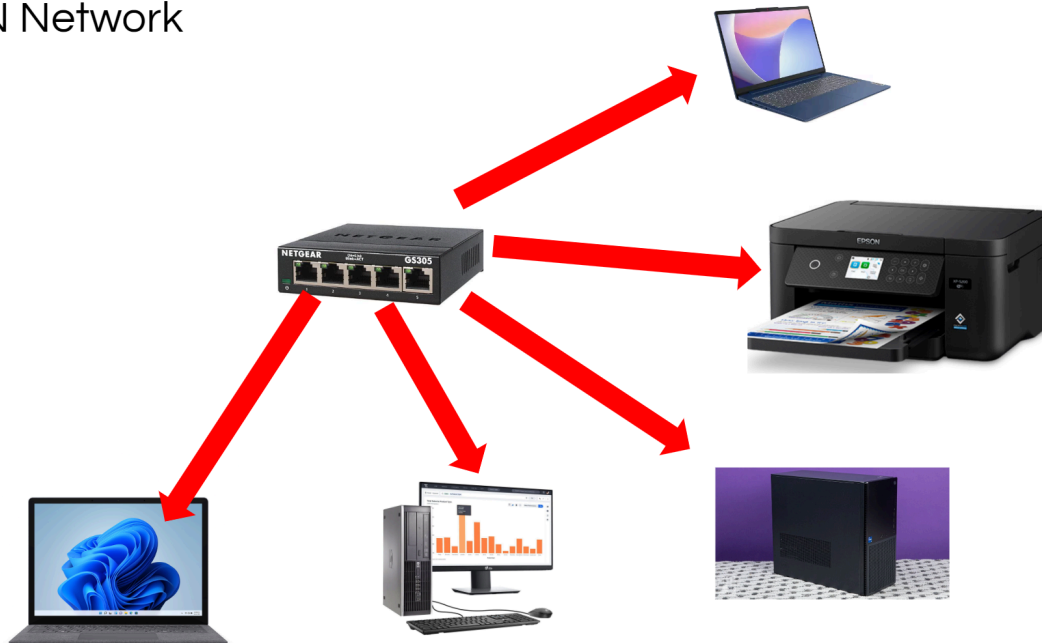


Network Topology

LAN Network

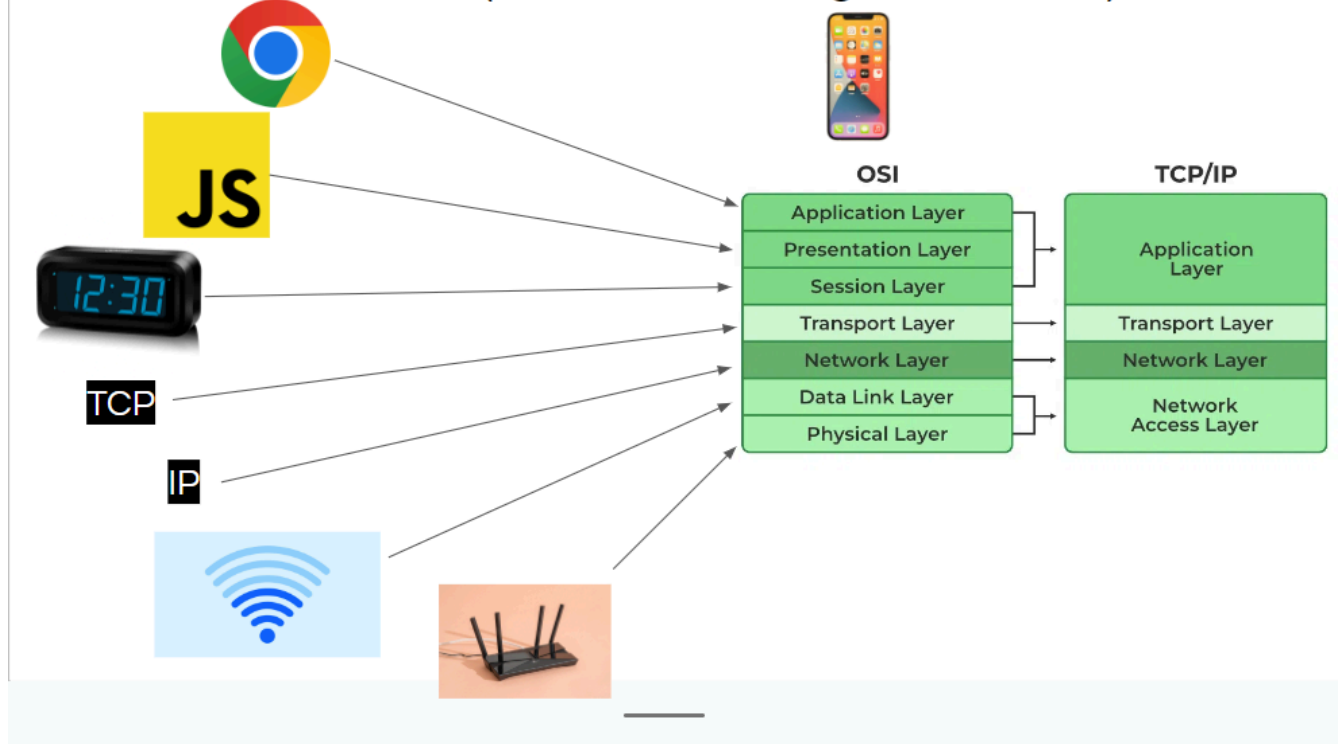


How This Topology Supports Network Management -

In this topology, a managed switch is being used to manage all of the devices contained within the LAN network. Managed switches are commonly used to enable centralized configuration, monitoring, and device management. An admin of this network is able to remotely control devices, send files, and distribute commands to the devices connected to this network. This network allows traffic monitoring, which enables secure communication within devices through early detection and troubleshooting.

Network Protocols and Architectures

OSI & TCP/IP Model (Phone Accessing the Internet)



Subnetting

Network Address: 172.25.144.0/21

Host Count: 50

Subnet Mask: /21 = 255.255.248.0

New Subnet Mask: /26 = 255.255.255.192

Subnet Range: 172.25.146.192 - 172.25.146.255

Network Address: 172.25.146.192

Broadcast Address: 172.25.146.255

Implement Network Security Fundamentals

Firewall Rule

Goal: Using Next-Generation Firewall, completely block access to X across this network.

Action: Deny

Protocol: Any

Source IP: 192.168.1.0/24 (Random IP)

Source Port: Any

Destination IP: 199.16.156.0/22

Destination Port: 80 or 443

IDS Configuration

Traffic Type: TCP

Source Port: 104.244.46.0/24

Destination Port: 104.244.46.0/24

Action: Creates an alert when traffic is detected on the X IP range

Message: “X Access Detected” is logged

IPS Configuration

Traffic Type: TCP

Source Port: 104.244.46.0/24

Destination Port: 104.244.46.0/24

Action: Blocks packets, preventing connection

Detected Event Example

IDS Example:

Twitter Access Detected - Source: 192.168.1.100 Destination: 8.25.194.20 Port: 443

IPS Example

Twitter Traffic Blocked - Source: 192.168.1.100 Destination: 8.25.194.20 Port: 443

Access Control Measures

ACL Configuration

Device: Proxy Server

Protocol: HTTPS

Requirement: Filter traffic based on website/app certificate validation status

- 1) Enable SSL Certificate inspection/validation on the proxy server
- 2) Allow website with valid certificates
- 3) Deny websites with expired, untrusted, or unknown certificates

Access Control Model

Discretionary Access Control (DAC)

Access Control to Information: Through company ownership

Flexibility for Accessing Information: High

Access Complexity: Very Complex

Support for Multilevel Database System: No

System: Unix Based Systems

Steps

- For both Windows and Unix systems
- Restrict users from disabling SSL validation in their browsers
- Enforce SSL/TLS validation to prevent certificate warning from being ignored
- Create group policy for all machines

User Access Level

Employees

- Employees are limited to website with valid SSL/TLS Certificates
- Attempts to access untrusted websites are automatically blocked
- Employees log in through Single Sign-On using Google Workspace
- SSO Enforces strict certificate validation for accessing services and websites
- Access to resources are managed centrally
- All SSO login attempts are logged in a central location

Admins

- Admins are granted access to all websites
- Admins are allowed to bypass standard web filtering rules
- Must provide justification however
- Access to dangerous websites are automatically logged and reviewed
- Admin access is constantly monitored
- All activity are logged for maintaining accountability
- Admins authenticate via a different SSO System than employees
- Admins are required to use multiple types of MFA
- Some options include (Biometrics, Pins, Devices, Notifications)

Secure Wireless Networks

WPA 3 Configuration

Network SSID: Billyboy

Passphrase: S3cure@Net!2024

Firmware: Pfsense Firewall

Authentication Protocol: WPA3

Encryption Method: AES-GCMP/ AES - CCMP

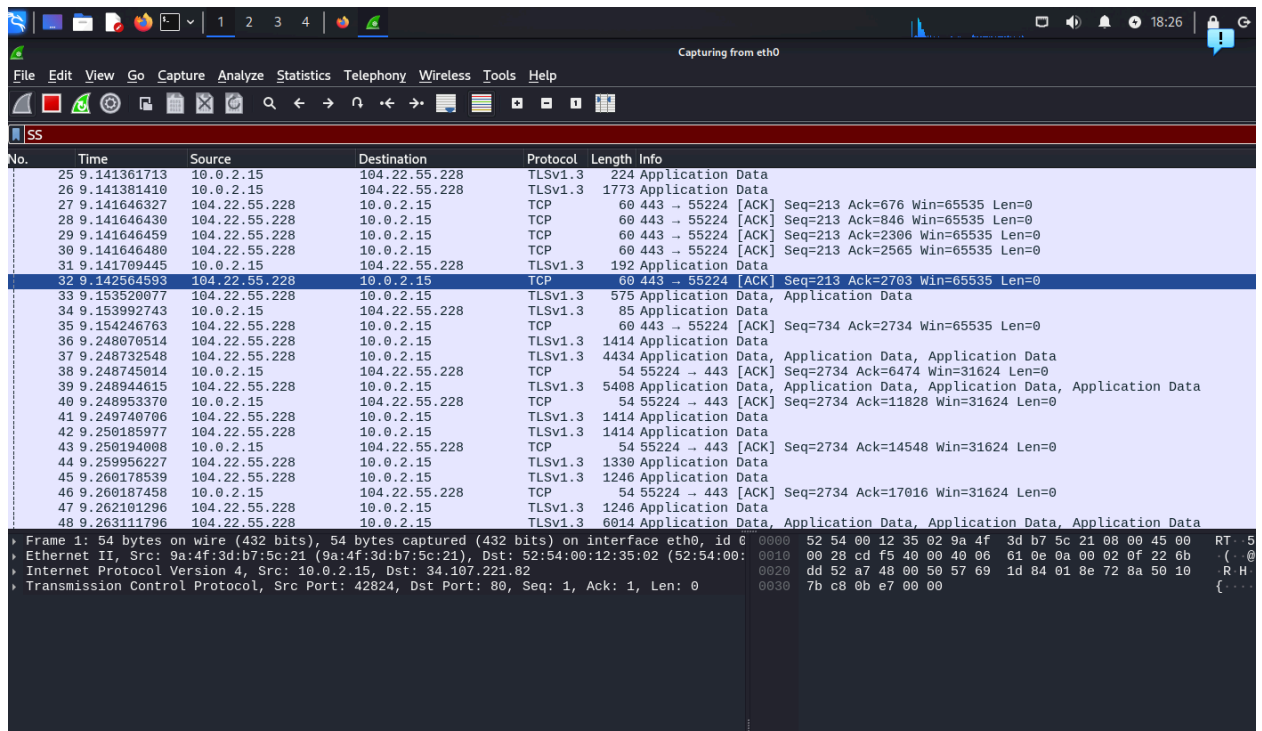
Disable WPA2 to ensure WPA 3 works properly on the router

Wireless Intrusion Prevention System (WIPS) Configuration

- Set monitoring policies
- Block rogue access points
- Create a whitelist of authorized MAC addressed in a given network
- Detect and block attacks
- Enable detection for DoS attacks
- Set email alerts for unauthorized access attempts
- Keep logs in a centralized location

Utilize Network Security Tools

Wireshark Capture



The image shows a Wireshark network capture interface. The top bar indicates 'Capturing on eth0'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The main window displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packet list shows a series of TCP and TLSv1.3 packets between 10.0.2.15 and 104.22.55.228. The details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet data is displayed in hexadecimal and ASCII format.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------|---------------|----------|--------|--|
| 25 | 9.141361713 | 10.0.2.15 | 104.22.55.228 | TLSv1.3 | 224 | Application Data |
| 26 | 9.141381410 | 10.0.2.15 | 104.22.55.228 | TLSv1.3 | 1773 | Application Data |
| 27 | 9.141646327 | 104.22.55.228 | 10.0.2.15 | TCP | 60 | 443 → 55224 [ACK] Seq=213 Ack=676 Win=65535 Len=0 |
| 28 | 9.141646430 | 104.22.55.228 | 10.0.2.15 | TCP | 60 | 443 → 55224 [ACK] Seq=213 Ack=846 Win=65535 Len=0 |
| 29 | 9.141646459 | 104.22.55.228 | 10.0.2.15 | TCP | 60 | 443 → 55224 [ACK] Seq=213 Ack=2306 Win=65535 Len=0 |
| 30 | 9.141646480 | 104.22.55.228 | 10.0.2.15 | TCP | 60 | 443 → 55224 [ACK] Seq=213 Ack=2565 Win=65535 Len=0 |
| 31 | 9.141709445 | 10.0.2.15 | 104.22.55.228 | TLSv1.3 | 192 | Application Data |
| 32 | 9.142564593 | 104.22.55.228 | 10.0.2.15 | TCP | 60 | 443 → 55224 [ACK] Seq=213 Ack=2703 Win=65535 Len=0 |
| 33 | 9.153520677 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 575 | Application Data, Application Data |
| 34 | 9.153992743 | 10.0.2.15 | 104.22.55.228 | TLSv1.3 | 85 | Application Data |
| 35 | 9.154246763 | 104.22.55.228 | 10.0.2.15 | TCP | 60 | 443 → 55224 [ACK] Seq=734 Ack=2734 Win=65535 Len=0 |
| 36 | 9.248070514 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 1414 | Application Data |
| 37 | 9.248732548 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 4434 | Application Data, Application Data, Application Data |
| 38 | 9.248745014 | 10.0.2.15 | 104.22.55.228 | TCP | 54 | 55224 → 443 [ACK] Seq=2734 Ack=6474 Win=31624 Len=0 |
| 39 | 9.248944615 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 5408 | Application Data, Application Data, Application Data, Application Data |
| 40 | 9.248953370 | 10.0.2.15 | 104.22.55.228 | TCP | 54 | 55224 → 443 [ACK] Seq=2734 Ack=11828 Win=31624 Len=0 |
| 41 | 9.249740706 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 1414 | Application Data |
| 42 | 9.250185977 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 1414 | Application Data |
| 43 | 9.250194008 | 10.0.2.15 | 104.22.55.228 | TCP | 54 | 55224 → 443 [ACK] Seq=2734 Ack=14548 Win=31624 Len=0 |
| 44 | 9.250956227 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 1330 | Application Data |
| 45 | 9.260178539 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 1246 | Application Data |
| 46 | 9.260187458 | 10.0.2.15 | 104.22.55.228 | TCP | 54 | 55224 → 443 [ACK] Seq=2734 Ack=17016 Win=31624 Len=0 |
| 47 | 9.262101296 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 1246 | Application Data |
| 48 | 9.263111796 | 104.22.55.228 | 10.0.2.15 | TLSv1.3 | 6014 | Application Data, Application Data, Application Data, Application Data |

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 9a:4f:3d:b7:5c:21 (9a:4f:3d:b7:5c:21), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 42824, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Vulnerability Scanner Report

```
(test@Test)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.138.16.223 netmask 255.255.255.0 broadcast 10.138.16.255
    inet6 fe80::a00:27ff:fe61:2b61 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:61:2b:61 txqueuelen 1000 (Ethernet)
    RX packets 15 bytes 4972 (4.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 6758 (6.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(test@Test)-[~]
$ nmap -sV --script=vuln 10.138.16.223
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 15:52 EST
Stats: 0:00:19 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 83.33% done; ETC: 15:52 (0:00:04 remaining)
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.138.16.223
Host is up (0.000071s latency).
All 1000 scanned ports on 10.138.16.223 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.35 seconds
```

Network Penetration Testing Tool

```
(test@test)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.8.105 netmask 255.255.255.0 broadcast 192.168.8.255
    inet6 fe80::a00:27ff:fe5d:d4d7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:5d:d4:d7 txqueuelen 1000 (Ethernet)
    RX packets 954 bytes 59579 (58.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1515 bytes 93602 (91.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(test@test)-[~]
$ sudo nmap -sn 192.168.8.105/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 18:45 EST

Nmap scan report for Pixel-6.lan (192.168.8.133)
Host is up (0.18s latency).
```

Monitor and Respond to Network Security Events

Logs

Firewall log Snippet

[2025-01-22 10:30:12] SRC=192.168.1.105 DST=192.168.1.10 PROTO=TCP DPT=22
ACTION=ACCEPT
[2025-01-22 10:30:15] SRC=192.168.1.105 DST=192.168.1.10 PROTO=TCP DPT=22
ACTION=ACCEPT
[2025-01-22 10:31:01] SRC=192.168.1.105 DST=192.168.1.10 PROTO=TCP DPT=22
ACTION=BLOCK

IDS Alert Log

[2025-01-22 10:34:45] ALERT: Potential Brute Force Attack
SRC_IP: 192.168.1.105
DST_IP: 192.168.1.10
PORT: 22
COUNT: 15 attempts in 2 minutes

Authentication Attempts

Jan 22 10:30:12 server sshd[1234]: Failed password for invalid user admin from 192.168.1.105
port 54123 ssh2

Jan 22 10:30:15 server sshd[1234]: Failed password for invalid user root from 192.168.1.105 port 54124 ssh2

Jan 22 10:30:17 server sshd[1235]: Failed password for invalid user test from 192.168.1.105 port 54125 ssh2

1.) Initial Detection

The IDS flagged a brute force attack targeting SSH on a critical server. The firewall log confirmed repeated connection attempts from 192.168.1.105.

2.) Immediate Actions

- Blocked the attacking IP address using the firewall:
`iptables -A INPUT -s 192.168.1.105 -j DROP`
- Disabled password-based SSH authentication on the server and enabled key-based authentication
`echo "PasswordAuthentication no" >> /etc/ssh/sshd_config`
`systemctl restart sshd`

3.) Investigation

- Reviewed logs to confirm no successful login occurred.
- Checked the server for any unauthorized changes or processes (none were found).
- Conducted a vulnerability scan to ensure the server was up to date.

4.) Remediation

- Updated SSH configurations to use a non-standard port and enabled two-factor authentication.
- Conducted a network-wide scan to identify other suspicious activities (none detected).

5.) Preventative Measures

- Deployed fail2ban to dynamically block IPs after multiple failed login attempts.
- Reviewed and hardened firewall rules for SSH traffic

