TRƯỜNG ĐẠI HỌC SÀI GÒN

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO HỌC PHẦN HỆ THỐNG ẢO VÀ KHẢ NĂNG MỞ RỘNG DỮ LIỆU

ĐỀ TÀI

XÂY DỰNG MÔ HÌNH MẠNG VỚI PHẦN MỀM GNS3, CẤU HÌNH VPN SITE TO SITE VỚI GRE VÀ IPSEC

Giảng viên hướng dẫn: Lương Minh Huấn

Nhóm sinh viên thực hiện:

Hồ Hữu Đại	3122410066
Huỳnh Tấn Dương	3122410061
Tô Khổng Mỹ Hằng	3122410104
Ngô Thị Minh Thi	3122410396

TP. HỒ CHÍ MINH, THÁNG 11 NĂM 2024

THÀNH VIÊN NHÓM		
Tên	**MSSV**	**Email**
Hồ Hữu Đại	3122410066	hohuudai103@gmail.com
Huỳnh Tấn Dương	3122410061	dhuynh529@gmail.com
Ngô Thị Minh Thi	3122410396	ntmthi.0234@gmail.com
Tô Khổng Mỹ Hằng	3122410104	myhang03112004@gmail.com

LỜI CẢM ƠN

Trong quá trình thực hiện đồ án này, nhóm chúng tôi xin gửi lời cảm ơn chân thành đến thầy Lương Minh Huấn – giảng viên bộ môn "Hệ thống ảo và khả năng mở rộng dữ liệu" thuộc Khoa Công Nghệ Thông Tin, trường Đại học Sài Gòn, đã tận tình hướng dẫn và hỗ trợ chúng tôi trong suốt quá trình nghiên cứu và phát triển đồ án. Chúng tôi cũng xin cảm ơn sự đóng góp của các thành viên trong nhóm. Sự cống hiến và chia sẻ ý tưởng từ các bạn đã giúp nhóm vượt qua những thử thách và hoàn thành đồ án một cách thành công. Cuối cùng, xin cảm ơn những người sẽ đọc và đánh giá đồ án này. Sự quan tâm của mọi người là động lực để chúng tôi hoàn thành dự án với sự nỗ lực cao nhất.

Trong quá trình hoàn thành đồ án, chúng tôi cũng đối mặt với nhiều khó khăn và thách thức, nhưng qua thời gian học tập và nghiên cứu chúng tôi cũng khắc phục được nhiều yếu điểm. Sự thiếu kinh nghiệm thực tế và kiến thức đã khiến cho chúng tôi gặp phải những sai sót và hạn chế. Chúng tôi xin trân trọng mọi sự góp ý và nhận xét từ các thầy cô để chúng tôi có thể học hỏi và phát triển kiến thức của mình, áp dụng chúng vào thực tế một cách hiệu quả trong tương lai.

Chúng tôi xin chân thành cảm ơn!

GIỚI THIỆU

Trong bối cảnh toàn cầu hóa và sự phát triển mạnh mẽ của công nghệ thông tin, nhu cầu kết nối các mạng riêng lẻ tại các địa điểm khác nhau ngày càng tăng. VPN Site-to-Site là một giải pháp hiệu quả để đáp ứng nhu cầu này, cho phép các tổ chức xây dựng một mạng riêng ảo an toàn và đáng tin cậy.

Đồ án giúp các doanh nghiệp và cá nhân xây dựng kết nối VPN site-to-site bảo mật dữ liệu khi truyền qua Internet hoặc giữa các chi nhánh, các văn phòng từ xa. Giải pháp này không chỉ tối ưu chi phí kết nối mà còn tăng cường hiệu quả làm việc, bảo vệ thông tin quan trọng và giảm thiểu rủi ro an ninh mạng. Đặc biệt, nó phù hợp cho các tổ chức có nhu cầu kết nối mạng từ xa một cách an toàn và đáng tin cậy.

Mục tiêu của đồ án:

- Tìm hiểu và nắm vững khái niệm, vai trò của VPN, GRE và IPSec.
- Thiết lập kết nối bảo mật giữa các chi nhánh, đảm bảo truyền dữ liệu an toàn giữa hai site từ xa thông qua GRE và IPSec.
- Triển khai và cấu hình VPN, kiểm tra tính khả dụng và bảo mật của kết nối.

Đối tượng nghiên cứu: VPN site-to-site, GRE, IPSec với công cụ mô phỏng GNS3, VMWare Workstation.

Phạm vi nghiên cứu: Đề tài tập trung vào việc triển khai và cấu hình VPN site-to-site (GRE và IPSec) trên phần mềm mô phỏng GNS3 theo hai topology khác nhau:

- Sử dụng 1 PC.
- Sử dụng 2 PC kết nối qua dây mạng vật lý.

Để hiểu rõ hơn về những nội dung trên, báo cáo của chúng tôi sẽ được tổ chức thành các phần sau:

- Chương I : Khái niệm tổng quát.
- Chương II : Ứng dụng.
- Chương III : Cách thức hoạt động.
- Chương IV : Thực hiện cấu hình VPN GRE IPSEC.
- Chương V : Kiểm tra kết quả.

Mục lục

DANH SÁCH HÌNH ẢNH

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Từ đầy đủ	Ý nghĩa
ERP	Enterprise Resource Planning	Hệ thống phần mềm quản lý và tích hợp các quy trình nội bộ của doanh nghiệp.
CRM	Customer Relationship Management	Hệ thống phần mềm quản lý mối quan hệ và thông tin khách hàng.
VPN	Virtual Private Network	Mạng riêng ảo
WAN	Wide Area Network	Mạng diện rộng
PBX	Private Branch Exchange	Các tổng đài thuê bao
GRE	Generic Routing Encapsulation	Phương thức đóng gói dữ liệu của gói tin
IP	Internet Protocol	Giao thức dùng để xác định nguồn/đích phục vụ truyền tải dữ liệu
IPSec	Internet Protocol Security	Giao thức được sử dụng để bảo mật dữ liệu khi truyền tải qua mạng internet
IETF	Internet Engineering Task Force	Một tổ chức tiêu chuẩn mở, phát triển và thúc đẩy các tiêu chuẩn Internet tự nguyện, đặc biệt là các tiêu chuẩn bao gồm bộ giao thức Internet (TCP/IP)
Hop	Hopping	Số lần gói dữ liệu đi qua các thiết bị mạng.
OSPF	Open Shortest Path First	Giao thức định tuyến động trong mạng
Ipv4, Ipv6	Internet Protocol version 4, Internet Protocol version 6	Giao thức Internet sử dụng địa chỉ 32-bit, Giao thức Internet sử dụng địa chỉ 128-bit

CHƯƠNG I : KHÁI NIỆM TỔNG QUÁT

1. Khái niệm VPN, VPN site to site

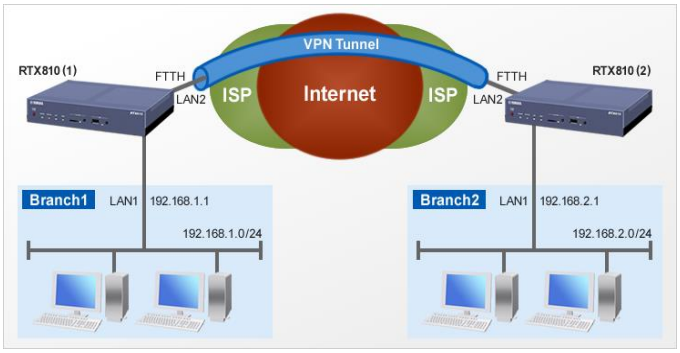
Mạng VPN xuất hiện từ khá sớm (đầu thập niên 1970).

Sự xuất hiện của VPN bắt nguồn từ yêu cầu của khách hàng, mong muốn có thể kết nối một cách có hiệu quả với các tổng đài thuê bao (PBX) lại với nhau thông qua mạng WAN.

VPN là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu.

Hình 1. Đường hầm VPN

VPN Site to Site là một mô hình kết nối VPN dùng để liên kết hai hay nhiều mạng riêng tư thông qua liên kết mã bảo mật và an toàn. Thay vì yêu cầu mỗi người dùng kết nối riêng lẻ như VPN Client to Site, VPN Site to Site tạo ra một đường truyền đã được mã hóa dữ liệu và bảo mật mạng.



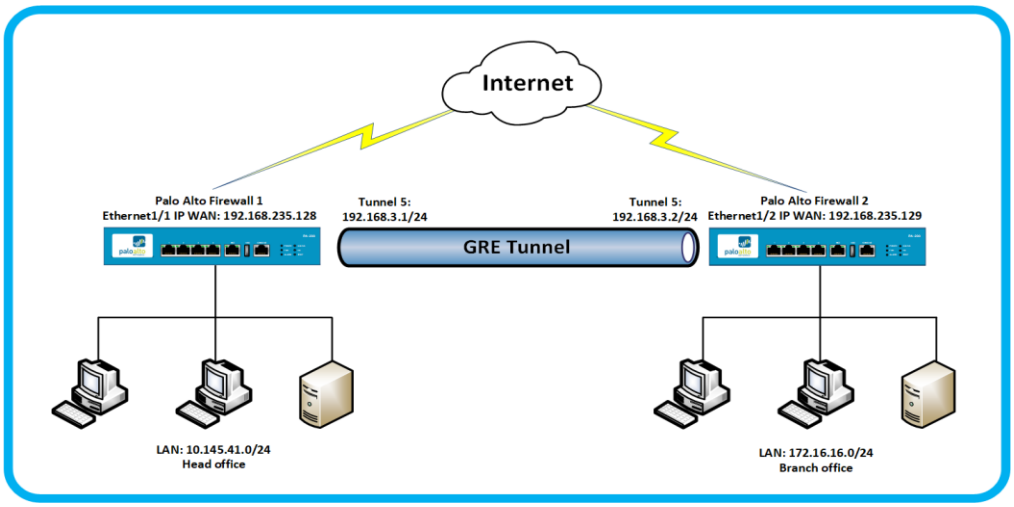
Hình 2. Đường hầm VPN

2. Khái niệm GRE

GRE (Generic Routing Encapsulation) là một giao thức để đóng gói các gói dữ liệu sử dụng một giao thức định tuyến bên trong các gói của một giao thức khác.

GRE Tunnel là giao thức đóng gói do Cisco tạo ra. Đây là giao thức cho phép một bộ định tuyến gửi gói tin đến một bộ định tuyến khác.

GRE Tunnel kết nối hai mạng với nhau cho phép dữ liệu được truyền giữa hai mạng như thể chúng được kết nối trực tiếp. GRE Tunnel hoạt động như một đường hầm giữa hai mạng qua Internet.



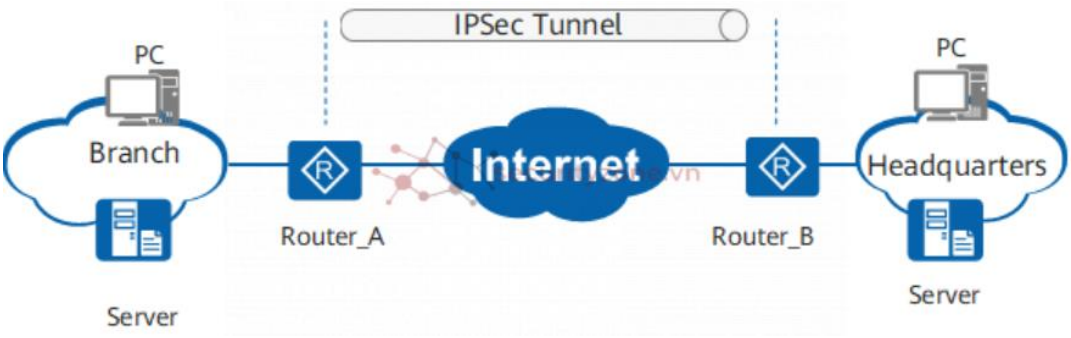
Hình 3. Đường hầm VPN GRE

3. Khái niệm IPSEC

IPSec là hệ thống các quy tắc hoặc giao thức truyền thông dùng để thiết lập kết nối an toàn qua một mạng.

IPSec được IETF phát triển vào những năm 1990 để đảm bảo tính bảo mật, tính toàn vẹn và tính xác thực của dữ liệu khi truy cập các mạng công cộng. IPSec bổ sung khả năng mã hóa và xác thực để tăng cường bảo mật giao thức.

Ví dụ: IPSec mã hóa dữ liệu tại nguồn và giải mã dữ liệu đã được mã hóa tại đích của giao thức này.



Hình 4. Cấu hình VPN sử dụng giao thức IPSEC

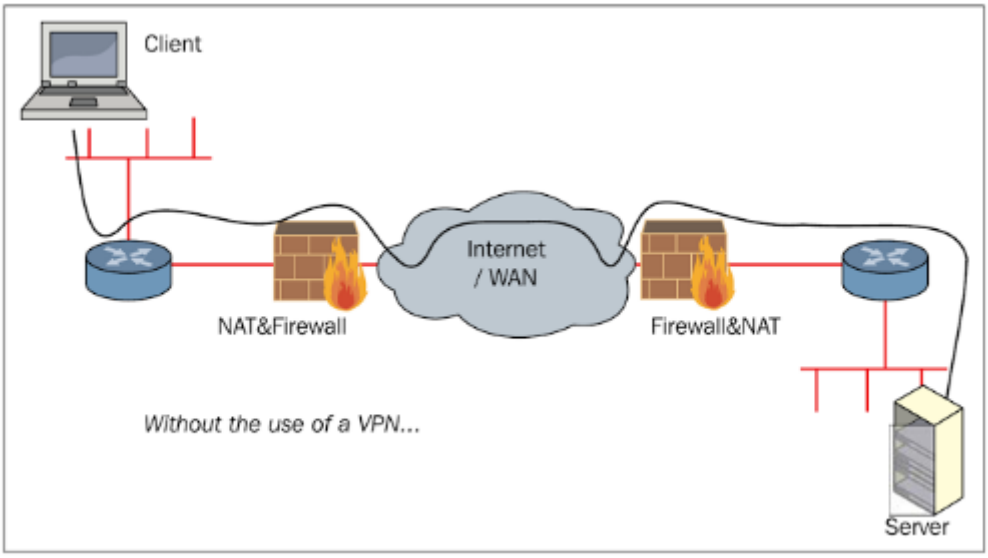
CHƯƠNG II: ỨNG DỤNG

1. VPN

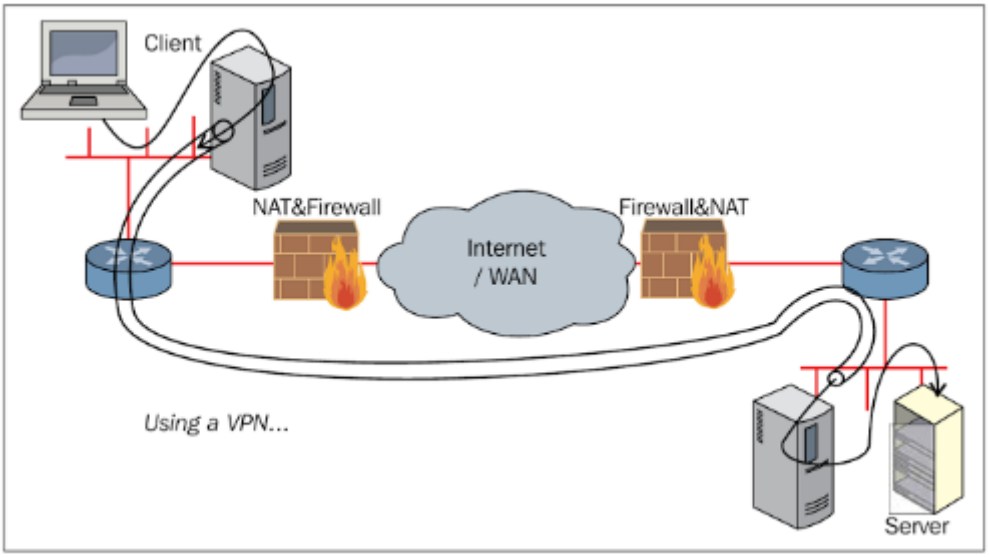
Với cơ chế hoạt động như trên, những ứng dụng mà VPN có thể mang lại gồm:

- Bảo mật gần như tuyệt đối khi kết nối Wifi công cộng.
- Bảo mật dữ liệu khỏi những ứng dụng và dịch vụ khả nghi.
- Bảo vệ dữ liệu mật của người dùng khỏi sự can thiệp của nhà cung cấp mạng.
- Truy cập trang web mọi lúc mọi nơi, không bị rào cản quốc gia.
- Download ẩn danh.

Hình 5. Lý do chính khiến người dùng lựa chọn sử dụng VPN



Hình 6. Kết nối mạng không an toàn khi không sử dụng VPN



Hình 7. Kết nối mạng khi sử dụng VPN

1.1. Ưu điểm:

- Tiết kiệm chi phí: Sử dụng hạ tầng Internet, giúp giảm chi phí.
- Linh hoạt: Hỗ trợ kết nối băng thông rộng như DSL, cáp; giúp truy cập từ xa hiệu quả.
- Bảo mật: Dùng mã hóa và giao thức bảo mật, ẩn IP nội bộ, chỉ hiển thị IP công khai.
- An toàn công cộng: Bảo vệ dữ liệu cá nhân khi truy cập mạng công cộng.

- Truy cập không giới hạn: Vượt tường lửa, truy cập các trang bị chặn và duy trì ẩn danh.

1.2. Hạn chế:

- Làm chậm mạng: Mã hóa, giải mã làm giảm tốc độ, đặc biệt khi mạng yếu.
- Tương thích thiết bị kém: Một số thiết bị không hỗ trợ VPN.
- Chi phí dịch vụ: VPN trả phí đắt đỏ cho doanh nghiệp.
- Quyền riêng tư phụ thuộc nhà cung cấp: VPN công cộng có nguy cơ lộ thông tin.
- Sự cố kết nối: Kết nối có thể gián đoạn, ảnh hưởng trải nghiệm.
- Cấu hình phức tạp: Đòi hỏi kỹ thuật cao; sai cấu hình giảm bảo mật.
- Giới hạn truy cập nội dung địa phương: Khó truy cập nội dung giới hạn vị trí.
- Tiêu hao pin di động cao: VPN liên tục chạy làm hao pin.
- Giảm hiệu suất mạng: Khi nhiều người dùng hoặc thiết bị xử lý kém.
- Không bảo vệ toàn diện: Không ngăn được phần mềm độc hại.
- Bị chặn bởi một số dịch vụ: Như Netflix có thể chặn IP VPN.

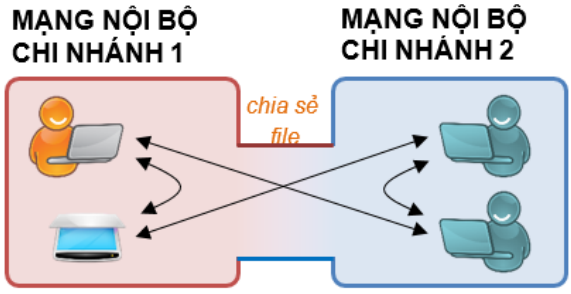
Hình 8. Nhược điểm của việc sử dụng VPN

2. VPN site to site

Những ứng dụng trong thực tiễn của VPN site to site được thể hiện thông nhiều mặt như sau:

- Kết nối chi nhánh và trụ sở chính: Site-to-site VPN được sử dụng để kết nối các văn phòng chi nhánh đến trụ sở chính của công ty, giúp các chi nhánh truy cập vào hệ thống mạng nội bộ trung tâm. Điều này giúp cải thiện khả năng cộng tác và trao đổi dữ liệu.
- Tối ưu hóa bảo mật dữ liệu: VPN site-to-site mã hóa dữ liệu truyền tải giữa hai mạng, giảm nguy cơ rò rỉ thông tin nhạy cảm khi dữ liệu được truyền qua mạng Internet. Điều này đóng vai trò quan trọng cho các tổ chức tài chính, ngân hàng, và công ty luật.
- Kết nối giữa các Data Center: Trong các tổ chức có nhiều Data Center ở các địa điểm khác nhau, VPN site-to-site giúp liên kết các trung tâm này, đảm bảo việc sao lưu và phục hồi dữ liệu nhanh chóng, an toàn.
- Hỗ trợ cho các ứng dụng nội bộ: VPN site-to-site cho phép các ứng dụng và dịch vụ nội bộ như hệ thống quản lý tài chính, ERP, CRM có thể được truy cập từ xa, giúp nhân viên dễ dàng làm việc và truy cập các tài nguyên từ các chi nhánh.
- Kết nối đối tác và khách hàng: Nhiều tổ chức sử dụng site-to-site VPN để liên kết mạng của họ với mạng của các đối tác chiến lược hoặc khách hàng quan trọng, giúp việc trao đổi dữ liệu an toàn và nhanh chóng hơn.
- Cải thiện hiệu quả làm việc từ xa: VPN site-to-site tạo ra một "mạng lưới riêng ảo" chung giữa các địa điểm, giúp người dùng truy cập vào mạng nội bộ từ xa mà không cần thiết lập kết nối VPN cá nhân, phù hợp cho các doanh nghiệp có nhiều người làm việc từ xa.

Ví dụ: VPN site-to-site có thể được sử dụng khi muốn kết nối 2 văn phòng của cùng một công ty. Lúc này, mọi nhân viên, thiết bị ở cả 2 văn phòng có thể trao đổi mọi thông tin với nhau thông qua kết nối VPN



Hình 9. Mạng nội bộ liên kết giữa 2 chi nhánh của 1 công ty

2.1. Ưu điểm:

- Kết nối an toàn: VPN site-to-site cho phép các văn phòng từ xa kết nối qua Internet công cộng với mã hóa bảo mật cao, ngăn chặn truy cập trái phép.
- Giảm chi phí: Giải pháp này tiết kiệm chi phí hơn so với các đường truyền riêng, sử dụng Internet thay vì đầu tư hạ tầng vật lý.
- Dễ mở rộng: Dễ dàng kết nối thêm chi nhánh vào mạng VPN mà không cần thay đổi cấu trúc hiện tại, tăng tính linh hoạt.
- Bảo mật cao: Sử dụng các giao thức như IPsec để mã hóa và xác thực, bảo vệ dữ liệu trên Internet.
- Quản lý hiệu quả: Tạo mạng chung cho các chi nhánh, giúp IT dễ giám sát và kiểm soát truy cập.
- Tăng năng suất: Kết nối ổn định giúp nhân viên chia sẻ dữ liệu và làm việc hiệu quả.
- Hỗ trợ ứng dụng thời gian thực: Đảm bảo băng thông ổn định cho VoIP, hội nghị truyền hình.
- Giảm rủi ro bảo mật: Kết nối các văn phòng qua Internet mà không lo các rủi ro từ mạng công cộng.

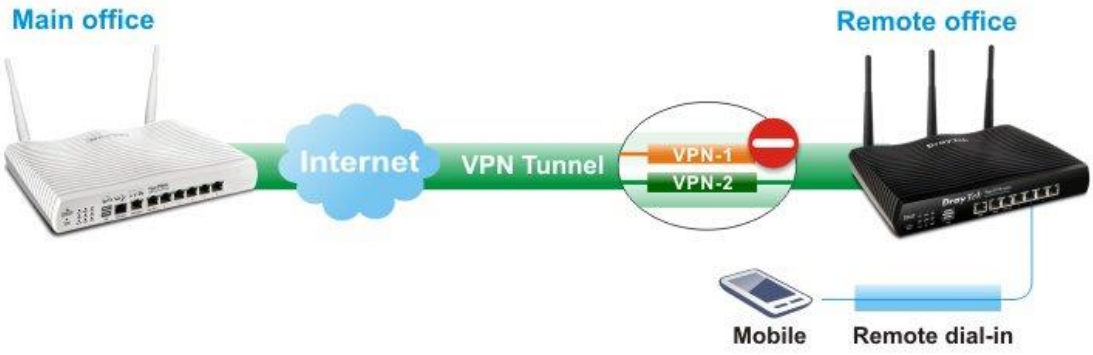
2.2. Hạn chế:

- Khả năng mở rộng hạn chế: VPN cần kết nối riêng cho mỗi cặp site, số lượng kết nối tăng nhanh khi số site tăng.
- Định tuyến không hiệu quả: Mô hình “trung tâm và nan hoa” giảm số đường hầm nhưng tăng độ trễ và tải cho trụ sở chính.
- Hiển thị phân mảnh: Mỗi kết nối VPN là độc lập, gây khó khăn cho việc giám sát toàn bộ mạng và phát hiện tấn công phân tán.
- Quản lý phức tạp: Mỗi đường hầm VPN phải được cấu hình và giám sát riêng, phức tạp cho quản lý.
- Thiếu bảo mật tích hợp: VPN chỉ mã hóa kết nối mà không kiểm tra bảo mật nội dung, cho phép quyền truy cập không hạn chế.

3. GRE Tunnel

Những tính GRE Tunnel mang lại bao gồm:

- Hỗ trợ nhiều giao thức: GRE đóng gói các giao thức không phải IP để truyền qua mạng IP, giúp truyền dữ liệu như IPX hoặc AppleTalk trên mạng IP.
- Kết hợp với VPN: Khi kết hợp với IPsec, GRE tạo VPN site-to-site an toàn, hỗ trợ đa giao thức qua IP và mã hóa dữ liệu với IPsec.
- Kết nối đa điểm: GRE hỗ trợ định tuyến qua nhiều hop, phù hợp cho các hệ thống mạng lớn và phức tạp.
- Hỗ trợ định tuyến động: GRE tunnel giúp triển khai OSPF, EIGRP, BGP qua VPN, đảm bảo tự động định tuyến hiệu quả.
- Kết nối nhiều chi nhánh: GRE kết nối các chi nhánh trong mạng riêng mà không cần nhiều VPN riêng lẻ.
- Hỗ trợ VoIP và video: GRE giúp truyền ổn định VoIP và video, phù hợp cho hội nghị và liên lạc doanh nghiệp.



Hình 10. Hệ thống mạng kết nối 2 văn phòng sử dụng giao thức GRE thông qua đường hầmVPN

3.1. Ưu điểm:

- Hỗ trợ đa giao thức: GRE đóng gói các giao thức như IPv4, IPv6, IPX, và AppleTalk, cho phép truyền tải đa dạng dữ liệu trên cùng kết nối.
- Kết hợp bảo mật: Kết hợp với IPsec để mã hóa và xác thực, đảm bảo an toàn dữ liệu.
- Thiết lập dễ dàng: Cấu hình GRE đơn giản, tiết kiệm thời gian và không yêu cầu phần cứng phức tạp.
- Kết nối mạng ảo: Tạo mạng ảo giữa các điểm qua Internet, phù hợp cho VPN site-to-site hoặc kết nối chi nhánh.

- Hỗ trợ mạng phức tạp: GRE cho phép tạo nhiều tunnel để thiết lập kiến trúc mạng như mesh hoặc đa điểm.
- Tương thích định tuyến động: Hỗ trợ OSPF và BGP, giúp cập nhật đường đi tự động.
- Hỗ trợ multicast/broadcast: GRE hỗ trợ truyền multicast và broadcast, phù hợp cho hội nghị truyền hình và phát sóng nhóm.
- Bảo toàn gói tin gốc: GRE đóng gói mà không thay đổi nội dung, đảm bảo tính toàn vẹn dữ liệu.

3.2. Hạn chế:

- Thiếu bảo mật: GRE không mã hóa hoặc xác thực, dễ lộ dữ liệu nếu không kết hợp IPsec.
- Tăng độ trễ, giảm hiệu suất: Đóng gói/giải nén gói tin gây chậm trễ, nhất là với gói lớn hoặc nhiều tunnel.
- Hạn chế băng thông: GRE thiếu cơ chế quản lý băng thông, dễ gây tắc nghẽn nếu không kiểm soát.
- Giới hạn giao thức: Chỉ hỗ trợ tốt cho một số giao thức và gói tin dưới 1476 byte.
- Thiếu QoS: Không hỗ trợ ưu tiên lưu lượng, khó đáp ứng ứng dụng quan trọng như VoIP.
- Cấu hình phức tạp: Khi tích hợp với IPsec, yêu cầu cấu hình phức tạp hơn.
- Tăng tài nguyên hệ thống: Đóng gói GRE tốn thêm tài nguyên, ảnh hưởng thiết bị yếu.
- Quản lý khó khăn: Giám sát và phân tích lưu lượng qua GRE phức tạp hơn các kết nối khác.

4. IPSec

4.1. Tính năng bảo mật của IPsec

– Bảo mật cho bộ định tuyến khi gửi dữ liệu qua Public Network: IPsec bảo vệ các gói tin được gửi qua kết nối Internet bằng các phường pháp xác thực kết nối, mã hóa gói tin, xác thực tính toàn vẹn,... nhằm bảo an toàn cho dữ liệu truyền qua mạng.
– Mã hóa dữ liệu ứng dụng: IPSec mã hóa dữ liệu ở mức IP, giúp bảo vệ các ứng

dụng quan trọng như email, truyền file, và các giao dịch tài chính.

- Xác thực dữ liệu nhanh chóng: IPSec đảm bảo dữ liệu chỉ được chấp nhận từ người gửi đã xác thực nhờ vào các thỏa thuận về thông số bảo mật được trao đổi, giúp ngăn ngừa việc giả mạo nguồn gốc dữ liệu, bảo vệ dữ liệu qua Tunnel.
- Hỗ trợ kết nối VPN: IPSec được sử dụng trong VPN để tạo kết nối bảo mật giữa các chi nhánh, văn phòng, hoặc người dùng từ xa với mạng công ty.
- Đảm bảo an toàn cho các giao thức định tuyến động: IPSec bảo vệ các giao thức định tuyến như OSPF, EIGRP và BGP, ngăn chặn việc giả mạo và tấn công vào hệ thống định tuyến.
- Bảo mật cho hệ thống IoT: IPec giúp mã hóa dữ liệu truyền từ các thiết bị IoT, bảo vệ thông tin trong các hệ thống tự động hóa hoặc giám sát an ninh.
- Ngăn chặn tấn công nghe lén và giả mạo IP: IPSec bảo vệ dữ liệu chống lại các cuộc tấn công như packet sniffing, IP spoofing,... giúp đảm bảo dữ liệu không bị xâm phạm hoặc thay đổi.
- Bảo mật liên lạc VoIP: IPSec bảo vệ các cuộc gọi VoIP và hội nghị truyền hình, đảm bảo tính bảo mật và riêng tư cho thông tin liên lạc.

4.2. Mã hóa IPSEC

Mã hóa IPSec là một tập hợp các giao thức và tiêu chuẩn bảo mật hoạt động ở tầng mạng làm nhiễu dữ liệu bằng cách chuyển đổi từ Plaintext sang Ciphertext để bảo vệ nội dung của nó khỏi các bên chưa được cho phép.

Dữ liệu được mã hóa bằng khóa mã hóa và cần có khóa giải mã để giải nhiễu thông tin.

IPSec hỗ trợ nhiều loại mã hóa khác nhau, bao gồm AES, Blowfish, Triple DES, ChaCha và DES-CBC.

IPSec sử dụng mã hóa không đối xứng và đối xứng để đảm bảo tốc độ và bảo mật trong quá trình truyền dữ liệu.

Đối với mã hóa không đối xứng, khóa mã hóa được đặt ở chế độ

công khai trong khi khóa giải mã được giữ bí mật.

Mã hóa đối xứng sử dụng cùng một khóa công khai để mã hóa và giải mã dữ liệu.

IPSec thiết lập kết nối bảo mật với mã hóa bất đối xứng và chuyểnsang mã hóa đối xứng để tăng tốc độ truyền dữ liệu.

4.3. Ưu điểm:

- Bảo mật mạnh mẽ: IPsec mã hóa dữ liệu bằng các thuật toán mạnh như AES, DES, bảo vệ thông tin khỏi truy cập trái phép.

- Khả năng tương thích: Hỗ trợ IPv4 và IPv6, triển khai dễ dàng trên nhiều loại mạng và thiết bị.

- Linh hoạt cao: Áp dụng cho VPN site-to-site, remote access, và kết nối giữa các thiết bị mạng.

- Độ ổn định: Đảm bảo tính toàn vẹn và sẵn sàng của dữ liệu, phù hợp với các ứng dụng yêu cầu độ tin cậy cao.

- Cải thiện hiệu năng: Kết hợp QoS để ưu tiên băng thông cho lưu lượng quan trọng, nâng cao hiệu suất mạng.

- Tính toàn vẹn và xác thực: Xác thực người gửi, đảm bảo dữ liệu không bị giả mạo và chỉ người được ủy quyền mới truy cập được.

4.4. Hạn chế:

- Cấu hình phức tạp: Thiết lập IPsec yêu cầu kỹ năng cao và cài đặt bảo mật chính xác, gây khó khăn trong triển khai, nhất là với môi trường lớn.
- Giới hạn bảo vệ: IPsec chủ yếu bảo vệ lưu lượng unicast, không phù hợp với multicast và broadcast.
- Quản lý khóa phức tạp: Cần hệ thống quản lý khóa hiệu quả; việc này có thể trở nên phức tạp và ảnh hưởng đến bảo mật.
- Tăng độ trễ: Mã hóa và giải mã làm tăng độ trễ, gây khó khăn cho ứng dụng thời gian thực.
- Tốn tài nguyên hệ thống: IPsec tiêu hao nhiều tài nguyên, ảnh hưởng đến hiệu suất thiết bị khi có lưu lượng lớn.
- Tương thích hạn chế: Một số thiết bị cũ không hỗ trợ tốt IPsec, gây khó khăn cho kết nối.
- Quản lý phức tạp: Duy trì và theo dõi IPsec đòi hỏi đội ngũ IT có kinh nghiệm, đặc biệt trong môi trường lớn.
- Vấn đề với NAT: IPsec gặp khó với NAT; NAT-T giúp giảm nhưng vẫn phức tạp trong cấu hình.

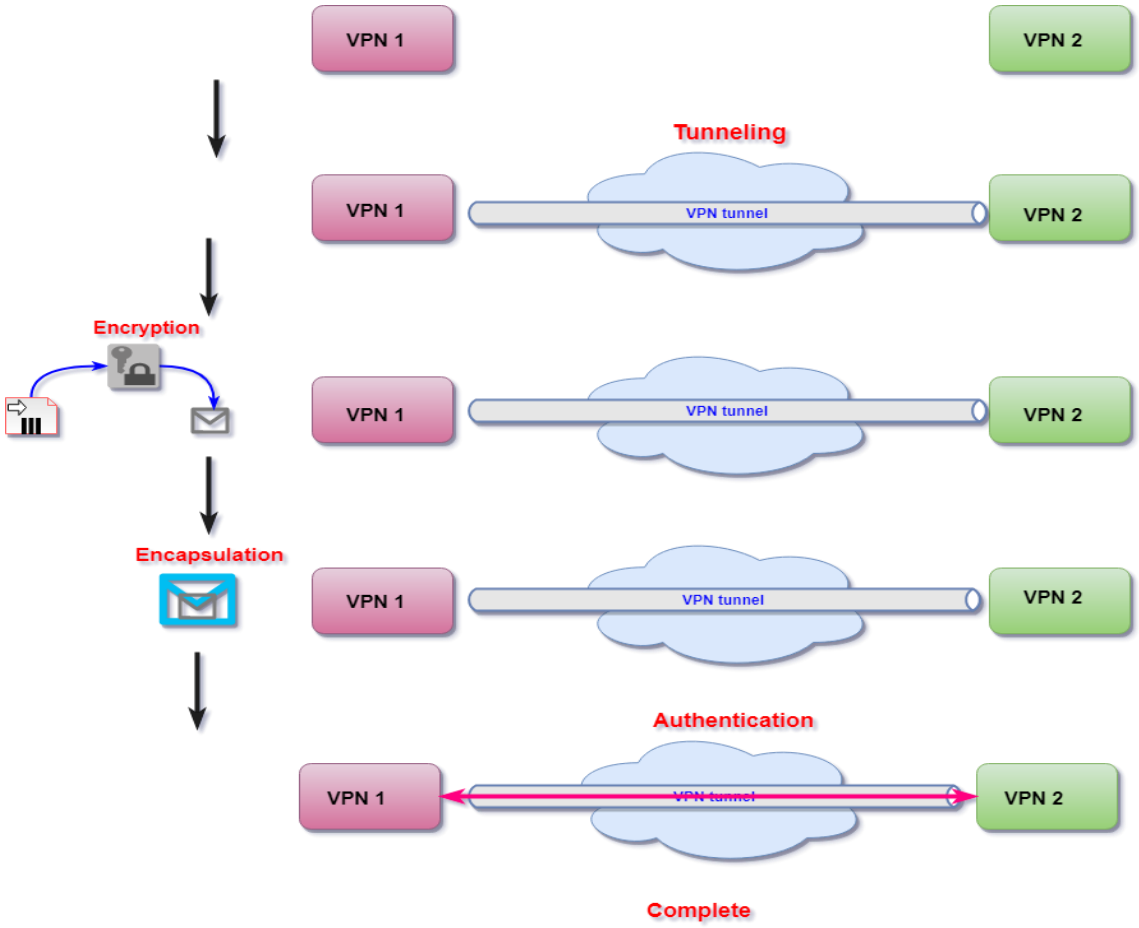
CHƯƠNG III: CÁCH THỨC HOẠT ĐỘNG

1. VPN và VPN site to site:

1.1. VPN:

VPN hoạt động bằng cách tạo ra một "đường hầm" an toàn giữa hai hoặc nhiều thiết bị. Bên trong đường hầm này, dữ liệu được mã hóa nhằm ngăn chặn truy cập trái phép. Sau đây là các bước của quá trình tạo kết nối VPN:

- Yêu cầu kết nối: Người dùng khởi tạo kết nối tới máy chủ VPN, thường bằng cách khởi động phần mềm VPN client.
- Xác thực: Máy chủ xác minh thông tin đăng nhập của người dùng (username/password, key). Nếu thông tin được xác minh, một kết nối an toàn sẽ được thiết lập.
- Thiết lập kết nối an toàn: Khi đã được xác thực, một đường hầm an toàn được hình thành giữa thiết bị của người dùng và máy chủ VPN. Đường hầm này hoạt động như một lối đi được bảo vệ.
- Đóng gói (Encapsulation): Dữ liệu của người dùng được bọc trong một giao thức VPN, tạo ra một "vỏ ngoài" bảo vệ nội dung bên trong.
- Mã hóa (Encryption): Dữ liệu truyền qua kết nối được mã hóa bằng các thuật toán như AES (Advanced Encryption Standard).
- Truyền tải: Dữ liệu đã mã hóa được gửi qua mạng công cộng đến máy chủ VPN.
- Giải đóng gói và giải mã (Decapsulation and Decryption): Khi đến máy chủ VPN, vỏ ngoài được loại bỏ (giải đóng gói) và dữ liệu được giải mã.
- Truyền tải lần cuối: Dữ liệu gốc được gửi an toàn từ máy chủ VPN đến địa chỉ đích.

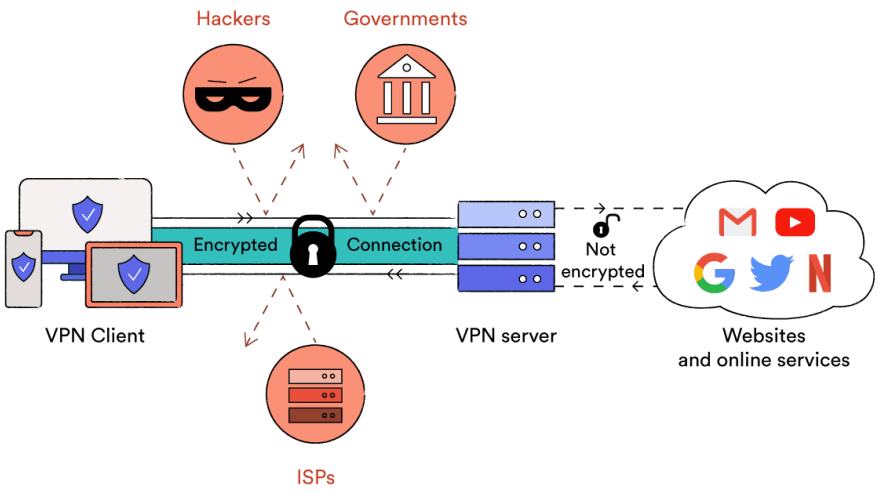


Hình 11. Quá trình thiết lập đường hầm VPN

Toàn bộ quá trình trên đảm bảo rằng dữ liệu vẫn giữ được tính riêng tư và an toàn khi di chuyển từ điểm này đến điểm khác.

Hình 12. VPN như một lớp áo giáp bảo vệ bạn khi hoạt động trực tuyến

1.2. VPN site to site:



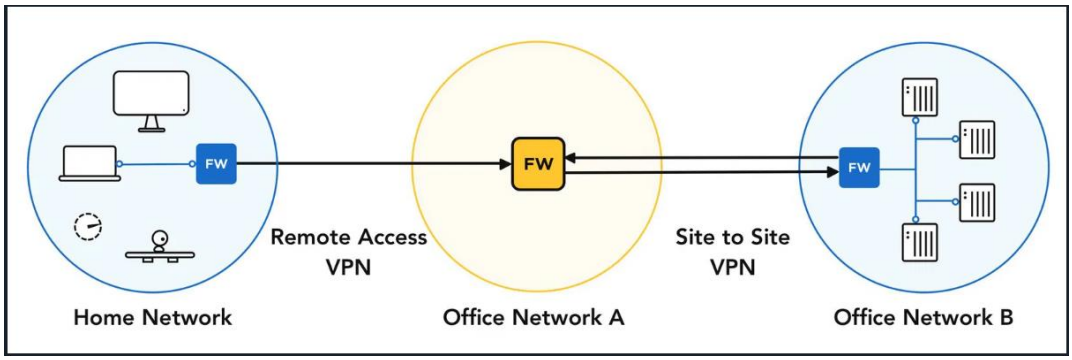
Hình 13. Cách thức hoạt động của VPN để bảo vệ dư liệu khi kết nối trực tiếp

VPN site-to-site (VPN giữa hai hoặc nhiều địa điểm) là một giải pháp VPN cho phép kết nối an toàn giữa các mạng LAN tại các địa điểm khác nhau thông qua Internet hoặc mạng riêng. Dưới đây là các bước cơ bản của quá trình thiết lập và hoạt động của VPN site-to-site:

- Cấu hình thiết bị VPN: Mỗi địa điểm cần có một thiết bị VPN, chẳng hạn như router hoặc firewall, được cấu hình để hỗ trợ kết nối VPN. Thiết bị này thường có khả năng mã hóa và giải mã dữ liệu.
- Xác thực: Khi một thiết bị tại một địa điểm cố gắng kết nối với thiết bị tại địa điểm khác, quá trình xác thực diễn ra. Thông tin đăng nhập, chẳng hạn như tên người dùng, mật khẩu hoặc khóa pre-shared key (PSK), được sử dụng để xác minh danh tính của thiết bị.
- Thiết lập kết nối an toàn: Sau khi xác thực thành công, một đường hầm VPN được tạo ra giữa hai thiết bị. Đường hầm này hoạt động như một kênh riêng tư để truyền tải dữ liệu giữa hai mạng LAN.
- Đóng gói (Encapsulation): Dữ liệu từ mạng LAN ở một địa điểm được bọc trong một giao thức VPN, tạo ra một "vỏ ngoài" bảo vệ cho dữ liệu.
- Mã hóa (Encryption): Dữ liệu được mã hóa để đảm bảo an toàn trong quá trình

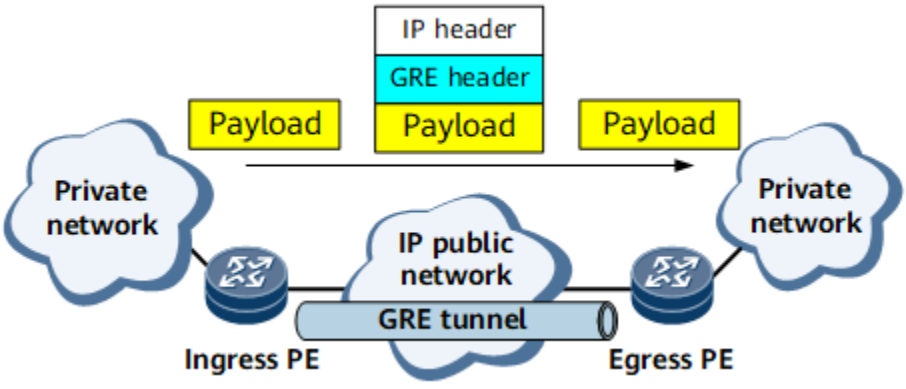
truyền tải qua Internet. Điều này giúp bảo vệ thông tin khỏi các mối đe dọa từ bên ngoài.

- Truyền tải: Dữ liệu đã mã hóa được gửi qua Internet đến thiết bị VPN ở địa điểm khác.
- Giải đóng gói và giải mã (Decapsulation and Decryption): Khi dữ liệu đến thiết bị VPN ở địa điểm đích, vỏ ngoài được loại bỏ, và dữ liệu được giải mã để trở về dạng ban đầu.
- Truyền tải đến mạng đích: Dữ liệu gốc được gửi an toàn từ thiết bị VPN đến mạng LAN đích, cho phép người dùng tại mỗi địa điểm truy cập tài nguyên như thể chúng nằm trong cùng một mạng nội bộ.



Hình 14. VPN tạo đường hầm bí mật, giúp bảo vệ dữ liệu từ xa

2. GRE Tunnel:



Hình 15. Quá trình hoạt động của đường hầm GRE

- **Thiết lập đường hầm:**

+ Khởi tạo kết nối: Hai thiết bị (router hoặc firewall) cần tạo đường hầm GRE phải được cấu hình để thiết lập kết nối. Mỗi thiết bị sẽ phải biết địa chỉ IP của nhau để thiết lập

kết nối.

+ Xác thực: Trong một số cấu hình, có thể có bước xác thực để đảm bảo rằng chỉ các thiết bị hợp lệ mới có thể thiết lập đường hầm.

- **Đóng gói dữ liệu (Encapsulation):**

+ Khi một gói dữ liệu (packet) từ giao thức bên ngoài (ví dụ: IP, IPX, hoặc AppleTalk) đến một thiết bị sử dụng GRE, gói này sẽ được đóng gói trong một gói GRE.

+ Gói GRE bao gồm một header GRE, trong đó chứa các thông tin cần thiết như loại giao thức của gói bên trong, cũng như một số thông tin kiểm soát khác.

- **Truyền tải qua đường hầm:**

+ Gói GRE sau khi được đóng gói sẽ được gửi qua mạng đến thiết bị đích thông qua đường hầm đã được thiết lập.

+ Gói này có thể đi qua nhiều mạng khác nhau, nhưng vì nó được đóng gói trong một gói GRE, thông tin gốc bên trong sẽ được bảo vệ.

- **Giải đóng gói dữ liệu (Decapsulation):**

+ Khi gói GRE đến thiết bị đích, thiết bị này sẽ giải đóng gói (decapsulate) gói GRE bằng cách loại bỏ header GRE.

+ Sau khi loại bỏ header, gói dữ liệu bên trong sẽ được phục hồi về dạng ban đầu và được xử lý theo giao thức gốc.

- Truyền tải đến đích cuối: Gói dữ liệu gốc sau khi được giải đóng gói sẽ được gửi đến địa chỉ IP đích trên mạng nội bộ của thiết bị đích.

3. IPSEC

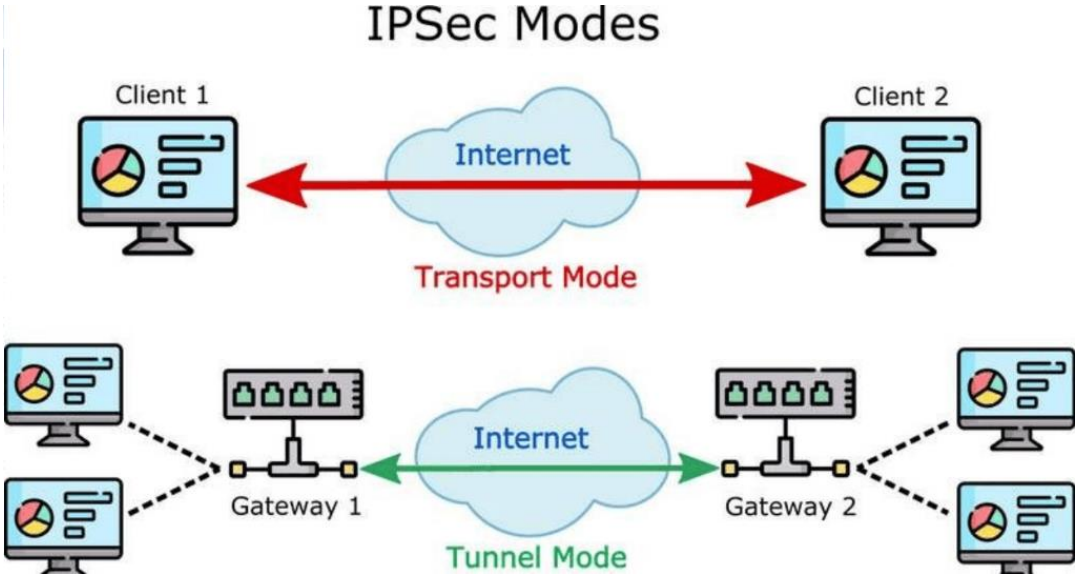
3.1. Chế độ hoạt động của IPSEC:

Giao thức IPSec bao gồm hai chế độ hoạt động khác nhau:

- Transport Mode: được sử dụng để bảo vệ dữ liệu giữa các thiết bị trong một mạng tin cậy. Trong chế độ này, chỉ có dữ liệu người dùng được mã hóa và bảo vệ, IP Header không bị thay đổi hay mã hóa. Transport Mode được sử dụng cho các kết nối VPN client-to-site.

- Tunnel Mode: được sử dụng để bảo vệ dữ liệu giữa hai mạng không tin cậy thông qua một VPN trung gian. Trong chế độ này, toàn bộ gói tin IP sẽ được mã hóa và bảo vệ, bao gồm cả IP Header và payload, để đảm bảo tính toàn vẹn của dữ liệu. Tunnel

Mode được sử dụng cho các kết nối site-to-site.



Hình 16. Chế độ hoạt động của Ipsec

3.2. Cách thức hoạt động của IPSEC:

Trao đổi khóa:

- Khóa là yếu tố thiết yếu trong quá trình mã hóa. Khóa được sử dụng để "khóa" (mã hóa) và "mở khóa" (giải mã) dữ liệu.
- IPsec thiết lập khóa thông qua trao đổi khóa giữa các thiết bị kết nối, đảm bảo rằng mỗi thiết bị có thể giải mã tin nhắn được gửi từ thiết bị khác. Quy trình này thường sử dụng các giao thức như Internet Key Exchange (IKE) để thương lượng và trao đổi khóa an toàn.

Tiêu đề và phần cuối của gói tin:

- Dữ liệu được gửi qua mạng được chia thành các phần nhỏ hơn gọi là gói tin. Mỗi gói tin chứa:

+ Tải trọng: Dữ liệu thực tế cần được gửi.

+ Tiêu đề: Thông tin về gói tin để máy tính nhận biết cách xử lý chúng. IPsec thêm tiêu đề vào gói dữ liệu để chứa thông tin xác thực và mã hóa.

- Ngoài ra, IPsec cũng thêm phần cuối vào sau tải trọng của mỗi gói tin, cung cấp thêm thông tin cần thiết cho việc xác thực và kiểm tra toàn vẹn.

Xác thực: IPsec cung cấp xác thực cho từng gói tin, đảm bảo rằng các gói đến từ nguồn đáng tin cậy và không bị thay đổi. Điều này giống như việc gắn một con dấu xác thực lên một vật phẩm, giúp nhận biết nguồn gốc và tính toàn vẹn của dữ liệu.

Mã hóa:

- IPsec mã hóa các tải trọng của từng gói tin và tiêu đề IP (trừ khi sử dụng chế độ vận chuyển thay vì chế độ đường hầm).
- Việc mã hóa này bảo vệ dữ liệu trong quá trình truyền tải, đảm bảo rằng dữ liệu được bảo mật và giữ tính riêng tư.

Truyền:

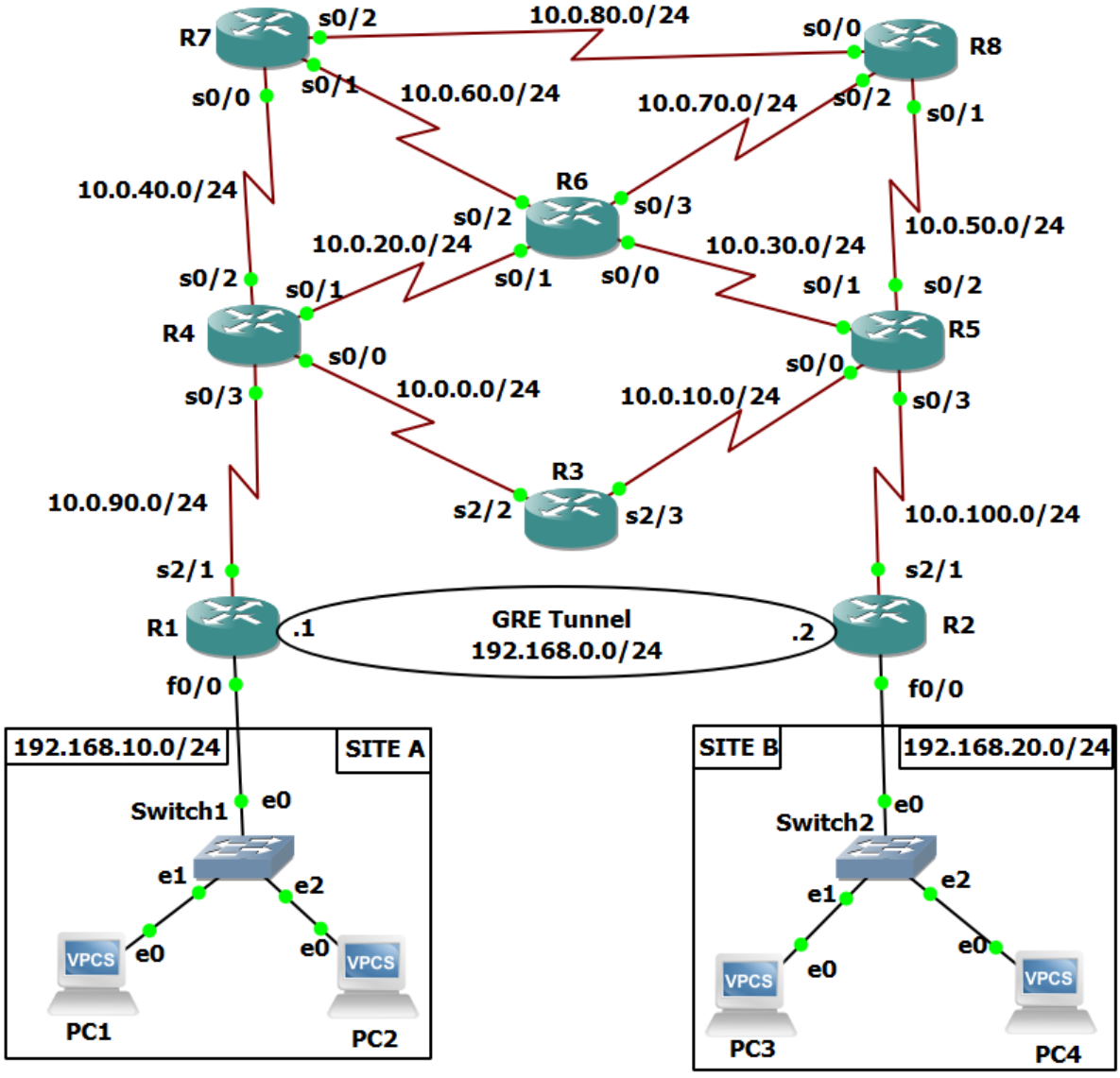
- Các gói IPsec được mã hóa sẽ được truyền qua một hoặc nhiều mạng đến đích. Trong giai đoạn này, lưu lượng IPsec thường sử dụng UDP (Giao thức dữ liệu người dùng) làm giao thức truyền tải, thay vì TCP (Giao thức điều khiển truyền tải).
- Việc sử dụng UDP cho phép các gói IPsec vượt qua tường lửa một cách dễ dàng hơn, vì UDP không thiết lập các kết nối chuyên dụng như TCP, giúp giảm thiểu sự chậm trễ và tăng tính linh hoạt.

Giải mã: Khi các gói tin IPsec đến đầu bên kia, chúng sẽ được giải mã và xác thực. Sau khi giải mã, dữ liệu có thể được sử dụng bởi các ứng dụng, chẳng hạn như trình duyệt web, để thực hiện các tác vụ cần thiết.

CHƯƠNG IV: THỰC HIỆN CẤU HÌNH VPN GRE IPSEC

1. Thực hiện trên GNS3

Để thực hiện cấu hình VPN GRE Tunel với IPSec trên GNS3 nhóm đã tiến hành xây dựng topology gồm có: 2 site chính là SiteA và SiteB dùng để kết nối với nhau bằng GRE tunnel qua R1 và R2, 6 router còn lại nhằm mô phỏng môi trường bên ngoài internet.



Hình 17. Mô hình mạng

Để các router có thể định tuyến được với nhau, nhóm chọn phương thức định tuyến OSPF trên cả 8 router. Tiến hành Ping đến một máy tính trong SiteB bằng một

máy tính trong SiteA:

```
PC1 : 192.168.20.20 255.255.255.0 gateway 192.168.20.1

PC4> ping 192.168.10.10
84 bytes from 192.168.10.10 icmp_seq=1 ttl=59 time=74.821 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=59 time=77.324 ms
84 bytes from 192.168.10.10 icmp_seq=3 ttl=59 time=76.775 ms
84 bytes from 192.168.10.10 icmp_seq=4 ttl=59 time=75.420 ms
84 bytes from 192.168.10.10 icmp_seq=5 ttl=59 time=76.818 ms

PC4>
```

```
PC1 : 192.168.10.10 255.255.255.0 gateway 192.168.10.1

PC1> ping 192.168.20.20
192.168.20.20 icmp_seq=1 timeout
84 bytes from 192.168.20.20 icmp_seq=2 ttl=59 time=75.810 ms
84 bytes from 192.168.20.20 icmp_seq=3 ttl=59 time=106.864 ms
84 bytes from 192.168.20.20 icmp_seq=4 ttl=59 time=75.997 ms
84 bytes from 192.168.20.20 icmp_seq=5 ttl=59 time=76.772 ms
```

Hình 18. Định tuyến OSPF trên router, ping 2 máy tính ở 2 sites

Thực hiện thành công chứng tỏ ta đã cấu hình OSPF chính xác và 2 Site giờ đây có thể giao tiếp với nhau, thử trace bằng ICMP để xem đường đi của gói tin giữa 2 PC này:

```
PC4> trace 192.168.10.10 -P 1
trace to 192.168.10.10, 8 hops max (ICMP), press Ctrl+C to stop
 1   192.168.20.1   15.503 ms  15.066 ms  15.129 ms
 2   10.0.100.2   30.992 ms  31.295 ms  30.338 ms
 3   10.0.30.2   31.746 ms  31.475 ms  30.838 ms
 4   10.0.20.1   30.454 ms  30.549 ms  30.177 ms
 5   10.0.90.1   46.691 ms  45.731 ms  45.539 ms
 6   192.168.10.10   76.069 ms  77.042 ms  76.211 ms
```

```
PC1> trace 192.168.20.20 -P 1
trace to 192.168.20.20, 8 hops max (ICMP), press Ctrl+C to stop
 1   192.168.10.1   15.196 ms  15.561 ms  15.755 ms
 2   10.0.90.2   30.054 ms  31.222 ms  31.306 ms
 3   10.0.0.1   45.293 ms  46.078 ms  45.988 ms
 4   10.0.10.2   46.301 ms  46.093 ms  46.629 ms
 5   10.0.100.1   60.228 ms  61.730 ms  61.174 ms
 6   192.168.20.20   76.617 ms  75.985 ms  76.543 ms
```

Hình 19. Traceroute để xem dường đi của 2 site

Sau khi hoàn tất bước trên, ta tạo một Tunnel với với tên Tunnel1, đồng thời tiến hành cấu hình Static Route để có thể giao tiếp giữa 2 site thông qua đường hầm,

(vì định tuyến bằng Static Route với AD = 1, độ ưu tiên sẽ cao hơn khi lựa chọn tuyến đường định tuyến bằng OSPF với AD = 110) với IP được hiển thị ở 2 router R1 và R2 cùng với bảng tóm tắt Interface của 2 router như sau:

Trên R1

```
SITE-A#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.10.1    YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0         unassigned      YES NVRAM  administratively down down
Serial2/0                  20.20.20.2      YES NVRAM  up                    down
Serial2/1                  10.0.90.1       YES NVRAM  up                    up
Serial2/2                  unassigned      YES NVRAM  administratively down down
Serial2/3                  unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
Tunnel1                    192.168.0.1     YES NVRAM  up                    up
```

Trên R2

```
SITE-B#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.20.1    YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0         unassigned      YES NVRAM  administratively down down
Serial2/0                  30.30.30.2      YES NVRAM  up                    down
Serial2/1                  10.0.100.1      YES NVRAM  up                    up
Serial2/2                  unassigned      YES NVRAM  administratively down down
Serial2/3                  unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
Tunnel1                    192.168.0.2     YES NVRAM  up                    up
```

Hình 20. Tạo tunnel, cấu hình static route chạy qua tunnel

Để biết chi tiết hơn về Tunnel này nhóm tiến hành show ra source và destination ở cả 2 bên router:

```
SITE-A#show interface tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.0.1/24
  MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.90.1, destination 10.0.100.1
```

```
SITE-B#show interfaces tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.0.2/24
  MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.100.1, destination 10.0.90.1
```

Hình 21. Source và destination của tunnel ở 2 sites

Lúc này ta đã dùng được Tunnel, việc dùng Ping để kiểm chứng có thể gây nhầm lẫn bởi khi không có Tunnel, việc Ping vẫn diễn ra, vì thế, cách kiểm tra hiệu quả chính là trace bằng ICMP như sau:

```
PC4> trace 192.168.10.10 -P 1
trace to 192.168.10.10, 8 hops max (ICMP), press Ctrl+C to stop
 1   192.168.20.1   15.167 ms  15.801 ms  15.932 ms
 2   192.168.0.1   60.191 ms  62.296 ms  62.025 ms
 3   192.168.10.10   76.113 ms  76.001 ms  75.696 ms
```

```
PC1> trace 192.168.20.20 -P 1
trace to 192.168.20.20, 8 hops max (ICMP), press Ctrl+C to stop
 1   192.168.10.1   15.735 ms  15.133 ms  15.266 ms
 2   192.168.0.2   60.184 ms  61.452 ms  60.638 ms
 3   192.168.20.20   76.209 ms  75.770 ms  76.482 ms
```

Hình 22. Kiểm tra đường hầm đã hoạt động

Như kết quả cho thấy, gói tin để đi được đến đích phải đi qua lớp mạng 192.168.0.1 cũng như 192.168.0.2 đây chính là 2 đầu của Tunnel ta vừa cấu hình được, điều này cho thấy Tunnel đã hoạt động chính xác.

Bước tiếp theo sẽ là cấu hình IPSec thông qua Tunnel vừa tạo được, việc cấu hình sẽ diễn ra ở 2 Phase như sau:

Ở Phase 1, nhóm cấu hình ISAKMP SA để trao đổi, thỏa thuận các thông số bảo mật, nhằm cung cấp một kênh truyền bảo mật giữa hai đầu Tunnel. Các thông số có thể liệt kê ngắn gọn như sau:

- Thuật toán mã hóa: AES dùng key 256 bit.
- Thuật toán hash: MD5.
- Phương pháp xác thực: Preshare-key.
- Nhóm khóa: Diffie-Hellman sử dụng thuật toán 2048-bit cho việc tạo khóa
- Life time: 3600s tương đương 1 giờ, chính là thời gian tồn tại một Session của IPSec, sau đó key sẽ được làm mới.

Ở Phase 2, nhóm sẽ cấu hình IPSec SA thiết lập và duy trì các kết nối bảo mật giữa

hai thiết bị, tại đây, các gói tin khi gửi đi sẽ chính thức được mã hóa. Cơ bản về IPSec SA được nhóm cấu hình như sau:

- Thuật toán mã hóa được sử dụng : AES.
- Thuật toán xác thực tính toàn vẹn của gói tin: HMAC-MD5.
- Chế độ hoạt động: transport mode.

Ngoài ra, ở Phase 2 này ta có đến 2 sự lựa chọn cho việc đặt IPSec ở đâu. Đầu tiên, IPSec sẽ được cấu hình trên **Network Interface Cards,** cách cấu hình này là **Crypto Map**. Cách thứ 2 chính là cấu hình IPSec ngay trên **Tunnel**, cách cấu hình này chính là **Tunnel IPSec Profile.** Sẽ có đôi nét khác biệt trong cách cấu hình trên, tuy nhiên 2 cách này hoàn toàn tương thích với nhau, ta có thể lựa chọn cấu hình R1 là Crypto Map, R2 là Tunnel IPSec Profile, hoặc ngược lại, hoặc có thể cả 2 cùng cấu hình Crypto Map cũng như Tunnel IPSec Profile.

Tóm lại, ta có một vài hướng cấu hình, tuy nhiên ở đây, nhóm sẽ chọn kết hợp cả 2 lại tức R1 ứng với SiteA sẽ cấu hình Crypto Map, R2 ứng với SiteB sẽ cấu hình Tunnel IPSec Profile. Và dưới đây là kết quả kiểm tra sau khi cấu hình xong.

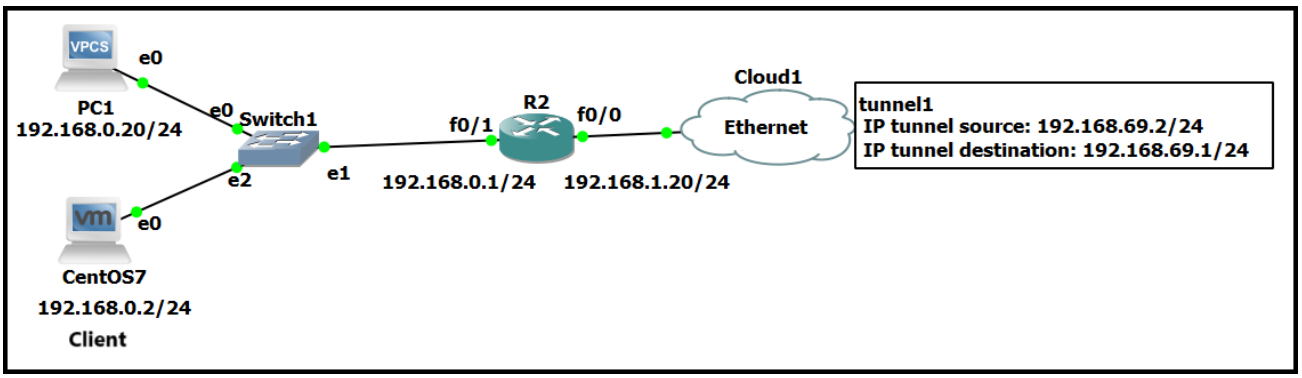
```
SITE-A#show running-config | include (crypto map|ipsec)
crypto ipsec transform-set HTD esp-aes 256 esp-md5-hmac
crypto map GRE-CMAP 10 ipsec-isakmp
 crypto map GRE-CMAP
```

```
SITE-B#show running-config | include (crypto map|ipsec)
crypto ipsec transform-set HTD esp-aes 256 esp-md5-hmac
crypto ipsec profile GRE-PROFILE
 tunnel protection ipsec profile GRE-PROFILE
```

Hình 23. Cấu hình Ipsec cho router ở 2 sites

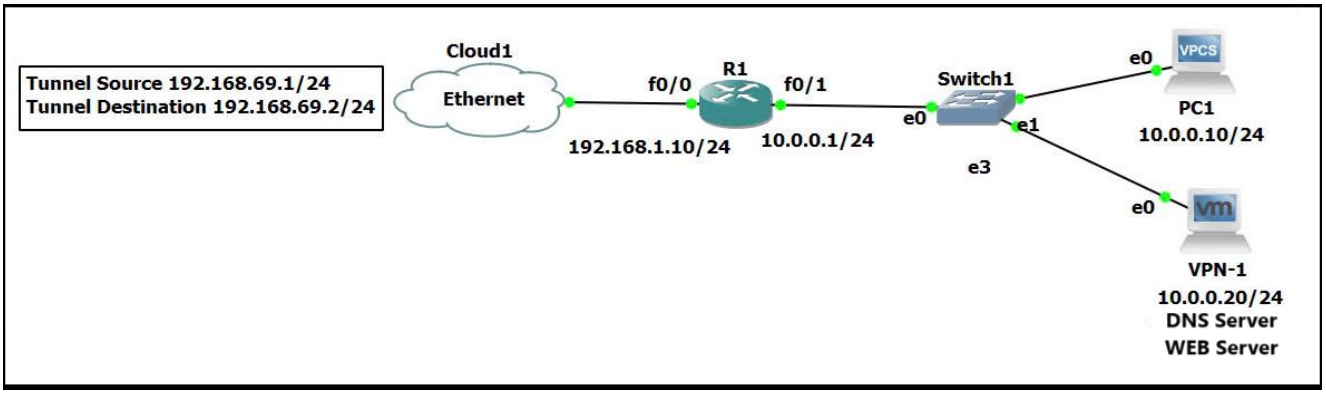
2. Thực hiện thông qua dây mạng LAN kết nối 2 thiết bị

Dưới đây là topology cũng như IP của từng thiết bị và Tunnel trên PC thứ nhất:



Hình 24. Mô hình mạng thông qua dây mạng LAN kết nối 2 thiết bị (ở site A)

Tương tự trên, dưới đây là trên PC thứ hai:



Hình 25. Mô hình mạng thông qua dây mạng Lan kết nối 2 thiết bị (ở site B)

Nhóm tiến hành kết nối 2 PC với nhau thông qua cáp mạng xoắn đôi UTP, giả lập 2 PC kết nối với nhau thông qua internet. Tiếp tục đến bước cấu hình IP và Static Route cho 2 PC như dưới:

```
R1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.10    YES NVRAM  up                    up
Serial0/0                  unassigned      YES NVRAM  administratively down down
FastEthernet0/1            10.0.0.1        YES NVRAM  up                    up
Serial0/1                  unassigned      YES NVRAM  administratively down down
Serial0/2                  unassigned      YES NVRAM  administratively down down
Serial0/3                  unassigned      YES NVRAM  administratively down down
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
Tunnel1                    192.168.69.1    YES NVRAM  up                    up
```

```
R2#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.20    YES NVRAM  up                    up
FastEthernet0/1            192.168.0.1     YES NVRAM  up                    up
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
Serial2/0                  unassigned      YES NVRAM  administratively down down
Serial2/1                  unassigned      YES NVRAM  administratively down down
Serial2/2                  unassigned      YES NVRAM  administratively down down
Serial2/3                  unassigned      YES NVRAM  administratively down down
Tunnel1                    192.168.69.2    YES NVRAM  up                    up
```

Hình 26. Cấu hình IP cho 2 thiết bị ở 2 sites

```
R1# show interface tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.69.1/24
  MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.1.10, destination 192.168.1.20
  Tunnel protocol/transport GRE/IP
```

```
R2#sh int tun1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.69.2/24
  MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.1.20, destination 192.168.1.10
  Tunnel protocol/transport GRE/IP
```

Hình 27. Thông tin Tunnel

```
     10.0.0.0/24 is subnetted, 1 subnets
S       10.0.0.0 [1/0] via 192.168.69.1
C    192.168.0.0/24 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.69.0/24 is directly connected, Tunnel1
```

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/1
S    192.168.0.0/24 [1/0] via 192.168.69.2
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.69.0/24 is directly connected, Tunnel1
```

Hình 28. Cấu hình Static Route cho Tunnel

```
R1#ping 192.168.69.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.69.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/65/68 ms
R1#traceroute 192.168.0.20

Type escape sequence to abort.
Tracing the route to 192.168.0.20

  1 192.168.69.2 96 msec 92 msec 92 msec
  2 192.168.0.20 96 msec 104 msec 96 msec
```

```
R2#ping 192.168.69.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.69.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/28/36 ms
R2#trace
R2#traceroute 10.0.0.20

Type escape sequence to abort.
Tracing the route to 10.0.0.20

  1 192.168.69.1 32 msec 16 msec 12 msec
  2 10.0.0.20 44 msec 48 msec 40 msec
```

Hình 29. Kiểm thử Tunnel

Ta thấy khi traceroute gói tin có đi qua 192.168.69.1 cũng như 192.168.69.2, điều này cho thấy Tunnel hoạt động tốt.

Tiếp đến ta cấu hình IPSec, ở Phase 1 ta có được ISKMP SA như hình dưới:

```
R1#show crypto isakmp sa
dst             src             state          conn-id slot status
192.168.1.10    192.168.1.20    QM_IDLE              2    0 ACTIVE
```

```
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.1.10    192.168.1.20    QM_IDLE           1001    0 ACTIVE
```

Hình 30. Xem trạng thái iskamp sa

```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

```
R2#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

Hình 31. isakmp policy

Tiếp tục cấu hình, ta sẽ có được kết quả cho IPSec :

Ở trên R1 của PC thứ 2

```
R1#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: GRE-CMAP, local addr 192.168.1.10

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.20/255.255.255.255/47/0)
   current_peer 192.168.1.20 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3125, #pkts encrypt: 3125, #pkts digest: 3125
    #pkts decaps: 5794, #pkts decrypt: 5794, #pkts verify: 5794
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.1.10, remote crypto endpt.: 192.168.1.20
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x5FA0FFAE(1604386734)

     inbound esp sas:
      spi: 0x8EE9DF77(2397691767)
        transform: esp-256-aes esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 2002, flow_id: SW:2, crypto map: GRE-CMAP
        sa timing: remaining key lifetime (k/sec): (4393904/1223)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x5FA0FFAE(1604386734)
        transform: esp-256-aes esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 2001, flow_id: SW:1, crypto map: GRE-CMAP
        sa timing: remaining key lifetime (k/sec): (4394097/1217)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Hình 32. ipsec sa trên R1 của PC thứ 2

Và ở trên R2 của PC thứ nhất:

```
R2#show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.1.20

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.10/255.255.255.255/47/0)
   current_peer 192.168.1.10 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1953, #pkts encrypt: 1953, #pkts digest: 1953
    #pkts decaps: 704, #pkts decrypt: 704, #pkts verify: 704
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.1.20, remote crypto endpt.: 192.168.1.10
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x8EE9DF77(2397691767)

     inbound esp sas:
      spi: 0x5FA0FFAE(1604386734)
        transform: esp-256-aes esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 1, flow_id: SW:1, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4543983/913)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x8EE9DF77(2397691767)
        transform: esp-256-aes esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 2, flow_id: SW:2, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4543789/913)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Hình 33. ipsec sa trên R1 của PC thứ nhất

Tiến hành show Session ta biết được đường đi của dữ liệu khi đi qua Tunnel như dưới kết quả :

```
R1#show crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 192.168.1.20 port 500
  IKE SA: local 192.168.1.10/500 remote 192.168.1.20/500 Active
  IPSEC FLOW: permit 47 host 192.168.1.10 host 192.168.1.20
        Active SAs: 2, origin: crypto map
```

```
R2#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 192.168.1.10 port 500
  IKE SA: local 192.168.1.20/500 remote 192.168.1.10/500 Active
  IPSEC FLOW: permit 47 host 192.168.1.20 host 192.168.1.10
        Active SAs: 2, origin: crypto map
```

Hình 34. crypto session ở 2 router

CHƯƠNG V: KIỂM TRA KẾT QUẢ

1. Thực hiện trên GNS3

Ta thực hiện dùng một PC trong SiteA Ping sang một PC ở SiteB đồng thời trace thấy rằng gói tin đã đi đúng vào Tunnel ta cấu hình.

```
PC1 : 192.168.20.10 255.255.255.0 gateway 192.168.20.1

PC3> ping 192.168.10.20
192.168.10.20 icmp_seq=1 timeout
192.168.10.20 icmp_seq=2 timeout
84 bytes from 192.168.10.20 icmp_seq=3 ttl=62 time=75.963 ms
84 bytes from 192.168.10.20 icmp_seq=4 ttl=62 time=75.543 ms
84 bytes from 192.168.10.20 icmp_seq=5 ttl=62 time=76.930 ms

PC3> trace 192.168.10.20 -P 1
trace to 192.168.10.20, 8 hops max (ICMP), press Ctrl+C to stop
 1   192.168.20.1   16.113 ms  15.867 ms  15.523 ms
 2   192.168.0.1   60.894 ms  60.865 ms  61.116 ms
 3   192.168.10.20   77.112 ms  75.260 ms  76.074 ms
```

```
PC1 : 192.168.10.20 255.255.255.0 gateway 192.168.10.1

PC2> ping 192.168.20.10
84 bytes from 192.168.20.10 icmp_seq=1 ttl=62 time=75.394 ms
84 bytes from 192.168.20.10 icmp_seq=2 ttl=62 time=76.035 ms
84 bytes from 192.168.20.10 icmp_seq=3 ttl=62 time=77.448 ms
84 bytes from 192.168.20.10 icmp_seq=4 ttl=62 time=77.260 ms
84 bytes from 192.168.20.10 icmp_seq=5 ttl=62 time=75.254 ms

PC2> trace 192.168.20.10 -P 1
trace to 192.168.20.10, 8 hops max (ICMP), press Ctrl+C to stop
 1   192.168.10.1   15.692 ms  15.961 ms  15.183 ms
 2   192.168.0.2   60.201 ms  60.710 ms  61.678 ms
 3   192.168.20.10   77.668 ms  77.046 ms  74.976 ms
```

Hình 35. Kiểm tra tunnel

Sau khi thực hiện các câu lệnh, ta Check số lượng gói tin được Encrypt cũng như Decrypt sẽ thấy có sự thay đổi, đồng thời chứng tỏ gói tin truyền qua lại Tunnel đề được mã hóa.

```
SITE-A#show crypto ipsec sa | include encrypt|decrypt
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
SITE-A#show crypto ipsec sa | include encrypt|decrypt
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
SITE-A#show crypto ipsec sa | include encrypt|decrypt
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
    #pkts decaps: 22, #pkts decrypt: 22, #pkts verify: 22
```

```
SITE-B#show crypto ipsec sa | include encrypt|decrypt
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
SITE-B#show crypto ipsec sa | include encrypt|decrypt
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
SITE-B#show crypto ipsec sa | include encrypt|decrypt
    #pkts encaps: 22, #pkts encrypt: 22, #pkts digest: 22
    #pkts decaps: 21, #pkts decrypt: 21, #pkts verify: 21
```

Hình 36. Kiểm tra mã hóa

2. Thực hiện thông qua dây mạng LAN kết nối 2 thiết bị

Ở một site sẽ có 1 máy ảo VMware đã được dựng sẵn Web server và DNS server có domain là sgu.edu.vn, site còn lại có 1 máy ảo truy cập đến thông qua tên miền sgu.edu.vn.

Hình 37. IP ở Web server và Client

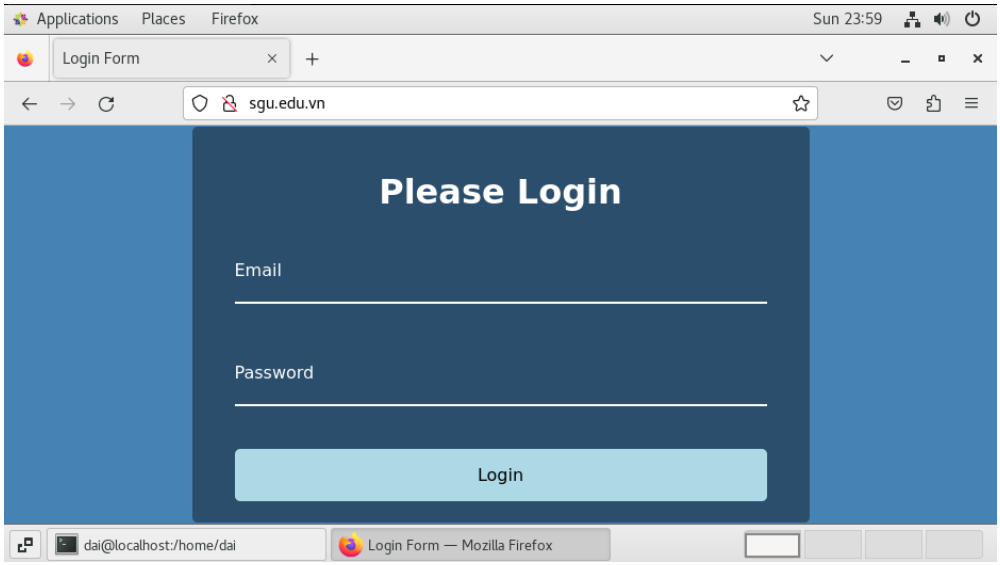
Bước tiếp theo ta tiến hành nslookup trên máy Client để kiểm tra kết nối đến và đã phân giải được Domain chưa.

```
[root@localhost dai]# nslookup
> sgu.edu.vn
Server:         10.0.0.20
Address:        10.0.0.20#53

Name:   sgu.edu.vn
Address: 10.0.0.20
>
```

Hình 38. Kiểm tra phân giải tên miền

Sau khi hoàn thành, ta tiến hành vào trình duyệt Web để truy cập vào sgu.edu.vn.



Hình 39. Truy cập web từ Client

Và bước cuối cùng để đảm bảo kết nối từ Client đến Server đã thông qua Tunnel thì nhóm tiến hành traceroute và được kết quả hoàn toàn chính xác:

```
[root@localhost dai]# traceroute sgu.edu.vn
traceroute to sgu.edu.vn (10.0.0.20), 30 hops max, 60 byte packets
 1  gateway (192.168.0.1)  13.738 ms  28.304 ms  43.259 ms
 2  192.168.69.1 (192.168.69.1)  57.715 ms  72.667 ms  87.269 ms
 3  ns1.sgu.edu.vn (10.0.0.20)  102.870 ms  132.875 ms  147.133 ms
[root@localhost dai]# traceroute 10.0.0.20
traceroute to 10.0.0.20 (10.0.0.20), 30 hops max, 60 byte packets
 1  gateway (192.168.0.1)  2.102 ms  17.013 ms  31.838 ms
 2  192.168.69.1 (192.168.69.1)  47.010 ms  62.672 ms  77.526 ms
 3  sgu.edu.vn (10.0.0.20)  123.569 ms  138.920 ms  168.732 ms
```

Hình 40. Kiểm tra traceroute đến tên miền

Đồng thời quay lại router kiểm tra thì số lượng gói tin được Encrypt và Decrypt có tăng lên sau lần truy cập đến Server trên.

```
R2#show crypto ipsec sa | include encrypt|decrypt
    #pkts encaps: 2081, #pkts encrypt: 2081, #pkts digest: 2081
    #pkts decaps: 752, #pkts decrypt: 752, #pkts verify: 752
```

Hình 41. Kiểm tra mã hóa

TÀI LIỆU THAM KHẢO

[1] Hocchudong (no date) Thuctap012017/TAMNT/VPN-openvpn/docs/1.tong_quan_vpn_(vpn_overview).md at master · Hocchudong/thuctap012017, GitHub. Available at: https://github.com/hocchudong/thuctap012017/blob/master/TamNT/VPN-OpenVPN/docs/1.Tong_quan_VPN_(VPN_overview).md (Accessed: 12 November 2024).

[2] nội, H. (2024) VPN LÀ GÌ? Giải Thích Cách Hoạt động CỦA VPN, 200Lab Blog. Available at: https://200lab.io/blog/vpn-la-gi-giai-thich-cach-hoat-dong-vpn/ (Accessed: 12 November 2024).

[3] Hưng, N. (2024) Những điều Bạn Cần Biết về VPN site to site MỚI NHẤT 2024, Vietnix. Available at: https://vietnix.vn/vpn-site-to-site/ (Accessed: 12 November 2024).

[4] (No date) Tìm Hiểu Về ipsec | lab network system security. Available at: https://securityzone.vn/t/tim-hieu-ve-ipsec.11921/ (Accessed: 12 November 2024).

[5] Viettuanvn (2024) VPN LÀ GÌ? ưu nhược điểm, Cách hoạt động, Công dụng Của VPN, Việt Tuấn - Phân Phối Thiết Bị Mạng, Wifi, Thiết Bị Lưu Trữ NAS. Available at: https://viettuans.vn/vpn-la-gi (Accessed: 12 November 2024).

[6] What is site-to-site VPN (no date) Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary/what-is-site-to-site-vpn (Accessed: 12 November 2024).

[7] Chkadmin (2024) What is a site to site VPN?, Check Point Software. Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-vpn/what-is-a-site-to-site-vpn/ (Accessed: 12 November 2024).

Chi tiết cấu hình trong báo cáo tại đường dẫn sau:
https://github.com/tanduong9424/VPN_GRE_TUNNEL_IPSEC