**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

**BỘ MÔN KỸ THUẬT MÁY TÍNH**

---------------o0o---------------



**Bài tập lớn: Nhập môn an toàn thông tin**

**IPSEC, GIAO THỨC VÀ VPN**

**GVHD: PGS.TS Nguyễn Linh Giang**

**SVTH: Nguyễn Văn Hải – 20173089**

**Phạm Thanh Hải – 20175627**

**Lương Thế Huy - 20173172**

**Lê Đình Bình - 20172971**

**TP. HÀ NỘI, THÁNG 5 NĂM 202**

**Danh mục hình ảnh**

[Hình 1 Ứng dụng của IPSec 2](#_Toc42514725)

[Hình 2 Kiến trúc của IPSec 3](#_Toc42514726)

[Hình 3 Cấu trúc gói tín AH 5](#_Toc42514727)

[Hình 4 Khuôn dạng gói tin IPv4 trước và sau khi xử lý AH ở kiểu Transport 7](#_Toc42514728)

[Hình 5 Khuôn dạng gói tin IPv6 trước và sau khi xử lý AH ở kiểu Transport 7](#_Toc42514729)

[Hình 6 Khuôn dạng gói tin đã xử lý AH ở kiểu Tunnel 8](#_Toc42514730)

[Hình 7 Phân mảnh và xác thức: Transport Mode host – host SA 9](#_Toc42514731)

[Hình 8 Phân mảnh và xác thực: Tunnel Mode gateway – gateway SA 10](#_Toc42514732)

[Hình 9 Xử lý đóng gói ESP 12](#_Toc42514733)

[Hình 10 Chi tiết gói ESP 13](#_Toc42514734)

[Hình 11 Khuôn dạng IPv4 trước và sau khi xử lý ESP theo kiểu Transport 14](#_Toc42514735)

[Hình 12 Khuôn dạng gói tin Ipv6 trước và sau khi xử lý ESP kiểu Transport 14](#_Toc42514736)

[Hình 13 Khuôn dạng gói tin đã xử lý ESP kiểu tunnel 15](#_Toc42514737)

[Hình 14 Các quá trình của IKE 19](#_Toc42514738)

[Hình 15 Quá trình trao đổi message thỏa thuận giữa các bên 20](#_Toc42514739)

[Hình 16 Quá trình chứng thực giữa các bên 20](#_Toc42514740)

[Hình 17 Quá trình NAT 22](#_Toc42514741)

[Hình 18 NAT Travesal 22](#_Toc42514742)

[Hình 19 Cấu hình địa chỉ IP các máy 23](#_Toc42514743)

[Hình 20 Gói tin gửi đến ISP 26](#_Toc42514744)

[Hình 21 Phân tích gói tin tại ISP 26](#_Toc42514745)

[Hình 22 Phân tích gói tin tại ISP 27](#_Toc42514746)

[Hình 23 Gói tin được nhận bới máy đích 27](#_Toc42514747)

**MỤC LỤC**

Nội dung

[I. LÝ THUYẾT 1](#_Toc42513808)

[1. Khái niệm về IPSec 1](#_Toc42513809)

[1.1 Khái niệm 1](#_Toc42513810)

[1.2 Đánh giá IPSec 1](#_Toc42513811)

[2. Ứng dụng của IPSec 2](#_Toc42513812)

[3. Kiến trúc của IPSec 3](#_Toc42513813)

[4. Giao thức đóng gói 4](#_Toc42513814)

[4.1. Giao thức AH 4](#_Toc42513815)

[4.1 Giao thức ESP 11](#_Toc42513816)

[5. Giao thức trao đổi khóa 18](#_Toc42513817)

[5.1 Giới thiệu 18](#_Toc42513818)

[5.2 Các quá trình của IKE 19](#_Toc42513819)

[5.3 Các chức năng khác của IKE giúp cho IKE hoạt động tối ưu hơn bao gồm: 21](#_Toc42513820)

[6. Tính năng của IPSec trong VPN 22](#_Toc42513821)

[II. THIẾT KẾ VÀ TRIỂN KHAI DEMO về IPSec trong VPN 23](#_Toc42513822)

[1. Xây dựng hệ thống mạng như trong hình dưới 23](#_Toc42513823)

[2. Cấu hình các route: 23](#_Toc42513824)

[3. Phân tích gói tin gửi từ mạng R1 đến mạng R3 26](#_Toc42513825)

# LÝ THUYẾT

## Khái niệm về IPSec

### 1.1 Khái niệm

Giao thức TCP/IP đóng một vai trò rất quan trọng trong các hệ thống hiện nay. Về nguyên tắc, có nhiều tùy chọn khác nhau về giao thức để triển khai các hệ thống mạng như TCP/IP, TPX/SPX, NetBEUI, Apple talk,… Tuy nhiên TCP/IP là sự lựa chọn gần như bắt buộc do giao thức này được sử dụng làm giao thức nền tảng của mạng Internet.

Vào thời điểm thiết kế giao thức này, vấn đề bảo mật thông tin chưa thật sự được quan tâm, do đó, các giao thức trong bộ TCP/IP hầu như không được trang bị bất cứ giao thức nào. Cấu trúc gói dữ liệu (IP, TCP,UDP và cả các giao thức ứng dụng) được mô tả công khai, bắt được gói IP trên mạng, ai cũng có thể phân tích gói để đọc phần dữ liệu chứa bên trong, đó là chưa kể hiện nay, các công cụ bắt và phân tích gói được xây dựng với tính năng mạnh và phát hành rộng rãi. Việc bổ sung các cơ chế bảo mật vào mô hình TCP/IP, bắt đầu từ giao thức IP là một nhu cầu cấp bách.

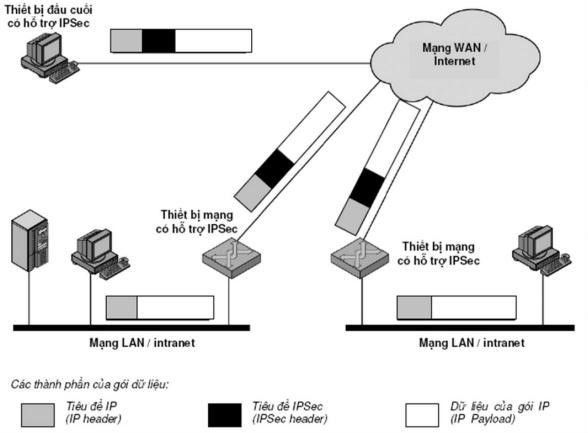
IP Security (IPSec – Internet Protocol Security) là một giao thức được chuẩn hoá bởi IETF (Internet Engineering Task Force) từ năm 1998 nhằm mục đích nâng cấp các cơ chế mã hoá và xác thực thông tin cho chuỗi thông tin truyền đi trên mạng bằng giao thức IP. Hay nói cách khác, IPSec là sự tập hợp của các chuẩn mở được thiết lập để đảm bảo sự cẩn mật dữ liệu, đảm bảo tính toàn vẹn dữ liệu và chứng thực dữ liệu giữa các thiết bị mạng.

### 1.2 Đánh giá IPSec

1. Ưu điểm
   * 1. Khi IPSec được triển khai trên bức tường lửa hoặc bộ định tuyến của một mạng riêng, thì tính năng an toàn của IPSec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan đến bảo mật.
     2. IPSec được thực hiện bên dưới lớp TCP và UDP, đồng thời nó hoạt động trong suốt đối với các lớp này. Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi IPSec được triển khai.
     3. IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối, điều này giúp che giấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua mạng Internet.
2. Hạn chế
   * 1. Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
     2. IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
     3. Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
     4. Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

## Ứng dụng của IPSec

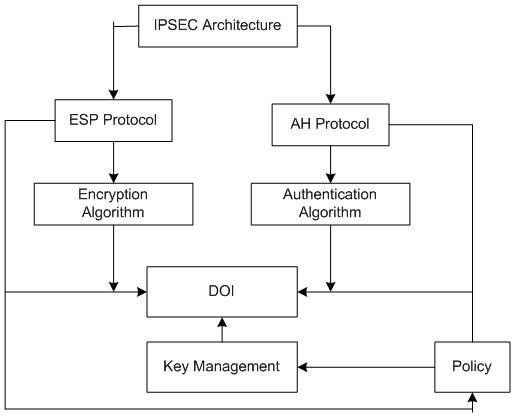
* + Bảo vệ kết nối từ các mạng chi nhánh đến mạng trung tâm thông qua Internet.
  + Bảo vệ kết nối truy cập từ xa (Remote Access).
  + Thiết lập các kết nối Intranet và Extranet .
  + Nâng cao tính bảo mật của các giao dịch thương mại điện tử



Hình Ứng dụng của IPSec

## Kiến trúc của IPSec

IPSec là một giao thức phức tạp, dựa trên nền của nhiều kỹ thuật cơ sở khác nhau như mật mã, xác thực, trao đổi khoá… Xét về mặt kiến trúc, IPSec được xây dựng dựa trên các thành phần cơ bản sau đây, mỗi thành phần được định nghĩa trong một tài liệu riêng tương ứng:



Hình Kiến trúc của IPSec

* Kiến trúc IPSec (RFC 2401): Quy định các cấu trúc, các khái niệm và yêu cầu của IPSec.
* Giao thức ESP (RFC 2406): Mô tả giao thức ESP, là một giao thức mật mã và xác thực thông tin trong IPSec.
* Giao thức AH (RFC 2402): Định nghĩa một giao thức khác với chức năng gần giống ESP. Như vậy khi triển khai IPSec, người sử dụng có thể chọn dùng ESP hoặc AH, mỗi giao thức có ưu và nhược điểm riêng.
* Thuật toán mật mã: Định nghĩa các thuật toán mã hoá và giải mã sử dụng trong IPSec. IPSec chủ yếu dựa vào các thuật toán mã hoá đối xứng.
* Thuật toán xác thực: Định nghĩa các thuật toán xác thực thông tin sử dụng trong AH và ESP.
* Quản lý khoá (RFC 2408): Mô tả các cơ chế quản lý và trao đổi khoá trong IPSec.
* Miền thực thi (Domain of Interpretation – DOI): Định nghĩa môi trường thực thi IPSec. IPSec không phải là một công nghệ riêng biệt mà là sự tổ hợp của nhiều cơ chế, giao thức và kỹ thuật khác nhau, trong đó mỗi giao thức, cơ chế đều có nhiều chế độ hoạt động khác nhau. Việc xác định một tập các chế độ cần thiết để triển khai IPSec trong một tình huống cụ thể là chức năng của miền thực thi. Xét về mặt ứng dụng, IPSec thực chất là một giao thức hoạt động song song với IP nhằm cung cấp 2 chức năng cơ bản mà IP nguyên thuỷ chưa có, đó là mã hoá và xác thực gói dữ liệu.

Một cách khái quát có thể xem IPSec là một tổ hợp gồm hai thành phần:

* Giao thức đóng gói, gồm AH và ESP: bảo về truyền thông IP, dựa vào SA (khóa, địa chỉ, các thuật toán mật mã)
* Giao thức trao đổi khoá IKE (Internet Key Exchange): để thiết lập các SA (Security Association) cho AH hoặc ESP, và duy trì/quản lý các kết nối

## Giao thức đóng gói

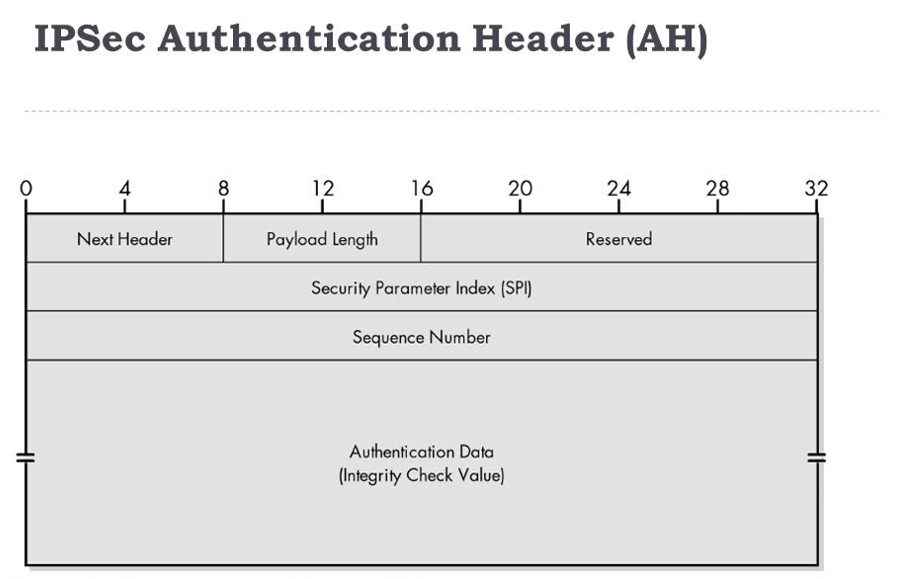
### 4.1. Giao thức AH

* + 1. Giới thiệu

AH cung cấp xác thực nguồn gốc dữ liệu (data origin authentication), kiểm tra tính toàn vẹn dữ liệu (data integrity), và dịch vụ chống phát lại (anti-replay service). Đến đây, cần phải phân biệt được hai khái niệm toàn vẹn dữ liệu và chống phát lại: toàn vẹn dữ liệu là kiểm tra những thay đổi của từng gói tin IP, không quan tâm đến vị trí các gói trong luồng lưu lượng; còn dịch vụ chống phát lại là kiểm tra sự phát lặp lại một gói tin tới địa chỉ đích nhiều hơn một lần. AH cho phép xác thực các trường của IP header cũng như dữ liệu của các giao thức lớp trên, tuy nhiên do một số trường của IP header thay đổi trong khi truyền và phía phát có thể không dự đoán trước được giá trị của chúng khi tới phía thu, do đó giá trị của các trường này không bảo vệ được bằng AH. Có thể nói AH chỉ bảo vệ một phần của IP header mà thôi. AH không cung cấp bất cứ xử lý nào về bảo mật dữ liệu của các lớp trên, tất cả đều được truyền dưới dạng văn bản rõ. AH nhanh hơn ESP, nên có thể chọn AH trong trường hợp chắc chắn về nguồn gốc và tính toàn vẹn của dữ liệu nhưng tính bảo mật dữ liệu không cần được chắc chắn.

Giao thức AH cung cấp chức năng xác thực bằng cách thực hiện một hàm băm một chiều (one-way hash function) đối với dữ liệu của gói để tạo ra một đoạn mã xác thực (hash hay message digest). Đoạn mã đó được chèn vào thông tin của gói truyền đi. Khi đó, bất cứ thay đổi nào đối với nội dung của gói trong quá trình truyền đi đều được phía thu phát hiện khi nó thực hiện cùng với một hàm băm một chiều đối với gói dữ liệu thu được và đối chiếu nó với giá trị hash đã truyền đi. Hàm băm được thực hiện trên toàn bộ gói dữ liệu, trừ một số trường trong IP header có giá trị bị thay đổi trong quá trình truyền mà phía thu không thể dự đoán trước được (ví dụ trường thời gian sống của gói tin bị các router thay đổi trên đường truyền dẫn)

* + 1. Cấu trúc gói tin AH



Hình Cấu trúc gói tín AH

• Next Header (tiêu đề tiếp theo): Có độ dài 8 bits để nhận dạng loại dữ liệu của phần tải tin theo sau AH. Giá trị này được chọn lựa từ tập các số giao thức IP đã được định nghĩa trong các RFC gần đây nhất.

• Payload length (độ dài tải tin): Có độ dài 8 bits và chứa độ dài của tiêu đề AH được diễn tả trong các từ 32 bit, trừ 2. Ví dụ trong trường hợp của thuật toán toàn vẹn mà mang lại một giá trị xác minh 96 bit (3x32 bit), cộng với 3 từ 32 bits đã cố định, trường độ dài này có giá trị là 4. Với IPv6, tổng độ dài của tiêu đề phải là bội của các khối 8.

• Reserved (dự trữ): Trường 16 bits này dự trữ cho ứng dụng trong tương lai

• Security Parameters Index (SPI: chỉ dẫn thông số an ninh): Trường này có độ dài 32 bit, mang tính chất bắt buộc.

• Sequence Number (số thứ tự): Đây là trường 32 bits không đánh dấu chứa một giá trị mà khi mỗi gói được gửi đi thì tăng một lần. Trường này có tính bắt buộc. Bên gửi luôn luôn bao gồm trường này ngay cả khi bên nhận không sử dụng dịch vụ chống phát lại. Bộ đếm bên gửi và nhận được khởi tạo ban đầu là 0, gói đầu tiên có số thứ tự là 1. Nếu dịch vụ chống phát lại được sử dụng, chỉ số này không thể lặp lại, sẽ có một yêu cầu kết thúc phiên truyền thông và SA sẽ được thiết lập mới trở lại trước khi truyền 232 gói mới.

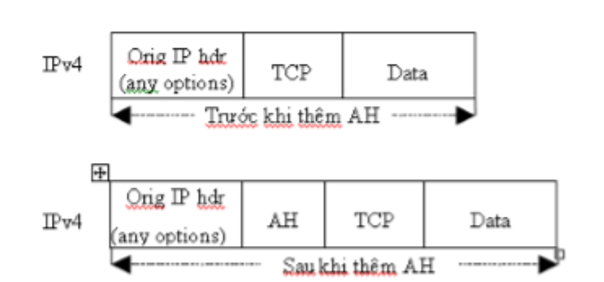
• Authentication Data (dữ liệu nhận thực): Còn được gọi là ICV (Integrity Check Value: giá trị kiểm tra tính toàn vẹn) có độ dài thay đổi, bằng số nguyên lần của 32 bit đối với IPv4 và 64 bit đối với IPv6, và có thể chứa đệm để lấp đầy cho đủ là bội số các bit như trên. ICV được tính toán sử dụng thuật toán nhận thực, bao gồm mã nhận thực bản tin (Message Authentication Code MACs). MACs đơn giản có thể là thuật toán mã hóa MD5 hoặc SHA-1. Các khóa dùng cho mã hóa AH là các khóa xác thực bí mật được chia sẻ giữa các phần truyền thông có thể là một số ngẫu nhiên, không phải là một chuỗi có thể đoán trước của bất cứ loại nào. Tính toán ICV được thực hiện sử dụng gói tin mới đưa vào. Bất kì trường có thể biến đổi của IP header nào đều được cài đặt bằng 0, dữ liệu lớp trên được giả sử là không thể biến đổi. Mỗi bên tại đầu cuối IP-VPN tính toán ICV này độc lập. Nếu ICV tính toán được ở phía thu và ICV được phía phát truyền đến khi so sánh với nhau mà không phù hợp thì gói tin bị loại bỏ, bằng cách như vậy sẽ đảm bảo rằng gói tin không bị giả mạo

* + 1. Quá trình xử lý AH

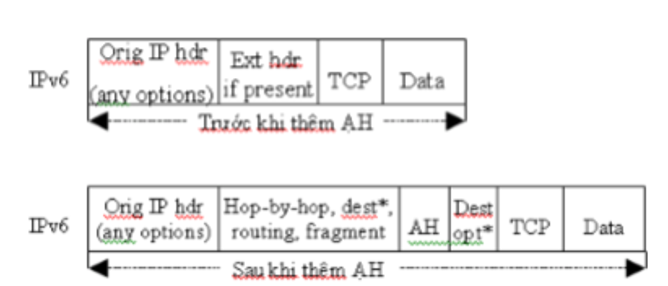
1. Vị trí của AH

AH có hai kiểu hoạt động, đó là kiểu Transport và kiểu Tunnel. Kiểu Transport là kiểu đầu tiên được sử dụng cho kết nối đầu cuối giữa các host hoặc các thiết bị hoạt động như host và kiểu Tunnel được sử dụng cho các ứng dụng còn lại.

Ở kiểu Transport cho phép bảo vệ các giao thức lớp trên, cùng với một số trường trong IP header. Trong kiểu này, AH được chèn vào sau IP header và trước một giao thức lớp trên (chẳng hạn như TCP, UDP, ICMP…) và trước các IPSec header đã được chen vào. Đối với IPv4, AH đặt sau IP header và trước giao thức lớp trên (ví dụ ở đây là TCP). Đối với IPv6, AH được xem như phần tải đầu cuối-tới - đầu cuối, nên sẽ xuất hiện sau các phần header mở rộng hop-to-hop, routing và fragmentation. Các lựa chọn đích (dest options extension headers) có thể trước hoặc sau AH.



Hình Khuôn dạng gói tin IPv4 trước và sau khi xử lý AH ở kiểu Transport



Hình Khuôn dạng gói tin IPv6 trước và sau khi xử lý AH ở kiểu Transport

Trong kiểu Tunnel, inner IP header mang địa chỉ nguồn và đích cuối cùng, còn outer IP header mang địa chỉ để định tuyến qua Internet. Trong kiểu này, AH bảo vệ toàn bộ gói tin IP bên trong, bao gồm cả inner IP header (trong khi AH Transport chỉ bảo vệ một số trường của IP header). So với outer IP header thì vị trí của AH giống như trong kiểu Trasport



Hình Khuôn dạng gói tin đã xử lý AH ở kiểu Tunnel

1. Các thuật toán xác thực

Thuật toán xác thực sử dụng để tính ICV được xác định bởi kết hợp an ninh SA (Security Association). Đối với truyền thông điểm tới điểm, các thuật toán xác thực thích hợp bao gồm các hàm băm một chiều (MD5, SHA-1). Đây chính là những thuật toán bắt buộc mà một ứng dụng AH phải hỗ trợ

1. Xử lý gói đầu ra

Trong kiểu Transport, phía phát chèn AH header vào sau IP header và trước một header của giao thức lớp trên. Trong kiểu Tunnel, có thêm sự xuất hiện của outer IP header. Quá trình xử lý gói tin đầu ra như sau:

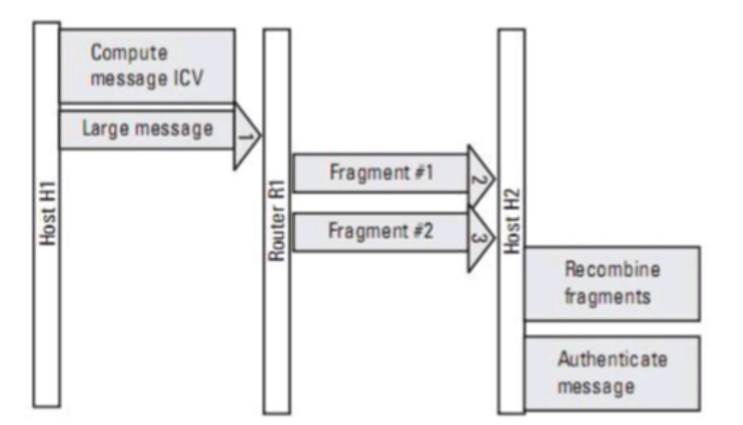
• Tìm kiếm SA: AH được thực hiện trên gói tin đầu ra chỉ khi quá trình IPSec đã xác định được gói tin đó được liên kết với một SA. SA đó sẽ yêu cầu AH xử lý gói tin. Việc xác định quá trình xử lý IPSec nào cần thực hiện trên lưu lượng đầu ra có thể xem trong RFC 2401

• Tạo SN: bộ đếm phía phát được khởi tạo 0 khi một SA được thiết lập. Phía phát tăng SN cho SA này và chèn giá trị SN đó vào trường Sequence Number. Nếu dịch vụ anti-replay (chống phát lại) được lựa chọn, phía phát kiểm tra để đảm bảo bộ đếm không bị lặp lại trước khi chèn một giá trị mới. Nếu dịch vụ anti-replay không được lựa chọn thì phía phát không cần giám sát đến, tuy nhiên nó vẫn được tăng cho đến khi quay trở lại 0

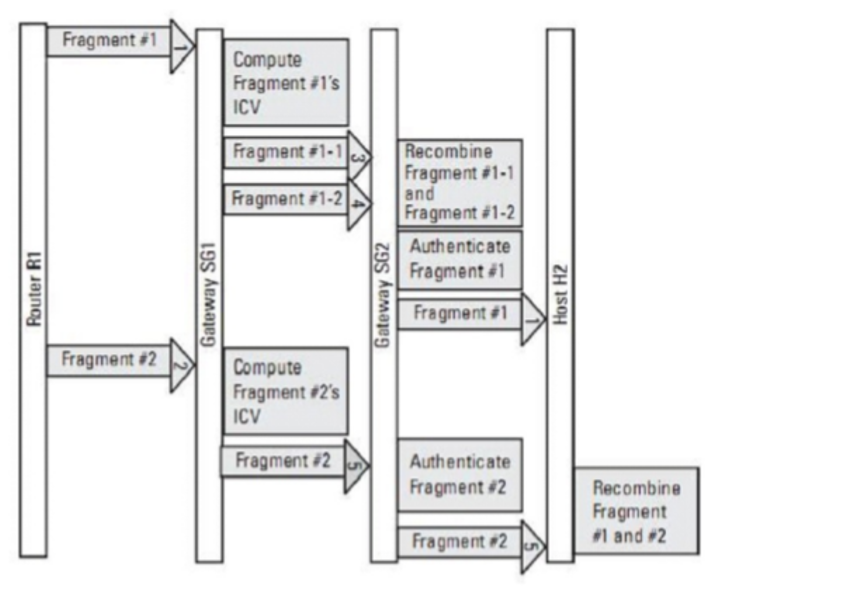
• Tính toán ICV: bằng cách sử dụng các thuật toán, phía thu sẽ tính toán lại ICV ở phía thu và so sánh nó với giá trị có trong AH để quyết định tới khả năng tồn tại của gói tin đó

• Chèn dữ liệu: có hai dạng chèn dữ liệu trong AH, đó là chèn dữ liệu xác thực (Authentication Data Padding) và chèn gói ngầm định (Implicit Packet Padding). Đối với chèn dữ liệu xác thực, nếu đầu ra của thuật toán xác thực là bội số của 96 bits thì không được chèn. Tuy nhiên nếu ICV có kích thước khác thì việc chèn thêm dữ liệu là cần thiết. Nội dung của phần dữ liệu chèn là tùy ý, cũng có mặt trong phép tính ICV và được truyền đi. Chèn gói ngầm định được sử dụng khi thuật toán xác thực yêu cầu tính ICV là số nguyên của một khối b byte nào đó và nếu độ dài gói IP không thỏa mãn điều kiện đó thì chèn gói ngầm định được thực hiện ở phía cuối của gói trước khi tính ICV. Các byte chèn này có giá trị là 0 và không được truyền đi cùng với gói

• Phân mảnh: khi cần thiết, phân mảnh sẽ được thực hiện sau khi đã xử lý AH. Vì vậy AH trong kiểu transport chỉ được thực hiện trên toàn bộ gói IP, không thực hiện trên từng mảnh. Nếu bản thân gói IP đã qua xử lý AH bị phân mảnh trên đường truyền thì ở phía thu phải được ghép lại trước khi xử lý AH. Ở kiểu Tunnel, AH có thể thực hiện trên gói IP mà phần tải tin là một gói IP phân mảnh



Hình Phân mảnh và xác thức: Transport Mode host – host SA



Hình Phân mảnh và xác thực: Tunnel Mode gateway – gateway SA

1. Xử lý gói đầu vào

Khi nhận được một thông điệp có chứa AH,quá trình xử lí ip trước tiên sẽ tống hợp các phân mảnh thành thông điệp hoàn chỉnh.Sau đó thông điệp này sẽ được chuyển tới quá trình xử lí IPSEC.Quá trình này gồm các bước như sau:

* *Bước 1:* Xác định inbound SA tương ứng trong SAD.Bước này được thực hiện dựa trên các thôngsố:SPI,địa chỉ nguồn,giao thức AH.SA tương ứng kiểm tra trong gói AH để xác định xem modenào được áp dụng transport mode hay tunnel mode hay cả hai.Gói cũng phải cung cấp một số thông số để giới hạn tầm tác động của SA(ví dụ:port hay protocol).Nếu đây là tunnel header SA phải so sánh các thông số này trong packer inner vì các thông số này không được sao chép sangtunnel header.Khi SA phù hợp được tìm thấy,quá trình được tiếp tục ,ngược lại gói tin sẽ bị hủy bỏ
* *Bước 2:* Nếu chức năng chống phát lại được kích hoạt,phía xuất phát của gói tin AH luôn tăng số đếm chống phát lại.Bên nhận có thể bỏ qua hoặc sử dụng chỉ số này để chống phát lại.Tuy nhiên giao thức IP không đảm bảo rằng trình tự của các gói khi đến bên nhận giống như trình tự các gói lúc chúng được gửi đi.Do đó chỉ số này không thể dùng để xác định thứ tự của các gói tin.Tuy nhiên chỉ số này vẫn có thể sử dụng để xác định mối liên hệ về thứ tự với một cửa sổ có chiều dài là bội số của 32 bits. Đối với mỗi inbound SA,SAD lưu trữ một cửa sổ chống phát lại.Kích thước của cửa sổ là bội số của 32 bits với giá trị mặc định là 64 bits.Một cửa sổ chống phát lại có kích thước N kiểm soát sequence number của N thông điệp được nhận gần nhất.Bất cứ thông điêp nào có sequence number nhỏ hơn miền giá trị của cửa sổ phát lại đểu bị hủy bỏ.Các thông điệp có số sequence number đã tồn tại trong cửa sổ phát lại cũng bị hủy bỏ. Một bit mask ( hoặc một cấu trúc tương tự ) được sứ dụng để kiểm soát sequence number của N thông điệp được nhận gần nhất đối với SA này .Ban đầu một bit-mask 64 bít có thể giám sát sequence number của các thông điệp có sequence number nằm trong đoạn 1 , 64.Một khi xuất hiện một thông điệp có số sequence number lớn hơn 64 ( ví dụ 70),bit-mask sẽ dịch chuyển để giám sát các số sequence number trong đoạn 7 70. Do đó nó sẽ hủy bỏ các thông điệp có sequence number nhỏ hơn 7, hoặc các thông điệp có số sequence number đã xuất hiện trong cứa sổ chống phát lại.hình dưới đây minh họa hoạt động của cửa sổ chống phát lại.
* *Bước 3:* Kiểm tra tính xác thực của dữ liệu.Hàm băm được tính toán tương tự như dữ liệu đầu ra.Nếu kết quả tính không trùng với ICV trong thông điệp thì hủy bỏ thông điệp ,ngược lại sẽ chuyển sang giai đoạn tiếp theo
* *Bước 4*: Loại bỏ AH và tiếp tục quá trình xử lí IPSEC cho các phần còn lại của tiêu đề IPSEC.Nếu có một nested IPSEC header xuất hiện tại đích đến này.Mỗi header cần phải được xử lí cho đến khi một trong hai điều kiện được thỏa mãn.Khi ipsec header cuối cùng đã được xử lí thành công và quá trình xử lí tiếp cận đến các protocol của lớp trên gói tin được gửi đến chu trình xử lí gói ip tiếp tục di chuyển trong tầng ip.Trong trường hợp khác,nếu quá trình xử lí tiếp cận với một tunnel ip header mà đích đến không phải là host này thì thông điệp được chuyển đến host phù hợp tại đó các giai đoạn tiếp theo của quá trình xử lí IPSEC được diễn ra.
* *Bước 5:* Kiểm tra trong SAD để đảm bảo rằng các ipsec policy áp dụng với thông điệp trên thỏa mãn hệ thống các policy yêu cầu.Giai đoạn quan trọng này rất khó minh họa trong trường hợp quá trình xác thực chỉ sử dụng mình AH.Một ví dụ có sức thuyết phục cao hơn khi chúng ta tiếp tục tìm hiểu một loại tiêu đề bảo mật khác, ESP.

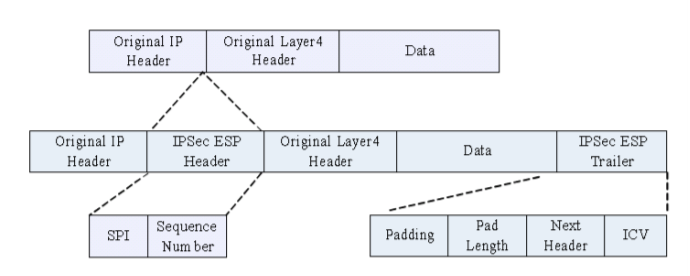
### Giao thức ESP

* + 1. Giới thiệu

Giao thức này cung cấp tính bí mật dữ liệu bằng việc mật mã hóa các gói tin. Thêm vào đó, ESP cũng cung cấp nhận thực nguồn gốc dữ liệu, kiểm tra tính toàn vẹn dữ liệu, dịch vụ chống phát lại và một số giới hạn về luồng lưu lượng cần bảo mật. Tập các dịch vụ cung cấp bởi ESP phụ thuộc vào các lựa chọn tại thời điểm thiết lập SA, dịch vụ bảo mật được cung cấp độc lập với các dịch vụ khác. Tuy nhiên nếu không kết hợp sử dụng với các dịch vụ nhận thực vào toàn vẹn dữ liệu thì hiệu quả bí mật sẽ không được đảm bảo. Hai dịch vụ nhận thực và toàn vẹn dữ liệu luôn đi kèm nhau. Dịch vụ chống phát lại chỉ có thể có nếu nhận thực được lựa chọn. Giao thức này được sử dụng khi yêu cầu về bí mật của lưu lượng IPSec cần truyền.

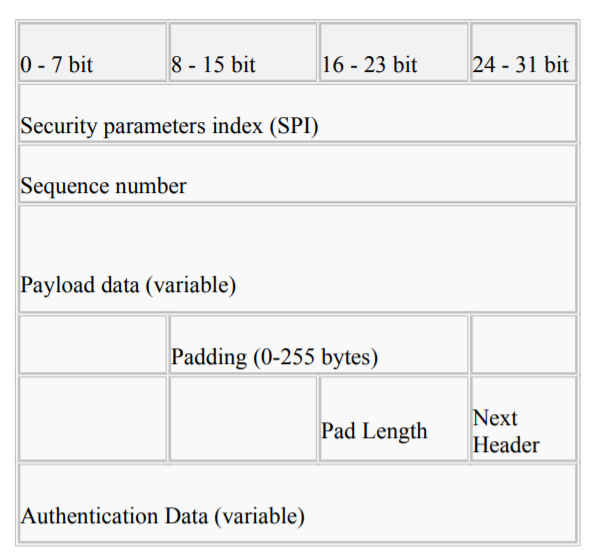
* + 1. Cấu trúc của gói tin ESP

Hoạt động của ESP khác hơn so với AH. Như ngụ ý trong tên gọi, ESP đóng gói tất cả hoặc một phần dữ liệu gốc. Do khả năng bảo mật dữ liệu nên xu hướng ESP được sử dụng rộng rãi hơn AH. Phần header của giao thức nằm ngay trước ESP header có giá trị 51 trong trường protocol của nó. Hình sau diễn tả quá trình xử lý đóng gói:



Hình Xử lý đóng gói ESP

Chi tiết cấu trúc gói ESP:



Hình Chi tiết gói ESP

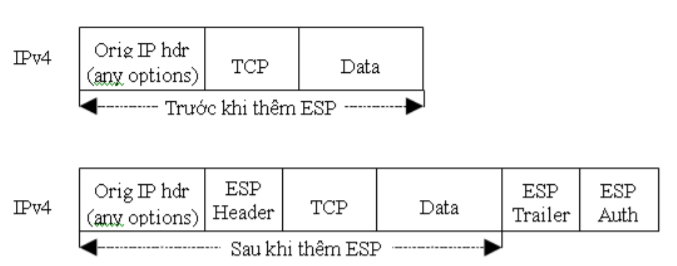
***Ý nghĩa của các phần:***

* SPI (chỉ dẫn thông số an ninh): Là một số bất kỳ 32 bit, cùng với địa chỉ IP đích và giao thức an ninh ESP cho phép nhận dạng duy nhất SA cho gói dữ liệu này. Các giá trị SPI từ 0255 được dành riêng để sử dụng trong tương lai. SPI thường được chọn lửa bởi phía thu khi thiết lập SA. SPI là trường bắt buộc.
* Sequence Number (số thứ tự): Tương tự như trường số thứ tự của AH
* Payload Data (trường dữ liệu tải tin): Đây là trường bắt buộc. Nó bao gồm một số lượng biến đổi các byte dữ liệu gốc hoặc một phần dữ liệu yêu cầu bảo mật đã được mô tả trong trường Next Header. Trường này được mã hóa cùng với thuật toán mã hóa đã chọn lựa trong suốt quá trình thiết lập SA. Nếu thuật toán yêu cầu các vectơ khởi tạo thì nó cũng được bao gồm ở đây. Thuật toán được dùng để mã hóa ESP thường là thuật toán DES-CBC. Đôi khi các thuật toán khác cũng được hỗ trợ như 3DES hay CDMF trong trường hợp nhà cung cấp dịch vụ IBM
* Padding (0->255 bytes): Có nhiều nguyên nhân dẫn đến sự có mặt của trường này
  + Nếu thuật toán mật mã được sử dụng yêu cầu bản rõ (plaintext) phải là nguyên lần khối các byte (ví dụ trường hợp mã khối) thì Padding được sử dụng để điền đầy vào plaintext (bao gồm Payload Data, Pad Length, Next Header và Padding) có kích thước theo yêu cầu.
  + Padding cũng cần thiết để đảm bảo phần dữ liệu mật mã (ciphertext) sẽ kết thúc ở biên giới 4 bytes để phân biết rõ ràng với trường Authentication Data.
* Authentiaction data (bội số của 32 bits):Thông tin xác thực được tình trên toàn bộ gói ESP ngoại trừ phần authentiaction data
  + 1. Quá trình xử lý ESP

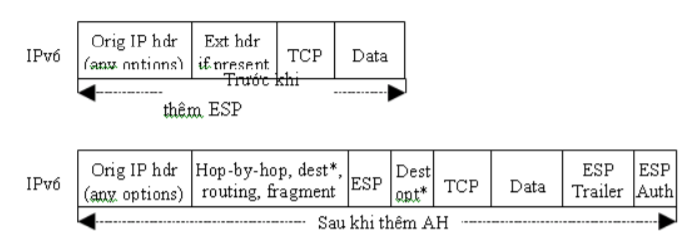
1. Vị trí của ESP header

ESP có hai kiểu hoạt động, đó là kiểu Transport và kiểu Tunnel.

Kiểu Transport cho phép bảo vệ các giao thức lớp trên, nhưng không bảo vệ IP header. Trong kiểu này, ESP được chèn vào sau một IP header và trước một giao thức lớp trên (chẳng hạn TCP, UDP hay ICMP…) và trước IPSec header đã được chèn vào. Đối với IPv4, ESP header đặt sau IP header và trước giao thức lớp trên (ví dụ ở đây là TCP). ESP trailer bao gồm các trường Paddinh, Pad length, và Next Header. Đối với IPv6, ESP được xem như phần tải đầu cuối-tới - đầu cuối, nên sẽ xuất hiện sau phần header mở rộng hop-to-hop, routing và fragmentation. Các lựa chọn đích (dest options extention headers) có thể trước hoặc sau ESP header. Tuy nhiên, do ESP chỉ bảo vệ các trường phía sau ESP header, nên các lựa chọn đích thường được đặt sau ESP header

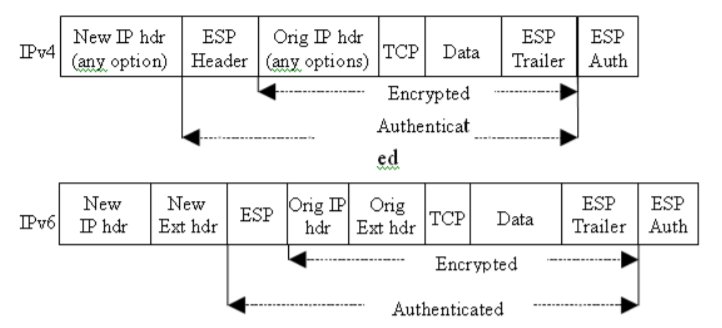


Hình Khuôn dạng IPv4 trước và sau khi xử lý ESP theo kiểu Transport



Hình Khuôn dạng gói tin Ipv6 trước và sau khi xử lý ESP kiểu Transport

Trong kiểu Tunnel, inner IP header mang địa chỉ nguồn và đích cuối cùng, còn outer IP header mạng địa chỉ để định tuyến qua Internet. Trong kiểu này, ESP sẽ bảo vệ toàn bộ gói tin IP bên trong, bao gồm cả inner IP header. So với outer IP header thì vị trí của ESP giống như kiểu Trasport



Hình Khuôn dạng gói tin đã xử lý ESP kiểu tunnel

1. Các thuật toán

Có các thuật toán sau được sử dụng với ESP:

* + - DES, 3DES in CBC.
    - HMAC with MD5.
    - HMAC with SHA-1.
    - NULL Authentication algorithm.
    - NULL Encryption algorithm.

Các thuật toán khác có thể được hỗ trợ. Lưu ý là ít nhất một trong hai dịch vụ bảo mật hoặc nhận thực phải được thực hiện, nên hai thuật toán xác thực và mật mã không đồng thời bằng NULL

* Các thuật toán mật mã: Thuật toán mật mã được xác định bởi SA. ESP làm việc với các thuật toán mật mã đối xứng. Vì các gói IP có thể đến không đúng thứ tự, nên mỗi gói phải mang thông tin cần thiết để phía thu có thể thiết lập đồng bộ mật mã (cryptographic synchronization) để giải mã. Dữ liệu này có thể được chỉ định trong trường Payload (chẳng hạn dưới dạng các vectơ khởi tạo IVInitialization Vector), hoặc thu được từ header của gói. Với sự có mặt của trường Padding, các thuật toán mật mã sử dụng với ESP có thể có các đặc tính khối (block) hoặc luồng (stream). Vì dịch vụ bảo mật là tùy chọn nên thuật toán mật mã có thể là NULL.
* Các thuật toãn xác thực: Thuật toán xác thực sử dụng để tính ICV được xác định bởi SA. Đối với truyền thông điểm-tới-điểm, các thuật toán xác thực thích hợp bao gồm các hàm băm một chiều (MD5, SHA1). Vì dịch vụ xác thực là tùy chọn nên thuật toán xác thực có thể là NULL.

1. Xử lý gói đầu ra

Trong kiểu Transport, phía phát đóng gói thông tin giao thức lớp trên vào ESP header/ trailer và giữ nguyên IP header (và tất cả IP extension headers đối với IPv6). Trong kiểu Tunnel, có thêm sự xuất hiện của outer IP header. Quá trình xử lý gói tin đầu ra như sau:

* Tìm kiếm SA: ESP được thực hiện trên một gói tin đầu ra chỉ khi quá trình IPSec đã xác định được gói tin đó được liên kết với một SA, SA đó sẽ yêu cầu ESP xử lý gói tin. Việc xác định quá trình xử lý IPSec nào cần thực hiện trên lưu lượng đầu ra có thể xen trong RFC 2401
* Mật mã gói tin: Đối với kiểu Transport chỉ đóng gói thông tin giao thức lớp cao. Đối với kiểu Tunnel, đóng gói toàn bộ gói IP ban đầu: Thêm trường Padding nếu cần thiết, mật mã các trường sử dụng khóa, thuật toán và kiểu thuật toán được chỉ ra bởi SA và dữ liệu đồng bộ mật mã nếu có

Các bước cụ thể để xây dựng outer IP header phụ thuộc vào kiểu sử dụng (Transport hay Tunnel). Nếu dịch vụ xác thực được lựa chọn thì mật mã được thực hiện trước, và quá trình mật mã không bao gồm trường Authentication Data. Thứ tự xử lý này cho phép nhanh chóng xác định và loại bỏ các gói lỗi hoặc lặp lại mà không cần phải thực hiện giải mã, qua đó làm ảnh hưởng của các tấn công kiểu từ chối dịch vụ (denial of service attacks), đồng thời cho phép phía thu xử lý song song: giải mã và xác thực tiến hành song song.

* Tạo SN: tương tự như tạo SN của AH.
* Tính toán ICV: nếu dịch vụ xác thực được lựa chọn cho SA thì phía phát sẽ tính toán giá trị ICV trên dữ liệu gói ESP trừ trường Authentication Data. Lưu ý là các trường mật mã được thực hiện trước xác thực. Chi tiết về tính toán ICV cũng tương tự như ở AH.
* Phân mảnh: Khi cần thiết, phân mảnh được thực hiện sau khi đã xử lý ESP. Vì vậy ESP trong kiểu Transport chỉ được thực hiện trên toàn bộ gói IP, không thực hiện trên từng mảnh. Nếu bản thân gói IP đã qua xử lý ESP bị phân mảnh bởi các router trên đường truyền thì các mảnh phải được ghép lại trước khi xử lý ESP ở phía thu. Trong kiểu Tunnel, ESP có thể thực hiện trên gói IP mà phần Payload là một gói IP phân mảnh.

1. Xử lý gói đầu vào

Quá trình xử lý gói đầu vào ngược với quá trình xử lý gói tin đầu ra:

* Ghép mảnh: Ghép mảnh được thực hiện trước khi xử lý ESP
* Tìm kiếm SA: khi nhận được gói đã ghép mảnh chứa ESP header, phía thu sẽ xác định một SA phù hợp dựa trên địa chỉ IP đích, giao thức an ninh ESP và SPI. Quá trình tìm kiếm có thể xem chi tiết trong RFC 2401. Thông tin trong SA sẽ cho biết có cần kiểm tra trường Sequence Number hay không, có cần thêm trường Authentication Data hay không và các thuật toán và khóa cần sử dụng để giải mã tính ICV nếu có. Nếu không có SA nào phù hợp được tìm thấy cho phiên truyền dẫn này (ví dụ phía thu không có khóa), phía thu sẽ loại bỏ gói.
* Kiểm tra SN: ESP luôn hỗ trợ dịch vụ chống phát lại (antirepley), mặc dù việc dịch vụ này hoàn toàn do lựa chọn phí thu trên cơ sở từng SA. Dịch vụ này không thực hiện được nếu dịch vụ xác thực không được lựa chọn, vì khi này Sequence Number không được bảo vệ tính toàn vẹn.

Nếu phía thu không lựa chọn dịch vụ chống phát lại cho một SA nào đó thì không cần kiển tra trường Sequence Number. Tuy nhiên phía phát mặc định là phía thu sử dụng dịch vụ này. Vì vậy, để phía phát không phải thực hiện giám sát SN cũng như thiết lập lại SA một cách không cần thiết, trong quá trình thiết lập SA phía thu sẽ thông báo cho phía phát việc không sử dụng dịch vụ chống phát lại (trong trường hợp một giao thức thết lập SA như IKE được sử dụng).

Nếu phía thu có lựa chọn dịch vụ chống phát lại cho một SA thì bộ đếm gói thu cho SA đó phải được khởi tạo 0 khi thiết lập SA. Với mỗi gói thu được, phía thu phải kiểm tra rằng gói đó có chứa số SN không lặp của bất kỳ một gói nào trong thời gian tồn tại của SA đó. Sau khi một gói đã được xác định là tương ứng với một SA nào đó thì phép kiểm tra này là cần được thực hiện đầu tiên để có thể nhanh chóng quyết định khả năng tồn tại của gói đó

Các gói bị loại bỏ thông qua sử dụng một cửa sổ thu trượt. Giá trị cửa sổ tối thiểu là 32 và mặc định là 64, phía thu cũng có thể sử dụng các cửa sổ có kích thước lớn hơn. Bên phải của cửa sổ đại diện cho SN hợp lệ lớn nhất đã thu được trong SA này. Các gói có SN nhỏ hơn bên trái của cửa sổ sẽ bị loại bỏ. Các gói có SN nằm trong khoảng giữa hai bên của cửa sổ sẽ được kiểm tra với một danh sách các gói đã thu được trong cửa sổ. Nếu gói thu được nằm trong vùng cửa sổ và là mới, hoặc gói đã tới bên phải của cửa sổ thì phía thu sẽ tiến hành xử lý tiếp ICV. Nếu việc kiểm tra ICV sai thì phía thu phải loại bỏ gói IP vì không hợp lệ. Cửa sổ thu chỉ được cập nhật sau khi việc kiểm tra ICV thành công.

Kiểm tra ICV: nếu dịch vụ xác thực được lựa chọn, phía thu sẽ tính ICV dựa trên dữ liệu của gói ESP ngoại trừ trường Authentication Data, sử dụng thuật toán xác thực xác định trong SA và so sánh với giá trị ICV trong trường Authentication của gói. Nếu hai giá trị ICV hoàn toàn trùng khớp thì gói tin là hợp lệ và được chấp nhận. Ngược lại, phía thu sẽ loại bỏ gói tin

Việc kiểm tra tiến hành như sau: trước hết giá trị ICV nằm trong trường Authentication Data được tách ra khỏi gói ESP và được lưu trữ. Tiếp theo kiểm tra độ dìa của gói ESP (ngoại trừ trườn Authentication Data). Nếu Padding ngầm định được yêu cầu bởi thuật toán xác thực thì các byte 0 được thêm vào cuối gói ESP, ngay sau trường Next Header. Tiếp theo thực hiện tính toán ICV và so sánh với giá trị đã lưu sử dụng các luật so sánh được định nghĩa bởi thuật toán.

1. Giải mã gói

Nếu ESP sử dụng mật mã thì sẽ phải thực hiện quá trình giải mã gói. Nếu dịch vụ bảo mật không được sử dụng, tại phía thu không có quá trình giải mã gói này. Quá trình giải mã gói diễn ra như sau:

* Giải mã ESP (bao gồm trường Payload Data, Padding, Pad Length, Next Header) sử dụng khóa. Thuật toán mật mã và kiểu thuật toán được xác định bởi SA.
* Xử lý phần Padding theo đặc tả của thuật toán. Phía thu cần tìm và loại bỏ phần Padding trước khi chuyển dữ liệu đã giải mã lên lớp trên
* Xây dựng lại cấu trúc gói IP ban đầu từ IP header ban đầu và thông tin giao thức lớp cao trong tải tin của ESP (ở kiểu Transport), hoặc outer IP header và toàn bộ gói IP ban đầu trong tải tin của ESP (ở kiểu Tunnel).

Nếu dịch vụ xác thực cũng được lựa chọn thì quá trình kiểm tra ICV và mật mã có thể tiến hành nối tiếp hoặc song song. Nếu tiến hành nối tiếp thì kiểm tra ICV phải được thực hiện trước. Nếu tiến hành song song thì kiểm tra ICV phải hoàn thành trước khi gói đã giải mã được chuyển tới bước xử lý tiếp theo. Trình tự này giúp loại bỏ nhanh chóng các gói không hợp lệ.

Có một số lý do như sau dẫn đến quá trình giải mã không thành công:

* SA được lựa chọn không đúng: SA có thể sai do các thông số SPI, địa chỉ đích, trương Protocol type sai.
* Độ dài phần Padding hoặc giá trị của nó bị sai.
* Gói ESP mật mã bị lỗi (có thể được lựa chọn nếu dịch vụ xác thực được lựa chọn cho SA)

## Giao thức trao đổi khóa

### Giới thiệu

Là giao thức thực hiện quá trình trao đổi khóa và thỏa thuận các thông số bảo mật với nhau như: mã hóa thế nào, mã hóa bằng thuật toán gì, bao lâu trao đổi khóa 1 lần. Sau khi trao đổi xong thì sẽ có được một “thỏa thuận” giữa 2 đầu cuối, khi đó IPSec SA (Security Association) được tạo ra.

SA là những thông số bảo mật đã được thỏa thuận thành công, các thông số SA này sẽ được lưu trong cơ sở dữ liệu của SA. Trong quá trình trao đổi khóa thì IKE dùng thuật toán mã hóa đối xứng, những khóa này sẽ được thay đổi theo thời gian. Đây là đặc tính rất hay của IKE, giúp hạn chế trình trạng bẻ khóa của các attacker.

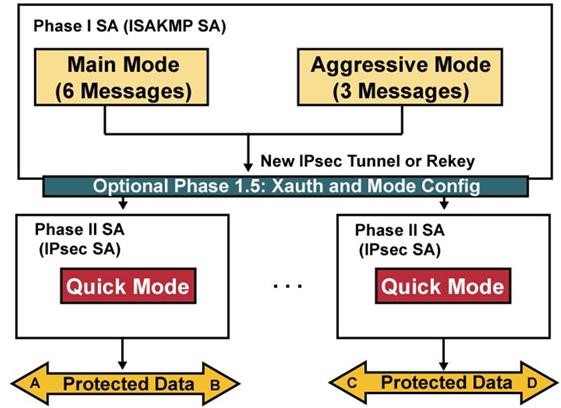
IKE còn dùng 2 giao thức khác để chứng thực đầu cuối và tạo khóa: ISAKMP (Internet Security Association and Key Management Protocol) và Oakley.

- ISAKMP: là giao thức thực hiện việc thiết lập, thỏa thuận và quản lý chính sách bảo mật SA.

- Oakley: là giao thức làm nhiệm vụ chứng thực khóa, bản chất là dùng thuật toán Diffie-Hellman để trao đổi khóa bí mật thông qua môi trường chưa bảo mật. Giao thức IKE dùng UDP port 500.

### 5.2 Các quá trình của IKE

Giai đoạn hoạt động của IKE cũng được xem tương tự như là quá trình bắt tay trong TCP/IP. Quá trình hoạt động của IKE được chia ra làm 2 phase chính: Phase 1 và Phase 2, cả hai phase này nhằm thiết lập kênh truyền an toàn giữa 2 điểm. Ngoài phase 1 và phase 2 còn có phase 1.5



Hình Các quá trình của IKE

2.1. IKE phase 1

Đây là giai đoạn bắt buộc phải có. Phase này thực hiện việc chứng thực và thỏa thuận các thông số bảo mật, nhằm cung cấp một kênh truyền bảo mật giữa hai đầu cuối.

Các thông số sau khi đồng ý giữa 2 bên gọi là SA, SA trong pha này gọi là ISAKMP SA hay IKE SA. Pha này sử dụng một trong 2 mode để thiết lập SA: Main mode và Aggressive mode.

Các thông số bảo mật bắt buộc phải thỏa thuận trong phase 1 này là:

- Thuật toán mã hóa: DES, 3DES, AES

- Thuật toán hash: MD5, SHA

- Phương pháp chứng thực: Preshare-key, RSA

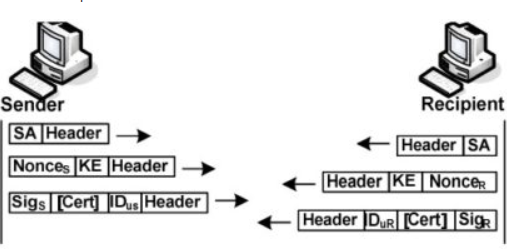
- Nhóm khóa Diffie-Hellman (version của Diffie-Hellman)

Main mode sử dụng 6 message để trao đổi thỏa thuận các thông số với nhau:

- 2 message đầu dùng để thỏa thuận các thông số của chính sách bảo mật.

- 2 message tiếp theo trao đổi khóa Diffire-Hellman.

- 2 message cuối cùng thực hiện chứng thực giữa các thiết bị.



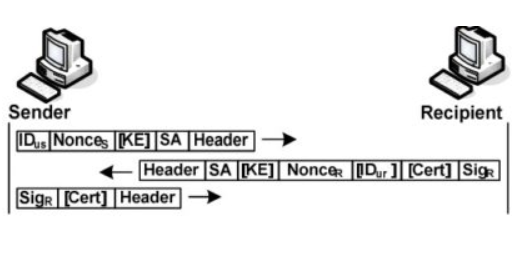
Hình Quá trình trao đổi message thỏa thuận giữa các bên

Aggressive mode: sử dụng 3 message:

- Message đầu tiên gồm các thông số của chính sách bảo mật, khóa Diffie-Hellman.

- Message thứ 2 sẽ phản hồi lại thông số của chính sách bảo mật được chấp nhận, khóa được chấp nhận và chứng thực bên nhận.

- Message cuối cùng sẽ chứng thực bên vừa gửi.



Hình Quá trình chứng thực giữa các bên

2.2. Phase 1.5

Đây là phase không bắt buộc (optional). Phase 1 cung cấp cơ chế chứng thực giữa 2 đầu cuối tạo nên một kênh truyền bảo mật. Phase 1.5 sử dụng giao thức Extended Authentication (Xauth). Phase này thường sử dụng trong Remote Access VPN.

2.3. Phase 2

Đây là phase bắt buộc, đến phase này thì thiết bị đầu cuối đã có đầy đủ các thông số cần thiết cho kênh truyền an toàn. Quá trình thỏa thuận các thông số ở phase 2 là để thiết lập IPSec SA dựa trên những thông số của phase 1.

Quick mode là phương thức được sử dụng trong phase 2. Các thông số mà Quick mode thỏa thuận trong phase 2:

- Giao thức IPSec: ESP hoặc AH

- IPSec mode: Tunnel hoặc transport

- IPSec SA lifetime: dùng để thỏa thuận lại IPSec SA sau một khoảng thời gian mặc định hoặc được chỉ định.

- Trao đổi khóa Diffie-Hellman IPSec SA của phase 2 hoàn toàn khác với IKE SA ở phase 1, IKE SA chứa các thông số để tạo nên kênh truyền bảo mật, còn IPSec SA chứa các thông số để đóng gói dữ liệu theo ESP hay AH, hoạt động theo tunnel mode hay transport mode

### 5.3 Các chức năng khác của IKE giúp cho IKE hoạt động tối ưu hơn bao gồm:

- Dead peer detection (DPD) and Cisco IOS keepalives là những chức năng bộ đếm thời gian. Nghĩa là sau khi 2 thiết bị đã tạo được VPN IPsec với nhau rồi thì nó sẽ thường xuyên gửi cho nhau gói keepalives để kiểm tra tình trạng của đối tác. Mục đích chính để phát hiện hỏng hóc của các thiết bị. Thông thường các gói keepalives sẽ gửi mỗi 10s.

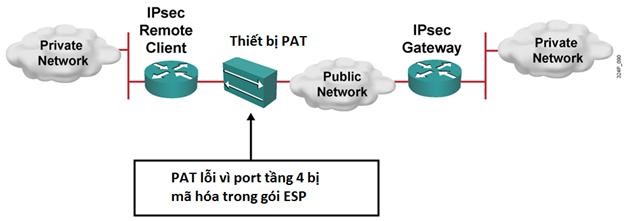
- Hỗ trợ chức năng NAT-Traversal: Chức năng này có ý nghĩa là nếu trên đường truyền từ A tới B có những thiết bị NAT or PAT đứng giữa thì lúc này IPSec nếu hoạt động ở chế độ tunel mode và enable chức năng NAT

- Trasersal sẽ vẫn chuyển gói tin đi được bình thường.

Lưu ý : Chức năng NAT-T bắt đầu được Cisco hỗ trợ từ phiên bản IOS Release 122.2T.

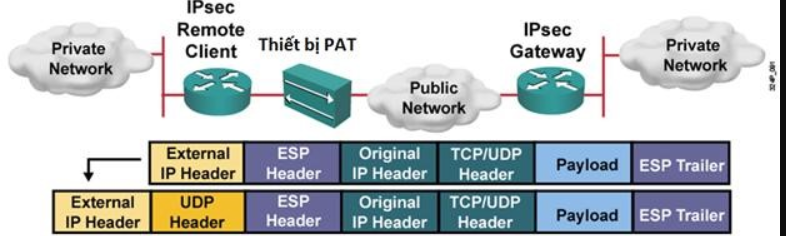
Nguyên nhân tại sao phải hỗ trợ chức năng NAT-T thì các packet mới tiếp tục đi được?

Khi thực hiện quá trình mã hóa bằng ESP thì lúc này các source IP, port và destination IP, port đều đã được mã hóa và nằm gọn tron ESP Header. Như vậy khi tất cả các thông tin IP và Port bị mã hóa thì kênh truyền IPSec không thể diễn ra quá trình NAT.



Hình Quá trình NAT

Do đó NAT Traversal ra đời trong quá trình hoạt động của IKE nhằm phát hiện và hỗ trợ NAT cho Ipsec. Các dữ liệu sẽ không bị đóng gói trực tiếp bởi giao thức IP mà nó sẽ đóng gói thông qua giao thức UDP. Và lúc này các thông tin về IP và Port sẽ nằm trong gói UDP này.



Hình NAT Travesal

NAT Travesal giúp hỗ trợ các gói tin đã được mã hoá có thể đi qua các thiết bị PAT

GRE - Generic Routing Encapsulation là giao thức được phát triển đầu tiên bởi Cisco, với mục đích chính tạo ra kênh truyền ảo (tunnel) để mang các giao thức lớp 3 thông qua mạng IP.

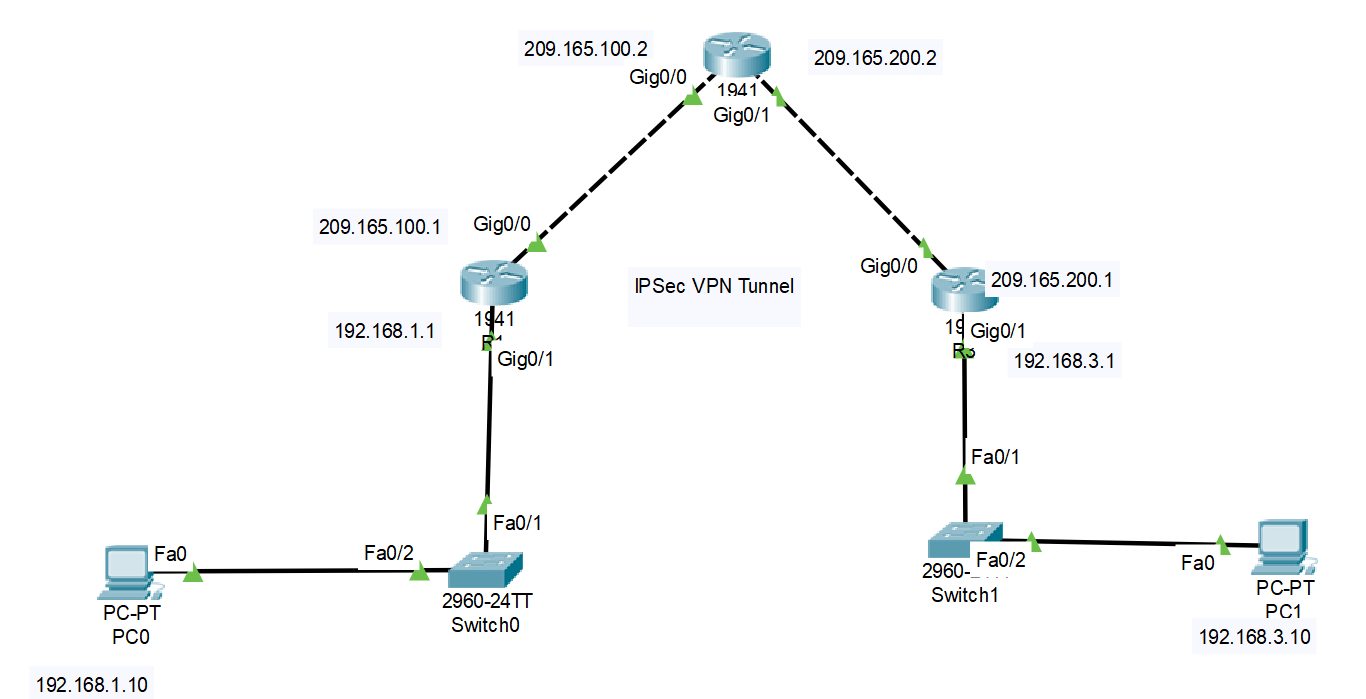
## Tính năng của IPSec trong VPN

Để thực hiện được chức năng chính của mình là bảo mật dữ liệu trong VPN, IPSec cung cấp những tính năng sau:

* 1. *Sự bảo mật dữ liệu (Data Confidentiality)*: Đảm bảo dữ liệu được an toàn, tránh những kẻ tấn công phá hoại bằng cách thay đổi nội dung hoặc đánh cắp dữ liệu quan trọng. Việc bảo vệ dữ liệu được thực hiện bằng các thuật toán mã hóa như DES, 3DES và AES. Tuy nhiên, đây là một tính năng tùy chọn trong IPSecSự toàn vẹn dữ liệu
  2. *Sự toàn vẹn dữ liệu (Data Integrity)*: Đảm bảo rằng dữ liệu không bị thay đổi trong suốt quá trình trao đổi. Data Integrity bản thân nó không cung cấp sự an toàn dữ liệu. Nó sử dụng thuật toán băm (hash) để kiểm tra dữ liệu bên trong gói tin có bị thay đổi hay không. Những gói tin nào bị phát hiện là đã bị thay đổi thì sẽ bị loại bỏ. Những thuật toán băm: MD5 hoặc SHA-1.Tránh trùng lặp
  3. *Chứng thực nguồn dữ liệu (Data Origin Authentication)*: Mỗi điểm cuối của VPN dùng tính năng này để xác định đầu phía bên kia có thực sự là người muốn kết nối đến mình hay không. Lưu ý là tính năng này không tồn tại một mình mà phụ thuộc vào tính năng toàn vẹn dữ liệu. Việc chứng thực dựa vào những kĩ thuật: Pre-shared key, RSA-encryption, RSA-signature.
  4. *Tránh trùng lặp (Anti-replay)*: Đảm bảo gói tin không bị trùng lặp bằng việc đánh số thứ tự. Gói tin nào trùng sẽ bị loại bỏ, đây cũng là tính năng tùy chọn

# THIẾT KẾ VÀ TRIỂN KHAI DEMO về IPSec trong VPN

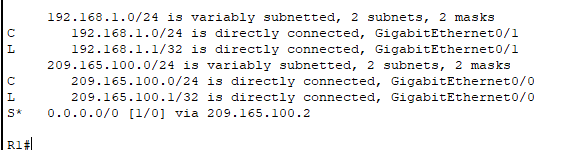
## Xây dựng hệ thống mạng như trong hình dưới

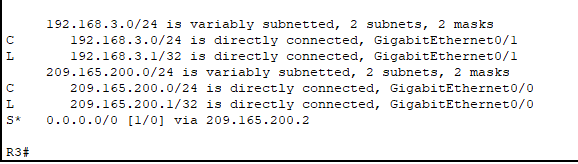


Hình Cấu hình địa chỉ IP các máy

## Cấu hình các route:

Đầu tiên sẽ cấu hình định tuyến cho R1 và R3 ra mạng internet





Cấu hình IPSec cho R1 (làm tương tự với R3)

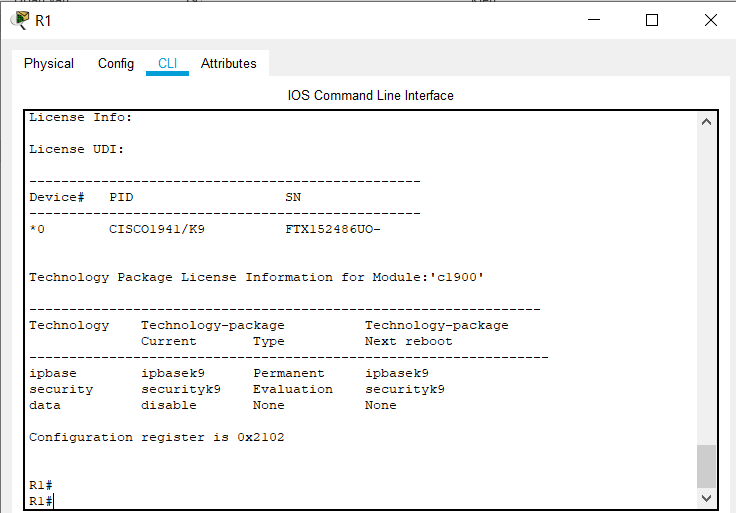
a, Bật security license:

*R1 (config) #* *license boot module c1900 technology-package securityk9*

*R1#copy run startup-config*

*R1#reload*

*R1#show version*



b, Danh sách chấp nhận kết nối

*R1 (config) #access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255*

b, Cấu hình isakmp

*R1 (config) #* *crypto isakmp policy 10* (Dùng chính sách 10)

*R1 (config-* *isakmp) # encryption aes 256*  (Mã hóa aes dùng 256 bit)

*R1 (config- isakmp) # authentication pre-share* (Xác thực dùng khóa chia sẻ trước)

*R1 (config- isakmp) # group 5* (Differ-hallman nhóm 5)

c, Cấu hình khóa bí mật

*R1 (config) # crypto isakmp key secretkey address 209.165.200.1*

d, Cấu hình tranform-set

*R1 (config) # crypto ipsec transform-set R1->R3 esp-aes 256 esp-sha-hmac*

e, Cấu hình crypto map

*R1 (config) # crypto map IPSEC-MAP 10 ipsec-isakmp*

*R1 (config-crypto-map) #set peer 209.165.200.1*

*R1 (config-crypto-map) #set pfs group5*

*R1 (config-crypto-map) #set security-association lifetime seconds 86400*

*R1 (config-crypto-map) #set transform-set R1->R3*

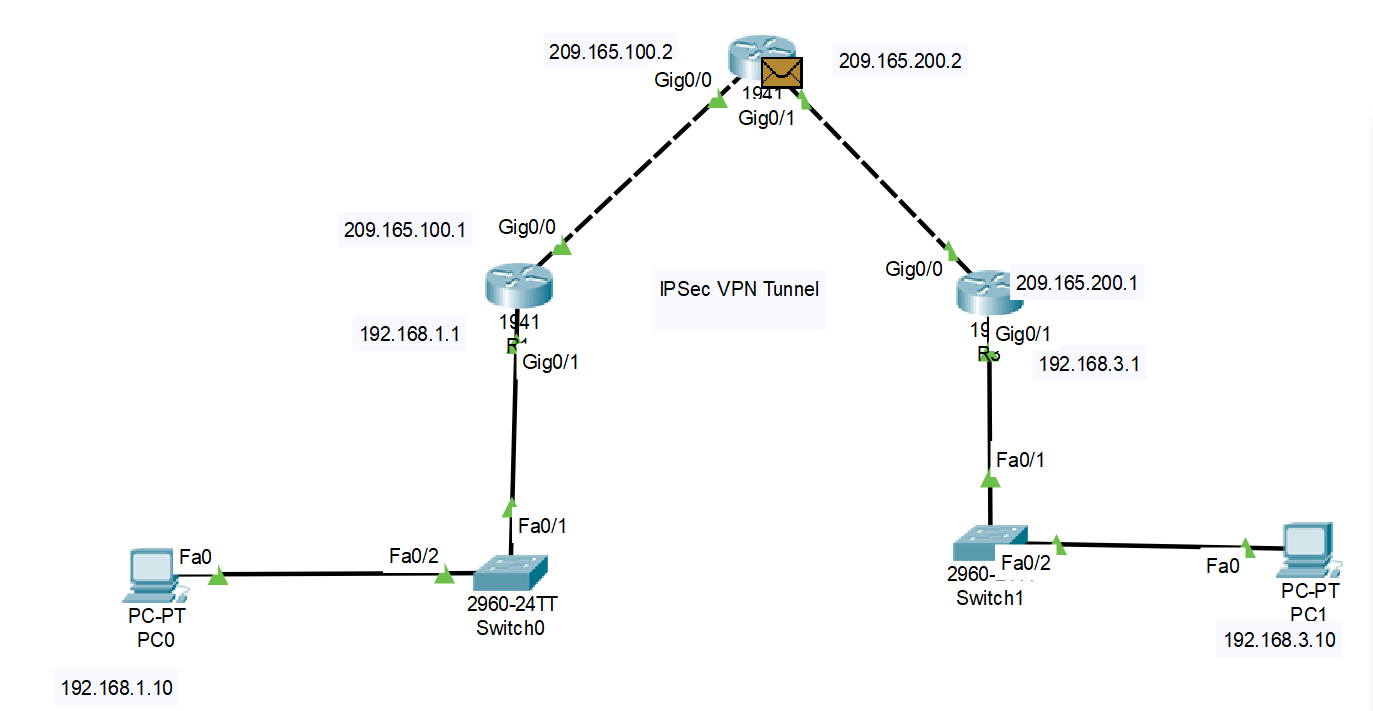
*R1 (config-crypto-map) #match address 100*

f, Bật mã hóa trên interface g0/0

*R1 (config) #interface GigabitEthernet0/0*

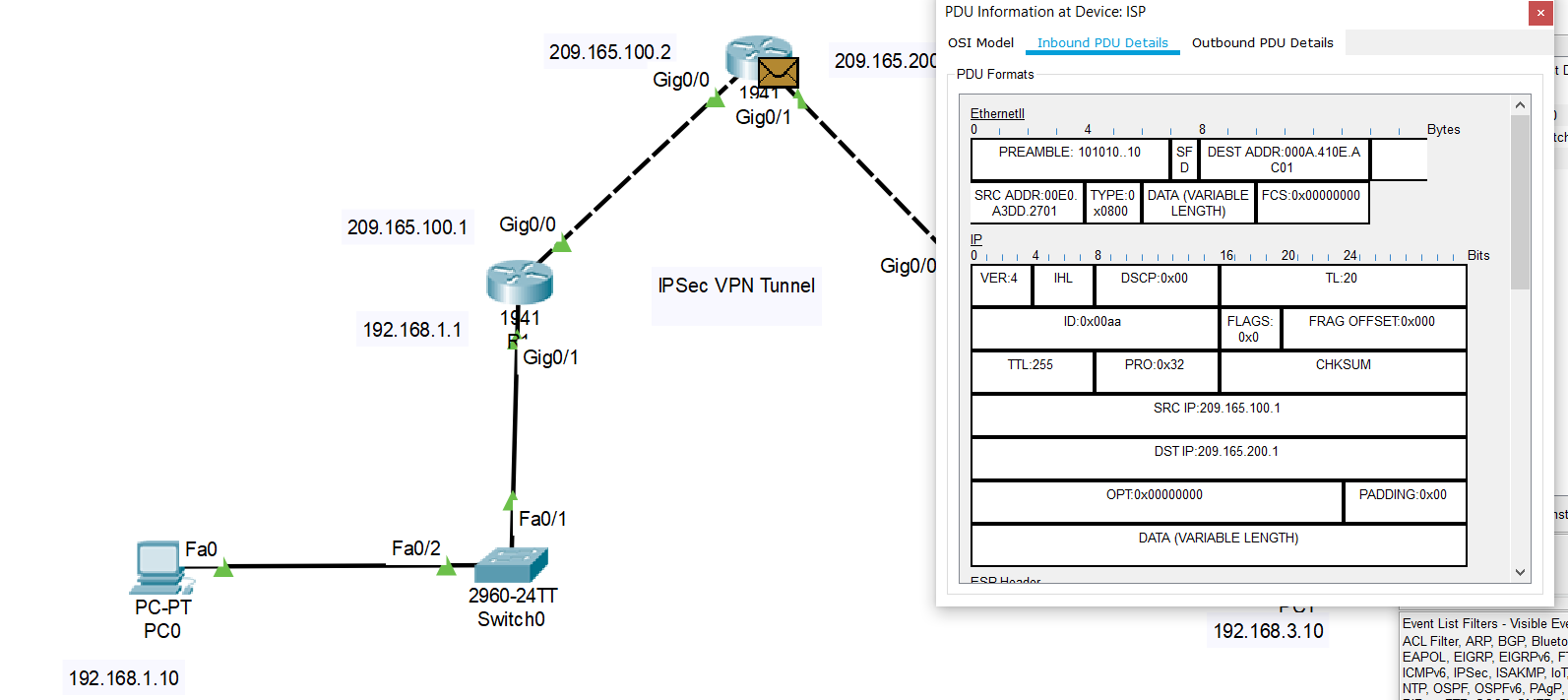
*R1 (config-if) # crypto map IPSEC-MAP*

## Phân tích gói tin gửi từ mạng R1 đến mạng R3



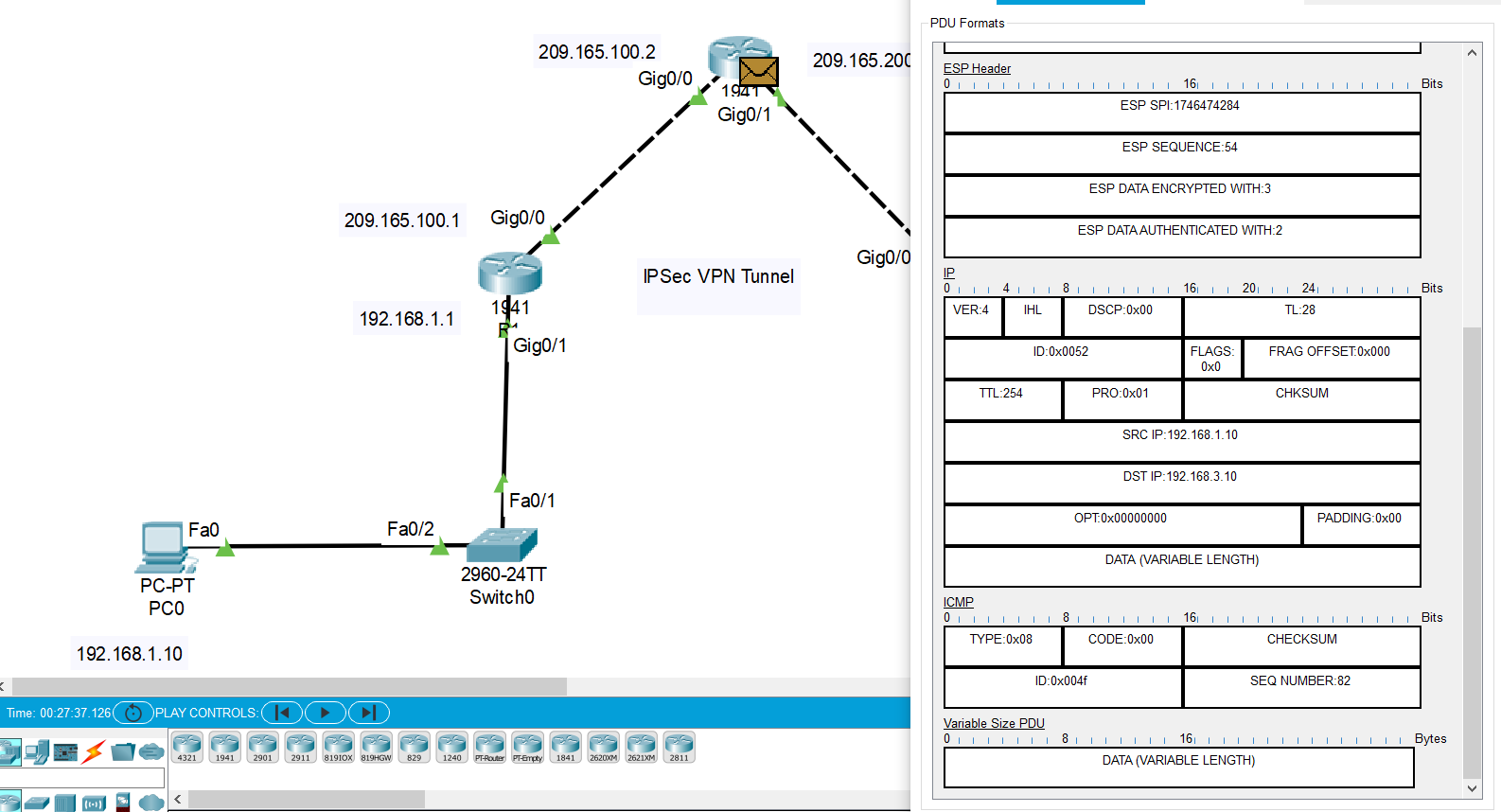
Hình Gói tin gửi đến ISP

Khi gửi gói tin từ máy PC0 đến PC1, phân tích gói tin tại Router ISP



Hình Phân tích gói tin tại ISP

Địa chỉ nguồn là 209.165.100.1, địa chỉ đích là 209.165.200.1

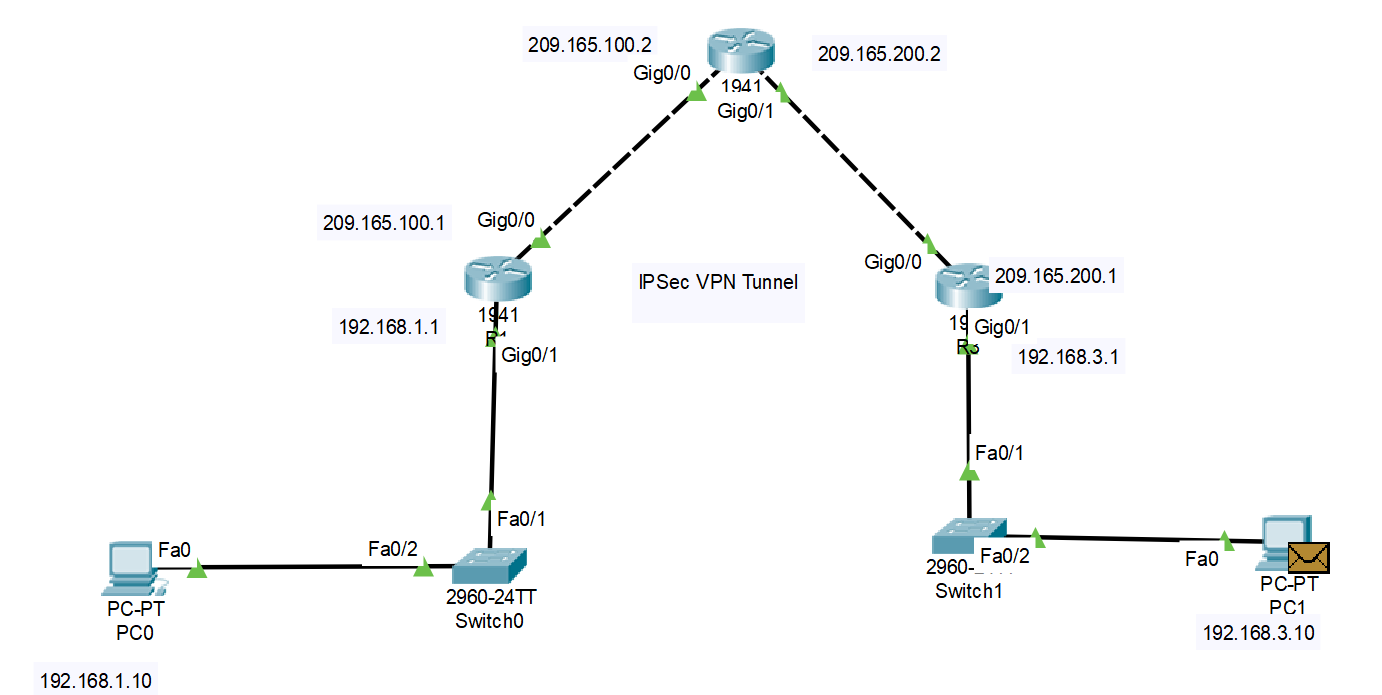


Hình Phân tích gói tin tại ISP

Nhưng bên trong là ESP header và sau đó là địa chỉ IP thứ 2 và được mã hóa trong đường hầm. Ta có thể thấy địa chỉ ip nguồn là 192.168.1.10 và địa chỉ ip đích là 192.168.3.10

ISP không thể thấy được đường hầm đó và sau đó chuyển tiếp gói tin đến R3

Cuối cùng gói tin đến được PC1



Hình Gói tin được nhận bới máy đích