iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.81992

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Strengthening Cyber Security for College Endpoint Devices via Firewall Architectures

Sandesh Baban Gaikwad, Varsha Ashok Khandagale
Modern College of Commerce & Computer Studies, Nigdi-44

Abstract: ***The introduction of "Bring Your Own Device" (BYOD) culture and the integration of Internet of Things (IoT) technology have significantly broadened the attack surface of modern educational networks. Unlike traditional commercial settings, educational institutions must balance an open, collaborative learning atmosphere with the stringent security requirements of administrative and research data. This article explores the critical role that firewall tools, such as network-level, host-based, and Next-Generation Firewalls (NGFW), play in securing various endpoint devices inside a college ecosystem.***
This study examines how automated policy enforcement and granular internal segmentation can minimize the risks of lateral malware movement and unauthorized data exfiltration through a qualitative review of defense-in-depth techniques. The study suggests a multi-layered security framework that combines conventional firewall topologies with Zero Trust concepts. In order to efficiently safeguard institutional integrity against more complex cyber-attacks, our findings show that while perimeter defenses are still required, the evolving threat landscape necessitates a change toward endpoint-centric security.
Keywords: Cybersecurity, Endpoint Security, Firewall Architectures, Higher Education, Network Segmentation, Zero Trust.

I. INTRODUCTION

Modern college campuses have become complex, hyperconnected centers of information exchange because of the digital transformation of higher education. In addition to promoting academic collaboration and innovation, this connectivity gives fraudsters a large and open attack surface. Academic institutions are distinguished by a Bring Your Own Device (BYOD) culture, compared to traditional corporate organizations, which often function under strict "top-down" hardware control. A broad variety of laptops, tablets, and smartphones, often with different levels of updated security patches, are connected to the college network by students, faculty, and administrative staff.

A. Problem Statement

Cyberattacks such as ransomware, phishing, and credential harvesting nowadays mainly target endpoint devices, which act as the last nodes of communication on a network. A single hacked student laptop can act as an entry point for lateral movement in a college setting, enabling a threat to move from a public Wi-Fi zone into high-value research servers or sensitive administrative databases. The movement of thousands of unmanaged devices causes the "perimeter" to constantly change, making traditional perimeter-based security ineffective.

B. Motivation

Three primary factors make colleges and universities extremely vulnerable:

- Data Sensitivity: They contain a "goldmine" of data, including financial records, thousands of students' personal data, and intellectual property (IP) from research.
- Open Access Requirements: Rigid safety standards may conflict with the academic mission's requirement for an open environment that supports resource sharing.
- Resource Challenges: Compared to their private sector counterparts, IT departments in education often have to manage massive, diverse networks with smaller budgets and fewer specialized security staff.

C. Scope and Objective

The execution and administration of firewall tools as a specific defense mechanism for endpoint protection are the main topics of this study. Although firewalls are typically thought of as "gatekeepers" at the network's edge, this paper analyzes the way they have developed into host-based and next-generation tools that offer fine-grained management at the device level.

The goal of the study is to recommend a layered firewall architecture that strikes a balance among the demand for strong data protection and the need for academic freedom. This study attempts to offer a roadmap for protecting the contemporary college endpoint by analyzing the shift from basic packet filtering to Zero Trust and Application-Layer filtering.

II. FIREWALL ARCHITECTURES: A COMPARATIVE OVERVIEW

Security in a college environment has to be both deep (covering individual student and staff devices) and broad (protecting the entire campus). Network-Based and Host-Based firewalls are put together to achieve this.

It is beneficial to think of these technologies as having multiple "layers" of security when trying to understand their ability to work to secure a college network.

A. Network-Based Firewalls (The Perimeter Guards)

The "gatekeepers" of the campus infrastructure are network-based firewalls. They typically serve as hardware appliances between departments (e.g., isolating the student Wi-Fi network from the administrative/finance network) or at the places where the internal campus network connects to the internet.

- Core Function: They maintain monitoring on every piece of traffic coming into and going out of the network.
- Key Strength: Centralized control is a key strength. From a single dashboard, IT administrators can implement security policies across the network.
- Limitation: The network-based firewall has limited visibility into what happens "inside" the network (between two student computers, for example) once a malicious packet has crossed the perimeter.

B. Host-Based Firewalls (The Personal Bodyguards)

Firewalls that have host-based (also referred to as personal bodyguards) Software programs deployed directly on particular endpoints (laptops, PCs, servers) are referred to as host-based firewalls. Regardless of the network the device is currently connected to, they function as a local agent, filtering traffic solely for that one device.

- Core Function: They keep an eye on traffic that is unique to that device, determining which programs—such as web browsers vs background system services—are attempting to send or receive data.
- Key Strength:Device-level granularity is a key strength. The host-based firewall is still in place even if a user moves their laptop outside of the campus firewall, such as to a public coffee shop.
- Limitation: Because they function on a single device, they use local system resources (CPU and RAM) and need to be constantly maintained to ensure that thousands of devices are configured correctly.

Feature	Network-Based Firewall	Host-Based Firewall
Placement	Perimeter/Gateway	Individual device (endpoint)
Visibility	Broad (Network-wide traffic)	Specific (Individual host traffic)
Primary Goal	Stop external threats entering	Stop local attacks/insider threats
Configuration	Centralized	Local or policy-managed
Mobility	Fixed location	Moves with the device

C. Why Colleges Need Both

In a campus setting, a "Defence-in-Depth" strategy is essential:

- Network Firewalls handle the "heavy lifting," blocking massive volumes of known malicious traffic (e.g., DDoS attacks) before they saturate the campus connection.
- Host-Based Firewalls provide the necessary "last mile" of security. If a student's device is already infected (e.g., from an infected USB drive or a previous network connection), the host-based firewall prevents that device from acting as a "patient zero" to spread malware laterally to other devices on the same Wi-Fi subnet.

III. PROPOSED FRAMEWORK FOR ENDPOINT SECURITY: THE UNIFIED DEFENCE STRATEGY

A "perimeter-only" approach must give way to a Zero Trust Architecture (ZTA) in order to secure a diverse academic environment. Within this framework, the firewall becomes an intelligent, dynamic part of the network instead of merely a static wall. A recommended framework for successfully integrating these tools is provided below.

A. Integrated Policy Management (Centralized Orchestration)

The primary problem in a college is the number of devices; it isn't feasible to manually set up host-based firewalls on each student laptop.

- Unified Endpoint Management (UEM) is the implementation of a centralized system that automatically pushes firewall policy updates to all managed devices (faculty/staff).
- Role-Based Access Control (RBAC): Based on the role assigned to the user, firewalls should dynamically apply policies. For example, a researcher's devices might require specific port access for remote transfer of data, while a student device in the computer lab has stricter "deny-all" incoming communication requirements.

B. Segmented Network Architecture

The campus should be separated into micro-segments utilizing network firewalls:

- Departmental Isolation: Maintain the Student and Guest networks separate from the Finance and Administration VLANs.
- IoT fencing: Setting up smart campus hardware (such as security cameras, HVAC sensors, and smart lighting) in a separate "IoT-only" area. The firewall prevents an attacker from accessing the student registration database through a hacked camera.

C. Automated Threat Response (The Feedback Loop)

A modern firewall should be connected to an Intrusion Detection/Prevention System (IDS/IPS).

Quarantine Logic: A host-based firewall on a student’s laptop detects suspicious activity (e.g., unauthorized port scanning or a ransomware-style file encryption attempt) and warns the central network firewall.

Dynamic Blocking: The main firewall then automatically moves the student’s connection to a “Quarantine VLAN” which restricts their internet access but allows them to get to only a college approved remediation page (i.e. a site to download antivirus cleaners or report the issue to IT).

D. The Human Firewall Element

There are some limits to what technology can do in the academic world. A strong framework should include:

Transparency – Explaining to students why certain firewall rules were set in place.

Self-Help Resources: Offer simplified, automated scripts or guides that enable students verifying that their local host-based firewall (e.g., Windows Firewall) is active and configured properly.

Layer	Technology	Primary Function
Edge	Next-Gen Firewall (NGFW)	Traffic inspection & application filtering

Layer	Technology	Primary Function
Internal	Segmentation Firewalls	Preventing lateral movement (east-west traffic)
Endpoint	Host-Based Firewall	Granular control & mobility protection
Intelligence	IDS/IPS + Automation	Triggering quarantine for infected nodes

IV. CHALLENGES AND BEST PRACTICES

Challenges are common in implementing a robust firewall strategy within a collegiate environment. IT administrators have to deal with a unique set of challenges when it comes to the “conflict” between “open access” and “security”.

A. Key Challenges

Academic Freedom in comparison to Security: Researchers and students may require access from around the world to a number of protocols, unauthorized ports or external databases that might send out security alerts. Rules that are too restrictive may block legitimate scientific research or collaborative tools.

The BYOD Management Gap: A corporate office can control the hardware it owns, but a college IT department can’t force deep configuration changes on a student’s personal laptop. The technical challenge of ensuring that thousands of different devices have their host-based firewalls configured on is massive.

Shadow IT: Students and faculty may use “Shadow IT” (personal hotspots or unauthorized VPNs) when campus networks are too restrictive, avoiding institutional security entirely and making the network blind to potential threats.

Performance Bottleneck: Deep Packet Inspection (DPI) in Next Generation Firewalls requires a lot of processing power. In a high-bandwidth environment such as a university, where thousands of students are continuously streaming high-definition educational content or research data, firewalls can become a performance bottleneck when they are not scaled properly.

B. Best Practices for Implementation

To navigate these challenges, institutions should adopt the following best practices

Go with a "Default Deny" strategy. Set firewalls to block everything unless it's necessary for daily operations. For academic work, have a clear exception process. This allows researchers to get the ports they need by explaining their importance; it should be simple and fast.

Automate enforcement as well. Let NAC systems check every device before it connects to the main campus Wi-Fi. If a student’s computer has its firewall turned off or isn't updated, the university firewall should send it to a remediation VLAN immediately. This way, the device can get patched up before returning to the network.

If the budget is tight, open-source firewalls like pfsense or OPNsense provide solid protection without the high cost of commercial gear.

Don't forget about traffic analysis and visibility. Firewalls are only as effective as the data they provide. Roll out central log management tools like ELK Stack or Splunk to monitor network traffic. If you see a sudden spike in outbound traffic from one device, it signals potential issues like data leaks or ransomware.

V. CONCLUSION

The cybersecurity of endpoint devices in a college setting can no longer depend on a strict perimeter. As the boundaries of the campus network grow through BYOD and IoT, the firewall needs to change into a distributed, smart system.

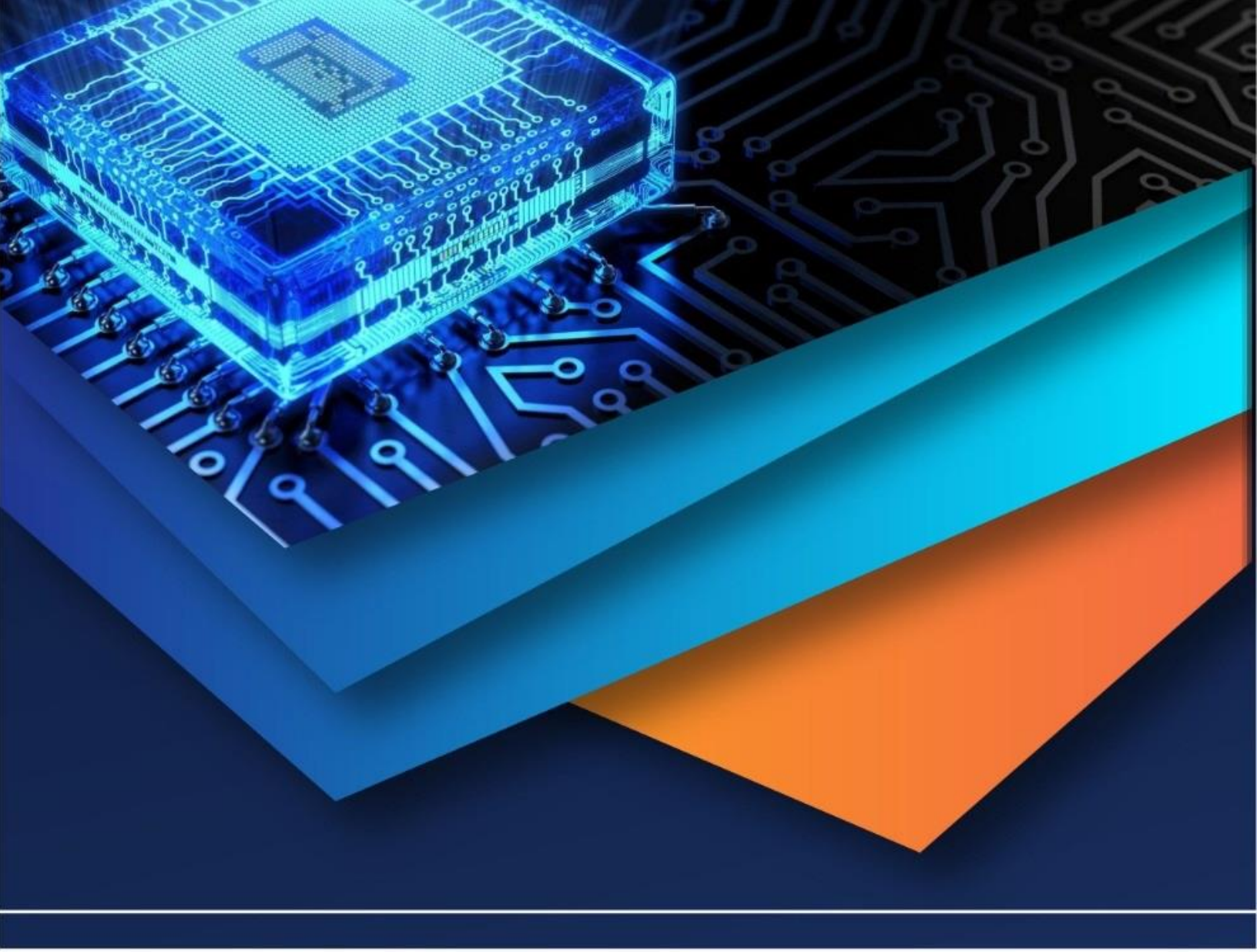
By merging the wide protection of Network-Based Firewalls with the detailed, mobile protection of Host-Based Firewalls, and layering them within a Zero Trust framework, institutions can safeguard their sensitive data while still encouraging academic exploration. In the end, the best security strategy is one that combines modern technology with a knowledgeable and proactive user base.

Core Cybersecurity Standards & Frameworks

1) National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-41 Revision 1: Guidelines on Firewalls and Firewall Policy. Gaithersburg, MD: U.S. Department of Commerce. Relevance: This text helps understand how to build and manage firewall policies.

2) National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-207: Zero Trust Architecture. Gaithersburg, MD: U.S. Department of Commerce. Relevance: This supports your section on shifting from perimeter-only defense to a "Never Trust, Always Verify" model.

3) Center for Internet Security (CIS). (2024). CIS Controls v8: Control 04 - Secure Configuration of Enterprise Assets and Software. Relevance: This gives specific guidelines for host-based firewalls and endpoint protection.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY