

IMPLEMENTATION AND EVALUATION OF NETWORK-LEVEL ZERO TRUST CONTROLS FOR ENTERPRISE NETWORK SECURITY USING CISCO PACKET TRACER

*Ismail Mahmoud Sifawa, M.O. Adenomon, M.I. Umar

Centre for Cyber Space Studies, Nasarawa State University, Keffi, Nigeria

*Corresponding Author Email Address: mahmoudismail700@gmail.com

ABSTRACT

This study aimed to implement and evaluate selected network-level Zero Trust controls within a simulated enterprise environment using Cisco Packet Tracer to mitigate unauthorized internal communication and lateral movement. A before-and-after experimental design was established across five logical Virtual Local Area Network (VLAN) segments—Finance, Human Resources, Information Technology, Guest, and Server—using Extended Access Control Lists (ACLs), controlled inter-VLAN routing, least-privilege access, and default-deny policy enforcement. Experimental connectivity testing across six documented scenarios demonstrated that all three authorized communication paths remained operational after policy implementation, whereas all three restricted scenarios were successfully blocked. The findings demonstrate that VLAN segmentation alone is insufficient for isolation once inter-VLAN routing is enabled, proving that explicit ACL enforcement is required to achieve effective, policy-based network isolation and prevent lateral movement.

Keywords: Zero Trust, enterprise network security, Cisco Packet Tracer, VLAN segmentation, Access Control Lists, least-privilege access.

INTRODUCTION

The rapid evolution of digital technologies has fundamentally transformed enterprise network environments, enabling organizations to support distributed workforces, cloud computing, Internet of Things (IoT) devices, mobile applications, and interconnected business services. These technological advancements have significantly improved organizational productivity, operational efficiency, and resource accessibility. However, they have also expanded the enterprise attack surface, exposing organizations to increasingly sophisticated cyber threats, including unauthorized access, ransomware, credential theft, insider attacks, and lateral movement across internal networks. Securing enterprise network infrastructures has become a strategic priority for organizations seeking to protect critical information assets while maintaining service availability and business continuity (Gadzali et al., 2023; Yuwono et al., 2024). Traditionally, enterprise security has relied on a perimeter-based security model in which internal users and devices are regarded as trustworthy once authenticated, while external entities are treated as untrusted. This approach has historically been enforced through technologies such as firewalls, Virtual Private Networks (VPNs), and Intrusion Detection and Prevention Systems (IDS/IPS). Although these mechanisms remain important components of enterprise cybersecurity, they are increasingly challenged by

modern computing environments characterized by hybrid work models, cloud services, Bring Your Own Device (BYOD) policies, and highly interconnected enterprise infrastructures (Tanimoto et al., 2023; Shaik, 2025). Once an attacker successfully bypasses the network perimeter through compromised credentials, software vulnerabilities, or insider abuse, unrestricted communication within flat network architectures often enables lateral movement and unauthorized access to sensitive organizational resources (Aithal, 2023; Narayanan et al., 2026).

To address these limitations, the Zero Trust security model has emerged as a modern cybersecurity paradigm founded on the principle of "Never Trust, Always Verify." Rather than assuming implicit trust based on network location, Zero Trust requires continuous verification of users, devices, and communication requests before granting access to protected resources. At the network layer, this is commonly implemented through network segmentation, least-privilege access, and Access Control Lists (ACLs), which collectively reduce unauthorized communication and restrict lateral movement between enterprise network segments (Kang et al., 2023; Arooj et al., 2024). These controls have become increasingly important as organizations seek practical ways to strengthen internal defenses without relying solely on perimeter protection.

Enterprise networks constitute the technological backbone of modern organizations, supporting communication, information sharing, business processes, and access to critical digital resources. The primary objective of enterprise network security is to preserve the confidentiality, integrity, and availability (CIA) of organizational information assets through technical, administrative, and physical security controls (Joseph et al., 2024; Lorenzo et al., 2025). Traditional perimeter protection alone is insufficient against modern ransomware campaigns and insider threats (Kundururu, 2023; Soundappan, 2025). Effective defense requires architectures that continuously validate network communications (Khouri et al., 2024; Afolalu & Tsoeu, 2025). Once attackers gain access, implicit trust allows rapid lateral movement across unsegmented internal networks (Zahedul & Aditya, 2023; Mardiyanto et al., 2026).

Previous literature has explored various security mechanisms supporting Zero Trust principles. Sunkara (2025) reviewed Zero Trust architectures, emphasizing continuous verification and policy-driven access control. Putra et al. (2024) demonstrated the effectiveness of Dynamic ARP Inspection (DAI) using Cisco Packet Tracer to mitigate ARP spoofing. Subhani & Arshad (2025) proposed an IoT networking framework incorporating ACLs, firewalls, and network slicing. Additional foundational studies evaluated multi-protocol enterprise designs (Panta, 2026),

organizational scaling frameworks (Prasanth, 2025), and SME network integration (Liu et al., 2025). However, existing studies largely focus on conceptual frameworks or isolated networking mechanisms rather than integrating and experimentally evaluating a comprehensive set of network-level Zero Trust controls within a unified enterprise environment.

A critical implementation gap exists in the literature: first, many studies remain conceptual; second, simulation studies frequently evaluate single mechanisms rather than an integrated suite of Zero Trust network controls; and third, few studies explicitly compare communication behavior before and after policy enforcement across documented authorized and unauthorized paths. This study addresses these gaps by integrating Virtual Local Area Network (VLAN) segmentation, Extended Access Control Lists (ACLs), and least-privilege access within a unified Cisco Packet Tracer simulation environment. This research primarily evaluates the effectiveness of these combined controls in restricting unauthorized communication and reducing lateral movement across departmental enterprise segments.

MATERIALS AND METHODS

A simulated medium-sized enterprise network was designed and implemented in Cisco Packet Tracer to evaluate selected network-level Zero Trust controls. The architecture consisted of five logical segments: Finance, Human Resources (HR), Information Technology (IT), Guest, and Server. Each segment was assigned a dedicated Virtual Local Area Network (VLAN) and IP subnet to provide logical isolation while allowing controlled inter-VLAN communication based on organizational requirements.

The topology followed a hierarchical structure comprising end-user devices, Layer 2 switches, a multilayer (Layer 3) switch for inter-VLAN routing, and a gateway router representing Internet connectivity. All devices were configured within a single Packet Tracer simulation environment using standard Ethernet links and the IPv4 protocol.

We implemented network segmentation by creating five independent VLANs. Inter-VLAN routing was performed on the Layer 3 switch only after evaluating security policies. The Guest VLAN received the highest level of restriction, while the IT VLAN retained controlled administrative access required for network management.

The Principle of Least Privilege was enforced by granting only the minimum access necessary for authorized functions. Extended Access Control Lists were configured on the Layer 3 switch to filter traffic based on source and destination IP addresses and organizational policy. The team explicitly permitted authorized traffic; all other traffic was denied by default.

Policy-based traffic enforcement combined the ACLs with routing policies so that communication between VLANs occurred only when explicitly authorized. The policy permitted administrative traffic from the IT segment to enterprise servers, while blocking unnecessary inter-departmental communication.

Effectiveness was evaluated with a before-and-after experimental design. Connectivity tests using the Internet Control Message Protocol (ICMP) were first performed after topology, VLAN, and inter-VLAN routing configuration but before ACL application (baseline). The same tests were repeated after applying the ACLs. We examined six communication scenarios: three authorized (Finance-to-Finance, Finance-to-Server, IT-to-Server) and three restricted (Finance-to-Human Resources, Guest-to-Server, Guest-to-Finance). Results were recorded as allowed or blocked.

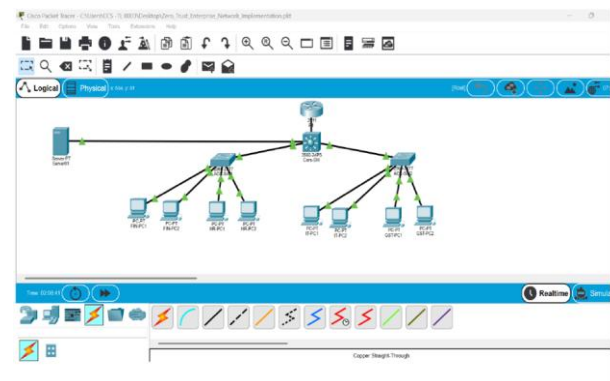


Figure 1. Proposed enterprise network topology designed in Cisco Packet Tracer

The implementation comprised four core technical mechanisms:

1. **Network Segmentation:** The enterprise network was divided into five independent VLANs (Finance, HR, IT, Guest, Server). Each VLAN was assigned a dedicated IP subnet and default gateway. Inter-VLAN communication occurred through a Layer 3 switch configured to route traffic only after evaluating security policies.
2. **Least-Privilege Access Control:** The Principle of Least Privilege (PoLP) was enforced by granting users and devices only the minimum level of access required for authorized functions. The team configured extended ACLs on the Layer 3 switch to regulate inter-VLAN communication.
3. **Policy-Based Traffic Enforcement:** Extended ACLs filtered traffic based on source and destination IP addresses, communication protocols, and organizational access requirements. The firewall discarded unauthorized requests before they reached protected resources.
4. **Controlled Inter-VLAN Communication:** Direct inter-departmental communication was blocked by default, while explicit authorization rules permitted essential operational paths (e.g., IT administrative access to enterprise servers).

Performance Evaluation Methodology: The effectiveness of the Zero Trust controls was evaluated through controlled connectivity and access control testing in two experimental phases. In Phase 1, baseline connectivity tests were conducted after establishing VLANs and inter-VLAN routing, but before applying ACLs. In Phase 2, the same connectivity tests were repeated after applying Extended ACLs and policy-based traffic rules. Connectivity testing was performed primarily using the Internet Control Message Protocol (ICMP) through Packet Tracer simulation tools. Table II details the criteria used for performance evaluation.

Table 1. Performance Evaluation Criteria

Evaluation Criterion	Description
VLAN Segmentation	Verifies that each department is isolated within its assigned VLAN.
ACL Enforcement	Confirms that Access Control Lists permit or deny traffic according to policies.
Authorized Access	Verifies that legitimate users can successfully access permitted resources.
Unauthorized Access Prevention	Confirms that unauthorized communication between departments is denied.
Network Connectivity	Ensures that approved communication paths operate correctly after policies are applied.

RESULTS

Baseline connectivity tests performed before ACL enforcement confirmed unrestricted communication between departmental VLANs once inter-VLAN routing was enabled. Devices within the Finance VLAN could communicate with one another, with the enterprise server, and with the Human Resources VLAN. Guest devices could also reach internal resources. After applying the Extended ACLs to the corresponding VLAN interfaces, we repeated the same tests. All three authorized scenarios remained operational: internal Finance communication, Finance-to-Server access, and IT-to-Server administrative access continued successfully. All three restricted scenarios were blocked: Finance-to-Human Resources, Guest-to-Server, and Guest-to-Finance communication were denied in accordance with the configured policies. These results show that VLAN segmentation alone did not enforce policy-based isolation once inter-VLAN routing was active. Explicit ACL enforcement was required to differentiate authorized from unauthorized paths while preserving legitimate operational connectivity.

Table 2. Configuration of the Simulated Enterprise Network

Component	Configuration
Simulation platform	Cisco Packet Tracer
Network architecture	Hierarchical enterprise network
Network segments	Finance, Human Resources, Information Technology, Guest, Server
Switching technology	Layer 2 and Layer 3 switching
Routing	Inter-VLAN routing
Security controls	VLANs, ACLs, Principle of Least Privilege
Communication protocol	IPv4
Evaluation method	Connectivity and access control Testing

Table 3. Comparative Network Connectivity Results

Communication Scenario	Before Implementation	After Implementation	Security Outcome
Finance → Finance	Allowed	Allowed	Internal communication maintained
Finance → Server	Allowed	Allowed	Authorized access preserved
Finance → Human Resources	Allowed	Blocked	Unauthorized communication prevented
Guest → Server	Allowed*	Blocked	Enterprise resources protected
Guest → Finance	Allowed*	Blocked	Internal network isolated
IT → Server	Allowed	Allowed	Administrative access maintained

DISCUSSION

The before-and-after evaluation shows that the implemented controls successfully enforced network segmentation, least-privilege access, and policy-based communication. Segmentation reduced default reachability at the logical-network level, while the ACLs imposed explicit rules on routed traffic. Consequently, a source in one VLAN could communicate with a destination only when an authorized rule matched, transforming broad routed connectivity into policy-governed Communication. These findings align with the Zero Trust principle that no user, device, or segment should be trusted by default. They also confirm earlier observations that individual mechanisms such as VLANs or ACLs, when used in isolation, are insufficient; integrated application is required for effective lateral-movement restriction (Putra et al., 2024; Subhani & Arshad, 2025). The study does not implement a complete Zero Trust Architecture. Advanced capabilities such as identity and access management, multi-factor authentication, continuous device posture assessment, and full continuous monitoring were outside the simulation scope. The results therefore provide evidence only for selected network-level Zero Trust controls. Future work may extend the design with identity-aware authentication, endpoint detection, SIEM integration, penetration testing, and evaluation on physical or virtualized enterprise infrastructure.

REFERENCES

Afolalu, O. & Tsoeu, M. S. (2025). Enterprise networking optimization: A review of challenges, solutions, and technological interventions. *Future Internet*, 17(4), 1-21.

Aithal, P. S. (2023). Enhancing Industrial Automation through Efficient Technology Management in Society. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 7(4), 184-215.

- Joseph, N. C., Adewale, A. A. & Osamuyi, O. (2024). Advanced modelling and recurrent analysis in network security: Scrutiny of data and fault resolution. *World Journal of Advanced Research and Reviews*, 23(2): 2373–2390.
- Kang, D., Park, J., Jo, Y., & Bak, J. (2023). From values to opinions: Predicting human behaviors and stances using value-injected large language models (pp. 15539–15559).
- Khoury, J., Klisura, D., Zanddzari, H., De La Torre Parra, G., Najafirad, P. & Bou-Harb, E. (2024). Jbeil: Temporal graph-based inductive learning to infer lateral movement in evolving enterprise networks. *Proceedings – IEEE Symposium on Security and Privacy*, 3644–3660.
- Kunduru, A. R. (2023). Security concerns and solutions for enterprise cloud computing applications. *Asian Journal of Research in Computer Science*, 15(4): 24–33.
- Liu, C., Shen, W., Lyu, W., Xu, X. & Ling, X. (2025). A study on network architectures and security for small and medium-sized enterprises. In *Proceedings of the 2025 8th International Conference on Computer Information Science and Artificial Intelligence (CISAI 2025)*. Association for Computing Machinery.
- Lorenzo, D., Pierpaolo, D. & Davide, P. (2025). Overview of intrusion detection systems for computer network security. *MDPI*, 4(2): 1–44.
- Mardiyanto, H., Syahlan, Z. & Aziz, S. (2026). Beyond the perimeter: Assessing the impact of Zero Trust Architecture on network latency and security resilience in large-scale enterprise environments. *Open Access*, 4(2): 175-187.
- Narayanan, S., et al. (2022). Hardware accelerators for ECC in IoT devices. *ACM Transactions on Embedded Computing Systems*
- Panta, P. (2026). Design and implementation of a secure, multi-protocol three-tier enterprise network architecture. *arXiv*.
- Prasanth, K. (2025). Mastering organizational network infrastructure: A strategic framework for understanding and scaling for the future. *World Journal of Advanced Engineering Technology and Sciences*, 15(2): 2688–2702.
- Putra, F. P. E., Ubaidi, U., Tamam, A. B. & Efendi, R. W. (2024). Implementation and simulation of Dynamic ARP Inspection in Cisco Packet Tracer for network security. *Brilliance: Research of Artificial Intelligence*, 4(1), 340–347.
- Shaik, A. (2024). A survey of emerging techniques for large networks of Virtual Local Area Networks (VLANs) with benefits and limitations. *International Journal of Current Engineering and Technology*, 14(6): 478–486.
- Shaik, K. (2025). Next-generation firewalls: Beyond traditional perimeter defense. *International Journal for Multidisciplinary Research*, 7(4): 1–6.
- Soundappan, D. S. J. (2025). Next-generation AI-enabled holistic cognitive platform for secure cloud network intelligence enterprise systems and digital trust optimization. *International Journal of Computer Technology and Electronics Communication*, 8(5): 11534–11542.
- Subhani, M. A. & Arshad, M. J. (2025). Optimizing IoT ecosystem through scalable, secure and efficient network management. *International Journal of Computer Science and Telecommunications*, 16(4): 1–8.
- Sunkara, G. (2025). Implementing Zero Trust Architecture in modern enterprise networks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, 17(03): 1–11.
- Tanimoto, S., Yangchen, P., Sato, H. & Kanai, A. (2023). Suitable scalability management model for software-defined perimeter based on zero-trust model. *International Journal of Service and Knowledge Management*, 7(1): 1–18.
- Yuwono, T., Suroso, A., & Novandari, W. (2024). Information and communication technology in SMEs: A systematic literature review. *Journal of Innovation and Entrepreneurship*, 13(31).
<https://doi.org/10.1186/s13731-024-00392-6>