BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC NHA TRANG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỀ TÀI THỰC TẬP CƠ SỞ**

**NGHIÊN CỨU TRIỂN KHAI GRE KẾT HỢP IPSEC TRONG MẠNG VPN VÀ DEMO TRÊN CISCO PACKET TRACER**

**GVHD:** Cấn Thị Phượng

**SVTH:** Ngô Quang

**Lớp:** 61.CNTT-3

**MSSV:** 61134224

Khánh Hòa – 01/2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC NHA TRANG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỀ TÀI THỰC TẬP CƠ SỞ**

**NGHIÊN CỨU TRIỂN KHAI GRE KẾT HỢP IPSEC TRONG MẠNG VPN VÀ DEMO TRÊN CISCO PACKET TRACER**

**GVHD:** Cấn Thị Phượng

**SVTH:** Ngô Quang

**Lớp:** 61.CNTT-3

**MSSV:** 61134224

Khánh Hòa – 01/2022

# **LỜI CÁM ƠN**

Để hoàn thành đề tài thực tập cơ sở này, trước hết em xin gửi đến quý thầy cô Khoa Công nghệ thông tin – Trường Đại học Nha Trang lời cám ơn chân thành.

Em xin gửi đến cô Cấn Thị Phượng, người đã tận tình giúp đỡ em hoàn thành đề tài thực tập cơ sở này lời cám ơn sâu sắc nhất.

Trong quá trình nghiên cứu thực hiện đề tài, cũng như là trong quá trình làm bài báo cáo thực tập cơ sở, khó tránh khỏi sai sót, rất mong các thầy, cô bỏ qua. Đồng thời do kiến thức cũng như kinh nghiệm thực tiễn của bản thân còn hạn chế nên đề tài, bài báo cáo thực tập cơ sở này khó có thể không tránh khỏi những thiếu sót, em rất mong nhận được ý kiến đóng góp từ quý thầy, cô để em học hỏi thêm được nhiều kinh nghiệm, cũng như kỹ năng cần thiết.

Em xin chân thành cám ơn!

# **PHẦN MỞ ĐẦU**

* **Lý do chọn đề tài:**

Ngày nay, xã hội ngày càng phát triển thì nhu cầu trao đổi thông tin trong xã hội ngày càng lớn, đặt biệt là ở các tổ chức và doanh nghiệp. Các tổ chức và doanh nghiệp có đặc thù là nhiều bộ phận, nhiều chi nhánh và quy mô lớn. Nhu cầu trao đổi thông tin giữa họ rẩt lớn, trong đó có các nội dụng liên quan đến bí mật kinh doanh quan trọng.

Nếu các thông tin của doanh nghiệp truyền tải qua mạng Internet thì sẽ gặp nhiều vấn đề về an toàn. Vì thế làm thế nào để đảm bảo việc trao đổi thông tin được an toàn và bào mật là vấn đề rất cấp thiết bên cạnh sự nổi lên ngày càng nhiều của vấn đề về an ninh mạng.

Để có thể giải quyết các vấn đề này VPN (Virtual Private Network) hay còn gọi là mạng riêng ảo là giải pháp cho vấn đề này, nó không chỉ an toàn mà còn có chi phí thấp rất phù hợp với các doanh nghiệp và tổ chức.

VPN là một mạng riêng ảo cung cấp các giải pháp điều khiển từ xa an toàn và rẻ tiếp cận cho các doanh nghiệp. Mạng riêng ảo an toàn được thiết lập trên Internet bằng cách sử dụng đường hầm bảo mật GRE với IPSec VPN. Qua đó, thông tin dữ liệu có thể bảo đảm an toàn một cách hiệu quả và giải quyết vấn đề về khả năng mở rộng của VPN.

Vì những lý do trên, nên em đã quyết định thực hiện đề tài: **“Nghiên cứu triển khai GRE kết hợp IPSec trong mạng VPN và demo trên Cisco Packet Tracer”.**

* **Cấu trúc của báo cáo bao gồm:**

**Chương 1:** Tổng quan về vấn đề nghiên cứu

**Chương 2:** Cơ sở lý thuyết

**Chương 3:** Nghiên cứu GRE và IPSec

**Chương 4:** Triển khai và demo trên Cisco Packet Tracer

**Chương 5:** Kết luận và hướng phát triển

**MỤC LỤC**

[LỜI CÁM ƠN 3](#_Toc93564082)

[PHẦN MỞ ĐẦU 4](#_Toc93564083)

[Chương 1: TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU 7](#_Toc93564084)

[1.1 GIỚI THIỆU VỀ ĐỀ TÀI 8](#_Toc93564085)

[1.2 MỤC TIÊU CỦA ĐỀ TÀI 8](#_Toc93564086)

[1.3 ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU 8](#_Toc93564087)

[Chương 2: CƠ SỞ LÝ THUYẾT 9](#_Toc93564088)

[2.1 GIỚI THIỆU VỀ PHẦN MỀM CISCO PACKET TRACER 9](#_Toc93564089)

[2.2 TỔNG QUAN VỀ VPN 10](#_Toc93564090)

[2.2.1 Khái niệm về VPN 10](#_Toc93564091)

[2.2.2 Ưu – nhược điểm của VPN 12](#_Toc93564092)

[2.3 GIAO THỨC VÀ ĐỊA CHỈ IP 12](#_Toc93564093)

[2.3.1 Giao thức 12](#_Toc93564094)

[2.3.2 Địa chỉ IP 13](#_Toc93564095)

[2.4 ĐỊNH TUYẾN 13](#_Toc93564096)

[2.4.1 Khái niệm 13](#_Toc93564097)

[2.4.2 Phân loại định tuyến 13](#_Toc93564098)

[Chương 3: NGHIÊN CỨU VỀ GRE VÀ IPSEC 16](#_Toc93564099)

[3.1 GRE 16](#_Toc93564100)

[3.2 IPSEC 16](#_Toc93564101)

[3.2.1 Khái niệm 16](#_Toc93564102)

[3.2.2 Chế độ làm việc của IPSec 16](#_Toc93564103)

[3.2.3 Giao thức bảo mật trong IPSec 17](#_Toc93564104)

[3.2.4 Các giai đoạn thực hiện IPSec VPN 18](#_Toc93564105)

[3.3 TẠI SAO PHẢI KẾT HỢP GRE VỚI IPSEC 19](#_Toc93564106)

[3.4 SO SÁNH GRE VÀ IPSEC 19](#_Toc93564107)

[Chương 4: TRIỂN KHAI VÀ DEMO TRÊN CISCO PACKET TRACER 21](#_Toc93564108)

[4.1 SƠ ĐỒ MẠNG TRIỂN KHAI 21](#_Toc93564109)

[4.2 CẤU HÌNH ĐỊA CHỈ IP 21](#_Toc93564110)

[4.3 KỊCH BẢN TRIỂN KHAI 22](#_Toc93564111)

[4.3.1 Cấu hình thông số trên Router R1 trụ sở Hà Nội 22](#_Toc93564112)

[4.3.2 Cấu hình thông số trên Router 2 26](#_Toc93564113)

[4.3.3 Cấu hình tham số trên Router 3 26](#_Toc93564114)

[4.3.4 Cấu hình tham số trên Router R4 27](#_Toc93564115)

[4.4 PHÂN TÍCH KẾT QUẢ 30](#_Toc93564116)

[4.4.1 Điều kiện để cấu hình được GRE kết hợp với IPSec VPN 30](#_Toc93564117)

[4.4.2 Kết quả đạt được 31](#_Toc93564118)

[Chương 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 38](#_Toc93564119)

[5.1 KẾT LUẬN 38](#_Toc93564120)

[5.2 HƯỚNG PHÁT TRIỂN 38](#_Toc93564121)

**DANH MỤC HÌNH ẢNH**

[Hình 2. 1 Cisco Packet Tracer 9](#_Toc93564278)

[Hình 2. 2 Mạng riêng ảo VPN 10](#_Toc93564279)

[Hình 3. 1 Transport mode 16](#_Toc93564285)

[Hình 3. 2 Tunnel mode 17](#_Toc93564286)

[Hình 4. 1 Sơ đồ triển khai 21](#_Toc93564380)

# **Chương 1: TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU**

* 1. **GIỚI THIỆU VỀ ĐỀ TÀI**

Dựa trên các kiến thức đã được học ở môn Mạng máy tính và môi trường giả lập mạng Cisco Packet Tracer từ đó xây dựng và nghiên cứu triển khai GRE kết hợp IPSec trong mạng VPN – demo trên Cisco Packet Tracer.

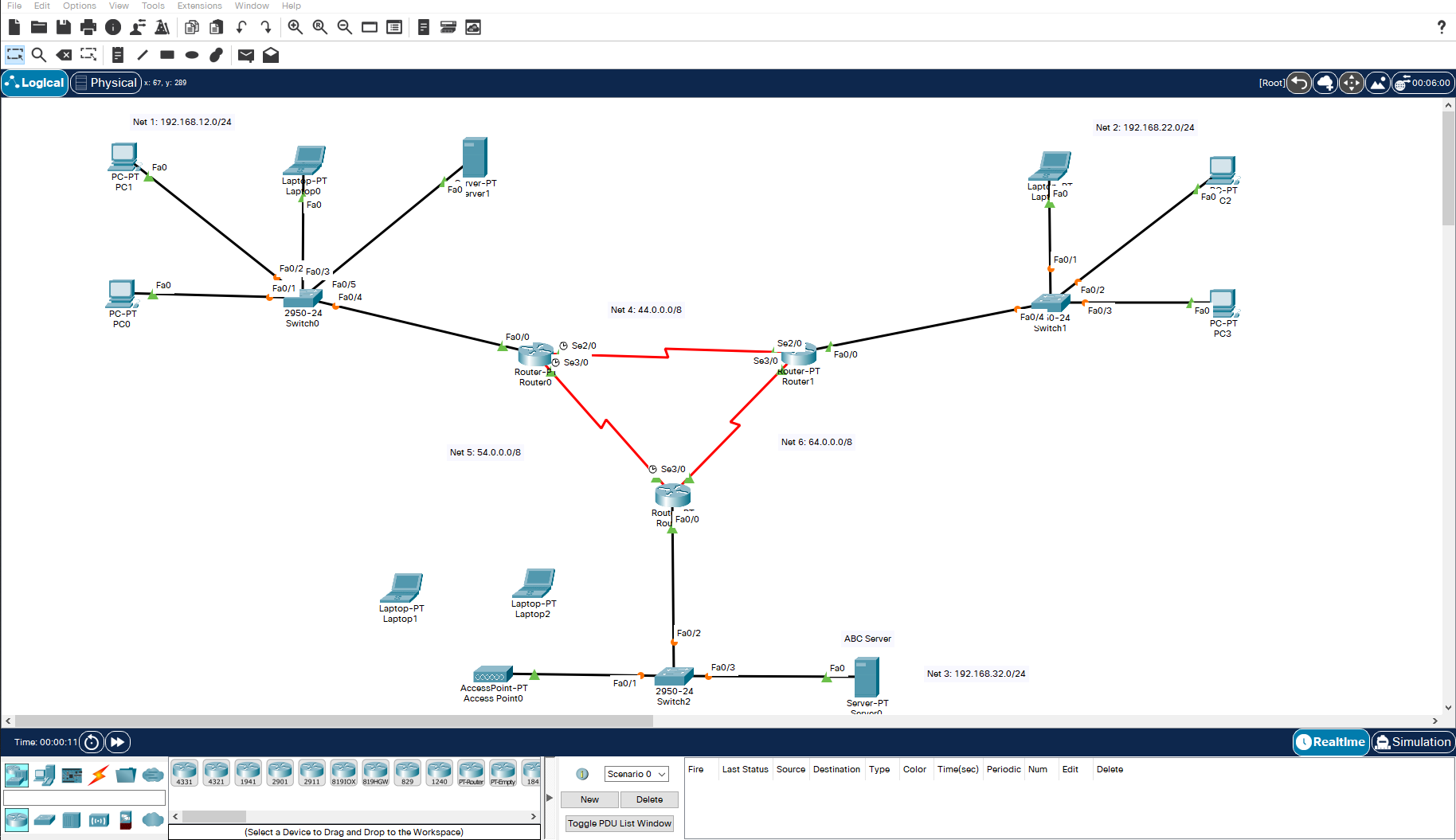
* 1. **MỤC TIÊU CỦA ĐỀ TÀI**
* **Mục tiêu chung:** Xây dựng và triển khai GRE kết hợp IPSec trong mạng VPN trên chương trình mô phỏng mạng Cisco Packet Tracer.
* **Mục tiêu cụ thể:**
* Tìm hiểu về VPN
* Tìm hiểu về GRE Tunnel
* Tìm hiểu về IPSec
* Triển khai GRE với IPSec trên Cisco Packet Tracer
  1. **ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU**
* **Đối tượng nghiên cứu:** VPN, GRE tunnel, IPSec VPN.
* **Phạm vi nghiên cứu:** Triển khai và cài đặt GRE kết hợp IPSec trên Cisco Packet Tracer.

# **Chương 2: CƠ SỞ LÝ THUYẾT**

* 1. **GIỚI THIỆU VỀ PHẦN MỀM CISCO PACKET TRACER**

Cisco Packet Tracer là một phần mềm mô phỏng hệ thống mạng sử dụng các thiết bị mạng của Cisco trên rất nhiều nền tảng được thiết kế bởi Cisco Systems, Inc. Công cụ này cho phép người dùng thiết kế và mô phỏng, giả lập hệ thống sơ đồ các mạng máy tính hiện đại.

Trong phần mềm này được thiết kế rất thân thiện với người dùng và dễ dàng sử dụng, người dùng chỉ cần kéo thả các thiết bị vào mô hình, cho phép thêm xóa và thiết kế sơ đồ mạng theo ý của mình tùy vào như cầu sử dụng của mỗi người. Ngoài ra, có thể cấu hình trực tiếp trên các thiết bị của Cisco, cũng như cho phép sử dụng mô phỏng trên giao diện dòng lệnh.



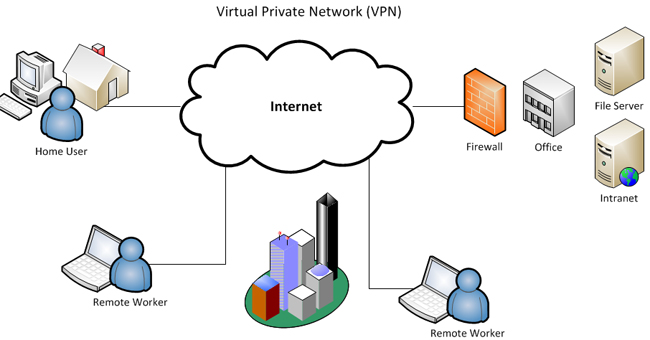
**Hình 2. 1 Cisco Packet Tracer**

* 1. **TỔNG QUAN VỀ VPN**

### **2.2.1 Khái niệm về VPN**

VPN (Virtual Private Network) hay còn gọi là mạng riêng ảo là một loại công nghệ thông qua mạng công cộng để xây dựng một mạng riêng biệt. Về cơ bản mỗi VPN là một mạng riêng rẽ sử dụng mạng chung (Internet) xây dựng một đường dây kết nối đặc biệt giữa các mạng riêng lẽ hay nhiều người sử dụng từ xa.

So với mạng riêng truyền thống, công nghệ VPN giúp giảm chi phí đáng kể. Nó thuận tiện và an toàn, trở thành công nghệ chính trong việc đạt được kết nối mạng an toàn xuyên khu vực.



**Hình 2. 2 Mạng riêng ảo VPN**

**Các dạng kết nối của VPN:**

* **Intranet VPN:** kết nối an toàn các mạng trụ sở chính và các chi nhánh từ xa qua một cơ sở hạ tầng mạng dùng chung như Internet thành một mạng riêng tư của một tập đoàn hay một tổ chức và gồm nhiều công ty và văn phòng làm việc, các kết nối này luôn luôn được mã hóa thông tin.
* **Remote Access VPN:** quyền truy cập từ xa của nhân viên kết nối đến các tài nguyên mạng của tổ chức, công ty để chia sẻ dữ liệu cũng như thực thi các ứng dụng nội bộ.
* **Extranet VPN:** là sự mở rộng từ những Intranet liên kết các khách hàng, những nhà cung cấp, những đối tác hay những nhân viên làm việc trong các Intranet qua cơ sở hạ tầng dùng chung chia sẻ những kết nối. Extranet cho phép truy nhập những tài nguyên mạng cần thiết kế của các đối tác kinh doanh, chẳng hạn như khách hang, nhà cung cấp, đối tác những người giữ vài trò quan trọng trong tổ chức.
* **Site-to-Site VPN:** Được áp dụng để cài đặt mạng từ một vị trí này kết nối tới mạng của một vị trí khác thông qua VPN. Site –to –Site VPN là sự kết nối hai mạng riêng lẻ thông qua một đường hầm bảo mật, đường hầm bảo mật này có thể sử dụng các giao thức PPTP, L2TP, hoặc IPSec, mục đích của Site-to-Site VPN là kết nối hại mạng không có đường nối lại với nhau, bất chấp khoảng cách vật lý.

**VPN chủ yếu áp dụng hai công nghệ: đường hầm (tunnel) và công nghệ bảo mật:**

* **Đường hầm:** Cung cấp các kết nối logic, vận chuyển các gói dữ liệu mã hoá bằng một đường hầm riêng biệt qua mạng IP, điều đó làm tăng tính bảo mật thông tin vì dữ liệu sau khi mã hoá sẽ lưu chuyển trong một đường hầm được thiết lập giữa người gửi và người nhận cho nên sẽ tránh được sự mất cắp, xem trộm thông tin, đường hầm chính là đặc tính ảo của VPN.
  + PPTP (Point-to-Point Tunneling Protocol)
  + L2TP (Layer 2 Tunneling Protocol): giao thức định đường hầm lớp 2
  + IPSec (IP Security)
* **Công nghệ bảo mật:** để đảm bảo tính bảo mật của quá trình truyền, một giao thức mã hóa an toàn được sử dụng để đảm bảo tính riêng tư và tính toàn vẹn của dữ liệu.

### **2.2.2 Ưu – nhược điểm của VPN**

* **Ưu điểm:** 
  + Tiết kiệm chi phí: chi phí thiết lập mạng VPN khá thấp do sử dụng chung hạ tầng mạng Internet.
  + Tính linh hoạt: khả năng tương thích với công nghệ băng thông rộng.
  + Tính bảo mật: VPN sử dụng các giao thức, thuật toán mã hóa, các phương pháp xác thực để bảo mật dữ liệu trong quá trình truyền tin.
* **Nhược điểm:**
  + VPN không có khả năng quản lý **Quality of Service (QoS)** qua môi trường Internet, do vậy các gói dữ liệu - Data package vẫn có nguy cơ bị thất lạc, rủi ro.
  1. **GIAO THỨC VÀ ĐỊA CHỈ IP**

### **2.3.1 Giao thức**

Giao thức được định nghĩa là các tập luật trên các ứng dụng, hoặc phần cứng giữa các thiết bị, các phần mềm với nhau hoặc phần mềm với phần cứng.

Các giao thức đều có điểm riêng của nó như: (tính năng) Function, (định dạng) Format, (tập luật) Rules.

* **Các loại hình giao thức:**
  + Giao tiếp (Network Communications): cho phép việc kết nối hai hay nhiều “thành phần” thông qua một hay nhiều mạng khác nhau.
  + Bảo mật (Network Security): đảm bảo an toàn cho dữ liệu, cung cấp các xác thực, sự toàn vẹn dữ liệu, mã hóa dữ liệu.
  + Định tuyến (Routing): các giải thuật giúp tìm đường đi tốt nhất cho gói tin trong hệ thống các mạng với nhau.
  + Xác định dịch vụ (Service Discovery): dùng cho việc nhận diện các thiết bị hoặc dịch vụ một cách tự động.

### **2.3.2 Địa chỉ IP**

Địa chỉ IP (Internet Protocol) là địa chỉ hoạt động ở layer 3 trong mô hình TCP/IP để xác định và nhận diện các thiết bị trong hệ thống mạng và là địa chỉ duy nhất, không trùng lắp với địa chỉ IP khác. Bản chất là một số nhị phân dài 32 bit biểu diễn thành bốn octet cách nhau bởi dấu chấm, mỗi octet có giá trị từ 0 đến 255.

**Địa chỉ IP bao gồm phần mạng và phần host:**

* Hai máy ở mạng khác nhau thì phần mạng khác nhau.
* Hai máy ở cùng mạng thì phần mạng giống nhau, phần host khác nhau.

Địa chỉ IP đầu tiên và IP cuối cùng của một mạng là địa chỉ đặc biệt.

* **Các loại địa chỉ IP:**
  + IP loopback (127.0.0.1): dùng để kiểm tra chức năng mạng của một máy có hoạt động không.
  + IP public: dùng để giao tiếp trong môi trường Internet.
  + IP private: dùng trong nội bộ và có thể tái sử dụng, không dùng trên môi trường Internet.
    - Dải IP private:
      * Lớp A: 10.0.0.0 -> 10.255.255.255
      * Lớp B: 172.16.0.0 -> 172.31.255.255
      * Lớp C:192.168.0.0 -> 192.168.255.255
    - Ngoại trừ dải địa chỉ này và IP loopback, còn lại là IP private.
  1. **ĐỊNH TUYẾN**

### **2.4.1 Khái niệm**

Định tuyến (Routing) là quá trình tìm kiếm, xác định và tìm đường đi tốt nhất đi từ một thiết bị tới một lớp mạng nào đó trong mạng máy tính để gói tin tới được đích thông qua các thiết bị định tuyến.

### **2.4.2 Phân loại định tuyến**

* **Định tuyến tĩnh (Static Route):** người quản trị sẽ khai báo thông tin định tuyến cho thiết bị định tuyến một cách thủ công.
  + Ưu điểm: dễ triển khai và cấu hình, bảo mật cao, sử dụng ít băng thông và không tốn tài nguyên .
  + Nhược điểm: không có khả năng tự cập nhật, phải cấu hình lại khi có sự thay đổi, khả năng mở rộng kém.
  + Trường hợp sử dụng định tuyến tĩnh:
    - Đường truyền có băng thông thấp
    - Người quản trị cần kiểm soát các kết nối trong hệ thống
    - Hệ thống có các tuyến kết nối ít
    - Kết nối dùng định tuyến tĩnh là kết nối dự phòng cho các kết nối dùng định tuyến động.
  + Phương thức triển khai định tuyến tĩnh:
    - Next hop: thông tin sẽ chuyển đến router kế tiếp nào trước khi đến đích
    - Exit interface: thông tin sẽ được đưa ra cổng nào trước khi đến đích.
* **Định tuyến động (Dynamic Route):** tự động chia sẻ, trao đổi thông tin giữa các thiết bị định tuyến dựa trên các giao thức định tuyến động.
  + Ưu điểm: tự động cập nhật thông tin bảng định tuyến nếu có sự thay đổi, tính toán và đưa ra đường đi chuyển thông tin tốt nhất.
  + Nhược điểm: sử dụng tài nguyên, tiêu tốn một phần băng thông mạng để xây dựng bảng định tuyến.
  + Mục đích của định tuyến động:
    - Khám phá mạng từ xa
    - Duy trì việc cập nhật thông tin định tuyến
    - Tính toán và chọn đường đi tốt nhất
    - Nếu tuyến đường chuyển thông tin bị lỗi, tự tính toán và đưa ra tuyến đường chuyển thông tin backup
  + Phân loại định tuyến động:
    - Exterior Gateway Protocols: có giao thức BGP
    - Interior Gateway Protocols: Distance Vector Protocols và Link-State Protocols
      * Giao thức Distance có giao thức: RIPv1, RIPv2 và IGRP, EIGRP
      * Giao thức Link-State có giao thức: OSPF và IS-IS

# **Chương 3: NGHIÊN CỨU VỀ GRE VÀ IPSEC**

## **3.1 GRE**

GRE (Generic Routing Encapsulation) là một loại giao thức cho phép đóng gói nhiều loại giao thức lớp Network sử dụng thiết lập kết nối Point-to-Point. Với GRE được cấu hình một đường hầm ảo được thiết lập giữa 2 đầu thiết bị router cho phép 2 bên chia sẽ dữ liệu với nhau thông qua GRE tunnel.

Tuy nhiên, bản thân GRE tunnel không hỗ trợ mã hóa dữ liệu, cần phải kết hợp với giao thức khác để thực hiện truyền mã hóa dữ liệu, chẳng hạn như IPSec.

GRE tunnel được xác định bởi IP nguồn (Source IP) và IP đích (Destination IP) ở cả hai đầu đường hầm và nó có hỗ trợ bởi các giao thức định tuyến khác nhau như RIP, OSPF,...

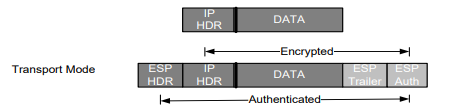
## **3.2 IPSEC**

### **3.2.1 Khái niệm**

IPSec (Internet Protocol Security) thực chất không phải là một giao thức đơn lẻ, IPSec là một Framework chạy ở lớp Network (layer 3) gồm tập hợp các giao thức cung cấp tính xác thực và toàn vẹn dữ liệu, bảo mật IP trong lớp mạng. Nó bọc các gói tin IP trong một lớp mã hóa và xác thực giúp bảo vệ tính bí mật và tính toàn vẹn của dữ liệu, xác định các nguồn dữ liệu và ngăn chặn việc truyền lại.

### **3.2.2 Chế độ làm việc của IPSec**

* **Chế độ chuyển vận (Transport mode)**: Trong chế độ Transport, IP header gốc vẫn còn và không được mã hóa. Chỉ có payload và ESP trailer được mã hóa.

****

**Hình 3. 1 Transport mode**

* **Chế độ đường hầm (Tunnel mode)**: Trong chế độ Tunnel, toàn bộ gói tin được bảo vệ. IPSec gói gói dữ liệu trong một packet mới, mã hóa nó và thêm một IP header mới.

****

**Hình 3. 2 Tunnel mode**

### **3.2.3 Giao thức bảo mật trong IPSec**

* **Giao thức đóng gói an toàn ESP (Encapsulation Security Payload)**

ESP là một giao thức bảo mật cung cấp tính xác thực và bảo mật của gói dữ liệu khỏi sự dòm ngó không được cho phép. ESP mã hóa các gói dữ liệu, xác thực dữ liệu và nguồn gốc của nó trong IPSec.

ESP là giao thức hỗ trợ và kiểu mã hoá đối xứng như: Blowfish, DES. Thuật toán mã hoá dữ liệu mặc định sử dụng trong IPSec là thuật toán DES 56 bit. Trong các sản phẩm và thiết bị mạng của Cisco dùng trong VPN còn sử dụng việc mã hoá dữ liệu tôt hơn bằng cách sử dụng thuật toán 3DES( Triple Data Encryption Security ) 128 bit.

* **Giao thức chứng thực mục đầu AH (Authentication Header)**

Đảm bảo tính toàn vẹn của gói dữ liệu chắc chắn gói tin sẽ không bị thay đổi trong quá trình gửi. Nhưng ở AH gói tin sẽ không được mã hóa và có thể bị nghe lén và đọc được. Nếu cần thêm tính bí mật có thể sử dụng ESP.

* **Giao thức trao đổi chìa khóa Internet Key Exchange (IKE)**

Là giao thức thực hiện quá trình trao đổi khóa và thỏa thuận các thông số bảo mật với nhau, khi trao đổi xong sẽ có một “thỏa thuận” giữa hai đầu kết nối, khi đó IPSec SA (Security Association) sẽ được tạo ra. SA là những thông số bảo mật sau khi đã thỏa thuận xong, các thông số SA này sẽ được lưu trong cơ sở dữ liệu của SA.

Giao thức IKE dựa trên các giao thức bảo mật như Internet Security Association and Key Management Protocol (ISAKMP) và giao thức phân phối khóa Oakley.

* + **Giao thức IKE có các đặc tính sau:**
    - Các chìa khóa phát sinh và thủ tục nhận biết.
    - Tự động làm mới chìa khóa.
    - Giải quyết vấn đề một khóa.
    - Mỗi một giao thức an toàn (AH, ESP) có cách bảo mật khác nhau
    - Gắn sẵn sự bảo vệ.
    - Chống lại các cuộc tấn công làm nghẽn mạch tài nguyên như: tấn công từ chối dịch vụ DoS (Denial-of-Service).
    - Sử dụng chữ ký số.
    - Dùng chung khóa.
  + **Giao thức IKE cung cấp 5 khả năng:**
    - Cung cấp những phương tiện cho hai bên về sự đồng ý những giao thức, thuật toán và những chìa khoá để sử dụng.
    - Đảm bảo trao đổi khoá đến đúng người dùng.
    - Quản lý những chìa khoá sau khi được chấp nhận.
    - Đảm bảo rằng sự điều khiển và trao đổi khoá an toàn.
    - Cho phép sự chứng thực động giữa các đối tượng ngang hàng.

### **3.2.4 Các giai đoạn thực hiện IPSec VPN**

Việc thực hiện IPSec VPN chủ yếu bao gồm hai giai đoạn:

* **Giai đoạn 1 (Phase 1):** Thiết lập các kết nối điều khiển và xây dựng một đường hầm an toàn ở hai đầu gồm:
  + Phương thức xác thực
  + Thuật toán mã hóa
  + Diffie-Hellman Group: key mã hóa
  + Giải thuật hàm băm
* **Giai đoạn 2 (Phase 2):** thiết lập các tham số, phương thức bảo mật để truyền dữ liệu
  + Sử dụng giao thức bảo mật ESP hoặc AH
  + Thuật toán mã hóa
  + Giải thuật hàm băm

## **3.3 TẠI SAO PHẢI KẾT HỢP GRE VỚI IPSEC**

Hiện nay, các vấn đề về an ninh mạng đang là một vấn đề rất nhức nhối ngày nay, VPN (mạng riêng ảo) là một giải pháp tối ưu cung cấp các giải pháp truy cập từ xa cho các tổ chức và doanh nghiệp trong việc kết nối và truyền tải thông tin.

Tại sao phải kết hợp GRE với IPSEC ?

* Thứ nhất GRE: ở giao thức GRE các gói tin sẽ được bọc trong một đường hầm. Nhưng vấn đề là các gói tin này sẽ không được hỗ trợ mã hóa. Dẫn đến sự bảo mật không được đảm bảo, có thể bị nghe lén và bị đánh cắp dữ liệu.
* Thứ hai IPSEC: ở IPSEC cung cấp rất nhiều các giao thức bảo mật cũng như các gói tin truyền đi luôn được đảm bảo về bảo mật và toàn vẹn thông tin. Bên cạnh đó IPSEC cũng có nhược điểm là không hỗ trợ mã hóa các gói tin multicast và broadcast.

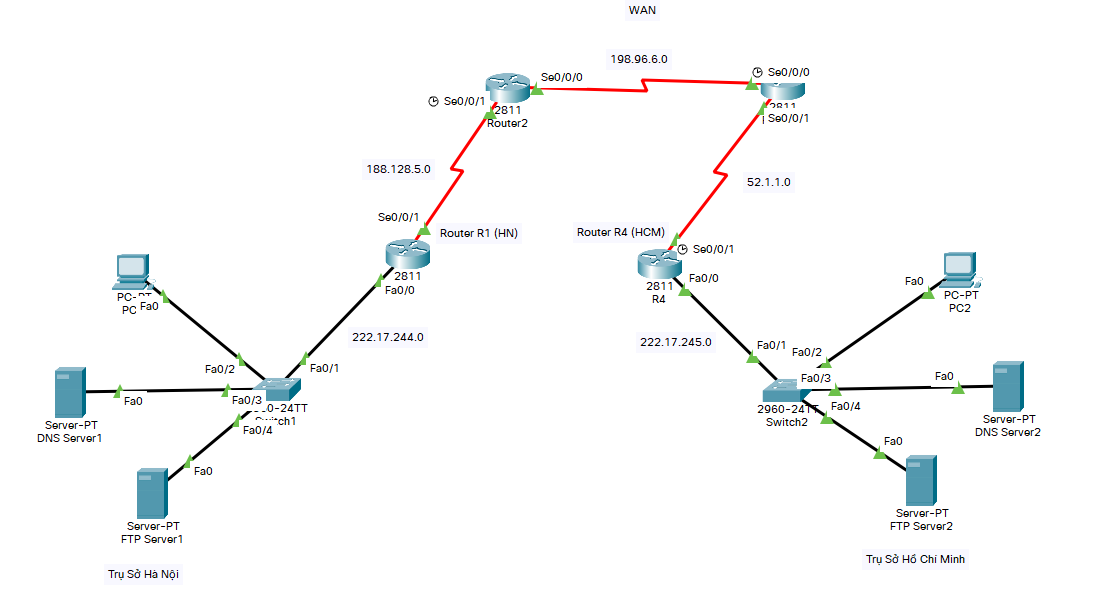
Vì thế, nếu kết hợp GRE với IPSEC thì các dữ liệu truyền đi sẽ được mã hóa an toàn, bảo mật dữ liệu sẽ được đảm bảo và vấn đề mở rộng mạng VPN sẽ được giải quyết.

## **3.4 SO SÁNH GRE VÀ IPSEC**

* **Giống nhau:** đều chia phép chia sẻ dữ liệu giữa các trụ sở của công ty, tổ chức với nhau thông qua đường hầm mạng riêng ảo trên Internet.
* **Khác nhau:**
  + **GRE:** là một giao thức đường hầm cho phép truyền dữ liệu trong nó, nó không có trạng thái và không có cơ chế kiểm soát dòng chảy. Các gói tin chạy trong đường hầm GRE sẽ gặp rủi ro rất nhiều vì GRE cung cấp bảo mật ít hơn. Nhưng ở GRE có hỗ trợ mang các giao thức định tuyến khác cũng như các gói IP trong mạng IP trong khi IPSec không thể
  + **IPSec:** được sử dụng để bảo vệ dữ liệu được chia sẻ giữa hai đầu, IPSec cho phép hai bên thiết lập xác thực lẫn nhau và thỏa thuận các khóa mật mã được sử dụng. Nó có các phương thức bảo mật và toàn vẹn thông tin như: Header xác thực (AH) bảo vệ chống lại các cuộc tấn công phát lại, Encapsulation Security Payloads (ESP) cung cấp bảo mật và Hiệp hội bảo mật (SA) cung cấp dữ liệu cho các hoạt động AH và ESP.

# **Chương 4: TRIỂN KHAI VÀ DEMO TRÊN CISCO PACKET TRACER**

## **4.1 SƠ ĐỒ MẠNG TRIỂN KHAI**



**Hình 4. 1 Sơ đồ triển khai**

Sơ đồ mạng triển khai trên **Hình 4.1** được thiết lập theo mô hình Site-to-Site VPN. Sỡ dĩ sơ đồ được thiết lập theo mô hình Site-to-Site bởi vì có một mạng riêng là trụ sở Hà Nội và một mạng riêng là trụ sở Hồ Chí Minh, 2 mạng riêng này kết nối với nhau để trao đổi dữ liệu, mô hình này gọi lại Site-to-Site – kết nối các chi nhánh hay các trụ sở với nhau thông qua 2 site là 2 router.

## **4.2 CẤU HÌNH ĐỊA CHỈ IP**

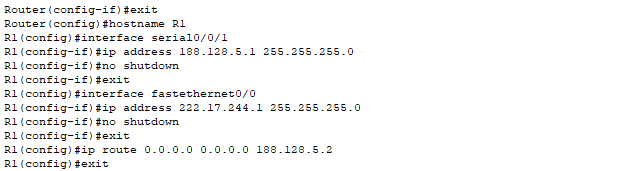
Các địa chỉ ở trụ sở Hà Nội được đặt là 222.17.244.0/24, đối với trụ sở ở Hồ Chí Minh là 222.17.245.0/24. Địa chỉ được đặt ở phân đoạn trụ sở Hà Nội và Internet là 188.128.5.0/24 và phân đoạn trụ sở Hồ Chí Minh và Internet là 52.1.1.0/24. Mạng giữa 2 router định tuyến mạng bên ngoài là 198.96.6.0/24.

* **Cấu hình IP cho trụ sở ở Hà Nội:**
  + Địa chỉ IP của PC1 được đặt là 222.17.244.2, subnet mask của PC1 là 255.255.255.0, địa chỉ gateway là 222.17.244.1.
  + Địa chỉ IP của DNS Server1 được đặt là 222.17.244.3, subnet mask của DNS Server1 là 255.255.255.0, địa chỉ gateway là 222.17.244.1.
  + Địa chỉ IP của FTP Server1 được đặt là 222.17.244.4, subnet mask của DNS Server1 là 255.255.255.0, địa chỉ gateway là 222.17.244.1.
* **Cấu hình IP cho trụ sở ở Hồ Chí Minh:**
  + Địa chỉ IP của PC2 được đặt là 222.17.245.2, subnet mask của PC1 là 255.255.255.0, địa chỉ gateway là 222.17.245.1.
  + Địa chỉ IP của DNS Server2 được đặt là 222.17.245.3, subnet mask của DNS Server1 là 255.255.255.0, địa chỉ gateway là 222.17.245.1.
  + Địa chỉ IP của FTP Server2 được đặt là 222.17.245.4, subnet mask của DNS Server1 là 255.255.255.0, địa chỉ gateway là 222.17.245.1.

## **4.3 KỊCH BẢN TRIỂN KHAI**

### **4.3.1 Cấu hình thông số trên Router R1 trụ sở Hà Nội**

* **Cấu hình địa chỉ IP**



Router(config)#hostname R1

R1(config)#interface serial0/0/1

R1(config-if)#ip address 188.128.5.1 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface fastethernet0/0

R1(config-if)#ip address 222.17.244.1 255.255.255.0

R1(config-if)#no shutdown

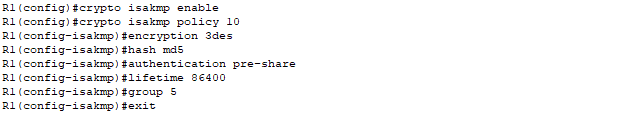
R1(config-if)#exit

R1(config)#ip route 0.0.0.0 0.0.0.0 188.128.5.2

R1(config)#exit

Ở bước này ta sẽ thiết lập địa chỉ IP và subnet mask cho từng cổng interface và thiết lập định tuyến tĩnh cho Router R1.

* **Tạo những chính sách IKE**

****

R1(config)#crypto isakmp enable

R1(config)#crypto isakmp policy 10

R1(config-isakmp)#encryption 3des

R1(config-isakmp)#hash md5

R1(config-isakmp)#authentication pre-share

R1(config-isakmp)#lifetime 86400

R1(config-isakmp)#group 5

R1(config-isakmp)#exit

Tiếp theo để tạo ra một chính sách IKE (thiết lập Phase 1), đầu tiên ta sẽ nhận dạng policy tạo ra (ứng với mỗi policy thì duy nhất và được nhận biết bởi số ưu tiên gán vào), ở đây được cấu hình là **policy 10**. Tiếp đến là chỉ rõ thuật toán mã hóa là 3des, hàm băm md5, phương thức xác thực là pre-share keys, thời gian tồn tại là 86400s, và cuối cùng là Diffie-Hellman được chọn là group 5.

* **Cấu hình khóa dùng chung và tạo ACL (Access-list)**



R1(config)#crypto isakmp key 123456 address 52.1.1.2

R1(config)#access-list 110 permit ip 222.17.244.0 0.0.0.255 222.17.245.0 0.0.0.255

Vì ban đầu ta sử dụng phương thức xác thực là pre-share key nên ở bước này ta sẽ khai báo key là 123456 và trỏ về địa chỉ 52.1.1.2, chỉ chấp nhận xây dựng đường hầm với router có địa chỉ là 52.1.1.2.

Tiếp theo, tạo access-list với tên là 110. Những địa chỉ thuộc lớp địa chỉ từ 222.17.244.0 và 222.17.245.0 sẽ được cho phép qua đường hầm.

* **Định nghĩa những tập hợp biến đổi và cấu hình tham số IPSec**



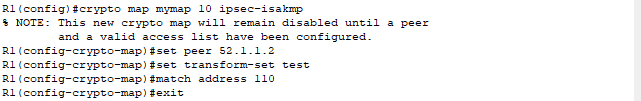
R1(config)#crypto ipsec transform-set test esp-3des esp-md5-hmac

Ở bước này ta sẽ thiết lập tham số IPSec (Phase 2) với transform-set tên là test, thuật toán mã hóa là esp-3des và thuật toán đảm bảo tính toàn vẹn là esp-md5-hmac. Sau khi cấu hình xong tham số đường hầm phase 2, ta sẽ thiết lập chế độ cho IPSec:

R1(cfg-crypto-trans)#mode tunnel

R1(cfg-crypto-trans)#exit

* **Cấu hình Crypto Map**

****

R1(config)#crypto map mymap 10 ipsec-isakmp

R1(config-crypto-map)#set peer 52.1.1.2

R1(config-crypto-map)#set transform-set test

R1(config-crypto-map)#match address 110

R1(config-crypto-map)#exit

Tạo 1 crypto map tên là mymap bao gồm các thông số. Mục đích của crypto map là sẽ tổng hợp lại các thông số đã cấu hình trước đó. Khi có gói tin ra khỏi cổng interface serial0/0/1 thì nó sẽ tra cứu crypto map, đầu tiên sẽ match tới địa chỉ 110 nếu gói tin khớp với dòng lệnh match này nó sẽ đi vào đường hầm kết nối với địa chỉ 52.1.1.2, gói tin sẽ được bảo về bởi transform-set test (bao gồm các thuật toán mã hóa và bảo toàn).

* **Áp dụng Crypto Map vào interface**



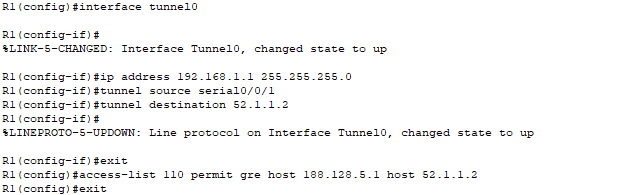
R1(config)#interface serial0/0/1

R1(config-if)#crypto map mymap

R1(config-if)#exit

Bước này ta sẽ áp dụng crypto map vào cổng interface serial0/0/1

* **Cấu hình đường hầm GRE**

****

R1(config)#interface tunnel0

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#tunnel source serial0/0/1

R1(config-if)#tunnel destination 52.1.1.2

R1(config-if)#exit

R1(config)#access-list 110 permit gre host 188.128.5.1 host 52.1.1.2

R1(config)#exit

Tiếp theo, chỉ rõ một tunnel interface number đưa vào chế độ cấu hình interface, và cấu hình địa chỉ IP và subnet mask cho tunnel interface. Với điểm đầu đường hầm là cổng serial0/0/1 và điểm cuối là trỏ về địa chỉ 52.1.1.2.

### **4.3.2 Cấu hình thông số trên Router 2**

Route2(config)#hostname R2

R2(config)#interface serial0/0/0

R2(config-if)#ip add 198.96.6.1 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface serial0/0/1

R2(config-if)#ip add 188.128.5.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#ip route 52.1.1.0 255.255.255.0 198.96.6.2

### **4.3.3 Cấu hình tham số trên Router 3**

R3(config)# interface serial0/0/0

R3(config-if)#ip add 198.96.6.2 255.255.255.0

R3(config-if)#no shut

R3(config-if)#exit

R3(config)# interface serial0/0/1

R3(config-if)#ip add 52.1.1.1 255.255.255.0

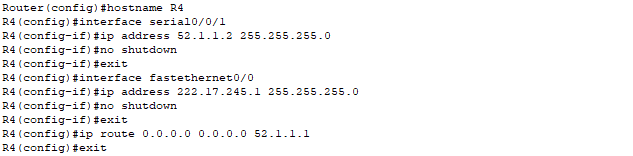
R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#ip route 188.128.5.0 255.255.255.0 198.96.6.1

### **4.3.4 Cấu hình tham số trên Router R4 trụ sở Hồ Chí Minh**

* **Cấu hình địa chỉ IP**



R4(config)#interface serial0/0/1

R4(config-if)#ip address 52.1.1.2 255.255.255.0

R4(config-if)#no shutdown

R4(config-if)#exit

R4(config)#interface fastethernet0/0

R4(config-if)#ip address 222.17.245.1 255.255.255.0

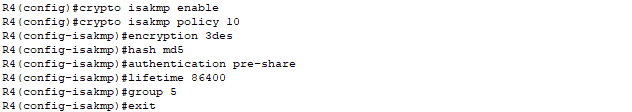
R4(config-if)#no shutdown

R4(config-if)#exit

R4(config)#ip route 0.0.0.0 0.0.0.0 52.1.1.1

Đầu tiên ta sẽ thiết lập địa chỉ IP và subnet mask cho từng cổng interface và tiến hành định tuyến tĩnh cho Router R4

* **Tạo những chính sách IKE**

****

R4(config)#crypto isakmp enable

R4(config)#crypto isakmp policy 10

R4(config-isakmp)#encryption 3des

R4(config-isakmp)#hash md5

R4(config-isakmp)#authentication pre-share

R4(config-isakmp)#lifetime 86400

R4(config-isakmp)#group 5

Tương tự với Router R1 vì ta sẽ tạo kết nối giữa hai Router nên cũng sẽ phải thiết lập các thông số giống nhau để đảm bảo tính thống nhất với policy 10, thuật toán mã hóa là 3des, hàm băm md5, phương thức xác thực là pre-share keys, và Diffie-Hellman được chọn là group 5.

* **Cấu hình khóa dùng chung và tạo ACL**



R4(config)#crypto isakmp key 123456 address 188.128.5.1

R4(config)#access-list 110 permit ip 222.17.245.0 0.0.0.255 222.17.244.0 0.0.0.255

Tiếp theo sẽ tạo key xác thực và trỏ về địa chỉ 188.128.5.1 cho phép chỉ tạo đường hầm với địa chỉ là 188.128.5.1

Tạo access-list với tên là 110. Những địa chỉ thuộc lớp địa chỉ từ 222.17.245.0 và 222.17.244.0 sẽ được cho phép qua đường hầm.

* **Định nghĩa những tập hợp biến đổi và cấu hình tham số IPSec**



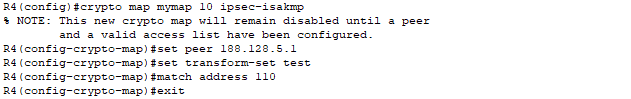
R4(config)#crypto ipsec transform-set test esp-3des esp-md5-hmac

Ở bước này ta sẽ thiết lập tham số IPSec (Phase 2) với transform-set tên là test, thuật toán mã hóa là esp-3des và thuật toán đảm bảo tính toàn vẹn là esp-md5-hmac. Tiếp theo, tương tự như Router R1 ta cũng sẽ cấu hình chế độ cho IPSec:

R1(cfg-crypto-trans)#mode tunnel

R1(cfg-crypto-trans)#exit

* **Cấu hình Crypto Map**



R4(config)#crypto map mymap 10 ipsec-isakmp

R4(config-crypto-map)#set peer 188.128.5.1

R4(config-crypto-map)#set transform-set test

R4(config-crypto-map)#match address 110

Tạo 1 crypto map để thống nhất các thông số đã thiết lập. Khi có địa chỉ ra khỏi cổng interface serial0/0/1 sẽ tiến hành match tới địa chỉ 110, nếu được phép sẽ được đi qua đường hầm tới địa chỉ 188.128.5.1 và sẽ được bảo vệ bởi transform-set test gồm các thuật toán mã hóa và toàn vẹn dữ liệu.

* **Áp dụng Crypto Map vào interface**



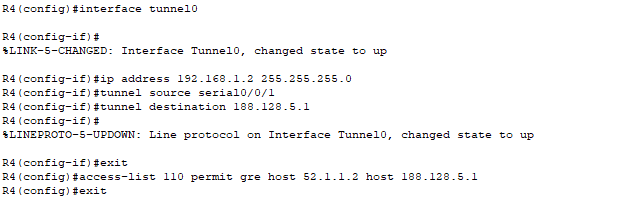
R4(config)#interface serial0/0/1

R4(config-if)#crypto map mymap

R4(config-if)#exit

Sau khi thiết lập xong crypto map mymap thì ta sẽ áp dụng vào cổng interface serial0/0/1.

* **Cấu hình đường hầm GRE**



R4(config-if)#ip add 192.168.1.2 255.255.255.0

R4(config-if)#tunnel source serial0/0/1

R4(config-if)#tunnel destination 188.128.5.1

R4(config-if)#exit

R4(config)#access-list 110 permit gre host 52.1.1.2 host 188.128.5.1

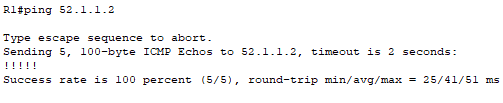
Tiếp theo, Chỉ rõ một tunnel interface number đưa vào chế độ cấu hình interface, và cấu hình địa chỉ IP và subnet mask cho tunnel interface. Với điểm đầu đường hầm là cổng serial0/0/1 và điểm cuối là trỏ về địa chỉ 188.128.5.1.

## **4.4 PHÂN TÍCH KẾT QUẢ**

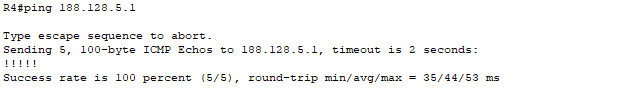
### **4.4.1 Điều kiện để cấu hình được GRE kết hợp với IPSec VPN**

Để có thể tiến hành cấu hình được GRE kết hợp IPSec VPN thì trước hết ta cần phải cấu hình đầy đủ địa chỉ giữa các cổng interface của các Router. Sau đó ta tiến hành định tuyến tĩnh giữa các Router, có thể sử dụng câu lệnh ping để kiểm tra sau khi thiết lập giữa 2 Router cần tiến hành cấu hình GRE kết hợp IPSec. Đây là điểu kiện để có thể cấu hình thành công.

* Router R1 trụ sở Hà Nội



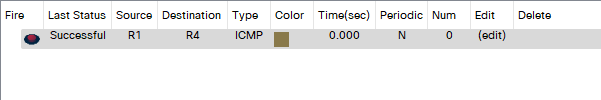
* Router R4 trụ sở Hồ Chí Minh



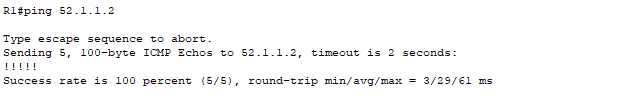
### **4.4.2 Kết quả đạt được**

* **Kiểm tra kết quả sau khi cấu hình**

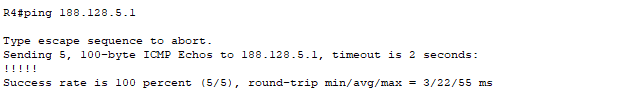
Sau khi cấu hình các thông số IPSec và GRE thì tại mỗi Router ta có gửi các gói tin qua lại với nhau tại Router R1 và Router R4 giữa trụ sở Hà Nội và Hồ Chí Minh hoặc cũng có thể sử dụng lại câu lệnh ping để kiểm tra.



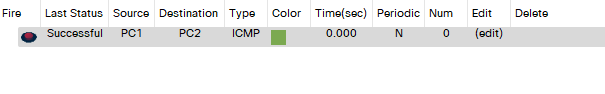
Router R1 trụ sở ở Hà Nội



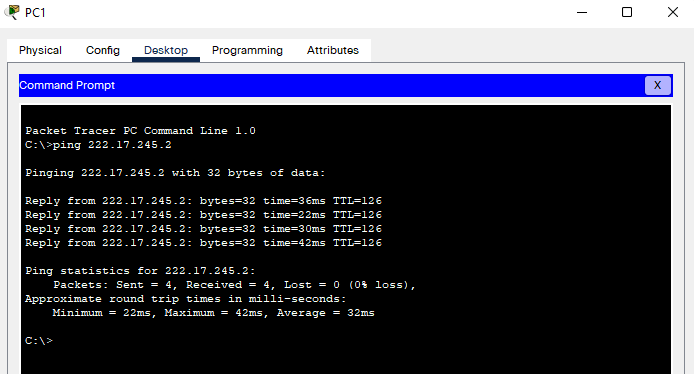
Router R2 trụ sở ở Hồ Chí Minh



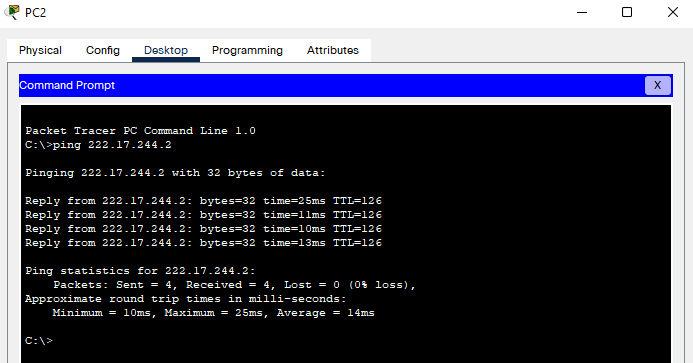
Ngoài ra từ PC1 ở trụ sở Hà Nội cũng có thể gửi tin thành công qua PC2 ở trụ sở Hồ Chí Minh và 2 máy có thể ping thông với nhau. Từ mỗi PC ta sẽ tiến hành ping thông lẫn nhau để kiểm tra



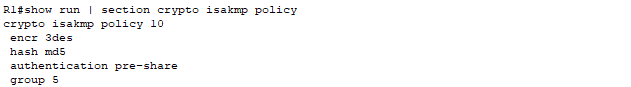
PC1 ở trụ sở Hà Nội



PC2 ở trụ sở Hồ Chí Minh



* **Kiểm tra các thông số đã cấu hình**
  + Sử dụng lệnh show run | section crypto isakmp policy để kiểm tra những chính sách IKE (Phase 1)



* + Sử dụng lệnh show run | i crypto isakmp key để kiểm tra khóa được thiết lập



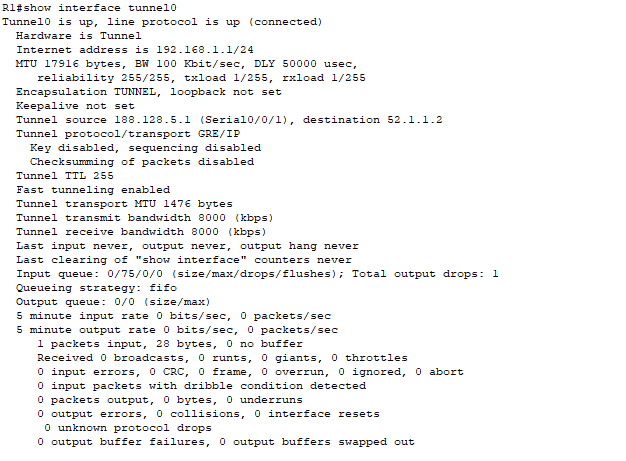
* + Sử dụng lệnh show run | section crypto ipsec để kiểm tra tham số cấu hình IPSec (Phase 2)



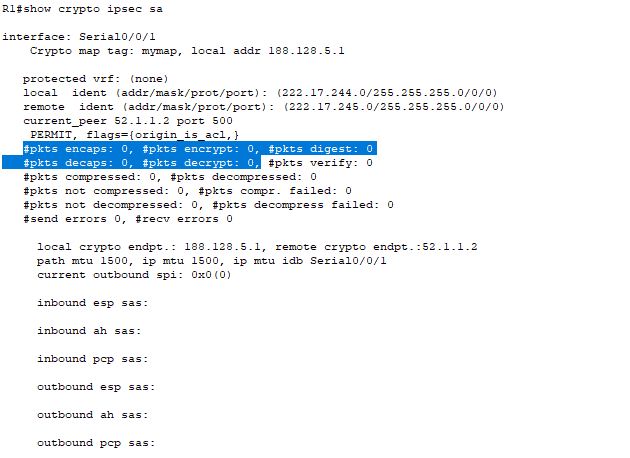
* + Sử dụng lệnh show run | section crypto map



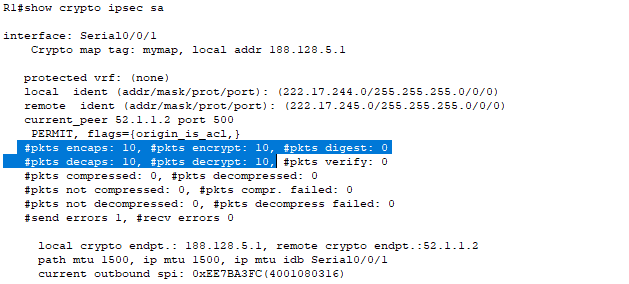
* + Sử dụng lệnh show interface tunnel0 để kiểm tra các thông số đường hầm



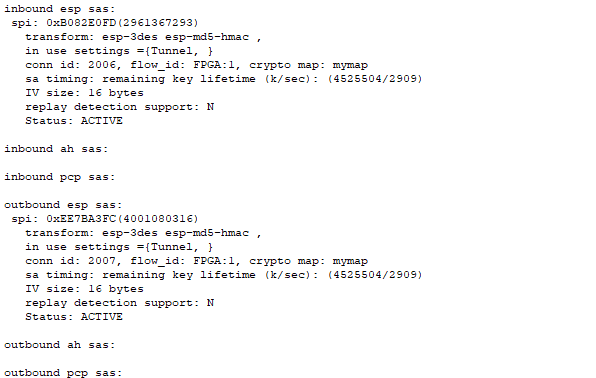
* **Kiểm tra lưu lượng các gói tin đi qua đường hầm**
  + Sử dụng câu lệnh show crypto ipsec sa để kiểm tra lưu lượng các gói tin cũng như các thông số đã thiết lập

****

* + - Sau khi chưa ping thông hay chưa gửi các gói tin thì ta có thể thấy các gói tin được mã hóa và giải mã là 0 cũng như các lưu lượng thông tin gói tin cũng chưa hiển thị.



* + - Tiến hành ping từ PC1 trụ sở Hà Nội tới PC2 trụ sở Hồ Chí Minh, ta có thể thấy sau khi ping thì gói tin mã hóa tăng lên là 10 và gói tin mã hóa là 10.



* + - Ngoài ra, ta cũng có thể xem những thông số khác như các gói tin sẽ được mã hóa bởi transform: esp-3des esp-md5-hmac, chế độ làm việc của IPSec được sử dụng là Tunnel và các thông số khác.
  + Chế độ làm việc trong IPSec mặc định tự động được cấu hình theo chế độ Tunnel nếu trước đó ta không cấu hình. Để cấu hình chế độ, sau khi ta thiết lập các tham số IPSec (Phase 2) ta sử dụng câu lệnh:

R1(config)#crypto ipsec transform-set test esp-3des esp-md5-hmac

R1(cfg-crypto-trans)#mode tunnel

R1(cfg-crypto-trans)#exit

# **Chương 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

## **5.1 KẾT LUẬN**

VPN là một công nghệ rất phổ biến hiện nay, nó cung cấp kết nối an toàn và đảm bảo về bảo mật hiệu quả cho các doanh nghiệp và công ty truy cập từ bên ngoài vào nội bộ thông qua mạng Internet. Mặc dù sử dụng hạ tầng chung nhưng ta vẫn đảm bảo được sự bảo mật của dữ liệu cũng như tính toàn vẹn trong bối cảnh sự nổi lên ngày càng nhiều của vấn đề về an ninh mạng.

Trong bài thực tập cơ sở này, em đã giới thiệu giải pháp công nghệ cho việc xây dựng một mạng riêng ảo an toàn là GRE kết hợp IPSec VPN. Triển khai từ lý thuyết đến thực tiễn trong các vấn đề mạng riêng ảo nói chung, mô hình mạng thiết lập và ứng dụng triển khai trên Cisco Packet Tracer.

Bên cạnh kết quả đạt được, chắc chắn em vẫn không thể tránh khỏi các thiếu sót. Em rất mong nhận được sự thông cảm từ các thầy cô.

## **5.2 HƯỚNG PHÁT TRIỂN**

Đối với đề tài thực tập của em thì em chỉ dừng lại ở cấu hình IPSec VPN ở mức Site-to-Site dùng để kết nối hai mạng LAN với nhau, điển hình là hai chi nhánh, văn phòng,... cho phép truyền dữ liệu an toàn ở hai site (hai đầu đường hầm là 2 router).

Ngoài cấu hình IPSec VPN site-to-site, em sẽ nghiên cứu thêm về thiết lập kết nối Client-to-Site là một công nghệ cho phép người dùng có thể sử dụng laptop, máy tính cá nhân để kết nối tới trụ sở của công ty hoặc danh nghiệp.