Secure BYOD (Bring Your Own Device) in a Corporate Environment

Gnanitha Garikipati, Sowmya Reddy Likkidi, Sri Teja Sudunagunta, Yusuf Mohammad

Department of Computer Engineering, University of New Mexico

ECE540: Advanced Networking Topics

Michael Devetsikiotis

December 13, 2024

1. Introduction

In today's corporate world, Bring Your Own Device (BYOD) policies are common as they enhance convenience and productivity. However, they pose security risks, as personal devices may not meet corporate security standards, increasing the chance of data breaches and unauthorized access. While BYOD improves flexibility and saves costs, it also requires security measures like encryption and VPNs to manage the risks and handle various device types.

Organizations use BYOD frameworks to secure personal devices accessing corporate resources. These frameworks restrict access to authorized devices, enforce security measures like encryption, grant role-based access, and monitor devices for threats. Our project aims to create a secure BYOD environment by simulating Mobile Device Management (MDM), Network Access Control (NAC), Zero Trust Network Access (ZTNA), and firewalls. The focus is to ensure devices comply with security policies, provide secure role-based access, and analyze how security measures affect network performance.

This report covers potential solutions (Section 2) the proposed system's details (Section 3), analysis results (Section 4) and concludes with future work (Section 5).

2. Potential Solutions

2.1 General Approach

A general BYOD policy focuses on establishing guidelines for personal device use within corporate environments. This includes device enrollment, acceptable use policies, data access management and ensuring security through encryption, remote wipe capabilities and basic network security configurations.

Pros:

1. Flexibility where employees can use their devices, boosting satisfaction and productivity.
2. Reduces hardware costs since employees use their own devices.
3. Enables seamless remote work and access to corporate resources.

Cons:

1. Personal devices increase the risk of data breaches and unauthorized access with low compliance.
2. Ensuring all devices comply with corporate policies is difficult.
3. Lack of granular check and strict policies might pose the risk of network compromise.

2.2 Integrated Approach

This approach integrates Mobile Device Management (MDM), Network Access Control (NAC), Zero Trust Network Architecture (ZTNA) and Firewall filtering for a robust BYOD strategy.

1. MDM: Enforces device policies and provides remote wipe capabilities for lost or compromised devices.
2. NAC: Verifies devices before granting access to the corporate network based on compliance with security policies.
3. ZTNA: Operates on 'never trust, always verify' principle, requiring strict identity verification and continuous monitoring of devices and users.
4. Firewall Filtering: Implements traffic filtering and segmentation.

Pros:

1. Combines multiple security layers to minimize vulnerabilities.
2. Allows precise access control on user's identity, device compliance and network behavior.
3. Accommodates a growing number of devices with robust security measures,
4. Meets regulatory standards with monitoring and control mechanisms.

Cons:

1. Integrating multiple systems requires significant expertise, resources and higher costs.
2. Security measures slightly increases network latency and decreases throughput.

However, this integrated approach strikes a balance between productivity and security, effectively addressing the challenges of BYOD in a corporate setting.

3. Solution Approach

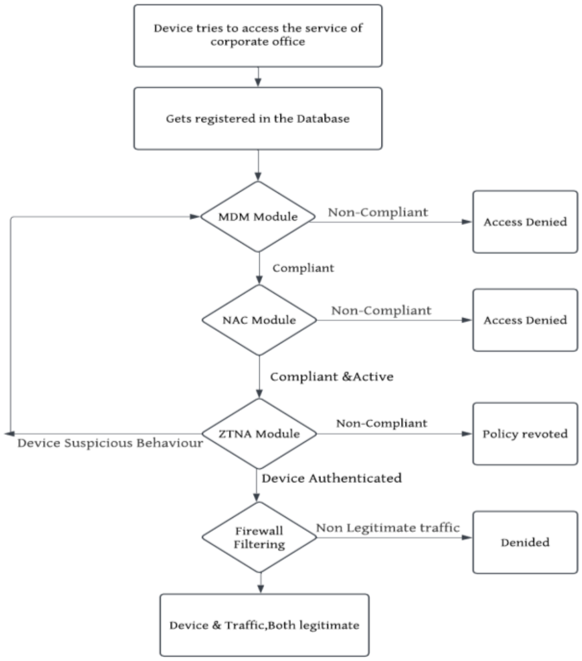


Figure 1: Block Diagram of the proposed solution

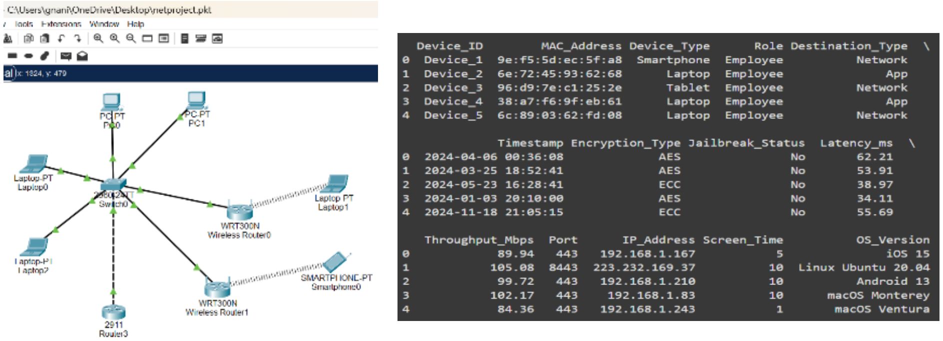
Our solution approach consists of 5 steps majorly:

1. **Network and Data simulation:** Initially, we created a small office network in Cisco Packet Tracer with both wired and wireless connections to simulate various device specifications. This network included different devices with varying configurations. To supplement this, we generated additional dataset using Python Faker library for about 100 devices, fixed the policy standards and are stored in the database. This dataset provided a broader foundation for analysis.
2. **MDM Compliance:** In this step,
   i) All devices in the simulated network were checked for compliance based on the OS type and version, encryption standard, Jailbreak/Root status and screen time limits.
   ii) Any device that did not meet the policy standards was flagged as non-compliant and denied further access.
   iii) Next, we ran the module to measure the latency and throughput for all compliant devices and calculated the average latency and throughput to evaluate the overall network performance and all the status is updated in the database.
3. **NAC Enforcement:** In this step, the following checks were performed to ensure secure access.
   i) Appropriate VLANs were assigned by authenticating users based on their roles.
   ii) Devices connecting from IP addresses outside the predefined ranges were prompted to connect via VPN to ensure secure access. Similarly, ports were checked to ensure they complied with policy standards.

iii) Any device violating rules, access is denied else the device gets access to the requested resources and sets the device status as active. Average latency and throughput were calculated, and the status is updated in the database.

4. **ZTNA:** For active devices, compliance is rechecked if any suspicious activity is detected. This module calls MDM and NAC functions, if the device passes it continues with the policy else access is revoked. Average latency and throughput were calculated and updated to the database.
5. **Firewall Filtering:** In this step the active device’s traffic is assessed for any anomaly dynamically, blocking UDP traffic and adjusting performance for active devices.

4. Results



```
  Device_ID        MAC_Address Device_Type      Role Destination_Type  \
0  Device_1  9e:f5:5d:ec:5f:a8  Smartphone  Employee          Network
1  Device_2  6e:72:45:93:62:68      Laptop  Employee              App
2  Device_3  96:d9:7e:c1:25:2e      Tablet  Employee          Network
3  Device_4  38:a7:f6:9f:eb:61      Laptop  Employee              App
4  Device_5  6c:89:03:62:fd:08      Laptop  Employee          Network

             Timestamp Encryption_Type Jailbreak_Status  Latency_ms  \
0  2024-04-06 00:36:08             AES               No       62.21
1  2024-03-25 18:52:41             AES               No       53.91
2  2024-05-23 16:28:41             ECC               No       38.97
3  2024-01-03 20:10:00             AES               No       34.11
4  2024-11-18 21:05:15             ECC               No       55.69

   Throughput_Mbps  Port     IP_Address Screen_Time         OS_Version
0            89.94   443  192.168.1.167           5             iOS 15
1           105.08  8443  223.232.169.37         10 Linux Ubuntu 20.04
2            99.72   443  192.168.1.210          10         Android 13
3           102.17   443   192.168.1.83          10     macOS Monterey
4            84.36   443  192.168.1.243           1      macOS Ventura
```

Figure 2: Simulation in Cisco Packet Tracer and Snapshot of database

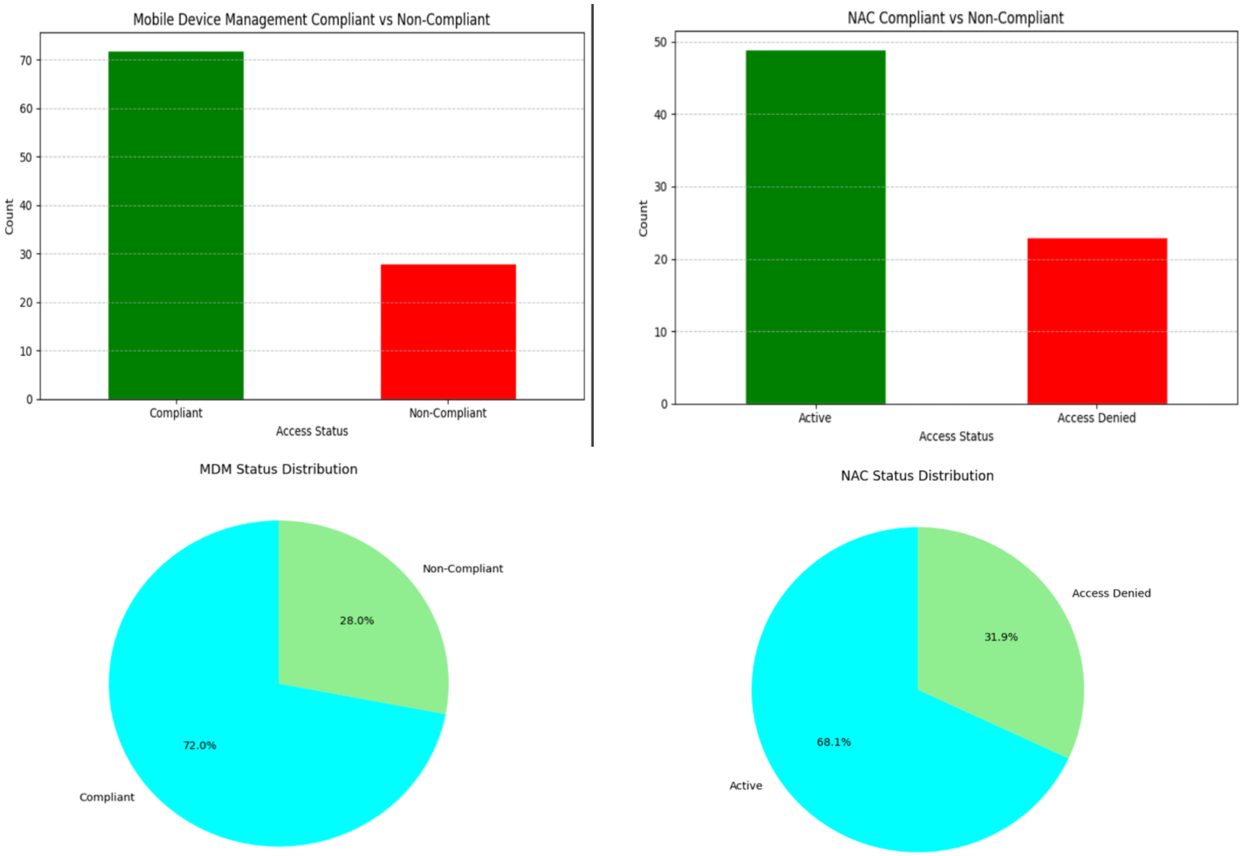


Figure 3: MDM and NAC compliancy status

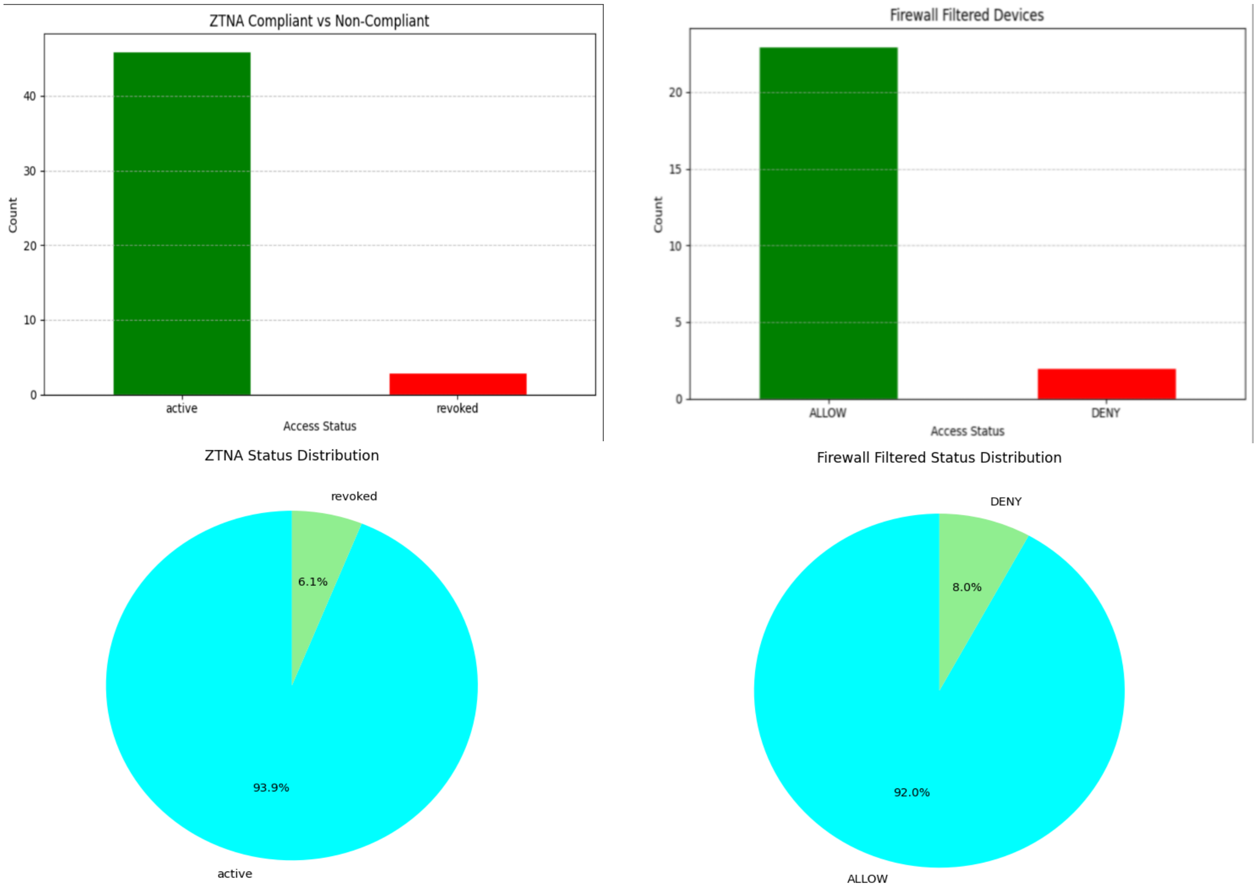


Figure 4: ZTNA and Firewall compliancy status

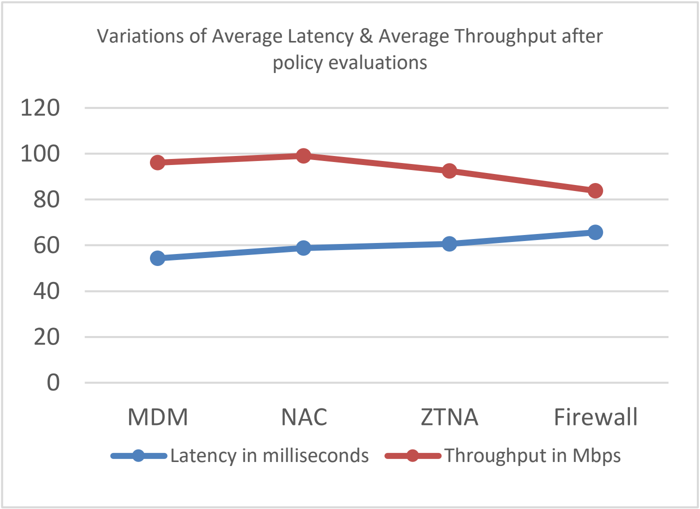


Figure 5: Statistics of average throughput and latency after each module

We simulated data for 100 devices, verifying compliance sequentially through MDM, NAC and ZTNA modules. Traffic from compliant, active devices was then filtered via the firewall for security. Finally, traffic from active devices was filtered through the firewall for enhanced security. Average latency is increased after each module due to policy complexity, while throughput generally decreased. However, after the NAC module, throughput slightly improved as non-compliant devices were eliminated, optimizing the network.

The Connection Success Rates show that 90% of employee and admin devices were compliant and granted access, while non-compliant devices were blocked. In terms of Performance Impact, latency increased by 5ms for compliant devices, and throughput decreased by 10%-15% for secure devices, balancing security and performance. For Data Leakage Prevention, all non-compliant devices were blocked, ensuring no unauthorized access and maintaining data security.

5. Conclusion

The Proposed Model balances security and performance, addressing BYOD challenges. It includes features like Zero Trust Network Access (ZTNA) and firewalls for real-time threat prevention, along with Mobile Device Management (MDM) and Network Access Control (NAC) for centralized management, ensuring a secure and scalable solution. This project successfully simulated a secure BYOD environment using MDM, NAC, ZTNA, and firewalls. Key achievements include detecting and blocking non-compliant devices, providing secure role-based access, and balancing security with acceptable performance trade-offs.

6. Future Work

We suggest scaling the simulation to thousands of devices for comprehensive scalability testing and incorporating AI for real-time threat detection and anomaly management. Additionally, we recommend experimenting with a variety of IoT devices.

References

[1] K. AlHarthy and W. Shawkat, "Implement Network Security Control Solutions in BYOD Environment," 2013 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, Nov. 29 - Dec. 1, 2013.

[2] G. A. Safdar and A. Mansour, "Security and Trust Issues in BYOD Networks," University of Bedfordshire, LU1 3JU, Luton, U.K..

[3] M. I. Ali and S. Kaur, "BYOD Cyber Threat Detection and Protection Model," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Phagwara, Punjab, India, 2021

[4] J. Anderson, Q. Huang, L. Cheng, and H. Hu, "BYOZ: Protecting BYOD Through Zero Trust Network Security," 2022 IEEE International Conference on Networking, Architecture and Storage (NAS), 2022

[5] https://www.ibm.com/topics/byod

[6] https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device

[7] https://learn.microsoft.com/en-us/windows/client-management/mdm-overview

[8] https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

[9] https://cloud.google.com/firewall/docs/firewall-policies-overview

[10] https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture