

# Context-Aware Access Control for the SSH Protocol: Beyond Zero-Trust

Sewoong Jeong\*, Cutillas Pardines Mario<sup>†</sup>, Samariddin\* Jaehoon (Paul) Jeong\*, and Utkarsha Jalindar Kshirsagar<sup>‡</sup>

\*Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea

<sup>†</sup>Department of Computer Science and Engineering, University of Alicante, Alicante, Spain

<sup>‡</sup>Department of Computer Science and Engineering, Rochester Institute of Technology, New York, United States of America

Email: {jsw1301, smavlitdinov, pauljeong}@skku.edu

{mcp173}@alu.ua.es {uk9263}@rit.edu

**Abstract**—Software-Defined Networking (SDN) is playing a key role in current network technology by providing greater flexibility and scalability to modern networks. However, SDN also has vulnerabilities to hacking attacks, because its centralized control plane is a possible single point of failure. This paper proposes a novel context-aware access controller framework to automate and simplify the authentication SSH connection. The framework leverages RESTCONF, YANG data models, the OpenDaylight controller, and OpenFlow to support standard-compliant and programmable security operations. By collecting contextual features, the system classifies each connection attempt as trusted or untrusted and then enforces the appropriate path—either direct forwarding or routing through a VPN tunnel. The proposed design improves remote authentication consistency while enhancing security and user experience in SDN-based communications.

**Index Terms**—Software-Defined Networking, Security Management Framework, Hybrid Control, OpenFlow, NETCONF, YANG.

## I. INTRODUCTION

By separating the control and data planes, Software-Defined Networking (SDN) offers centralized control and automation that traditional networks lack. However, this centralized architecture introduces critical vulnerability, making the control plane a single point of failure and a prime target for attacks [1]. In response, researchers are developing countermeasures like machine learning for anomaly detection and standardized frameworks such as NETCONF and YANG for consistent configuration. Despite these advancements, many solutions remain too complex or fragmented for dynamic network contexts. Our proposed framework addresses this gap by providing an integrated, context-aware solution.

## II. RELATED WORK

There is some research which tries to enhance the current authentication system. Wu et al. (2015) [2] proposed unified authentication and management platform with dynamic password opening, single sign-on scheme, and dynamic password algorithm. The research showed the ability for easy application. However, this platform is based on OTP, which is still uncomfortable for majority of human users. Also, this platform aims to be executed in a mobile environment, which is totally different from our research interest. A framework compatible

for the school cluster server is not yet studied. Zohaib et al. (2024) [3] reviewed contemporary network techniques including zero trust VPN (ZT-VPN), and emphasized high latency and low throughput. This research supports our project’s goal, to improve latency. The paper presents a comprehensive cybersecurity framework to enhance IT security and privacy for modern enterprises in remote work environments. However, the authors didn’t discard zero trust behavior of VPN tunnels. Considering prior research, there is a strong need for a new framework which works on SSH connection between server and PC client, which enhances latency by discarding zero trust behavior.

## III. DESIGN

The proposed framework, shown in Fig. 1, is designed to provide adaptive, context-aware access control within a Software-Defined Networking (SDN) environment. Its architecture separates intelligence from forwarding by placing all decision-making logic in a centralized SDN controller, while the data plane remains lightweight and programmable. A context collector first gathers attributes from each login attempt, including MAC and IP addresses, subnet category, geolocation [4], time-of-day, and history [5] information. This context is delivered to the SDN controller through a REST API, where a multi-factor risk engine evaluates the attempt using learned behavioral profiles stored in an internal database.

The controller computes a risk score by combining MAC trust, historical consistency, subnet familiarity, temporal deviation, and geographic patterns. Based on predefined policy thresholds, it determines whether the connection is trusted or requires additional security measures. For trusted connections, the controller installs temporary OpenFlow rules to allow direct forwarding to the server. For untrusted or anomalous attempts, the controller enforces step-up authentication by redirecting traffic through a VPN tunnel.

This design ensures consistent, automated authentication while maintaining SDN’s programmability, enabling scalable security that adapts to user behavior over time.

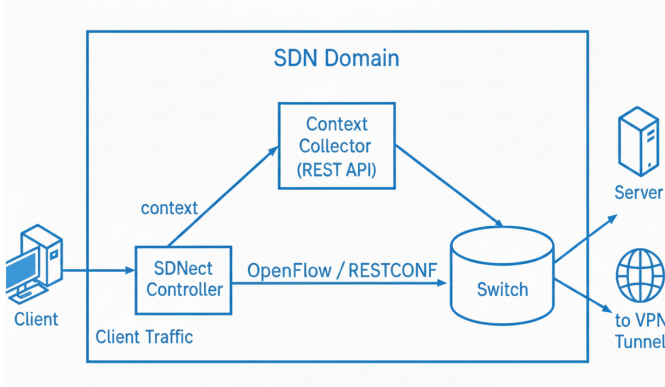


Fig. 1. A Framework of Context-Aware Access Control System.

#### IV. EMULATION RESULTS

This section details the emulation environment along with the results obtained from our experiments.

TABLE I  
EMULATION CONFIGURATION

Parameter	Description
Operating System	Ubuntu 18.04
SDN Controller	OpenDaylight v0.8.4.
Emulation Environment	Mininet v2.2.2.
Topology	Single controller with 1 server, 3 switches and 8 clients
Protocols	OpenFlow 1.3 and RESTCONF, ICMP, TCP
Network Monitoring Information	IP, MAC, history, location, time, and geographical information
Traffic Generation	SSH traffic

##### A. Emulation Setup

To quantify the performance implications of VPN redirection within our context-aware access control framework, we measured SSH-like throughput and latency under varying proportions of VPN-routed hosts. Experiments were conducted in a Mininet [6] SDN emulation environment with OpenDaylight [7] providing network control. Mininet allowed us to emulate SDN behavior and evaluate system responses under controlled conditions, while OpenDaylight's extensibility and OpenFlow support enabled seamless integration with our framework. Table I summarizes the system setup.

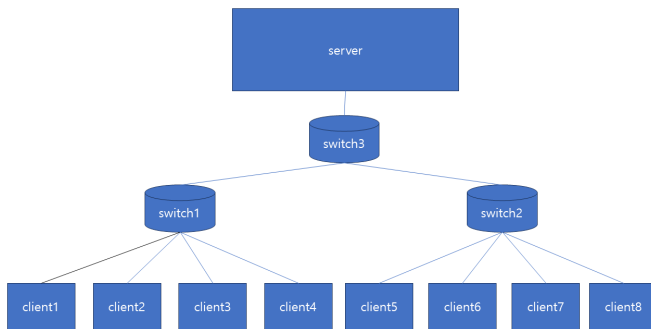


Fig. 2. Simplified Topology

The testbed includes eight client hosts, three OpenFlow switches, and an SSH server. WireGuard was deployed on all hosts to support on-demand VPN tunneling, and only a selected subset of clients was redirected through the tunnel, with the proportion of VPN-routed hosts reduced from 100% to 25% across scenarios. To emulate realistic bottlenecks and highlight the impact of tunnel contention, the server uplink was bandwidth-limited to 100 Mbps using TCLink. Figure 2 illustrates the simplified topology of the testbed.

##### B. Results

This section describes the emulation environment and the results obtained from evaluating the proposed context-aware access control framework. While the prior subsections focused on security attack detection and mitigation, we additionally evaluate the performance impact of VPN-redirection SSH sessions. This performance study highlights the cost of enforcing secure paths and validates that our context-aware controller must selectively enable VPN tunneling only when necessary.

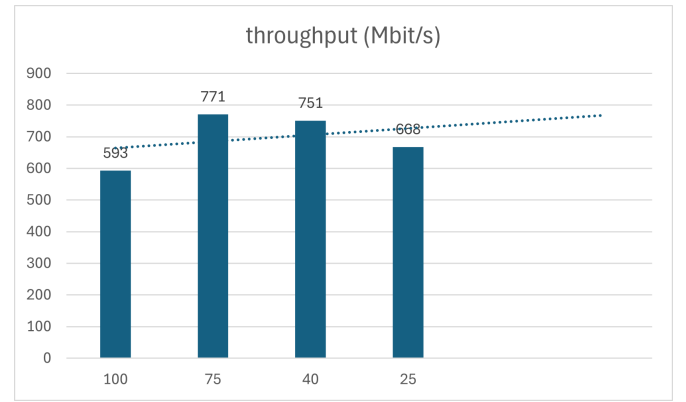


Fig. 3. Throughput plot with VPN ratio

Notably, the configuration in which all clients were forced into the VPN (100% VPN, i.e., a strict Zero-Trust enforcement) yielded the lowest throughput among all scenarios. Every partial-VPN configuration (75%, 50%, and 25%) achieved higher throughput than the fully tunneled case. This indicates that unconditional VPN redirection imposes the greatest performance penalty, while selectively reducing the number of VPN-routed clients alleviates tunnel contention and improves effective bandwidth. The result reinforces our design goal: a Zero-Trust model that blindly tunnels all traffic is inefficient, and context-aware, selective VPN activation provides a more balanced trade-off between security and performance.

Latency results exhibit a clearer pattern. As shown in Fig. 4, latency decreases markedly as fewer hosts participate in the VPN tunnel. With all clients routed through the VPN, the measured latency reached 4.9 ms, but it dropped to 2.3 ms, 1.2 ms, and 1.38 ms as the VPN proportion decreased to 75%, 40%, and 25%, respectively. This inverse relationship indicates that VPN congestion increases queuing delay within the encrypted tunnel, amplifying end-to-end latency. Since direct-path latency measured separately is consistently below

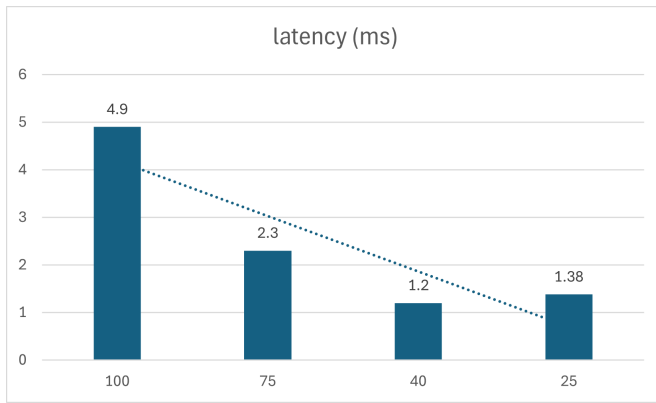


Fig. 4. Latency plot with VPN ratio

0.3 ms, the VPN tunnel introduces an order-of-magnitude increase in RTT even under moderate load.

Fig. ?? shows the detection and mitigation of a port scan attack. In this scenario, a TCP SYN port scan targeting all ports of host h2 was launched from host h5. After detecting the attack, the SDN controller issues drop commands for all packets from the attacker to the switches and generates an XML file to enforce mitigation measures. The XML file specifies actions such as blocking the attacker's IP address and setting a block duration. Since the attack is a TCP SYN scan, the controller configures detection parameters, including a short block duration, connection rate thresholds, and alert thresholds, based on the current network environment.

Overall, the results validate the design motivation behind context-aware VPN redirection. First, latency consistently improves as fewer clients are forced into the VPN, demonstrating that tunnel load directly affects delay. Second, throughput remains lower than the direct path in all cases, confirming that encryption and tunnel processing impose unavoidable overhead. The lack of a strictly monotonic throughput trend stems from TCP dynamics and emulation-environment interactions, but the performance penalty of VPN use is nonetheless apparent.

These findings reinforce that VPN redirection should be applied selectively, only under conditions of elevated risk. Mandatory or excessive VPN routing would degrade user experience without proportional security benefit, whereas context-triggered activation—as implemented in our framework—balances security and performance effectively.

The source code for the implementation of our Context-Aware Access Automation framework and experiment are available at GitHub of <https://github.com/jaehoonpauljeong/Data-Modeling-Group-6-Project>.

## V. CONCLUSION

This paper presented a context-aware access control framework that selectively redirects SSH traffic through a Wire-Guard VPN tunnel based on client risk level. Through emulation in an SDN environment, we showed that while VPN tunneling increases latency and reduces throughput, enforcing it only for high-risk clients achieves a better balance between

security and performance. Our results confirm that a strict 100% VPN—or Zero-Trust-by-tunneling—incurs the highest performance cost, whereas selective VPN activation maintains stronger security with significantly less impact on network efficiency.

Future work includes extending the framework with richer behavioral analytics, broader protocol coverage. Increase of overall throughput more scalable real-time risk assessment mechanisms should be also followed.

## ACKNOWLEDGMENTS

This work was supported by the Data Modeling for Intelligent Network System(ESW7002) in Sungkyunkwan University. Note that Jaehoon (Paul) Jeong is the corresponding author.

## REFERENCES

- [1] J. Arevalo-Herrera, J. C. Mendoza, J. I. M. Torre, T. Zona-Ortiz, and J. M. Ramirez, "Assessing sdn controller vulnerabilities: A survey on attack typologies, detection mechanisms, controller selection, and dataset application in machine learning," *Wireless Personal Communications*, vol. 140, no. 1, pp. 739–775, Feb. 2025. [Online]. Available: <https://doi.org/10.1007/s11277-025-11748-w>
- [2] S. Wu, J. Zou, C. Fan, and X. Zhang, "A unified authentication and management platform based on otp generated by smart phone," in *LISS 2013*, ser. Springer Books. Springer, Mar. 2015, pp. 983–990. [Online]. Available: [https://ideas.repec.org/h/spr/sprchp/978-3-642-40660-7\\_147.html](https://ideas.repec.org/h/spr/sprchp/978-3-642-40660-7_147.html)
- [3] E. Bertino and M. S. Kirkpatrick, "Location-based access control systems for mobile users: concepts and research directions," in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, ser. SPRINGL '11. New York, NY, USA: Association for Computing Machinery, 2011, pp. 49–52. [Online]. Available: <https://doi.org/10.1145/2071880.2071890>
- [4] G. Pavlov and N. Tagarev, "Enhancing cybersecurity through the integration of geographic information systems technologies," *International Journal of Science and Research (IJSR)*, vol. 13, 09 2024.
- [5] H. Sharma, "Behavioral analytics and zero trust," *International Journal of Information Technology and Management Information Systems (IJITMIS)*, vol. 12, no. 1, pp. 63–84, 2021.
- [6] Mininet, "An instant virtual network on your laptop," 2022, [Online]. Available: <http://mininet.org/>.
- [7] OpenDaylight project team, "OpenDaylight sdn controller," 2025, [Online]. Available: <https://www.opendaylight.org/>.