciar contas de usuários corporativos e registros de

identidade (por exemplo, LDAP). Este sistema contém as informações necessárias do assunto (por exemplo, nome, endereço de e-mail, certificados) e outras características da organização, como função, acesso atributos e ativos atribuídos. Este sistema geralmente utiliza outros sistemas (como uma PKI) para artefatos associados a contas de usuário. Estesistema pode fazer parte de um sistema federado maior comunidade e podeincluir funcionários não corporativos ou links para ativos não corporativos para colaboração.

- **Sistema de gerenciamento de eventos e informações de segurança (SIEM):** Coleta informações centradas na segurança para análise posterior.Esses dados são usados para refinar as políticas e alertar sobre possíveis ataques contra os ativos da organização. [13]

A Figura 04 demonstra a arquitetura dos componentes lógicos de acordo com o visualizado pela NIST em sua publicação especial citada.

Figura 04: Componentes lógicos de uma arquitetura zero trust.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

Ainda segundo a orientação da NIST SP 800-207 (2020), existem requisitos de rede para que o apoio a arquitetura Zero Trust seja devido:

1. Os ativos da organização devem ter conectividade de rede básica. A rede local (LAN), controlada pela organização ou não, deve fornecer o roteamento

básico e infraestrutura (por exemplo, DNS). O ativo remoto da organização, pode utilizar ou não, todos os serviços de infraestrutura.

2. A organização deve ser capaz de distinguir entre quais ativos são de propriedade ou gerenciados pela organização e a postura de segurança atual dos dispositivos. Isso é determinado por credenciais emitidas pela organização e negando o uso de informações que não podem ser autenticadas (por exemplo, endereços MAC de rede, que podem ser falsificados).

3. A organização deve observar todo o tráfego de rede. A organização deve registrar os pacotes vistos no plano de dados, mesmo que não seja capaz de realizar a inspeção da camada de aplicação (camada 7 OSI) em todos os pacotes. A organização deverá filtrar os metadados sobre a conexão (por exemplo, destino, hora, identidade do dispositivo) para atualizar dinamicamente as políticas e informar a PE à medida que avalia as solicitações de acesso.

4. Os recursos da organização não devem ser acessíveis sem antes acessar um PEP. Os recursos da organização devem negar conexões de entrada arbitrárias da Internet. Os recursos podem aceitar conexões de configuração personalizada somente após um cliente ter sido autenticado e autorizado. Esses caminhos de comunicação são configurados pelo PEP. Os recursos podem nem mesmo ser descobertos sem acessar um PEP. Isso evita que invasores identifiquem alvos por meio de varredura de rede ou lançamento de ataques de negação de serviço (DoS), contra os recursos da organização, localizados atrás de PEPs. É importante observar que nem todos os recursos devem ser ocultados dessa maneira; alguns componentes da infraestrutura de rede (por exemplo, servidores DNS) devem estar acessíveis.

5. O plano de dados e o plano de controle são logicamente separados. O mecanismo de política, o administrador de política e os PEPs se comunicam em uma rede que é logicamente separada e não pode ser acessada diretamente pelos ativos e recursos da organização. O plano de dados é usado para tráfego de dados de aplicativos/serviços. O mecanismo de política, o administrador de política e os PEPs usam o plano de controle para se comunicar e gerenciar os caminhos de comunicação entre os ativos. Os PEPs devem ser capazes de enviar e receber mensagens dos planos de dados e de controle.

6. Os ativos da organização podem atingir o componente PEP. Os ativos corporativos devem ser capazes de acessar o componente PEP para obter acesso

aos recursos. Isso pode assumir a forma de um portal da Web, dispositivo de rede ou agente de software no ativo corporativo que permite a conexão.

7. O PEP é o único componente que acessa o administrador de política como parte de um fluxo de negócios. Cada PEP operando na rede organizacional tem uma conexão com o administrador de política para estabelecer caminhos de comunicação de clientes para recursos. Todo o tráfego de processos de negócios corporativos passa por um ou mais PEPs.

8. Os ativos corporativos remotos devem ser capazes de acessar recursos corporativos sem a necessidade de atravessar primeiro a infraestrutura de rede organizacional. Por exemplo, um usuário remoto não deve ser obrigado a usar um link de volta à rede organizacional (ou seja, rede privada virtual - VPN) para acessar serviços utilizados pela organização e hospedados por um provedor de nuvem pública (por exemplo, e-mail).

9. A infraestrutura usada para dar suporte ao processo de decisão de acesso na arquitetura, deve ser escalável para levar em conta as mudanças na carga do processo. O(s) PE(s), PA(s) e PEPs usados nesta arquitetura, tornam-se os principais componentes de qualquer processo de negócios. Um atraso ou incapacidade de atingir um PEP (ou incapacidade dos PEPs de atingir o PA/PE) afeta negativamente a capacidade de executar o fluxo de trabalho. Uma organização que implementa uma arquitetura zero trust, precisa fornecer os componentes para a carga de trabalho esperada ou ser capaz de dimensionar rapidamente a infraestrutura para lidar com o aumento do uso quando necessário.

10. Os ativos da organização caso não estejam de acordo, não devem conseguir atingir determinados recursos de acordo com os PEPs, devido a políticas ou fatores observáveis. Por exemplo, pode haver uma política declarando que os ativos móveis podem não conseguir alcançar determinados recursos se o ativo solicitante estiver localizado fora do país de origem da organização. Esses fatores podem ser baseados na localização (geolocalização ou localização de rede), tipo de dispositivo ou outros critérios. [13]

De com a definição dada por Kindervag (2010) sobre a Zero Trust, três pontos centrais devem ser enfatizados. Todos os três devem conduzir a especificação e a construção de uma arquitetura de rede zero trust (Zero trust Network- ZTN). O primeiro tema é que as redes começam a partir de uma " postura de confiança zero" como

comportamento padrão. Isso significa que todas as formas de confiança implícita são inválidas e as organizações devem confiar em avaliações explícitas e dinâmicas do maior número possível de fontes de dados antes de permitir que um usuário realize uma operação [12].

O segundo ponto a ser enfatizado é que o acesso é "baseado na identidade, além de outros atributos e contexto (como hora/data, geolocalização e postura do dispositivo)". Algumas fontes consolidam os dados que se estendem além de um "usuário" tradicional em um único objeto chamado agente ou agente de rede [8] [15]. Outras entidades, como a BeyondCorp do Google, pioneira na ZTN, não o fazem. A iniciativa da BeyondCorp mantém as credenciais do usuário e do dispositivo como dois componentes separados, mas necessários e críticos, de uma solução ZTN [16]. Ao explicar os conceitos de rede de confiança zero, pode ser útil incluir o modelo de agente (ou seja, dados do usuário somados aos dados do dispositivo e outros dados na instância da solicitação).

O tema final é "oferecer adaptativamente a confiança apropriada necessária no momento". Para fornecer continuamente o acesso apropriado em tempo hábil, a arquitetura ZTN deve ser capaz de atualizar rapidamente sua lógica e, idealmente, criar uma lógica nova com base em condições em evolução. Um subconjunto da lógica pode ser capturado em uma estrutura baseada em regras. Essas regras devemser armazenadas externamente ao mecanismo que as executa e em um sistema de controle de versão com os seguintes benefícios:

- *As alterações na política podem ser rastreadas ao longo do tempo.*
- *A justificativa para alterar a política é rastreada no sistema de controle de versão.*
- *O estado atual esperado da política pode ser validado em relação aos mecanismos de execução reais para uma execução tempo real*. [8].

A arquitetura zero trust também deve aproveitar as tecnologias de aprendizado de máquina (Machine learning) para aumentar a adaptabilidade, descobrindo a lógica de validação que é difícil de ser reconhecida pelos seres humanos. O aprendizado de máquina pode identificar comportamentos de risco do usuário pesquisando padrões contextuais e suspeitos nos dados [4]. Atualmente, já existem soluções que abarcam essas possibilidades, como por exemplo, a autenticação em múltiplos fatores Adaptativa (A-MFA).

Além das afirmações fundamentais, a arquitetura da rede de confiança zero (zero trust) deve considerar as seguintes prioridades no estilo RFC para a construção de uma solução:

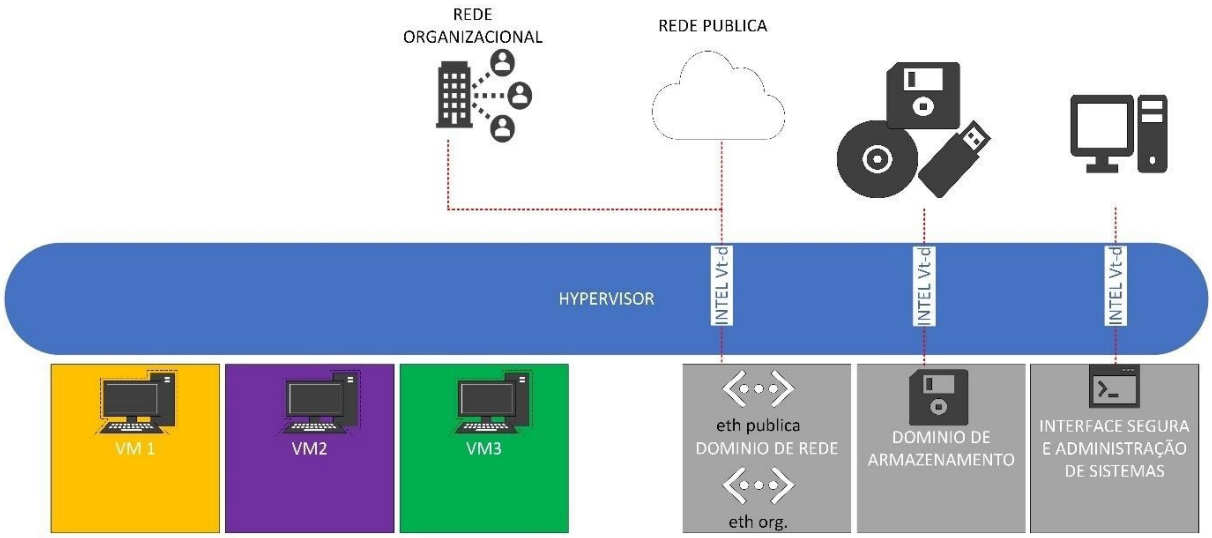
- *Todos os fluxos de rede devem ser autenticados antes de serem processados.*
- *Todos os fluxos de rede devem ser criptografados antes de serem transmitidos.*
- *A autenticação e a criptografia devem ser executadas pelos pontos de extremidade na rede.*
- *Todos os fluxos de rede devem ser enumerados para que o acesso possa ser imposto pelo sistema.*
- *Os pacotes de autenticação e criptografia mais fortes devem ser usados dentro da rede.*
- *A autenticação não deve depender de provedores públicos de PKI. Em vez disso, sistemas PKI privados devem ser usados.*
- *Os dispositivos devem ser verificados, corrigidos e rotacionados regularmente*.[8]

2.1. DEFININDO SISTEMAS DE MODELOS COM SEGURANÇA MULTINÍVEL:

Segurança multinível, também chamada de multiple level of security (mls), é a aplicação de um sistema de computador para processar informações com classificações diferentes e opostas, realizando assim uma segurança em diferentes níveis, de modo a permitir o acesso de usuários com diferentes privilégios de segurança e necessidades acesso e impedir usuários tenham acesso a informações para as quais não estão autorizados. Existem dois contextos para o qual pode ser usada a segurança multinível: A primeira é referir-se a um sistema que pode se proteger de ataques e possui mecanismos robustos para separar domínios de informação, ou seja, é confiável. O segundo contexto, refere-se a um aplicativo de computador onde o computador deve ser forte o suficiente para se proteger de ataques que tenha a intenção de subverter seus acessos definidos e deve ter mecanismos adequados para separar domínios de informação, ou seja, um sistema em que devemos confiar. essa distinção é importante porque os sistemas que devem ser confiáveis não são necessariamente confiáveis.

Um ambiente operacional baseado em múltiplos níveis de segurança, geralmente requer um sistema de processamento de informações altamente confiável. a maioria das funções pode ser suportada por um sistema composto inteiramente de computadores não confiáveis, embora isso possa exigir vários computadores independentes interconectados por canais de segurança de hardware. Um exemplo de um sistema de níveis múltiplos de segurança assistido por hardware é o isolamento assimétrico, como é apresentado na figura 05; quando um computador é usado em modos de múltiplas camadas de segurança; esse computador deve usar um sistema operacional confiável. Como todas as informações em um ambiente são fisicamente acessíveis por meio do ambiente do sistema operacional, controles lógicos rígidos devem ser implementados para garantir que o acesso às informações seja rigidamente controlado. Normalmente, isso envolve o controle de acesso obrigatório usando marcações de segurança.

Figura 05- Isolamento assimétrico através de virtualização e redes.

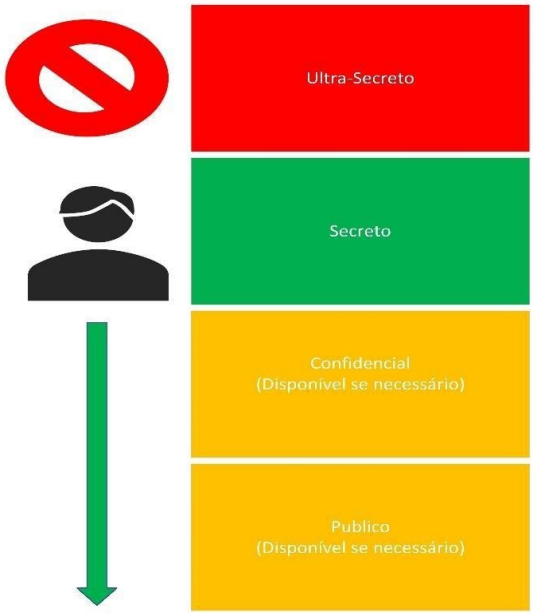


Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

Neste cenário, dois modelos se destacam, sendo eles o modelo Bell-Lapadula e o modelo BIBA. O modelo Bell-LaPadula é um modelo teórico de segurança que descreve um conjunto de regras de controle de acesso. Fora desenvolvido na década de 70 por desenvolvido por David Elliott Bell e Leonard J. LaPadula [1], funcionários do MITRE para o Departamento de defesa Americano. Este modelo é focado em confidencialidade dos dados e controle de acesso à informação classificada a fim de proteger de vazamentos ou transferência de informações[1][2]. Suas origens remontam ao uso em sistemas de mainframe militares. É focado em manter a confidencialidade dos objetos. Proteger a confidencialidade significa não permitir que usuários em um nível de segurança mais baixo acessem objetos em um nível de segurança mais alto. O modelo Bell-LaPadula opera observando duas regras: a Propriedade de Segurança Simples e a Propriedade de Segurança modelo estrela. Para o funcionamento desse modelo é necessário que a informação (Object) seja classificada para que o usuário (Subject) tenha o nível de acesso definido, geralmente nos seguintes níveis: Ultra-secreto, Secreto, Confidencial e Público (ou não classificado). Uma vez que tenhamos um ambiente onde a informação possua uma classificação (label), temos três regras não importando detalhes do usuário (Subject) desde que esse esteja em um dos níveis definido como explicado acima [1] [2].

O modelo de propriedade de segurança simples, afirma que não há “nenhuma leitura”: um usuário em um nível de classificação específico não pode ler um objeto em um nível de classificação mais alto. Usuários com uma autorização secreta não podem acessar objetos ultrassecreto, por exemplo; e o acesso a níveis inferiores deve ser concedido, apenas se necessário para a execução do trabalho, como pode ser observado na figura 06:

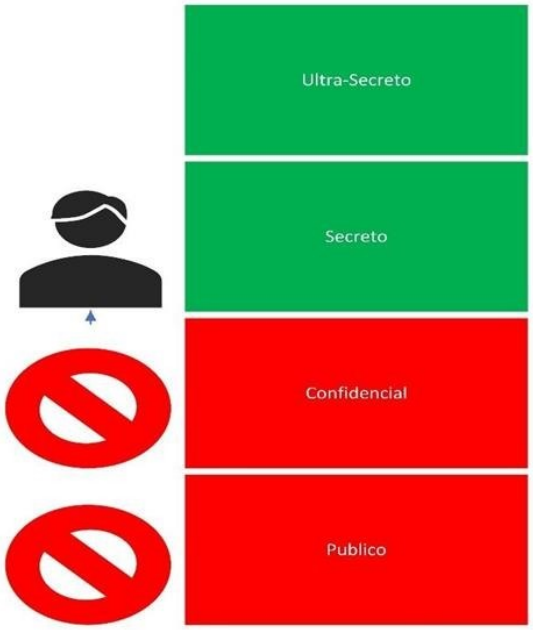
Figura 06: Demonstração do modelo Bell-LaPadula de propriedade simples.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

O modelo de propriedade de segurança estrela é “sem escrita” ou modificação. Um solicitante em um nível de classificação mais alto não pode gravar dados em um nível de classificação mais baixo. Por exemplo: usuários que estão logados em um sistema ultrassecreto não podem enviar e-mails para um sistema Secreto. Conforme podemos observar na figura 07:

Figura 07: Modelo Strong Star Bell-LaPadula.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

Dentro do modelo de controle de acesso Bell-LaPadula, existem duas propriedades que determinam como o sistema emitirá classificações de segurança para os objetos. A propriedade “Strong Tranquility” afirma que os rótulos de segurança não serão alterados enquanto o sistema estiver em operação. A propriedade “Weak Tranquility” afirma que os rótulos de segurança não serão alterados de forma que entre em conflito com as propriedades de segurança definidas. A figura 08 demonstra a aplicação Strong star aplicada com um modelo Strong Tranquility, não permitindo a leitura e escrita além do nível que o solicitante se encontra.

Figura 08: Modelo Star Strong tranquility aplicado.

Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

Apesar que o modelo Bell-Lapadula aborda o tema da confidencialidade das informações, em um cenário real, muitas organizações desejam garantir que a integridade das informações seja protegida no mais alto nível. O modelo BIBA é o modelo de escolha quando o elemento vital é a integridade da informação.

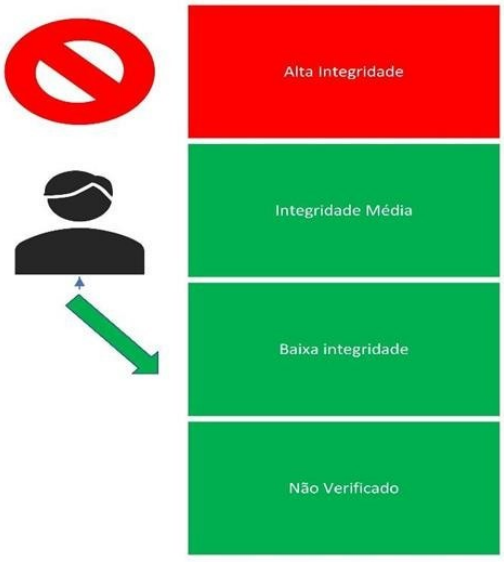
O modelo BIBA segue o mesmo formato que o modelo Bell-Lapadula, porém de forma inversa. Esse modelo possui duas regras principais: O primeiro é o modelo de Integridade Simples, onde um solicitante em um nível de classificação específico não pode ler dados em uma classificação inferior. Isso proíbe que os solicitantes acessem informações em um nível de integridade mais baixo, protegendo assim a integridade ao impedir que informações ruins subam de níveis de integridade mais baixos [3][20], conforme podemos observar na figura 09:

Figura 09: Modelo BIBA Simples.

Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

O segundo modelo a ser apresentado é o de Integridade estrela (STAR), no qual um solicitante em um nível de classificação específico não pode gravar dados em uma classificação superior, conforme podemos observar na figura 10. Isso evita que os solicitantes passem informações até um nível de integridade superior ao que eles têm permissão para alterar. Dessa forma, a integridade é protegida, evitando que informações incorretas subam para níveis de integridade mais altos.

Figura 10: Modelo BIBA STAR INTEGRITY.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio

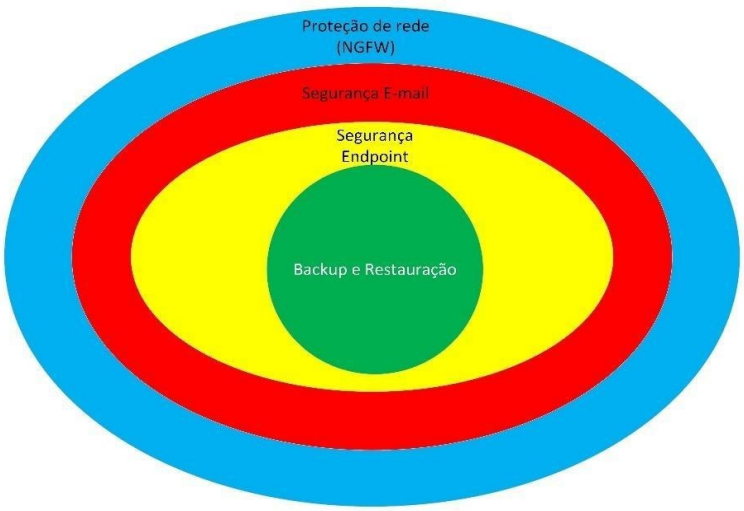
3. MODELOS DE SEGURANÇA EM CAMADAS:

A segurança em camadas é uma abordagem de segurança de rede que implanta vários controles de segurança para proteger as áreas mais vulneráveis de seu ambiente de tecnologia onde uma violação ou ataque cibernético pode ocorrer. o objetivo de uma abordagem de segurança em várias camadas é garantir que cada componente individual do seu plano de segurança cibernética tenha um backup para combater quaisquer falhas ou lacunas. essas camadas trabalham juntas para reforçar suas defesas e construir uma base sólida para seu programa de segurança cibernética. Quando é abordado o cenário tradicional do modelo de segurança em camadas, podem ser citados os seguintes controles para proteção: Administrativos, físicos e técnicos. Os controles administrativos consistem em políticas e procedimentos implementados por uma organização para minimizar vulnerabilidades e impedir que usuários da organização acessem informações que não estão autorizados a acessar. Entre as camadas de controles administrativos podemos incluir: Contas, de modo a garantir que apenas os funcionários atuais tenham contas de usuário, implementando um procedimento para fechar a conta de um funcionário na rede no caso de alguém sair da organização; Políticas implementadas e procedimentos detalhados para garantir que todos os funcionários tomem as medidas obrigatórias necessárias para proteger os dados corporativos, especialmente osdados confidenciais; A Implementação de controle de acesso baseado em função, demodo a permitir que apenas usuários autenticados acessem somente os dados que precisam para realizar seus próprios trabalhos e a minimização do uso de contas privilegiadas, como contas de administrador juntamente a imposição de restrições adicionais ao seu uso. Os controles físicos envolvem a implementação de dispositivosde segurança física tais como portas seguras com trancas nos locais onde s encontram os recursos de informação, scanners e sistemas digitais para acesso apenas autenticado e autorizado, câmeras, portões e o uso de recursos humanos como proteção vigiada. Ao abordarmos os controles técnicos, podemos citar: Autorização segura, exigindo que os usuários usem senhas fortes que sejam difíceis de adivinhar ou decifrar usando ferramentas de quebra de senha ou, se possível, implementar soluções sem senha, como cartões NFC ou dispositivos de autenticaçãofísica; a implementação de uma autenticação de dois fatores ou autenticação de

múltiplo fator (2FA/MFA) para verificar ainda mais a identidade do usuário usando vários dispositivos para fazer login e a autenticação biométrica para garantir a identidade de um usuário por meio do uso de reconhecimento facial ou digitalização de impressões digitais.

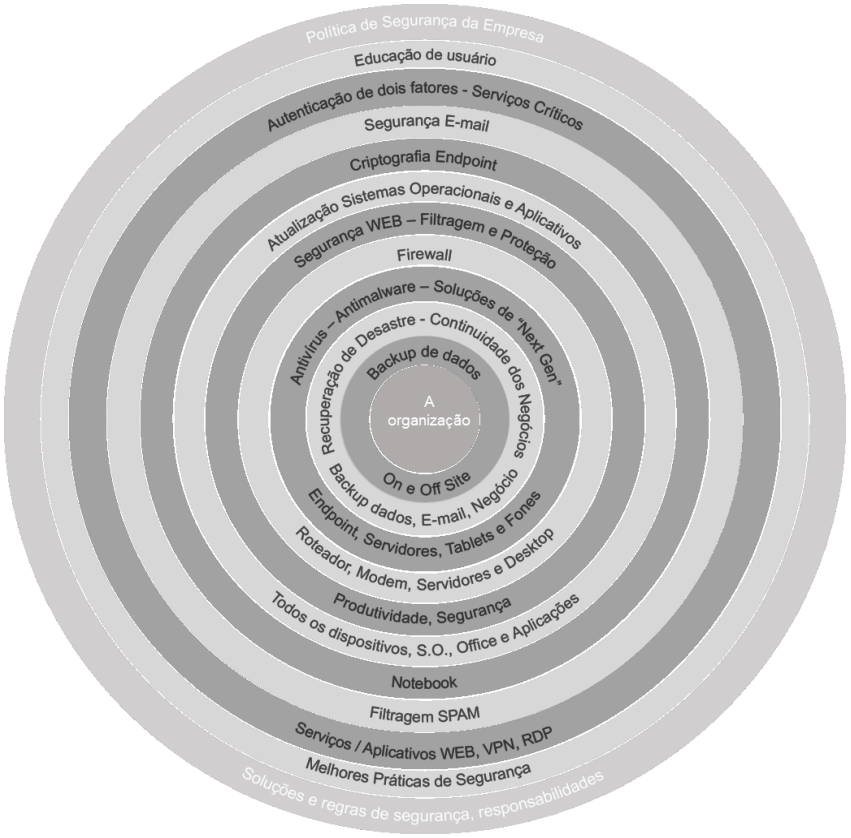
Os modelos de segurança, podem ser também cruzados para aumentar ainda mais sua eficiência, utilizando soluções de segurança de perímetro como restrições por firewall, implementação de uma rede de perímetro, sistemas de detecção de intrusão e sistemas de prevenção de perda de dados; Segurança de rede com sistemas ativos de SIEM, HIDS, IPS, IDS, correção de vulnerabilidades e gerenciamento, verificação de vulnerabilidade, segurança de dispositivos wireless e filtragem de conteúdo; Segurança de terminais (endpoints) através de sistemas de detecção e resposta (EDR), Firewall interno aos sistemas operacionais, gerenciamento de correções, sistemas anti-malware; Segurança de dados com criptografia ativa e backup, além de sistemas que chequem a validade desses backups, e finalmente a capacitação do fator “firewall humano”, que é a capacitação, conscientização e treinamento dos usuários na percepção dos riscos e ameaças. Ainda pode ser citado também como camadas de segurança, as políticas de segurança da informação, que devem abordar e manter cenários contínuos em ação e melhoria. Conforme as figuras 11 e 12, podemos observar uma arquitetura em múltiplas camadas a partir de seus componentes lógicos. Alguns dos elementos, os quais constituem um modelo de múltipla camada.

Figura 11: Modelo de segurança em camadas simples aplicado- Diagrama elaborado com a ferramenta Paint.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Paint

Figura 12: Diagrama de modelo de segurança em camadas completo- Diagrama elaborado com a ferramenta powerpoint.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Powerpoint.

4. CENÁRIOS POSSIVEIS E SUAS APLICAÇÕES:

Os conceitos de Zero Trust com modelos de segurança em múltiplos níveis, podem ser aplicados para diversos cenários e modelos no mundo real tal qual sua proposta original assim tenta explicar e trabalhar. Ao abordar sobre a arquitetura Zero Trust, é abordado também um conjunto de paradigmas de segurança da informação e cibernética, que tem como objetivo maior mover o foco das defesas dos perímetros organizacionais baseados em rede para usuários, ativos e recursos (dados, informações, etc.), porém, sem ignorar o modelo anterior.

Para que isso seja possível, o modelo Zero Trust lista alguns princípios básicos que devem ser considerados desde o primeiro momento, para planejamento e implantação da arquitetura de confiança zero:

- *Todas as fontes de dados e ativos que lidem com informações de forma computacional, são consideradas recursos;*
- *Todas as comunicações são protegidas independentemente da localização da rede;*
- *O acesso aos recursos individuais da organização é concedido tendo base a sessão;*
- *Os acessos aos recursos são determinados pela política dinâmica, incluindo o estado observado da identidade do cliente, aplicação ou serviço e dispositivo, podendo incluir outros atributos relacionados a comportamento, estado ambiente;*
- *A organização monitora e mede a integridade e postura de segurança de todos os ativos de sua propriedade ou associados a ela;*
- *Todas as autenticações e autorizações de recursos sãodinâmicas e estritamente aplicadas antes da liberação do acesso;*
- *A empresa coleta o máximo de informações possíveis sobre estado dos ativos, infraestrutura de rede e comunicação, utilizando-as para melhorar sua postura de segurança.*

Como dito anteriormente, o modelo Zero Trust exige autenticação e autorização contínua de dispositivos e usuários antes de haver a concessão de qualquer acesso aos recursos organizacionais, e também pode ser entendido como uma resposta à tendência das organizações em implementar políticas como BYOD (do Inglês Bring

Your Own Device, que significa “traga seu próprio dispositivo”), o uso crescente do acesso remoto e recursos, ou infraestruturas em nuvem, evidenciados especialmente na época da crise pandêmica causada pela COVID-19. Importante lembrar que a arquitetura de confiança zero não é composta de um único fator, e sim de um conjunto de princípios usados para direcionar as rotinas de trabalho, desenho e desenvolvimento de sistemas e realização de operações, que quando equilibrada com políticas e orientações sobre segurança cibernética, gerenciamento de identidade, de acessos e monitoramento contínuo de acordo com as melhores práticas, pode proteger contra as ameaças mais comuns, mitigar eventos inesperados e melhorar a segurança de uma organização.

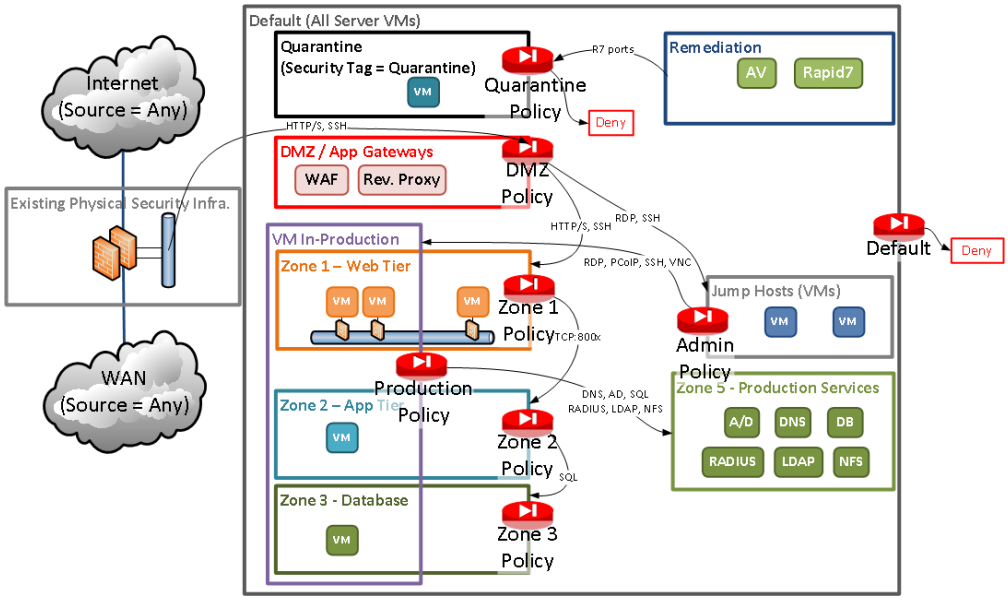
De acordo com o manual NIST SP.802-207 [13], a visão de confiança zero de rede contém algumas suposições básicas que também devem ser consideradas em seu planejamento e implementação, além dos princípios básicos citados anteriormente, levando em conta infraestruturas internas e externas, ativos e recursos pertencentes ou não à organização, entre outros cenários.

- Toda a rede local organizacional não deve ser considerada uma implícita zona de confiança, ou seja, mesmo perímetros de segurança devem ser tratados como inseguros;
- Os dispositivos na rede organizacional podem não ser de propriedade ou manipuláveis pela organização;
- Nenhum recurso é inerentemente confiável;
- Nem todos os recursos da organização estão em infraestruturas de sua propriedade (Abrindo assim a possibilidade para infraestruturas em nuvens proprietárias);
- Ativos e usuários remotos das organizações não podem confiar totalmente em sua rede local;
- Ativos e fluxos de trabalho que transitam entre infraestrutura organizacional e não-organizacional devem possuir políticas consistentes.

Atendidas as suposições básicas acima, a arquitetura de confiança zero, possui aplicação variada nos fluxos de trabalho, baseada nos componentes lógicos usados e na principal fonte de política de regras da organização. Cada aplicação implementa todos os princípios de confiança zero, citados anteriormente, mas pode utilizar um ou

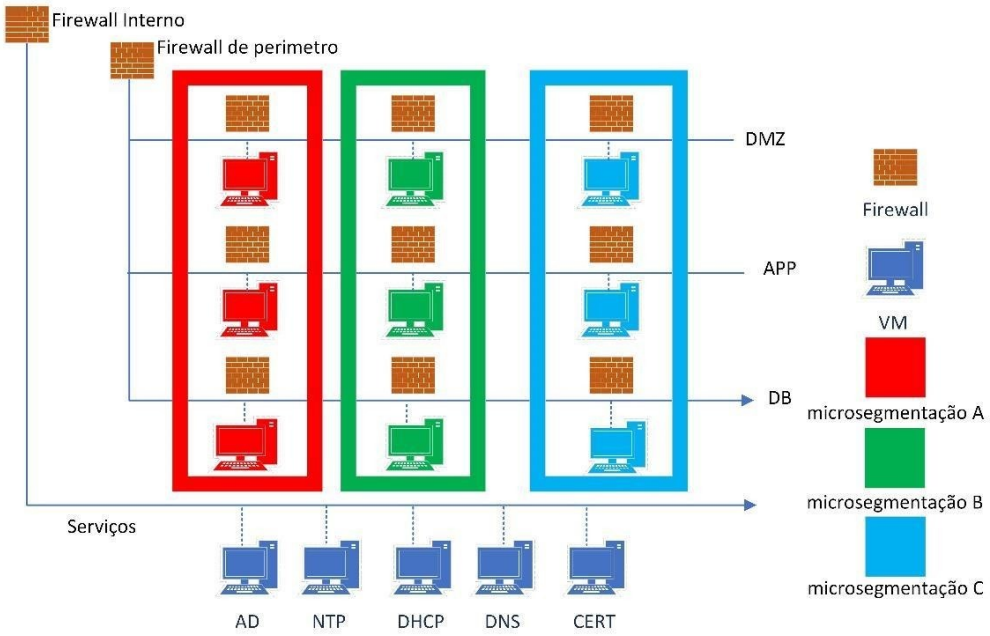
dois como principais para definição de suas políticas. Vale ressaltar que cada cenário possui particularidades que devem ser consideradas desde o planejamento para adequação a esta arquitetura e com o objetivo de atender às respectivas necessidades da organização. O elemento humano continua sendo muito relevante também neste modelo, uma vez que nos cenários modernos, consideramos que o fator humano é a principal e uma das primeiras camadas de segurança. Apesar da mitigação de movimentação lateral presente nessa arquitetura, credenciais roubadas através de golpes como Phishing (abrangentes ou direcionados) ou engenharia social ainda poderão realizar os acessos para que foram devidamente autorizados, o que pode representar um risco às respectivas informações ou recursos acessíveis por tais credenciais. Entretanto, vale lembrar que neste modelo, a identificação e resposta à um possível ataque poderá ser mais rápida e de melhor mitigação, uma vez que há uma análise do comportamento dos acessos ocorridos (como local, hora e recursos aos quais foi solicitado o acesso) e caso seja necessário, a negação imediata de acesso a estes recursos, juntamente a outras medidas de proteção ativas. Abaixo a partir da figura 13, podemos observar uma arquitetura de confiança zero com múltiplas camadas de segurança e micro segmentação aplicadas. Na figura 14, podemos observar uma arquitetura seguindo este mesmo cenário, porém, fazendo uso de máquinas virtuais e migro segmentada, onde cada máquina virtual (VM) possui seu próprio perímetro e políticas alinhadas com grupos lógicos.

Figura 13: Cenário com múltiplas camadas e segmentações.



Fonte: [24]

Figura 14: Cenário micro segmentado com máquinas virtuais. - Baseado no cenário VMware NSX-T.

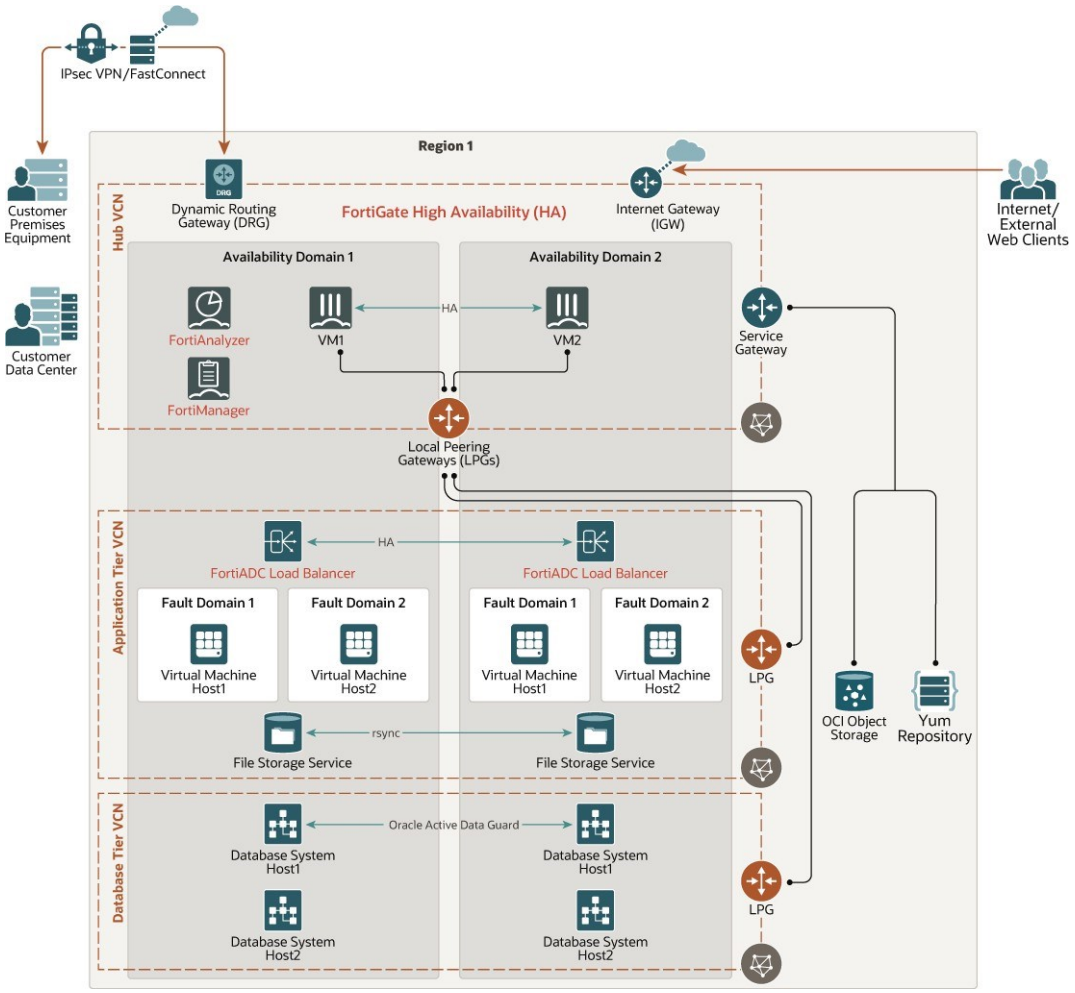


Fonte: Elaborado pelo próprio autor utilizando a ferramenta Visio.

4.1. CENÁRIO DE IMPLANTAÇÃO A PARTIR DE SOLUÇÕES PROPRIETÁRIAS:

Dentro de um cenário de implantação de uma rede Zero Trust, com soluções proprietárias, existem diversas possibilidades. Em um cenário onde a infraestrutura precisaria ser criada a partir do início, pode ser utilizado o exemplo de arquiteturas como a implantação prevista pela empresa Oracle em sua plataforma em nuvem, como podemos conferir a partir da figura 15 o modelo utilizando as duas soluções:

Figura 15: Implementação de arquitetura com soluções Fortinet e Oracle



Fonte: [25]

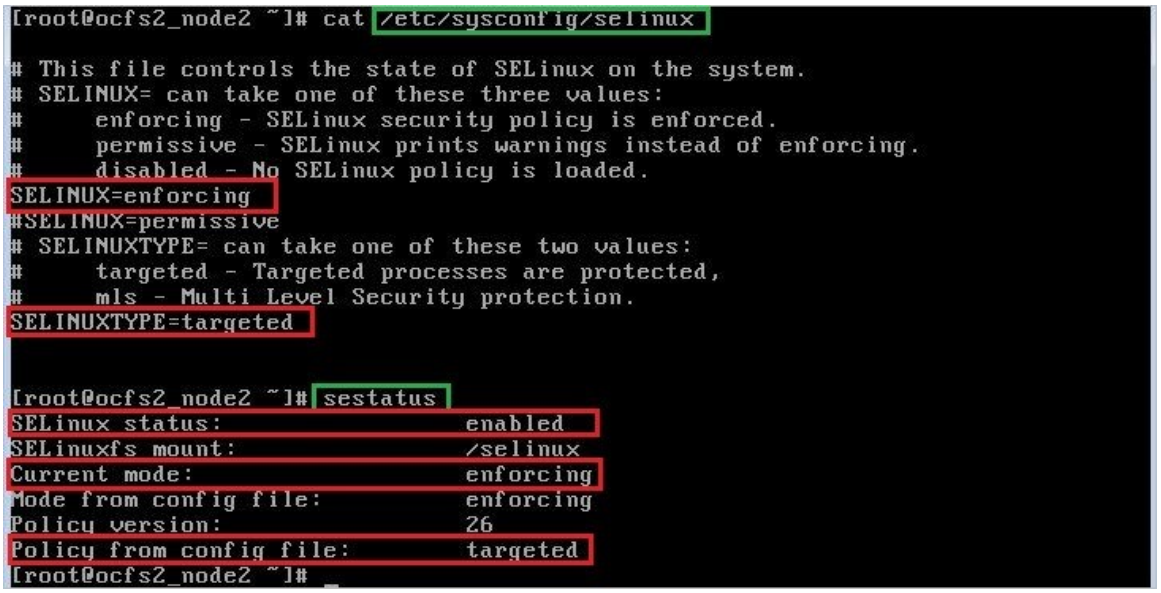
Na solução apresentada, pode se ver a implementação das soluções Oracle e Fortinet combinadas, de modo a criar um modelo de arquitetura Zero Trust. Um dos pontos interessantes durante a implementação com base na plataforma Oracle, é que a mesma segue um modelo de política que por padrão, os controles precisam ser liberados mediante a definição de políticas e diferentes níveis, por parte do administrador da nuvem, ou a pessoa autorizada a isso. Em sua estrutura de controle, sub compartimentos (Que podem ser parte de um micro segmentação), são subordinados a compartimentos aos quais estão inseridos em uma tenancy geral, aqui chamada de “estrutura raiz”. Na figura 16, podemos ver como essas políticas são implementadas a partir da plataforma da Oracle para infraestrutura em Nuvem. Toda a política para comunicação a transmissão de dados, deve descrever quais tipos de permissões devem ser dadas e quais compartimentos e grupos devem acessar os recursos especificados. Usuários, são controlados pelas políticas aplicadas aos grupos.

Figura 16: Política configurada de Oracle Cloud Infrastructure (OCI) –

Fonte: Elaborado pelo próprio autor através da captura realizada a partir de sistema OCI proprietário.

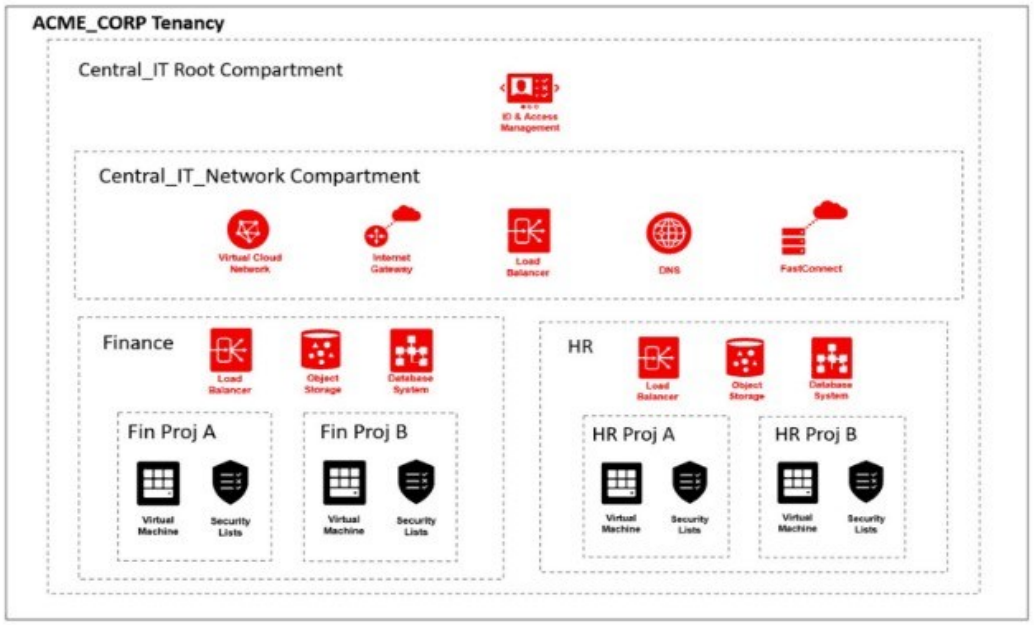
Outro ponto que pode ser destacado é que entre as máquinas virtuais Unix disponibilizadas para o uso dentro da OCI, O modelo com o sistema operacional Oracle Linux, é disponibilizado gratuitamente, possuindo por padrão o SElinux, uma melhoria também open source disponibilizada para sistemas Unix, de modo a implementar modelos de segurança em múltiplos níveis a partir da kernel. A partir da figura 17, podemos observar como é configurado um Oracle cluster File System (OCFS2), em um Oracle Linux, com a implementação do sistema MLS ativamente no modo “enforcing”. Na figura 18, podemos observar o modelo padrão de uma infraestrutura Oracle (OCI) descrevendo suas bases de estrutura e funcionamento.

Figura 17: OCFS2 em um Oracle Linux, com SElinux implementado.



Fonte: [26]

Figura 18: Estrutura básica de uma OCI (Oracle Cloud Infrastructure).

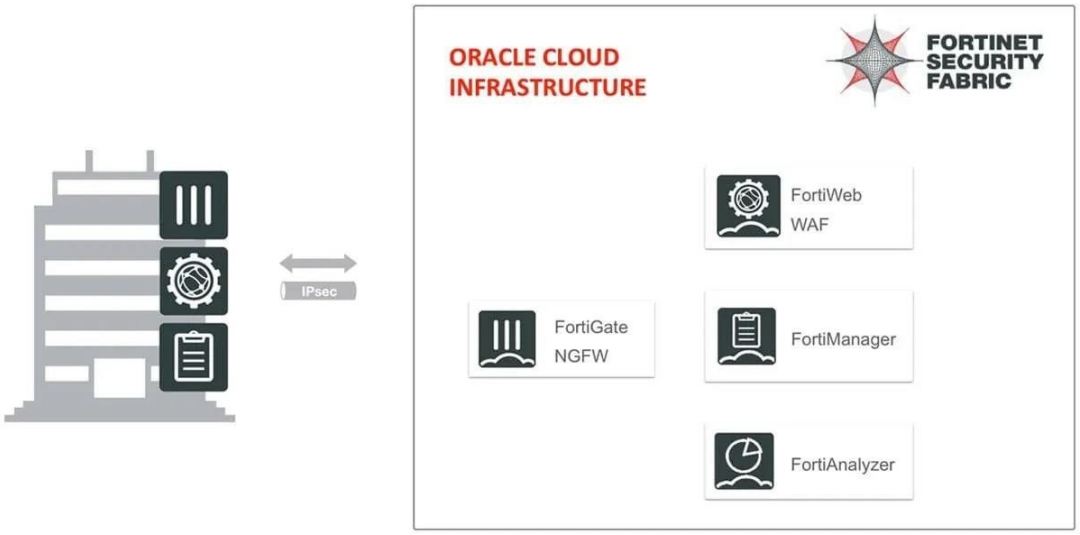


Fonte: [27]

Juntamente a estrutura disponibiliza também a possibilidade de uso de serviços para autenticação através de SAML (Security Assertion Markup Language) para o gerenciamento de identidades, monitoramento de dispositivos na nuvem, monitoramento de usuários, gerenciamento de ambiente e vulnerabilidades, VPNs e firewalls.

A aplicação dessa infraestrutura, demonstrado de forma descritiva na figura 19 e arquitetura, em conjunto com a Fortinet em conjunto com serviços como Fortinet NGFW (Firewall de nova geração), WAF, Forti Manager e FortiAnalyzer providenciam uma infraestrutura completa voltada para o ambiente organizacional em uma arquitetura devidamente estruturada para o modelo de confiança zero.

Figura 19: Infraestrutura utilizando VPN e serviços Fortinet no OCI.

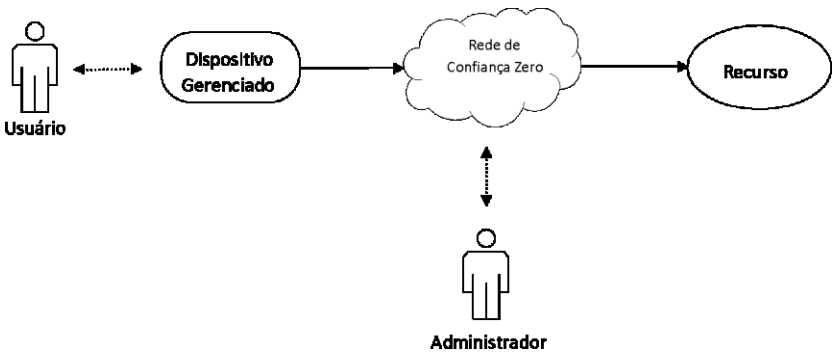


Fonte: [28]

4.2. CENÁRIO A PARTIR DE SOLUÇÕES OPEN SOURCE:

Em um cenário de implementação, através de soluções livres (open source), uma proposta teórica pode ser apresentada. O primeiro passo no processo de desenvolvimento desta solução, é definir o limite para o sistema. O limite define o que está dentro e o que está fora do domínio da solução. A definição de limite também identifica as interfaces que precisam ser refinadas ao longo do processo de desenvolvimento. Para este projeto, a rede de confiança zero é aplicada de uma forma padrão para o recurso protegido. O recurso a ser protegido é um serviço Webque fornece um conjunto de serviços relacionados ao tempo de forma segura e sem custo. Um diagrama do limite do sistema e seu diagrama teórico de infraestrutura é mostrado logo abaixo, como podemos observar descrito em passos na figura 20:

Figura 20: Limites do sistema-



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Microsoft Visio.

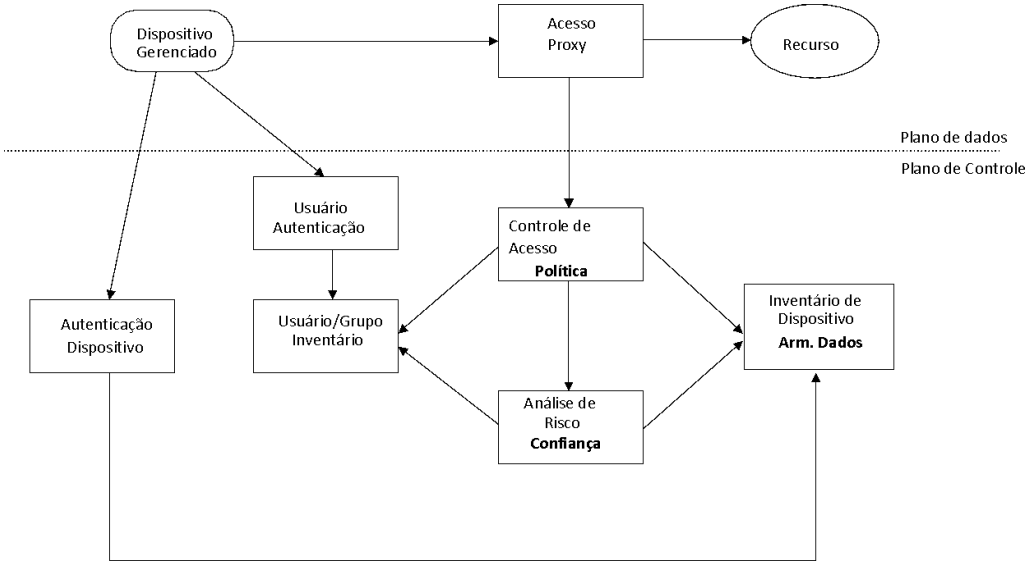
As principais entidades do nosso espaço em estudo incluem:

- **Usuário –** O usuário "atual" do dispositivo gerenciado. As credenciais dessa pessoa serão usadas nas tentativas de obter acesso ao recurso projetado.
- **Dispositivo gerenciado –** Este dispositivo é uma plataforma de computação, como um computador pessoal, tablet, smartphone, etc.
- **Recurso –** O recurso a ser protegido. Os recursos podem ser sites, aplicativos, serviços da Web, etc.
- **Administrador –** Esta função terá acesso para instalar e configurar os diferentes serviços da ZTN.

- **Zero Trust Network –** Este é o software que protege o recurso com base nos princípios das redes de confiança zero.

O próximo passo no processo é decompor o espaço de nossa arquitetura nos domínios naturais. O diagrama desses domínios é mostrado abaixo a partir a figura 21:

Figura 21: Domínios da ZTN



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Visio.

Os domínios do espaço do problema incluem:

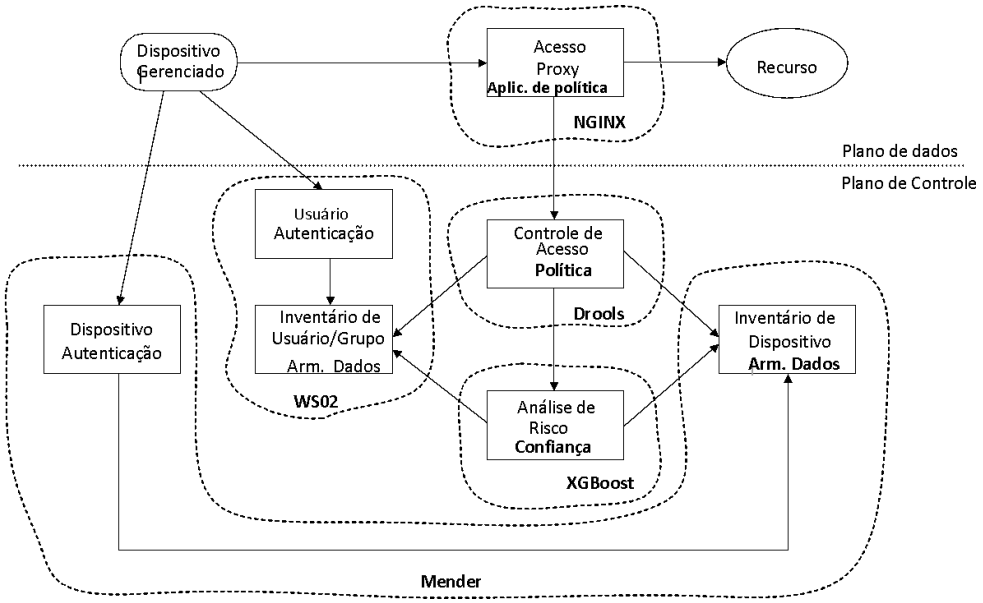
- **Proxy de Acesso –** Este domínio é responsável por fazer cumprir a decisão de permitir o acesso ou não para a solicitação especificada. Esse serviço pode ser intrusivo na medida em que o código que implementa o recurso é modificado ou padrão, o que não requer alterações. Para este projeto, a abordagem padrão é considerada.
- **Controle de Acesso –** Este domínio faz a determinação final de se o acesso é concedido ou não seguindo as diretivas de segurança. A decisão é baseada em vários tipos de informações de diferentes fontes. Idealmente, as políticas são dinâmicas e suas implementações podem ser mantidas por meio de um sistema de controle de versão.
- **Análise de Risco –** O domínio de análise de risco realiza análise de risco em solicitações específicas. Esse domínio pode implementar

regras estáticas, além de regras que são dinâmicas e evoluem com base nos padrões de tráfego do usuário e do dispositivo ao longo do tempo.

- **Autenticação de usuário –** Este domínio realiza a autenticação do usuário com base em métodos tradicionais que são aprovados pela organização.
- **Inventário de Usuário/Grupo –** O domínio de inventário de usuário/grupo armazena os dados do usuário e do grupo junto com suas associações. Essas informações são disponibilizadas aos outros domínios para análise de risco e criação de políticas.
- **Autenticação de dispositivo –** Este domínio realiza a autenticação dos dispositivos que estão acessando recursos na rede.
- **Inventário de dispositivos –** Este armazenamento de dados mantém as informações relacionadas a cada dispositivo gerenciado. Esses dados são disponibilizados aos outros domínios para análise de risco e criação de políticas.

Uma vez concluída a análise de domínio, a arquitetura de alto nível do espaço de solução pode ser construída. Cada um dos domínios será integrado por soluções comercialmente disponíveis, estruturas de código aberto, código personalizado ou uma combinação dessas opções. O diagrama da arquitetura é mostrado conforme a figura 22:

Figura 22: Diagrama da Arquitetura de alto nível.



Fonte: Elaborado pelo próprio autor utilizando as ferramentas Visio e Microsoft Paint.

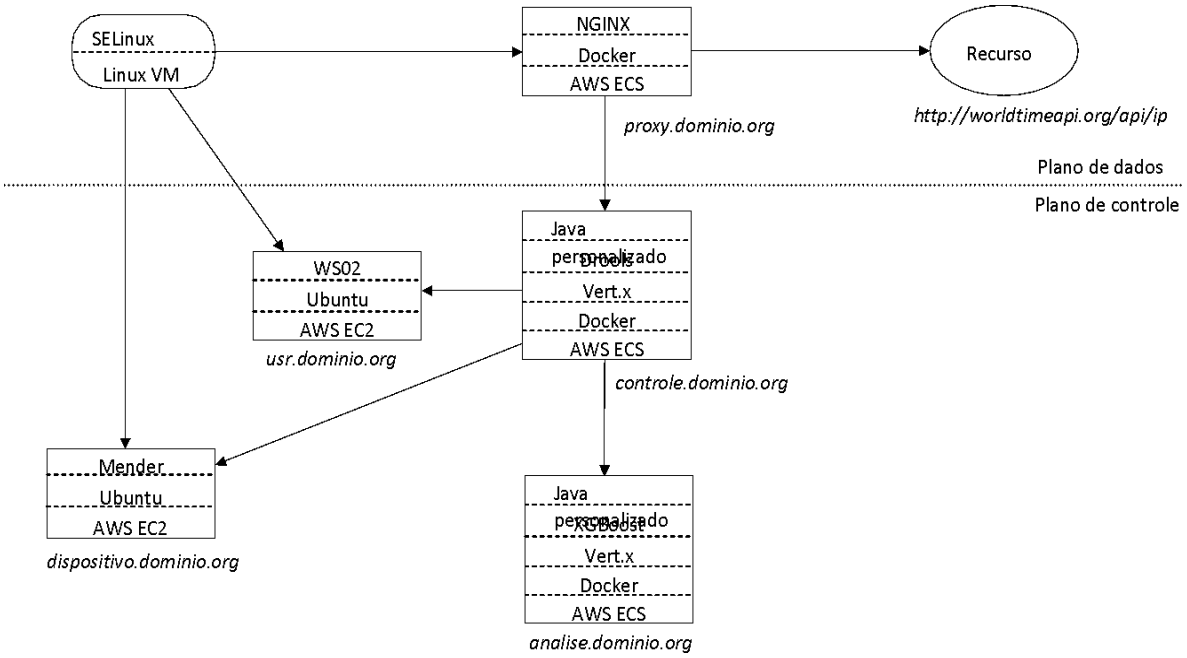
Os principais componentes da arquitetura de alto nível são:

- **Dispositivo gerenciado –** Para este projeto, uma máquina Virtual Linux, juntamente com o SELinux (Citado anteriormente).
- **Recurso –** O serviço Web para a API de horário mundial (http://worldtimeapi.org/api/ip) é usada como o recurso desprotegido. O acesso a este serviço Web será protegido pela ZTN.
- **NGINX –** Este software de código aberto é um mecanismo de proxy que intercepta as solicitações do dispositivo gerenciado e consulta o domínio do Controle de Acesso para permitir o acesso ou não. O NGINX fornece a imposição do domínio Proxy de Acesso.
- **Drools –** Drools é um Business Rules Management System (BPMS) de código aberto que fornece criação na Web e execução de regras em tempo de execução. Este software fornece a captura e execução de políticas para o domínio de Controle de Acesso.
- **XGBoost –** Este software é uma biblioteca otimizada de aumento de gradiente que implementa algoritmos de aprendizado de máquina. Ele executa a determinação de confiança para o domínio Análise de Risco.

- **Mender –** Este software fornece atualizações de nível de sistema e aplicativos para as plataformas de destino. Para este projeto, ele será usado para os domínios Autenticação de Dispositivo e Inventário de Dispositivos.
- **WS02 –** Este software fornece autenticação central e autorização para aplicações web e móveis. Para este projeto, o WSO2 é responsável pelos domínios Autenticação de Usuário e Inventário de Usuários/Grupos.
- **Docker –** Esta é uma tecnologia de contêiner que permite que o software seja facilmente implantado e dimensionado.
- **AWS ECS –** O Elastic Container Service é um serviço da Amazon que permite que imagens do Docker sejam executadas com pouca configuração.
- **Ubuntu –** Esta é uma versão popular do Linux e é um dos sistemas operacionais disponíveis na plataforma de computação da AWS.
- **AWS EC2 –** O Elastic Compute Cloud é um dos serviços da Amazon para máquinas virtuais.
- **Vert.x –** Esta é uma estrutura de microsserviços de alto desempenho fornecida pelo projeto de código aberto Eclipse.

Para a implementação da arquitetura, foi decidido usar tecnologias de serviços da Web. Todos os principais componentes são implementados como micros serviços com interfaces TLS. Os serviços foram hospedados na Amazon Web Services (AWS), assim como a máquina virtual. Com exceção do sistema de destino (worldtimeapi.org), todos os componentes do sistema foram hospedados na AWS. Um diagrama da arquitetura detalhada é demonstrado na figura 23:

Figura 23: A arquitetura em nuvem.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Visio.

Uma vez que todos os serviços foram identificados e descritos, o próximo passo é apresentar como suas interações coordenadas alcançam o comportamento desejado do sistema.

O processo de uma solicitação bem-sucedida pelo cliente consiste nas seguintes etapas:

1. *O programa cliente Java máquina virtual Linux usa o protocolo OAuth2 para solicitar um token de acesso para os dados do usuário do serviço "usr".*
2. *O programa Java, em seguida, usa o protocolo OAuth2 para solicitar um token de acesso para os dados do dispositivo do serviço "dispositivo".*
3. *O programa cliente Java personalizado envia uma solicitação para a hora junto com os dois tokens de acesso para o serviço "proxy".*
4. *O serviço "proxy" recebe a solicitação e a encaminha para o serviço "controle".*
5. *O serviço "controle" usa o token de acesso do usuário para recuperar os dados do perfil de usuário do serviço "usr".*

6. O serviço “controle” usa o token de acesso do dispositivo para recuperar os dados do perfil do dispositivo do serviço “dispositivo”.

7. O serviço “controle” aplica as regras do Drools aos dados. Se qualquer uma das regras retornar um resultado falso, um código de status "Não autorizado" será retornado ao serviço “proxy”. Se todas as regras retornarem um resultado verdadeiro, o processamento continuará para a próxima etapa.

8. O serviço “controle” envia uma solicitação junto com os perfis de usuário e dispositivo para o serviço “análise”.

9. O serviço “análise” aplica o algoritmo de aprendizado de máquina aos perfis e calcula uma previsão de risco que está no intervalo entre 0-100. Esse valor é retornado na mensagem de resposta.

10. O serviço “controle” aplica outra regra ao valor de previsão. Se a previsão for 75 ou superior, um código de status de sucesso será retornado. Se for menor que 75, um código de status de falha será retornado.

11. O serviço “proxy” examina o código de status retornado e, se aprovado, encaminha a solicitação para o serviço worldtime.api.org. Se a solicitação não foi aprovada, um código de status "não autorizado" é retornado ao originador da solicitação (ou seja, o código Java inserido na máquina virtual).

12. O serviço worldtime.api.org recebe a solicitação e retorna uma resposta com os dados de tempo baseados em JSON.

13. O serviço “proxy” recebe a resposta e a retorna ao programa Java personalizado na máquina virtual.

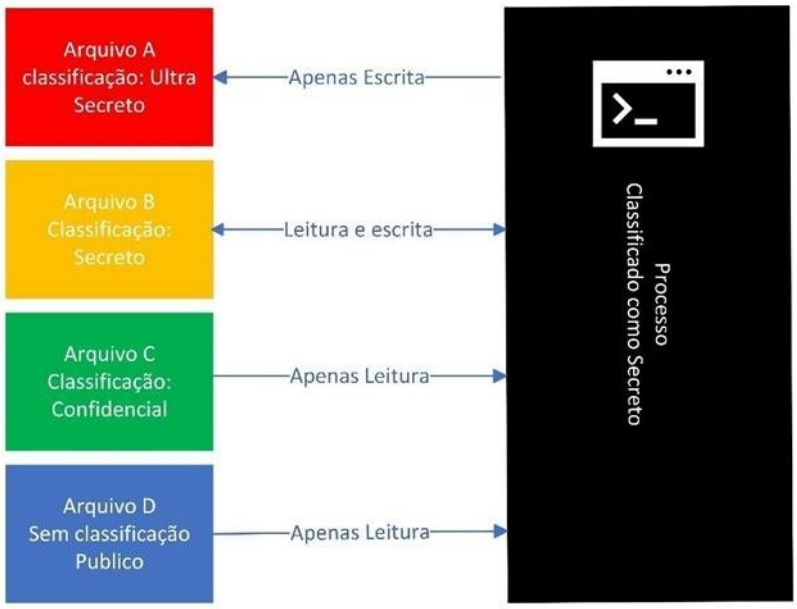
Para esta versão de uma rede de confiança zero, a profundidade e o tamanho dos dados são limitados a esses dois pontos: O primeiro são os sistemas de inventário de usuários e dispositivos (ou seja, WSO2 e Mender, respectivamente) e o segundo é a dimensão do tempo. Outras dimensões candidatas incluem geolocalizações das solicitações, padrões de sequência das solicitações e simultaneidade de solicitações de outros dispositivos gerenciados autorizados com o usuário.

Os dados do usuário mantidos no sistema WS02 podem ser acessados por meio de uma interface baseada em OAuth2. Essas informações são representadas em uma estrutura baseada em JSON de modo a armazenar as informações de modo legível e sistematizada.

Para as configurações da máquina virtual Linux com SElinux, foi optado por aplicar a regra “permissive” de modo a não conflitar com as políticas a serem

implementadas. Essa regra nega o acesso com base nas regras de política próprias do SELinux, um conjunto de diretrizes que controlam o mecanismo de segurança. As políticas aplicas foi a “MLS” de modo a estruturar um sistema de segurança multinível. A figura 24 apresenta um diagrama demonstrando o funcionamento de um sistema de fluxo de dados com o sistema MLS Oracle, aplicado através do Oracle Linux.

Figura 24: Demonstração de um sistema de fluxo de dados com a implementação da MLS baseada no modelo Bell-LaPadula.



Fonte: Elaborado pelo próprio autor utilizando a ferramenta Visio.

5. CONCLUSÃO:

Ao estudar as definições modelos e soluções possíveis de implementação do cenário de arquitetura zero trust, é possível observar que apesar de novos e aparentemente complexos temas e estruturas, ela é de um modelo de implementação simples, uma vez que a infraestrutura construída começa com a mesma arquitetura como guia. É importante lembrar também, que em cenários onde há uma infraestrutura de rede já existente, aplicar os conceitos e a arquitetura, requerem maiores estudos e uma abordagem mais complexa e cuidados, pois é necessário considerar os ativos lógicos e físicos ao mesmo tempo, que a interação dos dados e controle, para que o andamento de uma organização não seja impactado significativamente durante sua implementação e suas operações possam continuar.

Ainda no cenário brasileiro de segurança cibernética, pouco se sabe sobre o tema, apesar de que este tem sido um caminho tomado por muitas organizações, mesmo que de forma inconsciente. Esta forma de adaptação, inconsciente e movida por informações muitas vezes incompletas, tem relação com a falta ou parcialidade das informações sobre o tema, muitas vezes abordado de forma difícil e com terminologias difíceis, quando a premissa básica é que nunca se deve confiar, sempre verificar, mesmo que o dispositivo seja parte dos ativos e esteja dentro do perímetro de segurança da organização, e uma estratégia onde Sempre deve se autenticar e autorizar, aplicando o princípio de privilégios mínimos e através de um monitoramento constante e adaptabilidade continua, focada em melhorias constantes de acordo com as ameaças presentes no momento.

Com este trabalho, buscou-se presentar as possibilidades dos cenários a partir de suas definições e modelos possíveis de implementação, de acordo com o tempo presente e o cenário atual, de modo que se espera que este trabalho possa futuramente auxiliar em futuras implementações de arquiteturas ao qual se buscou apresentar.

REFERÊNCIAS:

1. BELL, David Elliott; LAPADULA, Leonard J. Secure Computer Systems: Mathematical Foundations. 1. Ed. Massachusetts: MITRE Corporation, 1973.
2. Bell, David Elliott and LaPadula, Leonard J. Secure Computer System: Unified Exposition and Multics Interpretation. 1. Ed. Massachusetts: MITRE Corporation, 1976.
3. BIBA, K. J. Integrity Considerations for Secure Computer Systems, MTR-3153. 1. Ed. Massachusetts: MITRE Corporation, 1975,
4. COLUMBUS, Louis. "Three Ways Machine Learning Is Revolutionizing Zero Trust Security". 11 de Mai. De 2018. Disponível em: https://www.forbes.com/sites/louiscolumbus/2018/05/11/three-ways-machine-learning-is-revolutionizing-zero-trust-security/?sh=5cd7ce1081ed. Acessado em:
5. CUNNINGHAM, Chase. The Zero Trust eXtended (ZTX) Ecosystem - Extending Zero Trust Security Across Your Digital Business Disponível em: https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf. Acessado em: Out. 2022.
6. DAOUEHI, Wadhah “Mount an OCFS2 while the SELinux status on enforcing mode”. 15 de Fev. de 2014. Disponível em https://wadhahdaouehi.tn/2014/02/mount-an-ocfs2-while-the-selinux-status-on-enforcing-mode/. Acessado em:
7. GARBIS, Jason; W. CHAPMAN, Jerry. Zero Trust Security: An Enterprise Guide. Atlanta: Appress, 2017.
8. GILMAN, Evan; BARTH, Doug. Zero Trust Networks: Building secure systems in untrusted networks. 1. ed. California: O’Reilly, 2017.
9. HILL, GT. "AI, machine learning and your access network," Network World. 20 de Fev. de 2018. Disponível em: https://www.networkworld.com/article/3256013/ai-machine-learning-andyour-access-network.html. Acessado em: Out. 2022
10. KINDERVAG, John “No More Chewy Centers: Introducing the Zero Trust Model of Information Security”. 1. Ed. Massachusetts: Forrester Research, 2010.

11. KUMAR, Atul “OCI IAM & IAM Policy | Compartment in OCI” 2 de Set. de 2022. Disponível em https://k21academy.com/1z0-1072/iam-in-oci-user-groups-compartment-policy-tags-federation-mfa/. Acessado em:
12. MCQUAID, Aaron; MACDONALD; Neil et al. "Market Guide for Zero Trust Network Access" 17 de Fev. de 2022. Disponível em: https://www.gartner.com/doc/reprints?id=1-29CX72CW&ct=220309&st=sb Acessado em:
13. NIST Special Publication 800-207: “Zero Trust Architecture”. National Institute of Standards and Technology, Gaithersburg, Agosto de 2020. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-207/final. Acessado em: Out.2021
14. NUNES, Luana. “Ciberataques aumentaram 16,17% no Brasil, só no primeiro semestre de 2021”. Gizmodo, São Paulo, 21 de Out. de 2021. Disponível em: https://gizmodo.uol.com.br/ciberataques-aumentaram-1617-no-brasil-so-no-primeiro-semestre-de-2021. Acessado em:
15. SINKEVIČIŪTĖ, Evelina, "Fyde: Zero Trust architecture and components,” 24de Dez. De 2019. Disponível em: https://www.fyde.com/resources/fyde-zero- trust-architecture-and-components. Acessado em: Mai. 2022.
16. WARD. Rory; BEYER, Betsy. "Beyond Corp - A New Approach to Enterprise Security," Disponível em: https://www.usenix.org/publications/login/dec14/ward. Acessado em:
17. “Fortinet Security Fabric para a Oracle Cloud”. Fortinet. Disponível em: https://www.fortinet.com/br/products/public-cloud-security/OracleCloud. Acessado em:
18. “Hybrid Reasoning”. JBoss Community Documentation. Disponivel em: https://docs.jboss.org/drools/release/6.4.0.Final/drools-docs/html/ch05.html. Acessado em: Ago. 2022.
19. “Implementing a Zero Trust Security Architecture”. Disponível em: https://networkinferno.net/implementing-a-zero-trust-security-architecture. Acessado em:
20. “mac_biba -- Biba data integrity policy”. FreeBSD. Disponível em: http://man.freebsd.org/mac_biba. Acessado em:
21. “Multi-Level Security (MLS). REDHAT. Disponível em https://access.redhat.com/documentation/en-

us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/mls Acesso em: Out.2022

22. “Proteger o Oracle PeopleSoft Suite com o Fortinet Security Fabric”. Fortinet. Disponível em: https://docs.oracle.com/pt-br/solutions/peoplesoft-fortinet-oci/index.html#GUID-7FEA0BDE-A0A3-4C68-8983-7B1EE2EBE279 Acessado em:

23. “What is Zero Trust?”. Paloalto Networks. Disponível em: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture. Acessado em: Mai. 2022.

24. “What Is Zero Trust?”. Ping Identity,.2 de ago. de 2021. Disponivel em: https://www.pingidentity.com/en/company/blog/posts/2019/what-is-zero-trust.html. Acessado em: Mar. 2022

25. “XGBoost Algorithm”. Amazon. Disponível em: https://docs.aws.amazon.com/sagemaker/latest/dg/xgboost.html. Acessado em: Out. 2022

26. “Zero Trust Security | What's a Zero Trust Network”. CloudFlare. Disponível em: https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/. Acessado em: Mai. 2022.