

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**  
**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**



**ĐỒ ÁN MÔN QUẢN TRỊ MẠNG VÀ HỆ THỐNG**

**ĐỀ TÀI**

**VPN & IPSec**

Học kỳ II (2023-2024)

**Trường Đại học Công nghệ thông tin – ĐHQGTPHCM**

**Lớp: NT132.022**

**Giảng viên hướng dẫn: NGUYỄN KHÁNH THUẬT**

**Sinh viên thực hiện:**

Họ Tên	MSSV
Phạm Hữu Thắng	22521340
Lương Cao Thắng	22521328
Bùi Phương Đại	22520180

**Thành phố Hồ Chí Minh, tháng 04 năm 2024**

## MỤC LỤC

<b>I.VPN</b>	<b>3</b>
1. Khái niệm	3
2. Công dụng	3
3. Cách để thiết lập VPN	4
4.Cách lựa chọn nhà cung cấp VPN uy tín	4
5.VPN trong doanh nghiệp	5
6.Sự khác biệt giữa VPN và proxy	6
<b>II IPSec</b>	<b>6</b>
1. Khái niệm	6
2. Công dụng	7
3. Mã hóa IPSec	7
4. Cách IPSec hoạt động	7
6.Chế độ IPSec là gì?	8
7.IPSec VPN	9
<b>III VPN site to site IPsec trong cisco</b>	<b>9</b>

## **I.VPN**

### **1. Khái niệm**

VPN hay Mạng riêng ảo tạo ra kết nối mạng riêng tư giữa các thiết bị thông qua Internet. VPN được sử dụng để truyền dữ liệu một cách an toàn và ẩn danh qua các mạng công cộng. VPN hoạt động bằng cách ẩn địa chỉ IP của người dùng và mã hóa dữ liệu để chỉ người được cấp quyền nhận dữ liệu mới có thể đọc được.

### **2. Công dụng**

Dịch vụ VPN chủ yếu được sử dụng để gửi dữ liệu một cách an toàn qua Internet. 3 chức năng chính của VPN là:

#### **● Quyền riêng tư**

Nếu không có mạng riêng ảo, dữ liệu cá nhân của bạn như mật khẩu, thông tin thẻ tín dụng và lịch sử duyệt web có thể bị ghi lại và rao bán bởi các bên thứ ba khi bạn truy cập vào các trang web không uy tín. VPN sử dụng mã hóa để giữ bí mật những thông tin này, đặc biệt là khi bạn kết nối qua mạng Wi-Fi công cộng.

Việc các nhà cung cấp dịch vụ Internet và trình duyệt web theo dõi lịch sử tìm kiếm của bạn không còn là bí mật nữa. Họ có thể và thường sẽ bán lịch sử tìm kiếm của bạn cho mục đích tiếp thị. Ví dụ: tìm bài viết về vòi nước bị rò rỉ có thể dẫn tới việc bắt gặp quảng cáo nhắm mục tiêu từ các công ty sửa ống nước địa phương. Kết nối VPN sẽ bảo vệ dữ liệu của bạn không bị sử dụng trái phép.

#### **● Tính ẩn danh**

Địa chỉ IP chứa thông tin về vị trí và hoạt động duyệt web của bạn. Tất cả các trang web trên Internet theo dõi dữ liệu này bằng cookie và công nghệ tương tự. Họ có thể nhận dạng bạn bất cứ khi nào bạn ghé thăm trang web của họ. Điều này sẽ lưu vết bạn trên internet khiến họ có thể theo dõi các hoạt động của bạn. Kết nối VPN sẽ ẩn địa chỉ IP của bạn, để bạn được ẩn danh trên Internet.

#### **● Truy cập dịch vụ phát trực tuyến trên toàn cầu**

Khi bạn rời khỏi quốc gia của mình, dịch vụ phát trực tuyến có trả phí của bạn có thể không hoạt động do điều khoản và quy định trong hợp đồng. Kết nối VPN cho phép bạn thay đổi địa chỉ IP từ quốc gia của bạn và truy cập vào những chương trình ưa thích từ nơi bạn đang ở.

#### **● Bảo mật**

Dịch vụ VPN sử dụng mật mã để bảo vệ kết nối Internet của bạn khỏi những truy cập trái phép. VPN cũng có thể hoạt động như một cơ chế tắt, hủy bỏ các chương trình được chọn trước đó phòng khi có hoạt động đáng ngờ trên Internet. Việc này làm giảm khả năng dữ liệu bị xâm phạm. Những tính năng trên cho phép các công ty cấp quyền truy cập từ xa cho người dùng được ủy quyền thuộc mạng lưới kinh doanh của họ.

Mạng riêng ảo giúp hoạt động truy cập web ở mọi lúc, mọi nơi trở nên an toàn hơn cho tất cả mọi người. Con người ngày nay thường đọc tin tức ở quán cà phê, kiểm tra email ở siêu thị hay đăng nhập vào tài khoản ngân hàng trên thiết bị di động của họ. Mạng kết nối Internet này dễ bị xâm phạm vì hoạt động trên web diễn ra thông qua Wi-Fi công cộng. Sử dụng dịch vụ VPN khi kết nối với điểm phát sóng Wi-Fi công cộng, không bảo mật giúp cho cả dữ liệu và thiết bị của bạn được an toàn.

### ● Điều khiển từ xa tới nơi làm việc hoặc mạng gia đình

Việc sử dụng VPN truy cập từ xa để đăng nhập vào mạng tại nơi làm việc là điều phổ biến. Nhưng cũng có thể thiết lập máy chủ VPN tại nhà. Điều đó sẽ cho phép truy cập mọi thứ trên mạng gia đình của bạn từ mọi nơi trên thế giới. Bạn có thể thiết lập máy chủ vật lý của riêng mình tại nhà để thực hiện việc này, nhưng một số bộ định tuyến đắt tiền hơn đi kèm với phần mềm máy chủ VPN tích hợp giúp việc này dễ dàng hơn nhiều. Hoặc, nếu bạn thích thử thách bạn có thể tạo bộ định tuyến VPN của riêng mình.

Một điều cần lưu ý: khi được kết nối với một địa điểm ở xa, tất cả hoạt động lướt web của bạn cũng nằm trong VPN. Điều này có nghĩa là bạn đang sử dụng kết nối internet của văn phòng để duyệt web. Trong trường hợp kết nối với văn phòng, nó sẽ xuất hiện trên Internet như thể bạn đang duyệt từ nơi làm việc. Điều đó có nghĩa là nơi làm việc của bạn cũng có thể thấy mọi thứ bạn đang lướt trong khi kết nối qua VPN.

## 3. Cách để thiết lập VPN

Có 2 cách phổ biến để truy cập vào dịch vụ VPN cho cá nhân:

### ● Sử dụng nhà cung cấp dịch vụ VPN

Bạn có thể lựa chọn một dịch vụ VPN có thể được truy cập thông qua trình duyệt hoặc bằng cách tải ứng dụng hay phần mềm về thiết bị của bạn. Có các dịch vụ theo gói đăng ký thường sẽ tính phí dựa trên mỗi thiết bị sử dụng dịch vụ. Do vậy, việc thiết lập các dịch vụ này có thể khá tốn kém. Đồng thời, mỗi thiết bị lại cần được cấu hình riêng biệt. Ví dụ như 1.1.1.1 ,

### ● Sử dụng bộ định tuyến VPN

Việc này bao gồm mua bộ định tuyến được cài đặt trước kết nối VPN hoặc tự cài phần mềm VPN trên bộ định tuyến tại nhà của bạn. Ưu điểm của cách tiếp cận này là tất cả các thiết bị truy cập vào Internet thông qua bộ định tuyến này sẽ được bảo vệ tự động.

## 4. Cách lựa chọn nhà cung cấp VPN uy tín

Với nhiều lựa chọn hiện nay, bạn có thể thấy khó khăn khi chọn dịch vụ VPN phù hợp. Hãy sử dụng danh sách bên dưới để đánh giá các nhà cung cấp dịch vụ VPN khác nhau và đưa ra lựa chọn phù hợp nhất cho bạn:

### **Chính sách ghi nhật ký**

Những nhà cung cấp VPN tốt nhất có chính sách ghi nhật ký tối thiểu hoặc không ghi để ngăn ngừa rò rỉ thông tin từ phía họ.

### **Phần mềm được cập nhật**

Kết nối VPN tốt nhất sẽ sử dụng giao thức đường hầm mới nhất. Giao thức OpenVPN đem lại khả năng bảo mật mạnh mẽ hơn so với các giao thức khác. Giao thức này là phần mềm có mã nguồn mở, tương thích với tất cả hệ điều hành phổ biến.

### **Giới hạn băng thông**

Tất cả các dịch vụ đều có hạn mức sử dụng dữ liệu. Bạn sẽ cần chọn một nhà cung cấp dịch vụ VPN đáp ứng nhu cầu dữ liệu của bạn trong tầm ngân sách.

### **Vị trí máy chủ VPN**

Bạn phải đảm bảo rằng nhà cung cấp dịch vụ VPN của bạn có máy chủ đặt ở quốc gia mà bạn yêu cầu quyền truy cập Internet riêng tư.

VPN miễn phí sẽ hữu ích nếu bạn có ngân sách hạn chế. Tuy nhiên, bạn cần lưu ý rằng nguồn doanh thu chính của nhà cung cấp dịch vụ VPN miễn phí đến từ quảng cáo. Bạn nên dự tính việc bị quảng cáo nhắm mục tiêu hoặc chính sách ghi nhật ký và bán dữ liệu được giấu trong điều khoản và điều kiện sử dụng.

### **Hầu hết các dịch vụ VPN miễn phí:**

- ◆ Không cung cấp giao thức VPN mới nhất
- ◆ Không có hỗ trợ kỹ thuật chất lượng tốt
- ◆ Có băng thông thấp và tốc độ chậm hơn cho người dùng miễn phí
- ◆ Có phí ngắt kết nối cao hơn
- ◆ Phân bổ số lượng máy chủ VPN bị giới hạn về mặt địa lý

## **5.VPN trong doanh nghiệp**

VPN là cách thức tiết kiệm chi phí, tốc độ cao và bảo mật để kết nối người dùng từ xa với mạng văn phòng. Vì kết nối VPN thường được thực hiện trên mạng Internet công cộng, chúng có thể rẻ tiền hơn và có mức băng thông cao hơn so với liên kết WAN (mạng diện rộng) chuyên dụng hoặc liên kết đường dài, quay số từ xa. So với liên kết LAN hoặc WAN (mạng diện rộng) chuyên dụng và đắt đỏ hay liên kết đường dài, quay số từ xa, kết nối VPN cung cấp khả năng truy cập Internet riêng tư với băng thông cao cho các công ty.

Các doanh nghiệp sử dụng VPN theo 3 cách thức chính như sau:

- **Site to site VPN**

Site-to-site VPN hoạt động như một mạng riêng nội bộ cho các công ty có nhiều địa điểm tách biệt về mặt địa lý. Dịch vụ này kết nối nhiều mạng nội bộ khác nhau một cách liền mạch và bảo mật, cho phép nhân viên chia sẻ tài nguyên giữa các mạng nội bộ khác nhau. AWS Site-to-Site VPN là một dịch vụ VPN được quản lý hoàn toàn, tạo kết nối bảo mật giữa mạng văn phòng và tài nguyên AWS sử dụng đường hầm IP Security (IPSec). Đối với các ứng dụng được phân phối toàn cầu, lựa chọn này mang tới hiệu năng vượt trội.

Dịch vụ này có thể được nâng cấp lên lưu lượng VPN định tuyến thông minh tới điểm cuối mạng lưới AWS ở gần nhất về mặt địa lý. Nó còn kết nối trung tâm dữ liệu của một công ty và các văn phòng chi nhánh tới ứng dụng và dịch vụ dựa trên đám mây mà không để lộ dữ liệu mật.

#### ➤ **Client VPN hay Open VPN**

Trong Client VPN, quản trị viên mạng chịu trách nhiệm thiết lập và cấu hình cho dịch vụ VPN. Sau đó, tệp cấu hình sẽ được phân phối cho khách hàng hoặc người dùng cuối cần quyền truy cập. Khách hàng sau đó có thể thiết lập kết nối VPN từ máy tính cục bộ hoặc thiết bị di động của họ tới mạng của công ty. AWS Client VPN là một giải pháp IVPN truy cập từ xa được quản lý hoàn toàn, nhân viên có thể sử dụng giải pháp này để truy cập tài nguyên một cách an toàn cả trên AWS và mạng lưới kinh doanh tại chỗ. Có tính linh hoạt toàn phần và tự động tăng hoặc giảm quy mô dựa trên nhu cầu.

#### ➤ **SSL VPN**

Mạng riêng ảo tăng ổ bảo mật (SSL VPN) cung cấp truy cập từ xa bảo mật thông qua cổng web và đường hầm được SSL bảo vệ, giữa thiết bị riêng tư và mạng văn phòng. Đối với các nhóm làm việc từ xa cỡ lớn, việc công ty cung cấp cho mỗi thành viên một thiết bị riêng có thể trở nên đắt đỏ. Trong trường hợp này, SSL VPN trở thành một lựa chọn tiết kiệm chi phí.

#### **6. Sự khác biệt giữa VPN và proxy**

Chúng giống nhau ở chỗ cả VPN và proxy sẽ định tuyến lưu lượng truy cập của bạn thông qua bên thứ ba. Sự khác biệt là lưu lượng truy cập họ định tuyến.

VPN bao bọc một đường hầm xung quanh toàn bộ kết nối của bạn. Mỗi byte đi qua kết nối của bạn đều được đưa vào đường hầm, bất kể đó là giao thức nào. Đây có thể là lưu lượng truy cập web (HTTP), DNS, FTP, bittorrent và mọi thứ khác. Có rất nhiều thứ đi qua kết nối mạng của bạn hơn là chỉ các trang web.

Mặt khác, proxy chỉ được thiết kế cho các loại lưu lượng truy cập cụ thể. Thông thường, proxy internet chỉ dành cho các trang web (HTTP và HTTPS) nhưng cũng có thể bao gồm các giao thức khác.

## **II. IPSec**

### **1. Khái niệm**

IPSec là hệ thống các quy tắc hoặc giao thức truyền thông dùng để thiết lập kết nối an toàn qua một mạng. Giao thức Internet (IP) là tiêu chuẩn phổ biến giúp xác định cách dữ liệu truyền qua Internet. IPSec bổ sung khả năng mã hóa và xác thực để tăng cường bảo mật giao thức. Ví dụ: IPSec xáo trộn dữ liệu tại nguồn và khôi phục dữ liệu bị xáo trộn tại đích của giao thức này. IPSec cũng xác thực nguồn dữ liệu.

## 2. Công dụng

Có thể sử dụng IPsec để tiến hành những tác vụ sau:

- Cung cấp bảo mật cho bộ định tuyến khi gửi dữ liệu qua kết nối Internet công cộng.
- Mã hóa dữ liệu ứng dụng.
- Xác thực dữ liệu nhanh chóng nếu dữ liệu được gửi từ một người gửi đã biết.
- Bảo vệ dữ liệu mạng bằng cách thiết lập các đường mạch được mã hóa, được gọi là đường hầm IPsec, thực hiện mã hóa tất cả dữ liệu được gửi giữa hai điểm cuối.

Ví dụ: người dùng kết nối Internet bằng IPsec để truy cập từ xa các tệp của công ty. Giao thức IPsec mã hóa thông tin nhạy cảm để ngăn chặn sự giám sát không mong muốn. Máy chủ cũng có thể xác minh rằng các gói dữ liệu nhận được đã được cho phép.

Các tổ chức sử dụng IPsec để bảo vệ khỏi các cuộc tấn công phát lại. Tấn công phát lại hay còn gọi là tấn công xen giữa, là một hành động chặn và thay đổi quá trình truyền dữ liệu đang diễn ra bằng cách định tuyến dữ liệu đến một máy tính trung gian. Giao thức IPsec ấn định một số thứ tự cho mỗi gói dữ liệu và tiến hành kiểm tra để phát hiện dấu hiệu của các gói trùng lặp.

## 3. Mã hóa IPsec

Mã hóa IPsec là một chức năng phần mềm làm nhiều dữ liệu 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 nhiều 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 chuyển sang mã hóa đối xứng để tăng tốc độ truyền dữ liệu.

## 4. Cách IPsec hoạt động

Máy tính trao đổi dữ liệu bằng giao thức IPsec thông qua các bước sau.

1. Máy tính của người gửi xác định xem việc truyền dữ liệu có yêu cầu bảo vệ IPsec hay không bằng cách xác minh chính sách bảo mật của nó. Nếu có, máy tính bắt đầu truyền dữ liệu IPsec bảo mật với máy tính của người nhận.
2. Cả hai máy tính đều thương lượng các yêu cầu để thiết lập kết nối bảo mật. Bao gồm việc đồng ý với nhau về các thông số mã hóa, xác thực và các tham số liên kết bảo mật (SA) khác.
3. Máy tính gửi và nhận dữ liệu được mã hóa, xác thực rằng dữ liệu đó đến từ các nguồn đáng tin cậy. Máy tính thực hiện các kiểm tra để đảm bảo nội dung cơ bản là đáng tin cậy.

4. Khi quá trình truyền dữ liệu hoàn tất hoặc phiên làm việc đã hết thời gian chờ, máy tính sẽ kết thúc kết nối IPSec.

## 5. Các giao thức IPSec

Giao thức IPSec gửi các gói dữ liệu một cách bảo mật. Gói dữ liệu là một cấu trúc cụ thể định dạng và chuẩn bị thông tin để truyền tải qua mạng. Nó bao gồm một phần đầu, tải trọng và phần đuôi.

- Phần đầu (header) là phần trước đó chứa thông tin hướng dẫn để định tuyến gói dữ liệu đến đúng đích.
- Tải trọng (payload) là một thuật ngữ mô tả thông tin thực tế chứa trong một gói dữ liệu.
- Phần đuôi (trailer) là dữ liệu bổ sung được nối vào phần đuôi của tải trọng để cho biết phần cuối của gói dữ liệu.

Dưới đây là một số giao thức IPSec.

### Phần đầu xác thực (AH)

Giao thức phần đầu xác thực (AH) thêm phần đầu có chứa dữ liệu xác thực người gửi và bảo vệ nội dung gói dữ liệu tránh bị các bên chưa được cho phép sửa đổi. Nó cảnh báo người nhận về các thao tác có thể đã thực hiện đối với gói dữ liệu gốc. Khi nhận được gói dữ liệu, máy tính sẽ so sánh hàm băm mật mã từ tải trọng với phần đầu để đảm bảo cả hai giá trị khớp nhau. Hàm băm mật mã là một hàm toán học tóm tắt dữ liệu thành một giá trị độc nhất.

### Đóng gói tải trọng bảo mật (ESP)

Tùy thuộc vào chế độ IPSec đã chọn, giao thức đóng gói tải trọng bảo mật (ESP) thực hiện mã hóa toàn bộ gói IP hoặc chỉ riêng tải trọng. ESP thêm phần đầu và phần đuôi vào gói dữ liệu sau khi mã hóa.

### Trao đổi khóa Internet (IKE)

Trao đổi khóa Internet (IKE) là một giao thức thiết lập kết nối bảo mật giữa hai thiết bị trên Internet. Cả hai thiết bị đều thiết lập liên kết bảo mật (SA), bao gồm thương lượng các khóa mã hóa và thuật toán để truyền và nhận các gói dữ liệu tiếp theo.

## 6. Chế độ IPSec là gì?

IPSec hoạt động ở hai chế độ khác nhau với các mức độ bảo vệ khác nhau.

### Đường hầm

Chế độ đường hầm IPSec thích hợp để truyền dữ liệu trên các mạng công cộng vì chế độ này tăng cường khả năng bảo vệ dữ liệu khỏi các bên chưa được cho phép. Máy tính mã hóa tất cả dữ liệu, bao gồm cả tải trọng và phần đầu, đồng thời gán một phần đầu mới cho dữ liệu đó.

### Truyền tải

Chế độ truyền tải IPSec chỉ mã hóa tải trọng của gói dữ liệu và giữ phần đầu IP ở dạng gốc. Phần đầu gói dữ liệu không được mã hóa cho phép các bộ định tuyến xác định địa



chỉ đích của mỗi gói dữ liệu. Do đó, truyền tải IPSec được sử dụng trong một mạng gần và đáng tin cậy, chẳng hạn như đảm bảo kết nối trực tiếp giữa hai máy tính.

## 7. IPSec VPN

VPN, hay còn gọi là mạng riêng ảo, là một phần mềm mạng cho phép người dùng duyệt Internet một cách ẩn danh và bảo mật. IPSec VPN là một phần mềm VPN sử dụng giao thức IPSec để tạo các đường hầm được mã hóa trên Internet. Phần mềm này cung cấp mã hóa toàn diện, có nghĩa là dữ liệu bị làm nhiễu tại máy tính và giải nhiễu tại máy chủ nhận. I

## SSL VPN

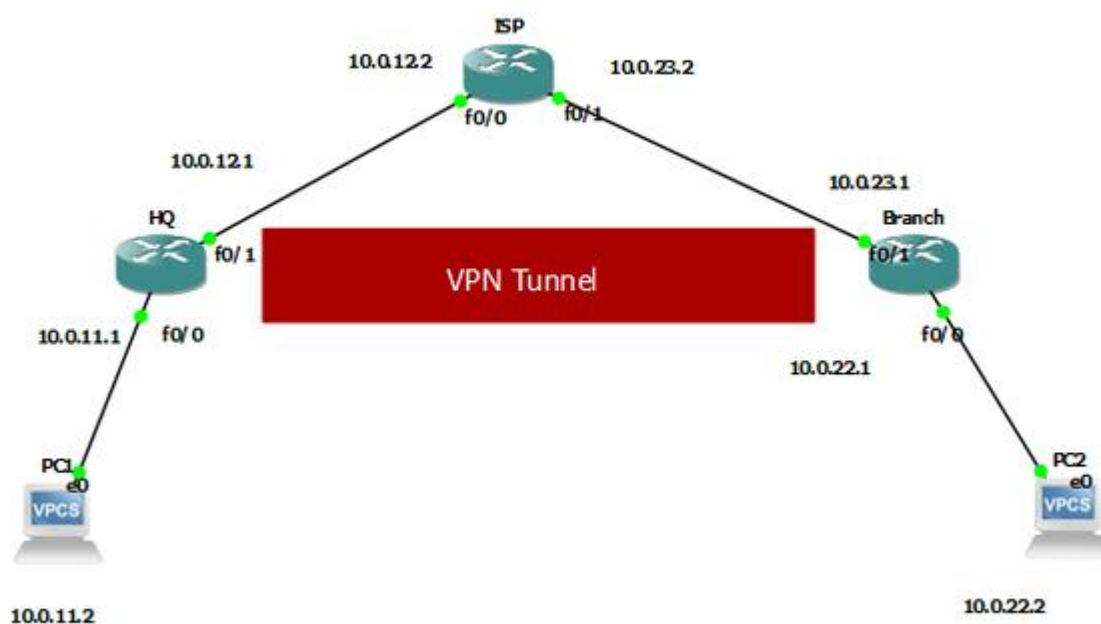
SSL là viết tắt của lớp cổng bảo mật. Đó là một giao thức bảo mật bảo vệ lưu lượng truy cập web. SSL VPN là một dịch vụ bảo mật mạng dựa trên trình duyệt sử dụng giao thức SSL tích hợp để mã hóa và bảo vệ giao tiếp mạng.

## Sự khác biệt giữa IPSec VPN và SSL VPN

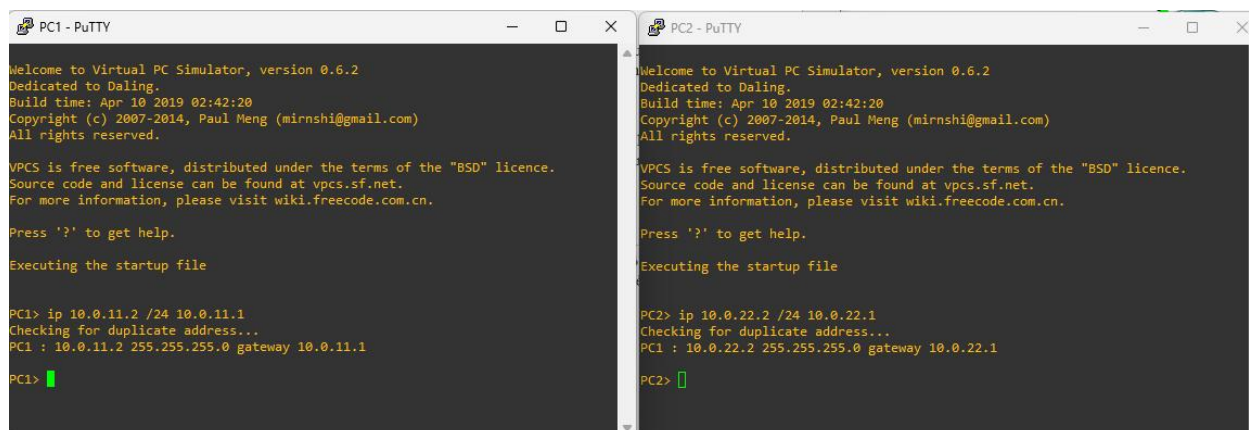
Cả hai giao thức bảo mật đều hoạt động trên các lớp khác nhau của mô hình liên kết hệ thống mở (OSI). Mô hình OSI xác định cấu trúc phân lớp về cách các máy tính trao đổi dữ liệu như thế nào trên một mạng.

Các giao thức IPSec được áp dụng cho mạng và các lớp truyền tải ở giữa mô hình OSI. Trong khi đó, SSL mã hóa dữ liệu trên lớp ứng dụng trên cùng. Bạn có thể kết nối với SSL VPN từ trình duyệt web nhưng phải cài đặt phần mềm riêng để sử dụng IPSec VPN.

## III VPN site to site IPsec trong cisco



## Cấu hình PC1 và PC2



```
PC1 - PuTTY
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC1> ip 10.0.11.2 /24 10.0.11.1
Checking for duplicate address...
PC1 : 10.0.11.2 255.255.255.0 gateway 10.0.11.1
PC1>

PC2 - PuTTY
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

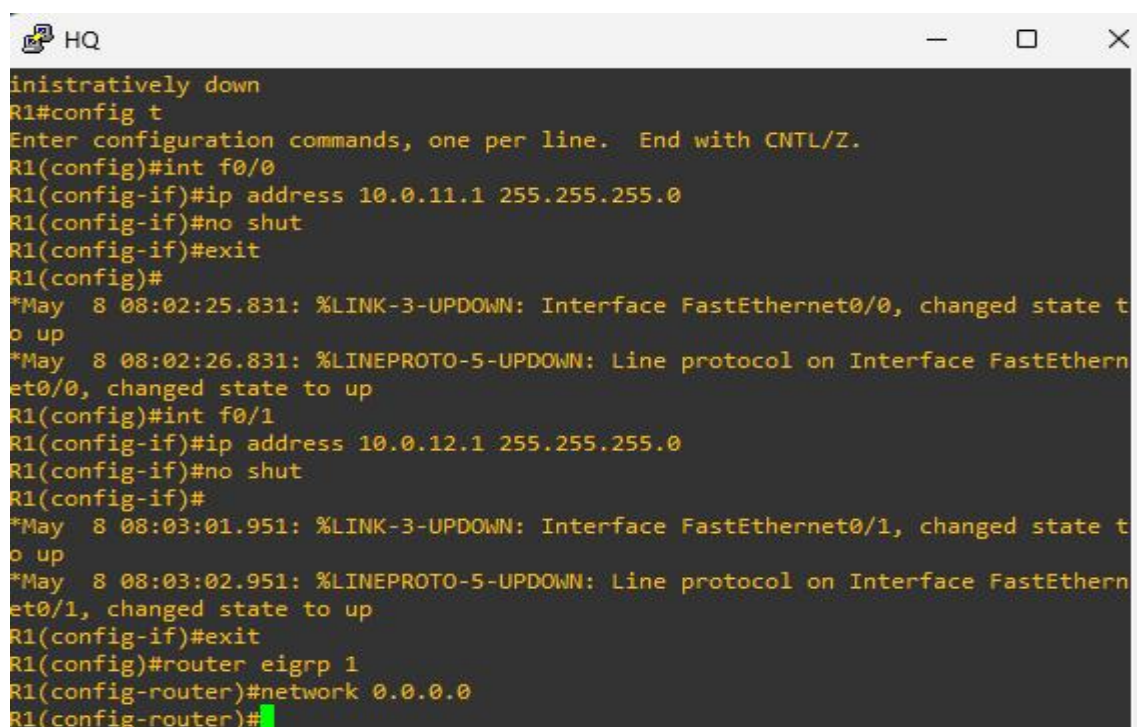
Press '?' to get help.

Executing the startup file

PC2> ip 10.0.22.2 /24 10.0.22.1
Checking for duplicate address...
PC2 : 10.0.22.2 255.255.255.0 gateway 10.0.22.1
PC2>
```

## Cấu hình và định tuyến Router

### ➤ HQ



```
HQ
administratively down
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip address 10.0.11.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
*May  8 08:02:25.831: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*May  8 08:02:26.831: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#int f0/1
R1(config-if)#ip address 10.0.12.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
*May  8 08:03:01.951: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*May  8 08:03:02.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1(config-if)#exit
R1(config)#router eigrp 1
R1(config-router)#network 0.0.0.0
R1(config-router)#
```

### ➤ ISP

```
ISP
ISP(config)#int f0/0
ISP(config-if)#ip addre
ISP(config-if)#ip address 10.0.12.2 255.255.255.0
ISP(config-if)#no shut
ISP(config-if)#
*May  8 08:04:41.983: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*May  8 08:04:42.983: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
ISP(config-if)#exit
ISP(config)#int f0/1
ISP(config-if)#ip add
ISP(config-if)#ip address 10.0.23.2 255.255.255.0
ISP(config-if)#no shut
ISP(config-if)#exit
ISP(config)#router ei
*May  8 08:05:31.111: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*May  8 08:05:32.111: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
ISP(config)#router eigrp 1
ISP(config-router)#network 0.0.0.0
ISP(config-router)#
*May  8 08:05:43.491: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.12.1 (Fast
```

## ➤ Branch

```
Branch
3(config)#int fastEthernet 0/1
3(config-if)#ip address 10.0.23.1 255.255.255.0
3(config-if)#no shut
3(config-if)#exit
3(config)#
May  8 08:06:25.279: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
up
May  8 08:06:26.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
t0/1, changed state to up
3(config)#int f0/0
3(config-if)#ip address 10.0.22.1 255.255.255.0
3(config-if)#no shut
3(config-if)#exit
3(config)#
May  8 08:07:01.487: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
up
May  8 08:07:02.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
t0/0, changed state to up
3(config)#router eigrp 1
3(config-router)#network 0.0.0.0
3(config-router)#
May  8 08:07:16.527: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.23.2 (Fast
thernet0/1) is up: new adjacency
3(config-router)#
```

## ➤ Kiểm tra kết nối



```
PC2 - PuTTY
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> ip 10.0.22.2 /24 10.0.22.1
Checking for duplicate address...
PC1 : 10.0.22.2 255.255.255.0 gateway 10.0.22.1

PC2> ping 10.0.11.2
84 bytes from 10.0.11.2 icmp_seq=1 ttl=61 time=76.762 ms
84 bytes from 10.0.11.2 icmp_seq=2 ttl=61 time=40.156 ms
84 bytes from 10.0.11.2 icmp_seq=3 ttl=61 time=37.859 ms
84 bytes from 10.0.11.2 icmp_seq=4 ttl=61 time=48.409 ms
84 bytes from 10.0.11.2 icmp_seq=5 ttl=61 time=37.802 ms

PC2>
```

## Cấu hình Isec Tunnel

### ➤ HQ

```
HQ
R1(config)#router eigrp 1
R1(config-router)#network 0.0.0.0
R1(config-router)#
*May  8 08:06:43.839: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.12.2 (Fast
Ethernet0/1) is up: new adjacency
R1(config-router)#exit
R1(config)#cry
R1(config)#crypto isa
R1(config)#crypto isakmp po
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encryption des 56
^
% Invalid input detected at '^' marker.

R1(config-isakmp)#encryption des
^
% Invalid input detected at '^' marker.

R1(config-isakmp)#encryption des
R1(config-isakmp)#group 2
R1(config-isakmp)#hash sha
R1(config-isakmp)#exit
R1(config)#cry
R1(config)#crypto
```

IKE policy được tạo ra nhằm xác thực và bảo vệ kết nối quản lý của 2 router. Bạn có thể tạo 1 hoặc nhiều hơn trên router của bạn. bạn có thể làm điều này nếu router của bạn có nhiều peers và mỗi peer có cấu hình xác thực và bảo vệ khác nhau.

1 **IKE policy** chứa rất nhiều tham số như: độ ưu tiên(prioritization), thuật toán mã hoá(encryption), mã hoá 1 chiều (hash) ,kĩ thuật xác thực của bạn (authentication method), DH group, thời gian sống của kết nối (connection lifetime). ở đây là những câu lệnh giúp tạo một policy cho kết nối quản lý

**Crypto isakmp policy** cho ta tạo 1 policy trong kết nối quản lý trên router, mỗi chính sách yêu cầu có 1 số thứ tự (priority or separate number), giá trị càng thấp thì càng ưu tiên giúp router thiết lập kết nối giữa các peer. Vì vậy nên gán chính sách bảo mật cao nhất tương ứng số priority nhỏ nhất và chính sách bảo mật kém an toàn nhất tương ứng với số cao nhất (như 10000). Sau khi gõ lệnh trên ta sẽ tiếp tục chọn các thuật toán mã hoá, xác thực trong cấu hình policy

Lệnh **Encryption** là để chọn thuật toán mã hoá như **DES, 3DES, AES** giúp mã hoá dữ liệu ,tăng cường bảo mật trên đường đi tránh bị kẻ xấu xem dữ liệu

Lệnh **hash** để chọn chức năng **HMAC** như **SHA, SHA1, MD5** là dạng mã hoá 1 chiều nên giúp xác thực người gửi ,ngoài ra còn giúp bảo vệ dữ liệu không bị chỉnh sửa khi đi trong môi trường internet

Lệnh **group** : một khi các peers thiết lập các chính sách bảo vệ để dùng trong kết nối quản lý ở Phase 1, **Diffie-Hellman** (gọi tắt là **DH**) được dùng để tạo ra 1 key chia sẻ. ISAKMP/IKE không có tiến trình chia sẻ key an toàn khi đi qua mạng không an toàn ,thay vì đó những thiết bị sẽ dùng **DH** cho mục đích ngăn chặn kẻ xấu thấy được key đang chia sẻ giữa các thiết bị. Mỗi group sẽ có giá trị riêng, số bit càng cao thì càng an toàn và khó khăn trong việc tìm được key đang chia sẻ.

```
R1(config)#crypto isakmp key 6 cisco address 0.0.0.0
R1(config)#crypto ipse
R1(config)#crypto ipsec tran
R1(config)#crypto ipsec transform-set OUR-SET
% Incomplete command.

R1(config)#crypto ipsec transform-set OUR-SET esp-des esp-
R1(config)#crypto ipsec transform-set OUR-SET esp-des esp-sha-hmac
R1(cfg-crypto-trans)#
```

**Crypto ipsec transform-set** xác định một tập hợp các tham số liên quan đến việc mã hoá và xác thực trong kết nối IPsec.OUR-SET là tên của tập hợp transform. Các tham số được chỉ định là:

**esp-des:** Sử dụng thuật toán mã hoá **DES (Data Encryption Standard)** để bảo vệ dữ liệu.

**esp-sha-hmac:** Sử dụng thuật toán xác thực **SHA (Secure Hash Algorithm)** để đảm bảo tính toàn vẹn của gói tin.

Như vậy, OUR-SET sẽ áp dụng mã hoá DES và xác thực SHA cho lưu lượng trong kết nối IPsec. Điều này đảm bảo rằng dữ liệu được truyền qua mạng công cộng sẽ được bảo vệ và xác thực một cách an toàn.

```
R1(config)#access-list 100
% Incomplete command.

R1(config)#access-list 100 permit ip 10.0.11.0 0.0.0.255 10.0.22.0 0.0.0.255
R1(config)#exit
```

**Access-list 100** là một danh sách kiểm soát truy cập (ACL) được sử dụng để xác định lưu lượng mạng được phép hoặc bị từ chối

```
R1(config)#crypto map OUR-MAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#
```

```
and a valid access list have been configured.
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#set peer 10.0.23.1
R1(config-crypto-map)#set transform-set OUR-SET
R1(config-crypto-map)#exit
R1(config)#int f0/1
R1(config-if)#cry
R1(config-if)#crypto map OUR-MAP
R1(config-if)#
*May 8 08:32:04.751: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Match address 100 xác định rằng crypto map này sẽ áp dụng cho lưu lượng được chỉ định bởi access-list 100. Các thông số mã hoá và cấu hình liên quan sẽ được thực hiện theo hồ sơ ISAKMP tương ứng.

Thiết lập kết nối IPsec giữa thiết bị của bạn và địa chỉ IP đích **10.0.23.1**.

### ➤ Branch

```
R3(config)#crypto isakmp enable
R3(config)#crypto isakmp policy 1
R3(config-isakmp)#encryption des
R3(config-isakmp)#auth
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#hash sha
R3(config-isakmp)#exit
R3(config)#crypto isakmp key 6 cisco addresss 0.0.0.0
                                     ^
% Invalid input detected at '^' marker.

R3(config)#crypto isakmp key 6 cisco address 0.0.0.0
R3(config)#crypto ipsec tran
R3(config)#crypto ipsec transform-set OUR-SET esp-des esp-sha-hmac
R3(cfg-crypto-trans)#exit
R3(config)#
```



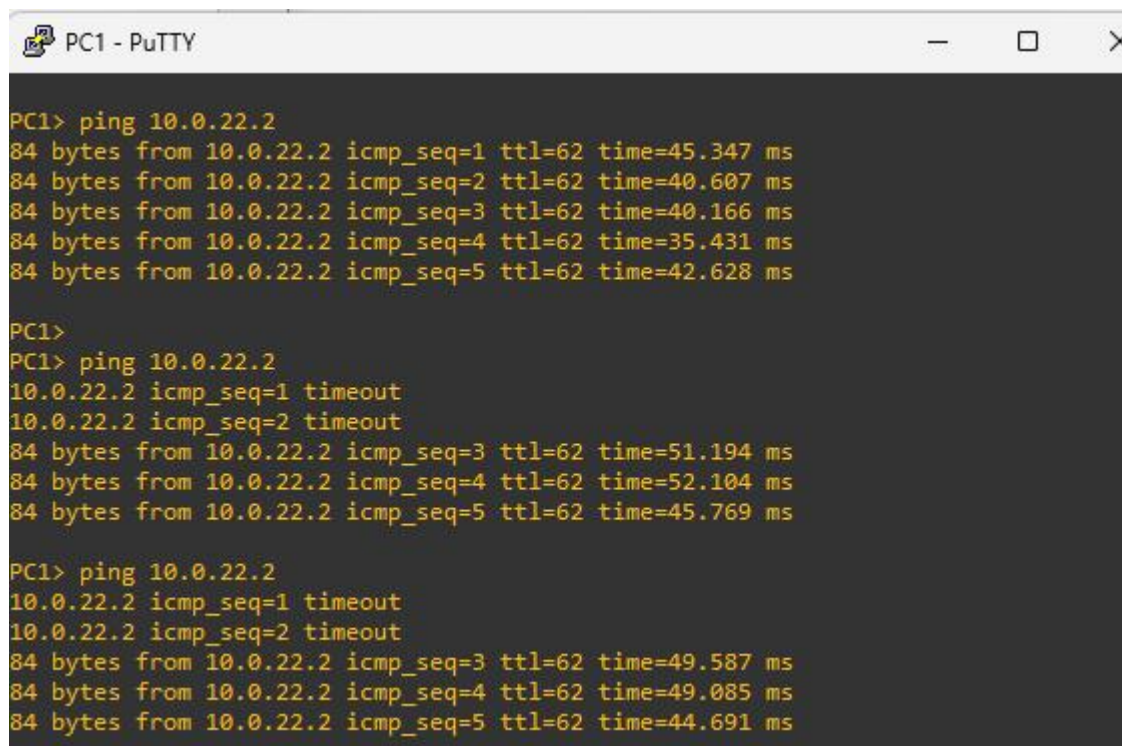
```

R3(config)#access-list 100 permit ip 10.0.22.0 0.0.0.255 10.0.11.0 0.0.0.255
R3(config)#crypto m
R3(config)#crypto map OUR-MAP 1 is
      ^
% Invalid input detected at '^' marker.

R3(config)#crypto map OUR-MAP 1
R3(config)#crypto map OUR-MAP 1 ipsec-isa
R3(config)#crypto map OUR-MAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
R3(config-crypto-map)#match add
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#set peer 10.0.12.1
R3(config-crypto-map)#set tran
R3(config-crypto-map)#set transform-set OUR-SET
R3(config-crypto-map)#exit
R3(config)#int f0/1
R3(config-if)#crypto map OUR-MAP
R3(config-if)#
*May  8 08:36:13.543: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#

```

**Ping từ PC1 tới PC2**



```

PC1> ping 10.0.22.2
84 bytes from 10.0.22.2 icmp_seq=1 ttl=62 time=45.347 ms
84 bytes from 10.0.22.2 icmp_seq=2 ttl=62 time=40.607 ms
84 bytes from 10.0.22.2 icmp_seq=3 ttl=62 time=40.166 ms
84 bytes from 10.0.22.2 icmp_seq=4 ttl=62 time=35.431 ms
84 bytes from 10.0.22.2 icmp_seq=5 ttl=62 time=42.628 ms

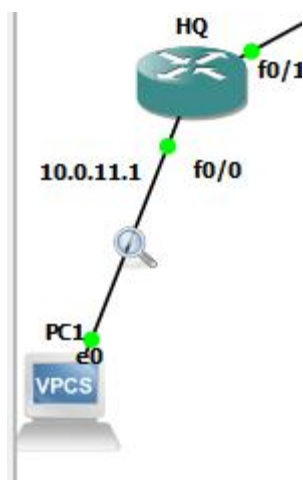
PC1>
PC1> ping 10.0.22.2
10.0.22.2 icmp_seq=1 timeout
10.0.22.2 icmp_seq=2 timeout
84 bytes from 10.0.22.2 icmp_seq=3 ttl=62 time=51.194 ms
84 bytes from 10.0.22.2 icmp_seq=4 ttl=62 time=52.104 ms
84 bytes from 10.0.22.2 icmp_seq=5 ttl=62 time=45.769 ms

PC1> ping 10.0.22.2
10.0.22.2 icmp_seq=1 timeout
10.0.22.2 icmp_seq=2 timeout
84 bytes from 10.0.22.2 icmp_seq=3 ttl=62 time=49.587 ms
84 bytes from 10.0.22.2 icmp_seq=4 ttl=62 time=49.085 ms
84 bytes from 10.0.22.2 icmp_seq=5 ttl=62 time=44.691 ms

```

## Dùng wireshark bắt gói tin

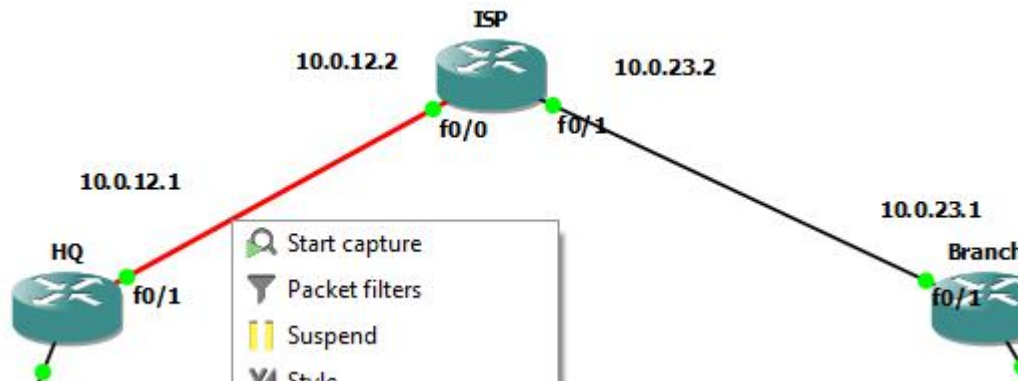
Gói tin không có Ipsec trước khi vào tunnel (thấy được Sourc IP của PC1 10.0.11.2 Dest IP của PC2 10.0.22.2, protocol và cả thông tin gói tin như ở đây là 2 máy Ping tới nhau )





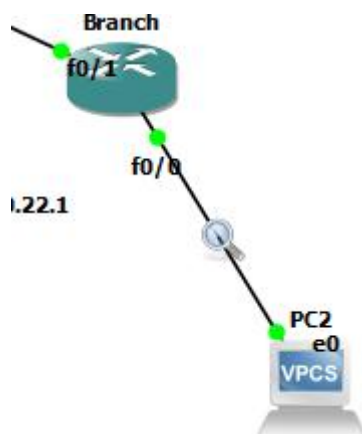
No.	Time	Source	Destination	Protocol	Length	Info
3	4.650389	10.0.11.1	224.0.0.10	EIGRP	74	Hello
4	9.611358	10.0.11.1	224.0.0.10	EIGRP	74	Hello
5	12.441420	ca:01:05:b3:00:08	CDP/VTP/DTP/PAGP/UD...	CDP	350	Device ID: R1 Port ID: FastEthernet0/0
6	13.497635	ca:01:05:b3:00:08	ca:01:05:b3:00:08	LOOP	60	Reply
7	14.274381	10.0.11.1	224.0.0.10	EIGRP	74	Hello
8	19.172480	10.0.11.1	224.0.0.10	EIGRP	74	Hello
9	22.571154	00:50:79:66:68:00	Broadcast	ARP	64	Who has 10.0.11.1? Tell 10.0.11.2
10	22.574548	ca:01:05:b3:00:08	00:50:79:66:68:00	ARP	60	10.0.11.1 is at ca:01:05:b3:00:08
11	22.586319	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0x1449, seq=1/256, ttl=64
12	23.508079	ca:01:05:b3:00:08	ca:01:05:b3:00:08	LOOP	60	Reply
13	23.612028	10.0.11.1	224.0.0.10	EIGRP	74	Hello
14	24.601712	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0x1649, seq=2/512, ttl=64
15	25.655853	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0x1449, seq=1/256, ttl=62
16	25.655918	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0x1649, seq=2/512, ttl=62
17	26.609062	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0x1849, seq=3/768, ttl=64
18	26.650949	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0x1849, seq=3/768, ttl=62
19	27.662460	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0x1949, seq=4/1024, ttl=64
20	27.706414	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0x1949, seq=4/1024, ttl=62
21	28.600178	10.0.11.1	224.0.0.10	EIGRP	74	Hello
22	28.718884	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0x1a49, seq=5/1280, ttl=64
23	28.755654	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0x1a49, seq=5/1280, ttl=62
24	33.256081	10.0.11.1	224.0.0.10	EIGRP	74	Hello
25	33.503934	ca:01:05:b3:00:08	ca:01:05:b3:00:08	LOOP	60	Reply
26	37.515830	10.0.11.1	224.0.0.10	EIGRP	74	Hello

Gói tin có Isec trong tunnel ( không lộ Sourc IP của PC1 10.0.11.2, Dest IP của PC2 10.0.22.2 và thông tin gói tin)



No.	Time	Source	Destination	Protocol	Length	Info
5	4.804012	10.0.12.2	224.0.0.10	EIGRP	74	Hello
6	6.651585	10.0.12.1	224.0.0.10	EIGRP	74	Hello
7	9.752880	10.0.12.2	224.0.0.10	EIGRP	74	Hello
8	11.576063	10.0.12.1	224.0.0.10	EIGRP	74	Hello
9	12.010864	ca:01:05:b3:00:06	ca:01:05:b3:00:06	LOOP	60	Reply
10	13.759959	10.0.12.1	10.0.23.1	ESP	166	ESP (SPI=0x97ad53ed)
11	13.889435	ca:03:06:21:00:08	ca:03:06:21:00:08	LOOP	60	Reply
12	14.734676	10.0.12.2	224.0.0.10	EIGRP	74	Hello
13	15.771522	10.0.12.1	10.0.23.1	ESP	166	ESP (SPI=0x97ad53ed)
14	16.206109	10.0.12.1	224.0.0.10	EIGRP	74	Hello
15	16.785703	10.0.23.1	10.0.12.1	ESP	166	ESP (SPI=0x2aa59002)
16	16.785735	10.0.23.1	10.0.12.1	ESP	166	ESP (SPI=0x2aa59002)
17	17.775581	10.0.12.1	10.0.23.1	ESP	166	ESP (SPI=0x97ad53ed)
18	17.809488	10.0.23.1	10.0.12.1	ESP	166	ESP (SPI=0x2aa59002)
19	18.840097	10.0.12.1	10.0.23.1	ESP	166	ESP (SPI=0x97ad53ed)
20	18.877073	10.0.23.1	10.0.12.1	ESP	166	ESP (SPI=0x2aa59002)
21	19.187878	10.0.12.2	224.0.0.10	EIGRP	74	Hello
22	19.897182	10.0.12.1	10.0.23.1	ESP	166	ESP (SPI=0x97ad53ed)
23	19.933033	10.0.23.1	10.0.12.1	ESP	166	ESP (SPI=0x2aa59002)
24	21.017875	10.0.12.1	224.0.0.10	EIGRP	74	Hello
25	22.005485	ca:01:05:b3:00:06	ca:01:05:b3:00:06	LOOP	60	Reply
26	23.894424	ca:03:06:21:00:08	ca:03:06:21:00:08	LOOP	60	Reply
27	23.956361	10.0.12.2	224.0.0.10	EIGRP	74	Hello
28	25.683497	10.0.12.1	224.0.0.10	EIGRP	74	Hello

## Gói tin không có Isec sau khi ra khỏi tunnel ( tương tự trước tunnel)



nolpsec-afterTunnel.pcapng [Branch FastEthernet0/0 to PC2 Ethernet0]

No.	Time	Source	Destination	Protocol	Length	Info
12	34.047255	10.0.22.1	224.0.0.10	EIGRP	74	Hello
13	38.304672	ca:02:05:f7:00:08	CDP/VTP/DTP/PAGP/UD...	CDP	350	Device ID: R3 Port ID: FastEthernet0/0
14	38.785209	10.0.22.1	224.0.0.10	EIGRP	74	Hello
15	40.558753	ca:02:05:f7:00:08	ca:02:05:f7:00:08	LOOP	60	Reply
16	42.444331	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0xe64a, seq=1/256, ttl=62
17	42.444692	00:50:79:66:68:01	Broadcast	ARP	64	Who has 10.0.22.1? Tell 10.0.22.2
18	42.454619	ca:02:05:f7:00:08	00:50:79:66:68:01	ARP	60	10.0.22.1 is at ca:02:05:f7:00:08
19	43.459200	00:50:79:66:68:01	Broadcast	ARP	64	Who has 10.0.22.1? Tell 10.0.22.2
20	43.462486	ca:02:05:f7:00:08	00:50:79:66:68:01	ARP	60	10.0.22.1 is at ca:02:05:f7:00:08
21	43.776998	10.0.22.1	224.0.0.10	EIGRP	74	Hello
22	44.453130	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0xe84a, seq=2/512, ttl=62
23	44.460567	00:50:79:66:68:01	Broadcast	ARP	64	Who has 10.0.22.1? Tell 10.0.22.2
24	44.463578	ca:02:05:f7:00:08	00:50:79:66:68:01	ARP	60	10.0.22.1 is at ca:02:05:f7:00:08
25	45.462750	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0xe64a, seq=1/256, ttl=64
26	45.462927	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0xe84a, seq=2/512, ttl=64
27	46.453197	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0xea4a, seq=3/768, ttl=62
28	46.453442	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0xea4a, seq=3/768, ttl=64
29	47.517029	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0xeb4a, seq=4/1024, ttl=62
30	47.517422	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0xeb4a, seq=4/1024, ttl=64
31	48.058128	10.0.22.1	224.0.0.10	EIGRP	74	Hello
32	48.578205	10.0.11.2	10.0.22.2	ICMP	98	Echo (ping) request id=0xec4a, seq=5/1280, ttl=62
33	48.578567	10.0.22.2	10.0.11.2	ICMP	98	Echo (ping) reply id=0xec4a, seq=5/1280, ttl=64
34	50.617806	ca:02:05:f7:00:08	ca:02:05:f7:00:08	LOOP	60	Reply
35	53.072736	10.0.22.1	224.0.0.10	EIGRP	74	Hello

## Decrypt ipsec khi không sử dụng thuật toán mã hóa

Đôi khi bạn muốn xem đường hầm và các chế độ truyền tải hoạt động như thế nào với tính năng đóng gói, đặc biệt là khi sử dụng GRE trên IPSEC và bạn muốn giải mã gói ESP hoặc IPSEC để xem gói GRE được đóng gói như thế nào với hai chế độ, đặc biệt là cho việc học tập, giảng dạy hoặc có thể để khắc phục sự cố.

Định cấu hình mã hóa ESP bằng null trong bộ biến đổi.

```
crypto ipsec transform-set TS esp-null esp-sha-hmac
```

Sao chép pre-shared key được cấu hình ở ISAKMP giai đoạn 1.

```
crypto isakmp key cisco address 23.0.0.1
```

Mở wireshark. nhấp chuột phải vào gói ESP, trong trường hợp này là ESP SA từ nguồn 12.0.0.1 đến đích 23.0.0.1. Trong Protocol Preferences, hãy chọn ba tùy chọn được hiển thị bên dưới.



No.	Time	Source	Destination	Protocol	Length	Info
7	7.948776...	12.0.0.1	23.0.0.1	ESP	162	ESP (SPI=0xdc1f45c1)[Malformed Packet]
8	10.00340...	aa:bb:cc:00:0...	aa:bb:cc:00:0...	LOOP	60	Reply
9	10.52017...	23.0.0.1	12.0.0.1	ESP	162	ESP (SPI=0x70fc225e)
10	12.37226...	12.0.0.1	23.0.0.1	ESP	162	ESP (SPI=0xdc1f45c1)
11	14.90114...	23.0.0.1	12.0.0.1			
12	17.20364...	12.0.0.1	23.0.0.1			
13	17.52322...	aa:bb:cc:00:0...	aa:bb:cc:00:0...			
14	19.38364...	23.0.0.1	12.0.0.1			
15	20.00480...	aa:bb:cc:00:0...	aa:bb:cc:00:0...			
16	22.18507...	12.0.0.1	23.0.0.1			
17	24.19585...	23.0.0.1	12.0.0.1			

Frame 10: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface eth0, id 0

Ethernet II, Src: aa:bb:cc:00:01:00 (aa:bb:cc:00:01:00), Dst: 23:00:aa:bb:cc:00:02:00 (aa:bb:cc:00:02:00)

Internet Protocol Version 4, Src: 12.0.0.1, Dst: 23.0.0.1

Encapsulating Security Payload

ESP SPI: 0xdc1f45c1 (3693036993)

ESP Sequence: 253

Mark/Unmark Packet(s) Ctrl+M

Ignore/Unignore Packet(s) Ctrl+D

Set/Unset Time Reference Ctrl+T

Time Shift... Ctrl+Shift+T

Packet Comment... Ctrl+Alt+C

Edit Resolved Name

Apply as Filter

Prepare as Filter

Conversation Filter

Colorize Conversation

SCTP

Follow

Copy

Protocol Preferences

Decode As...

Show Packet in New Window

Open Encapsulating Security Payload preferences...

☒ Attempt to detect/decode NULL encrypted ESP payloads

☒ Check sequence numbers of ESP frames

☒ Attempt to detect/decode encrypted ESP payloads

☐ Attempt to Check ESP Authentication

ESP SAs...

Disable ESP...

```

0000 aa bb cc 00 02 00 aa bb cc 00 01 00 08 00 45 c0 .....E
0010 00 94 03 07 00 00 ff 32 94 6f 0c 00 00 01 17 00 .....2..o
0020 00 01 dc 1f 45 c1 00 00 00 fd 45 c0 00 54 01 03 ....E...E.T
0030 00 00 ff 2f 96 b6 0c 00 00 01 17 00 00 01 00 00 ....//...
0040 08 00 45 c0 00 3c 01 fa 00 00 01 58 29 95 ac 10 ..E.<...X)
0050 01 01 e0 00 00 0a 02 05 e2 d1 00 00 00 00 00 00 .....
0060 00 00 00 00 00 00 00 00 00 01 00 01 00 0c 01 00 .....
0070 01 00 00 00 00 00 0f 00 04 00 08 17 00 02 00 01 02 .....
0080 02 04 0e df d4 ff 62 b4 c2 0d 6f f1 a1 c9 3a 70 .....b..o...p
0090 40 0c 0b 30 06 41 af f3 eb 5c 6c e3 2f b0 92 7f @..0.A.. \./...
00a0 c5 1c

```

Mở rộng Encapsulation Security Payload và sao chép giá trị SPI cho ESP SA này.  
*0xdc1f45c1*

No.	Time	Source	Destination	Protocol	Length	Info
80	118.371...	23.0.0.1	12.0.0.1	ESP	162	ESP (SPI=0x70fc225e)[Malformed Packet]
81	120.018...	aa:bb:cc:00:0...	aa:bb:cc:00:0...	LOOP	60	Reply
82	121.274...	12.0.0.1	23.0.0.1	ESP	162	ESP (SPI=0xdc1f45c1)
83	123.197...	23.0.0.1	12.0.0.1	ESP	162	ESP (SPI=0x70fc225e)[Malformed Packet]
84	126.085...	12.0.0.1	23.0.0.1	ESP	162	ESP (SPI=0xdc1f45c1)
85	127.556...	aa:bb:cc:00:0...	aa:bb:cc:00:0...	LOOP	60	Reply
86	128.178...	23.0.0.1	12.0.0.1	ESP	162	ESP (SPI=0x70fc225e)
87	130.020...	aa:bb:cc:00:0...	aa:bb:cc:00:0...	LOOP	60	Reply
88	130.392...	12.0.0.1	23.0.0.1	ESP	162	ESP (SPI=0xdc1f45c1)

Frame 84: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface eth0, id 0

Ethernet II, Src: aa:bb:cc:00:01:00 (aa:bb:cc:00:01:00), Dst: aa:bb:cc:00:02:00 (aa:bb:cc:00:02:00)

Internet Protocol Version 4, Src: 12.0.0.1, Dst: 23.0.0.1

Encapsulating Security Payload

ESP SPI: 0xdc1f45c1 (3693036993)

ESP Sequence: 89

Quay lại Protocol Preferences nhập vào ESP SA.

Nhập các thông tin liên quan đến ESP SA.

**Protocol:** IPv4

**Source IP:** 12.0.0.1

**Destination IP:** 23.0.0.1

**SPI:** 0xdc1f45c1

**Encryption:** NULL

**Authentication:** HMAC-SHA-1-96[RFC2404]

**Authentication Key:** cisco

Bấm OK, bạn sẽ thấy gói IPsec ở dạng văn bản rõ ràng.

No.	Time	Source	Destination	Protocol	Length	Info
50	71.7279...	23.0.0.1	12.0.0.1	ESP	162	ESP (SPI=0x70fc225e)
51	72.0365...	172.16.1.1	224.0.0.10	EIGRP	162	Hello
52	72.4964...	aa:bb:cc:00...	aa:bb:cc:00...	LOOP	60	Reply
53	74.8435...	10.1.1.10	10.3.3.10	ICMP	202	Echo (ping) request id=0x0000, seq=0/0, ttl=254 (no response found!)
54	74.8465...	23.0.0.1	12.0.0.1	ESP	202	ESP (SPI=0x70fc225e)
55	74.8479...	10.1.1.10	10.3.3.10	ICMP	202	Echo (ping) request id=0x0000, seq=1/256, ttl=254 (no response found!)
56	74.8499...	23.0.0.1	12.0.0.1	ESP	202	ESP (SPI=0x70fc225e)
57	74.8513...	10.1.1.10	10.3.3.10	ICMP	202	Echo (ping) request id=0x0000, seq=2/512, ttl=254 (no response found!)
58	74.8529...	23.0.0.1	12.0.0.1	ESP	202	Unknown IP Protocol: SATNET Monitoring (69)
59	74.8541...	10.1.1.10	10.3.3.10	ICMP	202	Echo (ping) request id=0x0000, seq=3/768, ttl=254 (no response found!)
* Frame 61: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits) on interface eth0, id 0						
Ethernet II, Src: aa:bb:cc:00:01:00 (aa:bb:cc:00:01:00), Dst: aa:bb:cc:00:02:00 (aa:bb:cc:00:02:00)						
Internet Protocol Version 4, Src: 12.0.0.1, Dst: 23.0.0.1						
Encapsulating Security Payload						
Internet Protocol Version 4, Src: 12.0.0.1, Dst: 23.0.0.1						
Generic Routing Encapsulation (IP)						
Internet Protocol Version 4, Src: 10.1.1.10, Dst: 10.3.3.10						
Internet Control Message Protocol						