**ĐỒ ÁN AN TOÀN MÁY CHỦ WINDOWS**

**TÌM HIỂU VÀ TRIỂN KHAI GIAO THỨC IPSEC VPN**

Môn học: An Toàn Máy Chủ Windows

Giảng viên hướng dẫn:

Sinh viên thực hiện :

TP. Hồ Chí Minh, 2022

**ĐỒ ÁN AN TOÀN MÁY CHỦ WINDOWS**

**TÌM HIỂU VÀ TRIỂN KHAI GIAO THỨC IPSEC VPN**

Môn học: An Toàn Máy Chủ Windows

Giảng viên hướng dẫn:

Sinh viên thực hiện :

TP. Hồ Chí Minh, 2022

**NHẬN XÉT CỦA GIẢNG VIÊN**

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

# MỤC LỤC

[MỤC LỤC 4](#_Toc106573476)

[LỜI MỞ ĐẦU 1](#_Toc106573477)

[CHƯƠNG 1: TỔNG QUAN 2](#_Toc106573478)

[1.1. Lý do chọn đề tài 2](#_Toc106573479)

[1.2. Đối tượng sử dụng 2](#_Toc106573480)

[1.3. Cấu trúc đề tài 2](#_Toc106573481)

[CHƯƠNG 2: CƠ SỞ LÝ THUYẾT 3](#_Toc106573482)

[2.1 VPN 3](#_Toc106573483)

[2.1.1. VPN LÀ GÌ ? 3](#_Toc106573484)

[2.1.2.VPN HOẠT ĐỘNG NHƯ THẾ NÀO 3](#_Toc106573485)

[2.1.3. VÌ SAO CẦN PHẢI SỬ DỤNG VPN 4](#_Toc106573486)

[2.1.4. CHỨC NĂNG CỦA VPN 4](#_Toc106573487)

[2.1.5. CÁC LOẠI GIAO THỨC HOẠT ĐỘNG CÓ TRONG VPN 5](#_Toc106573488)

[**2.1.6. ƯU, NHƯỢC ĐIỂM CỦA VPN** 6](#_Toc106573489)

[**2.1.7. Lịch sử phát triển của VPN** 6](#_Toc106573490)

[**2.2. IPSEC** 8](#_Toc106573491)

[**2.2.1. IPSEC LÀ GÌ ?** 8](#_Toc106573492)

[**2.2.2. SƠ LƯỢC VỀ LỊCH SỬ CỦA IPSEC** 8](#_Toc106573493)

[**2.2.3. CÁCH THỨC HOẠT ĐỘNG CỦA IPSEC** 8](#_Toc106573494)

[**2.2.4. VAI TRÒ CỦA IPSEC** 9](#_Toc106573495)

[**2.2.5. NHỮNG GIAO THỨC ĐƯỢC SỬ DỤNG TRONG IPSEC** 9](#_Toc106573496)

[**2.2.6. NHỮNG TÍNH NĂNG CỦA IPSEC (IPSEC Security Protocol)** 17](#_Toc106573497)

[**2.2.7. CẤU TRÚC BẢO MẬT** 18](#_Toc106573498)

[**2.2.8. SỰ KHÁC BIỆT GIỮA CHẾ ĐỘ IPSEC TUNNEL VÀ IPSEC TRANSPORT** 18](#_Toc106573499)

[**2.2.9. IPSEC SỬ DỤNG PORT NÀO ?** 19](#_Toc106573500)

[**2.2.10. IPSEC TÁC ĐỘNG ĐẾN MSS VÀ MTU NHƯ THẾ NÀO?** 19](#_Toc106573501)

[**2.2.11. Điểm giống nhau giữa IPSec và SSL:** 19](#_Toc106573502)

[**2.2.12. Điểm khác nhau giữa IPSec và SSL:** 20](#_Toc106573503)

[2.2.13. ƯU ĐIỂM VÀ KHUYẾT ĐIỂM CỦA IPSEC : 20](#_Toc106573504)

[**2.2.13.1.**  **Ưu điểm:** 20](#_Toc106573505)

[**2.2.13.2.**  **Nhược điểm:** 21](#_Toc106573506)

[**2.2.14.**  **LIÊN KẾT BẢO MẬT:** 21](#_Toc106573507)

[**CHƯƠNG III:KẾT QUẢ THỰC NGHIỆM** 24](#_Toc106573508)

[3.1 Sơ đồ kịch bản 24](#_Toc106573509)

[3.2. Công cụ 24](#_Toc106573510)

[3.3. Các bước thực hiện 24](#_Toc106573511)

[3.4. Kết quả: 25](#_Toc106573512)

[3.5. Demo 32](#_Toc106573513)

[**CHƯƠNG 4: KẾT LUẬN VÀ PHÁT TRIỂN** 33](#_Toc106573514)

# LỜI MỞ ĐẦU

Đầu tiên, em xin gửi lời cảm ơn chân thành đến Trường Đại Học đã đưa môn học An Toàn Máy Chủ Windows vào trương trình giảng dạy. Đặc biệt, em xin gửi lời cảm ơn sâu sắc đến giảng viên bộ môn - thầy Tống Thanh Văn đã dạy dỗ, truyền đạt những kiến thức quý báu cho em trong suốt thời gian học tập vừa qua. Trong thời gian tham gia lớp học của thầy, em đã có thêm cho mình nhiều kiến thức bổ ích, tinh thần học tập hiệu quả, nghiêm túc. Đây chắc chắn sẽ là những kiến thức quý báu, là hành trang để em có thể vững bước sau này.

Bộ môn An Toàn Máy Chủ Windows là môn học thú vị, vô cùng bổ ích và có tính thực tế cao, cung cấp rất nhiều kiến thức về mạng cũng như mọi thứ liên quan về mạng. Đảm bảo cung cấp đủ kiến thức, gắn liền với nhu cầu thực tiễn của sinh viên. Tuy nhiên, do vốn kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ.

Do chưa có nhiều kinh nghiệm nghiên cứu, thực hành nên đề tài thực hiện còn nhiều thiếu sót, chúng em mong nhận được đóng góp ý kiến của thầy để đề tài được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

Sinh viên thực hiện

# CHƯƠNG 1: TỔNG QUAN

## Lý do chọn đề tài

Để tìm hiểu rõ hơn về VPN cũng như giao thức IPSec, cách thức hoạt động của VPN và cách mà chúng thực hiện bảo mật cho các thông tin tránh các đối tượng xấu độc chiếm, chúng em đã chọn được đề tài tìm hiểu về IPSec VPN.

## 1.2. Đối tượng sử dụng

- Học hỏi thêm được các kiến thức mới thông qua tìm hiểu đề tài

- Giúp mọi người tiếp cận và hiểu hơn về VPN và phương thức IPSec.

## 1.3. **Cấu trúc đề tài**

Chương 1: Tổng quan

Chương 2: Cơ sở lý thuyết

Chương 3: Kết quả thực nghiệm

Chương 4: Kết luận và hướng phát triển

# CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

## 2.1 VPN

### 2.1.1. VPN LÀ GÌ ?

Có rất nhiều định nghĩa về VPN, trong đó VPN được hiểu là dịch vụ mạng riêng ảo (mạng ảo) hay là mạng kết nối các site khách hàng đảm bảo an ninh trên cơ sở hạ tầng mạng chung. Là thuật ngữ viết tắt của Virtual Private Network. VPN được triển khai trên cơ sở hạ tầng của hệ thống mạng công cộng, giúp tạo nên những kết nối mạng an toàn khi tham gia mạng riêng của nhà cung cấp dịch vụ hoặc mạng công cộng internet,…

Dựa trên diện tích địa lý, khu vực mà mỗi hệ thống mạng riêng ảo có thể kết nối với nhiều site khác nhau. Bạn có thể kết nối VPN với máy tính, điện thoại giống như nó đang nằm trên cùng mạng nội bộ. Tất cả traffic đều được gửi qua và kết nối an toàn đến VPN. Do đó, bạn hoàn toàn có thể yên tâm về độ bảo mật tài nguyên mạng nội bộ.

Ngoài ra, khi bạn đang sử dụng wifi public, truy cập web bị giới hạn địa lý hay bị chặn, bạn sẽ không phải lo lắng điều này sử dụng VPN. Nhờ kết nối VPN đã được mã hóa, tất cả thông tin, yêu cầu, dữ liệu trao đổi giữa bạn với website sẽ được bảo vệ trong một kết nối an toàn.

### 2.1.2.VPN HOẠT ĐỘNG NHƯ THẾ NÀO

VPN hoạt động nhờ vào sự kết hợp với các giao thức đóng gói: PPTP, L2TP, IPSec, GRE, MPLS, SSL, TLS. Việc thiết lập kênh truyền ảo phụ thuộc mô hình mạng và nhu cầu sử dụng mà chọn loại thiết kế cho phù hợp. Công nghệ VPN có thể được phân thành 2 loại cơ bản: Site-to-Site VPN và Remote Access VPN.

**Site-to-Site VPN:**

Đây là mô hình được sử dụng chủ yếu ở các văn phòng doanh nghiệp. Nếu nhiều văn phòng trong một công ty được kết nối với nhau được gọi là Intranet (VPN cục bộ). Ngược lại, nếu công ty sử dụng loại VPN Site-to-site để kết nối với văn phòng của một công ty khác thì được gọi là Extranet (VPN mở rộng). Site-to-site tạo ra một cầu nối ảo giữa các mạng tại các văn phòng ở xa và kết nối chúng thông qua Internet và duy trì truyền thông an toàn và riêng tư giữa các mạng.

**Remote Access VPN:**

Đây là mô hình VPN khách hàng kết nối với VPN máy chủ, nó được coi như dạng User-to-LAN, thích hợp cho người dùng ở xa. Ngoài ra, còn được áp dụng cho nhân viên làm việc lưu động hay làm việc ở nhà muốn kết nối vào mạng công ty một cách an toàn, hoặc cho văn phòng nhỏ ở xa kết nối vào Văn phòng trung tâm của công ty.

### 2.1.3. VÌ SAO CẦN PHẢI SỬ DỤNG VPN

VPN cung cấp nhiều đặc tính hữu ích cho người sử dụng, bao gồm:

**Chi phí thấp:** chi phí thiết lập mạng VPN thấp do sử dụng chung hạ tầng Internet. Chi phí VPN thấp hơn so với các mạng WAN truyền thống như Frame Relay, ATM, Leased Line.

**Tăng cường tính bảo mật cho hệ thống:** sử dụng các giao thức đóng gói, các thuật toán mã hóa và các phương pháp chứng thực để bảo mật dữ liệu trong quá trình truyền.

**Bảo mật địa chỉ IP:** các địa chỉ bên trong mạng riêng được che giấu và chỉ sử dụng các địa chỉ bên ngoài Internet do thông tin được gửi đi trên VPN đã được mã hóa.

**Tính mở rộng và linh động:** VPN có thể kết nối tất cả các hệ thống mạng trên toàn quốc, xóa bỏ rào cản địa lý, sẵn sàng kết nối các mạng riêng lại với nhau một cách dễ dàng thông qua môi trường Internet.

### 2.1.4. CHỨC NĂNG CỦA VPN

Dựa vào những phân tích trên, ta có thể thấy VPN là công cụ khá đơn giản, chi phí thấp mà còn có nhiều chức năng cho người sử dụng dễ dàng:

**Tải tệp tin**

Các traffic mà ISP của bạn sẽ không phải gặp trở ngại, tốc độ tải file nhanh chóng hơn nhiều nếu bạn tải BitTorrent trên công nghệ VPN

**Truy cập dễ dàng tới website bị chặn, giới hạn địa lý**

Dù bạn bất cứ nơi nào khoảng cách xa hay gần nếu có internet, VPN giúp bạn truy cập web dễ dàng. Xóa bỏ vướng mắc về thủ tục kiểm duyệt internet, vượt bức tường lửa.

**Truy cập vào mạng gia đình dù không ở nhà**

Bạn vẫn có thể dễ dàng truy cập vào mạng gia đình dù không có mặt ở nhà nếu thiết lập mạng riêng ảo VPN. Thao tác này sẽ giúp bạn truy cập Windows từ xa qua mạng internet. Bạn có thể sử dụng tập tin được chia sẻ trong mạng nội bộ, chơi game trên máy tính giống như đang sử dụng mạng LAN.

**Truy cập mạng doanh nghiệp từ xa**

Mọi nguồn lực bao gồm tài nguyên cục bộ, trong khi đi đường, du lịch, ở xa,.. phải tiếp xúc trực tiếp với internet để tăng tính bảo mật cao.

**Web ẩn danh được duyệt**

Thông thường các web không có khóa SSL thì khi bạn sử dụng wifi công cộng để duyệt web, tính an toàn dữ liệu sẽ không cao. Do đó, bạn cần ẩn hoạt động duyệt web thông qua việc kết nối với mạng riêng ảo VPN. Khi đó, mọi thông tin truyền qua sẽ được mã hóa.

### 2.1.5. CÁC LOẠI GIAO THỨC HOẠT ĐỘNG CÓ TRONG VPN

Hai loại VPN kể trên được giao thức bảo mật VPN khác nhau. Mỗi giao thức VPN cung cấp các tính năng và mức độ bảo mật khác nhau. Trong đó, có 6 loại chính:

**IP Security – IPSec:** là giao thức được sử dụng để đảm bảo giao tiếp Internet qua mạng IP. IPSec giữa giao thức Internet Protocol bằng cách xác thực phiên làm việc và mã hóa từng gói dữ liệu trong suốt quá trình kết nối.

**Secure Sockets Layer – SSL và Transport Layer Security – TLS:** Đây là hai giao thức tạo ra một kết nối VPN, nơi trình duyệt web hoạt động như truy cập của khách hàng và người dùng được giới hạn cho các ứng dụng cụ thể thay vì toàn bộ mạng.

**Point – to – point Tunneling protocol (PPTP):** Dựa vào giao thức này, VPN mã hóa dữ liệu giữa các kết nối. Đồng thời, tạo ra một đường hầm và gói gọn gói dữ dữ liệu bảo mật an toàn

**Secure Shell (SSH):** tạo ra đường hầm VPN qua đó chuyển dữ liệu sẽ xảy ra và đảm bảo rằng đường hầm được mã hóa. Các kết nối SSH được tạo bởi một máy khách SSH và dữ liệu được chuyển từ một cổng cục bộ tới máy chủ từ xa thông qua đường hầm được mã hóa.

**Layer 2 Tunneling Protocol – L2TP:** là một giao thức đường hầm thường kết hợp với một giao thức bảo mật VPN khác như IPSec để tạo kết nối VPN an toàn cao. L2TP tạo một đường hầm giữa hai điểm kết nối L2TP và giao thức IPSec mã hóa dữ liệu và xử lý truyền thông an toàn giữa đường hầm

**OpenVPN:** là một VPN nguồn mở hữu ích cho việc tạo các kết nối từ điểm đến điểm và kết nối từ trang web tới địa điểm. Nó sử dụng một giao thức bảo mật tùy chỉnh dựa trên giao thức SSL và TLS.

**2.1.6. ƯU, NHƯỢC ĐIỂM CỦA VPN**

**Ưu điểm của VPN**

**Tính linh hoạt:** VPN ngoài mang tính mềm dẻo đối với yêu cầu sử dụng mà nó còn linh hoạt trong suốt quá trình vận hành.

**Khả năng mở rộng:** VPN có thể sử dụng bất cứ địa lý nào có mạng, do hệ thống được xây dựng dựa trên hạ tầng mạng công cộng internet.

**Giảm thiểu hỗ trợ về mặt kỹ thuật:** Việc chuẩn hóa các yêu cầu bảo mật và chuẩn hóa trên cùng kiểu kết nối từ đối tượng di động đến POP của ISP

**Đáp ứng nhu cầu thương mại:** Với đa dạng các loại hình mạng riêng ảo MPV khác nhau đáp ứng đủ thị yếu khách hàng theo nhu cầu, ngân sách, vốn đầu tư.

**Nhược điểm của VPN**

VPN có thể làm chậm tốc độ truy cập Internet

Việc sử dụng VPN vào những mục đích sai có thể gây phản tác dụng

VPN chất lượng thường có chi phí khá cao. Điều này đòi hỏi bạn cần có một khoản ngân sách ổn định hàng tháng cho VPN.

Những trang web trực tuyến đang ngày càng cảnh giác với VPN, từ đó tạo ra những trở ngại nhằm giảm lượng truy cập vào nội dung bị hạn chế.

**2.1.7. Lịch sử phát triển của VPN**

Sự xuất hiện mạng chuyên dùng ảo, còn gọi là mạng riêng ảo (VPN), bắt nguồn từ yêu cầu của khách hàng (client), mong muốn có thể kết nối một cách có hiệu quả với các tổng đài thuê bao (PBX) lại với nhau thông qua mạng diện rộng (WAN). Trước kia, hệ thống điện thoại nhóm hoặc là mạng cục bộ (LAN) trước kia sử dụng các đường thuê riêng cho việc tổ chức mạng chuyên dùng để thực hiện việc thông tin với nhau.

**Các mốc đánh dấu sự phát triển của VPN:**

- **1975:** Franch Telecom đưa ra dịch vụ Colisee, cung cấp dịch vụ dây chuyền dùng cho các khách hàng lớn. Colisee có thể cung cấp phương thức gọi số chuyên dùng cho khách hàng. Dịch vụ này căn cứ vào lượng dịch vụ mà đưa ra cước phí và nhiều tính năng quản lý khác.

- **1985:** AT&T đưa ra dịch vụ VPN có tên riêng là mạng được định nghĩa bằng phần mềm SDN

- **1986:** Sprint đưa ra Vnet, Telefonica Tây Ban Nha đưa ra Ibercom.

- **1988:** Nổ ra đại chiến cước phí dịch vụ VPN ở Mỹ, làm cho một số xí nghiệp vừa và nhỏ mở rộng sử dụng VPN và có thể tiết kiệm gần 30% chi phí, đã kích thích sự phát triển nhanh chóng dịch vụ này tại Mỹ

- **1989:** AT&T đưa ra dịch vụ quốc tế IVPN là GSDN

- **1990:** Telstra của Ô-xtrây-li-a đưa ra dich vụ VPN trong nước đầu tiên ở khu vực châu Á – Thái Bình Dương.

- **1992:** Viễn thông Hà Lan và Telia Thuỵ Điển thành lập công ty hợp tác đầu tư Unisource, cung cấp dịch vụ VPN

- **1993:** AT&T, KDD và viễn thông Singapore tuyên bố thành lập Liên minh toàn cầu Worldpartners, cung cấp hàng loạt dịch vụ quốc tế, trong đó có dịch vụ VPN.

- **1994:** BT và MCI thành lập công ty hợp tác đầu tư Concert, cung cấp dịch vụ VPN, dịch vụ chuyển tiếp khung (Frame relay)…

- **1995:** ITU-T đưa ra khuyến nghị F-16 về dịch vụ VPN toàn cầu (GVPNS).

- **1996:** Sprint và viễn thông Đức (Deustch Telecom), Viễn thông Pháp (French Telecom) kết thành liên minh Global One.

- **1997:** Có thể coi là một năm rực rỡ đối với công nghệ VPN, công nghệ này có mặt trên khắp các tạp chí khoa học công nghệ, các cuộc hội thảo…Các mạng VPN xây dựng trên cơ sở hạ tầng mạng Internet công cộng đã mang lại một khả năng mới, một cái nhìn mới cho VPN.

Công nghệ VPN là giải pháp thông tin tối ưu cho các công ty, tổ chức có nhiều văn phòng, chi nhánh lựa chọn. Hiện nay, VPN không chỉ dùng cho dịch vụ thoại mà còn dùng cho các dịch vụ dữ liệu, hình ảnh và các dịch vụ đa phương tiện.

**2.2. IPSEC**

**2.2.1. IPSEC LÀ GÌ ?**

IPsec là một nhóm giao thức được sử dụng cùng nhau để thiết lập các kết nối được mã hóa giữa các thiết bị. Nó giúp bảo mật dữ liệu được gửi qua public network. Nhóm giao thức này này thường được sử dụng để thiết lập VPN. Nó hoạt động bằng cách mã hóa IP packet cùng với việc xác thực nguồn của các packet.

Trong thuật ngữ “IPsec”, “IP” là viết tắt của “Internet Protocol” và “sec” là “security”. Internet Protocol là một routing protocol chính được sử dụng trên Internet. Nó chỉ định nơi dữ liệu sẽ đi bằng địa chỉ IP. Nhóm giao thức này an toàn vì nó thêm mã hóa và xác thực vào quá trình này.

**2.2.2. SƠ LƯỢC VỀ LỊCH SỬ CỦA IPSEC**

Khi Internet Protocol được phát triển vào đầu những năm 80, tính bảo mật không nằm ở vị trí được ưu tiên cao. Tuy nhiên, khi số lượng người dùng Internet tiếp tục phát triển, nhu cầu bảo mật cao cũng vì thế mà ngày càng tăng.

 Để giải quyết nhu cầu này, Cơ quan An ninh Quốc gia đã tài trợ cho sự phát triển của các giao thức bảo mật vào giữa những năm 80, trong chương trình Secure Data Network Systems (Hệ thống mạng dữ liệu bảo mật). Điều này dẫn đến sự phát triển của Security Protocol (Giao thức bảo mật) ở Layer 3 và cuối cùng là Network Layer Security Protocol. Nhiều kỹ sư đã làm việc trong dự án này trong suốt những năm 90 và IPSec đã phát triển nhờ những nỗ lực này. IPSec hiện là một tiêu chuẩn mã nguồn mở và là một phần của IPv4

**2.2.3. CÁCH THỨC HOẠT ĐỘNG CỦA IPSEC**

Khi hai máy tính thiết lập kết nối VPN, chúng phải đồng thuận về một tập hợp các giao thức bảo mật và thuật toán mã hóa, đồng thời trao đổi key mật mã để mở khóa và xem dữ liệu đã mã hóa.

Đây là lúc IPSec phát huy vai trò. IPSec làm việc với các VPN tunnel để thiết lập kết nối hai chiều riêng tư giữa các thiết bị. IPSec không phải là một giao thức đơn lẻ; thay vào đó, đó là một bộ giao thức và tiêu chuẩn hoàn chỉnh, hoạt động cùng nhau để giúp đảm bảo tính bảo mật, toàn vẹn và xác thực của các gói dữ liệu Internet đi qua VPN tunnel.

Đây là cách IPSec tạo một VPN tunnel bảo mật:

IPSec xác thực dữ liệu để đảm bảo tính toàn vẹn của gói dữ liệu trong quá trình truyền tải.

IPSec mã hóa lưu lượng truy cập Internet qua các VPN tunnel để không thể xem dữ liệu.

IPSec bảo vệ dữ liệu khỏi các cuộc tấn công Replay Attack, có thể dẫn đến việc đăng nhập trái phép.

IPSec cho phép trao đổi key mật mã bảo mật giữa các máy tính.

IPSec cung cấp hai chế độ bảo mật: Tunnel và Transport.

VPN IPSec bảo vệ dữ liệu truyền từ host đến host, mạng đến mạng, host đến mạng và cổng đến gateway (được gọi là chế độ Tunnel, khi toàn bộ gói IP được mã hóa và xác thực).

**2.2.4. VAI TRÒ CỦA IPSEC**

Cho phép xác thực hai chiều, trước và trong quá trình truyền tải dữ liệu.

Mã hóa đường truyền giữa hai máy tính khi được gửi qua một mạng.

Bảo vệ gói dữ liệu IP và phòng ngự các cuộc tấn công mạng không bảo mật

IPSEC bảo vệ các lưu lượng mạng bằng việc sử dụng mã hóa và đánh dấu dữ liệu

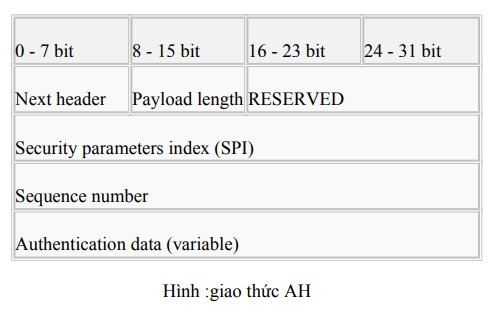
Một chính sách IPSec cho phép định nghĩa ra các loại lưu lượng mà IPSec sẽ kiểm tra và cách các lưu lượng đó sẽ được bảo mật và mã hóa như thế nào

**2.2.5. NHỮNG GIAO THỨC ĐƯỢC SỬ DỤNG TRONG IPSEC**

Trong mạng, protocol là một cách định dạng dữ liệu cụ thể để bất kỳ máy tính kết nối mạng nào cũng có thể diễn giải dữ liệu. Nhóm giao thức này không phải là một protocol, mà là một tập hợp các protocol. Các protocol sau tạo nên bộ IPsec:

**Authentication Header (AH):** protocol AH đảm bảo rằng các data packet đến từ một nguồn đáng tin cậy và dữ liệu không bị giả mạo, giống như một con dấu chống giả mạo trên một sản phẩm tiêu dùng. Các header này không cung cấp bất kỳ mã hóa nào, chúng không giúp che giấu dữ liệu khỏi hacker. AH sử dụng cả 2 kiểu hoạt động transport và tunnel.

Cấu trúc gói AH



Chú thích:

Next header (tiêu đề tiếp theo): có độ dài 8bit, 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 (đề nghị duyệt thảo) gần nhất

Payload length (độ dài tải tin): dung lượng tối đa của gói dữ liệu, có độ dài 8 bit 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 bit 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 bit 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 bit và có tính bắt buộc, mỗi gói được gửi đi thì tăng một lần, bộ đếm bên gửi và nhận được khởi tạo ban đầu là 0, gói đầu tiên có số thứ tự là 1

Authentication Data (dữ liệu xác 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

Quá trình xử lý của AH:

B1: Toàn bộ gói IP (bao gồm IP header và tải tin) được thực hiện qua một hàm băm một chiều.

B2: Mã hash thu được dùng để xây dựng một AH header, đưa header này vào gói dữ liệu ban đầu.

B3: Gói dữ liệu sau khi thêm AH header được truyền tới đối tác IPSec.

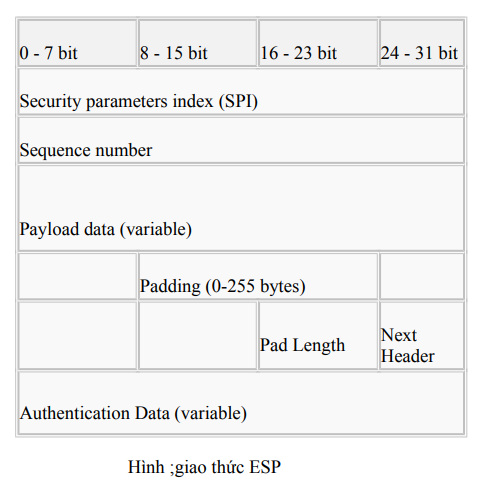
B4:  Bên thu thực hiện hàm băm với IP header và tải tin, kết quả thu được một mã hash.

B5: Bên thu tách mã hash trong AH header.

B6: Bên thu so sánh mã hash mà nó tính được mà mã hash tách ra từ AH header. Hai mã hash này phải hoàn toàn giống nhau. Nếu khác nhau chỉ một bit trong quá trình truyền thì 2 mã hash sẽ không giống nhau, bên thu lập tức phát hiện tính không toàn vẹn của dữ liệu.

**Encapsulating Security Protocol (ESP):** ESP mã hóa IP header cho mỗi packet – trừ khi transport data mode được sử dụng. Trong trường hợp này, nó chỉ mã hóa payload. ESP thêm header riêng và một đoạn trailer vào mỗi data packet.

Cấu trúc gói ESP



Chú thích:

SPI (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.

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

Padding (0-255 bytes): được thêm vào cho đủ kích thước của gói tin, giúp phân biệt với Authentication Data, ngoài ra còn có thể sử dụng để che dấu độ dài thực của Payload

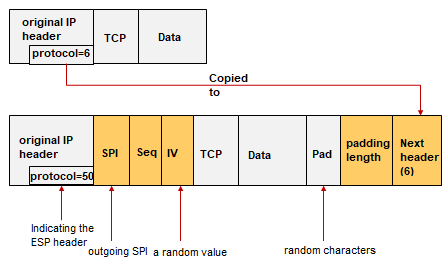
Pad Length và NextHeader: giống như của AH

Authentication Data: giúp xác thực thông tin trên gói ESP

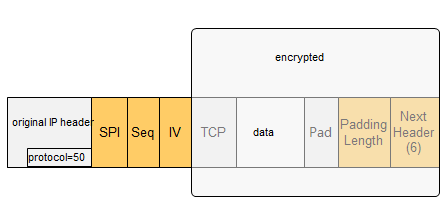
Quá trình xử lý của ESP:

Ở transport mode:

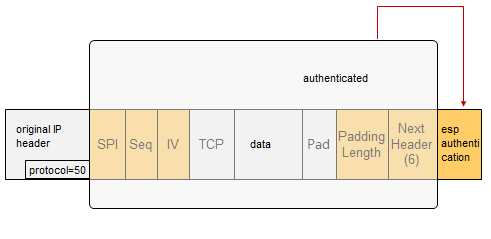
B1: trường giao thức IP Header gốc được sao chép sang trường NextHeader, và được cài đặt mặc định là 50 cho biết giao thức ấy là ESP.



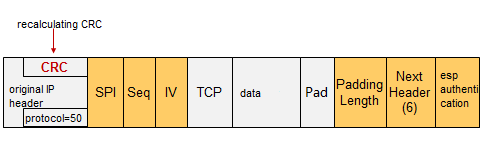
B2: Các nội dung như sau sẽ được mã hóa



B3: Tính toán mã băm được thực thi và trả kết quả về trường xác thực



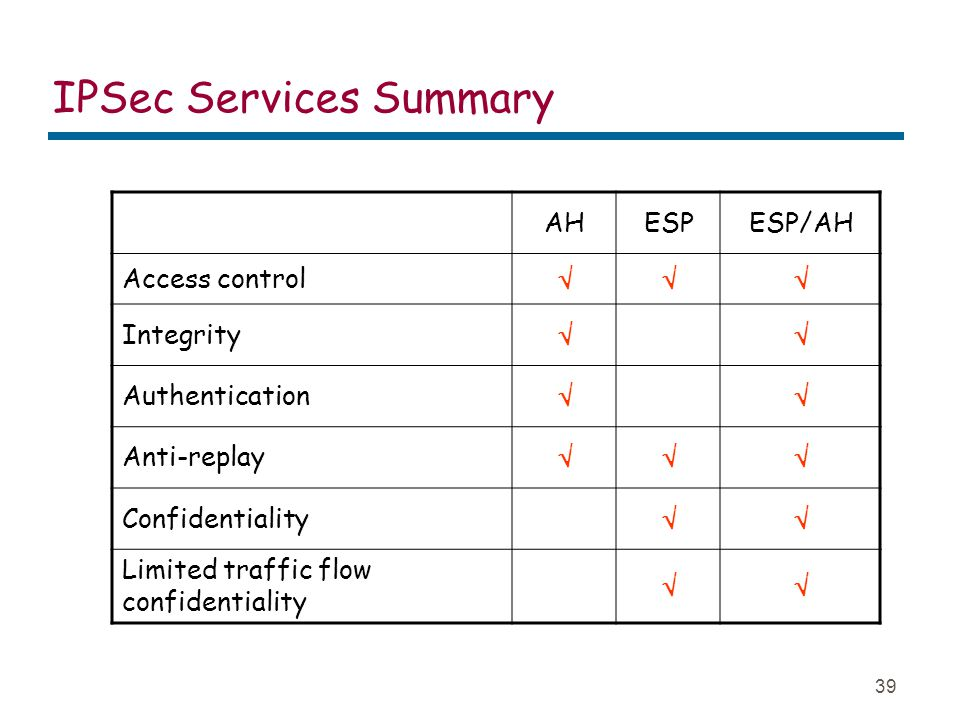
B4: CRC (kiểm tra định kỳ theo chu kỳ) ở IP Header tiến hành tính toán lại.



Ở tunnel mode:

Trước khi thực hiện các quy trình như trên, ESP Header sẽ được thêm vào trước gói IP gốc hỗ trợ cho quá trình bảo mật. Nếu gói IP gốc là IPv4 thì trường NextHeader là 4. Sau đó một địa chỉ IP mới được thêm vào trước ESP Header.

**SO SÁNH AH & ESP**



Chú thích:

* + Access control: khả năng điều khiển truy cập
  + Integrity: tính toàn vẹn
  + Authentication: tính xác thực
  + Anti-replay: tránh người dùng không mong muốn
  + Confidentiality: tính bảo mật
  + Limited traffic flow confidentiality: giới hạn lưu lượng băng thông

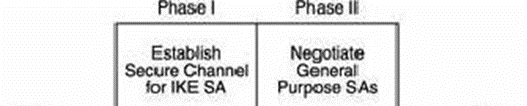
Vì không thực hiện công đoạn mã hóa nên AH sẽ nhanh hơn ESP

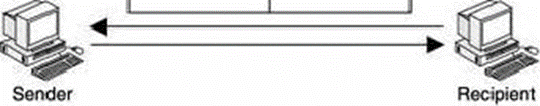
Tính toàn vẹn của dữ liệu được đảm bảo nhờ vào thông điệp phân loại, các thông điệp ấy được tạo ra từ thuật toán.

**Encryption and Hashing Algorithms:** Key mật mã hoạt động bằng cách sử dụng giá trị hash, được tạo bằng thuật toán hash. AH và ESP rất chung chung, chúng không chỉ định một loại mã hóa cụ thể. Tuy nhiên, IPsec thường sử dụng Message Digest 5 hoặc Secure Hash Algorithm 1 để mã hóa.

**Security Association (SA):** SA đề cập đến một số protocol được sử dụng để đàm phán các key và thuật toán mã hóa. Một trong những protocol SA phổ biến nhất là Internet Key Exchange (IKE).

IKE bao gồm 2 giai đoạn





Giai đoạn 1:

-   Đầu tiên, xác nhận các điểm thông tin , sau đó thiết lập một kênh bảo mật cho sự thiết lập SA.Tiếp đó các thông tin thỏa thuận một ISAKMP SA đồng ý lẫn nhau, bao gồm các thuật toán mã hóa, hàm băm , các phương pháp xác nhận bảo vệ mã khóa.

-   Sau khi cơ chế mã hóa và hàm băm đã được đồng ý ở trên, một khóa sẽ bí mật phát sinh. Theo Sau là những thông tin được dùng để phát sinh khóa bí mật: giá trị Diffie-Hellman, SPI của ISAKMP SA ở dạng cookies, số ngẫu nhiên known as nonces (dùng ký xác nhận)

-   Nếu hai bên đồng ý sử dụng phương pháp xác nhận dựa trên public key , chúng cũng cần trao đổi IDs. Sau khi trao đổi thông tin cần thiết, cả hai bên phát sinh những khóa riêng của chính mình sử dụng chúng để chia sẻ bí mật. Theo cách này, những khóa mã hóa được phát sinh mà không cần thực sự trao đổi bất kỳ khóa nào thông qua mạng.

Giai đoạn 2:

-   Trong khi giai đoạn 1 thỏa thuận thiết lập SA cho ISAKMP , giai đoạn 2 giải quyết bằng việc thiết lập SAs cho IPSec. Trong giai đoạn này SAs dùng nhiều dịch vụ khác nhau thỏa thuận. Cơ chế xác nhận, hàm băm, và thuật toán mã hóa bảo vệ gói dữ liệu IPSec tiếp theo (sử dụng AH và ESP) dưới hình thức một phần của giai đoạn SA.

-   Sự thỏa thuận của giai đoạn xảy ra thường xuyên hơn giai đoạn 1. Điển hình sự thỏa thuận có thể lặp lại sau 4- 5 phút. Sự thay đổi thường xuyên các mã khóa ngăn cản các hacker bẻ gãy những khóa này và sau đó là nội dung của gói dữ liệu.

-   Tổng quát một phiên làm việc ở giai đoạn 2 tương đương với một phiên làm việc đơn của giai đoạn 1. Tuy nhiên, nhiều sự thay đổi ở giai đoạn 2 cũng có thể được hỗ trợ bởi một trường hợp đơn ở giai đoạn 1. Điều này làm cho quá trình giao dịch chậm chạp có vẻ nhanh hơn.

IKE hiện nay có 2 phiên bản : Phiên bản đầu tiên của giao thức (IKEv1) được giới thiệu vào năm 1998 và phiên bản thứ hai (IKEv2) ra mắt 7 năm sau đó. Có một số điểm khác biệt giữa IKEv1 và IKEv2, trong đó nổi bật là việc IKEv2 giảm yêu cầu về băng thông.

**Bảo vệ chống lại các cuộc tấn công Replay Attack:** IPSec cũng kết hợp các tiêu chuẩn để ngăn việc replay (phát lại) bất kỳ gói dữ liệu nào, một phần của quá trình đăng nhập thành công. Tiêu chuẩn này ngăn chặn tin tặc sử dụng thông tin được replay để tự sao chép thông tin đăng nhập.

Cuối cùng, mặc dù Internet Protocol (IP) không phải là một phần của IPsec, những nhóm giao thức này chạy trực tiếp trên IP.

**2.2.6. NHỮNG TÍNH NĂNG CỦA IPSEC (IPSEC Security Protocol)**

Tính xác nhận và tính nguyên vẹn dữ liệu(Authentication and data integrity) IPSec cung cấp một cơ chế mạnh mẽ để xác nhận tính chất xác thực của người gửi và kiểm chứng bất kỳ sự sửa đổi không được bảo vệ trước đó của nội dung gói dữ liệu bởi người nhận. Các giao thức IPSec đưa ra khả năng bảo vệ mạnh để chống lại các dạng tấn công giả mạo, đánh hơi và từ chối dịch vụ.

Sự cẩn thận (Confidentiality) Các giao thức IPSec mã hóa dữ liệu bằng cách sử dụng kỹ thuật mã hóa cao cấp, giúp ngăn cản người chưa chứng thực truy cập dữ liệu trên đường đi của IPSec cũng dùng cơ chế tạo hầm để ẩn địa chỉ IP của nút nguồn (người gửi) và nút đích (người nhận) từ những kẻ nghe lén.

Quản lý khóa (Key management) IPSec dùng một giao thức thứ ba, Internet Key Exchange để thỏa thuận các giao thức bảo mật và các thuật toán mã hóa trước và trong suốt phiên giao dịch. Một phần quan trọng nữa, IPSec phân phối và kiểm tra các khóa mã và cập nhật những khóa đó khi được gửi các yêu cầu.

Hai tính năng đầu tiên của bộ IPSec, authentication and data integrity, confidentiality, được cung cấp bởi hai giao thức chính của trong bộ giao thức IPSec. Những giao thức này bao gồm Authentication Header (AH) và Encapsulating Security Payload (ESP)

Tính năng thứ ba, key management, nằm trong bộ giao thức khác, được bộ IPSec chấp nhận bởi nó là một dịch vụ quản lý khóa mạnh. Giao thức này là IKE

**2.2.7. CẤU TRÚC BẢO MẬT**

IPSec được triển khai sử dụng các giao thức cung cấp mật mã (cryptographic protocols) nhằm bảo mật gói tin (packet) trong quá trình truyền, phương thức xác thực và thiết lập các thông số mã hóa.

Xây dựng IPSec sử dụng khái niệm về bảo mật trên nền tảng IP. Một số kết hợp bảo mật rất đơn giản khi kết hợp các thuật toán và các thông số (ví như các khóa – keys) là nền tảng trong việc mã hóa và xác thực trong một chiều. Tuy nhiên trong các giao tiếp hai chiều, các giao thức bảo mật sẽ làm việc với nhau và đáp ứng quá trình giao tiếp. Thực tế lựa chọn các thuật toán mã hóa và xác thực lại phụ thuộc vào người quản trị IPSec bởi IPSec bao gồm một nhóm các giao thức bảo mật đáp ứng mã hóa và xác thực cho mỗi gói tin IP.

Trong các bước thực hiện phải quyết định cái gì cần bảo vệ và cung cấp cho gói tin outgoing (đi ra ngoài), IPSec sử dụng các thông số Security Parameter Index (SPI), mỗi quá trình index (đánh thứ tự và lưu trong dữ liệu – Index ví như cuốn danh bạ điện thoại) bao gồm Security Association Database (SADB), theo suốt chiều dài của địa chỉ đích trong header của gói tin, cùng với sự nhận dạng duy nhất của thỏa hiệp bảo mật (tạm dịch từ - security association) cho mỗi gói tin. Một quá trình tương tự cũng được làm với gói tin đi vào (incoming packet), nơi IPSec thực hiện quá trình giải mã và kiểm tra các khóa từ SADB.

Cho các gói multicast, một thỏa hiệp bảo mật sẽ cung cấp cho một group, và thực hiện cho toàn bộ các receiver trong group đó. Có thể có hơn một thỏa hiệp bảo mật cho một group, bằng cách sử dụng các SPI khác nhau, tuy nhiên nó cũng cho phép thực hiện nhiều mức độ bảo mật cho một group. Mỗi người gửi có thể có nhiều thỏa hiệp bảo mật, cho phép xác thực, trong khi người nhận chỉ biết được các keys được gửi đi trong dữ liệu.

**2.2.8. SỰ KHÁC BIỆT GIỮA CHẾ ĐỘ IPSEC TUNNEL VÀ IPSEC TRANSPORT**

- Chế độ Tunnel: Trong chế độ Tunnel, toàn bộ gói tin được bảo vệ. IPSec gói dữ liệu trong một packet mới, mã hóa nó và thêm một IP header mới. Nó thường được sử dụng trong thiết lập VPN site-to-site.

 - Chế độ Transport: Trong chế độ Transport, IP header gốc vẫn còn và không được mã hóa. Chỉ có payload và ESP trailer được mã hóa mà thôi. Chế độ Transport thường được sử dụng trong thiết lập VPN client-to-site.

Đối với các VPN, cấu hình IPSec phổ biến nhất mà bạn sẽ thấy là ESP với xác thực ở chế độ Tunnel. Cấu trúc này giúp lưu lượng truy cập Internet di chuyển bảo mật và ẩn danh bên trong VPN tunnel qua các mạng không bảo mật.

Chế độ IPsec tunnel được sử dụng giữa hai bộ router chuyên dụng, với một bộ router hoạt động như một đầu của “tunnel” ảo thông qua public network. Trong chế độ IPsec tunnel, IP header ban đầu chứa đích cuối cùng của packet được mã hóa, cùng với packet payload. Để cho các router trung gian biết nơi chuyển tiếp các packet, IPsec thêm một IP header mới. Tại mỗi đầu cuối của tunnel, các router giải mã các IP header để chuyển các packet đến đích của chúng.

Trong chế độ transport, payload của một packet được mã hóa, nhưng IP header ban đầu thì không. Do đó, các router trung gian có thể xem đích cuối cùng của mỗi packet – trừ khi sử dụng một tunneling protocol ( chẳng hạn như GRE).

**2.2.9. IPSEC SỬ DỤNG PORT NÀO ?**

Network port là vị trí ảo, nơi mà dữ liệu được truyền đi trong máy tính. Port là cách máy tính theo dõi các quá trình và kết nối khác nhau, nếu dữ liệu đi đến một port nhất định, hệ điều hành của máy tính sẽ biết nó thuộc tiến trình nào. Nhóm giao thức này thường sử dụng port 500.

**2.2.10. IPSEC TÁC ĐỘNG ĐẾN MSS VÀ MTU NHƯ THẾ NÀO?**

MSS và MTU là hai phép đo dung lượng packet. Các packet chỉ có thể đạt đến một dung lượng nhất định (tính bằng byte) trước khi máy tính, router và switch không thể xử lý chúng. MSS đo kích thước payload của mỗi packet, trong khi MTU đo toàn bộ packet, bao gồm cả các header. Các packet vượt quá MTU của mạng có thể bị phân mảnh. Có nghĩa là được chia thành các packet nhỏ hơn và sau đó được tập hợp lại. Các packet vượt quá MSS chỉ đơn giản là bị loại bỏ.

**2.2.11. Điểm giống nhau giữa IPSec và SSL:**

- IPSec và SSL cung cấp xác thực Client và Server

- IPSec và SSL cung cấp tính năng đảm bảo an toàn và xác thực đối với dữ liệu, thậm chí trên các mức khác nhau của chồng giao thức

- IPSec và SSL có thể dùng các thuật toán mật mã mạnh cho việc mã hoá và các hàm băm, có thể sử dụng xác thực dựa trên chứng chỉ

- IPSec và SSL cung cấp tính năng sinh khoá và làm tươi khoá mà không phải truyền bất kỳ khoá nào dưới dạng rõ hay ngoại tuyến

**2.2.12. Điểm khác nhau giữa IPSec và SSL:**

- SSL được thực thi như một API giữa tầng ứng dụng và tầng vận tải; IPSec được thực thi như một khung làm việc tại tầng liên mạng.

- SSL cung cấp tính năng bảo mật từ ứng dụng - tới - ứng dụng(ví dụ: giữa WebBrowser và WebServer); IPSec cung cấp tính năng bảo mật từ thiết bị - tới - thiết bị.

- SSL không bảo vệ lưu lượng UDP; IPSec thì có

- SSL hoạt động từ điểm cuối - tới - điểm cuối và không có khái niệm đường hầm. Điều này có thể là một vấn đề lúc lưu lượng cần được xem xét bằng cách kiểm tra nội dung và quét virus trước khi nó được phân phối thành công đến đích; IPSec có thể hoạt động theo hai cách, điểm cuối - tới - điểm cuối và như một đường hầm

 - SSL có thể vượt qua NAT hoặc SOCKS, chúng dùng để che dấu cấu trúc địa chỉ bên trong hoặc tránh sự xung đột địa chỉ IP riêng; IPSec trong chế độ vận tải (end – to- end) không thể sử dụng NAT nhưng nó có thể dùng một đường hầm IPSec để đạt được mục tiêu tương tự và thậm chí bảo mật hơn NAT vì đường hầm cũng có thể được mã hoá.

- Các ứng dụng cần phải sửa đổi để sử dụng SSL. Điều này có thể là một vấn đề lúc ta không truy cập được mã nguồn của ứng dụng hoặc không có thời gian hay kinh nghiệm để thay đổi mã nguồn của ứng dụng; IPSec hoàn toàn trong suốt với các ứng dụng.

Thông thường SSL là tốt lúc ta chỉ có một ứng dụng được bảo vệ và nó đã sẵn có trong một phiên bản SSL-aware. Đây là trường hợp có một ứng dụng chuẩn đa dạng, không chỉ với WebBrowser và WebServer. Ngoài ra, nếu có tuỳ chọn của việc thực thi khái niệm 3-tier bằng cách tận dụng các cổng ứng dụng Web tại vành đai của mạng, SSL là một sự lựa chọn tốt. Nếu có một số lượng lớn các ứng dụng để bảo đảm an toàn có thể phải chọn giải pháp tốt hơn cho mạng. Trong trường hợp này, IPSec là sự lựa chọn tốt hơn. Trừ khi tự ta phát triển các ứng dụng, IPSec mềm dẻo hơn SSL để thực thi một chính sách bảo mật yêu cầu nhiều mức khác nhau và sự kết hợp của xác thực, mã hoá và đường hầm.

### 2.2.13. ƯU ĐIỂM VÀ KHUYẾT ĐIỂM CỦA IPSEC :

**2.2.13.1.**  **Ưu điểm:**

-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 tới bảo mật

-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.

-IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối,điều này giúp che dấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua internet.

**2.2.13.2.**  **Nhược điểm:**

-  Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và 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.

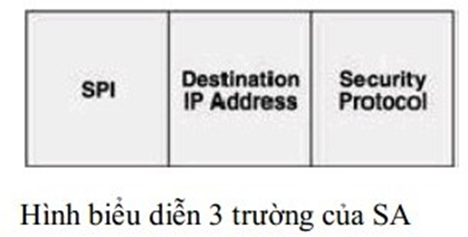
-  IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.

-  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.

-  Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

**2.2.14.**  **LIÊN KẾT BẢO MẬT:**

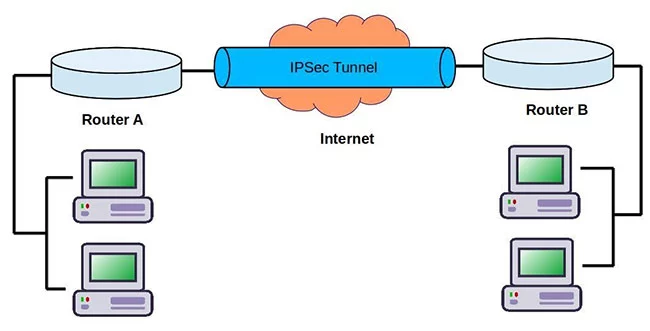
-SA(Security Associations): là một khái niệm cơ bản trong bộ giao thức IPSec.SA là một kết nối luận lý theo phương hướng duy nhất giữa hai thực thể sử dụng các dịch vụ IPSec.SA gồm có 3 trường:



  + SPI(Security Parameter Index):là một trường 32 bits dùng nhận dạng các giao thức bảo mật,được định nghĩa bởi các trường Security protocol trong bộ IPSec đang dung.SPI như là phần đầu của giao thức bảo mật và thường chọn bởi hệ thống đích trong suốt quá trình thỏa thuận của SA.

+Destination IP address:địa chỉ IP của nút đích.Cơ chế quản lý của SA chỉ được định nghĩa cho hệ thống unicast mặc dù nó có thể là hệ thống broadcast,unicast hay multicast.

+Security protocol;mô tả giao thức bảo mật IPSec,là AH hoặc ESP.SA trong IPSec được triển khai theo 2 chế độ :transport mode và tunnel mode.



Kết nối bộ giao thức này bao gồm các bước sau:

Trao đổi key: Key là yếu tố cần thiết để mã hóa, key là một chuỗi ký tự ngẫu nhiên có thể được sử dụng để “lock” (mã hóa) và “unlock” (giải mã) thông điệp. Nhóm giao thức này thiết lập các key với sự trao đổi key giữa các thiết bị được kết nối. Để mỗi thiết bị có thể giải mã tin nhắn của các thiết bị khác.

Header và trailer của packet: Tất cả dữ liệu được gửi qua mạng được chia thành các phần nhỏ hơn gọi là packet. Các packet chứa cả payload hoặc dữ liệu thực tế được gửi bao gồm cả các header hoặc thông tin về dữ liệu đó để các máy tính nhận packet biết phải làm gì với chúng. IPsec thêm một số header vào các packet dữ liệu chứa thông tin xác thực và mã hóa. Nhóm giao thức này cũng thêm các đoạn trailer, đi sau payload của một packet thay vì trước đó.

Xác thực: IPsec cung cấp xác thực cho mỗi packet, giống như một con dấu xác thực trên một vật phẩm sưu tầm được. Điều này đảm bảo rằng các packet đến từ một nguồn đáng tin và không phải là hacker.

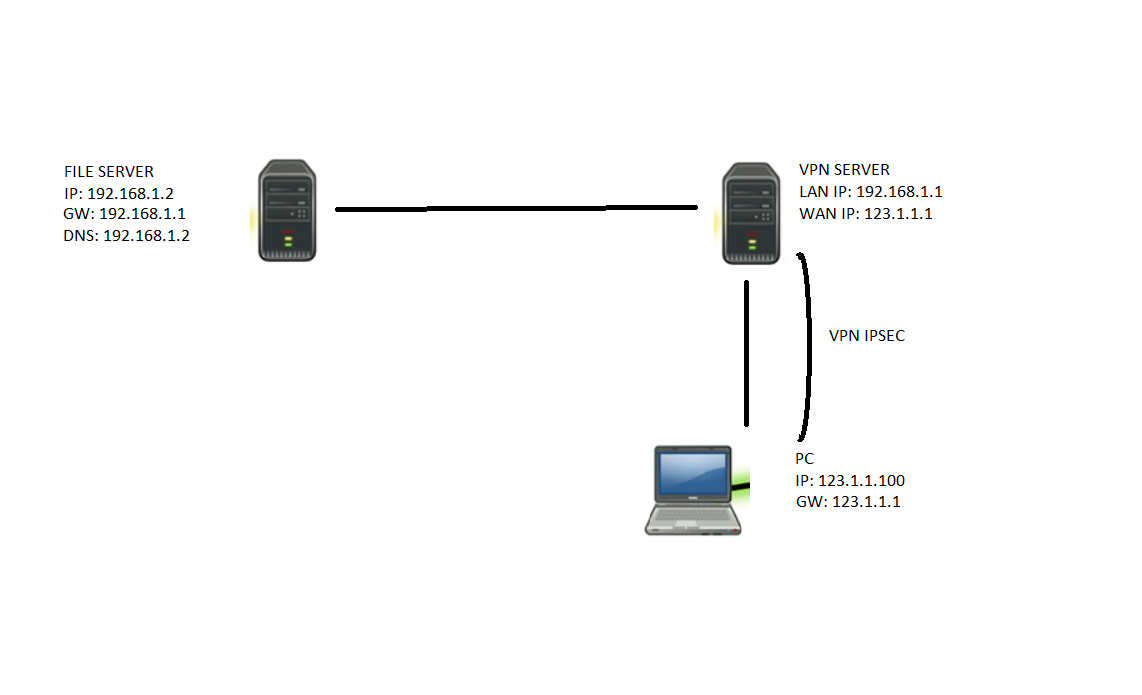
Mã hóa: IPsec mã hóa payload bên mỗi packet và IP header của mỗi packet. Điều này giữ cho dữ liệu được gửi qua nhóm giao thức này một cách an toàn và riêng tư.

Truyền dữ liệu: Các IPsec packet được mã hóa truyền dữ liệu qua một hoặc nhiều mạng đến đích của chúng bằng cách sử dụng một giao thức truyền tải. Ở giai đoạn này, lưu lượng IPsec khác với lưu lượng IP thông thường ở chỗ nó thường sử dụng UDP làm giao thức truyền tải hơn là TCP. TCP (Transmission Control Protocol) thiết lập các kết nối chuyên dụng giữa các thiết bị và đảm bảo rằng tất cả các packet đều được truyền đến đích. UDP (User Datagram Protocol) không thiết lập các kết nối chuyên dụng này. Nhóm giao thức này sử dụng UDP vì nó cho phép các IPsec packet vượt qua firewall.

Giải mã: Ở đầu kia của giao tiếp, các packet được giải mã và các app hiện có thể sử dụng dữ liệu được phân phối.

**CHƯƠNG III:KẾT QUẢ THỰC NGHIỆM**

* 1. Sơ đồ kịch bản



3.2. Công cụ

Vmware Workstation Pro ( Version 16.2.3 build-19376536 )

3.3. Các bước thực hiện

- Đặt IP cho các server và pc như sơ đồ

- Máy VPN Server có 2 card mạng Lan và Wan

- Ping thông giữa các máy kết nối trực tiếp

- Trên File Server tạo thư mực Data và cho phép chia sẻ dữ liệu

- Trên VPN Server tạo một tài khoản để thiết lập dịch vụ

- Thực hiện cài đặt Remote Access

- Thực hiện cấu hình dịch vụ VPN Server

- Trên PC thực hiện kết nối VPN

- Thiết lập giao thức IPSec

- Kết nối VPN nhập tài khoản mật khẩu vpn vừa tạo.

- Kết nối VPN với giao thức IPSec thành công

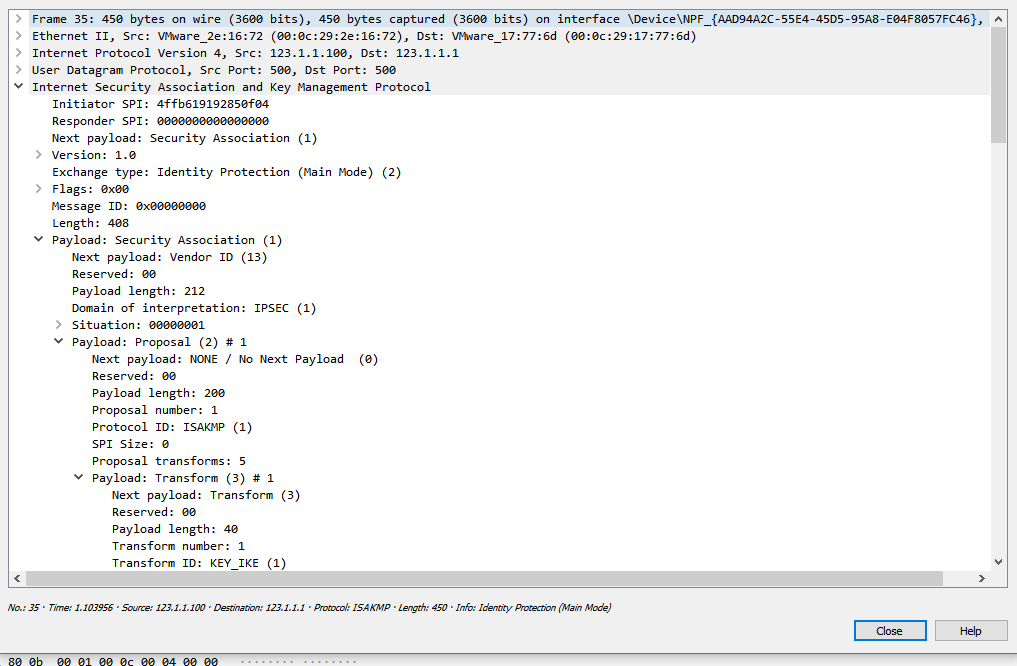
- Truy cập vào File Server để lấy file dữ liệu

- Kiểm tra quá trình bảo mật của giao thức IPSec

3.4. Kết quả:

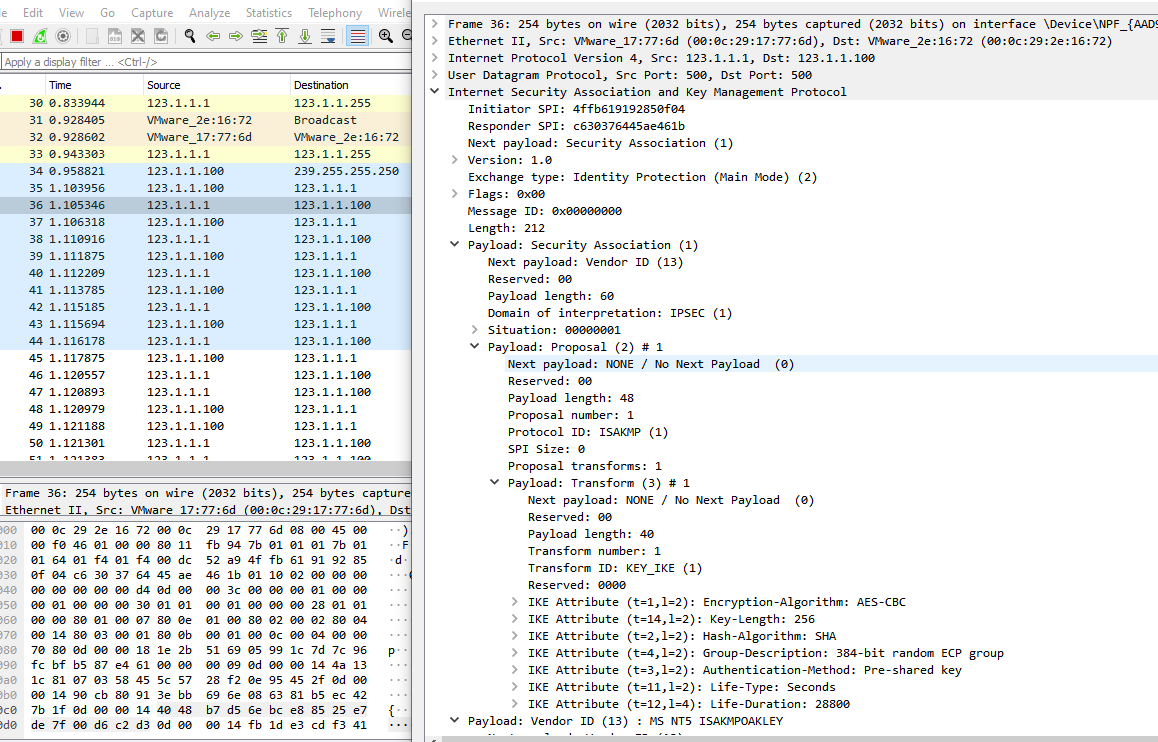
Giai đoạn 1  
  
- Hai bên tiến hành đàm phán về các thông tin sau :  
o Hashing (hàm băm)  
o Authentication (chứng thực )  
o DH (Diffie Hellman) group  
o Lifetime  
o Encryption  
  
2 Message đầu tiên được dùng để thỏa thuận các chính sách bảo mật IKE  
bao gồm: thuật toán mã hóa, độ dài key, thuật toán hash, phương pháp chứng thực,  
thời gian bao lâu trao đổi key

+ Messager 1:



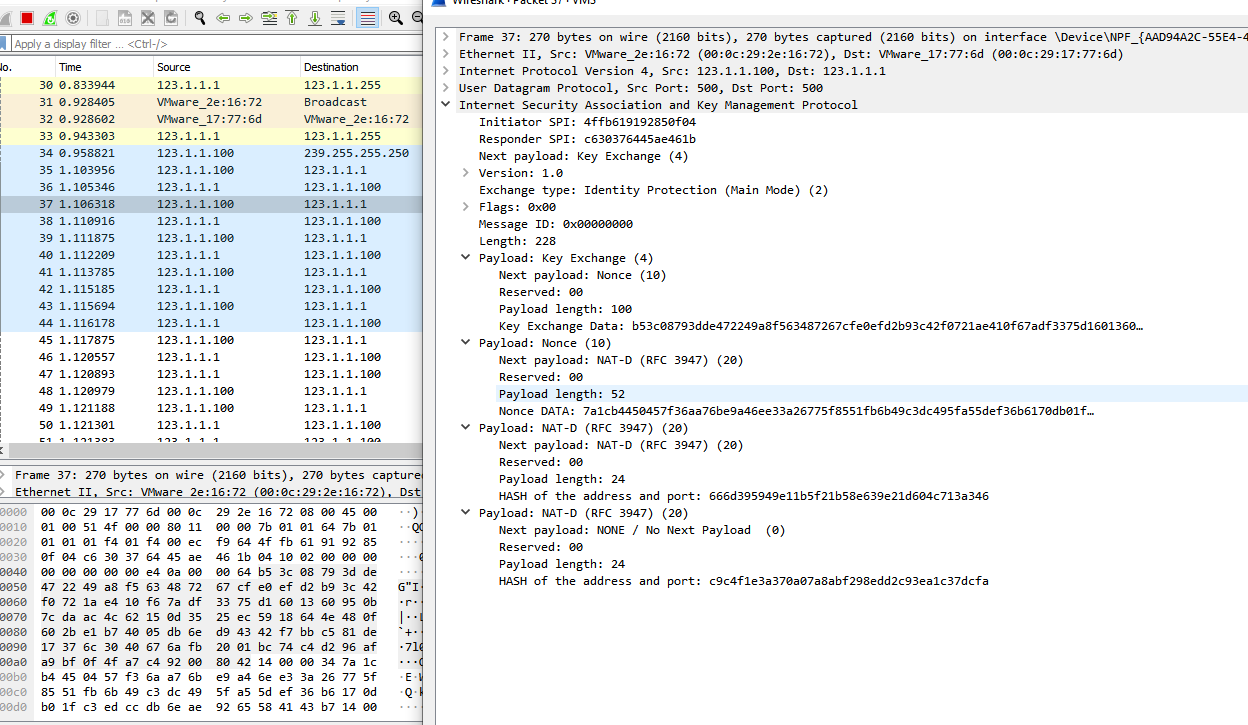
Ở message 1 .Bên A sẽ gửi message đầu tiên , sử dụng UDP port 500 .Trong message này có chuỗi SPI (Security Parameter Index), đây là giá trị duy nhất để xác định trong SA. Phiên bản sử dụng ở đây là ver1 và ở chế độ Main mode. Chúng ta có thể thấy được các thuộc tính(thuật toán mã hóa, hàm băm , các phương pháp xác nhận bảo vệ mã khóa.) sử dụng trong quá trình SA này ở phần Type Payload: transform

+ Messager 2:



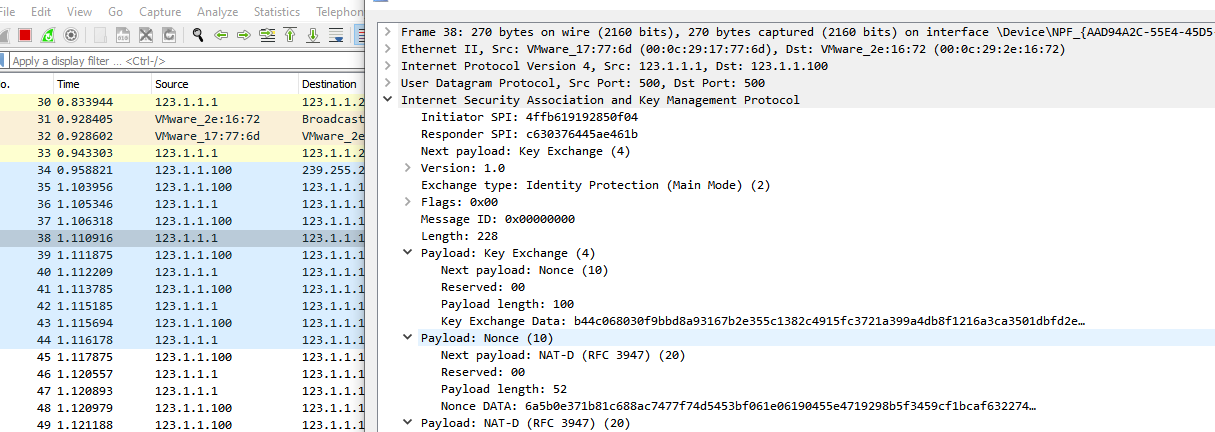
Sau khi bên B nhận được mesager từ bên A thì bên B tiến hành phản hồi lại. Messager này nhầm thông báo cho bên A về việc dồnd ý các thuốc tính trong payload transform như: thuật toán mã hóa, hash nào, giải mã, chiều dài của key. Và bên B cũng đã tự thiết lập SPI cho riêng mình.

+ Messager 3:



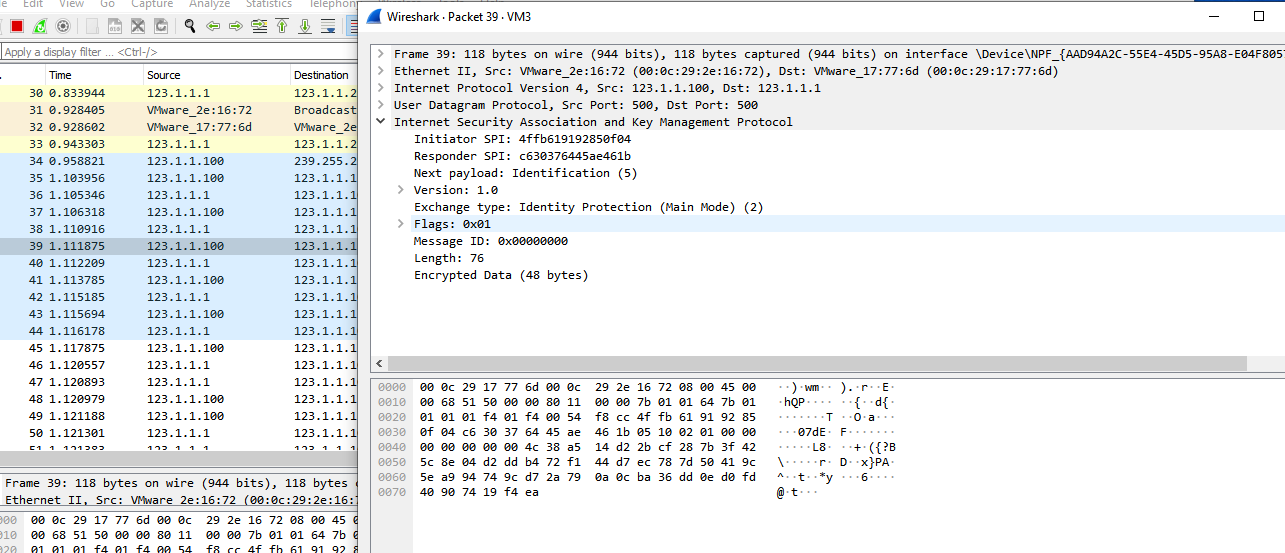
Sau khi cơ chế mã hóa và hãm băm đã được đồng ý ở trên, một khóa sẽ bí mật phát sinh. Bên A tiến hành dùng Diffie – Hellman, SPI của ISAKMP SA ở dạng cookies, số ngẫu nhiên known as nonces ( dùng ký xác nhận )

+ Messager 4



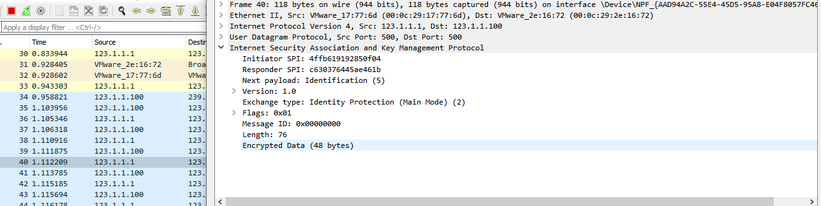
Bên B cũng sẽ gửi Diffie Hellman nonces cho bên A. Hai bên bắt đầu tính toán trong việc DiffieHellman shared key, 2 message cuối cùng được dùng để xác nhận lại các giao dịch đã sử dụng với sự giúp đỡ của chữ ký, các hàm băm và tùy chọn các chứng thực

+Message 5



Message 5 và 6 đã được mã hóa nên không thể xem được nội dung của chúng nữa.Cả 2 message cuối dùng để nhận dạng và xác thực của mỗi bên

+ Message 6



Bên B sẽ phản hồi các thông tin nhận dạng và xác thực của nó

Giai đoạn 2

Ở giai đoạn 2 dữ liệu người dùng sẽ được bảo vệ vì thế chỉ có 1 chế độ

Quick mode được sử dụng.

Cũng giống như giai đoạn 1 , ở giai đoạn 2 các Bên sẽ tiến hành thỏa

thuận các thông tin bảo mật IPSec như :

o IPsec Protocol : ESP hoặc AH

o IPSec mode: Tunnel hoặc transport.

o Trao đổi khóa Diffie-Hellman

o Encryption

o Authentication

o IPSec SA lifetime: dùng để thỏa thuận lại SA IPSec sau một

khoảng thời gian mặc định hoặc được chỉ định.

o (Optional) DH exchange.

o Session key được làm mới hoặc thay đổi, các SAs, key và SPI

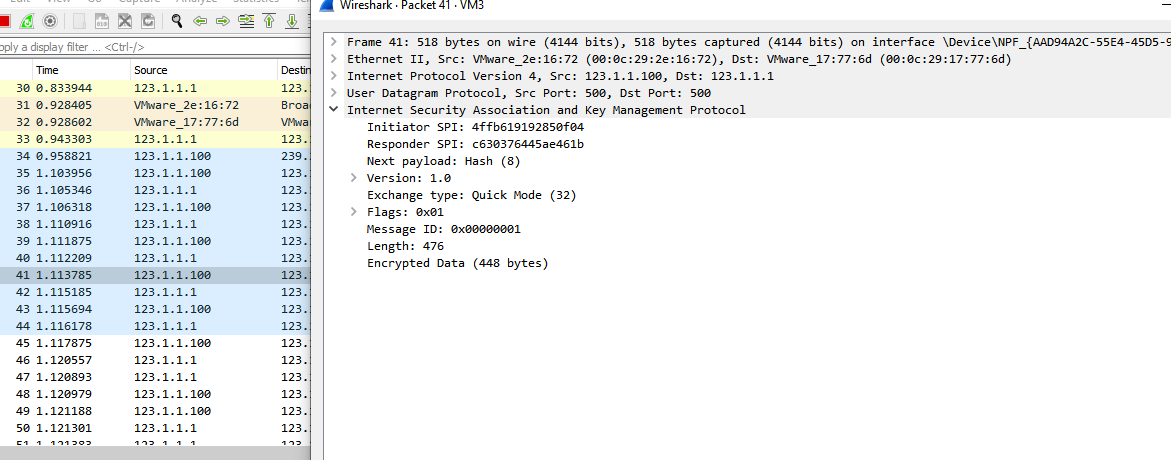
được thông qua cho IPSec.

SA IPSec của phase 2 hoàn toàn khác với SA IKE ở phase 1, SA

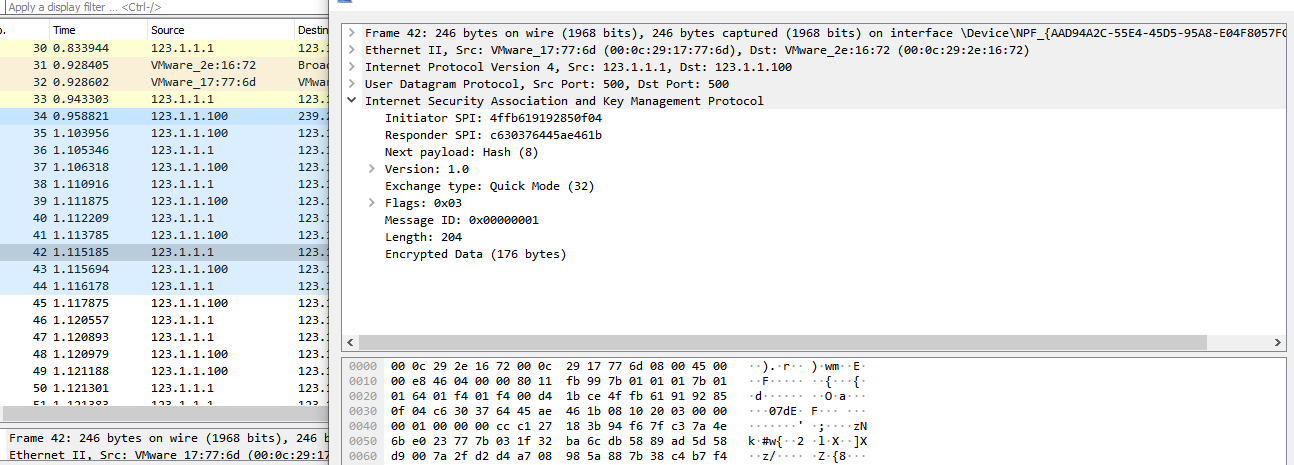
IKE chứa các thông số để tạo nên kênh truyền bảo mật, còn SA IPSec chứa các thông số để đóng gói dữ liệu theo ESP hay AH, hoạt động theo tunnel mode hay transport mode.

- Ở giai đoạn này các thỏa thuận sẽ xảy ra trong phạm vi bảo vệ của giai đoạn 1 vì vậy chúng ta sẽ không thấy bất cứ gì.

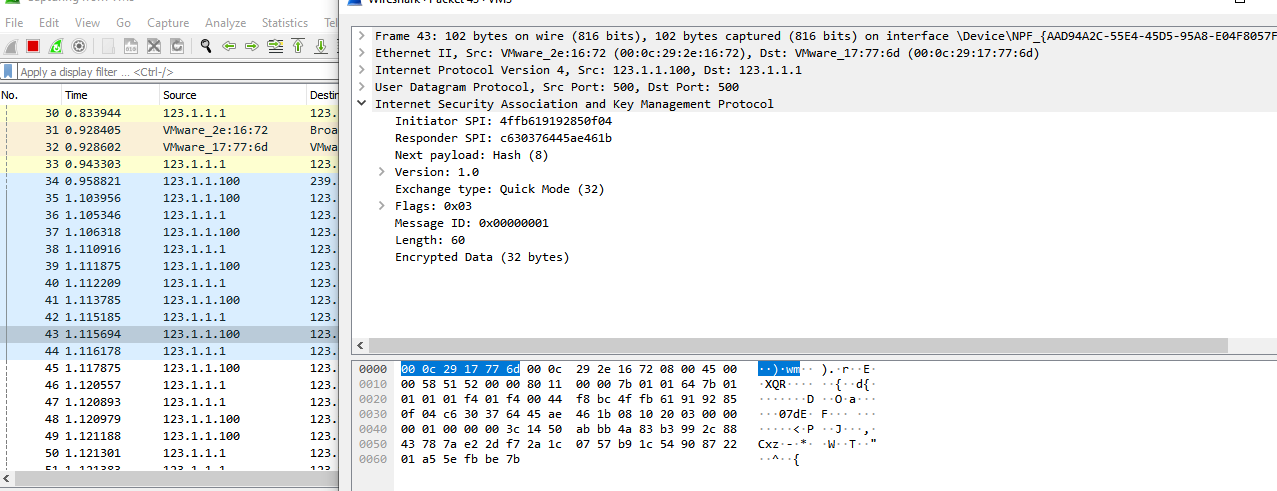
+ Message 7



+ Message 8



+ Message 9



3.5. Demo

**CHƯƠNG 4: KẾT LUẬN VÀ PHÁT TRIỂN**

* [https://123docz.net//document/3599575-ipsec-phan-tich-qua-trinh-isakmp-va-giai-ma-goi-tin-esp.htm](https://123docz.net/document/3599575-ipsec-phan-tich-qua-trinh-isakmp-va-giai-ma-goi-tin-esp.htm)
* <https://support.purevpn.com/how-to-setup-l2tp-on-kali-linux?fbclid=IwAR0QsMbs4xuJGT1FkPmcWEC-4GQvJSJChziNNI8tTNJkVKU9M3m2Tm1du2U>
* <https://quantrimang.com/huong-dan-cai-dat-ubuntu-tren-vmware-workstation-p1-116946?fbclid=IwAR2-CaFV377dKw7bkL-9iHRKQgFi4iEKBiwOd4gaeWmgq0Sc9Wvg7Td2nIc>
* <https://www.youtube.com/watch?v=zJ0aKaSucvg>