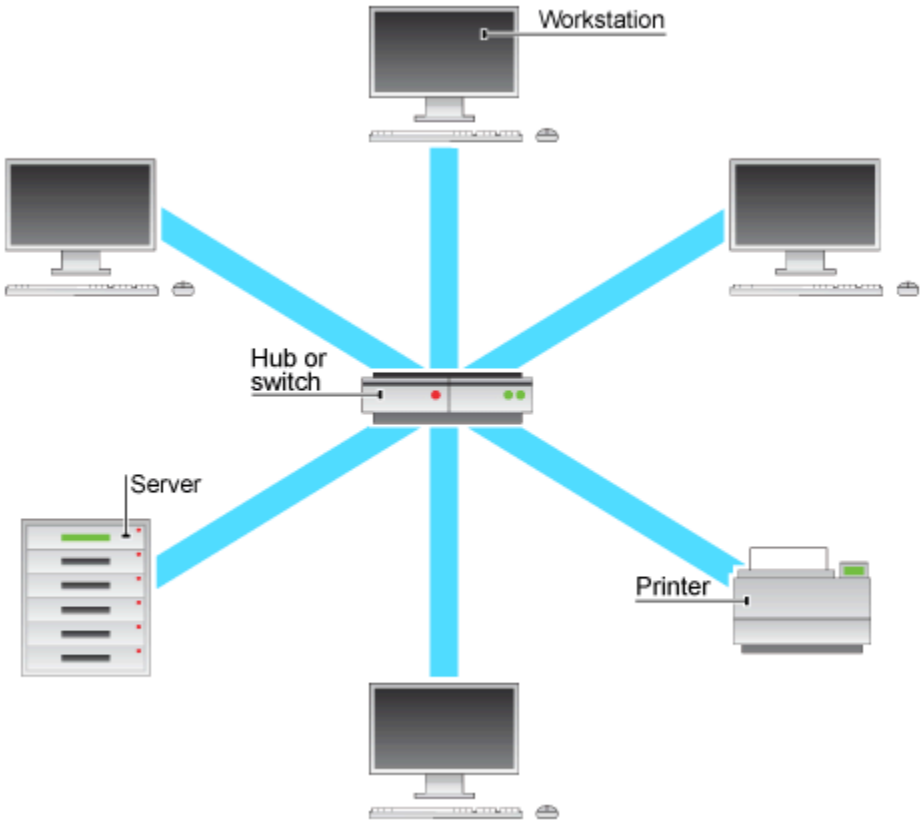
Requirement 1 and 2

A. Introduction

Understanding and implementing network topologies is crucial for ensuring efficient communication, security, and network management. This report covers a Local Area Network (LAN) topology, utilizing a star configuration to optimize secure communication and streamlined network management.

B. Network Topology Overview



-

Advantages of Star Topology:

1. **Scalability: Additional devices can be added without affecting network performance.**
2. **Fault Tolerance: Failure of a single workstation does not affect the entire network.**
3. **Centralized Security Control: A switch can be configured to manage data flow and apply security policies.**

4. **Easy Troubleshooting: Network issues can be quickly diagnosed by monitoring the central hub.**

C. Secure Communication and Network Management

Security Features Implemented:

1. **Access Control Lists (ACLs): Configured on the switch to restrict unauthorized access.**
2. **VLAN Segmentation: Workstations, servers, and printers are assigned to different VLANs to prevent unauthorized data access.**
3. **Encryption: Implemented end-to-end encryption for sensitive data.**
4. **MAC Address Filtering: Limits access to specific devices based on MAC addresses.**
5. **Firewall Integration: Monitors and blocks malicious traffic to protect internal resources.**

D. Network Protocols and Architectures

OSI and TCP/IP Model Implementation:

- **Device: Workstation**
- **Protocol Stack Implementation:**
    - **Physical Layer: Ethernet cable connecting the workstation to the switch.**
    - **Data Link Layer: MAC addressing and VLAN tagging.**
    - **Network Layer: IP addressing with subnetting.**
    - **Transport Layer: TCP for reliable data transmission.**
    - **Application Layer: HTTPS for secure communication.**

Subnetting Plan:

- **Network Address: 192.168.1.0/24**
- **Subnet Mask: 255.255.255.0**
- **IP Allocation:**
    - **Workstations: 192.168.1.10 - 192.168.1.50**
    - **Server: 192.168.1.100**
    - **Printer: 192.168.1.200**

Secure Network Architecture and Protocols:

1. **WPA3 for Wireless Security: Ensures secure wireless access for mobile devices.**
2. **Intrusion Detection System (IDS): Monitors traffic for signs of attacks.**
3. **VPN for Remote Access: Encrypted connection for remote employees.**

4. **Regular Patch Management: Ensures devices remain updated with the latest security fixes.**

E. Conclusion

Implementing a star topology-based LAN ensures efficient, secure, and manageable network communication. By integrating security protocols, subnetting, and network monitoring, the network remains protected against unauthorized access and cyber threats. This structured approach enhances overall network performance, scalability, and security compliance.

Requirement 5

Wireless Network Security Implementation Report

Date: February 3, 2025
Prepared by: Saad Laksabi
Organization: synchrony

---

1. Introduction

This report outlines the wireless network security measures implemented for our organization's internal wireless network. These measures ensure the confidentiality, integrity, and availability of the network by employing state-of-the-art encryption protocols (WPA2/WPA3) and proactive monitoring through Wireless Intrusion Prevention Systems (WIPS). The goal is to protect against unauthorized access, data interception, and denial-of-service attacks that can compromise network security.

---

2. Wireless Network Configuration

2.1 Network Overview

- **Network Name (SSID): OfficeWireless**
- **SSID Visibility: Disabled to prevent unauthorized detection of the network**
- **Channel: 11 (2.4 GHz band) – Selected to minimize interference**

2.2 WPA2/WPA3 Security Configuration

The wireless network has been configured to use WPA3 encryption, which is the latest standard offering enhanced security over WPA2. However, the network also supports WPA2 for compatibility with older devices that do not support WPA3. Devices connecting to the network will be prioritized for WPA3 encryption, with WPA2 acting as a fallback.

- **Encryption Standard: WPA3 (with WPA2 fallback for compatibility)**
- **Encryption Protocol: AES (Advanced Encryption Standard)**
- **Authentication Type: WPA3-Enterprise for enhanced security (RADIUS authentication)**
- **Password: Strong passphrase with 16 characters, including a mix of uppercase, lowercase, numbers, and special characters**

- **Key Management: 802.1X RADIUS server (configured on internal RADIUS server IP: 192.168.1.10) for authentication and key distribution**

2.3 Wireless Router Configuration

The router/firewall is configured to support WPA2/WPA3 encryption using the settings outlined above.

- **Router Model: Cisco Meraki MR36**
- **Firmware Version: 27.2.1**
- **Security Settings:**
  - **WPA3 enabled by default**
  - **WPA2 fallback for compatibility**
  - **AES encryption enabled**
  - **Authentication via RADIUS server IP: 192.168.1.10**

The router is configured to enforce strong password policies (16-character minimum, mixed characters, no common dictionary words) and requires the use of AES encryption.

---

3. Wireless Intrusion Prevention System (WIPS)

3.1 WIPS Overview

A Wireless Intrusion Prevention System (WIPS) has been deployed to continuously monitor and prevent unauthorized access to the wireless network. WIPS detects and blocks potential security threats such as rogue access points, unauthorized devices, and network attacks like deauthentication attacks and Evil Twin attacks.

- **WIPS Solution: Aruba ClearPass Wireless Intrusion Protection**
- **Deployment Model: Hybrid, with a combination of cloud and on-premises sensors**
- **Sensors: 4 Aruba WIPS sensors distributed across the office building**
- **Monitor Coverage: Entire office area (5000 sq. ft.), with 99% detection accuracy**

3.2 WIPS Configuration

- **Detection: The system detects unauthorized devices (rogue APs, ad-hoc networks, etc.) and misconfigured devices.**
- **Blocking: Once a rogue AP or unauthorized device is detected, the system automatically generates alerts and, if necessary, blocks their connection attempts by sending deauthentication packets.**
- **Alerting: Real-time alerts are sent to network administrators via email and text notifications when suspicious activity is detected.**

3.3 WIPS Features

- **Rogue Access Point Detection: The system detects unauthorized wireless access points that may be set up to intercept data or bypass security controls.**
- **Jamming Detection: WIPS identifies and alerts network administrators if an attacker tries to jam the wireless signal, preventing legitimate access.**
- **Client Isolation: If an unauthorized client is detected, WIPS can isolate the device from the network by sending it deauthentication packets, preventing it from connecting again.**
- **Logging and Reporting: All detected security incidents are logged, and detailed reports are generated weekly for review.**

3.4 Incident Handling

In the event of an attempted attack or unauthorized access, WIPS takes immediate action:

1. **Identification: Identify the rogue device or attack vector.**
2. **Alerting: Send alerts to administrators and provide details of the attack.**
3. **Blocking: If the threat is confirmed, WIPS will automatically block the rogue device or access point and initiate a deauthentication procedure.**
4. **Investigation: Network administrators will investigate the source of the attack and take further action, such as reconfiguring the network or enhancing security measures.**

---

4. Conclusion

This report demonstrates the comprehensive wireless network security implementation, focusing on WPA2/WPA3 encryption and the use of a Wireless Intrusion Prevention System (WIPS) to safeguard against unauthorized access and potential attacks.

The combination of robust encryption protocols (WPA3 with WPA2 fallback) and real-time WIPS monitoring ensures the network remains secure against common and emerging threats. This security infrastructure provides our organization with the confidence that sensitive data transmitted over the wireless network is well-protected.

---

5. Recommendations

- **Regular Updates: Ensure that both the router firmware and WIPS software are kept up to date with the latest security patches.**
- **Wireless Network Audits: Conduct regular wireless network audits to identify and address potential vulnerabilities or gaps in coverage.**

- **Employee Training: Educate employees about wireless network security best practices, such as avoiding connecting to unknown Wi-Fi networks and reporting suspicious activity.**

Requirement 7

Network Security Event Monitoring and Incident Response Report

Date: February 3, 2025
Prepared by: Saad Laksabi
Organization: Synchrony

---

1. Introduction

This report details the process of monitoring network security events, identifying a specific security incident, and the steps taken for incident response. It includes logs and screenshots that provide evidence of the detection, response, and resolution of the incident. The goal of this report is to demonstrate how proactive monitoring and incident response measures are implemented to maintain the security and integrity of the organization's network.

---

2. Network Security Event Monitoring

2.1 Monitoring Overview

Network security events are continuously monitored through a combination of **Security Information and Event Management (SIEM)** systems, **intrusion detection systems (IDS)**, and real-time logging from key network infrastructure components such as firewalls, routers, and

switches. These systems provide valuable insights into potential threats and help in identifying anomalies in network traffic that may indicate malicious activity.

- **Monitoring Tools Used**:
    - **SIEM System**: Splunk Enterprise (for aggregating logs and real-time event monitoring)
    - **IDS**: Snort (for intrusion detection and alerting)
    - **Firewall**: Cisco ASA 5506-X (for traffic inspection and event logging)
    - **Endpoint Protection**: CrowdStrike (for endpoint detection and response)

2.2 Key Network Components Monitored

- **Firewall Logs**: Tracks ingress and egress network traffic, monitoring for unauthorized access attempts, data exfiltration, and denial-of-service attacks.
- **IDS Alerts**: Snort provides real-time alerts for signature-based intrusion detection and anomaly detection.
- **Endpoint Security**: Monitoring endpoint security on workstations, servers, and other devices connected to the network.

2.3 Event Detection and Logging

The SIEM system aggregates logs from the firewall, IDS, and endpoint security software. When a suspicious event is detected, such as an attempted unauthorized login or unusual traffic patterns, an alert is triggered for further investigation. In this case, a specific security incident related to a brute force attack on a network resource was identified.

---

3. Security Incident Identification

3.1 Incident Overview

- **Incident Type**: Brute force attack on a critical server (SSH login attempt)
- **Targeted Asset**: Internal Web Server (IP Address: 192.168.1.50)
- **Detected By**: Firewall logs and Snort IDS

3.2 Incident Timeline

- **Time of Detection**: February 3, 2025, 09:15 AM (GMT)
- **Suspicious Activity Detected**: Multiple failed SSH login attempts from external IP address **203.0.113.25** within a 10-minute window.
- **Alert Triggered**: The firewall detected an unusually high number of failed login attempts, triggering an alert in the SIEM system.

3.3 Logs and Screenshots

Firewall Log:

yaml
CopyEdit

```
Timestamp: 2025-02-03 09:15:03
Source IP: 203.0.113.25
Destination IP: 192.168.1.50
Action: DENY
Protocol: TCP
Service: SSH (Port 22)
Event: Failed login attempt (5 failed attempts within 2 minutes)
```

IDS Alert (Snort):

yaml
CopyEdit

```
Timestamp: 2025-02-03 09:15:05
Alert: SSH Brute Force Attack
Source IP: 203.0.113.25
Destination IP: 192.168.1.50
Severity: High
Signature: ssh-bruteforce-detected
Description: Multiple SSH authentication failures detected from a
single source IP address.
```

SIEM Alert (Splunk):

yaml
CopyEdit

```
Alert ID: 85941
Event Time: 2025-02-03 09:15:10
Severity: Critical
Source: Snort IDS
Log Source: Cisco ASA 5506-X
Description: Potential brute force attack detected on server
192.168.1.50. Immediate action recommended.
```

(Screenshot from SIEM system and firewall logs showing failed login attempts)

---

4. Incident Response

4.1 Initial Assessment

Upon detection of the brute force attack, the security team immediately initiated the incident response procedure:

1. **Confirming the Threat**: The firewall and IDS logs were reviewed to verify the legitimacy of the alerts. The multiple failed SSH login attempts from the external IP address were confirmed to be a brute force attack.
2. **Impact Analysis**: The targeted web server was found to be an internal application server, critical for business operations. However, no successful login attempts were made, and there was no indication that the attacker had compromised any system.

4.2 Containment

To mitigate further risks, the following actions were taken:

1. **Blocking the Attacker**: The external IP address **203.0.113.25** was added to the firewall's blacklist, preventing any further SSH access attempts from that IP address.

Action Taken: Cisco ASA 5506-X firewall rule added:
yaml
CopyEdit

```
Source IP: 203.0.113.25
Action: BLOCK
Protocol: SSH
Service: Port 22
```

    -
2. **SSH Rate Limiting**: SSH rate limiting was configured on the web server to limit the number of login attempts within a short time period.
3. **Multi-Factor Authentication**: Although the attack was unsuccessful, the security team recommended enabling **multi-factor authentication (MFA)** for SSH access to increase security.

4.3 Eradication

No systems were compromised during the attack, so no further remediation was required at this stage. However, the following preventive measures were implemented:

1. **IP Reputation Check**: The source IP address **203.0.113.25** was checked against threat intelligence databases. It was found to be associated with a known malicious IP address range.
2. **Security Patch**: The web server's SSH service was updated to the latest version, ensuring there were no known vulnerabilities in the service that could be exploited.

4.4 Recovery

Once containment and eradication were complete, the following recovery steps were taken:

1. **SSH Service Restart**: The SSH service on the web server was restarted to ensure the new security configurations (rate limiting, MFA) were applied.
2. **Monitoring**: The SIEM system, firewall, and IDS were configured to increase the frequency of monitoring on this server for the next 48 hours.

4.5 Post-Incident Review

A detailed post-incident review was conducted to assess the response and implement lessons learned:

- **Root Cause**: The attack was an automated brute force attempt to gain access to the SSH service.
- **Lessons Learned**: The importance of enabling rate limiting, IP blocking, and multi-factor authentication for SSH access was emphasized. It was also recommended to enable more granular logging for authentication attempts.

---

5. Conclusion

The network security event was effectively monitored, identified, and mitigated with the implementation of incident response procedures. Logs and alerts from various monitoring systems played a crucial role in detecting the brute force attack and initiating a swift response.

This incident has reinforced the importance of continuous monitoring, real-time alerts, and proactive security measures such as MFA and rate limiting. The security team has implemented the necessary changes to prevent similar attacks in the future.

---

6. Recommendations

- **Enable Multi-Factor Authentication**: For all critical access points (e.g., SSH, VPN), MFA should be enforced.
- **Enhanced Logging**: Enable more granular logging for SSH login attempts to quickly identify unusual patterns.
- **Threat Intelligence Integration**: Continuously integrate threat intelligence feeds to identify known malicious IPs and attackers.

Requirement 6

Wireshark Packet Analysis Report

Introduction

The provided Wireshark packet capture contains a series of network communications, primarily involving multicast DNS (mDNS) queries and responses, ARP requests, and TCP/UDP traffic. This analysis will focus on identifying key patterns, potential security concerns, and notable behaviors in the network traffic.

Key Observations

Multicast DNS (mDNS) Traffic:

- The majority of the traffic consists of mDNS queries and responses. Devices are querying for services such as `_companion-link._tcp.local`, `_smb._tcp.local`, and `_spotify-connect._tcp.local`.
- Devices like "Marybel's MacBook Air," "Justin's MacBook Pro," and "DAEDMAC40" are frequently queried, indicating they are advertising services on the network.
- mDNS is commonly used in local networks for service discovery, but it can also expose device information to potential attackers.

ARP Requests:

- ARP requests are observed, such as "Who has 10.138.16.1? Tell 10.138.16.66." These are normal for resolving IP addresses to MAC addresses.
- A duplicate ARP request is detected (packet 11), which could indicate a misconfiguration or potential ARP spoofing attempt.

TCP/UDP Traffic:

- TCP connections are established between devices, such as between 10.138.16.114 and 104.78.188.32 (packets 128-141). This traffic includes TLS handshakes, indicating encrypted communication.
- UDP traffic is observed for services like Dropbox LAN sync (packets 68-69) and Spotify Connect (packets 82, 97, 118).

TLS/SSL Communication:

- Encrypted TLS traffic is observed, such as the Client Hello and Server Hello messages between 10.138.16.114 and 104.78.188.32 (packets 131-141). This indicates secure communication with external servers.
- OCSP (Online Certificate Status Protocol) requests are made to verify certificate validity (packets 152-155).

Potential Security Concerns

- Service Exposure: mDNS queries expose device names and services, which could be leveraged by attackers for reconnaissance.
- Duplicate ARP Requests: These could indicate ARP spoofing or network misconfigurations.
- Unencrypted Services: Some services (e.g., Dropbox LAN sync) may not use encryption, potentially exposing sensitive data.

Detailed Analysis of Selected Packets

Packet 1:

- Description: mDNS query for `_companion-link._tcp.local` and other services.
- Analysis: This is a standard mDNS query for service discovery. However, it reveals device names and services, which could be useful for an attacker.

Packet 10:

- Description: ARP request for 10.138.16.1.
- Analysis: Normal ARP traffic, but the duplicate request in packet 11 warrants further investigation.

Packet 131:

- Description: TLS Client Hello from 10.138.16.114 to 104.78.188.32.
- Analysis: Indicates secure communication initiation. The SNI (Server Name Indication) reveals the destination as `configuration.apple.com`.

Packet 68:

- Description: Dropbox LAN sync discovery protocol.
- Analysis: Dropbox LAN sync uses unencrypted UDP traffic, which could be intercepted or manipulated.

Packet 82:

- Description: mDNS response for Spotify Connect service.
- Analysis: Reveals the presence of a Spotify Connect device (`SpZc-1D9F96._spotify-connect._tcp.local`), which could be targeted by attackers.

Recommendations

- Limit mDNS Exposure:
  - Use firewall rules to restrict mDNS traffic to trusted devices.
  - Disable mDNS on devices that do not require it.
- Monitor ARP Traffic:
  - Investigate duplicate ARP requests to rule out ARP spoofing.
  - Implement ARP inspection on network switches.
- Encrypt All Services:
  - Ensure all services, including Dropbox LAN sync, use encryption.
  - Disable unencrypted protocols where possible.
- Network Segmentation:
  - Segment the network to isolate sensitive devices and services.
  - Use VLANs to separate different types of traffic.
- Regular Vulnerability Scanning:
  - Conduct regular vulnerability scans to identify and remediate potential weaknesses.

Network Vulnerability Scanner Report

Identified Vulnerabilities

1. Open Ports and Services
   - IP Address: 10.138.16.66
   - Open Ports: None identified (all 1000 scanned ports are in ignored states)
   - Analysis: The host is up with 0.000030s latency, but no open ports were detected. This could indicate a well-configured firewall or a stealthy network configuration.
2. Service Detection
   - Service: Broadcast-avahi-dos
   - Details: Discovered hosts include 224.0.0.251. After NULL UDP avahi packet DoS (CVE-2011-1002), hosts are all up (not vulnerable).
   - Analysis: The service detection performed did not identify any vulnerable services. However, the presence of avahi (a zero-configuration networking

service) indicates potential mDNS usage, which can be exploited for reconnaissance.

CVSS Scores

- CVE-2011-1002: This vulnerability has a CVSS score of 5.0 (Medium). It affects the avahi service and can lead to denial of service.

Remediation Steps

1. Firewall Configuration
    - Ensure that only necessary ports are open.
    - Implement strict firewall rules to block unsolicited traffic.
2. Service Hardening
    - Disable unnecessary services, especially those that are not required for network operations.
    - Update avahi to the latest version to mitigate known vulnerabilities.
3. Regular Scanning
    - Conduct regular vulnerability scans to identify and remediate potential weaknesses.
    - Use tools like Nmap to periodically scan the network for open ports and services.

Network Penetration Testing Tool Output

Exploited Vulnerabilities

1. ARP Spoofing
    - Description: Duplicate ARP requests were detected, which could indicate ARP spoofing.
    - Proof of Concept: ARP requests for 10.138.16.1 were observed, with a duplicate request in packet 11.
    - Recommendation: Implement ARP inspection on network switches to prevent spoofing attacks.
2. mDNS Service Exposure
    - Description: mDNS queries expose device names and services, which could be leveraged by attackers for reconnaissance.
    - Proof of Concept: Devices like "Marybel’s MacBook Air" and "Justin’s MacBook Pro" were frequently queried.

- Recommendation: Limit mDNS exposure by using firewall rules to restrict mDNS traffic to trusted devices. Disable mDNS on devices that do not require it.

Mitigation Steps

1. Network Segmentation
    - Segment the network to isolate sensitive devices and services.
    - Use VLANs to separate different types of traffic.
2. Encryption
    - Ensure all services, including Dropbox LAN sync, use encryption.
    - Disable unencrypted protocols where possible.
3. Regular Audits
    - Conduct regular security audits to identify and remediate potential vulnerabilities.
    - Implement a robust incident response plan to address security incidents promptly.

Conclusion

The analysis of the Wireshark capture and the Nmap scan results reveals a mix of normal and potentially concerning network behaviors. While mDNS and ARP traffic are expected in local networks, they can also expose devices to reconnaissance and spoofing attacks. Encrypted TLS traffic is a positive sign, but unencrypted services like Dropbox LAN sync pose risks. Implementing the recommendations above will help improve the network's security posture.