Thesis/Project on:

Implementing Zero Trust Network in an Enterprise Network

Submitted By:

Name	Roll
Ibrahim Khalid	24114
Md. Imran Hossen	24115
Md. Main Uddin	24103

A project report submitted to the Institute of Information Technology
in partial fulfilment of the requirements for the degree of
Post Graduate Diploma in Information Technology
(PGDIT)

Supervisor:

Prof. Dr. M. Mesbahuddin Sarker
Professor

Institute of Information Technology

Institute of Information Technology
Jahangirnagar University
Savar, Dhaka-1342

May, 2025

DECLARATION OF CANDIDATES

We hereby declare that this thesis/project titled “Implementing Zero Trust Network in an Enterprise Network” is based on the results found by us. Materials of work found by other researchers are mentioned by reference. This thesis, neither in whole nor in part, has been previously submitted for any degree.

Ibrahim Khalid
(Roll: 24114)

Md. Imran Hossen
(Roll: 24115)

Md. Main Uddin
(Roll: 24103)

CERTIFICATE

The thesis/project titled “Implementing Zero Trust Network in an Enterprise Network” Submitted by (1) Ibrahim Khalid, Exam. Roll: 24114, (2) Md. Imran Hossen, Exam. Roll.: 24115, & (3) Md. Main Uddin, Exam. Roll: 24103, Session: PGDIT Spring-2024, has been accepted as satisfactory in partial fulfillment of the requirement for the degree of “Post Grade Diploma in Information Technology (PGDIT)” on Date-of-Defense.

_____

Prof. Dr. M. Mesbahuddin Sarker,
Professor, IIT, JU & Supervisor

Accepted and approved in partial fulfillment of the requirement for the degree “Post Graduate Diploma in Information Technology (PGDIT)”.

BOARD OF EXAMINERS

_____

Dr. Shamim Al Mamun,
Professor, IIT, JU

Coordinator
PGDIT Coordination Committee

_____

Dr. Risala Tasin Khan
Professor, IIT, JU

Member
PGDIT Coordination Committee
& Director IIT

_____

Dr. Mohammad Shahidul Islam
Professor, IIT, JU

Member,
PGDIT Coordination Committee

ACKNOWLEDGEMENT

We are deeply grateful to our supervisor, Prof. Dr. M. Mesbahuddin Sarker, Professor, Institute of Information Technology, Jahangirnagar University, for his valuable guidance, encouragement, and support throughout the course of this project. His insight and feedback were instrumental in shaping our work. We would also like to thank the faculty and staff of the Institute of Information Technology, as well as our fellow classmates, for their cooperation and suggestions during our research and development process. Last but not least, we thank our families for their continuous support and motivation.

Sincerely,

Ibrahim Khalid, 24114
Md. Imran Hossen, 24115
Md. Main Uddin, 24103
May, 2025

ABSTRACT

In today’s rapidly evolving cybersecurity landscape, traditional perimeter-based security models are proving inadequate in defending against increasingly sophisticated threats. This project explores the design and implementation of a Zero Trust Network (ZTN) within an enterprise network environment. Unlike conventional models that assume implicit trust within the network perimeter, Zero Trust operates on the principle of "never trust, always verify," requiring strict identity verification and access control for every user and device, regardless of location. The project involves a detailed analysis of current enterprise network vulnerabilities, the architectural redesign required to implement Zero Trust principles, and the integration of key technologies such as micro-segmentation, multi-factor authentication (MFA), identity and access management (IAM), and continuous monitoring. A prototype Zero Trust framework was deployed and evaluated in a simulated enterprise setting, demonstrating improved security posture and reduced attack surface. The results validate Zero Trust as a viable and necessary paradigm shift for securing modern enterprise networks against internal and external threats

List of Figures

List of Tables

Contents

Chapter 1

Introduction

1.1 Background

The growing complexity of enterprise networks moment with pall operations, remote workers, and IoT bias has driven the swell in cybersecurity attacks. Perimeter- grounded security models that are based on the old notion of a trusted border no longer shield critical means. Zero Trust is an innovative cybersecurity architecture that breaks the traditional mindset, taking a “no trust, always corroborate" stance. Every device, store, and operation are authenticated, regardless of their position, so that only authenticated and authorized individuals have access to coffers.

The ideal of this design is to emplace a Zero Trust Network (ZTN) within an organizational setup through the use of open- source tools. Grounded on technologies similar as Active Directory(announcement) and Microsoft Entra, Wazuh, Suricata, Cilium, and pfSense, this design demonstrates the eventuality of associations to strengthen security structure and alleviate pitfalls due to unauthorized access, side movement, and data breaches.

1.2 About zero trust

Zero Trust is a security strategy. It is not a product or a service, but an approach in designing and enforcing the following set of security principles.

Table 1.1: Table of Zero Trust Principles

Principle	**Description**
Verify explicitly	Always authenticate and authorize based on all available data points.
Use least privilege access	Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
Assume breach	Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Zero Trust is a security strategy that assumes no user or device should be trusted by default, even if they are inside the network. Instead, every access request must be verified as if it comes from an untrusted source. This approach is designed to protect users, devices, applications, and data across modern, mobile, and cloud-based environments.

Rather than relying on perimeter defenses, Zero Trust enforces strict identity verification and access controls throughout the organization. It shifts the mindset from “trust by default” to “trust by exception,” requiring continuous validation to reduce the risk of breaches.

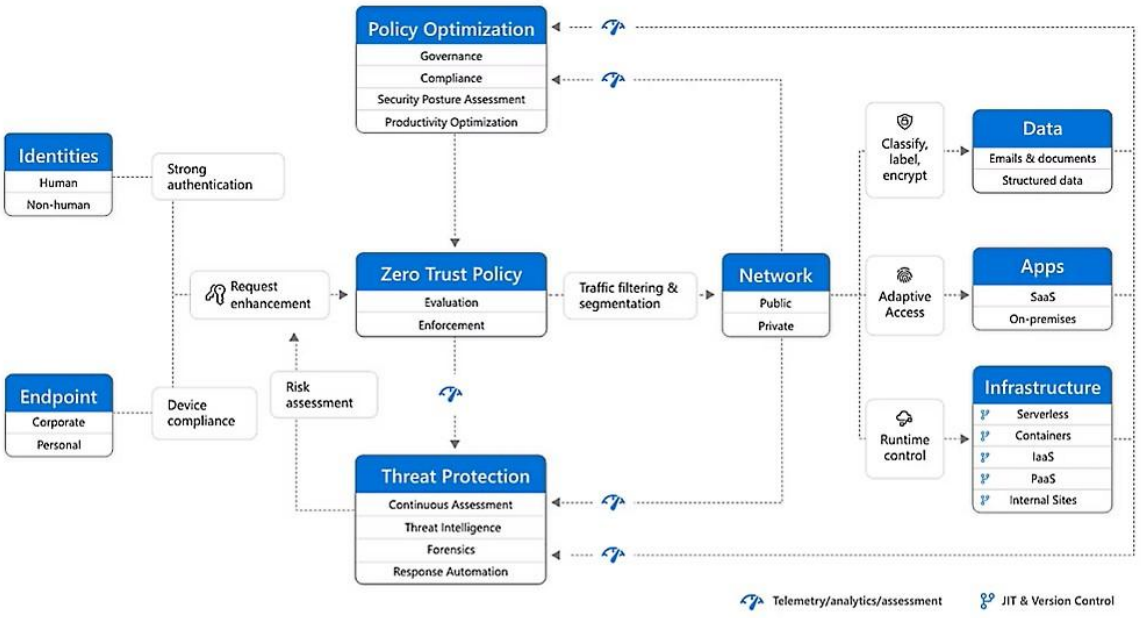

Figure 1.1: Zero Trust Architecture

1.3 The Zero Trust Security Model

An intertwined capability to automatically manage those exceptions and cautions is important. We can more fluently describe pitfalls, respond to pitfalls, and help or block uninvited events across our association. Zero Trust is an end- to- end security strategy that monitors and controls the six main pillars of security identity, endpoints, operations, network, structure, and data.

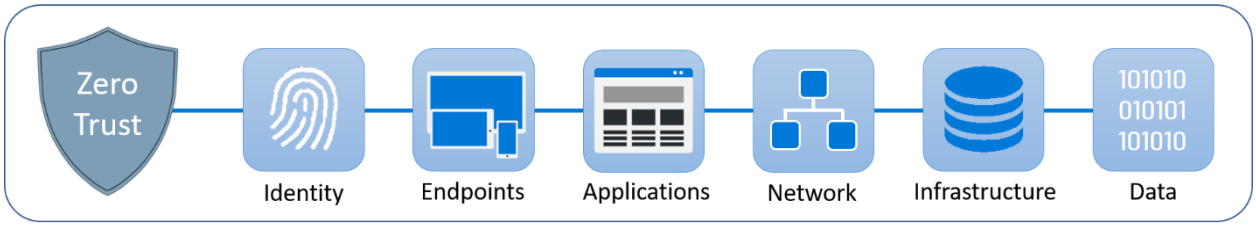

Figure 1.2: Zero Trust security model

The Zero Trust approach addresses the security enterprises that crop due to the evolving digital geography. Nearly every association has a mobile, remote or cold-blooded pool, pall operations, data stored in different surroundings, and bias enrolled from colorful locales. In the absence of a robust security model, all these factors can inadvertently lead to a major security breach.

In practice, the" trust no bone and corroborate everything" rule suggests that every request, device, or stoner must not be trusted and should be treated as an implicit trouble until vindicated by strong authentication styles, before allowing access to the network. This also means that druggies and bias are only allowed access to specific operations or data that they need.

1.4 Zero Trust Principles

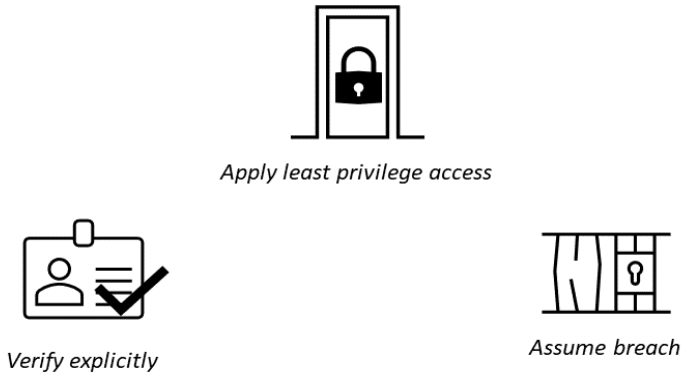

Figure 1.3: Zero Trust principles

The Zero Trust model is based on three key principles:

1. Verify explicitly – Always authenticate and authorize every user and device before granting access, using continuous and context-aware verification.
2. Use least privilege access – Limit access to only what is needed, for the shortest time necessary, using Just-In-Time and Just-Enough-Access methods.
3. Assume breach – Operate as if attackers are already inside the network. Monitor continuously, deny by default, and isolate threats to minimize damage.

1.5 Zero Trust as A Security Strategy

The traditional border-based security approach focuses on protecting network access by creating a secure perimeter using tools like firewalls and Virtual Private Networks (VPNs). Firewall filters incoming and outgoing traffic to block malicious content, while a VPN creates a secure, encrypted connection over public networks, keeping user data private and identity anonymous.

This model assumes that everything inside the network is safe, categorizing users and devices as either “trusted” or “untrusted” based on their location or ownership. For example, employees using company-owned devices on-site are considered trusted and granted broad access to internal resources. However, this assumption can be dangerous.

As organizations adopt remote and hybrid work models and allow BYOD (Bring Your Own Device) practices, the traditional perimeter becomes harder to define and defend. This model is vulnerable to:

- Insider threats leaking sensitive data,
- Cybercriminals using stolen credentials,
- Exploited users as entry points,
- Infected devices spreading malware.

In today’s dynamic digital environment, this outdated approach struggles to protect data and systems effectively, highlighting the need for more adaptive models like Zero Trust.

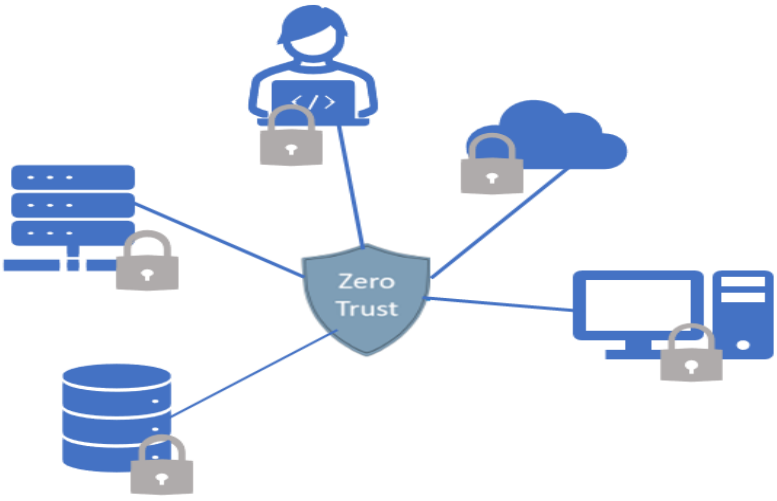

Figure 1.4: Zero Trust approach

1.6 Zero Trust Components

The Zero Trust model is a strategic, step-by-step security framework that ensures protection across all layers of an organization's digital environment. It is not a single product or service, but a comprehensive approach built after assessing all critical assets, systems, and connections. Zero Trust emphasizes continuous verification and minimal disruption while securing the entire digital estate.

At its core, Zero Trust focuses on six interconnected pillars:

1. Identities: These include users, services, and credentials. Every identity must be verified using strong authentication, and access should follow the principle of least privilege—only what's necessary, and only when needed.
2. Endpoints: Any device that connects to the network—whether corporate-issued, personal (BYOD), IoT, or guest—must be secured. Since data flows through these endpoints, they must be continuously monitored and protected.
3. Applications: Apps are gateways to data. They must be tightly controlled, with permissions managed and monitored for abnormal behavior to prevent unauthorized access or data leakage.
4. Networks: Networks enable access to resources. Zero Trust uses segmentation, real-time monitoring, and threat detection to prevent lateral movement by attackers and to isolate threats quickly.
5. Infrastructure: This includes both on-premises and cloud-based systems. Maintaining secure configurations and keeping software up to date is essential to reduce vulnerabilities.
6. Data: Data must be classified, access-controlled, and monitored. Strong data governance policies help prevent unauthorized sharing or leakage of sensitive information.

1.7 Problem Statement

The traditional border security model assumes that formerly a stoner or device enters the network, it can be trusted. Still, with the increase in remote work and pall operations, the network border is increasingly porous. This creates a need for a security model that continuously verifies every request, indeed, if the request originates from inside the network. The Zero Trust architecture addresses this need by ensuring that no device or user is trusted by default.

1.8 Zero Trust Network Architecture:

Below is the architecture diagram illustrating the components involved:

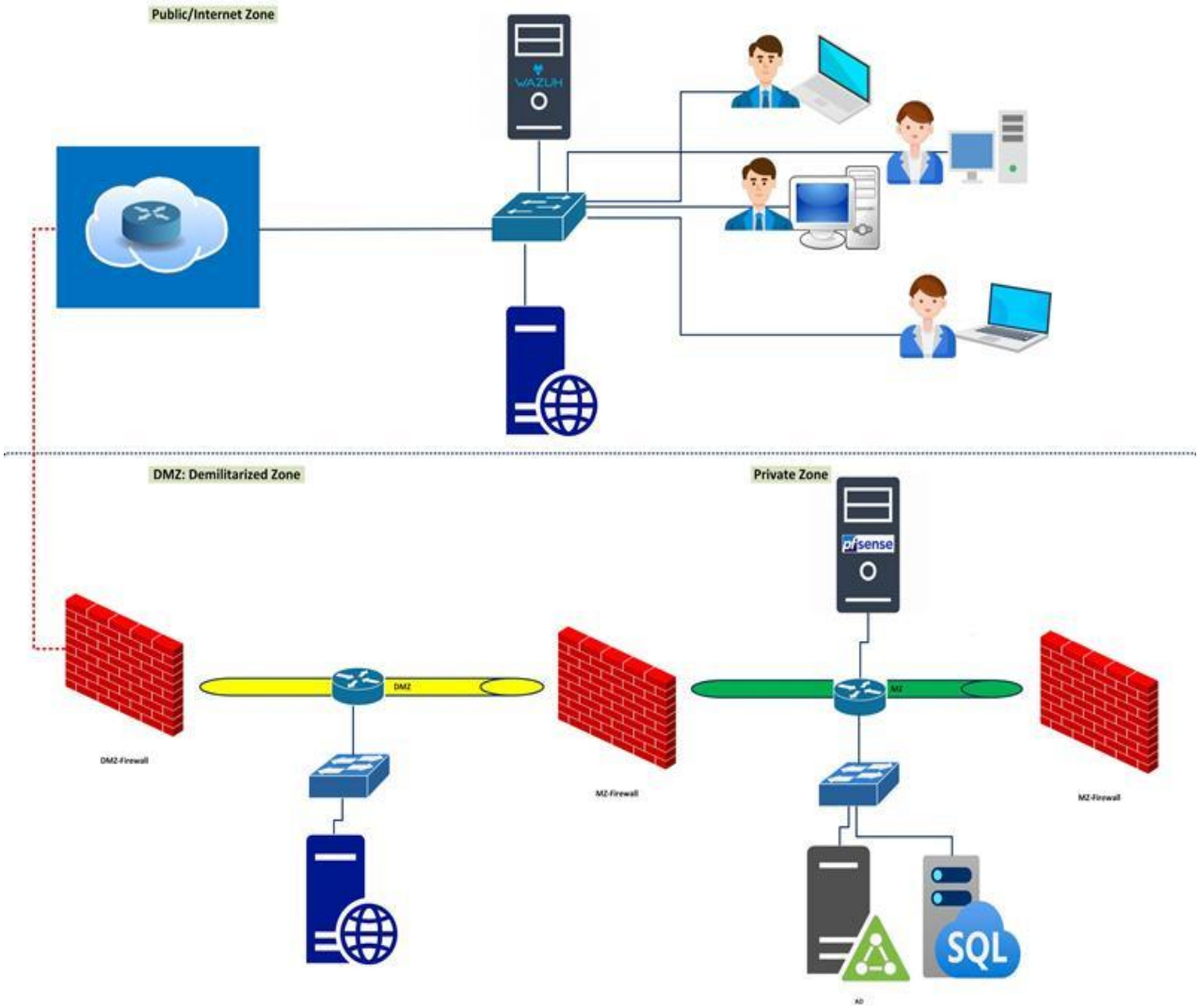

Figure 1.5: Zero Trust Network Design

- Active Directory (AD) and Microsoft Entra: Centralized authentication system ensuring that only authorized users can access the network.
- Cilium: Implements network segmentation and enforces access policies between different network zones.
- Wazuh: Monitors security events in real time and generate alerts.
- Suricata: Detects potential threats at the network level.
- pfSense: Manages traffic between network segments and applies firewall policies.

1.9 Scope:

- **Target Network:**
    - A dissembled enterprise network comprising servers, workstations, and cloud-based operations.
    - Includes both on-premises and hybrid cloud infrastructure.
    - Simulated internal and external threat environments for testing.
- **Tools:**
    - Open-source tools such as Wazuh (SIEM), Suricata (IDS/IPS), Cilium (network observability and security), and pfSense (firewall/router).
    - Microsoft Active Directory for centralized identity, authentication, and authorization management.
    - Integration with Elastic Stack for log aggregation and visualization.
    - Use of Ansible or Terraform for infrastructure automation and configuration management.
- **Security Focus:**
    - Identity and access management (IAM) with role-based access control (RBAC).
    - Network segmentation using microsegmentation and VLANs.
    - Real-time monitoring and alerting for anomalies and intrusions.
    - Threat detection and incident response workflows.
    - Log correlation and forensic analysis.
    - Policy enforcement and compliance auditing.
    - Zero Trust architecture principles implementation.
    - Endpoint detection and response (EDR) integration.

Chapter 2

Methodology

2.1 Tools & Technologies:

- Active Directory (AD) and Microsoft Entra– For managing user identities, authentication, and authorization.
- Suricata – For network intrusion detection and prevention.
- Wazuh – For Security Information and Event Management (SIEM).
- Cilium – For network micro-segmentation and access control.
- pfSense – For firewall configuration and controlling ingress/egress traffic.

2.2 Implementation Steps:

Identity and Access Management (IAM)

- Install announcement and Microsoft Entra to polarize stoner authentication and authorization.
- Enable Multi-Factor Authentication (MFA) for fresh security during login. o Define stoner places and warrants to apply the least honor access model.

Network Segmentation

- Implement Cilium to produce micro-segmentation within the network.
- Divide the network into distinct zones, similar as Internal, External, and Cloud, each with acclimatized access programs.

Monitoring and trouble Discovery

- Deploy Suricata at crucial network points (e.g., edge, garçon clusters) to descry suspicious conditioning like unauthorized access or malware. Configure Wazuh to collect logs from bias, waiters, and security events.
- Integrate Wazuh with announcement and Microsoft Entra to log authentication and authorization events.

Firewall Configuration

- Use pfSense to configure grainy firewall rules for controlling business between network parts.
- Produce access control programs to ensure that only authorized druggies and bias can pierce critical coffers.

Chapter 3

System Implementation

3.1 Install and Configure Active Directory and Microsoft Entra for Identity Management

To begin setting up identity management, you'll first need to install Active Directory Domain Services (AD DS). The steps below guide you through installing AD DS using the Server Manager graphical interface, either locally or remotely.

3.1.1 Installing Active Directory Domain Services via Server Manager:

- Open Server Manager, click Manage, and then choose Add Roles and Features to launch the wizard.
- On the Before You Begin page, click Next.
- On the Select Installation Type page, choose Role-based or feature-based installation, then click Next.
- On the Select Destination Server page, pick the server from the pool where AD DS will be installed, then click Next.

Note: If you're installing on a remote server, make sure you've created a server pool and added the target server. For details, refer to the "Add Servers to Server Manager" documentation.

- On the Select Server Roles page, check Active Directory Domain Services. When prompted by the dialog box, click Add Features, then continue by clicking Next.
- On the Select Features page, you can optionally select additional features if needed, then click Next.
- On the AD DS Overview page, review the role details, then click Next.
- On the Confirm Installation Selections page, click Install to begin the installation process.
- Once installation is complete, on the Results page, click Promote this server to a domain controller to proceed with the Active Directory configuration.

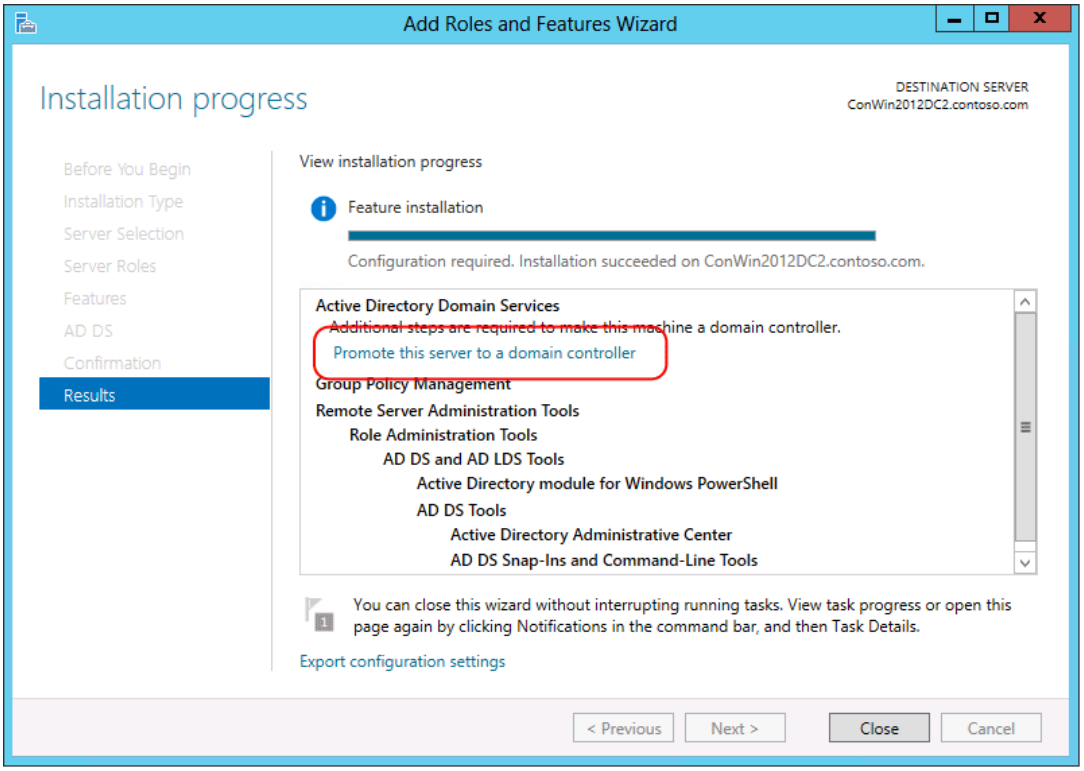

Figure 3.1: Install Active Directory Domain Services

Important: Suppose you accidentally close the Add Roles and Features Wizard before completing the setup. In that case, you can resume configuration anytime by going to Server Manager, selecting Tasks, and choosing Promote this server to a domain controller.

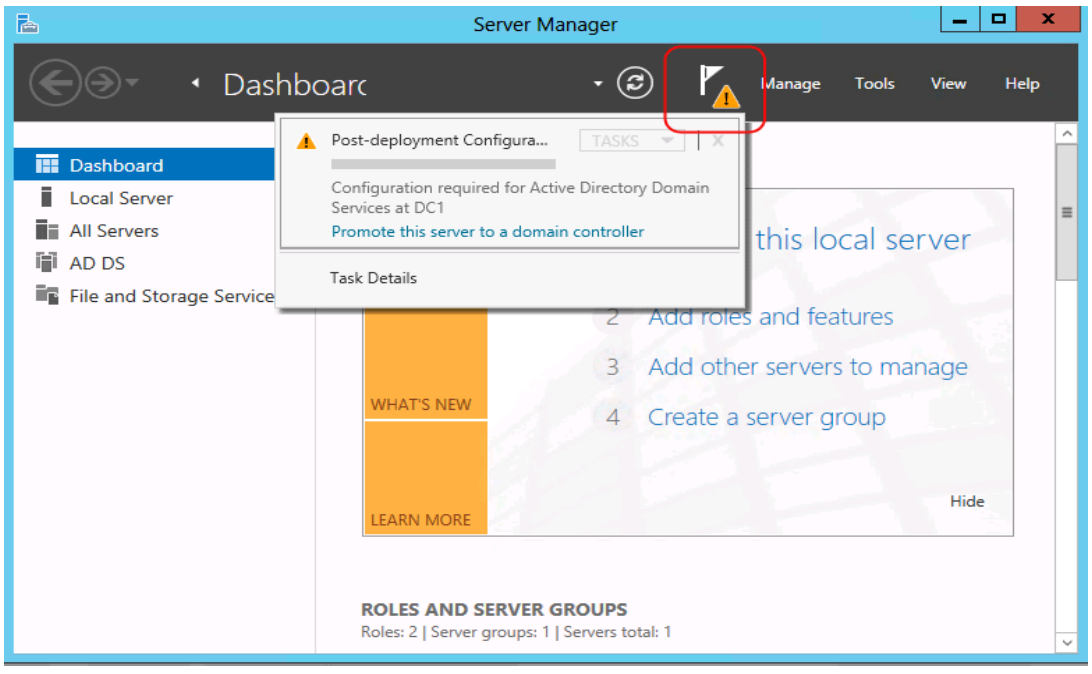

Figure 3.2: Promote Active Directory Server

3.1.2 Deployment Configuration

On the Deployment Configuration page, choose the appropriate option based on the scenario:

- Adding a Domain Controller to an Existing Domain Select "Add a domain controller to an existing domain", then enter the domain name (e.g., emea.corp.cloudbd24.net) or click Select... to browse for it. Provide credentials with Domain Admins privileges. If the server is already joined to the domain and you're doing a local install, the domain name and credentials may be auto-filled.
- Note: If you're installing Active Directory Domain Services (AD DS) on a remote server, you must manually provide credentials. If your current login lacks the necessary permissions, click Change... to specify different credentials.
- Creating a New Child Domain Choose "Add a new domain to an existing forest", set the domain type to Child Domain, then enter the parent domain (e.g., corp.cloudbd24.net) and the name of the new child domain. Provide credentials that have permission to create the new domain.
- Creating a New Domain Tree Choose "Add a new domain to an existing forest", set the domain type to Tree Domain, then enter the existing root domain (e.g., corp.cloudbd24.net) and the DNS name of the new domain (e.g., fabrikam.com). Provide the necessary credentials and continue.
- Creating a New Forest Select "Add a new forest", then enter the name of the root domain (e.g., corp.cloudbd24.net).

3.1.3 Domain Controller Options

- On the Domain Controller Options page, make the following selections based on your configuration:
- For a New Forest or Domain, choose the appropriate forest and domain functional levels, select the DNS server option, enter a password for Directory Services Restore Mode (DSRM), and proceed.
- For an Additional Domain Controller, select the roles you need, such as DNS server, Global Catalog (GC), or Read-Only Domain Controller (RODC). Choose the correct site name, enter the DSRM password, and click Next.

3.1.4 DNS Options

If you're installing the DNS Server role, the DNS Options page will appear:

- Choose whether to update the DNS delegation. If required, provide credentials with permission to modify delegation records in the parent DNS zone.
- If the system cannot reach the parent zone's DNS server, the update option will be disabled.

3.1.5: RODC Options

- If you're installing a Read-Only Domain Controller (RODC), the RODC Options page will be displayed:
- Specify a user or group responsible for managing the RODC.
- Add or remove accounts from the Allowed and Denied Password Replication Policy groups as needed, then click Next.

3.1.6: Additional Options

On the Additional Options page, make your selections based on the setup scenario:

- Creating a New Domain Enter a NetBIOS name for the new domain, or review the auto-generated name and confirm it. Then click Next.
- Adding a Domain Controller to an Existing Domain Select the domain controller you'd like to replicate from, or allow the wizard to automatically choose one. If you're using the Install from Media (IFM) method, select Install from media, specify the path to the backup media, and then click Next.

Note: You cannot use IFM to install the first domain controller in a domain. Also, IFM is not compatible across different Windows Server versions. To use IFM, the backup must be created on a domain controller running the same Windows Server version as the one you're installing.

3.1.7: Paths

On the Paths page, specify the file paths for the following components:

- Active Directory database
- Log files
- SYSVOL folder

Important: Avoid placing these files on volumes formatted with ReFS (Resilient File System), as it is not supported for Active Directory data.

3.1.8: Preparation Options

On the Preparation Options page, provide credentials that have the necessary permissions to run adprep. This step prepares the forest and domain for the new domain controller, especially if you're introducing a new version of Windows Server.

3.1.9: Review Options

On the Review Options page, go over your configuration selections. If you'd like to save these settings for future use or automation, click View Script to export the configuration as a Windows PowerShell script. Then select Next to continue.

3.1.10: Prerequisites Check

On the Prerequisites Check page, verify that all prerequisite checks have completed successfully. If everything is in order, click Install to begin the installation process.

3.1.11: Results

On the Results page, confirm that the server was successfully promoted to a domain controller. The system will automatically restart to complete the installation of Active Directory Domain Services (AD DS).

3.2 How to Create a New Tenant in Microsoft Entra ID

You can create and manage tenants directly from the Microsoft Entra admin center, provided your account meets the requirements.

Important: Only paid Microsoft Entra ID subscribers can create new tenants. Free or trial users won't see this option. To create a tenant, consider signing up for a free Azure account that supports it.

3.3 Why Create a New Tenant?

Creating a new tenant allows your organization to manage its own dedicated Microsoft Cloud environment, including users, apps, and services for both internal and external access.

3.4 Before You Begin

- If you're unable to create a Microsoft Entra ID or Azure AD B2C tenant, check the User Settings to ensure that tenant creation hasn't been restricted.
- Your account must be assigned the Tenant Creator role (at minimum) to successfully create a new tenant.
- This guide covers organizational tenets. For customer-facing applications, refer to Microsoft Entra External ID for Customer Identity and Access Management (CIAM) solutions.

3.5 Steps to Create a New Microsoft Entra Tenant

1. Sign in to the Azure portal.
2. From the left-hand menu, go to Microsoft Entra ID.
3. In the Overview section, select Manage tenants.
4. Click Create and follow the prompts to configure your new tenant.

Once complete, your new tenant will represent your organization and act as a standalone environment for managing identities, apps, and access policies.

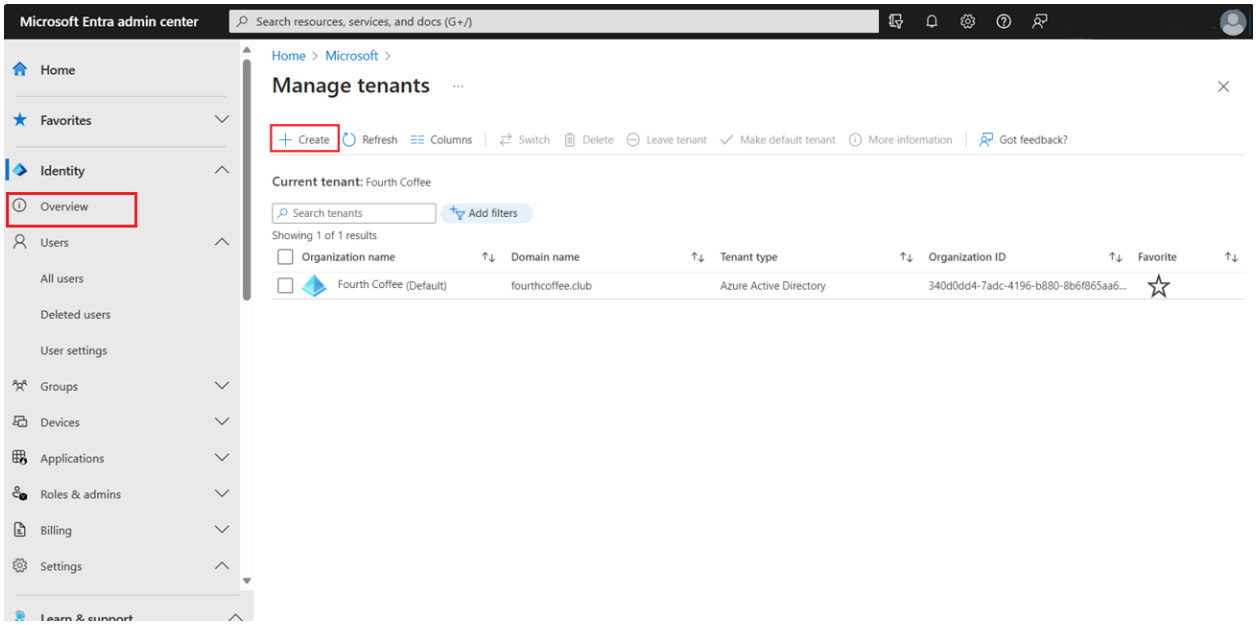

Figure 7.3: Create and Manage Tenants

5. Choose Tenant Type on the Basics tab, start by selecting the type of tenant you want to create:
    - Microsoft Entra ID – for organizational use
    - Microsoft Entra ID (B2C) – for customer-facing applications
6. Proceed to Configuration

    Click Next: Configuration to move to the next step.
7. Fill in Tenant Details
    On the Configuration tab, provide the required information to define your new tenant.

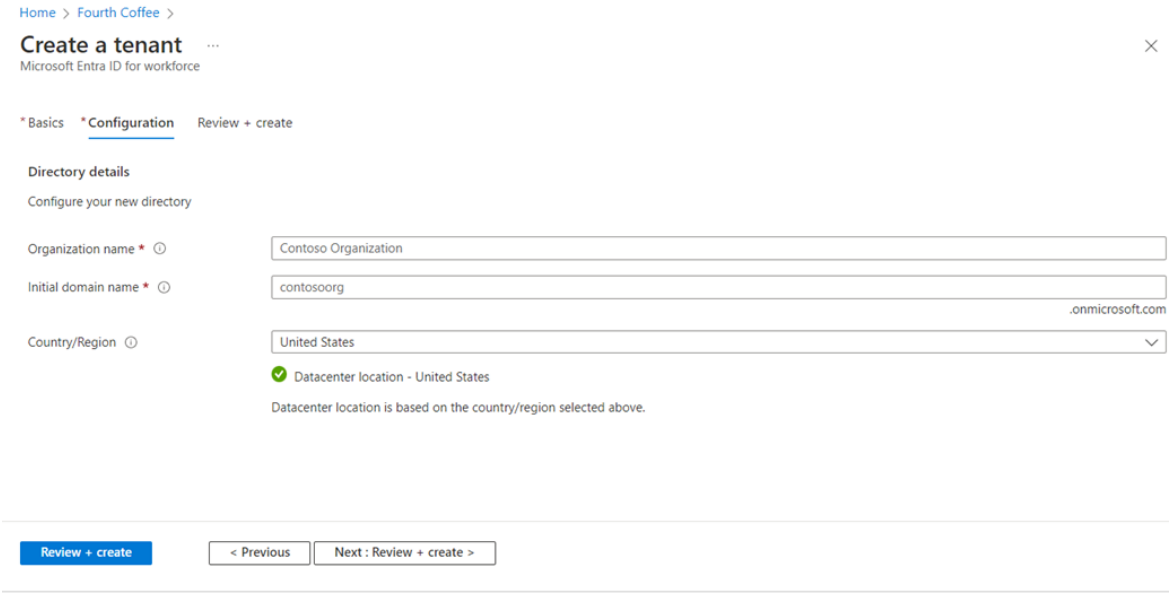

Figure 7.4: Create a Tenant from the Azure portal

- Enter the Organization Name
- Type your desired Organization name (for example, *Cloudbd24 Organization*) in the Organization name box.
- Enter the Initial Domain Name
  Type your preferred Initial domain name (*Cloudbd24org*) in the Initial domain name box.
- Select the Country/Region. Choose your desired Country/Region or leave the default option set to United States in the Country Region box.

2. Next: Review + Create

- Click Next: Review + Create to proceed.
- Review the information you've entered. If everything is correct, click Create in the lower-left corner to finalize the process.

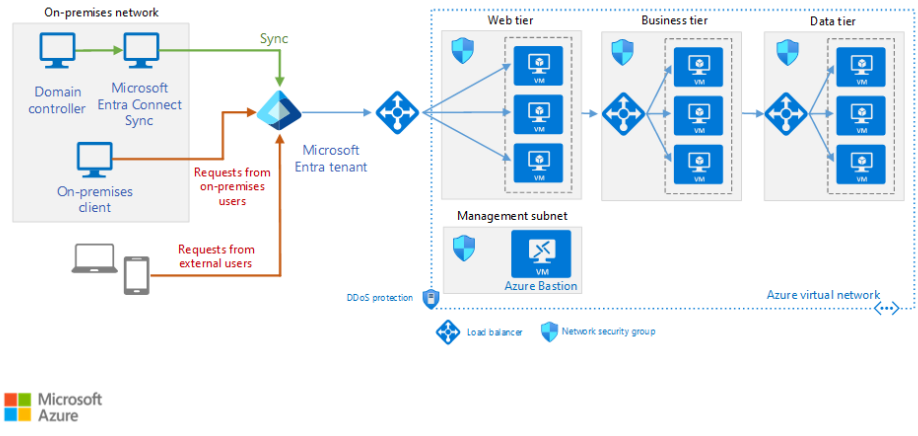

Figure 7.5: Integrate Active Directory Domain Service with Microsoft Entra

To begin the integration between our on-premises AD DS and Microsoft Entra ID, we first need to prepare the Microsoft Entra ID environment. This involves setting up a custom domain and configuring an account with the necessary administrative privileges.

3.6 Objectives:

1. Add a custom domain name in Azure.
2. Create a user account with the Global Administrator role.
3. Update the password for the Global Administrator account.

3.7 Add a Custom Domain in Azure

1. On the AD machine, launch Microsoft Edge and navigate to the Azure portal.
2. Sign in using the credentials provided by your instructor.
3. In the portal, go to Microsoft Entra ID from the navigation pane.
4. Under the Custom domain names section, click to add a new domain and enter: cloudbd24.net.
5. Review the DNS record types typically used for domain verification, but do not proceed with verification at this stage.

Note: In a real-world setup, DNS records are used to verify domain ownership. However, this lab environment does not require domain verification, so you can skip that step.

3.8 Create a Global Administrator User

1. On the AD machine, using the open Microsoft Edge window displaying the Microsoft Entra ID portal, navigate to the All Users section.
2. Create a new user with the following details:

    - Username: admin

    Make sure the domain selected in the username dropdown is the default one ending with.onmicrosoft.com

    - Name: admin
    - Role: Assign the Global Administrator role.
    - Password: Choose to use the autogenerated password.

    Click “Show Password” to view and record it—you’ll need this later in the lab.

3.9 Update the Global Administrator Password

1. Sign out from the Azure portal.
2. Log back in using the admin account created in the previous task.
3. When prompted, change the password to a new, secure one.

Be sure to write down the new password—it will be used again later in the lab.

3.10 Preparing On-Premises AD DS for Microsoft Entra ID Integration

3.10.1 Scenario:

To ensure a smooth integration between our on-premises Active Directory and Microsoft Entra ID, we need to verify that the environment is properly configured. We'll use the IdFix tool to detect and correct directory issues and align user UPNs with the custom domain name in Microsoft Entra ID.

3.10.2 Objectives:

1. Install the IdFix tool.
2. Run IdFix to identify any inconsistencies.

3.11 Install the IdFix Tool

1. On the AD machine, open Microsoft Edge and visit the official IdFix page at: https://github.com/microsoft/idfix
2. On the GitHub page, locate the ClickOnce Launch section and select Launch to install the tool.

Task 1: Accept the IdFix Privacy Statement

1. When the IdFix Privacy Statement dialog box appears, take a moment to read the disclaimer.
2. Once reviewed, click OK to proceed.

3.11.1 Run IdFix

1. In the IdFix tool window, click Query to scan your on-premises Active Directory for issues.
2. Review the list of directory entries returned. Focus on the ERROR and ATTRIBUTE columns to identify problems.

    - ✓ In this lab scenario, you'll notice that the displayName attribute for the Cloudbd24Admin account is missing. The recommended fix will appear in the UPDATE column.

3. From the ACTION drop-down list, select Edit, then click Apply to implement the recommended corrections.
4. In the confirmation dialog box labeled Apply Pending, choose Yes, then close the IdFix application.

3.12 Installing and Configuring Microsoft Entra Connect

3.12.1 Scenario:

We're now ready to complete the integration process by installing Microsoft Entra Connect on the AD server. This tool links our on-premises AD DS with Microsoft Entra ID, enabling directory synchronization.

3.12.2 Objective:

Download, install, and configure Microsoft Entra Connect.

3.12.3 Set Up Microsoft Entra Connect

- On the AD machine, return to the Azure portal using Microsoft Edge.
- From the Microsoft Entra ID page, navigate to the Microsoft Entra Connect section.
- Click Download to get the Entra Connect installation file.
- Launch the installer. On the first screen, accept the license terms and privacy notice, then click Continue.
- When prompted, choose Use express settings for a streamlined configuration.
- On the Connect to Microsoft Entra ID page, sign in with the Global Administrator account created earlier in Exercise.
- On the Connect to AD DS page, provide the following credentials:
    - ✓ Username: C24\Administrator
    - ✓ Password: Pa55w.rd
- On the Microsoft Entra ID Sign-in Configuration page, verify that your custom domain (e.g., cloudbd24.net) appears under the Active Directory UPN suffixes.
- Check the box labeled Continue without matching all UPN suffixes to verified domains, then proceed.

3.13 Verifying the Integration

3.13.1 Scenario:

With Microsoft Entra Connect now configured, we'll validate that synchronization between the on-premises AD DS and Microsoft Entra ID is working correctly. We'll do this by modifying and creating user accounts and checking if those changes sync to the cloud.

3.14 Key Tasks:

- Check synchronization status in the Azure portal.
- Review synchronization logs using the Synchronization Service Manager.
- Modify an existing user in Active Directory.
- Create a new user in Active Directory and confirm it appears in Microsoft Entra ID.
- Sync changes to Microsoft Entra ID

3.15 Confirm Synchronization via Azure Portal

- On the Active Directory (AD) server, open the Microsoft Edge browser where the Azure portal is already open.
- Refresh the Microsoft Entra Connect page and review the details under Provision from Active Directory.
- Navigate to Microsoft Entra ID > Users.
- Check the list of users to confirm that they have been synchronized from Active Directory.
- Next, go to the Groups section from the Entra ID navigation pane.
- Review the list of synchronized groups from Active Directory.

3.16 Confirm Synchronization via Synchronization Service Manager

- On the AD server, open the Start menu, expand Microsoft Entra Connect, and select Synchronization Service.
- In the Synchronization Service Manager, go to the Operations tab to review recent synchronization tasks.
- Open the Connectors tab and observe the two connectors:
  - ✓ One for Active Directory Domain Services (AD DS)
  - ✓ One for the Microsoft Entra tenant
- Close the Synchronization Service Manager when done.

3.17 Update a User Account in Active Directory

- On the AD server, launch Active Directory Users and Computers from Server Manager.
- Expand the Sales Organizational Unit (OU), then locate and right-click on Sumesh Rajan to open the Properties window.
- Select the Organization tab.
- In the Job Title field, enter: Manager, then click OK to save changes.

3.18 Create a New User in Active Directory

Create a new user in the **Sales OU** with the following details:

- First name: Jordan
- Last name: Mitchell
- User logon name: Jordan
- Password: Pa55w.rd

3.19 Manually Trigger Synchronization to Microsoft Entra ID

- On the AD server, open Windows PowerShell as an Administrator.
- In the PowerShell console, run the following command to start a synchronization cycle:

```
Start-ADSyncSyncCycle
```

```
Start-ADSyncSyncCycle -PolicyType Delta
```

3.20 Verify Synced Changes in Microsoft Entra ID

- On the AD server, return to the Microsoft Edge browser and navigate to the Microsoft Entra ID page.
- Go to Users > All Users and search for Sumesh.
- Open Sumesh Rajan's profile and verify that the Job Title field now shows "Manager", confirming that the update was successfully synced.
- In Microsoft Edge, go back to the All-Users page.
- On the All-Users page, search for the user Jordan.
- Open the properties page of the user Jordan Mitchell, and then review the attributes of the user account that have been synced from Active Directory.

3.21 Network Segmentation with Cilium

- Installation: Install Cilium using the following commands (for Linux-based systems):

curl -sSL https://github.com/cilium/cilium-cli/releases/download/v0.10.0/cilium-linux-amd64.tar.gz | tar -xzv

sudo mv cilium /usr/local/bin

- Deploy Cilium: Deploy Cilium in our Kubernetes or Docker environment:

Bash

kubectl create -f https://raw.githubusercontent.com/cilium/cilium/master/install/kubernetes/quick-install.yaml

1. Ensure that Cilium is installed correctly by checking the pods:

kubectl get pods -n kube-system

2. Define Network Policies: Define access control policies between different microservices, applications, or users. For example:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
 name: allow-app-traffic
spec:
 podSelector:
  matchLabels:
   app: app-name
 ingress:
  - from:
   - podSelector:
      matchLabels:
       app: authorized-app
```

3.22 Install and Configure Suricata for Intrusion Detection

- Installation:

Suricata can be installed on Linux or Windows using package managers.

For Ubuntu/Debian:
sudo apt update
sudo apt install suricata

For CentOS:
sudo yum install suricata

- Configuration:
  - ✓ Edit the Suricata configuration file (/etc/suricata/suricata.yaml) to define our network interfaces and rules.
  - ✓ Enable IDS (Intrusion Detection System) mode and configure the logging options.
- Starting Suricata:
  1. Start Suricata and check the logs:

sudo systemctl start suricata

sudo systemctl enable suricata

  2. Verify the Suricata process:

sudo suricata –

- Custom Rules:
  - ✓ Create and update custom Suricata rules for specific traffic patterns and attacks.
  - ✓ For example, add the following rule to detect suspicious traffic:

alert ip any any -> any any (msg:"Suspicious traffic detected"; sid:1000001;)

- Monitoring:
  3. Suricata generates alert logs that can be forwarded to Wazuh for centralized logging and real-time monitoring.

3.23 SIEM Configuration with Wazuh

- Install Wazuh:
    1. Install Wazuh manager and agents on our network.
        1. For Ubuntu/Debian systems: sudo apt update
           sudo apt install wazuh-manager
- Configure Wazuh Manager:
    2. Edit the configuration file (/var/ossec/etc/ossec.conf) to define the connection between Wazuh manager and agents.
    3. Specify the log sources and enable integration with AD and Microsoft Entra for authentication logs.
- Deploy Wazuh Agents:
    4. Install Wazuh agents on endpoints (servers, workstations).
    5. Configure the agent to send security logs to the Wazuh manager for processing.
- Real-Time Alerts:
    6. Set up real-time alerting by configuring custom rules or utilizing pre-built Wazuh rules for monitoring security events.
    7. Example: Detect failed login attempts in AD and Microsoft Entra and trigger an alert in Wazuh.

3.24 Install and Configure pfSense for Firewall

- Installation:
    1. Install pfSense on a dedicated VM or hardware. Follow the pfSense installation guide to set it up.
- Initial Setup:
    2. Access pfSense via the web interface (https://<pfsense-ip>/).
    3. Configure network interfaces, including the WAN and LAN interfaces.
- Define Firewall Rules:
    4. Create firewall rules to control the traffic between different segments:
        - ✓ Allow traffic from the Internal network to Cloud.

- ✓ Block traffic from External users to the Internal network unless authenticated.

5. Example rule:

Action: Pass

Interface: LAN

Source: Internal Network

Destination: Cloud Server

Protocol: TCP

Port: 443

- VPN Configuration:

6. Set up VPN (e.g., IPsec or OpenVPN) on pfSense for secure remote access.
7. Configure MFA for users connecting via VPN to ensure secure access.

3.24 Testing and Evaluation

3.24.1 Authentication and Access Control:

- Test authentication with AD and Microsoft Entra, ensuring that only authenticated users can access the network and resources.
- Test that MFA is enforced for users accessing critical services.

3.24.2 Suricata and Wazuh Monitoring:

1. Simulate a security attack (e.g., port scanning or brute force login) and check if Suricata detects the intrusion.
2. Confirm that Wazuh generates alerts for the detected attack.

3.24.3 Firewall Testing:

1. Test access between segments by attempting to access resources from restricted networks.
2. Confirm that pfSense firewall rules are blocking unauthorized traffic.

Chapter 4

Results and Discussion

4.1 Authentication and Access Control

Integrating Active Directory (AD) and Microsoft Entra for identity management proved highly effective. By centralizing authentication and enforcing Multi-Factor Authentication (MFA), we ensured that only authorized users could access network resources. The synchronization between AD and Microsoft Entra was seamless, providing a unified identity management system.

Key Findings: Seamless Synchronization: AD and Microsoft Entra sync flawlessly, ensuring consistent user identity across the network.

Enhanced Security: MFA added an extra layer of security, significantly reducing the risk of unauthorized access.

4.2 Network Segmentation

We deployed Cilium to enforce network segmentation, effectively limiting lateral movement within the network. By creating distinct network zones and applying tailored access policies, we minimized the potential attack surface.

Key Findings: Effective Segmentation: Cilium successfully segmented the network, isolating critical resources and reducing the risk of internal threats.

Controlled Access: Access policies were enforced based on user roles, ensuring that users only had access to necessary resources.

4.3 Real-Time Monitoring and Threat Detection

Suricata and Wazuh were instrumental in providing real-time monitoring and alerting. Suricata detected suspicious activities at the network level, while Wazuh centralized log management and generated alerts for unauthorized access attempts.

Key Findings: Proactive Detection: Suricata effectively identified potential threats, such as unauthorized access attempts and malware.

Centralized Monitoring: Wazuh provided a comprehensive view of security events, enabling quick response to incidents.

4.4 Firewall Enforcement

We used pfSense to enforce firewall rules, blocking unauthorized access between network segments. This further strengthened the Zero Trust security model by ensuring that only authenticated and authorized traffic could traverse the network.

Key Findings: Robust Firewall Policies: pfSense effectively managed traffic between network segments, preventing unauthorized access.

Enhanced Security Posture: The combination of firewall rules and network segmentation significantly improved the overall security of the network.

4.5 Overall Impact

The implementation of the Zero Trust Network has transformed our approach to network security. By adopting a "never trust, always verify" mindset, we have created a more resilient and secure network environment. The integration of various open-source tools has demonstrated that a robust Zero Trust architecture can be achieved without relying on proprietary solutions.

Key Findings: Improved Security: The Zero Trust model has significantly reduced the risk of both internal and external threats.

Scalability: The use of open-source tools provides flexibility and scalability, allowing the solution to grow with the organization.

4.7 Discussion

The results of this project validate the effectiveness of the Zero Trust Network in enhancing enterprise security. The seamless integration of identity management, network segmentation, real-time monitoring, and firewall enforcement has created a comprehensive security framework.

Key Insights:

Holistic Security Approach: The Zero Trust model addresses security at multiple layers, providing a comprehensive defense strategy.

Future Enhancements: Incorporating AI/ML and expanding to multi-cloud environments can further enhance the security and scalability of the solution.

Chapter 5

Recommendation and Future Work

5.1 Recommendations

Drawing from the insights and practical implementations discussed in this thesis, the following key recommendations are presented to support and advance Zero Trust adoption across enterprise environments.

- ✓ Routine Policy Audits and Updates: Regularly review security policies and access controls to keep Zero Trust aligned with evolving threats and organizational changes.

- ✓ Extending Zero Trust to Third Parties: Apply strict access controls and continuous verification to contractors, vendors, and remote partners to minimize external risks.

- ✓ Investing in Continuous User Awareness: Provide ongoing, role-based training to help employees understand Zero Trust principles, spot phishing, and protect credentials.

- ✓ Incorporating AI-Driven Threat Detection: Use AI and machine learning for real-time threat detection, anomaly identification, and automated response to enhance adaptive trust.

5.2 Future Work

The Zero Trust model is continuously evolving. Several areas warrant further research and development:

- ✓ Securing IoT and Unmanaged Devices: Apply Zero Trust to IoT and BYOD by assigning identities, establishing behavioral baselines, and using micro-segmentation to reduce risk.

- ✓ Evaluating SASE (Secure Access Service Edge): Integrate Zero Trust with SASE to deliver scalable, cloud-native security and unified policy enforcement for distributed environments.

- ✓ Testing in Cloud-Native Environments: Implement Zero Trust in platforms like Kubernetes through service authentication, namespace isolation, and dynamic runtime policies.

Chapter 6

References

- NIST Special Publication 800-207: Zero Trust Architecture
- Forrester Research: "The Zero Trust Extended Enterprise"
- AD and Microsoft Entra Documentation
- Wazuh Documentation

Project Repository

The full source code, configuration scripts, documentation files, and additional resources related to this project are available in the following GitHub repository:

🔗 **GitHub Repository**: https://github.com/kh4649/implementing-zero-trust-network