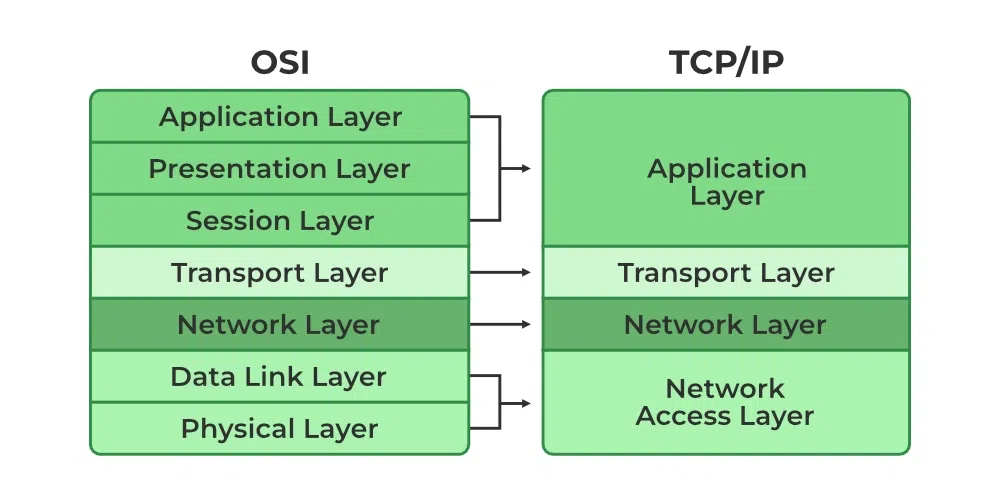


LAN Web Network -

This type of typology restricts operations to the Local Area Network though a centralized hub, in this case, its a network switch. Throught this network switch, an administrator the ability to enforce strict authentication and authorization of any network traffic that might come through the switch. It also allows the network to easily accommodate additional devices with minimal disruption since the devices cannot access each other directly. This also serves as a safety measure as any communication from devices within and outside of the network would have to go throught the network switch and its subsequent network rules.



Design Network Protocols and Architectures -

TCI/IP Has 4 layers - Application, transport, and network, and network access layer. Number one is the network switch and is incharge of the lowest layer, which is responsible for the physical transmission of data over the network. It handles how devices connect to the physical network and defines protocols like Ethernet or Wi-Fi. Number two is the router, which is responsible of the transport layer that does the logical addressing and routing data between devices on different networks.This includes IP address asisgnment to devices, packet fragmentation and reassembly, and defines protocols like IPv4, IPv6, and ICMP. Number three is the computer, which handles the network layer as it ensures the reliable or unreliable delivery of data between applications on devices. Lastly, number 4 is the actual network wires connecting the devices to the network itself. THis counds as the Network access layer that is in charge of handling communication between applications,and providing protocols and interfaces for data exchange.

Implement Network Security Fundamentals-

**Firewall Rule Implementation**

#### **Objective:**

To block unauthorized access to a specific port (Port 22 - SSH) from external sources while allowing internal communication.

#### **Configuration:**

* **Firewall Used**: pfSense
* **Rule Description**: Block all inbound traffic on port 22 from external IP addresses to prevent unauthorized SSH access.
* **Source**: ANY (0.0.0.0/0)
* **Destination**: 192.168.1.10 (Internal server IP)
* **Protocol**: TCP
* **Port**: 22
* **Action**: Block

#### **Steps:**

1. Accessed the pfSense web interface.
2. Navigated to **Firewall Rules** > **WAN**.
3. Created a new rule with the following:
   * **Action**: Block.
   * **Source**: Any.
   * **Destination**: Internal server (192.168.1.10).
   * **Protocol**: TCP.
   * **Port Range**: 22.
4. Saved and applied the rule.

### **Intrusion Detection System (IDS) Configuration**

#### **Objective:**

To detect port scanning attempts from external attackers using Snort.

#### **Configuration:**

* **IDS Tool**: Snort
* **Rule Description**: Detect and log TCP SYN packets from a single IP to multiple ports within a short timeframe.
* **Rule**: alert tcp any any -> any any (msg:"Port scan detected"; flags:S; threshold:type both, track by\_src, count 10, seconds 10; sid:1000001; rev:1;)

#### **Steps:**

1. Installed and configured Snort on a server running Ubuntu.
2. Created a custom rule in Snort to detect port scanning.
3. Enabled the rule and restarted Snort for the configuration to take effect.

#### **Evidence:**

Below is an example log entry generated by Snort:

yaml

CopyEdit

[\*\*] [1:1000001:1] Port scan detected [\*\*]

[Priority: 3]

Timestamp: 2025-01-27 10:15:30

Source IP: 203.0.113.45

Destination IP: 192.168.1.10

Ports Scanned: 22, 80, 443, 8080

#### **Impact:**

* Successfully detected and logged a port scanning event.

### **Intrusion Prevention System (IPS) Configuration**

#### **Objective:**

To prevent brute force login attempts targeting an internal web server using Suricata.

#### **Configuration:**

* **IPS Tool**: Suricata
* **Rule Description**: Block IP addresses with more than 5 failed login attempts within 1 minute.
* **Rule**: drop tcp any any -> 192.168.1.10 80 (msg:"Brute force login attempt detected"; flow:to\_server,established; content:"POST"; http\_client\_body; content:"login"; threshold:type both, track by\_src, count 5, seconds 60; sid:2000001; rev:1;)

#### **Steps:**

1. Installed Suricata on the same server as Snort.
2. Configured the rule to block traffic after repeated failed login attempts.
3. Verified the functionality by simulating failed login attempts using a testing tool.

#### **Evidence:**

Below is a log entry showing the blocked event:

yaml

CopyEdit

[\*\*] [1:2000001:1] Brute force login attempt detected [\*\*]

[Priority: 2]

Timestamp: 2025-01-27 10:30:15

Source IP: 203.0.113.55

Destination IP: 192.168.1.10

Blocked: Yes

#### **Impact:**

* Successfully blocked the IP address after detecting malicious activity.
* Prevented further brute force attempts.

Example of Detected Event

Event Description:

A port scan followed by a brute force attack was detected and mitigated.

Details:

Detected by IDS:

Snort detected a port scan originating from 203.0.113.45 at 10:15:30.

Logged the event with details on ports scanned.

Blocked by IPS:

Suricata detected multiple failed login attempts from the same source IP (203.0.113.55) at 10:30:15.

Automatically blocked the IP address, preventing further attempts.

Implement Access Control Measures-

**Access Control List (ACL) Configuration**

* **Objective**: Restrict web server access to the 192.168.1.0/24 subnet on Port 80.

**Rule**:  
arduino  
CopyEdit  
access-list ACL\_WEBSERVER permit tcp 192.168.1.0 255.255.255.0 any eq 80

access-list ACL\_WEBSERVER deny ip any any

* **Impact**: Ensures only trusted IPs can access the web server.

### **Access Control Model (DAC)**

* **Objective**: Apply user-defined permissions to a shared folder (\\Server01\SharedDocs).
* **Permissions**:
  + **User1**: Read-only.
  + **User2**: Full control.
  + **Group1**: Modify access.

**Impact**: Restricts access based on user needs, minimizing risk.

### **User Access Levels**

* **System**: CRM application.
* **Roles**:
  + **Admin**: Full control.
  + **Manager**: Edit and view records.
  + **Staff**: View records only.
* [admin@example.com](mailto:admin@example.com) - Admin Full control
* manager@example.com Manager Edit & View Records
* staff@example.com Staff View Records Only

### **Event Detection**

* **Event**: Unauthorized IP (10.0.0.55) attempted to access the web server.
* **Log Entry**:  
  csharp  
  CopyEdit  
  Deny tcp src 10.0.0.55/52000 dst 192.168.1.10/80 by ACL\_WEBSERVER

#### **Secure Wireless Networks - Network Details:**

* **SSID**: SecureNet-Office
* **Authentication Protocol**: WPA3-Personal
* **Encryption Method**: AES-GCMP
* **Pre-shared Key (PSK)**: Secure@2025!

#### **Configuration Steps:**

1. Logged into the wireless router interface at 192.168.1.1.
2. Navigated to **Wireless Settings** → **Security Options**.
3. Selected **WPA3-Personal** for the SSID SecureNet-Office.
4. Set the encryption to **AES-GCMP** and created a strong PSK: Secure@2025!.
5. Saved the configuration and tested the connection.

#### **WIPS Configuration:**

* **WIPS Tool**: Cisco Prime Infrastructure
* **Monitoring Scope**: All devices within the range of SecureNet-Office.
* **Policies**:
  + Detect and block rogue APs.
  + Alert and log MAC address spoofing attempts.
  + Disable devices attempting deauthentication attacks.

#### **Steps:**

1. Configured WIPS to monitor the SSID SecureNet-Office and log unauthorized device activity.
2. Set up automatic blocking of rogue access points and devices with spoofed MAC addresses.
3. Enabled email alerts for critical events.

#### **Tools Used:**

* **SIEM Tool**: Splunk
* **IDS/IPS**: Snort
* **Firewall**: Cisco ASA

#### **Monitor and Respond to Network Security Events -**

#### **Monitoring Scope:**

* Monitored traffic on the internal network (192.168.1.0/24) for unusual patterns, unauthorized access attempts, and potential breaches.