ĐẠI HỌC HUẾ
TRƯỜNG ĐẠI HỌC KHOA HỌC
KHOA CÔNG NGHỆ THÔNG TIN

———-*———-

TIỂU LUẬN

AN NINH MẠNG

TÌM HIỂU VÀ TRIỂN KHAI IPSEC VPN VỚI PHẦN MỀM GIẢ LẬP GNS3

Giảng viên hướng dẫn: **Ths.Võ Việt Dũng**

Sinh viên thực hiện: **Nhóm 10**

1. Lê Thị Thanh Huyền
2. Lê Thị Trang Nhung
3. Trương Nguyễn Thuỳ Dung
4. Phan Hữu Tuấn Kiệt
5. Nguyễn Đức Minh

Thừa Thiên Huế, Tháng 01 năm 2026

LỜI CẢM ƠN

Lời đầu tiên, nhóm chúng em xin gửi lời cảm ơn chân thành nhất đến **Thầy Võ Việt Dũng** – giảng viên trực tiếp hướng dẫn và định hướng. Trong quá trình học tập và tìm hiểu môn "An ninh mạng", chúng em đã nhận được sự giảng dạy tâm huyết, sự quan tâm và hướng dẫn tận tình của Thầy.

Những kiến thức nền tảng đó đã giúp nhóm có cơ sở vững chắc để thực hiện báo cáo **Tìm hiểu và triển khai IPSec VPN với phần mềm giả lập GNS3**.

Chúng em cũng nhận thức rằng trong quá trình làm bài không tránh khỏi những thiếu sót. Do đó, nhóm kính mong nhận được những lời góp ý của Thầy để bài làm ngày càng được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

MỤC LỤC

Danh mục hình ảnh

DANH MỤC CÁC TỪ VIẾT TẮT

STT	Từ viết tắt	Tiếng Anh
1	VPN	Virtual Private Network (Mạng riêng ảo)
2	IPSec	Internet Protocol Security
3	SA	Security Association (Hiệp hội bảo mật)
4	IKE	Internet Key Exchange
5	AH	Authentication Header
6	ESP	Encapsulating Security Payload
7	GNS3	Graphical Network Simulator 3
8	LAN	Local Area Network (Mạng cục bộ)
9	WAN	Wide Area Network (Mạng diện rộng)
10	NAT	Network Address Translation
11	PSK	Pre-Shared Key

MỞ ĐẦU

Trong bối cảnh công nghệ thông tin ngày càng phát triển, việc bảo mật thông tin trong các mạng máy tính trở nên vô cùng quan trọng. VPN (Virtual Private Network – Mạng riêng ảo) là một giải pháp giúp các tổ chức, doanh nghiệp có thể truyền tải dữ liệu qua Internet một cách an toàn, đảm bảo tính riêng tư và bảo mật. Trong đó, IPSec (Internet Protocol Security) là một trong những giao thức VPN phổ biến, cung cấp cơ chế mã hóa và xác thực mạnh mẽ, giúp bảo vệ dữ liệu khỏi các nguy cơ rò rỉ hoặc tấn công từ bên ngoài.

Việc triển khai và thử nghiệm các giải pháp mạng thực tế thường gặp khó khăn về chi phí và cơ sở vật chất. Vì vậy, các phần mềm giả lập mạng như GNS3 (Graphical Network Simulator-3) trở thành công cụ hữu ích, cho phép người học và kỹ sư mạng mô phỏng, triển khai và kiểm thử các cấu hình mạng phức tạp ngay trên máy tính cá nhân.

Đề tài này nhằm mục tiêu tìm hiểu cơ chế hoạt động của IPSec VPN và triển khai mô hình VPN trên GNS3, từ đó giúp người học nắm vững kiến thức về bảo mật mạng, thực hành cấu hình VPN an toàn, đồng thời đánh giá hiệu quả của giải pháp trong môi trường giả lập. Nội dung nghiên cứu sẽ tập trung vào lý thuyết về IPSec, các chế độ kết nối (Tunnel Mode và Transport Mode), phương thức xác thực và mã hóa dữ liệu, cũng như hướng dẫn chi tiết cách cấu hình và kiểm tra hoạt động VPN trong GNS3.

2. Cấu trúc đồ án

Đồ án gồm phần mở đầu, ba chương nội dung, phần kết luận và tài liệu tham khảo, cụ thể:

Chương 1: Cơ sở lý thuyết

Trình bày kiến thức về VPN, giao thức IPSec, các chế độ vận hành và phần mềm giả lập GNS3.

Chương 2: Triển khai VPN trên GNS3

Hướng dẫn cấu hình mô hình VPN Site-to-Site và Client-to-Site, bao gồm chuẩn bị môi trường, cấu hình thiết bị và kiểm tra kết nối.

Chương 3: Kết luận và hướng phát triển

Tổng kết các kết quả đạt được và đề xuất hướng mở rộng đề tài.

CHƯƠNG 1 CƠ SỞ LÝ THUYẾT

1.1 Tổng quan về Mạng riêng ảo (VPN)

Mạng riêng ảo (Virtual Private Network – VPN) là một giải pháp công nghệ cho phép thiết lập kênh liên lạc riêng tư và an toàn trên hạ tầng mạng Internet công cộng. Thông qua các cơ chế như mã hóa dữ liệu và xác thực người dùng, VPN giúp bảo vệ thông tin trong quá trình truyền tải và cho phép người dùng truy cập vào hệ thống, tài nguyên nội bộ từ xa một cách an toàn.

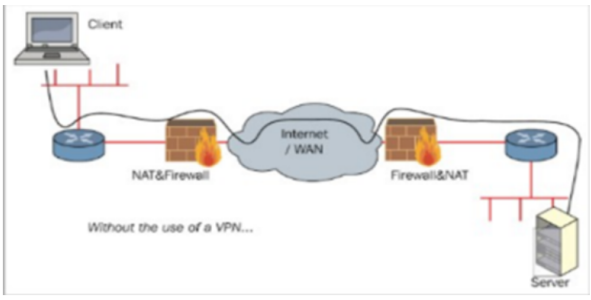

Figure 1.1: Không sử dụng VPN

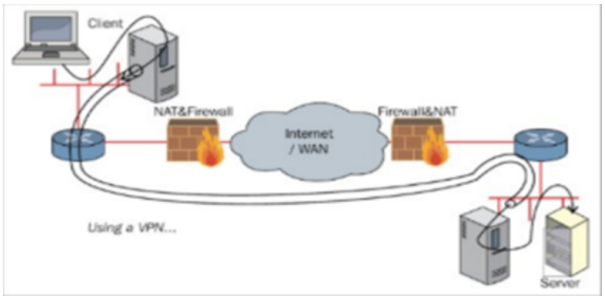

Figure 1.2: Sử dụng VPN

1.2 Phân loại VPN theo mô hình kết nối

Mạng riêng ảo (VPN) là khái niệm chung chỉ việc thiết lập các kênh truyền thông logic (virtual tunnel) trên hạ tầng mạng công cộng nhằm đảm bảo tính bảo mật và riêng tư cho dữ liệu truyền tải. Tùy theo mô hình mạng và mục đích sử dụng, VPN có thể được triển khai theo nhiều hình thức khác nhau. Trong thực tế, hai mô hình VPN cơ bản và được sử dụng phổ biến nhất là **Site-to-Site VPN** và **Remote Access VPN**.

1.2.1 Mô hình Site-to-Site VPN

Site-to-Site VPN là mô hình kết nối các mạng cục bộ (LAN) tại những vị trí địa lý khác nhau thông qua Internet, tạo thành một hệ thống mạng thống nhất. Trong mô hình này, việc xác thực và mã hóa không được thực hiện tại các máy trạm đầu cuối mà được triển khai trên các thiết bị biên (VPN Gateway) đặt tại mỗi site.

Các máy trạm trong mạng nội bộ không cần nhận biết sự tồn tại của VPN mà vẫn trao đổi dữ liệu thông thường theo giao thức TCP/IP. Gateway VPN sẽ đảm nhiệm việc đóng gói, mã hóa dữ liệu và truyền qua đường hầm bảo mật đến Gateway ở site đích, nơi dữ liệu được giải mã và chuyển tiếp đến mạng nội bộ tương ứng.

Mục đích sử dụng

- Kết nối an toàn giữa các mạng LAN của doanh nghiệp hoặc tổ chức tại nhiều chi nhánh.
- Truyền dữ liệu nội bộ qua Internet nhưng vẫn đảm bảo tính bảo mật, toàn vẹn và xác thực.
- Giảm chi phí triển khai so với việc sử dụng các đường truyền riêng chuyên dụng (leased line).
- Hỗ trợ mở rộng hệ thống mạng doanh nghiệp một cách linh hoạt.

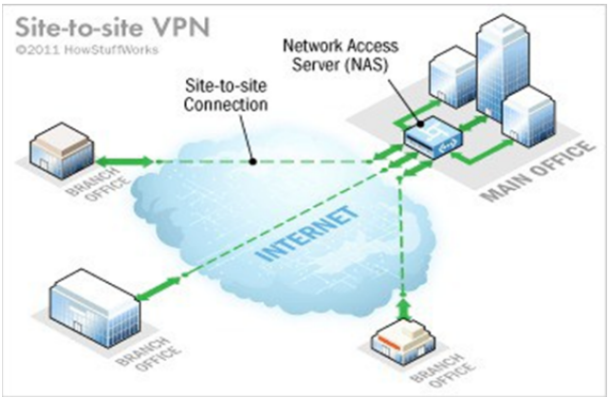

Figure 1.3: Mô hình Site-to-site VPN

1.2.2 Mô hình Remote Access VPN

Remote Access VPN cho phép người dùng cá nhân truy cập từ xa vào mạng riêng của tổ chức thông qua Internet. Trong mô hình này, người dùng cần cài đặt phần mềm VPN Client trên thiết bị đầu cuối để thiết lập kết nối bảo mật đến VPN Server hoặc VPN Gateway của hệ thống.

Sau khi kết nối thành công, thiết bị của người dùng sẽ hoạt động tương tự như một máy nằm trong mạng nội bộ, có thể truy cập các tài nguyên như máy chủ, cơ sở dữ liệu hoặc ứng dụng nội bộ. Mô hình này còn được gọi là *User-to-LAN VPN*.

Ngoài ra, một biến thể mở rộng là *Wireless VPN*, trong đó người dùng truy cập mạng doanh nghiệp thông qua kết nối không dây. Dù ở hình thức có dây hay không dây, dữ liệu đều được truyền qua các đường hầm bảo mật nhằm đảm bảo an toàn thông tin.

Mục đích sử dụng

- Cho phép người dùng truy cập từ xa vào hệ thống mạng riêng hoặc trung tâm dữ liệu (Datacenter).
- Hỗ trợ làm việc từ xa một cách an toàn và linh hoạt.
- Tăng cường bảo mật khi truy cập Internet thông qua việc ẩn địa chỉ IP công khai của người dùng.

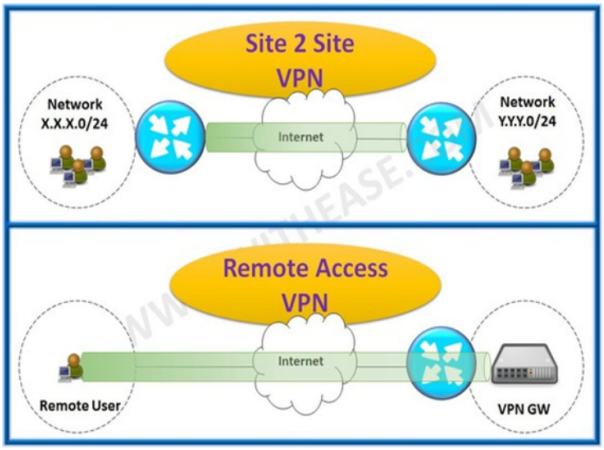

Figure 1.4: Remote Access VPN (Client to site)

1.2.3 Các giao thức VPN phổ biến

PPTP (Point-to-Point Tunneling Protocol): PPTP là một trong những giao thức VPN ra đời sớm, có ưu điểm là cấu hình đơn giản và yêu cầu tài nguyên thấp. Tuy nhiên, giao thức này tồn tại nhiều lỗ hổng bảo mật nghiêm trọng và cơ chế mã hóa yếu, do đó hiện nay hầu như không còn được khuyến nghị sử dụng trong các hệ thống hiện đại.

L2TP (Layer 2 Tunneling Protocol): L2TP không cung cấp cơ chế mã hóa riêng mà thường được triển khai kết hợp với IPSec để đảm bảo tính bảo mật cho dữ liệu truyền tải. So với PPTP, L2TP/IPSec có mức độ an toàn cao hơn, tuy nhiên việc cấu hình và triển khai phức tạp hơn, đồng thời có thể làm giảm hiệu năng hệ thống.

SSL VPN (Secure Sockets Layer VPN): SSL VPN sử dụng giao thức SSL/TLS để thiết lập các đường hầm bảo mật giữa người dùng và hệ thống mạng nội bộ. Ưu điểm nổi bật của SSL VPN là cho phép truy cập các ứng dụng web thông qua trình duyệt mà không yêu cầu cài đặt phần mềm VPN client chuyên dụng, rất phù hợp cho các kịch bản làm việc từ xa và truy cập linh hoạt.

IPSec VPN (Internet Protocol Security VPN): IPSec VPN là một trong những giải pháp VPN được sử dụng rộng rãi nhất hiện nay. Giao thức này cung cấp các cơ chế xác thực, mã hóa và đảm bảo toàn vẹn dữ liệu ở tầng mạng. IPSec có thể hoạt động ở hai chế độ chính là *Transport Mode* và *Tunnel Mode*, phù hợp cho cả kết nối từ xa (Remote Access) lẫn kết nối giữa các mạng (Site-to-Site).

Table 1.1: So sánh các giao thức VPN phổ biến

Giao thức VPN	**Đặc điểm chính**	**Mức độ bảo mật**	**Ứng dụng / Nhận xét**
PPTP	Cũ, dễ cấu hình	Thấp	Ít dùng do nhiều lỗ hổng bảo mật
L2TP/IPSec	Kết hợp IPSec để mã hóa	Trung bình – Khá	An toàn hơn PPTP, cấu hình phức tạp
SSL VPN	Dùng SSL/TLS tạo đường hầm	Cao	Truy cập web, làm việc từ xa, không cần client chuyên dụng
IPSec VPN	Hỗ trợ Tunnel & Transport Mode	Cao	Phù hợp kết nối từ xa và kết nối giữa các mạng

1.3 Giao thức IPSec (Internet Protocol Security)

Bộ giao thức TCP/IP là nền tảng cho sự phát triển của Internet, tuy nhiên trong thiết kế ban đầu, TCP/IP chưa tích hợp đầy đủ các cơ chế bảo mật. Do đó, dữ liệu truyền trên mạng có thể dễ dàng bị nghe lén, giả mạo hoặc chỉnh sửa thông qua các kỹ thuật như bắt gói tin (*packet sniffing*). Trước những hạn chế này, IPSec (Internet Protocol Security) đã được chuẩn hóa bởi IETF từ năm 1998 nhằm bổ sung các cơ chế bảo mật cho giao thức IP.

IPSec hoạt động tại tầng mạng (Network Layer – Layer 3) trong mô hình OSI. Việc triển khai bảo mật tại tầng này cho phép IPSec bảo vệ toàn bộ lưu lượng IP, độc lập với các giao thức tầng trên như TCP, UDP hay các ứng dụng sử dụng chúng. Nhờ đó, mọi hình thức truyền thông dựa trên IP đều có thể được mã hóa và xác thực một cách thống nhất.

Đối với IPv4, IPSec được xem là một tùy chọn triển khai, phụ thuộc vào yêu cầu bảo mật của từng hệ thống. Trong khi đó, với IPv6, IPSec được tích hợp như một thành phần bắt buộc trong kiến trúc giao thức, thể hiện vai trò quan trọng của IPSec trong việc đảm bảo an toàn thông tin trên các mạng Internet thế hệ mới.

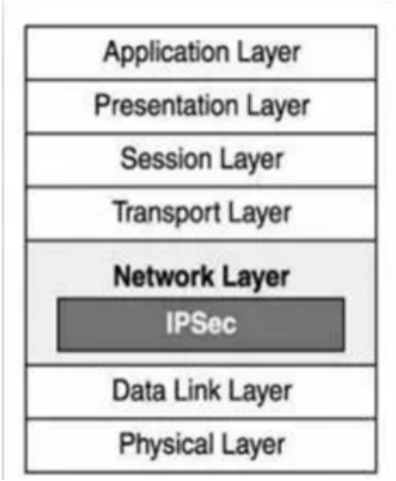

Figure 1.5: IPSec trong mô hình OSI

1.3.1 Kiến trúc và các dịch vụ bảo mật

IPSec là một tập hợp các cơ chế bảo mật phức tạp, được xây dựng dựa trên nhiều chuẩn và kỹ thuật khác nhau, trong đó kiến trúc tổng thể được mô tả trong RFC 2401. Thay vì là một giao thức đơn lẻ, IPSec hoạt động như một bộ khung (*framework*) cung cấp các dịch vụ bảo mật cho giao thức IP ở tầng mạng. Kiến trúc IPSec bao gồm các thành phần chính sau:

- **Giao thức ESP (Encapsulating Security Payload):** Cung cấp chức năng mã hóa dữ liệu và có thể kết hợp xác thực, giúp đảm bảo tính bảo mật và toàn vẹn của thông tin truyền tải.
- **Giao thức AH (Authentication Header):** Cung cấp chức năng xác thực và đảm bảo toàn vẹn dữ liệu, nhưng không thực hiện mã hóa nội dung gói tin.
- **Các thuật toán mật mã và xác thực:** Được sử dụng để mã hóa và kiểm tra tính toàn vẹn của dữ liệu.

- **Cơ chế quản lý và trao đổi khóa:** Được thực hiện thông qua giao thức IKE (Internet Key Exchange), hỗ trợ thiết lập và quản lý các khóa bảo mật một cách an toàn.
- **Miền thực thi (Domain of Interpretation – DOI):** Xác định cách thức diễn giải và áp dụng các tham số bảo mật trong IPSec.

Về mặt chức năng, IPSec có thể được chia thành hai nhóm giao thức chính:

- Nhóm giao thức đóng gói và bảo vệ dữ liệu, bao gồm AH và ESP.
- Nhóm giao thức trao đổi và quản lý khóa, tiêu biểu là IKE, đảm nhiệm việc thiết lập các tham số bảo mật cho quá trình truyền thông.

1.3.2 Các dịch vụ bảo mật do IPSec cung cấp

IPSec cung cấp một tập hợp các dịch vụ bảo mật quan trọng nhằm bảo vệ dữ liệu truyền trên mạng IP, bao gồm:

Bảo mật dữ liệu (Confidentiality): Dữ liệu được mã hóa để ngăn chặn việc đọc trộm trong quá trình truyền tải, thường sử dụng các thuật toán như DES, 3DES hoặc AES.

Toàn vẹn dữ liệu (Data Integrity): IPSec sử dụng các thuật toán băm mật mã như MD5 hoặc SHA-1 để phát hiện việc dữ liệu bị thay đổi trái phép trong quá trình truyền.

Chứng thực nguồn dữ liệu (Data Origin Authentication): Đảm bảo gói tin thực sự được gửi từ nguồn hợp lệ, giúp ngăn chặn các cuộc tấn công giả mạo.

Chống phát lại (Anti-replay): Thông qua việc đánh số thứ tự các gói tin, IPSec có khả năng phát hiện và loại bỏ các gói tin bị gửi lặp lại nhằm chống lại các cuộc tấn công phát lại.

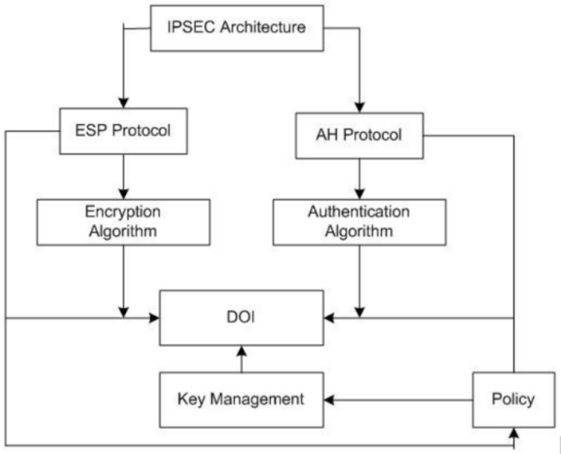

Figure 1.6: Kiến trúc IPSes

1.3.3 Các giao thức thành phần của IPSec

IPSec bao gồm hai giao thức lõi đảm nhiệm việc bảo vệ dữ liệu, cùng với các thành phần hỗ trợ nhằm đảm bảo quá trình truyền thông an toàn và tin cậy.

Authentication Header (AH): AH cung cấp các dịch vụ xác thực và đảm bảo toàn vẹn cho gói tin IP. Giao thức này bảo vệ phần tiêu đề IP và dữ liệu khỏi việc bị thay đổi trong quá trình truyền, đồng thời

xác thực nguồn gửi nhằm ngăn chặn các hành vi giả mạo. Tuy nhiên, AH không thực hiện mã hóa nội dung gói tin, do đó không đảm bảo tính bảo mật về mặt nội dung dữ liệu.

Encapsulating Security Payload (ESP): ESP là giao thức phổ biến nhất trong IPSec, cung cấp cơ chế mã hóa cho phần dữ liệu (*payload*) của gói tin nhằm đảm bảo tính riêng tư. Ngoài mã hóa, ESP còn có khả năng hỗ trợ xác thực và đảm bảo toàn vẹn dữ liệu. Việc mã hóa payload giúp che giấu nội dung và làm xáo trộn lưu lượng truyền thông, từ đó hạn chế khả năng phân tích và nghe lén.

1.3.4 Các thành phần hỗ trợ trong IPSec

Bên cạnh các giao thức lõi, IPSec còn sử dụng một số thành phần hỗ trợ quan trọng, bao gồm:

- **Security Association (SA):** SA là tập hợp các thỏa thuận bảo mật giữa hai thực thể truyền thông, quy định các tham số như thuật toán mã hóa, thuật toán xác thực, khóa bí mật và thời gian hiệu lực của kết nối.
- **Internet Key Exchange (IKE):** IKE là giao thức chịu trách nhiệm thiết lập, trao đổi và quản lý các khóa mật mã một cách an toàn khi khởi tạo kết nối IPSec hoặc VPN.
- **Các thuật toán mật mã (Algorithms):** Bao gồm các thuật toán mã hóa và băm được sử dụng để đảm bảo tính bảo mật và toàn vẹn dữ liệu trong quá trình truyền tải.
- **Cơ chế chống phát lại (Anti-Replay):** IPSec sử dụng số thứ tự gói tin để phát hiện và loại bỏ các gói tin bị gửi lại, qua đó ngăn chặn các cuộc tấn công phát lại (*replay attack*).

1.3.5 Cơ chế hoạt động và Hiệp hội bảo mật (SA)

Theo tiêu chuẩn RFC 4301, Hiệp hội bảo mật (Security Association – SA) là một tập hợp các tham số bảo mật được thiết lập giữa hai thực thể tham gia truyền thông. Các tham số này bao gồm thuật toán mã hóa, thuật toán xác thực, khóa mật mã, cơ chế chống phát lại và thời gian hiệu lực của kết nối.

Trước khi dữ liệu thực tế được truyền qua mạng, các bên tham gia cần tiến hành thương lượng và thiết lập các SA. Quá trình này được thực hiện thông qua giao thức Internet Key Exchange (IKE). IKE đảm nhiệm việc xác thực các thực thể, trao đổi khóa mật mã một cách an toàn và thống nhất các tham số bảo mật cần thiết. Sau khi SA được thiết lập thành công, các gói tin IP sẽ được xử lý và bảo vệ theo đúng các chính sách đã thỏa thuận trong SA.

1.3.6 Các chế độ vận hành: Transport Mode và Tunnel Mode

IPSec hỗ trợ hai chế độ vận hành chính là *Transport Mode* và *Tunnel Mode*, mỗi chế độ phù hợp với các kịch bản triển khai khác nhau. **Transport Mode:** Trong chế độ Transport, IPSec chỉ mã hóa và/hoặc xác thực phần dữ liệu (*payload*) của gói tin IP, trong khi phần tiêu đề IP gốc vẫn được giữ nguyên. Chế độ này thường được sử dụng cho các kết nối trực tiếp giữa hai máy đầu cuối.

Ứng dụng: Kết nối Host-to-Host, chẳng hạn như mô hình Client–Server.

Ưu điểm: Hiệu năng cao do không cần đóng gói thêm tiêu đề mới và vẫn giữ được thông tin điều khiển mạng.

Nhược điểm: Không che giấu được địa chỉ IP thật của các thực thể tham gia kết nối.

Tunnel Mode: Trong chế độ Tunnel, toàn bộ gói tin IP ban đầu, bao gồm cả phần tiêu đề và payload, đều được mã hóa và đóng gói vào bên trong một gói IP mới. Tiêu đề IP mới chứa thông tin định tuyến giữa các thiết bị đầu cuối của đường hầm.

Ứng dụng: Mô hình VPN Site-to-Site hoặc Gateway-to-Gateway.

Ưu điểm: Che giấu hoàn toàn thông tin IP gốc, mức độ bảo mật cao hơn so với Transport Mode.

Nhược điểm: Tốn nhiều tài nguyên hơn do phải thêm tiêu đề IP mới, làm tăng kích thước gói tin và chi phí xử lý.

Table 1.2: So sánh Transport Mode và Tunnel Mode

Tiêu chí	**Transport Mode**	**Tunnel Mode**
Phạm vi mã hóa	Chỉ phần dữ liệu (payload)	Toàn bộ gói IP gốc
Tiêu đề IP	Giữ nguyên header gốc	Tạo header IP mới chứa địa chỉ Gateway
Định tuyến	Router đọc được header gốc	Router chỉ thấy header mới
Bảo mật danh tính	Thấp hơn (lộ IP nguồn/đích)	Cao (che giấu IP gốc)
Đối tượng	Host-to-Host	Site-to-Site, qua Internet

1.4 Tổng quan về phần mềm giả lập GNS3

GNS3 (Graphical Network Simulator 3) là một phần mềm giả lập mạng mã nguồn mở, được sử dụng rộng rãi trong nghiên cứu, giảng dạy và thử nghiệm các mô hình mạng máy tính. Phần mềm cho phép người dùng xây dựng, cấu hình và kiểm thử các hệ thống mạng trong môi trường ảo, từ đó đánh giá hành vi và hiệu năng của mạng trước khi triển khai trong thực tế.

GNS3 hỗ trợ mô phỏng nhiều loại thiết bị mạng như router, switch, firewall và máy chủ. Đặc biệt, phần mềm cho phép chạy các hệ điều hành và firmware mạng thực tế như Cisco IOS, Linux hoặc Windows dưới dạng máy ảo, giúp quá trình cấu hình và vận hành hệ thống mạng đạt mức độ tương đồng cao với môi trường triển khai ngoài thực tế.

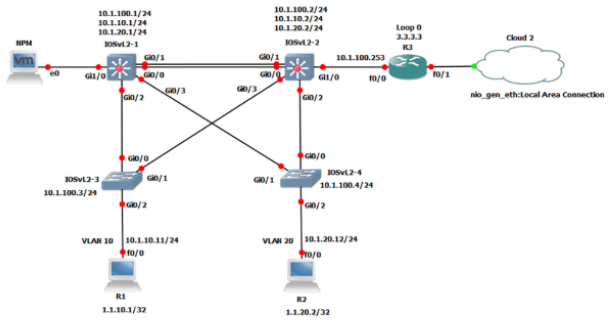

Figure 1.7: Giao diện mô hình mạng trong GNS3

1.4.1 Giới thiệu chung

GNS3 cung cấp giao diện đồ họa trực quan dựa trên cơ chế kéo–thả, cho phép người dùng dễ dàng thiết kế các topo mạng phức tạp. Bên cạnh đó, phần mềm hỗ trợ cấu hình thiết bị thông qua cả giao diện dòng lệnh (CLI) và giao diện đồ họa (GUI), đáp ứng linh hoạt nhu cầu của người học và nhà nghiên cứu.

Ngoài khả năng mô phỏng thiết bị mạng, GNS3 còn tích hợp tốt với các nền tảng ảo hóa như VMware, VirtualBox và Docker. Nhờ đó, người dùng có thể triển khai các máy ảo và container vào cùng một mô hình mạng, tạo điều kiện thuận lợi cho việc nghiên cứu và thử nghiệm các công nghệ như VPN và IPSec trong môi trường gần với thực tế.

1.4.2 Kiến trúc hoạt động của GNS3

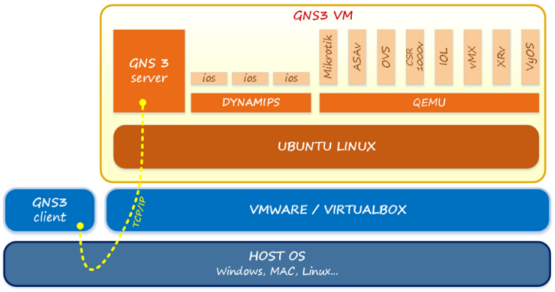

Figure 1.8: Kiến trúc GNS3 VM, Client, Server

GNS3 được xây dựng theo mô hình kiến trúc Client–Server, cho phép tách biệt giữa giao diện người dùng và quá trình xử lý, mô phỏng hệ thống mạng. Cách tiếp cận này giúp nâng cao hiệu năng, khả năng mở rộng và tính linh hoạt trong quá trình triển khai.

GNS3 Client đóng vai trò là thành phần giao diện, chịu trách nhiệm thiết kế và quản lý các mô hình mạng. Thông qua giao diện đồ họa, người dùng có thể tạo topology, cấu hình thiết bị, giám sát trạng thái hoạt động và gửi các yêu cầu điều khiển đến hệ thống.

GNS3 Server là thành phần xử lý trung tâm, đảm nhiệm việc khởi tạo và vận hành các thiết bị mạng ảo, đồng thời quản lý luồng dữ liệu trao đổi giữa các thiết bị trong mô hình. Server có thể được cài đặt trực tiếp trên máy tính cá nhân hoặc triển khai dưới dạng *GNS3 VM* trên các nền tảng ảo hóa. Việc sử dụng GNS3 VM giúp tận dụng tốt hơn tài nguyên phần cứng, cải thiện hiệu năng và đảm bảo sự ổn định khi mô phỏng các mô hình mạng phức tạp.

1.4.3 Lý do lựa chọn GNS3 cho đề tài

Việc lựa chọn công cụ mô phỏng phù hợp có ý nghĩa quan trọng đối với quá trình nghiên cứu và triển khai đề tài. GNS3 được lựa chọn trong nghiên cứu này dựa trên các lý do chính sau:

Tính chính xác và độ tin cậy cao: GNS3 cho phép triển khai và cấu hình các cơ chế bảo mật như IPSec trên các thiết bị mạng ảo sử dụng hệ điều hành và firmware tương tự thiết bị thực tế. Nhờ đó, kết quả thử nghiệm phản ánh sát với môi trường triển khai trong thực tiễn.

Tiết kiệm chi phí: Việc sử dụng GNS3 giúp giảm đáng kể chi phí đầu tư phần cứng mạng chuyên dụng. Người nghiên cứu có thể xây dựng và kiểm thử nhiều kịch bản mạng khác nhau mà không cần trang bị các thiết bị vật lý đắt tiền.

Tính linh hoạt và khả năng mở rộng: GNS3 cho phép dễ dàng thay đổi cấu trúc topo mạng, bổ sung hoặc loại bỏ thiết bị, từ đó hỗ trợ hiệu quả cho việc nghiên cứu, giảng dạy và học tập. Khả năng mở

rộng linh hoạt giúp người dùng thử nghiệm nhiều mô hình và tình huống khác nhau liên quan đến VPN và IPSec.

1.5 Tiểu kết chương 1

Trong Chương 1, đề tài đã trình bày các cơ sở lý thuyết liên quan đến mạng riêng ảo (VPN), giao thức bảo mật IPSec và phần mềm giả lập mạng GNS3. Trước hết, chương đã giới thiệu tổng quan về VPN, các nhu cầu thực tiễn cũng như các mô hình kết nối phổ biến, từ đó làm rõ vai trò của VPN trong việc bảo mật và kết nối mạng trên hạ tầng Internet công cộng.

Tiếp theo, chương đi sâu phân tích giao thức IPSec, bao gồm kiến trúc, các giao thức thành phần, cơ chế hoạt động thông qua Hiệp hội bảo mật (SA) và các chế độ vận hành như Transport Mode và Tunnel Mode. Những nội dung này cung cấp nền tảng lý thuyết cần thiết để hiểu rõ cách thức IPSec đảm bảo tính bảo mật, toàn vẹn và xác thực cho dữ liệu truyền tải trong các hệ thống VPN.

Cuối cùng, chương đã giới thiệu phần mềm giả lập mạng GNS3, kiến trúc hoạt động theo mô hình Client–Server và các lý do lựa chọn GNS3 cho đề tài. Đây là công cụ quan trọng giúp mô phỏng và kiểm thử các mô hình VPN IPSec trong môi trường ảo với độ chính xác cao và chi phí thấp.

Những kiến thức lý thuyết được trình bày trong chương này là cơ sở để triển khai các nội dung thực nghiệm và xây dựng mô hình VPN IPSec trên GNS3 ở các chương tiếp theo.

CHƯƠNG 2 TRIỂN KHAI VÀ CẤU HÌNH HỆ THỐNG TRÊN GNS3

2.1 Môi trường và công cụ thực hiện

Để hiện thực hóa và kiểm chứng giải pháp VPN IPSec, đồ án sử dụng phần mềm giả lập mạng GNS3 (Graphical Network Simulator-3). Đây là công cụ mô phỏng mạng mạnh mẽ, cho phép giả lập phần cứng thực tế của Cisco (Router dòng c7200) chạy trên nền tảng hệ điều hành IOS (Internetwork Operating System) phiên bản 12.4. Điều này đảm bảo các câu lệnh cấu hình và quy trình bắt tay (handshake) của giao thức IPSec diễn ra chính xác như trên thiết bị thật.

2.1.1 Sơ đồ quy hoạch địa chỉ IP

Hệ thống mạng mô phỏng được chia thành ba phân vùng mạng riêng biệt, kết nối với nhau qua hạ tầng Internet giả lập. Chi tiết phân hoạch địa chỉ IP cho các cổng giao tiếp được trình bày chi tiết trong Bảng 2.1.

Table 2.1: Bảng phân hoạch địa chỉ IP chi tiết cho hệ thống

Thiết bị	**Interface**	**Địa chỉ IP / Subnet**	**Vai trò / Mô tả**
R1 (Site A)	F0/0	**10.0.12.1** / 24	Cổng WAN kết nối ra ISP. Đóng vai trò VPN Gateway tại Trụ sở.
	F1/0	**192.168.1.1** / 24	Gateway cho mạng LAN nội bộ A.
R3 (Site B)	F0/0	**10.0.23.3** / 24	Cổng WAN kết nối ra ISP. Đóng vai trò VPN Gateway tại Chi nhánh.
	F1/0	**192.168.2.1** / 24	Gateway cho mạng LAN nội bộ B.
R2 (ISP)	F0/0	10.0.12.2 / 24	Gateway ISP phục vụ Site A.
	F0/1	10.0.23.2 / 24	Gateway ISP phục vụ Site B.
	F1/0	10.0.24.2 / 24	Gateway ISP phục vụ Client.
R4 (Client)	F0/0	**10.0.24.4** / 24	IP WAN của người dùng di động.
PC1	NIC	192.168.1.2 / 24	Máy trạm kiểm thử tại Site A.
PC2	NIC	192.168.2.2 / 24	Máy trạm kiểm thử tại Site B.

2.2 Kịch bản 1: Triển khai VPN Site-to-Site

2.2.1 Mô tả kịch bản và Sơ đồ nguyên lý

Kịch bản này mô phỏng nhu cầu kết nối an toàn giữa Trụ sở chính (Site A) và Chi nhánh (Site B). Dữ liệu trao đổi giữa hai mạng LAN (192.168.1.0/24 và 192.168.2.0/24) cần được truyền tải qua môi trường Internet không tin cậy nhưng vẫn phải đảm bảo tính bí mật, toàn vẹn và xác thực nguồn gốc.

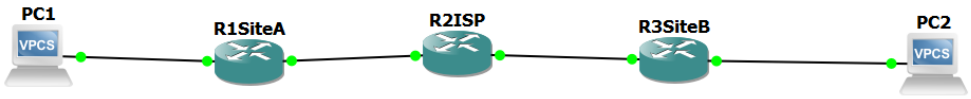

Figure 2.1: Sơ đồ nguyên lý kết nối VPN Site-to-Site trên GNS3

2.2.2 Thông số cấu hình kỹ thuật

Để thiết lập đường hầm VPN Site-to-Site, hai Router biên (R1 và R3) cần được cấu hình các tham số đồng bộ (Symmetry) trong cả hai giai đoạn của giao thức IKE/IPSec. Bảng 2.2 dưới đây liệt kê chi tiết các thông số đã sử dụng trong đồ án.

Table 2.2: Thông số cấu hình IPSec VPN (Site-to-Site)

Hạng mục	**Thông số tại R1 (Site A)**	**Thông số tại R3 (Site B)**
Giai đoạn 1: IKE Phase 1 (ISAKMP Policy)		
Encryption Algorithm	AES	AES
Hash Algorithm	SHA	SHA
Authentication	Pre-shared Key	Pre-shared Key
Diffie-Hellman Group	Group 2 (1024-bit)	Group 2 (1024-bit)
Key String	`vpn123`	`vpn123`
Giai đoạn 2: IPSec Phase 2		
Transform Set	`TSET` (esp-aes, sha-hmac)	`TSET` (esp-aes, sha-hmac)
Mode	Tunnel	Tunnel
Peer IP Address	**10.0.23.3**	**10.0.12.1**
Access Control List (ACL)	Permit 192.168.1.0 → 2.0	Permit 192.168.2.0 → 1.0

2.2.3 Kết quả cấu hình thực nghiệm

Dưới đây là hình ảnh thực tế quá trình cấu hình trên giao diện dòng lệnh (CLI) của thiết bị, khớp với bảng thông số kỹ thuật đã đề ra.

```
R1SiteA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1SiteA(config)#crypto isakmp policy 10
R1SiteA(config-isakmp)# encryption aes
R1SiteA(config-isakmp)# hash sha
R1SiteA(config-isakmp)# authentication pre-share
R1SiteA(config-isakmp)# group 2
R1SiteA(config-isakmp)# exit
R1SiteA(config)#
R1SiteA(config)#crypto isakmp key vpn123 address 10.0.23.3
R1SiteA(config)#
R1SiteA(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
R1SiteA(cfg-crypto-trans)# mode tunnel
R1SiteA(cfg-crypto-trans)# exit
R1SiteA(config)#
R1SiteA(config)#$ 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1SiteA(config)#
R1SiteA(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1SiteA(config-crypto-map)# set peer 10.0.23.3
R1SiteA(config-crypto-map)# set transform-set TSET
R1SiteA(config-crypto-map)# match address 100
R1SiteA(config-crypto-map)# exit
R1SiteA(config)#
R1SiteA(config)#interface f0/0
R1SiteA(config-if)# crypto map CMAP
R1SiteA(config-if)# exit
R1SiteA(config)#end
R1SiteA#wr
*Dec 30 12:57:36.647: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1SiteA#wr
*Dec 30 12:57:36.667: %SYS-5-CONFIG_I: Configured from console by console
R1SiteA#wr
Building configuration...
[OK]
```

Figure 2.2: Cấu hình chi tiết Crypto Map và ACL trên Router R1

```
[OK]
R3SiteB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3SiteB(config)#crypto isakmp policy 10
R3SiteB(config-isakmp)# encryption aes
R3SiteB(config-isakmp)# hash sha
R3SiteB(config-isakmp)# authentication pre-share
R3SiteB(config-isakmp)# group 2
R3SiteB(config-isakmp)# exit
R3SiteB(config)#crypto isakmp key vpn123 address 10.0.12.1
R3SiteB(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
R3SiteB(cfg-crypto-trans)# mode tunnel
R3SiteB(cfg-crypto-trans)# exit
R3SiteB(config)#$ 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R3SiteB(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3SiteB(config-crypto-map)# set peer 10.0.12.1
R3SiteB(config-crypto-map)# set transform-set TSET
R3SiteB(config-crypto-map)# match address 100
R3SiteB(config-crypto-map)# exit
R3SiteB(config)#interface f0/0
R3SiteB(config-if)# crypto map CMAP
R3SiteB(config-if)# exit
R3SiteB(config)#end
R3SiteB#wr
*Dec 30 12:58:00.715: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3SiteB#wr
*Dec 30 12:58:00.735: %SYS-5-CONFIG_I: Configured from console by console
R3SiteB#wr
Building configuration...
[OK]
```

Figure 2.3: Cấu hình chi tiết Crypto Map và ACL trên Router R3

2.2.4 Kiểm tra và đánh giá kết quả

Kiểm tra kết nối (Ping Connectivity)

Sử dụng công cụ VPCS để thực hiện lệnh Ping từ PC1 (Site A) tới PC2 (Site B).

- Gói tin đầu tiên bị `timeout`: Do hệ thống mất thời gian phân giải ARP và thiết lập pha 1, pha 2 của IPSec.
- Các gói tin tiếp theo phản hồi thành công: Chứng tỏ đường hầm đã được dựng và hoạt động ổn định.

```
PC1> ping 192.168.2.2
192.168.2.2 icmp_seq=1 timeout
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=106.713 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=90.535 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=92.191 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=91.732 ms
```

Figure 2.4: Kết quả Ping thông suốt từ PC1 sang PC2

Kiểm tra tính bảo mật (Packet Analysis)

Sử dụng Wireshark bắt gói tin trên đường truyền vật lý giữa R1 và ISP. Kết quả cho thấy toàn bộ nội dung trao đổi (ICMP Echo Request/Reply) đều được đóng gói trong giao thức **ESP (IP Protocol 50)**. Kẻ tấn công trên đường truyền chỉ thấy các gói tin mã hóa, không thể đọc được nội dung thực tế.

14	30.055765	ca:01:61:b0:00:00	ca:01:61:b0:00:00	LOOP	60 Reply
15	30.697829	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
16	30.758830	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)
17	31.807357	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
18	31.867450	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)
19	32.920228	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
20	32.980522	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)
21	34.030403	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
22	34.090802	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)
23	35.142962	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
24	35.203826	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)
25	36.255578	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
26	36.316378	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)
27	37.366122	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
28	37.426367	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)
29	38.477231	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
30	38.537875	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)
31	39.589432	10.0.12.1	10.0.23.3	ESP	166 ESP (SPI=0x673d6d6f)
32	39.650188	10.0.23.3	10.0.12.1	ESP	166 ESP (SPI=0x9e17cbeb)

Figure 2.5: Wireshark xác nhận gói tin được mã hóa bằng giao thức ESP

2.3 Kịch bản 2: Triển khai VPN Client-to-Site

2.3.1 Mô tả kịch bản và Sơ đồ nguyên lý

Kịch bản này mô phỏng mô hình "Truy cập từ xa" (Remote Access VPN). Một nhân viên di động (R4) kết nối internet từ quán cafe hoặc nhà riêng, cần truy cập an toàn vào tài nguyên nội bộ của công ty (Server tại R1).

- **Thách thức:** Địa chỉ IP của nhân viên là địa chỉ động (Dynamic IP), Server không thể biết trước IP của Client để cấu hình tĩnh.
- **Giải pháp:** Sử dụng kỹ thuật **Dynamic Crypto Map** trên Server để chấp nhận kết nối từ bất kỳ nguồn nào, kết hợp với xác thực Pre-shared Key.

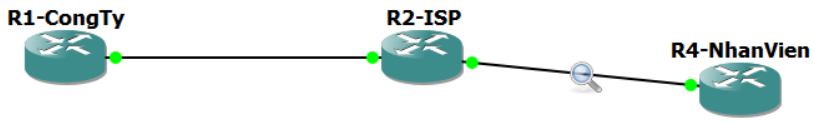

Figure 2.6: Sơ đồ mô phỏng kết nối VPN Client-to-Site

2.3.2 Thông số cấu hình kỹ thuật

Khác với mô hình Site-to-Site (cấu hình đối xứng), mô hình Client-to-Site có sự bất đối xứng trong cấu hình Crypto Map. Chi tiết được thể hiện ở Bảng 2.3.

Table 2.3: Bảng cấu hình VPN Client-to-Site (Dynamic vs Static)

Hạng mục	**Server (R1)**	**Client (R4)**
Map Type	**Dynamic Map**	**Static Map**
Peer IP Address	`0.0.0.0` (Chấp nhận tất cả)	`10.0.12.1` (IP của Server)
Authentication Key	`bietdoigiaiyeu`	`bietdoigiaiyeu`
Transform Set	`TSET` (esp-aes, sha-hmac)	`TSET` (esp-aes, sha-hmac)
ACL Traffic	Permit 192.168.1.0 → Any	Permit Host 10.0.24.4 → 192.168.1.0

2.3.3 Cấu hình thực nghiệm

Tại phía Client (R4), cấu hình trỏ cố định về Server. Hình ảnh dưới đây minh họa các bước tạo Policy, Key và Map trên R4.

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/60/76 ms
R4-NhanVien#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4-NhanVien(config)#
R4-NhanVien(config)#
R4-NhanVien(config)#crypto isakmp policy 10
R4-NhanVien(config-isakmp)# encr aes
R4-NhanVien(config-isakmp)# hash sha
R4-NhanVien(config-isakmp)# authentication pre-share
R4-NhanVien(config-isakmp)# group 2
R4-NhanVien(config-isakmp)#exit
R4-NhanVien(config)#
R4-NhanVien(config)#
R4-NhanVien(config)#crypto isakmp key bietdoigiaiyeu address 10.0.12.1
A pre-shared key for address mask 10.0.12.1 255.255.255.255 already exists!

R4-NhanVien(config)#
R4-NhanVien(config)#
R4-NhanVien(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
R4-NhanVien(cfg-crypto-trans)# mode tunnel
R4-NhanVien(cfg-crypto-trans)#exit
R4-NhanVien(config)#
R4-NhanVien(config)#! (Tu IP cua R4 den mang noi bo Cong ty)
```

Figure 2.7: Cấu hình Static Crypto Map trên thiết bị Client (R4)

2.3.4 Kiểm tra và đánh giá kết quả

Để chứng minh giải pháp hoạt động hiệu quả, quá trình kiểm tra được thực hiện qua 3 bước: Kiểm tra kết nối, Kiểm tra trạng thái đường hầm và Kiểm tra gói tin.

Bước 1: Kiểm tra kết nối mạng (Ping)

Từ Router R4 (Client), thực hiện lệnh Ping tới địa chỉ Loopback 0 (192.168.1.1) đại diện cho Server nội bộ. Kết quả trả về `!!!!!` (Success rate 100%) xác nhận kết nối IP đã thông suốt qua đường hầm.

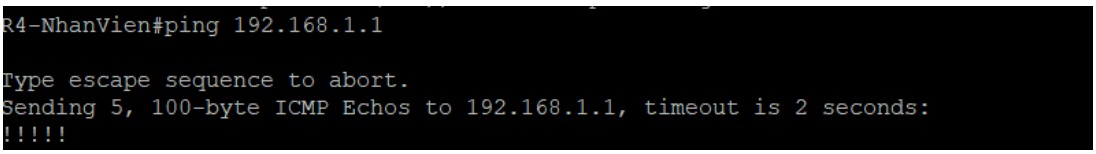

Figure 2.8: Client R4 truy cập thành công vào Server nội bộ

Bước 2: Kiểm tra trạng thái đường hầm (Tunnel Status)

Trên Server R1, các lệnh kiểm tra cho thấy hệ thống đã nhận diện chính xác kết nối từ IP động 10.0.24.4.

- **ISAKMP SA:** Trạng thái **QM_IDLE** cho thấy quá trình thỏa thuận khóa Phase 1 đã hoàn tất.

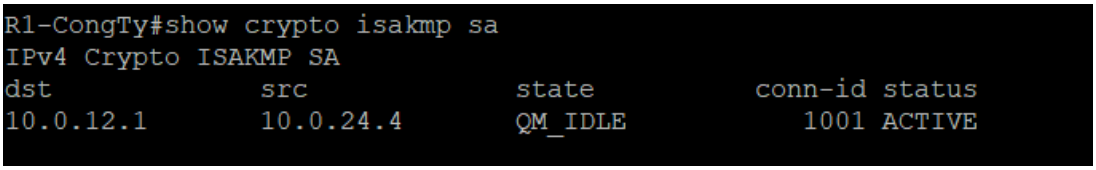

Figure 2.9: Trạng thái ISAKMP SA trên Server (Active)

- **IPSec SA:** Thống kê cho thấy số lượng gói tin mã hóa và giải mã tăng lên tương ứng (*#pkts encaps: 9, #pkts encrypt: 9*). Đây là bằng chứng rõ ràng nhất cho việc dữ liệu đang được bảo vệ.

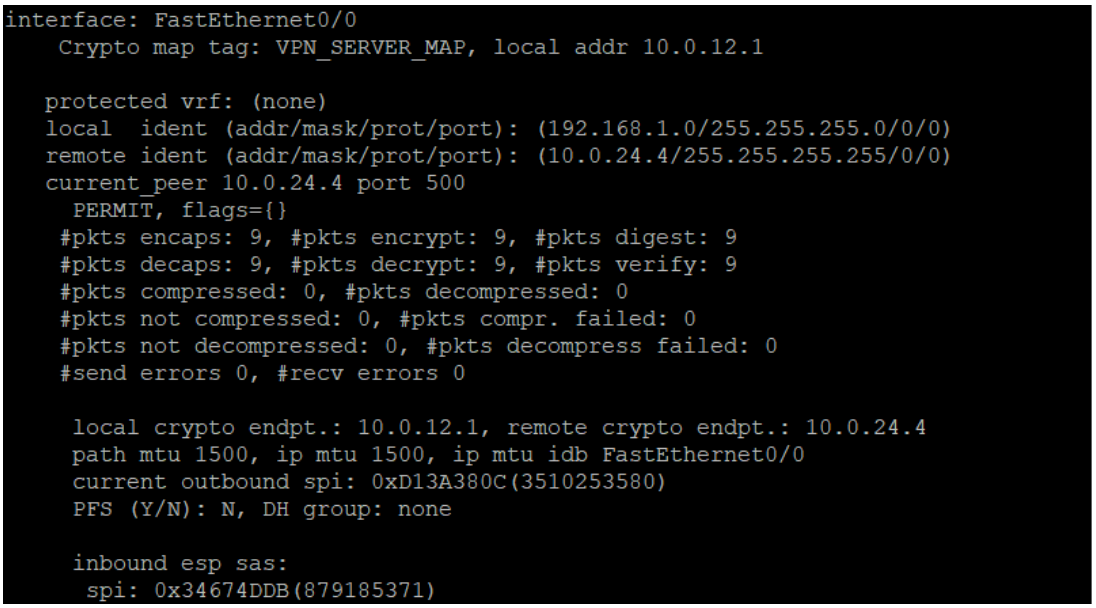

Figure 2.10: Thống kê IPSec SA xác nhận 9 gói tin đã được mã hóa/giải mã

Bước 3: Phân tích gói tin (Wireshark)

Bắt gói tin trên cổng kết nối của Client. Toàn bộ lưu lượng Ping ICMP giờ đây đã chuyển thành giao thức **ESP**. Điều này đảm bảo rằng ngay cả khi truy cập từ Wifi công cộng (như quán cafe), dữ liệu của nhân viên vẫn được bảo mật tuyệt đối.

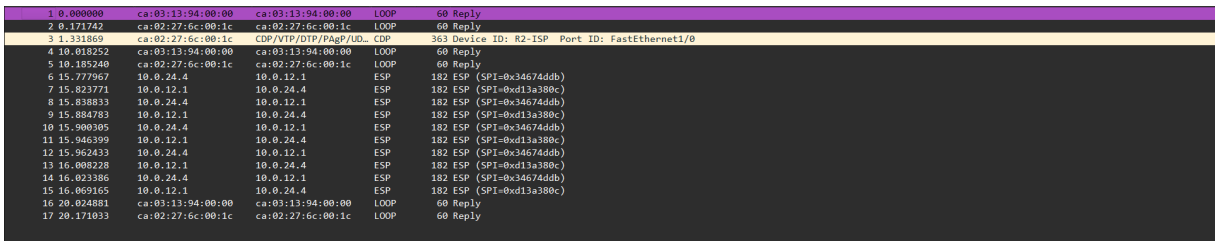

Figure 2.11: Wireshark hiển thị giao thức ESP bảo vệ dữ liệu người dùng

2.4 Tiểu kết chương 2

Trong Chương 2, đề tài đã trình bày chi tiết quá trình triển khai và cấu hình hệ thống VPN IPSec trên môi trường giả lập GNS3 nhằm kiểm chứng tính đúng đắn và hiệu quả của các kiến thức lý thuyết đã trình bày ở Chương 1. Trước hết, chương đã mô tả môi trường thực nghiệm, công cụ sử dụng và sơ đồ quy hoạch địa chỉ IP, đảm bảo hệ thống mạng được thiết kế rõ ràng, logic và phù hợp với các kịch bản triển khai VPN.

Tiếp theo, đề tài đã xây dựng và triển khai thành công kịch bản VPN Site-to-Site, mô phỏng kết nối an toàn giữa hai mạng LAN tại Trụ sở chính và Chi nhánh. Quá trình cấu hình IPSec được thực hiện đồng bộ trên các thiết bị Gateway với đầy đủ các tham số của IKE Phase 1 và IPSec Phase 2. Kết quả kiểm tra bằng công cụ Ping và phân tích gói tin bằng Wireshark cho thấy dữ liệu trao đổi giữa hai mạng được mã hóa hoàn toàn dưới dạng ESP, đảm bảo tính bảo mật, toàn vẹn và xác thực nguồn dữ liệu.

Bên cạnh đó, kịch bản VPN Client-to-Site cũng được triển khai nhằm mô phỏng nhu cầu truy cập từ xa của người dùng di động với địa chỉ IP động. Việc sử dụng Dynamic Crypto Map trên phía Server kết hợp với Static Crypto Map phía Client đã cho phép thiết lập đường hầm IPSec linh hoạt và an toàn. Các kết quả kiểm tra trạng thái SA, thống kê gói tin mã hóa/giải mã và phân tích lưu lượng mạng đều khẳng định hệ thống VPN hoạt động ổn định và đúng theo thiết kế.

Nhìn chung, các kết quả thực nghiệm trong Chương 2 đã chứng minh tính khả thi của giải pháp VPN IPSec khi triển khai trên nền tảng GNS3, đồng thời làm cơ sở quan trọng cho việc đánh giá, mở rộng và ứng dụng mô hình trong các hệ thống mạng doanh nghiệp thực tế ở các chương tiếp theo.

CHƯƠNG 3 KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

3.1 Kết luận chung

Sau quá trình nghiên cứu lý thuyết và triển khai thực nghiệm trên phần mềm mô phỏng GNS3, đồ án đã hoàn thành các mục tiêu đề ra ban đầu. Các kết quả đạt được cụ thể như sau:

- **Về mặt lý thuyết:** Đã tìm hiểu và phân tích sâu về giao thức IPSec, kiến trúc bảo mật mạng VPN, các thuật toán mã hóa (AES), hàm băm (SHA) và quy trình trao đổi khóa IKE (Phase 1 và Phase 2).
- **Về mặt thực nghiệm:**
  - Xây dựng thành công mô hình mạng giả lập gồm Trụ sở chính, Chi nhánh và Người dùng di động trên nền tảng Cisco IOS.
  - Cấu hình thành công VPN Site-to-Site kết nối hai mạng LAN, đảm bảo tính toàn vẹn và bí mật dữ liệu.
  - Triển khai thành công VPN Client-to-Site (Remote Access) sử dụng kỹ thuật Dynamic Map, cho phép nhân viên truy cập tài nguyên nội bộ từ môi trường Internet.
- **Về kiểm thử:** Kết quả kiểm tra bằng lệnh Ping và phân tích gói tin Wireshark đã chứng minh dữ liệu được đóng gói và mã hóa bằng giao thức ESP, ngăn chặn hoàn toàn việc nghe lén trên đường truyền.

3.2 Hạn chế của đề tài

Mặc dù đã đạt được những kết quả khả quan, đồ án vẫn còn tồn tại một số hạn chế nhất định do giới hạn về thời gian và thiết bị:

- **Môi trường giả lập:** Việc thực hiện trên GNS3 tuy mô phỏng chính xác logic hoạt động nhưng chưa đánh giá được hiệu năng thực tế (Throughput, Latency) khi chịu tải lượng truy cập lớn như trên thiết bị phần cứng chuyên dụng.
- **Phương thức xác thực:** Đồ án mới chỉ dừng lại ở phương thức xác thực *Pre-shared Key* (Khóa chia sẻ trước). Phương thức này đơn giản, dễ cấu hình nhưng khó quản lý và bảo mật kém hơn so với chứng thực số (Digital Certificates/PKI) khi quy mô mạng mở rộng.
- **Tính sẵn sàng cao:** Mô hình chưa triển khai các giải pháp dự phòng (Redundancy) cho VPN Gateway. Nếu Router biên gặp sự cố, kết nối VPN sẽ bị gián đoạn hoàn toàn.

3.3 Hướng phát triển

Dựa trên những hạn chế đã nêu, hướng phát triển mở rộng của đề tài trong tương lai bao gồm:

- **Nâng cao bảo mật:** Triển khai hệ thống CA (Certificate Authority) để sử dụng chứng thực số (Digital Certificates - RSA Signatures) thay cho Pre-shared Key.
- **Tích hợp Firewall:** Kết hợp VPN trên thiết bị tường lửa chuyên dụng (như Cisco ASA hoặc Firepower) để kiểm soát sâu hơn các luồng dữ liệu đi qua đường hầm.
- **Mở rộng quy mô:** Nghiên cứu giải pháp DMVPN (Dynamic Multipoint VPN) để giải quyết bài toán kết nối đa điểm (Full-mesh) một cách tự động khi số lượng chi nhánh tăng lên.
- **Quản lý người dùng tập trung:** Tích hợp với RADIUS hoặc TACACS+ Server để quản lý tài khoản và phân quyền truy cập VPN cho từng nhân viên cụ thể.

BIBLIOGRAPHY

[1] Nguyễn Thúc Hải, *Mạng máy tính và các hệ thống mở*, Nhà xuất bản Giáo dục, 2019.

[2] Quốc hội Việt Nam, *Luật An toàn thông tin mạng*, 2015.

[3] William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson, 2017.

[4] Yusuf Bhaiji, *Network Security Technologies and Solutions (CCIE Professional Development)*, Cisco Press, 2008.

[5] Andrew S. Tanenbaum, David J. Wetherall, *Computer Networks*, 5th Edition, Pearson, 2011.

[6] Douglas E. Comer, *Internetworking with TCP/IP, Volume 1*, 6th Edition, Pearson, 2014.

[7] S. Kent, R. Atkinson, *RFC 2401 – Security Architecture for the Internet Protocol*, IETF, 1998.

[8] S. Kent, R. Atkinson, *RFC 2402 – IP Authentication Header (AH)*, IETF, 1998.

[9] S. Kent, R. Atkinson, *RFC 2406 – IP Encapsulating Security Payload (ESP)*, IETF, 1998.

[10] D. Harkins, D. Carrel, *RFC 2409 – Internet Key Exchange (IKE)*, IETF, 1998.

[11] S. Kent, *RFC 4301 – Security Architecture for the Internet Protocol*, IETF, 2005.

[12] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, *RFC 7296 – Internet Key Exchange Protocol Version 2 (IKEv2)*, IETF, 2014.

[13] Cisco Systems, *Security for VPNs with IPsec Configuration Guide, Cisco IOS Release 15M&T*, 2023.

[14] Cisco Systems, *IPSec VPN Design Guide*, Cisco Press, 2022.

[15] NIST, *Guide to IPsec VPNs (SP 800-77)*, National Institute of Standards and Technology, 2021.

[16] GNS3 Technologies Inc., *GNS3 Documentation – Architecture and VM Deployment*, `https://docs.gns3.com/`.