Journal of Computer and Communications, 2026, 14(11), 135-152
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Evaluating the Effectiveness of VLAN Segmentation and Access Control Lists in Mitigating Lateral Movement in Enterprise Networks

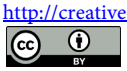
Paul Danquah

Council for Scientific and Industrial Research-Institute for Scientific and Technological Information (CSIR-INSTI), Accra, Ghana
Email: pauldanquah@yahoo.com

How to cite this paper: Danquah, P. (2026) Evaluating the Effectiveness of VLAN Segmentation and Access Control Lists in Mitigating Lateral Movement in Enterprise Networks. *Journal of Computer and Communications*, **14**, 135-152.
https://doi.org/10.4236/jcc.2026.1411006

Received: October 21, 2026
Accepted: November 17, 2026
Published: November 20, 2026

Copyright © 2026 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Open Access

Abstract

Fundamental to the requirement for an Enterprise network are effective access controls to mitigate lateral movement while preserving legitimate interdepartmental communication. This research assesses the effectiveness of Virtual Local Area Network (VLAN) segmentation and extended Access Control Lists (ACLs) in reducing unauthorized access within a simulated enterprise network. Employing Cisco Packet Tracer, three configurations were evaluated: a non-segmented baseline network, VLAN segmentation with inter-VLAN routing, and VLAN segmentation integrated with extended ACLs. ICMP echo requests and HTTP transactions were used to evaluate unauthorized access-blocking rates and legitimate communication success rates. The baseline and VLAN-only configurations recorded unauthorized access-blocking rates of 0%, while the combined VLAN-and-ACL configuration achieved 98.33%, with 59 of 60 unauthorized attempts confirmed as blocked. Legitimate communication success rates were 98.33%, 96.67%, and 98.33%, respectively. Further findings suggest that extended ACLs can complement VLAN segmentation by providing better access control while preserving legitimate connectivity, thus improving the effectiveness of the lateral movement mitigation.

Keywords

VLAN Segmentation, Access Control Lists, Lateral Movement, Enterprise Network Security, Cisco Packet Tracer

1. Introduction

Enterprise networks support communication, information sharing, and access to

digital resources across departments such as finance, human resources, administration, and information technology. The interconnectivity can however expose organizations to security threats when an attacker compromises an endpoint and subsequently attempts to access other systems within the network. This technique, known as lateral movement, enables attackers to expand their access, compromise additional resources, and potentially obtain sensitive organizational information. [1] highlights the limitations of traditional perimeter-based security, noting that compromising the network perimeter may leave internal resources vulnerable to further unauthorized access. Consequently, restricting unnecessary internal communication is an important consideration in enterprise network security.

Virtual Local Area Networks (VLANs) make it possible to divide a single physical network switch or infrastructure into multiple isolated logical networks, thereby creating separate broadcast domains. This feature essentially enables organizations to separate and create network access according to operational requirements or different departments. The VLAN segmentation by itself does not necessarily prevent communication between departments if inter-VLAN routing is enabled. The implementation of Access Control Lists (ACLs) could permit or deny traffic according to defined criteria, including source and destination IP addresses, protocols, and port numbers, this essentially complement segmentation. Collectively, these methods can implement network-level access restrictions and support the principle of least privilege by limiting communication to authorized requirements.

The efficacy of these restrictions depends on their setup and the link between security limitations and permitted business communication. ACLs that are too limiting may allow unauthorised access, whereas ACLs that are too loose may interrupt important services.

[1] further emphasizes that network location should not, by itself, establish trust in a user or device. This emphasizes the essence of evaluating segmentation and traffic-filtering controls by the results they achieve in terms of access control rather than by their existence in a network design.

The usage of a simulator creates an environment for controlled and repeatable method to investigation within this context. Cisco Packet Tracer simulator provides the opportunity to model relevant enterprise network topologies, configure VLANs and inter-VLAN routing, implement ACLs, and test communication between network segments. The comparison of the results between different configurations makes it possible for the assessment of whether security controls successfully restrict prohibited traffic while preserving permitted communications and connectivity.

This research therefore evaluates the adequacy of VLAN segmentation and ACLs in restricting lateral movement in a simulated enterprise network. Specifically, the research question addressed is: To what extent do VLAN segmentation and access control lists reduce unauthorized interdepartmental access while preserving legitimate enterprise network communication? The study seeks to gener-

ate measurable evidence of the security benefits and operational trade-offs associated with combining these controls.

2. Literature Review

2.1. Network Segmentation and Enterprise Network Security

The security of enterprise networks is not limited to perimeter defences, it also includes techniques that restrict lateral movement between internal systems. This is achieved via VLAN segmentation which typically divides a physical network into logically segregated broadcast domains. In an enterprise networked environment, different departments like marketing, human resources, finance and information technology may be assigned a different VLAN depending on the context, this is to avoid unnecessary connectivity and define boundaries for enforcing access regulations. Logical separation does not automatically prevent the different departments from communicating, especially when VLAN routing is enabled.

[2] researched on prescribed methods for network segmentation in complicated networks with various entry and connection points. In their research output, they suggested mathematical methods for segmenting networks and showed the implementation methods using Mininet software for networking emulators. The research emphasized the need for thorough segmentation design, especially in environments where many connectivity routes could compromise intended security restrictions. Their research work considered relatively more generic network architectures than traditional departmental VLANs, the conclusion was however ideal for enterprise networks. Segmentation needs to be based on permitted connectivity and communication channels and not only based on physical or logical grouping of devices. The study, however, does not explicitly determine the effectiveness of traditional VLAN configurations with Cisco access control lists (ACLs) in blocking unauthorized interdepartmental access.

2.2. Lateral Movement as an Enterprise Security Threat

Lateral movement is the method by which an attacker utilizes an initial foothold to gain access to other systems or resources in an environment that has been compromised. It may include unauthorized links between workstations, servers, and other networked devices, facilitating attackers to get closer to key organizational assets. [3] performed a systematic investigation of lateral movement detection and analyzed 53 publications covering endpoint detection and response, machine learning-based techniques, and graph-based solutions. Their review revealed that lateral movement is a complex security problem that requires analysis of attacker behaviour and relationships between systems. This viewpoint is crucial because a well implemented network segmentation should make it more difficult for movement between unauthorized network zones, this must be the case even if an endpoint has already been compromised. The detection of lateral movement and its restriction with network controls are however two different aims. Research focused on detection does not measure how well VLAN segmentation or ACLs work

to stop disallowed connections. This divergence leads to an essential evaluation requirement: it is essential for researchers to examine whether unauthorized communication is truly prohibited, rather than inferring security effectiveness from the presence of segmentation techniques. This implies that a good experimental design should contain cases where compromised or simulated unauthorized host attempts to gain access to system within other departmental VLANs.

2.3. Access Control Policies and Least-Privilege Enforcement

ACLs enhance the segmentation of VLANs via the definition of permitted traffic through routers. ACLs can filter traffic based on source and destination addresses, protocols, and transport-layer port numbers, depending on how they are configured. This makes them to be relevant in applying communication policies between departments, a typical example is allowing authorized access to application servers that are shared while preventing direct access to critical finance systems.

[4] performed a systematic literature evaluation of security and access-control measures in bring-your-own-device environments. Their 74-study review covered security requirements, policy technologies, privacy issues and ways to assess security performance. The outcome of the research emphasized the necessity to ensure that access-control policies are linked to operational and security concerns. Although the assessment is focused on "bring your own device" BYOD scenarios and not typical VLAN-based workplace networks, the findings of the research support the notion that access control policies should be reviewed against explicit requirements and not implemented as separate technological solutions.

Various approaches of Zero Trust Network Architecture were surveyed in [5]. The research studied authentication, access control, micro-segmentation, encryption and security automation. The findings argue in favour of networks that are controlled by defined permissions rather than trust based on placement in the internal network. This implies that ACL rules must have precise communication requirements of the departments. However, neither the general Zero Trust model nor ACLs alone will provide effective protection, the results will depend on how accurate and complete the implemented policies are.

2.4. Zero Trust, Fine-Grained Access Control, and Operational Trade-Offs

Recent research extends traditional network segmentation towards more granular, policy-driven enforcement. [6] examined Zero Trust security in the context of the Internet of Things, emphasizing continuous verification, least-privilege access, and segmentation as mechanisms for limiting the potential spread of compromise. The review done supports the basis that the location of the network should not be the sole criterion for permitting communications. This implies determining which hosts and services are allowed to communicate even if devices belong to the same organization [1] in a departmental business network.

[7] examined the incorporation of security service functionalities with access

control at the network level. Their solution includes contextual factors in traffic management decisions to increase the accuracy of access-control, eliminate incorrect decisions and maintain network visibility. Their research work also identifies an essential design concern of effective security enforcement: trade-off between blockage of legal traffic and prevention of unauthorized communication. The fundamental assessment idea is, however, directly applicable to this study even if their approach is more sophisticated than ordinary Cisco ACL configurations. [8] addressed automation and orchestration in Zero Trust systems, highlighting issues in the deployment and orchestration of security policies in actual networks. Their research suggests that policy enforcement should be evaluated in a larger network environment and not as an isolated configuration assignment. This also implies that, when VLAN and ACL are configured, it is essential to check both the effectiveness of the traffic restriction and the continuous accessibility of the authorized services.

Together, these studies demonstrate that successful segmentation requires clear instructions, appropriate execution and comprehensive validation. An ACL that denies all inter-VLAN communication may prevent unauthorized access, but it may also interfere with necessary company functions. In contrast, liberal rules may enable undesirable communication but keep the connection alive. This implies that, ultimately, security and functionality have to be measured jointly.

3. Methodology

The approach used for this research was a quantitative experimental network simulation, it was used to assess the efficiency of Virtual Local Area Network (VLAN) segmentation and Access Control Lists (ACLs), the fundamental objective was to mitigate lateral movement in enterprise networks. Cisco Packet Tracer was used to model an enterprise network with established security controls, and executed repeatable connectivity tests. This was approach in consistent with the simulation based studies of VLAN and ACL setups for network access control [9].

3.1. Network Design and Configuration

The simulated network comprises of three departmental VLANs, each VLAN will has a unique IP subnet and connected end devices. A router is used to provide inter-VLAN routing. The baseline configuration enabled the required routing and communication without the proposed interdepartmental restrictions.

Experimental Scenarios: Three configurations will be evaluated: 1) an unsegmented or unrestricted baseline network; 2) VLAN segmentation with inter-VLAN routing; and 3) VLAN segmentation combined with extended ACLs. ACL rules implemented least-privilege access by permitting authorized communication and denying prohibited traffic between departmental networks. This design reflects the importance of combining network segmentation with explicit traffic-filtering policies to constrain lateral movement [1].

3.2. Data Collection and Analysis

The connectivity tests mimicked authorized and unauthorized access attempts using ICMP echo requests and where supported HTTP and other relevant services. Each test was performed 3 times for all 3 configurations, and the results were recorded as allowed or blocked. The main metrics used were the proportion of unauthorized accesses blocked and the percentage of successful valid communications, measured against the total number of test attempts. The results were compared among settings using descriptive statistics and tables. The experimental approach describes the network configurations, ACL rules, test cases and results obtained to make it repeatable. The Packet Tracer simulation provides a controlled environment to study the effectiveness of the network access regulations [10].

The assessment of the three network configurations was represented by two main measures. The unauthorized access-blocking rate was calculated as the percentage of scheduled unauthorized communication attempts that were confirmed to have been blocked. The legitimate communication success rate was calculated as the percentage of scheduled authorized communication attempts that completed successfully. Both metrics were derived using the general percentage formula and operationally defined for this experiment. The evaluation approach was informed by established guidance on information security testing and access-control assessment [11] [12] and network security-device benchmarking methodology [13]. Confirmed blocks, successful communications, timeouts and other failures were recorded separately to avoid misclassifying unsuccessful attempts as confirmed security enforcement.

Each communication attempt was defined as one ICMP echo request or application-layer request, with a response timeout of 3 seconds for ICMP and 5 seconds for HTTP. Tests were executed in a fixed, documented order across all three configurations.

3.3. Networks Layout and Configuration

Figure 1 represents the logical layout of the three networks used for the research. The three networks are designed to evaluate the effect of network segmentation and extended Access Control Lists (ACLs) on unauthorized access prevention and legitimate communication. The same three end devices are used across the experiments: PC1, PC2 and a Web Server. The network topology and IP addressing are adjusted to reflect each security configuration. For consistency, all three routed subnets use a/24 subnet mask (255.255.255.0), and the gateway address is assigned .10 in each subnet.

Network 1: Unsegmented and unrestricted baseline network

The baseline network consists of one router, one Layer 2 switch, two PCs and one Web Server. All devices connect to the same LAN through the switch. There are no VLANs or extended ACLs restricting communication within the LAN.

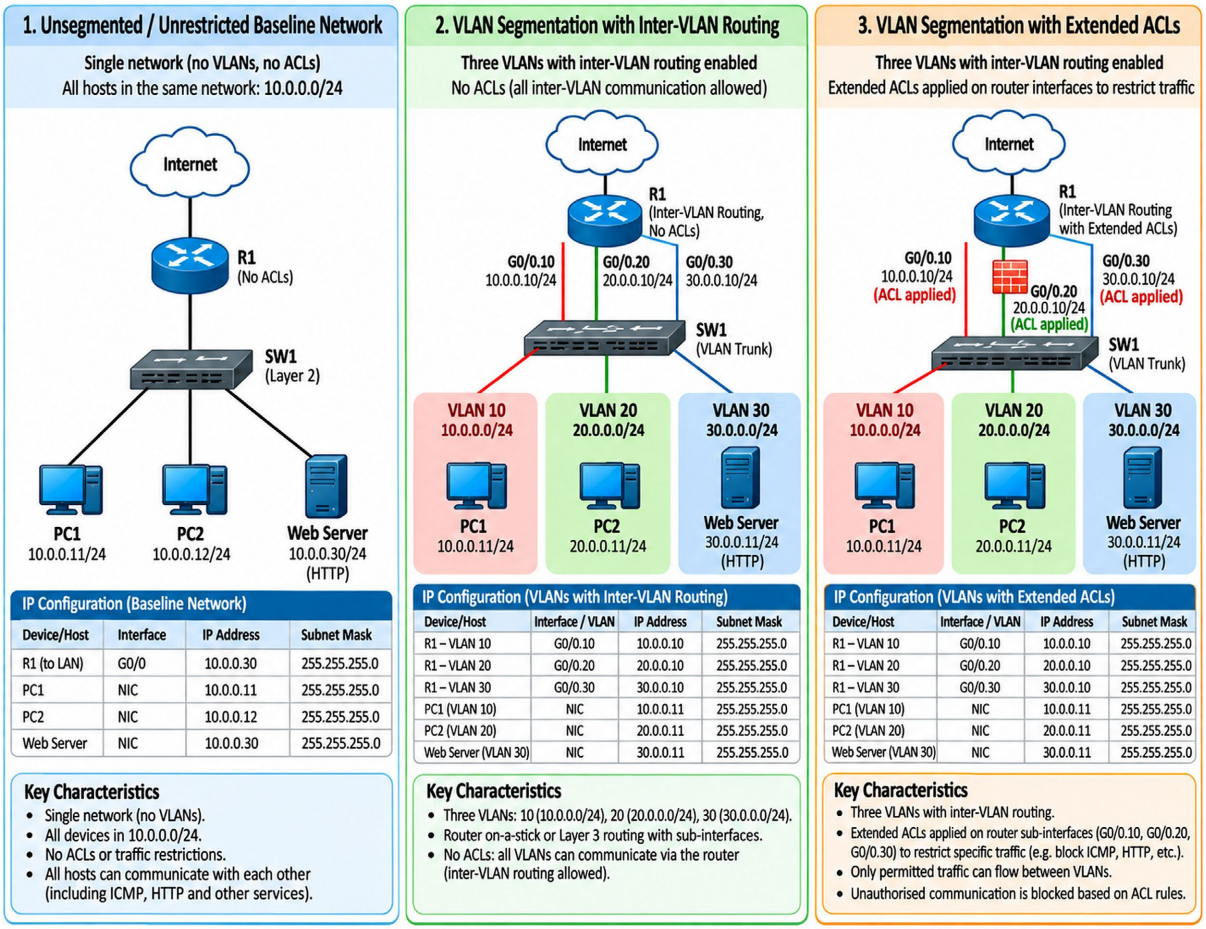


Figure 1. Logical representation of three networks.

The router provides the LAN gateway and can provide external connectivity if required. The switch forwards traffic between devices within the same subnet. For this experiment, the entire baseline LAN uses 10.0.0.0/24.

Table 1 below provides an overview of addressing for network one.

Table 1. Addressing for network 1.

Device	Interface	IP address	Subnet mask	Default gateway
Router R1	G0/0	10.0.0.10	255.255.255.0	N/A
PC1	NIC	10.0.0.11	255.255.255.0	10.0.0.10
PC2	NIC	10.0.0.12	255.255.255.0	10.0.0.10
Web Server	NIC	10.0.0.30	255.255.255.0	10.0.0.10

Expected communication behaviour:

- PC1 can communicate directly with PC2 and the Web Server.
- PC2 can communicate directly with PC1 and the Web Server.
- ICMP echo requests, HTTP requests and other enabled services are permitted unless blocked by an independent control, such as a host firewall.

- There is no VLAN-based isolation between the three end devices.

This network establishes the baseline against which the effects of VLAN segmentation and extended ACLs will be measured.

Network 2: VLAN Segmentation with Inter-VLAN Routing

This network uses one router, one VLAN-capable Layer 2 switch, two PCs and one Web Server. The switch is configured with three VLANs, each representing a separate logical network.

- VLAN 10 contains PC1.
- VLAN 20 contains PC2.
- VLAN 30 contains the Web Server.

The router uses a "router-on-a-stick" configuration. A single physical router interface connects to the switch through an 802.1Q trunk, and three logical sub interfaces provide routing between the VLANs.

Table 2 below provides an overview of addressing for network two.

Table 2. Addressing for network 2.

Device	Interface/VLAN	IP address	Subnet mask	Default gateway
R1	G0/0.10	10.0.0.10	255.255.255.0	N/A
R1	G0/0.20	20.0.0.10	255.255.255.0	N/A
R1	G0/0.30	30.0.0.10	255.255.255.0	N/A
PC1	VLAN 10	10.0.0.11	255.255.255.0	10.0.0.10
PC2	VLAN 20	20.0.0.11	255.255.255.0	20.0.0.10
Web Server	VLAN 30	30.0.0.11	255.255.255.0	30.0.0.10

The three networks are:

- VLAN 10: 10.0.0.0/24
- VLAN 20: 20.0.0.0/24
- VLAN 30: 30.0.0.0/24

Table 3 below provides an overview of the allocation for layer two interfaces, connected devices, mode of interfaces and VLANs.

Table 3. Allocation for the layer 2 switch (SW1) is shown below.

Switch port	Connected device	Mode	VLAN
Fa0/1	PC1	Access	10
Fa0/2	PC2	Access	20
Fa0/3	Web Server	Access	30
Gi0/1	Router R1 G0/0	802.1Q trunk	10, 20, 30

The communication behaviour of the network is setup for PC1 and PC2 to belong to different IP subnets and cannot communicate directly at Layer 2. PC1 can reach PC2 through R1 because inter-VLAN routing is enabled, PC1 and PC2 can

reach the Web Server, provided the relevant services are active and no other control blocks traffic. Lastly, ICMP, HTTP and other enabled services are not restricted by extended ACLs in this configuration. This network isolates the effect of VLAN segmentation while retaining inter-VLAN communication. It helps establish whether VLAN separation alone prevents unauthorized communication when routing remains enabled.

Network 3: VLAN Segmentation with Extended ACLs

The physical and logical topology is the same as Network 2. It contains the same router, switch, PCs and Web Server, with VLANs 10, 20 and 30 connected through "router-on-a-stick" inter-VLAN routing. The key difference is that extended ACLs are configured on the router sub-interfaces to enforce the intended communication policy. These ACLs can examine source and destination IP addresses, IP protocols and TCP/UDP port numbers.

Table 4 below provides an overview of addressing for network three.

Table 4. IP addressing for network 3.

Device	Interface/VLAN	IP address	Subnet mask	Default gateway
R1	G0/0.10	10.0.0.10	255.255.255.0	N/A
R1	G0/0.20	20.0.0.10	255.255.255.0	N/A
R1	G0/0.30	30.0.0.10	255.255.255.0	N/A
PC1	VLAN 10	10.0.0.11	255.255.255.0	10.0.0.10
PC2	VLAN 20	20.0.0.11	255.255.255.0	20.0.0.10
Web Server	VLAN 30	30.0.0.11	255.255.255.0	30.0.0.10

The following is the test policies detailed in Table 5.

Table 5. Access control list policies.

Source	Destination	Service	Policy	Expected outcome
PC1	PC2	ICMP echo	Deny	Ping blocked
PC1	Web Server	HTTP (TCP/80)	Deny	HTTP request blocked
PC1	Web Server	ICMP echo	Permit	Ping succeeds
PC2	Web Server	HTTP (TCP/80)	Permit	HTTP request succeeds
PC2	PC1	ICMP echo	Permit	Ping succeeds

These examples create both prohibited and permitted test cases, the communication behaviour involves the router passing traffic between VLANs, extended ACLs determine which routed traffic is permitted or denied, prohibited traffic to be blocked, while explicitly permitted traffic continues to work. Additionally, ACL placement and direction determine which packets are evaluated because Cisco ACLs end with an implicit deny, required legitimate traffic must be explicitly permitted where appropriate. This network measures the additional security benefit

of ACL enforcement beyond VLAN segmentation alone, while assessing the effect of the controls on legitimate communication.

The specific access control list configuration used is shown below in Figure 2.

Router sub interface configuration

```
interface GigabitEthernet0/0
 no ip address
 no shutdown
 exit

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.0.0.10 255.255.255.0
 ip access-group VLAN10-IN in
 no shutdown
 exit

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 20.0.0.10 255.255.255.0
 ip access-group VLAN20-IN in
 no shutdown
 exit

interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 30.0.0.10 255.255.255.0
 ip access-group VLAN30-IN in
 no shutdown
 exit
```

Extended ACL configuration

```
ip access-list extended VLAN10-IN
remark Deny PC1 ICMP echo requests to PC2
deny icmp host 10.0.0.11 host 20.0.0.11 echo

remark Deny PC1 HTTP access to Web Server
deny tcp host 10.0.0.11 host 30.0.0.11 eq 80

remark Permit ICMP echo replies from PC1 to PC2
permit icmp host 10.0.0.11 host 20.0.0.11 echo-reply

remark Permit PC1 to ping Web Server
permit icmp host 10.0.0.11 host 30.0.0.11 echo

remark Permit other required ICMP replies from PC1
permit icmp host 10.0.0.11 any echo-reply

remark Deny all other traffic from VLAN 10
deny ip any any
exit
```

```
ip access-list extended VLAN20-IN
remark Permit PC2 to ping PC1
permit icmp host 20.0.0.11 host 10.0.0.11 echo

remark Permit PC2 HTTP access to Web Server
permit tcp host 20.0.0.11 host 30.0.0.11 eq 80

remark Deny all other traffic from VLAN 20
deny ip any any
exit

ip access-list extended VLAN30-IN
remark Permit Web Server ping replies to PC1
permit icmp host 30.0.0.11 host 10.0.0.11 echo-reply

remark Permit HTTP return traffic to PC2
permit tcp host 30.0.0.11 eq 80 host 20.0.0.11 estab-
lished

remark Deny other traffic from VLAN 30
deny ip any any
exit
```

Figure 2. Network 3 router configuration.

Table 6 below provides a summarized comparison of the networks 1, 2 and 3.

Table 6. Summary comparison of the three networks.

Feature	Network 1: Baseline	Network 2: VLANs	Network 3: VLANs + ACLs
VLANs	None	10, 20, 30	10, 20, 30
IP subnets	One	Three	Three
Router-on-a-stick	No	Yes	Yes

Continued

Inter-VLAN routing	Not applicable	Enabled	Enabled, subject to ACLs
Extended ACLs	None	None	Applied
Unauthorized access control	Baseline conditions	VLAN separation only	VLAN separation plus policy enforcement
Legitimate communication	Expected to succeed	Expected to succeed	Expected to succeed for permitted flows

Experimental control and interpretation: To ensure that the results are scientifically defensible, the same end devices, services, test pairs and number of attempts are applied in all three configurations, and the IP addresses are unchanged between Networks 2 and 3. For the tests carried out, the intended policy for each test is defined before collecting results. Records of successful, blocked, timed-out and otherwise failed attempts are done separately, a calculation of the unauthorized access-blocking rate and legitimate communication success rate is done independently there is the interpretation of VLAN segmentation as logical separation, not as a substitute for access-control policy. The use of 10.0.0.0/24, 20.0.0.0/24 and 30.0.0.0/24 is valid for this laboratory design but not for a production network.

4. Results and Analysis

4.1. Experimental Results: VLAN Segmentation and Extended ACLs

This section presents a result obtained from experiment on Cisco Packet Tracer comparing:

- Network 1: Unsegmented baseline network.
- Network 2: VLAN segmentation with inter-VLAN routing.
- Network 3: VLAN segmentation with inter-VLAN routing and extended ACLs.

The experiment evaluates two independent security-performance metrics: the unauthorized access-blocking rate and the legitimate communication success rate. It also records successful, blocked, timed out and otherwise failed attempts separately.

The experiment results are recorded using three end devices: PC1, PC2 and a Web Server as shown below in Table 7.

Table 7. Devices used in recording results.

Device	Network 1: Baseline	Network 2 and 3: VLANs
PC1	10.0.0.11/24	VLAN 10: 10.0.0.11/24
PC2	10.0.0.12/24	VLAN 20: 20.0.0.11/24
Web Server	10.0.0.30/24	VLAN 30: 30.0.0.11/24
Default gateway	10.0.0.10	VLAN 10: 10.0.0.10; VLAN 20: 20.0.0.10; VLAN 30: 30.0.0.10

The subnet mask is 255.255.255.0 for all three VLAN subnets. Network 2 and

Network 3 use "router-on-a-stick" routing over an 802.1Q trunk. For the baseline, all devices are on the same subnet, for the other two configurations, each VLAN is a separate IP subnet, and communication between VLANs must traverse the router.

The following policy detailed in Table 8 is used for these tests.

Table 8. Policies for testing.

Test ID	Source-Destination	Service	Classification	Required policy outcome
U1	PC1 - PC2	ICMP echo	Unauthorized	Block
U2	PC1 - Web Server	HTTP, TCP/80	Unauthorized	Block
U3	PC2 - PC1	ICMP echo	Unauthorized	Block
L1	PC1 - Web Server	ICMP echo	Legitimate	Permit
L2	PC2 - Web Server	HTTP, TCP/80	Legitimate	Permit
L3	PC2 - PC1	ICMP echo	Legitimate	Permit

The policy represents a requirement to prevent selected peer-to-peer and application access while allowing specific operational traffic. There are no extended ACLs on Network 1 and Network 2 to enforce this policy. The observed results are therefore compared against the same policy to determine the effectiveness of the controls. All three devices in Network 1 are in the same subnet. In Network 2, the router enables inter VLAN routing with no extended ACL filtering.

Extended ACLs are configured to enforce the specified rules for Network 3. The test policy was continuously enforced including any required return traffic and allowed service rules.

Interpretation: VLANs create logical isolation, but when inter-VLAN routing is enabled, this separation does not by itself prevent routed communication. Network 3 introduces explicit policy enforcement with ACLs. For this experiment, each of the six tests is repeated 20 times for each network setup.

Each test attempt has a single, unique outcome:

Successful: Communication occurred

- Blocked: There is evidence that security control denied the traffic.
- Timed out: No response was received within the defined waiting period.
- Otherwise failed: Communication failed for another reason, such as a service error or connection refusal.

The four outcome categories are mutually exclusive and sum to 20 for every test row.

Table 9 below shows the results generated from the tests carried out.

Table 10 below depicts combined outcomes of the results by the respective networks.

Table 9. Test results.

Network	Test	Successful	Blocked	Timed out	Other failure	Total
N1 Baseline	U1	19	0	1	0	20
N1 Baseline	U2	20	0	0	0	20
N1 Baseline	U3	19	0	1	0	20
N1 Baseline	L1	20	0	0	0	20
N1 Baseline	L2	19	0	1	0	20
N1 Baseline	L3	20	0	0	0	20
N2 VLANs	U1	20	0	0	0	20
N2 VLANs	U2	19	0	1	0	20
N2 VLANs	U3	20	0	0	0	20
N2 VLANs	L1	19	0	1	0	20
N2 VLANs	L2	20	0	0	0	20
N2 VLANs	L3	19	0	1	0	20
N3 VLANs + ACLs	U1	0	20	0	0	20
N3 VLANs + ACLs	U2	0	19	1	0	20
N3 VLANs + ACLs	U3	0	20	0	0	20
N3 VLANs + ACLs	L1	20	0	0	0	20
N3 VLANs + ACLs	L2	19	0	1	0	20
N3 VLANs + ACLs	L3	20	0	0	0	20

U = unauthorized test; L = legitimate test.

Table 10. Aggregated outcomes by network Each network has 120 test attempts: 60 unauthorized and 60 legitimate.

Network	Test category	Successful	Blocked	Timed out	Other failure	Total
N1	Unauthorized	58	0	2	0	60
N1	Legitimate	59	0	1	0	60
N2	Unauthorized	59	0	1	0	60
N2	Legitimate	58	0	2	0	60
N3	Unauthorized	0	59	1	0	60
N3	Legitimate	59	0	1	0	60

Test outcomes were classified as successful, blocked, timed out, or other failure. A test was classified as a confirmed ACL block only when packet-level evidence identified the router's ACL filtering mechanism as the cause of packet discard, preferably corroborated by the corresponding ACL deny-rule counter. Timeouts without corroborating evidence were classified separately because they may result from ACL filtering, routing problems, endpoint unavailability, or other network conditions.

For Network N3, 59 of the 60 unauthorized attempts were recorded as blocked,

while one timed out. The 59 blocked outcomes are interpreted as confirmed ACL enforcement only to the extent that supporting packet-level or ACL-counter evidence is available. Networks N1 and N2 recorded no blocked attempts in the supplied results; their unauthorized-test outcomes were predominantly successful, with the remaining attempts timing out. These results indicate that the intended access restrictions were not demonstrated by the reported outcomes for N1 and N2.

Across all three networks, legitimate-test success was 176/180 (97.78%), while unauthorized-test success was 117/180 (65.00%). For N3 alone, legitimate-test success was 59/60 (98.33%), and reported unauthorized-test blocking was 59/60 (98.33%). These percentages describe the recorded outcomes; the unauthorized blocking rate should be interpreted as a confirmed ACL enforcement rate only when the blocked classifications are supported by appropriate evidence.

Calculation of the two principal metrics independently

Unauthorized access-blocking rate: Use only unauthorized attempts in the denominator.

$$\text{Blocking Rate} = \frac{\text{Confirmed blocked attempts}}{\text{Total unauthorised attempts}} \times 100$$

For Network 1:

$$\frac{0}{60} \times 100 = \boxed{0\%}$$

For Network 2:

$$\frac{0}{60} \times 100 = \boxed{0\%}$$

For Network 3:

$$\frac{59}{60} \times 100 = \boxed{98.33\%}$$

Caveat: The timed-out attempt in Network 3 is excluded from the numerator because it has not been confirmed as blocked. It remains in the denominator because it was one of the scheduled unauthorized test attempts.

Legitimate communication success rate: The denominators used in computation are only the legitimate attempts

$$\text{Success Rate} = \frac{\text{Successful legitimate attempts}}{\text{Total legitimate attempts}} \times 100$$

For Network 1:

$$\frac{59}{60} \times 100 = \boxed{98.33\%}$$

For Network 2:

$$\frac{58}{60} \times 100 = \boxed{96.67\%}$$

For Network 3:

$$\frac{59}{60}\times 100 = \boxed{98.33\%}$$

This metric measures the proportion of legitimate attempts that are completed successfully. It does not treat timeouts as successes, even if their cause remains uncertain.

Summary of calculated results

Results are based on 60 unauthorized and 60 legitimate attempts per network.

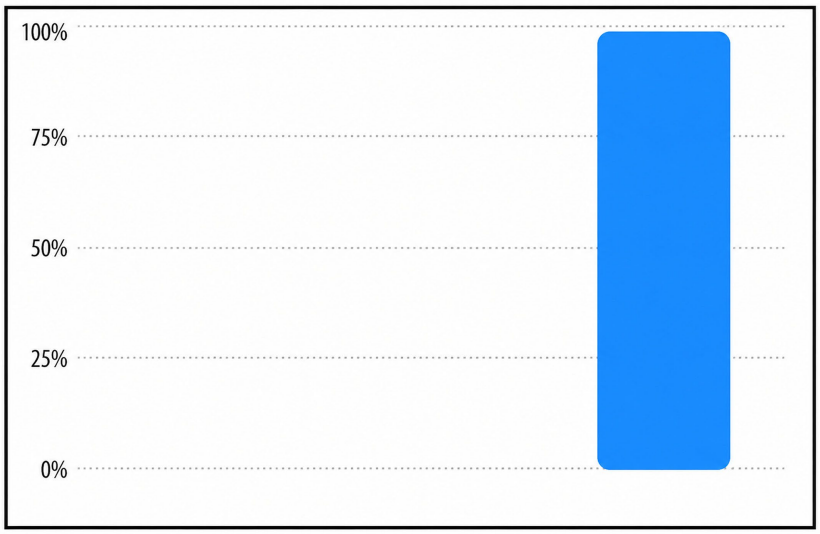


Figure 3. Percentage of all scheduled unauthorized attempts confirmed blocked.

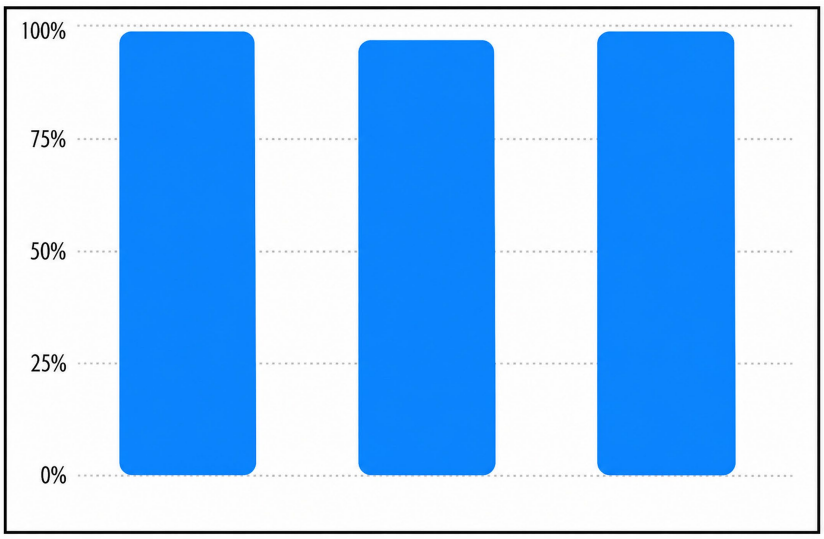


Figure 4. Percentage of scheduled legitimate attempts that succeeded.

Figure 3 and Figure 4 depict percentages of all scheduled unauthorized attempts confirmed blocked and scheduled legitimate attempts that succeeded respectively.

Table 11 further shows a comparative results between the different networks

based on performance indicators.

Table 11. Comparison of results based on performance indicators.

Performance indicator	N1: Baseline	N2: VLANs	N3: VLANs + ACLs
Unauthorized attempts	60	60	60
Confirmed blocked attempts	0	0	59
Unauthorized access-blocking rate	0.00%	0.00%	98.33%
Legitimate attempts	60	60	60
Successful legitimate attempts	59	58	59
Legitimate communication success rate	98.33%	96.67%	98.33%
Timed-out attempts, both categories combined	3	3	2
Otherwise failed attempts	0	0	0

4.2. Interpretation of Results

Finding 1: VLAN segmentation does not independently apply the requisite access policy. The specified restricted flows have a 0% blocking rate in Network 2. This demonstrates or reveals that separate VLANs do not always block connection between subnets in situations where inter-VLAN routing is enabled and no ACLs restrict the traffic.

Finding 2: It is evident that Extended ACLs provide a significant improvement in access control. Network 3 blocks 59 out of 60 unauthorized attempts, resulting in a blocking rate of 98.33%. The data does not support the assertion of a confirmed 100% blocking rate as the remaining timeout resolution is not yet available.

Finding 3: ACL configuration allows legitimate connectivity in this scenario. Network 3 has a valid communication success rate of 98.33% which is equal to the baseline. This means that the approach shown can improve security relative to the baseline, without any loss in the total success rate. The differences between the networks, however, do not indicate that there is a statistically significant difference in performance.

Finding 4: Conclusions are dependent on failure classification. Counting each timeout as a blocked attempt would increase the blocking rate. Similarly, treating a connection refusal or unsuccessful HTTP request as a security block without verifying the cause could lead to an flawed conclusion.

5. Conclusions

The outcome of this research depicts the relative influence of VLAN segmentation and extended Access Control Lists (ACLs) on network security and valid communication performance. Three network topologies were tested; a baseline network without segmentation, a VLAN segmented network with routing between VLANs and a VLAN segmented network with expanded ACLs. The evaluation was executed in the context of unauthorized access-blocking rate and the permitted communication success rate. ICMP echo requests and HTTP transactions were used

as the representative test services.

The baseline network had a 0% unauthorized access-blocking rate, and the VLAN-segmented network likewise had a 0% against the selected forbidden communication attempts. These example findings clarify that VLAN segmentation by itself does not necessarily prevent unauthorized communication when inter-VLAN routing is enabled without additional access-control rules. VLANs enable logical isolation by generating separate broadcast domains, but they do not independently enforce restrictions on routed traffic.

In contrast, the VLAN segmented network with enhanced ACLs provided 98.33% unauthorized access-blocking rate. The number of unauthorized attempts confirmed as stopped is 59 of 60. This is a major improvement over the other two configurations. The single attempt that timed out and could not be definitively labelled as blocked. The results, therefore, do not confirm a 100% blocking rate.

The VLAN, ACL and the baseline network succeeded in valid communication 98.33% of the time, whereas the VLAN only configuration succeeded 96.67% of the time. The results imply that extended ACLs designed effectively can enhance access control without negatively impacting the performance of legitimate network functions. These relatively minor changes in success rate should not be considered statistically significant until further testing and analysis is done.

In summary, the results suggest that the use of VLAN segmentation combined with expanded ACLs offers more policy-based access control than VLAN segmentation alone in a network with inter-VLAN routing. The results also show the need to evaluate security enforcement together with legitimate communication performance. A setup that efficiently blocks unauthorized traffic but disturbs authorized services is not an optimal security solution.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Alabbad, M., Mhaskar, N. and Khedri, R. (2024) Two Formal Design Solutions for the Generalization of Network Segmentation. *Journal of Network and Computer Applications*, **222**, Article 103763. https://doi.org/10.1016/j.jnca.2023.103763

[2] Ayedh M, A.T., Wahab, A.W.A. and Idris, M.Y.I. (2023) Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions. *Applied Sciences*, **13**, Article 8048. https://doi.org/10.3390/app13148048

[3] Azad, M.A., Abdullah, S., Arshad, J., Lallie, H. and Ahmed, Y.H. (2024) Verify and Trust: A Multidimensional Survey of Zero-Trust Security in the Age of IoT. *Internet of Things*, **27**, Article 101227. https://doi.org/10.1016/j.iot.2024.101227

[4] Balarajah, B., Rossenhoevel, C. and Monkman, B. (2023) Benchmarking Methodology for Network Security Device Performance. RFC 9411, Internet Engineering Task Force.

[5] Bradatsch, L. and Kargl, F. (2024) Integration of Security Service Functions into Network-Level Access Control. *IEEE Access*, **12**, 197783-197815.

https://doi.org/10.1109/access.2024.3522575

[6] Cao, Y., Pokhrel, S.R., Zhu, Y., Doss, R. and Li, G. (2024) Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges. *Machine Intelligence Research*, **21**, 294-317. https://doi.org/10.1007/s11633-023-1456-2

[7] Christofa, D. and Ariyadi, T. (2025) Simulasi ACL Standard Pada Jaringan VLAN Menggunakan Aplikasi Cisco Packet Tracer. *IJM*: *Journal of Multidisciplinary*, **3**, 32-47.

[8] Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K.U., *et al.* (2024) A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors*, **24**, Article 1328. https://doi.org/10.3390/s24041328

[9] Hu, V.C. and Scarfone, K. (2012) Guidelines for Access Control System Evaluation Metrics. National Institute of Standards and Technology.

[10] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. NIST Special Publication 800-207, National Institute of Standards and Technology.

[11] Sifawa, I.M., Adenomon, M.O. and Umar, M.I. (2026) Implementation and Evaluation of Network-Level Zero Trust Controls for Enterprise Network Security Using Cisco Packet Tracer. *Science World Journal*, **21**, 1340-1343. https://scienceworldjournal.org/article/view/24917

[12] Smiliotopoulos, C., Kambourakis, G. and Kolias, C. (2024) Detecting Lateral Movement: A Systematic Survey. *Heliyon*, **10**, e26317. https://doi.org/10.1016/j.heliyon.2024.e26317

[13] Sung, Y.E., Sun, X., Rao, S.G., Xie, G.G. and Maltz, D.A. (2011) Towards Systematic Design of Enterprise Networks. *IEEE/ACM Transactions on Networking*, **19**, 695-708. https://doi.org/10.1109/tnet.2010.2089640