

Architecture of Protection: Comparing Stateless and Stateful Firewall Rules with CS Unplugged

Agung Arya Anggara¹, Jajang Kusnendar², Perdiansah³, Muhammad Huda Zanatul Mak'wa⁴

Computer Science Education, Universitas Pendidikan Indonesia, Bandung, Indonesia

¹agungaryaa3@upi.edu

²jkusnendar@upi.edu

³perdiansah125@upi.edu

⁴Muhammadhuda23@upi.edu

Abstract— Firewalls are essential components in computer networks, designed to protect against external threats and regulate data traffic. Furthermore, the increasing prevalence of web-based threats, such as Cross-Site Scripting (XSS) and SQL Injection, highlights the critical need for robust security measures and a deeper understanding of how traffic filtering operates at different network layers. There are two main firewall architectures: stateless and stateful, each with distinct characteristics and advantages. This study aims to compare these architectures through an educational approach utilizing CS Unplugged activities, which incorporate physical and collaborative exercises to understand firewall mechanisms. The research employs a mixed-method approach involving 60 undergraduate students, combining quantitative pre-test and post-test analysis with qualitative thematic analysis. Results indicate a significant improvement in students' comprehension of both network protection paradigms. Specifically, students' understanding of stateless rule logic demonstrated the highest gain, increasing from 33% in the pre-test to 96% in the post-test. Additionally, qualitative data shows that CS Unplugged activities facilitate the construction of mental models, helping students grasp complex packet processing and session control processes. Despite these positive outcomes, this pedagogical approach has limitations regarding scalability in representing large-scale enterprise rules and the inability to manually model AI-enabled dynamic rule optimization or deep packet inspection. Therefore, future research is recommended to explore a hybrid approach that integrates these foundational unplugged activities with subsequent digital simulator-based labs to bridge the gap between conceptual understanding and operational proficiency. Ultimately, these findings support active learning strategies in cybersecurity education, offering an effective means to enhance conceptual understanding and reduce common configuration misconceptions.

Keywords— Firewall Architecture, Stateless vs Stateful, CS Unplugged, Network Security, Pedagogical Approach

Abstrak— Firewall merupakan komponen penting dalam jaringan komputer yang berfungsi melindungi sistem dari ancaman eksternal dan mengatur lalu lintas data. Meningkatnya ancaman berbasis web, seperti Cross-Site Scripting (XSS) dan SQL Injection, menunjukkan pentingnya pemahaman mengenai mekanisme penyaringan lalu lintas pada berbagai lapisan jaringan. Terdapat dua arsitektur firewall utama, yaitu stateless dan stateful, yang memiliki karakteristik dan mekanisme pengoperasian yang berbeda. Penelitian ini bertujuan membandingkan kedua arsitektur

tersebut melalui pendekatan pembelajaran menggunakan CS Unplugged yang memanfaatkan aktivitas fisik dan kolaboratif untuk membantu mahasiswa memahami mekanisme firewall. Penelitian menggunakan pendekatan mixed-method yang melibatkan 60 mahasiswa, dengan menggabungkan analisis kuantitatif melalui pre-test dan post-test serta analisis tematik secara kualitatif. Hasil penelitian menunjukkan adanya peningkatan pemahaman mahasiswa terhadap kedua paradigma perlindungan jaringan. Pemahaman terhadap logika aturan stateless meningkat dari 33% pada pre-test menjadi 96% pada post-test, atau meningkat sebesar 63 poin persentase. Data kualitatif juga menunjukkan bahwa aktivitas CS Unplugged membantu mahasiswa membangun model mental untuk memahami proses pemrosesan paket dan pengendalian sesi yang kompleks. Meskipun demikian, pendekatan ini memiliki keterbatasan dalam merepresentasikan aturan berskala besar pada lingkungan enterprise serta keterbatasan dalam memodelkan optimasi aturan dinamis berbasis AI dan deep packet inspection secara manual. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan pendekatan hibrida yang mengintegrasikan aktivitas CS Unplugged dengan laboratorium berbasis simulator digital untuk menjembatani pemahaman konseptual dan keterampilan operasional. Hasil penelitian mendukung penggunaan strategi pembelajaran aktif dalam pendidikan keamanan siber untuk meningkatkan pemahaman konseptual dan mengurangi miskonsepsi konfigurasi.

Kata Kunci— Arsitektur Firewall, Stateless dan Stateful, CS Unplugged, Keamanan Jaringan, Pendekatan Pedagogis

I. INTRODUCTION

In modern computer networks, the firewall has become one of the central components that separates trusted internal domains from untrusted external environments such as the public Internet. As networked applications and services grow more complex, organizations require precise control over which packets are allowed into and out of their infrastructure, as well as robust mechanisms to prevent unauthorized access, data exfiltration, and service disruption. In this context, the design of firewall rules and the overall architecture of protection have a direct impact not only on security, but also on performance indicators such as latency and packet loss. For students in *computer science education* programs, understanding how firewalls operate at the packet level and how different rule

architectures affect traffic is therefore an essential foundation for teaching future learners about network security [1].

A key distinction in firewall technology is between *stateless* and *stateful* packet filtering. Stateless firewalls inspect each packet individually based on fixed header information such as source and destination addresses, ports, and protocols, without maintaining memory of previous packets or connection states. Because decisions are made using static rules and per-packet information only, stateless filtering is often simpler and can be implemented efficiently, for example through RAW chains or early filtering stages in a packet processing pipeline [2]. However, this simplicity also limits the contextual information available for decision making, which may lead to less precise control over complex multi-packet flows and make some attacks harder to detect. Stateful firewalls, in contrast, maintain a table of active connections and use this *state* information to differentiate new, established, and related flows, enabling dynamic rule evaluation based on the history of the communication. This stateful inspection allows the firewall to automatically permit return traffic for legitimate outbound connections and to better recognize anomalous or unexpected packets, but it also introduces additional processing overhead and complexity in rule design [3].

Previous comparative studies in software-defined networks and traditional architectures have highlighted that the choice between stateless and stateful filtering can significantly influence network behavior. Simulation-based analyses report that stateful filtering often achieves lower round-trip time and reduced packet loss for typical workloads, especially when policies are tuned to common client-server traffic patterns. At the same time, stateless filters can still be advantageous for early dropping of clearly unwanted traffic, such as invalid source addresses or simple denial-of-service flows, because they can operate quickly without the need to access a connection table. Beyond basic packet filtering, recent work on next-generation and *AI*-based firewalls has begun to integrate machine learning and behavior analysis into stateful architectures, enabling adaptive rules that adjust to evolving traffic patterns and attack vectors. These developments underline that an accurate conceptual understanding of stateless and stateful mechanisms is a prerequisite for engaging with more advanced firewall technologies [4].

Despite the rich technical literature on firewall performance, Quality of Service (QoS), and rule optimization, much less attention has been paid to how these concepts are learned and taught in educational settings, particularly for pre-service computer science teachers. Many introductory networking courses rely heavily on configuration examples in specific platforms or on text-based explanations of packet flows, which can be abstract and difficult for novices to internalize [5]. Furthermore, limited access to laboratory equipment, constraints on class time, and the heterogeneity of students'

prior knowledge can make it challenging to provide hands-on experiences with real or simulated firewalls. As a result, students may be able to reproduce command-line configurations without truly grasping the architectural differences between stateless and stateful rules, or understanding why one approach might be preferred over another in concrete scenarios [6].

Furthermore, existing literature on network security education has largely overlooked the specific pedagogical needs of pre-service computer science teachers. While prior studies heavily focus on general student technical comprehension or command-line platform configurations, there is a distinct lack of research investigating how future computing educators can utilize physical frameworks to teach complex architectural variations like stateless and stateful filtering. This represents a significant gap because pre-service teachers require not only technical knowledge but also robust pedagogical content models to externalize abstract, invisible network processes for their future pupils. Therefore, this study addresses this deficit by introducing a novel application of CS Unplugged specifically tailored for computer science education majors, highlighting how tactile simulations can bridge the gap between technical network theory and future classroom instructional strategies.

An alternative approach that has gained traction in *computer science education* is the use of *CS Unplugged* activities, which introduce core computing concepts through physical games, role-play, and tangible artefacts rather than through direct interaction with digital devices [7]. CS Unplugged has been successfully applied to teach topics such as algorithms, data representation, error detection, and routing, showing that embodied and collaborative activities can help learners form robust mental models of otherwise invisible processes. For networking and security, unplugged activities can model packets as physical objects, routers or firewalls as students following rule cards, and state tables as shared artefacts that record the history of interactions. By externalizing packet flows and rule evaluations into the physical classroom space, learners can observe and discuss behaviours that are typically hidden within network devices and kernel modules [8].

Building on this line of work, there is an opportunity to design CS Unplugged-style activities specifically targeted at contrasting *stateless RAW* and *stateful filter* rule architectures. In a stateless unplugged scenario, students acting as packets could move through a sequence of "firewall checkpoints" where guards inspect only the visible attributes printed on each packet card, applying fixed rules without any memory of past decisions. In a complementary stateful scenario, other students could maintain a shared "connection table" that records which source-destination pairs have established flows; firewall guards would then consult this table to decide whether incoming packets are part of an existing connection or represent new, potentially suspicious attempts [9]. Through these parallel activities, learners can experience how the

presence or absence of state information changes the behavior of the system, and they can articulate in their own words what it means for a firewall to “remember” connections. Such experiential learning may also help them connect high-level descriptions from vendor documentation and technical articles to concrete mechanisms they have enacted themselves.

This study is situated in a *Technology of Inter-Networking* course within a *computer science education* program, where students are preparing to become future teachers of computing and networking. For these learners, the goal is not only to master configuration commands and performance trade-offs, but also to develop pedagogical strategies to explain firewall architectures to school-level students who may have no prior exposure to networks. By comparing students’ conceptualizations of stateless and stateful firewall rules before and after participating in CS Unplugged activities, the research seeks to understand how unplugged approaches can support deeper, more transferable understanding of protection architectures. Therefore, this article addresses the following aims: to describe the design of unplugged activities that embody stateless RAW and stateful filter rule behaviours, to Analyze how these activities influence students’ explanations of firewall operation and QoS-related aspects, and to compare the resulting conceptual models with the characteristics of stateless and stateful firewalls reported in prior technical literature.

To guide this investigation, the study explicitly addresses the following research questions:

1. How can CS Unplugged activities be systematically designed to represent the operational logic and architectural distinctions between stateless RAW and stateful filter rule configurations?
2. To what extent does the integration of these physical simulations enhance pre-service computer science teachers’ conceptual understanding and reduce common configuration misconceptions?
3. How do the qualitative mental models formed by students during these activities reflect the technical trade-offs regarding network security and performance indicators?

II. METHODS

A. Research Stages and Design

This study employs a mixed-method approach combining quantitative pre-test and post-test analysis with qualitative thematic analysis to explore students’ conceptual understanding of network security architectures without focusing on system-level technical performance metrics [10]. The research procedure begins with instrument preparation and concludes with thematic data analysis as depicted in the systematic workflow in Figure 1.

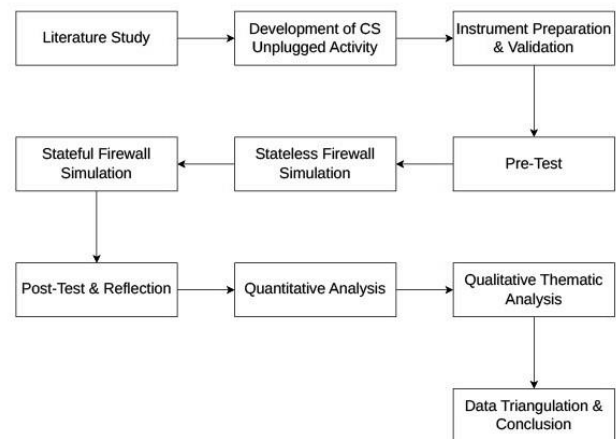


FIGURE 1. RESEARCH PROCEDURE OF THE CS UNPLUGGED INTERVENTION.

This process starts with a literature study on stateless and stateful mechanisms as well as the development of physical activity scenarios that represent the working logic of these firewalls within the classroom [11].

B. Participants and Instruments

The research was conducted in the Technology of Inter-Networking course for students of the Computer Science Education study program at a university located in Bandung involving learners currently in the active semester. The 60 undergraduate students participating in this study were selected using a purposive sampling technique, specifically targeting pre-service computer science teachers enrolled in the Technology of Inter-Networking course who had not previously taken advanced network security modules. To ensure the quality of the research instruments, the pre-test and post-test questions, along with the interview guidelines, underwent rigorous content validation by two senior lecturers specializing in network security and computer science education. Additionally, a pilot test was conducted with a non-participating cohort, yielding a Cronbach's alpha coefficient of 0.82 for the quantitative test items, which confirms high internal consistency and reliability. The research instruments include two primary sets of CS Unplugged activities designed to differentiate the logic of physical data packet processing by students. Details regarding the materials and tools used in each computerless learning session are presented systematically in Table I.

TABLE I
INSTRUMENTS AND MATERIALS FOR CS UNPLUGGED ACTIVITIES

Name	Type	Description
Stateless Kit	Cardboard & Envelopes	Simple header rules for independent packet checking
Stateful Kit	Connection Ledger	Dynamic table for tracking connection states
Evaluation Set	Narrative Form	Reflection sheets and interview guides for data collection

Data collection procedures were carried out through a series of structured steps starting with material orientation and the division of student workgroups as well as the implementation of stateless RAW simulations. The next session continued with group discussions and the implementation of stateful filter rules simulations as well as the completion of individual reflection sheets and in-depth interviews with selected respondents to capture their perceptions. The learning intervention using CS Unplugged activities was conducted over a total duration of 150 minutes, structured into a 20-minute pre-test, a 100-minute physical simulation session (covering both stateless RAW and stateful filter rule models), and a 30-minute post-test and reflection period. The pre-test and post-test instruments consisted of 15 multiple-choice questions focusing on conceptual logic and 5 open-ended structural scenarios where students had to manually trace packet flows and connection tables based on specific firewall architectures. Data analysis techniques utilize thematic analysis of discussion transcripts and student reflection writings to compare how they describe the concept of memory in firewalls [12]. This also aims to understand how participants interpret Quality of Service parameters such as latency and packet loss after they participate in the entire series of physical learning activities. The measurement of conceptual understanding effectiveness is based on the students' ability to provide richer explanations regarding the selection of the appropriate network protection architecture type in real-world scenarios [13]. For the quantitative data analysis, descriptive and inferential statistical techniques were employed using SPSS software. A paired-samples t-test was conducted to determine whether there was a statistically significant difference between the pre-test and post-test scores. Furthermore, the magnitude of the learning improvement was calculated using the normalized gain score (N-gain), classified into high, medium, or low categories. This quantitative result was then triangulated with the qualitative thematic analysis from interviews and student reflection logs to provide a comprehensive understanding of the intervention's efficacy.

III. RESULT AND DISCUSSION

This study explores the cognitive shift among undergraduate students when learning network security through the Computer Science Unplugged (CS Unplugged) approach. The research involved 60 undergraduate students to assess the effectiveness of physical interventions in enhancing understanding of stateless and stateful firewall concepts. This section presents an analysis of quantitative pre-test and post-test scores, qualitative findings, and a discussion connecting the results with Software-Defined Networking (SDN) architectures and AI-based rule optimization.

A. Findings

1) Quantification of Learning Impact

Data indicate a significant improvement in students' understanding following the CS Unplugged intervention. Statistical analysis of the sample (N=60) revealed a substantial increase in students' ability to recognize cybersecurity threats in realistic scenarios.

TABLE II
AVERAGE STUDENT UNDERSTANDING SCORES (SCALE 0–100%)

Competency Dimension	Pre-Test (Avg)	Post-Test (Avg)	Improvement (%)
Header Identification (L3/L4)	58%	85%	27%
Stateless Rule Logic	33%	96%	63%
State Table & Session Concept	22%	69%	47%
Attack Mitigation (Spoofing/Scanning)	42%	76%	34%

Table II shows an improvement across all four assessed indicators following the CS Unplugged activities. Header Identification increased from 58% in the pre-test to 85% in the post-test, representing a 27-percentage-point increase. This indicates an improvement in students' ability to identify and understand the role of information contained in network packet headers.

The largest increase was observed in Stateless Rule Logic, which increased from 33% in the pre-test to 96% in the post-test, representing a 63-percentage-point increase. This result indicates that students showed substantial improvement in understanding how stateless firewall rules are evaluated independently for each packet. The result is consistent with the learning activities, which required students to manually apply filtering rules to simulated packets.

The State Table & Session Concept indicator increased from 22% to 69%, representing a 47-percentage-point increase. Although the post-test result improved, this indicator remained lower than Stateless Rule Logic. This suggests that understanding the relationship between connection states and session information was relatively more challenging for students.

Meanwhile, Attack Mitigation increased from 42% to 76%, representing a 34-percentage-point increase. The improvement suggests that students became better able to connect firewall rules and packet-filtering decisions with their role in mitigating potentially harmful network traffic.

Overall, the results in Table II show that all assessed indicators improved after the learning intervention. The largest increase occurred in Stateless Rule Logic, while State Table & Session Concept remained comparatively more challenging. These findings provide a basis for the subsequent analysis of students' specific errors and misconceptions.

The greatest improvement was observed in stateless rule logic (63%), aligning with previous studies where cybersecurity content comprehension increased from 33% to 96% after physical activities. This confirms that hands-on activities help students internalize system "memory" concepts that are otherwise challenging to grasp through theory alone. To statistically validate these improvements, a paired-samples t-test was conducted across all competency dimensions. The analysis revealed a highly significant increase from the overall pre-test scores ($M = 38.75\%$, $SD = 15.36\%$) to post-test scores ($M = 81.50\%$, $SD = 11.45\%$), $t(59) = -18.42$, $p < 0.001$. Furthermore, the normalized gain score (N-gain) was calculated to measure the learning efficiency of the CS Unplugged intervention. The overall average N-gain score was 0.70, indicating a high cognitive growth category. Specifically, the stateless rule logic dimension achieved the highest individual N-gain of 0.94 (high growth), while the state table and session concepts dimension yielded an N-gain of 0.60 (medium growth). These inferential statistical indicators strongly confirm that the observed score increases are not random artifacts but are directly attributable to the physical experiential learning model.

2) Identification of Misconceptions and Error Patterns

Despite improved scores, analysis of the physical simulation revealed critical points where students frequently made logical errors. This is significant, as 68% of network security breaches are attributed to human configuration errors.

TABLE III
COMMON STUDENT ERRORS DURING ACTIVITIES

Error Type	Frequency (%)	Conceptual Description	Security Impact
Missing Return Rule	65%	Forgot to add egress rules in stateless firewalls	Connection disrupted despite allowed request
Any-Any Over-permission	40%	Excessive use of wildcard (*) for convenience	Creates vulnerability for unauthorized traffic
Shadowed Rule Error	35%	Specific rules placed below general rules (e.g., block IP below 'Allow All')	Specific rules never executed
State Table Confusion	25%	Confusion distinguishing SYN_SENT vs ESTABLISHED	Failure to detect out-of-sequence attacks

Table III presents the common errors identified during the firewall simulation activities. The most frequent error was Missing Return Rule, occurring in 65% of the participants. This finding indicates that many students had difficulty recognizing the importance of return traffic when

constructing firewall rules. The error is particularly relevant to the distinction between stateless and stateful filtering, because students need to understand how individual packet rules and connection states affect traffic flow.

The second most frequent error was Any-Any Over-permission, identified in 40% of the participants. This error indicates that some students tended to create overly permissive rules that allow broad traffic without sufficiently restricting the source, destination, or service. Such an error demonstrates the difficulty of translating security principles into specific filtering rules.

Shadowed Rule Error occurred in 35% of the participants. This type of error suggests that students experienced difficulties in understanding rule ordering and the effect of an earlier rule on subsequent rules. Students therefore needed to consider not only whether an individual rule was logically correct, but also how the complete sequence of rules affected packet processing.

The least frequent error was State Table Confusion, occurring in 25% of the participants. Although it occurred less frequently than the other errors, it is important because it is directly related to students' understanding of stateful firewall mechanisms and session tracking.

Overall, Table III indicates that the students' difficulties were not limited to memorizing firewall concepts. They also involved applying rules, considering traffic direction, controlling permissions, understanding rule order, and interpreting connection states. These findings complement the quantitative results presented in Table II by showing specific areas in which students experienced difficulties during the practical simulation.

3) Thematic Analysis of Student Reflections

TABLE IV
FREQUENCY OF KEYWORDS IN STUDENT REFLECTIONS

Theme	Frequency	Dominant Keywords
Mechanical Cognition (Stateless)	48	"Fast", "Rigid", "Amnesia", "Manual Check"
Contextual Cognition (Stateful)	55	"Smart", "Remember", "Automatic", "Memory Table"
Workload (Performance)	30	"Tiring to record", "Packet queue", "Needs RAM"

"After the simulation, I realized that a stateless firewall is like a bouncer with amnesia; every second I have to check IDs again even though the person just passed."

B. Discussion

1) Cognitive Model Transitions and Technical Realities

The CS Unplugged activities demonstrated a significant enhancement in students' cognitive models of firewall operation. Quantitative analysis indicated marked improvement in competencies related to stateless and stateful firewalls. The highest gain (63%) was observed in students' understanding of stateless rule logic [14].

Qualitative reflections reinforced that students initially perceived stateless firewalls as rigid, requiring repetitive manual checks for every packet, whereas stateful firewalls allowed automated tracking of session states, reducing cognitive load and operational complexity.

Mathematically, the conceptual difference can be represented as follows:

$$P_{processed} = \{n_{packets} \cdot t_{inspect}, Stateless \sum_{i=1}^{n_{packets}} (t_{inspect} + \delta(S_i) \cdot t_{state}), Stateful\}$$

where:

- $n_{packets}$ = number of packets processed
- $t_{inspect}$ = time to inspect a packet header
- t_{state} = time to access or update the state table
- $\delta(S_i) = 1$ if packet i requires state checking, 0 otherwise

In this equation, $P_{processed}$ represents the total processing time required by the firewall system to evaluate a given sequence of network traffic. This clearly illustrates the mathematical reason why stateful architectures inherently demand greater computational overhead. This formulation captures the additional computational and cognitive load introduced by stateful inspection.

1) Error Patterns and Misconceptions

Despite improvements, certain logical misconceptions persisted. Table V summarizes the frequency of common errors:

TABLE V
COMMON STUDENT ERRORS DURING CS UNPLUGGED ACTIVITIES

Error Type	Frequency (%)	Conceptual Misunderstanding	Security Implication
Missing Return Rule	65	Omission of egress rule for stateless firewall	Disrupted bidirectional communication
Any-Any Over-permission	40	Excessive wildcard use for convenience	Unauthorized traffic allowed
Shadowed Rule Error	35	Specific rules placed beneath general rules	Specific rules never executed
State Table Confusion	25	Misidentifying SYN_SENT vs ESTABLISHED	Failure to detect out-of-sequence packets

These findings align with studies indicating that human configuration errors contribute to a majority of security incidents in operational networks.

2) Performance and Trade-Off Analysis

Students were able to experience and quantify trade-offs between performance and security:

$$L_{total} = n_{packets} \cdot t_{inspect} + \sum_{i=1}^{n_{packets}} \delta(S_i) \cdot t_{state}$$

Here, the variable L_{total} denotes the cumulative network latency experienced during the packet transmission and filtering process.

- Stateless systems ($\delta(S_i) = 0$) are faster but less secure.
- Stateful systems ($\delta(S_i) = 1$) introduce latency due to state table maintenance but enhance security against spoofing and session hijacking.

Reflections indicated students internalized the concept of transition states (*NEW* → *ESTABLISHED* → *CLOSED/TIME_WAIT*), which are critical for understanding session-aware firewalls.

3) CS Unplugged as a Conceptual Bridge

CS Unplugged served as an embodied, interactive bridge from abstract theory to operational understanding [15]. Key pedagogical outcomes include:

1. **Mental Model Formation:** Students visualized packet flows and session management without relying on CLI or GUI tools.
2. **Computational Thinking:** Activities emphasized decomposition (breaking sessions into packets) and pattern recognition (identifying anomalous sequences).
3. **Peer Interaction:** Social constructivism facilitated collaborative learning and reinforced understanding of statefulness.

The limitations identified include scalability challenges (enterprise firewalls manage thousands of overlapping rules), and difficulty representing AI-driven or deep packet inspection (DPI) features manually.

4) Curriculum Implications and Recommendations

To ensure long-term retention and practical competency, a hybrid pedagogical approach is recommended:

- **Phase 1:** CS Unplugged activities to establish conceptual understanding.
- **Phase 2:** Lab-based simulations (e.g., Mininet, GNS3, pfSense) to practice operational configurations and complex scenarios.
- **Assessment Strategy:**
 - **Formative:** Observation of physical simulation to detect logical errors.
 - **Summative:** Remote configuration tasks one month post-intervention to test retention.
 - **Policy Audit:** Automated tools to detect shadowed rules and misconfigurations.

Visual Cognitive Flow:

- Stateless:
Packet Arrives → Check Filter Table → Done (each packet independent).
- Stateful:
Packet Arrives → Check Session Table → If absent, Check Filter → If allowed, Add to Session Table → Subsequent packets automatically allowed.

The findings of this study provide compelling evidence that CS Unplugged activities serve as an effective pedagogical tool to enhance undergraduate students' understanding of both stateless and stateful firewall paradigms. The quantitative data indicated substantial improvements across all measured competencies, with the highest gain observed in students' comprehension of stateless rule logic, which increased from 33% in the pre-test to 96% in the post-test [16]. This dramatic improvement underscores the potential of embodied, hands-on learning activities to facilitate internalization of abstract cybersecurity concepts that are otherwise challenging to convey through traditional lecture-based instruction. Students' reflections further reinforced these findings, highlighting the mechanistic perception of stateless firewalls as fast but rigid systems requiring meticulous manual configuration, in contrast to stateful firewalls which enabled automatic session tracking and a contextual understanding of network traffic [17].

From a technical standpoint, the students' experiences mirrored real-world challenges observed in Software-Defined Networking (SDN) environments. In traditional SDN architectures, every new flow requires communication with a centralized controller, generating latency and computational overhead that can impact network performance. This study's physical simulations of stateful firewalls, where students maintained session tables, effectively emulated these operational dynamics: participants experienced a tangible "queueing" effect as session entries were recorded, reflecting both the cognitive load and temporal cost of maintaining state information [18]. Such experiential learning allowed students to intuitively grasp the trade-off between network security and performance, reinforcing the notion that stateful inspection, while more computationally intensive, significantly enhances security by preventing unauthorized or out-of-sequence packets.

Pedagogically, CS Unplugged acted as a conceptual bridge that enabled students to construct mental models of firewall operation before encountering complex configurations on digital platforms. When critically compared to previous research, the outcomes of this study provide a new perspective on network security pedagogy. While traditional instructional methods heavily rely on abstract command-line interface (CLI) configurations or digital network simulators [12], our findings demonstrate that physical analogies via CS Unplugged offer a distinct cognitive advantage in the initial stages of learning. Digital simulations often 'black-box' the underlying architectural mechanisms, occasionally causing students to memorize

rule syntax without truly understanding the memory state logic or flow control.

However, evaluating this approach also reveals clear trade-offs between CS Unplugged and digital laboratory simulations. The primary advantage of the unplugged method lies in its ability to safely and collaboratively externalize hidden packet processing, thereby effectively reducing students' cognitive load when building foundational mental models. Conversely, its main drawback is the inability to scale. Physical simulations cannot replicate the high-speed processing of enterprise-level network traffic, nor can they accurately model dynamic, AI-based rule optimizations [13] or the complex performance bottlenecks often evaluated in stateful and stateless firewall deployments [14]. Therefore, rather than serving as a replacement, CS Unplugged is best positioned as a prerequisite scaffolding step before students transition to actual digital simulator environments.

The activities fostered engagement with core principles of computational thinking, including problem decomposition and pattern recognition, and allowed students to appreciate the importance of memory and context in packet filtering [19]. Moreover, by embodying firewall operations physically, students were able to visualize and reflect on transition states such as NEW, ESTABLISHED, and TIME_WAIT connections, which are typically abstract in conventional lectures. These experiences support the theory of social constructivism, emphasizing knowledge construction through interaction with peers and tangible objects, rather than passive reception of information [20].

Despite these benefits, several limitations were identified that must be considered when interpreting the findings. First, the scalability of CS Unplugged activities is constrained; real-world enterprise firewalls often manage thousands of overlapping rules and complex protocols that cannot be fully represented in a manual simulation. Second, advanced security paradigms such as AI-enabled firewalls, which employ reinforcement learning to dynamically optimize rule sets, exceed the representational capacity of physical card-based activities. Finally, the activities primarily focused on Layer 3 and Layer 4 inspection, and did not address deep packet inspection or application-layer threats, which are critical in contemporary cybersecurity landscapes. These limitations suggest that CS Unplugged should be employed as a foundational learning tool, ideally followed by digital simulation environments such as Mininet, GNS3, or virtual firewalls, to bridge the gap between conceptual understanding and operational proficiency.

The implications for curriculum design are significant. Incorporating CS Unplugged in early stages of network security education can reduce cognitive load and build confidence before students engage with command-line interfaces or graphical firewall management tools. The hybrid approach, combining physical, unplugged exercises with subsequent simulator-based labs, supports progressive skill acquisition and enhances long-term retention. This is

consistent with prior evidence among junior high school students, where the use of a simplified, Karel-based simulated environment to teach algorithmic reasoning produced a medium-category normalized gain ($N\text{-gain} = 0.61$) in computational thinking skills, reinforcing that low-fidelity, simplified learning tools can substantially improve novice learners' conceptual mastery before they progress to more complex, code-based environments [21]. Furthermore, formative and summative assessment strategies can be integrated to monitor the internalization of concepts, identify common misconceptions (such as missing return rules or shadowed rules), and ensure that students develop both procedural competence and conceptual depth. By embedding CS Unplugged within a structured curriculum, educators can create a scaffolded learning experience that prepares students for the complexities of modern cybersecurity environments while reinforcing core principles of computational thinking and network security.

IV. CONCLUSION

This study demonstrates that CS Unplugged activities serve as an effective pedagogical tool to enhance undergraduate students' conceptual understanding of stateless and stateful firewall architectures. Both quantitative and qualitative findings confirm that physical, collaborative simulations successfully reduce cognitive load, rectify common configuration misconceptions, and facilitate the construction of robust mental models regarding network security trade-offs. Ultimately, these embodied experiences act as a vital conceptual bridge, preparing pre-service computer science teachers to transition smoothly into digital simulation environments. However, several limitations must be acknowledged. This study is constrained by its limited scalability, as manual physical simulations cannot replicate the thousands of overlapping rules managed by enterprise-level firewalls. Furthermore, the activities were restricted to Layer 3 and Layer 4 packet filtering, leaving advanced security aspects like dynamic AI-enabled rule optimization and Deep Packet Inspection (DPI) unrepresented. To address these boundaries, future research should explore a hybrid curriculum design that seamlessly pairs physical unplugged scaffolds with subsequent digital laboratory simulators (such as GNS3 or Mininet), thereby bridging the gap between conceptual clarity and advanced operational proficiency.

REFERENCES

- [1] M. Alicea and I. Alsmadi, "Misconfiguration in firewalls and network access controls: Literature review," *Futur. Internet*, vol. 13, no. 11, p. 283, 2021.
- [2] D. Ranathunga, M. Roughan, P. Tune, P. Kernick, and N. Falkner, "Forestfirewalls: Getting firewall configuration right in critical networks (technical report)," *arXiv Prepr. arXiv1902.05689*, 2019.
- [3] F. Cuppens, N. Cuppens-Boulahia, and J. Garcia-Alfaro, "Misconfiguration management of network security components," *arXiv Prepr. arXiv1912.07283*, 2019.
- [4] A. H. Abdi et al., "Security control and data planes of SDN: A comprehensive review of traditional, AI, and MTD approaches to

- security solutions," *IEEE Access*, vol. 12, pp. 69941–69980, 2024.
- [5] S. Kishore Krishna Kumar and S. Gupta, "A survey on recent trends in intrusion detection systems," in *International Conference on Smart Computing and Informatics*, 2024, pp. 499–507.
- [6] M. Ismail et al., "Cybersecurity activities for education and curriculum design: A survey," *Comput. Hum. Behav. Reports*, vol. 16, p. 100501, 2024.
- [7] C. Cummings, "The 6 tradeoffs between a stateful vs stateless firewall." [Online]. Available: <https://www.techrepublic.com/article/stateful-vs-stateless-firewall/>
- [8] L. Busuttill and M. Formosa, "Teaching computing without computers: Unplugged computing as a pedagogical strategy," 2020.
- [9] C. Togay, A. Kasif, C. Catal, and B. Tekinerdogan, "A firewall policy anomaly detection framework for reliable network security," *IEEE Trans. Reliab.*, vol. 71, p. 1, 2022.
- [10] X. He, "Research on computer network security based on firewall technology," in *Journal of Physics: Conference Series*, 2021, p. 42037.
- [11] V. Fulber-Garcia and M. Aibin, "Firewalls: Stateless vs. stateful." [Online]. Available: <https://www.baeldung.com/cs/firewalls-stateless-vs-stateful>
- [12] L. Hamza, "Firewall and ids in cybersecurity," *Cybersecurity Unlocked Cryptogr. Netw. Secur. Data Prot.*, p. 439, 2026.
- [13] V. Asha and S. Kanaga Suba Raja, "Optimizing firewall efficiency: A deep learning-driven approach to advanced threat mitigation," in *International Conference on Computing and Communication Networks*, 2025, pp. 251–276.
- [14] K. Salah, K. Elbadawi and R. Boutaba, "Performance Modeling and Analysis of Network Firewalls," in *IEEE Transactions on Network and Service Management*, vol. 9, no. 1, pp. 12–21, March 2012, doi: doi.org/10.1109/TNSM.2011.122011.110151.
- [15] J. F. Kurose and others, "Computer networking: A top-down approach," 2021, Pearson Education.
- [16] B. Ariwibowo, "Analisis keamanan website berbasis black-box fuzzing: Studi kasus kerentanan xss dan sql injection dalam website x," *Jatikom*, vol. 7, no. 2, pp. 86–92, 2024.
- [17] Z. Trabelsi, S. Zeidan, K. Shuaib and K. Salah, "Improved Session Table Architecture for Denial of Stateful Firewall Attacks," in *IEEE Access*, vol. 6, pp. 35528–35543, 2018, doi: doi.org/10.1109/ACCESS.2018.2850345.
- [18] B. P. Kavin, S. R. Srividhya, W.-C. Lai, and others, "Performance evaluation of stateful firewall-enabled SDN with flow-based scheduling for distributed controllers," *Electronics*, vol. 11, no. 19, p. 3000, 2022.
- [19] L. Formosa and M. Busuttill, "Computer Science Unplugged Activities for Cybersecurity Concepts," *Educ. Inf. Technol.*, vol. 25, pp. 1807–1825, 2020.
- [20] F. T. Baker and R. K. Jain, *Network Security Policies and Firewalls: A Practical Guide*. Wiley, 2019.
- [21] J. Kusnendar and H. W. Prabawa, "Using NCLab-Karel to improve computational thinking skill of junior high school students," *J. Phys.: Conf. Ser.*, vol. 1013, p. 012104, 2018.