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 – 01/2021

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 – 01/2021

**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 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.

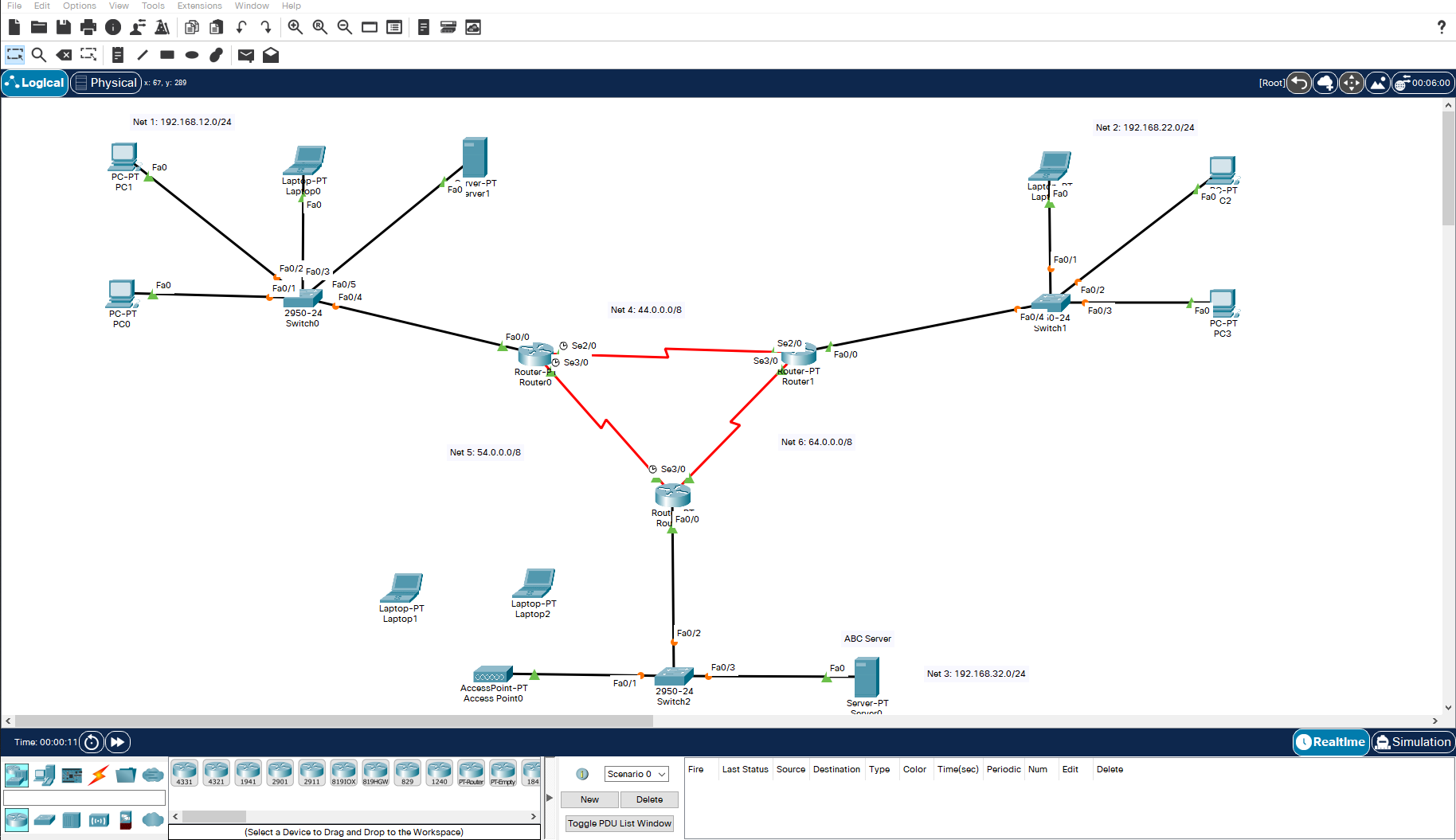
* 1. **MỤC TIÊU CỦA ĐỀ TÀI**
* **Mục tiêu chung:** Xây dựng và triển khai GRE kết hợp IPSec trong mạng VPN trên chương trình mô phỏng mạng Cisco Packet Tracer.
* **Mục tiêu cụ thể:**
* Tìm hiểu về VPN
* Tìm hiểu về GRE Tunnel
* Tìm hiểu về IPSec
* Triển khai GRE với IPSec trên Cisco Packet Tracer
  1. **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.

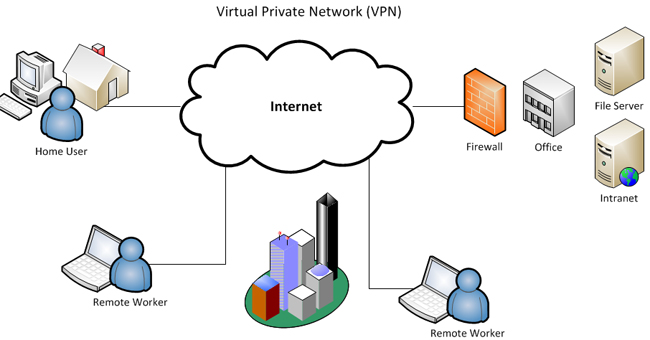


**Hình 2.1 Cisco Packet Tracer**

* 1. **TỔNG QUAN VỀ VPN**
     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**

VPN có thể được chia thành 3 loại:

* 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 mà 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. Remote Access VPN mô tả công việc các người dùng từ xa sử dụng các phần mềm VPN để truy cập vào mạng Intranet của công ty thông qua gateway hoặc VPN concentrator (bản chất là một server). Vì lý do này, giải pháp này thường được gọi là client/server. Trong giải pháp này, các người dùng thường thường sử dụng các công nghệ WAN truyền thống để tạo lại các tunnel về mạng của họ.
* 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. Không giống như Intranet và Remote Access, Extranet không an toàn cách ly từ bên ngoài (outer-world), 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.

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.