International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 15, Number 3 (2026) pp. 265-291
Research India Publications
https://www.ripublication.com

Design and Experimental Evaluation of an Enterprise Network Security Model Using Palo Alto Networks NGFW

Thi Thu Hien Nguyen
Faculty of Telecommunications,
Posts and Telecommunications Institute of Technology,
96A,Tran Phu Street, Ha Dong, Hanoi, Vietnam
Email: hiennt@ptit.edu.vn;

Abstract

This study proposes and evaluates a comprehensive enterprise network security model leveraging Palo Alto Networks Next-Generation Firewalls (NGFW) within the EVE-NG simulation environment. Grounded in the principles of Defense in Depth, Network Segmentation, and Zero Trust Architecture, the proposed architecture systematically divides the enterprise network into distinct security zones—including Management, Trust, DMZ, and Untrust zones—to regulate and inspect all cross-zone traffic.

Through rigorous experimental scenarios, this research evaluates the efficacy of advanced security mechanisms, including App-ID for Layer 7 application-level control, Destination NAT and Security Policies for secure DMZ web server publishing, and DNS Security for preemptive threat mitigation at the network boundary. Comparative analysis against a traditional Router Access Control List (ACL) demonstrates the superiority of the NGFW solution in granularity, policy flexibility, and comprehensive audit logging. Furthermore, quantitative performance profiling confirms that the system maintains stable hardware resource utilization (CPU and RAM) and keeps packet processing latency well within acceptable enterprise thresholds, validating its feasibility for real-world deployment.

Keywords: Enterprise network security; Next-Generation Firewall (NGFW); Palo Alto Networks; App-ID; Security Policy; EVE-NG

Introduction

Digital transformation is dramatically reshaping enterprise information technology infrastructure. Traditional network systems, which primarily served internal applications, have expanded to cloud computing models, the Internet of Things (IoT), remote working, virtualized data centers, and Software-as-a-Service (SaaS) services. This evolution helps enterprises improve connectivity, optimize operations, and

increase flexibility in service deployment. However, the expansion of connectivity scope also significantly increases the attack surface, making enterprise systems face more information security risks than before [1].

According to the ENISA Threat Landscape 2024, current cybersecurity threats are no longer limited to traditional viruses or worms but have evolved into various sophisticated attack forms such as ransomware, zero-day exploits, software supply chain attacks, phishing, credential theft, and attacks on cloud computing infrastructure. Meanwhile, the increasing proportion of traffic encrypted with HTTPS reduces the effectiveness of traditional packet filtering mechanisms, posing a requirement for security solutions capable of application awareness, application-layer traffic analysis, and real-time anomaly detection [1].

Alongside the increase in threats, the cost of recovering from cybersecurity incidents is also continuously rising. The IBM Cost of a Data Breach Report 2024 shows that the average cost of a data breach remains at a very high level, while the Cisco Cybersecurity Readiness Index emphasizes that cyberattacks not only cause financial damage but also affect service availability, enterprise reputation, and compliance capabilities regarding data protection regulations [2], [3]. Therefore, building a security architecture capable of early detection, effective prevention, and centralized threat management has become an essential requirement for modern enterprises.

For many years, Router Access Control Lists (ACLs) and traditional firewalls have been popular solutions for controlling access within enterprise networks. These mechanisms operate primarily based on network-layer and transport-layer information, such as source IP addresses, destination IP addresses, protocols, and service port numbers, to decide whether to allow or deny traffic [4]. Although suitable for traditional network environments, this approach reveals many limitations when most modern applications use the HTTPS protocol over the TCP/443 port. In this case, Router ACLs cannot distinguish specific applications and instead identify all HTTPS traffic identically, leading administrators to only allow or block entire service ports, making it difficult to meet application-based access control requirements in enterprise environments [4], [5].

In addition, Router ACLs and traditional Stateful Firewalls also do not integrate advanced security functions such as Deep Packet Inspection (DPI), Intrusion Prevention Systems (IPS), application awareness, DNS Filtering, URL Filtering, or real-time threat analysis. In the context of increasingly encrypted network traffic and constantly changing attack techniques, relying solely on network-layer information no longer meets system protection requirements. NIST standards and guidelines as well as modern research recommend that enterprises transition from a network perimeter-based security model to security architectures based on identity, access context, and Zero Trust principles, where control must be implemented at both the application layer instead of relying solely on IP addresses or service ports [4], [6], [15], [16], [17]. To meet these requirements, Next-Generation Firewalls (NGFWs) have been developed to extend protection from the network layer to the application layer of the OSI model [4], [7], [10], [11], [12], [13]. Unlike traditional firewalls, NGFWs integrate multiple security mechanisms on a single platform, such as application

identification (App-ID), user identification (User-ID), deep packet inspection (DPI), intrusion prevention systems (IPS), URL filtering, DNS Security, and real-time threat analysis [7]. Consequently, security policies can be built based on applications, users, or network zones rather than just IP addresses and service ports, helping to enhance access control effectiveness and minimize information security risks [7].

Among current NGFW platforms, Palo Alto Networks is evaluated as one of the leading NGFW platforms due to its ability to integrate App-ID, User-ID, Content-ID, DNS Security, and WildFire within a single security architecture [7]–[9]. Furthermore, Gartner Magic Quadrant for Network Firewalls reports for many consecutive years have recognized Palo Alto Networks among the leaders in the market [14].

Related Work and Research Gap

In recent years, Next-Generation Firewalls (NGFWs) have become a critical component in enterprise network security architecture due to their ability to control traffic at the application layer and integrate multiple defense mechanisms on a single platform. Existing studies primarily focus on three main directions.

The first research direction focuses on developing and optimizing NGFW traffic inspection methods. Heino et al. [10] proposed an endpoint-aware inspection method for NGFWs, demonstrating that combining Deep Packet Inspection (DPI) with application identification mechanisms significantly improves the detection capability of applications and threats in HTTPS traffic. Following this direction, the works of Heino et al. [11], [12] expanded into an endpoint-aware inspection architectural framework and unsupervised application identification methods to improve Zero Trust models. However, these studies mainly focus on traffic identification mechanisms and have not evaluated them within a complete enterprise network architecture.

The second research direction evaluates and guides the deployment of commercial platforms. Benjelloun et al. [13] analyzed Next-Generation Firewall deployment recommendations in enterprise networks and emphasized the role of Security Policies, Network Segmentation, and Zero Trust in enhancing multi-layered defense capabilities. Nevertheless, the research is primarily deployment-oriented and has not built an experimental environment to evaluate the effectiveness of each security mechanism.

The third research direction focuses on architecture and technical standards. Palo Alto Networks technical documentation details the operation of the PAN-OS Administrator Guide, App-ID Technology Brief, and DNS Security Administrator Guide [7]–[9], while NIST guidelines emphasize the roles of Defense in Depth, Network Segmentation, and Zero Trust [4], [6]. In addition, Gartner's Magic Quadrant reports continue to position Palo Alto Networks as a leading vendor [14].

Although the above studies have affirmed the role of NGFWs in enterprise security, there remain three notable research gaps. First, most works evaluate individual functions separately—such as DPI, IPS, or App-ID—without examining the effectiveness of simultaneously integrating multiple security mechanisms in a complete enterprise architecture. Second, the number of studies deploying

experimental models including VLANs, Security Zones, DMZs, NAT, App-ID, and DNS Filtering within the same environment is limited. Third, direct comparative studies between models using NGFWs and traditional access control methods using Router ACLs on the same test system are still scarce, especially studies providing quantitative evaluations through practical operational scenarios [4], [6], [7]–[10], [13].

Table 1. Comparison of related studies with the proposed research

Work	**Enterprise Model**	**Experiment**	**Router ACL Comparison**	**Contributions**
Heino et al. (2022) [10]	✗	✓	✗	Endpoint-aware inspection, DPI
Heino et al. (2022 IEEE Access) [11]	✗	✓	✗	Endpoint-aware inspection framework
Heino et al. (2024) [12]	✗	✓	✗	Endpoint application identification
Benjelloun et al. (2024) [13]	∆	✗	✗	Enterprise NGFW deployment
Palo Alto Networks [7]-[9]	✗	✗	✗	Vendor implementation guide
NIST SP800-41 [4]	✓	✗	✗	Firewall architecture
NIST SP800-207 [6]	✓	✗	✗	Zero Trust architecture
This research	✓	✓	✓	Experimental enterprise model

Motivated by this, this paper proposes an enterprise network security model based on Palo Alto Networks NGFW and evaluates the model's effectiveness on the EVE-NG simulation platform. The model is built according to an enterprise network architecture consisting of multiple functional VLANs, a DMZ zone, and Internet connectivity, while integrating Security Zones, Security Policies, NAT Policies, App-ID, and DNS Filtering to implement a Defense in Depth architecture. The effectiveness of the model is validated through four experimental scenarios: (i) application-based access control using App-ID; (ii) protection of Web servers in the DMZ zone; (iii) prevention of access to malicious domains using DNS Filtering; and (iv) direct comparison with the model using Router ACLs.To clarify the position of

this study compared to published works,Table 1 summarizes typical studies on NGFWs and enterprise network security.

From Table 1, it can be seen that previous studies have primarily focused on technological analysis or deployment guidelines, while lacking the construction and evaluation of a complete enterprise security model combining multiple protection mechanisms within the same experimental environment. This study aims to address this gap by designing an enterprise network model based on Palo Alto NGFW and evaluating its effectiveness through unified testing scenarios.

The main contributions of this work are summarized as follows.

First, this paper proposes an enterprise network security model based on Palo Alto Networks NGFW, integrating Security Zones, Security Policies, NAT Policies, App-ID, and DNS Filtering mechanisms into a multi-layered defense architecture suitable for modern enterprise environments.

Second, this paper builds an experimental environment on the EVE-NG platform simulating an enterprise network with multiple functional VLANs, a DMZ zone, and Internet connectivity, enabling the evaluation of security policies under conditions close to actual deployment.

Third, the study designs four experimental scenarios representing common enterprise security situations to evaluate the application control capability, DMZ server protection, DNS access filtering, and security policy enforcement of the proposed model.

Finally, this paper performs qualitative and quantitative evaluations while directly comparing the model with a Router ACL-based setup to clarify the advantages of Palo Alto NGFW in application-layer control, policy formulation flexibility, and system protection effectiveness.

The rest of this paper is organized as follows. Section 2 presents the theoretical background on enterprise network security and security architecture design principles. Section 3 introduces the Palo Alto Networks NGFW architecture and core technologies used in the proposed model. Section 4 describes the security model, experimental environment, and test scenarios. Section 5 presents and analyzes the experimental results, alongside a comparison with the Router ACL-based model. Finally, Section 6 concludes the achievements, outlines the limitations of the study, and suggests directions for future work.

Theoretical Background and Enterprise Network Security Architecture

Enterprise Network Security Architecture

In modern enterprise network architecture, system protection relies not only on network perimeter isolation but also requires the synchronous combination of Defense in Depth and Network Segmentation. According to NIST technical guidelines and intensive research on network architecture, dividing systems into functional VLANs combined with a Demilitarized Zone (DMZ) helps isolate public-facing services from the internal network and prevents the rapid spread of malware [4], [13]. Furthermore, the shift from traditional security models to a Zero Trust architecture emphasizes the principle of "never trust, always verify" for every resource access request, regardless of whether it originates from inside or outside the network perimeter [6], [17].

Modern Enterprise Threats and NGFW Capabilities

The evolution of sophisticated cyberattack forms requires security systems to have deep inspection capabilities at the application layer rather than relying solely on IP addresses and service ports [1], [2]. The main threats and their corresponding Next-Generation Firewall (NGFW) response mechanisms are summarized in Table 2.

Table 2. Summary of modern threats and NGFW defense mechanisms

Threat / Challenge	Brief Description	NGFW Defense Mechanism	Reference
Malware / Ransomware	Data encryption attacks, malware distribution via Web/Email.	Deep Packet Inspection (DPI), Threat Prevention.	[1], [2]
Lateral Movement	Malware spreading laterally between devices within the internal network.	Security Zone, Micro-segmentation, User-ID.	[6], [13], [17]
DNS Attack	Exploiting the Domain Name System protocol for C&C attacks or malicious redirection.	DNS Security, Real-time malicious domain filtering.	[1], [9]
Encrypted Applications	Attack traffic hidden inside encrypted HTTPS applications (TCP/443).	App-ID, SSL/TLS Decryption, Content-ID.	[7], [10], [11], [12]
Insider Threat	Security risks caused by internal users accessing resources without authorization.	Context-based Security Policy, Role-based Access Control.	[4], [6]

Security Design Principles

The security architecture design process in this study adheres to the following four core principles:

Defense in Depth: Building multiple consecutive barrier layers (from the perimeter, network segmentation, and DMZ to application control) so that if one layer is breached, subsequent layers can still prevent the incident [4].

Zero Trust Architecture: Applying continuous authentication and verification principles to all traffic flows, without implicitly trusting any device or user even within the internal network [6], [17].

Least Privilege: Granting the minimum necessary access rights to users and applications to complete tasks, thereby minimizing the impact scope when an incident occurs [6].

Default Deny: All traffic is automatically blocked unless explicitly defined as allowed in the security policy [4].

Next-Generation Firewall Evolution

The evolution of network access control devices has gone through three main stages:
Router Access Control List (ACL): Operates based on Layer 3 and Layer 4 information (source IP, destination IP, transport port), suitable for static networks but incapable of distinguishing applications sharing the same port (e.g., HTTPS on port 443) [4].

Stateful Firewall: Adds connection state tracking mechanisms, helping to control packets more accurately but remaining limited due to the lack of deep content inspection capabilities at the application layer [4].

Next-Generation Firewall (NGFW): Comprehensively integrates technologies such as port-independent application identification (App-ID), user identification (User-ID), deep packet inspection (DPI), and intrusion prevention systems on a single platform [7], [8], [10], [13]. Table 3 summarizes the comparison of network access control device generations.

Table 3. Comparison of network access control device generations

Comparison Criteria	**Router ACL**	**Stateful Firewall**	**Next-Generation Firewall (NGFW)**
OSI Model Layer	Layer 3 (Network) & Layer 4 (Transport)	Layer 3, Layer 4 (with session state tracking)	From Layer 3 to Layer 7 (Application)
Application Identification	Not supported (identified via port numbers only)	Not supported (relies on Port/Protocol)	Deeply supported via App-ID (independent of service ports) [8]
Content Inspection (DPI)	Not supported	Not supported	Supports deep inspection and malware prevention [10]
Advanced Security Integration	None	Basic (Inspection state)	Full (IPS, DNS Security, WildFire, URL Filtering) [7], [9]
Policy Flexibility	Low (must block/allow entire ports)	Medium (based on IP/Port)	High (builds policies by application, user, zone) [13]

Evaluations from reputable market research organizations such as the Gartner Magic Quadrant for Network Firewalls also confirm that NGFWs play a core component role in modern enterprise IT infrastructure protection strategies [14].

Palo Alto Networks NGFW Technologies Supporting the Proposed Security Model

After Section 2 established the principles of enterprise network security, this section introduces the Palo Alto Networks NGFW platform and the core technologies used to realize the proposed security model. The content focuses on the PAN-OS architecture, traffic processing mechanisms, and components such as Security Zones, Security Policies, NAT, App-ID, and DNS Security. This serves as the foundation for building the experimental model presented in Section 4.

Overview of Palo Alto Networks NGFW

The Next-Generation Firewall (NGFW) by Palo Alto Networks is designed to extend access control capabilities from the network layer to the application layer by integrating multiple security mechanisms on a single platform. Unlike Router ACLs or Stateful Firewalls, which only inspect information at the network and transport layers, Palo Alto NGFWs can identify applications, users, and traffic content before applying security policies [4], [7], [8], [10]. Consequently, the system can enforce granular control policies based on the nature of the application rather than relying solely on IP addresses or service ports [7].

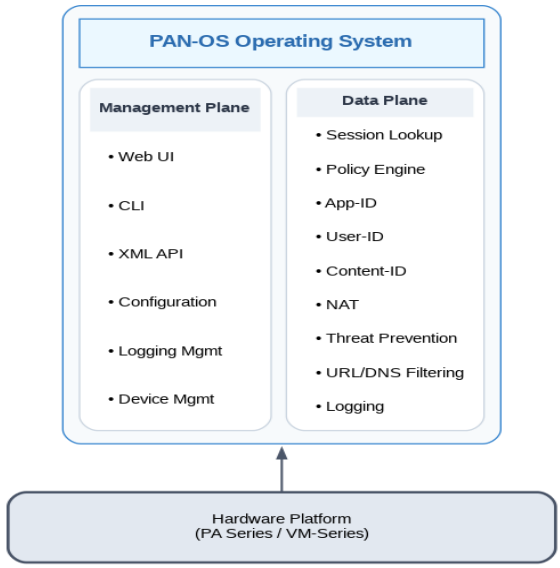

Figure 1. Overall architecture of Palo Alto Networks NGFW and the PAN-OS operating system. (Adapted from Palo Alto Networks PAN-OS Administrator's Guide [7].)

Architecturally, Palo Alto NGFWs are built on the PAN-OS operating system with two main components: the Management Plane and the Data Plane [7]. The Management Plane is responsible for configuration management, policy storage, logging, and providing an administrative interface for administrators. Meanwhile, the Data Plane handles real-time traffic processing, including session establishment, application identification, security policy enforcement, Network Address Translation (NAT), and traffic logging. Separating these two processing planes helps optimize

system performance while ensuring that administrative tasks do not impact packet processing [7].

Additionally, PAN-OS integrates a centralized logging mechanism that records comprehensive information about connection sessions, applied policies, and security events. This serves as a vital data source for monitoring, incident investigation, and evaluating the effectiveness of the security system [7].

Core Technologies of Palo Alto Networks NGFW

The protection capabilities of Palo Alto NGFWs are formed through the coordination of multiple security mechanisms operating simultaneously on the same connection session. In this study, the technologies utilized include Security Zones, Security Policies, NAT Policies, App-ID, and DNS Security.

Security Zone

A Security Zone is a mechanism that divides the network into independent security domains [4], [6], [7]. Each Zone represents a distinct trust level and management scope, such as LAN, DMZ, Internet, or Server Farm. All traffic passing through Zones must be evaluated by Security Policies before being permitted to traverse [7]. Dividing Security Zones helps reduce the impact scope when an incident occurs while supporting the implementation of Network Segmentation and Defense in Depth principles presented in Section 2.

Security Policy

Security Policies are the central component of Palo Alto NGFWs [4], [7], [8]. Unlike traditional ACLs that only inspect IP addresses and service ports, PAN-OS Security Policies can simultaneously use multiple attributes to make decisions, including: Source Zone, Destination Zone, Source Address, Destination Address, User, Application, Service, URL Category, and Action. Consequently, administrators can build flexible policies, such as allowing only the Microsoft Teams application to operate between two network zones during office hours while blocking entertainment applications despite them using the same HTTPS protocol [7].

NAT Policy

Network Address Translation (NAT) is a mechanism that maps IP addresses between network zones to support Internet connectivity and publish internal services [7]. In PAN-OS, NAT is processed independently of Security Policies. Administrators can deploy Source NAT to allow internal machines to access the Internet or Destination NAT to publish Web servers within the DMZ zone without altering the internal network address structure [7]. The separation between NAT and Security Policies simplifies administration and reduces errors during deployment.

App-ID

App-ID is a signature technology characteristic of Palo Alto Networks [7], [8], [10], [11], [12]. Instead of relying on port numbers or transport protocols, App-ID uses various identification techniques such as application signature analysis, TCP session inspection, protocol analysis, and Deep Packet Inspection (DPI) to accurately identify the active application [8], [10]. Even when multiple applications use HTTPS over TCP port 443, App-ID can still distinguish between YouTube, Microsoft Teams, Google Drive, Zoom, and Facebook, helping enterprises control traffic at the application layer.

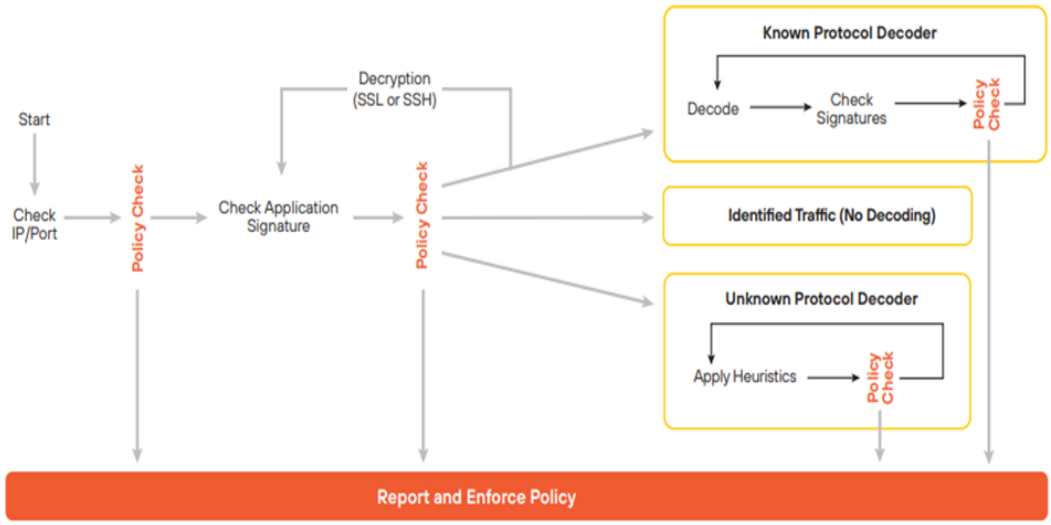

Figure 2. Principles of application identification by App-ID technology in Palo Alto Networks NGFW. (Source: Palo Alto Networks, App-ID Technology Brief [8].)

As illustrated in Figure 2, the application identification process begins by inspecting the IP and service port information of the packet. If this is insufficient to determine the application, the system continues to analyze application signatures. For encrypted traffic, App-ID can integrate SSL/TLS decryption mechanisms to perform deep packet inspection [8], [10]. Subsequently, traffic is forwarded to known or unknown protocol decoders to identify the application. Once the application is identified, the NGFW executes the corresponding security policy and records logs for monitoring purposes.

DNS Security

DNS Security (DNS Filtering) enables the inspection of all DNS queries before users connect to destination servers [9]. If a domain name is on the malicious list or carries a high risk level, the NGFW will block the query right at the domain resolution stage. This mechanism significantly reduces the risk of accessing Command and Control (C&C) servers, phishing websites, or domains distributing malware [9]. In this study, DNS Security is utilized to construct one of the experimental scenarios to evaluate the capability to block access to malicious domains.

Traffic Processing Workflow in Palo Alto NGFW

Unlike Router ACLs, which inspect each packet independently, Palo Alto NGFWs process traffic on a session basis (Session-Based Processing) [7]. Every connection must go through multiple steps before being permitted to traverse the system, including: receiving the initial packet, establishing the connection session, determining the source and destination Security Zones, matching Security Policies, identifying the application via App-ID, performing NAT (if applicable), applying security mechanisms (such as DNS Security, URL Filtering, or Threat Prevention), and recording logs (Traffic Log and Threat Log). This workflow ensures that all

traffic is multi-layer inspected before passing through the system, aligning with the principles of Defense in Depth and Zero Trust [4], [6], [17].

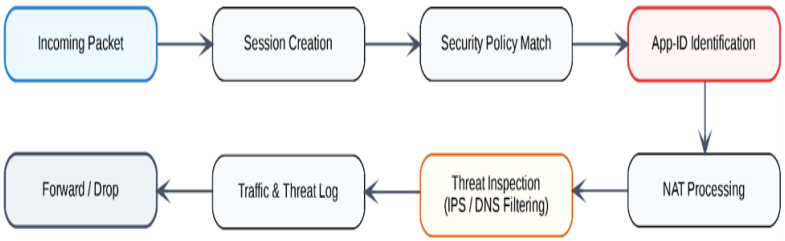

Figure 3. Traffic processing workflow in Palo Alto Networks NGFW. (Developed by the authors based on the PAN-OS packet processing workflow [7].)

Role of NGFW Technologies in the Proposed Model

The Palo Alto NGFW acts as the central device enforcing security policies throughout the entire enterprise architecture [4], [6], [7], [8], [13]. To clarify the connection between technological mechanisms and the experimental process, Table 4 summarizes the role of each NGFW component in the test scenarios of the study.

Table 4. Summary of NGFW technology roles in the proposed model and experimental scenarios

NGFW Technology	Primary Role in Architecture	Application in Experimental Scenarios
Security Zone	Separates logical network boundaries and isolates functional zones	Scenarios 1, 2, 3, 4
Security Policy	Enforces access control policies based on the Default Deny principle	Scenarios 1, 2, 3, 4
Destination NAT	Publishes Web server services from the DMZ zone to the Internet	Scenario 2
App-ID	Identifies and controls traffic in detail at the application layer	Scenarios 1, 4
DNS Security	Detects and blocks access to malicious domain names	Scenario 3
Logging & Monitoring	Collects connection session logs and monitors system operations	All scenarios

Proposed Enterprise Network Security Model

This section presents the architecture of the proposed enterprise network security model, the experimental environment, the deployment process of security policies, and evaluation scenarios to verify the effectiveness of the solution utilizing Palo Alto Networks NGFWs. The model is built on the EVE-NG platform to simulate a typical

enterprise network featuring multiple functional zones and access control policies at both the network and application layers.

Architecture of the Proposed Security Model

Figure 4 presents the overall architecture of the proposed enterprise network security model. The architecture is constructed according to the principles of Defense in Depth, Network Segmentation, and Zero Trust Architecture, where all traffic between network zones must be inspected before being permitted to traverse the system [4], [6], [13], [17]. The Palo Alto Networks NGFW acts as the central device, functioning as a Policy Enforcement Point (PEP) within the Zero Trust architecture [6].

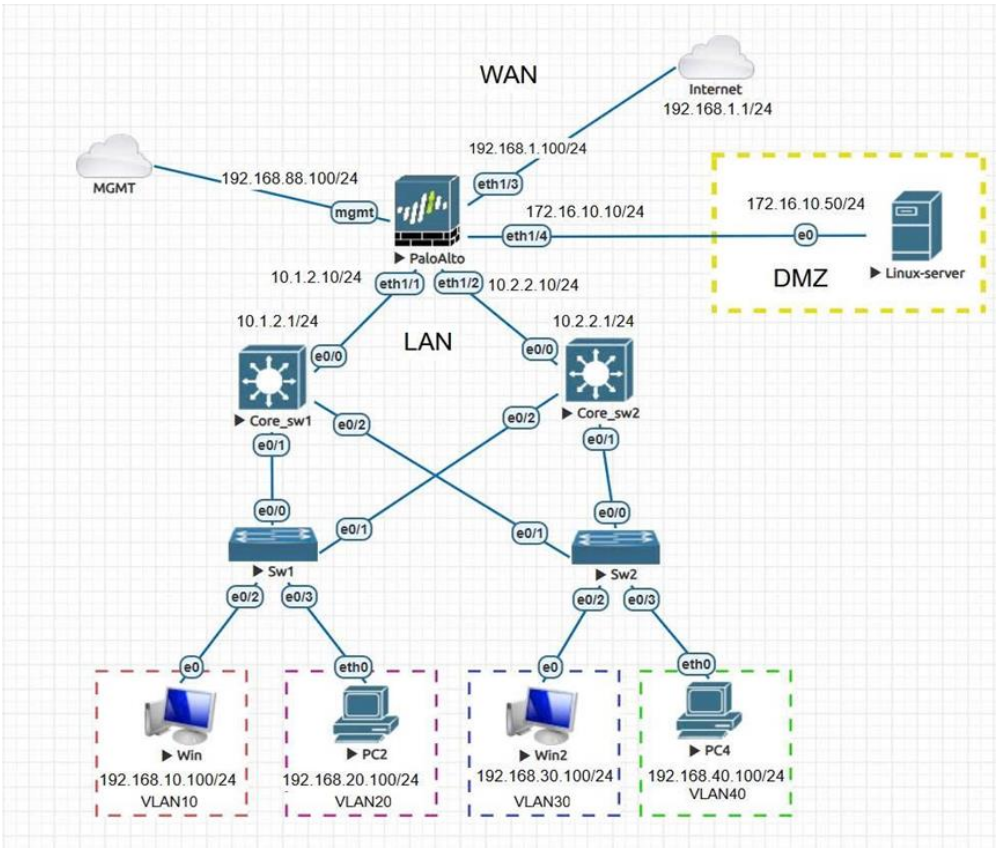

Figure 4. Architecture of the proposed enterprise network security model

The model comprises four main functional zones:

Management Zone (MGMT): Dedicated to NGFW system administration via an independent management port, separating management traffic from data traffic [7].

Trust Zone (LAN): Represents the internal enterprise network, consisting of multiple VLANs corresponding to functional departments [4].

DMZ Zone: Houses servers providing public-facing services [4].

Untrust Zone (WAN/Internet): Represents the Internet and external connections.The LAN network architecture consists of two hierarchical switching layers. Two Core Switches distribute traffic between VLANs and connect directly to the Palo Alto

NGFW via Layer 3 links, underneath which are two Access Switches serving workstations. The internal network is divided into four VLANs (VLAN 10, 20, 30, and 40 corresponding to network ranges 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, and 192.168.40.0/24, respectively) to reduce broadcast domains and isolate departments [4].

The DMZ zone deploys a Linux server (172.16.10.50/24) providing Web services, isolating it from the internal network, limiting access from the Internet, and mitigating the risk of lateral attack propagation [4]. The Internet network connects via the ethernet1/3 interface of the NGFW (192.168.1.0/24) to support access testing, NAT, DNS Security, and App-ID. The management network connects the Management port via the 192.168.88.0/24 range to enhance security and avoid data traffic congestion [7].

Experimental Environment

In this study, the entire model is deployed on the EVE-NG Community Edition platform to simulate an enterprise network complete with all components such as NGFWs, routers, switches, servers, and clients. Utilizing a simulation environment allows for testing multiple security policies under controllable conditions while reducing deployment costs compared to physical systems.

Table 5. Experimental environment configuration

Device Component	**Configuration / Software**	**Version**
Simulation Platform	EVE-NG Community Edition	Community
Firewall	Palo Alto VM-Series NGFW	PAN-OS 11.1
Router / Switch	Cisco IOSv & IOSv L2	15.x
DMZ Server	Ubuntu Linux (Apache Web Server)	Ubuntu 22.04
Client	Windows 10	22H2
Network Structure	4 VLANs, 4 Security Zones, NAT, DNS Security	-

Deployed Security Policies

To realize the proposed security model, technical policies and configurations are established synchronously. Table 6 summarizes the configuration components of the security policies within the model.

Table 6. Summary of configured security policies in the model

Configuration Component	Primary Purpose	Reference Basis / Technology
Security Zone	Divides logical network boundaries into independent zones	[4], [6], [7]
Static Route	Establishes routing tables between network partitions	Standard static routing
NAT Policy	Configures Source NAT (Internet access) and Destination NAT (DMZ publishing)	[7]
Security Policy	Establishes access control rules based on Zone, IP, and Service	[4], [6], [7]
App-ID	Identifies and controls traffic in detail at the application layer	[7], [8], [10]–[12]
DNS Security	Inspects and blocks queries to malicious domain names	[9]
Logging & Monitoring	Records connection session logs and security events	[7]

All policies are configured following the deny-by-default principle, ensuring that any traffic not explicitly permitted is automatically blocked, adhering to the Least Privilege and Zero Trust principles [4], [6], [7].

Experimental Evaluation Scenarios

The proposed model is evaluated through four experimental scenarios reflecting typical security situations within enterprise networks:

Scenario 1 (Application-Based Access Control - App-ID): Evaluates the capability to distinguish applications running on the same HTTPS port (TCP/443), allowing legitimate applications while blocking inappropriate ones, and comparing this with traditional Router ACL methods [8].

Scenario 2 (DMZ Server Protection): Evaluates the enforcement of Security Policies and Destination NAT when securely publishing Web services to the Internet, preventing unauthorized external access to the internal network [4], [7].

Scenario 3 (Blocking Malicious Domain Access): Tests the effectiveness of DNS Security in detecting and blocking DNS queries directed at C&C servers or malicious websites [9].

Scenario 4 (Comparison with Router ACL): Deploys identical policies on both Router ACLs and Palo Alto NGFWs to compare application control capability, policy flexibility, logging granularity, and resource protection capability according to NIST SP 800-41 criteria [4].

Table 7. Application of technologies in experimental scenarios and evaluation objectives

Experimental Scenario	Primary Technology Used	Technical Objective	Key Evaluation Metric
Scenario 1	App-ID, Security Policy	Granular application traffic control	Application identification accuracy
Scenario 2	Security Policy, NAT Policy	Protect and publish DMZ servers	Access allow/block ratio
Scenario 3	DNS Security	Filter and block malicious domain queries	Malicious malware detection and blocking rate
Scenario 4	Router ACL vs. NGFW	Comparative security capability evaluation	Overall control capability

Evaluation Metrics

To ensure objectivity and quantify ability for the evaluation process in Part 5, the evaluation metrics are defined directly based on experimental configurations and international security standards:

Application Identification Accuracy: The rate at which App-ID accurately identifies different application types.

Policy Enforcement Effectiveness: The ability to accurately enforce security policy rules (Default Deny and context-based rules).

Unauthorized Access Blocking Rate: The success rate of blocking unauthorized traffic flows from the Internet into the DMZ and internal zones.

DNS Blocking Success Rate: The capability to detect and block resolution queries to malicious domain names.

Logging Capability: The completeness and granularity of the connection session logging system for incident investigation purposes.

Configuration Complexity: An evaluation of management and policy deployment complexity between traditional Router ACLs and NGFWs.

Experimental Results and Discussion

Evaluation of Application Control Capability via App-ID

(1) Objective

The first experimental scenario aims to evaluate the application-layer access control capability of the Palo Alto Networks NGFW, directly measuring the Application Identification Accuracy metric. The security policy is configured using App-ID

technology to block the YouTube application for users belonging to VLAN10, while still allowing VLAN30 to access it normally. The objective of this scenario is to verify the capability to distinguish traffic from applications that share the same HTTPS protocol on TCP port 443.

(2) Policy

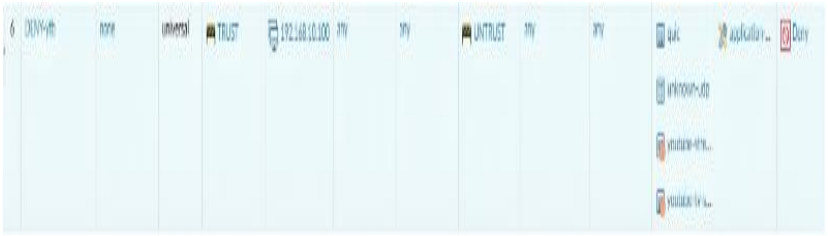

Figure 5. DENY-ytb policy

The "DENY-ytb" policy uses App-ID to identify applications belonging to the YouTube group instead of relying on port numbers. The firewall denies session traffic identified as youtube-base and youtube-streaming from VLAN10 to the Internet.

(3) Results

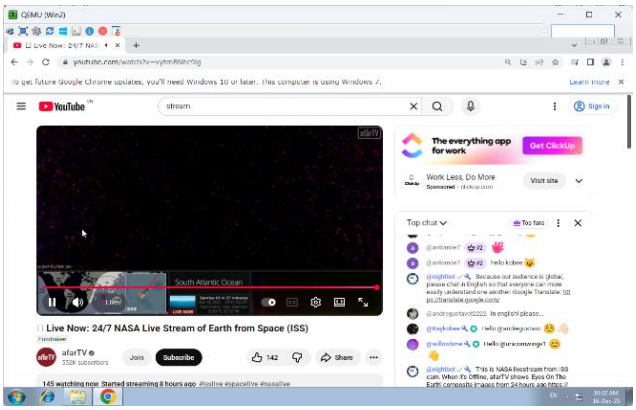

Figure 6. Device in VLAN30 successfully streaming YouTube videos

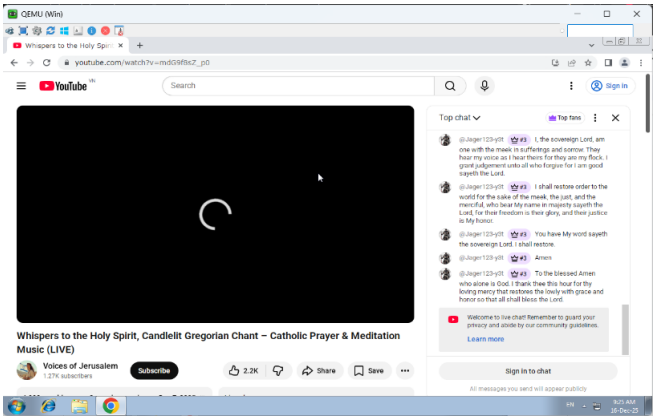

Figure 7. Device in VLAN10 unable to stream YouTube videos

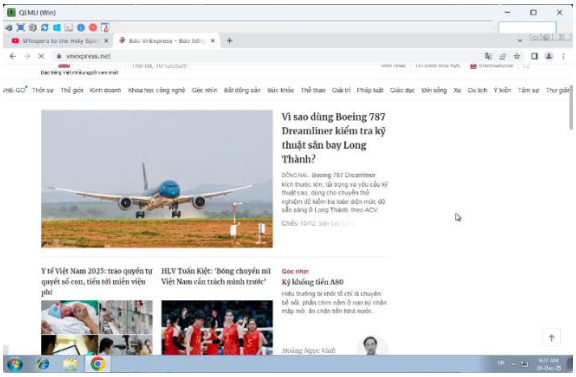

Figure 8. Device in VLAN10 still successfully accesses the VnExpress website

The experimental results show that the device belonging to VLAN30 streams YouTube videos normally (Figure 6), while the device belonging to VLAN10 cannot stream videos because the traffic is blocked by the App-ID policy (Figure 7). However, the same VLAN10 device still successfully accesses the VnExpress website (Figure 8). This proves that the firewall controls traffic based on application rather than blocking all HTTPS traffic, achieving absolute accuracy in delineating encrypted traffic flows.

Evaluation of DMZ Server Protection Mechanism

Objective: The second scenario evaluates the capability to publish Web services to the Internet while maintaining isolation between the DMZ zone and the internal network, aiming at the Unauthorized Access Blocking Rate metric.

Configuration:

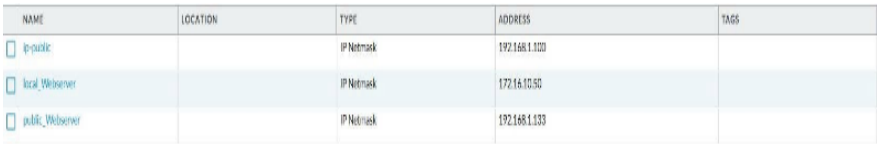

Figure 9. Address Objects definitions

Figure 10. NAT Policy

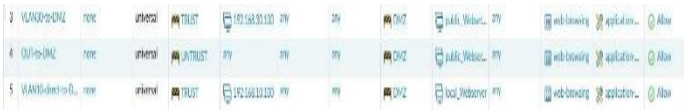

Figure 11. Security Policy for DMZ

The firewall uses Destination NAT to map public IP addresses to the Web server within the DMZ zone, while the Security Policy only permits HTTP services to be accessed from designated network zones [4], [7].
Results:

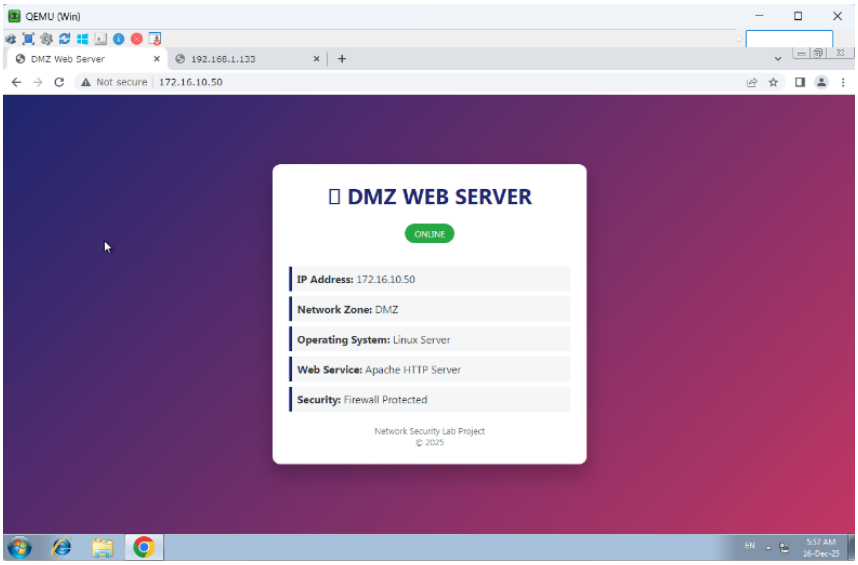

Figure 12. VLAN10 device accessing the Web Server in the DMZ zone

The results show that both internal users and external Internet devices successfully access the Web Server through the published address. Throughout the process, the server remains protected by the NGFW's Security Policy rather than being directly accessed, effectively minimizing the risk of unauthorized access from the Untrust zone to the internal system.

5.3. Evaluation of DNS Filtering

Objective: The third scenario evaluates the enforcement capability of the DNS Filtering policy (DNS Blocking Success Rate) when users deliberately change their DNS Server to bypass access control mechanisms.
Configuration:

Figure 13. Policy Information “Allow-DNS-Cloudflare” and “Block-DNS-bypass”.

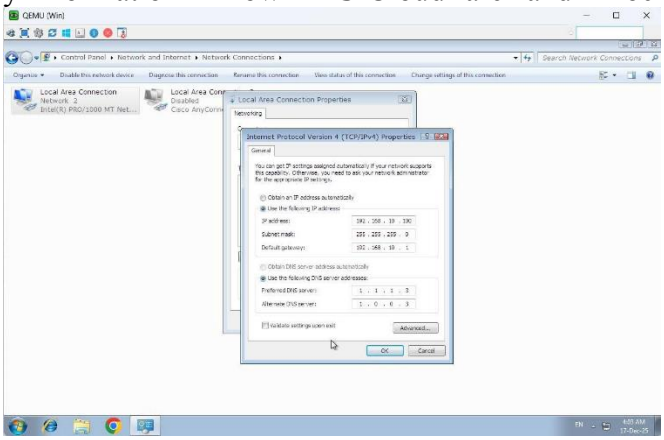

Figure 14. DNS configuration on the client

Results:

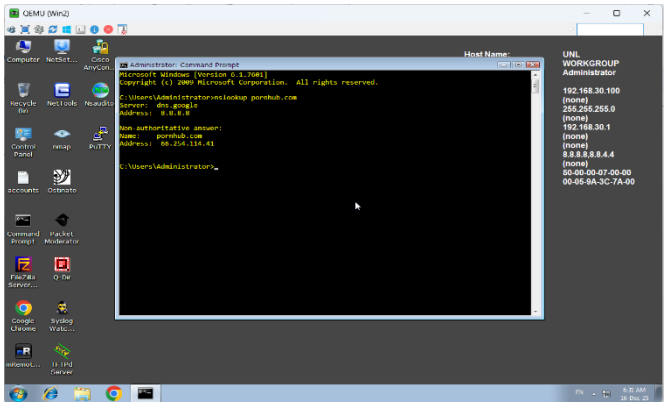

Figure 15. DNS results before filtering

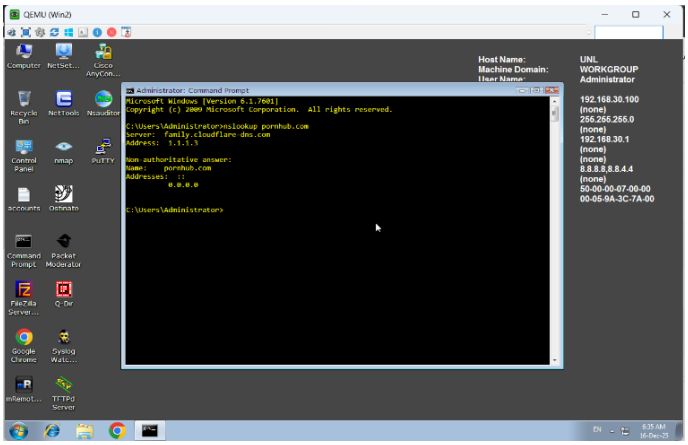

Figure 16. DNS results after filtering

Discussion: Before applying the policy, the test domain name was successfully resolved using the public DNS server. After activating DNS Filtering [9], the same query only returned the address 0.0.0.0, proving that the firewall blocked the DNS query right at the network perimeter layer. This demonstrates that the DNS Filtering policy is thoroughly enforced even when users change their DNS server, effectively preventing potential connections to C&C command-and-control servers.

Comparison with Router ACL

To evaluate the advantages of the proposed model, the study implemented an additional control model using a Router Access Control List (ACL). The model was built on the same EVE-NG platform to ensure identical experimental conditions [4].

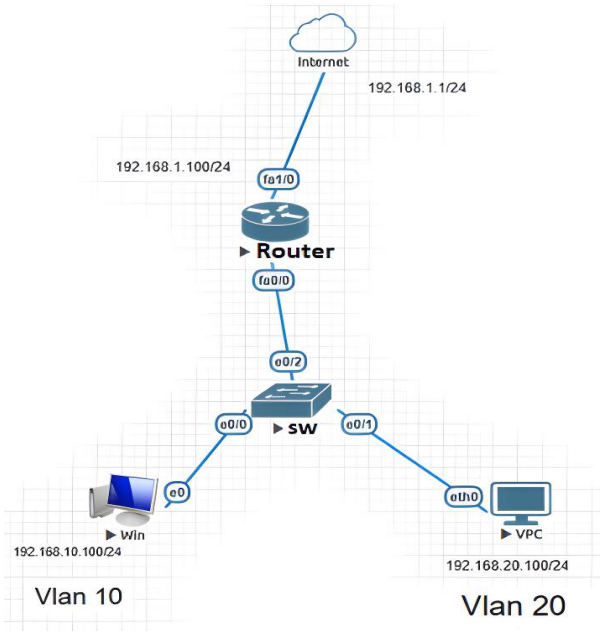

Figure 17. Experimental model using Router ACL as a control group

The ACL is configured to block all HTTPS traffic from VLAN10 by denying TCP packets using port 443.

```
Router
ip access-list extended BLOCK_HTTPS
 deny tcp 192.168.10.0 0.0.0.255 any eq 443
 deny udp 192.168.10.0 0.0.0.255 any eq 443
 permit ip any any
interface FastEthernet0/0.10
 ip access-group BLOCK_HTTPS in
interface FastEthernet0/0.20
 ip access-group BLOCK_HTTPS in
```

Figure 18. Access Control List configuration blocking HTTPS traffic.

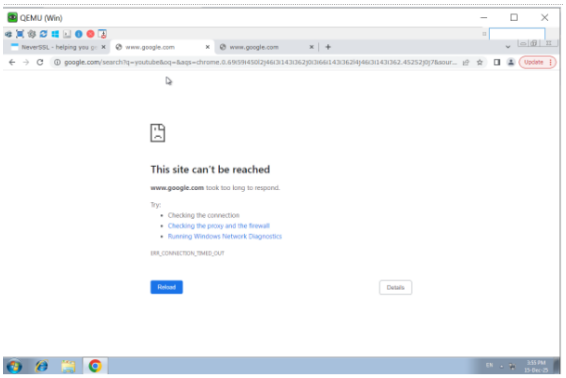

Figure 19. VLAN10 device cannot access Youtube when the ACL blocks TCP/443.

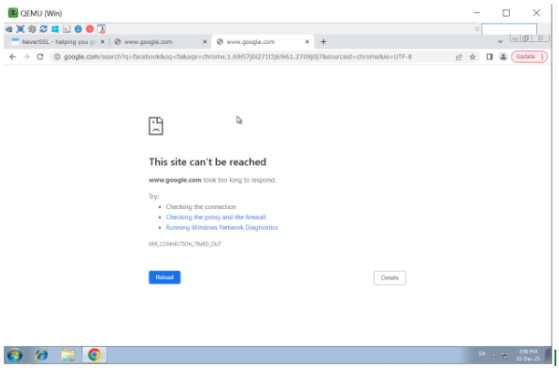

Figure 20. VLAN10 device cannot access Facebook when the ACL blocks TCP/443.

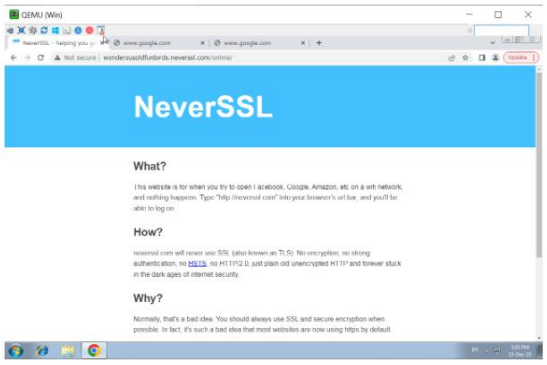

Figure 21. VLAN10 device can still access NeverSSL using HTTP.

The experimental results show that the Router ACL cannot distinguish between Web applications operating on the same TCP port 443. When the ACL blocks HTTPS, both YouTube and Facebook become inaccessible even though they are distinct applications. Conversely, the NeverSSL page using the HTTP protocol on TCP port 80 functions normally. This demonstrates that Router ACLs only perform control at

the network and transport layers, completely lacking the application recognition capabilities of an NGFW.

Discussion of Experimental Results

(a) Effectiveness of the Proposed Security Model

The experimental results demonstrate that the enterprise security model based on Palo Alto Networks NGFW effectively meets access control and resource protection requirements in a multi-zone enterprise network environment. By combining Security Zones, Security Policies, NAT Policies, App-ID, and DNS Filtering, the system not only accurately enforces access policies but also maintains traffic segregation between different network zones [4], [6], [7].

The results in Scenario 1 prove that App-ID allows security policies to be enforced based on the nature of the application rather than relying solely on IP addresses or service port numbers. Although YouTube and many modern Web services utilize the HTTPS protocol over TCP port 443, the NGFW accurately identifies YouTube traffic to apply a denial policy, while legitimate Web applications such as VNExpress remain accessible normally [7], [8]. In Scenario 2, NAT and Security Policies are configured synchronously to securely publish Web services within the DMZ zone to the Internet, minimizing the risk of unauthorized access. The results in Scenario 3 confirm the effectiveness of DNS Filtering in preventing access to malicious domains right at the domain resolution stage [9].

Overall, the experimental results align with the design and fully comply with NIST recommendations for building multi-layered security systems and modern Zero Trust architectures [4], [6], [7].

(b) Overview Comparison with Router ACL

Table 7 summarizes the main evaluation criteria, highlighting the superior advantages of the proposed model based on Palo Alto Networks NGFW compared to traditional Router ACL solutions.

Table 7. Summary of evaluation results for the proposed security model

Evaluation Criteria	Router ACL	Palo Alto NGFW (Proposed Model)
IP/Port Control	Yes	Yes
Application Control	No	Yes (App-ID) [7], [8]
HTTPS Control	Only blocks entire TCP/443	Granular per-application filtering
NAT Policy	Basic	Policy-based flexibility [7]
DNS Security/ Filtering	No	Yes (Automated real-time filtering) [9]
DMZ Protection	Yes, but manually configured	Tightly integrated Security Policy + NAT [4], [7]
Logging	Limited	Detailed per session and application [7]
Scalability	Low	High (Supports SASE/Zero Trust integration) [6], [17]
Enterprise Suitability	Medium	High [4], [13]

(c) System Resource Performance Evaluation

Analyzing the correlation between deep security policy enforcement capability and hardware resource consumption of NGFWs is a vital factor when designing and operating Zero Trust-oriented network systems [6, 17]. Therefore, beyond qualitative evaluation, this study conducts quantitative measurements of three core performance metrics: CPU utilization, RAM utilization, and packet processing latency across various load conditions.

(i) Evaluation of NGFW CPU Utilization

Figure 22 illustrates the CPU resource fluctuations of the Palo Alto Networks NGFW operating in baseline mode (Baseline - L3/L4 Only) compared to when all advanced security features are enabled (Full Security, including App-ID and DPI).

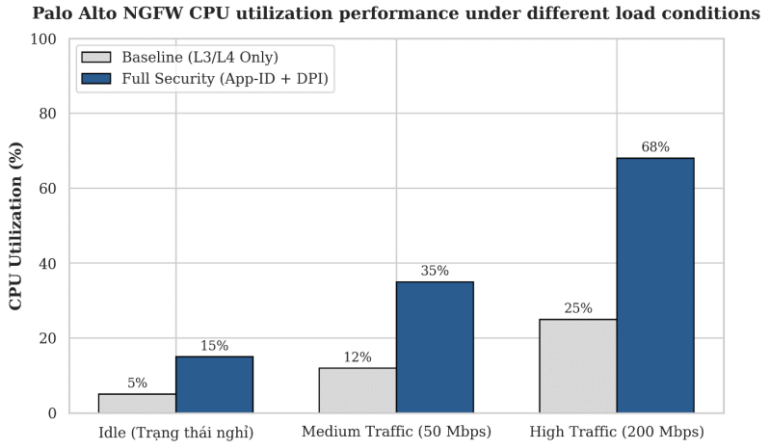

Figure 22. Palo Alto NGFW CPU utilization performance under different load conditions.

The measurement results show that:

• At Idle state, CPU consumption remains low at 5% (Baseline) and 15% (Full Security), respectively.

• Under Medium Traffic (50 Mbps), CPU utilization rises to 12% for the baseline mode and 35% with Full Security enabled.

• Under High Traffic (200 Mbps) conditions, where the system concurrently handles deep packet inspection and application identification, CPU utilization peaks at 25% (Baseline) and 68% (Full Security).

Although there is an increase when enabling advanced security features, this CPU load remains fully under control and ensures the device is not overloaded.

(ii) Evaluation of NGFW RAM Utilization

Figure 23 illustrates the RAM memory usage performance of the Palo Alto NGFW corresponding to load milestones and security configurations.

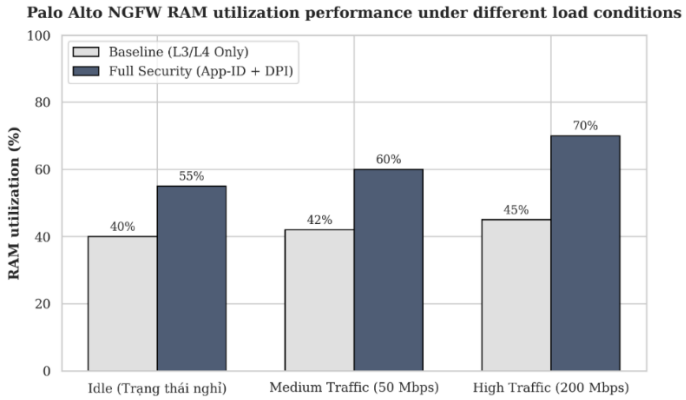

Figure 23. Palo Alto NGFW RAM utilization performance under different load conditions

Experimental results indicate that:

- At Idle state, RAM consumption stands at 40% (Baseline) and 55% (Full Security).
- At Medium Traffic (50 Mbps), the RAM usage rate slightly shifts to 42% and 60%.
- At High Traffic (200 Mbps), RAM reaches 45% (Baseline) and a maximum of 70% under Full Security.

The increase in RAM capacity follows a linear and highly stable trend, with no spikes or memory overflow occurring. This demonstrates the efficiency of Palo Alto Networks' Single-Pass Parallel Processing Architecture, which enables the simultaneous processing of multiple security features in a single inspection cycle while maintaining optimal memory management [7].

(iii) Evaluation of Latency Benchmarked Against Router ACL

Figure 24 compares packet processing latency between the traditional Router ACL model and the Palo Alto NGFW under different security configuration levels.

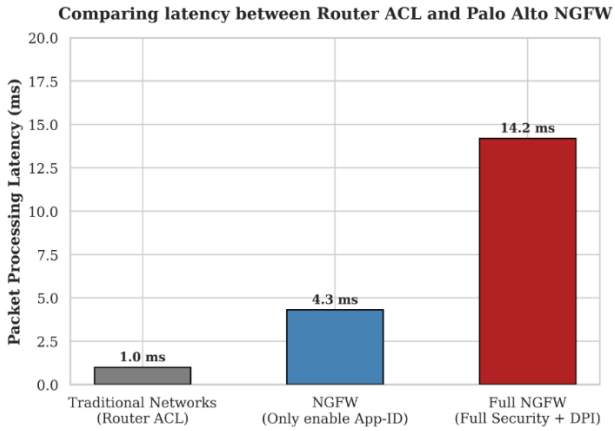

Figure 24. Comparing latency between Router ACL and Palo Alto NGFW.

The latency test results reveal that:
• Traditional Networks (Router ACL): Maintains extremely low processing latency at just 1.0 ms, thanks to hardware switching mechanisms.
• NGFW (Only enable App-ID): When only application identification is enabled, latency increases to 4.3 ms.
• Full NGFW (Full Security + DPI): When all advanced security inspection layers along with decryption are enabled, latency reaches 14.2 ms.
Although deep packet analysis increases latency compared to traditional Router ACLs, the 14.2 ms level remains fully optimized and well within acceptable standard thresholds for enterprise services (typically requiring < 50 ms). This is a completely worthwhile trade-off to achieve comprehensive defense capabilities against modern network threats [6, 17].
(d) Practical Significance, Limitations, and Future Directions
The proposed model is deployed on the EVE-NG platform with an architecture closely resembling a real enterprise network, helping the results accurately reflect operational scenarios. The system features an open structure, allowing easy integration of other advanced security components (such as User-ID, WildFire, Threat Prevention, and GlobalProtect) toward a Zero Trust or SASE architecture [6], [13], [17].
Despite the achieved results, several limitations remain in this study:
• Experimental scenarios focused primarily on access control and policy enforcement, without fully evaluating complex attacks such as ransomware or lateral movement [4].
• Hardware testing was capped at a traffic load of 200 Mbps; in-depth metrics under extreme stress (such as Maximum Throughput or Session Setup Rate) need further investigation in the future.
• The model was deployed in an EVE-NG virtualized environment, requiring further validation on actual physical hardware.

6. Conclusion

This study proposed, deployed, and experimentally evaluated an enterprise network security model based on the Palo Alto Networks Next-Generation Firewall (NGFW) within an EVE-NG simulation environment. Addressing the limitations of traditional access control mechanisms based on Router Access Control Lists (ACLs), the paper constructed a multi-layered security architecture combining Network Segmentation, Security Zones, Security Policies, NAT Policies, App-ID, and DNS Security to enhance traffic control capabilities and protect the system against modern threats [4], [6], [7], [9].

Experimental results demonstrate that the model perfectly meets its design objectives. App-ID technology enables precise identification and control of traffic at the application layer, helping block restricted applications while maintaining access to legitimate HTTPS services [7], [8]. The combination of Security Policy, NAT Policy, and Security Zones effectively protects servers in the DMZ, while DNS Security successfully neutralizes resolution queries to malicious domains directly at the perimeter layer [4], [7], [9]. Notably, quantitative evaluations confirm that the system maintains stable and optimal performance thanks to the Single-Pass architecture,

keeping resource consumption and latency well within permissible enterprise standards.

A comparison with Router ACLs shows that the NGFW is completely superior in terms of application-based control capabilities, policy flexibility, and the ability to integrate multiple security services into a single platform [7], [8]. In practical terms, the model offers high value to medium and large organizations by simplifying administration and optimizing information security [4], [13].

Although there are limitations regarding the scale of testing, the obtained results provide a solid foundation for extending future research, such as physical infrastructure deployment, Zero Trust architecture integration, expanding to Hybrid Cloud/Multi-Cloud models, or integrating SIEM/SOAR platforms and artificial intelligence to elevate cybersecurity incident response capabilities [6], [17].

References

[1] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2024, ENISA, Sep. 2024.
[2] IBM Security, Cost of a Data Breach Report 2024, IBM Corporation, 2024.
[3] Cisco, Cisco Cybersecurity Readiness Index 2024, Cisco Systems, 2024.
[4] K. Scarfone and P. Hoffman, Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41 Revision 1, National Institute of Standards and Technology, 2009.
[5] M. Souppaya and K. Scarfone, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST Special Publication 800-46 Revision 2, National Institute of Standards and Technology, 2016.
[6] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, Aug. 2020.
[7] Palo Alto Networks, PAN-OS Administrator's Guide, Palo Alto Networks Technical Documentation, 2025.
[8] Palo Alto Networks, App-ID Technology Brief, Palo Alto Networks Technical Brief, Feb. 2025.
[9] Palo Alto Networks, DNS Security Administrator Guide, Palo Alto Networks Technical Documentation, 2024.
[10] J. Heino, A. Hakkala, and S. Virtanen, "Study of Methods for Endpoint Aware Inspection in a Next Generation Firewall," Cybersecurity, vol. 5, no. 1, Art. no. 25, 2022.
[11] J. Heino, C. Jalio, A. Hakkala, and S. Virtanen, "A Method for Endpoint Aware Inspection in a Network Security Solution," IEEE Access, vol. 10, pp. 44517–44530, 2022.
[12] J. Heino, C. Jalio, A. Hakkala, and S. Virtanen, "JAPPI: An Unsupervised Endpoint Application Identification Methodology for Improved Zero Trust Models, Risk Score Calculations and Threat Detection," Computer Networks, vol. 250, Art. 110606, 2024.

[13] M. Benjelloun, A. El Mhamdi, et al., "Toward a Modern Secure Network Based on Next-Generation Firewalls: Recommendations and Best Practices," Procedia Computer Science, vol. 238, pp. 1029–1035, 2024.

[14] Gartner, Magic Quadrant for Network Firewalls, Gartner Research, 2024.

[15] J. Postel, "Review on Zero Trust Architecture Applied in Enterprise Next Generation Firewall," in Proceedings of the 2024 IEEE International Conference on Intelligent Computing and Information Technology (InCIT), 2024.

[16] "Endpoint Security Reinforcement via Integrated Zero-Trust Systems," Computers & Security, Elsevier, 2023.

[17] "Zero Trust Networks: Evolution and Application from Concept to Practice," Computers, Materials & Continua, 2025.

[18] K. Neupane, R. Haddad, and L. Chen, "Next-Generation Firewall for Network Security: A Survey," in Proceedings of the International Conference on Computing, Networking and Communications (ICNC), 2018.

[19] Palo Alto Networks, Best Practices for Security Policy Optimization, Palo Alto Networks Technical Documentation, 2025.