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 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.

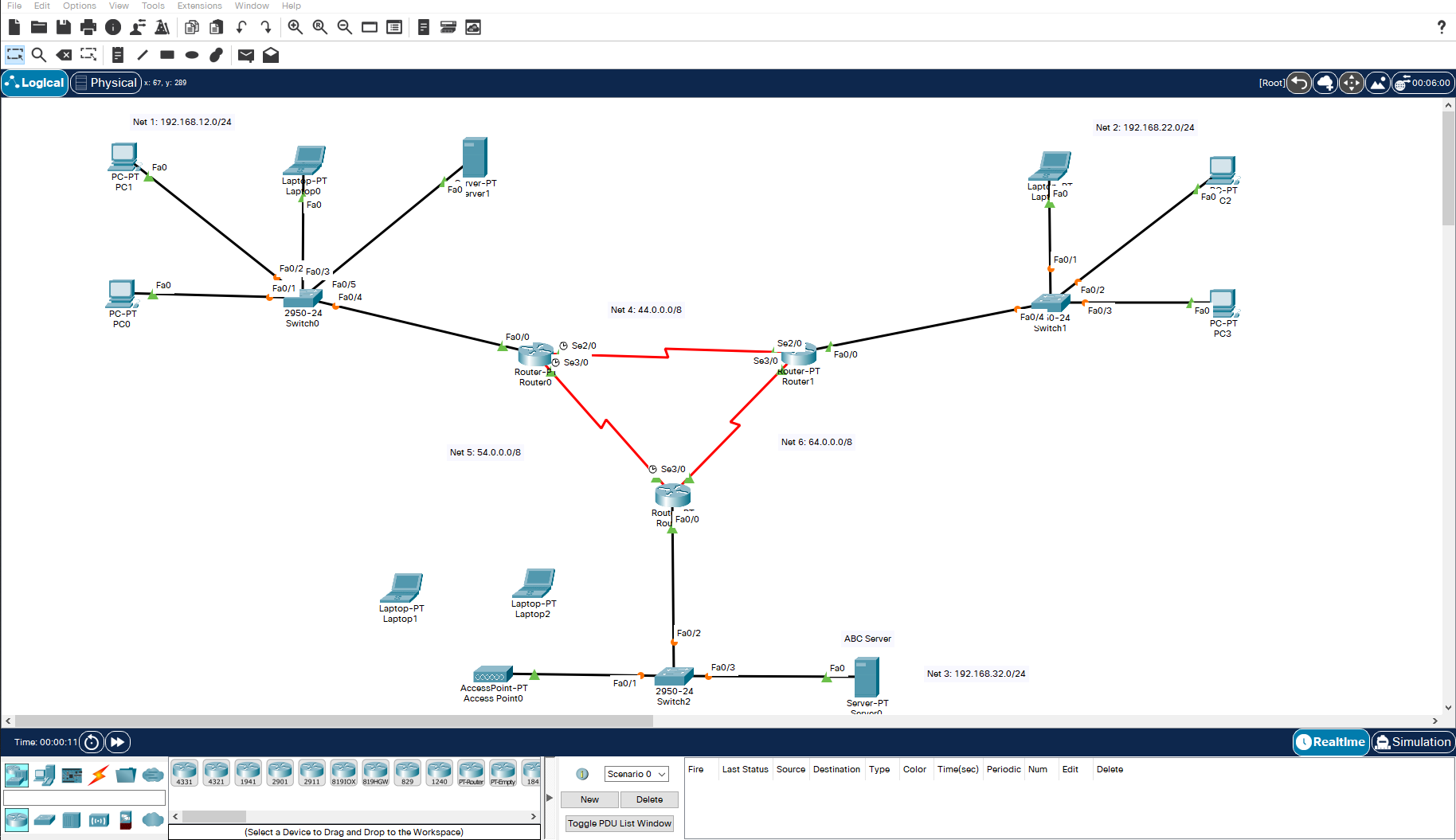
* 1. **MỤC TIÊU CỦA ĐỀ TÀI**
* **Mục tiêu chung:** Xây dựng và triển khai GRE kết hợp IPSec trong mạng VPN trên chương trình mô phỏng mạng Cisco Packet Tracer.
* **Mục tiêu cụ thể:**
* Tìm hiểu về VPN
* Tìm hiểu về GRE Tunnel
* Tìm hiểu về IPSec
* Triển khai GRE với IPSec trên Cisco Packet Tracer
  1.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



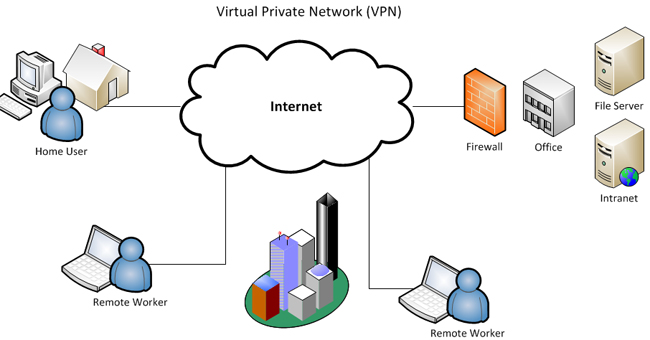
**Hình 2.1 Cisco Packet Tracer**

* 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
* **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.

**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,...

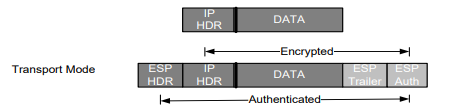
**3.2 IPSEC**

**3.2.1 Khái niệm**

IPSec (Internet Protocol Security) thực chất không phải là một giao thức, 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