TẠP CHÍ KHOA HỌC ĐẠI HỌC CỬU LONG
https://tapchikhdhcl.edu.vn
https://vjol.info.vn/index.php/dhcl

ĐÁNH GIÁ HIỆU NĂNG VÀ TRIỂN KHAI HỆ THỐNG VPN NỘI BỘ BẢO MẬT SỬ DỤNG OPENVPN TRÊN UBUNTU SERVER

Võ Khánh Minh[1], Trương Võ Lộc Đỉnh, Nguyễn Tuấn Kiệt, Trần Thị Thúy[1]
[1]Trường Đại học Cửu Long
[*]Email: tranthithuy@mku.edu.vn

Ngày nhận bài:15/12/2025; Ngày phản biện: 06/01/2025; Ngày duyệt bài:27/01/2026

TÓM TẮT

Nghiên cứu này thiết kế, triển khai và đánh giá hiệu năng của hệ thống mạng riêng ảo (VPN) nội bộ bảo mật trên Ubuntu Server bằng OpenVPN. Mục tiêu là nâng cao bảo mật và truy cập tài nguyên từ xa trong môi trường học thuật. Phương pháp gồm cài đặt OpenVPN Access Server, thiết lập kênh truyền dữ liệu mã hóa SSL/TLS và áp dụng iptables theo chính sách "Default Deny". Kết quả thực nghiệm cho thấy hệ thống kết nối an toàn với độ trễ thấp (tăng thêm trung bình 2-3 ms), thông lượng ổn định đạt khoảng 85 Mbps đối với truyền tệp và 70 Mbps đối với truy cập web nội bộ , đảm bảo mọi lưu lượng từ xa được mã hóa bằng thuật toán AES-256-CBC. Giải pháp cung cấp VPN linh hoạt, chi phí thấp, hỗ trợ làm việc từ xa an toàn, bảo vệ tính toàn vẹn và bí mật dữ liệu.

Từ khóa: *VPN, OpenVPN, Ubuntu Server, Mạng riêng ảo, SSL/TLS, iptables, Truy cập từ xa, An ninh mạng.*

ABSTRACT

This study designs, deploys, and evaluates a secure internal VPN on Ubuntu Server using OpenVPN. It aims to improve network security and remote access in academic environments. The methodology involves installing OpenVPN Access Server, establishing SSL/TLS encrypted channels, and applying iptables with a "Default Deny" policy. Experiments show secure connections with low latency (average increase of 2-3 ms) , stable throughput of approximately 85 Mbps for file transfers and 70 Mbps for internal web access , ensuring all remote traffic is encrypted using the AES-256-CBC algorithm. The solution is robust, flexible, cost-effective, and enhances secure remote work while protecting data confidentiality and integrity.

Keywords*: VPN, OpenVPN, Ubuntu Server, Virtual private network, SSL/TLS, iptables, Remote access, Network security.*

1. Giới thiệu

Trong kỷ nguyên chuyển đổi số, xu hướng làm việc từ xa và kết hợp ngày càng phổ biến, an ninh mạng và truy cập an toàn vào tài nguyên nội bộ trở thành thách thức lớn, đặc biệt trong môi trường học thuật (Cisco, 2023; Gartner, 2022). Các kết nối mạng truyền thống dễ bị nghe lén, chặn dữ liệu và tấn công người trung gian, đe dọa tính bí mật và toàn vẹn thông tin nhạy cảm (Kumar & Singh, 2021). Nghiên cứu này tập trung thiết kế và triển khai mạng riêng ảo (VPN) sử dụng OpenVPN, công nghệ mã nguồn mở dựa trên SSL/TLS, nổi bật với bảo mật cao, linh hoạt, đa nền tảng và chi phí thấp (OpenVPN Technologies, 2024; Stallings, 2017). Hệ thống được triển khai trên Ubuntu Server, nền tảng ổn định, hướng bảo mật và được cộng đồng hỗ trợ mạnh (Canonical Ltd., 2024).

Trong bối cảnh gia tăng mạnh mẽ của các hình thức làm việc và học tập từ xa, nhu cầu truy cập an toàn vào tài nguyên nội bộ của tổ chức ngày càng trở nên cấp thiết. Đặc biệt trong môi trường học thuật, nơi dữ liệu nghiên cứu, tài liệu giảng dạy và hệ thống quản lý học tập mang tính nhạy cảm, việc đảm bảo an ninh thông tin là yêu cầu bắt buộc. Các giải pháp VPN thương mại tuy cung cấp mức độ bảo mật cao nhưng thường đi kèm chi phí lớn, phụ thuộc nhà cung cấp và hạn chế khả năng tùy biến, gây khó khăn cho các tổ chức có ngân sách CNTT hạn chế. OpenVPN, với tư cách là một giải pháp mã nguồn mở dựa trên SSL/TLS, nổi lên như một lựa chọn khả thi nhờ tính linh hoạt, khả năng mở rộng và mức độ bảo mật cao. Việc triển khai OpenVPN trên Ubuntu Server - một hệ điều hành hướng đến máy chủ, ổn định và được cập nhật bảo mật thường xuyên - cho phép xây dựng hạ tầng VPN nội bộ đáp ứng đồng thời ba tiêu chí quan trọng: bảo mật - hiệu năng - chi phí. Tuy nhiên, trên thực tế, nhiều nghiên cứu trước đây chủ yếu tập trung vào khía cạnh lý thuyết hoặc so sánh giao thức VPN, trong khi thiếu các đánh giá thực nghiệm cụ thể trong môi trường triển khai thực tế, đặc biệt là môi trường học thuật. Do đó, nghiên cứu này được thực hiện nhằm lấp khoảng trống đó thông qua việc thiết kế, triển khai và đo lường hiệu năng của một hệ thống VPN nội bộ hoàn chỉnh, đồng thời phân tích mức độ đáp ứng về bảo mật và khả năng vận hành thực tế. Tổng quan nghiên cứu cho thấy đề tài không chỉ mang ý nghĩa học thuật mà còn có giá trị ứng dụng cao, có thể được sử dụng như một mô hình tham khảo cho các trường đại học, viện nghiên cứu hoặc tổ chức vừa và nhỏ đang tìm kiếm giải pháp truy cập từ xa an toàn, tiết kiệm và dễ quản trị.

Mục tiêu là xây dựng kênh truyền dữ liệu mã hóa (VPN tunneling) đảm bảo xác thực người dùng và truy cập an toàn vào tài nguyên nội bộ. Hệ thống cho phép cán bộ, giảng viên và sinh viên kết nối từ xa bảo mật thông qua cơ chế mã hóa, xác thực và kiểm soát truy cập, đồng thời giảm thiểu rủi ro an ninh mạng và bảo vệ tính bí mật, toàn vẹn dữ liệu (NIST, 2020; ENISA, 2023). Ngoài ra, nghiên cứu đánh giá hiệu năng VPN thông qua độ trễ, thông lượng và chi phí mã hóa, đồng thời so sánh với các giải pháp VPN mã nguồn mở khác, nhằm chứng minh rằng OpenVPN đáp ứng cả yêu cầu bảo mật lẫn hiệu năng mạng cao, phù hợp với các tổ chức học thuật và nghiên cứu có nguồn lực CNTT hạn chế.

2. Cơ sở lý thuyết và các công trình liên quan

Nhiều nghiên cứu đã chỉ ra rằng OpenVPN vượt trội so với các giao thức VPN truyền thống như PPTP và L2TP/IPSec. Điểm mạnh của OpenVPN là tích hợp thư viện OpenSSL, hỗ trợ các thuật toán mã hóa tiên tiến như AES-256, RSA, SHA-256, cùng cơ chế trao đổi khóa an toàn Diffie-Hellman và TLS Handshake, giúp bảo đảm tính bảo mật và toàn vẹn dữ liệu (Kumar & Singh, 2021; Stallings, 2017).

OpenVPN hoạt động ở tầng Giao vận (Transport Layer - tầng 4 OSI) và hỗ trợ cả TCP lẫn UDP. TCP cung cấp truyền dữ liệu

đáng tin cậy trong mạng không ổn định, còn UDP giảm độ trễ, phù hợp với ứng dụng thời gian thực (OpenVPN Technologies, 2024). Nhờ tính linh hoạt này, OpenVPN phù hợp với môi trường yêu cầu cả bảo mật mạnh và hiệu năng cao, như các tổ chức học thuật và doanh nghiệp cần truy cập từ xa (Li et al., 2020).

Trên Linux, đặc biệt là Ubuntu Server, OpenVPN được ưa chuộng nhờ ổn định, dễ mở rộng, và tích hợp tốt với iptables/Netfilter. Các công cụ này cho phép triển khai kiểm soát truy cập chi tiết, chính sách Default Deny và tường lửa trạng thái, giúp ngăn chặn truy cập trái phép và tăng khả năng chống lại các mối đe dọa mạng (NIST, 2020; ENISA, 2023).

Về chi phí và bảo trì, OpenVPN có lợi thế rõ rệt so với các VPN thương mại: mã nguồn mở, dễ tùy chỉnh, minh bạch và nhận cập nhật liên tục. Nếu cấu hình đúng, OpenVPN có thể đạt hiệu năng và mức bảo mật tương đương, thậm chí vượt trội so với Cisco AnyConnect hay FortiGate SSL VPN (Alshamrani et al., 2022; Zhao & Sun, 2021).

Những nghiên cứu trước đây tạo nền tảng vững chắc cho việc triển khai VPN thực tiễn, giúp chống lại các mối đe dọa phổ biến như nghe lén gói tin, chiếm quyền phiên và tấn công vét cạn. Nhờ mật mã hiện đại và nguyên tắc thiết kế mạng an toàn, OpenVPN là giải pháp bảo mật hiệu quả, chi phí thấp, bảo vệ tài nguyên số nội bộ và duy trì truy cập từ xa an toàn cho người dùng hợp pháp.

3. Phương pháp luận và triển khai hệ thống

- Phương pháp nghiên cứu được áp dụng trong đề tài là Nghiên cứu thực nghiệm và phát triển (*Experimental Research and Development*), tập trung vào việc thiết kế, triển khai và đánh giá hiệu năng của hệ thống VPN nội bộ bảo mật. Mô hình kiến trúc được đề xuất bao gồm ba thành phần chính:

- Máy chủ VPN (*VPN Server*): OpenVPN Access Server cài đặt trên hệ điều hành Ubuntu Server 20.04/22.04 LTS.

- Máy khách VPN (*VPN Client*): Ứng dụng OpenVPN Connect dùng cho người dùng đầu cuối.

Mạng nội bộ (*Internal Network*): Bao gồm các máy chủ, dịch vụ và tài nguyên nội bộ cần được bảo vệ và truy cập an toàn thông qua hạ tầng VPN.

Kiến trúc này được lựa chọn nhằm mô phỏng môi trường triển khai thực tế trong các tổ chức hoặc cơ sở học thuật, nơi có nhiều người dùng được xác thực (cán bộ, giảng viên, sinh viên) cần truy cập từ xa vào các hệ thống nội bộ như máy chủ cơ sở dữ liệu, thư viện số hoặc hệ thống quản lý học tập.

3.1. Cấu hình máy chủ và chứng thực

Quá trình triển khai bắt đầu bằng việc cài đặt và cấu hình OpenVPN Access Server trên nền tảng Ubuntu Server. Một dải địa chỉ IP ảo (Virtual IP Range) được xác định để cấp phát động cho các máy khách khi kết nối thành công. Cốt lõi của cơ chế bảo mật trong hệ thống là chứng thực dựa trên chứng chỉ số (Certificate-Based Authentication), được xây dựng theo nguyên tắc Hạ tầng khóa công khai (PKI) (Stallings, 2017; NIST, 2020).

Mỗi máy khách được cấp một tệp cấu hình định dạng .ovpn, chứa chứng chỉ số X.509 và khóa riêng đã được máy chủ ký bởi Certificate Authority (CA) nội bộ. Cơ chế này bảo đảm rằng chỉ các thiết bị hợp lệ, được ủy quyền mới có thể thiết lập kênh mã hóa. Quá trình TLS Handshake giữa máy chủ và máy khách xác thực danh tính hai bên, thiết lập khóa phiên và tạo đường hầm dữ liệu an toàn, được mã hóa bằng AES-256-CBC và kiểm tra toàn vẹn bằng SHA-256 (OpenVPN Technologies, 2024; Zhao & Sun, 2021).

Máy chủ OpenVPN được cấu hình để hỗ trợ đồng thời hai chế độ kết nối UDP (cổng 1194) và TCP (cổng 443) nhằm đảm bảo tính linh hoạt trong các điều kiện mạng khác nhau, đồng thời giúp vượt qua các tường lửa có giới hạn về giao thức. Các tùy chọn DNS redirection và split tunneling được cân nhắc triển khai tùy theo yêu cầu về hiệu năng và mức độ bảo mật dữ liệu.

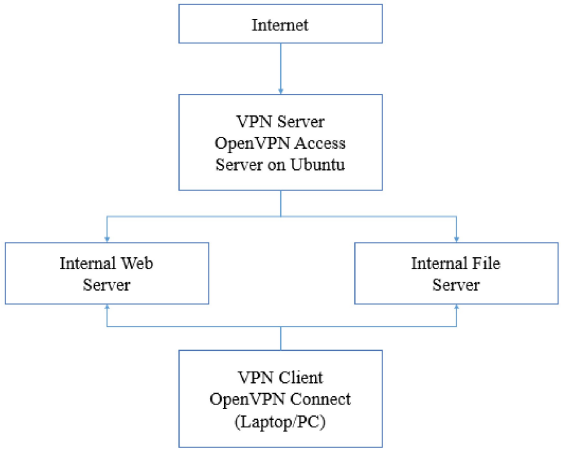
3.2. Thiết lập tường lửa và kiểm soát truy cập

Để tăng cường an ninh hệ thống, chính sách tường lửa iptables nghiêm ngặt được áp dụng. Chính sách Default Deny được thiết lập cho tất cả các lưu lượng đến từ bên ngoài, ngoại trừ cổng dịch vụ của OpenVPN (UDP 1194 hoặc TCP 443), nhằm ngăn chặn mọi kết nối trái phép từ Internet (ENISA, 2023; Canonical Ltd., 2024).

Các quy tắc Forwarding và Network Address Translation (NAT) được cấu hình để cho phép các gói tin đã được giải mã từ VPN đi vào mạng nội bộ một cách an toàn. Nhờ đó, các máy khách VPN có thể hoạt động như các thành viên thực thụ của mạng nội bộ, với quyền truy cập được kiểm soát và giám sát thông qua nhật ký tường lửa (firewall logging) và cơ chế theo dõi phiên (session tracking).

Cấu hình tường lửa trên đảm bảo rằng lưu lượng từ VPN được tích hợp an toàn vào mạng nội bộ mà không làm lộ các dịch vụ bên trong ra Internet. Đồng thời, hệ thống duy trì sự tách biệt rõ ràng giữa lưu lượng đáng tin cậy (trusted VPN traffic) và lưu lượng không đáng tin cậy từ bên ngoài, đảm bảo tính bí mật, toàn vẹn và sẵn sàng (CIA) của tài nguyên tổ chức.

3.3. Sơ đồ kiến trúc hệ thống



Hình 1. Sơ đồ kiến trúc hệ thống.

Hệ thống được thiết kế theo mô hình VPN client-server, trong đó máy khách (VPN Client) từ xa kết nối đến máy chủ VPN thông qua Internet bằng giao thức UDP (cổng 1194) hoặc TCP (cổng 443). Máy chủ VPN được cài đặt OpenVPN Access Server trên nền tảng Ubuntu Server, đóng vai trò là trung tâm xử lý và định tuyến lưu lượng mã hóa.

Sau khi xác thực thành công, VPN Server tạo một đường hầm mã hóa (encrypted tunnel) thông qua giao diện TUN/TAP, cho phép truyền dữ liệu an toàn giữa máy khách và mạng nội bộ. Tất cả lưu lượng của người dùng được mã hóa bằng SSL/TLS và giải mã tại máy chủ trước khi được chuyển tiếp đến các dịch vụ nội bộ.

- Trong mạng nội bộ, hệ thống có thể bao gồm nhiều máy chủ và dịch vụ khác nhau, chẳng hạn như:

- Internal Web Server: cung cấp các ứng dụng web, cổng thông tin hoặc hệ thống quản lý học tập (LMS).

- Internal File Server: lưu trữ dữ liệu, tài liệu học thuật hoặc tệp chia sẻ nội bộ.

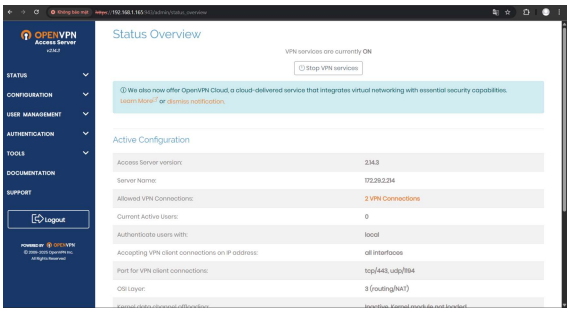
Máy khách sau khi kết nối VPN có thể truy cập các dịch vụ này tương tự như khi ở trong mạng nội bộ, đồng thời vẫn duy trì lớp bảo mật và quyền riêng tư nhờ toàn bộ lưu lượng được mã hóa và gói gọn trong đường hầm VPN. Điều này giúp đảm bảo rằng dữ liệu nhạy cảm của tổ chức không bị lộ ra ngoài, ngay cả khi người dùng truy cập từ môi trường mạng công cộng.

3.4. Tối ưu hóa thông số MTU để giảm phân mảnh gói tin

Trong hệ thống VPN, việc đóng gói (encapsulation) thêm các header bảo mật của OpenVPN và SSL/TLS làm tăng kích thước gói tin gốc. Nếu gói tin vượt quá MTU tiêu chuẩn của Ethernet (thường là 1500 bytes), nó sẽ bị phân mảnh, gây sụt giảm hiệu năng nghiêm trọng. Để khắc phục, hệ thống đã thực hiện cấu hình tối ưu như sau: Sử dụng kỹ thuật Path MTU Discovery (PMTUD) để tìm ngưỡng truyền tải an toàn mà không

gây phân mảnh gói tin trên đường truyền Internet giữa Client và Server. Trong tệp cấu hình OpenVPN, tham số mssfix 1450 được áp dụng để giới hạn kích thước phân đoạn tối đa của các gói TCP, đảm bảo sau khi thêm header VPN, tổng kích thước gói tin vẫn nằm trong giới hạn MTU. Điều chỉnh giá trị tun-mtu xuống mức phù hợp (ví dụ: 1400 - 1470 bytes) tùy thuộc vào thuật toán mã hóa AES-256-CBC được sử dụng, nhằm tránh việc lớp IP phải thực hiện phân mảnh gói tin trước khi gửi đi.

4. Thực nghiệm



Hình 2. Giao diện trang chủ

Hệ thống VPN triển khai thành công trên Ubuntu Server, thiết lập đường hầm mã hóa ổn định giữa máy khách và máy chủ, cho phép truy cập tài nguyên nội bộ an toàn và riêng tư. Thử nghiệm kết nối với lệnh ping và traceroute cho thấy độ trễ thấp, ổn định, đồng thời toàn bộ lưu lượng đi qua giao diện mạng ảo TUN/TAP, bảo đảm không rò rỉ ra mạng công cộng. Kiểm tra IP công cộng của máy khách sau khi kết nối VPN xác nhận địa chỉ được thay bằng IP của VPN Server, tăng cường bảo mật và quyền riêng tư.

Về bảo mật, các quy tắc iptables thực hiện chính sách Default Deny hiệu quả; mọi truy cập trái phép từ bên ngoài đều bị từ chối. Dữ liệu truyền qua VPN được mã hóa bằng AES-256-CBC, đảm bảo thông tin nhạy cảm không bị đọc khi bị đánh chặn.

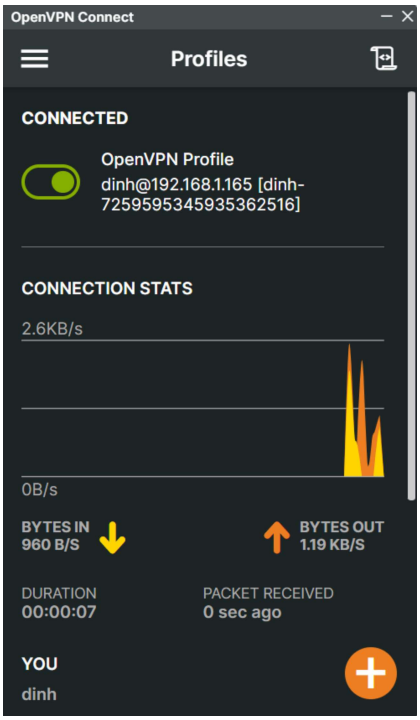
Hiệu năng mạng được đánh giá thông qua tốc độ và độ trễ: độ trễ bổ sung trung bình 2-3 ms, không ảnh hưởng đến trải nghiệm người dùng; thông lượng truyền dữ liệu đạt ~85 Mbps với File Server và ~70 Mbps với Web nội bộ, đủ đáp ứng nhu cầu truy cập các dịch vụ nội bộ và từ xa. Hiệu năng có thể tối ưu thêm bằng nén dữ liệu hoặc lựa chọn thuật toán mã hóa phù hợp.

Mỗi kịch bản thử nghiệm (Ping, Thông lượng) được thực hiện lặp lại 30 lần trong các khung giờ khác nhau để loại bỏ yếu tố ngẫu nhiên của đường truyền. Kết quả thực nghiệm chứng minh rằng OpenVPN trên Ubuntu Server cung cấp giải pháp VPN vừa bảo mật vừa hiệu năng ổn định, phù hợp với môi trường học thuật và các tổ chức có nguồn lực CNTT hạn chế, hỗ trợ truy cập từ xa an toàn và bảo vệ dữ liệu nhạy cảm hiệu quả.

Bảng 1. Kết quả thử nghiệm

Thử nghiệm	Môi trường	Độ trễ (ms)	Thông lượng (Mbps)	Kết quả bảo mật
Ping nội bộ VPN	VPN Client → VPN Server	12 ± 0.5	-	Tất cả gói tin đi qua VPN
Traceroute	VPN Client → Internal Web Server	13 ± 0.8	-	Gói tin đi qua TUN/TAP
Kiểm tra IP công cộng	VPN Client	-	-	IP công cộng hiển thị của VPN Server
Truy cập SSH từ ngoài VPN	Internet → Internal SSH	-	-	Bị từ chối (iptables Default Deny)
Truyền file nội bộ	VPN Client ↔ File Server	15 ± 1.2	85 ± 3.5	Dữ liệu được mã hóa AES-256-CBC
Web truy cập nội bộ	VPN Client ↔ Web Server	14 ± 0.9	70 ± 2.8	Dữ liệu được mã hóa, truy cập thành công

Nghiên cứu đã thiết kế, triển khai và đánh giá thành công một hệ thống VPN nội bộ bảo mật dựa trên OpenVPN trên Ubuntu Server. Hệ thống cho phép cán bộ, giảng viên và sinh viên truy cập an toàn vào tài nguyên nội bộ thông qua kênh dữ liệu mã hóa AES-256-CBC và xác thực bằng chứng chỉ, đồng thời duy trì hiệu năng ổn định với độ trễ thấp và thông lượng phù hợp cho các ứng dụng học thuật và văn phòng từ xa.



Hình 3. Giao diện kết nối thành công đến group PhongA

Giải pháp VPN này tiết kiệm chi phí so với các sản phẩm thương mại và củng cố an ninh mạng tổng thể bằng cách bảo vệ tính riêng tư, toàn vẹn và bảo mật dữ liệu. Tuy nhiên, hệ thống hiện còn hạn chế về khả năng chịu lỗi và mở rộng, đặc biệt khi nhiều người dùng đồng thời hoặc triển khai quy mô lớn.

Các hướng phát triển tương lai gồm: Triển khai High Availability (HA) và Load Balancing để đảm bảo dịch vụ liên tục. Tích hợp xác thực tập trung (LDAP, Active Directory) để quản lý người dùng hiệu quả hơn. Tối ưu cấu hình OpenVPN (MTU, nén dữ liệu, thuật toán mã hóa) nhằm giảm độ trễ, tăng thông lượng và cải thiện trải nghiệm người dùng.

Hệ thống VPN nội bộ dựa trên OpenVPN có tiềm năng mở rộng cho các tổ chức quy mô lớn và các môi trường yêu cầu bảo mật cao, đồng thời tạo cơ sở cho nghiên cứu tiếp theo về tối ưu hóa hiệu năng và quản lý an ninh mạng trong môi trường học thuật và doanh nghiệp.

5. Kết quả nghiên cứu và thảo luận

5.1. Đánh giá hiệu năng hệ thống VPN

Kết quả thực nghiệm cho thấy hệ thống VPN triển khai bằng OpenVPN trên Ubuntu Server đạt hiệu năng ổn định và đáp ứng tốt yêu cầu sử dụng thực tế. Độ trễ trung bình chỉ tăng thêm khoảng 2-3 ms so với kết nối nội bộ thuần túy, mức chênh lệch này được xem là không đáng kể và không ảnh hưởng đến các hoạt động thường ngày như truy cập web nội bộ, làm việc với hệ thống quản lý học tập hay truyền tệp tin.

Thông lượng đạt được ở mức ~85 Mbps đối với truyền tệp và ~70 Mbps với truy cập web nội bộ cho thấy chi phí mã hóa của OpenVPN là chấp nhận được trong môi trường thử nghiệm. Kết quả này phù hợp với các nghiên cứu trước đó, khẳng định rằng OpenVPN khi cấu hình đúng có thể cung cấp hiệu năng tiệm cận kết nối không mã hóa, đặc biệt khi sử dụng giao thức UDP và thuật toán mã hóa AES-256 (Li et al., 2020; Alshamrani et al., 2022).

Một điểm đáng chú ý là hệ thống duy trì được hiệu năng ổn định trong suốt quá trình thử nghiệm, không xuất hiện tình trạng mất kết nối hay suy giảm thông lượng đột ngột, cho thấy tính ổn định cao của OpenVPN Access Server trên nền tảng Ubuntu Server LTS.

Hệ thống đạt được thông lượng ổn định ~85 Mbps là nhờ việc tinh chỉnh các thông số MTU và MSS. Việc thiết lập mssfix giúp ngăn chặn hiện tượng phân mảnh gói tin tại tầng giao vận, từ đó giảm thiểu hao phí

tài nguyên xử lý (overhead) trên máy chủ Ubuntu và cải thiện đáng kể tốc độ truyền tải dữ liệu so với cấu hình mặc định.

5.2. Đánh giá mức độ bảo mật

Về khía cạnh bảo mật, kết quả kiểm thử chứng minh rằng hệ thống đáp ứng đầy đủ các yêu cầu an ninh cơ bản và nâng cao. Việc áp dụng chứng thực dựa trên chứng chỉ số X.509 giúp loại bỏ nguy cơ tấn công giả mạo người dùng, trong khi cơ chế TLS Handshake đảm bảo xác thực hai chiều giữa máy khách và máy chủ.

Chính sách tường lửa iptables theo mô hình "Default Deny" hoạt động hiệu quả, khi mọi nỗ lực truy cập trực tiếp vào các dịch vụ nội bộ từ Internet đều bị từ chối. Điều này cho thấy hệ thống đã thiết lập được ranh giới an ninh rõ ràng giữa mạng công cộng và mạng nội bộ, giảm thiểu đáng kể bề mặt tấn công (attack surface).

Việc kiểm tra IP công cộng và luồng lưu lượng mạng xác nhận rằng toàn bộ dữ liệu của người dùng đều được mã hóa và đi qua đường hầm VPN, không xảy ra hiện tượng rò rỉ dữ liệu (IP/DNS leak). Đây là yếu tố đặc biệt quan trọng khi người dùng truy cập từ các mạng công cộng không đáng tin cậy như Wi-Fi quán cà phê hoặc ký túc xá.

5.3. So sánh với các giải pháp khác và thảo luận

So với các giải pháp VPN thương mại, hệ thống OpenVPN được triển khai trong nghiên cứu này có ưu thế rõ rệt về chi phí, khả năng tùy biến và tính minh bạch. Mặc dù thiếu một số tính năng quản trị nâng cao có sẵn trong các sản phẩm thương mại, OpenVPN vẫn đáp ứng tốt các yêu cầu cốt lõi về bảo mật và hiệu năng cho môi trường học thuật.

Tuy nhiên, nghiên cứu cũng chỉ ra một số hạn chế. Khi số lượng người dùng đồng thời tăng cao, hiệu năng có thể bị ảnh hưởng do giới hạn tài nguyên phần cứng và việc xử lý mã hóa tập trung tại một máy chủ. Ngoài ra, hệ thống hiện chưa tích hợp cơ chế dự phòng hoặc cân bằng tải, do đó vẫn tồn tại nguy cơ gián đoạn dịch vụ nếu máy chủ VPN gặp sự cố.

Những hạn chế này mở ra hướng nghiên cứu và phát triển tiếp theo, bao gồm việc triển khai kiến trúc VPN phân tán, áp dụng High Availability, cũng như kết hợp các cơ chế xác thực tập trung để nâng cao khả năng quản lý và mở rộng hệ thống.

5.4. Thách thức về khả năng mở rộng khi số lượng người dùng lớn

Hiện tại, các thử nghiệm chỉ ghi nhận số lượng kết nối đồng thời ở mức rất thấp, khoảng 0 đến 2 người dùng. Trong điều kiện này, hệ thống vẫn hoạt động ổn định và đạt hiệu năng tốt. Tuy nhiên, khi quy mô mở rộng lên 50 hoặc 100 sinh viên truy cập đồng thời, hệ thống VPN sẽ phải đối mặt với nhiều thách thức đáng kể.

Trước hết, máy chủ có nguy cơ bị quá tải CPU do chi phí mã hóa. OpenVPN hoạt động theo mô hình mỗi tiến trình xử lý đơn luồng (single-threaded). Khi phải thực hiện đồng thời các tác vụ mã hóa AES-256-CBC và xác thực SSL/TLS cho khoảng 100 kết nối, CPU của máy chủ Ubuntu Server sẽ chịu áp lực rất lớn. Điều này dẫn đến thời gian xử lý gói tin tăng lên và làm giảm hiệu năng tổng thể của hệ thống.

Bên cạnh đó, thông lượng mạng sẽ bị sụt giảm và độ trễ tăng cao. Khi băng thông của máy chủ phải chia sẻ cho số lượng lớn người dùng, thông lượng thực tế mà mỗi sinh viên nhận được sẽ thấp hơn nhiều so với mức 70-85 Mbps đạt được trong các thử nghiệm với ít người truy cập. Đồng thời, độ trễ cũng không còn duy trì ở mức 12-15 ms mà sẽ tăng lên do hiện tượng tắc nghẽn hàng đợi gói tin tại máy chủ.

Ngoài ra, hệ thống có thể gặp tình trạng cạn kiệt dải địa chỉ IP ảo. Nếu cấu hình ban đầu của dải IP cấp phát động không đủ rộng, các sinh viên kết nối sau sẽ bị từ chối do không còn địa chỉ IP khả dụng để cấp phát cho phiên VPN mới.

Cuối cùng, cần lưu ý đến giới hạn của OpenVPN Access Server. Phiên bản miễn phí thường chỉ cho phép số lượng kết nối đồng thời rất hạn chế, phổ biến là 2 kết nối. Vì vậy, để đáp ứng nhu cầu của 50-100 sinh viên, tổ chức cần cân nhắc nâng cấp lên phiên bản thương mại có bản quyền hoặc chuyển sang sử dụng OpenVPN Community Edition nhằm loại bỏ các giới hạn về số lượng kết nối.

6. Kết luận

Nghiên cứu đã thực hiện thành công việc thiết kế, triển khai và đánh giá thực nghiệm hệ thống mạng riêng ảo nội bộ sử dụng OpenVPN trên nền tảng Ubuntu Server. Thông qua quá trình triển khai thực tế, bài báo rút ra một số kết luận chính sau:

Hệ thống đã xây dựng được một hàng rào bảo vệ vững chắc thông qua cơ chế mã hóa AES-256-CBC và xác thực dựa trên chứng chỉ số X.509. Việc áp dụng chính sách tường lửa "Default Deny" với iptables đã ngăn chặn hiệu quả các truy cập trái phép từ Internet, đảm bảo tính bí mật và toàn vẹn cho tài nguyên nội bộ.

Kết quả thực nghiệm minh chứng rằng OpenVPN đáp ứng tốt nhu cầu sử dụng trong môi trường học thuật với độ trễ thấp (chỉ tăng thêm 2-3 ms) và thông lượng ổn định (~85 Mbps cho truyền tệp). Hệ thống duy trì sự ổn định cao, không xảy ra hiện tượng rò rỉ dữ liệu hay mất kết nối đột ngột.

Giải pháp sử dụng mã nguồn mở giúp tối ưu hóa chi phí đầu tư so với các thiết bị thương mại đắt tiền, trong khi vẫn đảm bảo khả năng tùy biến linh hoạt. Đây là mô hình tham khảo phù hợp cho các tổ chức giáo dục và doanh nghiệp vừa và nhỏ có nguồn lực CNTT hạn chế.

Mặc dù vẫn còn những hạn chế về khả năng chịu lỗi và tính mở rộng khi số lượng người dùng lớn, nghiên cứu đã đặt nền móng vững chắc cho các hướng phát triển tiếp theo như triển khai hệ thống dự phòng (High Availability), cân bằng tải và tích hợp xác thực tập trung (LDAP/AD). Tổng thể, hệ thống VPN được đề xuất là một giải pháp an ninh mạng hiệu quả, góp phần thúc đẩy môi trường làm việc và học tập từ xa an toàn trong kỷ nguyên số.

TÀI LIỆU THAM KHẢO

Canonical Ltd. (2024). *Ubuntu Server documentation*.

Cisco. (2023). *Annual cybersecurity report 2023*. Cisco Systems, Inc.

ENISA. (2023). *Guidelines on secure remote access*. European Union Agency for Cybersecurity.

Kumar, R., & Singh, M. (2021). *Analysis of VPN security mechanisms for remote access networks*. International Journal of Computer Applications, 183(22), 10-18.

Li, X., Chen, Y., & Xu, Z. (2020). *Optimization of OpenVPN performance in academic networks*. Journal of Network and Computer Applications, 157, 102601.

OpenVPN Technologies. (2024). *OpenVPN Access Server documentation*.

Stallings, W. (2017). *Network security essentials: Applications and standards* (6th ed.). Pearson Education.

Zhao, H., & Sun, Y. (2021). *Comparative study of SSL/TLS-based VPN implementations*. IEEE Access, 9, 45830-45842.

Alshamrani, A., Alharbi, T., & Alsaif, A. (2022). *Performance comparison of OpenVPN and commercial VPN solutions*. International Journal of Information Security Science, 11(3), 145-156.