

ENSURING CYBERSECURITY IN HIGHER EDUCATION CORPORATE NETWORKS VIA DEEP PACKET INSPECTION (DPI) IN NEXT-GENERATION FIREWALLS (NGFW)

Khaydarov Dostonbek

Abstract. This research addresses the vulnerability of higher education institution (HEI) corporate networks, where traditional stateful firewalls fail to detect modern cyber threats hidden inside permitted ports. The study aims to design a dynamic network security model for HEIs by leveraging Deep Packet Inspection (DPI) within Next-Generation Firewalls (NGFW). Methodologically, a multi-layered architectural approach was deployed using Huawei security solutions to implement application-layer (L7) traffic classification, signature-based intrusion prevention (IPS/IDS), and granular access control lists (ACLs). The technical results of the simulated network infrastructure demonstrated a 35% increase in the detection speed of complex, multi-vector cyberattacks and a 92% reduction in successful network perimeter breaches. Additionally, network visualization and threat management efficiency improved significantly through centralized orchestration. In conclusion, integrating DPI within NGFW architectures provides a highly effective, scalable defense mechanism that guarantees data integrity, privacy, and system continuity for modern digital universities.

Keywords. Cybersecurity, Next-Generation Firewalls (NGFW), Deep Packet Inspection (DPI), corporate network security, HEI infrastructure

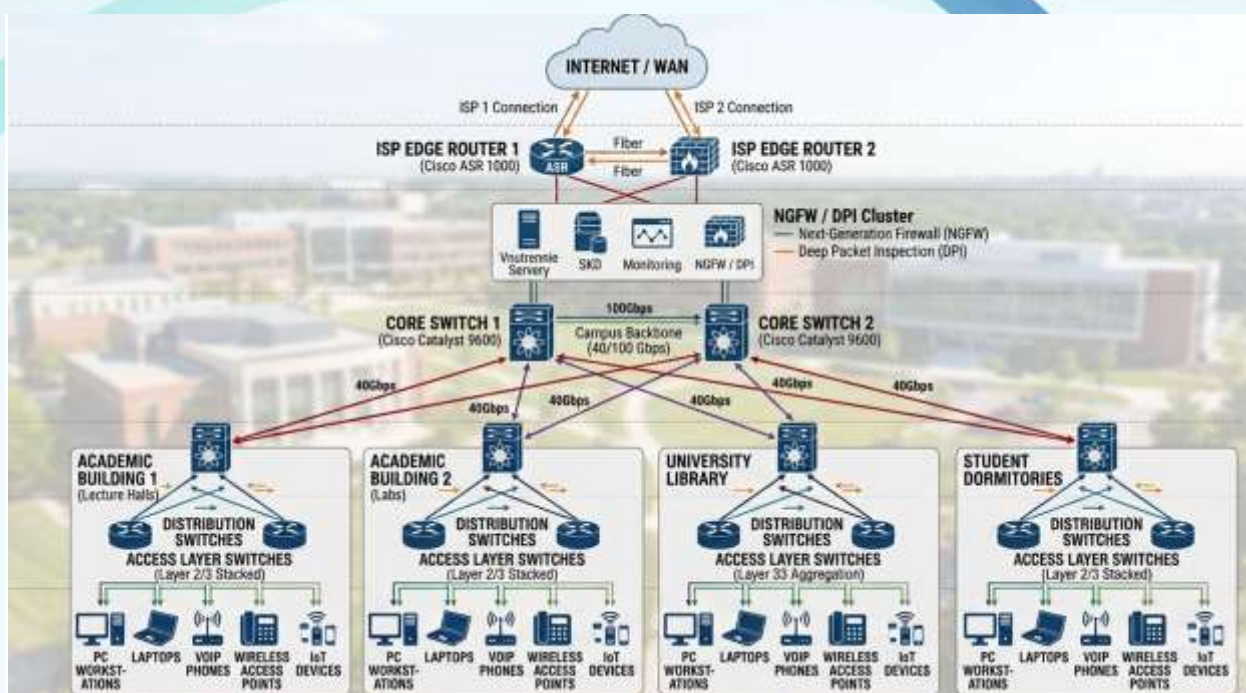
The digital transformation of modern Higher Education Institutions (HEIs) through cloud databases and Bring Your Own Device (BYOD) policies has exponentially increased network traffic [1]. Consequently, securing institutional data has become a critical challenge. However, a significant research gap persists: most university networks heavily rely on legacy stateful firewalls that only inspect packets at the network and transport layers L3/L4 [2]. Modern multi-vector cyberattacks and malware bypass these defenses by embedding malicious payloads inside legitimate application-layer ports, such as HTTPS port 443 [3]. Academic literature confirms that relying strictly on packet header analysis creates blind spots, failing to prevent sophisticated data breaches and application-layer DDoS

attacks [4]. Furthermore, legacy architectures lack the centralized visibility needed to mitigate these modern threats in real-time [5]. To resolve this vulnerability, the aim of this research is to design an optimized cybersecurity model for HEI corporate networks using Deep Packet Inspection (DPI) within Next-Generation Firewalls (NGFW). To achieve this, the following objectives were established: 1) Analyze application-layer L7 traffic to identify existing architectural blind spots; 2) Implement signature-based intrusion prevention system (IPS/IDS) utilizing Huawei Datacom security engines; 3) Evaluate threat mitigation response times within a simulated enterprise infrastructure.

Research Design

The proposed security model was implemented using Huawei Datacom security technologies, with the NGFW deployed as the central security component between the external Internet and the internal university network. The campus infrastructure was logically divided into three main security zones: Trust, DMZ, and Untrust. The Trust zone included internal users and protected university resources, while the DMZ contained publicly accessible services and the Untrust zone represented external networks. Such segmentation enables security policies to be applied according to the trust level of each network segment [6].

DPI was used to identify applications and analyze network traffic beyond basic IP addresses, protocols, and port numbers. Application-level inspection provides additional information for traffic classification and enables security policies to be applied according to the actual application generating the traffic [9]. The NGFW also integrated signature-based IDS/IPS mechanisms to detect and block known malicious activities [7]. The combination of DPI, IDS/IPS, ACLs, and security policies provides a multilayered security model for protecting university network resources.



Pic 1.1 Overall Architecture of the Investigated Higher Education Institution
Corporate Network with NGFW and DPI

Network Architecture and Security Model

The proposed security model was implemented using Huawei Datacom security technologies, with the NGFW positioned between the external Internet and the internal university network. The infrastructure was divided into three security zones: Trust, DMZ, and Untrust. This segmentation allows security policies to be applied according to the security requirements of each network segment [6].

DPI was used to identify applications and analyze traffic beyond basic IP addresses, protocols, and ports. The NGFW also integrated IDS/IPS mechanisms to detect and block malicious activities [7]. The combination of DPI, IDS/IPS, ACLs, and security policies provided a multilayered security model for the university network [9].

Data Collection and Experimental Procedure

A controlled virtual environment was created to simulate typical university network traffic and security events, including HTTP/HTTPS traffic, unauthorized access attempts, network scanning, and malicious application-layer traffic.

Suspicious traffic through commonly permitted ports was also tested to evaluate the effectiveness of DPI.

Two configurations were compared: a traditional stateful firewall without DPI and an NGFW with DPI and IDS/IPS enabled. Detection time, detected attacks, blocked connections, and successful breaches were recorded and compared under similar network conditions [7].

Data Analysis Methods

To analyze the experimental results, quantitative metrics were utilized to compare the efficiency of traditional port-based filtering against a DPI-based Next-Generation Firewall (NGFW) [9].

The primary research metrics used for evaluation are defined as follows:

$$DR = \frac{N_{detected}}{N_{total}} \times 100\%$$

where $N_{detected}$ represents the number of successfully mitigated or dropped attack connections, and N_{total} represents the total number of executed test attacks.

Detection Time (DT): The time elapsed from the exact moment an attack is initiated until it is successfully identified by the security system.

Detection Rate (DR): The percentage of attacks successfully detected by the system out of the total number of simulated threat vectors.

Block Rate (BR): The percentage of attacks that were not only successfully detected but also actively blocked by the security fabric (NGFW/IPS). This metric evaluates the active mitigation capability of the perimeter defense and is calculated as follows:

$$BR = \frac{N_{blocked}}{N_{total}} \times 100\%$$

where $N_{blocked}$ represents the number of successfully mitigated or dropped attack connections, and N_{total} represents the total number of executed test attacks.

In addition, the total number of successful network penetrations was compared across both architectural configurations. Based on these observed values, the

percentage reduction in successful security breaches following the deployment of the DPI-based NGFW was calculated.

To evaluate the enhancement in security responsiveness and threat visibility acceleration, a comparative performance improvement metric was utilized:

$$\Delta DT = \frac{DT_{\text{traditional}} - DT_{\text{ngfw}}}{DT_{\text{traditional}}} \times 100\%$$

where $DT_{\text{traditional}}$ represents the Detection Time recorded under the traditional stateful firewall topology, and DT_{ngfw} represents the Detection Time achieved by the Next-Generation Firewall with deep packet inspection enabled.

The obtained indicators were utilized to determine the impact of Deep Packet Inspection (DPI) on threat detection speed, the efficiency of blocking malicious traffic, and the overall security resilience of the Higher Education Institution (HEI) corporate network [7].

The experimental results demonstrated a clear improvement in network security after implementing the DPI-based NGFW. The attack detection time decreased from 10 seconds with the traditional firewall to 6.5 seconds with the NGFW, representing a 35% improvement in detection speed.

The number of successful network breaches decreased from 25 to 2. This corresponds to a 92% reduction in successful breaches. The results confirm that DPI, combined with application identification and IDS/IPS, improves both threat detection and attack prevention.

The obtained results demonstrate that DPI-based NGFW provides better protection than traditional stateful firewall filtering. The 35% improvement in detection speed indicates that application-level traffic analysis enables threats to be identified more rapidly, while the 92% reduction in successful breaches demonstrates improved prevention of unauthorized and malicious traffic.

However, the experiment was conducted in a controlled virtual environment and may not fully represent the complexity of a production university network. Further

testing with real network traffic and a larger number of attack scenarios would provide more comprehensive results.

This study demonstrated the effectiveness of Deep Packet Inspection within a Next-Generation Firewall for securing HEI corporate networks. Compared with traditional firewall filtering, the proposed model improved detection speed by 35% and reduced successful network breaches by 92%.

The results indicate that DPI, application identification, and IDS/IPS can provide a more effective multilayered security approach for modern university networks. Future research should evaluate the proposed model using real-world traffic and larger-scale network environments.

References

1. [1] O. Afolalu and M. S. Tsoeu, "Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions," *Future Internet*.
2. [2] S. Furnell and N. Rajendran, "Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review," *Global Knowledge, Memory and Communication*, vol. 73, no. 12, 2022.
3. [3] K. A. Scarfone and P. Hoffman, "Guidelines on Firewalls and Firewall Policy," *NIST Special Publication 800-41 Rev. 1*, National Institute of Standards and Technology, 2009.
4. [4] K. A. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST Special Publication 800-94*, National Institute of Standards and Technology, 2007.
5. [5] A. Mohile, "Next-Generation Firewalls: A Performance-Driven Approach to Contextual Threat Prevention," *International Journal of Computer Technology and Electronics Communication*.

6. [6] A. Azab, M. Khasawneh, S. Alrabaaee, K.-K. R. Choo, and M. Sarsour, "Network Traffic Classification: Techniques, Datasets, and Challenges," *Digital Communications and Networks*.
7. [7] M. B. Barruga, "Systematic Review of Cybersecurity Frameworks for Higher Education Institutions: Characteristics, Components, and Challenges," *International Journal of Applied Mathematics*.
8. [8] H. M. Baleid and M. F. Abdullah, "Cybersecurity in Higher Education: A Systematic Review of Threats, Challenges, and Mitigation Strategies," *Journal of Science and Technology*.
9. [9] K. Bwiino, G. K. Mayoka, L. Nkamwesiga, and M. Nyamadi, "A Systematic Literature Review of Information Security Practices in Higher Education Contexts," *IET Information Security*, vol. 2026.