**ĐẠI HỌC HUẾ**

**TRƯỜNG ĐẠI HỌC KHOA HỌC HUẾ**

**KHOA CÔNG NGHỆ THÔNG TIN**

-----🙞🙜🕮🙞🙜-----



**TIỂU LUẬN: TÌM HIỂU VÀ TRIỂN KHAI IPSec VPN VỚI PHẦN MỀM GIẢ LẬP GNS3**

|  |  |
| --- | --- |
| **TÊN HỌC PHẦN** | **: AN NINH MẠNG** |
| **MÃ HỌC PHẦN** | **: 2024-2025.1.TIN3163.006** |
| **GIẢNG VIÊN HƯỚNG DẪN** | **: VÕ VIỆT DŨNG** |

**Thừa Thiên Huế, tháng 1 năm 2025**

**ĐẠI HỌC HUẾ**

**TRƯỜNG ĐẠI HỌC KHOA HỌC HUẾ**

**KHOA CÔNG NGHỆ THÔNG TIN**

-----🙞🙜🕮🙞🙜-----



**TIỂU LUẬN: TÌM HIỂU VÀ TRIỂN KHAI IPSec VPN VỚI PHẦN MỀM GIẢ LẬP GNS3**

|  |  |
| --- | --- |
| **TÊN HỌC PHẦN** | **: AN NINH MẠNG** |
| **NHÓM THỰC HIỆN** | **: 06** |
| **DANH SÁCH THÀNH VIÊN** | **: TRẦN THỊ UYÊN NHI**  **PHAN THỊ ANH TRANG**  **NGUYỄN KHÁNH LINH**  **TÔN HUYỀN KIM KHÁNH** |

**LỜI MỞ ĐẦU**

Trong thời đại 4.0 hiện nay, bảo mật thông tin là yếu tố được quan tâm hàng đầu, là then chốt trong việc trao đổi thông tin cũng như dữ liệu. IPSec VPN với khả năng mã hóa và xác thực gói tin là giải pháp hiệu quả giúp bảo vệ giữ liệu trên môi trường internet.

Phần mềm giả lập GNS3 là công cụ mạnh mẽ để mô phỏng và thử nghiệm các mô hình mạng trước khi được đưa vào thực tế. Với đề tài: “**TÌM HIỂU VÀ TRIỂN KHAI IPSec VPN VỚI PHẦN MỀM GIẢ LẬP GNS3”** sẽ phần nào giúp chúng ta hiểu hơn về lý thuyết và cách thức triển khai mô hình, góp phần nâng cao nhận thức, kiến thức và kỹ năng bảo mật mạng.

Trong quá trình làm bài chúng em đã rất cố gắng để hoàn thành nhiệm vụ được giao , tuy nhiên với những hạn chế trong kiến thức và kinh nghiệm, đề tài của chúng em không tránh khỏi những thiếu sót. Chúng em rất mong nhận được những lời nhận xét, góp ý và phê bình quý báu từ Thầy để cải thiện và nâng cao hơn nữa chất lượng của đề tài.

Một lần nữa, chúng em xin chân thành cảm ơn Thầy!

MỤC LỤC

[LỜI MỞ ĐẦU iii](#_Toc187355987)

[MỤC LỤC iv](#_Toc187355988)

[I. LÝ THUYẾT 1](#_Toc187355989)

[**1. Tìm hiểu về giao thức IPSec** 1](#_Toc187355990)

[**1.1 Khái niệm về IPSec** 1](#_Toc187355991)

[**1.2** **IPSec VPN** 2](#_Toc187355992)

[**1.3 Thành phần của IPSec** 2](#_Toc187355994)

[**1.3.1  Authentication Header (AH)** 3](#_Toc187355995)

[**1.3.2 Encapsulating Security Payload (ESP)** 3](#_Toc187355996)

[**1.3.3 Internet Key Exchange (IKE)** 4](#_Toc187355997)

[**1.4 Các chế độ hoạt động** 4](#_Toc187355998)

[**1.4.1 Transport Mode** 4](#_Toc187355999)

[**1.4.2 Tunnel Mode** 4](#_Toc187356000)

[**1.5 Quy trình hoạt động** 5](#_Toc187356001)

[**1.5.1 Xác thực và mã hóa** 5](#_Toc187356002)

[**1.5.2 Thiết lập kênh bảo mật (Security Association - SA)** 5](#_Toc187356003)

[**1.5.3 Internet Key Exchange (IKE)** 5](#_Toc187356004)

[**1.6 Ưu nhược điểm của IPSec**. 6](#_Toc187356005)

[**1.6.1 Ưu điểm** 6](#_Toc187356006)

[**1.6.2 Nhược điểm của IPSec** 6](#_Toc187356007)

[2. Tìm hiểu về VPN 7](#_Toc187356008)

[**2.1 Khái niệm VPN** 7](#_Toc187356009)

[**2.2 Các loại VPN phổ biến** 8](#_Toc187356010)

[**2.2.1. Site-to-Site VPN** 8](#_Toc187356011)

[**2.2.2.** **Client-to-Site VPN** 9](#_Toc187356012)

[**2.2.3.** **Remote Access VPN** 9](#_Toc187356013)

[**2.3 Ưu nhược điểm của VPN** 10](#_Toc187356014)

[**2.4 Các giao thức VPN phổ biến** 10](#_Toc187356015)

[**2.5 Ứng dụng của VPN trong thực tế** 11](#_Toc187356016)

[II. THỰC HÀNH 12](#_Toc187356017)

[**1.** **Mô hình Sito – to – site** 12](#_Toc187356018)

[**2.** **Mô hình Client – to – site** 18](#_Toc187356019)

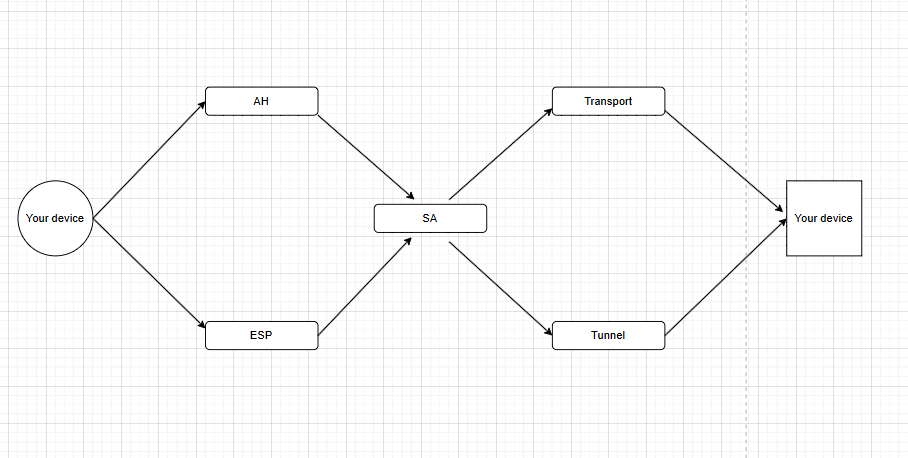
[TÀI LIỆU THAM KHẢO v](#_Toc187356020)

# LÝ THUYẾT

## Tìm hiểu về giao thức IPSec

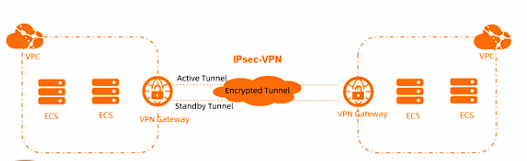
### **1.1 Khái niệm về IPSec**

* **IPSec là gì?**

****

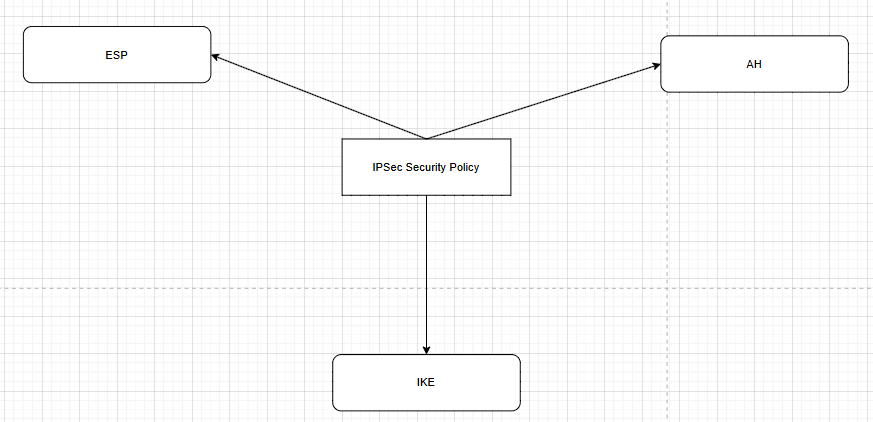
IPSec (Internet Protocol Security) là một bộ giao thức được thiết kế để bảo vệ dữ liệu khi truyền qua mạng IP bằng cách mã hóa và xác thực. IPSec hoạt động ở lớp mạng (Network Layer) của mô hình OSI, giúp đảm bảo an toàn cho dữ liệu khi di chuyển qua các mạng công cộng như Internet.

* **IPSec cung cấp**:
  + Bảo mật dữ liệu (Confidentiality): Mã hóa dữ liệu để ngăn chặn truy cập trái phép.
  + Toàn vẹn dữ liệu (Integrity): Đảm bảo dữ liệu không bị thay đổi trong quá trình truyền.
  + Xác thực (Authentication): Đảm bảo rằng các bên giao tiếp là hợp lệ.
  + Chống lặp lại (Anti-Replay): Ngăn chặn các cuộc tấn công lặp lại (Replay Attack) bằng cách gán số thứ tự cho mỗi gói tin.
* **Các ứng dụng của IPSec trong bảo mật mạng**
* Tạo kết nối VPN an toàn: Sử dụng IPSec để xây dựng các VPN bảo mật giữa các văn phòng, chi nhánh của tổ chức hoặc kết nối từ xa.
* Bảo vệ lưu lượng dữ liệu trên mạng công cộng: Đảm bảo an toàn cho lưu lượng truyền tải qua Internet bằng mã hóa và xác thực.
* Kiểm soát truy cập: Xác thực người dùng và thiết bị, đảm bảo chỉ các đối tượng được phép mới có thể truy cập mạng.
* Ứng dụng trong IoT và mạng 5G: IPSec bảo vệ giao tiếp giữa các thiết bị IoT và trong các môi trường mạng di động mới.
  1. **IPSec VPN**



IPSec VPN (Internet Protocol Security) là giao thức mạng về bảo mật (security) và thường được liên kết với VPN (tất nhiên bạn hoàn toàn có thể dùng IPSec ở trong mạng cục bộ LAN). IPSec VPN cho phép việc truyền tải dữ liệu được mã hóa an toàn ở lớp mạng (Network Layer) theo mô hình OSI thông qua các router mạng công cộng Internet được cung cấp phổ biến hiện nay như: ADSL router, FTTH router.v.v. VPN (ở lớp mạng-Network) đề cập đến những thách thức trong việc sử dụng Internet như là một môi trường truyền và đưa các dữ liệu đa giao thức và nhạy cảm. Việc thiết lập một đường hầm IPSec VPN (IPSec tunnel) giữa hai nơi, trước tiên, phải thỏa thuận về chính sách an ninh (security policy), giải thuật mã hóa (encryption algorithm), kiểu xác thực (authentication method) sẽ được dùng để tạo kênh đường hầm IPSec VPN. Trong IPSec tất cả dịch vụ mạng như TCP, UDP, SNMP, HTTP, POP, SMTP…đều được mã hóa một khi kênh IPSec được thiết lập trong mô hình mạng máy tính chuẩn OSI.

**1.3 Thành phần của IPSec**

****

**1.3.1  Authentication Header (AH)**

AH là một giao thức bảo mật của IPSec, cung cấp:

* Toàn vẹn dữ liệu: Đảm bảo dữ liệu không bị thay đổi trong quá trình truyền.
* Xác thực nguồn gốc: Đảm bảo gói tin được gửi từ nguồn đáng tin cậy.

AH **không cung cấp mã hóa**, nên dữ liệu vẫn có thể bị nhìn thấy trên đường truyền. AH hoạt động bằng cách thêm một tiêu đề (header) xác thực vào gói tin IP ban đầu.

* **Cấu trúc tiêu đề AH**:
  + Next Header: Xác định giao thức ở lớp trên (TCP, UDP, v.v.).
  + Payload Length: Độ dài của phần dữ liệu.
  + Security Parameters Index (SPI): Chỉ số nhận dạng kết nối IPSec.
  + Sequence Number: Ngăn chặn các tấn công lặp lại (Replay Attack).
  + Authentication Data: Dữ liệu dùng để xác thực gói tin.

**1.3.2 Encapsulating Security Payload (ESP)**

* **ESP cung cấp:**
* Mã hóa (Encryption): Bảo mật dữ liệu bằng cách mã hóa nội dung.
* Xác thực (Authentication): Bảo vệ toàn vẹn dữ liệu và xác thực nguồn gốc.
* ESP hoạt động bằng cách mã hóa và/hoặc xác thực phần dữ liệu trong gói tin IP.
* **Cấu trúc tiêu đề ESP**:
  + SPI: Nhận dạng SA.
  + Sequence Number: Ngăn chặn tấn công lặp lại.
  + Encrypted Data: Dữ liệu đã mã hóa.
  + Authentication Data: Đảm bảo toàn vẹn và xác thực.

**1.3.3 Internet Key Exchange (IKE)**

* **Chức năng của IKE:**
* Thỏa thuận tham số bảo mật (SA - Security Association): IKE giúp hai thiết bị đồng ý về thuật toán mã hóa, xác thực và các tham số khác trước khi thiết lập kết nối IPSec.
* Xác thực: Đảm bảo rằng các bên tham gia đều đáng tin cậy và hợp lệ.
* Trao đổi khóa: IKE thực hiện trao đổi khóa mã hóa để bảo vệ dữ liệu truyền tải.
* **Cấu trúc giao thức IKE:**
* Initiator Cookie và Responder Cookie**:** Dùng để xác định các bên tham gia giao tiếp.
* Payload Length: Độ dài của dữ liệu trong payload.
* Exchange Type: Loại trao đổi, ví dụ: Main Mode, Aggressive Mode.
* Message ID: Nhận dạng các tin nhắn trong một phiên giao tiếp.
* Payload Data**:** Chứa dữ liệu như khóa trao đổi, thông tin SA, hoặc thông tin xác thực.

**1.4 Các chế độ hoạt động**

**IPSec có hai chế độ hoạt động chính:**

**1.4.1 Transport Mode**

* Chỉ mã hóa phần **Payload** (nội dung) của gói tin IP gốc.
* Header IP gốc vẫn giữ nguyên.
* Thường được sử dụng trong kết nối giữa các thiết bị đầu cuối hoặc trong mạng nội bộ.

**1.4.2 Tunnel Mode**

* Mã hóa toàn bộ gói tin IP gốc (bao gồm cả Header và Payload).
* Gói tin đã mã hóa sẽ được đóng gói trong một gói tin IP mới với Header mới.
* Thường được sử dụng trong các kết nối VPN giữa các site hoặc thiết bị bảo mật như Router, Firewall.

**So sánh hai chế độ**:

|  |  |  |
| --- | --- | --- |
| **Đặc điểm** | **Transport Mode** | **Tunnel Mode** |
| Dữ liệu được bảo vệ | Chỉ Payload | Cả gói tin IP |
| Ứng dụng | Thiết bị đầu cuối | VPN giữa các site |

**1.5 Quy trình hoạt động**

**1.5.1 Xác thực và mã hóa**

* IPSec sử dụng các thuật toán mã hóa như AES, DES, hoặc 3DES để bảo mật dữ liệu.
* Quá trình xác thực sử dụng các thuật toán băm như HMAC-MD5 hoặc HMAC-SHA1 để đảm bảo dữ liệu không bị thay đổi.

**1.5.2 Thiết lập kênh bảo mật (Security Association - SA)**

* SA là một tập hợp các thông số (thuật toán, khóa mã hóa, v.v.) được sử dụng trong quá trình truyền dữ liệu an toàn.
* SA được xác định bằng SPI, địa chỉ IP nguồn, và giao thức (AH hoặc ESP).

**1.5.3 Internet Key Exchange (IKE)**

IKE là giao thức thiết lập và quản lý SA cho IPSec. Quá trình gồm:

* **Phase 1**: Thiết lập kênh IKE bảo mật.
  + Xác thực hai bên.
  + Thỏa thuận thuật toán mã hóa và xác thực.
* **Phase 2**: Thiết lập SA cho IPSec.
  + Xác định các thông số bảo mật cho AH/ESP.
* **Quy trình tổng quát của IPSec**:
* Hai bên bắt đầu giao tiếp qua IKE để thỏa thuận và xác thực.
* SA được thiết lập, và dữ liệu được truyền qua giao thức AH hoặc ESP.
* Dữ liệu được bảo mật trong suốt quá trình truyền thông qua mạng.

## 1.6 Ưu nhược điểm của IPSec.

### **1.6.1 Ưu điểm**

* **Bảo mật toàn diện**:
* Bảo mật dữ liệu (Confidentiality): IPSec mã hóa dữ liệu, đảm bảo chỉ người nhận hợp lệ mới có thể giải mã.
* Xác thực (Authentication): Đảm bảo các bên tham gia giao tiếp là hợp lệ.
* Toàn vẹn dữ liệu (Integrity): Ngăn chặn việc thay đổi dữ liệu trong quá trình truyền.
* Chống tấn công lặp lại (Anti-Replay): Ngăn chặn các cuộc tấn công lặp lại thông qua số thứ tự của gói tin.
* **Hoạt động ở lớp mạng (Network Layer)**: Bảo vệ dữ liệu độc lập với ứng dụng, hoạt động cho tất cả các giao thức lớp cao hơn như TCP, UDP.
* **Linh hoạt trong triển khai**: IPSec hỗ trợ cả hai chế độ **Transport Mode** và **Tunnel Mode**, phù hợp với các kịch bản bảo mật khác nhau như VPN site-to-site, client-to-site, hoặc bảo mật giữa các thiết bị đầu cuối.
* **Tích hợp với các giao thức khác**: Kết hợp với IKE để thiết lập và quản lý khóa mã hóa.
* **Khả năng mở rộng**: IPSec dễ dàng mở rộng để bảo vệ nhiều mạng, từ các kết nối VPN quy mô nhỏ đến các mạng lớn.
* **Hỗ trợ đa nền tảng**: IPSec tương thích với nhiều hệ điều hành và thiết bị mạng (Router, Firewall, VPN Gateway).

### **1.6.2 Nhược điểm của IPSec**

* **Độ phức tạp trong triển khai**:
* Cấu hình IPSec yêu cầu kiến thức chuyên sâu về bảo mật mạng và giao thức, đặc biệt khi sử dụng với các thiết bị khác nhau.
* Quá trình thiết lập SA (Security Association) và quản lý khóa (Key Management) phức tạp.
* **Hiệu năng**: Mã hóa và xác thực dữ liệu tiêu tốn tài nguyên CPU, dẫn đến giảm hiệu suất mạng, đặc biệt trên các thiết bị cũ hoặc có cấu hình thấp.
* **Tương thích**:
* Không phải tất cả các thiết bị đều hỗ trợ IPSec, hoặc các phiên bản IPSec khác nhau có thể gây ra vấn đề về tương thích.
* Một số ứng dụng NAT (Network Address Translation) không hỗ trợ IPSec, trừ khi sử dụng các kỹ thuật NAT-Traversal.
* **Không bảo vệ toàn bộ đường truyền**: IPSec chỉ bảo vệ dữ liệu từ nguồn đến đích (End-to-End hoặc Gateway-to-Gateway). Các phần khác trong mạng, như dữ liệu nội bộ hoặc giữa các thiết bị trên cùng một mạng LAN, có thể không được bảo vệ.
* **Khó theo dõi và xử lý sự cố**: Gói tin được mã hóa khó kiểm tra nội dung, gây khó khăn trong việc giám sát và xử lý sự cố mạng.
* **Chi phí triển khai**: Đòi hỏi phần cứng và phần mềm hỗ trợ IPSec, cùng với chi phí đào tạo nhân sự để cấu hình và bảo trì hệ thống.

# 2. Tìm hiểu về VPN

## 2.1 Khái niệm VPN

**VPN** (Virtual Private Network - Mạng riêng ảo) là một công nghệ cho phép kết nối các thiết bị qua một mạng công cộng, như Internet, bằng cách tạo ra một "kênh" truyền thông bảo mật, bảo vệ dữ liệu truyền tải giữa các điểm cuối trong mạng. VPN tạo ra một "tunnel" (đường hầm) bảo mật giữa các thiết bị và các máy chủ thông qua các giao thức mã hóa, giúp ngăn chặn các cuộc tấn công bên ngoài, và bảo vệ tính riêng tư của dữ liệu truyền tải.

Khi sử dụng VPN, dữ liệu được mã hóa trước khi truyền qua mạng công cộng, khiến cho dữ liệu không thể bị đọc hay thay đổi bởi các bên không có quyền truy cập. Vì vậy, VPN trở thành một công cụ quan trọng trong việc bảo vệ thông tin nhạy cảm trong môi trường mạng.

* **Cách thức VPN tạo ra kênh truyền an toàn trên mạng công cộng**

VPN sử dụng các kỹ thuật mã hóa để bảo vệ dữ liệu trong quá trình truyền tải. Cách thức hoạt động cơ bản của một VPN bao gồm các bước sau:

1. **Kết nối tới VPN Server**: Một thiết bị (như máy tính, điện thoại, router) kết nối với một máy chủ VPN thông qua một giao thức bảo mật.
2. **Mã hóa dữ liệu**: Dữ liệu được mã hóa ngay trên thiết bị gửi đi trước khi được truyền qua mạng công cộng, đảm bảo rằng ngay cả khi dữ liệu bị chặn, kẻ tấn công không thể giải mã thông tin.
3. **Tạo kênh bảo mật (Tunnel)**: Dữ liệu được gửi qua một "tunnel" bảo mật đến máy chủ VPN. Tunnel này được bảo vệ bởi các giao thức như IPSec hoặc SSL/TLS để ngăn chặn các cuộc tấn công từ bên ngoài.
4. **Giải mã và chuyển tiếp dữ liệu**: Máy chủ VPN nhận dữ liệu, giải mã nó, và chuyển tiếp đến đích cuối cùng (website hoặc dịch vụ mà người dùng muốn truy cập).
5. **Chuyển tiếp phản hồi về thiết bị gửi đi**: Khi thiết bị nhận phản hồi từ đích cuối (ví dụ: máy chủ web), dữ liệu sẽ được mã hóa lại và truyền qua tunnel tới thiết bị đầu cuối, nơi nó được giải mã để hiển thị.

## Các loại VPN phổ biến

**2.2.1. Site-to-Site VPN**

* + **Khái niệm**: Site-to-Site VPN kết nối hai hoặc nhiều mạng LAN tại các địa điểm khác nhau (ví dụ, một văn phòng chi nhánh kết nối với văn phòng chính) qua mạng công cộng (Internet).
  + **Cách thức hoạt động**: Mỗi địa điểm sẽ có một gateway VPN, kết nối giữa các gateway này tạo ra một đường hầm bảo mật giữa các mạng LAN, cho phép các máy tính trong các mạng khác nhau giao tiếp với nhau một cách an toàn.
  + **Ưu điểm**:
    - Cung cấp kết nối an toàn và hiệu quả giữa các văn phòng hoặc chi nhánh.
    - Dễ dàng quản lý, đặc biệt cho các tổ chức lớn với nhiều chi nhánh.
  + **Nhược điểm**:
    - Cần thiết lập và cấu hình phức tạp, đặc biệt khi kết nối nhiều địa điểm.
    - Có thể gặp vấn đề về hiệu suất nếu mạng Internet không ổn định.
    1. **Client-to-Site VPN**
  + **Khái niệm**: Client-to-Site VPN cho phép một thiết bị cá nhân (client) kết nối trực tiếp đến một mạng từ xa thông qua VPN, giống như Remote Access VPN nhưng thường được sử dụng cho các thiết bị như laptop, smartphone, hoặc máy tính cá nhân.
  + **Cách thức hoạt động**: Người dùng cài đặt phần mềm VPN client trên thiết bị của mình và kết nối đến mạng công ty thông qua máy chủ VPN.
  + **Ưu điểm**:
    - Bảo mật cao khi làm việc trên mạng công cộng.
    - Phù hợp cho các tổ chức muốn cung cấp truy cập từ xa cho nhân viên hoặc đối tác.
  + **Nhược điểm**:
    - Giới hạn về số lượng người dùng có thể kết nối cùng lúc.
    - Cần phải cài đặt phần mềm VPN trên thiết bị của người dùng.
    1. **Remote Access VPN**
  + **Khái niệm**: Remote Access VPN cho phép người dùng từ xa (như nhân viên làm việc tại nhà hoặc từ các địa điểm khác) kết nối an toàn với mạng nội bộ của công ty qua Internet. Người dùng có thể sử dụng máy tính hoặc điện thoại di động để kết nối với VPN.
  + **Cách thức hoạt động**: Người dùng kết nối từ thiết bị cá nhân đến máy chủ VPN của tổ chức, từ đó truy cập tài nguyên trong mạng nội bộ như thể đang ở trong cùng một mạng LAN.
  + **Ưu điểm**:
    - Cho phép truy cập mạng nội bộ từ xa.
    - Dễ dàng triển khai cho nhân viên làm việc tại nhà hoặc từ các địa điểm khác.
    - Bảo mật cao nhờ mã hóa dữ liệu.
  + **Nhược điểm**:
    - Cần phải duy trì một kết nối mạng ổn định và nhanh chóng.
    - Đôi khi có thể gặp phải vấn đề về hiệu suất khi kết nối qua mạng công cộng.

## 2.3 Ưu nhược điểm của VPN

* **Ưu điểm**:
  + Bảo mật: VPN bảo vệ dữ liệu qua mã hóa, đảm bảo thông tin không bị lộ khi truyền qua mạng công cộng.
  + Riêng tư: VPN giúp ẩn địa chỉ IP và vị trí của người dùng, giúp họ duyệt web ẩn danh.
  + Tiết kiệm chi phí: VPN cho phép kết nối từ xa mà không cần đến các kết nối riêng biệt tốn kém như các đường truyền thuê riêng.
  + Truy cập vào mạng nội bộ từ xa: Nhân viên có thể truy cập tài nguyên mạng nội bộ khi không ở văn phòng.
* **Nhược điểm**:
  + Hiệu suất: Mã hóa và giải mã có thể làm giảm tốc độ truy cập mạng.
  + Chi phí duy trì: Cần đầu tư vào thiết bị và phần mềm VPN để duy trì kết nối bảo mật.
  + Quản lý phức tạp: Việc cấu hình và duy trì VPN có thể phức tạp, đặc biệt khi có nhiều điểm kết nối từ xa.

## 2.4 Các giao thức VPN phổ biến

* **PPTP (Point-to-Point Tunneling Protocol)**:

Một giao thức VPN cũ, dễ cấu hình nhưng có mức độ bảo mật thấp, hiện nay đã ít được sử dụng do những lỗ hổng bảo mật.

* **L2TP (Layer 2 Tunneling Protocol)**:

L2TP kết hợp với IPSec để mã hóa và bảo mật dữ liệu. Được coi là an toàn hơn PPTP, nhưng yêu cầu cấu hình phức tạp hơn.

* **SSL VPN (Secure Sockets Layer VPN)**:
  + SSL VPN sử dụng giao thức SSL để tạo đường hầm bảo mật. Nó cho phép người dùng truy cập vào ứng dụng web mà không cần phần mềm VPN client đặc biệt.
  + Thường được sử dụng để truy cập vào các ứng dụng web hoặc tài nguyên mạng trong các trường hợp làm việc từ xa.
* **IPSec VPN**:

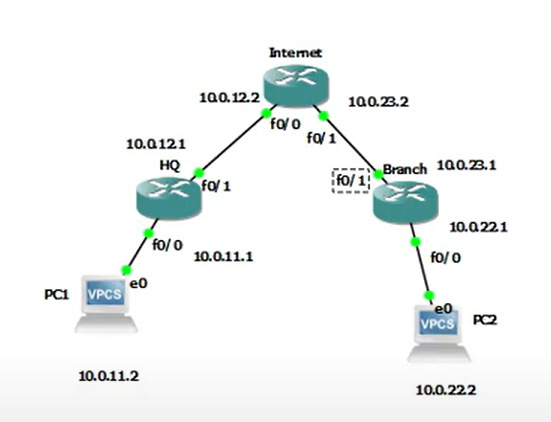
Một giao thức VPN rất phổ biến, sử dụng IPSec để bảo vệ và mã hóa dữ liệu. IPSec VPN có thể hoạt động trong cả hai chế độ Tunnel và Transport, thích hợp cho các kết nối từ xa hoặc kết nối giữa các mạng.

## Ứng dụng của VPN trong thực tế

* Bảo mật khi truy cập Internet công cộng: VPN giúp bảo vệ người dùng khi kết nối qua mạng Wi-Fi công cộng, như trong các quán cà phê, sân bay, hay khách sạn.
* Truy cập từ xa vào mạng công ty: Nhân viên có thể kết nối từ xa vào mạng công ty để làm việc từ bất kỳ đâu.
* Ẩn danh khi duyệt web: VPN giúp người dùng ẩn địa chỉ IP của mình khi duyệt web, tăng cường bảo mật và bảo vệ quyền riêng tư.
* Vượt qua các hạn chế địa lý: VPN cho phép người dùng truy cập các dịch vụ bị chặn hoặc giới hạn địa lý, chẳng hạn như các dịch vụ phát video (Netflix, BBC iPlayer) hoặc các trang web bị kiểm duyệt.
* Giảm thiểu các vấn đề bảo mật trong doanh nghiệp: Các doanh nghiệp sử dụng VPN để kết nối các chi nhánh và đảm bảo an toàn cho việc trao đổi dữ liệu giữa các địa điểm khác nhau.

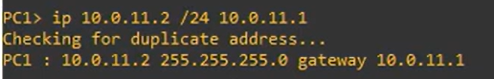
# THỰC HÀNH

1. **Mô hình Sito – to – site**

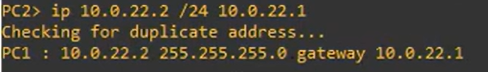


**B1: Cấu hình PC và Router**

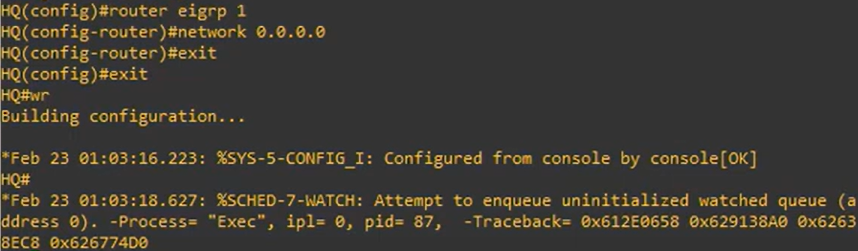
**PC1:**

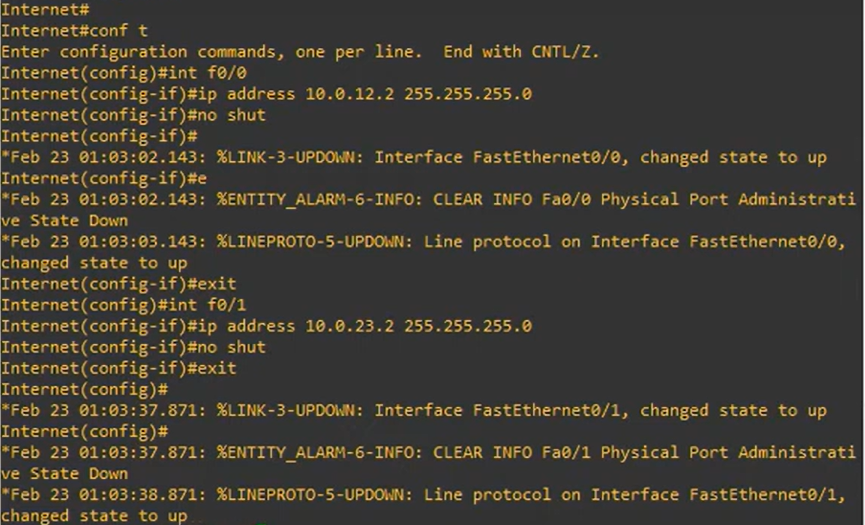


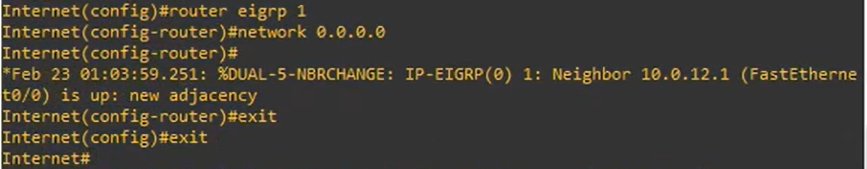
PC2:



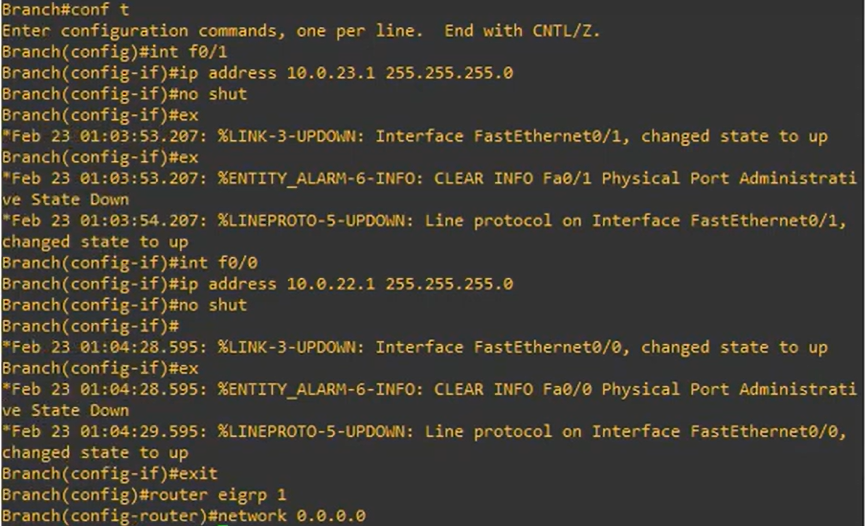
HQ: 

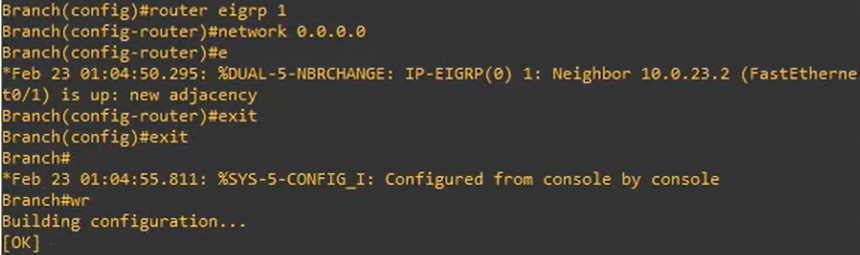


Internet: 

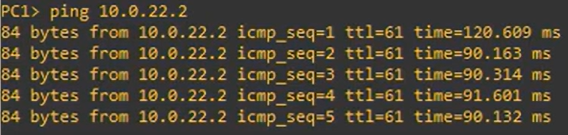


Branch:



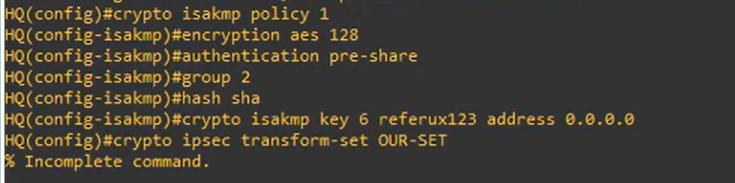


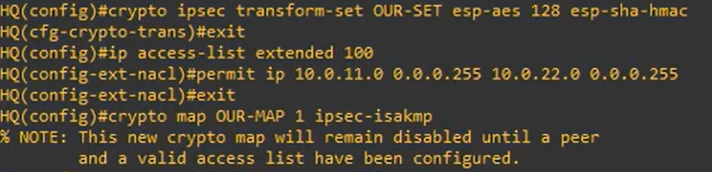
**B2: Kiểm tra cấu hình có kết nối không**

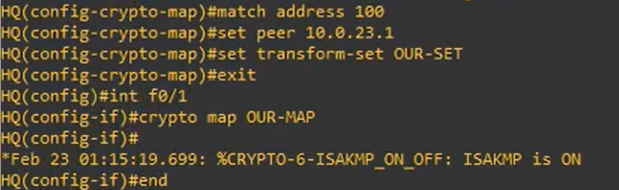


**B3: Cấu hình đường hầm VPN Ipsec**

HQ:



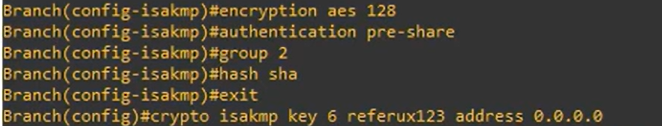


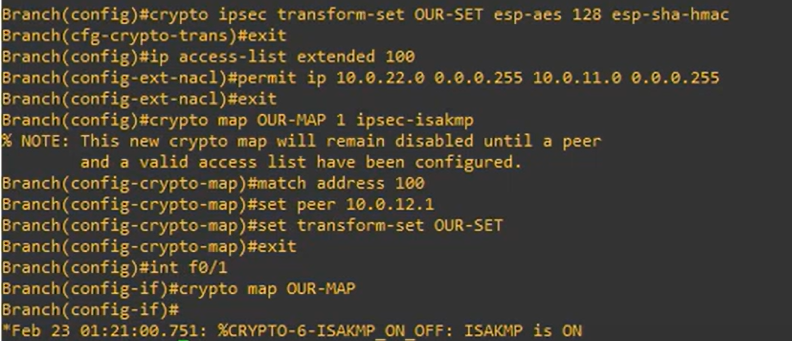


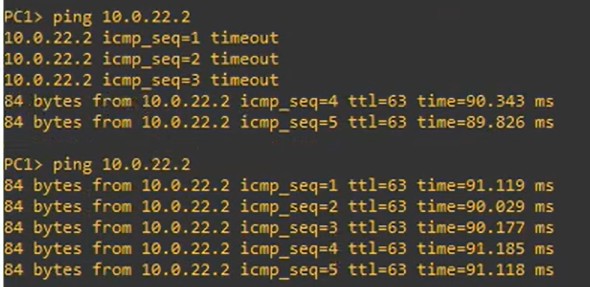
Branch:



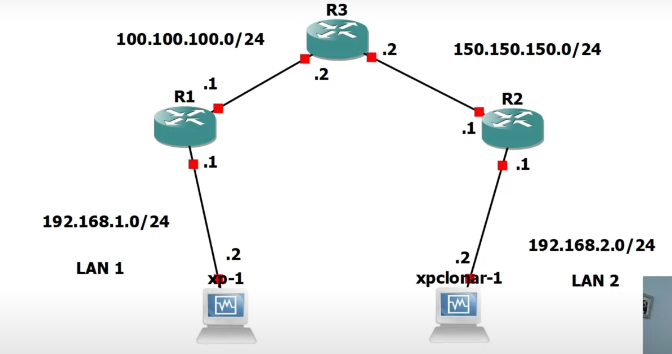




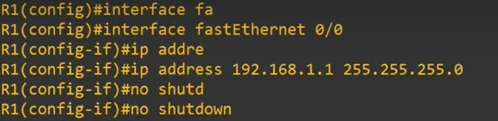


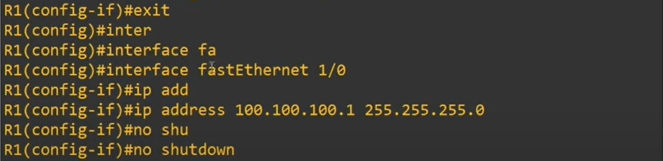
**B4: Kiểm tra kết nối**

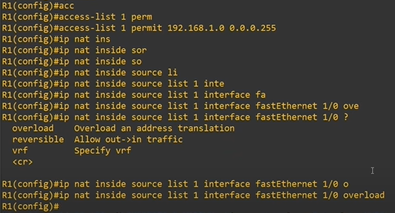
1. **Mô hình Client – to – site**

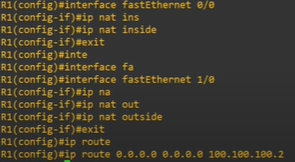


Router 1





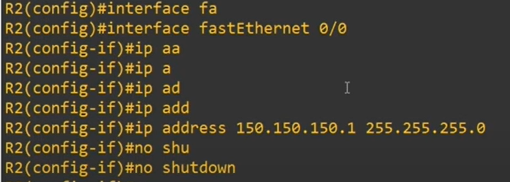


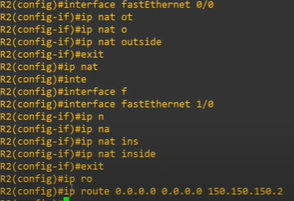


Show ip

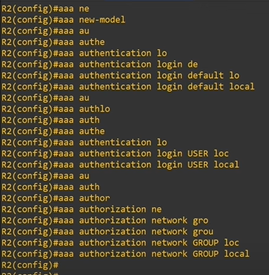


Router 2

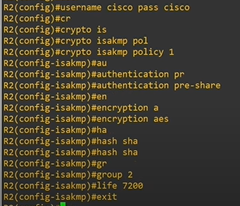


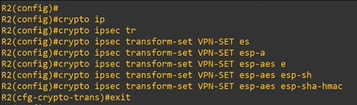


Tạo User

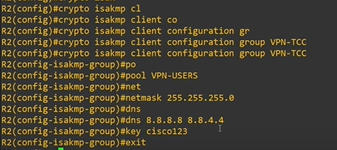




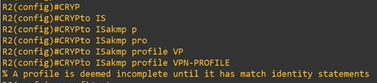


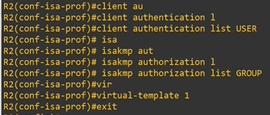


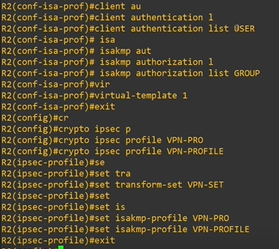


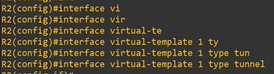


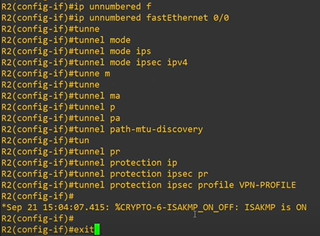
Profile











Kiểm tra kết nối



**TÀI LIỆU THAM KHẢO**

1. Khái niệm, phân loại và lợi ích của VPN -. (n.d.). Retrieved from https://vnpro.vn/thu-vien/khai-niem-phan-loai-va-loi-ich-cua-vpn-1963.html

2. Thoại V. N. (2024, December 13). IPSEC là gì? Cơ chế vận hành và ứng dụng của IPSEC. Retrieved from <https://mona.host/ipsec-la-gi/>

3. Minh L.N . (2023, May 5). IPSec là gì? Vai trò và cách thức hoạt động của IPSec trong không gian mạng. Retrieved from https://viettuans.vn/ipsec-la-gi

4. Tiên T. C. (2023, December 31). [2025] VPN Là Gì? | Hướng Dẫn Cài Đặt và Sử Dụng VPN [A-Z]. VinaHost - Nhà Cung Cấp Domain, Hosting, VPS, Server, Cloud. Retrieved from https://vinahost.vn